



でのサイバー脅威インテリジェンスの共有 AWS

AWS 規範ガイドンス



AWS 規範ガイド: でのサイバー脅威インテリジェンスの共有 AWS

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスは Amazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

序章	1
CTI 共有モデル	3
クラウドのセキュリティ	3
クラウド内のセキュリティ	4
CTI アーキテクチャ	5
脅威インテリジェンスプラットフォームのデプロイ	7
CTI の取り込み	8
セキュリティコントロールの自動化	8
Amazon GuardDuty	11
Amazon Route 53 Resolver DNS ファイアウォール	13
AWS Network Firewall	14
可視性の取得	16
ネットワークトラフィックのログ記録	16
でのセキュリティ検出結果の一元化 AWS	17
AWS セキュリティデータと他のエンタープライズデータの統合	19
CTI の共有	19
次のステップ	21
AWS リソース	21
AWS のサービス ドキュメント	21
STIX リソース	22
脅威インテリジェンスプラットフォーム	22
寄稿者	23
オーサリング	23
レビュー	23
テクニカルライティング	23
ドキュメント履歴	24
用語集	25
#	25
A	26
B	29
C	31
D	34
E	38
F	40

G	42
H	43
I	44
L	47
M	48
O	52
P	55
Q	58
R	58
S	61
T	65
U	66
V	67
W	67
Z	68
.....	lxx

でのサイバー脅威インテリジェンスの共有 AWS

アマゾン ウェブ サービス ([寄稿者](#))

2024 年 12 月 ([ドキュメント履歴](#))

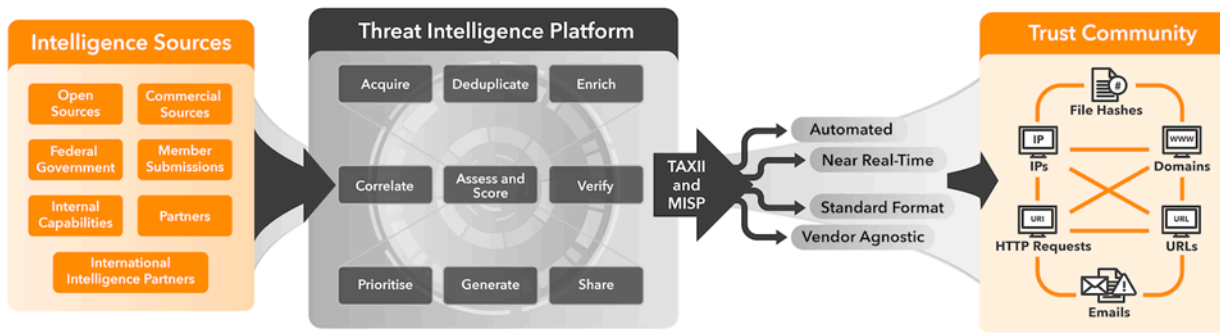
新しいリスクが発生すると、重要なクラウドワークロードを保護するためのベストプラクティスが継続的に進化します。保護を必要とするインターネットに接続されたアセットの数が増えるにつれて、脅威アクターに関連するセキュリティイベントのリスクも増加します。サイバー脅威インテリジェンス (CTI) は、脅威アクターの意図、機会、能力を示すデータの収集と分析です。これは証拠ベースで実用的なもので、サイバー防衛活動に役立ちます。多くの場合、アクター属性、戦術の手法と手順、動機、またはターゲットに関する情報が含まれます。

CTI は、組織内、信頼コミュニティ内の組織間、情報共有分析センター (ISACs)、または政府機関などの他のエンティティと共有できます。政府機関の例としては、[オーストラリアサイバーセキュリティセンター \(ACSC\)](#) や米国 [サイバーセキュリティインフラストラクチャセキュリティ局 \(CISA\)](#) などがあります。

あらゆる形式のインテリジェンスと同様に、脅威コンテキストは重要です。CTI 共有は、動的なサイバーセキュリティリスク管理に役立ちます。タイムリーなサイバーセキュリティの防御、対応、復旧に不可欠です。これにより、サイバーセキュリティ機能の効率と有効性が向上します。脅威コンテキストは、さまざまなターゲットに関連する CTI 機能要件を区別するためにも不可欠です。たとえば、高度なアクターは特定の企業や政府をターゲットにし、コモディティアクターはすぐに利用できるツールや手法を使用して個人や組織を広範囲に攻撃する可能性があります。

セキュリティ計画、オペレービリティ、脅威インテリジェンス分析、セキュリティコントロールの自動化、信頼コミュニティ内での共有は、脅威インテリジェンスライフサイクルの重要な部分です。AWS 手動のセキュリティタスクを自動化して、脅威をより正確に検出し、より迅速に対応し、共有できる高品質の脅威インテリジェンスを生成します。新しいサイバー攻撃を発見し、分析して、CTI を生成し、共有して、適用できます。これらはすべて、2 回目の攻撃の発生を防ぐように設計された速度です。

このガイドでは、脅威インテリジェンスプラットフォームを にデプロイする方法について説明します AWS。信頼コミュニティは CTI を提供し、プラットフォームはそれを取り込み、実用的なインテリジェンスを特定し、AWS 環境内の保護コントロールと検出コントロールを自動化します。次の図は、脅威インテリジェンスのライフサイクルを示しています。CTI はソースから到着し、脅威インテリジェンスプラットフォームによって処理されます。 [Trusted Automated Exchange of Intelligence Information \(TAXII\)](#) プロトコルまたは [Malware Information Sharing Platform \(MISP\)](#) を使用することで、CTI はアクションのために信頼コミュニティと共有されます。



脅威インテリジェンスプラットフォームは CTI を使用して、AWS 環境にセキュリティコントロールを自動的に実装するか、手動アクションが必要な場合はセキュリティチームに通知します。予防的コントロールは、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です。例としては、ネットワークファイアウォール、DNS リゾルバー、その他の侵入防止システム (IPSs) を使用して、既知の不正な IP アドレスまたはドメイン名のリストをブロックする自動化などがあります。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たセキュリティコントロールです。例としては、悪意のあるアクティビティの継続的なモニタリングや、問題やイベントの証拠のログの検索などがあります。

検出結果は、などの一元化されたセキュリティオブザーバビリティツールに集約できます [AWS Security Hub CSPM](#)。その後、結果を信頼コミュニティと共有して、包括的な脅威の全体像を共同で構築できます。

CTI 共有の責任共有モデル

[AWS 責任共有モデル](#)は、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 と責任を共有する方法を定義します。は、クラウドのセキュリティと呼ばれる AWS クラウド、 で提供されるすべてのサービスを実行するインフラストラクチャ AWS を保護します。データやアプリケーションなど、これらのサービスの使用を保護するのはお客様の責任です。これはクラウドのセキュリティと呼ばれます。

クラウドのセキュリティ

セキュリティが最優先事項です AWS。セキュリティ問題が組織を中断させないように努めています。インフラストラクチャとお客様のデータの保護に取り組む中で、グローバルスケールのインサイトを使用して、お客様の自動保護に役立つ大量のセキュリティインテリジェンスを大規模かつリアルタイムで収集します。可能な限り、AWS およびそのセキュリティシステムは、そのアクションが最も影響を与える脅威を中断します。多くの場合、この作業はバックグラウンドで行われます。

AWS クラウド インフラストラクチャ全体で毎日、破壊的でコストがかかる可能性のある何百ものサイバー攻撃を検出し、正常に阻止しています。これらの重要だがほとんど目に見えない成功は、センサーのグローバルネットワークと関連する一連の中断ツールによって達成されます。これらの機能を使用すると、ネットワークやインフラストラクチャに対するサイバー攻撃の実行がより困難で高価になります。

AWS は、クラウドプロバイダーの中で最大のパブリックネットワークフットプリントを備えています。これにより、インターネット上の特定のアクティビティに関する比類のないリアルタイムのインサイトが得られます AWS。 [MadPot](#) は、脅威センサー (ハニーポットと呼ばれる) のグローバルに分散されたネットワークです。MadPot は、AWS セキュリティチームが攻撃者の戦術と手法を理解するのに役立ちます。攻撃者が脅威センサーの 1 つをターゲットにしようとする、AWS はデータを収集して分析します。

Sonarix は、AWS がネットワークトラフィックの分析に使用するもう 1 つの内部ツールです。多数のアカウントとリソースにアクセスするための不正な試みを特定して停止します。2023 年 5 月から 2024 年 4 月の間、Sonarix は Amazon Simple Storage Service (Amazon S3) に保存されている顧客データのスキャンを 240 億回以上拒否しました。また、Amazon Elastic Compute Cloud (Amazon EC2) で実行されている脆弱なワークロードを検出する試みが約 2.6 兆回行われなくなりました。

