MAC/IPAD/IPHONE/APPLE TV向け

Appleデバイス セキュリティ

初心者ガイド

周到に計画されたサイバー攻撃を受けたり、意図せずマルウェアをダウンロードしてしまったりすると、生産的な1日を過ごす代わりにすべての業務を一旦停止せざるを得なくなります。ハッカーのやり口がより巧妙になるにつれ、顧客や従業員、または生徒の安全や全体的な収益を守るため、組織はセキュリティに常に気を配らなければなりません。

一般的なITセキュリティと同様に、Appleセキュリティにも多くの課題があります。

Appleは、自社製品のセキュリティ機能に多大な投資を行い、デバイスやデータのプライバシー保護やセキュリティの分野においてリーダー的存在となりました。しかし、セキュリティ上の課題と無縁なオペレーティングシステムなど存在しません。

そのため、管理者はセキュリティ上の問題に迅速に対応するだけでなく、それを未然に防ぐことを求められています。

Appleデバイスの組織的なセキュリティに真剣に取り組みたいと考える管理者やマネージャーのために作られたこのeBookは、初めての方には基本的な情報を、Apple管理のベテランには復習の機会を提供します。

Appleセキュリティの基本

セキュリティの基礎的要素

組織のハードウェアとデータのセキュリティを確保するためには、以下の6つの要素を連動させる必要があります。

Appleネイティブのセキュリティ

macOS、iOS、tvOSに内蔵されたセキュリティシステム

Page 4

デバイスのセキュリティ確保

物理的なデバイスと、そのユーザの保護

Page 6

データの暗号化

保存データと転送中データの基本的な暗号化

Page 8

コンプライアンスの監視

必要なアップデートを的確に判断するためのデバイスモニタリング

Page 11

アプリケーションのセキュリティ確保とパッチ適用

ソフトウェアを最新に保つ

Page 12

セキュアな導入

最高レベルのセキュリティで導入

Page 14

基礎的要素 その1 Appleネイティブのセキュリティ

Appleネイティブのセキュリティ機能をデバイス管理に活用する方法

macOS（Mac用オペレーティングシステム）、iOS（iPad/iPhone用オペレーティングシステム）、tvOS（Apple TV用オペレーティングシステム）には、すでに豊富なセキュリティ機能が内蔵されており、以下のような利点があります。

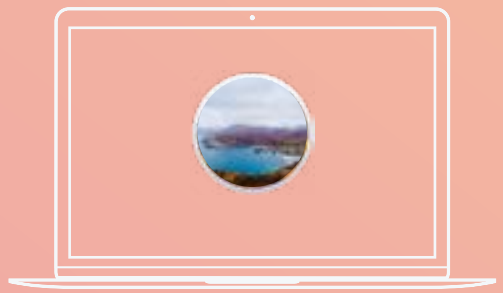
- 大幅な研究を経て開発されたUnixをベースに構築されており、安定性に優れている
- 強力なセキュリティフレームワーク
- ロック機能やデバイスを探す機能によるデバイスセキュリティの実現
- モバイルデバイス管理（MDM）の構成オプションを利用したセキュリティコントロールの実装と構成

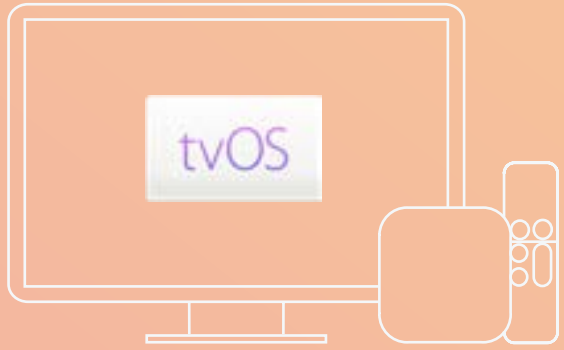
MDMソリューションを利用すると、Appleネイティブのセキュリティ構成を多数のデバイスに一括導入および適用することができます。これにより、何千台ものMacを安全にセットアップできます。

また、MDMツールを活用することで、紛失や盗難に遭ったデバイスをロックまたはワイプ（消去）できるため、セキュリティコントロールを拡大させることが可能です。

セキュリティ機能の詳細

macOS、iOS、tvOSに内蔵されたセキュリティ機能





macOSのセキュリティ機能

- ソフトウェアアップデート
- システム整合性保護（SIP）
- Gatekeeper
- App Store
- FileVault暗号化
- XProtect
- アプリのサンドボックス化
- プライバシー設定

iOSのセキュリティ機能

- ソフトウェアアップデート
- セキュアなシステム
- App Store
- Touch ID
- ハードウェアの暗号化
- アプリのサンドボックス化
- プライバシー
- 監視
- 紛失したデバイスを探す機能

tvOSのセキュリティ機能

- Appleによるダイレクトソフトウェアアップデート
- 審査を通った安全なApp Storeアプリ
- 監視（MDM使用時）
- アプリ制限
- AirPlayの設定とパスワード
- バナーとスクリーンのデフォルト設定

