

AWS-15

# 金融機関に求められる クラウドセキュリティの AWS 環境での実装

能仁 信亮

技術統括本部 金融ソリューション本部 シニア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



# 自己紹介

能仁 信亮 (のうにん しんりょう)



日々の活動:

金融機関のお客様へクラウド活用の技術的なご支援をさせていただいております

好きなAWSサービス

Amazon S3, AWS Lake Formation, AWS KMS

# 本セッションの目的

目的:

金融機関で求められるセキュリティレベルを自動化などのメカニズムにより実現する方法の勘所を理解いただく

前提:

具体的な実装方法などは、本セッション内でとりあげる関連セッション、参考資料などを参照ください

# 金融機関のクラウド活用における典型的な状況

## セキュリティ

社会インフラを担う金融機関として、高いセキュリティ水準が求められている

## アジリティ

ビジネス環境が急激に変化するなか、アジリティをもって新たなビジネスの起ち上げや変革が必要

チャレンジ: クラウド活用において、セキュリティとアジリティの2つの側面をどのように両立していけばよいのか

# AWS利用の拡大と新たな課題

- AWS活用が進んでいく中で、クラウドを利用するプロジェクトやシステムの数が急激に増えていく
- 多数のAWS環境をアジリティを確保しながら統制をとっていく メカニズム (仕組み) が求められている

