aws

アプリケーション所有者向けログ記録およびモニタリングガイド

AWS 規範ガイダンス

AWS 規範ガイダンス: アプリケーション所有者向け口グ記録およびモニタリングガイド

Table of Contents

アプリケーション所有者向けログ記録およびモニタリングガイド

John Buckley (Amazon Web Services (AWS))

2023 年 1 月 (ドキュメント履歴)

ワークロードとは、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) の集合のことです。ワークロードは、単一の AWS アカウント にあるリソースのサブセットで構成される場合もあれば、複数の AWS アカウント にまたがる場合もあります。クラウドのアプリケーションはワークロードの一種です。これはクラウド環境でのみデプロイされる場合もあれば、ローカルのオンプレミスハードウェアでサポートされる場合もあります。多くの出版物はクラウドインフラストラクチャのログ記録とモニタリングに重点を置いており、セキュリティチームを対象としています。このガイドはアプリケーション所有者を対象としており、AWS クラウド のアプリケーションのログ記録とモニタリングを効果的かつ効率的に行う方法を中心に説明しています。

このガイドを参考に、ログ記録とモニタリングを適切なレベルに設定することで、異常を迅速に特定し対応できるようになります。また、アプリケーションログがあらゆる問題の詳細な分析と解決をサポートできるようにします。

このガイドは AWS クラウド を使用したデプロイを想定していますが、これらのプリンシパルはオンプレミスや他のクラウドプロバイダーのインフラストラクチャで実行するアプリケーションにも適用できます。

ターゲットを絞ったビジネス成果

このガイドを読んだ後は、次のことを理解できるようになっているはずです。

- アプリケーションに関して一般的にログされるイベントの種類
- ログ記録を検討すべきイベント属性 (誰が、何を、どのタイミングで、など)
- ログからの除外を検討すべきデータの種類 (セキュリティ体制を侵害する可能性のあるデータや個人を特定できる情報など)
- ログ記録とモニタリングをアプリケーションに適したレベルに設定する方法
- アプリケーションログの管理およびアクセスが可能な人物

- AWS クラウド のアプリケーションをモニタリングおよびログ記録するために設定できる AWS のサービス および機能
- アプリケーションのログデータの使用方法と、問題の優先順位付けや診断を行うための AWS のサービス または機能

アプリケーションのロギングとモニタリングについて

ロギング、モニタリング、アラート、レポートはそれぞれ異なるセキュリティプロセスであり、これらが連携することでアプリケーションの正常性とパフォーマンスを可視化します。アプリケーションのアクションとイベントの詳細な記録を作成、維持して、記録されたアクティビティに基づいて監視、アラート、レポートを実行することが重要です。

アプリケーションロギングは、アプリケーションで生成されたイベントを収集し、1 つ以上のログファイルに記録するプロセスです。このイベント履歴は、セキュリティやパフォーマンスの分析、リソース変更の追跡、アプリケーションの問題のトラブルシューティングに役立ちます。

アプリケーションモニタリングは、アプリケーションの全体的なパフォーマンスと正常性を評価するプロセスです。アプリケーションのフロントエンドとバックエンドを常時監視できます。クラウド上でホストされるアプリケーションは高度に分散されているため、ロギングツールやモニタリングツールを使用することで、パフォーマンスの問題を迅速にトラブルシューティングしたり、セキュリティ上の脅威をリアルタイムで特定し、修正したりするのに役立ちます。ログデータはモニタリングにとって重要な入力です。

オブザーバビリティはモニタリングと似ていますが、さまざまなパラメータを使用してアプリケーションの動作を測定する方法を採用しているため、複雑な相関関係が可能になります。例えば、特定の地理的リージョンの一連のユーザーについて、特定の日の HTTP 成功率を測定する場合などです。詳細については、「モニタリングとオブザーバビリティ」(AWS マーケティング) を参照してください。

最終的に、アプリケーション所有者の目標は、安全かつ健全なアプリケーションと、それらのアプリケーションによる優れたユーザーエクスペリエンスを維持することです。ロギングとモニタリングを実装することで、開発者と運用チームは、アプリケーションの問題に対する計画とトラブルシューティングを迅速に行えるようになります。

必要なロギングとモニタリングのレベルは、アプリケーションごとに異なります。モニタリングとロギングのレベルに影響する要因には、組織のポリシーと手順、アプリケーションがもたらすセキュリティリスクのレベル、業務におけるアプリケーションの重要性、アプリケーションが管理するデータの機密性などがあります。一般的に、公開されているアプリケーションや顧客向けのアプリケーションには、組織内で使用されているアプリケーションよりも高いレベルのモニタリングとロギングが必要です。このガイドに記載されていることは一般的な情報とレコメンデーションのため、アプリケーションの要件に基づいてアプローチをカスタマイズする必要があります。

> **Note**
>
> 組織の標準や手順によっては、特定のロギングやモニタリング属性が義務付けられている場合があります。例えば、エンタープライズ使用権限レビューシステムにユーザーのアクセス許可を渡すことなどです。ロギングとモニタリングの計画が、組織の要件を満たしていることを確認してください。

AWS クラウド のアプリケーションのログ記録

AWS クラウド のログ記録アプリケーション用に、共通するイベントタイプ、イベントの属性、ベストプラクティスを確認してください。

このセクションでは、次のトピックについて説明します。

イベントタイプ

アプリケーションのログ記録戦略を確立する上で最も考慮すべき点の 1 つは、どのイベントとアクションを記録するかを決めることです。それを決める際、組織やアプリケーションの要件が影響する可能性はありますが、お使いのアプリケーションに当てはまる場合は次の情報を常に口グしておくことを推奨します。

