AWS CAF セキュリティ機能を実装するための推奨セキュリティコントロール

AWS 規範ガイダンス

AWS 規範ガイダンス: AWS CAF セキュリティ機能を実装するための推奨セキュリティコントロール

Table of Contents

AWS CAF セキュリティ機能を実装するための推奨セキュリティコントロール

Rwest Singla と Rovan Omar、Amazon Web Services (AWS)

2023 年 11 月 (ドキュメント履歴)

セキュリティが最優先事項です AWS。運用上の負担を軽減するために、クラウドのセキュリティとコンプライアンスの責任は と共有します AWS。 AWS はクラウドのセキュリティを担当します。つまり、 で提供されるサービスを実行するインフラストラクチャを保護します AWS クラウド。データやアプリケーションなど、クラウド内のセキュリティはお客様の責任となります。このガイドでは、AWS クラウドのセキュリティ上の責任を果たすのに役立つセキュリティコントロールについて説明します。

AWS クラウド導入フレームワーク (AWS CAF) は、クラウドの準備状況を改善するために設計されたベストプラクティスを提供します。 AWS CAF は、これらのベストプラクティスをビジネス、人材、ガバナンス、プラットフォーム、セキュリティ、運用の 6 つの視点に分類します。このガイドでは、セキュリティの観点から以下の機能に焦点を当てています。

- ID とアクセスの管理 – 人とマシンの ID とそのアクセス許可を大規模に管理します。
- 脅威検出 – ログ記録とモニタリングを設定して、潜在的なセキュリティ設定ミス、脅威、または予期しない動作を検出して調査します。
- インフラストラクチャの保護 – システムやサービスを、意図しない、または不正なアクセスや潜在的な脆弱性から保護します。
- データの保護 – 機密性のレベルに基づいてデータを分類します。組織内のデータおよびそのアクセス方法や利用状況に対する可視性と管理を維持します。
- インシデント対応 – セキュリティインシデントの潜在的な影響に対応し、軽減するメカニズムを確立します。

これらの AWS CAF セキュリティ機能に予防的、検出的、応答的なセキュリティコントロールを実装しないと、クラウド環境に重大なリスクが生じ、ビジネスが中断される可能性があります。このガイドのセキュリティコントロールを実装すると、組織のクラウド環境を保護するのに役立ちます。

> **Note**
>
> AWS は、 での安全な運用に役立つサービス、ツール、フレームワークを提供します AWS クラウド。このガイドは、 AWS Well-Architected フレームワーク、 AWS クラウド導入フレームワーク (AWS CAF)、 AWS セキュリティリファレンスアーキテクチャ (AWS SRA)、および が発行するその他のセキュリティ推奨事項に合致し、補足するものです AWS。このガイドのコントロールは、クラウドセキュリティに関するすべての考慮事項を網羅しているわけではなく、これらのフレームワークに代わるものではありません。

ID とアクセスを管理するためのセキュリティコントロールの推奨事項

ID は で作成することも AWS、外部 ID ソースに接続することもできます。 AWS Identity and Access Management (IAM) ポリシーを通じて、ユーザーが AWS リソースと統合アプリケーションにアクセスまたは管理するために必要なアクセス許可を付与します。効果的に ID とアクセスを管理することで、適切な人物とマシンが適切な条件下で適切なリソースにアクセスできることを確認できます。 AWS Well-Architected フレームワークは、ID とそのアクセス許可を管理するためのベストプラクティスを提供します。ベストプラクティスの例としては、一元化された ID プロバイダーの利用や、多要素認証 (MFA) などの強力なサインインメカニズムの使用などがあります。このセクションで説明するセキュリティコントロールは、これらのベストプラクティスを実装するのに役立ちます。

このセクションのコントロール:

- ルートユーザーアクティビティの通知をモニタリングして設定
- ルートユーザーのアクセスキーは作成しないでください
- ルートユーザーの MFA を有効化
- IAM のセキュリティのベストプラクティスに従う
- 最小特権のアクセス許可を付与
- ワークロードレベルでアクセス許可ガードレールを定義
- IAM アクセスキーを定期的にローテーション
- 外部エンティティと共有されているリソースを識別

ルートユーザーアクティビティの通知をモニタリングして設定

を初めて作成するときは AWS アカウント、ルートユーザーと呼ばれる単一のサインインアイデンティティから始めます。ルートユーザーには、デフォルトで、そのアカウント内のすべての AWS のサービス とリソースに完全にアクセスできる権限があります。ルートユーザーについては、厳密に制御およびモニタリングし、ルートユーザーの認証情報を必要とするタスクにのみ使用する必要があります。

詳細については、以下のリソースを参照してください。

- AWS Well-Architected フレームワークで最小特権アクセスを付与する
- AWS 規範ガイダンスで IAM ルートユーザーのアクティビティをモニタリングする

ルートユーザーのアクセスキーは作成しないでください

ルートユーザーは、最も権限のある AWS アカウントのユーザーです。ルートユーザーへのプログラムによるアクセスを無効にすると、ユーザーの認証情報が誤って公開され、クラウド環境が侵害されるリスクを軽減できます。 AWS アカウント やリソースにアクセスする際は、一時的な認証情報として IAM ロールを作成して使用することをお勧めします。

詳細については、以下のリソースを参照してください。

- IAM ルートユーザーアクセスキーがドキュメントに存在しないこと AWS Security Hub CSPM
- ルートユーザーのアクセスキーを削除する (IAM ドキュメント)
- IAM ロール (IAM ドキュメント)

ルートユーザーの MFA を有効化

AWS アカウント ルートユーザーと IAM ユーザーに対して複数の多要素認証 (MFA) デバイスを有効にすることをお勧めします。これにより、 AWS アカウント のセキュリティレベルが引き上げられ、アクセス管理が簡素化されます。ルートユーザーは特権操作を実行できる権限の高いユーザーであるため、MFA を必須とすることが重要です。タイムベースドワンタイムパスワード (TOTP) アルゴリズムに基づいて数値コードを生成するハードウェア MFA デバイス、FIDO ハードウェアセキュリティキー、または仮想認証アプリケーションを使用できます。

2024 年、MFA は任意の のルートユーザーにアクセスする必要があります AWS アカウント。詳細については、 AWS セキュリティブログの「Secure by Design: AWS to enhance MFA requirements in 2024」を参照してください。このセキュリティプラクティスを拡張し、 AWS 環境内のすべてのユーザータイプに MFA を要求することを強くお勧めします。

可能であれば、ルートユーザーにはハードウェア MFA デバイスを使用することをお勧めします。仮想 MFA はハードウェア MFA デバイスと同じレベルのセキュリティを提供しない可能性があります。仮想 MFA は、ハードウェアの購入承認または納品を待っている間に使用できます。

数百のアカウントを管理する状況では AWS Organizations、組織のリスク許容度によっては、組織単位 (OU) 内の各アカウントのルートユーザーにハードウェアベースの MFA を使用することがスケーラブルではない場合があります。このような場合は、OU 内のアカウントのうち 1 つを OU 管理アカウントとして選択し、その OU 内の他のアカウントのルートユーザーを無効にすることができます。デフォルトでは、OU 管理アカウントは他のアカウントにアクセスできません。緊急時に OU 管理アカウントから他のアカウントにアクセスできるよう、事前にクロスアカウントアクセスを設定し

ておいてください。クロスアカウントアクセスを設定するには、メンバーアカウントに IAM ロールを作成し、OU 管理アカウントのルートユーザーのみがこのロールを引き受けられるようにポリシーを定義します。詳細については、IAM ドキュメントの「チュートリアル: IAM ロール AWS アカウント を使用して 全体でアクセスを委任する」を参照してください。

ルートユーザーの認証情報に対して、複数の MFA デバイスを有効にすることをお勧めします。任意の組み合わせの MFA デバイスを最大で 8 台登録できます。

詳細については、以下のリソースを参照してください。

- ハードウェア TOTP トークンの有効化 (IAM ドキュメント)
- 多要素認証 (MFA) 仮想デバイスの有効化 (IAM ドキュメント)
- FIDO セキュリティキーの有効化 (IAM ドキュメント)
- 多要素認証 (MFA) でルートユーザーのサインインを保護する (IAM ドキュメント)

IAM のセキュリティのベストプラクティスに従う

IAM ドキュメントには、 AWS アカウント および リソースの保護に役立つベストプラクティスのリストが含まれています。これには、最小特権の原則に従ってアクセス権と許可を設定するための推奨事項が含まれています。IAM セキュリティのベストプラクティスの例としては、ID フェデレーションの設定、MFA の必須化、一時的な認証情報の使用などがあります。

詳細については、以下のリソースを参照してください。

- IAM でのセキュリティのベストプラクティス (IAM ドキュメント)
- IAM ドキュメントのAWS リソースでの一時的な認証情報の使用

最小特権のアクセス許可を付与

最小特権とは、タスクを実行するために必要なアクセス許可のみを付与する際のプラクティスです。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。

