でのスケーラブルな脆弱性管理プログラムの構築 AWS

AWS 規範ガイダンス

AWS 規範ガイダンス: でのスケーラブルな脆弱性管理プログラムの構築 AWS

Table of Contents

でのスケーラブルな脆弱性管理プログラムの構築 AWS

Anna McAbee と Megan O'Neil、Amazon Web Services (AWS)

2023 年 10 月 (ドキュメント履歴)

使用している基盤となるテクノロジーに応じて、さまざまなツールやスキャンがクラウド環境でセキュリティ上の検出結果を生成できます。これらの検出結果を処理するプロセスがないと、検出結果が蓄積し始め、多くの場合、短期間で数千から数万件に達することもあります。ただし、構造化された脆弱性管理プログラムとツールの適切な運用により、組織はさまざまなソースからの多数の検出結果を処理およびトリアージできます。

脆弱性管理は、脆弱性の検出、優先順位付け、評価、修復、報告に重点を置いています。一方、パッチ管理は、セキュリティの脆弱性を削除または修正するためのソフトウェアのパッチ適用または更新に重点を置いています。パッチ管理は脆弱性管理の一側面にすぎません。一般的に、重要な即時パッチ適用が求められるシナリオに対応する patch-in-place プロセス (mitigate-in-place プロセスとも呼ばれます) と、パッチ適用済みの Amazon マシンイメージ (AMI)、コンテナ、またはソフトウェアパッケージをリリースするために定期的に実行する標準プロセスの両方を確立することをお勧めします。これらのプロセスは、組織がゼロデイ脆弱性に迅速に対応するための準備に役立ちます。本番環境の重要なシステムでは、patch-in-place プロセスを使用すると、フリート全体に新しい AMI をロールアウトするよりも高速で信頼性が高くなります。オペレーティングシステム (OS) やソフトウェアパッチなど、定期的にスケジュールされたパッチについては、ソフトウェアレベルの変更と同様に、標準の開発プロセスを使用してビルドおよびテストすることをお勧めします。これにより、標準的な運用モードでの安定性が向上します。パッチマネージャー、 の一機能 AWS Systems Manager、またはその他のサードパーティー製品をpatch-in-placeソリューションとして使用できます。Patch Manager の使用の詳細については、「AWS クラウド導入フレームワーク: オペレーションのパースペクティブ」の「パッチ管理」を参照してください。また、EC2 Image Builder を使用して、カスタマイズされた最新のサーバーイメージの作成、管理、デプロイを自動化できます。

でスケーラブルな脆弱性管理プログラムを構築するには、クラウド設定リスクに加えて、従来のソフトウェアとネットワークの脆弱性を管理する AWS 必要があります。暗号化されていない Amazon Simple Storage Service (Amazon S3) バケットなどのクラウド設定リスクは、ソフトウェアの脆弱性と同様のトリアージおよび修復プロセスに従う必要があります。どちらの場合も、アプリケーションチームが、基盤となるインフラストラクチャを含むアプリケーションのセキュリティを所有し、責任を負う必要があります。この所有権の分散は、効果的でスケーラブルな脆弱性管理プログラムにとって重要です。

このガイドでは、全体的なリスクを軽減するために、脆弱性の特定と修復を合理化する方法について説明します。以下のセクションを使用して、脆弱性管理プログラムを構築してイテレーションします。

1. 準備 — 環境の脆弱性を特定、評価、修正するための人材、プロセス、テクノロジーを準備します。
2. トリアージと修復 — セキュリティの検出結果を関連するステークホルダーにルーティングし、適切な修復アクションを特定して実行します。
3. 報告と改善 — 報告メカニズムを使用して改善の機会を特定し、脆弱性管理プログラムをイテレーションします。

クラウド脆弱性管理プログラムの構築には、多くの場合、イテレーションが伴います。このガイドの推奨事項に優先順位を付け、バックログを定期的に見直すことで、テクノロジーの変化とビジネス要件に常に対応できます。

対象者

このガイドは、セキュリティ関連の検出結果を担当する 3 つの主要チームを持つ大企業を対象としています。セキュリティチーム、Cloud Center of Excellence (CCoE) またはクラウドチーム、アプリケーション (または開発者) チームです。このガイドでは、最も一般的なエンタープライズ運用モデルを使用し、これらの運用モデルに基づいて構築することで、セキュリティの検出結果により効率的に対応し、セキュリティの結果を向上させます。を使用する組織 AWS では、構造や運用モデルが異なる場合がありますが、このガイドの概念の多くは、運用モデルや小規模な組織に合わせて変更できます。

目的

このガイドは、お客様や組織が以下のことを行うのに役立ちます。

- 脆弱性管理を効率化し、説明責任を確実にするためのポリシーを策定する
- セキュリティの責任をアプリケーションチームに分散するメカニズムを確立する
- スケーラブルな脆弱性管理のベストプラクティス AWS のサービス に従って関連する を設定する
- セキュリティ検出結果の所有権を分散する
- 脆弱性管理プログラムについて報告し、イテレーションするメカニズムを確立する
- セキュリティ検出結果の可視性を向上させ、全体的なセキュリティ体制を改善する

スケーラブルな脆弱性管理プログラムを準備する

スケーラブルな脆弱性管理プログラムの構築を準備するには、人々を教育し、プロセスを開発し、ベストプラクティスに従って適切なテクノロジーを実装する必要があります。人々、プロセス、テクノロジーは、効果的な脆弱性管理プログラムにとって等しく重要であり、それらを緊密に統合して大規模に脆弱性を管理する必要があります。

ガイドのこのセクションでは、 AWSでスケーラブルな脆弱性管理プログラムを準備するために実行できる基本的なアクションについて説明します。

トピック

脆弱性管理計画を定義する

クラウド脆弱性管理プログラムを準備する最初のステップは、脆弱性管理計画を定義することです。この計画には、組織が従うポリシーとプロセスが含まれます。この計画は文書化され、すべての利害関係者がアクセスできるようにしておく必要があります。脆弱性管理計画は、通常、以下のセクションを含む高レベルのドキュメントです。

- 目標と範囲 — 脆弱性管理の目標、機能、範囲を概説します。
- 役割と責任 — 脆弱性管理の利害関係者を一覧表示し、それぞれの責任について詳しく説明します。
- 脆弱性の重要度と優先順位付けの定義 — 脆弱性の重要度を分類する方法と、優先順位の付け方を決定します。
- 修復のためのサービスレベルアグリーメント (SLA) – 重要度レベルごとに、修復所有者がセキュリティ検出結果を解決するために必要な最大時間を定義します。SLA コンプライアンスは、効果的でスケーラブルな脆弱性管理プログラムに不可欠な要素であるため、これらの SLA が満たされているかどうかを追跡する方法を検討します。

- 例外プロセス – 例外の提出、承認、更新のプロセスについて詳しく説明します。このプロセスでは、例外が正当であり、期限が設定され、追跡されていることを確実にする必要があります。
- 脆弱性情報のソース – セキュリティ検出結果を生成するソースまたはツールを一覧表示します。セキュリティ検出結果のソースとなる AWS のサービス 可能性のある の詳細については、このガイドAWS セキュリティサービスを設定するの「」を参照してください。

これらのセクションは、さまざまな規模や業界の企業で共通していますが、各組織の脆弱性管理計画は異なります。組織に最適な脆弱性管理計画を構築する必要があります。計画は、学んだ教訓と進化するテクノロジーを反映させるために、時間の経過と共に繰り返し更新されることが想定されます。

