

AWS-19

# セキュアでスケーラブルな AWS アカウント統制プラクティス最新動向

中島 智広

セキュリティソリューションアーキテクト  
アマゾン ウェブ サービス ジャパン合同会社



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# 自己紹介

名前：中島 智広（なかしま ともひろ）

職種：セキュリティソリューションアーキテクト

業務：お客様のセキュリティの取り組みを  
AWSの利活用の視点からご支援

- セキュリティアーキテクチャ、運用設計の支援
- コンプライアンスプログラムへの準拠支援  
など



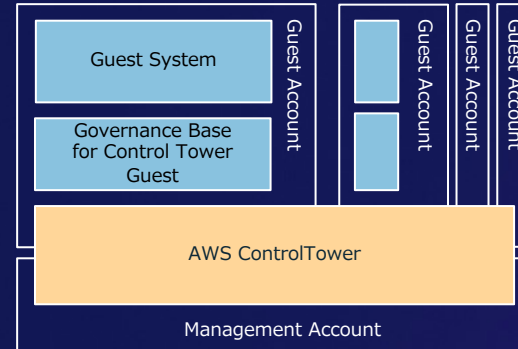
# AWSアカウント統制プラクティス最新動向

AWSアカウント統制を効率化する新しいサービスとソリューション

2021年  
東京リージョンでローンチ



AWS Control Tower



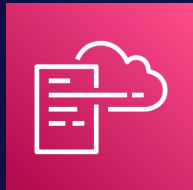
2021年  
GitHub公開

Baseline Environment on AWS (BLEA)

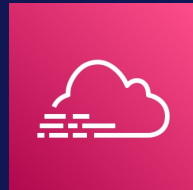
AWSアカウント統制を支える従来からのサービス群



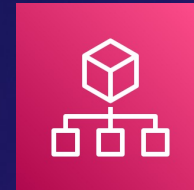
AWS Single  
Sign-On



AWS CloudFormation



AWS CloudTrail



AWS Organizations



AWS Config/  
Config Rules

# 本セッションの前提

## 対象者

- **AWSアカウントの統制、管理、運用に関わるお客様**
- **開発や運用の俊敏性を実現したいお客様**
- **AWSをご利用になる全てのお客様**

## ゴール

AWSアカウント統制の考え方と最新のプラクティスを紹介し、マルチアカウント統制の効率的な始め方、進め方を理解する。

# お伝えすること

なぜ、AWSでは複数のAWSアカウントからなる  
マルチアカウントアーキテクチャをおすすめしているのか？

AWSアカウントの統制にどのように取り組めば良いのか？  
取り組みを効率化するAWS Control Towerの役割や価値

既存のAWSアカウントに統制メカニズムを導入するプラクティス

# Agenda

1. なぜ、AWSアカウントを分割するのか？
2. AWSアカウント統制の考え方
3. 統制のプラクティスとそれを支えるAWSマネージドサービス
4. 既存のAWSアカウントに統制を導入するには
5. まとめ



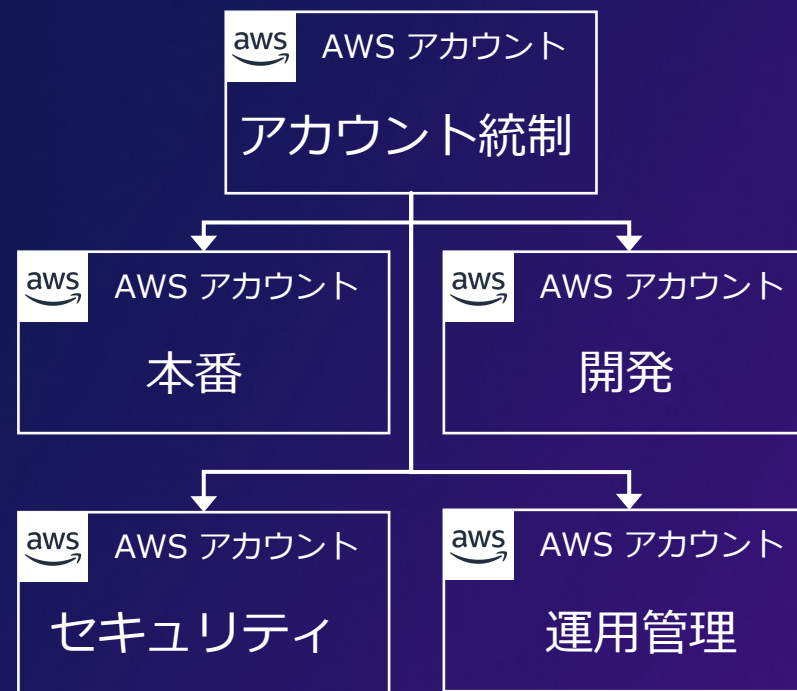
1. なぜ、AWSアカウントを分割するのか？
2. AWSアカウント統制の考え方
3. 統制のプラクティスとそれを支えるAWSマネージドサービス
4. 既存のAWSアカウントに統制を導入するには
5. まとめ

# AWSではマルチアカウントがベストプラクティス

小さな独立した複数のAWSアカウントでシステムを構成する、アーキテクチャ的、組織的アプローチを推奨



シングルアカウントアーキテクチャ



マルチアカウントアーキテクチャ



# マルチアカウントアーキテクチャを採用する主な理由

## 明確な環境分離

AWSアカウントはシンプルで強固な環境分離の単位、明示的に許可を追加しない限り、デフォルトで分離されている

## 複雑性の回避

ひとつひとつのAWSアカウントの構成がシンプルになり、可視性が高まる

## 権限委譲の単位

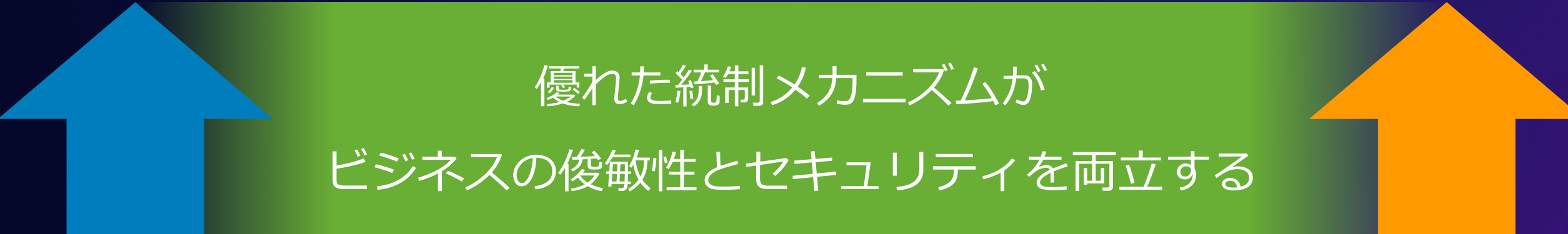
AWSアカウントはリソースのコンテナ、特定のビジネス部門に対し権限を委譲する単位として扱いやすい

