デバイスおよび企業データの管理

目次

概要

データは、企業にとって最も重要な資産の1つです。ユーザーが企業データに個人用デバイスからアクセスする場合でも、会社が提供するデバイスからアクセスする場合でも、個人データと企業データを分離することは、外部からの攻撃とユーザーの過失の両方からデータを保護する優れた方法です。Appleは、ユーザーが最大限に作業を効率化し、IT部門が様々なレベルのデバイス管理を簡単にサポートできるようにしています。

会社所有のデバイスの場合、IT部門はApple Business Managerを使ってデバイス登録を自動化できます。実際にデバイスに触れたり1台ずつデバイスを準備したりしなくても、すばやく簡単にユーザーにデバイスを提供できます。IT部門は監視モードを設定することで、ほかの導入モデルにはない管理機能を活用できます。追加のセキュリティ構成、削除不可のMDM、ソフトウェアアップデートの管理などが可能になります。

ユーザー登録によって管理される個人所有デバイスの場合、企業データと個人データは、それぞれ管理対象Apple IDと個人用Apple IDで分離されます。これにより企業データは、個人データとは別に安全に保持されます。社員が組織を離れる時やアプリケーションへのアクセスが不要になった時、企業データは削除されます。

Appleデバイスの管理

Appleは、デバイスの使いやすさを損なうことなく、必要な管理を適切に行うためのツールをIT部門に提供しています。これは、Appleの管理フレームワークと、お使いのモバイルデバイス管理（MDM）ソリューションとの緊密な統合によって実現します。

デバイス管理に対するAppleのアプローチ

AppleはiOS、iPadOS、tvOS、macOSに管理フレームワークを組み込み、IT部門が設定の構成と更新、アプリケーションの導入、コンプライアンスのモニタリング、デバイスの照会とリモートワイプまたはロックを行えるようにしています。このフレームワークは、会社所有デバイスと社員所有デバイスのどちらにも対応し、デバイスの導入と管理の基礎となっています。このフレームワークはAppleのオペレーティングシステムに組み込まれているため、組織は単に機能を停止したり無効にしたりするのではなく、簡単な操作で必要な機能を管理できるようになります。IT部門は、ユーザー体験を低下させたりプライバシーを犠牲にすることなく、必要な管理ができます。

MDMとは

Apple製品とMDMソリューションを一緒に使うことで、IT部門は、デバイスの導入、アプリケーションとブックの配付、デバイスの設定、セキュリティの確保を簡単に行えるようになります。

MDMは、各デバイスでのアプリケーション、アカウント、およびデータの構成をサポートします。これには、パスワードやポリシーの適用など、統合された機能が含まれます。社員に対する管理の透明性は保たれ、個人情報はしっかりと保護されます。デバイスを紛失した場合でも、IT部門はリモートでセキュアにデータを消去できます。

お使いのサーバがクラウドベースでもオンプレミスでも、幅広いベンダーが提供する様々な機能や価格帯から柔軟にMDMソリューションを選ぶことができます。

ほかのデバイス管理ツールでは、MDM機能をエンタープライズモバイル管理（EMM）、統合エンドポイント管理（UEM）といった名前で呼ぶこともありますが、組織のデバイスと企業データをワイヤレスで管理するという目的には変わりありません。

MDMがユーザーに与える影響

Appleは、社員のプライバシーを侵害したり日常業務を妨げたりすることなく、IT部門がデバイスを導入および管理できるようにします。つまり、デバイスの所有者が組織でも社員でも、機能とデバイスが全面的に停止や無効になることはなく、データの利用と収集は制限されます。

これができるのは、Appleが会社用と個人用でアプリケーションとデータを分離しているからです。そして、多くの他社製MDMソリューションとの緊密な統合によって、IT部門はAppleデバイスとやりとりができますが、特定の情報や設定へのアクセスは制限されます。どの導入モデルでも、Eメール、メッセージ、ブラウザの履歴といった個人情報にMDMフレームワークからアクセスすることはできません。

