



クローल、ウォーク、実行: でセキュリティ成熟を加速する AWS クラウド

AWS 規範ガイドンス



AWS 規範ガイド: クロール、ウォーク、実行: でセキュリティ成熟を加速する AWS クラウド

Table of Contents

序章	1
Crawl	3
計画	3
セキュリティスコープ	4
セキュリティモデル	7
ビジネス目標モデル	12
ビルド	13
評価	14
Prowler	15
AWS Security Hub	15
Walk	16
運用	16
AWS クラウド導入フレームワーク	16
期待される成果	17
成熟	18
プロセス	19
ツール	21
Risk	23
例	23
実行	27
最適化	27
結論	30
リソース	33
フレームワークとモデル	33
AWS のサービス	33
その他の AWS リソース	33
寄稿者	34
オーサリング	34
レビュー	34
テクニカルライティング	34
ドキュメント履歴	35
用語集	36
#	36
A	37

B	40
C	42
D	45
E	49
F	51
G	52
H	54
I	55
L	57
M	58
O	62
P	65
Q	68
R	68
S	71
T	75
U	76
V	77
W	77
Z	78
.....	lxxix

クロール、ウォーキング、実行: のセキュリティ成熟度の向上 AWS クラウド

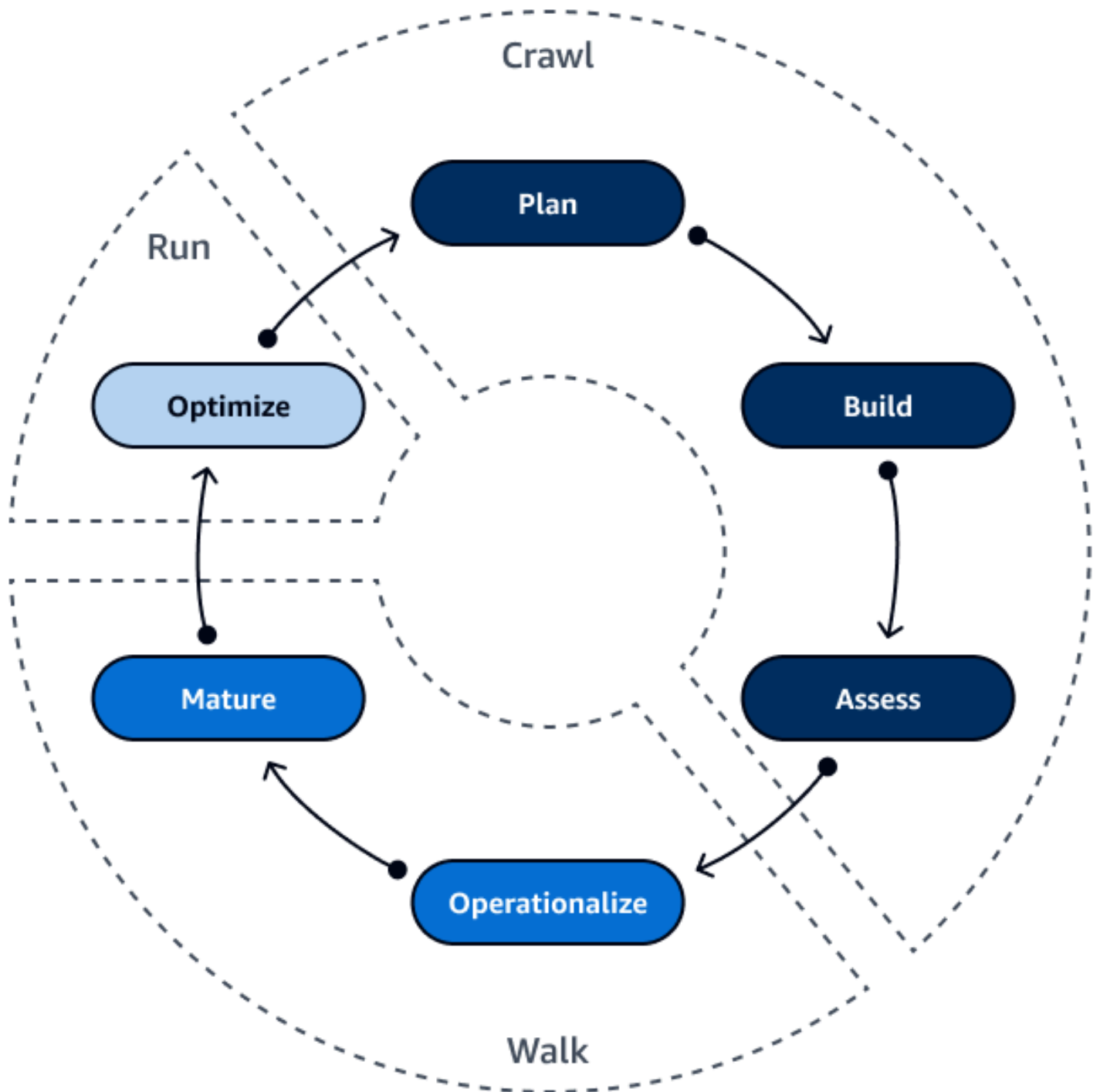
Amazon Web Services ([寄稿者](#))

2023 年 12 月 ([ドキュメント履歴](#))

多くの組織にとって、クラウドへの移行における最優先事項と考慮事項はセキュリティです。クラウドセキュリティ機能とコントロールの実装は 1 回限りのアクティビティではなく、反復モデルです。クラウド運用が増えるにつれて、セキュリティ体制と成熟度が徐々に向上します。例えば、AWS 管理ポリシーから始めて、組織の準備ができたら、最小特権の原則に従うカスタムポリシーを実装できます。

このガイドでは、クラウドセキュリティにおける組織の成熟を加速するためのクロール、ウォーク、実行の方法論を使用するためのロードマップを提供します。セキュリティ機能を自動化するための step-by-step アプローチを定義します。また、AWS のサービス および 機能を最大限に活用する方法を実用的に説明します。このガイドは、クラウドの課題と機会、および で迅速に前進し、成功を達成する方法を理解するのに役立ちます AWS。

クラウドジャーニーでは、フレームワークの構築、運用の管理と成熟、プロセスの最適化が必要です。次の図は、クロール、ウォーク、実行の方法論の各段階の段階である計画、構築、評価、運用化、成熟、最適化を示しています。



クロールステージは、現在のセキュリティ体制の計画、構築、評価で構成されます。ウォークステージでは、人材、プロセス、テクノロジーを運用し、調整と測定を通じて運用を成熟させます。実行ステージは、評価と自動化による最適化で構成されます。

クロールステージ: 計画、構築、評価



クロールステージは計画から始まります。計画には、セキュリティの範囲を決定し、組織に最適なモデルを選択することが含まれます。プランを確立したら、基盤の構築を開始できます。その後、現在のセキュリティ体制を評価し、セキュリティインフラストラクチャを構築するとすぐに規律を設定します。クロールステージは反復的です。クラウドでの反復は、オンプレミス環境での反復よりも高速です。クラウド機能を成熟させると、反復のプロセスが加速します。

クロールステージのフェーズは次のとおりです。

- [計画](#) – スコープを見極め、モデルを選択するにはどうすればよいですか？
- [ビルド](#) – フレームワークをどのように確立しますか？
- [評価](#) – 現在のセキュリティ体制はどのようなものですか？

計画: セキュリティの範囲とモデルを確立する

計画は、セキュリティモデルを成熟させる際の反復プロセスです。計画プロセスの主なステップは次のとおりです。

- [セキュリティスコープについて](#) – セキュリティの範囲はクラウドの使用方法によって異なります。
- [セキュリティモデルの選択](#) – セキュリティユースケースに最適なセキュリティモデルを特定します。
- [ビジネス目標モデルの作成](#) – 成功を測定するための明確な目標とメカニズムを定義します。

計画を立てるときは、次の点を考慮してください。

- 進んで反復します。反復はクラウド内で一定です。反復は、プランのギャップを特定するのに役立ちます。
- サービスから開始しないでください。必要なサービスを選択するのではなく、プランから始めます。これにより、組織は意図した成果を達成できます。

セキュリティスコープについて

責任 AWS 共有モデルでは、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、 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 AWS クラウド、データやアプリケーションなどのサービスの使用を保護する責任があります。

この共有モデルは、ホストオペレーティングシステムや仮想化レイヤーから、サービスが運用されている施設の物理的なセキュリティまで、多くのコンポーネントを AWS 運用、管理、制御するため、コンプライアンスと運用上の負担を軽減するのに役立ちます。マネージドサービスは、AWS がパッチ適用や脆弱性管理などの一部のセキュリティタスクを管理できるようにすることで、セキュリティとコンプライアンスの義務を軽減するのに役立ちます。Well[AWS -Architected フレームワーク](#)では、マネージドサービスを使用することがベストプラクティスです。一般的に、インフラストラクチャがモダナイズされると、サービスプロバイダーにより多くの責任が移ります。

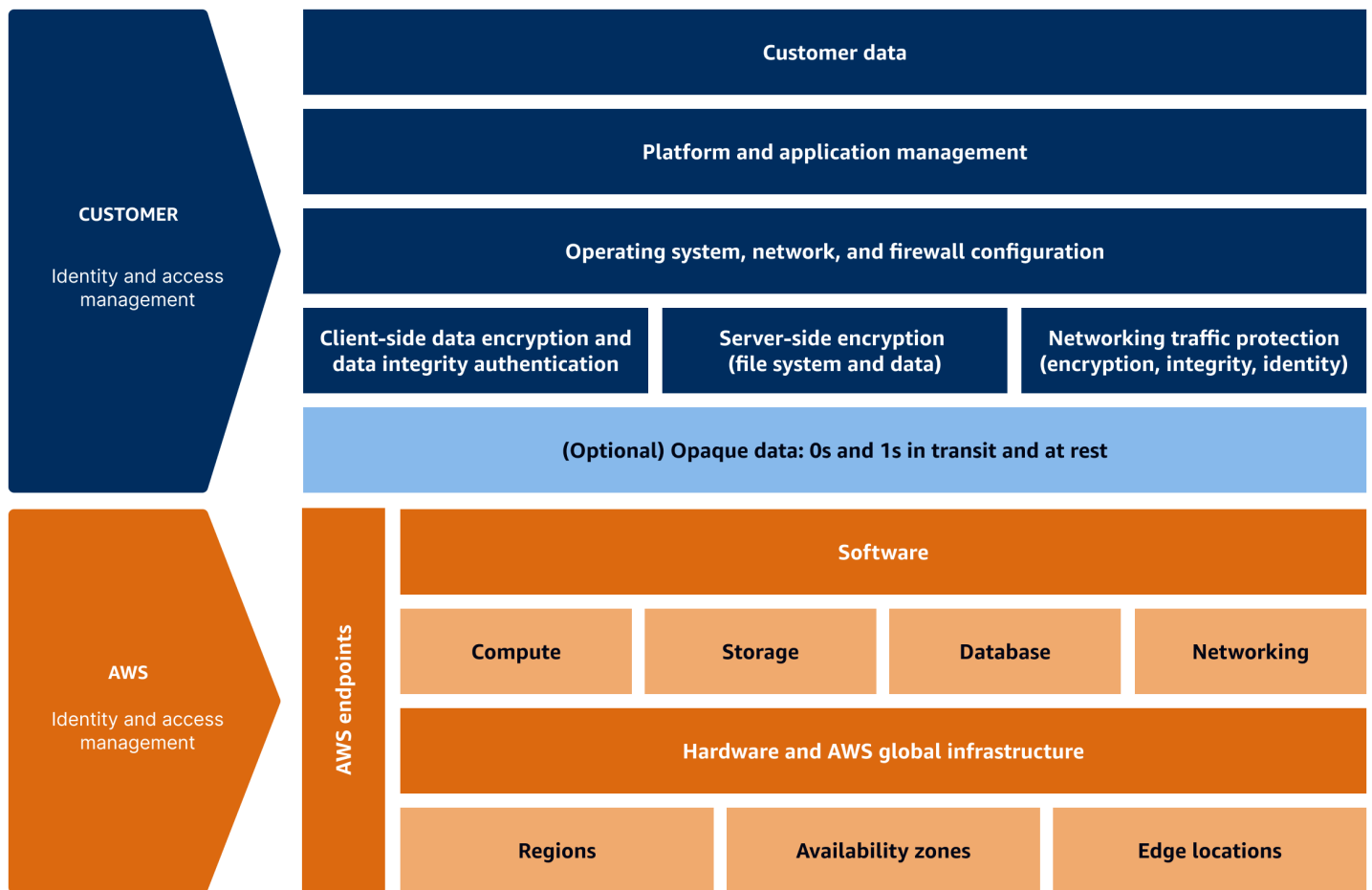
以下は、選択したサービスに基づいてセキュリティ範囲がどのように変化するかを理解するのに役立つ 3 つの異なるサービス例です。

- [インフラストラクチャサービス](#)
- [コンテナサービス](#)
- [サーバーレスサービス](#)

セキュリティに対するお客様の責任は静的ではなく、選択したアーキテクチャのタイプによって変わります。時間、労力、コストは、選択したクラウドアーキテクチャの影響を受けます。

