Mac導入の概要

概要

目次

Appleは、社員の能力を最大限に引き出すには、社員が最高のツールとテクノロジーにアクセスできるようにすることが重要と考えています。Appleの製品はすべて、オフィスでも外出先でも、社員がよりクリエイティブに、生産的に、新しい方法で仕事ができるようにデザインされています。この方針は、現代社会で社員が求める働き方と一致しています。社員は、情報にアクセスしやすくコラボレーションや共有が円滑にできること、どこにいても自由につながりを維持して仕事ができることを求めています。

ビジネス環境へのMacコンピュータの導入と設定は、今やこれまでになく簡単なものになりました。Appleが提供する主なサービスと他社製のモバイルデバイス管理（MDM）ソリューションを組み合わせれば、Macの大規模な導入とサポートを容易に行うことができます。すでにiOSおよびiPadOSデバイスを導入済みの組織なら、macOSの実装に必要なインフラストラクチャ作業のほとんどが、すでに完了している可能性があります。

最近改善されたMacのセキュリティ、管理、および導入に関する機能により、組織は、モノリシックイメージの作成や従来型のディレクトリバインド設定から、シームレスなプロビジョニングモデルおよび導入プロセスへと移行できます。この作業は、各ユーザーが中心となって、macOSに内蔵されたツールのみでほぼ対応することができます。

本書では、既存インフラストラクチャの理解からデバイス管理および効率的なプロビジョニングまで、Macの大規模導入に必要なあらゆることについてのガイダンスを提供します。本書で扱うトピックの詳細は、オンラインのMac導入リファレンス（support.apple.com/ja-jp/guide/deployment-reference-macos）で説明しています。

はじめに

導入方針と導入計画の策定および社員が使っている既存のmacOSの評価は、導入プロセスの重要な最初の手順です。必要なチームを早期に確保し、プログラムのビジョンと目標に足並みをそろえるようにしてください。チームによっては、環境独自の問題点を見つけるために、小規模な概念実証から始める場合もあります。さらに範囲を広げて既存ユーザーも含めたパイロットを実施し、組織全体でデバイスがどのように使われているかを把握し、問題があればチームがそれを認識できるようにすることが非常に重要です。

この段階で収集した情報は、どのような役割や機能を持つ社員がMacを最も有効に利用できるかを判断するのに役立つ場合があります。その後、IT部門は、macOSを組織全体の標準仕様として提供するのか、特定業務のための選択肢として提供するのかを評価できます。

この段階では、Macを広く導入する前に互換性を確保する必要がある社内アプリケーションやツールの包括的なリストも完成させることができます。多くのユーザーをカバーする生産性向上、コラボレーション、コミュニケーションのための主要アプリケーションに、主に焦点を合わせてください。企業イントラネット、ディレクトリ、経費管理ソフトウェアなどの重要な社内サービスも、組織の大部分の生産性を左右する重要な要素です。

ほかの社内ツールについての回避策や代替策を文書化して周知し、必要に応じて各アプリケーションの所有者に更新を促します。社員がMacを選んだ場合に使えるようになる様々なビジネスアプリケーションを明らかにし、ユーザーの需要に応じて更新作業の優先度を判断します。必要な場合は、アプリケーション所有者と一緒に、アプリケーションの更新方法について計画を立てます。その際は、macOS SDKとSwift、および開発支援を提供する様々なタイプのエンタープライズパートナーを活用できます。

一般に、Macコンピュータは会社所有のデバイスとして配布されます。企業によっては、個人所有デバイスの持ち込み（BYOD）プログラムを通じて、社員が職場でMacを使えるようにしている場合があります。どちらの所有モデルの場合も、社員がApple製品を職場で使用できるようにすると、組織全体のメリットにつながります。社員の生産性、創造性、意欲、仕事に対する満足度が向上するだけでなく、残存価値とサポートを考慮するとコスト削減にもなります。組織はまた、様々なリースおよびファイナンシングオプションを利用することによって、初期費用を抑えることもできます。アップグレード時に給与天引きで社員が負担したり、リース期間やライフサイクルの終了時に社員がデバイスを買い取れるようにしたりして、コストを埋め合わせることもできます。

企業ポリシー、および本書に記載されている導入、管理、サポートの各プロセスは、パイロット期間に収集された情報に応じて、異なってくる場合があります。すべてのユーザーがまったく同じポリシー、設定、アプリケーションを必要とするわけではありません。多くの場合、同じ社内でもグループやチームによって要件は大きく異なります。

導入の手順

macOSの導入には、主に4つの手順があります。環境の準備、MDMの設定、社員へのデバイス導入、そして継続的な管理タスクの遂行です。

1. 準備する

導入の最初のステップは、既存環境の検討です。この段階では、ネットワークと主なインフラストラクチャ、および導入を成功させるために必要なシステムのセットアップに対する理解を深めます。

インフラストラクチャを評価する

Macはほとんどの標準的なエンタープライズIT環境とシームレスに統合できますが、macOSが提供するすべての機能を最大限に活用するためには、既存のインフラストラクチャを評価することが重要です。この分野でサポートが必要な場合は、チャネルパートナーや取扱店のテクニカルチームのサポートを受けられます。

