AWS におけるエンドポイントセキュリティ対策の重要性と考え方

飯田 祐基
パートナー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 (AWS)

飯田祐基（いいだゆうき）

ロール

パートナーソリューションアーキテクト

経歴

- 大手ISPでネットワーク・サーバインフラエンジニア
- スタートアップでプロダクト開発、CTO
- バックオフィス系SaaS企業でVPoE、インフラ部門責任者
- 大手リテール企業でDX推進

本日のアジェンダ

- エンドポイントセキュリティの重要性
- AWS におけるゼロトラスト
- ゼロトラストアーキテクチャ実現に向けたアプローチ
- AWS Verified Access を利用したアクセス管理
- Jamf と AWS の連携
- まとめ

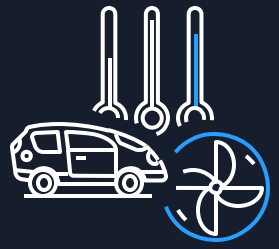
エンドポイントセキュリティの重要性

企業システムを取り巻く環境変化とセキュリティ

働き方の多様化とコラボレーション

アクセス経路の多様化やリモートアクセスによりネットワーク境界が曖昧に

DX (Digital Transformation)



様々な場所、業務でより IT システムが利用されるようになってきている。

高まるデータ保護のニーズとアプローチ変化

生成 AI の活用が進むなど、企業データがより活用されはじめている。

AWS はデータの宝庫

Matt Garman
CEO, AWS

https://www.youtube.com/watch?v=LY7m5LQliAo

AWS における脅威の例 (DDoS)

DDoS イベント
(2024 Q1)

