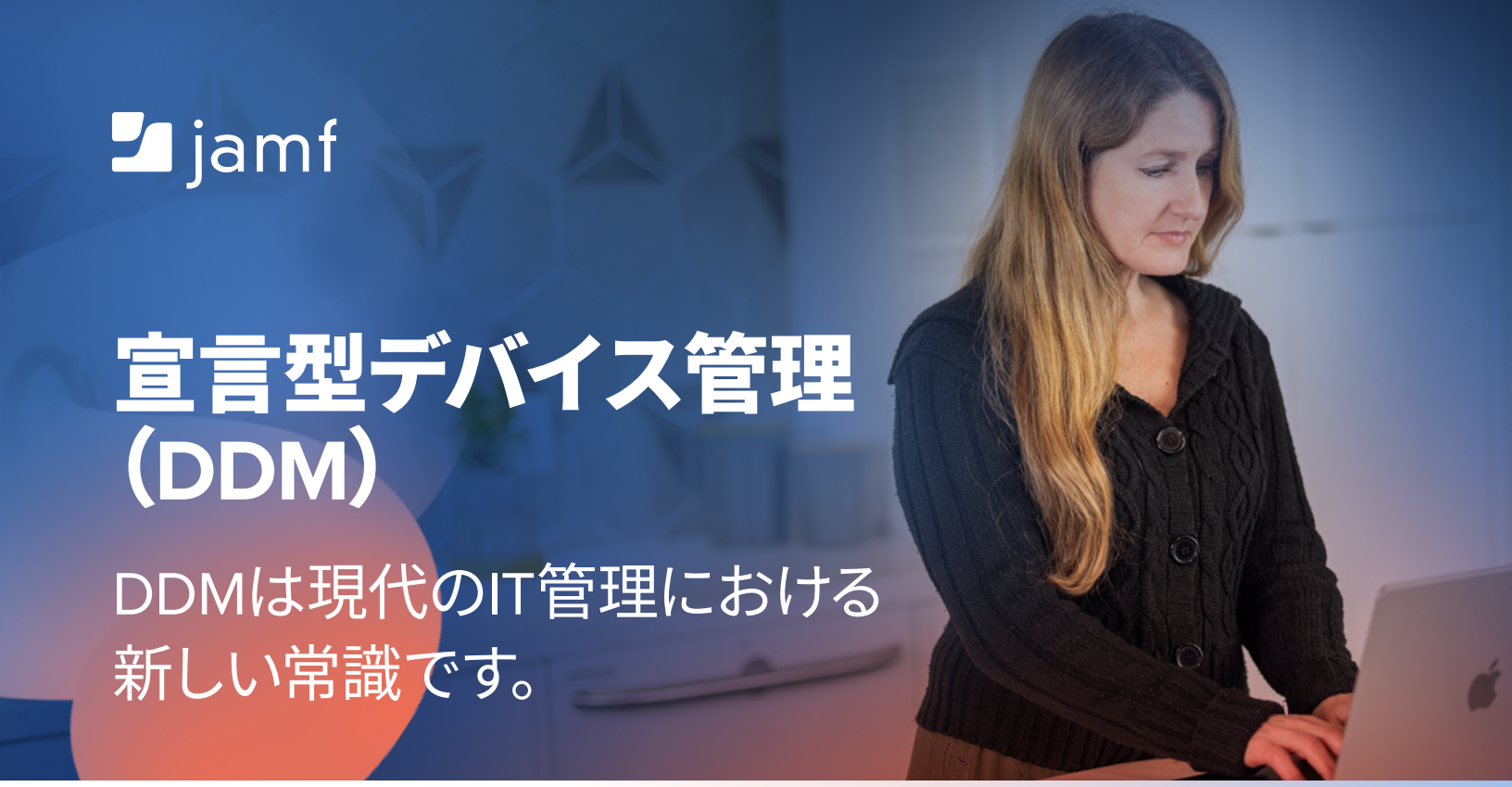


宣言型デバイス管理（DDM）

DDMは現代のIT管理における新しい常識です。

今や強力なツールとなった モバイルデバイス管理（MDM）

Apple製品のモバイルデバイス管理（MDM）は、もはやバイナリを使った「強制プル」型ではなく、柔軟で強力かつ使いやすい形に進化しています。JamfもこのMDMに注力していますが、これほどまでになるとは誰も想像できなかったに違いありません。

