

● JAMF NATION LIVE

Jamf for Mobileで実現する 安全性と運用効率を両立した モバイル管理



古賀 麻明利

セールス エンジニア

Jamf Japan 合同会社

Agenda

1 | Introduction

日本におけるモバイルデバイスのシェア
iPhoneが選ばれる理由

2 | Appleプラットフォームのセキュリティ

Appleの公開しているセキュリティガイド
ハードウェア・システム・アプリケーションについて

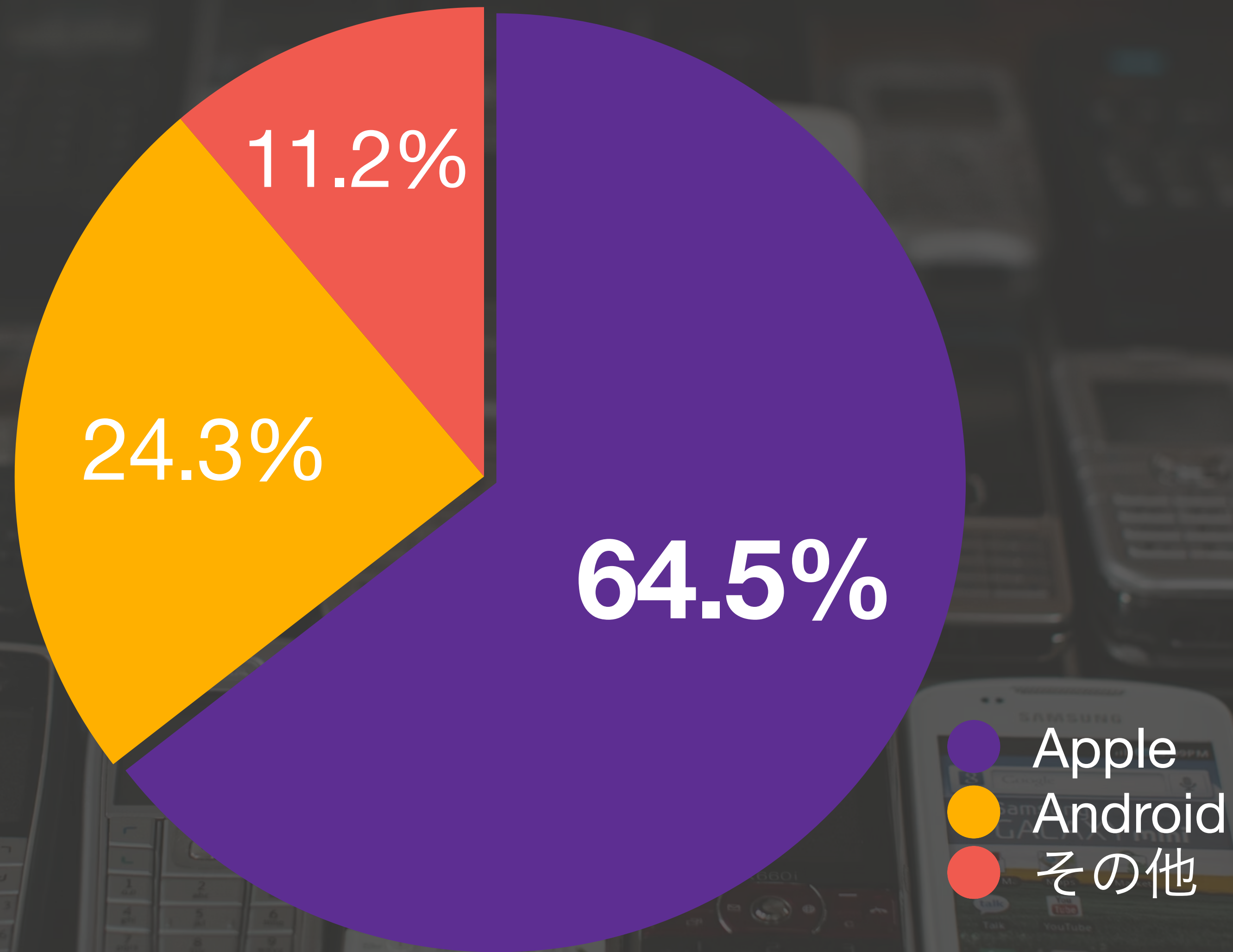
3 | Jamf for Mobile

Jamf for Mobile 機能紹介
安全性と運用効率を両立したモバイル管理とは



モバイルデバイスは
何を使っていますか？

日本におけるモバイルデバイスのシェア



iPhoneを選ぶ理由

私用でも使っている

安定的な供給

高いセキュリティ

直感的な操作性

耐久性

従業員の満足度向上

ナレッジが豊富

他Apple製品との連携のしやすさ

操作感の統一性

高品質なカメラ

企業ブランドイメージの向上

バッテリー持ちがいい

Face ID/Touch IDによる高い認証精度

安定した動作

デバイス紛失時の追跡

アクセサリの豊富さ

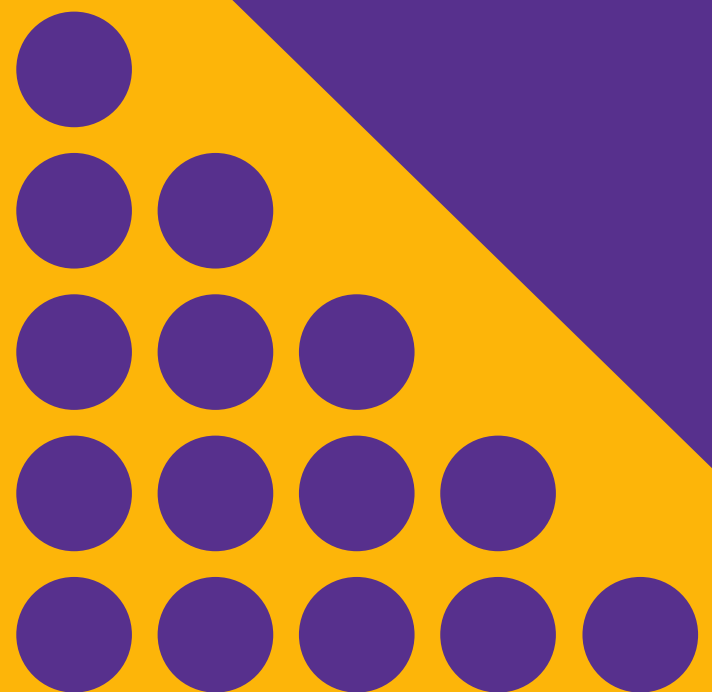
豊富なビジネスアプリ

サイズがちょうどいい

iPhoneを選ぶ理由

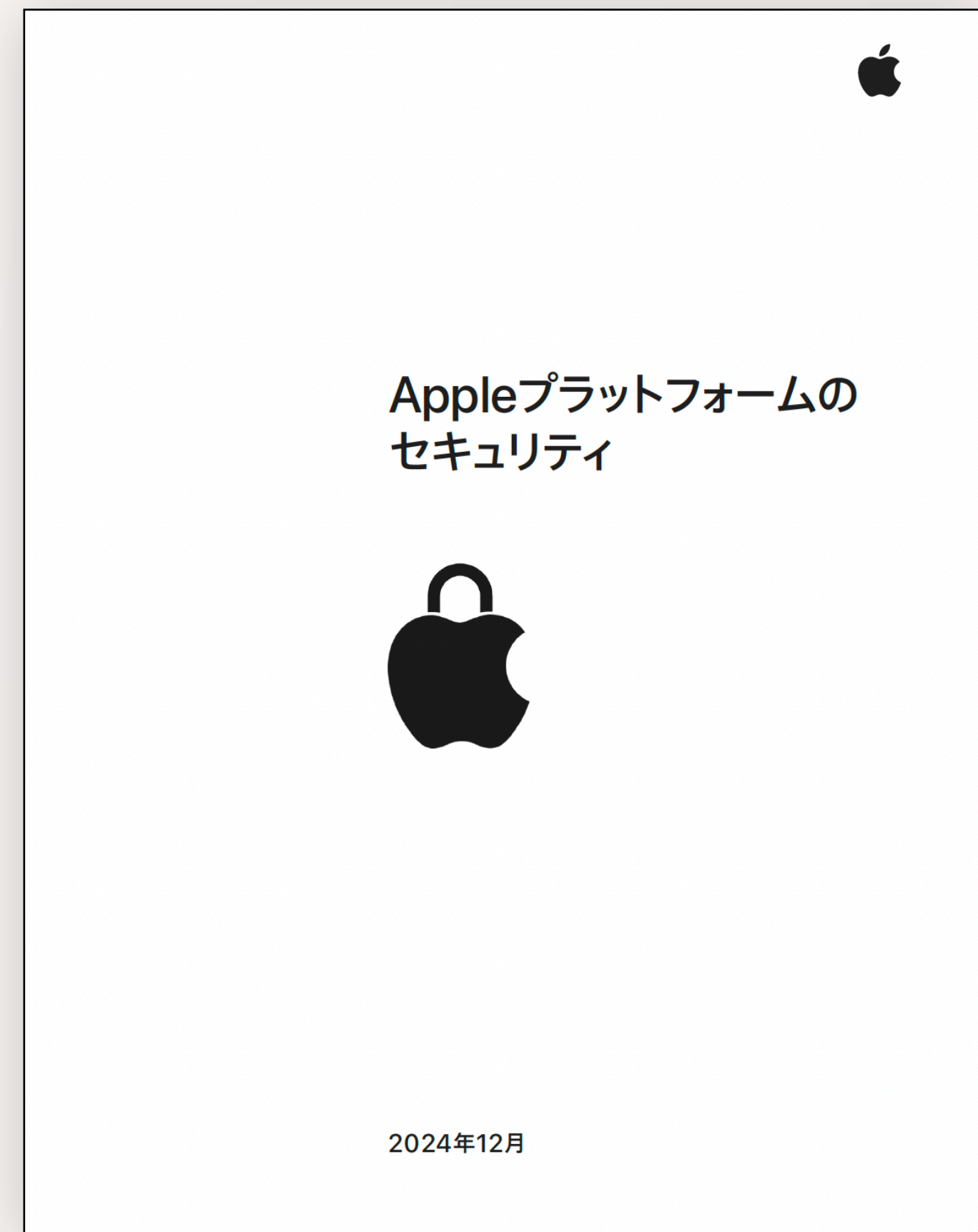
高いセキュリティ

Appleプラットフォームのセキュリティ



Appleプラットフォームのセキュリティ

- ▶ 2015年9月に初公開
- ▶ 最新版は2024年12月に改訂
 - ▶ 追加されたトピック
 - AppleデバイスでのWi-Fiプライバシー
 - 管理対象デバイス認証のセキュリティ など
 - ▶ 更新されたトピック
 - Apple SoCのセキュリティ
 - アクティベーションロックのセキュリティ
 - ワイヤレスネットワークに接続する際のセキュリティ機能 など

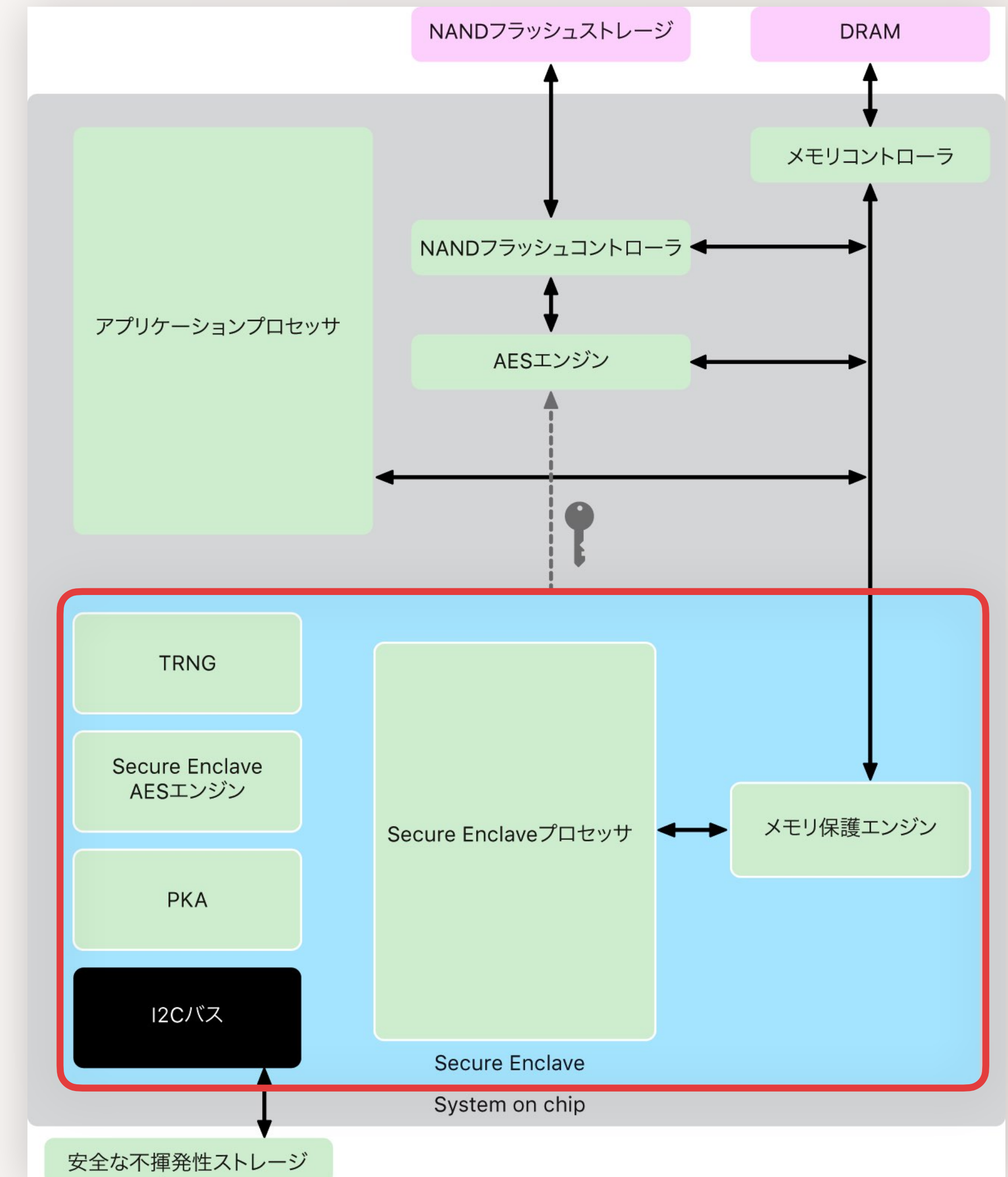


Appleプラットフォームのセキュリティ

1. ハードウェア セキュリティ

▶ Secure Enclave

- ▶ iPhone,iPad,Apple TV,Apple Watch, Apple Vision Pro,HomePodデバイスのすべての最新モデルに搭載
- ▶ Appleシリコン搭載Macおよび Apple T2セキュリティチップ搭載Macにも



