リモートワークを実現し強化する方法

jamf

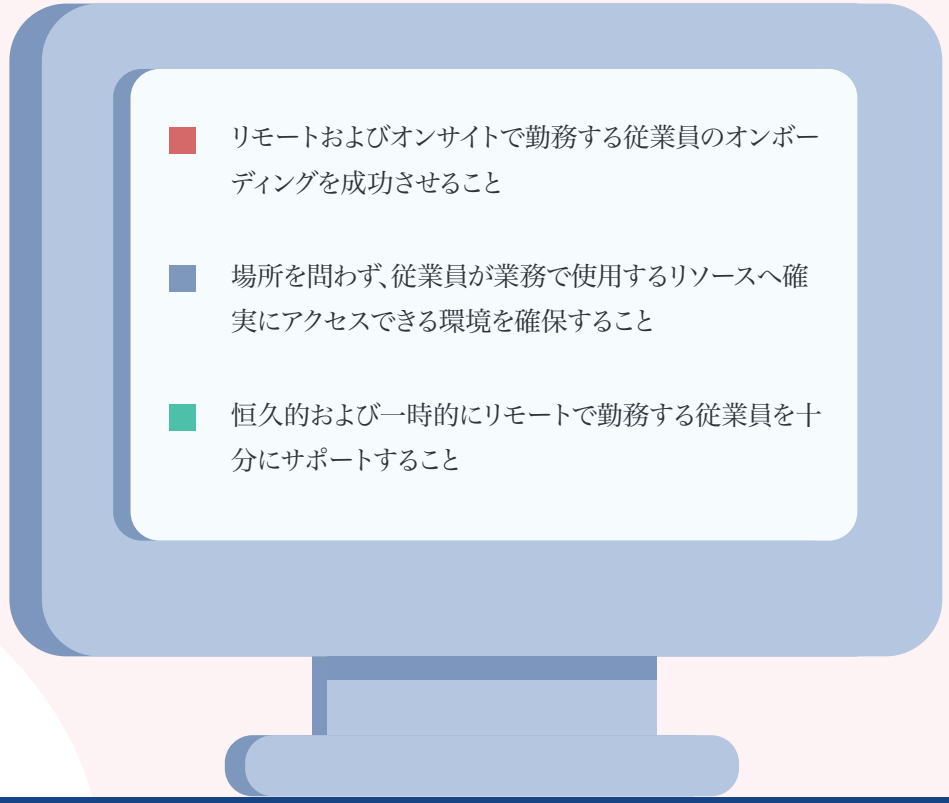
リモートワークを実現する、新たな働き方改革の推進

仕事が場所や時間に縛られることがなくなった今、もっぱらオフィスで 9 時から 5 時まで働く時代は終わりを迎えようとしています。全世界を対象に行われた調査結果によると1、66% の企業がリモートワークを認めており、16% の従業員がフルタイムでリモートワークを行っています。

これを可能にしたのが、ビジネスプロセスの改善と従業員の体験の強化を実現する、デジタル技術の進化でした。しかし、これらの成功は、IT 部門 の責任が高まっているとも言えます。

現在の状況においては、かつてないほどに多くの企業が、従業員の健康管理や定着率、生産性といった理由により、リモートワークや在宅勤務ポリシーを検討しています。

この電子書籍では、以下の通り従業員や企業全体への優れた貢献のあり方について説明します。



より良いオンボーディング体験の提供

企業が従業員の生産性向上の支援を行うことと、新入社員の定着率や生産性の水準は、直接相関しています。企業が素晴らしいオンボーディング体験を提供できれば、従業員の定着率を 82%、従業員の生産性を 70% 以上改善することができます2。

このため、企業が最適なテクノロジーを提供し、適切なツールを活用することで、リモートおよびオンサイトで勤務する従業員のオンボーディングプロセスの効率化を促進することが何よりも重要です。しかし、これらの目的に最も相応しい対応方法を選択する際に、すべてのテクノロジーやツールが同じように作られているわけではないということに気がつきます。

Apple デバイスは、世界中の企業でますます一般的になりつつあります。使いやすさと 従業員からの要望の高まり を受け、多くの企業は Mac、iPad、iPhone のサポートや提供を検討し始めています。こうした傾向は、従業員や IT 部門、組織全体にも非常に大きなメリットをもたらします。

