AWS プライバシーリファレンスアーキテクチャ

AWS 規範ガイダンス

AWS 規範ガイダンス: AWS プライバシーリファレンスアーキテクチャ

Table of Contents

序章 1
注意 1
序章 1
責任 AWS 共有モデルとプライバシー 1
PRA AWS について 3
PRA AWS と SRA AWS の使用 3
AWS Organizations と専用アカウント構造 4
AWS プライバシーサービスの運用 6
AWS プライバシーリファレンスアーキテクチャ 8
組織管理アカウント 10
AWS Artifact 11
AWS Control Tower 12
AWS Organizations 13
セキュリティ OU - Security Tooling アカウント 16
AWS CloudTrail 17
AWS Config 18
Amazon GuardDuty 19
IAM Access Analyzer 20
Amazon Macie 20
セキュリティ OU — ログアーカイブアカウント 21
一元化されたログストレージ 22
Amazon Security Lake 23
インフラストラクチャ OU — ネットワークアカウント 24
Amazon CloudFront 26
AWS Resource Access Manager 26
AWS Transit Gateway 27
AWS WAF 28
個人データ OU – PD アプリケーションアカウント 29
Amazon Athena 31
Amazon Bedrock 32
AWS Clean Rooms 33
Amazon CloudWatch Logs 34
Amazon CodeGuru Reviewer 35
Amazon Comprehend 35

Amazon Data Firehose 36
Amazon DataZone 36
AWS Glue 37
AWS Key Management Service 39
AWS Lake Formation 40
AWS Local Zones 41
AWS Nitro Enclaves 42
AWS PrivateLink 43
AWS Resource Access Manager 44
Amazon SageMaker AI 44
AWS データライフサイクルの管理に役立つ 機能 46
AWS のサービス データのセグメント化に役立つ および の機能 47
AWS のサービス データの検出、分類、カタログ化に役立つ および の機能 48
プライバシー関連のポリシーの例 49
特定の IP アドレスからのアクセスの要求 49
組織メンバーシップの VPC リソースへのアクセス要求 50
間でのデータ転送を制限する AWS リージョン 51
特定の Amazon DynamoDB 属性へのアクセス権の付与 53
VPC 設定の変更を制限する 55
AWS KMS キーを使用するには認証が必要です 56
グローバル展開の戦略 58
マネージドリージョンを持つ中央ランディングゾーン 59
リージョンのランディングゾーン 61
AWS 欧州主権雲 62
リソース 63
AWS 規範ガイダンス 63
AWS ドキュメント 63
その他の AWS リソース 63
寄稿者 64
ドキュメント履歴 65
用語集 66
..... 66
A 67
B 69
C 71
D 74

E 78
F 81
G 82
H 83
I 85
L 87
M 88
O 92
P 95
Q 98
R 98
S 101
T 105
U 106
V 107
W 107
Z 108
..... cix

AWS プライバシーリファレンスアーキテクチャ

Amazon Web Services (寄稿者)

2025 年 9 月 (ドキュメント履歴)

> **アンケート**
>
> 皆様からのご意見をお待ちしています。簡単なアンケートに回答して、PRA AWS に関するフィードバックを提供してください。

注意

このガイドは、情報提供のみを目的としています。これは法的な助言ではなく、法的な助言として頼るべきではありません。 は、プライバシーおよびデータ保護環境の実装、より一般的にはビジネスに関連する適用法について、適切な助言を受けるよう顧客に AWS 促します。

お客様は、本書に記載されている情報を独自に評価する責任を負うものとします。本書は、(a) 情報提供のみを目的としており、(b) 通知なしに変更される可能性がある現在の AWS 製品提供および慣行を表し、(c) AWS およびその関連会社、サプライヤー、または許諾者からのコミットメントまたは保証を作成しません。 AWS 製品またはサービスは、明示または黙示を問わず、いかなる種類の保証、表明、または条件もなしに「現状のまま」提供されます。

顧客 AWS に対する の責任と責任は契約によって AWS 管理され、本書は AWS とその顧客間の契約の一部でも変更もしません。

序章

AWS プライバシーリファレンスアーキテクチャ (AWS PRA) は、 でのプライバシーサポートコントロールの設計と設定に固有の一連のガイドラインを提供します AWS のサービス。このガイドは、AWS クラウドでプライバシーをサポートできる人、プロセス、テクノロジーに関する意思決定に役立ちます。

責任 AWS 共有モデルとプライバシー

では AWS クラウド、 のセキュリティとコンプライアンスの責任を共有します AWS。 AWS はクラウドのセキュリティを担当します。つまり、 AWS は で提供されるすべてのサービスを実行するイ

ンフラストラクチャを保護する責任を担います AWS クラウド。クラウドのセキュリティはお客様の責任となります。つまり、セキュリティとプライバシーの要件 AWS のサービス に従って設定および管理を行う責任があります。詳細については、AWS 「 責任共有モデル」を参照してください。

AWS のサービス は、プライバシー要件をサポートするために、独自のプライバシーコントロールをクラウドに実装できる機能を提供します。プライバシー責任は、選択した AWS のサービス および AWS リージョン 、それらのサービスの IT 環境への統合、組織やワークロードに適用される法律や規制など、さまざまな要因によって異なります。

を使用する場合は AWS のサービス、コンテンツの制御を維持します。具体的には、お客様のコンテンツは、ソフトウェア (マシンイメージを含む) 、データ、テキスト、オーディオ、ビデオ、またはイメージとして定義され、お客様またはエンドユーザーが、お客様のアカウント AWS のサービス に関連して によって処理、保存、またはホスティングのために当社に転送します。また、ユーザーまたはエンドユーザーが を使用して導き出す計算結果も含まれます AWS のサービス。お客様は、お客様の管理下にある以下の決定事項を管理する責任があります。

- で収集、保存、または処理するために選択したデータ AWS
- データ AWS のサービス で使用する
- データを収集、保存、または処理 AWS リージョン する 。
- データの形式と構造、およびマスキング、匿名化、暗号化を実行するかどうか
- 暗号化用に暗号化キーを定義、保存、ローテーション、運用する方法
- データにアクセスできるユーザー、データにアクセスするタイミング、それらのアクセス権の付与、管理、取り消しを実行する方法

責任 AWS 共有モデルとそのモデルがクラウドでの運用にどのように一般的に適用されるかを理解したら、ユースケースにどのように適用されるかを決定する必要があります。使用する AWS のサービス は、組織のプライバシー責任の一部として実行する必要がある設定の量を決定します。例えば、Amazon Elastic Compute Cloud (Amazon EC2) などのサービスは、Infrastructure as a Service (IaaS) に分類されます。そのため、Amazon EC2 を使用する場合は、ゲストオペレーティングシステムと EC2 インスタンスにインストールするアプリケーションソフトウェアまたはユーティリティに必要なプライバシー設定をすべて実行する必要があります。Amazon Simple Storage Service (Amazon S3) や Amazon DynamoDB などの抽象化されたサービスを使用する場合、 AWS はインフラストラクチャレイヤー、オペレーティングシステム、プラットフォームを担当します。お客様の責任は、データ (顧客のコンテンツ) を管理および分類し、データを保存および取得するためにエンドポイントへのアクセスに使用されるポリシーを設定することです。 AWS がデータとプライバシーを保護する方法の詳細については、「データ保護とプライバシー AWS」を参照してください。

PRA AWS について

> **アンケート**
>
> 皆様からのご意見をお待ちしています。簡単なアンケートに回答して、PRA AWS に関するフィードバックを提供してください。

このセクションでは、 AWS プライバシーリファレンスアーキテクチャ (AWS PRA) とその他の AWS ガイダンスの関係について説明します。このセクションでは、PRA AWS の AWS マルチアカウント環境の例の一般的なレイアウトと構造についても確認します。

このセクションは、以下のトピックで構成されます。

- PRA AWS と SRA AWS の使用
- AWS Organizations と専用アカウント構造
- AWS プライバシーサービスの運用

PRA AWS と SRA AWS の使用

> **アンケート**
>
> 皆様からのご意見をお待ちしています。簡単なアンケートに回答して、PRA AWS に関するフィードバックを提供してください。

AWS PRA は、インフラストラクチャとワークロードの基本的なプライバシーコントロールとアプリケーションレベルのプライバシーコントロールを計画する際に役立つパターンを提供します AWS。AWS セキュリティリファレンスアーキテクチャ (AWS SRA) は、 AWS ランディングゾーンとアプリケーション全体で適切な一連のセキュリティコントロールを実装およびサポートするアーキテクチャを構築するための一連のガイドラインを提供します。このガイドに詳述されているプライバシーコントロールを確立するために、PRA は AWS SRA AWS で説明されているのと同じ基本的なガイドラインとアカウント構造の多くを引き受けます。 AWS PRA と SRA AWS は、同じキーの多くを詳述します AWS のサービス。このガイドには、これらのサービスの簡単な説明のみが含まれています。これらのサービスの詳細と、 AWS SRA のセキュリティコンテキストでの使用方法について説明します。

AWS SRA は、 AWS セキュリティサービスを設計、実装、管理し、 AWS 推奨されるプラクティスに合わせるのに役立ちます。 AWS SRA をスタンドアロンガイドとして使用することも、SRA AWS と AWS PRA をコンパニオンガイドとして使用することもできます。SRA AWS に詳述されているセキュリティガイドラインの多くは、PRA AWS に詳述されているプライバシーコントロールと並行して従うことができます。これらの決定が組織のアカウント構造の設計に影響を与える可能性があるため、セキュリティと同様に、 AWS クラウド ジャーニーの早い段階で行うのに役立つ基本的なプライバシー上の考慮事項があります。例えば、次のような質問が考えられます。

- 組織では個人データをどのように定義していますか?
- 組織で、個人データを処理するアプリケーションをサポートしていますか?
- 他のタイプの規制対象データを処理するアプリケーションについてはどうですか?
- 開発者やクラウドエンジニアを個人データからできるだけ遠ざけるために、どのような組織レベルのコントロールを実装できますか?
- 個人データを他のタイプのデータから分離するにはどうすればよいですか?
- 組織の海外へのデータ転送要件は何ですか?

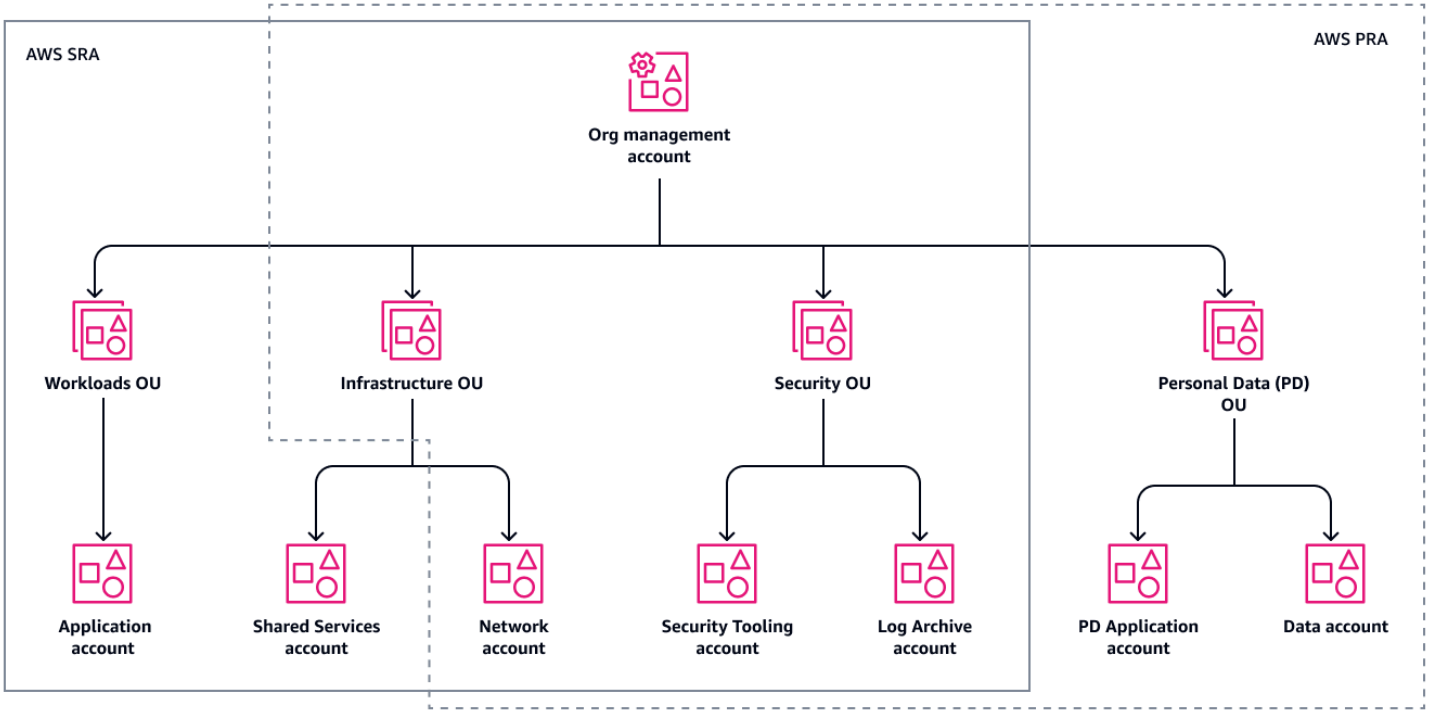
これらの質問の多くに対する回答は、 AWS アカウント 構造、サービスコントロールポリシー、AWS Identity and Access Management (IAM) ロールなど、クラウド環境の設計に影響を与える可能性があります。

AWS Organizations と専用アカウント構造

> **アンケート**
>
> 皆様からのご意見をお待ちしています。簡単なアンケートに回答して、PRA AWS に関するフィードバックを提供してください。

AWS Organizations は、複数の AWS アカウントを一元管理および統制するのに役立つアカウント管理サービスです。の使用は、適切に設計されたマルチアカウント AWS 環境の基礎 AWS Organizations です。詳細については、「ベストプラクティスの AWS 環境を確立する」を参照してください。

次の図は、PRA の大まかなアカウントと組織単位 (OU) AWS 構造を示しています。ほとんどの場合、PRA の組織構造は AWS SRA AWS の組織構造と一致します。



AWS SRA 組織からの逸脱には以下が含まれます。

- AWS PRA は、個人データの収集、保存、処理専用の個人データ (PD) OU を追加します。意図しない開示から個人データを保護するのに役立つ具体的かつきめ細かなコントロールを定義できるよう、この構造的な分離によって柔軟に対応します。
- インフラストラクチャ OU では、現在 PRA AWS には、SRA AWS で説明されている共有サービスアカウントに関する追加のガイダンスは含まれていません。
- PRA AWS には現在、SRA で説明されているワークロード OU AWS に関する追加のガイダンスは含まれていません。個人データを収集または処理するアプリケーションは、PD OU の専用アカウントにあります。

AWS Control Tower は、組織全体のセキュリティコントロールとプライバシーコントロールの、全体的な基盤ガバナンスおよび自動デプロイに使用できます。 AWS Control Tower が現在組織で使用されていない場合でも、サービスコントロールポリシーや AWS Config ルールなど AWS Control Tower、セキュリティおよびプライバシーコントロールの多くをそれぞれのサービスにデプロイできます。

アカウントと OU 構造をプラン作成するときは、アカウントセグメンテーション戦略など個人データの処理について検討すると役立つ場合があります。独自のユースケースや適用可能な法規制に対して、処理するデータの種類を検討する必要が生じる場合があります。例えば、カード所有者データは

Payment Card Industry Data Security Standard (PCI DSS) で保護されており、保護された医療情報は医療保険の相互運用性と説明責任に関する法令 (HIPAA) の対象となる場合があります。個人データを含む環境を確認し、それに関するセグメンテーション戦略を綿密に計画することが必要になる場合があります。一般的なアカウントセグメンテーション戦略には、開発、ステージング、品質保証 (QA)、および本番稼働に対する専用アカウントなど、ソフトウェア開発ライフサイクル (SDLC) に沿った専用の AWS アカウント を含めることができます。このようなセグメンテーション戦略は、設計に関する全体的な議論において重要な要素となる場合があり、OU では特定の規制要件に合わせる必要が生じる可能性があります。

一部のマルチアカウント AWS 環境では、 ごとに専用のアプリケーションアカウントが必要です。または AWS リージョン、マルチアカウントランディングゾーンが必要になる場合があります。この場合、顧客や規制当局の一意のデータ主権要件を満たすには、追加のセグメンテーションが必要です。詳細については、このガイドの「グローバル展開の戦略」を参照してください。

AWS プライバシーサービスの運用

> **アンケート**
>
> 皆様からのご意見をお待ちしています。簡単なアンケートに回答して、PRA AWS に関するフィードバックを提供してください。

多くの人にとって、プライバシーはクロスカットです。規制、コンプライアンス、エンジニアリングなど、さまざまなチームに果たすべき役割があります。組織でプライバシープログラムの主な担当者とポリシーコンポーネントの定義を開始したら、プライバシーコンプライアンスフレームワークに対するコントロールをマッピングして、一貫した運用を行うことができます。フレームワークは、AWS 環境内の個人データの基盤となるアプリケーション固有のプライバシーコントロールを実装するためのルーブリックとして機能します。

顧客がプライバシー要件の分類に使用するフレームワークにかかわらず、プライバシーコンプライアンスチーム、プライバシーエンジニアリングチーム、アプリケーションチームは、多くの場合、実装目標を達成するために協力する必要があります。例えば、規制チームとコンプライアンスチームが高レベルの要件を提供し、エンジニアリングチームとアプリケーションチームがこれらの要件に合わせて AWS のサービス と 機能を設定する場合があります。コントロールフレームワークから始めると、より規範的な組織的および技術的コントロールを定義できるようになります。

AWS のサービス および 機能の技術的コントロールを定義する際のもう 1 つの重要な決定は、コントロールを組織全体、OU、アカウント、または特定のリソースに適用するかどうかです。一部の

サービスと機能は、 AWS 組織全体にコントロールを実装するのに最適です。例えば、Amazon S3 バケットへのパブリックアクセスをブロックは、アカウントごとに個別に設定するのではなく、組織ルートで設定することが好ましい特定のコントロールです。ただし、保持ポリシーはアプリケーションによって異なる場合があります。つまり、リソースレベルでコントロールを適用できます。

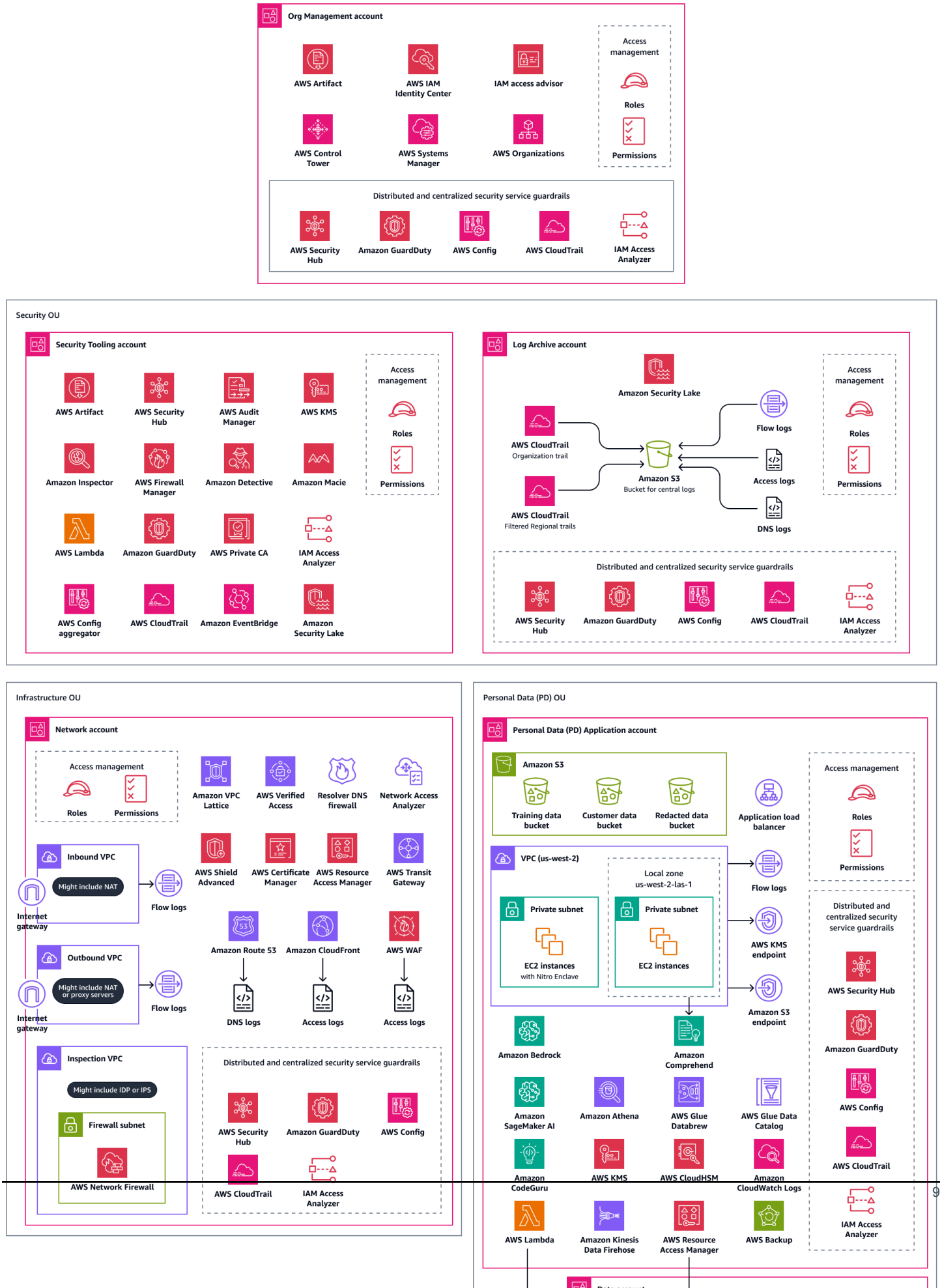
組織のプライバシーの運用を加速するために、 は AWS ワークロードの監査およびコンプライアンスアドバイザリサービス AWS を提供します。詳細については、AWS SAS にお問い合わせください。

AWS プライバシーリファレンスアーキテクチャ

アンケート

皆様からのご意見をお待ちしています。簡単なアンケートに回答して、PRA AWS に関するフィードバックを提供してください。

次の図は、 AWS プライバシーリファレンスアーキテクチャ (AWS PRA) を示しています。これは、多くのプライバシー関連の AWS のサービス および 機能を接続する アーキテクチャの例です。このアーキテクチャは、 AWS Control Towerによって管理されるランディングゾーン上に構築されています。


Org Management account
AWS Artifact
AWS IAM Identity Center
IAM access advisor
Access management
Roles
Permissions
AWS Control Tower
AWS Systems Manager
AWS Organizations
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Security OU
Security Tooling account
AWS Artifact
AWS Security Hub
AWS Audit Manager
AWS KMS
Access management
Roles
Permissions
Amazon Inspector
AWS Firewall Manager
Amazon Detective
Amazon Macie
AWS Lambda
Amazon GuardDuty
AWS Private CA
IAM Access Analyzer
AWS Config aggregator
AWS CloudTrail
Amazon EventBridge
Amazon Security Lake
Log Archive account
Amazon Security Lake
AWS CloudTrail
Organization trail
Flow logs
Access logs
Amazon S3
Bucket for central logs
AWS CloudTrail
Filtered Regional trails
DNS logs
Access management
Roles
Permissions
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Infrastructure OU
Network account
Access management
Roles
Permissions
Amazon VPC Lattice
AWS Verified Access
Resolver DNS firewall
Network Access Analyzer
Inbound VPC
Might include NAT
Internet gateway
Flow logs
AWS Shield Advanced
AWS Certificate Manager
AWS Resource Access Manager
AWS Transit Gateway
Outbound VPC
Might include NAT or proxy servers
Internet gateway
Flow logs
Amazon Route 53
Amazon CloudFront
AWS WAF
DNS logs
Access logs
Access logs
Inspection VPC
Might include IDP or IPS
Firewall subnet
AWS Network Firewall
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Personal Data (PD) OU
Personal Data (PD) Application account
Amazon S3
Training data bucket
Customer data bucket
Redacted data bucket
Application load balancer
Access management
Roles
Permissions
VPC (us-west-2)
Local zone us-west-2-las-1
Private subnet
EC2 instances with Nitro Enclave
Private subnet
EC2 instances
Flow logs
AWS KMS endpoint
Amazon S3 endpoint
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Amazon Bedrock
Amazon Comprehend
Amazon SageMaker AI
Amazon Athena
AWS Glue Databrew
AWS Glue Data Catalog
Amazon CodeGuru
AWS KMS
AWS CloudHSM
Amazon CloudWatch Logs
AWS Lambda
Amazon Kinesis Data Firehose
AWS Resource Access Manager
AWS Backup

AWS PRA には、個人データ (PD) アプリケーションアカウントでホストされるサーバーレスウェブアーキテクチャが含まれています。このアカウントのアーキテクチャは、コンシューマーから直接個人データを収集するワークロードの例です。このワークロードでは、ユーザーはウェブ層を介して接続されます。ウェブ層はアプリケーション層と相互に作用します。アプリケーション層は、ウェブ層からの入力を受け取り、データを処理および保存します。また、承認を受けた内部チームおよびサードパーティーによるデータへのアクセスを許可し、最終的に不要になったデータをアーカイブおよび削除します。これは、データレイク、コンテナ、コンピューティング、モノのインターネット (IoT) などの特定のユースケースを掘り下げるのではなく、基本的なプライバシーエンジニアリング手法の多くを実証するために意図的にモジュール化された、イベント駆動型のアーキテクチャです。

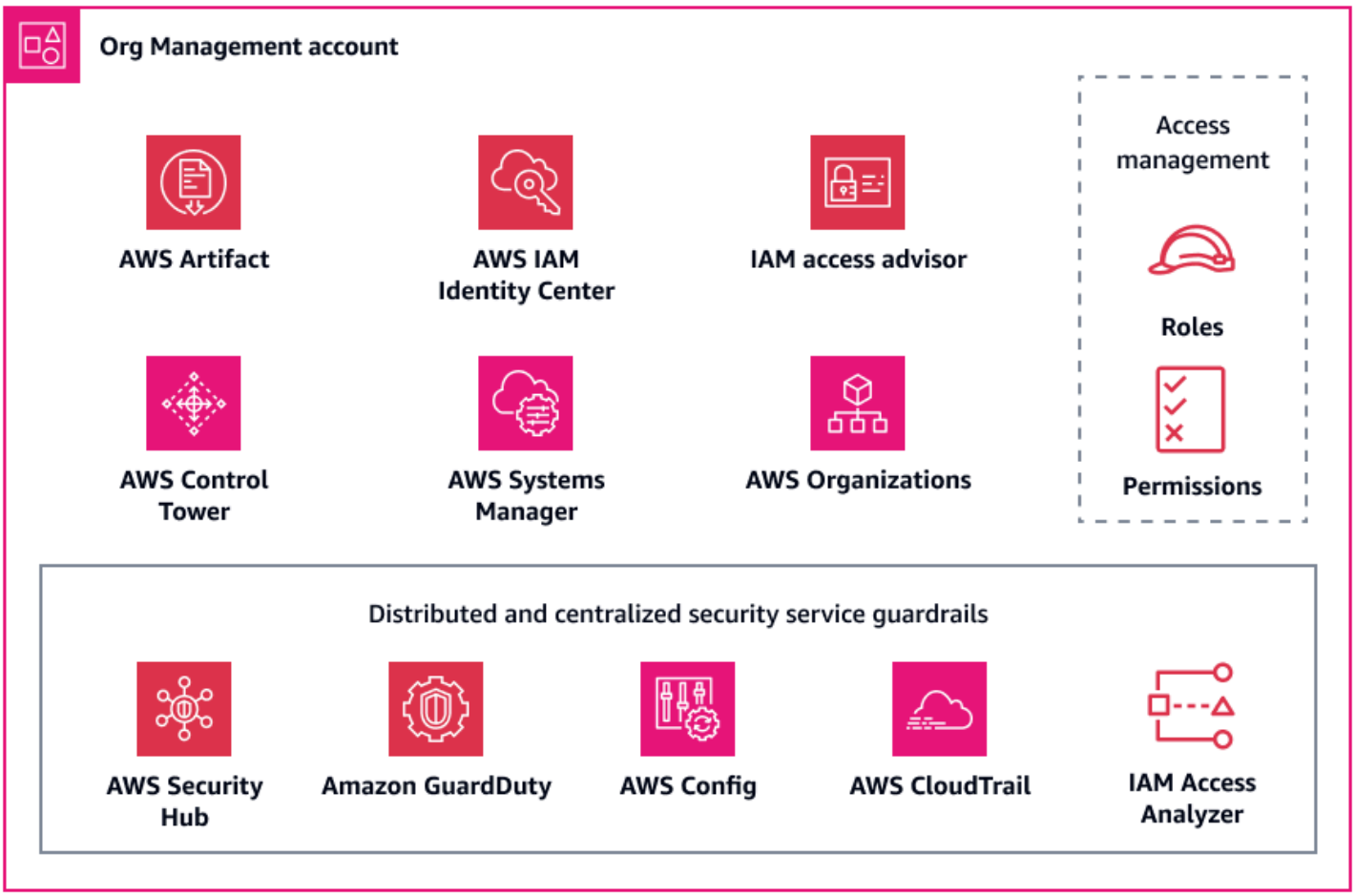
次に、このガイドでは、組織内の各アカウントについて詳しく説明します。以下の各アカウントのプライバシー関連のサービスと機能、考慮事項と推奨事項、および図について説明します。

