AWS 決定ガイド

AWS セキュリティ、アイデンティティ、ガバナンスサービスの選択

AWS セキュリティ、アイデンティティ、ガバナンスサービスの選択: AWS 決定ガイド

Table of Contents

AWS セキュリティ、アイデンティティ、ガバナンスサービスの選択

最初のステップを実行する

読み取り時間	27 分	
目的	どの AWS セキュリティ、アイデンティティ、ガバナンスサービスが組織に最適かを判断するのに役立ちます。	
最終更新日	2024 年 12 月 30 日	
対象サービス	• AWS Artifact • AWS Audit Manager • AWS Certificate Manager • AWS CloudHSM • AWS CloudTrail • Amazon Cognito • AWS Config • AWS Control Tower • Amazon Detective • AWS Firewall Manager • Amazon GuardDuty • AWS IAM • AWS IAM Identity Center • Amazon Inspector	• AWS KMS • Amazon Macie • AWS Network Firewall • AWS Organizations • AWS Payment Cryptography • AWS Private CA • AWS RAM • AWS Secrets Manager • AWS Security Hub CSPM • Amazon Security Lake • AWS セキュリティインシデント対応 • AWS Shield • AWS WAF

序章

クラウドのセキュリティ、アイデンティティ、ガバナンスは、データとサービスの完全性と安全性を達成し、維持するための重要な要素です。これは、Amazon Web Services () などのクラウドプロバイダーに移行する企業が増えるにつれて、特に重要ですAWS。

このガイドは、ニーズと組織に最適な AWS セキュリティ、アイデンティティ、ガバナンスのサービスとツールを選択するのに役立ちます。

まず、セキュリティ、アイデンティティ、ガバナンスの意味を見てみましょう。

- クラウドセキュリティとは、デジタルアセットを脅威から保護するための対策とプラクティスを使用することです。これには、データセンターの物理的なセキュリティと、オンラインの脅威から保護するためのサイバーセキュリティ対策の両方が含まれます。 は、暗号化されたデータストレージ、ネットワークセキュリティ、潜在的な脅威の継続的なモニタリングを通じてセキュリティを AWS 優先します。
- ID サービスは、スケーラブルな方法で ID、リソース、およびアクセス許可を安全に管理するのに役立ちます。 は、ワークフォースや顧客向けのアプリケーション、ワークロードやアプリケーションへのアクセスを管理するために設計された ID サービス AWS を提供します。
- クラウドガバナンスは、組織がベストプラクティスに従うための指針となる一連のルール、プロセス、レポートです。 AWS リソース全体でクラウドガバナンスを確立し、組み込みのベストプラクティスと標準を使用し、コンプライアンスと監査プロセスを自動化できます。クラウドでのコンプライアンスとは、データ保護とプライバシーに適用される法律と規制を遵守することです。AWS コンプライアンスプログラムは、 AWS と一致する証明書、規制、フレームワークに関する情報を提供します。

この one-and-a-half動画では、 が当社の中核となる強力なセキュリティ AWS を構築する方法をまとめています。

AWS セキュリティ、アイデンティティ、ガバナンスのサービスを理解する

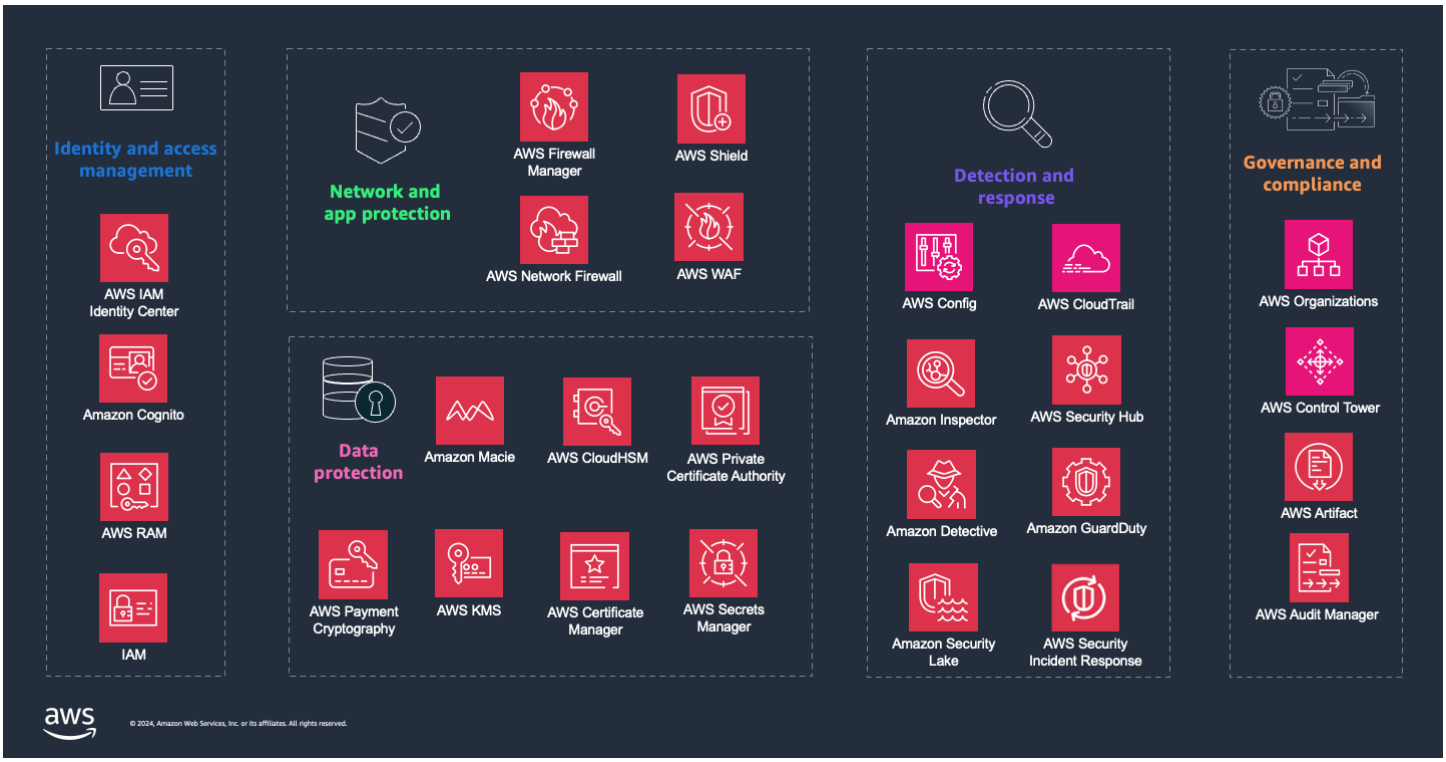
セキュリティとコンプライアンスは責任を共有します

AWS セキュリティ、アイデンティティ、ガバナンスサービスを選択する前に、セキュリティとコンプライアンスがお客様と の間で共有されている責任であることを理解することが重要です AWS。

