

● JAMF NATION LIVE

モバイルDX実現のために 必要となるモバイルセキュリティ

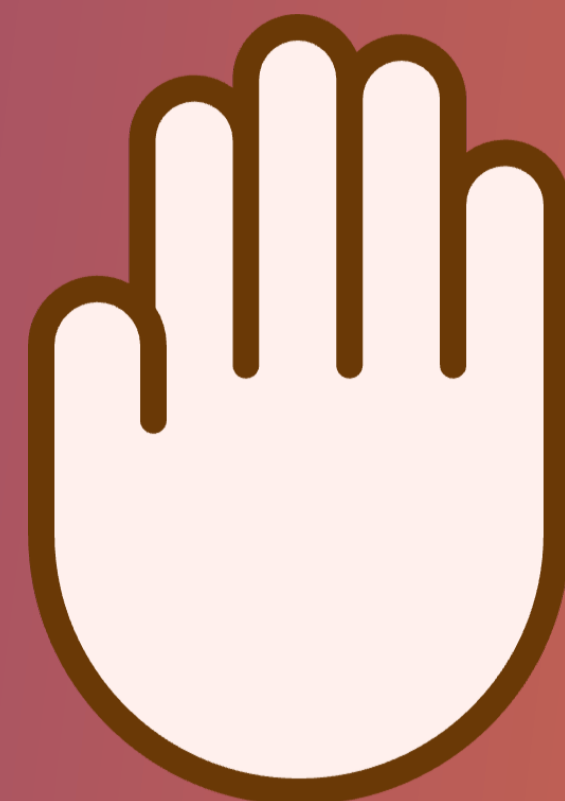


稲葉 祥紀

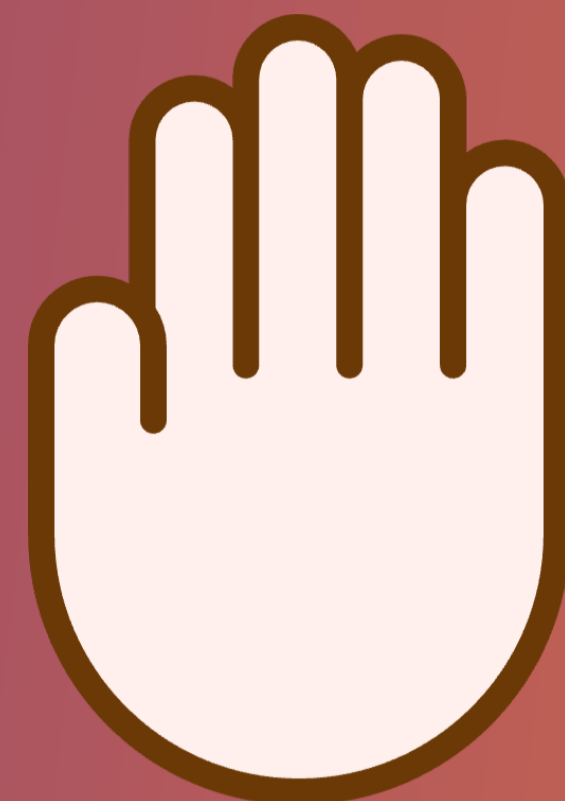
セールスエンジニア／マネージャー

Jamf Japan 合同会社

従業員のス마트フォンは
会社から貸与している



PCと同等のセキュリティ対策を
実施できている



DXとは？

モバイルDXとは？

“企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること。”

