



を使用してエンタープライズブループリントファクトリーを構築する AWS
Service Catalog

AWS 規範ガイドンス



AWS 規範ガイド: を使用してエンタープライズブループリントファクトリーを構築する AWS Service Catalog

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

序章	1
ビジネスの概要	1
ソリューションの概要	1
対象者	2
目的	2
アーキテクチャ	4
コンポーネント	6
製品リポジトリ	6
設定リポジトリ	6
設定ファイル	7
設定パイプライン	9
リリースパイプライン	11
設計図のライフサイクル	14
設計図の作成	14
設計図の更新	14
設計図の削除	15
設定	17
前提条件	17
ベストプラクティス	18
リポジトリの作成	18
ファクトリをセットアップする	19
ファクトリを削除する	27
ファクトリの使用	29
前提条件	29
ブループリントを作成する	29
ブループリントを更新する	32
ブループリントを削除する	33
トラブルシューティング	34
関連リソース	36
AWS ドキュメント	36
AWS ブログ投稿	36
寄稿者	37
オーサリング	37
レビュー	37

テクニカルライティング	37
ドキュメント履歴	38
用語集	39
#	39
A	40
B	43
C	45
D	48
E	52
F	54
G	55
H	57
I	58
L	60
M	61
O	65
P	68
Q	71
R	71
S	74
T	78
U	79
V	80
W	80
Z	81
.....	lxxxii

を使用してエンタープライズブループリントファクトリーを構築する AWS Service Catalog

アマゾン ウェブ サービス ([寄稿者](#))

2024 年 10 月 ([ドキュメント履歴](#))

ビジネスの概要

多くの企業は、クラウドでワークロードをスケーリングする際に課題に直面しています。これらの組織的な課題には、次のようなものがあります。

- 複数の で大規模に再利用できる infrastructure as code (IaC) テンプレートの作成 AWS のサービス
- IaC テンプレートがセキュリティのベストプラクティスに従っていることを検証する
- 開発者の生産性を大幅に低下させ、市場投入までの時間を短縮できる、[差別化されていないタスク](#)や反復的なタスクを減らす
- IaC テンプレートの整合性の確立
- リソース使用率、特にセキュリティチームを削減して、繰り返し行われる手動レビューを回避する

セキュリティのベストプラクティスに従う IaC テンプレートを作成するには、ガードレールとセキュリティコントロールを確立する必要があります。従来、クラウドプラットフォームチームまたはセキュリティチームは、各 IaC テンプレートのコードを手動でレビューしていました。または、開発者は IaC テンプレートを非本番環境にデプロイし、[検出コントロール](#)を使用してセキュリティ上の問題を見つけます。これらのアプローチはいずれも、反復的なフィードバックサイクルを必要とし、開発プロセスを遅らせ、手動エンジニアリングの労力を増やします。

その結果、多くの企業は IaC テンプレートの作成、検証、リリースを合理化したいと考えています。また、リリース後にこれらのテンプレートを管理および管理する手段も必要です。適切な管理とガバナンスのメカニズムは、テンプレートを更新し、開発者が最新バージョンにアクセスできることを確認するのに役立ちます。これらのメカニズムは、組織全体でのテンプレートの使用を監督および監査するのに役立ちます。

ソリューションの概要

このガイドでは、組織全体のInfrastructure as Code (IaC) テンプレートの作成、検証、公開、配布、消費を合理化するのに役立つ Enterprise Blueprint Factory ソリューションについて説明しま

す。これらの IaC テンプレートはブループリントとも呼ばれます。このソリューションは、AWS CloudFormation [テンプレート](#) または AWS Cloud Development Kit (AWS CDK) [コンストラクト](#) であるブループリントファイルをサポートします。

Enterprise Blueprint Factory は、設定駆動型のアプローチを使用して、ブループリントの共有、公開、配布を自動化します。開発者は、設計図を製品リポジトリに追加し、設計図情報を設定ファイルに追加します。これにより、継続的インテグレーションと継続的デリバリー (CI/CD) リリースパイプラインが自動的に開始されます。このパイプラインは、ブループリントが AWS セキュリティのベストプラクティスに従っていることを検証します。これにより、組織の設計図が設計上安全であることが保証されます。設計によるセキュリティは、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です。

Enterprise Blueprint Factory は、でブループリントを製品としてリリースします [AWS Service Catalog](#)。Service Catalog を使用すると、エンドユーザーは指定した承認済みブループリントをすばやくデプロイできます。Service Catalog は、管理者が [きめ細かなアクセスコントロール](#) を定義し、ブループリントの使用を監督できるように、管理およびガバナンス機能を提供するように設計されています。

対象者

[Enterprise Blueprint Factory アーキテクチャ](#) セクションは、アーキテクト、マネージャー、テクニカルリードがこのソリューションを評価し、それが組織に適しているかどうかを判断するのに役立ちます。このセクションでは、設計図とは何か、Service Catalog を使用して管理する方法、Enterprise Blueprint Factory のアーキテクチャについて説明します。

[「エンタープライズブループリントファクトリーのセットアップ」](#) セクションは、DevOps エンジニアがエンタープライズブループリントファクトリーを環境にデプロイするのに役立ちます AWS。これには、必要なリポジトリと設定パイプラインを設定する詳細な手順が含まれています。

[「エンタープライズブループリントファクトリーの使用」](#) セクションは、ブループリント開発者が環境でブループリントを作成、更新、または削除するのに役立ちます。ライフサイクル全体でブループリントを管理するための詳細な手順を示します。ブループリントを作成するには、開発者は CloudFormation テンプレートなどの IaC テンプレートを作成する方法を理解する必要があります。このガイドには、これらのブループリントを定義する方法に関する情報や手順は含まれていません。

目的

Enterprise Blueprint Factory は、組織が次の利点を達成するのに役立ちます。

- ブループリントが AWS セキュリティのベストプラクティスに従っていることを検証する
- ブループリントのリリースと検証プロセスを自動化および標準化する
- 実行する必要がある手動タスクの数を減らすことで、開発者の生産性を向上させる
- きめ細かなアクセスコントロールを使用して、エンドユーザーがアクセスできるブループリントを決定する
- バージョン管理を使用してブループリントの更新を管理し、エンドユーザーと共有する
- エンドユーザーがブループリントの検出と起動をセルフサービスできるようにする
- 組織全体でのブループリントの使用をモニタリングおよび監査する

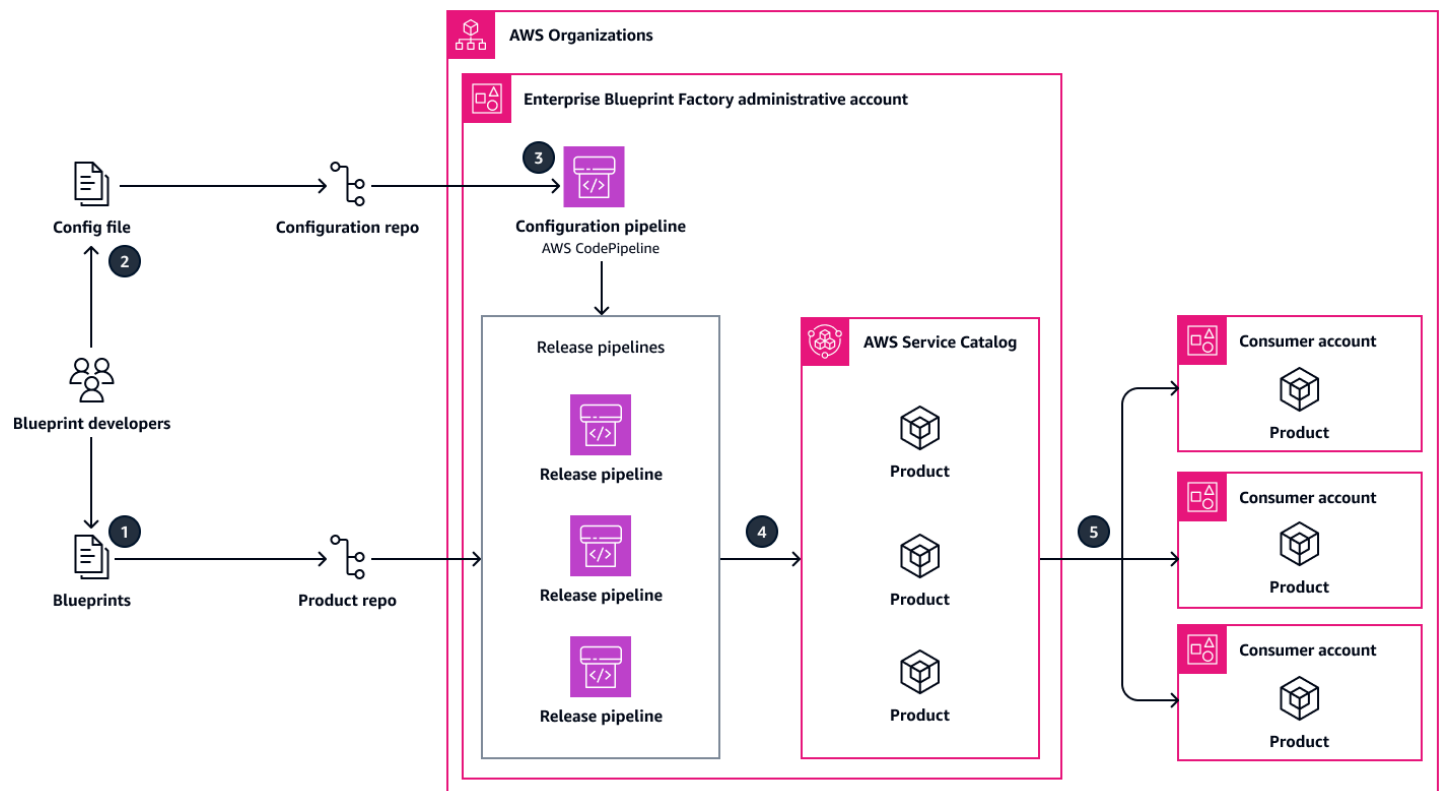
Enterprise Blueprint Factory アーキテクチャ

ブループリントとも呼ばれるInfrastructure as Code (IaC) テンプレートは、クラウドリソースのプロビジョニングと管理に役立つ設定ファイルです。ブループリントは 1 つのリソースをプロビジョニングしたり、複雑な多層アプリケーションのアーキテクチャをプロビジョニングしたりできます。IaC は、インフラストラクチャ管理の一元化、リソースの標準化、迅速なスケーリングを支援するように設計されています。