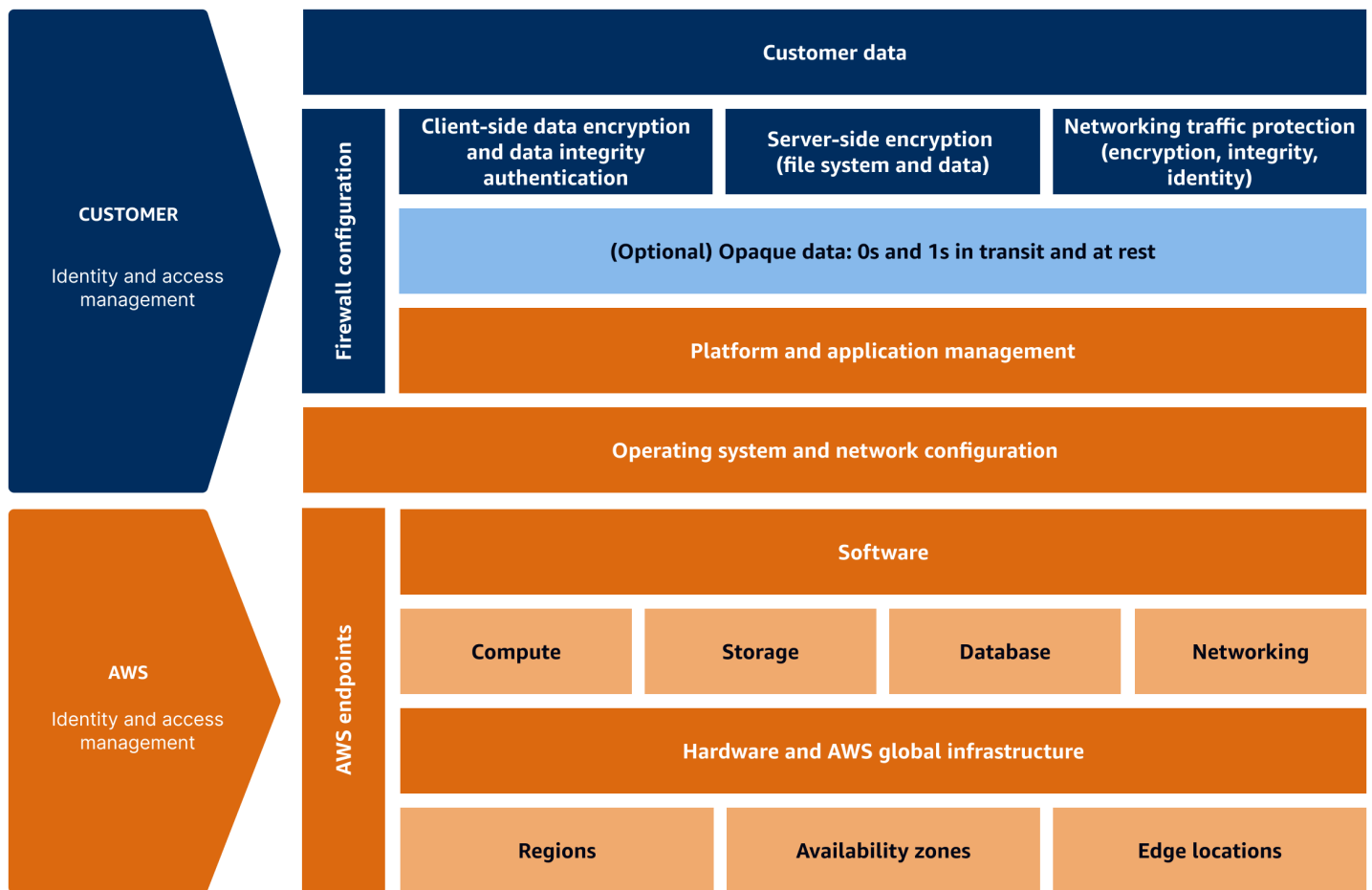
インフラストラクチャサービス

インフラストラクチャサービスの場合、基盤となるインフラストラクチャの保護 AWS に焦点を当てます。インフラストラクチャサービス内では、他のモデルと比較して、プラットフォームセキュリティ、OS パッチ適用、アプリケーション管理に対応する必要があるため、スコープはお客様にとって大きくなります。Amazon Elastic Compute Cloud (Amazon EC2) は、一般的なインフラストラクチャサービスの例です。



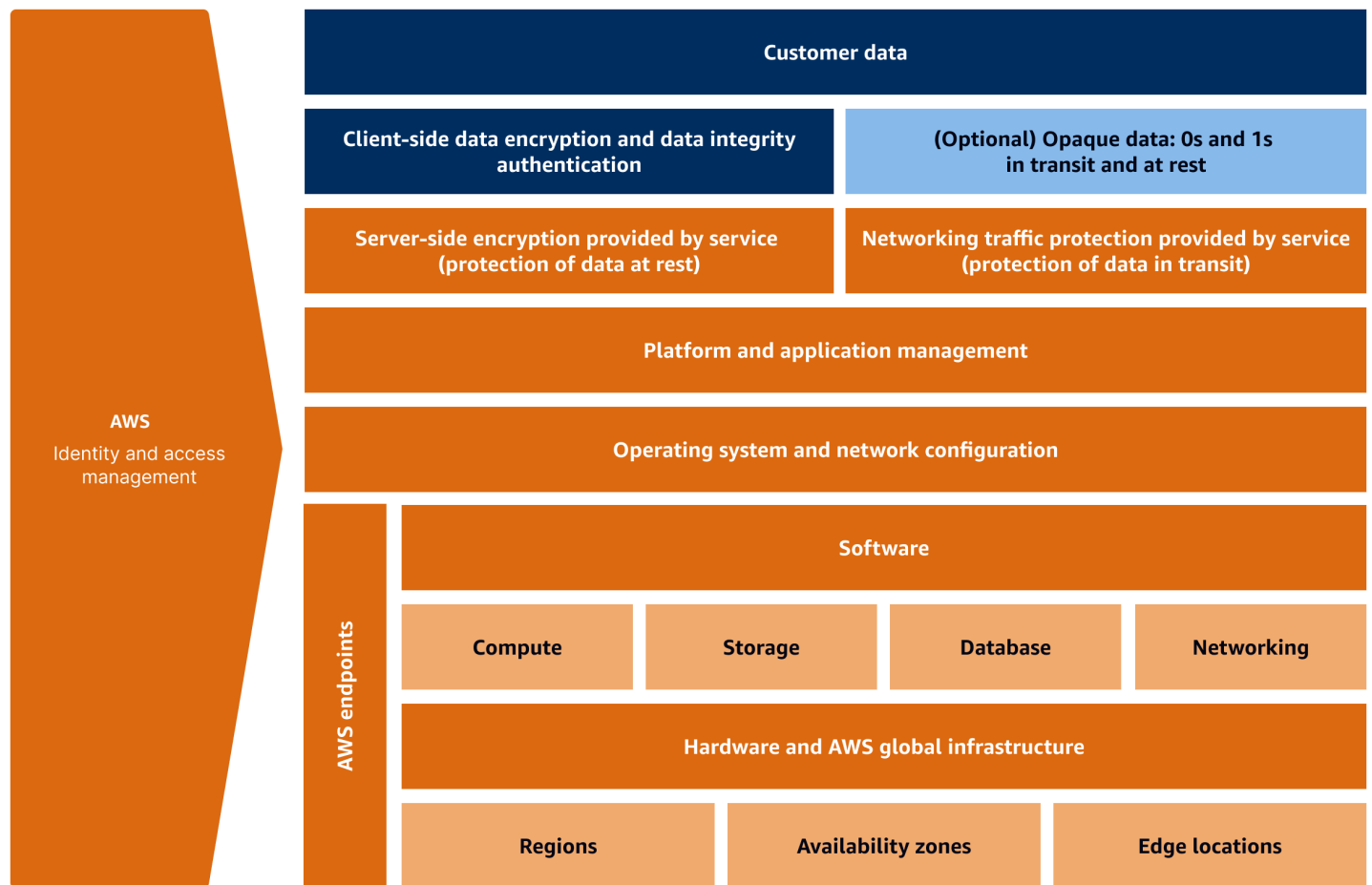
コンテナサービス

インフラストラクチャがより抽象化され、モダナイズされるにつれて、フットプリントは小さくなります。一部のセキュリティ要素の責任がにシフトするため、スコープは縮小します AWS。コンテナサービスは、バックエンドの責任の一部が戻る例です AWS。例えば、オペレーティングシステム (OS) の設定、ネットワーク設定、プラットフォーム管理、アプリケーション管理を担当 AWS します。一般的なコンテナサービスの例としては、Amazon Elastic Kubernetes Service (Amazon EKS)、Amazon Elastic Container Registry (Amazon ECR)、Amazon Elastic Container Service (Amazon ECS)、 などがあります AWS Fargate。



サーバーレスサービス

サーバーレスサービスを使用する場合、セキュリティの責任のほとんどすべてが に属します AWS。責任の範囲は最小限です。たとえば、マネージドサーバーレスデータベース (DB) を使用すると、ネットワーク、ハードウェア、オペレーティングシステムを保護する必要がなくなります。すべての OS と DB のパッチ適用は でカバーされています AWS。唯一の懸念事項は、暗号化と認証を通じてデータへのアクセスを保護することです。



セキュリティモデルの選択

さまざまなセキュリティモデルやアプローチから選択できます AWS。アプローチと最適なモデルの選択は、対象者、目標とするビジネス成果、全体的なビジネスプロセスによって異なります。複数のモデルのブレンドを使用できます。

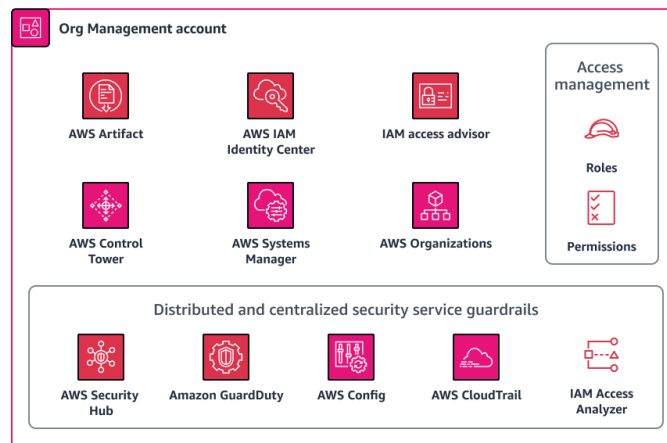
以下は、いくつかの一般的なモデルです。

- [アーキテクチャモデル](#)
- [成熟度モデル](#)
- [ガバナンスモデル](#)

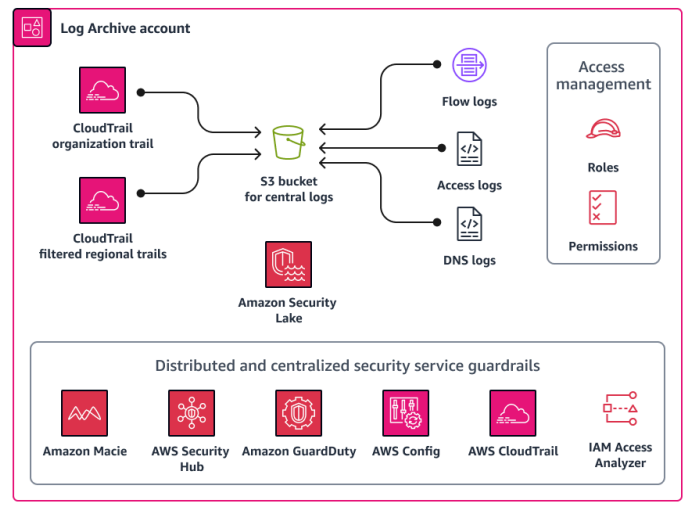
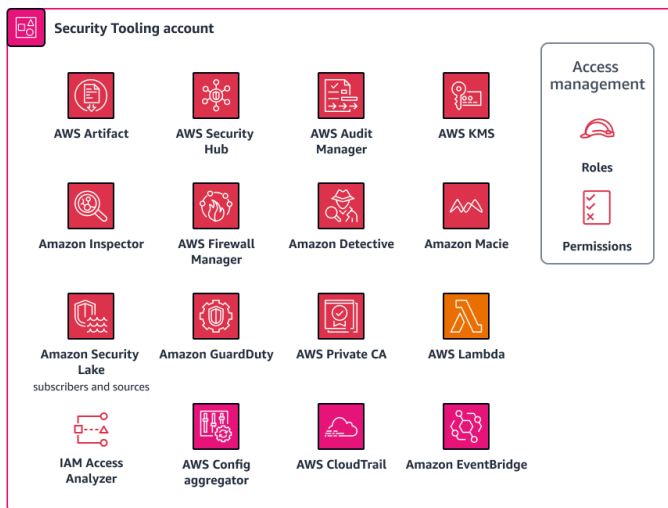
各モデルには独自の利点と欠点があります。どのアプローチが組織に最も適しているかを考慮することが重要です。インフラストラクチャをモダナイズし、クラウド戦略を採用するプロセスの早い段階で、セキュリティプロフェッショナルを関与させます。選択したモデルは、組織内の役割と責任に大きな影響を与えます。

アーキテクチャモデル

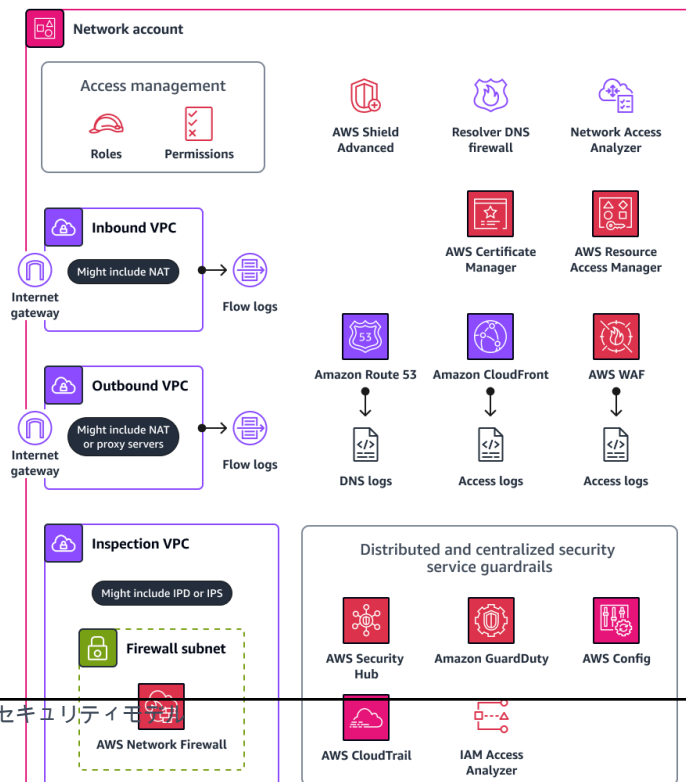
次の図は、[AWS セキュリティリファレンスアーキテクチャ](#)を示しています。このアーキテクチャアプローチは、セキュリティモデルのブループリントを提供します。このアプローチは、組織内の技術チームとやり取りする場合に最適です。これは、理想的な将来の目標を設定するのに役立ちます。また、多くのコンプライアンスと AWS フレームワークとも一致します。