21.2万
回

最大 Flood 攻撃

1.55 億
リクエスト/秒

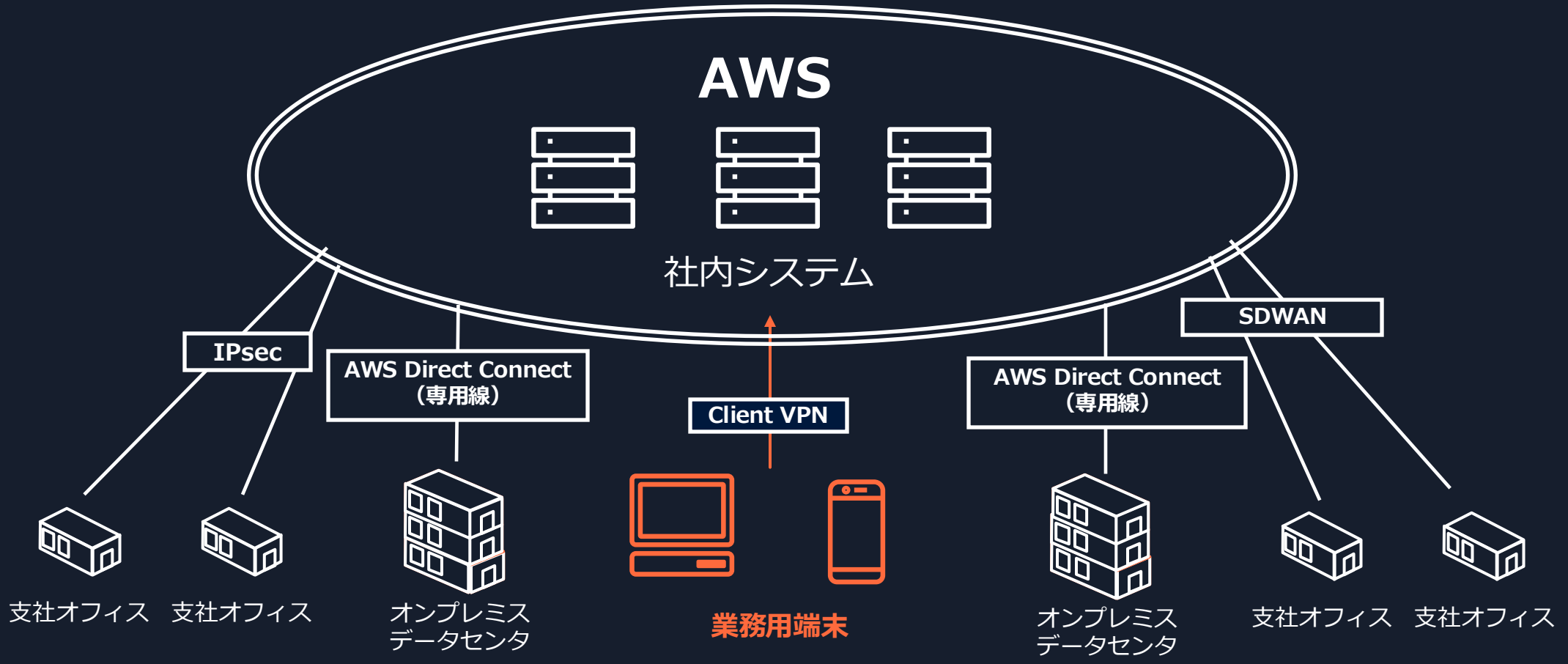
最大 NW 帯域

842
Gbit/秒

最大パケット

2.2 億
パケット/秒

AWS をコアとした社内ネットワーク



業務端末から様々な場所へアクセス可能 → 便利な反面、考慮すべき事がある

考慮すべきリスク: ランサムウェア攻撃

初期侵入

脆弱な箇所を見つけ出し侵入

業務端末へ侵入

内部活動

内部ネットワークを探索し情報収集、権限昇格

内部ネットワークを通じて AWS に侵入

データ持ち出し

目的のデータをネットワークから持ち出し

AWS 内に保存されているデータへアクセス

