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

R™ Singla and 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、 のセキュリティ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。

AWS Cloud Adoption Framework (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 – 人間とマシンの 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。データの可視性と制御、および組織内でのデータへのアクセスと使用方法を維持します。
- 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、および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、組織が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 によって公開されたその他のセキュリティレコメンデーションに合致し、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を置き換えることを意図した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) ポリシーを使用して、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。効果的な ID とアクセスの管理は、適切な人材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検証するのに役立ちます。 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 プロバイダーへの依存や、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。このセクションの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の実装に役立ちます。

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のモニタリングと設定
- 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 を有効にする
- 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する
- 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する
- IAM アクセスキーを定期的にローテーションする
- 外部エンティティと共有されているリソースを特定する

ルートユーザーアクティビティの通知のモニタリングと設定

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。デフォルトでは、ルートユーザーはアカウント内のすべての AWS のサービス およびリソースへのフルアクセスが許可されます。ルートユーザーを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
- 規範的ガイダンスで 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 AWS

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。および リソースにアクセス AWS アカウント するための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はドキュメントに存在してはいけません AWS Security Hub
- IAM ドキュメントのルートユーザーのアクセスキーの削除
- IAM ドキュメントの IAM ロール

ルートユーザーの MFA を有効にする

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、 のセキュリティバー AWS アカウント 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アクションを実行できる権限の高いユーザーであるため、ルートユーザーに MFA を要求することが重要です。時間ベースのワンタイムパスワード (TOTP) アルゴリズム、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 デバイスを使用できます。

2024 年、MFA は 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、ハードウェア購入の承認または配信を待っている間に使用できます。

で何百も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 を使用することはスケーラブルではない場合があります。この場合、OU 管理アカウントとして機能する OU 内の 1 つのアカウントを選択し、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。クロスアカウントアクセスを事前に設定することで、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

スできます。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 を使用した 間のアクセスの委任」を参照してください。

ルートユーザー認証情報用に複数の MFA デバイスを有効にすることをお勧めします。任意の組み合わせで最大 8 台の MFA デバイスを登録できます。

詳細については、以下のリソースを参照してください。

- IAM ドキュメントのハードウェア TOTP トークンの有効化
- IAM ドキュメントの仮想多要素認証 (MFA) デバイスを有効にする
- IAM ドキュメントの FIDO セキュリティキーの有効化
- IAM ドキュメントの「多要素認証 (MFA) を使用してルートユーザーのサインインを保護する」

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とアクセス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 の要求、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 ドキュメントの「IAM におけるセキュリティのベストプラクティス」
- 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する

最小特権とは、タスクの実行に必要なアクセス許可のみを付与する手法です。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コントロール (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、アイデンティティ、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、大規模な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、開発者グループが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アクセスすることを許可できます。

詳細については、以下のリソースを参照してください。

- IAM ドキュメントで最小特権のアクセス許可を適用する
- IAM ドキュメントの「 の ABAC とは AWS」

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する

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、マルチアカウント戦略を使用するのがベストプラクティスです。 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 で組織として管理されAWS Organizations、アカウントは組織単位 (OUs) にグループ化されます。

AWS のサービスなどの AWS Control Towerは、組織全体のコントロールを一元管理するのに役立ちます。組織内のアカウントまたは OU ごと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、イベントの発生後に検出、ログ記録、アラート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、プロビジョニング前にリソースをスキャンして、非準拠の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 規範ガイダンスのAWS 「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する

長期的な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ことをお勧めします。アクセスキーは 90 日以内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と、侵害されたアカウントまたは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軽減されます。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するこ

とで、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後は、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。

- IAM ドキュメントの長期的な認証情報を必要とするユースケースで、必要に応じてアクセスキーを更新する
- 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
- IAM ドキュメントのアクセスキーの更新

外部エンティティと共有されているリソースを特定する

外部エンティティとは、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。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、組織やアカウント内のリソースを特定することは、セキュリティのベストプラクティスです。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 ドキュメントの「IAM Access Analyzer を使用して リソースへのパブリックアクセスとクロスアカウントアクセスを検証する」
- 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
- IAM ドキュメントの の使用 AWS Identity and Access Management Access Analyzer

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設定ミス、脅威、予期しない動作を理解して特定できます。潜在的な脅威を理解することは、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する
- サービスとアプリケーションレベルでログ記録を設定する
- 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する
- 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止する
- セキュリティグループまたはネットワーク ACLs の変更に関するアラートを設定する
- ALARM 状態に入る CloudWatch アラームのアラートを設定する

