

# 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～

勝原 達也

技術統括本部 技術推進本部 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

# 自己紹介

勝原 達也 (Tatsuya Katsuhara)

セキュリティ ソリューション アーキテクト



略歴：

SIer にてデジタル・アイデンティティと認証・認可ソリューション担当、  
セキュリティ専門会社で Web、工場・プラント、IoT・自動車のセキュリティ、  
AWS にてお客様の AWS 活用におけるセキュリティ課題解決の支援に従事

好きな AWS サービス：

Amazon Cognito、AWS Single Sign-On、AWS IoT

# 本セッションについて

## 想定視聴者

- AWS Identity and Access Management (IAM) の基本的な機能について理解しており、権限管理とアクセスコントロール分野でのセキュリティ改善を検討している方
- AWS 環境に対するシングル・サインオンや多要素認証、モバイルアプリの認証・認可ワークフローに関心をお持ちのかた

## ゴール

- AWS Identity Services の各サービスが適しているワークフローを把握し、活用すべきサービスを正しく選択できるようになる
- AWS Identity Services を活用したセキュリティ改善の勘所をつかむ



# Agenda

- セキュリティ vs イノベーション
- AWS Identity Services によるセキュリティ改善の勘所 – 3つの視点
  1. 適切なアクセス制御を実現するアーキテクチャ
    - データ境界
    - 最小権限への旅路
    - クレデンシャルの強化
  2. 環境・人・ビジネスをシームレスに統合
    - 組織の AWS 環境の一元管理
    - アイデンティティ&アクセスの一元管理
  3. ユーザー体験に直結する Web・モバイルアプリケーション
    - アプリケーション向けアイデンティティ・サービス
- まとめ

# セキュリティ vs イノベーション

セキュリティはビジネスの成功に  
ブレーキをかける要因だと思いますか？

“セキュリティ対策の実施を  
**「コスト」と捉えるのではなく、**  
将来の事業活動・成長に必須なものと  
位置づけて**「投資」と捉える**ことが  
重要である。”

サイバーセキュリティ経営ガイドライン Ver 2.0  
経済産業省、独立行政法人 情報処理推進機構

[https://www.meti.go.jp/policy/netsecurity/mng\\_guide.html](https://www.meti.go.jp/policy/netsecurity/mng_guide.html)



セキュリティとビジネスの  
成功は**両立**していくべき

**ブレーキ**がついているから、  
**安心**して**アクセル**を踏み込む  
ことができる

**セキュリティを改善**することは  
**ビジネスの成功へ加速**すること



# AWSは、セキュリティはイノベーションの重要なドライバーの1つであると考えています



セキュリティ改善



アジャリティ向上



イノベーション加速

# イノベーションを加速するセキュリティの特徴



**自動化されスケールすること**  
**可視化され継続的に改善可能であること**  
**コスト対効果に優れていること**

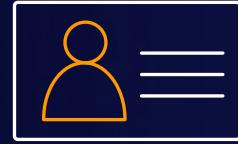


新たな活動に投入できる経営資源を生み出す



失敗コスト低減&積極的チャレンジのサイクル

# セキュリティ範囲は広く、様々な取り組み方がある



アイデンティティ  
&アクセス管理



発見的統制



インフラストラクチャ  
防御



データ保護

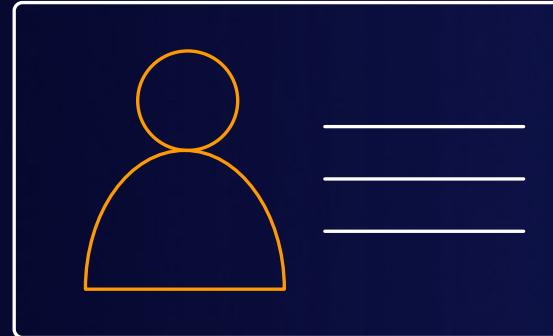


インシデント  
レスポンス



コンプライアンス

# ビジネスの成功を下支えする「礎」に取り組もう



## AWS Identity Services

アイデンティティ & アクセス管理に関する AWS サービスの総称

- AWS Identity and Access Management (IAM)
- AWS Organizations
- AWS Single Sign-On
- AWS Directory Service
- Amazon Cognito
- AWS Resource Access Manager
- AWS Control Tower

