jamf

DDMによる最新のAppleデバイス管理実践ガイド

Appleデバイスの増加に伴う、アップデートの迅速化、可視性の向上、そして手作業の削減を実現

企業でAppleデバイスの導入が進んでいる中、従来の手法による管理は運用効率を低下させる要因となります。ただでさえ過密な業務を抱える少人数のIT部門にとって、OSアップデートの遅れやデバイス状況の把握のタイムラグ、そして増え続ける手作業による修正は、大きな負担となっています。そこで役立つのがDDM（宣言型デバイス管理）です。

DDMが時間節約と成果向上をもたらす仕組み

ワークフローのシンプル化

DDMに対応したツールとプロセスを導入すると、スクリプトやチェックイン、手動ワークフローが減り、デバイス管理がシンプルになります。

デバイス全体の可視性の強化

このプロトコルでは各デバイスに状態を能動的に報告させるため、IT部門が全デバイスとアプリケーションの状態をリアルタイムに把握できます。

アップデートの高速化

各デバイスから構成の変化が能動的に報告されるので、より素早く確実にパッチとOSアップデートを適用し、修復が必要になる事態を減らして、業務効率を高められます。

エンドユーザエクスペリエンスの向上

デバイス自体に状態の変化へ対応させられるので、日常業務を妨げることなく、より多くのセキュリティアップデートや構成変更をバックグラウンドで行えます。

DDMの概要およびDDMを導入すべき理由

DDMはmacOS、iOS、iPadOS、watchOS、visionOS、tvOS向けのプロトコルで、Appleデバイスに構成の変更を能動的に報告させ、自動で構成を適用させて状態の変化に対応させられます。Jamfでは、ブループリントをはじめとする機能でDDMに対応しています。

従来のサーバコマンドを用いたモバイルデバイス管理（MDM）からDDMプロトコルに移行すると、以下のメリットが得られます。

- サーバコマンドの反復実行を削減し、システムの速度低下を防ぐ
- デバイス状態の変化を能動的に報告する
- デバイス自体によるコンプライアンス管理を増やし、修復にかかる時間をほぼゼロにする
- 手作業でのフォローアップの必要性を軽減する

管理をシンプル化してセキュリティを強化

DDMでは、以下を通じて管理ワークフローをシンプル化し、強固なセキュリティ体制を確立できます。

構成の不整合の軽減

アップデートの高速化

ベースラインの標準化と強化

オンデバイス対応の自動化

これにより、一般的なワークフローの手作業を減らしながら、一括的にコンプライアンスを確保しやすくなります。さらに、DDMではサイバーセキュリティを受動型から能動型へと転換し、組織の成長に伴い発生する高度な攻撃にも対応できます。例えば、デバイスが攻撃や不審な行動を受けたら瞬時にサンドボックスへ隔離させ、ネットワークの安全性を維持できます。

組織にDDMを導入することですぐに得られるメリット

DDMのメリットは、スムーズな規模拡張やIT業務時間の削減に留まりません。組織全体にわたる各種ワークフローについて、これまでにない様々な可能性をもたらします。

全デバイスで構成の一貫性を確保し、組織全体の信頼性と一貫性を高める

一貫性は重要です。組織全体で一貫性のあるポリシーと構成を適用すれば、以下のメリットが得られます。

- サポートへの問い合わせ頻度を抑え、手作業での修正や作業を減らす
- セキュリティ体制を強化し、不正アクセスの原因となる構成ミスを防ぐ
- 全デバイスの挙動の予測性を高め、トラブルシューティングの手間を減らす

DDMで構成ベースラインを確立する

DDMでは、違反の発生時に著しく複雑なものを除いてすべての問題をシステムが自動的に修正するため、アップデートとベースラインを確実に維持できます。

その結果、従業員が技術的な問題や効率低下に遭遇する事態を減らし、意識されることなくバックグラウンドで強固なセキュリティプロトコルを適用できます。

また、IT部門は重要な技術の問題に専念して、会社全体の日常業務の改善につなげられます。

DDMでミスを防ぐ

管理ツールとセキュリティツールを連携させることで、不整合を早期に検出して素早く修復できます。しかも多くの場合、人の操作は必要ありません。同様に、設定とコンプライアンス管理を自動化してヒューマンエラーを軽減できます。