基礎的要素 その2 デバイスのセキュリティ確保

デバイスとユーザの追跡、セキュリティ確保、保護

組織のセキュリティフレームワークやエンドユーザの安全性は、たった1台のデバイスを通して簡単に損なわれてしまいます。生徒、教師、ヘルスケアワーカー、リモートスタッフ、ショップ店員、出張の多い会社員など、組織に所属するユーザが誰であっても、その組織のデバイスは常に多数のロケーションに散らばっている可能性があります。

デバイスの紛失や盗難

iPadやiPhone、Macの紛失や盗難は、金銭的な損失だけでなく、セキュリティ上の大きなリスクとなります。紛失したノートパソコンから生徒の個人データが漏洩したり、組織のデータベースへのアクセスが可能になった場合、その被害は計り知れないものになる可能性があります。また、元従業員が業務用のノートパソコンを返却せずに、個人情報を公開したり、競合他社に提供したりするかもしれません。リモートソースからのマルウェアが持ち込まれる可能性もゼロではありません。

デバイスの紛失や盗難自体は珍しいことではありません。事故や不注意はつきものですが、肝心なのはそのデバイスの行方がわからなくなった時にどう対処するのかについてあらかじめ計画しておくことです。

さらに、生徒や患者に提供されるデバイスや複数のユーザが共有するデバイスは、他人のデータを偶然発見してしまった場合や、誤用、不適切なコンテンツの閲覧などに対する安全策が必要になります。

デバイスのセキュリティ確保や制限を手動で行う場合

Mac

- すべてのデバイスでパスワードの入力が必要
- [システム環境設定] > [Apple ID] > [iCloud]から「Macを探す」を有効にする
- ユーザが各自iCloudにサインインし、パスワードを記憶する必要あり
- すべてのMacのシリアル番号を追跡
- デバイスが紛失または盗難に遭った場合はAppleに連絡
- ウェブサイトをブロックする場合、デバイス上でペアレンタルコントロール機能を有効にする必要あり（ブラウザがSafariの場合）

iPad & iPhone

- すべてのデバイスでパスワードの入力が必要
- 設定Appで自分の名前をタップし、「探す」を選択して有効にする
- ユーザが各自iCloudにサインインし、パスワードを記憶する必要あり
- デバイスが紛失または盗難に遭った場合はAppleに連絡
- デバイスごとに異なるアカウントを作成し、個々のデバイスでペアレンタルコントロールを有効にする必要あり

Apple TV

- すべてのApple TVでパスワードの入力が必要
- 制限を追加：
  - メインメニューから「設定」を開き、[一般] > [制限]を選択
  - 制限を選んで有効にする
  - 4桁のパスコードを作成
  - もう一度4桁の数字を入力して確認し、OKを選択
  - パスコードを記憶する必要あり
  - すべてのApple TVで上記の手順を繰り返す必要あり

