

企業のIT管理者が頭を抱える 「iPhone/iPad導入」の困り事

iPhoneやiPadを企業導入する際、IT管理者はさまざまな課題や問題に直面します。端末を正しく従業員に配付し、効果的かつ安全に使ってもらうにはどうしたらいいのか？ 管理の現場から多く問い合わせいただく質問に回答します。

FAQ:弊社によくお問い合わせいただく質問

Q1 ガラケーからiPhoneへ切り替えました。MDMとは何でしょうか？

Q2 MDMを活用できていません！ どのような機能があるのか知りたいです。

MDM(エムディーエム)は、Mobile Device Managementの略で、日本語では「モバイルデバイス管理」とも呼ばれます。これは本来Appleが提供する端末管理のための仕組みのことですが、一般的にはこの仕組みを利用した「Jamf Pro」や「Jamf Now」などのMDMソリューション／ツールのことを指します。MDM(は、企業で利用する端末をIT管理者がリモートで効率的に管理するために用いられます。具体的には、主に以下の4つのことが可能です。

①組織内の端末の情報を効率的に収集する

→OSのバージョンやインストールされているアプリなどの情報を収集し、企業の運用ルールに則って正しく使用されているかなどをチェックできます

②組織内で利用するアプリなどのリモート配信を行う

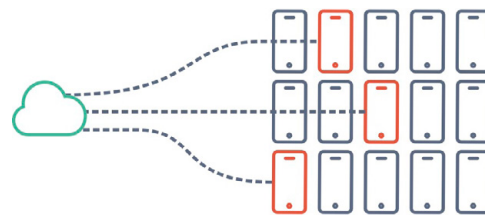
→iPhoneやiPadの場合、Appleの「App Store」や「ブック」で購入したアプリや電子書籍、または組織内のカスタムアプリを遠隔から配布できます

③組織内の運用ポリシーにあわせて端末の設定を一括で行う

→パスコードやWi-Fi、メール、セキュリティ、利用制限などを定義した構成プロファイルを作成し、ワイヤレスで端末に適用できます

④遠隔地からタスクを強制的に実行する

→端末の盗難や紛失時に、遠隔から端末内のデータを削除したり、端末にロックをかけたりできます

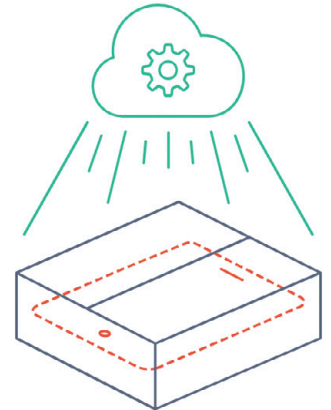


Q3 iPhoneやiPadを配備する際に必要な「キitting」とは何ですか？

企業にiPhoneやiPadなどを導入する場合は、端末に初期設定や必要なアプリのインストールなどを行い、エンドユーザが業務ですぐに使える状態にしておく必要があります。このセットアップ作業を「キitting」と言います。新規に端末を導入するときだけでなく、従業員の増加や端末の切り替え、故障端末の交換時にも発生し、導入端末が多かったり、役職や部署、支社ごとに異なる設定が必要だったりすると、IT管理者の大きな負担となります。

Q4 従業員の増加やガラケーからiPhoneへの切り替えなどで、IT管理者のキッキングの負担が増えています。キッキングを外注すると費用がかさんでしまいます…。

キッキングの負担を軽減するには、Appleが提供する「自動登録」というプログラムと「自動登録」に対応したMDMを利用するのが一番です（「自動登録」は、以前「DEP」: Device Enrollment Programと呼ばれていました）。「自動登録」に対応したiPhoneやiPadであれば、IT管理者が端末に触れることなくMDMの管理下に置くことができ、事前にMDMにて作成した構成プロファイルをMDMからワイヤレスで流し込むことキッキングの工数を大幅に減らすことが可能です。iPhoneやiPadを初めて起動する際にはさまざまな初期設定が求められますが、「自動登録」を使った場合は、エンドユーザ側でこの設定を行う必要はなく、初めて端末が通電した瞬間にMDMサービスへと接続され、MDMで設定した構成プロファイルが反映されます。そのほか、「自動登録」を使えば、エンドユーザによるMDMの構成プロファイルの解除を防止できたり、「監視モード」と呼ばれる強力な端末の管理設定をMDMから適用できたりするなどのメリットもあります。



Q5 端末の紛失や盗難に遭った際の対策や、端末のセキュリティ保護ができていません…。

MDMを利用して端末を監視下に置くことで、端末の紛失時/盗難時に遠隔から端末内のデータを消去できる「リモートワイプ」、または端末を一切操作できないようにする「リモートロック」が可能です。また、MDMからコマンドを送信することで、端末の画面に「拾った方はこちらへご連絡ください!」などのメッセージを送付したり、端末の現在位置の特定したりすることも可能です。



Q6 従業員にアプリをインストールしないよう注意喚起しているが、守られていません。

Q7 セキュリティリスクを回避するため、社用端末での従業員によるアプリの購入を禁止したい!

