最新の管理

MDMの未来

優れたIT責任者は自社のテクノロジーを熟知しており、彼らは、組織の従業員とビジネス目標をサポートする上で必要なものを慎重に検討した上で、最も効果的なテクノロジーを選択すべきであること、そして、今の職場をサポートする一方で、将来的なニーズの変化にも対応できなければならないことを理解しています。これはつまり、組織が最新のデバイス管理を採用してハイブリッドワークを導入し、従業員が世界中どこからでもセキュア&シームレスにデバイスを操作できる環境を整える必要があるということを意味しています。

Apple環境は、同社が先頭に立って急発展を遂げ、企業のニーズに応えるべく、さまざまなイノベーションが生まれています。それらに遅れを取らないようにするには、Appleと同じスピードでモバイルワーカーを支援し、ユーザのニーズを満たしていかなければなりません。

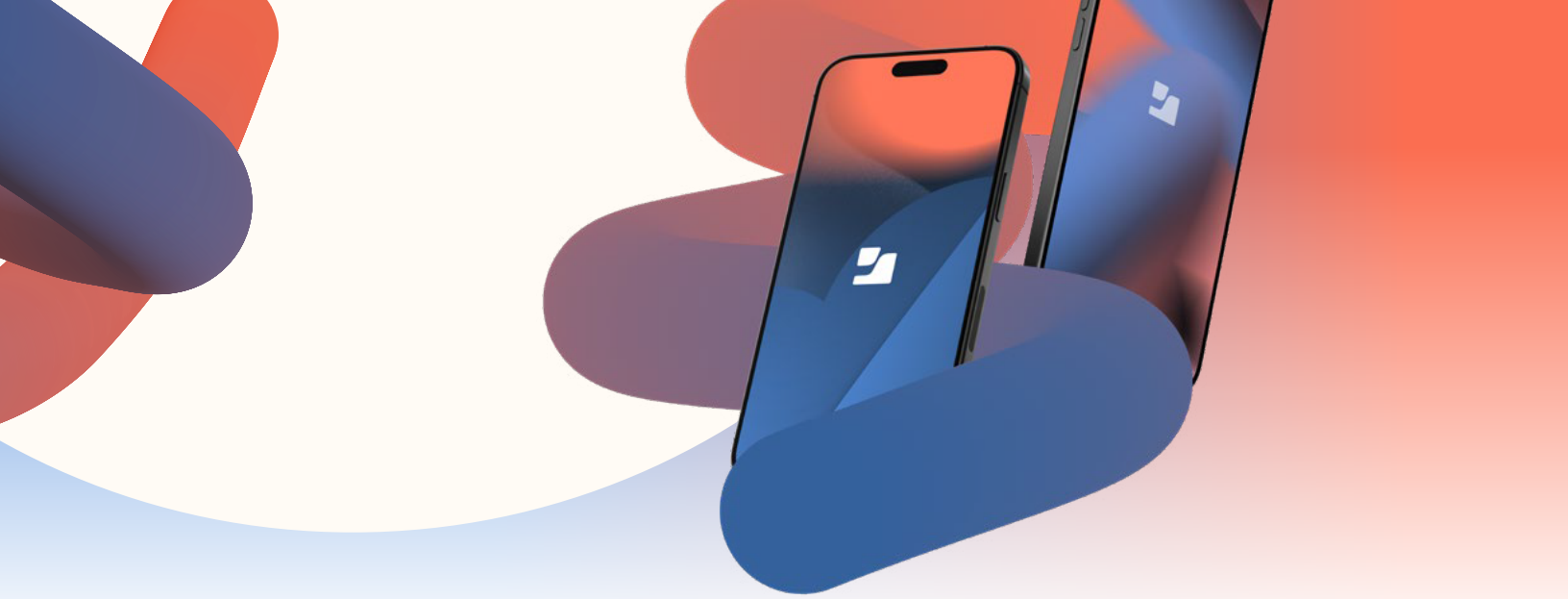
組織がハイブリッドやリモートなど柔軟な勤務形態にシフトすることで、業務コストが下がり、優秀な人材の定職率や従業員の生産性がアップするという**研究**が示されています。