経済産業省 デジタルガバナンス・コード2.0



デジタル技術の活用

・

ビジネスモデル・業務プロセスの変革

・

競争優位の確立



ITを用いて

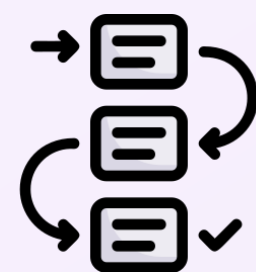
業務・提供価値・ビジネスそのものを

変えること



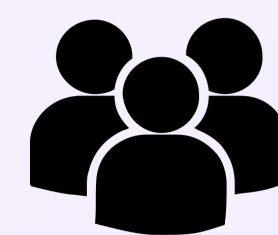
セキュリティ

MFA
WEBフィルタリング
ワイプ・ロック



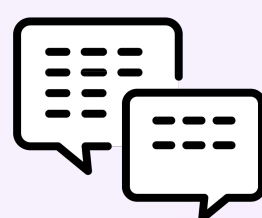
ワークフロー

稟議申請/承認
経費精算
勤怠申請



マネジメント

PJタスク管理
進捗管理・WBS
目標管理・評価



コミュニケーション

カレンダー
チャット
WEB会議



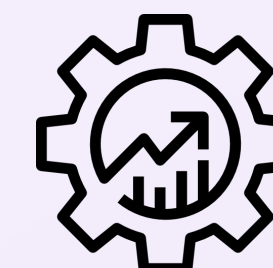
ドキュメント管理

クラウドストレージ
ファイル共有
ナレッジ・ポータル



営業・顧客管理

CRM(顧客管理)
SFA(案件管理)
名刺管理



経営管理

BIダッシュボード
管理会計レポート
予算管理



モバイルDXは

デバイス、時間、場所の制約を取り除く

コミュニケーション

カレンダー
チャット
WEB会議

ドキュメント管理

クラウドストレージ
ファイル共有
ナレッジ・ポータル

営業・顧客管理

CRM(顧客管理)
SFA(案件管理)
名刺管理

経営管理

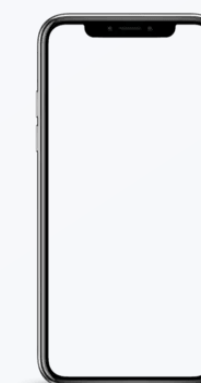
BIダッシュボード
管理会計レポート
予算管理



アクセスできるシステムやデータは同等



セキュリティ対策も同等？



データ侵害 1 件あたりの損害額



世界平均

488万米ドル (約7億円)



日本平均

419万米ドル (約6億円)



医療業界

977万米ドル (約14億円) ※10年以上トップ

攻撃の内訳

外部攻撃 **55%** : 内部原因 **45%**

対策により損害額を大きく削減



AIと自動化の導入で
(EDR/XDR+AI+SOC 等)

220万米ドル削減 (約3.2億円)



予防利用まですると
(ASM+DPSM+AI分析 等)

45.6% 削減



社員教育の徹底

95万米ドル削減 (約1.4億円)

モバイルDXには ”攻め”と”守り”の両立が必要

可用性

機密性・完全性





スマート x SaaS の活用度はどう？ 投資対効果を考える

会社貸与スマホのROIを考えてみる

前提1：ユーザを3タイプに分類 ▶ 働きアリの法則（2-6-2）



会社貸与スマホのROIを考えてみる

前提 2：スマホ 1 台あたりの年間コスト

項目	金額（年間）	備考
端末代	¥20,000	¥80,000/台を4年契約
通信費	¥36,000	¥3,000 x 12ヶ月
管理コスト（MDM等）	¥6,000	
保守・サポート費用	¥5,000	故障対応やITの工数など
合計	¥67,000	

会社貸与スマホのROIを考えてみる

前提 3：スマホ x SaaS の年間コスト（1ユーザあたりの投資額）

項目	金額（年間）	備考
スマホ代	¥67,000	前提2より
各SaaS	¥40,000	1人¥80,000/年でPCとスマホで按分
合計	¥107,000	

会社貸与スマホのROIを考えてみる

前提4：ユーザのタイプ別 ROI

タイプ	利用状況	想定効果額	投資額（前提3より）	ROI
パワーユーザ	SaaSフル活用	¥145,000	¥107,000	1.36
ふつう	コミュニケーション	¥36,000	¥107,000	0.34
ほぼ未使用	電話、MFAのみ	¥6,000	¥107,000	0.06

会社貸与スマホのROIを考えてみる

投資対効果 試算（100名規模）

タイプ	構成比	人数	ROI	投資額（円）	効果額（円）
パワーユーザ	20%	20人	1.36	$20 \times 107,000 = 2,140,000$	$2,140,000 \times 1.38 = 2,910,400$ （黒字）
ふつう	60%	60人	0.34	$60 \times 107,000 = 6,420,000$	$6,420,000 \times 0.34 = 2,182,800$ （赤字）
ほぼ未使用	20%	20人	0.06	$20 \times 107,000 = 2,140,000$	$2,140,000 \times 0.06 = 128,400$ （赤字）
合計	100%	100人	-	10,7000,000	5,221,600