CloudTrail で少なくとも 1 つのマルチリージョン証跡を設定する

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 Management Console、 AWS SDKs および APIs。このイベント履歴は、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に役立ちます。

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 でイベントを記録するように設定する必要があります AWS リージョン。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確実に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 ドキュメントの CloudTrail 検出セキュリティのベストプラクティス CloudTrail

- CloudTrail ドキュメントのすべてのリージョンに適用されるように、1 つのリージョンに適用される証跡を変換する
- CloudTrail ドキュメントのグローバルサービスイベントログ記録の有効化と無効化

サービスとアプリケーションレベルで口グ記録を設定する

AWS Well-Architected フレームワークでは、 サービスおよびアプリケーションから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) の基準、ポリシー、手順によって推進される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、ログと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潜在的な関心のある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」
- AWS Well-Architected フレームワークでサービスとアプリケーションの口グ記録を設定する

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する

ログの手動分析と情報の処理は、複雑なアーキテクチャに関連する情報の量に追いつくには不十分です。分析とレポートだけでは、適切なリソースへのイベント割り当てがタイムリーに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。

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

- 「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の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止する

デフォルトでは、CloudTrail ログファイルは 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は、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、可用性を維持できます。これはフォレンジックおよび監査の目的に不可欠です。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、この目的のために 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。

- Amazon S3 ドキュメントの S3 バケットのブロックパブリックアクセス設定の構成 Amazon S3
- CloudTrail ドキュメントの CloudTrail 予防的セキュリティのベストプラクティス
- CloudTrail ドキュメントの証跡の作成

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

Amazon Virtual Private Cloud (Amazon VPC) のセキュリティグループは、関連付けられているリソースに到達および送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トラフィックまたはアウトバウンド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重要です。

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、 AWS セキュリティグループを更新するために API コールが実行されるたびに警告します。Amazon EventBridge や などのサービスを使用してAWS Config、これらのタイプのセキュリティイベントに自動的に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 ドキュメントの「Amazon CloudWatch アラームの使用 CloudWatch 」
- 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

ALARM 状態に入る CloudWatch アラームのアラートを設定する

CloudWatch では、アラームが 、OK、ALARMおよび 状態の間でINSUFFICIENT_DATA状態を変更したときに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 人以上のユーザーに通知することです。アラームを設定して、 で OpsItems またはインシデントを作成することもできます AWS Systems Manager。

アラームアクションをアクティブ化して、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下回った場合に自動的にアラートを送信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、すべてのセキュリティプログラムの主要部分です。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制御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、defense-in-depth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。このセクションの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する
- 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する
- 専用 VPCs とサブネットを使用してネットワークレイヤーを作成する
- 受信トラフィックを許可されたポートのみに制限する
- Systems Manager ドキュメントへのパブリックアクセスをブロックする
- Lambda 関数へのパブリックアクセスをブロックする
- デフォルトの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する
- 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をスキャンする
- セットアップ AWS WAF
- DDoS 攻撃に対する高度な保護を設定する
- defense-in-depth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する

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する

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、リクエストは S3 バケット内のコンテンツの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を返すことがあります。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るの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。

- CloudFront ドキュメントでのデフォルトのルートオブジェクトの指定

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する

AWS Well-Architected フレームワークでは、ライブラリと依存関係をスキャンして問題や欠陥がないか確認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または Pythonアプリケーションの一般的なセキュリティ上の問題をスキャンし、修復に関する推奨事項を提供できます。

詳細については、以下のリソースを参照してください。

- CodeGuru ドキュメント
- OWASP Foundation ウェブサイトのソースコード分析ツール
- AWS Well-Architected フレームワークで脆弱性管理を実行する

専用 VPCs とサブネットを使用してネットワークレイヤーを作成する

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間のルートがないことを確認するために、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、VPCs 内の送信元リソースと送信先リソース間の接続をテストするのに役立つ設定分析ツールです。また、Network Access Analyzer は、 リソースへの意図しないネットワークアクセスを特定するのに役立ちます。

詳細については、以下のリソースを参照してください。

- AWS 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
- Amazon Virtual Private Cloud (Amazon VPC) ドキュメント」の「サブネットを作成する」