セキュリティ所有権を分散する

責任AWS 共有モデルは、クラウドのセキュリティ AWS とコンプライアンスに対する責任を共有する方法とその顧客を定義します。このモデルでは、 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 AWS を保護し AWS クラウド、 AWS お客様はデータとアプリケーションを保護する責任があります。

このモデルを組織内にミラーリングし、クラウドチームとアプリケーションチームの間で責任を分散できます。これにより、アプリケーションチームがアプリケーションの特定のセキュリティ面を担当するため、クラウドセキュリティプログラムをより効果的にスケールできます。責任共有モデルの最もわかりやすい解釈は、リソースの設定権限を持つ者が、そのリソースのセキュリティに責任を持つということです。

セキュリティ責任をアプリケーションチームに分散する上で重要なのは、アプリケーションチームが自動化を行えるようにするセルフサービスのセキュリティツールを構築することです。初期段階では、これは共同で取り組むことができます。セキュリティチームは、セキュリティ要件をコードスキャンツールに変換し、アプリケーションチームはこれらのツールを使用してソリューションを構築し、社内の開発者コミュニティと共有できます。これにより、同様のセキュリティ要件を満たす必要がある他のチーム全体の効率が向上します。

次の表は、所有権をアプリケーションチームに分散する手順と例を示しています。

[ステップ]	[アクション]	例
1	セキュリティ要件を定義する – 何を達成しようとしていますか? これは、セキュリティ	セキュリティ要件の例としては、アプリケーション ID の最小特権アクセスがあります。

[ステップ]	[アクション]	例
	標準またはコンプライアンス要件に要件に基づいて定義される場合があります。	
2	セキュリティ要件のコントロールを列挙する – この要件は、コントロールの観点から実際に何を意味しますか? これを実現するにはどうすればよいですか?	アプリケーション ID の最小特権を実現するために、次の 2 つのコントロールが例として挙げられます。 • AWS Identity and Access Management (IAM) ロールを使用する • IAM ポリシーでワイルドカードを使用しない
3	コントロールに関するガイダンスを文書化する – これらのコントロールについて、開発者がコントロールに準拠できるようにどのようなガイダンスを提供できますか?	最初は、安全な IAM ポリシーと安全でない IAM ポリシー、Amazon Simple Storage Service (Amazon S3) バケットポリシーなど、シンプルなポリシーの例を文書化することから始めるとよいでしょう。次に、プロアクティブ評価にAWS Config ルールを使用するなど、継続的インテグレーションおよび継続的デリバリー (CI/CD) パイプライン内にポリシースキャンソリューションを埋め込むことができます。

[ステップ]	[アクション]	例
4	再利用可能なアーティファクトを開発する – ガイダンスに基づいて、開発者がより簡単に活用できるよう、再利用可能なアーティファクトを開発できますか?	最小特権の原則に従う IAM ポリシーをデプロイするために、Infrastructure as Code (IaC) を作成できます。これらの再利用可能なアーティファクトは、コードリポジトリに保存できます。

セルフサービスは、すべてのセキュリティ要件に対応できるとは限りませんが、標準的なシナリオには対応できます。これらのステップに従うことで、組織はアプリケーションチームが自らのセキュリティ責任のより多くをスケーラブルに担えるようにすることができます。全体として、責任分散モデルは、多くの組織内で、より協調的なセキュリティプラクティスの実現につながります。

脆弱性開示プログラムを開発する

多層防御アプローチで脆弱性管理を行うために、組織内外のユーザーがセキュリティの脆弱性やリスクを報告できるよう、脆弱性開示プログラムを作成します。

組織内のユーザーには、リスクや脆弱性を送信するプロセスを確立します。これは、チケットシステムまたは E メールで行うことができます。選択したプロセスにかかわらず、従業員がプロセスを認識し、発生した脆弱性やリスクを簡単に送信できることが重要です。

組織外のユーザーには、潜在的なセキュリティ脆弱性を送信するための外部ウェブページを確立します。例として、「AWS Vulnerability Reporting」ウェブページを参照してください。このウェブページには、組織のデータとアセットを保護するための開示ガイドラインも含める必要があります。脆弱性開示プログラムは、潜在的に有害なアクティビティを助長すべきではないため、ガイドラインを含む明確なポリシーを持つことが不可欠です。プログラムの成熟に伴い、成熟した責任ある開示プログラムを構築することを目指します。ほとんどの場合、外部開示プログラムから始めることはなく、正しく整備するには時間がかかります。

AWS 環境を準備する

脆弱性管理ツールを実装する前に、スケーラブルな脆弱性管理プログラムをサポートするように、AWS 環境が設計されていることを確認してください。 AWS アカウント と組織のタグ付けポリシーの構造により、スケーラブルな脆弱性管理プログラムを構築するプロセスを簡素化できます。

AWS アカウント 構造を開発する

AWS Organizations は、ビジネスの成長と AWS リソースのスケーリングに応じて、 AWS 環境を一元的に管理および管理するのに役立ちます。の AWS Organizations 組織は AWS アカウント を論理グループまたは組織単位に統合し、単一の単位として管理できるようにします。 AWS Organizations は、管理アカウントと呼ばれる専用アカウントから管理します。詳しくは、[AWS Organizations terminology and concepts] (用語と概念) をご覧ください。

AWS マルチアカウント環境を管理することをお勧めします AWS Organizations。これにより、会社のアカウントとリソースの完全なインベントリを作成できます。この完全なアセットインベントリは、脆弱性管理の重要な側面です。アプリケーションチームは、組織外のアカウントを使用しないでください。

AWS Control Tower は、規範的なベストプラクティスに従って、 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。マルチアカウント環境をまだ確立していない場合 AWS Control Tower は、開始点として が適しています。

セキュリティAWS リファレンスアーキテクチャ (AWS SRA) で説明されている専用のアカウント構造とベストプラクティスを使用することをお勧めします。Security Tooling アカウントは、セキュリティサービスの委任管理者として機能する必要があります。このアカウントでの脆弱性管理ツールの設定の詳細については、このガイドの後半で説明します。アプリケーションは、ワークロード組織単位 (OU) の専用アカウントでホストします。これにより、各アプリケーションのワークロードレベルの強力な分離と明示的なセキュリティ境界が確立されます。マルチアカウントアプローチを使用する設計原則と利点については、「Organizing Your AWS Environment Using Multiple Accounts」(AWS ホワイトペーパー) を参照してください。

意図的なアカウント構造を持ち、専用アカウントからセキュリティサービスを一元管理することは、スケーラブルな脆弱性管理プログラムの重要な要素です。

タグを定義、実装、適用する

タグは、 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です。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。タグを使用して、ビジネスユニット、アプリケーション所有者、環境、コストセンターなどのビジネスコンテキストを提供できます。次の表は、サンプルタグのセットを示しています。

キー	値
BusinessUnit	HumanResources

キー	値
CostCenter	CC101
ApplicationTeam	HumanResourcesTechnology
環境	本番稼働

タグは、検出結果の優先順位付けに役立ちます。例えば、次のことに役立ちます。

- 脆弱性へのパッチ適用を担当するリソースの所有者を特定する
- 検出結果の数が多いアプリケーションまたはビジネスユニットを追跡する
- 個人を特定できる情報 (PII) や支払いカード業界 (PCI) データなどの特定のデータ分類に対して、検出結果の重要度をエスカレーションする
- 下位レベルの開発環境のテストデータや本番稼働用データなど、環境内のデータの種類を特定する

大規模な効果的なタグ付けを実現するには、「リソースのタグ付けのベストプラクティス」(ホワイトペーパー) の「タグ付け戦略の構築」の指示に従ってください。 AWS AWS

