ホワイトペーパー

JamfとMicrosoftの連携が生み出すシナジー

ハイブリッドやリモートワーク環境のサポートはかつてないほど重要になり、IT管理者は組織の成功にもっとも貢献してくれる専用の管理ツールを必要としています。例えば、Appleデバイスの管理にはJamfのソリューション、その他のデバイスの管理にはMicrosoftの製品があります。JamfのAppleに特化した脅威インテリジェンスとMicrosoftのID管理およびSIEMの長所を組み合わせ、エンタープライズセキュリティの土台であるデバイス管理にエンドポイントとネットワークセキュリティを重ね、多層的構造を構築します。

多くの人は、最適なプラットフォームをひとつ選択するのがベストだと考えるでしょう。しかし、組織で使用するデバイスの種類をひとつに限定したり、すべてのデバイスをひとつの非効率なプラットフォームで管理したりすることは、もはや時代遅れになりつつあります。すべてのデバイスが同じ機能性を持っているわけではないからです。今日の最適な解決策とは、各デバイスに最適なオプションを用意し、MicrosoftやJamfが提供している統合や連携を賢く活用することを意味します。

このホワイトペーパーのトピック

- 従業員と組織にとってのデバイス選択の重要性について
- JamfとMicrosoftの連携によって生まれる効率性、柔軟性、そして究極の使いやすさについて

選択できることのメリット

従業員にとっては働く場所を選ぶ際、雇用主にとっては優秀な人材を採用しつなぎ止めておく際、企業にとっては業界内での競争力を評価する際、ワークテクノロジーに選択の余地があることが不可欠です。2,000人以上を対象とした最近のグローバル調査*では、回答者の約10人中9人（87%）が、仕事用のデバイスを選択することは自分にとって重要であると答え、テクノロジーを選択できるようになるためなら給与の一部を犠牲にしても構わない（89%）と回答しています。

この調査から、従業員の選択が組織の従業員基盤に与える影響はかなり大きく、ウェルビーイング、採用、定着にプラスの効果があることがわかりました。

91% の回答者が従業員選択プログラムによるメリットを報告しており、生産性や積極性の改善、従業員がより大切されていると感じることなどが挙げられました。

従業員にとって選択肢があることが重要であるにもかかわらず、自分の組織には従業員選択プログラムおよび/または私的端末の業務利用（BYOD）戦略が導入されていると答えたのは回答者のおよそ半数（54%）でした。

選択肢を与えられれば、Appleユーザも非Appleユーザも Appleに関心を持つ

Appleユーザは自分が使っている製品への愛着度が強く、仕事でAppleデバイスを使いたいと答えたAppleユーザは98%に達しました。さらに、調査の結果、実際には労働者のほとんどがAppleを選ぶことに関心を示していることが判明。選択肢さえあれば、回答者全体の62%が仕事用デバイスにAppleを選ぶと答えました。

Appleデバイスの提供により、ユーザが愛用するMicrosoft生産性ツールの活用を妨害することはありません。JamfとMicrosoftが統合することで可能性が広がり、管理や保護を円滑化し、ユーザやAppleデバイスをMicrosoftソフトウェアとつなげます。

JamfとMicrosoft：共に歩むパートナー

JamfとAppleが非常に密接な関係にあることは周知の事実ですが、だからこそ、Microsoftとの安全かつ戦略的な統合によりユーザを支援することが重要になります。