Enterprise Blueprint Factory は、組織全体のブループリントの作成、検証、公開、配布、消費を合理化するのに役立ちます。このセクションでは、アーキテクチャの概要を提供するだけでなく、ソリューションの[アーキテクチャコンポーネント](#)と[ブループリントのライフサイクル](#)についても確認します。

Enterprise Blueprint Factory を使用してブループリントをリリースすると、ブループリントは [製品](#) になります [AWS Service Catalog](#)。製品を 1 つ以上の[ポートフォリオ](#)に収集し、エンドユーザーがそのポートフォリオ内の製品にアクセスできるようにするアクセス許可を付与します。[ポートフォリオ共有](#)を使用して、別の Service Catalog 管理者が製品をエンドユーザー AWS アカウント に配布することを許可できます。

次の図は、Enterprise Blueprint Factory アーキテクチャの概要を示しています。このワークフローは、設計図を Service Catalog の製品としてリリースします。また、ポートフォリオとポートフォリオ共有を作成または更新して、ブループリントをターゲットエンドユーザーが利用できるようにします。



この図は、次のワークフローを示しています。

- 開発者はブループリントを構築します。製品リポジトリに機能ブランチを作成し、ブループリントをブランチにプッシュしてから、プルリクエストを作成します。ブループリント管理チームとセキュリティチームは、プルリクエストを確認して、ブループリントが組織およびセキュリティ要件を満たしていることを確認します。これらのチームはプルリクエストを承認します。開発者は機能ブランチをメインブランチにマージします。詳細については、このガイドの「[製品リポジトリ](#)」を参照してください。
- 開発者は、設定リポジトリにある設定ファイルにブループリント情報を追加または更新します。詳細については、このガイドの「[設定リポジトリ](#)」と「[設定ファイル](#)」を参照してください。
- 設定ファイルの更新により、設定パイプラインが呼び出されます。このパイプラインは、[AWS CodePipeline](#)および[AWS CodeBuild](#)プロジェクトを使用して、Service Catalog ポートフォリオとポートフォリオ共有を作成または更新します。また、ブループリントのリリースパイプラインも作成します。詳細については、このガイドの「[設定パイプライン](#)」を参照してください。
- リリースパイプラインは、ブループリントに対してさまざまなセキュリティチェックを実行します。ブループリントが合格すると、リリースパイプラインはブループリントを Service Catalog の製品としてデプロイします。詳細については、このガイドの「[リリースパイプライン](#)」を参照してください。

5. ポートフォリオとポートフォリオ共有を通じて製品にアクセスすることで、エンドユーザーはターゲットコンシューマーアカウントにブループリントをデプロイします。

Enterprise Blueprint Factory コンポーネント

Enterprise Blueprint Factory は、次のコンポーネントで構成されています。

- [製品リポジトリ](#) – ブループリントを保存するリポジトリ。
- [設定リポジトリ](#) – AWS Service Catalog ポートフォリオと製品を定義する設定ファイルを保存するリポジトリ。
- [設定ファイル](#) – 使用可能なブループリント、使用できるユーザー、使用方法を定義する設定ファイル。
- [設定パイプライン](#) – Service Catalog ポートフォリオとポートフォリオ共有をセットアップし、各製品のリリースパイプラインを作成する DevOps CI/CD パイプライン。
- [リリースパイプライン](#) – ブループリントを Service Catalog 製品としてリリースする DevOps CI/CD パイプライン。

クラウドインフラストラクチャチームは、通常、エンタープライズブループリントファクトリー全体を管理します。これは、各ブループリントを承認する必要があるためです。ただし、DevOps コードチームは通常、設定パイプラインとリリースパイプラインを担当します。新しいブループリントをリリースするために、デベロッパーは製品リポジトリ、設定リポジトリ、および設定ファイルとのみやり取りします。

製品リポジトリ

製品リポジトリは、組織が承認する設計図を保存する一元的な場所です。設計図管理チームとセキュリティチームは、このリポジトリへのプルリクエストを確認して、各設計図が組織およびセキュリティ要件を満たしていることを確認します。このガイドでは、リポジトリに GitHub を使用しますが、別の方法を使用することもできます。

設定リポジトリ

設定リポジトリ (設定リポジトリ) は、組織が Enterprise Blueprint Factory を通じてリリースされた Service Catalog ポートフォリオと製品の設定ファイルを保存する場所です。このガイドでは、リポジトリに GitHub を使用しますが、別の方法を使用することもできます。

設定ファイル

Enterprise Blueprint Factory 設定ファイル (設定ファイル) は、設計図管理チームが所有する設定リポジトリに保存されます。このファイルの名前は `bp_config.yml` です。開発者がこのファイルを更新すると、ブループリント管理チームが変更を確認します。変更をメインブランチにマージすると、設定パイプラインが開始されます。設定ファイルは、Enterprise Blueprint Factory を通じて管理されるすべてのブループリントの公開、共有、配布を調整します。

設定ファイルは、`portfolios` との 2 つのメインオブジェクトで構成される YAML ファイルです `products`。以下は、サンプル設定ファイルの例です。

```
portfolios:
  - portfolio_name: blueprint-portfolio
    owner: Blueprint-team
    provider_name: AWS
    description: "Blueprint portfolio"
    portfolio_access_role:
      - arn:aws:iam::123456789012:role/examplerole
      - arn:aws:iam::123456789012:user/exampleuser
    share_to_ou:
      - org_id: "o-exampleOrgID"
    stack_tags:
      DataClassification: Confidential
      Organization: AWS
products:
  - name: BP-S3-Product
    description: "Blueprint for BP-S3 product"
    product_config_file: 'BP-S3/product_config.json'
    owner: Blueprint-team
    stack_tags:
      DataClassification: Confidential
      Organization: AWS
    portfolio_associations:
      - blueprint-portfolio
    launch_constraint_role: arn:aws:iam::123456789012:role/examplelaunchrole
```

`portfolios` オブジェクトで、ターゲット Service Catalog ポートフォリオを定義します。ポートフォリオごとに、次の属性を指定します。

- `portfolio_name` はポートフォリオの名前です。この属性は必須です。
- `owner` は、ポートフォリオを所有するチームの名前です。この属性はオプションです。

- `provider_name` は、ポートフォリオを管理するチームまたは組織の名前です。デフォルト値は AWS です。この属性は必須です。
- `description` はポートフォリオの簡単な説明です。この属性はオプションです。
- `portfolio_access_roles` は、ポートフォリオとその関連製品へのアクセスが許可されている AWS Identity and Access Management (IAM) [ID](#) (ユーザー、ロール、またはグループ) です。この属性はオプションです。
- `share_to_ou` は、ポートフォリオが共有 AWS Organizations されているの [組織単位](#) (OU) です。エンドユーザーは、ターゲット OU のメンバー AWS アカウント である にこのポートフォリオの製品をデプロイできます。この属性はオプションです。
- `stack_tags` は、ポートフォリオに適用される [タグ](#) です。この属性はオプションです。

`products` オブジェクトでは、Service Catalog で製品としてリリースする各ブループリントを定義します。製品ごとに、次の属性を指定します。

- `name` は、Service Catalog の製品の名前です。この属性は必須です。
- `description` は、製品の簡単な説明です。この属性は必須です。
- `product_config_file` は、製品リポジトリに保存されているブループリント製品設定ファイルの名前です。この属性は必須です。
- `owner` は、製品を所有するチームの名前です。この属性は必須です。
- `stack_tags` は、製品に適用されるタグです。この属性はオプションです。
- `portfolio_associations` は、製品を含むターゲットポートフォリオです。この属性はオプションです。

Note

Enterprise Blueprint Factory で管理されているポートフォリオにのみ製品を追加することをお勧めします。Enterprise Blueprint Factory で管理されていないポートフォリオに製品を追加する場合は、ユーザーの IAM ポリシーで [AssociateProductWithPortfolio](#) アクションを許可する必要があります。ただし、セキュリティのベストプラクティスとして、このアクションは Enterprise Blueprint Factory 設定パイプラインにのみ許可することをお勧めします。

- `launch_constraint_role` は、エンドユーザーが製品を起動するときに Service Catalog が引き受ける起動 [ロール](#) です。この属性は必須です。