- 組織管理アカウント
- セキュリティ OU - Security Tooling アカウント
- セキュリティ OU — ログアーカイブアカウント
- インフラストラクチャ OU — ネットワークアカウント
- 個人データ OU – PD アプリケーションアカウント

組織管理アカウント

> **アンケート**
>
> 皆様からのご意見をお待ちしています。簡単なアンケートに回答して、PRA AWS に関するフィードバックを提供してください。

組織管理アカウントは、 AWS Organizationsによって管理される組織内のすべてのアカウントに対して基本的なプライバシーコントロールのリソース設定ドリフトを管理するために使用されます。また、このアカウントは、多数の同一セキュリティコントロールおよびプライバシーコントロールにより、新しいメンバーアカウントを一貫してデプロイできる場所でもあります。このアカウントの詳細については、AWS 「セキュリティリファレンスアーキテクチャ (AWS SRA)」を参照してください。次の図は、組織管理アカウントで設定されている AWS セキュリティおよびプライバシーサービスを示しています。



このセクションでは、このアカウントで使用される以下の AWS のサービス に関する詳細情報を提供します。

- AWS Artifact
- AWS Control Tower
- AWS Organizations

AWS Artifact

AWS Artifact は、 AWS のセキュリティおよびコンプライアンスドキュメントのオンデマンドダウンロードを提供することで、監査に役立てることができます。セキュリティコンテキストでのこのサービスの使用方法についての詳細は、「AWS セキュリティリファレンスアーキテクチャ」を参照してください。

これにより AWS のサービス 、 から AWS 継承するコントロールを理解し、環境に実装するためにどのようなコントロールが残っているかを判断することができます。 は、System and Organization

Controls (SOC) レポートや Payment Card Industry (PCI) レポートなどの AWS セキュリティおよびコンプライアンスレポートへのアクセス AWS Artifact を提供します。また、 AWS コントロールの実装と運用の有効性を検証する、地理的およびコンプライアンス垂直的な認証機関からの証明書へのアクセスも提供します。を使用すると AWS Artifact、 AWS セキュリティおよびプライバシーコントロールの証拠として AWS 、監査アーティファクトを監査人または規制当局に提供 できます。以下のレポートは、 AWS プライバシーコントロールの有効性を示すのに役立つ場合があります。

- SOC 2 タイプ 2 プライバシーレポート – このレポートは、個人データの収集、使用、保持、開示、破棄方法に対する AWS コントロールの有効性を示しています。また、SOC 2 プライバシーコントロールについて大まかに説明した SOC 3 プライバシーレポートもあります。詳細については、「SOC FAQ」を参照してください。
- クラウドコンピューティングコンプライアンスコントロールカタログ (C5) – このレポートは、ドイツの国立サイバーセキュリティ機関である Bundesamt für Sicherheit in der Informationstechnik (BSI) によって作成されました。C5 の要件を満たすために AWS で実装されたセキュリティコントロールについて詳しく説明しています。また、データの場所、サービスのプロビジョニング、管轄区域、情報開示義務に関連した、プライバシーに対する追加のコントロール要件も含まれています。
- ISO/IEC 27701:2019 認定レポート –ISO/IEC 27701:2019 では、プライバシー情報管理システム (PIMS) を確立し、継続的に改善していくための要件とガイドラインについて説明しています。このレポートは、この証明書の範囲を詳述し、 AWS 証明書の証明として役立ちます。この標準の詳細については、ISO/IEC 27701:2019 (ISO ウェブサイト) を参照してください。

AWS Control Tower

AWS Control Tower は、規範的なセキュリティの推奨プラクティスに従う AWS マルチアカウント環境のセットアップと管理に役立ちます。セキュリティコンテキストでのこのサービスの使用方法についての詳細は、「AWS セキュリティリファレンスアーキテクチャ」を参照してください。

では AWS Control Tower、特にデータレジデンシーと主権に関するデータプライバシー要件に沿った、ガードレールとも呼ばれる多くのプロアクティブ、予防的、検出的なコントロールのデプロイを自動化することもできます。例えば、データ転送を承認された AWS リージョンのみに制限するガードレールを指定できます。さらにきめ細かな制御のために、Amazon Virtual Private Network (VPN) 接続の禁止、Amazon VPC インスタンスのインターネットアクセスの禁止、リクエストされた に基づく へのアクセスの拒否など、データレジデンシーを制御するように設計された 17 を超える ガードレールから選択できます。 AWS AWS リージョンこれらのガードレールは、組織全体に均一にデプロイできる多数の AWS CloudFormation フック、サービスコントロールポリシー、および AWS

Config ルールで構成されます。詳細については、 AWS Control Tower ドキュメントの「データレジデンシー保護を強化するコントロール」を参照してください。

データ主権については、 AWS Control Tower 現在、 は、アタッチされた Amazon EBS ボリュームが保管中のデータを暗号化するように設定されていること、および AWS KMS キーポリシーに AWS KMS 許可の作成を制限するステートメントがあることを要求する AWS のサービスなどの予防的コントロールを提供しています。主権コントロールは、単なるデータレジデンシーコントロールよりも広範です。データレジデンシー、きめ細かなアクセス制限、暗号化、耐障害性の要件に違反する可能性のあるアクションを防ぐのに役立ちます。詳細については、 AWS Control Tower ドキュメントの「デジタル主権を支援する予防的コントロール」を参照してください。

データレジデンシーと主権コントロールを超えてプライバシーガードレールをデプロイする必要がある場合、 にはいくつかの必須コントロール AWS Control Tower が含まれています。これらのコントロールは、ランディングゾーンを設定するときに、デフォルトですべての OU にデプロイされます。これらの多くは、「ログアーカイブの削除を許可しない」や「CloudTrail のログファイルの整合性検証を有効にする」など、ログを保護するように設計された予防的コントロールです。

AWS Control Tower は、検出コントロール AWS Security Hub CSPM を提供するために とも統合されています。これらのコントロールは、サービスマネージドスタンダード AWS Control Towerと呼ばれます。これらのコントロールを使用して、Amazon Relational Database Service (Amazon RDS) データベースインスタンスの保管時の暗号化など、プライバシーをサポートするコントロールの設定のドリフトをモニタリングできます。

AWS Organizations

AWS PRA は を使用して AWS Organizations 、アーキテクチャ内のすべてのアカウントを一元管理します。詳細については、このガイドの「AWS Organizations と専用アカウント構造」を参照してください。では AWS Organizations、サービスコントロールポリシー (SCPsと管理ポリシーを使用して、個人データとプライバシーを保護することができます。

サービスコントロールポリシー (SCP)

サービスコントロールポリシー (SCP) は、組織のアクセス許可の管理に使用できる組織ポリシーの一種です。ターゲットアカウント、組織単位 (OU)、または組織全体の AWS Identity and Access Management (IAM) ロールとユーザーに対して、使用可能なアクセス許可の最大数を一元的に制御できます。組織管理アカウントから SCP を作成して適用できます。

AWS Control Tower を使用して、アカウント間で SCPs均一にデプロイできます。適用できるデータレジデンシーコントロールの詳細については AWS Control Tower、AWS Control Towerこのガイドの

SCPs の完全な補完 AWS Control Tower が含まれています。 AWS Control Tower が組織で現在使用されていない場合は、これらのコントロールを手動でデプロイすることもできます。

SCP を使用してデータレジデンシー要件に対処する

特定の地理的リージョン内にデータを保存して処理することで、個人データレジデンシーの要件を管理するのが一般的です。管轄区域固有のデータレジデンシー要件が満たされていることを確認するには、規制チームと緊密に連携して要件を確認することをお勧めします。これらの要件が決定されると、サポートに役立つ AWS 基本的なプライバシーコントロールが多数あります。たとえば、SCPs を使用して、データの処理と保存 AWS リージョン に使用できる を制限できます。サンプルポリシーについては、このガイドの「間でのデータ転送を制限する AWS リージョン」を参照してください。

SCP を使用して高リスクの API コールを制限する

どのセキュリティコントロールとプライバシーコントロール AWS に責任があり、どのセキュリティコントロールとプライバシーコントロールに責任があるのかを理解することが重要です。例えば、利用する AWS のサービス に対して実行できる API コールの結果は、お客様の責任となります。また、これらのコールのうち、セキュリティ体制またはプライバシー体制の変更につながる可能性があるコールについて理解しておくことも、お客様の責任となります。特定のセキュリティ体制およびプライバシー体制を維持することに懸念がある場合は、特定の API コールを拒否する SCP を有効にできます。これらの API コールには、個人データの意図しない開示や特定の海外へのデータ転送違反といった内容が含まれる場合があります。例えば、次の API コールを禁止する必要が生じる場合があります。

- Amazon Simple Storage Service (Amazon S3) バケットへのパブリックアクセスの有効化
- Amazon GuardDuty の無効化、またはデータ漏えいを検出するための抑制ルールの作成 (Trojan:EC2/DNSDataExfiltration の検出など)
- AWS WAF データ流出ルールの削除
- Amazon Elastic Block Store (Amazon EBS) スナップショットのパブリック共有
- 組織からのメンバーアカウントの削除
- リポジトリからの Amazon CodeGuru Reviewer の関連付け解除

管理ポリシー

の管理ポリシー AWS Organizations は、 AWS のサービス とその機能を一元的に設定および管理するために役立ちます。ポリシーが OU とそれを継承するアカウントに与える影響は、選択した管理

ポリシーの種類によって異なります。タグポリシーは、プライバシー AWS Organizations に直接関連する の管理ポリシーの例です。

タグポリシーの使用

タグは、 AWS リソースの管理、識別、整理、検索、フィルタリングに役立つキーと値のペアです。個人データを処理する組織内のリソースを区別するタグを適用すると便利です。タグの使用は、このガイドの多くのプライバシーソリューションをサポートしています。例えば、リソース内で処理または保存されているデータの一般的なデータ分類を示すタグを適用するとします。特定のタグまたはタグのセットを使用するリソースへのアクセスを制限する、属性ベースのアクセス制御 (ABAC) ポリシーを作成できます。例えば、ポリシーで、SysAdmin ロールでは dataclassification:4 タグを使用するリソースにアクセスできないように指定できます。詳細とチュートリアルについては、IAM ドキュメントの「タグに基づいて AWS リソースにアクセスするためのアクセス許可を定義する」を参照してください。さらに、組織が AWS Backup を使用して多くのアカウントのバックアップにデータ保持ポリシーを広く適用する場合、そのリソースをそのバックアップポリシーの範囲内に配置するタグを適用できます。

タグポリシーは、組織全体で一貫したタグを維持するのに役立ちます。タグポリシーでは、リソースをタグ付けする際に適用するルールを指定します。例えば、リソースに DataClassification や DataSteward などの特定のキーによるタグ付けを要求したり、有効な大文字と小文字の処理やキーの値を指定したりできます。また、強制適用を使用して、非準拠のタグ付けリクエストが完了しないようにすることもできます。

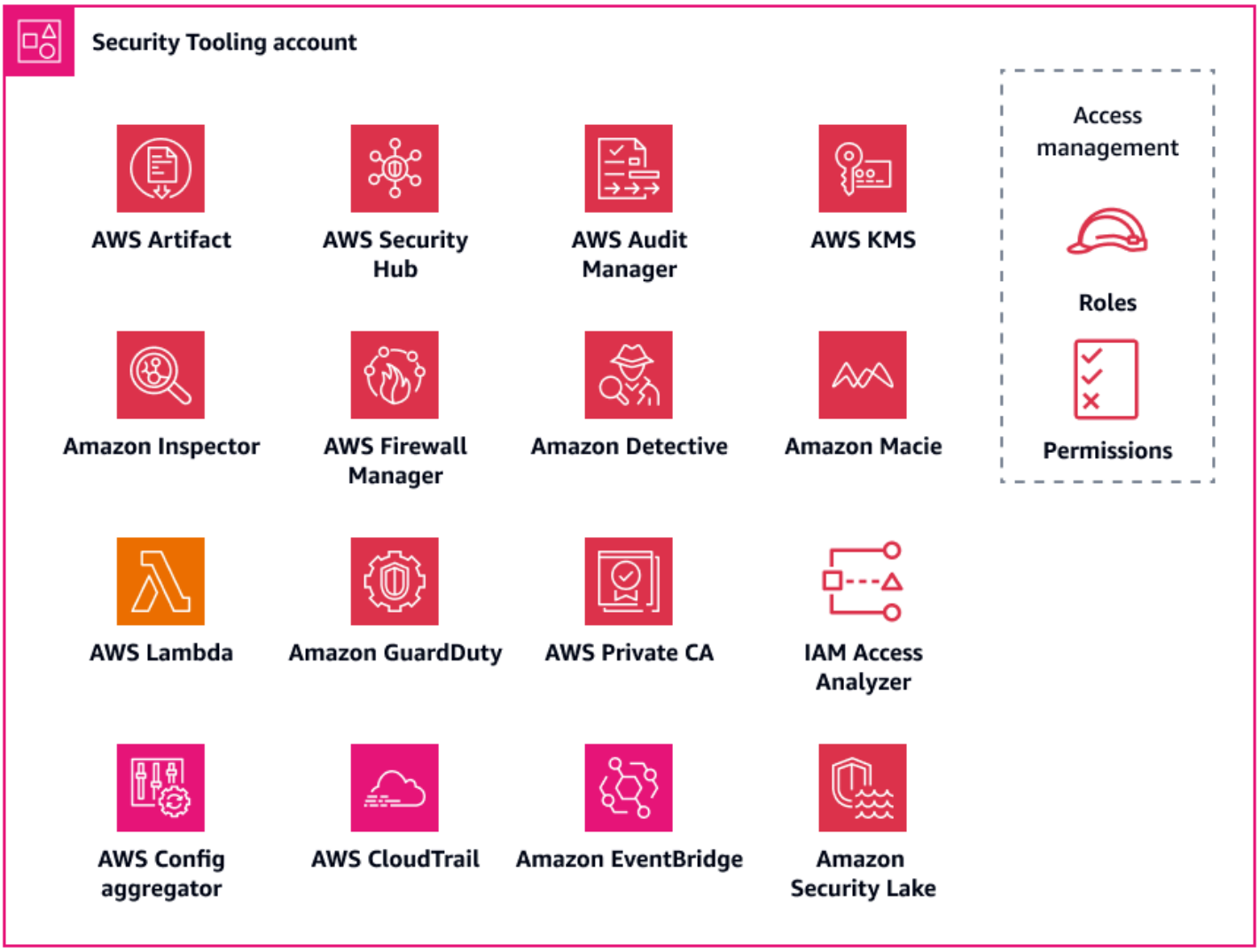
タグをプライバシーコントロール戦略のコアコンポーネントとして使用する場合は、次の点を考慮してください。

- 個人データやその他のタイプの機密データをタグキーまたは値に配置することの影響を考慮してください。テクニカルサポートが必要な場合は AWS 、タグやその他のリソース識別子を分析して問題の解決に役立て AWS てください。タグデータは暗号化されず AWS のサービス、 など AWS Billing and Cost Managementで読み取ることができます。したがって、タグ値を識別解除し、IT サービス管理 (ITSM) system など、自分で管理するシステムを使用して再識別することをお勧めします。 では、タグに個人を特定できる情報を含めない AWS ことをお勧めします。
- タグに依存する ABAC 条件など、技術的なコントロールの回避を防止するには、一部のタグ値をイミュータブル (変更不可) にする必要があることに注意してください。

セキュリティ OU - Security Tooling アカウント

> **アンケート**
>
> 皆様からのご意見をお待ちしています。簡単なアンケートに回答して、PRA AWS に関するフィードバックを提供してください。

Security Tooling アカウントは、セキュリティとプライバシーの基本的なサービスの運用、セキュリティ AWS アカウントとプライバシーのアラートと対応のモニタリングと自動化に専念しています。このアカウントの詳細については、AWS 「セキュリティリファレンスアーキテクチャ (AWS SRA)」を参照してください。次の図は、 AWS Security Tooling アカウントで設定されているセキュリティおよびプライバシーサービスを示しています。



このセクションでは、このアカウントの以下に関する詳細情報を提供します。

- AWS CloudTrail
- AWS Config
- Amazon GuardDuty
- IAM Access Analyzer
- Amazon Macie

AWS CloudTrail

AWS CloudTrail は、 の全体的な API アクティビティを監査するのに役立ちます AWS アカウント。個人データを保存、処理、または送信 AWS リージョン するすべての AWS アカウント および で CloudTrail を有効にすると、このデータの使用と開示を追跡するのに役立ちます。AWS セキュリティリファレンスアーキテクチャでは、組織の証跡を有効にすることをお勧めします。これは、組織内のすべてのアカウントのすべてのイベントを記録する単一の証跡です。ただし、この組織の証跡を有効にすると、マルチリージョンのログデータがログアーカイブアカウントの単一の Amazon Simple Storage Service (Amazon S3) バケットに集約されます。個人データを処理するアカウントの場合は、設計上の考慮事項がいくつか追加される可能性があります。ログレコードには、個人データへの参照が含まれている場合があります。データレジデンシーとデータ転送の要件を満たすには、S3 バケットがある単一リージョンへのクロスリージョンログデータの集約を再検討する必要が生じる場合があります。組織は、どのリージョンのワークロードを組織の証跡に含めるか除外するかを検討する場合があります。組織の証跡から除外するワークロードについては、個人データをマスクするリージョン固有の証跡の設定を検討できます。個人データのマスキングに関する詳細については、このガイドの「Amazon Data Firehose」セクションを参照してください。最終的に、組織には、一元化されたログアーカイブアカウントに集約される組織の証跡とリージョンの証跡の組み合わせが含まれる可能性があります。

単一リージョンの証跡を設定する方法の詳細については、AWS Command Line Interface (AWS CLI) または コンソールを使用する手順を参照してください。組織の証跡を作成するときは、AWS Control Tower でオプトイン設定を使用するか、CloudTrail コンソールで証跡を直接作成できます。

全体的なアプローチと、ログおよびデータ転送要件の一元化を管理する方法の詳細については、このガイドの「一元化されたログストレージ」セクションを参照してください。どの設定を選択しても、SRA に従って Security Tooling アカウントの証跡管理を Log Archive AWS アカウントのログストレージから分離できます。この設計を使用して、ログを管理する必要があるユーザーとログデータを使用する必要があるユーザーのために、最小特権のアクセスポリシーを作成することができます。

AWS Config

AWS Config では、 AWS アカウント におけるリソースとその構成方法についての詳細なビューを提供します。リソースがどのように相互に関連しているか、またそれらの構成が時間の経過とともにどのように変化したかを特定するのに役立ちます。セキュリティコンテキストでのこのサービスの使用方法についての詳細は、「AWS セキュリティリファレンスアーキテクチャ」を参照してください。

では AWS Config、一連の AWS Config ルールと修復アクションであるコンフォーマンスパックをデプロイできます。コンフォーマンスパックは、マネージドルールまたはカスタム AWS Config ルールを使用して、プライバシー、セキュリティ、運用、コスト最適化のガバナンスチェックを可能にするように設計された汎用フレームワークを提供します。このツールは、大規模な自動化ツールのセットの一部として使用して、 AWS リソース設定が独自のコントロールフレームワーク要件に準拠しているかどうかを追跡できます。

NIST プライバシーフレームワーク v1.0 オペレーションのベストプラクティスコンフォーマンスパックは、NIST プライバシーフレームワークの多くのプライバシー関連コントロールと一致しています。各 AWS Config ルールは特定の AWS リソースタイプに適用され、1 つ以上の NIST プライバシーフレームワークコントロールに関連しています。このコンフォーマンスパックを使用して、アカウントのリソース全体でプライバシー関連の継続的なコンプライアンスを追跡できます。以下は、このコンフォーマンスパックに含まれるルールの一部です。

- `no-unrestricted-route-to-igw` – このルールは、VPC ルートテーブルのデフォルトルートである `0.0.0.0/0` またはインターネットゲートウェイへの出力ルートである `::/0` を継続的にモニタリングすることで、データプレーン上のデータ流出を防ぐのに役立ちます。これにより、特に悪意のあることがわかっている CIDR 範囲がある場合に、インターネットにバインドされたトラフィックを送信できる場所を制限できます。
- `encrypted-volumes` – このルールは、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされている Amazon Elastic Block Store (Amazon EBS) ボリュームが暗号化されているかどうかを確認します。組織に個人データを保護するための AWS Key Management Service (AWS KMS) キーの使用に関連する特定の制御要件がある場合は、ルールの一部として特定のキー IDs を指定して、ボリュームが特定の AWS KMS キーで暗号化されていることを確認することができます。
- `restricted-common-ports` – このルールでは、Amazon EC2 セキュリティグループが指定されたポートへの無制限の TCP トラフィックを許可しているかどうかをチェックします。セキュリティグループは、入出力ネットワークトラフィックを AWS リソースにステートフルにフィルタリングすることで、ネットワークアクセスの管理に役立ちます。`0.0.0.0/0` からリソース上の TCP

3389 や TCP 21 などの共通ポートへの入力トラフィックをブロックすると、リモートアクセスを制限できます。

AWS Config は、 AWS リソースのプロアクティブコンプライアンスチェックとリアクティブコンプライアンスチェックの両方に使用できます。コンフォーマンスパックに含まれるルールを考慮するだけでなく、これらのルールを検出評価モードとプロアクティブ評価モードの両方に組み込むことができます。これにより、アプリケーション開発者はデプロイ前チェックの組み込みを開始できるため、ソフトウェア開発ライフサイクルの早い段階でプライバシーチェックを実装できます。たとえば、プロアクティブモードが有効になっているすべてのプライバシー関連 AWS Config ルールに対して AWS CloudFormation テンプレート内の宣言されたリソースをチェックするフックをテンプレートに含めることができます。詳細については、AWS Config 「 Rules Now Support Proactive Compliance」(AWS ブログ記事) を参照してください。

Amazon GuardDuty

AWS は、Amazon S3、Amazon Relational Database Service (Amazon RDS)、Kubernetes を使用した Amazon EC2 など、個人データの保存または処理に使用できる複数のサービスを提供します。Amazon GuardDuty は、インテリジェントな可視性と継続的なモニタリングを組み合わせて、個人データの意図しない開示に関連する可能性のある指標を検出します。セキュリティコンテキストでのこのサービスの使用方法についての詳細は、「AWS セキュリティリファレンスアーキテクチャ」を参照してください。

GuardDuty を使用すると、攻撃ライフサイクル全体で潜在的に悪意のあるプライバシー関連のアクティビティを特定できます。例えば、GuardDuty は、ブラックリストに登録されたサイトへの接続、異常なネットワークポートトラフィックまたはトラフィックボリューム、DNS 漏洩、予期しない EC2 インスタンスの起動、異常な ISP 発信者について警告できます。また、GuardDuty を設定して、独自の信頼できる IP リストに対するアラートと独自の脅威リストからの悪意のある既知の IP アドレスについてのアラートを停止することもできます。

AWS SRA で推奨されているように、組織 AWS アカウント 内のすべての に対して GuardDuty を有効にし、Security Tooling アカウントを GuardDuty 委任管理者として設定できます。GuardDuty では、組織全体の調査結果をこの 1 つのアカウントに集約します。詳細については、「 を使用した GuardDuty アカウントの管理 AWS Organizations」を参照してください。また、検出と分析から封じ込めと根絶まで、インシデント対応プロセスにおけるプライバシー関連のステークホルダーをすべて特定し、データ漏洩を伴う可能性のあるインシデントにそれらを含めることを検討することもできます。

IAM Access Analyzer

多くのお客様は、個人データが事前に承認され、意図されたサードパーティープロセッサと適切に共有され、他のエンティティとは共有されていないということが継続的に保証されることを望んでいます。データ境界とは、お使いの AWS 環境において、信頼できるアイデンティティのみが、期待されるネットワークから信頼できるリソースにアクセスできるよう設計された、予防的な一連のガードレールです。個人データの意図しない開示および意図された開示に対するコントロールを定義すると、信頼できる ID、信頼できるリソース、および期待されるネットワークを定義できます。

AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) を使用すると、組織は信頼 AWS アカウント ゾーンを定義し、その信頼ゾーンに対する違反のアラートを設定できます。IAM Access Analyzer では、IAM ポリシーを分析して機密性の高いリソースへの意図しないパブリックアクセスまたはクロスアカウントアクセスを特定し、解決することができます。IAM Access Analyzer は、数理論理と推論を使用して、 AWS アカウント以外からアクセスできるリソースの包括的な検出結果を生成します。最後に、過度に許可された IAM ポリシーに対応し、修復するために、IAM Access Analyzer を使用して、IAM の推奨プラクティスに照らして既存のポリシーを検証し、提案を提供できます。IAM Access Analyzer は、IAM プリンシパルの以前のアクセスアクティビティに基づいて、最小特権の IAM ポリシーを生成できます。CloudTrail ログを分析し、これらのタスクを引き続き実行するために必要なアクセス許可のみを付与するポリシーを生成します。

セキュリティコンテキストでの IAM Access Analyzer の使用方法に関する詳細については、「AWS セキュリティリファレンスアーキテクチャ」を参照してください。

Amazon Macie

Amazon Macie は、機械学習とパターンマッチングを使用して機密データを検出し、データセキュリティリスクを可視化し、それらのリスクに対する自動保護を可能にするサービスです。Macie では、Amazon S3 バケットのセキュリティまたはプライバシーに関して潜在的なポリシー違反や問題を検出した場合に、その検出結果を生成します。Macie は、組織がコンプライアンスの取り組みをサポートするための自動化の実装に使用できる、もう一つのツールです。セキュリティコンテキストでのこのサービスの使用方法についての詳細は、「AWS セキュリティリファレンスアーキテクチャ」を参照してください。

Macie は、名前、住所、その他の識別可能な属性など、個人を特定できる情報 (PII) を含む機密データタイプの、大規模かつ増え続けるリストを検出できます。組織による個人データの定義を反映する検出基準を定義するために、カスタムデータ識別子を作成することもできます。

組織は、個人データを含む Amazon S3 バケットの予防的コントロールを定義するため、Macie を検証メカニズムとして使用し、個人データの所在と保護方法を継続的に確認することができます。開始

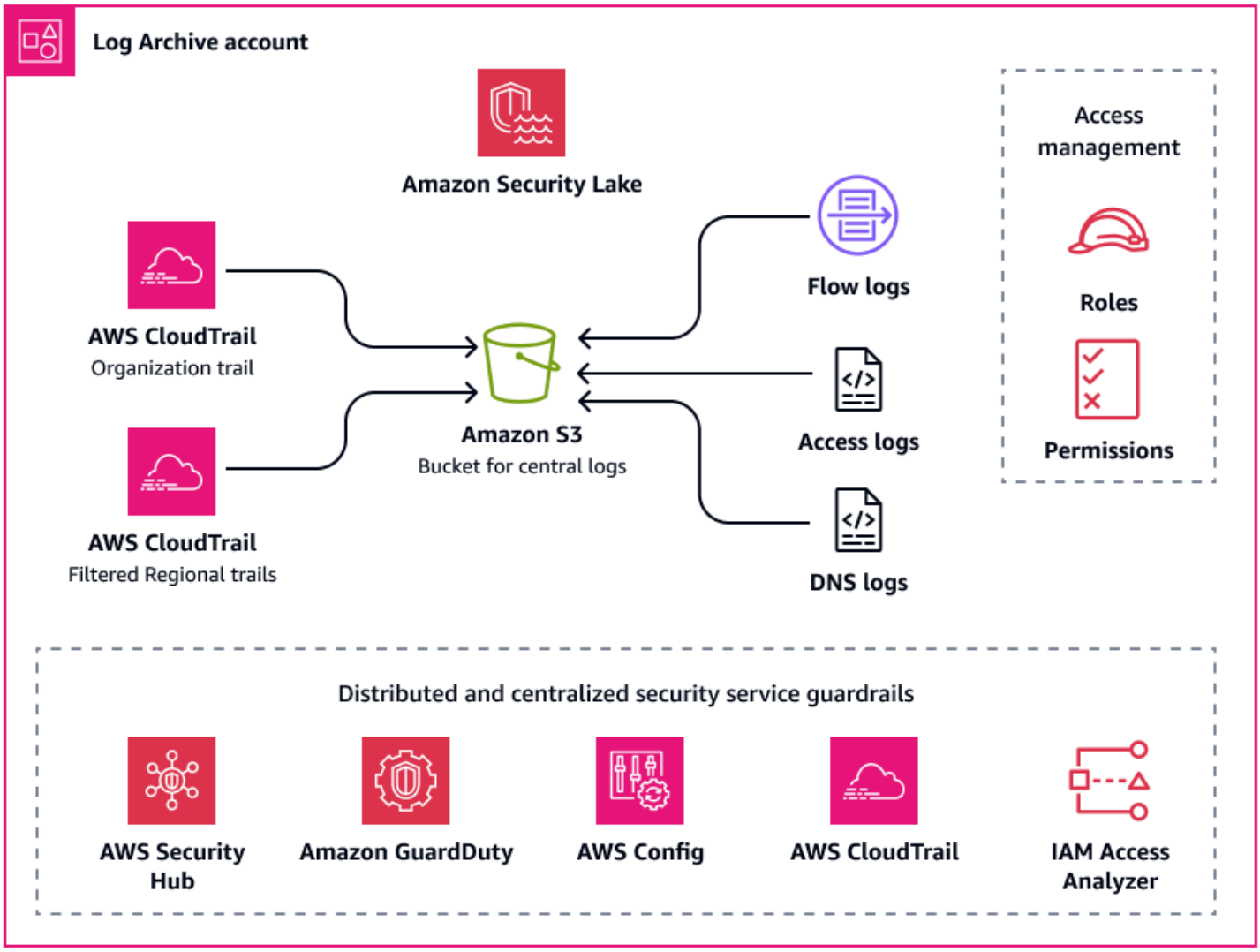
するには、Macie を有効にして、機密データの自動検出を設定します。Macie は、アカウントと 全体で、すべての S3 バケット内のオブジェクトを継続的に分析します AWS リージョン。Macie は、個人データが存在する場所を示すインタラクティブなヒートマップを生成して維持します。機密データの自動検出機能は、コストを削減し、検出ジョブを手動で設定する必要性を最小限に抑えるように設計されています。機密データの自動検出機能をベースに築き、Macie を使用して既存のバケット内の新しいバケットまたは新しいデータを自動的に検出し、割り当てられたデータ分類タグに対してデータを検証できます。このアーキテクチャを設定して、誤って分類されたバケットまたは未分類のバケットを適時に適切な開発チームとプライバシーチームに通知します。

