

現場作業者のための 技術革新

管理者に必要なセキュリティ情報と、
ユーザが求める使いやすさを両立



デスクレスワーカーの60%以上
が、支給されているテクノロジーに
不満があるか、改善が必要だと感
じています。

McKinsey & Company Technology Trends Outlook 2022



航空業や製造業、フィールドサービスなど、屋外で働く従業員がいる企業では、モバイルファースト戦略を導入することで現場作業の柔軟性と生産性を高めることができます。この戦略には、現場にとってのメリットだけでなく、組織や顧客のデータの保護体制を強化する効果もあります。

モバイルデバイスの導入・運用では、モバイル管理部門およびセキュリティ部門に以下のような課題が生じがちです。

- デバイス/アプリのセキュリティとユーザエクスペリエンスの両立
- ユーザのニーズまたはデバイスの用途に応じたカスタマイズ
- リスクを管理・軽減するためのデバイスとアプリの情報の取得
- 生産性を高めるアプリやリソースへのアクセスの保護および認証
- ビジネスプロセスを強化するデバイスワークフローの導入

もしユーザエクスペリエンス、生産性支援、セキュリティのすべてが一体となり、相乗効果を生み出せるとしたらいかがでしょうか。

Jamfが、それを可能にします。

Jamf のプラットフォームは、モバイル部門やセキュリティ部門が必要とするデバイス管理・アプリ管理・条件付きアクセスを提供します。しかも快適なユーザ体験も提供することができます。Jamfのアプリとパートナーエコシステムを利用してことで、各従業員への個別デバイスの配布からデバイスの共有、タイプやオペレーティングシステム(OS)の異なるデバイスの混合運用まで、多様な展開シナリオでモバイルファースト戦略を導入できます。

モバイルデバイスの可能性を広げよう



デバイスとユーザの登録

デバイスとアプリの一括管理を自動化・拡張し、業務用デバイスの構成を常に最適化。デバイスを共有する場合も、事前設定済みの役割/デバイス別構成を使用して業務に応じたアプリ設定を提供することができます。



利用規定の適用

デバイスで危険性の高いコンテンツや規定違反サイトを禁止し、利用規定に基づいた安全な運用を実現します。あらゆるアプリやブラウザに対応したフィルタ機能で、カテゴリまたはドメイン別に制限を定義できます。



モバイルデバイスのベースラインの設定

CIS BenchmarksやNIST、AC 91-78A、CMMCなどの標準に従ってセキュリティベースラインを設定し、デバイスのコンプライアンスを検証して、高度な脅威への対策を確立できます。



モバイルデバイスのデータ利用の管理

モバイルデバイスのデータ通信量を管理し、国内や海外でのローミング中におけるデータの使いすぎを抑制。通信コストを抑え、想定外の超過料金が発生する事態を防止します。



アプリとOSのリスクの管理

アプリ/OSのバージョンが古くなるか、リスクが生じた場合に自動でアップデートします。脆弱性やアプリの危険な挙動、CVE（共通脆弱性識別子）を監視し、不正なアプリやサイドローディングされたアプリを禁止または非表示にできます。



ユーザのアプリアクセスの保護

業務用リソースへのアクセスを、許可したデバイスを使用する信頼済みのユーザに限定します。Jamfなら、リスクを意識したアクセスポリシーとアプリごとの接続により、従業員の生産性を高めるためのアプリやデータへのゼロトラスト接続を実現できます。



ウェブ脅威防御

Jamf製機械学習エンジンの「MI:RIAM」がフィッシング、クリプトジャッキング、悪意あるドメインなどの脅威を未然に防ぎ、リアルタイムでユーザとデバイスを保護します。



主要業界を知り尽くす専門知識

Jamfは、製造業、建設、航空、小売、ヘルスケアなどの大手企業と提携し、幅広い運用環境に対応したAppleデバイス導入をサポートしています。Apple製品のエキスパートが、個々のお客様にとって最適なソリューションをガイドします。



www.jamf.com/ja/

© 2025 Jamf, LLC. All rights reserved.

こちらから無料トライアルをお申し込みのうえ、Jamfエキスパートにご相談ください。

または、販売代理店までお問い合わせください。