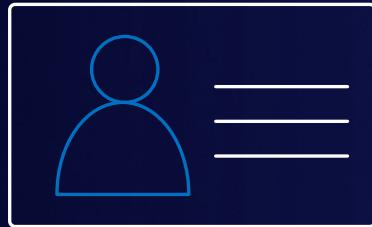
# アイデンティティ&アクセス管理

## Identity and Access Management (IAM)

誰が

(ある条件の元で)  
アクセスできる/できない

何に



アイデンティティ  
管理

アクセス  
管理

リソース  
管理

# AWS Identity Services を活用したスケールするセキュリティ改善の勘所 – 3つの視点

## 適切なアクセス制御を実現するアーキテクチャ

きめ細やか（細粒度）なアクセスコントロールにより、従業員・デバイス・アプリケーションに対する AWS サービスとリソースへ、必要とされるアクセス権を付与



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

## 環境・人・ビジネスをシームレスに統合

マルチアカウントの統合管理やオンプレミス・ビジネスアプリケーションに分散するアイデンティティの一元管理、適切なアイデンティティ・ソースとの接続による単一のアクセス戦略を確立



## ユーザーエクスペリエンスに直結するWeb・モバイルアプリ

シンプルでセキュア・スケーラブル、オープン標準に基づいた認証・認可アーキテクチャと、優れたユーザーエクスペリエンスのサインアップ・サインインを実現



# 1. 適切なアクセス制御を実現する アーキテクチャ



# お客様の思いはシンプル

ある部門の従業員だけが、会社の重要データにアクセスできるようにしたい。

従業員が重要なデータを社外に持ち出せないようにしたい。



# セキュリティとアジリティを 両立させるためのコンセプト

## セキュリティガードレール

- ・開発スピードを妨げない配慮をしつつ
- ・セキュリティ事故を防ぐために
- ・越えてはならない境界を定めておく



# データ境界 (Data Perimeter)



アイデンティティ境界



ネットワーク境界



リソース境界

信頼された  
**アイデンティティ**が

想定された  
**ネットワーク**から

信頼された  
**リソース**にアクセス

以上 3 つの観点を組合せ、セキュリティガードレールの考え方にして、データ境界を形作っていくことが大切

# IAM 領域でデータ境界を形作るための ポリシーベースのアプローチ



3つの境界要素



IAM 領域における 3 つのポリシー



# IAM の各種ポリシーの基本的な考え方

## IAM Policy の例

注: Principal はポリシーのアタッチ対象であるため、IAM Policy では記載なし

```
{  
    "version": "2012-10-17",  
    "Statement": [ {  
        "Effect": "Allow",  
        "Action": [ "ec2:Attachvolume", "ec2:Detachvolume" ],  
        "Resource": "arn:aws:ec2:*.*:instance/*",  
        "Condition": {  
            "StringEquals": {  
                "ec2:ResourceTag/Department": "Development"  
            }  
        }  
    } ]  
}
```

## PARC 要素

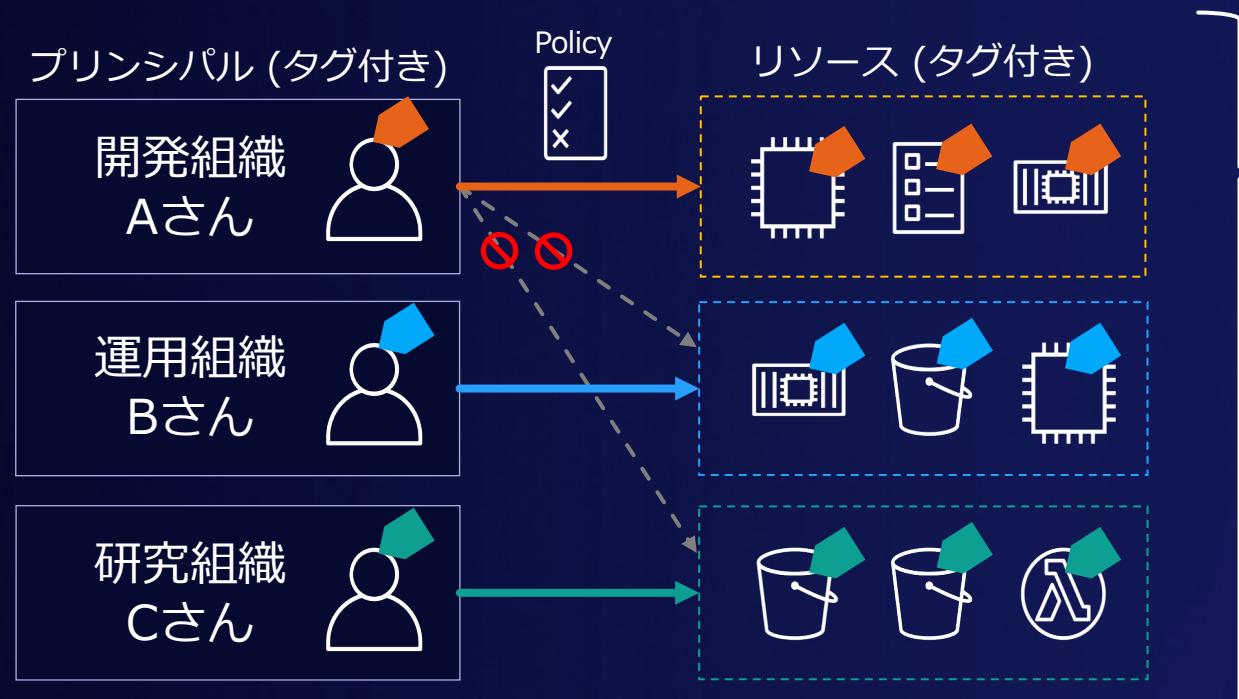
- **P**rincipal  
誰が
  - **A**ction  
どのような行為を
  - **R**esource  
どのような対象へ
  - **C**ondition  
どのような条件で
- 許可 (Allow)、拒否 (Deny)

