Mac導入の概要

はじめに

目次

MacとmacOSの組み合わせによって、社員はどこからでも最高の仕事ができるようになります。また、デバイス管理にかける時間が短くなるため、IT部門はビジネス戦略を構築したり、テクノロジーの修正やコスト削減以外のタスクに集中したりできるようになります。

この文書では、組織にmacOSデバイスを導入するためのガイダンスを提供します。また、組織の環境に最適な導入計画の基礎を構築できるようサポートします。

最新のmacOSアップデートを使った導入の新機能など、本書で取り上げるトピックについての詳細は、オンラインの「Appleプラットフォーム導入」ガイドを参照してください。

所有モデル

組織が使用するmacOSデバイスの所有モデルには、通常、次の2つがあります。

- 組織が所有
- ユーザーが所有

それぞれに独自のメリットがあるので、自分の組織に最適なモデルを選ぶことが重要です。ほとんどの組織には推奨モデルがありますが、組織の環境によっては複数のモデルを使用することも考えられます。

組織に最適なモデルを特定できたら、Appleが提供する導入と管理の機能についての詳細をチームで確認してください。

組織所有のデバイス

組織所有のモデルでは、組織がApple、またはプログラムに参加しているApple正規取扱店や通信事業者からデバイスを購入します。個々のユーザーにデバイスを提供する場合、これを「1人1台の導入」と言います。複数のユーザーが交代でデバイスを使うこともでき、この方法を「共有での導入」と言います。共有iPadは、複数のユーザーが情報を共有せずにiPadデバイスを共有できる所有モデルであり、「共有での導入」の一例です。組織全体で、「共有での導入」モデルと「1人1台の導入」モデルを組み合わせて使うことができます。

組織所有のモデルを使う場合、IT部門は監視モードや自動デバイス登録を使うことで、より高いレベルのコントロールを維持します。これにより、デバイスを箱から出した瞬間から、組織がデバイスを設定し管理することができます。

監視モードのデバイスの機能制限についてさらに詳しく：
support.apple.com/ja-jp/guide/deployment/welcome/web

Appleデバイスを監視モードにすると、IT部門はさらに多くのことを管理できます。

- アカウントを構成する
- グローバルプロキシを構成する
- アプリケーションをインストール、構成、削除する
- 複雑なパスコードを要求する
- すべての機能制限を適用する
- すべてのアプリケーションのインベントリにアクセスする
- 紛失モードにした上でデバイスの位置情報にアクセスする
- ソフトウェアアップデートを管理する
- システムアプリケーションを削除する
- 壁紙を変更する
- 単一のアプリケーションに固定する
- アクティベーションロックを省略する
- Wi-Fi使用を強制する
- デバイスを紛失モードにする

個人所有のデバイス

個人所有のモデルでは、ユーザーがデバイスの購入、設定、構成を行います。このタイプの導入は、一般的にBYOD（個人所有デバイスの持ち込み）と呼ばれます。macOSデバイスのBYOD導入はそれほど一般的ではありませんが、組織で使用できます。Wi-Fi、メール、カレンダーなど組織のサービスを使ったり、教育機関や企業ごとの要件に合わせてデバイスを構成したりするため、ユーザーは通常、組織のモバイルデバイス管理（MDM）ソリューションに自分のデバイスを登録します。これをユーザー登録と呼びます。

ユーザー登録では、ユーザーのプライバシー、個人データ、アプリケーションを尊重しながら、企業のリソースとデータを安全に管理できます。IT部門は、下の表に示されているように、特定機能の強制、アクセス、管理ができます。

ユーザーが自分のデバイスで企業データにアクセスするには、管理対象Apple IDを利用します。管理対象Apple IDはユーザー登録のプロファイルの一部となっていて、登録を完了するにはユーザーが認証に成功する必要があります。管理対象Apple IDは、すでにサインインに使っている個人用のApple IDと共に使用することができ、この2つが競合することはありません。これによってデバイス上でデータが分離されます。組織がiCloudストレージ容量を持っている場合、管理対象Apple IDで管理されるすべてのデータ用に、別のiCloud Driveが作成されます。

MDMソリューションのユーザー登録についてさらに詳しく：
support.apple.com/ja-jp/guide/deployment/welcome/web

