Mac管理

初心者ガイド

jamf

最近行われたアンケートによると、給料が多少減っても業務に使用するデバイスを選択できる仕事を選ぶと回答者の89%が答えています。

そして、デバイスの選択を求める人の大多数が、選択できるのならAppleがいいと考えています。**

世界中のビジネスや教育現場で使用されるAppleデバイスの数が増える中、組織はMac、iPad、iPhone、Apple TVを最大限に活用し、テクノロジーへの投資対効果を最大化する必要に迫られています。大量の新しいデバイスの管理はIT部門にとって大きな負担となります。これまでWindows環境で仕事をしてきた場合は特にそうです。

すでにApple製品のことを熟知している管理者もいれば、初めてMacやmacOSの管理に飛び込む人もいるでしょう。特に後者に向けて作られたこのガイドでは、Macの管理スキルのマスターに役立つ以下のトピックについて説明します。

- MacとmacOSの管理入門
- Macで利用できるサービスやプログラム
- ライフサイクル管理の各ステージの概要
- インフラ計画に必要な知識
- 業界トップのAppleデバイス管理ソリューションの概要

** 2021 年「Global Study: 従業員選択制と、その未来の働き方へのインパクト」

MacとmacOSの管理入門

Macの管理に取り組む際には、そのライフサイクルのステージごとに一般的なタスクを割り振るのがベストです。これらの管理タスクは、MacでもPCでも変わりません。

MDM（モバイルデバイス管理）のしくみ

OS X 10.7 LionおよびそれMacでは、内蔵のモバイルデバイス管理（MDM）フレームワークのおかげで、リモートワイプやパスコード制限などの設定の適用が可能になっています。MDMフレームワークの中核を成すのは、**構成プロファイル**と**管理コマンド**です。

これらがAppleプッシュ通知サービス（APNs）を介してデバイスと通信し、Appleから得られる証明書によりそのプライバシーが保たれます。IT管理者が何もしなくても、デバイスとの通信は継続的に行われ、デバイスが管理サーバに通信を戻したタイミングで、あらかじめ定義されたコマンド、設定、構成またはアプリが送信されます。

構成プロファイル

構成プロファイルは、Appleデバイスの様々な設定を定義し、動作を指示するためのXMLファイルで、パスコード設定やWi-Fiパスワード、VPN構成の自動化に使用することができます。また、App Storeやウェブブラウザなどのデバイス機能や、デバイスの名前を変更する機能などに制限を適用することもできます。構成プロファイルは、Jamfを使って指定・導入することができ、デバイスまたはユーザレベルで設定することが可能です。

管理コマンド

MDMコマンドは、管理対象のデバイスに特定のアクションを実行させるために送信するコマンドです。例えばデバイスが行方不明になった場合はリモートワイプコマンドを送信し、OSのアップグレードが必要な場合は、アップデートのダウンロードとインストールを行うコマンドを送信します。これらは、フルに管理されたMacで実行できる数々のアクションのほんの一例にすぎません。