を使用して、組織内のすべてのアカウントで Macie を有効にできます AWS Organizations。詳細については、「Amazon Macie 内で組織を統合および設定する」を参照してください。

セキュリティ OU — ログアーカイブアカウント

> **アンケート**
>
> 皆様からのご意見をお待ちしています。簡単なアンケートに回答して、PRA AWS に関するフィードバックを提供してください。

ログアーカイブアカウントは、インフラストラクチャ、サービス、アプリケーションのログタイプを一元化する場所です。このアカウントの詳細については、AWS 「セキュリティリファレンスアーキテクチャ (AWS SRA)」を参照してください。ログ専用のアカウントを使用すると、すべてのログタイプに一貫したアラートを適用し、インシデント対応者がこれらのログの集計に 1 か所からアクセスできることを確認できます。セキュリティコントロールとデータ保持ポリシーをすべて 1 か所から設定できるため、プライバシー運用オーバーヘッドが簡素化されます。以下の図は、ログアーカイブアカウントで設定されている AWS セキュリティおよびプライバシーサービスを示しています。



一元化されたログストレージ

ログファイル (AWS CloudTrail ログなど) には、個人データと見なされる可能性のある情報が含まれている場合があります。一部の組織は、可視性の目的で、アカウント間 AWS リージョン およびアカウント間で CloudTrail ログを 1 つの一元的な場所に集約するために、組織の証跡を使用することを選択します。詳細については、このガイドの「AWS CloudTrail」を参照してください。CloudTrail ログの一元化を実装する場合、通常、ログは 1 つのリージョンの Amazon Simple Storage Service (Amazon S3) バケットに保存されます。

組織における個人データの定義、顧客に対する契約上の義務、および適用される地域のプライバシー規制によっては、ログ集約に関して海外へのデータ転送を検討する必要がある生じる場合があります。さまざまなログタイプの個人データがこれらの制限に該当するかどうかを確認します。例えば、CloudTrail ログには組織の従業員データが含まれている場合がありますが、顧客の個人データは

含まれていない場合があります。組織が制限されたデータ転送要件に準拠する必要がある場合は、以下のオプションがサポートに役立つ可能性があります。

- 組織が のサービスを複数の国の AWS クラウド データセットに提供している場合は、データレジデンシー要件が最も厳しい国のすべてのログを集約することを選択できます。たとえば、ドイツで運用していて、最も厳しい要件がある場合は、 の S3 バケットにデータを集約eu-central-1 AWS リージョン して、ドイツで収集されたデータがドイツの境界を離れないようにすることができます。このオプションでは、CloudTrail で 1 つの組織証跡を設定し、すべてのアカウントからターゲットリージョン AWS リージョン にログを集約できます。
- データがコピーされて別のリージョンに集約される AWS リージョン 前に、 に保持する必要がある個人データを編集します。例えば、ログを別のリージョンに転送する前に、アプリケーションのホストリージョンで個人データをマスクできます。個人データのマスキングに関する詳細については、このガイドの「Amazon Data Firehose」セクションを参照してください。
- 厳格なデータ主権に関する懸念がある場合は、これらの要件を適用する別のマルチアカウントランディングゾーン AWS リージョン を に維持できます。これにより、リージョンのランディングゾーン設定を簡素化して、一元的なログ記録を行うことができます。また、追加のインフラストラクチャ分離の利点を提供し、ログを独自のリージョンにローカルに維持することができます。法律顧問と協力して、対象となる個人データと許容されるリージョン間の転送を決定します。詳細については、このガイドの「グローバル展開の戦略」を参照してください。

サービスログ、アプリケーションログ、オペレーティングシステム (OS) ログを通じて、Amazon CloudWatch を使用して、対応するアカウントとリージョンの AWS のサービス または リソースをデフォルトでモニタリングできます。顧客の多くは、これらのログとメトリクスを複数のアカウントとリージョンから 1 つのアカウントに一元化することを選択します。デフォルトでは、これらのログは、対応するアカウントと発信元のリージョンに保持されます。一元化では、サブスクリプションフィルターと Amazon S3 エクスポートタスクを使用して、一元化された場所にデータを共有できます。海外へのデータ転送要件が含まれるワークロードからログを集約するときは、適切なフィルターとエクスポートタスクを含めることが重要です。ワークロードのアクセスログに個人データが含まれている場合は、それらのログが特定のアカウントやリージョンに転送または保持されていることを確認する必要が生じる場合があります。

Amazon Security Lake

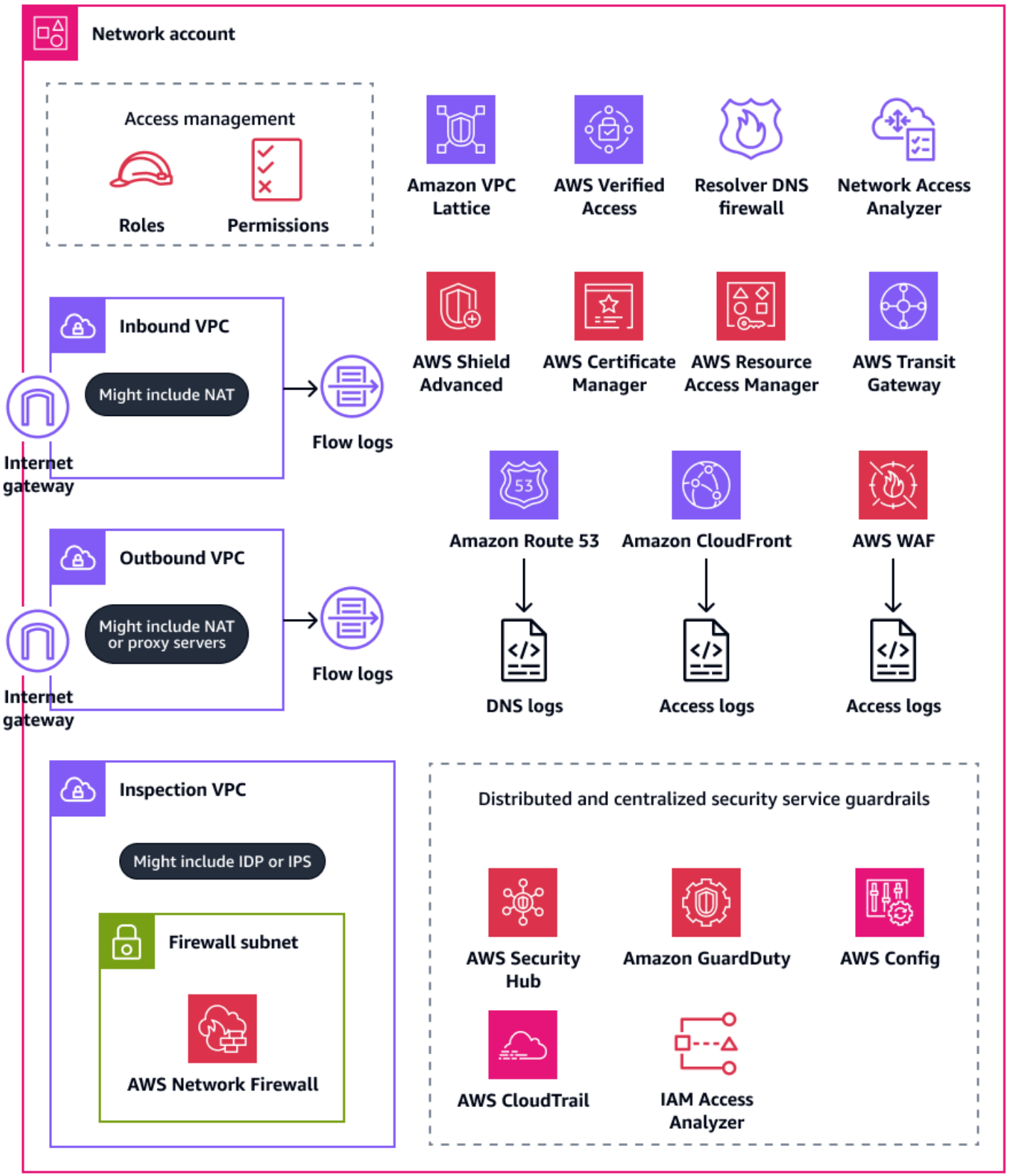
SRA で推奨されているように、Amazon Security Lake AWS の委任管理者アカウントとして Log Archive アカウントを使用できます。これを行うと、Security Lake は、他の SRA が推奨するセキュリティログと同じアカウントの専用の Amazon S3 バケットで、サポートされているログを収集します。

プライバシーの観点からは、インシデント対応者が AWS 環境、SaaS プロバイダー、オンプレミス、クラウドソース、サードパーティーソースのログにアクセスできることが重要です。これにより、個人データへの不正アクセスをより迅速にブロックして修復できます。ログストレージに関する同一の考慮事項は、Amazon Security Lake 内のログレジデンシーとリージョン移動に適用される可能性が最も高いです。これは、Security Lake が、サービスを有効にした AWS リージョン からセキュリティログとイベントを収集するためです。データレジデンシーの要件に準拠するには、ロールアップリージョンの設定を検討してください。ロールアップリージョンは、Security Lake が 1 つ以上の寄与するリージョンのデータを統合するリージョンで、お客様が選択します。Security Lake リージョンとロールアップリージョンを設定する前に、組織がデータレジデンシーのリージョンコンプライアンス要件に合わせる必要が生じる場合があります。

インフラストラクチャ OU — ネットワークアカウント

> **アンケート**
>
> 皆様からのご意見をお待ちしています。簡単なアンケートに回答して、PRA AWS に関するフィードバックを提供してください。

ネットワークアカウントでは、仮想プライベートクラウド (VPC) とより広範なインターネット間のネットワークを管理します。このアカウントでは、VPC サブネットと AWS Transit Gateway アタッチメントの共有に AWS Resource Access Manager (AWS RAM) を使用し AWS WAF、Amazon CloudFront を使用してターゲットを絞ったサービスの使用をサポートすることで、広範な開示制御メカニズムを実装できます。このアカウントの詳細については、AWS「セキュリティリファレンスアーキテクチャ (AWS SRA)」を参照してください。次の図は、ネットワークアカウントで設定されている AWS セキュリティおよびプライバシーサービスを示しています。


Network account
Access management
Roles
Permissions
Amazon VPC Lattice
AWS Verified Access
Resolver DNS firewall
Network Access Analyzer
AWS Shield Advanced
AWS Certificate Manager
AWS Resource Access Manager
AWS Transit Gateway
Inbound VPC
Might include NAT
Internet gateway
Flow logs
Outbound VPC
Might include NAT or proxy servers
Internet gateway
Flow logs
Amazon Route 53
Amazon CloudFront
AWS WAF
DNS logs
Access logs
Access logs
Inspection VPC
Might include IDP or IPS
Firewall subnet
AWS Network Firewall
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer

このセクションでは、このアカウントで使用される以下の AWS のサービス に関する詳細情報を提供します。

- Amazon CloudFront
- AWS Resource Access Manager
- AWS Transit Gateway
- AWS WAF

Amazon CloudFront

Amazon CloudFront は、フロントエンドアプリケーションとファイルホスティングの地理的制限をサポートしています。CloudFront では、エッジロケーションというデータセンターの世界的ネットワークを経由してコンテンツを配信できます。ユーザーが CloudFront を通じて提供しているコンテンツを要求すると、要求は最も遅延が少ないエッジロケーションにルーティングされます。セキュリティコンテキストでのこのサービスの使用方法についての詳細は、「AWS セキュリティリファレンスアーキテクチャ」を参照してください。

お客様のプライバシープログラムが、現在、特定の地域法への準拠をサポートしている可能性があります。ワークロードが、これらのリージョン内にのみ存在する顧客にのみサービスを提供するようスコープ設定されている場合は、他のリージョンでの使用を防止する技術的対策を実装できます。CloudFront の地理的制限を使用すると、CloudFront ディストリビューションを通じて配信しているコンテンツに対して特定地域のユーザーがアクセスできないようにすることができます。詳細および地理的制限の設定オプションについては、CloudFront ドキュメントの「コンテンツの地理的ディストリビューションの制限」を参照してください。

また、CloudFront が受信するすべてのユーザーリクエストに関する詳細情報を含めたアクセスログが作成されるように CloudFront を設定することもできます。詳細については、CloudFront ドキュメントの「標準ログ (アクセスログ) の設定および使用」を参照してください。最後に、CloudFront が一連のエッジロケーションでコンテンツをキャッシュするように設定されている場合は、キャッシュが発生する場所を検討できます。一部の組織では、クロスリージョンキャッシュが海外へのデータ転送要件の対象となる場合があります。

AWS Resource Access Manager

AWS Resource Access Manager (AWS RAM) は、 間でリソースを安全に共有 AWS アカウント し、運用オーバーヘッドを削減し、可視性と監査性を提供します。を使用すると AWS RAM、組織は組織 AWS アカウント 内の他の またはサードパーティーアカウントと共有できる AWS リソースを制

限できます。詳細については、「共有可能な AWS リソース」を参照してください。ネットワークアカウントでは、 AWS RAM を使用して VPC サブネットとトランジットゲートウェイ接続を共有できます。 AWS RAM を使用してデータプレーン接続を別の と共有する場合は AWS アカウント、接続が事前承認され、データレジデンシー要件 AWS リージョン に準拠していることをチェックするプロセスを確立することを検討してください。

VPCs とトランジットゲートウェイ接続の共有に加えて、 を使用して、IAM リソースベースのポリシーをサポートしていないリソースを共有 AWS RAM できます。個人データ OU でホストされているワークロードの場合、 AWS RAM を使用して、別の にある個人データにアクセスできます AWS アカウント。詳細については、「個人データ OU – PD アプリケーションアカウント」セクションの「AWS Resource Access Manager」を参照してください。

AWS Transit Gateway

組織のデータレジデンシー要件 AWS リージョン に沿った個人データを収集、保存、または処理する AWS リソースを にデプロイする場合で、適切な技術的保護策がある場合は、コントロールプレーンとデータプレーンで未承認のクロスボーダーデータフローを防ぐためにガードレールを実装することを検討してください。コントロールプレーンでは、IAM およびサービスコントロールポリシーを使用してリージョンの使用を制限し、その結果、クロスリージョンのデータフローも制限できます。

データプレーンでクロスリージョンデータフローを制御するには、複数のオプションがあります。例えば、ルートテーブル、VPC ピアリング、 AWS Transit Gateway アタッチメントを使用できます。AWS Transit Gateway は、仮想プライベートクラウド (VPC) とオンプレミスネットワークを接続する中心的なハブです。より大きな AWS ランディングゾーンの一部として、インターネットゲートウェイ AWS リージョン、VPC-to-VPC直接ピアリング、 とのリージョン間ピアリングなど、データが通過できるさまざまな方法を検討できます AWS Transit Gateway。例えば、 AWS Transit Gatewayで次を実行できます。

- VPC とオンプレミス環境間の東西接続と南北接続がプライバシー要件と一致していることを確認します。
- プライバシー要件に従って VPC の設定を構成します。
- AWS Organizations および IAM ポリシーでサービスコントロールポリシーを使用して、 AWS Transit Gateway および Amazon Virtual Private Cloud (Amazon VPC) 設定の変更を防止します。サービスコントロールポリシーのサンプルについては、このガイドの「VPC 設定の変更を制限する」を参照してください。

AWS WAF

個人データの意図しない開示を防ぐために、ウェブアプリケーションに defense-in-depth アプローチをデプロイできます。入力検証とレート制限をアプリケーションに構築することはできますが、別の防御線として機能する AWS WAF ことができます。 AWS WAFは、保護されたウェブアプリケーションリソースに転送される HTTP および HTTPS リクエストをモニタリングするのに役立つウェブアプリケーションファイアウォールです。セキュリティコンテキストでのこのサービスの使用方法についての詳細は、「AWS セキュリティリファレンスアーキテクチャ」を参照してください。

を使用すると AWS WAF、特定の条件を検査するルールを定義してデプロイできます。以下のアクティビティは、個人データの意図しない開示に関連している可能性があります。

- 不明または悪意のある IP アドレスまたは地理的場所からのトラフィック
- Open Worldwide Application Security Project (OWASP) による上位 10 件の攻撃 (SQL インジェクションなど漏洩関連の攻撃を含む)
- 割合の高いリクエスト
- 一般的なボットトラフィック
- コンテンツスクレイパー

によって管理される AWS WAF ルールグループをデプロイできます AWS。のマネージドルールグループの中には AWS WAF 、プライバシーや個人データに対する脅威を検出するために使用できるものもあります。次に例を示します。

- SQL データベース - このルールグループには、SQL インジェクション攻撃などの SQL データベースの悪用に関連する要求パターンをブロックするルールが含まれています。アプリケーションが SQL データベースと連結している場合は、このルールグループを検討してください。
- 既知の不正な入力 – このルールグループには、無効であることがわかっていて、脆弱性の悪用または検知に関連する要求パターンをブロックするルールが含まれています。
- Bot Control – このルールグループには、過剰なリソースを消費し、ビジネスメトリクスを歪め、ダウンタイムを引き起こし、悪意のあるアクティビティを実行する可能性があるボットからの要求を管理するように設計されたルールが含まれています。
- Account takeover prevention (ATP) – このルールグループには、悪意のあるアカウント乗っ取りの試みを防ぐように設計されたルールが含まれています。このルールグループでは、アプリケーションのログインエンドポイントに送信されたログイン試行が検査されます。

個人データ OU – PD アプリケーションアカウント

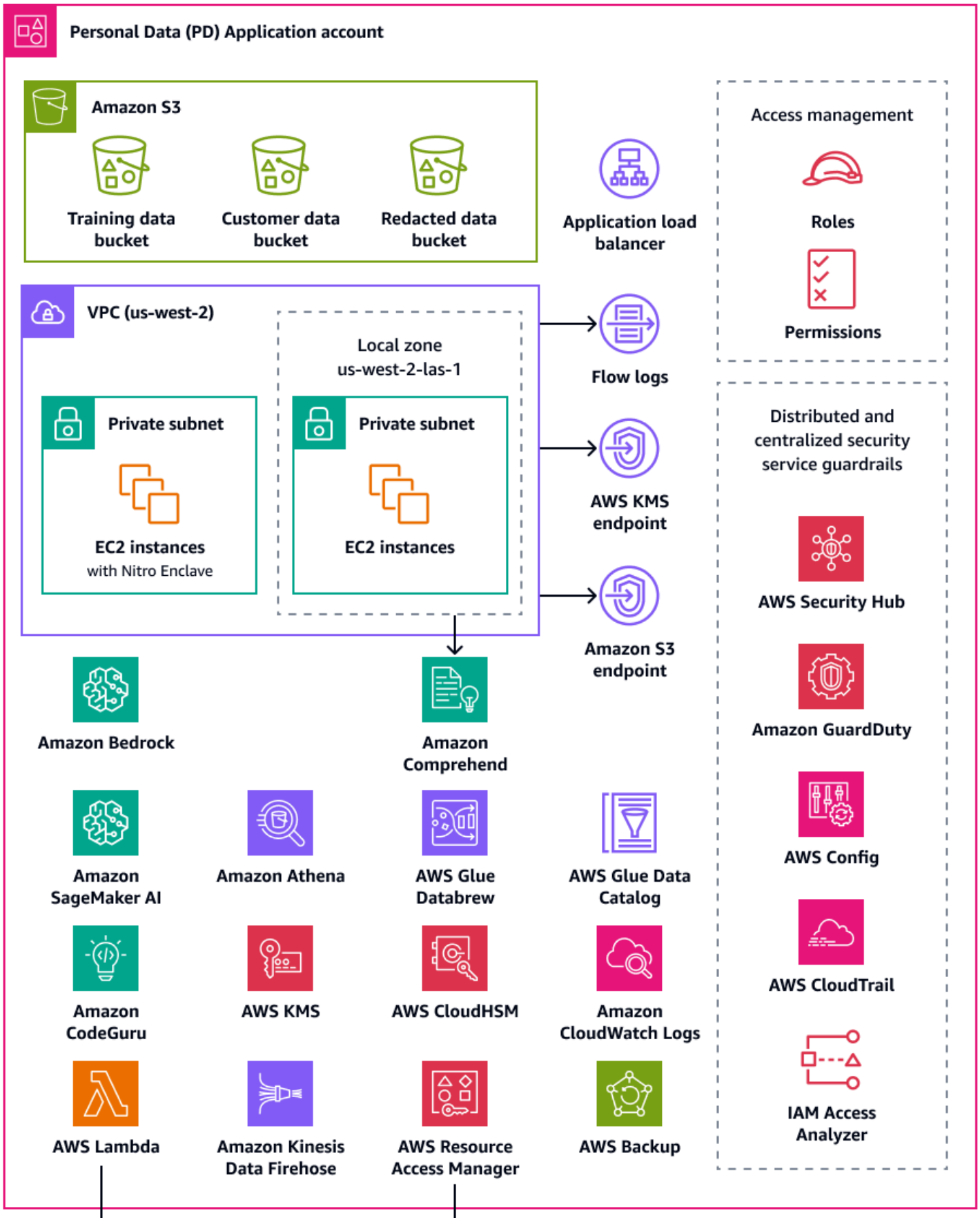
> **アンケート**
>
> 皆様からのご意見をお待ちしています。簡単なアンケートに回答して、PRA AWS に関するフィードバックを提供してください。

個人データ (PD) アプリケーションアカウントは、組織が個人データを収集および処理するサービスをホストする場所です。具体的には、個人データとして定義したものをこのアカウントに保存できます。 AWS PRA は、多層サーバーレスウェブアーキテクチャによるプライバシー設定の例を多数示しています。 AWS ランディングゾーン全体でワークロードを運用する場合、プライバシー設定をone-size-fits-allソリューションと見なすべきではありません。例えば、基礎となる概念、プライバシーを強化する方法、組織が特定のユースケースやアーキテクチャにソリューションを適用できる方法を理解することが目的の場合があります。

個人データを収集、保存、または処理する組織 AWS アカウント 内の では、 AWS Organizations とを使用して、基盤となる反復可能なガードレール AWS Control Tower をデプロイできます。これらのアカウント専用の組織単位 (OU) を確立することが重要です。例えば、データレジデンシーガードレールを、データレジデンシーが設計上の重要な考慮事項であるアカウントのサブセットにのみ適用する必要が生じる場合があります。多くの組織では、これらは個人データを保存および処理するアカウントです。

組織は、個人用データセットの信頼できるソースを保存する専用のデータアカウントのサポートを検討する場合があります。信頼できるデータソースは、データのプライマリバージョンを保存する場所であり、データの最も信頼性が高く正確なバージョンと見なされる可能性があります。例えば、信頼できるデータソースから、トレーニングデータ、顧客データのサブセット、秘匿化データの保存に使用される PD アプリケーションアカウントの Amazon Simple Storage Service (Amazon S3) バケットなどの他の場所にデータをコピーできます。このマルチアカウントアプローチを使用して、データアカウントの完全かつ最終的な個人データセットを PD アプリケーションアカウントのダウンストリームコンシューマーワークロードから分離することで、アカウントへの不正アクセスが発生した場合の影響範囲を減らすことができます。

次の図は、PD アプリケーションアカウントとデータアカウントで設定されている AWS セキュリティサービスとプライバシーサービスを示しています。


Personal Data (PD) Application account
Amazon S3
Training data bucket
Customer data bucket
Redacted data bucket
Application load balancer
Access management
Roles
Permissions
VPC (us-west-2)
Local zone us-west-2-las-1
Private subnet
EC2 instances with Nitro Enclave
Private subnet
EC2 instances
Flow logs
AWS KMS endpoint
Amazon S3 endpoint
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Amazon Bedrock
Amazon Comprehend
Amazon SageMaker AI
Amazon Athena
AWS Glue Databrew
AWS Glue Data Catalog
Amazon CodeGuru
AWS KMS
AWS CloudHSM
Amazon CloudWatch Logs
AWS Lambda
Amazon Kinesis Data Firehose
AWS Resource Access Manager
AWS Backup
Data account
Access management

このセクションでは、以下のアカウントで使用される以下の AWS のサービス に関する詳細情報について説明します。

- Amazon Athena
- Amazon Bedrock
- AWS Clean Rooms
- Amazon CloudWatch Logs
- Amazon CodeGuru Reviewer
- Amazon Comprehend
- Amazon Data Firehose
- Amazon DataZone
- AWS Glue
- AWS Key Management Service
- AWS Lake Formation
- AWS Local Zones
- AWS Nitro Enclaves
- AWS PrivateLink
- AWS Resource Access Manager
- Amazon SageMaker AI
- AWS データライフサイクルの管理に役立つ 機能
- AWS のサービス データのセグメント化に役立つ および の機能
- AWS のサービス データの検出、分類、カタログ化に役立つ および の機能

Amazon Athena

プライバシー目標を達成するために、データクエリ制限の制御について検討できます。Amazon Athena は、標準 SQL を使用して Amazon S3 でデータを直接分析するのに役立つ対話型のクエリサービスです。Athena にデータをロードする必要はありません。S3 バケットに保存されているデータと直接連携します。

Athena の一般的なユースケースは、データ分析チームに、カスタマイズされサニタイズされたデータセットを提供することです。データセットに個人データが含まれている場合は、データ分析チー

ムにとってほとんど価値のない個人データの列全体をマスクすることで、データセットをサニタイズできます。詳細については、Amazon Athena によるデータレイク内のデータの匿名化と管理 AWS Lake Formation」および「(AWS ブログ記事) 」を参照してください。

データ変換アプローチで、Athena でサポートされている関数以外の柔軟性が追加で必要になった場合は、ユーザー定義関数 (UDF) と呼ばれるカスタム関数を定義できます。Athena に送信された SQL クエリで UDF を呼び出すことができ、 AWS Lambdaで実行されます。SELECT および FILTER SQL クエリで UDF を使用し、同じクエリで複数の UDF を呼び出すことができます。プライバシーのために、列内のすべての値の末尾 4 文字のみを表示するなど、特殊なデータマスキングを実行する UDF を作成できます。

Amazon Bedrock

Amazon Bedrock は、AI21 Labs、Anthropic、Meta、Mistral AI、Amazon など主要な AI 企業からの基盤モデルへのアクセスを提供するフルマネージドサービスです。これは、組織が生成 AI アプリケーションを構築およびスケールするのに役立ちます。どのプラットフォームが使用されていても、生成 AI を使用すると、組織は個人データ漏洩の可能性、不正なデータアクセス、その他のコンプライアンス違反などのプライバシー関連のリスクにさらされる可能性があります。

Amazon Bedrock ガードレールは、Amazon Bedrock の生成 AI ワークロード全体にセキュリティとコンプライアンスのベストプラクティスを適用することで、これらのリスクを軽減するように設計されています。AI リソースのデプロイと使用は、必ずしも組織のプライバシー要件とコンプライアンス要件に合致するとは限りません。組織は生成 AI モデルを使用する際にデータプライバシーの維持に苦労する可能性があります。これは、これらのモデルが機密情報を記憶または再現する可能性があるためです。Amazon Bedrock ガードレールは、ユーザー入力とモデルレスポンスを評価することでプライバシーを保護することができます。全体として、入力データに個人データが含まれている場合、この情報がモデルの出力で公開されるリスクがあります。

Amazon Bedrock ガードレールは、データ保護ポリシーを適用し、不正なデータ漏洩を防ぐメカニズムを提供します。入力内の個人データを検出してブロックするコンテンツフィルタリング機能、不適切またはリスクのある対象領域へのアクセスを防ぐためのトピック制限、モデルプロンプトとレスポンスの機密用語をマスクまたは編集するワードフィルターを提供します。これらの機能は、バイアスのかかったレスポンスや顧客の信頼低下など、プライバシー違反につながる可能性のあるイベントを防止するのに役立ちます。これらの機能により、個人データが AI モデルによって誤って処理または開示されないようにできます。Amazon Bedrock ガードレールでは、Amazon Bedrock 以外での入力とレスポンスの評価についてもサポートしています。詳細については、「Implement model-independent safety measures with Amazon Bedrock Guardrails」(AWS のブログ記事) を参照してください。