個人のデバイスに適用されるMDMの機能は一部のみ。

- ✓ アカウントを構成する
- ✓ Per App VPNを設定する
- ✓ アプリケーションをインストールして構成する
- ✓ パスコードを要求する
- ✓ 特定の機能制限を強制する
- ✓ 仕事用アプリケーションのインベントリにアクセスする
- ✓ 仕事用データのみを削除する
- ✗ 個人用のアプリケーションを調べる
- ✗ 個人用アプリケーションのインベントリにアクセスする
- ✗ 個人のデータを削除する
- ✗ デバイスのログを収集する
- ✗ 個人用アプリケーションを会社の管理下に置く
- ✗ 複雑なパスコードを要求する
- ✗ デバイス全体をリモートで消去する
- ✗ デバイスの位置情報にアクセスする

導入の手順

このセクションでは、デバイスとコンテンツを導入するための4つの手順（統合と設定、導入計画とプロビジョニング、構成管理、コンテンツの配布）の概要を説明します。使用する手順は、デバイスの所有者が組織かユーザーかによって異なります。

これらの手順の詳細は、オンラインの「Appleプラットフォーム導入」ガイドを参照してください。

1. 統合と設定

組織に適した導入モデルを特定した後、導入の下準備を行うことが重要です。

MDMソリューション。AppleのmacOSのための管理フレームワークを利用すると、企業環境でのデバイスの安全な登録やワイヤレスでの構成とアップデート、ポリシーへの準拠のモニタリング、アプリケーションと本の導入、管理対象デバイスのリモートワイプやロックなどを行うことができます。これらの管理機能は、他社製のMDMソリューションを通じて提供されます。様々なサーバプラットフォーム用にいろいろなMDMソリューションが用意されています。提供される管理コンソール、機能、価格は、ソリューションごとに異なります。

Apple Business Manager。このウェブベースのポータルを使って、IT管理者はiPhone、iPad、iPod touch、Apple TV、およびMacの導入をすべて1か所で行うことができます。Apple Business ManagerはMDMソリューションとシームレスに連係するので、デバイス導入の自動化、アプリケーションの購入とコンテンツの配布、社員用の管理対象Apple IDの作成が簡単になります。

管理対象Apple ID。ユーザーはApple IDを使ってFaceTime、iMessage、App Store、iCloudといったAppleのサービスにサインインし、幅広いコンテンツやサービスにアクセスして生産性を向上させたり共同作業を行ったりできます。ほかのApple IDと同じように管理対象Apple IDは個人用デバイスへのサインインに使用するものであり、また、Appleデバイスの管理にも欠かせません。管理対象Apple IDでは個人用Apple IDと同じように、iCloud、iWorkおよびメモでの共同作業など、Appleの様々なサービスにアクセスできます。ただし、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。

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

Wi-Fiとネットワーク機能。Appleのデバイスは、安全性の高いワイヤレスネットワーク接続性を内蔵しています。複数のデバイスからユーザー全員が同時に、企業のWi-Fiネットワークに接続可能であることを確認してください。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、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に、ネットワークインフラが設定されていることも確認する必要があります。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対応のプリンタやApple TVのようなAirPlay対応のデバイスに接続します。また、アプリケーションおよびmacOSの内蔵機能の中には、共同作業や共有の際にBonjourを使ってほかのデバイスを検出するものもあります。

Wi-Fiおよびネットワークについてさらに詳しく：
support.apple.com/ja-jp/guide/deployment/welcome/web

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（英語）：
developer.apple.com/bonjour

VPN。お使いのVPNインフラを評価して、ユーザーがリモートで企業リソースに安全にアクセスできることを確認します。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。

メール、連絡先、カレンダー。iPhone、iPad、Macは、Microsoft ExchangeやOffice 365、Google Workspaceなどの一般的なEメールサービスと連係するので、暗号化されたSSL接続でプッシュメール、カレンダー、連絡先、タスクにも瞬時にアクセスできます。Microsoft Exchangeをご利用の場合は、ActiveSyncサービスが最新で、ネットワークのすべてのユーザーをサポートするよう構成されているか確認してください。クラウドベースのOffice 365を使用している場合は、接続が見込まれるmacOSデバイスの数をサポートできる十分なライセンスがあることを確認します。