Jamfをはじめと企業の間に立つMDMプロバイダは、Appleのイノベーションをエンタープライズ規模に行き渡らせ、そのメリットを最大化できるようサポートします。そのためには戦略に将来のニーズが反映されていることが不可欠です。

「今日の最善は、明日の期待となる」

- Fletcher Previn、Cisco最高情報責任者

出典：**エンタープライズにおけるMac：従業員選択プログラムから生まれる新たな働き方**



最新の管理とは？

最新の管理はデバイス、ユーザ、OS、アプリケーションをクラウドから一元的に管理します。従来のモバイルデバイス管理（MDM）をはるかに超える最新の管理は、エンドポイント管理やセキュリティの次なる進化と言えるでしょう。このアプローチは、異なる要素を統合することで全体的な視点を提供。IT部門のセキュリティ、管理、状況認識を強化し、彼らがより迅速なアクションを取れるようにします。

つまり、最新の管理を戦略に取り入れることで、従業員はどこで仕事をしていても、安全かつシームレスなデバイス体験を手に入れることができます。そしてそれにあたって、ITは現代の職場が求めるペースでサポートを提供するためのツールとシステムを整えておく必要があります。

この最新の管理は、組織に以下のようなApple環境に関する疑問を抱かせるでしょう：

- 自分たちの戦略は最新のデバイスの管理やセキュリティアプローチを反映しているだろうか？
- 最新の管理を採用することで何が得られるのか？
- このままでは何を失うのか？

これまでのApple管理のあゆみ

従来の管理はデバイスを核とし、企業所有デバイスが従業員に割り当てられ、これらの許可されたデバイスのみが必要なアプリケーションやサービスを利用するために企業内のネットワークにアクセスできるというというものでした。IT管理者はこのような伝統的あるいはレガシーな管理に固執し、労働者にとっても、つい最近までこれが当たり前でした。しかし今日のダイナミックな職場環境において、この方法では従業員のニーズを満たすことはできません。

こうした課題に取り組むAppleの進化をよりよく理解するために、Appleデバイスの管理の歴史を振り返ってみましょう。

モバイルデバイス管理（MDM）の前：バイナリ

Appleが2010年にMDMプロトコルをリリースするまで、組織が管理していたAppleのデバイスはmacOSだけでした。登録されたMacデバイスはまずローカルバイナリを取得し、そこに含まれたroot権限により、デバイスに関するデータを定期的に管理サーバに送信する仕組みになっていました。また、パッケージのダウンロードやローカルスクリプトの実行によって、ローカルクライアントにプログラムに関連するアクションを指示することもできました。**私たちはこれを「force pull（強制プル）」スタイルのデバイス管理と呼び、**

この頃のmacOSデバイス管理には膨大なITリソースが必要でした。

初期のMDM：デバイス中心

その後iPhoneが登場し、MDMスタイルが変化。root権限を持つエージェントが定期的に管理サーバと通信する時代は終わり、プッシュ通信が使われるようになりました。

当時のMDMは、デバイスがAppleと持続的に通信を維持することが必要で、設定、コマンドやクエリの受信、アプリのインストールの際には、管理サーバーがAppleにリクエストしてデバイスに通信させる必要がありました。

以下に具体的な例を示します：

1. 「OSをアップデートせよ」という内容のコマンドが出される。
2. それに続いて「現在のOSバージョンは？」というクエリが出される。
3. さらに正しくコマンドが実行されたことを管理者が確認するためのクエリが出される場合もある：「今はどんな状態か？」

…アップデートは無し？確認は明日するよね？

従来のMDMでは、コマンドが送信されたり完了したりすると管理者に通知が届き、デバイスから多くの情報を得ることができました。**しかし、そのために管理者は繰り返し質問しなければならず、**時には、大量の重複した情報が送られてくることもありました。複雑なコマンドや条件付きのワークフローを含むコマンドでは、情報の行き来が増えます。管理サーバに、その情報を解析し、変更部分を割り出すようリクエストすると、結果としてコマンドやクエリが発生するからです。