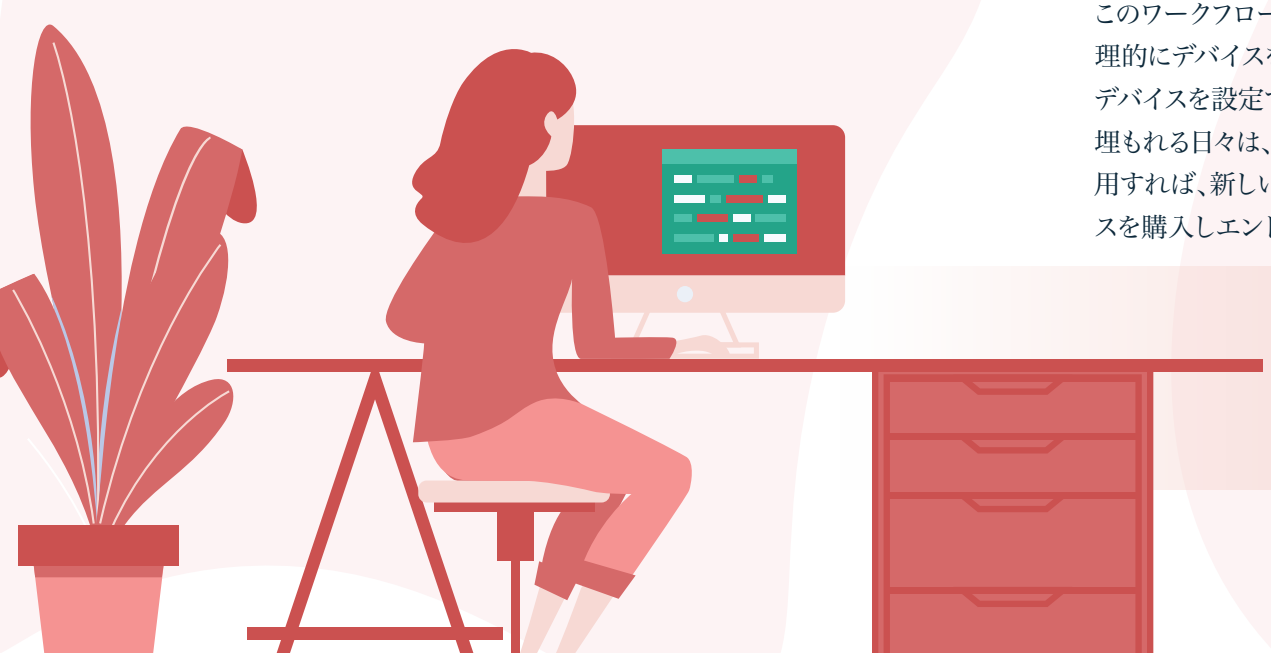
IT 部門による効率的なオンボーディング

IT 部門が優れた第一印象を与える最高のチャンスがあります。Apple Business Manager を活用して、全社的なデバイスのゼロタッチ導入を確立することで、素晴らしい第一印象をしっかりと刻むことができるでしょう。新しいデバイスを開封して電源を入れると、Apple Business Manager が Mac、iPad、iPhone に自動的に企業のモバイルデバイス管理（MDM）ソリューションを登録するよう指示します。

企業における Apple デバイス管理の代表的なソリューションである Jamf Pro は、Apple Business Manager を統合し、デバイス管理をさらなる高みへと導くために、まったくゼロから構築されました。スマートグループのようなパワフルなテクノロジーで、インタラクティブなコミュニケーションを必要とすることなくスマートに管理できる Jamf Pro は、拡大するリモートワークの支援に最高のプラットフォームです。小規模ビジネス向けには、誰でも使えるモバイルデバイス管理であるJamf Nowをご用意しています。