この責任共有の性質により、運用上の負担が軽減され、デプロイを柔軟に制御できます。この責任の区別は、一般的に「クラウドのセキュリティ」と呼ばれ、「クラウドのセキュリティ」と呼ばれます。

このモデルを理解することで、利用可能なオプションの範囲と、該当する がどのように AWS のサービス 適合するかを理解できます。

ワークロードの保護に役立つ AWS ツールとサービスを組み合わせることができます。



前の図に示すように、 AWS は、クラウドでの堅牢なセキュリティ、ID 管理、ガバナンスの達成と維持に役立つツールとサービスを 5 つのドメインにまたがって提供します。これらの 5 つのドメイン AWS のサービス で を使用すると、次のことを行うことができます。

- データや環境を保護するための多層アプローチを構築する
- 進化する脅威に対してクラウドインフラストラクチャを強化する
- 厳格な規制基準に従う

セキュリティドキュメントを含むセキュリティの詳細については、 AWS AWS 「 セキュリティドキュメント AWS のサービス」を参照してください。

以下のセクションでは、各ドメインについて詳しく説明します。

AWS ID とアクセス管理サービスを理解する

AWS セキュリティの中心にあるのは最小特権の原則です。個人とサービスには必要なアクセスのみがあります。 AWS IAM Identityは、 AWS リソースへのユーザーアクセスを管理する AWS

のサービス ために推奨されます。このサービスを使用して、外部 ID プロバイダーの ID など、アカウントへのアクセスとそれらのアカウント内のアクセス許可を管理できます。

次の表は、このガイドで説明されている ID とアクセスの管理サービスをまとめたものです。

AWS IAM Identity Center

AWS IAM Identity Center は、ID のソースを接続するか、ユーザーを作成するのに役立ちます。複数の AWS アカウント およびアプリケーションへのワークフォースアクセスを一元管理できます。

Amazon Cognito

Amazon Cognito は、組み込みユーザーディレクトリ、エンタープライズディレクトリ、コンシューマー ID プロバイダーからユーザーを認証および認可するためのウェブおよびモバイルアプリ用の ID ツールを提供します。

AWS RAM

AWS RAM を使用すると、リソースを組織全体 AWS アカウント、組織内、IAM ロールおよびユーザーと安全に共有できます。

IAM

IAM を使用すると、 AWS ワークロードリソースへのアクセスを安全かつきめ細かく制御できます。

AWS データ保護サービスを理解する

データ保護はクラウド上で不可欠であり、データ、アカウント、ワークロードの保護に役立つサービス AWS を提供します。たとえば、転送中と保管中の両方のデータを暗号化すると、データが公開されないように保護できます。AWS Key Management Service (AWS KMS) と AWS CloudHSM を使用すると、データを保護するために使用する暗号化キーを作成および制御できます。

次の表は、このガイドで説明されているデータ保護サービスをまとめたものです。

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、関連するリスクに対する自動保護を有効にします。

AWS KMS

AWS KMS は、データを保護するために使用する暗号化キーを作成および制御します。

AWS CloudHSM

AWS CloudHSM は、高可用性のクラウドベースのハードウェアセキュリティモジュール (HSMs。

AWS Certificate Manager

AWS Certificate Manager は、パブリックおよびプライベート SSL/TLS X.509 証明書とキーの作成、保存、更新の複雑さを処理します。

AWS Private CA

AWS Private CA は、ルート認証機関と下位認証機関 (CAs) を含むプライベート認証機関階層の作成に役立ちます。

AWS Secrets Manager

AWS Secrets Manager は、データベース認証情報、アプリケーション認証情報、OAuth トークン、API キー、およびその他のシークレットを管理、取得、ローテーションするのに役立ちます。

AWS Payment Cryptography

AWS Payment Cryptography は、支払いカード業界 (PCI) 標準に従って、支払い処理に使用される暗号化関数とキー管理へのアクセスを提供します。

AWS ネットワークおよびアプリケーション保護サービスを理解する

AWS は、ネットワークとアプリケーションを保護するための複数のサービスを提供します。 AWS Shieldは、分散型サービス拒否 (DDoS) 攻撃に対する保護を提供し、一般的なウェブ悪用攻撃からウェブアプリケーションを保護するAWS WAFのに役立ちます。

次の表は、このガイドで説明されているネットワークとアプリケーションの保護サービスをまとめたものです。

AWS Firewall Manager

AWS Firewall Manager は、保護のために複数のアカウントとリソースにわたる管理およびメンテナンスタスクを簡素化します。

AWS Network Firewall

AWS Network Firewall は、VPC でステートフルでマネージド型のネットワークファイアウォールと侵入検知および防止サービスを提供します。

AWS Shield

AWS Shield は、ネットワーク、トランスポート、アプリケーションレイヤーの AWS リソースに対する DDoS 攻撃に対する保護を提供します。

AWS WAF

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(S) リクエストをモニタリングできるように、ウェブアプリケーションファイアウォールを提供します。

AWS 検出および対応サービスを理解する

AWS には、マルチアカウント環境を含む環境全体のセキュリティオペレーションを AWS 合理化するのに役立つツールが用意されています。例えば、インテリジェントな脅威検出に Amazon GuardDuty を使用し、Amazon Detective を使用してログデータを収集することでセキュリティの検出結果を特定および分析できます。 は複数のセキュリティ標準AWS Security Hub CSPMをサポートし、セキュリティアラートとコンプライアンスステータスの概要を提供します AWS アカウント。 は、セキュリティイベントを理解して対応するために不可欠なユーザーアクティビティとアプリケーションプログラミングインターフェイス (API) の使用状況AWS CloudTrailを追跡します。