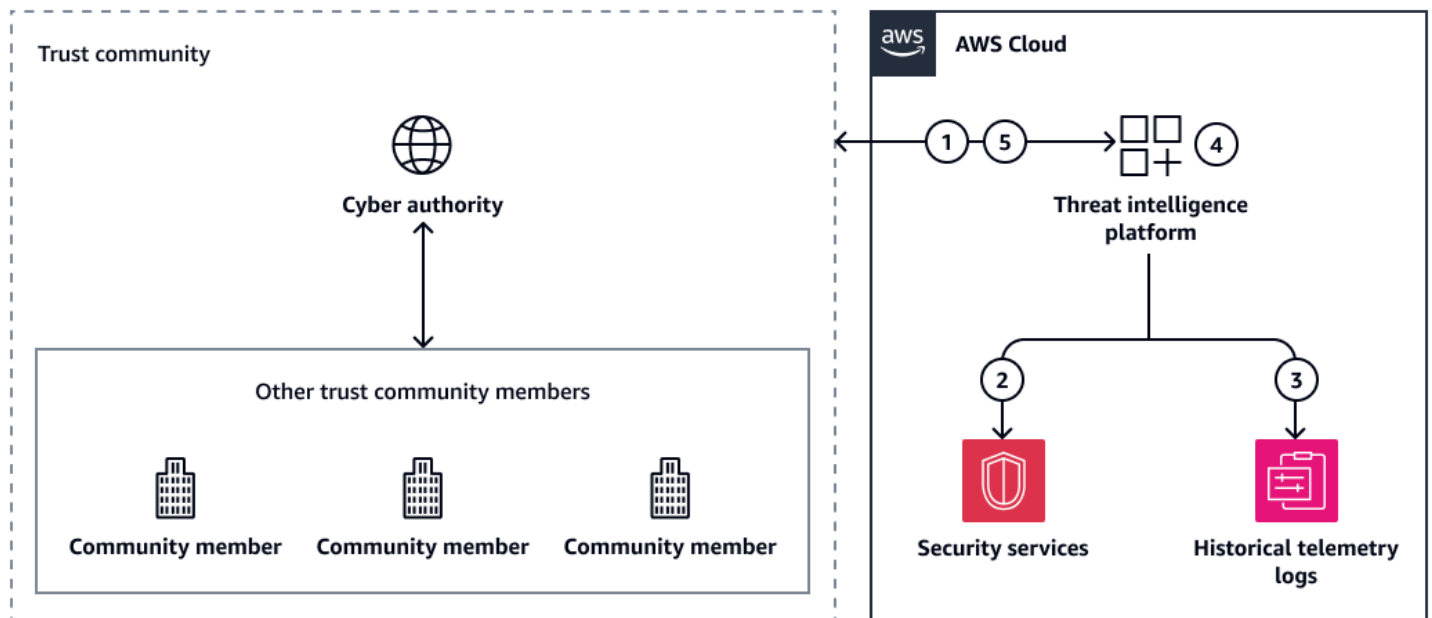
クラウド内のセキュリティ

このガイドは、のサイバー脅威インテリジェンス (CTI) のベストプラクティスに焦点を当てています AWS クラウド。お客様は、ローカライズされたコンテキスト化された CTI を生成する責任があります。データの保存場所、保護方法、アクセスできるユーザーを制御します。AWS には、ログ記録、モニタリング、監査データに対する可視性がないため、クラウド内の CTI ベースのセキュリティに不可欠です。

[構造化脅威情報表現 \(STIX\)](#) は、CTI の交換に使用されるオープンソースの言語およびシリアル化形式です。ファイルハッシュ、ドメイン、URLs、HTTP リクエスト、IP アドレスなどのインジケータは、脅威をブロックするために共有する重要な出力です。ただし、効果的なアクションは、確実性評価や侵入セットの相関関係などの追加のインテリジェンスに依存します。STIX 2.1 は、攻撃パターン、一連のアクション、脅威アクター、地理的位置、マルウェア情報など、18 [の STIX ドメインオブジェクト](#) を定義します。また、脅威インテリジェンスプラットフォームが収集する大量のデータのノイズからのシグナルをエンティティが判断するのに役立つ、信頼度評価や関係などの概念も紹介します。環境内の脅威に関するこのレベルの詳細を検出、分析、共有できます AWS。詳細については、このガイドの「[予防的および検出的なセキュリティコントロールの自動化](#)」を参照してください。

でのサイバー脅威インテリジェンスアーキテクチャ AWS

次の図は、脅威フィードを使用してサイバー脅威インテリジェンス (CTI) を AWS 環境に統合するための一般的なアーキテクチャを示しています。CTI は、の脅威インテリジェンスプラットフォーム AWS クラウド、選択したサイバーセキュリティ機関、およびその他の信頼コミュニティのメンバー間で共有されます。



次のワークフローが表示されます。

1. 脅威インテリジェンスプラットフォームは、サイバー当局または他の信頼コミュニティのメンバーから実用的な CTI を受け取ります。
2. 脅威インテリジェンスプラットフォームは AWS、セキュリティサービスをタスクしてイベントを検出および防止します。
3. 脅威インテリジェンスプラットフォームは、 から脅威インテリジェンスを受け取ります AWS のサービス。
4. イベントが発生した場合、脅威インテリジェンスプラットフォームは新しい CTI をキュレートします。
5. 脅威インテリジェンスプラットフォームは、新しい CTI をサイバー当局と共有します。CTI を他の信頼コミュニティのメンバーと共有することもできます。

CTI フィードを提供するサイバー機関は多数あります。例としては、[オーストラリアサイバーセキュリティセンター \(ACSC\)](#)、英国国家サイバーセキュリティセンターが提供する [Connect Inform Share Protect \(CISP\)](#) プログラム、ニュージーランド政府通信セキュリティ局が提供する [Malware Free Networks \(MFN\)](#) プログラムなどがあります。多くの AWS パートナーは CTI 共有フィードも提供しています。

CTI 共有を開始するには、以下を実行することをお勧めします。

1. [脅威インテリジェンスプラットフォームのデプロイ](#) – 複数のソースからさまざまな形式で脅威インテリジェンスデータを取り込み、集約し、整理するプラットフォームをデプロイします。
2. [サイバー脅威インテリジェンスの取り込み](#) – 脅威インテリジェンスプラットフォームを 1 つ以上の脅威フィードプロバイダーと統合します。脅威フィードを受け取ったら、脅威インテリジェンスプラットフォームを使用して新しい CTI を処理し、環境内のセキュリティオペレーションに関連する実用的なインテリジェンスを特定します。可能な限り自動化しますが、ヒューman-in-the-loop 決定が必要な状況がいくつかあります。
3. [予防的および検出的なセキュリティコントロールの自動化](#) – 予防的および検出的なコントロールを提供するアーキテクチャのセキュリティサービスに CTI をデプロイします。これらのサービスは、一般的に侵入防止システム (IPS) と呼ばれます。では AWS、サービス APIs を使用して、脅威フィードで提供される IP アドレスとドメイン名からのアクセスを拒否するブロックリストを設定します。
4. [オブザーバビリティメカニズムによる可視性の取得](#) – 環境でセキュリティオペレーションが実行されている間、新しい CTI を収集しています。たとえば、脅威フィードに含まれていた脅威や、侵入に関連する侵害の兆候 ([ゼロデイエクスプロイト](#)など) が見られる場合があります。脅威インテリジェンスを一元化することで、環境全体の状況認識が向上し、既存の CTI と新しく検出された CTI を 1 つのシステムで確認できるようになります。
5. [CTI を信頼コミュニティと共有する](#) – CTI 共有ライフサイクルを完了するには、独自の CTI を生成して信頼コミュニティに共有し直します。

次の動画、[Scaling Cyber Threat Intelligence Sharing with the AUS Cyber Security Center](#) では、これらのステップについて詳しく説明します。この動画では、オーストラリアサイバーセキュリティセンターの CTI 共有機能について説明しますが、選択した脅威フィードや場所に関係なく手順は同じです。

脅威インテリジェンスプラットフォームのデプロイ

脅威インテリジェンスプラットフォームは、複数のソースからさまざまな形式で脅威インテリジェンスデータを取り込み、集約し、整理します。これにより、アナリストは信頼コミュニティから受け取ったサイバー脅威インテリジェンス (CTI) を表示、優先順位付け、対応できます。

[OpenCTI](#) と [MISP](#) は、一般的なオープンソースの脅威インテリジェンスプラットフォームです。また、の AWS パートナーから利用できるソリューションもあります [AWS Marketplace](#)。脅威インテリジェンスプラットフォームを選択するときは、セキュリティチームのスキルレベルを考慮する必要があります。MISP は強力でありながら複雑であり、OpenCTI にはより直感的なユーザーインターフェイスがあります。

脅威インテリジェンスプラットフォームを選択するときは、次の点を考慮してください。

- 機能 — プラットフォームには、リアルタイムモニタリング、脅威検出、分析などの機能がありますか？
- データソース — プラットフォームは、脅威フィード、ダークウェブインテリジェンス、ソーシャルメディア、オープンソースインテリジェンスなど、さまざまなソースを使用していますか？
- データ品質 — プラットフォームには、情報が正確で信頼できることを確認するプロセスがありますか？
- スケーラビリティ — プラットフォームは、成長や進化する脅威など、組織の変化するニーズに適応できますか？
- 統合 — プラットフォームは既存のセキュリティツールやインフラストラクチャと統合できますか？
- ユーザーエクスペリエンス — プラットフォームの操作と使用は簡単ですか？
- カスタマイズ — プラットフォームは組織固有のニーズに合わせてカスタマイズできますか？
- コスト — ライセンスコストやメンテナンス要件など、プラットフォームは費用対効果が高いですか？

Virtual Private Cloud (VPC) 内に脅威インテリジェンスプラットフォームをデプロイできます。Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに直接デプロイすることも、Amazon Elastic Container Service (Amazon ECS) やなどのコンテナテクノロジーを使用してデプロイすることもできます AWS Fargate。最新のアプリケーション開発に適した AWS コンテナサービスの選択の詳細については、[AWS 「コンテナサービスの選択」](#) を参照してください。

サイバー脅威インテリジェンスの取り込み

取り込みプロセスの最初のステップは、サイバー脅威インテリジェンス (CTI) データを脅威フィードから脅威インテリジェンスプラットフォームが取り込むことができる形式に変換することです。これは CTI 変換と呼ばれます。脅威フィードデータは、[構造化脅威情報式 \(STIX\)](#) など、さまざまな形式で取得できます。受信データを、AWS 環境で使用しているセキュリティ製品に適した予測可能で簡単に使用できる形式に再構築する必要があります。

互換性を最大限に高めるために、データを JSON 形式に変換することをお勧めします。たとえば、JSON 形式のデータを [AWS Step Functions](#) で消費でき、自動化ワークフローはこの形式をより簡単かつ一貫して消費できます。自動ワークフローの構築の詳細については、次のセクション「[予防的および検出的なセキュリティコントロールの自動化](#)」を参照してください。