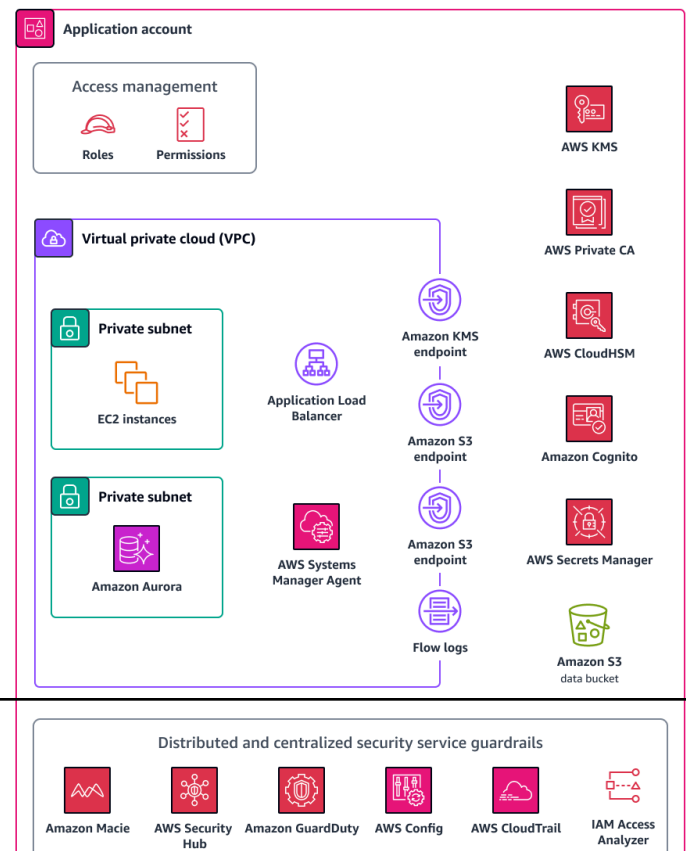
Security OU



Infrastructure OU



Workloads OU



アーキテクチャモデルの利点：

- Health Insurance Portability and Accountability Act (HIPAA) および Health Information Trust Alliance Common Security Framework (HITRUST CSF) の要件に準拠
- アーキテクチャの視点を提供する
- 大企業向けのクラウド戦略とガイダンスに合わせる
- [AWS クラウド導入フレームワーク \(AWS CAF\)](#) と連携
- [AWS Well-Architected フレームワーク](#) に合わせる

アーキテクチャモデルの欠点：

- ビジネス中心ではなくテクノロジー中心

成熟度モデル

[AWS セキュリティ成熟度モデル](#) アプローチは、セキュリティ対策の実装に優先順位を付け、リスクの管理と軽減に焦点を当てています。このアプローチはセキュリティディレクターや CISOs に適していますが、ビジネスに重点を置いていません。

成熟度モデルの利点：

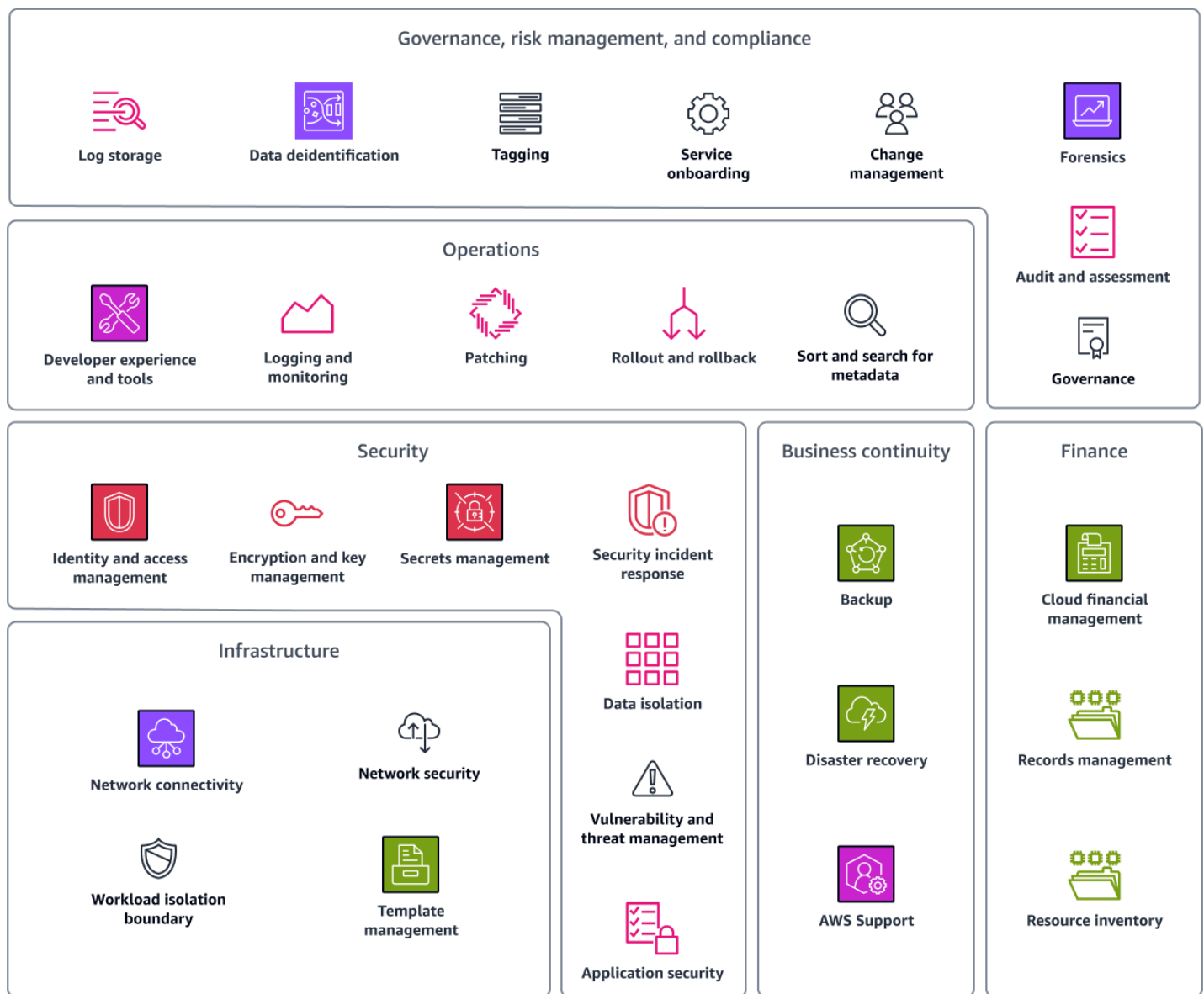
- セキュリティに重点を置いている
- アジャイルベースの実装アプローチの使用に焦点を当てたモデルである
- リスクの迅速な軽減に役立ちます
- [AWS クラウド導入フレームワーク \(AWS CAF\)](#) と連携

成熟度モデルの欠点：

- ビジネス中心ではなくテクノロジー中心

ガバナンスモデル

[Cloud Foundation on AWS](#) モデルは、ガバナンス、リスク管理、コンプライアンス (GRC) アプローチを使用して、組織がセキュリティとコンプライアンスの要件を満たすのに役立ちます。クラウド環境が従うべき全体的なポリシーを定義します。このモデル内の機能は、アクション項目の定義、リスク選好の定義、内部ポリシーの調整に役立ちます。



Cloud Foundation モデルは、AWS クラウド 環境の構築と進化に役立つ機能およびガバナンスガイドです。これは、一連の定義、シナリオ、ガイド、自動化に基づいています。このガイドには、環境を確立 AWS クラウド するための人材、プロセス、テクノロジーの側面が含まれています。クラウド基盤に不可欠な 6 つの機能カテゴリについて説明します。

- ガバナンス、リスク管理、コンプライアンス
- オペレーション
- セキュリティ
- ビジネス継続性
- 財務

• インフラストラクチャ

また、このガイドでは、各機能の例、タイムライン、さらに詳しい説明も提供しています。

ガバナンスモデルの利点：

- 幅広いテクノロジーに重点を置いている
- 信頼性を重視して設計されています
- 運用アプローチを使用する

ガバナンスモデルの欠点：

- ビジネス中心ではなくテクノロジー中心

ビジネス目標モデルの作成

ビジネス目標モデルには、ビジネス成果の定義が含まれます。これは、AWS クラウド導入フレームワークと AWS Well-Architected フレームワークに似ています。このアプローチは、ターゲットとなるビジネス成果を解釈することで、ビジネスが関心を持っていることに焦点を当てています。このアプローチの価値は、ビジネス目標をセキュリティ目標に簡単に結び付けることができることです。ビジネス目標の例は、「可視性を自動化し、ベストプラクティスに照らして測定して継続的にリスクを軽減することで、安全な外部接続と新しいユーザーや環境の高速プロビジョニングを有効にする」です。対応するビジネス成果を達成するのに役立つテクノロジー目標を確立します。ビジネス目標モデルは、可視性の維持などのセキュリティ目標に結びついています。次に、セキュリティリスクを軽減するために、AWS Identity and Access Management (IAM) セキュリティのベストプラクティスなどの技術的な目標を実装します。

ビジネス目標アプローチの利点：

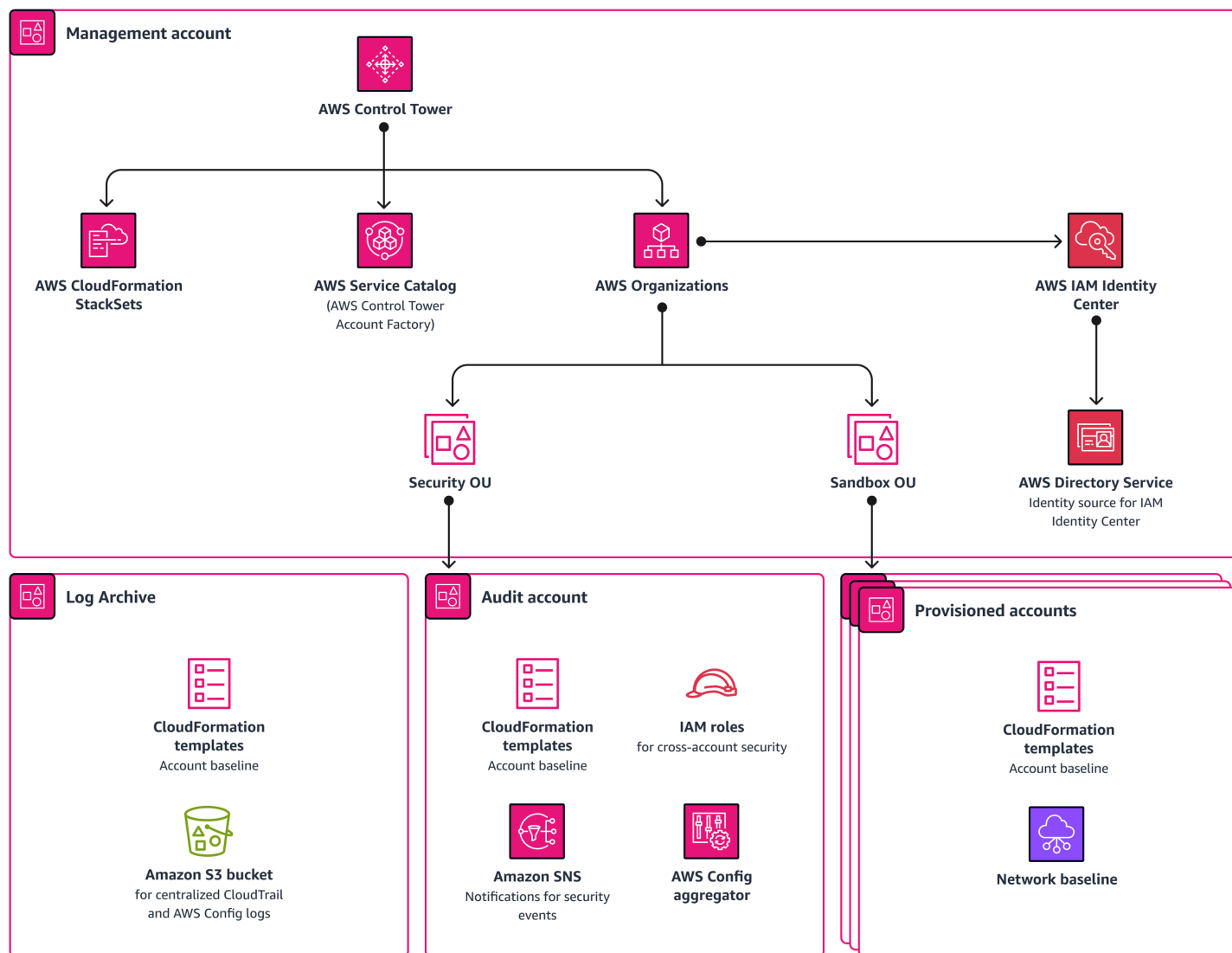
- コストの根拠を含む
- 明確でビジネスに沿ったセキュリティ上の方向性を提供します
- 目標とするビジネス成果を達成して成功の尺度を定義する

ビジネス目標アプローチの欠点：

- ビジネスが何を望んでいるかを把握する必要があるため、時間がかかる場合があります
- テクノロジーに重点を置いているのではなく、ビジネスに重点を置いている

ビルド: 強力なクラウドセキュリティ基盤の基礎を築く

計画を立てたので、次のステップは基礎を整えることです。このステップでは、複数のアカウントにわたって安全で回復力があり、スケーラブル AWS で、自動化された初期のクラウド基盤を構築する方法を示します。基盤の構築は、ビジネス目標に応じて特別に設計およびカスタマイズできます。コントロールを新しいランディングゾーンに適用させるか、既存のランディングゾーンに含めることができます。の自動化[AWS Control Tower](#)は、のセキュリティ基盤の構築に役立ちます AWS クラウド。次の図は、を介してセットアップされるランディングゾーンを示しています AWS Control Tower。



AWS Control Tower は、、、など AWS Organizations、AWS のサービス ユーザーに代わって複数の をオーケストレーション AWS Service Catalogします AWS IAM Identity Center。新しいランディングゾーンは 1 時間以内に設定でき、そのランディングゾーンはセキュリティとコンプライアンス

の要件を満たすように設計されています。AWS Control Tower は、規範的なセキュリティのベストプラクティスに従ってランディングゾーンを設定します。AWS Control Tower は、アカウントとエンドユーザーの可視性と制御を強化することで、クラウドプロビジョニングの管理に役立ちます。管理者は、コンピューティングリソースの効率的な割り当てと監視、ロールベースのアクセスコントロールの実装、ロギングとモニタリングツールによるパフォーマンスのモニタリング、コストの効果的な管理、デプロイプロセスの自動化、セキュリティ対策の強制、業界標準への準拠の確保を行うことができます。