MDMの登場は、Appleのデバイス管理にこれまでにないレベルの自動化、統制、可視性をもたらしました。繰り返し発生するタスクの負担を軽減しつつ、ヒューマンエラーの予防やセキュリティの強化にも効果を発揮したのです。

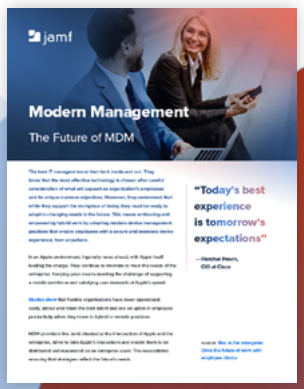
しかし、オフィス勤務が中心の時代から、多くの人が世界中のさまざまな場所で分散して働く状況が一般的になると、MDMに対するニーズも変わってきました。今求められているのは、これまで以上に柔軟で、場所を選ばず使える、そしてセキュリティに優れた新しい管理手法、それが**モダンマネジメント**です。

モダンマネジメントとは

モダンマネジメントとは、現代の職場のありように対応しつつ、その将来を計画していくための戦略です。

この戦略では、デバイス、ユーザ、オペレーティングシステム、アプリケーションのすべてをクラウドで管理します。セキュリティに関しても、クラウド経由で対応します。モダンマネジメントを導入すると、セキュリティ、管理、IT部門の状況認識のいずれも強化することができます。また、総合的なアプローチであるため、可視性が高まり、迅速な対応が可能になる効果も期待できます。

モダンマネジメントについて詳しくは、こちらの資料をご覧ください。>



従来型のデバイス管理に対する
モダンマネジメントの優位性

従来型のデバイス管理は、企業から従業員に支給するデバイスを主な対象としたものでした。社内のネットワークにアクセスできるのは、承認済みのデバイスのみです。かつては、これがデバイス管理の優れた方法であるとされていました。

しかし、今や職場のあり方は大きく変化しています。リモートワークやハイブリッドワークは当たり前になり、従来のオフィス環境と組み合わせる場合でも、自社のデータを危険にさらすことなく、あらゆるユーザの生産性を維持できなければならなくなりました。

モダンマネジメントでは、すべてをクラウドに移行し、暗号化された安全な接続を使用します。クラウド環境には、オンプレミス環境に比べて以下のようにセキュリティ面で多くのメリットがあります。

- **検証済みの登録方法の利用：**環境にあらかじめ用意されている登録方法を利用できるため、組織内で管理する各デバイスの完全性確保につながります。
- **ID&アクセス管理：**個々のクラウドIDに基づいて、誰が何にアクセスできるかをIT部門が管理できます。
- **特権管理：**ユーザがアクセスできる対象を必要な範囲に絞り、機密データを保護できます。
- **アプリとデータに関するきめ細かなアクセスポリシー：**アプリやデータへのアクセスを、信頼できるデバイスの許可されたユーザのみに制限し、セキュリティを強化できます。
- **ネットワークトラフィックの保護：**セキュアな暗号化により不正アクセスを防止できます。
- **条件付きアクセス：**リアルタイムのデータリスクしきい値に基づいて自動的にアクセスを制限し、ネットワークを安全に保ちます。

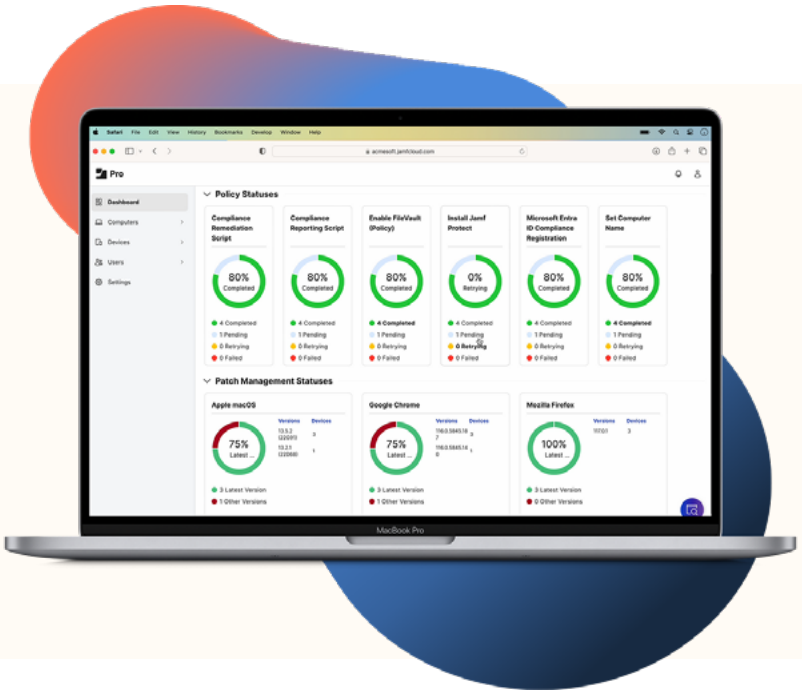
モダンマネジメントは柔軟性が非常に高いため、さまざまな勤務地や勤務時間に対応できます。また、企業所有のデバイスとユーザ所有のデバイスのどちらであるかも問いません。