設定パイプライン

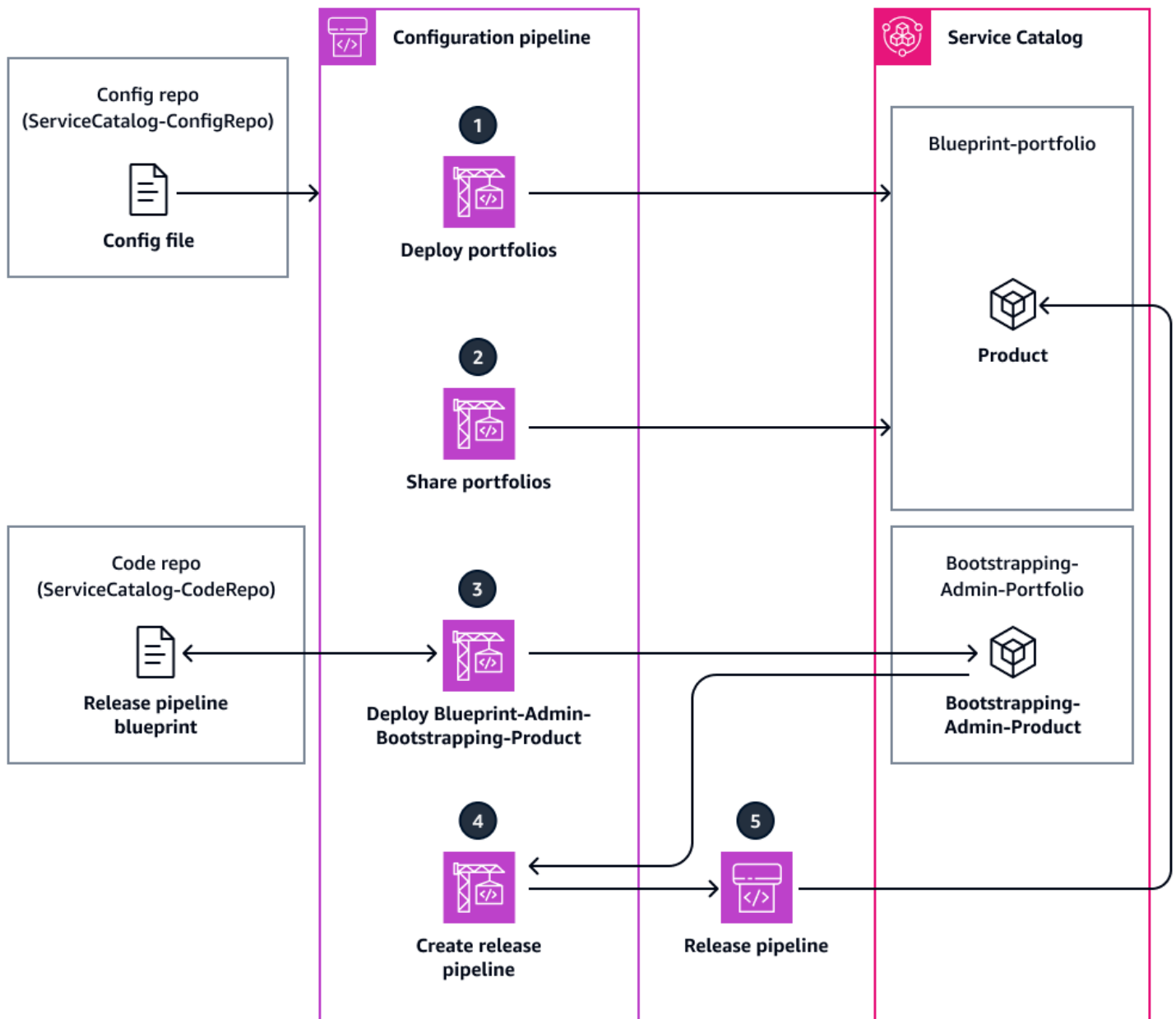
設定パイプライン (設定パイプライン) は、Service Catalog ポートフォリオとポートフォリオ共有の設定を自動化します。また、各製品のリリースパイプラインも作成されます。このパイプラインは [AWS CodePipeline](#) リソースです。設定ファイルを更新すると、設定パイプラインが呼び出されます。

設定パイプラインを初めて呼び出すと、設定ファイルで定義されていない 2 つの追加のポートフォリオが作成されます。

- Blueprint-portfolio – Enterprise Blueprint Factory を通じてデプロイするすべての製品が、このポートフォリオに追加されます。このポートフォリオは、設定ファイルで指定した IAM プリンシパルと組織単位で使用できます。
- Bootstrapping-Admin-Portfolio – Bootstrapping-Admin-Product製品はこのポートフォリオに関連付けられています。この製品は、リリースパイプライン用の CloudFormation テンプレートです。ブループリント管理チームのみがこのポートフォリオにアクセスして、管理製品を管理できるようにします。

設定パイプラインステージ

次の図は、設定パイプラインのステージと、パイプラインがやり取りするリソースを示しています。パイプラインの各ステージは [AWS CodeBuild](#) プロジェクトです。



設定パイプラインのステージは次のとおりです。

1. ポートフォリオのデプロイ – 設定パイプラインは、設定ファイルに追加されたポートフォリオをデプロイするか、設定ファイルから削除されたポートフォリオを削除します。ポートフォリオに変更がない場合、パイプラインはこのステージをスキップします。
2. ポートフォリオの共有 – 設定パイプラインは、ポートフォリオをターゲット組織単位 (OUs。ポートフォリオ共有に変更がない場合、パイプラインはこのステージをスキップします。
3. Blueprint-Admin-Bootstrapping-Product – 設定パイプラインはServiceCatalog-CodeRepo、リポジトリからbp-pipeline ブループリントを取得し、として Service Catalog にデプロイしま

す Bootstrapping-Admin-Product。この製品は、リリースパイプラインの作成に使用される CloudFormation テンプレートです。このテンプレートを Service Catalog 製品としてデプロイすると、バージョン管理の維持に役立ちます。bp-pipeline ブループリントに変更がない場合、パイプラインはこのステージをスキップします。

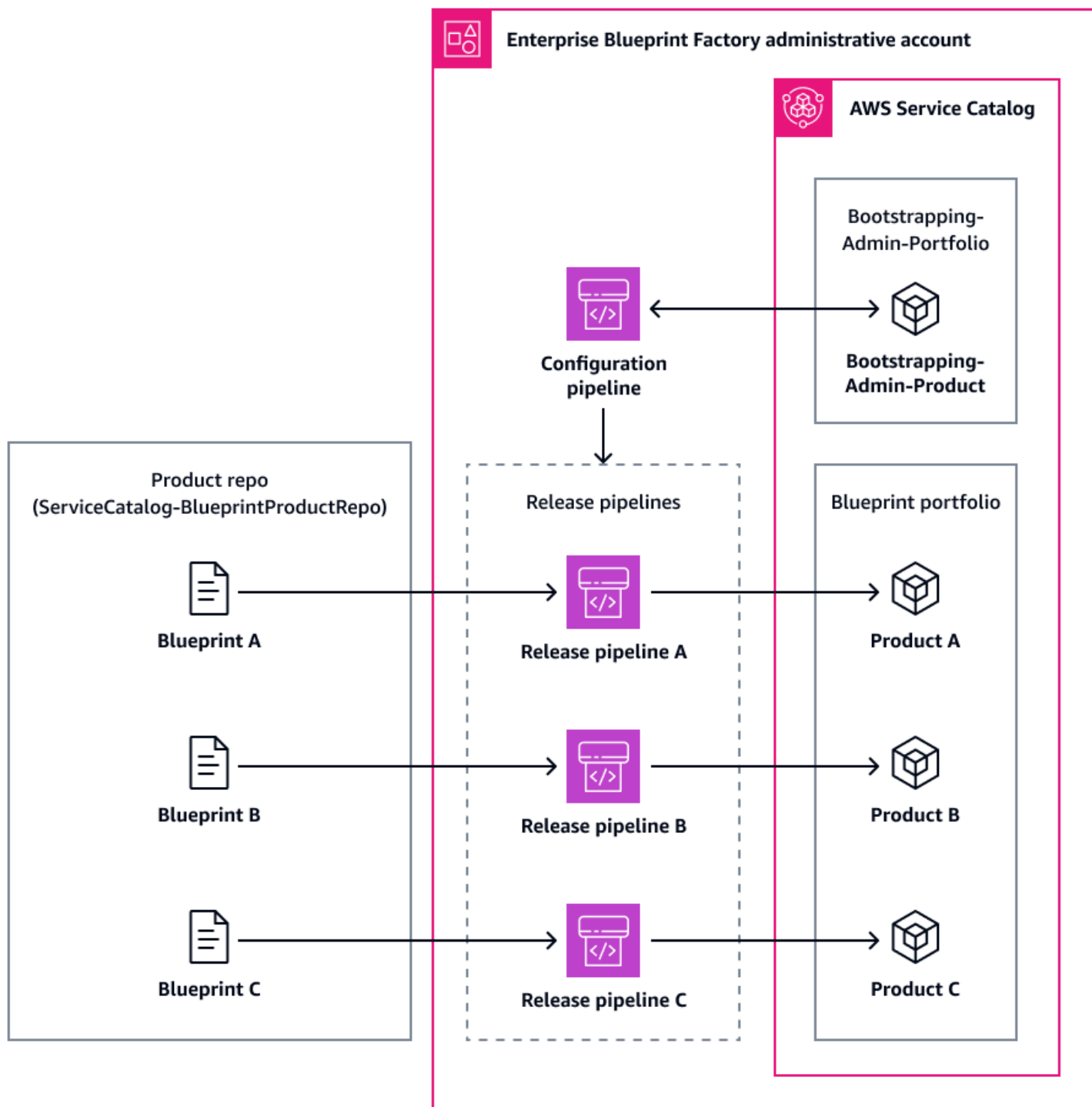
4. リリースパイプラインの作成 – 設定ファイルの製品属性に基づいて、設定パイプラインはスタックパラメータを準備し、製品のリリースパイプラインを作成する CloudFormation スタックを起動します。詳細については、このガイドの「[リリースパイプライン](#)」を参照してください。
5. 製品のデプロイ – リリースパイプラインは、設計図を Service Catalog 製品としてデプロイし、ターゲットポートフォリオに関連付けます。エンドユーザーは、ターゲット OU のメンバー AWS アカウントである製品を にデプロイできるようになりました。