AWS セキュリティ情報のモニタリング

AWS セキュリティ速報を定期的かつ頻繁にモニタリングすることを強くお勧めします。セキュリティ速報では、新しいセキュリティ関連の脆弱性、影響を受けるサービス、および該当する更新が通知されます。セキュリティ速報の RSS フィードをサブスクライブし、脆弱性管理プログラムの一環としてこれらの速報を取り込んで対処するプロセスを構築することもできます。

AWS セキュリティサービスを設定する

AWS は、 AWS 環境の保護に役立つように設計されたさまざまなセキュリティサービスを提供します。脆弱性管理プログラムでは、各アカウント AWS のサービス で以下を有効にすることをお勧めします。

- Amazon GuardDuty は、環境内のアクティブな脅威を検出するのに役立ちます。GuardDuty の検出結果は、環境で悪用された未知の脆弱性を特定するのに役立つ可能性があります。また、パッチが適用されていない脆弱性の影響を理解するのに役立ちます。

- AWS Health は、リソースのパフォーマンスと AWS のサービス および アカウントの可用性を継続的に可視化します。
- AWS Identity and Access Management Access Analyzer は、 AWS 環境内のリソースベースのポリシーを分析して、外部エンティティと共有されているリソースを特定します。これにより、リソースやデータへの意図しないアクセスに関連する脆弱性を特定できます。アカウントの外部で共有されているリソースのインスタンスごとに、IAM Access Analyzer は結果を生成します。
- Amazon Inspector は、ソフトウェアの脆弱性と意図しないネットワークへの露出について AWS ワークロードを継続的にスキャンする脆弱性管理サービスです。
- AWS Security Hub CSPM は、セキュリティ業界標準に照らして AWS 環境をチェックし、クラウド設定リスクを特定するのに役立ちます。また、他の AWS セキュリティサービスやサードパーティーのセキュリティツールから結果を集約することで AWS 、セキュリティ状態を包括的に把握できます。

このセクションでは、スケーラブルな脆弱性管理プログラムを確立するために Amazon Inspector と Security Hub CSPM を有効にして設定する方法について説明します。

脆弱性管理プログラムでの Amazon Inspector の使用

Amazon Inspector は、Amazon Elastic Compute Cloud (Amazon EC2) インスタンス、Amazon Elastic Container Registry (Amazon ECR) コンテナイメージ、 AWS Lambda 機能を継続的にスキャンし、ソフトウェアの脆弱性や意図しないネットワークの露出を検出する脆弱性管理サービスです。Amazon Inspector を使用すると、 AWS 環境全体のソフトウェアの脆弱性を可視化し、解決に優先順位を付けることができます。

Amazon Inspector は、リソースのライフサイクルを通じて環境を継続的に評価します。新しい脆弱性を引き起こす可能性のある変更に応じて、リソースを自動的に再スキャンします。例えば、EC2 インスタンスに新しいパッケージをインストールしたとき、パッチを適用したとき、またはリソースに影響を与える新しい共通脆弱性識別子 (CVE) が公開されたときに再スキャンします。Amazon Inspector により、脆弱性またはオープンネットワークパスが特定されると、調査可能な検出結果が生成されます。この検出結果は、以下を含む脆弱性に関する包括的な情報を提供します。

- Amazon Inspector リスクスコア
- 共通脆弱性評価システム (CVSS) のスコア
- 影響を受けるリソース
- Amazon、Recorded Future、および Cybersecurity and Infrastructure Security Agency (CISA) からの CVE に関する脆弱性インテリジェンスデータ

- 修復のレコメンデーション

Amazon Inspector のセットアップ手順については、「Getting started with Amazon Inspector」を参照してください。このチュートリアルの「Activate Amazon Inspector」ステップでは、スタンドアロンアカウント環境とマルチアカウント環境の 2 つの設定オプションが用意されています。組織のメンバー AWS アカウント である複数の をモニタリングする場合は、マルチアカウント環境オプションを使用することをお勧めします AWS Organizations。

マルチアカウント環境に Amazon Inspector を設定するときは、組織内のアカウントを Amazon Inspector の委任管理者に指定します。委任管理者は、組織のメンバーの検出結果と一部の設定を管理できます。例えば、委任管理者は、すべてのメンバーアカウントの集計された検出結果の詳細を表示したり、メンバーアカウントのスキャンを有効または無効にしたり、スキャンされたリソースを確認したりできます。SRA では、Security Tooling AWS アカウントを作成し、Amazon Inspector の委任管理者として使用することをお勧めします。 https://docs.aws.amazon.com/prescriptive-guidance/latest/security-reference-architecture/security-tooling.html

脆弱性管理プログラム AWS Security Hub CSPM での の使用

でスケーラブルな脆弱性管理プログラムを構築する AWS には、クラウド設定リスクに加えて、従来のソフトウェアとネットワークの脆弱性を管理する必要があります。 AWS Security Hub CSPM は、セキュリティ業界標準に照らして AWS 環境をチェックし、クラウド設定リスクを特定するのに役立ちます。Security Hub CSPM は、他のセキュリティサービスやサードパーティーのセキュリティツールからセキュリティ検出結果を集約 AWS することで、 AWS のセキュリティ状態を包括的に把握することもできます。

以下のセクションでは、脆弱性管理プログラムをサポートするために Security Hub CSPM を設定するためのベストプラクティスと推奨事項を示します。

- Security Hub CSPM のセットアップ
- Security Hub CSPM 標準を有効にする
- Security Hub CSPM の検出結果の管理
- 他のセキュリティサービスやツールからの検出結果の集約

Security Hub CSPM のセットアップ

セットアップの手順については、「AWS Security Hub CSPMのセットアップ」を参照してください。Security Hub CSPM を使用するには、 を有効にする必要がありますAWS Config。詳細については、Security Hub CSPM ドキュメントの「有効化と設定 AWS Config」を参照してください。

と統合されている場合は AWS Organizations、組織管理アカウントから、Security Hub CSPM 委任管理者となるアカウントを指定します。手順については、「Security Hub CSPM 委任管理者の指定」を参照してください。SRA では、Security Tooling AWS アカウントを作成し、Security Hub CSPM 委任管理者として使用することをお勧めします。 https://docs.aws.amazon.com/prescriptive-guidance/latest/security-reference-architecture/security-tooling.html

委任管理者は、組織内のすべてのメンバーアカウントに対して Security Hub CSPM を設定し、それらのアカウントに関連付けられた検出結果を表示するために自動的にアクセスできます。すべてので AWS Config Security Hub CSPM を有効にすることをお勧めします AWS リージョン AWS アカウント。新しい組織アカウントを Security Hub CSPM メンバーアカウントとして自動的に処理するように Security Hub CSPM を設定できます。手順については、「組織に属するメンバーアカウントの管理」を参照してください。

Security Hub CSPM 標準を有効にする

Security Hub CSPM は、セキュリティコントロールに対して自動的かつ継続的なセキュリティチェックを実行して検出結果を生成します。コントロールは 1 つ以上のセキュリティ標準に関連付けられています。コントロールは、標準の要件が満たされているかどうかの判断に役立ちます。

Security Hub CSPM で標準を有効にすると、Security Hub CSPM は標準に適用されるコントロールを自動的に有効にします。Security Hub CSPM は AWS Config ルールを使用して、コントロールのセキュリティチェックのほとんどを実行します。Security Hub CSPM 標準はいつでも有効または無効にできます。詳細については、「 のセキュリティコントロールと標準 AWS Security Hub CSPM」を参照してください。標準の完全なリストについては、「Security Hub CSPM 標準リファレンス」を参照してください。