# AWS Well-Architected Framework

## セキュリティの柱における設計原則

強力なアイデンティティ基盤の実装

トレーサビリティの実現

全レイヤーでセキュリティを適用する

セキュリティのベストプラクティスを自動化する

伝送中および保管中のデータの保護

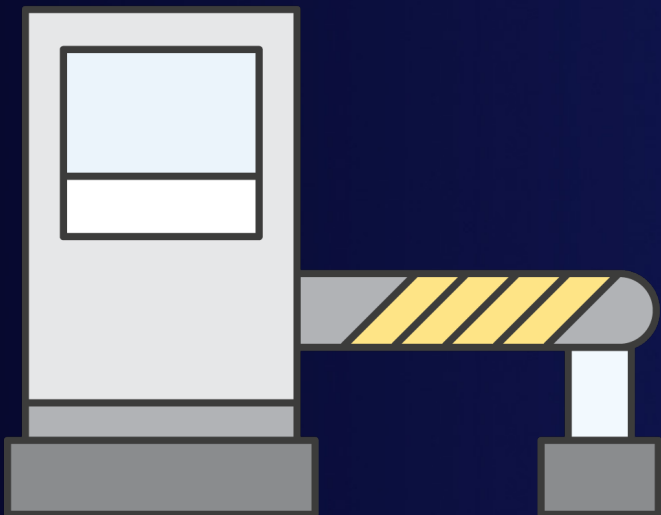
データに人の手を入れない

セキュリティイベントに備える



# 統制メカニズムの方向性

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



# アジェンダ

このセッションでは、セキュリティとアジリティを両立するために特に重要な以下の3つのポイントを取り上げる

- AWSアカウントの構成・統制のためのメカニズム
- AWS環境に発見的統制を実装するためのメカニズム
- 安全に権限を委譲するためのメカニズム



- AWSアカウントの構成・統制のためのメカニズム
- AWS環境に発見的統制を実装するためのメカニズム
- 安全に権限を委譲するためのメカニズム

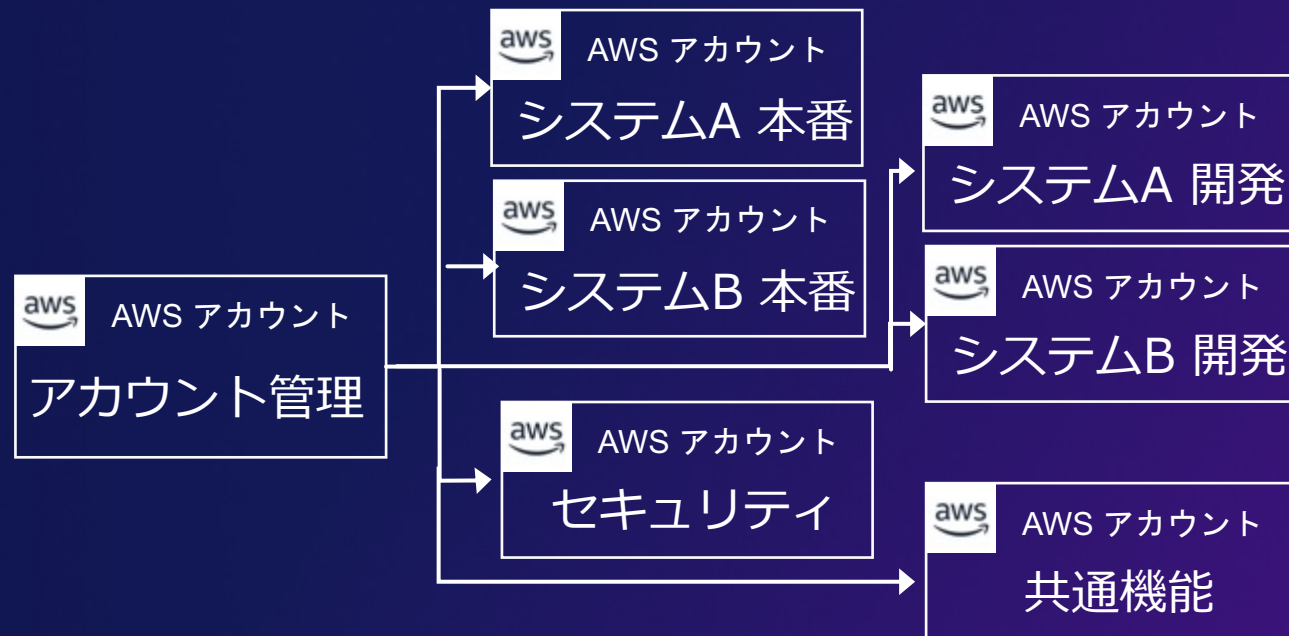
# AWSアカウント利用のパターン

## シングルアカウントアーキテクチャ



- 1つのアカウントの中で、複数のシステムや環境を構成する
- VPCやIAMによって、システムや環境の分離を行う

## マルチアカウントアーキテクチャ



- 独立した小さなAWSアカウントを利用したアーキテクチャ
- AWSアカウントによってリソースや権限を明確に分離できる

# マルチアカウントアーキテクチャを採用する理由

AWSを活用する際は、以下のような理由から、マルチアカウントアーキテクチャが選択されることが多く、ベストプラクティスとなっている

## 権限委譲が容易

システムや部門ごとにアカウントを分離することで、アカウント単位で権限を委譲しやすくなる

## ワークロードの明確な分離

システムの重要度やコンプライアンス要件などによって、必要な対応が異なる。ワークロードごとにAWSアカウントを分離することで、求められる要件に応じた対応を実施しやすい


## コストの明確化

システムや組織ごとにAWSのコストの把握が容易になる

# どのように多数のAWSアカウントを統制するか

- 典型的には、各プロジェクトに開発環境などを含めて複数のAWSアカウントを払い出すことになる
- 一例として以下のような課題に対応する必要がある
  - 多数のAWSアカウントに対して、一定のセキュリティ水準をどのように保つか
  - ログなどの必要な情報をどのように一元管理するか
  - アカウント払い出しに時間がかかる
- セキュアで事前設定済みのAWSアカウントを払い出す仕組みが必要となる

# 「Landing Zone」の実装

- Landing Zoneとは
  - セキュアで事前設定済みのAWSアカウントを提供する仕組みの総称
  - ツールを活用してスケーラブルかつ 高い柔軟性を提供
  - ビジネスのアジリティとイノベーションを実現
- 実装1: AWS Control Tower 
  - AWSサービスとして提供される Landing Zone
  - 最小限のマルチアカウント管理を迅速に開始できる
  - 特に新規にAWSを使い始める場合に有効
- 実装2: 独自実装の Landing Zone
  - マルチアカウント戦略に基づき独自に実装する Landing Zone
  - 自社の方針にしたがって自由にカスタマイズ可能
  - すでに管理の仕組みがあってControlTowerの適合が難しい場合に有効

