iOSおよびiPadOS
導入の概要

概要

目次

iPhoneとiOS、およびiPadとiPadOSの組み合わせを使うことで、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ニーズ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iOSおよびiPadOS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iOSおよびiPadOS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iOSおよびiPadOS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。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。MDMにデバイスを登録するには、ユーザー登録と呼ばれるAppleの機能を使います。

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5つの手順（統合と設定、ID管理、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iOSおよびiPadOS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。個人用Apple IDと同じように、管理対象Apple IDはAppleのデバイスやサービス（FaceTime、iMessage、App Store、iCloud、iWork、メモなど）へのサインインに使用され、ユーザーは幅広いコンテンツや機能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。ただし、管理対象Apple IDは組織が所有するものであり、Appleデバイスの管理に欠かせません。管理対象Apple IDにより、組織はパスワードのリセットや役割ベースの管理などを管理できます。また、管理対象Apple IDでは一部の制限が設定されています。

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機能を内蔵しています。企業のWi-Fiネットワークが、すべてのユーザーによる複数デバイスでの同時接続に対応していることを確認してください。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によって、デバイスがネットワーク上のサービスを自動的に検出できるようになります。iOSおよびiPadOSデバイスは、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

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iOSおよびiPadOSデバイスから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。必要な場合にのみVPN接続を開始できるように、iOSおよびiPadOSのVPNオンデマンドまたはPer App VPNの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確認し、適切なユーザー数と接続数をカバーす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iOSおよびiPadOS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。iOSおよびiPadOSは、OAuth 2.0と多要素認証を利用するOffice 365の先進認証にも対応しています。Exchangeを使用していない場合でも、iOSおよびiPadOS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。

2. ID管理

環境の準備に加えて、IT部門は導入の下準備として、認証や承認を管理する方法を選ぶ必要があります。これは、デバイスとデータのセキュリティを確保するのに役立ちます。

認証。認証には様々な方法があります。シングルサインオンと、管理対象Apple ID、iCloud、iMessageなどのAppleのサービスを使うと、組織のデータを損なうことなく、ユーザーが安全に連絡を取り合ったり、オンラインで書類を作成したり、個人データをバックアップしたりできます。各サービスは独自のセキュリティアーキテクチャを使用し、それによってデータ（Appleデバイス上にあるデータとワイヤレスネットワークで送受信されるデータの両方）を安全に取り扱い、ユーザーの個人情報を保護し、情報やサービスへの悪意のあるアクセスまたは不正アクセスなどの脅威から保護します。MDMソリューションを使用して、Appleデバイス上の特定サービスへのアクセスを制限したり管理したりできます。

シングルサインオンについてさらに詳しく：
support.apple.com/ja-jp/guide/deployment/depfdbf18f55/1/web/1.0

Kerberosシングルサインオンについてさらに詳しく：
support.apple.com/ja-jp/guide/deployment/depe6a1cda64/1/web/1.0

承認。承認は、認証とは異なります。認証は本人確認を行うものであり、一方、承認は何を行うことが許可されるかを定義します。例えば、IDプロバイダにユーザー名とパスワードを提供することによって実現できます。この例で、認証局はIDプロバイダまたはActive Directory、アサーションはユーザー名とパスワードであり、トークンは、サインインに成功した後に受け取るデータです。ほかに、証明書、スマートカード、その他の多要素デバイスなどをアサーションとして使用できます。

IDの連携。IDを連携するには、ユーザーの特定方法に関して双方が信頼し合意できるように、管理者がドメインを設定する必要があります。一般的な例として、エンタープライズアカウントを使ってクラウドIDプロバイダにサインインするケースがあります。IT部門は、Microsoft Azure Active Directory（Azure AD）とApple Business Managerの連携を有効にして、組織の管理対象Apple IDの作成を合理化するといったことができます。これにより、ユーザーは既存のAzure ADの資格情報を使って、Apple Business Managerに関連付けられたiCloudやAppleデバイスにサインインできます。

3. 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ソリューションとApple Business ManagerまたはApple Configurator 2を一緒に使うのが最適です。

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、デバイスが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。

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。iOSまたはiPadOS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。

4. 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。機能制限の例として、管理対象ソースからの添付ファイルや書類が管理対象外の出力先で開けないようにするManaged Open In、デバイスを1つのアプリケーションのみに制限するシングルAppモード、管理対象アプリケーションがiCloudやデバイスにデータをバックアップできないようにするバックアップ禁止などがあります。

管理タスク

デバイスが管理対象になっている場合、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、パスコードロックされたデバイスのソフトウェア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、ユーザーがパスワードを忘れた場合にリセットするためのパスコードロックの解除が含まれます。MDMサーバは、iPhoneまたはiPadに対し、特定の出力先へAirPlayミラーリングを開始するようリクエストしたり、現在のAirPlayセッションを停止したりできます。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、iOSまたはiPadOS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。

5. 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ソリューションまたは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。

デバイスのセキュリティ

Appleのデバイスには、最初から高度なセキュリティが組み込まれています。デバイスを設定した後、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、iOSとiPadOSデバイスでパスコ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。IT部門はManaged Open Inを利用して、添付ファイルや書類を管理対象外の出力先で開けないように制限できます。

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およびiPadOS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iOSおよびiPadOSデバイスでは、IT部門がデバイスを紛失モードにして位置情報を確認できます。また、IT部門は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。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

Appleは様々なプログラムやサポートリソースを提供しています。

AppleCare for Enterprise

包括的なサポートを必要とする企業は、AppleCare for Enterpriseを利用して社内ヘルプデスクの負担を軽減できます。AppleCare for Enterpriseは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、Appleのすべてのハードウェア製品およびソフトウェア製品に関するIT部門レベルのサポートを提供するほか、MDMやActive Directoryといった複雑な導入や統合のシナリオもサポートします。

AppleCare OS Support

AppleCare OS Supportは、IT部門に対し、iOSおよびiPadOSの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+ for iPhone、AppleCare+ for iPad、AppleCare+ for iPod touch

すべてのiOSおよびiPadOSデバイスには、製品購入後1年間のハードウェア製品限定保証と90日間の無償電話サポートが付いています。AppleCare+ for iPhone、AppleCare+ for iPad、AppleCare+ for iPod touchに加入すると、保証とサポートが購入日から2年間に延長されます。Appleのテクニカルサポートにお電話いただければ、専任スペシャリストが質問にお答えします。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。さらに、AppleCare+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最大2回まで所定のサービス料で利用することができます。

iOS Direct Service Program（日本未展開）

AppleCare+のメリットとして、iOS Direct Service Programをご利用いただくと、Appleサポートに電話したり、Apple Storeに来店することなく、社内ヘルプデスクでデバイスの問題のスクリーニングを行うことができます。必要であれば、組織からプログラムを通じてiPhone、iPad、iPod touchの交換品や付属のアクセサリを直接注文することができます。

AppleCareプログラム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iPhoneまたはiPad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。

iOSおよびiPadOS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 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