もっとも、モダンマネジメントが完全な形で実現できるようになったのは、Appleによる宣言型デバイス管理（DDM）のリリースがあってからのことです。

宣言型デバイス管理とは

DDMとは、Appleによれば、デバイスがあるべき状態に向けて積極的かつ自律的に動作できるよう、既存のMDMプロトコルに「変革的なアップデート」を加えたものです。

> 「宣言型の管理こそ、デバイス管理の未来です」
>
> — Apple（WWDC 2021にて）



Jamfは、DDMの革新性を早期から認識しており、早期からその対応に向けた準備を進めていました。

宣言型デバイス管理の基盤となるのが、積極的かつ自律的に動作するデバイスです。デバイスが「自律的」であるとは、自らの状態の変化に反応して命令を実行できることをいいます。命令が実行されると、プログラムに記述されている管理ロジックが適用され、必要なアクションが実行されます。

自律的なデバイスでは、コンプライアンスポリシーから逸脱したり、マルウェアの疑いがあるとされるアクティビティを検知した時点で、デバイス自体が即座に対策を講じることができます。そのため、サーバからステータスの確認を受け、サーバにレポートを送り、サーバから次のアクションに関する命令を受け取るというプロセスを経る必要がなくなります。

DDMの重要なメリットは以下のとおりです。

1. サーバとデバイスの間のトラフィックが減少し、パフォーマンスが向上する
2. マルウェアの疑いがあるプログラムをすばやくサンドボックス化・修復できるため、セキュリティが高まる
3. 従来よりも少ないリソースですばやくスケーラビリティを実現できる

DDMの仕組み

DDMは、**宣言**、**ステータス**、**拡張性**の3つを柱としています。

宣言

宣言は、サーバで定義され、デバイスに送られるペイロードであり、アカウント、設定、制限など、デバイスに直接適用するポリシーを定義します。宣言は、全ユーザに配布することも、一定のグループに配布することもできます。もちろん、個別のユーザやデバイスに配布することも可能です。

宣言には、以下の3つの**必須**プロパティがあります。

1. **タイプ:** 構成がどのポリシーを表すかを示します。
2. **識別子キー:** セット中の特定の宣言を識別するための情報です。宣言をサーバと同期させるために使用します。
3. **値:** 値の範囲または特定の値一式を指定し、データを制限するものです。文字列、数値、ブール値、配列、ディクショナリの5種類があります。

宣言のタイプ

アクティベーション

自動的に適用される一連の構成と、その構成で参照されるアセットを指定したものです。アクティベーションが適用されるには、構成とアセットのすべてが有効でなければなりません。例えば、アクションを特定のデバイスタイプやOS、特定のOSバージョンに対してのみ有効にするような使い方ができます。アクティベーションを使用すると、デバイスが要件に基づいて適用するものを判断するようになるため、サーバに対する負荷がデバイスに転嫁されます。

アセット

構成が機能するために必要なデータです。データのサイズが大きい場合のアセット宣言では、データのダウンロード元になるサーバのURLを記述します（MDMサーバまたは個別のコンテンツ配信サーバを指定）。アセットには名前、メールアドレス、パスワード、証明書など、さまざまなものを指定できます。