推奨されるセキュリティ標準が組織にまだない場合は、AWS Foundational Security Best Practices (FSBP) 標準を使用することをお勧めします。この標準は、 AWS アカウント および リソースがセキュリティのベストプラクティスから逸脱するタイミングを検出するように設計されています。 は、この標準を AWS キュレートし、新機能とサービスをカバーするように定期的に更新します。FSBP の検出結果をトリアージしたら、他の標準を有効にすることを検討してください。

Security Hub CSPM の検出結果の管理

Security Hub CSPM には、組織全体からの大量の検出結果に対処し、 AWS 環境のセキュリティ状態を理解するのに役立ついくつかの機能が用意されています。検出結果の管理に役立つように、次の 2 つの Security Hub CSPM 機能を有効にすることをお勧めします。

- クロスリージョン集約を使用して、複数の から単一の集約リージョンに検出結果、検出結果の更新、インサイト、コントロールコンプライアンスステータス、セキュリティスコア AWS リージョン を集約します。
- 統合されたコントロールの検出結果を使用して、重複した検出結果を削除することで検出結果のノイズを減らします。アカウントで統合コントロールの検出結果を有効にすると、コントロールが複数の有効な標準に適用されていても、Security Hub CSPM はコントロールのセキュリティチェックごとに 1 つの新しい検出結果または検出結果の更新を生成します。

他のセキュリティサービスやツールからの検出結果の集約

セキュリティ検出結果の生成に加えて、Security Hub CSPM を使用して、複数の AWS のサービス サポートされているサードパーティーのセキュリティソリューションから検出結果を集約できます。このセクションでは、Security Hub CSPM へのセキュリティ検出結果の送信に焦点を当てます。次のセクション ではセキュリティ検出結果を割り当てる準備をする、Security Hub CSPM から検出結果を受け取ることができる製品と Security Hub CSPM を統合する方法について説明します。

Security Hub CSPM と統合できる AWS のサービスサードパーティー製品やオープンソースソリューションが多数あります。使い始めたばかりの場合は、以下を実行することをお勧めします。

1. 統合を有効にする AWS のサービス – Security Hub CSPM に結果を送信するほとんどの AWS のサービス 統合は、Security Hub CSPM と統合サービスの両方を有効にすると自動的にアクティブ化されます。脆弱性管理プログラムでは、各アカウントで Amazon Inspector、Amazon GuardDuty AWS Health、IAM Access Analyzer を有効にすることをお勧めします。これらのサービスは、検出結果を Security Hub CSPM に自動的に送信します。サポートされている AWS のサービス 統合の完全なリストについては、AWS のサービス Security Hub CSPM に結果を送信する を参照してください。

> **Note**
>
> AWS Health は、次のいずれかの条件が満たされた場合、結果を Security Hub CSPM に送信します。
>
> - 検出結果が AWS セキュリティサービスに関連付けられている

- 検出結果の typecode に `security`、`abuse`、`certificate` という言葉が含まれている
- 検出結果 AWS Health サービスは `risk`または です。 `abuse`

2. サードパーティー統合のセットアップ – 現在サポートされている統合のリストについては、「Available third-party partner product integrations」を参照してください。Security Hub CSPM に結果を送受信できる追加のツールを選択します。これらのサードパーティーツールの一部は、既に導入済みである可能性があります。製品の手順に従って、Security Hub CSPM との統合を設定します。

セキュリティ検出結果を割り当てる準備をする

このセクションでは、チームがセキュリティ検出結果の管理と割り当てに使用するツールを設定します。このセクションでは、次のオプションについて説明します。

- 既存のツールとワークフローで検出結果を管理する – このオプションは AWS Security Hub CSPM 、チームが製品バックログなどの日常業務の管理に使用する既存のシステムと統合されます。このオプションは、ワークフローを管理するためのツールを確立しているチームに推奨されます。
- Security Hub CSPM で検出結果を管理する – このオプションは、適切なチームがアラートを受け取り、Security Hub CSPM で検出結果に対処できるように、Security Hub CSPM イベントの通知を設定します。

チームにとって最適なワークフローを決定し、セキュリティ検出結果がそれぞれの所有者に迅速に届くようにします。

既存のツールとワークフローで検出結果を管理する

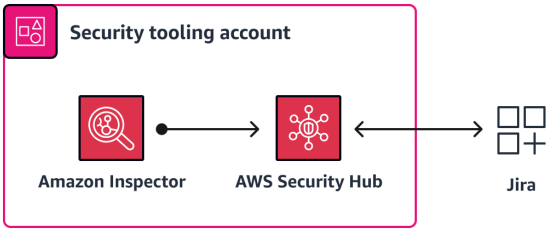
チームが日常業務を管理または実行するために使用するツールを確立しているエンタープライズ組織には、Security Hub CSPM 統合を追加することをお勧めします。Security Hub CSPM の検出結果を複数のテクノロジープラットフォームにインポートできます。以下に例を示します。

- セキュリティ情報とイベント管理 (SIEM) システムは、セキュリティチームが運用上のセキュリティイベントをトリアージするのに役立ちます。SIEM システムは、アプリケーションとネットワークハードウェアによって生成されたセキュリティアラートをリアルタイムで分析します。

- ガバナンス、リスク、コンプライアンス (GRC) システムは、コンプライアンスチームとガバナンスチームがリスク管理データをモニタリングおよび報告するのに役立ちます。GRC ツールは、企業がポリシーの管理、リスクの評価、ユーザーアクセスの制御、コンプライアンスの合理化に使用できるソフトウェアアプリケーションです。GRC ツールを使用して、ビジネスプロセスを統合し、コストを削減し、効率を向上させることができます。
- 製品バックログとチケット発行システムは、アプリケーションチームとクラウドチームが機能を管理し、開発タスクに優先順位を付けるのに役立ちます。Atlassian Jira と Microsoft Azure DevOps は、これらのシステムの例です。

Security Hub CSPM の検出結果をこれらの既存のエンタープライズシステムに直接統合すると、毎日の運用ワークフローが変更される必要がないため、平均復旧時間 (MTTR) とセキュリティの結果を向上させることができます。チームは、個別のワークフローやツールを使用する必要がないため、セキュリティ検出結果に迅速に対応して学習できます。統合により、セキュリティ検出結果への対応が通常の標準ワークフローの一部になります。

Security Hub CSPM は、複数のサードパーティーパートナー製品と統合されています。詳細なリストと手順については、Security Hub CSPM ドキュメントの「利用可能なサードパーティーパートナー製品統合」を参照してください。一般的な統合にはAtlassian - Jira Service Management、、Jira ソフトウェア AWS Security Hub CSPM との双方向統合、 などがありますServiceNow – ITSM。次の図は、Security Hub CSPM に結果を送信するように Amazon Inspector を設定し、すべての結果をに送信するように Security Hub CSPM を設定する方法を示していますJira。



Security Hub CSPM で検出結果を管理する

Amazon EventBridge ルールと Amazon Simple Notification Service (Amazon SNS) トピックを使用して、Security Hub CSPM の検出結果のクラウドベースの通知システムを構築できます。このシステムは、検出結果の作成時に、適切なチームに通知します。このアプローチでは、アプリケーションが専用アカウントに分割されるため、「AWS アカウント 構造を開発する」で説明されているマルチアカウント戦略が重要です。これにより、検出結果ごとに適切なチームに通知できます。

