jamf

Windows中心の企業環境におけるAppleデバイス活用戦略：卓越したユーザエクスペリエンス提供のガイドライン

はじめに

ユーザエクスペリエンスが、生産性を左右する

ユーザエクスペリエンスを重視するというAppleの思想をITプロセスにまで展開すると、社内のストレスが減り、生産性とROI（Return on Invenstment：投資利益率）の最大化につながります。

「Jamfが選ばれる理由」シリーズの第2弾となる本ガイドは、あらゆる習熟度のIT管理者/エグゼクティブの皆様へ、アイデンティティ、セキュリティ、自動化、そしてオブザーバビリティ（可観測性）への既存投資を最大限に活用するために必要な情報を提供します。これにより、従業員の生産性を維持しながら、課題の克服や一般的な阻害要因の排除を可能にします。

概要

デバイスの初期設定、アクセス管理、ソフトウェアアップデートや脅威対策を、手動のプロセスに頼っているようでは生産性は低下してしまいます。そこで、このガイドでは、デバイス管理、ID管理、セキュリティを統合し、ユーザエクスペリエンスの改善やITの運用効率化につなげていく方法を紹介します。Jamfのソリューションは、ゼロタッチ導入、ロールベースのアクセス制御、アプリのライフサイクル管理の自動化の機能が備わっており、オンボーディングの時間短縮や、デバイスのセキュリティとコンプライアンスの維持に大きな効果を発揮します。例えば、Self Service+は、承認済みのアプリのインストールやよくある問題の解決を従業員自身がオンデマンドで行えるツールであり、ポリシーの一貫した適用と、ヘルプデスクのチケット減少に寄与します。その結果、強固なセキュリティに守られた拡張性に優れた業務フローが実現し、管理業務の効率がアップします。また、従業員が初日から生産性を発揮することも可能になります。

Jamf製品で解決できる生産性関連の課題

開封して電源を入れれば「すぐに業務に取りかかれる」デバイスを用意し、**従業員をスムーズにオンボーディング**する

ゼロトラストによりデバイスや認証情報の健全性を検証し、重要リソースに対するリスクを軽減する

初回のログイン時点から**安全なベースライン構成を適用**する（さらに、役割に基づく最適化も実施する）

リアルタイムの可視性を確保し、問題に先回りで対処する（インシデントの後追い対応を脱する）

ソフトウェアのアップデートを自動化し、ダウンタイムを最小限にとどめ、コンプライアンスを最大限確保する

セルフサービスを活用することで、ユーザが必要な時に必要なサポートを受けられる環境を整え、**ヘルプデスクの負担を軽減**する

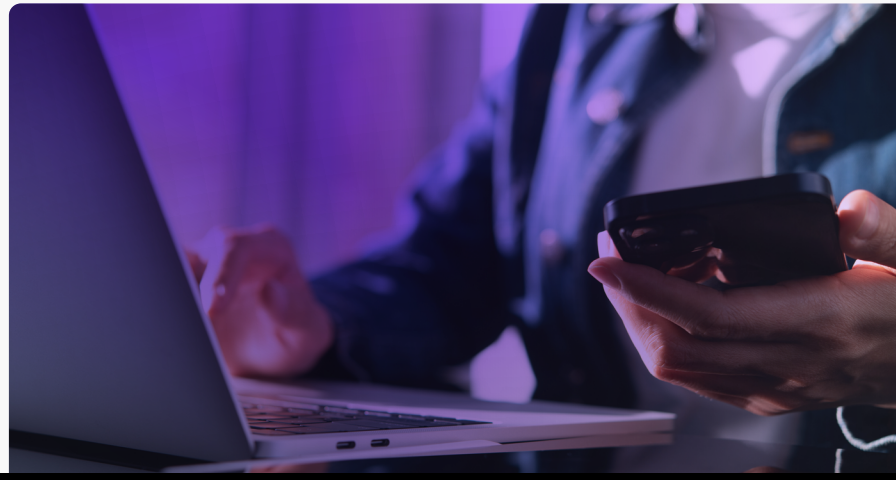
スムーズなオンボーディングで、勤務初日から生産性を発揮

以下は、初期設定のプロセスを手作業で実施している場合の流れの一例です。

1. **ハードウェアを調達する**
2. **デバイスを開封する**
3. **デバイスを一箇所に集める**
4. **画面に従って初期設定を進める**
5. **必要なものをインストールする**
   - OSアップデート
   - アプリケーション
   - エンドポイントセキュリティ
6. **必要な構成を実施する**
   - ハードウェア設定
   - ソフトウェア設定
   - セキュリティベースライン
7. **エンドポイントが監視できていることを確認する**
8. **エンドユーザに支給する**
9. **エンドユーザが認証できることを確認する**
10. **エンドユーザが必要なツールにアクセスできることを確認する**