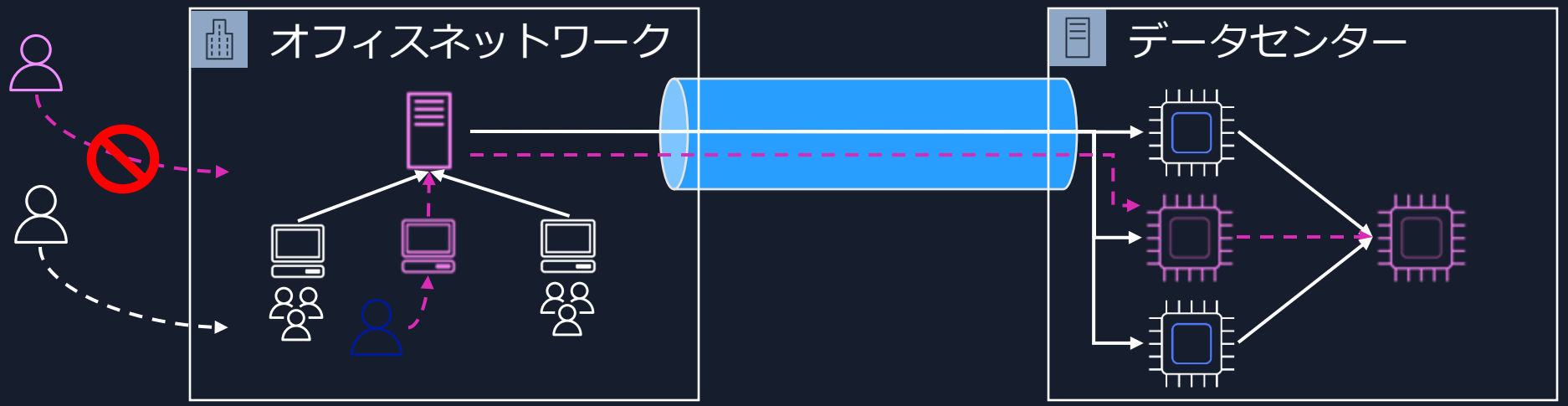
ランサムウェア実行

ファイルの暗号化、身代金の要求

AWS におけるゼロトラスト

Before “Zero Trust” – ネットワーク境界防御

- 境界の外側：
  - 信頼できる「ネットワークロケーション」からの接続のみを許可
- 境界の内側：
  - 相手を暗黙的に信頼しており、水平移動されやすく影響範囲を制限しにくい



信頼できるネットワーク同士での水平移動

“AWS は ゼロトラストが話題になる前に、
あらゆるセキュリティの話で最初から、
API を保護するためにネットワークに
依存しないアプローチを先導してきた”