- 入力検証エラー — 例としては、プロトコル違反、許容できないエンコーディング、無効なパラメータ名や値などがあります。
- 出力検証エラー — 例としては、データベースレコードセットの不一致や無効なデータエンコーディングなどがあります。
- ID 認証の成功と失敗 — 認証アクティビティは口グしますが、ユーザー名とパスワードは口グしません。ユーザーがユーザー名フィールドに誤ってパスワードを入力する可能性があるため、ユーザー名は口グしないことを推奨します。これにより、認証情報が意図せず公開され、アクセスが許可される可能性があります。認証データを含むすべての口グにセキュリティ制御を実装します。
- 承認 (アクセス制御) 失敗 — 関連する認証システム用に失敗したアクセス試行を口グします。この口グデータをモニタリングして、アプリケーションの認証システムに対する攻撃や問題を示す可能性のあるパターンがないか調べることができます。
- セッション管理の失敗 — 例としては、セッションの Cookie やトークンの変更などがあります。アプリケーションでは多くの場合、Cookie やトークンを使用してユーザー状態を管理します。悪意のあるユーザーは Cookie の値を変更して不正アクセスを試みることがあります。改ざんされたセッショントークンを口グに記録することで、この動作を検出できます。
- アプリケーションエラーとシステムイベント — 例としては、構文エラーやランタイムエラー、接続上の問題、パフォーマンスの問題、サードパーティサービスからのエラーメッセージ、ファイルシステムエラー、ファイルアップロード時のウイルス検出、設定の変更などがあります。

- アプリケーションの状態 — アプリケーションとその関連リソースを起動または停止します。
- ログ記録の状態 — ログ記録の開始、停止、一時停止。
- リスクの高い機能の使用 — 例としては、ネットワーク接続の変更、ユーザーの追加または削除、権限の変更、トークンへのユーザーの割り当て、トークンの追加または削除、システム管理権限の使用、アプリケーション管理者によるアクセス、管理者権限を持つユーザーが実行するすべてのアクション、支払いカード会員データへのアクセス、データ暗号化キーの使用、暗号化キーの変更、システムレベルのオブジェクトの作成と削除、ユーザー生成コンテンツの送信 (特にファイルのアップロード)、データ (特にファイルのアップロード)、データ (レポートを含む) のインポートとエクスポートなどがあります。
- 法務およびその他のオプトイン — 例としては、携帯電話機能の許可、利用規約、個人データの使用に関する同意、マーケティングコミュニケーションの受信許可などがあります。

アプリケーションの推奨属性に加えて、モニタリング、アラート、レポートに役立つデータを提供する追加の属性を検討してください。その例を以下に示します。

- シーケンシング失敗
- 組織の利用規定に違反するユーザーの行動を評価するのに役立つ属性
- データ変更
- 金融犯罪の防止、株式取引の制限、健康情報やその他の個人情報の収集など、基準や規制を遵守するために必要な属性。
- 不正な行為を試みるなど、疑わしい行動や予期しない行動を特定するのに役立つ属性
- 設定変更
- アプリケーションコードファイルまたはメモリの変更

イベントの属性

各ログのエントリには、モニタリングと分析を行うのに十分な詳細情報が含まれている必要があります。コンテンツデータ全体をログに記録することもできますが、抽出または概要プロパティを記録する方が効率的です。アプリケーションログには、各イベントのいつ、どこで、誰が、何を、どちらを、について記録する必要があります。これらのプロパティは、アーキテクチャ、アプリケーションのクラス、ホストシステムまたはデバイスによって異なります。

日付とタイムスタンプをログに記録するときは、協定世界時 (UTC) と ISO 8601 (ISO ウェブサイト) で国際的に認められている日付と時刻の形式を使用してください。

> **Note**
>
> 正確なタイムスタンプを付与するために、ネットワーク時刻同期サービスの使用を検討してください。Amazon は Amazon Time Sync Service を提供しており、Amazon Elastic Compute Cloud (Amazon EC2) を含む多くの AWS のサービス で使用されています。Amazon Time Sync Service は、各 AWS リージョン で衛星接続された原子基準クロックのフリートを使用し、ネットワークタイムプロトコル (NTP) を通じて世界標準時 (UTC) の正確な現在時刻を表示します。詳細については、「Amazon Time Sync Service で時間を維持する」(AWS ブログ記事) を参照してください。

通常、次のイベント属性がログに含まれます。

属性カテゴリ	イベントの属性	説明
メトリック	ログ記録の日付と時刻	イベントがログに追加された日付と時刻を記録します。
	イベントの日付と時刻	イベントが発生した日付と時刻を記録します。これは、クライアントアプリケーションが定期的または断続的にオンラインになっているリモートデバイスでホストされているためにログ記録が遅れる場合など、ログ記録レコードとは異なる場合があります。
	イベントの識別子	イベントを常に特定できるよう、ユーザー名、アカウント番号、またはその他の一意の属性をログします。
各パラメータの意味は次のとおりです。	アプリケーション識別子	アプリケーション名とバージョンをログします。
	アプリケーションアドレス	クラスターまたはホスト名、サーバーの IPv4 または IPv6

		アドレス、ポート番号、ワークステーション ID、ローカルデバイス識別子をログします。
	サービス	サービス名とプロトコルをログします。
	ジオロケーション	ユーザーの地理的位置をログします。
	ウィンドウ、フォーム、またはページ	アクションが実行されたエントリポイント URL、Web アプリケーションの HTTP メソッド、またはダイアログボックス名をログします。
	コードロケーション	スクリプトまたはモジュール名をログします。
誰 (人間またはマシンユーザー)	送信元アドレス	ユーザーのデバイス識別子、IP アドレス、携帯電話もしくは無線周波数 (RF) タワー ID、または携帯電話番号をログします。
	ユーザー ID	ユーザーが認証されているか、その他の方法でわかっている場合は、ユーザーデータベーステーブルのプライマリキー値、ユーザー名、またはライセンス番号をログします。