理論上は、新入社員のためにデバイスを準備する10のステップが、それほど大きな負担には見えないかもしれません。しかし実際には、1,000台以上のデバイスを管理している企業にとって、たとえ10台であってもこのような手動プロセスで対応することは、時間、生産性、そして予算への影響を考えると、躊躇せざるを得ないのが実情です。

場合によっては、手順5と6だけでも1台あたり数時間かかる事態も起こりえます。OSやソフトウェアのパッチ適用、業務用ソフトウェアのインストール、コンプライアンス確保に向けたソフトウェア設定などのシンプルな作業ですら、再起動に伴って作業が何度も中断したり、各種プロセスの完了を待つ時間が発生したりすることは避けられません。すべてが終わる頃には、既に半日が経っているということも珍しくないのです。



貴重なリソースを無駄にしないソリューションとは

ポイントは、デバイス管理、ID管理、セキュリティを統合し、それを基盤としてゼロタッチ導入でエンドユーザの役割に応じた初期設定を自動化することです。これにより、新規採用した従業員がハードウェアを『業務で使える状態』になるまで待機する時間を数分へと短縮できるだけでなく、業務を開始して生産性を発揮できるようになるまでのタイムラグを大幅に最小化することが可能です。

その具体的なメリットは以下のとおりです。

- IIT部門によるサポート待ちに伴う**オンボーディングの遅延を解消**
- オフィスでのデバイス受け渡しが不要
- ヒューマンエラーや繰り返しの作業による疲弊を排除
- 従業員が勤務初日から生産性を発揮し、組織に貢献
- 効率的な業務フローで時間とコストを節約

Jamfが選ばれる理由

Jamfは、IT部門がオンボーディング関連のサポートに費やす時間を削減する、柔軟かつ強力なワークフローを提供します。手作業による設定から自動導入モデルに移行できるため、エンドユーザが自分でデバイスを登録し、必要なソフトウェア、ツール、構成にセルフサービスでアクセス できる便利で効率的な業務フローが実現します。

アクセスポリシー：生産性を落とすことなくデータを守る

データセキュリティの基盤となるのが、アクセス制御リスト（ACL）です。これは、どのユーザアカウントにどのリソースに対するアクセス権限を付与するか（または、付与しないか）ということでもあります。ITサポート担当者の必要人数を判断する際には、デバイスの台数を考慮するのが一般的です。これに対して、ID管理に関するデータセキュリティ戦略を考えるにあたっては、IT担当者がサポートに対応するユーザの人数を考慮する必要があります。

構成を手作業で実施する場合の最大のポイントは、権限の設定作業の回数が、「必要な権限の数 × エンドユーザの総数」で決まるという点です。つまり、エンドユーザの人数が増えるほど、IT部門に求められる権限設定作業の回数が飛躍的に増えていくのです。作業が増えれば、完了までの時間が長くなるのはもちろんですが、ヒューマンエラーや同じ作業の繰り返しによるミスのリスクも高まります。パフォーマンスにとって大打撃となることは間違いありません。さらに、IT部門の手作業に頼る状況では、何か設定の変更が必要な事象（従業員の昇進、リスク許容度の変化など）が起こるたびに、アカウントやデバイス一つひとつに変更が必要になります。これでは、規模拡大に対応していくのはきわめて困難です。

拡張性に優れた最適なソリューションとは

デバイス管理とエンドポイントセキュリティにアイデンティティ&アクセス管理（IAM）を統合すると、企業のニーズに最大限対応できるカスタマイズ性が実現します。また、アカウントやデバイスごとの変更の手作業を減らし、一元的なセキュリティモデルに移行できる点も魅力です。このモデルでは、役割ベースのアクセス制御（RBAC）を使用し、機密性の高いリソースに対するユーザのアクセス権限を、個々人のアイデンティティや業務に使用するデバイスではなく、役割に基づいて定義します。