Apple の無料サービスである Apple Business Manager は、Jamf Pro や Jamf Now のようなモバイルデバイス管理ソリューションと組み合わせると、Apple ID の管理プロセスを効率化することができます。業務のために設計された管理対象 Apple ID は、Apple Business Manager で設定と管理をすべて行うことができるため、IT 管理者から個人の Apple ID を職場で利用すべきかどうかという混乱と迷いを取り除き、従業員に対してもメリットをもたらします。エンドユーザーが IT 部門のサポートを必要とすることなく自分のパスワードを管理しリセットできるようになることで、IT 管理者が対応するチケットを削減することができます。

このワークフローによって、IT 管理者が新規に購入したデバイスの箱を開封し物理的にデバイスを操作しなくても、それぞれの従業員向けにパーソナライズされたデバイスを設定できるようになります。IT 部門のスタッフが、新しいデバイスの山に埋もれる日々は、過去のものとなります。Jamf と Apple Business Manager を活用すれば、新しいデバイスの展開、Apple Business Manager を活用してデバイスを購入しエンドユーザーのデスクや自宅へ直接配送することのいずれも簡単に

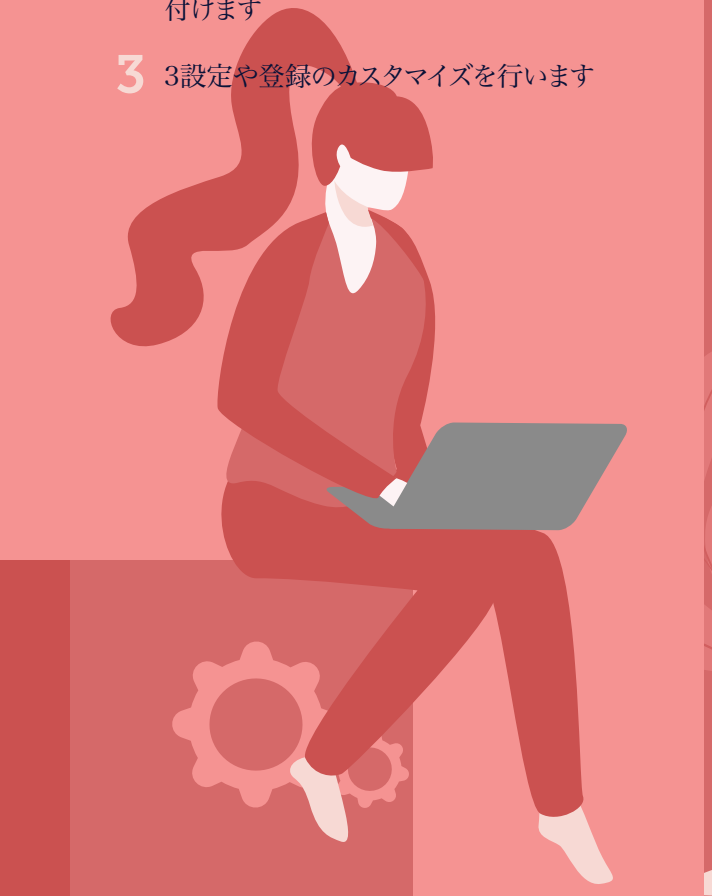


それ以降は IT 部門とのやりとりは必要ないため、リモートで働く従業員を様々な形でサポートすることに注力できます。

ゼロタッチ導入のプロセスを開始するために、企業が実施すべきことは、準備、購入、展開のみです。

準備

1. Apple Business Manager にサインアップします
2. Apple Business Managerに MDM サーバーを追加し、アカウント情報を紐付けます
3. 3設定や登録のカスタマイズを行います



購入

1. Apple や Apple 正規代理店から Apple デバイスを購入します
2. 登録するデバイスを割り当てます

展開

1. 購入した Apple デバイスを従業員に直接送付します
2. 従業員が開梱し、デバイスの電源を入れます
3. Apple デバイスは自動的に MDM に登録されます

従業員のためのシンプルなオンボーディング

入社初日というのは、どんな従業員でも緊張しているものです。初日から従業員の必要とする（そして希望する）ツールをゼロタッチ導入によって提供することで、従業員の不安を軽減しましょう。