属性ベースのアクセス制御 (ABAC) は、タグなどの属性に基づいてアクセス許可を定義する認可戦略です。グループ属性、ID 属性、リソース属性を使用して、個々のユーザーのアクセス許可を定義するのではなく、規模に応じてアクセス許可を動的に定義できます。例えば、ABAC を使用して、プロジェクトに関連付けられた特定のタグを持つリソースにのみ、開発者グループがアクセスできるように設定できます。

詳細については、以下のリソースを参照してください。

- 最小特権アクセス許可を適用する (IAM ドキュメント)
- AWSにおける ABAC とは (IAM ドキュメント)

ワークロードレベルでアクセス許可ガードレールを定義

マルチアカウント戦略を使用すると、ワークロードレベルでガードレールを柔軟に定義できるため、ベストプラクティスとされています。 AWS セキュリティリファレンスアーキテクチャは、アカウントを構築する方法に関する規範的なガイダンスを提供します。これらのアカウントは AWS Organizations の組織として管理され、アカウントは組織単位 (OU) ごとにグループ化されます。

AWS Control Tower などのAWS のサービスを使用すると、組織全体のコントロールを一元管理できます。組織内の各アカウントまたは OU に明確な目的を定義し、その目的に従ってコントロールを適用することをお勧めします。 は、リソースの管理とコンプライアンスのモニタリングに役立つ予防、検出、プロアクティブのコントロール AWS Control Tower を実装します。予防コントロールは、イベントの発生を防ぐように設計されています。検出コントロールは、イベントが発生した後に、検出、ログ記録、警告を行うように設計されています。プロアクティブコントロールは、リソースのプロビジョニング前にスキャンして、非準拠リソースのデプロイを防ぐように設計されています。

詳細については、以下のリソースを参照してください。

- AWS Well-Architected フレームワークのアカウントを使用してワークロードを分離する
- AWS 規範ガイダンスAWS のセキュリティリファレンスアーキテクチャ (AWS SRA)
- AWS Control Tower ドキュメントの のコントロールについて AWS Control Tower
- AWS 規範ガイダンスの でのセキュリティコントロールの実装 AWS
- サービスコントロールポリシーを使用して、 セキュリティブログの AWS 「Organization」のアカウント間でアクセス許可ガードレールを設定する AWS

IAM アクセスキーを定期的にローテーション

長期的に認証情報を必要とするユースケースでは、アクセスキーを更新するのがベストプラクティスです。アクセスキーは 90 日以内ごとにローテーションすることをお勧めします。アクセスキーをローテーションすることにより、侵害されたアカウントや終了したアカウントに関連付けられているアクセスキーが使用されるリスクが低くなります。また、紛失、侵害、盗難にあった可能性のある古

いキーを使用したアクセスを防止します。アクセスキーをローテーションしたら、必ずアプリケーションを更新してください。

詳細については、以下のリソースを参照してください。

- 長期的な認証情報を必要とするユースケースのためにアクセスキーを必要な時に更新する (IAM ドキュメント)
- AWS 規範ガイダンスの AWS Organizations および を使用して、IAM ユーザーアクセスキーを大規模に自動的にローテーション AWS Secrets Managerする
- アクセスキーの更新 (IAM ドキュメント)

外部エンティティと共有されているリソースを識別

外部エンティティは、別のユーザー、ルートユーザー、IAM ユーザーまたはロール、フェデレーティッドユーザー AWS アカウント、、匿名 (または認証されていない) ユーザーなど、 AWS 組織外のリソース、アプリケーション、サービス AWS のサービス、またはユーザーです。セキュリティのベストプラクティスは、IAM Access Analyzer を使用して、外部エンティティと共有されている Amazon Simple Storage Service (Amazon S3) バケットや IAM ロールなど、組織とアカウントのリソースを識別することです。これにより、セキュリティ上のリスクであるリソースやデータへの意図しないアクセスを特定できます。

詳細については、以下のリソースを参照してください。

- IAM Access Analyzer を使用して、リソースへのパブリックアクセスおよびクロスアカウントアクセスを確認する (IAM ドキュメント)
- AWS Well-Architected フレームワークでパブリックアクセスとクロスアカウントアクセスを分析する
- AWS Identity and Access Management Access Analyzerの使用 (IAM ドキュメント)

ログ記録とモニタリングに関するセキュリティコントロールの推奨事項

ログ記録とモニタリングは、脅威検出の重要な側面です。脅威検出は、 AWS クラウド導入フレームワーク (AWS CAF) のセキュリティパースペクティブ機能の 1 つです。ログデータを使用することで、組織は環境をモニタリングして、潜在的なセキュリティの設定ミス、脅威、予期しない動作を把握して特定できます。潜在的な脅威を把握することは、組織がセキュリティコントロールに優先順位を付けるのに役立ち、効果的な脅威検出は、脅威により迅速に対応するために役立ちます。

このセクションのコントロール:

- CloudTrail で少なくとも 1 つのマルチリージョン証跡を設定
- サービスとアプリケーションレベルのログ記録を設定
- ログを分析し、セキュリティイベントに対応するための一元的な場所を確立
- CloudTrail ログファイルを含む S3 バケットへの不正アクセスを防ぐ
- セキュリティグループまたはネットワーク ACL の変更に関するアラートを設定
- CloudWatch アラームが ALARM 状態になった場合のアラートを設定

CloudTrail で少なくとも 1 つのマルチリージョン証跡を設定

AWS CloudTrail は、 のガバナンス、コンプライアンス、運用リスクを監査するのに役立ちます AWS アカウント。ユーザー、ロール、または によって実行されたアクション AWS のサービス は、イベントとして CloudTrail に記録されます。イベントには、、 AWS Command Line Interface (AWS CLI) AWS マネジメントコンソール、および AWS SDKs と APIs で実行されたアクションが含まれます。このイベント履歴により、セキュリティ体制の分析、リソースの変更の追跡、コンプライアンスの監査が可能になります。

のイベントを継続的に記録するには AWS アカウント、証跡を作成する必要があります。各証跡は、すべての AWS リージョンでイベントを記録するように設定する必要があります。すべての でイベントをログに記録することで AWS リージョン、 AWS リージョン 発生したイベントに関係なく、で発生したすべてのイベント AWS アカウント がログに記録されます。マルチリージョン証跡により、グローバルサービスイベントがログに記録されます。

詳細については、以下のリソースを参照してください。

- CloudTrail 検出に関するセキュリティのベストプラクティス (CloudTrail ドキュメント)

- 1 つのリージョンに適用される証跡を変換してすべてのリージョンに適用 (CloudTrail ドキュメント)
- グローバルサービスイベントのログ記録の有効化と無効化 (CloudTrail ドキュメント)

サービスとアプリケーションレベルのログ記録を設定

AWS Well-Architected フレームワークでは、 サービスとアプリケーションのセキュリティイベントログを保持することをお勧めします。これは、監査、調査、運用上のユースケースにおけるセキュリティの基本原則です。サービスログとアプリケーションログの保持は、ガバナンス、リスク、コンプライアンス (GRC) 標準、ポリシー、手順に基づく一般的なセキュリティ要件です。

セキュリティ運用チームは、ログや検索ツールを使用して、不正なアクティビティや意図しない変更を示す可能性のある重要なイベントを検出します。ユースケースに応じて、さまざまなサービスのログ記録を有効にできます。例えば、Amazon S3 バケットアクセス、 AWS WAF ウェブ ACL トラフィック、ネットワークレイヤーの Amazon API Gateway トラフィック、または Amazon CloudFront ディストリビューションをログに記録できます。

詳細については、以下のリソースを参照してください。

- AWS アーキテクチャブログの「監査と分析のために Amazon CloudWatch Logs を一元化されたアカウントにストリーミングする」
- サービスとアプリケーションのログ記録を設定する (AWS Well-Architected フレームワーク)

ログを分析し、セキュリティイベントに対応するための一元的な場所を確立

手作業によるログ分析と情報処理では、複雑なアーキテクチャに関連する大量の情報に対応するには不十分です。分析とレポートだけでは、イベントを適切なリソースにタイムリーに割り当てることが容易になるわけではありません。 AWS Well-Architected フレームワークでは、 AWS セキュリティイベントと検出結果を、チケット発行、バグ、セキュリティ情報とイベント管理 (SIEM) システムなどの通知とワークフローシステムに統合することをお勧めします。これらのシステムは、セキュリティイベントの割り当て、ルーティング、管理に役立ちます。

詳細については、以下のリソースを参照してください。

- ログ、検出結果、メトリクスを一元的に分析(AWS Well-Architected フレームワーク)

- セキュリティブログの CloudTrail と Amazon Athena を使用してセキュリティ、コンプライアンス、運用アクティビティを分析する AWS
- AWS パートナーポートフォリオで脅威検出および対応サービスを提供する AWS パートナー