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

デバイスの所有方法

デバイスの所有者は、組織または社員のいずれかです。会社所有のデバイスは、多くの場合1人1台配付されます。つまり、IT部門による管理機能が実装された専用デバイスが、各ユーザーに割り当てられます。ただし、会社所有のデバイスを複数の社員で共有することもできます。共有デバイスの配付例として、交代勤務の社員がシフト間でデバイスを共有する場合や、小売業の社員が1台のデバイスをハンドヘルド型POSとして使う場合などがあります。会社所有のデバイスは監視モードに設定して管理することができます。これにより、デバイス全体の機能を停止することなく構成および機能制限をさらに制御できます。

ユーザー所有のデバイスはBYOD（個人所有デバイスの持ち込み）とも呼ばれ、ユーザー登録で管理します。この管理方法により、社員は自分の個人用デバイスを仕事に使えるようになります。

どちらの場合も、Appleはプライバシー、セキュリティ、データ分離を尊重しながら様々なレベルの管理をサポートします。

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

会社所有のデバイス

IT部門は、会社所有のデバイスに対して、業務に必要なデータ、アプリケーション、設定のみを保持するように構成することができます。これらのデバイスは、MDMソリューションを通じて自動的に導入できます。AppleまたはApple正規取扱店から直接購入したデバイスは、Apple Business Managerに自動的に登録され、ゼロタッチで導入できます。IT部門が1台ずつ処理する必要はありません。

会社所有のデバイスを使用する場合、組織は、ユーザーのプライバシーと使いやすさを犠牲にすることなく高いレベルで管理することができます。会社所有のデバイスを登録することで、IT部門は、アカウントと機能制限の構成とインストールに加えて、Wi-Fi、VPN、メール、カレンダーを設定できます。ユーザーがデバイスに自分のアカウントを追加できないように制限することもできます。

ユーザーが会社所有のデバイスを使用する場合、管理対象Apple IDを使う、自分の個人用Apple IDを使う、Apple IDを使わない、という選択肢がありますが、管理対象Apple IDを使うことをおすすめします。管理対象Apple IDは会社固有のものであり、自分で作成できるApple IDとは異なります。個人用Apple IDと異なり、管理対象Apple IDがアクセスできるサービスはIT管理者が管理します。さらに監視モードを設定することで、IT部門はほかの導入モデルにはない管理機能を活用できます。追加のセキュリティ構成、削除不可のMDM、ソフトウェアアップデートの管理などが可能になります。

会社所有のデバイスを社員一人ひとりに提供する場合でも、多くのユーザー間で共有して共通のタスクに使う場合でも、デバイス上のすべてのデータのセキュリティを簡単に保護できます。

個人所有のデバイス

社員が自分のデバイスを仕事に使う場合、社員が保持する企業データはユーザー登録によって管理されます。ユーザー登録はBYODプログラムのための仕組みであり、社員は、自分のプライバシーを守りながら、企業データを安全で、分離され、保護された状態で保持することができます。以前はできなかったデバイスのパーソナライズも可能になりました。IT部門にできるのは、特定の設定のみを適用すること、会社のコンプライアンスが守られているかモニタリングすること、会社のデータとアプリケーションのみを削除することです。IT部門は、デバイスをリモートワイプしたり、デバイスの位置情報にアクセスしたり、デバイス上の個人情報や個人用アプリケーションにアクセスしたりすることはできません。ユーザーはいつでもMDMプロファイルを削除できます。プロファイルを削除すると会社のアプリケーションとデータはすべて削除されます。また、会社所有デバイスの場合と比較して、ユーザーはアップデートやその他の構成について、より多くのことができます。

ユーザー登録では、組織のMDMソリューションに自分のデバイスを登録することをユーザーがオプトインする必要があります。これによってユーザーは、会社のリソースにアクセスしたり、様々な設定をしたり、構成プロファイルをインストールしたり、会社のアプリケーションをインストールしたりできるようになります。