CTI データの取り込みを高速化するために、データ変換を自動化できます。データは取り込み時に変換され、脅威インテリジェンスプラットフォームに直接渡されます。AWS Lambda 関数を使用して変換を完了し、AWS Step Functions や [Amazon EventBridge](#) AWS のサービスなどのを通じてプロセスをオーケストレーションできます。

CTI を取り込むときに、抽出して保持する属性を選択できます。必要な詳細の正確な量は、ビジネスニーズによって異なります。ただし、ファイアウォールやその他のセキュリティサービスを更新するには、次の最小属性をお勧めします。

- IP アドレスとドメイン
- 脅威
- 内部脅威リストへの追加または削除

使用する属性を抽出し、構造化された JSON テンプレートにフォーマットします。

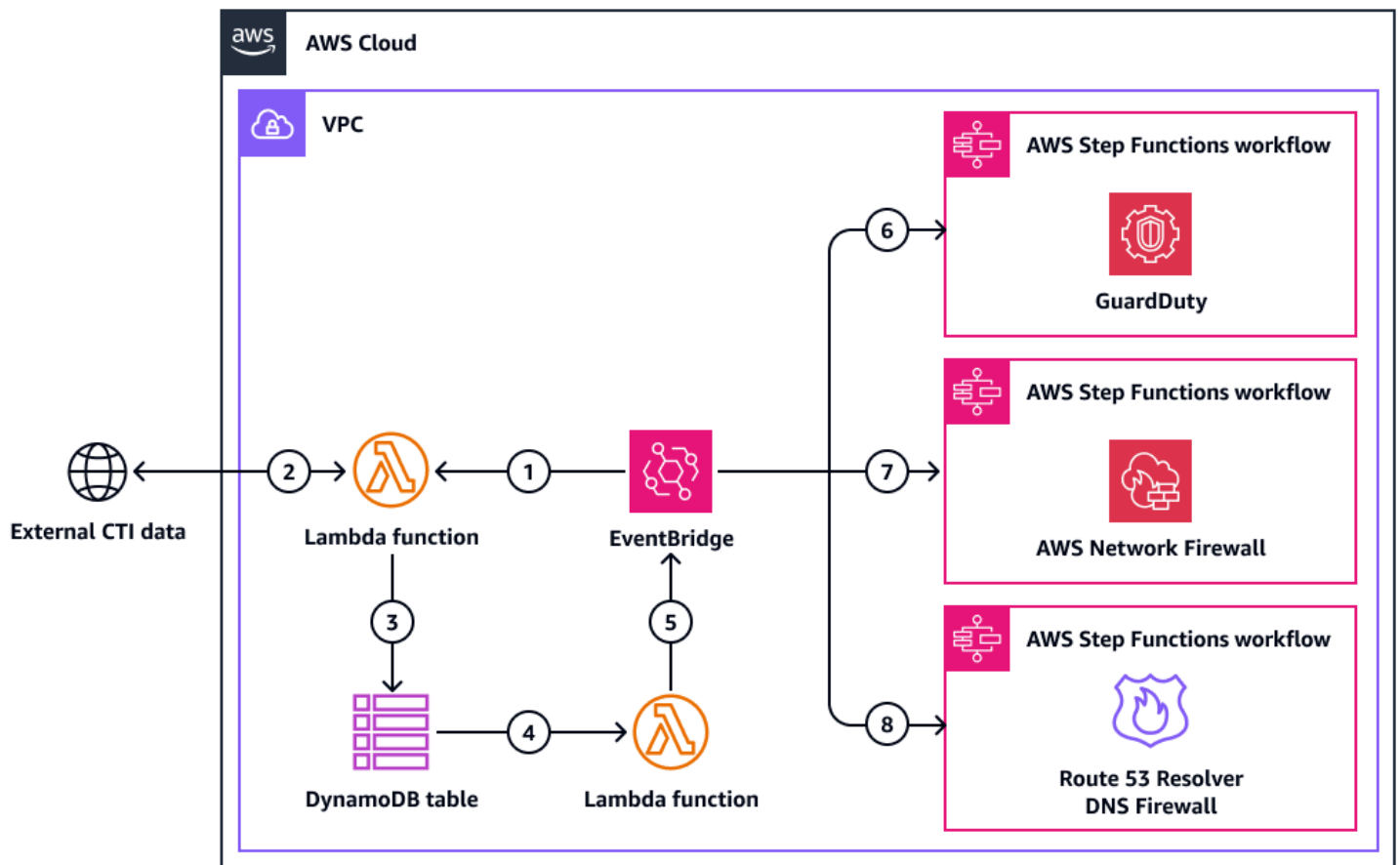
予防的および検出的なセキュリティコントロールの自動化

サイバー脅威インテリジェンス (CTI) が脅威インテリジェンスプラットフォームに取り込まれたら、データに応じて設定変更を行うプロセスを自動化できます。脅威インテリジェンスプラットフォームは、サイバー脅威インテリジェンスを管理し、環境を観察するのに役立ちます。サイバー脅威に関する技術情報と非技術情報を構築、保存、整理、視覚化する機能を提供します。これらは、脅威の全体像を構築し、さまざまなインテリジェンスソースを組み合わせ、[高度な永続脅威 \(APT\)](#) などの脅威をプロファイリングおよび追跡するのに役立ちます。

自動化により、脅威インテリジェンスの受信から環境の設定変更の実装までの時間を短縮できます。すべての CTI レスポンスを自動化できるわけではありません。ただし、できるだけ多くのレスポンスを自動化すると、セキュリティチームが残りの CTI をタイムリーに優先順位付けして評価するのに役立ちます。各組織は、自動化できる CTI レスポンスのタイプと手動分析が必要な CTI レスポンスを決定する必要があります。この決定は、リスク、アセット、リソースなどの組織のコンテキストに基づいて行います。例えば、既知の不正なドメインや IP アドレスのブロックを自動化することを選択する組織もありますが、内部 IP アドレスをブロックする前にアナリストの調査が必要になる場合があります。

このセクションでは、[Amazon GuardDuty](#)、[AWS Network Firewall](#)、[Amazon Route 53 Resolver DNS Firewall](#) で自動 CTI レスポンスを設定する方法の例を示します。これらの例は、互いに独立して実装できます。組織のセキュリティ要件とニーズに基づいて意思決定を行います。[AWS Step Functions](#) ワークフロー (ステートマシンとも呼ばれます) AWS のサービスを使用して、の設定変更を自動化できます。[AWS Lambda](#) 関数が CTI から JSON 形式への変換を完了すると、Step Functions ワークフローを開始する [Amazon EventBridge](#) イベントがトリガーされます。

次の図は、アーキテクチャの例を示しています。Step Functions ワークフローは、GuardDuty の脅威リスト、Route 53 Resolver DNS Firewall のドメインリスト、Network Firewall のルールグループを自動的に更新します。



この図は、次のワークフローを示しています。

1. EventBridge イベントは定期的を開始されます。このイベントは AWS Lambda 関数を開始します。
2. Lambda 関数は、外部脅威フィードから CTI データを取得します。
3. Lambda 関数は、取得した CTI データを Amazon DynamoDB テーブルに書き込みます。
4. DynamoDB テーブルにデータを書き込むと、Lambda 関数を開始する変更データキャプチャストリームイベントが開始されます。
5. 変更が発生した場合、Lambda 関数は EventBridge で新しいイベントを開始します。変更が行われなかった場合、ワークフローは完了します。
6. CTI が IP アドレスレコードに関連する場合、EventBridge は Amazon GuardDuty の脅威リストを自動的に更新する Step Functions ワークフローを開始します。詳細については、このセクションの [Amazon GuardDuty](#) を参照してください。
7. CTI が IP アドレスまたはドメインレコードに関連する場合、EventBridge はルールグループを自動的に更新する Step Functions ワークフローを開始します AWS Network Firewall。詳細については、このセクションの [AWS Network Firewall](#) を参照してください。

8. CTI がドメインレコードに関連する場合、EventBridge は DNS Firewall Amazon Route 53 Resolver でドメインリストを自動的に更新する Step Functions ワークフローを開始します。詳細については、このセクション [Amazon Route 53 Resolver の「DNS Firewall」](#) を参照してください。