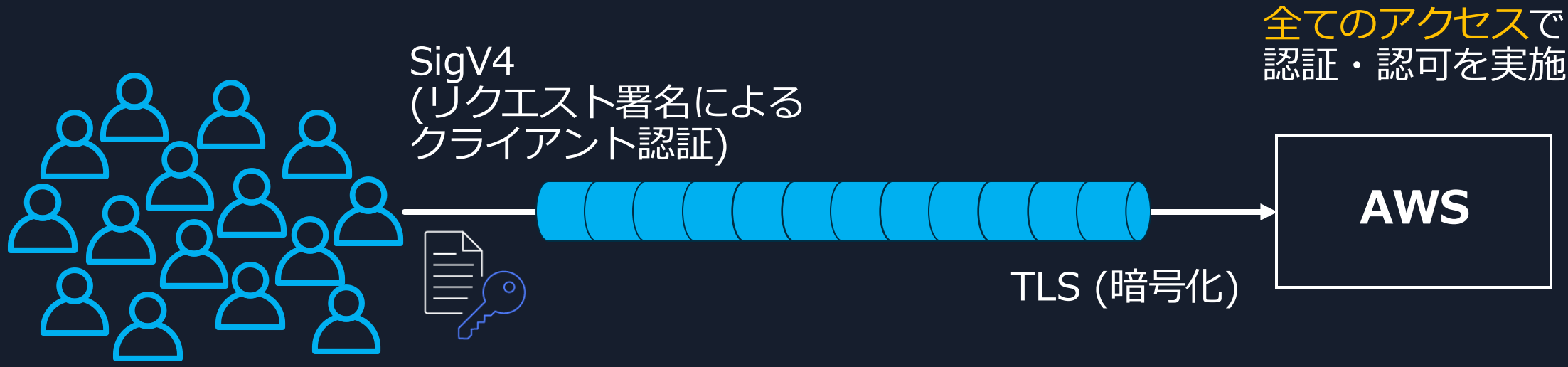
Stephen Schmidt

Chief Information Security Officer, AWS (now Amazon CSO)