	ユーザータイプの分類	公開、認証済み、CMS、検索エンジン、認定侵入テスター、稼働時間モニターなどのユーザーの種類を口グします。稼働時間モニターの詳細については、このガイドの「注意事項と除外事項」を参照してください。
	HTTP ヘッダーまたは HTTP ユーザーエージェントのリクエスト	(Web アプリケーションのみ) HTTP ユーザーエージェント文字列を含む HTTP リクエストヘッダー情報を口グします。これらの値は、クライアントがサーバーに送信する情報に影響を及ぼすためです。
何	イベントのタイプ	イベントが情報提供なのか、警告なのか、エラーなのかを口グします。
	イベントの重要度	イベントの重要度を、高、中、低などに分類します。
	セキュリティイベントフラグ	ログにセキュリティイベントに関係のないデータが含まれている場合は、セキュリティ関連イベントのフラグを作成して、それらを識別しやすくします。
	イベントの説明	(オプション) イベントの簡単な説明を含みます。
	アクションまたは意図	ログイン、セッション ID の更新、ログアウト、プロファイルの更新など、リクエストの本来の目的を口グします。

	ユーザーまたはアプリケーションの応答	ステータスコード、カスタムテキストメッセージ、セッションの停止、管理者アラートなど、イベントに対するユーザーまたはアプリケーションの応答を口グします。
	結果ステータス	成功、失敗、延期など、アクションが成功したかどうかをログします。
	結果理由	ステータスが発生した理由をログします。例えば、ユーザーがデータベースで認証されていないためにサインインリクエストが失敗することがあります。
	詳細情報を拡張	スタックトレース、システムエラーメッセージ、デバッグ情報、HTTP リクエスト本文など、イベントに関連する追加情報をすべてログします。
	HTTP レスポンスのステータスコード	(Web アプリケーションのみ) `200` または `301` など、ユーザーに返された HTTP レスポンスのステータスコードをログします。詳細については、このガイドの「ログ記録レベル」を参照してください。
どれ	影響を受けるリソース	どのリソースに基づいて処理が行われたかをログします。

	オブジェクト	影響を受けたコンポーネントや、ユーザーアカウント、データリソース、ファイル、URL、セッション ID などのオブジェクトをログします。
	リソース名	影響を受けたリソースの名前をログします。
	リソースタグ	影響を受けたリソースに割り当てられたタグをログします。タグの詳細については、「Tagging AWS resources」(AWS 全般のリファレンス) を参照してください。
その他	分析上の信頼性	低、中、高の評価や数値の割り当てなど、イベント検出に対するログ記録サービスの信頼度を記録します。
	内部分類	標準やコンプライアンスの遵守に関する内部分類をすべてログします。
	外部分類	NIST セキュリティコンテンツ自動化プロトコル (SCAP) など、標準やコンプライアンス遵守に関する外部分類をすべてログします。

ベストプラクティスのログ記録

ログ記録レベル

過剰量のデータをログしないように注意してください。ログには、有用で実用的なデータが記録されるべきです。過剰なログ記録はパフォーマンスに悪影響を及ぼす可能性があるだけでなく、ログ記録のストレージと処理コストも増加する可能性があります。過剰なログ記録により問題が発生したり、セキュリティイベントが検出されなくなったりする可能性もあります。

HTTP 応答ステータスコードをログに記録すると、特に 200 レベル (成功) と 300 レベル (リダイレクト) のステータスコードなど、大量のログデータが生成される可能性があります。400 レベル (クライアント側のエラー) と 500 レベル (サーバー側のエラー) のステータスコードのみをログ記録するよう検討することを推奨します。

アプリケーションログ記録フレームワークでは、情報、デバッグ、エラーなどさまざまなレベルのログ記録が可能です。開発環境では、開発者を支援するために情報やデバッグなどの詳細なログ記録を使用したいと考えるかもしれません。ただし、過剰なログデータを生成する可能性があるため、本番稼働環境では情報レベルとデバッグレベルは無効にしておくことを推奨します。

注意事項と除外事項

- ログ記録するデータが、特に組織が事業を展開する管轄地域で法的に許可されていることを確認してください。
- 既知のユーザー (他の内部システムなど)、信頼できるサードパーティー、検索エンジンロボット、稼働時間モニター、プロセスモニター、その他のリモートモニタリングシステムからのイベントは除外しないでください。ただし、記録されたデータにはそれぞれに分類フラグを含めることができます。アプリケーションが生成するログファイルは、アプリケーションが処理する機密データを閲覧する権限を持たないサードパーティーのログモニタリングソリューションや外部のサービスプロバイダーなどによって使用される可能性があることを考慮してください。
- 以下の属性はログに直接記録しないでください。以下を削除、マスキング、サニタイズ、ハッシュ、または暗号化します。
  - アプリケーションのソースコード
  - セッション ID 値 (セッション固有のイベントを追跡する必要がある場合は、これをハッシュ値に置き換えることを検討してください)
  - アクセストークン
  - 機密個人データと、健康情報や政府発行の識別子など何らかのかたちで個人を特定できる情報 (PII)

- 認証パスワード
- データベース接続文字列
- 暗号化キーとその他のプライマリシークレット
- 銀行口座または支払いカード名義人のデータ
- ロギングシステムで保存が許可されているよりも高いセキュリティ分類のデータ
- 商業的機密情報
- 関連する管轄地域で収集が違法な情報
- ユーザーが収集をオプトアウトした、または収集に明示的に同意していない情報
- 収集への同意が失効した情報

特殊データ型

場合によっては、以下のデータがログに記録されることもあります。調査やトラブルシューティングには役立ちますが、システムに関する機密情報が明らかになる可能性があります。イベントを記録する前に、これらのデータ型を匿名化、ハッシュ、または暗号化する必要があるかもしれません。

- ファイルパス
- 内部ネットワーク名とアドレス
- 個人名、電話番号、E メールアドレスなど、機密性の低い個人データ

個人の身元情報をログに記録する必要がない場合や、リスクが大きすぎると考えられる場合は、データの匿名化を使用してください。

アクセスと変更管理

- 管理者以外のユーザーは、特にコンプライアンス要件を満たすために必要なイベントのログ記録を無効にできないようにする必要があります。
- ログ記録サービスを一時停止または停止したり、設定を変更したりできるのは管理ユーザーのみとします。
- ログ記録サービスにログファイルの整合性検証機能がある場合は、それを有効にします。これにより、ログファイルの変更、削除、または偽造を検出できます。AWS のサービス で利用できるこの機能の詳細については、このガイドの「CloudTrail の使用」を参照してください。

