jamf

モバイル活用を次のステージへ

# Jamf for Mobile



**対応デバイス**

iPhone、iPad、Apple Watch、Vision Pro、Apple TV、Android

## Jamf for Mobileがモバイルセキュリティをサポート。企業の大切なリソースを守り、モバイル活用の幅をさらに広げていきます。

Jamf for Mobileは、デバイス管理からセキュリティ対策、安全なアクセスまでカバーするオールインワンソリューション。
Jamf for Mobileで、モバイルを守り、その力を最大限に活用して、モバイルを企業成長の原動力に。iPhone・Android両方に対応。

ご存知ですか？

今やビジネスに欠かせない存在となったモバイル。
利用シーンの広がりや重要性の高まりとともに、攻撃者の標的になるリスクが増えています。

## 世界中のWeb閲覧の 62% 以上はモバイルデバイスから

### OS・アプリの脆弱性の脅威

**55%**
**OSの脆弱性が修正されていない業務用モバイルデバイスの利用割合**
業務で日常的に使うスマートフォンが、攻撃者にとっての"入り口"に。更新されていないOSは、サイバー攻撃の格好の標的になります。

**32%**
**重大な脆弱性に未対応のモバイルデバイスを保有している企業の割合**
3社に1社がセキュリティホールを抱えたモバイルを業務に使用。そのデバイスが社内ネットワークにリスクを持ち込ませるきっかけに。

**4.3万**
**隠された機能や未申告の仕様でAppleに却下されたアプリの数**
普段使っているアプリにも、見えないリスクが。「便利そうだから」とインストールしたアプリから知らないうちに情報を抜き取られている可能性も。

### フィッシング攻撃の脅威

**90%**
**全サイバー攻撃のうちフィッシングから始まる攻撃の割合**
OSやデバイスの種類に関係なく、攻撃のほとんどがフィッシングから。従業員がクリックしてしまったリンクがリスクの入り口になっています。

**1/10人**
**フィッシングのリンクをクリックした従業員の割合**
多くの従業員がフィッシングと気づかずにリンクをクリックしてしまっています。不正アクセスや情報流出を招く重大リスクに。

**1.5倍**
**PCと比較したモバイルのフィッシング攻撃成功率**
「スマートフォンなら安全」と思っていませんか？実は、モバイルの方がフィッシング攻撃の成功率が高く、より狙われやすい状況にあります。

出典：Jamf Security 360: Annual Trends Report Mobile Devices（Jamf セキュリティ 360 最新トレンドレポート 2025年度版 モバイルデバイス編）

## Jamf for Mobileがモバイルをリスクから守り、最適な活用を実現します。

# 守りながら活かすJamf for Mobileの特徴

## デバイス管理

役職や利用状況に応じたデバイスのグルーピング管理、OS・アプリのバージョン管理、アプリの一斉配布など、業務で利用するモバイルデバイスを一括管理。
リモートロックやワイプ等の紛失対策はもちろん、スムーズな導入、プライバシーにも配慮したデバイス登録でセキュアなBYOD管理も実現します。

## セキュリティ
### ー モバイル脅威防御 ー


フィッシングや悪質なアプリなどWeb上に存在する様々な脅威を検知し、モバイルデバイスを守ります。
デバイスに存在する既知の脆弱性もレポートし、OSバージョンのアップデートを促進することができ、デバイスの状態を最新に保つことも可能です。

## 安全なアクセス
### ー ID・アクセス管理 ー

アプリやリソースへのアクセスを、煩雑な作業なしで安全に。
セキュリティポリシーに準拠したアクセスを実現します。
デバイスのセキュリティ状態に応じて、社内リソースへのアクセスも制御し、モバイルデバイスからの安全なアクセスを可能にします。

# モバイル活用の最適化を実現する主な機能

### マルチOS管理
デバイス管理

iOS中心の環境でも、Androidデバイスを含めて一元管理。すべてのモバイルに統一されたセキュリティポリシーとコンプライアンス基準を適用し、混在環境でも安全かつ効率的な運用を可能にします。

### MTD（モバイル脅威防御）
セキュリティ

フィッシングや悪意あるアプリ、不正なWi-Fi接続など、モバイル特有の脅威をリアルタイムで検知・防御。デバイスとネットワークの双方の脅威から、業務用モバイルを強力に保護します。

### BYOD (Bring Your Own Device)
デバイス管理

個人所有のスマートフォンでも、業務利用が可能に。iOS／Android問わず、従業員のプライバシーを守りながら、企業の機密情報も確実に保護。“2台持ち”からの解放と、柔軟な働き方を両立します。

### 脆弱性管理
セキュリティ

OSやAppの脆弱性は常に攻撃の対象に。OSやアプリに潜む既知の脆弱性を可視化し、影響度に応じた対応を促進。デバイスを常に最新・安全な状態に維持することで、攻撃リスクを最小限に抑えます。

### ゼロタッチ導入
デバイス管理

組織の設定や業務アプリ配布などの初期設定を自動化。IT管理者のキッティング作業を削減しながら、従業員はデバイスを開封したらすぐに業務利用が可能に。大規模導入でも、企業ポリシーに準拠した統一運用を実現します。

### ゼロトラストネットワーク
安全なアクセス

社内リソースや業務アプリへのアクセスを、MDM管理下のデバイスと認証済みユーザーに限定。VPN不要で、どこからでも柔軟で安全な接続を確立。さらに業界最先端の暗号化技術により、安心のアクセス環境を提供します。

jamf

https://www.jamf.com/ja/



※本資料の記載内容は2026年1月現在のものです。

お問い合わせ
japan@jamf.com

Jamf for Mobile　検索

製品ページおよび
無料トライアルはこちらから