AWS re:Inforce 2021 - Keynote

アイデンティティ中心の認証・認可

AWS の API アクセスにおける制御

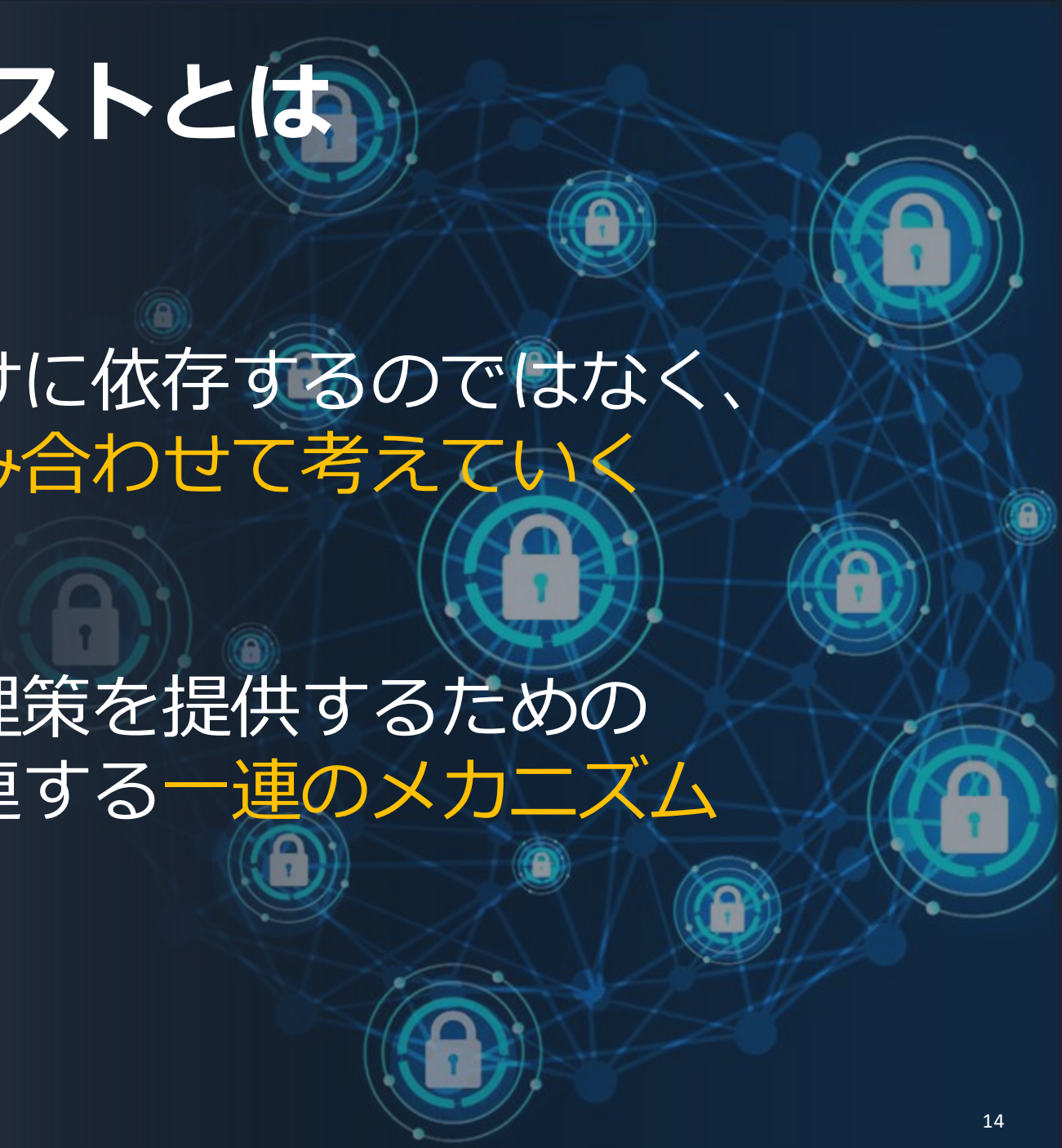


毎秒数億リクエストの割合で、個別に認証・認可が行われている

AWS が考えるゼロトラストとは

伝統的なネットワーク境界だけに依存するのではなく、
アイデンティティ境界との組み合わせて考えていく

データ保護のセキュリティ管理策を提供するための
コンセプトモデルとそれに関連する一連のメカニズム



「ゼロトラスト」は統合的な対策が必要

カテゴリ例	概要	キーワード例
アイデンティティ&アクセス管理	アイデンティティ管理とセキュアな認証・アクセス認可	• SSO, 多要素認証 • IDaaS(Identity as a Service)
スマートデバイス管理	アクセスする端末のインベントリ情報や構成・パッチ適用状況の管理	• MDM(Mobile Device Management) • EMM(Enterprise Mobility Management)
エンドポイント保護	アクセスする端末におけるマルウェアや不正アプリ対策	• EDR(Endpoint Detection & Response)
ネットワーク(リモートアクセス)	ネットワークやアプリケーションへのリモートアクセス	• SDP(Software Defined Perimeter) • SD-WAN(Software Defined WAN)
クラウドアクセス管理	外部アプリケーションに対するアクセス	• SWG(Secure Web Gateway), Web分離 • CASB(Cloud Access Service Broker) • DLP
アプリケーション・クラウド構成管理	クラウドサービスの構成管理およびアプリ／コンテナ等のセキュリティ管理	• CSPM(Cloud Security Posture Management) • CWPP(Cloud Workload Protection Platform)
インシデント・レスポンス	ログの統合、横断的なセキュリティ分析やスレットハンティング	• SIEM(Security Information and Event Management) • SOAR(Security Orchestration, Automation and Response)

※切り口およびカテゴリは例

ゼロトラストアーキテクチャ実現に向けたアプローチ

AWS でゼロトラストを実現するためのポイント

1. 二者択一ではなく、**ネットワーク**と**アイデンティティ**を組み合わせる

2. **ユースケース**にフォーカスして考える

3. 画一的に適用しようとせず**システムやデータの価値**の違いを考慮する

ネットワークとアイデンティティを組みあわせる

アイデンティティ中心　**AND**　ネットワーク中心

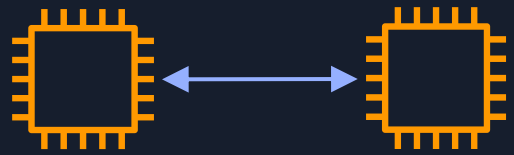
- AWS Identity and Access Management (IAM)
- AWS Verified Permissions
- AWS Verified Access

etc

Network Access Control List
(Network ACL)