## 請求の分離

部門単位やシステムの単位でAWSのコストが明確に分離できる

**これらはすべて運用性の向上に寄与**

# 俊敏性を得るために統制メカニズムを備える



優れた統制メカニズムが  
ビジネスの俊敏性とセキュリティを両立する

- 開発や運用の俊敏性を得るには利用者への権限の委譲（裁量）が必要
- 権限の委譲が許容されるにはリスクがコントロールされた状態が必要

**管理者がリスクを評価しコントロールする仕組み（=統制メカニズム）が解決策**

# 環境分離は統制の基本戦略

たとえば、「本番環境と開発環境の分離」によって得られる整理

## 本番環境

機微情報を保護するため、アクセスできる人を限定し、権限を厳密に管理する  
(権限委譲/裁量を最小限にする)

## 開発環境

機微情報がないことを前提に、開発者に許容できるリスクの範囲でできるだけ高い権限を委譲できる

環境分離が確かで本番環境の機微情報が侵害されないことを前提に得られる便益

環境分離は各種コンプライアンスでも要求される基本の管理策

例：ISO27001:2013 附A.12.1.4/PCI DSS Ver.3.2.1 要件6.4.1/FISC第9版 実76 等

# なぜ、AWSアカウントの分割を推奨するのか？

運用性を向上するアーキテクチャ的、組織的アプローチ

開発や運用の俊敏性を得るための統制メカニズム

1. なぜ、AWSアカウントを分割するのか？
2. AWSアカウント統制の考え方
3. 統制のプラクティスとそれを支えるAWSマネージドサービス
4. 既存のAWSアカウントに統制を導入するには
5. まとめ

# AWSアカウント統制のグランドデザイン

AWSアカウントの構成や統制メカニズムは  
統制にかかる運用の土台となる重要なデザイン



AWSアカウント構成からスタートする





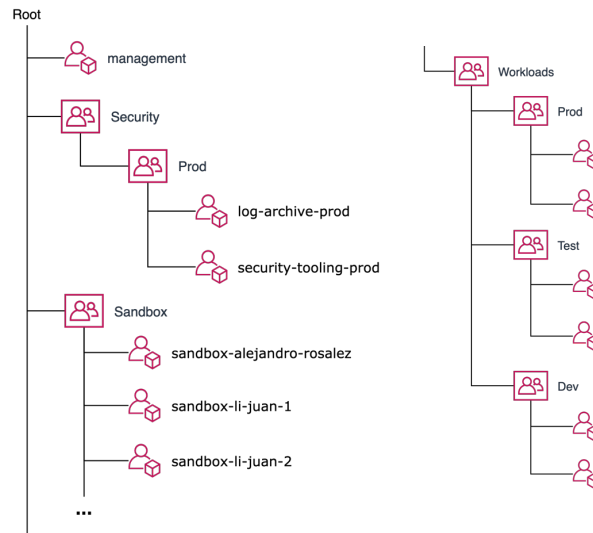
# AWSアカウント構成のリファレンス

お客様の利用規模に応じたデザインパターンと考え方を提供

## Basic organization

[https://docs.aws.amazon.com/ja\\_jp/whitepapers/latest/organizing-your-aws-environment/basic-organization.html](https://docs.aws.amazon.com/ja_jp/whitepapers/latest/organizing-your-aws-environment/basic-organization.html)

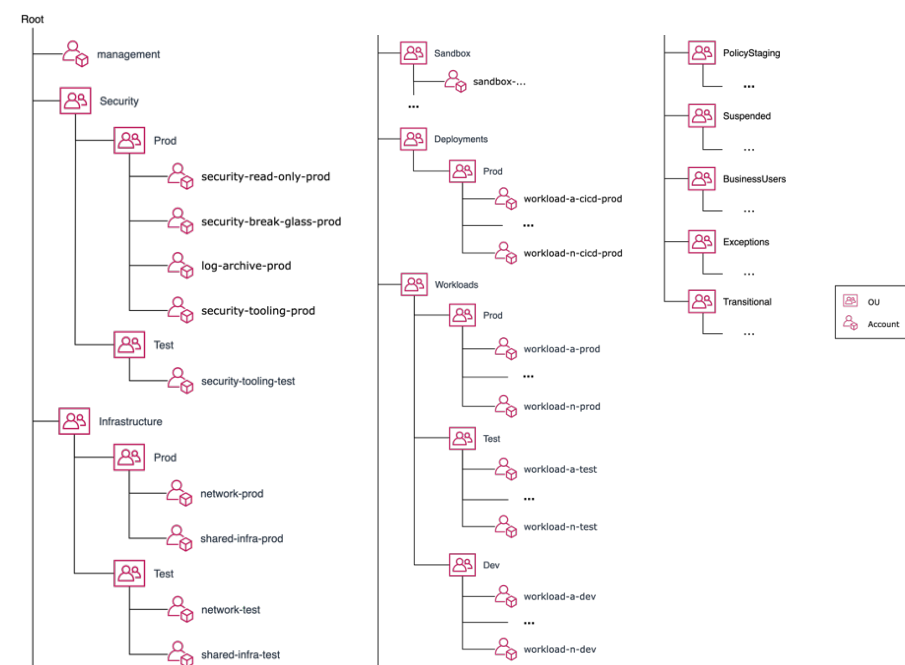
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