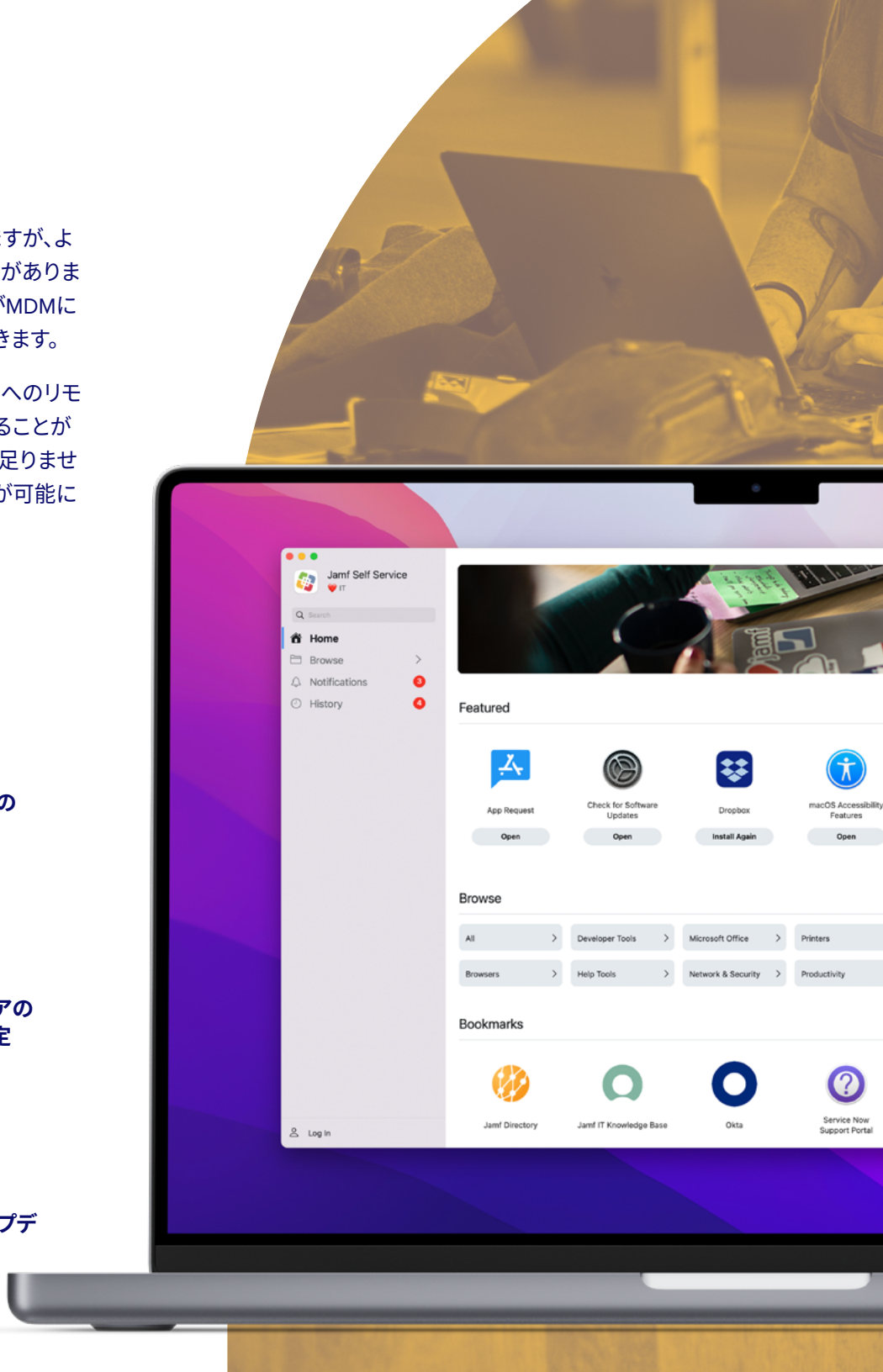
MDMとクライアント管理

AppleのMDMフレームワークはMacに対する基本的なコントロールを提供してくれますが、より堅牢なプラットフォームであるmacOSの場合は、より高度な機能が必要となる場合があります。macOSのみで利用可能なクライアント管理機能を活用することにより、デバイスがMDMに登録された直後からMacエージェント（またはバイナリ）をインストールすることができます。

このエージェントは、非表示の管理者アカウントの追加やルートユーザによるmacOSへのリモートアクセスを可能にし、コンピュータ上でより多くのポリシーやスクリプトを実行することができるようになります。エージェントベースのMac管理を行うには内蔵のMDMでは事足りません。Jamfのようなサードパーティのソリューションを活用することで、高度なMac管理が可能になります。

クライアント管理機能の例

- PKGやDMGのインストール
- FileVaultの実行
- ディレクトリへのバインド
- スクリプトの実行
- ドックのカスタマイズ
- EFIファームウェアのパスワード設定
- プリンタのインストール
- アカウント作成
- ソフトウェアアップデートの設定



Apple のサービスとプログラム

教育機関や企業でMacが普及するにつれ、デバイスを大規模に導入する最適な方法や、Apple IDやアプリ購入にどう対処するかについてさまざまな課題が生じるようになりました。そこでAppleは、これらの疑問を解消し、より簡単かつコスト効率の良いデバイスの一括管理を実現するために、より優れたデバイス管理プログラムやサービスを導入しました。

しかしながら、すべてのAppleデバイス管理ソリューションが、Appleのプログラムやサービスに対応しているわけではありません。ご利用中のソリューションがこれらのプログラムやAppleが定期的に行うアップデートに対応しているかどうか、ベンダーに確認することが大切です。

