



でのポットコントロール戦略の実装 AWS

AWS 規範ガイド



AWS 規範ガイド: でのボットコントロール戦略の実装 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
ボットの脅威とオペレーション	3
ボットネットの動作	4
ボット制御のテクニック	6
静的コントロール	7
一覧表示を許可する	8
IP ベースのコントロール	8
組み込みチェック	10
クライアント識別コントロール	10
CAPTCHA	11
ブラウザプロファイリング	12
デバイスのフィンガープリント	12
TLS フィンガープリント	13
高度な分析コントロール	14
ターゲットを絞ったユースケース	14
アプリケーションレベルまたは集計ボットの検出	14
機械学習分析	15
ボットコントロールのデプロイ	16
実装戦略	17
トラフィックパターンについて	17
コントロールの選択と追加	17
テストと本番環境へのデプロイ	18
コントロールの評価と調整	18
モニタリングガイドライン	20
上位ルールの追跡	21
上位ラベルと名前空間の追跡	21
数式の作成	22
異常検出の使用	22
CloudWatch メトリクスの使用	22
ダッシュボードの構築	23
コストの最適化	24
動的コンテンツと静的コンテンツの分離	24
低コストのルールを最初に適用する	24
評価領域の範囲を絞り込む	25

ポット保護と他のコントロールを組み合わせる	25
コストのモニタリング	26
リソース	27
AWS ドキュメント	27
その他の AWS リソース	27
寄稿者	28
オーサリング	28
のレビュー	28
テクニカルライティング	28
ドキュメント履歴	29
用語集	30
#	30
A	31
B	34
C	36
D	39
E	43
F	45
G	47
H	48
I	49
L	52
M	53
O	57
P	60
Q	63
R	63
S	66
T	70
U	71
V	72
W	72
Z	73
.....	lxxv

でのボットコントロール戦略の実装 AWS

Amazon Web Services ([寄稿者](#))

2024 年 2 月 ([ドキュメント履歴](#))

ボットなしではインターネットは不可能であることがわかっています。ボットは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します。これにより、企業はプロセスやタスクに効率を組み込むことができます。ウェブクローラーなどの便利なボットは、インターネット上の情報のインデックスを作成し、検索クエリに最も関連性の高い情報をすばやく見つけるのに役立ちます。ボットは、ビジネスを改善し、企業に価値を提供する優れたメカニズムです。ただし、時間の経過とともに、悪意のある攻撃者は既存のシステムやアプリケーションを新しくクリエイティブな方法で悪用する手段としてボットの使用を開始しました。

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。ボットネットは、[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の関係者の管理下にあるボットのネットワークです。1つの中心点から、オペレータはボットネット上のすべてのコンピュータに同時に調整されたアクションを実行するようにコマンドできます。そのため、ボットネットは command-and-control (C2) システムとも呼ばれます。

ボットネットの規模は数百万のボットになる可能性があります。ボットネットは、オペレータが大規模なアクションを実行するのに役立ちます。ボットネットはリモートオペレーターの管理下にあるため、感染したマシンは更新を受信し、その場で動作を変更できます。その結果、大きな財務上の利益のために、C2 システムはブラックマーケットのボットネットセグメントへのアクセスをレンタルできます。

ボットネットの保有率は引き続き増加しています。専門家は、悪意のある攻撃者のお気に入りのツールと見なされています。[Mirai](#) は最大のボットネットの 1 つです。2016 年に登場し、まだ運用されており、最大 350,000 台のモノのインターネット (IoT) デバイスに感染したと推定されています。このボットネットは、分散型サービス拒否 (DDoS) 攻撃など、さまざまなタイプのアクティビティに適用され、使用されています。最近、悪意のある攻撃者は、住宅プロキシサービスを使用して IP アドレスを取得することで、アクティビティをさらに難読化してトラフィックを調達しようとしてきました。これにより、アクティビティの洗練度を高め、検出と緩和をより困難にする、相互接続された正当な peer-to-peer システムが作成されます。

このドキュメントでは、ボットのランドスケープ、アプリケーションへの影響、使用可能な戦略と緩和オプションに焦点を当てています。この規範的なガイドとそのベストプラクティスは、さまざまなタイプのボット攻撃を理解し、軽減するのに役立ちます。さらに、このガイドでは、ボット緩和

戦略をサポートする AWS のサービス と の機能、および各戦略がアプリケーションの保護にどのように役立つかについて説明します。また、ボットのモニタリングの概要と、ソリューションコストを最適化するためのベストプラクティスも含まれています。

ボットの脅威とオペレーションについて

[Security Today](#) によると、インターネット上のすべてのトラフィックの 47% 以上がボットによるものです。これには、ボットの有用な部分、自己識別して価値を提供する部分が含まれます。ボットトラフィックの約 30% は、DDoS 攻撃、チケットスカルピング、インベントリスクレイピング、シャーディングなどの悪意のあるアクティビティを実行している未確認のボットです。[Security](#) は、2023 年前半にボリユーメトリック DDoS イベントが 300% 増加したことを報告しています。これにより、このトピックの関連性が高まり、利用可能な予防および保護ツールとテクノロジーに関する知識がますます重要になります。

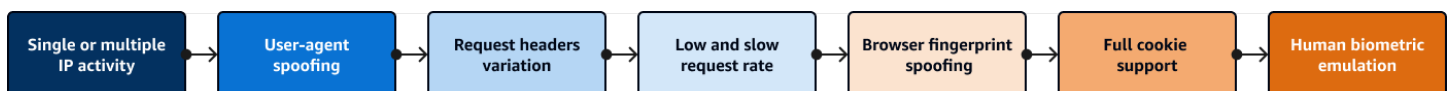
次の表は、さまざまなタイプのボットアクティビティと、それぞれが持つことができるビジネスへの影響を分類したものです。これは広範なリストではなく、最も一般的なボットアクティビティの概要です。モニタリングと緩和コントロールの重要性を強調しています。ボットの脅威の広範なリストについては、「[アプリケーションに対する OWASP 自動脅威ハンドブック \(OWASP ウェブサイト\)](#)」を参照してください。

ボットアクティビティタイプ	説明	潜在的な影響
コンテンツのスクレイピング	サードパーティーサイトで使用する独自のコンテンツのコピー	コンテンツの重複、ブランドへの影響、積極的なスクレイパーによるパフォーマンスの問題による SEO への影響
認証情報のスタッフィング	ウェブサイトで盗まれた認証情報データベースをテストして、情報にアクセスまたは検証する	サポートクエリを増やし、ブランドの信頼を低下させる不正やアカウントのロックアウトなどのユーザーの問題
カードのひび割れ	盗まれたクレジットカードデータのデータベースをテストして、不足している情報を検証または補完する	ID の盗難や不正、不正スコアの損傷など、ユーザーの問題
サービス妨害	特定のウェブサイトへのトラフィックを増やしてレスポンスを遅くしたり、正当なトラ	収益の損失と評判の低下

ボットアクティビティタイプ	説明	潜在的な影響
	フィックで利用できなくなったりする	
アカウントの作成	不正使用または金銭的利益を目的とした複数のアカウントの作成	抑制された成長と歪んだマーケティング分析
スケーリング	正規消費者に対する限定販売商品、頻繁なチケットの取得	販売されている商品にアクセスできないなど、ユーザーの収益と問題が失われる

ボットネットの動作

ボットネットオペレーターの戦術、手法、手順 (TTP) は、時間の経過とともに大きく進化しています。企業は、企業が開発した検出および緩和テクノロジーに対応する必要がありました。次の図は、この進化を示しています。ボットネットは単に IP アドレスを操作手段として使用することから始まり、最終的には高度な人間の生体認証エミュレーションを使用するように進化しました。この洗練度は高価であり、すべてのボットネットが最新のツールを使用しているわけではありません。インターネットにはオペレーターが混在しており、多くの場合、このジョブに最適なツールを評価して投資収益率を高めることができます。ボット防御の 1 つの目標は、ボットネットアクティビティを高価にして、ターゲットが実行不可能になるようにすることです。



