jamf

購入者向けガイド：企業のモバイル管理ソリューション

モバイルで解き放つビジネスの可能性

企業のモバイル活用が進む中で増大するセキュリティリスク

企業の真のモバイル活用を実現するためには、運用状況の把握、安全なアプリケーションアクセス、そして組織とユーザのニーズを満たすデバイス管理が欠かせません。

現場スタッフからオフィスワーカーに至るまで、業務効率化と生産性向上の観点から、モバイルデバイスの活用が急速に広がっています。多様な環境で利用されるモバイルデバイスの保護は、日々進化するセキュリティ脅威への対応も含め、企業の重要な課題となっています。組織の競争力を高めるには、快適な操作性を確保しつつ、新しい働き方による生産性向上の両立が求められています。

堅牢なモバイルセキュリティ対策に必要な要素：

モバイルフィッシング対策

モバイルデバイスのフィッシング被害リスクは、PCの**1.5倍**

- **攻撃のブロック**
- 利用ポリシー**の徹底**
- **業務効率化に向けたデバイスとユーザの**環境の整備
- アプリの総合的なリスク対策（脆弱性管理・マルウェア対策）
- 堅牢なフォレンジックによる**不正アクセスの検知**
- モバイルデータ通信量**の制御と利用超過防止**
- **モバイル運用基準の設定と**コンプライアンスの徹底
- **業務アプリや社内システムへの**安全なアクセス環境**の提供**
- **セキュリティ**設定ミス**の防止**

主な特徴:

企業のモバイルデバイスを最大限活用する主要機能

セキュアな構成管理

モバイルデバイスのセキュリティ強化

- セキュリティ基準の確立
- コンプライアンス監査の実施
- 構成の脆弱性の監視

パッチ管理

- 詳細な脆弱性レポートに基づき、パッチ適用の重要度を判断
- OSとアプリの脆弱性から生じるリスクを最小化

データ損失防止

- アプリ間のデータ連携を制御
- ユーザやデバイスの状態に応じて、アプリへのアクセスを制限

利用規約

- 脅威やコンテンツのカテゴリに基づいて柔軟にWebサイトへのアクセスを制御
- 利用ポリシーの適用範囲を、ユーザ、グループ、地域ごとに設定

攻撃対策

マルウェア・その他アプリのリスク管理

- マルウェアをブロック
- 脆弱性やリスクのあるアプリを特定
- アプリからの機密情報漏洩を防止
- 非公式アプリストアの利用状況を監視

中間者攻撃

- 不正アクセスポイントやプロトコル攻撃の検知
- 暗号化されたトンネルによる中間者攻撃対策

Web脅威

- ゼロデイ攻撃を含むフィッシング対策
- C2やデータ抽出などの悪意ある通信を遮断
- クリプトジャッキングやスパム、その他のWeb上の脅威を無効化

デバイス管理

導入&登録

- デバイスをエンドユーザや拠点へ直送
- 所有形態を問わないデバイス導入
- デバイス、ユーザ、アプリケーションの一元管理による業務効率化

設定&構成

- デバイス管理の自動化と大規模展開を実現
- 目的に応じたデバイスの利用制御
- セキュリティ要件を満たすデバイス運用管理

インベントリ&レポーティング

- IT資産の可視化（人・モノ・システム・セキュリティの一元管理）
- インベントリ項目のカスタマイズによる詳細な状況把握

オンデマンドコンテンツ

- 従業員自身による承認済みアプリのリクエスト・ダウンロード・アップデートを可能に

業務フローのカスタマイズ

共有デバイスの管理・運用

- 使用用途に応じたデバイスプロビジョニング・カスタマイズ・リフレッシュ
- 業務アプリへの即時アクセスを提供
- 役割に応じた構成でデバイスをカスタマイズ
- 現場管理者によるIT部門不要の基本サポート対応を実現

パートナーソリューション連携とAPI活用

- 即導入可能なソリューション・連携機能を Jamf Marketplace で提供
- 医療・小売・建設・航空業界に特化した主要パートナー
- 電子カルテ/EMRシステムとの連携による医療機関デバイス管理の効率化
- Jamf APIによる柔軟なシステム連携・ワークフロー統合の実現

