MDMで管理されていれば“信頼できる”…とは限らない？

── SecureW2ではじめる、“つながる前”のアクセス制御

ペンティオ株式会社
執行役 / IDaaS事業部 シニアマネージャー
長田 紘典（Kosuke Osada）

スピーカー

長田 紘典 / Kosuke Osada

@ペンティオ株式会社

▼略歴

- 某理系大学 情報科学科 → 某私立大 法学科
- 2014年 学生アルバイトでサポートエンジニアになる
- 2018年 登用後にOneLogin製品の技術責任者になる
- 2021年 執行役兼事業部シニアマネージャーになり、ソリューション/パートナリング拡大と組織化を担当
- 2023年 エンジニア人材育成と経営戦略策定を補佐

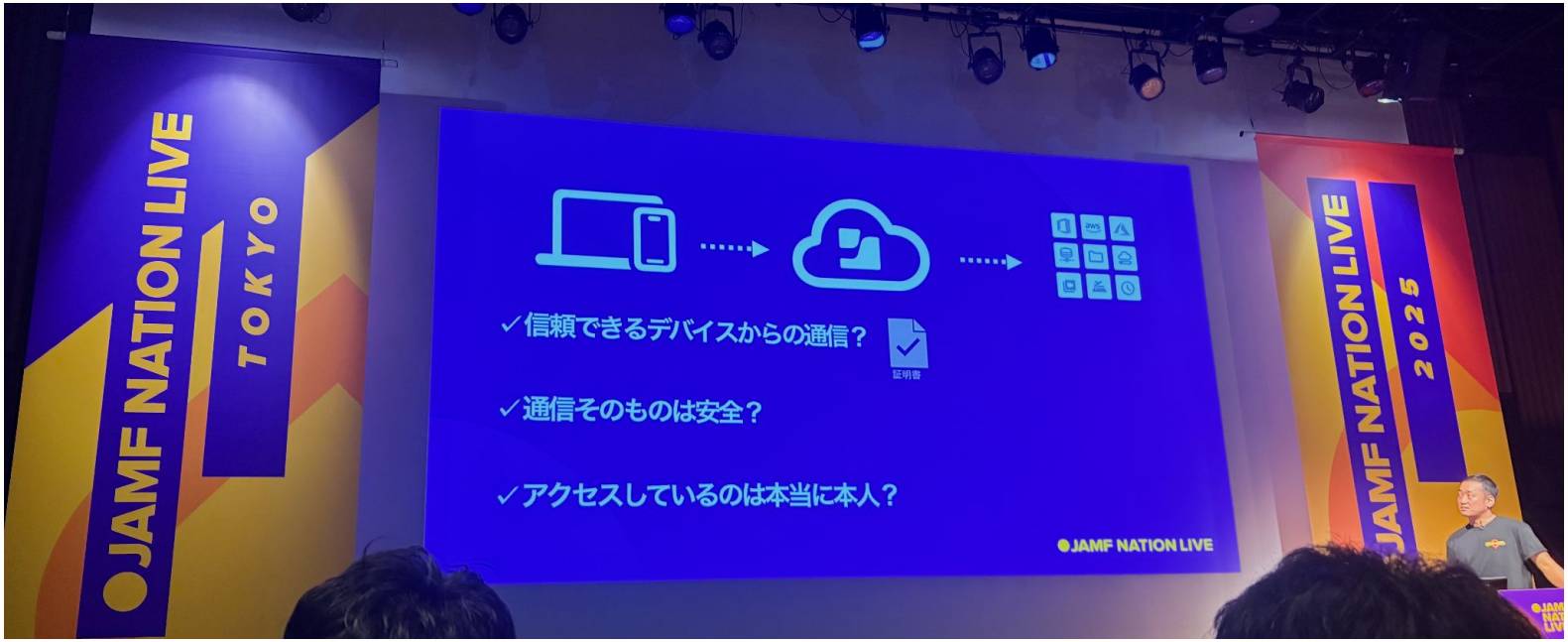
▼得意分野

2014年入社当時から**IDaaS「OneLogin」**を担当し、日本市場の立ち上げを行う。主にお客様の課題解決を目的とした導入提案、設計構築、運用支援を行う。

日本で要望の多い業務端末にアクセスを制限したいというお客様の思いを形にするため**PKI「SecureW2」**について2020年から取り組みを開始。現在は単なるデバイス認証ではく**“信頼できるデバイストラスト”**を実現するため日々ソリューション連携に取り組む。

本題に入る前に・・・

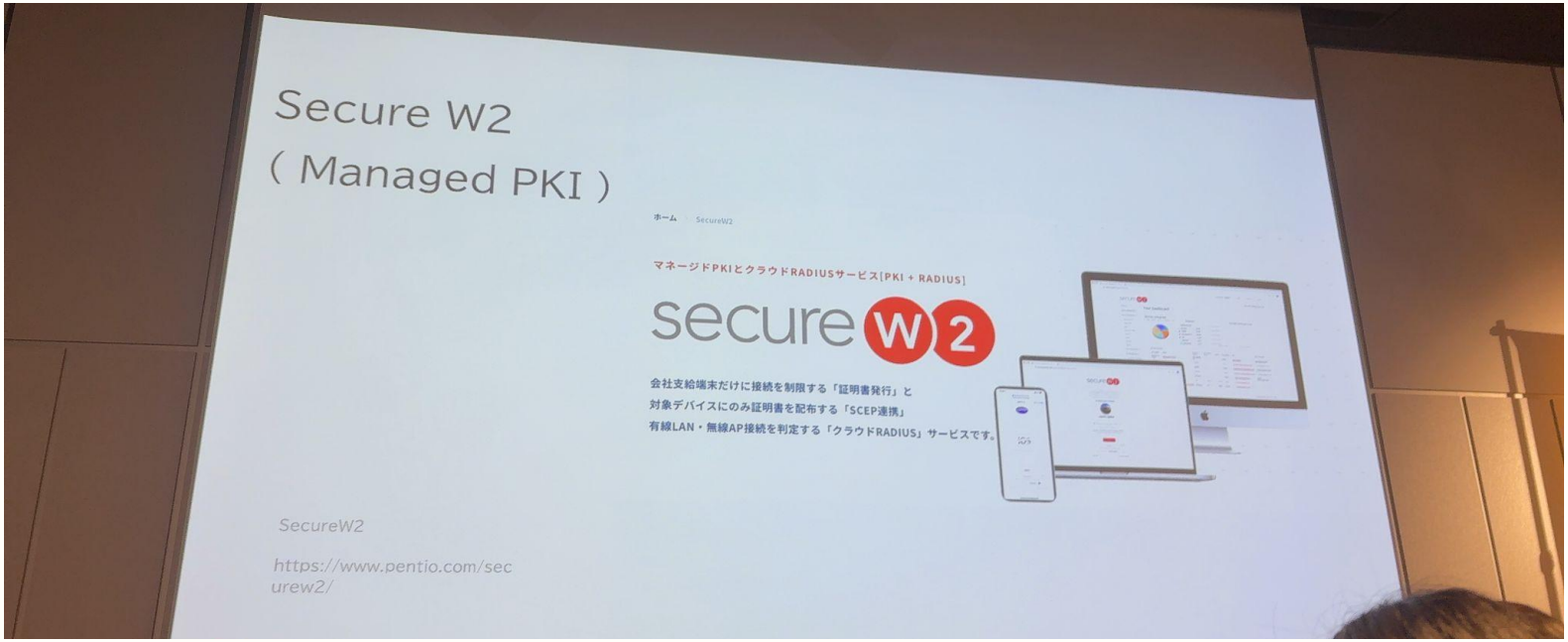
Network Relay 新機能紹介



Jamf Nation Live Tokyo 2025 基調講演にて

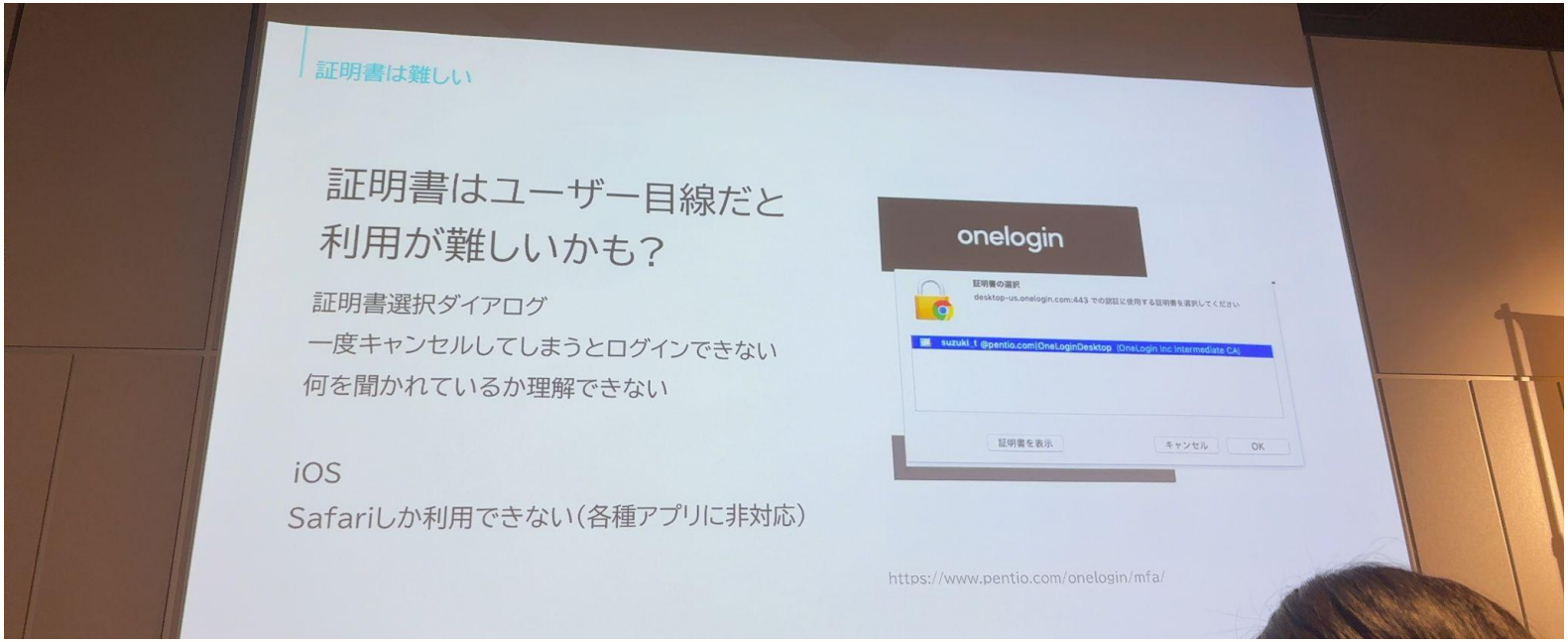
本題に入る前に・・・

Kyash 渡辺様によるHALL Cでの講演 “Jamf Connect ZTNAとMDMで実現! 金融ベンチャーにおける「デバイストラスト」実例と奇跡 ”



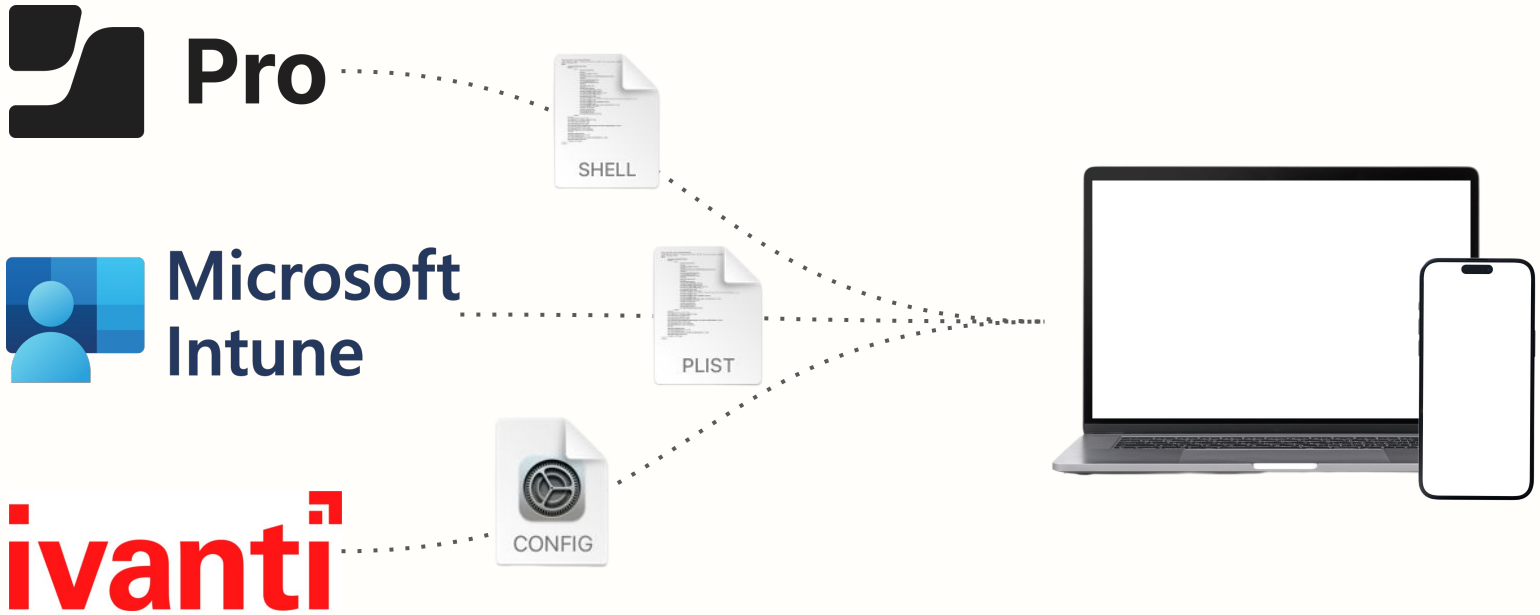
本題に入る前に・・・

Kyash 渡辺様によるHALL Cでの講演 “Jamf Connect ZTNAとMDMで実現! 金融ベンチャーにおける「デバイストラスト」実例と奇跡 ”