仕事に個人所有のデバイスを使用する人が増える中で、ユーザ登録によるBYODワークフローでは、MDM機能や可視性のサブセットが意図的に制限されてしまいます。デバイス管理がどんどん複雑になるのに伴い管理対象Apple IDに新たなワークフローが登場。**以前は、フルに管理するか、全くしないかのどちらかでしたが、この新たなワークフローはかつてのように単純なものではありません。**

この20年間で、さまざまなコマンドや詳細な設定が追加され、プロトコルは洗練化し、AppleのDDM（宣言型デバイス管理）プロトコルが誕生しました。

イノベーションの活用：宣言型デバイス管理

宣言型デバイス管理は、未来のデバイス管理と位置付けられ、効率的なセキュリティワークフローを支える重要なアップデートでもあります。宣言型デバイス管理は、設定した条件下でデバイスがどのように動作するかについて、はるかに詳細な指示を前もって送ることができます。この一連の指示とステータス報告機能を組み合わせることにより、デバイスの特定の値に変化が生じた際に管理サーバにアラートを出します。

言い換えれば、デバイスがコンプライアンスから逸脱した場合、能動的に行動し、最新情報を直接サーバに送信することができます。管理サーバからのレポートリクエストや指示を待つ必要はありません。**結果的に、デバイス情報はより正確になり、デバイスをコンプライアンスに準拠させておくためのポリシーを迅速に適応することができる他、**ネットワークトラフィックが大幅に削減されるため、パフォーマンスとスピードが著しく向上します。

宣言型デバイス管理が示すように、管理はアップデートされています。宣言型デバイス管理によって、管理者はより複雑で革新的なMDM戦略を構築できるようになり、加えてデフォルトでデバイスのセキュリティを強化したり、重要な状況変化が生じた際、社員に素早く通知できるようになります。

MDMの未来とは：

1. 宣言型管理で開封時からコンプライアンスに準拠するよう設定し、プログラムによる低レベルバイナリの扱いを制限することで、**よりセキュアになる**
2. 宣言に基づくエンドユーザのインタラクションが可能となり、**よりネイティブになる**
3. MDMの既にパワフルな基盤を宣言型デバイス管理でさらに強化し、**より便利になる**

最新の管理戦略がもたらすメリット

ハイブリッドな勤務形態が普及し、従業員からも求められるようになる中で、革新、創造、協業を成功させるために求められるツールの提供方法も進化しています。**ユーザは、Appleエコシステム全体を使って、地球上のほぼどこからでも自分が必要とするデータやツールにアクセスできるダイナミックな体験を求めています。**

OS、アプリケーションソフトウェア、セキュリティアップデートは、ユーザの体験を改善し、デバイスを攻撃から保護するために、定期的に新しい機能や保護を提供しています。現代

は開発サイクルやフィードバックループが高速化し、アップデートを迅速にユーザにプッシュすることが容易になりました。しかしその結果、デバイスは週に何度もアップデートを受けることになり、それがエンドユーザ体験を妨害。ユーザはアップデート、機能、パフォーマンス、セキュリティをより良くしたいと思う反面、重要なプロジェクトの最中や、最も生産性の高い勤務時間中に、デバイスから停止や再起動を指示されることは望んでいません。

これを解決するには、従来のオンプレミス型から、あらゆるAppleデバイス を、どこからでも効率的に管理し、セキュリティを確保する 最新のクラウドベースのシステムへの移行が必要です。

クラウドに移行することで、オンプレミスのリソースと比較して、組織はより迅速に行動し、ユーザが望む方法とタイミングで柔軟なリソースを提供できるようになります。最新のツールは定型的なIT機能を自動化し、時間のかかるIT作業の負担を軽減することで、管理者は他の特定の問題に集中する時間を確保できます。セルフサービスツールは、IT部門がチケットを発行したりパスワードをリセットしたりする必要性を減らし、従業員がアプリや情報にすぐにアクセスできるようにすることで、エンドユーザとIT部門をサポートします。

クラウドの導入は、オンプレミスの導入に比べて多くのセキュリティメリットがあります。特に、以下のようなクラウドセキュリティ機能やサービスが利用できるようになります：