受信トラフィックを許可されたポートのみに制限する

`0.0.0.0/0` 送信元 IP アドレスからのトラフィックなどの無制限のアクセスは、ハッキング、denial-of-service (DoS) 攻撃、データ損失などの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 リソースへの送受信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) などのよく知られているポートへの無制限の進入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の場合、セキュリティグループで、許可されたポートで 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 アクセスの代わりに Session Manager または Run Command を使用します。 https://docs.aws.amazon.com/systems-manager/latest/userguide/run-command.html

詳細については、以下のリソースを参照してください。

- Amazon EC2 ドキュメントのセキュリティグループの使用
- 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する

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。パブリック共有は、ドキュメントへの意図しないアクセスを提供する場合があります。パブリック 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重要で機密性の高い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。

- Systems Manager ドキュメントの共有 Systems Manager ドキュメントのベストプラクティス
- Systems Manager ドキュメントの共有 Systems Manager ドキュメントのアクセス許可を変更する

Lambda 関数へのパブリックアクセスをブロックする

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、パブリックにアクセスできません。

Lambda 関数のリソースベースのポリシーを設定して、 アカウントの外部からのアクセスを拒否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 API または AWS Command Line Interface () を使用して、Lambda 関数のリソースベースのポリシーを更新できますAWS CLI。

また、[Lambda.1] Lambda 関数ポリシーを有効にして、パブリックアクセスコントロールを禁止することをお勧めします AWS Security Hub。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す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 ドキュメントの AWS Lambda コントロール
- Lambda ドキュメントの「Lambda のリソースベースのポリシーの使用」
- Lambda ドキュメントの Lambda アクションのリソースと条件

デフォルトの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する

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を許可し、すべてのアウトバウンド IPv4 および IPv6 トラフィックを許可します。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る場合があります。

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グループ用の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お勧めします。セキュリティグループルールを設定するときは、最小特権の原則に従います。

また、[EC2.2] VPC のデフォルトのセキュリティグループを有効にして、Security Hub 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トラフィックとアウトバウンドトラフィックを拒否す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
- Amazon VPCsの VPC のデフォルトのセキュリティグループ
- Security Hub 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をスキャンする

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て、ソフトウェアの脆弱性や意図しないネットワークへの露出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 が脆弱性またはオープンネットワークパスを特定すると、調査できる検出結果が生成されます。Amazon Inspector と Security Hub の両方がアカウントで設定されている場合、Amazon Inspector は自動的にセキュリティ検出結果を Security Hub に送信して一元管理を行います。

詳細については、以下のリソースを参照してください。

- Amazon Inspector ドキュメントの「Amazon Inspector によるリソースのスキャンAmazon Inspector 」
- Amazon Inspector ドキュメントの「Amazon Inspector Deep inspection for Amazon EC2Amazon Inspector 」
- AWS セキュリティブログの Amazon Inspector を使用して EC2 AMI をスキャン AMIsする
- AWS 規範ガイダンスの「 でのスケーラブルな脆弱性管理プログラムの構築 AWS」

- AWS Well-Architected フレームワークでのネットワーク保護の自動化
- 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 などの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。 APIs 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 AWS アカウント 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 AWS WAF方法」
- 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する

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型サービス拒否 (DDoS) 攻撃に対する保護を提供します。このサービスには、 AWS Shield Standard と の 2 つのオプションがあります 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 に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 攻撃に対する保護を強化します。Shield Advanced から受け取る保護は、アーキテクチャと設定の選択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 攻撃の影響を受ける可能性があることを AWS が認識し、AWS からの攻撃の通知と、セキュリティチームまたは運用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。

- Shield ドキュメントAWS Shield Advanced の概要
- Shield ドキュメントの AWS Shield Advanced で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
- Shield ドキュメントの DDoS イベントへの対応
- AWS Well-Architected フレームワークで検査と保護を実装する

defense-in-depth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する

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、または VPN または を介したトラフィックの送受信のフィルタリングが含まれます AWS Direct Connect。Network Firewall には、一般的なネットワーク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から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 3 つのカテゴリにグループ化します。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です。このセクションのセキュリティコントロールは、データ保護のベストプラクティスを実装するのに役立ちます。クラウド内のワークロードを設計する前に、これらの基本的なベストプラクティスを実施する必要があります。データの誤処理を防ぎ、組織、規制、コンプライアンスの義務を満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ます。

