JamfとAppleで実現するモバイルBYOD

デバイスの種類を問わず仕事ができる環境のためのソリューション

「業務用デバイス = 会社支給デバイス」とは限りません。

会社から支給されたノートパソコンだけが業務に使用される時代は終わりました。今や、多くの従業員が私用のスマートフォンやタブレットを業務に使用しています。これはBYOD（私用デバイスの業務利用）と呼ばれ、企業によっては正式にBYODプログラムが設けられている場合もあります。

最近**ZIPPIAが行った調査**によると、実に**17%の従業員**がIT部門に内緒で私用デバイスを業務に使用しています。

ユーザはすでに自分のデバイスを業務に利用しており、この現実を変えることはできません。

しかし、これはセキュリティの観点から大きな問題となります。なぜなら、IT部門が把握していないデバイスを保護することはできないからです。例えば、Jamfが最近発表した**セキュリティ360レポート**では、「21%の従業員が正しく構成されていないデバイスを使用し、リスクにさらされている」という結果が出ています。

幸いにも、データやネットワークの安全を保つための、正式かつ包括的なBYODプログラムを提供するという選択肢があります。そして、そのために必要なのは、ユーザのプライバシーとデータを保護しながら、高い満足度と生産性を提供することができるソリューションです。

仕事に使用される私用デバイスに求められるものとは？

使い勝手の良さ、セキュリティ、プライバシーの保護

セキュリティの向上と同じくらい大切なのが、優れたユーザエクスペリエンスです。組織は従業員に対し、デバイスをできるだけ安全に使って最大限の生産性を達成してもらいたいと願っています。それには私用デバイスを簡単に使用できる環境が必要です。

このような環境を実現するには、仕事に必要なアプリとプライベートで使用するアプリをシームレスに行き来できるようにしながら、デバイスの業務領域を適切に構成し、セキュリティを担保する必要があります。また、管理されていないデバイスと同じレベルでプライバシーが保護されていることも大切です。

従来のBYODオプション

組織や従業員は、従来のBYODソリューションの採用と導入に対して前向きではありません。従業員のプライバシー、ユーザエクスペリエンス、組織のセキュリティなどの面で多くの課題や懸念が存在するからです。

モバイルアプリケーション管理（MAM）で十分なのでは？

MAMを単独で使用する場合：

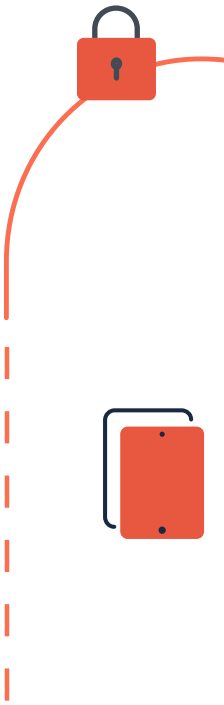
- Wi-Fiやメールの構成、アプリの自動インストールなどを行うことができない（一括購入したアプリも含む）
- アプリはユーザが自分でダウンロードしなければならず、選択肢が少ない場合もある
- MAM専用にアプリを開発する必要があるため、開発コストが高くなる

デバイスをフルに管理する場合

- プライバシーの侵害やユーザへの配慮に欠けた管理につながることがあります。このようなBYOD環境を望む従業員はいません。

デバイスを管理しない場合

- ITや情報セキュリティチームが把握していない、またはなんのセキュリティ対策もされていない私用デバイスが、業務リソースにアクセスすることになります。



JamfとAppleの採用でBYODプログラムを成功に導く

企業データを保護するAppleの機能が、ユーザが個人的に使用するコンテンツのプライバシーも守ってくれるため、企業から閲覧または監視される心配はありません。つまり、真の意味での「1台2役」が可能になるのです。

JamfのBYODサポート

JamfではApple独自の**ユーザ登録**ワークフローと管理対象Apple ID（MAID）を使用しています。これにより、仕事用とプライベートのアカウントを分離して従業員のプライバシーを保護しながら、デバイス上の仕事用アカウントの構成とセキュアな運用を支援することができます。さらにIT部門は、デバイスが企業が定める基準に準拠していることを確認し、個人または部署のニーズに基づいてユーザにアクセス権限やアプリを付与することができます。

Appleの堅牢なセキュリティ態勢と比類のないプライバシー保護をベースにしたJamfの機能

- 従業員のプライバシーの徹底的な保護
- ユーザエクスペリエンスを阻害しない業務リソースへのアクセス
- アプリや企業データを狙う脅威からの保護
- 業務用アプリへのセキュアなアクセス

個人のプライバシーに対するAppleの真剣な姿勢

Appleのユーザ登録ワークフローと内蔵されたプライバシー保護機能により、Apple管理者はデバイスの仕事用アカウントだけを構成することができます。いかなる理由があってもプライベートのアカウントに触れることはできません。