会社貸与スマホのROIを考えてみる

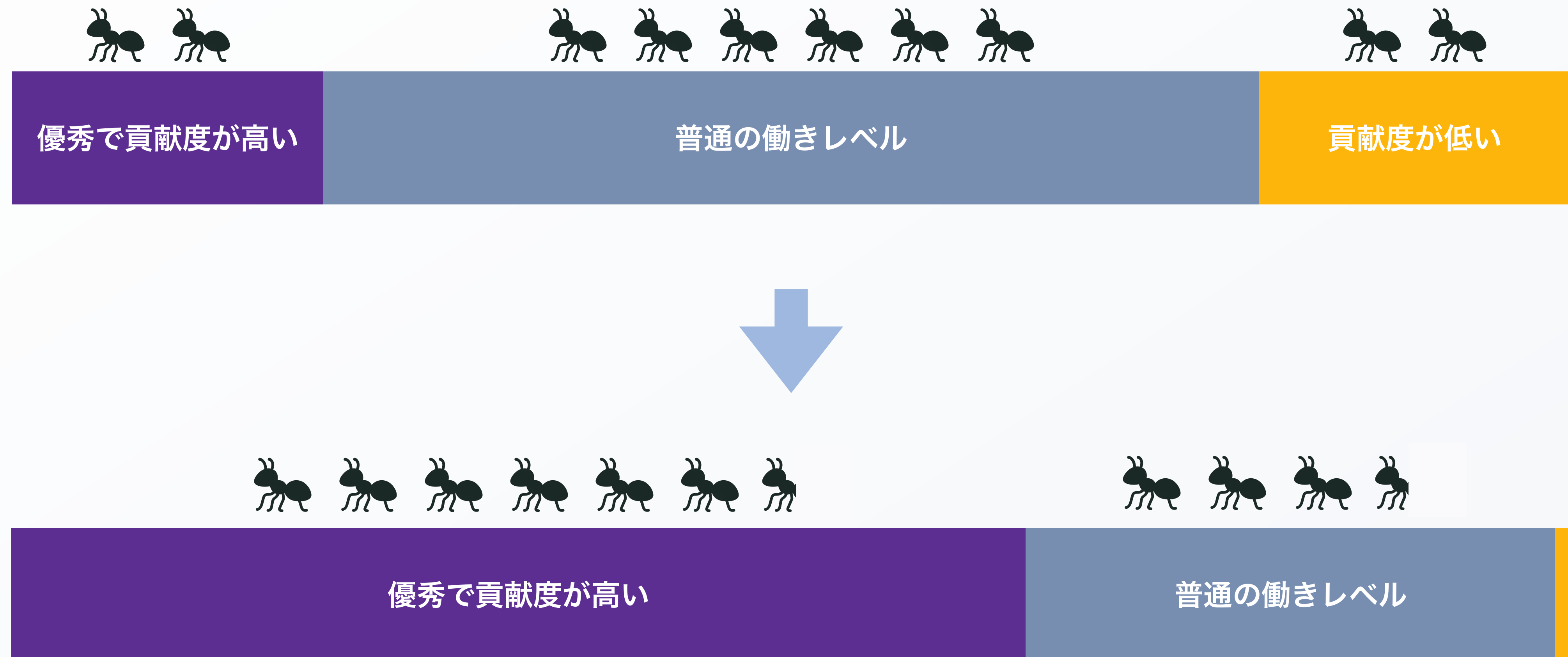
投資額 合計	¥10,700,000
--------	-------------

効果額 合計	¥5,221,600
--------	------------

差分（≡ 損失）	▲ ¥5,478,400
----------	--------------

平均ROI ≒ 0.49（半分しか回収できていない）

会社貸与スマホのROIを考えてみる



なぜ使いこなされないのか？

従業員



- スマホをもっと使いたい
- 移動中にも情報にアクセスしたい
- アプリの使い方が分からない

IT部門



- セキュリティの対応がまだ不足も予算がつかない
- MFAやテザリングのためにスマホを求められることも...
- 運用を増やしたくない
- アプリの教育する時間ない

経営層



- 本当にスマホ必要？
- 費用対効果は？
- 投資判断材料が少ない

なぜ使いこなされないのか？

従業員

IT部門

経営層

三者の意志が微妙に噛み合わず、なかなか進まない



“動かない状態”こそが最大のリスク

- セキュリティの対応がまだ不足も
- スマホを求められることも...
- 運用を増やしたくない
- アプリの教育する時間ない
- 投資判断材料が少ない

モバイルの脅威

Security 360: Annual Trends Report Mobile Devices

実際の脅威データに基づいて
モバイルセキュリティの最新動向と
リスク対策をまとめた年次レポート

Download for free here !