CloudTrail ログファイルを含む S3 バケットへの不正アクセスを防ぐ

CloudTrail ログファイルは、デフォルトで Amazon S3 バケットに保存されます。CloudTrail ログファイルを含む Amazon S3 バケットへの不正アクセスを防ぐことが、セキュリティのベストプラクティスです。これにより、これらのログの整合性、完全性、および可用性が維持できます。これは、フォレンジックおよび監査の観点で非常に重要です。CloudTrail ログファイルを含む S3 バケットのデータイベントをログに記録する場合は、そのための CloudTrail 証跡を作成できます。

詳細については、以下のリソースを参照してください。

- S3 バケットへのパブリックアクセスブロック設定の構成 (Amazon S3 ドキュメント)
- CloudTrail 予防的セキュリティのベストプラクティス (CloudTrail ドキュメント)
- 証跡の作成 (CloudTrail ドキュメント)

セキュリティグループまたはネットワーク ACL の変更に関するアラートを設定

Amazon Virtual Private Cloud (Amazon VPC) のセキュリティグループは、関連付けられたリソースに到達できるトラフィックおよびリソースから発信できるトラフィックを制御します。ネットワークアクセスコントロールリスト (ACL) は、VPC のサブネットレベルで特定のインバウンドまたはアウトバウンドのトラフィックを許可または拒否します。これらのリソースは、 AWS 環境でアクセスを管理するために不可欠です。

セキュリティグループまたはネットワーク ACL 設定が変更された場合に通知する Amazon CloudWatch アラームを作成して設定します。このアラームを設定して、セキュリティグループを更新する AWS API コールが実行されるたびにアラートが届くように設定します。また、Amazon EventBridge や AWS Config などのサービスを使用して、これらのタイプのセキュリティイベントに自動で応答することもできます。

詳細については、以下のリソースを参照してください。

- AWS セキュリティブログの Amazon VPC セキュリティグループの変更に関する通知を自動的に元に戻して受信する
- Amazon CloudWatch でのアラームの使用 (CloudWatch ドキュメント)
- AWS Well-Architected フレームワークで実用的なセキュリティイベントを実装する
- AWS Well-Architected フレームワークのイベントへの応答を自動化する

CloudWatch アラームが ALARM 状態になった場合のアラートを設定

CloudWatch では、OK、ALARM、INSUFFICIENT_DATA の状態の間で状態が変わったときに、アラームが実行するアクションを指定できます。アラームアクションの最も一般的なタイプは、Amazon Simple Notification Service (Amazon SNS) トピックにメッセージを送信して、1 人または複数のユーザーに通知することです。アラームを設定して、 AWS Systems Managerで OpsItems またはインシデントを作成することもできます。

モニタリング対象のメトリクスが定義されたしきい値を超えると自動的に警告するアラームアクションを有効にすることをお勧めします。アラームをモニタリングすることで、異常なアクティビティを特定し、セキュリティや運用上の問題に迅速に対応できます。

詳細については、以下のリソースを参照してください。

- AWS Well-Architected フレームワークで実用的なセキュリティイベントを実装する
- CloudWatch ドキュメントのアラームアクション

インフラストラクチャを保護するためのセキュリティコントロールの推奨事項

インフラストラクチャ保護は、セキュリティプログラムの重要な部分です。これには、ネットワークとコンピューティングリソースの保護に役立つコントロール方法論が含まれています。インフラストラクチャ保護の例としては、信頼境界、多層防御アプローチ、セキュリティ強化、パッチ管理、オペレーティングシステムの認証と認可などがあります。詳細については、 AWS 「 Well-Architected フレームワーク」の「インフラストラクチャの保護」を参照してください。このセクションで説明するセキュリティコントロールは、インフラストラクチャ保護のベストプラクティスを実装するのに役立ちます。

このセクションのコントロール:

- CloudFront ディストリビューションのデフォルトのルートオブジェクトを指定
- アプリケーションコードをスキャンして一般的なセキュリティ問題を特定
- 専用 VPC とサブネットを使用してネットワークレイヤーを作成
- 受信トラフィックを認可されたポートのみに制限
- Systems Manager ドキュメントへのパブリックアクセスをブロック
- Lambda 関数へのパブリックアクセスをブロック
- デフォルトセキュリティグループの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
- 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がないかスキャン
- セットアップ AWS WAF
- DDoS 攻撃に対する高度な保護を設定
- 多層防御アプローチを使用してネットワークトラフィックを制御

CloudFront ディストリビューションのデフォルトのルートオブジェクトを指定

Amazon CloudFront は、世界中のデータセンターネットワークを通じて配信することで、ウェブコンテンツの配信を高速化します。これにより、レイテンシーが減少し、パフォーマンスが向上します。デフォルトルートオブジェクトを定義しない場合、ディストリビューションのルートの要求はオ

リジンサーバーに渡されます。Amazon Simple Storage Service (Amazon S3) オリジンを使用している場合、S3 バケット内のコンテンツリストまたはオリジンのプライベートコンテンツのリストが返される場合があります。デフォルトのルートオブジェクトを指定すると、ディストリビューションのコンテンツが公開されなくなります。

詳細については、以下のリソースを参照してください。

- デフォルトのルートオブジェクトを指定する (CloudFront ドキュメント)

アプリケーションコードをスキャンして一般的なセキュリティ問題を特定

AWS Well-Architected フレームワークでは、ライブラリと依存関係に問題や欠陥がないかスキャンすることをお勧めします。ソースコードのスキャンに使用できるソースコード分析ツールは多数あります。例えば、Amazon CodeGuru は、Java アプリケーションや Python アプリケーションの一般的なセキュリティ問題をスキャンし、修正するためのレコメンデーションを提示します。

詳細については、以下のリソースを参照してください。

- CodeGuru ドキュメント
- Source code analysis tools (OWASP Foundation ウェブサイト)
- AWS Well-Architected フレームワークで脆弱性管理を実行する

専用 VPC とサブネットを使用してネットワークレイヤーを作成

AWS Well-Architected フレームワークでは、機密性要件を共有するコンポーネントをレイヤーにグループ化することをお勧めします。これにより、不正アクセスが発生した場合の潜在的な影響範囲が最小限に抑えられます。例えば、インターネットアクセスを必要としないデータベースクラスターは、インターネットとのルートが存在しないように、VPC のプライベートサブネットに配置する必要があります。

AWS は、パブリック到達可能性のテストと特定に役立つ多くのサービスを提供します。例えば、Reachability Analyzer は、VPC 内のソースリソースと送信先リソースとの間の接続性をテストできる設定分析ツールです。また、Network Access Analyzer を使用すると、リソースへの意図しないネットワークアクセスを識別できます。

詳細については、以下のリソースを参照してください。

- AWS Well-Architected フレームワークでネットワークレイヤーを作成する
- Reachability Analyzer のドキュメント
- Network Access Analyzer のドキュメント
- サブネットの作成 (Amazon Virtual Private Cloud (Amazon VPC) ドキュメント)

受信トラフィックを認可されたポートのみに制限

無制限アクセス (`0.0.0.0/0` をソースとする IP アドレスからのトラフィックなど) は、ハッキング、サービス拒否 (DoS) 攻撃、データ損失など、悪意のあるアクティビティのリスクを高めます。セキュリティグループは、 AWS リソースへの入出力ネットワークトラフィックをステートフルにフィルタリングします。セキュリティグループでは、SSH やWindows リモートデスクトッププロトコル (RDP) など、よく知られたポートへの外部からの無制限アクセスを許可しないでください。インバウンドトラフィックについては、セキュリティグループで、認可されたポートに対する TCP または UDP 接続のみを許可します。Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに接続するには、直接 SSH または RDP アクセスではなく、Session Manager または Run Command を使用します。

詳細については、以下のリソースを参照してください。

- セキュリティグループを操作 (Amazon EC2 ドキュメント)
- Amazon VPC ドキュメントのセキュリティグループを使用して AWS リソースへのトラフィックを制御する

Systems Manager ドキュメントへのパブリックアクセスをブロック

ユースケースでパブリック共有を有効にする必要がある場合を除き、 AWS Systems Manager ベストプラクティスでは、Systems Manager ドキュメントのパブリック共有をブロックすることをお勧めします。パブリック共有を行うと、ドキュメントへの意図しないアクセスが発生する場合があります。パブリックな Systems Manager ドキュメントは、アカウント、リソース、および内部プロセスに関する貴重な機密情報を公開する可能性があります。

詳細については、以下のリソースを参照してください。

- 共有 SSM ドキュメントのベストプラクティス (Systems Manager ドキュメント)

- 共有 Systems Manager ドキュメントのアクセス許可を変更する (Systems Manager ドキュメント)

Lambda 関数へのパブリックアクセスをブロック

AWS Lambda は、サーバーのプロビジョニングや管理を行うことなくコードを実行できるコンピューティングサービスです。Lambda 関数は、関数コードへの意図しないアクセスを許可する可能性があるため、パブリックからアクセスできない必要があります。