セキュリティチームまたはクラウドチームは、すべての からイベントを受信することを選択できます AWS アカウント。この場合、Security Hub CSPM 委任管理者アカウント内に EventBridge ルールを構築し、これらのチームに通知する Amazon SNS トピックをサブスクライブします。アプリケーションチームの場合は、それぞれのアプリケーションアカウント内で EventBridge ルールと SNS トピックを設定します。アプリケーションアカウント内で Security Hub CSPM の検出結果が発生すると、担当チームにその検出結果が通知されます。

Security Hub CSPM は、すべての新しい検出結果と既存の検出結果へのすべての更新を Security Hub CSPM 検出結果 - インポートされたイベントとして EventBridge に自動的に送信します。Security Hub CSPM の検出結果 - インポートされた各イベントには、1 つの検出結果が含まれます。EventBridge ルールにフィルターを適用して、検出結果がフィルターと一致する場合にのみ、その検出結果によってルールを起動できます。手順については、「自動的に送信される結果の EventBridge ルールの設定」を参照してください。Amazon SNS トピックの作成とサブスクライブの詳細については、「Amazon SNS を設定する」を参照してください。

このアプローチを使用する場合は、次の点を考慮してください。

- アプリケーションチームの場合は、アプリケーションがホストされている各 AWS アカウント と AWS リージョン 内に EventBridge ルールを作成します。
- セキュリティチームとクラウドチームの場合は、Security Hub CSPM 委任管理者アカウントに EventBridge ルールを作成します。これにより、メンバーアカウント内のすべての検出結果についてチームに通知されます。
- セキュリティ検出結果のステータスが `NEW` の場合、Amazon SNS は毎日通知を送信します。毎日の通知をオフにする場合は、Amazon SNS サブスクライバーが通知を受信`NOTIFIED`した後、検出結果のステータスを `NEW` から に変更するカスタム AWS Lambda 関数を作成できます。

AWS 環境でのセキュリティ検出結果のトリアージと修復

セキュリティ検出結果のトリアージには、検出結果を適切なステークホルダーにルーティングし、検出結果を評価して優先順位を付け、修復することが含まれます。このセクションでは、これらの各ステップを詳しく確認し、スケーラビリティと効率に関する推奨事項を提供します。また、トリアージと修復のプロセスを説明するのに役立つ例も含まれています。

トピック

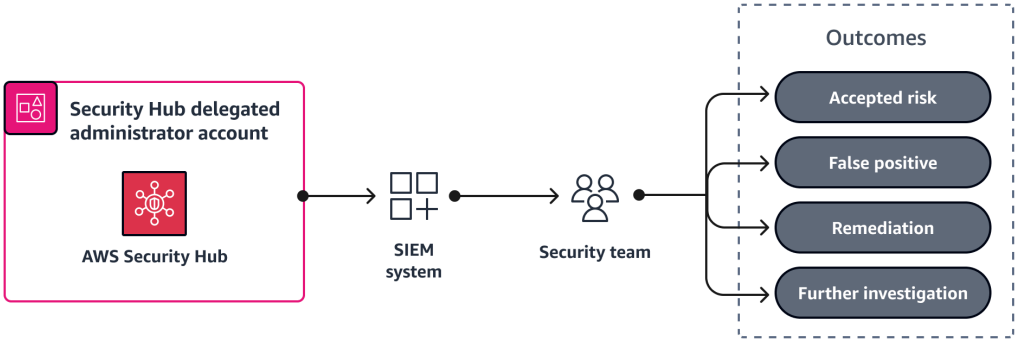
セキュリティ検出結果の所有権を定義する

セキュリティ検出結果をトリアージするための所有権モデルの定義は難しい場合がありますが、必ずしもそうである必要はありません。セキュリティ環境は常に変化しており、実務者はこれらの変化に柔軟に対応できる必要があります。セキュリティ検出結果の所有権モデルを開発するには、柔軟なアプローチを採用します。初期モデルは、チームがすぐに対応できるようにする必要があります。基本的な所有権ロジックから開始し、そのロジックを時間をかけて改良していくことをお勧めします。完全な所有権基準の定義を遅らせると、セキュリティ検出結果の数は増え続けます。

結果を適切なチームやリソースに簡単に割り当てられるように、チームが日常業務の管理に使用する AWS Security Hub CSPM 既存のシステムと統合することをお勧めします。例えば、Security Hub CSPM をセキュリティ情報イベント管理 (SIEM) システムまたは製品バックログおよびチケット発行システムと統合できます。詳細については、このガイドの「セキュリティ検出結果を割り当てる準備をする」を参照してください。

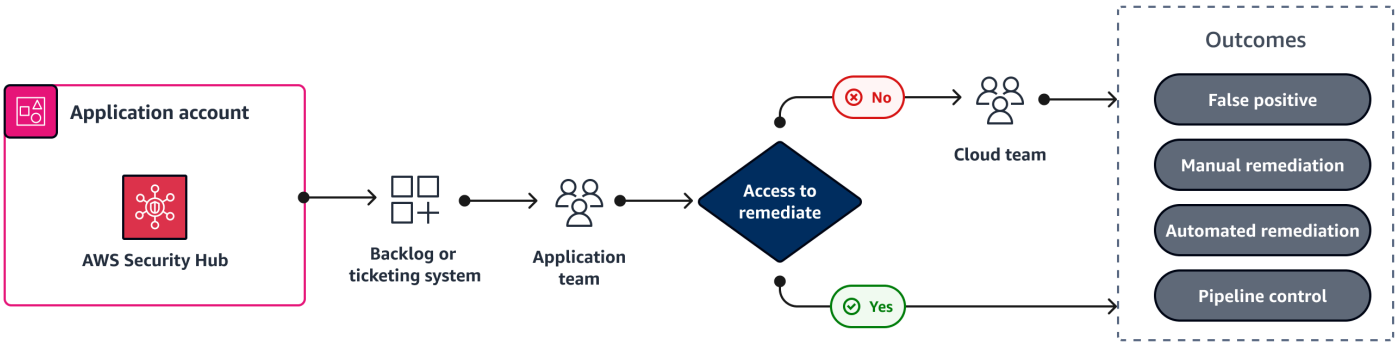
以下は、開始点として使用できる所有権モデルの例です。

- セキュリティチームは、潜在的にアクティブな脅威を確認し、セキュリティ検出結果の評価と優先順位付けを支援します。セキュリティチームには、コンテキストを適切に評価するための専門知識とツールがあります。脆弱性の評価と優先順位付け、脅威検出イベントの調査に役立つ追加のセキュリティ関連データを理解しています。検出結果の重要度または追加のチューニングが必要な場合は、このガイドの「セキュリティ検出結果の評価と優先順位付けを行う」セクションを参照してください。例については、このガイドの「セキュリティチームの例」を参照してください。



- クラウドチームとアプリケーションチーム間でセキュリティ検出結果を分散する – 「セキュリティ所有権を分散する」セクションで説明したように、リソースを設定するためのアクセス権を持つチームが、安全な設定を担当します。アプリケーションチームは、構築および設定するリソースに関連するセキュリティ検出結果に責任を負い、クラウドチームは広範な設定に関連するセキュリティ検出結果に責任を負います。ほとんどの場合、アプリケーションチームは、 のサービスコントロールポリシー (SCPs) AWS のサービス、 AWS Organizationsネットワーク関連の VPC 設定 AWS Control Tower、AWS IAM Identity Center など、広範な設定を変更することはできません。

  アプリケーションを専用アカウントに分離するマルチアカウント環境では、通常、アカウントのセキュリティ関連の検出結果をアプリケーションのバックログまたはチケット発行システムに統合できます。そのシステムから、クラウドチームまたはアプリケーションチームが検出結果に対処できます。例については、このガイドの「クラウドチームの例」または「アプリケーションチームの例」を参照してください。



