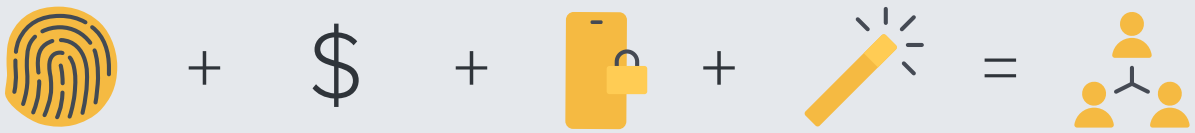
jamf

プライバシーとユーザエクスペリエンス に配慮したBYODプログラムをJamfで実現

プライバシーやユーザエクスペリエンスに配慮したモバイルデバイスの
セキュアな運用を通して、BYODプログラムを成功させましょう

生産性向上のもっとも優れたツールとしてiPhoneやiPadの人気が上昇したことにより、多くの人が場所や時間を問わず常にオンラインで業務を行うようになりました。そしてこれは、現代のIT管理に大きな課題をもたらしました。

優れたモバイルデバイス向けBYODソリューションに不可欠な要素



モバイルデバイスは今や誰もが所有するものであり、ほとんどの従業員が職場にそれを持ち込みます。しかし、個人所有のデバイスのポテンシャルを引き出そうとするここ数年の試みは、決して簡単なものではありませんでした。多くの場合、BYODソリューションはコンセプトとしては素晴らしいものの、その実用には大きな欠点がありました。「従業員がハードウェアを提供し、組織がアクセスを提供する」これは口で言うほど簡単ではなく、デバイスが過剰に管理されたり、従業員のニーズが十分に満たされなかったりすることが往々にしてあります。

フルスケールのデバイス管理のフレームワークは、時として配慮にかけることがあります。仕事だけでなくプライベートで使うデバイス上のすべてのアプリケーションがIT管理者に見えてしまうからです。また、IT管理者はデバイス自体をロック、解除、またはワイプする力も持っています。モバイルデバイスのユーザは自分のデバイスのコントロールを他人に委ねることを好みません。さらに、プライバシーが侵害されることはもちろん、侵害されていると「感じる」ことさえ嫌います。

BYODプログラムにおけるモバイルデバイス管理方法のもう1つの方法は、モバイルアプリケーション管理（MAM）です。これは、IT部門がデバイスにプロビジョニングされた特定のアプリケーションに企業ポリシーを適用するもので、デバイスではなくアプリケーションのセキュリティを担保します。しかし、MAMを導入しても、Wi-Fiやメールの構成やアプリ（一括購入されたものを含む）の自動インストールなどといった企業のIT部門が行う典型的なタスクを、ユーザの手を煩わせずに行うことはできません。このような基本的なサービスが不足している状態では、従業員は不満を感じ、IT部門はセキュリティの脆弱性を常に心配することになります。

結局のところ、BYODプログラムの成功（または失敗）は、デバイスの機能性、データセキュリティの維持、プライバシーの保護にかかっているのです。**このホワイトペーパーでは、これらの要素のバランスが取れたBYODソリューションをJamfとAppleで実現する方法について見ていきます。**

ユーザにとって重要なのはプライバシー

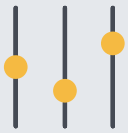
個人所有のデバイスには、メッセージや写真、連絡先、ドキュメントなど、もっともプライベートなデータが詰まっています。デバイスにどのようなアプリがインストールされているか見るだけでも、その人の趣味や習慣、ライフスタイルなどに関する非常にプライベートな情報がわかってしまいます。ディストピア小説に登場する「ビッグブラザー」のような得体の知れない何かに監視されることを人々は恐れています。会社のIT部門の支配下にあるモバイルデバイス管理（MDM）システムに個人情報が詰まったデバイスを登録することを多くの従業員が躊躇するのも当然です。

BYODプログラムが失敗する一般的な理由の1つに、ユーザがこの種の個人データへのアクセスをIT管理者に許すことを嫌がるという点があります。誰にとってもプライバシーは重要であり、IT管理の名のもとにプライバシーが侵害されることにユーザはこれまで以上に敏感になっています。

ITにとって重要なのはセキュリティ

IT管理者にとって、構成やセキュリティの状態が不明な個人のモバイルデバイスが社内リソースに自由にアクセスできるというのは、悪夢のような話です。**モバイルデバイスはマルウェアやフィッシング攻撃のターゲットになることが多く**、組織のネットワークへのアクセスを通じて攻撃者の侵入を許してしまう可能性はゼロではありません。