みなさんはMDMでデバイス管理をしていますか？

MDMはデバイスをコントロールできる



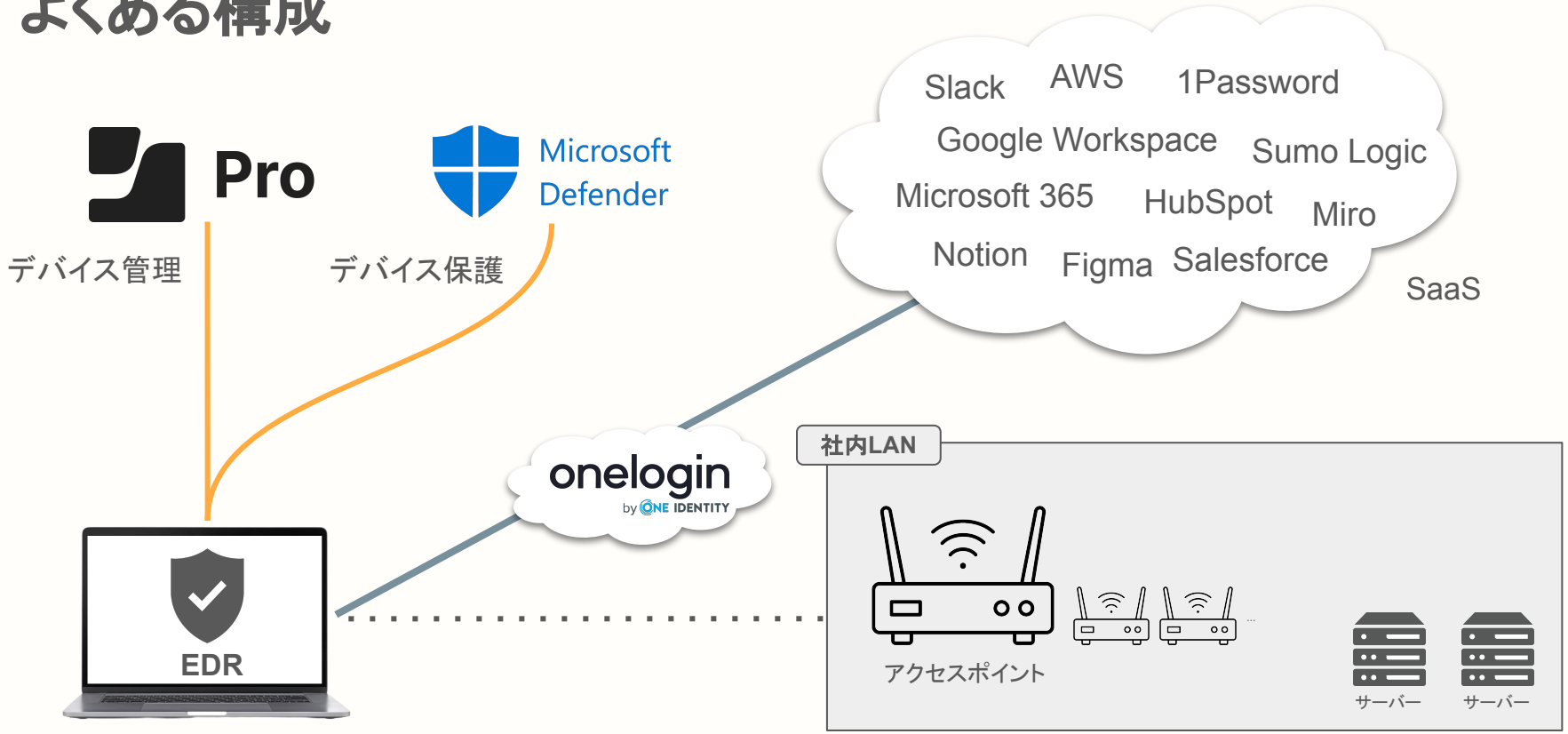
他にもWorkspace ONE UEM など...