ID管理。IDおよびその他のユーザーデータを管理するため、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以降の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。また、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をMDMソリューションで管理して、IDが自動的に信頼されるようにできます。

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

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

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、およびその他の生産性向上と共同作業のためのエンタープライズ向け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

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

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サーバからのコンテンツのローカルコピーを保存し、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

2. 導入計画とプロビジョニング

下準備ができたら、デバイスを構成し、コンテンツの配布準備を行います。どの所有モデルおよび導入モデルでも、MDMとApple Business Manager、またはMDMとApple Configurator 2を使うのが最適です。

自動デバイス登録

この登録方法を使うと、実際に各デバイスに触れて準備をしなくても、すばやく合理的に会社所有のAppleデバイスを導入してMDMに登録できます。IT部門は、設定アシスタントの手順を合理化してエンドユーザーの設定プロセスを簡素化でき、社員は、アクティベーションされるとすぐに適切な構成を確実に受け取れます。自動デバイス登録による導入ができるのは、Appleまたはプログラムに参加しているApple正規取扱店または通信事業者でデバイスを購入した場合のみです。ただし、自動デバイス登録に対応している通常のチャネル以外でMacコンピュータを購入したり、Macコンピュータを寄贈されたりすることもあります。このような場合は、Appleが新しく導入したApple Configurator for iPhoneアプリケーションを利用できます。Apple Configurator for iPhoneを使うと、macOS Monterey以降を搭載した対応するMacを組織のApple Business Managerアカウントに簡単に割り当てることができます。これによりIT部門は、自動デバイス登録で可能になる優れたデバイス管理機能を、すべて利用できるようになります。

Apple Configurator for iPhoneについてさらに詳しく：
support.apple.com/ja-jp/guide/apple-configurator/welcome/ios

デバイス登録

Apple Configurator 2と組織のMDMソリューションを使って、手動でデバイスを導入することもできます。会社所有デバイスとユーザー所有デバイスのどちらも、デバイス登録を使って導入できます。手動で管理されるデバイスは、その他の割り当てられたデバイスと同じように動作し、監視モードとMDM登録が必須です。この導入方法は、Appleやプログラムに参加しているApple正規取扱店または通信事業者以外で購入したデバイスをIT部門が管理する場合に最適です。

Apple Configurator 2についてさらに詳しく：
support.apple.com/ja-jp/apple-configurator

ユーザー登録

ユーザー所有のデバイスは、ユーザー登録を使って構成および導入できます。この方法を使うと、IT部門はデバイス全体の機能を停止することなく会社のデータを保護できます。ユーザー登録の詳細は、所有モデルのセクションを参照してください。

デバイスを組織が所有する場合でも、ユーザーが所有する場合でも、IT部門は設定アシスタントを通じて、デバイス配布時の設定の体験をコントロールできます。MDMソリューションによって設定アシスタントを構成することで、ユーザーはすぐにデバイスで作業を開始できるようになります。

デバイスの登録後、管理者はMDMポリシー、オプション、またはコマンドを開始できます。デバイスに対して実行できる管理アクションは、監視モードの有無や登録方法によって異なります。macOSデバイスはAppleプッシュ通知サービス（APNs）を通じて管理者のアクションに関する通知を受信し、安全な接続を使ってMDMサーバと直接通信できます。ネットワーク接続があれば、世界中のどんな場所にあるデバイスにもAPNsでコマンドを送信できます。ただし、APNsで機密情報や個人情報を送信することはできません。

3. 構成管理

Appleデバイスは安全な管理フレームワークを内蔵しているので、IT部門は幅広い管理機能を使ってデバイスを管理できます。この管理フレームワークは4つのセクションに分けることができます。

構成プロファイル

構成プロファイルは、Appleデバイスに設定および認証情報を読み込むペイロードで構成されています。構成プロファイルを使うと、設定、アカウント、機能制限、資格情報の構成を自動化できます。MDMソリューションプロバイダおよび社内システムとの統合方法にもよりますが、アカウントペイロードには、ユーザー名、Eメールアドレスに加え、該当する場合は認証と署名のための証明書IDをあらかじめ入力しておくことができます。