ゼロタッチ導入

AppleのMDM自動登録ソリューションを使用すると、組織の規模に関わらず、AppleまたはAppleの正規販売代理店から購入したデバイスを事前に構成することができます。その際、デバイスに触れる必要は一切ありません。ゼロタッチ導入（旧DEP）を活用することで、新しいデバイスの受け取り、開封、構成をIT管理者が一手に担う必要がなくなり、代わりにデバイスを従業員の自宅に直接発送することができます。箱を開けて初めてデバイスの電源を入れると、自動的にAppleとMDMが通信し、必要な構成や設定、管理タスクが実行されます。

Appとブック

Appsとブック（旧VPP）では、AppleからAppやブックを一括購入し、Apple ID経由またはApple IDがない場合は直接、ユーザに配布することができます。導入のニーズに応じて、Appの再割り当てを行うことも可能です。Appleから受け取ったAppやブックのサービストークンは、Appleデバイス管理ソリューションにリンクして割り当てや配布を行うことができます。

Apple Business Manager

IT管理者向けのウェブベースのポータルであるApple Business Managerでは、「ゼロタッチ導入」と「Appとブック」を組み合わせてすべてを一元的に管理することができます。教育機関以外のすべての組織で利用でき、既存のDEPまたはVPPアカウントがある場合は簡単にApple Business Managerにアップグレードすることが可能です。既存アカウントがない場合は、business.apple.comから登録できます。

Apple School Manager

Apple School Managerは、ユーザ、デバイス、コンテンツを一ヶ所で管理できる、IT管理者向けのウェブポータルです。教育機関専用のこのポータルには、Appとブック、ゼロタッチ導入に加えて、クラスルームAppなどの教室管理ツールも揃っており、管理対象Apple IDや共有iPadの管理、生徒情報システム（SIS）との統合が可能です。

Apple ID

Apple IDは、App Store、iTunes Store、iCloud、iMessageなどのサービスにアクセスするためにユーザが使用するアカウント認証情報です。組織のニーズに応じて、エンドユーザのApple IDを業務に使用したり、またはApple IDをまったく使わないこともできます。教育機関の場合、生徒には異なる種類のApple IDが提供されます。

管理対象Apple ID

教育機関向けのApple School Managerは、生徒による管理対象Apple IDの利用や生徒情報システム（SIS）との統合を可能にします。管理対象Apple IDは、生徒に割り当てることのできる特殊なApple IDです。特別な権限を必要とせず、IT管理者はユーザ情報を作成または動的にアップデートすることができます。管理対象Apple IDはApple School Managerのポータルで作成でき、クラスルームAppのデータだけでなく、学校のSISとも同期させることが可能です。

企業や政府組織の場合、管理対象Apple IDはApple Business Manager内で管理目的にのみ使用されます。

クラスルームApp

クラスルームAppは、クラスでの指導を効率化し、コミュニケーションやコラボレーションを促進し、生産性を向上させるための教育者向けツールです。生徒のデバイスから特定のアプリやウェブページだけにアクセスできるように設定できるほか、生徒のデバイスをモニタリングして授業の理解度を確認することもできます。

ライフサイクル管理のステージ

Appleのデバイス管理フレームワーク（「MDMフレームワーク」）には、Appleデバイスのライフサイクルを構成する6つの要素が含まれています。

macOS、iOS、iPadOSおよびtvOSが搭載されたAppleデバイスに内蔵されているMDMは、以下の機能を提供します。

1 Macの導入とプロビジョニング

デバイスをエンドユーザに届けます。

2 構成管理

デバイスに正しい設定を適用します。

3 アプリ管理

各デバイスに正しく最新なソフトウェアとアプリがインストールされていることを確認します。

4 macOSのインベントリ

各デバイスの状態を報告します。

5 Macのセキュリティ

組織の基準に沿ってデバイスを保護します。

6 ユーザ支援

リソースやサービスへのセルフアクセスをユーザに提供します。

導入からエンドユーザエクスペリエンスに至るまで、組織の環境におけるMacのライフサイクル全体を理解し、管理・サポートすることが重要です。これにより、デバイスのセキュリティを確保すると同時に、デバイスの力を最大限に引き出すことができます。