ユースケースにフォーカスして考える

Human-to-application



Machine-to-machine

- 技術的な原理原則は「同じ」
- 解決したい課題に立ち返って考える
- 高付加価値な論点に取り組む

システムやデータの価値に応じた適用

- **保護したいシステムやデータの特性**を踏まえてアーキテクチャを考える
- **「画一的」**なやり方にこだわらず対象に応じて**適したもの**を模索しよう

AWS Verified Access を利用したアクセス管理

より簡単でセキュアな接続ニーズの高まり

オンプレミス環境を経由したアクセス

AWS Direct Connect

AWS Site-to-Site VPN

VPN を用いたダイレクトアクセス

AWS Client VPN

シームレスなアクセスときめ細やかなアクセス制御の両立

ネットワークに制約されない自由なアクセス

アプリケーションとセッション単位アクセス認可

ゼロトラストの考え方に近づいていく

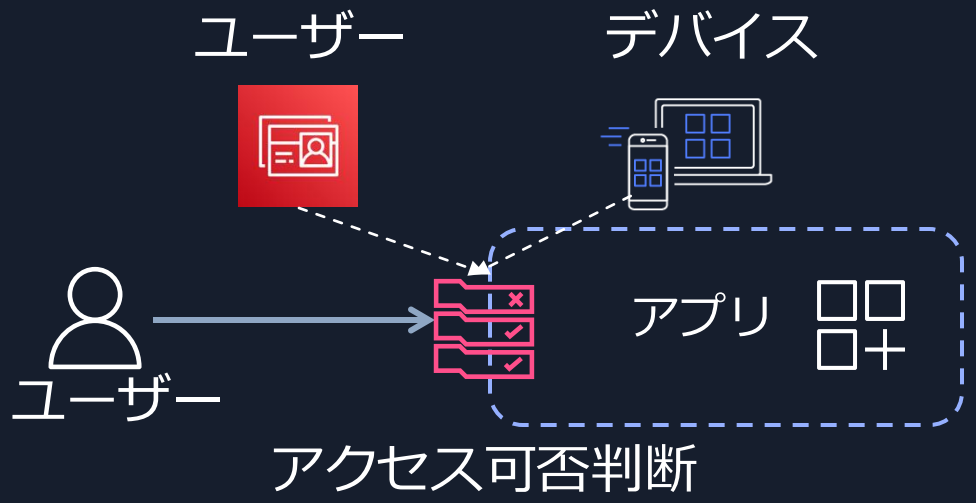
シームレスで安全なリモートアクセスを実現

AWS Verified Access

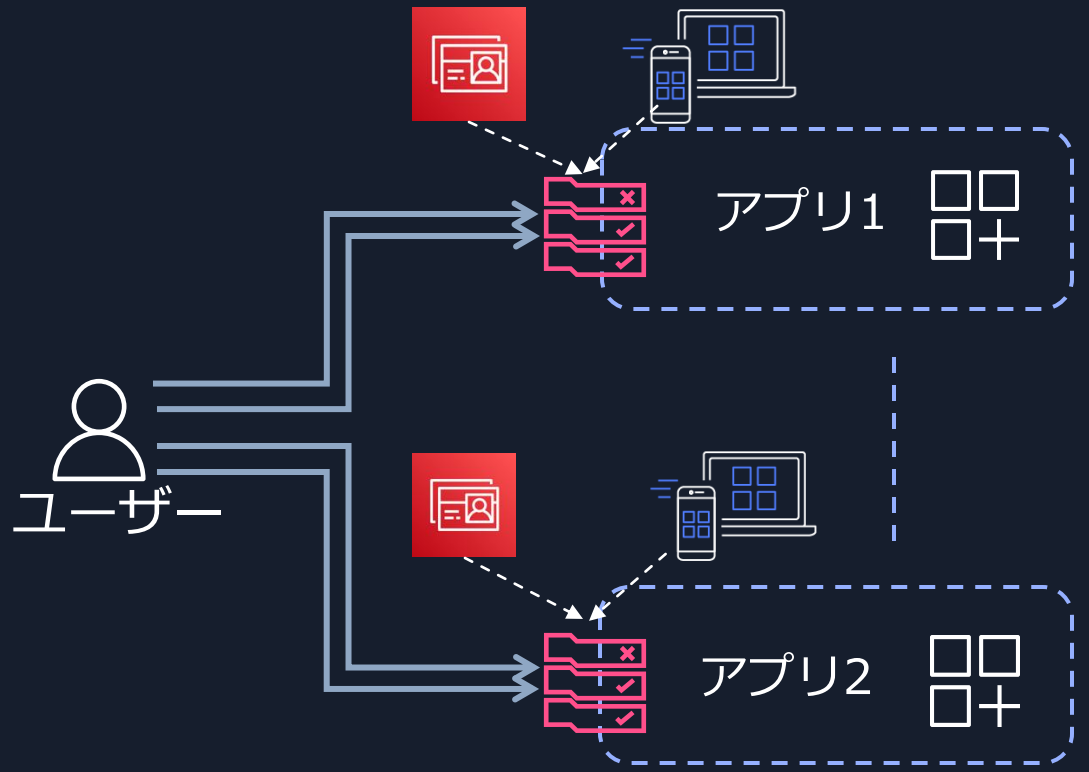
- **あらゆる場所からのシームレスなアクセス**
  - VPN を使う事なく、安全に企業アプリケーションを利用
- **ユーザーとデバイスに基づくアクセス制御**
  - ネットワークの場所に依存しない「信頼」を検証
  - 全てのリクエストを継続的にリアルタイム評価
- **セキュリティ運用をシンプルに**
  - 一元化されたポリシーの作成と管理
  - ログ一元化で監視・監査への迅速な対応と分析