Q8 端末が増えるたびにApple IDの数も増え、管理するのが大変です。

「自動登録」を利用していれば、MDMを使ってApp Storeからのアプリの購入（インストール）やアップデートを無効し、App Storeのアイコンをホーム画面から削除できます。また、Appleが提供する「法人一括購入プログラム」（以前は「VPP」: Volume Purchase Program）を使えば、IT管理者がアプリをまとめて購入し、MDM経由で従業員に配付することが可能です。購入時にIT管理者用のApple IDを準備するだけでいいので、従業員のApple IDを発行する必要はありません。また、アプリのライセンスはMDMから確認できるので、台帳管理の手間から解放されます。「法人一括購入プログラム」の機能は、企業の場合はApple Business Managerに登録することで利用できます。

| 組織 | 合計22件 |
|-----------|-------|
| アクティビティ | |
| 場所 | |
| ユーザ | |
| アカラント | |
| 役割 | |
| デバイス | |
| MDMサーバ | |
| デバイスの割り当て | |
| 割り当て履歴 | |
| コンテンツ | |
| Appとブック | |

| アプリ | 利用可能数 |
|--------------|------------------|
| Evernote | 30個利用可能 |
| Google | 100個利用可能 |
| Google Earth | 120個利用可能 |
| Netflix | 2個を使用中 8個利用可能 |
| iMovie | 10個利用可能 |

Google

Google LLC · iOS App
✓ デバイス割り当て可能
[詳細を表示](#)

ライセンスを購入

割当先: 虎ノ門

価格 数量 お支払い方法

Q9 Apple Business Managerはどんなプログラムですか？登録は必要でしょうか？

Appleが無償で提供している企業のIT管理者向けWEBポータルです。iPhoneやiPadをはじめとするApple製品の端末管理や、業務用アプリやブックの購入・管理、企業から提供する業務用Apple ID(管理対象Apple ID)の作成・管理、組織内のメンバー(従業員等)のアカウント情報の作成・管理などを行うことができます。また、Apple Business Manager(以下、ABM)に対応するMDMと連携して「自動登録」を使った端末導入の自動化および管理、「法人一括購入プログラム」を使ったアプリやブックの配付などを行うことができます。

iPhoneやiPadをはじめとするApple製品はMDMソリューションだけでも管理することができますが、「自動登録」や

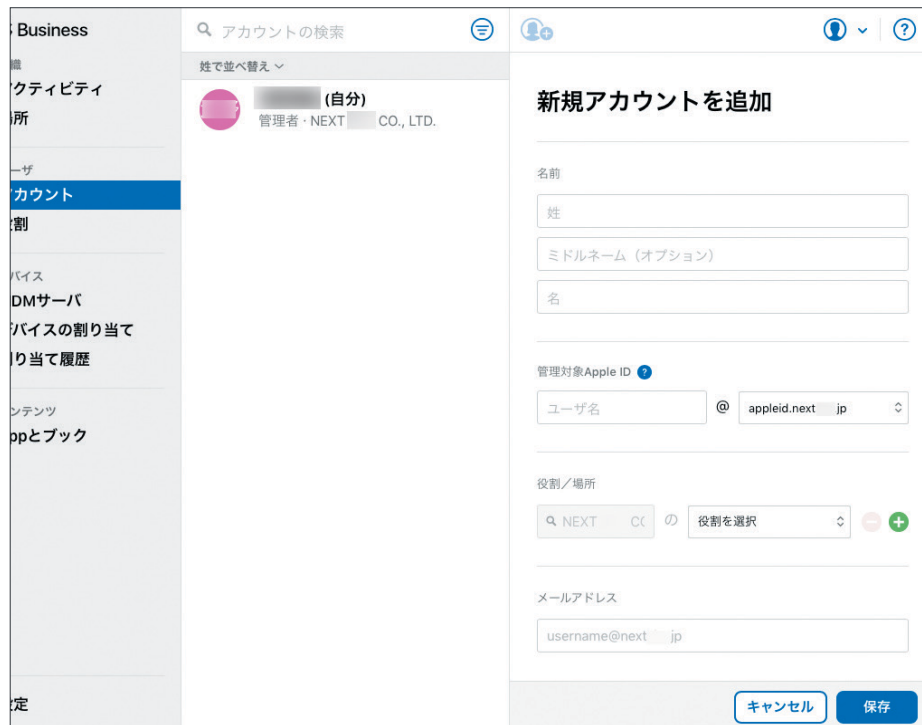
「法人一括購入プログラム」を利用するにはABMへの登録が前提となります。導入の主な流れは、まずABMに新規登録し、その後「自動登録」に対応した端末をABMへ登録、その後MDMをABMへ登録し、「自動登録」端末とMDMをABM上で紐付けます。このようにすることで、たとえばABM上で購入したアプリやブックを、MDMの管理化にある「自動登録」端末へ配付することができます(ABMはアプリの配付機能は持っていません)。また、ABM上の「自動登録」端末の情報はMDMと連携されますので、MDMを通して端末の管理を行うことができます。ABMには複数のMDMを登録でき、端末に応じて紐付けるMDMを選択することも可能です。