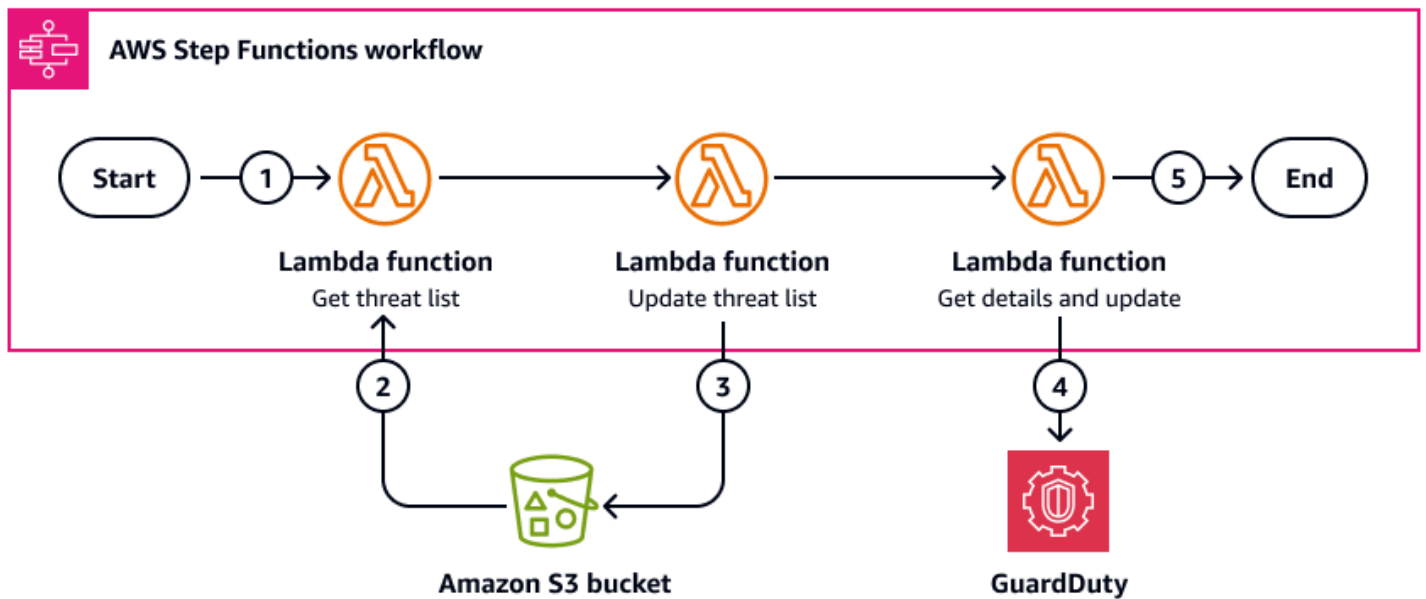
Amazon GuardDuty

[Amazon GuardDuty](#) は、AWS アカウント および ワークロードの不正なアクティビティを継続的にモニタリングし、可視性と修復のための詳細なセキュリティ検出結果を提供する脅威検出サービスです。CTI フィードから GuardDuty 脅威リストを自動的に更新することで、ワークロードにアクセスしている可能性のある脅威に関するインサイトを得ることができます。GuardDuty は検出制御機能を向上させます。

Tip

GuardDuty は ネイティブに統合されます [AWS Security Hub CSPM](#)。Security Hub CSPM は、 のセキュリティ状態を包括的に把握 AWS し、セキュリティ業界標準とベストプラクティスに照らして環境をチェックするのに役立ちます。GuardDuty を Security Hub CSPM と統合すると、GuardDuty の検出結果は Security Hub CSPM に自動的に送信されます。Security Hub CSPM は、セキュリティ体制の分析にこれらの検出結果を含めることができます。詳細については、GuardDuty ドキュメントの [「との統合 AWS Security Hub CSPM」](#) を参照してください。Security Hub CSPM では、 [自動化](#) を使用して検出機能と応答性の高いセキュリティコントロール機能を改善できます。

次の図は、Step Functions ワークフローが脅威フィードの CTI を使用して GuardDuty の脅威リストを更新する方法を示しています。Lambda 関数が CTI の JSON 形式への変換を完了すると、ワークフローを開始する EventBridge イベントがトリガーされます。



図表に示す内容は以下のステップです。

1. CTI が IP アドレスレコードに関連する場合、EventBridge は Step Functions ワークフローを開始します。
2. Lambda 関数は脅威リストを取得し、Amazon Simple Storage Service (Amazon S3) バケットにオブジェクトとして保存されます。
3. Lambda 関数は、脅威リストを CTI の IP アドレスの変更で更新します。これにより、脅威リストが元の Amazon S3 バケットにオブジェクトの新しいバージョンとして保存されます。オブジェクト名は変更されません。
4. Lambda 関数は API コールを使用して GuardDuty デテクター ID と脅威インテリジェンスセット ID を取得します。これらの IDs を使用して GuardDuty を更新し、脅威リストの新しいバージョンを参照します。

Note

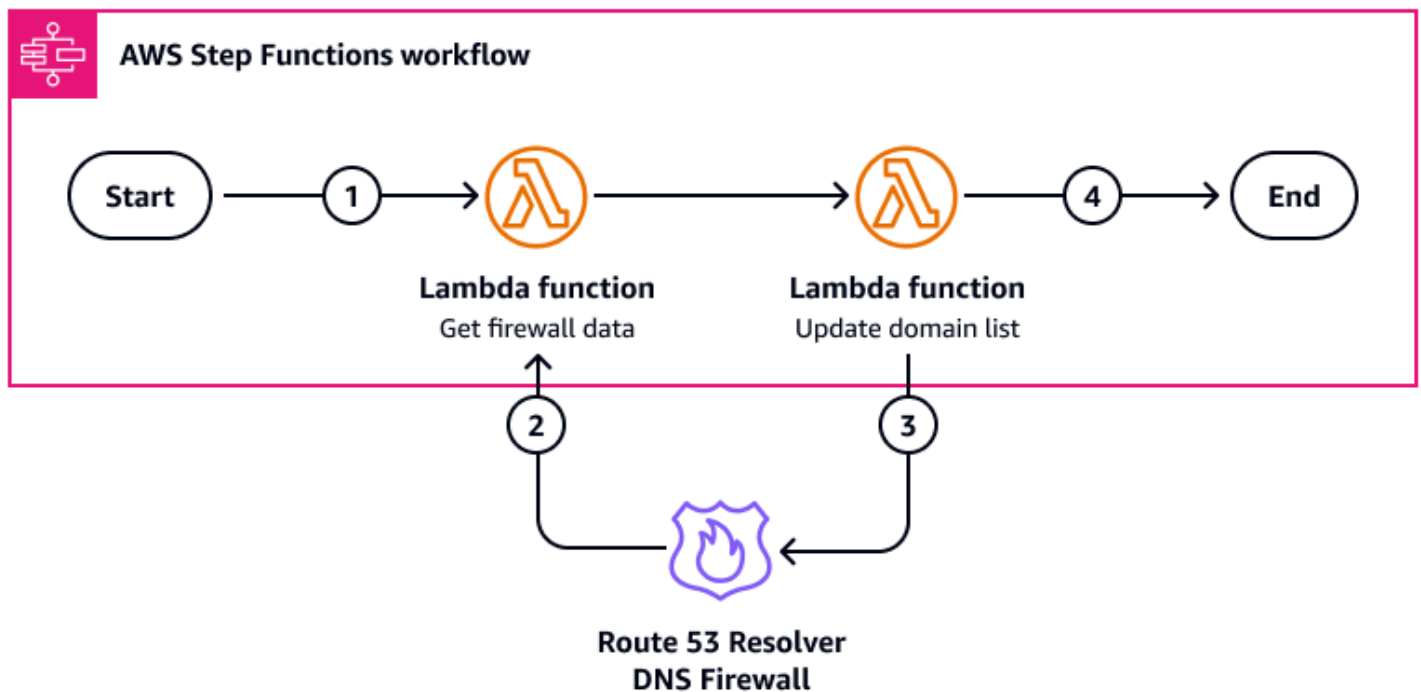
特定の GuardDuty デテクターと IP アドレスリストは配列として取得されるため、取得できません。したがって、ターゲットには各 1 つのみを含めることをお勧めします AWS アカウント。それ以上の場合は、このワークフローの最後の Lambda 関数で正しいデータが抽出されていることを確認する必要があります。

5. Step Functions ワークフローは終了します。

Amazon Route 53 Resolver DNS ファイアウォール

[Amazon Route 53 Resolver DNS Firewall](#) は、Virtual Private Cloud (VPC) のアウトバウンド DNS トラフィックをフィルタリングおよび規制するのに役立ちます。DNS Firewall では、CTI フィードによって識別されるドメインアドレスをブロックするルールグループを作成します。Step Functions ワークフローを設定して、このルールグループからドメインを自動的に追加および削除します。

次の図は、Step Functions ワークフローが脅威フィードの CTI を使用して DNS Firewall Amazon Route 53 Resolver のドメインリストを更新する方法を示しています。Lambda 関数が CTI の JSON 形式への変換を完了すると、ワークフローを開始する EventBridge イベントがトリガーされます。



図表に示す内容は以下のステップです。

1. CTI がドメインレコードに関連する場合、EventBridge は Step Functions ワークフローを開始します。
2. Lambda 関数は、ファイアウォールのドメインリストデータを取得します。この Lambda 関数の作成の詳細については、AWS SDK for Python (Boto3) ドキュメントの「[get_firewall_domain_list](#)」を参照してください。
3. Lambda 関数は、CTI と取得されたデータを使用してドメインリストを更新します。この Lambda 関数の作成の詳細については、Boto3 ドキュメントの [update_firewall_domains](#) を参照してください。Lambda 関数は、ドメインを追加、削除、または置き換えることができます。

4. Step Functions ワークフローは終了します。

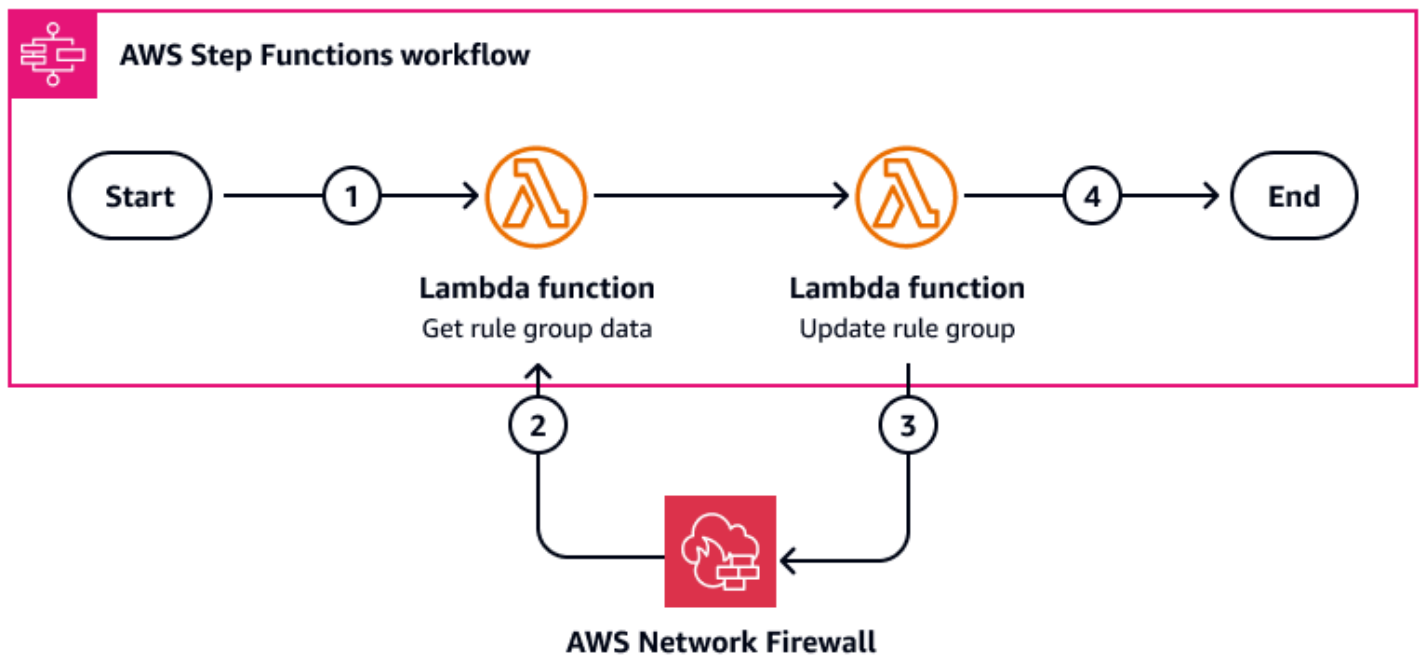
推奨されるベストプラクティスを以下に示します:

- Route 53 Resolver DNS Firewall と の両方を使用することをお勧めします AWS Network Firewall。DNS Firewall は DNS トラフィックをフィルタリングし、Network Firewall は他のすべてのトラフィックをフィルタリングします。
- DNS Firewall のログ記録を有効にすることをお勧めします。ログデータをモニタリングし、制限されたドメインがファイアウォール経由でトラフィックを送信しようとする警告を検出コントロールを作成できます。詳細については、[Amazon CloudWatch を使用した Route 53 Resolver DNS Firewall ルールグループのモニタリング](#)」を参照してください。

AWS Network Firewall

[AWS Network Firewall](#) は、 の 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。VPC の境界でトラフィックをフィルタリングし、脅威をブロックするのに役立ちます。脅威インテリジェンスフィードを使用して Network Firewall ルールグループを自動的に更新すると、組織のクラウドワークロードとデータを悪意のある攻撃者から保護できます。

次の図は、Step Functions ワークフローが脅威フィードの CTI を使用して Network Firewall の 1 つ以上のルールグループを更新する方法を示しています。Lambda 関数が CTI の JSON 形式への変換を完了すると、ワークフローを開始する EventBridge イベントがトリガーされます。



図表に示す内容は以下のステップです。

1. CTI が IP アドレスまたはドメインレコードに関連する場合、EventBridge は、Network Firewall のルールグループを自動的に更新する Step Functions ワークフローを開始します。
2. Lambda 関数は、Network Firewall からルールグループデータを取得します。
3. Lambda 関数は CTI を使用してルールグループを更新します。IP アドレスまたはドメインを追加または削除します。
4. Step Functions ワークフローは終了します。

推奨されるベストプラクティスを以下に示します:

- Network Firewall には、複数のルールグループを含めることができます。ドメインと IP アドレス用に個別のルールグループを作成します。
- Network Firewall のログ記録を有効にすることをお勧めします。ログデータをモニタリングし、制限されたドメインまたは IP アドレスがファイアウォール経由でトラフィックを送信しようとすると警告する検出コントロールを作成できます。詳細については、「[からのネットワークトラフィックのログ記録 AWS Network Firewall](#)」を参照してください。
- Route 53 Resolver DNS Firewall と の両方を使用することをお勧めします AWS Network Firewall。DNS Firewall は DNS トラフィックをフィルタリングし、Network Firewall は他のすべてのトラフィックをフィルタリングします。

オブザーバビリティメカニズムによる可視性の取得

発生したセキュリティイベントを表示する機能は、適切なセキュリティコントロールを確立するのと同じくらい重要です。AWS Well-Architected フレームワークのセキュリティの柱では、検出のベストプラクティスとして、[Configure service and application logging](#) and [Capture logs, findings, and metrics in standardized locations](#) があります。これらのベストプラクティスを実装するには、イベントを識別し、その情報を人間が消費可能な形式、理想的には一元的な場所に処理するのに役立つ情報を記録する必要があります。

このガイドでは、[Amazon Simple Storage Service \(Amazon S3\)](#) を使用してログデータを一元化することをお勧めします。Amazon S3 は、AWS Network Firewall と DNS Firewall Amazon Route 53 Resolver の両方のログストレージをサポートしています。次に、[AWS Security Hub CSPM](#) と [Amazon Security Lake](#) を使用して、Amazon GuardDuty の検出結果やその他のセキュリティの検出結果を1つの場所に一元化します。

ネットワークトラフィックのログ記録

このガイドの「[予防的および検出的なセキュリティコントロールの自動化](#)」セクションでは、と Amazon Route 53 Resolver DNS Firewall を使用して AWS Network Firewall サイバー脅威インテリジェンス (CTI) への対応を自動化する方法について説明します。これらのサービスの両方のログ記録を設定することをお勧めします。ログデータをモニタリングし、制限されたドメインまたは IP アドレスがファイアウォール経由でトラフィックを送信しようとする警告を検出コントロールを作成できます。

これらのリソースを設定するときは、個々のログ記録要件を考慮してください。例えば、Network Firewall のログ記録は、ステートフルルールエンジンに転送するトラフィックに対してのみ使用できます。ゼロトラストモデルに従い、すべてのトラフィックをステートフルルールエンジンに転送することをお勧めします。ただし、コストを削減する場合は、組織が信頼するトラフィックを除外できません。

Network Firewall と DNS Firewall はどちらも Amazon S3 へのログ記録をサポートしています。これらのサービスのログ記録の設定の詳細については、「[からのネットワークトラフィックのログ記録 AWS Network Firewall](#)」および「[DNS Firewall のログ記録の設定](#)」を参照してください。どちらのサービスでも、を使用して Amazon S3 バケットへのログ記録を設定できます AWS マネジメントコンソール。

でのセキュリティ検出結果の一元化 AWS

[AWS Security Hub CSPM](#) は、のセキュリティ状態を包括的に把握し、セキュリティ業界標準とベストプラクティスに照らして AWS 環境を評価するのに役立ちます。Security Hub CSPM は、セキュリティコントロールに関連付けられた検出結果を生成できます。また、Amazon GuardDuty AWS のサービスなどの他の から結果を受け取ることもできます。Security Hub CSPM を使用して、全体、およびサポートされているサードパーティー製品からの結果 AWS アカウント AWS のサービスとデータを一元化できます。統合の詳細については、[Security Hub CSPM ドキュメントの「Security Hub CSPM の統合について」](#)を参照してください。

Security Hub CSPM には、セキュリティ問題の優先順位付けと修復に役立つ自動化機能も含まれています。たとえば、自動化ルールを使用して、セキュリティチェックが失敗した場合に重要な検出結果を自動的に更新できます。Amazon EventBridge との統合を使用して、特定の検出結果への自動応答を開始することもできます。詳細については、[Security Hub CSPM ドキュメントの「Security Hub CSPM の検出結果を自動的に変更して処理する」](#)を参照してください。

Amazon GuardDuty を使用する場合は、検出結果を Security Hub CSPM に送信するように GuardDuty を設定することをお勧めします。Security Hub CSPM は、セキュリティ体制の分析にこれらの検出結果を含めることができます。詳細については、GuardDuty ドキュメントの [「との統合 AWS Security Hub CSPM」](#)を参照してください。

Network Firewall と Route 53 Resolver DNS Firewall の両方で、ログ記録するネットワークトラフィックからカスタム検出結果を作成できます。[Amazon Athena](#) は、標準 SQL を使用して Amazon S3 でデータを直接分析するのに役立つ対話型のクエリサービスです。Amazon S3 のログをスキャンし、関連するデータを抽出するクエリを Athena で作成できます。手順については、Athena ドキュメントの [「開始方法」](#)を参照してください。次に、AWS Lambda 関数を使用して関連するログデータを [AWS Security Finding 形式 \(ASFF\)](#) に変換し、結果を Security Hub CSPM に送信できます。Network Firewall から Security Hub CSPM の検出結果にログデータを変換する Lambda 関数の例を次に示します。

```
import { SecurityHubClient, BatchImportFindingsCommand, GetFindingsCommand } from
"@aws-sdk/client-securityhub";

export const handler = async(event) => {
  const date = new Date().toISOString();

  const config = {
    Region: REGION
  };
```

```
const input = {
  Findings: [
    {
      SchemaVersion: '2018-10-08',
      Id: ALERTLOGS3BUCKETID,
      ProductArn: FIREWALLMANAGERARN,
      GeneratorId: 'alertlogs-to-findings',
      AwsAccountId: ACCOUNTID,
      Types: 'Unusual Behaviours/Network Flow/Alert',
      CreatedAt: date,
      UpdatedAt: date,
      Severity: {
        Normalized: 80,
        Product: 8
      },
      Confidence: 100,
      Title: 'Alert Log to Findings',
      Description: 'Network Firewall Alert Log into Finding - add
        top level dynamic detail',
      Resources: [
        {
          /*these are custom resources. Contain deeper details of your event
here*/
          firewallName: 'Example Name',
          event: 'Example details here'
        }
      ]
    }
  ]
};

const client = new SecurityHubClient(config);
const command = new BatchImportFindingsCommand(input);
const response = await client.send(command);
return { statusCode: 200, response };
};
```

Security Hub CSPM に情報を抽出して送信するためのパターンは、個々のビジネスニーズによって異なります。定期的なスケジュールでデータを送信する必要がある場合は、EventBridge を使用してプロセスを開始できます。情報の追加時にアラートを受信する場合は、[Amazon Simple Notification Service \(Amazon SNS\)](#) を使用できます。このアーキテクチャには多くの方法があるため、ビジネスニーズを満たすように適切に計画することが重要です。