● JAMF NATION LIVE



モバイルの脅威

フィッシング

年間1,000万件以上の攻撃が観測され、**10人に1人が悪意あるリンクをクリック**している

脆弱性

55%以上のスマホがOSを最新に保っておらず、**32%が重大な脆弱性を抱えたまま**企業ネットワークに接続している

アプリリスク

正規アプリに見せかけたマルウェアやTCCバイパスといった手法が使われ、**許可なく**位置情報や写真にアクセスされるケースも

標的型攻撃

Appleは150カ国のiOSユーザに対して、**スパイウェア攻撃の警告**を通知している

所有モデルの多様化？混乱？

COBO

理想

Corporate Owned, Business Only

- 企業貸与
- 業務のみ利用許可

COPE

現実

Corporate Owned, Personally Enabled

- 企業貸与
- 一定の範囲で私的利用許可

CYOD

満足度 ↑

Choose Your Own Device

- 企業貸与
- 企業が指定した機種から従業員が選択
- COBO/COPEと組み合わせ

BYAD

教育現場

Bring Your Assigned Device

- 私用機器
- 許可機種の制限あり

BYOD

響きよし

Bring Your Own Device

- 私用機器
- 許可機種の制限なし

NORA

課題

- 野良
- 未管理、放置

所有モデルの多様化？混乱？

COBO

Corporate Owned, Business Only

- 企業貸与
- 業務のみ利用許可

COPE

Corporate Owned, Personally Enabled

- 企業貸与
- 一定の範囲で私的利用許可

CYOD

Choose Your Own Device

- 企業貸与
- 企業が指定した機種から従業員が選択
- COBO/COPEと組み合わせ

MDMで管理

BYAD

Bring Your Assigned Device

- 私用機器
- 許可機種の制限あり

BYOD

Bring Your Own Device

- 私用機器
- 許可機種の制限なし

MDMで管理したい

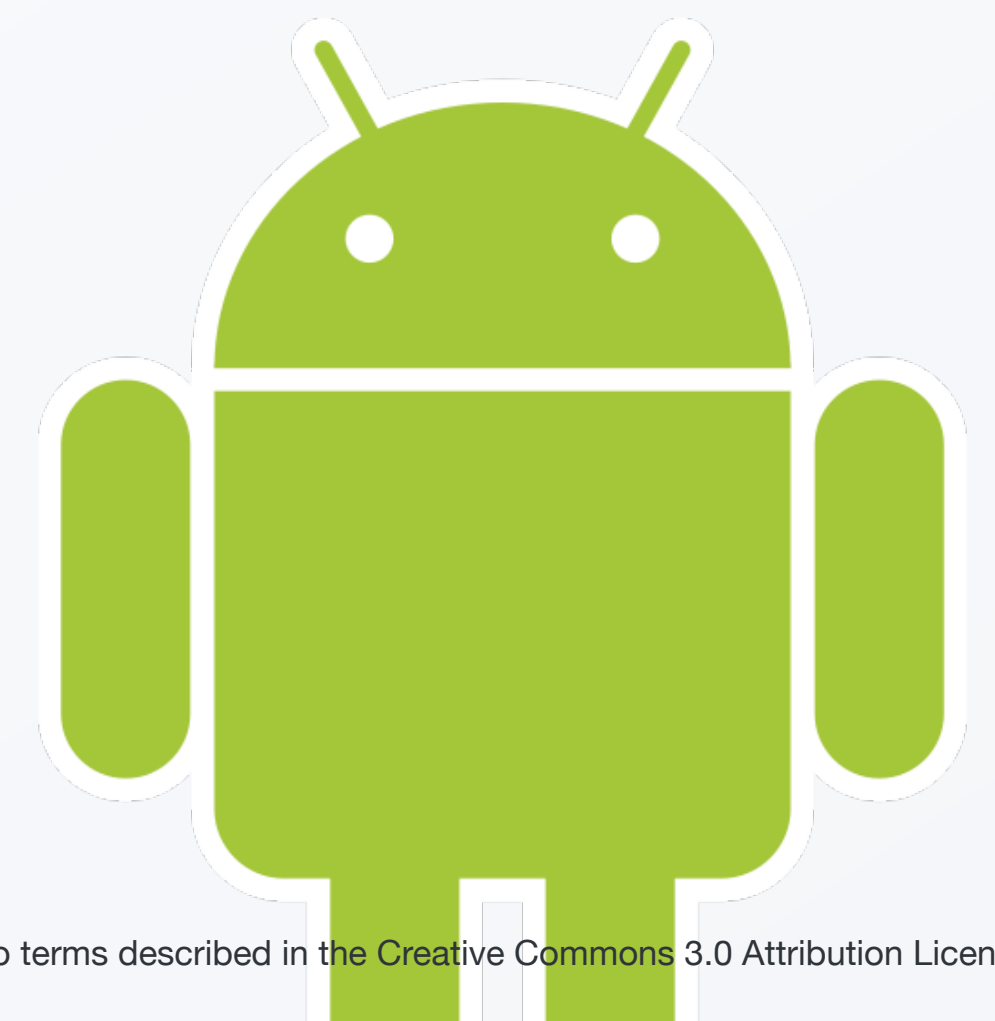
NORA

- 野良
- 未管理、放置

なんとかしたい気持ち

Androidも放置できない

- ▶ Android も業務端末として拡大中
 - ▶ 価格面のメリット、ユーザからみたときの大差ない使い勝手
- ▶ OS 断片化／脆弱性／サイドロード／モデルごとの違いなどiOSとは異なる注意点
- ▶ iOSと”同等のセキュリティ設計”が不可欠に



Jamf が解決します

Comprehensive Mobile management and security for enterprise organizations.

Capabilities



Mobile Management & Security

Zero-Touch Deployment	App Management	Smart Groups	BYOD	Compliance	Data Streams & Risk Signaling	App Risk Monitoring
Reporting	Self Service Workflows	Shared Devices	Vulnerability Management	Web Protection	Data Capping	ZTNA



Platform & Services

Onboarding Services	Integrations & APIs
AI Assistant	Partner Ecosystem
Jamf Account	Jamf Marketplace

Portals

Jamf Pro	Manager for Android	Jamf Security Cloud Portal
----------	---------------------	----------------------------

Platforms

iOS / iPadOS visionOS tvOS watchOS	Android	iOS / iPadOS visionOS tvOS watchOS	Android
---	---------	---	---------

Agents & Apps

Self Service app 	Jamf Companion app 	Jamf Trust app 
---	---	---

紛失デバイス対策
(リモートロック/ワイプ)

BYODの管理

フィッシング・マルウェア対策

インベントリ・資産管理

パスワードや機能のポリシー適用

ウェブ保護・コンテンツフィルタリング

OSアップデートの管理

共有デバイスの管理

ゼロトラストネットワークアクセス
(ZTNA)

