jamf

拡大し続けるセキュリティギャップ。解消するための方法とは。

ハイブリッドワークとモバイルデバイスが浸透し、それに伴って脅威も高度化した今、境界型のセキュリティは限界に。未来を拓くのは多層型のアプローチ。

従来型が通用しない理由

境界は消えたが、リスクは消えていない。

デバイスの増加	→	攻撃対象領域の拡大
モバイルの増加	→	制御の弱化
複雑さの増大	→	対応の遅れ

クラウドサービス、リモートワーク、BYOD、信頼できないネットワークの普及により、従来のツールが保護の対象としていた境界は曖昧になっています。

脅威を取り巻く現状

今日の脅威は、高度化し、複合化し、執拗化している。

1億以上
最近のデータ侵害で漏えいした顧客記録の件数

21億
2023年に実行された既知の脆弱性を持つダウンロードの数

2,500万ドル
CFOを標的にしたディープフェイク攻撃の被害額

90%以上
攻撃のうち暗号化ではなくデータの窃取を狙う攻撃の割合

主要な脅威カテゴリ

ソーシャルエンジニアリングとフィッシング
Eメール型、スピア型、ホエーリング型、スミッシング型、ビッシング型、QRコード型フィッシングに加え、偽装機内モードや偽装ロックダウンモードといった新たな手口も出現

国家主導型/APT攻撃
アラートの90%は重要インフラ以外から発生。主な標的：教育機関、政府機関、シンクタンク。インシデント1件あたりの平均被害額：160万ドル

サプライチェーン攻撃
2023年に3倍に増加。パートナーやサプライヤを間接的な侵入口として悪用

モバイルデバイスを狙う脅威
侵害を受けたデバイスの43%が完全に乗っ取られた状態に（前年比187%増）。フィッシングサイトの80%はモバイルデバイスが標的。新型のモバイルマルウェアは51%増加

AIを活用した脅威
少なくとも5つのAPTグループがAIを武器化して攻撃能力を強化

国家主導型の脅威

数字で見る標的型攻撃の実情

主要な標的

- 教育機関：100%
- 政府機関：75%
- シンクタンク/NGO：69%
- IT組織：69%

10社中9社
国家支援を受ける攻撃グループから攻撃を受けた可能性があると回答

160万ドル
国家主導型インシデント1件あたりの平均被害額

汎用型が通用しない理由

デバイスを取り巻く状況が劇的に変化。

オフィスに固定されたデスクトップコンピュータ向けに設計されている従来のソリューションでは、今日の動的かつマルチデバイスな環境を保護することはできません。

25%
米国におけるmacOSの市場シェア

96%
12～24ヶ月以内にMacデバイス数が増加すると予測するCIOの割合

3.6
世界におけるユーザ1人あたりの平均デバイス数（2023年）

96%
企業ネットワーク上のモバイルデバイスのうち個人所有の割合

モバイルデバイス：未対策のリスク

モバイルデバイスは誰も警備していない玄関。

平均的なユーザが所有するデバイスは3.6台。つまり1人あたりの攻撃経路は以前の約4倍に増加しています。そのほとんどで専用のエンドポイントセキュリティが講じられていません。

43%
侵害を受けたデバイスのうち完全に乗っ取られた割合（前年比187%増）

80%
フィッシングサイトのうちモバイルデバイスを標的にしている割合

51%
新型のモバイルマルウェアの増加率（92万サンプル以上）

96%
企業ネットワーク上のモバイルデバイスのうち個人所有の割合

戦略的フレームワーク

セキュリティギャップを解消する4つのC

1. **一貫性（Consistency）**
デバイスの種類、サイズ・形状、OS、オーナーシップモデルに関わらず、すべてのエンドポイントを同様に扱う。

2. **コンプライアンス（Compliance）**
テレメトリデータを活用して、ベースラインを確立し、逸脱を監視し、監査可能な証拠を維持する。

3. **統合（Consolidation）**
IT担当者とセキュリティ担当者を1つのチームとして結束させてサイロ化を解消し、インテリジェンスの共有と業務フローの一元化を図る。

4. **コスト削減（Cost savings）**
ネイティブツール、自動化、プロセスの効率化、BYODプログラムを通じて、ROIを向上させる。

多層型セキュリティモデル

多層防御＝他の層が逃した脅威も別の層で捕捉。

脅威が1つの防御層をすり抜けたとしても、次の層がそれを阻止。以下の3つの基盤を統合することで、インフラ全体にわたる救急時対策を構築できます。

デバイス管理
大規模なデバイス環境でも、構成を展開し、ポリシーを適用し、制御を維持

アイデンティティ（ID）＆アクセス
保護対象リソースへのアクセスを許可する前にユーザとデバイスを認証

エンドポイントセキュリティ
あらゆるデバイスの脅威をリアルタイムで検出・対応

管理＋ID＋セキュリティ → 多層防御

主要なテクノロジー

各層の実際の機能

ゼロタッチ導入
初めて電源を入れた時からデバイスを保護状態に。企業所有デバイスとBYODデバイスの両方で、セットアップ時に設定・アプリ・ポリシーが自動的に展開されます。

脅威ハンティング
ベースライン、テレメトリ、自動修復ワークフローを通じて、未知の脅威も未然に検出します。

ZTNA
絶対に信頼せず、必ず検証。従来のVPNに代わってZTNA（ゼロトラストネットワークアクセス）が、暗号化されたマイクロトンネル、最小権限アクセス、継続的な健全性チェックを実現します。

高度な脅威対策
IoC/IoA分析、タイムラインの作成、APT（持続的標的型攻撃）の排除を実現。数週間かかっていた調査を数分に短縮します。

導入の成果

実装するメリット

デバイス全体にわたって保護を強化

脅威の検出から対応までを高速化

業務の負担を軽減

環境全体で一貫したセキュリティを実現

組織全体にわたる統合型多層防御セキュリティを構築するフレームワークの詳細をぜひご確認ください。

jamf

ホワイトペーパーをダウンロード