ユーザー登録では、1台のデバイスで個人用のApple IDと管理対象Apple IDを併用できます。ユーザー個人のすべてのiCloudデータには、既存の個人用Apple IDが使用されます。組織から提供される管理対象Apple IDを使用する場合、組織のすべてのiCloudデータは会社の管理対象iCloud Driveやメモに保存されます。

iOS 15とiPadOS 15で、ユーザーは「設定」アプリケーションから直接、自分のデバイスを登録できるようになりました。「設定」で「一般」を選択し、「VPNとデバイス管理」を選択して、「勤務先または学校のアカウントでサインインしてください」をタップします。管理対象Apple IDのユーザー名とパスワードを入力すると、認証プロセスが開始されます。

この方法でデータを管理することにより、自分のデバイスに関するユーザーの自律性が高まります。また、メモとiCloud Driveアプリケーションを使って、個人データ用から分離され暗号で保護されたAPFS（Apple File System）ボリュームに企業データを保存することによって、企業データのセキュリティが向上します。このような仕組みにより、BYODプログラムでのセキュリティとプライバシー、ユーザー体験のバランスが、より優れたものになりました。また、ユーザーが自分の管理対象デバイスを変更する場合や組織を離れる場合は、デバイスの登録を解除するとすぐ、APFSボリュームのすべてのデータが破棄されます。

企業データを分離するためのツール

Appleは、どの所有モデルを採用する場合でも、デバイス上で企業データと個人データをシンプルに分離できるようにする様々なツールを用意しています。このセクションでは、管理対象のアプリケーション、ブック、設定、アカウントなどでデータを管理する方法を学びます。

管理対象アプリケーション

組織から割り当てられたアプリケーションを受け取るには、デバイスがMDMソリューションに登録されている必要があります。アプリケーションは、デバイスに割り当てられた後、MDMからデバイスに配信されます。監視モードで管理されている会社所有デバイスでは、アプリケーションはサイレントにインストールされます。ユーザーによる操作やApple IDは必要ありません。

デバイスの所有者が会社でもユーザーでも、IT部門またはユーザーがMDMからデバイスを登録解除すると、管理対象アプリケーションに保存されたデータは削除されます。また、IT部門は、管理対象アプリケーションのデータがFinder、iTunes、またはiCloudにバックアップされないようにすることができます。バックアップを禁止すると、MDMソリューションによって削除された管理対象アプリケーションをユーザーが後で再インストールしても、データは復元できません。

管理対象のブック

Apple Business Managerで購入したブックは、管理対象Apple IDまたは個人用Apple IDを使ってユーザーに割り当てることができます。ブックをユーザーに割り当てる場合、それらのブックにはアプリケーションと同じ国や地域のダウンロード制限が適用されます。

管理対象アプリケーションと同じように、MDMでは、管理対象のブックがバックアップされないようにすることができます。管理対象のブックは、管理対象アプリケーションと異なり、無効にしたり再割り当てしたりすることはできません。

管理対象の設定

MDMに登録されたユーザーは、どのアプリケーション、ブック、アカウントが管理されているか、どのような制限が課されているかを「設定」で簡単に見ることができます。MDMによってインストールされたすべてのエンタープライズ設定、アカウント、およびコンテンツは管理対象としてフラグが付きます。これには、Wi-FiやVPNの構成およびパスワードの要件が含まれます。すべての設定は、いつでも更新または削除できます。

機能制限

共有オプションへのアクセスや特定のアプリケーションのダウンロードを制限することは、IT部門が企業データを安全に保つための方法の1つです。Apple製品とMDMソリューションで監視モードを設定することにより、IT部門は会社所有のデバイスをより高いレベルで管理できます。監視モードでは、削除不可のMDMなど、ほかの導入モデルでは利用できない追加のデバイス管理機能が提供されます。IT部門はさらに、iPhoneのカメラを無効にする、iCloudを無効にする、Siriを無効にするなど、様々な機能制限を実装できます。

管理対象のアカウント

IT部門は、ユーザーがすばやくデバイスを使い始められるように、デバイス上の会社のメール、カレンダー、連絡先を管理することができます。アカウントを管理すると、ユーザーは自分の個人用のメール、カレンダー、連絡先を追加できなくなり、ユーザーによるパーソナライズはできなくなりますが、IT部門はより強力にデバイス上のデータを保護できるようになります。