# AWS Control Tower



AWS Control  
Tower

マルチアカウントAWS環境をセットアップおよび管理するためのサービス



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



# S O M P Oホールディングス株式会社様

## 課題

グループ内でクラウド活用が進むなか、セキュリティ対応が各社の現場任せで、グループ全体として組織的に取り組めていなかった

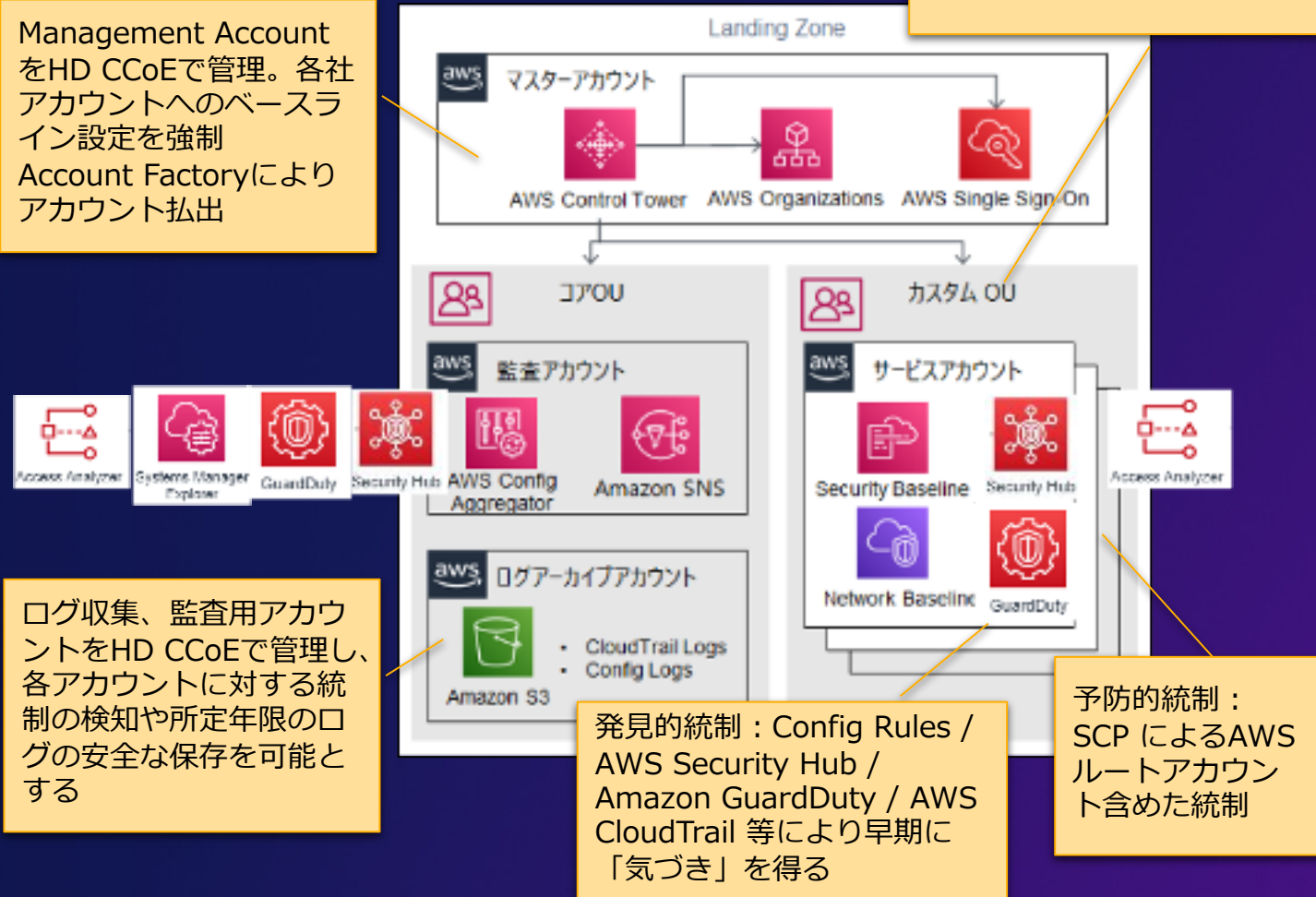
## 解決策

AWS Control Towerを活用して、各アカウントのセキュリティ水準を一定レベル以上に集中管理し、より安全に使えるようにする  
統制（予防的／発見的）により、セキュリティインシデントの発生リスク低減と発生時の早期発見・回復を図る

Management Account  
をHD CCoEで管理。各社  
アカウントへのベースラ  
イン設定を強制  
Account Factoryにより  
アカウント払出

