AWS スタートアップセキュリティベースライン (AWS SSB)

AWS 規範ガイダンス

AWS 規範ガイダンス: AWS スタートアップセキュリティベースライン (AWS SSB)

Table of Contents

AWS Startup Security Baseline (AWS SSB)

Jay Michael (Amazon Web Services (AWS))

2023 年 5 月 (ドキュメント履歴)

AWS Startup Security Baseline (SSB) は、企業が俊敏性を低下させることなく AWS にセキュリティを構築するための、最小限の基盤を作成する一連のコントロールです。これらのコントロールは、セキュリティ体制の基礎を形成し、認証情報のセキュリティ保護、ログ記録と可視性の有効化、連絡先情報の管理、基本的なデータ境界の実装に重点を置いています。

このガイドのコントロールは、初期のスタートアップを念頭に置いて設計されており、多大な労力を要することなく、最も一般的なセキュリティリスクを軽減します。多くのスタートアップは、単一の AWS アカウント で AWS クラウド のジャーニーを始めます。組織が成長するにつれて、スタートアップはマルチアカウントアーキテクチャに移行します。このガイドのガイダンスは単一アカウントアーキテクチャ向けに設計されていますが、マルチアカウントアーキテクチャへの移行時に、簡単に移行または変更できるセキュリティコントロールの設定にも役立ちます。

AWS SSB の管理は、アカウントとワークロードの 2 つのカテゴリに分類されます。アカウント管理は、AWS アカウントの安全を維持するのに役立ちます ユーザーアクセス、ポリシー、アクセス許可の設定に関する推奨事項のほか、アカウント内の不正または潜在的に悪意のあるアクティビティを監視する方法に関する推奨事項も含まれています。ワークロード管理は、アプリケーション、バックエンドプロセス、データなど、クラウド内のリソースとコードを保護するのに役立ちます。暗号化やアクセス範囲の縮小などに関する推奨事項も含まれています。

> **Note**
>
> このガイドで推奨されている管理の中には、初期設定時に設定したデフォルトを変更するものもありますが、新しい設定やポリシーを設定するものがほとんどです。このドキュメントは、利用可能なすべての管理を網羅してはいません。

対象者

このガイドは、開発の初期段階にあり、スタッフとオペレーションが最小限であるスタートアップに最適です。

オペレーションおよび成長の後期段階にあるスタートアップやその他の企業は、これらの管理を現在のプラクティスと照らし合わせて見直すことで、大きな価値を引き出すことができます。ギャップが

見つかった場合は、このガイドに記載されている個々の管理を実装し、長期的なソリューションとして適切かどうかを評価できます。

> **Note**
>
> このガイドで推奨されている管理は、本質的に基本的なものです。スケールアップや高度化を進める後期段階のスタートアップやその他の企業は、必要に応じて管理を追加する必要があります。

基本的なフレームワークとセキュリティ上の責任

AWS Well-Architected は、クラウドアーキテクトがアプリケーションやワークロード向けに、安全で高性能、かつ、回復力のある効率的なインフラストラクチャを構築するのに役立ちます。AWS Startup Security Baseline は、AWS Well-Architected フレームワークのセキュリティの柱と一致しています。セキュリティの柱では、クラウドテクノロジーを活用して、ユーザーのセキュリティ体制を向上させる方法でデータ、システム、アセットを保護する方法について説明します。現在の AWS 推奨事項に従うことで、お客様のビジネス要件や規制要件を満たすことができます。

Well-Architected のベストプラクティスへの準拠を評価するには、AWS アカウントで AWS Well-Architected Tool を使用します。

AWS とお客様の間で、セキュリティとコンプライアンスの責任を共有します。この責任共有モデルは多くの場合、次のように説明されます: AWS はクラウドのセキュリティ (AWS クラウド で提供されるすべてのサービスを実行するインフラストラクチャの保護) に責任があり、ユーザーは (選択した AWS クラウド サービスによって決定される) クラウドのセキュリティに責任があります。　責任共有モデルでは、このドキュメントに記載されているセキュリティコントロールの実装は、お客様の責任の一部となります。

アカウントの保護

このセクションのコントロールと推奨事項は、 AWS アカウントを安全に保つのに役立ちます。人間とマシンの両方のアクセスに AWS Identity and Access Management (IAM) ユーザー、ユーザーグループ、ロール (プリンシパル とも呼ばれます) を使用し、ルートユーザーの使用を制限し、多要素認証が必要であることを強調しています。このセクションでは、 にアカウントのアクティビティとステータスについて連絡するために必要な連絡先情報 AWS があることを確認します。また、、Amazon AWS Trusted Advisor、 などのモニタリングサービスを設定して AWS Budgets、アカウント内のアクティビティの通知を受け取り GuardDuty、アクティビティが不正または予期しないものである場合に迅速に対応できるようにします。

このセクションは、以下のトピックで構成されます。

ACCT.01 – アカウントレベルの連絡先を有効な E メール配布リストに設定する

AWS アカウントの主要連絡先と代替連絡先を設定するときは、個人の E メールアドレスの代わりに E メール配布リストを使用します。E メール配布リストを使用すると、個人が組織内を移動しても、所有権と到達可能性を維持することができます。請求、オペレーション、セキュリティ通知用の代替連絡先を設定し、それに応じて適切な E メール配布リストを使用します。 AWS はこれらの E メールアドレスを使用して連絡するため、それらへのアクセスを保持することが重要です。

アカウント名、 ルートユーザーパスワード、または ルートユーザー E メールアドレスを編集するには

1. 次のページで、Billing and Cost Management コンソールの [アカウント設定] ページにサインインします: https://console.aws.amazon.com/billing/home?#/account。
2. [アカウント設定] で、[アカウント設定] の横の [編集] を選択します。
3. 更新するフィールドの横にある [編集] を選択します。
4. 変更を入力したら、[変更の保存] を選択します。
5. 変更を行ったら、[完了] を選択します。

連絡先情報を編集するには

1. [アカウント設定] ページの [連絡先情報] で、[編集] を選択します。
2. 変更したいフィールドに最新の情報を入力し、[更新] を選択します。

代替の連絡先を追加、更新、または削除するには

1. [アカウント設定] ページの [代替の連絡先] で、[編集] を選択します。
2. 変更したいフィールドに最新の情報を入力し、[更新] を選択します。

ACCT.02 — ルートユーザーの使用を制限する

ルートユーザーは AWS 、アカウントにサインアップしたときに作成され、このユーザーは、アカウントに対する完全な所有権とアクセス許可を持ち、変更することはできません。ルートユーザーは、これを必要とする特定のタスクのみに使用します。詳細については、「Tasks that require root user credentials」(AWS Account Management) を参照してください。アカウント内の他のすべてのアクションは、他の種類の IAM ID (IAM ロールを持つフェデレーションユーザーなど) を使用して実行します。詳細については、「AWS セキュリティ認証情報」(IAM ドキュメント) を参照してください。

ルートユーザーの使用を制限するには

1. ACCT.05 — ログインのための多要素認証 (MFA) を要求する で説明されているとおり、ルートユーザー用の多要素認証 (MFA) を要求します。
2. 日常的なタスクでルートユーザーを使用しないよう、管理ユーザーを作成します。ユーザーアクセスの設定に関する詳細は、「ACCT.03 — 各ユーザーのコンソールアクセスを設定する」を参照してください。

ACCT.03 — 各ユーザーのコンソールアクセスを設定する

ベストプラクティスとして、 は一時的な認証情報を使用して AWS アカウント および リソースへのアクセスを許可することを AWS 推奨しています。一時的な認証情報には有効期限が設けられているため、不要になった場合にローテーションしたり、明示的に取り消したりする必要がありません。詳細については、「一時的な認証情報」(IAM ドキュメント) を参照してください。

人間のユーザーの場合、、Okta、Active Directory AWS IAM Identity Center、Ping Identity など、一元化された ID プロバイダー (IdP) のフェデレーティッド ID を使用する AWS ことをお勧めします。ユーザーをフェデレーションすることで、ID を一元的に定義でき、ユーザーは 1 セットの認証情報のみ AWSを使用して、 を含む複数のアプリケーションやウェブサイトに対して安全に認証できます。詳細については、「 での ID フェデレーション AWS」および「IAM Identity Center (AWS ウェブサイト) 」を参照してください。

> **Note**
>
> ID フェデレーションを使用すると、シングルアカウントアーキテクチャからマルチアカウントアーキテクチャへの移行が、複雑になることがあります。スタートアップでは、 AWS Organizationsで管理されるマルチアカウントアーキテクチャが完成するまで、ID フェデレーションの実装を遅らせるのが一般的です。

ID フェデレーションをセットアップするには

1. IAM アイデンティティセンターを使用している場合は、「Getting started」(IAM アイデンティティセンタードキュメント) を参照してください。

   外部またはサードパーティの IdP を使用している場合は、「Creating IAM identity providers」(IAM ドキュメント) を参照してください。
2. IdP が多要素認証 (MFA) を適用していることを確認します。
3. ACCT.04 — アクセス許可を割り当てる に従ってアクセス許可を適用します。

ID フェデレーションを設定する準備が整っていないスタートアップの場合は、IAM でユーザーを直接作成することができます。これは有効期限のない長期的な認証情報であるため、セキュリティベストプラクティスとしては推奨されていません。ただし、オペレーションの初期段階にあるスタートアップには一般的な方法です。オペレーションの準備が整ってからマルチアカウントアーキテクチャへ移行するときの、複雑さを防ぐことができるためです。

基準線として、 AWS Management Consoleにアクセスする必要のある各ユーザーに、IAM ユーザーを作成できます。IAM ユーザーを設定するときは、ユーザー間で認証情報を共有するのではなく、長期認証情報を定期的にローテーションします。

> ⚠ Warning
>
> IAM ユーザーには長期的な認証情報があり、セキュリティ上のリスクをもたらします。このリスクを軽減するために、これらのユーザーにはタスクの実行に必要な権限のみを付与し、不要になったユーザーを削除することをお勧めします。