Amazon Bedrock ガードレールでは、根拠とレスポンスの関連性を評価するコンテキストグラウンディングチェックを使用して、モデルハルシネーションのリスクを制限できます。例えば、検索拡張生成 (RAG) アプリケーションでサードパーティーのデータソースを使用する生成 AI の顧客向けアプリケーションをデプロイします。コンテキストグラウンディングチェックを使用して、これらのデータソースに対するモデルレスポンスを検証し、不正確なレスポンスを除外できます。 AWS PRA のコンテキストでは、ワークロードアカウント全体に Amazon Bedrock ガードレールを実装できます。これにより、各ワークロードの要件に合わせた特定のプライバシーガードレールが適用されます。

AWS Clean Rooms

組織は、機密性の高いデータセットを交差または重複させる分析を通じて相互に連携させる方法を模索しているため、その共有データのセキュリティとプライバシーを維持することが懸念事項となります。AWS Clean Rooms によって、組織が未加工データ自体を共有するのではなく、結合されたデータセットを分析できる安全で中立的な環境であるデータクリーンルームをデプロイできるようになります。また、自分のアカウントからデータを移動またはコピーしたり、基盤となるデータセットを公開 AWS したりすることなく、 で他の組織にアクセスできるようにすることで、独自のインサイトを生成できます。すべてのデータはソースの場所に残ります。組み込みの分析ルールで、出力を抑制し、SQL クエリを制限します。すべてのクエリがログに記録され、コラボレーションメンバーはデータのクエリ方法を表示できます。

AWS Clean Rooms コラボレーションを作成し、他の AWS 顧客をそのコラボレーションのメンバーに招待できます。メンバーデータセットをクエリする機能を 1 人のメンバーに付与し、追加のメンバーを選択してそれらのクエリ結果を受け取れるようにできます。複数のメンバーがデータセットをクエリする必要がある場合は、同じデータソースと異なるメンバー設定を使用して追加のコラボレーションを作成できます。各メンバーは、コラボレーションメンバーと共有されているデータをフィルタリングできます。また、カスタム分析ルールを使用して、コラボレーションに提供するデータの分析方法に関する制限事項を設定できます。

は、コラボレーションに提示されるデータと他のメンバーによる使用方法を制限するだけでなく、プライバシーの保護に役立つ以下の機能 AWS Clean Rooms を提供します。

- 差分プライバシーは、慎重に調整されたノイズ量をデータに追加することでユーザーのプライバシーを強化する数学的な手法です。これにより、目的の値を隠すことなく、データセット内の個々のユーザーを再識別するリスクを軽減できます。AWS Clean Rooms 差分プライバシーの使用には、差分プライバシーの専門知識は必要ありません。
- AWS Clean Rooms ML により、データを相互に直接共有しなくても、複数の関係者がデータ内で類似したユーザーを識別できます。これにより、コラボレーションのメンバーによって他のメン

バーのデータセット内の個人を特定できる、メンバーシップ推論攻撃のリスクが軽減されます。類似モデルを作成し、類似セグメントを生成することで、 AWS Clean Rooms ML は元のデータを公開せずにデータセットを比較するのに役立ちます。これには、メンバーに ML の専門知識を持たせたり、外部で作業を実行したりする必要はありません AWS Clean Rooms。トレーニング済みモデルのフルコントロールと所有権は保持されます。

- クリーンルームの暗号コンピューティング (C3R) は、分析ルールで使用して、機密データからインサイトを引き出すことができます。これにより、コラボレーションの相手が学習できる内容が暗号的に制限されます。C3R 暗号化クライアントを使用すると、データはクライアントで暗号化されてから提供されます AWS Clean Rooms。データテーブルは Amazon S3 にアップロードされる前にクライアント側の暗号化ツールを使用して暗号化されるため、データは暗号化されたままになり、処理中も保持されます。

AWS PRA では、データアカウントで AWS Clean Rooms コラボレーションを作成することをお勧めします。これらのコラボレーションを使用して、暗号化された顧客データをサードパーティーと共有できます。コラボレーションは、提供されたデータセットに重複がある場合にのみ使用してください。重複を判断する方法の詳細については、 AWS Clean Rooms ドキュメントの「分析ルールを一覧表示する」を参照してください。

Amazon CloudWatch Logs

Amazon CloudWatch Logs は、すべてのシステム、アプリケーション、 AWS のサービス からのログを一元化するのに役立ちます。一元化により、ログを監視して安全にアーカイブできます。CloudWatch Logs では、新規または既存のロググループのデータ保護ポリシーを使用して、個人データの開示リスクを最小限に抑えることができます。データ保護ポリシーにより、個人データなどログ内の機密データを検出できます。データ保護ポリシーでは、ユーザーが AWS マネジメントコンソールを介してログにアクセスするときに、そのデータをマスクできます。ユーザーが個人データに直接アクセスする必要がある場合は、ワークロードの全体的な目的仕様に従って、それらのユーザーに `logs:Unmask` のアクセス許可を割り当てることができます。また、アカウント全体のデータ保護ポリシーを作成し、このポリシーを組織内のすべてのアカウントに一貫して適用することもできます。これにより、CloudWatch Logs の現在および将来のすべてのロググループに対して、デフォルトでマスキングが設定されます。また、監査レポートを有効にし、別のロググループ、Amazon S3 バケット、または Amazon Data Firehose に送信することをお勧めします。これらのレポートには、各ロググループに対するデータ保護検出結果の詳細な記録が含まれています。

Amazon CodeGuru Reviewer

プライバシーとセキュリティの両方において、多くの組織が、デプロイフェーズとデプロイ後のフェーズの両方で継続的なコンプライアンスをサポートすることが重要です。 AWS PRA には、個人データを処理するアプリケーションのデプロイパイプラインにプロアクティブコントロールが含まれています。Amazon CodeGuru Reviewer は、Java、JavaScript、Python コード内の個人データを漏洩する可能性がある潜在的な欠陥を検出できます。コードを改善するための提案を開発者に提供します。CodeGuru Reviewer は、さまざまなセキュリティ、プライバシー、一般的な推奨プラクティスにおける欠陥を特定できます。 AWS CodeCommit、Bitbucket、GitHub、Amazon S3 など、複数のソースプロバイダーと連携するように設計されています。CodeGuru Reviewer が検出できるプライバシー関連の欠陥には、次のようなものがあります。

- SQL インジェクション
- セキュリティで保護されていない Cookie
- 認可の欠落
- クライアント側の AWS KMS 再暗号化

CodeGuru Reviewer で検出できる内容の完全なリストについては、「Amazon CodeGuru Detector Library」を参照してください。

Amazon Comprehend

Amazon Comprehend は、機械学習を使用して英語のテキスト内で貴重なインサイトや接続を検出する自然言語処理 (NLP) サービスです。Amazon Comprehend は、構造化、半構造化、または非構造化テキストドキュメント内の個人データを検出して編集できます。詳細については、Amazon Comprehend ドキュメントの「個人を特定できる情報 (PII)」を参照してください。

Amazon Comprehend には AWS SDKs を介したアプリケーション統合のオプションが多数あるため、Amazon Comprehend を使用して、データを収集、保存、処理するさまざまな場所で個人データを識別できます。Amazon Comprehend ML 機能を使用すると、アプリケーションログ (AWS ブログ記事) 、顧客の E メール、サポートチケットなどの個人データを検出して編集できます。PD アプリケーションアカウントのアーキテクチャ図は、Amazon EC2 のアプリケーションログに対してこの関数を実行する方法を示しています。Amazon Comprehend には、次の 2 つの編集モードがあります。

- `REPLACE_WITH_PII_ENTITY_TYPE` は、各 PII エンティティをそのタイプに置き換えます。例えば、Jane Doe は NAME に置き換えられます。

- MASK は、PII エンティティの文字を任意の文字 (!、#、$、%、&、、@) に置き換えます。例えば、Jane Doe は **** *** に置き換えることができます。

Amazon Data Firehose

Amazon Data Firehose は、ストリーミングデータをキャプチャして変換し、Amazon Managed Service for Apache Flink や Amazon S3 などのダウンストリーム サービスにロードします。Firehose は、処理パイプラインをゼロから構築することなく、アプリケーションログなどの大量のストリーミングデータを転送するために使用されることが多くあります。

Lambda 関数を使用して、データがダウンストリームに送信される前に、カスタマイズされた処理または組み込み処理を実行できます。プライバシーについて、この機能はデータの最小化と海外へのデータ転送に関する要件をサポートします。例えば、Lambda と Firehose を使用して、ログアーカイブアカウントに一元化される前にマルチリージョンログデータを変換できます。詳細については、「Biogen: Centralized Logging Solution for Multi Accounts」(YouTube 動画) を参照してください。PD アプリケーションアカウントで、Firehose 配信ストリームにログをプッシュ AWS CloudTrail するように Amazon CloudWatch と を設定します。Lambda 関数でログを変換し、ログアーカイブアカウントの中央 S3 バケットに送信します。個人データを含む特定のフィールドをマスクするように Lambda 関数を設定できます。これにより、 AWS リージョン間での個人データの転送を防ぐことができます。このアプローチを使用すると、個人データは転送や一元化の後ではなく、その前にマスクされます。海外への転送要件の対象ではない管轄区域のアプリケーションでは、通常、CloudTrail の組織証跡を通じてログを集計すると、運用効率とコスト効率が向上します。詳細については、このガイドの「セキュリティ OU – Security Tooling アカウント」セクションの「AWS CloudTrail」を参照してください。

Amazon DataZone

組織が AWS のサービス などの を通じてデータを共有するアプローチをスケールするにつれて AWS Lake Formation、差分アクセスがデータに最も精通しているユーザー、つまりデータ所有者によって制御されるようにしたいと考えています。ただし、こうしたデータ所有者は、同意や海外へのデータ転送に関する考慮事項などのプライバシー要件を認識している可能性があります。Amazon DataZone を使用すれば、データ所有者とデータガバナンスチームが、データガバナンスポリシーに従い組織全体でデータを共有および使用できるようになります。Amazon DataZone では、事業部門 (LOB) が独自のデータを管理し、カタログでこの所有権を追跡します。利害関係者は、ビジネスタスクの一環としてデータを検索し、アクセスをリクエストできます。データパブリッシャーによって確立されたポリシーに従っている限り、データ所有者は、管理者を必要とせず、またデータを移動することなく、基盤となるテーブルへのアクセスを付与できます。

プライバシーのコンテキストにおいて、Amazon DataZone は次のユースケースの例で役立ちます。

- 顧客向けアプリケーションで、別のマーケティング LOB と共有できる使用状況データを生成します。マーケティングにオプトインした顧客のデータのみがカタログに公開されていることを確認する必要があります。
- 欧州の顧客データは公開されますが、欧州経済地域 (EEA) のローカル LOB のみがサブスクライブできます。詳細については、「Amazon DataZone の細かな粒度のアクセス制御によるデータセキュリティの強化」を参照してください。

AWS PRA では、共有 Amazon S3 バケット内のデータをデータプロデューサーとして Amazon DataZone に接続できます。

AWS Glue

個人データを含むデータセットの維持は、プライバシーバイデザインの主要なコンポーネントです。組織のデータは、構造化、半構造化、または非構造化の形式で存在する場合があります。構造化されていない個人用データセットでは、データ最小化、データ主体要求の一部として単一のデータ主体に起因するデータの追跡、一貫したデータ品質の確保、データセットの全体的なセグメンテーションなど、プライバシーを強化するオペレーションを多数実行することが困難になる可能性があります。AWS Glue はフルマネージドの抽出、変換、ロード (ETL) サービスです。データストアとデータストリーム間でデータを分類、クリーンアップ、強化、移動するのに役立ちます。 AWS Glue 機能は、分析、機械学習、アプリケーション開発用のデータセットを検出、準備、構造化、結合するのに役立ちます。 AWS Glue を使用して、既存のデータセット上に予測可能で共通の構造を作成できます。 AWS Glue Data Catalog、 AWS Glue DataBrew、および AWS Glue Data Quality は、組織のプライバシー要件をサポートするのに役立つ AWS Glue 機能です。

AWS Glue Data Catalog

AWS Glue Data Catalog を使用して、メンテナンス可能なデータセットを確立できます。データカタログには、抽出、変換、ロード (ETL) ジョブのソースおよびターゲットとして使用されるデータへの参照が含まれています AWS Glue。Data Catalog の情報はメタデータテーブルとして保存され、各テーブルが 1 つのデータストアを指定します。 AWS Glue クローラーを実行して、さまざまなデータストアタイプのデータを調査します。組み込み分類子とカスタム分類子をクローラーに追加すると、これらの分類子によって個人データのデータ形式とスキーマが推測されます。次に、クローラーによってメタデータが Data Catalog に書き込まれます。一元化されたメタデータテーブルを使用すると、 AWS 環境内の個人データのさまざまなソースに構造と予測可能性が追加されるため、データセットリクエスト (消去する権利など) への対応が容易になります。Data Catalog を使用して

これらのリクエストに自動的に応答する方法の包括的な例については、Amazon S3 Find and Forget によるデータレイク内のデータ消去リクエストの処理」(AWS ブログ記事) を参照してください。最後に、組織が AWS Lake Formation を使用してデータベース、テーブル、行、セル間できめ細かなアクセスを管理および提供している場合、Data Catalog は主要なコンポーネントとなります。Data Catalog はクロスアカウントデータ共有を提供し、タグベースのアクセスコントロールを使用してデータレイクを大規模に管理するのに役立ちます (AWS ブログ記事) 。詳細については、このセクションの「AWS Lake Formation」を参照してください。

AWS Glue DataBrew

AWS Glue DataBrew は、データのクリーンアップと正規化に役立ち、個人を特定できる情報の削除やマスキング、データパイプライン内の機密データフィールドの暗号化など、データ上で変換を実行できます。また、データの系統を視覚的にマッピングして、データが通過したさまざまなデータソースと変換ステップを理解することもできます。この機能は、組織が個人データの出所をよりよく理解して追跡するにつれて、ますます重要になっています。DataBrew は、データの準備中に個人データをマスクするのに役立ちます。データプロファイリングジョブの一部として個人データを検出し、個人データを含む可能性のある列の数やカテゴリなどの統計情報を収集できます。また、置換、ハッシュ、暗号化、復号など、組み込みの可逆的または不可逆的なデータ変換手法を、コードを記述することなく使用できます。さらに、クリーンアップ済みデータセットやマスク済みデータセットのダウンストリームを分析、報告、機械学習タスクに使用できます。DataBrew で使用できるデータマスキング手法には、次のようなものがあります。

- ハッシュ — ハッシュ関数を列値に適用します。
- 置換 – 個人データを他の、本物そっくりの値に置き換えます。
- Null 化または削除 – 特定のフィールドを null 値に置き換えるか、列を削除します。
- マスキング — 文字スクランブルを使用するか、列内の特定の部分をマスクします。

使用可能な暗号化手法は、次のとおりです。

- 確定的暗号化 – 確定的暗号化アルゴリズムを列値に適用します。確定的暗号化では、値に対して常に同じ暗号文が生成されます。
- 確率的暗号化 – 確率的暗号化アルゴリズムを列値に適用します。確率的暗号化は、適用されるたびに異なる暗号文が生成されます。

DataBrew で提供される個人データ変換レシピの完全なリストについては、「Personally identifiable information (PII) recipe steps」を参照してください。

AWS Glue データ品質

AWS Glue Data Quality は、データパイプラインがデータコンシューマーに配信される前に、データパイプライン間の高品質のデータの配信をプロアクティブに自動化および運用するのに役立ちます。 AWS Glue Data Quality は、データパイプライン全体のデータ品質問題の統計分析を提供し、Amazon EventBridge でアラートをトリガーし、修復のための品質ルールのレコメンデーションを行うことができます。 AWS Glue Data Quality は、カスタムデータ品質ルールを作成できるように、ドメイン固有の言語でのルールの作成もサポートします。

AWS Key Management Service

AWS Key Management Service (AWS KMS) は、データの保護に役立つ暗号化キーの作成と制御に役立ちます。 は、ハードウェアセキュリティモジュール AWS KMS を使用して、FIPS 140-2 暗号化モジュール検証プログラム AWS KMS keys で保護と検証を行います。セキュリティコンテキストでのこのサービスの使用方法についての詳細は、「AWS セキュリティリファレンスアーキテクチャ」を参照してください。

AWS KMS は、暗号化 AWS のサービス を提供するほとんどの と統合されており、個人データを処理して保存するアプリケーションで KMS キーを使用できます。 AWS KMS を使用して、次のようなさまざまなプライバシー要件をサポートし、個人データを保護することができます。

- カスタマーマネージドキーを使用して、強度、ローテーション、有効期限、その他のオプションをより詳細に制御できます。
- 専用のカスタマーマネージドキーを使用すると、個人データや、個人データへのアクセスを許可するシークレットを保護できます。
- データ分類レベルを定義し、レベルごとに少なくとも 1 つの専用カスタマーマネージドキーを指定します。例えば、運用データを暗号化する 1 つのキーと、個人データを暗号化する別のキーがあるとします。
- KMS キーへの意図しないクロスアカウントアクセスを防止します。
- 暗号化するリソース AWS アカウント と同じ 内に KMS キーを保存します。
- KMS キーの管理と使用に対して権限の分離を実装します。詳細については、「KMS と IAM を使用して S3 で暗号化されたデータの独立したセキュリティコントロールを有効にする方法」(AWS ブログ記事) を参照してください。
- 予防的ガードレールと事後対応ガードレールによる自動キーローテーションの適用。

デフォルトでは、KMS キーは保存され、作成されたリージョンでのみ使用できます。組織にデータレジデンシーと主権に関する特定の要件がある場合は、マルチリージョン KMS キーがユースケー

スに適しているかどうかを検討してください。マルチリージョンキーは、異なる の専用 KMS キー AWS リージョン で、同じ意味で使用できます。マルチリージョンキーを作成するプロセスは、キーマテリアルを内部の AWS リージョン 境界を越えて移動するため AWS KMS、このリージョン分離の欠如は、組織の主権とレジデンシーの目標と互換性がない可能性があります。これを解決する 1 つの方法は、リージョン固有のカスタマーマネージドキーなど、別のタイプの KMS キーを使用することです。

外部キーストア

多くの組織では、 のデフォルト AWS KMS キーストアは、データ主権と一般的な規制要件を満たす AWS クラウド ことができます。ただし、中には暗号化キーがクラウド環境の外部で作成および管理され、独立した認可パスと監査パスがあることが必要になる場合があります。の外部キーストアを使用すると AWS KMS、組織が の外部で所有および管理するキーマテリアルを使用して個人データを暗号化できます AWS クラウド。 AWS KMS API は通常どおり操作しますが、指定した外部キーストアプロキシ (XKS プロキシ) ソフトウェアとのみ AWS KMS 操作します。その後、外部キーストアプロキシは、 AWS KMS と外部キーマネージャーとの間のすべての通信を仲介します。

データ暗号化に外部キーストアを使用する場合は、 AWS KMSでキーを維持する場合と比較して、追加の運用オーバーヘッドを考慮することが重要です。外部キーストアを使用して、外部キーストアを作成、設定、維持する必要があります。また、XKS プロキシなど、維持する必要がある追加のインフラストラクチャで エラーが発生し、接続が失われた場合、ユーザーは一時的にデータの復号やアクセスができなくなる可能性があります。コンプライアンスおよび規制関係者と緊密に連携し、個人データの暗号化に関する法的および契約上の義務と、可用性と回復性に関するサービスレベル契約について理解します。

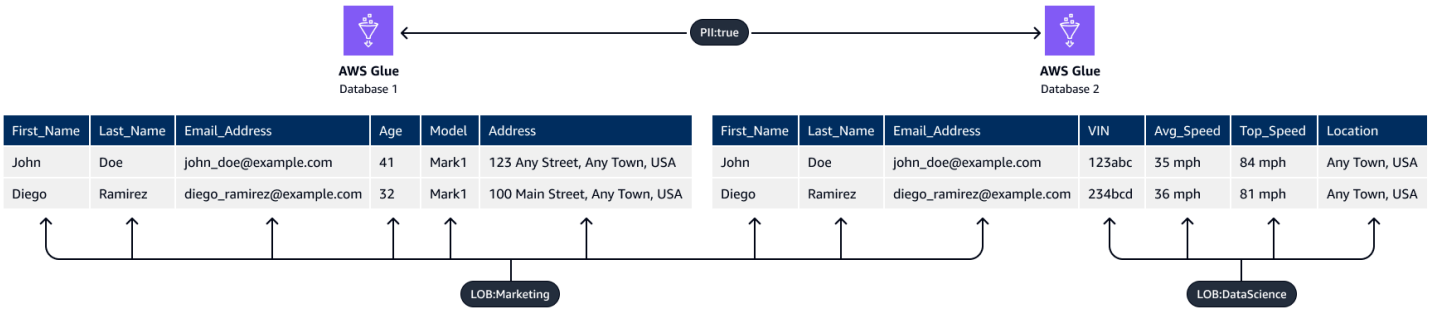
AWS Lake Formation

構造化メタデータカタログを介してデータセットをカタログ化および分類する多くの組織が、それらのデータセットを組織全体で共有したいと考えています。 AWS Identity and Access Management (IAM) アクセス許可ポリシーを使用してデータセット全体へのアクセスを制御できますが、さまざまな機密性の個人データを含むデータセットには、より詳細な制御が必要になることがよくあります。例えば、目的仕様と使用制限 (FPC ウェブサイト) では、マーケティングチームが顧客の住所へのアクセスを必要とする一方で、データサイエンスチームではそれを必要としていないことを示すことができます。

データレイクには、元の形式で大量の機密データへのアクセスを一元化するというプライバシー上の課題もあります。組織のデータの大部分は 1 か所で一元的にアクセスできるため、データセットの論理的な分離、特に個人データを含むデータセットの論理的な分離が最優先事項となります。AWS

Lake Formation では、データを共有するときに、単一のソースからであってもデータレイクに含まれる多数のソースからであっても、ガバナンスとモニタリングを設定することができます。 AWS PRA では、Lake Formation を使用して、データアカウントの共有データバケット内のデータへのきめ細かなアクセスコントロールを提供できます。

Lake Formation でタグベースのアクセスコントロール機能を使用できます。タグベースのアクセスコントロールは、属性に基づいて許可を定義する認可戦略です。これらの属性は、Lake Formation で LF タグと呼ばれています。LF タグを使用すると、これらのタグを Data Catalog データベース、テーブル、列にアタッチし、IAM プリンシパルに同じタグを付与できます。Lake Formation は、プリンシパルでリソースのタグ値と一致するタグ値にアクセス許可が付与されたときに、それらのリソースに対する操作を許可します。次の図は、LF タグとアクセス許可を割り当てて、個人データへの差別化されたアクセスを提供する方法を示しています。



この例では、タグの階層的な性質を使用します。どちらのデータベースにも個人を特定できる情報 (PII:true) が含まれていますが、列レベルのタグによって特定の列が異なるチームに制限されます。この例では、LF タグを持つ IAM PII:true プリンシパルは、このタグを持つ AWS Glue データベースリソースにアクセスできます。LOB:DataScience LF タグを持つプリンシパルは、このタグを持つ特定の列にアクセスでき、LOB:Marketing LF タグを持つプリンシパルは、このタグを持つ列にのみアクセスできます。マーケティングは、マーケティングユースケースに関連する PII にのみアクセスでき、データサイエンスチームは、データサイエンスユースケースに関連する PII にのみアクセスできます。

AWS Local Zones

データレジデンシー要件に準拠する必要がある場合は、これらの要件をサポートするために、特定の に個人データを保存および処理するリソース AWS リージョン をデプロイできます。また、 を使用することもできます。これはAWS Local Zones、コンピューティング、ストレージ、データベース、その他の一部の AWS リソースを大規模な人口や業界の中心の近くに配置するのに役立ちます。ローカルゾーンは、大都市圏に地理的に近い AWS リージョン の拡張子です。ローカルゾーンが対応するリージョンの近くで、特定のタイプのリソースをローカルゾーン内に配置できます。ローカルゾーンは、同じ法的管轄区域内でリージョンが利用できない場合に、データレジデンシー要件を満た

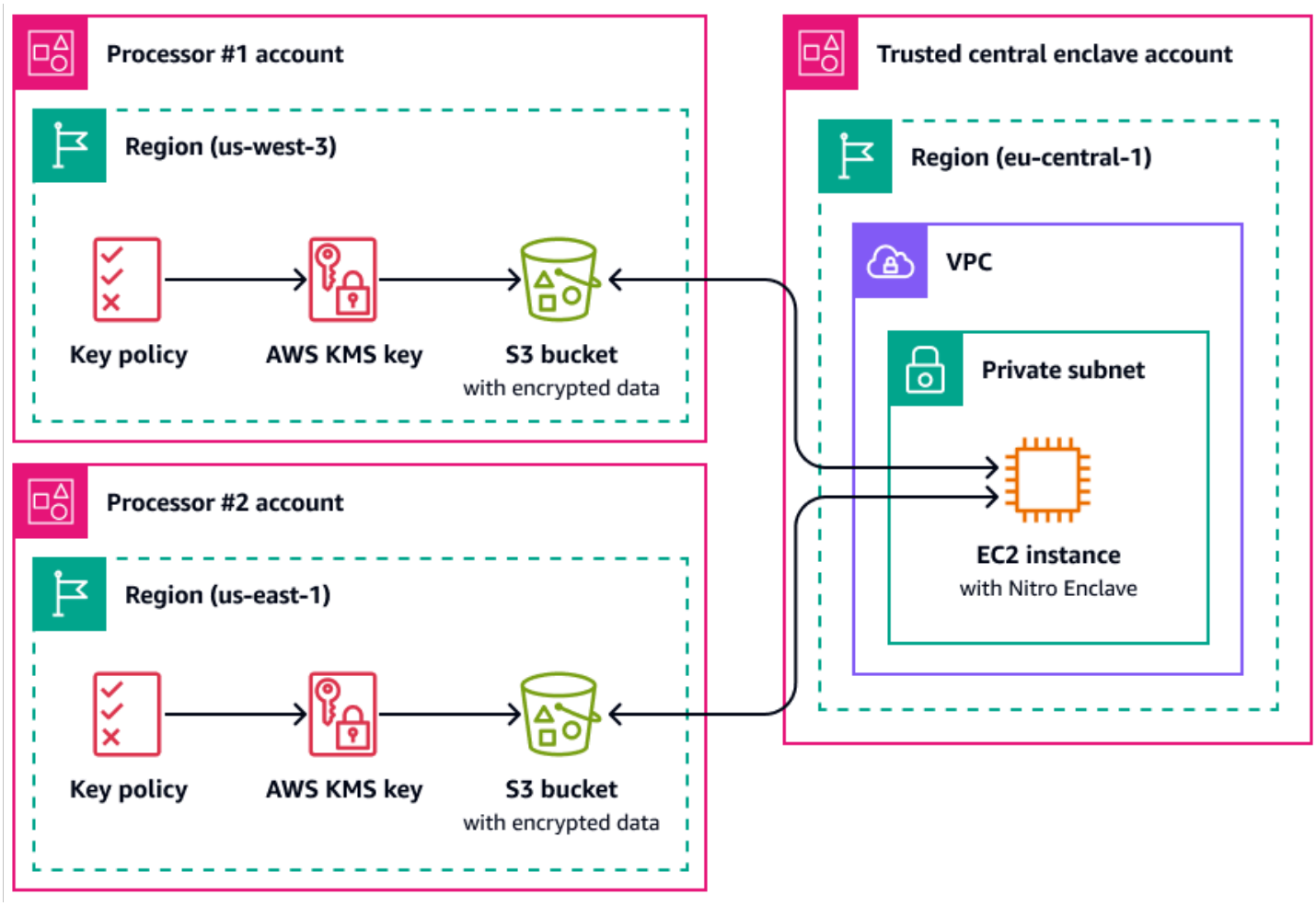
すのに役立ちます。ローカルゾーンを使用する場合は、組織内にデプロイされているデータレジデンシーコントロールを検討してください。例えば、特定のローカルゾーンから別のリージョンへのデータ転送を防ぐためにコントロールが必要となる場合があります。SCPs「ランディングゾーンコントロール AWS Local Zones を使用して のデータレジデンシーを管理するためのベストプラクティス」(AWS ブログ記事) を参照してください。

AWS Nitro Enclaves

Amazon Elastic Compute Cloud (Amazon EC2) などのコンピューティングサービスを使用して個人データを処理するなど、処理の観点からデータセグメンテーション戦略を検討してください。大規模なアーキテクチャ戦略の一環としての機密コンピューティングは、隔離され、保護され、信頼できる CPU エンクレーブで個人データの処理を分離するのに役立ちます。エンクレーブは、分離され、強化され、制約の厳しい仮想マシンです。AWS Nitro Enclaves は、これらの分離されたコンピューティング環境の作成に役立つ Amazon EC2 の機能です。詳細については、「The Security Design of the AWS Nitro System」(AWS ホワイトペーパー) を参照してください。