デバイスの変化を自律的に報告させるとほぼ全方面にメリットがある

能動的なデバイス状態報告

DDMでは、デバイス状態が自律的に報告されます。これにより、主要な値（OSバージョンなど）の変更があった場合に、デバイスから自動的に管理サーバへ通知を行い、OSインベントリの能動性を高めて、アップデートを遅滞なく能動的に適用できます。

デバイスの明確な可視化

デバイスが自律的に管理サーバへの報告を行うので、IT部門はデバイス全体の状態を継続的に確認できます。

これにより、以下のことを把握しやすくなります。

- デバイスの位置
- 構成状態
- OSバージョンとインストールされているアプリケーション

さらに、デバイスが攻撃や不審な行動に対応していた場合、IT部門は該当するデバイスとその対応内容も確認できます。

IT部門の代わりにDDMの自動化機能が現場をサポートした場合でも、セキュリティの改善の余地、つまりフィッシングに関する再研修を受けるべき従業員を把握できます。

IT部門でデバイス全体の変化をリアルタイムに把握できるようになれば、不測の事態は減少します。デバイスでパスワードの解除や必須アプリケーションの削除のようなコンプライアンス違反が突然起きた場合、IT部門が直ちに把握できます。

即座に把握し修復を行うことはきわめて重要です。これが不可能であると、高度なマルウェア攻撃を受けたとしても、数時間後の定期サーバチェックインまで気づけない可能性があります。

アップデートサイクルの予測性向上

アップデートの強制適用は、これまでIT部門にとって手間のかかる作業でした。

DDMの導入前

DDMがないと、IT部門でOSやアプリ、ポリシー、構成のアップデートをプッシュする際、常に以下のような問題がつきまとっていました。

- 従業員が作業中断を避けるために重要なアップデートを何度も延期する
- 重要アップデートが手遅れになる前にMDMコマンドで強制適用された結果、何時間も業務が中断される
- IT部門がデバイス状態を把握できないままアップデートをプッシュしており、時として予期せぬ問題に至る

DDMの導入後

DDMプロトコルを導入すると、エコシステムの状況が一変します。

IT部門の設定したポリシーに従いデバイスから状態が継続的に報告されるので、明確な状況をリアルタイムに把握できます。アップデートの待機中も、ダウンロード中も、インストール中も、あるいは問題が生じた場合も、デバイスを追跡したりユーザの情報に頼ったりすることなく進捗がわかります。

- DDMではユーザが常に情報を得られる。デバイスからアップデートに向けて通知がタイムリーに送られてくるため、ユーザはインストールのタイミングを適切に選択できる
- エンドユーザが対応しない場合、デバイスにより自動でアップデートが強制適用される
- 強制適用の日時はクライアントの設定時刻に基づくので、アップデートのタイミングは業務時間外に調整される。DDMプロトコルのデバイスでは電源オフ状態のデバイスもアップデートでき、次回の電源投入時にすぐにアップデートが実行される
- IT部門が状況を把握しないままアップデートを送信することがなくなる。デバイス状態を完全に可視化し、一般的なコンプライアンス問題用の事前プログラミング済みの対応を使用して、IT部門の介入をまったく必要とせずに多くのアップデートを行える

これにより、エンドユーザの業務を中断、あるいは台無しにすることなく、IT部門の作業なしでデバイスをいつでも最新かつ安全な状態に保てます。

受動的なトラブルシューティングと修復から能動的なプランニングに移行

DDMでは、制御の主体を管理サーバからデバイスへと移し、事後対応のトラブルシューティングが必要になる事態を抑制します。

問題が起きた場合、IT部門があらかじめ設定したポリシーと指示に従い、デバイスからサーバに重要な状態の変化が報告されます。

報告対象には、バッテリー残量不足またはストレージ不足によるアップデートの失敗や、FileVaultの暗号化状態などのセキュリティの変化を設定できます。

このようなレベルの透明性を確保することで、直接的なサポートが必要になったとしても、多くの場合はユーザに影響が及ぶ前にIT部門がすぐに介入できます。

能動的なプランニングがビジネスにもたらすメリット

成果は、アップデートの予測性と制御性が高まることです。IT部門は進捗の追跡や個々のデバイスのトラブルシューティングにかける時間を減らし、成果に専念できるようになります。