- 残りの未解決の検出結果をクラウドチームに割り当てる – 残った検出結果は、クラウドチームが対処できるデフォルト設定または広範な設定に関連している可能性があります。このチームは、検出結果を解決するための最も多くの知識とアクセス権を持っている可能性があります。全体として、これは通常、検出結果全体の中でもごく一部にとどまります。

セキュリティ検出結果の評価と優先順位付けを行う

効果的な脆弱性管理プログラムの重要な要素の 1 つは、セキュリティの検出結果を評価して優先順位を付ける能力です。この段階では、コンテキストや組織の履歴を取り入れ、検出システムをチューニングします。セキュリティ検出結果の優先順位付けは、適切な対応スピードの確立に役立ちます。

Amazon Inspector、 AWS Security Hub CSPMおよび Amazon GuardDuty の場合、検出結果には重要度ラベルまたはスコアが含まれます。Foundational Security Best Practices (FSBP) 標準、Amazon Inspector、GuardDuty に関連する検出結果を含め、Security Hub CSPM のすべての重大度の高い検出結果の調査を優先することをお勧めします。検出結果の重要度ラベルは、次のようにスコアが決定されます。

- Amazon Inspector スコアは、検出結果ごとに高度にコンテキスト化されたスコアです。これは、共通脆弱性評価システム (CVSS) の基本スコア情報と、ネットワーク到達可能性の結果、および悪用可能性データを相関させて計算されます。このスコアを使用すると、検出結果に優先順位を付け、最も重要な検出結果と脆弱なリソースに集中できます。Amazon Inspector は、スコアに加えて、共通脆弱性識別子 (CVE) に関する強化された脆弱性インテリジェンスも提供します。これは、Amazon が提供する CVE に関する情報の他、Recorded Future や Cybersecurity and Infrastructure Security Agency (CISA) などの業界標準のセキュリティインテリジェンスソースについてまとめたものです。例えば、Amazon Inspector は、脆弱性の悪用に使用される既知のマルウェアキットの名前を提供できます。詳細については、「Vulnerability Intelligence」を参照してください。
- GuardDuty の各検出結果には、その検出結果が環境にもたらす潜在的なリスクを反映する重要度レベルと値が割り当てられています。このレベルと値は、 AWS のセキュリティエンジニアによって決定されます。例えば、High 重要度レベルは、リソースが侵害され、不正な目的で実際に使用されていることを示します。High 重要度の GuardDuty 検出結果は優先的に対応し、さらなる不正使用を防ぐためにすぐに修復することをお勧めします。
- Security Hub CSPM コントロールの検出結果の重要度は、悪用の難しさと侵害の可能性によって決まります。この難易度は、弱点を利用して脅威シナリオを実行するために必要な洗練度または複雑さの度合いによって決まります。侵害の可能性は、脅威シナリオが AWS のサービス または リソースの中断または違反につながる可能性を示します。

検出結果をチューニングするには、それぞれのサービスコンソールで、またはサービスの API を使用して、特定の検出結果を直接抑制またはアーカイブできます。さらに、自動化ルールを使用して、Security Hub CSPM で検出結果を変更することもできます。GuardDuty および Amazon Inspector の検出結果は、Security Hub CSPM に自動的に送信されます。定義した基準に基づき、自

動化ルールを使用して、検出結果をほぼリアルタイムで自動的に更新 (重要度の変更など) または抑制できます。自動化ルールを作成するときは、作成日や変更日、作成者、ルールが必要な理由など、ルールの説明にコンテキストを追加することをお勧めします。この情報は、将来の参照時に役立ちます。

セキュリティ検出結果を修復する

検出結果を評価して優先順位を付けた後は、次のアクションとして検出結果を修復します。検出結果を修復するために実行できるアクションは多数あります。ソフトウェアの脆弱性については、オペレーティングシステムを更新したり、パッチを適用したりできます。クラウド設定の検出結果については、リソース設定を更新できます。一般的に、修復のために実行するアクションは、次のいずれかの結果に分類できます。

- 手動修復 – AWS リソースのプロパティを変更して暗号化を有効にするなど、脆弱性の修正を手動で提供します。検出結果が Security Hub CSPM の 1 つのマネージドチェックからのものである場合、検出結果には、検出結果を手動で修正する手順へのリンクが含まれます。
- 再利用可能なアーティファクト – Infrastructure as Code (IaC) を更新して脆弱性を修復します。同様の解決策が他のユーザーにも役立つと考えられる場合は、更新済みの IaC と解決策の簡単な概要を内部共有コードリポジトリにアップロードすることを検討してください。
- 自動修復 – 脆弱性は、作成したメカニズムによって自動的に修復されます。
- パイプラインコントロール – 脆弱性が存在する場合にデプロイを防ぐよう、継続的インテグレーションおよび継続的デリバリー (CI/CD) パイプライン内にコントロールを適用します。
- 許容可能なリスク – アクションを実行したり、補償コントロールを実装したりせず、脆弱性がもたらすリスクを受け入れます。許容可能なリスクは、リスクレジストリなどの専用の場所で追跡します。
- 誤検出 – 検出結果が脆弱性を正しく特定しなかったと判断したため、何も実行しません。

脆弱性の修復に使用できるさまざまなアクションとツールの完全なリストは、このガイドの対象外です。ただし、大規模な脆弱性の修復に役立つサービスやツールには、次のような注目に値するものがあります。

- の一機能である Patch Manager は AWS Systems Manager、セキュリティ関連の更新と他のタイプの更新の両方を使用してマネージドノードにパッチを適用するプロセスを自動化します。Patch Manager を使用して、オペレーティングシステムとアプリケーションの両方にパッチを適用することができます。

- AWS Firewall Manager では、 のアカウントとアプリケーション全体でファイアウォールルールを一元的に設定および管理できます AWS Organizations。新しいアプリケーションが作成されると、Firewall Manager は、共通の一連のセキュリティルールを適用することで、新しいアプリケーションとリソースをコンプライアンスに適合させやすくします。
- の自動セキュリティ対応 AWSは、Security Hub CSPM と連携する AWS ソリューションであり、業界のコンプライアンス標準とセキュリティ脅威のベストプラクティスに基づいて事前定義された対応と修復アクションを提供します。

セキュリティ検出結果のトリアージと修復の例

このセクションでは、セキュリティ、クラウド、アプリケーションチームのトリアージプロセスの例を示します。ここでは、各チームが一般的に対処する検出結果のタイプについて説明し、対応方法の例を示します。大まかな修復ガイダンスも含まれています。

このセクションには、次の例が含まれます。

- セキュリティチームの例: Security Hub CSPM 自動化ルールの作成
- クラウドチームの例: VPC 設定の変更
- アプリケーションチームの例: AWS Config ルールの作成

セキュリティチームの例: Security Hub CSPM 自動化ルールの作成

セキュリティチームは、Amazon GuardDuty の検出結果など、脅威の検出に関連する検出結果を受け取ります。 AWS リソースタイプ別に分類された GuardDuty 検出結果タイプの詳細なリストについては、GuardDuty ドキュメントの「検出結果タイプ」を参照してください。セキュリティチームは、これらのすべての検出結果タイプに精通している必要があります。