- ログ記録の変更は、承認されたアルゴリズムに基づいてアプリケーションが自動的に行うなど、アプリケーション固有のものでなければなりません。また、設定データを変更したりソースコードを変更したりする場合など、承認された変更管理プロセスに従う必要があります。

AWS のサービス でのロギングとモニタリング

このガイドでは、AWS クラウド にデプロイされているアプリケーションのロギングとモニタリングに焦点を当てています。AWS のサービス を使用することで、ロギングとモニタリングの計画を実行したり、現在のソリューションを補強したりできます。例えば、アプリケーションの問題をトラブルシューティングする場合、次のようなことを実行できます。

- Amazon Virtual Private Cloud (Amazon VPC) の VPC フローログ機能を使用してアプリケーションログをトリアージし、問題に対応するネットワークトラフィックを表示します。
- AWS CloudTrail を使用して、問題イベント時間に対応する API 呼び出しを表示します。
- Amazon CloudWatch Logs のログを確認して、問題イベント時間に対応する CPU スパイクがないかをチェックします。

以下の AWS のサービス と、アプリケーションのロギングとモニタリングのための機能をデプロイできます

- AWS CloudTrail は、ユーザー、ロール、AWS のサービス によって実行されたアクションを記録することにより、AWS アカウント 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。このサービスを使用してアプリケーションのイベントを記録または監視する方法の詳細については、このガイドの「CloudTrail」を参照してください。
- Amazon CloudWatch を使用すると、ログを分析し、リアルタイムで AWS リソースとホストアプリケーションのメトリクスを監視できます。ServiceLens 機能を使用してアプリケーションの正常性を監視したり、Synthetics 機能を使用してエンドポイントと API を監視する canary を作成したりすることもできます。このサービスを使用してアプリケーションを監視する方法の詳細については、このガイドの「CloudWatch」を参照してください。
- Amazon CloudWatch Logs は、すべてのシステム、アプリケーション、AWS のサービス からのログを一元化するのに役立ちます。一元化により、ログを監視して安全にアーカイブできます。このサービスを使用してアプリケーションのイベントを記録する方法の詳細については、このガイドの「CloudWatch Logs」を参照してください。
- Amazon Virtual Private Cloud (Amazon VPC) の VPC フローログ機能は、VPC のネットワークインターフェイスとの間を行き来する IP トラフィックに関する情報をキャプチャします。このサービスを使用してアプリケーションのイベントを記録する方法の詳細については、このガイドの「VPC Flow Logs」を参照してください。
- AWS X-Ray は、アプリケーションが処理するリクエストに関するデータを収集するとともに、データを表示、フィルタリングし、データからインサイトを取得することによって、問題や最適

化の機会を特定します。このサービスを使用してアプリケーションを監視する方法の詳細については、このガイドの「X-Ray」を参照してください。

AWS CloudTrail を使用したアプリケーションのロギングとモニタリング

AWS CloudTrail は、AWS アカウント の運用とリスクの監査、ガバナンス、コンプライアンスを可能にする AWS のサービス です。ユーザー、ロール、または AWS のサービス によって実行されたアクションは、CloudTrail にイベントとして記録されます。イベントには、AWS Management Console、AWS Command Line Interface (AWS CLI)、および AWS SDK と API で実行されたアクションなどが考えられます。

CloudTrail の使用

CloudTrail は、アカウント作成時に AWS アカウント で有効になります。AWS アカウント アカウントでアクティビティが発生した場合、そのアクティビティは CloudTrail イベントに記録されます。イベント履歴に移動し、CloudTrail コンソールで簡単に最近のイベントを表示できます。

AWS アカウント のアクティビティおよびイベントを継続的に記録するには、「証跡」を作成します。単一の AWS リージョン またはすべてのリージョンの証跡を作成できます。証跡は各リージョンのログファイルを記録し、CloudTrail はログファイルを単一の統合された Amazon Simple Storage Service (Amazon S3) バケットに配信します。

証跡が指定したイベントのみを処理してログに記録するように、複数の証跡を異なる方法で設定することができます。これは、AWS アカウント で発生するイベントと、アプリケーションで発生するイベントをトリアージする場合に便利です。

> **Note**
>
> CloudTrail には検証機能があり、CloudTrail がログファイルを配信した後で、ログファイルが変更、削除されているか、もしくは変更されていないかを判断するために使用できます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。AWS CLI を使用して CloudTrail が配信した場所のファイルを検証することができます。この機能の詳細と有効化の方法については、「CloudTrail ログファイルの整合性の検証」(CloudTrail ドキュメント) を参照してください。。

CloudTrail のユースケース

- コンプライアンス支援 — CloudTrail を使用すると、AWS アカウント でのイベント履歴が提供されるため、社内ポリシーや規制への準拠に役立ちます。
- セキュリティ分析 — CloudTrail ログファイルを CloudWatch Logs、Amazon EventBridge、Amazon Athena、Amazon OpenSearch Service、またはその他のサードパーティソリューションなどのログ管理および分析ソリューションに取り込むことで、セキュリティ分析を実行し、ユーザーの行動パターンを検出できます。
- データ流出 — CloudTrail に記録されたオブジェクトレベルの API イベントを介して Amazon S3 オブジェクトのアクティビティデータを収集することで、データ流出を検出できます。アクティビティデータが収集されたら、EventBridge や AWS Lambda などの他の AWS のサービス を使用して、自動応答をトリガーできます。
- 運用上の問題のトラブルシューティング — CloudTrail ログファイルを使用して、運用上の問題をトラブルシューティングできます。例えば、AWS リソースの作成、変更、削除など、環境内のリソースに加えられた最新の変更をすばやく特定できます。

