



このコンテンツは公開から3年以上経過しており内容が古い可能性があります
最新情報については[サービス別資料](#)もしくはサービスのドキュメントをご確認ください



AWS

Black Belt
Online Seminar

【AWS Black Belt Online Seminar】

AWS Service Catalog

Archived

アマゾンウェブ サービス ジャパン株式会社

ソリューションアーキテクト 能仁 信亮

2018.07.18

自己紹介

能仁 信亮(のうにん しんりょう)

エンタープライズ ソリューション部
ソリューション アーキテクト

普段の業務

主に金融機関のお客様のクラウドへのマイグレーション支援



好きなAWSサービス

- Amazon S3、AWS Service Catalog

AWS Black Belt Online Seminarとは

AWSJのTechメンバがAWSに関する様々な事を紹介するオンラインセミナーです

【火曜 12:00～13:00】

主にAWSのソリューションや業界カットでの使いどころなどを紹介(例：IoT、金融業界向け etc.)

【水曜 18:00～19:00】

主にAWSサービスの紹介やアップデートの解説(例：EC2、RDS、Lambda etc.)

※開催曜日と時間帯は変更となる場合がございます。最新の情報は下記をご確認下さい。

オンラインセミナーのスケジュール＆申し込みサイト <https://aws.amazon.com/jp/about-aws/events/webinars/>

内容についての注意点

- 本資料では2018年7月18日時点のサービス内容および価格についてご説明しています。最新の情報は AWS公式ウェブサイト(<http://aws.amazon.com>)にてご確認ください。
- 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます。
- 価格は税抜表記となっています。日本居住者のお客様が東京リージョンを使用する場合、別途消費税をご請求させていただきます。
- AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at <http://aws.amazon.com/agreement/>. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

Agenda

- はじめに
- AWS Service Catalog の機能概要
 - 用語と概念
 - 設定方法
 - 各種機能
 - 料金
- AWS Service Catalog を利用したアーキテクチャパターン
- AWS Service Catalog の活用事例
- まとめ

Agenda

- はじめに
- AWS Service Catalog の機能概要
 - 用語と概念
 - 設定方法
 - 各種機能
 - 料金
- AWS Service Catalog を利用したアーキテクチャパターン
- AWS Service Catalog の活用事例
- まとめ

インフラのプロビジョニングに関する典型的な課題

① プロビジョニングの
自動化

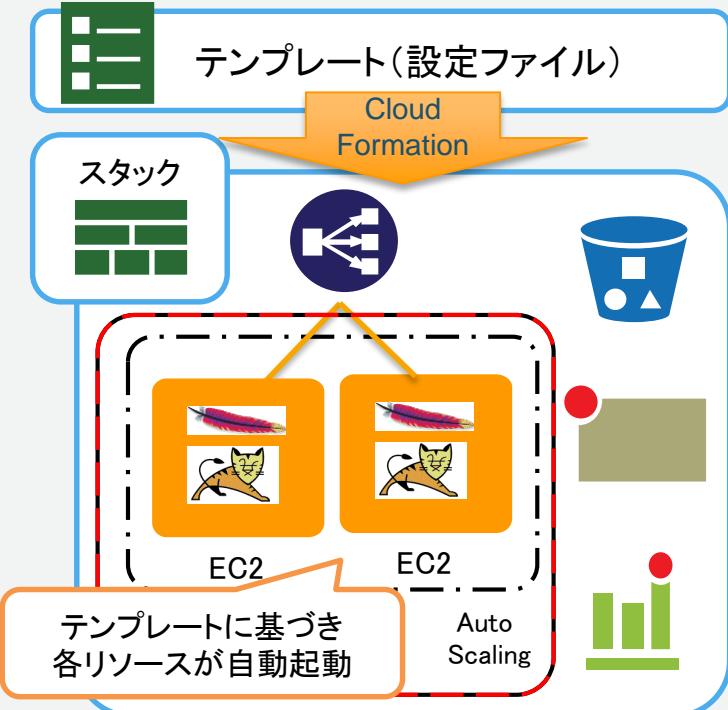
=

Infrastructure as Code

AWS CloudFormation



設定管理 & クラウドのオーケストレーション サービス



- テンプレートを元に、EC2やELBといったAWSリソースの環境構築を自動
- YAMLやJSONで、テンプレートを自由に記述可能
- Microsoft Windows Server や SAP HANAなどのクイックスタートリファレンスを用意

インフラのプロビジョニングに関する典型的な課題

① プロビジョニングの
自動化

=

Infrastructure as Code

② 統制を取りつつ
各チーム/プロジェクトが
セルフサービスで
プロビジョニングできる
仕組み作り

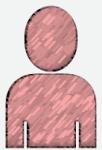
アジャリティとガバナンスの両立



社内ユーザ
(開発者)

スピードが重要！必要な権限が欲しい

業務チームや開発チームは、ビジネス機会を逃さないように可能な限り速く動きたい。そのためにはセルフサービスで環境を準備できるようにしたい



コンプライアンス
/システム管理
担当

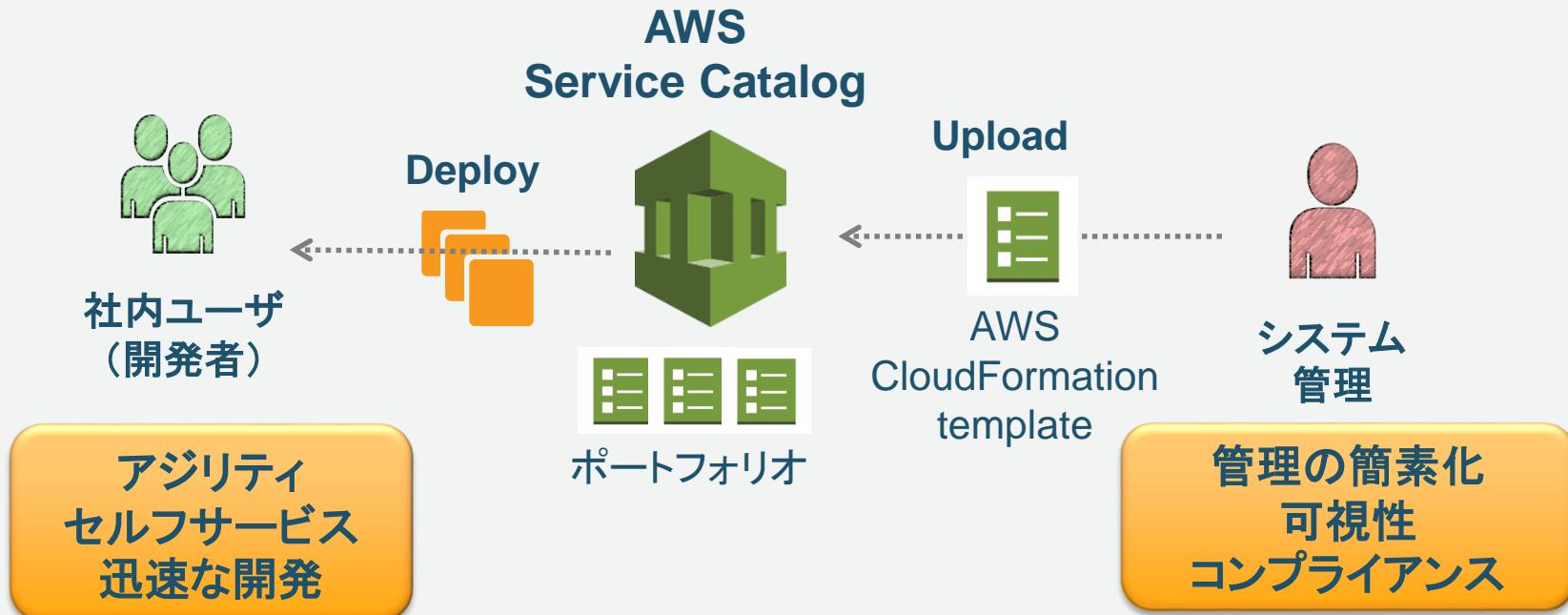
そんなに急がないで... ルールがあるから

組織全体としては、セキュリティやコンプライアンスを担保してリスクを最小化する必要がある

AWS Service Catalog



組織内サービスポータル提供サービス



AWS Service Catalog を利用する利点

分散したITサービスのライフサイクルを全体として最適化する

AWSのプロビジョニングに関するリスクを低減する (コスト、セキュリティ、ガバナンス)

セルフ サービス チーム ポータル

標準的なAWS環境のデプロイをテンプレート化する

テンプレートのバージョン管理を行う

プロアクティブにガバナンスやコンプライアンスを遵守させる

API経由でITSMツールと連携する

AWS Marketplace と連携する (製品のコピー)



Agenda

- はじめに
- AWS Service Catalog の機能概要
 - 用語と概念
 - 設定方法
 - 各種機能
 - 料金
- AWS Service Catalog を利用したアーキテクチャパターン
- AWS Service Catalog の活用事例
- まとめ

AWS Service Catalogの用語



製品



制約



ポートフォリオ



プロビジョニング
された製品

製品

- CloudFormationテンプレートをパッケージ化したもの
- EC2やストレージ、データベースなどの1つ以上のAWSリソースからなる
- バージョンが管理可能

ポートフォリオ

- 製品の集合
- ポートフォリオの単位でユーザーに製品の使用を許可
- 製品の使用方法(次ページの制約を参照)の管理も可能
- ポートフォリオを他のAWSアカウントに共有することも可能

制約

- 製品のデプロイ方法を制御。ポートフォリオごとに各製品に制約を追加
- テンプレート制約
製品を起動する際に、ユーザーが使用できるパラメータ(EC2インスタンスタイプなど)を制限
- 起動制約
起動時にリソースをプロビジョニングするのに利用するロール。
起動制約を利用することで、ユーザーの権限を最小にたもったまま、製品の起動が可能となる
- 通知制約
Amazon SNS トピックを使用してスタックのイベントに関する通知を受けることが可能となる

プロビジョニングされた製品

- AWS Service Catalogから起動された製品のインスタンス

管理者とエンドユーザーのコンソールビュー

管理者用コンソール

ポートフォリオや製品などの登録・管理

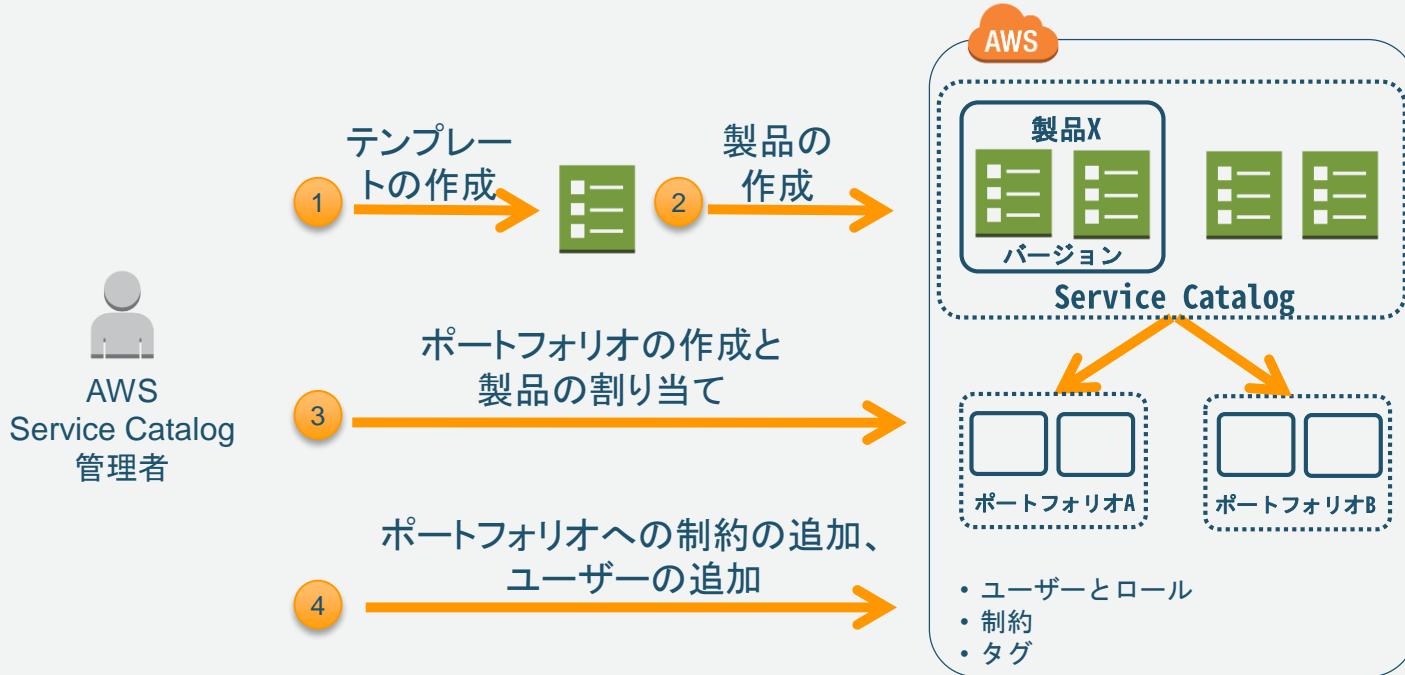
The screenshot shows the AWS Service Catalog Manager interface. The left sidebar includes options like 'aws service catalog', 'プロダクトリスト', 'プロビジョニングされた製品のリスト', '管理者', '製品リスト', 'ポートフォリオリスト' (selected), 'TagOption ライブラリ', '設定', and 'Marketplace ソフトウェア'. The main area is titled 'ポートフォリオリスト' and shows a 'ポートフォリオ' section with a 'ローカルポートフォリオ' tab selected. It displays a table with columns '名前' (Name) and '作成時刻' (Created At). A single item is listed: '開発環境用ポートフォリオ' created on Jul 12th 2018 10:13:05 UTC+....

エンドユーザー用コンソール

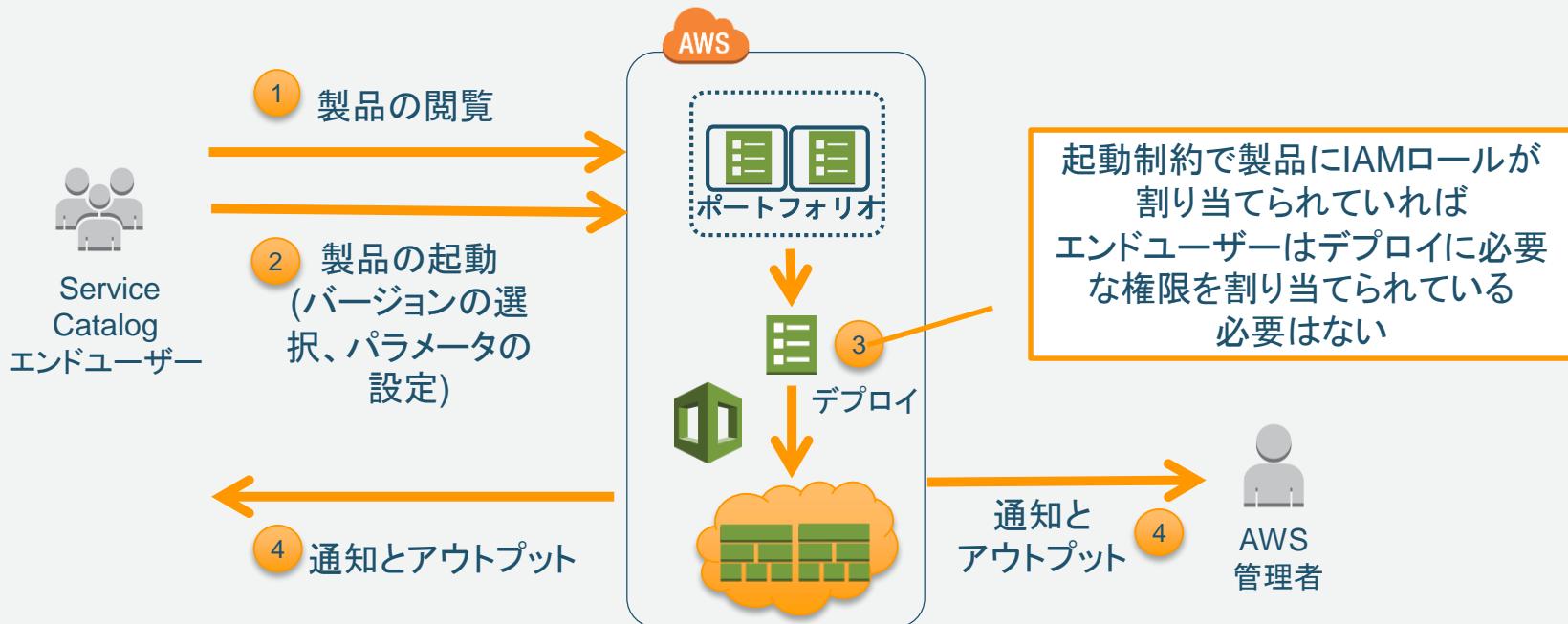
製品の閲覧・検索・起動

The screenshot shows the AWS Service Catalog End User interface. The left sidebar includes 'aws service catalog', '製品リスト' (selected), and 'プロビジョニングされた製品のリスト'. The main area is titled 'プロビジョニングされた製品のリスト - プロビジョニン' and shows a 'Web2' section. It features a large blue button labeled 'Internal App'. To the right, product details are shown: '状態' (Status) '利用可能' (Available), '製品' (Product) '標準Webシステム' (Standard Web System), 'バージョン' (Version) 'v1.0', and '提供元' (Provider) 'ITインフラ統括部'. Below this is a 'イベント (1)' (Events) section with one entry for Jul 12th 2018 at 12:07:40 UTC+0900, status '成功' (Success), record ID 'Record ID:rec-co3sil3maytyq', and output 'プロビジョニングされた製品の ID:pp-dfkyoa7g2ae46'.

管理の流れ



エンドユーザーの操作の流れ



Service CatalogのIAM 管理ポリシー

- 管理者用
 - **AWSServiceCatalogAdminFullAccess**
管理コンソールビューへのフルアクセス権と、製品とポートフォリオの作成および管理の権限を付与します。
 - **ServiceCatalogAdminReadOnlyAccess**
管理者コンソールビューへのフルアクセス権を付与します。製品とポートフォリオを作成または管理するためのアクセス権は付与しません。
- エンドユーザー用
 - **AWSServiceCatalogEndUserFullAccess**
エンドユーザー コンソールビューへのフルアクセス権を付与します。製品を起動し、プロビジョニング済み製品を管理するアクセス権を付与します。
 - **ServiceCatalogEndUserAccess**
エンドユーザー コンソールビューへの読み取り専用アクセス権を付与します。製品を起動し、プロビジョニング済み製品を管理するアクセス権は付与しません。

Agenda

- はじめに
- AWS Service Catalog の機能概要
 - 用語と概念
 - 設定方法
 - 各種機能
 - 料金
- AWS Service Catalog を利用したアーキテクチャパターン
- AWS Service Catalog の活用事例
- まとめ

設定の流れ

ポートフォリオ
の作成

製品の追加

制約の追加

ポートフォリオ
へのアクセス
権の追加

設定の流れ: ポートフォリオの作成



ポートフォリオの作成

製品を整理してエンドユーザーに配信するには、ポートフォリオを使用します。ポートフォリオに製品を追加し、アクセス権限を付与して、ユーザーが製品を表示および起動できるようにします。

ポートフォリオ名* 開発環境用ポートフォリオ

わかりやすい ID (最大 100 文字) を入力します。

説明

開発環境で利用できる製品群

ポートフォリオの詳細ページに表示される情報を追加します。

所有者* ITインフラ統括部

ポートフォリオの作成者を示します (最大 50 文字)。

*必須

キャンセル 作成

設定の流れ: 製品の追加



ポートフォリオ: 開発環境用ポートフォリオ /

説明 開発環境で利用できる製品群
所有者 ITインフラ統括部
ポートフォリオ ID [REDACTED]
ポートフォリオ ARN [REDACTED]

▼ 製品

i このポートフォリオに製品はありません

独自の製品を追加するか、AWS Marketplace から製品を選択できます。新しい製品を作成する必要がある場合は、プロセスを完了するために CloudFormation のテンプレートが必要です。

新しい製品のアップロード 製品の追加

名前でフィルター 製品が見つかりません。

製品名	作成時刻	ベンダー	提供元
-----	------	------	-----

この例では、新規に CloudFormationテンプレートをアップロードし、製品としてポートフォリオに追加します

設定の流れ: 製品の追加



手順 1: 製品の詳細の入力

手順 2: サポート詳細の入力

手順 3: バージョンの詳細の入力

手順 4: 確認

製品の詳細の入力

組織内のプライベートな使用のために独自の製品を作成できます。作成した製品は、ポートフォリオに追加してエンドユーザーが使用するようになります。

製品名* 標準Webシステム
例: My Test Product, My Packaged LOB App

説明* 標準的な3層アプリケーションの開発環境

提供元* ITインフラ統括部
製品を公開するユーザーまたは組織を示します。

ベンダー この製品に、公開元とは違うソースがある場合、
のフィールドを設定できます。

製品を作成した会社を追加します。

手順 1: 製品の詳細の入力

手順 2: サポート詳細の入力

手順 3: バージョンの詳細の入力

手順 4: 確認

サポート詳細の入力

この情報により、このアプリケーションを公開する組織が識別されます

連絡先 E メール support@example.com
例: support@mycompany.com

サポートリンク <https://dev-support.example.com>
サポート詳細のためにアプリケーションユーザーに提供されるリンク。

サポートの説明 本製品の不明点に関して
はサポートリンク先の
FAQをご覧ください

製品に関する情報を入力します。ここで入力した内容は、エンドユーザーがみる製品詳細ページに表示されます

設定の流れ: 製品の追加



手順 1: 製品の詳細の入力
手順 2: サポート詳細の入力
手順 3: バージョンの詳細の入力
手順 4: 確認

バージョンの詳細

テンプレートの選択

テンプレートファイルをアップロード
ファイルを選択 development-....nt.template

Amazon CloudFormation のテンプレートで、URL の場所を選択します

バージョンタイトル* v1.0

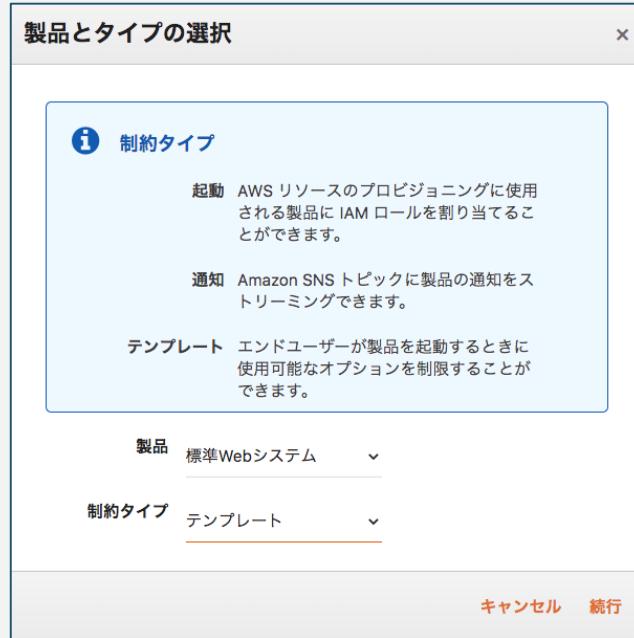
説明 初期リリース|
この説明では、このバージョンと以前のバージョンとの違いを明確に示す必要があります。

*必須

キャンセル 戻る 次へ

製品で利用する CloudFormationテンプレートをアップロードします

設定の流れ: テンプレート制約の追加



テンプレート制約ビルダー

AWS CloudFormation のテンプレートに定義されたパラメータの使用可能な値を絞り込むことにより、エンドユーザーが製品を起動するときに使用できるオプションを制限できます。

説明* この説明では、適用中の制約の概要を示します。

ルールビルダー 制約テキストエディター

テンプレートの制約*

```
{
  "Rules": [
    "Rule": [
      "Assertions": [
        {
          "Assert": {"Fn::Contains": ["t2.micro", "t2.small"]}, {"Ref": "InstanceType"}
        ],
        "AssertDescription": "インスタンスタイプは、t2.micro または t2.small のみ利用可能"
      ]
    ]
  ]
}
```

サンプルの制約

サンプル 1
サンプル 2
サンプル 3

*必須

キャンセル 送信

テンプレート制約を定義します。
この例では、選択可能なインスタンスタイプを制限しています

テンプレート制約の例

```
{  
  "Rules": {  
    "Rule1": {  
      "Assertions": [  
        {  
          "Assert": {  
            "Fn::Contains": [{"t2.micro", "t2.small"}], {"Ref": "InstanceType"}]  
          },  
          "AssertDescription": "Instance type should be t2.micro or t2.small"  
        }  
      ]  
    }  
  }  
}
```

Fn::Contains関数を利用して、"InstanceType"パラメータは、"t2.micro"か"t2.small"でなければならぬと制限をかけている

テンプレート制約ビルダー

この説明では、適用中の制約の概要を示します。

ルールビルダー 制約テキストエディター

名前	ルールの説明
名前*	Rule1
ルールの説明	Instance type should be t2.micro or t2.small
制約事項*	インタラクティブエディタ... パラメータ InstanceType パラメータタイプ String パラメータの説明 EC2 instance type. <input checked="" type="radio"/> 値のリストに含まれている必要があります <input type="radio"/> 値に等しい必要があります 値 t2.micro,t2small

*必須 キャンセル 送信 フィールドのクリア ルールを追加する

シンプルなルールであれば、JSONを書かなくても、ルールビルダーを利用して、簡単にルール設定が可能

より複雑なテンプレート制約の例

```
"Rules" : {  
    "testInstanceType" : {  
        "RuleCondition" : {"Fn::Equals": [{"Ref": "Environment"}, "test"]},  
        "Assertions" : [  
            {  
                "Assert" : { "Fn::Contains" : [ ["m1.small"], {"Ref" : "InstanceType"} ] },  
                "AssertDescription" : "For the test environment, the instance type must  
be m1.small"  
            }  
        ]  
    }  
}
```

RuleConditionを利用すると特定の条件に合致する場合のみルールを適用することが可能

テンプレート制約のルールの構文や利用可能なルール関数はドキュメントを参照ください

https://docs.aws.amazon.com/ja_jp/servicecatalog/latest/adminguide/catalogs_constraints_template-constraints.html

設定の流れ: 起動制約の追加



製品とタイプの選択

i 制約タイプ

起動AWSリソースのプロビジョニングに使用される製品にIAMロールを割り当てることができます。

通知Amazon SNSトピックに製品の通知をストリーミングできます。

テンプレートエンドユーザーが製品を起動するときに使用可能なオプションを制限することができます。

製品 標準Webシステム

制約タイプ 起動

キャンセル 続行

起動の制約

起動時にリソースをプロビジョニングするために使用されるIAMロールを割り当て、ユーザーがカタログから製品をプロビジョニングします。

IAM ロール Dev_WebAP_Role

ロールの ARN を入力します

説明 開発環境用Webアプリケーション用のロールを利用して起動

この説明では、適用中の制約の概要を示します。

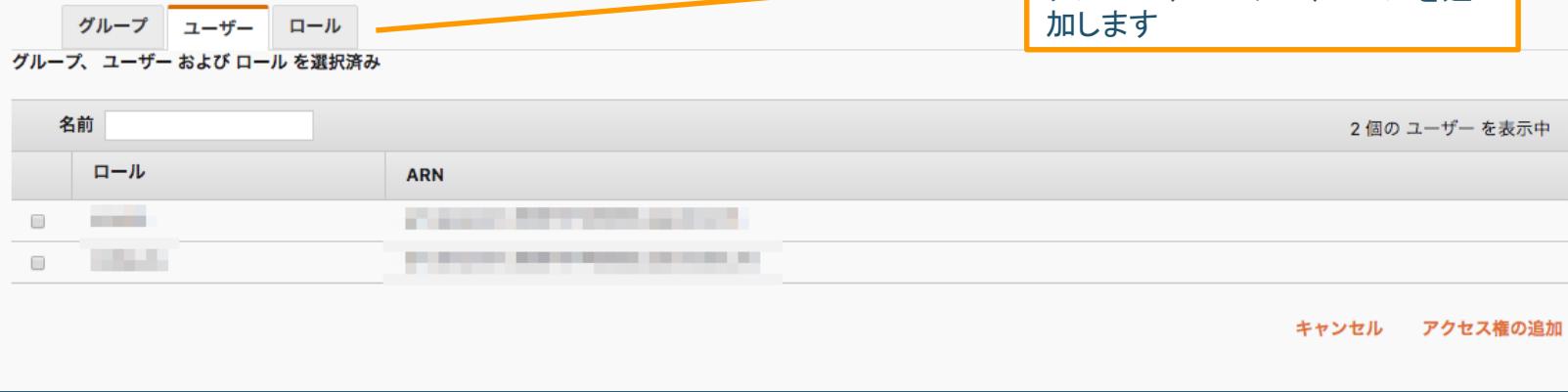
製品の起動時に、ここで指定したIAMロールを利用して製品を起動します。

設定の流れ: ポートフォリオの作成



開発環境用ポートフォリオ用にユーザー、グループ、およびロールを追加

アカウントで、ポートフォリオにアクセスし、そのアプリケーションを表示および起動できるユーザーを選択します。



ポートフォリオにアクセスさせたい
グループ、ユーザー、ロールを追
加します

名前	2 個の ユーザー を表示中	
ロール	ARN	
awsuser1	arn:aws:iam::123456789012:root	
awsuser2	arn:aws:iam::123456789012:root	

キャンセル アクセス権の追加

ユーザーによるポータルへのアクセス: 製品リスト

三 製品リスト	古い外観に戻す	
サーチ	並べ替え	
例:名前	製品名 ▼	
製品名	ベンダー	
所有者	説明	
標準Webシステム	ITインフラ統括部	標準的な3層アプリケーションの開発環境

ユーザーによるポータルへのアクセス: 製品詳細

The screenshot shows a product details page with the following elements:

- Header:** 製品リスト - 製品の詳細 (Product List - Product Details) and 古い外観に戻す (Return to Old Look).
- Product Summary:** 標準Webシステム (Standard Web System) icon and description: 標準的な3層アプリケーションの開発環境 (Development environment for standard 3-layer application).
- Product Information:** 所有者 (Owner): ITインフラ統括部; Distributor: None listed.
- Contact & Support:** 連絡先 E メール (Contact Email): support@example.com; サポートリンク (Support Link): <https://dev-support.example.com>; サポートの説明 (Support Description): 本製品の不明点に関してはサポートリンク先のFAQをご覧ください (For details, please refer to the FAQ on the support link).
- Action Buttons:** A large orange box highlights the "製品の起動リンクをクリックしてこの製品を起動します" (Click the product start link to start this product) text, which points to the "製品の起動" (Start Product) button.
- Version History:** A table showing one version entry: v1.0, Jul 12th 2018 10:18:39 UTC..., 初期リリース (Initial Release).
- Startup Options:** A section titled "起動オプション (1)" (Startup Options (1)) containing "起動オプション - 1" (Startup Option - 1).

An orange callout box on the right side states: 製品の作成時に入力した情報が表示されます (The information entered during product creation is displayed).

ユーザーによるポータルへのアクセス: 製品の起動

The screenshot shows the AWS CloudFormation Launch Wizard interface. On the left, a sidebar lists steps: 1. Product Version, 2. Parameters, 3. Tag Options, 4. Notifications, and 5. Confirmation. The main area is divided into two sections: 'Product Version' and 'Launch - Standard Web System'.

Product Version: A step where the user selects a product version. It includes a table with columns 'Name' (v1.0), 'Version' (v1.0), and 'Source' (IT Infra Structure). A note states: "The selected product is a single unit, so it is projected as a product." A required field indicator (*必須) is present.

Launch - Standard Web System: This section is titled 'Launch - Standard Web System'. It contains the following steps:

- Step 1: Product Version:** Shows the selected product version 'Dev_WebAP_System'.
- Step 2: Parameters:** A step where users can specify parameter values or use default values. It includes a note: "Specify the parameter value or use the default value." A sub-section 'Instance Configuration' shows 'Server size: t2.micro'.
- Step 3: Tag Options:**
- Step 4: Notifications:**
- Step 5: Confirmation:**

An orange callout box highlights the 'Server size' dropdown in the 'Instance Configuration' section, which is set to 't2.micro'. The text inside the callout box reads: "テンプレート制約で制限を受けたインスタンスタイプのみが選択肢として表示されます" (Only instance types constrained by the template are displayed as options).

At the bottom right of the main window, there are buttons: キャンセル (Cancel), 戻る (Back), and 次へ (Next).

ユーザーによるポータルへのアクセス:製品の起動

起動 - 標準Webシステム

手順 1: 製品バージョン
手順 2: パラメータ
手順 3: TagOptions
手順 4: 通知
手順 5: 確認

TagOption

次の TagOption は、管理者によって製品またはポートフォリオに追加されています。一部の TagOption には複数の値があり、最も該当する値の選択を求められる場合があります。[詳細はこちら。](#)

キー (最大 127 文字)	値 (最大 255 文字)
新しいキー	新しい値

起動されるAWSリソース (EC2など)に、TagOptionで指定したタグが付与される

キャンセル 戻る 次へ

ユーザーによるポータルへのアクセス: プロビジョニングされた製品のリスト

プロビジョニングされた製品のリスト				古い外観に戻す
サーチ	Filter by	並べ替え		
例:名前	ユーザー	ID		
プロビジョニングされた製品名	作成時刻	状況	状況メッセージ	
Dev_WebAP_SystemA	2018-07-12 10:50:37 UTC+0900	UNDER_CHANGE		

ユーザーによるポータルへのアクセス: プロビジョニングされた製品の詳細

Dev_WebAP_SystemA

Internal App

状態 利用可能
製品 標準Webシステム
バージョン v1.0
提供元 ITインフラ統括部

▼ イベント (1)

状況	タイプ	イベントメッセージ
成功	PROVISION_PRODUCT	Record ID:rec-vqezfzcjzqwg プロビジョニングされた製品の ID:pp-ntz24byqig6ee ▼ 出力:

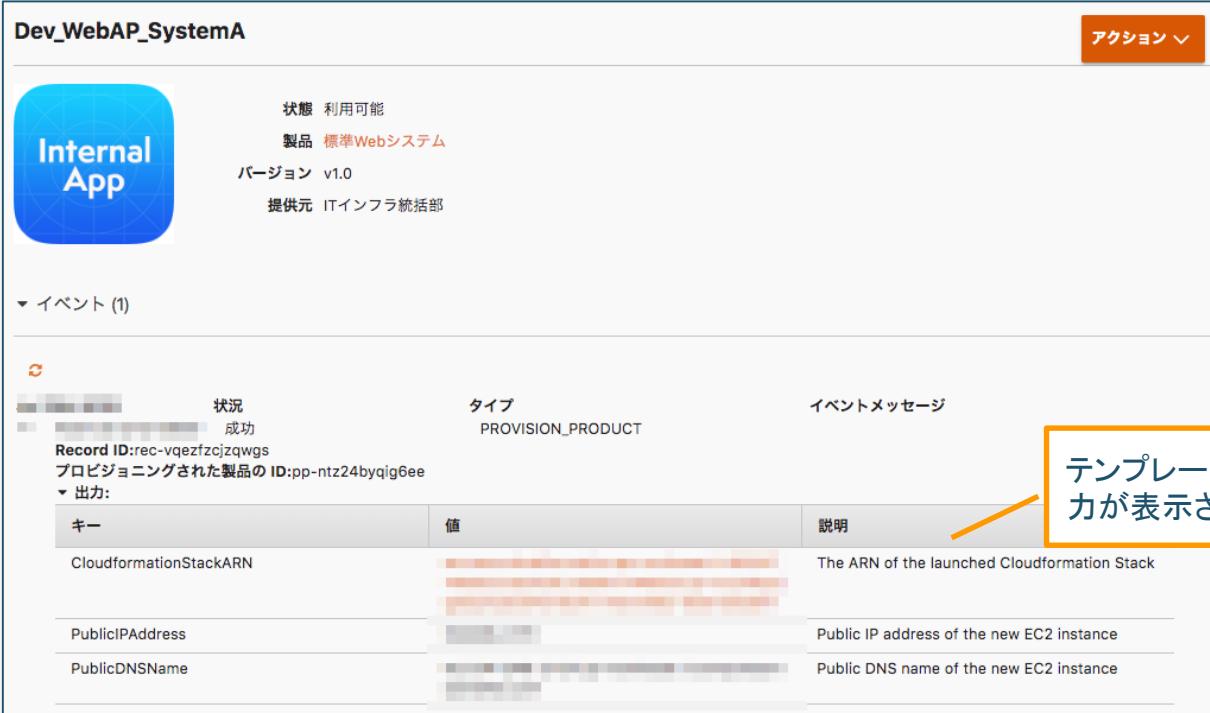
キー 値 説明

CloudformationStackARN [REDACTED] The ARN of the launched Cloudformation Stack

PublicIPAddress [REDACTED]

PublicDNSName [REDACTED]

テンプレートで定義された出力が表示される

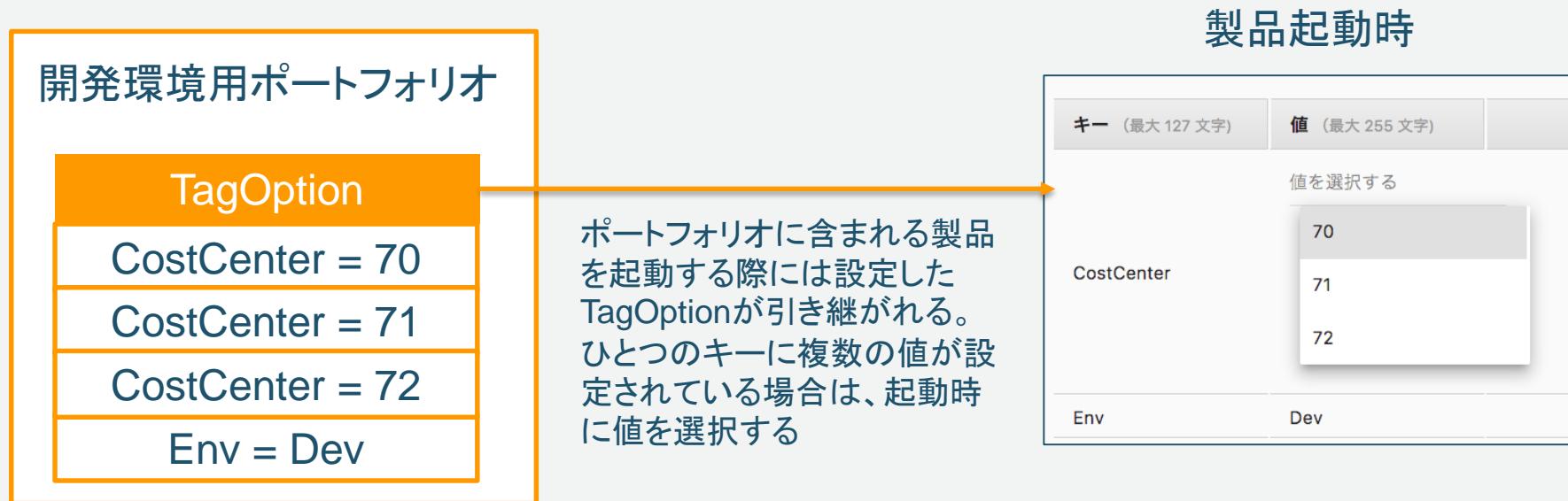


Agenda

- はじめに
- AWS Service Catalog の機能概要
 - 用語と概念
 - 設定方法
 - 各種機能
 - 料金
- AWS Service Catalog を利用したアーキテクチャパターン
- AWS Service Catalog の活用事例
- まとめ

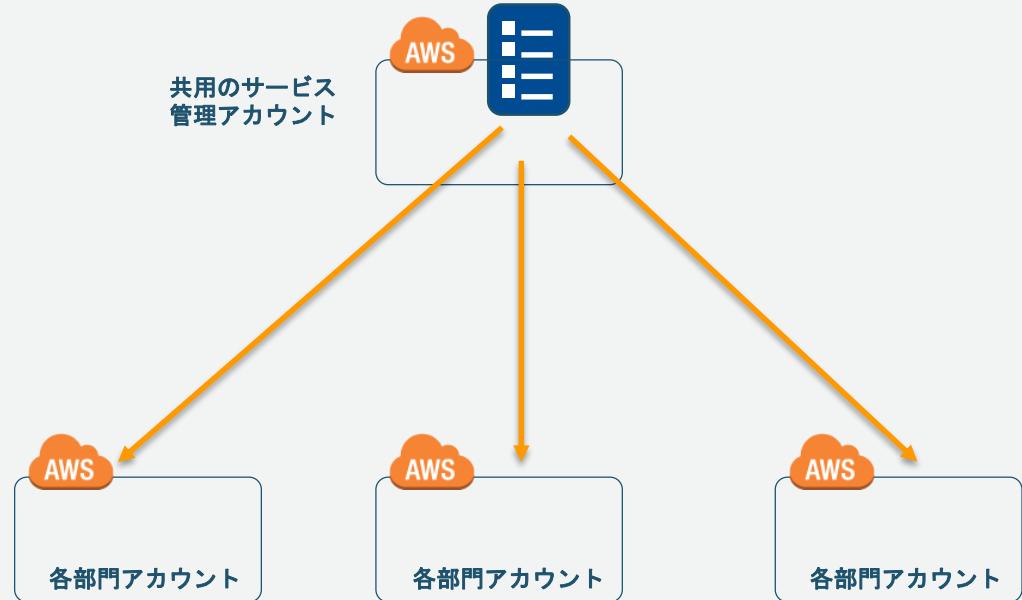
TagOptionライブラリ

- ポートフォリオや製品に対してTagOptionを指定し、製品起動時に設定したTagOptionが引き継がれる仕組み
- リソースのタグを統一的に付与するのに役立つ



アカウント間でのポートフォリオの共有

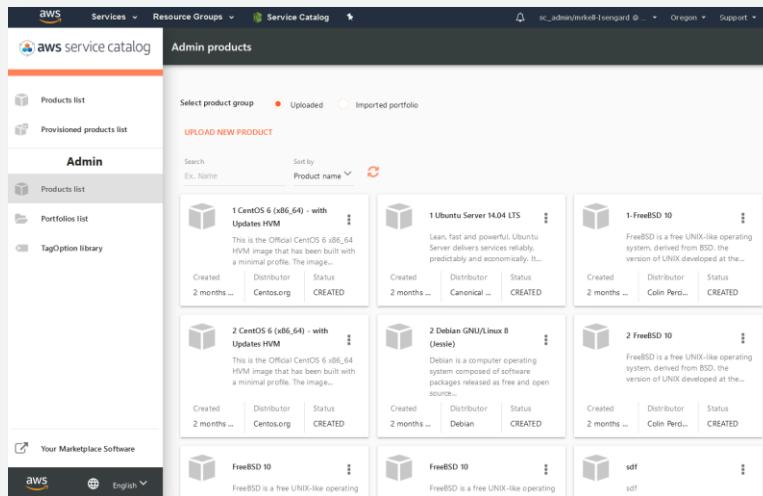
- ・アカウント間でポートフォリオの共有が可能
- ・テンプレート制約、起動制約も継承される
- ・共有されたポートフォリオからローカルのポートフォリオに製品をコピーすることで、起動制約は上書き可能



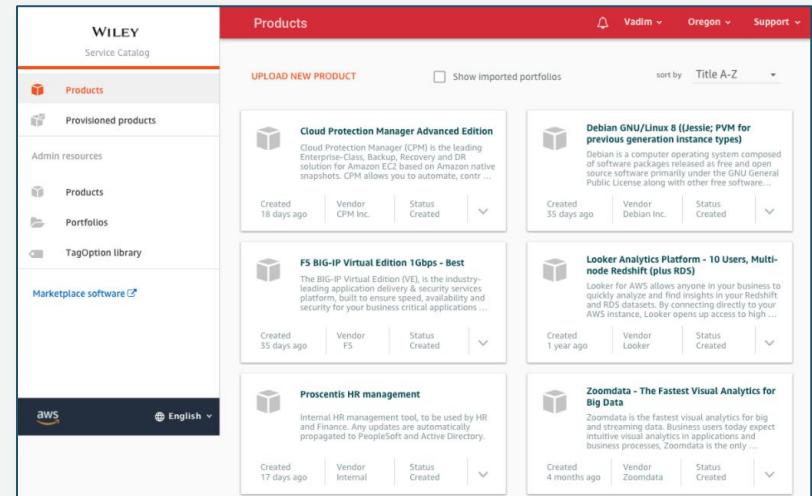
AWS Service Catalogでコンソールのルックアンドフィールのカスタマイズ

コンソールのロゴや配色などがカスタマイズ可能となった
ポータルなどの社内システムからのアクセス時にシームレスなユーザ一体
験を提供可能

デフォルトのコンソール画面



カスタマイズされたコンソール画面

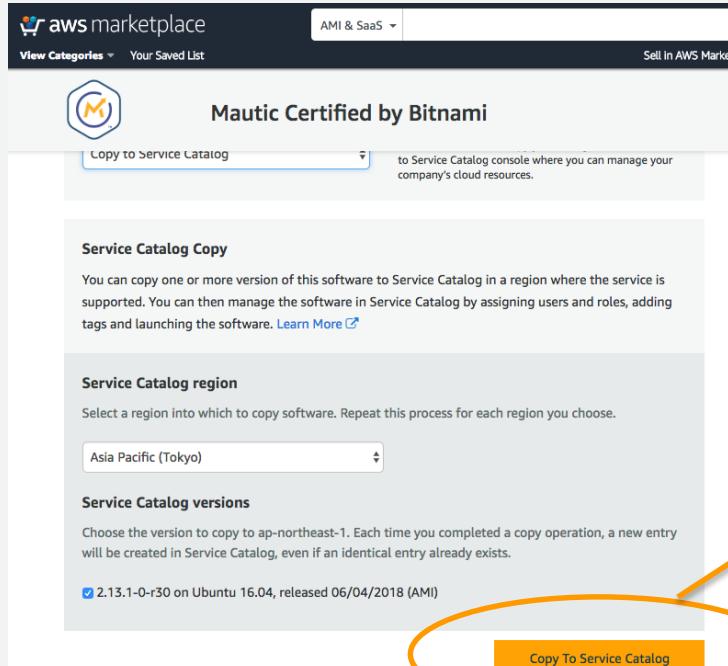


<https://aws.amazon.com/jp/about-aws/whats-new/2018/03/aws-service-catalog-launches-brand-your-console-to-deliver-a-customizable-user-experience/>



連携機能: Marketplace

AWS Marketplace



Mautic Certified by Bitnami

Copy to Service Catalog

Service Catalog Copy

You can copy one or more version of this software to Service Catalog in a region where the service is supported. You can then manage the software in Service Catalog by assigning users and roles, adding tags and launching the software. [Learn More](#)

Service Catalog region

Select a region into which to copy software. Repeat this process for each region you choose.

Asia Pacific (Tokyo)

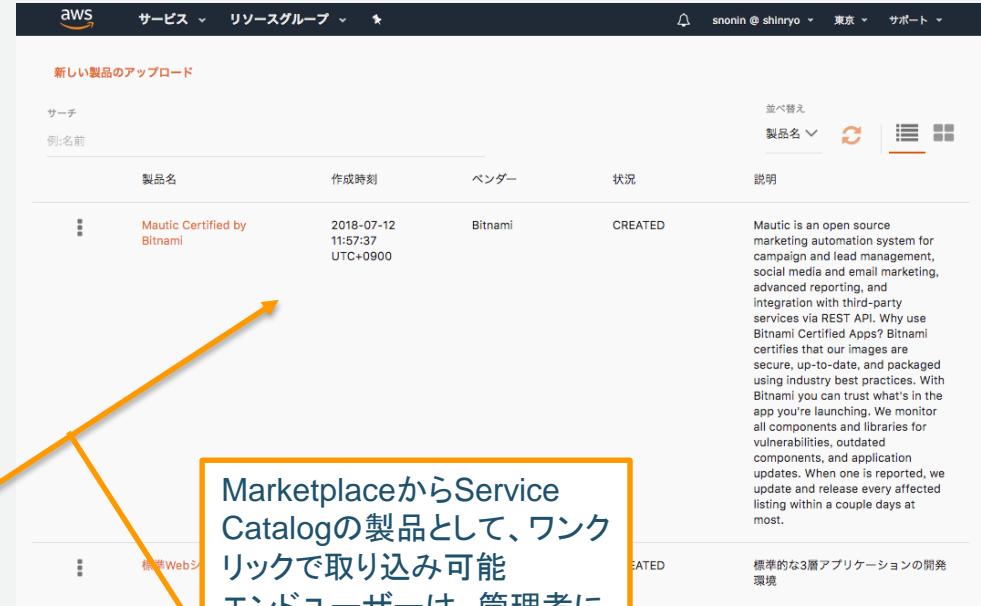
Service Catalog versions

Choose the version to copy to ap-northeast-1. Each time you completed a copy operation, a new entry will be created in Service Catalog, even if an identical entry already exists.

2.13.1-0-r30 on Ubuntu 16.04, released 06/04/2018 (AMI)

Copy To Service Catalog

Service Catalogの製品管理画面

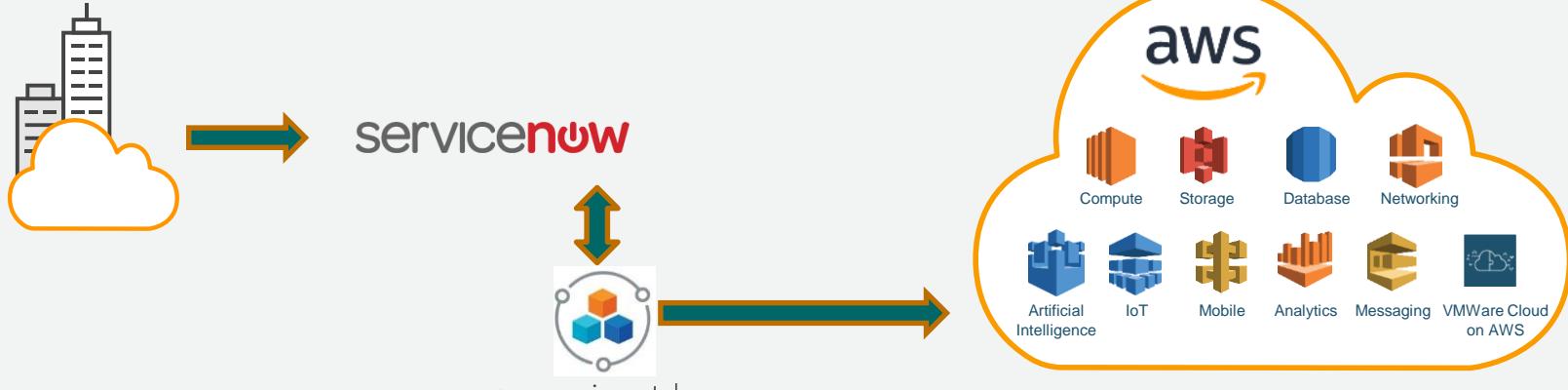


新しい製品のアップロード

名前	作成時刻	ベンダー	状況	説明
Mautic Certified by Bitnami	2018-07-12 11:57:37 UTC+0900	Bitnami	CREATED	Mautic is an open source marketing automation system for campaign and lead management, social media and email marketing, advanced reporting, and integration with third-party services via REST API. Why use Bitnami Certified Apps? Bitnami certifies that our images are secure, up-to-date, and packaged using industry best practices. With Bitnami you can trust what's in the app you're launching. We monitor all components and libraries for vulnerabilities, outdated components, and application updates. When one is reported, we update and release every affected listing within a couple days at most.

MarketplaceからService Catalogの製品として、ワンクリックで取り込み可能
エンドユーザーは、管理者により許可されたMarketplaceの製品をService Catalogから起動できる

連携機能: ServiceNow



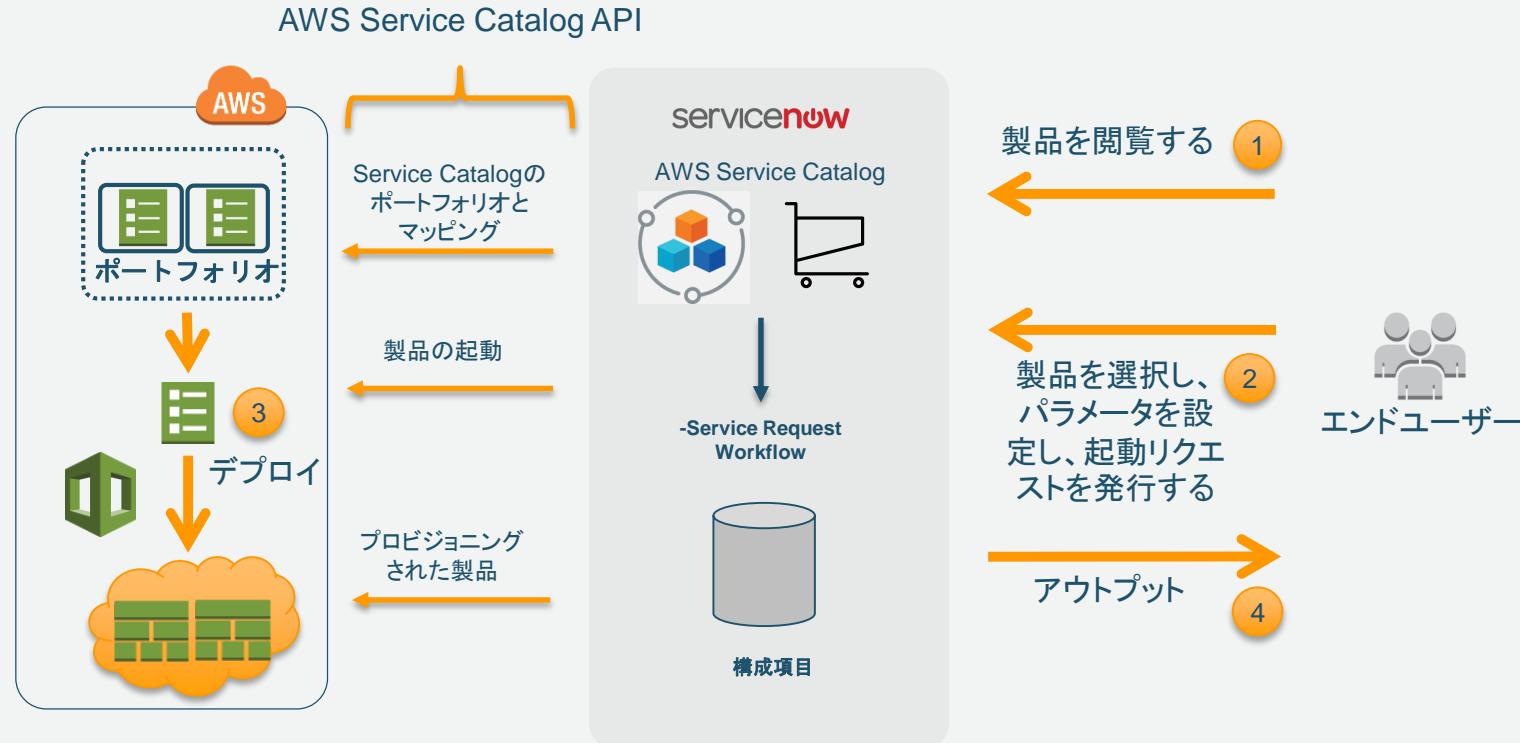
ServiceNow
ユーザーは
AWSのサービスを
ServiceNow経由で
閲覧し、リクエスト

aws service catalog
Service Catalog カタ
ログ管理者は、利用
可能なAWSサービス
を管理する

運用管理者は
AWSサービスを監
視・運用する

連携機能: ServiceNow

エンドユーザーの処理の流れ



Agenda

- はじめに
- AWS Service Catalog の機能概要
 - 用語と概念
 - 設定方法
 - 各種機能
 - 料金
- AWS Service Catalog を利用したアーキテクチャパターン
- AWS Service Catalog の活用事例
- まとめ

料金

- ポートフォリオ毎に1ヶ月あたり 5 USD
- 1人以上のユーザーが割り当てられたポートフォリオが課金対象
- 割り当てられた製品やユーザーの数、製品起動数によって料金は変動しない

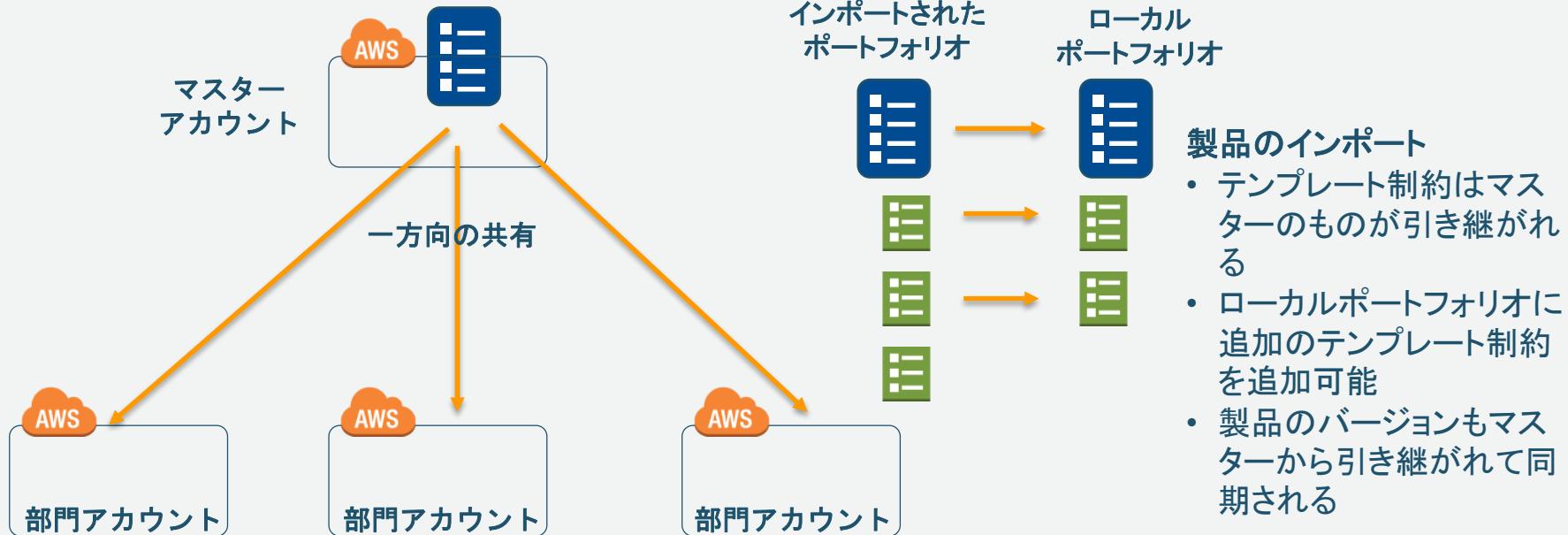
<https://aws.amazon.com/jp/servicecatalog/pricing/>

Agenda

- はじめに
- AWS Service Catalog の機能概要
 - 用語と概念
 - 設定方法
 - 各種機能
 - 料金
- AWS Service Catalog を利用したアーキテクチャパターン
- AWS Service Catalog の活用事例
- まとめ

Hub-Spoke パターン

マスター アカウントで製品を一元的に管理。各アカウントは、共有されたポートフォリオから、ローカルポートフォリオに製品をコピーして利用



Consumer – Creator – Managerパターン

役割ごとに権限を分割する

セルフサービスを促進するためにCreatorが、Service Catalogの管理などを行う



Consumers



Creators



Managers

典型的には開発者

- Service Catalogのエン
ドユーザー権限
- ログや監視の参照権限

典型的にはリリース管理
者/自動化担当者

- Service Catalogの管理
者権限
- ログや監視のアラーム・
ダッシュボードの作成権
限

典型的にはAWS管理者

- AWSの管理者権限

Agile Governance パターン

製品に対するテンプレート制約を動的に追加するパターン



Baseline Setup –VPC、サブネット、セキュリティグループ、踏み台などを作成



Linux Server

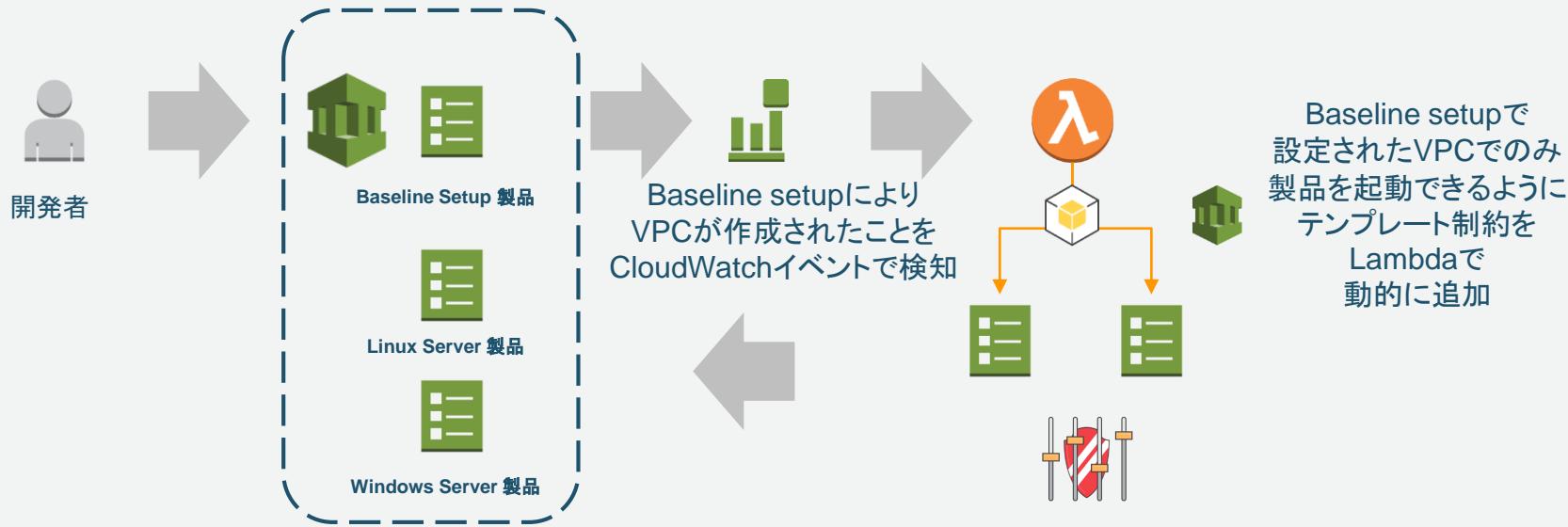


Windows Server



サーバーの起動をBaselineで作成された
VPCやサブネットに制限したい

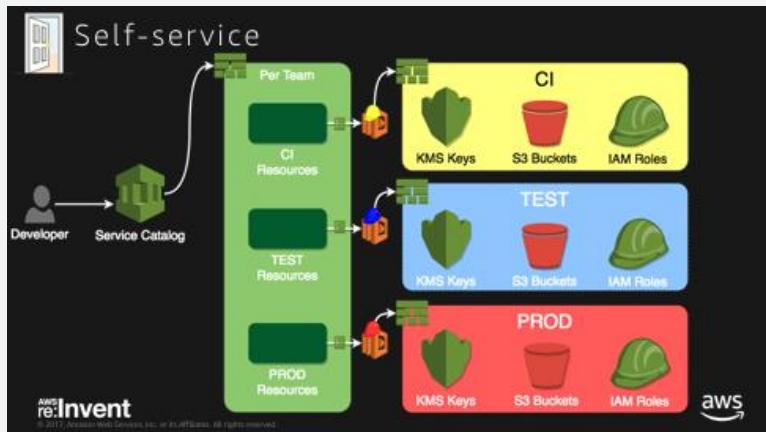
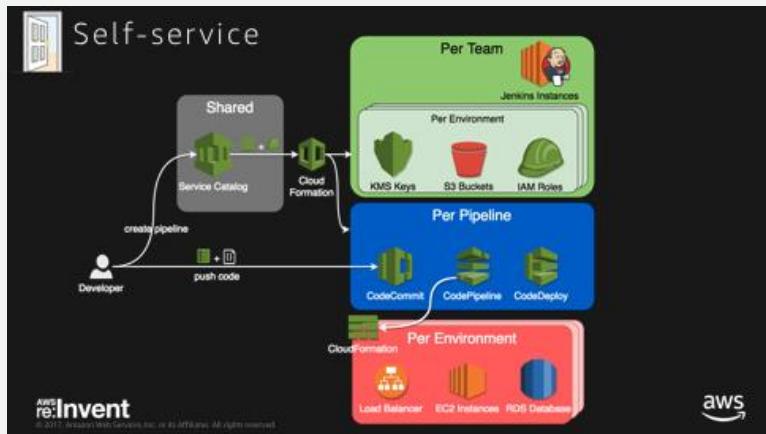
Agile Governance パターン



Agenda

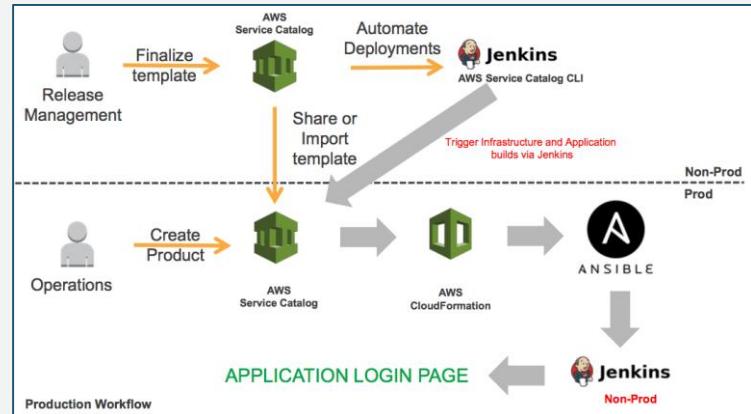
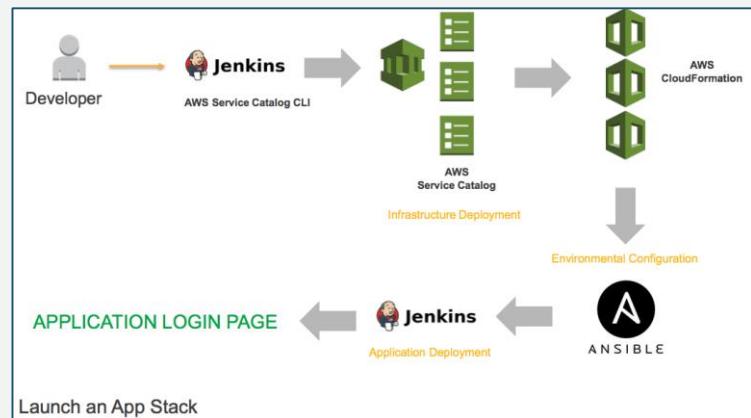
- はじめに
- AWS Service Catalog の機能概要
 - 用語と概念
 - 設定方法
 - 各種機能
 - 料金
- AWS Service Catalog を利用したアーキテクチャパターン
- AWS Service Catalog の活用事例
- まとめ

- re:Invent 2017 で講演
 - Using AWS to Achieve Both Autonomy and Governance at 3M (DEV332)
 - <https://www.youtube.com/watch?v=tSZZC1cf4h8>
 - <https://www.slideshare.net/AmazonWebServices/dev332using-aws-to-achieve-both-autonomy-and-governance-at-3m>
- 開発者がセルフサービスで継続的デリバリの環境を構築するために利用



John Wiley & Sons

- re:Invent 2016 で講演
 - Enabling DevOps for an Enterprise with AWS Service Catalog (DEV321)
 - <https://www.youtube.com/watch?v=J6XeDtCuERM>
 - <https://www.slideshare.net/AmazonWebServices/aws-reinvent-2016-enabling-devops-for-an-enterprise-with-aws-service-catalog-the-john-wiley-sons-journey-with-aws-professional-services-dev321>
- AWS Service CatalogとAnsible、Jenkinsを組み合わせて、開発環境のプロビジョニングをセルフサービス化し、本番環境のプロビジョニングのフローも自動化



Fannie Mae

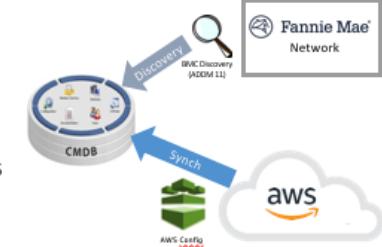
- re:Invent 2017 で講演
 - Building end-to-end IT Lifecycle Mgmt & Workflows with AWS Service Catalog (MSC201)
 - https://www.youtube.com/watch?v=rbGGGoUnp_Q
 - <https://www.slideshare.net/AmazonWebServices/building-endtoend-it-lifecycle-mgmt-workflows-with-aws-service-catalog-msc201-reinvent-2017>
- ServiceNowとAWS Service Catalogを組み合わせて、オンプレミスとAWS双方を統合してITサービスマネジメントを実現

MyServices ServiceNow Based Solution



AWS to CMDB Synchronization (1 of 2)

- BMC Discovery (ADDM 11) is used to discover IT assets on the Fannie Mae network
- ADDM 11 cannot discover AWS IT assets as they are outside the corporate network
- Custom solution built using native AWS Config services, which synchronizes AWS resources with the CMDB



Agenda

- はじめに
- AWS Service Catalog の機能概要
 - 用語と概念
 - 設定方法
 - 各種機能
 - 料金
- AWS Service Catalog を利用したアーキテクチャパターン
- AWS Service Catalog の活用事例
- まとめ

まとめ

- AWS Service Catalogを利用してすることで、ガバナンスやセキュリティを担保しながら、開発者などがセルフサービスでAWS環境を迅速にプロビジョニングできるようになります
- エンタープライズ組織で、統制をとりながらDevOpsを推進するためのツールとして活用されています

参考資料

- AWS Service Catalog 製品ページ
<https://aws.amazon.com/jp/servicecatalog/>
- ドキュメント
<https://aws.amazon.com/jp/documentation/servicecatalog/>
- Forum
<https://forums.aws.amazon.com/forum.jspa?forumID=198>
- Blog
<https://aws.amazon.com/jp/blogs/mt/category/management-tools/aws-service-catalog/>

オンラインセミナー資料の配置場所

AWS クラウドサービス活用資料集

- <https://aws.amazon.com/jp/aws-jp-introduction/>



Amazon Web Services ブログ

- 最新の情報、セミナー中のQ&A等が掲載されています。
- <https://aws.amazon.com/jp/blogs/news/>

公式Twitter/Facebook AWSの最新情報をお届けします



@awscloud_jp



検索

もしくは
<http://on.fb.me/1vR8yWm>

最新技術情報、イベント情報、お役立ち情報、
お得なキャンペーン情報などを日々更新しています！

AWSの導入、お問い合わせのご相談

AWSクラウド導入に関するご質問、お見積、資料請求をご希望のお客様は以下のリンクよりお気軽にご相談下さい。

<https://aws.amazon.com/jp/contact-us/aws-sales/>

お問い合わせ

日本担当チームへのお問い合わせ >

関連リンク

フォーラム

日本担当チームへのお問い合わせ

AWS クラウド導入に関するご質問、お見積り、資料請求をご希望のお客様は、以下のフォームよりお気軽にご相談ください。平日営業時間内に日本オフィス担当者よりご連絡させていただきます。

※ご請求金額またはアカウントに関する質問は[こちらからお問い合わせください](#)。
※Amazon.com または Kindle のサポートに問い合わせは[こちらからお問い合わせください](#)。

アスタリスク (*) は必須情報となります。

姓*

名*

※「AWS 問い合わせ」で検索して下さい。

AWS Well Architected 個別技術相談会お知らせ

- Well Architectedフレームワークに基づく数十個の質問項目を元に、お客様がAWS上で構築するシステムに潜むリスクやその回避方法をお伝えする個別相談会です。

<https://pages.awscloud.com/well-architected-consulting-jp.html>

- 参加無料
- 毎週火曜・木曜開催

【毎週火、木曜開催】 AWS Well-Architected 個別技術相談会

AWS 上で構築するシステムのリスクの把握・回避方法をご希望のお客様

この度 AWS をご活用頂いているお客様を対象に「AWS Well-Architected 個別技術相談会」を開催致します。

Well-Architected 個別技術相談会では、リスクの把握・回避を目的として、セキュリティ・信頼性・パフォーマンス・コスト・運用の5つの観点で、お客様の AWS 活用状況や構成についてお伺いします。AWS のベストプラクティスに基づき作成された Well-Architected フレームワークを元に、今までお客様がお気づきでなかったリスクや AWS 活用の改善点を見つけることができます。例えば、自動車においては納車前点検、車検を定期的に行うのと同様に、本相談会はお客様の AWS 上のシステムをよりよく活用頂くことを目的にしております。

» 説明資料(PDF) [AWS Well-Architected Framework -クラウド設計・運用ベストプラクティスの活用-]

Well-Architected 個別技術相談会にご参加頂くには、本ページにてお申込み後、弊社担当者からお送りするヒアリングシートにご記入・担当者にご送付頂く必要があります。その内容を元に、当日の相談会では AWS のソリューションアーキテクトと共に技術的なディスカッションをさせて頂きます。また、遠方のお客様、アマゾン東京オフィスへのご来社が時間等の関係で難しいお客様は、Web のプレインテーションツールや、お電話を活用いたりメールでのご相談も承ります。



下記のフォームよりお申込みください。

* 姓:

* 名:





AWS Cloud Development Kit (CDK)

Basic #1

概要

高野 賢司

Solutions Architect

2023/07



こうの けんじ
高野 賢司

ソリューションアーキテクト @名古屋
アマゾンウェブサービスジャパン合同会社

Baseline Environment on AWS (BLEA) 開発者

<https://github.com/aws-samples/baseline-environment-on-aws>

好きな AWS サービス： AWS CDK

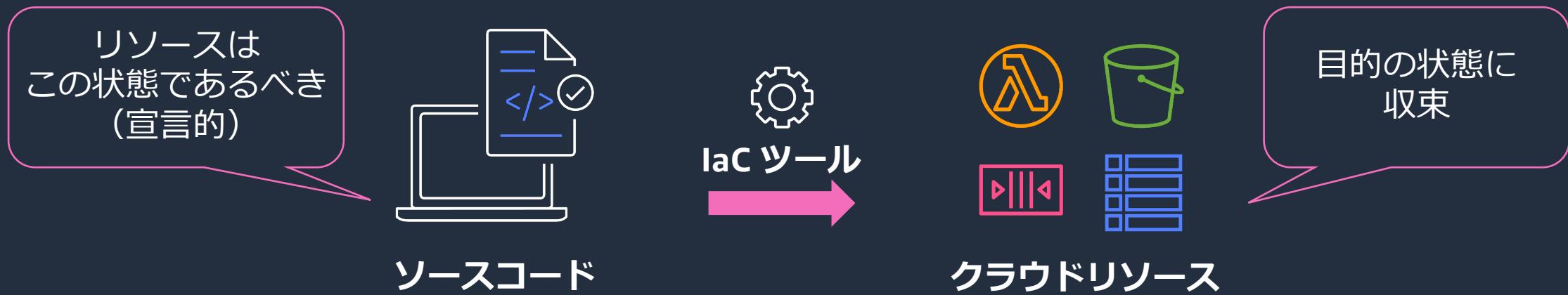
アジェンダ

1. AWS Cloud Development Kit (CDK) とは
2. AWS CDK のコンセプト
3. AWS CDK と他のサービスの連携
4. TypeScript での開発の流れ
5. 各言語におけるプロジェクト構成
6. デモ（TypeScript でのプロジェクト作成～Amazon VPC をデプロイ）
7. AWS CDK の学習リソース

AWS Cloud Development Kit (CDK) とは

Infrastructure as Code (IaC) とは？

手動ではなく、コードによって
インフラストラクチャの管理やプロビジョニングを行うプロセス

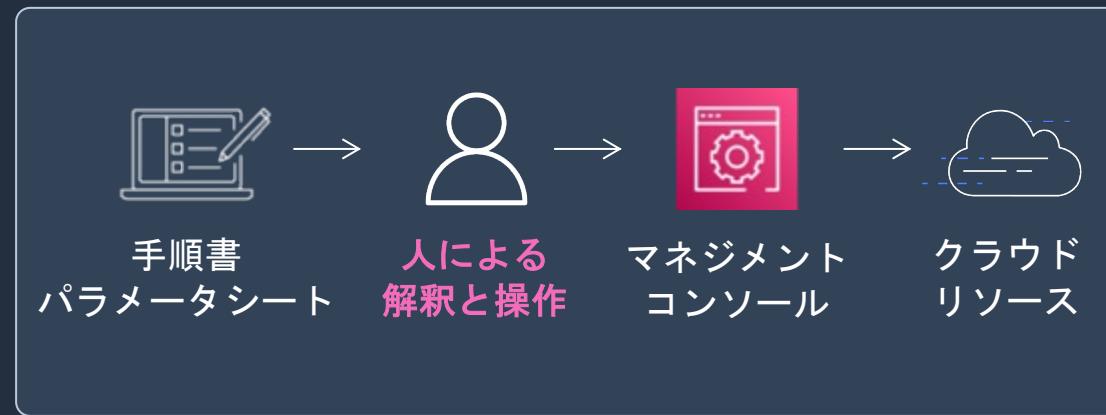


ソフトウェア開発のプラクティスをインフラ構築の自動化に活かす
継続的デリバリーに必須の技術のひとつ

<https://docs.aws.amazon.com/whitepapers/latest/introduction-devops-aws/infrastructure-as-code.html>

なぜ Infrastructure as Code (IaC) が必要なのか？

手動操作（マネジメントコンソール）



スクリプト (CLI, SDK)



手動操作と手続き型スクリプトの課題

- 現在の状態がわからずリリースしづらい
- 人による解釈違いや操作ミスのリスクあり
- 何度も同じ構成を作るのが大変
- 手順書やスクリプトの作成に時間がかかり継続的な更新やテストが困難（陳腐化）
- リソースの状態による判断やエラー処理、ロールバックを網羅しづらい

Infrastructure as Code (IaC) のメリット



コスト削減

- 手順書の作成、メンテナンス、引継ぎコストを削減
- 手順書と実環境の乖離によるブラックボックス化を防止
- デプロイ作業時間を削減
- 必要なときにリソースを作成、まとめて破棄

スピードアップ

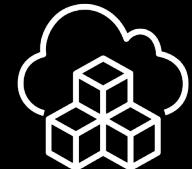
- CI/CD で自動テスト、デプロイ
- 変更を予測可能にして頻繁にデプロイ
- 同じ構成を何度もデプロイ
- 構成パターンとベストプラクティスの共有

リスク低減

- 人的ミスの排除
- バージョン管理による変更の追跡と承認プロセス
- 信頼できる唯一の情報源としての Git リポジトリ
- 必要に応じて前のバージョンにロールバック

AWS Cloud Development Kit (CDK)

<https://github.com/aws/aws-cdk>



AWS CDK

使い慣れたプログラミング言語で
クラウドリソースを定義できる
OSSのフレームワーク



開発者体験を改善

- ・ アプリと同じ言語で記述でき
ドメイン固有言語の習得が不要
- ・ ソフトウェア開発の技法と
プラクティス、ツールを活用
- ・ 型付けとバリデーションで
素早くフィードバックを得る
- ・ リソースとスタックの依存関係を
自動的に解決

アプリ全体をコードで定義

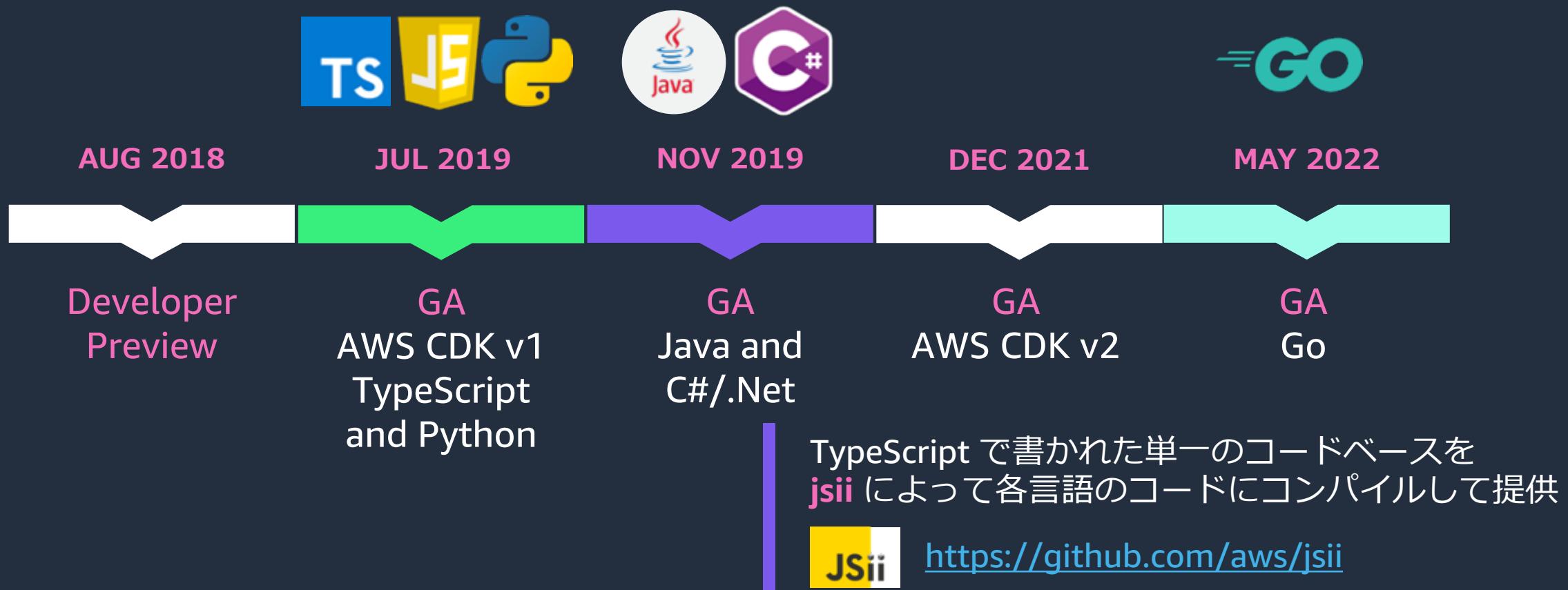
- ・ クラウドリソースだけでなく
AWS Lambda 関数のコードや
コンテナイメージなど
アプリ全体をまとめて管理
- ・ CI/CD パイプラインを自動構築
- ・ 複数の AWS アカウントに
またがる環境を管理

高レベルの抽象化

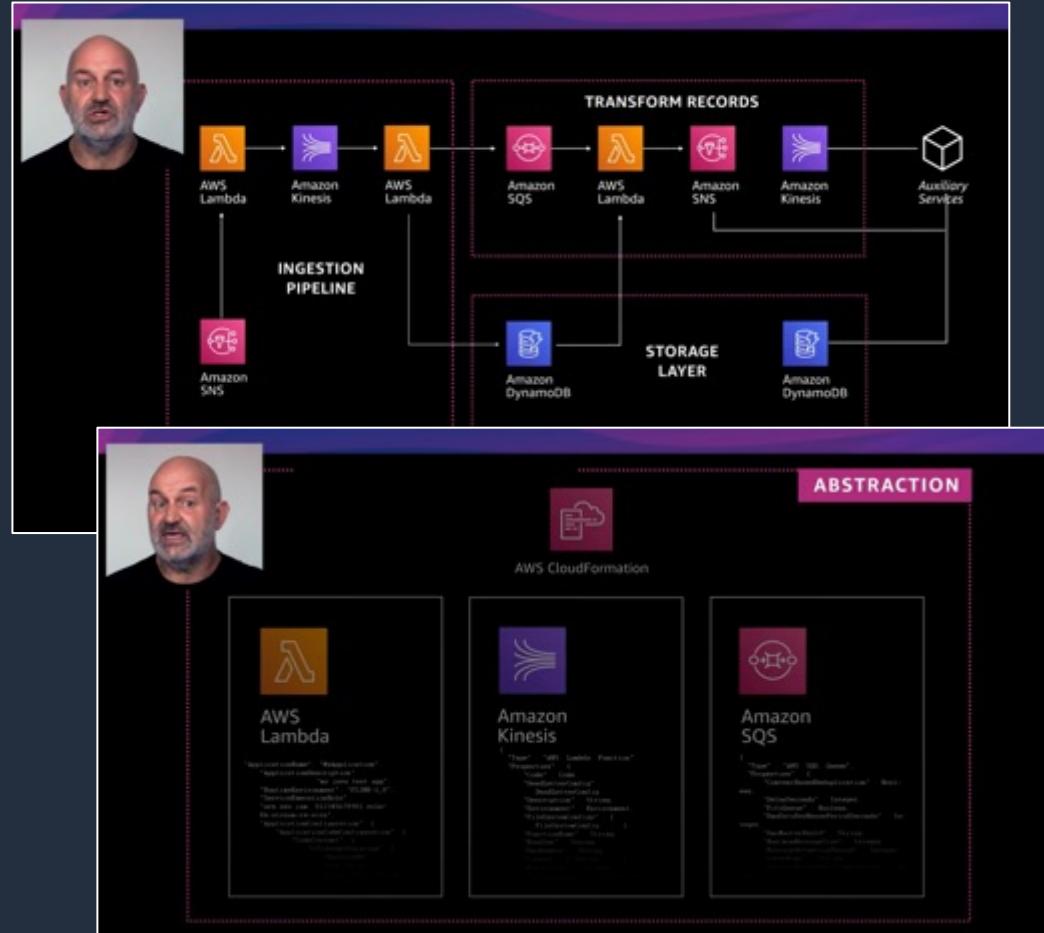
- ・ 複雑な設定を抽象化し
コード量と学習コストを削減
- ・ いつでも抽象化から抜け出して
個別の設定にアクセス可能
- ・ ベストプラクティスに基づく
デフォルト値と設定を提供
- ・ チームの構成パターンや
ガードレールを共有・再利用



6つのプログラミング言語をサポート



なぜ Amazon は AWS CDK を作ったか？



Amazon.com の検索システムを再構築し
トレンド商品をリアルタイムに特定したい。

AWS CloudFormation で構築していたが . . .

- 複数のチームが独立して開発・デプロイ可能にするために**モジュール化**したい
- 繰り返し複雑なものを作成することを避けるために**抽象化**したい
- JSON や YAML のような設定言語よりも
自分たちの**アイデア**を表現できる言語を使いたい

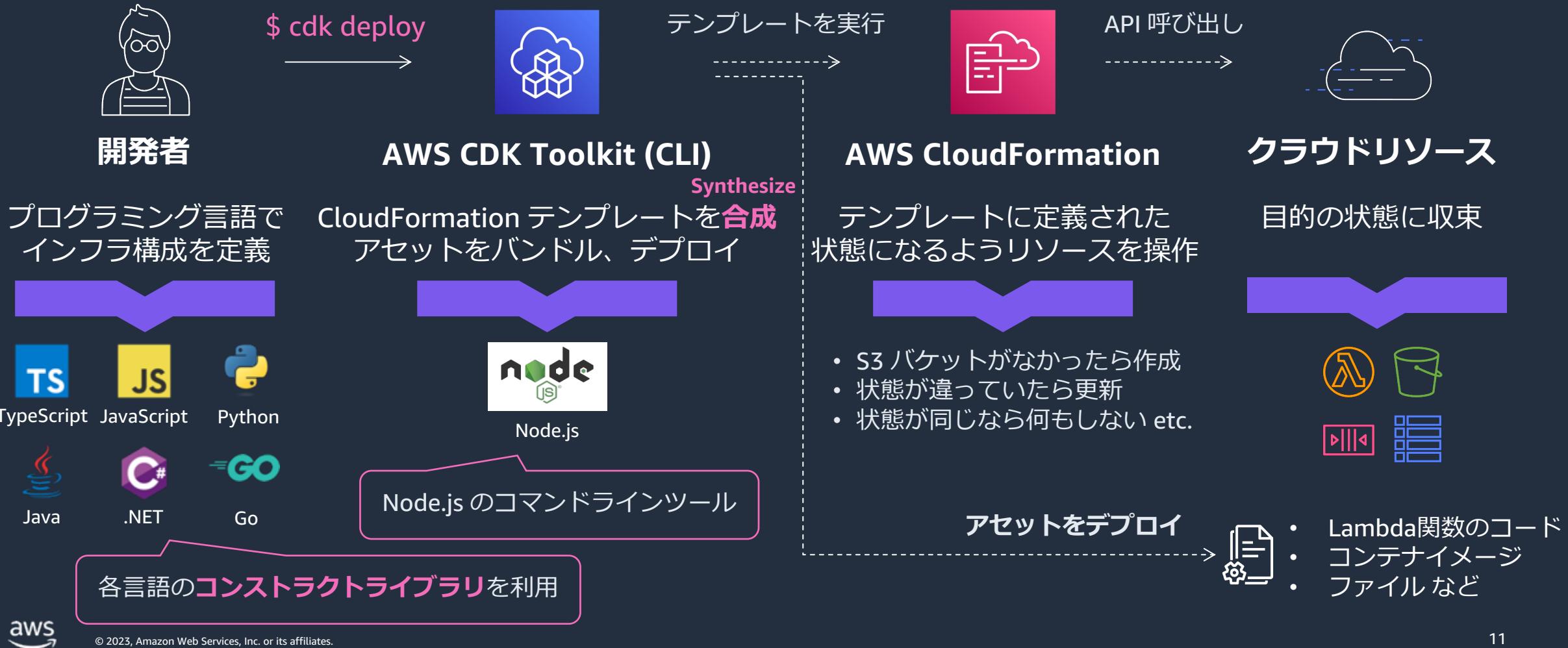


これらの課題を解決するために作成された
オブジェクト指向ライブラリが AWS CDK の起源。

AWS の社内で CDK はデファクトスタンダードになった

<https://www.youtube.com/watch?v=AYYTrDaEwLs>

AWS CDK のしくみ



AWS CDK v2

2021年12月リリース

- コンストラクトライブラリを1つのモノリシックなパッケージに統合。依存関係の管理が容易に
- Semantic Versioning に準拠し安全にアップデート可能に
- v2へのマイグレーションガイドを提供
https://docs.aws.amazon.com/ja_jp/cdk/v2/guide/migrating-v2.html

experimental / deprecated なAPIを使っていなければパッケージのインポートを修正するだけ



The screenshot shows a comparison of dependency files for AWS CDK v1 and v2. The v1 file lists many specific AWS services like core, apigateway, autoscaling, dynamodb, cloudwatch, etc., each at version 1.127.0. The v2 file lists constructs and aws-iot-alpha at versions 2.0.0 and 2.0.0-alpha.0 respectively. Both files import App and Stack from the core module.

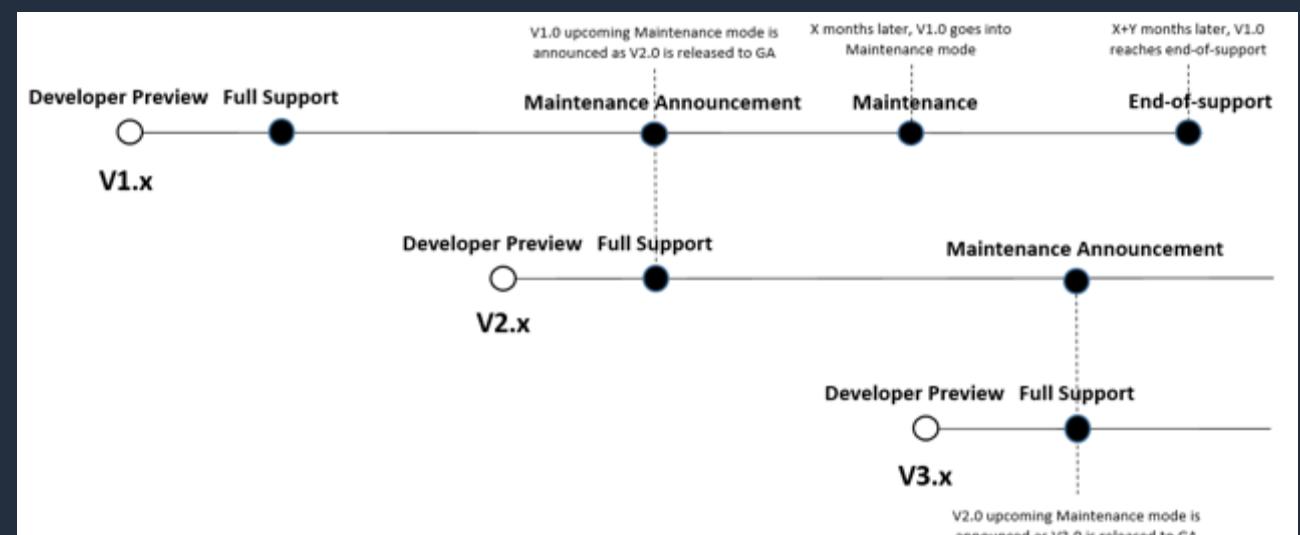
```
CDK v1 (TS)
dependencies: {
  "aws-cdk/core": "1.127.0",
  "aws-cdk/aws-apigateway": "1.127.0",
  "aws-cdk/aws-autoscaling": "1.127.0",
  "aws-cdk/aws-dynamodb": "1.127.0",
  "aws-cdk/aws-cloudwatch": "1.127.0",
  "aws-cdk/aws-cloudwatch-actions": "1.127.0",
  "aws-cdk/aws-eks": "1.127.0",
  "aws-cdk/aws-events": "1.127.0",
  "aws-cdk/aws-events-targets": "1.127.0",
  "aws-cdk/aws-ec2": "1.127.0",
  "aws-cdk/aws-ecs": "1.127.0",
  "aws-cdk/aws-iot": "1.127.0"
}

import { App, Stack } from "@aws-cdk/core";
import * as s3 from "@aws-cdk/aws-s3";

CDK v2 (TS)
dependencies: {
  "aws-cdk-lib": "2.0.0",
  "constructs": "2.0.0",
  "aws-cdk/aws-iot-alpha": "2.0.0-alpha.0"
}

import { App, Stack } from "aws-cdk-lib";
import * as s3 from "aws-cdk-lib/aws-s3";
```

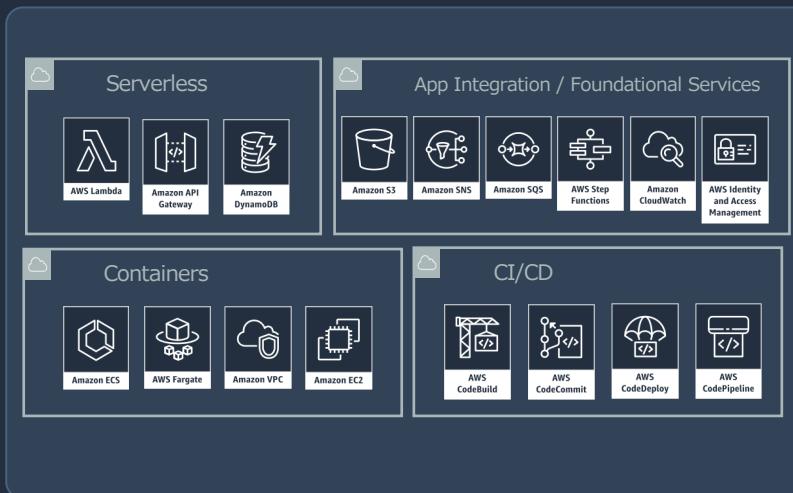
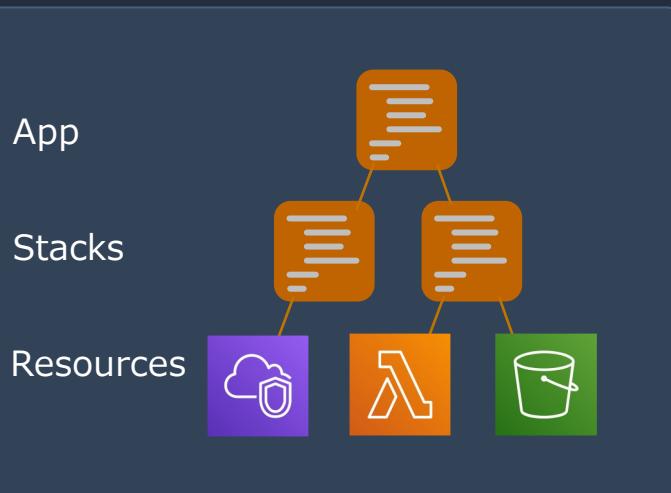
https://mplay-assets.s3.amazonaws.com/sites/awvreinv21/_uploads/assets/otmqsererizzcufy_awvreinv21.pdf



AWS CDK のコンセプト



AWS CDK の構成要素



コアフレームワーク

npm package: constructs

コンストラクトライブラリ

npm package: [aws-cdk-lib](#)

プログラミング言語ごとに専用のパッケージ
※ サードパーティ製または自作のコンストラクトライブラリも利用可能

AWS CDK Toolkit (CLI)

npm package: [aws-cdk](#)

プログラミング言語によらず**共通**

※ Node.js で動作



AWS CDK の概念

<https://docs.aws.amazon.com/cdk/v2/guide/home.html>

App

- ・ アプリケーション全体
- ・ 複数のAWSアカウント、リージョンにまたがることが可能

Stack

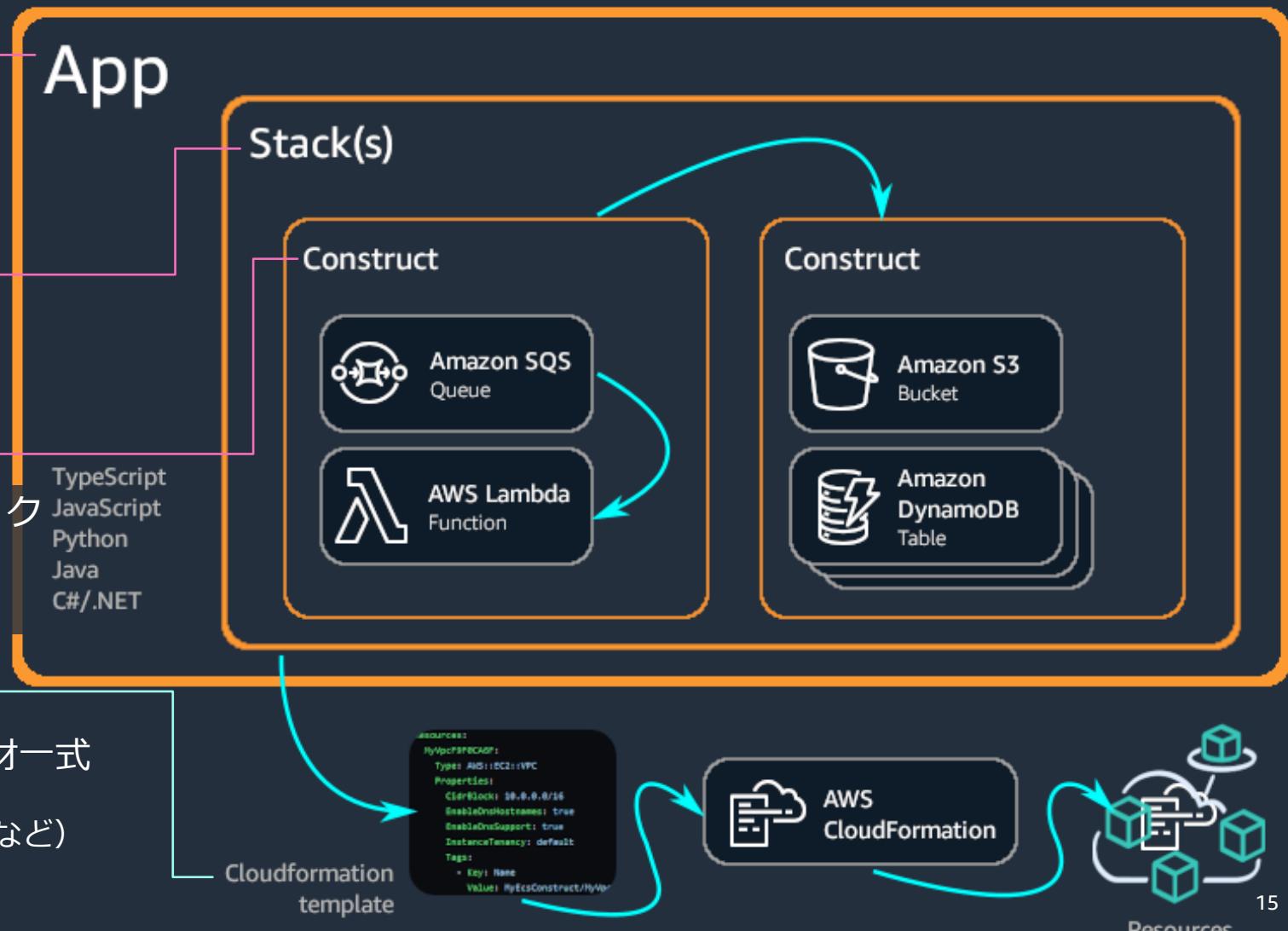
- ・ CloudFormation スタックに対応
- ・ デプロイ可能な最小単位

Construct

- ・ CDKの最も基本的なビルディングブロック
- ・ 1つまたは複数のAWSリソースを表現
- ・ ユーザーにより定義・配布が可能

Cloud Assembly

- ・ CDK App の出力。デプロイに必要な資材一式
 - ・ CloudFormation テンプレート
 - ・ アセット（ファイル、Docker イメージなど）



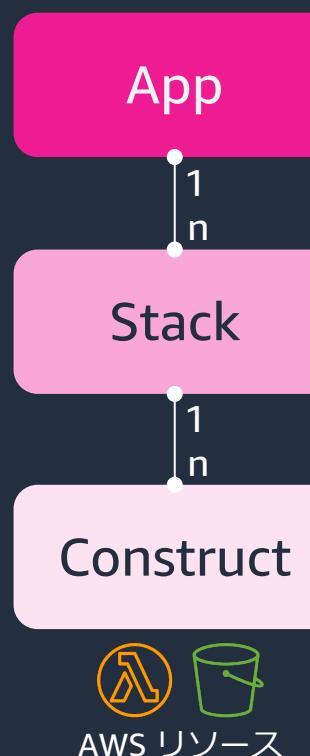
AWS CDK の概念 - CloudFormation との比較

AWS CloudFormation



- スタックを1つずつデプロイ
`$ aws cloudformation deploy --stack-name HogeStack --template-file hoge.yaml`
- 依存関係を考慮して
人がデプロイ順序を決める
- 複数のスタックを一括デプロイ
するためにはスクリプトや
Makefile, CodePipeline 等が必要
- CloudFormation Module による
カプセル化と再利用

AWS CDK



- 複数のスタックをまとめて
1つのアプリとしてデプロイ
(スタックを指定してデプロイも可能)
`$ cdk deploy --all`
- スタック間の依存関係を CDK が
解決してデプロイ順序を決定
- Construct による抽象化と再利用
- 複数の Stack をまとめる Stage
を追加することで環境の複製も
容易 (Dev, Staging, Prod ...)