1

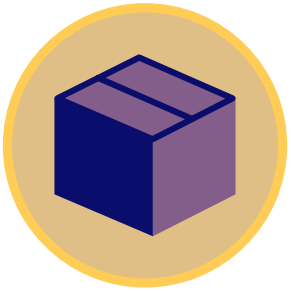
Macの導入とプロビジョニング

デバイスは、エンドユーザ向けに構成する前にAppleデバイス管理ソリューションに登録する必要があります。登録方法は複数あり、効率的でポジティブなユーザエクスペリエンスを求める企業や教育機関には以下の方法を推奨します。

	説明	ユーザ体験	最適なケース
Apple Business ManagerまたはApple School Managerによるゼロタッチ登録	自動登録機能（オンライン）	ユーザがデバイスを受け取って電源を入れた瞬間に自動的に構成されます	開封してすぐに使用できるため、リモートワークをする従業員に直接デバイスを発送したい、または迅速なセットアップを希望する場合に最適です
ユーザ主導の登録（URL経由）	手動登録（オンライン）	ユーザが特定のURLにアクセスし、デバイスの設定を行います	管理されていないリモートデバイスがある場合、またはデバイスを新しいMDMサーバに再登録する必要がある場合

ゼロタッチ導入

1. Appleの公式サイトからAppleの導入プログラムに登録し、使用しているMDMサーバをポータルに追加します。

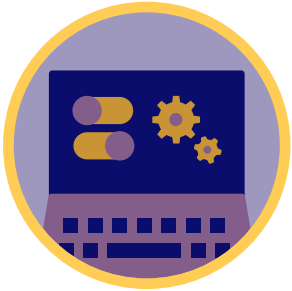


2. Macを購入し、Appleの導入プログラムのアカウントに紐付けた後で、ユーザに直接発送します。

3. ユーザが初めてMacの電源を入れたタイミングで自動的に登録されるため、特別な操作は必要ありません。

4. MacがMDMサーバに登録されます。デバイスに適用したい構成プロファイルやアプリを用意します。

5. Microsoft Officeのインストールやカスタムスクリプトの実行などといった高度な管理タスクを行う場合は、クライアント管理エージェントであらかじめ定義しておく必要があります。



6. デバイスが構成とアプリを受信し、ユーザはホーム画面に戻ります。ITが指一本触れずにデバイスの構成が完了し、管理対象下に置かれました。

Appleの導入プログラムが利用できない場合は、ゼロタッチ導入には劣りますが、従来のワークフローまたはユーザ主導の登録ワークフローを使用してMacをプロビジョニングすることも可能です。

2

構成管理

Macコンピュータの構成には無限の可能性が秘められています。エンドユーザのニーズに応じて、個々のデバイスやデバイスのグループをさまざまな形でパーソナライズし、カスタマイズすることができます。

構成プロファイル

構成プロファイルはmacOSの設定を定義するために作成されるXMLファイルで、管理ソリューションを利用してデバイスに配布します。ユーザが必要なリソースにシームレスにアクセスできるように、Wi-Fi、VPN、メール設定などを含む数多くの設定を適用させることができます。

ポリシー

MacOSのクライアント管理ソリューション特有の機能であるポリシーは、MDMの構成プロファイルが持つ基本的なデバイス管理機能を超えて、カスタムソフトウェアやプリンタのインストール、ローカルユーザアカウントの管理、高度な管理ワークフローの実行などを可能にします。これにより、自動化したいタスク、実行の頻度やタイミング、どのユーザまたはデバイスに対して実行するかなどを指定することができます。

Apple製品の管理ソリューションの中には、ポリシーやスマートターゲティングの機能を提供していないものもあります。詳細はご利用のベンダーにご確認ください。

何から始めたらいいのかわからない場合は、一般的なMDMの構成プロファイルが記載された**こちらのリスト**をご参照ください。また、**JamfNation**で相談することもできます。

スクリプト

ポリシーの一環として、クライアント管理ソリューションに含まれるAppleデバイス管理能力を利用して、macOS上でシェルスクリプトを実行します。ターミナルでコマンドラインを使って実行できるものであれば、何でもスクリプトにすることができます。スクリプトは標準的な構成プロファイルよりもはるかに柔軟性があり、無限のデバイス管理能力を可能にします。