※Jamf Pro、Microsoft Intune、ivanti は各社の商標です

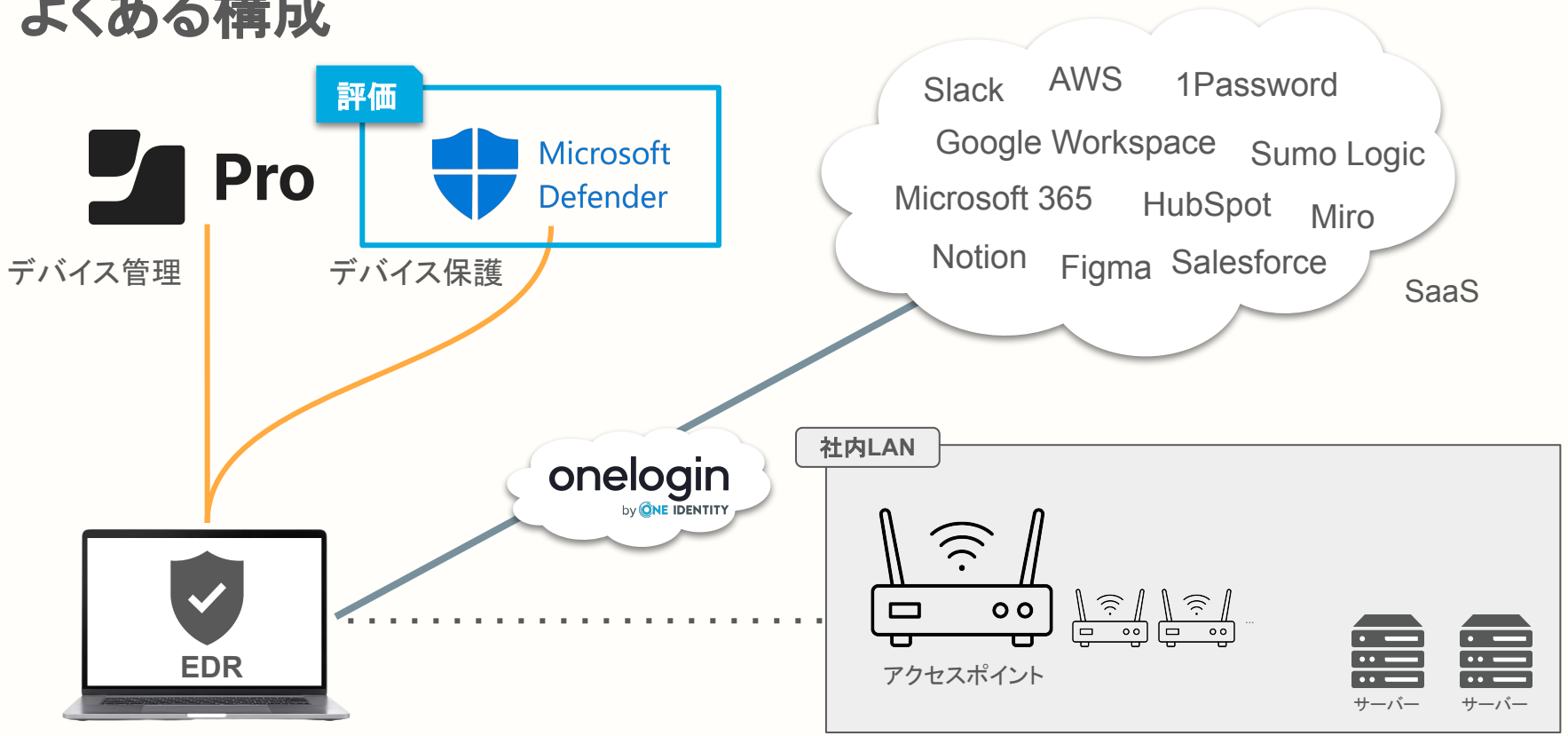
ところで、MDMに登録されていれば
デバイスは安全なのでしょうか❓

よくある構成を見てましょう👉

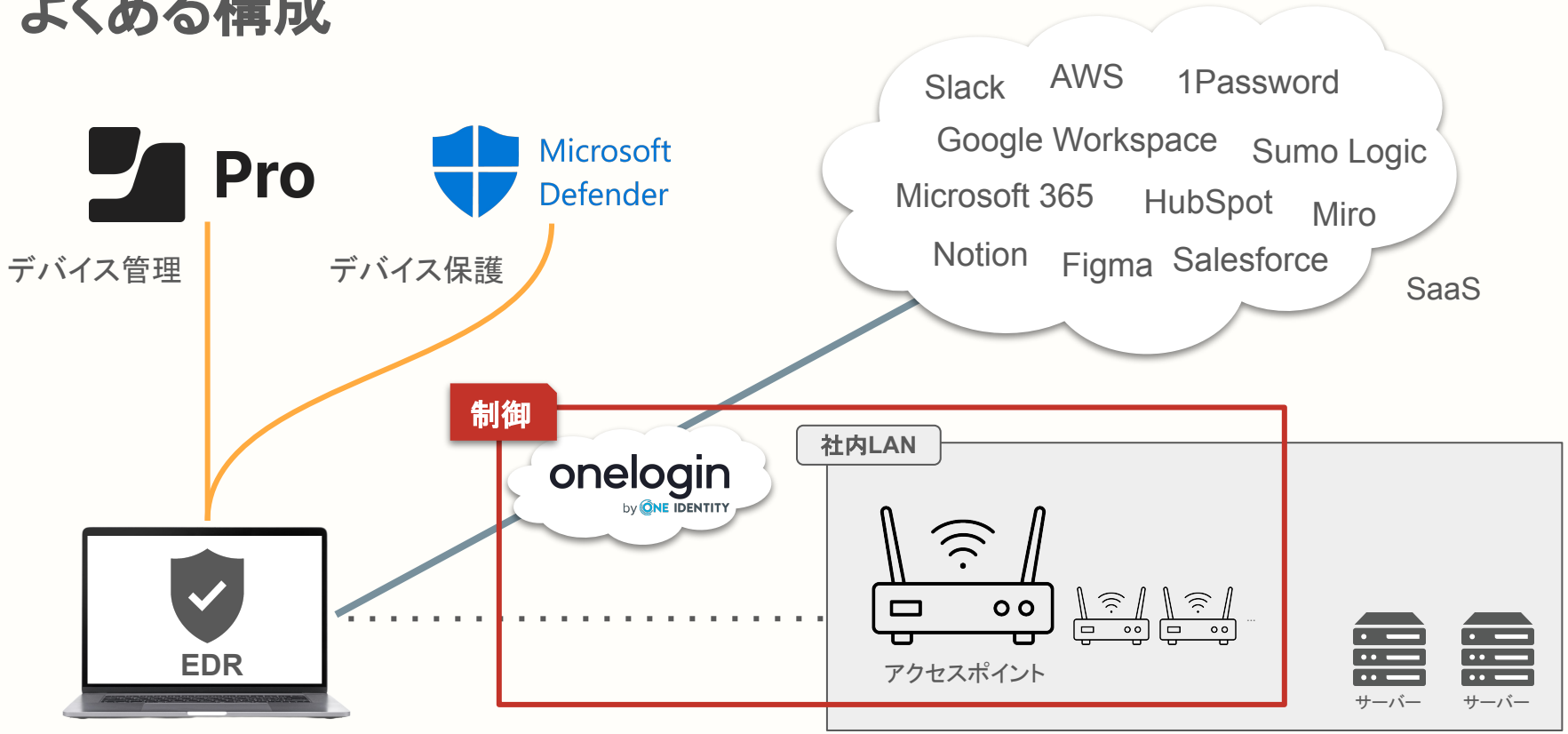
よくある構成



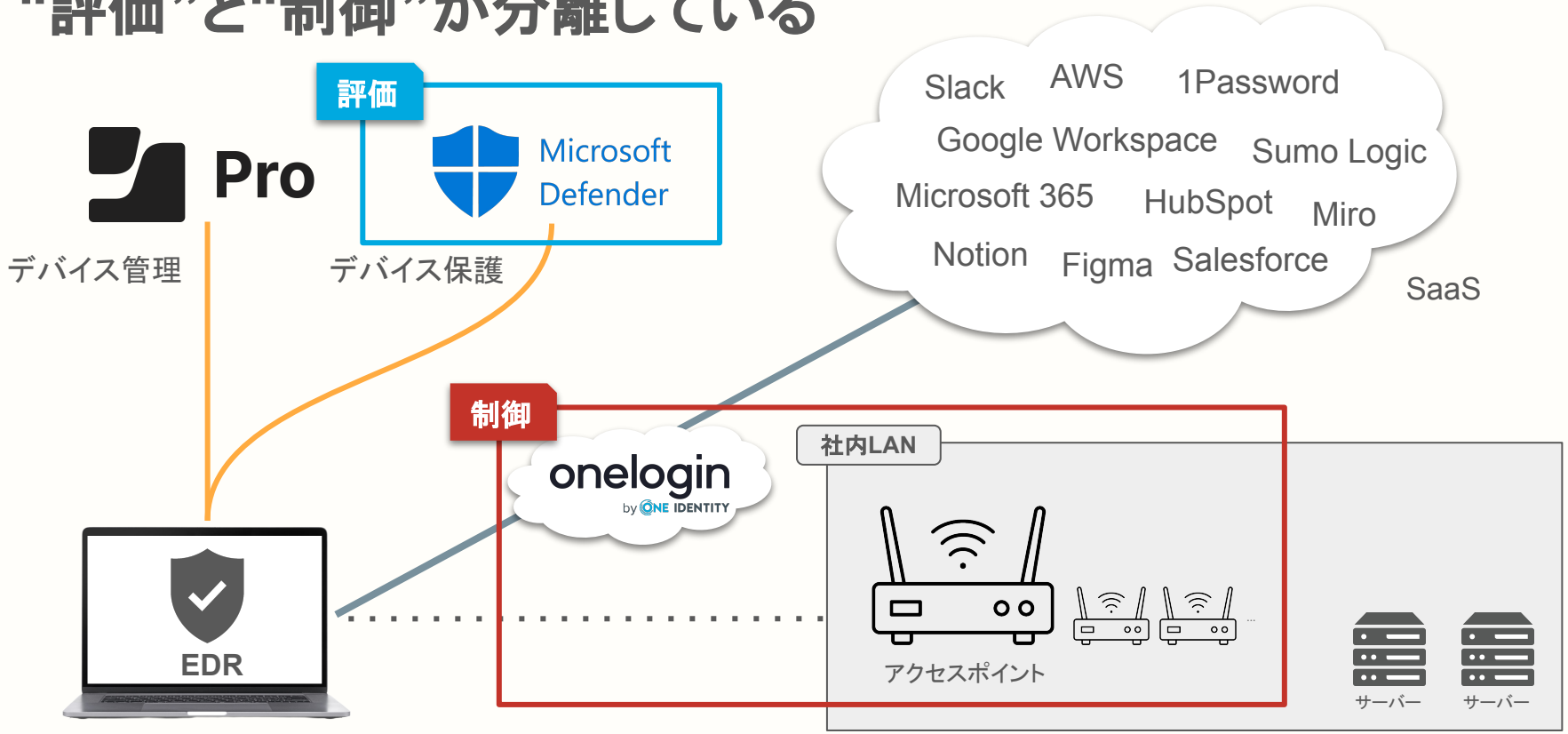
よくある構成



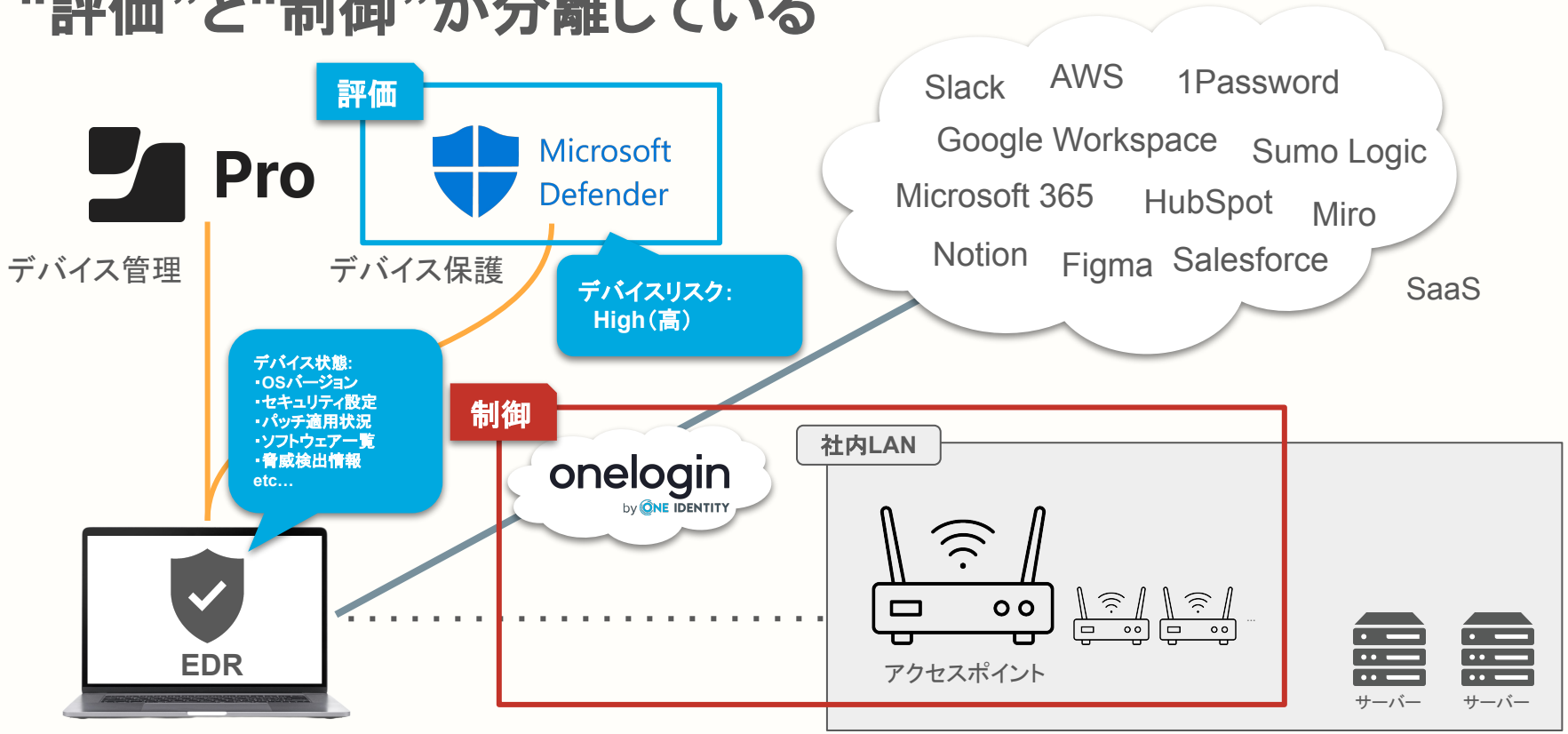
よくある構成



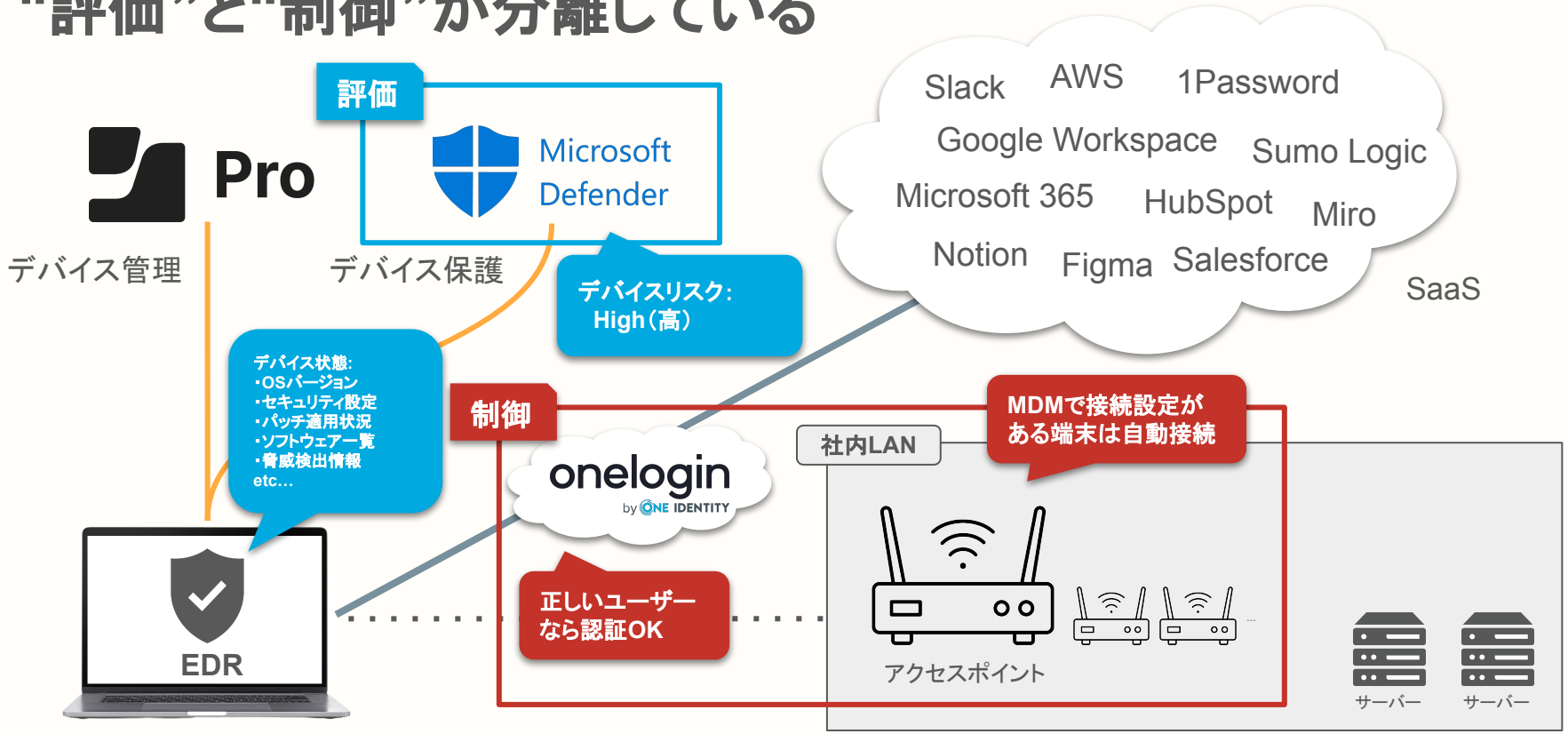
“評価”と“制御”が分離している



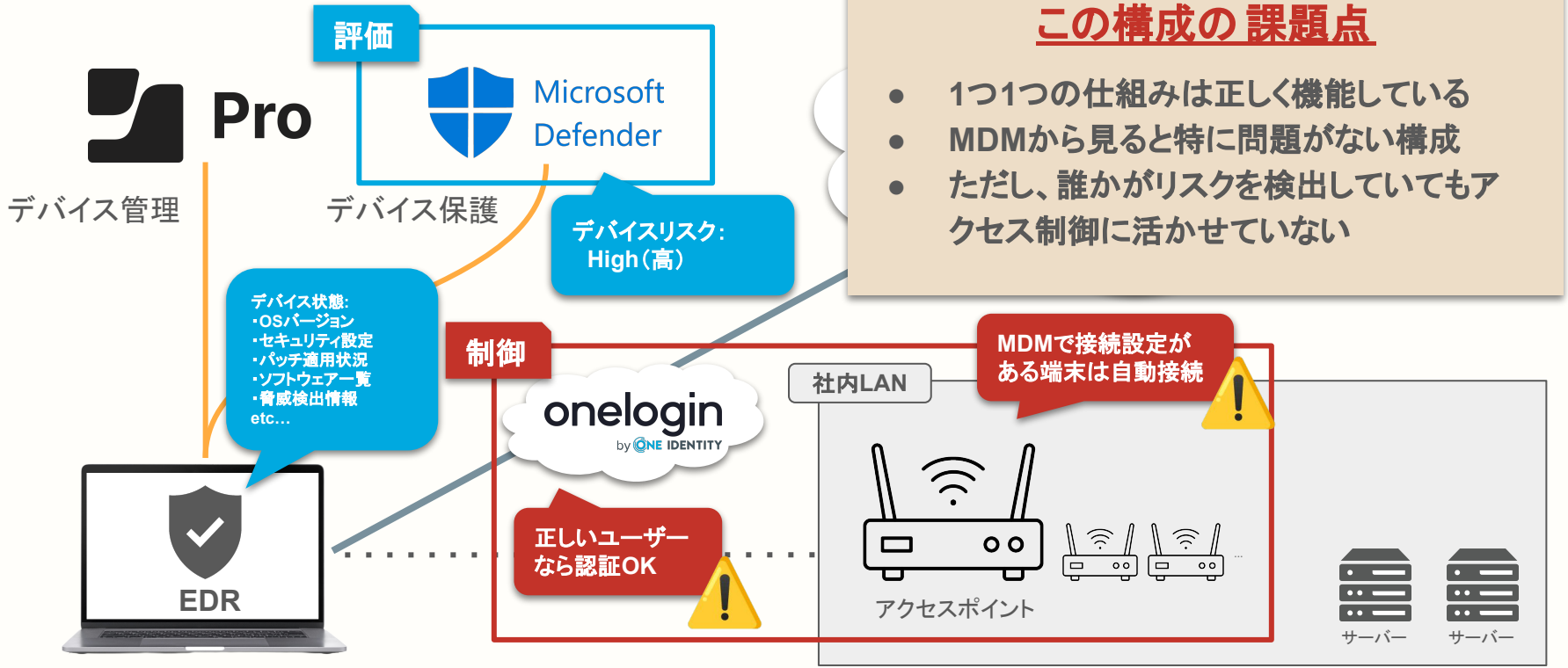
“評価”と“制御”が分離している



“評価”と“制御”が分離している



“評価”と“制御”が分離している



この構成の課題点

- 1つ1つの仕組みは正しく機能している
- MDMから見ると特に問題がない構成
- ただし、誰かがリスクを検出していてもアクセス制御に活かせていない

評価と制御が“分離”しているとリスクを止められない

顕在化していないリスク

- 脆弱なOSバージョンを継続利用している
- 重大な脆弱性を含むアプリケーションが放置されている
- MDMで配信されたAV/EDRが無効化・未稼働状態にある
- マルウェアに感染後の自動検疫結果・状態が分からない
- 不正な認証局が信頼されている
- 不審な構成プロファイルがインストールされている
- 有効なアクセス権をもった従業員のデバイスではない