ログ収集、監査用アカ  
ウントをHD CCoEで管理し、  
各アカウントに対する統  
制の検知や所定年限のロ  
グの安全な保存を可能と  
する

各社別にカスタムOUを設置  
OUには各々 Prod / Dev  
のOUを設け、AWSアカ  
ウントを収容



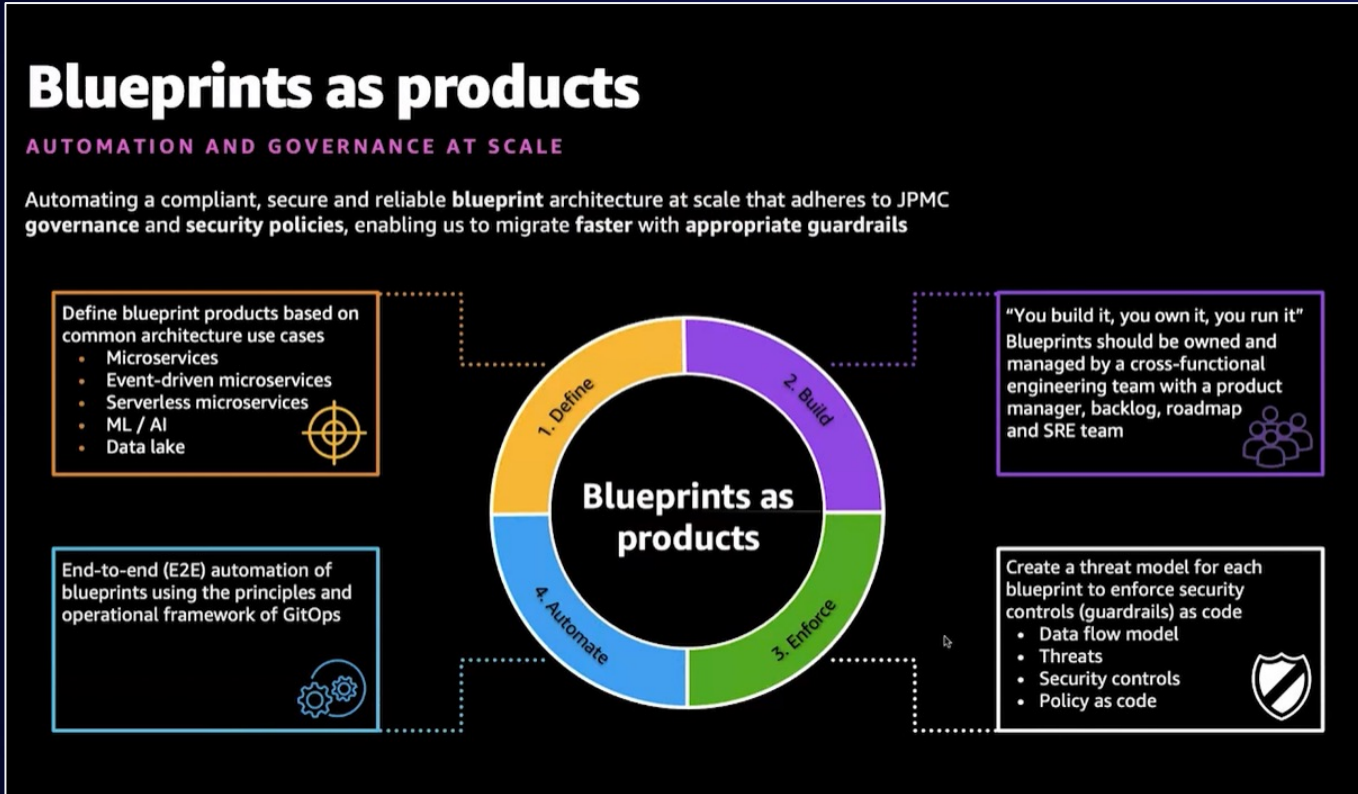


# 独自の統制を追加する

- AWS Control Tower での標準的な統制に加えて、アカウント払い出しの際に、独自の統制を追加するにはどうすればよいか
- (例) アカウントを払い出す際に組織として標準的な構成を事前設定して払い出しを行いたい

# JPMorgan Chase & Co.

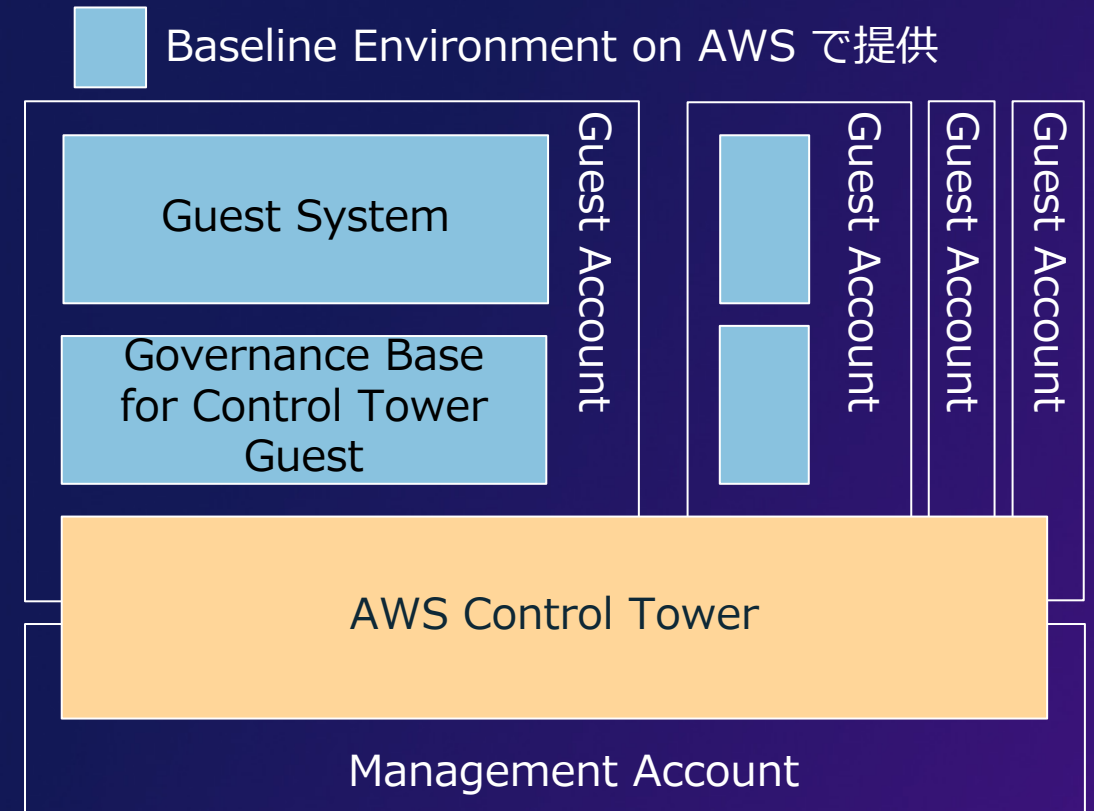
## “Migrations at scale through cloud blueprints and automation”



- 全てのビジネスラインに渡ってクラウド移行を加速するための戦略的取組み
- 再利用可能なクラウド・ブループリントを提供
  - ユースケースごとにブループリントを開発（ウェブアプリ、データレイク等）
  - セキュリティ、コンプライアンス、レジリエンスを事前に定義
  - CCoEが開発者に向けて提供するプロダクトとして位置付け
- 開発者はセルフサービスで開発に取り組むことが可能となり、クラウド移行が加速

# 利用可能なサンプルテンプレート

- AWSのセキュリティベストプラクティスを実装したサンプルテンプレートであるBaseline Environment on AWS (BLEA)
- AWSセキュリティサービスを活用したアカウント保護と記録
- 拡張の起点となる解説コメント付きのCloud Development Kit (CDK) コード