スマートターゲティング

ソフトウェアアップデートやセキュリティ強化、あらかじめ定義されたカスタムインベントリ属性を必要とするデバイスを含む、すべての管理対象デバイスのインベントリ詳細を収集します。また、インベントリの基準に基づいてグループを作成し、特定の個人またはグループに対してデバイス管理タスクを自動的に有効化したり、ユーザが自分でアクセスできるようにアイテムを組織のアプリカタログに用意したりすることも可能です（ご利用のデバイス管理ソリューションによってはできない場合もあります）。

アプリ管理

アプリの基礎

多くの組織が、Mac App StoreからMacソフトウェアを入手しています。Appleは、アプリのセキュリティとパフォーマンスを確保するために、Mac App Storeで開発者のコードを審査します。これが、Appleがセキュリティ面で高い評価を得ている理由のひとつです。しかし、Mac App Store以外で手に入るMac用のソフトウェアも存在します。

その中にはGoogle Chrome、Microsoft Office、Adobe Creative Suiteなどの人気ソフトウェアも含まれており、カスタムソフトウェアを導入できるMacクライアント管理ツールが必要になります。Apple製品の管理ソリューションの中には、インストール前後のスナップショットを作成することで、カスタムの.pkgや.dmg（Macソフトウェアのインストールファイルタイプ）を構築することのできる機能を持つものがあります。このようなソフトウェアパッケージは、ユーザ側で何もしなくても管理対象のMacに導入することができます。

コミュニケーションや学習、生産性を促進させるためのネイティブなツールが内蔵されているMacは、消費者に広く普及しています。そして、その人気をさらに際立たせているのが豊富に用意されたアプリケーションです。アプリの導入を管理するデバイス管理ソリューションを採用することで、ユーザが必要なアプリを適切に使用できるようにするとともに、組織の環境に合わせたセキュアな運用を実現することができます。Appleにプリインストールされたアプリ、Mac App Storeで入手可能なアプリ、サードパーティ製アプリ、あるいは自社製のカスタムアプリのいずれを利用する場合でも、必要なアプリが安全に利用できる環境を用意することが重要です。

ソフトウェアインストール時のスナップショットを作成

カスタムの.pkgまたは.dmgファイルの作成

Jamf Agent経由でプッシュインストール

Mac App Storeで提供されているソフトウェアの場合、Appleの導入プログラムを利用することで、Apple IDを使わずにすべてのデバイスに対してアプリを配布することができます。

ソフトウェアのインストールとパッチの適用

Jamf Title Editorは、Jamf Proが提供するmacOSデバイス向けのパッチ管理機能を拡張し、カスタムソフトウェアタイトルの提供や既存のパッチ定義の上書き、カスタムパッチ定義の作成を可能にします。さらに、Jamfではサードパーティ製アプリを効率的に導入するための「Appインストーラ」と呼ばれるインストーラパッケージも提供しています。

カスタムパッケージの導入

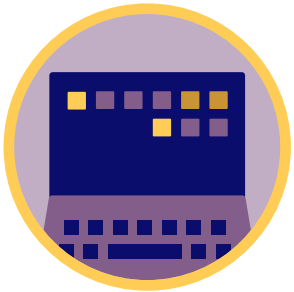
アプリを単に導入するだけでなく、いくつかの設定を事前にカスタマイズしたい場合には、アプリ構成の使用をお勧めします。アプリ開発者は、MDM サーバで事前に構成できる項目をあらかじめ定義することができます。たとえば、サーバの URLがすでに入力された状態でBoxアプリを導入するように定義しておけば、ユーザはユーザ名とパスワードを入力するだけでアプリを起動できるようになります。まずは、ご利用のMDMがカスタムソフトウェアをパッケージ化してMacに導入する機能を提供しているかどうかをご確認ください。

Apple製品の導入プログラムでMac用のアプリやブックを導入する

Appleが提供する導入プログラムを利用することにより、組織はアプリを一括購入し、エンドユーザやデバイスに自動的に配布することができます。

1 Apple Business ManagerまたはApple School Managerに登録する

2 Apple Business ManagerまたはApple School Managerのアカウントをを MDMサーバにリンクします。



3 各導入プログラムのポータルでアプリやブックを検索・購入します（無料アプリの場合も「購入手続き」を行う必要があります）。

4 無料アプリを含むアプリライセンスをMDMサーバに追加します。アプリは、デバイスに直接割り当てることができるほか、ユーザのApple IDに割り当てることもできます。