2017年、JamfとMicrosoftは、Jamf ProからMicrosoft Intuneへのインベントリデータの共有、条件付きアクセスの適用、修復パスの提供といった機能などの提供を含め、macOSにおける条件付きアクセス（デバイスコンプライアンス）を可能にするコラボレーションを発表しました。これにより、信頼できるユーザが信頼できるデバイスで信頼できるアプリケーションを使ってのみ、企業データにアクセスできるようになりました。**2018年**、Jamfはエンドユーザによりシームレスなログイン体験を提供するため、Microsoftテクノロジーの統合を再び拡大。**2019年**にはOffice for Macにアプリとカスタム設定の提供を始めました。**2020年**、Microsoftは条件付きアクセスをAppleモバイルデバイスにも拡大することを発表し、Jamfとパートナーを組んでiOSのデバイスのコンプライアンスをサポートしました。直近では**2021年**、Apple特有の脅威インテリジェンスをMicrosoft環境のITとセキュリティに最適なSIEMツールにリアルタイムで直接ストリーミングするためにMicrosoft SentinelとJamf Protectを統合し、セキュリティパートナーシップにおける重要な一歩を踏み出しました。

ここ数年でワークフローやユーザプロセスが変化し、適応していく中、エンドユーザとITチームの双方にとって合理的な体験を生み出すために、JamfとMicrosoftの関係はより密接なものへと変化しています。

IT管理者にとってのメリット

アップデート、保護、メンテナンスが簡単で、信頼性が高くセキュアなデバイスを組織に浸透させることは、IT管理者の重要な仕事のひとつと言えます。選んだデバイスがMacであってもWindowsであっても、エンドユーザは同等のサービスやセキュリティ、管理性を求めています。

管理者のバックグラウンドがAppleであれWindowsであれ、不慣れなシステムを理解しようとする過程において失敗するのはよくあることです。Mac管理者はJamf Proをよく理解し、使いこなしています。しかし、JamfとMicrosoftの新しい統合とパートナーシップが実現した今、IntuneでMacを管理するMicrosoft出身の管理者の多くが、この2つを組み合わせるタイミングについて考えを巡らせています。

Microsoft は、新しいEntraプラットフォームにより、ゼロトラストソリューションを個々の管理ソリューションから完全に独立させました。Microsoft Entra ID Conditional Accessは、IntuneやJamf Proのようなパートナーデバイス管理ソリューションからデバイスの信頼性を確立します。

これを実現するために、Windows管理者はAppleのエコシステムの仕組みを理解しなければなりません。暗号化の方法やマルウェア対策の効果性、サインインの方法など、疑問は尽きません。

JamfとMicrosoft Entra ID による条件付きアクセス

Jamf Proはデバイスを管理し、組織のコンプライアンスポリシーを計算するエンジンであり、スマートコンピュータグループとスマートデバイスグループのほぼ無限の計算機能を基に、デバイスが準拠していることをMicrosoftに報告します。エンドユーザがデバイスからクラウドリソースにアクセスする際、Microsoft Entra ID Conditional Access は、デバイスのコンプライアンスとユーザのリスクレベルおよびロケーションを用いてアクセスを許可します。

コンプライアンスをどのように管理するかは、完全に管理者次第です。特定の設定、複雑なパスワード、暗号化、アクティブでない状態が続いた後のスリープ状態など、必要に応じて要求するか否かを決めることができます。コンプライアンス計算をJamf Proに移行することで、Microsoftはアプリが Appleデバイス上で収集できる限られた情報に制限されなくなります。Microsoft Entra IDは、コンプライアンスステータスに基づいて判断するだけで済むため、よりアジャイルになります。また、デバイスが適合していない場合は、ユーザをJamf Self Serviceに戻し、ITが関与することなく自己修復できるようにします。

JamfとMicrosoftパートナーシップの良さはまさにここにあります。Microsoft Entra IDを使ってMacからサービスへのアクセスやアイデンティティや保護しながら、Jamf Proが提供する管理能力をフルに活用することができるため、1つのプラットフォームに限定される必要がなくなります。

MicrosoftのEnterprise Mobility + Security &デバイスコンプライアンス

リモートワーカーをサポートする必要性から、セキュリティの焦点はこれまでの企業ネットワークの内側から、オフィスの壁を越えたところにまで広がっています。このため、組織はすべてのデバイスを管理しセキュリティを確保するための合理的な方法を求めています。MicrosoftとJamfのパートナーシップは、信頼できるユーザが信頼できるデバイスで信頼できるアプリにアクセスするという共通の最終目標の下、デバイスのコンプライアンスにも拡張されました。