構成

アカウント、設定、制限など、デバイスに適用するポリシーを記述したもので、MDMの既存のプロファイルペイロードによく似ています。

管理

各デバイスの全体的な管理状態を伝えるための宣言です。サーバや組織に関する静的な情報が記述されます。

ステータスチャネル

ステータスチャネルは、デバイスの状態の変化を追跡するための仕組みです。ステータスチャネルでは、デバイスからサーバに「ステータスレポート」が送られます。サーバは、このステータスレポートの情報のうち、自らにとって重要な項目（OSのバージョン、異常なアクティビティ、コンプライアンス違反など）に絞ってアップデートを受け取ることができます。

2回目以降のレポートでは、差分のデータのみが送られます。つまり、デバイスの状態の全容が送られてくることはなくなり、初回のステータスレポートから変更があった部分だけのデータが報告されます。そのため、重要性の高い情報を迅速に入手できるようになります。また、このレポートは、サーバがデバイスを詳細に監視するうえで役立つだけにとどまりません。アップデートが非同期的に送信されるので、データノイズやネットワークトラフィックの抑制にもつながります。**その結果、パフォーマンスの向上にも寄与します。**

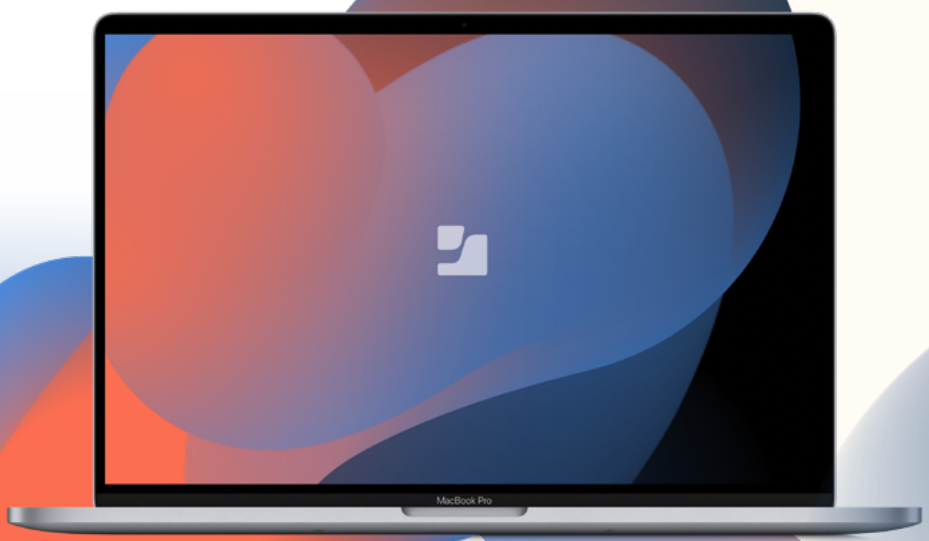
拡張性

社内で利用するApple製品やそのOSのバージョンを1つに統一できている会社はほとんどないはずです。これはつまり、Apple製品はそれだけ長く使えるということです。しかし、投資したデバイスを最大限活用していくためには、バージョンの異なるソフトウェアや、ハードウェアのさまざまな機能の間に互換性を維持することが欠かせません。

DDMなら、デバイスとサーバが変更について自律的にやり取りするので、デバイスもサーバも新たな機能が利用可能になった時点ですぐに認識できます。ソフトウェアのバージョンやハードウェアの依存関係をハードコーディングする必要もありません。

例えば、IT部門がサーバをアップグレードした場合には、デバイスに新機能が自動で同期され、デバイス側ですぐに利用できるようになります。逆にデバイスがアップデートされた場合には、そのデバイスで新たに何ができるようになったかをサーバー側ですぐに把握できます。

宣言型管理データモデルにはこのような拡張性が備わっているため、現在はもちろん将来にも対応できる体制を構築するうえで大いに役立ちます。



DDMで広がる明るい未来

現在は、DDMとMDMの進化のほんの始まりにすぎません。DDMは将来、次のような価値をもたらす可能性を秘めています。

- 複雑な管理戦略にも、シンプルかつ効率的に対応
- 会社支給・個人所有を問わず、管理対象デバイスでの快適な使い心地を実現
- より快適で信頼性の高いユーザ体験
- オンボーディングの迅速化
- IT部門は面倒なルーチン作業から解放され、より価値ある業務に集中可能に