リモートで勤務する従業員にとって、まさに「タップ数回」や「クリックするだけ」の操作によって、生産性向上を実現することができます。新しい Apple のデバイスが郵送されてくるのを待ち、開封して電源を入れるだけ。これだけでいいのです。従業員は、オンサイトで勤務する仕事相手とまったく同じ方法で、メール、VPN、生産性向上のためのアプリケーションなどの業務リソースをただちに使用することができます。お使いのデバイス管理ソリューションで、登録カスタマイズのワークフローを柔軟に設定でき、これによって新入社員が自身のデバイスで登録画面をクリックすると、ビデオやドキュメント、その他の情報を簡単に表示できるようになります。

リモートで勤務する従業員は、社内の全エンドユーザーが利用できる無料のアプリポータルである Self Service で、お気に入りのアプリやその他の重要リソースをすばやく検索したり、活用したりできるようになります。

IT 部門はデバイスを手動で操作し各種設定を行う必要はなく、また従業員はデバイスを受け取るためだけにオフィスへ足を運ばなくてよいのです。

ゼロトラストアクセスで従業員をつなぐ

企業は、最新の認証方法やセキュリティ対策に関心を向けつつあります。それらは、デバイスの展開プロセスや、リモートおよびオンサイトで勤務する従業員の現行のライフサイクル管理をさらに差別化してカスタマイズするために必要なテク

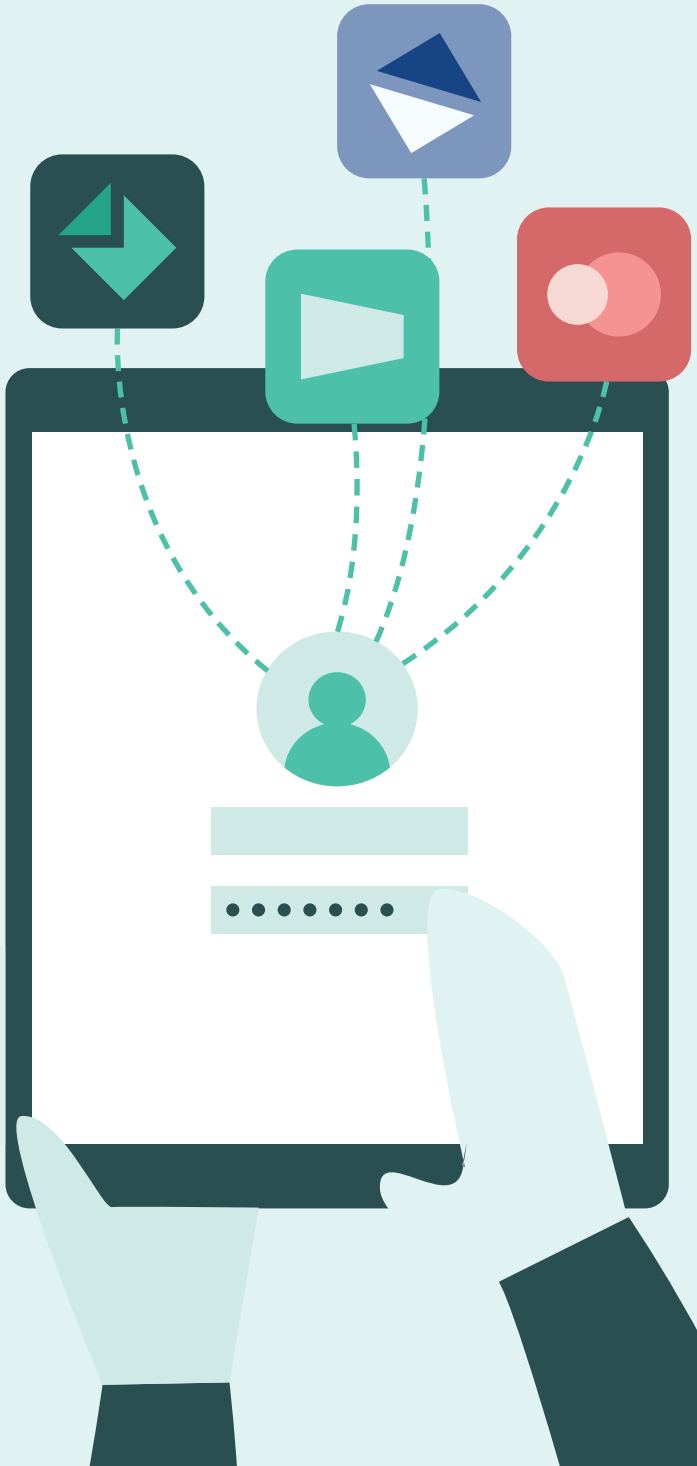
Jamf Connect のような認証および ID 管理ソリューションを活用し、企業は「Never trust, always verify（信頼できないことを前提として、必ず認証する）」戦略を推進することができます。安全でないネットワークを通じて機密情報やリソースにアクセスする可能性があるリモートワークを行う従業員とって、非常に重要なことです。