4 メールやプッシュ通知でアプリの導入にユーザを誘導します。

4 アプリが直接デバイスに導入されます（Apple IDやユーザによるアクションは必要ありません）。

5 アプリがユーザのApple IDにリンクされ、Mac App Storeの「購入済み」タブに表示されます。

4

macOSのインベントリ

トップクラスのAppleデバイス管理ソリューションは、クエリを作成してAppleデバイス上で大量のインベントリデータを収集することができるため、常に最新のデバイス情報を入手し、十分な情報に基づいた管理上の意思決定を行うことができます。シリアル番号、OSバージョン、インストールされているアプリなどのインベントリ情報を、さまざまな頻度で収集することが可能です。

MDMのデバイス管理およびクライアント管理機能を使用して収集されたデータには以下のようなものが含まれます。

ハードウェアの詳細

- デバイスの種類
- デバイスモデル
- デバイス名
- シリアル番号
- UDID
- バッテリレベル

ソフトウェアの詳細

- OSバージョン
- インストール済みのアプリ
- ストレージ容量
- 空き容量
- iTunes Storeのステータス

管理の詳細

- 管理ステータス
- 監視ステータス
- IPアドレス
- 登録方法
- セキュリティステータス

追加情報

- インストール済みのプロファイル
- インストール済みの証明書
- アクティベーションロックのステータス
- 購入情報
- インベントリの最終アップデート

macOSのインベントリ

インベントリが重要な理由

状態がわからないものを管理することはできません。Appleデバイス管理ソリューションが収集するインベントリデータは、さまざまなビジネスにニーズに応え、よくある疑問に答えてくれます。

すべてのデバイスに対して安全が確保されているか

いくつのアプリが導入されているか

特定のデバイスに搭載されているiOSのバージョン

管理ソリューションの中には、特定のハードウェアやソフトウェアのアドオンに関するカスタムインベントリを追加で収集できるものもあります。例えば、サードパーティ製のバックアップツールが最後に実行されたのはいつか、どのプリンタドライバがインストールされているかなどを把握することができます。

Appleデバイスの管理ソリューションを選ぶ際には、**できるだけ幅広いインベントリ情報を収集**できるものを選ぶことをお勧めします。

スマートターゲティング

インベントリデータを活用したスマートターゲティングでは、デバイスを動的にグループ化し、構成プロファイルや制限を導入することができます。Jamfでは、これを以下のように定義しています。

スタティックグループ

プロファイルまたはポリシーを適用

スマートグループ（特許取得済み）

8GB RAM、80%%の空き容量があるハードディスク、バージョン12.2.1かそれ以降を搭載しているすべてのMacを検索

プロファイルまたはポリシーを適用

スタティックグループとスマートグループの比較

スタティックグループは、例えば教室や研究室などで使用される特定のデバイスから構成され、グループ全体に管理ポリシーを適用することが可能です。

スマートグループは、インベントリデータに基づき常に変化する動的なもので、デバイスを動的にグループ化して構成プロファイルや制限を自動的に導入することができます。

5

Macのセキュリティ

デバイスのセキュリティやプライバシー、企業リソースへのアクセスは、どの組織にとっても一番の懸念点となっています。このような懸念を和らげるため、macOSには数々のセキュリティ機能が搭載されています。Appleデバイスの管理 のソリューションと組み合わせることで、デバイスだけでなくアプリやネットワークの安全性も確保できます。

MacOSのセキュリティ機能やMacに特化したエンドポイント保護に興味のある方は、こちらの**初心者ガイド**をご覧ください。

macOSのセキュリティ機能

- ソフトウェアアップデート
- システム整合性保護（SIP）
- Gatekeeper
- App Store
- FileVault暗号化
- XProtect
- アプリのサンドボックス化
- プライバシー

Macのセキュリティ

Unixをベースに作られているAppleのオペレーティングシステム（OS）は、中核に強力なカーネルを備えています。AppleのOSはセキュリティを考えて設計され、独自のセキュリティ設定が用意されており、Appleデバイスの管理ソリューション経由で管理することができます。

さらに、Appleデバイスの導入プログラムとAppleデバイス管理ソリューションを併用することで、組織の環境内でこれらの設定をより細かく管理することが可能になります。

5

Macのセキュリティ

Mac向けの MDMセキュリティ コマンド

- FileVaultの強制適用
- Gatekeeperの設定適用
- ソフトウェアアップデートの設定
- コンピュータのロックとワイプ
- 制限されたアプリの削除
- MDMの削除
- AirDrop経由のパスワード共有の制限