CloudTrail のベストプラクティス

- すべての AWS リージョン の CloudTrail を有効にします。
- ログファイルの整合性検証を有効にします。
- ログを暗号化します。
- CloudTrail ログファイルを CloudWatch Logs に取り込みます。
- すべての AWS アカウント およびリージョンのログを一元化します。
- ログファイルを含む S3 バケットにライフサイクルポリシーを適用します。
- ユーザーが CloudTrail でロギングをオフにできないようにします。AWS Organizations で次のサービスコントロールポリシーを適用します。この SCP は、組織全体の `StopLogging` および `DeleteTrail` アクションに明示的な拒否ルールを設定します。

```
{
"Version": "2012-10-17",
"Statement":
       [
                 { "Action":
                     [
                     "cloudtrail:StopLogging",
```

```
                    "cloudtrail:DeleteTrail"
                    ],
                    "Resource": "*",
                    "Effect": "Deny"
                }
        ]
}
```

Amazon CloudWatch を使用したアプリケーションのロギングとモニタリング

Amazon CloudWatch は、AWS のリソースおよび AWS で実行しているアプリケーションをリアルタイムでモニタリングします。CloudWatch を使用してメトリクスを収集および追跡できます。メトリクスとは、リソースやアプリケーションについて測定できる変数です。

CloudWatch の使用

CloudWatch は 基本的にメトリクスリポジトリです。AWS のサービス (Amazon EC2 など) は、メトリクスをリポジトリに置き、これらのメトリクスを基に統計を取得します。独自のカスタムメトリクスをリポジトリに置いた場合も、それらのメトリクスを基に統計を取得できます。詳細については、「CloudWatch メトリクスの使用」(CloudWatch ドキュメント) を参照してください。

ユーザーに代わってアクションを自動的に開始するアラームを設定することもできます。アラームは、指定した期間の単一のメトリクスを監視し、一定期間のしきい値に対するメトリクスの値に基づいて、1 つ以上の指定されたアクションを実行します。例えば、アラームは Amazon Simple Notification Service (Amazon SNS) トピックに通知を送信します。アラームはダッシュボードに追加することもできます。詳細については、「CloudWatch アラームの使用」(CloudWatch ドキュメント) を参照してください。

CloudWatch コンソールには、使用しているすべての AWS のサービス に関するメトリクスが自動的に表示されます。追加のカスタムダッシュボードを作成して、アプリケーションのメトリクスとアラームを表示できます。詳細については、「CloudWatch ダッシュボードの使用」(CloudWatch ドキュメント) を参照してください。

CloudWatch は自動的にクロスリージョン機能をサポートします。追加のステップを実行しなくても、単一のアカウントで異なる AWS リージョン からのメトリクスを、同じグラフやダッシュボードに表示できます。クロスアカウントのオブザーバビリティ (CloudWatch ドキュメント) を実装することで、クロスアカウント機能を実現できます。

CloudWatch を使用して AWS クラウド にワークロードを記録し、監視する方法の詳細とガイダンスについては、「Amazon CloudWatch を使用したロギングとモニタリングの設計と実装」(AWS 規範ガイダンス) を参照してください。

CloudWatch のユースケース

- アプリケーションのヘルスモニタリング – CloudWatch ServiceLens は、トレース、メトリクス、ログ、アラーム、およびその他のリソースヘルス情報を 1 か所に統合することで、サービスとアプリケーションのオブザーバビリティを強化します。ServiceLens は CloudWatch を AWS X-Ray と統合して、アプリケーションのエンドツーエンドのビューを提供し、パフォーマンスのボトルネックをより効率的に特定して、影響を受けるユーザーを特定するのに役立ちます。詳細については、「ServiceLens を使用したアプリケーションのヘルスモニタリング」(CloudWatch ドキュメント) を参照してください。
- 模擬モニタリング – CloudWatch Synthetics を使用することで、スケジュールに沿って実行される設定可能なスクリプトである canary を作成し、エンドポイントと API を監視できます。Canary は顧客と同じルートをたどり、同じアクションを実行します。これにより、アプリケーションに顧客トラフィックがない場合でも、顧客エクスペリエンスを継続的に検証できます。Canary はエンドポイントの可用性とレイテンシーをチェックし、読み込み時間のデータと UI のスクリーンショットを保存できます。Synthetics は REST API、URL、ウェブサイトのコンテンツを監視し、フィッシング、コードインジェクション、クロスサイトスクリプティングによる不正な変更をチェックできます。詳細については、「模擬モニタリングの使用」(CloudWatch ドキュメント) を参照してください。。
- ユーザーモニタリング – CloudWatch RUM を使用すると、実際のユーザーモニターリングを実行し、ウェブアプリケーションのパフォーマンスに関するクライアント側データを収集して、表示することができます。このデータには、ページのロード時間、クライアント側のエラー、ユーザー行動が含まれます。収集されたデータは、クライアント側で発生するパフォーマンスの問題をすばやく特定し、デバッグを行う際に利用できます。詳細については、「CloudWatch RUM の使用」(CloudWatch ドキュメント) を参照してください。
- 異常な動作の検出 – メトリクスの異常検出を有効にすると、CloudWatch は統計アルゴリズムと機械学習アルゴリズムを適用します。これらのアルゴリズムは、システムやアプリケーションのメトリクスを継続的に分析し、正常なベースラインを決定して、異常を検出します。詳細については、「CloudWatch 異常検出の使用」(CloudWatch ドキュメント) を参照してください。
- 機能の検証と A/B 実験 – Amazon CloudWatch Evidently を使用すると、機能のロールアウト中に指定した割合のユーザーに新機能を提供することで、新機能を安全に検証できます。また、A/B 実験を実行して、証拠とデータに基づいて機能の設計を決定することもできます。詳細については、

「CloudWatch Evidently での起動と A/B 実験を実行する」(CloudWatch ドキュメント) を参照してください。

Amazon CloudWatch Logs を使用したアプリケーションのロギングとモニタリング

Amazon CloudWatch Logs により、使用中のすべてのシステム、アプリケーション、AWS のサービス からのログを、スケーラビリティに優れた単一のサービスで一元管理できます。これにより、ログを簡単に表示したり、特定のエラーコードやパターンを検索したり、特定のフィールドに基づいてフィルタリングしたり、将来の分析のために安全にアーカイブしたりできます。すべてのログイベントを、ソースにかかわらず時系列で並べられた単一の一貫したイベントフローとして表示できます。クエリを実行してログイベントを並べ替えたり、特定のフィールドでログイベントをグループ化したり、カスタム計算を作成したり、ダッシュボードでログデータを可視化したりできます。