Nitro Enclaves は、親インスタンスのカーネルから分離されたカーネルをデプロイします。親インスタンスのカーネルは、エンクレーブにアクセスできません。ユーザーは、エンクレーブ内のデータやアプリケーションに SSH またはリモートでアクセスすることはできません。個人データを処理するアプリケーションはエンクレーブに埋め込み、エンクレーブの Vsock を使用するように設定できます。これは、エンクレーブと親インスタンス間の通信を促進するソケットです。

Nitro Enclaves が役立つユースケースの 1 つは、別々の 2 つのデータプロセッサ間のジョイント処理 AWS リージョン であり、相互に信頼しない可能性があります。次の図は、エンクレーブを中央処理に使用する方法、エンクレーブに送信される前に個人データを暗号化するための KMS キー、および復号をリクエストするエンクレーブが認証ドキュメントで一意の測定値を持っていることを確認する AWS KMS key ポリシーについて示しています。詳細と手順については、「 での暗号化認証の使用 AWS KMS」を参照してください。サンプルキーポリシーについては、このガイドの「AWS KMS キーを使用するには認証が必要です」を参照してください。



この実装では、それぞれのデータ処理者と基盤となるエンクレーブのみがプレーンテキストの個人データにアクセスできます。それぞれのデータ処理者の環境外でデータが公開される唯一の場所は、エンクレーブ自体にあります。エンクレーブ自体は、アクセスや改ざんを防ぐように設計されています。

AWS PrivateLink

多くの組織は、信頼できないネットワークへの個人データの公開を制限したいと考えています。例えば、アプリケーションアーキテクチャ設計全体のプライバシーを強化する場合、データの機密性に基づいてネットワークをセグメント化できます (「AWS のサービス データのセグメント化に役立つ および の機能」セクションで説明されているデータセットの論理的および物理的な分離に似ています)。AWS PrivateLink は、仮想プライベートクラウド (VPC) から VPC 外のサービスへの一方向のプライベート接続を作成するのに役立ちます。 AWS PrivateLinkを使用すると、お使いの環境に個人データを保存または処理するサービスへの専用プライベート接続を設定できます。パブリックエンドポイントに接続する必要も、信頼できないパブリックネットワークを介してこのデータを転送する必要もありません。対象範囲内 AWS PrivateLink のサービスのサービスエンドポイントを有

効にすると、通信にインターネットゲートウェイ、NAT デバイス、パブリック IP アドレス、 AWS Direct Connect 接続、または AWS Site-to-Site VPN 接続は必要ありません。 AWS PrivateLink を使用して個人データへのアクセスを提供するサービスに接続する場合、VPC エンドポイントポリシーとセキュリティグループを使用して、組織のデータ境界定義に従ってアクセスを制御できます。信頼された組織内の IAM 原則と AWS リソースのみがサービスエンドポイントにアクセスできるようにするサンプル VPC エンドポイントポリシーについては、このガイド組織メンバーシップの VPC リソースへのアクセス要求の「」を参照してください。

AWS Resource Access Manager

AWS Resource Access Manager (AWS RAM) は、 間でリソースを安全に共有 AWS アカウント し、運用オーバーヘッドを削減し、可視性と監査性を提供します。マルチアカウントセグメンテーション戦略を計画する際には、 AWS RAM を使用して、分離された別のアカウントに保存されている個人データストアを共有することを検討してください。その個人データは、処理を目的として他の信頼されたアカウントと共有できます。では AWS RAM、共有リソースに対して実行できるアクションを定義するアクセス許可を管理できます。へのすべての API コール AWS RAM は CloudTrail に記録されます。また、リソース共有に変更が加えられたときなど AWS RAM、 の特定のイベントについて自動的に通知するように Amazon CloudWatch Events を設定できます。

Amazon S3 の IAM またはバケットポリシーでリソースベースのポリシー AWS アカウント を使用することで、他の と多くのタイプの AWS リソースを共有できますが、 AWS RAM にはプライバシーに関するいくつかの追加の利点があります。 は、データ所有者が 間でデータを共有する方法とユーザーについて、次のような追加の可視性 AWS を提供します AWS アカウント。

- アカウント ID のリストを手動で更新するのではなく、OU 全体とリソースを共有できるようにする
- コンシューマーアカウントが組織に含まれていない場合に、共有を開始するための招待プロセスの適用
- 特定の IAM プリンシパルが個々のリソースにアクセスできる可視性

以前にリソースベースのポリシーを使用してリソース共有を管理し、 AWS RAM 代わりに を使用する場合は、PromoteResourceShareCreatedFromPolicy API オペレーションを使用します。

Amazon SageMaker AI

Amazon SageMaker AI はマネージド型の機械学習 (ML) サービスで、ML モデルの構築とトレーニングを行い、それらを本番稼働環境に対応したホスティング環境にデプロイします。SageMaker AI は、トレーニングデータの準備とモデル機能の作成を容易に実行できるように設計されています。

Amazon SageMaker Model Monitor

多くの組織は、ML モデルのトレーニング時にデータドリフトを検討しています。データドリフトとは、実稼働データと ML モデルのトレーニングに使用されたデータとの間に有意な差異が生じたり、入力データが時間の経過と共に有意に変化したりすることです。データドリフトは、ML モデル予測の全体的な品質、精度、公平性を低下させる可能性があります。本番稼働中に ML モデルが受け取るデータの統計的性質が、トレーニングに使用されたベースラインデータの性質からドリフトすると、モデルの予測精度が低下していきます。Amazon SageMaker Model Monitor は本番稼働中の Amazon SageMaker AI 機械学習モデルの品質およびデータ品質を継続的に監視します。データドリフトを早期かつプロアクティブに検出することで、モデルの再トレーニング、アップストリームシステムの監査、データ品質の問題の修正などの是正措置を実装できます。Model Monitor を使用すると、モデルを手動で監視したり、追加のツールを構築したりする必要性を軽減できます。

Amazon SageMaker Clarify

Amazon SageMaker Clarify は、モデルのバイアスと説明可能性に関するインサイトを提供します。SageMaker Clarify は、ML モデルデータの準備と全体的な開発フェーズで一般的に使用されます。開発者が性別や年齢などの関心のある属性を指定すると、SageMaker Clarify は一連のアルゴリズムを実行して、これらの属性にバイアスがあるかどうかを検出します。アルゴリズムの実行後、SageMaker Clarify は、バイアスの可能性のある発生源と測定値に関する説明を含むビジュアルレポートを提供するため、バイアスを軽減するステップを計画できます。例えば、ある年齢グループに対するビジネスローンの例が、他の年齢グループと比較して少ない財務データセットで、SageMaker は不均衡にフラグを立てて、その年齢グループに不利なモデルを回避できます。また、その予測を確認し、それらの ML モデルにバイアスがないか継続的に監視することで、トレーニング済みのモデルにバイアスがないかを確認することもできます。最後に、SageMaker Clarify は Amazon SageMaker AI Experiments と統合され、モデルの全体的な予測プロセスに最も寄与した機能について説明するグラフを提供します。この情報は、説明可能性の結果を満たすのに役立ちます。また、特定のモデル入力がモデル動作全体に与える影響よりも大きいかどうかを判断することもできます。

Amazon SageMaker Model Card

Amazon SageMaker Model Card を使用すると、機械学習 (ML) モデルに関する重要な詳細を文書化して、ガバナンスとレポート作成に役立てることができます。これらの詳細には、モデル所有者、汎用、意図したユースケース、実施された仮定、モデルのリスク評価、トレーニングの詳細とメトリクス、評価結果が含まれます。詳細については、AWS 「人工知能とMachine Learningソリューションによるモデルの説明可能性」(AWS ホワイトペーパー) を参照してください。

Amazon SageMaker Data Wrangler

Amazon SageMaker Data Wrangler は、データ準備と特徴量エンジニアリングプロセスを合理化するのに役立つ機械学習ツールです。データサイエンティストや機械学習エンジニアが、機械学習モデルで使用するデータを迅速かつ簡単に準備して変換するのに役立つビジュアルインターフェイスを提供します。Data Wrangler を使用すると、Amazon S3、Amazon Redshift、Amazon Athena などのさまざまなソースからデータをインポートできます。その後、300 を超える組み込みデータ変換を使用して、コードを記述することなく機能をクリーンアップ、正規化、結合できます。

Data Wrangler は、 AWS PRA のデータ準備および機能エンジニアリングプロセスの一部として使用できます。を使用して保管中および転送中のデータ暗号化をサポートし AWS KMS、IAM ロールとポリシーを使用してデータやリソースへのアクセスを制御します。 AWS Glue または Amazon SageMaker Feature Store によるデータマスキングをサポートしています。Data Wrangler を と統合すると AWS Lake Formation、きめ細かなデータアクセスコントロールとアクセス許可を適用できます。Amazon Comprehend で Data Wrangler を使用して、より広範な ML Ops ワークフローの一部として表形式データから個人データを自動的に編集することもできます。詳細については、Amazon SageMaker Data Wrangler を使用して機械学習用の PII を自動的に編集する」(AWS ブログ記事) を参照してください。

Data Wrangler の汎用性により、アカウント番号、クレジットカード番号、社会保障番号、患者名、医療記録や軍事記録など、多くの業界の機密データをマスクできます。機密データへのアクセスを制限するか、編集することを選択できます。

AWS データライフサイクルの管理に役立つ 機能

個人データが不要になった場合は、さまざまなデータストアのデータにライフサイクルポリシーと有効期限ポリシーを使用できます。データ保持ポリシーを設定するときは、個人データが含まれている可能性のある以下の場所を考慮してください。

- Amazon DynamoDB や Amazon Relational Database Service (Amazon RDS) などのデータベース
- Amazon S3 バケット
- CloudWatch および CloudTrail のログ
- AWS Database Migration Service (AWS DMS) および AWS Glue DataBrew プロジェクトの移行からのキャッシュされたデータ
- バックアップとスナップショット

以下の AWS のサービス および 機能は、 AWS 環境でデータ保持ポリシーを設定するのに役立ちます。

- Amazon S3 ライフサイクル - Amazon S3 がオブジェクトのグループに適用するアクションを定義するルールセット。Amazon S3 ライフサイクル設定では、Amazon S3 がお客様に代わって期限切れのオブジェクトを削除するタイミングを定義する有効期限アクションを作成できます。詳細については、「ストレージのライフサイクルの管理」を参照してください。
- Amazon Data Lifecycle Manager – Amazon EC2 で、Amazon Elastic Block Store (Amazon EBS) スナップショットと EBS-backed Amazon マシンイメージ (AMI) の作成、保持、削除を自動化するポリシーを作成します。
- DynamoDB の有効期限 (TTL) – 項目ごとのタイムスタンプを定義して、項目が不要になる時期を特定できます。指定されたタイムスタンプの日付と時刻の直後に、DynamoDB によってテーブルから項目が削除されます。
- CloudWatch Logs のログ保持期間の設定 – 各ロググループの保持ポリシーを 1 日から 10 年の値で調整できます。
- AWS Backup – データ保護ポリシーを一元的にデプロイして、S3 バケット、RDS データベースインスタンス、DynamoDB テーブル、EBS ボリュームなど、さまざまな AWS リソース間でバックアップアクティビティを設定、管理、管理します。バックアップポリシーを AWS リソースに適用するには、リソースタイプを指定するか、既存のリソースタグに基づいて を適用します。一元化されたコンソールからバックアップアクティビティを監査して報告し、バックアップコンプライアンス要件を満たすことができます。

AWS のサービス データのセグメント化に役立つ および の機能

データセグメンテーションは、データを別々のコンテナに保存するためのプロセスです。これにより、各データセットに差別化されたセキュリティと認証措置を提供し、データセット全体に対して公開する影響の範囲を減らすことができます。例えば、すべての顧客データを 1 つの大きなデータベースに保存する代わりに、このデータをより小さく管理しやすいグループにセグメント化できます。

物理的および論理的な分離を使用して、個人データをセグメント化できます。

- 物理的な分離 – データを別々のデータストアに保存するか、データを別々の AWS リソースに分散する行為。データは物理的に分離されますが、両方のリソースから同じプリンシパルにアクセスできる可能性があります。そのため、物理的な分離と論理的な分離を組み合わせることをお勧めします。
- 論理的な分離 – アクセスコントロールを使用してデータを分離する行為。職務機能に応じて、個人データのサブセットへのさまざまなレベルのアクセスが必要となります。論理的な分離を実装す

るサンプルポリシーについては、このガイドの「特定の Amazon DynamoDB 属性へのアクセス権の付与」を参照してください。

論理的な分離と物理的な分離を組み合わせることで、アイデンティティベースのポリシーとリソースベースのポリシーを記述する際の柔軟性、シンプルさ、詳細度を提供し、職務機能間で区別されたアクセスをサポートします。例えば、1 つの S3 バケットで異なるデータ分類を論理的に分離するポリシーを作成するのは、運用上複雑な場合があります。各データ分類に専用の S3 バケットを使用すると、ポリシーの設定と管理が簡単になります。

AWS のサービス データの検出、分類、カタログ化に役立つ および の機能

一部の組織は、データをプロアクティブにカタログ化するための、環境での抽出、ロード、変換 (ELT) ツールの使用を開始していません。これらのお客様は、保存および処理するデータと、その構造化 AWS および分類方法をよりよく理解したいという、データ検出の初期段階にいるかもしれません。Amazon Macie を使用すると、Amazon S3 の PII データをよりよく理解できます。ただし、Amazon Macie は、Amazon Relational Database Service (Amazon RDS) や Amazon Redshift などの他のデータソースの分析には役立ちません。次の 2 つのアプローチを使用すると、大規模なデータマッピング演習の開始時における初期検出を高速化できます。

- 手動アプローチ – 2 つの列と必要な数の行を含むテーブルを作成します。最初の列には、ネットワークパケットのヘッダーまたは本文、または指定した任意のサービスに含まれるデータ特性 (ユーザー名、住所、性別など) を記述します。2 番目の列については、コンプライアンスチームに入力を依頼します。データが個人用と見なされる場合は、2 番目の列に「はい」と入力し、そうでない場合は「いいえ」と入力します。宗教的な分位数や健康データなど、特に機密性が高いと見なされる個人データのタイプを示します。
- 自動アプローチ – AWS Marketplaceを通じて提供されるツールを使用します。このようなツールの 1 つが、Securiti です。これらのソリューションでは、複数の AWS リソースタイプにわたるデータや、他のクラウドサービスプラットフォームのアセットをスキャンおよび検出できる統合機能を提供します。これらの同じソリューションの多くで、一元化されたデータカタログ内のデータアセットとデータ処理アクティビティのインベントリを継続的に収集および維持できます。自動分類を実行するツールに依存している場合、組織内の個人データの定義に合わせて検出および分類ルールを調整する必要が生じる場合があります。

プライバシー関連のポリシーの例

> **アンケート**
>
> 皆様からのご意見をお待ちしています。簡単なアンケートに回答して、PRA AWS に関するフィードバックを提供してください。

機密データを処理する組織の多くが予防的アプローチを取り、検出および事後対応コントロールレイヤーを全体に実装しています。このセクションでは、 AWS Identity and Access Management (IAM) AWS Organizations、および AWS Key Management Service () のプライバシー関連ポリシーの例を示しますAWS KMS。これらのポリシーは、予防的アプローチを使用することで、組織がさまざまな使用、開示制限、海外へのデータ転送に関するプライバシー目標を達成するのに役立ちます。これらのポリシーの多くは、このガイドの前のセクションで参照されています。

このセクションには、次のサンプルポリシーが含まれています。

- 特定の IP アドレスからのアクセスの要求
- 組織メンバーシップの VPC リソースへのアクセス要求
- 間でのデータ転送を制限する AWS リージョン
- 特定の Amazon DynamoDB 属性へのアクセス権の付与
- VPC 設定の変更を制限する
- AWS KMS キーを使用するには認証が必要です

特定の IP アドレスからのアクセスの要求

> **アンケート**
>
> 皆様からのご意見をお待ちしています。簡単なアンケートに回答して、PRA AWS に関するフィードバックを提供してください。

このポリシーでは、通話が `192.0.2.0/24` または `203.0.113.0/24` の範囲内にある IP アドレスからのものである場合にのみ、`john_stiles` ユーザーが IAM ロールを引き受けることができます。このポリシーは、個人データの意図しない開示や海外への不要なデータ転送を防ぐのに役立ちま

す。例えば、組織に個人データへのアクセスを必要とするカスタマーサポートスタッフがいる場合、そのサポートスタッフが特定の のサブセットにあるオフィスからのみそのデータにアクセスすることが必要になる場合があります AWS リージョン。また、一部のポリシーでは、特定のユーザーまたは IP アドレスへのアクセスを制限する Condition または Principal セクションが必要になる場合があるため、組織の PII の定義を確認してください。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/john_stiles"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/john_stiles"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "NotIpAddress": {
          "aws:SourceIp": [
            "192.0.2.0/24",
            "203.0.113.0/24"
          ]
        }
      }
    }
  ]
}
```

組織メンバーシップの VPC リソースへのアクセス要求

> **アンケート**
>
> 皆様からのご意見をお待ちしています。簡単なアンケートに回答して、PRA AWS に関するフィードバックを提供してください。

この VPC エンドポイントポリシーは、o-1abcde123組織の AWS Identity and Access Management (IAM) プリンシパルとリソースのみが Amazon Personalize (Amazon S3) エンドポイントにアクセスすることを許可します。この予防的コントロールは、信頼ゾーンを確立し、個人データの境界を定義するのに役立ちます。このポリシーによって組織内のプライバシーと個人データを保護する方法の詳細については、このガイドの「AWS PrivateLink」を参照してください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowOnlyIntendedResourcesAndPrincipals",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "o-1abcde123",
                    "aws:ResourceOrgID": "o-1abcde123"
                }
            }
        }
    ]
}
```

間でのデータ転送を制限する AWS リージョン

> **アンケート**
>
> 皆様からのご意見をお待ちしています。簡単なアンケートに回答して、PRA AWS に関するフィードバックを提供してください。

2 つの AWS Identity and Access Management (IAM) ロールを除き、このサービスコントロールポリシーは eu-west-1および AWS リージョン 以外の のリージョン AWS のサービス への API コールを拒否しますeu-central-1。この SCP は、未承認のリージョンでの AWS ストレージおよび処理サービスの作成を防ぐのに役立ちます。これにより、それらのリージョン AWS のサービスで によって個人データが完全に処理されるのを防ぐことができます。このポリシーは、IAM などのグローバル AWS のサービス、および AWS Key Management Service (AWS KMS) や Amazon

CloudFront などのグローバルサービスと統合するサービスを考慮するため、 NotActionパラメータを使用します。パラメータ値では、これらのグローバルサービスやその他の適用不可能なサービスを例外として指定できます。このポリシーによって組織内のプライバシーと個人データを保護する方法の詳細については、このガイドの「AWS Organizations」を参照してください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "a4b:*",
                "acm:*",
                "aws-marketplace-management:*",
                "aws-marketplace:*",
                "aws-portal:*",
                "budgets:*",
                "ce:*",
                "cloudfront:*",
                "config:*",
                "cur:*",
                "directconnect:*",
                "ec2:DescribeRegions",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeVpnGateways",
                "fms:*",
                "globalaccelerator:*",
                "health:*",
                "iam:*",
                "importexport:*",
                "kms:*",
                "mobileanalytics:*",
                "networkmanager:*",
                "organizations:*",
                "pricing:*",
                "route53:*",
                "route53domains:*",
                "route53-recovery-cluster:*",
                "route53-recovery-control-config:*",
                "route53-recovery-readiness:*",
                "s3:GetAccountPublic*",
                "s3:ListAllMyBuckets",
```

```
                "s3:ListMultiRegionAccessPoints",
                "s3:PutAccountPublic*",
                "shield:*",
                "sts:*",
                "support:*",
                "trustedadvisor:*",
                "waf-regional:*",
                "waf:*",
                "wafv2:*",
                "wellarchitected:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

特定の Amazon DynamoDB 属性へのアクセス権の付与

> **アンケート**
>
> 皆様からのご意見をお待ちしています。簡単なアンケートに回答して、PRA AWS に関するフィードバックを提供してください。

組織が個人データを物理的および論理的に分離する戦略について議論するときは、 AWS Identity and Access Management (IAM) できめ細かなアクセスコントロールポリシーをサポートする AWS ストレージサービスを検討してください。次のアイデンティティベースのポリシーで

は、UserID、SignUpTime、および LastLoggedIn 属性のみを Users という名前の Amazon DynamoDB テーブルから取得できます。例えば、このロールに完全な個人用データセットへのアクセス権を付与する代わりに、このポリシーをカスタマーサポートロールにアタッチできます。このポリシーによって組織内のプライバシーと個人データを保護する方法の詳細については、このガイドの「AWS のサービス データのセグメント化に役立つ および の機能」を参照してください。

```
{
   "Version": "2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "dynamodb:GetItem",
            "dynamodb:BatchGetItem",
            "dynamodb:Query",
            "dynamodb:Scan"
         ],
         "Resource":[
            "arn:aws:dynamodb:us-west-2:123456789012:dynamodb:table/Users"
         ],
         "Condition":{
            "ForAllValues:StringEquals":{
               "dynamodb:Attributes":[
                  "UserID",
                  "SignUpTime",
                  "LastLoggedIn"
               ]
            },
            "StringEquals":{
               "dynamodb:Select":[
                  "SPECIFIC_ATTRIBUTES"
               ]
            }
         }
      }
   ]
}
```

VPC 設定の変更を制限する

> **アンケート**
>
> 皆様からのご意見をお待ちしています。簡単なアンケートに回答して、PRA AWS に関するフィードバックを提供してください。

ネットワークデータフローを含むクロスボーダーデータ転送要件をサポートする AWS インフラストラクチャを設計してデプロイしたら、変更を防ぐことができます。次のサービスコントロールポリシーは、VPC 設定のドリフトや意図しない変更を防ぐのに役立ちます。新しいインターネットゲートウェイアタッチメント、VPC ピアリング接続、トランジットゲートウェイアタッチメント、および新しい VPN 接続を拒否します。このポリシーによって組織内のプライバシーと個人データを保護する方法の詳細については、このガイドの「AWS Transit Gateway」を参照してください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachInternetGateway",
                "ec2:CreateInternetGateway",
                "ec2:CreateVpcPeeringConnection",
                "ec2:AcceptVpcPeeringConnection",
                "ec2:CreateVpc",
                "ec2:CreateSubnet",
                "ec2:CreateRouteTable",
                "ec2:CreateRoute",
                "ec2:AssociateRouteTable",
                "ec2:ModifyVpcAttribute",
                "ec2:*TransitGateway",
                "ec2:*TransitGateway*",
                "globalaccelerator:Create*",
                "globalaccelerator:Update*"

            ],
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalARN": [
```

```
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

AWS KMS キーを使用するには認証が必要です

> **アンケート**
>
> 皆様からのご意見をお待ちしています。簡単なアンケートに回答して、PRA AWS に関するフィードバックを提供してください。

次の AWS Key Management Service (AWS KMS) キーポリシーは、リクエスト内のエンクレーブのアテステーションドキュメントが条件ステートメントの測定値と一致する場合にのみ、 AWS Nitro Enclave インスタンスが KMS キーを使用することを許可します。このポリシーでは、信頼できるエンクレーブのみがデータを復号できます。このポリシーによって組織内のプライバシーと個人データを保護する方法の詳細については、このガイドの「AWS Nitro Enclaves」を参照してください。キーポリシーおよび AWS Identity and Access Management (IAM) ポリシーで使用できる条件キーの完全なリスト AWS KMS については、「 の条件キー AWS KMS」を参照してください。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Enable enclave data processing",
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::123456789012:role/data-processing"
         },
         "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey",
            "kms:GenerateRandom"
         ],
         "Resource": "*",
```