AWS Control Tower は、ベストプラクティスに基づいて、安全で準拠したマルチアカウント AWS 環境をセットアップして管理するための最速の方法です。マルチアカウント戦略で説明されている の操作 AWS Control Tower とベストプラクティスの詳細については、AWS [AWS 「マルチアカウント戦略: ベストプラクティスガイド」](#) を参照してください。

AWS Control Tower が最速のアプローチですが、それだけではありません。重要なのは、ランディングゾーンをセットアップして、少なくとも以下を提供することです。

- マルチアカウント管理
- ID とフェデレーティッドアクセス管理
- ログの一元化されたアーカイブ
- クロスアカウント監査アクセス
- エンドユーザーアカウントのプロビジョニング
- 一元的なモニタリングと通知

評価: 現在のクラウドセキュリティ体制を評価する

ランディングゾーンに何かをデプロイする前に、ランディングゾーンを評価して要件を満たし、ベースラインを確立します。この手法は、雲の姿勢の評価と呼ばれます。クラウドインフラストラクチャ全体のリスクを特定して修正するのに役立ちます。クラウドセキュリティ体制を評価すると、クラウド環境内の関連するセキュリティコントロールが可視化されます。

クラウド体制評価の利点は次のとおりです。

- 現在のセキュリティ体制を理解し、リスクプロファイルの軽減、既存の脆弱性の修復、設定ミスの修正に関する推奨事項を取得するのに役立ちます。
- これにより、セキュリティのベストプラクティスを特定して、誤った手順を回避し、ビジネスリスクを軽減できます。
- 改善を追跡し、成功を測定するのに役立つメトリクスを提供します。

このセクションでは、環境でクラウド体制評価を実行するために使用できる サービスとツール Prowler、AWS Security Hub および について説明します。

Prowler

[Prowler](#) は、セキュリティのベストプラクティスやその他の AWS セキュリティフレームワークや標準への準拠について、アカウントを評価、監査、モニタリングするのに役立つオープンソースのコマンドラインツールです。設定を検査し、セキュリティの問題を特定します。Prowler マルチアカウント環境で を使用することも、サードパーティーベンダーがこれを使用して AWS 環境のセキュリティを評価することもできます。

の利点は次のとおりですProwler。

- 無料およびオープンソースです。
- 柔軟なデプロイオプションがあり、スケーラブルです。
- の [Center for Internet Security \(CIS\) Benchmark AWS](#)、一般データ保護規則 (GDPR)、HIPAA などのコンプライアンスチェックを実行します。
- スナップショットとベースラインの作成に役立ちます。

[Prowler Pro](#) は継続的な評価のオプションでもあります。は 250 を超えるチェックProwler Proを実行し、スキャン結果を視覚化するのに役立つ高速スキャンとダッシュボードを提供します。

AWS Security Hub

[AWS Security Hub](#) は、 のセキュリティ状態の包括的なビューを提供します AWS。また、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。と統合 AWS Control Tower されているため、AWS Control Tower サービスを通じて Security Hub の検出コントロールを設定できます。セキュリティの成熟度を高める目的は、評価プロセスを 1 回限りのスナップショットから、進行状況をモニタリングするための継続的なプロセスに成熟させることです。

Security Hub の利点は次のとおりです。

- 環境の現在のステータスを表示する統合ダッシュボードを提供し、問題の特定と修復に役立ちます。
- 自動チェックを使用して継続的な評価を実行します。

ウォークステージ: 運用と成熟



ウォークステージでは、運用化に焦点を当てます。この段階では、組織は現在の運用モデルを評価し、クラウドにどのように適応させるかを決定し、それらの変更を実装して、進捗状況を測定する必要があります。これには、スキル、運用プロセス、テクノロジーへの対応が含まれます。クラウドデプロイの調整と進行状況の測定は、成功を検証するためにウォークステージ全体で不可欠です。

ウォークステージのフェーズは次のとおりです。

- [運用](#) – クラウドの人材、テクノロジー、プロセスをどのように準備しますか？
- [成熟](#) – 進捗状況と成功はどのように測定しますか？

運用: 組織が成熟したクラウドセキュリティ体制に備える

運用負荷をクラウドにデプロイするプロセスを進めるには、人、プロセス、テクノロジーの連携に集中することが重要です。プロセスとスキルはオンプレミスの運用とは異なる可能性が高いため、これはクラウド環境で特に重要です。このセクションでは、フレームワークを使用して人材、プロセス、テクノロジーを連携させ、フレームワークが期待される成果の達成に役立っていることを確認します。

AWS クラウド導入フレームワーク

[AWS クラウド導入フレームワーク \(AWS CAF\)](#) は、AWS のサービスと機能を革新的な方法で使用することで、ビジネス成果を加速するのに役立ちます。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、クラウドトランスフォーメーションの成功を支える 6 つの特定の組織的視点を特定します。各視点には、クラウドの準備状況を向上させ、クラウドトランスフォーメーションジャーニーを加速するのに役立つ機能が含まれています。

次の図は、CAF の 6 AWS の視点と各視点の機能を示しています。詳細については、[「クラウド導入フレームワークの概要」の「基本的な機能 AWS」](#)を参照してください。



期待される成果

AWS CAF を使用して人材、プロセス、テクノロジーを連携させると、次の成果が期待できます。

- DevSecOps パイプラインとプロセス – 統合されたセキュリティツールを使用して DevOps パイプラインを実装すると、Infrastructure as a Code (IaC) をより安全にデプロイできます。オープンソースの静的コードアナライザーである [cfn_nag](#) (GitHub) などのコードスキャンとセキュリティチェックをパイプラインプロセスに実装できます。
- タグ付けとアセット管理 – タグは、クラウド内のリソースをより効率的かつ一貫して管理するのに役立ちます。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。クラウド

の絶えず変化する性質に適応できる動的なアセット管理戦略を策定することが重要です。[AWS Systems Manager インベントリ](#)は、タグの割り当てに役立つため、リソースをすばやく検索、管理、識別できます。

- モニタリングと検出の統合 – クラウドからオンプレミスのセキュリティオペレーションセンター (SOCs) およびセキュリティ情報とイベント管理 (SIEM) システムにアラートを送信する方法を確立することが重要です。[Amazon GuardDuty](#) は、ログを分析して処理し、環境内の予期しないアクティビティや不正なアクティビティの可能性を特定する継続的なセキュリティモニタリングサービスです AWS。また、多くのサードパーティー製ツールとも統合されています。
- クラウドインシデント対応計画とプログラム – クラウドアラートの処理を担当する担当者が、オンプレミスアラートと比較して、これらのアラートを取り込むプロセスに精通し、クラウドアラートへの対応方法を理解していることが重要です。インシデント対応機能を向上させるには、ログ分析に Amazon Detective を使用するように担当者をトレーニングします。[Amazon Detective](#) は、セキュリティ上の検出結果や疑わしいアクティビティの根本原因の分析、調査、特定に役立ちます。Amazon Detective はインシデント対応計画の一部である必要があります。
- クラウド脆弱性管理 – クラウドの脆弱性を管理するプロセスは、オンプレミス環境とは異なります。従来の脆弱性管理に加えて、インフラストラクチャコードレイヤーも評価する必要があります。[Amazon Inspector](#) は、リソースの脆弱性と意図しないネットワークへの露出を継続的に評価する自動脆弱性管理サービスです。
- クラウド体制管理 – 「[評価](#)」セクションで説明されているように、クラウド体制管理はクラウドセキュリティの重要な側面です。AWS Security Hub を使用して、セキュリティのベストプラクティスチェックを自動化し、すべての で全体的なクラウド体制を評価できます AWS アカウント。
- クラウドセキュリティトレーニング – 従業員がクラウドセキュリティに習熟できるように、適切なトレーニングを提供することが重要です。これには、リソースへのアクセスを提供し、従業員が必要な知識とスキルを習得するための時間を割り当てることが含まれます。は、[AWS スキルビルダー](#)など、スキルアップと教育のための多くのトレーニングリソース AWS を提供します。

成熟: プロセス、ツール、リスクの調整と測定

クラウドセキュリティモデルの成熟段階では、セキュリティチームを AWS クラウド導入フレームワーク (AWS CAF) セキュリティ機能と連携させ、アジャイルプロセスを導入することに重点が置かれています。この連携により、専門チームはロードマップや長期計画を組み込んで、短いスプリントでイノベーションを加速できます。成熟フェーズでは、IT 運用とのコラボレーションと、深く専門的なクラウドスキルのスケールアップが強調されます。各セキュリティ機能は、効率と影響を強化す

るための主要なツールとプロセスを実装し、段階的な変更と全体的な影響を測定するメトリクスとレポートメカニズムの開発も行います。

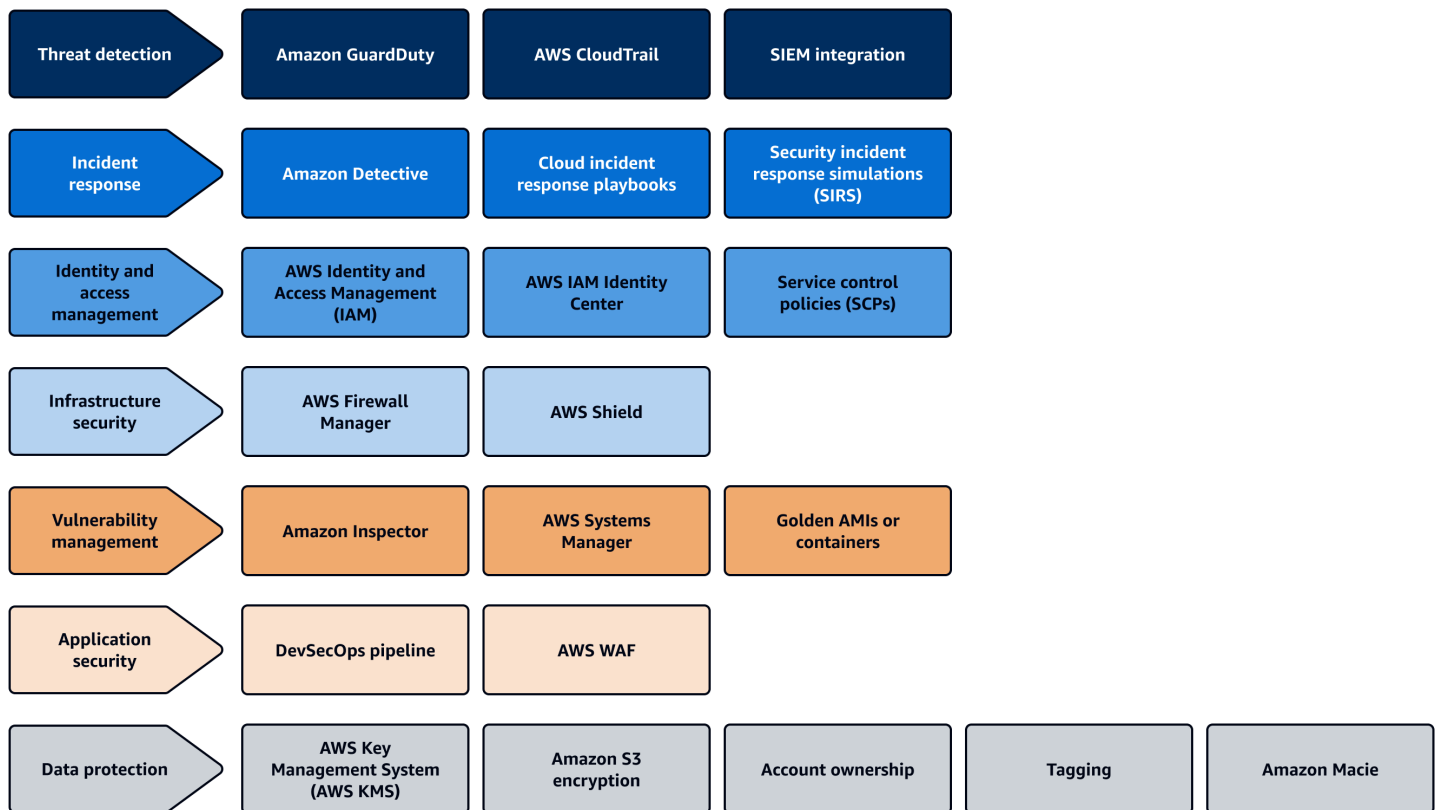
このフェーズでは、次の操作を行います。

- [プロセスのチューニングと測定](#)
- [ツールの調整と測定](#)
- [リスクの調整と測定](#)
- [成熟フェーズのユースケースの例を確認する](#)

プロセスのチューニングと測定

[アジャイルアプローチ](#)は、より柔軟性とイノベーションを提供し、新しいアイデアを迅速にテストして実装するのに役立ちます。セキュリティチームをインシデント対応者や脆弱性マネージャーなどの特殊な役割に分割します。ロールは、AWS クラウド導入フレームワーク (AWS CAF) の機能に対応する次のイメージのカテゴリと一致する必要があります。アジャイルアプローチは、チームがセキュリティの潜在的なギャップを大規模に考え、発見し、簡素化し、特定することを奨励します。これにより、将来の改善のためのユースストーリーやロードマップのバックログが作成されます。

アジャイルプロセスでは、特定のツールの機能だけに頼るのではなく、より動的で適応的なソリューションが可能になります。フェイルファストは、開発ライフサイクルを短縮するために頻繁かつ段階的なテストを使用する哲学であり、アジャイルアプローチの重要な部分です。変更を加えてテストし、現在のアプローチを継続するか、別のアプローチに切り替えるかを決定します。チームがこのサイクルで作業する場合、組織はクラウドの高速な性質を最新の状態に保つのに役立ちます。集中トレーニングも重要であり、クラウドセキュリティの特定のドメインに固有のトレーニングを提供する必要があります。



Note

このイメージには、CAF AWS のセキュリティ保証機能とセキュリティガバナンス機能は含まれていません。このガイドはセキュリティオペレーションに焦点を当てており、セキュリティの保証とガバナンスはこのガイドの対象外です。セキュリティ保証の詳細については、YouTube の [AWS re:Inforce 2023 - Scaling compliance with AWS Control Tower](#) を参照してください。