AWS Constructs Library

AWS CDK が標準で提供する `CONSTRUCT` のライブラリ



Patterns (L3)

- 複数のリソースを含む一般的な構成パターンを抽象化
 - `aws-ecs-patterns.LoadBalancedFargateService` など

High-level constructs (L2)

- デフォルト値や便利なメソッドを定義した 単一の AWS リソースを表すクラス
 - `s3.Bucket` クラスのインスタンスは `addLifecycleRule()` メソッドを実装
- より特定のシナリオに合わせて單一リソースを抽象化した **L2.5 constructs** も存在
 - `aws-lambda-nodejs.NodeJsFunction`, `eks.FargateCluster` など

Low-level constructs (L1)

- CloudFormationリソースおよびプロパティと1:1で対応（自動生成される）
- `CfnXXX` という名前（例：`s3.CfnBucket` は `AWS::S3::Bucket` を意味）
- すべてのプロパティを明示的に設定する必要がある

CloudFormation テンプレートの例

例: IAM User からの
読み取り専用アクセスを許可する S3 Bucket を作成

Resources:

MyBucket:

Type: AWS::S3::Bucket

MyUser:

Type: AWS::IAM::User

MyUserPolicy:

Type: AWS::IAM::Policy

Properties:

PolicyDocument:

Statement:

- Action:

- s3:GetObject*
- s3:GetBucket*
- s3>List*

Effect: Allow

Resource:

- Fn::GetAtt: [MyBucket, Arn]
- Fn::Sub: "\${MyBucket.Arn}/*"

Version: "2012-10-17"

PolicyName: MyUserPolicy

Users:

- Ref: MyUser

AWS CloudFormation
template language



L1 Constructs を 使用した例

CloudFormation テンプレートとほぼ1:1対応
型チェックや補完、ループなどは使用可能

AWS CloudFormation
resources



AWS CDK



"L1"

CloudFormation から
自動的に生成

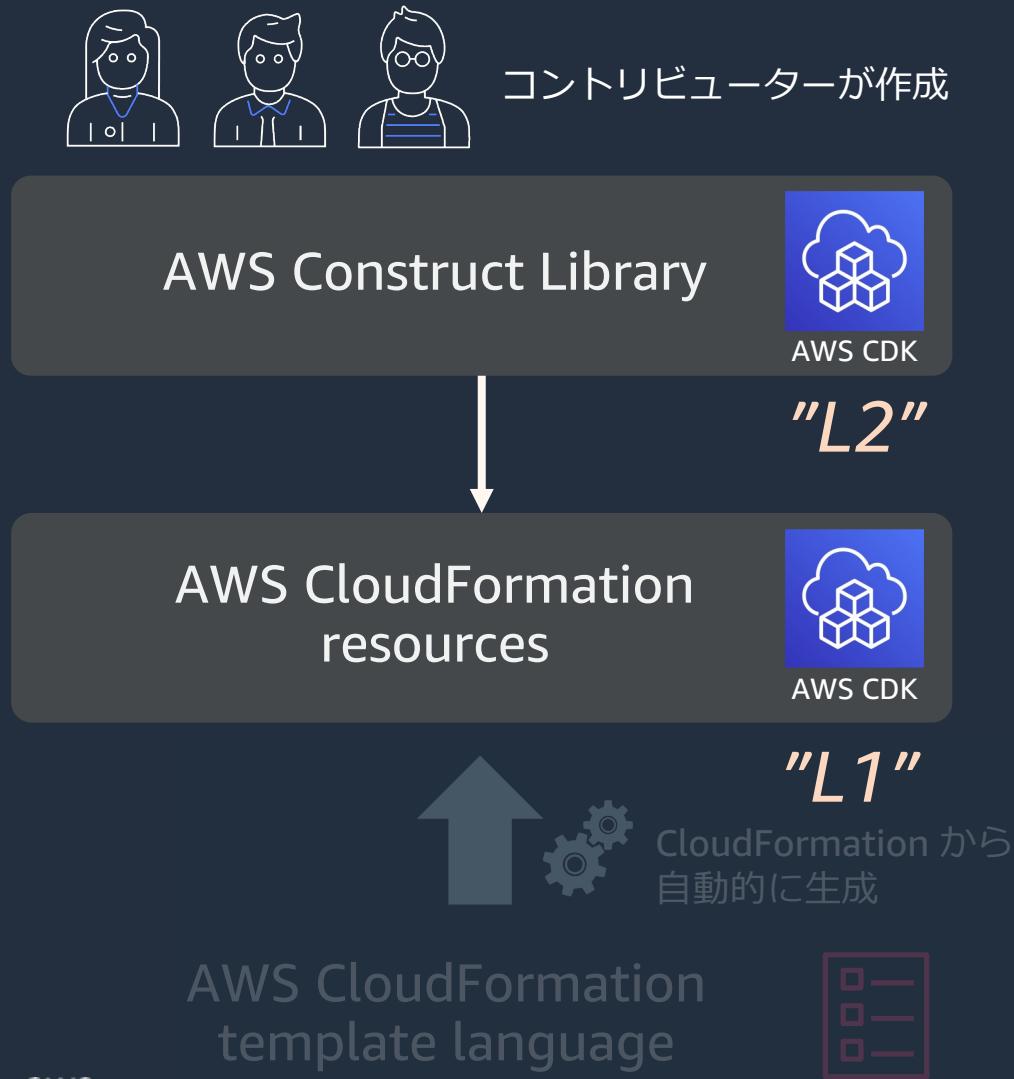
AWS CloudFormation
template language



```
const bucket = new CfnBucket(this, 'MyBucket');
const user = new CfnUser(this, 'MyUser');
new CfnPolicy(this, 'MyUserPolicy', {
  policyName: 'MyUserPolicy',
  policyDocument: new PolicyDocument({
    statements: [new PolicyStatement({
      actions: [
        's3:GetObject*',
        's3:GetBucket*',
        's3>List*' ],
      resources: [
        bucket.bucketArn,
        `${bucket.bucketArn}/*` ]
    })]
  }),
  users: [user.userName],
});
```



L2 Constructs を使用した例



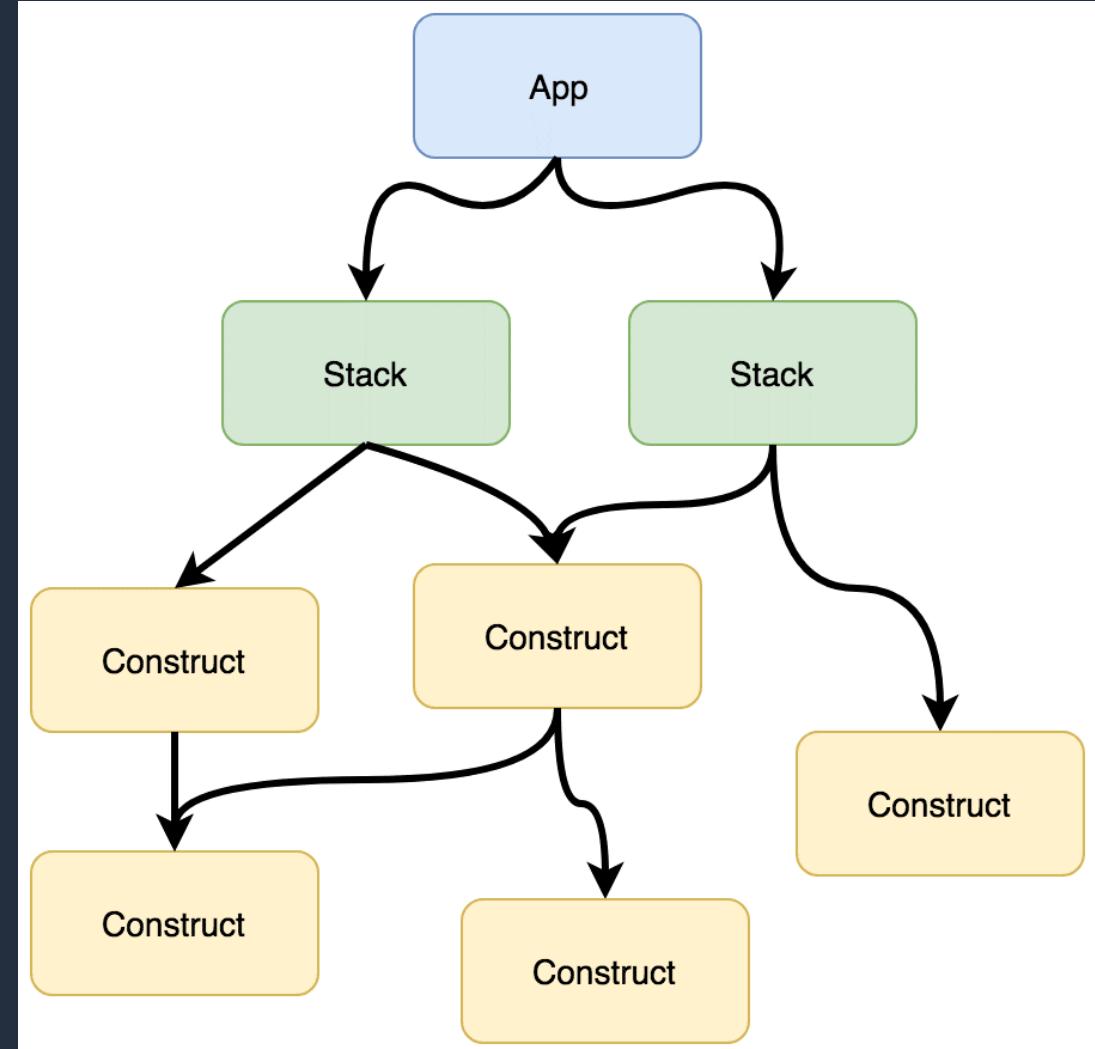
```
const bucket = new s3.Bucket(this, 'MyBucket');  
const user = new iam.User(this, 'MyUser');  
bucket.grantRead(user);
```

→ grant() メソッドにより IAM Policy を自動生成
コードから意図が明確に

Construct ツリー

- App をルートとして自由に Construct を構造化できる
- すべての Construct で明示的に scope (親) を指定して初期化
- AWS リソースを作成する Construct は Stack の子孫でなければならない
 - Stack クラスも Construct の一つ
- Node クラスで Construct ツリーにアクセス
- Aspect で各 Node への操作を実装可能 *

* Aspect の詳細は今後の Blackbelt または AWS CDK 開発者ガイドを参照



Construct ツリー の可視化

Construct は自由に構造化できる（ツリー構造）
構造化によってコードとリソースの可読性が向上

AWS CloudFormation コンソール

<https://aws.amazon.com/jp/about-aws/whats-new/2022/09/aws-cloud-development-kit-cdk-announces-cdk-construct-tree-view-cloudformation-console/>

AWS Toolkit for Visual Studio Code

<https://docs.aws.amazon.com/toolkit-for-vscode/latest/userguide/cdk-explorer.html>

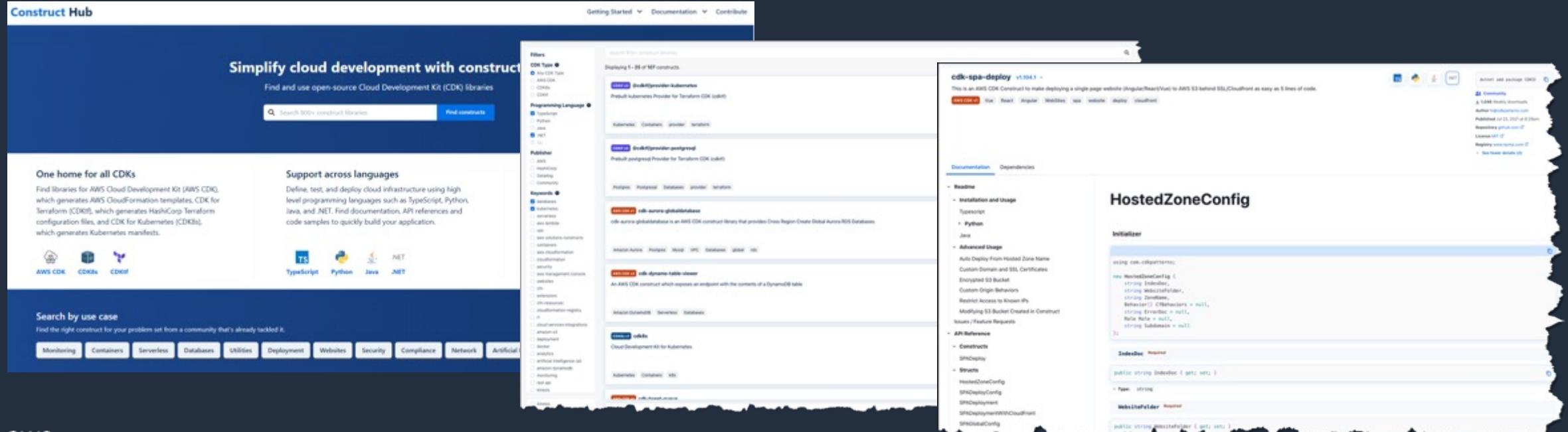
The screenshot shows the AWS CloudFormation console with the 'Resources' tab selected. The left pane displays a hierarchical tree of resources under the stack 'NetworkingFlowLogB'. The tree includes categories like Monitoring, CMK, Networking, Vpc, Key, and a selected node 'FlowLogBucket' which has a child 'Policy'. The right pane shows the CloudFormation JSON template for this stack, highlighting the 'FlowLogBucket' resource definition.

```
const app = new App();
const ecsapp = new BLEAEcsAppStack(app, 'Dev-BLEAEcsApp', {
  env: devParameter.env,
  crossRegionReferences: true,
  tags: {
    Repository: 'aws-samples/baseline-environment-on-aws',
    Environment: devParameter.envName,
  },
  // from parameter.ts
  monitoringNotifyEmail: devParameter.monitoringNotifyEmail,
  monitoringSlackWorkspaceId: devParameter.
  monitoringSlackWorkspaceId,
  monitoringSlackChannelId: devParameter.monitoringSlackChannelId,
  vpcCidr: devParameter.vpcCidr,
});
```

Construct Hub

<https://constructs.dev/>

- 1,000 以上のオープンソースのコンストラクトを公開
 - 公開されたコンストラクトを組み合わせることで、目的に合わせたアプリケーション環境をさらに迅速に構成できる
 - AWS CDK, CDK8s, CDKtf などのタイプやバージョン、言語、パブリッシャーなどで検索可能



エスケープハッチ (代替手段)

L2コンストラクトがない場合 (CloudFormation で対応しているリソースの場合)

- CfnBucket や CfnRole など、Cfn で始まる L1 コンストラクトを使う
- L1 コンストラクトもない場合、`cdk.CfnResource` を使う (CFnテンプレートとほぼ同等の記述)

L2 コンストラクトでプロパティが設定できない場合

- `construct.node.defaultChild` で L1 コンストラクトを取得し、プロパティを変更する

CloudFormation で対応していない機能の場合

- **Provider Framework** を使用してカスタムリソースを作成する
https://docs.aws.amazon.com/cdk/api/v2/docs/aws-cdk-lib.custom_resources-readme.html#provider-framework
- AWS の API を呼び出すシンプルなカスタムリソースは `AwsCustomResource` コンストラクトを使用することで、Lambda 関数のコードを記述することなく簡単に作成可能
https://docs.aws.amazon.com/cdk/api/v2/docs/aws-cdk-lib.custom_resources-readme.html#custom-resources-for-aws-apis

AWS CDK と 他のサービスの連携

AWS SAM でローカルデバッグを実行

AWS CDK で作成したサーバーレスアプリケーションを AWS SAM CLI を使用してローカルでデバッグ可能

sam local invoke, start-api, start-lambda に対応。デプロイは CDK で行う

ステップ 4: Lambda 関数をテストする

AWS CDK アプリケーションで定義されている Lambda 関数は、AWS SAM CLI を使用してローカルに呼び出すことができます。これを行うには、呼び出す関数のコンストラクト識別子と、合成した AWS CloudFormation テンプレートへのパスが必要です。

実行するコマンド:

```
cdk synth --no-staging
```



```
sam local invoke MyFunction --no-event -t ./cdk.out/CdkSamExampleStack.template.json
```



https://docs.aws.amazon.com/ja_jp/serverless-application-model/latest/developerguide/serverless-cdk-getting-started.html



AWS Amplify と CDK の連携

\$ amplify override ... バックエンドリソースをCDKで上書き

- AWS Amplify が自動生成したリソースを CDK でカスタマイズ
IAM ロール、Cognito による認証機構、S3 バケット、DynamoDB テーブルに対応
<https://docs.amplify.aws/cli/restapi/override/>

\$ amplify add custom ... CDK でカスタムバックエンドを追加

- AWS Amplify が生成できるバックエンドリソースに加え、CDK で任意のリソースを定義
<https://docs.amplify.aws/cli/custom/cdk/>

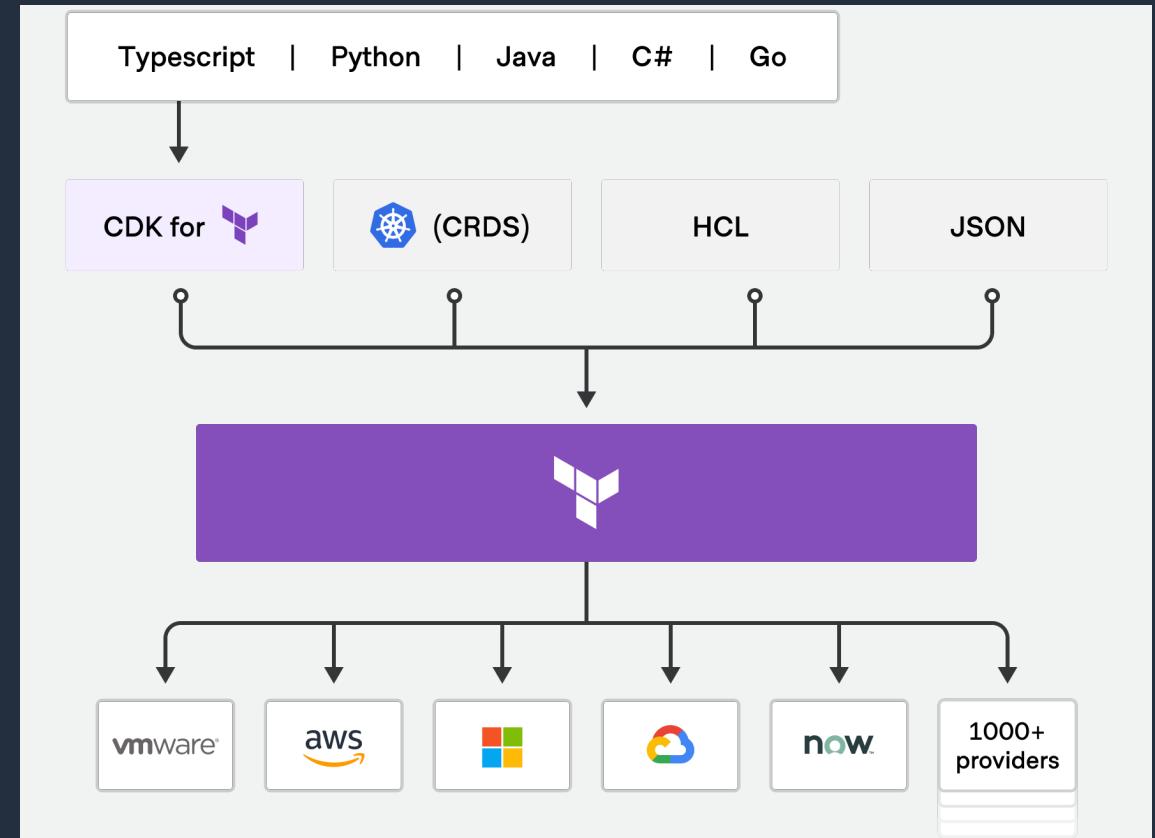
\$ amplify export ... バックエンドリソースをCDKでエクスポート

- AWS Amplify で生成したバックエンドをエクスポートして AWS CDK からデプロイ。
CDK Pipelines や Amazon CodeCatalyst の CDK deploy action が利用可能
<https://docs.amplify.aws/cli/usage/export-to-cdk/>

CDK for Terraform = CDKTF

- HashiCorp 社と AWS CDK チームが共同開発
- AWS CDK がコードから CloudFormation テンプレートを生成するのと同様に、Terraform の JSON 構成を生成
- cdktf-cli により、初期化や合成の他、Terraform レジストリのプロバイダーをプロジェクトにインポート可能

<https://www.terraform.io/cdktf>



CDK for Terraform on AWS 一般提供 (GA) のお知らせ
<https://aws.amazon.com/jp/blogs/news/cdk-for-terraform-on-aws-jp/>

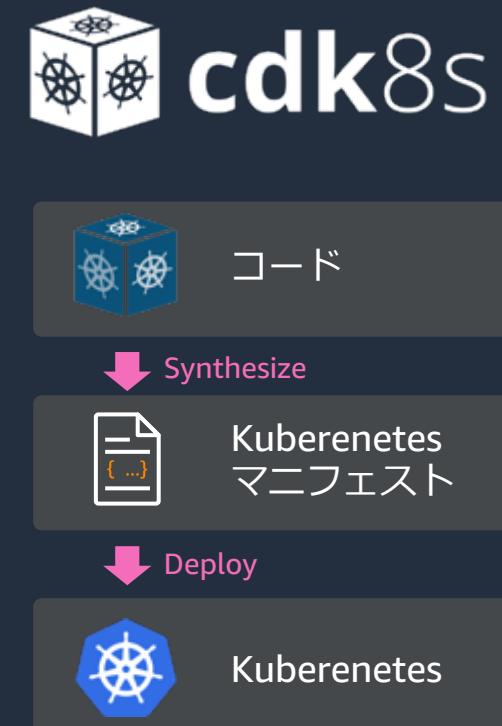
CDK for Kubernetes = CDK8s

<https://cdk8s.io/>

プログラミング言語で KUBERNETES のマニフェストファイルを生成できるツールキット

- ソースコードから Kubernetes のマニフェスト YAML を生成
 - 制御構文やクラス・継承などの概念で効率的に書くことが可能
 - エディタによる型チェック、サジェスト、API 仕様の参照
- オープンソースとして開発
 - ベストプラクティスを定義した Construct として拡張・共有
- 任意の Kubernetes クラスターで利用可能
- 言語サポート
 - TypeScript/JavaScript、Python、Java
- 任意の Kubernetes API バージョンとカスタムリソースを使用可能
- CDK8s+ で高レベルなコンストラクトを提供

<https://aws.amazon.com/jp/blogs/news/announcing-general-availability-of-cdk8s-plus-and-support-for-manifest-validation/>



TypeScript での開発の流れ



AWS CDK の開発に必要なもの

Git



- **Git** <https://git-scm.com/>
| IaC の原則としてバージョン管理は必須 ※ AWS CDK の直接的な依存関係ではない

AWS CLI と言語ランタイム



- **AWS CLI v2** <https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2.html>
- **Node.js** <https://nodejs.org/en/> ※ アクティブな LTS 版を推奨

| JavaScript / TypeScript 以外の言語で記述する場合は
その言語のランタイムやコンパイラも必要

テキストエディタ / IDE



- **VSCode** <https://code.visualstudio.com/> ※ またはお好きなテキストエディタ
| 各言語のコード補完やリファクタリング機能を持つツールの利用を強く推奨

AWS CLI の認証情報を設定

IAM ユーザーのアクセスキーを使用する場合

Console ➔

```
$ aws configure --profile <your-profile-name>
```

または環境変数 `AWS_ACCESS_KEY_ID`, `AWS_SECRET_ACCESS_KEY`, `AWS_DEFAULT_REGION` を指定
https://docs.aws.amazon.com/cdk/v2/guide/getting_started.html#getting_started_prerequisites

AWS IAM Identity Center (SSO) を使用する場合

https://docs.aws.amazon.com/ja_jp/cli/latest/userguide/cli-configure-sso.html

v2.18.0 ~

Console ➔

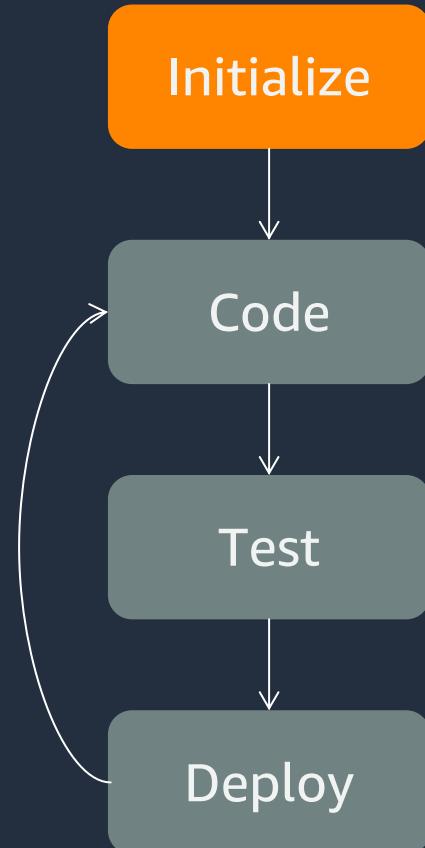
```
$ aws configure sso
```

一時的な認証情報を使用して
セキュリティベストプラクティスに準拠



AWS CDK (TypeScript) での開発フロー 1/4 Initialize

cdk init でプロジェクトを作成



Console

ディレクトリを作成

\$ mkdir cdk-sample

\$ cd cdk-sample

CDK プロジェクトを作成

\$ npx aws-cdk init app --language=typescript

CDK Bootstrapping

\$ npx aws-cdk bootstrap

cdk init はディレクトリ名を使用してファイル名や Stack 名を生成

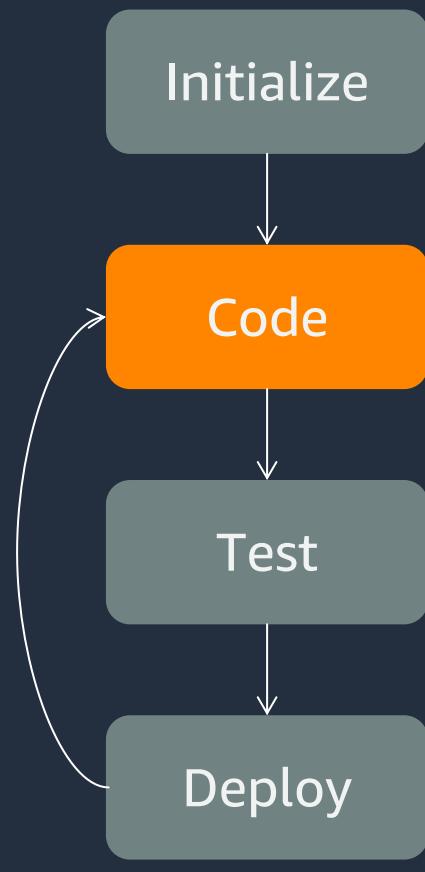
空のテンプレートを生成。 sample-app を指定するとサンプルが追加

CDK が使用する IAM ロール、S3 バケット、ECR リポジトリなどを作成
対象アカウント、リージョンにつき1回だけ実施

Tips: npx について

cdk コマンドをグローバルインストールした状態 (npm i -g aws-cdk) を前提に cdk init と記載されることも。
cdk init 時 (npm プロジェクト外) は最新の aws-cdk を使用すること、
cdk synth や deploy 時 (npm プロジェクト内) はローカルインストールの aws-cdk を使用することを目的として
本資料ではコマンドを npx aws-cdk に統一する。なお npx cdk としてもよい (一部状況下では少し挙動が異なる)

AWS CDK (TypeScript) での開発フロー 2/4 Code



IDE やテキストエディタを使用して CDK アプリをコーディング

cdk init で生成されるファイルの例

File Structure

```
.├── README.md
├── bin
│   └── cdk-sample.ts
├── cdk.json
├── jest.config.js
└── lib
    └── cdk-sample-stack.ts
├── node_modules
├── package-lock.json
└── package.json
└── test
    └── cdk-sample.test.ts
└── tsconfig.json
```

コード例 (引数など一部省略)

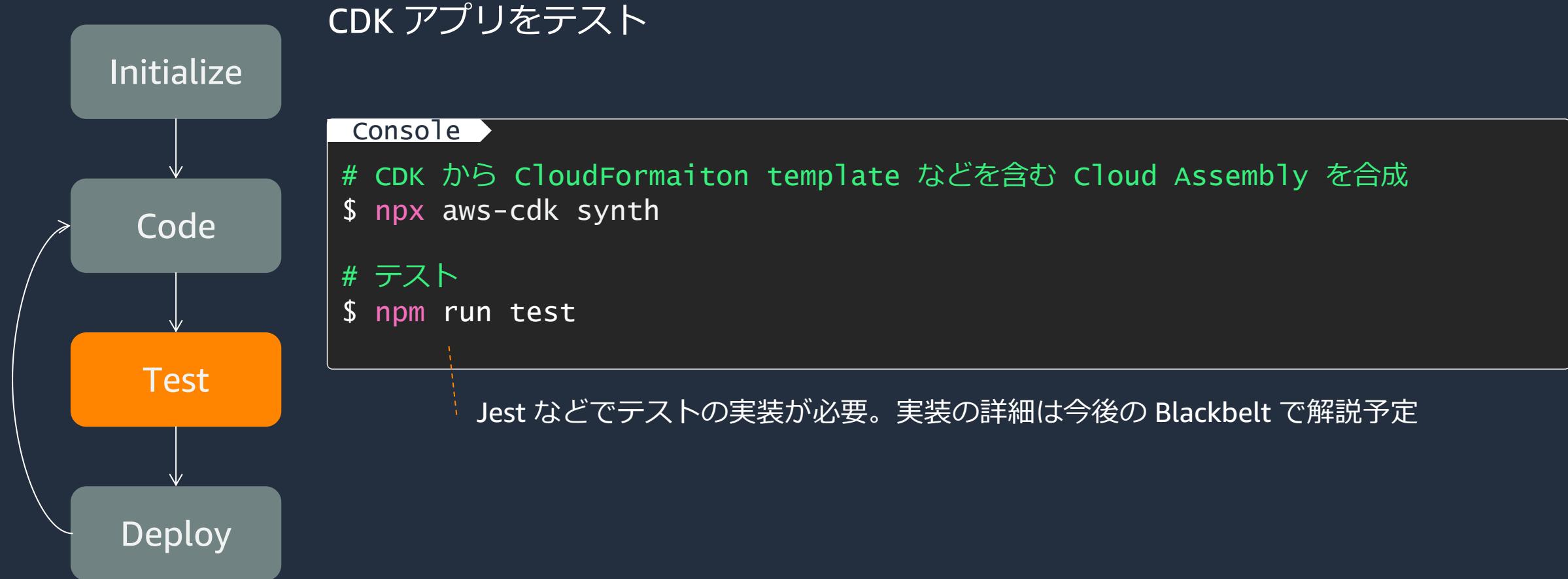
bin/cdk-sample.ts

```
// App を作成
const app = new cdk.App();
// App に Stack を追加
new CdkSampleStack(app, "MyApp");
```

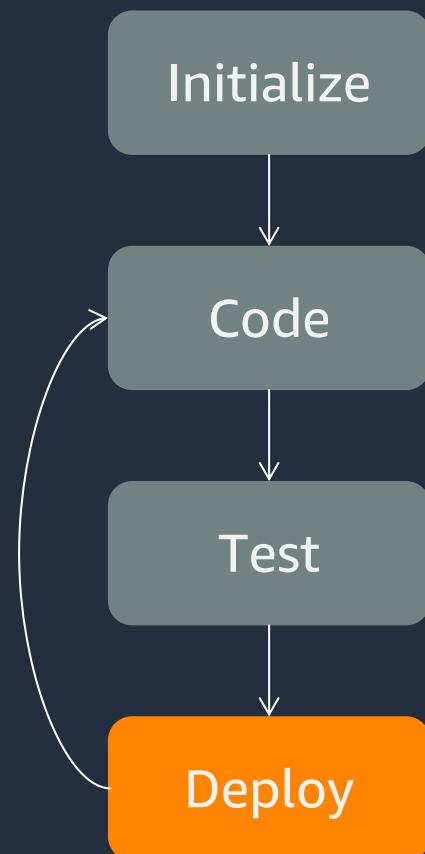
lib/cdk-sample-stack.ts

```
// Stack を定義
export class CdkSampleStack extends Stack {
    constructor() {
        // コンストラクタ内で Construct を追加
        new s3.Bucket(this, "HogeBucket");
        new sqs.Queue(this, "HogeQueue");
    }
}
```

AWS CDK (TypeScript) での開発フロー 3/4 Test



AWS CDK (TypeScript) での開発フロー 4/4 Deploy



CDK アプリを AWS にデプロイ

Console ➔

```
# デプロイ済みの cloudFormation Template との差分を確認  
$ npx aws-cdk diff  
  
# AWS に CDK アプリをデプロイ  
$ npx aws-cdk deploy --all
```

* cdk deploy の代表的なオプション

Console ➔

```
$ npx aws-cdk deploy Samplestack # スタックを指定してデプロイ  
$ npx aws-cdk deploy --all --require-approval=never # デプロイ時の確認を行わない  
$ npx aws-cdk deploy --all --hotswap # Lambda関数などの開発時に変更を高速に反映する  
$ npx aws-cdk deploy --all --no-rollback # スタックの更新失敗時に自動ロールバックしない  
$ npx aws-cdk deploy --all -c key=value # Context を指定
```

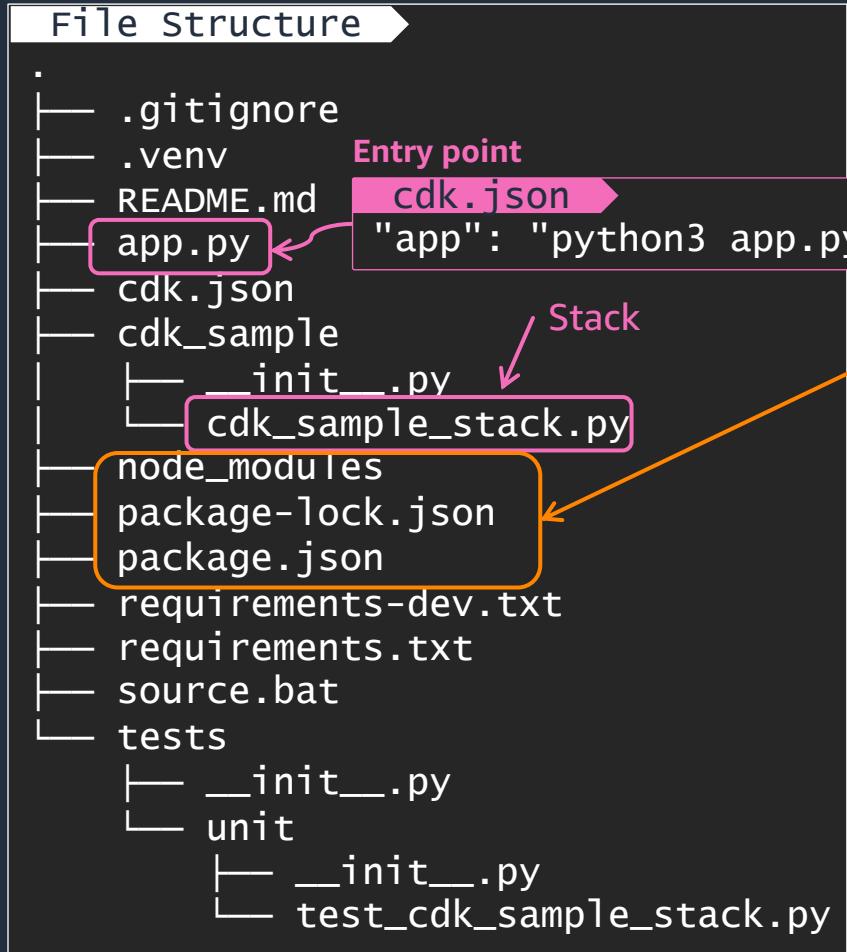
* 最新のコマンドリファレンスは GitHub を参照

<https://github.com/aws/aws-cdk/blob/main/packages/aws-cdk/README.md>

各言語における プロジェクト構成



AWS CDK in Python



前提条件や言語固有のイディオムなど、詳細はこちちら
<https://docs.aws.amazon.com/cdk/v2/guide/work-with-cdk-python.html>

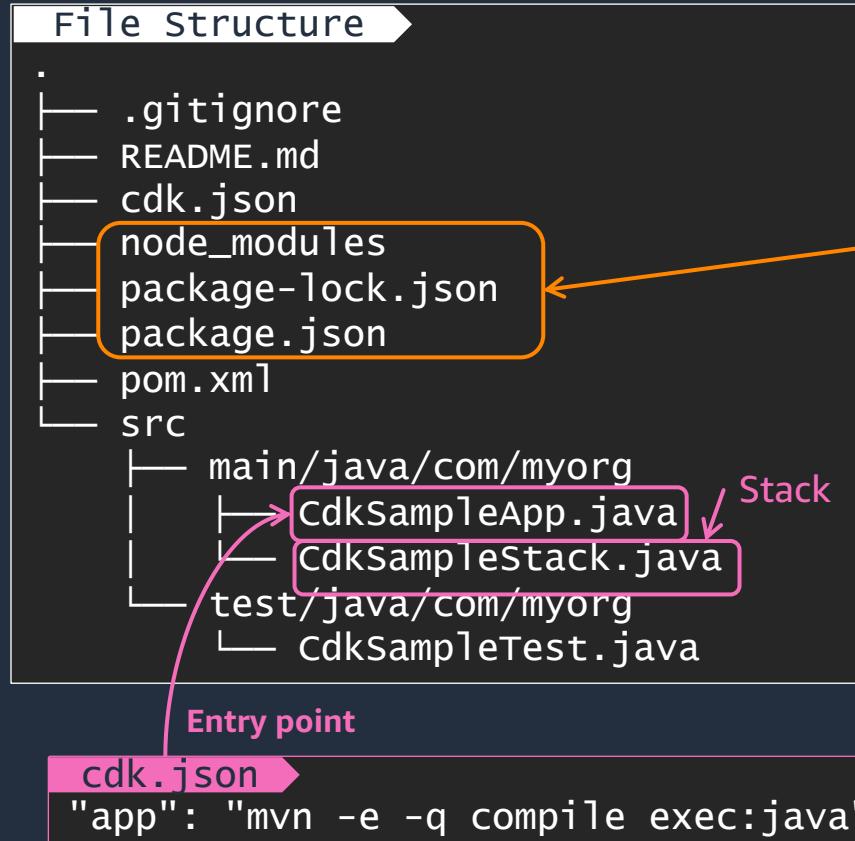
Console

```
# CDK プロジェクトを作成
$ npx aws-cdk init app --language=python
$ source .venv/bin/activate
$ pip install -r requirements.txt
# CDK Toolkitをローカルインストールしてバージョンを固定（推奨）
$ npm init -y
$ npm install -D aws-cdk
$ echo node_modules >> .gitignore
# CDK Bootstrapping
$ npx aws-cdk bootstrap
# デプロイ
$ npx aws-cdk deploy --all
```

Console

```
# CDK Toolkit のアップデート
$ npx npm-check-updates -u
$ npm install
# コンストラクトライブラリのアップデート
$ pip list -o | sed -e '1,2d' | cut -f1 -d' ' | xargs pip
install -U
```

AWS CDK in Java



前提条件や言語固有のイディオムなど、詳細はこちら
<https://docs.aws.amazon.com/cdk/v2/guide/work-with-cdk-java.html>

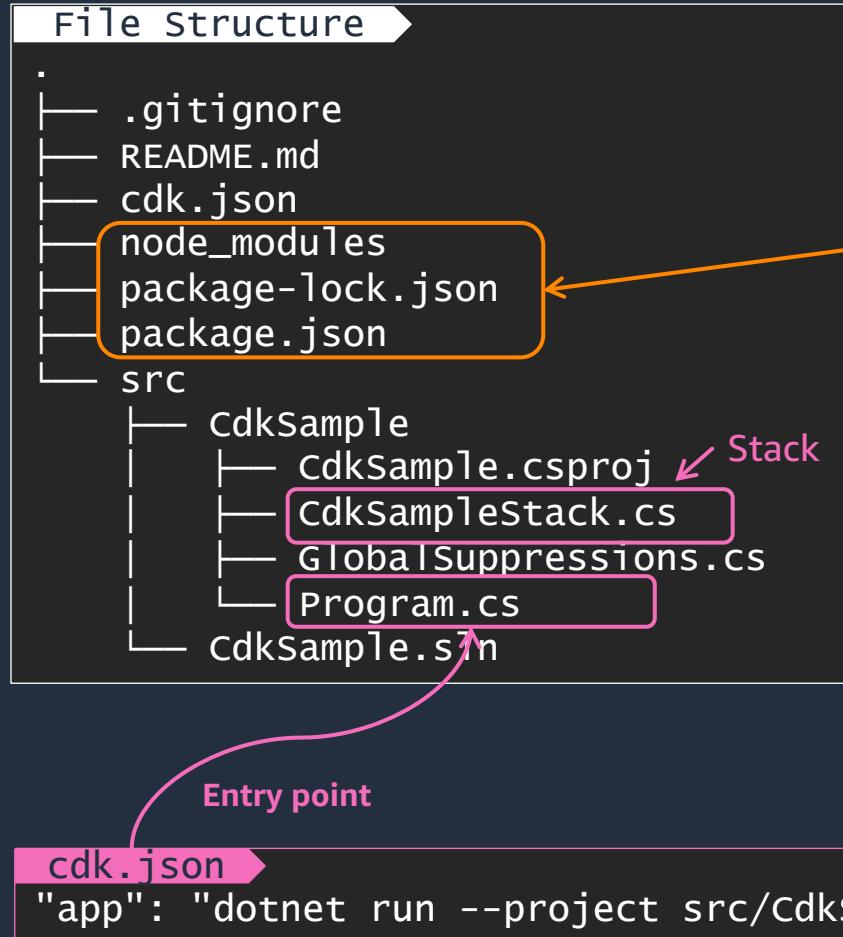
Console →

```
# CDK プロジェクトを作成  
$ npx aws-cdk init app --language=java  
# CDK Toolkitをローカルインストールしてバージョンを固定（推奨）  
$ npm init -y  
$ npm install -D aws-cdk  
$ echo node_modules >> .gitignore  
# CDK Bootstrapping  
$ npx aws-cdk bootstrap  
# デプロイ  
$ npx aws-cdk deploy --all  
# (参考) コンパイルとテストを実行  
$ mvn package
```

Console →

```
# CDK Toolkit のアップデート  
$ npx npm-check-updates -u  
$ npm install  
# コンストラクトライブラリのアップデート  
$ mvn versions:use-latest-versions
```

AWS CDK in C#



前提条件や言語固有のイディオムなど、詳細はこちら
<https://docs.aws.amazon.com/cdk/v2/guide/work-with-cdk-csharp.html>

Console

```
# CDK プロジェクトを作成  
$ npx aws-cdk init app --language=csharp  
# CDK Toolkitをローカルインストールしてバージョンを固定（推奨）  
$ npm init -y  
$ npm install -D aws-cdk  
$ echo node_modules >> .gitignore  
# CDK Bootstrapping  
$ npx aws-cdk bootstrap  
# デプロイ  
$ npx aws-cdk deploy --all  
# (参考) コンパイルとテストを実行  
$ dotnet build src
```

Console

```
# CDK Toolkit のアップデート  
$ npx npm-check-updates -u  
$ npm install
```

AWS CDK in Go

File Structure

```
.  
├── .gitignore  
├── README.md  
└── cdk-sample.go  
    └── cdk-sample_test.go  
├── cdk.json  
├── go.mod  
├── go.sum  
└── node_modules  
    └── package-lock.json  
    └── package.json
```

App & Stack

Entry point

cdk.json

```
"app": "go mod download && go run cdk-sample.go"
```

前提条件や言語固有のイディオムなど、詳細はこちちら

<https://docs.aws.amazon.com/cdk/v2/guide/work-with-cdk-go.html>

Console

```
# CDK プロジェクトを作成  
$ npx aws-cdk init app --language=go
```

```
# CDK Toolkitをローカルインストールしてバージョンを固定（推奨）  
$ npm init -y
```

```
$ npm install -D aws-cdk
```

```
$ echo node_modules >> .gitignore
```

CDK Bootstrapping

```
$ npx aws-cdk bootstrap
```

```
# パッケージのインストール
```

```
$ go get
```

```
# デプロイ
```

```
$ npx aws-cdk deploy --all
```

```
# (参考) コンパイルとテストを実行
```

```
$ go test
```

Console

```
# CDK Toolkit のアップデート
```

```
$ npx npm-check-updates -u
```

```
$ npm install
```

```
# コンストラクトライブラリのアップデート
```

```
$ go get -u
```

```
$ go mod tidy
```



デモ

TypeScript での AWS CDK プロジェクト作成～
Amazon VPC をデプロイ





EXPLORER

•

✓ OPEN EDITORS

CDK-BLAC...

PROBLEMS OUTPUT TERMINAL CODEWHISPERER REFERENCE LOG DEBUG CONSOLE

zsh + - ⌂ ... ^ x

cdk-blackbelt \$

> OUTLINE

AWS CDK の学習リソース

AWS CDK のドキュメント

AWS CDK Developer Guide

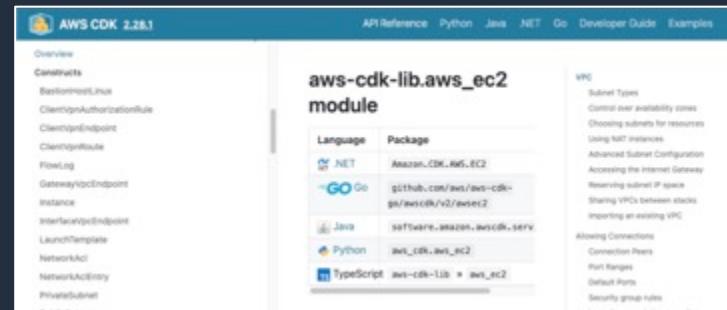


This screenshot shows the AWS CDK v2 Developer Guide homepage. It features a sidebar with navigation links like 'Getting started', 'Working with the AWS CDK', and 'Managing dependencies'. The main content area includes a 'What is the AWS CDK?' section, a 'Welcome' message for v2, and a 'CDK v1 maintenance notice' stating it entered maintenance on June 1, 2022.

https://docs.aws.amazon.com/ja_jp/cdk/v2/guide/home.html

AWS CDK のコンセプトや
実践的なベストプラクティスなど
開発に役立つ情報を記載

API Reference

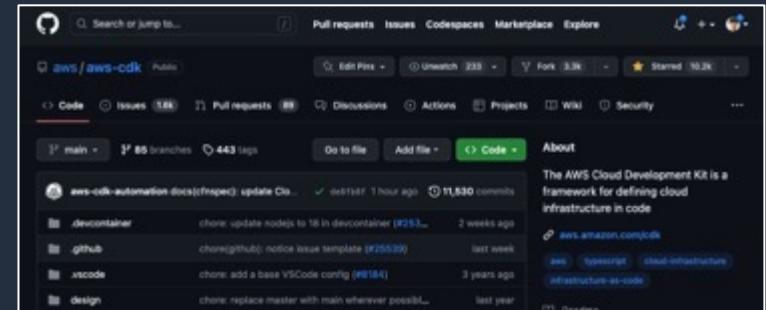


This screenshot shows the API Reference for the 'aws-cdk-lib.aws_ec2' module. It lists various languages (NET, Go, Java, Python, TypeScript) and their corresponding package names. To the right, there's a detailed description of the VPC construct, including sections on Subnet Types, Choosing subnets for resources, Using NAT instances, Advanced Subnet Configuration, Accessing the Internet Gateway, Reserving subnet IP space, Sharing VPCs between stacks, Importing an existing VPC, Allowing Connections, Connection Peers, Port Range, Default Ports, and Security group rules.

<https://docs.aws.amazon.com/cdk/api/v2/docs/aws-construct-library.html>

API の仕様はこちちらで確認

GitHub repository



This screenshot shows the GitHub repository page for 'aws/aws-cdk'. It displays basic repository statistics like 85 branches and 443 tags. The 'Code' tab is selected, showing a list of recent commits from contributors like 'aws-cdk-automation', 'devcontainer', 'github', 'vscode', and 'design'. The repository description states: 'The AWS Cloud Development Kit is a framework for defining cloud infrastructure in code.'

<https://github.com/aws/aws-cdk>

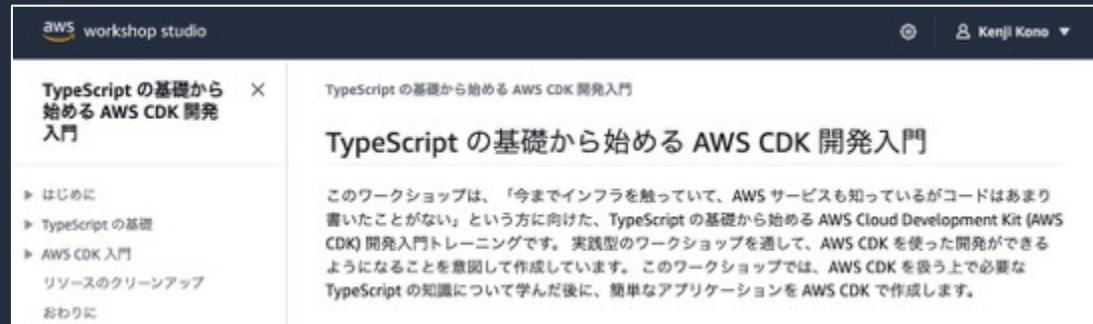
AWS CDK の開発リポジトリ

最新の開発状況や Design Doc などを確認できる



AWS CDK のワークショップ (日本語)

TypeScript の基礎から始める AWS CDK 開発入門



The screenshot shows the AWS Workshop Studio interface. On the left, there's a sidebar with a navigation menu:

- TypeScript の基礎から始める AWS CDK 開発入門
- はじめに
- TypeScript の基礎
- AWS CDK 入門
- リソースのクリーンアップ
- おわりに

The main content area displays the workshop details:

TypeScript の基礎から始める AWS CDK 開発入門

このワークショップは、「今までインフラを触っていて、AWS サービスも知っているがコードはあまり書いたことがない」という方に向けた、TypeScript の基礎から始める AWS Cloud Development Kit (AWS CDK) 開発入門トレーニングです。実践型のワークショップを通して、AWS CDK を使った開発ができるようになることを意図して作成しています。このワークショップでは、AWS CDK を使う上で必要な TypeScript の知識について学んだ後に、簡単なアプリケーションを AWS CDK で作成します。

<https://catalog.workshops.aws/typescript-and-cdk-for-beginner/>

あまりコードを書いたことがない方向けに
TypeScript の基礎から
CDK を学べるワークショップ

CDK Workshop



The screenshot shows the AWS CDK Workshop landing page. It features a sidebar with the following navigation:

- 日本語 (selected)
- 必要条件
- TypeScript ワークショップ
- Python ワークショップ
- .NET ワークショップ
- Java ワークショップ
- Go Workshop

The main content area has a heading "開発者の皆様、ようこそ！" (Welcome, developers!) and a brief introduction:

本日、このワークショップにご参加いただき、誠にありがとうございます。このワークショップでは、“AWS Cloud Development Kit”(AWS CDK) を紹介します。AWS CDK は AWS が提供する新しいソフトウェア開発フレームワークです。楽しくかつ簡単にクラウドのインフラストラクチャーを自分に好きな開発言語で定義ができる、最終的に AWS CloudFormation を用いてデプロイできることを目的としています。

このワークショップで何を作りますか？簡単なものから始めます。



<https://cdkworkshop.com/>

実際にコードを書きながら
CDK を学べるワークショップ

TypeScript, Python, C#/.NET, Java, Go に対応





Thank you!

AWS Black Belt Online Seminar とは

- ・ 「サービス別」「ソリューション別」「業種別」などのテーマに分け、アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナーシリーズです
- ・ AWS の技術担当者が、AWS の各サービスやソリューションについてテーマごとに動画を公開します
- ・ 以下の URL より、過去のセミナー含めた資料などをダウンロードすることができます
 - ・ <https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/>
 - ・ <https://www.youtube.com/playlist?list=PLzWGOASvSx6FlwIC2X1nObr1KcMCBBlqY>



ご感想は Twitter へ！ハッシュタグは以下をご利用ください
#awsblackbelt

内容についての注意点

- ・ 本資料では 2023 年 7 月時点のサービス内容および価格についてご説明しています。AWS のサービスは常にアップデートを続けているため、最新の情報は AWS 公式ウェブサイト (<https://aws.amazon.com/>) にてご確認ください
- ・ 資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます
- ・ 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます
- ・ 技術的な内容に関しましては、有料の [AWS サポート窓口](#)へお問い合わせください
- ・ 料金面でのお問い合わせに関しましては、[カスタマーサポート窓口](#)へお問い合わせください (マネジメントコンソールへのログインが必要です)



AWS Certificate Manager

AWS Black Belt Online Seminar

Arisa Hase
Solutions Architect
2023/10

AWS Black Belt Online Seminarとは

- ・「サービス別」「ソリューション別」「業種別」などのテーマに分け、
アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナーシリーズです
- ・AWSの技術担当者が、AWSの各サービスやソリューションについてテーマごとに動画を公開します
- ・動画を一時停止・スキップすることで、興味がある分野・項目だけの聴講も可能、スキマ時間の学習にもお役立ていただけます
- ・以下のURLより、過去のセミナー含めた資料などをダウンロードすることができます
 - ・<https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/>
 - ・<https://www.youtube.com/playlist?list=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBlqY>

内容についての注意点

- 本資料では2023年10月時点のサービス内容および価格についてご説明しています。
最新の情報は AWS 公式ウェブサイト(<https://aws.amazon.com>)にてご確認ください
- 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます
- 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます

自己紹介

長谷 有沙（はせ ありさ）

技術統括本部 西日本ソリューション本部
ソリューションアーキテクト



前職までの経験

コンサルタントとしてデータマネジメント系を中心にシステム導入や要件定義を経験

好きなAWSサービス

AWS Certificate Manager



本セミナーの対象者・ゴール

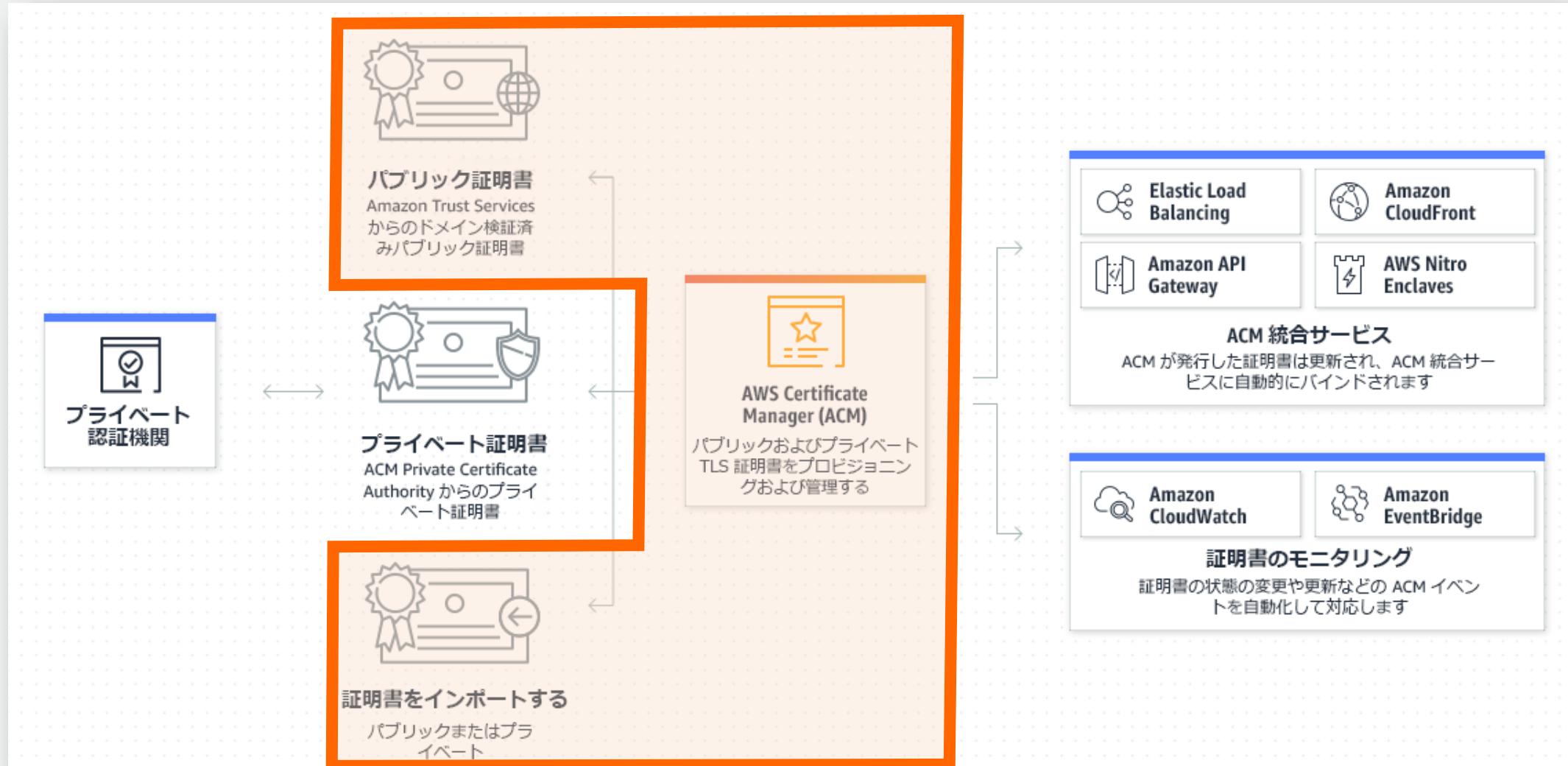
- **対象者**

- これからAWS Certificate Manager (ACM) をご利用されたい、もしくは理解を深めたい
- SSL/TLS サーバ証明書管理、その運用に興味・関心がある
- Web サーバの SSL/TLS による暗号化の仕組みについて理解されている

- **本資料の対象外サービス**

- AWS Private Certificate Authority (AWS Private CA)

本セミナーのスコープ

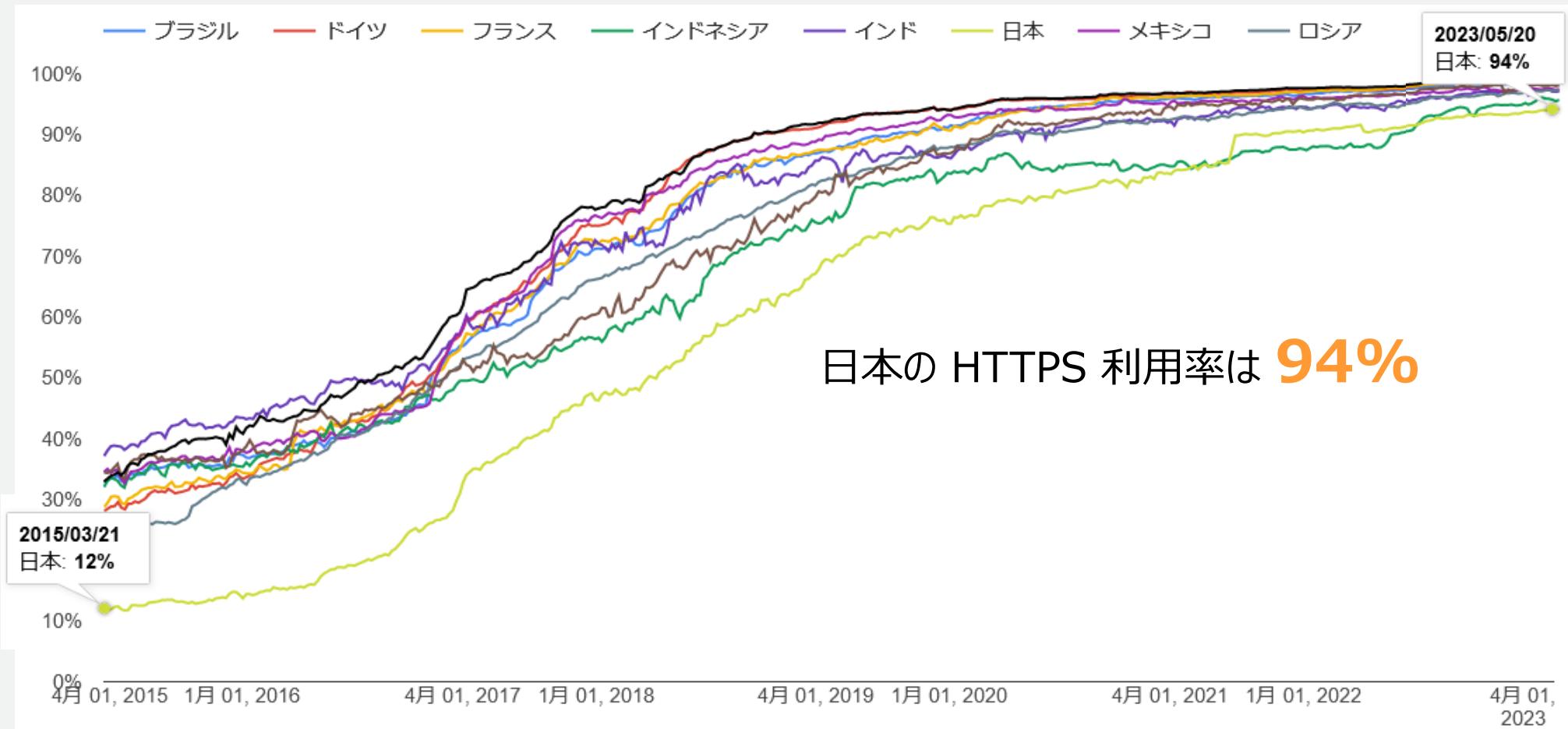


アジェンダ

1. HTTPS の現状と課題
2. サービス概要
3. サービス機能詳細
4. サービス利用時の留意事項
5. 料金とリージョン
6. まとめ

1. HTTPS の現状と課題

HTTPS の利用状況



世界各国におけるHTTPSの利用状況(*1)

(*1) 出典 : Google Transparency Report

<https://transparencyreport.google.com/https/overview?hl=ja>



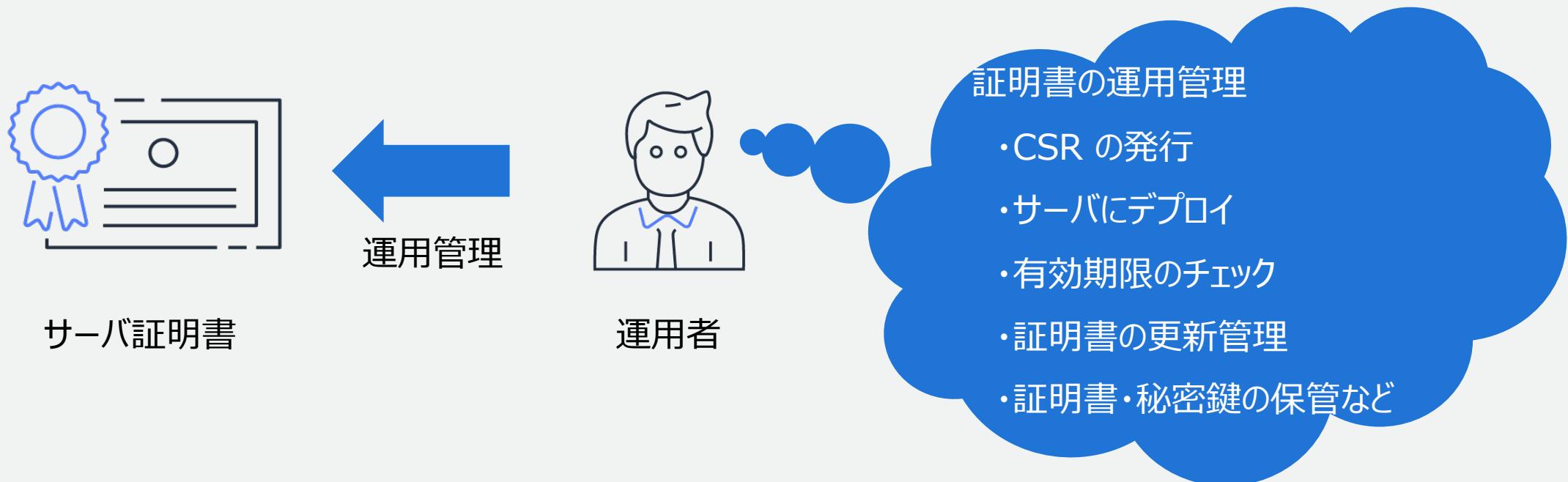
HTTPS を利用する代表的な理由

- ・「盗聴」「改ざん」「なりすまし」への対策
- ・CA/ Browser Forum によるガイドライン策定
(例 : HTTPS 採用サイトの視認性向上など)
- ・常時 SSL/TLS によるメリットの享受
 - + Cookie 情報の盗聴防止
 - + SEO の順位向上など

参考 : 総務省 https://www.soumu.go.jp/main_content/000615559.pdf

サーバ証明書の運用課題の例

HTTPS を実装するためにはサーバ証明書が必要となり、同時に運用者は**証明書の運用管理が必要**となります



簡単かつ効率的にサーバ証明書の運用をしたい！

2. AWS Certification Manager (ACM) サービス概要

AWS Certificate Manager (ACM) とは



- SSL/TLS サーバー証明書のプロビジョニング、管理、デプロイを簡単に実現するサービス
- SSL/TLS サーバー証明書の購入・アップロード・更新という手間のかかるプロセスの自動化・簡素化

AWS Certificate Manager (ACM) のメリット

証明書を集中管理する

AWS リージョンでの SSL/TLS 証明書すべてを集中管理できます。

安全なキー管理

ACM は、SSL/TLS 証明書で使用される秘密鍵を保護し管理するよう設計されています。

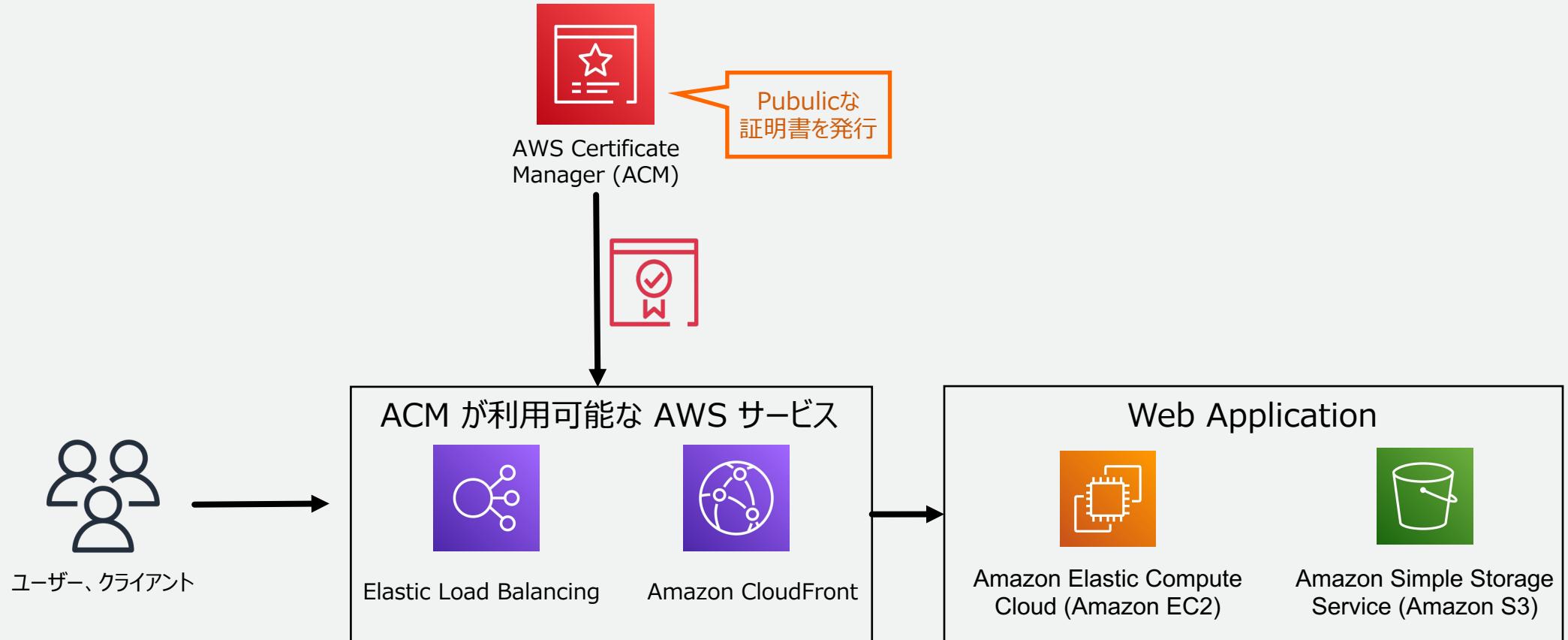
AWSのサービス統合

SSL/TLS 証明書をプロビジョニングし、Elastic Load Balancing や Amazon CloudFront ディストリビューション、Amazon API Gateway でデプロイできます。

サードパーティの証明書をインポートする

サードパーティの認証機関 (CA) により発行される SSL/TLS 証明書をインポートし、統合可能な AWS サービスに簡単にデプロイできます。

ACMの典型的な利用例



3. サービス機能詳細

機能概要

a. 証明書を発行する機能

- ・ 証明書の発行とインポート
- ・ ACM で発行できる証明書と種類
- ・ 利用できるドメイン名
- ・ ドメイン検証方法
- ・ インポートできる証明書
- ・ サポートされるキーアルゴリズム
- ・ ACM が発行する証明書のルート証明書について

b. 証明書を管理する機能

- ・ 証明書の自動更新
- ・ 証明書の失効
- ・ ACM 証明書が利用可能な AWS サービス

c. モニタリング・ロギング機能

- ・ モニタリングとロギングの概要
- ・ Amazon EventBridge でサポートされるイベント
- ・ CloudWatch でサポートされるメトリクス
- ・ CloudTrail でサポートされる ACM API

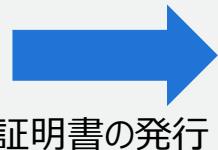
a. 証明書を発行する機能

証明書の発行とインポート

証明書の発行



AWS Certificate
Manager (ACM)



証明書の発行



サーバー証明書

証明書のインポート



AWS Certificate
Manager (ACM)



証明書インポート



サーバー証明書

Amazon CloudFront、Elastic Load Balancing、Amazon API Gateway などの ACM 統合サービスでサークルパーティの証明書を使用する必要がある場合は、証明書を ACM にインポートできます。インポートされた証明書を更新することはできませんが、更新プロセスの管理をサポートします。

- AWS CLI による証明書インポート方法

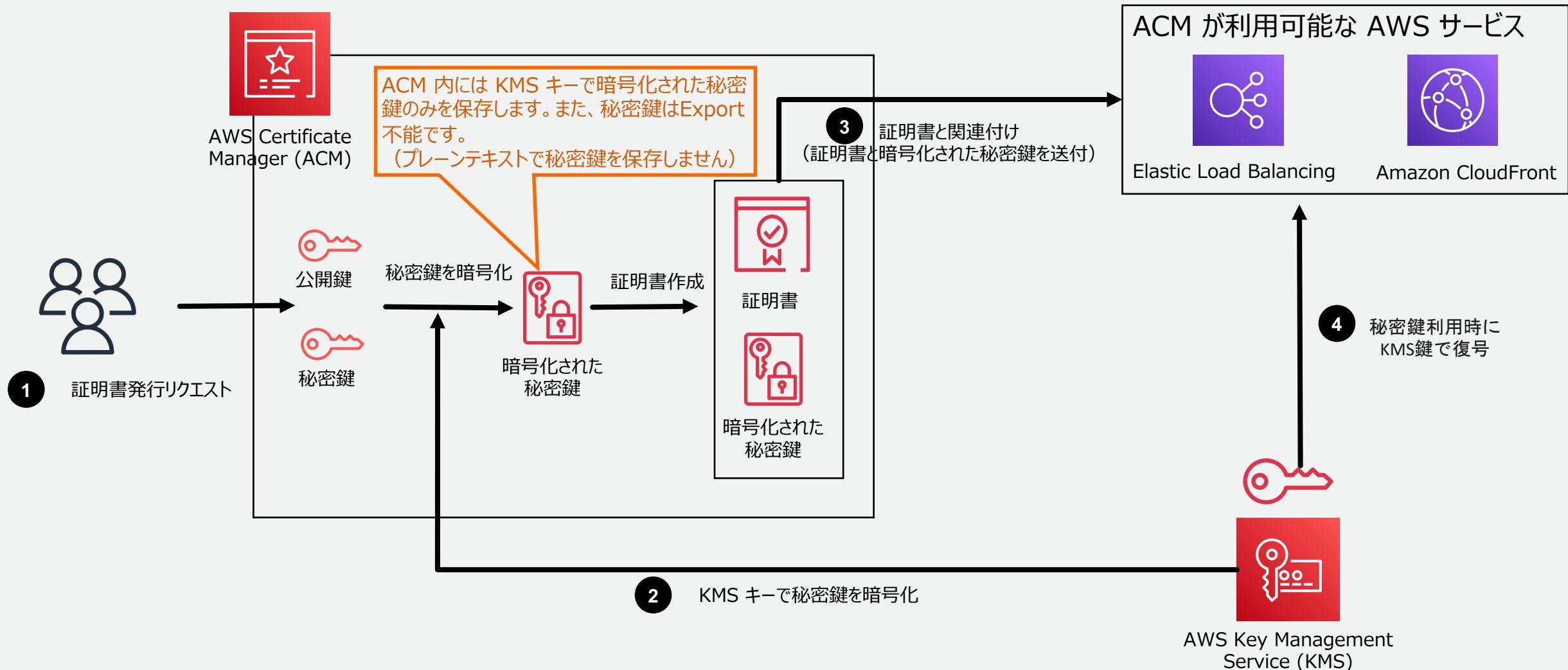
https://docs.aws.amazon.com/ja_jp/acm/latest/userguide/import-certificate-api-cli.html

- インポート時の前提条件の詳細

https://docs.aws.amazon.com/ja_jp/acm/latest/userguide/import-certificate-prerequisites.html



サーバ証明書の発行と秘密鍵保護の仕組み



ACM で発行できるパブリック証明書と種類

証明書種類	説明
ドメイン認証 (DV) 証明書	サーバの運営組織が、サーバ証明書に記載されるドメインの利用権を有することを確認したうえで発行される証明書。
組織認証 (OV) 証明書	ドメイン名の利用権に加えて、サーバ運営組織の実在性の確認やドメイン名と運営組織との関係などについても確認した上で発行される証明書。
拡張認証 (EV) 証明書	OV 証明書と同様、ドメイン名の利用権に加えて、サーバ運営組織の実在性等の確認やドメイン名と運営組織との関係などについても確認した上で発行される証明書。

項目	パブリック証明書
発行できる証明書	ドメイン認証 (DV) 証明書
有効期間	有効期間は、 13か月(395日) 固定
アプリケーション、 ブラウザのサポート	Google Chrome, Microsoft Edge, Mozilla Firefox, Apple Safari を含む主要なブラウザと Java
サブジェクト	有効なパブリック DNS 名
ルート CA	パブリックルート CA (*)
検証方法	DNS 認証あるいは E メール認証で検証

参考 : TLS 暗号設定ガイドライン Ver. 3.0.1
<https://www.ipa.go.jp/security/crypto/guideline/gmcbt80000005ufv-att/ipa-cryptrec-gl-3001-3.0.1.pdf>

*: Amazon Trust Services 自社認証局があらゆるところで確実に使えるようにするために、2005年以降のほとんどのブラウザで信頼されているルート認証局である Starfield Services の認証局の一つを購入しております。 詳細は、以下を参照ください。

<https://www.amazontrust.com/repository/>

利用できるドメイン名

- DNS に準拠するサブジェクト名であれば利用可能
 - 國際化ドメイン名(e.g. 日本語を使ったドメイン名)
 - Punycode 要件(RFC3492)に準拠
 - Zone Apex (ネイキッドドメイン)でも利用可能
 - E.g. example.com ドメイン検証が必要
 - ドメイン検証を実施する必要がある。
- 複数ドメイン名もサポート
 - 1つの証明書に複数ドメイン名を追加可能
- ワイルドカード名
 - ドメイン名にアスタリスク (*) を使うことで、同じドメイン内の複数サイトを保護できるワイルドカード名の利用可能



ドメイン検証方法

DV 証明書を発行する際の、ドメイン検証方法は以下の 2 つから選択

- **DNS 検証 (推奨)**
 - DNS に CNAME レコード (ACM が指定) を追加し、ACM で自動的に検証
 - 外部 DNS, AWS の DNS サービスである Route 53 (ワンクリックで検証) の両方可能
 - 証明書更新時、CNAME レコードが残っていれば、検証は自動で実施され、運用負荷軽減
- **E メール検証**
 - WHOIS データベースに記載されている連絡先(ドメイン登録者、技術担当者、ドメイン管理者)と各ドメインに対して指定した 5 つの共通システムのアドレスに E メールを送信し検証を行い、少なくとも 3 つのメール対応が必要
 - 証明書更新時に都度対応が必要
 - E メール検証を使用して証明書を作成後、DNS による検証に切り替え不可

インポートできる証明書

- 以下の種類の外部認証機関で発行された証明書をインポート可能
 - ドメイン認証 (DV) 証明書
 - 組織認証 (OV) 証明書
 - 拡張認証 (EV) 証明書

サードパーティーの証明書をすでに取得している場合、または ACM 発行の証明書によって満たされないアプリケーション固有の要件がある場合に行います。

サポートされるキーアルゴリズム

種類	ACMで発行する証明書	ACMにインポートする証明書
RSA	RSA 2048 ビット (RSA_2048)	RSA 1024 ビット (RSA_1024) (*) RSA 2048 ビット (RSA_2048) RSA 3072 ビット (RSA_3072) RSA 4096 ビット (RSA_4096)
ECDSA	ECDSA 256 ビット(EC_prime256v1) ECDSA 384 ビット (EC_secp384r1)	ECDSA 256 ビット(EC_prime256v1) ECDSA 384 ビット (EC_secp384r1) ECDSA 521 ビット (EC_secp521r1)

*: RSA 1024 bit 証明書のインポートは可能ですが、セキュリティ観点で、2048bit 以上の証明書を利用されることを推奨します。

参考 : TLS 暗号設定ガイドライン Ver. 3.0.1

<https://www.ipa.go.jp/security/crypto/guideline/qmcbt80000005ufv-att/ipa-cryptrec-ql-3001-3.0.1.pdf>

ACM が発行する証明書のルート証明書について

Amazon ルートCAはFirefoxやChromeやMicrosoft Edgeといった主要なブラウザに登録されているため追加設定をせず利用できます。

- ACM パブリック証明書は Amazon の認証機関 (CA) で検証されます。Amazon Root CA 1
- Amazon Root CA 2、Amazon Root CA 3、Amazon Root CA 4、Starfield サービスルート認証機関証明書 - G2 を含むブラウザ、アプリケーション、OS では、ACM 証明書が信頼されます。

Firefox



Chrome

SHA 256 Hash	Subject
18ce6cf7bf14e60b2e347b8dfe868cb31d02ebb3ada271569f50343b46db3a4	CN=Amazon Root CA 3,O=Amazon,C=US
1ba5b2aa8c65401a82960118f80bec4f62304d83cec4713a19c39c011ea46db4	CN=Amazon Root CA 2,O=Amazon,C=US
568d6905a2c88708a4b3025190edcfedb1974a606a13c6e5290fc2ae63edab5	CN=Starfield Services Root Certificate Authority - G2,O=Starfield Technologies, Inc.,L=Scottsdale,ST=Arizona,C=US
8ecde6884f3d87b1125ba31ac3fcb13d7016de7f57cc904fe1cb97c6ae98196e	CN=Amazon Root CA 1,O=Amazon,C=US
e35d28419ed02025cfa69038cd623962458da5c695fbdea3c22b0fb25897092	CN=Amazon Root CA 4,O=Amazon,C=US

参考 : Amazon Trust Services Repository

<https://www.amazontrust.com/repository/>

参考 : ACM証明書の特徴

https://docs.aws.amazon.com/ja_jp/acm/latest/userguide/acm-certificate.html

b. 証明書を管理する機能

証明書の自動更新

自動更新対象の証明書

- Elastic Load Balancing や Amazon CloudFront などの AWS サービスに関連付けられている証明書
※インポートした証明書の更新は対象外、また有効期限切れの更新は対象外

証明書更新プロセス(DNS検証の場合)

- 有効期限切れの 60 日前までに DNS 検証を実施
- 自動更新対象の証明書かどうか、ACM が指定した CNAME レコードにアクセスできるどうかを確認
- DNS 検証できない場合、AWS Health イベントと Amazon EventBridge イベントを通じて有効期限切れの 45 日、30 日、15 日、7 日、3 日、1 日前に送信されます

特記事項

- 証明書の更新時、証明書の Amazon リソースネーム (ARN) は変更されません
- **自動更新による HTTPS 通信の瞬断は発生しません**

証明書の失効

サービス提供の終了など何らかの理由で
サーバ証明書の有効期間内であってもサーバ証明書を失効させる

- ・ マネジメントコンソール、CLI を利用して証明書を削除(*1)
- ・ サポートに依頼して証明書を失効させる(*2)

ACM から発行された証明書の有効性については、以下で確認可能

- ・ Online Certificate Status Protocol (OCSP)
- ・ Certificate Revocation List (CRL)

(*1) 証明書の削除

https://docs.aws.amazon.com/ja_jp/acm/latest/userguide/gs-acm-delete.html

(*2) ACM パブリック証明書を取り消すにはどうすればよいですか？

<https://aws.amazon.com/jp/premiumsupport/knowledge-center/revoke-acm-public-certificate/>



ACM証明書が利用可能なAWSサービス

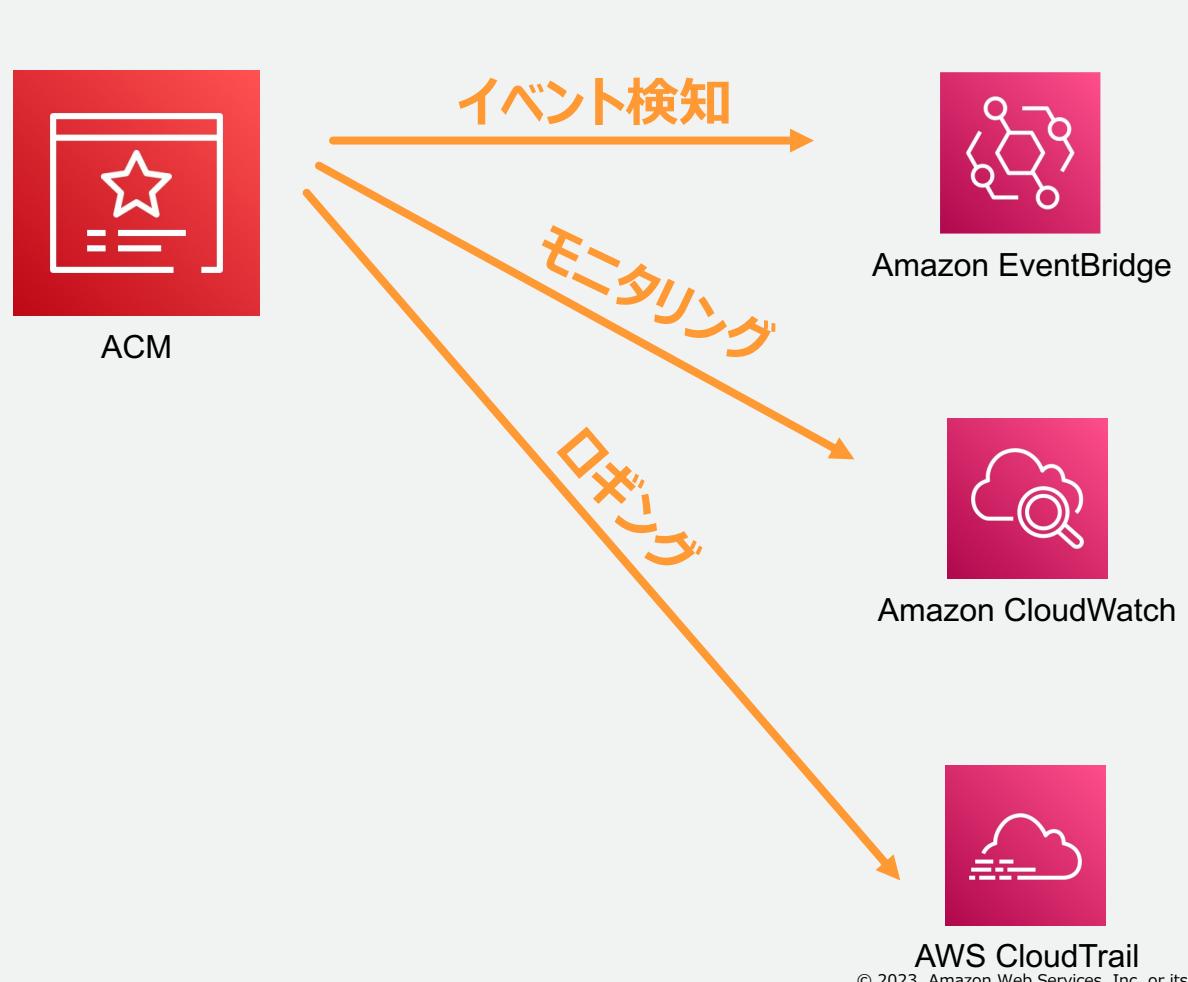
- Amazon CloudFront
- Elastic Load Balancing
- Amazon API Gateway
- AWS Nitro Enclaves
- Amazon Cognito
- AWS Network Firewall
- AWS Elastic Beanstalk
- AWS App Runner
- AWS CloudFormation
- AWS Amplify
- Amazon OpenSearch Service

2023年7月時点の情報です。最新情報は以下のURLからご確認ください。
https://docs.aws.amazon.com/ja_jp/acm/latest/userguide/acm-services.html

c. モニタリング・ロギング機能

モニタリングとロギング概要

イベント管理、モニタリング、ロギング機能をAWSサービスと連携して提供



イベント管理機能

- ・イベントは、ニアリアルタイムで Amazon EventBridge に配信
- ・イベントを使用して、AWS Lambda 関数、
AWS Batch ジョブ、Amazon SNS トピックと連携が可能

モニタリング機能

- ・メトリクスの収集と追跡、アラーム設定が可能
- ・証明書の有効期限が切れるまで、アカウント内の
証明書ごとにデイリーでメトリクスを更新

ロギング機能

- ・ACM コンソールからの呼び出しや SDK/ACM API
経由での操作を含む、API コールをイベントを記録

Amazon EventBridge で通知可能なイベント (1/2)

証明書の有効期限

- 有効期限日の45日前から、すべての有効な証明書有効期限イベントを毎日送信

証明書期限切れ

- 証明書の有効期限が切れた場合にアラートを送信

証明書利用可能

- 証明書が使用可能になったときに通知を送信

Amazon EventBridge で通知可能なイベント (2/2)

証明書更新アクション

- 証明書を更新するためにアクションが必要な時にアラートを送信
 - 例えば、証明書の更新を妨げる CAA レコードを追加した場合、有効期限の45日前に自動更新が失敗したときにこのイベントを通知
 - アクションされないことが継続される場合、30日、15日、3日、1日の時点でアラートを再送

ヘルスチェック

- 証明書を正常に更新した場合にステータスを通知
- 証明書更新を行うためのアクションを実行する必要があるとき、ステータスを通知
 - AWS_ACN_RENEWAL_STATE_CHANGE, CAA_CHECK_FAILURE, AWS_ACN_RENEWAL_FAILURE

CloudWatch でサポートされているメトリクス

証明書の有効期限が切れるまでの日数

- メトリクス : DaysToExpiry
- 証明書の有効期限が切れるまでの日数をデイリー更新。
- 証明書の有効期限が切れると更新しません。

CloudTrail でサポートされる ACM API

API	内容
AddTagsToCertificate	証明書へのタグの追加
DeleteCertificate	証明書の削除
DescribeCertificate	証明書についての説明
ExportCertificate	証明書のエクスポート
ImportCertificate	証明書のインポート
ListCertificates	証明書の一覧表示
ListTagsForCertificate	証明書のタグの一覧表示
RemoveTagsFromCertificate	証明書からタグを削除
RequestCertificate	証明書のリクエスト
ResendValidationEmail	検証 E メールの再送信
GetCertificate	証明書の取得

4. サービス利用時の留意事項

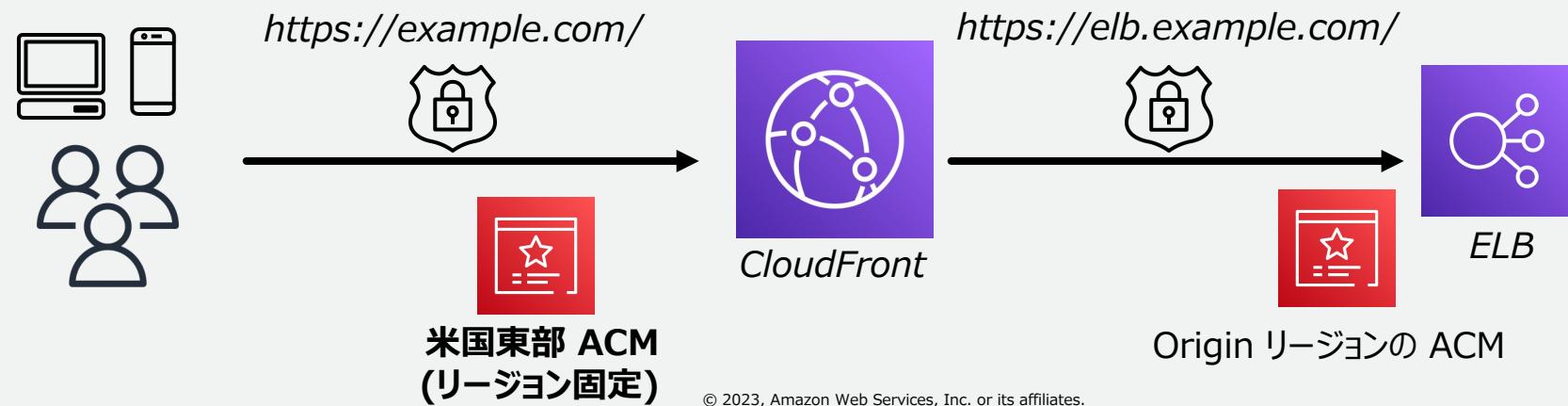
サービス利用時の留意事項の概要

以下 2 つのケースにおける留意事項について、ご紹介します

- Amazon CloudFront と連携するケース
- AWS CloudFormation を利用して開発、テスト環境など複数環境で ACM 証明書のプロビジョニングをするケース

Amazon CloudFront と連携するケース

- 米国東部（バージニア北部）リージョンの ACM で証明書を管理
- ACM で発行した証明書を利用する場合、サポートするキーアルゴリズムは、**RSA 2048bit** あるいは **ECDSA 256 bit**
- Amazon CloudFront とオリジンとの間で HTTPS を必須にする場合、オリジンとして Elastic Load Balancing を使用していれば、任意の AWS リージョンで証明書をリクエストあるいはインポート可能



AWS CloudFormation を利用して開発、テスト環境など複数環境で ACM 証明書のプロビジョニングをするケース

- プログラムバージョン、テストフェーズごとに証明書を発行すると、ACM の証明書発行数の上限値に達する可能性
 - 対策として、以下を事前に検討しておく
 - ワイルドカード証明書の活用する
 - 例えば、<version>.service.example.com の場合、<*>.service.example.com のワイルドカード証明書を作成する
 - サポートに上限値緩和を申請する

サービス上限

項目	デフォルト上限
ACM 証明書の数 アカウントごとに各 AWS リージョンに適用されます。 期限切れの証明書と失効した証明書もカウントされます。	2,500
1 年間の ACM 証明書の数 (過去 365 日間) 年間でリージョンおよびアカウントごとに、ACM 証明書のクオータを最大2倍に増やすことをリクエストできます。たとえば、クオータが2,500の場合は、年間でリージョンおよびアカウントごとに、最大5,000の ACM 証明書をリクエストできます。ただし一度に所有できる証明書は 2,500 のみです。2,500を超える証明書が必要な場合はその都度 AWS サポートセンター連絡する必要があります。	アカウント上限の 2 倍

サービス上限 (1/2)

項目	デフォルト上限
インポートされた証明書の数	2,500
1 年間にインポートされた証明書の数 (過去 365 日間)	アカウント上限の 2 倍
ACM 証明書ごとのドメイン名の数	10

詳細については、以下を参照ください。

https://docs.aws.amazon.com/ja_jp/acm/latest/userguide/acm-limits.html

上限緩和については AWS Support センターへお問い合わせください。

<https://console.aws.amazon.com/support/home#/case/create?issueType=service-limit-increase&limitType=service-code-acm>

5. 料金とリージョン

料金

ACM で管理するパブリック SSL/TLS 証明書は、**料金はかかりません**

- ウェブサイトあるいはアプリケーションを実行するために作成する AWS リソースのみに料金が発生
- 最新の ACM の料金情報については、以下を参照
 - AWS Certificate Manager サービス料金表
<http://aws.amazon.com/certificate-manager/pricing/>

サポートされるリージョン

バージニア北部
オハイオ
北カリフォルニア
オレゴン
米国東部
米国西部
米国中部
サンパウロ
香港特別行政区
メルボルン
ムンバイ
ソウル
シンガポール
シドニー
バーレーン
アラブ首長国連邦

東京
大阪
北京
寧夏
ジャカルタ
ハイデラバード
バーレーン
ケープタウン
フランクフルト
アイルランド
ロンドン
ミラノ
パリ
スペイン
ストックホルム
チューリッヒ



32 リージョンで利用可能
(2023年10月現在)

最新情報は、以下を参照ください

https://docs.aws.amazon.com/ja_jp/acm/latest/userguide/acm-regions.html

6. まとめ

まとめ

- **証明書を集中管理と効率化**

- AWS リージョンでの集中管理
- Amazon EventBridge や Amazon CloudWatch で有効期限の可視化や通知が可能
- 証明書の更新、デプロイ、プロビジョニングの自動化・簡素化
- 秘密鍵を安全に管理

- **サーバ証明書費用の最適化**

- AWS Certificate Manager でプロビジョニングされたパブリックSSL/TLS 証明書は無料

参考情報

AWS Certificate Manager メインページ

<https://aws.amazon.com/jp/certificate-manager/>

AWS Certificate Manager ドキュメント

https://docs.aws.amazon.com/ja_jp/acm/

AWS Certificate Manager の料金

<https://aws.amazon.com/jp/certificate-manager/pricing/>

AWS Certificate Manager のよくある質問

<https://aws.amazon.com/jp/certificate-manager/faqs/>

本資料に関するお問い合わせ・ご感想

技術的な内容に関しては、有料のAWSサポート窓口へ
お問い合わせください

<https://aws.amazon.com/jp/premiumsupport/>

料金面でのお問い合わせに関しては、カスタマーサポート窓口へ
お問い合わせください（マネジメントコンソールへのログインが必要です）

<https://console.aws.amazon.com/support/home#/case/create?issueType=customer-service>

具体的な案件に対する構成相談は、後述する個別相談会をご活用ください



ご感想はTwitterへ！ハッシュタグは以下をご利用ください
#awsblackbelt



その他コンテンツのご紹介

ウェビナーなど、AWSのイベントスケジュールをご参照いただけます

<https://aws.amazon.com/jp/events/>

ハンズオンコンテンツ

<https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-hands-on/>

AWS 個別相談会

AWSのソリューションアーキテクトと直接会話いただけます

<https://pages.awscloud.com/JAPAN-event-SP-Weekly-Sales-Consulting-Seminar-2021-reg-event.html>



Thank you!



AWS Control Tower

基礎編

桂井 俊朗

Solutions Architect

2023/08

自己紹介

名前：

桂井俊朗 (かつらい としお)

所属：

アマゾンウェブサービスジャパン合同会社
技術統括本部 ISV/SaaS ソリューション本部
ソリューションアーキテクト

好きなAWSサービス：

AWS Control Tower



本セミナーの対象者

マルチアカウント管理について興味のある方

AWS Control Tower に関心のある方

AWS Control Tower をご利用予定の方

アジェンダ

1. マルチアカウント構成
2. AWS Control Tower とは
3. AWS Control Tower 主要機能
4. まとめ

マルチアカウント構成

ビジネスが求めている環境

Secure & compliant

組織のセキュリティや監査要件に適合する

Scalable & resilient

高可用性でスケーラブルなワークフローに対応できる

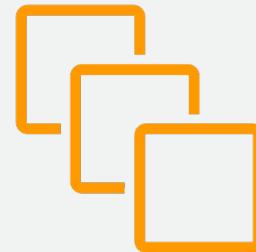
Adaptable & flexible

ビジネス要件の変更に対応するよう設定変更が可能

複数の AWS アカウントを利用することの効果



セキュリティ境界

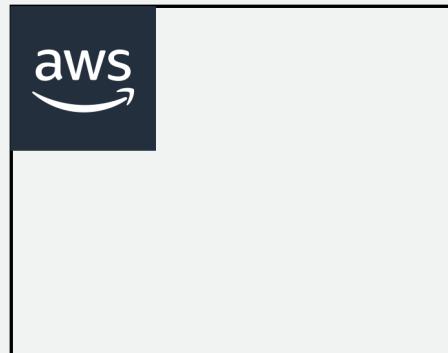


リソースの分離



請求の分離

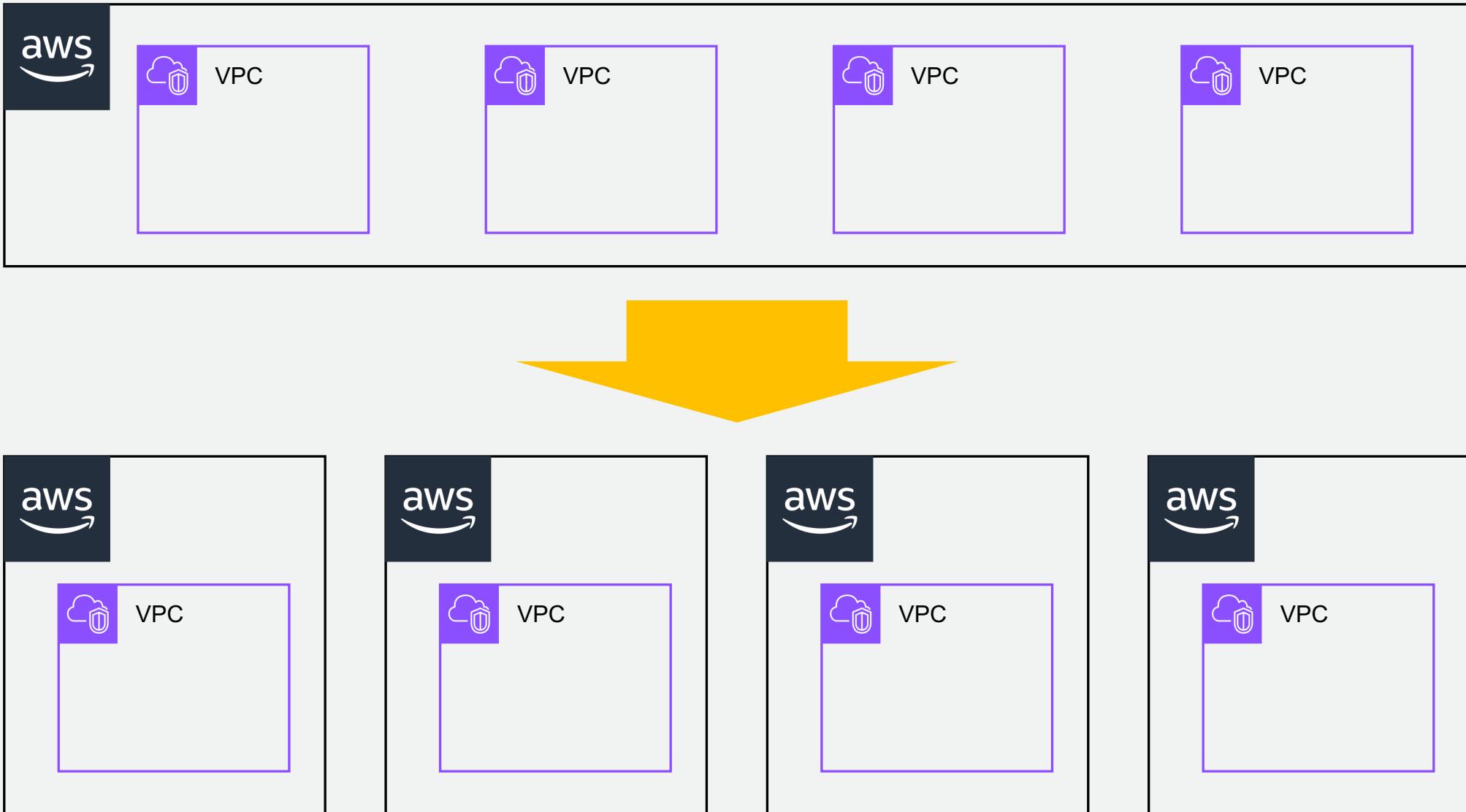
単一の AWS アカウントだけで全てを構成した場合



Everything

- 「グレーな」境界
- 時間経過に伴って複雑で管理が面倒
- リソースのトラッキングが困難
- 責任の範囲が不明確

だから、マルチアカウント構成



マルチアカウント構成に対するよくある疑問

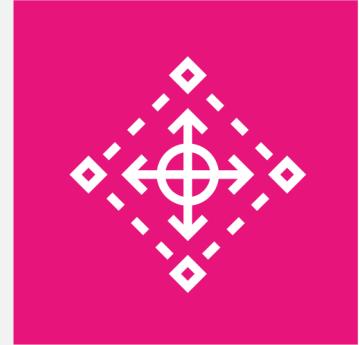


AWS Control Tower とは



AWS Control Tower

マルチアカウント環境のセットアップを自動化する
マネージドサービス



AWS Control Tower



マネージド
サービス

ベストプラクティス
に基づく環境

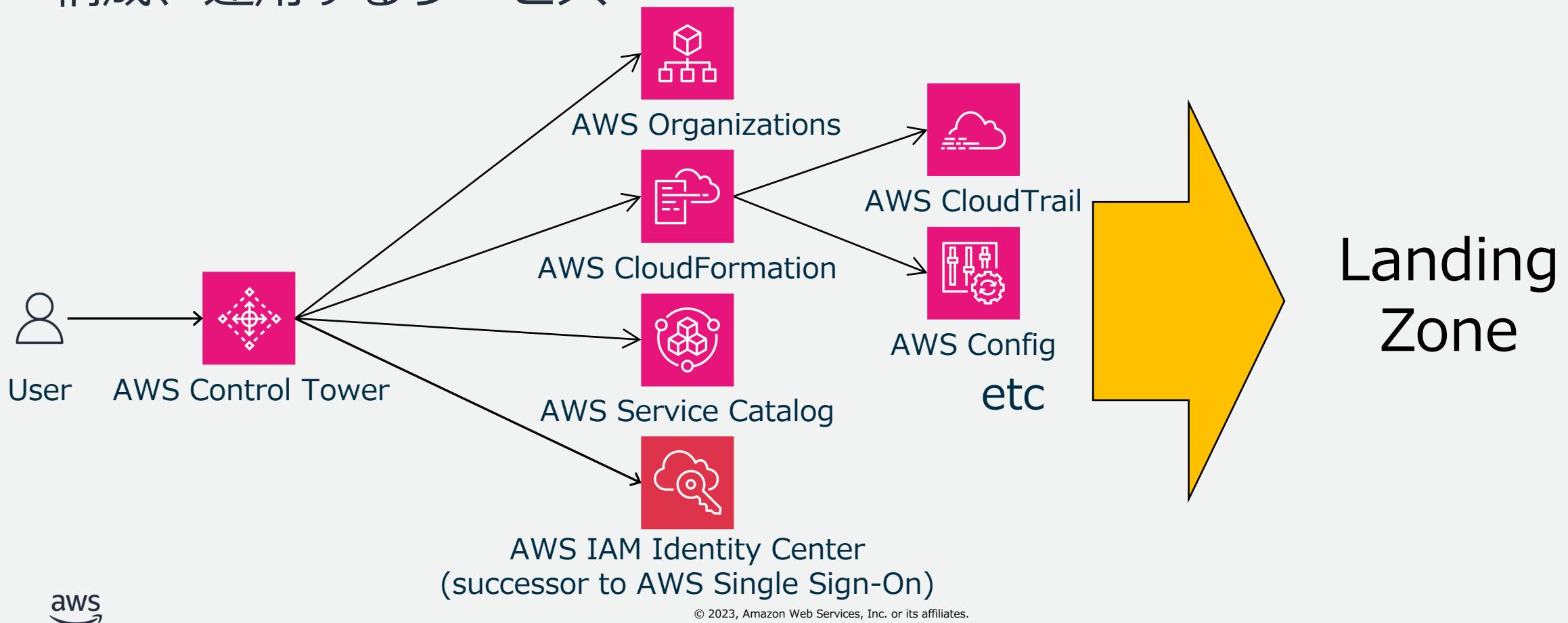
追加料金なし



注意) AWS Control Tower を通じてセットアップするように設定されたサービスは費用が発生する可能性があります

AWS Control Tower = コンフィグジェネレータ

AWS セキュリティサービス群にベストプラクティスに則った設定を投入し、統制を利かせたマルチアカウント環境 (Landing Zone) を構成、運用するサービス

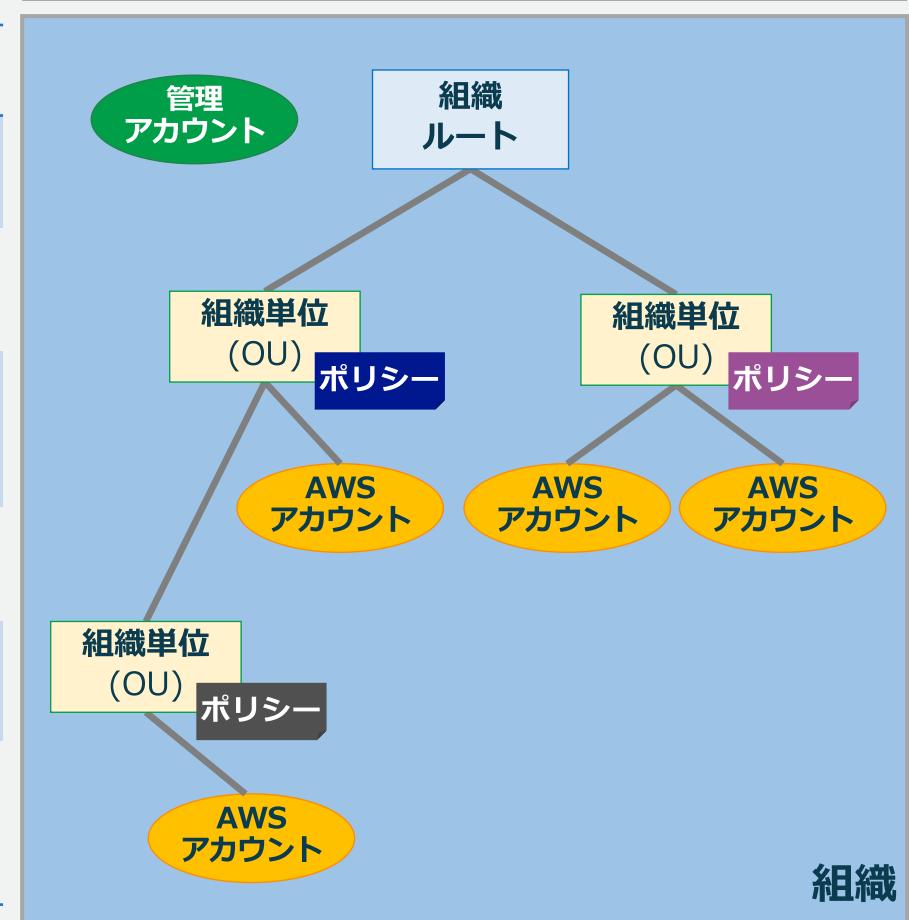


AWS Organizations 概要

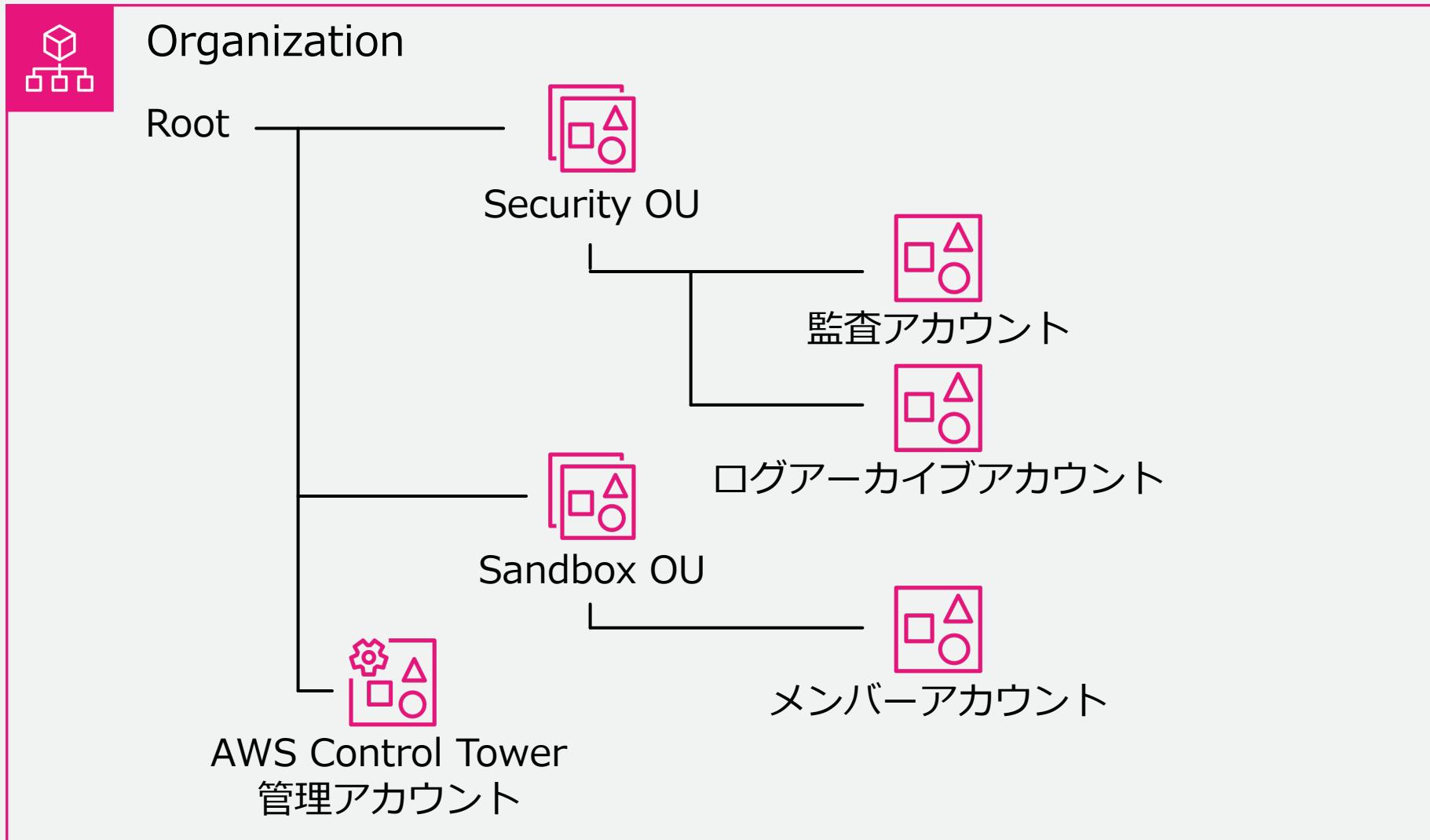
AWS Control Tower も利用する AWS アカウントの一元管理を実現するサービス

用語	説明
組織	・一元管理可能な AWS アカウントの集まり ・最低 1 つの管理アカウントから構成される
管理アカウント	アカウントの作成、招待、削除、ポリシーの適用および組織における支払いアカウント
AWS アカウント	AWS Organizations で管理する最小単位
組織単位 (OU)	組織内の AWS アカウントのグループ
組織ルート	組織単位 (OU) の階層全体の開始点
サービスコントロールポリシー (SCP)	アカウントに適用するコントロールを定義したドキュメントで AWS サービスの API へのアクセスを制御 (許可・拒否) する