一般的に、ボットは共通またはターゲットとして分類されます。

- 一般的なボット – これらのボットは自己識別し、ブラウザのエミュレートを試みません。これらのボットの多くは、コンテンツクロール、検索エンジン最適化 (SEO)、集約などの便利なタスクを実行します。これらの一般的なボットのうち、どのボットがサイトに届き、それがトラフィックとパフォーマンスに与える影響を特定して理解することが重要です。
- ターゲットボット – これらのボットは、ブラウザをエミュレートして検出を回避しようとしています。ヘッドレスブラウザなどのブラウザテクノロジーを使用するか、ブラウザのフィンガープリントを偽装します。JavaScript を実行し、Cookie をサポートできます。インテントは常に明確ではなく、生成するトラフィックは通常のユーザートラフィックのように見える可能性があります。

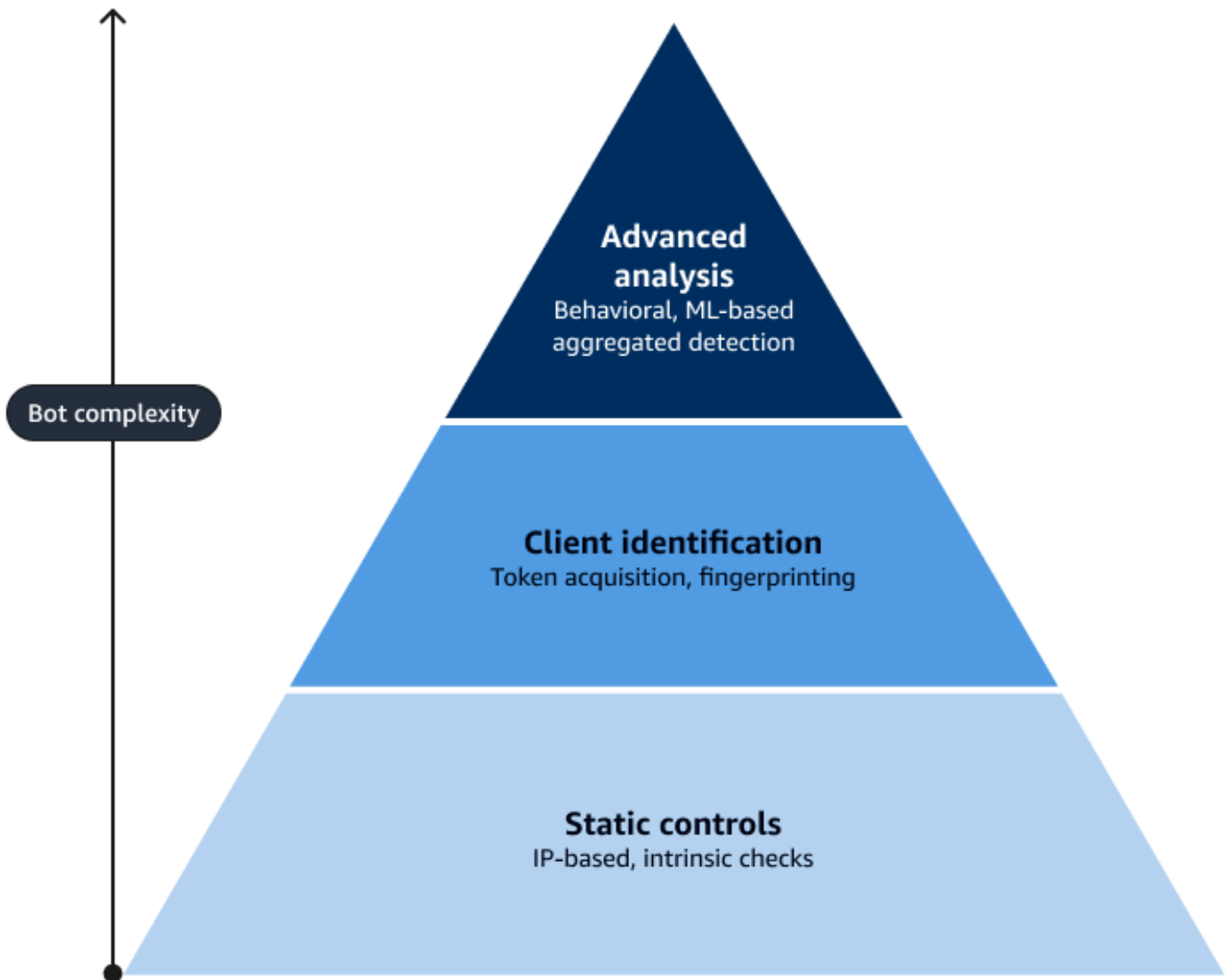
最も高度で永続的なターゲットボットは、人間のようなマウスの動きを生成し、ウェブサイトをクリックすることで、人間の動作をエミュレートします。これらは最も高度で検出が難しいですが、運用コストも最も高くなります。

多くの場合、演算子はこれらの手法を組み合わせます。これにより、オペレーターの最新技術に適應するために保護と緩和のアプローチを頻繁に変更する必要がある、継続的な追及のゲームが作成されます。これらのボットは、高度で永続的な脅威 (APT) と見なされます。詳細については、NIST リソースセンターの「[Advanced persistent threat](#)」を参照してください。

ボット制御のテクニック

ボット緩和の主な目的は、自動化されたボットアクティビティが組織のウェブサイト、サービス、アプリケーションに与える悪影響を制限することです。使用するテクノロジーと手法は、防御するトラフィックまたはアクティビティのタイプによって異なります。これを実現するには、アプリケーションとそのトラフィックを理解することが重要です。開始する場所の詳細については、このガイドの[ボットコントロール戦略のモニタリングに関するガイドライン](#)「」セクションを参照してください。

一般的に、ボット緩和ソリューションが提供するコントロールは、静的、クライアント識別、高度な分析の大まかなカテゴリにグループ化できます。次の図は、利用可能なさまざまな手法と、ボットアクティビティの複雑さに応じてどのように使用できるかを示しています。これにより、許可リストや組み込みチェックなどの静的コントロールを使用して、ベースまたは最も広範な緩和策を取得する方法が浮き彫りになります。ボットの最小部分は常に最も高度であり、これらのボットに対する緩和には、より高度なテクノロジーとコントロールの組み合わせが必要です。



次に、このガイドでは各カテゴリとその手法について説明します。また、これらのコントロールを実装 [AWS WAF](#) するために使用できるオプションについても説明します。

- [ボットを管理するための静的コントロール](#)
- [ボットを管理するためのクライアント識別コントロール](#)
- [ボットを管理するための高度な分析コントロール](#)

ボットを管理するための静的コントロール

アクションを実行するために、静的コントロールは IP アドレスやヘッダーなど、HTTP(S) リクエストからの静的情報を評価します。これらのコントロールは、洗練度の低い悪質なボットアクティビ

ティや、検証および管理が必要な予想される有益なポットトラフィックに役立ちます。静的コントロール手法には、許可リスト、IP ベースのコントロール、組み込みチェックなどがあります。

一覧表示を許可する

許可リストは、既存のポット緩和コントロールを通じて識別されたフレンドリトラフィックを許可するコントロールです。これを実現するには、さまざまな方法があります。最も簡単なのは、[一連の IP アドレス](#)または同様の一致条件に一致するルールを使用することです。リクエストがアクションに設定されたルールと一致すると Allow、後続のルールでは評価されません。場合によっては、特定のルールのみが実行されるのを防ぐ必要があります。つまり、1つのルールのリストを許可する必要がありますが、すべてのルールを許可することはできません。これは、ルールの誤検出を処理するための一般的なシナリオです。許可リストは、広範なルールと見なされます。偽陰性の可能性を減らすために、パスやヘッダーの一致など、より詳細な別のオプションと組み合わせることをお勧めします。