組織では、組織がクラウドでの迅速な開発と変化に対応できるアジャイルアプローチを使用します。以下は、クラウド環境で実験と反復を開始するいくつかの方法です。

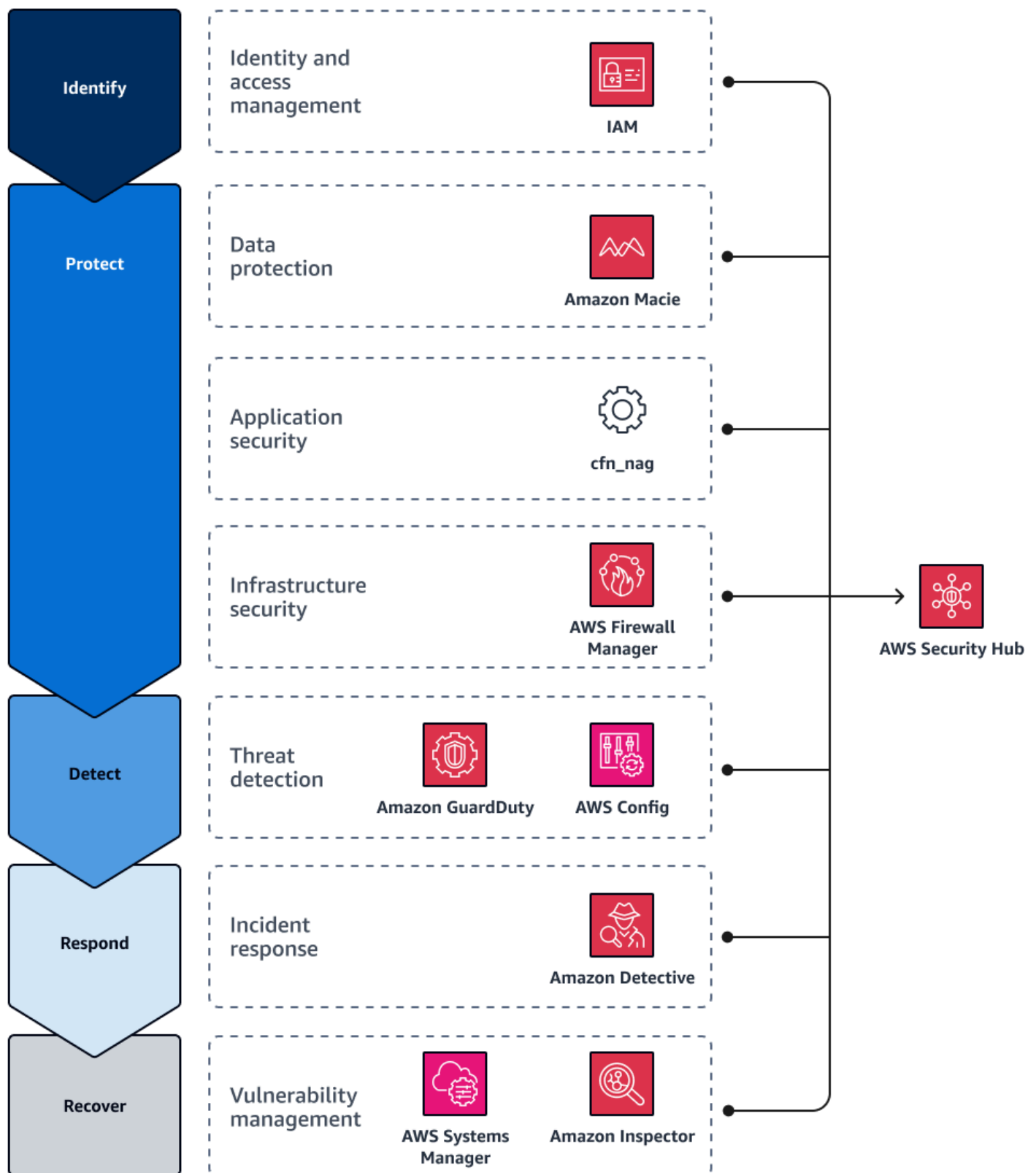
- 前の図に示すように、CAF AWS で定義されているカテゴリに特化します。
- より動的にするには、オペレーションではなくイノベーションに焦点を当てます。
- テスト、フェイルファスト、実装を迅速に実行し、このサイクルを続行してビジネスに追いつくことができるようにすることで、スプリントをすばやく進めます。
- 継続的な運用をサポートするには、可能であれば、クラウドベースの環境とオンプレミス環境に合わせてプロセスを調整します。

- 個人がドリルダウンして 1 つの領域に集中できるようにするには、広範なトレーニングではなく、集中トレーニングを提供します。
- 大きな考え方をし、「What ifs」を調査し、バックログ (ロードマップやギャップなど) を作成するよう促します。

ツールの調整と測定

さまざまなセキュリティドメインに特化したチームを確立したら、チームを連携させます。[AWS Security Hub](#)は、これを実現するのに役立ちます。Security Hub は、フレームワークの進行状況をモニタリングするための一元化された統合ダッシュボードを提供します。また、多くのサードパーティ製ツールを AWS セキュリティサービスと統合します。

NIST ウェブサイトの米国国立標準技術研究所 (NIST) [Cybersecurity Framework](#) は、識別、保護、検出、対応、復旧の 5 つの機能で構成されています。次の図は、各関数 AWS のサービスで異なるを使用し、統合レポート用に Security Hub に結果を送信するようにそれらのサービスを設定する方法を示しています。他のツールを使用する場合は、Security Hub API、AWS Command Line Interface (AWS CLI)、AWS Security Finding 形式 (ASFF) を使用してカスタム統合を作成できます。Security Hub と他のサービスとの統合の詳細については、Security Hub ドキュメントの「[での製品の統合 AWS Security Hub](#)」を参照してください。



Security Hub は、これらのすべてのサービスおよびツールと統合され、以下を提供します。

- 更新を表示し、チームが所定の手順を繰り返すのに役立つ統合ダッシュボードを提供します。
- Amazon [Amazon Macie](#) [Amazon GuardDuty](#) [Detective](#) などの AWS セキュリティサービスと自動的に統合
- [Prowler](#) や などのサードパーティーツールとの統合をサポート [cfn_nag](#)
- Security Hub API AWS CLI や AWS Security Finding 形式 (ASFF) などのツールとのカスタム統合をサポート

リスクの調整と測定

ウォークステージの成熟フェーズでは、AWS Security Hub を使用してセキュリティリスクを継続的に調整および測定できます。Security Hub は、組織のセキュリティ体制を継続的に評価し、特定された問題を修正するためのアクションを実行します。Security Hub は、全体、サービス AWS アカウント、およびサポートされているサードパーティーパートナーからのセキュリティ検出結果を一元化し、優先順位を付けます。これにより、セキュリティの傾向を分析し、優先度の高いセキュリティ問題を特定できます。

Security Hub は数百のセキュリティチェックを実行し、AWS 環境に対するリスクに基づいて分類します。Security Hub コンソールの統合ダッシュボードで、セキュリティコントロールに対するスコアを表示できます。詳細については、[Security Hub ドキュメントの「セキュリティスコアの決定」](#)を参照してください。このダッシュボードを通じて、DevSecOps 関数は、失敗したチェック、セキュリティ問題の重要度、影響を受けると AWS リージョン リソースをすばやく特定できます。特定されると、DevSecOps チームは問題の優先順位付けと修正を行うことができます。問題が修正されると、Security Hub は自動的に状態を更新します。

成熟フェーズのユースケースの例を確認する

成熟段階の例を次に示します。これらの例では、さまざまなビジネス目標のモデル、ツール、プロセスを実用的なレベルで詳しく説明します。

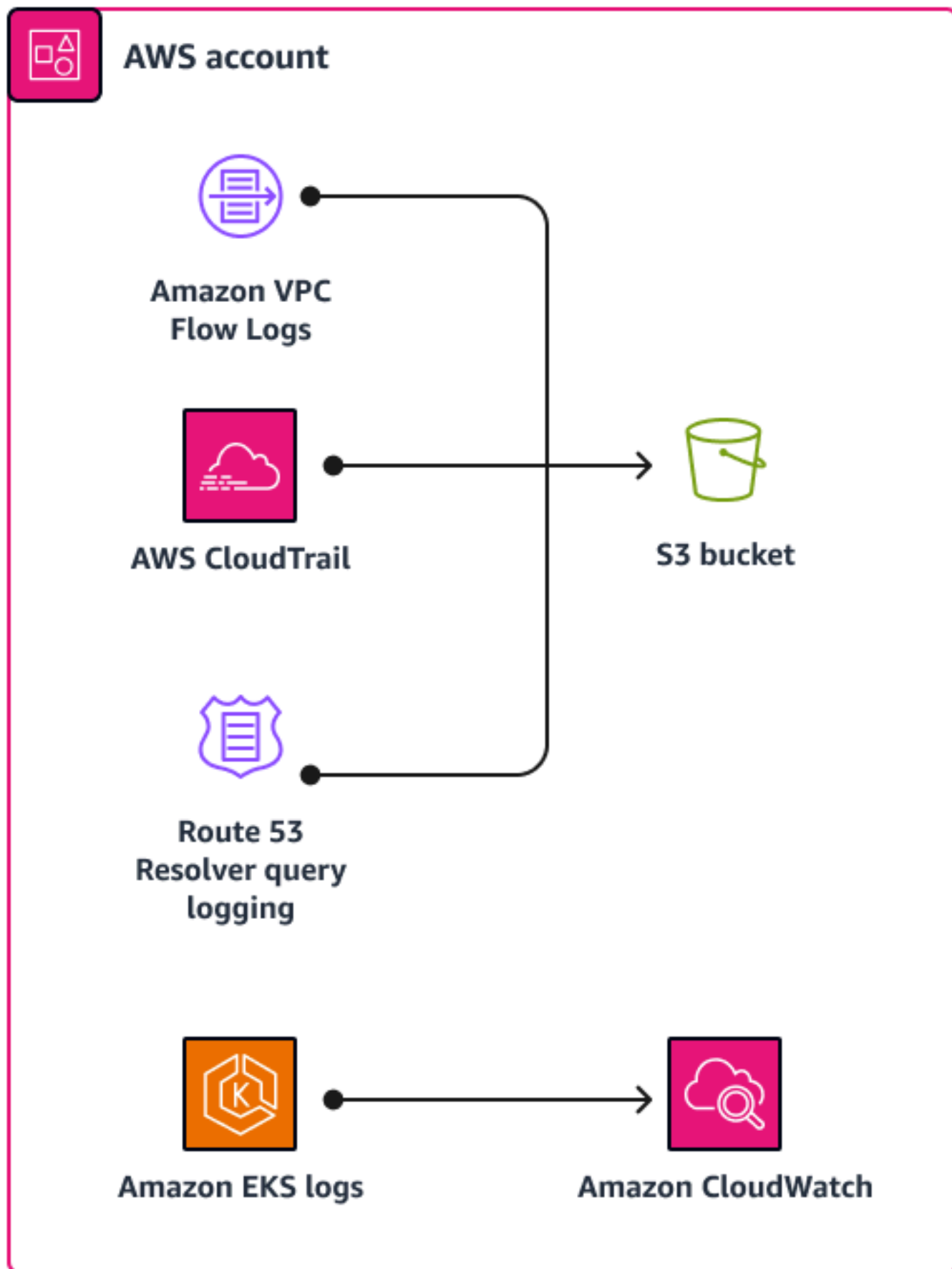
成熟: 脅威検出の例

検出コントロールのビジネス成果: リスクを軽減し、クラウドリソースの迅速な使用と開発を可能にするために、クラウドインシデントの可視性と検出速度を向上させます。

ツール: [Assisted Log Enabler for AWS](#) (GitHub) は、セキュリティインシデントの途中でログ記録を有効にするのに役立つオープンソースツールです。これにより、インシデントの可視性をすばやく向上させることができます。

ユースケースの例：次の図に示す単一アカウントのユースケースについて考えてみましょう。詳細な調査が必要なイベントがあります。ログ記録が有効になっているかどうか分かりません。この場合、最適なアクションは、でリハーサルを実行して、有効または無効にされているサービスAssisted Log Enablerを確認することです。は、AWS CloudTrail 証跡、DNS クエリログ、VPC フローログ、およびその他のログAssisted Log Enablerをチェックします。有効になっていない場合、はそれらAssisted Log Enablerを有効にします。はすべての でログ記録をチェックしてオンにAssisted Log Enablerできます AWS リージョン。

また、スロットAssisted Log Enablerリングアップまたはスロットリングダウンもできます。ドライランを完了し、イベントを閉じて問題を解決したら、このレベルのログ記録が不要になったことに気付きます。デプロイをすばやくクリーンアップしてログ記録を停止できます。この機能を使用すると、をトリアージツールAssisted Log Enablerとして使用できます。



の主な機能は次のとおりです Assisted Log Enabler for AWS。

- 単一アカウントまたはマルチアカウント環境で実行できます。
- これを使用して、環境にログインするためのベースラインを確立できます。
- ドライラン機能を使用して、現在の状態を確認し、ログ記録が有効になっているサービスを確認できます。
- ログ記録を有効にするサービスを選択できます。
- ユースケースに合わせて、スロット Assisted Log Enabler リングアップまたはスロットリングダウンを行うことができます。

成熟: IAM の例

IAM ビジネス成果: 可視性を自動化し、ベストプラクティスに照らして測定することで、リスクを継続的に軽減し、安全な外部接続を可能にし、新しいユーザーと環境を迅速にプロビジョニングします。

ツール: [AWS Identity and Access Management Access Analyzer \(IAM Access Analyzer\)](#) は、外部エンティティと共有されているリソースを識別し、ポリシーの文法とベストプラクティスに照らして IAM ポリシーを検証し、過去のアクセスアクティビティに基づいて IAM ポリシーを生成するのに役立ちます。アカウントレベルと組織レベルの両方で IAM Access Analyzer を有効にすることを強くお勧めします。

サービスのメリット: IAM Access Analyzer は、豊富なインサイト豊富な検出結果を提供します。外部エンティティと共有されている組織のリソースとアカウントを識別できます。パブリック S3 バケット、別のアカウント AWS KMS key と共有されている、または外部アカウントと共有されているロールなどのリソースを検出できるため、組織の管理下でないリソースを識別するための優れた可視性が得られます。IAM ポリシーを検証するだけでなく、自動的に生成することもできます。