IAM ユーザーを作成するには

1. IAM ユーザーを作成します (IAM ドキュメント)。
2. ACCT.04 — アクセス許可を割り当てる に従ってアクセス許可を適用します。

ACCT.04 — アクセス許可を割り当てる

ポリシーを IAM ID (ユーザーグループまたはロール) に割り当てて、アカウントのユーザーアクセス許可を設定します。アクセス許可をカスタマイズすることも、 AWS マネージドポリシー をアタッチすることもできます。これは、多くの一般的ユースケース AWS にアクセス許可を提供するためによって設計されたスタンドアロンポリシーです。アクセス許可をカスタマイズするときは、最小特権アクセス許可の付与に関するベストプラクティスに従います。最小特権とは、各ユーザーにそれぞれのタスクを実行するための必要最小限のアクセス許可を付与する方法です。

フェデレーティッド ID を使用している場合、ユーザーは、外部の ID プロバイダーを介して IAM ロールを引き受け、アカウントにアクセスします。IAM ロールは、組織の IdP によって認証されたユーザーが で実行できる操作を定義します AWS。このロールにカスタムポリシーまたは AWS 管理ポリシーを適用して、アクセス許可を設定します。

フェデレーティッド ID にアクセス許可を割り当てるには

- IAM アイデンティティセンターを使用している場合は、「Use IAM policies in permission sets」(IAM アイデンティティセンタードキュメント)。

  外部またはサードパーティの IdP を使用している場合は、「IAM ID アクセス許可の追加」(IAM ドキュメント) を参照してください。

IAM ユーザーを使用している場合は、ユーザーグループまたはロールを使用することで、複数の IAM ユーザーのアクセス許可を管理できます。ユーザーグループは、管理が容易で、アカウントにセキュリティリスクをもたらす設定ミスが発生しにくいため、スタートアップに推奨されています。ユーザーを、それぞれの職務機能に基づいてユーザーグループに割り当てます。ユーザーグループの例には、アプリケーション、データ、ネットワーク、開発オペレーション (DevOps) エンジニアなどがあります。また、ユーザータイプは、意思決定の権限に基づいて、シニアエンジニアや非シニアエンジニアなどさらに小規模なユーザーグループに分けることもできます。

IAM ユーザーのアクセス許可を割り当てるには

1. IAM ユーザーグループを作成します (IAM ドキュメント)。
2. IAM ユーザーグループに AWS 管理ポリシーをアタッチする (IAM ドキュメント) 。

ACCT.05 — ログインのための多要素認証 (MFA) を要求する

MFA では、ユーザーは認証チャレンジに対するレスポンスを生成するデバイスを所有します。サインインプロセスを完了するには、各ユーザーの認証情報とデバイス生成のレスポンスの両方が必要です。セキュリティのベストプラクティスとして、MFA による AWS アカウント アクセス、特にアカウントのルートユーザーや IAM ユーザーなどの長期的な認証情報を有効にします。

ルートユーザーに MFA を設定するには

1. AWS Management Console で にサインインしますhttps://console.aws.amazon.com/。
2. ナビゲーションバーの右側でアカウント名を選択し、[マイセキュリティ資格情報] を選択します。
3. 必要に応じて、[セキュリティ認証情報に進む] を選択します。
4. [Multi-Factor Authentication (MFA)] セクションを展開します。
5. [Activate MFA] (MFA の有効化) を選択します。
6. ウィザードの指示に従って、MFA デバイスを適宜設定します。詳細については、「AWSでのユーザーの MFA デバイスの有効化」(IAM ドキュメント) を参照してください。

MFA を IAM アイデンティティセンターで設定するには

- MFA を有効にします (IAM アイデンティティセンタードキュメント)。

MFA を自分の IAM ユーザー用に設定するには

1. https://console.aws.amazon.com/iam で、サインインの認証情報を使用して IAM コンソールにサインインします。
2. 右上のナビゲーションバーでユーザー名を選択し、続いて [My Security Credentials (セキュリティ認証情報)] を選択します。
3. [AWS IAM 認証情報] タブの [Multi-Factor Authentication] セクションで、[MFA デバイスの管理] を選択します。

他の IAM ユーザーに MFA を設定するには

1. にサインイン AWS Management Console し、 で IAM コンソールを開きますhttps://console.aws.amazon.com/iam。
2. ナビゲーションペインで [Users (ユーザー)] を選択します。
3. MFA を有効にする対象のユーザー名を選択し、[Security credentials] タブを選択します。
4. [Assigned MFA device] (割り当て済み MFA デバイス) の横で、[Manage] (管理) を選択します。
5. ウィザードの指示に従って、MFA デバイスを適宜設定します。詳細については、「AWSでのユーザーの MFA デバイスの有効化」(IAM ドキュメント) を参照してください。

ACCT.06 — パスワードポリシーを適用する

ユーザーはサインイン認証情報 AWS Management Console を入力して にログインします。MFA をお勧めします。ブルートフォース攻撃やソーシャルエンジニアリング攻撃による検出を回避するには、強力なパスワードポリシーに従うパスワードが必要になります。

強力なパスワードに関する最新の推奨事項については、米国の Center for Internet Security (CIS) のウェブサイトにある「Password Policy Guide」を参照してください。

IAM ユーザーの場合、カスタム IAM パスワードポリシーでパスワード要件を設定できます。詳細については、「Setting an account password policy」(IAM ドキュメント) を参照してください。

カスタムパスワードポリシーを作成するには

1. にサインイン AWS Management Console し、 で IAM コンソールを開きますhttps://console.aws.amazon.com/iam。
2. ナビゲーションペインで [アカウント設定] を選択します。

3. [Password policy] (パスワードポリシー) セクションで、[Change password policy] (パスワードポリシーを変更する) を選択します。
4. パスワードポリシーに適用するオプションを選択し、[変更の保存] を選択します。

ACCT.07 — 保護された S3 バケットに CloudTrail ログを配信する

AWS アカウント内のユーザー、ロール、およびサービスによって実行されたアクションは、 にイベントとして記録されます AWS CloudTrail。 CloudTrail はデフォルトで有効になっており、CloudTrail コンソールでは 90 日間のイベント履歴情報にアクセスできます。 AWS インフラストラクチャ全体のアカウントアクティビティを表示、検索、ダウンロード、アーカイブ、分析、応答するには、「イベント履歴による CloudTrailイベントの表示 (CloudTrail ドキュメント)」を参照してください。

追加データを含む CloudTrail 履歴を 90 日間保持するには、すべてのイベントタイプの Amazon Simple Storage Service (Amazon S3) バケットにログファイルを配信する新しい証跡を作成します。CloudTrail コンソールで証跡を作成するときは、マルチリージョンの証跡を作成します。

すべての のログを S3 バケット AWS リージョン に配信する証跡を作成するには

1. 証跡 (ドキュメント) を作成します。CloudTrail [ログイベントの選択] ページで、次の操作を行います。

   a. [API アクティビティ] で、[読み取り] と [書き込み] の両方を選択します。

   b. 本番前の環境の場合は、[AWS KMS イベントを除外] を選択します。これは、証跡からすべての AWS Key Management Service （ AWS KMS) イベントを除外します。AWS KMS `Encrypt`、、 `Decrypt`などの読み取りアクションは、大量のイベントを生成`GenerateDataKey`できます。

      本番環境の場合は、書き込み管理イベントの記録を選択し、 AWS KMS イベントを除外のチェックボックスをオフにします。大量の AWS KMS 読み取りイベントは除外されますが、`Disable`、、 などの関連する書き込みイベント`Delete`は記録されます`ScheduleKey`。これらは、実稼働環境に推奨される最小限の AWS KMS ログ記録設定です。

2. 新しい証跡が [Trails] (証跡) ページに表示されます。約 15 分で、 はアカウントで行われた AWS アプリケーションプログラミングインターフェイス (API) 呼び出しを示すログファイル CloudTrail を発行します。ユーザーは、指定した S3 バケット内のログファイルを確認することができます。

CloudTrail ログファイルを保存する S3 バケットをセキュリティで保護するには

1. ログファイルを保存するすべてのバケットについて Amazon S3 バケットポリシー (CloudTrail ドキュメント) を確認し、必要に応じて調整して不要なアクセスを削除します。
2. セキュリティのベストプラクティスとして、バケットポリシーに必ず手動で `aws:SourceArn` 条件キーを追加します。　詳細については、「組織の証跡のログファイルを保存するために使用する Amazon S3 バケットを作成または更新する (CloudTrail ドキュメント) 」を参照してください。
3. MFA 削除を有効にします (Amazon S3 ドキュメント)。

ACCT.08 — プライベート S3 バケットへのパブリックアクセスを阻止する

デフォルトでは、 のルートユーザー AWS アカウント と IAM プリンシパルのみが、使用した場合、そのプリンシパルによって作成された Amazon S3 バケットに対する読み取りと書き込みのアクセス許可を持ちます。その他の IAM プリンシパルには、アイデンティティベースのポリシーを使用してアクセス権限が付与され、アクセス条件はバケットポリシーを使用して適用されます。ユーザーは、一般ユーザーにパブリックバケットへのアクセスを許可するバケットポリシーを作成できます。

2023 年 4 月 28 日以降に作成されたバケットでは、パブリックアクセスブロック設定がデフォルトで有効になっています。この日付以前に作成されたバケットでは、ユーザーがバケットポリシーを誤って設定し、一般ユーザーに意図せずアクセス権限を付与することがありました。パブリックアクセスブロック設定を各バケットで有効にすると、このような設定ミスを防ぐことができます。パブリック S3 バケットの現在または将来のユースケースがない場合は、この設定を AWS アカウント レベルで有効にします。設定すると、ポリシーによってパブリックアクセスが許可されることを阻止できます。