# データ境界の構成に便利なポリシー変数の例

データ境界の構成要素	ポリシー変数	意味
アイデンティティ境界	PrincipalAccount	特定の AWS アカウント ID
	PrincipalArn	特定のプリンシパルの ARN
	PrincipalIsAWSService	プリンシパルが AWS サービスかどうか (bool)
	PrincipalOrgId	特定の組織 ID
ネットワーク境界	SourceIP	アクセス元 IP アドレス
	SourceVpce	アクセス元 VPC Endpoint
	SourceVpc	アクセス元 VPC
リソース境界	ViaAWSService	AWS サービスを介したアクセスかどうか (bool)
	CalledVia	アクセスを代行した AWS サービスプリンシパル名
リソース境界	ResourceTag/ <i>key-name</i>	リソースが持つ <i>key-name</i> タグの値

# タグを用いてリソース境界を構成する手法※

「あるタグ」が付与されたプリンシパルだけが「同じタグ」のリソースへアクセス可能、といった制御が可能



## 実現のポイント

- タグ標準化  
キーと値の標準化で「効果」を高める
- AWS Resource Groups & Tag Editor  
効率的なタグ管理で「実現性」を高める

※管理対象サービスがタグに対応している前提

# 最小権限へ至る道

最小権限は一日にして成らず

優れた道具を使いこなし  
権限の見直しサイクルを回す



# IAM Access Analyzer

データ境界の構成と最小権限のための改善サイクルを支援



## ポリシー自動生成

過去のアクセス履歴を分析し、素早く・適切な権限を自動生成

## ポリシーチェック

100 以上のチェック観点で、セキュアで機能的なポリシーの作成を支援

## 外部アクセスレビュー

意図しない外部公開設定の有無を、ポリシー反映前に確認、未然に防止

## 外部アクセス分析

意図しない外部公開設定の有無を、現状ポリシーを元に分析、要否確認

## 最終アクセス時刻

最終アクセス時刻を元に、利用していない権限の発見と削除

“発生するインシデントの 80% は  
侵害された、あるいは弱い  
クレデンシャルに起因する”

**Stephen Schmidt**

Chief Information Security Officer, AWS (now CSO, Amazon)

AWS re:Inforce 2021 - Keynote



# 多要素認証 (MFA※)

※Multi Factor Authentication

多要素認証はもはや「**必須**」

- AWS アカウント/IAM アカウント
- シングル・サインオン
- エンドユーザー向けアプリケーション

AWS 環境、お客様、  
更にエンドユーザーを守る



# 一時クレデンシャルを活用したセキュアなアクセス

- 漏洩リスク軽減：有効期限の長い IAM アクセスキーをそもそも使わない
- 影響範囲の局所化：有効期限切れで自動無効化
- スケールする仕組み：事前ユーザー登録不要な動的ロールベースアクセス許可