実行ステージ: クラウドセキュリティオペレーションの最適化



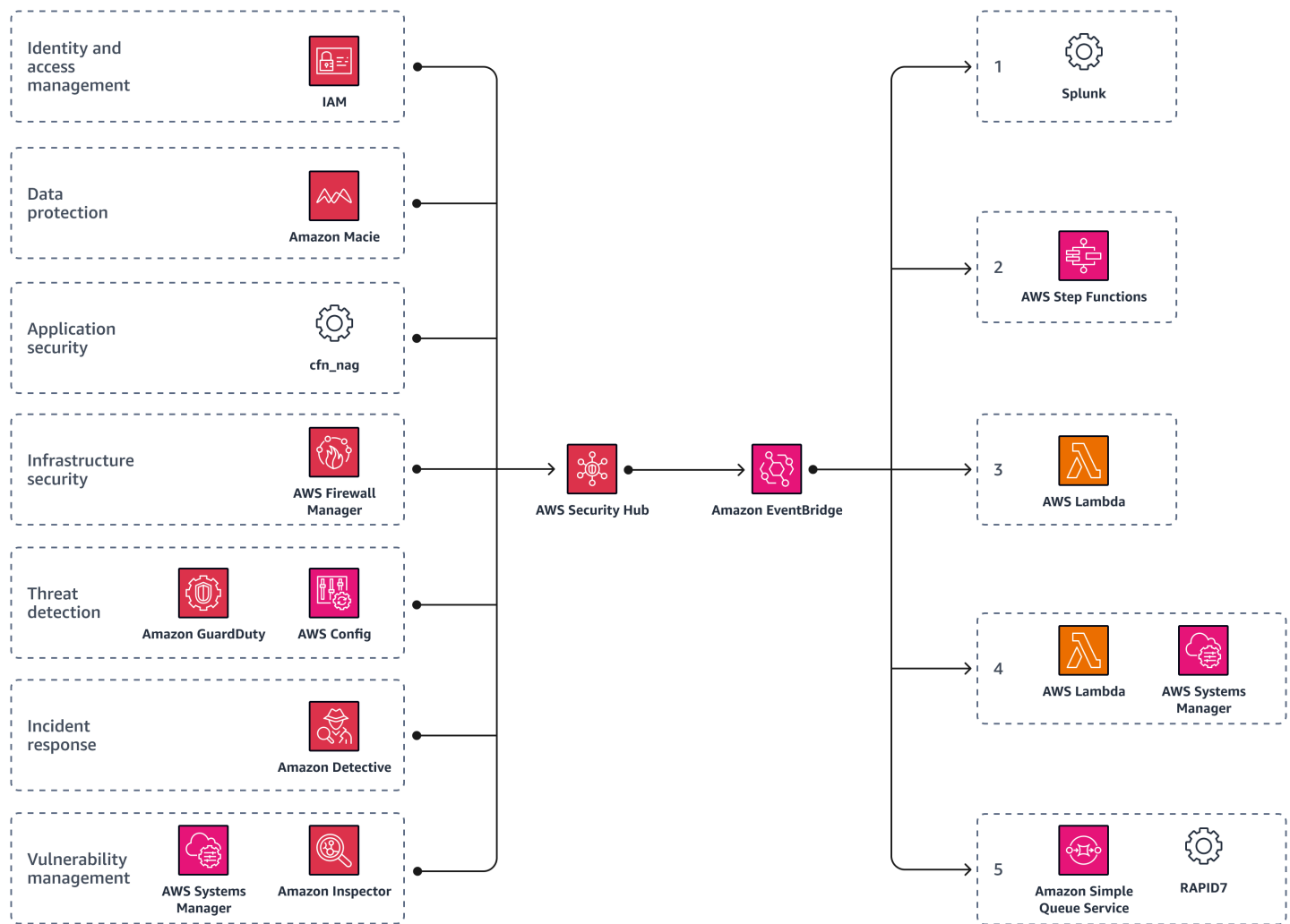
ウォークステージにベースラインを実装すると、組織は実行ステージに進みます。このステージでは、クラウドで利用できるサイバーセキュリティ機能のデモンストレーションに焦点を当てます。その多くは、オンプレミスソリューションで実装できないか、非常に困難です。このステージでは、さまざまなセキュリティコンポーネントを結合し、プロセスを自動化します。自動化によりリソースが解放され、高価値の作業に集中できるようになります。

以下は、実行ステージの唯一のフェーズです。

- [最適化](#) – このプロセスを改善し、自動化を追加する方法を教えてください。

最適化: クラウドセキュリティオペレーションを自動化して反復する

最適化フェーズでは、セキュリティオペレーションを自動化します。クロールステージやウォークステージと同様に、実行ステージ AWS Security Hub で を使用して自動化と反復を実現できます。次の図は、Security Hub が特定の検出結果とインサイトに対して実行する自動アクションを定義するカスタム [Amazon EventBridge](#) ルールをトリガーする方法を示しています。詳細については、Security Hub ドキュメントの「[オートメーション](#)」を参照してください。



Security Hub を中央オートメーションハブとして使用することで、アクティビティを に転送することもできます [Splunk](#)。は、異常であるアクティビティを検出し、対応するアクションを EventBridge でトリガー Splunk できます。これにより、反復的なタスクを自動化し、スキルのあるチームメンバーが価値の高いアクティビティに集中する時間が増えます。 [AWS Step Functions](#) を使用して、ログの収集、フォレンジックスナップショットの作成、侵害されたサーバーの隔離、ゴールデンイメージへの置換を行うこともできます。さらに、 [AWS Lambda](#) を使用して環境全体の脆弱性 [AWS Systems Manager](#) を修正し、 [Amazon Simple Queue Service \(Amazon SQS\)](#) 関数を使用してシステムのセキュリティを検証する 関数を使用できます。このアプローチを採用することで、通常の業務への影響を最小限に抑えながら、セキュリティインシデントを迅速に封じ込めて修正できます。

以下は、前の図に示すように、繰り返し実行される自動アクションの例です。

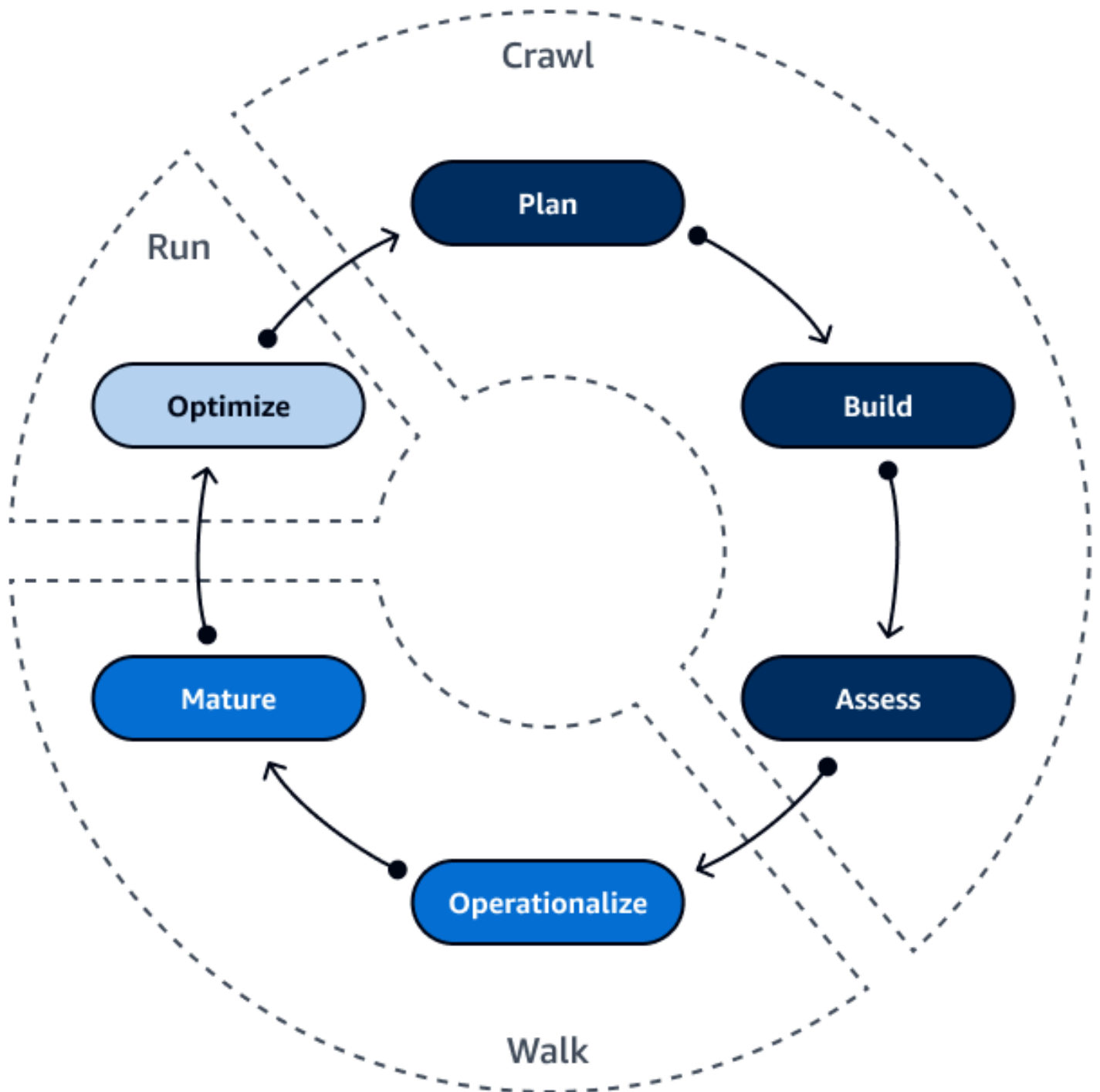
1. を使用して、疑わしいアクティビティを検出 Splunk します。

2. Step Functions を使用して、ログの収集、アクセスの取り消し、隔離、フォレンジックスナップショットの作成を行います。
3. EventBridge ルールを使用して、侵害されたサーバーを隔離し、フォレンジックスナップショットを作成し、ゴールデンイメージに置き換える Lambda 関数を開始します。
4. Systems Manager を使用して、残りの環境全体にパッチを修正して適用する Lambda 関数を開始します。
5. [Rapid7](#) スキャナーを使用して AWS リソースが安全かどうかをスキャンおよび検証する Amazon SQS メッセージを開始します。

詳細については、AWS セキュリティブログの[EC2 インスタンスの でインシデント対応を自動化する方法 AWS クラウド](#)」を参照してください。

結論: クロール、ウォーキング、実行、飛行。

要約すると、クロール、ウォーク、実行モデルは、セキュリティ体制を徐々に改善し、インフラストラクチャを保護するため AWS のベストプラクティスを採用するのに役立つフレームワークです。このプロセスは、新しいテクノロジーやビジネスニーズが発生するにつれて進化し続けます。このフレームワークに従い、 が提供するリソースを使用することで AWS、クラウドセキュリティの強固な基盤を確立し、セキュリティリスクを効果的に管理し、セキュリティの成熟度を高め、イノベーションを推進できます。

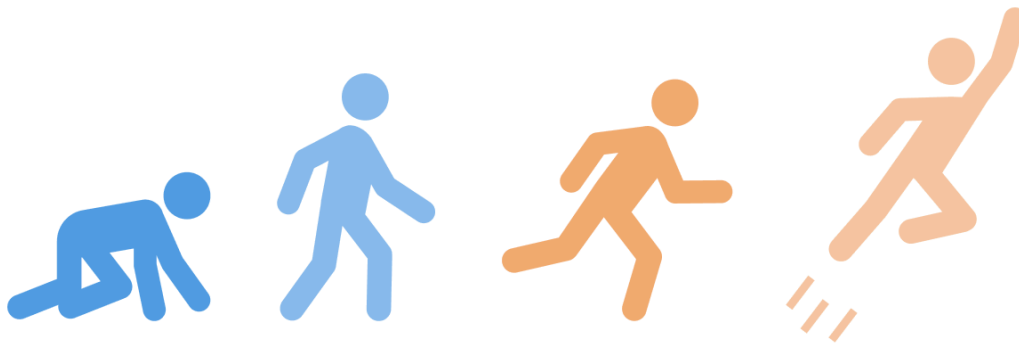


クロールステージでは、基盤を設定します。セキュリティプランを定義し、定義されたセキュリティのベストプラクティスアーキテクチャを使用し、組織のビジネス目標に向けて継続的な評価を推進します。

ウォークステージでは、最初のステップを実行します。ポリシーを確認し、プレイブックを構築し、人材をトレーニングし、戦略を調整できます。この段階は、イノベーションを活用してクラウド内のテクノロジーに対応する方法を理解するのに役立ちます。

実行段階では、大きく考えます。自動化を使用し、スキルのある人材を適切な場所に戦略的に配置します。自動化を実装して、組織のビジネス目標に向けて継続的な評価を推進します。

次は、飛行する時間です。このガイドの推奨事項を使用して、のセキュリティ成熟度を加速します AWS クラウド。



リソース

フレームワークとモデル

- [AWS クラウド導入フレームワーク \(AWS CAF\)](#)
- [AWS Well-Architected フレームワーク](#)
- [AWS セキュリティリファレンスアーキテクチャ \(AWS SRA\)](#)
- [AWS セキュリティ成熟度モデル](#)
- [HIPAA リファレンスアーキテクチャ](#)
- [HITRUST リファレンスアーキテクチャ](#)

AWS のサービス

- [AWS Control Tower](#)
- [AWS Identity and Access Management Access Analyzer](#)
- [AWS Security Hub](#)

その他の AWS リソース

- AWS ソリューションライブラリの [の自動セキュリティレスポンス AWS](#)
- コンピューティングブログの「[AWS Step Functions と Amazon CloudWatch Events を使用して IT 運用を自動化する AWS](#)」
- AWS セキュリティブログの [EC2 インスタンス AWS クラウド の でインシデント対応を自動化する方法](#)
- AWS セキュリティブログの「[マルチアカウント環境で自動インシデント対応を実行する方法](#)」
- [AWS re:Inforce 2022 - クロール、ウォーキング、実行: のセキュリティ成熟度ビデオの高速化 YouTube](#)
- [AWS re:Inforce 2022 - クロール、ウォーク、実行: セキュリティ成熟度の向上に関する PowerPoint プレゼンテーション](#) (添付ファイル)