条件付きアクセス

従来の業務時間や働く場所が変化し、現代のモバイルワークフォースが生まれました。従業員が従来の業務時間に拘らずオフィス以外の場所で仕事をするようになり、クラウド上にあるリソースにアクセスする必要性が生じたことで、ITチームが建てた「壁」で従業員やデバイス、機密データを保護する時代は過去のものとなりました。クラウドに移行した組織やデバイスの選択肢を従業員に提供する組織では、Macデバイスのために条件付きアクセスを提供することが重要になります。また、Windows Azure ADやOffice 365を活用している組織の場合は、条件付きアクセスとの統合が内蔵されたトップクラスのAppleデバイス管理ソリューションが必要となります。MacOSと条件付きアクセスの詳細については、JamfとMicrosoft Enterprise Mobility＋Security（EMS）とのパートナーシップについて説明した**こちらのページ**をご覧ください。これにより、Azure AD認証によりセットアップされたアプリケーションにアクセスするデバイスのコンプライアンス管理を自動的に行い、条件付きアクセスを活用して、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ます。

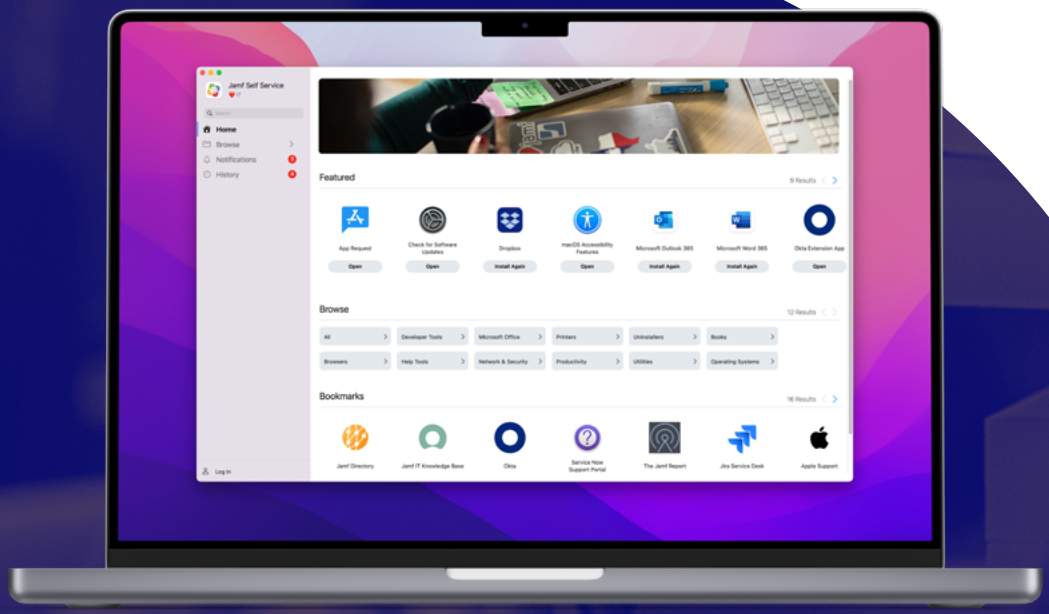
ソフトウェアのアップグレード

macOSの大型リリースを毎年行うことで、Appleはペースを落とさずにイノベーションを突き進めてきました。Appleは毎年、消費者向けに新機能を発表するだけでなく、セキュリティの強化と脆弱性の修正を行います。これらのアップデートは、従業員や生徒が使用するデバイス上のデータを保護する上で非常に重要です。そのため、Appleからリリースされたアップデートの導入はもちろんのこと、それに伴う新しい管理機能も迅速にサポートしてくれる管理ソリューションが必要になります（**即日サポートが理想的**）。

6

ニーズに応じたユーザ支援

Lyft、Headspace、Duolingoのようなオンデマンドツールの台頭により、今日のワーカーは必要な時に必要なツールを入手することを求めています。エンタープライズのアプリカタログは、リソースやコンテンツ、ヘルプ、信頼できるアプリへのワンクリックアクセスを提供します。これにより、ユーザはIT部門に問い合わせることなく、必要なものを手に入れることができます。