AWS セキュリティデータと他のエンタープライズデータの統合

[Amazon Security Lake](#) は、統合された およびサードパーティーのサービスからのセキュリティ関連のログ AWS のサービス とイベントデータの収集を自動化できます。また、保存とレプリケーションの設定をカスタマイズできるため、データのライフサイクル管理にも役立ちます。Security Lake は、取り込んだデータを Apache Parquet 形式と OCSF (OCSF) と呼ばれる標準のオープンソーススキーマに変換します。OCSF サポートにより、Security Lake は のセキュリティデータと幅広いエンタープライズセキュリティデータソースを正規化 AWS し、組み合わせます。他の AWS のサービスやサードパーティーのサービスが Security Lake に保存されているデータをサブスクライブして、インシデント対応やセキュリティデータ分析を行うことができます。

Security Hub CSPM から結果を受信するように Security Lake を設定できます。この統合をアクティブ化するには、両方のサービスを有効にし、Security Lake のソースとして Security Hub CSPM を追加する必要があります。これらの手順を完了すると、Security Hub CSPM はすべての検出結果を Security Lake に送信し始めます。Security Lake は、Security Hub CSPM の検出結果を自動的に正規化し、OCSF に変換します。Security Lake では、Security Hub CSPM の検出結果を使用するサブスクライバーを 1 人以上追加できません。詳細については、Security Lake ドキュメントの「[との統合 AWS Security Hub CSPM](#)」を参照してください。

次の動画 [AWS re:Inforce 2024 - Cyber Threat Intelligence Sharing on AWS](#) では、Security Hub CSPM と Security Lake の統合を使用して CTI を共有する方法について説明します。

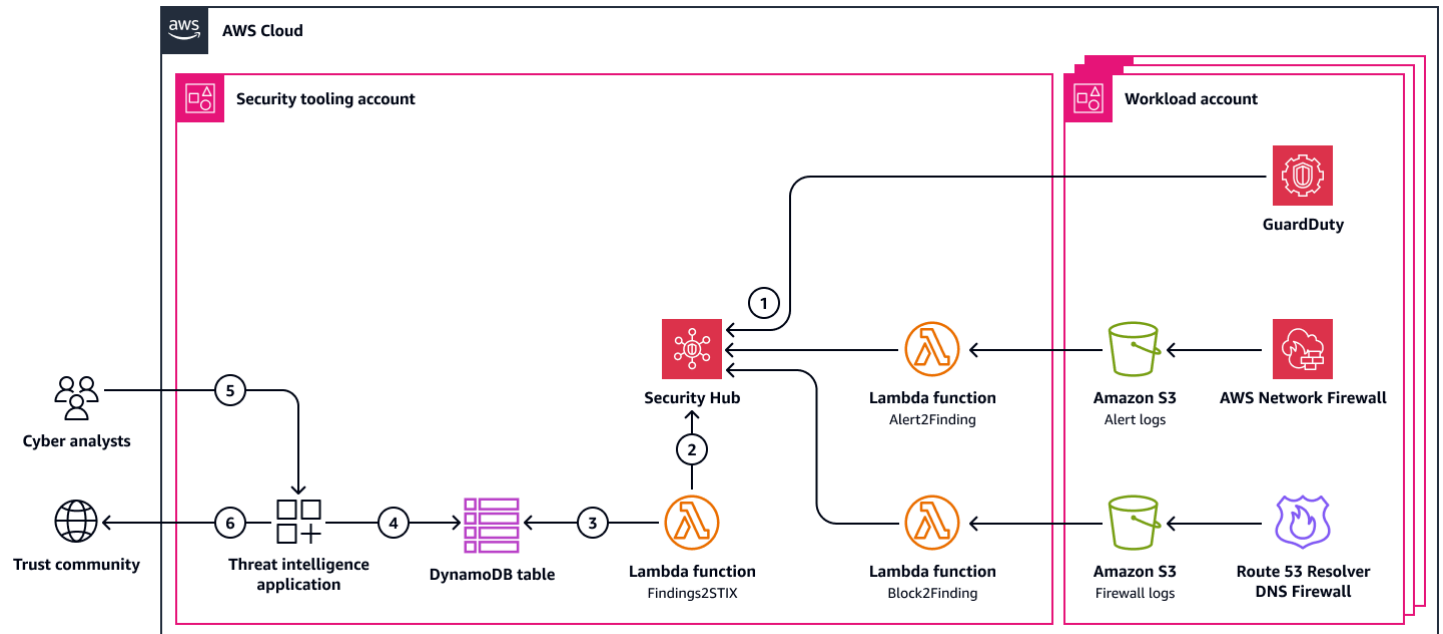
CTI を信頼コミュニティと共有する

サイバー脅威インテリジェンス (CTI) を送信するコミュニティは通常、CTI を受け取るコミュニティと同じです。ただし、共有先を増やすこともできます。例えば、国のサイバーセキュリティセンターや情報共有分析センター (ISACs) など、信頼できる政府または規制機関と共有することを選択できます。目標は、複数の組織からの結果をプールすることで、CTI を迅速に伝播して実装することです。脅威インテリジェンスプラットフォームは、複数のフィードと共有するための API 統合を管理します。

信頼コミュニティへの CTI の送信は、予防的コントロールと検出的コントロールの実装と同時に行われます。ログを使用して、セキュリティイベントを識別します。次に、イベントと検出結果を一元化して、 のセキュリティ体制の概要をすばやく把握できるようにします AWS アカウント。その後、サイバーアナリストなどのセキュリティチームが、価値のある情報を特定できます。にすでに検出結果があるため AWS Security Hub CSPM、これらの検出結果を JSON や STIX などの脅威フィードで使用される形式に変換できます。次に、CTI をフィードプロバイダーに送信します。脅威イン

脅威インテリジェンスプラットフォームは、指定した CTI を取り込み、匿名化し、検証します。その後、CTI はより広範なコミュニティと共有されます。

次の図は、AWS のサービスを使用して CTI を生成し、サイバーセキュリティ機関やその他のコミュニティメンバーを含む信頼コミュニティと共有する方法を示しています。



この図は、次のワークフローを示しています。

1. 検出結果は に作成されます AWS Security Hub CSPM。
2. AWS Lambda 関数は Security Hub CSPM から検出結果を取得し、JSON や STIX などの共有可能な形式に変換します。
3. Lambda 関数は、検出結果を Amazon DynamoDB テーブルに保存します。
4. Amazon Elastic Compute Cloud (Amazon EC2) または Amazon Elastic Container Service (Amazon ECS) で実行されているサードパーティーの脅威インテリジェンスプラットフォームは、DynamoDB テーブルから検出結果を取得します。
5. サイバーアナリストは、脅威インテリジェンスプラットフォームの CTI を確認します。
6. 脅威インテリジェンスプラットフォームは、他の CTI プロデューサーとコンシューマーで構成される信頼コミュニティに CTI を発行します。

次のステップとリソース

組織のアセット、セクター、脅威環境を考慮してください。これらの要因は、サイバー脅威インテリジェンスの共有に参加することを選択した信頼コミュニティに通知する必要があります。世界中の多くのサイバー機関が脅威インテリジェンスフィードを提供しています。オファーの内容を検討し、組織のユースケースに最適なものを選択します。このガイドをモジュラーアプローチとして使用し、組織に合わせてカスタマイズします。

以下の追加リソースを確認することをお勧めします。これらのリソースは、AWS 環境に脅威インテリジェンスプラットフォームを構築またはデプロイし、サイバー脅威インテリジェンス共有を設定するのに役立ちます。

AWS リソース

- [AWS アーキテクチャセンター](#)
- [AWS re:Inforce 2024 - でのサイバー脅威インテリジェンスの共有 AWS \(ビデオ\)](#)
- [AWS Summit ANZ 2023: AUS Cyber Security Center とのサイバー脅威インテリジェンス共有のスクリーニング \(ビデオ\)](#)

AWS のサービス ドキュメント

- [Amazon DynamoDB ドキュメント](#)
- [Amazon EventBridge ドキュメント](#)
- [Amazon GuardDuty ドキュメント](#)
- [「AWS Lambda ドキュメント」](#)
- [AWS Network Firewall ドキュメント](#)
- [Amazon Route 53 Resolver DNS Firewall ドキュメント](#)
- [「AWS Security Hub CSPM ドキュメント」](#)
- [Amazon Security Lake のドキュメント](#)
- [Amazon Simple Storage Service \(Amazon S3\) ドキュメント](#)
- [AWS Step Functions ドキュメント](#)

STIX リソース

- [STIX 2.1 の例](#)
- [悪意のある URL のインジケータ](#)

脅威インテリジェンスプラットフォーム

- [OpenCTI](#)
- [MISP](#)

寄稿者

以下の個人がこのガイドに貢献しました。

オーサリング

- Jess Modini、シニア技術者、AWS
- Alexa Donovan、Associate Solutions Architect、AWS
- Steven Ryan、パートナーソリューションアーキテクト、AWS
- セキュリティソリューションアーキテクト、バイロン・ポグソン AWS

レビュー

- Brian Farnhill、シニアソフトウェア開発エンジニア、AWS
- Marc Luescher、シニアソリューションアーキテクト、AWS
- Stefan Mijic、セキュリティ保証スペシャリスト、AWS
- Timothy Woodill、パブリックセクターソリューションアーキテクト、AWS

テクニカルライティング

- " AbouHarb、シニアテクニカルライター、AWS

ドキュメント履歴

以下の表は、本ガイドの重要な変更点について説明したものです。今後の更新に関する通知を受け取る場合は、[RSS フィード](#) をサブスクライブできます。

変更	説明	日付
初版発行	—	2024 年 12 月 12 日

AWS 規範ガイドの用語集

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

数字

7 Rs

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

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

- 廃止 — お客様のソース環境で不要になったアプリケーションを停止または削除します。

A

A2A (Agent-to-Agent)