さらに、「it just works（とにかくちゃんと動く）」の効果も得られます。

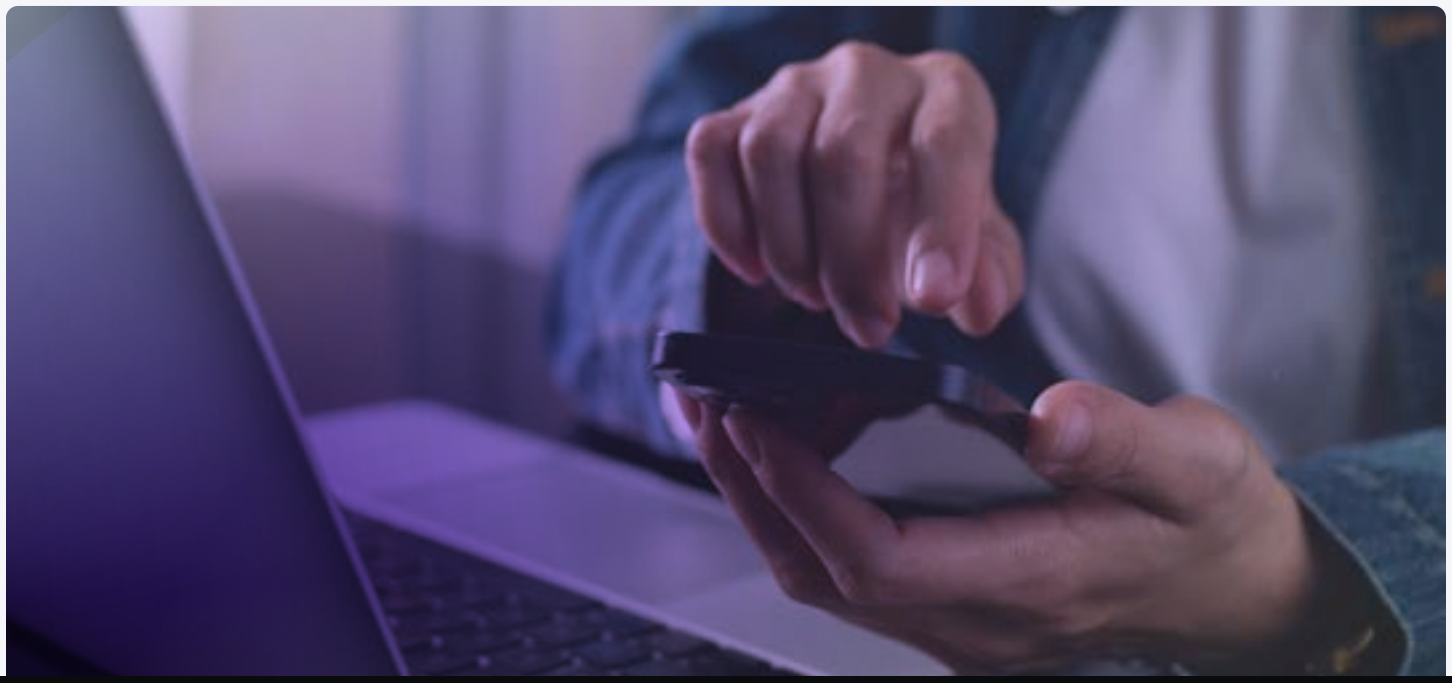
デバイスが継続的に構成され、アップデートされ、内蔵のインテリジェンスで制御されるようになれば、解決すべき問題は著しく減少します。自動対応によりデバイスがポリシーに準拠した状態が維持されるので、ユーザの手間が減るだけでなく、サポートもほとんど必要ありません。

DDMで業務を拡張、自動化、効率化

人員の限られたIT部門にとって、DDMは、デバイス管理の効率を高め、業務上の摩擦を減らし、規模拡大を効果的にサポートするうえで役立つ最先端の管理プロトコルです。

さらに、DDMにはアップデートをバックグラウンドで維持し、コンプライアンス管理を自動化して、エンドユーザのエクスペリエンスを強化する効果もあります。これにより生産性と従業員度の満足度を高められます。

DDMを導入して時間を節約し、負担を増やすことなく規模を拡大して、サイバーセキュリティを強化しましょう。



jamf

www.jamf.com/ja/

DDMによる管理のシンプル化とセキュリティの強化を体感してください。

無料トライアルを申し込む。