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して分類する
- 各データ分類レベルのコントロールを確立する
- 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する
- 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する
- 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する
- 重要な Amazon S3 バケット内のデータの削除を MFA に要求する
- VPC で Amazon OpenSearch Service ドメインを設定する
- 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
- セキュアプロトコルを使用するようにロードバランサーリスナーを設定する

ワークロードレベルでデータを特定して分類する

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。データ分類は、多くの場合、データ重複の頻度を減らします。これにより、ストレージとバックアップのコストを削減し、検索を高速化できます。

ワークロードが処理するデータの種類と分類、関連するビジネスプロセス、データの保存場所、データの所有者を把握することをお勧めします。データ分類は、ワークロード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決定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する

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。たとえば、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で機密データを保護します。データに直接アクセスしたり、手動で処理したりする必要性を軽減または排除するメカニズムとツールを使用します。データ識別と分類を自動化することで、誤分類、誤処理、変更、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) バケットをスキャンし、個人を特定できる情報 (PII) などの機密データを探す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の検出を自動化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
- AWS Well-Architected フレームワークでの識別と分類の自動化
- 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 による機密データの検出」
- Amazon VPC ドキュメントの VPC フローログを使用した IP トラフィックのログ記録
- 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

保管中のデータは、ストレージにあるデータなど、ネットワーク内で静止しているデータです。保管中のデータの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。コンテンツ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。

で説明したように各データ分類レベルのコントロールを確立する、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し、どのデータをトークン化やハッシュ化などの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 ドキュメントのデフォルトの暗号化の設定
- Amazon EC2 ドキュメントの新しい EBS ボリュームとスナップショットコピーのデフォルトでの暗号化
- Amazon Aurora ドキュメントの Amazon Aurora リソースの暗号化
- ドキュメントの の暗号化の詳細の概要 AWS KMS AWS KMS
- AWS 規範ガイダンスの保管中のデータのエンタープライズ暗号化戦略の作成
- 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

1 つは転送中のデータで、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。安全な TLS プロトコルと暗号スイートを使用して、転送中のすべてのデータを暗号化します。データへの不正アクセスを防ぐために、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は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。

- Amazon CloudFront ドキュメントのビューワーと CloudFront 間の通信に HTTPS を要求する Amazon CloudFront

- 「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する

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、他のすべてのスナップショット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 スナップショットをパブリックに共有しないことをお勧めします。これにより、誤って機密データが公開される可能性があります。スナップショットを共有すると、スナップショット内のデータへのアクセス権が他のユーザーに付与されます。スナップショットは、このすべてのデータで信頼するユーザーとのみ共有します。

詳細については、以下のリソースを参照してください。

- Amazon EC2 ドキュメントでスナップショットを共有する
- Amazon EBS スナップショットは、ドキュメントでパブリックに復元できません AWS Security Hub
- ドキュメントの AWS Config ebs-snapshot-public-restorable-check

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する

Amazon Relational Database Service (Amazon RDS) は、 でリレーショナルデータベースをセットアップ、運用、スケーリングするのに役立ちます AWS クラウド。Amazon RDS は、DB インスタンスのバックアップウィンドウ中に、データベース (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、データにアクセスするためのすべての AWS アカウント アクセス許可が付与されます。これにより、Amazon RDS インスタンス内のデータが意図せず公開され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。

- Amazon RDS ドキュメントでの DB スナップショットの共有
- AWS Config rdrds-snapshots-public-prohibited ドキュメント
- RDS スナップショットは Security Hub ドキュメントでプライベートにする必要があります

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 の場合`true`、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、データリークが発生する可能性があります。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 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。再作成するときは、パブリックにアクセス可能な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 Hub ドキュメントでAWS DMS 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 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
- Amazon Redshift クラスターは、Security Hub 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」
- ドキュメントの AWS Config redshift-cluster-public-access-check
- Amazon RDS ドキュメントの Amazon RDS DB インスタンスの変更
- Amazon Redshift ドキュメントのクラスターの変更

Amazon S3 バケットへのパブリックアクセスをブロックする

バケットにパブリックにアクセスできないようにすることは、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誰かがバケットを読み書きできるように明示的に要求しない限り、バケットがパブリックでないことを確認してください。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 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 ドキュメントの Amazon S3 セキュリティのベストプラクティス Amazon S3
- Security Hub 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 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 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
- ドキュメントの AWS Config s3-bucket-public-read-prohibited ルール
- 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の削除を MFA に要求する