CloudWatch Logs の使用

CloudWatch Logs では、ログイベントはログストリームおよびロググループに整理されます。ログストリームは、同じソースを共有する一連のログイベントです。より具体的には、ログストリームは一般的に、モニタリングされているアプリケーションインスタンスやリソースから送信された順序でイベントを表すものです。ロググループは、保持、モニタリング、アクセス制御に関して同じ設定を共有する、1 つ以上のログストリームを定義します。各ログストリームは、1 つ以上のロググループに属している必要があります。詳細については、「ロググループとログストリームの操作」(CloudWatch Logs ドキュメント) を参照してください。

CloudWatch Logs Insights を使用すると、Amazon CloudWatch Logs のログデータを検索し、分析することができます。クエリを実行することで、運用上の問題に効率的かつ効果的に対応できます。問題が発生した場合は、CloudWatch Logs Insights を使用して、潜在的な原因を特定し、デプロイされた修正を検証することができます。詳細については、「CloudWatch Logs Insights を使用したログデータの分析」(CloudWatch Logs ドキュメント) を参照してください。

1 つまたは複数のメトリクスフィルターを作成することで、CloudWatch Logs で受信するログデータを検索およびフィルタリングできます。メトリクスフィルタは CloudWatch Logs に送信されたログデータを検索するための語句とパターンを定義します。CloudWatch Logs は、これらのメトリクスフィルタを使用して、ログデータを数値の CloudWatch メトリクスに変換し、グラフを作成したり、アラームを設定したりできます。詳細については、「フィルターを使用したログイベントからのメトリクスの作成」(CloudWatch Logs ドキュメント) を参照してください。

CloudWatch Logs のユースケース

- CloudTrail Logs のモニタリング – CloudWatch にアラームを作成して、CloudTrail がキャプチャした特定の API アクティビティの通知を受け取り、通知をトラブルシューティングの実行に使用できます。詳細については、「Sending CloudTrail Events to CloudWatch Logs」(CloudTrail ドキュメント) を参照してください。
- AWS API コールのログ作成 — サードパーティのモニタリングソリューションを導入している場合は、CloudWatch Logs を使用して AWS API コールのログを作成できます。サードパーティのモニタリングサービスを設定して、このログとアプリケーションレベルの API を評価します。
- ログ保持の設定 — デフォルトでは、CloudWatch Logs のログは無期限に保持され、失効しません。ロググループごとに保持ポリシーを調整し、無期限の保持期間を維持するか、1 日間 ~ 10 年間の保持期間を選択できます。
- ログのアーカイブと保存 — CloudWatch Logs を使用して、ログデータを耐久性の高いストレージに保存できます。CloudWatch Logs エージェントは、ローテーションするログデータもローテーションしないログデータも、ログサービスに送信します。その後は、必要なときに生のログデータにアクセスできます。

VPC Flow Logs を使用したアプリケーションのロギングとモニタリング

VPC Flow Logs は Amazon Virtual Private Cloud (Amazon VPC) の機能で、VPC のネットワークインターフェイスとの間で送受信される IP トラフィックに関する情報をキャプチャするのに役立ちます。

VPC Flow Logs の使用

仮想プライベートクラウド (VPC)、サブネット、ネットワークインターフェイスのフローログを作成できます。サブネットまたは VPC のフローログを作成する場合、そのサブネットまたは VPC 内の各ネットワークインターフェイスが監視されます。詳細については、「フローログの使用」(Amazon VPC ドキュメント) を参照してください。

監視対象ネットワークインターフェイスのフローログデータは、フローログレコードとして記録されます。フローログレコードは、VPC のネットワークフローを表します。デフォルトでは、各レコードは、集約間隔内に発生するネットワーク IP トラフィックフローをキャプチャします。各レコードは、スペースで区切られたフィールドから成る文字列です。送信元、送信先、プロトコルなど、レコードには IP フローのさまざまなコンポーネントの値が含まれています。フローログを作成すると

きは、フローログレコードのデフォルトの形式を使用するか、カスタム形式を指定できます。詳細については、「フローログレコードの例」(Amazon VPC ドキュメント) を参照してください。

フローログは以下の情報をキャプチャしません。

- Amazon Domain Name System (DNS) サーバー接続時にインスタンスによって生成されるトラフィック。独自の DNS サーバーを使用する場合は、その DNS サーバーへのすべてのトラフィックが記録されます。
- Amazon Windows ライセンスのアクティベーション用に Windows インスタンスによって生成されたトラフィック。
- インスタンスメタデータ用に 254.169.254 との間で送受信されるトラフィック。
- Amazon Time Sync Service 用に 254.169.123 との間で送受信されるトラフィック。
- Dynamic Host Configuration Protocol (DHCP) のトラフィック。
- デフォルト VPC ルーターの予約済み IP アドレスへのトラフィック。
- エンドポイントのネットワークインターフェイスと Network Load Balancer のネットワークインターフェイスの間のトラフィック。

フローログデータは、Amazon CloudWatch Logs を含む複数の AWS のサービス に発行できます。フローログを作成したら、設定したロググループの CloudWatch Logs でフローログレコードを取得し、表示できます。詳細については、「CloudWatch Logs へのフローログの発行」(Amazon VPC ドキュメント) を参照してください。

フローログデータはネットワークトラフィックのパスの外で収集されるため、ネットワークのスループットやレイテンシーには影響しません。ネットワークパフォーマンスに影響を与えるリスクなしに、フローログを作成または削除できます。

VPC Flow Logs のユースケース

- 過度に制限の厳しいセキュリティグループルールを診断する
- アプリケーションインスタンスに到達するトラフィックを監視する
- トラフィックの方向を決定する

AWS X-Ray を使用したアプリケーションのロギングとモニタリング

AWS X-Ray は、アプリケーションが処理するリクエストに関するデータを収集するとともに、データを表示、フィルタリングし、データからインサイトを取得することによって、問題や最適化の機会を特定します。