機能制限

機能制限を使うと、デバイス全体の機能を停止することなく、セキュリティポリシーを強制したりユーザーが集中できるようサポートしたりできます。機能制限には「すべてのコンテンツと設定を消去」などの機能が含まれます。「すべてのコンテンツと設定を消去」を使うと、Macをすばやく最新のOSバージョンにリセットし、このプロセス中にすべてのユーザーデータを暗号の仕組みによって削除できます。

管理タスク

デバイスが管理対象である場合、MDMサーバ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。また、ユーザーが監視モードのデバイスを手動でワイヤレスアップデートできないよう、最大90日間制限できます。監視モードのデバイスのソフトウェアアップデートを、MDMソリューションを使ってスケジュールすることもできます。

クエリ

MDMサーバはデバイスに対して各種情報を照会できます。シリアル番号、デバイスのUDID、Wi-FiのMACアドレスなどのハードウェアの詳細のほか、macOSのバージョン、デバイスにインストールされているすべてのアプリケーションのリストなど、ソフトウェアの詳細に関する情報を照会できます。MDMソリューションはこの情報を使って、インベントリ情報を最新の状態に保持したり、情報に基づいて管理上の意思決定を行ったりするほか、ユーザーが適切なアプリケーションを保持しているか確認するといった管理タスクを自動化することもできます。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。

管理対象のソフトウェアアップデート

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ときに、IT部門は、最新バージョンにアップグレードする選択肢をユーザーに提供できます。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がmacOSの新バージョンと互換性があることを確認したら、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が延期され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。

管理対象のその他のソフトウェア

組織が最初にユーザーに配布したアプリケーションに加えて、別のアプリケーションを配布しなければならないケースは多くあります。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。

4. コンテンツの配布

デバイスの登録後、管理者は管理配布の機能も使えるようになります。MDMまたはApple Configurator 2を使うと、Apple Business Managerのストアで購入したすべてのアプリケーションと本を、それらが利用可能なすべての国で管理できます。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サーバに接続されると、デバイスでApp Storeが無効になっていても、Apple Business Managerのアプリケーションと本を割り当てることができます。

ユーザーに配布できるコンテンツには、管理対象のアプリケーション、および管理対象の本と書類の2種類があります。管理対象のアプリケーションは、MDMサーバを使ってリモートで配布および削除できます。また、ユーザーが自分のデバイスをMDMから削除すると、管理対象のアプリケーションは削除されます。アプリケーションを削除すると、アプリケーションに関連付けられたデータも削除されます。管理対象の本と書類は、ユーザーのデバイスに自動的にプッシュでき、ほかの管理対象アプリケーションとだけ共有でき、管理対象アカウントを使ってのみメールで送信できます。管理対象の書類は自動的に削除できますが、管理対象の本は、Apple Business Managerで割り当てられたものであっても無効化や再割り当てができません。

コンテンツをユーザーに配布する方法には、以下の2つがあります。

アプリケーションをデバイスに割り当てる。MDMソリューションまたはApple Configurator 2を使って、デバイスに直接アプリケーションを割り当てることができます。この方法では、初期ロールアウトで一部の手順を省略することで、管理対象のデバイスおよびコンテンツを完全にコントロールしながら、導入を非常に簡単かつ迅速に進めることができます。アプリケーションがデバイスに割り当てられると、MDMを通じてデバイスにアプリケーションがプッシュされます。ユーザーを招待する必要はありません。そのデバイスを使用するユーザーは、誰でもアプリケーションにアクセスすることができます。

アプリケーションや本をユーザーに割り当てる。もう1つの方法では、MDMソリューションを使用して、Eメールやプッシュ通知のメッセージでユーザーにアプリケーションや本をダウンロードするよう招待します。ユーザーが招待を承諾するには、個人のApple IDを使ってデバイスにサインインします。Apple IDはApple Business Managerサービスに登録されますが、公開されることはなく、管理者にも表示されません。ユーザーが招待を承諾すると、MDMサーバに接続され、自分に割り当てられたアプリケーションと本を受け取ることができます。アプリケーションはユーザーのすべてのデバイスで自動的にダウンロード可能となるので、管理者が操作する必要はなく、コストも一切かかりません。