## Advanced Organization

[https://docs.aws.amazon.com/ja\\_jp/whitepapers/latest/organizing-your-aws-environment/basic-organization.html](https://docs.aws.amazon.com/ja_jp/whitepapers/latest/organizing-your-aws-environment/basic-organization.html)

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



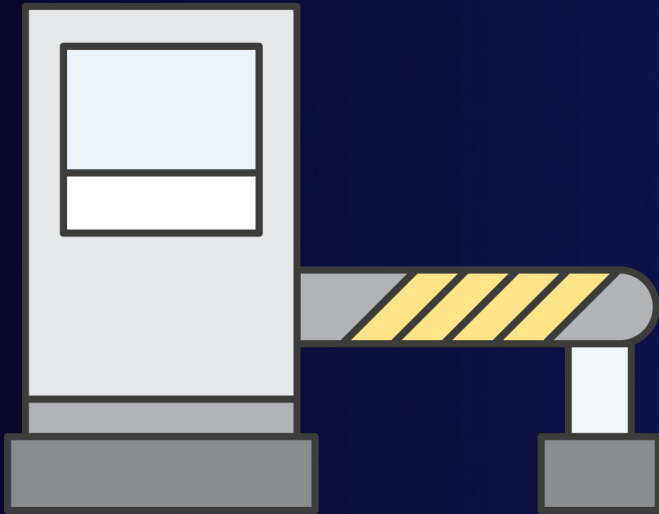
## Organizing Your AWS Environment Using Multiple Accounts

[https://docs.aws.amazon.com/ja\\_jp/whitepapers/latest/organizing-your-aws-environment/organizing-your-aws-environment.html](https://docs.aws.amazon.com/ja_jp/whitepapers/latest/organizing-your-aws-environment/organizing-your-aws-environment.html)

# 統制メカニズムの方向性

組織に必要なのはイノベーションを阻害しない統制メカニズム

ゲートキーパー



V.S.

ガードレール

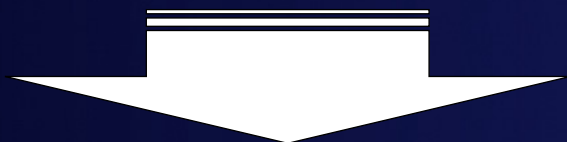


利用を事前承認制にすると管理業務がボトルネックになりイノベーションが阻害される

できるだけ自由に使いわせる一方で利用者を守るためガードレールを整備する

# 再構築より再利用

セキュリティ & ガバナンスはリファレンス  
が明確な領域、ベースラインとなる基本的  
な統制はワークロード毎に相反しない



ベースラインはすでにあるものを使い  
迅速に展開し、固有の統制のみを  
ビルディングブロックすると効率的



# AWS Control Towerからスタートが第一選択肢



AWS Control Tower

AWSの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、統制を利かせたアカウント統制環境（Landing Zone）を構成するサービス