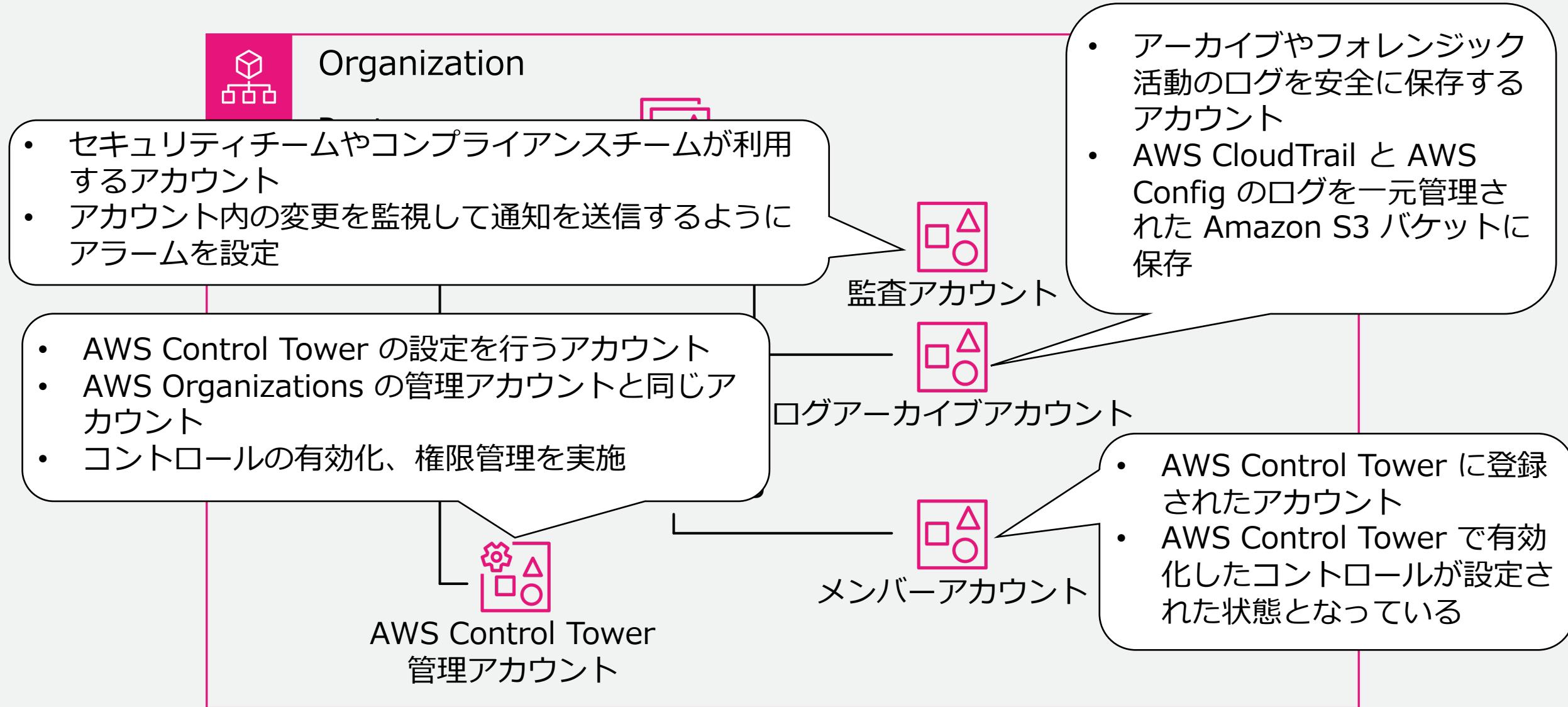
AWS Organizations 概念図



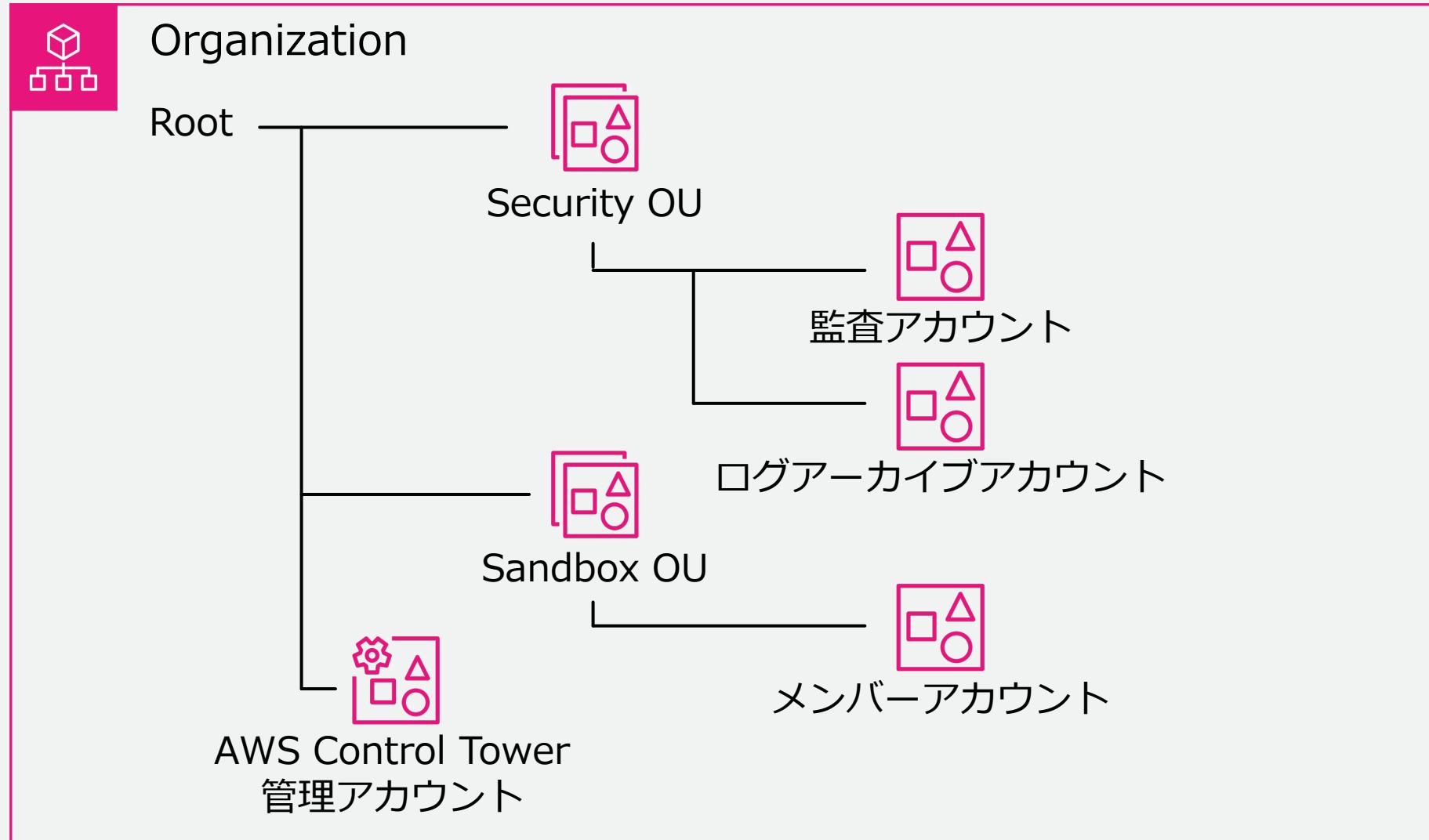
AWS Control Tower のアカウント区分



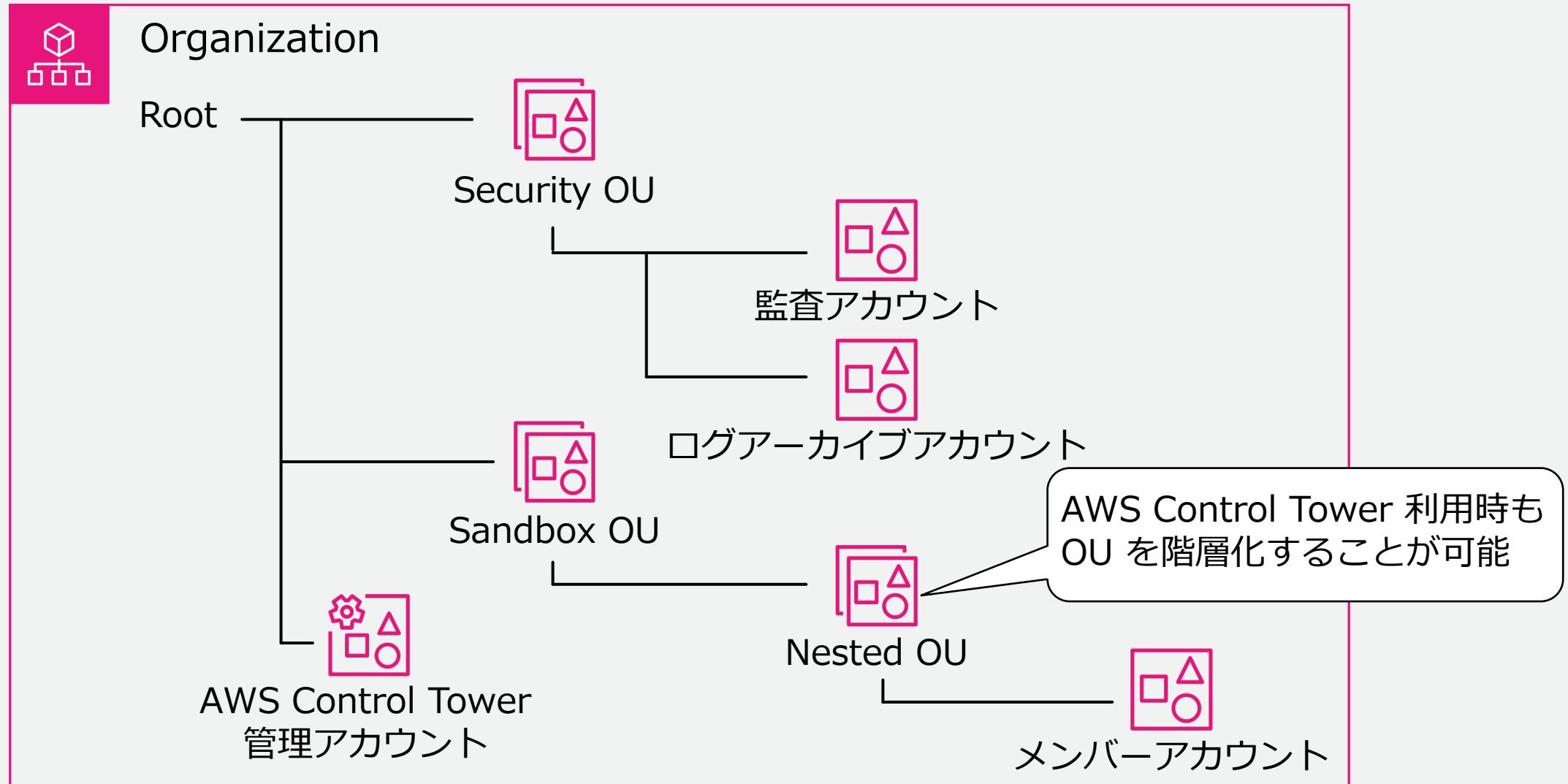
AWS Control Tower のアカウント区分



AWS Control Tower のアカウント区分



AWS Control Tower の OU の階層化



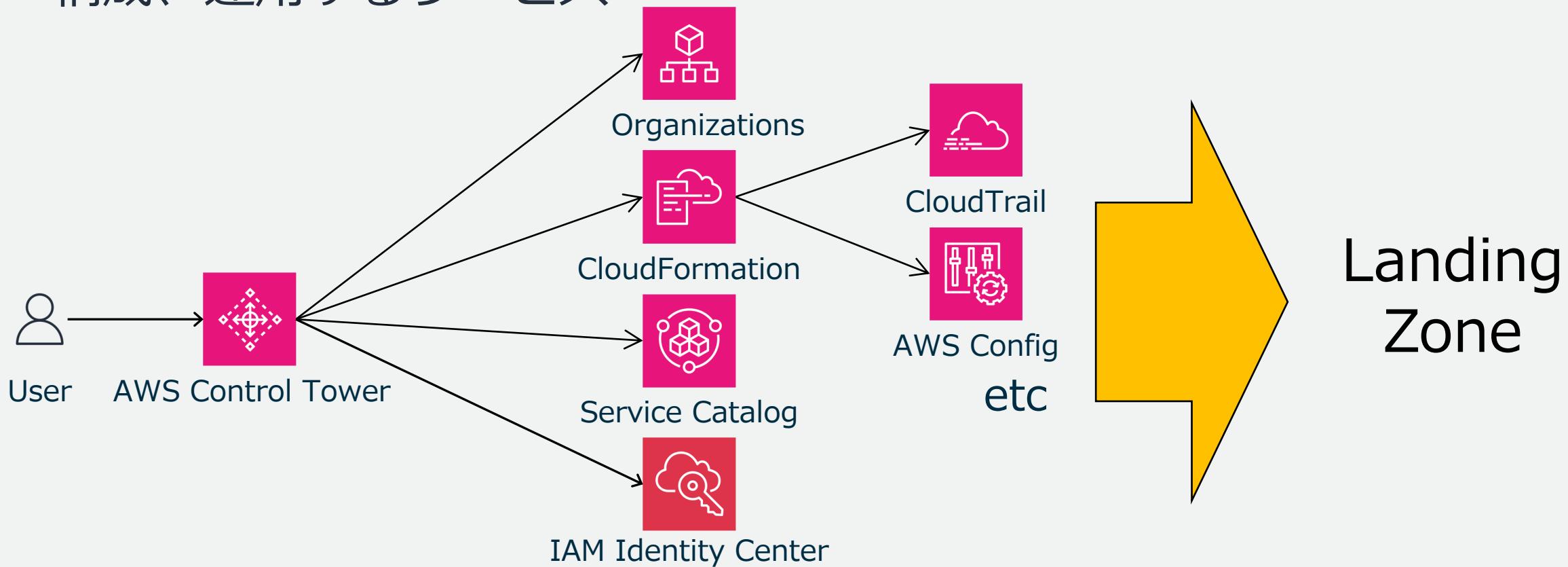
AWS Control Tower 主要機能

AWS Control Tower 主要機能

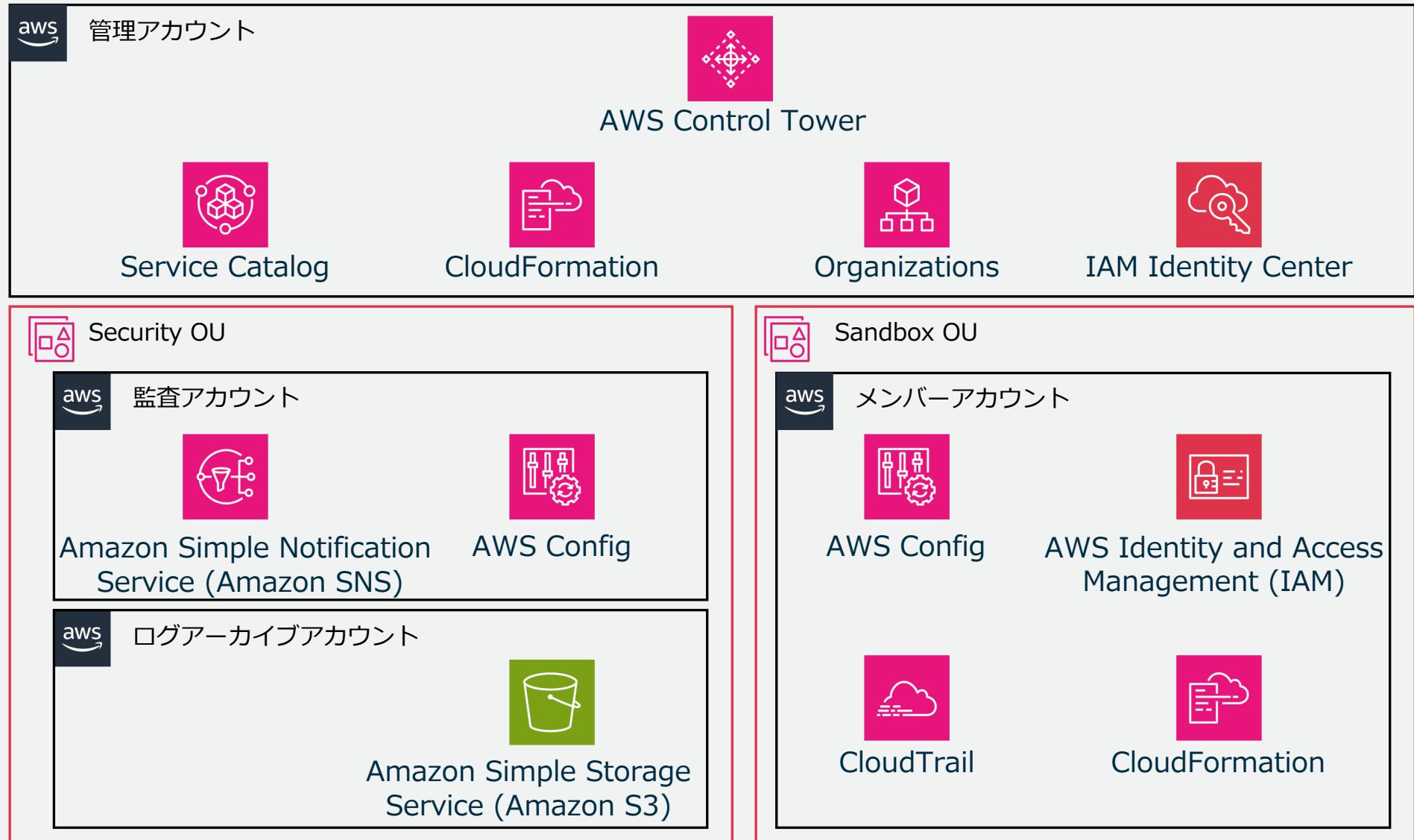
1. ログ集約
2. コントロール適用
3. 通知
4. ID 一元管理
5. AWS アカウント作成とプロビジョニング

AWS Control Tower = コンフィグジェネレータ

AWS セキュリティサービス群にベストプラクティスに則った設定を投入し、統制を利かせたマルチアカウント環境 (Landing Zone) を構成、運用するサービス



ランディングゾーンの実体



AWS Control Tower で実現できること

ログ集約

コントロール適用

通知

ID 一元管理

AWS アカウント作成と
プロビジョニング

aws 管理アカウント



AWS Control Tower



Service Catalog



CloudFormation



Organizations



IAM Identity Center

aws Security OU



Amazon SNS



AWS Config

aws Sandbox OU



AWS Config



IAM

aws ログアーカイブアカウント



Amazon S3



CloudTrail



CloudFormation



AWS Control Tower で実現できること 1

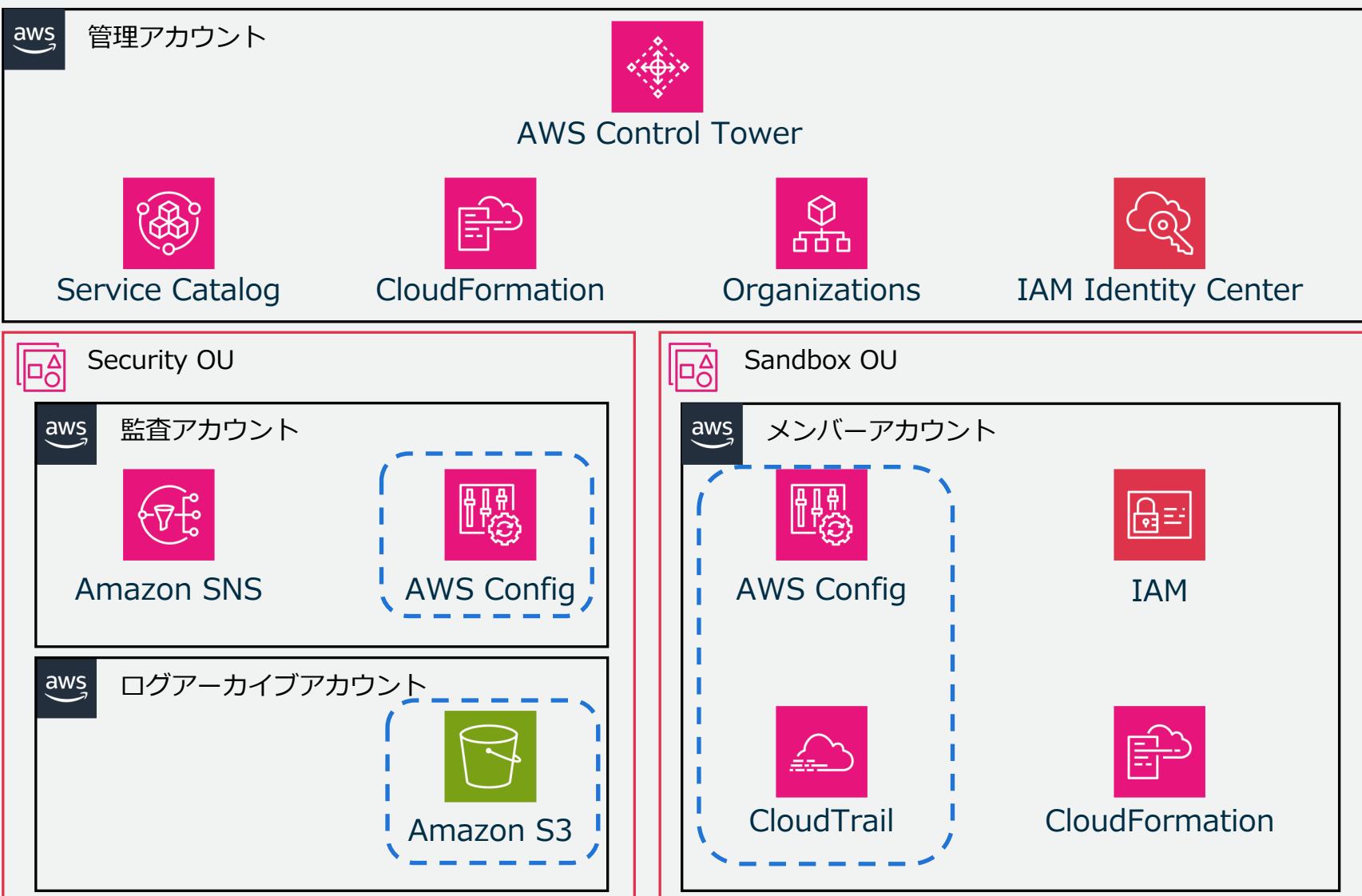
ログ集約

コントロール適用

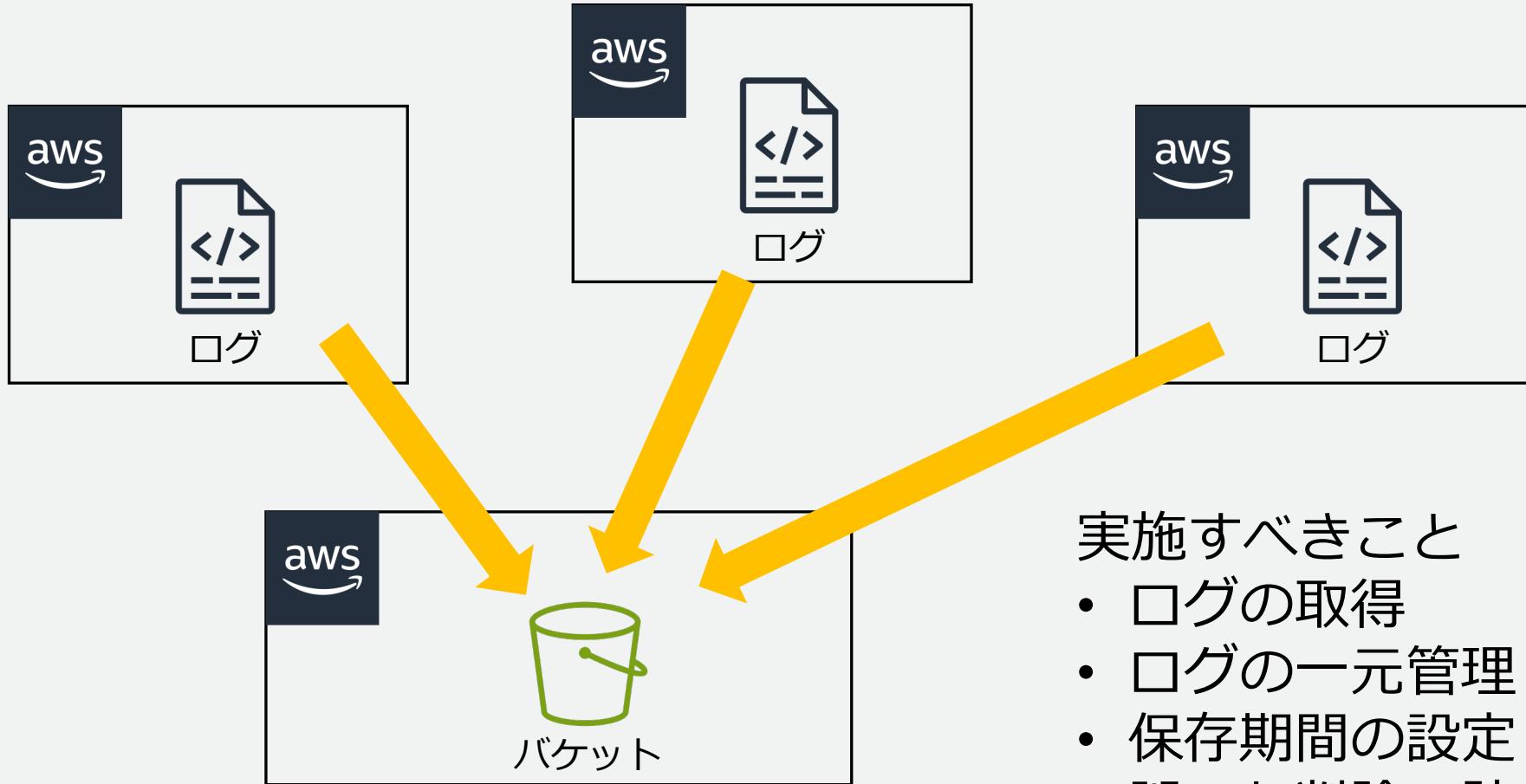
通知

ID 一元管理

AWS アカウント作成と
プロビジョニング



ログ取得の強制と集約



AWS Control Tower で実現できること 1

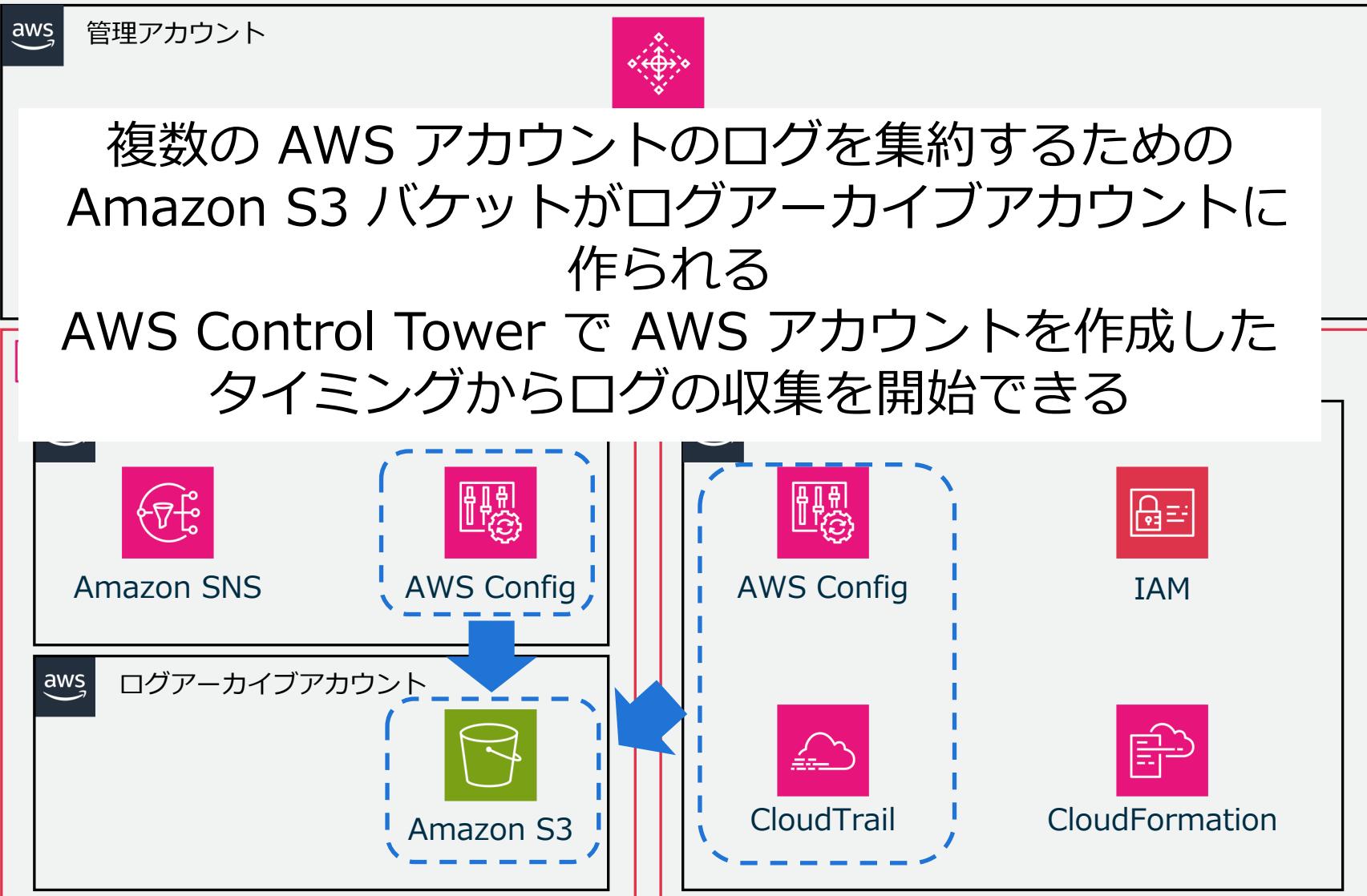
ログ集約

コントロール適用

通知

ID 一元管理

AWS アカウント作成と
プロビジョニング



AWS Control Tower で実現できること 2

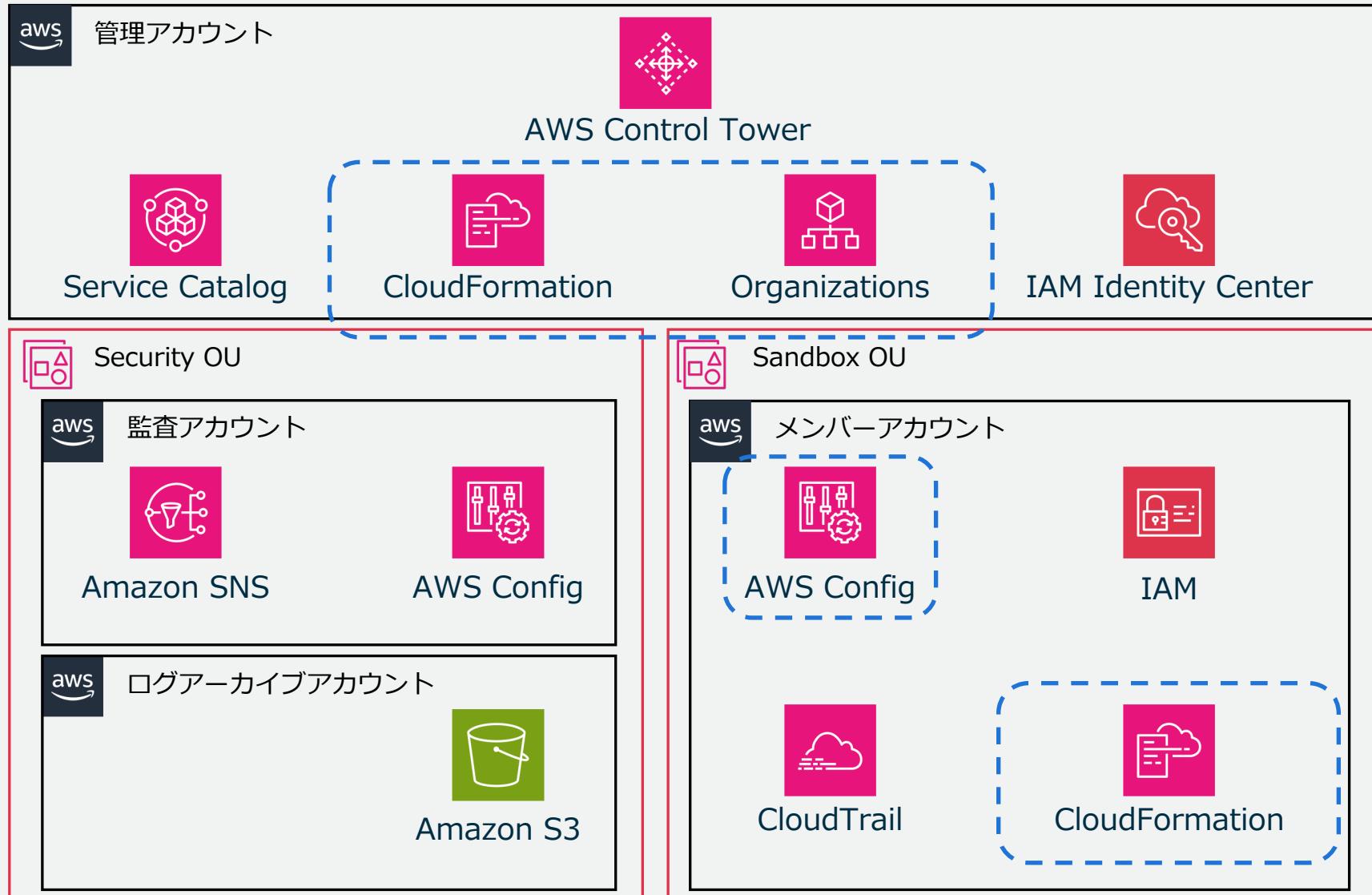
ログ集約

コントロール適用

通知

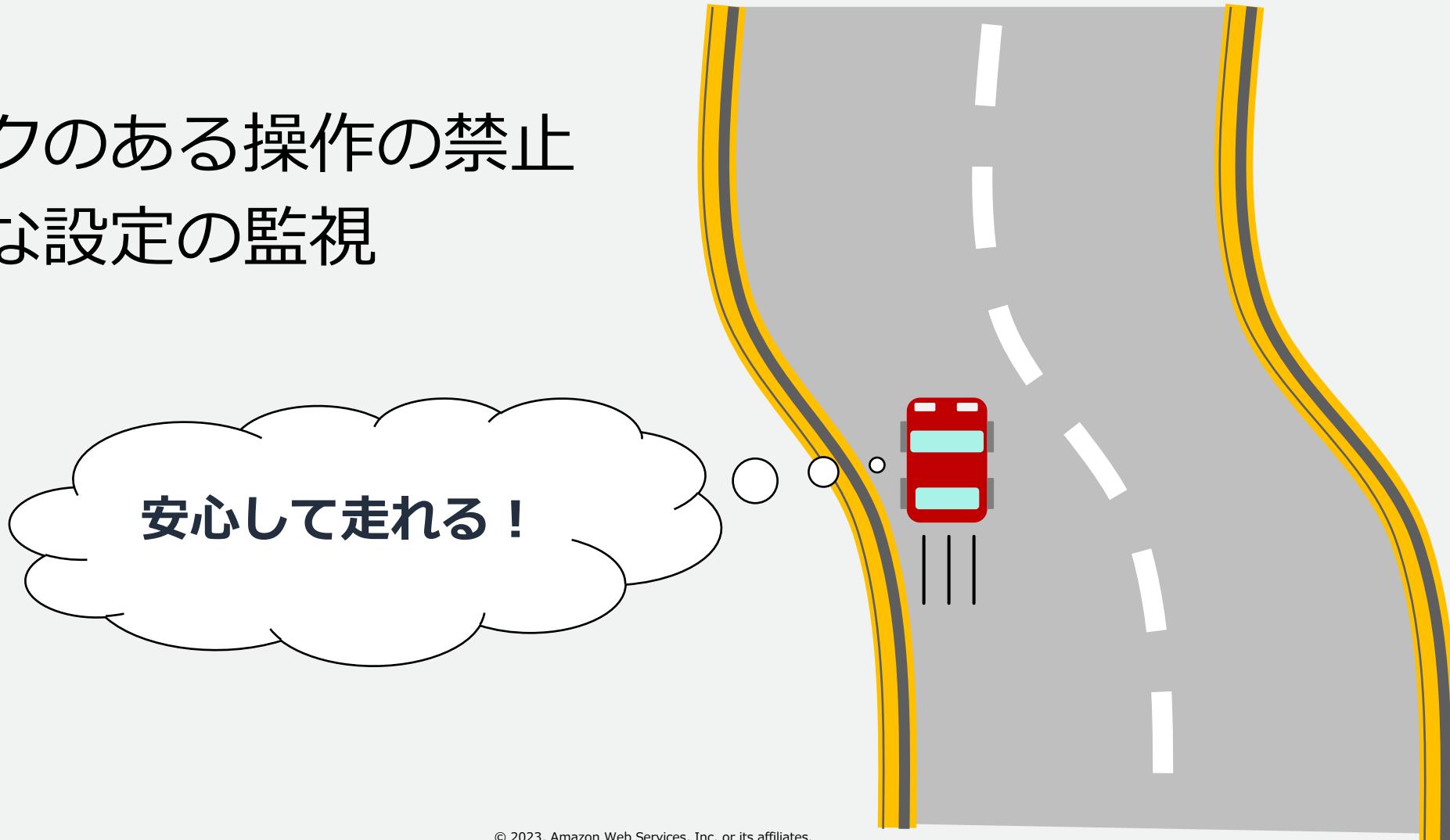
ID 一元管理

AWS アカウント作成と
プロビジョニング



ガードレールという考え方

- ・リスクのある操作の禁止
- ・危険な設定の監視



コントロールの概要

400 を超えるプリセットから要件に合わせて選択

項目	値
サービス	Amazon Kinesis
名前	[SH.Kinesis.1] Kinesis ストリームは保存時に暗号化する必要があります
統制目標	保管中のデータを暗号化
動作	検出
ガイダンス	選択的

動作の種類

- 予防コントロール
 - 対象の操作を実施できないようにする AWS Organizations の SCP で実装
- 検出コントロール
 - 望ましくない操作を行なった場合に発見する AWS Config Rules で実装、AWS Security Hub と連携
- プロアクティブコントロール
 - ルールに沿ったリソースのみを作成可能にする AWS CloudFormation Hooks で実装

ガイダンスの種類

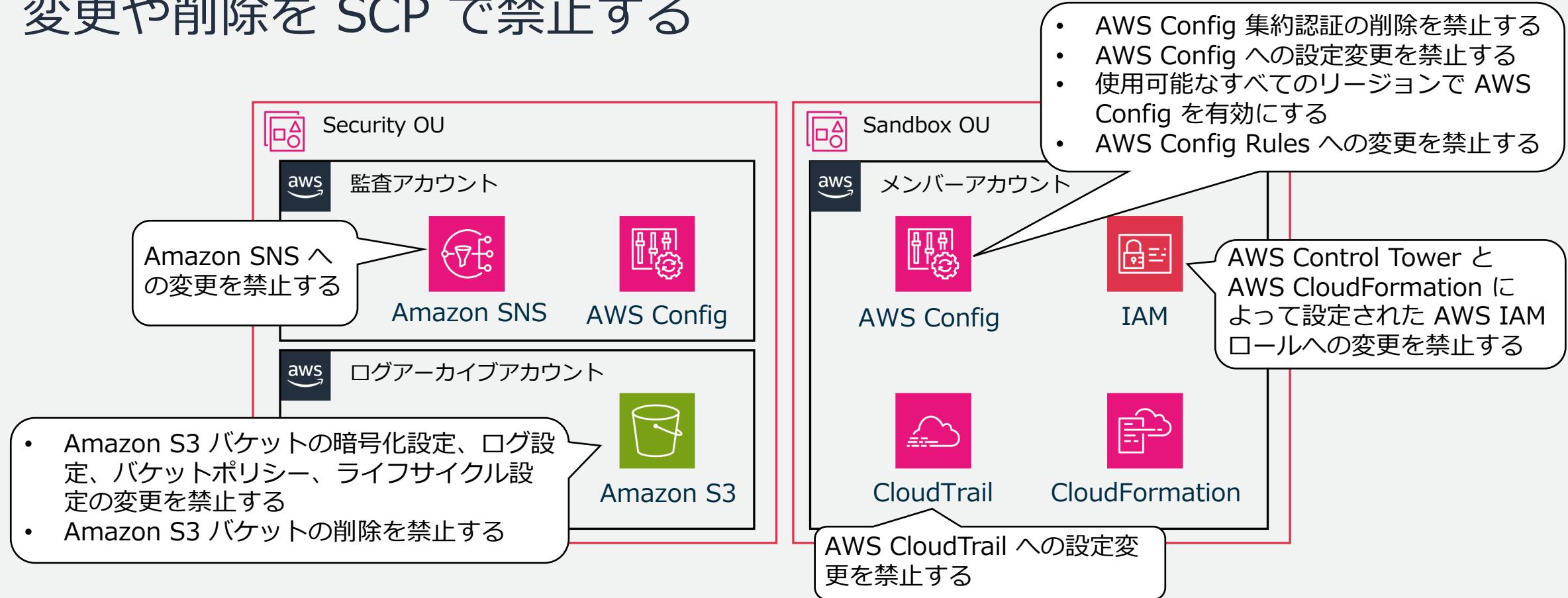
必須、強く推奨、選択的が存在

必須のコントロールはセットアップ時に必ず適用される



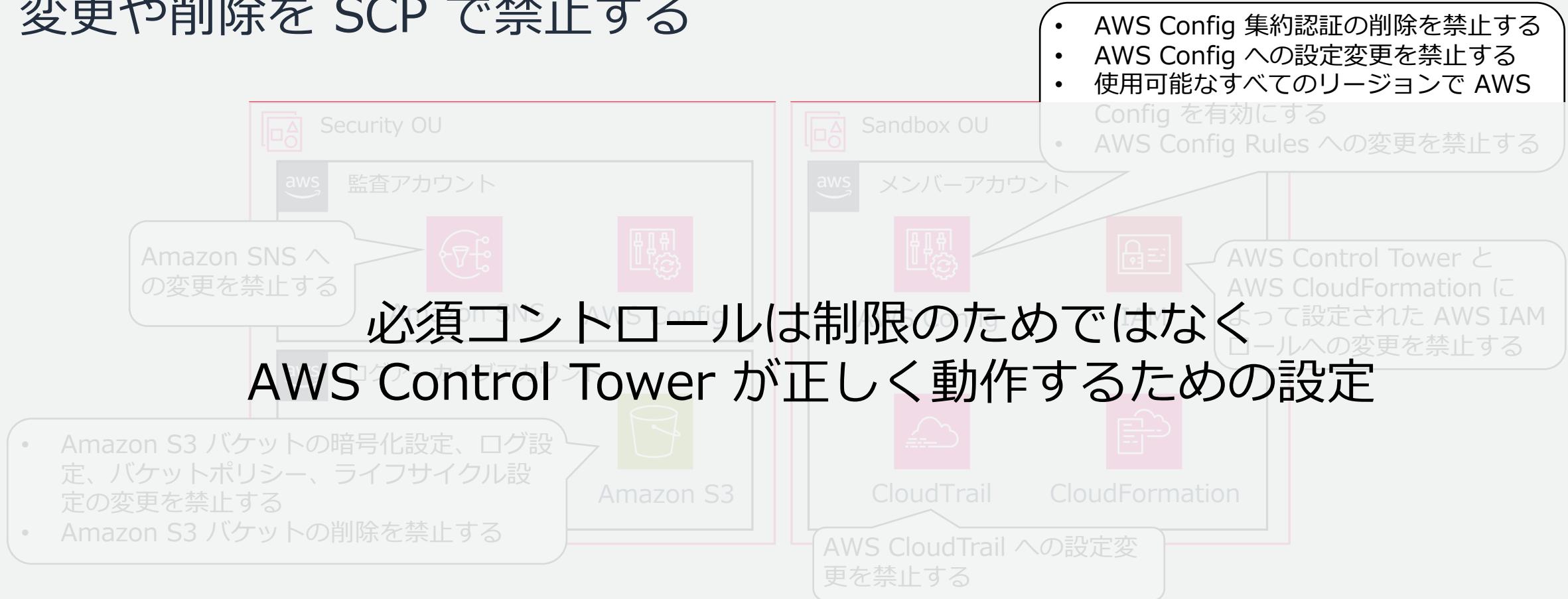
ガイダンスが必須の予防コントロール例

AWS Control Tower で作成、設定したリソースへの
変更や削除を SCP で禁止する



ガイダンスが必須の予防コントロール例

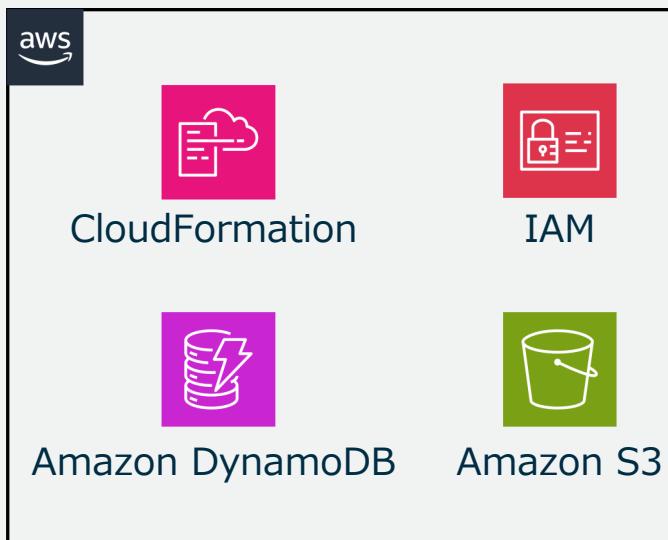
AWS Control Tower で作成、設定したリソースへの
変更や削除を SCP で禁止する



https://docs.aws.amazon.com/ja_jp/controlltower/latest/userguide/mandatory-controls.html

コントロール適用例

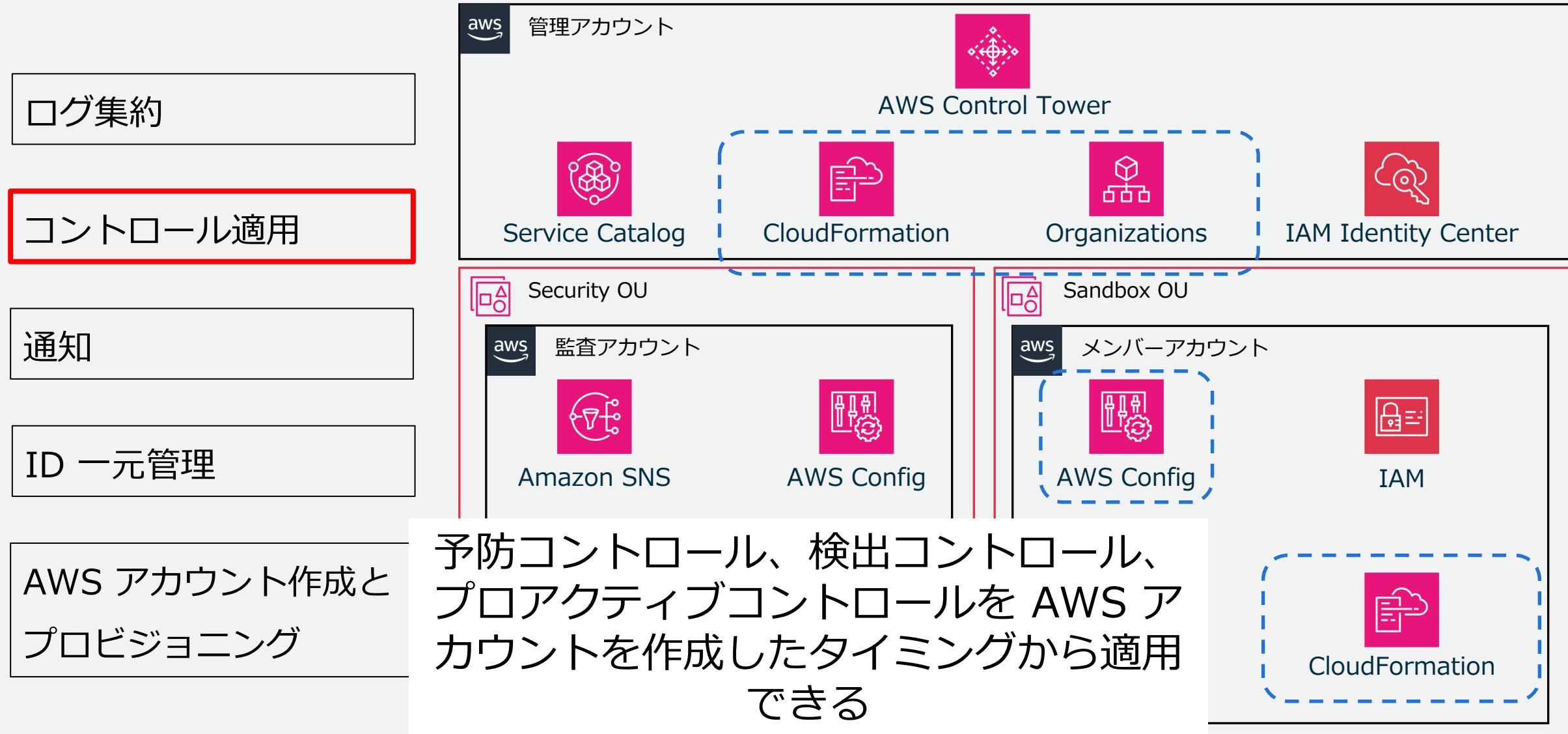
項目	値
サービス	Amazon DynamoDB
名前	[CT.DYNAMODB.PR.2] Amazon DynamoDB テーブルが AWS KMS キーを使用して保管中に 暗号化されることを要求 する
統制目標	保管中のデータを暗号化
動作	プロアクティブ
ガイダンス	選択的



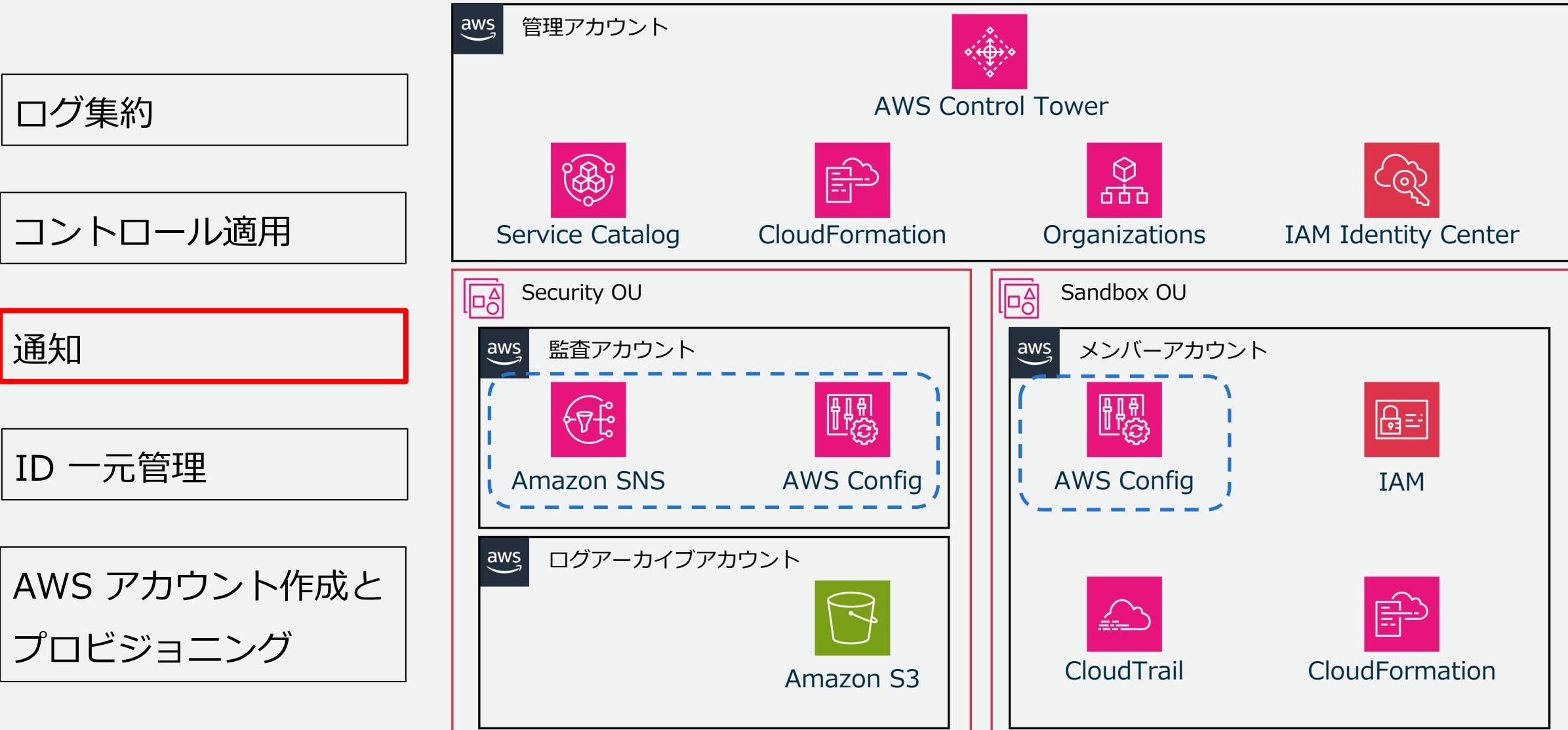
項目	値
サービス	IAM
名前	[AWS- GR_RESTRICT_ROO T_USER] ルートユー ザーとしてのアクショ ンを許可しない
統制目標	最小特権を強制
動作	予防
ガイダンス	強く推奨
項目	値
サービス	Amazon S3
名前	[SH.S3.2] S3 バケッ トはパブリック読み取 りアクセスを禁止する べきです
統制目標	最小特権を強制
動作	検出
ガイダンス	選択的



AWS Control Tower で実現できること 2



AWS Control Tower で実現できること 3

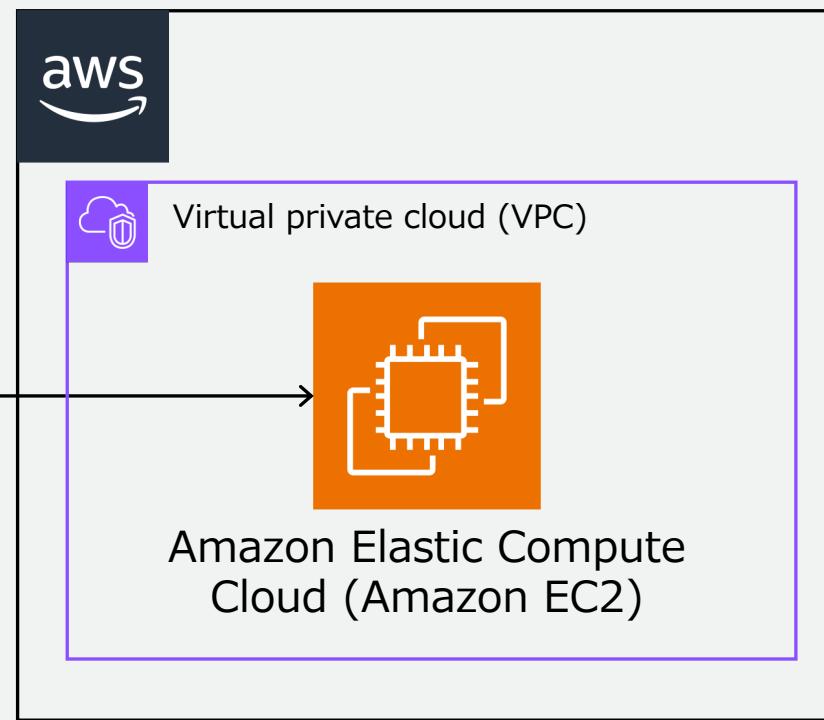


リスクある操作に気づく

急いで検証したいのでセキュリティグループは全開にします！



開発者



その設定はリスクがあるので
変更お願いします！



セキュリティ担当者

AWS Control Tower で実現できること 3



管理アカウント



ログ集約

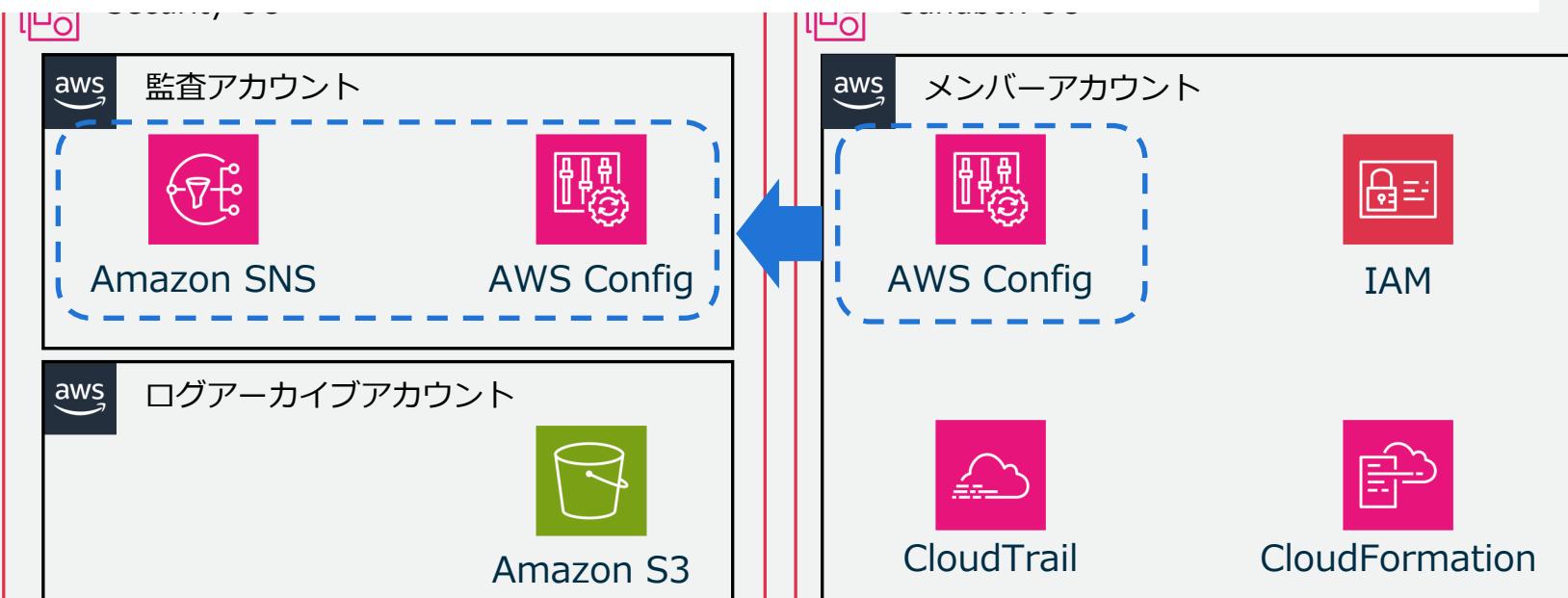
コントロール

通知

ID 一元管理

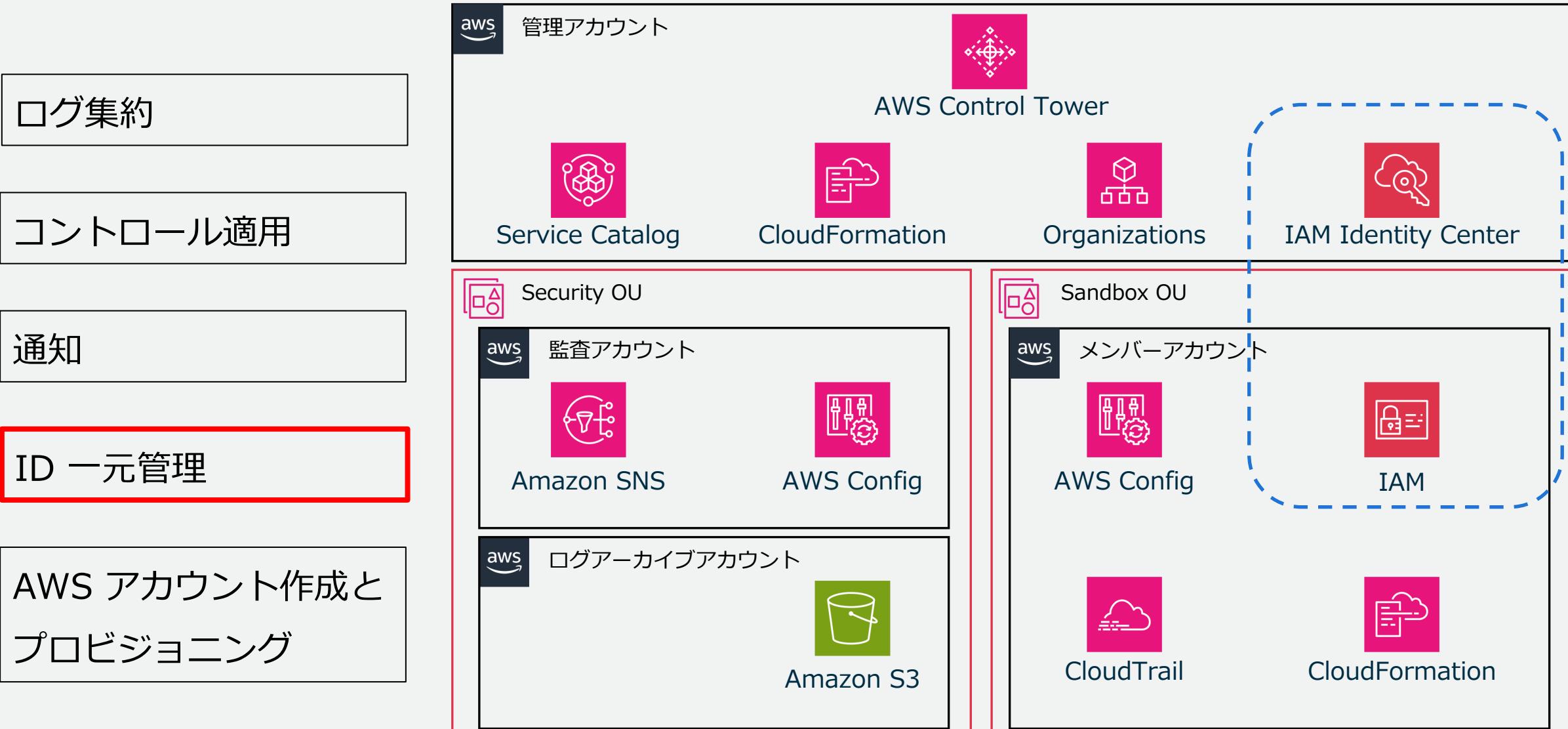
AWS アカウント作成と
プロビジョニング

AWS Config で把握した AWS リソースの変更情報と
AWS Config rules の準拠状況を Amazon SNS を使用して
通知することができる

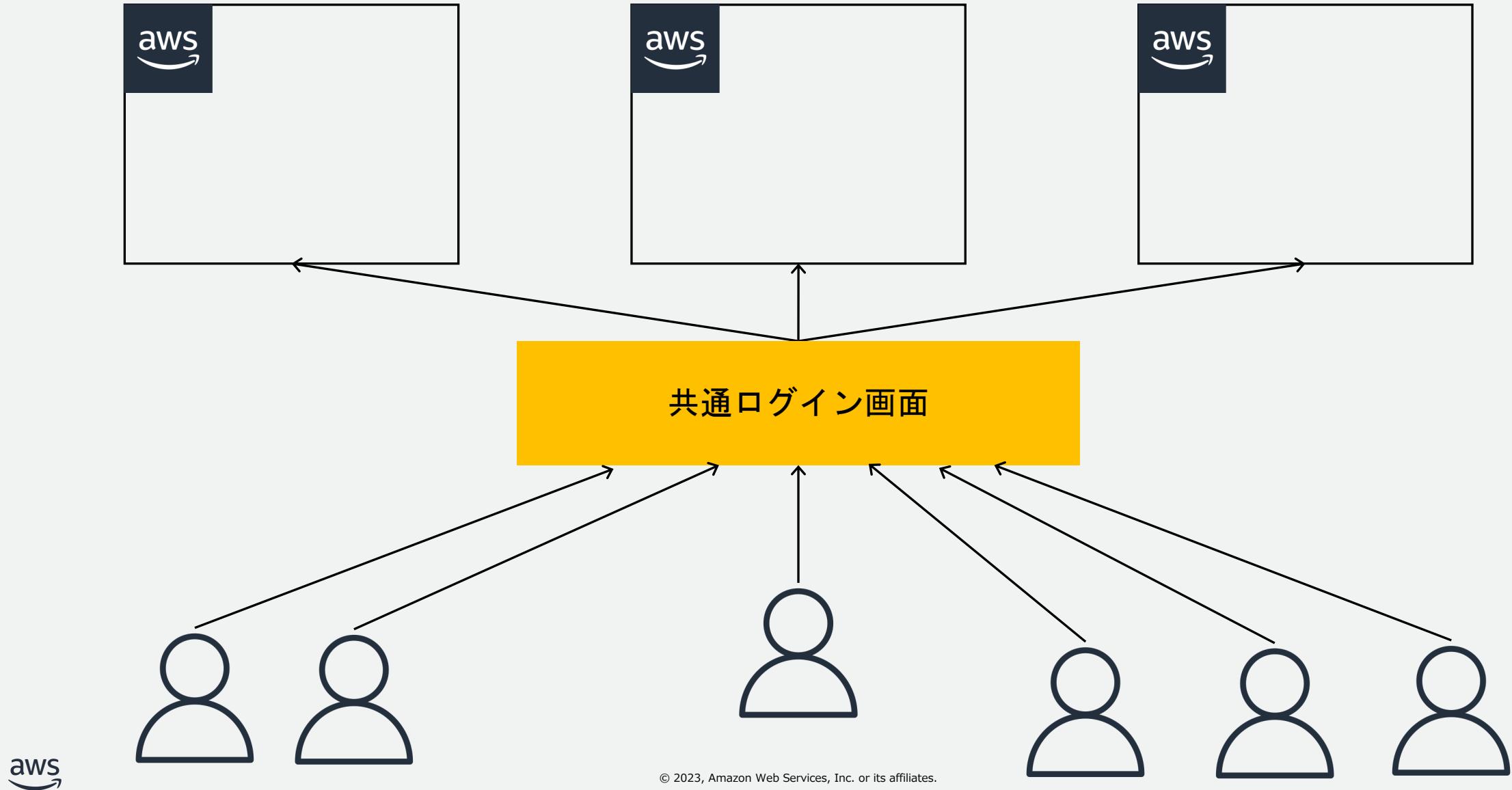


https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/receive-notifications.html

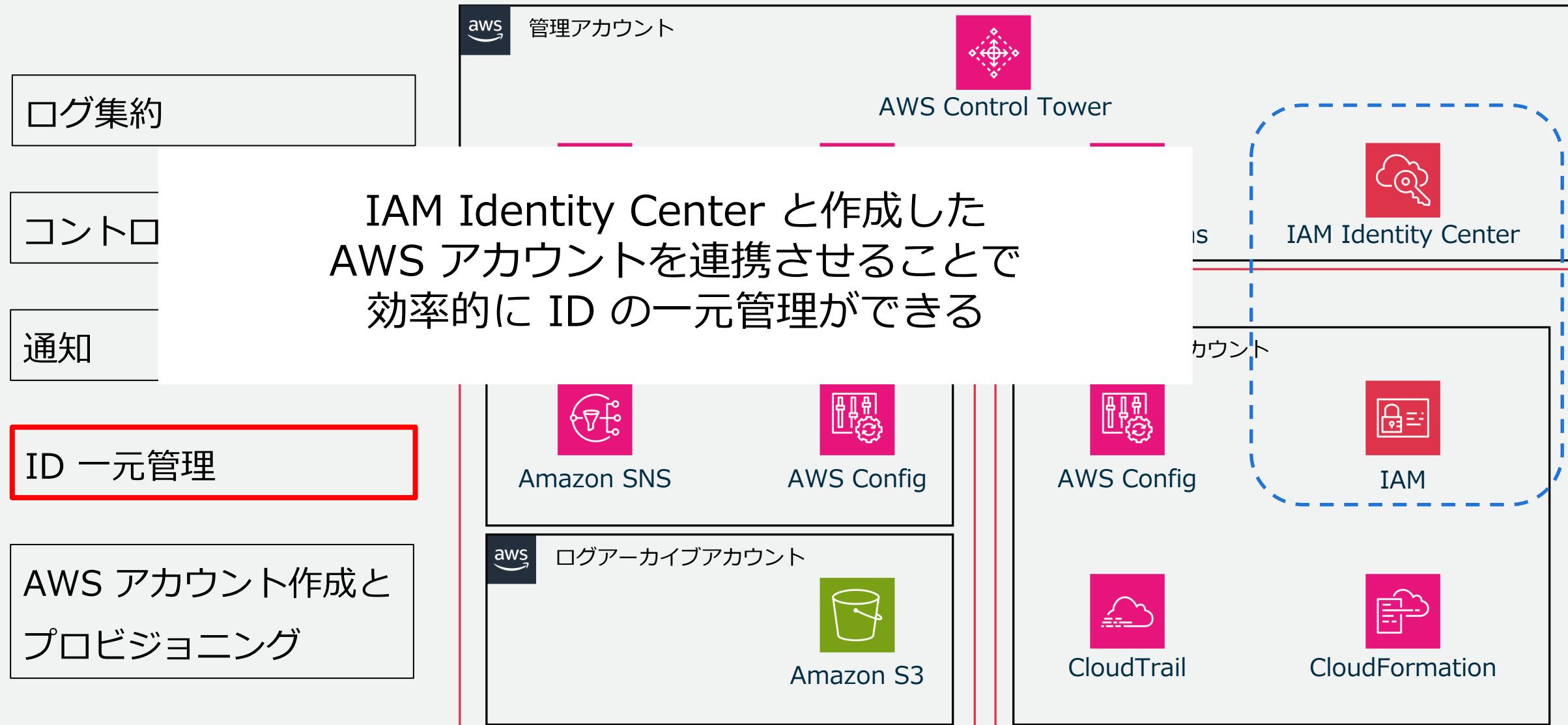
AWS Control Tower で実現できること 4



ログインの導線とユーザ管理を一本化



AWS Control Tower で実現できること 4



AWS Control Tower で実現できること 5

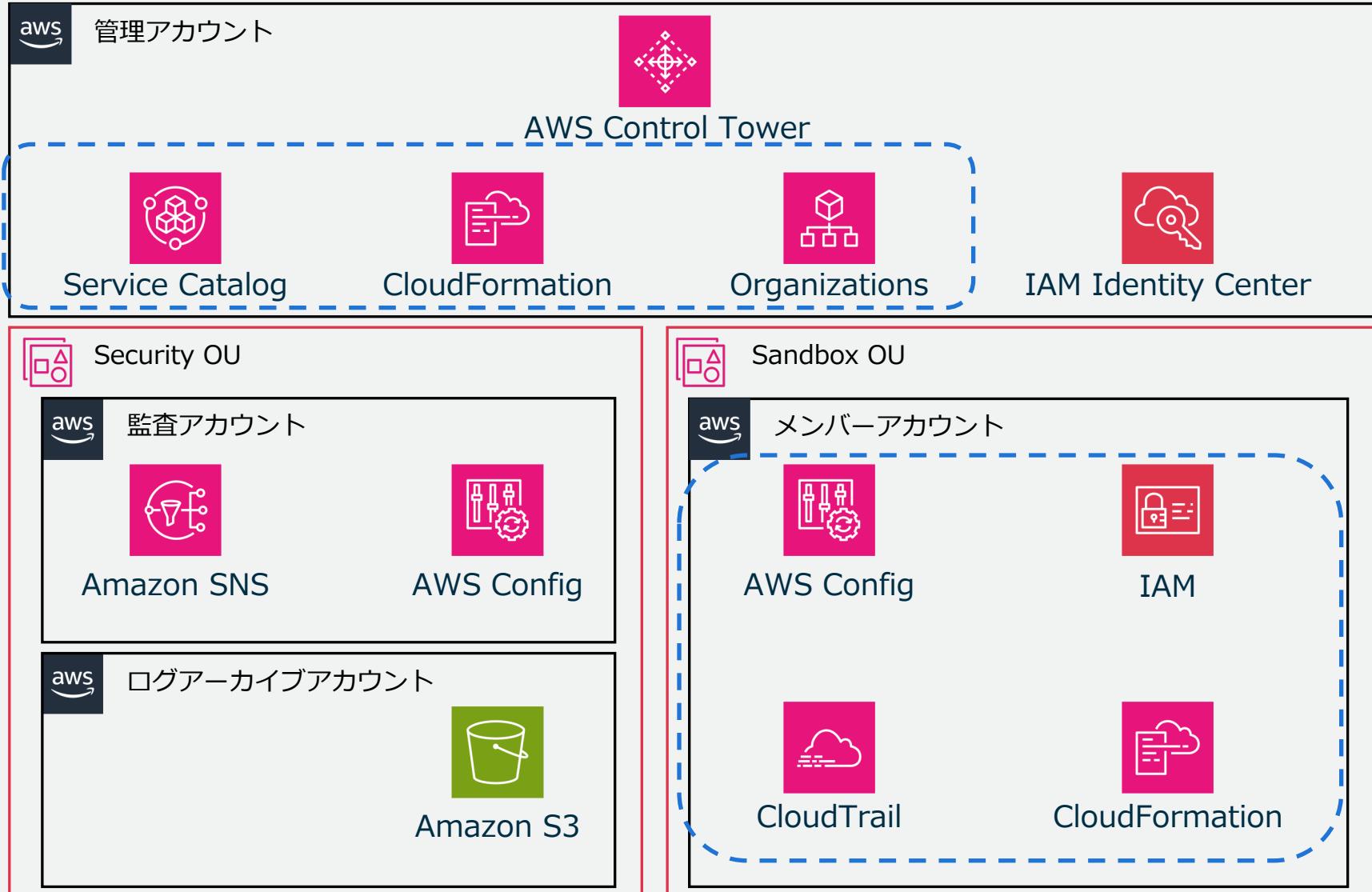
ログ集約

コントロール適用

通知

ID 一元管理

AWS アカウント作成と
プロビジョニング

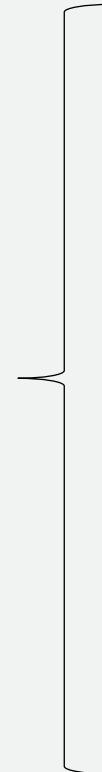


Account Factory で AWS アカウントのプロビジョニング

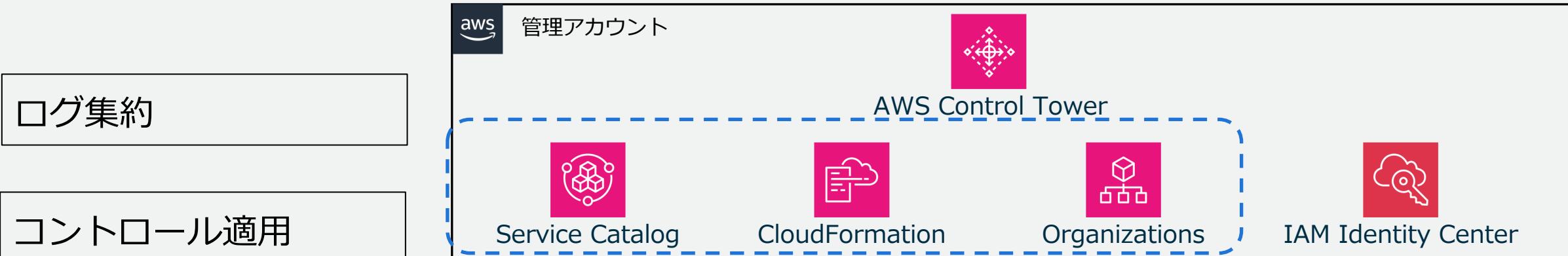
- 各種機能がはじめから設定



- ログ集約
- コントロール

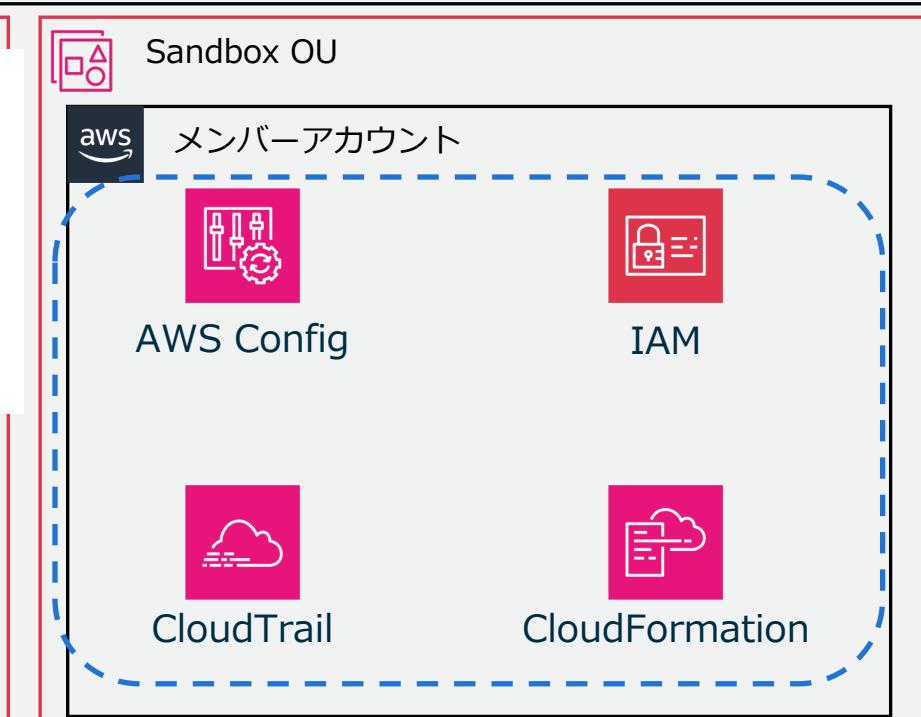


AWS Control Tower で実現できること 5



AWS アカウントの作成とコントロールの適用や
ログ集約の設定を含むプロビジョニングを
効率的に行う事ができる

AWS アカウント作成と
プロビジョニング

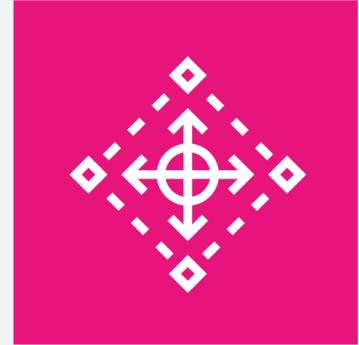


まとめ



AWS Control Tower

マルチアカウント環境のセットアップを自動化する
マネージドサービス



AWS Control Tower



マネージド
サービス

ベストプラクティス
に基づく環境

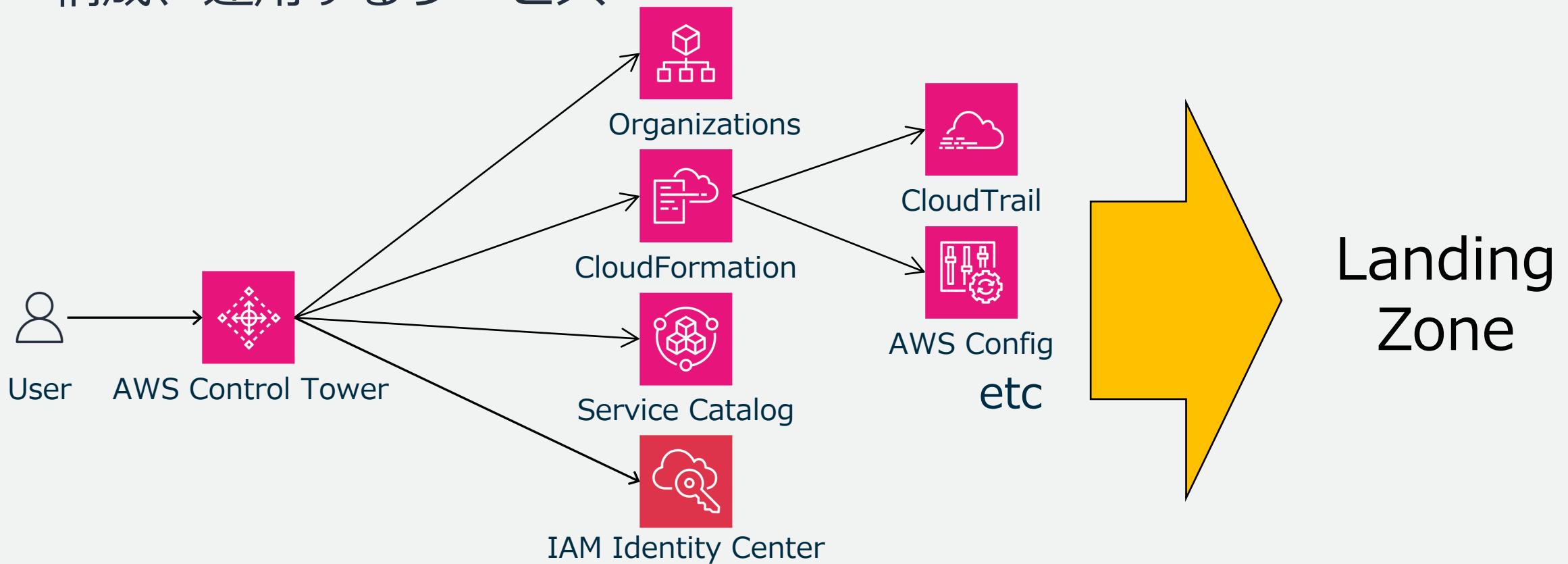
追加料金なし



注意) AWS Control Tower を通じてセットアップするように設定されたサービスは費用が発生する可能性があります

AWS Control Tower = コンフィグジェネレータ

AWS セキュリティサービス群にベストプラクティスに則った設定を投入し、統制を利かせたマルチアカウント環境 (Landing Zone) を構成、運用するサービス



AWS Control Tower で実現できること

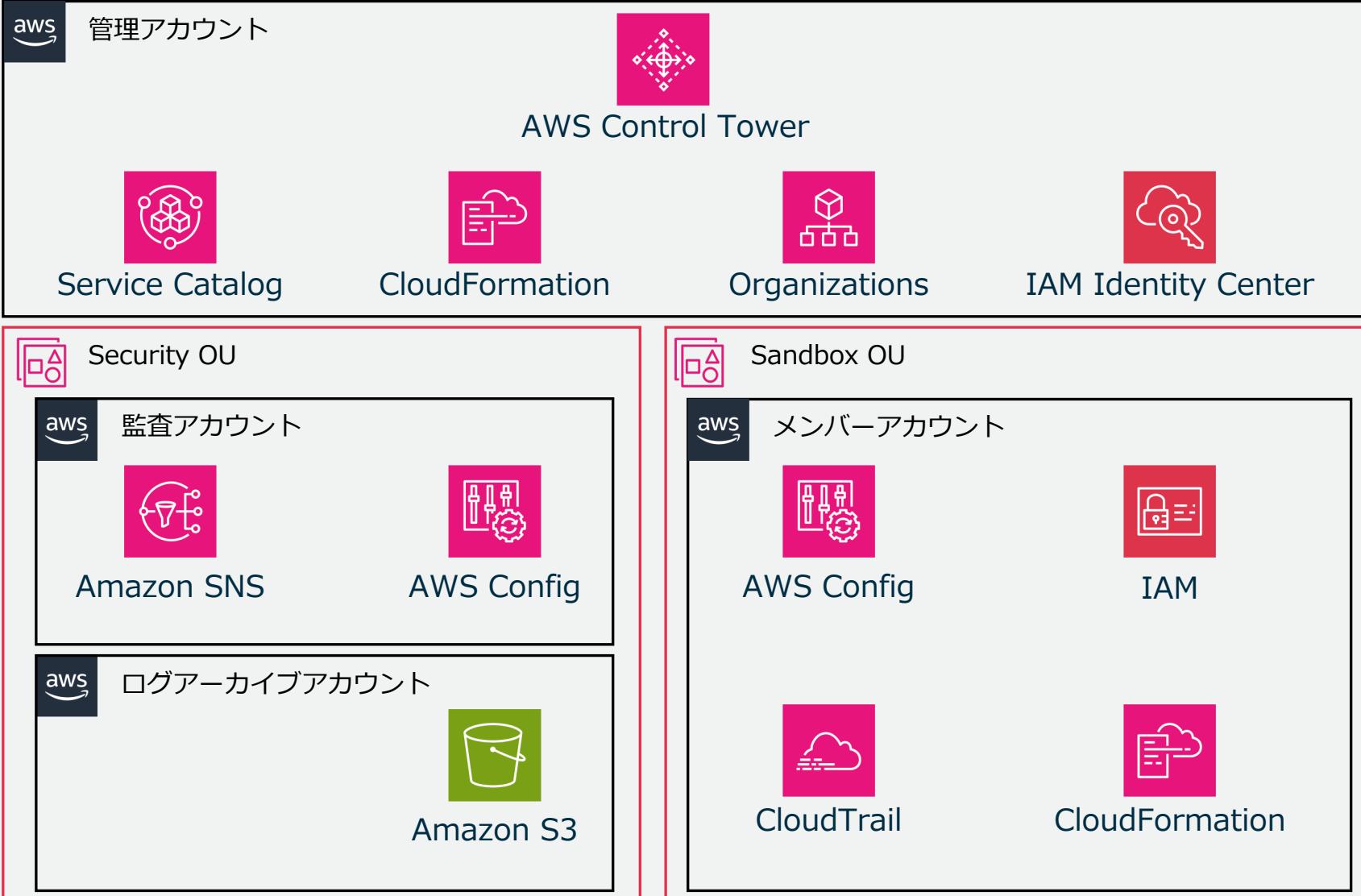
ログ集約

コントロール適用

通知

ID 一元管理

AWS アカウント作成と
プロビジョニング



AWS Black Belt Online Seminar とは

- ・ 「サービス別」「ソリューション別」「業種別」などのテーマに分け、
アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナー
シリーズです
- ・ AWS の技術担当者が、AWS の各サービスやソリューションについてテーマ
ごとに動画を公開します
- ・ 以下の URL より、過去のセミナー含めた資料などをダウンロードするこ
とができます
 - ・ <https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/>
 - ・ <https://www.youtube.com/playlist?list=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBlqY>



ご感想は X (Twitter) へ！ハッシュタグは以下をご利用ください
#awsblackbelt



内容についての注意点

- ・ 本資料では 2023 年 8 月時点のサービス内容および価格についてご説明しています。AWS のサービスは常にアップデートを続けているため、最新の情報は AWS 公式ウェブサイト (<https://aws.amazon.com/>) にてご確認ください
- ・ 資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます
- ・ 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます
- ・ 技術的な内容に関しましては、有料の [AWS サポート窓口](#)へお問い合わせください
- ・ 料金面でのお問い合わせに関しましては、[カスタマーサポート窓口](#)へお問い合わせください (マネジメントコンソールへのログインが必要です)



Thank you!



AWS Control Tower

機能紹介編

桂井 俊朗

Solutions Architect

2023/09

自己紹介

名前：

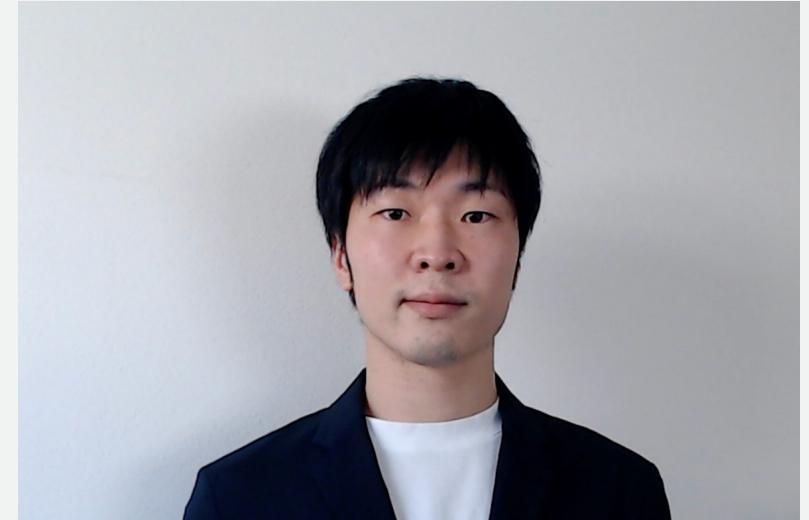
桂井俊朗 (かつらい としお)

所属：

アマゾンウェブサービスジャパン合同会社
技術統括本部 ISV/SaaS ソリューション本部
ソリューションアーキテクト

好きなAWSサービス：

AWS Control Tower



本セミナーの対象者

AWS Control Tower に興味のある方

AWS Control Tower について深く学びたい方

本セミナーの前提知識

AWS Black Belt Online Seminar AWS Control Tower 基礎編

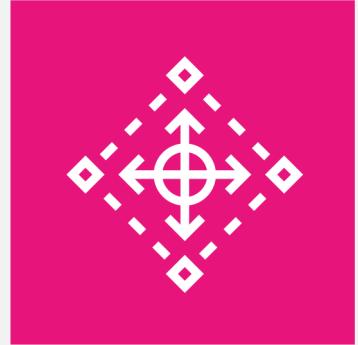
アジェンダ

1. AWS Control Tower とは
2. AWS Control Tower の状態と作成されるリソース
3. AWS Control Tower 機能紹介
4. まとめ

AWS Control Tower とは

AWS Control Tower

マルチアカウント環境のセットアップを自動化する
マネージドサービス



AWS Control Tower



マネージド
サービス



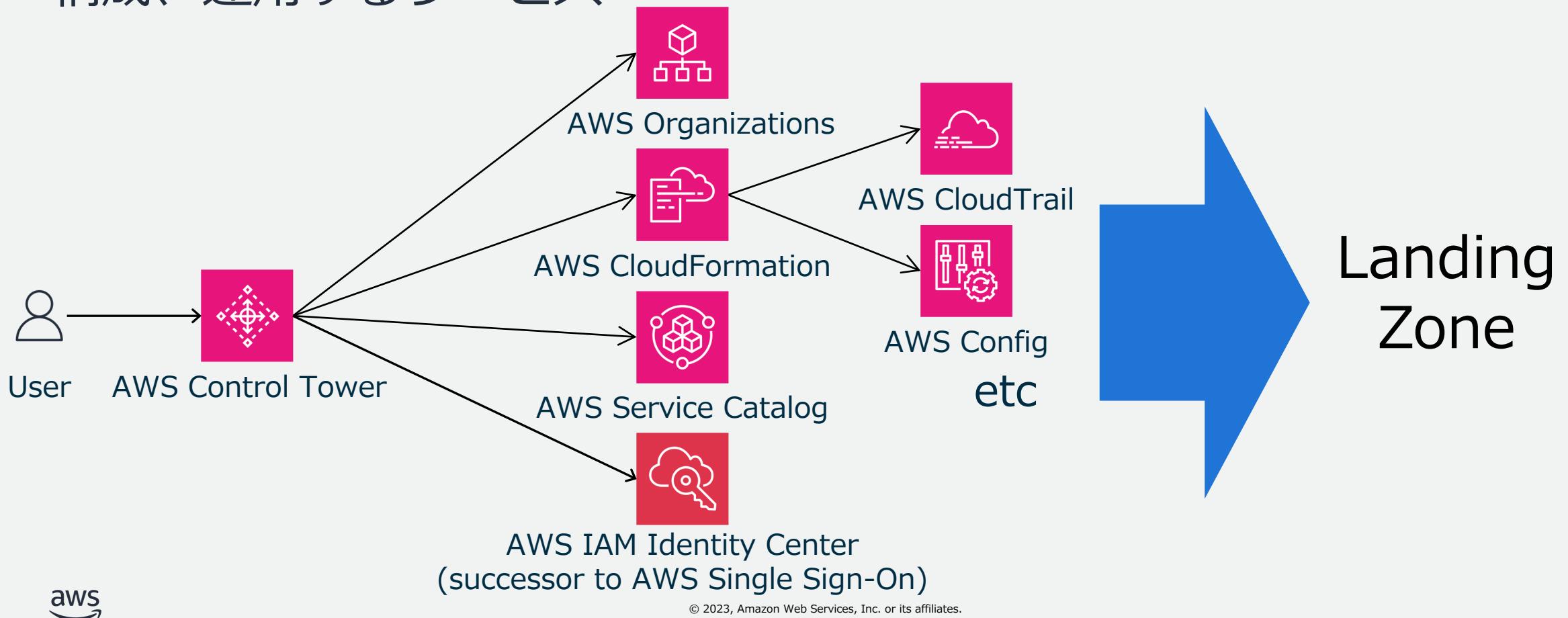
ベストプラクティス
に基づく環境



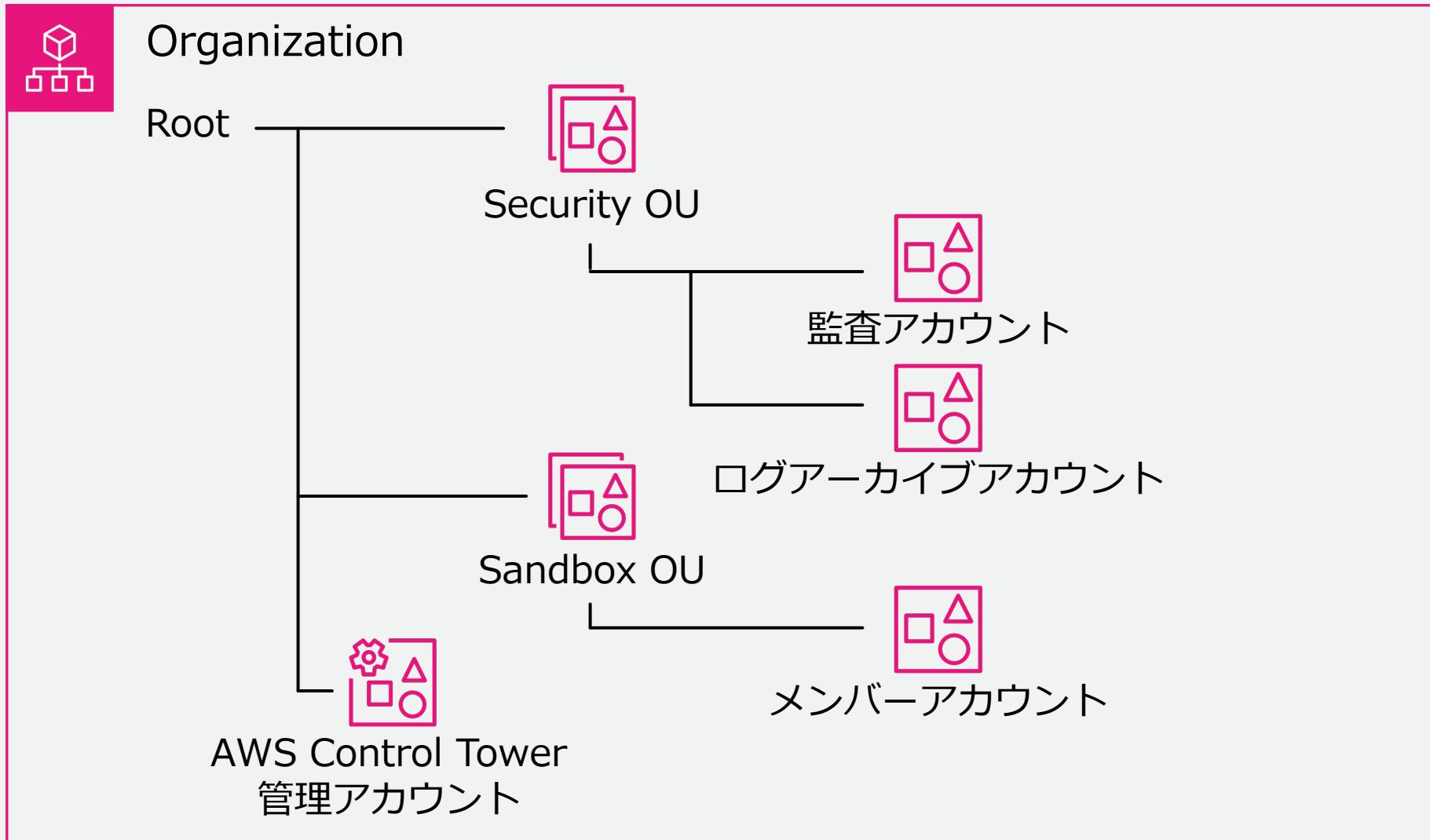
追加料金なし

AWS Control Tower = コンフィグジェネレータ

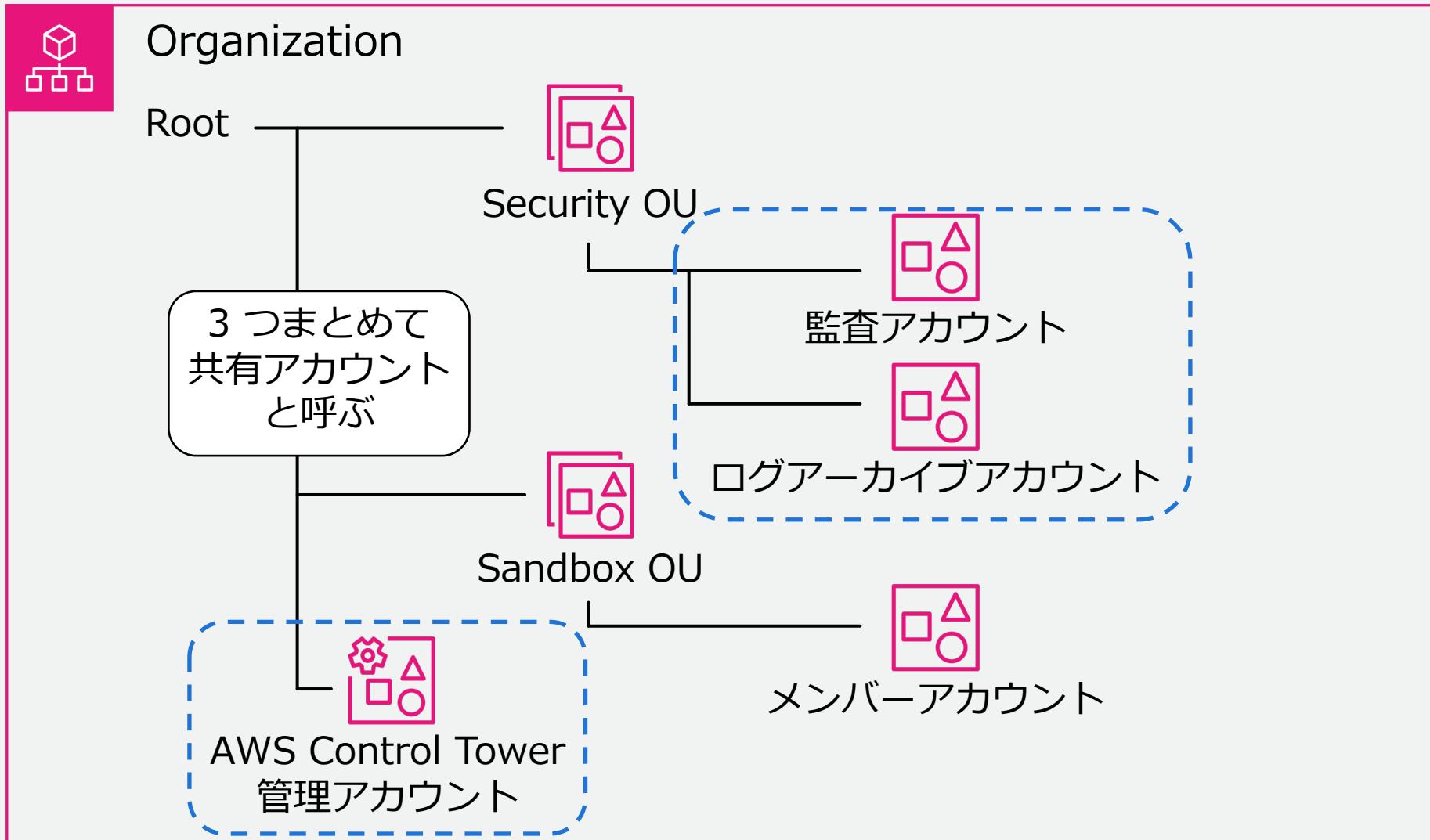
AWS セキュリティサービス群にベストプラクティスに則った設定を投入し、統制を利かせたマルチアカウント環境 (Landing Zone) を構成、運用するサービス



AWS Control Tower のアカウント区分



AWS Control Tower のアカウント区分



AWS Control Tower で実現できること

ログ集約

コントロール適用

通知

ID 一元管理

AWS アカウント作成と
プロビジョニング

aws 管理アカウント



AWS Control Tower



AWS Service Catalog



AWS CloudFormation



AWS Organizations



AWS IAM Identity Center

aws Security OU



Amazon Simple Notification Service (Amazon SNS)



AWS Config

aws Sandbox OU



メンバーアカウント



AWS Identity and Access Management (IAM)

aws ログアーカイブアカウント



Amazon Simple Storage Service (Amazon S3)



AWS CloudTrail



AWS CloudFormation



AWS Control Tower の状態と 作成されるリソース

AWS Control Tower の状態

AWS Control Tower で管理対象となるアカウントには
状態が存在する

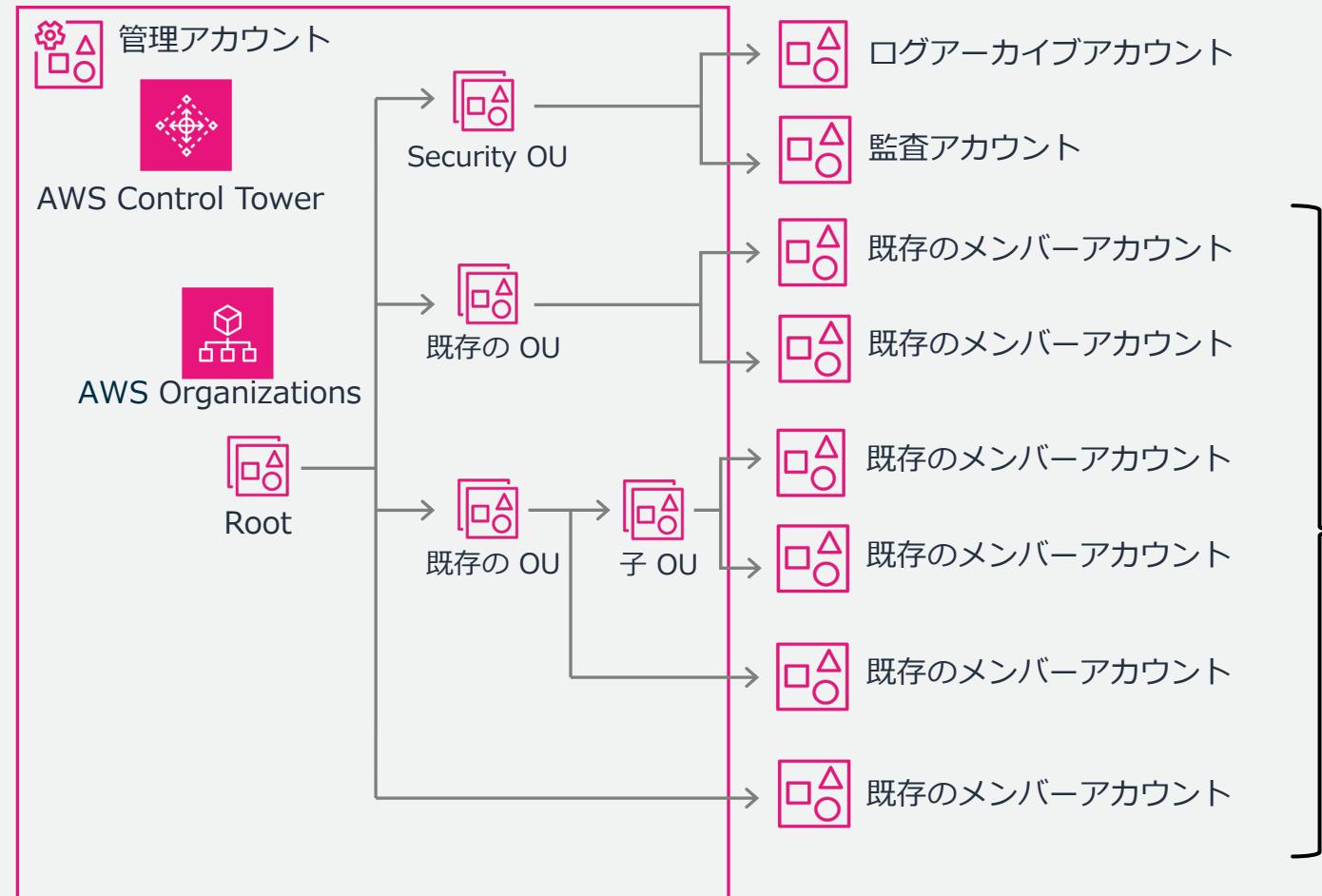
状態	説明
未登録	アカウントは親 OU のメンバーですが、AWS Control Tower によって管理されていません
登録中	AWS Control Tower の管理対象になっています。親 OU のコントロール設定に適合するようにアカウントが調整されています
登録済み	アカウントは、その親 OU 用に設定されたコントロールによって管理されています。AWS Control Tower によって管理されています
登録に失敗しました	登録を試みましたが、アカウントを AWS Control Tower に登録できません
更新が利用可能	アカウントは登録済みですが、アカウントには利用可能な更新があります。環境に加えられた最近の変更を反映するには、アカウントを更新する必要があります

初期は「未登録」で登録を実行すると「登録済み」に遷移する



メンバーアカウントの登録

- ・ランディングゾーンのセットアップだけでは、登録されない



別途 AWS Control Tower への登録作業が必要となる

AWS Control Tower 利用時のリソース作成タイミング

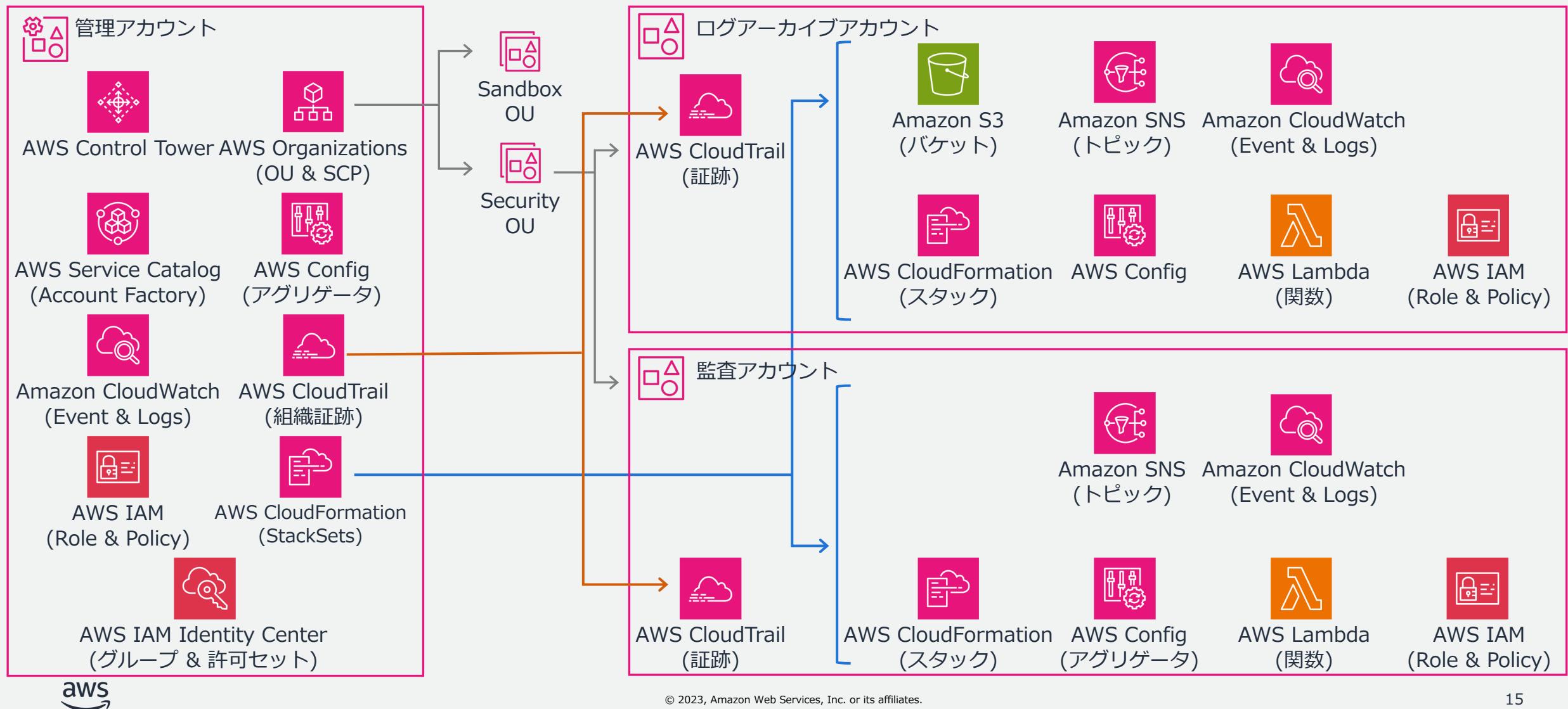
いつ、どのアカウントでリソース作成が行われるか

管理アカウント	監査アカウント	ログアーカイブ アカウント	メンバーアカウント
ランディングゾーン セットアップ	リソース作成あり	リソース作成あり	リソース作成あり AWS CloudTrail 証跡 が作成される
Account Factory で アカウント作成	リソース作成なし	リソース作成なし	リソース作成なし リソース作成あり
AWS Control Tower への登録	リソース作成なし	リソース作成なし	リソース作成なし リソース作成あり

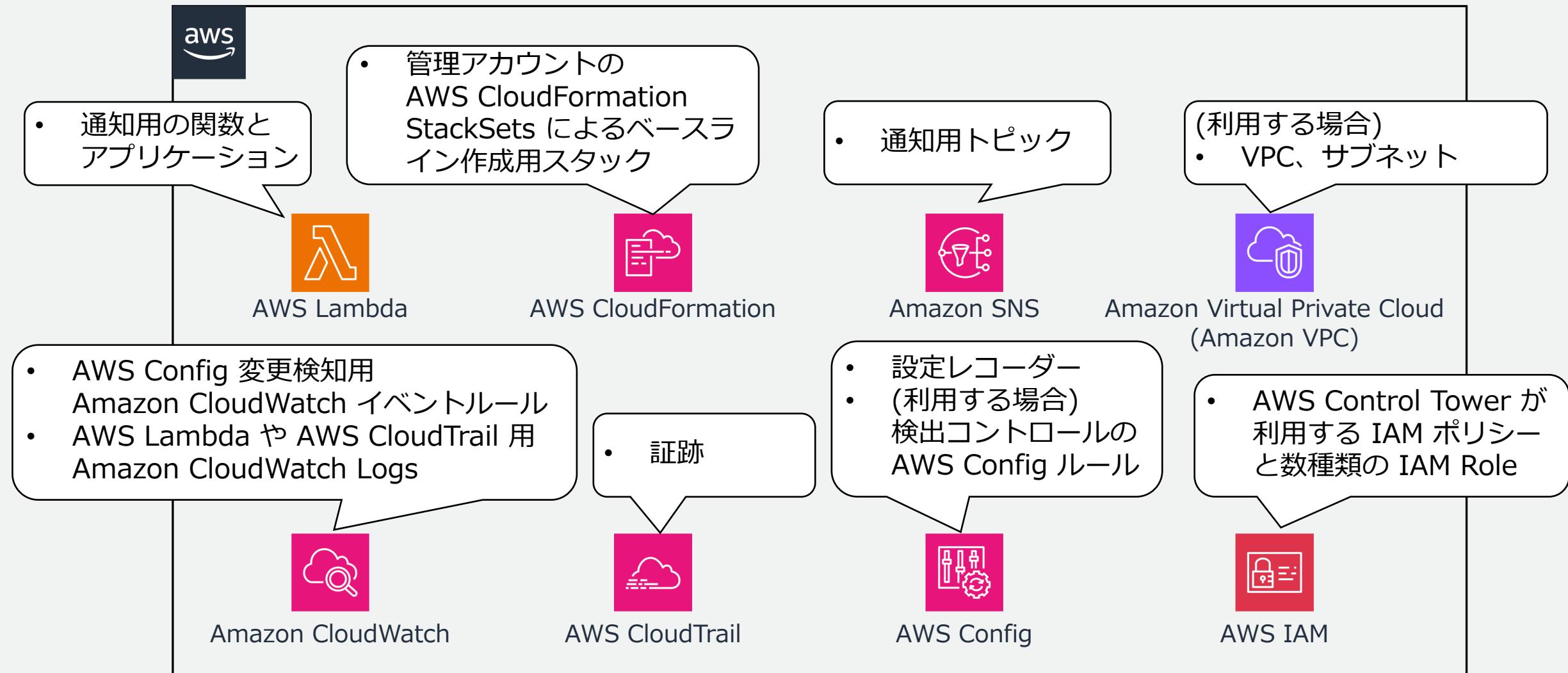
ランディングゾーンセットアップによるメンバーアカウントへの変化は
AWS CloudTrail 証跡が作成されること

Account Factory でアカウント作成もしくは AWS Control Tower への登録によって
AWS Control Tower 管理対象となった時点でメンバーアカウントにリソース作成される

AWS Control Tower の有効化で作成されるリソース



メンバーアカウントで作成される AWS リソース



https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/account-factory-considerations.html

AWS Control Tower 機能紹介

紹介する機能

The screenshot shows the AWS Control Tower dashboard with several navigation links highlighted by a red box:

- ダッシュボード
- はじめに
- 組織
- Account Factory
- ▼ コントロールライブラリ
 - カテゴリー
 - すべてのコントロール
- ユーザーとアクセス
 - 共有アカウント
 - ランディングゾーン設定
- Control Tower 向け AWS Marketplace
- AWS Control Tower の新機能を見る
- AWS Control Tower ブログを表示
- 入門ライブラリでソリューションを起動
- フィードバックパネルに参加

Below the sidebar, there are five main sections:

- ## 1. ランディングゾーン

環境の概略 有効な統制の概要

組織単位	アカウント
27	5
予防管理	検出管理
プロアクティブ管理	
- ## 2. コントロール

組織単位 9 アカウント
- ## 3. Account Factory

リソース ID | リソースタイプ | サービス | リージョン | アカウント名 | 組織単位 | コントロール

非準拠リソース
非準拠リソースが見つかりませんでした
Clear ステータスのコントロールでは、非準拠のリソースは検出されませんでした。
- ## 4. 組織

登録済み組織単位

組織単位	状態	コンプライアンス
Root	登録済み	準拠
Security	登録済み	準拠
- ## 5. ダッシュボード

ランディングゾーン

ランディングゾーン設定の項目

- 現在のバージョン
- AWS KMS キーの暗号化
- AWS CloudTrail
- ホームリージョン
- ランディングゾーンリージョン
- AWS IAM Identity Center
- バージョンステータス
- リージョン拒否コントロール

AWS Control Tower > ランディングゾーン設定

ランディングゾーン設定 情報

ランディングゾーンのバージョンの詳細を表示します。必要に応じて、更新と修復を行います。

詳細	設定を変更する
現在のバージョン 3.2	
KMS キーの暗号化 15	fe 情報
AWS CloudTrail ☑ 有効	
ホームリージョン 米国東部 (バージニア北部) 情報	
ランディングゾーンリージョン 4 管理対象	
AWS IAM Identity Center ☑ 有効	
バージョンステータス ☑ 最新状態	
リージョン拒否コントロール ☑ 有効	
	統制の詳細を表示



ランディングゾーン設定の項目

- 現在のバージョン
- AWS KMS キーの暗号化
- AWS CloudTrail
- ホームリージョン
- ランディングゾーンリージョン
- AWS IAM Identity Center
- バージョンステータス
- リージョン拒否コントロール