S3 バケットへのパブリックアクセスを阻止するには

- S3 バケットにパブリックアクセスブロックを設定します (Amazon S3 ドキュメント)。

AWS Trusted Advisor は、パブリックへのリストアクセスまたは読み取りアクセスを許可する S3 バケットの黄色の結果を生成し、パブリックアップロードまたは削除を許可するバケットの赤色の結果を生成します。基準線として、コントロール ACCT.12 — Trusted Advisorを使用してハイリスクな問題をモニタリングし解決する に従い、設定ミスのあるバケットを特定して修正します。パブリックアクセス可能な S3 バケットは、Amazon S3 コンソールにも表示されます。

ACCT.09 — 使用していない VPC、サブネット、セキュリティグループを削除する

セキュリティ問題の発生を減らすため、使用していないリソースがあればすべて削除するかオフにします。新しい AWS アカウントでは、デフォルトですべての に Virtual Private Cloud (VPC) が自動的に作成されます。これにより AWS リージョン、パブリックサブネットにパブリック IP アドレスを割り当てることができます。ただし VPC が不要な場合、これによりリソースを意図せず公開するリスクが高まります。

使用していない場合は、ワークロードをデプロイする可能性のあるリージョンだけでなくすべてのリージョンでデフォルトの VPC を削除します。VPC を削除すると、サブネットやセキュリティグループなど、そのコンポーネントも削除されます。

> **Note**
>
> すべてのリージョンと VPC は、次の場所にある Amazon EC2 グローバルビューコンソールで確認できます。https://console.aws.amazon.com/ec2globalview/home詳細については、「Amazon EC2 Global View を使用して、リージョン間のリソースを一覧表示およびフィルターをかけます」(Amazon EC2 ドキュメント) を参照してください。

使用していないデフォルト VPC を削除するには

1. VPC を削除します(Amazon VPC ドキュメント)。
2. 必要であれば他のリージョンでも同じ手順を繰り返します。

ACCT.10 — 支出をモニタリング AWS Budgets するように を設定する

AWS Budgets は、コストが目標しきい値を超えることが予測される場合に、通知による月額コストと使用状況のモニタリングを可能にします。予測コスト通知は、予期しないアクティビティを示すことができ、 AWS Trusted Advisor や Amazon などの他のモニタリングシステムに加えて、防御を強化します GuardDuty。 AWS コストのモニタリングと理解は、優れた運用上の成果の一部でもあります。

で予算を設定するには AWS Budgets

- コスト予算 (AWS Budgets ドキュメント) を作成します。

ACCT.11 — GuardDuty 通知を有効にして応答する

Amazon GuardDuty は、 AWS アカウント、ワークロード、データを保護するために、悪意のある動作や不正な動作を継続的にモニタリングする脅威検出サービスです。予期しないアクティビティや潜在的に悪意のあるアクティビティを検出すると、 は詳細なセキュリティ検出結果 GuardDuty を提供して可視性と修復を行います。 は、暗号通貨マイニングアクティビティ、Tor クライアントやリレーからのアクセス、予期しない動作、侵害された IAM 認証情報などの脅威を検出 GuardDuty できます。検出結果を有効に GuardDuty して対応し、 AWS 環境内の潜在的に悪意のある、または不正な動作を停止します。での検出結果の詳細については GuardDuty、「検出結果タイプ (GuardDuty ドキュメント) 」を参照してください。

Amazon CloudWatch Events を使用して、 が結果 GuardDuty を作成したとき、または結果が変更されたときの自動通知を設定できます。まず、Amazon Simple Notification Service (Amazon SNS) トピックを設定し、そのトピックに、エンドポイントか E メールアドレスを追加します。次に、GuardDuty 検出結果の CloudWatch イベントを設定し、イベントルールが Amazon SNS トピックのエンドポイントに通知します。

GuardDuty および GuardDuty 通知を有効にするには

1. Amazon (ドキュメント) を有効にします GuardDuty。GuardDuty
2. GuardDuty 検出結果を通知する CloudWatch イベントルールを作成します (ドキュメント) 。GuardDuty

ACCT.12 — Trusted Advisorを使用してハイリスクな問題をモニタリングし解決する

AWS Trusted Advisor は、 AWS インフラストラクチャをスキャンして、セキュリティ、パフォーマンス、コスト、信頼性に関連するリスクまたは影響の高い問題がないかを確認します。影響を受けるリソースと推奨される修復方法について、詳細な情報を提供します。チェックと説明の完全なリストについては、AWS Trusted Advisor 「チェックリファレンス (Trusted Advisor ドキュメント) 」を参照してください。

Trusted Advisor 結果を定期的に確認し、必要に応じて問題を修復します。 AWS ビジネスサポートプランまたはエンタープライズサポートプランをご利用の場合は、毎週の結果 E メールをサブスクライブできます。詳細については、「通知設定の設定」(AWS Support ドキュメント) を参照してください。

で問題を表示するには Trusted Advisor

- 「チェックカテゴリの表示 (AWS Support ドキュメント）」の指示に従って、各チェックカテゴリを確認します。少なくとも、赤色で表示される推奨のアクションを確認することが推奨されます。

ワークロードのセキュリティ保護

このセクションの制御と推奨事項は、AWS で実行されるワークロードの構築中に、それらを保護するのに役立ちます。アプリケーションのシークレットとアクセス範囲の管理、プライベートリソースへのアクセスルートの最小化、暗号化による転送中および保存中のデータの保護など、安全なプラクティスを重視しています。

このセクションは、以下のトピックで構成されます。

WKLD.01 — コンピューティング環境へのアクセス許可に IAM ロールを使用する

AWS Identity and Access Management (IAM) では、ロールは、設定可能な期間にユーザーまたはサービスが引き受けることのできる一連のアクセス許可を表します。ロールを使用すると、認証情報の長期保存や管理が不要になり、想定外の使用の可能性が大幅に低減されます。Amazon Elastic

Compute Cloud (Amazon EC2) インスタンス、AWS Fargate タスクとサービス、AWS Lambda 機能、その他の AWS コンピューティングサービスに IAM ロールを直接割り当てます (サポートされている場合)。AWS SDK を使用し、これらのコンピューティング環境で実行されるアプリケーションは、認証に IAM ロール認証情報を自動的に使用します。

各サービスで IAM ロールを使用する方法と手順については、サービスごとの「AWS のドキュメント」を参照してください。例えば、以下を参照してください。

- Amazon EC2 の IAM ロール (Amazon EC2 のドキュメント)
- タスク用の IAM ロール (Amazon Elastic Container Service のドキュメント)
- Lambda 実行ロール (Lambda のドキュメント)

WKLD.02 — リソースベースのポリシー権限で認証情報の使用範囲を制限する

ポリシーとは、アクセス許可を定義したり、アクセス条件を指定したりできるオブジェクトです。ポリシーには主に 2 種類あります。

- アイデンティティベースのポリシーはプリンシパルにアタッチされ、プリンシパルの AWS 環境でのアクセス許可を定義します。
- リソースベースのポリシーは、Amazon Simple Storage Service (Amazon S3) バケットや仮想プライベートクラウド (VPC) エンドポイントなどのリソースにアタッチされます。これらのポリシーは、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、満たすべき条件を指定します。

プリンシパルがアクセスを許可され、リソースに対してアクションを実行するには、プリンシパルに ID ベースのポリシーでアクセス許可が付与され、リソースベースのポリシーの条件を満たす必要があります。詳細については、「アイデンティティベースおよびリソースベースのポリシー」(IAM のドキュメント) を参照してください。

リソースベースのポリシーの推奨条件は次のとおりです。

- (AWS Organizationsで定義した) 特定の組織のプリンシパルのみに、`aws:PrincipalOrgID` 条件を使用してアクセスを制限します。
- 特定の VPC または VPC エンドポイントから発信されるトラフィックへのアクセスを、それぞれ `aws:SourceVpc` または `aws:SourceVpce` 条件を使用して制限します。

- aws:SourceIp 条件を使用して、送信元 IP アドレスに基づいてトラフィックを許可または拒否します。

以下は、aws:PrincipalOrgID 条件を使用して、**<o-xxxxxxxxxxx>** 組織内のプリンシパルのみに **<bucket-name>** S3 バケットへのアクセスを許可するリソースベースのポリシーの例です。

```
{
   "Version":"2012-10-17",
   "Statement":[
     {
       "Sid":"AllowFromOrganization",
       "Effect":"Allow",
       "Principal":"*",
       "Action":"s3:*",
       "Resource":"arn:aws:s3:::<bucket-name>/*",
       "Condition": {
         "StringEquals": {"aws:PrincipalOrgID":"<o-xxxxxxxxxxx>"}
       }
     }
   ]
}
```

WKLD.03 — エフェメラルシークレットまたはシークレット管理サービスを使用する

アプリケーションシークレットは、主にキーペア、アクセストークン、デジタル証明書、サインイン認証情報などの認証情報で構成されています。アプリケーションはこれらのシークレットを使用して、データベースなど、依存している他のサービスにアクセスします。これらのシークレットを保護するには、エフェメラルなもの (リクエスト時に生成され、IAM ロールなどでは有効期間が短いもの) にするか、シークレット管理サービスから取得することをお勧めします。これにより、静的な設定ファイルに保持するなど、安全性の低いメカニズムにより誤って公開されるのを防ぐことができます。また、アプリケーションコードを開発環境から本番環境に移行することも容易になります。

シークレット管理サービスの場合は、パラメータストア、AWS Systems Manager の機能、AWS Secrets Manager を組み合わせて使用することをお勧めします。

- パラメータストアを使用すると、シークレットやその他のパラメータ (個別のキーと値のペア、文字列ベース、全体の長さが短いもの、頻繁にアクセスするものなど) を管理できます。AWS Key Management Service (AWS KMS) キーを使用して、シークレットを暗号化します。パラメータス