IP ベースのコントロール

単一の IP アドレスブロック

ポットの影響を軽減するために一般的に使用されるツールは、単一のリクエスタからのリクエストを制限することです。最も簡単な例は、トラフィックの送信元 IP アドレスのリクエストが悪意のあるものであるか、ボリュームが多い場合、そのトラフィックの送信元 IP アドレスをブロックすることです。これは AWS WAF [IP セット一致ルール](#)を使用して IP ベースのブロックを実装します。これらのルールは IP アドレスに一致し、Block、Challengeまたは CAPTCHA のアクションを適用します。IP アドレスからのリクエストが多すぎる場合は、コンテンツ配信ネットワーク (CDN)、ウェブアプリケーションファイアウォール、またはアプリケーションとサービスログを確認することで判断できます。ただし、ほとんどの場合、このコントロールは自動化なしでは実用的ではありません。

での IP アドレスブロックリストの自動化 AWS WAF は、一般的にレートベースのルールで行われます。詳細については、このガイドの「[レートベースのルール](#)」を参照してください。ソリューションの[セキュリティオートメーション AWS WAF](#)を実装することもできます。このソリューションは、ブロックする IP アドレスのリストを自動的に更新し、AWS WAF ルールはそれらの IP アドレスに一致するリクエストを拒否します。

ポット攻撃を認識する 1つの方法は、同じ IP アドレスからの多数のリクエストが少数のウェブページに集中している場合です。これは、ポットが料金スクレイプしているか、高い割合で失敗したログインを繰り返し試行していることを示します。このパターンをすぐに認識するオートメーションを作

成できます。自動化により IP アドレスがブロックされるため、攻撃をすばやく特定して軽減することで、攻撃の有効性が低下します。特定の IP アドレスをブロックすることは、攻撃者が攻撃を開始するための大量の IP アドレスのコレクションを持っている場合、または攻撃動作を認識して通常のトラフィックから分離するのが困難な場合、あまり効果的ではありません。

IP アドレスの評価

IP 評価サービスは、IP アドレスの信頼性を評価するのに役立つインテリジェンスを提供します。このインテリジェンスは、通常、その IP アドレスからの過去のアクティビティから IP 関連情報を集約することによって算出されます。以前のアクティビティは、IP アドレスが悪意のあるリクエストを生成する可能性を示すのに役立ちます。データは、IP アドレスの動作を追跡するマネージドリストに追加されます。

匿名 IP アドレスは、IP アドレスの評価の特殊なケースです。ソース IP アドレスは、クラウドベースの仮想マシンなどの簡単に取得できる IP アドレスの既知のソース、または既知の VPN プロバイダーや Tor ノードなどのプロキシから取得されます。AWS WAF [Amazon IP 評価リスト](#)と[匿名 IP リスト](#)マネージドルールグループは、Amazon 内部脅威インテリジェンスを使用して、これらの IP アドレスを識別します。

これらのマネージドリストによって提供されるインテリジェンスは、これらのソースから特定されたアクティビティに対処するのに役立ちます。このインテリジェンスに基づいて、トラフィックを直接ブロックするルールや、リクエストの数を制限するルール (レートベースのルールなど) を作成できます。このインテリジェンスを使用して、COUNT モードでルールを使用してトラフィックのソースを評価することもできます。これにより、一致基準が調べられ、カスタムルールの作成に使用できるラベルが適用されます。

レートベースのルール

レートベースのルールは、特定のシナリオにとって貴重なツールです。たとえば、レートベースのルールは、ポットトラフィックが機密性の高いユニフォームリソース識別子 (URIs) のユーザーと比較して大量の に達した場合や、トラフィックボリュームが通常のオペレーションに影響を与え始めた場合に有効です。レート制限は、リクエストを管理可能なレベルで維持し、アクセスを制限および制御できます。は、レートベースのルールステートメントを使用して、[ウェブアクセスコントロールリスト \(ウェブ ACL\)](#) にレート制限ルールを実装 AWS WAF できます。 <https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-rate-based.html> レートベースのルールを使用する場合に推奨されるアプローチは、サイト全体を対象とする包括的なルール、URI 固有のルール、および IP 評価レートベースのルールを含めることです。IP 評価レートベースのルールは、IP アドレス評価のインテリジェンスとレート制限機能を組み合わせます。

サイト全体について、包括的な IP 評価レートベースのルールは、少数の IPs からサイトを氾濫する、洗練されていないポットを防止する上限を作成します。レート制限は、ログインページやアカウント作成ページなど、コストや影響が大きい URIs を保護する場合に特に推奨されます。

レート制限ルールは、コスト効率の高い第 1 防御層を提供できます。より高度なルールを使用して、機密性の高い URIs を保護できます。URI 固有のレートベースのルールは、重要なページや、データベースアクセスなどのバックエンドに影響する APIs への影響を制限できます。このガイドで後述する特定の URIs を保護するための高度な緩和策では、追加コストが発生することが多く、これらの URI 固有のレートベースのルールはコストの制御に役立ちます。一般的に推奨されるレートベースのルールの詳細については、AWS セキュリティブログの「[最も重要な 3 つの AWS WAF レートベースのルール](#)」を参照してください。状況によっては、レートベースのルールによって評価されるリクエストのタイプを制限すると便利です。[スコープダウンステートメント](#)を使用して、ソース IP アドレスの地理的領域でレートベースのルールを制限できます。

AWS WAF は、[集約キー](#)を使用してレートベースのルールの高度な機能を提供します。この機能を使用すると、ソース IP アドレス以外のさまざまな集約キーとキーの組み合わせを使用するようにレートベースのルールを設定できます。たとえば、単一の組み合わせとして、転送された IP アドレス、HTTP メソッド、およびクエリ引数に基づいてリクエストを集約できます。これにより、高度なボリュームメトリックトラフィックの軽減のために、よりきめ細かなルールを設定できます。

組み込みチェック

組み込みチェックは、システムまたはプロセス内のさまざまなタイプの内部または固有の検証または検証です。ポット制御の場合、AWS WAF はリクエストで送信された情報がシステムシグナルと一致することを確認して、組み込みチェックを実行します。たとえば、逆引き DNS ルックアップやその他のシステム検証を実行します。SEO 関連のリクエストなど、一部の自動リクエストが必要です。許可リストは、期待される適切なポットを許可する方法です。ただし、悪意のあるポットが適切なポットをエミュレートすることがあり、それらを分離するのは難しい場合があります。は、マネージド [AWS WAF Bot Control ルールグループ](#)を通じてこれを実現する方法 AWS WAF を提供します。このグループのルールは、自己識別ポットが本人であることを検証します。は、リクエストの詳細をそのポットの既知のパターンと AWS WAF 照合し、逆引き DNS ルックアップやその他の目標検証も実行します。

ポットを管理するためのクライアント識別コントロール

攻撃関連のトラフィックが静的属性で簡単に認識できない場合、検出はリクエストを行うクライアントを正確に識別する必要があります。例えば、レートベースのルールは、レート制限されている属

性が Cookie やトークンなどのアプリケーション固有である場合に、より効果的で回避が難しいことがよくあります。セッションに関連付けられた Cookie を使用すると、ボットネットオペレーターが多くのボット間で同様のリクエストフローを複製できなくなります。

トークン取得は、クライアント識別に一般的に使用されます。トークン取得の場合、JavaScript コードは情報を収集して、サーバー側で評価されるトークンを生成します。評価は、JavaScript がクライアントで実行されていることの検証から、フィンガープリント用のデバイス情報の収集まで多岐にわたります。トークンの取得では、JavaScript SDK をサイトまたはアプリケーションに統合するか、サービスプロバイダーが動的にインジェクションを実行する必要があります。

JavaScript サポートを必須にすると、ボットがブラウザをエミュレートしようとする際のハードルが追加されます。モバイルアプリケーションなどの SDK が関与する場合、トークン取得は SDK の実装を検証し、ボットがアプリケーションのリクエストを模倣しないようにします。