エンドポイント上の組織データに対する可視性やコントロールがなければ、効果的なセキュリティ対策を行うのはほぼ無理と言っていいでしょう。組織がBYODプログラムの運用にMDMを使用し、社内ネットワークやメール、カレンダー、VPNなどに代表される企業リソースにアクセスするために個人所有のデバイスの登録を要求するのも、まさにこれが理由です。



IT管理者ができること

- データ損失を防止するための対策の採用
- ユーザが自身で管理できるアプリカタログの提供（例：Self Service）
- Wi-Fi、VPN、パスコードなど企業に必要な構成の適用
- 組織向けAppやブック、および関連データのインストールと削除
- 業務アカウントからセキュリティ情報を収集
- 企業データを保護するための制限の追加と削除

IT管理者ができないこと

- 写真、メール、連絡先などの個人データの消去
- プライベートで使用するアプリの削除
- プライベートで使用するアプリの名前を含む個人データの閲覧
- デバイスの使用やプライベート用アプリのインストールに対する制限の設定
- デバイスの位置情報の取得
- ユーザがインストールしたアイテムの削除
- デバイスからユーザ情報を収集

バランスの取れたアプローチ

ユーザとITの懸念は、どちらも理解できるものばかりです。従業員にしてみれば、1台のデバイスですべてを済ませることができれば理想的ですが、かといってプライベートなデータへのアクセスやコントロールを手放すことはしたくありません。一方IT部門は、デバイスの購入にかかるコストを削減し、従業員のユーザエクスペリエンスを向上させたいと考えていますが、同時に基本的なセキュリティは守らなければなりません。多くの組織は、この2つのバランスに苦戦してBYODプログラムを成功させることができませんでした。

ユーザとITの両方の懸念に対処する方法のひとつは、BYODを採用する上でMDMの役割を見直すことです。画一的なアプローチではなく、BYODのために設計され、従業員を安心させるプライバシー保護と、ITおよび情報セキュリティチームのニーズを満たす強力なセキュリティ制御を備えたツールを選択するのです。

現代のワークフォースに最適なBYOD

最先端を行く組織は、無意味な複雑さや追加コストなしで両者のニーズを満たすために、BYODを念頭に置いて作られた一連の機能を採用しています。重要なのは、ITとエンドユーザの両方がBYODプログラムのメリットについて明確に理解できるよう、十分なコミュニケーションと透明性を提供することです。これはプログラムの成功に不可欠なだけでなく、個人所有のデバイスを職場で使用することに対する従業員の不安を緩和するのに役立ちます。以下は、優れた設計のBYODプログラムから組織やその従業員が得られるメリットの一例です。

すべての人がメリットを得られるプログラム

従業員にとってのメリット

公私を問わず1つのデバイスで素晴らしいAppleエクスペリエンスを得られます

- 個人所有デバイスに対するITの管理能力や個人データの保護について登録前に明確に説明
- メール、カレンダー、Wi-Fi、アプリなどの生産性維持に役立つ企業リソースへのセキュアなアクセスを提供

組織にとってのメリット

セキュリティとエンドユーザのプライバシーのバランスを1つのデバイスで実現できます

- 企業データやリソースへのアクセスやデバイスのセキュリティを確保し、従業員の保護と生産性を維持
- デバイスの購入台数が減ることによるコスト削減

「Jamf + Apple」でユーザのプライバシーを守る

前述したように、もっとも大切なのは絶妙なバランスを達成することです。そのためには、個人所有デバイスを過剰に管理することなく、業務に必要なソフトウェアやアプリへの簡単かつ安全なアクセスを提供し、組織とその従業員の両方にメリットを与えなければなりません。Jamfはこのことを理解した上で、Appleの機能を活用してBYODプログラムのメリットや可能性を増大させるためのソリューションを作りました。