トアの標準階層にパラメータを保存しても料金はかかりません。パラメータ階層の詳細については、「パラメータ階層の管理」(Systems Manager のドキュメント) を参照してください。

- シークレットマネージャーを使用して、ドキュメント形式のシークレット (関連する複数のキーと値のペアなど)、4 KB を超えるシークレット (デジタル証明書など)、または自動ローテーションのメリットを得られるシークレットを保存します。

パラメータストア API を使用して、シークレットマネージャーに保存されているシークレットを取得できます。これにより、両方のサービスを組み合わせて使用する際に、アプリケーションのコードを標準化できます。

パラメータストアでシークレットを管理するには

1. 対称 AWS KMS キーの作成 (AWS KMS のドキュメント)
2. SecureString パラメータを作成する (Systems Manager のドキュメント) パラメータストアのシークレットは `SecureString` データタイプを使用します。
3. アプリケーションでは、プログラミング言語用の AWS SDK を使用して、パラメータストアからパラメータを取得します。Java の例については、「GetParameter.java」(AWS Code Sample Catalog) を参照してください。

Secrets Manager でシークレットを管理するには

1. シークレットの作成 (Secrets Manager のドキュメント)
2. コードの AWS Secrets Manager からシークレットを取得する (Secrets Manager のドキュメント)

   「AWS Secrets Manager クライアント側のキャッシュライブラリを使用して、シークレット使用の可用性とレイテンシーを改善する」(AWS ブログ記事) を読むことが重要です。既にベストプラクティスが実装されているクライアント側の SDK を使用すると、Secrets Manager の使用と統合が迅速かつ簡単になります。

WKLD.04 — アプリケーションシークレットが公開されるのを防ぐ

ローカルでの開発中、アプリケーションシークレットがローカルの設定ファイルやコードファイルに保存され、誤ってソースコードリポジトリにチェックインされてしまう場合があります。公共サービスプロバイダーがホストする、安全でないリポジトリは不正アクセスの対象となり、シークレットを発見されるおそれがあります。利用可能なツールで、シークレットのチェックインを防止してくださ

い。手動のコードレビュープロセスの一環として、公開されたシークレットのチェックを組み込みます。

アプリケーションシークレットがソースコードリポジトリにチェックインされることを防ぐ一般的なツールは以下のとおりです。

- Gitleaks (GitHub リポジトリ)
- Whispers (GitHub リポジトリ)
- detect-secrets (GitHub リポジトリ)
- git-secrets (GitHub リポジトリ)
- TruffleHog (GitHub リポジトリ)

WKLD.05 — 公開されたシークレットを検出して修正する

WKLD.03 — エフェメラルシークレットまたはシークレット管理サービスを使用する および WKLD.04 — アプリケーションシークレットが公開されるのを防ぐ で、シークレットを保護するための対策を講じます。この制御により、シークレットがこれらの予防措置をバイパスしたかどうかを検出するソリューションをデプロイし、それに従って修正することができます。

Amazon CodeGuru Reviewer は、ソースコード内のアプリケーションシークレットを検出し、検出したシークレットを修正して Secrets Manager に公開するメカニズムを提供します。Secrets Manager からシークレットを取得するためのアプリケーションコードも提供されています。費用対効果の分析を実施して、このソリューションがビジネスに適しているかどうかを判断してください。別の方法として、WKLD.04 — アプリケーションシークレットが公開されるのを防ぐ のオープンソース ソリューションの一部は、既存のシークレットの検出機能を提供しています。

CodeGuru Reviewer と Secrets Manager の統合を設定するには

- CodeGuru Reviewer を使用して、ハードコーディングされたシークレットと AWS Secrets Manager を特定し、それらを保護する (AWS ブログ記事とガイド付きウォークスルー)

WKLD.06 — SSH または RDP の代わりに Systems Manager を使用する

インターネットゲートウェイを指すデフォルトルートを持つパブリックサブネットは、インターネットへのルートを持たないプライベートサブネットよりも本質的にセキュリティリスクが高くなりま

す。プライベートサブネットで EC2 インスタンスを実行し、AWS Systems Manager の Session Manager 機能を使用して、AWS Command Line Interface (AWS CLI) または AWS Management Console を介してインスタンスにリモートアクセスできます。その後、AWS CLI またはコンソールを使用して、セキュアなトンネルを介してインスタンスに接続するセッションを開始することで、Secure Shell (SSH) や Windows リモートデスクトッププロトコル (RDP) に使用される追加の認証情報を管理する必要がなくなります。

パブリックサブネットで EC2 インスタンスを実行したり、ジャンプボックスを実行したり、踏み台ホストを実行したりする代わりに、Session Manager を使用してください。

Session Manager を設定するには

1. EC2 インスタンスが Amazon Linux 2 や Ubuntu など、最新のオペレーティングシステムの Amazon マシンイメージ (AMI) を使用していることを確認します。AWS Systems Manager エージェント (SSM エージェント) は AMI にあらかじめインストールされています。
2. インスタンスが、インターネットゲートウェイまたは VPC エンドポイントを経由して、(**<region>** の代わりに適切な AWS リージョン で) これらのアドレスに接続していることを確認します。
    a. Ec2messages.<region>.amazonaws.com
    b. ssm.<region>.amazonaws.com
    c. ssmmessages.<region>.amazonaws.com
3. AWS マネージドポリシー `AmazonSSMManagedInstanceCore` を、インスタンスに関連付けられている IAM ロールにアタッチします。

詳細については、「Session Manager のセットアップ」(Systems Manager のドキュメント) を参照してください。

セッションを開始するには

- セッションを開始する (Systems Manager のドキュメント)

WKLD.07 — 機密データを含む S3 バケットのデータイベントを記録する

デフォルトでは、AWS CloudTrail は管理イベントや、アカウント内のリソースの作成、変更、削除のイベントをキャプチャします。これらの管理イベントは、Amazon Simple Storage Service バケッ

ト内の個々のオブジェクトに対する読み取りまたは書き込みオペレーションをキャプチャしません。セキュリティイベント中は、データへの不正なアクセスや使用を個々のレコードまたはオブジェクトレベルでキャプチャすることが重要です。CloudTrail を使用して、機密データやビジネスクリティカルなデータを保存する任意の S3 バケットのデータイベントを、検出と監査のために記録します。

> **Note**
>
> データイベントのログ記録には追加料金が適用されます。詳細については、AWS CloudTrail 料金を参照してください。

証跡のデータイベントを記録するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ で CloudTrail コンソールを開きます。
2. ナビゲーションメニューで、 [証跡] を選択し、証跡を選択します。
3. [一般的な詳細情報] で [編集] を選択し、次の設定を変更します。証跡の名前は変更できません。
    a. [データイベント] で [編集] を選択します。
    b. [Data source] で、[S3] を選択します。
    c. [現在および将来のすべての S3 バケット]で、[読み取り] および [書き込み] をクリアします。
    d. [個々のバケットの選択] で、データイベントを記録するバケットを参照します。このウィンドウで、複数のバケットを選択できます。[Add bucket] を選択してより多くのバケットのデータイベントをログ記録します。[読み取り] イベント (例: `GetObject`) か、[書き込み] イベント (例: `PutObject`)、または両方を選択します。
    e. [証跡の作成] を選択します。

WKLD.08 — Amazon EBS ボリュームを暗号化する

AWS アカウントのデフォルト動作として、Amazon Elastic Block Store (Amazon EBS) ボリュームの暗号化を強制します。暗号化されたボリュームの 1 秒あたりの入出力オペレーション (IOPS) パフォーマンスは、暗号化されていないボリュームと同じですが、レイテンシーへの影響は最小限に抑えられます。これにより、コンプライアンスやその他の理由で後日、ボリュームを再構築する必要がなくなります。詳細については、「Amazon EBS 暗号化の必須ベストプラクティス」(AWS ブログ記事) を参照してください。

Amazon EBS ボリュームを暗号化するには

- デフォルトで暗号化を有効にする (Amazon EC2 のドキュメント)。

WKLD.09 — Amazon RDS データベースを暗号化する

WKLD.08 — Amazon EBS ボリュームを暗号化する と同様に、Amazon Relational Database Service (Amazon RDS) データベースの暗号化を有効にします。この暗号化は、基盤となるボリュームレベルで実行され、レイテンシーへの影響を最小限に抑えながら、暗号化されていないボリュームと同じ IOPS パフォーマンスを発揮します。詳細については、「Amazon RDS リソースの暗号化の概要」(Amazon RDS のドキュメント) を参照してください。

RDS データベースインスタンスを暗号化するには

- データベースインスタンスの暗号化 (Amazon RDS のドキュメント)。

WKLD.10 — プライベートリソースをプライベートサブネットにデプロイする

EC2 インスタンス、データベース、キュー、キャッシュ、その他のインフラストラクチャなど、インターネットへの直接アクセスを必要としないリソースを VPC プライベートサブネットにデプロイします。プライベートサブネットでは、アタッチされたインターネットゲートウェイへのルートがルートテーブルに宣言されていないため、インターネットトラフィックを受信できません。プライベートサブネットから発信される、インターネット宛てのトラフィックは、マネージド AWS NAT ゲートウェイ、またはパブリックサブネットで NAT プロセスを実行する EC2 インスタンスのいずれかを介してネットワークアドレス変換 (NAT) を受ける必要があります。ネットワーク隔離の詳細については、「Amazon VPC のインフラストラクチャセキュリティ」(Amazon VPC のドキュメント) を参照してください。。

プライベートリソースとサブネットを作成するときは、以下のプラクティスを使用してください。

- プライベートサブネットを作成するときは、[パブリック IPv4 アドレスの自動割り当て] を無効にします。
- プライベート EC2 インスタンスを作成するときは、[自動割り当てパブリック IP] を無効にします。これにより、設定ミスによりインスタンスがパブリックサブネットに想定外にデプロイされても、パブリック IP が割り当てられるのを防ぐことができます。