セキュアなアクセス

通信中データの保護

- 重要な業務アプリやデータアクセスの暗号化トンネリング構築

重要業務アプリの利用状況分析

- モバイルデバイスからのアプリの利用状況の可視化

リアルタイムアクセスポリシーの実行

- ユーザ属性とデバイス状態に基づくアクセス制御ポリシーの設定

脅威の検出と対応 (TDR)

高精度テレメトリデータの収集

- オフライン分析用に詳細なログ収集

アノマリ検知

- 悪意のある活動の痕跡を探知する脅威ハンティング機能の実装
- IoC及び新規知見の脅威インテリジェンス統合による検知能力の強化

脅威修復

- 侵害検知時における業務アプリやワークロードへのアクセス制御
- マルウェアの駆除と業務環境の復元

Jamf で実現するゼロトラストセキュリティ

Jamf は、登録済みデバイスと認証済みユーザのみが、セキュリティ要件を満たした状態で重要な業務アプリケーションにアクセスできる環境を実現し、組織の重要な情報資産を保護します。

モバイルセキュリティ機能の選択は慎重に

セキュリティリスクも働き方も、常に進化し続けています。昨日まで有効だった対策が、今日の安全性を保証するとは限りません。そして、今日の働き方は明日には変わっているかもしれません。このような状況下で、効果的なセキュリティ対策を実現するためには、適切なソリューションの選択が不可欠です。ここでは、モバイルセキュリティソリューション選定における重要な評価ポイントをご紹介します。

ソリューションの機能を詳しく精査する

「モバイルセキュリティ」機能を謳っているというだけでは十分ではありません。ソリューションが実際にどのような機能を備えているのかを詳細に確認することが重要です。適切なソリューションは、単にコンピュータのセキュリティ概念をモバイルデバイスに当てはめるのではなく、モバイルデバイス特有の脅威に対応し、かつユーザ体験にも配慮したものであるべきです。

セキュリティにはデバイス管理が不可欠

セキュリティソリューションを1つ導入しただけでは、すべての要件を満たすことはできません。また、セキュリティソフトウェアの導入だけでは不十分です。可視化できないデバイスを守ることはできません。そのため、デバイス管理はセキュリティ対策の基盤となります。デバイス管理ソフトウェアにより、セキュリティ要件への準拠を確保し、リスクを事前に特定・対処できます。

ユーザエクスペリエンスが重要

モバイルデバイスは、どこにいても業務を継続できる機動力を備え、従業員の働き方をより効率的にします。この利便性を活かすためには、セキュリティと使いやすさのバランスが重要です。過剰な制限は、かえって従業員を危険な代替手段に導く結果となりかねません。

モバイルデバイスは、今やビジネスに不可欠なツールとして定着しています。デバイスに対するセキュリティ制御が必要となった場合でも、業務の中断を最小限に抑える対応フローを事前に確立しておくことが重要です。

すべてのデバイスに対して同一のセキュリティ対策が求められるわけではありません。セキュリティ対策やポリシー構成を適用する際は、ビジネスの実態と利用状況を踏まえて十分に検討しましょう。例えば

- まずは、従業員が実際にどのようにデバイスを活用しているのかを確認しましょう。役職や業務内容によって、セキュリティリスクは異なります。具体的には：
  一般的な従業員の場合、業務上の機密情報を扱いWebも利用するため、標準的なセキュリティ対策が不可欠です。デバイスには常にセキュリティ要件を遵守させ、フィッシング攻撃やマルウェア感染から防御する必要があります。セキュリティをより強固にするため、コンテンツフィルタリング、脅威防御、ゼロトラストネットワークアクセスを活用します。
- 一方、小売店などの現場スタッフには、コンテンツフィルタリングやアプリの安全性確保が効果的です。ブラウザへのアクセスがないデバイスでは、フィッシングのリスクは相対的に低くなります。
- 経営幹部や機密情報を扱う立場の人々は、攻撃の標的になりやすく、高度なセキュリティ対策と各種規制要件への対応が必須となります。

© 2025 Jamf, LLC. All rights reserved.

モバイルDXで業務に変革を
導入のご相談は、Jamfのエキスパートまで