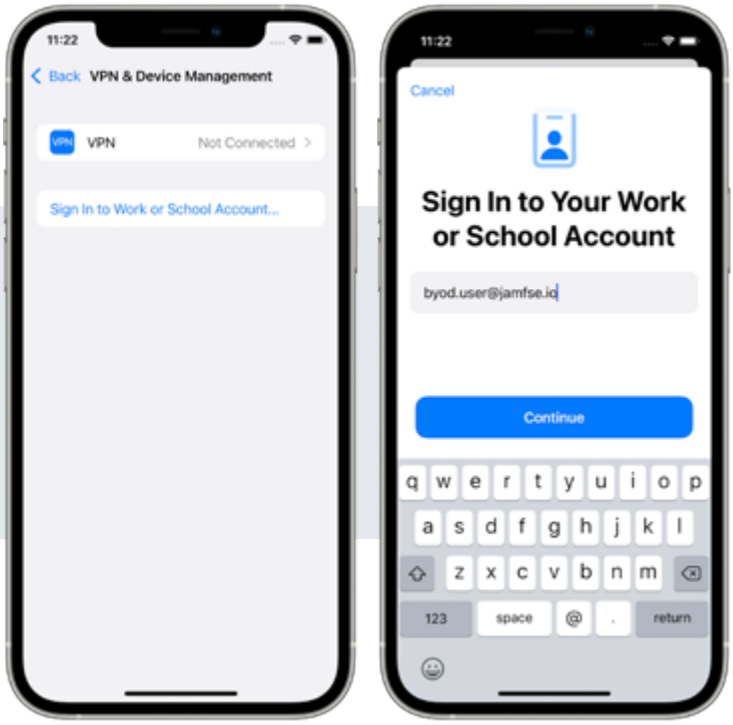
セキュリティとプライバシーに重点を置いたiOSおよびiPadOSデバイス向けのBYODソリューションであるAppleの**アカウントベースのユーザ登録**は、ユーザ登録のセットアッププロセスを効率化し、個人所有のデバイスを業務に使用するユーザのプライバシーに配慮しながら企業リソースへのアクセスを提供することにフォーカスしています。組織はこの新たなワークフローを利用して、iOS/iPadOS 15以降を搭載した個人所有のモバイルデバイスを、Jamf Pro（10.33以降）で登録することができます。JamfはApple独自の**ユーザ登録**ワークフローに対応しており、仕事用とプライベートのフォルダを分離することで従業員のプライバシーを保護します。個人所有デバイスの登録方法には「アカウントベースのユーザ登録」と「プロファイルベースのユーザ登録」の2種類があります。Jamfでは、従業員が設定Appから行うアカウントベースのユーザ登録を推奨しています。

ユーザ登録では、ユーザのApple IDを個人データに関連付け、管理対象Apple IDを組織のデータに関連付けることにより、プライベートのデータと業務用のデータを分離します。Appleのサービスディスカバリ機能を採用しているJamf Proでは、デバイスそのものではなく、ユーザやデバイスの使われ方を管理するための一連の構成を利用することができます。ITがデバイスに触れたり登録用のリンクを送ったりしなくても、従業員はセキュアな方法で企業データにアクセスできるため、フィッシング攻撃を受ける可能性も低くなります。さらに、JamfのSelf Serviceアプリを使用して企業アプリケーションを自分でインストールすることも可能です。このような登録プロセスは、従業員にとっては安心かつ信頼性のある体験となり、管理者にとってはゼロタッチ導入と同じく、組織リソースへのセキュアなアクセスを提供できるというメリットがあります。