Wi-Fiとネットワーク機能

継続的で信頼できるワイヤレスネットワークへのアクセスは、macOSデバイスの設定と構成に不可欠です。アクセスポイントの配置や性能を慎重に検討するなど、企業のWi-Fiネットワークが適切に設計されていることを確認し、ローミングと容量のニーズに対応できることを確認します。

デバイスがAppleのサーバ、Appleプッシュ通知サービス（APNs）、iCloud、またはiTunes Storeにアクセスできない場合は、ウェブプロキシまたはファイアウォールポート構成の調整が必要になる可能性もあります。iPadやiPhoneの場合と同様、Mac導入プロセスの特定の段階（特に新しいMacハードウェアの場合）では、インストール時のファームウェアアップデートなどを行うため、これらのサービスへのアクセスが必要です。

AppleとCiscoはMacコンピュータがCiscoのワイヤレスネットワークと通信する方法を最適化し、macOSではQuality of Service（QoS）のような高度なネットワーク機能をサポートしています。Ciscoのネットワーク機器をお使いの場合は、社内チームと協力し、Macが重要なトラフィックを確実に最適化できるようにしてください。

また、ユーザーがリモートから企業リソースに安全にアクセスできるようにするために、VPNインフラストラクチャも評価する必要があります。必要な場合のみVPN接続を開始できるように、macOSのVPNオンデマンド機能を利用することを検討してください。Per-App VPNを使う場合は、お使いのVPNゲートウェイがこれらの機能をサポートしていることと、適切なユーザー数と接続数に対応できる十分なライセンスを購入していることを確認します。

ネットワークインフラストラクチャで、Appleの標準ベースのゼロ構成ネットワークプロトコルであるBonjourが、正しく動作するよう設定されていることも確認します。Bonjourには、ネットワーク上のサービスをデバイスが自動的に検出できるようにする役割があります。macOSはBonjourを使って、AirPrint対応プリンタや、Apple TVなどのAirPlay対応デバイスに接続します。アプリケーションおよびmacOSの内蔵機能の中には、Bonjourを使用してほかのデバイスを検出し、コラボレーションや共有を行うものもあります。

Wi-Fiネットワークの設計についてさらに詳しく：
support.apple.com/ja-jp/guide/deployment-reference-macos

MDM向けのネットワーク構成についてさらに詳しく：
support.apple.com/ja-jp/HT210060

Bonjourについてさらに詳しく：
support.apple.com/ja-jp/guide/deployment-reference-macos

IDの管理

macOSは、Active Directory、Open Directory、LDAPなどのディレクトリサービスにアクセスして、IDやその他のユーザーデータを管理することができます。一部のMDMベンダーは、自社の管理ソリューションをActive DirectoryおよびLDAPディレクトリとすぐに統合できるツールを提供しています。macOS CatalinaのKerberosシングルサインオンExtensionなどの追加ツールを使えば、Active Directoryのポリシーと機能に統合でき、従来のバインド設定やモバイルアカウントは必要ありません。IDが自動的に信頼されるように、社内外の認証局（CA）から発行された様々なタイプの証明書もMDMソリューションで管理できます。

新しいKerberosシングルサインオンExtensionについてさらに詳しく：
support.apple.com/ja-jp/guide/deployment-reference-macos

ディレクトリの統合についてさらに詳しく：
support.apple.com/ja-jp/guide/deployment-reference-macos

社員が使用する主要サービス

Microsoft Exchangeサービスが最新の状態になっており、ネットワークのすべてのユーザーをサポートするように構成されていることを確認してください。Exchangeを使用していない場合でも、macOSはIMAP、POP、SMTP、CalDAV、CardDAV、LDAPなど、標準ベースのサーバに対応しています。ユーザーの日々の重要なワークフローの大部分を占める、Eメール、連絡先、カレンダー、およびその他のエンタープライズ向け生産性向上ソフトウェアとコラボレーションソフトウェアの基本ワークフローをテストします。

Microsoft Exchangeの構成についてさらに詳しく：
support.apple.com/ja-jp/guide/deployment-reference-macos

標準規格に基づくサービスについてさらに詳しく：
support.apple.com/ja-jp/guide/deployment-reference-macos

コンテンツキャッシュ

コンテンツキャッシュはmacOSに統合された機能です。頻繁にリクエストされるAppleサーバのコンテンツはローカルにコピーが保存されるため、ネットワークでコンテンツのダウンロードに必要な帯域を節約するのに役立ちます。キャッシュを使って、Mac App Storeからのソフトウェアのダウンロードと配布を高速化できます。ソフトウェアアップデートもキャッシュできるので、組織が所有するmacOS、iOS、iPadOSのどのデバイスにも、高速でダウンロードできます。CiscoやAkamaiの他社製ソリューションを使えば、その他のコンテンツもキャッシュできます。