- 自動登録やユーザ登録などのビルトインの登録方法を活用した、組織内で管理される全デバイスの完全性を保証する検証済み登録
- 個人のクラウドIDに基づいてリソースへのアクセスを管理し、機密データやアプリケーションへの不正アクセスを防止するIDおよびアクセス管理
- 機密データ部分へのアクセスをユーザに必要な分だけ与える権限管理
- 管理対象デバイスを使用する正規のユーザのみに業務関連アプリやデータへのアクセスを許可する、アプリやデータに対するきめ細やかなアクセスポリシー
- すべての作業トラフィックを暗号化し、不正アクセスを防止するセキュアなネットワークトラフィック
- 管理対象デバイスからリアルタイムで得られるセキュリティデータにより、リスクシグナルを継続的に評価し、カスタマイズ可能なリスクしきい値に基づいて業務ソースへのアクセスに制限を自動適用する、条件アクセス

多様な種類のデバイスを使用する、ワークフォースの分散化は多くの課題を生み出しますが、最新の管理を導入することでそれらの課題を解決し、ユーザとITチームの両方に一貫した体験を提供できるようになります。

Appleに最新の管理を導入するのにJamf以上の適任はいません。

JamfはApple MDMで20年以上の実績があります。JamfとAppleの間には緊密な結びつきがあり、JamfはAppleの新リリース初日からサポートが可能です。

しかし、テクノロジーの世界において約20年は一生のように長く、そのためJamfは、もはや守りに入っているのではないかと感じる人もいるかもしれません。**しかしAppleが革新を続けるように、Jamfもまた革新を続けています。**AppleもJamfもずっと最先端の管理を模索し続け、デバイス管理とセキュリティの仕組みを大きく変えました。

Jamfはクラウドベースのソリューションへの移行を牽引。環境内のデバイス数が増加するにつれて、それらを効果的に管理するためのスケーラブルで、世界中どこからでもアクセス可能なサービスが必要という認識が高まり、これがクラウドベースへのシフトを後押ししたのです。そこでJamfでは、Jamf Pro MDMサーバを**Jamf Cloud**でホスティングできるようにしています。

サーバーをクラウドでホスティングする他にも、**Jamf Pro**は**Appインストーラー**、**Jamf Cloud 配布サービス**、宣言型デバイス管理による**管理対象ソフトウェアアップデートなどさまざまなクラウドベースの機能を提供しています。**

ソフトウェアのアップデート管理は、デバイス管理の要であり、私たちのコミュニティが必要としている機能。Appleとの緊密な関係のおかげで、JamfはDDMによる管理ソフトウェアアップデートに素早く対応することができました。今では、Jamf Cloud の管理者はソフトウェアのアップデートを特定の日時までに完了するよう予約することが可能。DDMによって、これらのアップデートはMacやモバイルデバイスすべてに自動的に適用されます。このワークフローをサポートすることで、管理者のソフトウェアアップデート体験が改善され、サードパーティツールへの依存度が下がるだけでなく、デバイスは最新のOSアップデートやセキュリティ修正に対応し続けるようになります。

Jamf Connect はクラウドIDプロバイダと統合し、許可されたユーザのみが企業リソースにアクセスできるように、ローカルMacアカウントのプロビジョニングとパスワード同期をジャストインタイムで実施し、最新のセキュアなMac認証を実現します。Jamf Connectがあれば、ユーザはMacを開封して電源を入れたあと、単一のクラウド認証情報でサインインするだけで業務に必要なアプリケーションやリソースにアクセスできるようになります。

最新の管理戦略で革命を：
Appleエコシステムの可能性を解き放つ

クラウド環境と宣言型デバイス管理を組み合わせることで、デバイスの管理とセキュリティをより迅速、円滑、安全に実行できるようになり、従来型管理のIT負担を取り除きながら、現代の職場が求めるユーザエクスペリエンスを提供します。

最新の管理へのアップデートをご検討中、あるいはクラウドとDDMの導入にご興味がお持ちでしたら、**私たちJamfがお手伝いいたします。**