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

ABAC

「[属性ベースのアクセス制御](#)」をご覧ください。

抽象化されたサービス

「[マネージドユーザー](#)」をご覧ください。

ACID

「[原子性、一貫性、分離性、耐久性 \(ACID\)](#)」をご覧ください。

アクティブ/アクティブ移行

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

アクティブ/パッシブ移行

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

[エージェント]

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

エージェントオペレーション

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

集計関数

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

AI

[「人工知能」](#)をご覧ください。

AIOps

[「AI オペレーション」](#)をご覧ください。

匿名化

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

アンチパターン

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

アプリケーション制御

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

アプリケーションポートフォリオ

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

人工知能 (AI)

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

AI オペレーション (AIOps)

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

非対称暗号化

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

原子性、一貫性、分離性、耐久性 (ACID)

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

属性ベースのアクセス制御 (ABAC)

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

信頼できるデータソース

最も信頼性のある情報源とされるデータのプライマリ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。

アベイラビリティゾーン (AZ)

他のアベイラビリティゾーンの障害から 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ためのガイダンスを提供します。詳細については、[AWS CAF ウェブサイト](#)と [AWS CAF のホワイトペーパー](#) を参照してください。

AWS ワークロード認定フレームワーク (AWS WQF)

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

B

不正なボット

個人や組織に混乱や損害を与えることを目的とした[ボット](#)。

BCP

「[ビジネス継続性計画 \(BCP\)](#)」をご覧ください。

動作グラフ

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

ビッグエンディアンシステム

最上位バイトを最初に格納するシステム。「[エンディアン性](#)」もご覧ください。

二項分類

バイナリ結果 (2 つの可能なクラスのうちの一つ) を予測するプロセス。例えば、お客様の機械学習モデルで「この E メールはスパムですか、それともスパムではありませんか」などの問題を予測する必要があるかもしれません。または「この製品は書籍ですか、車ですか」などの問題を予測する必要があるかもしれません。

ブルームフィルター

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

ブルー/グリーンデプロイ

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

ボット

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

ボットネット

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

ブランチ

コードリポジトリに含まれる領域。リポジトリに最初に作成するブランチは、メインブランチといます。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なら、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。

ブレイクグラスアクセス

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なります。詳細については、AWS Well-Architected ガイドの「[ブレイクグラス手順の実装](#)」インジケータを参照してください。

ブラウн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н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нフィールド戦略と[グリーンフィールド](#)戦略を融合させることもできます。

バッファキャッシュ

アクセス頻度が最も高いデータが保存されるメモリ領域。

ビジネス能力

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

ビジネス継続性計画 (BCP)

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

C

CAF

「[AWS クラウド導入フレームワーク](#)」を参照してください。

カナリアデプロイ

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

CCoE

「[Cloud Center of Excellence](#)」を参照してください。

CDC

「[変更データキャプチャ](#)」を参照してください。

変更データキャプチャ (CDC)

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

カオスエンジニアリング

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

CI/CD

「[継続的インテグレーションと継続的デリバリー](#)」を参照してください。

分類

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

シチズンデベロッパー

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

クライアント側の暗号化

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

Cloud Center of Excellence (CCoE)

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

クラウドコンピューティング

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

クラウド運用モデル

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

導入のクラウドステージ

組織が、AWS クラウドへの移行時に通常実行する 4 つの段階。

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

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

CMDB

「[構成管理データベース \(CMDB\)](#)」を参照してください。

コードリポジトリ

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

コールドキャッシュ

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

コールドデータ

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

コンピュータビジョン (CV)

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

設定ドリフト

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

構成管理データベース (CMDB)

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

コンフォーマンスパック

コンプライアンスチェックとセキュリティチェックをカスタマイズするためにアセンブルできる AWS Config ルールと修復アクションのコレクション。YAML テンプレートを使用して、コンフォーマンスパックを AWS アカウント および リージョンの単一のエンティティとしてデプロイ

することも、組織全体にデプロイすることもできます。詳細については、AWS Config ドキュメントの「[コンフォーマンスパック](#)」を参照してください。

継続的インテグレーションと継続的デリバリー (CI/CD)

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

CV

「[コンピュータビジョン](#)」を参照してください。

D

保管中のデータ

ストレージ内にあるデータなど、常に自社のネットワーク内にあるデータ。

データ分類

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

データドリフト

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

転送中のデータ

ネットワーク内 (ネットワークリソース間など) を活発に移動するデータ。

データメッシュ

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

データ最小化

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

データ境界

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

データの前処理

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

データ出所

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

データ件名

データを収集、処理している個人。

データウェアハウス

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

データベース定義言語 (DDL)

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

データベース操作言語 (DML)

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

DDL

[「データベース定義言語」](#)を参照してください。

ディープアンサンブル

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

深層学習

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

多層防御

一連のセキュリティメカニズムとコントロールをコンピュータネットワーク全体に層状に重ねて、ネットワークとその内部にあるデータの機密性、整合性、可用性を保護する情報セキュリティの手法。この戦略を採用するときは 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で利用できるサービス](#)」を参照してください。

トラブルシューティング

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

開発環境

「[環境](#)」を参照してください。

検出管理

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

開発バリューストリームマッピング (DVSM)

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

デジタルツイン

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

ディメンションテーブル

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

ディザスタ

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

ディザスタリカバリ (DR)

[ディザスタ](#)によるダウンタイムとデータ損失を最小限に抑えるための戦略とプロセス。詳細については、AWS Well-Architected フレームワークの「[でのワークロードのディザスタリカバリ](#)」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 (ポストン: Addison-Wesley Professional, 2003)。strangler fig パターンでドメイン駆動型設計を使用す

る方法の詳細については、「[コンテナと Amazon API Gateway を使用して、従来の Microsoft ASP.NET \(ASMX\) ウェブサービスを段階的にモダナイズ](#)」を参照してください。

DR

「[ディザスタリカバリ](#)」を参照してください。

ドリフト検出

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

DVSM

「[開発バリューストリームマッピング](#)」を参照してください。

E

EDA

「[探索的データ分析](#)」を参照してください。

EDI

「[電子データ交換](#)」を参照してください。

エッジコンピューティング

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

電子データ交換 (EDI)

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

暗号化

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

暗号化キー

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

エンディアン

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

エンドポイント

「[サービスエンドポイント](#)」を参照してください。

エンドポイントサービス

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

エンタープライズリソースプランニング (ERP)

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

エンベロープ暗号化

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

環境

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

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

- 上位環境 — コア開発チーム以外のユーザーがアクセスできるすべての環境。これには、本番環境、本番前環境、ユーザー承認テスト環境などが含まれます。

エピック

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

ERP

「[エンタープライズリソース計画](#)」を参照してください。

探索的データ分析 (EDA)

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

F

ファクトテーブル

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

フェイルファスト

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

障害分離境界

では AWS クラウド、アベイラビリティゾーン 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、障害の影響を制限し、ワークロードの耐障害性を向上させるのに役立ちます。詳細については、「[AWS 障害分離境界](#)」を参照してください。

機能ブランチ

「[ブランチ](#)」を参照してください。

特徴量

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

特徴量重要度

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

機能変換

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

数ショットプロンプト

[LLM](#) に、タスクと望ましい出力を示す例を少数提示した後に、類似のタスクを実行させること。この手法は、プロンプトに記述された例 (ショット) からモデルが学習する「インコンテキスト学習」の一種です。数ショットプロンプトは、特定のフォーマット、推論、専門知識が必要なタスクに効果的です。[「ゼロショットプロンプト」](#)も参照してください。

FGAC

[「きめ細かなアクセス制御」](#)を参照してください。

きめ細かなアクセス制御 (FGAC)

複数の条件を使用してアクセス要求を許可または拒否すること。

フラッシュカット移行

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

FM

[「基盤モデル」](#)を参照してください。

基盤モデル (FM)

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

FM ゲートウェイ

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

G

生成 AI

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

ジオブロッキング

「[地理的制限](#)」を参照してください。

地理的制限 (ジオブロッキング)

特定の国のユーザーがコンテンツ配信にアクセスできないようにするための、Amazon CloudFront のオプション。アクセスを許可する国と禁止する国は、許可リストまたは禁止リストを使って指定します。詳細については、CloudFront ドキュメントの「[コンテンツの地理的ディストリビューションの制限](#)」を参照してください。

Gitflow ワークフロー

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

ゴールデンイメージ

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

グリーンフィールド戦略

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

ガードレール

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

ガードレール (AI)

[エージェント](#)の入出力をフィルタリング、検証、制約して、責任のある安全な AI の動作を確保するのに役立つ安全メカニズム。

H

HA

「[高可用性](#)」を参照してください。

異種混在データベースの移行

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

高可用性 (HA)

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

ヒストリアンのモダナイゼーション

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

ホールドアウトデータ

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

ヒューman-in-the-loop (HitL)

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

同種データベースの移行

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

ホットデータ

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

ホットフィックス

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

ハイパーケア期間

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

|

laC

「[Infrastructure as Code](#)」を参照してください。

|

ID ベースのポリシー

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

アイドル状態のアプリケーション

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

IIoT

「[インダストリアル IIoT](#)」を参照してください。

イミュータブルインフラストラクチャ

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

インバウンド (受信) VPC

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

増分移行

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

インダストリー 4.0

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

インフラストラクチャ

アプリケーションの環境に含まれるすべてのリソースとアセット。

Infrastructure as Code (IaC)

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

インダストリアル IoT (IIoT)

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

インスペクション VPC

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

IoT

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

解釈可能性

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

IoT

「[IoT](#)」を参照してください。

IT 情報ライブラリ (ITIL)

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

IT サービス管理 (ITSM)

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

ITIL

「[IT 情報ライブラリ](#)」を参照してください。

ITSM

「[IT サービス管理](#)」を参照してください。

L

ラベルベースアクセス制御 (LBAC)