コンテンツキャッシュについてさらに詳しく：
support.apple.com/ja-jp/guide/deployment-reference-macos

管理ソリューションを確立する

MDMを利用すると、ビジネス環境でMacを安全に登録する、設定やアップデートをワイヤレスで行う、アプリケーションを導入する、ポリシーのコンプライアンスをモニタリングする、デバイスの照会を行う、管理対象デバイスをリモートでワイプまたはロックする、といった操作ができます。IT部門は、プロファイルを作成して社員のアカウントを管理したり、システムを設定したり、制限を適用したり、パスワードポリシーを設定したりすることができます。これらはすべて、iPhoneとiPad向けに現在使っているモバイルデバイス管理ソリューションをそのまま使用して、簡単に実行できます。

すべてのAppleプラットフォームにはAppleの共通管理フレームワークが組み込まれているため、お客様は他社製の様々なMDMソリューションを利用することができます。Jamf、VMware、MobileIronなど、幅広いデバイス管理ソリューションが他社から提供されています。macOSは、デバイス管理についてiOSやiPadOSと同じフレームワークを多く共有していますが、他社製のMDMソリューションは管理機能、オペレーティングシステムのサポート、価格体系、ホスティングモデルに若干の違いがあります。また、統合、トレーニング、サポートについても様々なレベルのサービスが提供されています。ソリューションを選ぶ前に、自分の組織にとって最も重要な機能は何かを評価してください。

使用するMDMを選択したら、Apple Push Certificates Portalにアクセスしてログインし、新しいMDMプッシュ証明書を作成する必要があります。

MDMの導入についてさらに詳しく：
support.apple.com/ja-jp/guide/deployment-reference-macos

Apple Push Certificates Portalを開く（英語）：identity.apple.com/pushcert/

Apple Business Managerに登録する

Apple Business Managerは、IT管理者がiPhone、iPad、iPod touch、Apple TV、およびMacの導入をすべて1か所で行える、ウェブベースのポータルです。既存のモバイルデバイス管理（MDM）ソリューションとシームレスに連係することで、Apple Business Managerでは、デバイス導入の自動化、アプリケーション購入とコンテンツ配布、社員の管理対象Apple IDの作成を簡単に行うことができます。

Device Enrollment Program（DEP）とVolume Purchase Program（VPP）はApple Business Managerに完全に統合され、Appleのデバイスを導入するために必要なものがすべて1か所に集まりました。2019年12月1日より、統合前のプログラムは使用できなくなります。

デバイス

Apple Business Managerでは、Automated Device Enrollmentによって、企業が所有するAppleデバイスをすばやく効率的に導入し、デバイスに触れたり準備したりすることなくMDMに登録できます。

- 設定アシスタントのステップを合理化することで、ユーザーの設定プロセスを簡略化できます。社員はアクティベーション後すぐに正しい構成を確実に受け取れるようになります。IT部門はこのプロセスをさらにカスタマイズし、同意文書、企業のブランディング、最新の認証方法を社員に提供できるようになりました。
- 監視モードを使うと、ほかの導入モデルにはないデバイス管理コントロール（削除不可のMDMなど）を利用して、会社所有のデバイスをより高度なレベルで制御できます。

- デバイスの種類に応じてデフォルトのサーバを設定することで、デフォルトのMDMサーバがさらに管理しやすくなります。また、Apple Configurator 2を使用することで、購入方法にかかわらずiPhone、iPad、Apple TVを手動で登録できるようになりました。

コンテンツ

Apple Business Managerでは、コンテンツを簡単に一括購入できます。社員が使用するデバイスがiPhoneでも、iPadでも、Macでも、フレキシブルでセキュアな配布方法を利用して、すぐに使える優れたコンテンツを提供できます。

- アプリケーションや本、カスタムアプリケーションを一括購入でき、社内で開発したアプリケーションも入手できます。ある拠点から別の拠点へアプリケーションのライセンスを転送したり、ライセンスを同じ拠点の購入担当者間で共有したりできます。また、MDMで使用中のライセンスの数を含め、購入履歴をまとめて一覧表示することも可能です。
- 管理対象デバイスまたは承認済みユーザーにアプリケーションや本を直接配布し、どのコンテンツがどのユーザーやデバイスに割り当てられているかを簡単に把握することができます。管理配布により、組織がアプリケーションの所有権を完全に保持したまま、配布プロセス全体をコントロールできます。デバイスまたはユーザーが必要としなくなったアプリケーションは、割り当てを無効にし、組織内の別のデバイスまたはユーザーに割り当て直すことができます。
- 支払いには、クレジットカードや発注書など複数の方法を利用できます。組織は一定の金額のVolume Creditを現地通貨でAppleまたはApple正規取扱店から購入でき（利用可能な場合）、購入したVolume Creditはアカウントの所有者にストアクレジットとして電子的に届けられます。
- アプリケーションは、そのアプリケーションが利用可能な国なら、どの国のデバイスやユーザーにも配布できるので、複数の国への配布が可能です。デベロッパはApp Storeで通常の公開手続きをするだけで、複数の国でアプリケーションを提供できます。

注意：一部の国と地域では、Apple Business Managerを使って本を購入することができません。国や地域ごとに利用可能な機能と購入方法について詳しくは、support.apple.com/ja-jp/HT207305/を参照してください。

ユーザー

Apple Business Managerでは、組織が社員用のアカウントを作成して管理できます。このアカウントは既存のインフラに統合され、Appleのアプリケーションやサービス、Apple Business Managerへのアクセスを提供します。