IT部門に大きなことを考える時間が増える効果とは

DDM戦略に取り組めば、組織にさまざまな可能性が広がっていきます。DDMの成長速度、つまりはAppleと同じスピードでビジネスを成長させることだって夢ではありません。

自社には近い将来、どんな可能性があると思いますか？あるいは、ご自身の目標や仕事のあり方そのものに、DDMはどのような可能性をもたらしてくれるでしょうか？

DDMは、仕事のあり方を大きく変えるだけでなく、増大を続けるモダンマネジメントのニーズに対応できる可能性を秘めています。しかし、現在の私たちはまだ、その片鱗を見ているにすぎません。そこで、ここからはDDMの発展により今後どんなことが予想されるかを見ていくことにしましょう。

DDMはMDMの未来をどう変えていくのか

未来は誰にもわかりません。しかし、AppleがDDMで新たな可能性を切り開くことはまず間違いないと思われます。そこで、ここではAppleユーザと管理者に関連して今後進展が予想される分野をいくつか紹介します。

セキュリティの強化

DDMを他の最近の変化と合わせて考えると、あるパターンが浮かび上がってきます。

Appleシリコンは、root権限を持つローカルエージェントやスクリプトによって引き起こされる無人アップデートを基本的にブロックしています。そうすることにより、ハッカーが好むマルウェア戦略のいくつかを遮断するとともに、カーネル拡張のようにOSに対するリスクをはらんだ慣行を阻止することができるからです。

管理者の間では今後、リスク抑制につながる優れた管理ツールを求める声がますます大きくなってくることが予想されます。

きめ細かなアクセス制御

管理対象Apple IDを採用する組織では今後、iCloudキーチェーンのパスキーやウォレットに対応し、各種サービスやファシリティに対するアクセス制御を強めていくことが予想されます。

もっとも、これは必ずしも、組織がこれまで以上に強権的になることを意味するものではありません。DDMの登場により、管理者がアクセス制御の方法や場面を従来よりもはるかに細かく設定できるようになっているからです。

IDサポートの強化による
ユーザエクスペリエンスの向上

Apple Business ManagerとApple School Managerは、カスタムIDに簡単に対応できます。どちらも、Microsoft、Google、Okta、Open ID/SKIMなど、あらゆるIDプロバイダと連携しているため、簡単に管理対象IDを作成できます。Appleデバイスとユーザを管理するなら、管理対象IDがベストです。1つのキーで業務に必要なものすべてにアクセスできれば、ユーザにとっての利便性が増すだけでなく、安全性も高まるからです。

ここまでに挙げた進化は、MDMが以下のように変わっていくことを意味します。

- **セキュリティの向上**：宣言により当初からコンプライアンスを確保できるほか、プログラムを使った低レベルバイナリの取り扱いを制限することが可能になる
- **よりネイティブな管理**：宣言に基づくエンドユーザのインタラクションが可能になる
- **さらに便利に**：MDMのパワフルな基盤がDDMにより強化される

この大きな変化の影響について詳しくは、JNUC 2023の発表「**MDMのネクストステージ**」をご覧ください。

未来は今、ここから始まる

DDMの発展の最も大きなメリットの1つに、既存のMDMベンダーが今すぐにでも宣言型管理機能を使えるようになったことが挙げられます。宣言とステータスチャネルは、既存のMDMコマンドやプロファイルと並行して動作することができます。そのため、新しいプロトコルやサーバインフラストラクチャへの対応のために作業を中断する必要はありません。**DDMは、MDMの動作に微塵も影響を与えることがないのです。**

このことは、既存のMDMワークフローを一気に更新する必要がないということでもあります。つまり、IT部門は自らにとって最善のペースでDDMの導入を進めていくことができます。

もちろん、今すぐDDMを全面的に導入したいという場合でも、問題なく対応可能です。

DDMに対するJamfの対応状況

JamfはAppleと緊密な協力関係にあり、DDMに関しても初日から対応しています。

当初からのサポート

Jamf Proは、2022年10月以来、管理対象デバイスについて宣言型デバイス管理機能を自動で有効にしています（同機能を利用可能なデバイスに限ります）。宣言型デバイス管理が有効になっているデバイスは、状態の変更を自動的にMDMサーバに報告します。また、特定の変更が発生した場合には、当該変更をプロアクティブに報告するとともに、デバイスインベントリ情報にも記録します。なお、デバイスの状態は、管理者がカスタマイズできます。