その具体的なメリットは以下のとおりです。

- **権限の割り当て**が効率化（一元的なリポジトリで管理されている役割とグループメンバーシップをベースとしたものに変わる）
- 最小権限の原則を適用し、必要なものだけに**アクセスを制限**
- **ユーザが認証し**、アクセス権限を付与したら、その後はデバイスや役割が変わってもアクセス権限を維持
- IT部門の変更作業が（デバイスやユーザが増えても）1回で済むため、**管理業務の負担が軽減**
- 情報を一元的に可視化するとともに、コンプライアンスの実施状況をログに記録し、統制状況の監査を**効率化**

Jamfが選ばれる理由

クラウドアイデンティティプロバイダー（IdP）のネイティブサポートにより、ユーザの認証情報やエンドポイントを管理する一元的なアイデンティティベースのセキュリティ制御を、Jamfインスタンスにもそのまま適用できるようになります。また、アイデンティティの統合を基盤としたシームレスなユーザ体験を提供するだけでなく、Windows PCからMac、モバイルデバイスに至るまでのリソース全体にIAM戦略を適用できるため、カスタマイズ性と拡張性のどちらにも優れた一元的なID管理の枠組みが実現します。

アプリのライフサイクル管理を効率化

業務に使用するソフトウェアソリューションを何にするかは、非常に大きな問題です。ユーザエクスペリエンスは重要ですが、会社としてはコンプライアンスの確保も欠かせません。そこで、以下のような要素を検討する必要があります。

- **会社のニーズ**
- **ユーザの好み**
- **複数のプラットフォーム**
- **さまざまな種類のデバイス**

多種多様な企業の要求とユーザの利便性を両立させ、かつコンプライアンスを完全に遵守することは、まさに至難の業です。さらには、ネイティブアプリ、社内開発のプログラムやシステム、クラウドソフトウェアなどへの対応も大きな課題として立ちはだかります。

多数のオペレーティングシステムのパッチ管理の作業は、最初こそ数分程度で済んでいても、やがて数時間、数日単位の仕事へと簡単に膨れ上がってしまいます。セキュリティリリースやアプリのアップデートが次々に発生するほか、デバイスの種類も数もどんどん増えていき、IT部門の手に負えなくなってくるからです。

IT部門の人数に対してデバイスの台数がさほど多くない状況であっても、アプリのアップデートやデバイスのOSのアップグレードに手作業で対応していては、エンドユーザが業務を進められない時間が発生する原因になります。また、組織には以下のようなリスクも出てきます。

- **パッチ未適用の脆弱性：**
  アップデートの適用漏れが原因で発生
- **ソフトウェアの破損：**
  不完全なアップデートが原因で発生
- **セキュリティ状態の弱体化：**
  断片的なパッチ展開が原因で発生
- **未承認のアプリの利用：**
  いわゆるシャドーITの問題
- **アプリケーションの完全性の問題：**
  または**安全でないアプリのインストール**

アプリのライフサイクル管理を一元化するソリューションとは

アプリケーションの一元管理とネイティブ導入を実現したうえで、エンドポイントの可視化、ポリシーベースのコンプライアンス適用、ソフトウェアアップデートの自動化の機能を組み込めば、OSや種類を問わず常にデバイスを（ユーザの作業を中断させることなく）最新の状態に保ちつつ、企業データの侵害につながる既知の脆弱性をインフラ全体にわたって均一に緩和できます。