X-Ray の使用

AWS X-Ray は、アプリケーションからトレースを受信します。X-Ray と統合されている場合は、アプリケーションが使用する AWS のサービス からトレースを受信します。X-Ray は、アプリケーションコンポーネントを通過するリクエストをサービスグラフでサンプリングして可視化します。X-Ray はリクエストが複数のコンポーネントを流れるときに、トレース識別子を生成して相関させることができるため、リクエストをエンドツーエンドで表示できます。注釈とメタデータを含めることにより、リクエストの特性を一意に検索して識別できるようにすることで、この機能をさらに強化できます。

X-Ray を使用して、アプリケーションの各サーバーまたはエンドポイントを設定することをお勧めします。X-Ray は、X-Ray サービスを呼び出すことによって、アプリケーションコードに実装されます。X-Ray は、X-Ray に自動的にデータを送信するインストルメント化クライアントなど、複数の言語に対応した AWS SDK を提供します。X-Ray SDK は、他のサービス (HTTP、MySQL、PostgreSQL、MongoDB など) への呼び出しに使用される共通ライブラリへのパッチを提供します。

詳細については、「Tracing applications with AWS X-Ray」(AWS 規範ガイダンス) を参照してください。

X-Ray のユースケース

- アプリケーションの分析とデバッグ — トレースデータは、リクエストのエンドツーエンドのビューを提供することでアプリケーションをデバッグし、ボトルネックの特定や問題のトラブルシューティングを可能にします。X-Ray サービスマップは、エラーの発生箇所、レイテンシーの高い接続、失敗したリクエストのトレースを特定するのに役立つビジュアルツールです。
- パフォーマンスの分析 – Analytics コンソールは、トレースデータを解釈して、アプリケーションやその基盤となるサービスのパフォーマンスをすばやく把握するためのインタラクティブなツールです。コンソールは、トレースの調査、分析、可視化に役立ちます。また、さまざまな条件のトレースセットを比較して、根本原因を分析することもできます。

よくある質問

現在利用しているモニタリングサービスは利用できますか?

Amazon CloudWatch は、DevOps エンジニア、開発者、サイト信頼性エンジニア (SRE)、ITマネージャー、アプリケーション所有者向けに構築された、モニタリングおよびオブザーバビリティサービスです。このサービスは、データと実用的なインサイトを利用して、アプリケーションのモニタリング、システム全体のパフォーマンスの変化への対応、リソース使用率の最適化を支援します。ただし、すでに確立されたモニタリングサービスがある場合は、それと置き換える必要はありません。

ログファイルの改ざんを防止する方法はありますか?

ログファイルの整合性検証を有効にできます。ログは専用の AWS アカウント で管理および保存し、アカウントへのアクセスは制限することを推奨します。詳細については、このガイドの「CloudTrail の使用」を参照してください。

アプリケーションごとに別々のログファイルを保持する必要はありますか?

いいえ、複数のアプリケーションのログデータを同じログファイルに統合できます。ただし、各アプリケーションに対する一意の識別子を、必ずログストリームに記録するようにします。

リソース

AWSドキュメント

- AWS CloudTrail ドキュメント
- AWS クラウドWatch ドキュメント
- AWS クラウドWatch Logs ドキュメント
- Amazon VPC フローログのドキュメント
- AWS X-Ray ドキュメント
- Designing and implementing logging and monitoring with Amazon CloudWatch (AWS 規範ガイダンス)

AWS マーケティング

- AWS CloudTrail
- Amazon CloudWatch
- AWS での統合ログ管理 (AWS ソリューション)
- モニタリングとオブザーバビリティ (AWS クラウドオペレーション)
- How to Monitor your Applications Effectively (AWS スタートアップ)

ドキュメント履歴

このガイドは、このドキュメントの大きな変更点をまとめたものです。今後の更新に関する通知を受け取る場合は、RSS フィードをサブスクライブできます。

変更	説明	日付
初版発行	—	2023 年 1 月 6 日

AWS 規範的ガイダンスの用語集

以下は、 AWS 規範的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: オンプレミスの Oracle データベースを AWS クラウドの Oracle 用 Amazon Relational Database Service (Amazon RDS) に移行します。
- 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: AWS クラウドの EC2 インスタンスでオンプレミスの Oracle データベースを Oracle に移行します。
- 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。この移行シナリオは、オンプレミス環境と 間の仮想マシン (VM) の互換性とワークロードの移植性 AWSをサポートする VMware Cloud on に固有のものです AWS。 AWSのVMware Cloud にインフラを移行する際、オンプレミスのデータセンターから VMware Cloud Foundation のテクノロジーを使用することができます。例: Oracle データベースをホストするハイパーバイザーを VMware Cloud on に再配置します 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

「原子性、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。アクティブ/パッシブ移行よりも柔軟ですが、より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

行のグループを操作し、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)

組織がクラウドに正常に移行 AWS するための効率的で効果的な計画を立てるのに役立つ、 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。 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編成します。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

個人または組織に混乱や損害を与えることを目的としたボット。

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。エンディアンネス 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は 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は他の環境 (グリーン) で実行します。この戦略は、影響を最小限に抑えながら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インタラクション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、個人や組織に混乱を与えたり、損害を与えたりすることを意図しているものがあります。

ボットネット

マルウェアに感染し、ボットのヘルダーまたはボットオペレーター と呼ばれる、単一関係者の管理下にあ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、「ブランチについて (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

例外的な状況や承認されたプロセスを通じて、ユーザーが通常アクセス許可を持たない AWS アカウント にすばやくアクセスできるようになります。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」インジケータを参照してください。 AWS

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低速かつ増分的なリリース。確信できたら、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 ワークロードに負荷をかけ、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 を受信する前に、ローカルでデータを暗号化します。

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 の投稿」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 AWS クラウドに移行する際に通常実行する 4 つのフェーズ：