Jamf Connect と、Okta および Microsoft Azure Active Directory といったクラウド ID プロバイダ（クラウド IdP）は、ユーザーおよびデバイスの高度な信頼性を企業に提供しつつ、従業員に対しては、シームレスで途切れることのない体験を実現しています。

以下の 3 つの領域を通じて実現することができます。

アカウントのプロビジョニングと認証

IT 管理者は、従業員のクラウド IdP 認証情報のみに基づき、生産性を実現するために必要なあらゆるビジネス・アプリケーションを 、Mac にプロビジョニングすることができます。これにより、ゼロタッチ導入をさらに一歩進め、ユーザーは単一セットの認証情報でログインし、多要素認証も完備しているため、企業は適切な従業員が適切なデバイスで適切なリソースにアクセスしていることを確認することができます。

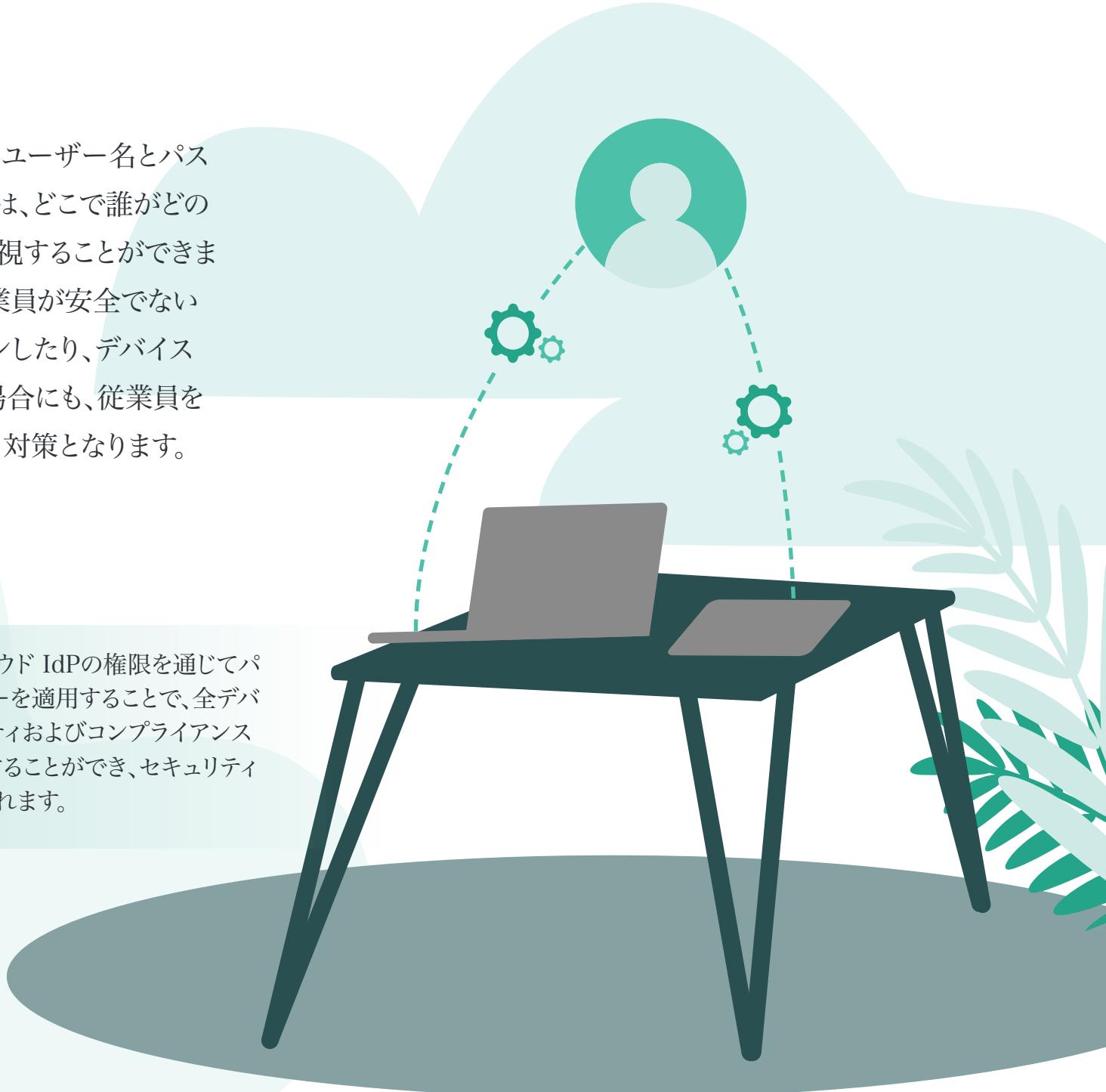


日々の運用において、このようなシンプルでありながら安全性を確保したログイン体験が、ユーザーのログインのたびに実行され

ID 管理

Jamf Connect はクラウド IdP のユーザー名とパスワードを要求するため、IT 管理者は、どこで誰がどのデバイスにアクセスしているかを監視することができます。これは、リモートで勤務する従業員が安全でないネットワークからデバイスにログインしたり、デバイスを紛失したり盗難にあったりした場合にも、従業員を保護するための強力なセキュリティ対策となります。

IT 部門は、クラウド IdPの権限を通じてパスワードポリシーを適用することで、全デバイスにセキュリティおよびコンプライアンスの基準を維持することができ、セキュリティがさらに強化されます。



ユーザー ID とデバイスの認証情報の同期

Jamf Connect により、従業員は自身の企業 ID（クラウド IdP の ID）を、ローカルの Mac アカウントのパスワードと常に同期させておくことができます。つまり、従業員は何度もパスワードを入力することなく、必要とするあらゆるものにアクセスできるようになるのです。