AWS Verified Access のコンセプト

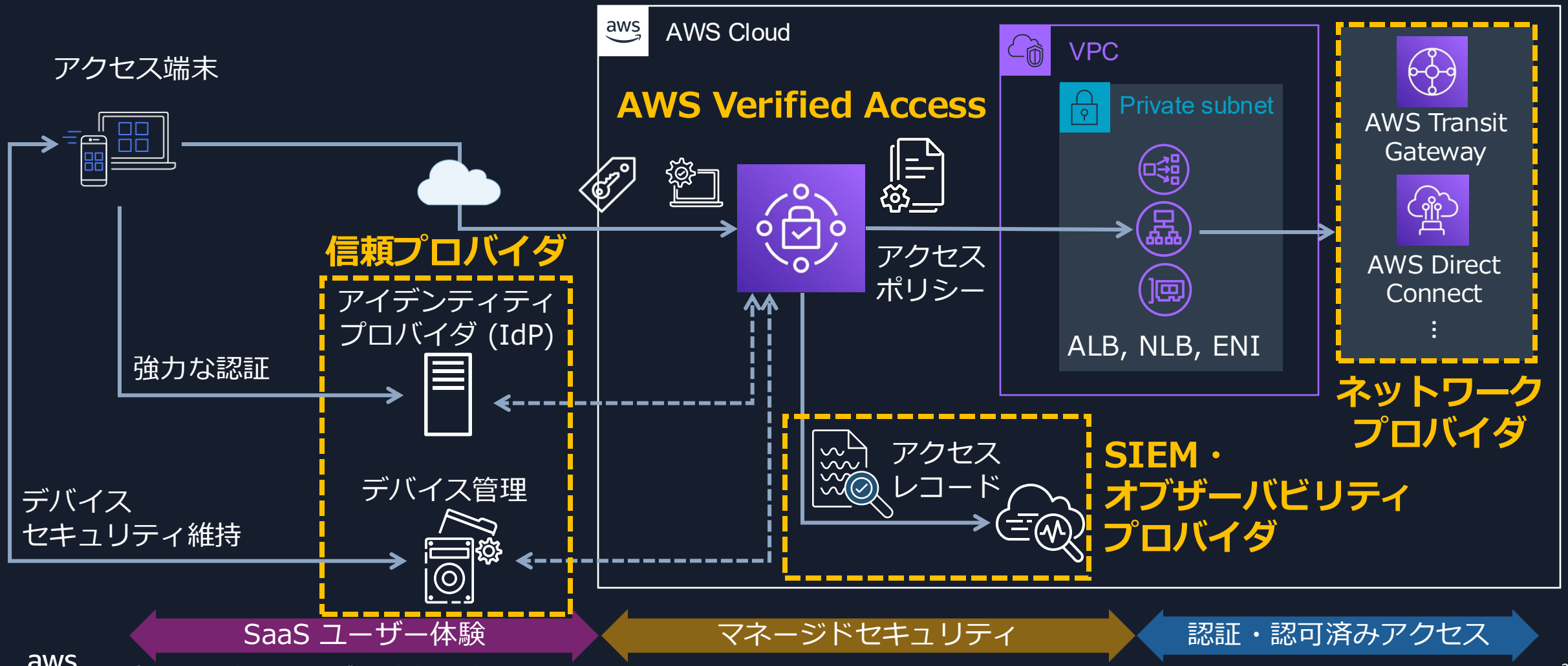
複数のソースを利用して
信頼できるアクセス元か検証



リクエストごとの継続的な検証



シームレスなリモートアクセス体験

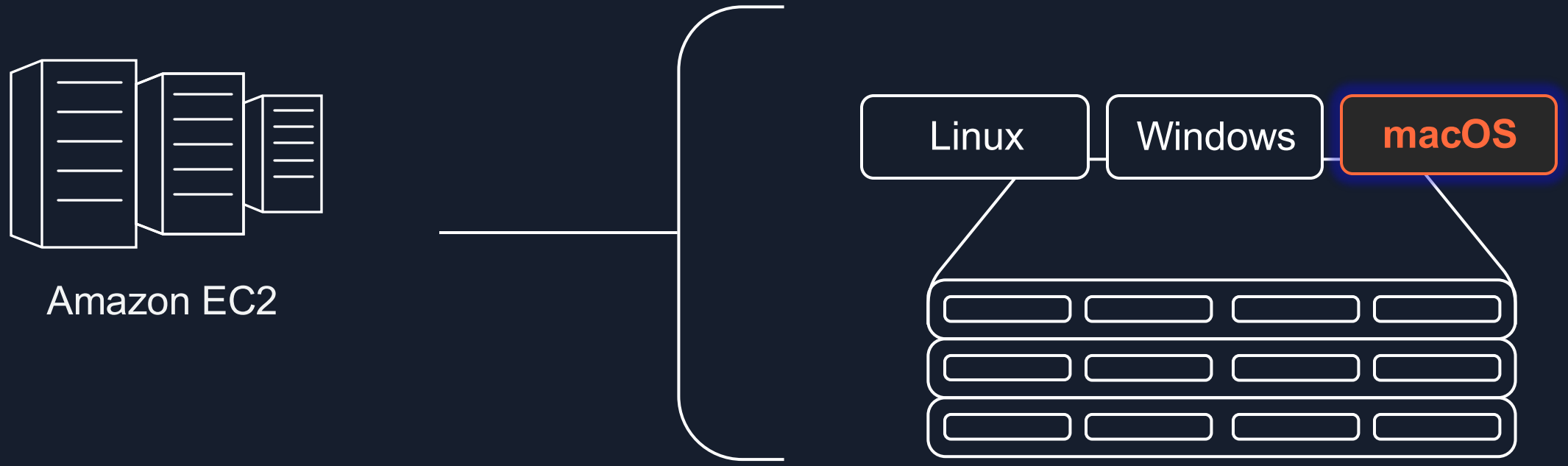


Jamf と AWS の連携

AWS Verified Access との連携

Integrating AWS Verified Access with Jamf as a device trust provider
https://aws.amazon.com/jp/blogs/security/integrating-aws-verified-access-with-jamf-as-a-device-trust-provider/