アプリケーション配布・更新管理

セルフサービスポータル提供

セキュアな通信

不要アプリ・Siriの制限

ポリシー適用対象の動的管理

リスクシグナリングによるアラート検知

不要プロファイル・証明書のブロック

データ通信量の制限

脆弱性管理

キッティングを楽しみたい

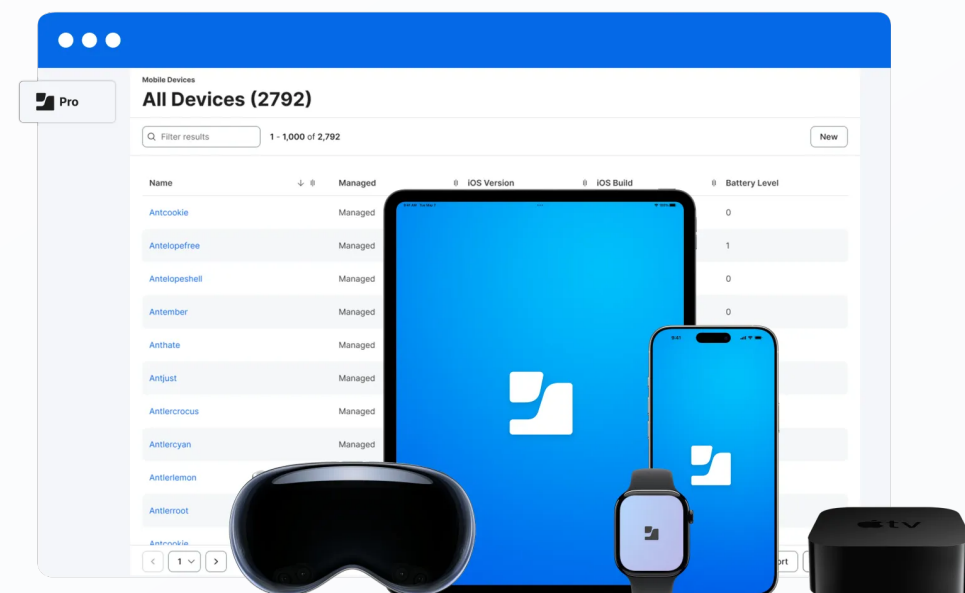
Apple Intelligenceを制限したい

監査の回答を楽しみたい

MDM

Mobile Device Management

デバイスの構成管理、OS/Appのバージョン管理、リモートロック/ワイプ等の紛失対策、BYOD管理 等



iOS / iPadOS

MTD

Mobile Threat Defense

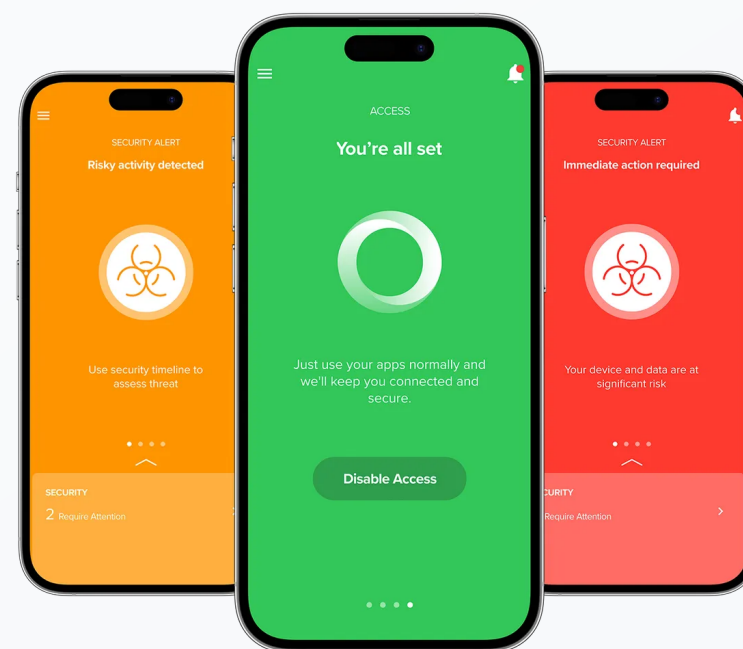
Webの脅威に対する検知・防御（フィッシング、悪質なアプリ、ゼロデイ攻撃などへの対策） 等