40% Gartner によると、ヘルプデスクが対応する問合せの 40% は、パスワードのリセットに関するものです[3]。Jamf Connect はこのような問合せを削減することによって IT 部門の対応時間を大幅に節約し、さらに、これまで従業員が問合せ完了まで業務を行うこと

リモートワークを行う従業員への継続的サポート

ここまで説明してきた、「オンボーディング」と「即時かつ安全なリソースへの接続」は、生産的なリモートワークを促進するために必要な 2 ステップです。加えて、デバイスの継続的な管理も同様に重要です。

Jamf Pro および Jamf Now は、Apple プッシュ通知サービス（APNs）を通じてデバイスと通信し、デバイスがどのように動作しているのかを知らせます。これによりデバイスとの常時接続が維持されるため、IT 部門が対応する必要はありません。

IT 部門が（リモートであれオンサイトであれ）デバイスの設定変更を行うときには、構成プロファイルや管理コマンドを APNs 経由で送信するだけです。VPN、電子メール、Wi-Fi、その他多数の設定を、従業員とやりとりせずデバイスへ自動的に適用することができます。

対象デバイスの一括指定

特許取得済みテクノロジーである Jamf Pro のスマートグループ機能を使って、対象となるデバイスやデバイスグループを指定します。これによって、管理対象の全デバイスのインベントリ情報を収集し、必要に応じてグループ全体またはサブセットに対してアクションを自動的に実行することができます。例えば、より多くの従業員がリモートワークを行う場合、そのような従業員をすべてスマートグループ内に設定し、対象デバイスに対して VPN 構成プロファイルを自動的に展開することで、企業リソースへのシームレスなアクセスを実現します。

また、Self Service を通じて、従業員がオンデマンドで必要なアイテムを利用することもできます。IT 部門が Self Service に、承認された構成プロファイル、リソース、一般的な問題のトラブルシューティング用スクリプト、ブックマーク、信頼済みアプリを構成しておくことで、従業員が自らこれらにアクセスし、ダウンロードすることができるようになります。