## アプリケーションのロールによる実現

例：EC2 インスタンスロール



## フェデレーションによる実現

例：クロスアカウント、AWS Single Sign-On、Amazon Cognito



## 2. 環境・人・ビジネスをシームレスに統合



# マルチアカウント運用の必要性が高まっている

「AWS アカウント ≈ リソースのコンテナ ≈ 分離境界」

AWS アカウントを分けて解決できる様々なビジネス要件がある



チーム特性に  
合った環境整備

チーム、プロジェクト、プロダクトの特性に合わせてアカウントを分け、メリハリの効いた統制



請求の  
簡素化

部門毎に AWS アカウントを分けることで、コスト責任を明確化



ビジネスプロセス  
との整合性

ビジネスプロセスにおける運用や規制、職務分掌などを、AWS アカウントに沿えて整理する



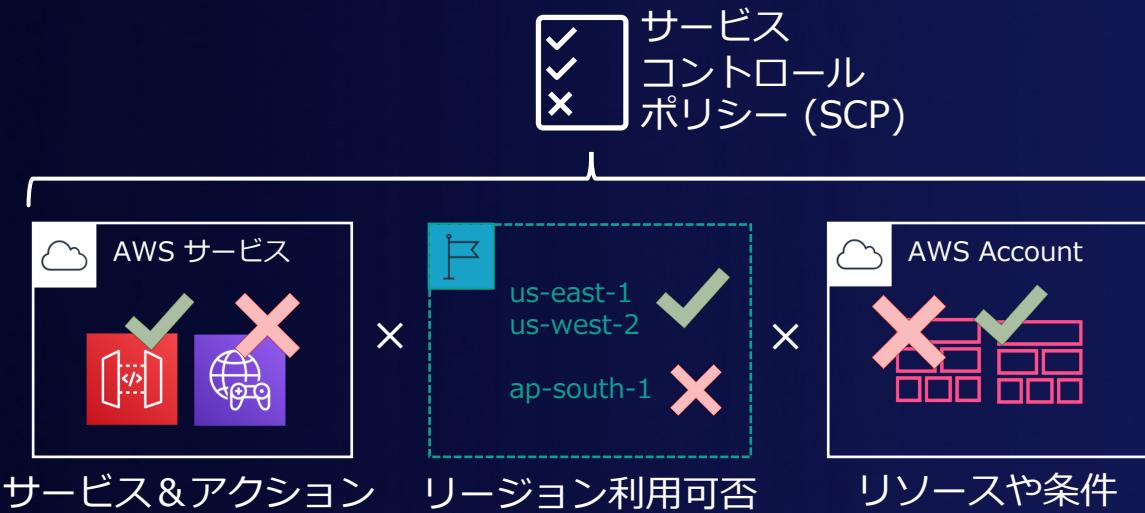
柔軟な  
セキュリティ制御

リスクや機能・取り扱いデータ等の類似性をもとにアカウントを分け、管理を容易に

# マルチアカウントに統制を - AWS Organizations

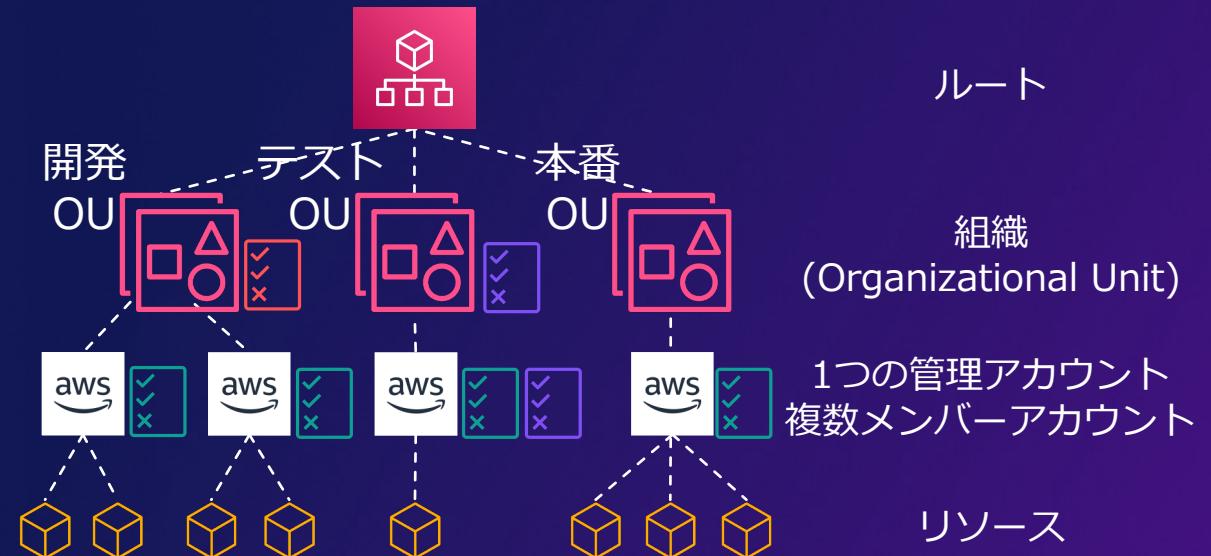
## 組織横断的に権限をコントロール

- サービスコントロールポリシーで横断的統制
- きめ細やかな制御を活かし、セキュリティガードレールの考えに沿ったデータ境界を構成



## AWS アカウントの一元管理

- 階層化による組織管理
- AWS アカウント作成の自動化・権限一括反映などによる一元化と効率化



# コラボレーションによる アクセスコントロール多様化

アクセスする人