なお、AMBを利用するには、初めにABM上で企業情報を登録して、Appleの承認を得る必要があります。



Q10 Apple Business Managerで利用可能な「管理対象Apple ID」とは何ですか？

App Storeでアプリを購入したり、iCloudを利用したり、iWorkアプリでコラボレーションをしたりする際には、Apple IDを利用しますが、この通常のApple IDの機能を一部制限したものが「管理対象Apple ID」です。たとえば、管理対象Apple IDではApp Storeでのアプリの購入、Apple PayやiPhoneを探す機能、iCloudメールなどを利用することができません。管理対象Apple IDは端末へのサインインやiCloudの利用などAppleのサービスを便利に利用できる一方で、組織を守るためにあらかじめ「できないこと」が制限されているのです。管理対象Apple IDはIT管理者が一括で作成できるため管理が容易なこと、また付与した管理対象Apple IDに対して役割や権限を設定できることもメリットです。管理対象Apple IDは会社に固有のIDとなり、従業員が各自のApple IDとは区別されます。



Q11 業務に利用するアプリが新OSに対応していません。OSのアップデートを制御できますか？

Q12 セキュリティリスクを回避するため、最新のOSへ強制的にアップデートしたいです。

「自動登録」を利用していれば、MDMを使ってOSのアップデートを最大90日間遅延させることが可能です。また、最新OSへアップデートする場合はMDMからコマンドを送って強制アップデートを行えます。