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。この機能は、組織にとって重要なデータを含むバケットに対して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偶発的な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。

- Amazon S3 ドキュメントの MFA 削除の設定

VPC で Amazon OpenSearch Service ドメインを設定する

Amazon OpenSearch Service は、 でOpenSearchクラスターをデプロイ、運用、スケーリングするのに役立つマネージドサービスです AWS クラウド。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せず、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。

- Amazon OpenSearch Service ドキュメントの VPC 内で Amazon OpenSearch Service ドメインを起動する OpenSearch
- AWS Config ドキュメントの opensearch-in-vpc-only
- OpenSearch ドメインは Security Hub 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 キーが削除された場合、そのキーで暗号化されたデータは完全に回復できません。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。

誰かが KMS キーの削除を開始したときに通知する 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。これにより、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。

- ドキュメントの AWS KMS 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 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、 へのアクセスを制御するための主要な方法です AWS KMS keys。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。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、パブリックにアクセス可能な KMS キーを特定し、それらの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

セキュアプロトコルを使用するようにロードバランサーリスナーを設定する

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。ロードバランサーの各タイプは、さまざまなプロトコルとポートをサポートしています。

- 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、ロードバランサーはクライアントとターゲット間のトラフィックを暗号化および復号化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。

- Elastic Load Balancing ドキュメントの Application Load Balancer のリスナー
- Elastic Load Balancing Load Balancing ドキュメントの Classic Load Balancer のリスナー
- Elastic Load Balancing Load Balancing ドキュメントの Network Load Balancer のリスナー
- AWS 規範ガイダンスの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 ドキュメントの HTTPS または TLS 終了を使用して設定する必要があります
- Application Load Balancer は、Security Hub 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。

インシデントに対応するためのセキュリティレコメンデーション

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する準備ができている必要があります。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。理想的には、潜在的なセキュリティイベントが発生する前に組織を準備することです。 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するか、イベントに自動的に応答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確立できるコントロールは限られています。強力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して、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する
- インシデント対応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する
- 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する

インシデント対応計画を定義する

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盤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。

- 「 セキュリティインシデント対応ガイド」の「インシデント対応計画の策定とテストAWS 」
- 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
- AWS Well-Architected フレームワークの主要な担当者と外部リソースを特定する

インシデント対応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の準備の重要な部分は、プレイブックの開発です。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ユーザーが従う一連の推奨ステップが用意されています。構造と手順を明確にすることで、レスポンスが簡素化され、人為的ミスの可能性が軽減されます。

詳細については、以下のリソースを参照してください。

- 「 セキュリティインシデント対応ガイド」の「 のプレイブックを作成する方法AWS 」
- でのAWS インシデント対応プレイブックのサンプル GitHub
- AWS Well-Architected フレームワークでセキュリティインシデント対応プレイブックを開発してテストする

イベント駆動型セキュリティオートメーションを実装する

セキュリティレスポンスの自動化は、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、事前定義されたプログラムされたアクションです。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としては、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わったときにアラームがアクションを開始できます。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 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。

- セキュリティブログの Amazon Inspector のセキュリティ検出結果を自動的に修正する AWS
- 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 に対する自動セキュリティレスポンス AWS

- Amazon CloudWatch ドキュメントの Amazon CloudWatch アラームの使用 CloudWatch
- Security Hub ドキュメントの自動対応と修復
- Amazon Inspector ドキュメントの Amazon EventBridge を使用した Amazon Inspector の検出結果へのカスタムレスポンスの作成 Amazon Inspector

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に限られたリソースを持つ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 アカウント管理ガイドの の代替連絡先を更新する AWS アカウント
- 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する

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、チームがアクションを実行するための関連情報が含まれていることを確認します。

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検出

- 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続行するときは、これらの文書化されたコントロール、ガイダンス、および修復オプションを適用することが重要です。これらのレコメンデーションは、クラウドのセキュリティ体制を改善し AWS クラウド、 責任 AWS 共有モデルで定義されている のセキュリティ上の責任を果たすのに役立ちます。

次のステップでは、以下をお勧めします。

- 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 つの柱を確認してください。
- 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 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ます。
- 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ます。