次の表は、このガイドで説明されている検出とレスポンスのサービスをまとめたものです。

AWS Config

AWS Config は、 内の AWS リソースの設定の詳細ビューを提供します AWS アカウント。

AWS CloudTrail

AWS CloudTrail は、ユーザー、ロール、または によって実行されたアクションを記録します AWS のサービス。

AWS Security Hub CSPM

AWS Security Hub CSPM は、 のセキュリティ状態の包括的なビューを提供します AWS。

Amazon GuardDuty

Amazon GuardDuty は AWS アカウント、悪意のあるアクティビティがないか、ワークロード、ランタイムアクティビティ、データを継続的にモニタリングします。

Amazon Inspector

Amazon Inspector は、ソフトウェアの脆弱性や意図しないネットワークへの露出がないか AWS ワークロードをスキャンします。

Amazon Security Lake

Amazon Security Lake は、 AWS 環境、SaaS プロバイダー、オンプレミス環境、クラウドソース、サードパーティーソースのセキュリティデータをデータレイクに自動的に一元化します。

Amazon Detective

Amazon Detective を使用すると、セキュリティに関する検出結果や疑わしいアクティビティの根本原因を分析、調査、および迅速に特定できます。

AWS Security Incident Response

AWS セキュリティインシデント対応

セキュリティインシデントからの復旧に役立つガイダンスを迅速に準備、対応、受け取るのに役立ちます。

AWS ガバナンスおよびコンプライアンスサービスを理解する

AWS には、セキュリティ、運用、コンプライアンス、コスト標準の遵守に役立つツールが用意されています。たとえば、 AWS Control Towerを使用して、規範的なコントロールを使用してマルチアカウント環境を設定および管理できます。を使用するとAWS Organizations、組織内の複数のアカウントにポリシーベースの管理を設定できます。

AWS は、コンプライアンスステータスを包括的に把握し、組織が従う AWS ベストプラクティスと業界標準に基づいて自動化されたコンプライアンスチェックを使用して環境を継続的にモニタリングすることもできます。例えば、 AWS Artifactはコンプライアンスレポートへのオンデマンドアクセスを提供し、証拠収集AWS Audit Managerを自動化して、コントロールが効果的に動作しているかどうかをより簡単に評価できるようにします。

次の表は、このガイドで説明されているガバナンスとコンプライアンスのサービスをまとめたものです。

AWS Organizations

AWS Organizations は、作成して一元管理する AWS アカウント 組織に複数の を統合するのに役立ちます。

AWS Control Tower

AWS Control Tower は、ベストプラクティスに基づく 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。

AWS Artifact

AWS Artifact は、 AWS 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します。

AWS Audit Manager

AWS Audit Manager

AWS 使用状況を継続的に監査し、リスクとコンプライアンスの評価方法を簡素化するのに役立ちます。

AWS セキュリティ、アイデンティティ、ガバナンスの基準を検討する

で適切なセキュリティ、アイデンティティ、ガバナンスサービスを選択するかどうか AWS は、特定の要件とユースケースによって異なります。AWS セキュリティサービスの導入を決定すると、セキュリティ、アイデンティティ、ガバナンス AWS のサービス の採用が組織に適しているかどうかを判断するのに役立つ決定木が提供されます。さらに、使用するサービスを決定する際に考慮すべき基準をいくつか示します。

Security requirements and threat landscape

組織固有の脆弱性と脅威を包括的に評価します。これには、個人情報、財務記録、専有ビジネスデータなど、処理するデータの種類を特定することが含まれます。それぞれに関連する潜在的なリスクを理解します。

アプリケーションとインフラストラクチャのアーキテクチャを評価します。アプリケーションが公開されているかどうか、およびそれらが処理するウェブトラフィックの種類を決定します。これは、ウェブの悪用から保護 AWS WAF するための などのサービスの必要性に影響します。内部アプリケーションの場合、異常なアクセスパターンや不正なデプロイを特定できる Amazon GuardDuty による内部脅威検出と継続的なモニタリングの重要性を考慮してください。

最後に、既存のセキュリティ体制の洗練とセキュリティチームの専門知識を検討してください。チームのリソースが限られている場合、より多くの自動化と統合を提供するサービスを選択すると、チームを圧倒することなく、効果的なセキュリティ強化を実現できます。サービスの例としては、DDoS 保護 AWS Shield や集中型セキュリティモニタリング AWS Security Hub CSPM などがあります。

Compliance and regulatory requirements

一般データ保護規則 (GDPR)、1996 年の米国の医療保険の相互運用性と説明責任に関する法律 (HIPAA)、Payment Card Industry Data Security Standard (PCI DSS) など、業界または地域に関連する法律と基準を特定します。

AWS は、さまざまな標準への準拠を管理するのに役立つ AWS Config や AWS Artifact などのサービスを提供します。を使用すると AWS Config、 AWS リソースの設定を評価、監査、評価できるため、内部ポリシーと規制要件への準拠が容易になります。 AWS Artifact は AWS コンプライアンスドキュメントへのオンデマンドアクセスを提供し、監査とコンプライアンスレポートに役立ちます。

特定のコンプライアンスニーズに合ったサービスを選択すると、組織が法的要件を満たし、データに対して安全で信頼できる環境を構築するのに役立ちます。詳細についてはAWS 、コンプライアンスプログラムを参照してください。

Scalability and flexibility

組織の成長とスピードを考慮してください。セキュリティ対策 AWS のサービス がインフラストラクチャとシームレスに成長し、進化する脅威に適応するのに役立つ を選択します。

迅速なスケーリングをサポートするために、 は、 AWS Organizations や IAM Identity Center などAWS のサービス、他のいくつかの の機能 AWS Control Tower を調整して、1 AWS 時間以内にランディングゾーンを構築します。Control Tower は、ユーザーに代わってリソースを設定および管理します。

AWS は、脅威の検出やウェブアプリケーションの保護のために Amazon GuardDuty など、アプリケーションのトラフィックと使用パターンに合わせて自動的にスケーリング AWS WAF する多くの サービスを設計します。ビジネスがスケールアップすると、これらのサービスは、手動による調整やボトルネックを発生させることなく、それに合わせてスケールされます。

さらに、ビジネス要件や脅威の状況に合わせてセキュリティコントロールをカスタマイズできることが重要です。複数のアカウントで 40 以上のサービスのリソースを管理できるように AWS Organizations、 を使用してアカウントを管理することを検討してください。これにより、個々のアプリケーションチームはワークロード固有のセキュリティニーズを管理する柔軟性と可視性を得ると同時に、一元化されたセキュリティチームにガバナンスと可視性を提供します。