AWS Control Tower > ランディングゾーン設定

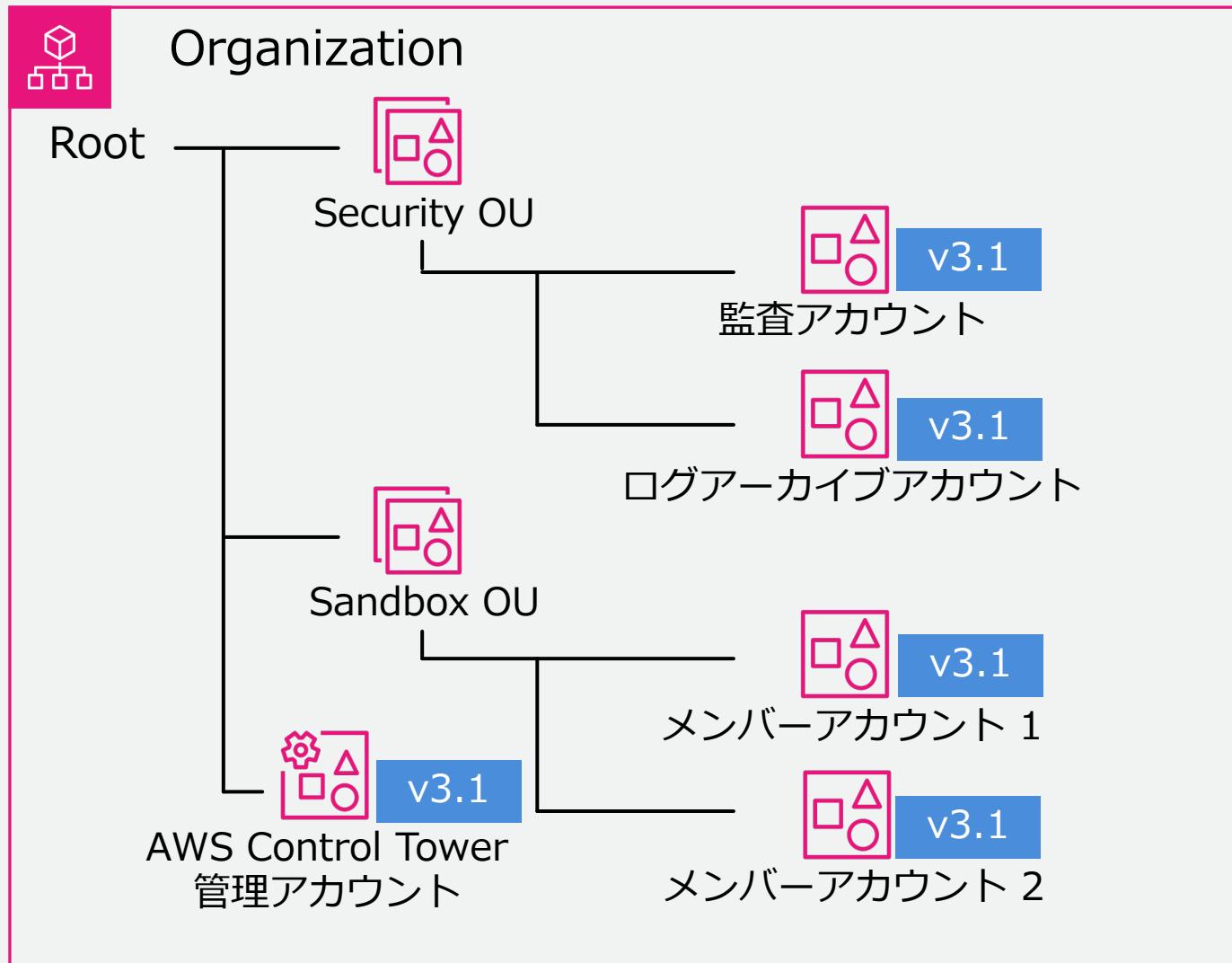
ランディングゾーン設定 情報

ランディングゾーンのバージョンの詳細を表示します。必要に応じて、更新と修復を行います。

詳細	設定を変更する
現在のバージョン 3.2	
KMS キーの暗号化 15	fe 情報
AWS CloudTrail ☑ 有効	
ホームリージョン 米国東部 (バージニア北部) 情報	
ランディングゾーンリージョン 4 管理対象	
AWS IAM Identity Center ☑ 有効	
バージョンステータス ☑ 最新状態	
リージョン拒否コントロール ☑ 有効	
	統制の詳細を表示



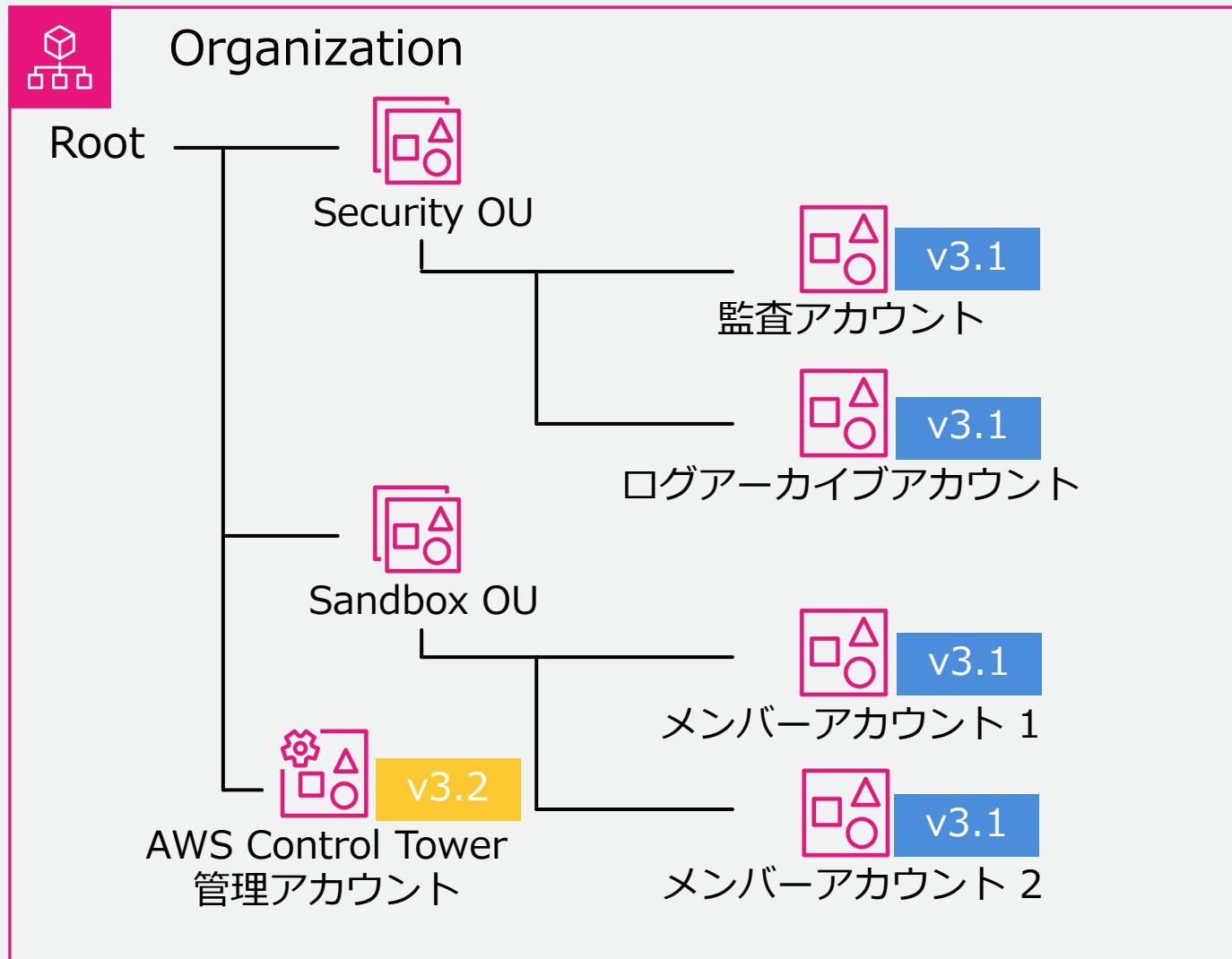
ランディングゾーンバージョン



- ・ランディングゾーンはバージョンがある
 - AWS Control Tower 管理アカウント
 - 各アカウント
- ・新しいバージョンがリリースされた場合には更新を推奨
 - バージョンステータスで状態を把握できる

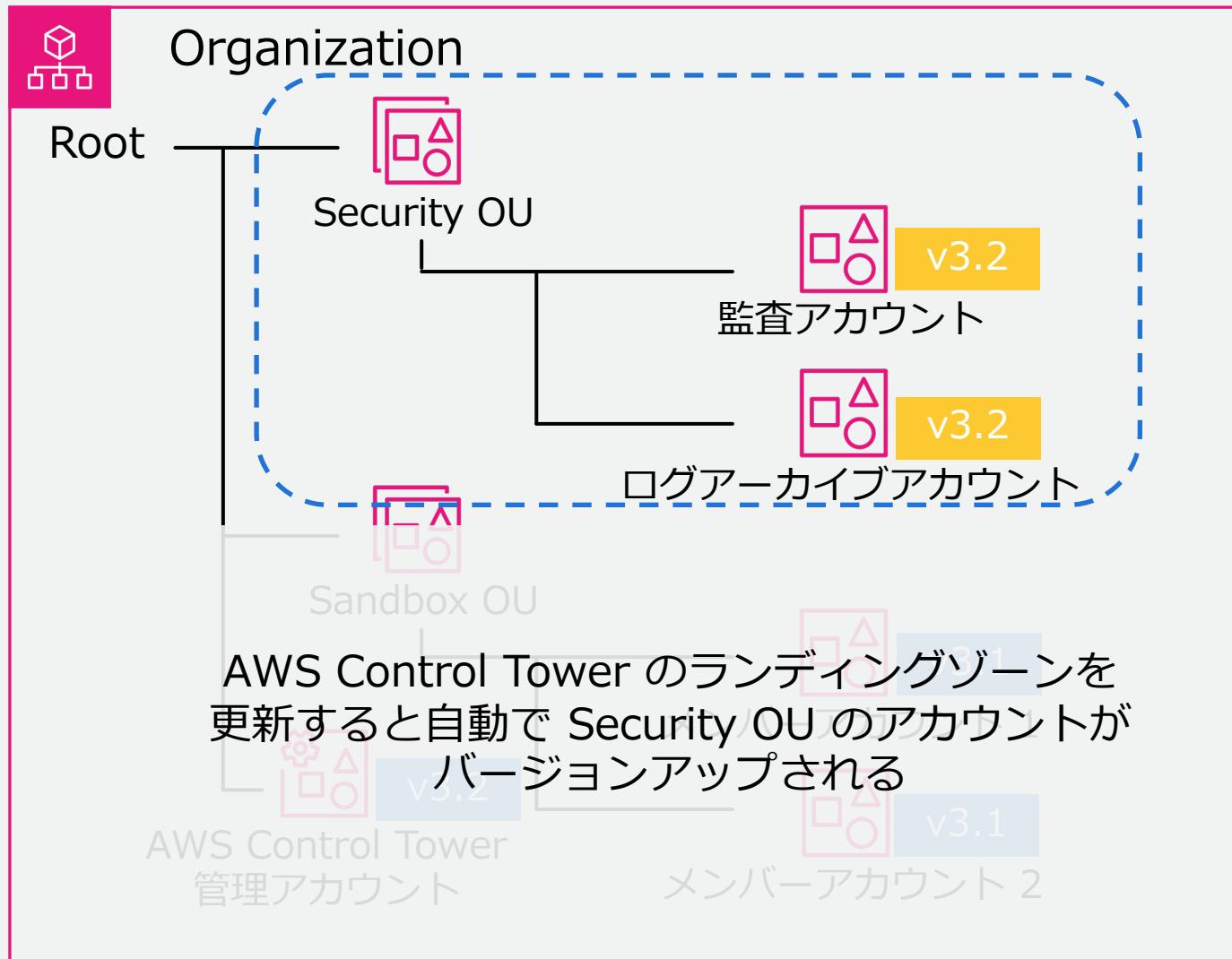
https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/configuration-updates.html

ランディングゾーンバージョン更新



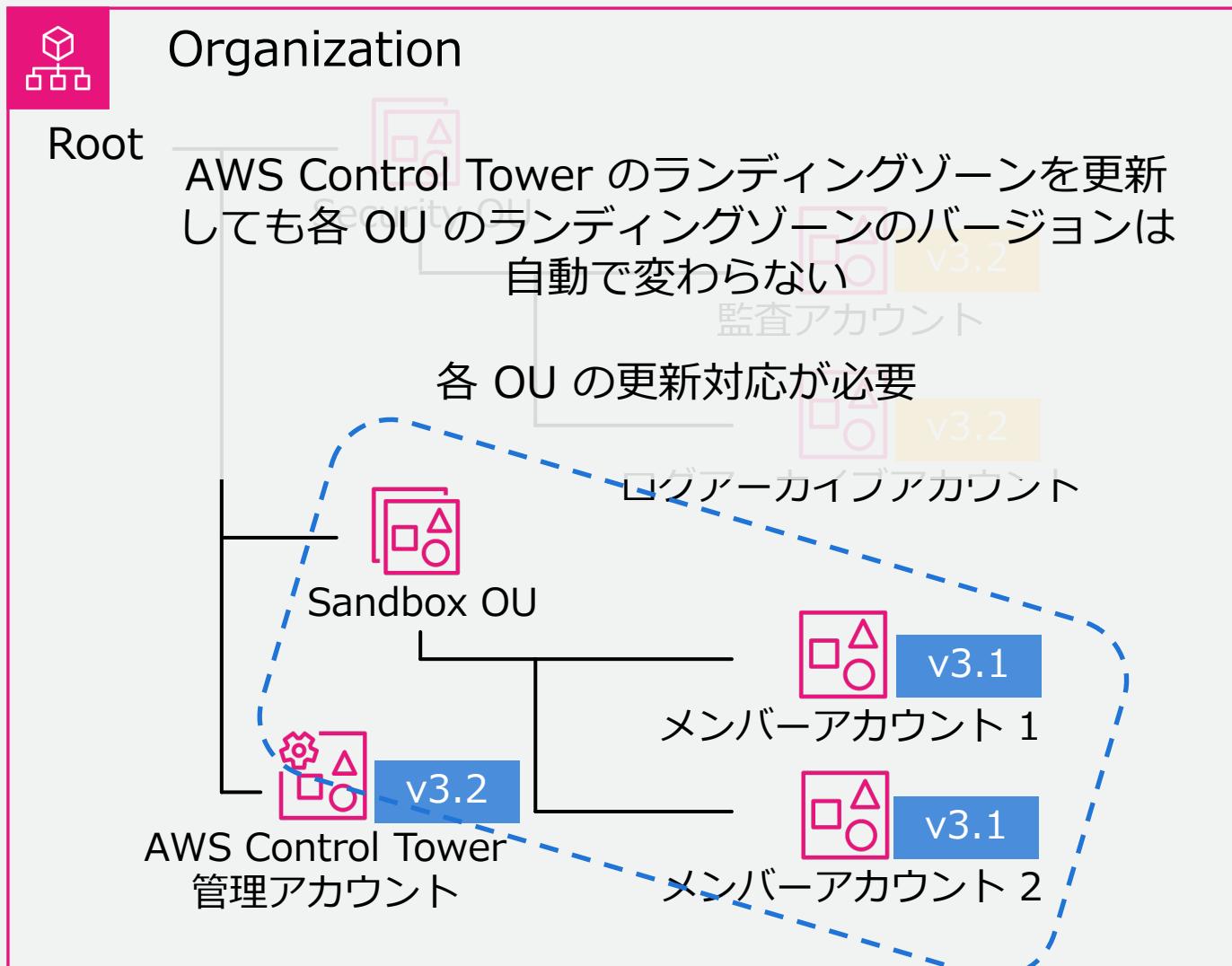
- AWS Control Tower のランディングゾーンを更新後、OU もしくはアカウントのバージョンを更新
- Security OU 配下のアカウントは自動更新

ランディングゾーンバージョン更新



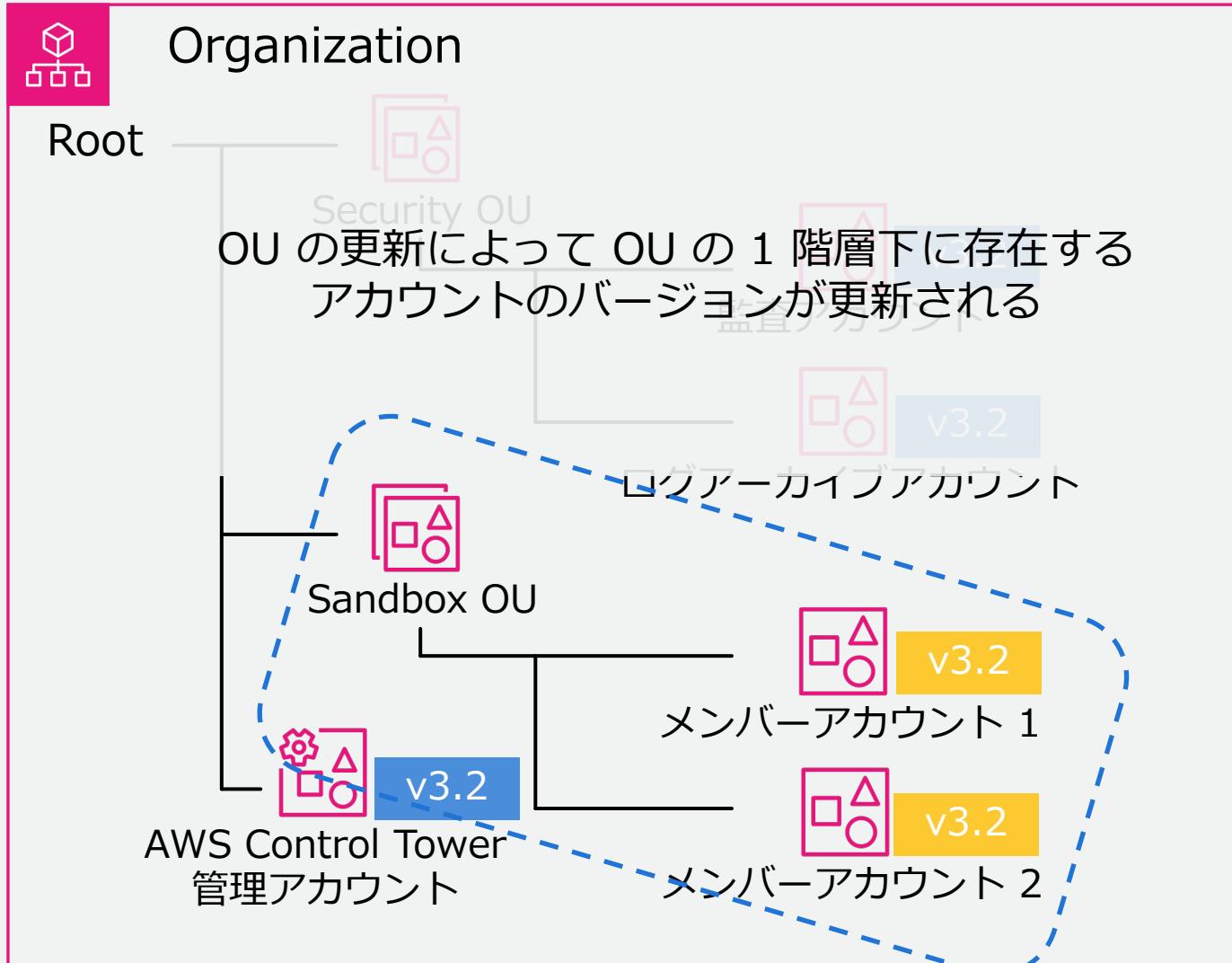
- AWS Control Tower のランディングゾーンを更新後、OU もしくはアカウントのバージョンを更新
- Security OU 配下のアカウントは自動更新

ランディングゾーンバージョン更新



- AWS Control Tower のランディングゾーンを更新後、OU もしくはアカウントのバージョンを更新
- Security OU 配下のアカウントは自動更新

ランディングゾーンバージョン更新



- AWS Control Tower のランディングゾーンを更新後、OU もしくはアカウントのバージョンを更新
- Security OU 配下のアカウントは自動更新

ランディングゾーン設定の項目

- 現在のバージョン
- AWS KMS キーの暗号化
- AWS CloudTrail
- ホームリージョン
- ランディングゾーンリージョン
- AWS IAM Identity Center
- バージョンステータス
- リージョン拒否コントロール

AWS Control Tower > ランディングゾーン設定

ランディングゾーン設定 情報

ランディングゾーンのバージョンの詳細を表示します。必要に応じて、更新と修復を行います。

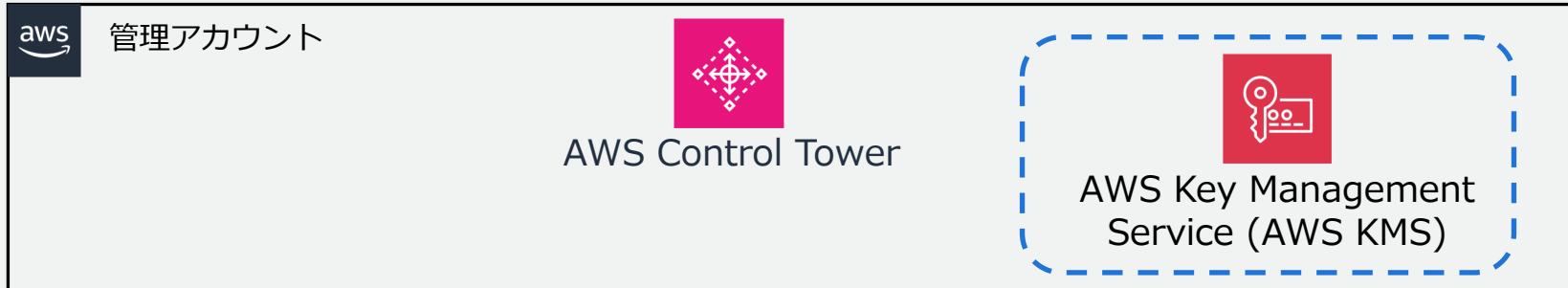
詳細	設定を変更する
現在のバージョン 3.2	
KMS キーの暗号化 15	fe 情報
AWS CloudTrail ☑ 有効	
ホームリージョン 米国東部 (バージニア北部) 情報	
ランディングゾーンリージョン 4 管理対象	
AWS IAM Identity Center ☑ 有効	
バージョンステータス ☑ 最新状態	
リージョン拒否コントロール ☑ 有効	
	統制の詳細を表示



ランディングゾーン AWS KMS キー

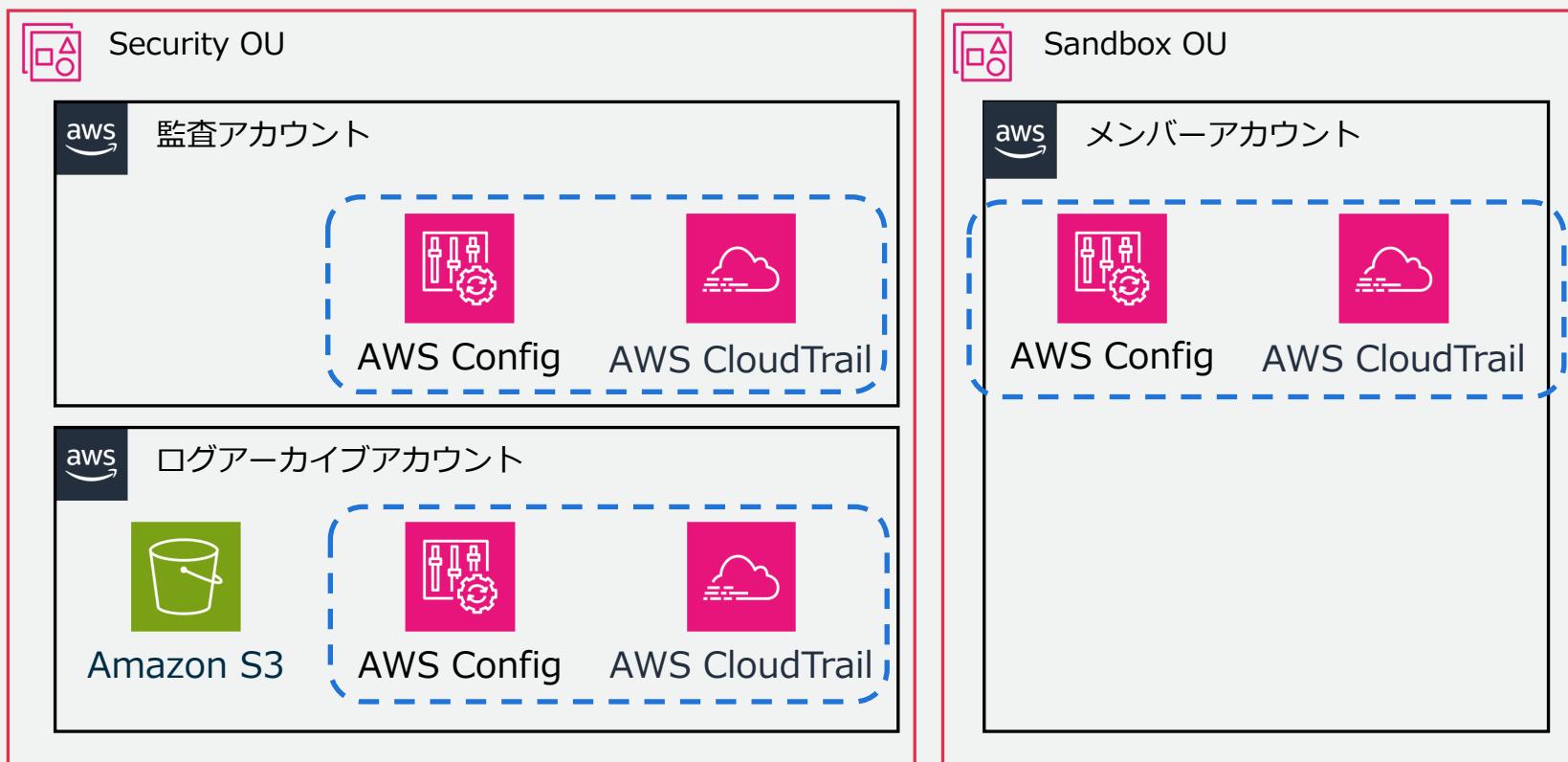
オプション

暗号化設定を有効にして、
カスタマイズする



管理アカウントで
AWS KMS の CMK を作
成しランディングゾーン
で設定する

AWS CloudTrail と
AWS Config に暗号化を
適用してログアーカイブ
アカウントに保存する



ランディングゾーン設定の項目

- 現在のバージョン
- AWS KMS キーの暗号化
- AWS CloudTrail
- ホームリージョン
- ランディングゾーンリージョン
- AWS IAM Identity Center
- バージョンステータス
- リージョン拒否コントロール

AWS Control Tower > ランディングゾーン設定

ランディングゾーン設定 情報

ランディングゾーンのバージョンの詳細を表示します。必要に応じて、更新と修復を行います。

詳細	設定を変更する
現在のバージョン 3.2	
KMS キーの暗号化 15	fe 情報
AWS CloudTrail ☑ 有効	
ホームリージョン 米国東部 (バージニア北部) 情報	
ランディングゾーンリージョン 4 管理対象	
AWS IAM Identity Center ☑ 有効	
バージョンステータス ☑ 最新状態	
リージョン拒否コントロール ☑ 有効	
	統制の詳細を表示

ランディングゾーン AWS CloudTrail

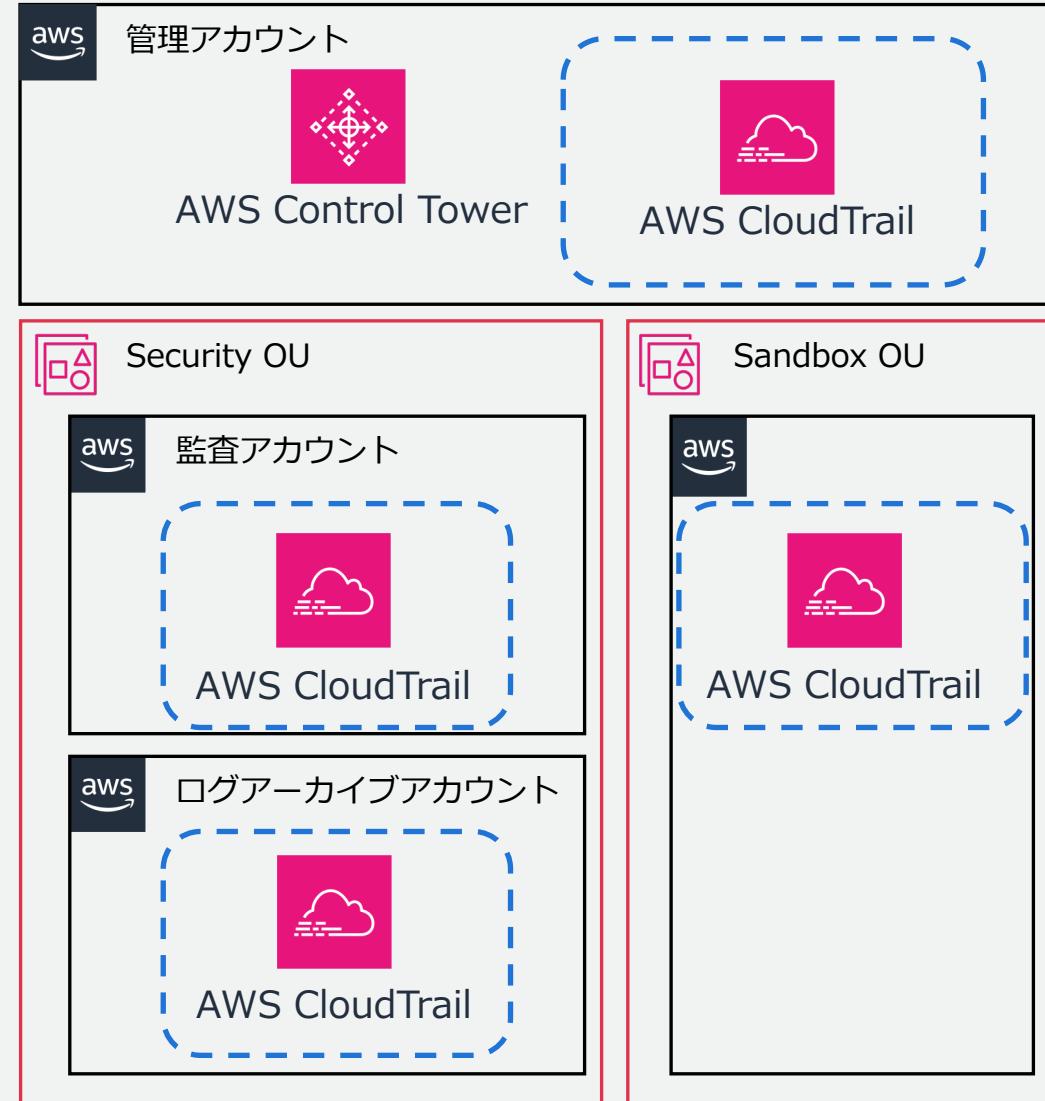
2つの方法から選択

1. AWS CloudTrail の組織証跡を有効化する
2. 有効化しない

1 が推奨

1 は組織証跡が有効化され、ログアーカイブアカウントに保存される

2 は組織証跡が無効なため、別の証跡を作成する必要がある



ランディングゾーン設定の項目

- 現在のバージョン
- AWS KMS キーの暗号化
- AWS CloudTrail
- ホームリージョン
- ランディングゾーンリージョン
- AWS IAM Identity Center
- バージョンステータス
- リージョン拒否コントロール

AWS Control Tower > ランディングゾーン設定

ランディングゾーン設定 情報

ランディングゾーンのバージョンの詳細を表示します。必要に応じて、更新と修復を行います。

詳細	設定を変更する
現在のバージョン 3.2	
KMS キーの暗号化 15	fe 情報
AWS CloudTrail ☑ 有効	
ホームリージョン 米国東部 (バージニア北部) 情報	
ランディングゾーンリージョン 4 管理対象	
AWS IAM Identity Center ☑ 有効	
バージョンステータス ☑ 最新状態	
リージョン拒否コントロール ☑ 有効	
	統制の詳細を表示

ランディングゾーン リージョン

- ホームリージョン

- 1 つのリージョンのみ設定可能
- AWS Control Tower を有効化するリージョン
- AWS IAM Identity Center や AWS Organizations を利用するリージョン

- ランディングゾーンリージョン

- AWS Control Tower の管理対象でランディングゾーンを設定するリージョン
- AWS Control Tower によって AWS リソースが生成される
- 追加することも削除することも可能

ランディングゾーン設定の項目

- 現在のバージョン
- AWS KMS キーの暗号化
- AWS CloudTrail
- ホームリージョン
- ランディングゾーンリージョン
- AWS IAM Identity Center
- バージョンステータス
- リージョン拒否コントロール

AWS Control Tower > ランディングゾーン設定

ランディングゾーン設定 情報

ランディングゾーンのバージョンの詳細を表示します。必要に応じて、更新と修復を行います。

詳細	設定を変更する
現在のバージョン 3.2	
KMS キーの暗号化 15	fe 情報
AWS CloudTrail ☑ 有効	
ホームリージョン 米国東部 (バージニア北部) 情報	
ランディングゾーンリージョン 4 管理対象	
AWS IAM Identity Center ☑ 有効	
バージョンステータス ☑ 最新状態	
リージョン拒否コントロール ☑ 有効	
	統制の詳細を表示

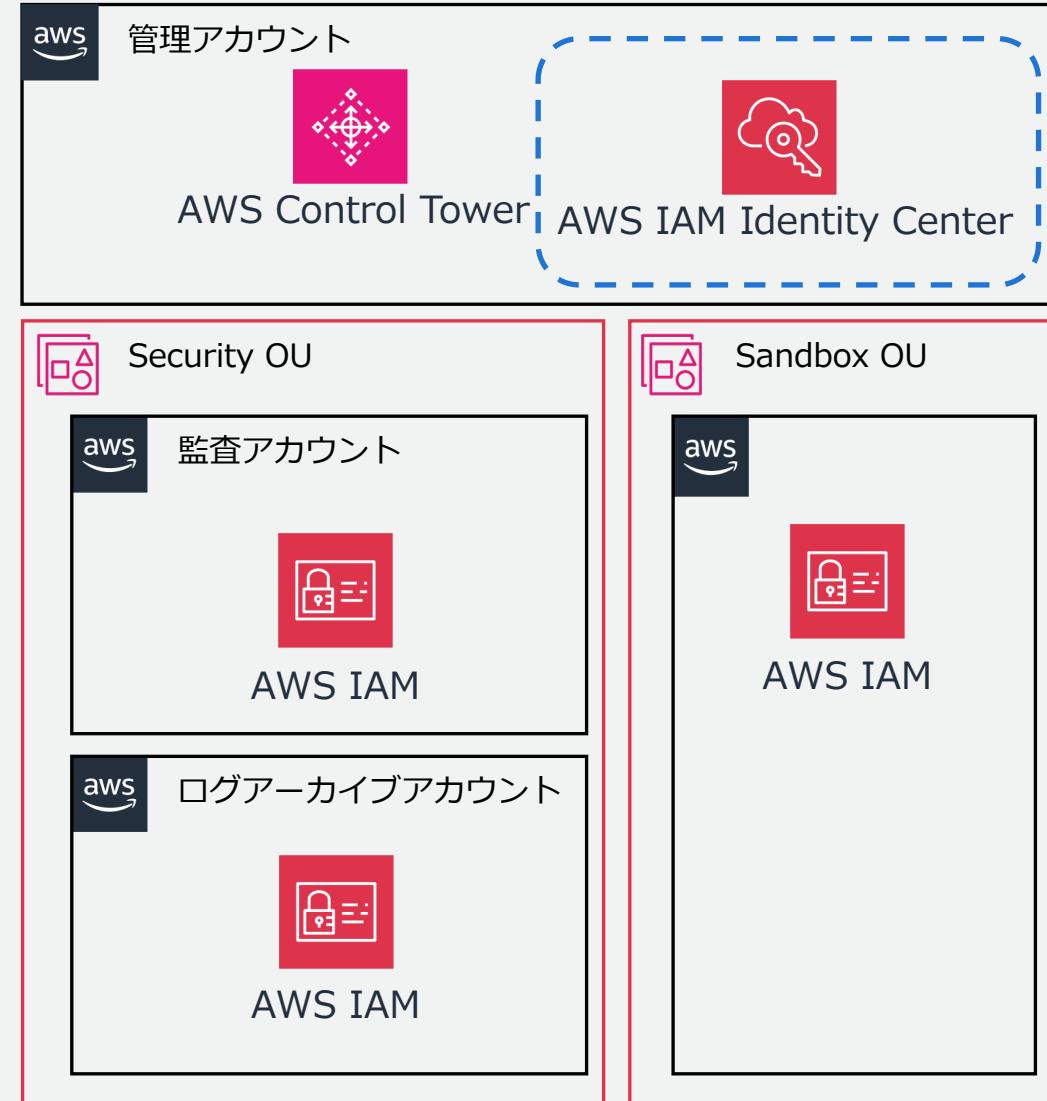


ランディングゾーン AWS IAM Identity Center

2つの方法から選択

1. AWS Control Tower は AWS IAM Identity Center を使用して AWS アカウントアクセスを設定します
2. AWS IAM Identity Center または その他の方法によるセルフマネージド型 AWS アカウントアクセス

- 1 は AWS IAM Identity Center のグループと権限セットが作成される
- 2 は何も作成されない



ランディングゾーン設定の項目

- 現在のバージョン
- AWS KMS キーの暗号化
- AWS CloudTrail
- ホームリージョン
- ランディングゾーンリージョン
- AWS IAM Identity Center
- バージョンステータス
- リージョン拒否コントロール

AWS Control Tower > ランディングゾーン設定

ランディングゾーン設定 情報

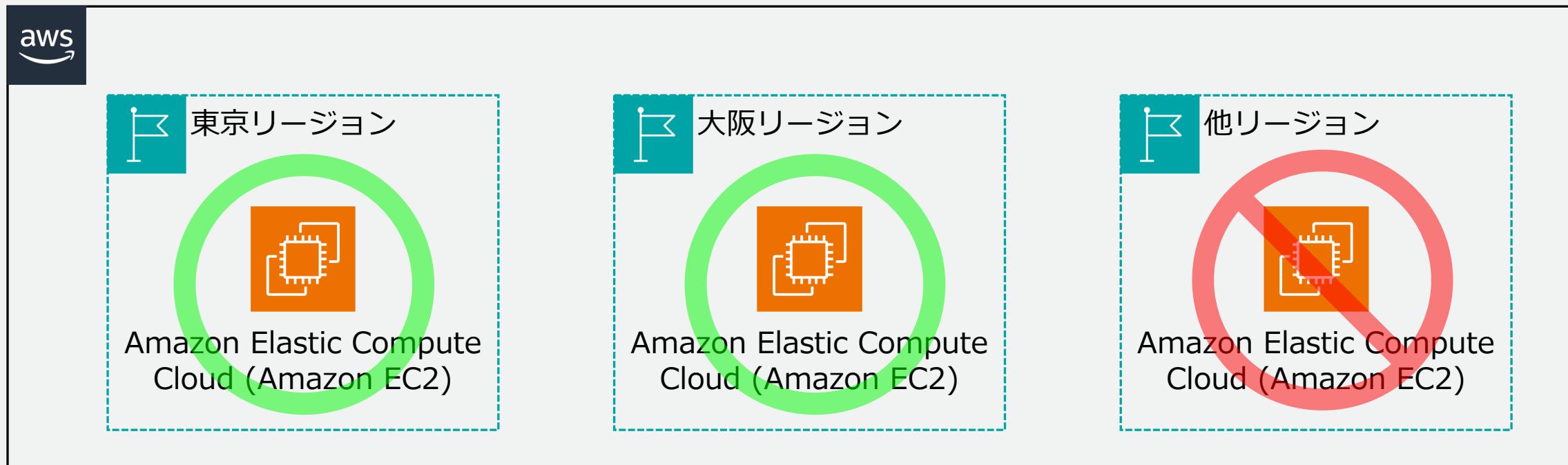
ランディングゾーンのバージョンの詳細を表示します。必要に応じて、更新と修復を行います。

詳細	設定を変更する
現在のバージョン 3.2	
KMS キーの暗号化 15	fe 情報
AWS CloudTrail ☑ 有効	
ホームリージョン 米国東部 (バージニア北部) 情報	
ランディングゾーンリージョン 4 管理対象	
AWS IAM Identity Center ☑ 有効	
バージョンステータス ☑ 最新状態	
リージョン拒否コントロール ☑ 有効	
	統制の詳細を表示



ランディングゾーン リージョン拒否コントロール

- AWS Control Tower のランディングゾーンリージョンに含まれないリージョンの利用を禁止
 - AWS Control Tower で登録されている OU に対して SCP を適用



https://docs.aws.amazon.com/ja_jp/controlltower/latest/userguide/data-residency-controls.html

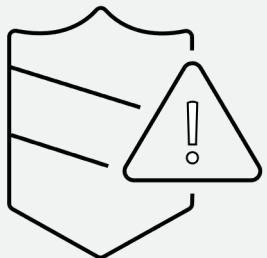
コントロール

コントロール

様々な項目による包括的なガイダンス

サービス	名前	統制目標	動作	フレームワーク	ガイダンス
AWS CloudFormation	[CT.CLOUDFORMATION.PR.1] AWS CloudFormation レジストリ内のリソースタイプ、モジュール、フックの管理を禁止する	設定を保護	予防	NIST 800-53 Rev 5 PCI DSS version 3.2.1	選択的
AWS Identity and Access Management (IAM)	[AWS-GR_ROOT_ACCOUNT_MFA_ENABLE] ルートユーザーの MFA が有効になっているかどうかを検出する	最小特権を強制	検出	CIS AWS Benchmark 1.4 NIST 800-53 Rev 5 PCI DSS version 3.2.1	強く推奨
Amazon S3	[AWS-GR_AUDIT_BUCKET_DELETION_PROHIBITED] ログアーカイブの削除を許可しない	データの完全性を保護	予防	NIST 800-53 Rev 5 PCI DSS version 3.2.1	必須
AWS Lambda	[CT.LAMBDA.PR.3] AWS Lambda 関数がカスタマーマネージド Amazon Virtual Private Cloud (VPC) に配置されていることを要求する	ネットワークアクセスを制限	プロアクティブ	NIST 800-53 Rev 5 PCI DSS version 3.2.1	選択的
Amazon Kinesis	[SH.Kinesis.1] Kinesis ストリームは保存時に暗号化する必要があります	保管中のデータを暗号化	検出	NIST 800-53 Rev 5 PCI DSS version 3.2.1	選択的

コントロールのタイプ



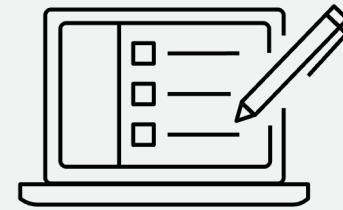
予防

サービスコントロール
ポリシー (SCP)



検出

AWS Config ルール



プロアクティブ

AWS CloudFormation
Hooks

予防コントロール

- AWS Organizations の SCP を利用したコントロール
 - ポリシー違反につながるアクションを禁止するため、アカウントはコンプライアンスを維持できる
 - すべての AWS リージョンで適用される

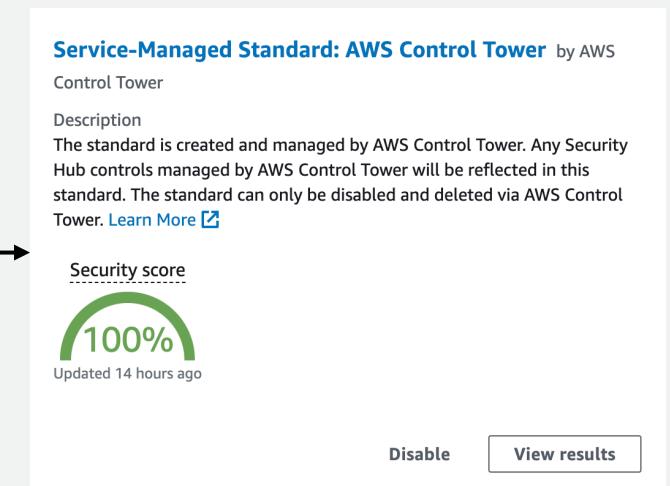
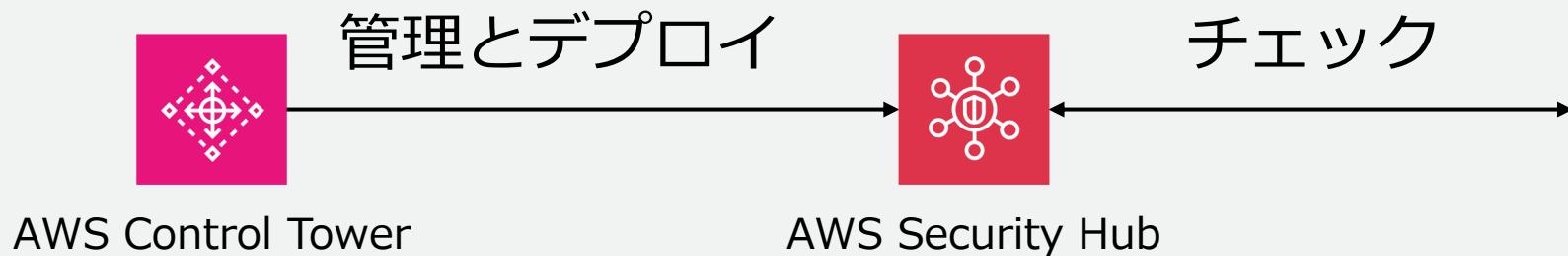
予防コントロールで
ルートユーザーとしてのアクションを許可しない場合



検出コントロール

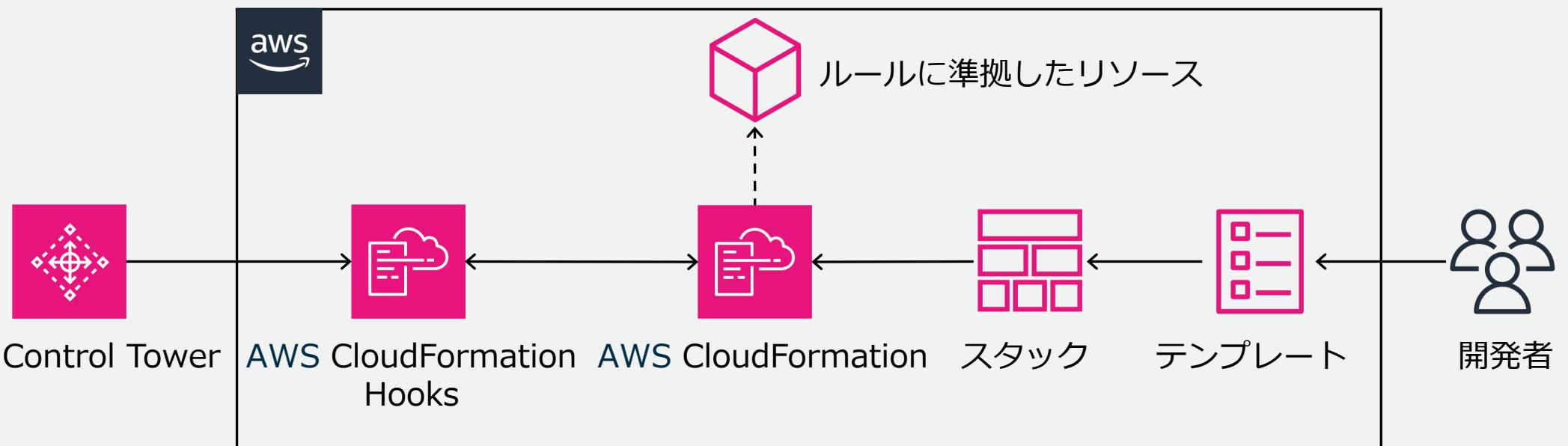
- AWS Config を利用したコントロール
 - AWS Control Tower 管理下のアカウント内リソースの準拠状態を検出し、非準拠の場合はダッシュボードを通じてアラートを提供する
 - AWS Control Tower ランディングゾーンリージョンに適用される
 - コントロールオーナーは AWS Control Tower と AWS Security Hub の 2 種類

コントロールオーナーが AWS Security Hub の
検出コントロールを有効化した場合

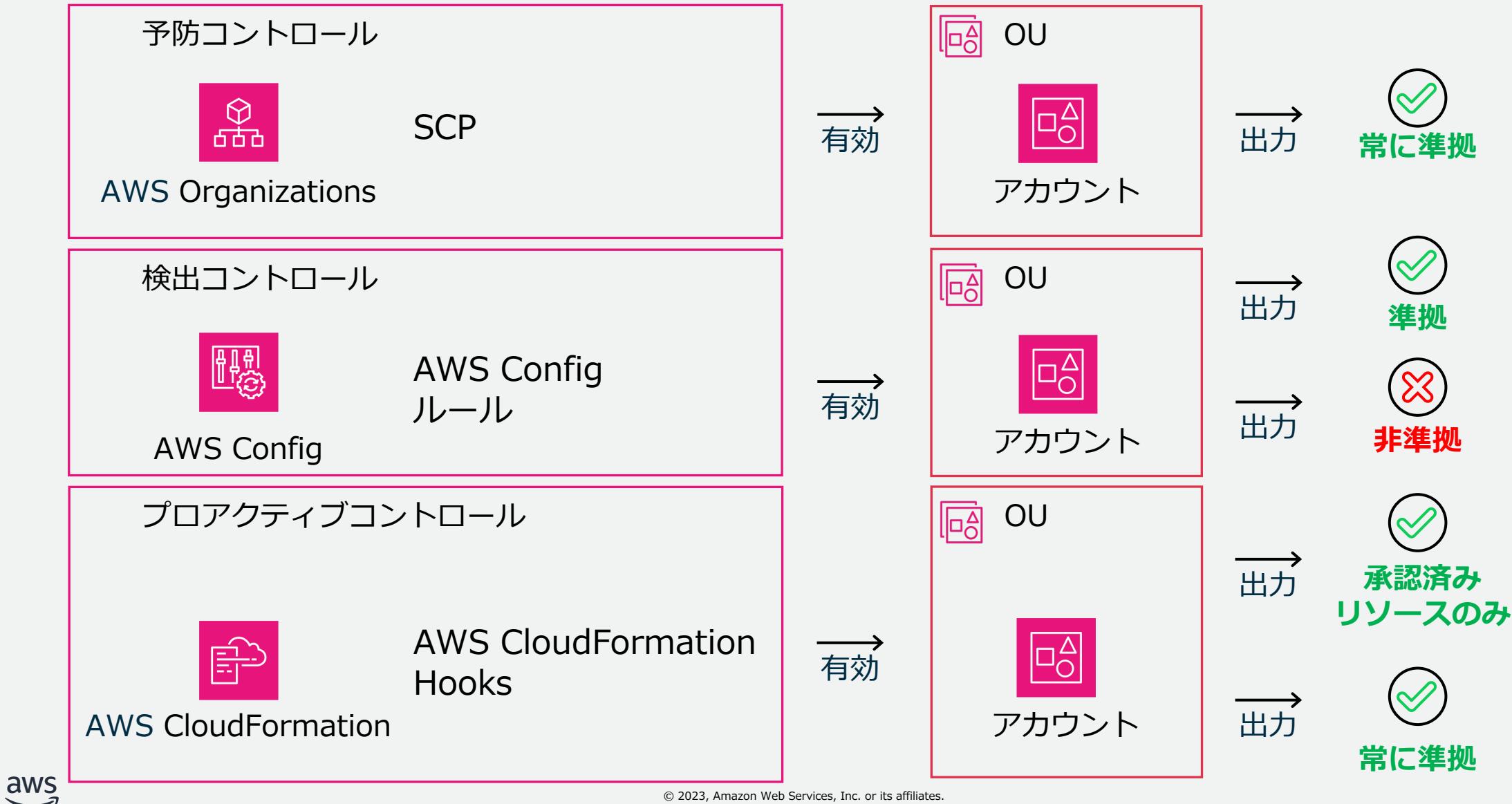


プロアクティブコントロール

- AWS CloudFormation Hooks を利用したコントロール
 - プロビジョニング前にリソースをスキャンし準拠状態を確認し、非準拠の場合はリソースがプロビジョニングされない
 - AWS CloudFormation でプロビジョニングするリソースに適用される



コントロールの制御動作



コントロール

様々な項目による包括的なガイダンス

サービス	名前	統制目標	動作	フレームワーク	ガイダンス
AWS CloudFormation	[CT.CLOUDFORMATION.PR.1] AWS CloudFormation レジストリ内のリソースタイプ、モジュール、フックの管理を禁止する	設定を保護	予防	NIST 800-53 Rev 5 PCI DSS version 3.2.1	選択的
AWS Identity and Access Management (IAM)	[AWS-GR_ROOT_ACCOUNT_MFA_ENABLE] ルートユーザーの MFA が有効になっているかどうかを検出する	最小特権を強制	検出	CIS AWS Benchmark 1.4 NIST 800-53 Rev 5 PCI DSS version 3.2.1	強く推奨
Amazon S3	[AWS-GR_AUDIT_BUCKET_DELETION_PROHIBITED] ログアーカイブの削除を許可しない	データの完全性を保護	予防	NIST 800-53 Rev 5 PCI DSS version 3.2.1	必須
AWS Lambda	[CT.LAMBDA.PR.3] AWS Lambda 関数がカスタマーマネージド Amazon Virtual Private Cloud (VPC) に配置されていることを要求する	ネットワークアクセスを制限	プロアクティブ	NIST 800-53 Rev 5 PCI DSS version 3.2.1	選択的
Amazon Kinesis	[SH.Kinesis.1] Kinesis ストリームは保存時に暗号化する必要があります	保管中のデータを暗号化	検出	NIST 800-53 Rev 5 PCI DSS version 3.2.1	選択的

コントロールのガイダンス



必須



強く推奨



選択的

必須コントロール



必須

- AWS Control Tower のランディングゾーンを保護するための設定
- お客様のワークフローに影響を与えるものではない

必須コントロール一覧

名前	動作
AWS Control Tower がログアーカイブに作成した Amazon S3 バケットの暗号化設定の変更を許可しない	予防
AWS Control Tower がログアーカイブに作成した Amazon S3 バケットのログ設定の変更を許可しない	予防
AWS Control Tower がログアーカイブに作成した Amazon S3 バケットのバケットポリシーの変更を許可しない	予防
AWS Control Tower がログアーカイブに作成した Amazon S3 バケットのライフサイクル設定の変更を許可しない	予防
AWS Control Tower によって設定された Amazon CloudWatch Logs ロググループへの変更を不許可にする	予防
ログアーカイブの削除を禁止する	予防
ログアーカイブのパブリック読み取りアクセス設定を検出する	検出
ログアーカイブのパブリック書き込みアクセス設定を検出する	検出
CloudTrail への設定変更を不許可にする	予防
AWS Config への設定変更を許可しない	予防
AWS Control Tower によって設定された AWS Config ルールへの変更を許可しない	予防
AWS Control Tower が作成した AWS Config 集約認証の削除を許可しない	予防
AWS Control Tower が作成した リソースのタグの変更を許可しない	予防
AWS Control Tower によって設定された Amazon CloudWatch への変更を不許可にする	予防
AWS Control Tower と AWS CloudFormation によって設定された AWS IAM ロールへの変更を不許可にする	予防
AWS Control Tower によって設定された AWS Lambda 関数の変更を許可しない	予防
AWS Control Tower によって設定された Amazon SNS への変更を不許可にする	予防
AWS Control Tower によって設定された Amazon SNS サブスクリプションへの変更を不許可にする	予防
セキュリティ組織単位の共有アカウントで AWS CloudTrail または CloudTrail Lake が有効になっているかどうかを検出する	検出

必須コントロール一覧

名前		動作
AWS Control Tower がログアーカイブに作成した Amazon S3 バケットの暗号化設定の変更を許可しない		予防
AWS Control Tower がログアーカイブに作成した Amazon S3 バケットのログ設定の変更を許可しない		予防
AWS Control Tower がログアーカイブに作成した Amazon S3 バケットのバケットポリシーの変更を許可しない		予防
AWS Control Tower がログアーカイブに作成した Amazon S3 バケットのライフサイクル設定の変更を許可しない		予防
AWS Control Tower によって設定された Amazon CloudWatch Logs ロググループへの変更を不許可にする		予防
ログアーカイブの削除を禁止する	aws-controltower* が対象	予防
ログアーカイブのパブリック読み取りアクセス設定を検出する	検出コントロール	検出
ログアーカイブのパブリック書き込みアクセス設定を検出する	検出コントロール	検出
CloudTrail への設定変更を不許可にする	aws-controltower-* が対象	予防
AWS Config への設定変更を許可しない	設定レコーダーは各リージョンに1つだけ	予防
AWS Control Tower によって設定された AWS Config ルールへの変更を許可しない		予防
AWS Control Tower が作成した AWS Config 集約認証の削除を許可しない		予防
AWS Control Tower が作成した リソースのタグの変更を許可しない		予防
AWS Control Tower によって設定された Amazon CloudWatch への変更を不許可にする		予防
AWS Control Tower と AWS CloudFormation によって設定された AWS IAM ロールへの変更を不許可にする		予防
AWS Control Tower によって設定された AWS Lambda 関数の変更を許可しない		予防
AWS Control Tower によって設定された Amazon SNS への変更を不許可にする		予防
AWS Control Tower によって設定された Amazon SNS サブスク 検出コントロール		予防
セキュリティ組織単位の共有アカウントで AWS CloudTrail または CloudTrail Lake が有効になっているかどうかを検出する		検出



コントロール

様々な項目による包括的なガイダンス

サービス	名前	統制目標	動作	フレームワーク	ガイダンス
AWS CloudFormation	[CT.CLOUDFORMATION.PR.1] AWS CloudFormation レジストリ内のリソースタイプ、モジュール、フックの管理を禁止する	設定を保護	予防	NIST 800-53 Rev 5 PCI DSS version 3.2.1	選択的
AWS Identity and Access Management (IAM)	[AWS-GR_ROOT_ACCOUNT_MFA_ENABLE] ルートユーザーの MFA が有効になっているかどうかを検出する	最小特権を強制	検出	CIS AWS Benchmark 1.4 NIST 800-53 Rev 5 PCI DSS version 3.2.1	強く推奨
Amazon S3	[AWS-GR_AUDIT_BUCKET_DELETION_PROHIBITED] ログアーカイブの削除を許可しない	データの完全性を保護	予防	NIST 800-53 Rev 5 PCI DSS version 3.2.1	必須
AWS Lambda	[CT.LAMBDA.PR.3] AWS Lambda 関数がカスタマーマネージド Amazon Virtual Private Cloud (VPC) に配置されていることを要求する	ネットワークアクセスを制限	プロアクティブ	NIST 800-53 Rev 5 PCI DSS version 3.2.1	選択的
Amazon Kinesis	[SH.Kinesis.1] Kinesis ストリームは保存時に暗号化する必要があります	保管中のデータを暗号化	検出	NIST 800-53 Rev 5 PCI DSS version 3.2.1	選択的

コントロールのカテゴリー

統制目標、サービス、フレームワークのカテゴリーを利用して適切なコントロールの検討を簡略化

[AWS Control Tower](#) > [コントロールライブラリ: カテゴリ](#) > 統制目標

カテゴリー

カテゴリーは、環境についてのコンプライアンスを達成するのに役立つ AWS マネージドコントロールのグループです。コントロールは、コントロールの目標、AWS のサービス、フレームワークごとにグループ化されます。

[統制目標](#) | [サービス](#) | [フレームワーク](#)

統制目標 (14) 情報	
<input type="text"/> 統制目標を見つける	
統制目標	
<input type="radio"/>	ログ記録とモニタリングを確立
<input type="radio"/>	保管中のデータを暗号化
<input type="radio"/>	強力な認証を使用
<input type="radio"/>	転送中のデータを暗号化
<input type="radio"/>	設定を保護
<input type="radio"/>	脆弱性を管理



[AWS Control Tower](#) > [コントロールライブラリ: カテゴリ](#) > サービス

カテゴリー

カテゴリーは、環境についてのコンプライアンスを達成するのに役立つ AWS マネージドコントロールのグループです。コントロールは、コントロールの目標、AWS のサービス、フレームワークごとにグループ化されます。

[統制目標](#) | [サービス](#) | [フレームワーク](#)

サービス (45) 情報	
<input type="text"/> サービスを探す	
サービス	▼

- [Amazon API Gateway](#)
- [Amazon CloudFront](#)
- [Amazon CloudWatch](#)
- [Amazon DocumentDB](#)
- [Amazon DynamoDB](#)
- [Amazon EC2](#)
- [Amazon EC2 Auto Scaling](#)

[AWS Control Tower](#) > [コントロールライブラリ: カテゴリ](#) > フレームワーク

カテゴリー

カテゴリーは、環境についてのコンプライアンスを達成するのに役立つ AWS マネージドコントロールのグループです。コントロールは、コントロールの目標、AWS のサービス、フレームワークごとにグループ化されます。

[統制目標](#) | [サービス](#) | [フレームワーク](#)

フレームワーク (3) 情報			
<input type="button"/> 詳細を表示			
フレームワーク	▼	統制目標	▼
<input type="radio"/> NIST 800-53 Rev 5	14	410	▼
<input type="radio"/> PCI DSS version 3.2.1	14	354	▼
<input type="radio"/> CIS AWS Benchmark 1.4	9	58	▼

コントロールの画面

- 統制目標
- サービス
- 動作
- フレームワーク
- ガイダンス
- 関係

適用するコントロールに
依存関係がある場合は事前に適用する

AWS Control Tower > コントロールライブラリ: すべてのコントロール > [CT.S3.PR.2] Amazon S3 バケットにサーバーアクセスロギングの設定をする必要がある

[CT.S3.PR.2] Amazon S3 バケットにサーバーアクセスロギングの設定をする必要がある

The screenshot shows the AWS Control Tower Control Library interface. A specific control, [CT.S3.PR.2] Amazon S3 バケットにサーバーアクセスロギングの設定をする必要がある, is selected. The details page displays the following information:

詳細	情報	コントロール ID
名前	Amazon S3 バケットにサーバーアクセスロギングの設定をする必要がある	CT.S3.PR.2
統制目標	Establish logging and monitoring	ガイダンス 選択的
サービス	Amazon S3	重大度 中
コントロールオーナー	AWS Control Tower	リリース日 2022年11月28日
API コントロール識別子	arn:aws:controltower:ap-northeast-1::control/EEJURBQMFYKX	
動作	プロアクティブ 情報	
実装	CloudFormation guard rule 情報	
リソース	AWS::S3::Bucket	
フレームワーク	CIS AWS Benchmark 1.4 IDs ; NIST 800-53 Rev 5 IDs ; PCI DSS version 3.2.1 IDs	

説明
このコントロールは、Amazon S3 バケットのサーバーアクセスロギングが有効になっているかどうかを確認します。ドキュメンテーションの詳細 [Logging requests using server access logging](#).

コントロールの関係 [情報](#)

⚠ このコントロールは 1 つ以上のコントロールと依存関係にあります。統制目標を達成するには、OU の依存統制との統制を有効にする必要があります。

[CT.CLOUDFORMATION.PR.1] AWS CloudFormation レジストリ内のリソースタイプ、モジュール、フックの管理を禁止する

- このコントロールでは、AWS CloudFormation レジストリ内の次の拡張タイプ(リソースタイプ、モジュール、フック)の管理が禁止されます。

ⓘ このコントロールは、関連するコントロールと連携できます。セキュリティを強化するには、関連する統制を評価し、環境に適用できる統制を有効にしてください。

[SH.S3.9] S3 バケットサーバーアクセスロギングを有効にする必要があります

- このコントロールは、Amazon S3 バケットで、選択したターゲットバケットへのサーバーアクセスロギングが有効になっているかどうかを確認します。

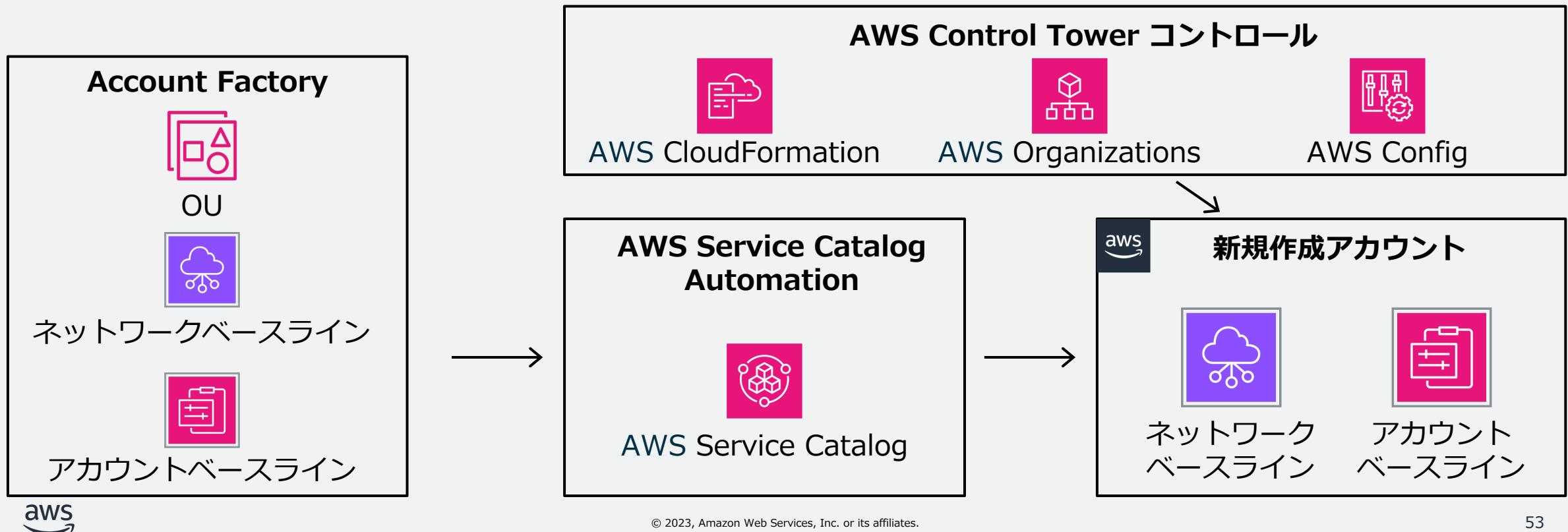
Account Factory



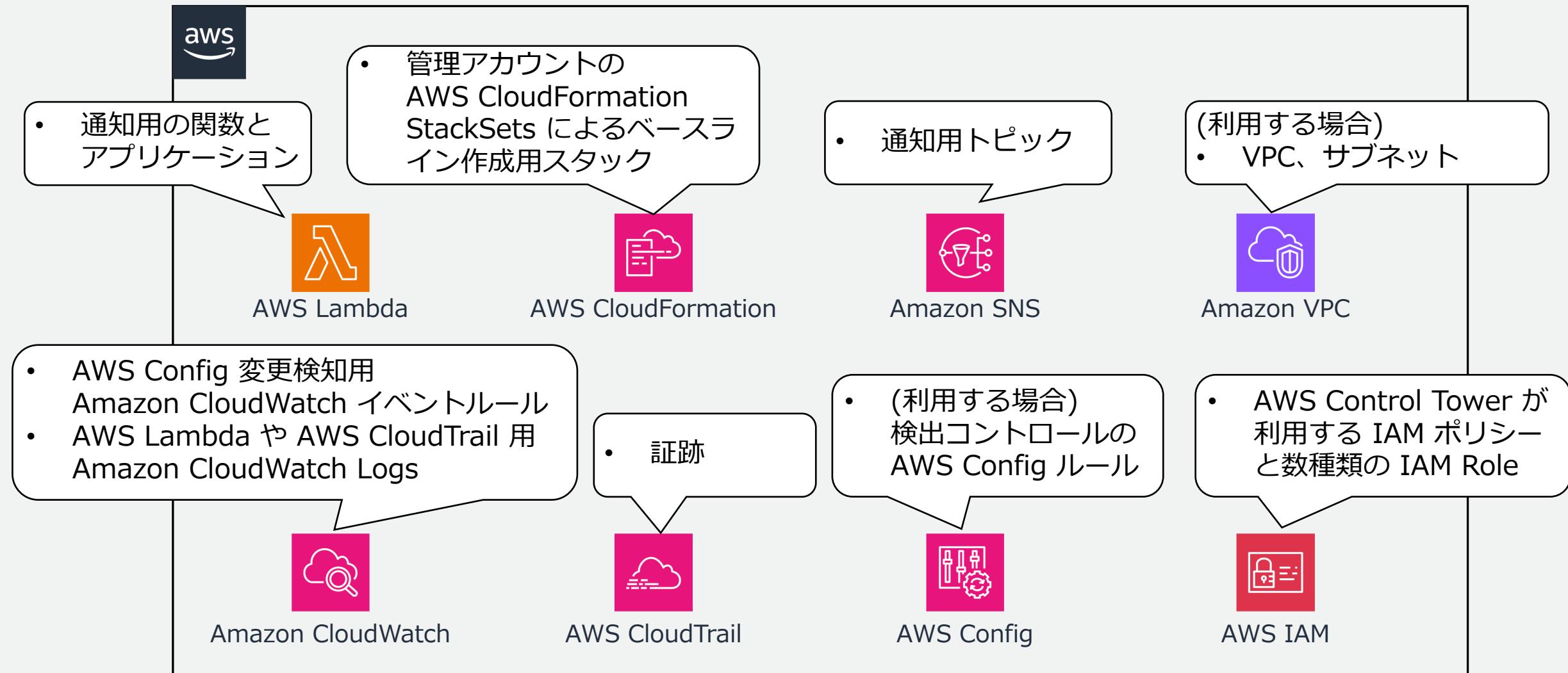
Account Factory

AWS Control Tower のガバナンスの効いた AWS アカウントを作成するための機能

AWS Service Catalog を活用し、Amazon VPC やコントロールが設定されたアカウントをプロビジョニングする



メンバーアカウントで作成される AWS リソース

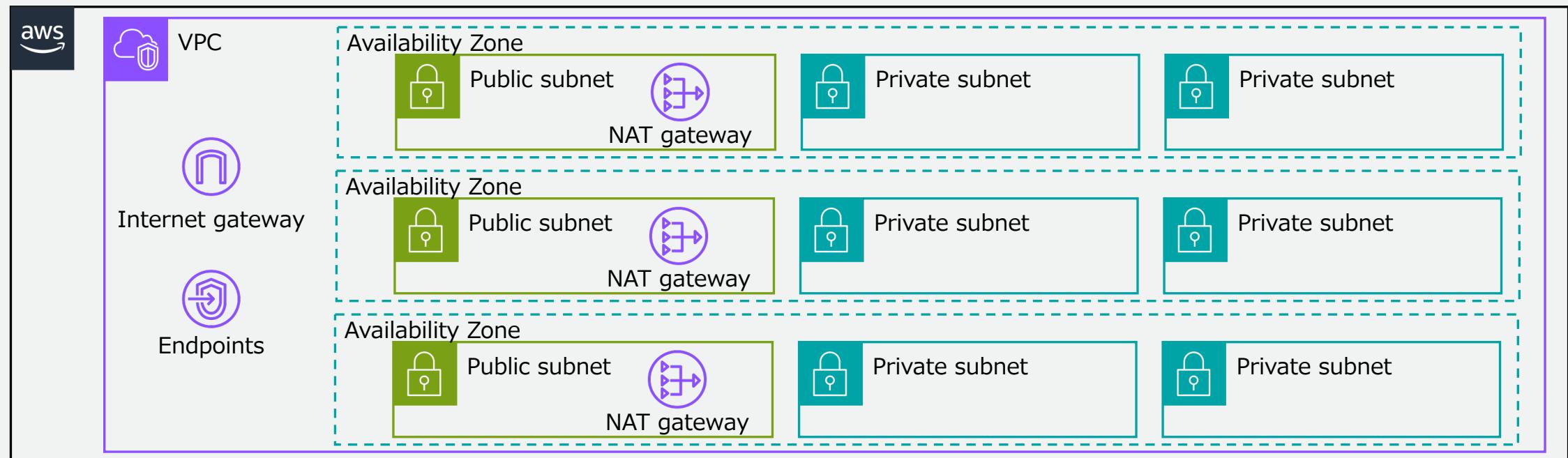


https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/account-factory-considerations.html

VPC 設定により作成されるリソース

インターネットアクセス可能なサブネット、プライベートサブネットの最大数、CIDR、VPC 作成のリージョンを設定することで新しい VPC が作成される

インターネットアクセス可能なサブネット許可、プライベートサブネットの最大数 2 の場合



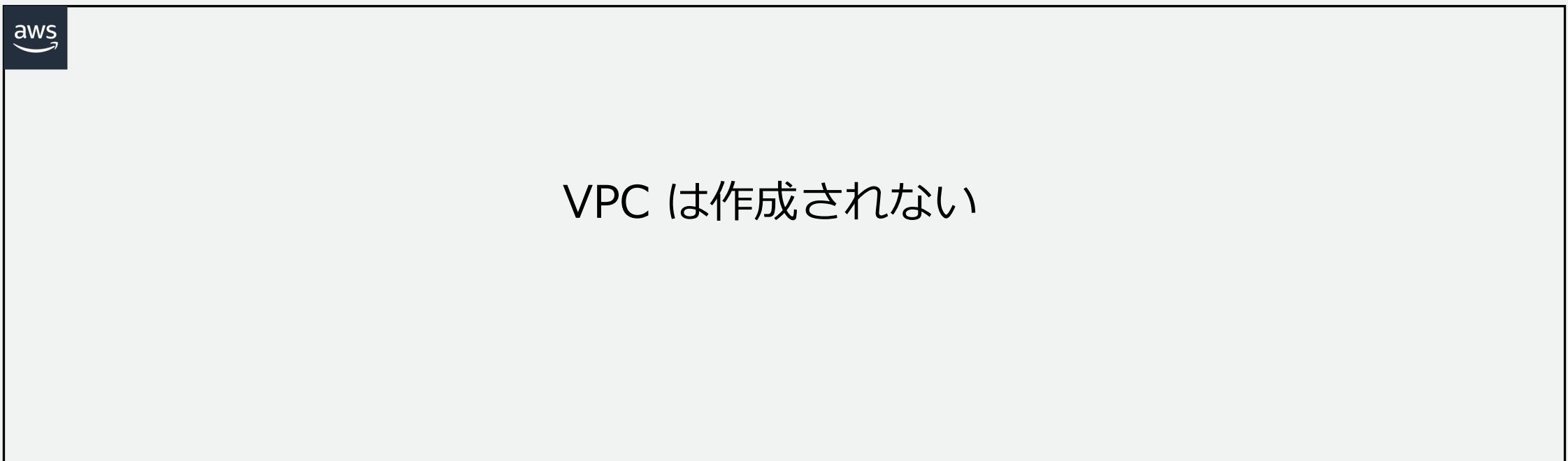
https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/vpc-concepts.html

© 2023, Amazon Web Services, Inc. or its affiliates.

VPC 設定により作成されるリソース 続き

インターネットアクセス可能なサブネット、プライベートサブネットの最大数、CIDR、VPC 作成のリージョンを設定することで新しい VPC が作成される

インターネットアクセス可能なサブネット不許可、プライベートサブネットの最大数 0 の場合



https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/vpc-concepts.html

© 2023, Amazon Web Services, Inc. or its affiliates.

AWS Control Tower で作成するアカウントのカスタマイズ

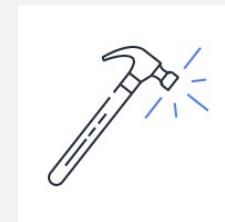
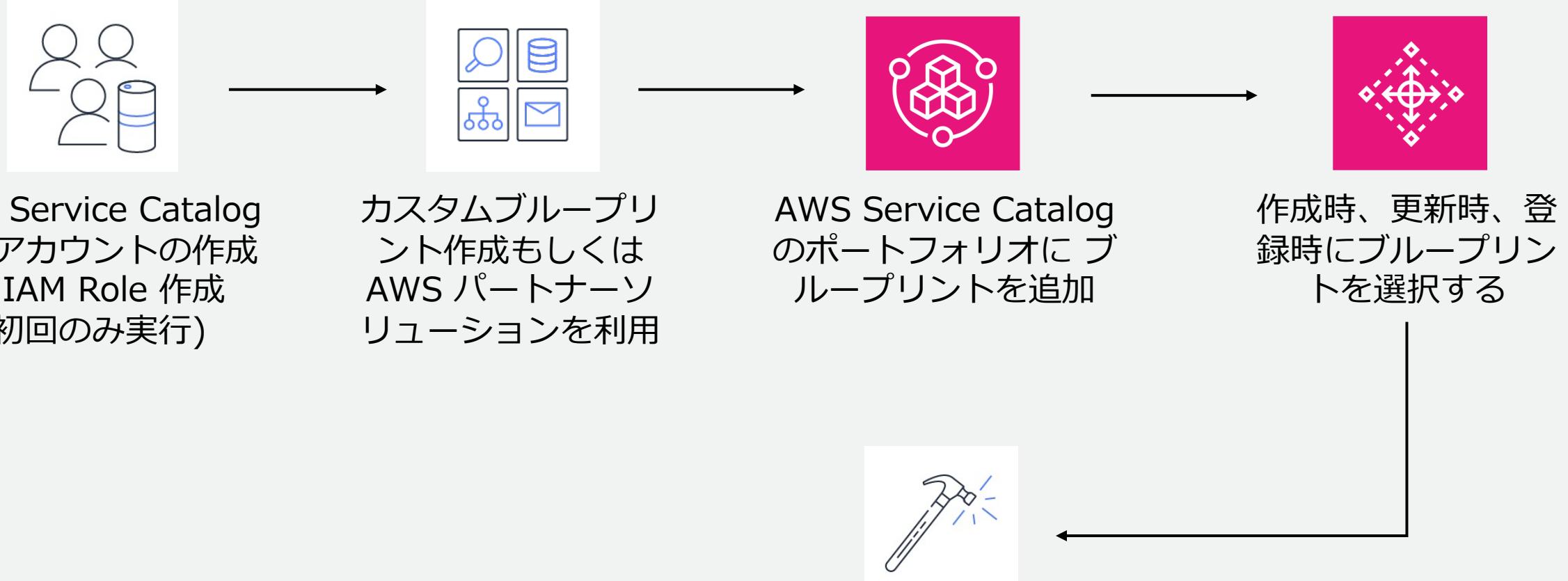
AWS サービス活用

- Account Factory Customization (AFC)
- AWS CloudFormation StackSets (Organizations)

AWS ソリューション活用

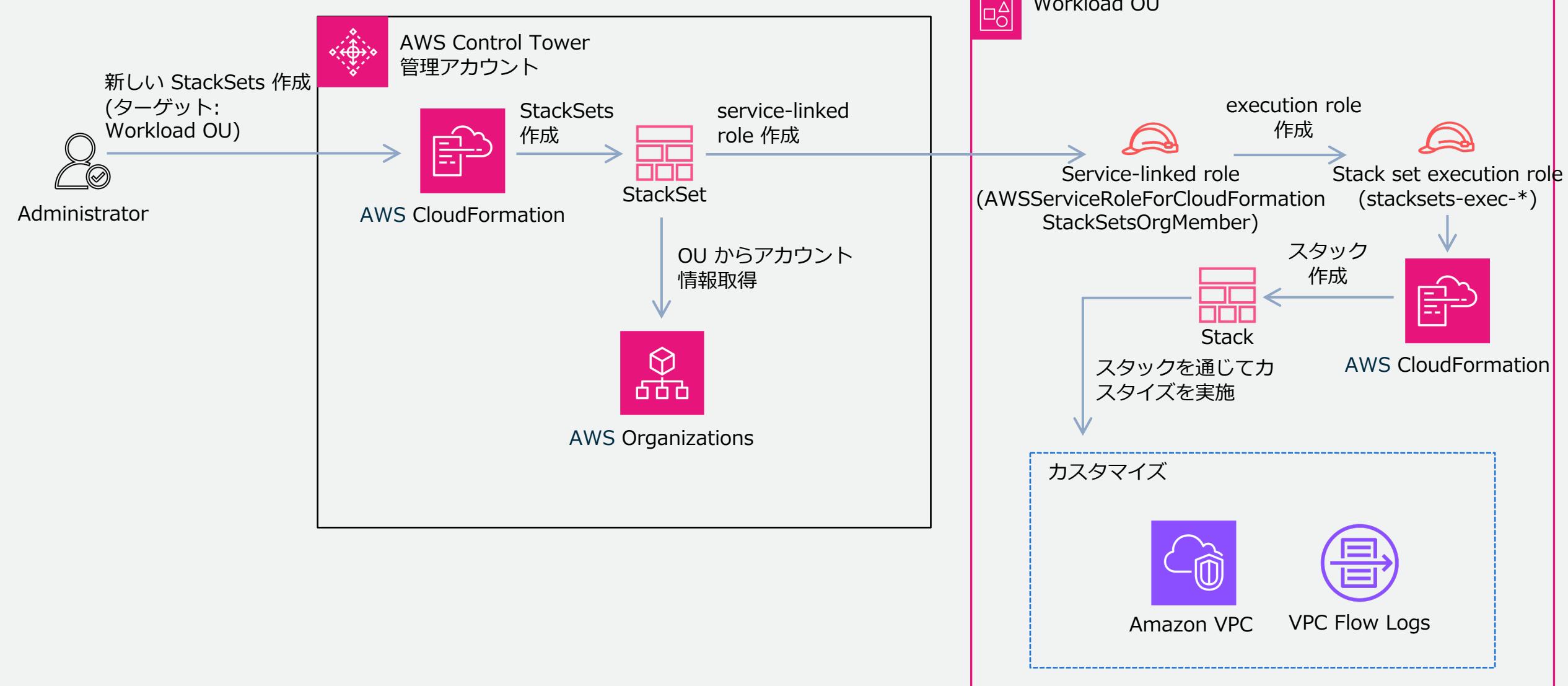
- Customizations for AWS Control Tower (CfCT)
- Account Factory for Terraform (AFT)

Account Factory Customization (AFC)

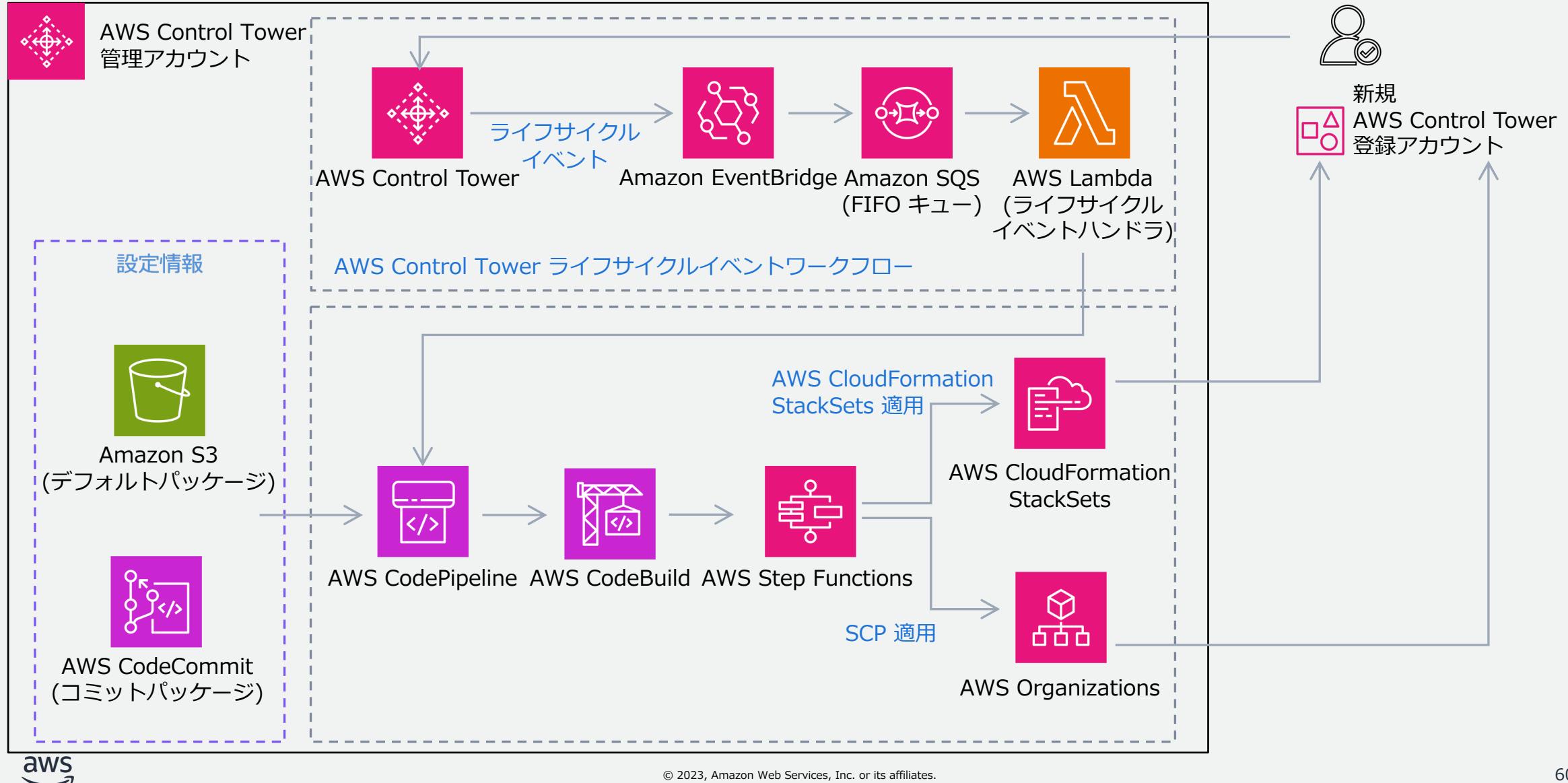


カスタマイズされた
アカウント作成

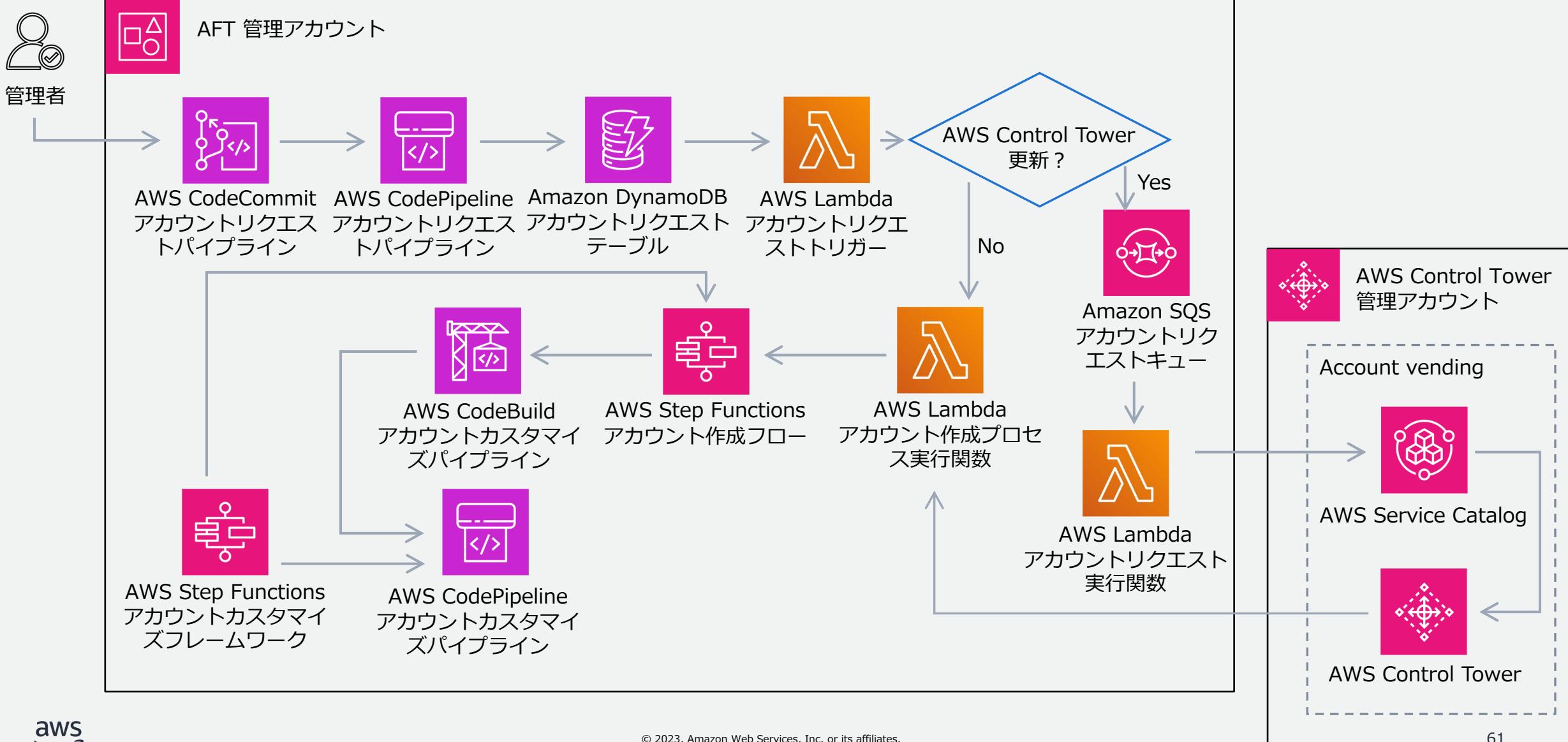
AWS CloudFormation StackSets



Customizations for AWS Control Tower (CfCT)



Account Factory for Terraform (AFT)



カスタマイズ方法の違い

利用する IaC(Infrastructure as Code) やカスタマイズのレベルで選択肢が変わる

名前	マネージドサービス	IaC	SCP設定	複数の設定
Account Factory Customization (AFC)	Yes	AWS CloudFormation Terraform	不可	不可
AWS CloudFormation StackSets	Yes	AWS CloudFormation	不可	可能
Customization for AWS Control Tower (CfCT)	No	AWS CloudFormation	可能	可能
Account Factory for Terraform (AFT)	No	Terraform	可能	可能

組織

AWS Control Tower の状態

AWS Control Tower で管理対象となるアカウントには
状態が存在する

状態	説明
未登録	アカウントは親 OU のメンバーですが、AWS Control Tower によって管理されていません
登録中	AWS Control Tower の管理対象になっています。親 OU のコントロール設定に適合するようにアカウントが調整されています
登録済み	アカウントは、その親 OU 用に設定されたコントロールによって管理されています。AWS Control Tower によって管理されています
登録に失敗しました	登録を試みましたが、アカウントを AWS Control Tower に登録できません
更新が利用可能	アカウントは登録済みですが、アカウントには利用可能な更新があります。環境に加えられた最近の変更を反映するには、アカウントを更新する必要があります

初期は「未登録」で登録を実行すると「登録済み」に遷移する



AWS Control Tower の組織

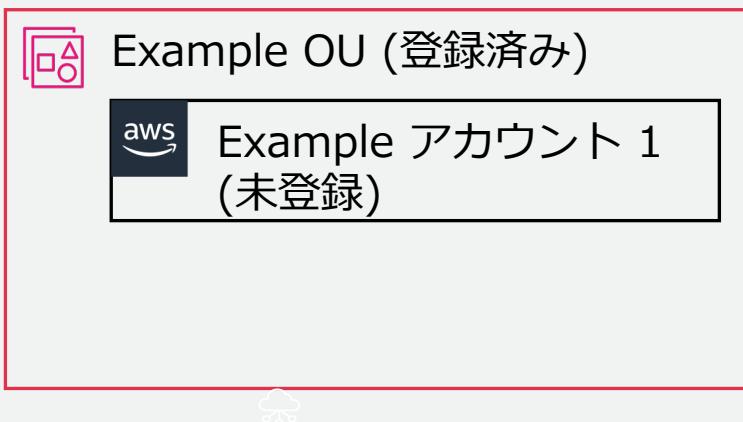
メンバーアカウントの状態を管理し AWS Control Tower の管理下への追加やランディングゾーンの更新を行う

実行可能なアクション

- 組織単位 (OU)
 - 登録、再登録、削除
- アカウント
 - 登録、更新、解除

アカウントの登録

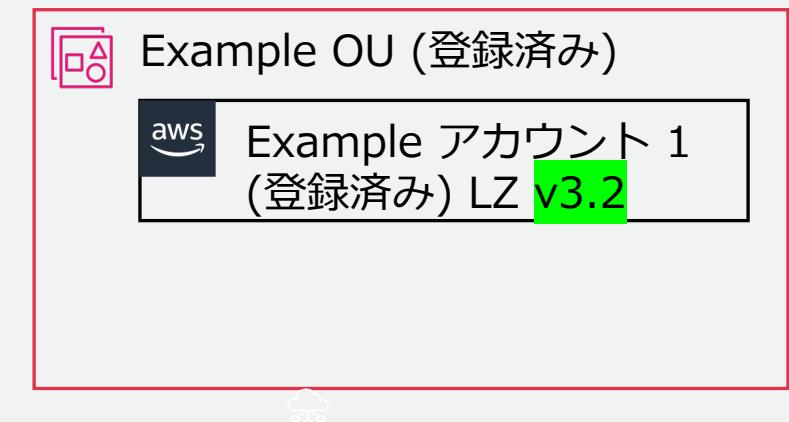
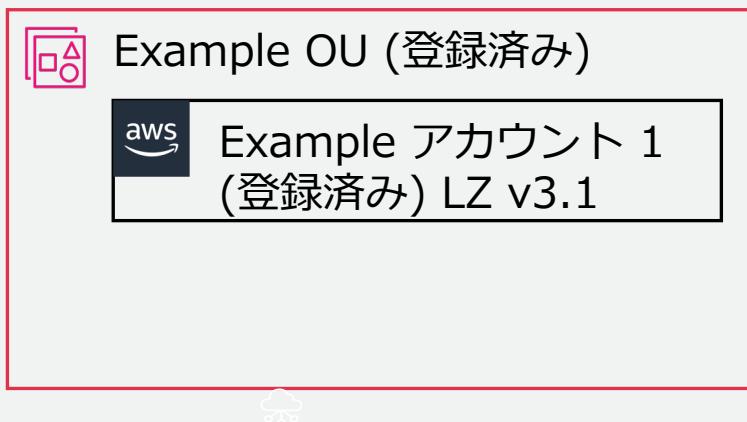
AWS Control Tower のガバナンスを未適用のアカウントに対し
アカウントごとに AWS Control Tower のガバナンスを適用する
状態は未登録から登録済みとなる



アカウントの更新

AWS Control Tower のガバナンスを適用済みのアカウントに
対しランディングゾーン (LZ) の更新を行う

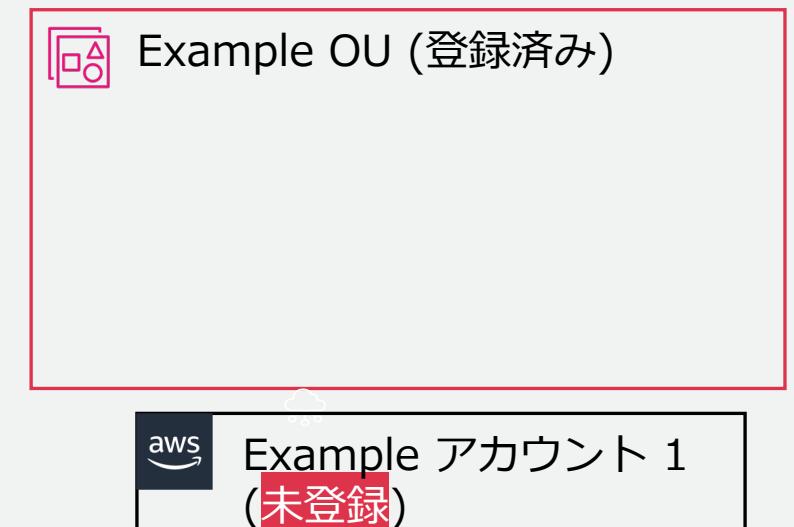
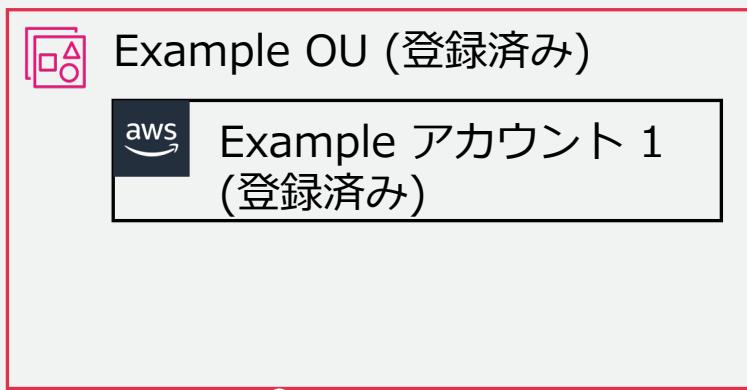
状態は登録済みのままでランディングゾーンのバージョンが更
新される



アカウントの解除

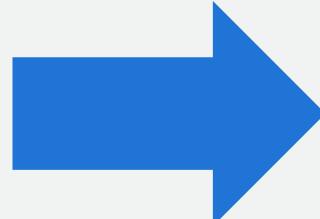
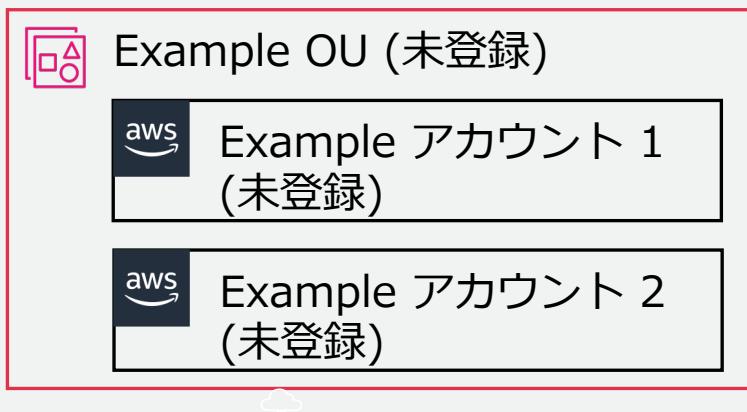
AWS Control Tower のガバナンスを適用済みのアカウントに
対して AWS Control Tower の管理対象から外す

状態は登録済みから未登録となる



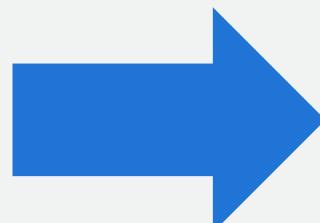
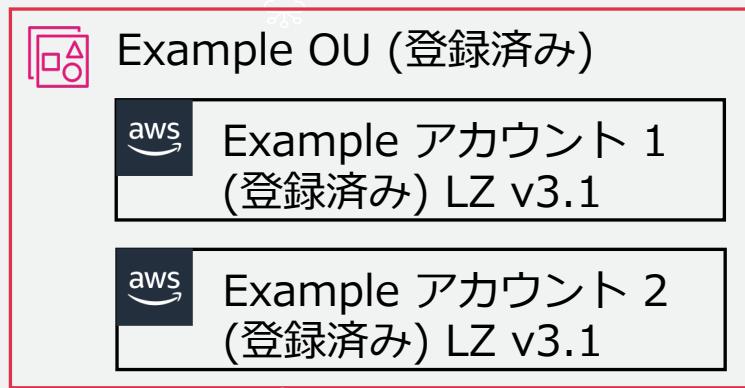
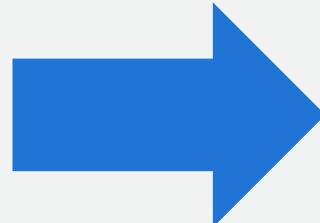
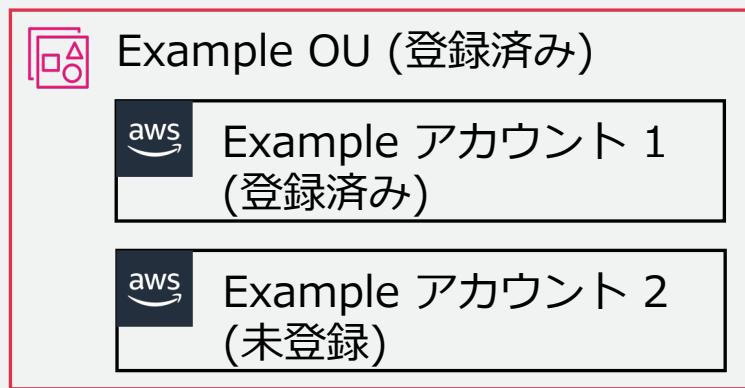
OU の登録

AWS Control Tower のガバナンスを未適用のアカウントに対し
OU ごとに AWS Control Tower のガバナンスを適用する
OU 直下のアカウントを未登録から登録済みに変更する



OU の再登録

AWS Control Tower のガバナンスを未適用のアカウントに対し
OU ごとに AWS Control Tower のガバナンスを適用する
ランディングゾーンのバージョンを更新する



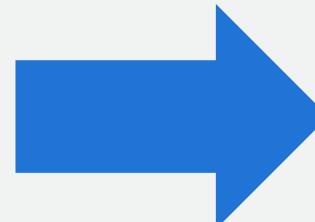
OU の削除

存在する OU を削除する

AWS Control Tower の状態を変更するアクションではない



Example OU (登録済み)



OU を削除する
アカウントが存在する場合
には実行できない

ダッシュボード

情報の一元管理

- アカウント数や非準拠リソースを把握できる

The screenshot shows the AWS Control Tower dashboard with the following key sections:

- Left Sidebar:** Includes links for 'AWS Control Tower' (ダッシュボード), 'はじめに', '組織', 'Account Factory', 'コントロールライブラリ' (with 'カテゴリー' and 'すべてのコントロール'), 'ユーザーとアクセス' (with '共有アカウント', 'ランディングゾーン設定', and 'アクティビティ'), 'Control Tower 向け AWS Marketplace', 'AWS Control Tower の新機能を見る', 'AWS Control Tower ブログを表示', '入門ライブラリでソリューションを起動', and 'フィードバックパネルに参加'.
- Top Header:** AWS Control Tower > ダッシュボード
- Top Bar:** 推奨されるアクション
- Summary Metrics:** 環境の概略 (組織単位: 5, アカウント: 9) and 有効な統制の概要 (予防管理: 27, 検出管理: 5, プロアクティブ管理: 2)
- Non-Compliant Resources:** 非準拠リソース (No results found). Includes a search bar and pagination controls (< 1 >).
- Registered Organizations:** 登録済み組織単位 (Root, Security). Includes a search bar and pagination controls (< 1 2 >).

まとめ



紹介した機能

The screenshot shows the AWS Control Tower dashboard with several key features highlighted:

- Left sidebar:** Includes links for "ダッシュボード", "はじめに", "組織", "Account Factory", "コントロールライブラリ", "ユーザーとアクセス", "共有アカウント", "ランディングゾーン設定", "Control Tower 向け AWS Marketplace", "AWS Control Tower の新機能を見る", "AWS Control Tower ブログを表示", "入門ライブラリでソリューションを起動", and "フィードバックパネルに参加".
- Top navigation:** AWS Control Tower > ダッシュボード
- Main content area:** Five numbered sections describing features:
 - 1. ランディングゾーン**
統制の効いた環境を作る
 - 2. コントロール**
ガバナンス強化を実現する
 - 3. Account Factory**
統制の効いたアカウントを作成する
 - 4. 組織**
アカウントや OU の状態を管理する
 - 5. ダッシュボード**
情報を一元管理する
- Bottom right corner:** AWS Control Tower ブログを表示

AWS Black Belt Online Seminar とは

- ・ 「サービス別」「ソリューション別」「業種別」などのテーマに分け、
アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナー
シリーズです
- ・ AWS の技術担当者が、AWS の各サービスやソリューションについてテーマ
ごとに動画を公開します
- ・ 以下の URL より、過去のセミナー含めた資料などをダウンロードするこ
とができます
 - ・ <https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/>
 - ・ <https://www.youtube.com/playlist?list=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBlqY>



ご感想は X (Twitter) へ！ハッシュタグは以下をご利用ください
#awsblackbelt



内容についての注意点

- ・ 本資料では 2023 年 9 月時点のサービス内容および価格についてご説明しています。AWS のサービスは常にアップデートを続けているため、最新の情報は AWS 公式ウェブサイト (<https://aws.amazon.com/>) にてご確認ください
- ・ 資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます
- ・ 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます
- ・ 技術的な内容に関しましては、有料の [AWS サポート窓口](#)へお問い合わせください
- ・ 料金面でのお問い合わせに関しましては、[カスタマーサポート窓口](#)へお問い合わせください (マネジメントコンソールへのログインが必要です)



Thank you!