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 セクションに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 規範ガイダンスが提供する戦略、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します。
- 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: オンプレミスの Oracle データベースを の Oracle 用 Amazon Relational Database Service (Amazon RDS) に移行します AWS クラウド。
- 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: カスタマーリレーションシップ管理 (CRM) システムを Salesforce.com に移行します。
- 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: オンプレミスの Oracle データベースを の EC2 インスタンス上の Oracle に移行します AWS クラウド。
- 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。

- 使用停止 — 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コントロール」を参照してください。

抽象化されたサービス

「 マネージドサービス」を参照してください。

ACID

アトミック性、一貫性、分離性、耐久性を参照してください。

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。より柔軟ですが、アクティブ/パッシブ移行よりも多くの作業が必要です。

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の方法。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

行のグループで動作し、グループの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 などがありますMAX。

AI

「人工知能」を参照してください。

AIOps

「人工知能オペレーション」を参照してください。

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。

アプリケーションコントロール

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 の需要要素であり、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?」を参照してください。

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

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

個人や組織を混乱させたり、損害を与えたりすることを意図したボット。

BCP

「事業継続計画」を参照してください。

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Data in a behavior graph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。エンディアン性も参照してください。

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

2 つの異なる同一の環境を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 (青) 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 (緑) 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、ボットハーダーまたはボットオペレーターとして知られる 1 人の当事者が管理しているボットのネットワーク。ボットは、ボットとその影響をスケールするための最もよく知られているメカニズムです。

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、 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 AWS 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、ホワイトペーパー AWSでのコンテナ化されたマイクロサービスの実行 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。

Canary デプロイ

エンドユーザーへのバージョンのスローリリースと増分リリース。確信が持てば、新しいバージョンをデプロイし、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

「データキャプチャの変更」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します。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テクノロジー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 に移行するときに通常実行する 4 つのフェーズ AWS クラウド :

- 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

「設定管理データベース」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または が含まれますBitbucket Cloud。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などのビジュアル形式から情報を分析および抽出する AI の分野。例えば、Amazon SageMaker AI は CV 用の画像処理アルゴリズムを提供します。

設定ドリフト

ワークロードの場合、設定が想定状態から変化します。これにより、ワークロードが非準拠になる可能性があり、通常は段階的かつ意図的ではありません。

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

一元管理とガバナンスを備えた分散型の分散型データ所有権を提供す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、予想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通常、大量の履歴データが含まれており、通常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る。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。

ディープラーニング

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。

デプロイ

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、Implementing security controls on AWSのDetective controls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

スタースキーマでは、ファクトテーブル内の量的データに関するデータ属性を含む小さなテーブル。ディメンションテーブル属性は通常、テキストフィールドまたはテキストのように動作する

離散数値です。これらの属性は、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一般的に使用されます。

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)

災害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に使用する戦略とプロセス。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

「開発値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、応答時間を短縮できます。

電子データ交換 (EDI)

組織間の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プロセス。

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

星スキーマの中央テーブル。事業運営に関する量的データを保存します。通常、ファクトテーブルには、メジャーを含む列とディメンションテーブルへの外部キーを含む列の 2 つのタイプの列が含まれます。

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で段階的なテストを使用する哲学。これはアジャイルアプローチの重要な部分です。

障害分離の境界

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

同様のタスクの実行を求める前に、タスクと必要な出力を示す少数の例を LLM に提供します。この手法は、プロンプトに埋め込まれた例 (ショット) からモデルが学習するコンテキスト内学習のアプリケーションです。少数ショットプロンプトは、特定のフォーマット、推論、またはドメインの知識を必要とする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コントロール」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

段階的なアプローチを使用する代わりに、変更データキャプチャによる継続的なデータレプリケーションを使用して、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)

一般化およびラベル付けされていないデータの大規模なデータセットでトレーニングされている大規模な深層学習ニューラルネットワーク。FMs は、言語の理解、テキストと画像の生成、自然言語の会話など、さまざまな一般的なタスクを実行できます。詳細については、「基盤モデルとは」を参照してください。

G

生成 AI

大量のデータでトレーニングされ、シンプルなテキストプロンプトを使用してイメージ、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る AI モデルのサブセット。詳細については、「生成 AI とは」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 ワークフローはレガシーと見なされ、トランクベースのワークフローはモダンで推奨されるアプローチです。