評価と制御が“分離”しているとリスクを止められない

顕在化していないリスク

- 脆弱なOSバージョンを継続利用している
- 重大な脆弱性を含む
- [illegible]状態が分からない
- [illegible]が信頼されている
- 不審な構成プロファイルがインストールされている
- 有効なアクセス権をもった従業員のデバイスではない

“今、この瞬間の状態”に応じて“止める”仕組みが、どこにもないんです。

では、“止める”ならどこが正解❓

では、“止める”ならどこが正解 ❓

EDR は「深刻な脅威」には反応できるが、**「信頼できない状態」では遮断しない**

MDM は「端末の状態」は収集できるが、**「直接的なアクセス制御」はできない**

IDaaS は「ユーザー」は信頼しても、**「デバイスの実態」を詳細には見れない**

では、“止める”ならどこが正解 ❓

EDR は「深刻な脅威」には反応できるが、**「信頼できない状態」では遮断しない**

MDM は「端末の状態」は収集できるが、**「直接的なアクセス制御」はできない**

IDaaS は「ユーザー」は信頼しても、**「デバイスの実態」を詳細には見れない**

👉 **“つながる前” の入口に信頼の判定を組み込むべき**

“つながる前”のアクセス制御を実現する 2つのレイヤー

Connect

secure W2

クラウドに “アクセスする前” に止める

- デバイスのリスクをリアルタイムに評価
- ZTNAポリシーによる細やかなアクセス制御
- SaaSやVPNなどへの論理層のブロック

ネットワークに “つながる前” に止める

- 802.1X認証(EAP-TLS)によるデバイス認証
- デバイスリスクレベルによるアクセス制御
- 有線 / 無線ネットワークの物理層を遮断

pentio

“評価”と“制御”の連携を実現する 2つの製品

デバイスの健全性を評価する 機能を持ったZTNA「Jamf Connect」と、
その 評価結果をもとに “即座にアクセス制御” できるのがAPP「SecureW2」

APP = Adaptive Passwordless Platform

Connect × secure W2

👉 この2つがゼロトラストを “現実にする”

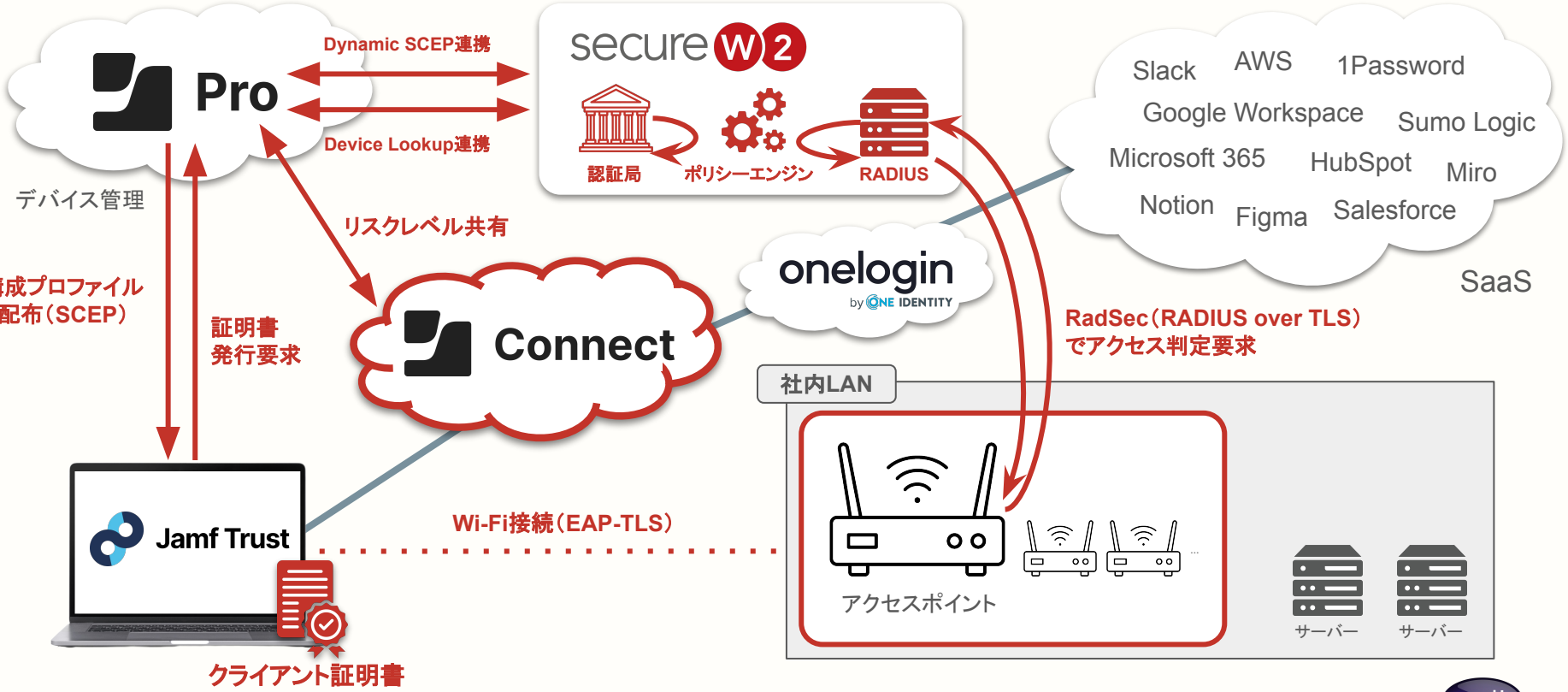
顕在化していないリスク

- 脆弱なOSバージョンを継続利用している
- 重大な脆弱性を含む
- 状態が分からない
- 信頼されている
- 不審な構成プロファイルがインストールされている
- 有効なアクセス権をもった従業員のデバイスではない