トークンの取得には、接続のクライアント側で実装された SDKs を使用する必要があります。次の AWS WAF 機能は、ブラウザ用の JavaScript ベースの SDK とモバイルデバイス用のアプリケーションベースの SDK を提供します: [Bot Control](#)、[Fraud Control Account Takeover Prevention \(ATP\)](#)、[Fraud Control Account Creation Fraud Prevention \(ACFP\)](#)。

クライアント識別の手法には、CAPTCHA、ブラウザプロファイリング、デバイスのフィンガープリント、TLS フィンガープリントなどがあります。

CAPTCHA

コンピュータと人間を区別するための完全に自動化されたパブリックチューリングテスト ([CAPTCHA](#)) は、ロボット訪問者と人間訪問者を区別し、ウェブスクレイピング、認証情報スタッフィング、スパムを防ぐために使用されます。実装にはさまざまなものがありますが、多くの場合、人間が解決できるパズルが含まれます。CAPTCHA は、一般的なボットに対する追加の防御レイヤーを提供し、ボット検出の誤検出を減らすことができます。

AWS WAF は、ルールの検査基準に一致するウェブリクエストに対して CAPTCHA アクションを実行することをルールに許可します。このアクションは、サービスによって収集されたクライアント識別情報の評価の結果です。AWS WAF ルールでは、ログイン、検索、フォーム送信など、ボットによって頻繁にターゲットにされる特定のリソースに対して CAPTCHA チャレンジを解決する必要があります。AWS WAF は、相互手段または SDK を使用して直接 CAPTCHA を提供してクライアント側で処理できます。詳細については、[「CAPTCHA」と「チャレンジ AWS WAF」](#)を参照してください。

ブラウザプロファイリング

ブラウザプロファイリングは、トークン取得の一環としてブラウザの特性を収集して評価し、インタラクティブブラウザを使用して実際の人間を分散ボットアクティビティと区別する方法です。ブラウザのプロファイリングは、ヘッダー、ヘッダーの順序、およびブラウザの動作に固有のリクエストのその他の特性を通じてパッシブに実行できます。

トークン取得を使用してコードでブラウザプロファイリングを実行することもできます。ブラウザプロファイリングに JavaScript を使用すると、クライアントが JavaScript をサポートしているかどうかをすばやく判断できます。これにより、サポートされていない単純なボットを検出できます。ブラウザプロファイリングは、HTTP ヘッダーと JavaScript サポートだけでなく、ボットがウェブブラウザを完全にエミュレートすることが困難になります。どちらのブラウザプロファイリングオプションも、実際のブラウザの動作との不整合を示すパターンをブラウザプロファイルで検索するという同じ目標を持っています。

AWS WAF ターゲットボットのボットコントロールは、トークン評価の一環として、ブラウザが自動化の証拠を示しているか、一貫性のないシグナルを示しているかを示します。は、ルールで指定されたアクションを実行するためにリクエストを AWS WAF フラグ付けします。詳細については、AWS セキュリティブログの [「高度なボットトラフィックを検出してブロックする」](#) を参照してください。

デバイスのフィンガープリント

デバイスのフィンガープリントはブラウザプロファイリングに似ていますが、ブラウザに限定されません。デバイス (モバイルデバイスまたはウェブブラウザ) で実行されているコードは、デバイスの詳細を収集し、バックエンドサーバーに報告します。詳細には、メモリ、CPU タイプ、オペレーティングシステム (OS) カーネルタイプ、OS バージョン、仮想化などのシステム属性を含めることができます。

デバイスフィンガープリントを使用して、ボットが環境をエミュレートしているかどうか、またはオートメーションが使用されている直接の兆候があるかどうかを認識できます。さらに、デバイスのフィンガープリントを使用して、同じデバイスからの繰り返しのリクエストを認識することもできます。

同じデバイスから繰り返されるリクエストを認識すると、デバイスがリクエストの特性を変更しようとしても、バックエンドシステムはレート制限ルールを適用できます。デバイスのフィンガープリントに基づくレート制限ルールは、通常、IP アドレスに基づくレート制限ルールよりも効果的です。これにより、VPNs またはプロキシ間でローテーションしているが、少数のデバイスから取得されているボットトラフィックを軽減できます。

ターゲットポットの AWS WAF ポット制御をアプリケーション統合 SDKs で使用すると、はクライアントセッションリクエストの動作を 集約できます。これにより、両方が同じ IP アドレスから発信された場合でも、正当なクライアントセッションを検出して悪意のあるクライアントセッションから分離できます。ターゲット AWS WAF ポットのポット制御の詳細については、AWS セキュリティブログの「[高度なポットトラフィックを検出してブロックする](#)」を参照してください。

TLS フィンガープリント

署名ベースのルールとも呼ばれる TLS フィンガープリントは、ポットが多くの IP アドレスから発信されるが、同様の特性を示す場合によく使用されます。HTTPS を使用する場合、クライアント側とサーバー側はメッセージを交換して相互に確認および検証します。暗号化アルゴリズムとセッションキーを確立します。これは TLS ハンドシェイクと呼ばれます。TLS ハンドシェイクの実装方法は、多くの IP アドレスにまたがる大規模な攻撃を認識する上でしばしば役立つ署名です。

TLS フィンガープリントを使用すると、ウェブサーバーはウェブクライアントのアイデンティティを高い精度で判断できます。アプリケーションデータ交換が発生する前に、最初のパケット接続のパラメータのみが必要です。この場合、ウェブクライアントとは、ブラウザ、CLI ツール、スクリプト (ポット)、ネイティブアプリケーション、またはその他のクライアントなど、リクエストを開始するアプリケーションを指します。

1 つの SSL および TLS フィンガープリントアプローチは [JA3 フィンガープリント](#) です。JA3 は、SSL または TLS ハンドシェイクからの Client Hello メッセージ内のフィールドに基づいてクライアント接続をフィンガープリントします。これにより、異なるソース IP アドレス、ポート、および X.509 証明書間で特定の SSL および TLS クライアントをプロファイリングできます。

Amazon CloudFront は、リクエストへの [JA3 ヘッダーの追加](#) をサポートしています。CloudFront-Viewer-JA3-Fingerprint ヘッダーには、受信ビューワーリクエストの TLS Client Hello パケットの 32 文字のハッシュフィンガープリントが含まれます。フィンガープリントは、クライアントがどのように通信するかに関する情報をカプセル化します。この情報は、同じパターンを共有するクライアントをプロファイリングするために使用できます。CloudFront-Viewer-JA3-Fingerprint ヘッダーをオリジンリクエストポリシーに追加し、そのポリシーを CloudFront デイストリビューションにアタッチできます。その後、オリジンアプリケーションまたは Lambda@Edge および CloudFront Functions でヘッダー値を検査できます。ヘッダー値を既知のマルウェアフィンガープリントのリストと比較して、悪意のあるクライアントをブロックできます。ヘッダー値と予想されるフィンガープリントのリストを比較して、既知のクライアントからのリクエストのみを許可することもできます。

ボットを管理するための高度な分析コントロール

一部のボットでは、高度な偽装ツールを使用して検出を積極的に回避しています。これらのボットは、頭皮などの特定のアクティビティを実行するために人間の動作を模倣します。これらのボットには目的があり、通常は大きな金銭的報酬にリンクされています。

これらの高度な永続ボットは、さまざまなテクノロジーを使用して検出を回避したり、通常のトラフィックとブレンドしたりします。また、悪意のあるトラフィックを正確に識別して軽減するには、さまざまな検出テクノロジーの組み合わせも必要です。

ターゲットを絞ったユースケース

ユースケースデータは、ボット検出の機会を提供することができます。不正検出は、特別な緩和が必要とされる特別なユースケースです。たとえば、アカウントの乗っ取りを防ぐために、侵害されたアカウントのユーザー名とパスワードのリストをログインまたはアカウント作成リクエストと比較できます。これにより、ウェブサイトの所有者は、侵害された認証情報を使用するログイン試行を検出できます。侵害された認証情報を使用すると、ボットがアカウントを乗っ取ろうとしているか、認証情報が侵害されていることに気付いていないユーザーである可能性があります。このユースケースでは、ウェブサイト所有者は、ユーザーを検証し、パスワードの変更に役立つ追加の手順を実行できます。は、このユースケースの [Fraud Control アカウント乗っ取り防止 \(ATP\)](#) マネージドルール AWS WAF を提供します。