デバイスのセキュリティ確保

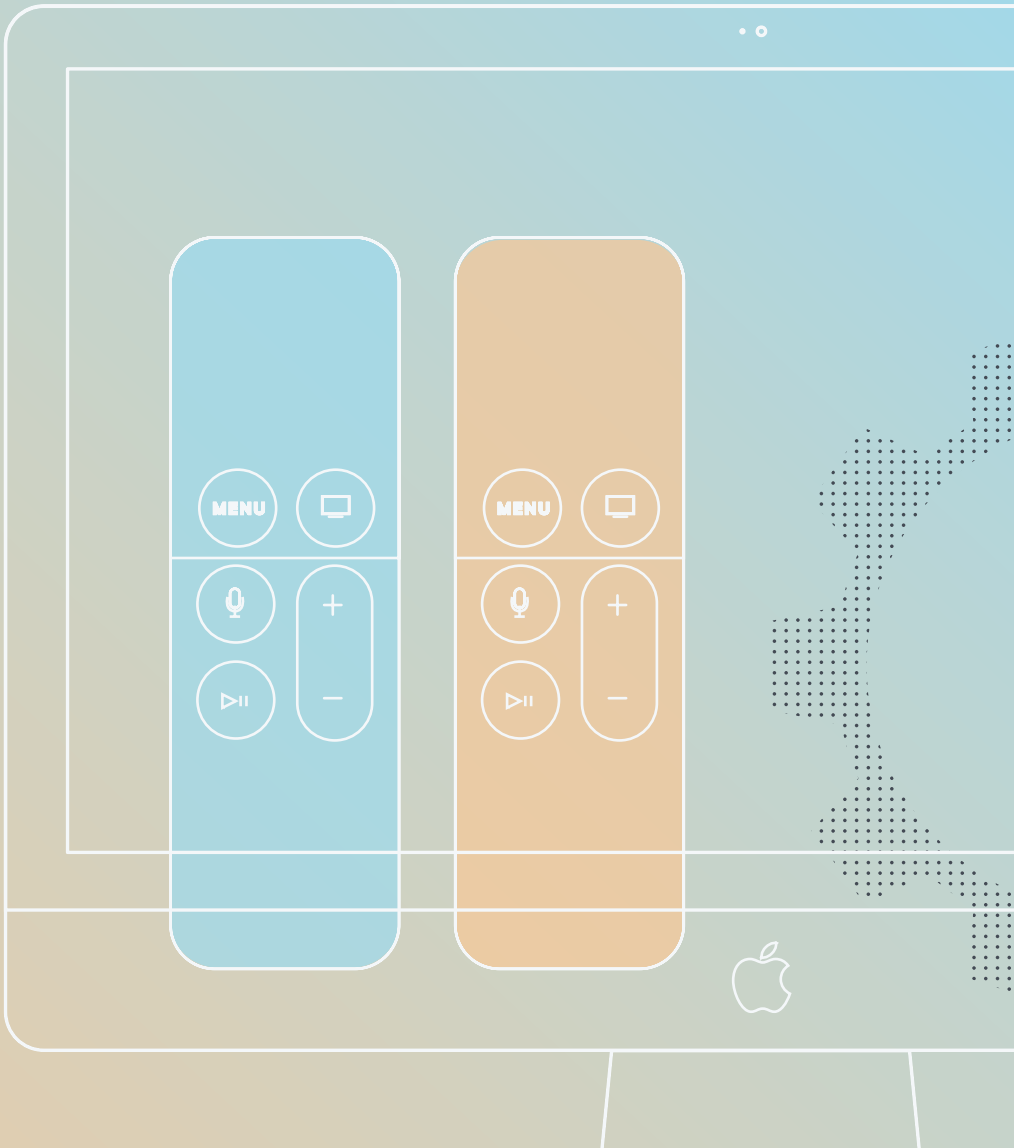
Apple TVにAirPlayの制限を追加

- メインメニューから[設定] > [AirPlay]を選択
- AirPlayを有効または無効にする
- 次のいずれかを選択：
  - 全員
  - 同じネットワーク上の全員
- すべてのApple TVで上記の手順を繰り返す必要あり

JamfなどのMDMでデバイスのセキュリティを確保または制限を追加

Mac, iPad, iPhone, Apple TV

- 初回使用時にすべての制限やセキュリティ機能を設定、または構成プロファイルやポリシーで設定
- 紛失または不正使用されたデバイスを一元的にロック
- 紛失または不正使用されたデバイスを一元的にワイプ（消去）
- 複数のユーザが独自にサインインする形でデバイスの安全な共有を実現、または別のユーザが使用する前にデバイスをワイプ（例：病室での使用時など）



基礎的要素 その3 データの暗号化

保存データと転送中のデータの基本的な違いと、両方のデータのセキュリティを維持する方法

学校における生徒の個人情報、ヘルスケア施設における患者の医療データ、企業における知的財産など、組織の大切なデータを守る上で暗号化はもはや選択肢のひとつというよりは不可欠なものとなっています。デバイス上のすべてのデータを暗号化することは、ビジネスにおけるベストプラクティスと言えます。

データには2つのタイプがあります

デバイスまたはデータベース上のデータ

ネットワーク上を移動する情報

データの暗号化

保存データ
ディスクまたはデバイスの暗号化

- macOSでディスクの暗号化を行うには内蔵のFileVaultを使用します。ドライブを暗号化するためにソフトウェアを追加する必要はありません。
- FileVaultはFIPS 140-2の認証を受けています。これは、Appleの暗号化システムが連邦政府レベルの最高基準を満たしていることを意味します。
- FileVaultは手動またはリモートで有効にすることができます。各ユーザにデバイス上でオプションを選択してもらう方法と、IT管理者が（Jamfを使用して）数百、数千のデバイスに対して一斉にFileVaultを有効にする方法があります。
- Jamfでは、暗号化を解除する必要のある時や、ユーザがパスワードを忘れた場合などに備えて、暗号化キーを一元的に保管することができます。