```
         "Condition": {
            "StringEqualsIgnoreCase": {
               "kms:RecipientAttestation:ImageSha384":
 "EXAMPLE8abcdef7abcdef6abcdef5abcdef4abcdef3abcdef2abcdef1abcdef1abcdef0abcdef1abcdEXAMPLE",
               "kms:RecipientAttestation:PCR0":
 "EXAMPLEbc2ecbb68ed99a13d7122abfc0666b926a79d5379bc58b9445c84217f59cfdd36c08b2c79552928702EXAM
               "kms:RecipientAttestation:PCR1":
 "EXAMPLE050abf6b993c915505f3220e2d82b51aff830ad14cbecc2eec1bf0b4ae749d311c663f464cde9f718aEXAM
               "kms:RecipientAttestation:PCR2":
 "EXAMPLEc300289e872e6ac4d19b0b5ac4a9b020c98295643ff3978610750ce6a86f7edff24e3c0a4a445f2ff8EXAM
               "kms:RecipientAttestation:PCR3":
 "EXAMPLE11de9baee597508183477f097ae385d4a2c885aa655432365b53b812694e230bbe8e1bb1b8de748fe1EXAM
               "kms:RecipientAttestation:PCR4":
 "EXAMPLE6b9b3d89a53b13f5dfd14a1049ec0b80a9ae4b159adde479e9f7f512f33e835a0b9023ca51ada02160EXAM
               "kms:RecipientAttestation:PCR8":
 "EXAMPLE34a884328944cd806127c7784677ab60a154249fd21546a217299ccfa1ebfe4fa96a163bf41d3bcfaeEXAM
            }
         }
      }
   ]
}
```

グローバル展開の戦略

> **アンケート**
>
> 皆様からのご意見をお待ちしています。簡単なアンケートに回答して、PRA AWS に関するフィードバックを提供してください。

AWS セキュリティ保証サービスは、グローバルに展開する AWS 際の でのプライバシー設計に関する質問を頻繁に受け取ります。質問は、データ主権の義務や顧客契約など、独自のプライバシー要件への準拠を維持しながら、追加コストや運用上のオーバーヘッドを回避することに対する懸念が中心となります。設計上の考慮事項には、多くの場合、データレジデンシー、オペレーターのアクセス制限、回復性と存続可能性、全体的な独立性が含まれます。詳細については、「 でのデジタル主権要件の達成 AWS」(AWS re:Invent 2022 プレゼンテーション) を参照してください。

以下の質問は一般的なものであり、お客様はご自身のユースケースに応じて回答できます。

- 顧客の個人データはどこに保存する必要がありますか?
- 顧客のデータはどこに保存されていますか?
- 個人データは、どこでどのように国境を越えることができますか?
- リージョンをまたいだデータへの人的アクセスまたはサービスアクセスによって、転送が行われますか?
- 顧客の個人データに外国政府がアクセスしていないことを確認するにはどうすればよいですか?
- バックアップ、ホットサイト、コールドサイトはどこに保存できますか?
- データをローカルに維持するために、サービスを提供するすべてのリージョンで AWS ランディングゾーンを維持する必要がありますか? または、既存の AWS Control Tower ランディングゾーンを使用できますか?

データレジデンシーの要件では、アーキテクチャのデプロイ方法を変えることで、さまざまな組織がうまく機能することがあります。中には、顧客の個人データを特定のリージョン内で保持するという要件を設けている組織もあります。その場合は、これらの義務を順守しながら一般的な規制に準拠する方法について、懸念が生じるかもしれません。状況に関係なく、マルチアカウントデプロイ戦略を選択する際には、複数の考慮事項があります。

主要なアーキテクチャ設計コンポーネントを定義するには、コンプライアンスチームや契約チームと緊密に連携し、個人データがどこで、いつ、どのように AWS リージョンをまたいだかに応じた要件

を確認します。移動、コピー、表示など、データ転送の対象として適格な内容を判断します。さらに、実装する必要がある特定の回復性とデータ保護統制があるかどうかを理解します。バックアップ戦略やディザスタリカバリ戦略に、クロスリージョンフェイルオーバーは必要ですか? 必要な場合は、バックアップデータの保存に使用できるリージョンを決定します。特定の暗号化アルゴリズムやキー生成専用のハードウェアセキュリティモジュールなど、データ暗号化の要件があるかどうかを確認します。これらのトピックについてコンプライアンス関係者と調整したら、マルチアカウント環境での設計アプローチについて検討を開始します。

AWS のマルチアカウント戦略のプラン作成に使用できる 3 つのアプローチを、インフラストラクチャ分離の昇順で次に示します。

- マネージドリージョンを持つ中央ランディングゾーン
- リージョンのランディングゾーン
- AWS 欧州主権雲

また、プライバシーコンプライアンスはデータ主権だけで停止するわけではないと覚えておくことも重要です。このガイドの残りの部分を確認し、同意管理、データ主体の要求、データガバナンス、AI バイアスなど、他の多くの課題に対して考えられる解決策を理解するようにしてください。

マネージドリージョンを持つ中央ランディングゾーン

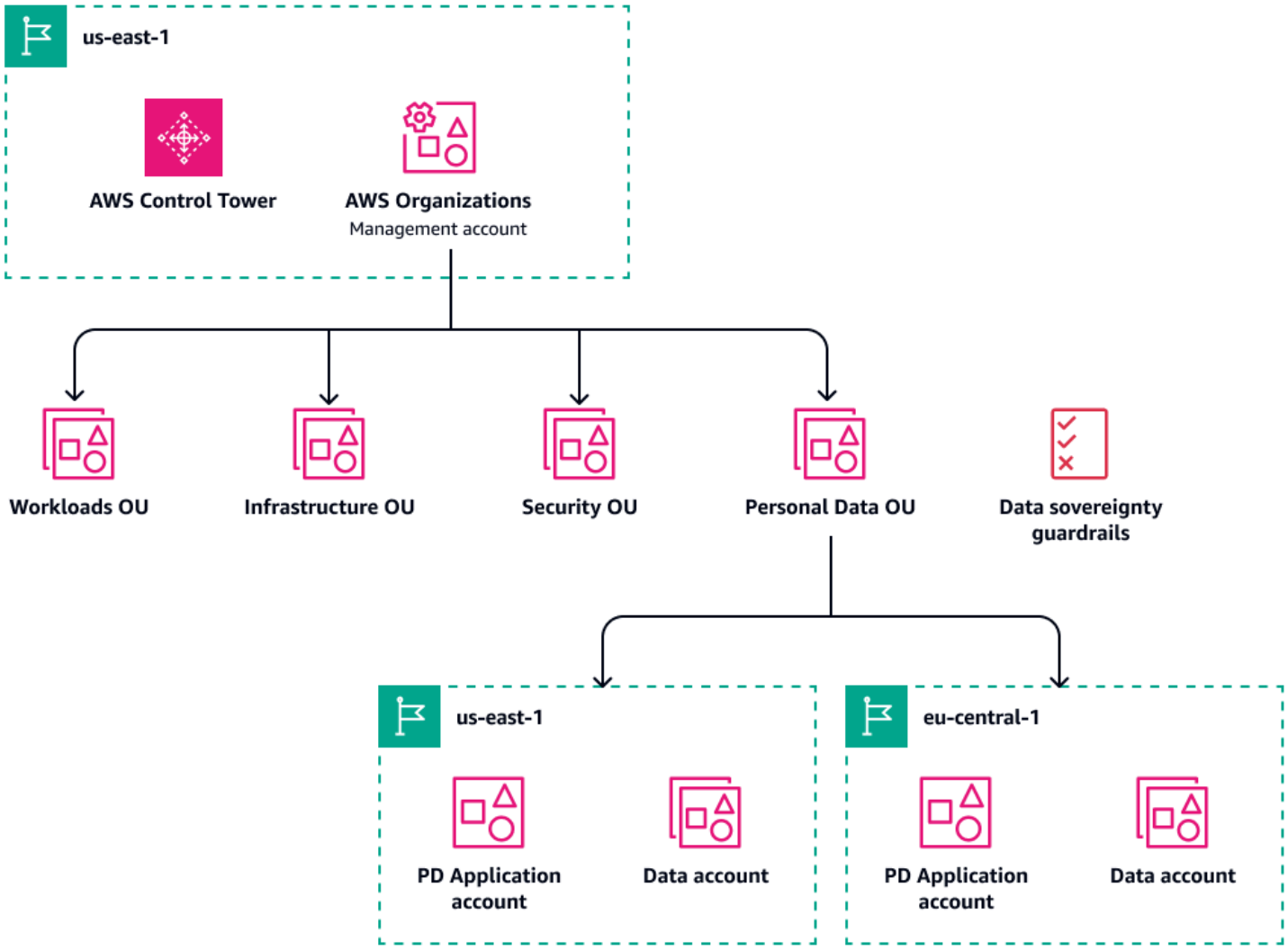
グローバルに拡張したいが、すでにマルチアカウントアーキテクチャを確立している場合は AWS、同じマルチアカウントランディングゾーン (MALZ) を使用して追加を管理することが一般的です AWS リージョン。この設定では、作成したリージョンで、既存の AWS Control Tower ランディングゾーンからのログ記録、Account Factory、一般管理などのインフラストラクチャサービスを引き続き運用します。

本番稼働ワークロードでは、 AWS Control Tower Landing Zone を新しいリージョンに拡張することで、リージョンデプロイを運用できます。これにより、 AWS Control Tower ガバナンスを新しいリージョンに拡張できます。これにより、特定のマネージドリージョン内に個人データストアを保持できます。データは、インフラストラクチャサービスと AWS Control Tower ガバナンスの恩恵を受けるアカウントにまだ存在します。では AWS Organizations、個人データを含むアカウントは引き続き専用の個人データ OU にロールアップされ、 のすべてのデータ主権ガードレール AWS Control Tower が実装されます。さらに、リージョン固有のワークロードは、複数のリージョンに同じワークロードを含む本番稼働用アカウントを確立するのではなく、専用アカウントに含まれています。

このデプロイは最も費用対効果が高い場合がありますが、 AWS アカウント およびリージョンの境界を越えて個人データの流れを制御するには、追加の考慮事項が必要です。以下の点を考慮してください。

- ログには個人データが含まれている可能性があることから、集計中にリージョンをまたぐ転送を防ぐために、機密性の高いフィールドを格納または編集するには追加の設定が必要になる場合があります。リージョン間でのログ集計を制御するための詳細と推奨プラクティスについては、このガイドの「一元化されたログストレージ」を参照してください。
- VPCs の分離と、 AWS Transit Gateway 設計における適切な双方向ネットワークトラフィックフローを考慮します。どの Transit Gateway アタッチメントを許可および承認するかを制限したり、VPC ルートテーブルを変更できるユーザーや内容を制限したりできます。
- クラウド運用チームのメンバーが個人データにアクセスできないようにする必要が生じる場合があります。例えば、顧客のトランザクションデータを含むアプリケーションログは、他のログソースよりも機密性が高いと見なされる可能性があります。ロールベースのアクセスコントロールや属性ベースのアクセスコントロールなど、追加の承認と技術的なガードレールが必要になる場合があります。また、アクセスに関しては、データにレジデンシーの制限が適用されることがあります。例えば、1 つのリージョン A のデータは、そのリージョン内からのみアクセスできます。

次の図は、リージョンデプロイによる一元化されたランディングゾーンを示しています。



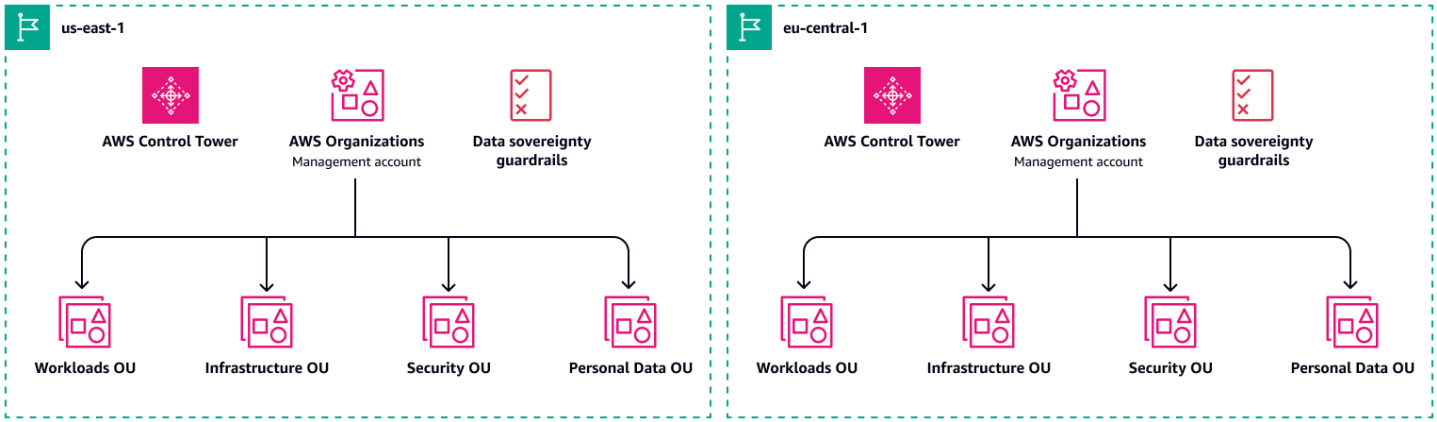
リージョンのランディングゾーン

複数の MALZ を使用すると、非重要なワークロードと比較して個人データを処理するワークロードを完全に分離することで、より厳格なコンプライアンス要件を満たすことができます。 AWS Control Tower 一元化されたログ集約はデフォルトで設定できるため、簡素化されます。このアプローチでは、編集が必要なログの個別のストリームによるログ記録の例外を維持する必要はありません。MALZ ごとにローカルおよび専用のクラウド運用チームを配置し、オペレーターのローカルレジデンシーへのアクセスを制限することもできます。

多くの組織では、米国と欧州のランディングゾーンを別々にデプロイしています。各リージョンのランディングゾーンには、リージョン内のアカウントに対して単一の、包括的なセキュリティ体制と関連するガバナンスがあります。例えば、専用の HSM を使用した個人データの暗号化は、ある MALZ のワークロードでは必要ではないかもしれませんが、別の MALZ では必要になる場合があります。

この戦略は、現在および将来の多くの要件を満たすようにスケールできますが、複数の MALZ の維持に関連する追加コストと運用オーバーヘッドについて理解しておくことが重要です。詳細については、AWS Control Tower 料金表を参照してください。

次の図は、2 つのリージョンの個別のランディングゾーンを示しています。



AWS 欧州主権雲

一部の組織では、欧州経済地域 (EEA) で運用されているワークロードと、他の場所で運用されているワークロードを完全に分離する必要があります。この状況では、AWS European Sovereign Cloud を検討してください。 AWS European Sovereign Cloud は、厳格なデータレジデンシー、運用上の自律性、回復性に関する要件など、顧客が進化するリージョンの主権ニーズを満たすことができるよう設計された、欧州向けの新しい独立したクラウドです。

European Sovereign Cloud AWS は、同じセキュリティ AWS リージョン、可用性、パフォーマンスを提供しながら、既存の から物理的および論理的に分離されています。EU に拠点を置く AWS 従業員のみが、 AWS 欧州主権クラウドの運用とサポートを管理できます。厳格なデータレジデンシー要件がある場合、 AWS European Sovereign Cloud は、作成したすべてのメタデータ (ロール、アクセス許可、リソースラベル、実行に使用する設定など AWS) を EU に保持します。 AWS European Sovereign Cloud には、独自の請求および使用量計測システムも用意されています。

このアプローチでは、前のセクションのリージョンランディングゾーンと同様のパターンを使用します。ただし、欧州のお客様に提供するサービスについては、 AWS 欧州の主権クラウドに専用の MALZ をデプロイできます。

リソース

> **アンケート**
>
> 皆様からのご意見をお待ちしています。簡単なアンケートに回答し、AWS PRA に関するフィードバックをお寄せください。

AWS 規範ガイダンス

- AWS Security Reference ArchitectureAWS (SRA)

AWS ドキュメント

- データ保護 (AWS Well-Architected フレームワーク)
- Data classification (AWS のホワイトペーパー)
- Amazon Web Services: Risk and Compliance (AWS のホワイトペーパー)
- Hybrid architectures to address personal data processing requirements (AWS のホワイトペーパー)
- Navigating GDPR Compliance on AWS (AWS のホワイトペーパー)
- Building a data perimeter on AWS (AWS のホワイトペーパー)
- AWS セキュリティドキュメント

その他の AWS リソース

- AWS Compliance Programs
- AWS 責任共有モデル
- データプライバシーに関するよくある質問
- AWS セキュリティ保証サービス
- AWS Digital Sovereignty Pledge の実現: 妥協のないコントロールの実践 (AWS のブログ記事)
- AWS セキュリティ学習

寄稿者

> **アンケート**
>
> 皆様からのご意見をお待ちしています。簡単なアンケートに回答し、AWS PRA に関するフィードバックをお寄せください。

このガイドは AWS セキュリティ保証サービスチームによって作成されました。このガイドの推奨事項の実装とワークロードの運用については、AWS セキュリティ保証サービスチームにお問い合わせください。

主要著者

- AWS Senior Privacy Consultant、Amber Welch
- AWS Principal Privacy Consultant、Daniel Nieters
- AWS Technical Program Manager、Robert Carter

寄稿者

- AWS Senior Security Consultant、Avik Mukherjee
- AWS Senior Solutions Architect、David Bounds
- AWS Senior Security Solutions Architect、Jeff Lombardo
- AWS Principal Security Solutions Architect、Ram Ramani
- AWS Senior Security Consultant、Vanessa Jacobs
- AWS Senior Privacy Consultant、Thomas Nicholson
- AWS Senior Assurance Consultant、Jose DeJesus
- AWS Solutions Architect Manager、Doug Pardue

テクニカルライター

- AWS Senior Technical Writer、Lilly AbouHarb

ドキュメント履歴

アンケート

皆様からのご意見をお待ちしています。簡単なアンケートに回答し、AWS PRA に関するフィードバックをお寄せください。

以下の表は、本ガイドの重要な変更点について説明したものです。今後の更新に関する通知を受け取る場合は、RSS フィード をサブスクライブできます。

変更	説明	日付
重要な更新	クラウドコンピューティングコンプライアンスコントロールカタログ (C5) を「AWS Artifact」セクションに追加しました。Amazon Security Lake をログアーカイブアカウントに追加しました。Amazon Bedrock、AWS Clean Rooms、Amazon DataZone、AWS Lake Formation、Amazon SageMaker AI、データの検出、分類、カタログ化に役立つ AWS のサービスおよび機能を PD アプリケーションアカウントに追加しました。「グローバル展開の戦略」セクションを追加しました。	2025 年 9 月 16 日
重要な更新	全体的に大幅な更新を行いました。	2024 年 3 月 26 日
初版発行	—	2023 年 10 月 2 日

AWS 規範ガイダンスの用語集

以下は、 AWS 規範ガイダンスによって提供される戦略、ガイド、パターンで一般的に使用される用語です。エントリを提案するには、用語集の最後のフィードバックの提供リンクを使用します。

数字

7 Rs

アプリケーションをクラウドに移行するための 7 つの一般的な移行戦略。これらの戦略は、ガートナーが 2011 年に特定した 5 Rs に基づいて構築され、以下で構成されています。

- リファクタリング/アーキテクチャの再設計 — クラウドネイティブ特徴を最大限に活用して、俊敏性、パフォーマンス、スケーラビリティを向上させ、アプリケーションを移動させ、アーキテクチャを変更します。これには、通常、オペレーティングシステムとデータベースの移植が含まれます。例: オンプレミスの Oracle データベースを Amazon Aurora PostgreSQL 互換エディションに移行する。
- リプラットフォーム (リフトアンドリシェイプ) — アプリケーションをクラウドに移行し、クラウド機能を活用するための最適化レベルを導入します。例: お客様のオンプレミスの Oracle データベースを AWS クラウドの Oracle 用の Amazon Relational Database Service (Amazon RDS) に移行する。
- 再購入 (ドロップアンドショップ) — 通常、従来のライセンスから SaaS モデルに移行して、別の製品に切り替えます。例: 顧客関係管理 (CRM) システムを Salesforce.com に移行する。
- リホスト (リフトアンドシフト) — クラウド機能を活用するための変更を加えずに、アプリケーションをクラウドに移行します。例: お客様のオンプレミスの Oracle データベースを AWS クラウドの EC2 インスタンス上の Oracle に移行する。
- 再配置 (ハイパーバイザーレベルのリフトアンドシフト) – 新しいハードウェアを購入したり、アプリケーションを書き換えたり、既存の運用を変更したりすることなく、インフラストラクチャをクラウドに移行できます。オンプレミスプラットフォームから同じプラットフォームのクラウドサービスにサーバーを移行します。例： Microsoft Hyper-Vアプリケーションを に移行します AWS。
- 保持 (再アクセス) — アプリケーションをお客様のソース環境で保持します。これには、主要なリファクタリングを必要とするアプリケーションや、お客様がその作業を後日まで延期したいアプリケーション、およびそれらを移行するためのビジネス上の正当性がないため、お客様が保持するレガシーアプリケーションなどがあります。
- 廃止 — お客様のソース環境で不要になったアプリケーションを停止または削除します。

A

ABAC

「属性ベースのアクセス制御」をご覧ください。

抽象化されたサービス

「マネージドユーザー」をご覧ください。

ACID

「原子性、一貫性、分離性、耐久性 (ACID)」をご覧ください。

アクティブ/アクティブ移行

(双方向レプリケーションツールまたは二重書き込み操作を使用して) ソースデータベースとターゲットデータベースを同期させ、移行中に両方のデータベースが接続アプリケーションからのトランザクションを処理するデータベース移行方法。この方法では、1 回限りのカットオーバーの必要がなく、管理された小規模なバッチで移行できます。アクティブ/パッシブ移行よりも柔軟な方法ですが、さらに多くの作業が必要となります。

アクティブ/パッシブ移行

ソースデータベースとターゲットデータベースを同期させながら、データがターゲットデータベースにレプリケートされている間、接続しているアプリケーションからのトランザクションをソースデータベースのみで処理するデータベース移行方法。移行中、ターゲットデータベースはトランザクションを受け付けません。

集計関数

複数行に処理を行い、グループ全体を対象に単一の戻り値を計算する SQL 関数。集計関数の例としては、SUM や MAX などがあります。

AI

「人工知能」をご覧ください。

AIOps

「AI オペレーション」をご覧ください。

匿名化

データセット内の個人情報を完全に削除するプロセス。匿名化は個人のプライバシー保護に役立ちます。匿名化されたデータは、もはや個人データとは見なされません。

アンチパターン

繰り返し起こる問題に対して頻繁に用いられる解決策で、その解決策が逆効果であったり、効果がなかったり、代替案よりも効果が低かったりするもの。

アプリケーション制御

マルウェアからシステムを保護するために、承認されたアプリケーションのみを使用できるようにするセキュリティアプローチ。

アプリケーションポートフォリオ

アプリケーションの構築と維持にかかるコスト、およびそのビジネス価値を含む、組織が使用する各アプリケーションに関する詳細情報の集まり。この情報は、ポートフォリオの検出と分析プロセス の重要な要素であり、移行、モダナイズ、最適化するアプリケーションを特定し、優先順位を付けるのに役立ちます。

人工知能 (AI)

コンピューティングテクノロジーを使用し、学習、問題の解決、パターンの認識など、通常は人間に関連づけられる認知機能の実行に特化したコンピュータサイエンスの分野。詳細については、「人工知能 (AI) とは何ですか?」をご覧ください。

AI オペレーション (AIOps)

機械学習技術を使用して運用上の問題を解決し、運用上のインシデントと人の介入を減らし、サービス品質を向上させるプロセス。 AWS 移行戦略での AIOps の使用方法については、オペレーション統合ガイド を参照してください。

非対称暗号化

暗号化用のパブリックキーと復号用のプライベートキーから成る 1 組のキーを使用した、暗号化のアルゴリズム。パブリックキーは復号には使用されないため共有しても問題ありませんが、プライベートキーの利用は厳しく制限する必要があります。

原子性、一貫性、分離性、耐久性 (ACID)

エラー、停電、その他の問題が発生した場合でも、データベースのデータ有効性と運用上の信頼性を保証する一連のソフトウェアプロパティ。

属性ベースのアクセス制御 (ABAC)

部署、役職、チーム名など、ユーザーの属性に基づいてアクセス許可をきめ細かく設定する方法。詳細については、 AWS Identity and Access Management (IAM) ドキュメントの「 の ABAC AWS」を参照してください。

信頼できるデータソース

最も信頼性のある情報源とされるデータのプライマリーバージョンを保存する場所。匿名化、編集、仮名化など、データを処理または変更する目的で、信頼できるデータソースから他の場所にデータをコピーすることができます。

アベイラビリティーゾーン (AZ)

他のアベイラビリティーゾーンの障害から AWS リージョン 隔離され、同じリージョン内の他のアベイラビリティーゾーンへの低コストで低レイテンシーのネットワーク接続を提供する 内の別の場所。

AWS クラウド導入フレームワーク (AWS CAF)

組織がクラウドへの移行を成功させるための効率的で効果的な計画を立て AWS るための、 のガイドラインとベストプラクティスのフレームワークです。 AWS CAF は、ビジネス、人材、ガバナンス、プラットフォーム、セキュリティ、運用という 6 つの重点分野にガイダンスを整理しています。ビジネス、人材、ガバナンスの観点では、ビジネススキルとプロセスに重点を置き、プラットフォーム、セキュリティ、オペレーションの視点は技術的なスキルとプロセスに焦点を当てています。例えば、人材の観点では、人事 (HR)、人材派遣機能、および人材管理を扱うステークホルダーを対象としています。この観点から、 AWS CAF は、クラウド導入を成功させるための組織の準備に役立つ人材開発、トレーニング、コミュニケーションに関するガイダンスを提供します。詳細については、AWS CAF ウェブサイトと AWS CAF のホワイトペーパー を参照してください。

AWS ワークロード認定フレームワーク (AWS WQF)

データベース移行ワークロードを評価し、移行戦略を推奨し、作業見積もりを提供するツール。AWS WQF は AWS Schema Conversion Tool (AWS SCT) に含まれています。データベーススキーマとコードオブジェクト、アプリケーションコード、依存関係、およびパフォーマンス特性を分析し、評価レポートを提供します。

B

不正なボット

個人や組織に混乱や損害を与えることを目的としたボット。

BCP

「ビジネス継続性計画 (BCP)」をご覧ください。

動作グラフ

リソースの動作とインタラクションを経時的に示した、一元的なインタラクティブビュー。Amazon Detective の動作グラフを使用すると、失敗したログオンの試行、不審な API 呼び出し、その他同様のアクションを調べることができます。詳細については、Detective ドキュメントの「動作グラフのデータ」を参照してください。

ビッグエンディアンシステム

最上位バイトを最初に格納するシステム。「エンディアン性」もご覧ください。

二項分類

バイナリ結果 (2 つの可能なクラスのうちの 1 つ) を予測するプロセス。例えば、お客様の機械学習モデルで「この E メールはスパムですか、それともスパムではありませんか」などの問題を予測する必要があるかもしれません。または「この製品は書籍ですか、車ですか」などの問題を予測する必要があるかもしれません。

ブルームフィルター

要素がセットのメンバーであるかどうかをテストするために使用される、確率的でメモリ効率の高いデータ構造。

ブルー/グリーンデプロイ

それぞれが独立しているが、同一の環境を 2 つ作成するデプロイ戦略。現在のアプリケーションバージョンを 1 つの環境 (ブルー) で実行し、新しいアプリケーションバージョンを別の環境 (グリーン) で実行します。この戦略は、最小限の影響で迅速にロールバックするのに役立ちます。

ボット

インターネット経由で自動タスクを実行し、人間のアクティビティややり取りをシミュレートするソフトウェアアプリケーション。インターネット上の情報のインデックスを作成するウェブクローラーなど、一部のボットは有用または有益です。悪質なボットと呼ばれる他のボットの中には、個人や組織を混乱させたり、損害を与えたりすることを意図したものもあります。

ボットネット

マルウェアに感染しており、ボットハーダーまたはボットオペレーターと呼ばれる単一の当事者によって制御されているボットのネットワーク。ボットネットは、ボットとその影響力を拡大する仕組みとして、非常によく知られています。

ブランチ

コードリポジトリに含まれる領域。リポジトリに最初に作成するブランチは、メインブランチといいます。既存のブランチから新しいブランチを作成し、その新しいブランチで機能を開発した

り、バグを修正したりできます。機能を構築するために作成するブランチは、通常、機能ブランチと呼ばれます。機能をリリースする準備ができたら、機能ブランチをメインブランチに統合します。詳細については、「ブランチの概要」(GitHub ドキュメント) を参照してください。

ブレークグラスアクセス

例外的な状況では、承認されたプロセスを通じて、ユーザーが AWS アカウント 通常アクセス許可を持たない にすばやくアクセスできるようにします。詳細については、 AWS Well-Architected ガイダンスの「ブレークグラス手順の実装」インジケータを参照してください。

ブラウンフィールド戦略

環境の既存インフラストラクチャ。システムアーキテクチャにブラウンフィールド戦略を導入する場合、現在のシステムとインフラストラクチャの制約に基づいてアーキテクチャを設計します。既存のインフラストラクチャを拡張している場合は、ブラウンフィールド戦略とグリーンフィールド戦略を融合させることもできます。

バッファキャッシュ

アクセス頻度が最も高いデータが保存されるメモリ領域。

ビジネス能力

価値を生み出すためにビジネスが行うこと (営業、カスタマーサービス、マーケティングなど)。マイクロサービスのアーキテクチャと開発の決定は、ビジネス能力によって推進できます。詳細については、AWSでのコンテナ化されたマイクロサービスの実行ホワイトペーパーの「ビジネス機能を中心に組織化」セクションを参照してください。

ビジネス継続性計画 (BCP)

大規模移行など、中断を伴うイベントが運用に与える潜在的な影響に対処し、ビジネスを迅速に再開できるようにする計画。

C

CAF

「AWS クラウド導入フレームワーク」を参照してください

カナリアデプロイ

エンドユーザーへのバージョンリリースを、時間をかけて段階的に行うこと。確信が持てたら新規バージョンをデプロイして、現在のバージョン全体を置き換えます。

CCoE

「Cloud Center of Excellence」を参照してください。

CDC

「変更データキャプチャ」を参照してください。

変更データキャプチャ (CDC)

データソース (データベーステーブルなど) の変更を追跡し、その変更に関するメタデータを記録するプロセス。CDC は、ターゲットシステムでの変更を監査またはレプリケートして同期を維持するなど、さまざまな目的に使用できます。

カオスエンジニアリング

障害や破壊的なイベントを意図的に導入して、システムの耐障害性をテストすること。AWS Fault Injection Service (AWS FIS) を使用して、 AWS ワークロードにストレスを与え、その応答を評価する実験を実行できます。

CI/CD

「継続的インテグレーションと継続的デリバリー」を参照してください。

分類

予測を生成するのに役立つ分類プロセス。分類問題の機械学習モデルは、離散値を予測します。離散値は、常に互いに区別されます。例えば、モデルがイメージ内に車があるかどうかを評価する必要がある場合があります。

クライアント側の暗号化

ターゲットがデータ AWS のサービス を受信する前のローカルでのデータの暗号化。

Cloud Center of Excellence (CCoE)

クラウドのベストプラクティスの作成、リソースの移動、移行のタイムラインの確立、大規模変革を通じて組織をリードするなど、組織全体のクラウド導入の取り組みを推進する学際的なチーム。詳細については、 AWS クラウド エンタープライズ戦略ブログの CCoE 投稿を参照してください。

クラウドコンピューティング

リモートデータストレージと IoT デバイス管理に通常使用されるクラウドテクノロジー。クラウドコンピューティングは、一般的に、エッジコンピューティングに接続されています。

クラウド運用モデル

IT 組織において、1 つ以上のクラウド環境を構築、成熟、最適化するために使用される運用モデル。詳細については、「クラウド運用モデルの構築」を参照してください。

導入のクラウドステージ

組織が、 AWS クラウドへの移行時に通常実行する 4 つの段階。

- プロジェクト — 概念実証と学習を目的として、クラウド関連のプロジェクトをいくつか実行する
- 基礎固め — お客様のクラウドの導入を拡大するための基礎的な投資 (ランディングゾーンの作成、CCoE の定義、運用モデルの確立など)
- 移行 — 個々のアプリケーションの移行
- 再発明 — 製品とサービスの最適化、クラウドでのイノベーション

これらのステージは、 AWS クラウド エンタープライズ戦略ブログのブログ記事「クラウドファーストへのジャーニー」と「導入のステージ」で Stephen Orban によって定義されました。移行戦略との関連性については、 AWS「移行準備ガイド」を参照してください。

CMDB

「構成管理データベース (CMDB)」を参照してください。

コードリポジトリ

ソースコードやその他の資産 (ドキュメント、サンプル、スクリプトなど) が保存され、バージョン管理プロセスを通じて更新される場所。一般的なクラウドリポジトリには、GitHub や Bitbucket Cloud があります。コードの各バージョンはブランチと呼ばれます。マイクロサービスの構造では、各リポジトリは 1 つの機能専用です。1 つの CI/CD パイプラインで複数のリポジトリを使用できます。

コールドキャッシュ

空である、または、かなり空きがある、もしくは、古いデータや無関係なデータが含まれているバッファキャッシュ。データベースインスタンスはメインメモリまたはディスクから読み取る必要があり、バッファキャッシュから読み取るよりも時間がかかるため、パフォーマンスに影響します。

コールドデータ

めったにアクセスされず、通常は過去のデータです。この種類のデータをクエリする場合、通常は低速なクエリでも問題ありません。このデータを低パフォーマンスで安価なストレージ階層またはクラスに移動すると、コストを削減することができます。

コンピュータビジョン (CV)

機械学習を使用してデジタルイメージやビデオといった、ビジュアル形式の情報を分析および抽出する AI の分野。例えば、Amazon SageMaker AI では、CV 用の画像処理アルゴリズムを利用できます。

設定ドリフト

ワークロードにおいて、設定が想定した状態から変化すること。これによって、ワークロードが非準拠になる可能性がありますが、この状態は、徐々に生じ、意図的なものではありません。