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

# ここまでのまとめ

- マルチアカウントアーキテクチャはベストプラクティス
- AWS Control Towerの活用
- 独自の統制の追加 (Baseline Environment on AWSの活用など)

# 関連情報

- AWS Summit Japan での関連セッション
  - 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
  - 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 -
- 過去のセッション
  - AWS re:Invent 2020: JPMC: Migrations at scale through cloud blueprints and automation [動画](#) | [資料](#)
- その他のリソース
  - Baseline Environment on AWS [Blog](#) | [GitHub](#)
  - ホワイトペーパー: Organizing Your AWS Environment Using Multiple Accounts [資料](#)

- AWSアカウントの構成・統制のためのメカニズム
- AWS環境に発見的統制を実装するためのメカニズム
- 安全に権限を委譲するためのメカニズム

# 発見的統制に関する典型的な状況と課題

- 金融機関では、セキュリティオペレーションセンター(SOC)を含めて、発見的統制を行う組織や仕組みを保持している
- 他業界と比較して古くから取り組みをされており、オンプレミス環境での統制がベースとなっている場合が多い
- これまでの知見や仕組みを活かしながら、クラウドの特性を活かした発見的統制のメカニズムを考えていく必要がある



# インテリジェントな脅威検出 Amazon GuardDuty



Amazon GuardDuty

- **脅威検出**
  - セキュリティリスクを可視化・検知するAWS マネージド・サービス
- **人的コストを削減**
  - AWS各種ログの連続ストリームを自動的に分析
- **既知と未知の振る舞い検知**
  - 悪意のある IP アドレス、異常検出、機械学習などの統合脅威インテリジェンスを使用して脅威を認識

# 検知の例: 不正なIAMクレデンシャル利用の検知

EC2インスタンス専用に作成された一時クレデンシャルが、AWSの外部や、別のAWSアカウントで利用された際には、Amazon GuardDutyが検知

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS

インスタンス作成ロールで EC2 インスタンス専用に作成された認証情報が外部 IP アドレスから使用されています。

デフォルトの重要度: 高

- データソース: CloudTrail 管理イベントまたは S3 データイベント

この発見は、外部のホストであることを知らせますAWSを実行しようとしたAWS一時的なAPI 操作AWSの EC2 インスタンスに作成された認証情報をAWS環境。リスト内の EC2 インスタンスが侵害されていて、このインスタンスの一時的な認証情報が密かにAWS。AWSは、一時的な認証情報を作成したエンティティ外にその認証情報を再配布することはお勧めしません(AWSアプリケーション、EC2、または Lambda)。ただし、承認されたユーザーは EC2 インスタンスから認証情報をエクスポートして正当な API コールを行うことができます。攻撃の可能性を排除してアクティビティが正当であることを確認するには、結果にリモート IP からのインスタンス認証情報の使用が予期されているかどうかを検証します。

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS

インスタンス起動ロールを通じて EC2 インスタンス専用に作成された認証情報が内の別のアカウントから使用されています

デフォルトの重要度: ハイ\*

## ④ 注記

この結果のデフォルトの重要度は「高」です。ただし、API がお客様と提携しているアカウントによって呼び出された場合AWS環境、重要度は「中」です。

- データソース: CloudTrail 管理イベントまたは S3 データイベント

この結果により、EC2 インスタンスの認証情報が、別のインスタンスによって所有されている IP アドレスから API を呼び出すときに通知されます。AWS関連付けられた EC2 インスタンスが実行されているアカウント以外のアカウント。

[https://docs.aws.amazon.com/guardduty/latest/ug/guardduty\\_finding-types-iam.html](https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_finding-types-iam.html)

# AWS Security Hub

組織内の様々なセキュリティデータを集約して、一元的に可視化



# AWS Security Hub セキュリティ基準

業界標準やベストプラクティスに基づいた自動セキュリティチェック

これまでのセキュリティチェック  
年次などのタイミングでチェックリスト  
をもとに手動でコンプライアンスやセ  
キュリティベストプラクティスへの準拠  
状況を確認



AWS Security Hub セキュリティ基準  
最新の環境の情報をもとに自動でコンプ  
ライアンスやセキュリティベストプラク  
ティスへの準拠状況を随時確認

- AWS Foundational Security Best Practices v1.0.0
  - AWSセキュリティ専門家により定義された統制項目。セキュリティベストプラクティスに沿わないAWSアカウントやリソースを検知する
- CIS AWS Foundations Benchmark v1.2.0
  - Center for Internet Security が定義した要件の一部に対してチェックをする
- PCI DSS v3.2.1
  - クレジットカード情報を保存・処理・転送する組織が従うセキュリティ標準であるPCI DSS要件の一部に対してチェックする