管理対象のExtension

App Extensionにより、サードパーティのデベロッパは、ほかのアプリケーションや、オペレーションシステムに内蔵された主要システムに機能を提供し、アプリケーション間の新しいビジネスワークフローを実現できます。Extensionを管理すると、非管理対象のExtension機能は管理対象のExtensionとやりとりできなくなります。Extensionの例として、仕事効率化アプリケーションが様々なクラウドサービスから書類を開けるようにするドキュメントプロバイダExtension、ユーザーがほかのエンティティとコンテンツを共有するための便利な方法を提供するShare Extension、ユーザーがほかのアプリケーションのコンテキスト内でコンテンツを操作または表示できるようにするAction Extensionがあります。

iOSとiPadOS向けのManaged Open In

Managed Open Inは、以下の3つの機能を使って企業データを保護します。

- **管理対象出力先で非管理対象のソースからの書類を許可。**この機能制限を適用すると、ユーザーは個人のソースおよびアカウントからの書類を組織の管理対象出力先で開くことができなくなります。例えば、この機能制限を適用した場合、ユーザーは組織のPDFアプリケーションを使って任意のウェブサイトからPDFを開くことはできません。

- **非管理対象の出力先で管理対象ソースからの書類を許可。**この機能制限を適用すると、組織の管理対象ソースおよびアカウントからの書類をユーザーの個人出力先で開くことができなくなります。この機能制限を適用した場合、組織の管理対象メールアカウントにある機密メールの添付ファイルを、ユーザーの個人アプリケーションで開くことはできません。

- **管理対象のペーストボード。**iOS 15とiPadOS 15以降では、この機能制限を適用することで、管理対象と非管理対象の出力先の間でのコンテンツのペーストを制御できます。この機能制限を適用すると、コンテンツのペーストは、他社製アプリケーションまたはApple製アプリケーション（カレンダー、ファイル、メール、メモなど）の間のManaged Open Inの境界に従って行われます。この機能制限を適用した場合、アプリケーションでは、管理対象の境界を越えるコンテンツに対してペーストボードの項目をリクエストすることはできません。

これらの3つの機能は、最も基本的なレベルで管理対象デバイスを2つの環境に分離する上で役立ちます。1つは管理対象の企業アプリケーションとデータの環境、もう1つは非管理対象の個人用アプリケーションとデータの環境です。

Managed Open Inを使ってデータを分離することにより、ユーザー体験をより優れたものにすることができます。Appleは、デバイス全体の機能を停止するのではなく、ユーザーにとって使いやすくするアプローチを取っています。これにより、IT部門は従来の高圧的な方法を取ることなく、データソースと出力先を管理するために必要な可視性を確保できます。

iOSとiPadOSの管理対象ドメイン

IT部門は、iPhoneおよびiPadで特定のURLおよびサブドメインを管理できます。例えば、ユーザーが管理対象のドメインからPDFをダウンロードした場合、そのPDFは管理対象の書類のすべての設定に準拠していることが求められます。ドメインに続くパスはデフォルトで管理対象です。

デバイスの紛失または盗難

残念ながら、デバイスは紛失や盗難に遭うことがあります。Apple製品とMDMソリューションを導入していれば、デバイスを失くしても誰かが企業データに自由にアクセスすることはありません。MDMソリューションでは、データ保護を設定し、パスコードを使って自動的に有効にすることができます。さらに、管理対象の設定では、ユーザーが見破られにくいパスコードをすべての管理対象デバイスで確実に使えるようにすることができます。

IT部門は簡単に、失くしたmacOSデバイスをリモートでロックしたり、失くしたiOSデバイスやiPadOSデバイスを紛失モードにしたりできます。どちらの場合も、正しいパスワードまたはパスコードが入力されるまでデバイスはロックされたままです。デバイスの場所を特定できない場合、MDMソリューションはデバイスに対してリモートロックおよびリモートワイプを行うことができます。このようにすることで、ほかの誰かが会社の機密データにアクセスすることはできなくなります。