ゴールデンイメージ

そのシステムまたはソフトウェアの新しいインスタンスをデプロイするためのテンプレートとして使用されるシステムまたはソフトウェアのスナップショット。例えば、製造では、ゴールデンイメージを使用して複数のデバイスにソフトウェアをプロビジョニングし、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、、 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。

ハイアベイラビリティ (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に使用されるデータセットから保留される、ラベル付きの履歴データの一部。モデル予測をホールドアウトデータと比較することで、ホールドアウトデータを使用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

「産業用モノのインターネット」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

既存のインフラストラクチャを更新、パッチ適用、または変更する代わりに、本番環境のワークロード用に新しいインフラストラクチャをデプロイするモデル。イミュータブルインフラストラクチャは、本質的に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、予測性が高くなります。詳細については、 AWS 「 Well-Architected フレームワーク」の「イミュータブルインフラストラクチャを使用したデプロイ」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 によって導入された用語で、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ゼーションを指します。

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。

産業分野における 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、「Building an industrial Internet of Things (IIoT) digital transformation strategy」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 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

「モノのインターネット」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)

大量のデータに対して事前トレーニングされた深層学習 AI モデル。LLM は、質問への回答、ドキュメントの要約、テキストの他の言語への翻訳、文の完了など、複数のタスクを実行できます。詳細については、LLMs」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

「ラベルベースのアクセスコントロール」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。エンディアン性も参照してください。

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または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、不正アクセスにつながる可能性があります。マルウェアの例としては、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。Amazon Simple Storage Service (Amazon S3) と Amazon DynamoDB は、マネージドサービスの例です。これら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、制御するためのソフトウェアシステムで、原材料を工場の完成製品に変換します。

MAP

「移行促進プログラム」を参照してください。

メカニズム

ツールを作成し、ツールの導入を推進し、調整を行うために結果を検査する完全なプロセス。メカニズムは、動作中にそれ自体を強化して改善するサイクルです。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。

メッセージキューイングテレメトリトランスポート (MQTT)

リソースに制約のある IoT デバイス用の、パブリッシュ/サブスクライブパターンに基づく軽量 machine-to-machine (M2M) 通信プロトコル。

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)

に移行するためのビジネスケースを検証するための情報を提供するオンラインツール AWS クラウド。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 に移行するために使用するアプローチ AWS クラウド。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、「」の「アプリケーションをモダナイズするための戦略 AWS クラウド」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、『』の「アプリケーションのモダナイゼーション準備状況の評価 AWS クラウド」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

「移行ポートフォリオ評価」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。

ミュータブルインフラストラクチャ

本番ワークロードの既存のインフラストラクチャを更新および変更するモデル。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

「オリジンアクセスコントロール」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

「 オペレーションの統合」を参照してください。

OLA

「運用レベルの契約」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。

オープンプロセス通信 - 統合アーキテクチャ (OPC-UA)

産業用オートメーション用のmachine-to-machine (M2M) 通信プロトコル。OPC-UA は、データの暗号化、認証、認可スキームを備えた相互運用性標準を提供します。

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)

インシデントや潜在的な障害の理解、評価、防止、または範囲の縮小に役立つ質問とそれに関連するベストプラクティスのチェックリスト。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するハードウェアおよびソフトウェアシステム。製造では、OT と情報技術 (IT) システムの統合が、Industry 4.0 変換の主な焦点です。

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のため、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。

オリジンアクセスコントロール (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コントロールが可能です。

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

「プログラム可能な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

アクセス許可を定義 (アイデンティティベースのポリシーを参照)、アクセス条件を指定 (リソースベースのポリシーを参照)、または の組織内のすべてのアカウントに対する最大アクセス許可を定義 AWS Organizations （ サービスコントロールポリシーを参照) できるオブジェクト。

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。詳細については、マイクロサービスでのデータ永続性の有効化 を参照してください。

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、「移行準備状況ガイド」を参照してください。

述語

`true` または を返すクエリ条件。一般的に`false`は `WHERE`句にあります。

述語プッシュダウン

転送前にクエリ内のデータをフィルタリングするデータベースクエリ最適化手法。これにより、リレーショナルデータベースから取得して処理する必要があるデータの量が減少し、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、Implementing security controls on AWSのPreventative controls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内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じてプライバシーを考慮するシステムエンジニアリングアプローチ。

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を防ぐ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、プロビジョニング前にリソースをスキャンします。リソースがコントロールに準拠していない場合、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)