リリースパイプライン

リリースパイプラインは、Service Catalog 製品としてのブループリントのリリースを自動化します。このパイプラインは [AWS CodePipeline](#) リソースです。組織が新しいブループリントをリリースする場合、開発者は IaC テンプレートとその製品設定ファイルを製品リポジトリにアップロードします。製品の詳細を設定ファイルに追加すると、設定パイプラインがトリガーされます。設定パイプラインは、このブループリントのリリースパイプラインを作成します。ブループリントの後続の更新により、このリリースパイプラインがトリガーされ、Service Catalog の製品が新しいバージョンで更新されます。

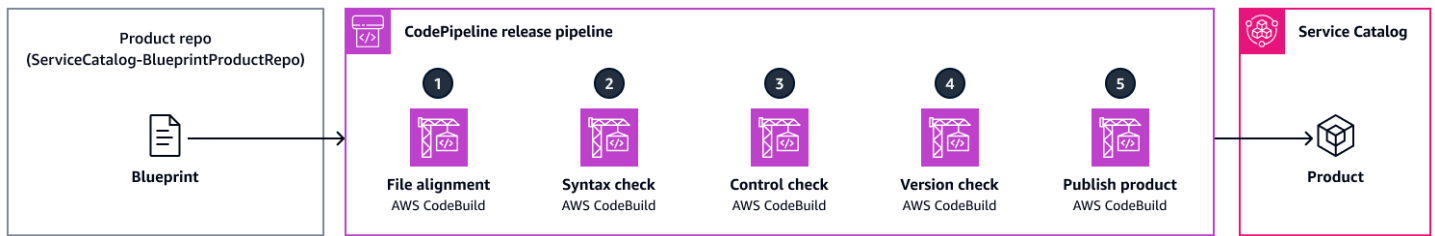
リリースパイプラインには、ブループリントのセキュリティとコンプライアンスチェックを自動化する [プロアクティブコントロール](#) が含まれています。プロアクティブコントロールは、非準拠のリソースの作成を防ぐように設計されています。これらのコントロールは、応答コントロールや検出コントロールなど、他のタイプの [セキュリティコントロールによって処理されるセキュリティ](#) イベントの数を減らすことができます。プロアクティブコントロールは、デプロイされたリソースがデプロイされる前に準拠していることを確実にするため、対応や修復を必要とする検出イベントはありません。

設定パイプラインを初めて呼び出すと、という名前の Service Catalog 製品が作成されます Bootstrapping-Admin-Product。この製品は、リリースパイプラインの CloudFormation テンプレートです。次の図に示すように、設定パイプラインは Bootstrapping-Admin-Product 製品を使用して、新しいブループリントごとに専用のリリースパイプラインを作成します。ブループリントとリリースパイプラインの間には one-to-one の関係があります。



リリースパイプラインステージ

次の図は、リリースパイプラインのデフォルトステージと、パイプラインがやり取りするリソースを示しています。パイプラインの各ステージは CodeBuild プロジェクトです。



リリースパイプラインのステージは次のとおりです。

1. ファイルアラインメント – このステージでは、ブループリントが [CloudFormation テンプレート](#) または [AWS Cloud Development Kit \(AWS CDK\) コンストラクト](#) であることを確認します。ブループリントが AWS CDK コンストラクトの場合、このステージは AWS CDK コンストラクトを CloudFormation テンプレートに合成します。このプロセスは、CloudFormation を通じてデプロイを自動化および標準化します。エラーが見つかった場合、パイプラインは失敗します。
2. 構文チェック – 構文エラーは CloudFormation デプロイエラーの一般的な原因です。この段階では、[AWS CloudFormation Linter \(cfn-lint\)](#) はテンプレートを [AWS CloudFormation リソース仕様](#) と比較することで構文エラーをチェックします。また、リソースプロパティの有効な値の確認やベストプラクティスの遵守など、他のチェックも実行します。エラーが見つかった場合、パイプラインは失敗し、cfn-lint は提案を返します。
3. コントロールチェック – この段階では、[cfn_nag](#) はパターンを検索して潜在的なセキュリティ問題をチェックします。たとえば、過度に寛容なセキュリティグループと AWS Identity and Access Management (IAM) ポリシー、暗号化の欠落、パスワードリテラルをチェックします。エラーが見つかった場合、パイプラインは失敗し、cfn_nag は提案を返します。
4. バージョンチェック – リリースパイプラインは、製品設定ファイルで定義されているバージョン戦略に基づいてバージョン管理を実行します。製品バージョンが [イミュータブル](#) と定義されている場合、Service Catalog は以前の製品バージョンを非アクティブ化します。
5. 製品の公開 – リリースパイプラインは、Service Catalog で製品をリリースします。

Note

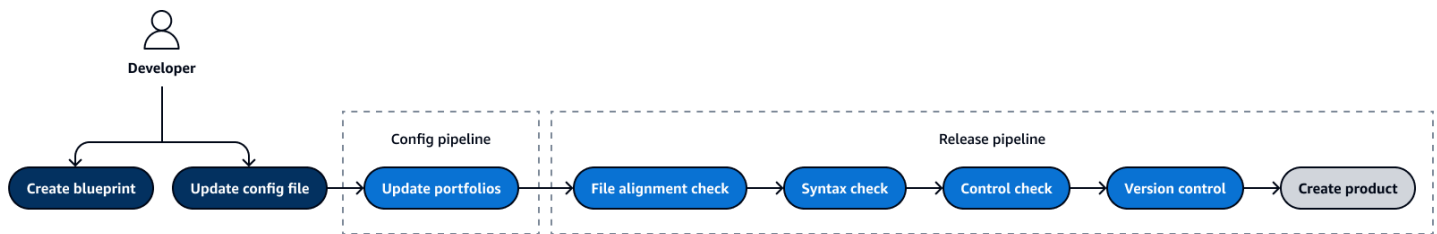
リリースパイプラインはカスタマイズ可能です。たとえば、ユースケースに適用されないステージを削除できます。他のコントロールチェック、追加の検証、または手動承認ステップを追加する場合は、ステージをさらに追加することもできます。このガイドには、リリースパイプラインを変更する手順は含まれていません。詳細については、[CodePipeline](#) と [CodeBuild](#) のドキュメントを参照してください。

Enterprise Blueprint Factory の設計図のライフサイクル

Enterprise Blueprint Factory の設計図のライフサイクルは、作成、更新、削除の 3 つの一般的な段階で構成されます。ライフサイクルステージは、設定パイプラインとリリースパイプラインが実行するアクションに影響します。

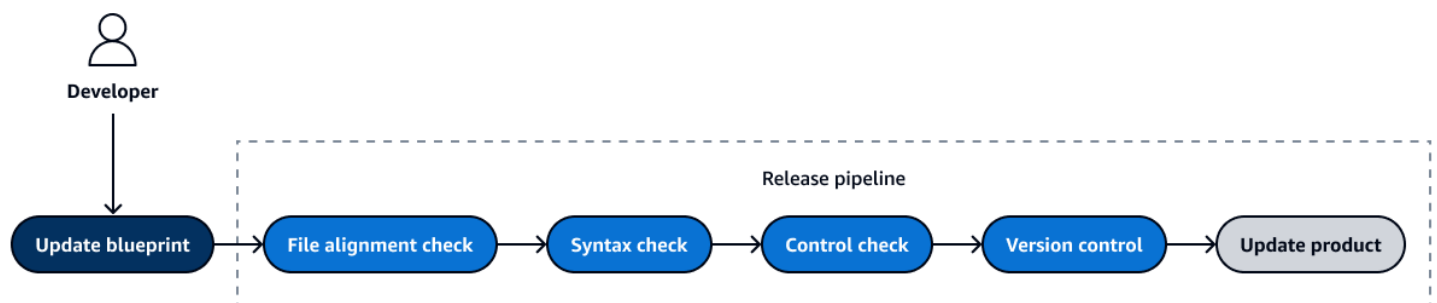
設計図の作成

で新しいブループリントを製品としてリリースするために AWS Service Catalog、開発者はブループリントを製品リポジトリにマージし、設定ファイルのポートフォリオを更新して、新しい製品を設定ファイルに追加します。これにより、設定パイプラインが呼び出されます。設定パイプラインは、製品のリリースパイプラインを作成します。リリースパイプラインでは、ブループリントは複数のセキュリティチェックを受けます。次に、リリースパイプラインは設計図を Service Catalog 製品としてデプロイします。