Lambda 関数に対して、アカウントの外部からのアクセスを拒否するよう、リソースベースのポリシーを設定することをお勧めします。これを実現するには、アクセス許可を削除するか、アクセスを許可するステートメントに `AWS:SourceAccount` 条件を追加します。Lambda 関数のリソースベースのポリシーは、Lambda API または AWS Command Line Interface (AWS CLI) を使用して更新できます。

また、 AWS Security Hub CSPMで、「[Lambda.1] Lambda 関数ポリシーでは、パブリックアクセスを禁止する必要があります」というコントロールを有効にすることをお勧めします。このコントロールは、Lambda 関数のリソースベースのポリシーがパブリックアクセスを禁止していることを検証します。

詳細については、以下のリソースを参照してください。

- Security Hub CSPM ドキュメントの AWS Lambda コントロール
- Lambda でのリソースベースのポリシーの使用 (Lambda ドキュメント)
- Lambda アクションのリソースと条件 (Lambda ドキュメント)

デフォルトセキュリティグループの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

AWS リソースをプロビジョニングするときにカスタムセキュリティグループを関連付けない場合、リソースは VPC のデフォルトのセキュリティグループに関連付けられます。このセキュリティグループのデフォルトルールでは、このセキュリティグループに割り当てられたすべてのリソースからのすべてのインバウンドトラフィックが許可され、すべての IPv4 および IPv6 のアウトバウンドトラフィックが許可されます。これにより、リソースへの意図しないトラフィックが許可されてしまう可能性があります。

AWS では、デフォルトのセキュリティグループを使用しないことをお勧めします。代わりに、特定のリソースまたはリソースのグループごとにカスタムセキュリティグループを作成します。

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、デフォルトのセキュリティグループルールを変更して、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を推奨します。セキュリティグループルールを設定する際は、最小特権の原則に従います。

また、[EC2.2] VPC のデフォルトセキュリティグループを有効にして、Security Hub CSPM でインバウンドまたはアウトバウンドのトラフィック制御を許可しないようにすることをお勧めします。このコントロールは、VPC のデフォルトのセキュリティグループがインバウンドとアウトバウンドのトラフィックを拒否していることを検証します。

詳細については、以下のリソースを参照してください。

- Amazon VPC ドキュメントのセキュリティグループを使用して AWS リソースへのトラフィックを制御する
- VPC のデフォルトセキュリティグループ (Amazon VPC ドキュメント)
- Security Hub CSPM ドキュメントのAmazon EC2 コントロール」

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がないかスキャン

すべてのアカウントで Amazon Inspector を有効にすることをお勧めします。Amazon Inspector は、Amazon EC2 インスタンス、Amazon Elastic Container Registry (Amazon ECR) コンテナイメージ、Lambda 関数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。また、Amazon EC2 インスタンスの詳細な検査もサポートしています。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。Amazon Inspector と Security Hub CSPM の両方がアカウントで設定されている場合、Amazon Inspector はセキュリティ検出結果を Security Hub CSPM に自動的に送信して一元管理します。

詳細については、以下のリソースを参照してください。

- Amazon Inspector を使用したリソースのスキャン (Amazon Inspector ドキュメント)
- Amazon EC2 向け Amazon Inspector Deep inspection (Amazon Inspector ドキュメント)
- AWS セキュリティブログの Amazon Inspector を使用して EC2 AMIs をスキャンする
- AWSでのスケーラブルな脆弱性管理プログラムの構築 (AWS 規範ガイダンス)
- AWS Well-Architected フレームワークでネットワーク保護を自動化する
- AWS Well-Architected フレームワークでコンピューティング保護を自動化する

セットアップ AWS WAF

AWS WAF は、Amazon API Gateway API、Amazon CloudFront ディストリビューション、Application Load Balancer など、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 または HTTPS リクエストをモニタリングおよびブロックするのに役立つウェブアプリケーションファイアウォールです。指定した基準に基づいて、サービスはリクエストされたコンテンツ、HTTP 403 ステータスコード (禁止) 、またはカスタムレスポンスでリクエストに応答します。AWS WAF は、可用性に影響を与えたり、セキュリティを侵害したり、過剰なリソースを消費したりする可能性のある一般的なウェブエクスプロイトからウェブアプリケーションまたは APIs を保護するのに役立ちます。 AWS WAF で を設定し、 AWS マネージドルール、カスタムルール、パートナー統合を組み合わせて AWS アカウント 使用して、アプリケーションレイヤー (レイヤー 7) 攻撃からアプリケーションを保護することを検討してください。

詳細については、以下のリソースを参照してください。

- AWS WAF ドキュメントの「 の開始方法 AWS WAF」
- AWS ウェブサイトの AWS WAF 配信パートナー
- AWS ソリューションライブラリの のセキュリティオートメーション AWS WAF
- AWS Well-Architected フレームワークで検査と保護を実装する

DDoS 攻撃に対する高度な保護を設定

AWS Shield は、ネットワークレイヤー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 リソースに対する分散サービス拒否 (DDoS) 攻撃に対する保護を提供します。このサービスは、 AWS Shield Standard と の 2 つのオプションで利用できます AWS Shield Advanced。Shield Standard は、サポートされている AWS リソースを追加料金なしで自動的に保護します。

Shield Advanced をサブスクライブすることをお勧めします。Shield Advanced は、保護されたリソースに対する DDoS 攻撃の保護を拡張します。Shield Advanced から受ける保護は、アーキテクチャと設定の選択内容によって異なります。次のいずれかが必要なアプリケーションには、Shield Advanced 保護を実装することを検討してください。

- アプリケーションのユーザーに保証された可用性。
- DDoS 攻撃によってアプリケーションが影響を受ける場合における、DDoS 緩和のエキスパートへの迅速なアクセス。

- アプリケーションが DDoS 攻撃の影響を受けている可能性があることの AWS による認識、および攻撃に関する AWS からの通知とセキュリティチームまたはオペレーションチームへのエスカレーション。
- DDoS 攻撃が の使用に影響する場合など、クラウドコストの予測可能性 AWS のサービス。

詳細については、以下のリソースを参照してください。

- AWS Shield Advanced 概要 (Shield ドキュメント)
- Shield ドキュメントのAWS Shield Advanced 保護されたリソース
- Shield ドキュメントの AWS Shield Advanced 機能とオプション
- DDoS イベントへの対応 (Shield ドキュメント)
- AWS Well-Architected フレームワークで検査と保護を実装する

多層防御アプローチを使用してネットワークトラフィックを制御

AWS Network Firewall は、 の仮想プライベートクラウド (VPCs) 用の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および侵入検知および防止サービスです AWS クラウド。これは、VPC の境界に重要なネットワーク保護をデプロイするのに役立ちます。これには、インターネットゲートウェイ、NAT ゲートウェイ、VPN、 AWS Direct Connectを介して送受信されるトラフィックのフィルタリングが含まれます。Network Firewall には、一般的なネットワークの脅威からの保護に役立つ機能が含まれています。Network Firewall のステートフルファイアウォールは、接続やプロトコルなどのトラフィックフローのコンテキストを組み込み、ポリシーを適用できます。

詳細については、以下のリソースを参照してください。

- AWS Network Firewall ドキュメント
- AWS Well-Architected フレームワークのすべてのレイヤーでトラフィックを制御する

データを保護するためのセキュリティコントロールの推奨事項

AWS Well-Architected フレームワークは、データを保護するためのベストプラクティスを、データ分類、保管中のデータの保護、転送中のデータの保護の 3 つのカテゴリにグループ化します。このセクションで説明するセキュリティコントロールは、データ保護に関するベストプラクティスを実装するのに役立ちます。これらの基盤となるベストプラクティスは、クラウドでワークロードを設計する前に実施する必要があります。データの誤処理を防ぎ、組織的、法的、コンプライアンス上の義務を果たすのに役立ちます。このセクションのセキュリティコントロールを使用して、データ保護のベストプラクティスを実装してください。

このセクションのコントロール:

- ワークロードレベルでデータを特定および分類
- 各データ分類レベルのコントロールを確立
- 保管中のデータを暗号化する
- 転送中のデータを暗号化する
- Amazon EBS スナップショットへのパブリックアクセスをブロック
- Amazon RDS スナップショットへのパブリックアクセスをブロック
- Amazon RDS、Amazon Redshift、および AWS DMS リソースへのパブリックアクセスをブロックする
- Amazon S3 バケットへのパブリックアクセスをブロック
- 重要な Amazon S3 バケット内のデータ削除に MFA を必須とする
- VPC に Amazon OpenSearch Service ドメインを設定
- AWS KMS key 削除のアラートを設定する
- へのパブリックアクセスをブロックする AWS KMS keys
- セキュアなプロトコルを使用してロードバランサーのリスナーを設定