この例では、セキュリティチームは、学習目的で厳密に AWS アカウント 使用され、重要なデータや機密データを含まない のセキュリティ検出結果に関連するリスクのレベルを受け入れています。このアカウントの名前は sandbox で、アカウント ID は 123456789012 です。セキュリティチームは、このアカウントからのすべての GuardDuty 検出結果を抑制する AWS Security Hub CSPM 自動化ルールを作成できます。多くの一般的なユースケースをカバーするテンプレートからルールを作成することも、カスタムルールを作成することもできます。Security Hub CSPM では、条件の結果をプレビューして、ルールが意図した検出結果を返すことを確認することをお勧めします。

> **Note**
>
> この例では、自動化ルールの機能に焦点を当てています。アカウントのすべての GuardDuty 検出結果を抑制することはお勧めしません。コンテキストは重要であり、各組織はデータ型、分類、緩和コントロールに基づいて抑制する検出結果を選択する必要があります。

この自動化ルールの作成に使用されるパラメータを次に示します。

- ルール:
  - ルール名は `Suppress findings from Sandbox account` です
  - ルールの説明は `Date: 06/25/23 Authored by: John Doe Reason: Suppress GuardDuty findings from the sandbox account` です
- 条件:
  - `AwsAccountId` = `123456789012`
  - `ProductName` = `GuardDuty`
  - `WorkflowStatus` = `NEW`
  - `RecordState` = `ACTIVE`
- 自動アクション:
  - `Workflow.status` は `SUPPRESSED`

詳細については、Security Hub CSPM ドキュメントの「オートメーションルール」を参照してください。セキュリティチームには、検出された脅威の検出結果を調査および修復するための多くのオプションがあります。詳細なガイダンスについては、「AWS Security Incident Response テクニカルガイド」を参照してください。このガイドを確認して、強力なインシデント対応プロセスが確立されていることを確認することをお勧めします。

クラウドチームの例: VPC 設定の変更

クラウドチームは、ユースケースに合わない AWS デフォルト設定の変更など、一般的な傾向を持つセキュリティ検出結果の優先順位付けと修復を担当します。これらの検出結果は、VPC 設定などの多くの AWS アカウント またはリソースに影響を与える傾向があり、環境全体に配置する必要がある制限が含まれています。ほとんどの場合、クラウドチームはポリシーの追加や更新など、手動による 1 回限りの変更を行います。

組織が AWS 環境をしばらく使用した後、一連のアンチパターンが開発されている場合があります。アンチパターンとは、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です。これらのアンチパターンの代わりに、組織は AWS Organizations サービスコントロールポリシー (SCPs) や IAM Identity Center アクセス許可セットなど、より効果的な環境全体の制限を使用できます。SCP とアクセス許可セットは、ユーザーがパブリックな Amazon Simple Storage Service (Amazon S3) バケットを設定できないようにするなど、リソースタイプに対する追加の制限を提供することができます。すべての考え得るセキュリティ設定を制限したくなることもありますが、SCP とアクセス許可セットにはポリシーサイズ制限があります。予防的コントロールと検出的コントロールには、バランスの取れたアプローチをお勧めします。

以下は、クラウドチームが担当する AWS Security Hub CSPM 可能性のある基盤セキュリティベストプラクティス (FSBP) 標準のコントロールです。

- [EC2.2] VPC のデフォルトのセキュリティグループは、インバウンドトラフィックとアウトバウンドトラフィックを許可しないでください
- [EC2.6] VPC フローログ記録はすべての VPCsで有効にする必要があります
- [EC2.23] Amazon EC2 Transit Gateway は VPC アタッチメントリクエストを自動的に受け入れないでください
- [CloudTrail.1] CloudTrail を有効にし、読み取りおよび書き込み管理イベントを含む少なくとも 1 つのマルチリージョン証跡を設定する必要があります
- [Config.1] AWS Config を有効にする必要があります

この例では、クラウドチームが FSBP コントロール EC2.2 の検出結果に対処しています。このコントロールのドキュメントでは、デフォルトのインバウンドルールとアウトバウンドルールによって広範なアクセスが許可されるため、デフォルトのセキュリティグループを使用しないことが推奨されています。デフォルトのセキュリティグループは削除できないため、ルール設定を変更して、インバウンドトラフィックとアウトバウンドトラフィックを制限することが推奨されています。この問題に効率的に対処するには、各 VPC にこのデフォルトのセキュリティグループがあるため、クラウドチームは確立されたメカニズムを使用してすべての VPC のセキュリティグループルールを変更する必要があります。ほとんどの場合、クラウドチームは AWS Control Tower のカスタマイズや、HashiCorp Terraform、AWS CloudFormation などの Infrastructure as Code (IaC) ツールを使用して VPC 設定を管理します。

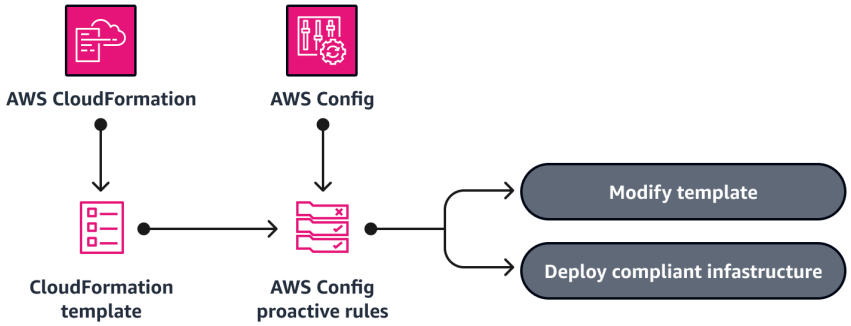
アプリケーションチームの例: AWS Config ルールの作成

以下は、アプリケーションまたは開発チームが担当する Security Hub CSPM Foundational Security Best Practices (FSBP) セキュリティ標準のコントロールです。

- [CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- [EC2.19] セキュリティグループは、高リスクのポートへの無制限アクセスを許可しないでください
- [CodeBuild.1] CodeBuild GitHub または Bitbucket ソースリポジトリ URLsは OAuth を使用する必要があります
- [ECS.4] ECS コンテナは非特権として実行する必要があります
- [ELB.1] Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります

この例では、アプリケーションチームが FSBP コントロール EC2.19 の検出結果に対処しています。このコントロールは、指定した高リスクのポートにセキュリティグループの受信 SSH トラフィックがアクセス可能かどうかをチェックします。セキュリティグループ内のルールがこれらのポートについて、`0.0.0.0/0` または `::/0` からの着信トラフィックを許可している場合、このコントロールは失敗します。このコントロールのドキュメントでは、このトラフィックを許可するルールを削除することを推奨しています。

個々のセキュリティグループルールに対処することに加えて、これは新しい AWS Config ルールになる結果の優れた例です。プロアクティブ評価モードを使用すると、将来的にリスクの高いセキュリティグループルールのデプロイを防ぐことができます。プロアクティブモードでは、リソースがデプロイされる前に評価されるため、リソースの設定ミスや関連するセキュリティ検出結果を防ぐことができます。新しいサービスまたは新機能を実装する場合、アプリケーションチームは継続的インテグレーションおよび継続的デリバリー (CI/CD) パイプラインの一部としてプロアクティブモードでルールを実行して、非準拠リソースを特定できます。次の図は、プロアクティブ AWS Config ルールを使用して、 AWS CloudFormation テンプレートで定義されたインフラストラクチャが準拠していることを確認する方法を示しています。



この例では、もう 1 つの重要な効率向上が得られます。アプリケーションチームがプロアクティブ AWS Config ルールを作成すると、他のアプリケーションチームがそれを使用できるように、共通のコードリポジトリで共有できます。