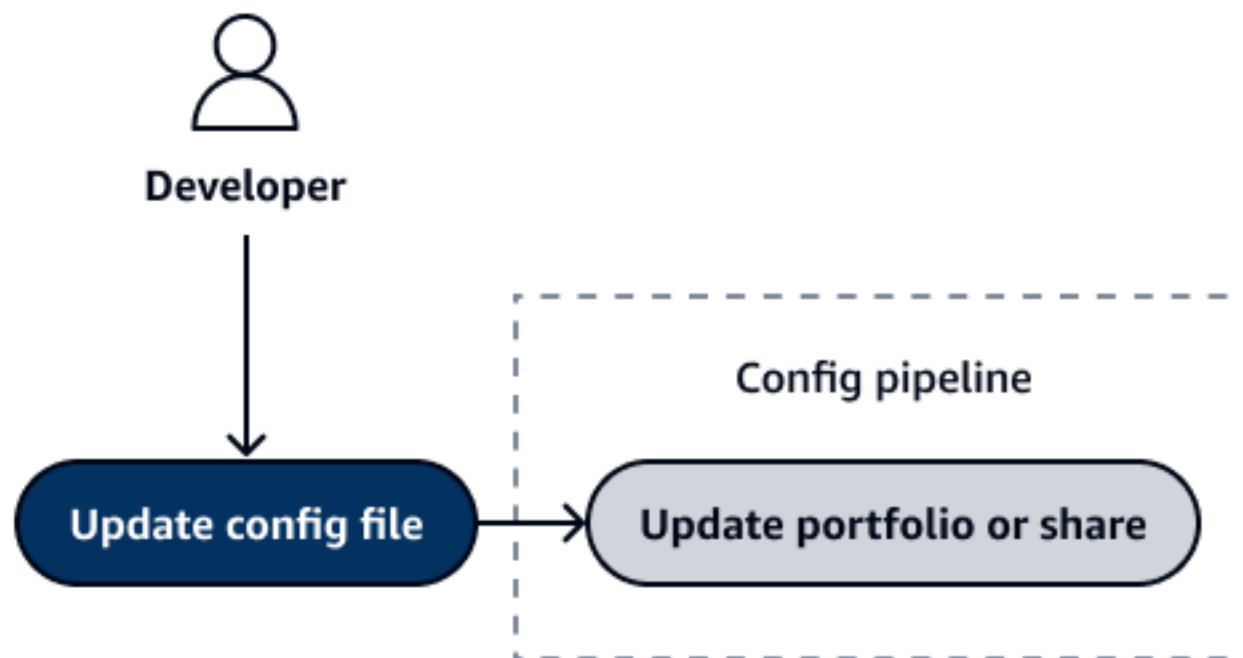


設計図の更新

デベロッパーは、更新されたバージョンのブループリントを製品リポジトリにマージすることで、Service Catalog で製品を更新できます。この更新により、製品のリリースパイプラインが呼び出されます。更新されたテンプレートは、リリースパイプラインでセキュリティチェックを受けます。リリースパイプラインは、Service Catalog 製品の新しいバージョンをデプロイします。Service Catalog が製品バージョンを更新する方法の詳細については、Service Catalog ドキュメントの「[バージョンの管理](#)」を参照してください。



または、ブループリントが関連付けられている Service Catalog ポートフォリオを更新したり、それらのポートフォリオの共有設定を変更したりできます。この場合、開発者は設定リポジトリの設定ファイルを更新します。設定パイプラインは、ポートフォリオまたはポートフォリオ共有を更新します。この場合、Service Catalog の製品は変更されませんが、異なるポートフォリオに含まれる可能性があります。



設計図の削除

⚠ Important

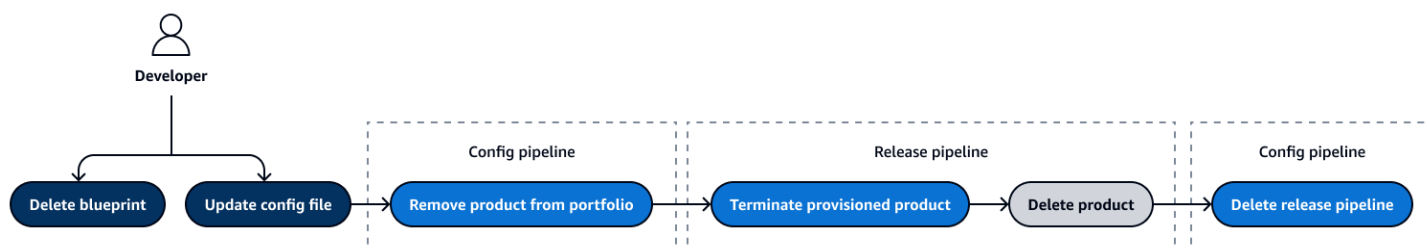
削除後に Service Catalog 製品を復元することはできません。ただし、ブループリントを新しい製品として再デプロイすることはできます。

製品を削除すると、Service Catalog は製品を含むすべてのポートフォリオからすべての製品バージョンを削除します。詳細については、Service Catalog ドキュメントの「製品 [の削除](#)」を参照してください。

Service Catalog にデプロイされたブループリントを削除するには、開発者は製品リポジトリのブループリントを削除します。次に、設定ファイルから製品を削除します。設定パイプラインは、製品を含むポートフォリオから製品の関連付けを解除し、すべての製品関連付けを削除します。リリース

パイプラインは、Service Catalog 製品と [プロビジョニング済み製品を終了](#) します。次に、設定パイプラインは製品のリリースパイプラインを削除します。

設定パイプラインが製品のすべてのリソースの関連付けを解除できない場合、製品は削除されず、パイプラインは失敗します。失敗したリソースの関連付け解除を解決してから、パイプラインを再起動する必要があります。詳細については、[「製品を削除するときに失敗したリソースの関連付け解除を解決する」](#)を参照してください。



Enterprise Blueprint Factory のセットアップ

このセクションでは、AWS 環境で Enterprise Blueprint Factory をセットアップする方法について説明します。これには、Enterprise Blueprint Factory に必要なリポジトリと AWS リソースをセットアップするための詳細な手順が含まれています。

前提条件

以下は、AWS 環境で Enterprise Blueprint Factory をセットアップするための前提条件です。

- 以下を実行します AWS アカウント。
 - Enterprise Blueprint Factory の管理と製品のリリースに使用されるアカウント
 - リリースされた製品を消費する 1 つ以上のアカウント
- すべてのアカウントは次のとおりです。
 - で組織として管理 [AWS Organizations](#)
 - 同じ[組織単位 \(OU\)](#) にある
 - 組織は[account-per-tenantモデルに従います。](#)
- AWS Command Line Interface (AWS CLI)、[インストール](#)および[設定](#)済み
- 次の AWS リソースを作成する AWS CloudFormation スタックをデプロイするアクセス許可。
 - Amazon CloudWatch Logs ロググループ
 - AWS CodePipeline パイプライン
 - AWS CodeBuild プロジェクト
 - Amazon EventBridge イベントバスポリシーとルール
 - AWS Identity and Access Management (IAM) ロールとポリシー
 - AWS Key Management Service (AWS KMS) キーとキーポリシー
 - AWS Service Catalog ポートフォリオ、製品、プロビジョニング済み製品
 - Amazon Simple Notification Service (Amazon SNS) トピック、トピックポリシー、サブスクリプション
 - Amazon Simple Storage Service (Amazon S3) のバケット
 - AWS Systems Manager Parameter Store パラメータ

これらのアクセス許可の設定の詳細については、[CloudFormation ドキュメント](#)と「[最小特権アクセス許可のポリシーの実装 AWS CloudFormation](#)」を参照してください。

- GitHub アカウント

ベストプラクティス

AWS 環境で Enterprise Blueprint Factory を設定するときは、次のベストプラクティスに従うことをお勧めします。

- Enterprise Blueprint Factory をデプロイするために必要なアクセス許可を設定するときは、最小権限の原則に従い、必要な最小限のアクセス許可を付与します。詳細については、IAM ドキュメントの「[最小特権の付与](#)」と「[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。
- Service Catalog ポートフォリオへのアクセスを設定するときは、最小特権の原則に従い、特定のロール、ユーザー、または管理者にのみアクセスを許可します。Service Catalog [のセキュリティのベストプラクティス](#)に従ってください。

リポジトリの作成

このセクションでは、Enterprise Blueprint Factory [の設定リポジトリ](#)と[製品リポジトリ](#)を設定するのに役立ちます。リポジトリを設定するには、GitHub で指定されたリポジトリを[フォーク](#)します。次に、AWS CodeConnections を使用して GitHub リポジトリ [への接続](#)を作成します。次に、GitHub リポジトリをローカルマシンにクローンします。

GitHub リポジトリをフォークするには

1. [GitHub](#) にログインします。
2. Configuration [repo](#) GitHub リポジトリに移動します。
3. フォークを選択します。
4. 「新しいフォークを作成する」ページの「リポジトリ名」ボックスに「」と入力しますServiceCatalog-ConfigRepo。
5. (オプション) 説明を入力します。
6. メインブランチのみをコピーを選択します。
7. フォークの作成 を選択します。
8. これらのステップを繰り返して、[Code repo](#) GitHub リポジトリをフォークします。このリポジトリServiceCatalog-CodeRepoの名前を入力します。
9. これらのステップを繰り返して、[Product repo](#) GitHub リポジトリをフォークします。このリポジトリServiceCatalog-BlueprintProductRepoの名前を入力します。

CodeConnections 接続を作成するには

1. AWS CLI で次のコマンドを入力して、GitHub への CodeConnections 接続を作成します。

```
aws codeconnections create-connection --provider-type GitHub --connection-name  
<MyConnection>
```

2. AWS デベロッパーツールコンソールを使用して接続を完了します。詳細については、「[Update a pending connection](#)」を参照してください。

フォークされたリポジトリのクローンを作成するには

- 次のコマンドを入力して、GitHub リポジトリをローカルワークステーションにクローンします。

```
git clone git@github.com:<user>/aws-enterprise-blueprint-factory-config-repo  
ServiceCatalog-ConfigRepo  
git clone git@github.com:<user>/aws-enterprise-blueprint-factory-blueprint-repo  
ServiceCatalog-BlueprintProductRepo  
git clone git@github.com:<user>/aws-enterprise-blueprint-factory-code-repo  
ServiceCatalog-CodeRepo
```