必要に応じて、設定の一部としてリソースのサブネットを指定します。Modular and Scalable VPC Architecture Quick Start (AWS クイックスタート) を使用して、ベストプラクティスに従った VPC をデプロイできます。

WKLD.11 — セキュリティグループを使用してネットワークアクセスを制限する

セキュリティグループを使用して、EC2 インスタンス、RDS データベース、その他のサポートされているリソースへのトラフィックを制御します。セキュリティグループは、関連するリソースのあらゆるグループに適用できる仮想ファイアウォールとして機能し、インバウンドトラフィックとアウトバウンドトラフィックを許可するルールを一貫して定義します。IP アドレスとポートに基づくルールに加えて、セキュリティグループは他のセキュリティグループに関連するリソースからのトラフィックを許可するルールをサポートしています。例えば、データベースセキュリティグループには、アプリケーションサーバーセキュリティグループからのトラフィックのみを許可するルールを設定できます。

デフォルトでは、セキュリティグループはすべてのアウトバウンドトラフィックを許可しますが、インバウンドトラフィックは許可しません。アウトバウンドトラフィックルールは、削除することも、アウトバウンドトラフィックを制限してインバウンドトラフィックを許可する追加ルールを設定することもできます。セキュリティグループにアウトバウンドルールがない場合、インスタンスから送信されるアウトバウンドトラフィックは許可されません。詳細については、「セキュリティグループを使用してリソースへのトラフィックを制御する」(Amazon VPC のドキュメント) を参照してください。

次の例には、Application Load Balancer から、Amazon RDS for MySQL データベースに接続する EC2 インスタンスへのトラフィックを制御する、3 つのセキュリティグループがあります。

セキュリティグループ	インバウンドルール	アウトバウンドルール
Application Load Balancer のセキュリティグループ	説明: 任意の場所からの HTTPS トラフィックを許可する タイプ: HTTPS 送信元: Anywhere-IPv4 (0.0.0.0/0)	説明: すべてのトラフィックを任意の場所で許可する タイプ: すべてのトラフィック 送信先: Anywhere-IPv4 (0.0.0.0/0)

セキュリティグループ	インバウンドルール	アウトバウンドルール
EC2 インスタンスのセキュリティグループ	説明: Application Load Balancer からの HTTP トラフィックを許可する [Type]: HTTP 送信元: Application Load Balancer のセキュリティグループ	説明: すべてのトラフィックを任意の場所で許可する タイプ: すべてのトラフィック 送信先: Anywhere-IPv4 (0.0.0.0/0)
RDS データベースセキュリティグループ	説明: EC2 インスタンスからの MySQL トラフィックを許可する タイプ: MySQL 送信元: EC2 インスタンスのセキュリティグループ	アウトバウンドルールなし

WKLD.12 — VPC エンドポイントを使用して、サポート対象のサービスにアクセスする

VPC では、AWS やその他の外部サービスにアクセスする必要があるリソースに、インターネット (0.0.0.0/0) またはターゲットサービスのパブリック IP アドレスへのルートが必要です VPC エンドポイントを使用して、VPC からサポート対象の AWS またはその他のサービスまでのプライベート IP ルートを有効化し、インターネットゲートウェイ、NAT デバイス、仮想プライベートネットワーク (VPN) 接続、または AWS Direct Connect 接続を不要にします。

VPC エンドポイントは、サービスへのアクセスをさらに制御するためのポリシーとセキュリティグループのアタッチをサポートします。例えば、Amazon DynamoDB の VPC エンドポイントポリシーを作成して、独自のアクセス許可ポリシーに関係なく、VPC 内のすべてのリソースに対して項目レベルのアクションのみを許可し、テーブルレベルのアクションを防止できます。特定の VPC エンドポイントからのリクエストのみを許可し、その他すべての外部アクセスを拒否する S3 バケットポリシーを作成することもできます。VPC エンドポイントには、ウェブアプリケーションのビジネス口

ジック層など、アプリケーション固有のセキュリティグループに関連付けられた EC2 インスタンスのみにアクセスを制限するセキュリティグループルールを設定することもできます。

VPC エンドポイントにはさまざまな種類があります。VPC インターフェイスエンドポイントを使用して、ほとんどのサービスにアクセスできます。DynamoDB には、ゲートウェイエンドポイントを使用してアクセスします。Amazon S3 は、インターフェイスエンドポイントとゲートウェイエンドポイントの両方をサポートしています。1 つの AWS アカウントとリージョンに含まれるワークロードには、ゲートウェイエンドポイントをお勧めします。追加料金はかかりません。他の VPC、オンプレミスネットワーク、または別の AWS リージョン から S3 バケットにアクセスするなど、より拡張性の高いアクセスが必要な場合は、インターフェイスエンドポイントをお勧めします。インターフェイスエンドポイントには、1 時間あたりの稼働時間料金と GB 単位のデータ処理料金が課金されますが、どちらも AWS NAT ゲートウェイ経由で `0.0.0.0/0` にデータを送信するそれぞれの料金よりも低額になります。

VPC エンドポイントの使用の詳細については、以下のリソースを参照してください。

- Amazon S3 のゲートウェイエンドポイントとインターフェイスエンドポイントの選択の詳細については、「Amazon S3 の VPC エンドポイント戦略の選択」(AWS ブログ記事) を参照してください。
- インターフェイスエンドポイントの作成 (Amazon VPC のドキュメント)
- ゲートウェイエンドポイントの作成 (Amazon VPC のドキュメント)
- 特定の VPC または VPC エンドポイントへのアクセスを制限する S3 バケットポリシーの例については、「特定の VPC へのアクセスの制限」(Amazon S3 のドキュメント) を参照してください。。
- アクションを制限する DynamoDB エンドポイントポリシーの例については、「DynamoDB のエンドポイントポリシー」(Amazon VPC のドキュメント) を参照してください。

WKLD.13 — すべてのパブリックウェブエンドポイントに HTTPS を要求する

HTTPS を要求してウェブエンドポイントの信頼性を高め、エンドポイントが証明書を使用してアイデンティティを証明することで、エンドポイントと、接続しているクライアント間のすべてのトラフィックが暗号化されていることを確認できるようにします。公開ウェブサイトの場合、これにより検索エンジンのランキングが高くなるという利点もあります。

多くの AWS サービスは、AWS Elastic Beanstalk、Amazon CloudFront、Amazon API Gateway、Elastic Load Balancing、AWS Amplify のようなリソース用のパブリックウェザエンドポ

イントを提供しています。これらのサービスに HTTPS を要求する方法については、以下を参照してください。

- Elastic Beanstalk (Elastic Beanstalk のドキュメント)
- CloudFront (CloudFront のドキュメント)
- Application Load Balancer (AWS ナレッジセンター)
- Classic Load Balancer (AWS ナレッジセンター)
- Amplify (Amplify のドキュメント)

Amazon S3 でホストされている静的ウェブサイトは、HTTPS をサポートしていません。これらのウェブサイトに HTTPS を要求するには、CloudFront を使用します。CloudFront を通じてコンテンツを提供する S3 バケットへのパブリックアクセスは不要です。

CloudFront を使用して、Amazon S3 でホストされる静的ウェブサイトを提供するには

1. CloudFront を使用して、Amazon S3 でホストされる静的ウェブサイトを提供する (AWS ナレッジセンター)
2. パブリック S3 バケットへのアクセスを設定している場合、ビューワーと CloudFront 間の通信で HTTPS を必須にします (CloudFront のドキュメントを参照)。

   プライベート S3 バケットへのアクセスを設定している場合、オリジンアクセスアイデンティティを使用して Amazon S3 コンテンツへのアクセスを制限します (CloudFront のドキュメントを参照)。

古いプロトコルとの互換性が必要でない限り、最新の Transport Layer Security (TLS) プロトコルと暗号を要求するように、HTTPS エンドポイントを設定します。例えば、デフォルトの `ELBSecurityPolicy-2016-08` ではなく、`ELBSecurityPolicy-FS-1-2-Res-2020-10` または、Application Load Balancer の HTTPS リスナーで使用できる最新のポリシーを使用します。最新のポリシーでは、最低 TLS 1.2、前方秘匿性、および最新のウェブブラウザと互換性のある強力な暗号が必要です。

HTTPS パブリックエンドポイントで使用できるセキュリティポリシーの詳細については、以下を参照してください。

- Classic Load Balancer 用の事前定義済み SSL セキュリティポリシー (Elastic Load Balancingの ドキュメント)
- Application Load Balancer のセキュリティポリシー (Elastic Load Balancing のドキュメント)

- ビューワーと CloudFront との間でサポートされているプロトコルと暗号 (CloudFront のドキュメント)

WKLD.14 — パブリックエンドポイントにエッジプロテクションサービスを使用する

EC2 インスタンスやコンテナなどのコンピューティングサービスから直接トラフィックを処理するのではなく、エッジプロテクションサービスを使用してください。これにより、インターネットからの受信トラフィックと、そのトラフィックを処理するリソースとの間にセキュリティレイヤーが追加されます。これらのサービスは、トラフィックが内部リソースに到達する前に、不要なトラフィックをフィルタリングし、暗号化を強制し、ルーティングやその他のルール (負荷分散など) を適用できます。

パブリックエンドポイントを保護できる AWS サービスには、AWS WAF、CloudFront、Elastic Load Balancing、API Gateway、Amplify Hosting などがあります。Elastic Load Balancing などの VPC ベースのサービスを、プライベートサブネットで実行されるウェブサービスリソースへのプロキシとして、パブリックサブネットで実行します。

CloudFront、API Gateway、Amazon Route 53 は、レイヤー 3 や 4 の分散型サービス妨害 (DDoS) 攻撃からの保護を無料で提供します。AWS WAF はレイヤー 7 攻撃に対する保護を提供します。