寄稿者

このガイドには、以下の個人が貢献しました。

オーサリング

- Chad Lorenc、Security Practice Manager、AWS
- Ivy Gin、セキュリティ保証コンサルタント、AWS
- Sayali Paseband、セキュリティコンサルタント、AWS

レビュー

- Deeps Baisya、Senior Security Architect、AWS
- Mike LaRue、Senior Security Consultant、AWS
- Raul Radu、シニアセキュリティエンジニア、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	—	2023 年 12 月 20 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します。
- リプラットフォーム (リフトアンドリシェイプ) — アプリケーションをクラウドに移行し、クラウド機能を活用するための最適化レベルを導入します。例: オンプレミスの Oracle データベースをの Oracle 用 Amazon Relational Database Service (Amazon RDS) に移行します AWS クラウド。
- 再購入 (ドロップアンドショップ) — 通常、従来のライセンスから SaaS モデルに移行して、別の製品に切り替えます。例: カスタマーリレーションシップ管理 (CRM) システムを Salesforce.com に移行します。
- リホスト (リフトアンドシフト) — クラウド機能を活用するための変更を加えずに、アプリケーションをクラウドに移行します。例: オンプレミスの Oracle データベースをの EC2 インスタンス上の Oracle に移行します AWS クラウド。
- 再配置 (ハイパーバイザーレベルのリフトアンドシフト) — 新しいハードウェアを購入したり、アプリケーションを書き換えたり、既存の運用を変更したりすることなく、インフラストラクチャをクラウドに移行できます。オンプレミスプラットフォームから同じプラットフォームのクラウドサービスにサーバーを移行します。例: Microsoft Hyper-Vアプリケーションをに移行します AWS。
- 保持 (再アクセス) — アプリケーションをお客様のソース環境で保持します。これには、主要なリファクタリングを必要とするアプリケーションや、お客様がその作業を後日まで延期したいアプリケーション、およびそれらを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。

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

A

ABAC

[「属性ベースのアクセスコントロール」](#)を参照してください。

抽象化されたサービス

[「マネージドサービス」](#)を参照してください。

ACID

[アトミック性、一貫性、分離性、耐久性](#)を参照してください。

アクティブ - アクティブ移行

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

アクティブ - パッシブ移行

ソースデータベースとターゲットデータベースが同期されるデータベース移行方法。ただし、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、ソースデータベースのみ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します。移行中、ターゲットデータベースはトランザクションを受け付けません。

集計関数

行のグループで動作し、グループの単一の戻り値を計算する SQL 関数。集計関数の例としては、SUMや などがありますMAX。

AI

[「人工知能」](#)を参照してください。

AIOps

[「人工知能オペレーション」](#)を参照してください。

匿名化

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

アンチパターン

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

アプリケーションコントロール

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

アプリケーションポートフォリオ

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

人工知能 (AI)

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

AI オペレーション (AIOps)

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

非対称暗号化

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

原子性、一貫性、分離性、耐久性 (ACID)

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

属性ベースのアクセス制御 (ABAC)

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

信頼できるデータソース

最も信頼性のある情報源とされるデータのプライマリ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

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 AWS するための、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

個人や組織を混乱させたり、損害を与えたりすることを意図した[ボット](#)。

BCP

[「事業継続計画」](#)を参照してください。

動作グラフ

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

ビッグエンディアンシステム

最上位バイトを最初に格納するシステム。[エンディアン性](#)も参照してください。

二項分類

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

ブルームフィルター

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

ブルー/グリーンデプロイ

2 つの異なる同一の環境を作成するデプロイ戦略。現在のアプリケーションバージョンを 1 つの環境 (青) で実行し、新しいアプリケーションバージョンを別の環境 (緑) で実行します。この戦略は、最小限の影響で迅速にロールバックするのに役立ちます。

ボット

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

ボットネット

[マルウェア](#)に感染し、[ボット](#)ハーダーまたはボットオペレーターとして知られる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。ボットは、ボットとその影響をスケールするための最もよく知られているメカニズムです。

ブランチ

コードリポジトリに含まれる領域。リポジトリに最初に作成するブランチは、メインブランチといます。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、Well-Architected [ガイド](#)の「[ブレイクグラス手順の実装](#)」インジケータ AWS を参照してください。

ブラウンフィールド戦略

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

バッファキャッシュ

アクセス頻度が最も高いデータが保存されるメモリ領域。

ビジネス能力

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

ビジネス継続性計画 (BCP)

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

C

CAF

[AWS 「クラウド導入フレームワーク」](#) を参照してください。

Canary デプロイ

エンドユーザーへのバージョンのスローリリースと増分リリース。確信できたら、新しいバージョンをデプロイし、現在のバージョン全体を置き換えます。

CCoE

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

CDC

[「データキャプチャの変更」](#) を参照してください。

変更データキャプチャ (CDC)

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

カオスエンジニアリング

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

CI/CD

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

分類

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

クライアント側の暗号化

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

Cloud Center of Excellence (CCoE)

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

クラウドコンピューティング

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

クラウド運用モデル

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

導入のクラウドステージ

組織が 移行するときに通常実行する 4 つのフェーズ AWS クラウド :

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

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

CMDB

[「設定管理データベース」](#) を参照してください。

コードリポジトリ

ソースコードやその他の資産 (ドキュメント、サンプル、スクリプトなど) が保存され、バージョン管理プロセスを通じて更新される場所。一般的なクラウドリポジトリには、GitHub または が含まれます Bitbucket Cloud。コードの各バージョンはブランチと呼ばれます。マイクロサービス

の構造では、各リポジトリは 1 つの機能専用です。1 つの CI/CD パイプラインで複数のリポジトリを使用できます。

コールドキャッシュ

空である、または、かなり空きがある、もしくは、古いデータや無関係なデータが含まれているバッファキャッシュ。データベースインスタンスはメインメモリまたはディスクから読み取る必要があります、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などのビジュアル形式から情報を分析および抽出する [AI](#) の分野。例えば、Amazon SageMaker AI は CV 用の画像処理アルゴリズムを提供します。

設定ドリフト

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

構成管理データベース (CMDB)

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

コンフォーマンスパック

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

継続的インテグレーションと継続的デリバリー (CI/CD)

ソフトウェアリリースプロセスのソース、ビルド、テスト、ステージング、本番の各ステージを自動化するプロセス。CI/CD は一般的にパイプラインと呼ばれます。プロセスの自動化、生産性

の向上、コード品質の向上、配信の加速化を可能にします。詳細については、「[継続的デリバリーの利点](#)」を参照してください。CD は継続的デプロイ (Continuous Deployment) の略語でもあります。詳細については「[継続的デリバリーと継続的なデプロイ](#)」を参照してください。

CV

[「コンピュータビジョン」](#)を参照してください。

D

保管中のデータ

ストレージ内にあるデータなど、常に自社のネットワーク内にあるデータ。

データ分類

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

データドリフト

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

転送中のデータ

ネットワーク内 (ネットワークリソース間など) を活発に移動するデータ。

データメッシュ

一元管理とガバナンスを備えた分散型の分散型データ所有権を提供するアーキテクチャフレームワーク。

データ最小化

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

データ境界

AWS 環境内の一連の予防ガードレール。信頼された ID のみが、予想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。

データの事前処理

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。データの事前処理とは、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。

データの出所

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。

データの種類

データを収集、処理している個人。

データウェアハウス

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

データベース定義言語 (DDL)

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

データベース操作言語 (DML)

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

DDL

[「データベース定義言語」](#) を参照してください。

ディープアンサンブル

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

ディープラーニング

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

多層防御

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

委任管理者

では AWS Organizations、互換性のあるサービスが AWS メンバーアカウントを登録して組織のアカウントを管理し、そのサービスのアクセス許可を管理できます。このアカウントを、そのサービスの委任管理者と呼びます。詳細、および互換性のあるサービスの一覧は、AWS Organizations ドキュメントの[AWS Organizationsで利用できるサービス](#)を参照してください。

デプロイ

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

開発環境

[「環境」](#)を参照してください。

検出管理

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

開発バリューストリームマッピング (DVSM)

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

デジタルツイン

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

ディメンションテーブル

[スタースキーマ](#)では、ファクトテーブル内の量的データに関するデータ属性を含む小さなテーブル。ディメンションテーブル属性は通常、テキストフィールドまたはテキストのように動作する離散数値です。これらの属性は、クエリの制約、フィルタリング、結果セットのラベル付けに一般的に使用されます。

ディザスタ

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

ディザスタリカバリ (DR)

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

DML

[「データベース操作言語」](#)を参照してください。

ドメイン駆動型設計

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

DR

[「ディザスタリカバリ」](#)を参照してください。

ドリフト検出

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

DVSM

[「開発値ストリームマッピング」](#)を参照してください。

E

EDA

[「探索的データ分析」](#)を参照してください。

EDI

[「電子データ交換」](#)を参照してください。

エッジコンピューティング

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

電子データ交換 (EDI)

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

暗号化

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

暗号化キー

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

エンディアン

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

エンドポイント

[「サービスエンドポイント」](#)を参照してください。

エンドポイントサービス

仮想プライベートクラウド (VPC) 内でホストして、他のユーザーと共有できるサービス。を使用してエンドポイントサービスを作成し AWS PrivateLink、他の AWS アカウント または AWS Identity and Access Management (IAM) プリンシパルにアクセス許可を付与できます。これら

のアカウントまたはプリンシパルは、インターフェイス VPC エンドポイントを作成することで、エンドポイントサービスにプライベートに接続できます。詳細については、Amazon Virtual Private Cloud (Amazon VPC) ドキュメントの「[エンドポイントサービスを作成する](#)」を参照してください。

エンタープライズリソースプランニング (ERP)

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

エンベロープ暗号化

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

環境

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

- 開発環境 — アプリケーションのメンテナンスを担当するコアチームのみが利用できる、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力カテゴリー。エピックでは、要件と実装タスクの概要についてハイレベルな説明を提供します。例えば、AWS CAF セキュリティエピックには、ID とアクセスの管理、検出コントロール、インフラストラクチャセキュリティ、データ保護、インシデント対応が含まれます。AWS 移行戦略のエピックの詳細については、[プログラム実装ガイド](#) を参照してください。

ERP

「[エンタープライズリソース計画](#)」を参照してください。

探索的データ分析 (EDA)

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

F

ファクトテーブル

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

フェイルファスト

開発ライフサイクルを短縮するために頻繁で段階的なテストを使用する哲学。これはアジャイルアプローチの重要な部分です。

障害分離の境界

では AWS クラウド、アベイラビリティーゾーン AWS リージョン、コントロールプレーン、データプレーンなどの境界で、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

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

FGAC

[「きめ細かなアクセスコントロール」](#) を参照してください。

きめ細かなアクセス制御 (FGAC)

複数の条件を使用してアクセス要求を許可または拒否すること。

フラッシュカット移行

段階的なアプローチを使用する代わりに、[変更データキャプチャ](#) による継続的なデータレプリケーションを使用して、可能な限り短時間でデータを移行するデータベース移行方法。目的はダウンタイムを最小限に抑えることです。

FM

[「基盤モデル」](#) を参照してください。

基盤モデル (FM)

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

G

生成 AI

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

ジオブロッキング

[地理的制限](#)を参照してください。

地理的制限 (ジオブロッキング)

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

Gitflow ワークフロー

下位環境と上位環境が、ソースコードリポジトリでそれぞれ異なるブランチを使用する方法。Gitflow ワークフローはレガシーと見なされ、[トランクベースのワークフロー](#)はモダンで推奨されるアプローチです。

ゴールデンイメージ

そのシステムまたはソフトウェアの新しいインスタンスをデプロイするためのテンプレートとして使用されるシステムまたはソフトウェアのスナップショット。例えば、製造では、ゴールデンイメージを使用して複数のデバイスにソフトウェアをプロビジョニングし、デバイス製造オペレーションの速度、スケーラビリティ、生産性を向上させることができます。

グリーンフィールド戦略

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

ガードレール

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

H

HA

[「高可用性」](#)を参照してください。

異種混在データベースの移行

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

ハイアベイラビリティ (HA)

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

ヒストリアンのモダナイゼーション

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

ホールドアウトデータ

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

同種データベースの移行

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

ホットデータ

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

ホットフィックス

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

ハイパーケア期間

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

I

IaC

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

ID ベースのポリシー

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

アイドル状態のアプリケーション

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

IIoT

[「産業用モノのインターネット」](#) を参照してください。

イミュータブルインフラストラクチャ

既存のインフラストラクチャを更新、パッチ適用、または変更する代わりに、本番環境のワークロード用に新しいインフラストラクチャをデプロイするモデル。イミュータブルインフラストラクチャは、本質的に [ミュータブルインフラストラクチャ](#) よりも一貫性、信頼性、予測性が高くなります。詳細については、AWS 「Well-Architected Framework」の「[Deploy using immutable infrastructure](#) best practice」を参照してください。

インバウンド (受信) VPC

AWS マルチアカウントアーキテクチャでは、アプリケーションの外部からネットワーク接続を受け入れ、検査し、ルーティングする VPC。 [AWS Security Reference Architecture](#) では、アプリ

ケーションとより広範なインターネット間の双方向のインターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションの各 VPC を使用してネットワークアカウントを設定することを推奨しています。

増分移行

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

インダストリー 4.0

2016 年に [Klaus Schwab](#) によって導入された用語で、接続、リアルタイムデータ、オートメーション、分析、AI/ML の進歩によるビジネスプロセスのモダナイゼーションを指します。

インフラストラクチャ

アプリケーションの環境に含まれるすべてのリソースとアセット。

Infrastructure as Code (IaC)

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

産業分野における IoT (IIoT)

製造、エネルギー、自動車、ヘルスケア、ライフサイエンス、農業などの産業部門におけるインターネットに接続されたセンサーやデバイスの使用。詳細については、「[Building an industrial Internet of Things \(IIoT\) digital transformation strategy](#)」を参照してください。

インスペクション VPC

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

IoT

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

解釈可能性

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

IoT

「[モノのインターネット](#)」を参照してください。

IT 情報ライブラリ (ITIL)

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

IT サービス管理 (ITSM)

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

ITIL

「[IT 情報ライブラリ](#)」を参照してください。

ITSM

「[IT サービス管理](#)」を参照してください。

L

ラベルベースアクセス制御 (LBAC)