- 管理対象Apple IDを作成すれば、社員はAppleのアプリケーションやサービスを使って共同作業できるほか、iCloud Driveを使用する管理対象アプリケーションで業務用データにアクセスできるようになります。管理対象Apple IDは、組織が所有および管理します。
- Apple Business ManagerをMicrosoft Azure Active Directoryに接続して、Federated Authenticationを活用することもできます。対応するAppleデバイスで社員が既存の資格情報を使ってはじめてサインインすると、管理対象Apple IDが自動的に作成されます。
- iOS 13、iPadOS、macOS Catalinaで利用可能になった新しいUser Enrollment機能を使うと、社員が所有するデバイスで個人用と管理対象の両方のApple IDを使用することができます。また、どのデバイスでも、管理対象Apple IDをプライマリ（かつ唯一の）Apple IDとして使うこともできます。Appleデバイスにはじめてサインインした後は、管理対象Apple IDでウェブ上のiCloudにアクセスすることもできます。

- 社内のIT部門にその他の役割を割り当て、Apple Business Managerでデバイス、アプリケーション、アカウントを効率的に管理することができます。管理者の役割を使用すると、必要に応じて利用規約に同意したり、離職した人の権限を簡単に移行したりできます。

注意：User Enrollmentは、現在iCloud Driveをサポートしていません。管理対象Apple IDがデバイス上の唯一のApple IDである場合にはiCloud Driveを使うことができます。

Apple Business Managerについてさらに詳しく：apple.com/jp/business/it

Apple Developer Enterprise Programに登録する

Apple Developer Enterprise Programは、アプリケーションを開発、テスト、ユーザーに配布するための全ツールのセットを提供します。アプリケーションを配布する際は、ウェブサーバでホストするか、MDMソリューションを使います。Macのアプリケーションとインストーラに Developer IDを使って署名して認証を受けると、Gatekeeperに対応できます。Gatekeeperは、マルウェアからmacOSを保護する機能です。

Developer Enterprise Programについてさらに詳しく：
developer.apple.com/programs/enterprise/jp

2. 設定する

導入の設定では、企業ポリシーを定義し、社員のMacを構成できるようにモバイルデバイス管理ソリューションを準備します。

macOSのセキュリティを理解する

セキュリティとプライバシーは、Appleのすべてのハードウェア、ソフトウェア、サービスのデザインの基盤です。Appleは、強力な暗号化機能と、すべてのデータの扱い方を定めた厳格なポリシーによって、お客様のプライバシーを保護します。Appleデバイスのための安全なコンピューティングプラットフォームを実現するには、以下が必要です。

- デバイスの不正使用を防ぐ方法
- デバイスの紛失時または盗難時でも、デバイスに保存されているデータを保護する機能
- ネットワークプロトコルおよびデータ転送時の暗号化
- プラットフォームの完全性を損なうことなく、アプリケーションを安全に実行する機能

Appleのデバイスが安全にネットワークサービスにアクセスできるように、また、重要なデータを保護するために、Appleのすべてのデバイスには何層ものセキュリティが組み込まれています。macOS、iOS、およびiPadOSには、パスコードとパスワードのポリシーによるセキュリティ機能もあります。これらのポリシーはMDMで配布し、適用できます。デバイスが悪意のある人の手に渡ってしまった場合、ユーザーまたは管理者は、リモートコマンドを使ってすべての個人情報を消去できます。

IT部門は、MDMを使って、デバイスのセキュリティを保護するための幅広いポリシーを導入できます。例えば、MDMを使ったFileVaultと復旧キーエスクローの適用、特定のパスワードポリシーやスクリーンセーバロックの適用、内蔵ファイアウォールの有効化などがあります。

Appleプラットフォームのセキュリティについてさらに詳しく：
support.apple.com/ja-jp/guide/security/

企業ポリシーを定義する

企業ポリシーの作成では、まず、社内の大多数のMacユーザーを対象とする全般的なポリシーを確立します。MDMソリューションを使って、アカウントや特定アプリケーションへのアクセスなど、ユーザー固有のカスタマイズを定義できます。また、部門に固有のソフトウェアや設定を導入するなど、ユーザーの組織やその他のグループについて特定のポリシーを設定することもできます。

社内の各チームと協力しながら、Macコンピュータの使用に関するポリシーを既存の企業ポリシーに組み込んでください。パスワードの複雑さや有効期間の要件、スクリーンセーバのタイムアウト、利用規定など、中核となるポリシーはどのプラットフォームでも同じです。

企業ポリシーで、別のプラットフォームで使用される特定のテクノロジーが義務付けられている場合は、そのポリシーが意図する目的を理解し、代替としてmacOSの内蔵テクノロジーを採用するようにポリシーの調整を検討してください。すべてのコンピュータが特定の他社製ソリューションを使ってディスク全体を暗号化することを義務付けるのではなく、企業データは暗号化して保存することを規定するポリシーの作成を検討し、FileVaultでそれを実現してください。マルウェア対策に特定ソフトウェアを使うことがポリシーで定められている場合は、Gatekeeperなどの内蔵機能についてチームに説明し、その使用を認めるようポリシーを更新してください。