その具体的なメリットは以下のとおりです。

インベントリ情報が**リアルタイムで更新**されるようになり、管理対象デバイスにインストールされているアプリやそのバージョンの可視性が高まります。

完全性と開発元がデジタル署名で検証されたアプリケーションを、**正規の開発者から確実に入手**できるようになります。

ソフトウェアをネイティブにインストールし、その**アップデートを自動化**できるため、アプリのライフサイクル管理が効率化し、IT部門の負担が軽くなります。

ポリシーにより**コンプライアンス**が確保されるため、管理対象アプリがどのデバイスでも同一の構成で入手できるようになります。

監査証跡の記録が**効率化します**。ログが一元的に記録されるため、コンプライアンスの証明や、監査人との共有が簡単に進められます。

Jamfが選ばれる理由

パッチ管理戦略で重要な要素は、セキュリティ、実効性、拡張性、一貫性の4つです。Jamf App インストーラを使えば、この4要素をクリアしつつ、コンプライアンス管理を自動化し、サードパーティソフトウェアの導入に際してエンドポイントにベースラインとしてのセキュリティを確保できます。加えて、各種ベンチマークに基づく強力かつ柔軟なポリシーも活用すれば、OSやシステムにも最新のセキュリティパッチを確実に適用し、デバイスに強固なセキュリティ状態を実現できます。それがひいては、会社全体のセキュリティ状態の強化にもつながっていきます。

ユーザに到達する前に脅威に対処する

悪意のある脅威ほど生産性を悪化させるものはありません。データへのアクセスが妨害されたり、業務に影響が出るほどインターネットの速度が遅くなったり、企業データが侵害を受けて完全性が損なわれたりすれば、生産性に大きな悪影響が及びます。

ここまでのセクションでは、デバイス導入、アクセス権限、アプリのライフサイクル管理についてそれぞれ説明してきました。このセクションのトピックは、脅威の対策と予防です。最新鋭の脅威を予防することは、従業員の生産性を維持するうえできわめて重要です。特に、モバイルデバイスや多様なプラットフォーム、そしてクラウドベースのサービスへの依存といった現代の企業環境を突く、巧妙な脅威が増えています。こうした脅威は、オフィス勤務かリモートワークかを問わず、あらゆる環境のエンドユーザを標的にしています。

既存の脅威の悪影響が深刻化しないようにするうえでは、優れたインシデント対応が欠かせません。しかし、脆弱性を抱えるエンドポイントが侵害された場合、その対応を開始する頃には、エンドユーザが既に悪影響を実感してしまっているのが現実です。加えて、問題の修復には大きな混乱を伴うことから、業務の遅れはいっそう長期化する傾向にあります。**その結果は以下のとおりです。**

- **生産性**の**低下**
- **ダウンタイム**の長期化
- 多数の部門に**影響が拡大**
- 悪影響が**会社全体に波及**
- **収益**機会の**逸失**
- お客様からの信用の**毀損**
- 修復のための**コスト**が増大

脅威を未然に防ぐためのソリューションとは

脅威を阻止するためには、そもそも脅威を特定できていなければなりません。企業データにとってのリスクがコンプライアンス違反のアプリであるか、ユーザの自己判断による設定変更であるかを問わず、侵害を予防するための鍵は、脅威を未然に防ぐことにあります。

その具体的なメリットは以下のとおりです。

- **エンドポイントの健全性など、コンテキスト情報が豊富なテレメトリデータを積極的に監視**できる
- エンドポイントのリスクマトリックスを深く理解したうえで、**脅威の深刻度および対応の優先順位の評価が可能になる**
- **デバイスが管理対象であるかどうかを問わず、保護されたリソースにアクセスするデバイスの可視性**が高まる
- **各種のソリューションを統合**することにより、デバイス管理、ID管理、エンドポイントセキュリティのすべてを横断する一元的戦略が実現する
- **機械学習（ML）**テクノロジーを活用し、既知の脅威の特定と解決の精度および拡張性を高められる

Jamfが選ばれる理由

Jamf製品なら、多層防御を通じてエンドポイントのコンプライアンスを検証・確保できます。リアルタイムの監視によりデバイスの健全性を常に確認できるほか、問題が発見された場合にはログに記録のうえ、IT部門にレポートが送られるため、会社のリソースに対するリスクに発展する前に対処できます。さらに、そのデータを基にデバイスをコンプライアンス状態に自動で復帰させるので、IT部門が介入することなく、エンドユーザにも気づかれないままに問題を解決できます。

ダウンタイムゼロを目指して:
従業員と業務を止めないために

包括的なIT管理戦略を考えるうえで考慮が必要な要素には、
以下のようなものがあります。

- **クロスプラットフォーム対応**
- **デスクトップデバイスとモバイルデバイスの併用**
- **ハイブリッドクラウドテクノロジーの利用状況**
- **勤務場所の多様化**
- **デバイスの所有モデルの混在**