元Microsoftコーポレートバイスプレジデントの Brad Anderson氏は次のように語っています。「従業員選択プログラムやITのコンシューマライゼーションなどのトレンドは広がり続けており、組織はハイブリッド環境に適応できる管理ツールを必要としています。MicrosoftとJamfのパートナーシップにより、IT管理者はエコシステムに特化した重要な機能を提供しつつ、従業員のデバイス管理を一元化することができます。」

Jamf ProとMicrosoft Entra IDを統合することで、Jamfが管理する組織所有のmacOS、iOS、iPadOSデバイスのコンプライアンスが強化され、これにより組織は、準拠デバイスを使用する信頼できるユーザのみが会社のリソースにアクセスできるようにすることができます。Jamf Proデバイスコンプライアンスと Microsoft Intuneの統合は、パートナーコンプライアンス管理APIを利用しています。

Jamfは、Entra IDと連携したアプリ（Microsoft 365アプリを含む）にアクセスしようとするユーザにデバイスの登録を義務付けることで、これに対応しています。まず、Jamfによってデバイスのコンプライアンス基準が設定および評価され、次に、Jamfが収集したデバイスの情報がMicrosoftに送信されます。最後に、ユーザが保護されたリソースにアクセスすると、Microsoft Entra IDはデバイスのコンプライアンス状態をチェックし、動的にアクセスを許可または拒否します。

この機能により、組織はMicrosoftでコンプライアンス状況などの重要なデバイス情報を共有しながら、Jamfでデバイス管理を行うことができます。IT管理者は、Apple製品のエコシステム管理にJamfの機能を利用しながら、Entra IDと Microsoft Intuneによる条件付きアクセスを活用することで、コンプライアンスに準拠したデバイスを使用する信頼できるユーザのみに企業データへのアクセスを許可することができるのです。

Jamf ProtectとMicrosoft Sentinelの統合

組織のデバイスやネットワークインフラがより複雑になるにつれ、その環境のセキュリティを確保するために、セキュリティチームはSIEM（セキュリティ情報イベント管理）やSOAR（セキュリティ運用の自動化および効率化）などのツールにますます依存するようになっています。Macの世界に確固たるセキュリティとコントロールをもたらすため、Jamfはエンドポイントセキュリティツールであるjamf ProtectをMicrosoft Sentinelのデータフローに統合しました。

Mac専用のエンドポイント保護ツールであるJamf Protectは、最小限の構成でMac固有のすべてのセキュリティデータとアラートをSentinelに直接プッシュすることができます。不審、または悪意のあるアクティビティやマルウェアの通知はすべて、既存のワークフローと簡単に統合できるため、セキュリティ担当者の労力や時間はほとんど必要ありません。Jamf Protectの攻撃検出とログ情報により、Sentinelはその機能を拡張することができます。これにより、組織の環境下にあるすべてのMacデバイスに対する幅広い攻撃を特定・修復しながら、組織全体のセキュリティを向上させます。

MicrosoftとJamfの機能を組み合わせることで、組織は使い慣れたSentinelのインターフェースから離れることなく、すべてのMacのセキュリティアクティビティに対して完全な可視性を手に入れることができます。

最後に

このような統合やJamfとMicrosoftのパートナーシップが存在する今、組織に積極的にMacを導入すべきでない理由はもはやありません。Windows管理者であっても、MacをWindowsデバイスと同じように保護、管理、統合できる時代になったのです。

Jamfの**トライアルをお申し込**いただくか、正規販売代理店にお問い合わせください。

パートナーシップと統合に関する詳細は、**Jamf.com/integrations/Microsoft**をご覧ください。

出典：
**jamf.com/ja/resources/e-books/global-study-employee-choice-2021/*