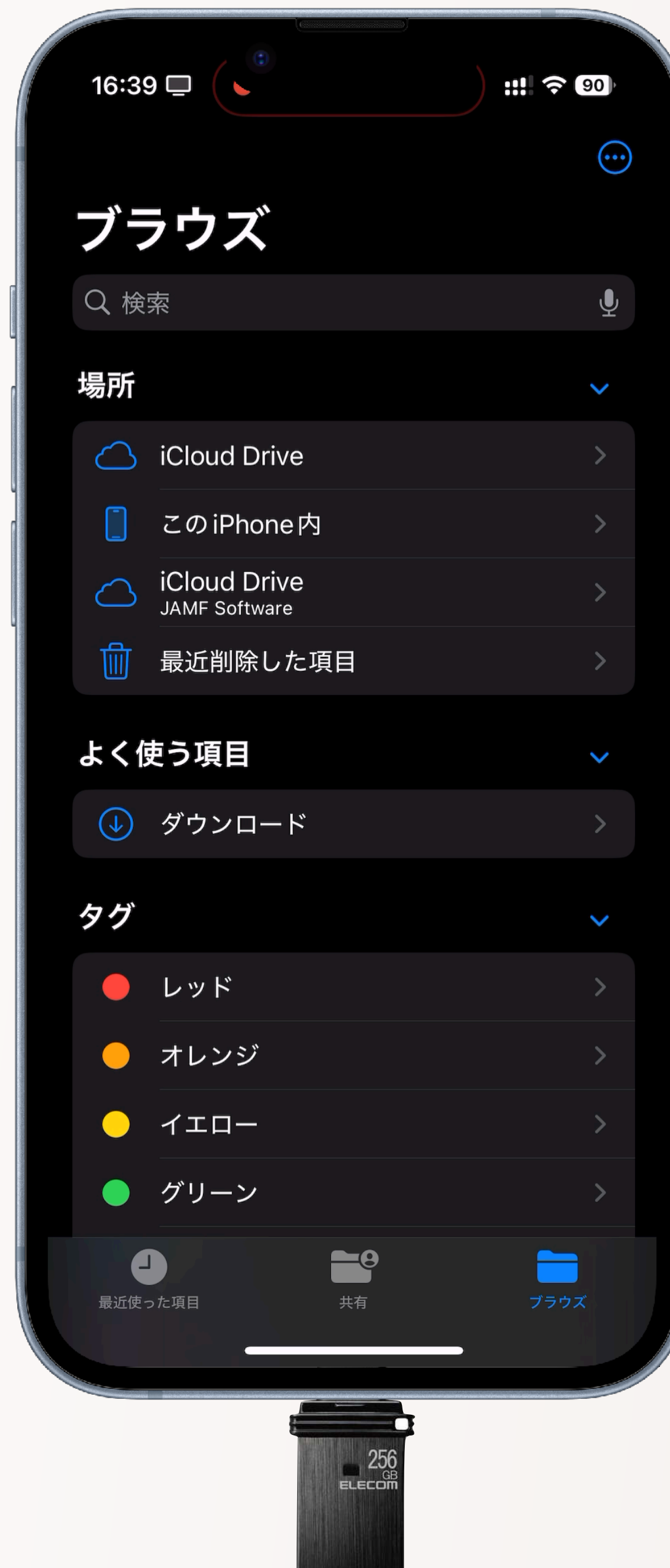
Appleプラットフォームのセキュリティ

1. ハードウェア セキュリティ

- ▶ USB-Cコネクタ

🚨 ファイルApp経由の情報漏洩

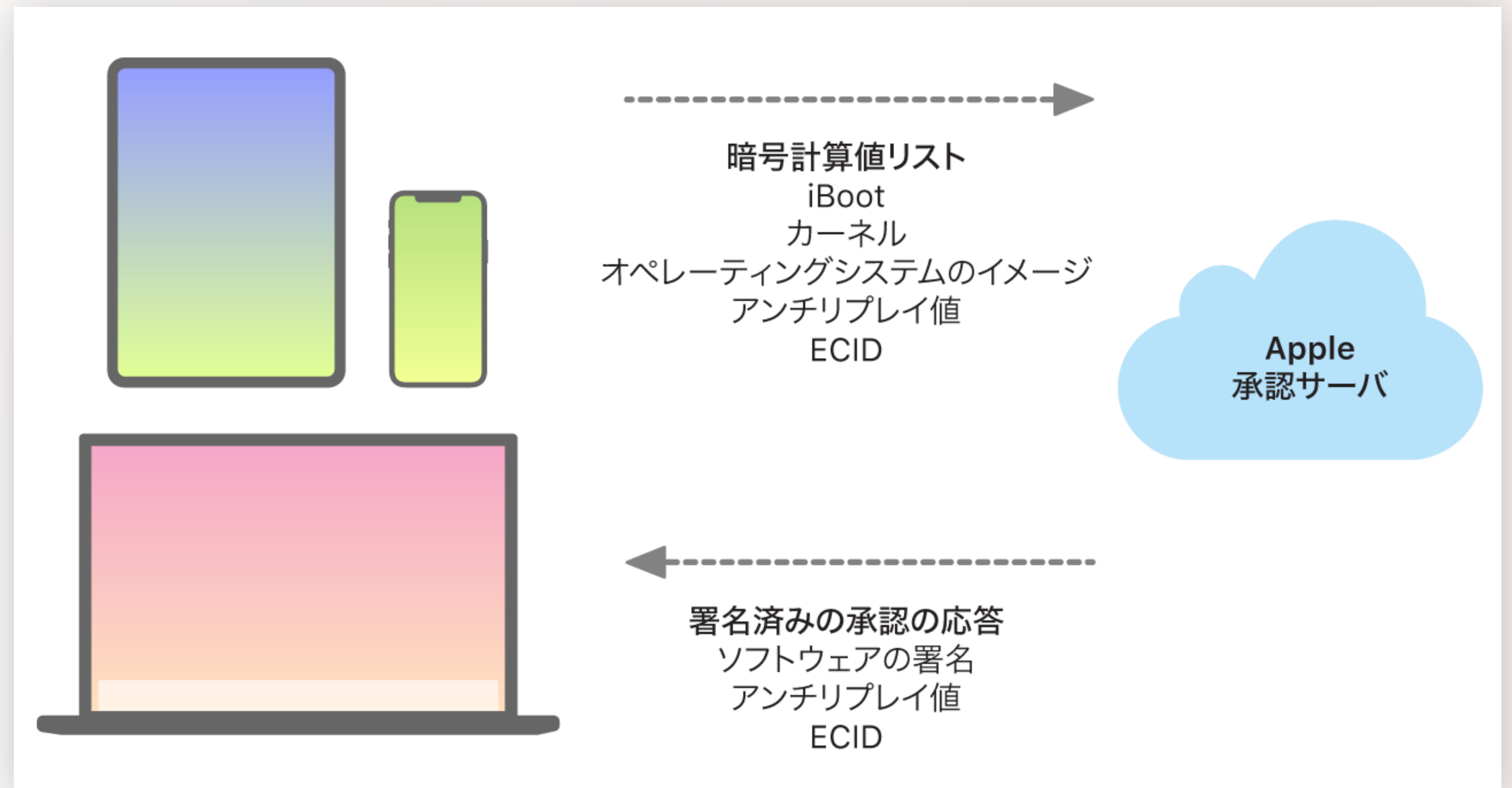




Appleプラットフォームのセキュリティ

2. システム セキュリティ

▶ OSアップデート



Appleプラットフォームのセキュリティ

2. システム セキュリティ

- ▶ パスコード
- ▶ 緊急セキュリティ対応
- ▶ ロックダウンモード などなど...

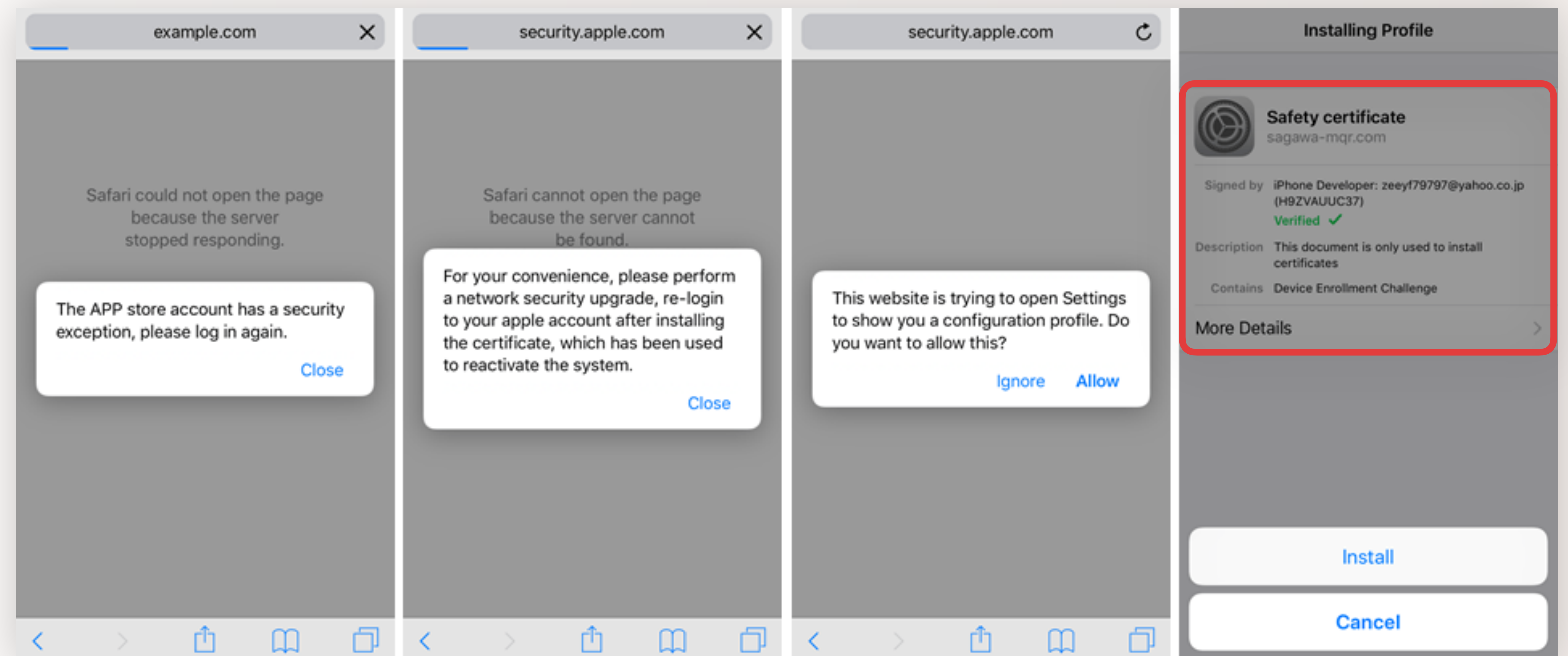
 設定の強制、標準化

Appleプラットフォームのセキュリティ

2. システム セキュリティ

▶ 構成プロファイル

 構成プロファイルを悪用した不正アプリのインストール



Appleプラットフォームのセキュリティ

3. アプリケーション セキュリティ

- ▶ App Store
 - ▶ すべてのアプリは審査プロセスを経て公開
 - ▶ マルウェア対策と品質管理の実施
 - ▶ アプリのコード署名による改ざん防止

macOS/iOS TCCの脆弱性 CVE-2024-44131が修正：セキュリティ・バイパスの恐れ

2024年12月10日

脆弱性

Apple、Apple TCC、CVE-2024-44131、iOS、Jamf Threat Labs、macOS、脆弱性

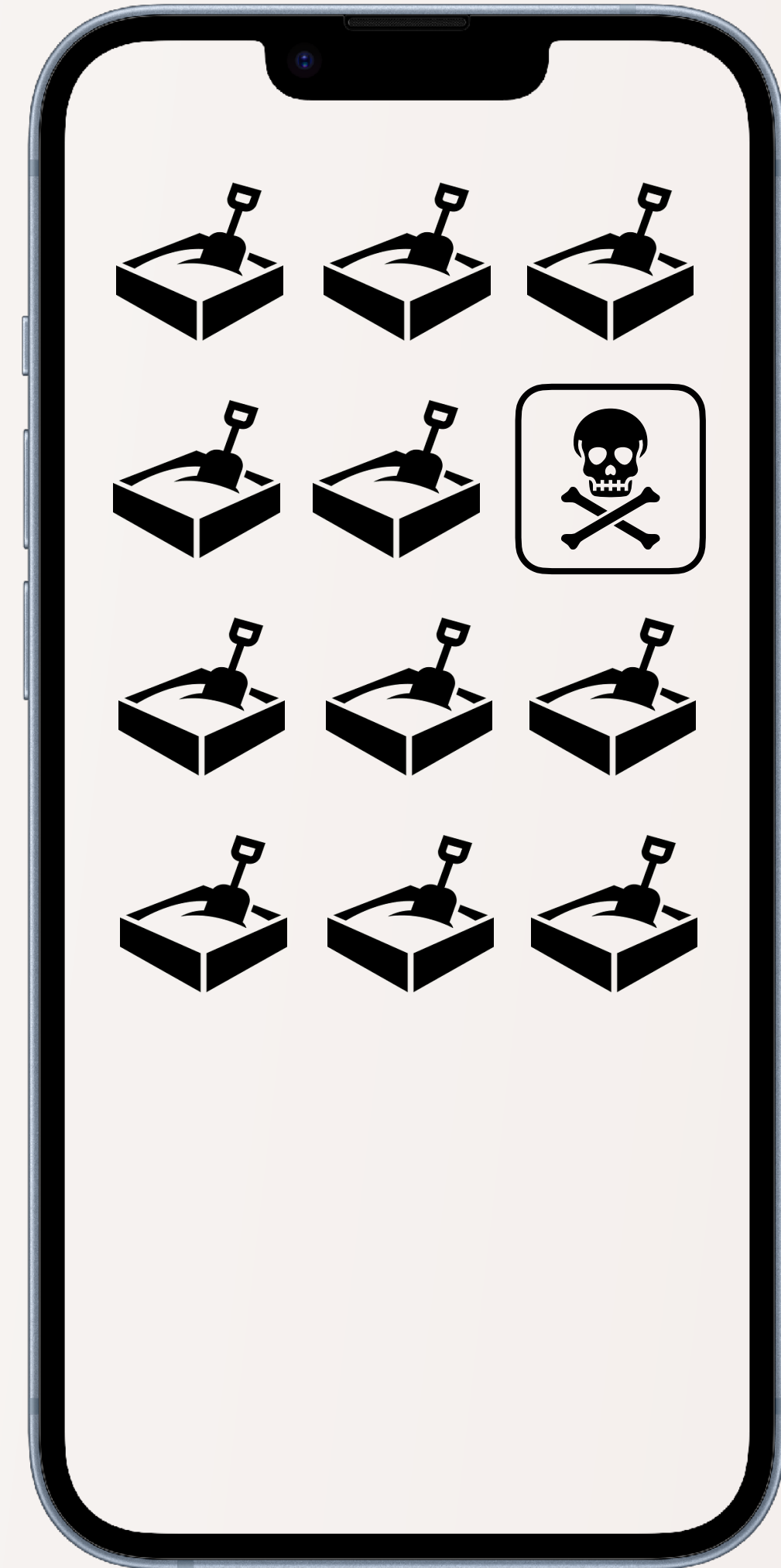
[研究者がCVE-2024-44131の詳細を公開 – macOSとiOSにおける重大なTCCバイパス](#)