SecureW2 with Jamf Connect ZTNA で クラウドもネットワークも課題解決！

SecureW2 × Jamf Connect ZTNA
構成イメージ

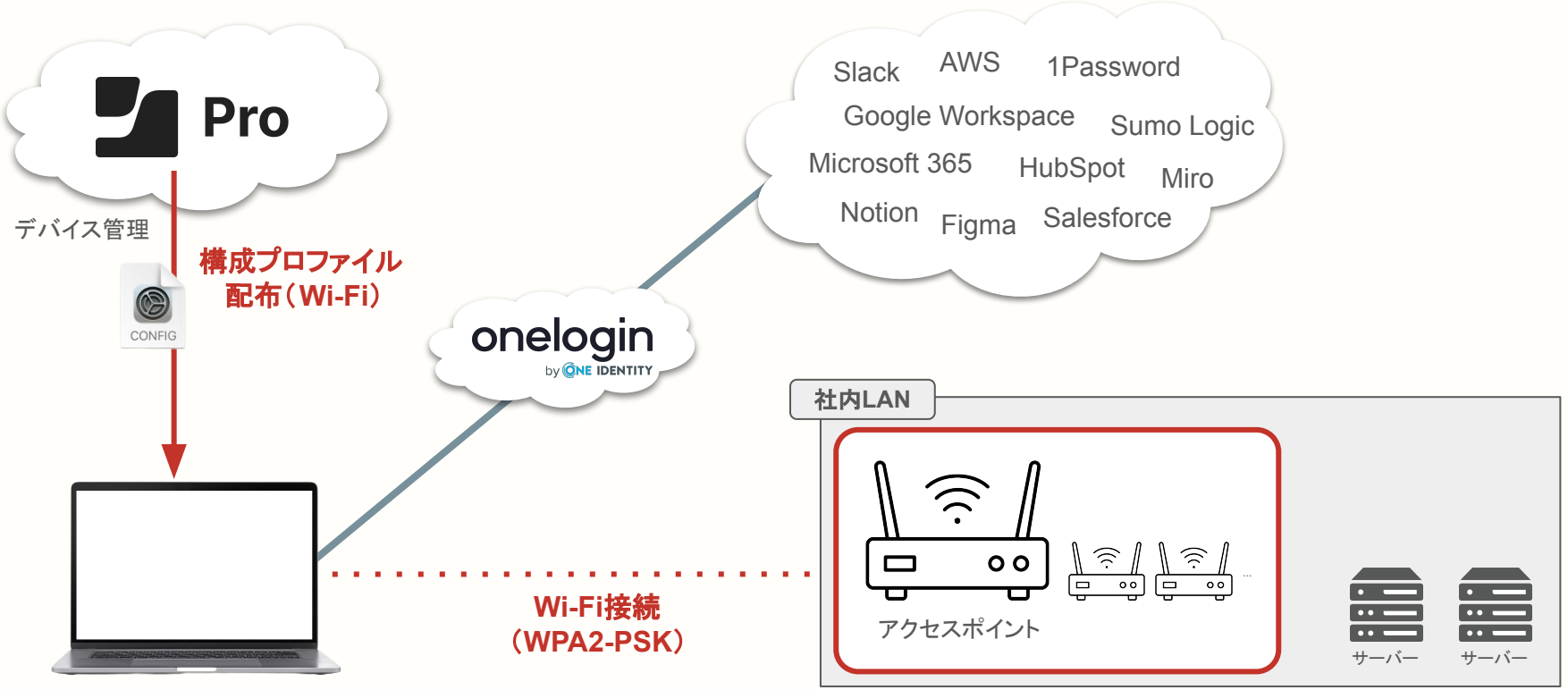
✅ SecureW2 × Jamf Connect ZTNA の構成例



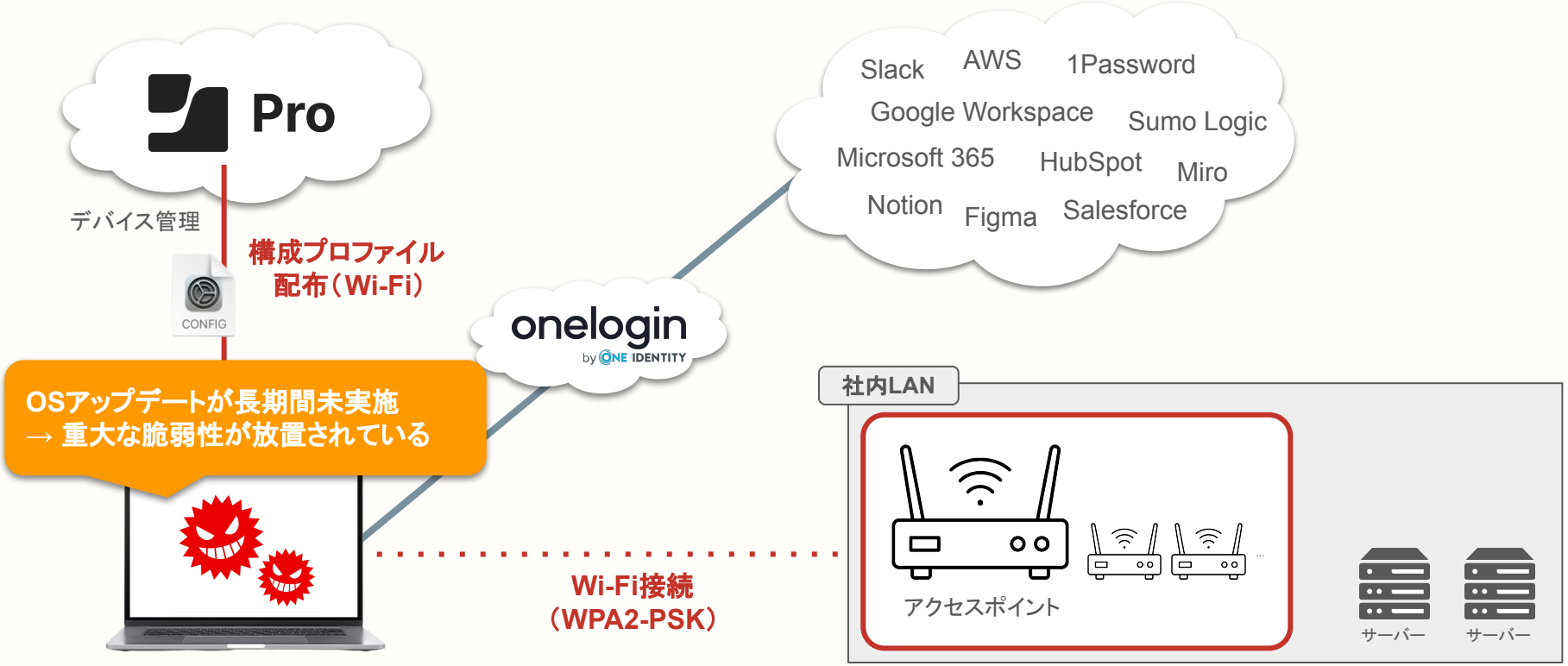
👉具体的なユースケースを見ていきましょう

Case1:
Wi-Fi 接続端末の即時遮断

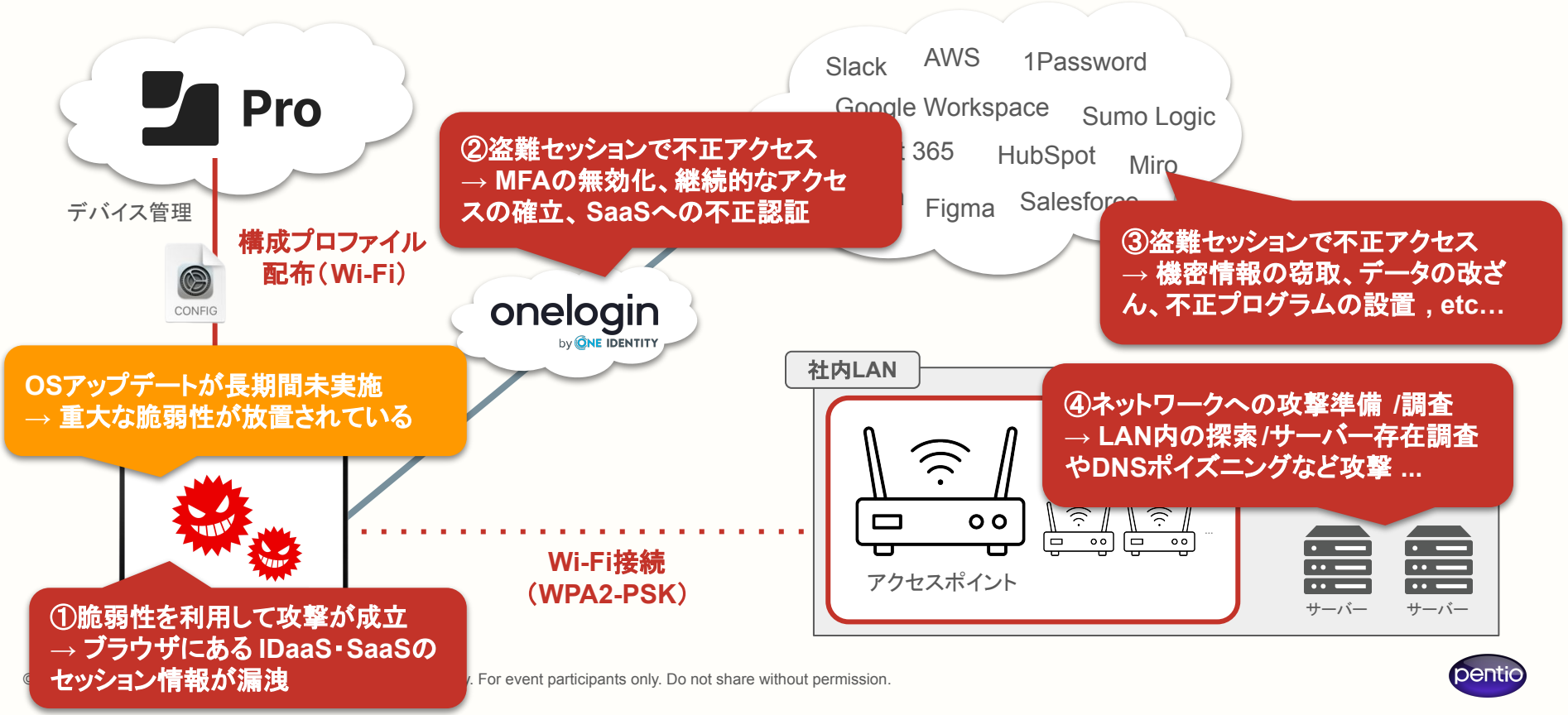
よくあるオフィスの無線 LAN接続



よくあるオフィスの無線 LAN接続【デバイスに問題あり】

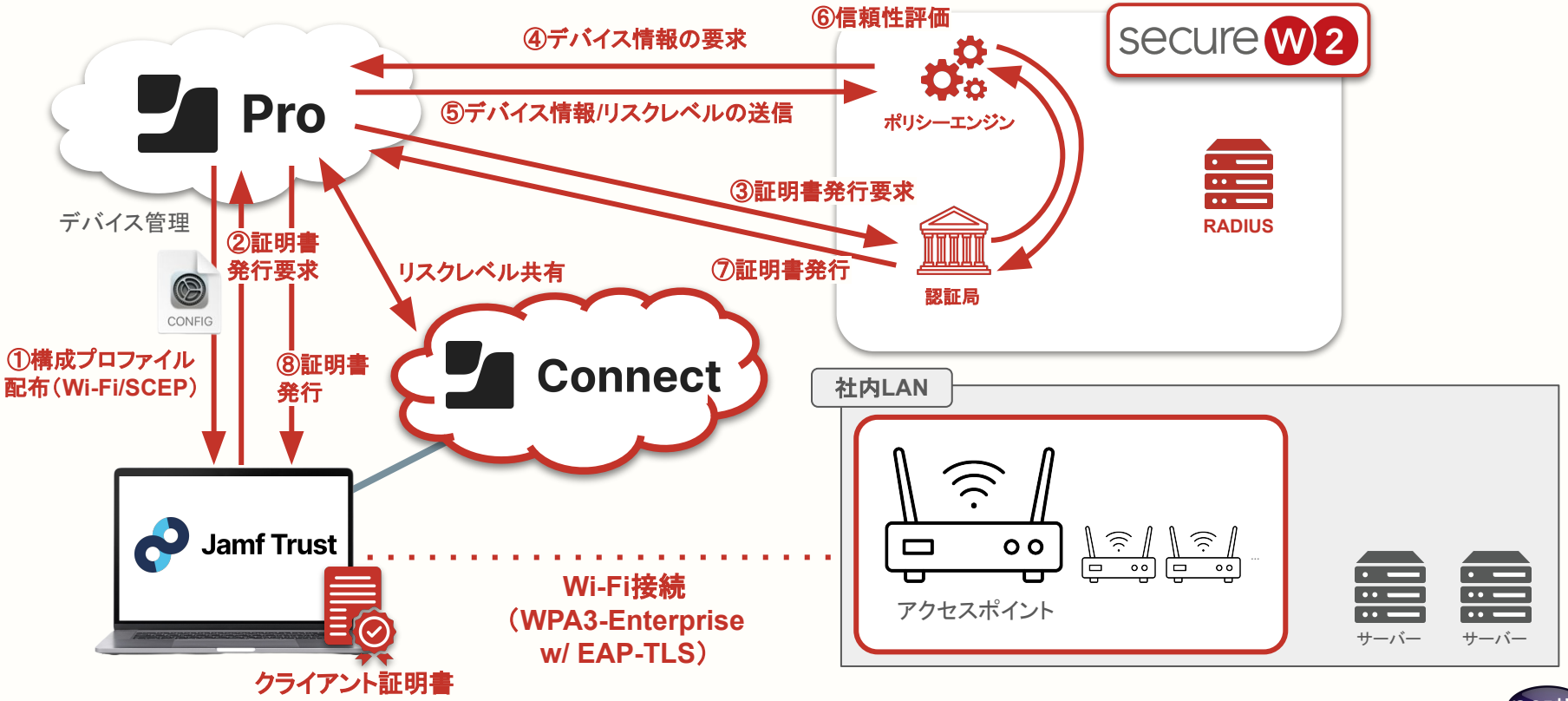


よくあるオフィスの無線 LAN接続【デバイスに問題あり】

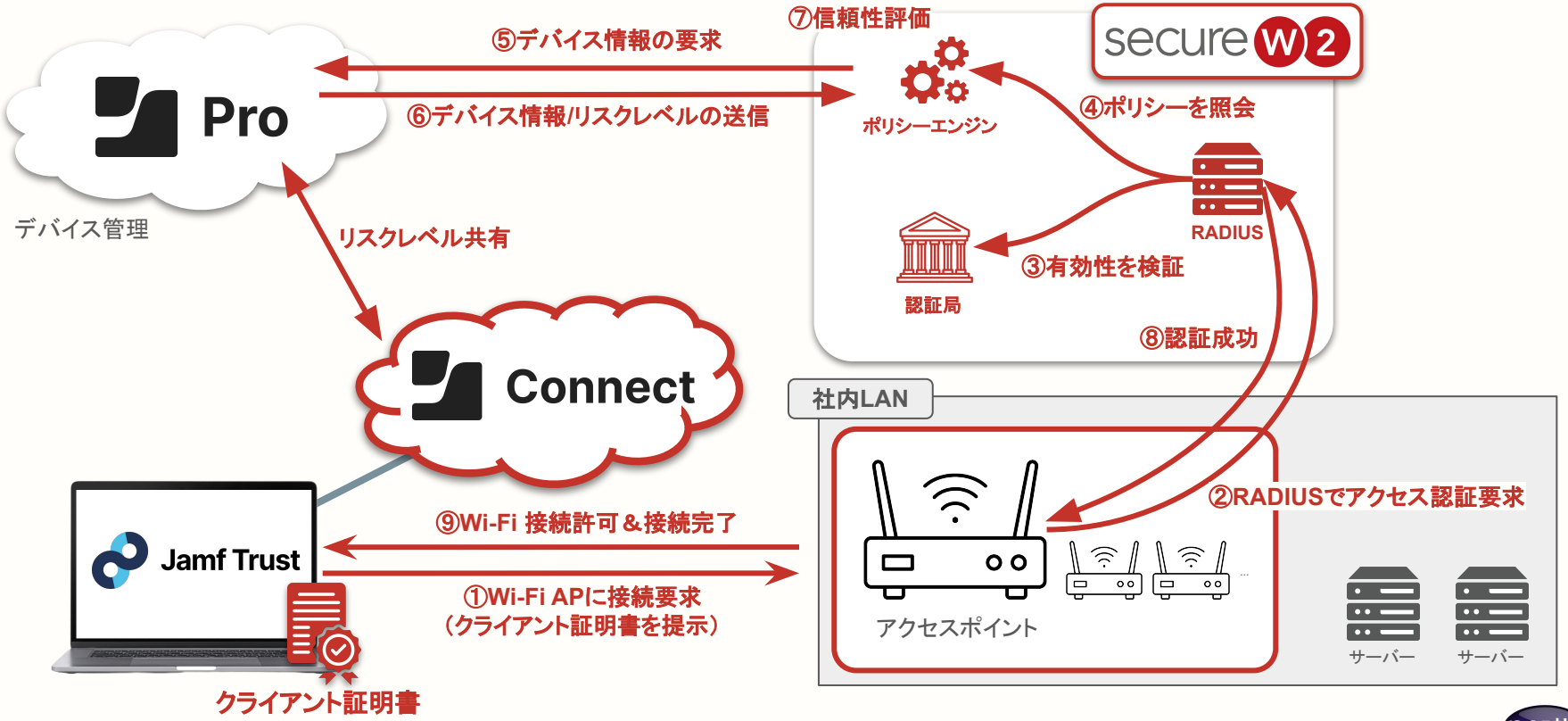


SecureW2とJamf Connect ZTNA を導入すると…

✅ 導入後の無線 LAN接続（クライアント証明書発行時）



✅ 導入後の無線 LAN接続（ネットワーク接続時）



では、実際の画面と動きを見てましょう
～ デモンストレーション ～

👨‍💻デモンストレーション①

- 通常時の無線 LAN接続
  → 接続成功

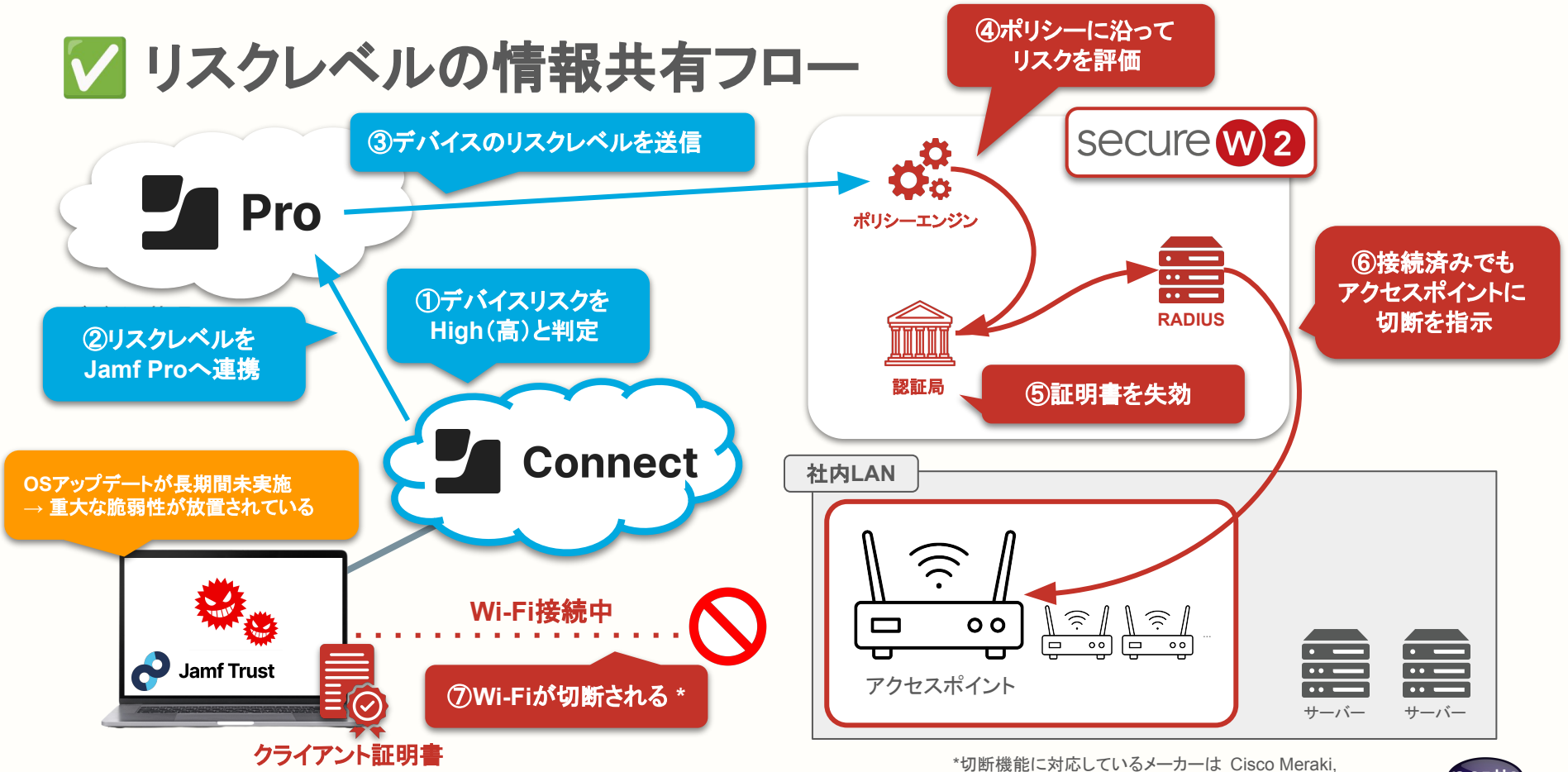