ZTNA

Zero Trust Network Access

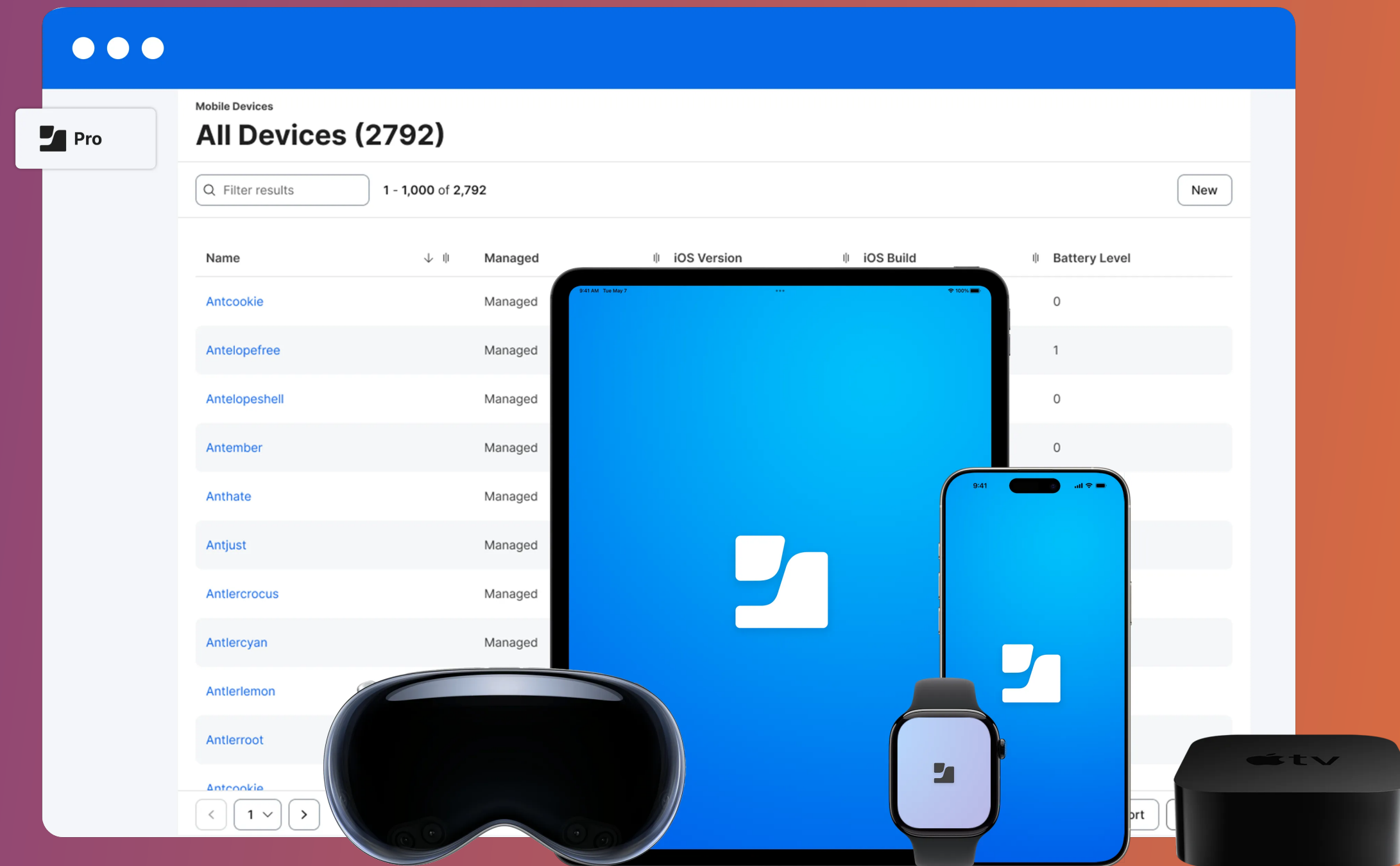
信頼できるユーザ＋安全なデバイス
＝ 仕事のリソースへのアクセス許可



Android



for Mobile



所有形態問わず、生産性をすぐに発揮できる登録機能

Webの脅威からデバイスを保護し、IT投資効果を最大化

高度な監視・検出・修復で多種多様なリスクに対応

OS・アプリを常に最新で安全な状態に維持

SSOや初期化、トラブルの自己解決の支援など、最適なエクスペリエンスをさらに強化