2024/12/10 SecurityOnline — Apple TCC (Transparency, Consent, and Control) に存在する脆弱性 CVE-2024-44131 が、Jamf Threat Labs により発見された。この脆弱性を悪用する攻撃者は、ユーザーの同意を考慮したアプリで回避し、ユーザーに見えるセキュリティデータにアクセスしていく。システムに決められたものであり、macOS 15/iOS 18で修正されています。

Appleプラットフォームのセキュリティ

3. アプリケーション セキュリティ

- ▶ サンドボックス
 - ▶ 他のアプリやシステムへの影響を最小限に抑える
 - ▶ プライバシーの保護
 - ▶ アプリの悪用を防ぐ



Appleプラットフォームのセキュリティ

3. アプリケーション セキュリティ

- ▶ サイドローディング

- サイドローディングAppのリスク

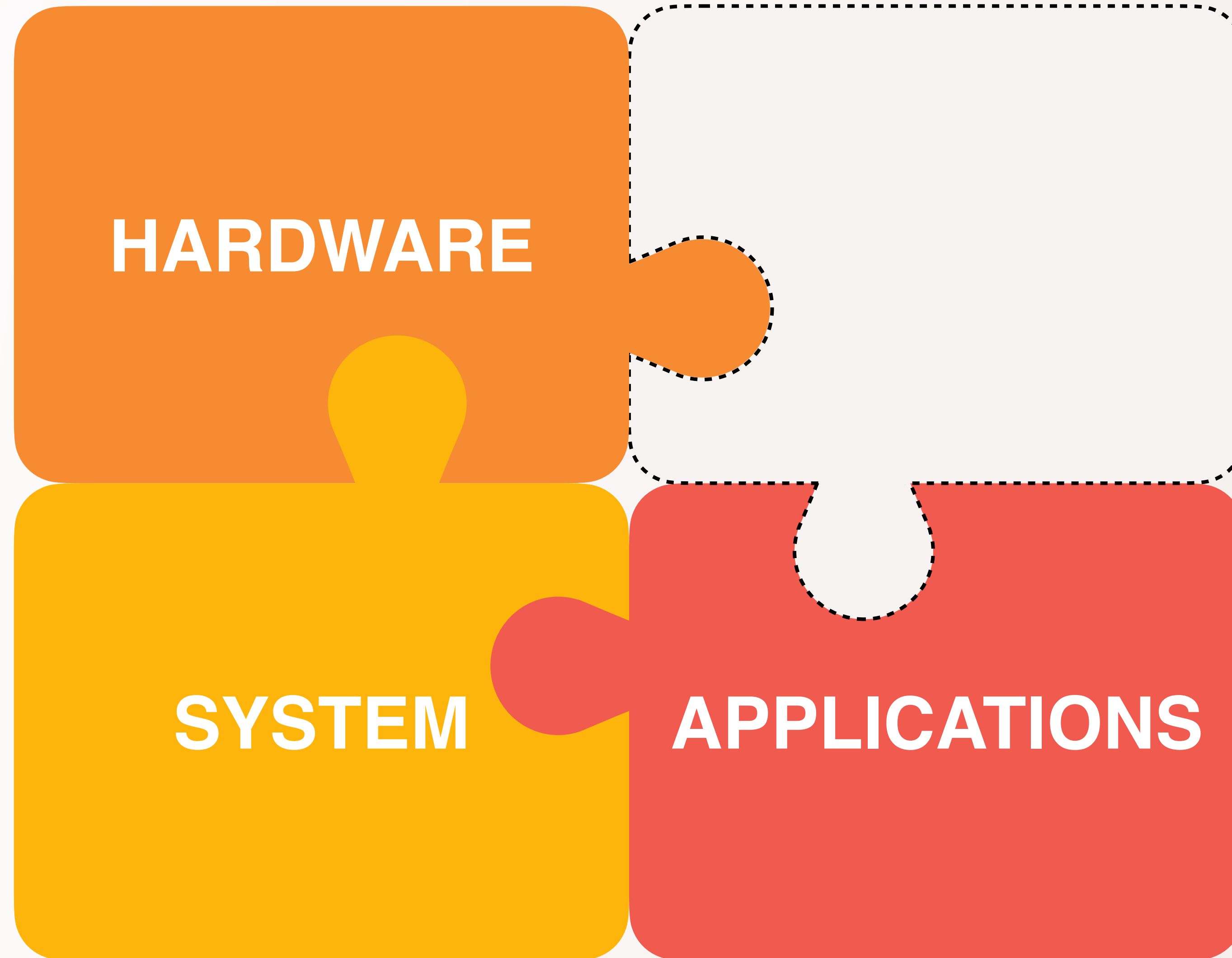
- ▶ 欧州連合のデジタル市場法（DMA）

- ▶ EU (欧州連合) 諸国ではiOS 17.4以降でサイドローディングが許可

- ▶ スマホソフトウェア競争促進法（スマホ新法）

- ▶ 日本でもApp Store以外のアプリストアが開放される見込み

企業や組織でモバイル管理をする上で

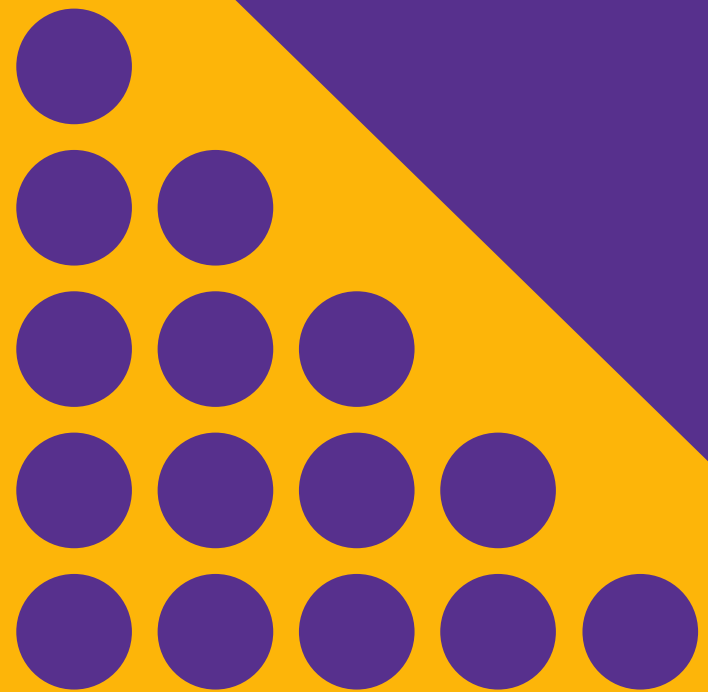


より安全性と運用効率を高めて
管理したい場合はどうすればいい？