MAC用アプリカタログ

例：JamfのSelf Serviceは、組織のリソースやイントラネットとのシームレスな統合も可能なMac用アプリです。

エンタープライズのアプリカタログ経由でアクセスできるもの：

- App Storeのアプリや自社アプリ、サードパーティーソフトウェア
- メール、VPN、その他の構成
- 電子書籍、ガイド、ビデオ
- ブックマークとショートカット
- プリンタのマッピングとドライバ
- ヘルプデスクへの問い合わせやハードウェアのリクエスト
- パスワードのリセットとコンプライアンス情報
- 基本的なメンテナンスやシステム診断
- ソフトウェアとOSのアップグレード
- シングルサインオン（SSO）との統合
- 英語、フランス語、ドイツ語、日本語、中国語（簡体字）の言語対応

ニーズに応じたユーザ支援

オンデマンドアプリとリソースカタログのメリット

ITチームにとってのメリット

- 組織の環境をコントロールしながら、ヘルプデスクへの問い合わせやサポートコストを削減
- 管理対象のMacにアプリカタログ（例：Jamf Self Service）を自動インストール
- ディレクトリサービスとの統合により、部署、ユーザの役割、ロケーションなどに基づいてコンテンツをパーソナライズ
- パスワードのリセットやシステム診断など、一般的なITタスクを自動化

ユーザにとってのメリット

- さまざまなリソースに好きな時に自分でアクセス
- 使用言語や環境に合わせてパーソナライズされた直感的なユーザインターフェース
- 企業情報へのアクセスを提供する、HR関連ツール、コミュニケーションプラットフォーム、社内リソースなどの一般的なウェブサービスをブックマーク
- ITの助けを借りずに組織が承認したアプリをセルフインストール
- プリンタのインストールやソフトウェアのアップデートなど、一般的なITタスクを迅速に解決
- 利用可能なサービスやセキュリティの強化について、リアルタイムで通知を受けることが可能

サードパーティとの統合

Macの管理は、組織が行わなければならない多数のITタスクのほんのひとつに過ぎませんが、非常に重要かつ不可欠な要素です。ServiceNowのようなヘルプデスクのチケット管理ツールや、OktaのようなSSO認証ツールを含め、既存のITツールとシームレスに統合できるAppleデバイス管理ソリューションを見つけることが重要になります。

Jamf Marketplaceに見られるようなサードパーティツールとの統合は、既存のツールやエコシステムの持つ力を増幅してくれます。業界の枠組みを超えた統合から特定のソリューションまで、このような統合はITチームと各サービスの架け橋となり、統合された安全でシームレスな体験をエンドユーザに提供します。

トップクラスのAppleデバイスの管理ソリューションは、既存の企業リソースに合わせてアプリカタログをブランディングできる機能を提供します。これにより、既存の社内ツールとシームレスに統合した、ユーザにとって馴染みやすく使い勝手の良いアプリカタログが実現します。

インフラ計画

デバイス管理ソリューションの選択と同じくらい重要なのが、それをどこでホスティングするかです。クラウドでホスティングする場合、アップグレードが容易になるだけでなく、サーバの管理やトラブル処理などを含む多くのタスクからITチームを解放してくれます。

クラウドに移行する組織がますます増えています

エンタープライズは以下を含む多くの理由からクラウドを利用しています。

クラウドホスティングのメリット

- サーバのプロビジョニング、セキュリティの維持、アップデート管理
- バックアップ管理と検証
- 世界中どこからでもアクセス可能なストレージ
- オフサイトでトラブルが発生した際の対応
- データベース管理、セキュリティの維持、アップデート
- サーバの監視と対応チーム

業界トップクラスの Apple管理ソリューション

エンタープライズ間のパートナーシップ（IBM、Cisco、SAPなど）や従業員選択プログラムの拡大に伴い、Mac、iPad、iPhone、Apple TVの業務利用はますます増加する見込みです。

Appleデバイスの持つ力やテクノロジーへの投資を最大限に活かすには、Appleに寄り添った管理ソリューションが必要です。

トップクラスのAppleデバイス管理ソリューションを提供するJamfは、エコシステム全体で一貫した管理体制を確立したいと考える企業や教育機関から大きな信頼を得ています。

無料トライアルでJamfのパワーを実際に体験してみませんか？

トライアルに申し込む

または販売代理店経由でお試しいただくことも可能です。