プロジェクトメンバ、外部委託先、お客様…

アクセスする経路

自社・お客様ネットワーク、自宅、モバイル…

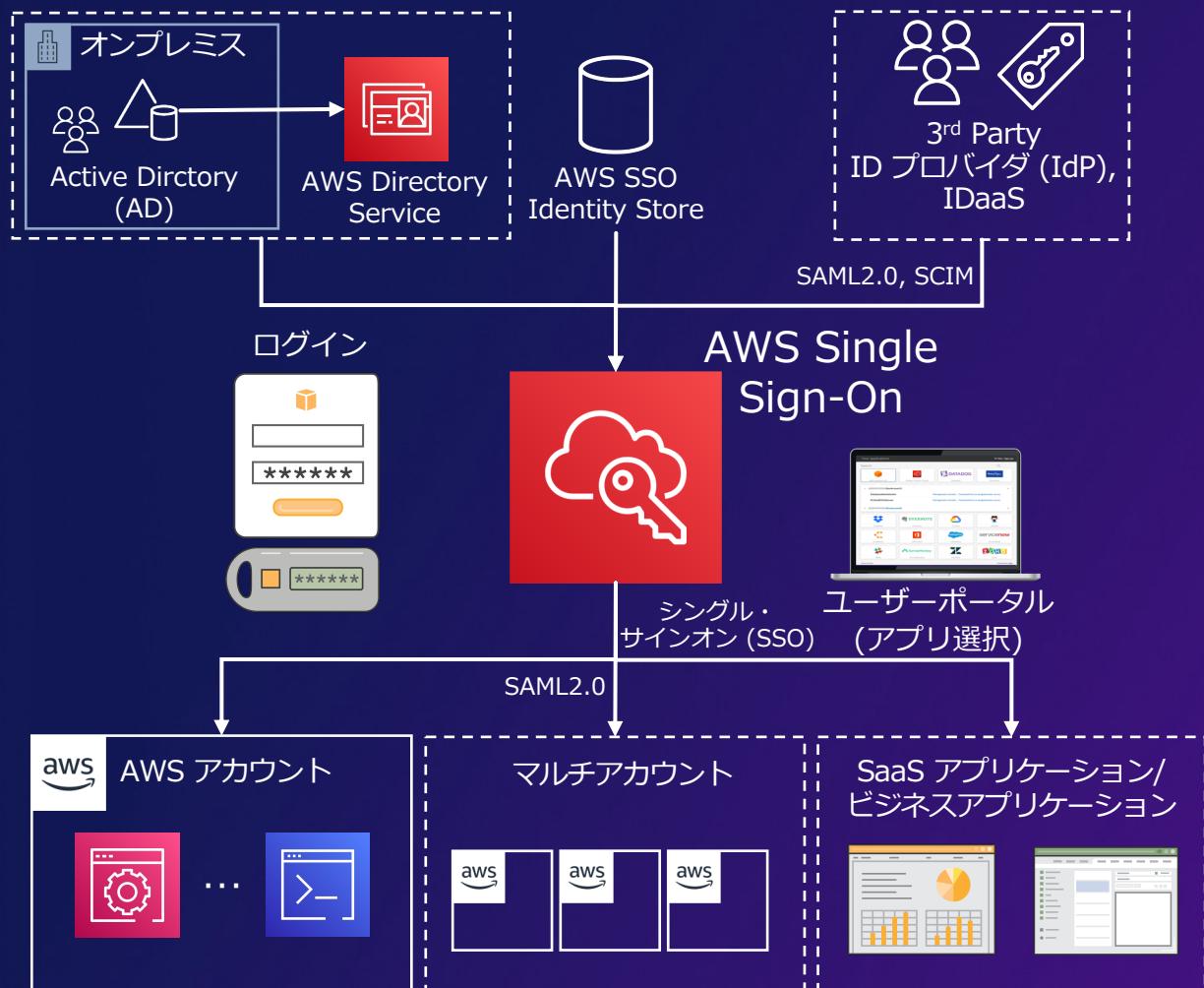
アクセスする先

オンプレミス、AWS アカウント、SaaS…

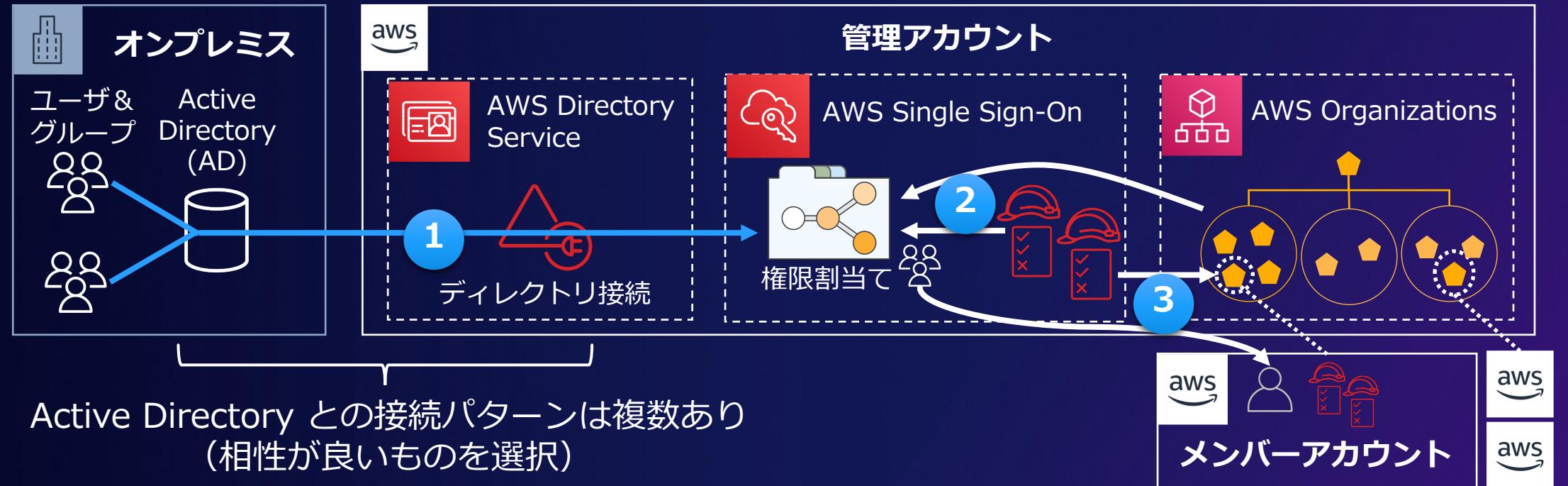


# AWS Single Sign-On – アイデンティティ・ハブ

- ユーザー認証とアクセス認可、アイデンティティの一元管理
- マルチ AWS アカウントやビジネスアプリケーションへのシングル・サインオン (SSO)
- 組織に合わせたアイデンティティストアを選択可能
- AWS コマンドラインインターフェース (CLI) v2 との統合  
一時クレデンシャル活用によるセキュリティ向上