従業員によるデバイス登録

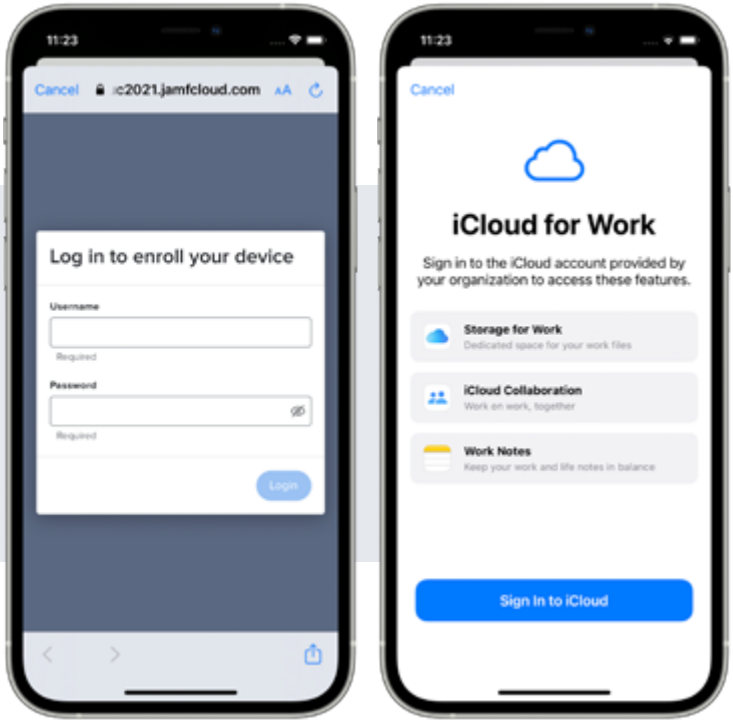
1

「設定」→「一般」→「VPNとデバイス管理」から管理対象Apple IDで職場や学校のアカウントにサインインし、デバイス認証を行います。管理対象Apple IDを入力したあと「続ける」をタップします。



2

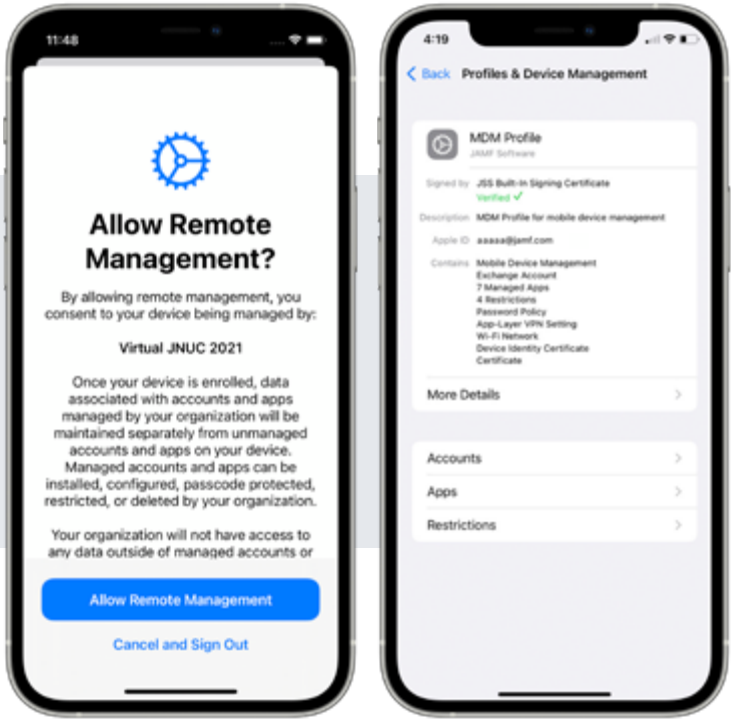
登録ポータルが表示されたら、Jamf Proのユーザアカウントまたはディレクトリ（LDAPやAzure ADなど）の認証情報を入力し、「ログイン」をタップします。次に、管理対象Apple IDのメールアドレスとパスワードを使用してiCloudにサインインします。



3

リモート管理を許可するためのプロンプトが表示され、MDMプロファイルがデバイスにダウンロードされます。

登録はこれで完了です。エンドユーザにとって非常にシンプルで、組織にとってはセキュアな体験です。



BYODのために設計されたアクセス&セキュリティソリューション

これにアクセスおよびセキュリティソリューションを加えたいと考える組織には、Jamf ConnectとJamf Protectをお勧めします。

ゼロトラストネットワークアクセス（ZTNA）機能が搭載されたJamf Connectでは、安全であることが確認されたデバイスを使用する信頼できるユーザのみに企業アプリやデータへのアクセスを許可することができます。また、Jamf Protectは、Appleの強力なセキュリティ機能をさらに強化して組織のデータをしっかりと保護してくれます。

Jamf ConnectとJamf Protectが機能するためには、そのアクセスおよびセキュリティ機能を従業員のモバイルデバイスに届けてくれるJamf Trustアプリを導入する必要があります。Jamf Trustはデバイスのワークフォルダのみで機能するため、個人アカウントのプライバシーは完全に守られます。

最後に

優れたBYODプログラムは従業員とIT管理者の両方に大きなメリットを与えてくれます。適切なソリューションがあれば、ITはデバイスやユーザに負担をかけることなく、エンタープライズの重要なニーズへの対応に集中することができます。また、ITの過剰な介入がないことで、ユーザも安心して使い慣れた自分のデバイスを業務に役立てることができます。

BYODユーザの登録方法やJamfとAppleの力を借りてBYODプログラムを成功させる方法に興味のある方は、ぜひ**無料トライアル**へのお申し込みをご検討ください。