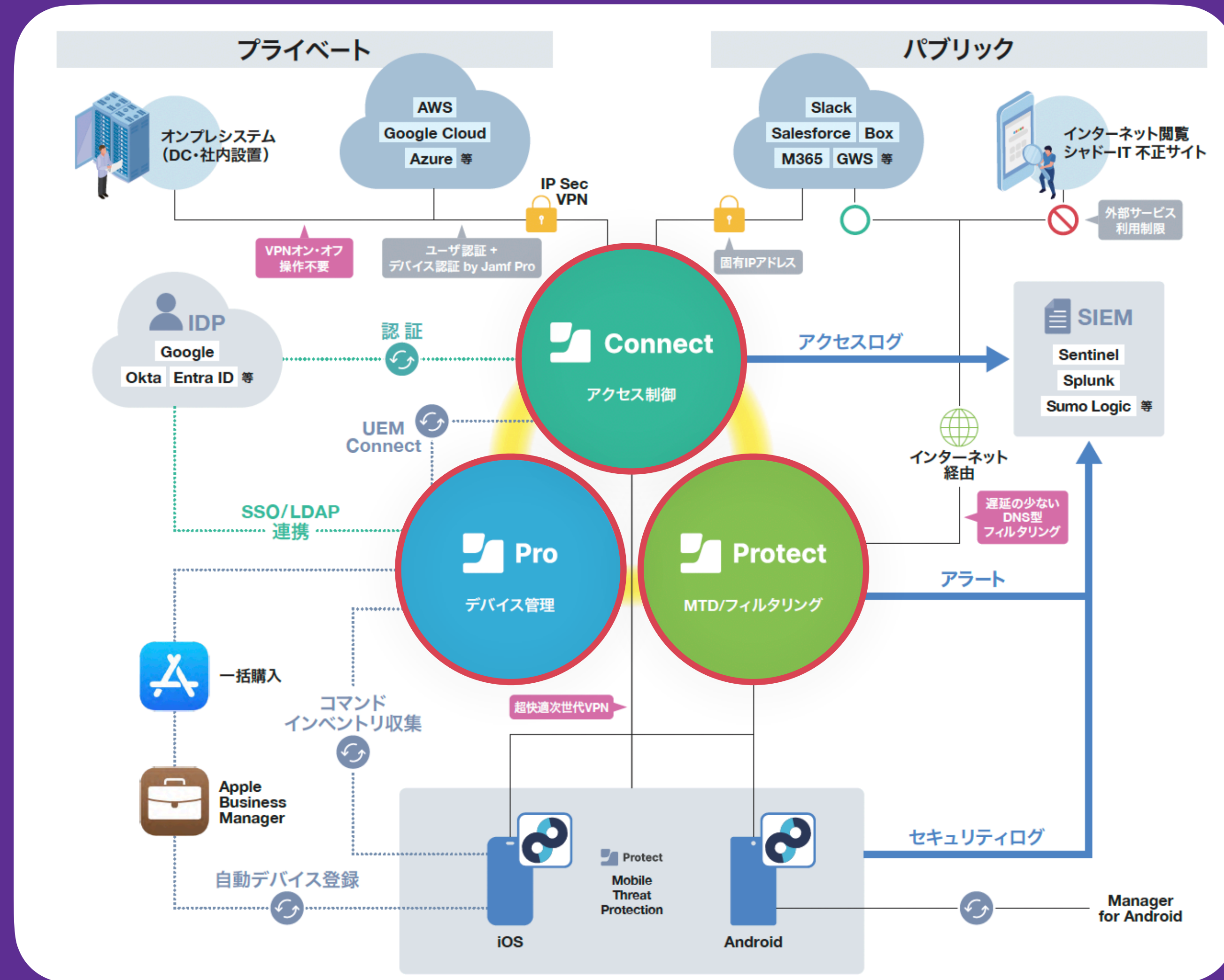


Jamf for Mobileで解決

Jamf for Mobile



Jamf for Mobile 構成図



Jamf for Mobile



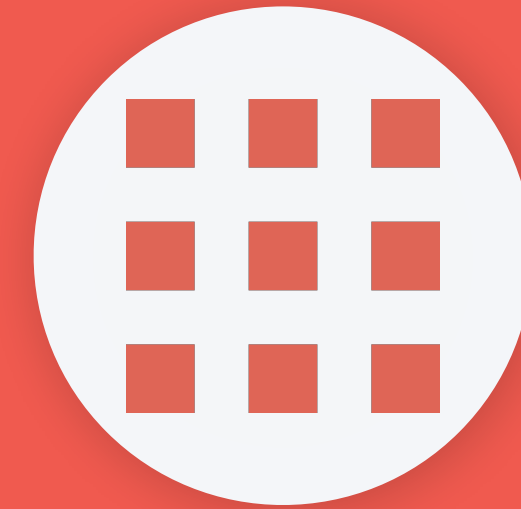
HARDWARE

- ・ MDMによる管理
- ・ 設定の自動化、効率化
- ・ ブループリント



SYSTEM

- ・ セキュリティの可視化
- ・ 対処と修復
- ・ BYOD



APPLICATIONS

- ・ アプリケーション管理
- ・ アプリケーション脅威
評価
- ・ ZTNA

HARDWARE

- ▶ MDMによる管理
- ▶ 設定の自動化、効率化
- ▶ ブループリント



MDMによる管理

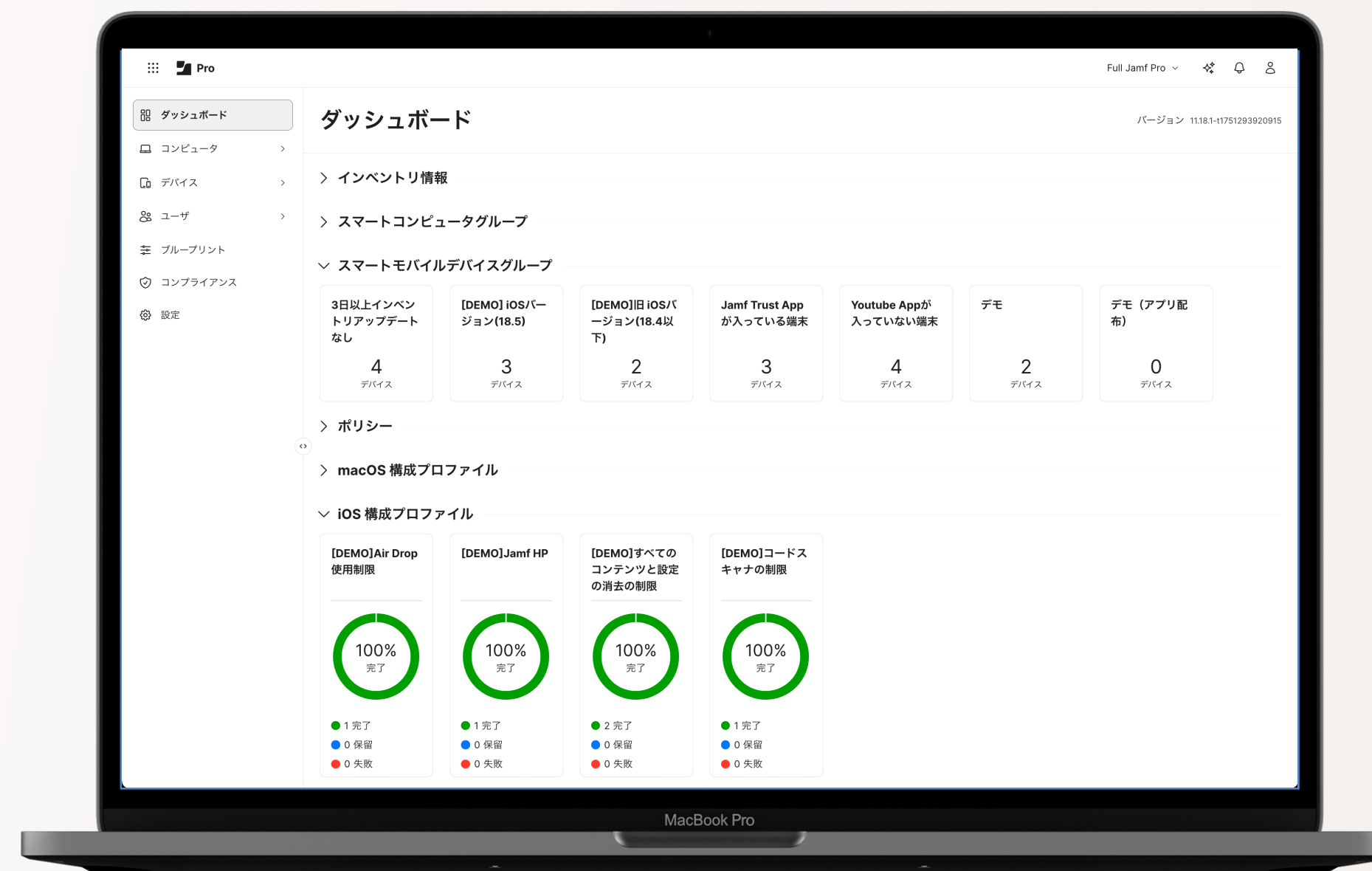
▶ 構成プロファイルの配布

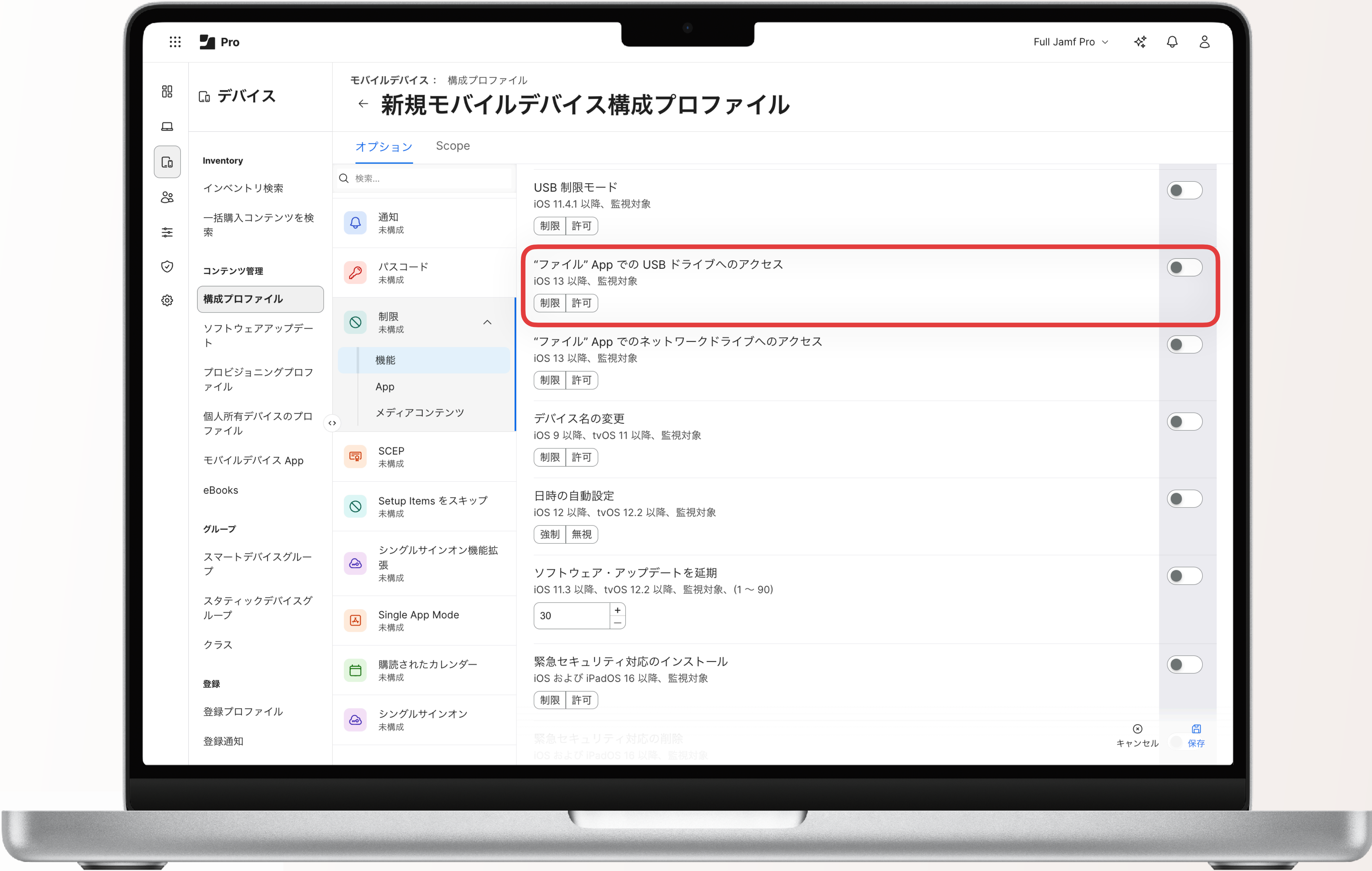


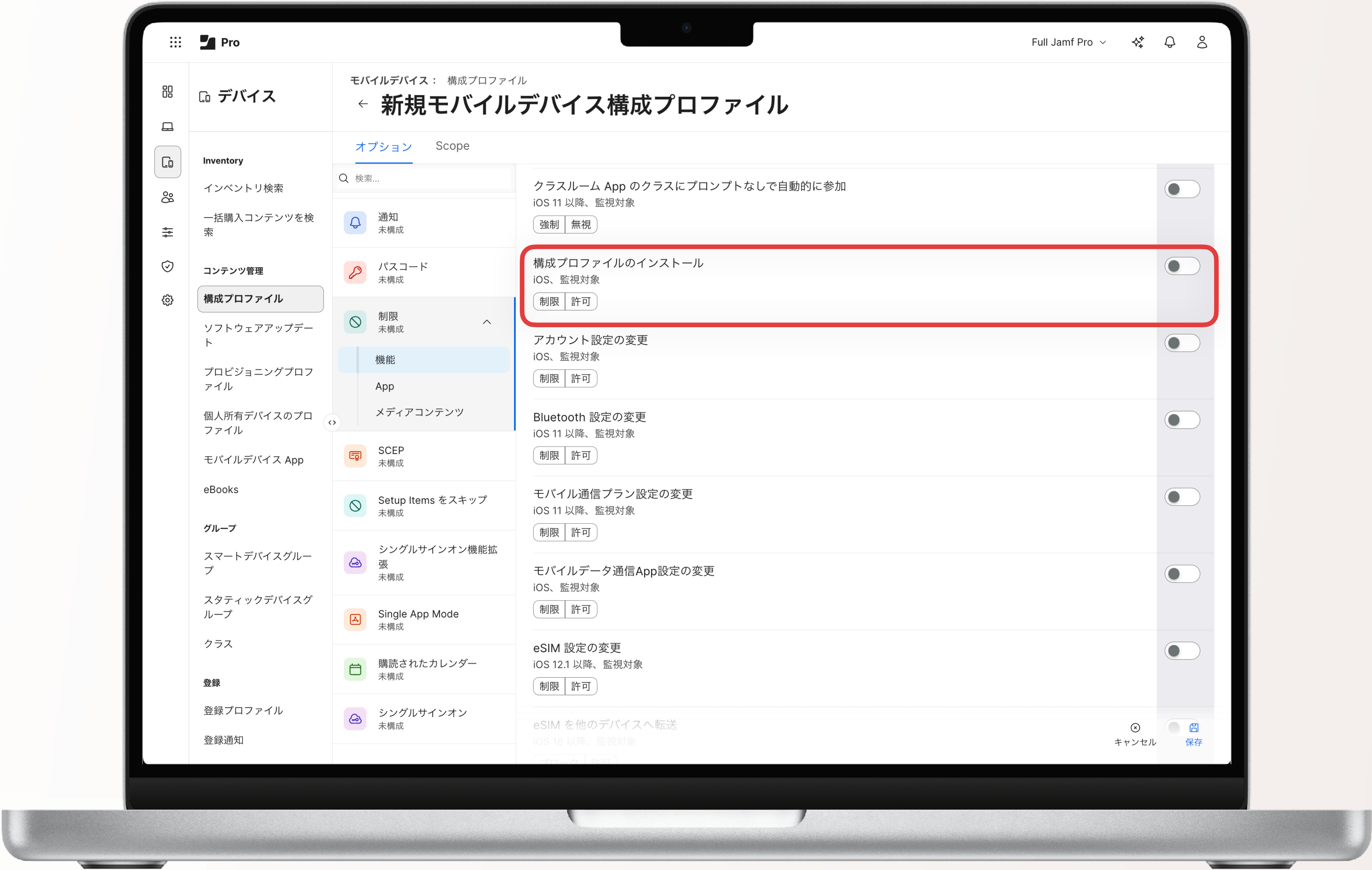
▶ リモートコマンド



▶ インベントリ情報の収集







設定の自動化、効率化

▶ゼロタッチキットティング

 Pro  Protect  Connect

▶APIの活用

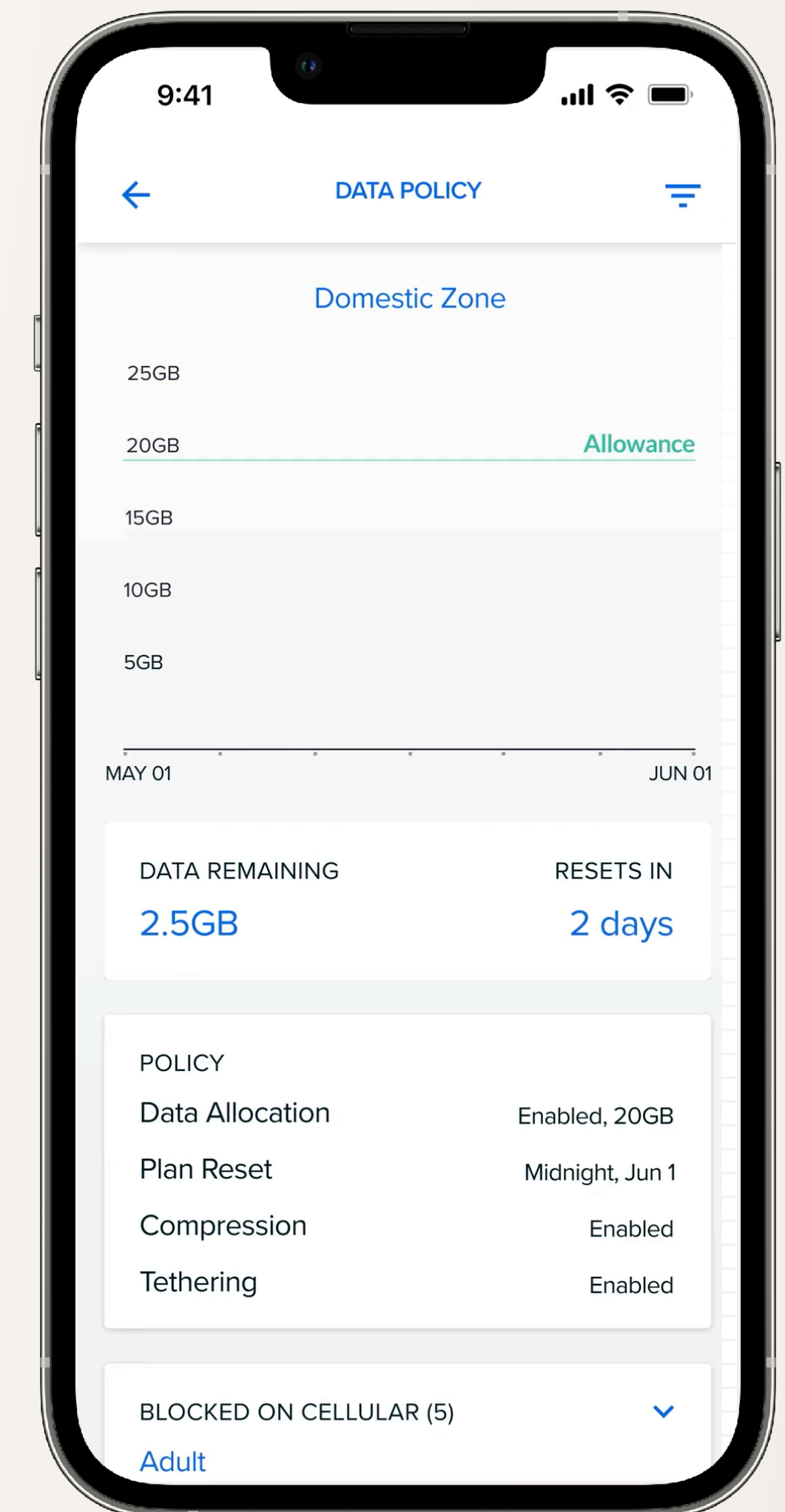
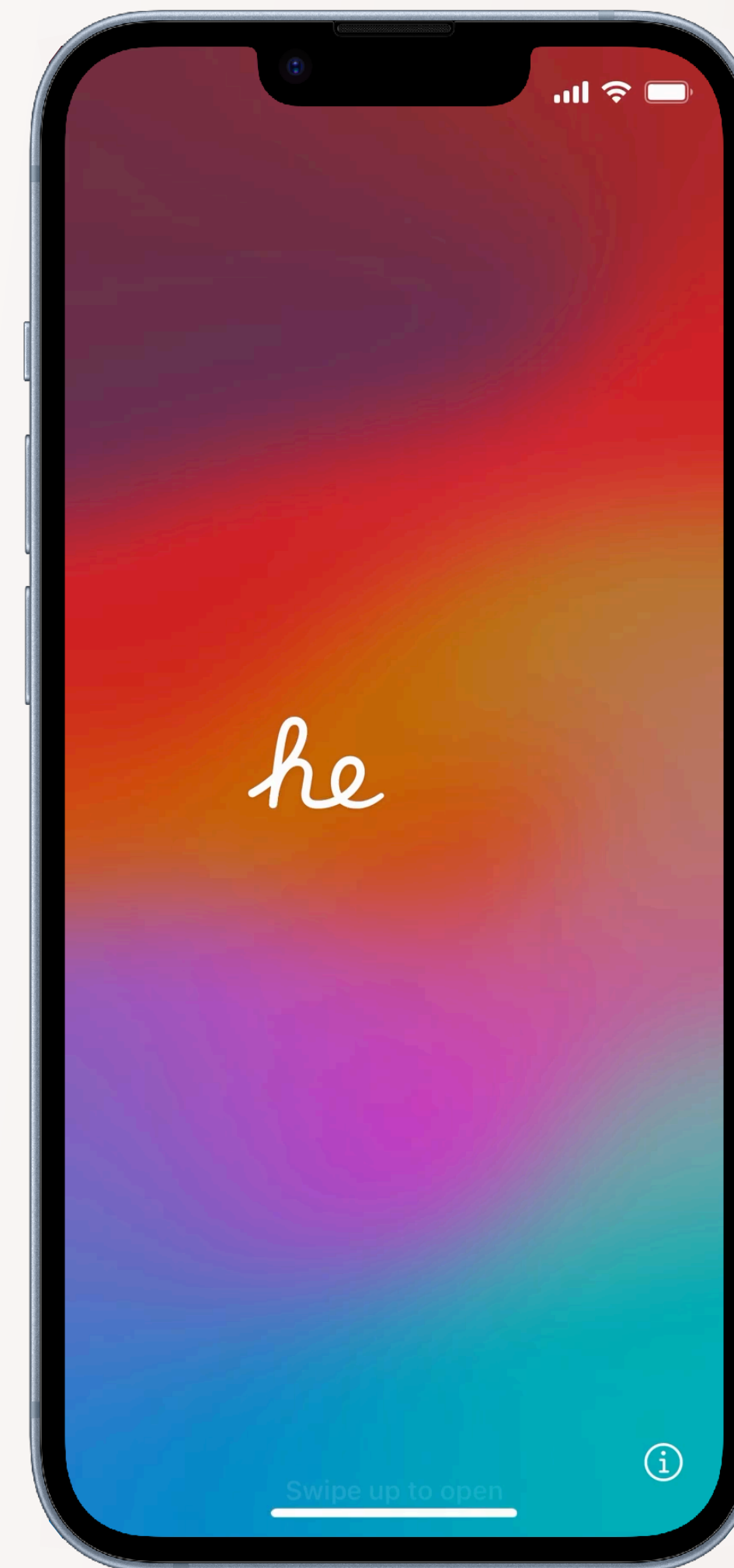
 Pro