IT 部門によるヘルプデスクチケットの対応を必要とすることなく、昼夜を問わず、また世界のどこからでも、ユーザー自身ですべてを実行できるのです。

高度なアプリ管理

デバイスや企業のセキュリティにとって、最新のアプリや OS を展開することも重要です。Jamf Pro および Jamf Now では、IT 部門がアプリや OS を効率的に展開し、インベントリ情報を通じてプロセスを監視することができます。

ビジネスの世界はアプリ上で動いています。企業の経営戦略も、これに適切に対応する必要があります。Apple Business Manager と Jamf Pro を統合することによって、App Store（または自社のアプリディレクトリ）からアプリを購入し、デバイスへ直接展開することができます。これらのアプリは、デバイスにプッシュ配信で提供したり、Self Service を経由してユーザー自身がダウンロードして利用したりすることも可能です。

最新のOS の利用開始を遅らせて、IT 部門が新しい OS の検証を行ってから、リモートで勤務するエンドユーザーに利用させることも可能です。これは Jamf Pro が IT ヘルプデスクの負荷を軽減し、エンドユーザーが IT 部門のサポートを必要とすることなく対応できる状態を実現する、もう 1 つの方法です。

強力な Mac の保護

多くの従業員が仕事で Mac を活用するにつれて、Mac 専用のセキュリティ対策の必要性が高まっています。従業員が自宅でコンピュータを使用する場合、社内アセットに対する攻撃というまったく新しいリスクが生じます。企業のネットワークであれば通常は閲覧しないような Web サイトに従業員がアクセスしたり、デバイス上で個人的な電子メールのやりとりをしたり、子どもを信頼して Web サイトのゲームをプレイさせたりするなど、いつも以上に気の緩みが見られるかもしれません。その結果、デバイスがマルウェアに感染した場合、セキュリティチームや IT 部門は、こうした攻撃にリモートで対処しなければならないという新たな課題に直面します。

Jamf は、デバイスに関わる体験や従業員のプライバシーに影響を与えることなく、リモートの macOS エンドポイントセキュリティを保護します。

Jamf Protect は、Apple の新しい Endpoint Security フレームワークや macOS システムイベントのデバイス上の分析など、ネイティブのセキュリティツールを活用することで、テレメトリーや検出のカスタマイズを作成し、デバイスがどこにある場合でも、すべての macOS の状態について優れた可視性を企業のセキュリティチームが利用できるようになります。

Jamf Protect と Jamf Pro により、デバイスを企業のネットワークに接続することなく、macOS 上のインシデントを特定して対処するための最適なツールを利用することができます。

- 悪意のある動作についてのリアルタイムアラートを受信
- デバイス上の動作を調査
- 既知の不正なアプリケーションに対するプロアクティブなブロック設定
- 機密情報を扱うリソースからデバイスを隔離
- デバイス上の悪意あるファイルを除去
- macOS とインストール済みアプリケーションを再度展開

機動力を備えた最新の働き方の実現

企業がワークフローを整備し、従業員がどこにいようとも安全性と生産性を確保する必要性があるのは、昨今の感染症がもたらした重大な局面に対応するためだけではありません。

リモートワークのトレンドは今後も継続していくでしょう。ポジティブな企業文化を維持するためには、オンサイトの従業員と同じように、リモートで勤務する従業員にも権限を与える必要があります。Jamf は、最高レベルのセキュリティを備えた優れた体験を従業員に提供して、このようなビジョンを実現します。

今すぐ Jamf Pro の試用版をご利用いただき、従業員のリモートワーク移行にいち早く着手しましょう。Jamf のお客様には、Jamf を最大限活用する方法を解説した 130 の無料オンライントレーニングモジュールをご利用いただけます。

試用版を申し込む

1 https://www.talentlms.com/blog/remote-work-statistics-survey/

2 https://b2b-assets.glassdoor.com/the-true-cost-of-a-bad-hire.pdf

3 https://342sv54cwf1w32bxz36tm0bv-wpengine.netdna-ssl.com/wp-content/uploads/2015/05/AD-Password-reset-tool.pdf