ワークロードレベルでデータを特定および分類

データ分類とは、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、分類するプロセスのことです。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。データ分類を行うと、多くの場合、データ重複の頻度を減らせます。これにより、ストレージとバックアップのコストを削減すると共に、検索を高速化できます。

ワークロードが処理しているデータの種類と分類、それに関連するビジネスプロセス、データの保存場所、データの所有者について理解しておくことが推奨されます。データ分類は、ワークロードの所有者が機密データを保存する場所を特定し、そのデータにアクセスして共有する方法を判断するのに役立ちます。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。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、以下のリソースを参照してください。

- AWS ホワイトペーパーのデータ分類
- AWS Well-Architected フレームワークでワークロード内のデータを特定する

各データ分類レベルのコントロールを確立

分類レベルごとにデータ保護コントロールを定義します。例えば、推奨されるコントロールを使用してパブリックに分類されるデータを保護し、追加のコントロールを使用して機密データを保護します。メカニズムとツールを使用して、データに直接アクセスしたり、手動でデータを処理したりする必要性を軽減または排除できます。データの識別と分類を自動化することで、誤分類、誤処理、改ざん、人為的ミスのリスクが軽減されます。

例えば、Amazon Macie を使用して Amazon Simple Storage Service (Amazon S3) バケット内の個人を特定できる情報 (PII) などの機密データをスキャンすることを検討してください。また、Amazon Virtual Private Cloud (Amazon VPC) の VPC フローログを使用して、意図しないデータアクセスを自動的に検出することもできます。

詳細については、以下のリソースを参照してください。

- AWS Well-Architected フレームワークでデータ保護コントロールを定義する
- 識別および分類を自動化する (AWS Well-Architected フレームワーク)
- AWS 規範ガイダンスのAWS プライバシーリファレンスアーキテクチャ (AWS PRA)
- Amazon Macie で機密データを検出 (Macie ドキュメント)
- VPC フローログを使用した IP トラフィックのログ記録 (Amazon VPC ドキュメント)
- for Things ブログの「 を使用して PHI および PII データを検出する一般的な手法 AWS のサービス AWS 」

保管中のデータを暗号化する

保管中のデータとは、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を指します。保管中のデータに対して暗号化と適切なアクセスコントロールを実装することで、不正アクセスのリスクを軽減できます。暗号化とは、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プロセスです。暗号文をプレーンテキストに復号して使用できるようにするには、暗号化キーが必要です。では AWS クラウド、 AWS Key Management Service (AWS KMS) を使用して、データの保護に役立つ暗号化キーを作成および制御できます。

各データ分類レベルのコントロールを確立 で説明されているように、暗号化が必要なデータのタイプを指定するポリシーを作成することをお勧めします。どのデータを暗号化するか、またどのデータをトークン化やハッシュ化など別の手法で保護するかを決定する方法に関する基準を含めてください。

詳細については、以下のリソースを参照してください。

- デフォルトの暗号化の設定 (Amazon S3 ドキュメント)
- 新しい EBS ボリュームとスナップショットコピーに対するデフォルトの暗号化 (Amazon EC2 ドキュメント)
- Amazon Aurora リソースの暗号化 (Amazon Aurora ドキュメント)
- AWS KMSの暗号化の詳細の概要 (AWS KMS ドキュメント)
- Creating an enterprise encryption strategy for data at rest (AWS 規範ガイダンス)
- AWS Well-Architected フレームワークで保管時の暗号化を適用する
- 特定の での暗号化の詳細については AWS のサービス、そのサービスのAWS ドキュメントを参照してください。

転送中のデータを暗号化する

転送中のデータとは、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のことです。転送中のデータはすべて、安全な TLS プロトコルと暗号スイートを使用して暗号化します。データへの不正なアクセスを防止するためには、リソースとインターネット間のネットワークトラフィックを暗号化する必要があります。可能であれば、TLS を使用して内部 AWS 環境内のネットワークトラフィックを暗号化します。

詳細については、以下のリソースを参照してください。

- ビューワーと CloudFront の間の通信に HTTPS を要求する (Amazon CloudFront ドキュメント)
- AWS PrivateLink ドキュメント
- AWS Well-Architected フレームワークで転送中の暗号化を強制する
- 特定の での暗号化の詳細については AWS のサービス、そのサービスのAWS ドキュメントを参照してください。

Amazon EBS スナップショットへのパブリックアクセスをブロック

Amazon Elastic Block Store (Amazon EBS) は、 Amazon Elastic Compute Cloud (Amazon EC2) インスタンスで使用するブロックレベルストレージのボリュームを提供します。ポイントインタイムスナップショットを作成することで、Amazon EBSボリュームのデータを Amazon S3 にバックアップできます。スナップショットは、他のすべての とパブリックに共有することも AWS アカウント、AWS アカウント 指定した個人とプライベートに共有することもできます。

Amazon EBS スナップショットはパブリックに共有しないことをお勧めします。これは、誤って機密データが公開されるおそれがあるためです。スナップショットを共有すると、スナップショットのデータに他人がアクセスできるようになります。スナップショットは、そのすべてのデータを信頼して共有できる人とのみ共有してください。

詳細については、以下のリソースを参照してください。

- スナップショットの共有 (Amazon EC2 ドキュメント)
- Amazon EBS スナップショットはパブリックに復元できないようにすることをお勧めします (AWS Security Hub CSPM ドキュメント)
- ebs-snapshot-public-restorable-check (AWS Config ドキュメント)

Amazon RDS スナップショットへのパブリックアクセスをブロック

Amazon Relational Database Service (Amazon RDS) を使用すると、 AWS クラウドでリレーショナルデータベースをセットアップ、運用、スケーリングできます。Amazon RDS は、DB インスタンスのバックアップウィンドウ中に、DB インスタンスまたはマルチ AZ DB クラスターの自動バックアップを作成して保存します。Amazon RDS は DB インスタンスのストレージボリュームのスナップショットを作成し、個々のデータベースだけではなく、その DB インスタンス全体をバックアップ

します。手動スナップショットは、スナップショットをコピーしたり、そこから DB インスタンスを復元したりするために共有できます。

スナップショットをパブリックとして共有する場合は、スナップショット内のデータがプライベートでも機密でもないことを確認してください。スナップショットがパブリックに共有されると、すべての AWS アカウント にデータへのアクセス権が付与されます。これにより、Amazon RDS インスタンスのデータが意図せず漏えいしてしまうおそれがあります。

詳細については、以下のリソースを参照してください。

- DB スナップショットを共有する (Amazon RDS ドキュメント)
- AWS Config rdrds-snapshots-public-prohibited ドキュメント
- RDS スナップショットは Security Hub CSPM ドキュメントのプライベートである必要があります

Amazon RDS、Amazon Redshift、および AWS DMS リソースへのパブリックアクセスをブロックする

Amazon RDS DB インスタンス、Amazon Redshift クラスター、および AWS Database Migration Service (AWS DMS) レプリケーションインスタンスをパブリックにアクセス可能に設定できます。`publiclyAccessible` フィールド値が `true` の場合、これらのリソースはパブリックにアクセスできます。パブリックアクセスを許可すると、不要なトラフィック、露出、データ漏えいが発生するおそれがあります。これらのリソースへのパブリックアクセスを許可しないことをお勧めします。

Amazon RDS DB インスタンス、 AWS DMS レプリケーションインスタンス、または Amazon Redshift クラスターがパブリックアクセスを許可するかどうかを検出するには、 AWS Config ルールまたは Security Hub CSPM コントロールを有効にすることをお勧めします。

> **Note**
>
> レ AWS DMS プリケーションインスタンスのパブリックアクセス設定は、インスタンスのプロビジョニング後に変更することはできません。パブリックアクセス設定を変更するには、現在のインスタンスを削除してから再作成します。再作成する際は、[パブリックアクセス可能] オプションを選択しないでください。

詳細については、以下のリソースを参照してください。

- Security AWS DMS Hub CSPM ドキュメントでレプリケーションインスタンスを公開しないでください
- RDS DB インスタンスは、Security Hub CSPM ドキュメントでパブリックアクセスを禁止する必要があります
- Amazon Redshift クラスターは、Security Hub CSPM ドキュメントのパブリックアクセスを禁止する必要があります
- AWS Config ドキュメントの rds-instance-public-access-check
- AWS Config ドキュメントの「dms-replication-not-public」
- redshift-cluster-public-access-check (AWS Config ドキュメント)
- Amazon RDS DB インスタンスを変更する (Amazon RDS ドキュメント)
- クラスターの変更 (Amazon Redshift ドキュメント)

Amazon S3 バケットへのパブリックアクセスをブロック

Amazon S3 バケットへのパブリックアクセスを不可にすることが、Amazon S3 セキュリティのベストプラクティスです。インターネット上のだれもがバケットを読み書きできる必要が明確にない限り、バケットがパブリックではないことを確認する必要があります。これにより、データの整合性とセキュリティが保護されます。 AWS Config ルールと Security Hub CSPM コントロールを使用して、Amazon S3 バケットがこのベストプラクティスに準拠していることを確認することができます。