スケーラビリティと柔軟性を考慮すると、セキュリティ体制が堅牢で応答性が高く、動的なビジネス環境をサポートできるようになります。

Integration with existing systems

現在のオペレーションを中断するのではなく強化するセキュリティ対策を検討してください。例えば、次のことを考えてみます。

- からセキュリティデータとアラートを集約 AWS のサービス し、既存のセキュリティ情報イベント管理 (SIEM) システムとともに分析することで、ワークフローを合理化します。
- AWS とオンプレミス環境の両方で、セキュリティの脅威と脆弱性の統合ビューを作成します。
- を既存のログ管理ソリューション AWS CloudTrail と統合して、 AWS インフラストラクチャと既存のアプリケーション全体のユーザーアクティビティと API 使用状況を包括的にモニタリングします。
- リソース使用率を最適化し、環境全体にセキュリティポリシーを一貫して適用する方法を検討します。これにより、セキュリティカバレッジのギャップのリスクを軽減できます。

Cost and budget considerations

検討している各サービスの料金モデルを確認します。API コールの数、処理されるデータ量、保存されるデータ量など、使用量に基づいて料金が発生する AWS ことがよくあります。例えば、Amazon GuardDuty は脅威検出のために分析されたログデータの量に基づいて課金しますが AWS WAF 、請求はデプロイされたルールの数と受信したウェブリクエストの数に基づいています。

予想される使用量を見積もり、コストを正確に予測します。現在のニーズと潜在的な需要の増加または急増の両方を考慮してください。例えば、スケーラビリティは の主要な機能ですが AWS のサービス、慎重に管理しないとコストが増加する可能性もあります。を使用してさまざまなシナリオAWS 料金見積りツールをモデル化し、その財務上の影響を評価します。

管理とメンテナンスに必要な時間とリソースなど、直接コストと間接コストの両方を含む総所有コスト (TCO) を評価します。マネージドサービスを選択すると、運用上のオーバーヘッドを減らすことができますが、料金が高くなる可能性があります。

最後に、リスク評価に基づいてセキュリティ投資を優先します。すべてのセキュリティサービスがインフラストラクチャにとって等しく重要なわけではないため、リスクを軽減し、コンプライアンスを確保する上で最も大きな影響を与える分野に予算を集中させます。セキュリティ AWS 戦略を成功させるには、費用対効果と必要なセキュリティレベルのバランスを取ることが重要です。

Organizational structure and access needs

組織の構造と運用、およびアクセスニーズがチーム、プロジェクト、または場所によってどのように異なるかを評価します。これは、ユーザー ID の管理と認証、ロールの割り当て、環境全体のアクセスコントロールの適用方法に影響します AWS 。最小特権のアクセス許可の適用や多要素認証 (MFA) の要求などのベストプラクティスを実装します。

ほとんどの組織には、マルチアカウント環境が必要です。このタイプの環境のベストプラクティスを確認し、実装に役立つ AWS Control Tower AWS Organizations と の使用を検討してください。

もう 1 つの側面は、認証情報とアクセスキーの管理です。IAM Identity Center を使用して、複数の AWS アカウント およびビジネスアプリケーション間でアクセス管理を一元化することを検討してください。これにより、セキュリティとユーザーの利便性の両方が向上します。組織のアカウント間のアクセスをスムーズに管理できるように、IAM Identity Center は と統合されています AWS Organizations。

さらに、これらの ID およびアクセス管理サービスが既存のディレクトリサービスとどのように統合されるかを評価します。既存の ID プロバイダーがある場合は、SAML 2.0 または OpenID Connect (OIDC) を使用して、IAM アイデンティティセンターと統合できます。IAM Identity Center では、ディレクトリの同期を維持するために、クロスドメイン ID 管理 (SCIM) プロビジョニングもサポートされています。これにより、 AWS リソースへのアクセス中にシームレスで安全なユーザーエクスペリエンスを確保できます。

AWS セキュリティ、アイデンティティ、ガバナンスサービスを選択する

セキュリティオプションを評価する基準がわかったので、組織の要件に適した AWS セキュリティサービスを選択する準備が整いました。

次の表は、どのサービスがどの状況に最適化されているかを示しています。テーブルを使用して、組織やユースケースに最適なサービスを判断します。

Note

[1] との統合 AWS Security Hub CSPM (完全なリスト)

[2] Amazon GuardDuty との統合 (完全なリスト)

[3] Amazon Security Lake との統合 (完全なリスト)

AWS ID とアクセス管理サービスを選択する

適切な個人に、システム、アプリケーション、データへの適切なレベルのアクセスを付与します。

いつ使用すべきですか?	何に最適化されていますか?	セキュリティ、アイデンティティ、ガバナンスサービス
これらのサービスを使用すると、顧客、ワークフォース、ワークロードのアクセスを安全に管理できます。	ID のソースを接続するか、ユーザーを作成するのに役立ちます。複数の AWS アカウントやアプリケーションへのワークフォースアクセスを一元管理できます。	AWS IAM Identity Center
	ウェブおよびモバイルアプリケーションのユーザーを認証および認可するために最適化されています。	Amazon Cognito
	内でリソースを安全に共有するために最適化されています AWS。	AWS RAM
	AWS ワークロードリソースへのアクセスを安全かつきめ細かく制御できます。	IAM [1]

AWS データ保護サービスを選択する

キー管理や機密データ検出から認証情報管理まで、データ保護とセキュリティのタスクを自動化および簡素化します。

いつ使用すべきですか?	何に最適化されていますか?	データ保護サービス
これらのサービスを使用して、 AWS 環境内で保存および処理される機密データの機密性、完全性、可用性を達成および維持できます。	機密データを検出するために最適化されています。	Amazon Macie [1]
	暗号化キー用に最適化されています。	AWS KMS
	HSMs。	AWS CloudHSM
	プライベート SSL/TLS X.509 証明書とキー用に最適化されています。	AWS Certificate Manager
	プライベート認証機関の階層を作成するために最適化されました。	AWS Private CA
	データベース認証情報、アプリケーション認証情報、OAuth トークン、API キー、およびその他のシークレット用に最適化されています。	AWS Secrets Manager
	PCI 標準に従って支払い処理に使用される暗号化関数とキー管理へのアクセスを提供するように最適化されています。	AWS Payment Cryptography