これら各サービスの使用を開始する手順については、以下を参照してください。

- AWS WAF の開始方法 (AWS ウェブサイト)
- Amazon CloudFront の開始方法 (CloudFront のドキュメント)
- Elastic Load Balancing の開始方法 (Elastic Load Balancing のドキュメント)
- API Gateway の開始方法 (API Gateway のドキュメント)
- Amplify Hosting の開始方法 (Amplify のドキュメント)

WKLD.15 — テンプレートでセキュリティコントロールを定義し、CI/CD プラクティスを使用してデプロイする

Infrastructure as code (IaC) は、ソフトウェア アプリケーションのデプロイに使用されるものと同じ継続的インテグレーションと継続的デリバリー (CI/CD) パイプラインを使用してデプロイするテンプレートとコードであり、すべての AWS サービスリソースと設定を定義するプラクティスで

す。AWS CloudFormation などの IaC サービスは、IAM アイデンティティベースのポリシーとリソースベースのポリシーの両方をサポートし、Amazon GuardDuty、AWS WAF、Amazon VPC などの AWS セキュリティサービスをサポートしています。これらのアーティファクトを IaC テンプレートとしてキャプチャし、テンプレートをソースコードリポジトリにコミットし、CI/CD パイプラインを使用してそれらをデプロイします。

特に必要でない限り、同じリポジトリ内のアプリケーションコードでアプリケーション権限ポリシーをコミットし、一般的なリソースポリシーとセキュリティサービス設定を別々のコードリポジトリとデプロイパイプラインで管理します。

AWS で IaC の使用を開始する方法の詳細については、「AWS Cloud Development Kit (AWS CDK)」のドキュメントを参照してください。

寄稿者

本ドキュメントの寄稿者は次のとおりです。

- Principal Solutions Architect、Jay Michael
- Principal Solutions Architect、Cole Calistra
- Principal Solutions Architect、Justin Plock
- Solutions Architect、Faisal Farooq
- Sr. Solutions Architect、Michael Nguyen
- Sr. Solutions Architect、Ritik Khatwani
- Office of the Chief Information Security Officer (CISO)、Principal、Paul Hawkins

また、指導および評価を通じて支援してくださった以下の方々にも深く感謝いたします。

- Robert Put
- Mike Sullivan
- Bob Lee III

ドキュメント履歴

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

変更	説明	日付
Amazon S3 バケットの設定	「ACCT.08 – プライベート S3 バケットへのパブリックアクセスを禁止する」セクションを更新し、2023 年 4 月 28 日以降に作成された Amazon S3 バケットでは、ブロックパブリックアクセス設定がデフォルトで有効になっていることを反映しました。	2023 年 5 月 18 日
IAM セキュリティのベストプラクティス	このガイドは、最新の AWS Identity and Access Management (IAM) のベストプラクティスと一致するように更新されました。。詳細については、IAM ドキュメントの「セキュリティのベストプラクティス」を参照してください。	2023 年 2 月 1 日
IAM ロール	「WKLD.01 – コンピューティング環境へのアクセス許可に IAM ロールを使用する」セクションに AWS のサービス ドキュメントへのリンクを追加しました。	2022 年 9 月 22 日
パスワードポリシー	Center for Internet Security (CIS) の最新ガイダンスを使用するように、強力なパスワー	2022 年 5 月 10 日

	ドに関する推奨事項を更新しました。	
初版発行	—	2022 年 4 月 13 日

AWS 規範的ガイダンスの用語集

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

数字

7 Rs

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

- リファクタリング/アーキテクチャの再設計 — クラウドネイティブ特徴を最大限に活用して、俊敏性、パフォーマンス、スケーラビリティを向上させ、アプリケーションを移動させ、アーキテクチャを変更します。これには、通常、オペレーティングシステムとデータベースの移植が含まれます。例: オンプレミスの Oracle データベースを Amazon Aurora PostgreSQL 互換エディションに移行する。
- リプラットフォーム (リフトアンドリシェイプ) — アプリケーションをクラウドに移行し、クラウド機能を活用するための最適化レベルを導入します。例: オンプレミスの Oracle データベースを AWS クラウドの Oracle 用 Amazon Relational Database Service (Amazon RDS) に移行します。
- 再購入 (ドロップアンドショップ) — 通常、従来のライセンスから SaaS モデルに移行して、別の製品に切り替えます。例: 顧客関係管理 (CRM) システムを Salesforce.com に移行する。
- リホスト (リフトアンドシフト) — クラウド機能を活用するための変更を加えずに、アプリケーションをクラウドに移行します。例: AWS クラウドの EC2 インスタンスでオンプレミスの Oracle データベースを Oracle に移行します。
- 再配置 (ハイパーバイザーレベルのリフトアンドシフト) – 新しいハードウェアを購入したり、アプリケーションを書き換えたり、既存の運用を変更したりすることなく、インフラストラクチャをクラウドに移行できます。この移行シナリオは、オンプレミス環境と 間の仮想マシン (VM) の互換性とワークロードの移植性 AWSをサポートする VMware Cloud on に固有のものです AWS。 AWSのVMware Cloud にインフラを移行する際、オンプレミスのデータセンターから VMware Cloud Foundation のテクノロジーを使用することができます。例: Oracle データベースをホストするハイパーバイザーを VMware Cloud on に再配置します AWS。
- 保持 (再アクセス) — アプリケーションをお客様のソース環境で保持します。これには、主要なリファクタリングを必要とするアプリケーションや、お客様がその作業を後日まで延期したい

アプリケーション、およびそれらを移行するためのビジネス上の正当性がないため、お客様が保持するレガシーアプリケーションなどがあります。

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

A

ABAC

「属性ベースのアクセスコントロール」を参照してください。

抽象化されたサービス

「マネージドサービス」を参照してください。

ACID

「原子性、一貫性、分離性、耐久性」を参照してください。

アクティブ - アクティブ移行

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

アクティブ - パッシブ移行

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

集計関数

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

AI

「人工知能」を参照してください。

AIOps

「人工知能オペレーション」を参照してください。

匿名化

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

アンチパターン

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

アプリケーションコントロール

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

アプリケーションポートフォリオ

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

人工知能 (AI)

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

AI オペレーション (AIOps)

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

非対称暗号化

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

原子性、一貫性、分離性、耐久性 (ACID)

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

属性ベースのアクセス制御 (ABAC)

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

信頼できるデータソース

最も信頼性のある情報源とされるデータのプライマリーバージョンを保存する場所。匿名化、編集、仮名化など、データを処理または変更する目的で、信頼できるデータソースから他の場所にデータをコピーすることができます。

アベイラビリティーゾーン

他のアベイラビリティーゾーンの障害から AWS リージョン 隔離され、同じリージョン内の他のアベイラビリティーゾーンへの低コストで低レイテンシーのネットワーク接続を提供する 内の別の場所。

AWS クラウド導入フレームワーク (AWS CAF)

組織がクラウドに正常に移行 AWS するための効率的で効果的な計画を立てるのに役立つ、 のガイドラインとベストプラクティスのフレームワーク。 AWS CAF は、ビジネス、人材、ガバナンス、プラットフォーム、セキュリティ、運用という 6 つの重点分野にガイダンスを編成します。ビジネス、人材、ガバナンスの観点では、ビジネススキルとプロセスに重点を置き、プラットフォーム、セキュリティ、オペレーションの視点は技術的なスキルとプロセスに焦点を当てています。例えば、人材の観点では、人事 (HR)、人材派遣機能、および人材管理を扱うステークホルダーを対象としています。この観点から、 AWS CAF は、組織がクラウド導入を成功させるための準備に役立つ、人材開発、トレーニング、コミュニケーションに関するガイダンスを提供します。詳細については、AWS CAF ウェブサイト と AWS CAF のホワイトペーパー を参照してください。

AWS ワークロード認定フレームワーク (AWS WQF)

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

B

不正なボット

個人や組織に混乱や損害を与えることを目的としたボット。

BCP

「事業継続計画」を参照してください。

動作グラフ

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

ビッグエンディアンシステム

最上位バイトを最初に格納するシステム。エンディアンネス も参照してください。

二項分類

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

ブルームフィルター

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

ブルー/グリーンデプロイ

2 つの異なる同一の環境を作成するデプロイ戦略。現在のアプリケーションバージョンは 1 つの環境 (青) で実行し、新しいアプリケーションバージョンは他の環境 (緑) で実行します。この戦略は、影響を最小限に抑えながら迅速にロールバックするのに役立ちます。

ボット

インターネット経由で自動タスクを実行し、人間のアクティビティやインタラクションをシミュレートするソフトウェアアプリケーション。インターネット上の情報のインデックスを作成するウェブクローラーなど、一部のボットは有用または有益です。悪質なボット と呼ばれる他のボッ

トの中には、個人や組織に混乱を与えたり、損害を与えたりすることを意図しているものがあります。

ボットネット

マルウェアに感染し、ボットのヘルダーまたはボットオペレーター と呼ばれる、単一関係者の管理下にあるボットのネットワーク。ボットは、ボットとその影響をスケールするための最もよく知られているメカニズムです。

ブランチ

コードリポジトリに含まれる領域。リポジトリに最初に作成するブランチは、メインブランチといいます。既存のブランチから新しいブランチを作成し、その新しいブランチで機能を開発したり、バグを修正したりできます。機能を構築するために作成するブランチは、通常、機能ブランチと呼ばれます。機能をリリースする準備ができたら、機能ブランチをメインブランチに統合します。詳細については、「ブランチについて (GitHub ドキュメント) 」を参照してください。

ブレークグラスアクセス

例外的な状況や承認されたプロセスを通じて、ユーザーが通常アクセス許可を持たない AWS アカウント にすばやくアクセスできるようになります。詳細については、 Well-Architected ガイダンスの「ブレークグラスプロシージャの実装」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低速かつ増分的なリリース。確信できたら、新しいバージョンをデプロイし、現在のバージョン全体を置き換えます。