- 高いリスクが検出された場合の無線 LAN接続
  → 接続失敗

実は... 接続後でも無線LANの遮断、できます

接続後にデバイスのリスクが高くなると…

Case1: Wi-Fi 接続端末の即時遮断【シナリオ】

✅ リスクレベルの情報共有フロー



*切断機能に対応しているメーカーは Cisco Meraki, HPE Aruba, Juniper Mist, Ubiquiti Unifiのみです
*その他製品によりシステム要件があります

pentio

👨‍💻デモンストレーション②

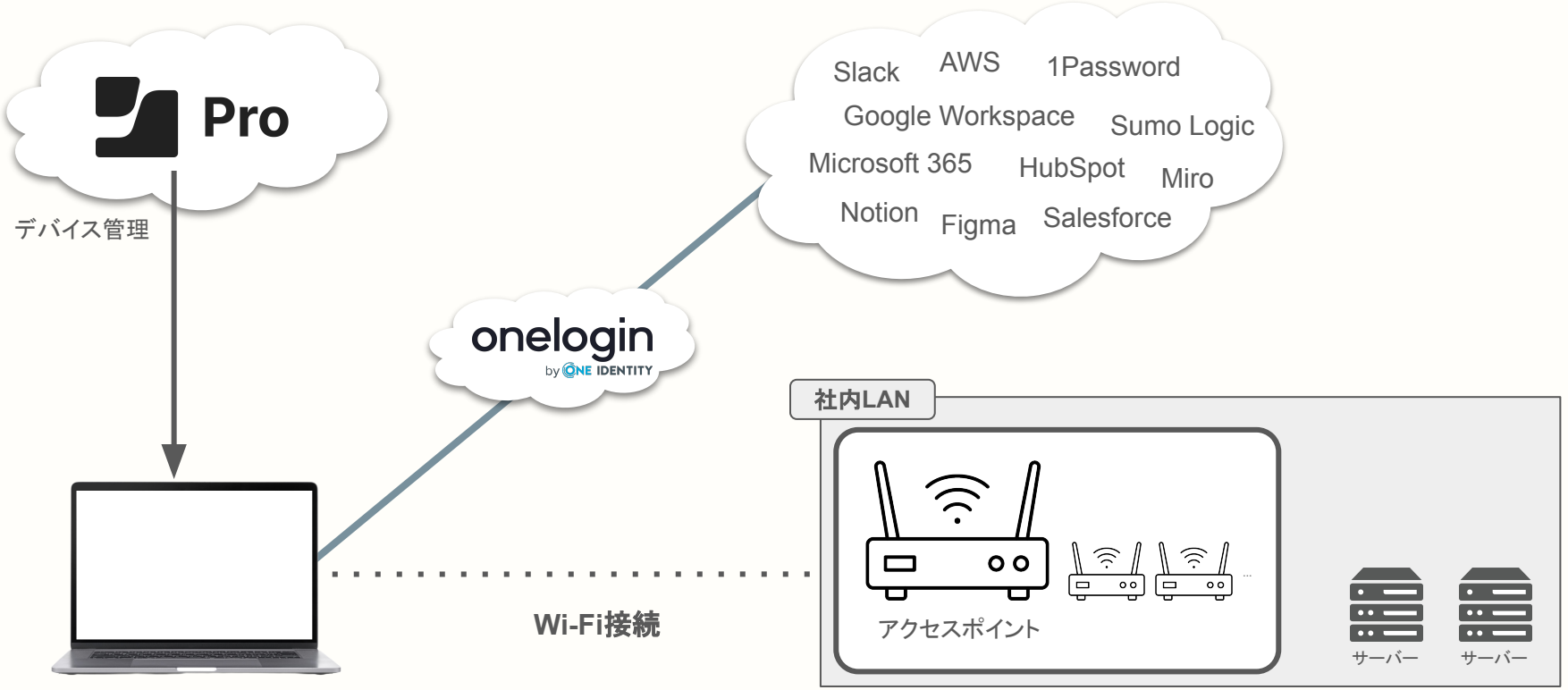
- 通常どおり無線 LANに接続中
- 接続中に高いリスクが検出される
- 証明書が失効＆無線 LANが繋がらなくなる
  → NW利用不可

📒 Case1のまとめ

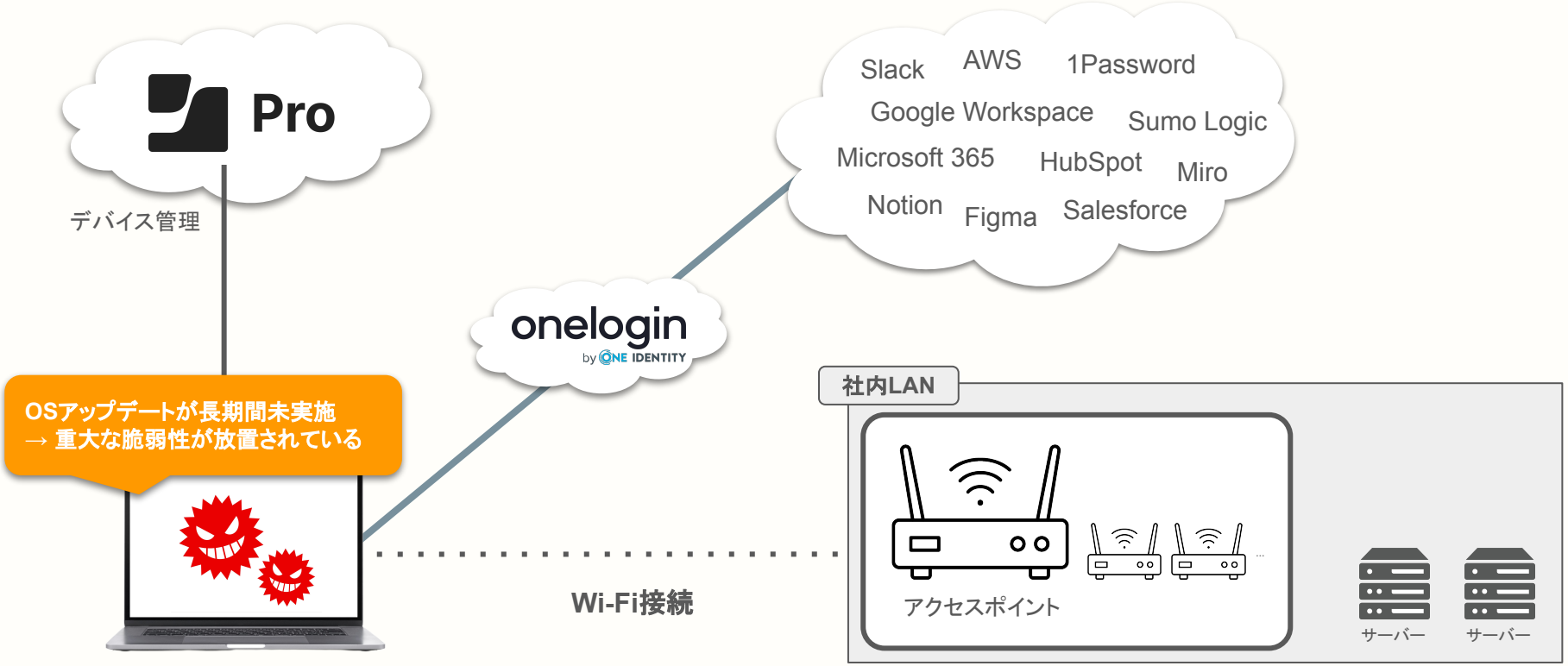
- Jamf Connect ZTNAはデバイスのリスクスコアリングを行う
- 無線LANに接続するときにパスワードではなくクライアント証明書を使う
- SecureW2のクラウドRADIUSは証明書の有効性だけではなく、Jamf Connect ZTNAが持つリスクレベル情報をJamf Proから取得して、ネットワークに接続させてよいかをコンテキストに基づき動的に判断する
- SecureW2のクラウドRADIUSは、接続中のデバイスでも切断を指示できる
- 再接続を防止するためSecureW2はクライアント証明書も失効できる