モバイルデバイス管理（MDM）ソリューションの機能には、絶対的なリミットがあります。

MDMの線引き

IT部門にできること

- アカウントの構成
- 管理対象アプリのインベントリへのアクセス
- 管理対象データの削除
- アプリの構成とインストール
- 6桁のパスコードの要求
- 特定の制限の適用
- アプリごとのVPNの構成

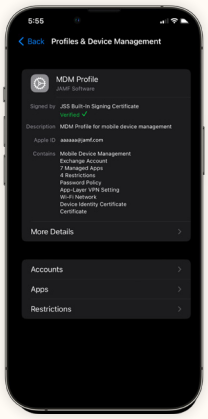
IT部門にできないこと

- 個人情報、データ使用状況、またはログの閲覧
- プライベートで使用されるアプリのインベントリへのアクセス
- 個人データの削除
- プライベートで使用されるアプリの管理
- 複雑なパスコードまたはパスワードの要求
- デバイスの位置情報の取得
- ユニークデバイス識別子（UDI）の取得
- デバイス全体のリモートワイプ
- アクティベーションロックの管理
- ローミングステータスの取得
- 紛失モードの有効化

出典：APPLE「ユーザ登録とMDM」

JamfによるBYODの実現

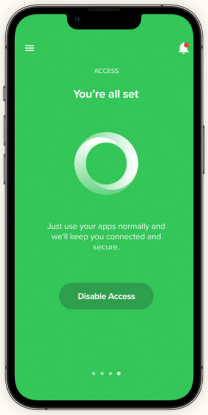
Jamfのソリューションは、組み合わせて使用することで、業務リソースやアプリ、データへのセキュアなアクセスを確保し、**Trusted Access**（信頼できるアクセス）を達成するように設計されています。さらに、ユーザのプライバシーを確実に保護することもできます。



プライバシーを配慮したデバイス登録

Jamf Proは、Appleのユーザ登録ワークフローを使用して仕事とプライベートのアカウントを分離することができます。これにより、組織が従業員の個人データを閲覧したり管理したりすることができなくなります。

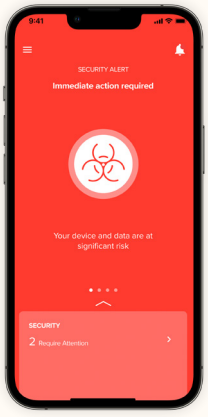
- WiFi、メール、連絡先など、企業サービスへのアクセスの構成
- 仕事用のすべてのiOS/iPadOS用アプリの配布と管理
- 管理対象アプリから管理対象外アプリへのデータの流れを止めるための、データ損失防止ポリシーの導入
- デバイス登録から日々の使用まで、iOSユーザが求めるAppleエクスペリエンスを一貫して提供



セキュアなアクセスとコネクション

Jamf Connectを使用することで、管理対象デバイスを使用する認可されたユーザのみに業務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、エンドユーザアプリであるJamf Trustも利用可能です。

- ゼロトラストネットワークアクセス（ZTNA）によるビジネスアプリケーションへのセキュアで暗号化された接続
- アプリレベルでネットワークトラフィックを管理し、アプリごとのVPN経由でZTNAを構成してプライバシー保護をさらに強化



モバイル向けのエンドポイント保護

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。また、エンドユーザアプリであるJamf Trustも利用可能です。

- 脆弱性またはデータ漏洩のリスクがあるアプリを取り除くワークフローによるリスク管理
- 中間者（MitM）攻撃の検出と阻止
- 古いOSや脆弱性のあるOSバージョンの監視を含む、セキュリティチェックの実行