# AWS Directory Service と AWS SSO で実現する オンプレミスとのハイブリッドなアクセス制御



1. AWS Directory Service を用い、  
オンプレミス Active Directory と  
AWS Single Sign-On を接続

2. AWS Single Sign-On で、  
各組織へ SSO するための設定と  
ユーザーへの権限割り当てを実施

3. Organizations で、  
メンバーアカウントに権限を  
一括反映し、SSO してくる  
ユーザーを受け入れる設定を実施

### 3. ユーザー体験に直結する Web・モバイルアプリケーション



# モダンな Web・モバイルアプリ開発の共通の悩み



差別化要素でない重厚な  
アイデンティティ関連の  
処理をオフロードしたい



既存または  
クラウドネイティブな  
アイデンティティを選択さ  
せてユーザーを増やしたい



アプリケーションに  
標準に基づいた認証・認可の  
仕組みと先進的な  
セキュリティを実装したい

# Amazon Cognito はお手軽かつフルマネージドな アプリケーション向けアイデンティティ・サービス

柔軟かつスケーラブルな  
API と SDK のサポート



Build-in UI コンポーネント



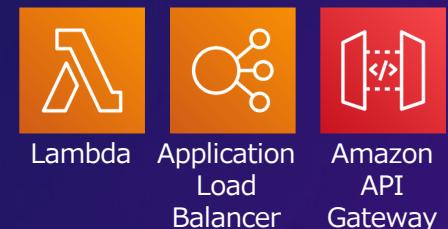
巨大な利用者を持つ ID プロバイダ  
(IdP) との接続を簡単に構成



セキュア/可用性



拡張可能な認証・認可



オープン標準への対応を  
簡単に構成



# アーキテクチャ概要

## ユーザープール (①~④)

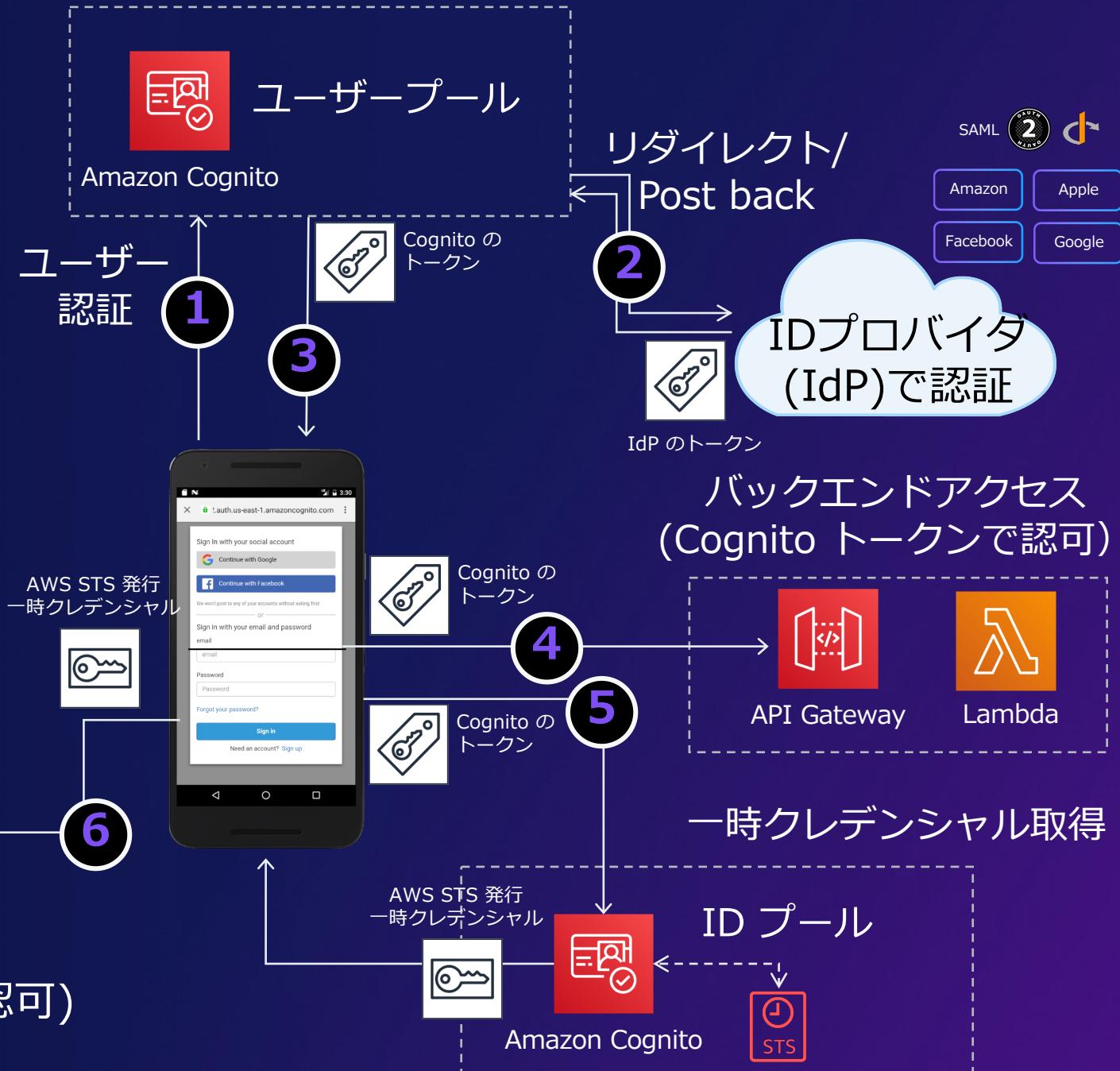
- IdP のユーザー認証結果に基づいて Cognito トークンを生成
- Cognito トークンはバックエンドへのアクセス認可に利用