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

ランディングゾーン

ランディングゾーンは、スケーラブルで安全な、適切に設計されたマルチアカウント AWS 環境です。これは、組織がセキュリティおよびインフラストラクチャ環境に自信を持ってワークロー

ドとアプリケーションを迅速に起動してデプロイできる出発点です。ランディングゾーンの詳細については、[安全でスケーラブルなマルチアカウント AWS 環境のセットアップ](#) を参照してください。

大規模言語モデル (LLM)

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

大規模な移行

300 台以上のサーバの移行。

LBAC

[「ラベルベースのアクセスコントロール」](#) を参照してください。

最小特権

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

リフトアンドシフト

[「7 Rs」](#) を参照してください。

リトルエンディアンシステム

最下位バイトを最初に格納するシステム。 [エンディアンネス](#) も参照してください。

LLM

[「大規模言語モデル」](#) を参照してください。

下位環境

[「環境」](#) を参照してください。

M

機械学習 (ML)

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

メインランチ

[「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、不正アクセスにつながる可能性があります。マルウェアの例としては、ウイルス、ワーム、ランサムウェア、トロイの木馬、スパイウェア、キーロガーなどがあります。

マネージドサービス

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

製造実行システム (MES)

生産プロセスを追跡、モニタリング、文書化、制御するためのソフトウェアシステムで、原材料を工場の完成製品に変換します。

MAP

[「移行促進プログラム」](#)を参照してください。

メカニズム

ツールを作成し、ツールの導入を推進し、調整を行うために結果を検査する完全なプロセス。メカニズムは、動作中にそれ自体を強化および改善するサイクルです。詳細については、AWS「Well-Architected フレームワーク」の[「メカニズムの構築」](#)を参照してください。

メンバーアカウント

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

MES

[「製造実行システム」](#)を参照してください。

メッセージキューイングテレメトリトランスポート (MQTT)

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

マイクロサービス

明確に定義された API を介して通信し、通常は小規模な自己完結型のチームが所有する、小規模で独立したサービスです。例えば、保険システムには、販売やマーケティングなどのビジネス機能、または購買、請求、分析などのサブドメインにマッピングするマイクロサービスが含まれる場合があります。マイクロサービスの利点には、俊敏性、柔軟なスケーリング、容易なデプロイ、再利用可能なコード、回復力などがあります。詳細については、[AWS「サーバーレスサービスを使用したマイクロサービスの統合」](#)を参照してください。

マイクロサービスアーキテクチャ

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

Migration Acceleration Program (MAP)

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

大規模な移行

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

移行ファクトリー

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

移行メタデータ

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

移行パターン

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

Migration Portfolio Assessment (MPA)

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

移行準備状況評価 (MRA)

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

移行戦略

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

ML

[??? 「機械学習」](#) を参照してください。

モダナイゼーション

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

モダナイゼーション準備状況評価

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

モノリシックアプリケーション (モノリス)

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

MPA

[「移行ポートフォリオ評価」](#)を参照してください。

MQTT

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

多クラス分類

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

ミュータブルインフラストラクチャ

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

O

OAC

[「オリジンアクセスコントロール」](#)を参照してください。

OAI

[「オリジンアクセスアイデンティティ」](#)を参照してください。

OCM

[「組織変更管理」](#)を参照してください。

オフライン移行

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

OI

[「オペレーションの統合」](#)を参照してください。

OLA

[「運用レベルの契約」](#)を参照してください。

オンライン移行

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

OPC-UA

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

オープンプロセス通信 - 統合アーキテクチャ (OPC-UA)

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

オペレーショナルレベルアグリーメント (OLA)

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

運用準備状況レビュー (ORR)

インシデントや潜在的な障害の理解、評価、防止、または範囲の縮小に役立つ質問とそれに関連するベストプラクティスのチェックリスト。詳細については、AWS Well-Architected フレームワークの [「Operational Readiness Reviews \(ORR\)」](#)を参照してください。

運用テクノロジー (OT)

産業オペレーション、機器、インフラストラクチャを制御するために物理環境と連携するハードウェアおよびソフトウェアシステム。製造では、OT と情報技術 (IT) システムの統合が、[Industry 4.0](#) 変換の主な焦点です。

オペレーション統合 (OI)

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

組織の証跡

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

組織変更管理 (OCM)

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

オリジンアクセスコントロール (OAC)

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

オリジンアクセスアイデンティティ (OAI)

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

ORR

[「運用準備状況レビュー」](#) を参照してください。

OT

[「運用テクノロジー」](#)を参照してください。

アウトバウンド (送信) VPC

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

P

アクセス許可の境界

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

個人を特定できる情報 (PII)

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

PII

[個人を特定できる情報](#)を参照してください。

プレイブック

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

PLC

[「プログラム可能なロジックコントローラー」](#)を参照してください。

PLM

[「製品ライフサイクル管理」](#)を参照してください。

ポリシー

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

多言語の永続性

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

ポートフォリオ評価

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

述語

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

述語プッシュダウン

転送前にクエリ内のデータをフィルタリングするデータベースクエリ最適化手法。これにより、リレーショナルデータベースから取得して処理する必要があるデータの量が減少し、クエリのパフォーマンスが向上します。

予防的コントロール

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

プリンシパル

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

プライバシーバイデザイン

開発プロセス全体を通じてプライバシーを考慮するシステムエンジニアリングアプローチ。

プライベートホストゾーン

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

プロアクティブコントロール

非標準のリソースのデプロイを防ぐように設計された[セキュリティコントロール](#)。これらのコントロールは、プロビジョニング前にリソースをスキャンします。リソースがコントロールに準拠していない場合、プロビジョニングされません。詳細については、AWS Control Tower ドキュメントの「[コントロールリファレンスガイド](#)」および「[セキュリティコントロールの実装](#)」の「[プロアクティブコントロール](#)」を参照してください。 AWS

製品ライフサイクル管理 (PLM)

設計、開発、発売から成長と成熟まで、ライフサイクル全体を通じて製品のデータとプロセスを管理し、辞退と削除を行います。

本番環境

[「環境」](#)を参照してください。

プログラム可能なロジックコントローラー (PLC)

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

プロンプトの連鎖

1 つの [LLM](#) プロンプトの出力を次のプロンプトの入力として使用して、より良いレスポンスを生成します。この手法は、複雑なタスクをサブタスクに分割したり、予備応答を反復的に絞り込んだり拡張したりするために使用されます。これにより、モデルのレスポンスの精度と関連性が向上し、より詳細でパーソナライズされた結果が得られます。

仮名化

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

パブリッシュ/サブスクライブ (pub/sub)

マイクロサービス間の非同期通信を可能にするパターン。スケーラビリティと応答性を向上させます。たとえば、マイクロサービスベースの [MES](#) では、マイクロサービスは他のマイクロサー

ビスがサブスクライブできるチャンネルにイベントメッセージを発行できます。システムは、公開サービスを変更せずに新しいマイクロサービスを追加できます。

Q

クエリプラン

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

クエリプランのリグレッション

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

R

RACI マトリックス

[責任、説明責任、相談、通知 \(RACI\)](#) を参照してください。

RAG

[「取得拡張生成」](#) を参照してください。

ランサムウェア

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

RASCI マトリックス

[責任、説明責任、相談、通知 \(RACI\)](#) を参照してください。

RCAC

[「行と列のアクセスコントロール」](#) を参照してください。

リードレプリカ

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

再設計

[「7 Rs」](#)を参照してください。

目標復旧時点 (RPO)

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

目標復旧時間 (RTO)

サービスの中断から復旧までの最大許容遅延時間。

リファクタリング

[「7 Rs」](#)を参照してください。

リージョン

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

回帰

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

リホスト

[「7 Rs」](#)を参照してください。

リリース

デプロイプロセスで、変更を本番環境に昇格させること。

再配置

[「7 Rs」](#)を参照してください。

プラットフォーム変更

[「7 Rs」](#)を参照してください。

再購入

[「7 Rs」](#)を参照してください。

回復性

中断に抵抗または回復するアプリケーションの機能。[高可用性](#)と[ディザスタリカバリ](#)は、で回復性を計画する際の一般的な考慮事項です AWS クラウド。詳細については、[AWS クラウド「レジリエンス」](#)を参照してください。

リソースベースのポリシー

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

実行責任者、説明責任者、協業先、報告先 (RACI) に基づくマトリックス

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

レスポンスコントロール

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、Implementing security controls on AWSの[Responsive controls](#)を参照してください。

保持

[「7 Rs」](#)を参照してください。

廃止

[「7 Rs」](#)を参照してください。

取得拡張生成 (RAG)

[LLM](#) がレスポンスを生成する前にトレーニングデータソースの外部にある信頼できるデータソースを参照する[生成 AI](#) テクノロジー。例えば、RAG モデルは組織のナレッジベースまたはカスタムデータのセマンティック検索を実行する場合があります。詳細については、[「RAG とは」](#)を参照してください。

ローテーション

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

行と列のアクセス制御 (RCAC)

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

RPO

[「目標復旧時点」](#)を参照してください。

RTO

[目標復旧時間](#)を参照してください。

ランブック

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

S

SAML 2.0

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

SCADA

[「監視コントロールとデータ取得」](#)を参照してください。

SCP

[「サービスコントロールポリシー」](#)を参照してください。

シークレット

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

設計によるセキュリティ

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

セキュリティコントロール

脅威アクターによるセキュリティ脆弱性の悪用を防止、検出、軽減するための、技術上または管理上のガードレール。セキュリティコントロールには、[予防的](#)、[検出的](#)、[応答的](#)、[プロ](#)アクティブの 4 つの主なタイプがあります。

セキュリティ強化

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

Security Information and Event Management (SIEM) システム

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

セキュリティレスポンスの自動化

セキュリティイベントに自動的に応答または修復するように設計された、事前定義されたプログラムされたアクション。これらの自動化は、セキュリティのベストプラクティスを実装するのに役立つ[検出的](#)または[応答的](#)な AWS セキュリティコントロールとして機能します。自動レスポンスアクションの例としては、VPC セキュリティグループの変更、Amazon EC2 インスタンスへのパッチ適用、認証情報の更新などがあります。

サーバー側の暗号化

送信先で、それ AWS のサービス を受け取る によるデータの暗号化。

サービスコントロールポリシー (SCP)

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

サービスエンドポイント

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

サービスレベルアグリーメント (SLA)

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

サービスレベルインジケータ (SLI)

エラー率、可用性、スループットなど、サービスのパフォーマンス側面の測定。

サービスレベルの目標 (SLO)

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

責任共有モデル

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

SIEM

[セキュリティ情報とイベント管理システム](#) を参照してください。

単一障害点 (SPOF)

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

SLA

[「サービスレベルアグリーメント」](#) を参照してください。

SLI

[「サービスレベルインジケータ」](#) を参照してください。

SLO

[「サービスレベルの目標」](#) を参照してください。

スプリットアンドシードモデル

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

SPOF

[単一障害点](#)を参照してください。

スタースキーマ

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

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。

監視コントロールとデータ取得 (SCADA)

製造では、ハードウェアとソフトウェアを使用して物理アセットと本番稼働をモニタリングするシステム。

対称暗号化

データの暗号化と復号に同じキーを使用する暗号化のアルゴリズム。

合成テスト

ユーザーとのやり取りをシミュレートして潜在的な問題を検出したり、パフォーマンスをモニタリングしたりする方法でシステムをテストします。[Amazon CloudWatch Synthetics](#) を使用してこれらのテストを作成できます。

システムプロンプト

[LLM](#) にコンテキスト、指示、またはガイドラインを提供して動作を指示する手法。システムプロンプトは、コンテキストを設定し、ユーザーとのやり取りのルールを確立するのに役立ちます。

T

tags

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

ターゲット変数

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

タスクリスト

ランブックの進行状況を追跡するために使用されるツール。タスクリストには、ランブックの概要と完了する必要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。

トランジットゲートウェイ

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

トランクベースのワークフロー

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

信頼されたアクセス

ユーザーに代わって AWS Organizations およびそのアカウントで組織内でタスクを実行するために指定したサービスにアクセス許可を付与します。信頼されたサービスは、サービスにリンクされたロールを必要なときに各アカウントに作成し、ユーザーに代わって管理タスクを実行します。詳細については、ドキュメントの「[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 枚のピザで養うことができるくらい小さな DevOps チーム。ツーピザチームの規模では、ソフトウェア開発におけるコラボレーションに最適な機会が確保されます。

U

不確実性

予測機械学習モデルの信頼性を損なう可能性がある、不正確、不完全、または未知の情報を指す概念。不確実性には、次の 2 つのタイプがあります。認識論的不確実性は、限られた、不完全なデータによって引き起こされ、弁論的不確実性は、データに固有のノイズとランダム性によって引き起こされます。詳細については、[深層学習システムにおける不確実性の定量化](#) ガイドを参照してください。

未分化なタスク

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

上位環境

[「環境」](#) を参照してください。

V

バキューミング

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

バージョンコントロール

リポジトリ内のソースコードへの変更など、変更を追跡するプロセスとツール。

VPC ピアリング

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

脆弱性

システムのセキュリティを脅かすソフトウェアまたはハードウェアの欠陥。

W

ウォームキャッシュ

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

ウォームデータ

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

ウィンドウ関数

現在のレコードに何らかの形で関連する行のグループに対して計算を実行する SQL 関数。ウィンドウ関数は、移動平均の計算や、現在の行の相対位置に基づく行の値へのアクセスなどのタスクの処理に役立ちます。

ワークロード

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

ワークストリーム

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

WORM

[「書き込み 1 回」、「読み取り多数」](#)を参照してください。

WQF

[AWS「ワークロード認定フレームワーク」](#)を参照してください。

Write Once, Read Many (WORM)

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

Z

ゼロデイエクスプロイト

[ゼロデイ脆弱性](#)を利用する攻撃、通常はマルウェア。

ゼロデイ脆弱性

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

ゼロショットプロンプト

[LLM](#) にタスクを実行する手順を提供しますが、タスクのガイドに役立つ例 (ショット) はありません。LLM は、事前トレーニング済みの知識を使用してタスクを処理する必要があります。ゼロショットプロンプトの有効性は、タスクの複雑さとプロンプトの品質によって異なります。[「数ショットプロンプト」](#)も参照してください。

ゾンビアプリケーション

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

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