構成管理データベース (CMDB)

データベースとその IT 環境 (ハードウェアとソフトウェアの両方のコンポーネントとその設定を含む) に関する情報を保存、管理するリポジトリ。通常、CMDB のデータは、移行のポートフォリオの検出と分析の段階で使用します。

コンフォーマンスパック

コンプライアンスチェックとセキュリティチェックをカスタマイズするためにアセンブルできる AWS Config ルールと修復アクションのコレクション。YAML テンプレートを使用して、コンフォーマンスパックを AWS アカウント および リージョンの単一のエンティティとしてデプロイすることも、組織全体にデプロイすることもできます。詳細については、 AWS Config ドキュメントの「コンフォーマンスパック」を参照してください。

継続的インテグレーションと継続的デリバリー (CI/CD)

ソフトウェアリリースプロセスのソース、ビルド、テスト、ステージング、本番の各ステージを自動化するプロセス。CI/CD は一般的にパイプラインと呼ばれます。プロセスの自動化、生産性の向上、コード品質の向上、配信の加速化を可能にします。詳細については、「継続的デリバリーの利点」を参照してください。CD は継続的デプロイ (Continuous Deployment) の略語でもあります。詳細については「継続的デリバリーと継続的なデプロイ」を参照してください。

CV

「コンピュータビジョン」を参照してください。

D

保管中のデータ

ストレージ内にあるデータなど、常に自社のネットワーク内にあるデータ。

データ分類

ネットワーク内のデータを重要度と機密性に基づいて識別、分類するプロセス。データに適した保護および保持のコントロールを判断する際に役立つため、あらゆるサイバーセキュリティのリスク管理戦略において重要な要素です。データ分類は、 AWS Well-Architected フレームワークのセキュリティの柱のコンポーネントです。詳細については、「データ分類」を参照してください。

データドリフト

実稼働データと ML モデルのトレーニングに使用されたデータとの間に有意な差異が生じたり、入力データが時間の経過と共に有意に変化したりすることです。データドリフトは、ML モデル予測の全体的な品質、精度、公平性を低下させる可能性があります。

転送中のデータ

ネットワーク内 (ネットワークリソース間など) を活発に移動するデータ。

データメッシュ

非一元的で分散型のデータ所有権を持つとともに、一元的な管理およびガバナンスを行えるアーキテクチャフレームワーク。

データ最小化

厳密に必要なデータのみを収集し、処理するという原則。でデータ最小化を実践 AWS クラウドすることで、プライバシーリスク、コスト、分析のカーボンフットプリントを削減できます。

データ境界

AWS 環境内の一連の予防ガードレール。信頼された ID のみが、期待されるネットワークから信頼されたリソースにアクセスできるようにします。詳細については、「 でのデータ境界の構築 AWS」を参照してください。

データの前処理

raw データをお客様の機械学習モデルで簡単に解析できる形式に変換すること。データの前処理とは、特定の列または行を削除して、欠落している、矛盾している、または重複する値に対処することを意味します。

データ出所

データの生成、送信、保存の方法など、データのライフサイクル全体を通じてデータの出所と履歴を追跡するプロセス。

データ件名

データを収集、処理している個人。

データウェアハウス

分析などのビジネスインテリジェンスをサポートするデータ管理システム。データウェアハウスには、一般的に、大量の履歴データが含まれており、多くの場合、それらはクエリや分析に使用されます。

データベース定義言語 (DDL)

データベース内のテーブルやオブジェクトの構造を作成または変更するためのステートメントまたはコマンド。

データベース操作言語 (DML)

データベース内の情報を変更 (挿入、更新、削除) するためのステートメントまたはコマンド。

DDL

「データベース定義言語」を参照してください。

ディープアンサンブル

予測のために複数の深層学習モデルを組み合わせます。ディープアンサンブルを使用して、より正確な予測を取得したり、予測の不確実性を推定したりできます。

深層学習

人工ニューラルネットワークの複数層を使用して、入力データと対象のターゲット変数の間のマッピングを識別する機械学習サブフィールド。

多層防御

一連のセキュリティメカニズムとコントロールをコンピュータネットワーク全体に層状に重ねて、ネットワークとその内部にあるデータの機密性、整合性、可用性を保護する情報セキュリティの手法。この戦略を に採用するときは AWS、リソースの保護に役立つように、 AWS Organizations 構造の異なるレイヤーに複数のコントロールを追加します。たとえば、多層防御アプローチでは、多要素認証、ネットワークセグメンテーション、暗号化を組み合わせることができます。

委任管理者

では AWS Organizations、互換性のあるサービスが AWS メンバーアカウントを登録して組織のアカウントを管理し、そのサービスのアクセス許可を管理できます。このアカウントを、そのサービスの委任管理者と呼びます。詳細、および互換性のあるサービスの一覧は、 AWS

Organizations ドキュメントの「AWS Organizationsで使用できるサービス」を参照してください。

トラブルシューティング

アプリケーション、新機能、コードの修正をターゲットの環境で利用できるようにするプロセス。デプロイでは、コードベースに変更を施した後、アプリケーションの環境でそのコードベースを構築して実行します。

開発環境

「環境」を参照してください。

検出管理

イベントが発生したときに、検出、ログ記録、警告を行うように設計されたセキュリティコントロール。これらのコントロールは副次的な防衛手段であり、実行中の予防的コントロールをすり抜けたセキュリティイベントをユーザーに警告します。詳細については、「 AWSでのセキュリティコントロールの実装」の「検出的コントロール」を参照してください。

開発バリューストリームマッピング (DVSM)

ソフトウェア開発ライフサイクルのスピードと品質に悪影響を及ぼす制約を特定し、優先順位を付けるために使用されるプロセス。DVSM は、もともとリーンマニュファクチャリング・プラクティスのために設計されたバリューストリームマッピング・プロセスを拡張したものです。ソフトウェア開発プロセスを通じて価値を創造し、動かすために必要なステップとチームに焦点を当てています。

デジタルツイン

建物、工場、産業機器、生産ラインなど、現実世界のシステムを仮想的に表現したものです。デジタルツインは、予知保全、リモートモニタリング、生産最適化をサポートします。

ディメンションテーブル

スタースキーマにおいて、ファクトテーブルの定量データに関するデータ属性が含まれる小さいテーブル。ディメンションテーブルの属性は、通常、テキストフィールド、またはテキストのように扱える個別の数値で示されます。これらの属性は、一般的に、クエリの制約、フィルタリング、結果セットのラベル付けに使用されます。

ディザスタ

ワークロードまたはシステムが、導入されている主要な場所でのビジネス目標の達成を妨げるイベント。これらのイベントは、自然災害、技術的障害、または意図しない設定ミスやマルウェア攻撃などの人間の行動の結果である場合があります。

ディザスタリカバリ (DR)

ディザスタによるダウンタイムとデータ損失を最小限に抑えるための戦略とプロセス。詳細については、 AWS Well-Architected フレームワークの「 でのワークロードのディザスタリカバリ AWS: クラウドでのリカバリ」を参照してください。

DML

「データベース操作言語」を参照してください。

ドメイン駆動型設計

各コンポーネントが提供している変化を続けるドメイン、またはコアビジネス目標にコンポーネントを接続して、複雑なソフトウェアシステムを開発するアプローチ。この概念は、エリック・エヴァンスの著書、Domain-Driven Design: Tackling Complexity in the Heart of Software (ドメイン駆動設計:ソフトウェアの中心における複雑さへの取り組み) で紹介されています (ボストン: Addison-Wesley Professional、2003)。strangler fig パターンでドメイン駆動型設計を使用する方法の詳細については、「コンテナと Amazon API Gateway を使用して、従来の Microsoft ASP.NET (ASMX) ウェブサービスを段階的にモダナイズ」を参照してください。

DR

「ディザスタリカバリ」を参照してください。

ドリフト検出

ベースライン設定からの偏差を追跡します。たとえば、 AWS CloudFormation を使用してシステムリソースのドリフトを検出したり、 を使用して AWS Control Tower 、ガバナンス要件への準拠に影響するランディングゾーンの変更を検出したりできます。

DVSM

「開発バリューストリームマッピング」を参照してください。

E

EDA

「探索的データ分析」を参照してください。

EDI

「電子データ交換」を参照してください。

エッジコンピューティング

IoT ネットワークのエッジにあるスマートデバイスの計算能力を高めるテクノロジー。クラウドコンピューティングと比較すると、エッジコンピューティングは通信レイテンシーを短縮し、応答時間を改善できます。

電子データ交換 (EDI)

組織間で行う、ビジネスドキュメントの自動交換。詳細については、「電子データ交換とは」を参照してください。

暗号化

人間が読み取り可能なプレーンテキストデータを暗号文に変換するコンピューティング処理。

暗号化キー

暗号化アルゴリズムが生成した、ランダム化されたビットからなる暗号文字列。キーの長さは決まっておらず、各キーは予測できないように、一意になるように設計されています。

エンディアン

コンピュータメモリにバイトが格納される順序。ビッグエンディアンシステムでは、最上位バイトが最初に格納されます。リトルエンディアンシステムでは、最下位バイトが最初に格納されます。

エンドポイント

「サービスエンドポイント」を参照してください。

エンドポイントサービス

仮想プライベートクラウド (VPC) 内でホストして、他のユーザーと共有できるサービス。を使用してエンドポイントサービスを作成し AWS PrivateLink 、他の AWS アカウント または AWS Identity and Access Management (IAM) プリンシパルにアクセス許可を付与できます。これらのアカウントまたはプリンシパルは、インターフェイス VPC エンドポイントを作成することで、エンドポイントサービスにプライベートに接続できます。詳細については、Amazon Virtual Private Cloud (Amazon VPC) ドキュメントの「エンドポイントサービスを作成する」を参照してください。

エンタープライズリソースプランニング (ERP)

エンタープライズの主要なビジネスプロセス (会計、MES、プロジェクト管理など) を自動化および管理するシステム。

エンベロープ暗号化

暗号化キーを、別の暗号化キーを使用して暗号化するプロセス。詳細については、 AWS Key Management Service (AWS KMS) ドキュメントの「エンベロープ暗号化」を参照してください。

環境

実行中のアプリケーションのインスタンス。クラウドコンピューティングにおける一般的な環境の種類は以下のとおりです。

- 開発環境 — アプリケーションのメンテナンスを担当するコアチームのみが使用できる、実行中のアプリケーションのインスタンス。開発環境は、上位の環境に昇格させる変更をテストするときに使用します。このタイプの環境は、テスト環境と呼ばれることもあります。
- 下位環境 — 初期ビルドやテストに使用される環境など、アプリケーションのすべての開発環境。
- 本番環境 — エンドユーザーがアクセスできる、実行中のアプリケーションのインスタンス。CI/CD パイプラインでは、本番環境が最後のデプロイ環境になります。
- 上位環境 — コア開発チーム以外のユーザーがアクセスできるすべての環境。これには、本番環境、本番前環境、ユーザー承認テスト環境などが含まれます。

エピック

アジャイル方法論で、お客様の作業の整理と優先順位付けに役立つ機能カテゴリ。エピックでは、要件と実装タスクの概要についてハイレベルな説明を提供します。例えば、 AWS CAF セキュリティエピックには、ID とアクセスの管理、検出コントロール、インフラストラクチャセキュリティ、データ保護、インシデント対応が含まれます。 AWS 移行戦略のエピックの詳細については、プログラム実装ガイドを参照してください。

ERP

「エンタープライズリソース計画」を参照してください。

探索的データ分析 (EDA)

データセットを分析してその主な特性を理解するプロセス。お客様は、データを収集または集計してから、パターンの検出、異常の検出、および前提条件のチェックのための初期調査を実行します。EDA は、統計の概要を計算し、データの可視化を作成することによって実行されます。

F

ファクトテーブル

スタースキーマの中央にあるテーブル。ビジネスオペレーションに関する定量的データが保存されます。一般的に、ファクトテーブルは、2 種類の列で構成されます。1 つは測定値が含まれる列、もう 1 つはディメンションテーブルへの外部キーが含まれる列です。

フェイルファスト

開発ライフサイクルを短縮するために、頻繁かつ段階的にテストを行う哲学であり、アジャイルアプローチでは、この考え方がきわめて重要です。

障害分離境界

では AWS クラウド、障害の影響を制限し、ワークロードの耐障害性を高めるのに役立つアベイラビリティーゾーン AWS リージョン、コントロールプレーン、データプレーンなどの境界。詳細については、「AWS 障害分離境界」を参照してください。

機能ブランチ

「ブランチ」を参照してください。

特徴量

お客様が予測に使用する入力データ。例えば、製造コンテキストでは、特徴量は製造ラインから定期的にキャプチャされるイメージの可能性もあります。

特徴量重要度

モデルの予測に対する特徴量の重要性。これは通常、Shapley Additive Deskonations (SHAP) や積分勾配など、さまざまな手法で計算できる数値スコアで表されます。詳細については、「 を使用した機械学習モデルの解釈可能性 AWS」を参照してください。

機能変換

追加のソースによるデータのエンリッチ化、値のスケーリング、単一のデータフィールドからの複数の情報セットの抽出など、機械学習プロセスのデータを最適化すること。これにより、機械学習モデルはデータの恩恵を受けることができます。例えば、「2021-05-27 00:15:37」の日付を「2021 年」、「5 月」、「木」、「15」に分解すると、学習アルゴリズムがさまざまなデータコンポーネントに関連する微妙に異なるパターンを学習するのに役立ちます。

数ショットプロンプト

LLM に、タスクと望ましい出力を示す例を少数提示した後に、類似のタスクを実行させること。この手法は、プロンプトに記述された例 (ショット) からモデルが学習する「インコンテキスト学

習」の一種です。数ショットプロンプトは、特定のフォーマット、推論、専門知識が必要なタスクに効果的です。「ゼロショットプロンプト」も参照してください。

FGAC

「きめ細かなアクセス制御」を参照してください。

きめ細かなアクセス制御 (FGAC)

複数の条件を使用してアクセス要求を許可または拒否すること。

フラッシュカット移行

変更データのキャプチャによる継続的なデータ複製を利用して、段階的なアプローチではなく、可能な限り短時間でデータを移行するデータベース移行方法。目的はダウンタイムを最小限に抑えることです。

FM

「基盤モデル」を参照してください。

基盤モデル (FM)

大規模な深層学習ニューラルネットワークであり、一般化およびラベル付けされていないデータからなる大規模データセットでトレーニングされています。FM により、言語理解、テキストおよび画像生成、自然言語での会話といった、一般的な各種タスクを実行できます。詳細については、「基盤モデルとは何ですか?」を参照してください。

G

生成 AI

AI モデルのサブセット。大量のデータでトレーニングされており、シンプルなテキストプロンプトを使用して、画像、動画、テキスト、オーディオなどの新しいコンテンツやアーティファクトを作成できます。詳細については、「生成 AI とは何ですか?」を参照してください。

ジオブロッキング

「地理的制限」を参照してください。

地理的制限 (ジオブロッキング)

特定の国のユーザーがコンテンツ配信にアクセスできないようにするための、Amazon CloudFront のオプション。アクセスを許可する国と禁止する国は、許可リストまたは禁止リスト

を使って指定します。詳細については、CloudFront ドキュメントの「コンテンツの地理的ディストリビューションの制限」を参照してください。

Gitflow ワークフロー

下位環境と上位環境が、ソースコードリポジトリでそれぞれ異なるブランチを使用する方法。Gitflow ワークフローは古いと見なされている方法であり、トランクベースのワークフローは推奨されている新しい方法です。

ゴールデンイメージ

システムまたはソフトウェアのスナップショットであり、システムまたはソフトウェアの新規インスタンスをデプロイするテンプレートとして使用されます。製造の例で言えば、ゴールデンイメージを使用すると、複数のデバイスにソフトウェアをプロビジョニングして、デバイス製造オペレーションの速度、スケーラビリティ、生産性を向上させることができます。

グリーンフィールド戦略

新しい環境に既存のインフラストラクチャが存在しないこと。システムアーキテクチャにグリーンフィールド戦略を導入する場合、既存のインフラストラクチャ (別名ブラウンフィールド) との互換性の制約を受けることなく、あらゆる新しいテクノロジーを選択できます。既存のインフラストラクチャを拡張している場合は、ブラウンフィールド戦略とグリーンフィールド戦略を融合させることもできます。

ガードレール

組織単位 (OU) 全般のリソース、ポリシー、コンプライアンスを管理するのに役立つ概略的なルール。予防ガードレールは、コンプライアンス基準に一致するようにポリシーを実施します。これらは、サービスコントロールポリシーと IAM アクセス許可の境界を使用して実装されます。検出ガードレールは、ポリシー違反やコンプライアンス上の問題を検出し、修復のためのアラートを発信します。これらは AWS Config、、 AWS Security Hub CSPM、Amazon GuardDuty、、 AWS Trusted Advisor Amazon Inspector、およびカスタム AWS Lambda チェックを使用して実装されます。

H

HA

「高可用性」を参照してください。

異種混在データベースの移行

別のデータベースエンジンを使用するターゲットデータベースへお客様の出典データベースの移行 (例えば、Oracle から Amazon Aurora)。異種間移行は通常、アーキテクチャの再設計作業の一部であり、スキーマの変換は複雑なタスクになる可能性があります。AWS は、スキーマの変換に役立つ AWS SCTを提供します。

高可用性 (HA)

課題や災害が発生した場合に、介入なしにワークロードを継続的に運用できること。HA システムは、自動的にフェイルオーバーし、一貫して高品質のパフォーマンスを提供し、パフォーマンスへの影響を最小限に抑えながらさまざまな負荷や障害を処理するように設計されています。

ヒストリアンのモダナイゼーション

製造業のニーズによりよく応えるために、オペレーションテクノロジー (OT) システムをモダナイズし、アップグレードするためのアプローチ。ヒストリアンは、工場内のさまざまなソースからデータを収集して保存するために使用されるデータベースの一種です。

ホールドアウトデータ

機械学習モデルのトレーニング用データセットから保留される、ラベル付き履歴データの一部。ホールドアウトデータを使用すると、モデル予測をホールドアウトデータと比較して、モデルのパフォーマンスを評価できます。

同種データベースの移行

お客様の出典データベースを、同じデータベースエンジンを共有するターゲットデータベース (Microsoft SQL Server から Amazon RDS for SQL Server など) に移行する。同種間移行は、通常、リホストまたはリプラットフォーム化の作業の一部です。ネイティブデータベースユーティリティを使用して、スキーマを移行できます。

ホットデータ

リアルタイムデータや最近の翻訳データなど、頻繁にアクセスされるデータ。通常、このデータには高速なクエリ応答を提供する高性能なストレージ階層またはクラスが必要です。

ホットフィックス

本番環境の重大な問題を修正するために緊急で配布されるプログラム。緊急性が高いため、通常の DevOps のリリースワークフローからは外れた形で実施されます。

ハイパーケア期間

カットオーバー直後、移行したアプリケーションを移行チームがクラウドで管理、監視して問題に対処する期間。通常、この期間は 1～4 日です。ハイパーケア期間が終了すると、アプリケーションに対する責任は一般的に移行チームからクラウドオペレーションチームに移ります。

I

IaC

「Infrastructure as Code」を参照してください。

ID ベースのポリシー

AWS クラウド 環境内のアクセス許可を定義する 1 つ以上の IAM プリンシパルにアタッチされたポリシー。

アイドル状態のアプリケーション

90 日間の平均的な CPU およびメモリ使用率が 5～20% のアプリケーション。移行プロジェクトでは、これらのアプリケーションを廃止するか、オンプレミスに保持するのが一般的です。

IIoT

「インダストリアル IoT」を参照してください。

イミュータブルインフラストラクチャ

既存インフラストラクチャの更新、パッチ適用、変更などを行わずに、本番環境ワークロードに使用する新規インフラストラクチャをデプロイするモデル。本質的に、イミュータブルインフラストラクチャは、ミュータブルインフラストラクチャよりも一貫性、信頼性、予測性に優れています。詳細については、 AWS Well-Architected フレームワークにある「イミュータブルインフラストラクチャを使用してデプロイする」のベストプラクティスを参照してください。

インバウンド (受信) VPC

AWS マルチアカウントアーキテクチャでは、アプリケーションの外部からネットワーク接続を受け入れ、検査し、ルーティングする VPC。AWS Security Reference Architecture では、アプリケーションとより広範なインターネット間の双方向のインターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションの各 VPC を使用してネットワークアカウントを設定することを推奨しています。

増分移行

アプリケーションを 1 回ですべてカットオーバーするのではなく、小さい要素に分けて移行するカットオーバー戦略。例えば、最初は少数のマイクロサービスまたはユーザーのみを新しいシステムに移行する場合があります。すべてが正常に機能することを確認できたら、残りのマイクロサービスやユーザーを段階的に移行し、レガシーシステムを廃止できるようにします。この戦略により、大規模な移行に伴うリスクが軽減されます。

インダストリー 4.0

2016 年に Klaus Schwab 氏が提唱した用語で、接続、リアルタイムデータ、オートメーション、分析、AI/ML の進歩による、ビジネスプロセスのモダナイズを意味します。

インフラストラクチャ

アプリケーションの環境に含まれるすべてのリソースとアセット。

Infrastructure as Code (IaC)

アプリケーションのインフラストラクチャを一連の設定ファイルを使用してプロビジョニングし、管理するプロセス。IaC は、新しい環境を再現可能で信頼性が高く、一貫性のあるものにするため、インフラストラクチャを一元的に管理し、リソースを標準化し、スケールを迅速に行えるように設計されています。

インダストリアル IoT (IIoT)

製造、エネルギー、自動車、ヘルスケア、ライフサイエンス、農業などの産業部門におけるインターネットに接続されたセンサーやデバイスの使用。詳細については、「インダストリアル IoT (IIoT) デジタルトランスフォーメーション戦略の構築」を参照してください。

インスペクション VPC

AWS マルチアカウントアーキテクチャでは、VPC (同一または異なる 内 AWS リージョン)、インターネット、オンプレミスネットワーク間のネットワークトラフィックの検査を管理する一元化された VPCs。AWS Security Reference Architecture では、アプリケーションとより広範なインターネット間の双方向のインターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションの各 VPC を使用してネットワークアカウントを設定することを推奨しています。

IoT

インターネットまたはローカル通信ネットワークを介して他のデバイスやシステムと通信する、センサーまたはプロセッサが組み込まれた接続済み物理オブジェクトのネットワーク。詳細については、「IoT とは」を参照してください。

解釈可能性

機械学習モデルの特性で、モデルの予測がその入力にどのように依存するかを人間が理解できる度合いを表します。詳細については、「 を使用した機械学習モデルの解釈可能性 AWS」を参照してください。

IoT

「IoT」を参照してください。

IT 情報ライブラリ (ITIL)

IT サービスを提供し、これらのサービスをビジネス要件に合わせるための一連のベストプラクティス。ITIL は ITSM の基盤を提供します。

IT サービス管理 (ITSM)

組織の IT サービスの設計、実装、管理、およびサポートに関連する活動。クラウドオペレーションと ITSM ツールの統合については、オペレーション統合ガイドを参照してください。

ITIL

「IT 情報ライブラリ」を参照してください。

ITSM

「IT サービス管理」を参照してください。

L

ラベルベースアクセス制御 (LBAC)

強制アクセス制御 (MAC) の実装で、ユーザーとデータ自体にそれぞれセキュリティラベル値が明示的に割り当てられます。ユーザーセキュリティラベルとデータセキュリティラベルが交差する部分によって、ユーザーに表示される行と列が決まります。

ランディングゾーン

ランディングゾーンは、スケーラブルで安全な、適切に設計されたマルチアカウント AWS 環境です。これは、組織がセキュリティおよびインフラストラクチャ環境に自信を持ってワークロードとアプリケーションを迅速に起動してデプロイできる出発点です。ランディングゾーンの詳細については、「安全でスケーラブルなマルチアカウント AWS 環境のセットアップ」を参照してください。

大規模言語モデル (LLM)

大量のデータで事前トレーニングされた深層学習 AI モデル。LLM では、質問への回答、ドキュメントの要約、他言語へのテキスト翻訳、文を完成させるなど、さまざまなタスクを実行できます。詳細については、「大規模言語モデル (LLM) とは何ですか?」を参照してください。

大規模な移行

300 台以上のサーバの移行。

LBAC

「ラベルベースアクセス制御」を参照してください。

最小特権

タスクの実行には必要最低限の権限を付与するという、セキュリティのベストプラクティス。詳細については、IAM ドキュメントの「最小特権アクセス許可を適用する」を参照してください。

リフトアンドシフト

「7 Rs」を参照してください。

リトルエンディアンシステム

最下位バイトを最初に格納するシステム。「エンディアン性」もご覧ください。

LLM

「大規模言語モデル」を参照してください。

下位環境

「環境」を参照してください。

M

機械学習 (ML)

パターン認識と学習にアルゴリズムと手法を使用する人工知能の一種。ML は、モノのインターネット (IoT) データなどの記録されたデータを分析して学習し、パターンに基づく統計モデルを生成します。詳細については、「機械学習」を参照してください。

メインブランチ

「ブランチ」を参照してください。

マルウェア

コンピュータのセキュリティやプライバシーを侵害するように設計されたソフトウェア。マルウェアは、コンピュータシステムの中断、機密情報の漏洩、不正アクセスを招く可能性があります。マルウェアの例には、ウイルス、ワーム、ランサムウェア、トロイの木馬、スパイウェア、キーロガーなどがあります。

マネージドサービス

AWS のサービス はインフラストラクチャレイヤー、オペレーティングシステム、プラットフォーム AWS を運用し、エンドポイントにアクセスしてデータを保存および取得します。マネージドサービスの例として、Amazon Simple Storage Service (Amazon S3) と Amazon DynamoDB が挙げられます。このサービスは、抽象化されたサービスとも呼ばれます。

製造実行システム (MES)

生産プロセスを追跡、モニタリング、文書化、制御するソフトウェアシステムであり、工場では、これによって、原材料から製品を完成させます。

MAP

「Migration Acceleration Program」を参照してください。

メカニズム

ツールを作成してその導入を推進し、導入結果を調べて調整を行うための包括的なプロセス。メカニズムとは、運用中にそれ自体を強化し改善するサイクルを意味します。詳細については、AWS 「 Well-Architected フレームワーク」の「メカニズムの構築」を参照してください。

メンバーアカウント

組織の一部である管理アカウント AWS アカウント 以外のすべて AWS Organizations。 アカウントが 組織のメンバーになることができるのは、一度に 1 つのみです。

MES

「製造実行システム」を参照してください。

Message Queuing Telemetry Transport (MQTT)

発行/サブスクライブのパターンに基づく、軽量のマシンツーマシン (M2M) 通信プロトコルであり、リソースに限りのある IoT デバイスに使用されます。

マイクロサービス

明確に定義された API を介して通信し、通常は小規模な自己完結型のチームが所有する、小規模で独立したサービスです。例えば、保険システムには、販売やマーケティングなどのビジネス

機能、または購買、請求、分析などのサブドメインにマッピングするマイクロサービスが含まれる場合があります。マイクロサービスの利点には、俊敏性、柔軟なスケーリング、容易なデプロイ、再利用可能なコード、回復力などがあります。詳細については、AWS「サーバーレスサービスを使用したマイクロサービスの統合」を参照してください。

マイクロサービスアーキテクチャ

各アプリケーションプロセスをマイクロサービスとして実行する独立したコンポーネントを使用してアプリケーションを構築するアプローチ。これらのマイクロサービスは、軽量 API を使用して、明確に定義されたインターフェイスを介して通信します。このアーキテクチャの各マイクロサービスは、アプリケーションの特定の機能に対する需要を満たすように更新、デプロイ、およびスケーリングできます。詳細については、「 でのマイクロサービスの実装 AWS」を参照してください。

Migration Acceleration Program (MAP)

組織がクラウドに移行するための強力な運用基盤を構築し、移行の初期コストを相殺するのに役立つコンサルティングサポート、トレーニング、サービスを提供する AWS プログラム。MAP には、組織的な方法でレガシー移行を実行するための移行方法論と、一般的な移行シナリオを自動化および高速化する一連のツールが含まれています。

大規模な移行

アプリケーションポートフォリオの大部分を次々にクラウドに移行し、各ウェーブでより多くのアプリケーションを高速に移動させるプロセス。この段階では、以前の段階から学んだベストプラクティスと教訓を使用して、移行ファクトリー チーム、ツール、プロセスのうち、オートメーションとアジャイルデリバリーによってワークロードの移行を合理化します。これは、AWS 移行戦略 の第 3 段階です。

移行ファクトリー

自動化された俊敏性のあるアプローチにより、ワークロードの移行を合理化する部門横断的なチーム。移行ファクトリーチームには、通常、運用、ビジネスアナリストおよび所有者、移行エンジニア、デベロッパー、およびスプリントで作業する DevOps プロフェッショナルが含まれます。エンタープライズアプリケーションポートフォリオの 20～50% は、ファクトリーのアプローチによって最適化できる反復パターンで構成されています。詳細については、このコンテンツセットの移行ファクトリーに関する解説とCloud Migration Factory ガイドを参照してください。

移行メタデータ

移行を完了するために必要なアプリケーションおよびサーバーに関する情報。移行パターンごとに、異なる一連の移行メタデータが必要です。移行メタデータの例としては、ターゲットサブネット、セキュリティグループ、 AWS アカウントなどがあります。

移行パターン

移行戦略、移行先、および使用する移行アプリケーションまたはサービスを詳述する、反復可能な移行タスク。例: AWS Application Migration Service を使用して Amazon EC2 への移行をリホストします。

Migration Portfolio Assessment (MPA)