詳細については、以下のリソースを参照してください。

- Amazon S3 のセキュリティベストプラクティス (Amazon S3 ドキュメント)
- Security Hub CSPM ドキュメントで S3 パブリックアクセスブロック設定を有効にする必要があります
- S3 バケットは、Security Hub CSPM ドキュメントのパブリック読み取りアクセスを禁止する必要があります
- S3 バケットは、Security Hub CSPM ドキュメントのパブリック書き込みアクセスを禁止する必要があります
- s3-bucket-public-read-prohibited ルール (AWS Config ドキュメント)
- AWS Config ドキュメントで禁止されている s3-bucket-public-write-prohibited

重要な Amazon S3 バケット内のデータ削除に MFA を必須とする

Amazon S3 バケットで S3 バージョニングを行うときに、MFA (多要素認証) Delete が有効になるようにバケットを設定すれば、セキュリティをさらに強化できます。この設定を行うと、バケット所有者は、特定のバージョンを削除したりバケットのバージョニング状態を変更したりするリクエストに、2 つの認証形式を含めることが必要になります。組織にとって重要なデータを含むバケットに対して、この機能を有効にすることをお勧めします。これにより、バケットやデータの誤削除を防ぐことができます。

詳細については、以下のリソースを参照してください。

- MFA 削除の設定 (Amazon S3 ドキュメント)

VPC に Amazon OpenSearch Service ドメインを設定

Amazon OpenSearch Service は、 AWS クラウドにおける OpenSearch クラスターのデプロイ、オペレーション、スケーリングを支援するマネージドサービスです。Amazon OpenSearch Service は、OpenSearch とレガシー Elasticsearch オープンソースソフトウェア (OSS) をサポートしています。VPC 内にデプロイされた Amazon OpenSearch Service ドメインは、パブリックインターネットを経由することなく、プライベート AWS ネットワーク経由で VPC リソースと通信できます。この設定により、転送中のデータへのアクセスが制限されるため、セキュリティ体制が向上します。Amazon OpenSearch Service ドメインをパブリックサブネットにアタッチしないこと、および VPC をベストプラクティスに従って設定することをお勧めします。

詳細については、以下のリソースを参照してください。

- VPC 内で Amazon OpenSearch Service ドメインを起動する (Amazon OpenSearch Service デベロッパーガイド)
- AWS Config ドキュメントの opensearch-in-vpc-only
- OpenSearch ドメインは Security Hub CSPM ドキュメントの VPC にある必要があります

AWS KMS key 削除のアラートを設定する

AWS Key Management Service (AWS KMS) キーは、削除後に復元することはできません。KMS キーが削除されると、KMS キーで暗号化されたデータは永久に復元できません。データへのアクセスを保持する必要がある場合は、キーを削除する前に、データを復号するか、新しい KMS キーで再

暗号化する必要があります。KMS キーの削除は、そのキーをもう使用しないことが確実である場合にのみ行ってください。

KMS キーの削除が開始された場合に通知を受け取れるよう、Amazon CloudWatch アラームを設定することをお勧めします。KMS キーの削除は破壊的で潜在的に危険であるため、 AWS KMS では待機期間を設定し、7～30 日以内に削除をスケジュールする必要があります。このため、スケジュールされた削除を確認し、必要に応じてキャンセルすることができます。

詳細については、以下のリソースを参照してください。

- キー削除のスケジュールとキャンセル (AWS KMS ドキュメント)
- AWS KMS ドキュメントの削除保留中の KMS キーの使用を検出するアラームの作成
- Security Hub CSPM ドキュメントでAWS KMS keys 意図せずに削除しないでください

へのパブリックアクセスをブロックする AWS KMS keys

キーポリシーは、 AWS KMS keysへのアクセスを制御するための主な方法です。すべての KMS キーには、厳密に 1 つのキーポリシーが必要です。KMS キーへの匿名アクセスを許可すると、機密データの漏洩につながる可能性があります。パブリックにアクセス可能な KMS キーを特定し、これらのリソースに対する署名されていないリクエストが行われないように、アクセスポリシーを更新することをお勧めします。

詳細については、以下のリソースを参照してください。

- AWS KMS ドキュメントの のセキュリティのベストプラクティス AWS Key Management Service
- AWS KMS ドキュメントのキーポリシーの変更
- AWS KMS ドキュメントの へのアクセスの確認 AWS KMS keys

セキュアなプロトコルを使用してロードバランサーのリスナーを設定

Elastic Load Balancing は、受信アプリケーショントラフィックを複数のターゲットに自動的に分散します。1 つ以上のリスナーを指定することで、受信トラフィックを受け入れるようにロードバランサーを設定します。リスナーとは、設定したプロトコルとポートを使用して接続リクエストをチェックするプロセスです。各タイプのロードバランサーは、以下のようにサポートするプロトコルとポートが異なります。

- Application Load Balancer はアプリケーションレイヤーでルーティングを決定し、HTTP または HTTPS プロトコルを使用します。
- Network Load Balancer はトランスポートレイヤーでルーティングを決定し、TCP、TLS、UDP、または TCP_UDP プロトコルを使用します。
- Classic Load Balancer は、トランスポートレイヤー (TCP または SSL プロトコルを使用) またはアプリケーションレイヤー (HTTP または HTTPS プロトコルを使用) でルーティングを決定します。

常に HTTPS または TLS プロトコルを使用することをお勧めします。これらのプロトコルにより、クライアントとターゲット間のトラフィックの暗号化および復号化をロードバランサーが担当することが保証されます。

詳細については、以下のリソースを参照してください。

- Application Load Balancer のリスナー (Elastic Load Balancing のドキュメント)
- Listeners for your Classic Load Balancer (Elastic Load Balancing ドキュメント)
- Network Load Balancer のリスナー (Elastic Load Balancing ドキュメント)
- AWS 規範ガイダンスでAWS ロードバランサーが安全なリスナープロトコルを使用していることを確認する
- AWS Config ドキュメントの「elb-tls-https-listeners-only」
- Classic Load Balancer リスナーは、Security Hub CSPM ドキュメントの HTTPS または TLS 終了で設定する必要があります
- Application Load Balancer は、Security Hub CSPM ドキュメントのすべての 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。

インシデント対応に関するセキュリティ推奨事項

組織でセキュリティイベントが発生した場合、ユーザーは問題に対処できるよう準備しておく必要があります。すべてのユーザーは、組織のセキュリティ対応プロセスの基本を理解している必要があります。インシデント対応プログラムを成功させるには、計画、トレーニング、経験が不可欠です。潜在的なセキュリティイベントが発生する前に、組織としての準備を整えておくことが理想です。AWS Well-Architected フレームワークは、クラウドでのインシデント対応プログラムを成功させるために必要な、準備、運用、インシデント後のアクティビティの 3 つの基盤を特定します。詳細については、「 Well-Architected フレームワーク」の AWS 「インシデント対応の側面」を参照してください。 AWS

イベントについて通知したりイベントに自動的に応答したりするセキュリティコントロールを除き、インシデント対応のために設定できるコントロールは限られています。強固なインシデント対応体制は、主に組織で使用する計画、プロセス、ランブック、プレイブック、トレーニングプログラムを通じて確立されます。このセクションのコントロールと推奨事項を使用することで、インシデント対応プログラムのベストプラクティスを実装できます。インシデント対応のベストプラクティスと実装ガイダンスの詳細については、 AWS 「 Well-Architected フレームワーク」の「インシデント対応」を参照してください。

このセクションの推奨事項:

- インシデント対応計画を定義
- インシデント対応のランブックとプレイブックの作成と保守
- イベント駆動型セキュリティオートメーションを実装
- 運用チームが と連携する方法を文書化する サポート
- セキュリティイベントのアラートを設定

インシデント対応計画を定義

明確に定義されたインシデント対応計画 (IRP) を確立します。インシデント対応計画は、インシデント対応プログラムの基礎となるように設計されています。この計画は、各組織のニーズに合わせてカスタマイズする必要があります。

詳細については、以下のリソースを参照してください。

- インシデント対応計画を作成してテストする (AWS Security Incident Response ガイド)

- AWS Well-Architected フレームワークでインシデント管理計画を作成する
- 重要な人員と外部リソースを特定する (AWS Well-Architected フレームワーク)

インシデント対応のランブックとプレイブックの作成と保守

インシデント対応プロセスを準備する上で重要なのは、プレイブックを作成することです。インシデント対応プレイブックには、セキュリティイベントが発生したときに従うべき一連の手順が記載されています。明確な体制と手順があると、対応が簡単になり、人為的ミスの可能性が低くなります。