MDMで設定を構成する

企業ポリシーの管理を有効化し、社員が必要なリソースにアクセスできるようにするために、MDMソリューションを使って各Macを安全に登録します。Macの登録後、MDMソリューションで構成プロファイルを使って、ポリシーや設定を適用します。構成プロファイルは、MDMソリューションによって作成されるXMLファイルであり、デバイスに設定を配布できます。プロファイルを使うと、設定、アカウント、ポリシー、機能制限、資格情報の構成を自動化できます。システムのセキュリティを向上させるために、プロファイルは署名し暗号化することができます。

デバイスがMDMに登録されたら、管理者はMDMポリシー、クエリ、またはコマンドを開始できます。その後デバイスは、ネットワーク接続を使ってAppleプッシュ通知サービス（APNs）からの通知を一度受け取ります。この通知は、管理者の操作を処理するために、安全な接続を使ってMDMソリューションと直接通信するよう指示するものです。通信はMDMソリューションとデバイスとの間でのみ行われ、APNsが秘密情報を送信することはありません。デバイスを管理対象から削除すると、構成プロファイルによって管理されていた設定とポリシーは削除されます。企業は、必要に応じてデバイスをリモートでワイプすることもできます。

多くの組織は、既存のディレクトリサービスにMDMソリューションを接続しています。macOSの設定アシスタントで、Automated Device Enrollmentを行う際に、ディレクトリサービスの資格情報を使ってログインするようユーザーに求めることができます。macOS Catalinaの新しい登録カスタマイズオプションを使えば、設定アシスタントでクラウドIDプロバイダによる認証を表示できます。デバイスを個々のユーザーに割り当てたら、次に個人またはグループに固有の構成やアカウントのカスタマイズが行われます。例えば、登録時にユーザー個人のMicrosoft Exchangeアカウントを自動的にプロビジョニングできます。また、802.1xやVPNなどのテクノロジーの証明書IDを使うこともできます。

これらのシステムによって管理機能が確保されるため、多くの場合、企業はユーザーに各自のMacに対する管理者アクセス権を付与しています。これにより、MDMでユーザーを企業ポリシーの管理範囲内にとどめつつ、ユーザーは設定を完全にパーソナライズでき、アプリケーションのインストールや問題のトラブルシューティングも行えるようになります。このモデルは、管理下にあるiPhoneまたはiPadに対してユーザーが持つ権限と管理のタイプに従います。

構成プロファイルについてさらに詳しく：
support.apple.com/ja-jp/guide/deployment-reference-macos

Automated Device Enrollmentの準備をする

MDMにデバイスを登録する最も簡単な方法は、Apple Business ManagerのAutomated Device Enrollment機能を使って設定アシスタントで登録する方法です。IT部門が関与することなく登録でき、設定アシスタントの特定画面を省いてユーザー側のプロセスをさらに高速化できます。

Automated Device Enrollmentを構成するには、セキュアなトークンを使ってMDMソリューションとApple Business Managerアカウントをリンクさせます。MDMソリューションを安全に認証するには、2ステップ確認プロセスを使います。特定の実装について詳しくは、MDMベンダーが提供する文書を参照してください。

社員がすでにデバイスを使っている場合や個人所有デバイスの場合は、ユーザーが単一の構成プロファイルを開き、システム環境設定で確認して登録を完了します。これを「User Approved MDM Enrollment」（ユーザー承認型MDM登録）と呼びます。Kernel Extension Policyや「プライバシー」環境設定ポリシー制御など、セキュリティに関わる設定を管理するために、登録は、Device EnrollmentまたはUser Approved MDM Enrollmentを通じて行う必要があります。

Kernel Extensionの読み込みについてさらに詳しく：
support.apple.com/ja-jp/guide/deployment-reference-macos

「プライバシー」環境設定ポリシー制御についてさらに詳しく：
support.apple.com/ja-jp/guide/mdm

アプリケーションと本の配布準備をする

Appleは、macOSで利用可能な素晴らしいアプリケーションやコンテンツを組織が利用できるように、拡張プログラムを提供しています。これらの機能を使うと、独自の社内アプリケーションを含むアプリケーションや本をApple Business Managerで購入して社員に配布し、生産性を高めるために必要なものすべてを社員に提供できます。MDMでは、Mac App Storeで提供されないソフトウェアについても、アプリケーションを配布し、パッケージをインストールすることができます。

MDMソリューションでは、管理配布を使って、Apple Business Managerで購入したアプリケーションと本を配布できます。購入したアプリケーションは、そのアプリケーションが利用可能な国であればどこでも配布できます。管理配布を有効にするには、まずセキュアなトークンでMDMソリューションとApple Business Managerアカウントを関連付ける必要があります。MDMソリューションに接続されると、デバイスでApp Storeが無効になっていても、アプリケーションと本をユーザーに割り当てることができます。また、デバイスにアプリケーションを直接割り当てることもできます。この方法では、そのデバイスを使うユーザーは誰でも各アプリケーションにアクセスできるため、導入を非常に簡素化できます。

Apple Business Managerでのコンテンツ購入についてさらに詳しく：
support.apple.com/ja-jp/guide/apple-business-manager