AWS Control Tower

手順編 AWS Control Tower の有効化

Hajime Onishi

Cloud Support Engineer

2023/08

自己紹介

名前：大西 朔 (Hajime Onishi)

所属：アマゾン ウェブ サービス ジャパン合同会社
技術支援本部 クラウドサポートエンジニア

好きな AWS サービス：



AWS Control Tower



AWS CodeDeploy



AWS CodePipeline



AWS Distro for
OpenTelemetry

AWS Black Belt Online Seminar とは

- ・ 「サービス別」「ソリューション別」「業種別」などのテーマに分け、
アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナー
シリーズです
- ・ AWS の技術担当者が、AWS の各サービスやソリューションについてテーマ
ごとに動画を公開します
- ・ 以下の URL より、過去のセミナー含めた資料などをダウンロードするこ
とができます
 - ・ <https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/>
 - ・ <https://www.youtube.com/playlist?list=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBlqY>



ご感想は X (Twitter) へ！ハッシュタグは以下をご利用ください
#awsblackbelt



内容についての注意点

- ・ 本資料では 2023 年 8 月時点のサービス内容および価格についてご説明しています。AWS のサービスは常にアップデートを続けているため、最新の情報は AWS 公式ウェブサイト (<https://aws.amazon.com/>) にてご確認ください
- ・ 資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます
- ・ 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます
- ・ 技術的な内容に関しましては、有料の [AWS サポート窓口](#)へお問い合わせください
- ・ 料金面でのお問い合わせに関しましては、[カスタマーサポート窓口](#)へお問い合わせください (マネジメントコンソールへのログインが必要です)

本セミナーの対象者

- ・ 複数の AWS アカウントを管理されている方
- ・ AWS Control Tower を導入予定・検討中の方
- ・ AWS Control Tower におけるアカウントの登録手順を整理したい方

本セミナーの Goal

- ・ AWS Control Tower を有効化する手順と留意点を知る

本セミナーの前提知識

- ・ AWS Black Belt Online Seminar AWS Control Tower 基礎編

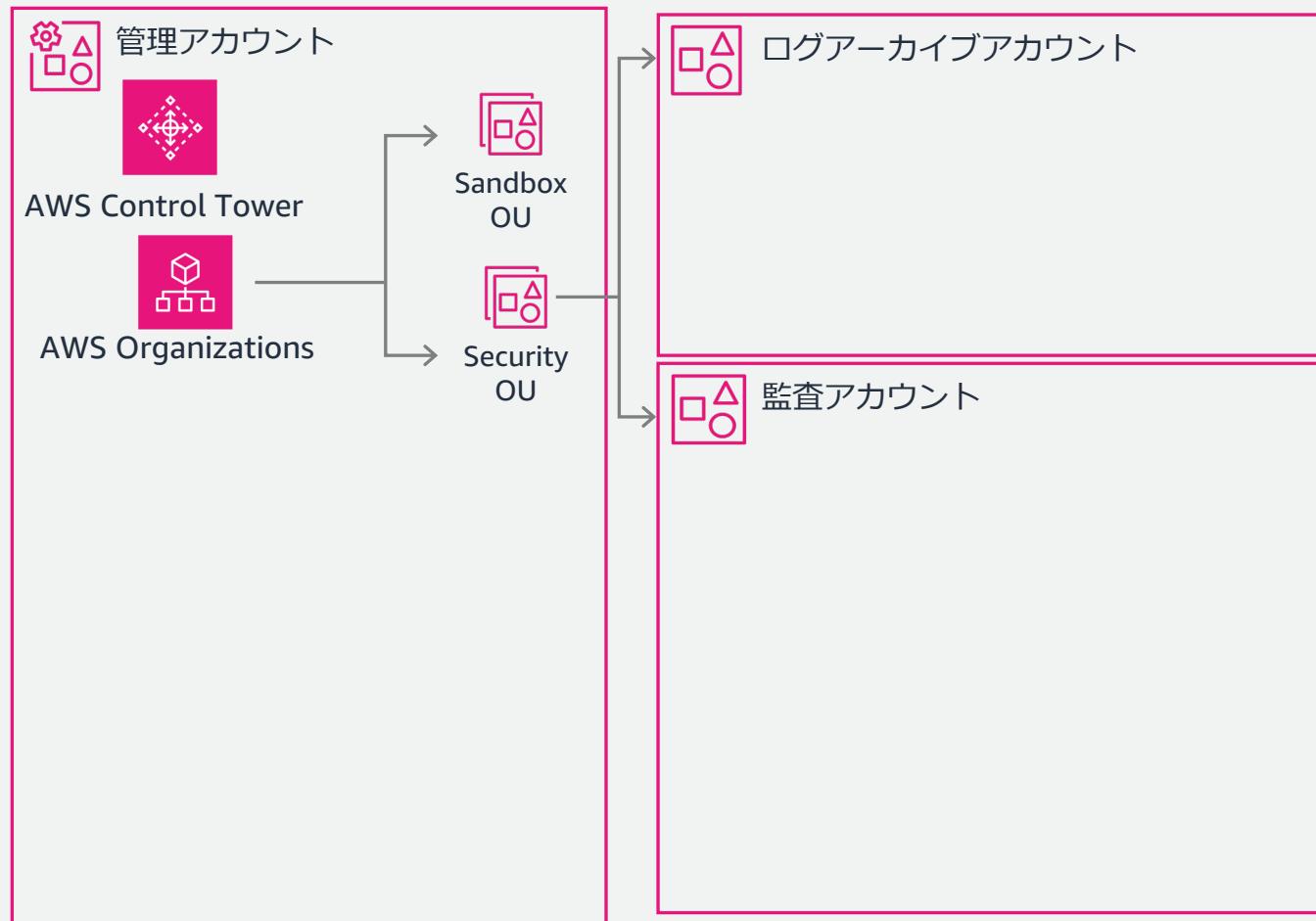
アジェンダ

1. ランディングゾーンのセットアップ
 1. AWS Control Tower ランディングゾーンの概要
 2. コンソールでのセットアップ手順
 3. よくあるエラーと修正方法・セットアップ時の留意点
2. メンバーアカウントの登録
 1. 組織単位とその直下のメンバーアカウントの登録手順
 2. Root 直下のメンバーアカウントの登録手順
 3. AWS Config を有効化済みの AWS アカウントの登録申請
 4. 登録手順のまとめ

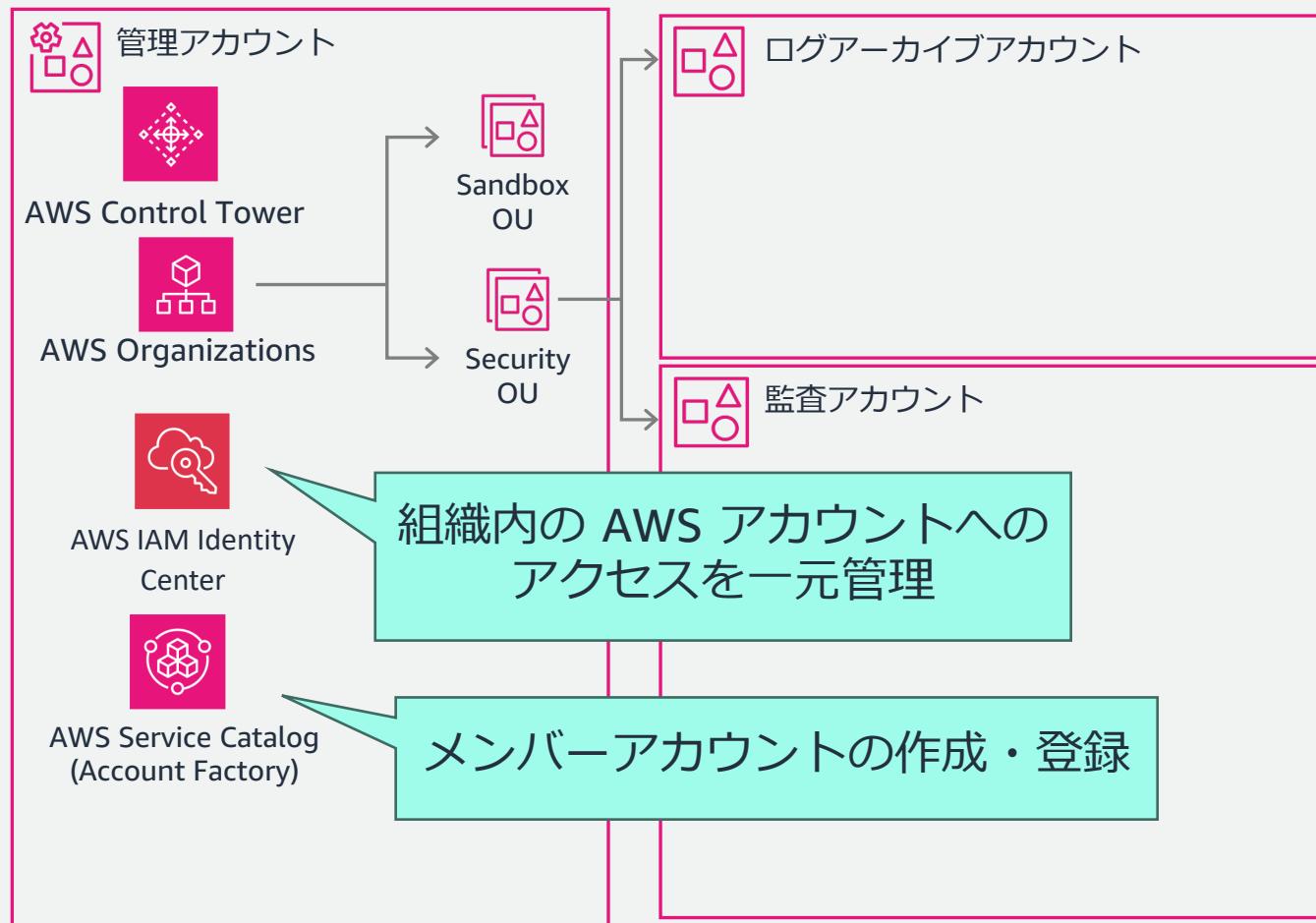
ランディングゾーンの セットアップ

1.1 AWS Control Tower ランディングゾーンの概要

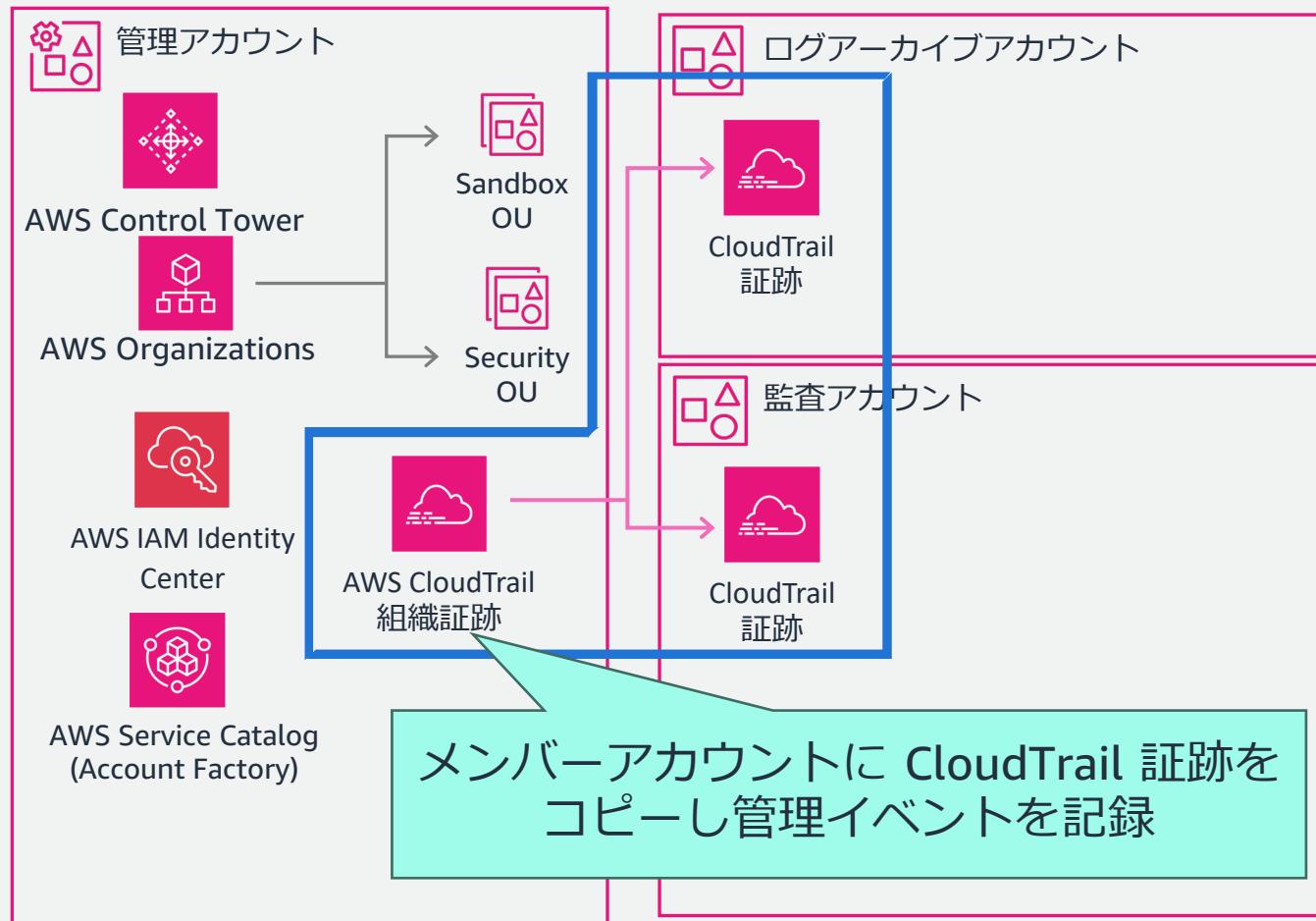
AWS Control Tower が管理アカウントで以下を実行



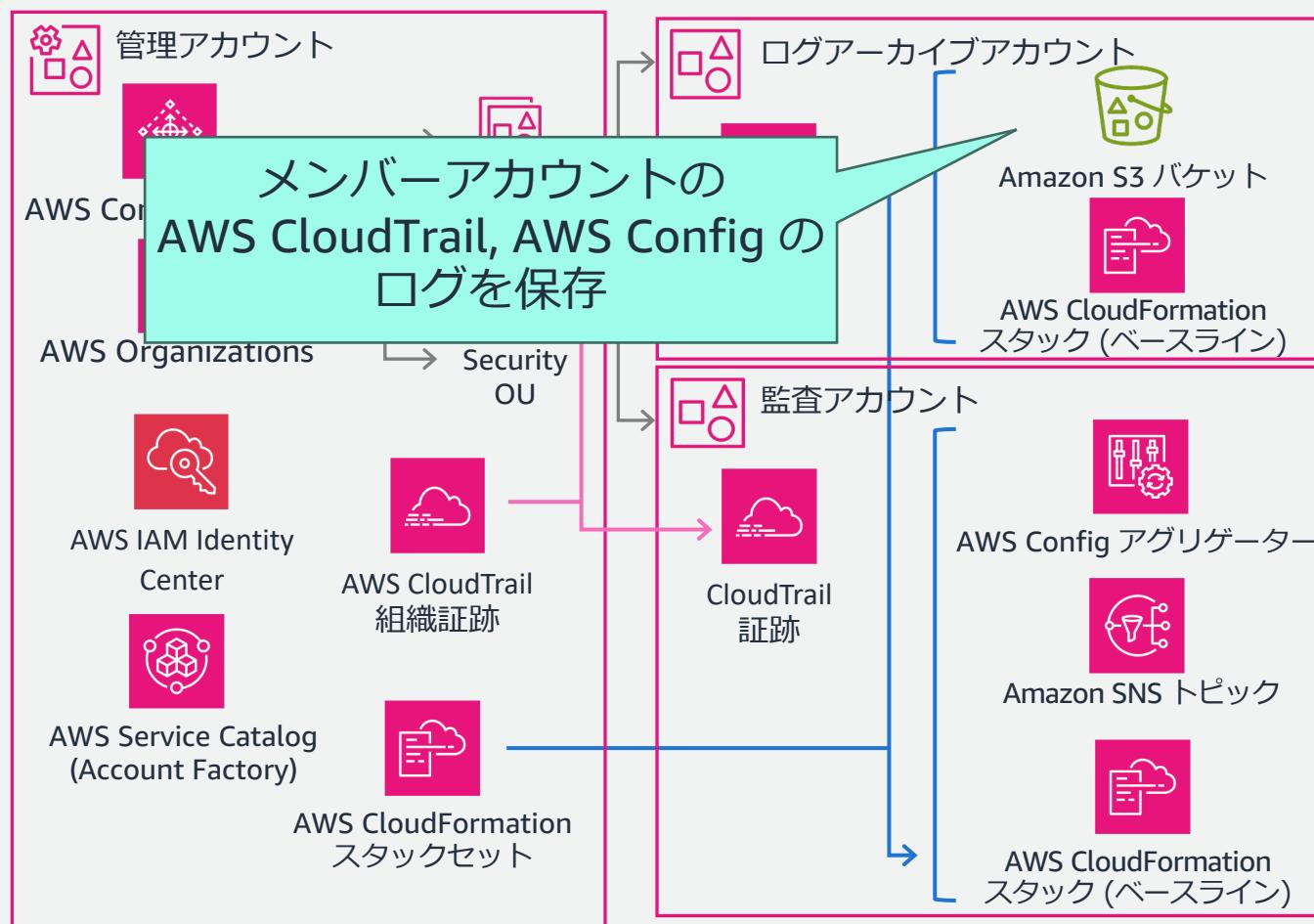
AWS Control Tower が管理アカウントで以下を実行



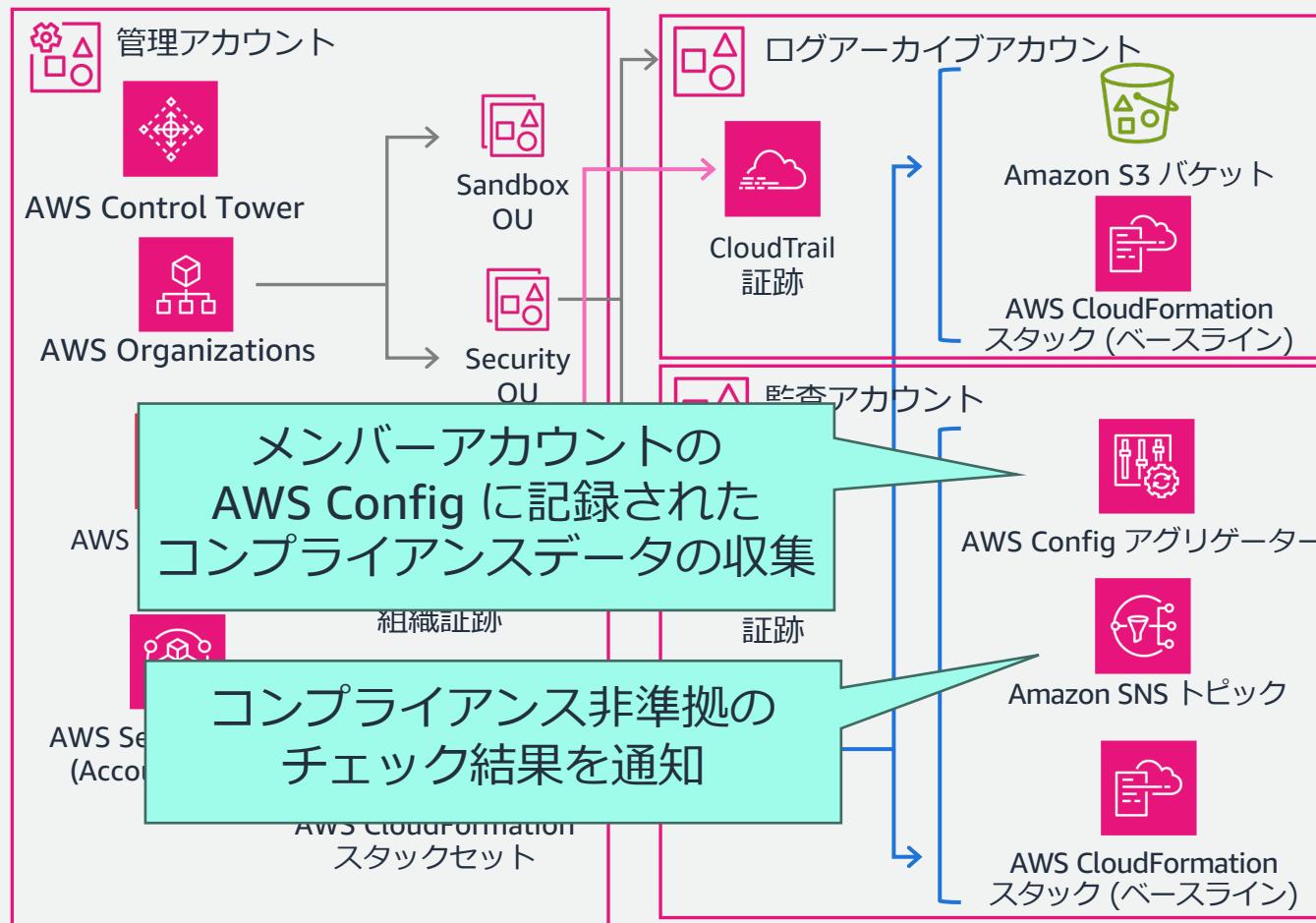
AWS Control Tower が管理アカウントで以下を実行



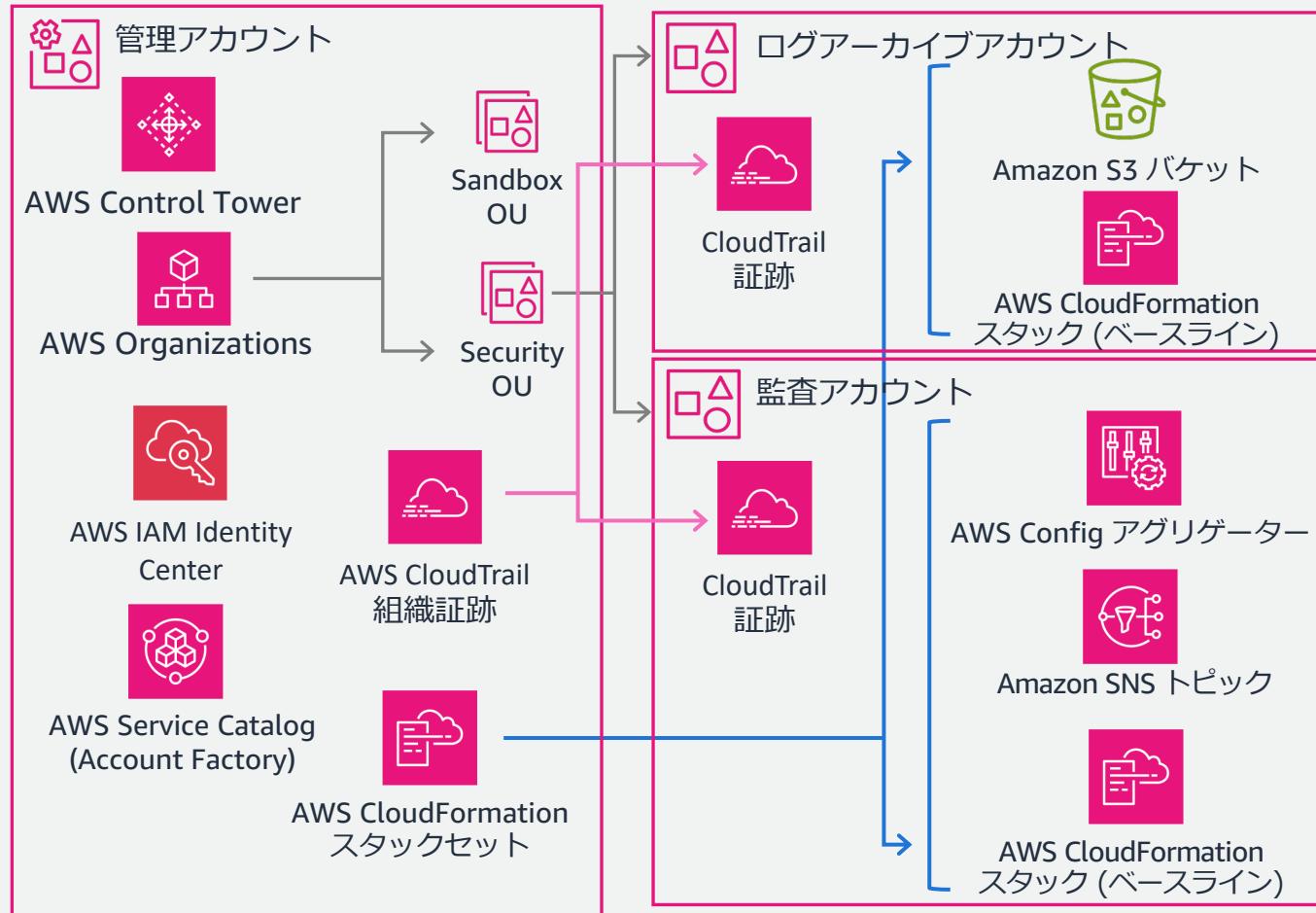
AWS Control Tower が管理アカウントで以下を実行



AWS Control Tower が管理アカウントで以下を実行



まとめ: セットアップ内容の概要



作成されるリソースの詳細は、
下記ドキュメントをご参照ください

https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/how-control-tower-works.html#what-shared

ランディングゾーンの セットアップ

1.2 コンソールでのセットアップ手順

セットアップ手順の概要

- 事前確認
- ステップ 1: リージョンを選択
- ステップ 2: 組織単位 (OU) の設定
- ステップ 3: 共有アカウントの設定
- ステップ 4: その他の設定
- ステップ 5: 確認とセットアップ

事前確認

- 操作する IAM ユーザー・ロールは **管理者権限 (AdministratorAccess)** を持つ
- AWS Control Tower によるリソース作成を妨げる SCP を Root にアタッチしていない
 - Root には FullAWSAccess ポリシーのみアタッチするのが無難**
 - 登録メンバーアカウントは必ず いずれかの組織単位に所属するので 組織単位にアタッチする独自の SCP や 予防コントロールでアクセス制御する

AWS Control Tower コンソールは、管理アカウントの管理者権限を持つユーザーだけが使用できます。それらのユーザーだけが、ランディングゾーン内で管理作業を実行できます。これは、ベストプラクティスに従って、ほとんどのユーザーとメンバーアカウント管理者に AWS Control Tower コンソールが表示されることがないことを意味します。管理アカウントの管理者グループのメンバーは、必要に応じて、ユーザーとメンバーアカウントの管理者に次の情報を説明する必要があります。

https://docs.aws.amazon.com/ja_jp/controlltower/latest/userguide/best-practices.html

ポリシーの詳細	
名前	FullAWSAccess
ARN	arn:aws:organizations::aws:policy/service_control_policy/p-FullAWSAccess
ポリシータイプ	サービスコントロールポリシー (AWS マネージド)
説明	Allows access to every operation

コンテンツ	ターゲット
{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", >Action": "*", "Resource": "*" }] }	

AWS マネージドポリシー: FullAWSAccess の内容



事前確認

- サポートするすべてのリージョンで AWS STS を有効化している

① 注記

起動時に、AWS Control Tower が管理するすべてのリージョンの管理アカウントで、AWS Security Token Service (STS) エンドポイントをアクティブにする必要があります。この操作を行わないと、設定プロセスの途中で起動が失敗する可能性があります。

https://docs.aws.amazon.com/ja_jp/controlltower/latest/userguide/getting-started-prereqs.html

・ 確認・修正方法

- IAM コンソールにアクセス
- [アクセス管理] -> [アカウント設定]
- Security Token Service (STS)
エンドポイントのステータスを
アクティブに変更

リージョン名	エンドポイント	STS ステータス
グローバルエンドポイント	https://sts.amazonaws.com	常にアクティブ
米国東部 (バージニア北部)	https://sts.us-east-1.amazonaws.com	常にアクティブ
アジアパシフィック (東京)	https://sts.ap-northeast-1.amazonaws.com	● アクティブ
アジアパシフィック (ソウル)	https://sts.ap-northeast-2.amazonaws.com	● アクティブ
アジアパシフィック (大阪)	https://sts.ap-northeast-3.amazonaws.com	● アクティブ
アジアパシフィック (ムンバイ)	https://sts.ap-south-1.amazonaws.com	● アクティブ
アジアパシフィック (シンガポール)	https://sts.ap-southeast-1.amazonaws.com	● アクティブ
アジアパシフィック (シドニー)	https://sts.ap-southeast-2.amazonaws.com	● アクティブ
カナダ (中部)	https://sts.ca-central-1.amazonaws.com	● アクティブ
欧州 (フランクフルト)	https://sts.eu-central-1.amazonaws.com	● アクティブ
欧州 (ストックホルム)	https://sts.eu-north-1.amazonaws.com	● アクティブ
欧州 (アイルランド)	https://sts.eu-west-1.amazonaws.com	● アクティブ
欧州 (ロンドン)	https://sts.eu-west-2.amazonaws.com	● アクティブ
欧州 (パリ)	https://sts.eu-west-3.amazonaws.com	● アクティブ
南米 (サンパウロ)	https://sts.sa-east-1.amazonaws.com	● アクティブ

IAM コンソールでの AWS STS 設定確認

1. リージョンを選択

1. ホームリージョンを選択

- **設定後に変更できない**
- 最も使用頻度の高いリージョンを選択する
- AWS IAM Identity Center を有効化済みの場合同じリージョンを選択する

https://docs.aws.amazon.com/ja_jp/controltower/latest/userguide/region-how.html



事前確認の後、Control Tower コンソールで
ランディングゾーンの設定を開始

ホームリージョン

AWS リージョンセレクター、または以下のドロップダウンからリージョンを選択して AWS Control Tower のホームリージョンを選択します。これは、共有アカウントのリソースがプロビジョニングされるデフォルトのリージョンです。

ランディングゾーンの設定後にホームリージョンを変更することはできません。

アジアパシフィック (東京)

Control Tower コンソールでのランディングゾーンのセットアップ
ステップ 1-1: ホームリージョンの選択

1. リージョンを選択

2. 管理対象リージョンを選択

- AWS Control Tower による ガバナンスを有効にするリージョン
- AWS Config などのリージョナルな AWS サービスをデプロイする
- 設定後にリージョンを 変更・追加・削除できる

ガバナンスのための追加リージョンを選択 (1/22) [情報](#) [C](#)

AWS Control Tower によるガバナンスのための追加リージョンを選択します。ホームリージョンは自動的に選択され、選択を解除することはできません。ステータスが「非アクティブ」のリージョンを選択すると、AWS Control Tower はセットアップ中に自動的にリージョンをアクティビ化します。

① AWS Control Tower のランディングゾーンは、ワークフローを実行する必要がある AWS リージョンにのみ拡張することをお勧めします。

AWS Control Tower の一部のコントロールは、すべての AWS リージョンで利用できるわけではありません。詳細については、次をご覧ください: [コントロールの制限](#). [\[リンク\]](#)

- AWS Security Hub コントロールは、バーレーン (me-south-1)、ジャカルタ (ap-southeast-3)、ケープタウン (af-south-1)、香港 (ap-east-1)、大阪 (ap-northeast-3)、ミラノ (eu-south-1) ではご利用いただけません。
- ジャカルタ (ap-southeast-3)、ケープタウン (af-south-1)、大阪 (ap-northeast-3)、ミラノ (eu-south-1)、および北カリフォルニア (us-west-1) では 16 件の検出コントロールがご利用いただけません。

リージョン名	リージョンコード	AWS Control Tower ステータス	AWS リージョンのステータス
アジアパシフィック (東京) [ホームリージョン]	ap-northeast-1	管理対象外	デフォルトでアクティブ
米国東部 (バージニア北部)	us-east-1	管理対象外	デフォルトでアクティブ
米国東部 (オハイオ)	us-east-2	管理対象外	デフォルトでアクティブ

ステップ 1-2: 管理対象リージョンの選択

1. リージョンを選択

3. リージョン拒否設定

- 管理対象リージョン以外では AWS サービスのアクセスを拒否する
- 登録済み組織単位に対して リージョン拒否 SCP を設定する
- 一部のグローバルサービスなどは 例外的にアクセスを許可

https://docs.aws.amazon.com/ja_jp/controlltower/latest/userguide/data-residency-controls.html#primary-region-deny-policy

リージョン拒否設定 [情報](#)

AWS Control Tower のステータスが [管理対象外] と表示されている AWS リージョン、および AWS Control Tower が利用できないリージョンで、AWS のサービスおよびオペレーションへのアクセスを拒否できます。ホームリージョンへのアクセスを拒否することはできません。リージョン拒否コントロールから免除される AWS のサービスを選択します。

⚠️ リージョン拒否機能は、AWS Control Tower のリージョン設定に基づいて AWS のサービスへのアクセスを禁止します。ステータスが [管理対象外] の AWS リージョンへのアクセスが拒否されます。リージョン拒否機能は、AWS Control Tower が利用できないリージョンへのアクセスも拒否します。この設定は後で変更できます。

コントロールの適用後はリソースにアクセスできなくなるため、リージョン拒否コントロールを有効にする前に、これらのリージョンに既存のリソースがないことを確認してください。**有効** を選択すると、AWS Control Tower はすべての登録済みの OU に [リージョン拒否予防コントロール](#) を適用します。

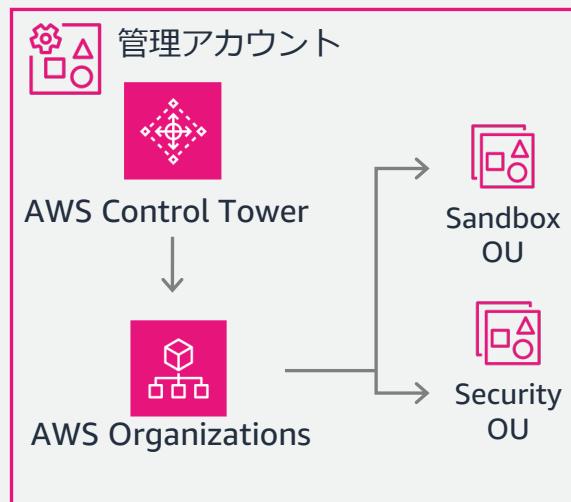
有効 を選択すると、AWS Control Tower は登録済みの OU のコントロールを削除します。すべての管理対象外リージョンは [管理対象外] のステータスのままであり、AWS Control Tower が利用できないリージョンにリソースをデプロイできます。

有効 有効になっていません

ステップ 1-3: リージョン拒否設定

2. 組織単位 (OU) の設定

- 組織単位 (OU) を作成
 - 基礎となる OU (必須): デフォルト名は Security
 - 追加の OU (任意): デフォルト名は Sandbox



基礎となる OU

AWS Control Tower は、ランディングゾーンで適切に計画された OU 構造を開始するために、ユーザー用のセキュリティ OU をセットアップします。この OU には、ログアーカイブアカウントとセキュリティ監査アカウント (監査アカウントとも呼ばれます) の 2 つの共有アカウントが含まれています。

OU 名を変更 - オプション

「Security」は、共有アカウントについてのデフォルト OU 名です。OU 名は一意である必要があります、ランディングゾーンのセットアップ後に編集できます。

Security

追加の OU

マルチアカウントシステムのセットアップをサポートするために、AWS Control Tower はランディングゾーンのセットアップ時にセカンダリ OU を作成することを推奨します。この OU は、任意のプロダクションアカウントまたは開発アカウントを保存するために使用できます。追加の OU は、ランディングゾーンのセットアップ後に作成することができます。

新しい OU を作成 - 推奨

OU の作成をオプトアウト

新しい OU を作成 - 推奨

OU 名を変更 - オプション

「Sandbox」は、追加 OU についてのデフォルト OU 名です。OU 名は一意である必要があります、ランディングゾーンのセットアップ後に編集できます。

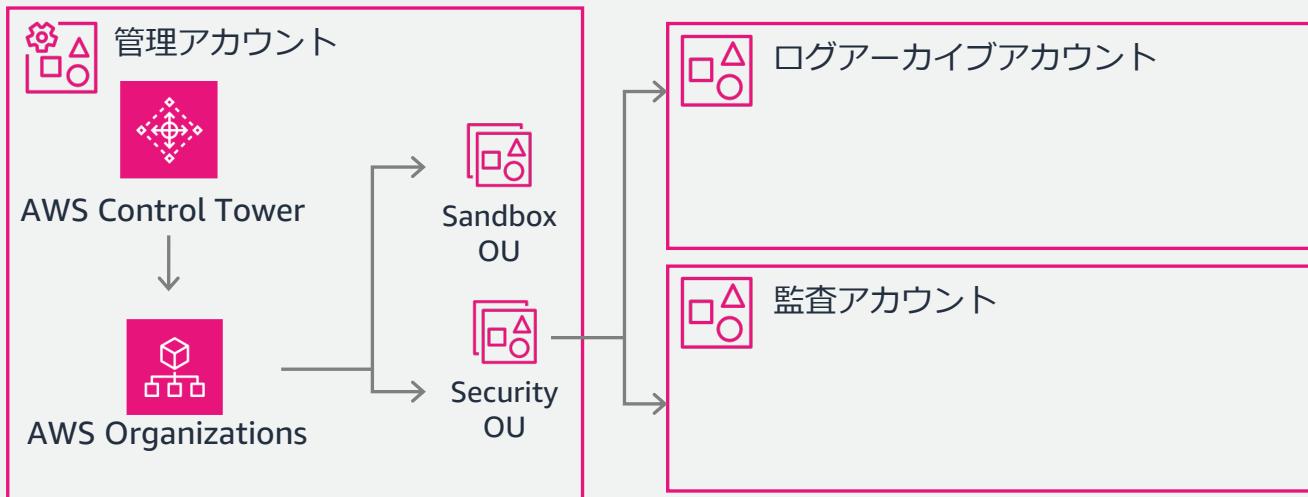
Sandbox

ステップ 2: 組織単位の設定

3. 共有アカウントの設定

- ログアーカイブ・監査アカウント
 - メールアドレスとアカウント名を指定して新規で作成する
 - メンバーアカウントのアカウント ID を指定して使用する

<https://aws.amazon.com/jp/blogs/news/use-existing-logging-and-security-account-with-aws-control-tower/>



ログアーカイブアカウント

ログアーカイブアカウントは、すべてのアカウントの API アクティビティとリソース設定の immutable ログのリポジトリです。

新規アカウントの作成
ログアーカイブアカウント用の新しいメールアドレスを作成します。この E メールアドレスを既存の AWS アカウントで使用することはできません。

既存のアカウントの使用
組織に存在するログアーカイブアカウントのアカウント ID を入力します。

AWS Organizations に存在するアカウント ID を入力します
xxxxxxxxxxxxxx
12 行の数字である必要があります。アカウントの桁数が 12 行未満の場合は、先頭にゼロを追加します。

既存の AWS アカウントの詳細

アカウント E メール
-
アカウント名
-

アカウントの監査

監査アカウントは制限付きアカウントです。これにより、セキュリティおよびコンプライアンスチームは、組織内のすべてのアカウントへのアクセスを取得できます。

新規アカウントの作成
アカウントの監査用の新しいメールアドレスを作成します。この E メールアドレスを既存の AWS アカウントで使用することはできません。

既存のアカウントの使用
組織に存在するアカウントの監査のアカウント ID を入力します。

アカウントの作成
audit@example.com
監査アカウント E メールアドレスを既存の AWS アカウントで使用することはできません。さらに、6~64 文字である必要があります。
アカウント名を変更 - オプション
監査アカウント名は、他のアカウント名と重複しないようにしてください。ランディングゾーンをセットアップした後で名前を編集することはできません。

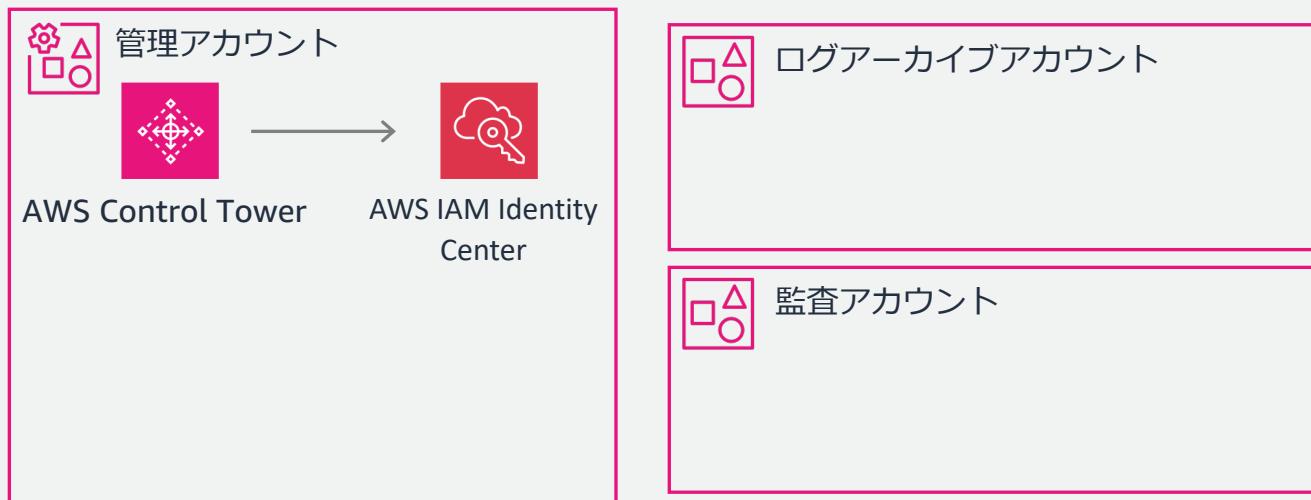
Audit

ステップ 3: 共有アカウントの設定

4. その他の設定

- AWS IAM Identity Center による AWS アカウントアクセスの設定
 - ユーザーグループ・許可セットを設定
 - 使用するかしないか選択可能

https://docs.aws.amazon.com/ja_jp/controlltower/latest/userguide/sso.html



AWS アカウントアクセス設定 情報
AWS Control Tower に登録されている AWS アカウントへのアクセスを管理する方法を選択します。これは後で変更できます。

AWS Control Tower は IAM Identity Center を使用して AWS アカウントアクセスを設定します。
AWS を使い始めたばかりの場合や、アクセス管理構造が AWS Control Tower のグループとアクセス許可セット  と連携している場合に最適です。後で IAM Identity Center で外部 ID プロバイダー (IdP) に接続できます。

IAM Identity Center またはその他の方法によるセルフマネージド型 AWS アカウントアクセス。
AWS アカウントアクセス管理に関するカスタム要件がある場合に最適です。AWS Control Tower はアカウントアクセスを管理しません。IAM Identity Center または別のアクセス方法を設定する必要があります。

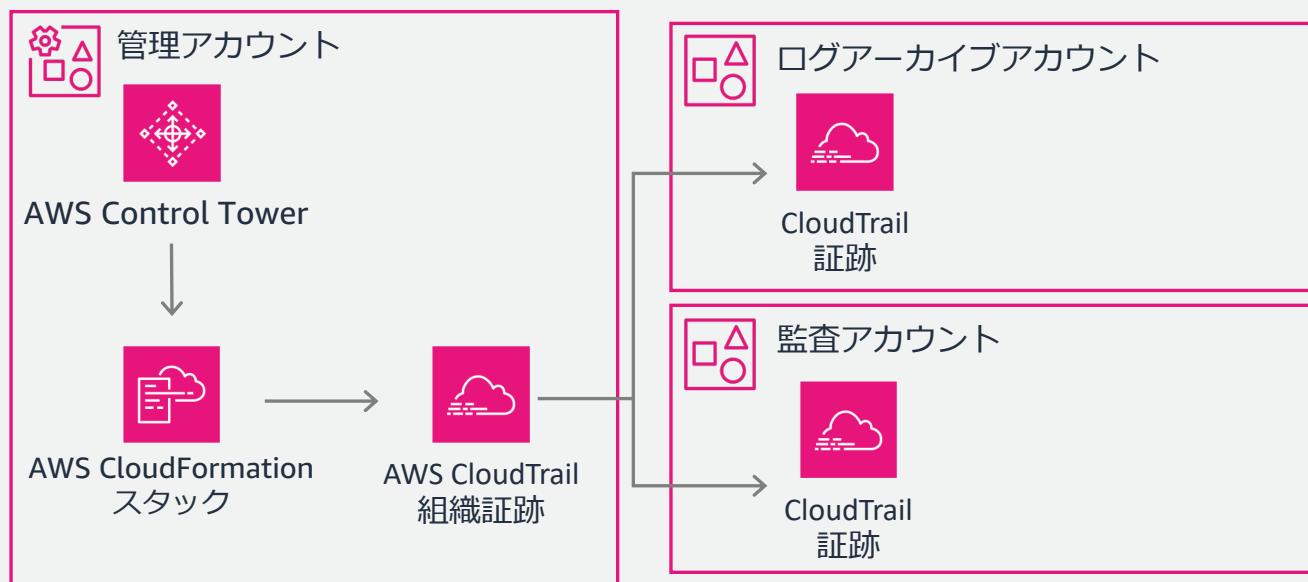
ステップ 4-1: IAM Identity Center による
アクセス設定の有効・無効

4. その他の設定

- 管理アカウントのリソース作成

- AWS CloudTrail 組織証跡を作成

- 必ず証跡は作成するが
有効・無効を選択可能**



AWS CloudTrail の設定 情報

AWS CloudTrail は、AWS Control Tower のアクションをイベントとしてキャプチャします。証跡を作成すると、Amazon S3 バケットへの CloudTrail イベントの継続的デリバリーを有効にできます。

組織レベルの CloudTrail では、AWS Control Tower はすべてのアカウントの情報を組織の証跡に集約し、ログ情報を指定された Amazon S3 バケットに配信します。ファイルパスには、組織 ID がプレフィックスとして含まれています。

⚠️ 組織レベルの CloudTrails を有効にしない場合、AWS Control Tower は AWS CloudTrail ログを管理しません。この設定は、ランディングゾーンを更新するときに変更できます。

AWS Control Tower では、すべての組織またはアカウントが AWS CloudTrail のログ記録を確立することを強く推奨します。AWS Control Tower で管理されないカスタム証跡を作成するか、[有効] を選択できます。必須の検出コントロールは、登録されたアカウントが CloudTrail のログ記録が有効かどうかを検出します。詳細は[こちら](#)

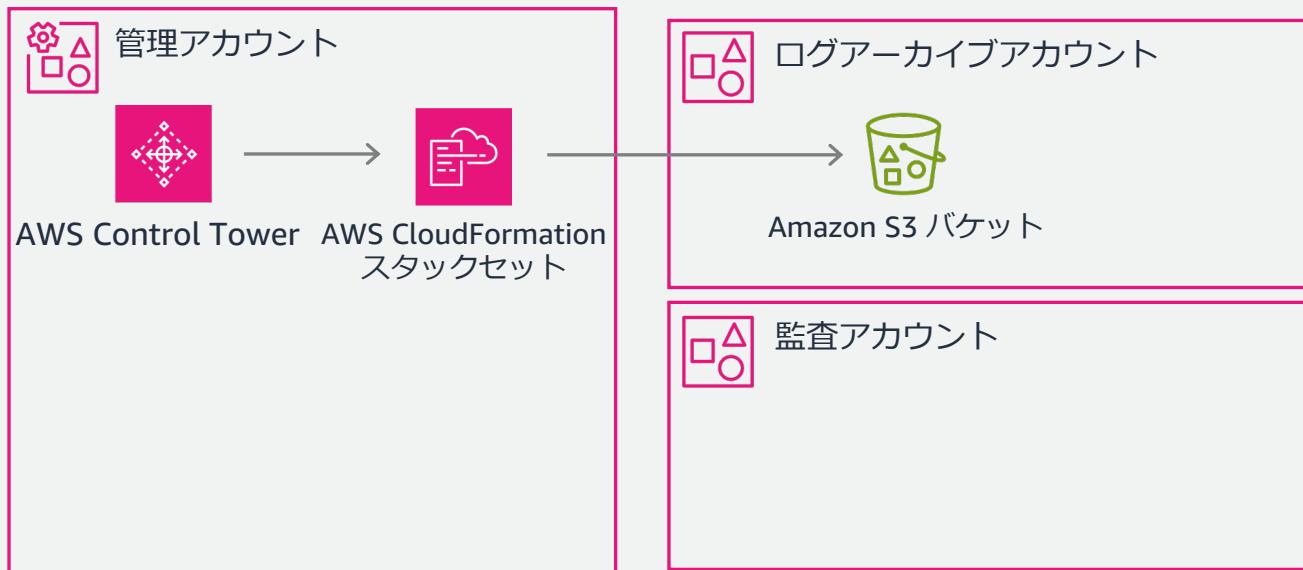
有効

有効になっていません

ステップ 4.2: AWS CloudTrail 組織証跡の有効・無効

4. その他の設定

- AWS CloudTrail と AWS Config ログ用の Amazon Simple Storage Service (Amazon S3) バケットの保持期間 (1 日 ~ 15 年)
 - **ログ用のバケットの保持期間:**
デフォルト 1 年
 - **アクセスログ用のバケットの保持期間:**
デフォルト 10 年



Amazon S3 のログ設定 - オプション 情報

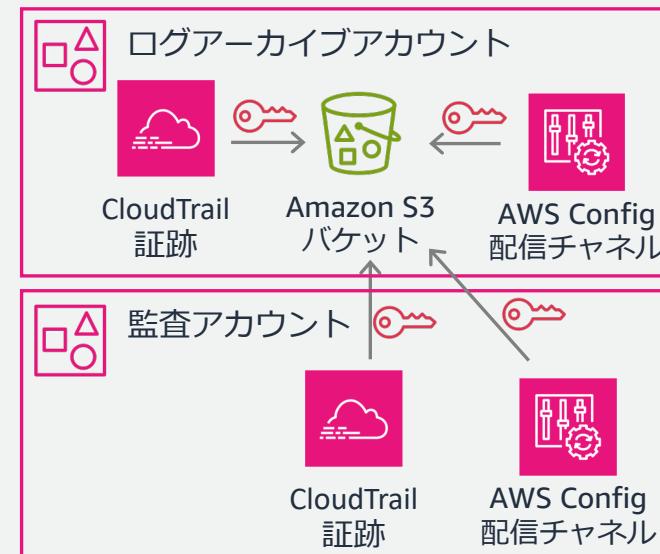
これらの 2 つのフィールドに、Amazon S3 ロギングバケットとアクセスロギングバケットのライフサイクル保持時間を表す数値を入力します。どちらのバケットでも指定できる最小保持時間は 1 日です。年の場合は、小数点以下 2 衆まで表すことができます。日の場合は整数を指定する必要があります。例えば、5 日や 1.02 年を指定できますが、1.34 日は指定できません。1.34 日間を指定する場合は、数値を切り上げるか切り下げるかで整数値にします。1 年未満 (0.02 年など) の期間の場合は、日数に変換してください。

ログ用の Amazon S3 バケットの保持	Format for logging
Default: 1	years
1 ~ 15 の整数と小数点以下 2 衆まで含める必要があります。	
アクセスログ用の Amazon S3 バケットの保持	Format for access logging
Default: 10	years
1 ~ 15 の整数と小数点以下 2 衆まで含める必要があります。	

ステップ 4.3: ログバケットの保持期間設定

4. その他の設定

- AWS Key Management Service (AWS KMS) 暗号化
 - AWS CloudTrail, AWS Config のログを管理アカウントの AWS KMS キーで暗号化する
 - 使用するかしないか選択可能



KMS 暗号化 - オプション [情報](#)

AWS Key Management Service (KMS) は、暗号化キーを作成および管理し、AWS Control Tower でリソースをコントロールするのに役立ちます。キーを選択するには、チェックボックスをオンにします。KMS キーには、AWS CloudTrail および AWS Config のアクセス許可が必要です。マルチリージョンキーはサポートされていません。詳細は[こちら](#)

暗号化設定を有効にして、カスタマイズする
暗号化設定を無効にするには、このチェックボックスをオフにします。

AWS KMS カスタマーキーを選択する
このキーは、リソースの暗号化と復号化に使用されます。

AWS KMS キーを選択するか、ARN を入力します。

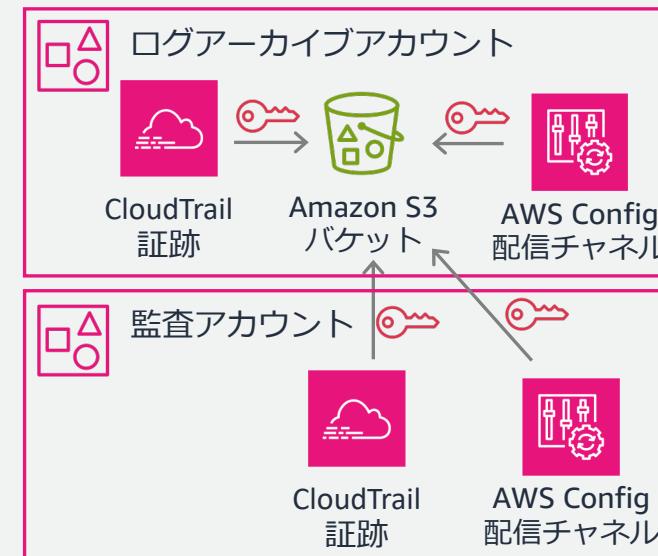
対称キーのみが表示されます。非対称キーはサポートされていません。

[KMS キーを作成する](#)

ステップ 4.4: ログの AWS KMS による暗号化

4. その他の設定

- AWS KMS 暗号化の要確認事項
 - 対称な單一リージョンキーか
 - キーにアクセス許可
 - AWS CloudTrail, AWS Config のサービスプリンシパルに KMS キーへのアクセス許可を追加



KMS 暗号化 - オプション [情報](#)

AWS Key Management Service (KMS) は、暗号化キーを作成および管理し、AWS Control Tower でリソースをコントロールするのに役立ちます。キーを選択するには、チェックボックスをオンにします。KMS キーには、AWS CloudTrail および AWS Config のアクセス許可が必要です。マルチリージョンキーはサポートされていません。詳細は[こちら](#)。

暗号化設定を有効にして、カスタマイズする
暗号化設定を無効にするには、このチェックボックスをオフにします。

AWS KMS カスタマーキーを選択する
このキーは、リソースの暗号化と復号化に使用されます。

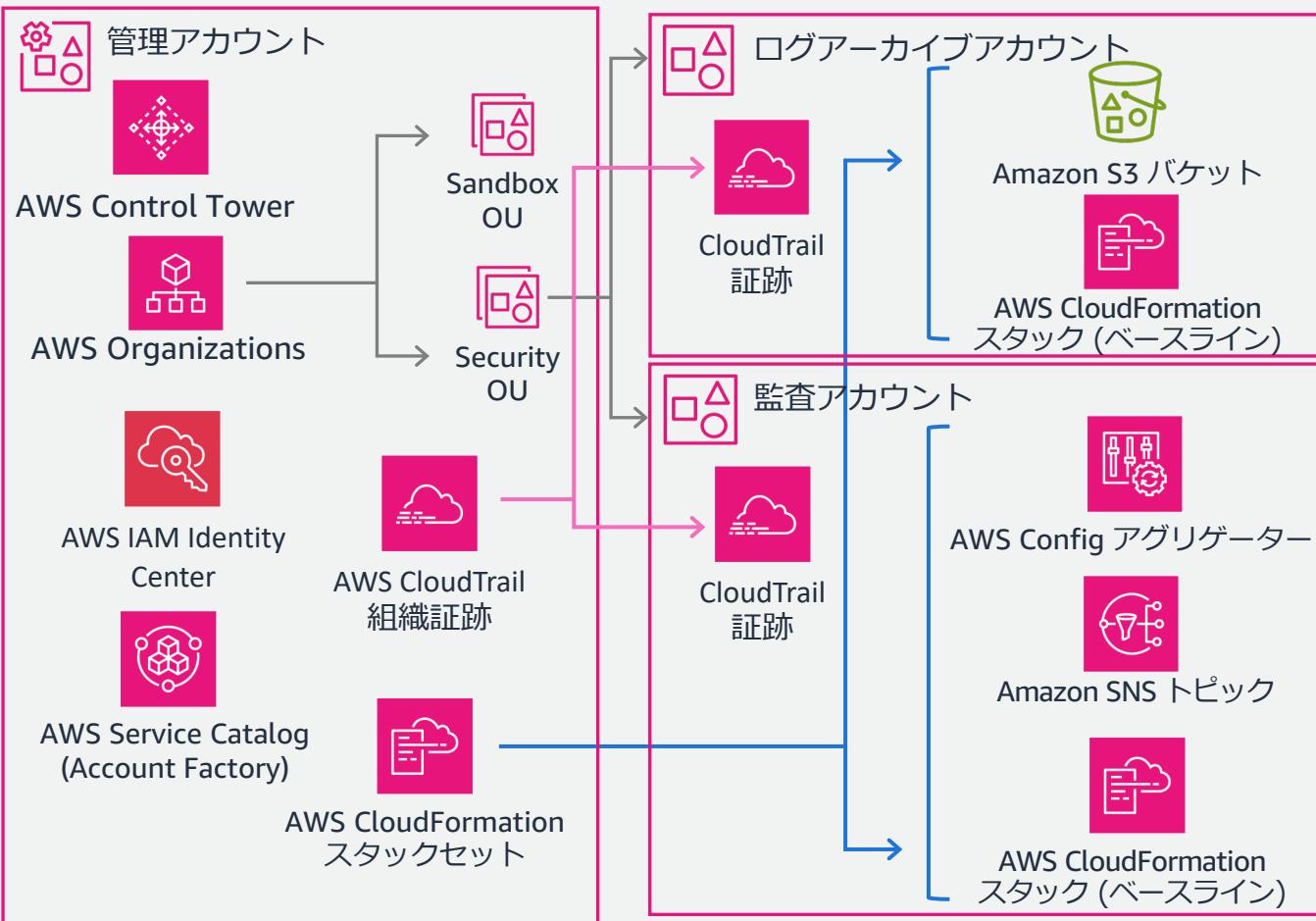
AWS KMS キーを選択するか、ARN を入力します。

対称キーのみが表示されます。非対称キーはサポートされていません。

KMS キーを作成する

ステップ 4.4: ログの AWS KMS による暗号化

5. 確認とセットアップ



サービスのアクセス許可

AWS Control Tower には、AWS リソースを管理し、お客様に代わってルールを適用するためのアクセス許可が必要です。

▶ アクセス許可の詳細

▶ ガイダンスの詳細

私は、AWS リソースを管理する目的で、および私に代わってルールを適用する目的で、AWS Control Tower がアクセス許可を使用することを了承しています。また、AWS Control Tower の使用に関するガイダンス、およびその基盤となる AWS リソースについても了承しています。

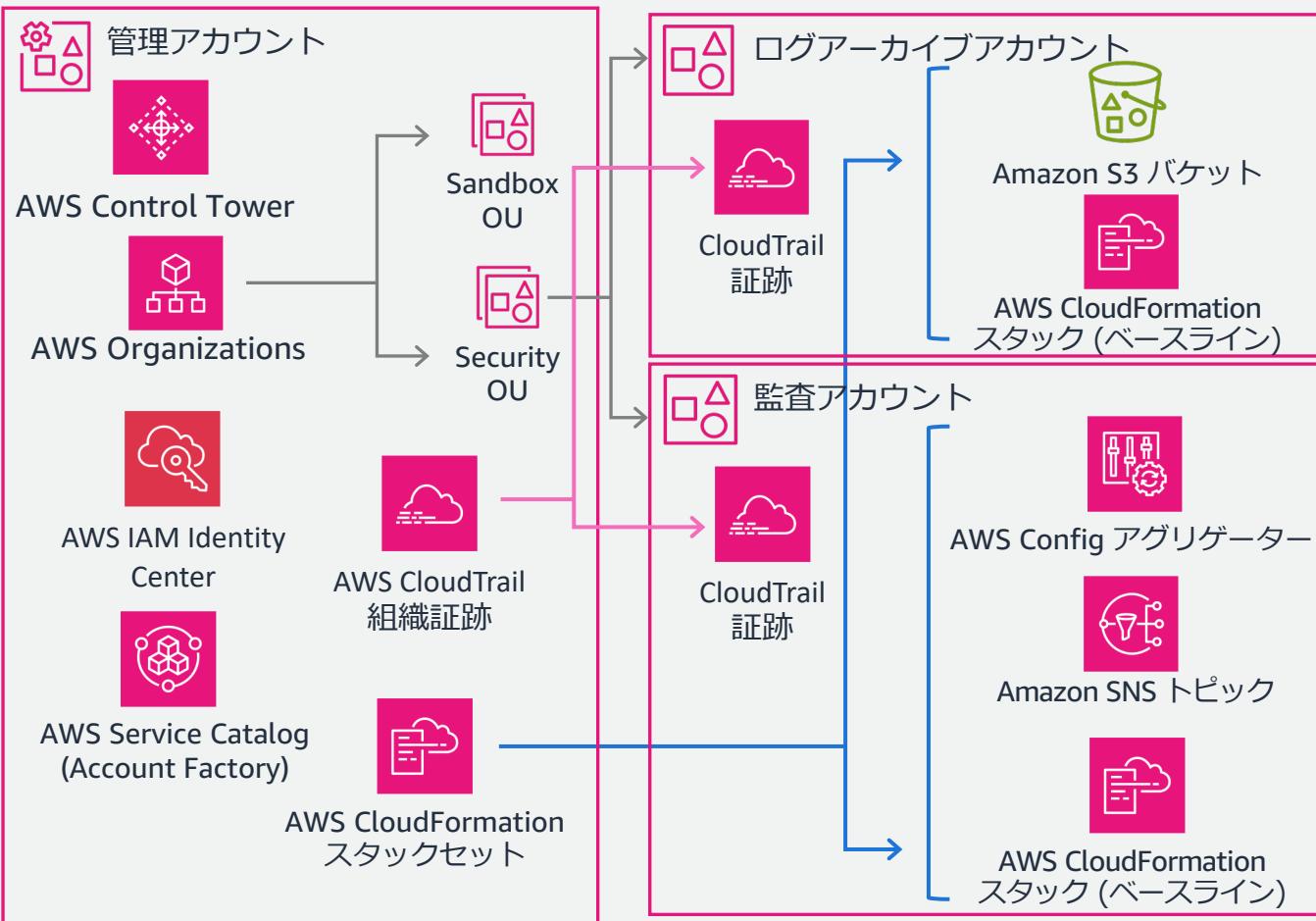
キャンセル

戻る

ランディングゾーンの設定

ステップ 5: セットアップの開始

5. 確認とセットアップ



ランディングゾーンのステータス

詳細	ステータス
セキュリティ OU で、監査とログ記録のための共有アカウントを作成または登録しています	成功
管理アカウント、監査アカウント、およびログ記録アカウントのすべてのユーザー権限を設定しています	成功
AWS Control Tower メンバーアカウントをプロビジョニングするため Account Factory を設定しています	成功
監査アカウントを設定しています	成功
ログアーカイブアカウントを設定しています	成功
組織ユニットで必須のコントロールを有効にする	進行中

セットアップ中、進捗状況を確認可能

⌚ ランディングゾーンの設定が完了しました。

[AWS Control Tower > ダッシュボード](#)

**コンソールで上記のように表示されると
セットアップ完了**

ランディングゾーンの セットアップ

1.3 よくあるエラーと修正方法
セットアップ時の留意点

セットアップ時の事前エラーと修正

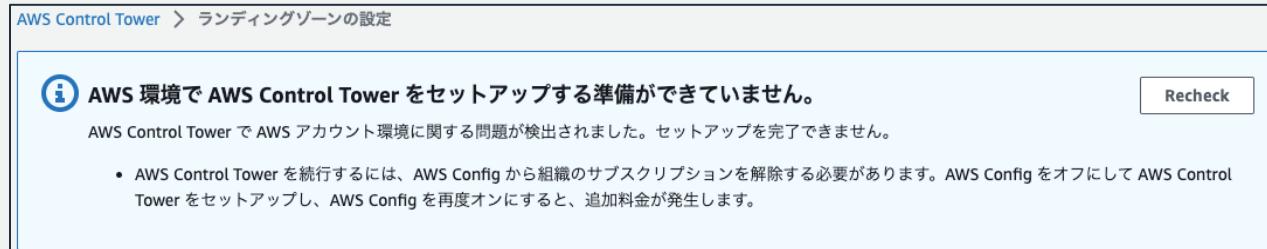
- AWS Control Tower のセットアップ時には事前チェックが実行される

https://docs.aws.amazon.com/ja_jp/controlltower/latest/userguide/getting-started-prereqs.html

- よくある事前エラーの例

1. AWS Config の信頼されたアクセスが有効

対処方法:
Organizations コンソールで
信頼されたアクセスを無効化する



セットアップの事前エラー例 1:
AWS Config の信頼されたアクセスが有効



対処方法:
Organizations コンソールで
信頼されたアクセスを無効化

セットアップ時の事前エラーと修正

- よくある事前エラーの例

2. IAM Identity Center と ホームリージョンが異なる

対処方法:

- ホームリージョンを同じリージョンに変更する
- IAM Identity Center 設定を削除する
ユーザー・グループ・許可セットなどすべてのデータが削除されてしまう

留意点:

- セルフマネージド IAM Identity Center 設定の場合も、同一リージョンでなければならない

AWS Control Tower > ランディングゾーンの設定

i AWS 環境で AWS Control Tower をセットアップする準備ができていません。

AWS Control Tower で AWS アカウント環境に関する問題が検出されました。セットアップを完了できません。

- 現在のアカウントでは、IAM Identity Center が異なるリージョンで設定されています。Identity Center を設定したのと同じホームリージョンで AWS Control Tower ランディングゾーンを設定してください。

Recheck

セットアップの事前エラー例 2:
既存の IAM Identity Center と異なるリージョンがホームリージョン

IAM アイデンティティセンターの設定を削除する		
削除されるデータについて	接続されているディレクトリ (AWS Managed Microsoft AD または AD Connector)	IAM アイデンティティセンター ID ストア
設定したすべての権限セット AWS アカウント	✓	✓
IAM アイデンティティセンターで設定したすべてのアプリケーション	✓	✓
AWS アカウント設定したすべてのユーザー割り当てとアプリケーション	✓	✓
ディレクトリまたはストア内のすべてのユーザーとグループ	該当なし	✓

https://docs.aws.amazon.com/ja_jp/singlesignon/latest/userguide/regions.html#delete-config

まとめ: ランディングゾーンのセットアップ時の留意点

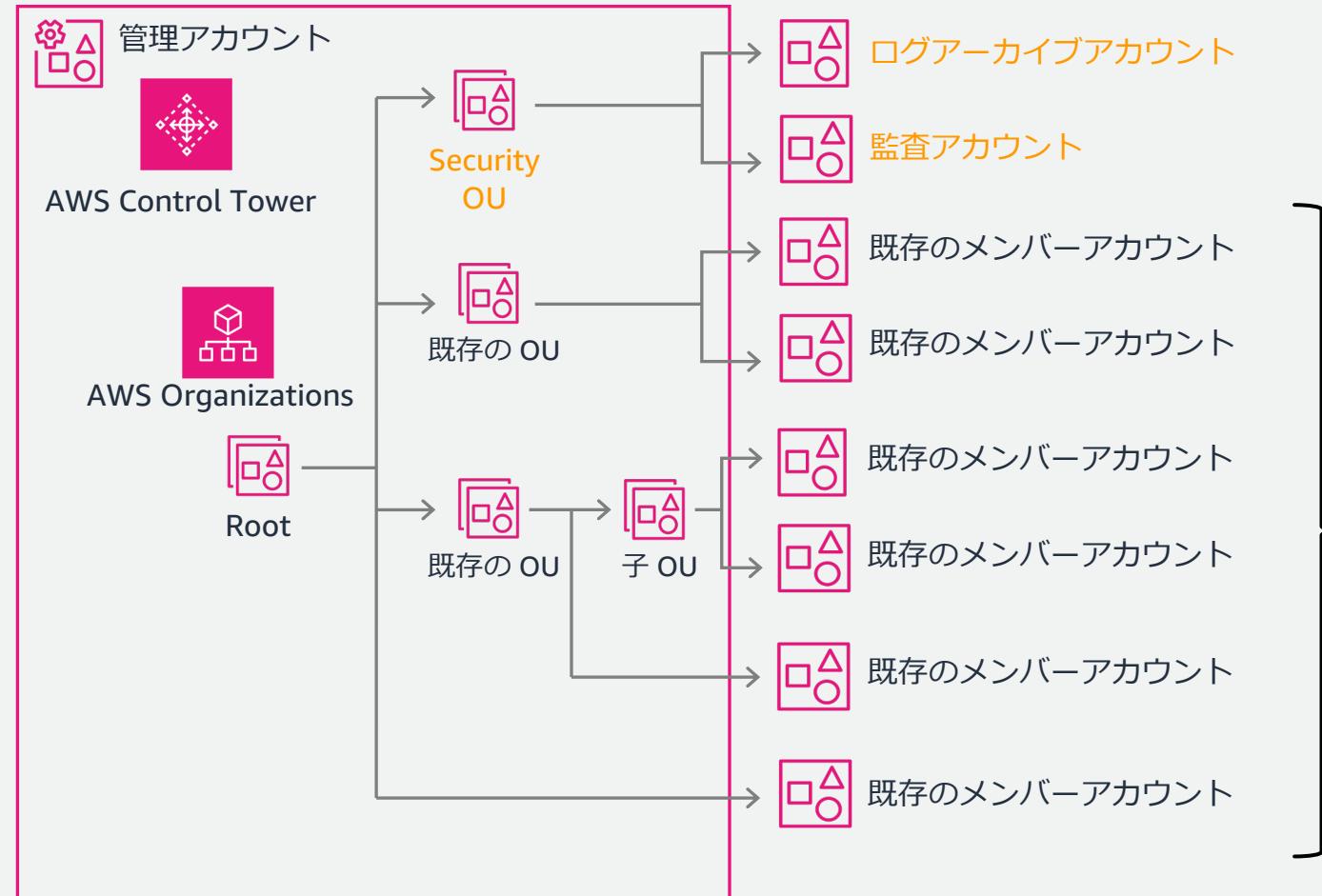
- 管理アカウント
 - 事前チェックなし: **セットアップ前の確認を推奨**
 1. 管理者権限を持つ IAM ユーザー・ロールでセットアップする
 2. Root にリソース作成を妨げる SCP を設定しない
 3. サポートするすべてのリージョンの AWS STS を有効化する
 4. (AWS KMS 暗号化キーを使用する場合)
キーポリシーに正しいアクセス許可があるか・対称な単一リージョンキーか
 - 事前チェックあり: エラー発生後に確認して対応
 1. AWS Config の信頼されたアクセスを無効化する
 2. ホームリージョンと AWS IAM Identity Center のリージョンは一致しているか etc.
- ログアーカイブ・監査アカウント (既存アカウントの場合): **セットアップ前の確認を推奨**
 1. AWS Config 設定レコーダーと配信チャネルは削除する
 2. サポートするすべてのリージョンの AWS STS を有効化する



メンバーアカウントの登録

メンバーアカウントの登録

- ・ランディングゾーンのセットアップだけでは、登録されない



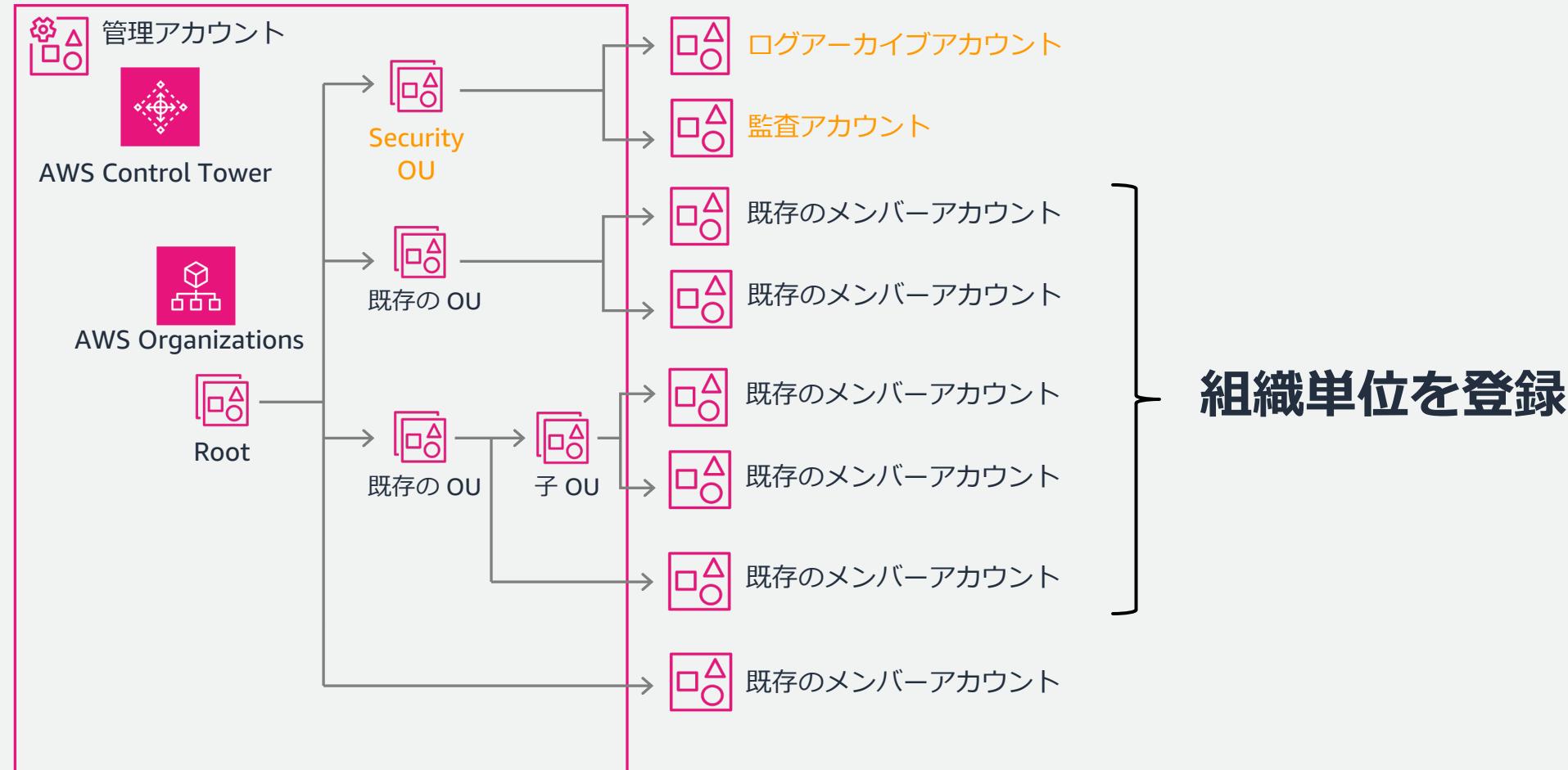
**別途 AWS Control Tower への
登録作業が必要となる**

メンバーアカウントの登録

1.1 組織単位とその直下の メンバーアカウントの登録手順

メンバーアカウントの登録

- 組織単位とその直下のメンバーアカウントの登録



組織単位の登録

組織単位と直下のメンバーアカウントをまとめて登録する

https://docs.aws.amazon.com/ja_jp/controlltower/latest/userguide/importing-existing.html

- 処理内容

1. AWSControlTowerExecution ロールをメンバーアカウントにデプロイする
2. 組織単位と各アカウントが登録前提条件を満たしているか事前チェックする
3. 1つでも事前チェックに失敗すると残りのメンバーアカウントの登録も中止する
4. 成功後、メンバーアカウントの登録を開始する (Account Factory をプロビジョニング)
 - ✓ ネストされた組織単位とそのメンバーアカウントは組織単位の登録後、さらに登録作業を実施する

名前	状態	ID	Eメール	登組	アカウント	登録	更新	管理を解除
Root	登録済み	Root の ID	-					
登録したい既存OU 1	未登録	OU の ID	-					
既存OU 2	未登録	OU の ID	-	0/0	0/0			
Security	登録済み	OU の ID	-	0/0	2/2			
既存OU 3	未登録	OU の ID	-	0/1	0/2			
管理アカウント	登録済み	アカウント ID	アカウントのメールアドレス	-	-	-	-	-

Control Tower コンソール -> [組織] での
[組織単位を登録]

組織単位への事前チェック

- 操作する IAM ユーザー・ロールが Account Factory のポートフォリオにあるか
- 所属するメンバーアカウント数が 300 を超える組織単位は登録できない
- 組織単位にアタッチできる SCP の上限数 (5 個) を超えていると登録できない
 - SCP を削除・結合するか、SCP の継承を使う
- 登録を妨げるSCP があるか

など

組織 情報		すべて展開	グループリソース	G	アクション ▾	リソースを作成 ▾
名前		状態	ID	E メール	登録済み組織単位	登録済みアカウント
●	□ Root	登録済み	Root の ID	-	△ 3 / 4	△ 6 / 7
○	□ 登録したい既存 OU 1	未登録、事前チェックに失敗しました	OU の ID	-	⊖ 0 / 0	⚠ 0 / 1
○	登録したい直下のメンバーアカウント	未登録	アカウント ID	アカウントのメールアドレス	-	-

事前チェック失敗時のエラー

AWS Control Tower > 組織 > 組織単位: 登録したい既存の OU 1

組織単位: 登録したい既存の OU 1

✖ 1つ以上の事前チェックに失敗したため、この組織単位を登録できませんでした。
失敗した事前チェックのリストをダウンロードし、詳細について [ドキュメント](#) を参照してから、リストされている項目を修正してください。その後、OU の登録を再試行してください。

事前チェックをダウンロード

コンソールから、事前チェックの失敗原因レポートを取得可能

組織単位への事前チェック

- 操作する IAM ユーザー・ロールが Account Factory のポートフォリオにあるか
- 所属するメンバーアカウント数が 300 を超える組織単位は登録できない
- 組織単位にアタッチできる SCP の上限数 (5 個) を超えていると登録できない
 - SCP を削除・結合するか、SCP の継承を使う
- 登録を妨げるSCP があるか

など

レポートでのエラー内容

- OU を登録する前に、IAM ユーザーを AWS Service Catalog ポートフォリオに追加します。
- AWS Control Tower は、登録時に各 OU のアカウント数を 300 個に制限します。
- OUあたりの SCP の制限を超えているか、別のクォータに達した可能性があります。AWS Control Tower のランディングゾーンの OU には、OUあたり 5 SCP の制限が適用されます。それ以上ある場合は、それらを削除する必要があります。
- この OU には、AWS Control Tower がアカウントを登録できない既存の SCP があります。AWS Control Tower SCP と競合するポリシーの SCP を確認してください。

メンバーアカウントへの事前チェック

- 1. 管理対象リージョンの AWS Config を無効化 (設定レコーダー・配信チャネルがない)しているか**
 - 後述のサポートケースでの申請によって有効化していても例外的に登録可能
- 2. サポートするすべてのリージョンの AWS STS を有効化しているか**
- 3. 停止 (Suspended) 状態のメンバーアカウントがあると登録できない**
 - 停止済みアカウント専用の未登録組織単位 (Suspended OU) を用意して移動する

<https://docs.aws.amazon.com/whitepapers/latest/organizing-your-aws-environment/suspended-ou.html>

など

レポートでのエラー内容

アカウントに既存の AWS Config 設定レコーダーがある場合があります。これらの設定レコーダーは、アカウントを登録する前に、AWS CLI を使用してすべてのリージョンで削除する必要があります。

1. アカウントに既存の AWS Config 配信チャネルがある場合があります。これらのチャネルは、アカウントを登録する前に、AWS CLI を使用してすべてのリージョンで削除する必要があります。

2. AWS STS は、アカウント内で無効にすることができます。AWS STS エンドポイントは、AWS Control Tower でサポートされているすべてのリージョンのアカウントでアクティブ化する必要があります。

3. このアカウントは停止されており、AWS Control Tower に登録できません。OU からこのアカウントを削除してください。

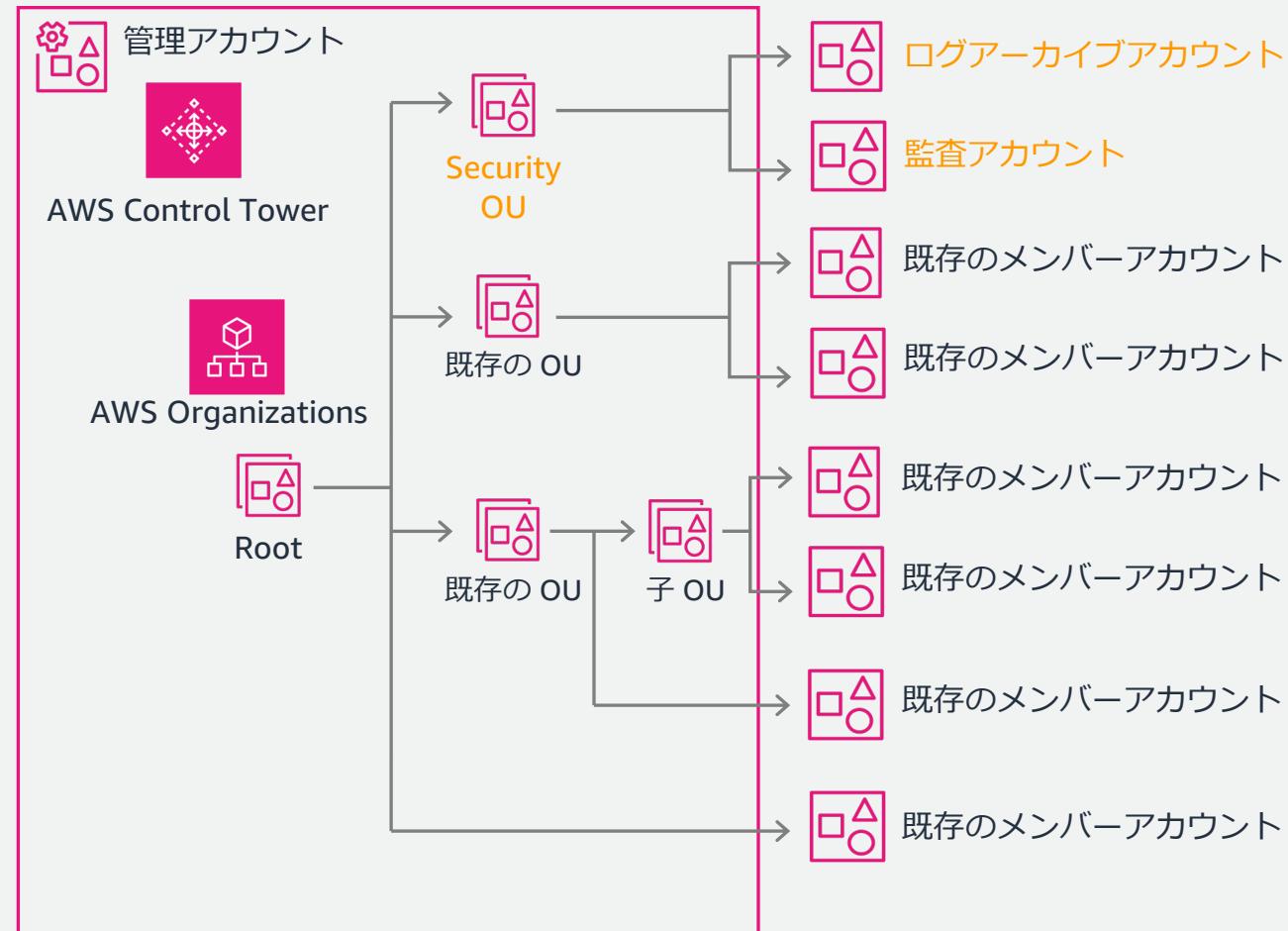


メンバーアカウントの登録

1.2 Root 直下の メンバーアカウントの登録手順

メンバーアカウントの登録

- Root 直下のメンバーアカウントの登録

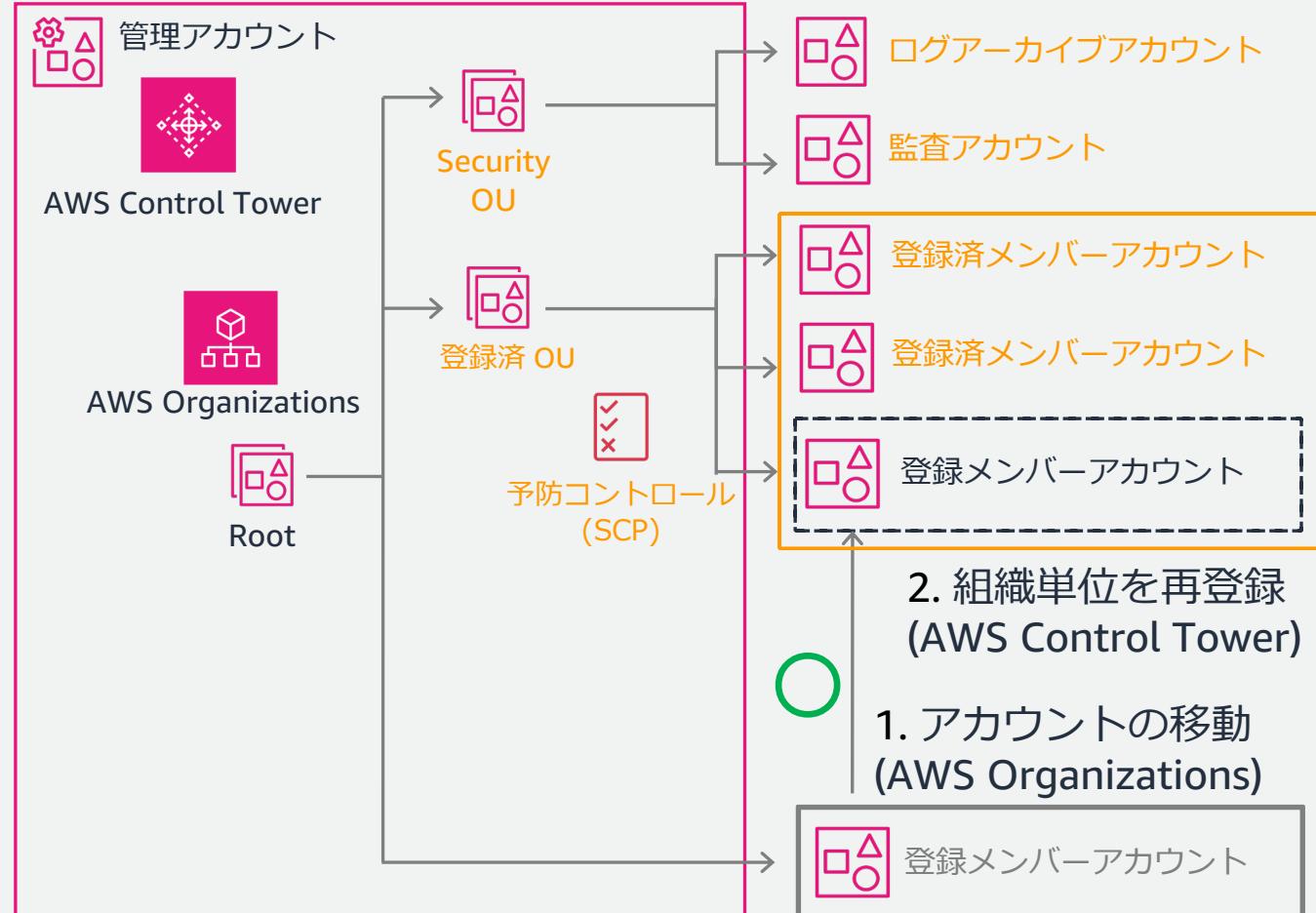


Root 直下のまま AWS Control Tower に登録はできない

1. 先に組織単位を移動して [組織単位を再登録] を実行 推奨
2. [アカウントの登録] を実行し Account Factory によって組織単位を移動

(推奨) 組織単位の再登録

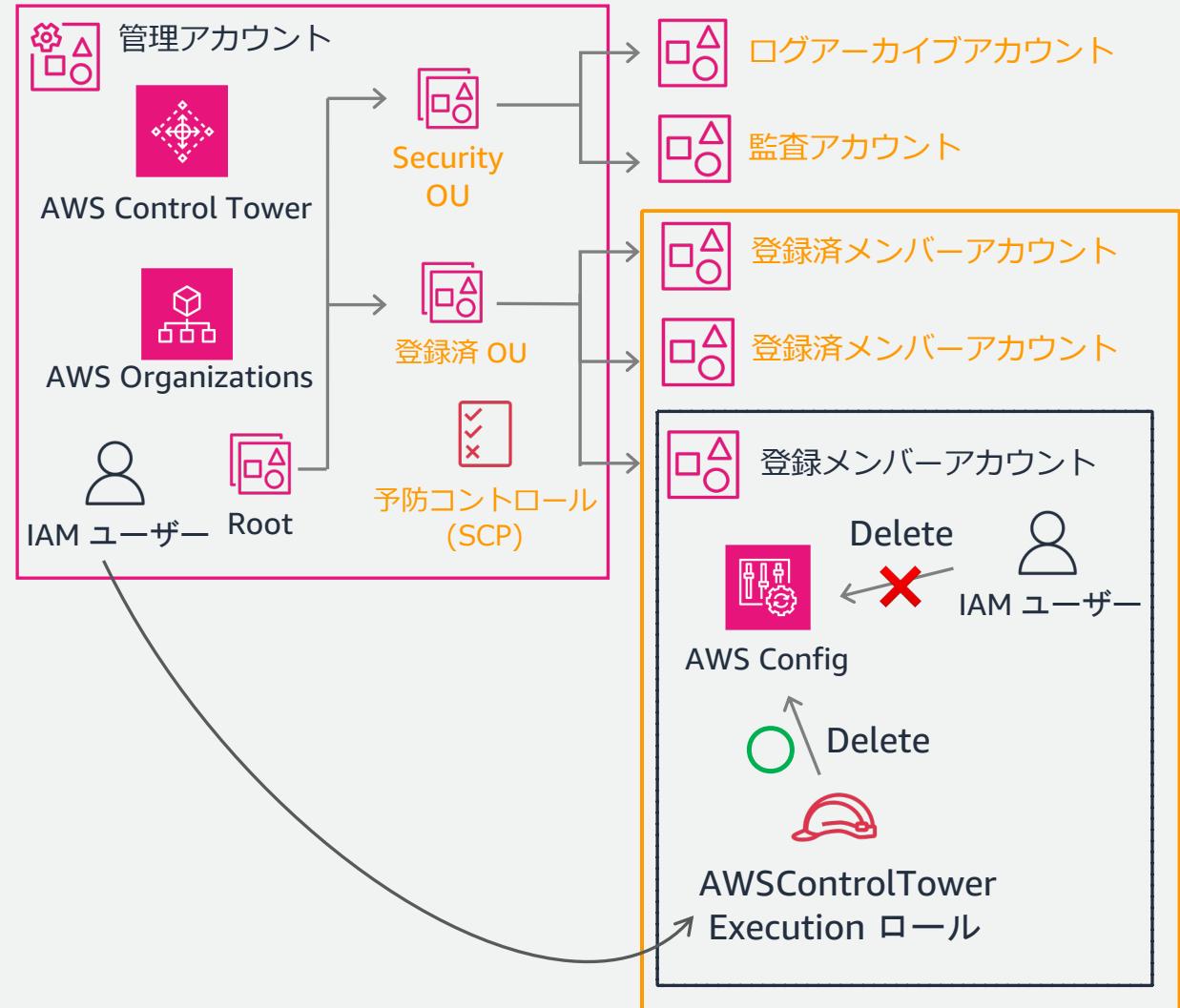
- ・ [組織単位を再登録] の実行で組織単位に追加した未登録のアカウントも登録可能
- ・ 処理内容は組織単位の登録と同様
 - AWSControlTowerExecution ロールのデプロイ
 - 前提条件を満たしているかの事前チェックを実行
- ・ 基本的に登録済のアカウントに影響はない
 - AWS Control Tower がデプロイしたリソースに変更を加えていない前提



(推奨) 組織単位の再登録

留意点

- 事前チェックの失敗を修正時
予防コントロールでアクセスが
拒否される場合がある
- 予防コントロールは
AWSControlTowerExecution の
アクセスを例外的に許可する
- 管理アカウントから
メンバーアカウントの
AWSControlTowerExecution に
AssumeRole して修正する



メンバーアカウントの登録

- アカウント単体の登録も可能
 - 登録時に移動する組織単位を選択する

https://docs.aws.amazon.com/ja_jp/controlltower/latest/userguide/importing-existing.html

制限事項

- 5 個のアカウントまで同時に登録作業可能

事前の実施事項

- メンバーアカウントに AWSControlTowerExecution ロールを手動で作成する
- 事前チェックを実施しないため、メンバーアカウントが登録前提条件を満たしているか利用者で確認する必要がある

The screenshot shows the AWS Control Tower Organization console. It lists several accounts under the '既存のアカウント' section. The columns include Name, Status, ID, Email, Registered Organization Units (OU), Registered Accounts, and Group Products. The 'Root' account is registered with 4 OUs and 6 accounts. Other accounts like '既存のOU1' and '既存のOU3' are also listed. A new account entry for '登録したい メンバーアカウント' is shown at the bottom.

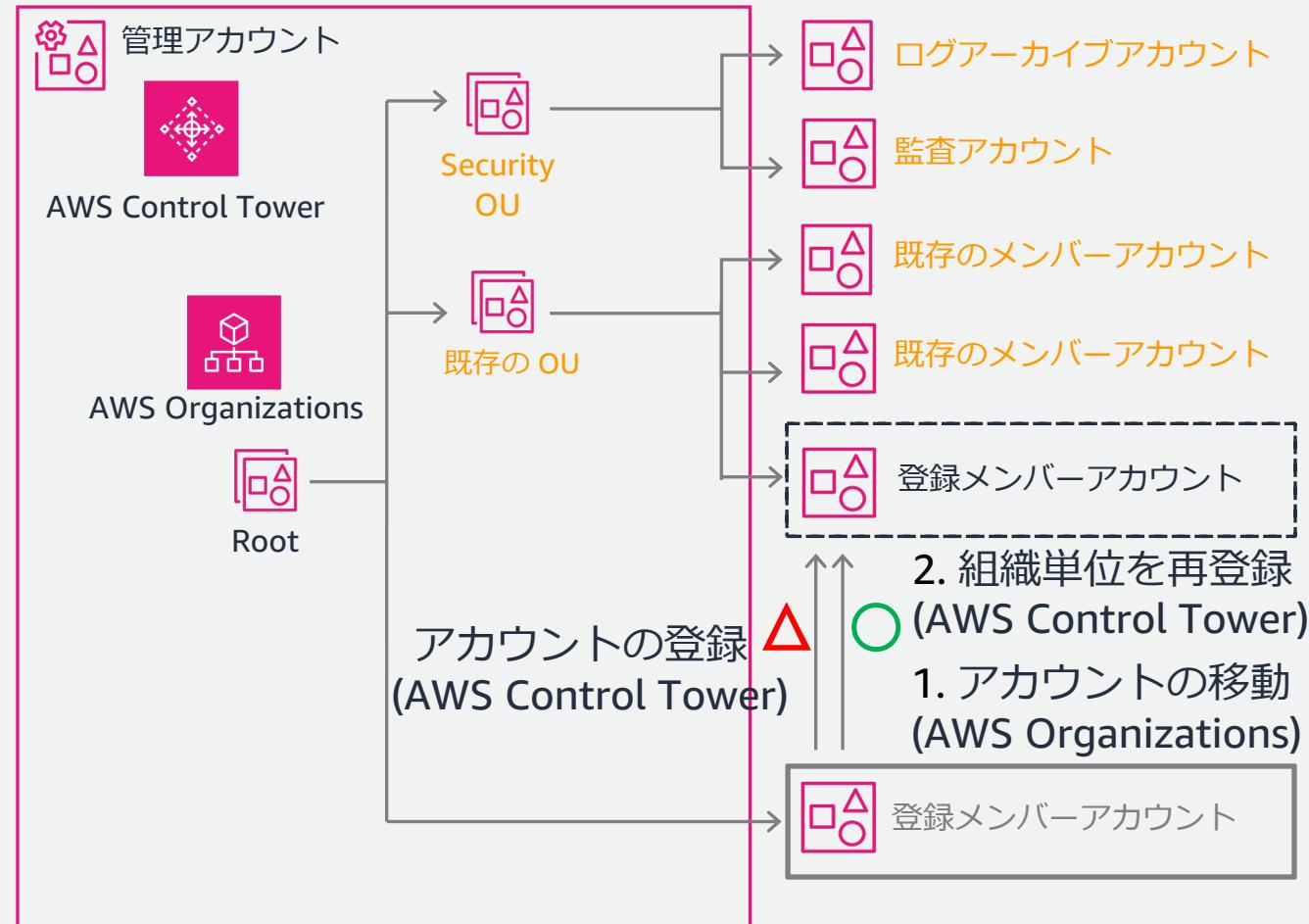
The screenshot shows the 'Account Registration' step in the AWS Control Tower wizard. It displays the 'Account Registration Settings' section with a note about projecting the account into AWS Control Tower. It also shows the 'Organization Unit' selection dropdown, which lists 'Registered Organization Units 1 (Level 1)', 'Registered Organization Units 2 (Level 1)', 'Nested Registered Organization Units (Level 2)', and 'Registered Organization Units 3 (Level 1)'. The 'Account Registration' button is at the bottom right.



組織単位の再登録を推奨する理由

[組織単位の再登録] の利点

- 複数のメンバーアカウント登録が簡単
 - 5つを超えるアカウント数でも順次登録可能
- アカウントの登録に比べて必要手順が簡潔
 - AWSControlTowerExecution ロールを自動で作成してくれる
- 登録可能性と必要な修正の確認が容易
 - 登録の前提条件を満たしているかの事前チェックが可能



メンバーアカウントの登録

1.3 AWS Config を有効化済みの
AWS アカウントの登録申請

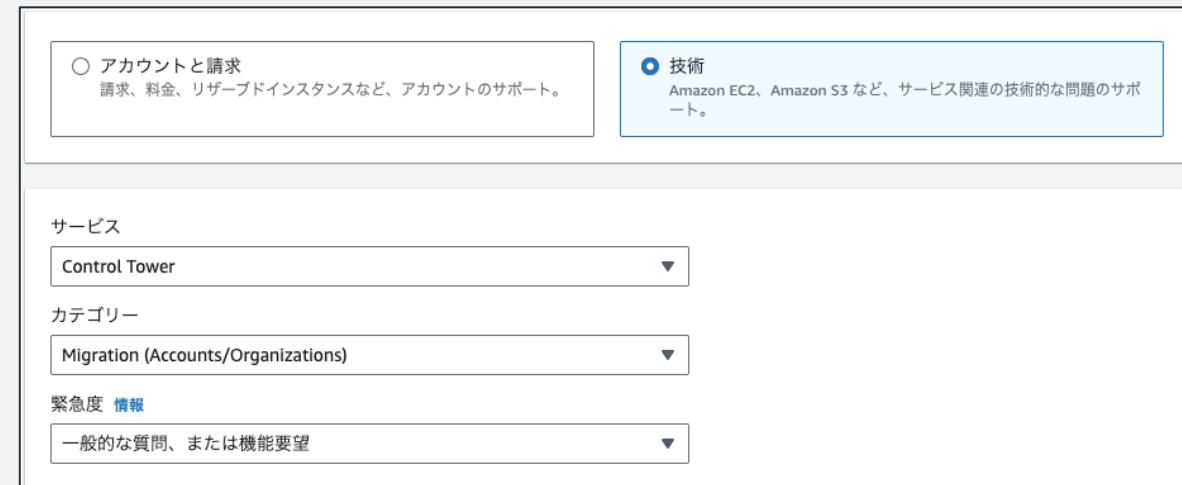
AWS Config が有効化済みのアカウントの登録申請

- 管理対象リージョンに AWS Config 設定レコーダー・配信チャネルがある

- 基本的には AWS Control Tower に登録できない
- サポートケースでの申請で例外的に登録できるよう許可リストに加えられる
- 管理アカウントからの 1 サポートケースで複数のメンバーアカウントについて申請可能
- 申請後、本来 AWS Control Tower が作成する AWS Config の設定と一致するよう変更してから組織単位の登録・再登録を行う

https://docs.aws.amazon.com/ja_jp/controlltower/latest/userguide/existing-config-resources.html

- 申請以外の作業を自動化した blog もご一読ください
<https://aws.amazon.com/jp/blogs/mt/automate-enrollment-of-accounts-with-existing-aws-config-resources-into-aws-control-tower/>
- (注意点) AWS Control Tower は AWS Config リソースを管理・更新・修復しない



The screenshot shows the AWS Support case creation interface. It includes fields for 'Category' (set to 'Migration (Accounts/Organizations)'), 'Service' (set to 'Control Tower'), and 'Priority' (set to 'Information'). There are also tabs for 'Case creation' and 'Case history'.

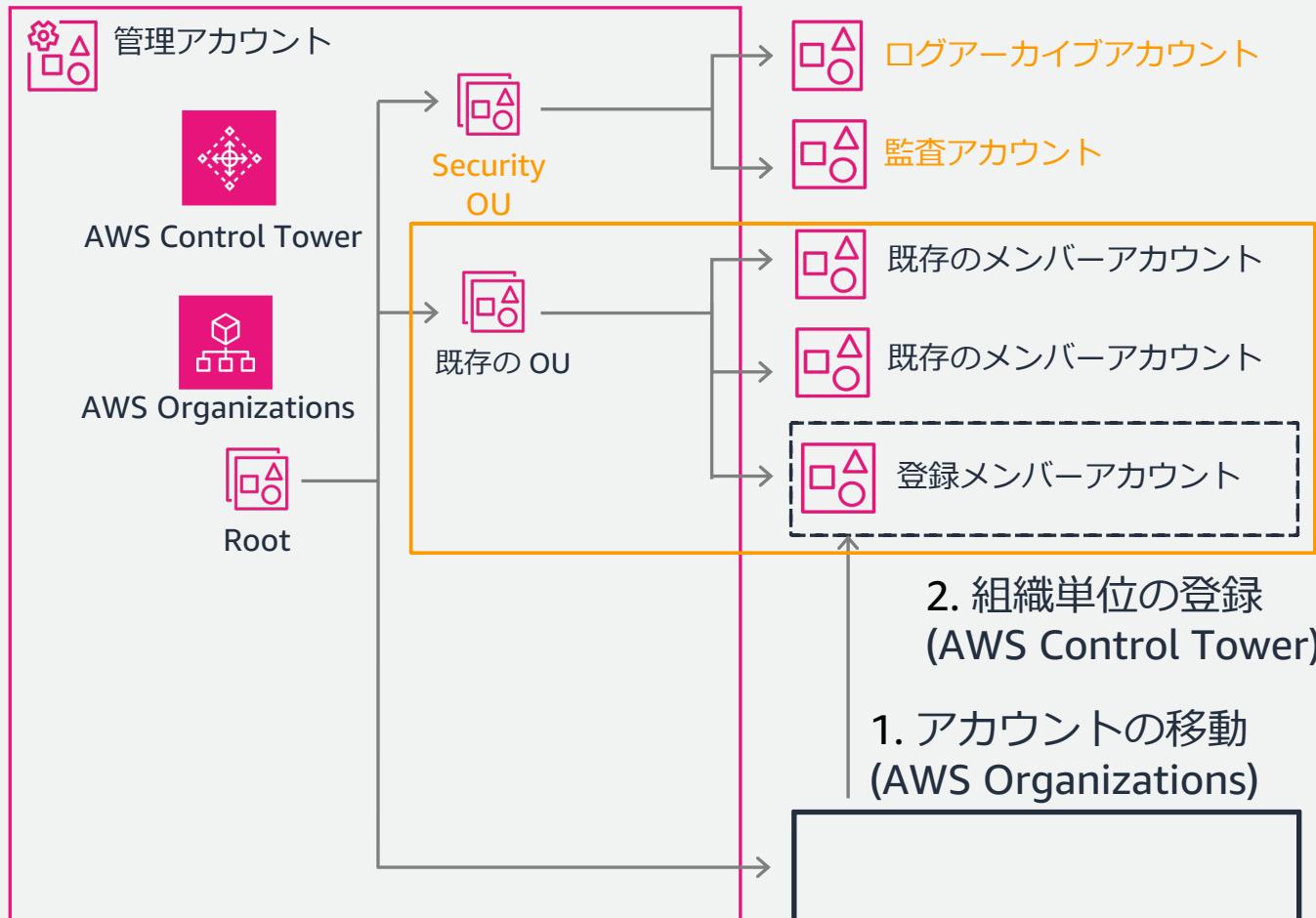
- ケースの作成時
技術
サービス: Control Tower
カテゴリ: Migration (Account/Organization)
- ケースの件名
既存の AWS Config リソースを持つアカウントを AWS Control Tower に登録する
- ケースの本文に記載する内容
管理アカウントの ID (12 桁の数字)
AWS Config リソースを持つメンバーアカウント ID
AWS Control Tower のホームリージョン

メンバーアカウントの登録

1.4 登録手順のまとめ

まとめ: 既存の組織単位・メンバーアカウントの登録手順

1. Root 直下のアカウントは登録したい組織単位へ移動する
2. 組織単位の登録を実行
3. 事前チェックに失敗した場合:
 1. レポートをダウンロードして対処方法を確認
 2. AWS Config 有効化済みによるエラー:
 - AWS Control Tower で設定レコーダー配信チャネルを作成・管理する場合:**AWSControlTowerExecution** ロールで **AWS Config** リソースを削除
 - 既存の設定レコーダー・配信チャネルを用いて利用者で管理する場合:**サポートケースで申請**
4. 事前チェックのエラーへの対処後組織単位の登録を再度実行





Thank you!