▶コンプライアンスベンチマークの適用

 Pro  Protect

▶データ通信使用量ポリシーの設定

 Pro  Protect



ブループリント

▶ 宣言型デバイス管理 (DDM)の活用



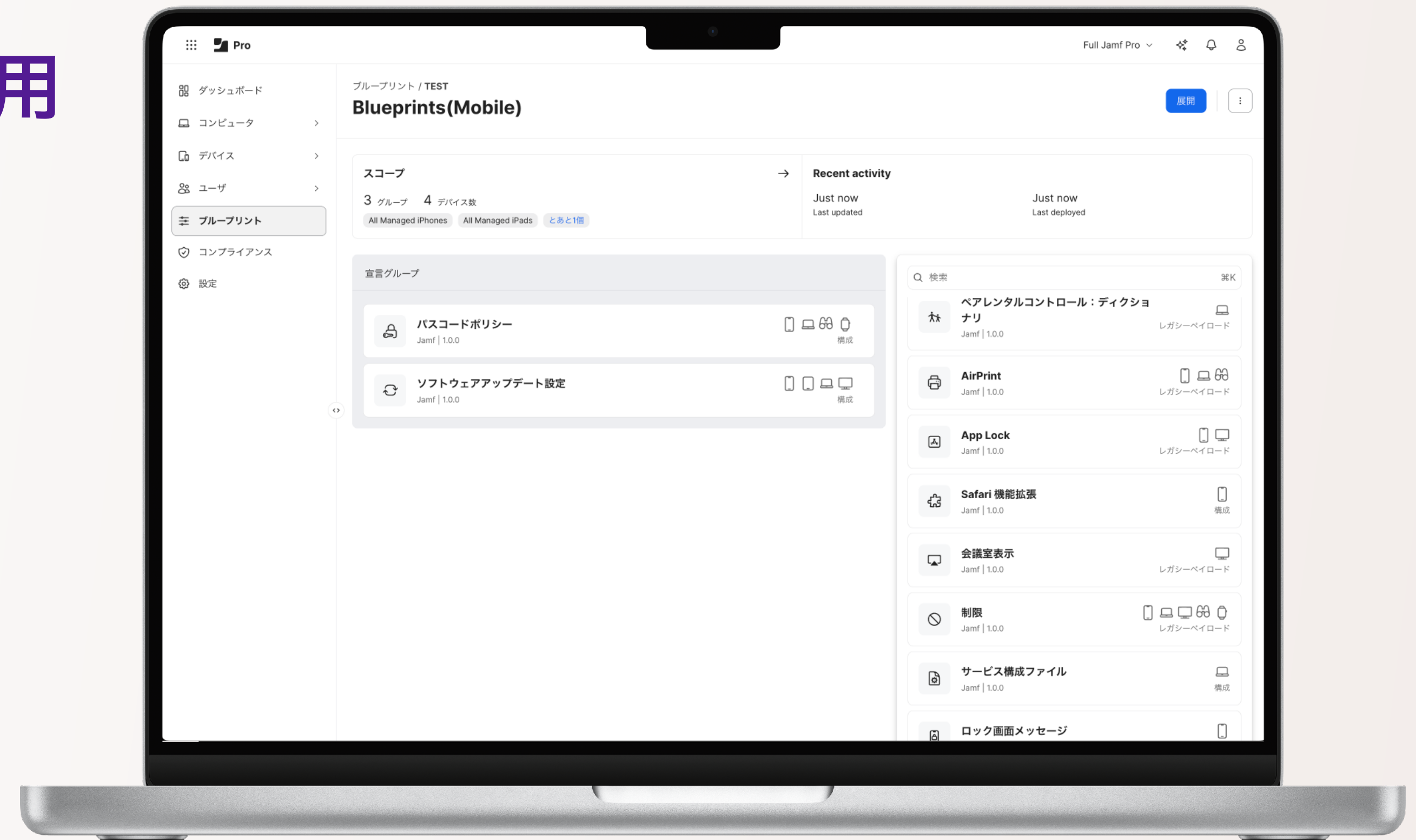
▶ パスコードポリシーの設定



▶ 計算設定

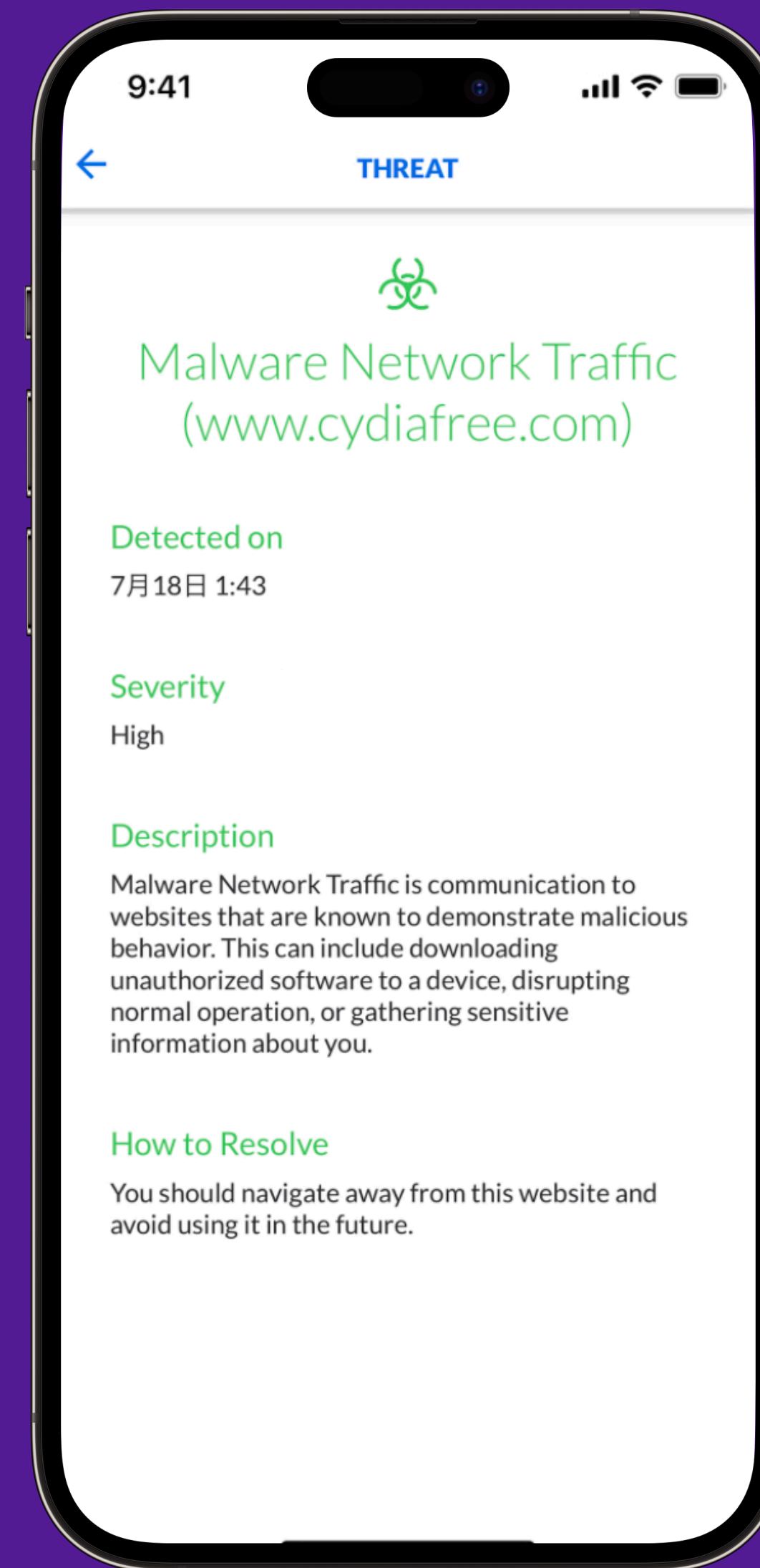


▶ ソフトウェアアップデート設定



SYSTEM

- ▶ セキュリティの可視化
- ▶ 対処と修復
- ▶ BYOD



セキュリティの可視化

▶ 脆弱性管理



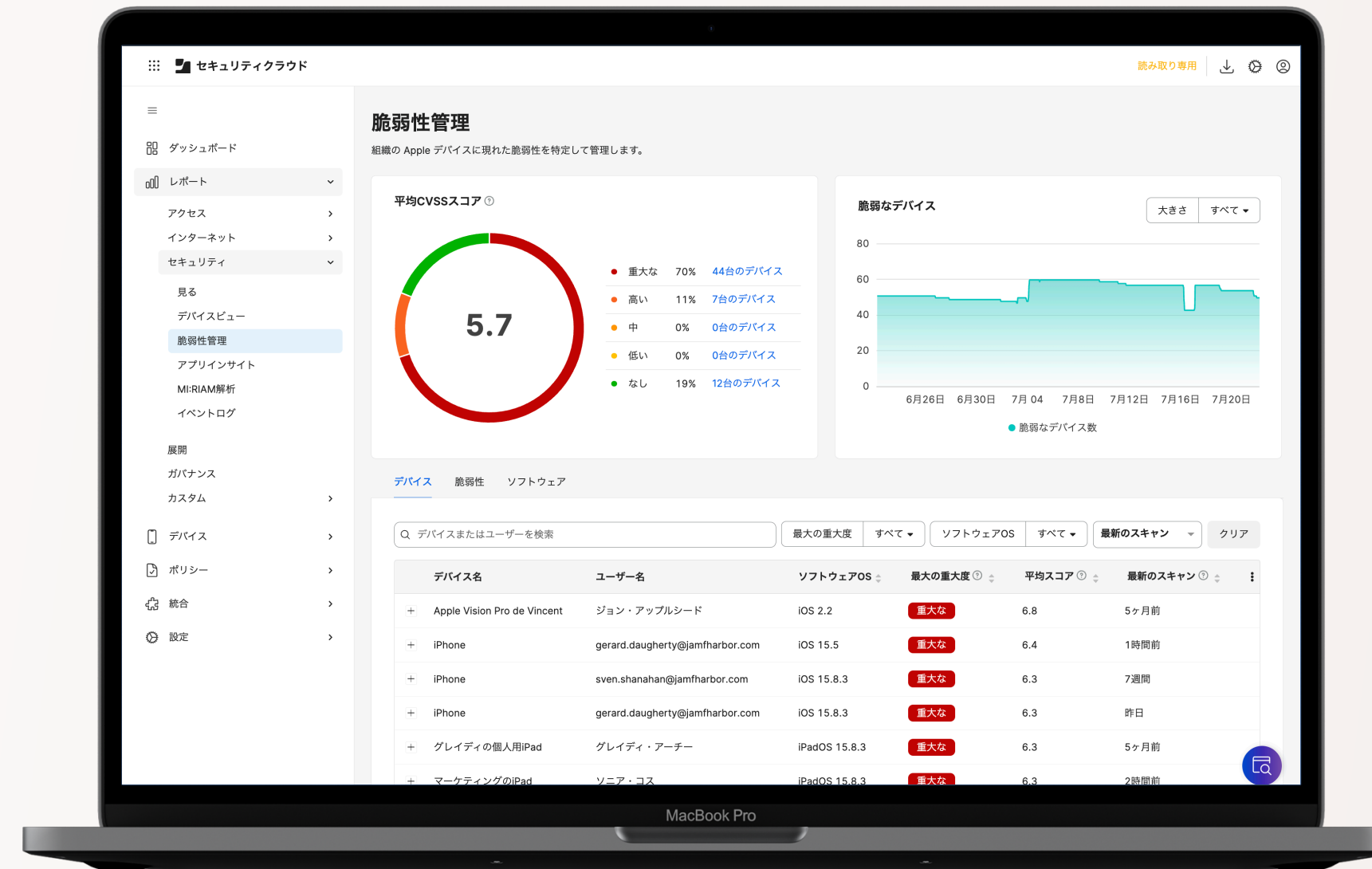
▶ マルウェア対策



▶ 豊富なテレメトリの収集



▶ SIEMへのストリーミング



対応と修復

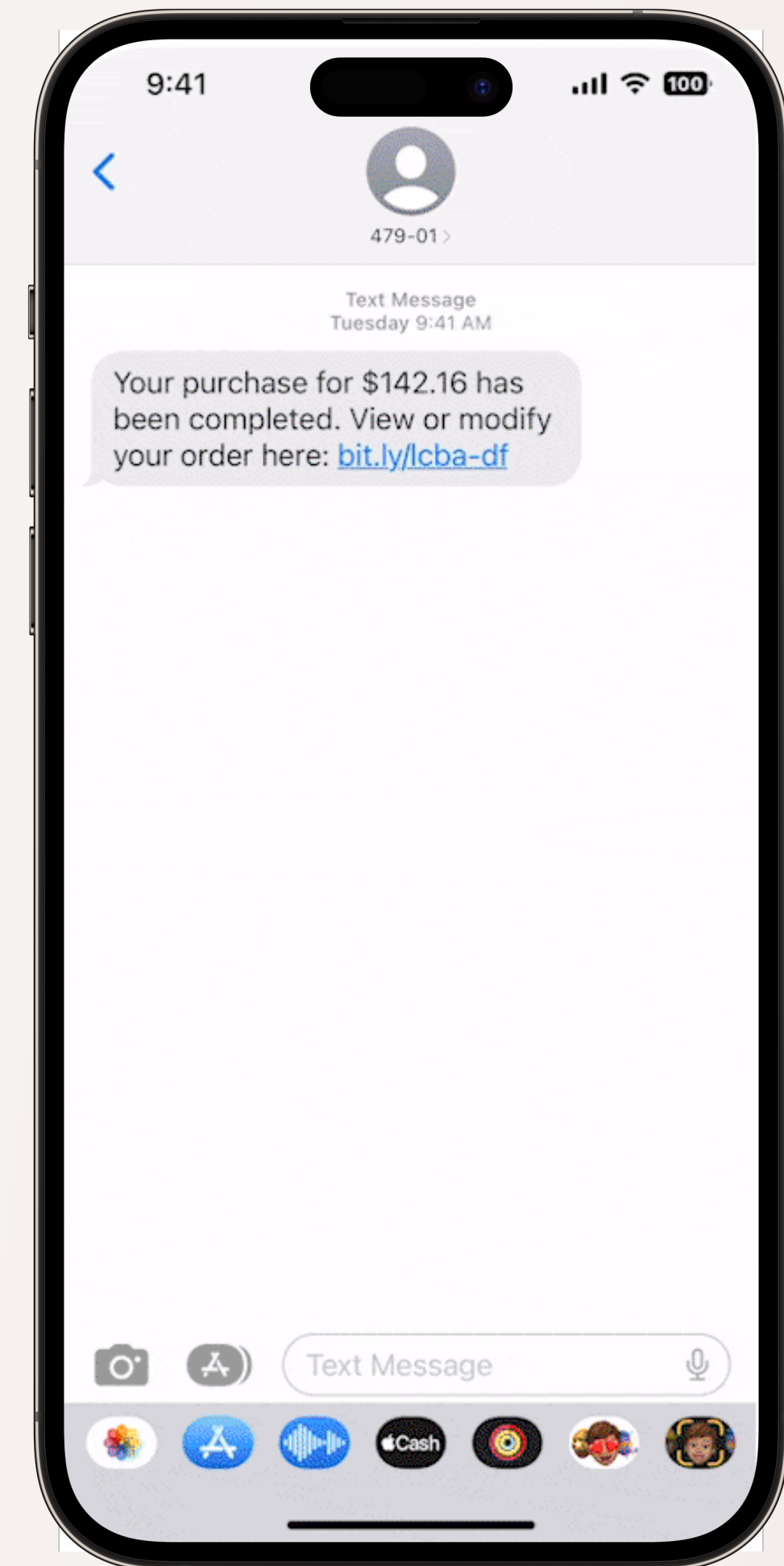
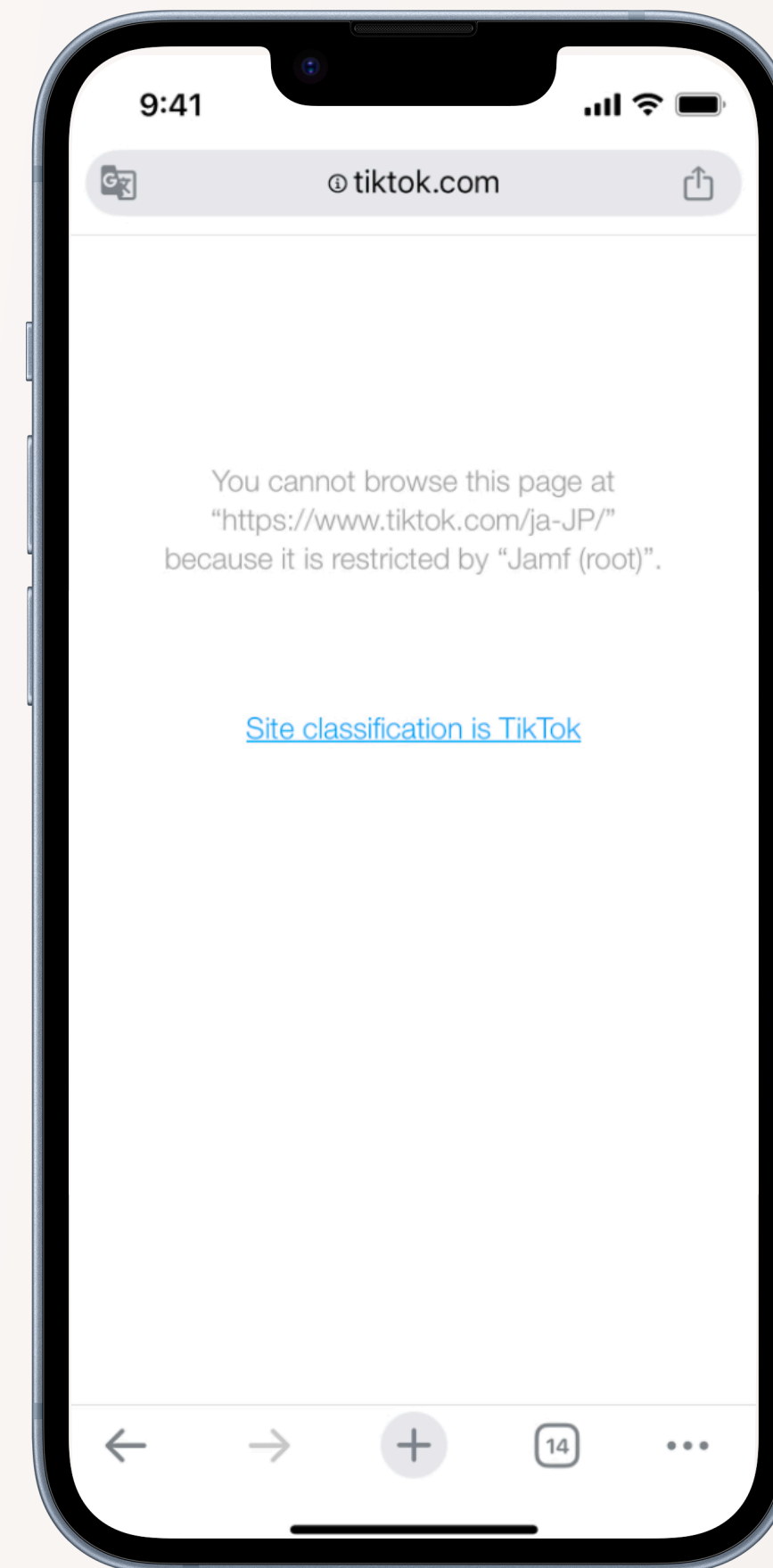
▶ プロアクティブな対応