## ID プール (⑤~⑥)

- ユーザープールから取得した Cognito トークンをもとに AWS サービスにアクセスするための一時クレデンシャルを発行・利用



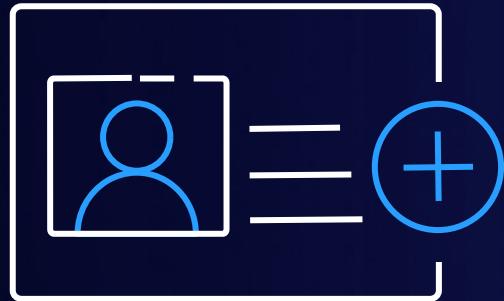
AWS サービスへのアクセス  
(有効期間の短いアクセキーで認可)



# まとめ



# AWS Identity Services は様々なワークフローのセキュリティを自動化し、改善し、スケールさせる



## ポリシーと条件を用いたデータ境界

AWS Identity and Access Management

## 最小権限への継続的な取り組み

IAM Access Analyzer

## クレデンシャルの強化

多要素認証と一時クレデンシャル

## マルチアカウント統制

AWS Organizations

## アイデンティティ & アクセスの一元管理

AWS Single Sign-On と AWS Directory Service

## セキュアでユーザー体験に優れたサインイン&サインナップ<sup>®</sup>

Amazon Cognito

# 参考情報

- AWS Identity Services  
<https://aws.amazon.com/jp/identity/>
- AWS 環境で重要データを保護するセキュリティモデル : データ境界 (Data Perimeter) を学ぶ  
[https://www.awssecevents.com/ja/ondemandtracks/tech\\_track\\_5/](https://www.awssecevents.com/ja/ondemandtracks/tech_track_5/)
- IAM の一時的な認証情報  
[https://docs.aws.amazon.com/ja\\_jp/IAM/latest/UserGuide/id\\_credentials\\_temp.html](https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_temp.html)
- AWS Organizations における組織単位のベストプラクティス  
<https://aws.amazon.com/jp/blogs/news/best-practices-for-organizational-units-with-aws-organizations/>
- [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  
(URL は AWS Summit Online 2022 セッションリストをご確認ください)
- AWS アカウント シングルサインオンの設計と運用  
[https://d1.awsstatic.com/webinars/jp/pdf/services/20200722\\_AWSBlackbelt\\_シングルサインオンの設計と運用.pdf](https://d1.awsstatic.com/webinars/jp/pdf/services/20200722_AWSBlackbelt_シングルサインオンの設計と運用.pdf)
- Amazon Cognito (Blackbelt サービス別紹介資料)  
[https://d1.awsstatic.com/webinars/jp/pdf/services/20200630\\_AWS\\_BlackBelt\\_Amazon\\_Cognito.pdf](https://d1.awsstatic.com/webinars/jp/pdf/services/20200630_AWS_BlackBelt_Amazon_Cognito.pdf)



# セキュリティ改善で イノベーションを加速しよう



# Thank you!

Tatsuya Katsuhara

Specialist Solutions Architect, Security  
Amazon Web Services Japan G.K.



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

# 付録: AWSのセキュリティサービス

本セッションで  
フォーカス



## アイデンティティ・ アクセス管理

- AWS Identity and Access Management (IAM)
- AWS Single Sign-On
- AWS Organizations
- AWS Directory Service
- Amazon Cognito
- AWS Resource Access Manager



## 発見的統制

- AWS Security Hub
- Amazon GuardDuty
- Amazon Inspector
- Amazon CloudWatch
- AWS Config
- AWS CloudTrail
- VPC Flow Logs
- AWS IoT Device Defender



## インフラストラクチャ 防護

- AWS Firewall Manager
- AWS Network Firewall
- AWS Shield
- AWS WAF – Web application firewall
- Amazon Virtual Private Cloud
- AWS PrivateLink
- AWS Systems Manager



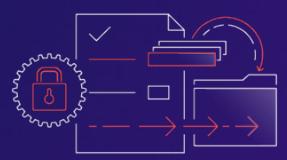
## データ保護

- Amazon Macie
- AWS Key Management Service (KMS)
- AWS CloudHSM
- AWS Certificate Manager
- AWS Secrets Manager
- AWS VPN
- Server-Side Encryption



## インシデント レスポンス

- Amazon Detective
- Amazon EventBridge
- AWS Backup
- AWS Security Hub
- AWS Elastic Disaster Recovery



## コンプライアンス

- AWS Artifact
- AWS Audit Manager