詳細については、以下のリソースを参照してください。

- プレイブックの作成対象 (AWS Security Incident Response ガイド)
- でのAWS インシデント対応プレイブックのサンプル GitHub
- セキュリティインシデント対応プレイブックを作成し、テストする (AWS Well-Architected フレームワーク)

イベント駆動型セキュリティオートメーションを実装

セキュリティレスポンスの自動化とは、セキュリティイベントに自動的に応答または修正するように設計された、事前定義されプログラムされたアクションのことです。こうした自動化は、検出またはレスポンシブのセキュリティコントロールとして機能し、 AWS セキュリティのベストプラクティス実装に役立ちます。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。

多くの は自動応答 AWS のサービス をサポートしています。例えば、特定のメトリクスに対して Amazon CloudWatch アラームを設定し、アラームの状態が変化した際にアクションを開始するようにできます。Amazon EventBridge を使用して、 および Amazon Inspector の検出結果の自動応答 AWS Security Hub CSPM と修復を設定することもできます。

詳細については、以下のリソースを参照してください。

- Remediate Amazon Inspector security findings automatically (AWS Security Blog)
- セキュリティブログの でセキュリティレスポンスの自動化を開始する AWS AWS
- AWS ソリューションライブラリの でのセキュリティ自動応答 AWS
- Amazon CloudWatch でのアラームの使用 (CloudWatch ドキュメント)
- Security Hub CSPM ドキュメントの「自動応答と修復」

- Amazon EventBridge を使用して Amazon Inspector の検出結果に対するカスタムレスポンスを作成する (Amazon Inspector ドキュメント)

運用チームが と連携する方法を文書化する サポート

では AWS アカウント、プライマリ連絡先と 3 つの代替連絡先を定義できます。各 AWS アカウントまたは組織のセキュリティ連絡先を指定することをお勧めします。

AWS サポート は、 AWS ソリューションの成功と運用の健全性をサポートできるツールと専門知識へのアクセスを提供するさまざまなプランを提供します。また、組織が サポート プラン AWS Managed Services の代わりに を使用することのメリットがあるかどうかを検討してください。AWS Managed Services (AMS) は、モニタリング、インシデント管理、セキュリティガイダンス、パッチサポート、 AWS ワークロードのバックアップなど、 AWS インフラストラクチャを継続的に管理することで、より効率的かつ安全に運用するのに役立ちます。AMS サポートモデルは、クラウド運用チームのリソースが限られている組織に適しています。これらのモデルと計画を比較して、組織のユースケースとクラウド成熟度レベルに最適なものを選択することをお勧めします。

詳細については、以下のリソースを参照してください。

- AWS 「 セキュリティインシデント対応ガイド」の「対応チームとサポート」を理解する AWS
- AWS アカウントの代替連絡先の更新 (AWS アカウント管理ガイド)
- AWS ウェブサイトで計画を比較する サポート
- AWS 規範ガイダンスの目標ビジネス成果を達成するために AWS Managed Services を使用する戦略

セキュリティイベントのアラートを設定

異常の検出は、その異常を制御するために実装される対策と同じくらい重要です。アラートは、検出フェーズの主要コンポーネントです。目的の AWS アカウント アクティビティに基づいてインシデント対応プロセスを開始する通知を生成します。アラートには、チームが対応するための関連情報が含まれるようにしてください。

詳細については、以下のリソースを参照してください。

- 検出 (AWS Security Incident Response ガイド)
- AWS Well-Architected フレームワークでフォレンジック機能を準備する
- AWS Well-Architected フレームワークで実用的なセキュリティイベントを実装する

次のステップ

クラウドジャーニーを進める際は、これらの文書化されたコントロール、ガイダンス、修復オプションを適用することが重要です。これらの推奨事項を取り入れることで、AWS クラウド におけるクラウドセキュリティ体制の改善につながり、AWS の責任共有モデルで定義されているセキュリティ上の責任を果たすのに役立ちます。

次のステップとして、以下を推奨します。

- ベストプラクティスと実装ガイダンスの詳細については、「AWS Well-Architected フレームワーク」の 6 つの柱を参照してください。
- 組織が使用する AWS のサービスについては、使用可能なAWS Security Hub CSPM コントロールのリストを確認し、環境でこれらのコントロールのいずれかを有効にする必要があるかどうかを評価してください。
- 組織が使用する AWS のサービスについては、使用可能なAWS Configマネージドルールのリストを確認し、環境でこれらのルールのいずれかを有効にする必要があるかどうかを評価してください。

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
ルートユーザーの MFA	推奨事項を更新し、ルートユーザーの MFA セクションで詳細情報を提供しました。	2023 年 11 月 9 日
初版発行	—	2023 年 10 月 27 日

AWS 規範ガイダンスの用語集

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

数字

7 Rs

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

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

A

ABAC

「属性ベースのアクセス制御」をご覧ください。

抽象化されたサービス

「マネージドユーザー」をご覧ください。

ACID

「原子性、一貫性、分離性、耐久性 (ACID)」をご覧ください。

アクティブ/アクティブ移行

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

アクティブ/パッシブ移行

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

集計関数

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

AI

「人工知能」をご覧ください。

AIOps

「AI オペレーション」をご覧ください。

匿名化

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

アンチパターン

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

アプリケーション制御

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

アプリケーションポートフォリオ

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

人工知能 (AI)

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

AI オペレーション (AIOps)

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

非対称暗号化

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

原子性、一貫性、分離性、耐久性 (ACID)

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

属性ベースのアクセス制御 (ABAC)

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

信頼できるデータソース

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

アベイラビリティーゾーン (AZ)

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

AWS クラウド導入フレームワーク (AWS CAF)

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

AWS ワークロード認定フレームワーク (AWS WQF)

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

B

不正なボット

個人や組織に混乱や損害を与えることを目的としたボット。

BCP

「ビジネス継続性計画 (BCP)」をご覧ください。

動作グラフ

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

ビッグエンディアンシステム

最上位バイトを最初に格納するシステム。「エンディアン性」もご覧ください。

二項分類

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

ブルームフィルター

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

ブルー/グリーンデプロイ

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

ボット

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

ボットネット

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

ブランチ

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

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

ブレークグラスアクセス

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

ブラウンフィールド戦略

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

バッファキャッシュ

アクセス頻度が最も高いデータが保存されるメモリ領域。

ビジネス能力

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

ビジネス継続性計画 (BCP)

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

C

CAF

「AWS クラウド導入フレームワーク」を参照してください

カナリアデプロイ

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

CCoE

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

CDC

「変更データキャプチャ」を参照してください。

変更データキャプチャ (CDC)

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

カオスエンジニアリング

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

CI/CD

「継続的インテグレーションと継続的デリバリー」を参照してください。

分類

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

クライアント側の暗号化

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

Cloud Center of Excellence (CCoE)

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

クラウドコンピューティング

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

クラウド運用モデル

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

導入のクラウドステージ

組織が、 AWS クラウドへの移行時に通常実行する 4 つの段階。

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

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

CMDB

「構成管理データベース (CMDB)」を参照してください。

コードリポジトリ

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

コールドキャッシュ

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

コールドデータ

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

コンピュータビジョン (CV)

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

設定ドリフト

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

構成管理データベース (CMDB)

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

コンフォーマンスパック

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

継続的インテグレーションと継続的デリバリー (CI/CD)

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

CV

「コンピュータビジョン」を参照してください。

D

保管中のデータ

ストレージ内にあるデータなど、常に自社のネットワーク内にあるデータ。

データ分類

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

データドリフト

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

転送中のデータ

ネットワーク内 (ネットワークリソース間など) を活発に移動するデータ。

データメッシュ

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

データ最小化

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

データ境界

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

データの前処理

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

データ出所

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

データ件名

データを収集、処理している個人。

データウェアハウス

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

データベース定義言語 (DDL)

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

データベース操作言語 (DML)

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

DDL

「データベース定義言語」を参照してください。

ディープアンサンブル

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

深層学習

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

多層防御

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

委任管理者

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

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

トラブルシューティング

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

開発環境

「環境」を参照してください。

検出管理

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

開発バリューストリームマッピング (DVSM)

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

デジタルツイン

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

ディメンションテーブル

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

ディザスタ

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

ディザスタリカバリ (DR)

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

DML

「データベース操作言語」を参照してください。

ドメイン駆動型設計

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

DR

「ディザスタリカバリ」を参照してください。

ドリフト検出

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

DVSM

「開発バリューストリームマッピング」を参照してください。

E

EDA

「探索的データ分析」を参照してください。

EDI

「電子データ交換」を参照してください。

エッジコンピューティング

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

電子データ交換 (EDI)

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

暗号化

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

暗号化キー

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

エンディアン

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

エンドポイント

「サービスエンドポイント」を参照してください。

エンドポイントサービス

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

エンタープライズリソースプランニング (ERP)

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

エンベロープ暗号化

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

環境

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

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

エピック

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

ERP

「エンタープライズリソース計画」を参照してください。

探索的データ分析 (EDA)