▶ セキュリティ業務の自動化



▶ 通信経路の途中で直接検知して遮断



BYOD

▶ アカウント駆動型 ユーザ登録



Pro

▶ データ分離とプライバシー保護



Pro

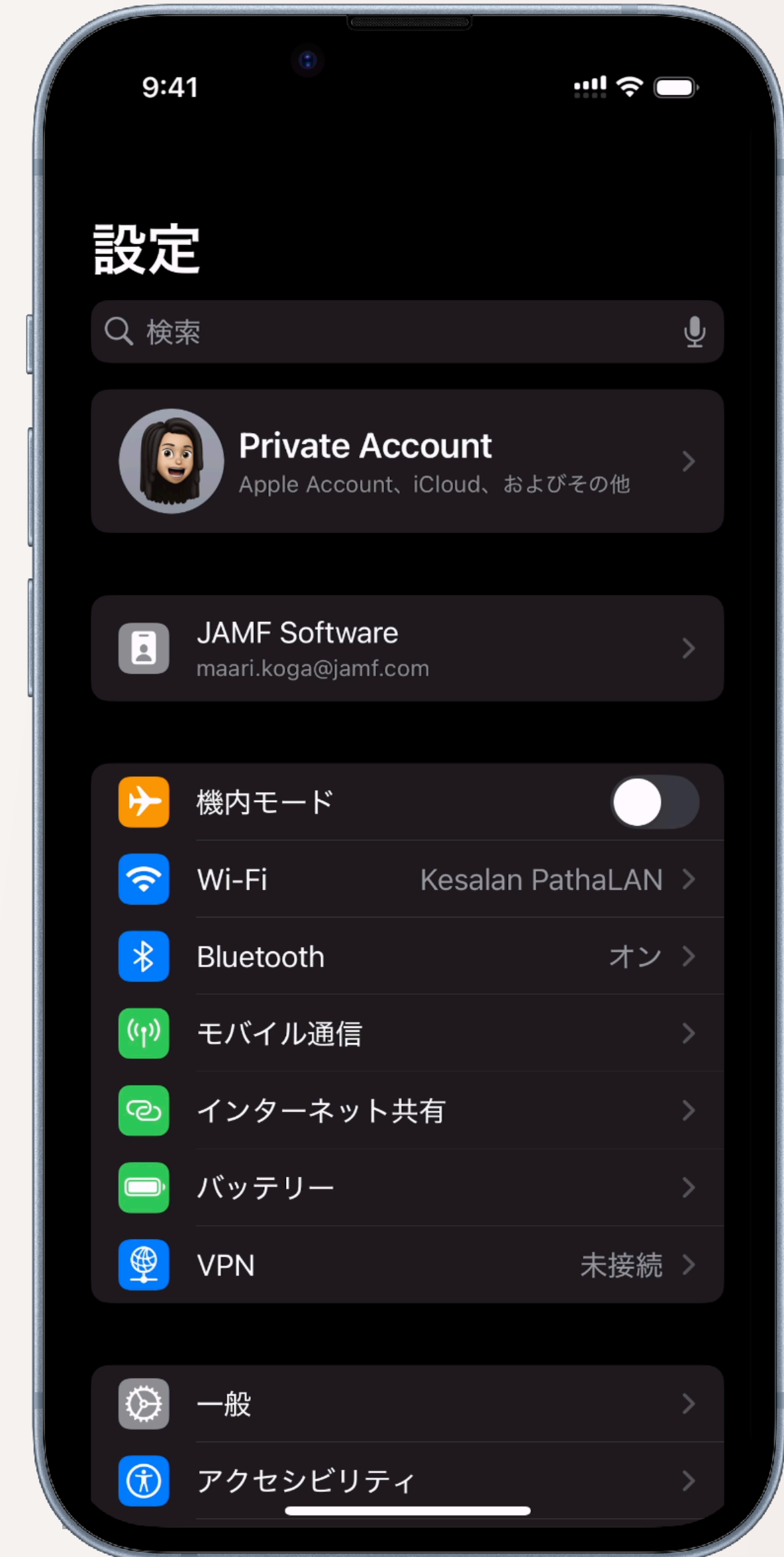
▶ 企業リソースへの安全なアクセス



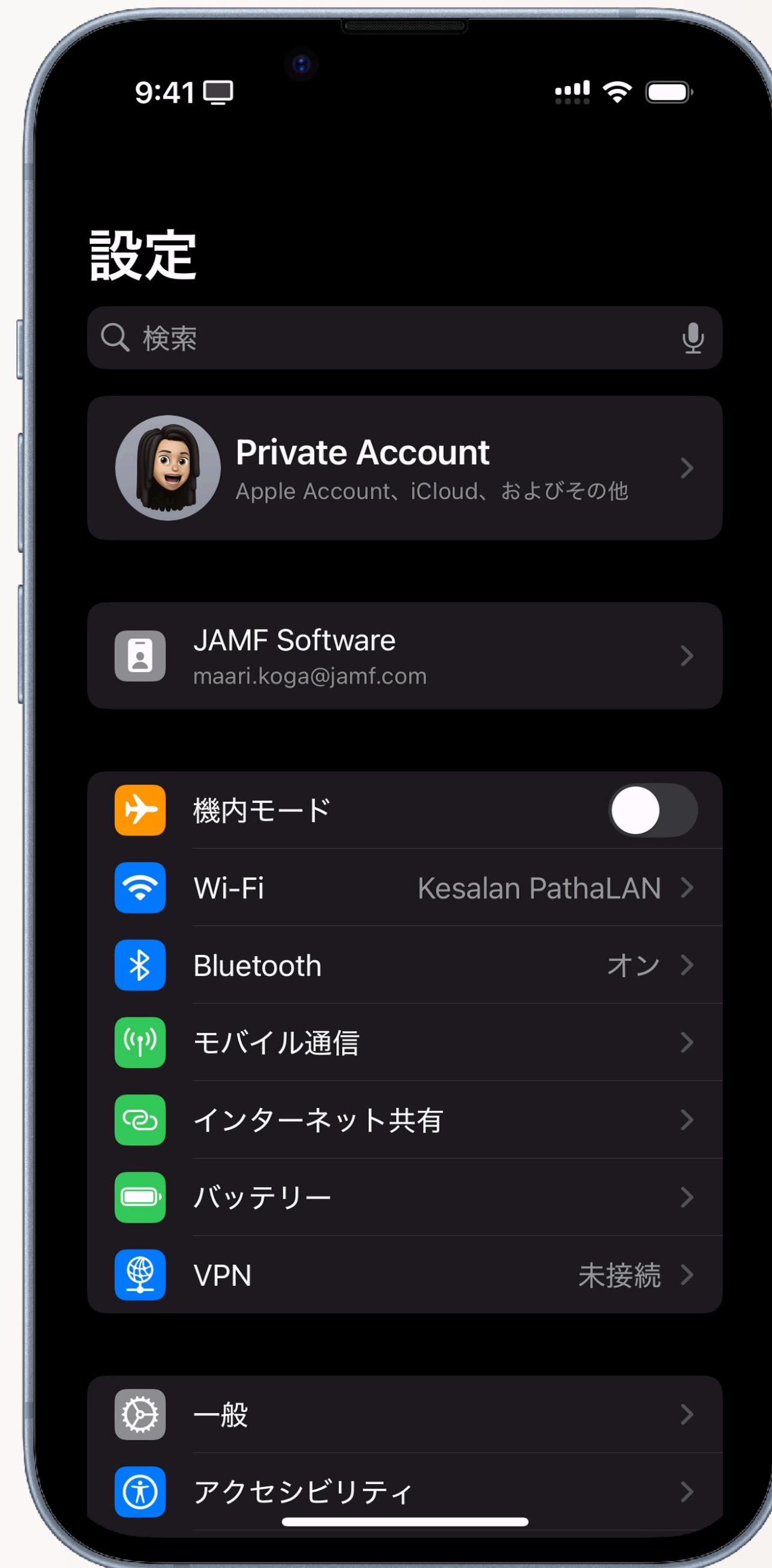
Pro



Protect



BYOD



APPLICATIONS

- ▶ アプリケーション管理
- ▶ アプリケーション脅威評価