Enterprise Blueprint Factory のセットアップ

このセクションの手順では、ターゲットアカウントで Enterprise Blueprint Factory を設定する方法について説明します。GitHub からクローンした製品リポジトリには、2 つのサンプル CloudFormation テンプレート BP-S3 と BP-SNS が含まれています。これらの手順に従って、これら 2 つのサンプルブループリントを製品として Service Catalog にデプロイします。

ロールを設定するには

1. ブループリント開発者のアカウントで、次の信頼ポリシーを作成し、次のように保存します `sc-enduserrole-trust-policy.json`。

```
{  
  "Version": "2012-10-17",  
  "Statement": {  
    "Effect": "Allow",  
    "Principal": {
```

```
"AWS": "arn:aws:iam::123456789012:role/ServiceCatalogEndUserRole"
},
"Action": "sts:AssumeRole"
}
}
```

2. ServiceCatalogEndUserRole IAM ロールを作成するには、次のコマンドを入力します。

```
aws iam create-role \
--role-name ServiceCatalogEndUserRole \
--assume-role-policy-document file://sc-enduserrole-trust-policy.json
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess \
-- role-name ServiceCatalogEndUserRole
```

 Note

開発者は、ServiceCatalogEndUserRoleロールを使用して Service Catalog 製品をプロビジョニングします。このロールには、ブループリントで定義されたリソースを作成するためのアクセス許可は必要ありません。これは、最小特権のアクセス許可と職務分離のベストプラクティスに従います。

3. 次の信頼ポリシーを作成し、として保存しますsc-launchconstraintrole-trust-policy.json。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {
      "Service": "servicecatalog.amazonaws.com"
    },
    "Action": "sts:AssumeRole"
  }
}
```

4. IAM ServiceCataloglogLaunchConstraintRole ロールを作成するには、次のコマンドを入力します。

```
aws iam create-role \
--role-name ServiceCataloglogLaunchConstraintRole \
```

```
--assume-role-policy-document file://sc-launchconstraintrole-trust-policy.json
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AmazonSNSFullAccess \
--role-name ServiceCataloglogLaunchConstraintRole
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSCloudFormationFullAccess \
--role-name ServiceCataloglogLaunchConstraintRole
```

5. IAM ServiceCataloglogLaunchConstraintRole ロールに次のポリシーを追加します。Service Catalog ドキュメントの「[起動ロールの設定](#)」で説明されているように、製品リソースに必要なその他のアクセス許可を含めます。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
        }
      }
    }
  ]
}
```

 Note

Service Catalog は、このロールを使用して CloudFormation スタックを Service Catalog の製品としてデプロイします。このロールの信頼ポリシーにより、Service Catalog のみが引き受けることができます。他のユーザーまたはサービスは、このロールを引き受けることができません。これは職務分離のベストプラクティスに従います。

6. 次の信頼ポリシーを作成し、次のように保存します sc-codebuild-trust-policy.json。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
```

```
"Principal": {
  "Service": "codebuild.amazonaws.com"
},
"Action": "sts:AssumeRole"
}
}
```

7. IAM `codebuild-servicecatalog-admin-role` ロールを作成するには、次のコマンドを入力します。

```
aws iam create-role \
--role-name codebuild-servicecatalog-admin-role \
--assume-role-policy-document file://sc-codebuild-trust-policy.json
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess \
--role-name codebuild-servicecatalog-admin-role
```

 Note

設定パイプラインの CodeBuild ジョブはこのロールを使用します。

Amazon S3 バケットを設定するには

- CodePipeline アーティファクトの保存に使用される Amazon Simple Storage Service (Amazon S3) バケットを作成するには、Amazon S3 ドキュメントの「[バケットの作成](#)」の手順に従います。[Amazon S3 のセキュリティのベストプラクティス](#)に従います。

AWS Systems Manager パラメータを設定するには

- 次の表の [Systems Manager パラメータを作成するには、「Systems Manager でパラメータストアパラメータを作成する」](#)の手順に従います。これらのパラメータは、設定パイプラインをデプロイする CloudFormation テンプレートで使用されます。

パラメータ名	タイプ	説明
/blueprints/resources/vpc_id	文字列	ターゲット Virtual Private Cloud (VPC) の ID を保存するパラメータ。

パラメータ名	タイプ	説明
/blueprints/resources/subnets	StringList	ターゲットサブネットIDs を保存するパラメータ。
/blueprints/resources/securitygroups	StringList	ターゲットセキュリティグループの IDs を保存するパラメータ。
/blueprints/resources/artifacts-bucket-name	String	CodePipeline アーティファクトに使用される Amazon S3 バケット名を保存するパラメータ。
/blueprints/resources/BlueprintRepo	String	Enterprise Blueprint Factory ブループリントが保存されている GitHub リポジトリを保存するパラメータ。デフォルト値は <user>/aws-enterprise-blueprint-factory-blueprint-repo です。
/blueprints/resources/CodeRepo	String	Enterprise Blueprint Factory 設定パイプラインコードとBootstrapping-Admin-Product コードが保存される GitHub リポジトリを保存するパラメータ。デフォルト値は <user>/aws-enterprise-blueprint-factory-code-repo です。

パラメータ名	タイプ	説明
/blueprints/resources/ConfigRepo	String	Enterprise Blueprint Factory 設定ファイルが保存されている GitHub リポジトリを保存するパラメータ。デフォルト値は <user>/aws-enterprise-blueprint-factory-config-repo です。

CloudFormation テンプレートを更新するには

1. コードリポジトリ (ServiceCatalog-CodeRepo) で、ServiceCatalog-Pipeline.yml ファイルを開きます。
2. このファイルの次のパラメータのデフォルト値を編集します。
 - ConfigRepositoryName は、Enterprise Blueprint Factory 設定ファイルが保存されている GitHub リポジトリを保存する Systems Manager パラメータです。デフォルト値は /blueprints/resources/ConfigRepo です。
 - CodeRepositoryName は、Enterprise Blueprint Factory 設定パイプラインコードと Bootstrapping-Admin-Product コードが保存されている GitHub リポジトリを保存する Systems Manager パラメータです。デフォルト値は /blueprints/resources/CodeRepo です。
 - BlueprintRepositoryName は、Enterprise Blueprint Factory ブループリントが保存されている GitHub リポジトリを保存する Systems Manager パラメータです。デフォルト値は /blueprints/resources/BlueprintRepo です。
 - BranchName は、設定ファイルが保存されている設定リポジトリのブランチです。デフォルト値は main です。
 - VPCID は、ターゲット VPC の ID を保存する Systems Manager パラメータです。デフォルト値は /blueprints/resources/vpc_id です。
 - Subnets は、ターゲットサブネットの IDs を保存する Systems Manager パラメータです。デフォルト値は /blueprints/resources/subnets です。
 - SecurityGroupIds は、ターゲットセキュリティグループの IDs パラメータです。デフォルト値は /blueprints/resources/securitygroups です。

- `IamRoleName` は、CodeBuild ジョブが使用する IAM ロールの名前です。デフォルト値は `codebuild-servicecatalog-admin-role`。
 - `EnvironmentType` は、Enterprise Blueprint Factory をデプロイする環境です。デフォルト値は `DEV` です。
 - `ArtifactBucket` は、CodePipeline がアーティファクトを保存する Amazon S3 バケットを保存する Systems Manager パラメータです。デフォルト値は `/blueprints/resources/artifacts-bucket-name`。
 - `CodeConnectionArn` は、GitHub への CodeConnections 接続の Amazon リソースネーム (ARN) です。
3. `ServiceCatalog-Pipeline.yml` ファイルを保存して閉じます。
 4. 次のコマンドを入力して、変更をコードリポジトリにマージします。

```
cd ServiceCatalog-CodeRepo
git add ServiceCatalog-Pipeline.yml
git commit -m "<description of change>"
git push origin main
```

5. 設定リポジトリ (`ServiceCatalog-ConfigRepo`) で、`bp_config.yml` ファイルを開きます。
6. 組織に必要なポートフォリオセクションの値を更新します。たとえば、`portfolio_access_roles` および `share_to_ou` 属性を更新します。詳細については、このガイドの「[設定ファイル](#)」を参照してください。
7. `bp_config.yml` ファイルを保存して閉じます。
8. 次のコマンドを入力して、変更をコードリポジトリにマージします。