CCoE

「Cloud Center of Excellence」を参照してください。

CDC

「データキャプチャの変更」を参照してください。

変更データキャプチャ (CDC)

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

カオスエンジニアリング

障害や破壊的なイベントを意図的に導入して、システムの耐障害性をテストします。AWS Fault Injection Service （ AWS FIS ） を使用して、 AWS ワークロードに負荷をかけてレスポンスを評価する実験を実行できます。

CI/CD

「継続的インテグレーションと継続的デリバリー」を参照してください。

分類

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

クライアント側の暗号化

ターゲットがデータ AWS のサービス を受信する前に、ローカルでデータを暗号化します。

Cloud Center of Excellence (CCoE)

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

クラウドコンピューティング

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

クラウド運用モデル

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

導入のクラウドステージ

組織が AWS クラウドに移行する際に通常実行する 4 つのフェーズ：

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

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

CMDB

「設定管理データベース」を参照してください。

コードリポジトリ

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

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

コールドキャッシュ

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

コールドデータ

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

コンピュータビジョン (CV)

機械学習を使用してデジタルイメージやビデオなどのビジュアル形式から情報を分析および抽出する AI の分野。例えば、 はオンプレミスのカメラネットワークに CV を追加するデバイス AWS Panorama を提供し、Amazon SageMaker は CV の画像処理アルゴリズムを提供します。

設定ドリフト

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

構成管理データベース (CMDB)

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

コンフォーマンスパック

コンプライアンスチェックとセキュリティチェックをカスタマイズするためにアセンブルできる AWS Config ルールと修復アクションのコレクション。YAML テンプレートを使用して、コンフォーマンスパックを AWS アカウント および リージョンに、または組織全体に 1 つのエンティティとしてデプロイできます。詳細については、 AWS Config ドキュメントの「コンフォーマンスパック」を参照してください。

継続的インテグレーションと継続的デリバリー (CI/CD)

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

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

CV

「コンピュータビジョン」を参照してください。

D

保管中のデータ

ストレージ内にあるデータなど、常に自社のネットワーク内にあるデータ。

データ分類

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

データドリフト

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

転送中のデータ

ネットワーク内 (ネットワークリソース間など) を活発に移動するデータ。

データメッシュ

一元化された管理とガバナンスにより、分散型の分散型データ所有権を提供するアーキテクチャフレームワーク。

データ最小化

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

データ境界

AWS 環境内の一連の予防ガードレール。信頼できる ID のみが、期待されるネットワークから信頼できるリソースにアクセスしていることを確認できます。詳細については、「 でのデータ境界の構築 AWS」を参照してください。

データの前処理

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

データ出所

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

データ件名

データを収集、処理している個人。

データウェアハウス

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

データベース定義言語 (DDL)

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

データベース操作言語 (DML)

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

DDL

「データベース定義言語」を参照してください。

ディープアンサンブル

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

ディープラーニング

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

defense-in-depth

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

委任管理者

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

デプロイメント

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

開発環境

「環境」を参照してください。

検出管理

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

開発バリューストリームマッピング (DVSM)

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

デジタルツイン

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

ディメンションテーブル

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

ディザスタ

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

ディザスタリカバリ (DR)

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

DML

「データベース操作言語」を参照してください。

ドメイン駆動型設計

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

DR

「ディザスタリカバリ」を参照してください。

ドリフト検出

ベースライン設定からの偏差の追跡。例えば、 AWS CloudFormation を使用してシステムリソース のドリフトを検出したり、 を使用して AWS Control Tower ガバナンス要件への準拠に影響を与える可能性のあるランディングゾーンの変更を検出したりできます。

DVSM

「開発値ストリームマッピング」を参照してください。

E

EDA

「探索的データ分析」を参照してください。

エッジコンピューティング

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

暗号化

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

暗号化キー

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

エンディアン

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

エンドポイント

「サービスエンドポイント」を参照してください。

エンドポイントサービス

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

エンタープライズリソースプランニング (ERP)

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

エンベロープ暗号化

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

環境

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

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

エピック

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

ERP

「エンタープライズリソース計画」を参照してください。

探索的データ分析 (EDA)

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

F

ファクトテーブル

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

フェイルファスト

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

障害分離境界

では AWS クラウド、障害の影響を制限し、ワークロードの耐障害性を向上させるアベイラビリティーゾーン AWS リージョン、コントロールプレーン、データプレーンなどの境界です。詳細については、AWS 「障害分離境界」を参照してください。

機能ブランチ

「ブランチ」を参照してください。

特徴量

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

特徴量重要度

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

機能変換

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

FGAC

「きめ細かなアクセスコントロール」を参照してください。

きめ細かなアクセス制御 (FGAC)

複数の条件を使用してアクセス要求を許可または拒否すること。

フラッシュカット移行

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

G

Geo Blocking

「地理的制限」を参照してください。

地理的制限 (ジオブロッキング)

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

Gitflow ワークフロー

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

グリーンフィールド戦略

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

ガードレール

組織単位 (OU) 全般のリソース、ポリシー、コンプライアンスを管理するのに役立つ概略的なルール。予防ガードレールは、コンプライアンス基準に一致するようにポリシーを実施します。これらは、サービスコントロールポリシーと IAM アクセス許可の境界を使用して実装

されます。検出ガードレールは、ポリシー違反やコンプライアンス上の問題を検出し、修復のためのアラートを発信します。これらは、 AWS Config、、Amazon AWS Security Hub、GuardDuty、Amazon Inspector AWS Trusted Advisor、およびカスタム AWS Lambda チェックを使用して実装されます。

H

HA

「高可用性」を参照してください。

異種混在データベースの移行

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

ハイアベイラビリティ (HA)

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

ヒストリアンのモダナイゼーション

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

同種データベースの移行

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

ホットデータ

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

ホットフィックス

本番環境の重大な問題を修正するために緊急で配布されるプログラム。緊急性のため、通常、修正は一般的な DevOps リリースワークフローの外で行われます。

ハイパーケア期間

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

I

IaC

「Infrastructure as Code」を参照してください。

ID ベースのポリシー

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

アイドル状態のアプリケーション

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

IIoT

「産業モノのインターネット」を参照してください。

イミュータブルインフラストラクチャ

既存のインフラストラクチャを更新、パッチ適用、または変更するのではなく、本番ワークロード用の新しいインフラストラクチャをデプロイするモデル。イミュータブルなインフラストラクチャは、本質的にミュータブルなインフラストラクチャ よりも一貫性、信頼性、予測性が高くなります。詳細については、 AWS Well-Architected フレームワークの「変更不可能なインフラストラクチャを使用したデプロイ」のベストプラクティスを参照してください。

インバウンド (受信) VPC

AWS マルチアカウントアーキテクチャでは、アプリケーション外からのネットワーク接続を受け入れ、検査し、ルーティングする VPC。AWS Security Reference Architecture では、アプリ

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

増分移行

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

インダストリー 4.0

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

インフラストラクチャ

アプリケーションの環境に含まれるすべてのリソースとアセット。

Infrastructure as Code (IaC)

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

産業分野における IoT (IIoT)

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

インスペクション VPC

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

IoT

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

解釈可能性

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

IoT

「モノのインターネット」を参照してください。

IT 情報ライブラリ (ITIL)

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

IT サービス管理 (ITSM)

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

ITIL

「IT 情報ライブラリ」を参照してください。

ITSM

「IT サービス管理」を参照してください。

L

ラベルベースアクセス制御 (LBAC)

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

ランディングゾーン

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

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

大規模な移行

300 台以上のサーバの移行。

LBAC

「ラベルベースのアクセスコントロール」を参照してください。

最小特権

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

リフトアンドシフト

「7 R」を参照してください。

リトルエンディアンシステム

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

下位環境

「環境」を参照してください。

M

機械学習 (ML)

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

メインブランチ

「ブランチ」を参照してください。

マルウェア

コンピュータのセキュリティまたはプライバシーを侵害するように設計されているソフトウェア。マルウェアは、コンピュータシステムの中断、機密情報の漏洩、不正アクセスにつながる

可能性があります。マルウェアの例としては、ウイルス、ワーム、ランサムウェア、トロイの木馬、スパイウェア、キーロガーなどがあります。

マネージドサービス

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

製造実行システム (MES)

生産プロセスを追跡、モニタリング、文書化、制御するためのソフトウェアシステム。このソフトウェアシステムは、加工品を現場の完成製品に変換します。

MAP

「移行促進プログラム」を参照してください。

メカニズム

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

メンバーアカウント

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

MES

「製造実行システム」を参照してください。

メッセージキューイングテレメトリトランスポート (MQTT)

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

マイクロサービス

明確に定義された API を介して通信し、通常は小規模な自己完結型のチームが所有する、小規模で独立したサービスです。例えば、保険システムには、販売やマーケティングなどのビジネス機能、または購買、請求、分析などのサブドメインにマッピングするマイクロサービスが含まれる場合があります。マイクロサービスの利点には、俊敏性、柔軟なスケーリング、容易なデプロ

イ、再利用可能なコード、回復力などがあります。詳細については、AWS 「サーバーレスサービスを使用したマイクロサービスの統合」を参照してください。

マイクロサービスアーキテクチャ

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

Migration Acceleration Program (MAP)

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

大規模な移行

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

移行ファクトリー

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

移行メタデータ

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

移行パターン

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

Migration Portfolio Assessment (MPA)

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

移行準備状況評価 (MRA)

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

移行戦略

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

ML

「機械学習」を参照してください。

モダナイゼーション

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

モダナイゼーション準備状況評価

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

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

モノリシックアプリケーション (モノリス)

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

MPA

「移行ポートフォリオ評価」を参照してください。

MQTT

「Message Queuing Telemetry Transport」を参照してください。

多クラス分類

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

変更可能なインフラストラクチャ

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

O

OAC

「オリジンアクセスコントロール」を参照してください。

OAI

「オリジンアクセスアイデンティティ」を参照してください。

OCM

「組織変更管理」を参照してください。

オフライン移行

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

OI

「 オペレーション統合」を参照してください。

OLA

「運用レベルの契約」を参照してください。

オンライン移行

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

OPC-UA

「Open Process Communications - Unified Architecture」を参照してください。

オープンプロセス通信 - 統合アーキテクチャ (OPC-UA)