- ▶ ZTNA



アプリケーション管理

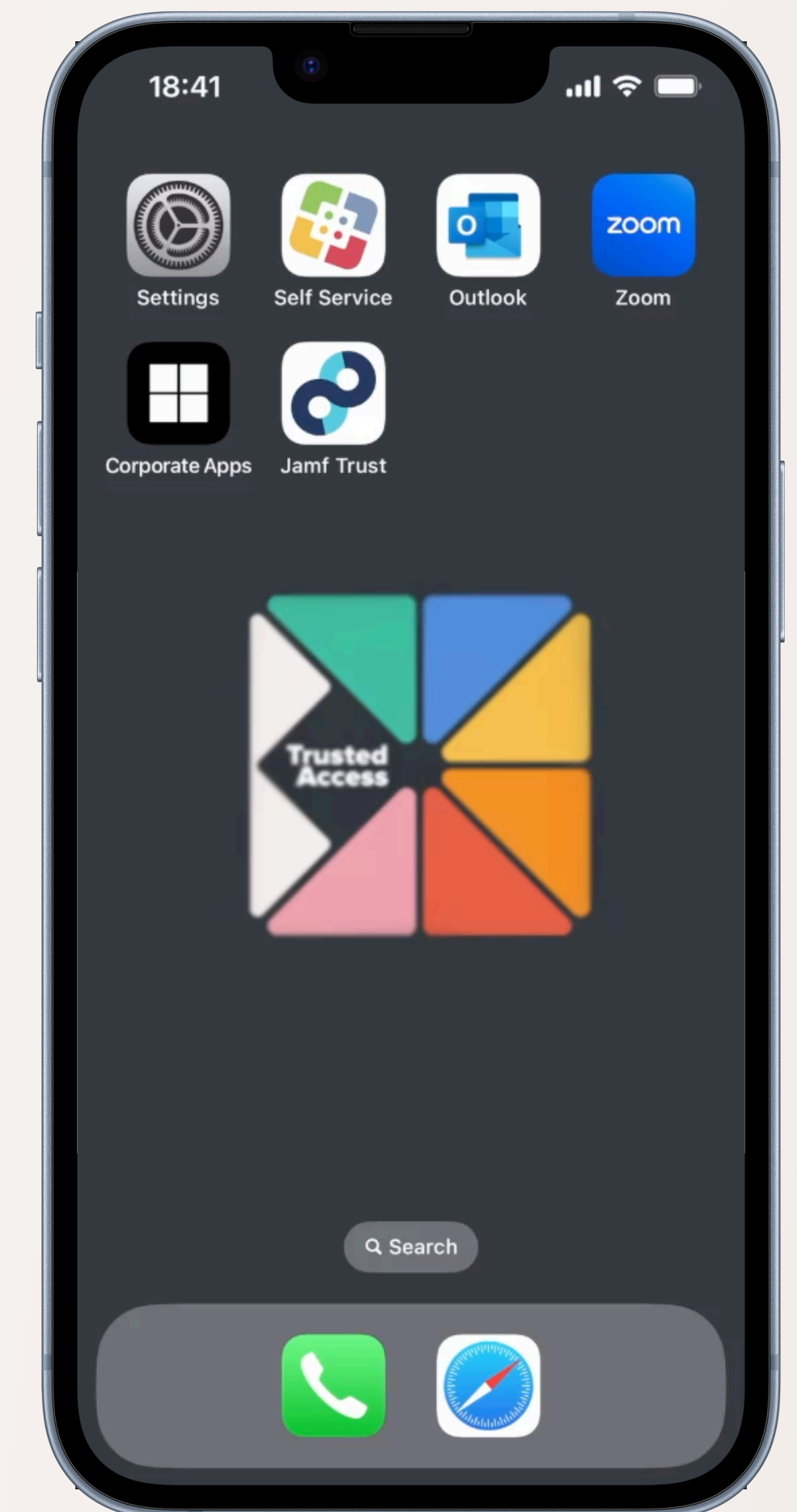
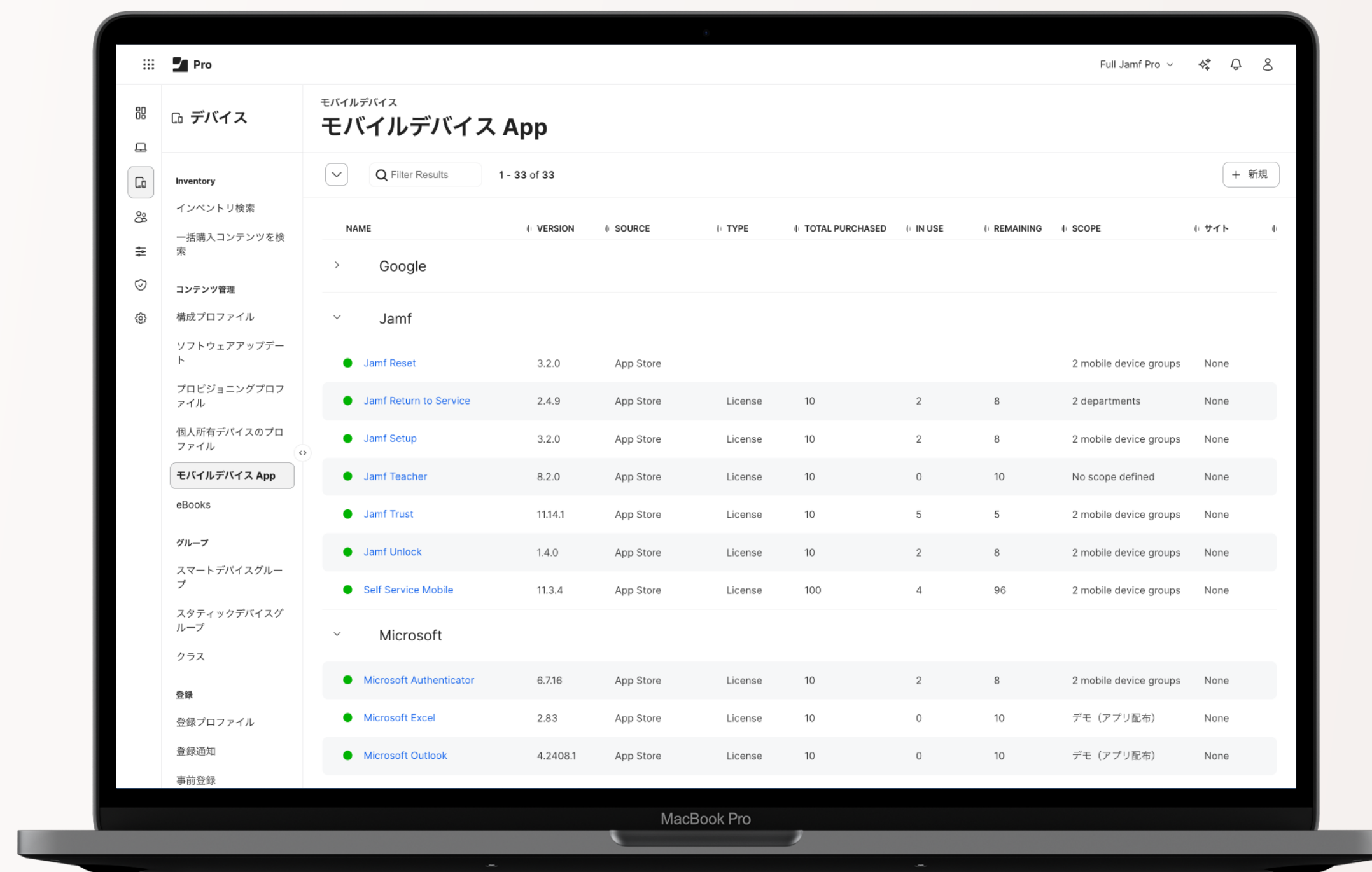
▶ アプリの割り当て



▶ アプリレポート



▶ アプリ制限



アプリケーション脅威評価

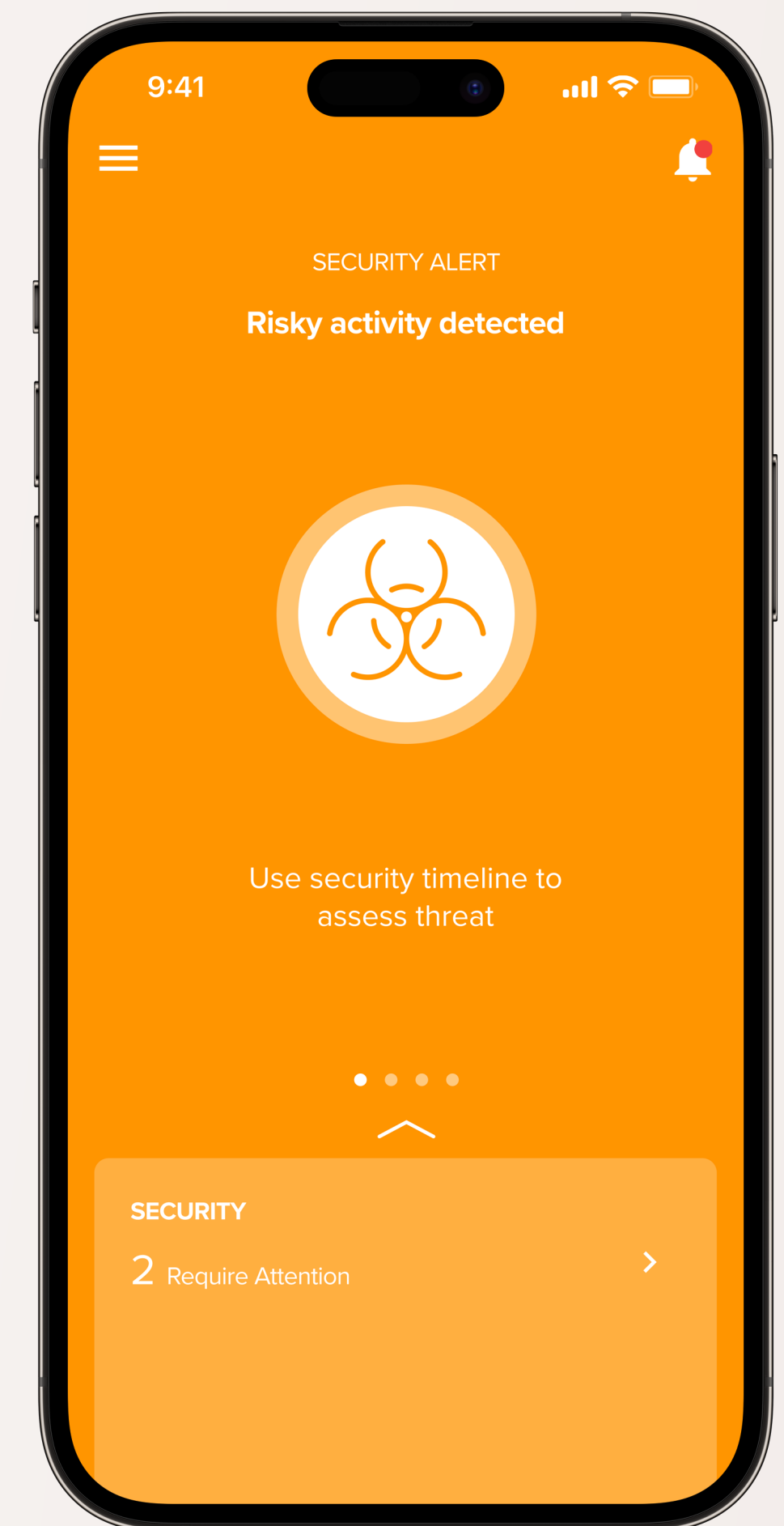
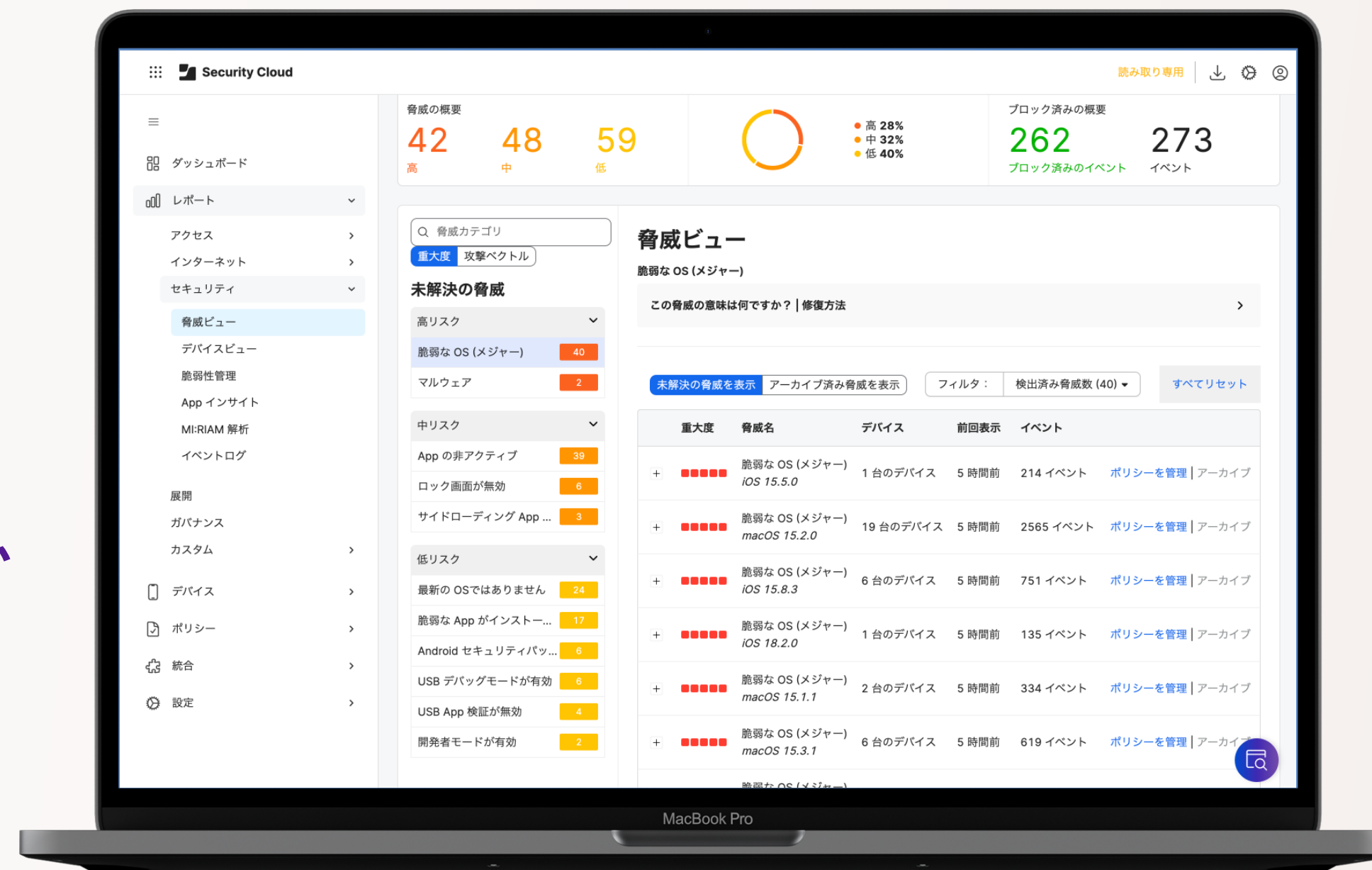
▶ アプリのリスク監視