設計、開発、発売から成長と成熟まで、製品のデータとプロセスのライフサイクル全体にわたる管理。

本番環境

「環境」を参照してください。

プログラム可能なロジックコントローラー (PLC)

製造では、マシンをモニタリングし、製造プロセスを自動化する、信頼性の高い適応可能なコンピュータです。

プロンプトの連鎖

1 つの LLM プロンプトの出力を次のプロンプトの入力として使用して、より良いレスポンスを生成します。この手法は、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善または拡張したりするために使用されます。これにより、モデルのレスポンスの精度と関連性が向上し、より詳細でパーソナライズされた結果が得られます。

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。

パブリッシュ/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。スケーラビリティと応答性を向上させます。たとえば、マイクロサービスベースの MES では、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できるチャネルにイベントメッセージを発行できます。システムは、公開サービスを変更せずに新しいマイクロサービスを追加できます。

Q

クエリプラン

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る手順などの一連のステップ。

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

責任、説明責任、相談、通知 (RACI) を参照してください。

RAG

「取得拡張生成」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

責任、説明責任、相談、情報 (RACI) を参照してください。

RCAC

「行と列のアクセスコントロール」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。

再設計

「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、AWS リージョン「アカウントで使用できる を指定する」を参照してください。

回帰

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。

プラットフォーム変更

「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

中断に抵抗または回復するアプリケーションの機能。高可用性とディザスタリカバリは、 で回復性を計画する際の一般的な考慮事項です AWS クラウド。詳細については、AWS クラウド「レジリエンス」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。サポートを含めると、そのマトリックスは RASCI マトリックスと呼ばれ、サポートを除外すると 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、Implementing security controls on AWSのResponsive controls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。

取得拡張生成 (RAG)

LLM がレスポンスを生成する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を参照する生成 AI テクノロジー。たとえば、RAG モデルは、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する場合があります。詳細については、「RAG とは」を参照してください。

ローテーション

攻撃者が認証情報にアクセスすることをより困難にするために、シークレットを定期的に更新するプロセス。

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 Management Console 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

「監視コントロールとデータ取得」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。シークレット値は、バイナリ、1 つの文字列、または複数の文字列にすることができます。詳細については、Secrets Manager ドキュメントの「Secrets Manager シークレットの内容」を参照してください。

設計によるセキュリティ

開発プロセス全体でセキュリティを考慮するシステムエンジニアリングアプローチ。

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、予防的、検出的、応答的、プロアクティブの 4 つの主なタイプがあります。

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に自動的に応答または修復するように設計された、事前定義された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。自動応答アクションの例としては、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、スループットなど、サービスのパフォーマンス側面の測定。

サービスレベルの目標 (SLO)

サービスレベルのインジケータによって測定される、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。

SIEM

セキュリティ情報とイベント管理システムを参照してください。

単一障害点 (SPOF)

システムを中断する可能性のあるアプリケーションの 1 つの重要なコンポーネントの障害。

SLA

「サービスレベルの契約」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、『』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 AWS クラウド」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

1 つの大きなファクトテーブルを使用してトランザクションデータまたは測定データを保存し、1 つ以上の小さなディメンションテーブルを使用してデータ属性を保存するデータベース組織構造。この構造は、データウェアハウスまたはビジネスインテリジェンスの目的で使用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。

監視コントロールとデータ収集 (SCADA)

製造では、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稼働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潜在的な問題を検出したり、パフォーマンスをモニタリングしたりする方法でシステムをテストします。Amazon CloudWatch Synthetics を使用してこれらのテストを作成できます。

システムプロンプト

LLM にコンテキスト、指示、またはガイドラインを提供して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、ユーザーとのやり取りのルールを確立するのに役立ちます。

T

tags

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 枚のピザで養う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。詳細については、深層学習システムにおける不確実性の定量化 ガイドを参照してください。

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

現在のレコードに関連する行のグループに対して計算を実行する SQL 関数。ウィンドウ関数は、移動平均の計算や、現在の行の相対位置に基づく行の値へのアクセスなどの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 「ワークロード認定フレームワーク」を参照してください。

write once, read many (WORM)

データを 1 回書き込み、データの削除や変更を防ぐストレージモデル。承認されたユーザーは、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

ゼロデイ脆弱性を利用する攻撃、通常はマルウェア。

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 にタスクを実行する手順を提供しますが、タスクのガイドに役立つ例 (ショット) はありません。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。