アプリケーションレベルまたは集計ボットの検出

一部のユースケースでは、コンテンツ配信ネットワーク (CDN) からのリクエストと AWS WAF、アプリケーションまたはサービスのバックエンドに関するデータを組み合わせる必要があります。場合によっては、ボットに関する信頼性の高い意思決定を行うために、サードパーティーのインテリジェンスを統合する必要もあります。

[Amazon CloudFront](#) および の機能は AWS WAF、バックエンドインフラストラクチャにシグナルを送信したり、ヘッダーと [ラベル](#) を介してルールを集約したりできます。CloudFront は、前述のように JA3 フィンガープリントヘッダーを公開します。これは、CloudFront がヘッダーを介してそのようなデータを提供する例です。は、ルールで一致するときにラベルを送信 AWS WAF できます。後続のルールでは、これらのラベルを使用してボットに関するより良い意思決定を行うことができます。複数のルールを組み合わせると、非常に詳細なコントロールを実装できます。一般的なユースケースは、ラベルを介してマネージドルールの一部を照合し、それを他のリクエストデータと組み合わせることです。詳細については、AWS WAF ドキュメントの [「ラベル一致の例」](#) を参照してください。

機械学習分析

機械学習 (ML) は、ボットを処理するための強力な手法です。ML は詳細の変化に対応でき、他のツールと組み合わせると、誤検出を最小限に抑えてボットを軽減するための最も堅牢で完全な方法を提供します。最も一般的な ML 手法は、動作分析と異常検出の 2 つです。動作分析では、システム (クライアント、サーバー、またはその両方) はユーザーがアプリケーションまたはウェブサイトとやり取りする方法をモニタリングします。マウスの動きパターンまたはクリックとタッチのやり取りの頻度をモニタリングします。その後、動作は ML モデルで分析され、ボットを認識します。異常検出も同様です。アプリケーションまたはウェブサイトに定義されているベースラインとは大幅に異なる動作やパターンを検出することに重点を置いています。

AWS WAF ボットのターゲットコントロールは、予測 ML テクノロジーを提供します。このテクノロジーは、検出を回避するように設計されたボットによって行われる分散型のプロキシベースの攻撃に対する防御に役立ちます。マネージド [AWS WAF Bot Control ルールグループ](#)は、ウェブサイトトラフィック統計の自動 ML 分析を使用して、分散された調整されたボットアクティビティを示す異常な動作を検出します。

ボットコントロール戦略のデプロイと実装

ボットコントロールのデプロイ戦略を計画するときは、複数の要素を考慮する必要があります。ウェブアプリケーションの固有の特性に加えて、環境サイズ、開発プロセス、組織構造がデプロイ戦略に影響します。環境とアプリケーションの特性に応じて、集中型または分散型のデプロイ戦略を使用できます。

- 一元化されたデプロイ戦略 – 一元化されたアプローチにより、ボット制御を厳密に実施したい場合に、より高いレベルの制御が可能になります。このアプローチは、アプリケーションチームが管理をオフロードする場合に適しています。一元化されたアプローチは、ウェブアプリケーションが同様の特性を共有する場合に最も効果的です。この場合、アプリケーションは一般的なボットコントロールルールとボット緩和アクションのセットから恩恵を受けます。
- 分散型デプロイ戦略 – 分散型アプローチは、アプリケーションチームにボット制御設定を個別に定義して実装する自律性を提供します。このアプローチは、小規模な環境や、アプリケーションチームがボットコントロールポリシーの制御を維持する必要がある場合に一般的です。多くのウェブアプリケーションの性質上、独自のアプリケーション特性に合わせてカスタマイズされた独立したボット制御ポリシーを維持することが必要になることがよくあり、その結果として分散アプローチが生まれます。
- 複合戦略 – これら 2 つのアプローチの組み合わせは、ウェブアプリケーションの混在に適しています。たとえば、これにはすべてのウェブ ACLs に適用される一連の基本ルールが含まれる場合がありますが、より具体的なボット制御ポリシーの管理はアプリケーションチームに委任されます。

を使用して [AWS Firewall Manager](#)、ボット制御ポリシーを定義する AWS WAF ウェブ ACLs を一元化および自動化できます。Firewall Manager を使用する場合は、アプリケーションチームに委任する必要があるかどうかを含め、ボットコントロールポリシーを一元化することが適切かどうかを検討してください。Firewall Manager では、タグ付けを使用して、アプリケーションチームが AWS WAF ポリシーをオプトインできるようにします。これにより AWS WAF、インテリジェントな脅威軽減機能が提供されます。アプリケーションおよびセキュリティオペレーションの集中 AWS WAF ログ記録を有効にすることもできます。

使用するデプロイ戦略にかかわらず、[AWS CloudFormation](#) Infrastructure as Code (IaC) ベースのフレームワークを使用してオンボーディングプロセスを定義および管理することをお勧めします [AWS Cloud Development Kit \(AWS CDK\)](#)。これにより、設定オブジェクトを保存およびバージョン管理するようにソースコントロールを設定できます。詳細については、[AWS CDK](#) 「(GitHub) および [CloudFormation](#) (AWS ドキュメント) AWS WAF の設定サンプル」を参照してください。

実装戦略

デプロイ戦略を選択すると、実装を開始できます。デプロイ戦略は、ルールをさまざまなアプリケーションにロールアウトする方法を定義します。実装戦略では、コントロールの追加、テスト、継続的なモニタリング、効果の評価の反復プロセスに焦点を当てています。

トラフィックパターンについて

トラフィックパターンを実際に理解するには、アプリケーションのビジネス機能や、使用パターン、キーリソース、ユーザーペルソナなどの予想される属性について理解することが重要です。アプリケーションに対するテスト中に生成された本稼働トラフィックとトラフィックを組み込み、評価のベースラインを確立します。時間枠に、複数の使用量のピークを十分に表すトラフィックデータが含まれていることを確認します。

任意のツールを使用して、代表的な使用期間におけるトラフィックログとメトリクスを確認します。(headers User-Agentや などReferer)、[などの AWS WAF ログフィールドでフィルタリングして、異常なリクエストのログ](#)データを分析しますclientIp。countryユニフォームリソース識別子 (URIs) とそのアクセス頻度を書き留めます。適切なボットの特定など、トラフィックを分類します。たとえば、検索エンジンのクローラやモニターなどの有益なボットへのアクセスを許可します。

AWS WAF コンソールの Bot Control ダッシュボードで、アクティブなウェブ ACL でボットアクティビティのサンプルを使用できます。これにより、一般的なボットリクエストボリュームの初期視点が得られますが、ボットのアクティビティをよりよく理解するために、さらなる設定と分析を実行します。

効果的な実装を行うには、ボットトラフィックとその効果、およびどのボットリクエストが有益か悪意があるかを十分に理解する必要があります。これは、次のフェーズ、コントロールの選択、ボットトラフィックの並列評価に役立ちます。

コントロールの選択と追加

初期トラフィック分析は、使用するボットコントロールと、それぞれに対して選択するアクションを決定するのに役立ちます。また、今後のアクションの可能性について、アクティビティをログに記録してモニタリングすることもできます。初期トラフィック分析は、トラフィックを管理するための最適なコントロールを選択するのに役立ちます。使用可能なコントロールの詳細については、このガイドの[ボット制御のテクニック](#)「」を参照してください。

このステップでは、追加の SDK 実装を含めることを検討してください。これにより、必要なすべてのアプリケーションで SDK 実装をテストして完了できます。AWS WAF ポット制御および不正制御ルールは、JavaScript SDK またはモバイル SDK を実装するときに完全なトークン評価の利点を提供します。詳細については、AWS WAF ドキュメントの「[Bot Control でアプリケーション統合 SDKs](#)」を参照してください。