アプリケーションと本の配布についてさらに詳しく：
support.apple.com/ja-jp/guide/apple-business-manager

追加コンテンツを準備する

MDMソリューションは、Mac App Store以外のコンテンツで作成した追加パッケージを配布するのに役立ちます。これは、社内カスタムアプリケーションや、ChromeやFirefoxのようなアプリケーションなど、多くのエンタープライズソフトウェアパッケージを配布する場合に一般的な方法です。登録の完了後、必要なソフトウェアをこの方法でプッシュして、自動的にインストールできます。フォント、スクリプト、およびその他のアイテムもパッケージを使ってインストールや実行ができます。このようなパッケージは、Developer Enterprise ProgramのDeveloper IDを使って適切に署名してください。

追加コンテンツのインストールについてさらに詳しく：
support.apple.com/ja-jp/guide/deployment-reference-macos

3. 導入する

macOSは、IT部門の関与を必要とせずに社員にデバイスを導入し、必要に応じてパーソナライズして簡単に使い始めることができます。

設定アシスタントを利用する

社員は、起動時にmacOSの設定アシスタントユーティリティを使って、言語や地域を設定したりネットワークに接続したりすることができます。インターネットに接続すると、ユーザーに対して一連の設定アシスタントウインドウが表示され、これに従って新しいMacの基本的な設定手順を完了できます。Apple Business Managerに登録されたデバイスは、このプロセスでMDMに自動的に登録できます。デバイス登録されたMacシステムでは、利用規約、Apple IDのサインイン、位置情報サービスなど、特定の画面を省くように構成することもできます。

ユーザーがコンピュータに対して完全な管理者権限を持つかどうかの設定など、設定アシスタントによる様々な初期設定が行われた後、MDMが利用できるようになります。iPhoneやiPadの場合と同様に、ユーザーが自分のデバイスを管理できるようにしながら、MDMで管理する企業ポリシーと設定を遵守させることができます。設定アシスタントの完了後にユーザーがすぐ生産性を高められるようにするために、バックグラウンドでダウンロードとインストールを開始するのは最も重要なアプリケーションとパッケージのみとし、社員が仕事を始める妨げにならないようにします。大きなアプリケーションは、バックグラウンドでダウンロードとインストールを行うようにスケジュールするか、ユーザーがMDMソリューションのセルフサービスツールを使って後で行うようにします。

企業アカウントを構成する

MDMを使って、Eメールアカウントおよびその他のユーザーアカウントを自動的に設定できます。MDMソリューションおよび社内システムとの統合方法にもよりますが、ユーザー名、Eメールアドレス、認証と署名のための証明書IDもアカウントペイロードにあらかじめ入力しておくことができます。

ユーザーによるパーソナライズを可能にする

ユーザーが自分のデバイスをパーソナライズできるようにすると、生産性が高まります。これは、ユーザー自身が自分のタスクと目標達成のために最適なアプリケーションとコンテンツを選択できるようになるからです。また、macOS Catalinaでは管理対象Apple IDとUser Enrollmentを利用できるので、組織は、ユーザーが組織所有のApple IDを使ってAppleサービスにアクセスしたり、個人のApple IDと併用したりできるよう設定できます。

Apple IDと管理対象Apple ID

社員がApple IDを使ってAppleのサービス（FaceTime、iMessage、App Store、iCloudなど）にサインインすると、ビジネスタスクの合理化、生産性の向上、共同作業のサポートを実現する多彩なコンテンツにアクセスできます。管理対象Apple IDは、通常のApple IDと同じように個人デバイスのサインインに使用します。また、iCloudなどのAppleのサービスにアクセスしたり、iWorkやメモを使って共同制作したりするほか、Apple Business Managerにアクセスする場合にも使用します。通常のApple IDとは異なり、管理対象Apple IDは組織が所有および管理します。パスワードのリセットや役割ベースの管理も組織が行います。管理対象Apple IDでは、一部の設定が制限されています。

User Enrollmentで登録されたデバイスには管理対象Apple IDが必要です。User Enrollmentでは、オプションで個人のApple IDも併用できます。ほかの登録オプションでは、個人用または管理対象のいずれかのApple IDのみサポートされます。複数のApple IDをサポートしているのは、User Enrollmentのみです。

ユーザーがこれらのサービスを最大限活用するには、自分のApple ID、または自分用に作成された管理対象Apple IDを使用する必要があります。Apple IDを持っていないユーザーは、デバイスを受け取る前でもApple IDを作成することができます。ユーザーが個人のApple IDを持っていない場合は、設定アシスタントで作成できます。ユーザーがApple IDを作成するのに、クレジットカードは必要ありません。