AWS ネットワークおよびアプリケーション保護サービスを選択する

インターネットリソースを一般的な DDoS 攻撃やアプリケーション攻撃から一元的に保護します。

いつ使用すべきですか?	何に最適化されていますか?	ネットワークおよびアプリケーション保護サービス
これらのサービスを使用すると、すべてのネットワークコントロールポイントで詳細なセキュリティポリシーを適用できます。	ファイアウォールルールを一元的に設定および管理するために最適化されています。	AWS Firewall Manager [1]
	ステートフルでマネージド型のネットワークファイアウォールと侵入検知および防止サービスを提供するために最適化されています。	AWS Network Firewall
	ネットワーク、トランスポート、アプリケーションレイヤーの AWS リソースに対する DDoS 攻撃から保護するために最適化されています。	AWS Shield
	ウェブアプリケーションファイアウォールを提供するために最適化されています。	AWS WAF

AWS 検出およびレスポンスサービスを選択する

セキュリティのベストプラクティスを早期に統合しながら、セキュリティリスクを継続的に特定して優先順位を付けます。

いつ使用すべきですか?	何に最適化されていますか?	検出および対応サービス
これらのサービスを使用すると、アカウント全体のセキュリティリスクを検出して対応できるため、ワークロードを大規模に保護できます。	セキュリティチェックを自動化し、 AWS およびサードパーティーの統合でセキュリティアラートを一元化するために最適化されています。	AWS Security Hub CSPM [2、3]

いつ使用すべきですか?	何に最適化されていますか?	検出および対応サービス
	リソースの設定を評価、監査、評価するために最適化されています。	AWS Config [1]
	他の からのイベントを監査証跡 AWS のサービス として口グ記録するために最適化されています。	AWS CloudTrail
	インテリジェントな脅威検出と詳細なレポート用に最適化されています。	Amazon GuardDuty [1]
	脆弱性管理用に最適化されています。	Amazon Inspector [1]
	セキュリティデータを一元化するために最適化されています。	Amazon Security Lake [1]
	潜在的なセキュリティ問題の集約と要約に最適化されています。	Amazon Detective [1、2、3]
	検出結果の優先順位付け、セキュリティイベントのエスカレーション、即時対応が必要なケースの管理に役立つように最適化されています。	AWS セキュリティインシデント対応

AWS ガバナンスおよびコンプライアンスサービスを選択する

リソース全体でクラウドガバナンスを確立し、コンプライアンスと監査プロセスを自動化します。

いつ使用すべきですか?	何に最適化されていますか?	ガバナンスおよびコンプライアンスサービス
これらのサービスを使用して、ベストプラクティスを実装し、使用時に業界標準を満たすことができます AWS。	複数のアカウントと一括請求を一元管理するために最適化されています。	AWS Organizations
	AWS セキュリティおよびコンプライアンスドキュメントをオンデマンドでダウンロードできるように最適化されています。	AWS Artifact
	AWS 使用状況の監査用に最適化されています。	AWS Audit Manager [1]
	AWS マルチアカウント環境のセットアップと管理に最適化されています。	AWS Control Tower

AWS セキュリティ、アイデンティティ、ガバナンスサービスを使用する

これで、各 AWS セキュリティ、アイデンティティ、ガバナンスサービス (およびサポート AWS ツールとサービス) の動作と、どちらが適切かを明確に理解できたはずです。

を使用して、利用可能な各 AWS セキュリティ、アイデンティティ、ガバナンスサービスの詳細について調べる方法を検討するために、各サービスの仕組みを調べるための経路を用意しました。以下のセクションでは、詳細なドキュメント、実践的なチュートリアル、開始するためのリソースへのリンクを提供します。