Appendix

- 参考となる公式ドキュメント
 - Control Tower がサポートするリージョン
https://docs.aws.amazon.com/ja_jp/controlltower/latest/userguide/region-how.html
 - ランディングゾーンのセットアップ前の自動チェック
https://docs.aws.amazon.com/ja_jp/controlltower/latest/userguide/getting-started-prereqs.html
 - AWS KMS キーに設定するキーポリシー
https://docs.aws.amazon.com/ja_jp/controlltower/latest/userguide/configure-kms-keys.html
 - 組織単位の登録・再登録時の事前チェックとよくあるエラー原因
https://docs.aws.amazon.com/ja_jp/controlltower/latest/userguide/common-eg-failures.html

Appendix

- AWS Config 設定レコーダー・配信チャネルの削除
 - AWS CLI でのみ削除可能

https://docs.aws.amazon.com/ja_jp/controlltower/latest/userguide/using-aws-with-cloudshell.html

- リソースのステータスを確認 (リソース名をメモしてください)

```
$ aws configservice describe-delivery-channels  
$ aws configservice describe-delivery-channel-status  
$ aws configservice describe-configuration-recorders
```

- 設定レコーダーを停止

```
$ aws configservice stop-configuration-recorder --configuration-recorder-name <NAME-FROM-DESCRIBE-OUTPUT>
```

- 配信チャネルと設定レコーダーを削除

```
$ aws configservice delete-delivery-channel --delivery-channel-name <NAME-FROM-DESCRIBE-OUTPUT>  
$ aws configservice delete-configuration-recorder --configuration-recorder-name <NAME-FROM-DESCRIBE-OUTPUT>
```



AWS Application Discovery Service の概要 (AWS 移行準備シリーズ)

鈴木 槟将

Solutions Architect

2023/10

自己紹介

名前：鈴木 槟将 (Suzuki Shinsuke)

所属：パートナーアライアンス統括本部

パートナーコアテクノロジー部

マイグレーションパートナー ソリューションアーキテクト

経歴：SIerにてサーバ、データ、ネットワーク基盤

の移行・開発・運用保守

好きなAWSサービス：AWS MGN, AWS CloudFormation



本セミナーの対象者と目的

対象者

- ・ オンプレミスからクラウド移行を企画・検討している方
- ・ 移行プランの策定をこれから行う方
- ・ IT 資産の棚卸しを検討している方
- ・ 特に、上記に取り組まれる PM 、アーキテクトの方

目的

- ・ AWS Application Discovery Service (**AWS ADS**) について、
 - ・ どのようなことができるサービスなのか知っていただく
 - ・ どのような仕組みで、どのような情報を収集しているのかを知っていただく

アジェンダ

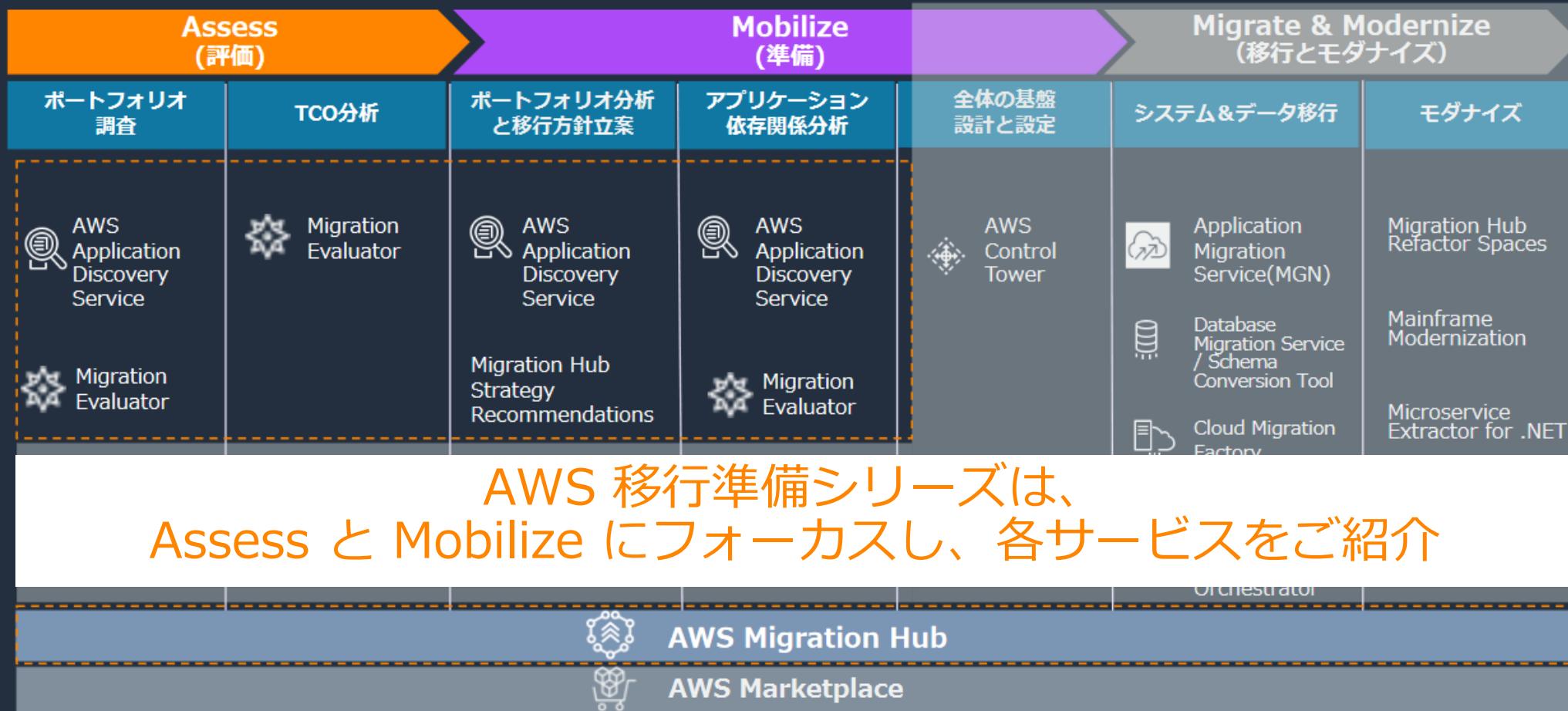
1. はじめに
2. ポートフォリオ調査の必要性
3. AWS ADS サービス概要
4. AWS ADS の情報収集の仕組み
5. まとめ

はじめに



AWS 移行準備シリーズについて (1/2)

クラウド移行に関する AWS Service と AWS Marketplace



AWS 移行準備シリーズについて (2/2)



AWS Application Discovery Service



Migration Evaluator



AWS Migration Hub



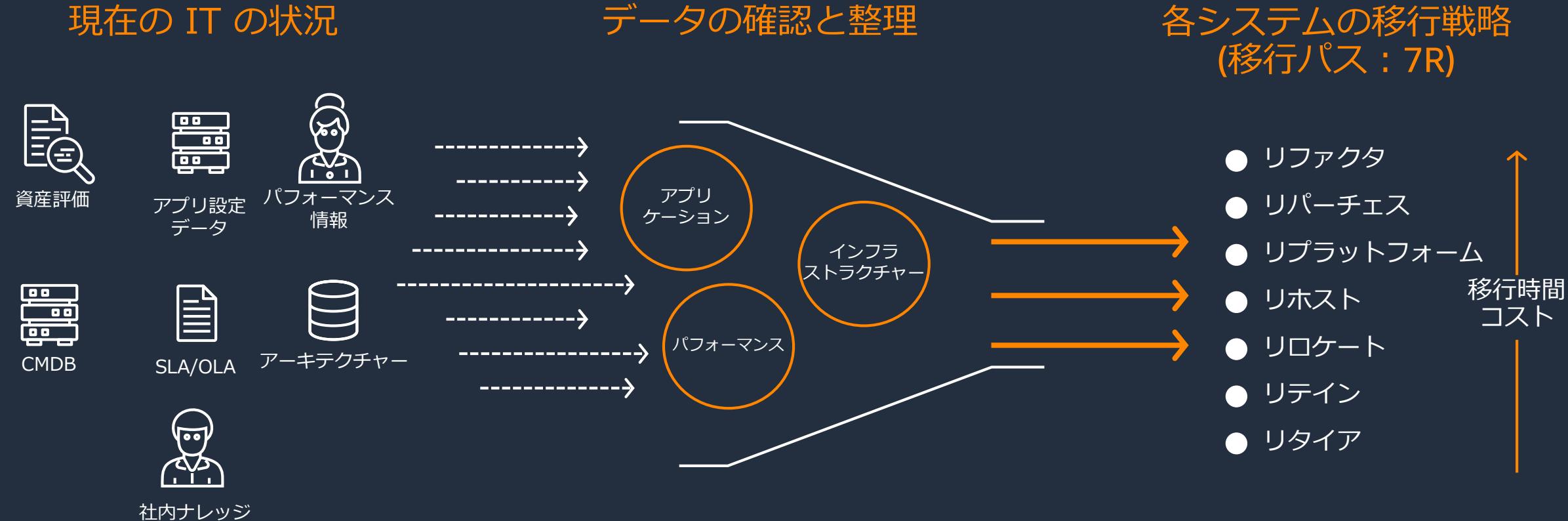
本セミナーは
「クラウド移行における Discovery ツールの必要性」 の続編の位置づけ

3 つの代表的なディスカバリサービスの内、

AWS ADS (および AWS Migration Hub の一部機能)
について解説

ポートフォリオ調査の必要性

クラウド移行の進め方

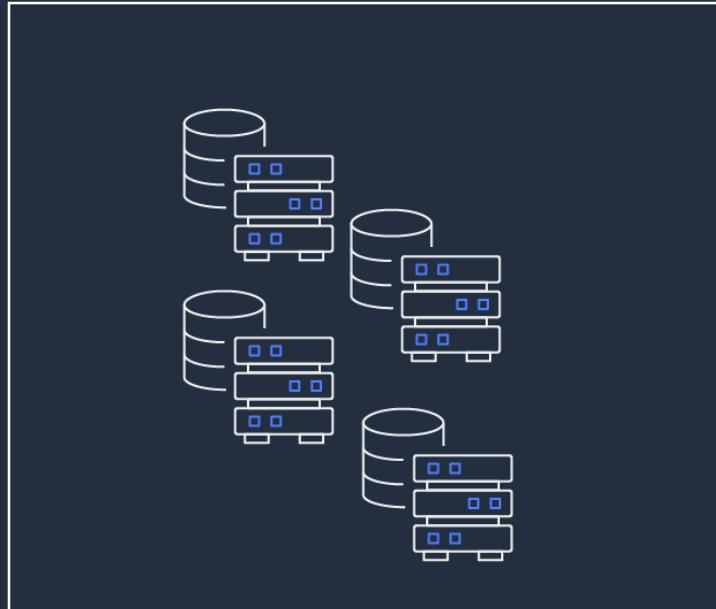


移行パス（7R）

移行パスの名称	概要	例
リファクタ (Refactor)	アーキテクチャーを再設計し、クラウドネイティブに置き換え	Lambda や Amazon Elastic Container Service 等のサーバーレスを取り入れたクラウド最適化
リパーチエス (Repurchase)	アプリケーションの買い替え	SaaS やパッケージの適用
リプラットフォーム (Replatform)	OS やミドルウェアを変更/アップグレードして移行	OS やミドルウェアのバージョンアップ、Amazon Relational Database Service の採用、メインフレームや商用 Unix からの移行
リホスト (Rehost)	OS やアプリケーションをそのまま移行	3 層 Web アプリであれば Amazon Elastic Compute Cloud で 3 層を構築するなど、既存オンプレミスのアーキテクチャそのままを AWS に移行
リロケート (Relocate)	Vmware 環境をそのまま移行	VMware Cloud on AWS を用いて、既存オンプレミスのアーキテクチャそのままを AWS に移行
リテイン (Retain)	現行の環境で引き続き運用	クラウド移行せず残置
リタイア (Retire)	サーバやアプリケーションを停止/廃止	システムの統廃合による廃止

ポートフォリオ調査とは

複数のシステムを調査し、インベントリ全体を可視化し、パフォーマンス情報などのシステム関連の情報を取得すること



複数システム
(ポートフォリオ)



調査

- ✓ インベントリの全体像の把握
(サーバ台数, H/W 情報)
- ✓ パフォーマンス情報の調査
(平均およびピーク)
- ✓ システム間の依存関係の把握

ポートフォリオ調査の必要性とは

- データに基づいた意思決定
- コスト試算が可能になり、ビジネスケースへの反映
- 大規模、またはクリティカルなシステムのロードマップの策定
- 移行計画のフィージビリティ（実現可能性）の確認

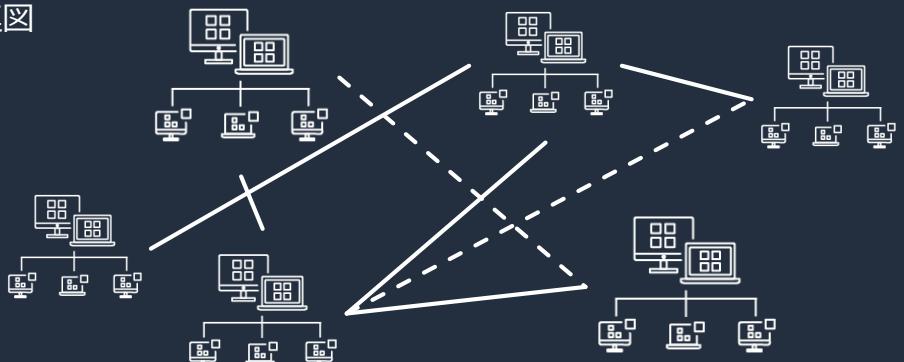
ポートフォリオ調査の課題

■インベントリ台帳

No	集約サーバー名	台数	プロセッサー数 ／サーバー	コア数 ／プロセッサ	メモリ容量 (GB)	ピーク時の CPU使用率	ピーク時の メモリ使用率	(仮想サーバ台帳)	
1	No	ストレージ名	ストレージタイプ	容量区分	ストレージ容量 (TB)	ストレージ利用率 (%)	OS	(Win) HDDの割合(%) (Linux)低頻度アクセスの割合(%)	(ストレージ台帳)
2	No	サーバー名	サーバー名称	集約 サーバー	システム名称 (略称)	環境区分	サーバーの稼 働率 (%)	サーバー種別	(システム台帳)
1	J01-DB01	統合DBサーバー	-	統合DB	Production(本番)	100	DB Server (OLTP & OLAP)		
2	J01-SCMAP1	SCM APサーバー	-	SCMシステム	Production(本番)	65	AP Server (Online)		
3	J01-DB01	統合DBサーバー	-	統合DB	Development(開発)	30	DB Server (OLTP & OLAP)		
4	J01-SCMAP1	SCM APサーバー	-	SCMシステム	Development(開発)				
5	J01-DB01	統合DBサーバー	-	統合DB	Staging(準備番)	10	DB Server (OLTP & OLAP)		
6	J01-SCMAP1	SCM APサーバー	-	SCMシステム	Staging(準備番)				

※赤フォント：正確ではない台帳情報

■システム関連図



台帳の把握

- 台帳の存在有無
- 複数の台帳の整合性
- 台帳の正確性や充足性
- 移行に適合した項目有無

パフォーマンスの把握

- CPU 使用率
- メモリ使用率
- ストレージ性能 (スループット等)

システム間の依存関係

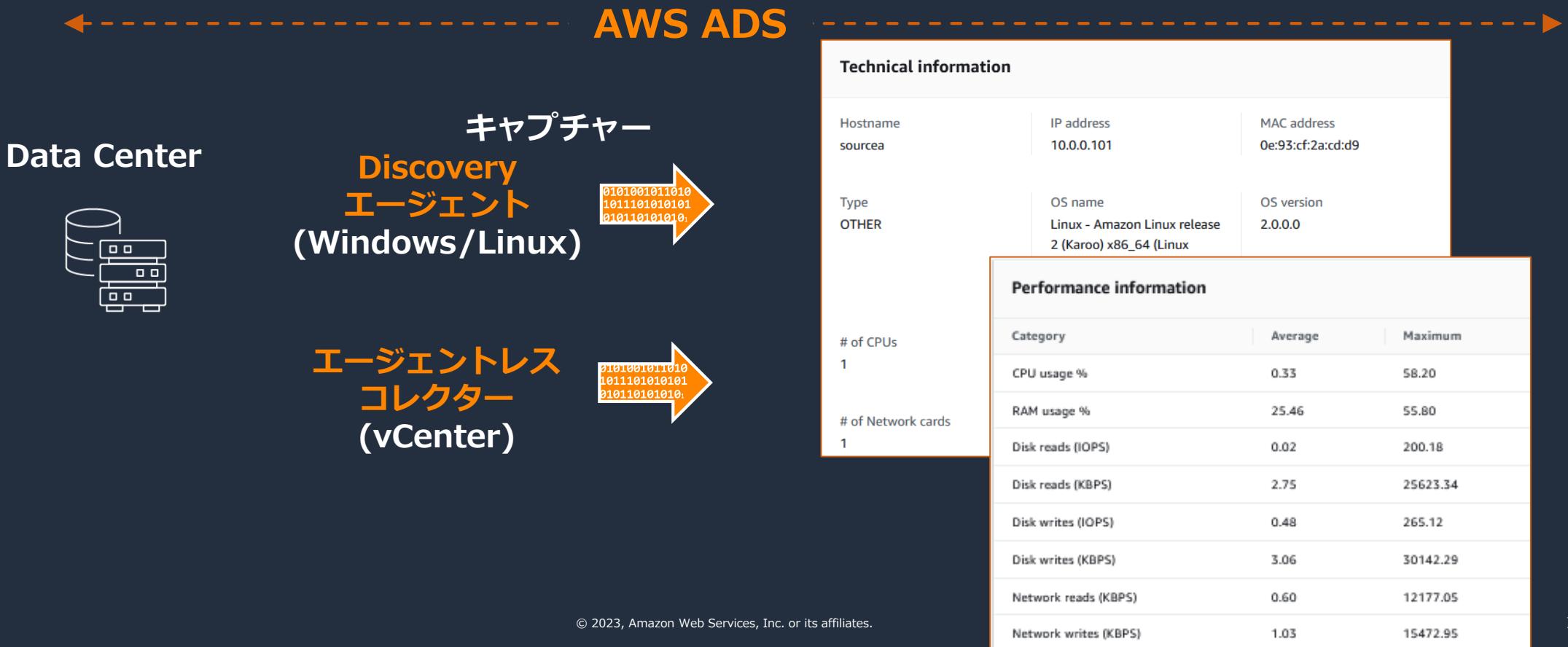
- ネットワーク通信の状況
- 正確なシステム関連図
- 対象システムの充足性

AWS ADS サービス概要

AWS Application Discovery Service (AWS ADS)

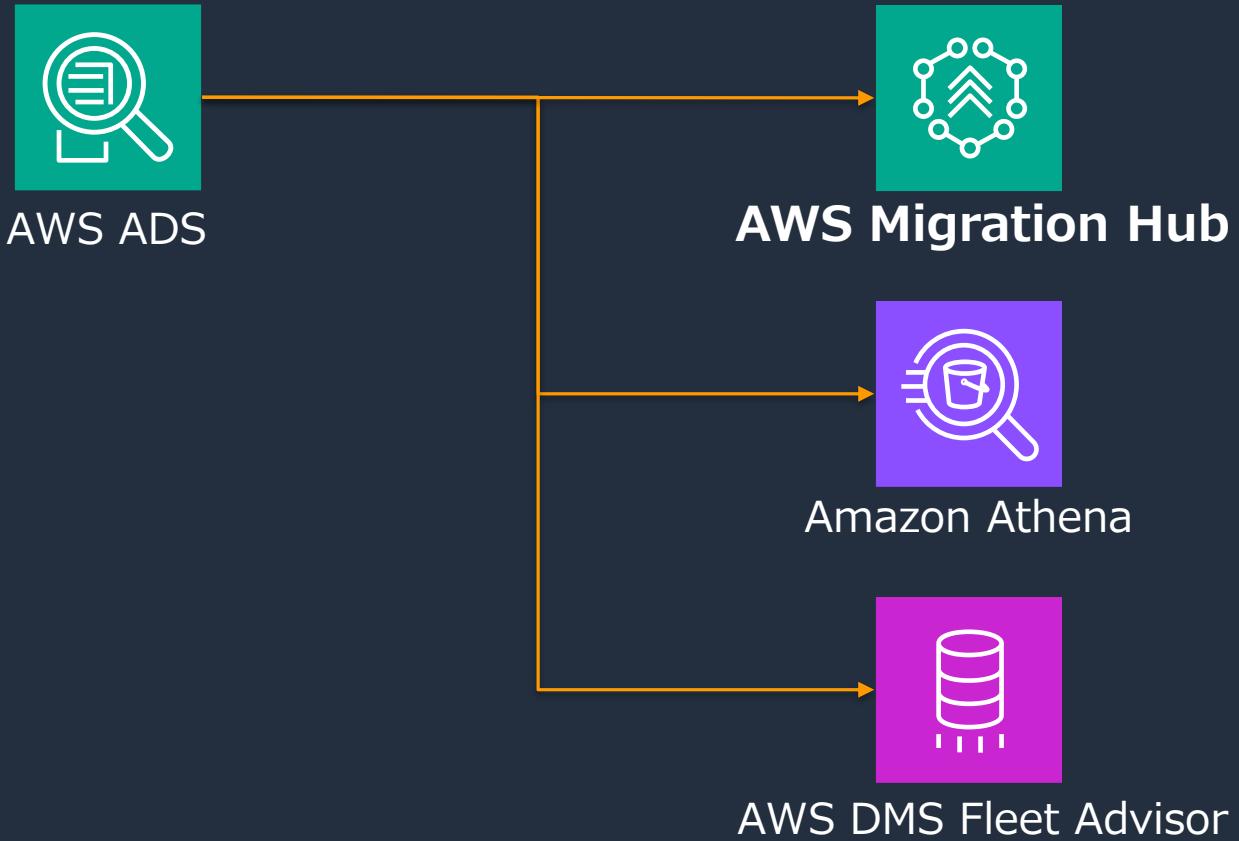
インベントリ、パフォーマンス、依存関係をキャプチャ

- エージェントまたはエージェントレスの仕組みを用いて、自動で情報をキャプチャ
- 利用料は無料



AWS ADS と連携するサービス

AWS ADS は他サービスと連携することで、収集した情報の確認や情報を用いた分析を実施することが可能

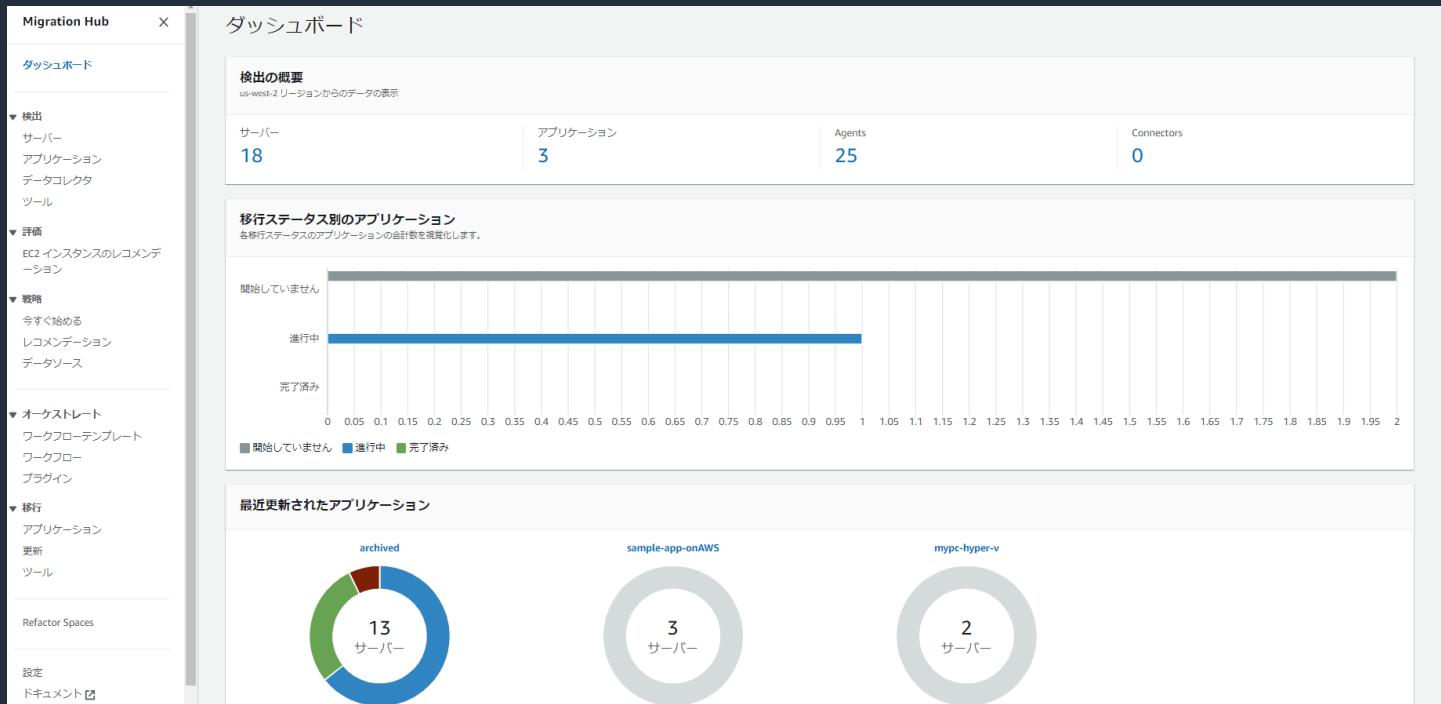


- ・ 収集した情報の参照・分析
 - ・ 推奨 EC2 インスタンスの取得
 - ・ 情報収集の停止・再開
 - ・ 収集した情報のエクスポート
-
- ・ Amazon Athena でのデータ探索を有効にし、クエリを用いた分析が可能
 - ・ Amazon QuickSight と統合して、クエリ出力を視覚化
-
- ・ データベースサーバのインベントリ情報を評価し、潜在的な推奨移行パスを取得
 - ・ エージェントレスのみが連携可能

AWS Migration Hub とは

移行のスピードを損なうことなく、移行アクティビティに関わる情報の集約・追跡を可能とするサービス

- ・ シンプルで直感的な、クロスリージョン対応の移行ダッシュボードの提供
- ・ 複数の移行ツールと統合され、収集した情報の集約、移行状況の追跡が容易に可能



AWS ADS によって収集されるサーバ情報

AWS ADS が収集したシステム設定、使用率、パフォーマンス情報を AWS Migration Hub から参照することが可能

【システム設定情報】

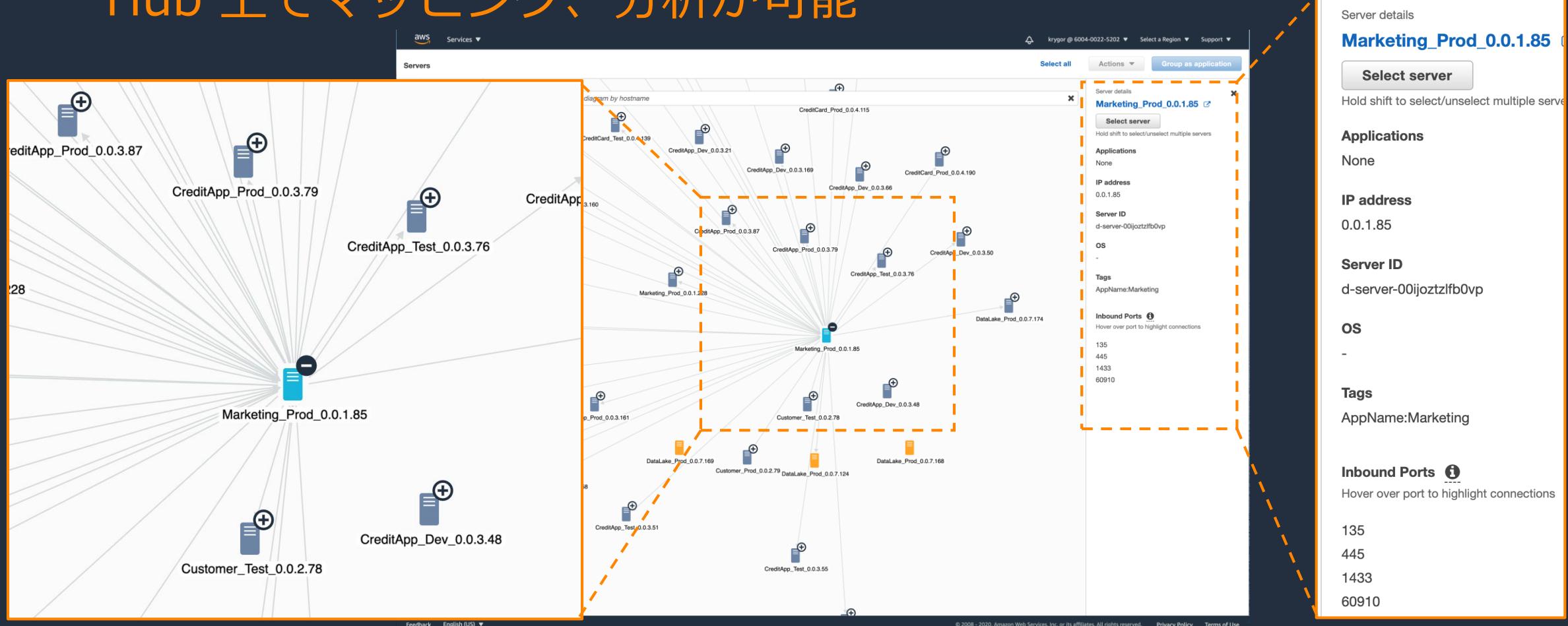
Technical information			
Hostname sourcea	IP address 10.0.0.101	MAC address 0e:93:cf:2a:cd:d9	Server ID d-server-03r8zi8eijjkss
Type OTHER	OS name Linux - Amazon Linux release 2 (Karoo) x86_64 (Linux 4.14.268-205.500.amzn2.x8 6_64)	OS version 2.0.0.0	Hypervisor xen
# of CPUs 1	CPU type x86_64	# of Cores 1	# of Disks 1
# of Network cards 1	Free disk size (MB) 5324.71	Total disk size (MB) 8192.00	Total RAM (MB) 1024.00
VM name -	VMware moref ID -	Manufacturer -	VMware guest tools status -
VMware vCenter ID -	VMware host system ID -	Data center ID -	VM folder path -

【使用率、パフォーマンス情報】

Performance information			
Category	Average	Maximum	Minimum
CPU usage %	0.33	58.20	-
RAM usage %	25.46	55.80	-
Disk reads (IOPS)	0.02	200.18	-
Disk reads (KBPS)	2.75	25623.34	-
Disk writes (IOPS)	0.48	265.12	-
Disk writes (KBPS)	3.06	30142.29	-
Network reads (KBPS)	0.60	12177.05	-
Network writes (KBPS)	1.03	15472.95	-
Free RAM (MB)	763.31	-	452.56

AWS ADS によって収集されるネットワーク接続情報

AWS ADS が収集したネットワーク接続情報を AWS Migration Hub 上でマッピング、分析が可能



AWS ADS の情報を基にした推奨 EC2 インスタンスの取得

AWS ADS の収集情報を活用し、 AWS Migration Hub がワークロードの実行に必要かつ最も安価な推奨インスタンスタイプを提案

- ・ サーバーの仕様、CPU、メモリ使用率など、収集されたデータを分析
- ・ CPU/RAM 使用率のメトリクス（平均、ピーク、パーセンタイル）
インスタンス購入オプション、リージョン、推奨しないインスタンスタイプなどが指定可能

EC2インスタンス推奨のアウトプット例(.csv)

Server.HostName	Server.OS.Name	Server.CPU. NumberOfCores	Recommendation. EC2.RequestedCPU. UsagePct	Recommendation.EC2. RequestedRAMinMB	Recommendation. EC2.Instance.Model	...
server1	Linux - Ubuntu 20.04.3 LTS x86_64	1	100	1024.458752	t3a.micro	...
server2	Linux - Ubuntu 18.04.3 LTS x86_64	1	84.5129	1024.458752	t3a.micro	...
server3	Linux - Ubuntu 18.04.3 LTS x86_64	2	30.2645	2048.917504	t3a.small	...
...

推奨された
EC2 インスタンスタイプ

AWS ADS による情報収集の制御（停止・再開）

AWS Migration Hub 上で各情報収集手段ごとに、収集状況などの情報を確認しつつ、データ収集の停止・再開の制御が可能

The screenshot shows the AWS Migration Hub Data collectors interface. The navigation path is Migration Hub > Data collectors > Discovery agents. The main title is Data collectors. Below it is a navigation bar with tabs: Agentless collectors, Discovery connectors, **Discovery agents**, and Migration Evaluator collector. The Discovery agents tab is selected. A secondary navigation bar above the table lists: データ収集手段の選択 (Agentless collectors, Discovery connectors, Discovery agents, Migration Evaluator collector), データ収集の制御 (Start data collection, Stop data collection). The main content area displays a table of discovery agents with columns: Agent ID, Hostname, Collection status, and Health. Three entries are listed:

Agent ID	Hostname	Collection status	Health
o-307ntfxuweu3ev6ze	target-ec2-demo-20...	Collecting	Shutdown
o-3j1ydy86so7ehdyn	target-ec2-demo-20...	Stop scheduled	Shutdown
o-261zs1c5mvqwcu5et	target-ec2-demo-20...	Collecting	Shutdown

AWS ADS によって収集された情報のエクスポート

各サーバごとに、 AWS Migration Hub 上で収集したデータをファイル（ CSV ）形式でエクスポートすることが可能

- ・ 特定のサーバに関する詳細ページ（の下部）から実行可能
- ・ 収集したデータが含まれる CSV ファイルと、エクスポートタスクの結果を示す JSON ファイルを取得可能

Exports

Last updated: 9/5/2023 5:00 PM

If you would like to see detailed discovery data for multiple servers, consider [Data Exploration in Amazon Athena](#).

Export ID	From date / time	To date / time
export-c5a7278e-ccfd-... (selected)	Jul 25, 9:00 AM	...
export-4b3c6ef1-1fc3-...	Aug 28, 9:00 AM	...

名前

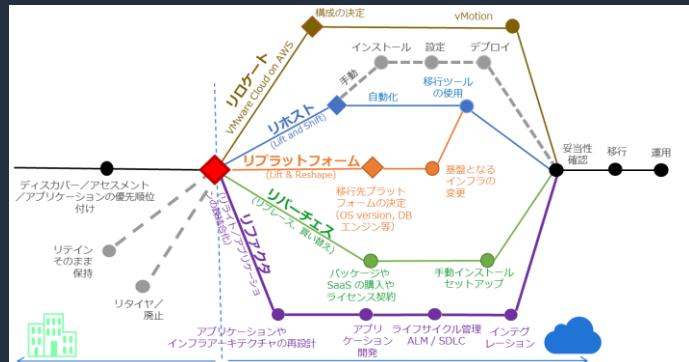
- 000000000000_networkInterface.csv
- 000000000000_osInfo.csv
- 000000000000_process.csv
- 000000000000_sourceProcessConnection.csv
- 000000000000_systemPerformance.csv
- results.json

(参考) AWS Migration Hub のその他機能

移行作業状況の追跡以外にも、多様な機能が AWS Migration Hub には搭載されており、移行作業に利用することが可能

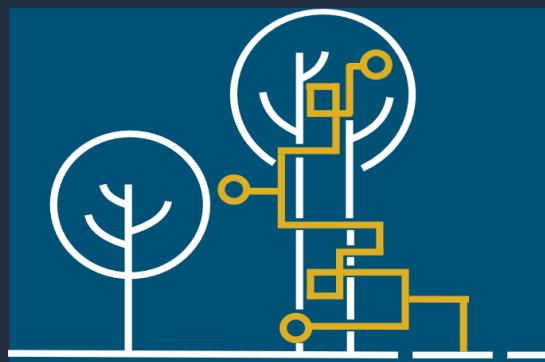
AWS Migration Hub Strategy Recommendations

アプリケーションを分析して、大規模の移行や最新化を最適に行うための戦略（7R）を推奨



AWS Migration Hub Refactor Spaces

マイクロサービスを意図した Strangler Fig パターンによる、リファクタリングを加速



AWS Migration Hub Orchestrator

特定の移行パターンに対して、移行ワークフローテンプレートを用いた移行プロセスの自動化／簡素化

The screenshot shows the "Workflow templates (1/2)" section of the AWS Migration Hub Orchestrator interface. It displays two templates:

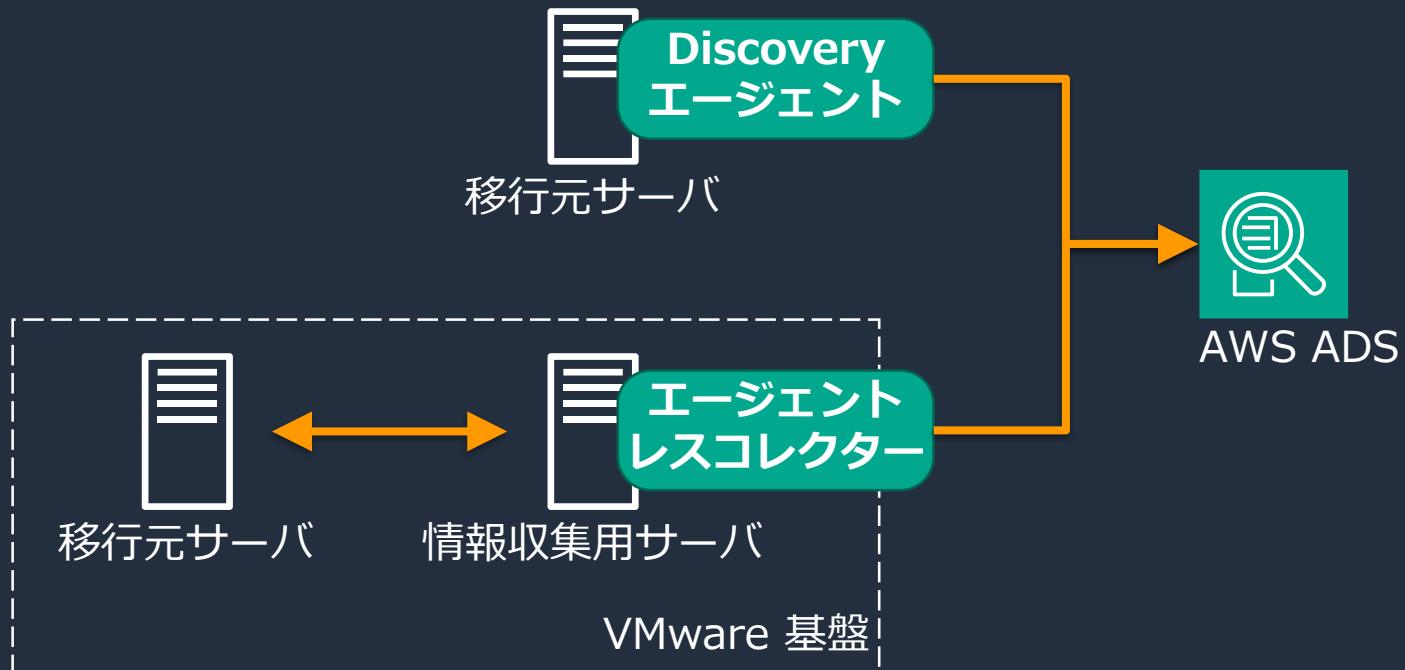
- Rehost applications on Amazon EC2:** A template to rehost applications on Amazon EC2 using AWS Application Migration Service (AWS MGN). It includes a preview button and a "Learn more" link.
- Migrate SAP NetWeaver applications to AWS:** A template to migrate SAP NetWeaver based applications (S/4HANA, BW4HANA, and ECC on HANA) running on SAP HANA database to AWS. It includes a preview button and a "Learn more" link.

AWS ADS の情報収集の仕組み

AWS ADS による情報収集の仕組み

Discovery エージェント、またはエージェントレスコレクターにより情報が収集され、AWS に送信される

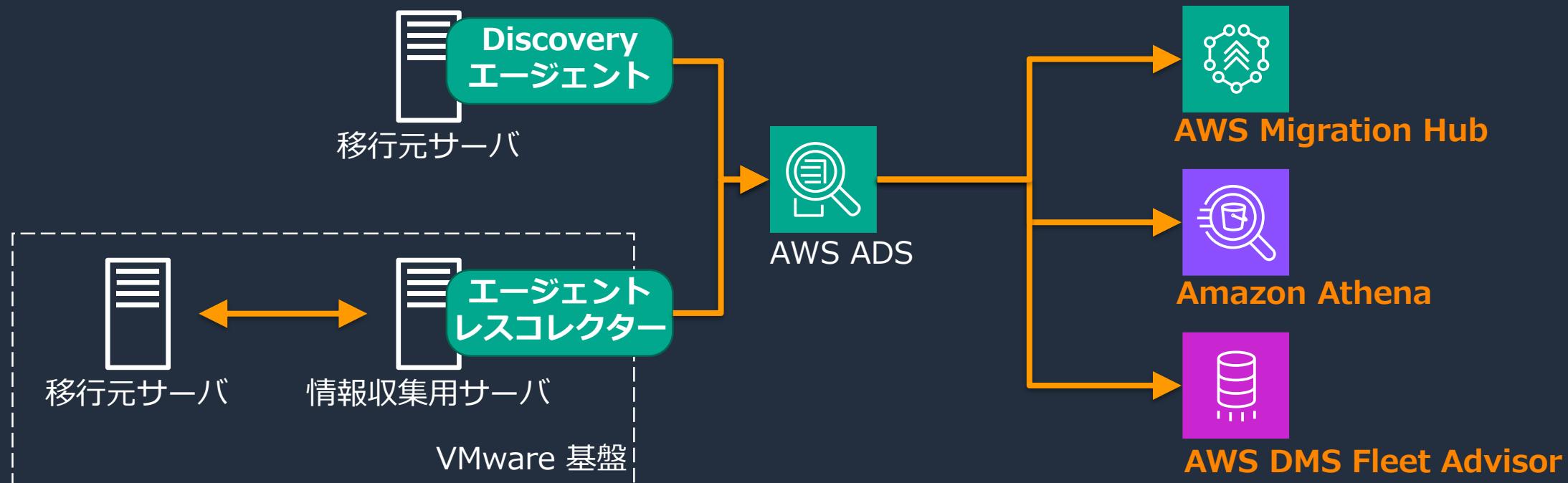
- Discovery エージェントを使用する場合は移行元サーバへのインストール（変更作業）が必須
- エージェントレスコレクターは、対象 VMware 基盤上のサーバのみ利用可能
- Discovery エージェントとエージェントレスコレクターとで、収集される情報が異なる



AWS ADS による収集情報の活用

AWS ADS は他サービスと連携することで、収集した情報の確認や情報を用いた分析を実施することが可能

- AWS Migration Hub で収集した情報の参照・分析や推奨 EC2 インスタンスの取得が可能
- Amazon Athena でのデータ探索を有効にすることで、クエリを用いた分析が可能
- AWS DMS Fleet Advisor データベース関連のインベントリ情報を評価し、潜在的な推奨移行パスを取得



Discovery エージェント とは

移行元サーバにインストールし、インベントリ情報の収集を行う
ソフトウェア

- AWS Application Discovery Agent を導入することで、システム設定、使用率、パフォーマンス情報、プロセステータ、およびネットワーク接続情報を収集
- 公開 S3 バケット上に配置されている専用のインストーラを使用して、情報収集対象である移行元サーバにインストール
- サポート対象 OS
 - Linux : Amazon Linux 2012.03, 2015.03 / Amazon Linux 2 (2018 年 9 月 25 日更新以降) / Ubuntu 12.04, 14.04, 16.04, 18.04, 20.04 / Red Hat Enterprise Linux 5.11, 6.10, 7.3, 7.7, 8.1 / CentOS 5.11, 6.9, 7.3 / SUSE 11 SP4, 12 SP5
 - Windows : Windows Server 2003 R2 SP2 / 2008 R1 SP2, 2008 R2 SP1 / 2012 R1, 2012 R2 / 2016 / 2019
- 使用するための前提条件
 - アカウントで、AWS Migration Hub のホームリージョンの設定がされていること
 - 移行元サーバから TCP ポート 443 を介した arsenal エンドポイントへのインターネットアクセス
 - 必要なポリシーが設定された IAM ユーザーのアクセスキーが使用できること
 - 移行元サーバの時刻が正しいこと（NTP と同期が取れていること）

Discovery エージェント により収集される主要な情報

- システム設定
 - ホスト名
 - OS 名・バージョン、ハイパーテザー
 - CPU タイプ、CPU コア数、CPU ユニット数
 - ディスク数、ディスク容量、ディスク空き容量
 - IP アドレス、MAC アドレス、ネットワークカード数
- 使用率／パフォーマンス情報
 - CPU 使用率
 - メモリ使用率、空きメモリ容量
 - ディスク読み込み（ IOPS/KBPS ）、ディスク書き込み（ IOPS/KBPS ）
- **ネットワーク通信情報 (Discoveryエージェントでのみ収集可能)**
 - 送信元 IP アドレス、送信元ポート
 - 送信先 IP アドレス、送信先ポート

詳細は[こちら](#)のユーザーガイドを参照



エージェントレスコレクター とは (1/2)

移行元サーバにソフトウェアをインストールしない、エージェントレスでのインベントリ情報の収集を行うアプリケーション

- VMware vCenter Server 環境に仮想マシンとしてインストール
- 仮想マシンの仕様
 - オペレーティングシステム – Amazon Linux 2
 - RAM – 16 GB
 - CPU – 4 コア
- **2種類のモジュール**によって、システム設定、使用率、データベースメタデータ、などの情報を収集
 - VMware vCenter data collection module (以降 **VMware モジュール**)
 - database and analytics data collection module (以降 **D&A モジュール**)

エージェントレスコレクター とは (2/2)

移行元サーバにソフトウェアをインストールしない、エージェントレスでのインベントリ情報の収集を行うアプリケーション

- 使用するための前提条件

(エージェントと共通／類似)

- AWS Migration Hub のホームリージョンの設定がされていること
- エージェントレスコレクターから TCP ポート 443 を介したエンドポイントへのインターネットアクセス
- 必要なポリシーが設定された IAM ユーザーのアクセスキーが使用できること

(エージェントレス固有)

- VMware vCenter Server のバージョンが V5.5, V6, V6.5, 6.7 or 7.0
- Read/View 権限のある vCenter クレデンシャルを使用できること

D&A モジュールのサポート対象 OS およびデータベース

- サポート対象 OS
 - Amazon Linux 2
 - CentOS Linux version 6 and higher
 - Debian version 10 and higher
 - Red Hat Enterprise Linux version 7 and higher
 - SUSE Linux Enterprise Server version 12 and higher
 - Ubuntu version 16.01 and higher
 - Windows Server 2012 and higher
 - Windows XP and higher
- 情報収集サポート対象
 - Microsoft SQL Server version 2012 and up to 2019
 - MySQL version 5.6 and up to 8
 - Oracle version 11g Release 2 and up to 12c, 19c, and 21c
 - PostgreSQL version 9.6 and up to 13

エージェントレスコレクター により収集される主要な情報

VMware モジュール

- ・ システム設定
 - ・ 仮想マシン名、ホスト名
 - ・ OS 名・バージョン
 - ・ ハイパーバイザ、ホストのタイプ
 - ・ CPU コア数、CPU ユニット数
 - ・ ディスク数、ディスク容量
 - ・ MAC アドレス、ネットワークカード数
- ・ 使用率／パフォーマンス情報
 - ・ CPU 使用率
 - ・ 空きメモリ容量
 - ・ ディスク読み込み（IOPS/KBPS）、ディスク書き込み（IOPS/KBPS）

D&A モジュール

- ・ データベースのメタデータ、キャパシティ
 - ・ CPU 数、メモリ、ストレージ容量
 - ・ データベースバージョンとエディション
 - ・ スキーマ数、ストアドプロシージャ数、テーブル数、トリガー数、ビュー数
 - ・ スキーマ構造
- ・ 使用率／パフォーマンス情報
 - ・ I/O スループット
 - ・ IOPS
 - ・ OS レベルのメモリ使用量、ディスク使用量、CPU 使用数

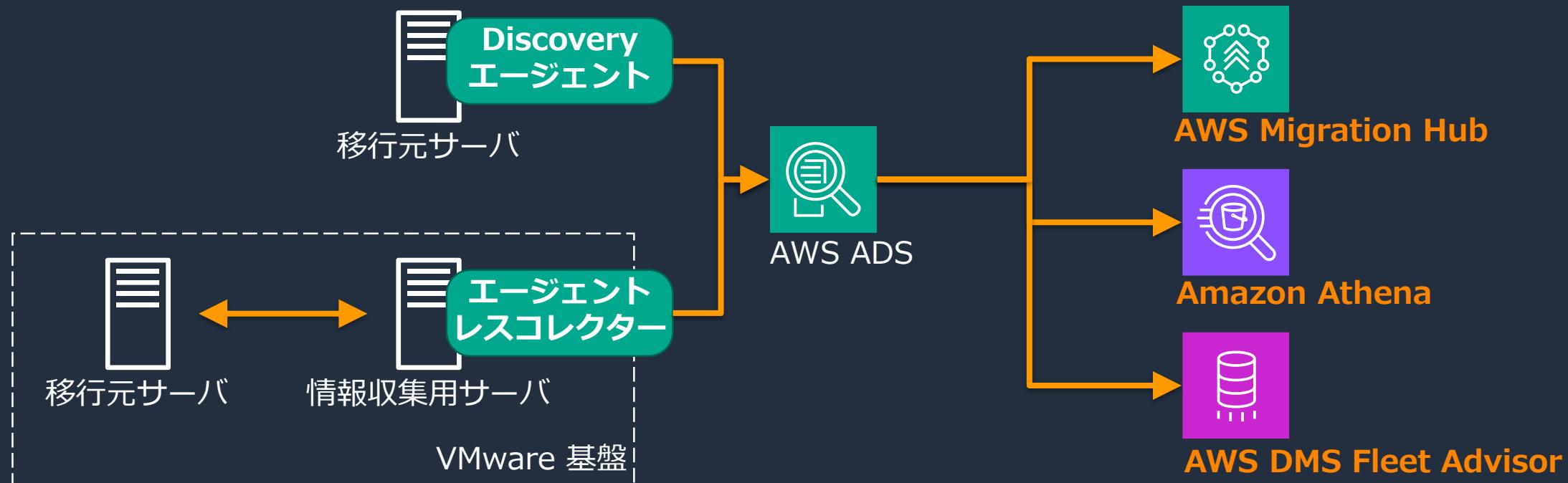
注) PostgreSQL および MySQL データベースは
メタデータのみ情報収集可能

詳細は[こちら](#)および[こちら](#)ユーザーガイドを参照

(再掲) AWS ADS による収集情報の活用

AWS ADS は他サービスと連携することで、収集した情報の確認や情報を用いた分析を実施することが可能

- AWS Migration Hub で収集した情報の参照・分析や推奨 EC2 インスタンスの取得が可能
- Amazon Athena でのデータ探索を有効にすることで、クエリを用いた分析が可能
- AWS DMS Fleet Advisor データベース関連のインベントリ情報を評価し、潜在的な推奨移行パスを取得



まとめ



本セッションのまとめ

- ・移行を進めるためには、ポートフォリオ調査による現状把握結果に基づいた移行戦略の策定が重要
- ・AWS ADS を用いることで、ポートフォリオ調査として必要な移行元サーバの情報を自動でキャプチャすることが可能
- ・関連サービスと連携して AWS ADS を使用することで、収集した情報に基づいた様々な分析が実施可能

参考資料

【AWS ADS 関連ページ】

- [AWS Application Discovery Service](#)
- [AWS Application Discovery Service User Guide](#)

【本セミナー関連 Black Belt コンテンツ】

- [クラウド移行における Discovery ツールの必要性
\(AWS 移行準備シリーズ\) 【AWS Black Belt】](#)

AWS Black Belt Online Seminar とは

- ・ 「サービス別」「ソリューション別」「業種別」などのテーマに分け、
アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナー
シリーズです
- ・ AWS の技術担当者が、AWS の各サービスやソリューションについてテーマ
ごとに動画を公開します
- ・ 以下の URL より、過去のセミナー含めた資料などをダウンロードするこ
とができます
 - ・ <https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/>
 - ・ <https://www.youtube.com/playlist?list=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBlqY>



ご感想は X (Twitter) へ！ハッシュタグは以下をご利用ください
#awsblackbelt

内容についての注意点

- ・ 本資料では資料作成時点のサービス内容および価格についてご説明しています。AWS のサービスは常にアップデートを続けているため、最新の情報は AWS 公式ウェブサイト (<https://aws.amazon.com/>) にてご確認ください
- ・ 資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます
- ・ 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます
- ・ 技術的な内容に関しましては、有料の [AWS サポート窓口](#)へお問い合わせください
- ・ 料金面でのお問い合わせに関しましては、[カスタマーサポート窓口](#)へお問い合わせください（マネジメントコンソールへのログインが必要です）



Thank you!

AWS Black Belt Online Seminar

AWS DataSync

佐藤 真也

Solutions Architect

2024/09



AWS Black Belt Online Seminar とは

- ・ 「サービス別」「ソリューション別」「業種別」などのテーマに分け、
アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナーシリーズです
- ・ AWS の技術担当者が、 AWS の各サービスやソリューションについてテーマごとに動画を公開します
- ・ 以下の URL より、過去のセミナー含めた資料などをダウンロードすることができます
 - <https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/>
 - <https://www.youtube.com/playlist?list=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBlqY>

𝕏 ご感想は X (Twitter) へ！ハッシュタグは以下をご利用ください
#awsblackbelt

内容についての注意点

- ・ 本資料では資料作成時点のサービス内容および価格についてご説明しています。AWS のサービスは常にアップデートを続けているため、最新の情報は AWS 公式ウェブサイト (<https://aws.amazon.com/>) にてご確認ください
- ・ 資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます
- ・ 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます
- ・ 技術的な内容に関しましては、有料の [AWS サポート窓口](#)へお問い合わせください
- ・ 料金面でのお問い合わせに関しては、[カスタマーサポート窓口](#)へお問い合わせください (マネジメントコンソールへのログインが必要です)

自己紹介

佐藤 真也



アマゾン ウェブ サービス ジャパン合同会社
技術統括本部 フィナンシャルサービス インダストリ 技術本部
保険ソリューション部

好きな AWS サービス

- Amazon Simple Storage Service (S3)
- Amazon FSx シリーズ



前提知識と本セミナーの対象者

前提知識

- AWS のグローバルインフラストラクチャや基本サービスの知識
- AWS のストレージサービスの概要

対象者

- AWS へのデータ移行方法を学びたい方
- AWS DataSync の機能を深く知りたい方

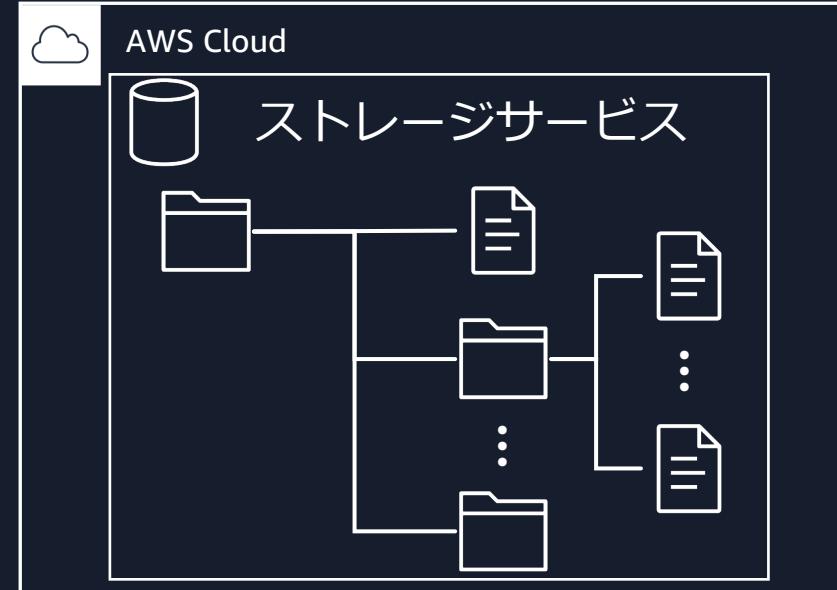
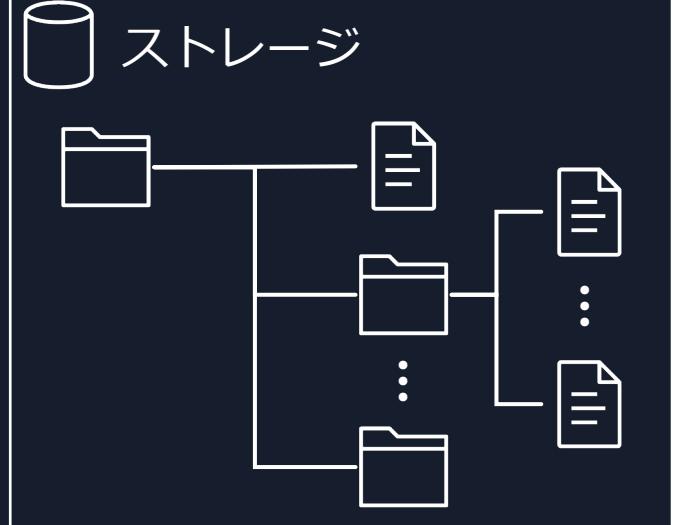
アジェンダ

1. AWS DataSync とは
2. AWS DataSync Agent
3. AWS DataSync タスク
4. AWS DataSync を用いたデータ転送の流れ
5. 他のデータ転送ソリューションとの比較
6. 補足と注意点

AWS DataSync とは

大量のデータを転送するときの課題

送信元ストレージから、LAN や WAN を経由して AWS クラウドへ辿り着くまでに多くの課題に直面する



送信元ストレージのボトルネック

LAN のボトルネック

WAN のボトルネック

送信先ストレージのボトルネック

送信対象のファイル整理

伝送路の暗号化

データとメタデータの整合性検証

スケジューリング・エラーハンドリング・パフォーマンスの向上

+スクリプトの開発とデプロイ



AWS DataSync とは

データの転送に関するマネージドサービスで、AWS ストレージサービスとオンプレミス、他クラウドサービス間でデータの移動が「簡単に」「高速に」「安全に」「低コストで」実現できる



簡単なデータ転送



高速なデータ転送



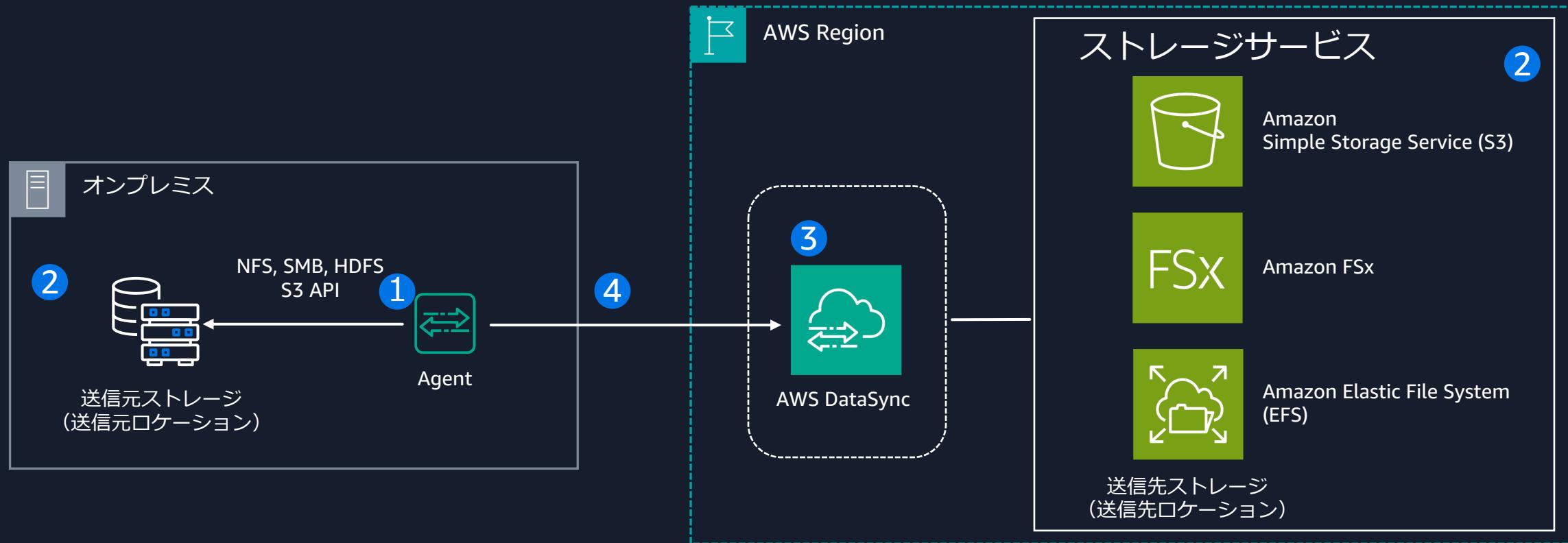
セキュリティ
高い信頼性



低コスト

AWS DataSync 全体像: データ転送の流れ

1. オンプレミスに Agent を配置する
2. 送信元と送信先ストレージを、それぞれ送信元口ケーションと送信先口ケーションとして設定する
3. 転送スケジュールなどを定義したタスクを設定する
4. その後タスクを実行し、Agent は送信元口ケーションからデータを読み取り、AWS DataSync へ送信する
AWS DataSync は送信先口ケーションへデータを保存する





簡単なデータ転送

Agent をデプロイしタスクを作成し実行するだけで、データを転送できる



Vmware

Hyper-V

KVM

Agent

簡単にセットアップできる仮想マシンアプライアンスで、データ転送を実行する



タスクで

- 送信元ロケーションと送信先ロケーション
- 送信対象ファイルの整理
- データの整合検証方法、スケジュール、帯域制限などを設定する

タスク実行

特定のスケジュールで特定のフォルダ・ファイルだけを、帯域制限しながら自動的にデータを転送し、データの整合性も検証する

高速なデータ転送

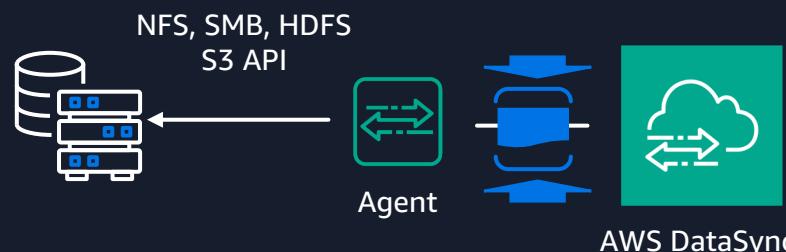


Agent は AWS DataSync へデータを転送する時、マルチセッション・圧縮・ロードバランス機能を自動的に用いるため、高速なデータ転送が実現できる



マルチセッション

Agent と AWS DataSync の間では、同時に複数の TCP セッションを生成し、並列にデータを転送する



圧縮

Agent と AWS DataSync の間では、データを圧縮し転送を効率化できる



ロードバランス

AWS DataSync 側に複数のエンドポイントを自動生成し、Agent からのデータ転送を負荷分散できる



セキュリティと高い信頼性

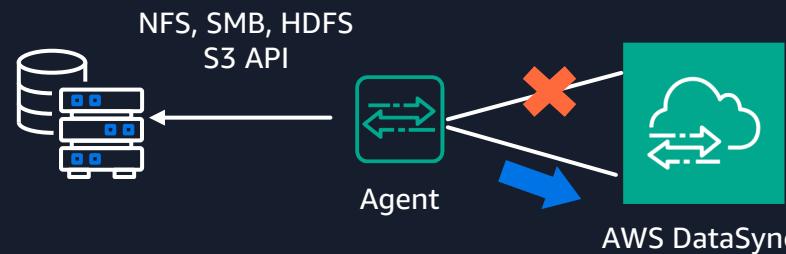
AWS DataSync はデータの暗号化とエラーハンドリングに対応している



伝送路の暗号化
Agent と AWS DataSync の間では、TLS で暗号化できる



保管時の暗号化
送信先の Amazon S3 や Amazon EFS、Amazon FSx シリーズではデータ保管時に暗号化することができる



エラーハンドリング
ネットワークの切断などで転送に失敗した場合、エラーを記録しつつ、次のスケジュールタスクで再送することができる



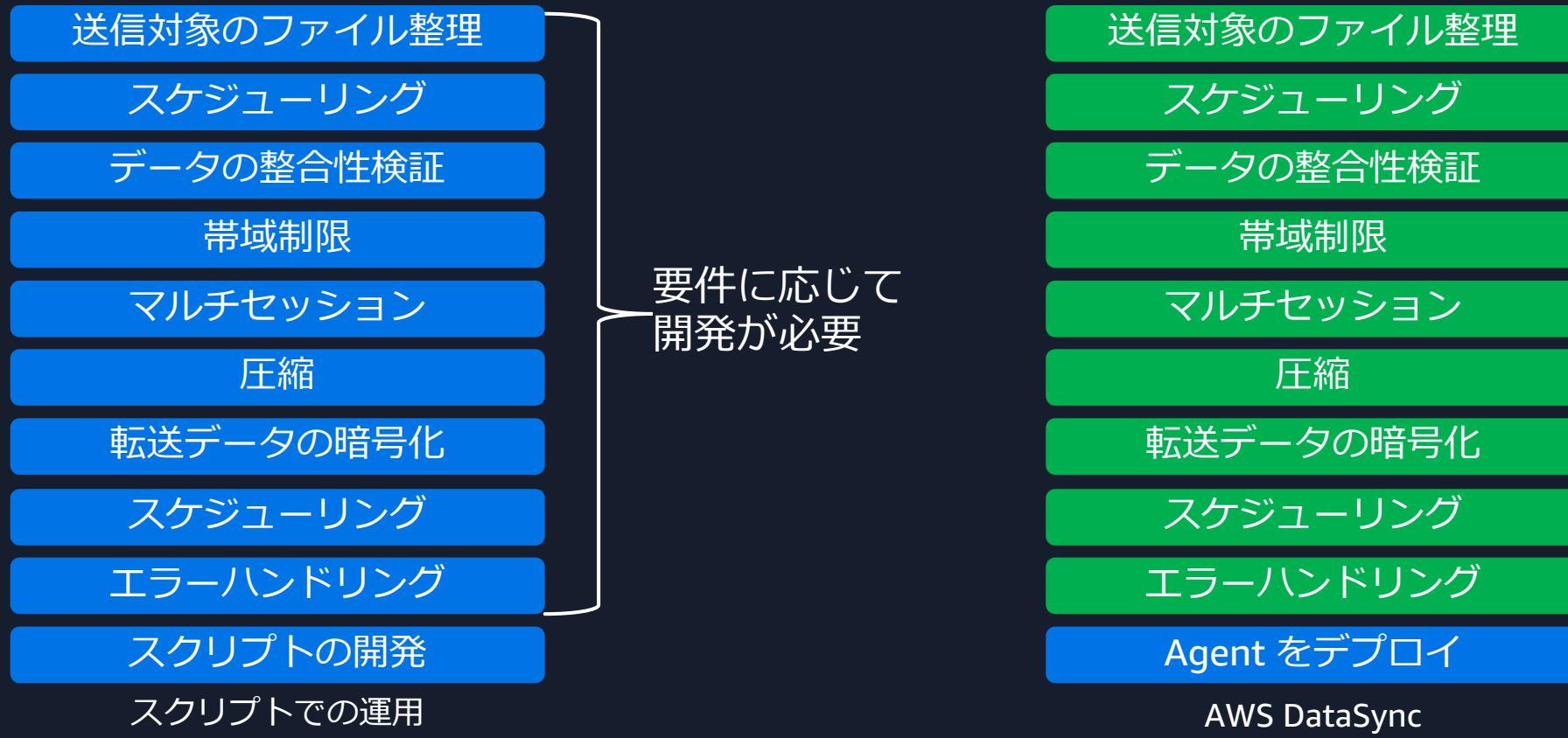
低成本

AWS DataSync は 1 GBあたり 0.0125 USD のデータの転送料金で、データ転送に便利な機能を独自開発・デプロイすることなく利用でき、開発・運用コストを削減できる

データ転送に便利な機能の例

お客様が担当する作業

AWS が提供する機能



AWS DataSync と同じアカウント上の AWS サービスを送信先に指定する

送信元ロケーション	送信先ロケーション
<ul style="list-style-type: none">Amazon S3Amazon EFSAmazon FSx シリーズ※	<ul style="list-style-type: none">お客様管理の NFS/SMB/HDFS ストレージまたは、S3 API 互換ストレージ他クラウドストレージサービスAWS Snowball Edge S3 互換ストレージ
<ul style="list-style-type: none">お客様管理の NFS/SMB/HDFS ストレージまたは、S3 API 互換ストレージ他クラウドストレージサービスAWS Snowball Edge S3 互換ストレージ	<ul style="list-style-type: none">Amazon S3Amazon EFSAmazon FSx シリーズ※
<ul style="list-style-type: none">Amazon S3Amazon EFSAmazon FSx シリーズ※	<ul style="list-style-type: none">Amazon S3Amazon EFSAmazon FSx シリーズ※
Amazon S3	Amazon S3 on Outposts
Amazon S3 on Outposts	Amazon S3

※ Amazon FSx for NetApp ONTAP、Windows File Server、Open ZFS、Lustre



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

参考: <https://docs.aws.amazon.com/datasync/latest/userguide/working-with-locations.html>

AWS DataSync と異なるアカウント上の AWS サービスを送信先に指定する

送信元ロケーション	送信先ロケーション
<ul style="list-style-type: none">NFS ロケーションとして設定した Amazon EFS ※1SMB ロケーションとして設定した Amazon FSx for Windows File Server ※1	<ul style="list-style-type: none">Amazon S3Amazon EFSAmazon FSx シリーズ※2
Amazon S3	<ul style="list-style-type: none">Amazon S3Amazon EFSAmazon FSx シリーズ※2
<ul style="list-style-type: none">Amazon S3Amazon EFSAmazon FSx シリーズ※2	Amazon S3
お客様管理の NFS/SMB/HDFS ストレージまたは、S3 API 互換ストレージ	Amazon S3

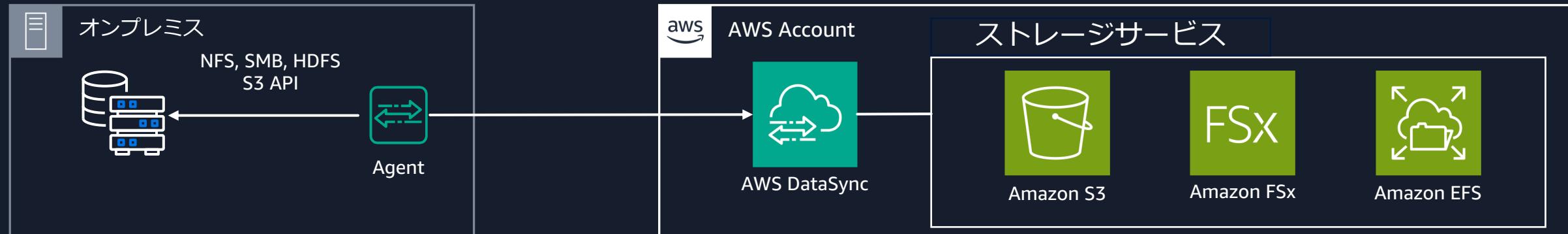
※1 Amazon EFS を送信元ロケーションとして選択するのではなく、NFS を送信元ロケーションとして一旦設定する。その上で、Amazon EFS のファイルシステムのドメイン名を NFS サーバのドメイン名として設定する。Amazon FSx for Windows File Server の場合も同様である。

※2 Amazon FSx for NetApp ONTAP、Windows File Server、Open ZFS、Lustre

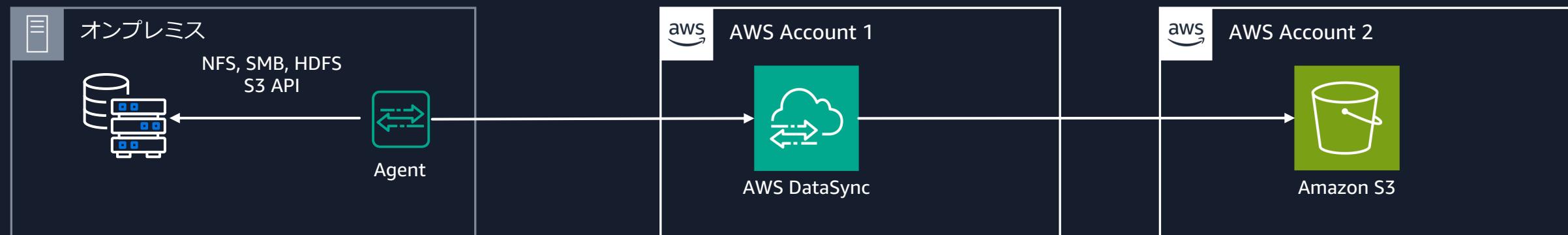


データ転送アーキテクチャの例

AWS DataSync と同じアカウント上の AWS サービスを送信先ロケーションに指定する場合



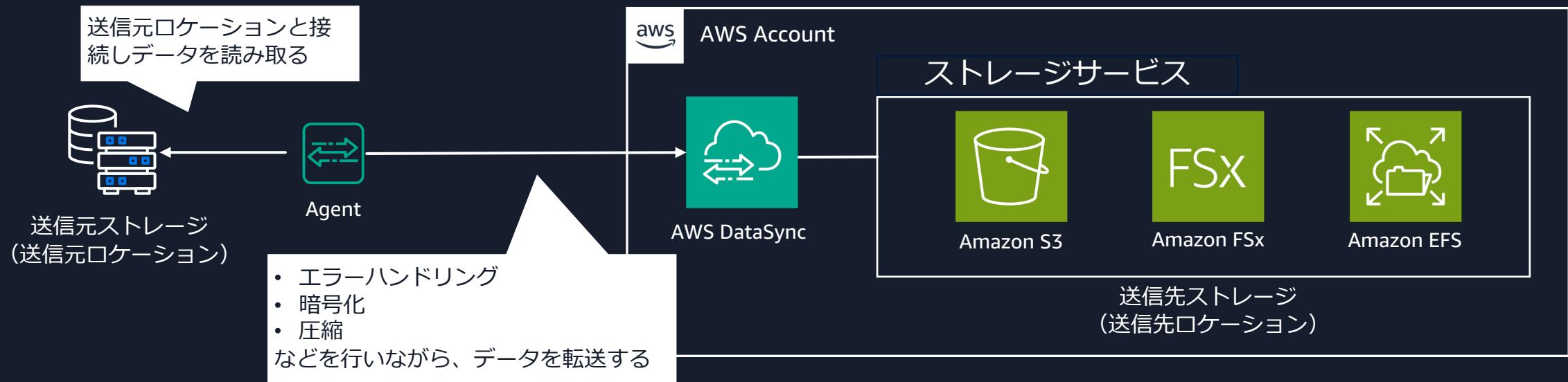
AWS DataSync と異なるアカウント上の AWS サービスを送信先ロケーションに指定する場合



AWS DataSync Agent

AWS DataSync Agent とは

仮想マシンアプライアンスで、送信元ストレージからデータを読み取り、AWS DataSync へデータを転送する



AWS DataSync Agent の要件

Agent はハイパーバイザまたは Amazon EC2、Amazon Outposts 上で実行できる



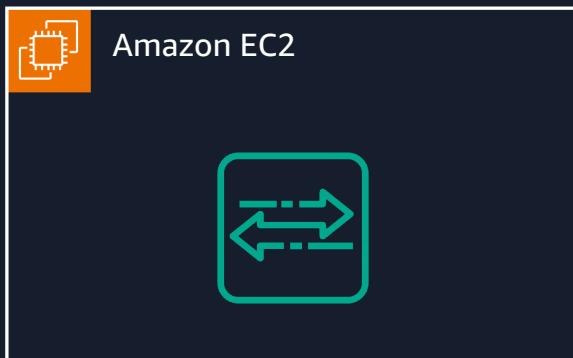
対応ハイパーバイザ:

- VMware ESXi (version 6.5, 6.7, 7.0, or 8.0)
- Linux Kernel-based Virtual Machine (KVM)
- Microsoft Hyper-V (version 2012 R2, 2016, or 2019)

ディスク容量と RAM の要件:

- VM イメージとシステムデータのインストールに利用する 80 GB のディスク容量
- 1 回のタスクで取り扱うファイル数が 2,000 万ファイル以下の場合 32 GB RAM
2,000 万ファイルを超える場合 64 GB RAM

詳細: <https://docs.aws.amazon.com/datasync/latest/userguide/agent-requirements.html>



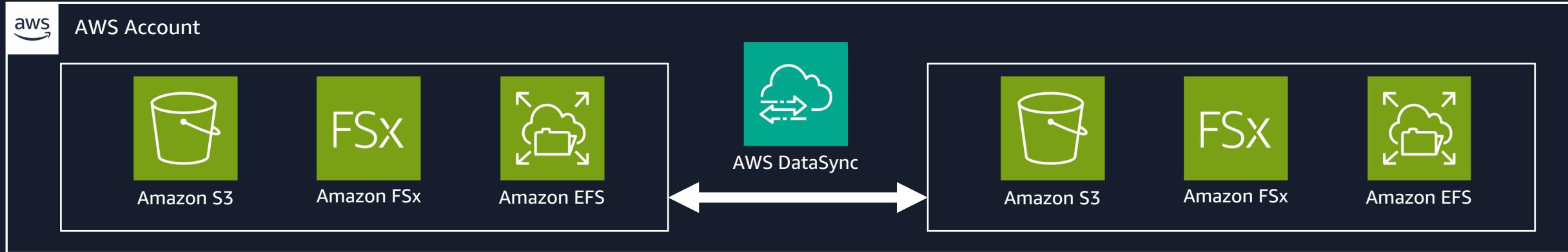
Amazon EC2:

- AWS DataSync Agent を含む AMI を使用する
- 1 回のタスクで取り扱うファイル数が 2,000 万ファイル以下の場合 m5.2xlarge
2,000 万ファイルを超える場合 m5.4xlarge

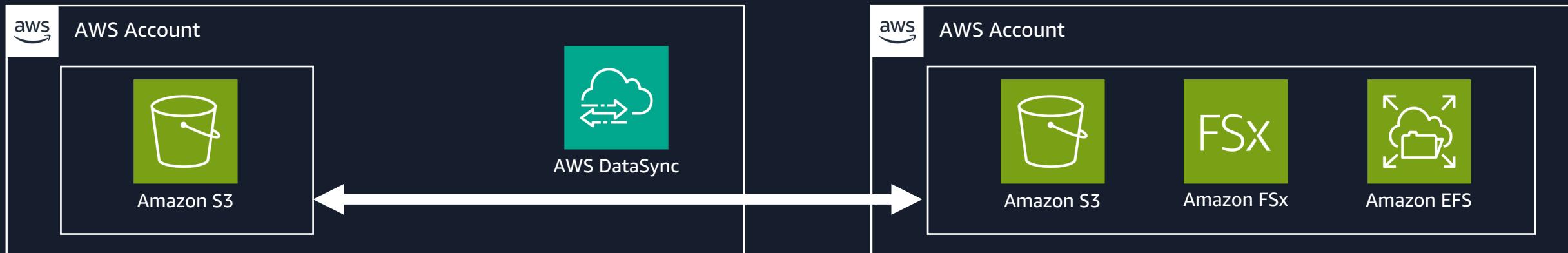
AWS DataSync Agent が不要なケース

次のパターンはクロスリージョンを含み、Agent が不要である。記載がないパターンは Agent が必須となる

- 同じアカウントにおける AWS ストレージサービス間でのデータ転送



- Amazon S3 と他の AWS ストレージサービス間で、クロスアカウントデータ転送

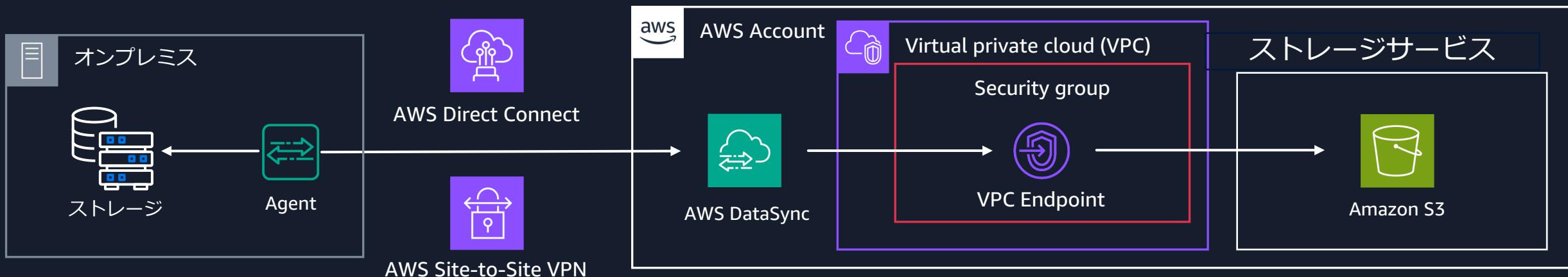


AWS DataSync のエンドポイント

AWS DataSync と Agent が通信するエンドポイントを要件に合わせて選択できる

検証方法	説明
パブリックエンドポイント	インターネット経由で、AWS DataSync と通信する
FIPS サービスエンドポイント	インターネット経由で、AWS DataSync と通信する。FIPS に準拠したプロセスでデータを転送する
VPC エンドポイント	Amazon VPC 経由で AWS DataSync と通信する

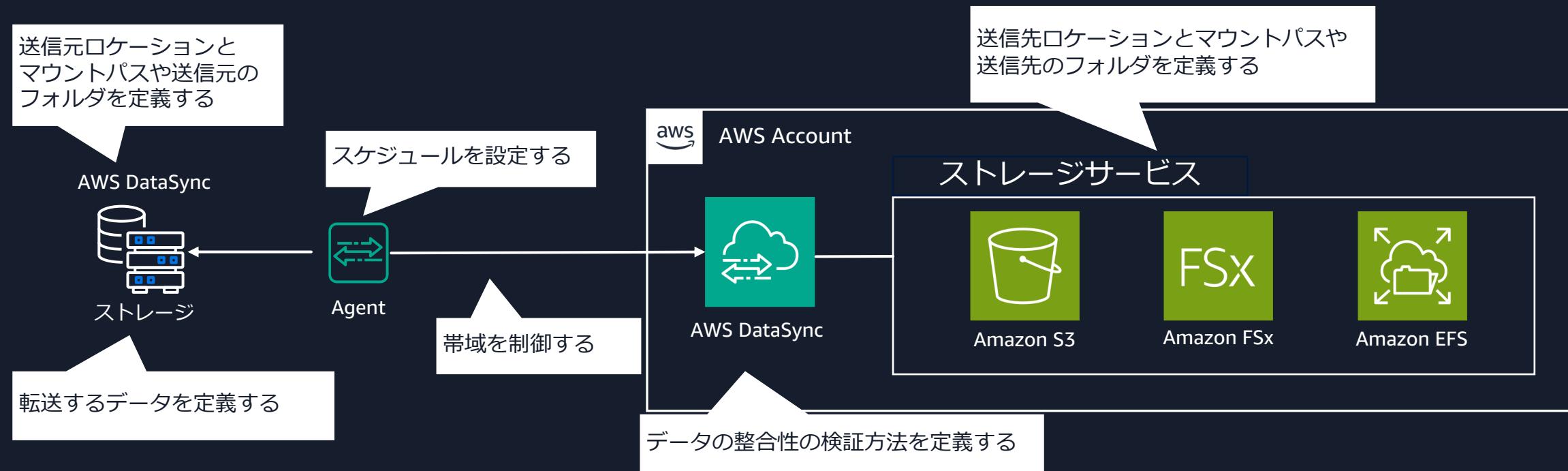
VPC エンドポイントを利用した際のデータ転送アーキテクチャ



AWS DataSync タスク

AWS DataSync タスクとは

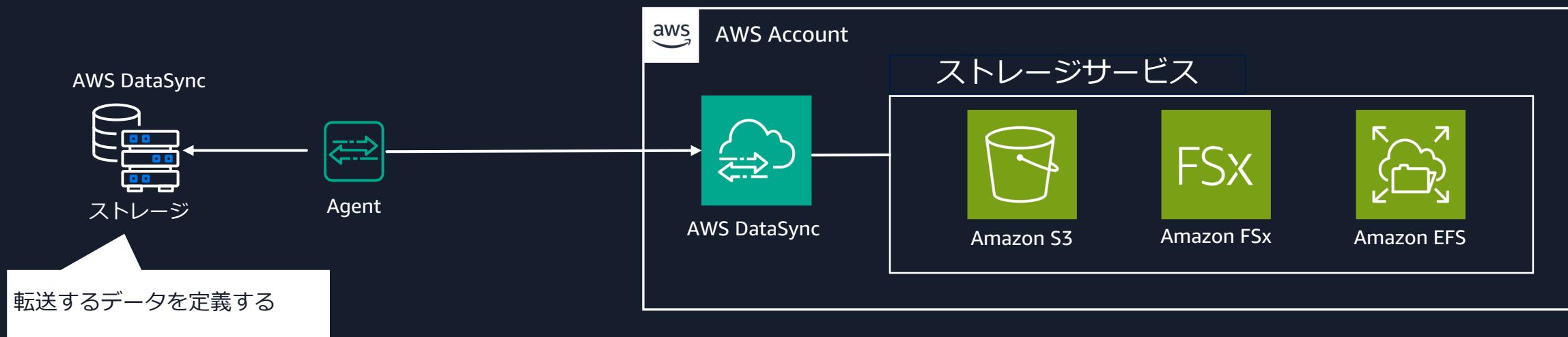
AWS DataSync が「どこから」「どこへ」「何を」「どのように」転送するかを設定するタスクを実行することで、AWS DataSync はデータの転送をスケジュールに従って開始する



転送するデータを定義する

送信元ロケーションから送信先ロケーションへデータを送信する場合に、次の設定ができる

- ・ マニフェストによる送信対象データのリスト化
- ・ フィルタを用いて特定の名前のファイルやフォルダのみ送信または送信から除外
- ・ データの同期方法



マニフェスト

マニフェストはファイルをリスト化し、特定のファイルだけを送信できる

- 指定した送信元ロケーションの起点となるフォルダを基準に、ファイル名をリスト化する
送信対象のファイルが複数ある場合には改行する

NFS ストレージの場合

```
photos/picture1.png  
photos/picture2.png  
photos/picture3.png
```

Amazon S3 の場合、Version ID を含むことができる

```
photos/picture1.png,111111  
photos/picture2.png,121212  
photos/picture3.png
```

- ファイル名にカンマや改行、引用符を含む場合は、「"」を用いる

ファイル名が
「filename,with,commas.txt」の場合

```
"filename,with,commas.txt"
```

ファイル名に改行が入る場合

```
"Thank  
You."
```

ファイル名が
「filename"with"commas.txt」の場合

```
filename""with""quotes.txt
```

- マニフェストを csv または txt ファイルとして、AWS DataSync と同じアカウント/リージョンの Amazon S3 バケットへと保存する

マニフェストの注意点および TIPS

- ・ ディレクトリやフォルダ単位で指定することはできない。ファイル名を含めたフルパスを指定する
- ・ 4,096 文字または 1,024 バイトを超えるファイル名やオブジェクトパスは定義できない
- ・ 重複したファイル名やオブジェクトパスを定義できない
- ・ フィルタと併用することはできない
- ・ マニフェストを用いる場合、送信先ロケーションのファイルは削除しない。そのため、データ転送時のオプションとして「Keep deleted files」を選択できず、デフォルトで保持される
- ・ マニフェスト使用時には、AWS DataSync のタスク設定時に「s3:GetObject」と「s3:GetObjectVersion」の権限を与える必要がある

その他の注意事項は[こちら](#)を参照する

フィルタ

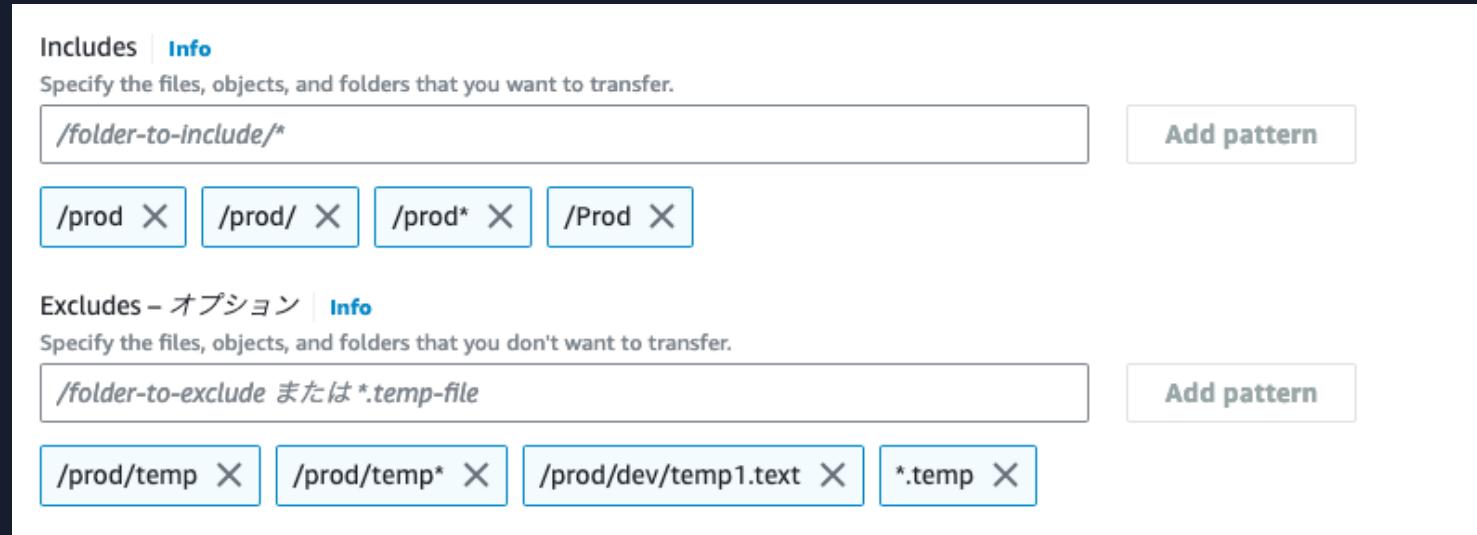
特定のパス、名前、拡張子を記述することで、そのパターンに一致するデータを転送することができる
また、転送から除外するパターンも記述できる

- フィルタで利用できる特殊文字

特殊文字	意味
* (ワイルドカード)	前方または後方一致を表す。例、/movies* は /movies も /movies_folder も含む
(パイプ)	OR を表す。例、*.tmp *.temp は tmp または temp の拡張子を持つファイルを含む
¥ (バックスラッシュ)	*, , ¥ に対するエスケープ文字。例、¥*.temp と ¥¥.temp はそれぞれ *.temp と ¥.temp というファイル名を表す。

- 送信元ロケーションの起点となるフォルダを基準にパス、名前、拡張子を記述する
この際、起点となるフォルダ直下のフォルダは、/ から記述する
- 複数の記述を行う場合には、| で区切る必要がある。ただし、AWS DataSync コンソールから設定する場合には不要である

フィルタの例



- 起点となるフォルダ直下の /prod フォルダ、 /prod と前方一致するフォルダまたはファイル、 /Prod フォルダが転送対象となる
 - /prod と /prod/ は同じ意味で解釈される
 - 大文字と小文字は区別される
- 起点となるフォルダ直下の /prod/temp フォルダ、 /prod/temp と前方一致するフォルダまたはファイル、 /prod/dev/temp1.text、 .temp ファイルは転送対象から除外される

フィルタの注意点および TIPS

- ワイルドカードを用いた後方一致は、除外パターンを記述するときのみ利用できる
*.text のような後方一致を転送対象として記述することはできない
- 送信元または送信先ロケーションに Amazon S3 を選択した場合、/ というオブジェクトキーをファイルシステムにおけるフォルダとして扱う
- デフォルトで以下のフォルダの転送を AWS DataSync は除外する
 - .snapshot
 - /.aws-datasync および /.awssync
 - /.zfs

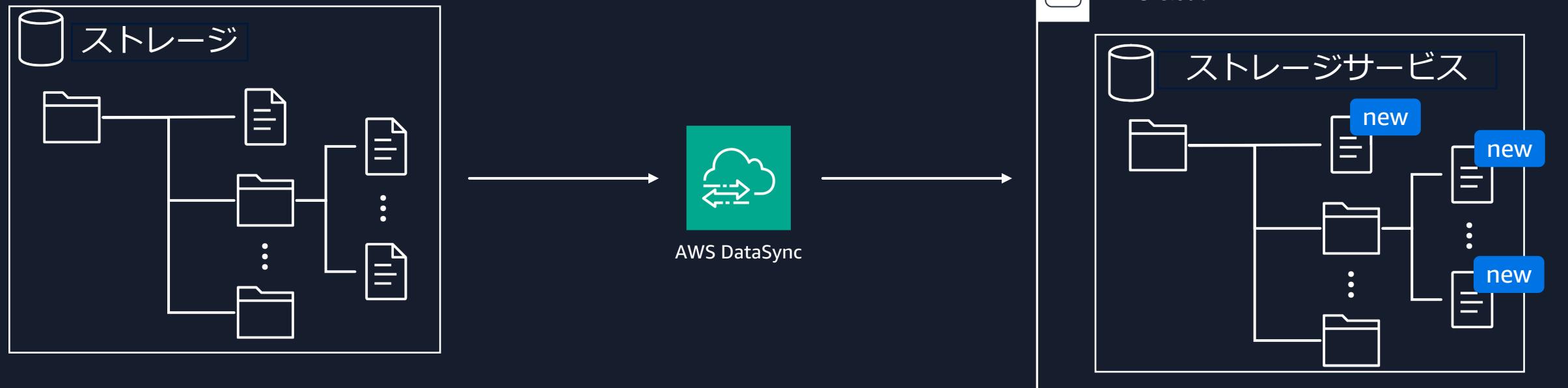
その他の注意事項は[こちら](#)を参照する

AWS DataSync のデータ同期方法（1）

AWS DataSync ではタスクを設定する際に、送信元と送信先のケーションで差分が存在するときの挙動として「すべてのデータを送信する」か「変更したデータだけ送信する」か定義できる

すべてのデータを送信する場合

すべてのデータを送信元のケーションから送信先のケーションへと送信し、送信先のケーション上のデータを上書きする



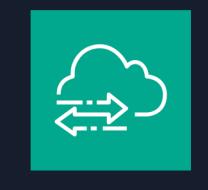
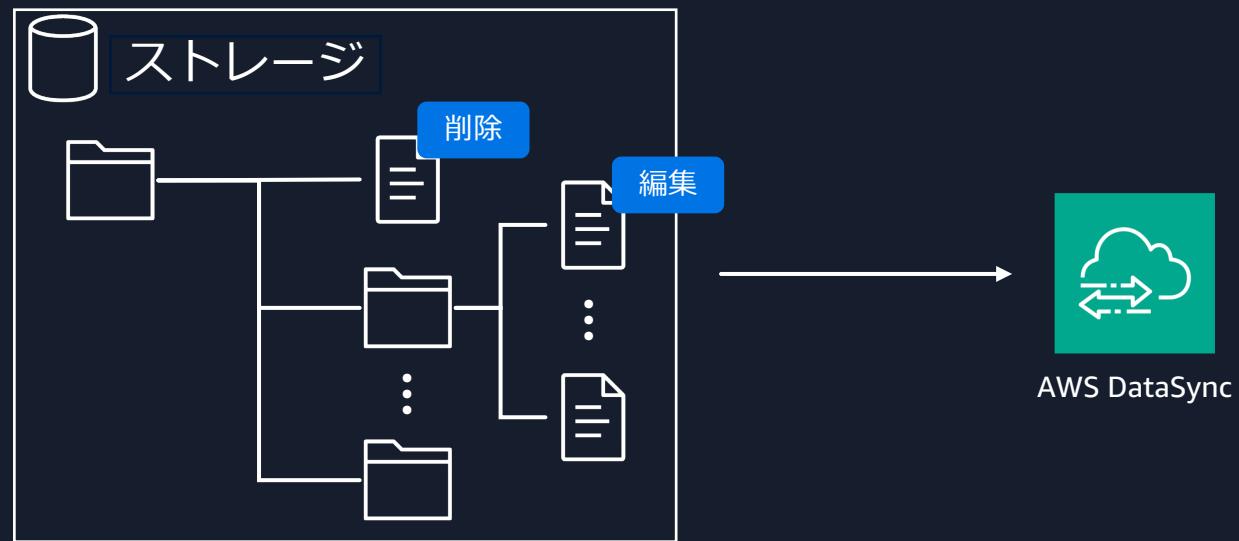
AWS DataSync のデータ同期方法（2）

AWS DataSync ではタスクを設定する際に、送信元と送信先の差分が存在するとき
「すべてのデータを送信する」か「変更したデータだけ送信する」か定義できる

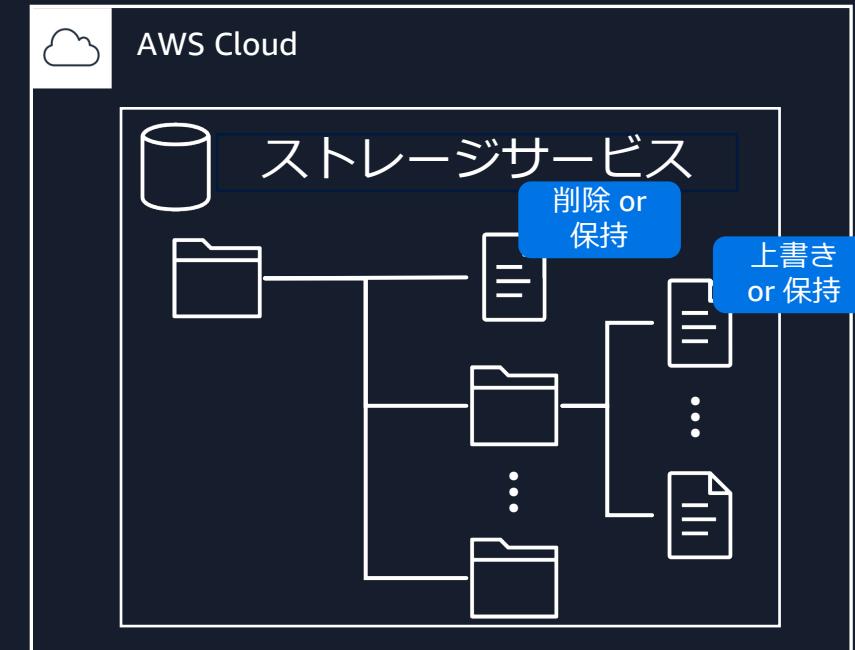
変更したデータだけ送信する場合

AWS DataSync はストレージ間のデータとメタデータをスキャンした上で、差分を判断する

- 送信元ストレージでデータを編集した場合、送信先の差分として上書きするか否か選択できる
- 送信元ストレージでデータを削除した場合、送信先の差分として削除しない設定ができる（Keep deleted files）



AWS DataSync



AWS DataSync におけるデータの整合性の検証

3つの検証方法があり、(1) Verify only the data transferred を推奨する

検証方法	説明
(1) Verify only the data transferred	<ul style="list-style-type: none">データの転送中、チェックサムに基づいて整合性を検証する送信処理完了後、送信したデータとそのメタデータのチェックサムをストレージ間で比較し検証する
(2) Verify all data in the destination	<ul style="list-style-type: none">データの転送中、チェックサムに基づいて整合性を検証する送信処理完了後、すべてのデータとそのメタデータのチェックサムをストレージ間で比較し、完全に同期していることを確認する
(3) Check integrity during transfer	データの転送中のみ、チェックサムに基づいて整合性を検証する

(2) Verify all data in the destination の注意点/TIPS

- ストレージ間で完全に同期していることを確認できるものの、ストレージヘリクエストが発生する
例えば Amazon S3 を用いた場合、リクエストにかかる料金に注意する
- マニフェストを利用する場合には、記載したファイルのみ整合性を検証する
- Amazon S3 Glacier Flexible Retrieval や Glacier Deep Archive をロケーションに用いる場合には使えない

AWS DataSync におけるメタデータの扱い（1）

コピーされるメタデータは送信元と送信先の組み合わせに依存する
ここでは一部の例のみ取り扱い、すべての組み合わせは[こちら](#)を参照する

送信元	送信先	コピーされるメタデータ※1
<ul style="list-style-type: none">• NFS• Amazon EFS• Amazon FSx for NetApp ONTAP (NFS)/ Lustre/OpenZFS	<ul style="list-style-type: none">• Amazon S3	<ul style="list-style-type: none">• ファイルとディレクトリの更新日時• ファイルとディレクトリのアクセス日時※2• User ID と group ID• POSIX permission
送信元	送信先	コピーされるメタデータ
<ul style="list-style-type: none">• NFS• Amazon EFS• Amazon FSx for NetApp ONTAP (NFS)/ Lustre/OpenZFS	<ul style="list-style-type: none">• NFS• Amazon EFS• Amazon FSx for NetApp ONTAP (NFS)/ Lustre/OpenZFS	<ul style="list-style-type: none">• ファイルとディレクトリの更新日時• ファイルとディレクトリのアクセス日時※2• User ID と group ID• POSIX permission

※1 AWS DataSync を用いて NFS ヘリストアすることで、これらのメタデータを復元できる
※2 ただし、ベストエフォートでの反映となる



AWS DataSync におけるメタデータの扱い（2）

コピーされるメタデータは送信元と送信先の組合せに依存する
ここでは一部の例のみ取り扱い、すべての組合せは[こちら](#)を参照する

送信元	送信先	コピーされるメタデータ
<ul style="list-style-type: none">• SMB• Amazon FSx for NetApp ONTAP (SMB)/ Windows File Server	<ul style="list-style-type: none">• SMB• Amazon FSx for NetApp ONTAP (SMB)/ Windows File Server	<ul style="list-style-type: none">• ファイルのアクセス/更新/作成日時• ファイル所有者の SID• Read-only、system などの属性※• NTFS DACL/SACL
送信元	送信先	コピーされるメタデータ
<ul style="list-style-type: none">• SMB• Amazon FSx for NetApp ONTAP (SMB)/ Windows File Server	<ul style="list-style-type: none">• Amazon S3	<ul style="list-style-type: none">• デフォルトの POSIX メタデータが作成され、Windows のメタデータは破棄される



タスクを作成する（1）

送信元ロケーションの作成

送信元のロケーションのオプション
送信元のロケーションを作成または選択する

データ転送元のロケーションを選択する

新しいロケーションを作成する 既存のロケーションを選択する

設定

ロケーションタイプ
Amazon EFS ファイルシステム

リージョン
US West (Oregon) us-west-2

ファイルシステム
[選択] [削除]



そのほか、マウントパス、サブネット、セキュリティグループを設定する

送信先ロケーションの作成

送信先ロケーションのオプション
送信先のロケーションを作成または選択する

データ転送先のロケーションを選択する

新しいロケーションを作成する 既存のロケーションを選択する

設定

ロケーションタイプ
Simple Storage Service (Amazon S3)

リージョン
US West (Oregon) us-west-2

S3 バケット
[選択] [削除]
us-west-2 の Simple Storage Service (Amazon S3) バケットである必要があります。



そのほか、Amazon S3 のストレージクラスやフォルダ、AWS IAM ロールを設定する

タスクを作成する (2)

送信対象のデータを定義する

特定のデータを転送対象に設定する場合には、フィルタまたはマニフェストを使用する

Task name – オプション

datasync-BB

Source data options [Info](#)

Contents to scan
Specify the data in your source location that you want to transfer to your destination.

Everything

Excludes – オプション [Info](#)
Specify the files, objects, and folders that you don't want to transfer.

/folder-to-exclude または *.temp-file

Add pattern

OR

Task name – オプション

datasync-BB

Source data options [Info](#)

Contents to scan
Specify the data in your source location that you want to transfer to your destination.

Specific files, objects, and folders

Using filters
Scan files, objects, and folders matching include patterns.
Exclude those that match any exclude patterns.

Using a manifest
Scan files or objects declared in a manifest.

マニフェストファイル [Info](#)
Simple Storage Service (Amazon S3) のマニフェストファイルを選択します。マニフェストファイルの各ファイルまたはオブジェクトパスは、次の条件を満たす必要があります。{bulletedList}たとえば、/my-folder/my-text.txt がタスクの送信元ロケーションのすぐ下にある場合は、/my-folder/my-text.txt をマニフェストファイルの個別の行として指定します。

S3 URI
 s3://bucket/prefix/object

オブジェクトのバージョン
 バージョンを選... 表示 S3 を参照

マニフェストのアクセスロール [Info](#)
S3 からマニフェストファイルを読み取るために DataSync が使用するロールを選択します。

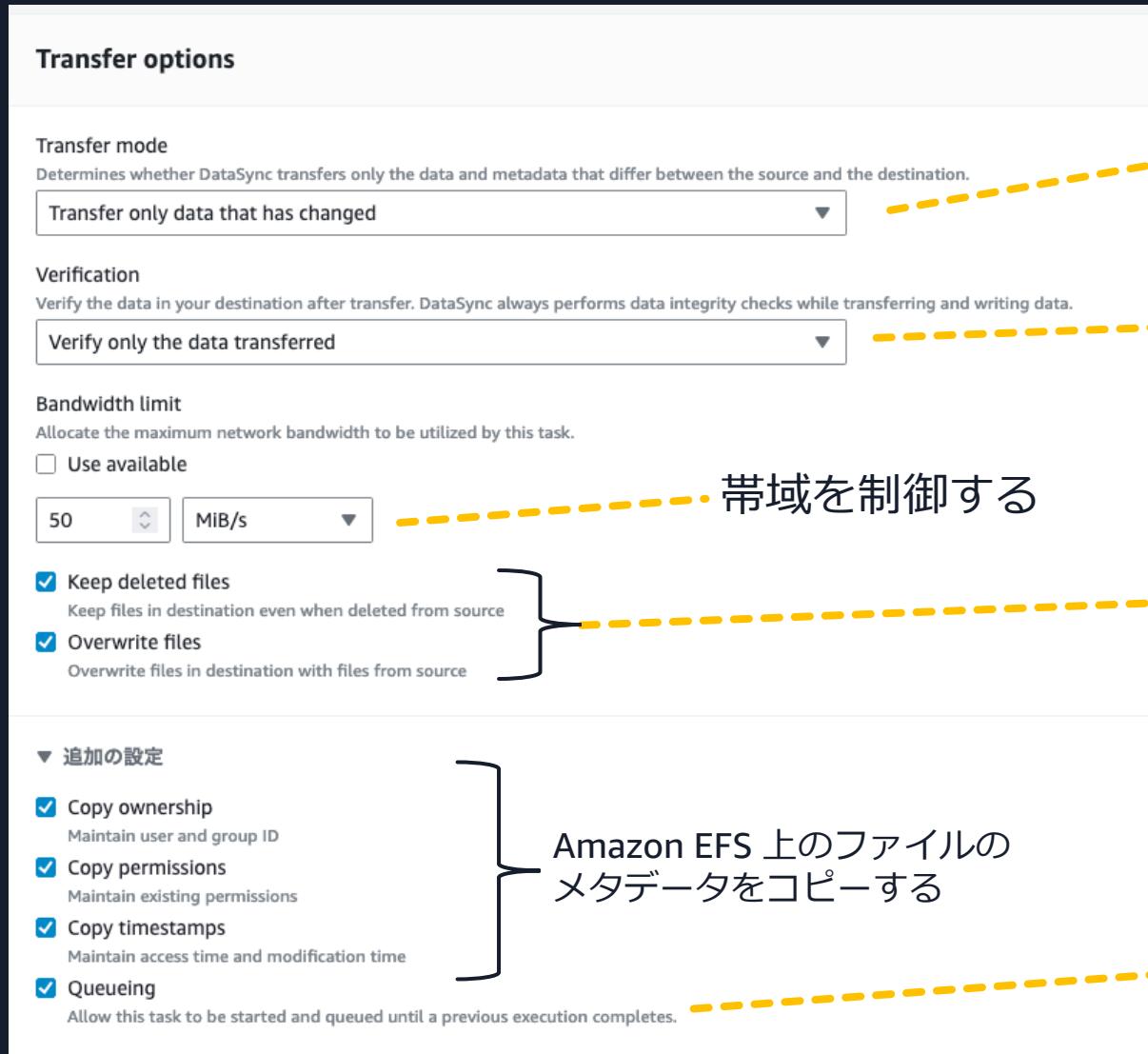
Choose a role

Role must allow: s3:GetObject s3:GetObjectVersion

C 自動生成する



タスクを作成する（3）



データの同期方法を定義する

データの整合性の検証方法を定義する

帯域を制御する

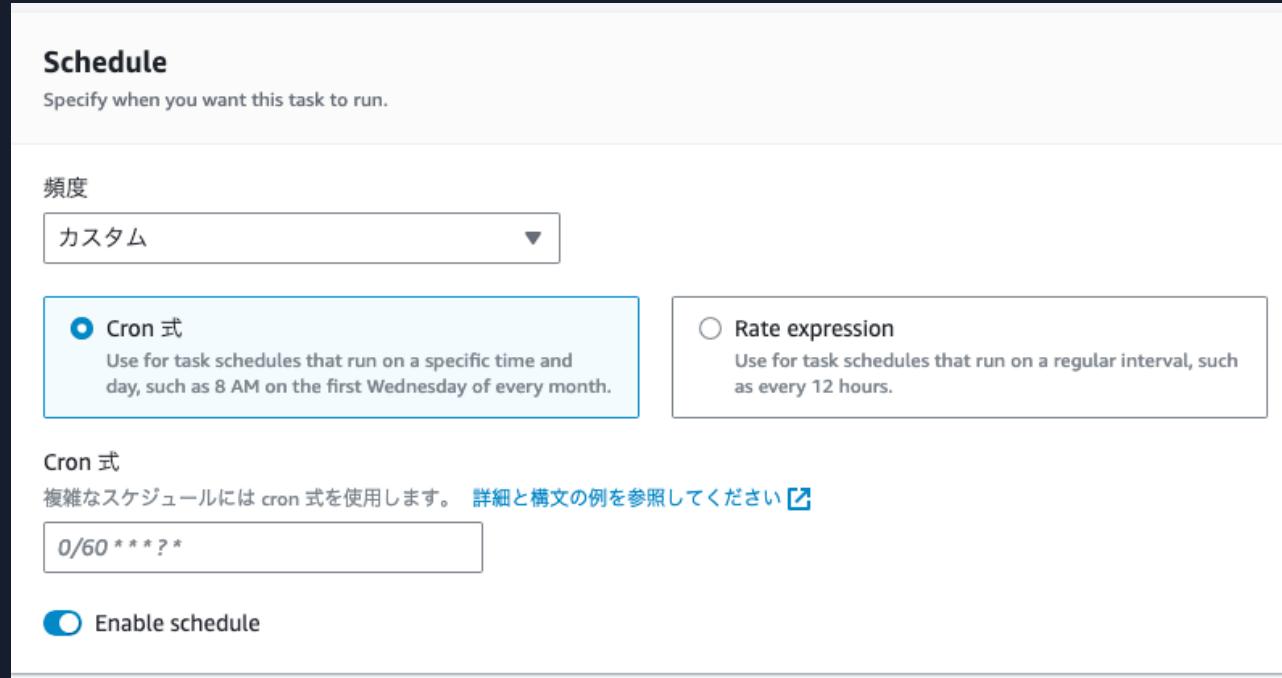
変更したデータだけ送信する際の同期方法を定義する

Amazon EFS 上のファイルの
メタデータをコピーする

キューの有無を設定する
以前のタスクが完了するまで
キューに保存できる

タスクを作成する（4）

スケジュールの設定では、毎時などの頻度や Cron 式に基づいた設定ができる



AWS DataSync では 1 時間未満の間隔でデータの転送をスケジュールすることはできないので注意する

※ 1 時間未満の間隔で、AWS DataSync を用いたデータの転送が必須な場合、以下の方法で実現できる

- ・ タスクを複数作成する
- ・ 定期的なタスクの実行をスクリプトなどで実装する

タスクを作成する (5)

タスク実行のレポートやログを保存できる

Task report - オプション
Get a detailed report for your DataSync transfer task, including specific file names and how much data you moved. Amazon S3 pricing applies. [詳細はこちら](#)

Report type

Logging

ログレベル
CloudWatch Logs に記録される詳細レベルを定義します。CloudWatch Logs の料金は、DataSync によって生成されるログに適用されます。

転送エラーなどの基本情報をログに記録する

CloudWatch Log グループ
エラーやその他の障害などのタスク実行アクティビティをログに記録します。

CloudWatch リソースポリシーを作成する
ロググループにログをアップロードするには、DataSync に十分なアクセス許可を付与するリソースポリシーが必要です。 [詳細はこちら](#)



設定することで、指定した Amazon S3 バケットへと次のいずれかを配信する

- ファイル数などの概要レポート
- ファイルのリストなどの詳細レポート

Amazon CloudWatch Logs へ配信する
ログレベルを設定できる

- エラーなどの基本情報
- 転送した全てのファイル

タスクを実行した際のステータス

タスクを実行した際、Agent が別のタスクを実行中の場合にはタスクのステータスが **Queueing** となる
Launching ではタスクを開始しており、その後 **Preparing** の段階で転送対象のデータを決定する
AWS DataSync は **Transferring** ではデータを転送し、データ転送完了後に **Verifying** で整合性を検証する



AWS DataSync を用いたデータ転送の流れ

(例) NFS ストレージから Amazon S3 へのデータ移行

想定ケース

Amazon EC2 上に Agent をデプロイし、NFS サーバから Amazon S3 へと AWS DataSync を通じてデータを転送する。なお、今回は NFS サーバとして Amazon EFS を利用する※



NFS サーバの起点となるディレクトリ直下に、次のようなメタデータを持つファイルとディレクトリを作成する

```
|drwxr-xr-x. 2 0 0 6144 Aug 23 07:30 dir1
|-rw-r--r--. 1 0 0 1024 Aug 23 07:30 test.dat
```

POSIX permission

User ID と group ID

ファイルの更新日時

※ Amazon EFS は Agent を用いずにロケーションの設定が可能であり、ロケーション作成時に「Amazon EFS」が候補として表示される。しかし、ここでは任意の NFS ストレージを模擬しているため、「NFS」としてロケーションを登録する。

Agent のインストール/アクティベート (1)

Amazon EC2 上へと Agent をインストールする

- (1) 以下のようなコマンドを発行し、AWS DataSync Agent が含まれる AMI ID を取得する

```
aws ssm get-parameter --name /aws/service/datasync/ami --region リージョン名
```

- (2) 取得した AMI を用いて、m5.2xlarge タイプのインスタンスを起動する
この際、HTTP 80 のポートおよび NFS サーバとの通信に必要なポートを開放する
今回はパブリックエンドポイント経由で AWS DataSync と通信するため、Public IP アドレスを付与する

注意: 2,000 万ファイルを超える場合には m5.4xlarge を用意する

Agent のインストール/アクティベート (2)

AWS DataSync のコンソールにおいて、エージェントを作成する

エージェントを作成する

エージェントをデプロイする

セルフマネージドストレージと AWS ストレージサービスの間でデータを転送するには、エージェント VM をデプロイして開始していることを確認してください。エージェントは、オンプレミスのハイパーバイザーまたは Amazon EC2 のいずれかで実行できます。

ハイパーバイザー

ユーザーガイドに記載されている AMI を使用して EC2 インスタンスを作成します。[詳細はこちら](#)

サービスエンドポイント

エンドポイントタイプ
このエージェントが接続するサービスエンドポイントを選択します。[詳細はこちら](#)

US West (Oregon) の公開サービスエンドポイント

アクティベーションキー

アクティベーションは、デプロイしたエージェントを AWS アカウントに安全に関連付けます。[詳細はこちら](#)

エージェントのアクティベーションキーを取得する方法を選択します。[詳細はこちら](#)

エージェントからアクティベーションキーを自動的に取得する
ブラウザは HTTP 経由でエージェントに接続し、一意のアクティベーションキーを取得します。

エージェントのアクティベーションキーを手動で入力する
アクティベーションキーが既にあり、手動で入力する必要がある場合は、このオプションを選択します。

エージェントのアドレス
DataSync エージェントがデプロイされたら、そのドメイン名または IP アドレスを入力します。キーを取得するをクリックすると、ブラウザはこのアドレスに接続して一意のアクティベーションキーを取得します。

http://

このアドレスにブラウザからアクセスできることを確認してください。

[キャンセル](#) [キーを取得する](#)

Agent のインストール/アクティベート (3)

アクティベーションキーが自動的に取得でき、エージェントの作成に成功する

The screenshot shows the AWS DataSync Agent configuration interface. At the top, there's a section for 'サービスエンドポイント' (Service Endpoint) and 'エンドポイントタイプ' (Endpoint Type), which is set to 'US West (Oregon)' public endpoint. Below this, the 'アクティベーションキー' (Activation Key) section shows a checked checkbox indicating successful key retrieval from the agent, with a link to the DataSync > Agent > bb-agent details page. The main table displays the 'bb-agent' entry with its status as 'オンライン' (Online). Other details shown include the service endpoint type as '公開' (Public) and US West (Oregon), the agent ARN, and a creation time of 2024年8月23日 16:49:37 JST.

詳細	エージェントのステータス	Creation time
サービスエンドポイント 公開 US West (Oregon)	オンライン	2024年8月23日 16:49:37 JST
Agent ARN		

タスクの設定

送信元ロケーションを Amazon EFS ではなく、今回は NFS とする
メタデータが送信先ロケーションである Amazon S3 へとコピーされるように設定する

ロケーションタイプ

ネットワークファイルシステム (NFS)

リージョン

US West (Oregon) us-west-2

Transfers to or from NFS must stay in the current Region.

エージェント

選択したエージェントは NFS サーバーにアクセスできる必要があります。

1 つ以上のエージェントを選択する

bb-agent (agent-02dd3b9fc7c43002b) 公開 - US West (Oregon) X

NFS サーバー

ドメイン名または IP アドレス。

マウントパス

NFS サーバーによってエクスポートされたマウントパス、またはエクスポートされたパスのサブディレクトリ。

/

▶ 追加の設定

Transfer options

Transfer mode

Determines whether DataSync transfers only the data and metadata that differ between the source and the destination.

Transfer only data that has changed

Verification

Verify the data in your destination after transfer. DataSync always performs data integrity checks while transferring and writing data.

Verify only the data transferred

Bandwidth limit

Allocate the maximum network bandwidth to be utilized by this task.

Use available

Keep deleted files

Keep files in destination even when deleted from source

Overwrite files

Overwrite files in destination with files from source

▼ 追加の設定

Copy ownership

Maintain user and group ID

Copy permissions

Maintain existing permissions

Copy timestamps

Maintain access time and modification time

Queueing

Allow this task to be started and queued until a previous execution completes.

タスクの開始と完了

タスクを実行する。必要に応じて、履歴からログやステータスを確認する

The screenshot shows the AWS Lambda console interface for a function named "bb-task".

Top Bar: Includes buttons for "開始" (Start), "停止" (Stop), "編集" (Edit), and "削除" (Delete). The "開始" button is highlighted with a yellow box.

Left Sidebar: Shows the function name "bb-task" and a "概要" (Overview) section. It displays the task status as "利用可能" (Available) with a green checkmark, and the Task ARN.