ログ取得の強制とアーカイブ集約



アイデンティティ & アクセス管理



セキュリティモニタリングの集約



リスクあるアクションを  
予防/発見するガードレール



管理のためのダッシュボード

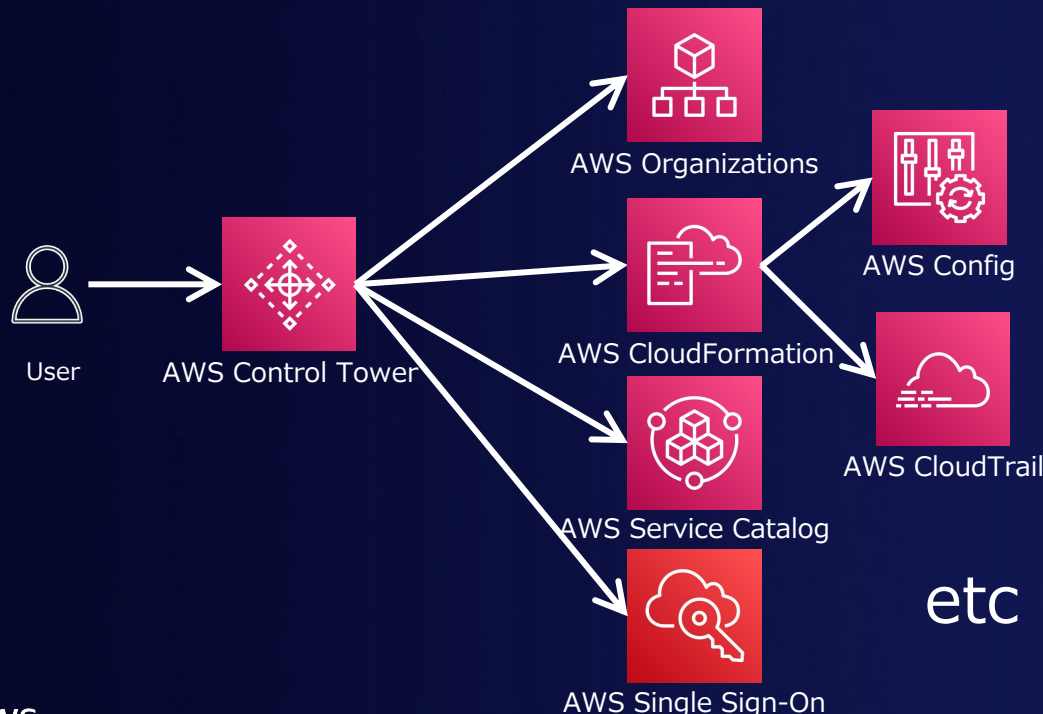


新規作成AWSアカウントに対する  
ベースライン統制の展開



# AWS Control TowerはAWSアカウント統制の模範

- AWS Control Towerを通じてAWSアカウント統制の理解が深まる
- 同じアプローチでお客様は独自の統制メカニズムを展開、拡張できる



AWSが考えるベストプラクティス実装



再利用可能なエッセンスの集合体

# 再販されたAWSアカウントにもAWS Control Tower

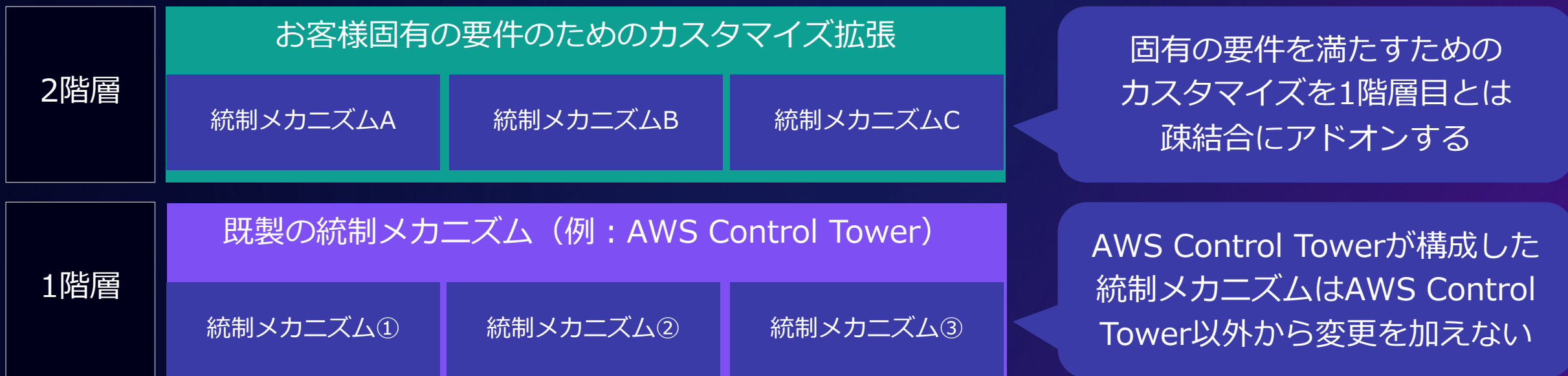
- ソリューションプロバイダーから再販、提供されるAWSアカウントにおいてもAWS Control Towerの利用は可能
- 東京リージョンでのローンチ（2021年4月）を機に、複数の国内ソリューションプロバイダーが、再販、提供するAWSアカウントにおけるAWS Control Towerの利用をサポート
- 利用可否や条件、利用可能時期はソリューションプロバイダーによって異なる

お取引のある事業者やAWSにご相談ください



# 統制を効率よくカスタマイズし保守するには

ベースライン（1階層目）は既製の統制メカニズムをそのまま利用し、カスタマイズ拡張（2階層目）を疎結合に構成することで、各々の機能追加やバージョンアップにシームレスに追従できる