管理対象Apple IDについてさらに詳しく：
support.apple.com/ja-jp/guide/deployment-reference-macos

iCloud

iCloudを利用すると、連絡先、カレンダー、写真など、書類や個人のコンテンツを自動的に同期して、複数のデバイス間で最新の状態に保つことができます。「探す」を使うと、ユーザーは、紛失や盗難に遭ったMac、iPhone、iPad、iPod touchの場所を特定できます。手動でデバイスを操作するか、MDMを使って設定を行うことで、制限を施すことができ、iCloudキーチェーンやiCloud Driveなど、iCloudの特定部分を無効にすることができます。これにより、組織はどのアカウントにどのデータが保存されるのかについて、より細かく制御できます。

iCloudの管理についてさらに詳しく：
support.apple.com/ja-jp/guide/deployment-reference-macos

4. 管理する

ユーザーがデバイスの使用を開始したら、様々な管理機能を利用してデバイスとコンテンツの長期的な管理と維持を行うことができます。

デバイスの管理

MDMソリューションを使うと、一連のタスクを通じて管理対象のデバイスを管理できます。これらのタスクには、デバイスへのクエリのほか、ポリシー違反のデバイスや紛失または盗難に遭ったデバイスに対応するための管理タスクの実行などがあります。

クエリ

MDMソリューションでは、デバイスに対して様々な情報を照会し、ユーザーがアプリケーションと設定の適切なセットを維持していることを確認できます。シリアル番号やデバイスモデルなどのハードウェア情報、macOSのバージョンやインストールされているアプリケーションのリストといったソフトウェア情報を照会できます。さらに、MDMは、FileVaultや内蔵ファイアウォールなどの主要なセキュリティ機能の状態も照会できます。

管理タスク

デバイスが管理対象である場合、MDMソリューションは様々な管理タスクを実行できます。これには、ユーザーの操作を必要としない自動での設定変更、macOSのアップデートの実行、リモートからのデバイスのロックまたはワイプ、パスワードの管理などが含まれます。

管理タスクについてさらに詳しく：
support.apple.com/ja-jp/guide/deployment-reference-macos

ソフトウェアアップデートの管理

最新のオペレーティングシステムが利用できるようになった場合、IT部門はユーザーに対し、最新バージョンにアップグレードする選択肢を提供できます。IT部門は、macOSのプレリリースバージョンをテストしてアプリケーション互換性の問題を早期に特定し、最終リリース前にデベロッパと問題に取り組むことができます。IT部門は、Apple Beta Software ProgramやAppleSeed for ITを通じて各リリースのテストに参加できます。ユーザーとデータを保護するには、Macコンピュータを最新の状態に維持するための包括的なアプローチが必要です。アップデートは頻繁に行い、会社のワークフロー全体でmacOSの新バージョンと互換性があることが確認でき次第、ただちにアップデートしてください。

MDMでは、デバイス登録済みのMacにmacOSアップデートを自動的にプッシュできます。重要なシステムの準備が整っていない場合、デバイス登録済みのMacは最大90日までアップデートおよびアップデートの通知を保留するように構成することもできます。ポリシーが削除されるかMDMがインストールコマンドを送信するまで、ユーザーが手動でアップデートを開始することはできません。

Appleは、macOSをアップグレードする際のモノリシックシステムイメージの作成を推奨もサポートもしていません。iPhoneやiPadのように、Macコンピュータのファームウェアアップデートは多くの場合モデルに依存します。同様に、Macのオペレーティングシステムをアップデートするには、これらのファームウェアアップデートをAppleから直接インストールする必要があります。macOSインストーラまたはMDMコマンドを使ってアップデートするのが最も信頼性の高い方法です。

追加ソフトウェアの管理

組織では、初期設定の後にも頻繁にユーザーに追加アプリケーションを配布する必要があります。重要なアプリケーションやアップデートについてはMDMで自動的に行うことができます。または、MDMソリューションによって提供されるセルフサービスポータルから社員がアプリケーションをリクエストできるようにしてオンデマンドで提供することもできます。このようなポータルでは、Apple Business ManagerでApp Storeから購入したソフトウェア、App Store以外のアプリケーション、スクリプト、その他のユーティリティなど、あらゆるものをインストールできます。

多くのソフトウェアは自動的にインストールできますが、特定のインストールではユーザーの操作が必要な場合があります。セキュリティを強化するために、Kernel Extensionを必要とするアプリケーションでは、ユーザーが読み込みに同意する必要があります。これはUser Approved Kernel Extension Loading（ユーザー承認型Kernel Extensionの読み込み）と呼ばれ、MDMで管理できます。

デバイスセキュリティの維持

デバイス導入前に確立するセキュリティポリシーの初期セットの運用以外にも、MDMソリューションを使って、コンピュータのコンプライアンス状態をモニタリングし、できるだけ多彩なレポートを取得できることが望まれます。これには例えば、各デバイスのセキュリティ態勢のモニタリングや、ソフトウェアパッチのインストールに関する情報収集が含まれます。ほとんどの組織はネイティブツールを使って各Macを暗号化し保護していますが、組織によっては、追加のファイル同期／共有サービス、またはデータロスを防止するツールを使って、企業データの漏洩を防止したり機密データに関する詳細なレポートを提供することが必須となっている場合があります。

Macが紛失や盗難に遭った場合は、iCloudの「Macを探す」機能で、すべてのデータを削除してMacを無効にするリモートワイプを開始できます。ITチームは、MDMを使ってリモートワイプを実行することもできます。