素晴らしいユーザエクスペリエンスの提供

業務リソースにアクセスする従業員に、Appleならではの素晴らしいユーザエクスペリエンスを提供します。

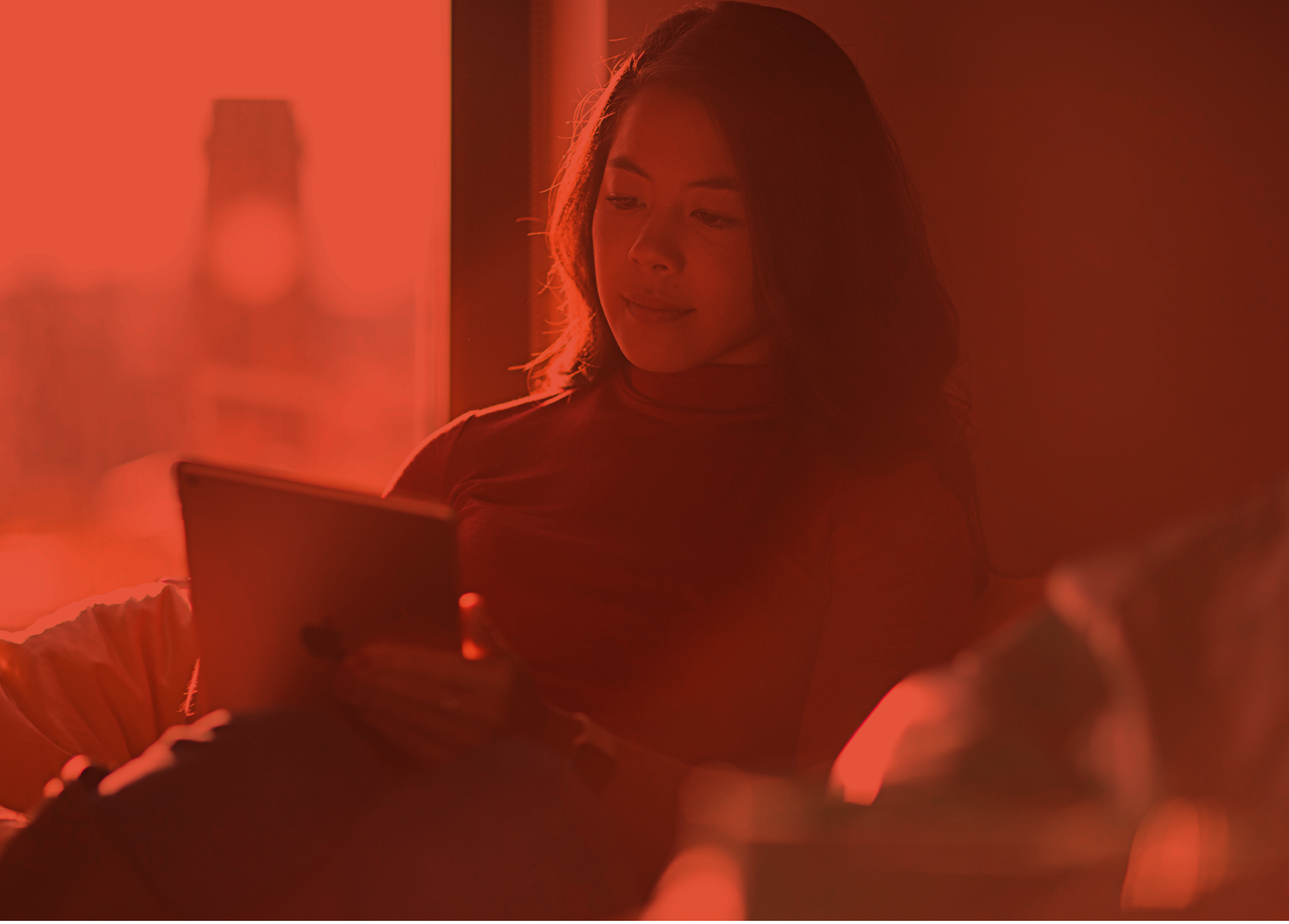
BYODプログラムの成功は、組織が個人情報にアクセスできないこと、そしてユーザエクスペリエンスが維持されることが前提となります。JamfとAppleを組み合わせることで、この両方が実現できます。

Jamf Proによるユーザ登録の機能

- 登録された私用デバイスがITによってどのように管理されているかを明確に可視化
- Appleのネイティブアプリをプライベートと仕事の両方でシームレスに使用
- 承認済みアプリを従業員が自分で**Self Service**からダウンロード
- プライベートのApple IDと管理対象Apple IDを個人用と業務用で分けて使用
- アカウント主導ユーザ登録（管理対象Apple IDを使って設定Appからユーザの認証を行う方法）により、フィッシング攻撃を受ける可能性を低減

Jamf Trust：モバイルBYODのセキュリティの正解

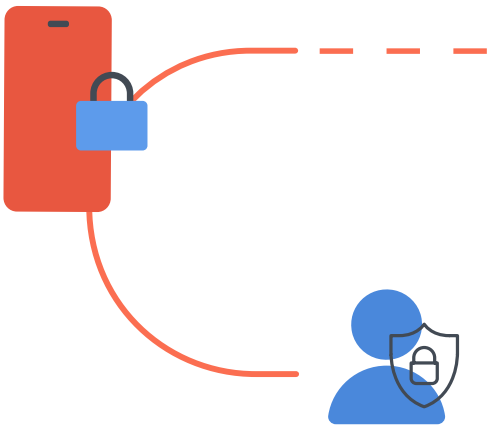
すべての従業員の安全と生産性を守る最適な方法は、物事をシンプルにすることです。**Jamf Trust**アプリを従業員のデバイスに導入するだけで、Jamf ConnectとJamf Protectのアクセスおよびセキュリティ機能をモバイルデバイスが利用できるようになります。Jamf Trustはデバイスのワークアカウントのみで機能するため、個人データのプライバシーは完全に守られます。



JamfはAppleを知り尽くしています

各OSに最適なBYODソリューションを用意することは、組織においてセキュリティやアクセス、デバイスを構成する上で不可欠です。私用デバイスを登録するにあたって、Appleの提供するユーザビリティやセキュリティ、プライバシーの機能を活用することで、組織や従業員にとって理想的な環境を実現することができます。そして、Appleに関する専門知識においてJamfの上に出る企業はありません。

Jamfで組織のセキュリティを向上させながらユーザのプライバシーを保護する方法にご興味をお持ちの方は、**Jamfの担当者もしくは販売代理店までお問い合わせください**。



無料トライアルに申し込む