```
cd ServiceCatalog-ConfigRepo
git add bp_config.yml
git commit -m "<description of change>"
git push origin main
```

CloudFormation スタックをデプロイするには

1. Enterprise Blueprint Factory 管理アカウントにサインインします。
2. [管理権限を持つ](#) IAM ロールに切り替えます。
3. [クラウドフォーメーション コンソール](#)を開きます。
4. 画面上部のナビゲーションバーで、ターゲットを選択します AWS リージョン。

5. [スタック] ページでは、右上の [スタックの作成] を選択してから、[新しいリソースを使用 (標準)] を選択します。
6. [Prepare template] (テンプレートの準備) の [Template is ready] (テンプレートの準備が完了しました) を選択します。
7. [テンプレートの指定] で、[テンプレートファイルのアップロード] を選択します。
8. ファイルの選択 を選択し、ServiceCatalog-CodeRepoフォルダに移動し、ServiceCatalog-Pipeline.yml を選択します。
9. [次へ] を選択して続行し、テンプレートを検証します。
10. スタック名には、スタックの名前を入力します。
11. Parameters セクションで、デフォルト値を変更しないでください。
12. [次へ] を選択します。
13. スタックオプションの設定ページで、デフォルト値を変更せずに、次へを選択します。
14. 確認と作成ページで、テンプレートとスタックの詳細を確認し、送信を選択します。
15. スタックデプロイの進行状況をモニタリングします。詳細については、[CloudFormation ドキュメント](#)を参照してください。
16. ステータスが になるまで待ちますCREATE_COMPLETE。

デプロイを検証するには

1. [AWS Service Catalog コンソール](#)を開きます。
2. ナビゲーションペインで、[Products] (製品) を選択します。
3. ServiceCatalog-Pipeline が製品リストで使用可能であることを確認します。
4. [AWS CodePipeline コンソール](#)を開きます。
5. Name で、設定パイプラインを選択します。デフォルトでは、パイプライン名は ですServiceCatalog-Pipeline。
6. [View history (履歴の表示)] を選択します。
7. パイプラインとステージの実行のステータスを表示します。ステータスの詳細については、CodePipeline ドキュメントの「[実行ステータスの表示](#)」を参照してください。
8. 設定パイプラインのステータスが になるまで待ちますSucceeded。
9. [Service Catalog コンソール](#)を開きます。
10. ナビゲーションペインで、[Products] (製品) を選択します。

11. BP-S3-Product および BP-SNS-Product 製品が使用可能であることを確認します。これは、サンプルブループリントの製品リリースパイプラインが正常に完了したことを示します。
12. Enterprise Blueprint Factory のセットアップ時にデプロイしたサンプルブループリントを削除する場合は、[「ブループリントの削除」](#)の手順に従います。

Enterprise Blueprint Factory を削除する

Enterprise Blueprint Factory を使用していない場合は、それを削除して、その AWS リソースに関連するコストの発生を停止できます。

リソースを削除するには

1. Enterprise Blueprint Factory 管理アカウントにデプロイされた IAM ロールを削除するには、次のコマンドを入力します。

```
aws iam detach-role-policy \  
--policy-arn arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess \  
--role-name ServiceCatalogEndUserRole  
aws iam delete-role --role-name ServiceCatalogEndUserRole  
aws iam detach-role-policy \  
--policy-arn arn:aws:iam::aws:policy/AmazonSNSFullAccess \  
--role-name ServiceCatalogLogLaunchConstraintRole  
aws iam delete-role --role-name ServiceCatalogLogLaunchConstraintRole
```

2. Enterprise Blueprint Factory の CloudFormation スタックを削除します。手順については、[CloudFormation コンソールからスタック](#)を削除する」または「[からスタックを削除する AWS CLI](#)」を参照してください。
3. CodePipeline アーティファクトの保存に使用される Amazon S3 バケットを削除します。手順については、Amazon S3 ドキュメントの[「バケットの削除」](#)を参照してください。
4. Parameter Store から次の Systems Manager パラメータを削除します。
 - /blueprints/resources/vpc_id
 - /blueprints/resources/subnets
 - /blueprints/resources/securitygroups
 - /blueprints/resources/artifacts-bucket-name
 - /blueprints/resources/BlueprintRepo
 - /blueprints/resources/CodeRepo

- /blueprints/resources/ConfigRepo

手順については、Systems Manager ドキュメントの [「パラメータストアからのパラメータの削除」](#) を参照してください。

Enterprise Blueprint Factory の使用

このセクションでは、環境でブループリントを作成、更新、削除する方法について説明します。[ライフサイクル](#)全体でブループリントを管理するための詳細な手順を示します。

カスタムブループリントを作成または更新するには、AWS CloudFormation [テンプレート](#)や AWS Cloud Development Kit (AWS CDK) [コンストラクト](#)などの IaC テンプレートを作成する方法を理解する必要があります。このガイドには、Enterprise Blueprint Factory を通じてリリースするブループリントを定義する方法に関する情報や手順は含まれていません。

前提条件

以下は、AWS 環境で Enterprise Blueprint Factory を使用するための前提条件です。

- AWS Command Line Interface (AWS CLI)、[インストール](#)および[設定](#)済み
- ServiceCatalogEndUserRole AWS Identity and Access Management (IAM) ロールを引き受けるアクセス許可
- CloudFormation テンプレートまたは AWS CDK コンストラクト

ブループリントの作成

Enterprise Blueprint Factory パイプラインは、設定ファイルで定義したブループリントをデプロイします。開発者は、設定ファイルを設定リポジトリにマージして設定パイプラインを開始します。次に、エンタープライズブループリントファクトリーは、を使用して ServiceCatalogLaunchConstraintRole、ブループリントを Service Catalog の製品としてデプロイします。ブループリントの作成時に設定パイプラインとリリースパイプラインが実行するアクションの詳細については、このガイドの「[ブループリントの作成](#)」を参照してください。

設計図を製品リポジトリに追加するには

1. このガイドの「エンタープライズブループリントファクトリーのセットアップ」の指示に従って、[エンタープライズブループリントファクトリーをセットアップ](#)していることを確認します。
2. ServiceCataloglogLaunchConstraintRole ロールのポリシーで、ブループリントで定義されたリソースをプロビジョニングできることを確認します。
3. 製品リポジトリ (ServiceCatalog-BlueprintProductRepo) で、新しいブループリントのフォルダを作成します。

4. IaC テンプレート (CloudFormation テンプレートまたは AWS CDK コンストラクト) を、作成したフォルダに貼り付けます。
5. 作成したフォルダに `product_config.json` という名前のファイルを作成します。
6. `product_config.json` ファイルを開き、ファイルに以下を貼り付けます。

```
{
  "SchemaVersion": "1.0",
  "ProductVersionName": "1.0.1",
  "Deprecated_Versions" : [],
  "ProductVersionDescription": "<description>",
  "ProductType": "CLOUD_FORMATION_TEMPLATE",
  "Properties": {
    "TemplateFilePath": "./<folder name>/<file name>"
  }
}
```

コードの説明は以下のとおりです。

- `<description>` は、ブループリントバージョンの簡単な説明です。
- `<folder name>` は、製品リポジトリで作成したフォルダの名前です。
- `<file name>` は IaC テンプレートの名前です

Note

スキーマバージョンまたは製品バージョン名は、組織のポリシーに合わせて更新できます。

7. `product_config.json` ファイルを保存して閉じます。
8. 次のコマンドを入力して、変更を製品リポジトリにマージします。

```
cd ServiceCatalog-BlueprintProductRepo
git add <folder name>/<file name> <folder name>\product_config.json
git commit -m "The first version of <file name> blueprint"
git push origin main
```

設定ファイルを更新するには

1. 設定リポジトリ (ServiceCatalog-ConfigRepo) で、config.yml ファイルを開きます。
2. 新しいブループリントに必要な portfolios セクションと products セクションを編集します。詳細については、このガイドの「[設定ファイル](#)」を参照してください。
3. config.yml ファイルを保存して閉じます。
4. 次のコマンドを入力して、変更を設定リポジトリにマージします。

```
cd ServiceCatalog-ConfigRepo
git add config.yml
git commit -m "<description of change>"
git push origin main
```

このプルリクエストを承認すると、設定パイプラインが開始されます。設定パイプラインは、製品のリリースパイプラインを作成します。

デプロイログを確認するには

1. Enterprise Blueprint Factory 管理アカウントにサインインします。
2. [AWS CodePipeline コンソール](#)を開きます。
3. Name で、製品のリリースパイプラインを選択します。デフォルトでは、パイプライン名は `BluePrint_<Product-Name>-<CloudFormation-Stack-Name>` です。
4. [View history (履歴の表示)] を選択します。
5. パイプラインとステージ実行のステータスを表示します。ステータスの詳細については、CodePipeline ドキュメントの「[実行ステータスの表示](#)」を参照してください。
6. パイプラインが失敗した場合、失敗の原因を確認します。パイプラインのモニタリングを設定する方法については、CodePipeline ドキュメントの「[パイプラインのモニタリング](#)」を参照してください。cfn-lint または cfn_nag チェックが原因でリリースパイプラインが失敗した場合は、テンプレートのエラーを修正します。別のプルリクエストを製品リポジトリに送信します。これにより、リリースパイプラインが再起動されます。テンプレートエラーの修正の詳細については、このガイドの「[トラブルシューティング](#)」セクションを参照してください。
7. リリースパイプラインのステータスが `Succeeded` になるまで待ちます。

デプロイを検証するには

1. 組織内のコンシューマーアカウントにサインインします。
2. IAM ServiceCatalogEndUserRole ロールを引き受けます。
3. [Service Catalog コンソール](#)を開きます。
4. ナビゲーションペインで、[Products] (製品) を選択します。
5. 新製品が製品リストで使用可能であることを確認します。

設計図の更新

ブループリントの作成時に設定パイプラインとリリースパイプラインが実行するアクションの詳細については、このガイドの「[ブループリントの更新](#)」を参照してください。

ブループリントを更新するには

1. 製品リポジトリで、製品の フォルダに移動します。
2. 更新された IaC テンプレートを貼り付けます。ファイル名が以前のバージョンと同じであることを確認します。
3. product_config.json ファイルを開きます。
4. ではProductVersionName、バージョン番号を更新します。
5. 以前の製品バージョンが将来デプロイされないようにするには、にDeprecated_Versions以前のバージョン番号をカンマ区切りリストに入力します。
6. 次のコマンドを入力して、変更を製品リポジトリにマージします。