ステータスチャネルに新たに3種類のフィールドを追加

Jamf Pro 10.46では、DDMステータスチャネルで新たに以下の3種類のフィールドのレポートが可能になりました。

```
`SupplementalBuildVersion`
`SupplementalOSVersionExtra`
`PasscodeCompliance`
```

ここに挙げた3つはいずれも、レポートが自動で有効になっているため、ステータスの更新があれば即座にデバイスからJamf Proに通知されます。

iOS固有のサポート

ここまでに見てきたとおり、DDMは既に多くのことが可能です。しかし、今なお急速に変化を続けているのも事実です。そこで、ここでは利便性と安全性の向上に向けたDDMの活用法を1つ見ていきましょう。

- iOSデバイスのアップデートに、ロック画面でパスコードを入力すると生成される認可トークンを使用します。このトークンは、セキュリティ強化のため、一定期間が経過すると期限切れになります。
- エンドユーザがこのトークンでアクティベーションを終えると、以後しばらくはユーザがデバイスのロックを解除しなくてもデバイスがアップデートされるようになります。
- 一定期間にわたりデバイスのロックが解除されなかった場合には、デバイスがアップデートを受け取ることができなくなります。この場合、ユーザが次にデバイスのロックを解除した時点で、アップデートの許可を促すメッセージが表示されます。

DDMによる管理対象ソフトウェアのアップデート

AppleがDDM機能を導入する前は、管理対象ソフトウェアのアップデートと言えば、管理者から一括アクションかポリシーを送る程度でした。DDMの登場以後は、以下のようなことが実現しています。

- ソフトウェアのアップデート計画の構成が格段にシンプルに
- エンドユーザに細かくアップデート延期の選択肢を提供
- 自動化および強制適用の新機能により、IT管理者による統制を強化
- アップデートの進捗状況がデバイスからプロアクティブに報告されるため、管理者の可視性が向上

今後の展望

Jamfでは、今後も拡充が見込まれるDDMプロトコルを最大限活用するとともに、その導入・活用に向けたお客様の一歩一歩を支え続けます。Appleと足並みを揃え、Apple Vision ProやApple Watchのような新しいタイプの業務デバイスへの対応を充実させていくのもその一環であり、多種多様な働き方のエンドユーザの生産性向上に貢献するという使命を果たすためにほかなりません。

Appleデバイスの管理はかつてないほど面白い時代に

宣言型デバイス管理は、モダンマネジメントの実現を大きく加速させました。まるで、ロケットエンジンでも付いているかのようです。

従来のデバイス管理手法は、もはや終わったと言えるでしょう。管理対象デバイスとAppleやMDMサーバとの間で何度もpingを送り合い、大量の通信をするのが普通だった時代から、ほとんど一夜にして自律的デバイスの時代が到来したのです。Jamfは、その新しい時代に対応するための取り組みを積極的に進めています。

デバイス管理とMDMは、皆様がこれをお読みになっている間も進化を続けています。今こそ、その未来を一緒に作り上げていくチャンスではないでしょうか。

そして、次にやってくるのはモダンマネジメントの時代です。

この成長のチャンスを活かせる、柔軟で行動の早い組織こそが、未来に備えることができます。Apple製品の導入は、その第一歩です。

検討すべきポイント

まずは、自社の現在の技術戦略を確認しましょう。柔軟性はあるでしょうか？どこでも使える設計になっていますか？デバイスの管理とセキュリティには、モダンマネジメントのアプローチが反映されているでしょうか？

いずれかの答えが「ノー」であるなら、モダンマネジメントのアプローチを採用するメリットを考えてみましょう。それは、急速な成長かもしれません。状況に機敏に対応できるようになったり、優秀な人材を採用できる可能性が高まったりする効果も期待できるでしょう。あるいは、従業員全員の連携とセキュリティも強化できる可能性があります。

逆に、変化に乗り遅れたとき、失うものは何ですか？

モダンマネジメントの時代は、まもなくやってきます。チャンスを掴み、明るい未来を手にすることができるかどうかは、皆様次第です。

Jamfは、皆様が歩む道のりをサポートします。

クラウドとDDMの力を、あなたの組織でも。 **AppleとJamf**とともに、**モダンマネジメント**の未来へ踏み出しましょう — **私たちがしっかりサポートします。**

jamf