Case2:
SaaSへの接続制御

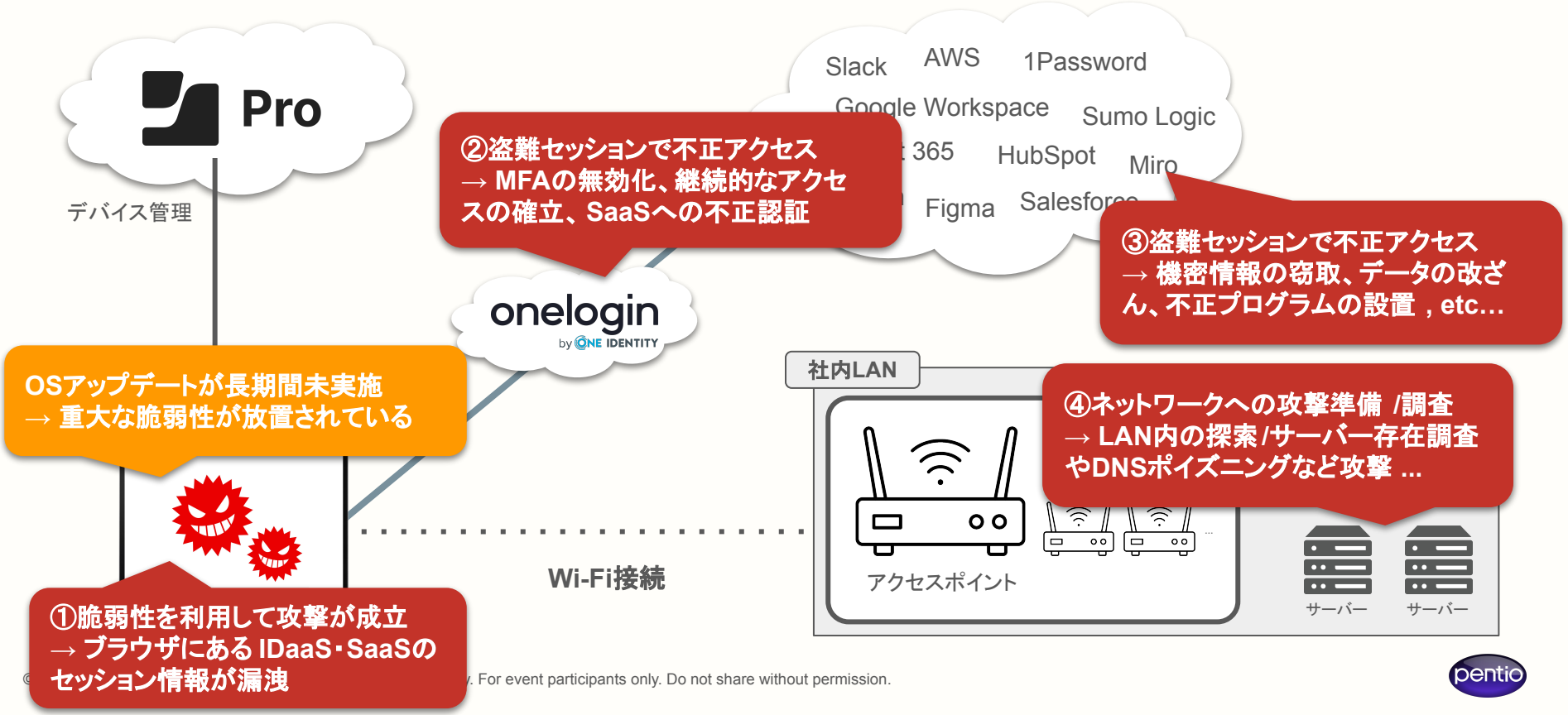
よくある業務でのクラウド利用



よくある業務でのクラウド利用【デバイスに問題あり】



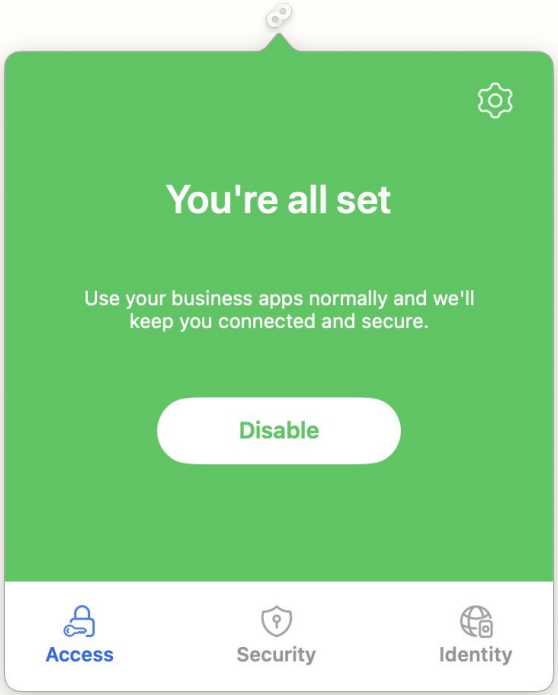
よくある業務でのクラウド利用【デバイスに問題あり】



pentio

SecureW2とJamf Connect ZTNA を導入すると…

✅ クラウドアクセスは Jamf Connect ZTNAで制御



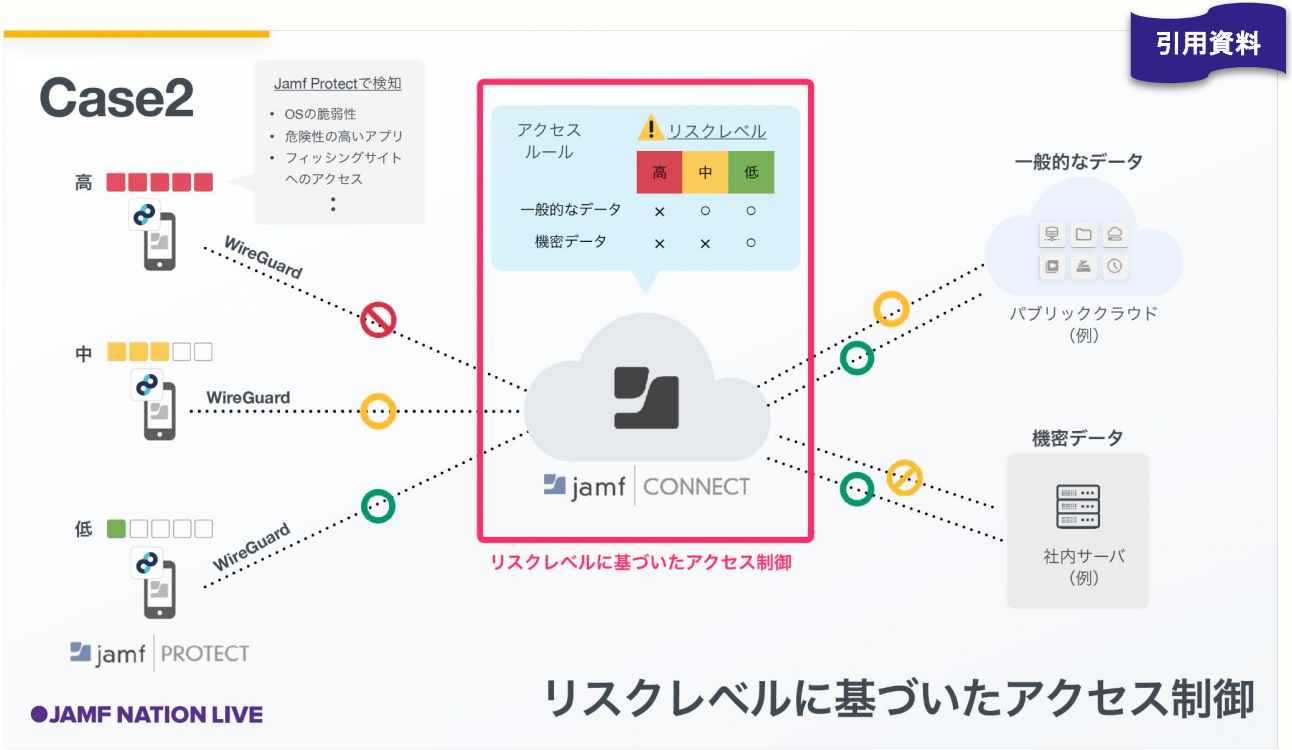
Connect

リスクレベル別にアクセスを許可するアプリケーションやサービス、ネットワークを制御

1. 機密性の高いデータへのアクセスは “安全” とされたデバイスにのみ制限
2. 一般的なデータへのアクセスは “低” リスクのデバイスからでも接続可能

pentio

✅ クラウドアクセスは Jamf Connect ZTNAで制御



リスクレベルに応じたクラウド、Jamfと接続したVPNサイトへのアクセス制御はSecureW2がなくても十分に制御可能です

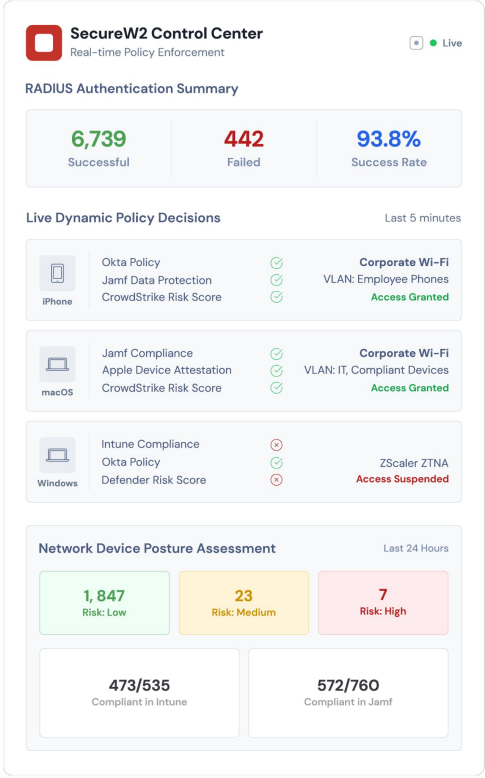
参考: JNL Tokyo 2024のJamf様講演資料から抜粋

✅ SecureW2がプラスアルファ貢献すること

証明書の有効性を Jamfで評価したデバイスのリスクレベルと連動させることができる

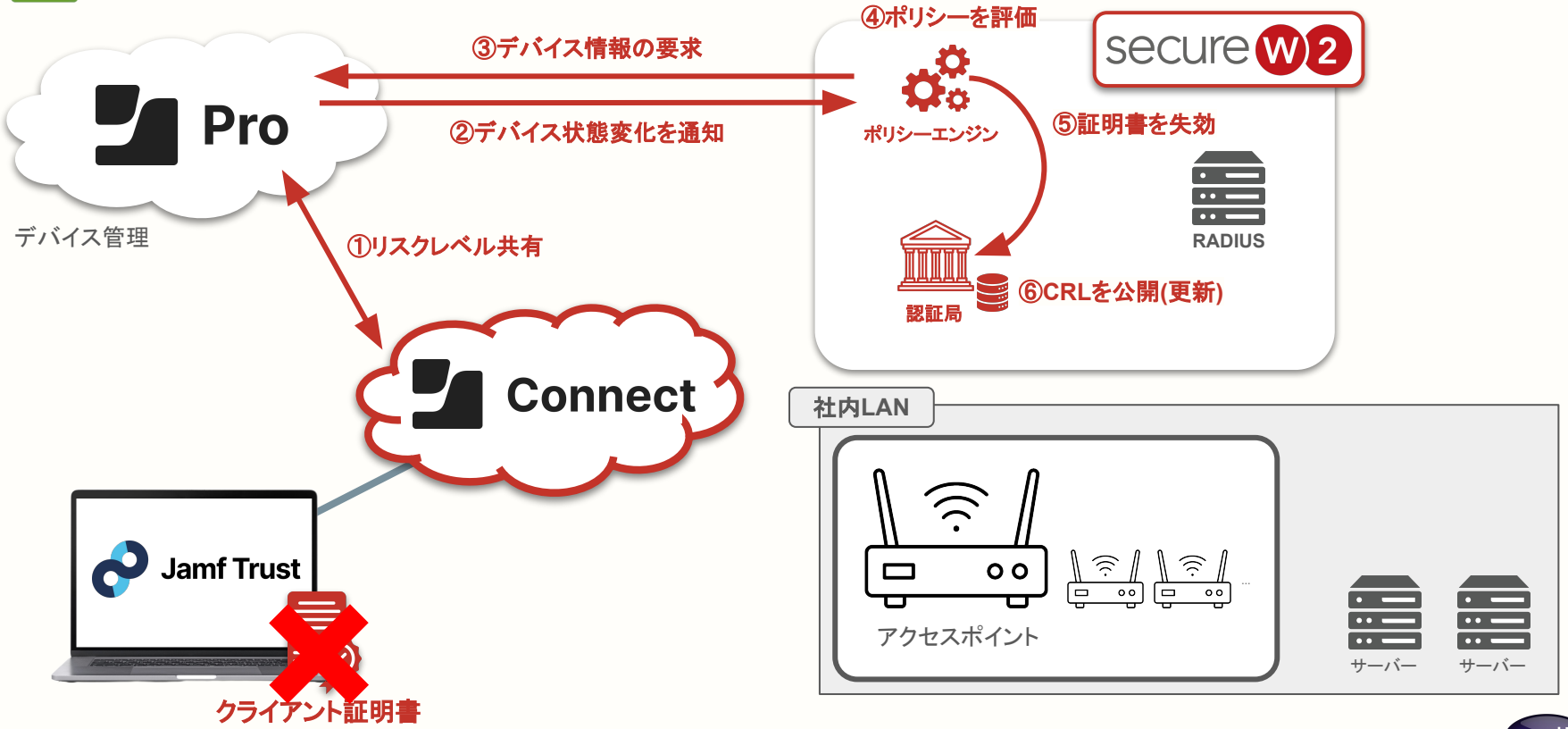
1. 従来のPKIでは「クライアント証明書がインストールされていて有効ならば OK」だった静的なデバイストラストをより動的なものにします

2. Jamf Connect ZTNA でカバー出来ない証明書認証が求められるアプリ、ネットワーク、 VPNにもカバー範囲を拡大出来ます



リスクレベルの情報共有フロー

✅ リスクレベルの情報共有フロー（証明書の自動失効）



📒 Case2のまとめ

- Jamf Connect ZTNAはデバイスのリスクスコアリングを行う
- クラウドサービスへのアクセス制御はJamf Connect ZTNAが単独で実現
- SecureW2はJamf Connect ZTNAが持つリスクレベルの変化に応じて、クライアント証明書を自動的に失効する
- クライアント証明書を用いてアクセス制御を行うIDaaS（OneLogin／Okta／Entra ID）やリモートアクセスVPNにも動的なアクセス制御を持ち込める