AWS ID とアクセス管理サービスを使用する

次の表は、使用開始に役立つ ID とアクセス管理リソースをサービス別にまとめたものです。

AWS IAM Identity Center

- IAM アイデンティティセンター AWS の有効化

  IAM Identity Center を有効にし、 で使用を開始します AWS Organizations。

  ガイドを見る
- デフォルトの IAM Identity Center ディレクトリを使用してユーザーアクセスを設定する

  デフォルトのディレクトリを ID ソースとして使用し、ユーザーアクセスをセットアップしてテストします。

  チュートリアルの開始方法
- Active Directory を ID ソースとして使用する

  Active Directory を IAM アイデンティティセンターの ID ソースとして使用するための基本的なセットアップを完了します。

  チュートリアルの開始方法
- Okta と IAM アイデンティティセンターで SAML と SCIM を設定する

  Okta および IAM Identity Center との SAML 接続を設定します。

  チュートリアルの開始方法

Amazon Cognito

- Amazon Cognito の開始方法

  最も一般的な Amazon Cognito タスクについて説明します。

  ガイドを見る
- チュートリアル: ユーザープールの作成

  ユーザープールを作成します。これにより、ユーザーはウェブまたはモバイルアプリにサインインできます。

  チュートリアルの開始方法
- チュートリアル: ID プールの作成

ID プールを作成します。これにより、ユーザーは一時的な AWS 認証情報を取得してアクセスできます AWS のサービス。

チュートリアルの開始方法

- Amazon Cognito ワークショップ

  Amazon Cognito を使用して、架空のペットストアの認証ソリューションを構築する練習をします。

  チュートリアルの開始方法

AWS RAM

- の開始方法 AWS RAM

  AWS RAM 用語と概念について説明します。

  ガイドを見る
- 共有 AWS リソースの使用

  所有している AWS リソースを共有し、共有されている AWS リソースにアクセスします。

  ガイドを見る
- RAM AWS でのアクセス許可の管理

  管理アクセス許可とカスタマー管理アクセス許可の 2 種類の AWS 管理アクセス許可について説明します。

  ガイドを見る
- RAM AWS を使用して共有されるリソースへの詳細なアクセスを設定する

  カスタマー管理アクセス許可を使用してリソースアクセスをカスタマイズし、最小特権のベストプラクティスを達成します。

  ブログを読む

IAM

- IAM の開始方法

を使用して IAM ロール、ユーザー、ポリシーを作成します AWS マネジメントコンソール。

チュートリアルの開始方法

- ロール AWS アカウント を使用して 間でアクセスを委任する

  ロールを使用して、ProductionandDevelopment という、所有している異なる AWS アカウントのリソースへのアクセスを委任します。

  チュートリアルの開始方法

- カスタマー管理ポリシーを作成する

  AWS マネジメントコンソール を使用してカスタマー管理ポリシーを作成し、そのポリシーをの IAM ユーザーにアタッチします AWS アカウント。

  チュートリアルの開始方法

- 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

  プリンシパルタグを持つ IAM ロールが一致するタグを持つリソースにアクセスできるようにするポリシーを作成してテストします。

  チュートリアルの開始方法

- IAM でのセキュリティのベストプラクティス

  IAM のベストプラクティスを使用して、 AWS リソースを保護するのに役立ちます。

  ガイドを見る

AWS データ保護サービスを使用する

次のセクションでは、データ保護について説明する AWS 詳細なリソースへのリンクを提供します。

Macie

- Amazon Macie の開始方法

  で Macie を有効にし AWS アカウント、Amazon S3 セキュリティ体制を評価し、S3 バケット内の機密データを検出してレポートするためのキー設定とリソースを設定します。

  ガイドを見る

- Amazon Macie によるデータセキュリティとプライバシーのモニタリング

  Amazon Macie を使用して Amazon S3 データセキュリティをモニタリングし、セキュリティ体制を評価します。

  ガイドを見る

- Amazon Macie の検出結果の分析

  Amazon Macie の検出結果を確認、分析、管理します。

  ガイドを見る

- Amazon Macie の検出結果を使用した機密データサンプルの取得

  Amazon Macie を使用して、個々の検出結果によって報告された機密データのサンプルを取得して公開します。

  ガイドを見る

- Amazon Macie による機密データの検出

  Amazon S3 データ資産内の機密データの検出、ログ記録、レポートを自動化します。

  ガイドを見る

AWS KMS

- の開始方法 AWS KMS

  作成から削除まで、対称暗号化 KMS キーを管理します。

  ガイドを見る

- 専用キー

  対称暗号化 KMS キーに加えて、 が AWS KMS サポートするさまざまなタイプのキーについて説明します。

  ガイドを見る

- を使用した保管時の暗号化機能のスケーリング AWS KMS

  内で利用可能な保管時の暗号化オプションについて説明します AWS。

ワークショップの詳細

AWS CloudHSM

- の開始方法 AWS CloudHSM

  AWS CloudHSM クラスターを作成、初期化、アクティブ化します。

  ガイドを見る
- AWS CloudHSM クラスターの管理

  AWS CloudHSM クラスターと、クラスターの管理におけるさまざまな管理タスクに接続します。

  ガイドを見る
- での HSM ユーザーとキーの管理 AWS CloudHSM

  クラスター内の HSMs にユーザーとキーを作成します。

  ガイドを見る
- CloudHSM で Amazon ECS と TLS オフロードを使用して NGINX ウェブサービスのデプロイを自動化する

  を使用して AWS CloudHSM 、クラウドでホストされているウェブサイトのプライベートキーを保存します。

  ブログを読む

AWS Certificate Manager

- パブリック証明書のリクエスト

  AWS Certificate Manager (ACM) コンソールまたは AWS CLI を使用して、パブリック ACM 証明書をリクエストします。

  ガイドを見る
- のベストプラクティス AWS Certificate Manager

  現在の ACM 顧客の実際の経験に基づくベストプラクティスについて説明します。

ガイドを見る

- AWS Certificate Manager を使用して証明書発行コントロールを適用する方法

  IAM 条件キーを使用して、ユーザーが組織のガイドラインに従って TLS 証明書を発行またはリクエストしていることを確認します。

  ブログを読む

AWS Private CA

- AWS Private CA デプロイの計画

  プライベート認証機関を作成する前に、使用 AWS Private CA の準備をします。

  ガイドを見る
- AWS Private CA 管理

  組織による内部使用のために、ルート認証機関と下位認証機関の完全 AWS ホスト階層を作成します。

  ガイドを見る
- 証明書の管理

  プライベート証明書の発行 AWS Private CA、取得、一覧表示など、 を使用して基本的な証明書管理タスクを実行します。

  ガイドを見る
- AWS Private CA ワークショップ

  プライベート認証機関のさまざまなユースケースに関する実践的な経験を開発します。

  ワークショップの詳細
- を使用して Active Directory での証明書のプロビジョニングを簡素化する方法 AWS Private CA

  を使用して AWS Private CA 、Microsoft Active Directory 環境内のユーザーとマシンの証明書をより簡単にプロビジョニングできます。

  ブログを読む
- で DNS 名制約を適用する方法 AWS Private CA

AWS Private CA サービスを使用して、DNS 名の制約を下位 CA に適用します。

ブログを読む

AWS Secrets Manager

- AWS Secrets Manager の概念

  プライベート証明書の発行 AWS Private CA、取得、一覧表示など、 を使用して基本的な証明書管理タスクを実行します。

  ガイドを見る
- の交代ユーザーローテーションを設定する AWS Secrets Manager

  データベース認証情報を含むシークレットの交代ユーザーローテーションを設定します。

  ガイドを見る
- Kubernetes での AWS Secrets Manager シークレットの使用

  Secrets and Configuration Provider (ASCP) を使用して、Secrets Manager からの AWS シークレットを Amazon EKS ポッドにマウントされたファイルとして表示します。