次のように、さまざまなアプリケーションタイプにトークン取得を実装することをお勧めします。

- 単一ページアプリケーション (SPA) – JavaScript SDK (リダイレクトなし)
- モバイルブラウザ – JavaScript SDK またはルールアクション (CAPTCHA またはチャレンジ)
- ウェブビュー – JavaScript SDK またはルールアクション (CAPTCHA またはチャレンジ)
- ネイティブアプリケーション – Mobile SDK
- iFrames – JavaScript SDK

SDKs [AWS WAF 「クライアントアプリケーション統合」](#) を参照してください。AWS WAF

テストと本番環境へのデプロイ

コントロールは、最初に非本番環境にデプロイする必要があります。この環境では、テストを実行して、期待されるウェブアプリケーションの機能が保持されていることを確認することができます。本番環境にデプロイする前に、テスト環境で常に徹底的な検証を実行します。

非本番稼働環境でテストと検証を行った後、本番稼働用リリースを続行できます。予想されるユーザートラフィックが最も少ない日時を選択します。デプロイする前に、アプリケーションチームとセキュリティチームが運用準備状況を確認し、変更をロールバックする方法を説明し、ダッシュボードを確認して、必要なすべてのメトリクスとアラームが設定されていることを確認する必要があります。

[Amazon CloudFront の継続的デプロイ](#)では、ポット制御評価専用 AWS WAF ウェブ ACL が設定されたステージングディストリビューションに少量のトラフィックを送信できます。は、新規または更新されたマネージドルール [のバージョン管理](#) AWS WAF を提供し、本番トラフィックの評価を開始する前に変更をテストして承認できるようにします。

コントロールの評価と調整

実装されたコントロールは、トラフィックのアクティビティとパターンに関する詳細なインサイトと可視性を提供できます。セキュリティコントロールを追加または調整するために、アプリケーショントラフィックを頻繁にモニタリングおよび分析します。通常、潜在的な偽陰性と偽陽性を軽減するた

めの調整フェーズがあります。偽陰性は、コントロールによって検出されず、ルールを強化する必要がある攻撃です。誤検出は、攻撃として誤って識別され、結果としてブロックされた正当なリクエストを表します。

分析と調整は、手動またはツールを使用して行うことができます。Security Information and Event Management (SIEM) システムは、メトリクスとインテリジェントなモニタリングを提供するのに役立つ一般的なツールです。さまざまなレベルの洗練度で利用できるものが多数ありますが、それらはすべてトラフィックインサイトを取得するための良い出発点となります。

ウェブサイトやアプリケーションの重要な主要業績評価指標 (KPIs) を定義すると、モノが期待どおりに機能していないタイミングをより迅速に特定できます。たとえば、クレジットカードのチャージバック、アカウントあたりの売上、または変換率を、ボットによって生成される可能性のあるビジネス異常の指標として使用できます。モニタリングする価値のあるメトリクスと KPIs を定義して理解することは、単なるモニタリング行為よりもさらに重要です。

ボット制御ソリューションから適切なメトリクスとログを取得する方法を理解することは、モニタリングするメトリクスを特定するのと同じくらい重要です。次のセクション [ボットコントロール戦略のモニタリングに関するガイドライン](#) では、考慮すべきモニタリングと可視性のオプションについて詳しく説明します。

ボットコントロール戦略のモニタリングに関するガイドライン

ボットトラフィックとウェブアプリケーショントラフィックでは、モニタリングと可視性が非常に重要です。アクティビティとセキュリティオペレーションの優先順位を付けるのに役立ちます。詳細なログ記録や SIEM システムの使用が不可能な場合は、選択したソリューションまたはベンダーが提供する基本的なメトリクスをモニタリングすることをお勧めします。

この可視性は、脅威インテリジェンス、ルールの強化、誤検出のトラブルシューティング、インシデントへの対応に役立ちます。では、複数のモニタリングオプションを使用できます AWS WAF。高レベルモニタリング AWS WAF の場合、はトラフィックの概要情報を に提供します AWS マネジメントコンソール。これは、ウェブ ACL で Bot Control ルールグループが有効になっている場合、すべてのトラフィックとボットトラフィックの詳細ビューで使用できます。

AWS WAF は、[ウェブ ACL トラフィックの詳細なログ記録](#)にさまざまなオプションを提供します。リクエストにラベルを追加することもできます。これを使用して、ログ分析を容易にし、ボット評価ルールを設定できます。[Amazon CloudWatch Logs Insights](#) を統合することで、AWS WAF ログをクエリして結果を視覚化できます。

詳細ログ記録を有効にすると、AWS WAF は事前設定された Bot Control ダッシュボード 以外の可視性を提供します。AWS WAF ログを使用してトラフィックを可視化し、アドホック調査を行うことで、ウェブアプリケーションのトラフィックパターンと緩和策のオプションを詳細に把握できます。

AWS WAF ログデータは、Amazon CloudWatch Logs、Amazon Simple Storage Service (Amazon S3)、または Amazon Data Firehose と統合できます。詳細については、[AWS WAF 「ログ記録を有効にして、Amazon S3 CloudWatch、または Amazon Data Firehose にログを送信する」](#)を参照してください。また、Amazon OpenSearch Service や [AWS Marketplace](#) ソリューションなど、分析のためにさまざまなターゲットにログを送信することもできます。詳細については、Firehose ドキュメントの「[送信先設定](#)」を参照してください。複数のログソースを使用する場合は、ソースを関連付けるために一元的なログ記録ソリューションが推奨されます。

次に、このガイドでは、Amazon を使用してボットトラフィックのモニタリングを開始し、可視性を得る方法に関する推奨事項を提供します CloudWatch。

上位ルールの追跡

上位のルールを追跡すると、傾向や異常なアクティビティの可能性が強調されます。特定のルールのレートが上昇すると、調査すべき誤検出またはターゲットを絞ったアクティビティの可能性を示している可能性があります。追跡の最も一般的なルールは[IP ベースのコントロール](#)、ジオブロッキングルール (ここで急増すると、自動的にブロックされない可能性のある異常な国からのトラフィックが表示される可能性があります)、および [レートベースのルール](#)。これらのルールには常に固有のバリエーションがありますが、トラフィックパターンの異常はボットのアクティビティを示している可能性があります。手動でしきい値を設定する場合は、この点を考慮してください。

上位ラベルと名前空間の追跡

CloudWatch メトリクスを使用して上位[ラベル](#)を追跡することで、頻繁に呼び出される AWS WAF ルールを確認できます。これにより、スクレイパーアクティビティの増加、疑わしいソースからのトラフィック、アプリケーションログインページまたは API の悪用の試みなどの異常を検出できます。

以下は、関心のあるラベルの例です。

- `aws:wafv2:managed:aws:bot-control:signal:non_browser_user_agent`
- `aws:wafv2:managed:aws:bot-control:bot:category:http_library`
- `aws:wafv2:managed:aws:bot-control:bot:name:curl`
- `aws:wafv2:managed:aws:atp:signal:credential_compromised`
- `aws:wafv2:managed:aws:core-rule-set:NoUserAgent_Header`
- `aws:wafv2:managed:token:rejected`

以下は、関心のあるラベル名前空間の例です。

- `aws:wafv2:managed:aws:bot-control:`
- `aws:wafv2:managed:aws:atp:`
- `aws:wafv2:managed:aws:anonymous-ip-list:`

数式の作成

Amazon では CloudWatch、任意のルールまたはすべてのルール [に対して数式](#) を作成できます。数式にアラートを設定すると、特定のメトリクスの数量ではなくレートの異常に関する通知が届きます。これは、アラートの疲労を軽減するための重要なツールです。

数式から構築されたカスタムメトリクスを作成します。アプリケーションへのリクエストの総数のうち、ルールの相対レートを確認します。以下は一般的な数式です。

```
[ruleX count * 100]/[All allowed requests + All blocked requests]
```