▶ アプリベースの脅威防御



▶ アプリのリスクスコアリング



ZTNA

▶ 安全な接続の確保



▶ セキュアなネットワーク通信



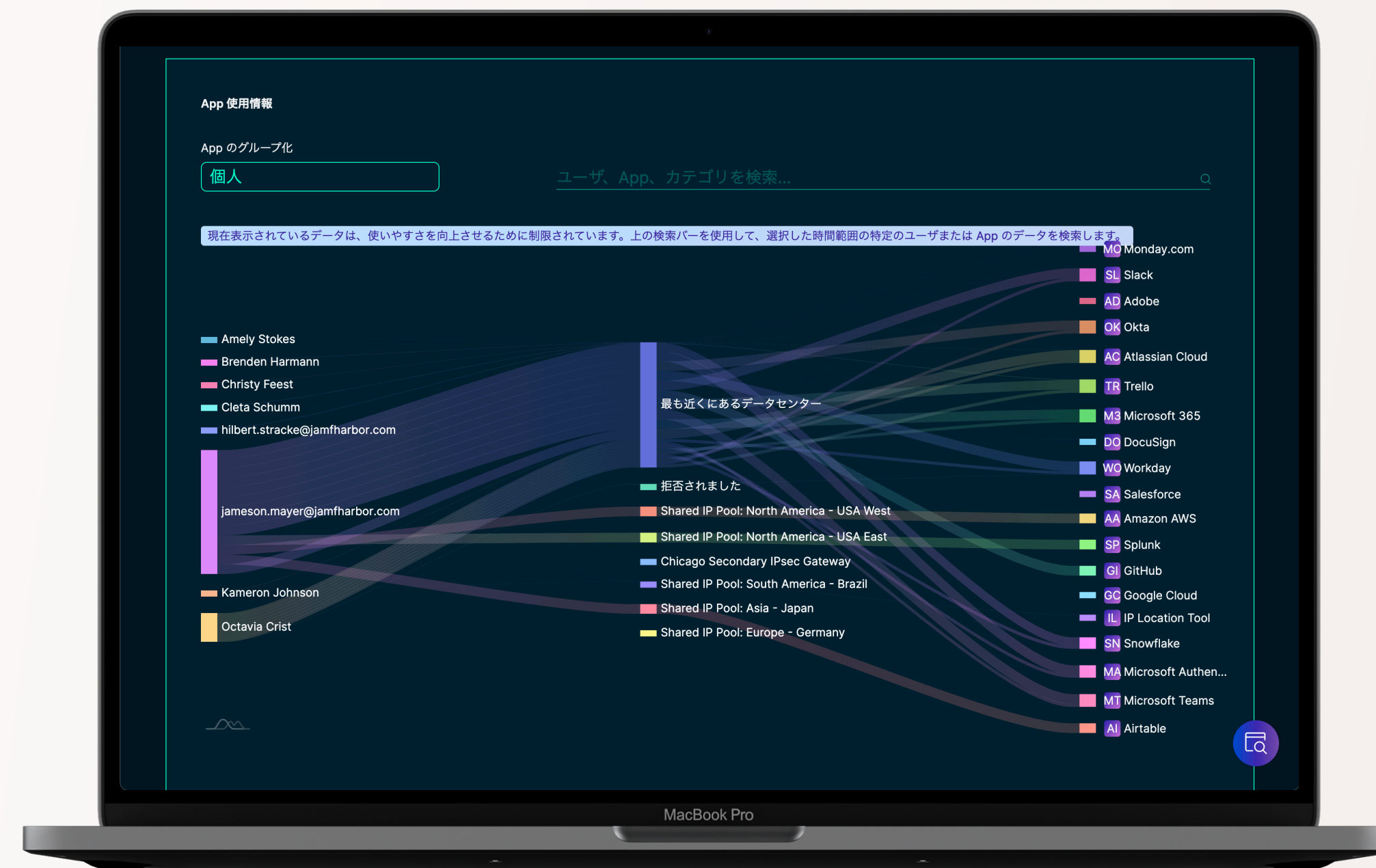
▶ 継続的な条件付きアクセス

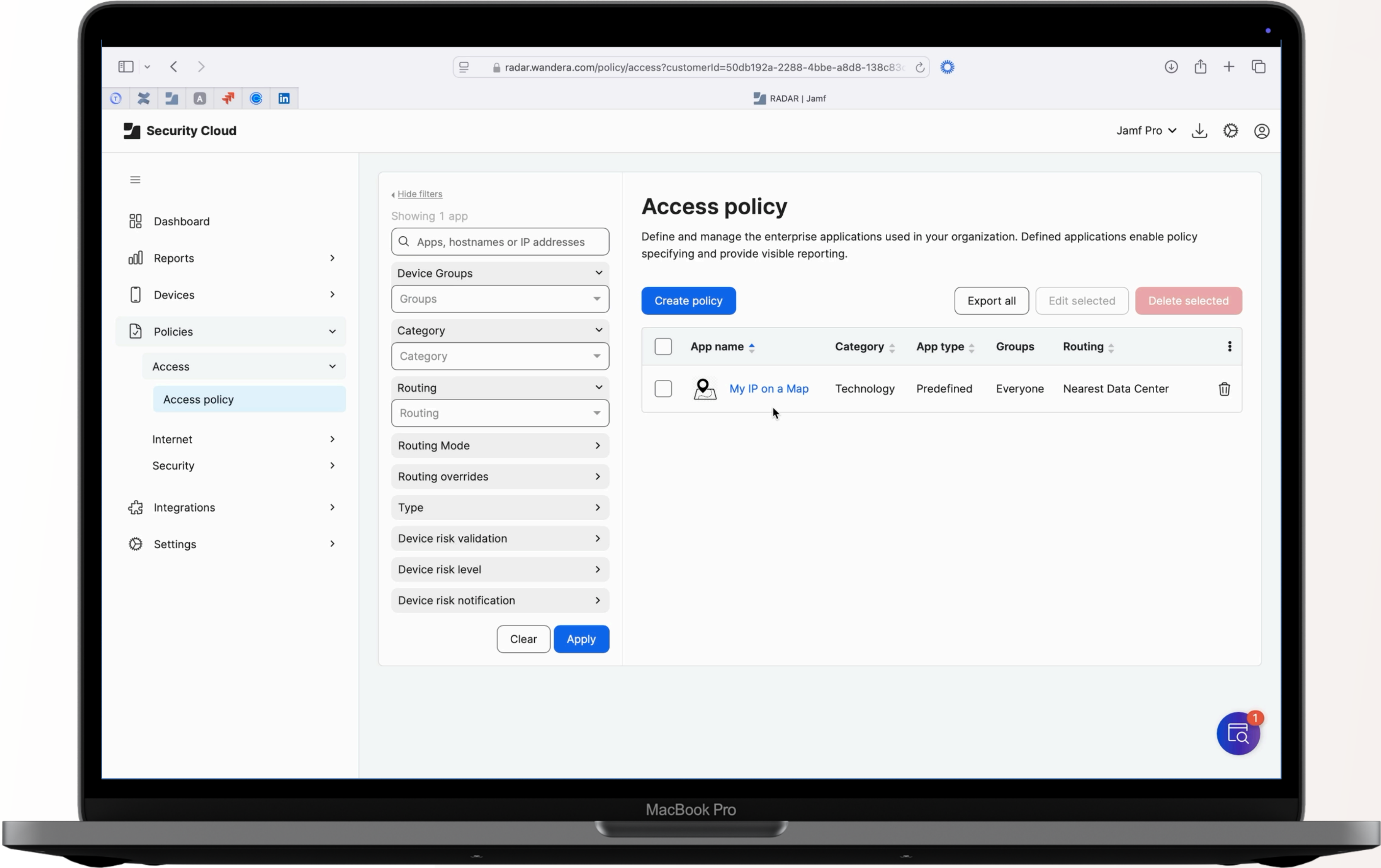


▶ アクセス制御

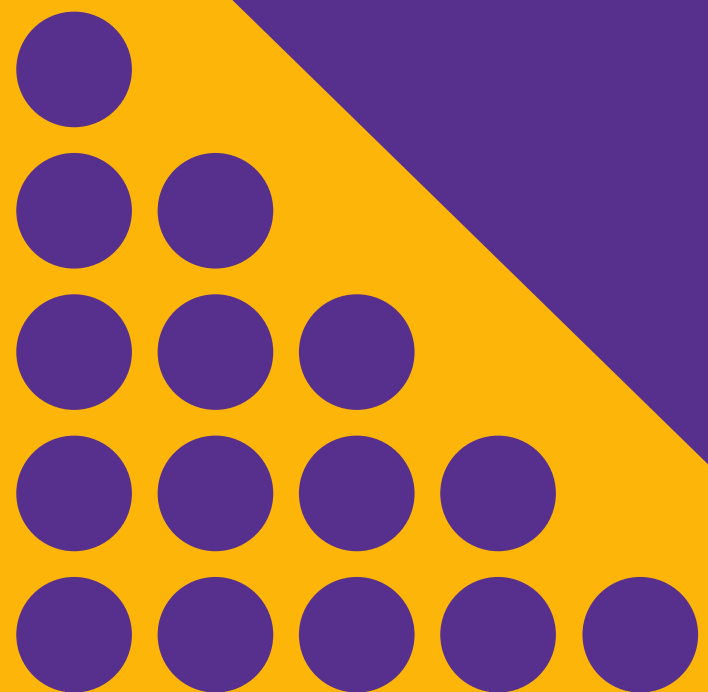


● JAMF NATION LIVE

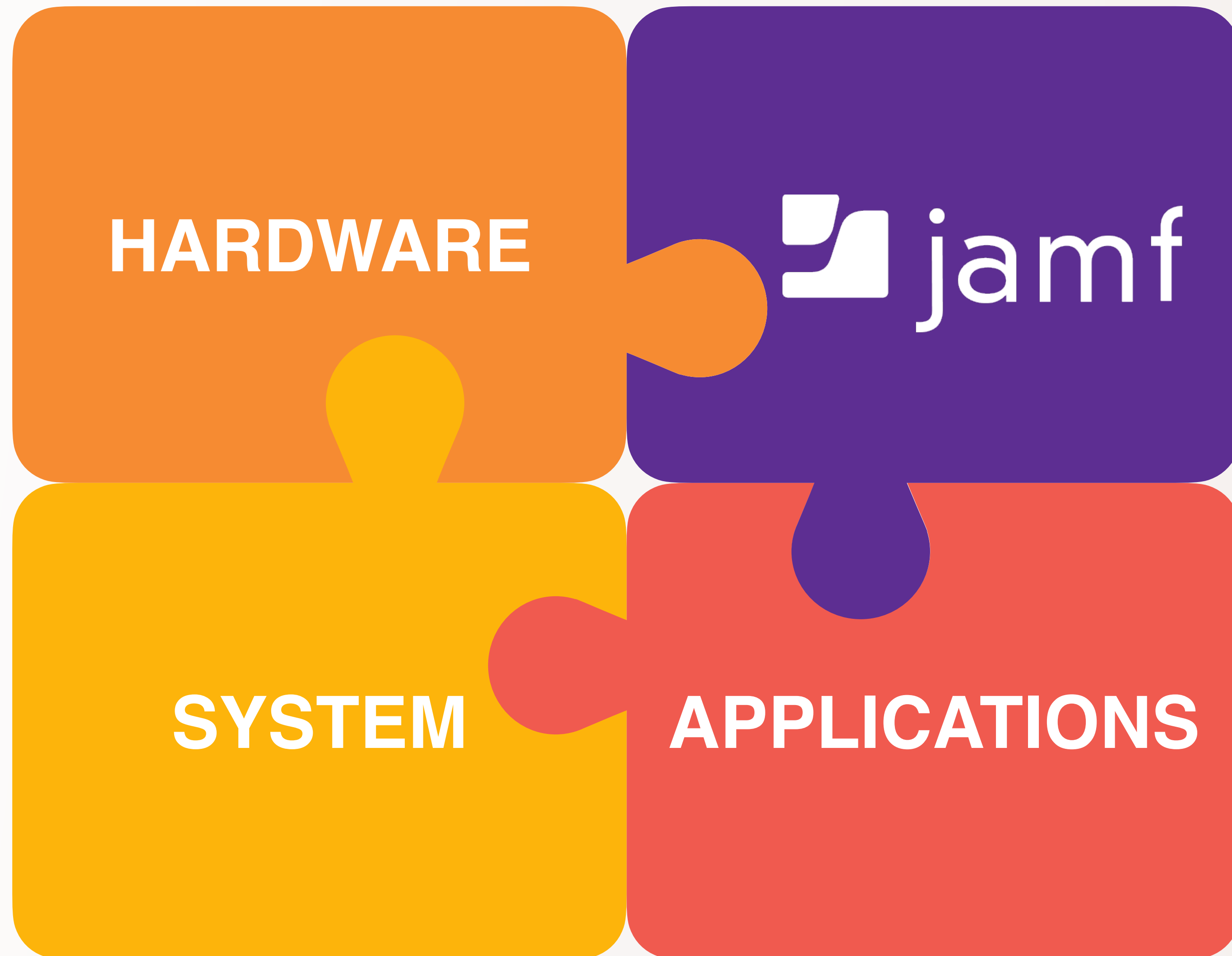




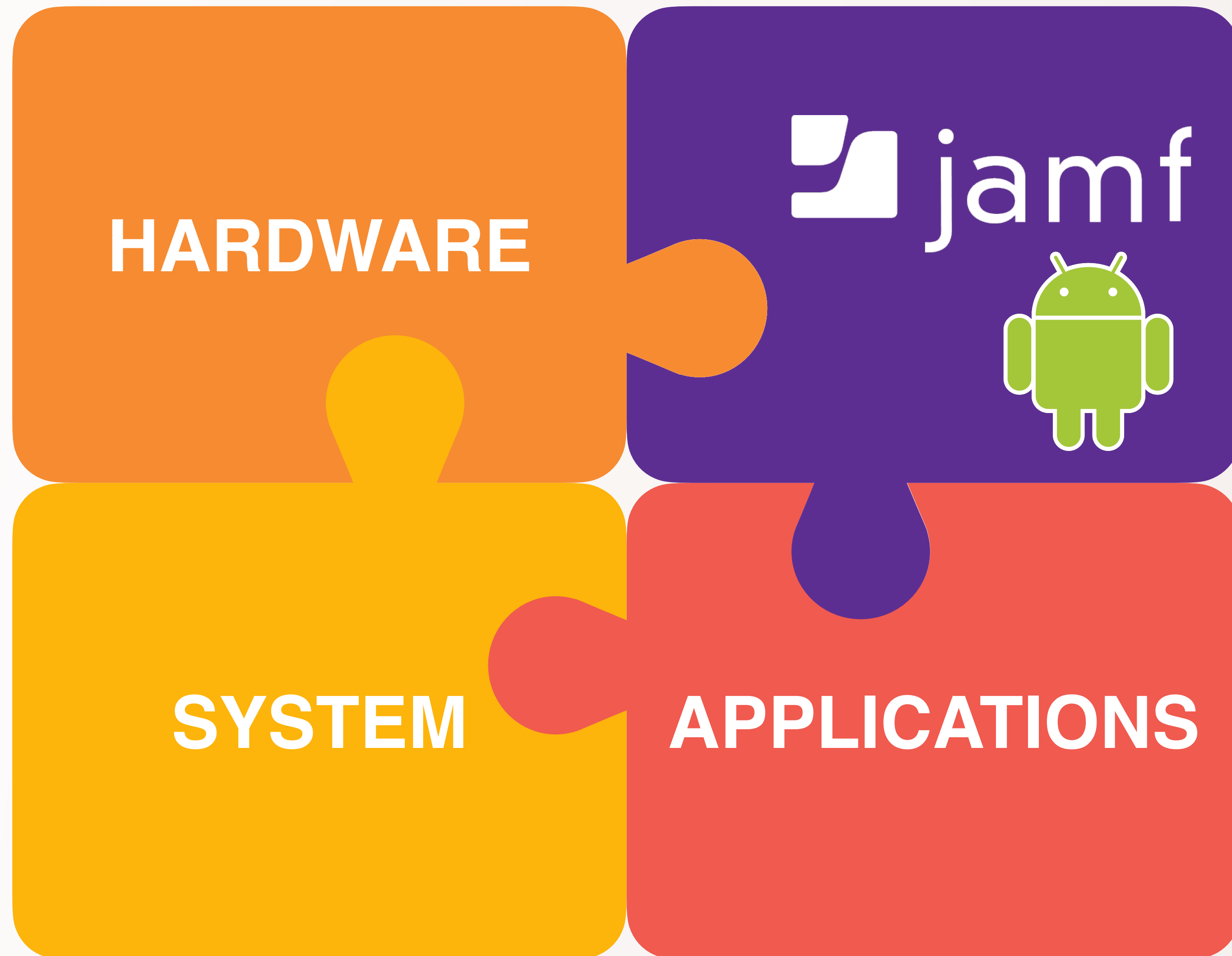
まとめ



安全性と運用効率を両立したモバイル管理



安全性と運用効率を両立したモバイル管理



● **JAMF NATION LIVE**

THANK YOU