  ガイドを詳しく見る

AWS Payment Cryptography

- の開始方法 AWS Payment Cryptography

  キーを作成し、さまざまな暗号化オペレーションで使用します。

  ガイドを見る
- AWS Payment Cryptography よくある質問

  の基本を理解します AWS Payment Cryptography。

  FAQsを確認する

AWS ネットワークおよびアプリケーション保護サービスを使用する

次の表は、 AWS ネットワークとアプリケーションの保護を説明する詳細なリソースへのリンクを示しています。

AWS Firewall Manager

- AWS Firewall Manager ポリシーの開始方法

  を使用して AWS Firewall Manager 、さまざまなタイプのセキュリティポリシーをアクティブ化します。

  ガイドを見る
- を使用してセキュリティグループを継続的に監査および制限する方法 AWS Firewall Manager

  を使用してセキュリティグループを制限 AWS Firewall Manager し、必要なポートのみが開かれるようにします。

  ブログを読む
- を使用して保護 AWS Firewall Manager を大規模にデプロイする AWS Organizations

  を使用して AWS Firewall Manager 、 全体にセキュリティポリシーをデプロイおよび管理します AWS Organizations。

  ブログを読む

AWS Network Firewall

- の開始方法 AWS Network Firewall

  基本的なインターネットゲートウェイアーキテクチャで VPC の AWS Network Firewall ファイアウォールを設定して実装します。

  ガイドを見る
- AWS Network Firewall ワークショップ

  Infrastructure as Code を使用して AWS Network Firewall をデプロイします。

  ワークショップの詳細
- AWS Network Firewall 柔軟なルールエンジンの実践的なチュートリアル – パート 1

ルールエンジンを操作する AWS アカウント には、 AWS Network Firewall 内に のデモをデプロイします。

ブログを読む

- AWS Network Firewall 柔軟なルールエンジンの実践的なチュートリアル – パート 2

  厳格なルール順序でファイアウォールポリシーを作成し、1 つ以上のデフォルトアクションを設定します。

  ブログを読む

- のデプロイモデル AWS Network Firewall

  トラフィックパスに追加 AWS Network Firewall できる一般的なユースケースのデプロイモデルについて説明します。

  ブログを読む

- VPC ルーティングが強化された AWS Network Firewall のデプロイモデル

  拡張 VPC ルーティングプリミティブを使用して、同じ VPC の異なるサブネット内のワークロード AWS Network Firewall 間に挿入します。

  ブログを読む

AWS Shield

- の AWS Shield 仕組み

  ネットワークレイヤー AWS Shield Standard とトランスポートレイヤー (レイヤー 3 と 4) およびアプリケーションレイヤー (レイヤー 7) の AWS リソースに対する DDoS 攻撃に対する保護 AWS Shield Advanced を が提供する方法について説明します。

  ガイドを見る

- の開始方法 AWS Shield Advanced

  Shield Advanced コンソール AWS Shield Advanced を使用して の使用を開始します。

  ガイドを見る

- AWS Shield Advanced ワークショップ

インターネットに公開されているリソースを DDoS 攻撃から保護し、インフラストラクチャに対する DDoS 攻撃をモニタリングして、適切なチームに通知します。

ワークショップの詳細

AWS WAF

- の開始方法 AWS WAF

  ウェブ ACL を設定 AWS WAF、作成し、ウェブリクエストをフィルタリングするルールとルールグループを追加して Amazon CloudFront を保護します。

  チュートリアルの開始方法
- Amazon CloudWatch AWS WAF Logs でのログの分析

  Amazon CloudWatch logs へのネイティブ AWS WAF ログ記録を設定し、ログ内のデータを視覚化および分析します。

  ブログを読む
- Amazon CloudWatch ダッシュボードを使用して AWS WAF ログを視覚化する

  Amazon CloudWatch を使用して、CloudWatch メトリクス、Contributor Insights、および Logs Insights を使用して AWS WAF アクティビティをモニタリングおよび分析します。

  ブログを読む

AWS 検出およびレスポンスサービスを使用する

次の表は、 AWS 検出およびレスポンスサービスを説明する詳細なリソースへのリンクを示しています。

AWS Config

- の開始方法 AWS Config

  SDK をセットアップ AWS Config して操作します。 AWS SDKs

  ガイドを見る
- リスクとコンプライアンスワークショップ

AWS Config と AWS マネージド Config ルールを使用してコントロールを自動化します。

ワークショップの詳細

- AWS Config Rule Development Kit ライブラリ: 大規模なルールの構築と運用

  Rule Development Kit (RDK) を使用してカスタム AWS Config ルールを構築し、RDKLib でデプロイします。

  ブログを読む

AWS CloudTrail

- イベント履歴の表示

  CloudTrail をサポートするサービス AWS アカウント については、 の AWS API アクティビティを確認してください。

  チュートリアルの開始方法
- 管理イベントをログに記録する証跡を作成する

  証跡を作成して、すべてのリージョンの管理イベントを記録します。

  チュートリアルの開始方法

AWS Security Hub CSPM

- 有効化 AWS Security Hub CSPM

  スタンドアロンアカウントで AWS Security Hub CSPM AWS Organizations または で を有効にします。

  ガイドを見る
- クロスリージョン集約

  AWS Security Hub CSPM 結果を複数の から単一の集約リージョン AWS リージョン に集約します。

  ガイドを見る
- AWS Security Hub CSPM ワークショップ

AWS Security Hub CSPM と を使用して AWS 環境のセキュリティ体制を管理および改善する方法について説明します。

ワークショップの詳細

- 3 つの定期的な Security Hub の使用パターンとそのデプロイ方法

  最も一般的な 3 つの AWS Security Hub CSPM 使用パターンと、検出結果を特定して管理するための戦略を改善する方法について説明します。

  ブログを読む

Amazon GuardDuty

- Amazon GuardDuty の開始方法

  Amazon GuardDuty を有効にし、検出結果のサンプルを生成して、アラートを設定します。

  チュートリアルを見る

- Amazon GuardDuty での EKS 保護

  Amazon GuardDuty を使用して、Amazon Elastic Kubernetes Service (Amazon EKS) 監査ログをモニタリングします。

  ガイドを見る

- Amazon GuardDuty での Lambda 保護

  AWS Lambda 関数を呼び出すときに潜在的なセキュリティ脅威を特定します。

  ガイドを見る

- GuardDuty Amazon RDS 保護

  Amazon GuardDuty を使用して、Amazon Aurora データベースへの潜在的なアクセス脅威について、Amazon Relational Database Service (Amazon RDS) ログインアクティビティを分析し、プロファイリングします。

  ガイドを見る

- Amazon GuardDuty での Amazon S3 Amazon GuardDuty 保護

GuardDuty を使用して CloudTrail データイベントをモニタリングし、S3 バケット内の潜在的なセキュリティリスクを特定します。

ガイドを見る

- Amazon GuardDuty と Amazon Detective による脅威の検出と対応

  Amazon GuardDuty と Amazon Detective の基本について説明します。

  ワークショップの詳細

Amazon Inspector

- Amazon Inspector の開始方法

  Amazon Inspector スキャンをアクティブ化して、コンソールでの検出結果を理解します。

  チュートリアルの開始方法

- Amazon Inspector による脆弱性管理

  Amazon Inspector を使用して、Amazon Elastic Container Registry (Amazon ECR) の Amazon EC2 インスタンスとコンテナイメージをスキャンしてソフトウェアの脆弱性を確認します。