- 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、 クラウド AWS 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。移行戦略とどのように関連しているかについては、 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 AWS CodeCommit。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、 はオンプレミスのカメラネットワークに CV を追加するデバイス AWS Panorama を提供し、Amazon SageMaker は CV 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、設定は想定した状態から変わります。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

一元化された管理とガバナンスにより、分散され分散された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、期待されるネットワークから信頼できるリソースにアクセスしていることを確認できます。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、クエリや分析によく使用されます。

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。

defense-in-depth

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、 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。例えば、 defense-in-depth 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。

デプロイメント

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の追跡。例えば、 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を与える可能性のあ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。

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。

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 (アカウンティング、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 の中央テーブル。事業運営に関する定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 種類の列が含まれます。

フェイルファスト

頻繁で段階的なテストを使用して開発ライフサイクルを短縮する哲学。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向上させる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です。詳細については、AWS 「障害分離境界」を参照してください。

機能ブランチ

「ブランチ」を参照してください。

特徴量

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

特徴量重要度

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

機能変換

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

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のではなく、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。

G

Geo Blocking

「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)

Amazon では CloudFront、特定の国のユーザーがコンテンツディストリビューションにアクセスできないようにするオプションです。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。

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 AWS Security Hub、GuardDuty、Amazon Inspector AWS Trusted Advisor、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。

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。緊急性のため、通常、修正は一般的な DevOps リリースワークフローの外で行われます。

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、または変更するのではなく、本番ワークロード用の新しいインフラストラクチャをデプロイするモデル。イミュータブルなインフラストラクチャは、本質的にミュータブルな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「変更不可能な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、アプリケーション外からの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

接続、リアルタイムデータ、自動化、分析、AI/ML の進歩を通じて、 のビジネスプロセスのモダナイゼーションを指すために 2016 年に Klaus Schwab によって導入された用語。

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 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、「AWS を使用した機械学習モデルの解釈」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 R」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。エンディアンネス も参照してください。

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ているソフトウェア。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 がインフラストラクチャレイヤー、オペレーティングシステム、プラットフォーム AWS を運用し、ユーザーがエンドポイントにアクセスしてデータを保存および取得します。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。このソフトウェアシステムは、加工品を現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、調整の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

内の組織の一部である管理アカウント AWS アカウント を除くすべての 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の 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)

組織がクラウドへの移行のための強固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、オペレーション、ビジネスアナリストと所有者、移行エンジニア、デベロッパー、スプリントに取り組む 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には、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: Application Migration Service を使用して Amazon EC2 AWS への移行をリホストします。

Migration Portfolio Assessment (MPA)

AWS クラウド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。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されるアプローチ。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、「」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、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

「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。

変更可能な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 Framework 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および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「運用準備状況レビュー (ORR)」を参照してください。

運用テクノロジー (OT)

産業運用、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 トランスフォーメーションの主要な焦点です。

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

の組織 AWS アカウント 内のすべての のすべてのイベントをログ AWS CloudTrail 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、 ドキュメントの「組織の証跡の作成」を参照してください。 CloudTrail

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から、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)

では CloudFront、Amazon Simple Storage Service (Amazon S3) コンテンツを保護するためのアクセスを制限するための拡張オプションです。OAC は、すべての のすべての S3 バケット AWS リージョン、 AWS KMS (SSE-KMS) によるサーバー側の暗号化、および 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)

では CloudFront、Amazon S3 コンテンツを保護するためのアクセスを制限するオプションです。OAI を使用する場合、 は Amazon S3 が認証できるプリンシパル CloudFront を作成します。認証されたプリンシパルは、特定の CloudFront ディストリビューションを介してのみ S3 バケット内のコンテンツにアクセスできます。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

「運用技術」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る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

アクセス許可の定義 (アイデンティティベースのポリシー を参照) 、アクセス条件の指定 (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の定義 AWS Organizations (サービスコントロールポリシー を参照) が可能なオブジェクト。

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。`false`通常は `WHERE`句にあります。

述語のプッシュダウン

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 ロール AWS アカウント、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

エンジニアリングプロセス全体を通してプライバシーを考慮に入れた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

非準拠のリソースのデプロイを防止する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「 での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。

プログラミング可能ロジックコントローラー (NAL)

製造では、マシンをモニタリングし、承認プロセスを自動化する、信頼性が高く、適応性の高いコンピュータです。

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。例えば、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、情報 (RACI) 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。

再構築

「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 とは分離され、独立しています。詳細については、AWS リージョン 「 を使用できるアカウントを指定する」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 R」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 R」を参照してください。

プラットフォーム変更

「7 R」を参照してください。

再購入

「7 R」を参照してください。

回復性

中断に耐えたり、中断から回復したりするアプリケーションの機能。で障害耐性を計画する場合、高可用性とディザスタリカバリが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 R」を参照してください。

廃止

「7 R」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 (IdPs) が使用するオープンスタンダード。この機能により、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 にログイン AWS

Management Console したり、組織内のすべてのユーザーを IAM で作成しなくても 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収集」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

では AWS Secrets Manager、暗号化された形式で保存される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「シークレット」を参照してください。

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。これらのオートメーションは、セキュリティのベストプラクティスの実装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、認証情報のローテーションなどがあります。

サーバー側の暗号化

送信先にあるデータの、それを受け取る AWS のサービス による暗号化。

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)

システムを中断させる可能性のあるアプリケーションの単一の重要なコンポーネントの障害。

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。

split-and-seed 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。

star スキーマ

トランザクションデータまたは測定データを保存するために 1 つの大きなファクトテーブルを使用し、データ属性を保存するために 1 つ以上の小さなディメンションテーブルを使用するデータベースの組織構造。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生産オペレーション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

ユーザーインタラクション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。

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 と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するサービスへの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「 AWS Organizations を他の AWS のサービスで使用する AWS Organizations 」を参照してください。

チューニング

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

ツーピザチーム

2 つのピザを食べることができる小さな 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

「書き込み 1 回」を参照し、多くの を読み取ります。

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な 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。

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。