Main View: The main content area is titled "bb-task" and contains the following sections:

- 概要 (Overview):** Displays the task status as "利用可能" (Available), the latest execution date and time as "2024年8月23日 17:05:14 JST", and the creation date as "2024年8月23日 17:04:49 JST".
- 履歴 (History):** Shows a history tab with 1 entry. The entry details are:

実行 ID	開始時刻	期間	ステータス	MIB/秒	ファイル/秒
exec-0406aa30dab5bdf87	2024年8月23日 17:05:14 JST	4 秒	成功	0	1.89

タスクの完了

Amazon S3 上に NFS サーバ上のファイルとディレクトリがコピーされていることが確認できる
また、メタデータも意図した通りに保存される

名前	タイプ	最終更新日時	サイズ	ストレージクラス
.aws-datasync-metadata	aws-datasync-metadata	2024/08/23 05:08:16 PM JST	0 B	スタンダード
dir1/	フォルダ	-	-	-
test.dat	dat	2024/08/23 05:08:16 PM JST	1.0 KB	スタンダード

メタデータ (7)

メタデータは、名前-値(キーと値)のペアとして提供されるオプションの情報です。[詳細](#)

タイプ	キー	値
システム定義	Content-Type	application/octet-stream
ユーザー定義	x-amz-meta-user-agent	aws-datasync/3.8.2831.0-b4a75425
ユーザー定義	x-amz-meta-atime	1724398224584000000ns
ユーザー定義	x-amz-meta-file-owner	0
ユーザー定義	x-amz-meta-file-permissions	100644
ユーザー定義	x-amz-meta-file-group	0
ユーザー定義	x-amz-meta-file-mtime	1724398224584000000ns

- ファイルのアクセス日時
- User ID
- POSIX permission
- group ID
- ファイルの更新日時

他のデータ転送ソリューションとの比較

オンプレミスから AWS へのデータ移行方法

オンライン転送とオフライン転送に別れる

オンライン転送では、AWS マネージドサービス・ツール・スクリプトでの実装という選択肢がある

オンライン転送



スクリプト
robocopy
aws s3
copy



AWS DataSync



Amazon FSx for
NetApp ONTAP
SnapMirror

データ移行を
早く開始したい

安定したネットワーク
帯域が確保できる

Amazon FSx シリーズや
Amazon EFS へ移行したい

移行時のボトルネックは
オンプレミスと AWS 間の
ネットワーク帯域である

移行中にデータを
オフラインにできる

データ移行のスケジュールに
余裕がある

オフライン転送



AWS Snowball Edge
Storage Optimized
210 TB

AWS Snowball Edge を利用する際は
メタデータの取り扱いに注意する

オンライン転送の選択肢

AWS DataSync はエラーハンドリング、データの整合性検証、スケジューリングなどの便利な機能をマネージドサービスとして提供するため、利用することで**楽にデータを AWS へ送信できることがポイント**である

ただし、オンライン転送の手段は、移行元と移行先ストレージ、データ転送の要件に応じて選択する

例 1: NFS サーバから Amazon EFS へと楽にデータを同期したい

AWS DataSync ではスケジュールを設定でき、データの同期方法や整合性確認も機能として提供する

例 2: Amazon FSx for NetApp ONTAP へとデータを送信したい

転送元ストレージが ONTAP である場合、スナップショット単位でブロック転送が可能な SnapMirror の活用が適するケースが多い。AWS DataSync や robocopy はファイル単位での送信となる

例 3: Amazon S3 へとデータを数分ごとの間隔で定期的に送信したい

aws s3 コマンドを用いたスクリプトベースのデータ転送基盤を構築する

※ AWS DataSync のタスクをスケジュール以外の仕組みで実行すれば、実現できる

オンライン転送の選択肢

オンライン転送の手段は、移行元と移行先ストレージ、データ転送の要件に応じて選択する

例えば、移行元と移行先ストレージが同じでも、要件が変われば当然適したツールは変わる

例 4: NFS サーバから Amazon S3 へとデータを転送したい。ただし、メタデータを保存したい

AWS DataSync を用いることで、NFS サーバ上のファイルやディレクトリのメタデータが Amazon S3 上でも保存される

一方で、aws s3 コマンドを用いてメタデータを保存することは困難である

参考

送信元	送信先	コピーされるメタデータ
• NFS	• Amazon S3	<ul style="list-style-type: none">• ファイルとディレクトリの更新日時/アクセス日時• User ID と group ID、POSIX permission

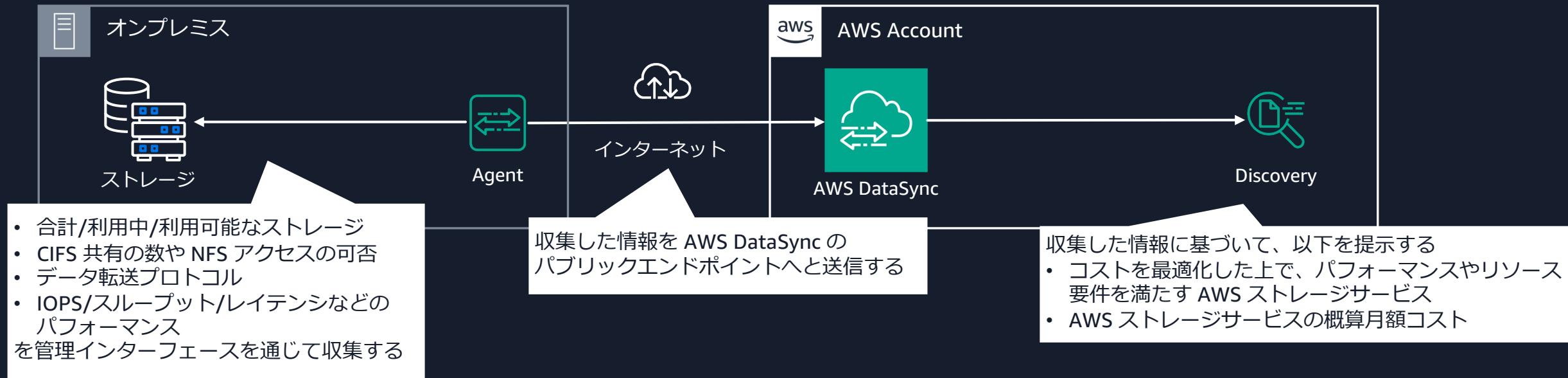
補足と注意点

補足と注意点一覧

1. ストレージの検出
2. Agent と送信元ストレージの組み合わせパターン
3. 複数の Agent を用いることのメリット
4. Agent はどこに配置すべきか
5. 開いたファイルとロックされたファイルの扱い
6. リンクとディレクトリの扱い
7. SMB サーバからデータを転送する際の注意

ストレージの検出（オプション）

AWS DataSync によるストレージの検出を利用し、移行に関する推奨情報を取得できる
Agent はオンプレミスストレージの情報を収集し、AWS DataSync へと送信する



- 本機能を利用する際、AWS DataSync への通信にはパブリックエンドポイントが利用される
- 正確な推奨情報の出力には、14 日間以上の情報収集を推奨する
- Amazon FSx for NetApp ONTAP の Single AZ 構成、Amazon EFS の One Zone ストレージクラス、Amazon FSx for Windows File Server の Single AZ 構成はストレージの検出では考慮しない
- Amazon VPC 内に Agent を配置し、Amazon VPC 内部のリソースに対するストレージの検出もできる

Agent と送信元ストレージの組み合わせパターン

1 vs N

単一の Agent に対して、
複数のストレージを設定する



1 vs 1

単一の Agent に対して、
単一のストレージを設定する



N vs 1

複数の Agent に対して
単一のストレージを設定する



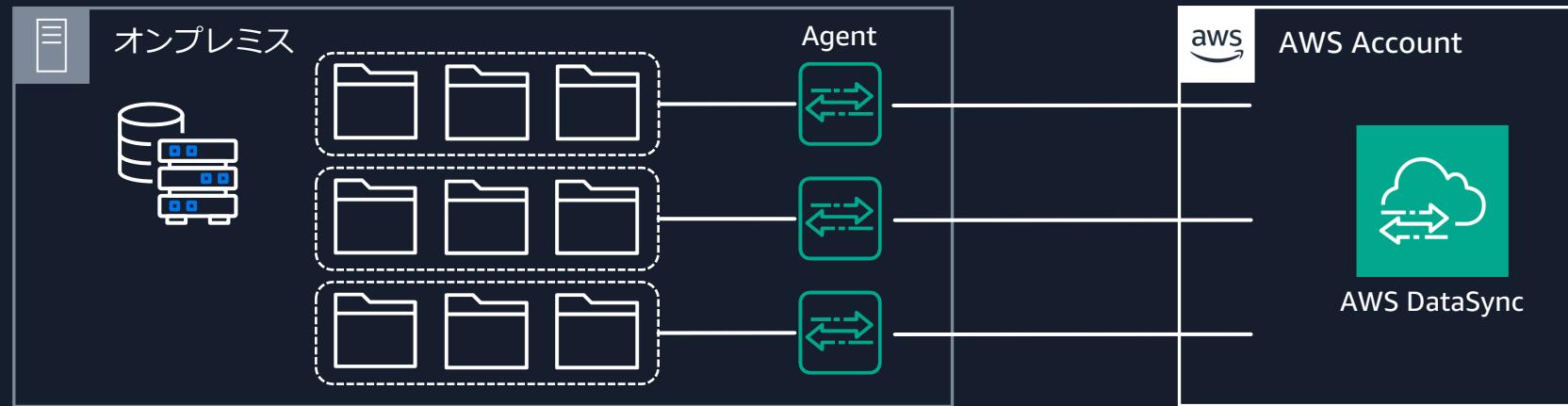
複数のタスクを設定する
タスクは必要に応じ、
キューに入れられる

大規模データの移行が
高速に実現できる

複数の Agent を用いることのメリット

Agent ごとに異なるタスクを設定し並列でデータを転送することで、大規模データの送信を高速化できる

タスクごとに送信元ストレージのマウントパスを分けたり、マニフェストやフィルタを利用してすることで、データセットのタスクごとの区分を明確化できる



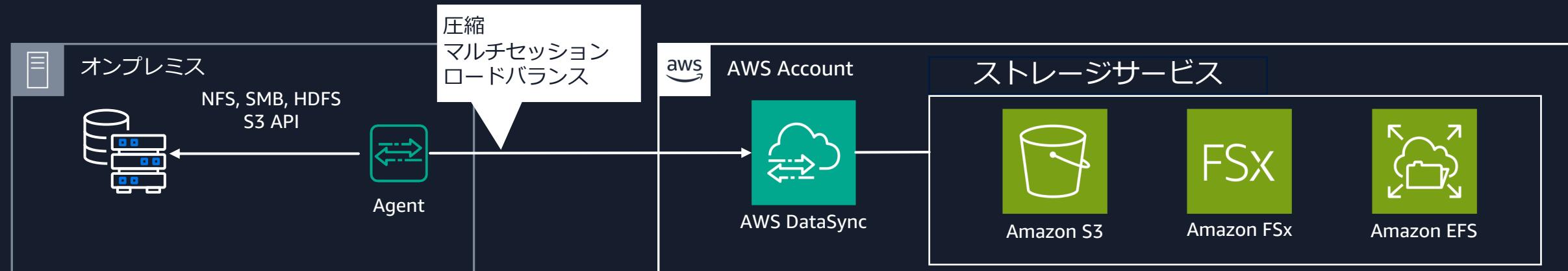
注意点

- 送信元ストレージやネットワークへの負荷が発生する
- Agent はそれぞれ別のタスクを設定するため、可用性を高くすることとは関係がない
- ストレージの検出を行う場合には、1つのストレージに対して Agent は1つのみ設定できる

Agent はどこに配置すべきか

オンプレミスからのデータ移行の場合、送信元ロケーションと近い場所へ配置する

データ送信時に AWS DataSync が実装する圧縮・マルチセッション・ロードバランスの効果範囲が広くなる



仮に Amazon EC2 上に Agent を配置すると、オンプレミスの送信元ストレージと Agent は NFS や SMB などの通信となり、AWS DataSync が提供する圧縮・マルチセッション・ロードバランスの恩恵を受けられない

開いたファイルとロックされたファイルの扱い

開いているファイルとロックされたファイルを AWS DataSync の転送対象とするとき注意する

開いたファイル

通常、AWS DataSync は開いたファイルを送信できる

ただし、転送中にデータが送信元ストレージで編集された場合、データの整合性検証時に不一致と判断する最新のバージョンを送信するためには、タスクを再度実行する

ロックされたファイル

AWS DataSync はファイルのロックまたはロック解除はできない

AWS DataSync がロックされたファイルを開けない場合、そのファイルの転送をスキップし、エラーを記録する



ハードリンクの扱い

ハードリンク、シンボリックリンク、ディレクトリの扱いは送信元と送信先の組み合わせに依存する
一例のみ紹介し、すべてのパターンは[こちら](#)を参照する

ハードリンクの扱いの例

送信元	送信先	ハードリンクの扱い
<ul style="list-style-type: none">• NFS• Amazon EFS• Amazon FSx for NetApp ONTAP (NFS)/Lustre/OpenZFS	<ul style="list-style-type: none">• NFS• Amazon EFS• Amazon FSx for NetApp ONTAP (NFS)/Lustre/OpenZFS	ハードリンクは保存される
<ul style="list-style-type: none">• SMB• Amazon FSx for NetApp ONTAP (SMB)/Windows File Server	<ul style="list-style-type: none">• SMB• Amazon FSx for NetApp ONTAP (SMB)/Windows File Server	ハードリンクはサポートしない。データ転送は完了するものの、ログにエラーが記録される
• 任意のストレージ	<ul style="list-style-type: none">• Amazon S3	ハードリンクとその参照先は別のオブジェクトとして保存される。 Amazon S3 上でハードリンクを変更しなければ※、AWS DataSync を用いて NFS、Amazon EFS、Amazon FSx for NetApp ONTAP (NFS)/Lustre/OpenZFS へ復元した時、ハードリンクも復元できる

※ 例えば、Amazon S3 から参照先ファイルをダウンロードし、再度アップロードした場合、復元時にハードリンクは復元できない。参照先とは異なる inode 番号を示す



ハードリンクを NFS から Amazon S3 へコピー

Amazon EFS 上の source ディレクトリ上に hello.text とそのハードリンクを作成する

```
5930988602823351302 -rwxrwxrwx. 2 root root 6 Aug 24 10:30 hello.lnk  
5930988602823351302 -rwxrwxrwx. 2 root root 6 Aug 24 10:30 hello.text
```

同じ inode 番号

AWS DataSync でこれらのファイルを Amazon S3 へ送信すると、ハードリンクと参照先が作成される

<input type="checkbox"/>	 hello.lnk	lnk	2024/08/24 07:34:20 PM JST	6.0 B	スタンダード
<input type="checkbox"/>	 hello.text	text	2024/08/24 07:34:20 PM JST	6.0 B	スタンダード

Amazon EFS 上の hello.text を変更し再度タスクを実行すると、共に更新される

<input type="checkbox"/>	 hello.lnk	lnk	2024/08/24 07:39:22 PM JST	6.0 B	スタンダード
<input type="checkbox"/>	 hello.text	text	2024/08/24 07:39:22 PM JST	6.0 B	スタンダード

Amazon EFS 上の target ディレクトリ上へ、AWS DataSync で復元するとハードリンクは保持されている

```
9934453109177352605 -rwxrwxrwx. 2 root root 6 Aug 24 10:35 hello.lnk  
9934453109177352605 -rwxrwxrwx. 2 root root 6 Aug 24 10:35 hello.text
```

同じ inode 番号

aws s3 コマンドで復元すると、ハードリンクは保持されないので注意する



シンボリックリンクとディレクトリの扱い

ハードリンク、シンボリックリンク、ディレクトリの扱いは送信元と送信先の組み合わせに依存する
一例のみ紹介し、すべてのパターンは[こちら](#)を参照する

シンボリックリンクの扱いの例

送信元	送信先	シンボリックリンクの扱い
<ul style="list-style-type: none">NFSAmazon EFSAmazon FSx for NetApp ONTAP (NFS)/ Lustre/OpenZFS	<ul style="list-style-type: none">NFSAmazon EFSAmazon FSx for NetApp ONTAP (NFS)/ Lustre/OpenZFS	シンボリックリンクは保存される
<ul style="list-style-type: none">SMBAmazon FSx for NetApp ONTAP (SMB)/ Windows File Server	<ul style="list-style-type: none">SMBAmazon FSx for NetApp ONTAP (SMB)/ Windows File Server	シンボリックリンクはサポートしない 転送は完了するが、ログにエラーが記録される
<ul style="list-style-type: none">任意のストレージ	<ul style="list-style-type: none">Amazon S3	ターゲットパスは保存される NFS、Amazon EFS、Amazon FSx for NetApp ONTAP (NFS)/ Lustre/OpenZFS へ復元した時、リンクも復元できる

ディレクトリの扱いの例

送信元	送信先	ディレクトリの扱い
<ul style="list-style-type: none">任意のストレージ	<ul style="list-style-type: none">Amazon S3	/ がパスの末尾となる空のオブジェクトとして、登録される test という空のディレクトリを送信した場合の挙動の例: 

SMB サーバからデータを転送する際の注意

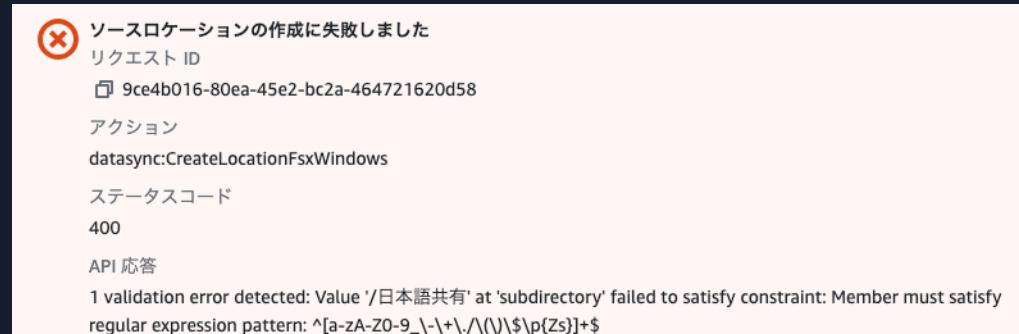
SMB サーバをマウントし、ファイル・フォルダ・メタデータを読み取れる権限が必要である
特に Microsoft Active Directory を利用している場合、次の権限が必要である

ユーザー権限	説明
Restore files and directories (SE_RESTORE_NAME)	オブジェクト所用者、権限、ファイルメタデータ、NTFS DACLs を AWS DataSync がコピーする際に必要である 通常は、Domain Admins または Backup Operators グループに所属している
Manage auditing and security log (SE_SECURITY_NAME)	AWS DataSync が NTFS SACLs をコピーする際に利用する 通常は Domain Admins グループに所属している

DFS 名前空間はサポートしない

AWS DataSync の SMB サーバへのアクセスには、Kerberos 認証は使えない。代わりに NTLM 認証を用いる

ファイル共有名が日本語の場合、ロケーションの作成ができない（2024 年 8 月 23 日現在）



まとめ

- AWS DataSync を用いることで、AWS ストレージサービスとオンプレミス、他クラウドサービス間でデータの移動を実現できる
- データの整合性の検証・差分同期・スケジューリング・帯域制御・エラーハンドリング・圧縮などのデータ転送時に便利な機能を、AWS DataSync はマネージドサービスとして提供する
- データを送信する際には、送信元と送信先ストレージの組み合わせや要件に応じて適切な手段を選択する

Thank you!



AWS Black Belt Online Seminar

AWS Fargate 入門

吉田 英史

Solutions Architect

2024/10



自己紹介

吉田 英史

アマゾンウェブサービスジャパン
ソリューションアーキテクト

小売・消費財のお客様を中心にご支援しています。
生活に欠かせない様々なビジネスをクラウドで加速するお手伝いができるなどを、何より嬉しく感じています。

好きな AWS サービス
AWS Fargate



本セミナーの主な対象者

- ・ これから AWS を利用される予定の、アプリケーションおよびインフラ担当者
- ・ サーバレスコンテナ実行環境である、AWS Fargate の概要や始め方を知りたい方
- ・ クラウド上の既存ワークロードの、コンテナ化を検討している方
- ・ オンプレミスの既存コンテナワークロードの、クラウド移行を検討している方

アジェンダ

1. AWS Fargate とは
2. AWS Fargate と Amazon EC2 の違い
3. AWS Fargate の始め方
4. まとめ

AWS Fargate とは

AWS のコンテナサービス

オーケストレーション

コンテナのデプロイ、スケジューリング、スケーリング



Amazon ECS



Amazon EKS

イメージレジストリ

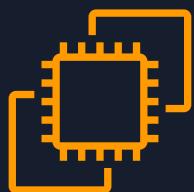
コンテナイマークの格納



Amazon ECR

ホスティング

コンテナ実行環境



Amazon EC2



AWS Fargate

その他の関連サービス



AWS App Runner



AWS Cloud Map



Amazon CloudWatch
Container Insights

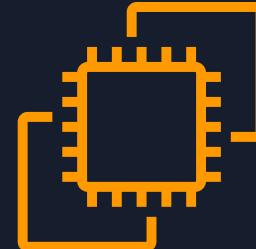
コンテナ実行環境の選択肢

コンテナ
オーケストレーター
(コントロールプレーン)

コンテナの実行環境
(データプレーン)



Amazon ECS



Amazon EC2



Amazon EKS



AWS Fargate

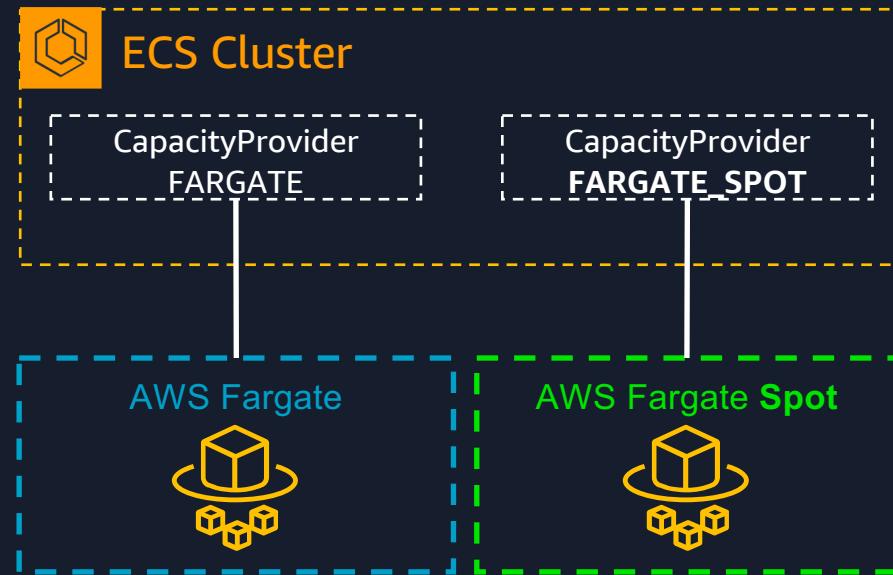
AWS Fargate はサーバレスのコンテナ実行環境



- ホストのアップグレード、パッチ適用が対応不要
- クラスターのキャパシティ管理が不要
- 設計による分離とセキュリティの担保
- 前払い料金なし、利用リソースに応じた従量課金
※ Compute Savings Plans 対象
- Fargate Spot と Fargate Graviton によるコスト削減
※ Amazon EKS では未サポート

AWS Fargate Spot (ECS のみ)

- AWS Fargate で中斷処理に強いワークロードを実行するためのオプション
- 通常の Fargate の価格と比較して最大 70% 割引
- Capacity Provider の FARGATE_SPOT キャパシティとして利用可能
- AWS Graviton も利用可能



https://docs.aws.amazon.com/ja_jp/AmazonECS/latest/developerguide/fargate-capacity-providers.html

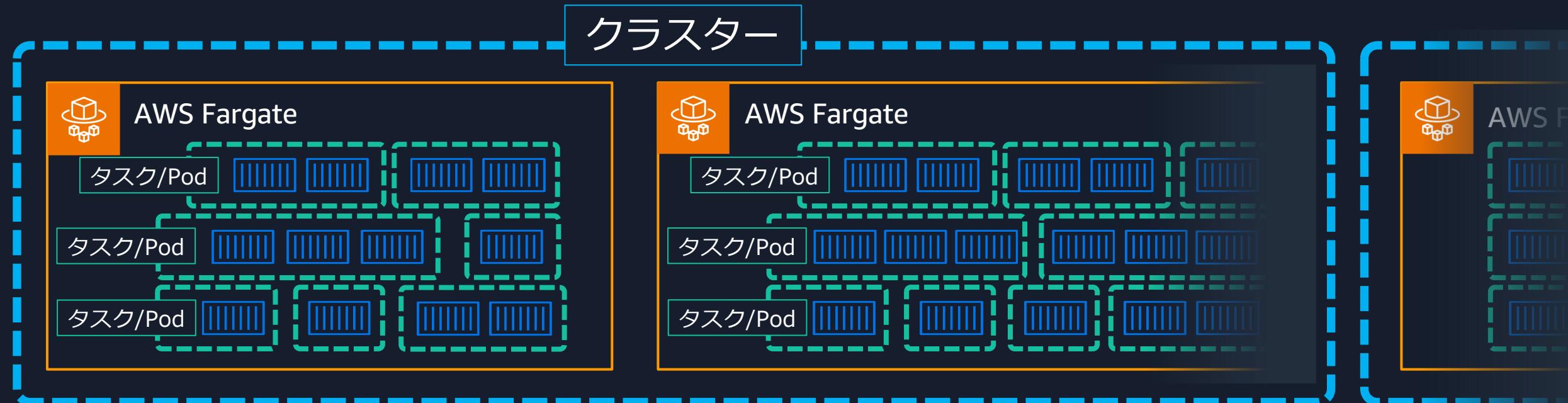
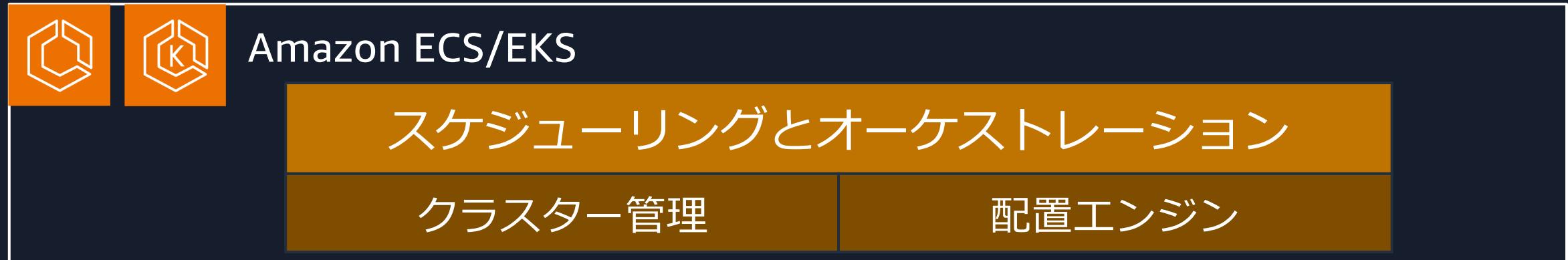
<https://aws.amazon.com/jp/about-aws/whats-new/2024/09/amazon-ecs-graviton-based-spot-compute-fargate/>

ECS/EKS におけるコンテナ実行環境の比較



Fargate を活用することで、アプリケーションコンテナの開発に集中できる

Amazon ECS/EKS on Fargate の動作イメージ

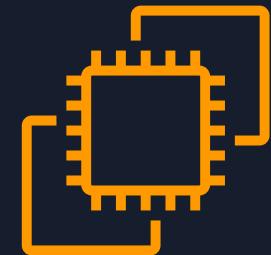


AWS Fargate と Amazon EC2 の違い

Amazon EC2 との違い

AWS Fargate と Amazon EC2 で異なる **5** つの観点

1. vCPU とメモリ
2. ホスト
3. ネットワークモード
4. データボリューム
5. セキュリティ



Amazon EC2

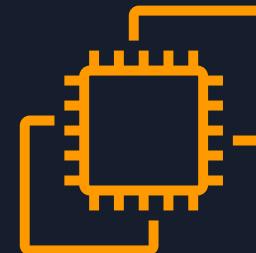


AWS Fargate

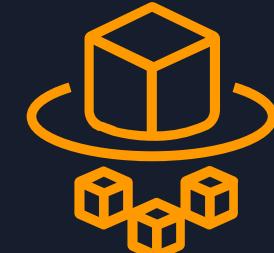
Amazon EC2 との違い

AWS Fargate と Amazon EC2 で異なる **5** つの観点

1. vCPU とメモリ
2. ホスト
3. ネットワークモード
4. データボリューム
5. セキュリティ



Amazon EC2



AWS Fargate

タスク/Pod に割り当てる vCPU とメモリ設定

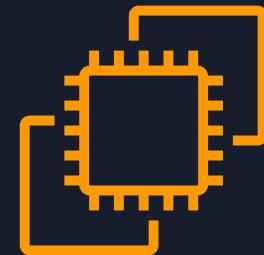
vCPU	Memory	
256 (.25 vCPU)	0.5GB, 1GB, 2GB	→ 3 種類
512 (.5 vCPU)	1GB ~ 4GB (1GB 刻み)	→ 4 種類
1,024 (1 vCPU)	2GB ~ 8GB (1GB 刻み)	→ 7 種類
2,048 (2 vCPU)	4GB ~ 16GB (1GB 刻み)	→ 13 種類
4,096 (4 vCPU)	8GB ~ 30GB (1GB 刻み)	→ 23 種類
8,192 (8 vCPU)	16GB ~ 60GB (4GB 刻み)	→ 12 種類
16,384 (16 vCPU)	32GB ~ 120GB (8GB 刻み)	→ 12 種類

柔軟な設定の選択肢 : 74 パターン の vCPU, メモリの組み合わせから選択可能

Amazon EC2 との違い

AWS Fargate と Amazon EC2 で異なる **5** つの観点

1. vCPU とメモリ
2. ホスト
3. ネットワークモード
4. データボリューム
5. セキュリティ



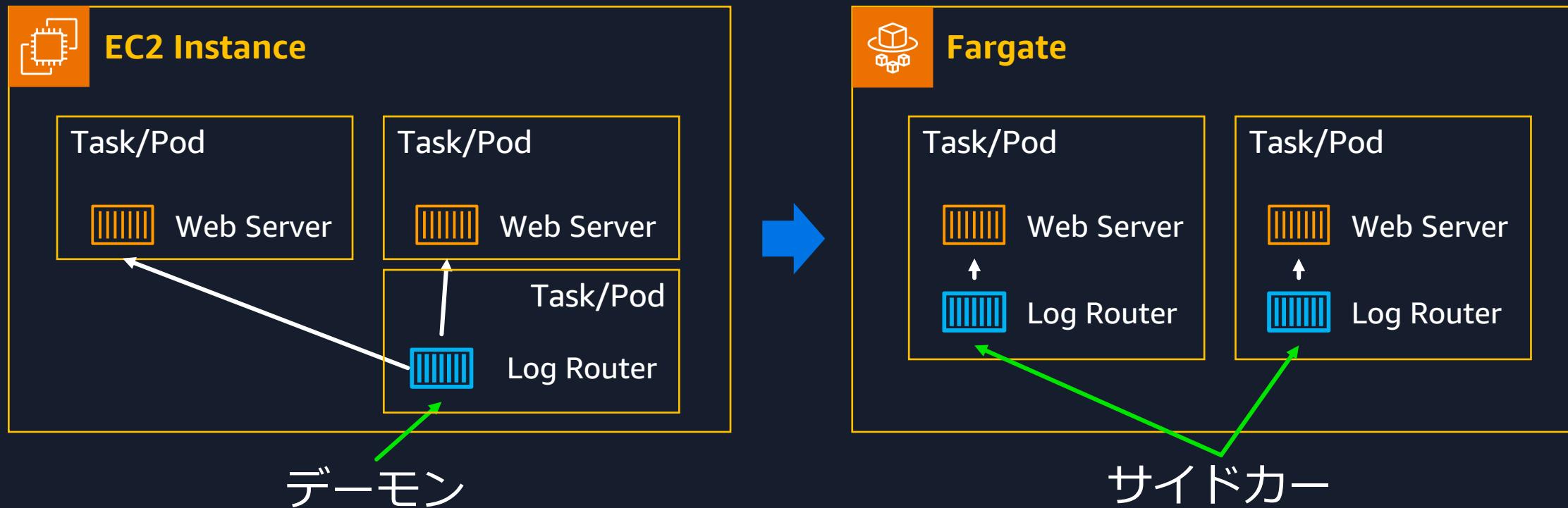
Amazon EC2



AWS Fargate

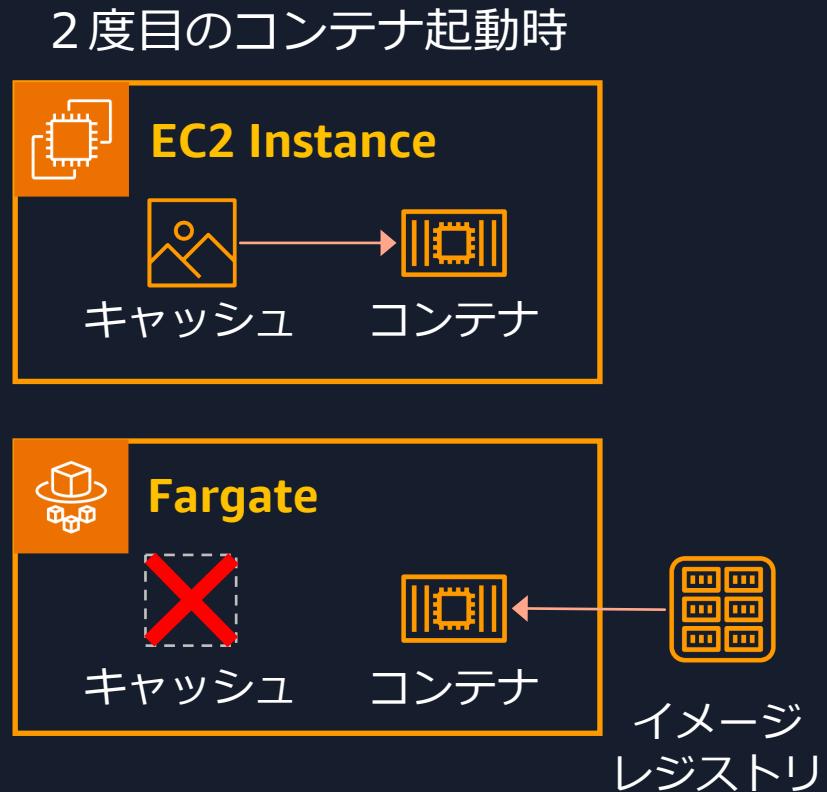
ホスト環境の違いによる Fargate の制約 1/2

- GPU など、ハードウェアアクセラレーターが未サポート (2024年9月時点)
- デーモンスケジューリング戦略 (ECS)、デーモンセット (EKS) はサポート外
→ サイドカーパターンに



ホスト環境の違いによる Fargate の制約 2/2

- Fargate はホストを都度作り直すため、コンテナイメージを Pull する際にローカルキャッシュが使用できない
→ コンテナ起動時間の短縮のアイデア
 - イメージサイズの最適化
 - イメージの圧縮
 - 遅延読み込み Seekable OCI (SOCI) (ECS のみ)



zstd 圧縮したコンテナイメージを使用して AWS Fargate の起動時間を短縮する

<https://aws.amazon.com/jp/blogs/news/reducing-aws-fargate-startup-times-with-zstd-compressed-container-images/>

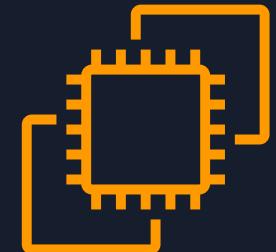
AWS Fargate はシーク可能な OCI を使用してより高速なコンテナ起動を可能に

<https://aws.amazon.com/jp/blogs/news/aws-fargate-enables-faster-container-startup-using-seekable-oci/>

Amazon EC2 との違い

AWS Fargate と Amazon EC2 で異なる **5** つの観点

1. vCPU とメモリ
2. ホスト
3. **ネットワークモード**
4. データボリューム
5. セキュリティ



Amazon EC2



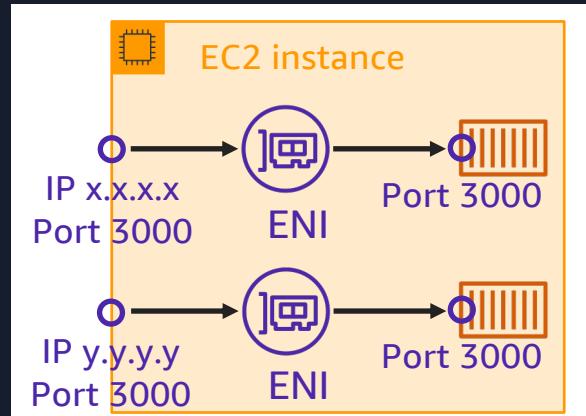
AWS Fargate

利用可能なネットワークモード

Fargate
実行環境

awsVpc モード

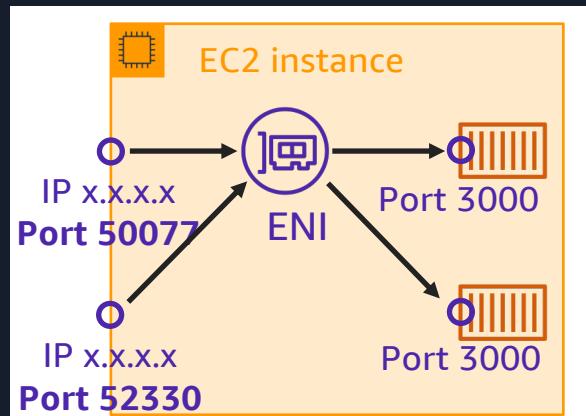
- ECS/EKS 管理下の ENI（仮想サーバーの仮想ネットワークカード）がタスクにアタッチされる



EC2
実行環境

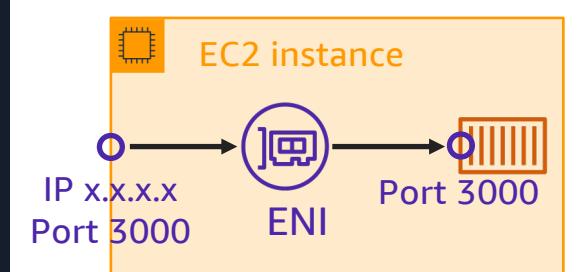
bridge モード

- 仮想ネットワークブリッジを利用してホスト/コンテナポートをマッピングして通信



host モード

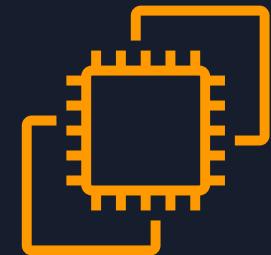
- コンテナをホストしている EC2 インスタンスの IP/ポートを介して通信



Amazon EC2 との違い

AWS Fargate と Amazon EC2 で異なる **5** つの観点

1. vCPU とメモリ
2. ホスト
3. ネットワークモード
4. データボリューム
5. セキュリティ



Amazon EC2



AWS Fargate

利用可能なデータボリューム

Fargate 実行環境

Fargate バインドマウント / エフェメラルストレージ

- 揮発性のストレージをコンテナにマウントし、コンテナ間で共有
- 使用するすべてのコンテナが停止するとデータが削除される
- 20GiB まで無料、追加分にのみ課金 (ECS Max 200GiB / EKS Max 175GiB)

Amazon EBS ボリューム (Fargate は ECS のみ)

- 高スループットなトランザクション集約型アプリケーション向け
- タスクごとに1つの EBS ボリュームにアタッチ可能

Amazon EFS ボリューム

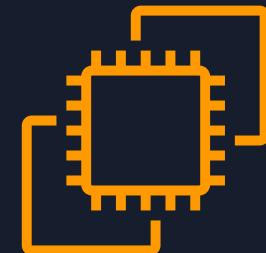
- ストレージ容量が伸縮自在で、自動的に拡大および縮小される

Amazon ECS: https://docs.aws.amazon.com/ja_jp/AmazonECS/latest/developerguide/using_data_volumes.html
Amazon EKS: https://docs.aws.amazon.com/ja_jp/eks/latest/userguide/storage.html

Amazon EC2 との違い

AWS Fargate と Amazon EC2 で異なる **5** つの観点

1. vCPU とメモリ
2. ホスト
3. ネットワークモード
4. データボリューム
5. **セキュリティ**



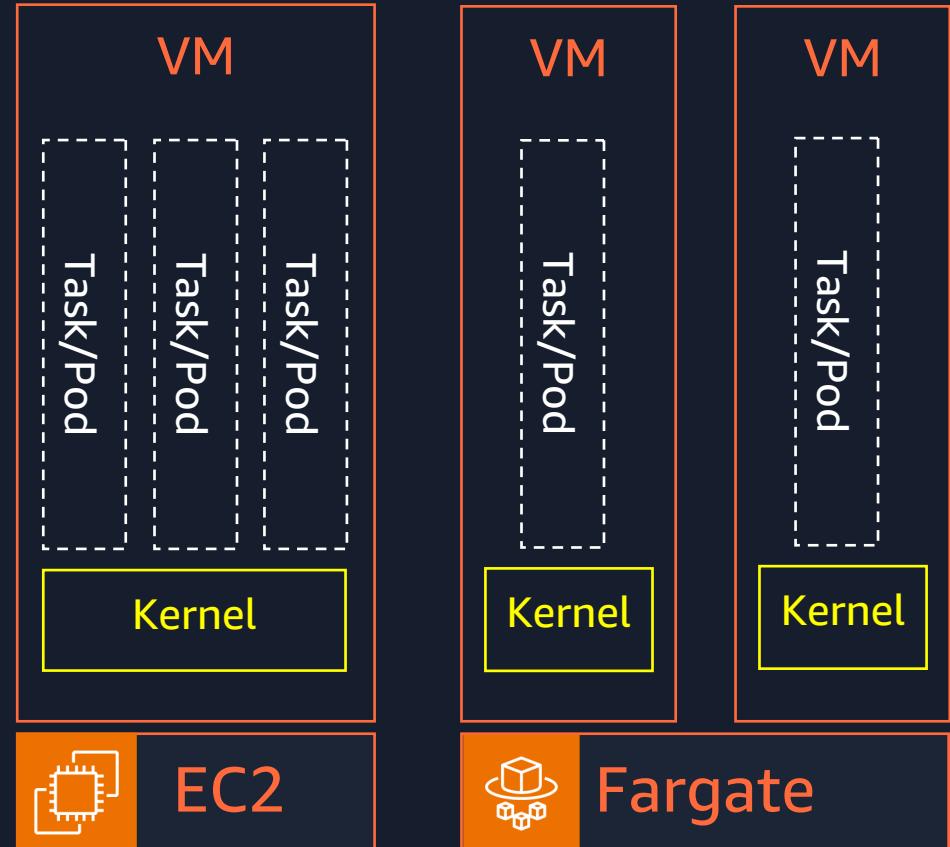
Amazon EC2



AWS Fargate

セキュリティにおける Fargate のメリット

- OS、コンテナエンジン、エージェントなどのパッチ当てが不要
- タスク/Pod ごとに実行環境が分離されている
- コンテナに特権モードが使用できない
- awsvpc ネットワークモードのため ENI や SG がタスク/Pod ごとに独立
- ssh などによるホストへのアクセスが不可能

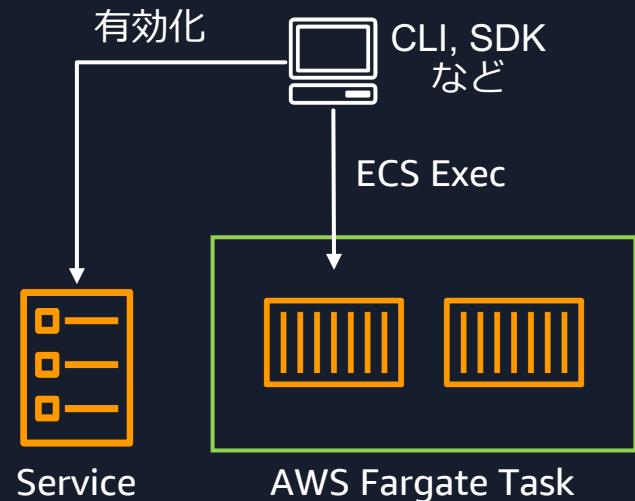


Fargate セキュリティのベストプラクティス

https://docs.aws.amazon.com/ja_jp/AmazonECS/latest/developerguide/security-fargate.html

Fargate 上のコンテナのデバッグ (ECS のみ)

- Fargate 上のコンテナにログインするには **ECS Exec** を使用
- AWS Systems Manager セッションマネージャーを使用するため、事前にプラグインの導入が必要



※ 2024/09 時点でコンソールからの有効化は未対応
ECS Exec を使用して Amazon ECS コンテナをモニタリングする
https://docs.aws.amazon.com/ja_jp/AmazonECS/latest/developerguide/ecs-exec.html

```
aws ecs execute-command ¥
--cluster cluster-name ¥
--task task-id ¥
--container container-name ¥
--interactive ¥
--command "/bin/sh"
```

AWS Fargate の始め方

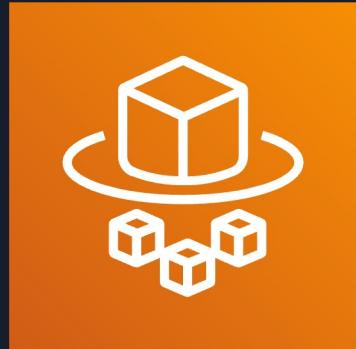
AWS Fargate の始め方

- AWS Fargate の開始方法
 - <https://aws.amazon.com/jp/fargate/getting-started/>
- AWS Fargate の料金
 - <https://aws.amazon.com/jp/fargate/pricing/>
- Amazon ECS/AWS Fargate 利用構成と料金試算例
 - <https://aws.amazon.com/jp/cdp/ec-container/>
- AWS Fargate のお客様導入事例
 - <https://aws.amazon.com/jp/containers/customers/>
- AWS Fargate に関する AWS Blog 記事
 - <https://aws.amazon.com/jp/blogs/news/tag/aws-fargate/>

The screenshot shows the AWS Fargate Getting Started page. At the top, there's a navigation bar with links for AWSについて, お問い合わせ, サポート, 日本語, アカウント, and ログイン. Below the navigation, there's a breadcrumb trail: 製品 > コンピューティング > AWS Fargate > AWS Fargate の開始方法. The main content area has a title "AWS Fargate の開始方法". It features a video thumbnail titled "AWS Fargate の概要の動画" with a play button. Below the video, there's a section titled "ドキュメント" with links to "AWS Fargate ユーザーガイド", "AWS Fargate を使用した Amazon ECS デベロッパーガイド", "AWS Fargate を使用した Amazon ECS コンソールの開始方法", and "Amazon ECS を使用した AWS Fargate の開始方法". There's also a "チュートリアル" section with a box titled "AWS Fargate のご紹介" containing text about getting started with Fargate and its integration with Amazon ECS. To the right, there are sections for "料金に関するリソース" (including links to AWS Cloud Economics Center and Pricing计算器), "ホワイトペーパー" (including a link to AWS Fargate Security Best Practices), and "Amazon ECS Copilot を使用して AWS Fargate の使用を開始する" (with a link to "構築を開始する"). A small orange speech bubble icon with the number "1" is located in the bottom right corner.

まとめ

- AWS Fargate とは
 - サーバレスのコンテナ実行環境
 - コンテナクラスターの運用負荷を軽減することが可能
- AWS Fargate の、Amazon EC2 と異なる 5 つの観点
 - vCPUとメモリ / ホスト / ネットワーク / ボリューム / セキュリティ
 - タスク定義の詳細
- Amazon ECS の始め方



AWS Black Belt Online Seminar とは

- ・ 「サービス別」「ソリューション別」「業種別」などのテーマに分け、
アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナーシリーズです
- ・ AWS の技術担当者が、 AWS の各サービスやソリューションについてテーマごとに動画を公開します
- ・ 以下の URL より、過去のセミナー含めた資料などをダウンロードすることができます
 - <https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/>
 - <https://www.youtube.com/playlist?list=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBlqY>



ご感想は X (Twitter) へ！ハッシュタグは以下をご利用ください
#awsblackbelt

内容についての注意点

- ・ 本資料では資料作成時点のサービス内容および価格についてご説明しています。AWS のサービスは常にアップデートを続けているため、最新の情報は AWS 公式ウェブサイト (<https://aws.amazon.com/>) にてご確認ください
- ・ 資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます
- ・ 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます
- ・ 技術的な内容に関しましては、有料の [AWS サポート窓口](#)へお問い合わせください
- ・ 料金面でのお問い合わせに関しては、[カスタマーサポート窓口](#)へお問い合わせください (マネジメントコンソールへのログインが必要です)

Thank you!



AWS Black Belt Online Seminar

Amazon ECS 入門

吉田 英史

Solutions Architect

2024/08



自己紹介

吉田 英史

アマゾンウェブサービスジャパン
ソリューションアーキテクト

小売・消費財のお客様を中心にご支援しています。
生活に欠かせない様々なビジネスをクラウドで加速するお手伝いができるなどを、何より嬉しく感じています。

好きな AWS サービス
AWS Fargate



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.



本セミナーの主な対象者

- これから AWS を利用される予定の、アプリケーションおよびインフラ担当者
- Amazon Elastic Container Service (Amazon ECS) の概要や始め方を知りたい方
- クラウド上の既存ワークロードの、コンテナ化を検討している方
- オンプレミスの既存コンテナワークロードの、クラウド移行を検討している方

アジェンダ

1. Amazon Elastic Container Service (Amazon ECS) とは
2. Amazon ECS の構成
3. Amazon ECS の始め方
4. まとめ

Amazon Elastic Container Service (Amazon ECS) とは

AWS のコンテナサービス

オーケストレーション

コンテナのデプロイ、スケジューリング、スケーリング



Amazon ECS



Amazon EKS

イメージレジストリ

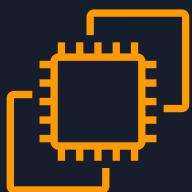
コンテナイマークの格納



Amazon ECR

ホスティング

コンテナ実行環境



Amazon EC2



AWS Fargate

その他の関連サービス



AWS App Runner



Amazon CloudWatch
Container Insights



AWS Cloud Map

Amazon ECS: フルマネージドコンテナサービス

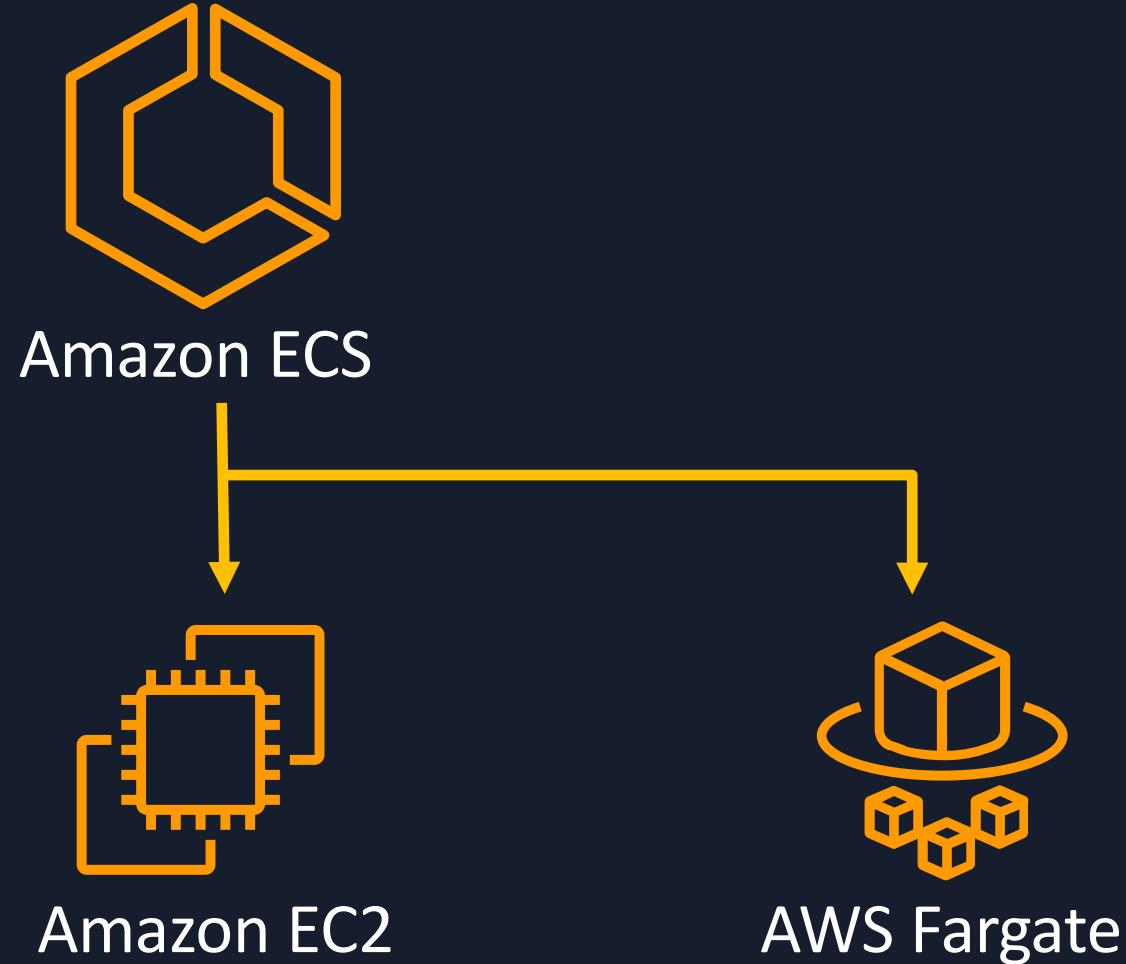


- ミドルウェアへのパッチ、アップグレード、セキュリティ対応不要
- 他の AWS サービスとのネイティブな統合
- ログ、メトリクス、イベントを最初からサポート
- グローバルに利用可能で、パフォーマンスが高く、スケーラブル
- 追加料金不要！

コンテナ実行環境の選択肢

コンテナ
オーケストレーター
(コントロールプレーン)

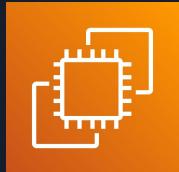
コンテナの実行環境
(データプレーン)



Amazon ECS におけるコンテナ実行環境

ECS on EC2

(コンテナを仮想サーバー上で動作)



アプリケーションコンテナ

ホストのスケーリング

コンテナエージェント設定

ホスト OS / ライブラリ設定

ECS on Fargate

(コンテナをサーバーレスで動作)



アプリケーションコンテナ

ホストのスケーリング

コンテナエージェント設定

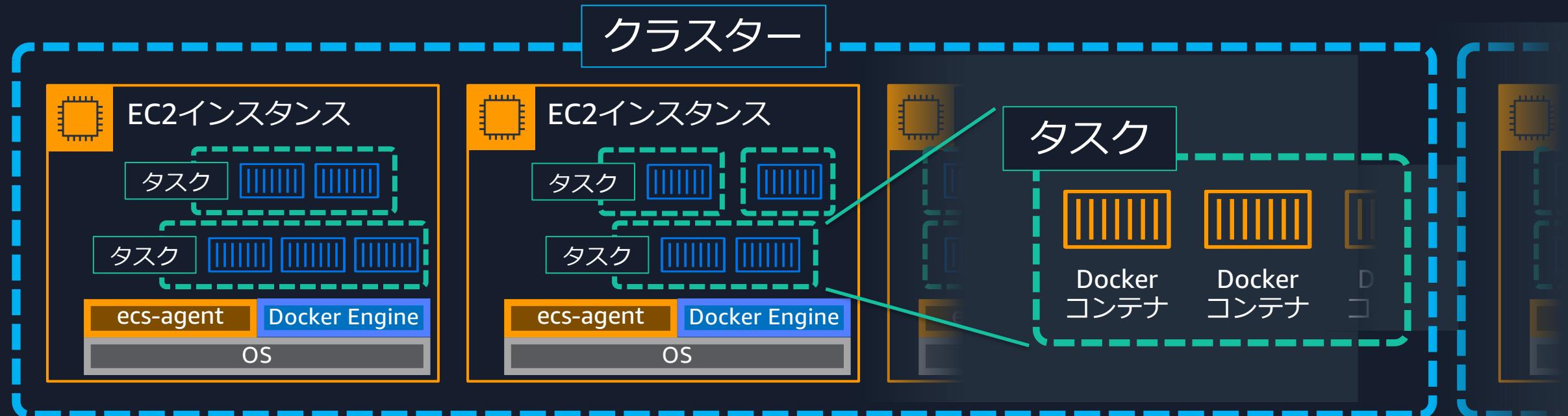
ホスト OS / ライブラリ設定

お客様が管理するレイヤー

AWSが提供するレイヤー

Fargateを活用するとアプリケーションコンテナの開発に集中できる

Amazon ECS の動作イメージ (on EC2)



Amazon ECS (on EC2) の特徴と課題

特徴

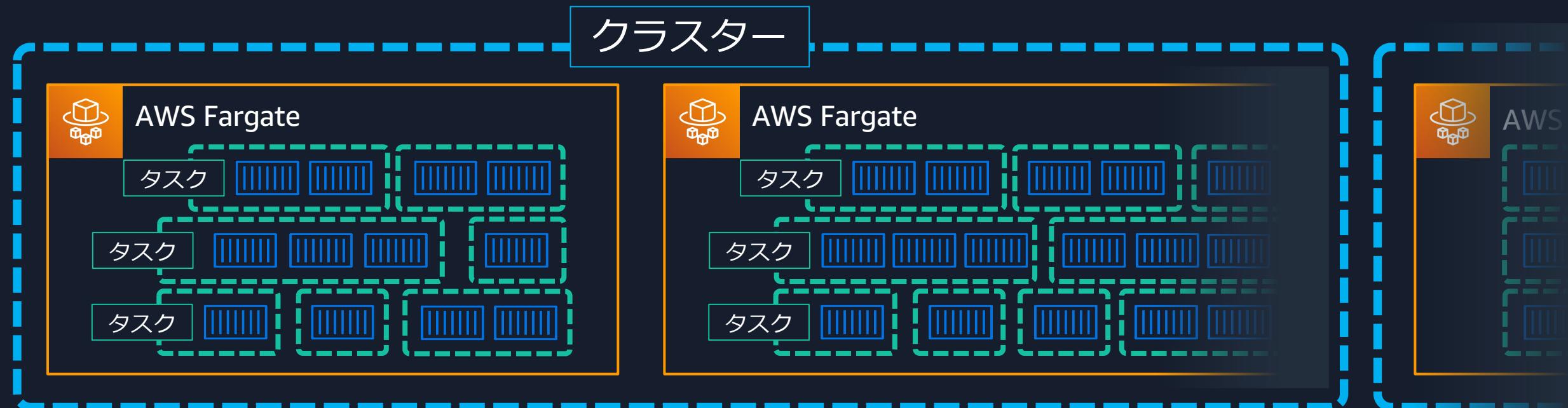
- コンテナホストを自由に選択、設定できる
- CPU、メモリ、ディスク、OS、バージョンなど
- ネットワークモードの選択 (外部接続しない、ホストのネットワークを利用、ENIへのアタッチなど)
- 柔軟なデータボリューム利用

課題

- コンテナホストの管理が必要
- OSやエージェント類へのパッチ当てや更新
- EC2インスタンス数のスケーリング

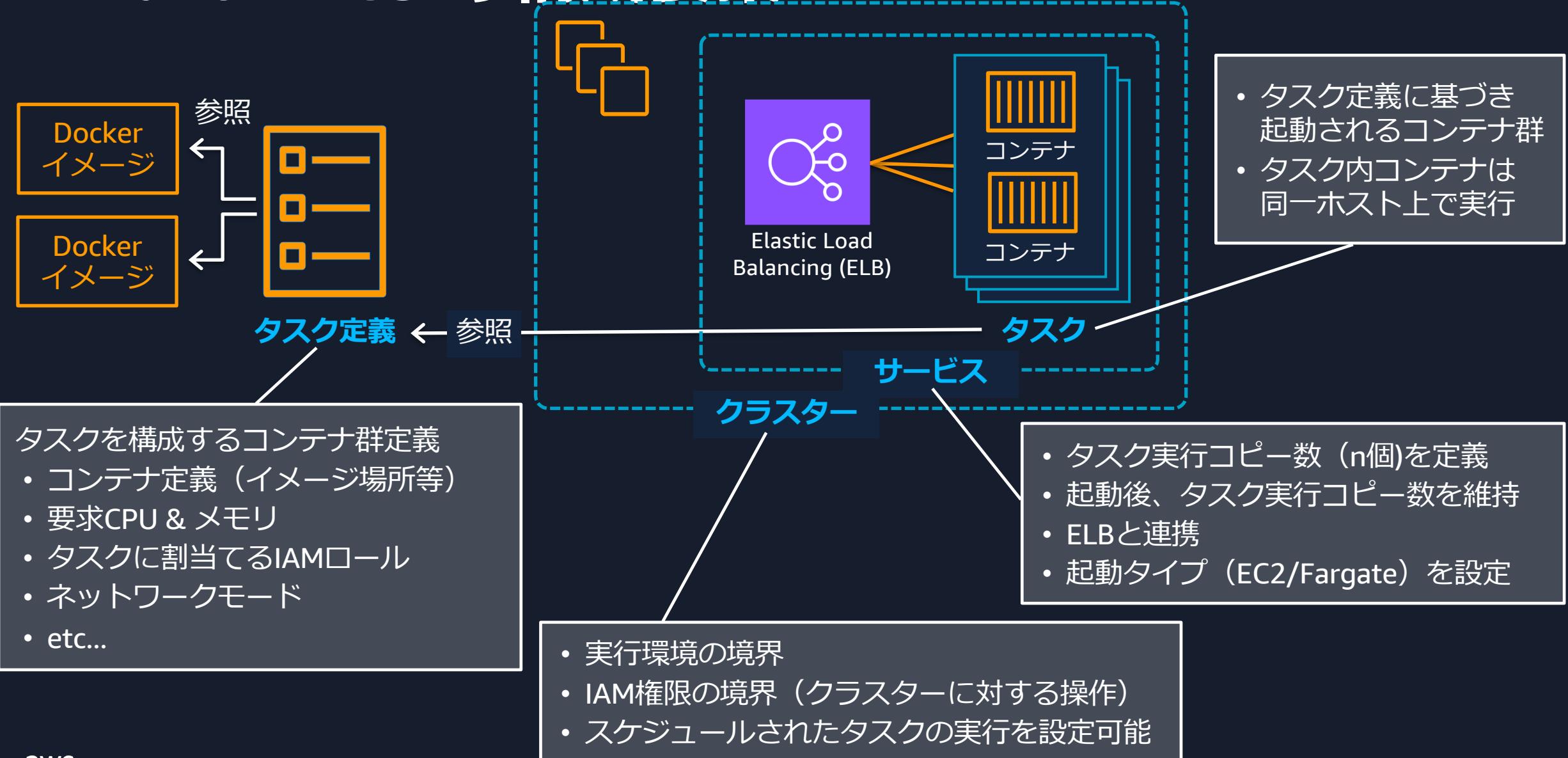
- ✓ Amazon ECS **on Fargate** で解決
 - ✓ コンテナホストがマネージドになるため、トレードオフがある

Amazon ECS の動作イメージ (on Fargate)

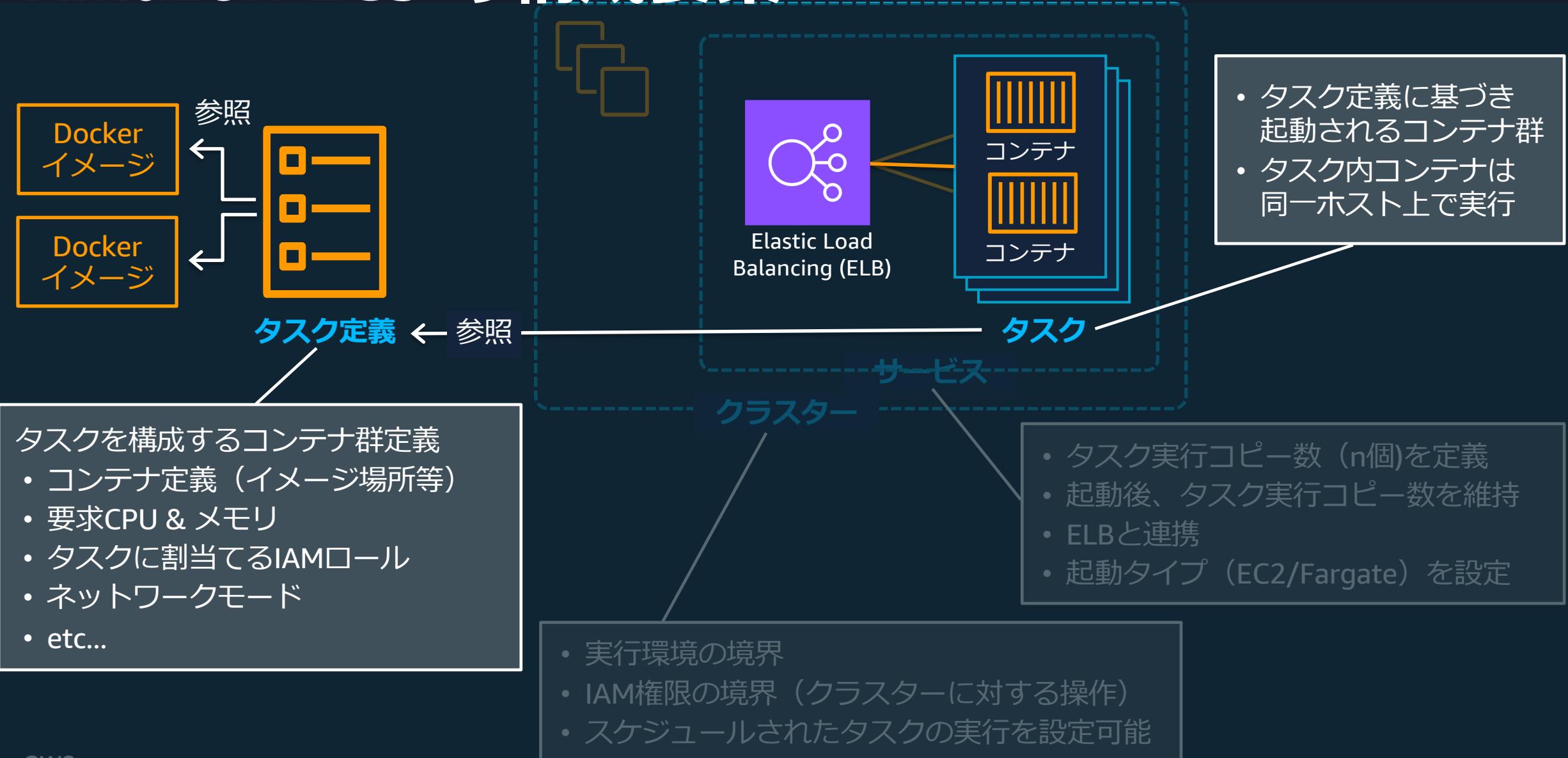


Amazon ECS の構成

Amazon ECS の構成要素



Amazon ECS の構成要素



タスク定義 = コンテナ(群)の実行単位定義

タスクとしてのまとまりを
所定の JSON 書式で定義したもの

- 例 : Front-end サービス、 Back-end サービス、 ...
- family と revision (1から始まる数)で特定

スタンドアロンタスク or サービスによって、
タスク定義から起動される

- 1つ以上のコンテナを実行するリソース
- タスク内のコンテナ群は必ず同じホスト上で実行
- 1つのタスク定義は最大 10 コンテナ指定可能

タスク定義

```
{  
  "family": "scorekeep",  
  "containerDefinitions": [  
    {  
      "name": "scorekeep-frontend",  
      "image": "xxx.dkr.ecr.us-east-1.amazonaws.com/fe"  
    },  
    {  
      "name": "scorekeep-api",  
      "image": "xxx.dkr.ecr.us-east-1.amazonaws.com/api"  
    }  
]  
}
```

実行

タスク



タスク定義 | 代表的なパラメータ

必須

1. ファミリー (family)
2. コンテナ定義 (containerDefinitions)

オプション

3. タスクサイズ (cpu / memory)
4. タスクロール (taskRoleArn)
5. タスク実行ロール (executionRoleArn)
6. ネットワークモード (networkMode)
7. ボリューム (volumes)

```
{  
  "family": "",  
  "taskRoleArn": "",  
  "executionRoleArn": "",  
  "networkMode": "none",  
  "containerDefinitions": [...],  
  "volumes": [...],  
  "placementConstraints": [...],  
  "requiresCompatibilities": [...],  
  "cpu": "",  
  "memory": "",  
  "tags": [...],  
  "pidMode": "host",  
  "ipcMode": "host",  
  "proxyConfiguration": {...}  
}
```



タスク定義 | ファミリー

必須

1. ファミリー (family)
2. コンテナ定義 (containerDefinitions)

- ・タスク定義の名前のようなもの
- ・タスク定義を登録する際に必ず指定する
- ・ファミリーとリビジョン番号(最初は1)で1つのタスク定義が特定される

7. ボリューム (volumes)

```
{  
  "family": "",  
  "taskRoleArn": "",  
  "executionRoleArn": "",  
  "networkMode": "none",  
  "containerDefinitions": [...],  
  "volumes": [...],  
  "placementConstraints": [...],  
  "requiresCompatibilities": [...],  
  "cpu": "",  
  "memory": "",  
  "tags": [...],  
  "pidMode": "host",  
  "ipcMode": "host",  
  "proxyConfiguration": {...}  
}
```

タスク定義 | コンテナ定義

必須

1. ファミリー (family)
2. コンテナ定義 (containerDefinitions)

オプション

- ・タスク実行時、コンテナランタイムに渡されるコンテナ定義
- ・コンテナのイメージ/ポートマッピング/メモリ制限などを指定

```
{  
  "family": "",  
  "taskRoleArn": "",  
  "executionRoleArn": "",  
  "networkMode": "none",  
  "containerDefinitions": [...],  
  "volumes": [...],  
  "placementConstraints": [...],  
  "requiresCompatibilities": [...],  
  "cpu": "",  
  "memory": "",  
  "tags": [...],  
  "pidMode": "host",  
  "ipcMode": "host",  
  "proxyConfiguration": {...}  
}
```

コンテナ定義 | 代表的なパラメータ (1/3)

名前 (name)

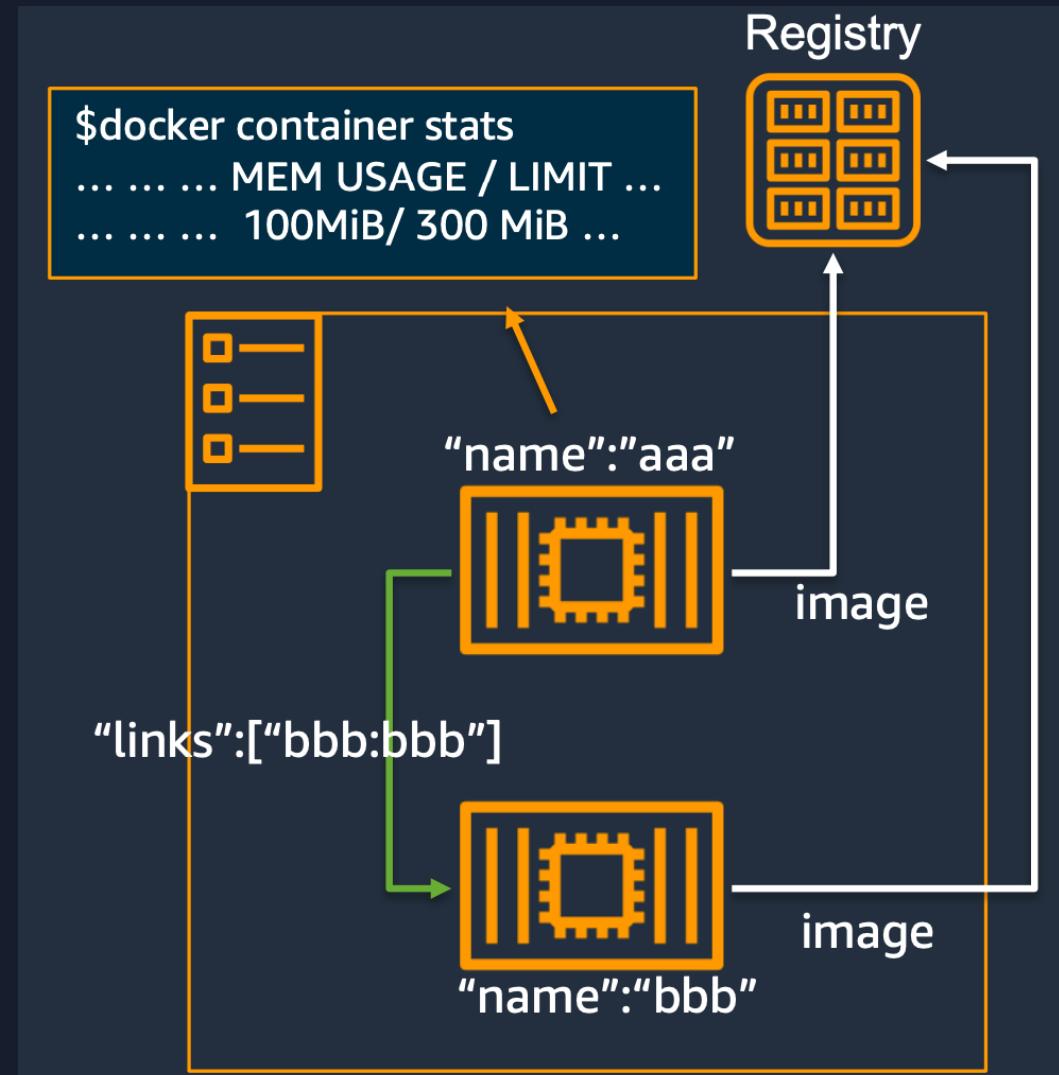
- ・コンテナの名前。
- ・ECS Exec を用いてコンテナ内で作業する際や、bridge モードのタスク内で複数のコンテナをリンクする際に、この名前を利用

イメージ (image)

- ・使用するコンテナのイメージ URI を指定

メモリ (memory, memoryReservation)

- ・使用するメモリ容量を指定



コンテナ定義 | 代表的なパラメータ (2/3)

環境変数 (environment)

- コンテナに環境変数として設定する
- 定義ファイルに平文で記述されるので
機密情報には向かない

```
"environment": [  
    {"name": "hoge", "value": "fuga"}  
]
```

シークレット (secrets)

- 機密データを環境変数に設定する場合に利用
 - AWS Secrets Manager シークレット
 - AWS Systems Manager パラメータストアのパラメータを参照可能
- それぞれタスク実行ロールに適切なIAMアクセス許可の設定が必要

```
"secrets": [  
    {"name": "environment_variable_name",  
     "valueFrom": "arn:aws:secretsmanager:region:aws_account_id:secret:secret_name-AbCdEf"  
    }  
]
```

コンテナ定義 | 代表的なパラメータ (3/3)

ログ設定 (logConfiguration)

- 標準出力 (stdout) と標準エラー出力 (stderr) に出力し、ストリームとして扱うのがベスト プラクティス
- 出力されるログの形式や、保存・転送などを制御するログドライバーやオプションを指定

#	logDriver 名	説明	EC2	Fargate
1	awslogs	CloudWatch Logs へ転送	○	○
2	awsfirelens	Fluentd, CloudWatch Logs, Kinesis へ転送	○	○
3	gelf	Graylog Extended Log Format 形式ログ出力	○	-
4	json-file	JSON 形式ログを出力	○	-
5	journald	systemd のログ管理システムに転送	○	-
6	logentries	Logentries ログ管理システムへ転送	○	-
7	splunk	Splunk ログ管理システムへ転送	○	○
8	fluentd	EC2 インスタンスの fluentd へ転送	○	-
9	syslog	EC2 インスタンスの syslog へ転送	○	-

タスク定義 | タスクサイズ

必須

1. ファミリー (family)
2. コンテナ定義 (containerDefinitions)

オプション

3. タスクサイズ (cpu / memory)
4. タスクロール (taskRoleArn)
5. 実行ロール (executionRoleArn)

- タスクが使用する CPU とメモリの合計値
- Fargate でホストされるタスクの場合は、必須のフィールド

```
{  
  "family": "",  
  "taskRoleArn": "",  
  "executionRoleArn": "",  
  "networkMode": "none",  
  "containerDefinitions": [...],  
  "volumes": [...],  
  "placementConstraints": [...],  
  "requiresCompatibilities": [...],  
  "cpu": "",  
  "memory": "",  
  "tags": [...],  
  "pidMode": "host",  
  "ipcMode": "host",  
  "proxyConfiguration": {...}}
```

タスク定義 | CPU とメモリ定義

タスクレベルリソース

- ✓ タスク単位の要求リソース量を定義

- cpu : cpu-unit 数を指定
 - 1 vCPU = 1,024 cpu-units
- memory : MiB 単位で指定
- Fargate では必須パラメータ

コンテナレベルリソース

- ✓ 各コンテナへのタスクリソースの分配を定義
- オプション指定

```
{  
  "family": "scorekeep",  
  "cpu": 1024,  
  "memory": 2048,  
  "containerDefinitions": [  
    {  
      "name": "scorekeep-frontend",  
      "image": "xxx.dkr.ecr.us-east-1.amazonaws.com/fe",  
      "cpu": 256,  
      "memory": 768,  
      "memoryReservation": 512  
    },  
    {  
      "name": "scorekeep-api",  
      "image": "xxx.dkr.ecr.us-east-1.amazonaws.com/api",  
      "cpu": 768,  
      "memoryReservation": 512  
    }  
  ]  
}
```

タスクレベル
リソース指定

コンテナレベル
リソース指定

タスク定義 | IAM との連携

必須

1. ファミリー (family)

- コンテナが利用できる IAM ロールを指定
- アプリケーションはこの IAM ロールで許可された AWS サービスのAPIを実行できる

2. ブラウジング (cpu / memory)

4. タスクロール (taskRoleArn)

5. タスク実行ロール (executionRoleArn)

6. ネットワークエード (networkMode)

- ECS コンテナエージェントが利用する IAM ロールを指定
- この権限を使ってコンテナのイメージを pull したり CloudWatch Logs に書き込みを行う

```
{  
  "family": "",  
  "taskRoleArn": "",  
  "executionRoleArn": "",  
  "networkMode": "none",  
  "containerDefinitions": [...],  
  "volumes": [...],  
  "placementConstraints": [...],  
  "requiresCompatibilities": [...],  
  "cpu": "",  
  "memory": "",  
  "tags": [...],  
  "pidMode": "host",  
  "ipcMode": "host",  
  "proxyConfiguration": {...}  
}
```



タスク定義 | ネットワークモード (1/2)

必須

1. ファミリー (family)

- タスクに属するコンテナが使用するネットワークモードを指定
- awsVpc, bridge, host, default, none のいずれかを指定

5. タスク実行ロール (executionRoleArn)

6. ネットワークモード (networkMode)

7. ボリューム (volumes)

```
{  
  "family": "",  
  "taskRoleArn": "",  
  "executionRoleArn": "",  
  "networkMode  "containerDefinitions": [...],  
  "volumes": [...],  
  "placementConstraints": [...],  
  "requiresCompatibilities": [...],  
  "cpu": "",  
  "memory": "",  
  "tags": [...],  
  "pidMode": "host",  
  "ipcMode": "host",  
  "proxyConfiguration": {...}  
}
```

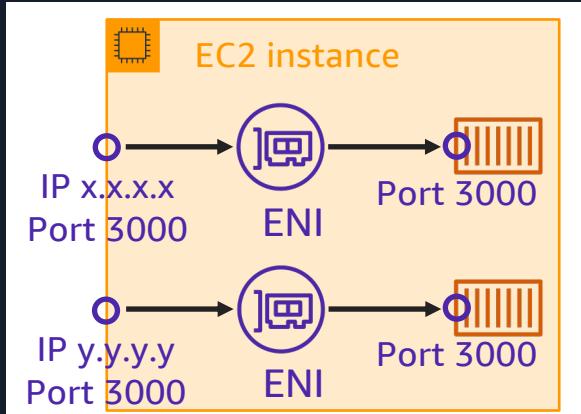


タスク定義 | ネットワークモード (2/2)

Fargate
実行環境

awsVpc モード

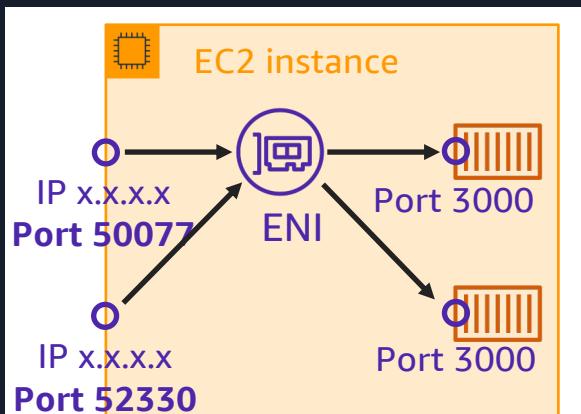
- ECS 管理下の ENI (仮想サーバーの仮想ネットワークカード) がタスクにアタッチされる



EC2
実行環境

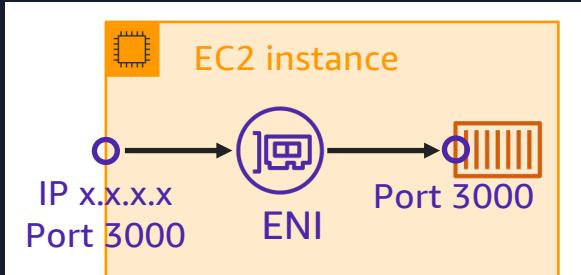
bridge モード

- 仮想ネットワークブリッジを利用してホスト/コンテナポートをマッピングして通信



host モード

- コンテナをホストしている EC2 インスタンスの IP/ポートを介して通信



タスク定義 | ボリューム

必須

- データを共有・永続化するためのボリュームのリスト
- Docker ボリューム、バインドマウント、EBS ボリューム、EFS ボリューム、FSx for Windows File Server ボリュームの 5 種類が利用可能

- ネットワークモード (networkMode)
- ボリューム (volumes)**

```
"family": "",  
"taskRoleArn": "",  
"executionRoleArn": "",  
"networkMode": "none",  
"containerDefinitions": [...],  
"volumes": [...],  
"placementConstraints": [...],  
"requiresCompatibilities": [...],  
"cpu": "",  
"memory": "",  
"tags": [...],  
"pidMode": "host",  
"ipcMode": "host",  
"proxyConfiguration": {...}  
}
```

タスクからのデータボリュームの使用

Fargate
実行環境

Fargate バインドマウント

- 揮発性のストレージをコンテナにマウントし、コンテナ間で共有
- 使用するすべてのコンテナが停止するとデータが削除される

Amazon EBS ボリューム

- 高スループットなトランザクション集約型アプリケーション向け
- タスクごとに1つの EBS ボリュームにアタッチ可能

Amazon EFS ボリューム

- ストレージ容量が伸縮自在で、自動的に拡大および縮小される

Docker ボリューム

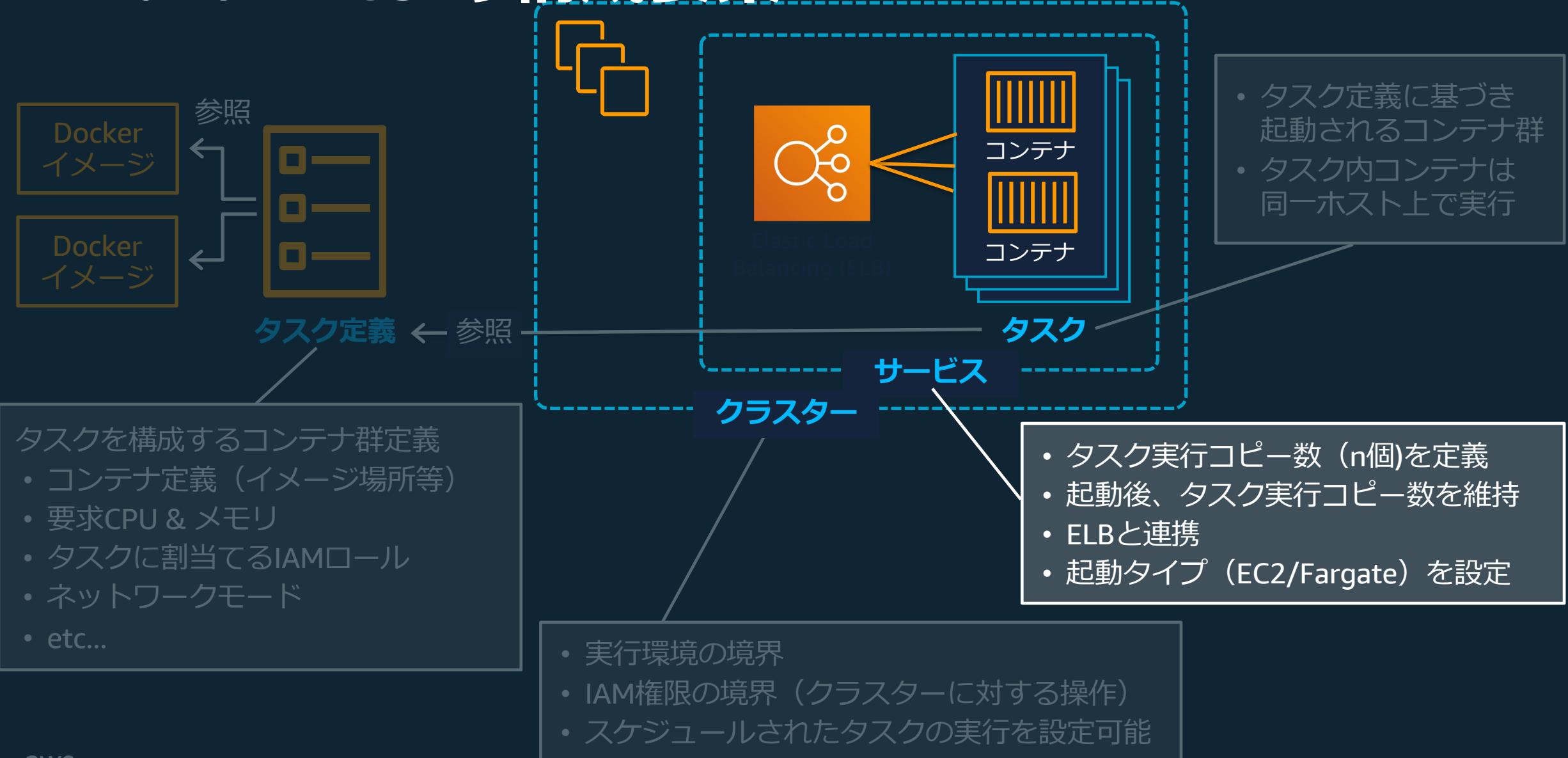
- タスク間での共有や明示的なライフサイクル管理
- 3rd Party のボリュームドライバーの利用ができる

EC2 バインドマウント

- ホストマシン上のファイルやディレクトリをコンテナにマウント
- タスク定義によってデータをホストのライフサイクルに関連付けが可能



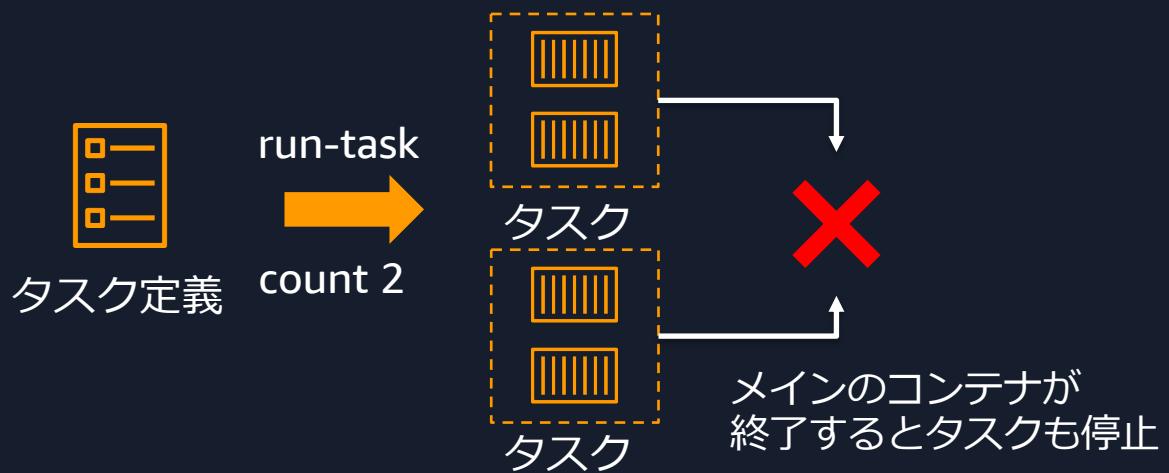
Amazon ECS の構成要素



コンテナの実行方法

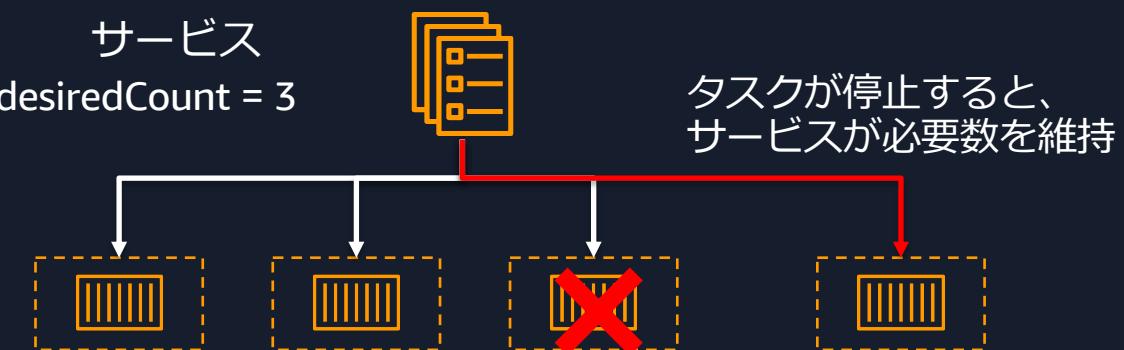
スタンドアロンタスク

- タスク定義に従って実行されるアプリケーションの実行単位
- タスク定義の一部のパラメータはタスク実行時に上書き可能
- 用途：バッチジョブなど処理が終わると停止するワークフローなど



サービス

- 指定した数のタスクを維持する
- タスクが失敗/停止した場合は新しいタスクを起動して置き換え
- 用途：Web アプリケーションなど長時間実行するワークフロー
- ELB との連携 / Auto Scaling 機能



サービス | タスク数のAuto Scaling

1. ターゲット追跡スケーリングポリシー

- 指定したメトリクスがターゲットの値に近づくように自動的に調整

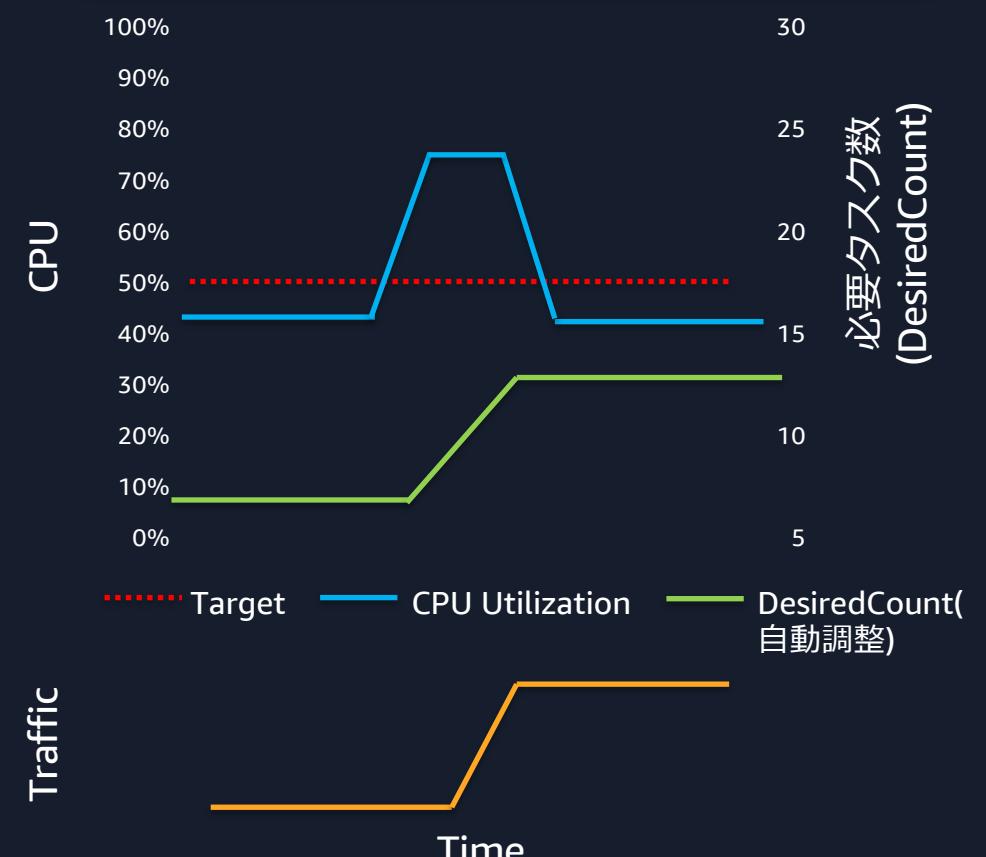
2. ステップスケーリングポリシー

- アラームをトリガーに調整値に基づいて増減
- ターゲット追跡スケーリングポリシーと組み合わせることでより高度なスケーリングも可能

3. スケジュールに基づくスケーリング

- 日付と時刻に基づいてタスク数を増減

ターゲット追跡スケーリングポリシーの動作イメージ



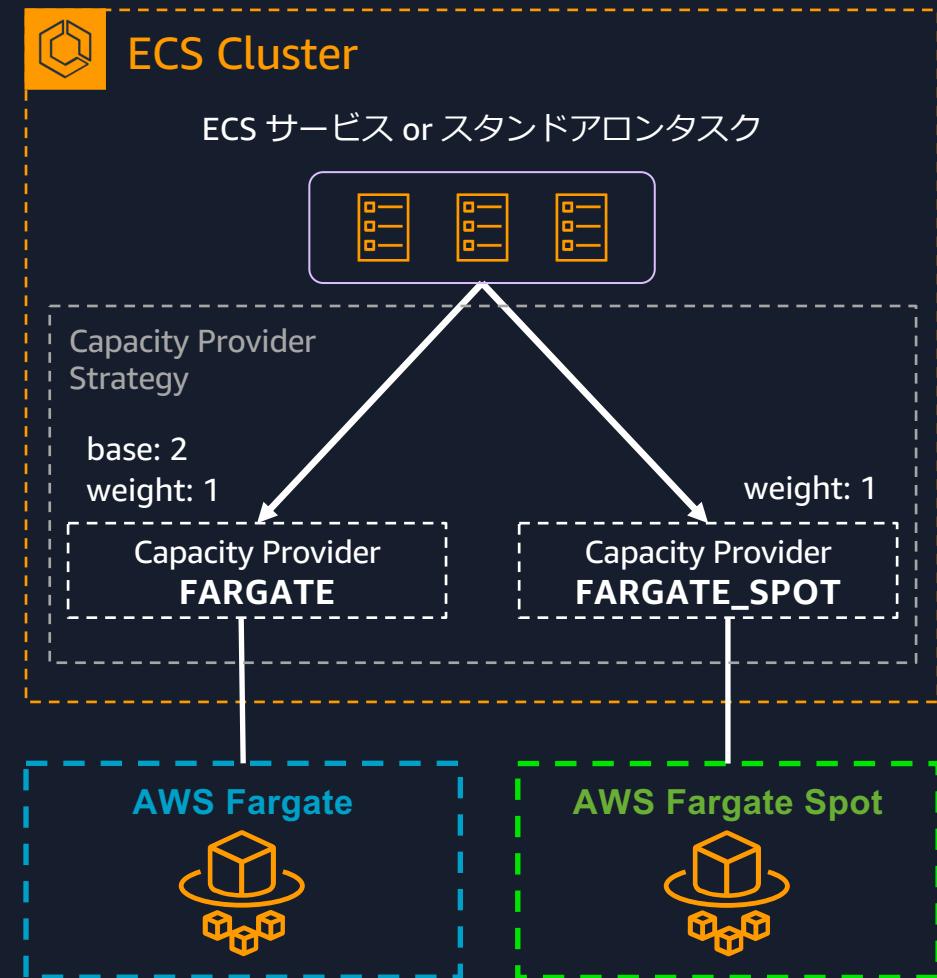
Capacity Providers の概要

Capacity Provider

- ・ タスクが実行されるインフラストラクチャを設定
- ・ Auto Scaling グループや Fargate を指定
- ・ Fargate キャパシティプロバイダーは予約済み
 - FARGATE
 - FARGATE_SPOT

Capacity Provider Strategy

- ・ タスクをどのキャパシティプロバイダーに配置するかを決定する「戦略」
- ・ ベース値やウェイト値で配置を細かく制御可能



Amazon ECS の始め方

Amazon ECS の始め方

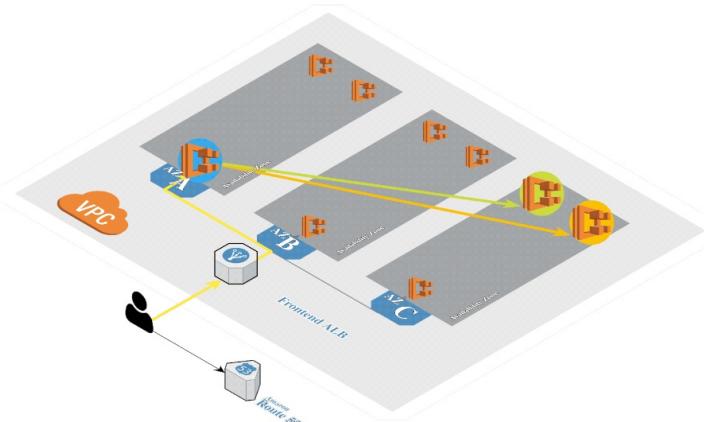
- Amazon Elastic Container Service の開始方法
 - <https://aws.amazon.com/jp/ecs/getting-started/>
- Amazon ECS を始めるにあたって、追加料金は不要
 - ワークロードが使用するリソースに対しての課金
 - <https://aws.amazon.com/jp/ecs/pricing/>
- Amazon ECS のお客様導入事例
 - <https://aws.amazon.com/jp/containers/customers/>
- Amazon ECS に関する AWS Blog 記事
 - <https://aws.amazon.com/jp/blogs/news/tag/amazon-ecs/>

The screenshot shows the AWS Elastic Container Service (ECS) Getting Started page. At the top, there's a navigation bar with links for AWSについて, お問い合わせ, サポート, 日本語, アカウント, and ログイン. Below the navigation is a breadcrumb trail: 製品 / コンピューティング / Amazon Elastic Container Service. The main title is "Amazon Elastic Container Service の開始方法". There are two prominent orange buttons at the bottom: "ECS コンソールチュートリアル" and "AWS Copilot のダウンロード". The page content includes sections for "ログインとセットアップ" (Login and Setup) and "Amazon ECS デジタルトレーニング" (Amazon ECS Digital Training), each with a brief description and a "詳細はこちら" link.

その他のリソース

- Amazon ECS の導入を加速させる Workshop およびツール
 - ECS Blueprints
 - <https://github.com/aws-ia/ecs-blueprints>
 - <https://aws.amazon.com/jp/blogs/news/accelerate-amazon-ecs-based-workloads-with-ecs-blueprints/>
 - AWS Copilot CLI
 - <https://aws.github.io/copilot-cli/ja/>
 - <https://aws.amazon.com/jp/blogs/news/introducing-aws-copilot/>
 - Amazon ECS Workshop
 - <https://ecsworkshop.com/>

Amazon ECS Workshop



In this workshop, we will launch a frontend and multiple backend services on Amazon Elastic Container Service, and explore how you might adopt this workflow into your environment.

まとめ

- Amazon ECS とは
 - フルマネージドのコンテナオーケストレーションサービス
- Amazon ECS の構成要素
 - タスク定義 / タスク / サービス / クラスター
 - タスク定義の詳細
- Amazon ECS の始め方



Amazon **Elastic Container Service**

AWS Black Belt Online Seminar とは

- ・ 「サービス別」「ソリューション別」「業種別」などのテーマに分け、
アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナーシリーズです
- ・ AWS の技術担当者が、 AWS の各サービスやソリューションについてテーマごとに動画を公開します
- ・ 以下の URL より、過去のセミナー含めた資料などをダウンロードすることができます

– <https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/>
– <https://www.youtube.com/playlist?list=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBlqY>

𝕏 ご感想は X (Twitter) へ！ハッシュタグは以下をご利用ください
#awsblackbelt

内容についての注意点

- ・ 本資料では資料作成時点のサービス内容および価格についてご説明しています。AWS のサービスは常にアップデートを続けているため、最新の情報は AWS 公式ウェブサイト (<https://aws.amazon.com/>) にてご確認ください
- ・ 資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます
- ・ 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます
- ・ 技術的な内容に関しましては、有料の [AWS サポート窓口](#)へお問い合わせください
- ・ 料金面でのお問い合わせに関しては、[カスタマーサポート窓口](#)へお問い合わせください (マネジメントコンソールへのログインが必要です)

Thank you!