  ワークショップの詳細

- Amazon Inspector を使用して EC2 AMIsスキャンする方法

  複数の を使用して AMIs AWS のサービス をスキャンし、既知の脆弱性がないかソリューションを構築します。

  ブログを読む

Amazon Security Lake

- Amazon Security Lake の開始方法

  Amazon Security Lake を有効にして使用を開始します。

  ガイドを見る

- を使用した複数のアカウントの管理 AWS Organizations

複数の からセキュリティログとイベントを収集します AWS アカウント。

ガイドを見る

- Amazon Security Lake によって発行されたイベントを Amazon OpenSearch Service に取り込み、変換し、配信する

  Amazon Security Lake データを取り込み、変換して Amazon OpenSearch Service に配信し、SecOps チームで使用します。

  ブログを読む

- How to visualize Amazon Security Lake findings with Quick Suite

  Amazon Athenaand Quick Suite を使用して、Amazon Security Lake からデータをクエリおよび視覚化します。

  ブログを読む

Amazon Detective

- Amazon Detective の用語と概念

  Amazon Detective とその仕組みを理解する上で重要な用語と概念について説明します。

  ガイドを見る

- Amazon Detective のセットアップ

  Amazon Detective コンソール、Amazon Detective API、または から Amazon Detective を有効にします AWS CLI。

  ガイドを見る

- Amazon GuardDuty と Amazon Detective による脅威の検出と対応

  Amazon GuardDuty と Amazon Detective の基本について説明します。

  ワークショップの詳細

AWS ガバナンスおよびコンプライアンスサービスを使用する

次の表に、ガバナンスとコンプライアンスを説明する詳細なリソースへのリンクを示します。

AWS Organizations

- 組織の作成と設定

  組織を作成し、2 つの AWS メンバーアカウントで設定します。

  チュートリアルの開始方法
- と連携するサービス AWS Organizations

  で使用できる AWS Organizations と、組織全体レベルで各サービスを使用する利点を理解 AWS のサービス します。

  ガイドを見る
- 複数のアカウントを使用して AWS 環境を整理する

  AWS 環境全体を整理するためのベストプラクティスと現在の推奨事項を実装します。

  ホワイトペーパーを読む

AWS Artifact

- の開始方法 AWS Artifact

  セキュリティおよびコンプライアンスレポートのダウンロード、法的契約の管理、通知の管理を行います。

  ガイドを見る
- での契約の管理 AWS Artifact

  を使用して、アカウントまたは組織の契約 AWS マネジメントコンソール を確認、受諾、管理します。

  ガイドを見る
- AWS パート 1 の監査の準備 – AWS 監査マネージャー AWS Config、 AWS およびアーティファクト

AWS のサービス を使用して、監査で使用される証拠の収集を自動化できます。

ブログを読む

AWS Audit Manager

- AWS Audit Manager の有効化

  AWS マネジメントコンソール、Audit Manager API、または を使用して Audit Manager を有効にします AWS CLI。

  ガイドを見る
- 監査所有者向けチュートリアル: 評価の作成

  Audit Manager サンプルフレームワークを使用して評価を作成します。

  ガイドを見る
- 受任者向けチュートリアル: コントロールセットの確認

  Audit Manager の監査所有者によって共有されたコントロールセットを確認します。

  ガイドを見る

AWS Control Tower

- の開始方法 AWS Control Tower

  ランディングゾーンと呼ばれるマルチアカウント環境をセットアップして起動し、規範的なベストプラクティスに従います。

  ガイドを見る
- Amazon Bedrock と を使用したアカウント管理のモダナイズ AWS Control Tower

  セキュリティツールアカウントをプロビジョニングし、生成 AI を活用して AWS アカウントセットアップと管理プロセスを迅速化します。

  ブログを読む
- を使用して適切に設計された AWS GovCloud (米国) 環境を構築する AWS Control Tower

組織単位 (OUs) と を使用して AWS ワークロードを管理するなど、 AWS GovCloud (米国) リージョンでガバナンスを設定します AWS アカウント。

ブログを読む

AWS セキュリティ、アイデンティティ、ガバナンスのサービスを調べる

Editable architecture diagrams

リファレンスアーキテクチャ図

セキュリティ、アイデンティティ、ガバナンス戦略の開発に役立つリファレンスアーキテクチャ図をご覧ください。

セキュリティ、アイデンティティ、ガバナンスのリファレンスアーキテクチャを調べる

Ready-to-use code

注目のソリューション	AWS ソリューション
での Security Insights AWS Amazon Security Lake でデータを視覚化し、セキュリティイベントをより迅速に調査して対応できるように構築 AWSされたコードをデプロイします。 このソリューションの詳細	によって構築された、事前設定済みのデプロイ可能なソリューションとその実装ガイドについて説明します AWS。 すべての AWS セキュリティ、アイデンティティ、ガバナンスのソリューションを調べる

Documentation

セキュリティ、アイデンティティ、ガバナンスに関するホワイトペーパー	AWS セキュリティブログ
ホワイトペーパーでは、組織に最適なセキュリティ、アイデンティティ、ガバナンスサー	特定のセキュリティユースケースに対応するブログ記事をご覧ください。

ビスの選択、実装、使用に関する詳細なインサイトとベストプラクティスについて説明します。

セキュリティ、アイデンティティ、ガバナンスのホワイトペーパーを見る

AWS セキュリティブログを見る

ドキュメント履歴

次の表に、この決定ガイドの重要な変更点を示します。このガイドの更新に関する通知については、RSS フィードをサブスクライブできます。

変更	説明	日付
re:Invent 更新	AWS セキュリティインシデント対応 および に関する情報を追加しました AWS Payment Cryptography。 AWS Identity and Access Management および のサービス情報を更新しました AWS IAM Identity Center。	2024 年 12 月 30 日
動画の更新	re:Inforce 2024 からの最近の稲妻トークで入門ビデオを更新しました。	2024 年 6 月 25 日
ガバナンスサービスを追加	AWS CloudTrail、 AWS Control Tower、 の追加など、ガバナンスを含めるようにドキュメントの範囲を拡大しました AWS Organizations。新しいスコープを反映するようにグラフィックを更新しました。ID のベストプラクティスを明確にしました。全体を通した編集。	2024 年 6 月 7 日
初版発行	ガイドが最初に公開されました。	2024 年 3 月 21 日

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。