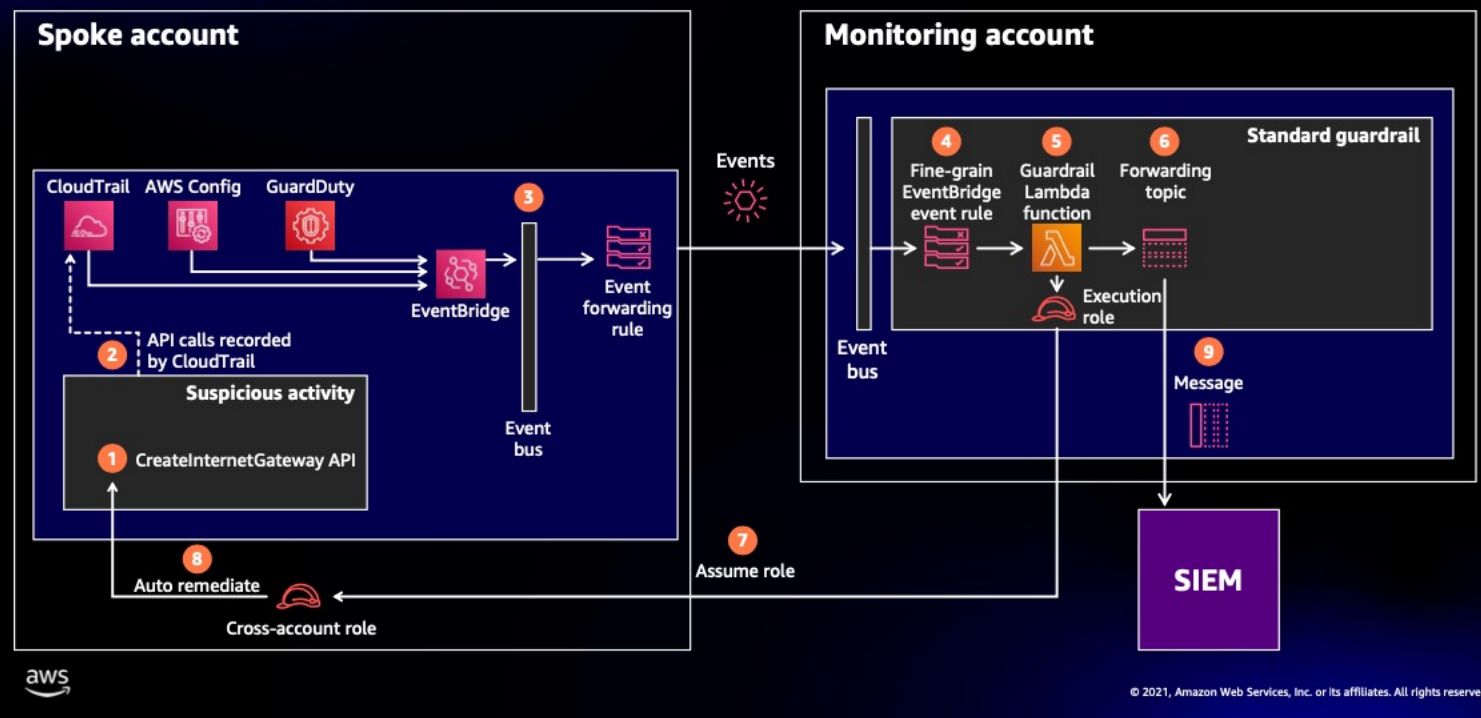


# 自動修復

- リスクが相対的に高いセキュリティイベントに対しては、対応の自動化を行うことも考えられる
- 例) クレデンシャルの漏洩の可能性が高いセキュリティイベントが検知された場合に、クレデンシャルを無効化する

# Citi : AWS CDK によるSecurity Guardrail開発のスケーリング

## Guardrail system-level design



- Citiが当初CloudFormationで発見的統制およびイベント駆動型自動修復用ガードレールの開発・実装していたが、スケールするにはより多くのファイルが必要になり仕組みが複雑化
- AWS CDKを使用することで、基盤も1つのプロダクトのように扱うことができ、レビュープロセスの簡素化、リリースサイクルの短縮化、複雑さの軽減、バージョン管理の効率化を実現した
- ガードレールの開発・実装期間は2週間から2日に短縮

# ここまでのまとめ

- クラウドの特性を活かした発見的統制を考える
- Amazon GuardDuty や AWS Security Hub など AWS環境の特性が考慮されている発見的統制の仕組みを利用することも有効
- APIを利用して環境の操作が可能なAWS環境では、検知されたイベントに対して、自動修復を行うことも可能



# 関連情報

- AWS Summit Japan での関連セッション
  - 運用視点で考えるAWSのセキュリティ体制強化
- 過去のセッション
  - AWS re:Invent 2021: Citi: Scaling security guardrail development via AWS CDK [動画](#) | [資料](#)
- その他のリソース
  - ワークショップ AWS 環境における脅威検知と対応 [資料](#)