この数式はパーセンテージを提供するため、特定のルールを追跡し、その傾向を経時的に視覚化できます。

異常検出の使用

任意の CloudWatch メトリクスに [CloudWatch 異常検出](#) を使用すると、実際のしきい値を手動で設定しなくても、異常に低いまたは高い傾向に関するアラートを提供できます。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、通常のベースラインを決定し、ユーザーの介入を最小限に抑えて異常を検出します。CloudWatch は、統計アルゴリズムと ML アルゴリズムを異常検出機能に適用します。

Amazon CloudWatch メトリクスの使用

AWS WAF はトラフィックを処理し、ウェブ ACL で定義されたルールに一致するリクエストにラベルを追加します。各ラベルは [メトリクス](#) を作成します CloudWatch。同時に、各ウェブ ACL ルールは、可能な各アクションのメトリクスも作成します。これらのラベルとアクションのメトリクスを使用して、ポットトラフィックの概要を把握します。これは、トレンドを視覚化するための費用対効果の高いアプローチです。詳細については、CloudWatch ドキュメントの [「使用可能なメトリクスの表示」](#) と [「メトリクスのグラフ化」](#) を参照してください。

CloudWatch は、またはサードパーティーのソリューションのいずれであっても、ログコレクタ AWS のサービス — または アグリゲータにデータを送信するオプションを提供します。からデータを取り込むと、複数のソースからのデータを関連付けることができる、より統合されたセキュリティオペレータビリティエクスペリエンス CloudWatch を提供できます。これにより、アラートとセキュリティオートメーションの調査、表示、またはセットアップに役立ちます。

ダッシュボードの構築

追跡する重要なメトリクスを特定したら、最も関連性の高いメトリクスを含むダッシュボードを作成します。これらを1つのペインの下に表示することで side-by-side、可視性と制御を強化できます。

異常なメトリクス値には、常にアラートと自動化ルールを設定することをお勧めします。ダッシュボードを見て異常を特定する際、人間に依存しないでください。ただし、ダッシュボードは、アラートを受信した後の調査目的に役立ちます。

ボット制御戦略のコストの最適化

ウェブトラフィックの性質は動的です。つまり、脅威の軽減に使用されるテクノロジーとサービスは、時間の経過とともに変化し、調整される可能性があります。これは、ボットコントロール戦略とその戦略に含まれるコントロールを検討する場合に重要です。時間の経過に伴う最適化は、覚えておくべき主な原則であり、AWS Well-Architected フレームワークの[コスト最適化の柱](#)に基づいています。

AWS WAF ウェブ ACLs は、特に新機能がリリースされた場合や、新しい脅威を軽減しようとしている場合に動的になる可能性があります。コストを監視するには、AWS WAF サービスの[コスト](#) [ディメンション](#)と、それぞれが最終的な支出にどのように影響するかを理解する必要があります。主な運転コストは、サービスによって評価されるリクエストの数です。[Bot Control](#) と [アカウント乗っ取り防止 \(ATP\)](#) マネージドルールグループを使用する場合、または [CAPTCHA](#) や [チャレンジ](#) などの高度なアクションを使用する場合、追加料金が発生します。

特殊なボットコントロールにはプレミアムコストがかかるため、主なコスト最適化の目標は、これらの高度なコントロールによって検査されるリクエストの数を減らすことです。適用可能な手法には、高価値コンテンツの分離、低コストの対策の適用、評価範囲の絞り込み、ボット保護と他のタイプのコントロールの組み合わせなどがあります。コストモニタリング手法は、組織全体の可視性を高めます。

動的コンテンツと静的コンテンツの分離

コスト削減手法の1つは、静的コンテンツを動的アプリケーションから分離することです。一般的なウェブアプリケーションへのリクエストの大部分は、静的オブジェクトへのリクエストです。アプリケーションサーバーの負荷を軽減するための一般的な方法は、静的コンテンツを [static.example.com](#) などの独自の URL に移動することです。これは、静的コンテンツに最適化されたキャッシュ設定で一意的なコンテンツ配信ディストリビューションを作成することで実現されることがよくあります。この手法は、静的コンテンツがサイトやアプリケーションで一般的にターゲットにされていない場合に、ボット制御コストを削減するのに役立ちます。静的コンテンツを動的アプリケーションから分離することで、高度なボット制御をより正確に適用できます。

低コストのルールを最初に適用する

もう1つの手法は、高度なコントロールを使用する前に不要なトラフィックを除外する低コストのベースラインルールを適用することです。実際には、これはボットコントロールの緩和策を最後の防

御レイヤーとして配置し、前述のコントロールを使用して不要なトラフィックを除外することを意味します。このピラミッドアプローチについては、このガイド [ボット制御のテクニック](#) で前述しました。主な目的は、これらの低コストオプションを使用して不要なトラフィックを停止し、高度でコストの高い緩和手法によって処理されるリクエストの数を減らすことです。

評価領域の範囲を絞り込む

AWS WAF [スコープダウンステートメント](#) は、高度なルールによって検査されるリクエストの数を減らすための強力な手法を提供します。静的コンテンツを独自の URL に分離できない場合、スコープダウンステートメントは、高度な緩和手法を必要としないリクエストを除外するもう 1 つの方法です。これを行うには、特定のアプリケーションパス、HTTP メソッド (POST など)、または同様の組み合わせを定義します。

ボット保護と他のコントロールを組み合わせる

不要なボットトラフィックに加えて複数の脅威からアプリケーションを保護する場合は、追加のコスト管理上の考慮事項を検討する必要があります。たとえば、分散型サービス拒否 (DDoS) 攻撃やアカウント乗っ取りから保護するには、コストに影響を与える可能性のある追加の設定が必要です。[Shield Advanced](#) は、DDoS 攻撃からアプリケーションを保護するために推奨されます。特に、アプリケーションレイヤーの緩和策では、リクエストフラッドに自動的に対処できるため、ルールを AWS WAF 評価順序に先行させるときに Bot Control ルールグループによって処理される可能性のあるリクエストの数を減らすことができます。Shield Advanced には追加の利点があります。標準マネージドルールとカスタム AWS WAF ルールは、Shield Advanced で保護されたリソースに追加コストがかかりません。Bot Control を含むインテリジェントな脅威軽減ルールグループでは、Shield Advanced で保護されたリソースに対しても追加コストが発生することに注意してください。

アカウント乗っ取り防止を必要とするアプリケーションは、Fraud Control アカウント乗っ取り防止 (ATP) ルールグループを使用できます。ATP ルールグループのリクエストごとの検査コストは、Bot Control ルールグループのコストよりも高くなります。コストが高くなると、ATP ルールグループを可能な限り正確に適用することが重要になります。Bot Control ルールグループを ATP と組み合わせて使用すると、この目標を達成できます。AWS WAF <https://docs.aws.amazon.com/waf/latest/developerguide/aws-managed-rule-groups-acfp.html> Bot Control ルールグループは、ボットリクエストを除外し、ATP によって検査されるリクエストの数を減らすために、ウェブ ACL の ATP の前に配置する必要があります。

継続的な最適化のために、最も重要なアクティビティは Bot Control ルールグループに関連付けられた [CloudWatch メトリクス](#) のモニタリングです。長期的な目標は、Bot Control ルールグループに

よって評価されるリクエストの数を、不要なポットアクティビティから保護するために必要なリソースのみをターゲットとするリクエストの数に減らすことです。CloudWatch ダッシュボード を構築すると、AWS WAF コストや使用状況など、アプリケーションの最も重要なメトリクスを可視化できます。

コストのモニタリング

[AWS Cost Explorer](#) は、コストと使用状況を表示および分析するために使用できるツールです。Cost Explorer は、発生した AWS コストを含む AWS WAF コストの分析を容易にします。このツールは、過去 12 か月間のコスト情報を提供し、今後 12 か月間の将来の支出を予測します。

[AWS コスト異常検出](#) は、コストのモニタリングに役立つもう 1 つの AWS WAF コスト管理コントロールツールです。高度な ML テクノロジーを使用して、異常な支出と根本原因を特定します。これにより、予期しないコストの増加が発生した場合に迅速にアクションを実行したり、アラートを受信したりできます。特定のコストしきい値に達したときにアラートを受信するには、[AWS Budgets](#) はその追跡およびモニタリング機能を提供します。