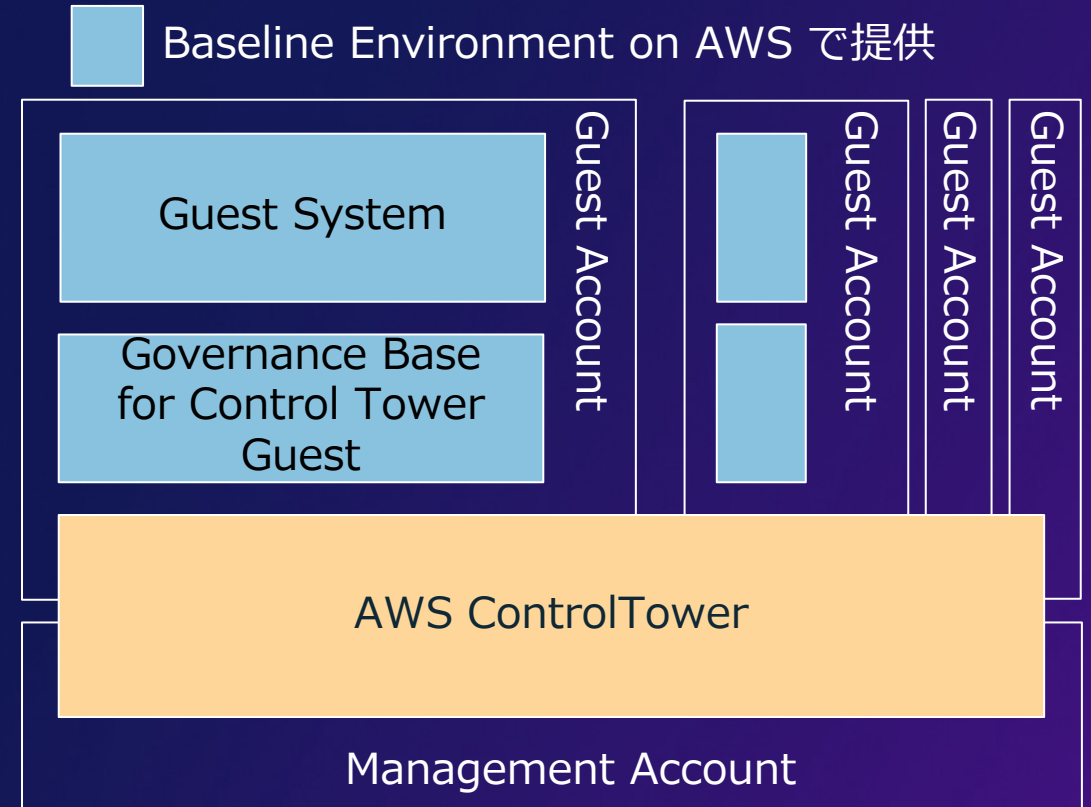


# カスタマイズ拡張もテンプレート化して再利用

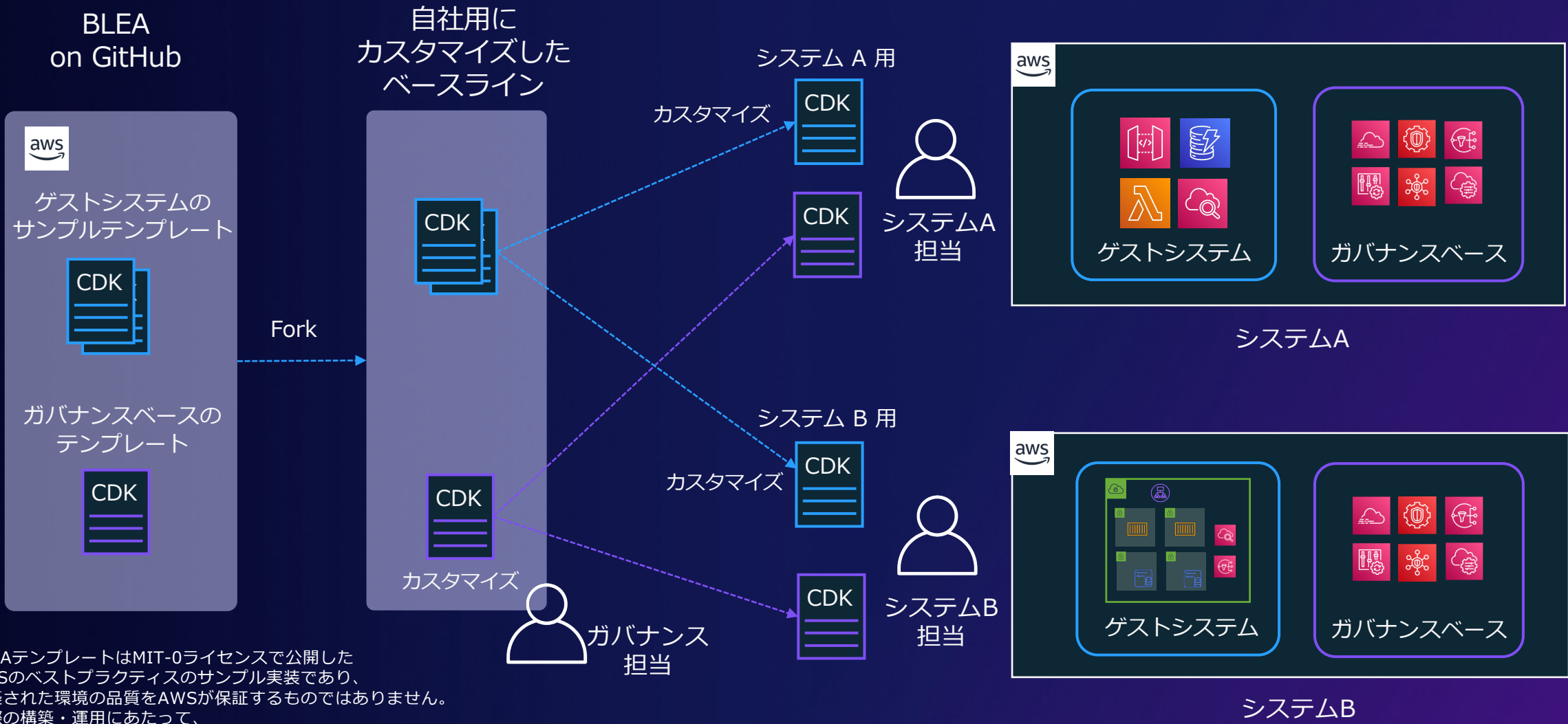
たとえば、

## Baseline Environment on AWS (BLEA)

- AWS Control Tower 環境へ展開可能な統制のサンプル実装
- メンテナンスしやすい Cloud Development Kit (CDK) コード
- AWS Japan の SA が開発・メンテナンス



# テンプレートの活用イメージ（BLEAを題材に）



※BLEAテンプレートはMIT-0ライセンスで公開したAWSのベストプラクティスのサンプル実装であり、構築された環境の品質をAWSが保証するものではありません。実際の構築・運用にあたって、お客様でテンプレートのカスタマイズやテストの実装が必要です。

# テンプレートを用いた統制の展開を詳しく学ぶには

## AWS-22

### テンプレートを使ったAWS環境のガバナンス管理 - Baseline Environment on AWS (BLEA) 徹底解説 -

AWS上に多様なシステムを構築するにあたり、全社共通で実施すべきセキュリティなど基本設定を、どうやって展開およびチェックするのか？

その一つの方法として、カスタマイズ性の高いベースライン（基本的な設定）、アプリケーションサンプルテンプレート、そしてガードレールを使い、ガバナンスを実現する方法を紹介します。

実装例として、AWS Samplesで公開している CDK テンプレート "Baseline Environment on AWS (BLEA)" を紹介します。その設計思想やマルチアカウント環境での利用方法も解説します。



大村 幸敬  
部長/シニアソリューションアーキテクト

# AWSアカウント統制の考え方

再構築より再利用、ベースラインはすでにあるものを使い迅速に展開

AWS Control TowerをAWSアカウント統制の模範として活用

カスタマイズ拡張は疎結合に構成、再利用性と保守性を高める

1. なぜ、AWSアカウントを分割するのか？
2. AWSアカウント統制の考え方
3. 統制のプラクティスとそれを支えるAWSマネージドサービス
4. 既存のAWSアカウントに統制を導入するには
5. まとめ