デバイスの再プロビジョニング

社員が離職した時は、インターネット復元とローカルの復元パーティションを使って別のユーザー向けにMacをプロビジョニングし直すことができます。これによって、Macのコンテンツがワイプされ、最新バージョンのオペレーティングシステムがインストールされます。Apple Business Managerで特定のMDMに割り当てられているMacは、設定アシスタントの実行中に自動的にMDMに再登録され、新しいユーザーの設定が構成され、企業ポリシーが適用され、適切なすべてのソフトウェアが導入されます。登録されていないMacコンピュータは、同じプロセスでワイプしてプロビジョニングし直した後、手動で再登録します。

サポートオプション

Macユーザーは IT部門のサポートをほとんど必要としないことに、多くの組織が気付いています。セルフサポートを促しサポートの質を向上させるために、多くのITチームがセルフサポートツールを開発しています。例としては、充実したMacサポートウェブページの作成、セルフヘルプフォーラムの提供、オンサイトでのヘルプデスクカウンターの開設などが挙げられます。MDMソリューションで、ユーザーがセルフサービスポータルからソフトウェアのインストールやアップデートなどのサポートタスクを実行できるようにすることもできます。

ベストプラクティスとして、企業はユーザーによるセルフサポートに全面的に依存すべきではありません。協力して問題解決に取り組むアプローチを取り、ユーザー自身が問題のトラブルシューティングを実行してからヘルプデスクに問い合わせるようにすることを重視します。プロセスにおいてユーザーも責任を共有し、サポートを依頼する前に自分で問題を調べてもらうようにします。

サポートの責任を共有することにより、社員のダウンタイムを短縮でき、サポートコストとサポート担当スタッフの全体的なフットプリントを削減できます。サポートの強化を必要とする組織には、社員とITのために社内サポート体制を補完する様々なプログラムとサービスをAppleCareが提供します。

AppleCare for Enterprise

完全なサポートを必要とする企業の場合、AppleCare for Enterpriseを利用すれば、社内ヘルプデスクの負担が軽くなります。社員を対象とした電話でのテクニカルサポートを24時間年中無休で提供し、優先度の高い問題には1時間以内に対応します。このプログラムは、MDMやActive Directoryなど、IT部門レベルの統合シナリオを提供します。

AppleCare OS Support

AppleCare OS Supportは、IT部門に対し、iOS、iPadOS、macOS、およびmacOS Server導入に関するエンタープライズレベルの電話サポートおよびEメールサポートを提供します。購入するサポートのレベルに応じて、最大24時間年中無休でサポートを提供し、お客様の組織を担当するテクニカルアカウントマネージャーを選任します。統合、移行、および高度なサーバ運用の問題について技術者に直接質問できるため、AppleCare OS SupportはITスタッフがデバイスを導入および管理し、問題を解決する効率を高めます。

AppleCare Help Desk Support

AppleCare Help Desk Supportでは、Appleの上級テクニカルサポートスタッフの電話サポートを優先的に受けることができます。さらに、Apple製ハードウェアの診断と問題解決のための各種ツールが提供されるため、大規模な組織でのリソース管理の効率アップやサポート応答時間の短縮、トレーニングコストの削減を図ることができます。AppleCare Help Desk Supportでは、ハードウェアやソフトウェアの診断とトラブルシューティング、iOSおよびiPadOSデバイスの問題の切り分けなどを、インシデント件数の制限なくサポートします。

MacのためのAppleCareとAppleCare+

すべてのMacコンピュータには、製品購入後1年間のハードウェア製品限定保証と90日間の無償電話テクニカルサポートが付いています。AppleCare+またはAppleCare Protection Planに加入すると、保証とサポートが購入日から3年間に延長されます。社員は、Appleのハードウェアまたはソフトウェアについて質問がある場合、Appleサポートに問い合わせることができます。Appleは、デバイスの修理が必要になった場合に、便利なサービスオプションも提供します。また、AppleCare+ for Macでは、過失や事故による損傷に対する修理などのサービスを所定のサービス料で利用することができます。

AppleCareのサポートオプションについてさらに詳しく：
apple.com/jp/support/professional/

まとめ

企業がMacコンピュータをユーザーグループまたは組織全体のどちらに導入する場合でも、導入と管理を簡単に行うためのオプションが多数用意されています。組織に最適な戦略を選択することで、社員の生産性が向上し、仕事を遂行するまったく新しい方法を手に入れることができます。

macOSの導入、管理、セキュリティ機能についてさらに詳しく：
support.apple.com/ja-jp/guide/deployment-reference-macos

IT向けモバイルデバイス管理設定についてさらに詳しく：
support.apple.com/ja-jp/guide/mdm

Apple Business Managerについてさらに詳しく：
support.apple.com/ja-jp/guide/apple-business-manager

ビジネス向けの管理対象Apple IDについてさらに詳しく：
apple.com/jp/business/site/docs/site/Overview_of_Managed_Apple_IDs_for_Business.pdf

Apple at Workについてさらに詳しく：
www.apple.com/jp/business/

IT部門向けの機能についてさらに詳しく：
www.apple.com/jp/business/it/

Appleプラットフォームのセキュリティについてさらに詳しく：
support.apple.com/ja-jp/guide/security/welcome/web

利用可能なAppleCareプログラムを探す：
www.apple.com/jp/support/professional/

Appleのトレーニングと認定資格を調べる（英語）：
training.apple.com

Apple Professional Serviceに問い合わせる：
consultingservices@apple.com