オンラインツール。これによって、 AWS クラウドに移行するビジネスケースの検証に必要な情報を得られます。MPA は、詳細なポートフォリオ評価 (サーバーの適切なサイジング、価格設定、TCO 比較、移行コスト分析) および移行プラン (アプリケーションデータの分析とデータ収集、アプリケーションのグループ化、移行の優先順位付け、およびウェーブプランニング) を提供します。MPA ツール (ログインが必要) は、すべての AWS コンサルタントと APN パートナーコンサルタントが無料で利用できます。

移行準備状況評価 (MRA)

AWS CAF を使用して、組織のクラウド準備状況に関するインサイトを取得し、長所と短所を特定し、特定されたギャップを埋めるためのアクションプランを構築するプロセス。詳細については、移行準備状況ガイドを参照してください。MRA は、AWS 移行戦略の第一段階です。

移行戦略

ワークロードを AWS クラウドに移行するために使用するアプローチ。詳細については、この用語集の 7 Rs エントリと、「組織を動員して大規模な移行を加速する」を参照してください。

ML

「機械学習」を参照してください。

モダナイゼーション

古い (レガシーまたはモノリシック) アプリケーションとそのインフラストラクチャをクラウド内の俊敏で弾力性のある高可用性システムに変換して、コストを削減し、効率を高め、イノベーションを活用します。詳細については、「AWS クラウドでのアプリケーションのモダナイズ戦略」を参照してください。

モダナイゼーション準備状況評価

組織のアプリケーションのモダナイゼーションの準備状況を判断し、利点、リスク、依存関係を特定し、組織がこれらのアプリケーションの将来の状態をどの程度適切にサポートできるかを決定するのに役立つ評価。評価の結果として、ターゲットアーキテクチャのブループリント、モダナイゼーションプロセスの開発段階とマイルストーンを詳述したロードマップ、特定されたギャップに対処するためのアクションプランが得られます。詳細については、「AWS クラウドでのアプリケーションのモダナイゼーションの準備状況を評価する」を参照してください。

モノリシックアプリケーション (モノリス)

緊密に結合されたプロセスを持つ単一のサービスとして実行されるアプリケーション。モノリシックアプリケーションにはいくつかの欠点があります。1 つのアプリケーション機能エクスペリエンスの需要が急増する場合は、アーキテクチャ全体をスケーリングする必要があります。モノリシックアプリケーションの特徴を追加または改善することは、コードベースが大きくなると複雑になります。これらの問題に対処するには、マイクロサービスアーキテクチャを使用できます。詳細については、「モノリスをマイクロサービスに分解する」を参照してください。

MPA

「Migration Portfolio Assessment」を参照してください。

MQTT

「Message Queuing Telemetry Transport」を参照してください。

多クラス分類

複数のクラスの予測を生成するプロセス (2 つ以上の結果の 1 つを予測します)。例えば、機械学習モデルが、「この製品は書籍、自動車、電話のいずれですか?」 または、「このお客様にとって最も関心のある商品のカテゴリはどれですか?」と聞くかもしれません。

ミュータブルなインフラストラクチャ

本番ワークロードに使用する既存のインフラストラクチャを更新および変更するためのモデル。Well-Architected AWS フレームワークでは、一貫性、信頼性、予測可能性を向上させるために、イミュータブルインフラストラクチャの使用をベストプラクティスとして推奨しています。

O

OAC

「オリジンアクセス制御」を参照してください。

OAI

「オリジンアクセスアイデンティティ」を参照してください。

OCM

「組織変更管理」を参照してください。

オフライン移行

移行プロセス中にソースワークロードを停止させる移行方法。この方法はダウンタイムが長くなるため、通常は重要ではない小規模なワークロードに使用されます。

OI

「オペレーション統合」を参照してください。

Ola

「オペレーショナルレベルアグリーメント」を参照してください。

オンライン移行

ソースワークロードをオフラインにせずにターゲットシステムにコピーする移行方法。ワークロードに接続されているアプリケーションは、移行中も動作し続けることができます。この方法はダウンタイムがゼロから最小限で済むため、通常は重要な本番稼働環境のワークロードに使用されます。

OPC-UA

「Open Process Communications - Unified Architecture」を参照してください。

Open Process Communications - Unified Architecture (OPC-UA)

産業オートメーション用のマシンツーマシン (M2M) 通信プロトコル。OPC-UA により、相互運用の際に、データ暗号化、認証、認可の各スキームを標準化できます。

オペレーショナルレベルアグリーメント (OLA)

サービスレベルアグリーメント (SLA) をサポートするために、どの機能的 IT グループが互いに提供することを約束するかを明確にする契約。

運用準備状況レビュー (ORR)

質問と関連するベストプラクティスのチェックリスト。インシデントや起こり得る障害を理解、評価、防止したり、その範囲を縮小したりする際に役立ちます。詳細については、 AWS Well-Architected フレームワークの「Operational Readiness Reviews (ORR)」を参照してください。

運用テクノロジー (OT)

産業オペレーション、機器、インフラストラクチャを制御するために物理環境と連携させるハードウェアおよびソフトウェアシステム。製造分野では、Industry 4.0 への変革を進める上で、OT と情報技術 (IT) システムの統合に焦点が当てられています。

オペレーション統合 (OI)

クラウドでオペレーションをモダナイズするプロセスには、準備計画、オートメーション、統合が含まれます。詳細については、オペレーション統合ガイドを参照してください。

組織の証跡

組織 AWS アカウント 内のすべての のすべてのイベント AWS CloudTrail を ログに記録する によって作成された証跡 AWS Organizations。証跡は、組織に含まれている各 AWS アカウント に作成され、各アカウントのアクティビティを追跡します。詳細については、CloudTrail ドキュメントの「組織の証跡の作成」を参照してください。

組織変更管理 (OCM)

人材、文化、リーダーシップの観点から、主要な破壊的なビジネス変革を管理するためのフレームワーク。OCM は、変化の導入を加速し、移行問題に対処し、文化や組織の変化を推進することで、組織が新しいシステムと戦略の準備と移行するのを支援します。 AWS 移行戦略では、クラウド導入プロジェクトに必要な変化のスピードにより、このフレームワークは人材アクセラレーションと呼ばれます。詳細については、OCM ガイドを参照してください。

オリジンアクセス制御 (OAC)

Amazon Simple Storage Service (Amazon S3) コンテンツを保護するための、CloudFront のアクセス制限の強化オプション。OAC は AWS リージョン、すべての S3 バケット、 AWS KMS (SSE-KMS) によるサーバー側の暗号化、S3 バケットへの動的 PUT および DELETEリクエストをサポートします。

オリジンアクセスアイデンティティ (OAI)

CloudFront の、Amazon S3 コンテンツを保護するためのアクセス制限オプション。OAI を使用すると、CloudFront が、Amazon S3 に認証可能なプリンシパルを作成します。認証されたプリンシパルは、S3 バケット内のコンテンツに、特定の CloudFront ディストリビューションを介してのみアクセスできます。OAC も併せて参照してください。OAC では、より詳細な、強化されたアクセス制御が可能です。

ORR

「運用準備状況レビュー」を参照してください。

OT

「運用テクノロジー」を参照してください。

アウトバウンド (送信) VPC

AWS マルチアカウントアーキテクチャでは、アプリケーション内から開始されたネットワーク接続を処理する VPC。AWS Security Reference Architecture では、アプリケーションとより広範なインターネット間の双方向のインターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションの各 VPC を使用してネットワークアカウントを設定することを推奨しています。

P

アクセス許可の境界

ユーザーまたはロールが使用できるアクセス許可の上限を設定する、IAM プリンシパルにアタッチされる IAM 管理ポリシー。詳細については、IAM ドキュメントのアクセス許可の境界を参照してください。

個人を特定できる情報 (PII)

直接閲覧した場合、または他の関連データと組み合わせた場合に、個人の身元を合理的に推測するために使用できる情報。PII の例には、氏名、住所、連絡先情報などがあります。

PII

「個人を特定できる情報」を参照してください。

プレイブック

クラウドでのコアオペレーション機能の提供など、移行に関連する作業を取り込む、事前定義された一連のステップ。プレイブックは、スクリプト、自動ランブック、またはお客様のモダナイズされた環境を運用するために必要なプロセスや手順の要約などの形式をとることができます。

PLC

「プログラマブルロジックコントローラー」を参照してください。

PLM

「製品ライフサイクル管理」を参照してください。

ポリシー

次の操作を可能にするオブジェクト: アクセス許可を定義する (ID ベースのポリシーを参照)。アクセス条件を指定する (リソースベースのポリシーを参照)。 AWS Organizations の組織における全アカウントにアクセス許可の上限を定義する (サービスコントロールポリシーを参照)。

多言語の永続性

データアクセスパターンやその他の要件に基づいて、マイクロサービスのデータストレージテクノロジーを個別に選択します。マイクロサービスが同じデータストレージテクノロジーを使用している場合、実装上の問題が発生したり、パフォーマンスが低下する可能性があります。マイクロサービスは、要件に最も適合したデータストアを使用すると、より簡単に実装でき、パフォーマンスとスケーラビリティが向上します。

ポートフォリオ評価

移行を計画するために、アプリケーションポートフォリオの検出、分析、優先順位付けを行うプロセス。詳細については、「移行の準備状況の評価」を参照してください。

述語

`true` または `false` を返すためのクエリ条件。一般的に、`WHERE` 句に記述されます。

述語プッシュダウン

データベースクエリを最適化する手法。これによって、転送前にクエリ内のデータをフィルタリングします。この手法を取ると、リレーショナルデータベースから取得し処理する必要のあるデータの量が減少するため、クエリのパフォーマンスが向上します。

予防的コントロール

イベントの発生を防ぐように設計されたセキュリティコントロール。このコントロールは、ネットワークへの不正アクセスや好ましくない変更を防ぐ最前線の防御です。詳細については、「AWSでのセキュリティコントロールの実装」の「予防的コントロール」を参照してください。

プリンシパル

アクションを実行し AWS 、リソースにアクセスできる のエンティティ。このエンティティは通常、、IAM AWS アカウントロール、または ユーザーのルートユーザーです。詳細については、IAM ドキュメントの「ロールに関する用語と概念」にあるプリンシパルを参照してください。

プライバシーバイデザイン

開発プロセス全体を通してプライバシーが考慮されているシステムエンジニアリングのアプローチ。

プライベートホストゾーン

1 つ以上の VPC 内のドメインとそのサブドメインへの DNS クエリに対し、Amazon Route 53 がどのように応答するかに関する情報を保持するコンテナ。詳細については、Route 53 ドキュメントの「プライベートホストゾーンの使用」を参照してください。

プロアクティブコントロール

非準拠リソースのデプロイ防止を目的としたセキュリティコントロール。このコントロールにより、プロビジョニング前にリソースをスキャンします。コントロールに準拠していないリソースは、プロビジョニングされません。詳細については、 AWS Control Tower ドキュメントの「コントロールリファレンスガイド」および「 セキュリティコントロールの実装」の「プロアクティブコントロール」を参照してください。 AWS

製品ライフサイクル管理 (PLM)

製品の設計、開発、発売から、成長、成熟、衰退、廃棄に至る、製品のライフサイクル全体を通してデータとプロセスを管理すること。

本番環境

「環境」を参照してください。

プログラマブルロジックコントローラー (PLC)

製造分野で使用される、信頼性と適応性に優れたコンピュータであり、これによって、マシンをモニタリングするとともに、製造プロセスを自動化します。

プロンプトチェイニング

1 つの LLM プロンプトによる出力を次のプロンプトの入力に使用して、より良いレスポンスを生成します。この手法を使用すると、複雑なタスクをサブタスクに分割したり、事前レスポンスを繰り返し改良または拡張したりできます。これによって、モデルのレスポンスの精度と関連性が向上し、粒度の高いパーソナライズされた結果を得られます。

仮名化

データセット内の個人識別子をプレースホルダー値に置き換えるプロセス。仮名化は個人のプライバシー保護に役立ちます。仮名化されたデータは、依然として個人データとみなされます。

発行/サブスクライブ (pub/sub)

マイクロサービス間の非同期通信を可能にするパターン。これにより、スケーラビリティと応答性を向上させます。例えば、マイクロサービスベースの MES の場合、マイクロサービスは、他のマイクロサービスがサブスクライブ可能なチャネルにイベントメッセージを発行できます。このシステムでは、発行サービスの変更なしに、新規マイクロサービスを追加できます。

Q

クエリプラン

手順などの一連のステップであり、SQL リレーショナルデータベースシステムのデータにアクセスするために使用されます。

クエリプランのリグレッション

データベースサービスのオプティマイザーが、データベース環境に特定の変更が加えられる前に選択されたプランよりも最適性の低いプランを選択すること。これは、統計、制限事項、環境設定、クエリパラメータのバインディングの変更、およびデータベースエンジンの更新などが原因である可能性があります。

R

RACI マトリックス

「実行責任者、説明責任者、協業先、報告先 (RACI)」を参照してください。

RAG

「検索拡張生成」を参照してください。

ランサムウェア

決済が完了するまでコンピュータシステムまたはデータへのアクセスをブロックするように設計された、悪意のあるソフトウェア。

RASCI マトリックス

「実行責任者、説明責任者、協業先、報告先 (RACI)」を参照してください。

RCAC

「行と列のアクセス制御」を参照してください。

リードレプリカ

読み取り専用に使用されるデータベースのコピー。クエリをリードレプリカにルーティングして、プライマリデータベースへの負荷を軽減できます。

リアーキテクト

「7 Rs」を参照してください。

目標復旧時点 (RPO)

最後のデータリカバリポイントからの最大許容時間です。これにより、最後の回復時点からサービスが中断されるまでの間に許容できるデータ損失の程度が決まります。

目標復旧時間 (RTO)

サービスの中断から復旧までの最大許容遅延時間。

リファクタリング

「7 Rs」を参照してください。

リージョン

地理的エリア内の AWS リソースのコレクション。各 AWS リージョン は、耐障害性、安定性、耐障害性を提供するために、他の から分離され、独立しています。詳細については、「アカウントが使用できる AWS リージョン を指定する」を参照してください。

リグレッション

数値を予測する機械学習手法。例えば、「この家はどれくらいの値段で売れるでしょうか?」という問題を解決するために、機械学習モデルは、線形回帰モデルを使用して、この家に関する既知の事実 (平方フィートなど) に基づいて家の販売価格を予測できます。

リホスト

「7 Rs」を参照してください。

リリース

デプロイプロセスで、変更を本番環境に昇格させること。

再配置

「7 Rs」を参照してください。

リプラットフォーム

「7 Rs」を参照してください。

再購入

「7 Rs」を参照してください。

回復性

中断に抵抗または中断から回復するアプリケーションの機能。 AWS クラウドでの回復力を計画する際には、一般的に、高可用性とディザスタリカバリが考慮されます。詳細については、「AWS クラウド の耐障害性」を参照してください。

リソースベースのポリシー

Amazon S3 バケット、エンドポイント、暗号化キーなどのリソースにアタッチされたポリシー。このタイプのポリシーは、アクセスが許可されているプリンシパル、サポートされているアクション、その他の満たすべき条件を指定します。

実行責任者、説明責任者、協業先、報告先 (RACI) に基づくマトリックス

移行活動とクラウド運用に関わるすべての関係者の役割と責任を定義したマトリックス。マトリックスの名前は、マトリックスで定義されている責任の種類、すなわち責任 (R) 、説明責任 (A) 、協議 (C) 、情報提供 (I) に由来します。サポート (S) タイプはオプションです。サポートが含まれる場合は RASCI マトリックスと呼ばれ、含まれない場合は RACI マトリックスと呼ばれます。

レスポンシブコントロール

有害事象やセキュリティベースラインからの逸脱について、修復を促すように設計されたセキュリティコントロール。詳細については、「 AWSでのセキュリティコントロールの実装」の「レスポンシブコントロール」を参照してください。

保持

「7 Rs」を参照してください。

廃止

「7 Rs」を参照してください。

検索拡張生成 (RAG)

生成 AI の技術。これにより、LLM では、レスポンスの生成前に、トレーニングデータソースの外部にある信頼できるデータソースが参照されます。例えば、RAG モデルによって、組織のナレッジベースまたはカスタムデータのセマンティック検索を実行できる場合があります。細については、「RAG (検索拡張生成) とは何ですか?」を参照してください。

ローテーション

定期的にシークレット情報を更新して、攻撃者が認証情報にアクセスするのをより困難にするプロセス。

行と列のアクセス制御 (RCAC)

アクセスルールが定義された、基本的で柔軟な SQL 表現の使用。RCAC は行権限と列マスクで構成されています。

RPO

「目標復旧時点」を参照してください。

RTO

「目標復旧時間」を参照してください。

ランブック

特定のタスクを実行するために必要な手動または自動化された一連の手順。これらは通常、エラー率の高い反復操作や手順を合理化するために構築されています。

S

SAML 2.0

多くの ID プロバイダー (IdP) が使用しているオープンスタンダード。この機能を使用すると、フェデレーティッドシングルサインオン (SSO) が有効になるため、ユーザーは組織内のすべてのユーザーを IAM で作成しなくても、 AWS マネジメントコンソール にログインしたり AWS 、API オペレーションを呼び出すことができます。SAML 2.0 ベースのフェデレーションの詳細については、IAM ドキュメントの「SAML 2.0 ベースのフェデレーションについて」を参照してください。

SCADA

「監視制御とデータ取得」を参照してください。

SCP

「サービスコントロールポリシー」を参照してください。

シークレット

暗号化された形式で保存する AWS Secrets Managerパスワードやユーザー認証情報などの機密情報または制限付き情報。シークレット値とそのメタデータで構成されます。シークレット値には、バイナリ、1 つの文字列、複数の文字列を指定できます。詳細については、Secrets Manager ドキュメントの「Secrets Manager シークレットの概要」を参照してください。

セキュリティバイデザイン

開発プロセス全体を通してセキュリティが考慮されているシステムエンジニアリングのアプローチ。

セキュリティコントロール

脅威アクターによるセキュリティ脆弱性の悪用を防止、検出、軽減するための、技術上または管理上のガードレール。セキュリティコントロールには、主に 4 つの種類があります。4 つとは、予防、検出、レスポンシブ、プロアクティブです。

セキュリティ強化

アタックサーフェスを狭めて攻撃への耐性を高めるプロセス。このプロセスには、不要になったリソースの削除、最小特権を付与するセキュリティのベストプラクティスの実装、設定ファイル内の不要な機能の無効化、といったアクションが含まれています。

Security Information and Event Management (SIEM) システム

セキュリティ情報管理 (SIM) とセキュリティイベント管理 (SEM) のシステムを組み合わせたツールとサービス。SIEM システムは、サーバー、ネットワーク、デバイス、その他ソースからデータを収集、モニタリング、分析して、脅威やセキュリティ違反を検出し、アラートを発信します。

セキュリティレスポンスの自動化

セキュリティイベントへの自動レスポンスまたは自動修復を目的として、事前定義およびプログラムされたアクション。これらの自動化は、セキュリティのベストプラクティスを実装するのに役立つ検出的または応答的な AWS セキュリティコントロールとして機能します。自動レスポンスアクションの例には、VPC セキュリティグループの変更、Amazon EC2 インスタンスへのパッチ適用、認証情報の更新などがあります。

サーバー側の暗号化

送信先で、それ AWS のサービス を受け取る によるデータの暗号化。

サービスコントロールポリシー (SCP)

AWS Organizationsの組織内の、すべてのアカウントのアクセス許可を一元的に管理するポリシー。SCP は、管理者がユーザーまたはロールに委任するアクションに、ガードレールを定義したり、アクションの制限を設定したりします。SCP は、許可リストまたは拒否リストとして、許可または禁止するサービスやアクションを指定する際に使用できます。詳細については、 AWS Organizations ドキュメントの「サービスコントロールポリシー」を参照してください。

サービスエンドポイント

のエントリポイントの URL AWS のサービス。ターゲットサービスにプログラムで接続するには、エンドポイントを使用します。詳細については、「AWS 全般のリファレンス」の「AWS のサービス エンドポイント」を参照してください。

サービスレベルアグリーメント (SLA)

サービスのアップタイムやパフォーマンスなど、IT チームがお客様に提供すると約束したものを明示した合意書。

サービスレベルインジケータ (SLI)

エラー率、可用性、スループットといった、サービスパフォーマンス面の指標。

サービスレベル目標 (SLO)

サービスレベルインジケータによって測定され、サービスの状態を表すターゲットメトリクス。

責任共有モデル

クラウドのセキュリティとコンプライアンス AWS について と共有する責任を説明するモデル。AWS はクラウドのセキュリティを担当しますが、 はクラウドのセキュリティを担当します。詳細については、「責任共有モデル」を参照してください。

SIEM

「Security Information and Event Management システム」を参照してください。

単一障害点 (SPOF)

特定のアプリケーションを構成する単一の重要なコンポーネントで発生し、システム稼働に支障をきたす可能性のある障害。

SLA

「サービスレベルアグリーメント」を参照してください。

SLI

「サービスレベルインジケータ」を参照してください。

SLO

「サービスレベルの目標」を参照してください。

スプリットアンドシードモデル

モダナイゼーションプロジェクトのスケーリングと加速のためのパターン。新機能と製品リリースが定義されると、コアチームは解放されて新しい製品チームを作成します。これにより、お客様の組織の能力とサービスの拡張、デベロッパーの生産性の向上、迅速なイノベーションのサポートに役立ちます。詳細については、「AWS クラウドでのアプリケーションをモダナイズするための段階的アプローチ」を参照してください。

SPOF

「単一障害点」を参照してください。

スタースキーマ

データベースの編成構造を意味し、1 つの大きいファクトテーブルにトランザクションデータまたは測定データが保存され、1 つ以上の小さいディメンションテーブルにデータ属性が保存されます。この構造は、データウェアハウスやビジネスインテリジェンスを用途とするように設計されています。

strangler fig パターン

レガシーシステムが廃止されるまで、システム機能を段階的に書き換えて置き換えることにより、モノリシックシステムをモダナイズするアプローチ。このパターンは、宿主の樹木から根を成長させ、最終的にその宿主を包み込み、宿主に取って代わるイチジクのつるを例えています。そのパターンは、モノリシックシステムを書き換えるときのリスクを管理する方法として Martin Fowler により提唱されました。このパターンの適用方法の例については、「コンテナと Amazon API Gateway を使用して、従来の Microsoft ASP.NET (ASMX) ウェブサービスを段階的にモダナイズ」を参照してください。

サブネット

VPC 内の IP アドレスの範囲。サブネットは、1 つのアベイラビリティーゾーンに存在する必要があります。

監視制御とデータ取得 (SCADA)

製造分野において、ハードウェアとソフトウェアを使用して物理アセットと本番運用をモニタリングするシステム。

対称暗号化

データの暗号化と復号に同じキーを使用する暗号化のアルゴリズム。

合成テスト

ユーザーとのやり取りをシミュレートして、起こり得る問題を検出したり、パフォーマンスをモニタリングしたりすることで、システムをテストします。Amazon CloudWatch Synthetics を使用すると、こうしたテストを作成できます。

システムプロンプト

コンテキスト、指示、ガイドラインなどを提示して、LLM に動作を指示する手法。システムプロンプトは、コンテキストを設定して、ユーザーとやり取りするルールを確立するのに有用です。

T

タグ

AWS リソースを整理するためのメタデータとして機能するキーと値のペア。タグは、 リソースの管理、識別、整理、検索、フィルタリングに役立ちます。詳細については、「AWS リソースのタグ付け」を参照してください。

ターゲット変数

監督された機械学習でお客様が予測しようとしている値。これは、結果変数のことも指します。例えば、製造設定では、ターゲット変数が製品の欠陥である可能性があります。

タスクリスト

ランブックの進行状況を追跡するために使用されるツール。タスクリストには、ランブックの概要と完了する必要のある一般的なタスクのリストが含まれています。各一般的なタスクには、推定所要時間、所有者、進捗状況が含まれています。

テスト環境

「環境」を参照してください。

トレーニング

お客様の機械学習モデルに学習するデータを提供すること。トレーニングデータには正しい答えが含まれている必要があります。学習アルゴリズムは入力データ属性をターゲット (お客様が予測したい答え) にマッピングするトレーニングデータのパターンを検出します。これらのパターンをキャプチャする機械学習モデルを出力します。そして、お客様が機械学習モデルを使用して、ターゲットがわからない新しいデータでターゲットを予測できます。

トランジットゲートウェイ

VPC とオンプレミスネットワークを相互接続するために使用できる、ネットワークの中継ハブ。詳細については、 AWS Transit Gateway ドキュメントの「トランジットゲートウェイとは」を参照してください。

トランクベースのワークフロー

デベロッパーが機能ブランチで機能をローカルにビルドしてテストし、その変更をメインブランチにマージするアプローチ。メインブランチはその後、開発環境、本番前環境、本番環境に合わせて順次構築されます。

信頼されたアクセス

ユーザーに代わって AWS Organizations およびそのアカウントで組織内でタスクを実行するために指定したサービスにアクセス許可を付与します。信頼されたサービスは、サービスにリンクされたロールを必要なときに各アカウントに作成し、ユーザーに代わって管理タスクを実行します。詳細については、 ドキュメントの「Using AWS Organizations with other AWS services AWS Organizations 」を参照してください。

チューニング

機械学習モデルの精度を向上させるために、お客様のトレーニングプロセスの側面を変更する。例えば、お客様が機械学習モデルをトレーニングするには、ラベル付けセットを生成し、ラベルを追加します。これらのステップを、異なる設定で複数回繰り返して、モデルを最適化します。

ツーピザチーム

2 枚のピザを分け合えることができるくらい小さな DevOps チーム。ツーピザチームの規模では、ソフトウェア開発におけるコラボレーションに最適な機会が確保されます。

U

不確実性

予測機械学習モデルの信頼性を損なう可能性がある、不正確、不完全、または未知の情報を指す概念。不確実性には、次の 2 つのタイプがあります。認識論的不確実性は、限られた、不完全なデータによって引き起こされ、弁論的不確実性 は、データに固有のノイズとランダム性によって引き起こされます。

未分化なタスク

ヘビーリフティングとも呼ばれ、アプリケーションの作成と運用には必要だが、エンドユーザーに直接的な価値をもたらさなかったり、競争上の優位性をもたらしたりしない作業です。未分化なタスクの例としては、調達、メンテナンス、キャパシティプランニングなどがあります。

上位環境

「環境」を参照してください。

V

バキューミング

ストレージを再利用してパフォーマンスを向上させるために、増分更新後にクリーンアップを行うデータベースのメンテナンス操作。

バージョンコントロール

リポジトリ内のソースコードへの変更など、変更を追跡するプロセスとツール。

VPC ピアリング

プライベート IP アドレスを使用してトラフィックをルーティングできる、2 つの VPC 間の接続。詳細については、Amazon VPC ドキュメントの「VPC ピア機能とは」を参照してください。

脆弱性

システムのセキュリティを脅かすソフトウェアまたはハードウェアの欠陥。

W

ウォームキャッシュ

頻繁にアクセスされる最新の関連データを含むバッファキャッシュ。データベースインスタンスはバッファキャッシュから、メインメモリまたはディスクからよりも短い時間で読み取りを行うことができます。

ウォームデータ

アクセス頻度の低いデータ。この種類のデータをクエリする場合、通常は適度に遅いクエリでも問題ありません。

ウィンドウ関数

現在のレコードに何らかの形で関連している行のグループに計算を実行する SQL 関数。ウィンドウ関数は、移動平均を計算したり、現在の行の相対位置に基づいて他の行の値にアクセスするといったタスクの処理に役立ちます。

ワークロード

ビジネス価値をもたらすリソースとコード (顧客向けアプリケーションやバックエンドプロセスなど) の総称。

ワークストリーム

特定のタスクセットを担当する移行プロジェクト内の機能グループ。各ワークストリームは独立していますが、プロジェクト内の他のワークストリームをサポートしています。たとえば、ポートフォリオワークストリームは、アプリケーションの優先順位付け、ウェーブ計画、および移行メタデータの収集を担当します。ポートフォリオワークストリームは、これらの設備を移行ワークストリームで実現し、サーバーとアプリケーションを移行します。

WORM

「Write-Once-Read-Many」を参照してください。

WQF

「AWS ワークロード資格フレームワーク」を参照してください

Write-Once-Read-Many (WORM)

データを 1 回のみ書き込むことで、データの削除や変更を防ぐストレージモデル。承認済みユーザーは、必要な回数だけデータを読み取ることができますが、変更することはできません。このデータストレージインフラストラクチャは、イミュータブルと見なされます。

Z

ゼロデイエクスプロイト

ゼロデイ脆弱性を悪用した攻撃 (一般的にマルウェアによる)。

ゼロデイ脆弱性

実稼働システムにおける未解決の欠陥または脆弱性。脅威アクターは、このような脆弱性を利用してシステムを攻撃する可能性があります。開発者は、よく攻撃の結果で脆弱性に気付きます。

ゼロショットプロンプト

LLM にタスク実行の手順は提示するが、実行のガイドとして役立つ例 (ショット) は提示しない方法。LLM は、事前トレーニング済みの知識を使用してタスクを処理する必要があります。ゼロショットプロンプトの有効性は、タスクの複雑さとプロンプトの品質によって異なります。「数ショットプロンプト」も参照してください。

ゾンビアプリケーション

平均 CPU およびメモリ使用率が 5% 未満のアプリケーション。移行プロジェクトでは、これらのアプリケーションを廃止するのが一般的です。

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。