まとめ

ここまでのまとめ

導入前

- デバイスの基本的な管理・保護は出来ている
- MDM・EDR・IDaaS をそれぞれ導入して個別の運用はできている
- “問題が発生したあと” の対処の準備は出来ているが、“問題が発生する前の高いリスク” に対処出来ていない

✅ SecureW2 × Jamf 導入後

- デバイスの基本的な管理・保護に加えて、**管理状態の監視とリスクのスコアリングができる**ようになる
- MDM・EDR・IDaaS がそれぞれ持つ **情報を統合してデバイス・ユーザーの信頼性を常に確認できる** ようになる
- “問題が発生したあと ” の対処だけでなく、**“問題が発生する前の高いリスク ” にも事前に対処できる** ため、より安全な業務環境を構築・維持できる

secureW2 の簡単なご紹介

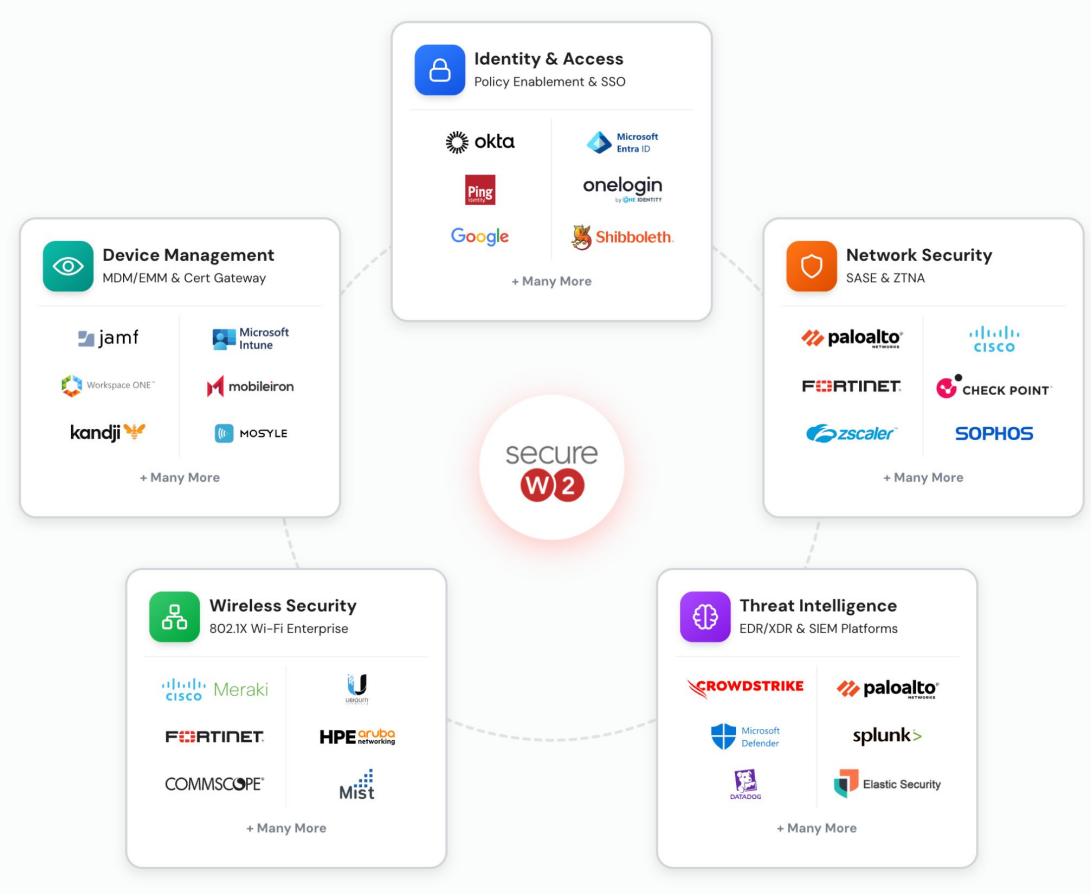
SecureW2 とは？

The Adaptive Passwordless Platform That Continuously Enforces Trust

継続的に信頼を強制する、パスワードレス対応の適応型プラットフォーム

Wi-Fi、SSO、アプリケーション、DevOps、IoT、スマートカード、AIエージェントなどへのアクセスを証明書で制御し、**侵害を防止し、セキュリティ運用を自動化します。**

追加のインフラ不要で、クラウドネイティブな信頼レイヤーを通じて、動的な　PKIとRADIUSを導入できます。



SecureW2 メーカーHPから引用（引用元 : https://www.securew2.com/）

SecureW2 とは？

クラウドマネージド PKI

クラウドRADIUS

適応型ポリシーエンジン

- パスワードレスな証明書認証（PEAP→EAP-TLS への移行）
- 導入コストはオンプレPKIの1/3 程度（UIベース／API駆動）
- 主要IDaaS（OneLogin／Okta／Entra ID）とリアルタイム連携可能
- ゼロトラストの“つながせない”を自動化する Dynamic PKI 体制

SecureW2 が実現できること

クラウドマネージド PKI

SecureW2が提供するマネージドPKIでは、**クラウド上ですべての認証局・証明書管理が完結** します。例えば、SecureW2はお客様組織がもともと保有するプライベートCAを取り込み、今後の証明書発行・管理をすべてクラウド化することも可能です。

また、これから新たにPKI基盤を活用するお客様では、**複数のルート認証局・中間認証局を無制限で作成**、運用することができ、特定の用途に制限されない認証設計を支援します。また、SevureW2以外の証明書発行基盤との連携もでき、外部の中間認証局のCSRに署名を行うことで信頼のトラストチェーンを構築することができます。

証明書の失効もCRLを最短15分間隔でインターネットに公開 することで、LANの中に限らず多くのシステムで有効性確認を実現し、リソースの安全性に寄与します。

SecureW2 が実現できること

クラウドRADIUS

SecureW2が提供するクラウドRADIUSでは、従来のように**拠点へのアプライアンス設置、固定 IPアドレスの取得は一切不要**です。RADIUSを利用するWi-Fiのコントローラやネットワークスイッチは、常にクラウドにあるSecureW2のRADIUSエンドポイントと通信します。

これにより複数の拠点がある組織では、**拠点単位でのRADIUSサーバーの構築やSD-WANの設定・維持が不要**となり、ネットワーク設計が非常にシンプルとなります。また、工場や生産ラインなどネットワークの安全性が求められる場面においても、SecureW2はRADIUSエンドポイントを固定IPアドレス、お客様ごとのポート番号でご用意しており、コントローラとSecureW2間の限定的なネットワークアクセスだけで、認証をご利用頂けます。

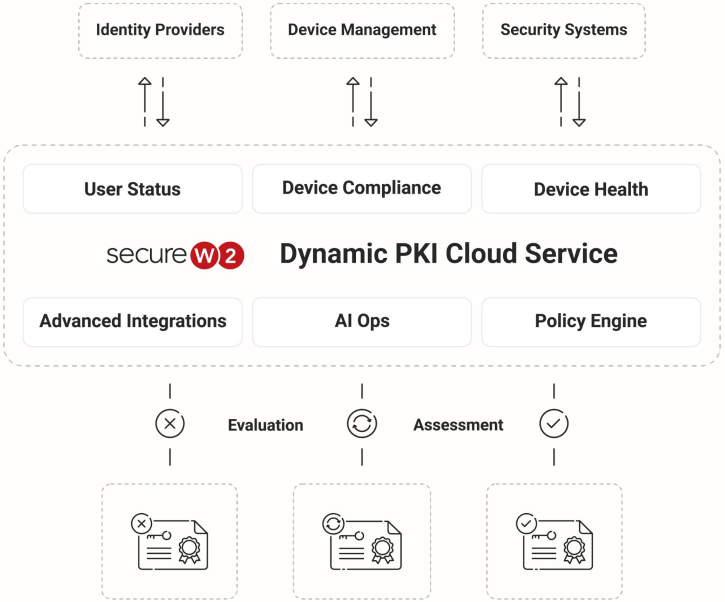
他にも**RADIUSの通信をTLSで暗号化する最新のRadSecに準拠**しており、Cisco Meraki、Juniper MistやHPE ArubaなどRadSec対応機器とは通信経路上も暗号通信を実現します。

SecureW2 が実現できること

適応型ポリシーエンジン

SecureW2が提供する適応型ポリシーエンジンでは、**IdP（IDaas）・MDM・EDR/XDRなどと連携** することで、**ユーザーのステータス・デバイスのコンプライアンス準拠状態・デバイスの健全性を常に検証** し、クライアント証明書の有効性またはRADIUS応答をコントロールします。

IdPでユーザーアカウントが停止したり、MDMでデバイスが非準拠になったり、EDR/XDRでデバイスの信頼性が失われた場合には、**証明書の失効によるアクセス権の剥奪やネットワーク接続の即時遮断にも対応** します。



ペンティオ株式会社について

About us

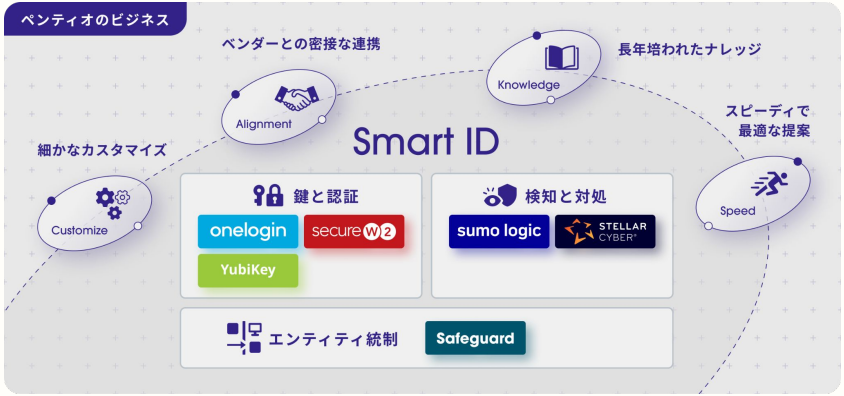
ペンティオ株式会社

pentio

コーポレートミッション

Smart ID

安全でストレスフリーな
セキュリティ設計



提供プロダクト

2025年現在の中心的なプロダクトラインナップ

onelogin

secure W2

Yubikey 5

sumo logic

STELLAR CYBER®

Safeguard

pentio

提供プロダクト

🔐その他の事業

- PKIソリューション
  - スマートカードログオン
  - USBトークン＆ICカード（J-LIS認定）※現在は保守サポートのみ
- タイムサーバー
  - 電波調査・設置工事・保守
- Web受託開発
  - ホームページ/ECサイト 等

🏛️2010年代以前の取り組み

- プライベート認証局アプライアンスの自社開発・サービス提供
- F5 / Juniper VPN製品とUSBトークンの一体提供
- 地方公共団体・警察・防衛省・日本銀行などにも提供

導入事例をウェブサイトで多数公開中

https://www.pentio.com/case/

毎月オンラインセミナーを開催中

👉 次回は8月22日(金)開催 ❗

https://www.pentio.com/events/

技術検証記事も多数公開しています！

https://www.pentio.com/securew2/support/document/

リンク集

導入事例

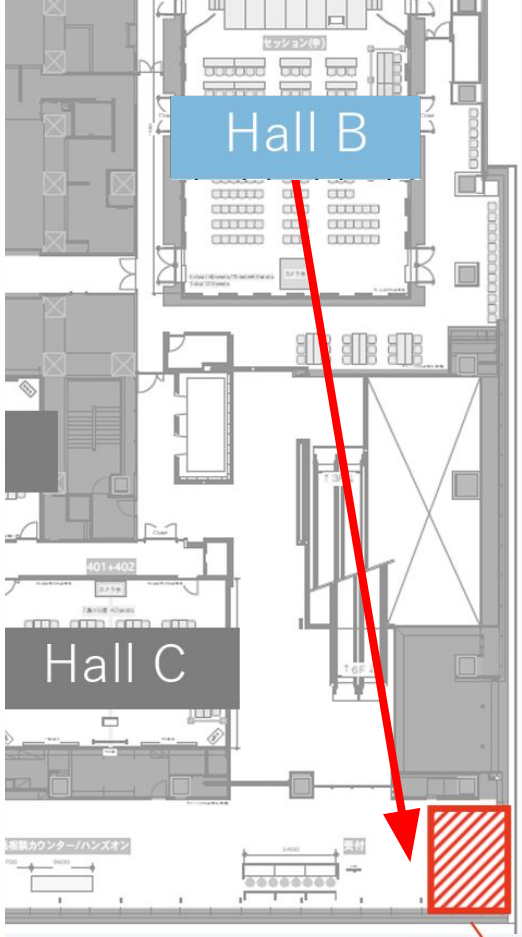
セミナー情報

技術検証レポート

本日はご清聴頂きありがとうございました！

私（おさだ）以外にも、
SecureW2担当エンジニア
がお待ちしています

Meet the Speaker でお話しましょう



Meet the Speaker
コーナー