# セキュリティ管理者が求める統制プラクティス

## 一元管理

システム全体の可視性を高め、セキュリティ管理業務の負荷を低減すると共に、全てのAWSアカウントに統制を徹底

## 証跡の保全

トラブルシューティングやインシデントの全容解明、ステークホルダーへの説明責任を果たすために不可欠

## ガードレール

利用者を守るためのメカニズム、やってはいけない操作を未然に防ぐ（予防的統制）や逸脱を検知する（発見的統制）から構成

# ガードレール設計のポイント

- 複数のアプローチを組み合わせやすい統制をデザインする
- 予防的統制に偏って設計しないことがポイント

## 予防的統制

対象の操作をあらかじめ実施できないように制限する

管理者が利用者の要件を把握し、依存関係を考慮する必要があるため、要件の整理と実装、保守が煩雑

## 発見的統制

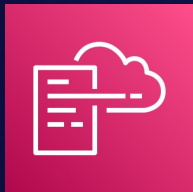
望ましい状態から逸脱した場合、それを発見する

利用者やワークロードに影響がないため、管理者は一般的な観点に基づいて実装すればよい、このため予防的統制に比べて実装、保守が容易

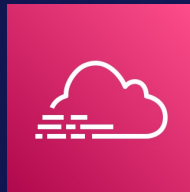
# AWSアカウント統制を支えるAWSマネージドサービス



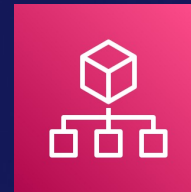
AWS Single  
Sign-On



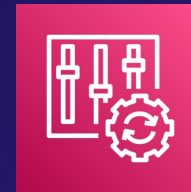
AWS CloudFormation



AWS CloudTrail



AWS Organizations



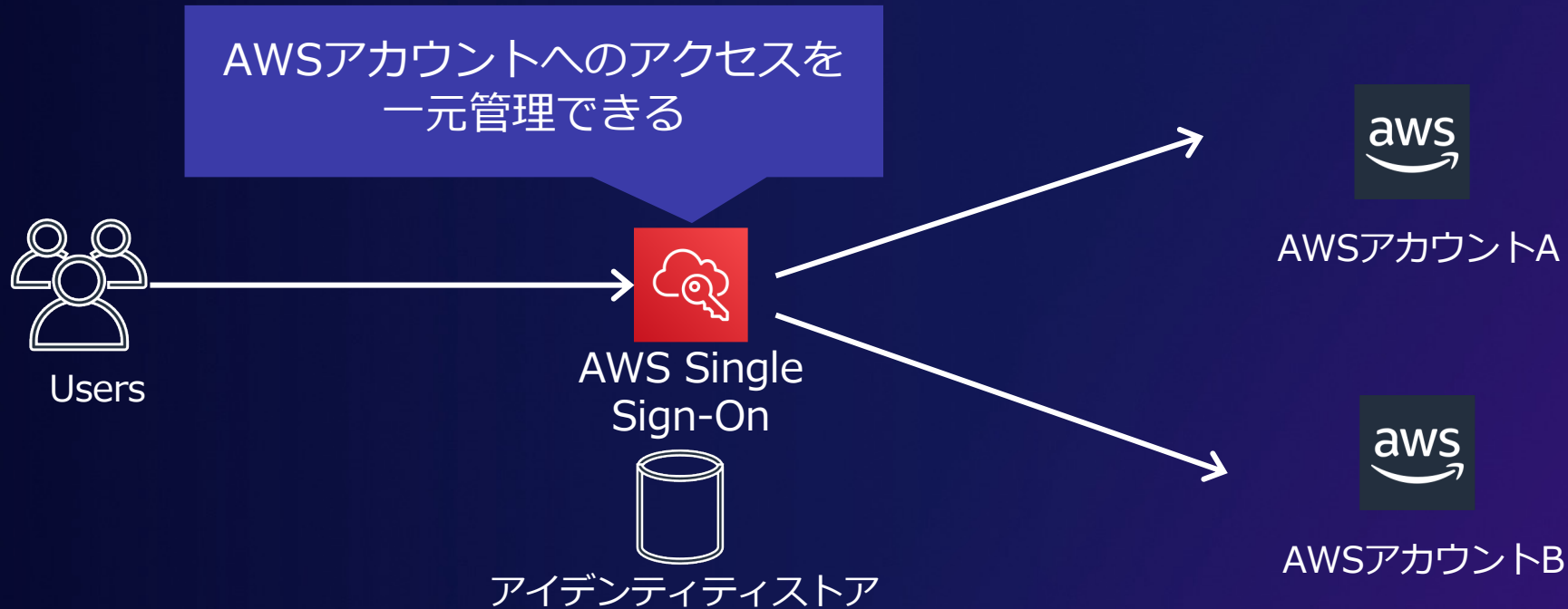