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

F

ファクトテーブル

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

フェイルファスト

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

障害分離境界

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

機能ブランチ

「ブランチ」を参照してください。

特徴量

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

特徴量重要度

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

機能変換

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

数ショットプロンプト

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

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

FGAC

「きめ細かなアクセス制御」を参照してください。

きめ細かなアクセス制御 (FGAC)

複数の条件を使用してアクセス要求を許可または拒否すること。

フラッシュカット移行

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

FM

「基盤モデル」を参照してください。

基盤モデル (FM)

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

G

生成 AI

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

ジオブロッキング

「地理的制限」を参照してください。

地理的制限 (ジオブロッキング)

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

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

Gitflow ワークフロー

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

ゴールデンイメージ

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

グリーンフィールド戦略

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

ガードレール

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

H

HA

「高可用性」を参照してください。

異種混在データベースの移行

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

高可用性 (HA)

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

ヒストリアンのモダナイゼーション

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

ホールドアウトデータ

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

同種データベースの移行

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

ホットデータ

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

ホットフィックス

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

ハイパーケア期間

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

I

IaC

「Infrastructure as Code」を参照してください。

ID ベースのポリシー

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

アイドル状態のアプリケーション

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

IIoT

「インダストリアル IoT」を参照してください。

イミュータブルインフラストラクチャ

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

インバウンド (受信) VPC

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

増分移行

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

インダストリー 4.0

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

インフラストラクチャ

アプリケーションの環境に含まれるすべてのリソースとアセット。

Infrastructure as Code (IaC)

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

インダストリアル IoT (IIoT)

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

インスペクション VPC

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

IoT

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

解釈可能性

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

IoT

「IoT」を参照してください。

IT 情報ライブラリ (ITIL)

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

IT サービス管理 (ITSM)

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

ITIL

「IT 情報ライブラリ」を参照してください。

ITSM

「IT サービス管理」を参照してください。

L

ラベルベースアクセス制御 (LBAC)

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

ランディングゾーン

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

大規模言語モデル (LLM)

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

大規模な移行

300 台以上のサーバの移行。

LBAC

「ラベルベースアクセス制御」を参照してください。

最小特権

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

リフトアンドシフト

「7 Rs」を参照してください。

リトルエンディアンシステム

最下位バイトを最初に格納するシステム。「エンディアン性」もご覧ください。

LLM

「大規模言語モデル」を参照してください。

下位環境

「環境」を参照してください。

M

機械学習 (ML)

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

メインブランチ

「ブランチ」を参照してください。

マルウェア

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

マネージドサービス

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

製造実行システム (MES)

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

MAP

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

メカニズム

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

メンバーアカウント

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

MES

「製造実行システム」を参照してください。

Message Queuing Telemetry Transport (MQTT)

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

マイクロサービス

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

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

マイクロサービスアーキテクチャ

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

Migration Acceleration Program (MAP)

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

大規模な移行

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

移行ファクトリー

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

移行メタデータ

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

移行パターン

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

Migration Portfolio Assessment (MPA)

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

移行準備状況評価 (MRA)

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

移行戦略

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

ML

「機械学習」を参照してください。

モダナイゼーション

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

モダナイゼーション準備状況評価

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

モノリシックアプリケーション (モノリス)

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

MPA

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

MQTT

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

多クラス分類

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

ミュータブルなインフラストラクチャ

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

O

OAC

「オリジンアクセス制御」を参照してください。

OAI

「オリジンアクセスアイデンティティ」を参照してください。

OCM

「組織変更管理」を参照してください。

オフライン移行

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

OI

「オペレーション統合」を参照してください。

Ola

「オペレーショナルレベルアグリーメント」を参照してください。

オンライン移行

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

OPC-UA

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

Open Process Communications - Unified Architecture (OPC-UA)

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

オペレーショナルレベルアグリーメント (OLA)

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

運用準備状況レビュー (ORR)

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

運用テクノロジー (OT)

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

オペレーション統合 (OI)

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

組織の証跡

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

組織変更管理 (OCM)

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

オリジンアクセス制御 (OAC)

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

オリジンアクセスアイデンティティ (OAI)

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

ORR

「運用準備状況レビュー」を参照してください。

OT

「運用テクノロジー」を参照してください。

アウトバウンド (送信) VPC

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

P

アクセス許可の境界

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

個人を特定できる情報 (PII)

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

PII

「個人を特定できる情報」を参照してください。

プレイブック

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

PLC

「プログラマブルロジックコントローラー」を参照してください。

PLM

「製品ライフサイクル管理」を参照してください。

ポリシー

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

多言語の永続性

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

ポートフォリオ評価

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

述語

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

述語プッシュダウン

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

予防的コントロール

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

プリンシパル

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

プライバシーバイデザイン

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

プライベートホストゾーン

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

プロアクティブコントロール

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

製品ライフサイクル管理 (PLM)

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

本番環境

「環境」を参照してください。

プログラマブルロジックコントローラー (PLC)

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

プロンプトチェイニング

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

仮名化

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

発行/サブスクライブ (pub/sub)

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

Q

クエリプラン

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

クエリプランのリグレッション

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

R

RACI マトリックス

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

RAG

「検索拡張生成」を参照してください。

ランサムウェア

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

RASCI マトリックス

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

RCAC

「行と列のアクセス制御」を参照してください。

リードレプリカ

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

リアーキテクト

「7 Rs」を参照してください。

目標復旧時点 (RPO)

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

目標復旧時間 (RTO)

サービスの中断から復旧までの最大許容遅延時間。

リファクタリング

「7 Rs」を参照してください。

リージョン

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

リグレッション

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

リホスト

「7 Rs」を参照してください。

リリース

デプロイプロセスで、変更を本番環境に昇格させること。

再配置

「7 Rs」を参照してください。

リプラットフォーム

「7 Rs」を参照してください。

再購入

「7 Rs」を参照してください。

回復性

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

リソースベースのポリシー

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

実行責任者、説明責任者、協業先、報告先 (RACI) に基づくマトリックス

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

レスポンシブコントロール

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

保持

「7 Rs」を参照してください。

廃止

「7 Rs」を参照してください。

検索拡張生成 (RAG)

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

ローテーション

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

行と列のアクセス制御 (RCAC)

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

RPO

「目標復旧時点」を参照してください。

RTO

「目標復旧時間」を参照してください。

ランブック

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

S

SAML 2.0

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

SCADA

「監視制御とデータ取得」を参照してください。

SCP

「サービスコントロールポリシー」を参照してください。

シークレット

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

セキュリティバイデザイン

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

セキュリティコントロール

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

セキュリティ強化

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

Security Information and Event Management (SIEM) システム

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

セキュリティレスポンスの自動化

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

サーバー側の暗号化

送信先で、それ AWS のサービス を受け取る によるデータの暗号化。

サービスコントロールポリシー (SCP)

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

サービスエンドポイント

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

サービスレベルアグリーメント (SLA)

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

サービスレベルインジケータ (SLI)

エラー率、可用性、スループットといった、サービスパフォーマンス面の指標。

サービスレベル目標 (SLO)

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

責任共有モデル

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

SIEM

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

単一障害点 (SPOF)

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

SLA

「サービスレベルアグリーメント」を参照してください。

SLI

「サービスレベルインジケータ」を参照してください。

SLO

「サービスレベルの目標」を参照してください。

スプリットアンドシードモデル

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

SPOF

「単一障害点」を参照してください。

スタースキーマ

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

strangler fig パターン

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

サブネット

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

監視制御とデータ取得 (SCADA)

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

対称暗号化

データの暗号化と復号に同じキーを使用する暗号化のアルゴリズム。

合成テスト

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

システムプロンプト

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

T

タグ

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

ターゲット変数

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

タスクリスト

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

テスト環境

「環境」を参照してください。

トレーニング

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

トランジットゲートウェイ

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

トランクベースのワークフロー

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

信頼されたアクセス

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

チューニング

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

ツーピザチーム

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

U

不確実性

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

未分化なタスク

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

上位環境

「環境」を参照してください。

V

バキューミング

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

バージョンコントロール

リポジトリ内のソースコードへの変更など、変更を追跡するプロセスとツール。

VPC ピアリング

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

脆弱性

システムのセキュリティを脅かすソフトウェアまたはハードウェアの欠陥。

W

ウォームキャッシュ

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

ウォームデータ

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

ウィンドウ関数

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

ワークロード

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

ワークストリーム

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

WORM

「Write-Once-Read-Many」を参照してください。

WQF

「AWS ワークロード資格フレームワーク」を参照してください

Write-Once-Read-Many (WORM)

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

Z

ゼロデイエクスプロイト

ゼロデイ脆弱性を悪用した攻撃 (一般的にマルウェアによる)。

ゼロデイ脆弱性

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

ゼロショットプロンプト

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

ゾンビアプリケーション

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

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