このような要素が複雑に絡み合うことから、戦略策定は困難を極めます。IT部門は、自社が右肩上がりの成長を続けられるよう、多種多様な課題を検討しなければなりません。例えば、オフィス勤務のメンバーとリモート勤務のメンバーのどちらも生産性を維持できるようにする必要がありますし、様々なベンダーのソリューションをシームレスに統合したり、インフラの隅々までセキュリティを拡張したりすることも重要です。

世界各地でビジネスを展開する現代の企業は、多方面に足を伸ばすタコのようです。それぞれの足が、デジタルトランスフォーメーション（DX）の実現に向けた戦略的な取り組みです。

ファイアウォール、ウイルス対策ソフト、オンプレミスドメイン、VPN接続などを駆使して、通信を境界ネットワークという安全な壁の中に封じ込めておけば済む時代はもう終わりました。今日では、「足」（戦略的取り組みの各領域）の一つひとつを効果的に管理および保護できる動的かつ柔軟なソリューションが求められています。このソリューションは、デバイスや場所、オペレーティングシステムを問わず使える必要があるほか、ユーザが期待するレベルの利便性とアクセスを保障しつつ、デバイスや企業リソース、ユーザプライバシーのすべてを保護できなければなりません。

プラットフォームの垣根を越えて重要リソースを動的に保護できるソリューションとは

従来のソリューションでは、データ侵害につながるセキュリティギャップの解消は困難です。今日の企業が必要としているのは、様々な状況に柔軟に適応できるテクノロジーです。具体的には、ゼロトラストアーキテクチャを基盤とし、IAM、デバイス管理、エンドポイントセキュリティを駆使して最新の脅威や攻撃を防ぎつつ、コンプライアンス確保にも寄与する包括的なソリューションです。

その具体的なメリットは以下のとおりです。

- 暗黙的な信頼モデルから**デフォルトではアクセスを拒否**（無条件に信頼はせず、常に検証する）するモデルへ移行できる
- **認証情報**と**デバイスの健全性を明示的に確認**したうえでアクセスを許可できるようになる
- **文脈認識**のレイヤーが追加され、行動分析で高度な脅威に対抗できるようになる
- トラフィックをそれぞれ別個のマイクロトンネルに分離する**ネットワーク内防御**を実装し、傍受や横展開を予防できる
- インシデント対応の**迅速化**と修復ワークフローの自動化により、ダウンタイムを短縮できる

Jamfが選ばれる理由

Jamfのゼロトラストネットワークアクセス（ZTNA）では、最新鋭の脅威への対策をサポート対象のあらゆるデバイスに適用できます。デバイスの場所やネットワーク接続の手段を問わず、クロスプラットフォームの均一な保護が実現するため、セキュリティ戦略の効率化に大きな効果を発揮します。また、設計段階から多層防御の仕組みを組み込んである点も大きなポイントです。これにより、エンドユーザが各種企業リソースにネイティブアクセスできる状態を保ちつつ、業務運営とコンプライアンス関連のどちらのニーズについてもIT部門の対応を強化できます。

ヘルプデスクへの問い合わせを最小限に減らし、ユーザの生産性を最大化

IT部門の役割のなかで最も重要なものといえば、ユーザのニーズへの対応です。しかし、ほとんどの組織では、従業員数に対してIT専門職が圧倒的に足りていません。IT部門が問題の対応・トリアージ・解決を迅速に、効率的かつ効果的に進めていけるかどうかは、以下のような要因に左右されます。

- **平均的な問い合わせ処理量**
- **業務フローの効率**
- **IT部門の規模**
- **企業文化**
- **IT担当者のスキルセット**

上記のいずれか1つにでも問題があれば、それが原因となって生まれるズレにより、状況がどんどん悪化していきます。業務効率が低下するのはもちろんのこと、最終的には業務とビジネス目標との連続性が失われる事態にもなりかねません。

長期的な帰結としては上に挙げたとおりですが、現場の関係者にはもっと直接的な悪影響が現れます。具体的には、以下のような問題が原因となって、各種の作業に遅れが生じます。

- ソフトウェアの**インストール漏れ**
- **不適切な**設定
- 権限の**設定ミス**
- システムの**エラー**メッセージ
- ハードウェアの**互換性の問題**