リソース

AWS ドキュメント

- [AWS WAF デベロッパーガイド](#)
- [AWS DDoS レジリエンシーのベストプラクティス](#) (AWS ホワイトペーパー)
- [実装のガイドライン AWS WAF](#) (AWS ホワイトペーパー)

その他の AWS リソース

- [Amazon AWS WAF Logs での CloudWatch ログの分析](#) (AWS ブログ記事)
- [最小限の労力 AWS WAF でのダッシュボードをデプロイする](#) (AWS ブログ記事)
- [のセキュリティオートメーション AWS WAF](#) (AWS ソリューションライブラリ)
- [AWS WAF レートベースの最も重要な 3 つのルール](#) (AWS ブログ記事)
- [Amazon CloudWatch ダッシュボードで AWS WAF ログを視覚化する](#) (AWS ブログ記事)

寄稿者

オーサリング

- Diana Alvarado、シニアソリューションアーキテクト、AWS
- キャメロン・ウォレル、エンタープライズアーキテクト、AWS
- 、ソリューションアーキテクト、Arcary Scherer AWS
- Tzoori Tamam、プリンシパルソリューションアーキテクト、AWS

のレビュー

- Jess Izen、シニアソフトウェア開発エンジニア、AWS
- Kaustubh Phatak、シニアプロダクトマネージャー、AWS
- Vikramaditya Bhatnagar、シニアセキュリティコンサルタント、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 2 月 21 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コラボレーション用のステートフルプロトコル。

ABAC

「[属性ベースのアクセス制御](#)」をご覧ください。

抽象化されたサービス

「[マネージドユーザー](#)」をご覧ください。

ACID

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

アクティブ/アクティブ移行

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

アクティブ/パッシブ移行

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

[エージェント]

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

エージェントオペレーション

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

集計関数

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

AI

「[人工知能](#)」をご覧ください。

AIOps

「[AI オペレーション](#)」をご覧ください。

匿名化

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

アンチパターン

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

アプリケーション制御

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

アプリケーションポートフォリオ

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

人工知能 (AI)

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

AI オペレーション (AIOps)

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

非対称暗号化

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

原子性、一貫性、分離性、耐久性 (ACID)

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

属性ベースのアクセス制御 (ABAC)

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

信頼できるデータソース

最も信頼性のある情報源とされるデータのプライマリ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

不正なポット

個人や組織に混乱や損害を与えることを目的とした[ポット](#)。

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。

ポット

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、一部のポットは有用または有益です。悪質なポットと呼ばれる他のポットの中には、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。

ポットネット

[マルウェア](#)に感染しており、ポットハーダーまたはポ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**ポット**のネットワーク。ポットネットは、ポ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します。詳細については、AWS Well-Architected ガイダンスの「[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 AWS のサービス 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 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

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

機能ブランチ

「[ブランチ](#)」を参照してください。

特徴量

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

特徴量重要度

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

機能変換

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

数ショットプロンプト

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

FGAC

[「きめ細かなアクセス制御」](#)を参照してください。

きめ細かなアクセス制御 (FGAC)

複数の条件を使用してアクセス要求を許可または拒否すること。

フラッシュカット移行

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

FM

[「基盤モデル」](#)を参照してください。

基盤モデル (FM)

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

FM ゲートウェイ

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

G

生成 AI

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

ジオブロッキング

「[地理的制限](#)」を参照してください。

地理的制限 (ジオブロッキング)

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

Gitflow ワークフロー

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

ゴールデンイメージ

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

グリーンフィールド戦略

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

ガードレール

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

ガードレール (AI)

[エージェント](#)の入力と出力をフィルタリング、検証、制約して、責任ある安全な AI 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 内 AWS リージョン)、インターネット、オンプレミスネットワーク間のネットワークトラフィックの検査を管理する一元化された VPCs。 [AWS Security Reference Architecture](#) では、アプリケーションとより広範なインターネット間の双方向のインターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションの各 VPC を使用してネットワークアカウントを設定することを推奨しています。

IoT

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

解釈可能性

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

IoT

「[IoT](#)」を参照してください。

IT 情報ライブラリ (ITIL)

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

IT サービス管理 (ITSM)

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

ITIL

「[IT 情報ライブラリ](#)」を参照してください。

ITSM

「[IT サービス管理](#)」を参照してください。

L

ラベルベースアクセス制御 (LBAC)

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

ランディングゾーン

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

大規模言語モデル (LLM)

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

大規模な移行

300 台以上のサーバの移行。

LBAC

「[ラベルベースアクセス制御](#)」を参照してください。

最小特権

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

リフトアンドシフト

「[7 Rs](#)」を参照してください。

リトルエンディアンシステム

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

LLM

「[大規模言語モデル](#)」を参照してください。

下位環境

「[環境](#)」を参照してください。

M

機械学習 (ML)

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

メインブランチ

「[ブランチ](#)」を参照してください。

マルウェア

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

マネージドサービス

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

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

製造実行システム (MES)

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

MAP

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

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)

[エージェントツーツール](#)通信のステートレスプロトコル。

MCP サーバー

Model [Context Protocol](#) を通じて 1 つ以上の [ツール](#) を公開するサービス。

メカニズム

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

メンバーアカウント

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

MES

「[製造実行システム](#)」を参照してください。

Message Queuing Telemetry Transport (MQTT)

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

マイクロサービス

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

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

マイクロサービスアーキテクチャ

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

Migration Acceleration Program (MAP)

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

大規模な移行

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

移行ファクトリー

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

移行メタデータ

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

移行パターン

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

Migration Portfolio Assessment (MPA)

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

移行準備状況評価 (MRA)

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

移行戦略

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

ML

「[機械学習](#)」を参照してください。

モダナイゼーション

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

モダナイゼーション準備状況評価

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

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

モノリシックアプリケーション (モノリス)

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

MPA

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

MQTT

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

多クラス分類

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

ミュータブルなインフラストラクチャ

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

O

OAC

「[オリジンアクセス制御](#)」を参照してください。

OAI

「[オリジンアクセスアイデンティティ](#)」を参照してください。

OCM

「[組織変更管理](#)」を参照してください。

オフライン移行

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

OI

「[オペレーション統合](#)」を参照してください。

Ola

「[オペレーショナルレベルアグリーメント](#)」を参照してください。

オンライン移行

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

OPC-UA

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

Open Process Communications - Unified Architecture (OPC-UA)

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

オペレーショナルレベルアグリーメント (OLA)

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

運用準備状況レビュー (ORR)

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

運用テクノロジー (OT)

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

オペレーション統合 (OI)

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

組織の証跡

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

組織変更管理 (OCM)

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

オリジンアクセス制御 (OAC)

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

オリジンアクセスアイデンティティ (OAI)

CloudFront の、Amazon S3 コンテンツを保護するためのアクセス制限オプション。OAI を使用すると、CloudFront が、Amazon S3 に認証可能なプリンシパルを作成します。認証されたプリンシパルは、S3 バケット内のコンテンツに、特定の CloudFront デ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 [AWS マネジメントコンソール](#) したり [AWS API オペレーション](#) を呼び出したりでき、組織内のすべてのユーザーを IAM で作成する必要はありません。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

送信先にあるデータを、AWS のサービスが受信する によって暗号化します。

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、ウェブ計画、および移行メタデータの収集を担当します。ポートフォリオワークストリームは、これらの設備を移行ワークストリームで実現し、サーバーとアプリケーションを移行します。

WORM

「[Write-Once-Read-Many](#)」を参照してください。

WQF

「[AWS ワークロード資格フレームワーク](#)」を参照してください

Write-Once-Read-Many (WORM)

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

Z

ゼロデイエクスプロイト

[ゼロデイ脆弱性](#)を悪用した攻撃 (一般的にマルウェアによる)。

ゼロデイ脆弱性

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

ゼロショットプロンプト

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

ゾンビアプリケーション

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

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