Security Hub CSPM コントロールに関連付けられた各検出結果には、検出結果の詳細と、問題を修正する手順へのリンクが含まれています。クラウドチームは、1 回限りの手動修復を必要とする検出結果に遭遇する可能性がありますが、必要に応じて、開発プロセスのできるだけ早い段階で問題を特定するプロアクティブチェックを構築することをお勧めします。

脆弱性管理プログラムの報告と改善

脆弱性管理の効果的な報告には、データのレビュー、傾向のモニタリング、知識の共有が含まれます。これにより、可視性が提供され、チームが AWS クラウドで組織のセキュリティ体制を改善するのに役立ちます。

毎月のセキュリティ運用会議を実施する

毎月のセキュリティ運用会議は、チーム間の継続的な所有権、説明責任、調整を促進するための効果的なメカニズムです。会議では、セキュリティ、クラウド、アプリケーションチームのステークホルダーが、未解決のセキュリティ検出結果、サービスレベルアグリーメント (SLA) 外の検出結果、および検出結果が最も多いチームに関するデータを確認します。

これらの会議は、チームが、さらに制限を追加する機会のようなアンチパターンを特定するのに役立ちます。予防的コントロールと自動化の機会を発見して共有することもできます。また、この会議は、脆弱性管理プログラム内で何がうまくいき、何がうまくいっていないかを特定し、改善を行うのにも役立ちます。

データの確認、アンチパターンや問題の特定、コントロールや自動化に関する情報の共有を通じて、チームは貴重なインサイトを得て、継続的な改善を行うことでセキュリティ体制を強化し、セキュリティ関連の SLA を削減できます。

Security Hub CSPM インサイトを使用してアンチパターンを特定する

AWS Security Hub CSPM インサイトは、アンチパターンを特定し、検出結果の修復の進行状況を追跡するのに役立ちます。Security Hub CSPM インサイトは、関連する検出結果のコレクションです。注意と介入が必要なセキュリティエリアを識別します。Security Hub CSPM インサイトは、特定の要件を特定し、レポートを作成するのに役立ちます。Security Hub CSPM には、いくつかの組み込みのマネージド型インサイトが用意されています。 AWS 環境と使用状況に固有のセキュリティ問題を追跡するには、カスタムインサイトを作成できます。

結論と次のステップ

要約すると、効果的な脆弱性管理プログラムには十分な準備が必要であり、適切なツールと統合を有効にし、それらのツールをファインチューニングし、問題を効率的に優先順位付けし、継続的に報告して改善する必要があります。このガイドのベストプラクティスに従うことで、組織はクラウド環境の保護に役立つスケーラブルな脆弱性管理プログラム AWS を に構築できます。

このプログラムを拡張して、アプリケーションセキュリティの脆弱性など、セキュリティ関連の脆弱性や検出結果を追加することができます。 はカスタム製品統合 AWS Security Hub CSPM をサポートしています。追加のセキュリティツールと製品の統合ポイントとして Security Hub CSPM を使用することを検討してください。この統合により、製品のバックログとの直接統合や、毎月のセキュリティレビュー会議など、脆弱性管理プログラムで既に確立したプロセスとワークフローを活用できます。

次の表は、このガイドで説明されているフェーズとアクション項目をまとめたものです。

[Phase] (フェーズ)	アクション項目
準備	• 脆弱性管理計画を定義します。 • 検出結果の所有権を分散します。 • 脆弱性開示プログラムを開発します。 • AWS アカウント 構造を開発します。 • タグを定義、実装、適用します。 • AWS セキュリティ情報を監視します。 • 委任された管理者で Amazon Inspector を有効にします。 • 委任された管理者で Security Hub CSPM を有効にします。 • Security Hub CSPM 標準を有効にします。 • Security Hub CSPM クロスリージョン集約を設定します。 • Security Hub CSPM で統合コントロールの検出結果を有効にします。 • SIEM、GRC、または製品バックログまたはチケットシステムとの適切なダウンストリー

[Phase] (フェーズ)	アクション項目
	ム統合など、Security Hub CSPM 統合を設定および管理します。
トリアージと修復	• マルチアカウント戦略に基づいて検出結果をルーティングします。 • 検出結果をセキュリティ、クラウド、アプリケーション、または開発者チームにルーティングします。 • セキュリティ検出結果を調整して、特定の環境で実行可能であることを確認します。 • 可能な場合は、自動修復メカニズムを開発します。 • 可能な場合は、セキュリティ検出結果が発生しないようにする CI/CD パイプラインコントロールまたはその他のガードレールを実装します。 • Security Hub CSPM オートメーションルールを使用して、検出結果をエスカレートまたは抑制します。
報告と改善	• 毎月のセキュリティ運用会議を開催します。 • Security Hub CSPM インサイトを使用して、アンチパターンを特定します。

リソース

AWS サービスのドキュメント

- 製品の統合 (AWS Security Hub CSPM)
- Jira Service Management Cloud での AWS Security Hub CSPM の統合 (AWS Security Hub CSPM)
- 自動化ルール (AWS Security Hub CSPM)
- プロアクティブ評価ルール (AWS Config)
- Patch Manager (AWS Systems Manager)

その他の AWS リソース

- Best practices for tagging AWS resources (AWS ホワイトペーパー)
- Automated Security Response on AWS (AWS ソリューションライブラリ)
- AWS セキュリティインシデント対応ガイド (AWS テクニカルガイド)
- AWS セキュリティ速報

ドキュメント履歴

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
初版発行	—	2023 年 10 月 12 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

A2A (Agent-to-Agent)

タスクの委任と状態転送をサポートするagent-to-agentコラボレーション用のステートフルプロトコル。

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。

[エージェント]

目標を達成するためのツールを使用して、自律的に推論、計画、アクションを実行できる AI システム。

エージェントオペレーション

AI エージェントを本番環境で大規模に構築、テスト、デプロイ、実行するための運用プラクティス。

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の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。

シチズンデベロッパー

専門的な技術スキルを持たないノーコード/ローコードプラットフォームを使用して AI アプリケーションを作成するビジネスユーザー。

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。信頼できる ID 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。この戦略を採用するときは AWS、 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て、リソースの安全性を確保します。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、アベイラビリティーゾーン、コントロールプレーン AWS リージョン、データプレーンなどの境界で、障害の影響を制限し、ワークロードの耐障害性を向上させるのに役立ちます。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。

FM ゲートウェイ

基盤モデルへのアクセスを制御および正規化する一元化された仲介者。LLM ゲートウェイとも呼ばれます。

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、、Amazon GuardDuty AWS Security Hub CSPM、、 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。

ガードレール (AI)

エージェントの入力と出力をフィルタリング、検証、制約する安全メカニズムは、責任ある安全な AI の動作を確保するのに役立ちます。

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。

ヒューhuman-in-the-loop (HitL)

エージェントの実行が重要な決定時点で人間によるレビューと承認のために一時停止するワークフローパターン。

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 が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 AWS 運用し、ユーザーが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。

MCP

「モデルコンテキストプロトコル」を参照してください。

モデルコンテキストプロトコル (MCP)

エージェントとツール間の通信のためのステートレスプロトコル。

MCP サーバー

Model Context Protocol を通じて 1 つ以上のツールを公開するサービス。

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 とは独立しています。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、 にログイン AWS マネジメントコンソール 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、お客様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。

シャドウ AI

組織内の管理対象チャネルの外部で構築または使用される認可されていない AI アプリケーション。

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。

tool

エージェントが外部システムでオペレーションを実行するために呼び出すことができる関数または API。

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「 を他の AWS のサービス AWS Organizations で使用する 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。