- AWSアカウントの構成・統制のためのメカニズム
- AWS環境に発見的統制を実装するためのメカニズム
- 安全に権限を委譲するためのメカニズム

# 権限委譲を行う上での考慮点

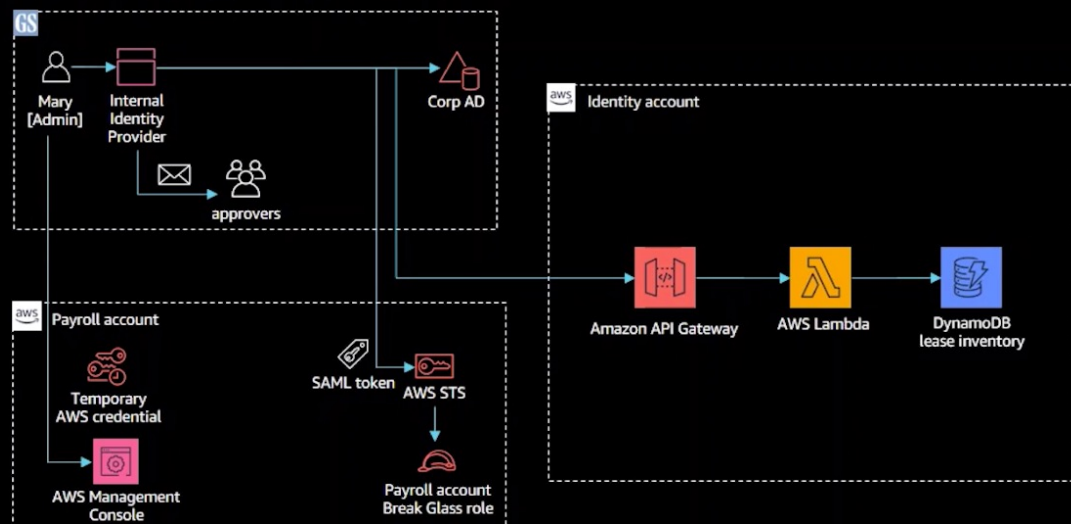
- Landing Zoneや発見的統制で、一定水準のセキュリティレベルを保ちながら、システムや業務を担当するチームに権限を可能な限り委譲することがアジリティという観点では望ましい
- 金融機関では、関連する規制や内部統制の観点から、無条件に権限を委譲することが難しいケースも存在する
- そういった制約がある中で、権限委譲を行うための仕組みや工夫を取り上げる

# 必要な権限を一時的に払い出すメカニズム

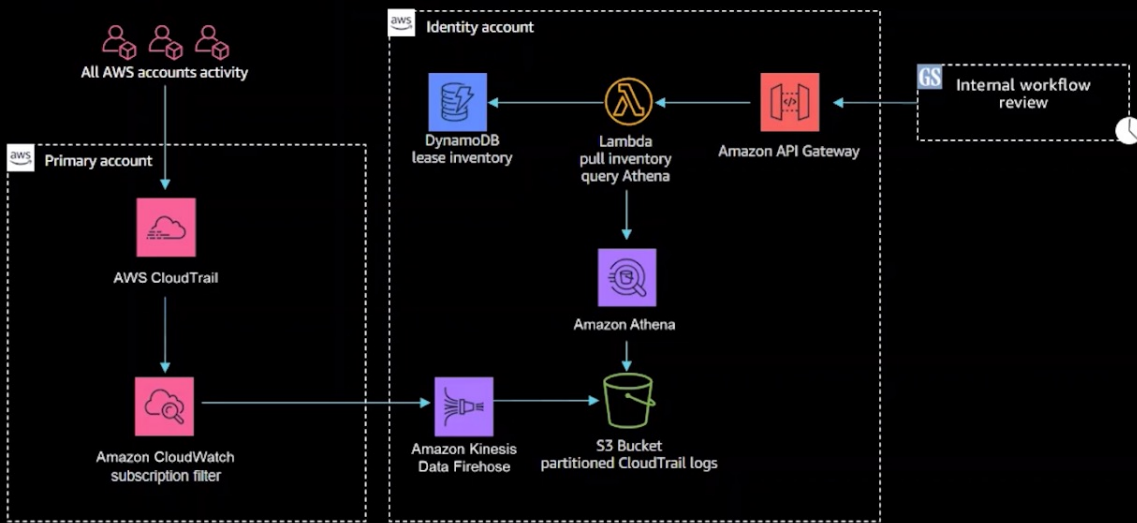
- 常時付与されていないが、必要な操作に関しては、申請をもとにして、一時的に権限を払い出すことも考えられる
- 権限の払い出しの仕組みを自動化し、監査に必要な情報を収集することで、ガバナンスを効かせた上で、権限の委譲を行う