何かからすればよい？

モバイルセキュリティ診断



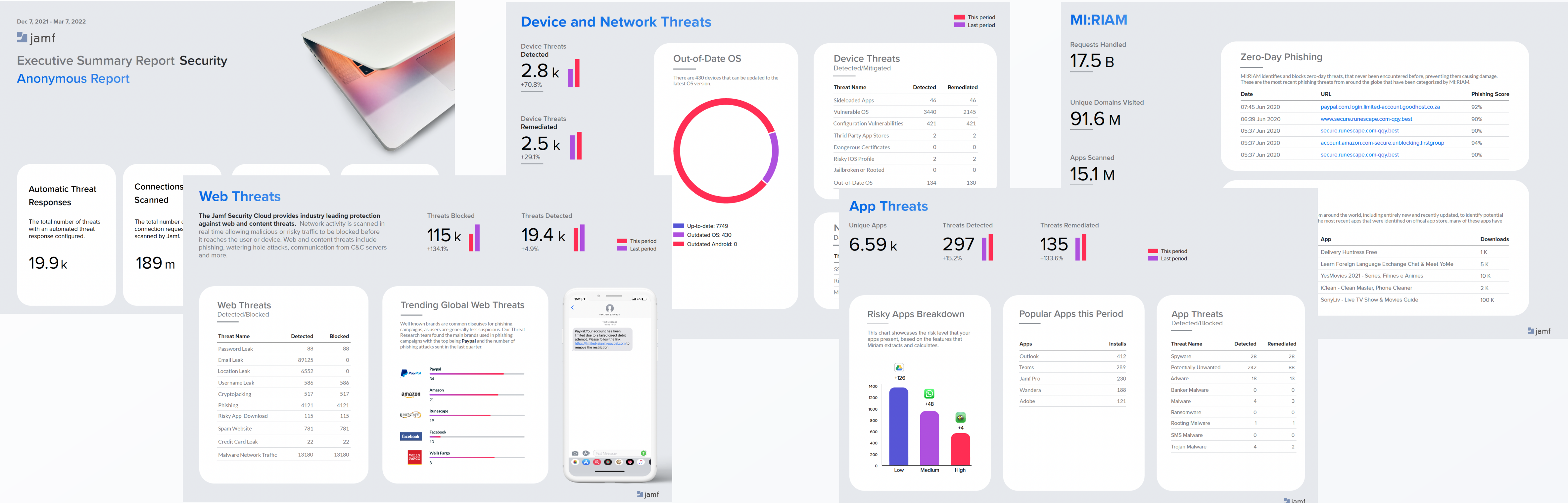
・

無償



● JAMF NATION LIVE

現状のリスクの可視化から



モバイルDXには”攻め”と”守り”の両立

可用性

機密性・完全性

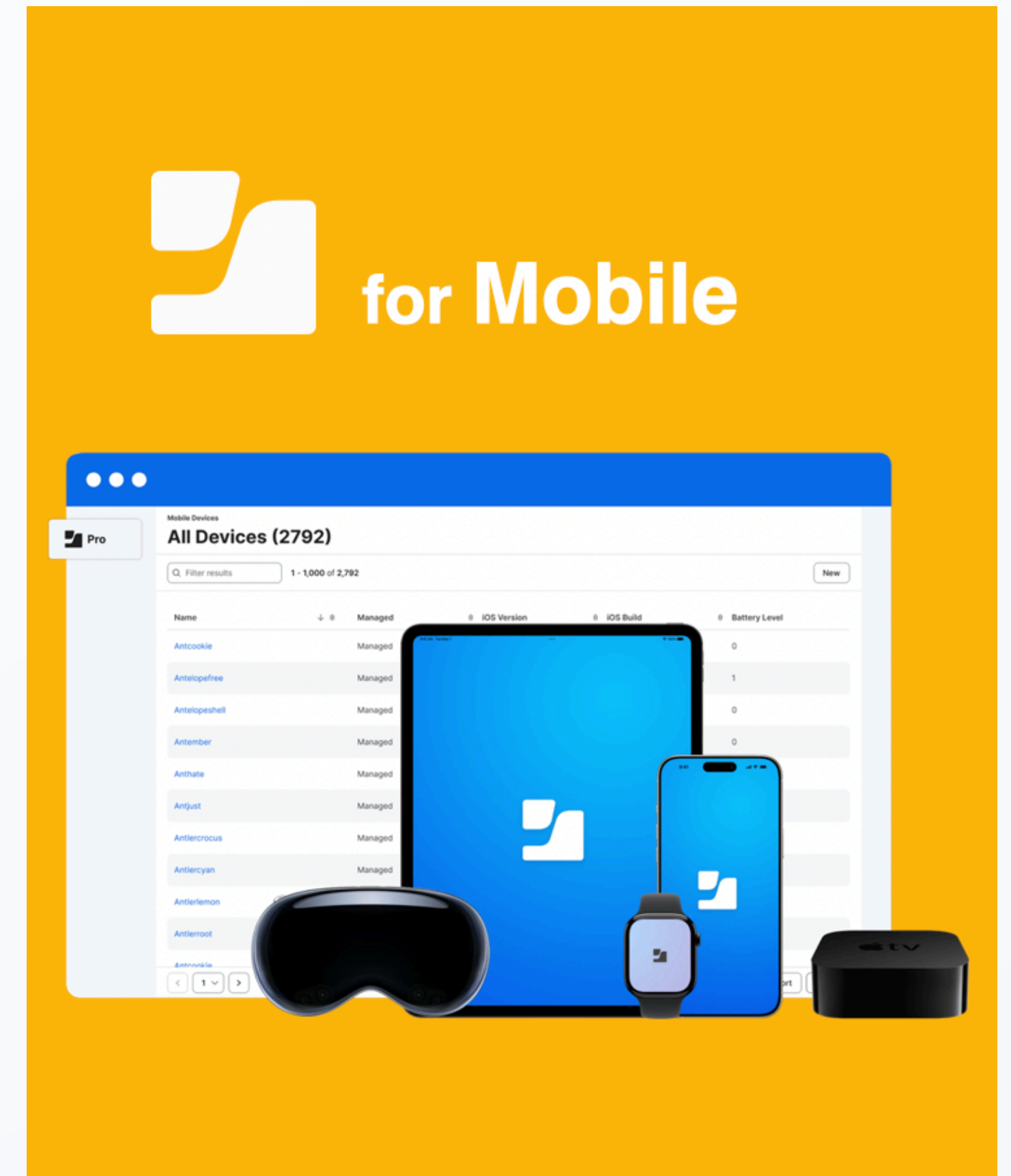


for Mobile

モバイルセキュリティを整え、モバイルDXの実現へ

スマホ x SaaS の
効果の可視化
ToBe の設定

モバイルデバイスの
課題の把握
AsIs の整理



● **JAMF NATION LIVE**

THANK YOU

Thank you



関連セッションのご案内

15:00 - 15:30

Hall B

グローバル展開におけるAppleデバイス管理、
Android デバイス管理とセキュリティ

15:45 - 16:15

Hall C

iPhoneをJamfProでBYODして管理しよう！

17:15 - 17:45

Hall B

モバイルセキュリティを実現する！Jamf Pro APIを活用した
セキュリティ対応の『自動化』とモバイルアプリのセキュリティ標準