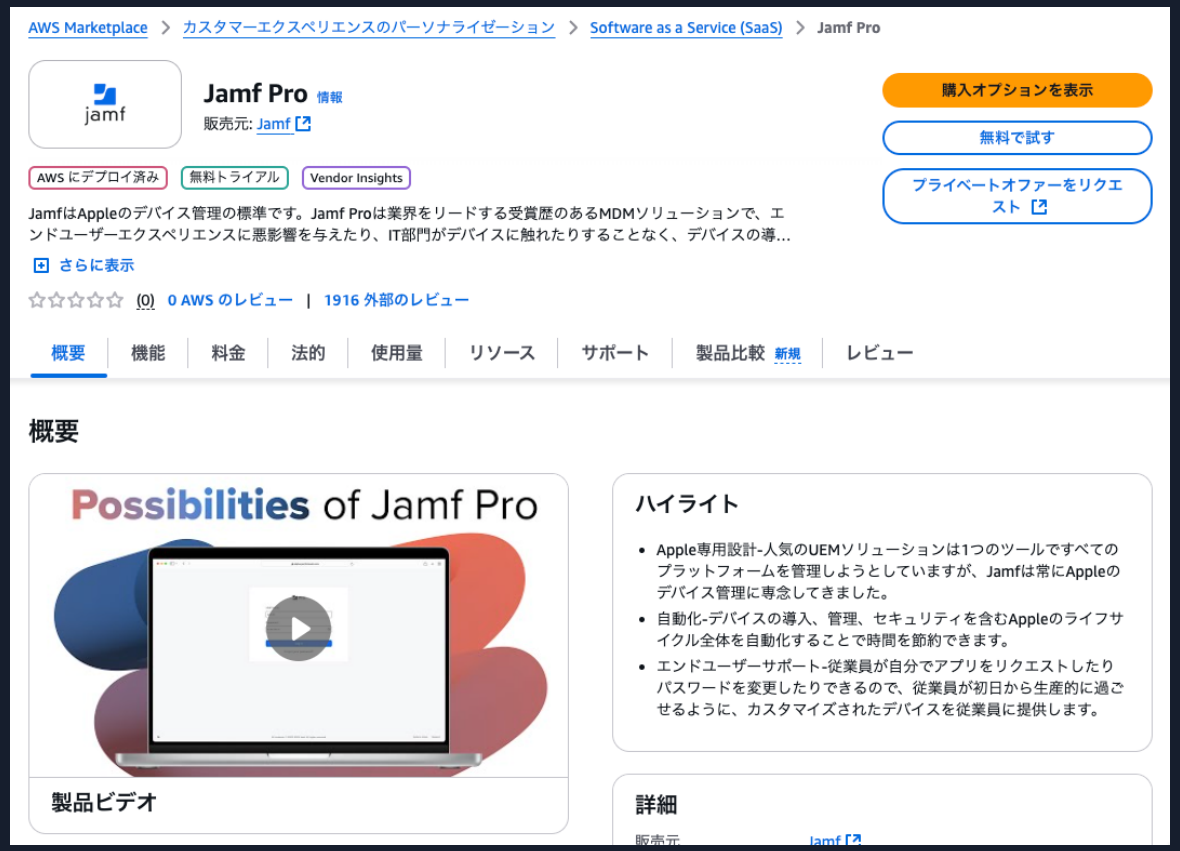
Amazon EC2 Mac インスタンスのセットアップ効率化



- AWS 上（仮想環境）で Mac OS を利用する事が可能
- 主に iOS アプリケーション開発時の動作確認での利用を想定
- Jamf を使う事でテストに必要なソフトウェアの自動インストールが可能

AWS Marketplace での販売

Jamf が提供する各ソリューションAWS Marketplace を通じて購入可能



- Jamf Pro
- Jamf Connect
- Jamf Protect

https://aws.amazon.com/marketplace/seller-profile?id=33afbdc6-58a7-4ec3-86cf-6cbab05f0a5c

まとめ

まとめ

- AWS においてエンドポイントセキュリティがなぜ重要なのか
- AWS におけるゼロトラスト
  - ネットワークと認証を合わせた制御
  - AWS Verified Access を利用したシンプルなアクセスコントロール
- Jamf と AWS の連携

Thank you!

飯田 祐基
アマゾン ウェブ サービス ジャパン合同会社
パートナーソリューションアーキテクト