Q13 業務で利用するアプリを個人のApple IDではなく、会社の資産として購入するには？

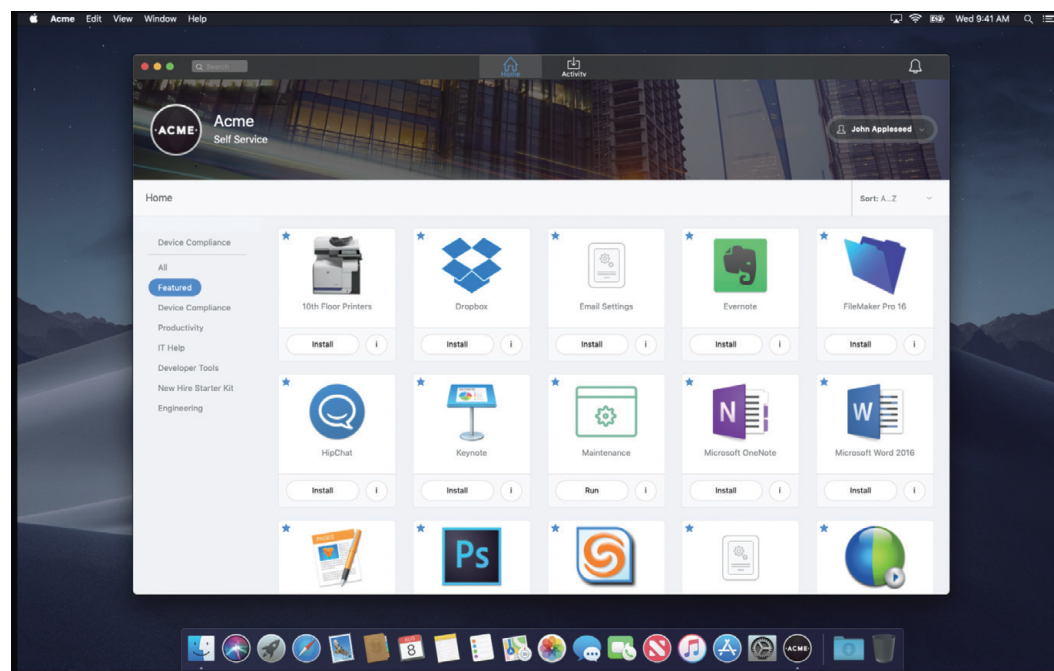
App Storeでは、アプリの購入をクレジットカードまたはiTunesカードで決済することが可能です。法人名義のクレジットカードや使い切りタイプのクレジットカードがあれば決済可能ですが、iTunesカードの場合はアプリ購入後の残額をほかのユーザに移行できないので、余ったお金が問題となります。さらに、ユーザに購入してもらったアプリはユーザのApple IDに紐付いてしまい、再利用できなくなります。そうした問題を解決するのが、「法人一括購入プログラム」です。以前、VPPとも呼ばれていたこの仕組みを活用すれば、IT管理者はアプリのライセンスを一括購入して各端末に割り振ることができ、購入と運用の手間を大幅に減らすことができます。購入したアプリは配布したデバイスに紐付けられるため、アプリの回収・再配付が可能。MDMと関係させることで一括で配付することができます。

Q14 App Storeからのアプリのインストールを禁止すると、従業員から強い反発がありそうです。

「自動登録」を利用していれば、従業員が勝手にApp Storeからアプリを端末にインストールすることを禁止できますが、逆に「禁止しない」こともできます。そのため、業務で利用するアプリはApple Business Managerから「法人一括購入プログラム」を使ってIT管理者が配付し、個別に必要なアプリは従業員個人のApple IDを使ってインストールさせるなどの柔軟な運用が可能です。

また、どうしても従業員個人のApple IDを利用させたくない場合は、業務で最低限利用するアプリ以外の「許可済みアプリ」を「Self Service」(企業専用のApp Store)に掲載し、そこから従業員にダウンロードしてもらうことも可能です。

すべてのアプリを自由にインストールできるわけではないものの、従業員の満足度を高めることにつながるほか、IT管理者にとってはSelf Serviceにアプリをアップロードしておくだけなので手間がかからず、ダウンロードには管理対象Apple IDを利用するので管理の面でも安心できます。



Q15 「法人一括購入プログラム」で社員にアプリを配付したところ、従業員個人で購入したアプリとの間で、データのコピーが行えません。

「法」 法人一括購入プログラムを使って購入し、MDM経由で配付したApp Storeの無料／有料アプリやカスタム社内アプリは、「管理対象アプリケーション」と呼ばれます。業務で利用するアプリには機密情報を含むことが多いため、MDMを利用して管理対象アプリケーションとそれに関連付けられたデータを細かく制御できます。たとえば、「Managed Open In」によって制御を行うと、管理対象アプリケーションとそれに関連付けられたデータを「管理対象ではないアプリ」（個人で購入したアプリなど）で開けないようにできます。また、逆に「管理対象でないアプリ」およびそれに関連付けられたデータも、管理対象アプリケーションでは開くことができません。また、「Managed Extension」を制御することで、両者間でデータのコピー＆ペーストもできないようになります。

そのほか、MDMを利用して管理対象アプリケーションとそれに関連付けられたデータをオンデマンドで削除したり、MDMプロファイルが削除されたときにアプリを削除するかどうか指示したり、アプリのデータをiTunesやiCloudにバックアップされないようにしたり、承認されていないキーボードを使って利用できないようにすることができます。

Q16 MDMからアプリを配信する際に途中で失敗してしまい、どの端末まで配付したか確認するのが面倒です。

「法」 法人一括購入プログラムで購入したアプリをMDMを使ってiPhoneやiPadに配付するとき、MDMによってはネットワークの問題などで、アプリとライセンスが正しく送信されない場合があります。こうしたトラブルが生じたとき、アプリとライセンスを「別々に」配付するMDMの場合は、どの端末までアプリとライセンスの配付が完了したかを「別々に」確認しなくてはならず、とても面倒です。