AWS Config/  
Config Rules

# AWSアカウントアクセスの一元管理



AWS Single  
Sign-On

単一のIDを用いた複数のAWSアカウントに対するシングルサインオンを実現する仕組み、複数のAWSアカウントやアプリケーションへのアクセスの一元管理を実現

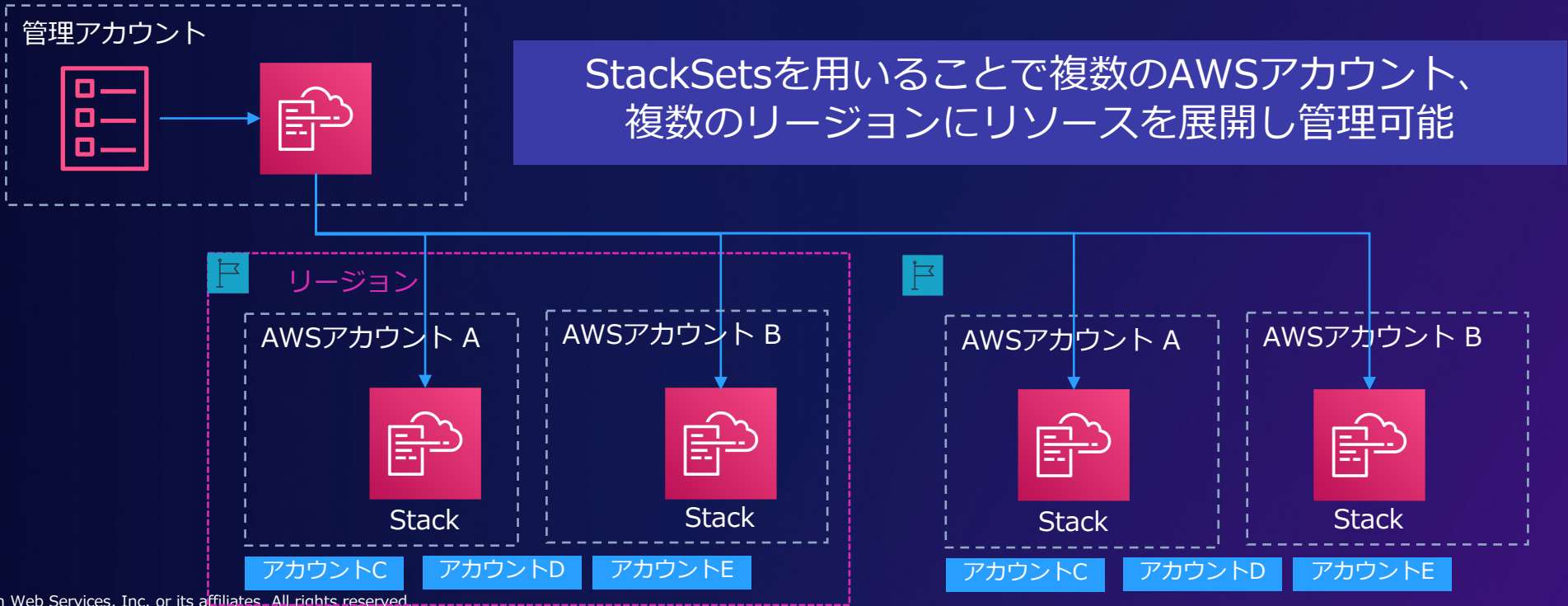


# 統制の展開や保守を一元管理



AWS CloudFormation

インフラストラクチャをコードとして扱うことで、AWS  
およびサードパーティーのリソースをモデル化、プロビ  
ジョニング、管理を実現

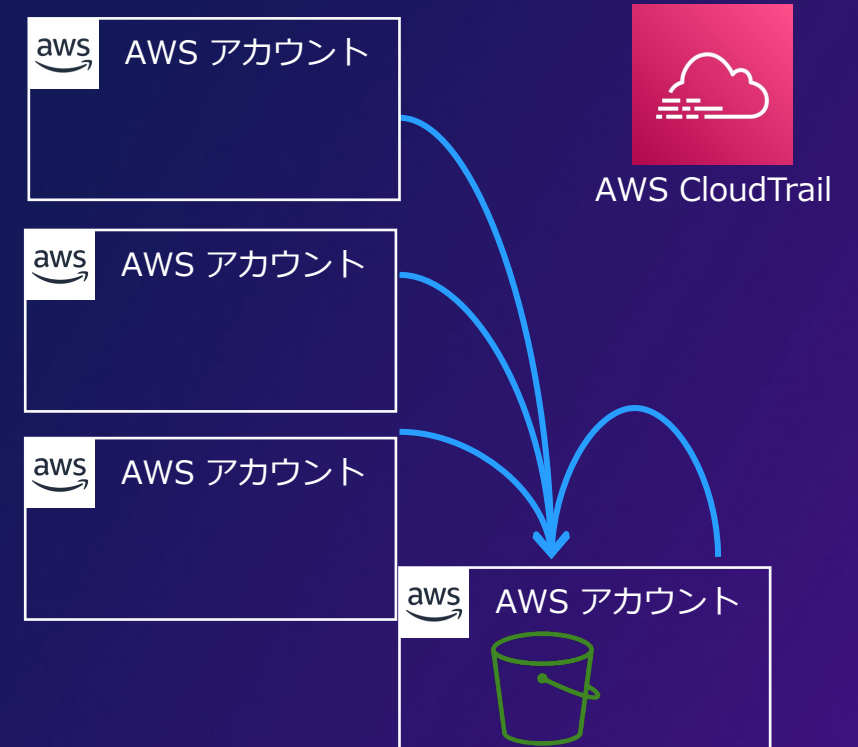


# 証跡の保全と一元管理

専用のAWSアカウントに集約することで

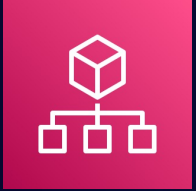
すべてのアカウントのログを  
1つのアカウントへ

- AWSアカウントの侵害や内部不正、  
オペレーションミスへの耐性を獲得する
- 調査や分析をしやすくする





# AWSアカウント単位での強力な予防的統制

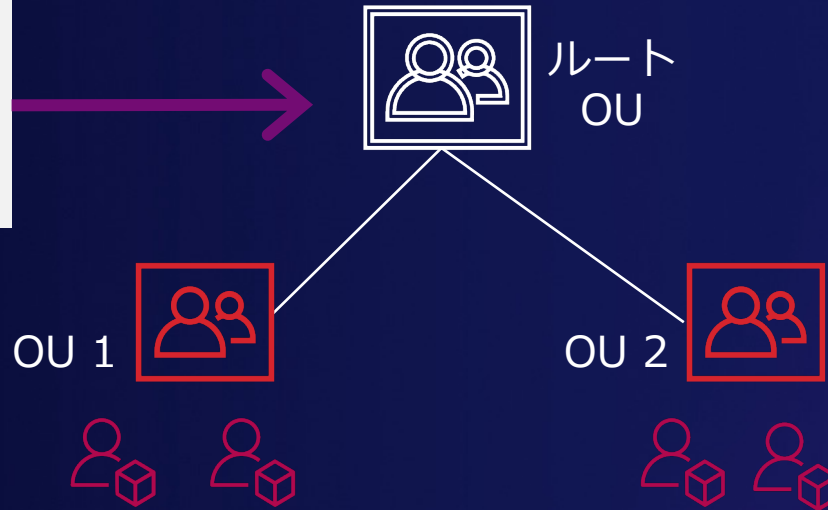


AWS Organizations

AWSアカウントのrootユーザーの権限も制限できる  
Service Control Policyを提供、AWSアカウントをまとめ  
てグループ化する組織単位（OU）に対して適用する

アタッチ済み: FullAWSAccess

```
{
  "Effect": "Allow",
  "Action": "*",
  "Resource": "*"
}
```