IT部門の生産性を高めるソリューションとは

よく知られているように、ユーザのアクセス権限を増やしても、ユーザエクスペリエンスに関する問題は解決しません。それどころか、データの完全性が損なわれたり、セキュリティインシデントにつながったりするという意味で、むしろリスクを大きくする行為です。

これに対して、関係者が（技術的なバックグラウンドがなくても）自分たちで問題を解決できるようサポートする一元的リポジトリを構築すれば、ユーザに必要な時点で必要なサポートを届けることができます。また、IT部門がユーザの生産性を最大限高める業務フローの検討に割ける時間が増え、会社の目標達成に貢献できるようになるのも大きなポイントです。

その具体的なメリットは以下のとおりです。

- 関係者を守るべき対象ではなく、**ソリューションの一部として巻き込む**ことが可能になる
- 権限の標準を変更しなくても、エンドユーザが**承認済みのアプリをインストール**し、**承認済みの設定を適用**できるようになる
- ユーザにとって使いやすいストア形式の画面で、**アプリケーションのアップデート**をワンクリックで自動完了できる
- 企業のアプリストアを**クラウドベースのIdP**と連携し、ユーザの状況に即した対応が可能になる
- ユーザエクスペリエンスを損なわない**ネイティブなアプリストア**が実現する（アプリのアップデート通知も提供できるようになる）

Jamfが選ばれる理由

Mac、iPhone、iPad向けのSelf-Service+では、Appleネイティブの自社専用アプリストアを構築できます。ストアにはアプリケーションやツールだけでなく、スクリプトや（プリンターなどの）機材の設定、アップデートなども公開しておくことができ、いずれも管理者権限を使わずに1クリックで利用できるので非常に便利です。また、IdPと統合すれば、各種アクセス要求をシームレスに承認することも可能です。この承認はあくまでも一時的なものなので、コンプライアンスに対する影響を最小限に抑えられます。加えて、監査証跡もしっかり残ります。

まとめ

組織が生産性を高めるためには、ITの運用と従業員のユーザエクスペリエンスの両方の問題解決に取り組むことが欠かせません。そのために重要なのは、デバイス管理、ID管理、エンドポイントセキュリティの3つを統合することです。この3つを統合すれば、オンボーディングの自動化、一貫したアクセス制御、アプリケーションの健全性維持、脅威の予防など、さまざまなメリットがもたらされます。Jamfは、ユーザの生産性・セキュリティを維持しつつ多種多様なデバイスに対応できる拡張性を備えたワークフローで、ここに挙げたメリットの実現をサポートします。また、ゼロタッチ導入、攻撃の先手を打つ保護、(従業員がよくある問題を自分で解決できる)セルフサービスの機能は、IT部門が運用オーバーヘッドを削減しつつ、コンプライアンスやレジリエンスを強化するうえで大きな効果を発揮します。従業員が勤務初日から有意義な業務に集中できる安全かつ効率的な環境の実現に、ぜひお役立てください。

本資料の要点

- **大量のデバイスのオンボーディングにはゼロタッチ導入が効果的**：ゼロタッチ導入を使えば、手作業による初期設定が不要になるため、業務利用に向けたデバイスの準備を短時間で完了できます。
- **役割ベースのアクセス制御は拡張性に優れ、ユーザの生産性も落とさない**：役割ベースのアクセス制御なら、組織が拡大してもアイデンティティに応じた権限を自動で設定できます。
- **パッチやアップデートを自動化し、大量のエンドポイントのアプリの健全性を維持**：パッチやアップデートの適用を自動化すれば、生産性を落とすことなくソフトウェアに強固なセキュリティを確保できます。
- **脅威は、業務に影響が及ぶ前に阻止**：継続的な監視とコンプライアンス管理を徹底すれば、従業員の勤務場所が分散していてもダウンタイムを抑えられます。
- **セルフサービスでユーザの利便性向上とIT部門の負担軽減を両立**：アプリのインストールやよくある問題の解決をサポートに頼らず、ユーザが自分でできる環境を整えれば、ユーザとIT部門の双方の時間を節約できます。
- **プラットフォームや勤務場所を問わず一貫したユーザエクスペリエンスを実現することが重要**：一元的な業務フローを構築すれば、オフィスで働く従業員も、リモートワークの従業員も、デバイスのセキュリティを維持しながら生産性を発揮できます。

jamf

ぜひお試しください

トライアルを申し込む