```
cd ServiceCatalog-BlueprintProductRepo
git add <folder name>/<file name> <folder name>\product_config.json
git commit -m "Version <number> of <file name> blueprint"
git push origin main
```

このプルリクエストを承認すると、製品のリリースパイプラインが開始されます。

デプロイログを確認するには

1. Enterprise Blueprint Factory 管理アカウントにサインインします。
2. [AWS CodePipeline コンソール](#)を開きます。

3. Name で、リリースパイプラインを選択します。デフォルトでは、パイプライン名は `Blueprint_<Product-Name>-<CloudFormation-Stack-Name>`。
4. [View history (履歴の表示)] を選択します。
5. パイプラインとステージ実行のステータスを表示します。ステータスの詳細については、CodePipeline ドキュメントの「[実行ステータスの表示](#)」を参照してください。
6. パイプラインが失敗した場合、失敗の原因を確認します。パイプラインのモニタリングを設定する方法については、CodePipeline ドキュメントの「[パイプラインのモニタリング](#)」を参照してください。cfn-lint または cfn_nag チェックが原因でリリースパイプラインが失敗した場合は、テンプレートのエラーを修正します。別のプルリクエストを製品リポジトリに送信します。これにより、リリースパイプラインが再起動されます。テンプレートエラーの修正の詳細については、このガイドの「[トラブルシューティング](#)」セクションを参照してください。
7. リリースパイプラインのステータスが `Succeeded` になるまで待ちます。

更新を検証するには

1. 組織内のコンシューマーアカウントにサインインします。
2. IAM ServiceCatalogEndUserRole ロールを引き受けます。
3. [Service Catalog コンソール](#)を開きます。
4. ナビゲーションペインで、[Products] (製品) を選択します。
5. 新しい製品バージョンが製品リストで使用可能であることを確認します。

ブループリントの削除

製品を削除すると、Service Catalog は製品を含むすべてのポートフォリオからすべての製品バージョンを削除します。詳細については、Service Catalog ドキュメントの「[製品の削除](#)」を参照してください。ブループリントの作成時に設定パイプラインとリリースパイプラインが実行するアクションの詳細については、このガイドの「[ブループリントの削除](#)」を参照してください。

ブループリントを削除するには

1. 設定リポジトリで、config.yml ファイルを開きます。
2. 製品セクションを編集し、削除する製品を削除またはコメントアウトします。
3. config.yml ファイルを保存して閉じます。
4. 次のコマンドを入力して、変更を設定リポジトリにマージします。

```
cd ServiceCatalog-ConfigRepo
git add config.yml
git commit -m "<description of change>"
git push origin main
```

このプルリクエストを承認すると、設定パイプラインが開始されます。設定パイプラインは、製品とそのリリースパイプラインを削除します。

5. 製品リポジトリで、製品の内容を含む製品のフォルダを削除します。
6. 次のコマンドを入力して、変更を製品リポジトリにマージします。

```
cd ServiceCatalog-BlueprintProductRepo
git add .
git commit -m "Delete <file name> blueprint"
git push origin main
```

削除を検証するには

1. 組織内のコンシューマーアカウントにサインインします。
2. IAM ServiceCatalogEndUserRole ロールを引き受けます。
3. [Service Catalog コンソール](#)を開きます。
4. ナビゲーションペインで、[Products] (製品) を選択します。
5. 削除した製品が使用できなくなったことを確認します。

トラブルシューティング

ブループリントを作成または更新すると、cfn-lint ツールと cfn-nag ツールによってブループリントが検証されます。リリースパイプラインの検証の詳細については、このガイドの「[リリースパイプライン](#)」を参照してください。報告された構文またはセキュリティエラーにより、パイプラインは失敗します。リリースパイプラインを介してブループリントを正常にデプロイするには、ブループリントのエラーを修正する必要があります。

以下は、障害と警告の 2 つのセキュリティ関連のエラーを示す出力例です。

```
BP-SNS.yml
-----
BP-SNS.yml
```

```
-----  
| WARN W47  
|  
| Resource: ["ExampleTopic"]  
| Line numbers: [5]  
|  
| SNS Topic should specify KmsMasterKeyId property  
-----  
| FAIL F18  
|  
| Resource: ["ExampleTopicPolicy"]  
| Line numbers: [10]  
|  
| SNS topic policy should not allow * principal  
  
Failures count: 1  
Warnings count: 1
```

これらのエラーを修正するには、設計図ファイルで、Amazon Simple Notification Service (Amazon SNS) トピックポリシーの*プリンシパルを置き換え、AWS Key Management Service (AWS KMS) キーをトピックに関連付けます。次のコード例は、これらの更新を示しています。

```
ExampleTopic:  
  Type: AWS::SNS::Topic  
  Properties:  
    TopicName: ExampleTopic  
ExampleTopicPolicy:  
  Type: AWS::SNS::TopicPolicy  
  Properties:  
    KmsMasterKeyId: alias/aws/sns # Added KMS key  
    PolicyDocument:  
      Id: Id1  
      Version: '2012-10-17'  
      Statement:  
        - Sid: Sid2  
          Effect: Allow  
          Principal:  
            "Service" : "s3.amazonaws.com" # Replaced "AWS": '*'  
          Action: 'sns:Publish'  
          Resource: !Ref ExampleTopic  
    Topics:  
      - !Ref ExampleTopic
```

関連リソース

AWS ドキュメント

- [チュートリアル: Service Catalog にデプロイするパイプラインを作成する \(ドキュメント\)](#) AWS CodePipeline
- [AWS CodePipeline ドキュメント](#)
- [AWS CodeBuild ドキュメント](#)
- [AWS Service Catalog 管理者ガイド](#)
- [AWS Service Catalog ユーザーガイド](#)

AWS ブログ投稿

- [AWS Service Catalog エステートのレポートと視覚化](#) (AWS ブログ記事)
- [スタックの AWS CloudFormation ドリフトを自動的に検出するアラームの実装](#) (AWS ブログ記事)

寄稿者

以下の個人がこのガイドに貢献しました。

オーサリング

- Haofei Feng、シニアクラウドアーキテクト、AWS
- Cam Maxwell、Principal Security Advisor、AWS
- Joe Guo、クラウドサポートエンジニア、AWS
- Shreejesh MV、シニアクラウドアーキテクト、AWS

レビュー

- Joseph Dominic、クラウドアーキテクト、AWS
- Naresh Rajaram、コンサルティングパートナーソリューションアーキテクト、AWS

テクニカルライティング

- " AbouHarb、シニアテクニカルライター、AWS

ドキュメント履歴

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

変更	説明	日付
初版発行	—	2024 年 10 月 10 日

AWS 規範ガイドの用語集

以下は、AWS 規範ガイドが提供する戦略、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 1 人の当事者が管理し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。確信が持てば、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 に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。移行戦略との関連性については、AWS [「移行準備ガイド」](#) を参照してください。

CMDB

[「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、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、ワークロードが非準拠になる可能性があり、通常は段階的かつ意図的ではありません。

構成管理データベース (CMDB)

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

コンフォーマンスパック

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

継続的インテグレーションと継続的デリバリー (CI/CD)

ソフトウェアリリースプロセスのソース、ビルド、テスト、ステージング、本番の各ステージを自動化するプロセス。CI/CD は一般的にパイプラインと呼ばれます。プロセスの自動化、生産性の向上、コード品質の向上、配信の加速化を可能にします。詳細については、「[継続的デリバ](#)

[リーの利点](#)」を参照してください。CD は継続的デプロイ (Continuous Deployment) の略語でもあります。詳細については「[継続的デリバリーと継続的なデプロイ](#)」を参照してください。

CV

[「コンピュータビジョン」](#)を参照してください。

D

保管中のデータ

ストレージ内にあるデータなど、常に自社のネットワーク内にあるデータ。

データ分類

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

データドリフト

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

転送中のデータ

ネットワーク内 (ネットワークリソース間など) を活発に移動するデータ。

データメッシュ

一元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。信頼できる ID のみが、予想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、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

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

機能ブランチ

[「ブランチ」](#)を参照してください。

特徴量

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

特徴量重要度

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

機能変換

追加のソースによるデータのエンリッチ化、値のスケーリング、単一のデータフィールドからの複数の情報セットの抽出など、機械学習プロセスのデータを最適化すること。これにより、機械

学習モデルはデータの恩恵を受けることができます。例えば、「2021-05-27 00:15:37」の日付を「2021 年」、「5 月」、「木」、「15」に分解すると、学習アルゴリズムがさまざまなデータコンポーネントに関連する微妙に異なるパターンを学習するのに役立ちます。

数ショットプロンプト

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 フレームワーク」の「[イミュータブル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。 [エンディアン性](#) 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または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

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

MES

[「製造実行システム」](#)を参照してください。

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により、このフレームワークは人材アクセラレーションと呼ばれます。詳細については、[OCM ガイド](#) を参照してください。

オリジンアクセスコントロール (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

非準拠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、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、事前レスポンスを繰り返し改善または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、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

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

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「アカウントで利用できるを指定する」](#)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。たとえば、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、単一の文字列、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。自動応答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

送信先にあるデータの、それ AWS のサービス を受け取る 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

[「サービスレベルの契約」](#) 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。

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。

監視制御とデータ収集 (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とときに各アカウントに作成し、ユーザーに代わって管理タスクを実行します。詳細については、ドキュメントの「[を他の AWS のサービス AWS Organizations で使用する AWS Organizations](#)」を参照してください。

チューニング

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

ツーピザチーム

2 枚のピザ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

「[Write Once](#)」、「[Read Many](#)」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。