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

オペレーショナルレベルアグリーメント (OLA)

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

運用準備状況レビュー (ORR)

インシデントや潜在的な障害の理解、評価、防止、または範囲の縮小に役立つ質問および関連するベストプラクティスのチェックリスト。詳細については、 AWS Well-Architected フレームワークの「運用準備状況レビュー (ORR)」を参照してください。

運用テクノロジー (OT)

産業運用、機器、インフラストラクチャを制御するために物理環境と連携するハードウェアおよびソフトウェアシステム。製造では、OT と情報技術 (IT) システムの統合が、Industry 4.0 トランスフォーメーションの主要な焦点です。

オペレーション統合 (OI)

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

組織の証跡

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

組織変更管理 (OCM)

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

オリジンアクセスコントロール (OAC)

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

オリジンアクセスアイデンティティ (OAI)

では CloudFront、Amazon S3 コンテンツを保護するためのアクセスを制限するオプションです。OAI を使用する場合、 は Amazon S3 が認証できるプリンシパル CloudFront を作成します。認証されたプリンシパルは、特定の CloudFront ディストリビューションを介してのみ S3 バケット内のコンテンツにアクセスできます。OACも併せて参照してください。OAC では、より詳細な、強化されたアクセスコントロールが可能です。

ORR

「運用準備状況レビュー」を参照してください。

OT

「運用技術」を参照してください。

アウトバウンド (送信) VPC

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

P

アクセス許可の境界

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

個人を特定できる情報 (PII)

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

PII

個人を特定できる情報を参照してください。

プレイブック

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

PLC

「プログラム可能なロジックコントローラー」を参照してください。

PLM

「製品ライフサイクル管理」を参照してください。

ポリシー

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

多言語の永続性

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

ポートフォリオ評価

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

述語

`true` または を返すクエリ条件。`false`通常は `WHERE`句にあります。

述語のプッシュダウン

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

予防的コントロール

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

プリンシパル

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

プライバシーバイデザイン

エンジニアリングプロセス全体を通してプライバシーを考慮に入れたシステムエンジニアリングのアプローチ。

プライベートホストゾーン

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

プロアクティブコントロール

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

製品ライフサイクル管理 (PLM)

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

本番環境

「環境」を参照してください。

プログラミング可能ロジックコントローラー (NAL)

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

仮名化

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

パブリッシュ/サブスクライブ (pub/sub)

マイクロサービス間の非同期通信を可能にするパターン。スケーラビリティと応答性を向上させます。例えば、マイクロサービスベースの MES では、マイクロサービスは他のマイクロサービスがサブスクライブできるチャネルにイベントメッセージを発行できます。システムは、公開サービスを変更せずに新しいマイクロサービスを追加できます。

Q

クエリプラン

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

クエリプランのリグレッション

データベースサービスのオプティマイザーが、データベース環境に特定の変更が加えられる前に選択されたプランよりも最適性の低いプランを選択すること。これは、統計、制限事項、環境設

定、クエリパラメータのバインディングの変更、およびデータベースエンジンの更新などが原因である可能性があります。

R

RACI マトリックス

責任、説明責任、相談、情報 (RACI) を参照してください。

ランサムウェア

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

RASCI マトリックス

責任、説明責任、相談、情報 (RACI) を参照してください。

RCAC

「行と列のアクセスコントロール」を参照してください。

リードレプリカ

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

再構築

「7 Rs」を参照してください。

目標復旧時点 (RPO)

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

目標復旧時間 (RTO)

サービスの中断から復旧までの最大許容遅延時間。

リファクタリング

「7 Rs」を参照してください。

リージョン

地理的エリア内の AWS リソースのコレクション。各 AWS リージョン は、耐障害性、安定性、耐障害性を提供するために、他の とは分離され、独立しています。詳細については、AWS リージョン 「 を使用できるアカウントを指定する」を参照してください。

回帰

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

リホスト

「7 R」を参照してください。

リリース

デプロイプロセスで、変更を本番環境に昇格させること。

再配置

「7 R」を参照してください。

プラットフォーム変更

「7 R」を参照してください。

再購入

「7 R」を参照してください。

回復性

中断に耐えたり、中断から回復したりするアプリケーションの機能。で障害耐性を計画する場合、高可用性とディザスタリカバリが一般的な考慮事項です AWS クラウド。詳細については、AWS クラウド 「レジリエンス」を参照してください。

リソースベースのポリシー

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

実行責任者、説明責任者、協業先、報告先 (RACI) に基づくマトリックス

移行活動とクラウド運用に関わるすべての関係者の役割と責任を定義したマトリックス。マトリックスの名前は、マトリックスで定義されている責任の種類、すなわち責任 (R) 、説明責任

(A) 、協議 (C) 、情報提供 (I) に由来します。サポート (S) タイプはオプションです。サポートを含めると、そのマトリックスは RASCI マトリックスと呼ばれ、サポートを除外すると RACI マトリックスと呼ばれます。

レスポンシブコントロール

有害事象やセキュリティベースラインからの逸脱について、修復を促すように設計されたセキュリティコントロール。詳細については、Implementing security controls on AWSのResponsive controlsを参照してください。

保持

「7 R」を参照してください。

廃止

「7 R」を参照してください。

ローテーション

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

行と列のアクセス制御 (RCAC)

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

RPO

「目標復旧時点」を参照してください。

RTO

「目標復旧時間」を参照してください。

ランブック

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

S

SAML 2.0

多くの ID プロバイダー (IdPs) が使用するオープンスタンダード。この機能により、フェデレーティッドシングルサインオン (SSO) が有効になるため、ユーザーは にログイン AWS

Management Console したり、組織内のすべてのユーザーを IAM で作成しなくても AWS API オペレーションを呼び出すことができます。SAML 2.0 ベースのフェデレーションの詳細については、IAM ドキュメントのSAML 2.0 ベースのフェデレーションについてを参照してください。

SCADA

「監視コントロールとデータ収集」を参照してください。

SCP

「サービスコントロールポリシー」を参照してください。

シークレット

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

セキュリティコントロール

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

セキュリティ強化

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

Security Information and Event Management (SIEM) システム

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

セキュリティレスポンスの自動化

セキュリティイベントに自動的に応答または修正するように設計された、事前定義されたプログラムされたアクション。これらのオートメーションは、セキュリティのベストプラクティスの実装に役立つ検出的または応答的な AWS セキュリティコントロールとして機能します。自動レスポンスアクションの例としては、VPC セキュリティグループの変更、Amazon EC2 インスタンスへのパッチ適用、認証情報のローテーションなどがあります。

サーバー側の暗号化

送信先にあるデータの、それを受け取る AWS のサービス による暗号化。

サービスコントロールポリシー (SCP)

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

サービスエンドポイント

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

サービスレベルアグリーメント (SLA)

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

サービスレベルインジケータ (SLI)

エラー率、可用性、スループットなど、サービスのパフォーマンス側面の測定。

サービスレベルの目標 (SLO)

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

責任共有モデル

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

SIEM

「セキュリティ情報とイベント管理システム」を参照してください。

単一障害点 (SPOF)

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

SLA

「サービスレベルアグリーメント」を参照してください。

SLI

「サービスレベルインジケータ」を参照してください。

SLO

「サービスレベルの目標」を参照してください。

split-and-seed モデル

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

SPOF

単一障害点 を参照してください。

star スキーマ

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

strangler fig パターン

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

サブネット

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

監視統制とデータ収集 (SCADA)

製造では、ハードウェアとソフトウェアを使用して物理アセットと生産オペレーションをモニタリングするシステム。

対称暗号化

データの暗号化と復号に同じキーを使用する暗号化のアルゴリズム。

合成テスト

ユーザーインタラクションをシミュレートして潜在的な問題を検出したり、パフォーマンスをモニタリングしたりする方法でシステムをテストします。Amazon CloudWatch Synthetics を使用してこれらのテストを作成できます。

T

タグ

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

ターゲット変数

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

タスクリスト

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

テスト環境

「環境」を参照してください。

トレーニング

お客様の機械学習モデルに学習するデータを提供すること。トレーニングデータには正しい答えが含まれている必要があります。学習アルゴリズムは入力データ属性をターゲット (お客様が予測したい答え) にマッピングするトレーニングデータのパターンを検出します。これらのパター

ンをキャプチャする機械学習モデルを出力します。そして、お客様が機械学習モデルを使用して、ターゲットがわからない新しいデータでターゲットを予測できます。

トランジットゲートウェイ

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

トランクベースのワークフロー

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

信頼されたアクセス

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

チューニング

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

ツーピザチーム

2 つのピザを食べることができる小さな DevOps チーム。ツーピザチームの規模では、ソフトウェア開発におけるコラボレーションに最適な機会が確保されます。

U

不確実性

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

未分化なタスク

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

上位環境

「環境」を参照してください。

V

バキューミング

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

バージョンコントロール

リポジトリ内のソースコードへの変更など、変更を追跡するプロセスとツール。

VPC ピアリング

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

脆弱性

システムのセキュリティを脅かすソフトウェアまたはハードウェアの欠陥。

W

ウォームキャッシュ

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

ウォームデータ

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

ウィンドウ関数

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

ワークロード

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

ワークストリーム

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

WORM

「書き込み 1 回」を参照し、多くの を読み取ります。

WQF

「AWS ワークロード認定フレームワーク」を参照してください。

Write Once, Read Many (WORM)

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

Z

ゼロデイエクスプロイト

ゼロデイ脆弱性 を利用する攻撃、通常はマルウェア。

ゼロデイ脆弱性

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

ゾンビアプリケーション

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

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