割り当てたアプリケーションをデバイスまたはユーザーが必要としなくなった場合は、割り当てを無効にして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るので、組織は購入したアプリケーションを完全に所有し、管理できます。ただし、本を配布した場合は受け取った人の所有物になるので、無効化して割り当て直すことはできません。

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。

デバイスのセキュリティ

Appleのデバイスは、設計時から安全性が考慮されています。デバイスを設定した後、内蔵のセキュリティ機能とMDM経由で利用できるその他の機能によって、企業のデータを管理および保護できます。IT部門は内蔵のセキュリティ機能とMDM経由で利用できるその他の機能によって、企業のデータを管理および保護できます。複数のアプリケーションに共通するフレームワークにより、構成と設定の継続的な管理が可能になります。

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/welcome/web

仕事のデータの保護。IT部門は、MDMを通じてセキュリティポリシーを適用したり、適用状況をモニタリングしたりできます。例えば、macOSデバイスでMDMからパスワードを要求するとデータ保護機能が自動的に有効になり、デバイスのファイルが暗号化されます。また、MDMでWi-FiやVPNを構成し、証明書を実装してセキュリティを強化することもできます。

MDMソリューションでは、コンテナを使用せずに詳細なレベルでデバイスを管理して、企業データを安全に保つことが可能です。内蔵セキュリティ機能により、IT部門はデータを暗号化したり、マルウェアからデバイスを保護したり、セキュリティ設定を適用したりできます。他社製のツールを使う必要はありません。

ロック、位置情報の特定、消去。デバイスを紛失しても、企業データは失われません。IT部門は、iOS、iPadOS、macOSデバイスをリモートでロックし、すべての機密データを消去することで企業の情報を保護できます。監視モードを設定したmacOSデバイスでは、IT部門が「探す」を有効にしてデバイスの位置情報を確認できます。また、IT部門が企業アプリケーションを管理するツールを利用して、個人データを残したままデバイスから企業アプリケーションを削除することもできます。

アプリケーション。共通フレームワークとコントロールされたエコシステムによって、Appleプラットフォーム上のアプリケーションは設計段階から安全性が確保されています。AppleはDeveloper Programを通じてすべてのデベロッパの身元を確認し、App Storeで公開する前にシステムによりアプリケーションを検証しています。また、署名、App Extension、エンタイトルメント、サンドボックス化といった機能をデベロッパに提供し、さらに高度なセキュリティを提供しています。

紛失モード。MDMソリューションでは、監視モードのデバイスをリモートから紛失モードにすることができます。この操作によってデバイスをロックし、ロック画面に電話番号を含むメッセージを表示できます。紛失モードでは、デバイスが最後にオンラインだった位置をMDMによってリモートで照会するので、紛失または盗難に遭った監視モードのデバイスの位置を特定できます。紛失モードにする際に「探す」を有効にする必要はありません。

アクティベーションロック。macOS Catalina以降では、監視モードのデバイスでユーザーが「探す」をオンにした場合、MDMを使ってアクティベーションロックを有効にできます。これにより、組織はアクティベーションロックの盗難防止機能を活用しながら、ユーザーがApple IDで認証ができない場合には、この盗難防止機能をバイパスすることができます。

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部門がセルフサポートツールを開発しています。例としては、信頼できる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。また、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、企業はユーザーのセルフサポートに任せるのではなく、協力して問題解決に取り組むアプローチを取る必要があります。ヘルプデスクに問い合わせる前にユーザーが自分で問題を調査したりトラブルシューティングを行ったりできるようにして、プロセスにおいてユーザーにも責任を共有してもらいます。

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

包括的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利用できます。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。

AppleCareおよびAppleCare+ for Mac

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+ for Mac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

まとめとリソース

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、まったく新しい方法で業務を推進することができます。

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/welcome/web

Apple Configuratorユーザガイド：
support.apple.com/ja-jp/guide/apple-configurator/welcome/ios

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：
apple.com/jp/business

IT部門向けの機能についてさらに詳しく：
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

利用可能なAppleCareプログラムを探す：
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 Servicesに問い合わせる（日本未展開）：
consultingservices@apple.com

ベータ版ソフトウェアのテスト、テストプランへのアクセス、フィードバックの提供：
appleseed.apple.com/sp/ja/welcome