ID管理

Appleデバイスの導入規模にかかわらず、デバイス、ウェブサイト、アプリケーション、サービスのユーザー認証を行う方法の中心となるのがIDです。IDはすべてのオペレーティングシステムに密接に統合されています。これにより、気付かないくらいのシームレスな体験をユーザーに提供します。また、ユーザーがどこで仕事をする場合でも、IT部門は必要な可視性と管理機能を確保できます。強力なID管理方法により、IT部門はデータ漏洩を発生前に防ぎ、万が一漏洩した場合のフォローアップのための明確なパスを用意できます。Appleは、この体験を実現するために様々なツールとテクノロジーを開発しています。そのいくつかについて、以下で説明します。

デバイス認証

AppleデバイスのID管理は、ロック画面またはログインウインドウでのデバイス認証から始まり、これはデバイス全体にわたり有効です。共有iPadまたは共有Macのどちらを使用する場合でも、社員は自分のアカウントを選択して自分の資格情報を入力することで、パーソナライズされた体験を得ることができます。IT部門はデバイス認証を通じて、誰がどのファイルにアクセスし、それを誰と共有したかなど、コマンドのデータチェーンを明確に把握できます。共有iPadでのデバイス認証は、管理対象Apple IDによって可能になります。共有Macでは、ローカルアカウントまたはネットワークアカウントを利用できます。

シングルサインオンExtension

シングルサインオン（SSO）ExtensionはMDMソリューションを通じて構成され、これによってネイティブアプリケーションとWebKitは、よりシームレスなサインオン体験を提供できます。これは、ユーザーが個別のログインおよびパスワードを作成しなくても、既存の資格情報を活用してアプリケーションにセキュアにアクセスできることを意味します。macOS Big SurとiPadOS 14以降では、IT部門は、macOSと共有iPadを使用するiPadOSの両方でSSO Extensionを構成できます。macOSでは、KerberosシングルサインオンExtensionなどの追加ツールを使えば、従来のバインド設定やモバイルアカウントがなくてもActive Directoryのポリシーと機能に統合することができます。また、社内外の認証局（CA）から発行された証明書をMDMソリューションで管理することにより、クライアント証明書を、安全かつ管理面で信頼できるサービスの透過的な認証に使用することができます。

管理対象Apple ID

IT部門は管理対象Apple IDを使用して、Apple Business Managerで組織のデバイスとアプリケーションの購入を管理します。管理対象Apple IDを、シンプルかつセキュアなID管理アーキテクチャであるFederated Authenticationに利用することもできます。管理対象Apple IDを使ったFederated Authenticationにより、Apple Business Managerに登録された組織を既存のIDシステムに接続できるようになります。これによってAppleサービスへのユーザーアクセスが自動的に設定されるので、サインインのための新しい資格情報は必要ありません。ユーザーがはじめてFederated Authenticationを使ってAppleデバイスにサインインする時、Appleのサービスにアクセスするために必要な管理対象Apple IDが自動的に作成されます。Federated Authenticationは、IT部門とエンドユーザーのアカウント関連業務を削減します。また、組織内で使用されるすべてのアプリケーションとサービスに対し、ID管理ポリシーを確実に適用できるようになります。

まとめ

社員とともに移動する企業データを確実に保護することは、非常に重要です。Appleの管理フレームワークとお使いのMDMソリューションは、ユーザーがどこにいても優れた仕事ができるようサポートします。

デバイスを管理し、データ分離フレームワークを構築する際は、次の重要なポイントを念頭に置いてください。

- 会社所有のデバイスの仕組みは、企業データを最大限に管理し保護します。
- ユーザー登録を通じて管理されるユーザー所有デバイスは、個人データにアクセスすることなく、企業データを保護された状態で保持するため、ユーザーのプライバシーも守られます。
- ユーザーのプライバシーとセキュリティは、企業データの保護と同じように重要です。
- デバイスとデータの管理は共通の取り組みであり、優れたIT部門は使いやすいアプローチを採用しています。

その他のリソース

Appleデバイスの導入についてさらに詳しく：
support.apple.com/ja-jp/guide/deployment/welcome/web

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