一方、Jamf Proは「法人一括購入プログラム」で購入したアプリとライセンスを「同時に」配付するため、こうした問題が起きたときでもJamf Pro上で未配信の端末を素早く割り出すことができます（実機を確認することなく、リモートで効率的に作業できます）。多数のiPhone／iPadをリモートで管理するために、確実性を重視しているJamf Proならではの特徴です。

もし、何らかの原因でJamf Proからアプリを配付できない場合は、アプリ配信コマンドを何度か送ってみてください。一度や二度失敗したあとに、成功する場合があります。また、もし一部の端末がネットワークの障害や遅延などでアプリの配付に失敗していた場合は、Jamf Pro上で対象デバイスを割り出して再配付することが可能です。また、Jamf Proと「法人一括購入プログラム」を併用している場合は、アプリの配付とライセンスの管理が連動して行われるため、ライセンス数も自動的に管理できるのが特徴です。

The screenshot shows the Jamf Pro web interface for configuring a mobile device app distribution. The main content area is titled "モバイルデバイス : モバイルデバイス App" and "Swift Playgrounds". It features a navigation menu on the left with options like "インベントリ", "コンテンツ管理", and "グループ". The main area has tabs for "一般", "Scope", "Self Service", "Managed Distribution", and "App の構成". Under "Scope", there are sections for "Targets" and "Limitations". The "Targets" section includes "ターゲットモバイルデバイス" (Target Mobile Devices) and "ターゲットユーザ" (Target Users), both with dropdown menus set to "Specific Mobile Devices" and "Specific Users" respectively. Below this is a table of "選択された展開ターゲット" (Selected Deployment Targets) with columns for "ターゲット" (Target) and "タイプ" (Type), listing two mobile devices.

| ターゲット | タイプ | 操作 |
|------------|---------------|--------|
| [Redacted] | Mobile Device | Remove |
| [Redacted] | Mobile Device | Remove |

Q17 最新のiOSの新機能がMDMから制限できません。そのため、Apple Configurator 2を使って、MacにiPhoneを1台1台つないで設定するのは大変です。

Appleは、さまざまな新機能を搭載したiOSの最新バージョンを毎年秋に発表します。企業利用の観点からすると、これらの新機能にMDMが対応していない場合は端末の管理が難しくなるため、従業員へ配付した端末のアップデートを禁止するしかありません。ただし、セキュリティの観点からは、OSやアプリの脆弱性が少ない最新のOSの状態にしておくほうが望ましいとも言えます。また、新機能の中には利用を許可することで、従業員の生産性を高めるものもあるでしょう。つまり、AppleのOSのアップデートに即座に対応することはMDMにとって非常に重要であり、Jamf Proは2012年以降の9年間、最新iOSリリース同日に新機能等をサポートする「ゼロデイサポート」を実現しています。

Q18 iPhoneのホーム画面のレイアウトは変更できますか？

従業員へ配付するiPhoneやiPadには、業務で利用するアプリ以外を表示させないなど、企業のポリシーに従ってホーム画面のレイアウトを変更したいことがあるでしょう。Jamf Proを利用すれば、iPhoneやiPadのホーム画面やDockに表示されるアプリの変更や、ホーム画面のページの追加、各ページに表示されるアプリなどをカスタマイズ可能です。また、ホーム画面やロック画面の壁紙を企業のロゴなどに変更することも可能です。



Q19 MDMのユーザインターフェイス (UI) が頻繁に変わるため、使い慣れたメニューや機能などをその都度探すのに苦労しています。



Jamf Proの大きな特徴の1つに、使いやすいUIがあります。たとえば、iOSやAndroid、WindowsなどのマルチOSに対応したMDMの場合、UIが複雑になり、またUIが頻繁に変わるために目的の機能を探すのに大変時間がかかることがあります。一方、Jamf ProはApple製品に特化しているMDMであるため、UIが非常にシンプルであるのが特徴です。また、マルチOS対応MDMと比較した場合のJamf Proの大きな優位性は操作性にもあります。Jamf Proでは数ステップで実行可能だが操作が、マルチOS対応MDMだと目的の操作定項目までたどり着くのにさらにステップを踏む必要があります。

Q20 iPhoneをどのようなポリシーで運用したらいいのかわかりません。他社はどのように運用しているのでしょうか？

業務端末の運用ポリシーは企業ごとに異なります。そのため、弊社ではMDMの構築の段階から、企業としてどのように業務端末を利用したいかをヒアリングしたうえで、最適な提案をさせていただいております。