# Goldman Sachs : 一時的な権限昇格のコントロール

## Break Glass workflow



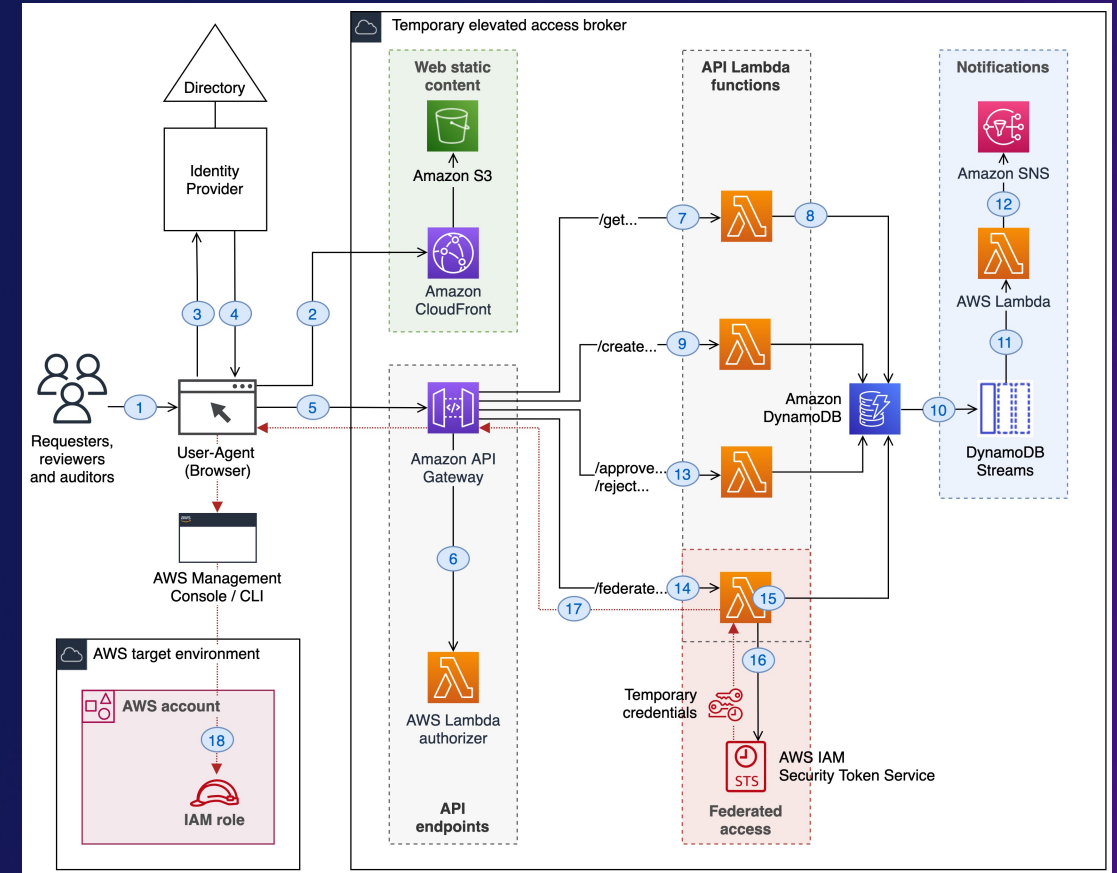
## Post access workflow



- 常時割り当てられているわけではないが、追加で権限が必要な作業が発生した際には、承認をもとに一時的なアクセス権限を払い出す。このプロセスを自動化
- セッションに付与する権限を制限するセッションポリシーを利用して制限。セッションごとに最小権限を付与
- 事後の監査のために、セッション名にユーザーIDと払い出しIDを付与。これによりCloudTrailログと、申請内容を紐付けて監査できる

# リファレンス実装: AWS 環境への一時的な昇格アクセスの管理

- 一時的に必要な権限の利用を申請・付与・監査するための最小限のリファレンス実装
- [GitHub](#)でリファレンス実装を提供するとともに、[Blog 記事](#)にて実装内容を紹介





# 多様なAWSサービスの利用

- AWSには、200を超えるサービスがあり、新しいサービスも高頻度で利用可能となる
- アジリティの観点では、すべてのAWSサービスを制限なく利用できることが望ましいが、構築するシステム特性によって、サービスごとのセキュリティ上の考慮点などを事前に確認しておくことが望ましい場合も存在する
- AWSサービスのセキュリティ上の考慮点の確認を効率的に進める仕組みが必要となる



# セキュリティリスク評価共同化 WG

## 課題

AWSサービスを利用する上でのリスクの洗い出しと統制機能の整理・確認を金融機関各社が個別に実施していたが、その負荷が高い



## 解決策

10社の金融機関とAWSが共同で、各サービスの評価を実施。これまで16のサービスの評価を実施(2022年3月時点)



## 効果

新規セキュリティ評価実施時に、WGの成果物があると、無い場合に比べ3割程度の省力化(工数削減)できる見込み  
(みずほリサーチ&テクノロジーズ様の例)

## 金融機関の知見を反映した評価シートの作成

シート名	説明
利用シナリオと接続経路	サービスへの接続経路と利用シナリオを記載
セキュリティクライテリア	セキュリティリスクに関する7評価観点19対策 分類の観点から、当該サービスで利用可能な統制の概要情報を整理したもの
サービス利用時の留意事項	サービスの利用時に留意すべきTips

# ここまでのまとめ

- 必要な権限を一時的に払い出すメカニズムの実装
- 多様なAWSサービスを活用していく上でのサービスのリスク評価共同化の仕組み

# 関連情報

- AWS Summit Japan での関連セッション
  - イノベーションを加速するセキュリティ - AWS Identity Servicesでビジネスの成功の礎をつくる -
- 過去のセッション
  - AWS re:Invent 2020: How Goldman Sachs administers temporary elevated AWS access [動画](#) | [資料](#)
- その他のリソース
  - AWS 環境への一時的な昇格アクセスの管理 [Blog](#) | [GitHub](#)

# まとめ

- アジリティとセキュリティの両立のためには、セキュリティのベストプラクティスをメカニズムとして実装することが有効
- メカニズムを実装するために AWSサービス、リファレンス実装、事例などを活用する
  - マルチアカウントの統制: AWS Control Towerなどを利用したLanding Zoneの構築
  - 発見的統制: Amazon GuardDuty、AWS Security Hub、自動修復などクラウドの特性を活かした発見的統制と対応
  - 権限委譲: 権限払い出しや監査、セキュリティ評価を行うための仕組み

# Thank you!