AWS Black Belt Online Seminar

AWS Backup で考える DR 戦略 #1 基本編

小島 七海

Cloud Support Engineer

2025/03



自己紹介

小島 七海

アマゾン ウェブ サービス ジャパン合同会社
技術支援本部 クラウドサポートエンジニア



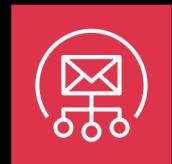
好きな AWS サービス



AWS Backup



Amazon Simple Storage
Service (Amazon S3)



Amazon Simple Email
Service (Amazon SES)

AWS Black Belt Online Seminar とは

- ・ 「サービス別」「ソリューション別」「業種別」などのテーマに分け、
アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナーシリーズです
- ・ AWS の技術担当者が、 AWS の各サービスやソリューションについてテーマごとに動画を公開します
- ・ 以下の URL より、過去のセミナー含めた資料などをダウンロードすることができます
 - > <https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/>
 - > <https://www.youtube.com/playlist?list=PLzWGOASvSx6FlwIC2X1nObr1KcMCBBlqY>



ご感想は X (Twitter) へ！ハッシュタグは以下をご利用ください
#awsblackbelt



内容についての注意点

- ・ 本資料では資料作成時点のサービス内容および価格についてご説明しています。AWS のサービスは常にアップデートを続けているため、最新の情報は AWS 公式ウェブサイト (<https://aws.amazon.com/>) にてご確認ください
- ・ 資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます
- ・ 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます
- ・ 技術的な内容に関しては、有料の [AWS サポート窓口](#)へお問い合わせください
- ・ 料金面でのお問い合わせに関しては、[カスタマーサポート窓口](#)へお問い合わせください (マネジメントコンソールへのログインが必要です)

本セミナーの対象者

対象者

- DR 戦略において AWS Backup がどのように活用できるか知りたい方
- AWS Backup を用いたバックアップ方法を学びたい方

アジェンダ

1. AWS における DR 戦略
2. AWS Backup の概要
3. AWS Backup の DR への応用
4. まとめ

AWS における DR 戦略

災害対策 (Disaster Recovery: DR) の重要性

災害による被害シナリオとは？

- 広範囲での障害やシステムの停止が発生し、ワークフローがビジネス目標を達成することが困難となるイベント

想定する災害の例

- 地震や洪水などの自然災害
- 大規模停電や広域ネットワークなど、社会のインフラ設備障害
- 不注意による設定ミス、不正アクセス/外部からのアクセス、改ざんなどの人的行為

災害が発生してもサービスの中斷を最小限に抑えられるようあらかじめ **DR** 戦略を準備しておくことが重要

DR と High Availability の違い

	DR	High Availability
対象	発生確率は小さいがビジネス影響が甚大となる災害への対策	コンポーネントの障害、ネットワーク障害、負荷のスパイクなど災害と比較し頻度は高い障害への対策
このセミナーでの具体例	リージョン単位に着目したソリューション	AZ 単位以下に着目したソリューション
目標	個々の災害イベントに対する目標で、RTO/RPO といった時間が基準	可用性 99.99 といった一定期間のメトリクスが基準

本セミナーでは DR におけるバックアップ & リストアで
賄うことのできるビジネス継続にフォーカス

DR における AWS の強み

オンプレミス

- 1. 初期投資が必要**
 - データセンターやサーバーの確保などが必要
- 2. 設備維持コストがかかる**
 - インフラ維持費が必要
- 3. 運用手順が煩雑**
 - インフラ運用に手間がかかる



AWS

- 1. 初期投資が不要**
 - 必要なリソースをオンデマンドで提供
- 2. 設備維持コストを最小化**
 - 必要時のみ立ち上げることで、平常時のコストを最小化
 - 使用した分だけの料金
- 3. 豊富なマネージドサービス**
 - 手間のかかるインフラ運用を削減
 - AWS CloudFormation や AWS CDKなどを活用することで手順の自動化も可能

DR の検討事項

RPO

(Recovery Point Objective: 目標復旧時点)

最後の復旧可能時点からサービス中断までの間に
どの程度のデータ損失を許容するか

RTO

(Recovery Time Objective: 目標復旧時間)

サービスの中断から復旧までに
どの程度の時間を許容するか



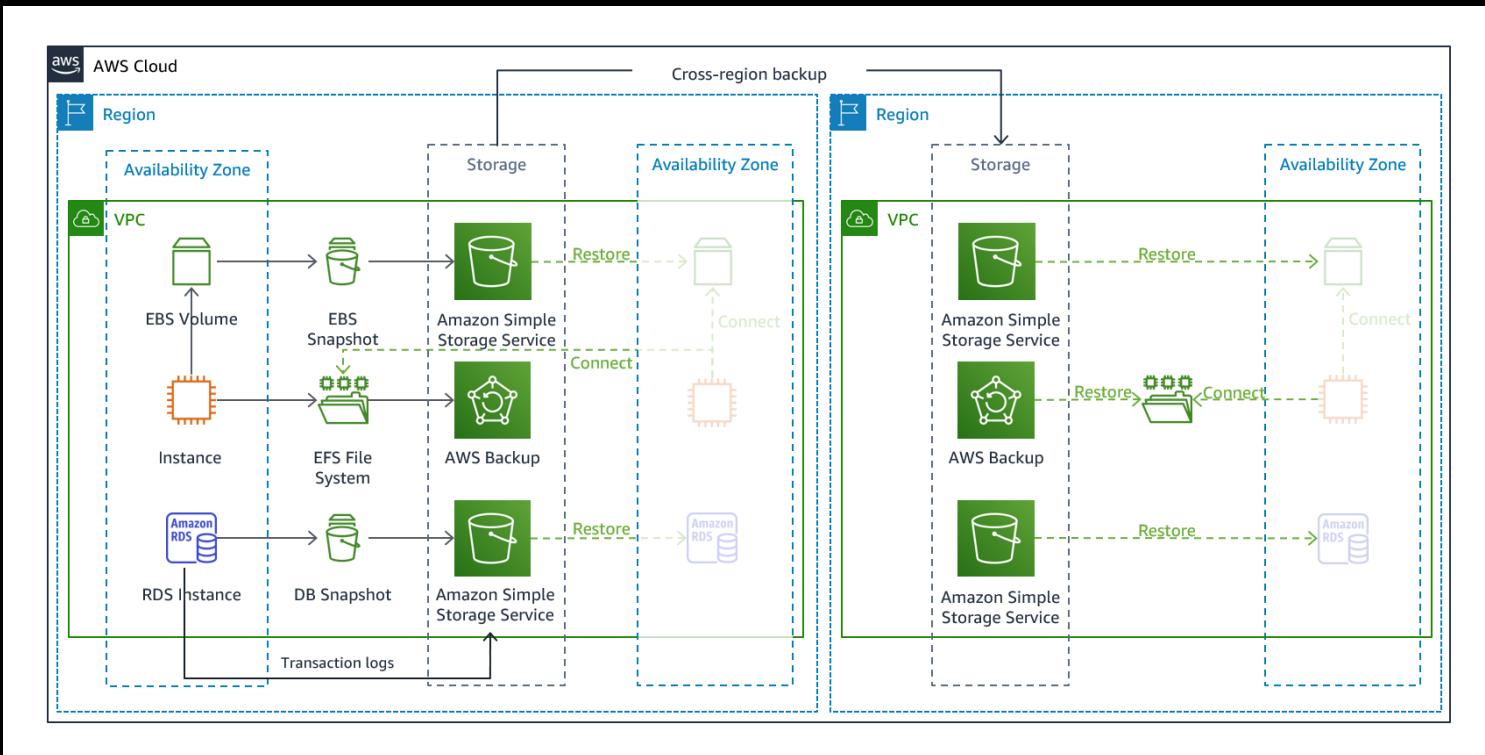
AWS 上での DR における 4 つのシナリオ

バックアップ&リストア	パイロットライト	ウォームスタンバイ	マルチサイトアクティブ/アクティブ
RPO / RTO: Hours	RPO / RTO: 10s of minutes	RPO / RTO: Minutes	RPO / RTO: Real-time
<ul style="list-style-type: none">データ/アプリケーションのバックアップイベント発生後リソースをプロビジョニング費用 \$	<ul style="list-style-type: none">データのレプリケーションコア要素の実行環境のみプロビジョニング費用 \$\$	<ul style="list-style-type: none">本番環境のスケールダウンしたコピーを別リージョンで稼働費用 \$\$\$	<ul style="list-style-type: none">ワークロードを複数のリージョンで同時に実行費用\$\$\$\$

本セミナーでは
こちらにフォーカス

バックアップ & リストアとは

- データの損失や破損を軽減するために適したアプローチ
- 他の AWS リージョンにデータをレプリケートすることによる別リージョンでの復旧や、操作ミス・設定ミスからの回復に備えるために使用
- データに加え、インフラストラクチャ、設定、アプリケーションコードを復旧先リージョンにデプロイする
- インフラストラクチャについては AWS CloudFormation や AWS CDK などを使用してデプロイ



https://docs.aws.amazon.com/ja_jp/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html#backup-and-restore

データのバックアップ & リストアのプロセス

バックアップの設計

- ・ワークフローにおける全てのデータソースを特定
- ・データソースを重要性に基づいて分類
- ・バックアップの必要性を評価
- ・バックアップの頻度、保持期間を決定
- ・バックアップ取得方法の決定

バックアップの保護

- ・バックアップに対するアクセス制御を設定
- ・バックアップを暗号化

バックアップの自動化

- ・RPO をもとにバックアップが自動で行われるよう設定

バックアップの復旧

- ・復元手順の確認
- ・復元可能であるかの確認
- ・定期的に復旧し、RPO/RTO を満たすか検証
- ・復旧プロセスの自動化

詳細なプロセスは AWS Well-Architected フレームワークを参照ください:
https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/back-up-data.html

AWS Backup の概要

AWS Backup とは

AWS サービス全体のデータのバックアップを一元的にオーケストレーションし、自動化できるフルマネージドバックアップサービス



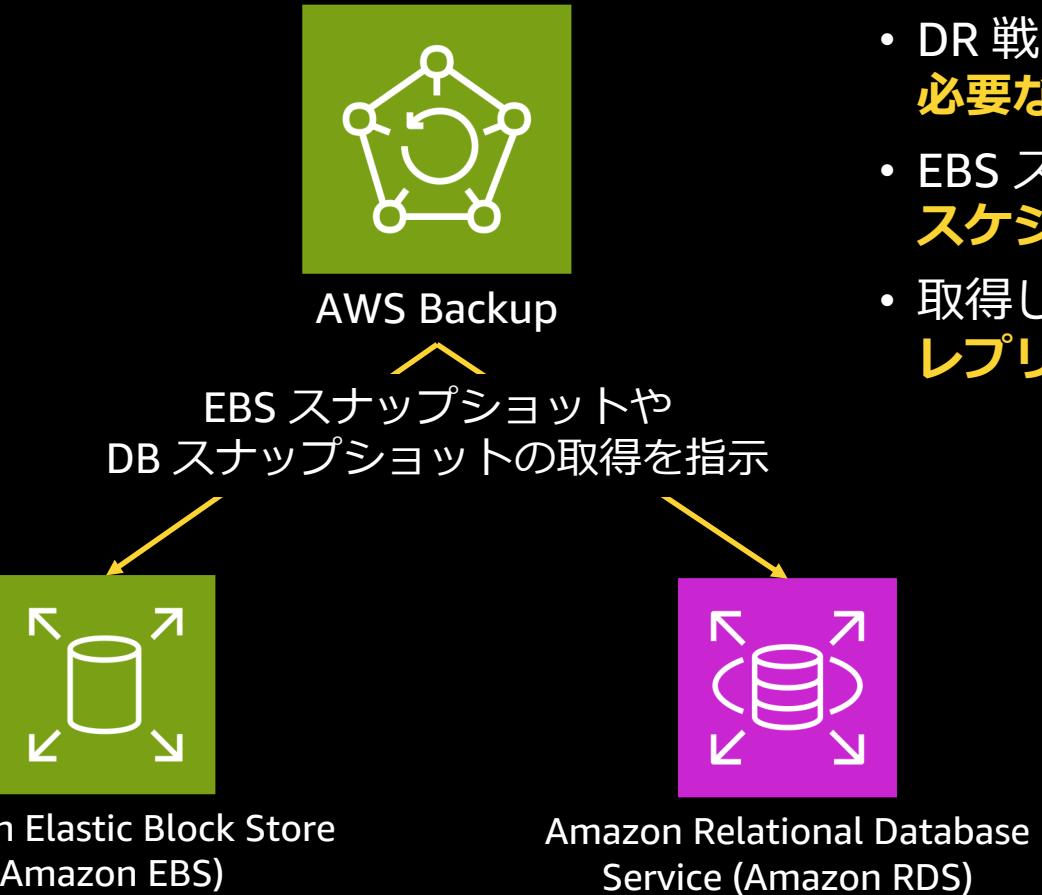
AWS Backup

AWS とハイブリッドサービス上のアプリケーションリソース
データ保護を簡素化

DR と事業継続の基盤を構築

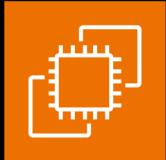
ランサムウェアやアカウントの侵害から保護およびリカバリする
データ保護コンプライアンスを管理する

DR 戦略における AWS Backup の位置付け



- DR 戦略におけるデータのバックアップ & リストアに必要なプロセスをマネージドに実現
- EBS スナップショットや DB スナップショット等の取得をスケジュールに従って AWS Backup が指示
- 取得したスナップショットを AWS Backup が管理し、レプリケーションや復元までサポート

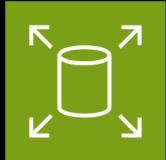
対応 AWS サービス



Amazon Elastic Compute
Cloud (Amazon EC2)



VMware Cloud on AWS



Amazon Elastic Block Store
(Amazon EBS)



Amazon Simple Storage
Service (Amazon S3)



Amazon Elastic File System
(Amazon EFS)



AWS Storage
Gateway



Amazon FSx
for Lustre



Amazon FSx for
Windows File Server



Amazon FSx for NetApp
ONTAP



Amazon FSx for OpenZFS



Amazon Redshift



AWS CloudFormation



Amazon Aurora



Amazon DocumentDB
(with MongoDB compatibility)



Amazon DynamoDB



Amazon Neptune

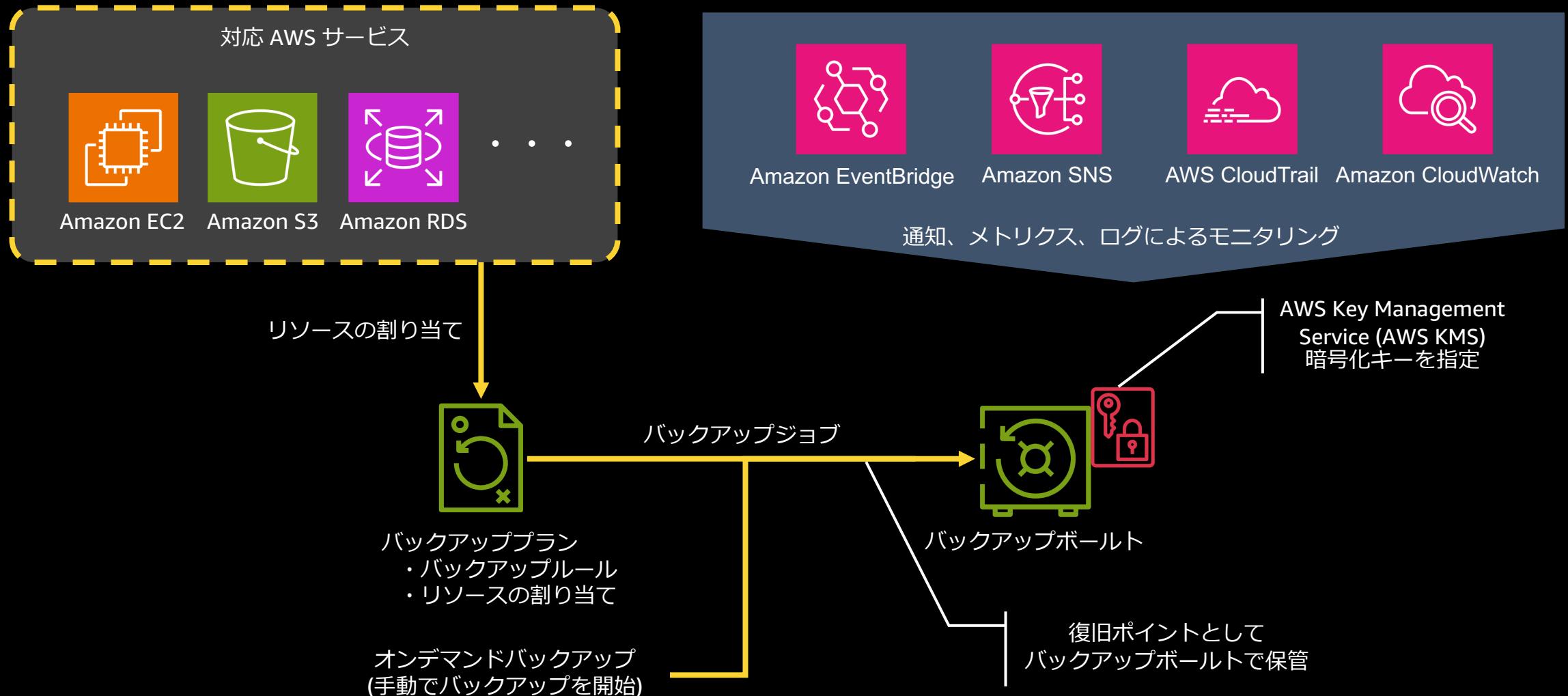


Amazon Timestream



Amazon Relational Database
Service (Amazon RDS)

AWS Backup の基本アーキテクチャ



AWS Backup で使用される用語

バックアップボルト	バックアップを保存および整理するためのコンテナ（入れ物）
バックアッププラン	AWS リソースをいつどのようにバックアップするかを定めるポリシー「バックアップルール」と「リソースの割り当て」を設定
バックアップルール	バックアップスケジュールやバックアップウィンドウ、バックアップの保持期間を定義するルール
リソースの割り当て	バックアップ対象リソースの定義
復旧ポイント	取得された個々のバックアップを指し、バックアップボルトで管理される
保持期間	バックアップルールごとに、復旧ポイントを保存する期間である保持期間を設定 この期間を過ぎた復旧ポイントは自動的に AWS Backup が削除する

※ 2025 年 3 月現在、バックアップルール作成において、保持期間を世代数ベースで行うことはできません。
取得頻度と保持期間から逆算する必要があります。

AWS Backup の料金

AWS Backup では以下に対して支払いが発生し、最低利用料金および初期費用は不要

- 使用するバックアップストレージ
- AWS リージョン間で転送されるバックアップデータのデータ転送料金
- 復元するバックアップデータ
- 復元テストの評価
- Backup search, Backup Audit Manager (本セミナーでは扱っておりません)

リソースタイプに応じて料金は異なりますので、詳細は AWS 公式ウェブサイトをご参照ください。

<https://aws.amazon.com/jp/backup/pricing/>

AWS Backup の DR への応用

データのバックアップ & リストアのプロセス

再掲

バックアップの設計

- ・ワークフローにおける全てのデータソースを特定
- ・データソースを重要性に基づいて分類
- ・バックアップの必要性を評価
- ・バックアップの頻度、保持期間を決定
- ・バックアップ取得方法の決定

バックアップの保護

- ・バックアップに対するアクセス制御を設定
- ・バックアップを暗号化

バックアップの自動化

- ・RPO をもとにバックアップが自動で行われるよう設定

バックアップの復旧

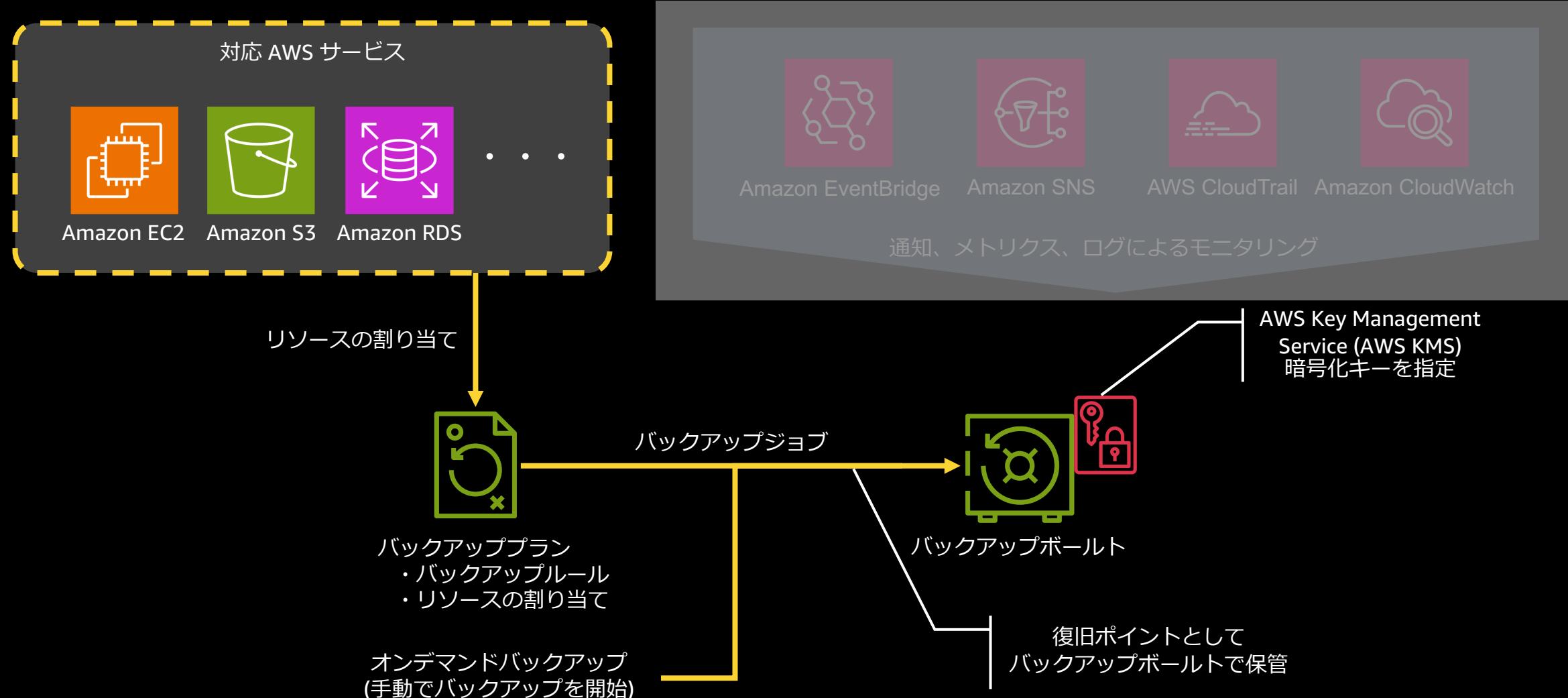
- ・復元手順の確認
- ・復元可能であるかの確認
- ・定期的に復旧し、RPO/RTO を満たすか検証
- ・復旧プロセスの自動化

詳細なプロセスは AWS Well-Architected フレームワークを参照ください:
https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/back-up-data.html



AWS Backup の基本アーキテクチャ

再掲



バックアップボルト

バックアップの設計

バックアップの保護

バックアップの自動化

バックアップの復旧

ボルトを作成 情報

全般

ボルト名
BackupVault_Tokyo

ボルト名では大文字と小文字が区別されます。2~50 文字の英数字または「_」を含める必要があります。

ボルトタイプ

バックアップボルト
バックアップボルトには、リースインスタンスとは別のイミュータブルなバックアップが保存されます。

- 暗号化キーはお客様が管理するか、AWS が管理します
- ボルトロックはオプションです

論理的にエアギャップのあるボルト
論理的にエアギャップのあるボルトには、バックアップのコピーが保存されます。

- 暗号化キーは AWS が所有しており、削除できません
- 直接復元をサポートするアカウント間および組織間の共有
- ボルトロックは必須です

暗号化キー | 情報

(デフォルト) aws/backup

説明	アカウント	キー ID	ステータス
Default key that protects my Backup data when no other key is defined	このアカウント	[REDACTED]	有効

ボルトタグ - オプション

ここで指定するタグは、ボルトの整理と追跡に役立ちます。

このボルトにはタグが関連付けられていません。

新しいタグを追加

最大 50 個のタグをさらに追加できます。

キャンセル ボルトを作成

- 復旧ポイント（バックアップ）を保存および整理するコンテナ
- 作成時にはボルト名と AWS KMS 暗号化キーを指定
 - デフォルトでは aws/backup の KMS キーを使用
 - カスタマーマネージドキーも使用可能

(注) バックアップボルトで指定した暗号化キーは特定のリソースタイプのバックアップのみに適用されます。
対象外となるリソースタイプの場合は、元となるリソースの暗号化に使用されたキーを使用してバックアップを暗号化します。

https://docs.aws.amazon.com/ja_jp/aws-backup/latest/devguide/encryption.html



バックアップポールト

バックアップの設計

バックアップの保護

バックアップの自動化

バックアップの復旧

BackupVault_Tokyo 情報

概要

ポート名 BackupVault_Tokyo	KMS 暗号化キー ID [REDACTED]	ポートロック -
ポートタイプ バックアップポート	作成日 2025年2月18日, 17:00 (UTC+09:00)	ポートロックの保持期間 最小保持期間: - 最大保持期間: -
ポート ARN arn:aws:backup:ap-northeast-1:[REDACTED]backup-vault:BackupVault_Tokyo		

復旧ポイント 保護されたリソース

復旧ポイント (1) 情報

復旧ポイント ID	ステータス	リソース名	リソース ID	リソースタイプ	バックアップタイプ
image/ami-[REDACTED]	完了	Test_EC2_Instance	instance/i-[REDACTED]	EC2	イメージ

復旧ポイントを選択して復元操作を行うことで、取得時点の状態にデータを復元

アクセスポリシー

- ・バックアップポートに割り当てる
- ・バックアップポートや復旧ポイントに対するアクセスを制限することが可能

例) 特定のプリンシパル以外へ復旧ポイントの削除を禁止するポリシー

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Deny",  
      "Principal": "*",  
      "Action": "backup:DeleteRecoveryPoint",  
      "Resource": "*",  
      "Condition": {  
        "ArnNotEquals": {  
          "aws:PrincipalArn": [  
            "arn:aws:iam::112233445566:user/Alice",  
            "arn:aws:iam::112233445566:role/Backup_Admin"  
          ]  
        }  
      }  
    }  
  ]  
}
```



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

バックアップの設計

バックアップの保護

バックアップの自動化

バックアップの復旧

アクセスポリシーを編集

アクセスポリシーを編集するときは、バックアップポートとそれに含まれるリソースにポリシーを割り当てる事ができます。ポリシーを割り当てる、バックアッププランやオンデマンドバックアップを作成するためのアクセス権をユーザーに付与するなどの操作を実行できますが、作成後に復旧ポイントを削除する権限は制限されます。

アクセスポリシーの詳細 情報

① ポリシー JSON は、すぐ下で編集できます。 [詳細ははこちら](#)

```
1  [ {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Deny",  
6       "Principal": "*",  
7       "Action": "backup:DeleteRecoveryPoint",  
8       "Resource": "*",  
9       "Condition": {  
10         "ArnNotEquals": {  
11           "aws:PrincipalArn": [  
12             "arn:aws:iam::112233445566:user/Alice",  
13             "arn:aws:iam::112233445566:role/Backup_Admin"  
14           ]  
15         }  
16       }  
17     }  
18   ]  
19 }
```

ポリシージェネレータ [\[\]](#) を使用して、ポリシーの許可を構築できます。

キャンセル

ポリシーを保存

バックアッププラン ～バックアップルール～

バックアップの設計

バックアップの保護

バックアップの自動化

バックアップの復旧

バックアップルールの設定 [情報](#)

スケジュール

バックアップルール名

バックアップルール名では大文字と小文字が区別されます。1~50 文字の英数字または「_」を含める必要があります。

バックアップボートルト [情報](#)  [新しいボートルトを作成](#) 

バックアップボートルト

バックアップ頻度 [情報](#)

バックアップ期間 [情報](#)

開始時間

バックアップを開始する時刻を指定します。時間単位の頻度では、開始時刻は 1 日のうちで初めてバックアップが作成される時刻です。該当する場合、時刻はサマータイムに合わせて調整され、1 年を通して同じ現地時間が維持されます。

:

次の時間以内に開始 [情報](#)

指定した時間にバックアッププランが開始されない場合は、バックアッププランが開始される期間を指定します。

次の時間以内に完了 [情報](#)

合計保持期間 [情報](#)
バックアップを保存する期間を AWS Backup に指示します。



合計保持 (日)


0 10 20 30 40 50 60 70 80 90 100

■ ウォームストレージ

コピー先にコピー - オプション [情報](#)

別のバックアップボートルトまたは論理的にエアギャップのあるボートルトにバックアップのコピーを作成します。

リージョン  

別のアカウントのボートルトにコピー

送信先ボートルト

バックアップコピーが作成されるボートルト。
  [新しいボートルトを作成](#) 

バックアップボートルト

ライフサイクル

追加のバックアップコピーの合計保持期間とコールドストレージ設定を指定します。

バックアップルールと同じ設定を使用する
コールドストレージ: 有効になっていません; 合計保持期間: 5 週

ライフサイクルをカスタマイズ

[コピーを追加](#)



バックアッププラン ~リソースの割り当て~

バックアップの設計

バックアップの保護

バックアップの自動化

バックアップの復旧

リソースの選択 情報
タグとリソース ID を使用して、このバックアッププランにリソースを割り当てます。

1. リソース選択を定義 情報
すべてのリソースを保護するか、タイプまたは ID でリソースを指定します。

すべてのリソースタイプを含める
アカウントで有効になっているすべてのリソースタイプを保護します。

特定のリソースタイプを含める
タイプ別にリソースを選択するか、ID で個別のリソースを指定します。

2. 特定のリソースタイプを選択 情報
このバックアップ計画で保護する特定のリソースタイプを選択します。特定のリソース ID を選択から除外することもできます。

リソースタイプを選択 ▾

3. 選択したリソースタイプから特定のリソース ID を除外する - オプション 情報
この割り当てから除外する特定のリソース ID を選択します。

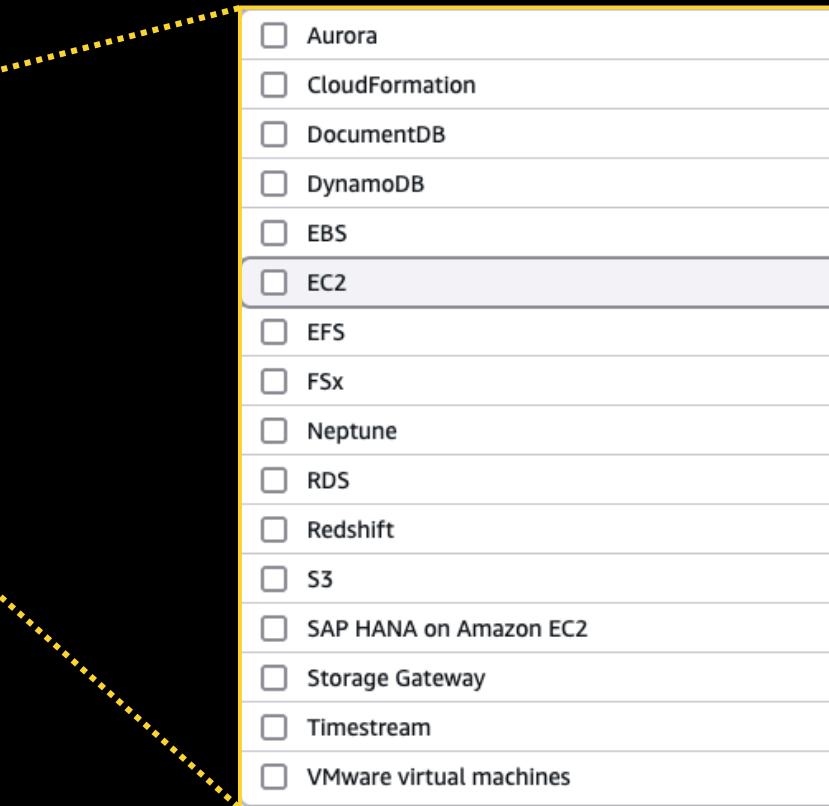
リソースタイプを選択 ▾

4. タグを使用して選択を絞り込む - オプション 情報
タグでリソースをフィルタリングします。タグが複数ある場合、リソースはすべてのタグ条件を満たす場合にのみバックアッププランに割り当てられます。

リソースの選択を絞り込むためのタグが選択されていません。

タグを追加

最大 30 個のタグを追加できます。



特定のリソースタイプ・リソース ID での割り当てや
特定のタグを持つリソースを割り当てることが可能

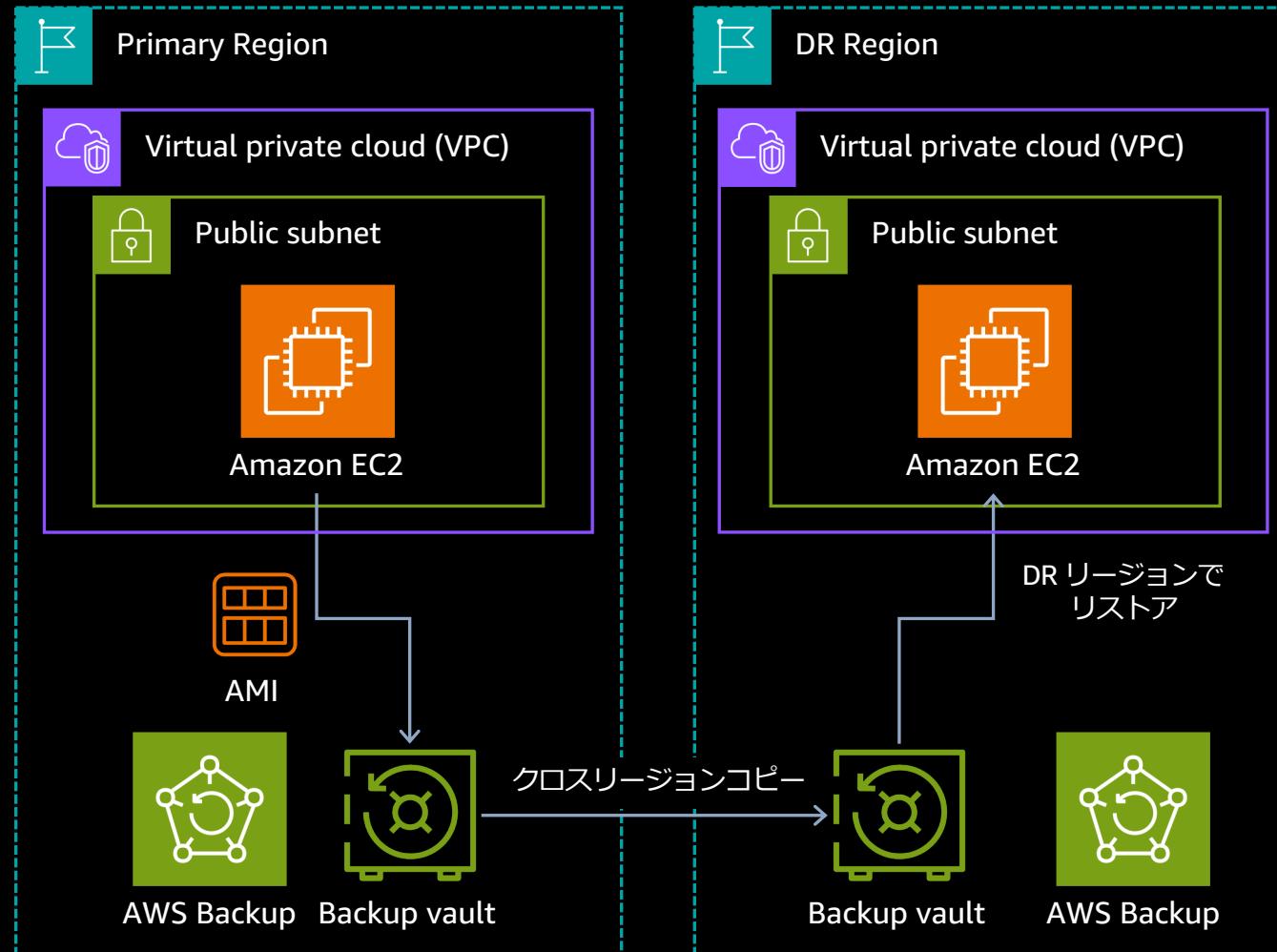
クロスリージョンコピー

バックアップの設計

バックアップの保護

バックアップの自動化

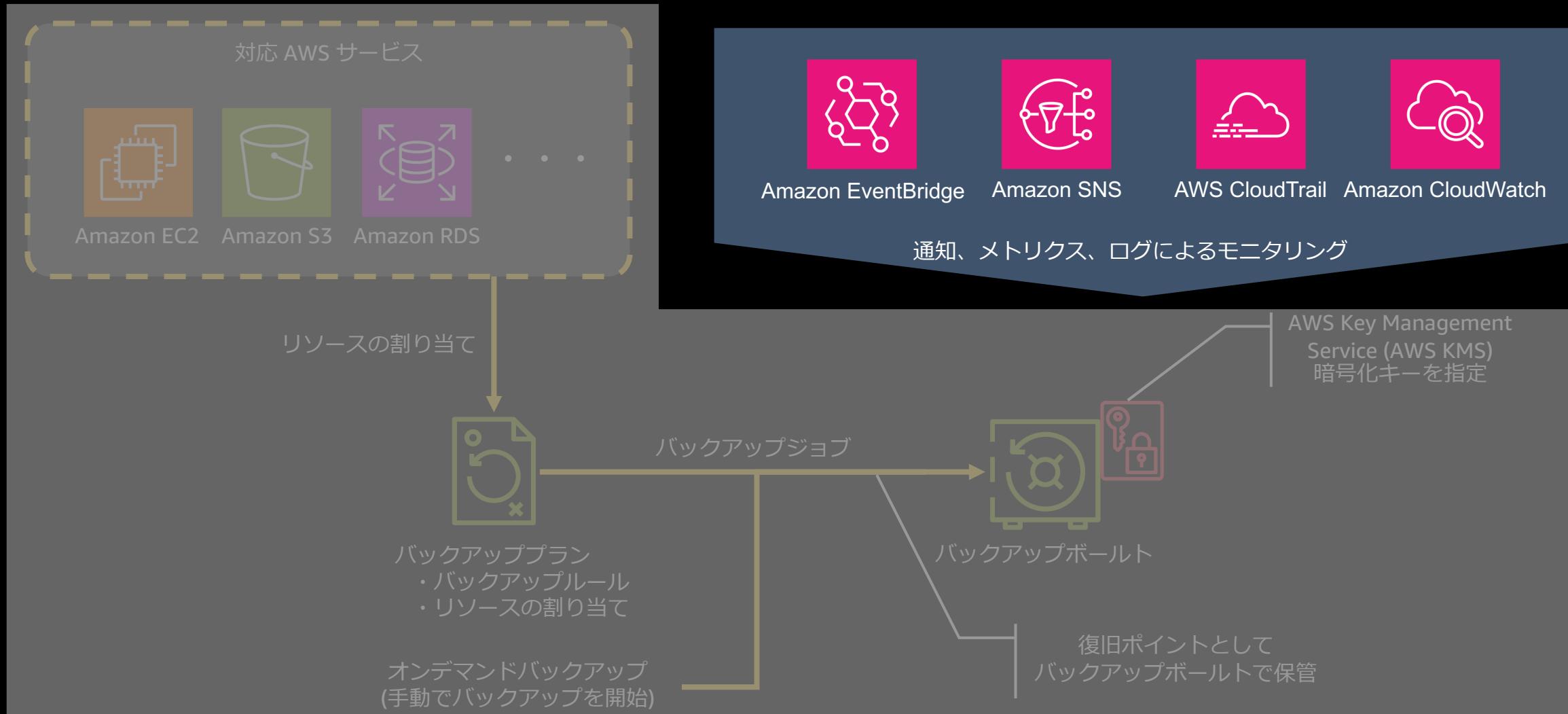
バックアップの復旧



- ・バックアップルールでクロスリージョンコピーの設定が可能
- ・Primary Region でバックアップ取得後、指定した DR リージョンのバックアップボルトへ復旧ポイントをコピー
- ・Primary Region 被災時は DR リージョンにコピーした復旧ポイントからリストアし、ワークロードを復旧
- ・あくまでデータの復旧がメインであるため、インフラストラクチャなどについては別途検討が必要

AWS Backup の基本アーキテクチャ

再掲



モニタリング

バックアップの設計

バックアップの保護

バックアップの自動化

バックアップの復旧



Amazon EventBridge

AWS Backup のバックアップジョブなどの状態が変更された時に発生するイベントをモニタリング



AWS CloudTrail

AWS Backup API コールをイベントとしてキャプチャ



Amazon SNS

バックアップジョブやコピージョブなどのイベントを通知



Amazon CloudWatch

AWS Backup メトリクスのモニタリング



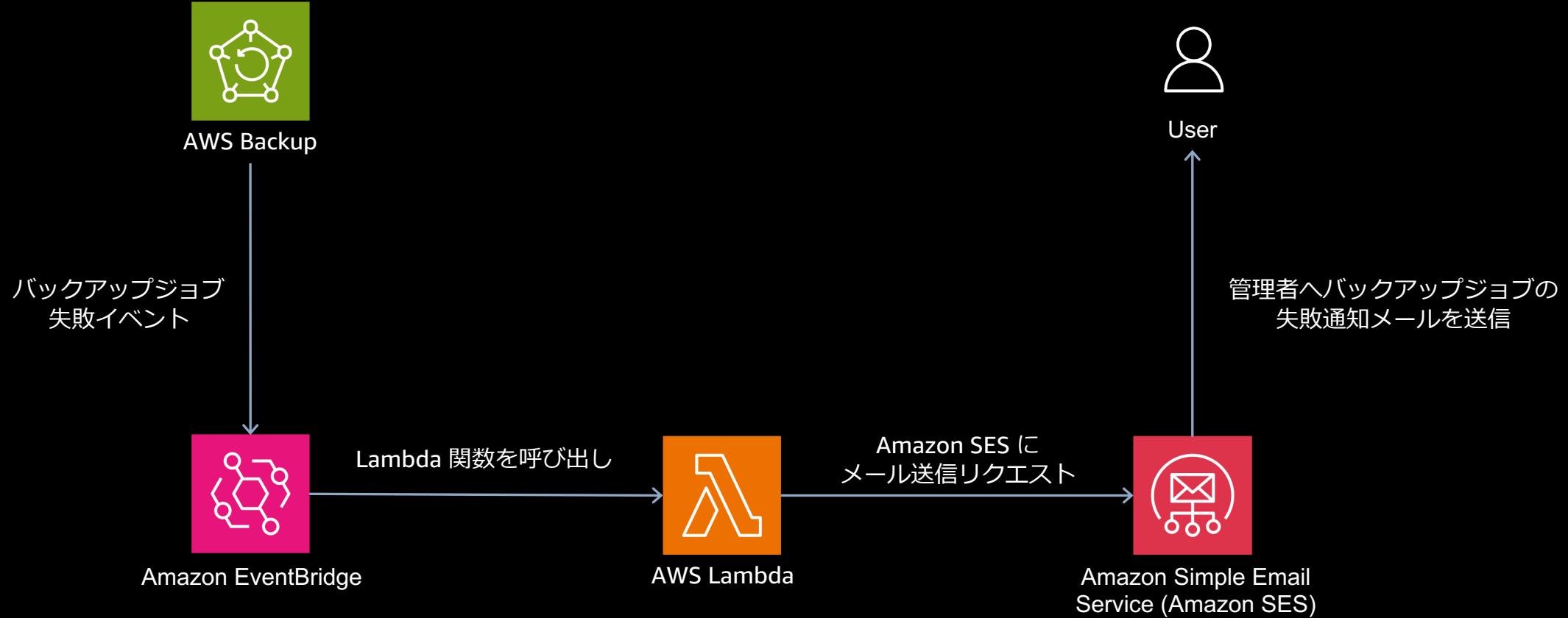
モニタリング

バックアップの設計

バックアップの保護

バックアップの自動化

バックアップの復旧



復元

バックアップの設計

バックアップの保護

バックアップの自動化

バックアップの復旧

バックアップを復元

EC2 インスタンスを復元して、スケジュール済みバックアップ、ライフサイクル管理、迅速な復元などの主要な機能を使用しながら、他のリソースでバックアップを一元管理できるようにします。インスタンス全体の復元機能にアクセスするには、次に移動してください。[インスタンス起動ウィザード](#)

ネットワーク設定

インスタンスタイプ 情報

インスタンスの計算容量とメモリ容量を定義します。

t2.micro - 1 vCPU, 1 GiB RAM

仮想プライベートクラウド (VPC)

VPC を選択して、仮想ネットワーキング環境を定義します。

デフォルトの VPC [REDACTED]



サブネット 情報

異なる EC2 リソースを相互またはインターネットから分離するために使用できる VPC の IP アドレスの範囲を指定します。各サブネットは 1 つのアベイラビリティーゾーンに存在します。

指定なし (任意のアベイラビリティーゾーンのデフォルトサブネット)



セキュリティグループ 情報

セキュリティグループを指定して、インスタンスのトラフィックを制御するファイアウォールルールのセットを決定します。

セキュリティグループを追加



default X

インスタンス IAM ロール 情報

EC2 インスタンスに AWS 認証情報を自動的にデプロイする IAM ロールを指定します。

- IAM ロールなしで続行
- 元の IAM ロールで復元

▼ 詳細設定

シャットダウンと休止動作、終了保護、プレイスメントグループ、テナンシー、およびその他の詳細設定をカスタマイズします。

シャットダウンの動作 情報

OS レベルのシャットダウンを実行したときのインスタンスの動作を指定します。

停止

停止 - 休止動作 情報

- 追加の停止動作として休止を有効化

終了保護を有効化

インスタンスが誤って終了しないように保護します。有効にすると、終了保護が無効になるまで、API または AWS マネジメントコンソールからこのインスタンスを終了することはできません。

プレイスメントグループ 情報

1 つのアベイラビリティーゾーン内のインスタンスの論理グループの名前を指定します。この名前は、ネットワークレイテンシーが低く、全体のネットワークが高いという利点があります。

- プレイスマントグループにインスタンスを追加

T2/T3 無制限

T2/T3 無制限を有効にすると、アプリケーションはいつでも必要なだけベースラインを超えてペーストできます。インスタンスの平均 CPU 使用率がベースライン以下である場合、すべての使用量に対して時間単位のインスタンス料金が自動的に適用されます。それ以外の場合、ベ

- 復元時には復元先の VPC やインスタンスタイプなどリソースタイプに応じたパラメータを指定して復元
- AWS Backup を使用した復元では、既存リソースを上書きすることではなく、新規リソースが作成される



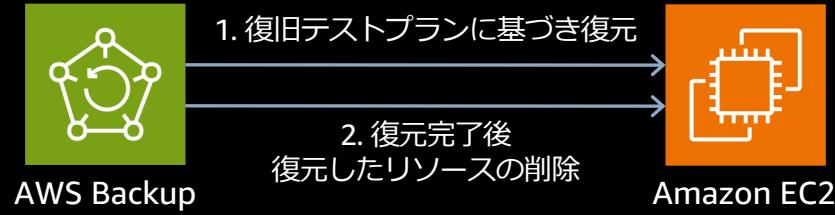
復元テスト

バックアップの設計

バックアップの保護

バックアップの自動化

バックアップの復旧



- ・復元テストプランを作成し、プランに含めるリソースを割り当てる
- ・プランで指定されたスケジュールに基づき復元ジョブが作成され、復元の完了にかかる時間をモニタリング
- ・復元テストが終了すると、復元したリソースは自動的に削除される
- ・オプションとして Amazon EventBridge を使用し、AWS Lambda などを呼び出すことで復元したリソースの検証プロセスを自動化可能

(注) 検証プロセスの実現においては、復元した EC2 インスタンスに対してヘルスチェックを行う等の処理を AWS Lambda などで実装いただく必要があります。

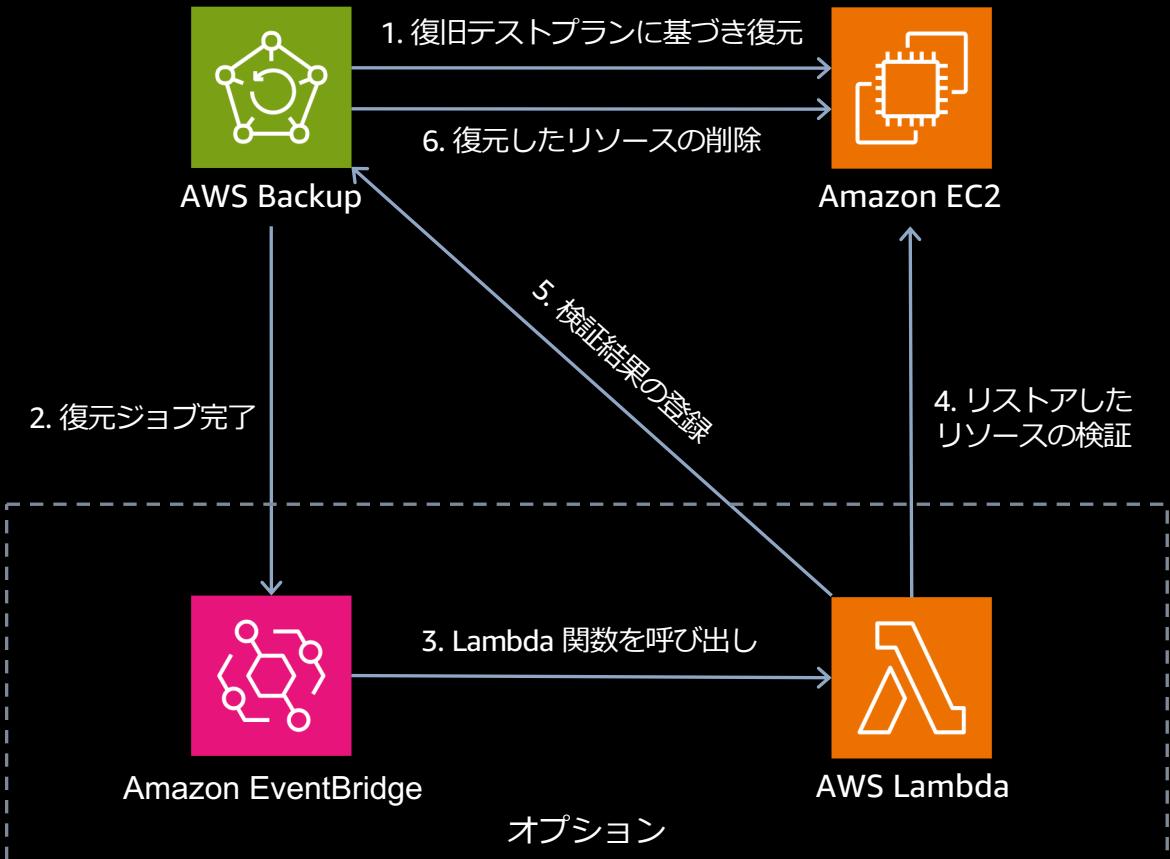
復元テスト

バックアップの設計

バックアップの保護

バックアップの自動化

バックアップの復旧



- 復元テストプランを作成し、プランに含めるリソースを割り当てる
- プランで指定されたスケジュールに基づき復元ジョブが作成され、復元の完了にかかる時間をモニタリング
- 復元テストが終了すると、復元したリソースは自動的に削除される
- オプションとして Amazon EventBridge を使用し、AWS Lambda などを呼び出すことで復元したリソースの検証プロセスを自動化可能

(注) 検証プロセスの実現においては、復元した EC2 インスタンスに対してヘルスチェックを行う等の処理を AWS Lambda などで実装いただく必要があります。

復元テスト

バックアップの設計

バックアップの保護

バックアップの自動化

バックアップの復旧

復元テストプランを作成 情報

頻度、回復ポイント選択ルール、およびその他の項目を指定して、定期的な復元テストを容易に行えるようにします。

全般

復元テストプラン名

RestoreTest_Tokyo

復元テストプラン名では大文字と小文字が区別されます。1~50 文字の英数字またはアンダースコアを含める必要があります。プランの作成後は編集できません。

テスト頻度

復元テストプランを実行する頻度を指定します。

毎日

開始時間

復元テストを開始する時刻を指定します。

00 : 30 Asia/Tokyo (UTC+09:00)

次の時間以内に開始

復元ジョブは、指定された時間枠内に開始されます。例えば、8 時間を選択した場合、復元ジョブはプランの開始予定時刻から 8 時間に内にランダムに開始されます。

8 時間

回復ポイントの選択 情報

この復元テストプランを実行するときにどの復旧ポイントを復元するかを指定します。

ソースポールト

どのポールトから回復ポイントを取得するかを選択します。

- 利用可能なすべてのポールト
- 特定のポールト

特定のポールト

ポールトを選択

BackupVault_Tokyo

リソースを割り当てる 情報

この復元テストプランに含める保護されたリソースを、一度に 1 種類ずつ選択してください。

全般

リソース割り当て名

RestoreTestSelection_Tokyo

リソースの割り当て名では大文字と小文字が区別されます。1~50 文字の英数字またはアンダースコアを含める必要があります。リソースの割り当てが作成された後は編集できません。

IAM ロールを復元

復元テストの実行時に AWS Backup が引き受ける IAM ロールを指定します。

- デフォルトのロール
AWS Backup のデフォルトのロールが存在しない場合は、正しい許可を持つロールが作成されます。
- IAM ロールを選択してください

クリーンアップ前の保持期間 | 情報

復元されたデータが保存される期間（削除されるまでの期間）を指定して、コストを最適化します。クリーンアップ前に検証が必要な場合は、検証の実行に必要な時間を反映するようにこの時間を変更してください。検証が成功すると、データは保持期間にかかわらず削除されます。

- [すぐに削除] を開始
- 特定の時間数について保持

保護されたリソース 情報

リソース ID またはタグを使用して、この復元テストプランにリソースを割り当てます。

リソースタイプ

リソースタイプを選択

復元テストプランの一環として復元するリソースタイプを選択します。

EC2

リソースの選択の範囲

- このリソースタイプのすべての保護されたリソースを含める
- このリソースタイプの特定の保護されたリソースを含める



データのバックアップ & リストアのプロセス

バックアップの設計

バックアップの保護

バックアップの自動化

バックアップの復旧

バックアップボルト

アクセスポリシー

バックアッププラン

バックアッププラン

クロスリージョンコピー

復元

復元テスト

データのバックアップ & リストアのプロセスを網羅的に実現

まとめ

まとめ

- AWS 上の DR 戦略では、バックアップ&リストア・パイロットライト・ウォームスタンバイ・マルチサイトアクティブ/アクティブの 4 つのシナリオがある
- 目標とする RPO/RTO とコストとのトレードオフで、適用するシナリオを決定する
- バックアップ&リストアは短い RPO/RTO が求められないワークフローに適している
- AWS Backup を使用することでバックアップ&リストアに必要なプロセスをマネージドで実現
- バックアップの取得から復旧プロセスまで一元的に管理・自動化

まとめ

- 本セミナーでご紹介していない機能については、別の Black Belt Online Seminar で紹介予定です
 - AWS Backup における継続的バックアップ
 - AWS Organizations と統合した組織内アカウントにおけるバックアップの一元管理
 - バックアップポルトロックによるセキュリティの強化
 - Backup Audit Manager によるコンプライアンス要件の監査
 - ...etc

Thank you!



AWS Black Belt Online Seminar

Savings Plans

Yuki Kasuya / 加須屋 悠己

Technical Account Manager

2025/04



自己紹介

Yuki Kasuya / 加須屋 悠己

アマゾンウェブサービスジャパン

Technical Account Manager



Digital Native Business のお客様を中心に支援しています

好きな AWS サービス : AWS Support

本セミナーの対象者

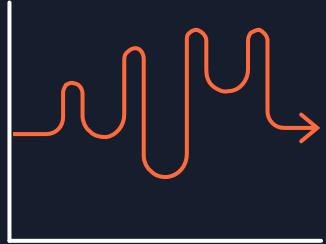
- Savings Plans の概要や購入方法を知りたい方
- Savings Plans のコミットメントに迷っている方
- コンピューティングワークロードのコスト最適化を促進したい方

アジェンダ

1. Savings Plans 概要
2. 購入・設定
3. 購入計画
4. 購入後のモニタリング
5. 制限・注意事項
6. まとめ

Savings Plans 概要

Savings Plans とは



オンデマンド

長期契約なしで、時間または秒単位での支払い



Savings Plans

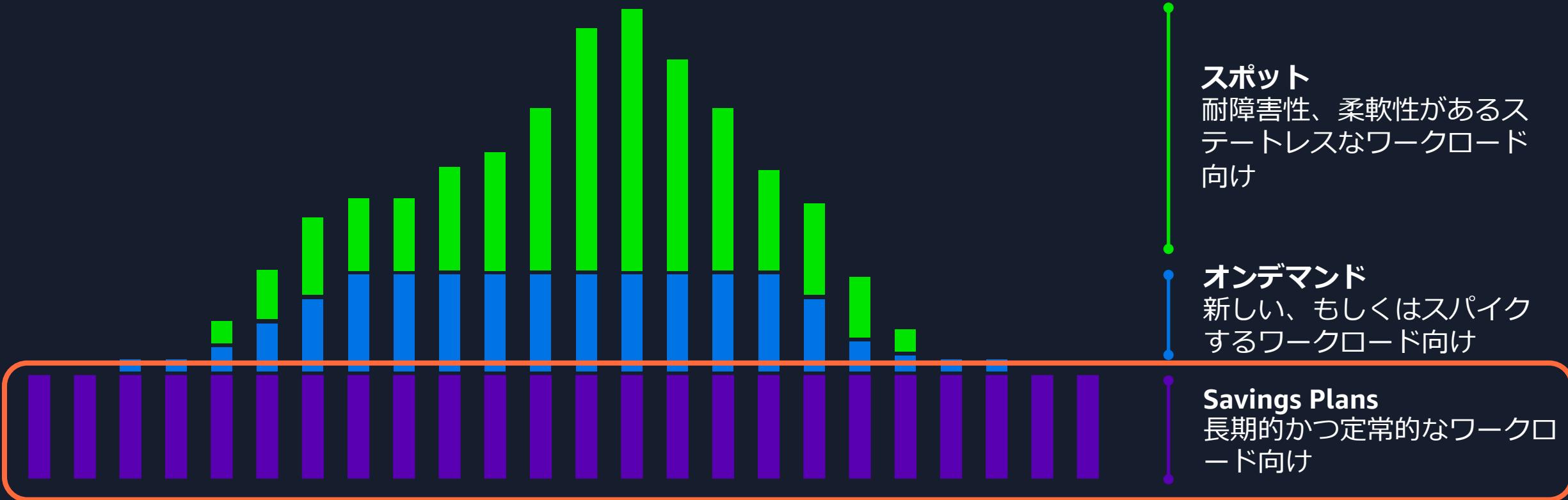
1 年または 3 年間の時間単位のコミットメントで最大 72% 割引



スポット

余剰キャパシティの利用でオンデマンド料金の最大 90% 割引

Savings Plans に適したワークロード



Savings Plans タイプ



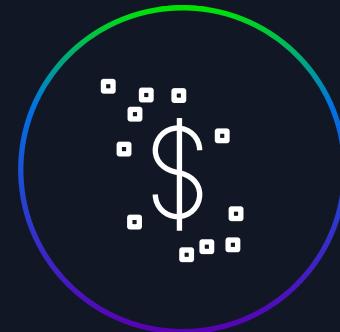
Compute Savings Plans

柔軟性が最も高く、オンデマンド料金から最大 66% の割引が受けられます。EC2, Fargate, Lambda に適用されます。



EC2 Instance Savings Plans

選択した AWS リージョンの特定のインスタンスファミリー(バージニアの M5 など)に対するコミットメントと引き換えに、料金をオンデマンドから最大 72% の割引が受けられます。



SageMaker Savings Plans

SageMaker インスタンスの使用に自動的に適用され、オンデマンド料金から最大 64% の割引が受けられます。

Savings Plans タイプ別比較表

	Compute Savings Plans	EC2 Instance Savings Plans	SageMaker Savings Plans
割引率	最大 66%	最大 72%	最大 64%
適用サービス	EC2, Fargate, Lambda	EC2	SageMaker
インスタンスファミリー	○	固定	○
インスタンスサイズ	○	○	○
リージョン	○	固定	○
OS	○	○	○
テナント	○	○	○

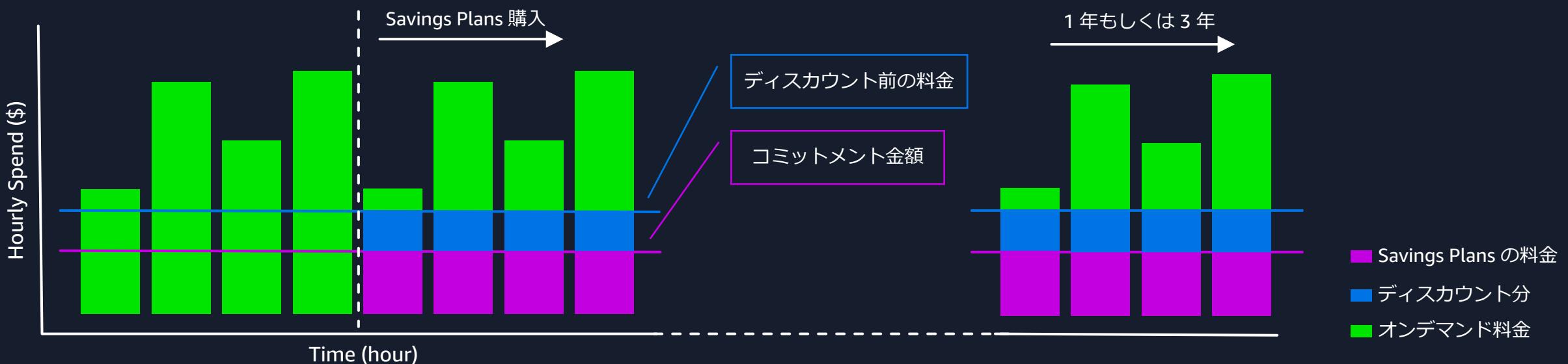
※ ○ はファミリーやサイズなどに関係なく自動的に適用されます

- Compute Savings Plans、EC2 Instance Savings Plans は、Amazon EMR、Amazon EKS や Amazon ECS で利用している EC2 インスタンスにも適用されます
- SageMaker Savings Plans は、SageMaker Studio Notebook, SageMaker Processing, SageMaker Data Wrangler など各機能で利用するインスタンスの使用に自動的に適用されます

コミットメントとは 1/2

Savings Plans は、1 時間あたり \$N を必ず支払う（コミットメント）ので \$N 分までディスカウント後の料金で利用できるというディスカウントプランです。

コミットメント金額は 1 時間あたりの Savings Plans の料金（ディスカウント後の料金）で計算し、1 年か 3 年のどちらかの期間分のお支払いが必要です。



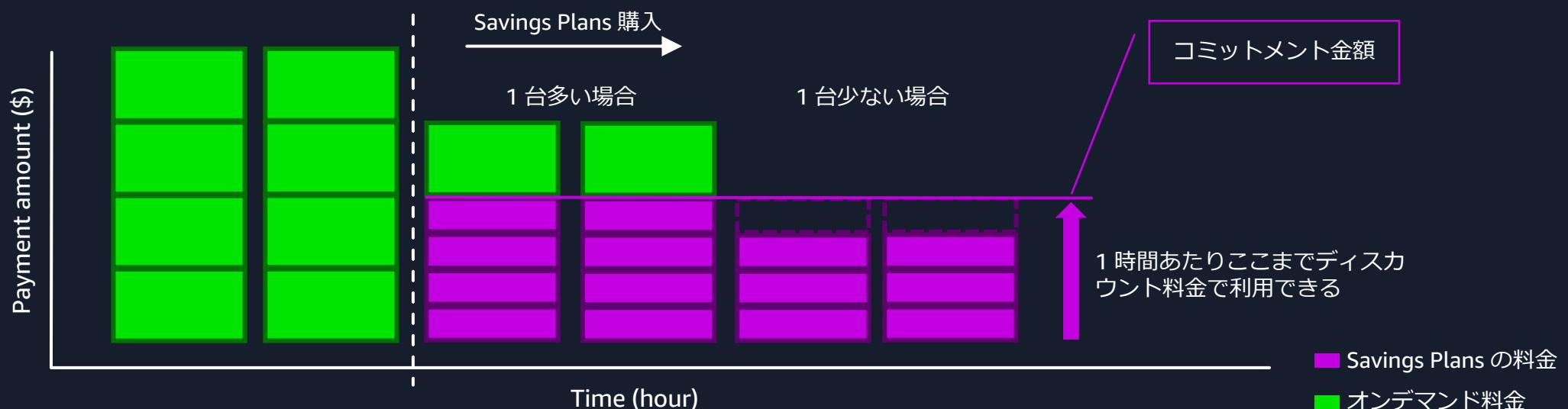
コミットメントとは 2/2

例えば 4 台分の Savings Plans の料金をコミットメント金額とした場合は次となります。

- 1 台多い 5 台 / 1 時間利用した場合、コミットメント金額 + 1 台分のオンデマンド料金のお支払い
- 1 台少ない 3 台 / 1 時間利用した場合、コミットメント金額のお支払い

コミットメント金額は、リソース利用の有無に関わらずお支払いいただく必要があります。

コミットメント金額から取り崩して利用したり、未使用分を繰り越しできるタイプのプランではありません。



支払いオプション

コミットメント金額は3種類の方法のいずれかから選択してお支払いいただくことができます。それぞれ支払いタイミングや割引率が異なりますので状況に応じてご選択ください。

	全額前払い	一部前払い	前払いなし
Savings Plans 開始時の支払い	コミットメント金額一括支払い	コミットメント総額の50%以上で任意に指定可能	なし
毎月の支払い	なし	コミットメント残金を月額費用として支払い	月額費用として支払い
割引率	高	中	低

割引率

Savings Plans の種類、期間、支払いオプション、サービス、インスタンスタイプやリージョンなどにより割引率が異なります。

次のドキュメントでそれぞれの条件における割引率を確認することができます。

- <https://aws.amazon.com/jp/savingsplans/compute-pricing/>
- <https://aws.amazon.com/jp/savingsplans/ml-pricing/>

The screenshot shows the 'Amazon EC2 の Compute Savings Plans' section. It includes dropdown menus for 'AWS リージョン' (US East (Ohio)) and 'リージョン' (US East (Ohio)). It also has dropdowns for '期間' (1年) and '支払いオプション' (前払いなし). At the bottom, there are dropdowns for 'オペレーティングシステム' (Linux) and 'テナント' (共有).

条件選択例

The screenshot displays a table titled '777 個の利用可能なインスタンスを表示' showing savings for various m7g instance types. The columns include 'インスタンス名', 'Savings Plans の料金', 'オンデマンドと比較した費用節減', 'オンデマンド料金', 'リージョン', and 'オペレーティングシステム'. All instances show a 29% savings compared to on-demand rates.

インスタンス名	Savings Plans の料金	オンデマンドと比較した費用節減	オンデマンド料金	リージョン	オペレーティングシステム
m7g.medium	USD 0.0373	29%	USD 0.0527	アジアパシフィック (東京)	Linux
m7g.large	USD 0.0745	29%	USD 0.1054	アジアパシフィック (東京)	Linux
m7g.xlarge	USD 0.149	29%	USD 0.2108	アジアパシフィック (東京)	Linux
m7g.2xlarge	USD 0.2981	29%	USD 0.4216	アジアパシフィック (東京)	Linux
m7g.4xlarge	USD 0.5961	29%	USD 0.8432	アジアパシフィック (東京)	Linux
m7g.8xlarge	USD 1.1922	29%	USD 1.6864	アジアパシフィック (東京)	Linux
m7g.12xlarge	USD 1.7884	29%	USD 2.5296	アジアパシフィック (東京)	Linux

割引率例

(参考) 割引率の違い

Compute Savings Plans

インスタンス名	期間	支払いオプション	Savings Plans の料金	割引率	オンデマンド料金
c6in.large	1	前払いなし	USD 0.11803	17%	USD 0.1428
c6in.large	1	全額前払い	USD 0.11016	23%	USD 0.1428
c6in.large	3	前払いなし	USD 0.07321	49%	USD 0.1428
c6in.large	3	全額前払い	USD 0.06643	53%	USD 0.1428
m7g.large	1	前払いなし	USD 0.0798	24%	USD 0.1054
m7g.large	1	全額前払い	USD 0.0745	29%	USD 0.1054
m7g.large	3	前払いなし	USD 0.0548	48%	USD 0.1054
m7g.large	3	全額前払い	USD 0.0497	53%	USD 0.1054

EC2 Instance Savings Plans

インスタンス名	期間	支払いオプション	Savings Plans の料金	割引率	オンデマンド料金
m7g.large	1	前払いなし	USD 0.0698	34%	USD 0.1054
m7g.large	1	全額前払い	USD 0.0652	38%	USD 0.1054
m7g.large	3	前払いなし	USD 0.0477	55%	USD 0.1054
m7g.large	3	全額前払い	USD 0.0415	61%	USD 0.1054

※ リージョンは東京、OS は Linux、テナントは共有、2025/01 時点

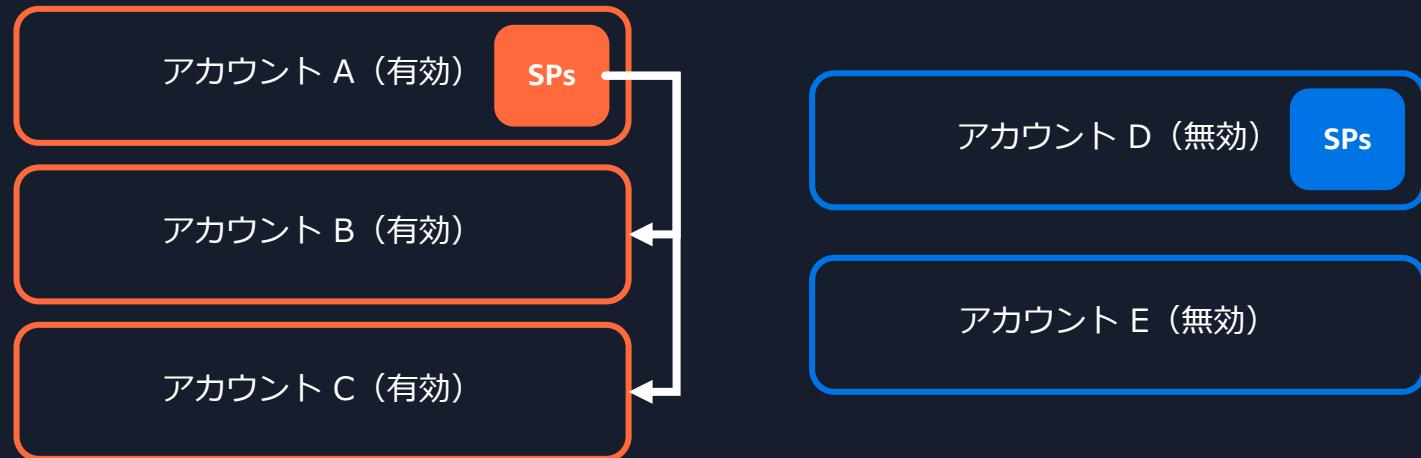
Savings Plans の割引共有

Savings Plans の割引は組織内のアカウントで共有することができます。

アカウント A とアカウント D で Savings Plans を購入し、アカウント A, B, C で共有設定を有効、アカウント D, E の共有設定を無効とする場合、次のようにになります。

- アカウント A の Savings Plans は、まずアカウント A に適用され、未使用の時間単位のコミットメントがある場合、アカウント B, C に適用されます
- アカウント D の Savings Plans に未使用の時間単位のコミットメントがある場合、他のアカウントに共有されません
- アカウント D の Savings Plans をアカウント E にのみ共有するといった設定はできません
- 組織をまたいだ共有もできません

Organization X



Organization Y



適用の仕組み

Savings Plans は、自動的にもっとも割引率が高くなるように適用されます。

- 割引率がもっとも高いリソースから適用されます
- 割引率が同じリソースが複数ある場合は、Savings Plans の料金が低いリソースから適用されます
 - たとえば Fargate の場合、同じ割引率である memory のほうが vCPU よりも Savings Plans の料金が低いため memory に先に適用されます

EC2 リザーブドインスタンスや複数の Savings Plans を購入している場合は、次の順番で適用されます。

1. Savings Plans は EC2 リザーブドインスタンスが適用されたあとに適用されます
2. EC2 Instance Savings Plans は Compute Savings Plans よりも優先して適用されます

共有が有効の場合は、次の順番で適用されます。

1. Savings Plans を購入したアカウントで Savings Plans が適用されます
2. 未使用の時間単位のコミットメントがある場合、Savings Plans は共有が有効になっている組織内の他のアカウントにそれらを自動的に適用します



Savings Plans とリザーブドインスタンスの違い

	Compute Savings Plans	EC2 Instance Savings Plans	コンバーティブル RI*	スタンダード RI
オンデマンドからの削減	最大 66%	最大 72%	最大 72%	最大 72%
金銭的コミットメントと引き換えの低価格	✓	✓	—	—
すべてのインスタンスファミリーに自動的に価格を適用	✓	—	—	—
すべてのインスタンスサイズに自動的に価格を適用	✓	✓	—**	—**
すべてのテナントや OS に自動的に価格を適用	✓	✓	—	—
Fargate を使用して Amazon ECS と Amazon EKS に自動的に適用	✓	—	—	—
Lambda に自動的に適用	✓	—	—	—
AWS リージョン全体に自動的に価格を適用	✓	—	—	—
1 年または 3 年の期間オプション	✓	✓	✓	✓

* コンバーティブル RI は、異なるインスタンスファミリー、サイズ、OS、テナントに変更できますが、交換は手動で行う必要があります。

** リージョンのコンバーティブル RI とリージョンのスタンダード RI により、インスタンスサイズに柔軟に対応できます。

https://docs.aws.amazon.com/ja_jp/savingsplans/latest/userguide/sp-ris.html



購入・設定

カート

Savings Plans にはカート機能があり、購入準備が整うまでカートに保管されます。カートに追加後、レビューしてから購入することができます。

カート 情報

Savings Plans (3) 情報

開始日を設定 カートから削除 カートをクリア

□ タイプ	期間	リージョン	インスタンスタイプ	購入オプション	開始日	コミットメント	前払い料金	月額料金	合計コスト
□ Compute	1年間	-	-	No Upfront	2026-01-01 00:00:00 UTC	\$1.00000/時間	\$0.00	\$730.00	\$8,760.00
□ EC2 Instance	1年間	Asia Pacific (Tokyo)	c7g	No Upfront	2027-01-01 10:00:00 UTC	\$2.00000/時間	\$0.00	\$1,460.00	\$17,520.00
□ SageMaker	3年間	-	-	All Upfront	今すぐ	\$1.00000/時間	\$26,280.00	\$0.00	\$26,280.00

概要

コミットメントの総額	\$52,560.00
今すぐ開始されるコミットメントの総額	\$26,280.00
キューに登録されたコミットメントの総額	\$26,280.00
現在支払期日となっている前払い料金の合計額	\$26,280.00

税金が加算される場合があります。

別の Savings Plan を追加 注文書の送信

カート画面

推奨事項からの購入

推奨事項で提示されるコミットメント金額を直接カートに追加できます。

1. ナビゲーションペインの [Savings Plans] で [推奨事項] を選択します
2. 推奨事項の更新日が古い場合、[推奨事項を更新] から手動で推奨事項を更新します
3. 推奨事項パラメータで購入する Savings Plans タイプを選択し、推奨事項オプションを適切に設定します
4. [詳細を表示] からカバレッジや使用率をグラフで確認します
5. 購入したい Savings Plans のカラムにチェックを入れます
6. [Savings Plans をカートに追加] を選択します
7. カートを確認し、問題なければ購入します

The screenshot shows the AWS Savings Plans purchase interface. At the top, there's a header bar with a 'CSV' download button and a 'Purchase Analyzer' button. Below it, the main area has two tabs: '推奨事項' (Recommended) and '購入' (Purchase).
推奨事項 (Recommended) Tab:
This tab displays a list of recommended Savings Plans. It includes columns for 'アクション' (Action), 'Savings Plans 期間' (Period), '支払いオプション' (Payment Option), 'コミットメント' (Commitment), and '推定期間' (Projected Period). A '詳細を表示' (View Details) button is also present.
詳細 (Details) Tab:
This tab provides a detailed view of a selected Savings Plan. It features a chart showing 'カバレッジ' (Coverage) over time, with bars representing usage and a blue line representing the commitment amount. Below the chart, there are three summary boxes:

- Savings Plan の推奨事項:** \$0.75/時間
- 推定期間:** \$245.83/月
- 推定期間割合 (%):** 11%

Cart Summary (Purchase Tab):
The cart summary shows a total of \$1.02 (27%) for a 1-year commitment. It includes buttons for 'CSV のダウンロード' (Download CSV), 'Purchase Analyzer', and 'Savings Plans をカートに追加' (Add to Cart).

推奨事項画面

カスタムコミットメントによる購入

1. ナビゲーションペインの [Savings Plans] で [Savings Plans の購入] を選択します
2. 購入の詳細で、Savings Plans タイプと期間を選択します
3. 購入コミットメントで、時間単位のコミットメント金額を入力し、支払いオプションを選択します
4. (オプション) Savings Plans を開始する日付を指定する場合、開始日で日付と時刻 (UTC) を入力します
5. 購入の概要で、コストを確認し [カートに追加] を選択します
6. カートを確認し、問題なければ購入します



カスタムコミットメント画面

キューイングによる購入

Savings Plans の購入を将来の日付で行うようにキューに登録することや、スケジュールを設定することができます。

前払い料金または定期料金は、選択した開始日にキューに登録されている購入が処理された場合にのみ請求されます。

このキューに登録されている Savings Plans は、インベントリから確認でき、開始日の前であればいつでも削除できます。希望するコミットメント金額が変わった場合はキューから削除し新しく設定してください。

開始日を設定する

選択された Savings Plan を開始する日付と時刻 (UTC) を設定します。

日付 時刻
2026/01/01 00:00:00

開始する日付と時刻は、お使いのブラウザのローカルタイムゾーン (+09:00) の 2026-01-01 09:00:00 に設定されます。

キャンセル 開始日を削除 確認

開始日の設定画面

Savings Plan の詳細 情報		キューに登録された Savings Plan を削除する	
アカウント名	account_name	Savings Plan ID	xxxx-xxxx-xxxx-xxxx-xxxx
アカウント ID	12345678912	Savings Plans タイプ	コンピューティング
ステータス	④ キューに入れられました	インスタンスファミリー	-
開始日 (UTC)	2026-01-01 00:00:00 UTC	リージョン	-
終了日 (UTC)	2026-12-31 23:59:59 UTC	Savings Plan 料金	↓ Savings Plan 料金をダウンロード
		支払いオプション	No Upfront
		MTD 実割引額	-
		MTD 使用率	-
		MTD コミットメント	-
		使用履歴	使用状況レポートを表示

キューイングされた Savings Plan



更新

1. ナビゲーションペインの [Savings Plans] で [インベントリ] を選択します
2. 更新対象の Savings Plan をチェックします
3. [アクション] を選択します
4. [Savings Plan を更新する] を選択します
5. カートに追加されます

もしくは、更新対象の Savings Plan の詳細ページの [Savings Plan を更新する] から更新します。

更新する場合は同じプランとなり Savings Plans の開始日は現在の Savings Plans の有効期限の 1 秒後に設定されキューに登録されます。

Savings Plans (2) 情報

このアカウントが所有する Savings Plans のインベントリ。Savings P

キューに登録された Savings Plan を削除する

Savings Plan を更新する

アクション ▲ CSV のダウンロード ▼ Savings Plan を購入

プロパティまたは値別にリソースをフィルター

Savings Plan ID | ステータス | タイプ | インスタンスファミリー | リージョン

xxxx-xxxx-xxxx-xxxx-xxxx | キュー済み - 削除済み | コンピューティング | - | -

yyyy-yyyy-yyyy-yyyy-yyyy | アクティブ | コンピューティング | - | -

インベントリページ

Savings Plan の詳細 情報

Savings Plan を返却する Savings Plan を更新する

アカウント名 account_name	Savings Plan ID xxxx-xxxx-xxxx-xxxx-xxxx	支払いオプション No Upfront	MTD 実割引額 -
アカウント ID 123456789012	Savings Plans タイプ コンピューティング	コミットメント \$1.00000/時間	MTD 使用率 -
ステータス ④ アクティブ	インスタンスファミリー -	前払い料金 \$0.00	MTD コミットメント -
開始日 (UTC) 2025-03-05 07:01:41 UTC	リージョン -	定期料金 \$1.00000	使用履歴 使用状況レポートを表示
終了日 (UTC) 2026-03-05 07:01:40 UTC	Savings Plan 料金 Savings Plan 料金をダウンロード	返却可能期限 2025-03-12 07:01:41 UTC	詳細は こちら

Savings Plans 詳細ページ

解除（キャンセル・返却）

2024/03 から Savings Plans 購入後 7 日間以内であれば解除（キャンセル・返却）することが可能になりました。コミットメント金額を間違えてしまった場合などにご利用いただけます。

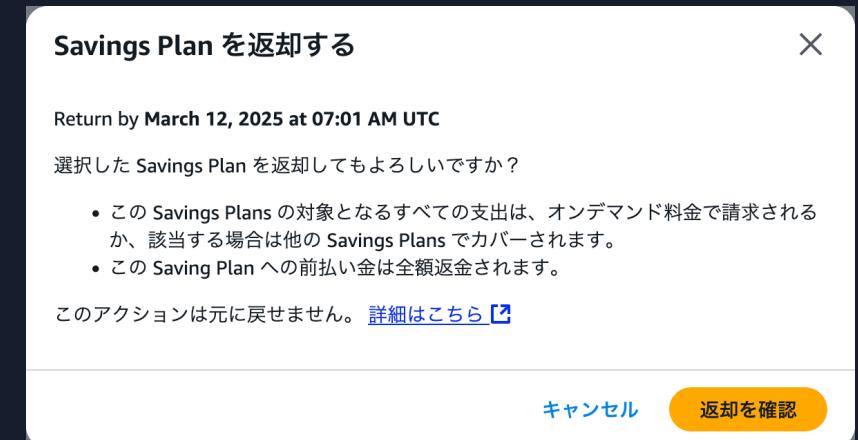
- <https://aws.amazon.com/jp/about-aws/what-new/2024/03/aws-7-day-window-return-savings-plans/>

次の制限事項があります。

- **1 時間あたりのコミットメント額が \$100 以下**
- **購入から 7 日以内**
- **購入した暦月内**
- **管理アカウントごとに年間 10 回まで**

解除リクエストがエラーとなった場合は、次のドキュメントをご参照ください。

- https://docs.aws.amazon.com/ja_jp/savingsplans/latest/userguide/return-sp.html#return-sp-restrictions



キャンセル画面例

割引共有の設定

管理アカウントから共有の設定を変更できます。

- ・ [請求とコスト管理] -> [請求設定] から共有を有効化・無効化することができます
 - ・ 新しく作成されたメンバーアカウントとの共有をデフォルト有効にするかどうかを設定できます
- 共有が有効になっている場合のコストの見え方と請求は次に従います。
- ・ Cost Explorer などに表示される推定のコストは、その時点の共有の設定に基づきます
 - ・ 最終的な請求に関しては、月の最終日の午後 11 時 59 分 59 秒 (UTC 時) に指定されている共有の設定に基づいて決定されます

リザーブドインスタンスおよび Savings Plans の割引共有設定 [情報](#)

新しく作成したメンバーアカウントとのデフォルト共有
 有効化済み

共有が有効になっているアカウント
2/2 アカウント

アカウント名	アカウント ID	共有設定
accountX	123456789012	<input checked="" type="radio"/> 有効化済み
accountY	987654321098	<input checked="" type="radio"/> 有効化済み

アクション ▾ 無効化 有効化

共有設定画面



アラートサブスクリプション

Savings Plans の有効期限が近づいている場合やキューに入れた Savings Plans の購入日が近づいたときにメールで通知することが可能です。

[概要] -> [アラートサブスクリプションを管理] から設定できます。



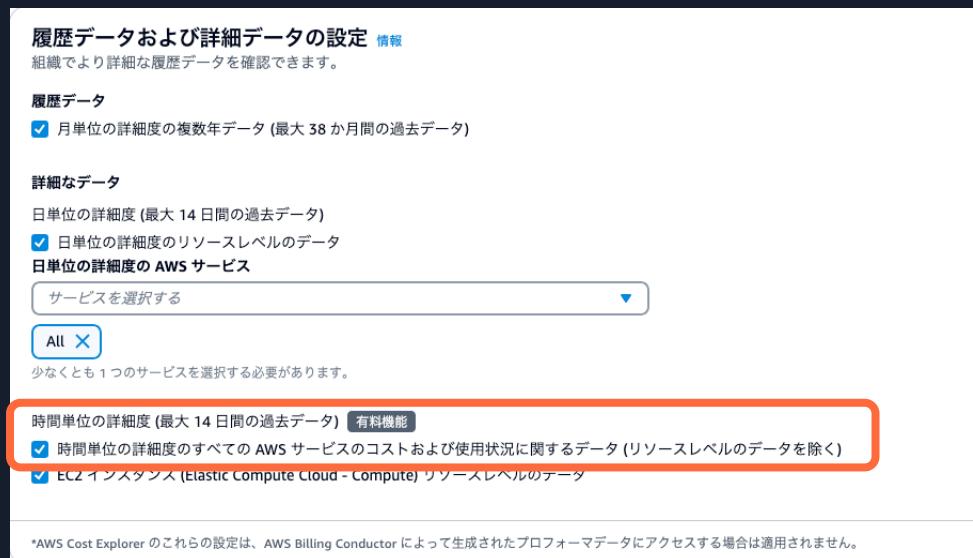
アラートサブスクリプション画面

時間単位のデータ（有料機能）

Cost Explorer の設定で時間単位の粒度のデータを有効にすることができます。Savings Plans のコミットメントは 1 時間単位となりますので、より詳細なデータで購入計画を立てたい・モニタリングしたい場合は、時間単位の詳細度の設定を有効にしてください。

Savings Plans の使用状況レポートとカバレッジレポートでも利用できます。

[コスト管理の設定] -> [Cost Explorer] タブから設定できます。



設定画面

アクセスコントロール

IAM ポリシーにより、個々のユーザーの Savings Plans の購入や閲覧などを管理できます。

次の 2 つの AWS マネージドポリシーをご利用いただけます。

- AWSSavingsPlansFullAccess
 - Savings Plans へのフルアクセスを付与します
- AWSSavingsPlansReadOnlyAccess
 - Savings Plans への読み取り専用アクセスを付与します
- https://docs.aws.amazon.com/ja_jp/savingsplans/latest/userguide/identity-access-management.html
詳細にアクセスを管理したい場合は、次のドキュメントをご参照ください。
- https://docs.aws.amazon.com/ja_jp/service-authorization/latest/reference/list_awssavingsplans.html

アクション例	概要
savingsplans:CreateSavingsPlan	Savings Plan を購入する許可を付与
savingsplans:DescribeSavingsPlans	アカウントに関連付けられた Savings Plans を参照する許可を付与
savingsplans:ReturnSavingsPlan	Savings Plan を解除（キャンセル・返却）する許可を付与

購入計画

コミットメント



購入アカウント

- 管理アカウントや購入専用アカウントでの購入
- 個別のメンバー アカウントでの購入



タイプ・オプション

- Compute Savings Plans
- EC2 Instance Savings Plans
- 全額前払い
- 前払いなし



コミットメント金額

- 推奨事項での購入
- カスタムコミットメントでの購入

推奨事項

推奨事項では、過去の利用状況を分析し、最大限のディスカウントを受けられる最適なコミットメント金額を提示します。将来の予測は含まれていません。

推奨事項での購入は、次の場合に検討します。

- ・コスト最適化が進んでいる
- ・将来のワークロードが増加することが決まっている
- ・別の組織へのアカウント譲渡予定がない

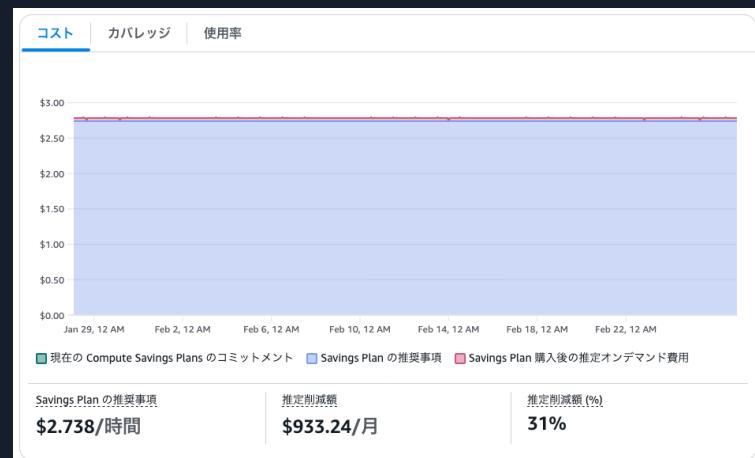
推奨事項での購入が適切でない場合もあります。コスト最適化が進んでいない状況や今後ワークロードの減少が見込まれる場合はオーバーコミットメントとなるリスクがあります。

The screenshot shows a summary table for a recommended savings plan:

推奨される購入の前	推奨される購入の後	推奨事項の詳細
現在の月別オンデマンド使用量 \$2,965.73 (\$4.06/時間)	推定月別支出額 \$2,032.49 (\$2.78/時間)	推定月別削減額 \$933.24 (\$1.28/時間)

Below the table, a note states: "1件の推奨される コンピューティング Savings Plan を合計 \$2.738/時間のコミットメントで購入すると、毎月推定 \$933 を削減できます。" A detailed description follows, mentioning a 30-day usage baseline and a projected savings of \$933 per month.

At the bottom, there are buttons for "CSV のダウンロード" and "Savings Plans をカードに追加".

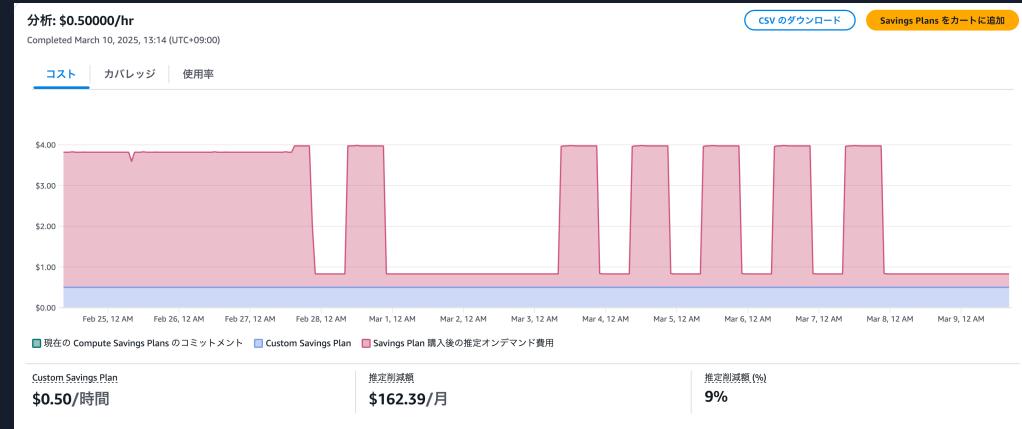


推奨事項画面例

Savings Plans Purchase Analyzer

2024/11 から Savings Plans Purchase Analyzer が利用可能になり、自分で決めたコミットメント金額でどの程度のコスト、カバレッジや使用率になるか確認できます。次を設定できます。

- カスタムコミットメント金額
- 柔軟なルックバック期間
- 期限切れが近い Savings Plans の除外
 - 従来、期限が切れた後に推奨事項などを確認し、どの程度のコミットメント金額にするかの判断基準とする場合がありましたが、期限切れを待たずに対応・クーニングでの購入が実現できます



(参考) コミットメントの決め方例

組織内にメンバーアカウントが 100 以上あり複数リージョンで利用中。数アカウントには今後 3 年以上リソースの変動がない安定したワークロードがあるが、多くのアカウントでは将来の利用予測はできずコスト最適化の状況はまちまち。組織全体としてコスト最適化を進めるがリスクをとらない戦略。今後組織全体としてのワークロードの増減は不透明という想定の例です。

1. アカウント

- 管理アカウントで購入します。組織全体でコスト最適化を進め、最大のディスカウントを受けるためです

2. タイプ・オプション

- Compute Savings Plans を購入します。複数リージョンで稼働していることやコスト最適化の状況がまちまちでありインスタンスタイプ変更の可能性などがあるためです
- 安定したワークロード向けに 3 年・前払いなし、その他のワークロード向けに 1 年・全額前払いの組み合わせとします。割引率は大きくするが、ワークロードの増減が不透明なため 1 年単位で調整しやすくするためです

3. コミットメント金額

- 1 年目は 60% 前後のカバレッジを目標とします。コスト最適化の余地があり、今後ワークロードの増減が不透明のためです
- 3 年・前払いなし分について、リソースを把握できるため手動でコミットメント金額を計算します
- 1 年・全額前払い分について、Savings Plans Purchase Analyzer を利用して 60% カバレッジとなるコミットメント金額を確認します

Savings Plans の使用率とカバレッジをモニタリング、ワークロードの状況も考慮し、次年度の 1 年・全額前払いのコミットメント金額を調整して中長期に渡るコスト最適化を進めます。

損益分岐点

東京リージョンで 1 年、全額前払いとし t3a.medium を対象とした場合の 1 年間の損益分岐点の例です。

- ・ オンデマンド料金は、 $\$0.049000 * 730 \text{ 時間} * 12 \text{ヶ月} = \429.24
- ・ Savings Plans 料金は、 $\$0.0359 * 730 \text{ 時間} * 12 \text{ヶ月} = \314.484
- ・ 損益分岐率は、 $314.484 / 429.24 = 0.732$
- ・ 損益分岐点は、 $0.732 * 730 \text{ 時間} * 12 \text{ヶ月} = 6412.32 \text{ 時間}$

となり、1 年間の t3a.medium の起動時間が 6412.32 時間を超える（概ね 9 ヶ月程度）場合は Savings Plans の方が得に利用できます。

EC2 に関しては、AWS Pricing Calculator で各インスタンスタイプ個別の損益分岐点が確認できます。

- ・ <https://calculator.aws/#/createCalculator/ec2-enhancement>

コミットメント金額の計算方法

コミットメント金額を手動で算出する場合、次のドキュメントに Savings Plans の料金が記載されています、こちらをご利用ください。（コミットメント金額は割引後の Savings Plans の料金であり、オンデマンド料金ではありませんのでご注意ください）

- <https://aws.amazon.com/jp/savingsplans/compute-pricing/>

(参考) コミットメント金額の計算方法 EC2

[Amazon EC2 の使用に適用される Compute Savings Plans] もしくは [EC2 Instance Savings Plans] タブを選択し、リージョン、期間、支払いオプション、OS や CPU アーキテクチャを選択します。

- <https://aws.amazon.com/jp/savingsplans/compute-pricing/>

東京リージョンで 1 年、全額前払いの m7g.large の Compute Savings Plans 料金は、1 時間あたり \$0.0745 となります。

たとえば、東京リージョンで m7g.large を 4 台利用しており、すべてに Savings Plans を適用させたい場合は、Savings Plans の料金が \$0.0745 となるため、コミットメント金額は $\$0.0745 * 4 = \$0.298 / \text{hour}$ となります。

(参考) コミットメント金額の計算方法 Fargate

[AWS Fargate の使用に適用される Compute Savings Plans] タブを選択し、リージョン、期間、支払いオプション、OS や CPU アーキテクチャを選択します。

- <https://aws.amazon.com/jp/savingsplans/compute-pricing/>

Fargate に関する、東京リージョン、1 年、全額前払いの Compute Savings Plans 料金は、1 時間あたりの GB 単位は \$ 0.0043134、vCPU 単位は \$ 0.0394368 となります。

たとえば、1 時間あたり 0.25 vCPU, メモリ 0.5G のタスクを 80 個、0.5 vCPU, メモリ 1G のタスクを 20 個利用の場合は、 $(0.25 \text{ vCPU} * 80 + 0.5 \text{ vCPU} * 20) * \$ 0.0394368 + (0.5 \text{ G} * 80 + 1 \text{ G} * 20) * \$ 0.0043134 = \$ 1.441908 / \text{hour}$ となります

。

(参考) コミットメント金額の計算方法 Lambda

[AWS Lambda の使用に適用される Compute Savings Plans] タブを選択し、リージョン、期間や支払いオプションを選択します。

- <https://aws.amazon.com/jp/savingsplans/compute-pricing/>

Lambda に関する、東京リージョン、1年、全額前払いの Compute Savings Plans 料金は、1M リクエストあたり \$0.2、1 秒間あたり 1 GB が \$0.0000142 となります。なお、リクエストの使用量については特別な割引はありませんが、Savings Plans の契約対象となります。（Provisioned Concurrency や ARM を利用している場合は料金が異なります。）

たとえば、1 時間あたりのリクエスト数が 1,000 万で メモリが 0.5GB の関数を 3,600 秒利用の場合は、 $(1,000 \text{ 万} / 100 \text{ 万}) * \$0.2 + 3,600 * (0.5\text{GB} / 1\text{GB}) * \$0.0000142 = \$2.02556 / \text{hour}$ で計算します。

購入後のモニタリング

Savings Plans の一覧

現在組織またはアカウントで購入している Savings Plans の一覧とステータスがインベントリで確認できます。
これらの一覧は CSV としてダウンロードできます。

インベントリ 情報

Savings Plans (3) 情報

このアカウントが所有する Savings Plans のインベントリ。Savings Plans のデータが使用できるようになるまでに最大 48 時間かかることがあります。

プロパティまたは値別にリソースをフィルター

アクション ▾ CSV のダウンロード ▾ Savings Plan を購入

Savings Plan ID	ステータス	タイプ	インスタンスファミリー	リージョン	コミットメント	開始日 (UTC)	終了日 (UTC)
xxxx-xxxx-xxxx-xxxx-xxxx	☑ アクティブ	コンピューティング	-	-	\$0.50000/時間	2025-03-17 06:47:02	2026-03-17 06:47:01
xxxx-xxxx-xxxx-xxxx-xxxx	☒ キュー済み - 削除済み	コンピューティング	-	-	\$1.00000/時間	2026-01-01 00:00:00	2026-12-31 23:59:59
xxxx-xxxx-xxxx-xxxx-xxxx	⊖ 返却済み	コンピューティング	-	-	\$1.00000/時間	2025-03-05 07:01:41	2025-03-05 07:01:41

インベントリ

使用状況

使用率とは、Savings Planが利用された割合を示す指標です。

使用状況レポートの上段の各項目は次となります。

- **Savings Plans の支出**
 - Savings Plans の金額
 - 前払いした場合でも選択した期間で按分した金額となります
- **オンデマンド支出の相当額**
 - オンデマンド料金で計算した場合の金額
- **正味の合計削減額**
 - オンデマンド支出の相当額 - Savings Plans の支出で算出されるSavings Plans によるコスト削減効果



使用状況レポート画面

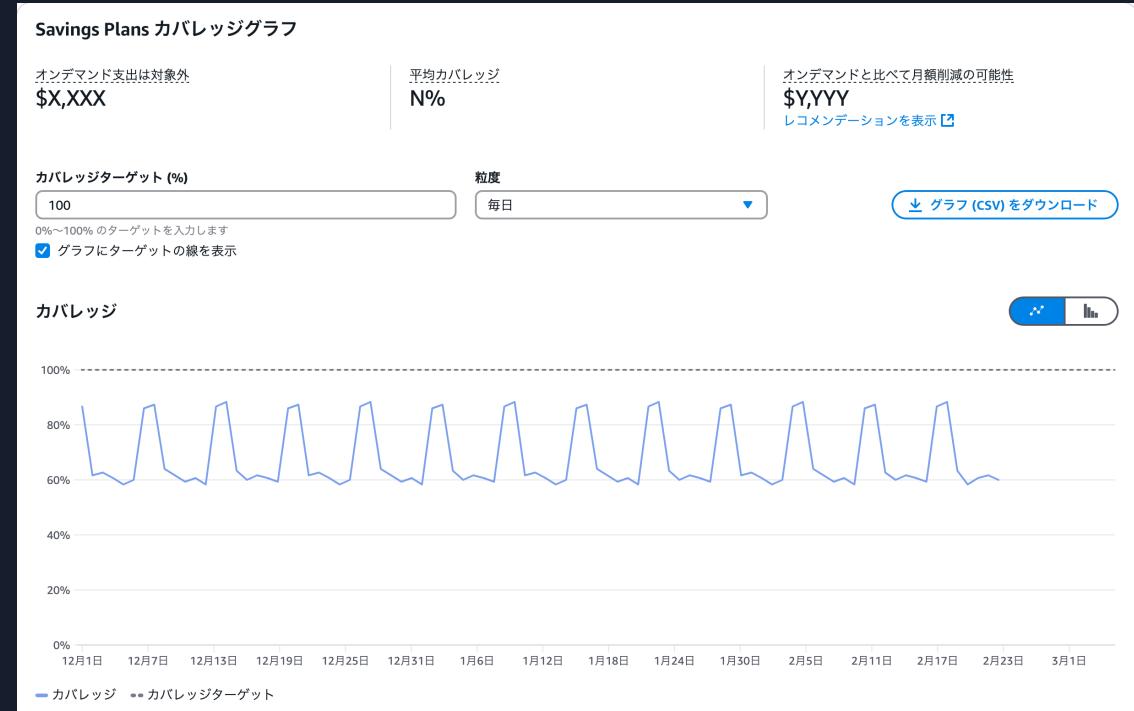
カバレッジ

カバレッジとは、Savings Plans の対象であるリソースの利用料のうち Savings Plans でカバーしている割合です。

カバレッジレポートの上段の各項目は次となります。

- ・ **オンデマンド支出は対象外**
 - オンデマンド料金でお支払いいただいた金額
- ・ **平均カバレッジ**
 - 日付範囲の平均カバー率
- ・ **オンデマンドと比べて月額削減の可能性**
 - 推奨事項の Savings Plans を購入した場合に削減可能な金額

下部のテーブルの内訳から、各リソース個別の Savings Plans の適用状況が把握できます。



カバレッジレポート画面

AWS Budgets による追跡

AWS Budgets を利用し、Savings Plans の使用率とカバレッジを追跡できます。使用率またはカバレッジが下がっている場合に通知できるため、無駄なく利用したい場合に設定しご利用ください。

予算タイプ

- コスト予算 - 推奨**
指定された金額に照らしてコストを監視し、ユーザー定義のしきい値に達したときにアラートを受け取ります。コスト予算を使用するときは、設定する予算額が、予想されるクラウド支出を表します。例えば、ある事業部門に対してコスト予算を設定してから、関連付けられたメンバーアカウントなどの追加のパラメータを設定できます。
- 使用量予算**
指定された 1 つ、または複数の使用タイプまたは使用タイプグループの使用量を監視し、ユーザー定義のしきい値に達したときにアラートを受け取ります。使用量予算を使用するときは、予算額が、予想される使用量を表します。例えば、使用量予算を使用して、Amazon EC2 や Amazon S3 などの特定のサービスの使用量を監視できます。
- Savings Plans の予算**
Savings Plans に関連付けられている使用率またはカバレッジを追跡して、それらの割合がユーザー定義のしきい値を下回った場合にアラートを受け取ります。カバレッジターゲットを設定すると、Savings Plans の対象となるインスタンスの使用量を確認できます。使用率ターゲットを設定すると、Savings Plans が使用されていない、または使用率が低いかどうかを確認できます。
- 予約予算**
予約に関連付けられている使用率またはカバレッジを追跡して、それらの割合がユーザー定義のしきい値を下回った場合にアラートを受け取ります。カバレッジターゲットを設定すると、予約の対象となるインスタンスの使用量を確認できます。使用率ターゲットを設定すると、予約が使用されていない、または使用率が低いかどうかを確認できます。予約アラートは、Amazon EC2、Amazon RDS、Amazon Redshift、Amazon ElastiCache、および Amazon Elasticsearch の予約でサポートされています。

予算タイプ

使用率のしきい値

期間
日次予算は、予測アラート、または日次予算計画の有効化をサポートしません。

月

支出のモニタリング | 情報
Savings Plans に対する予算の設定に使用率 (%)、カバレッジ (%) のどちらを使用するかを選択します。

- Savings Plans の使用率**
使用率は、未使用または使用率が低い Savings Plans がないかどうかを測定します。
- Savings Plans のカバレッジ**
カバレッジは、Savings Plans の対象となっているインスタンスの使用量を測定します。

使用率のしきい値 (%)
最低限必要と考える Savings Plans の使用率を、パーセント値で入力してください。

① 推奨予算: 0.00% (前月に基づく)

しきい値設定

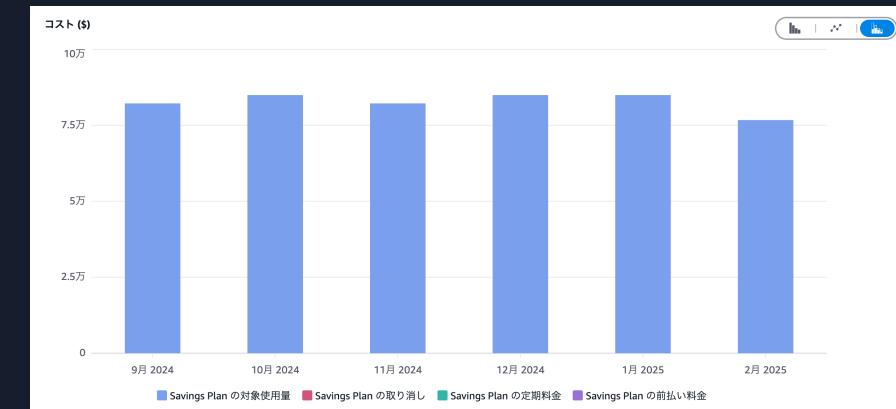
Cost Explorer 詳細オプション

詳細オプションで、コストの表示方法を切り替えられます。

- 非ブレンドコスト
 - 請求書通り支払うコスト表示。Savings Plans の前払い料金や定期的な料金およびオンデマンド料金のコストを確認できます
- 償却コスト
 - 前払い料金をコミットメント期間で按分したコスト表示。実効コストやリソースの利用状況を確認できます



非ブレンドコスト表示



償却コスト表示

▼ グループ化の条件
ディメンション クリア
料金タイプ

料金タイプ クリア
料金タイプを含む (1)
Savings Plan の対象使用量

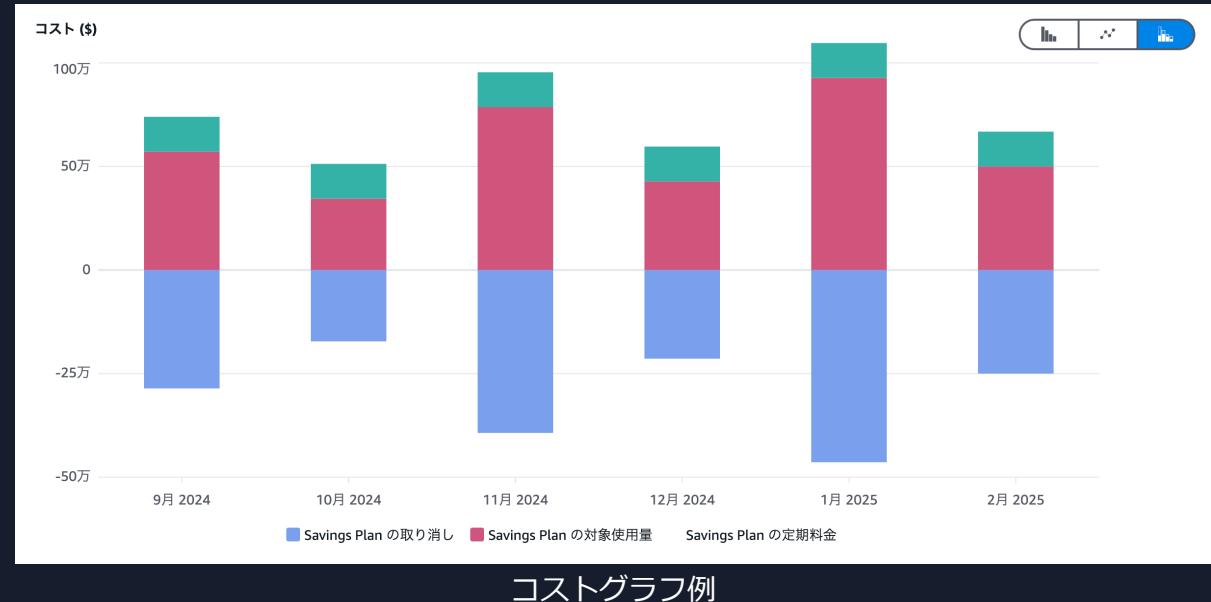
▼ 詳細オプション
次で集計したコスト: 情報
非ブレンドコスト
償却コスト

フィルタ例

Cost Explorer 料金タイプフィルタ

Cost Explorer のフィルタを利用し Savings Plans の各料金を把握できます。（非ブレンドコスト表示）

- 料金タイプ
 - **Savings Plan の前払い料金**
 - 全額前払い、一部前払いで一括でお支払いいただいた金額
 - **Savings Plan の定期料金**
 - 一部前払い、前払いなしで毎月お支払いいただいた金額
 - **Savings Plan の対象使用量**
 - Savings Plans でカバーされた金額
 - **Savings Plan の取り消し**
 - Savings Plans が適用され相殺されたマイナスの金額

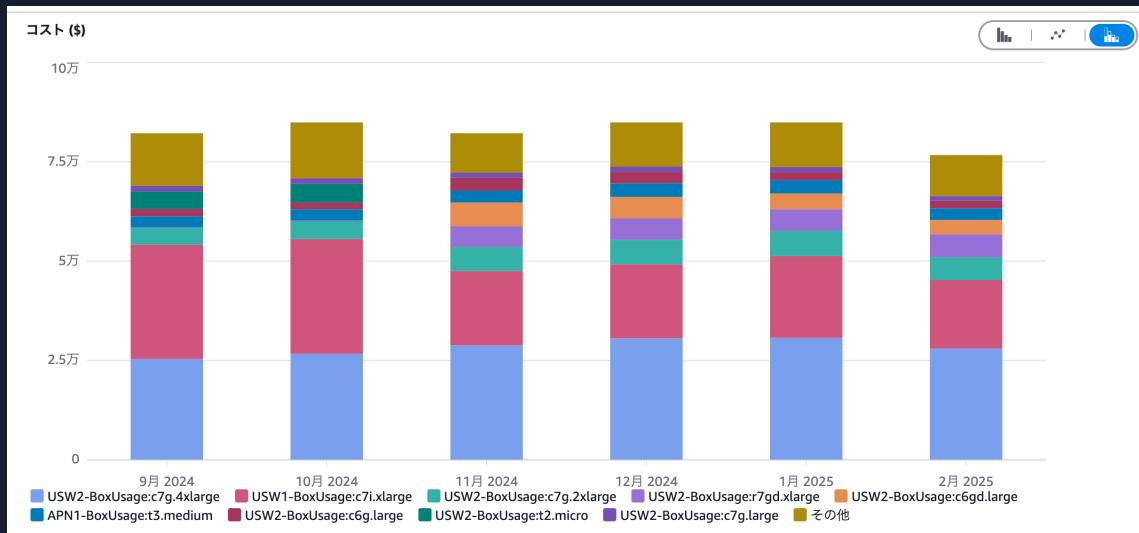


コストグラフ例

Cost Explorer Savings Plan の対象使用量

Savings Plans が適用されたリソースを確認できます。オンデマンド料金の場合のコストと Savings Plans の料金の場合のコストを確認できます。実際にお支払いいただく金額と一致しない場合があります。

- ・ オンデマンド料金のコスト表示
 - 使用タイプでグループ化、料金タイプを Savings Plan の対象使用量、非ブレンドコスト表示
- ・ Savings Plans の料金のコスト表示
 - 使用タイプでグループ化、料金タイプを Savings Plan の対象使用量、償却コスト表示



非ブレンドコストグラフ例

The screenshot shows the AWS Cost Explorer interface with three filter panels on the right:

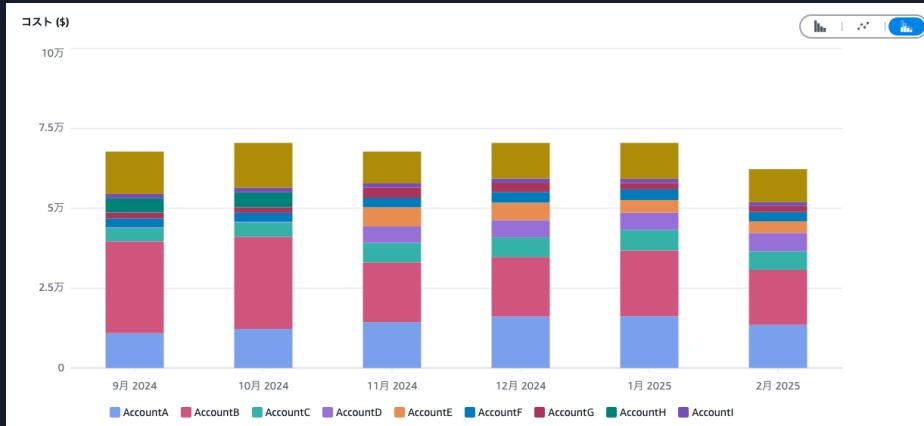
- ▼ グループ化の条件**: ディメンション (クリア)、使用タイプ (選択)
- ▼ 料金タイプ**: 料金タイプを含む (1) (クリア)、Savings Plan の対象使用量 (選択)
- ▼ 詳細オプション**: 次で集計したコスト: 情報、非ブレンドコスト (選択)、償却コスト (選択)

フィルタ例

Cost Explorer アカウントへの適用状況

Cost Explorer でグループ化の条件を連結アカウント、フィルターの料金タイプを Savings Plan の対象使用量とすることで、どのアカウントに Savings Plans が適用されているのかを確認できます。

カバレッジレポートでは、各アカウントのどのサービス・インスタンスファミリーに適用されたか確認できます。



▼ グループ化の条件

ディメンション [クリア](#)
連結アカウント ▾

料金タイプ [クリア](#)
料金タイプを含む (1)
Savings Plan の対象使用量 [X](#)

▼ 詳細オプション

次で集計したコスト: [情報](#)
非ブレンドコスト ▾

フィルタ例

リンクされたアカウント [クリア](#)
連結アカウントを選択してください ▾

Savings Plans のカバレッジの内訳 (12) [情報](#)

テーブル (CSV をダウンロード)

サービス	インスタンスファミリー	リージョン	Savings Plan の対象となる支出	オンデマンド支出	カバレッジ
EC2	c7i	米国西部 (北カリフォルニア)	\$xxxx	\$1,808.86	83%
Lambda	-	アジアパシフィック (東京)	\$xxxx	\$0.00	83%
Fargate	-	アジアパシフィック (東京)	\$xxxx	\$33.28	83%
EC2	c7g	米国西部 (オレゴン)	\$xxxx	\$5,580.59	88%
EC2	r7gd	米国西部 (オレゴン)	\$xxxx	\$581.95	88%
EC2	t3	アジアパシフィック (東京)	\$xxxx	\$235.01	90%
EC2	t2	米国西部 (オレゴン)	\$xxxx	\$25.95	90%
EC2	c6g	米国西部 (オレゴン)	\$xxxx	\$145.36	90%
Lambda	-	米国西部 (オレゴン)	\$xxxx	\$0.00	90%
EC2	c6gd	米国西部 (オレゴン)	\$xxxx	\$164.20	90%
Lambda	-	米国東部 (バージニア北部)	\$xxxx	\$0.00	90%
Fargate	-	米国西部 (オレゴン)	\$xxxx	\$26.66	100%

カバレッジ内訳

(参考) その他フィルタ

- サービスの *Savings Plans for Compute usage*
 - 非ブレンドコスト表示の場合、前払いありと前払いなしの請求書の金額と一致します
 - 償却コスト表示の場合、使用率が100%を切っている際に未使用分（合計コミットメント - 使用済みのコミットメント）が *Savings Plans for Compute usage* として表示されます
- 購入オプション
 - グループ化の条件を購入オプション、使用タイプグループで EC2: Running Hours でフィルタすると EC2 インスタンスの利用時間におけるオンデマンド、Spot、*Savings Plans* の割合を確認できます
 - グループ化の条件を購入オプション、使用タイプで * Fargate * GB-Hours (Hrs)、* Fargate-vCPU * Hours:perCPU (Hrs) (Spot、ARM 含む) でフィルタすると Fargate の利用時間におけるオンデマンド、Spot、*Savings Plans* の割合を確認できます

AWS Cost and Usage Reports での確認方法

Savings Plans の適用状況

- Savings Plans が適用された場合に追加されます
 - linelItem/LinelItemType が 「SavingsPlanCoveredUsage」と 「SavingsPlanNegation」で表示されます
 - 「SavingsPlanCoveredUsage」の linelItem/UnblendedCost ・・・ オンデマンド料金が計上
 - 「SavingsPlanNegation」の linelItem/UnblendedCost ・・・ 同額のマイナスが計上
- Savings Plans の実質的な料金は savingsPlan/SavingsPlanEffectiveCost で確認できます
- オンデマンド料金と比較した費用削減額は
 - (linelItem/LinelItemType が 「SavingsPlanCoveredUsage」の) linelItem/UnblendedCost -
 - (linelItem/LinelItemType が 「SavingsPlanCoveredUsage」の) savingsPlan/SavingsPlanEffectiveCost で確認できます

詳細は、AWS Cost and Usage Reports の Blackbelt をご参照ください。

- <https://youtu.be/YMo4PNDsEvA>

削減額の確認

Savings Plans による削減効果を使用状況レポートおよび Cost Explorer のフィルタで確認することができます。それぞれ次の値が削減額となります。

- 使用状況レポート
 - 正味の合計削減額
- Cost Explorer
 - 前払いなしの場合
 - (非ブレンドコスト) Savings Plan の対象使用量 - (非ブレンドコスト) Savings Plan の定期料金
 - (非ブレンドコスト) Savings Plan の対象使用量 - (償却コスト) Savings Plan の対象使用量
 - 全額前払いの場合
 - (非ブレンドコスト) Savings Plan の対象使用量 - (償却コスト) Savings Plan の対象使用量



使用状況レポート



日付範囲

制限・注意事項

制限・注意事項

コミットメント期間は次のとおり定義されます。うるう年に 1 日ずれる場合があります。

- 1 年: 1 年は 365 日 (31,536,000 秒) として定義されます。
- 3 年: 3 年は 1,095 日 (94,608,000 秒) として定義されます。

- https://docs.aws.amazon.com/ja_jp/savingsplans/latest/userguide/what-is-savings-plans.html

時間あたりのコミットメントは、\$5,000 以下である必要があります。

解除（キャンセル・返却）には、次の制限事項があります。

- 1 時間あたりのコミットメント額が \$100 以下
- 購入から 7 日以内
- 購入した暦月内
- 管理アカウントごとに年間 10 回まで

まとめ

まとめ

Savings Plans は AWS の使用料金を割引する柔軟な料金モデルを提供します。

- 1 年 または 3 年間の時間単位のコミットメントで最大 72% の割引が受けられます
- 長期的かつ定常的なワークフローに向いています
購入前後の検討・モニタリングも重要です。
- 購入計画では、 購入アカウント、 タイプ・オプション、 コミットメント金額を検討します
- 購入後は、 使用率やカバレッジをモニタリングし中長期的な観点でコスト最適化を実践します

參考資料

- Savings Plans ユーザーガイド
 - https://docs.aws.amazon.com/ja_jp/savingsplans/latest/userguide/what-is-savings-plans.html
- AWS Cost Explorer Black Belt
 - 資料
 - https://pages.awscloud.com/rs/112-TZM-766/images/AWS-Black-Belt_2024_AWS-CostExplorer_0630_v1.pdf
 - 動画
 - <https://youtu.be/poZiRvLYkoo>
- AWS Budgets Black Belt
 - 資料
 - https://pages.awscloud.com/rs/112-TZM-766/images/AWS-Black-Belt_2023_AWS-Budgets_1031_v1.pdf
 - 動画
 - https://youtu.be/PV03xqmT4_q
- AWS Cost and Usage Reports
 - 資料
 - https://pages.awscloud.com/rs/112-TZM-766/images/AWS-Black-Belt_2023_AWS-CostAndUsageReports_1031_v1.pdf
 - 動画
 - <https://youtu.be/YMo4PNDsEvA>

AWS Black Belt Online Seminar とは

- ・ 「サービス別」「ソリューション別」「業種別」などのテーマに分け、
アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナーシリーズです
- ・ AWS の技術担当者が、 AWS の各サービスやソリューションについてテーマごとに動画を公開します
- ・ 以下の URL より、過去のセミナー含めた資料などをダウンロードすることができます
 - <https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/>
 - <https://www.youtube.com/playlist?list=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBlqY>

𝕏 ご感想は X (Twitter) へ！ハッシュタグは以下をご利用ください
#awsblackbelt

内容についての注意点

- ・ 本資料では資料作成時点のサービス内容および価格についてご説明しています。AWS のサービスは常にアップデートを続けているため、最新の情報は AWS 公式ウェブサイト (<https://aws.amazon.com/>) にてご確認ください
- ・ 資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます
- ・ 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます
- ・ 技術的な内容に関しましては、有料の [AWS サポート窓口](#)へお問い合わせください
- ・ 料金面でのお問い合わせに関しては、[カスタマーサポート窓口](#)へお問い合わせください (マネジメントコンソールへのログインが必要です)

Thank you!