継承: FullAWSAccess  
アタッチ済み: Deny\_DeleteLogs

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:DeleteFlowLogs",
    "logs:DeleteLogGroup",
    "logs:DeleteLogStream",
  ],
  "Resource": "*"
}
```

# 構成変更に対する発見的統制



AWS Config/  
Config Rules

AWSインフラストラクチャの変更管理を担うサービス、自動で変更を保存、さらに変更内容をルールに則って評価、必要な場合は修復アクション（Remediation）まで行う

## AWS Managed Rules

AWSにより定義・提供される  
ベーシック・ルール

## Customer Managed Rules

自分でAWS Lambdaをベースにルールを作成可能  
管理自体は作成者（自分）で実施

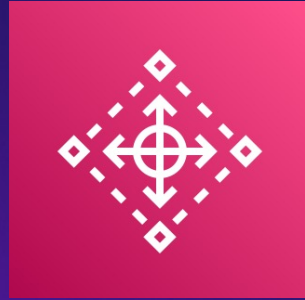


## 修復アクション

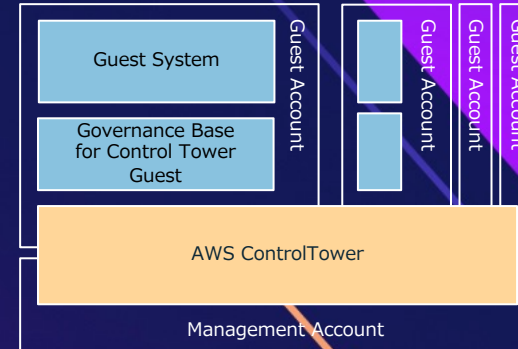
AWSにより定義・提供される  
AWS Systems Manager Automationのほか  
Lambdaをベースに独自の修復アクションも可能

# 統制のプラクティスを支えるAWSマネージドサービス

AWSアカウント統制を効率化する新しいサービスとソリューション



AWS Control Tower

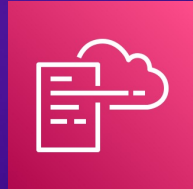


Baseline Environment on AWS (BLEA)

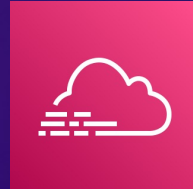
AWSアカウント統制を支える従来からのサービス群



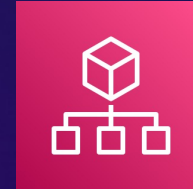
AWS Single  
Sign-On



AWS CloudFormation



AWS CloudTrail



AWS Organizations



AWS Config/  
Config Rules

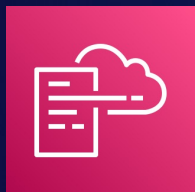
1. なぜ、AWSアカウントを分割するのか？
2. AWSアカウント統制の考え方
3. 統制のプラクティスとそれを支えるAWSマネージドサービス
4. 既存のAWSアカウントに統制を導入するには
5. まとめ

# 既存ワークロードへの影響を考える

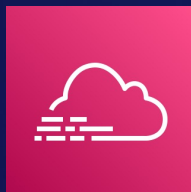
- 以下のAWSマネージドサービスの中で既存ワークロードの動作を制限する機能はAWS OrganizationsのService Control Policyのみ
- 「メカニズムの理解」が導入の懸念を払拭する



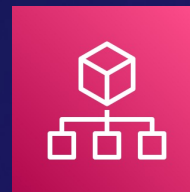
AWS Single  
Sign-On



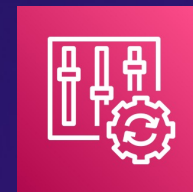
AWS CloudFormation



AWS CloudTrail



AWS Organizations



AWS Config/  
Config Rules



# AWS Control Tower導入のポイント

## 「メカニズムの理解」が導入の懸念を払拭する

- 指定した組織単位（OU）に属するAWSアカウントのみが統制対象、恒久的に一部の組織単位（OU）を統制対象外とすることもできる
- 必須のガードレール以外は選択式、利用者自身が有効化する
- 必須の予防的ガードレールはLanding Zoneの破壊を防ぐためのもの、利用者の作成したリソースを対象としていない
- 適用されるService Control Policyは公式ドキュメントから確認可能



# 予防的ガードレールからスタートしない

- 優れた統制メカニズムの実現は旅路、導入しやすいものから小さな成功体験を積み重ねる
- 利用者の声に基づくフィードバックループを速く回すことで、よりよい統制に早く近づく



# 既存のAWSアカウントに統制を導入するには

「メカニズムの理解」が導入の懸念を払拭する

導入しやすいものから小さな成功体験を積み重ねる

1. なぜ、AWSアカウントを分割するのか？
2. AWSアカウント統制の考え方
3. 統制のプラクティスとそれを支えるAWSマネージドサービス
4. 既存のAWSアカウントに統制を導入するには
5. まとめ

# お伝えしたこと

なぜ、AWSでは複数のAWSアカウントからなる  
マルチアカウントアーキテクチャをおすすめしているのか？

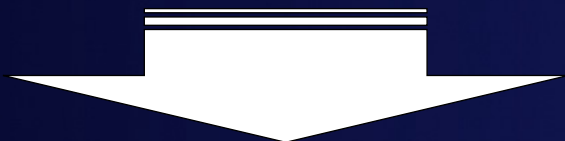
AWSアカウントの統制にどのように取り組めば良いのか？  
取り組みを効率化するAWS Control Towerの役割や価値

既存のAWSアカウントに統制メカニズムを導入するプラクティス



# 再構築より再利用

セキュリティ & ガバナンスはリファレンス  
が明確な領域、ベースラインとなる基本的  
な統制はワークロード毎に相反しない



ベースラインはすでにあるものを使い  
迅速に展開し、固有の統制のみを  
ビルディングブロックすると効率的



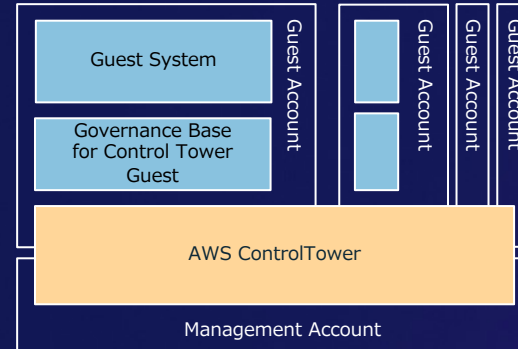
# AWSアカウント統制プラクティス最新動向

AWSアカウント統制を効率化する新しいサービスとソリューション

2021年  
東京リージョンでローンチ



AWS Control Tower



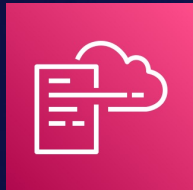
2021年  
GitHub公開

Baseline Environment on AWS (BLEA)

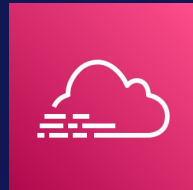
AWSアカウント統制を支える従来からのサービス群



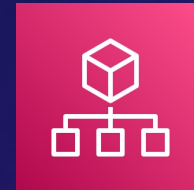
AWS Single  
Sign-On



AWS CloudFormation



AWS CloudTrail



AWS Organizations



AWS Config/  
Config Rules



# Thank you!