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

ランディングゾーン

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

大規模言語モデル (LLM)

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

大規模な移行

300 台以上のサーバの移行。

LBAC

「[ラベルベースアクセス制御](#)」を参照してください。

最小特権

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

リフトアンドシフト

「[7 Rs](#)」を参照してください。

リトルエンディアンシステム

最下位バイトを最初に格納するシステム。「[エンディアン性](#)」もご覧ください。

LLM

「[大規模言語モデル](#)」を参照してください。

下位環境

「[環境](#)」を参照してください。

M

機械学習 (ML)

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

メインブランチ

「[ブランチ](#)」を参照してください。

マルウェア

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

マネージドサービス

AWS のサービスはインフラストラクチャレイヤー、オペレーティングシステム、プラットフォーム AWS を運用し、エンドポイントにアクセスしてデータを保存および取得します。

マネージドサービスの例として、Amazon Simple Storage Service (Amazon S3) と Amazon DynamoDB が挙げられます。このサービスは、抽象化されたサービスとも呼ばれます。

製造実行システム (MES)

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

MAP

「[Migration Acceleration Program](#)」を参照してください。

MCP

「[モデルコンテキストプロトコル](#)」を参照してください。

モデルコンテキストプロトコル (MCP)

[エージェント](#)と[ツール](#)間の通信のためのステートレスプロトコル。

MCP サーバー

[モデルコンテキストプロトコル](#)を通じて1つ以上の[ツール](#)を公開するサービス。

メカニズム

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

メンバーアカウント

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

MES

「[製造実行システム](#)」を参照してください。

Message Queuing Telemetry Transport (MQTT)

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

マイクロサービス

明確に定義された API を介して通信し、通常は小規模な自己完結型のチームが所有する、小規模で独立したサービスです。例えば、保険システムには、販売やマーケティングなどのビジネス機能、または購買、請求、分析などのサブドメインにマッピングするマイクロサービスが含まれ

場合があります。マイクロサービスの利点には、俊敏性、柔軟なスケーリング、容易なデプロイ、再利用可能なコード、回復力などがあります。詳細については、[AWS「サーバーレスサービスを使用したマイクロサービスの統合」](#)を参照してください。

マイクロサービスアーキテクチャ

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

Migration Acceleration Program (MAP)

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

大規模な移行

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

移行ファクトリー

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

移行メタデータ

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

移行パターン

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

Migration Portfolio Assessment (MPA)

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

移行準備状況評価 (MRA)

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

移行戦略

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

ML

「[機械学習](#)」を参照してください。

モダナイゼーション

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

モダナイゼーション準備状況評価

組織のアプリケーションのモダナイゼーションの準備状況を判断し、利点、リスク、依存関係を特定し、組織がこれらのアプリケーションの将来の状態をどの程度適切にサポートできるかを決定するのに役立つ評価。評価の結果として、ターゲットアーキテクチャのブループリント、モダナイゼーションプロセスの開発段階とマイルストーンを詳述したロードマップ、特定された

ギャップに対処するためのアクションプランが得られます。詳細については、「[AWS クラウドでのアプリケーションのモダナイゼーションの準備状況を評価する](#)」を参照してください。

モノリシックアプリケーション (モノリス)

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

MPA

「[Migration Portfolio Assessment](#)」を参照してください。

MQTT

「[Message Queuing Telemetry Transport](#)」を参照してください。

多クラス分類

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

ミュータブルなインフラストラクチャ

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

O

OAC

「[オリジンアクセス制御](#)」を参照してください。

OAI

「[オリジンアクセスアイデンティティ](#)」を参照してください。

OCM

「[組織変更管理](#)」を参照してください。

オフライン移行

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

OI

「[オペレーション統合](#)」を参照してください。

Ola

「[オペレーショナルレベルアグリーメント](#)」を参照してください。

オンライン移行

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

OPC-UA

「[Open Process Communications - Unified Architecture](#)」を参照してください。

Open Process Communications - Unified Architecture (OPC-UA)

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

オペレーショナルレベルアグリーメント (OLA)

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

運用準備状況レビュー (ORR)

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

運用テクノロジー (OT)

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

オペレーション統合 (OI)

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

組織の証跡

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

組織変更管理 (OCM)

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

オリジンアクセス制御 (OAC)

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

オリジンアクセスアイデンティティ (OAI)

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

ORR

「[運用準備状況レビュー](#)」を参照してください。

OT

「[運用テクノロジー](#)」を参照してください。

アウトバウンド (送信) VPC

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

P

アクセス許可の境界

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

個人を特定できる情報 (PII)

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

PII

「[個人を特定できる情報](#)」を参照してください。

プレイブック

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

PLC

「[プログラマブルロジックコントローラー](#)」を参照してください。

PLM

「[製品ライフサイクル管理](#)」を参照してください。

ポリシー

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

多言語の永続性

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

ポートフォリオ評価

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

述語

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

述語プッシュダウン

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

予防的コントロール

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

プリンシパル

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

プライバシーバイデザイン

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

プライベートホストゾーン

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

プロアクティブコントロール

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

製品ライフサイクル管理 (PLM)

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

本番環境

「[環境](#)」を参照してください。

プログラマブルロジックコントローラー (PLC)

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

プロンプトチェイニング

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

仮名化

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

発行/サブスクライブ (pub/sub)

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

Q

クエリプラン

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

クエリプランのリグレッション

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

R

RACI マトリックス

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

RAG

「[検索拡張生成](#)」を参照してください。

ランサムウェア

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

RASCI マトリックス

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

RCAC

「[行と列のアクセス制御](#)」を参照してください。

リードレプリカ

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

リアーキテクト

「[7 Rs](#)」を参照してください。

目標復旧時点 (RPO)

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

目標復旧時間 (RTO)

サービスが中断から復旧までの最大許容遅延時間。

リファクタリング

「[7 Rs](#)」を参照してください。

リージョン

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

リグレッション

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

リホスト

「[7 Rs](#)」を参照してください。

リリース

デプロイプロセスで、変更を本番環境に昇格させること。

再配置

「[7 Rs](#)」を参照してください。

リプラットフォーム

「[7 Rs](#)」を参照してください。

再購入

「[7 Rs](#)」を参照してください。

回復性

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

リソースベースのポリシー

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

実行責任者、説明責任者、協業先、報告先 (RACI) に基づくマトリックス

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

レスポンスコントロール

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

保持

「[7 Rs](#)」を参照してください。

廃止

「[7 Rs](#)」を参照してください。

検索拡張生成 (RAG)

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

ローテーション

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

行と列のアクセス制御 (RCAC)

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

RPO

「[目標復旧時点](#)」を参照してください。

RTO

「[目標復旧時間](#)」を参照してください。

ランブック

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

S

SAML 2.0

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

SCADA

「[監視制御とデータ取得](#)」を参照してください。

SCP

「[サービスコントロールポリシー](#)」を参照してください。

シークレット

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

セキュリティバイデザイン

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

セキュリティコントロール

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

セキュリティ強化

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

Security Information and Event Management (SIEM) システム

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

セキュリティレスポンスの自動化

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

サーバー側の暗号化

送信先で、それ AWS のサービスを受け取る によるデータの暗号化。

サービスコントロールポリシー (SCP)

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

サービスエンドポイント

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

サービスレベルアグリーメント (SLA)

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

サービスレベルインジケータ (SLI)

エラー率、可用性、スループットといった、サービスパフォーマンス面の指標。

サービスレベル目標 (SLO)

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

責任共有モデル

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

シャドウ AI

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

SIEM

「[Security Information and Event Management システム](#)」を参照してください。

単一障害点 (SPOF)

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

SLA

「[サービスレベルアグリーメント](#)」を参照してください。

SLI

「[サービスレベルインジケータ](#)」を参照してください。

SLO

「[サービスレベルの目標](#)」を参照してください。

スプリットアンドシードモデル

モダナイゼーションプロジェクトのスケーリングと加速のためのパターン。新機能と製品リリースが定義されると、コアチームは解放されて新しい製品チームを作成します。これにより、お

お客様の組織の能力とサービスの拡張、デベロッパーの生産性の向上、迅速なイノベーションのサポートに役立ちます。詳細については、「[AWS クラウドでのアプリケーションをモダナイズするための段階的アプローチ](#)」を参照してください。

SPOF

「[単一障害点](#)」を参照してください。

スタースキーマ

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

strangler fig パターン

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

サブネット

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

監視制御とデータ取得 (SCADA)

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

対称暗号化

データの暗号化と復号に同じキーを使用する暗号化のアルゴリズム。

合成テスト

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

システムプロンプト

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

T

タグ

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

ターゲット変数

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

タスクリスト

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

テスト環境

「[環境](#)」を参照してください。

トレーニング

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

tool

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

トランジットゲートウェイ

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

トランクベースのワークフロー

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

信頼されたアクセス

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

チューニング

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

ツーピザチーム

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

U

不確実性

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

未分化なタスク

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

上位環境

「[環境](#)」を参照してください。

V

バキューミング

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

バージョンコントロール

リポジトリ内のソースコードへの変更など、変更を追跡するプロセスとツール。

VPC ピアリング

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

脆弱性

システムのセキュリティを脅かすソフトウェアまたはハードウェアの欠陥。

W

ウォームキャッシュ

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

ウォームデータ

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

ウィンドウ関数

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

ワークロード

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

ワークストリーム

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

WORM

「[Write-Once-Read-Many](#)」を参照してください。

WQF

「[AWS ワークロード資格フレームワーク](#)」を参照してください

Write-Once-Read-Many (WORM)

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

Z

ゼロデイ 익스プロイト

[ゼロデイ脆弱性](#)を悪用した攻撃 (一般的にマルウェアによる)。

ゼロデイ脆弱性

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

ゼロショットプロンプト

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

ゾンビアプリケーション

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

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