FileVaultを手動で有効にする場合

1. [システム環境設定] > [セキュリティとプライバシー] > [FileVault]
2. 「FireVaultをオンにする」を選択する
3. すべてのデバイスで上記の手順を繰り返す

組織のすべてのデバイスでFileVaultを有効にするためには、MDMソリューションを活用して暗号化の自動化、導入、適応を行うのがベストです。FileVaultを有効にする構成プロファイルやポリシーを導入し、スタッフが将来的にデバイスの暗号化を解除する必要がある場合に備えて、IT管理者が暗号化キーを取得しておくこともできます。

1. Jamfで必要なオプションを選択して構成プロファイルを簡単に作成
2. 必要な台数のデバイスを導入
3. ステップ3はありません

Jamfでは、ユーザが自分でFileVaultを有効にした場合でも、復旧キーがリダイレクトされるように構成することが可能です。この場合、キーはITの管理ソリューションに保管されます。

iPadやiPhoneの場合は？

iOSデバイスの場合、暗号化はさらに簡単です。パスコードが設定されると同時に内蔵の暗号化を利用できるようになります。パスワードの設定は各ユーザに行ってもらうか、Jamfを使って行うことができ、パスコードの長さや複雑さなどのパラメータを設定することも可能です。

データの暗号化

転送中のデータ

VPN（仮想プライベートネットワーク）は、デバイスから別のサービスへとネットワーク上を移動するデータを保護してくれます。

リモートで働く場合や出張中は、VPNを使用して組織のネットワークに接続するのがベストです。これにより、信頼できる組織のネットワークへの安全な接続が確保され、データがエンドツーエンドで暗号化された状態で送信されるようになります。

macOSとiOSのどちらにもVPNクライアントが内蔵されており、複数の大手VPNサービスプロバイダに接続することができます。

転送中のデータに必要なもの

- セキュアなネットワーク接続環境
- VPNサーバ

VPNに手動で接続する場合

VPNプロバイダを設定した上で：

1. [システム環境設定] → [ネットワーク]
2. デバイスのVPNサーバーのアドレスを入力
3. ネットワークオプションからアドレスを選択
4. すべてのデバイスで上記の手順を繰り返す

複数のデバイスをVPNに接続する場合

VPNプロバイダを設定した上で：

1. iOSやMac用のMDM（例：Jamf）で構成プロファイルを作成
2. すべてのデバイスに構成を導入
3. ステップ3はありません

暗号化がシームレスに行われていることを確認するには？

セキュリティと一貫した暗号化を確保するための重要な方法のひとつが、MDMをクラウドでホストすることです。Jamf Cloudのような評判の良い製品であれば、サーバのセキュリティやデータの安全性はもちろん、アップデートやパッチがリリース後すぐに適用されるので安心です。

基礎的要素 その4 コンプライアンスの監視

すべてのデバイスに確実にプロトコルとコントロールを適用

セキュリティシステムに弱点はつきものです。最大限のセキュリティを提供するために、管理者は組織のデバイスを監視し、すべてのデバイスに最新のアップデートとパッチが適用されていることや、正しい暗号化オプションが有効になっていることを確認しなければなりません。

コンプライアンスの監視を手動で行う場合

組織内のすべてのデバイスを確実に保護するためには、デバイスを常に監査する必要があります。

1. すべてのデバイスを個別に追跡
2. 以下の点について各オプションを個別に確認：
   - 最新のアップデートが適用されているか
   - 暗号化されているか
   - マルウェアやウイルスを侵入させていないか
3. アップデートがあるたびに以上の手順を繰り返し実行
4. そしてさらに繰り返す
5. 常に注意を払い、エンドユーザから賛同と協力を得ることが必要

Jamfを使ってコンプライアンス監視を行う場合

Jamfのインベントリ機能を通して組織内のすべてのデバイスを保護するために：

1. すべてのデバイスの最新リアルタイム情報を確認
2. セキュリティが不十分なデバイスに対してアップデートやセキュリティ構成を導入
3. ステップ3はありません

デバイスのステータスを確認できることで、管理者はどのアップデートをどこに送信すべきか、どのセキュリティ機能を構成すべきかを知ることができます。部署や権限、デバイスの種類などの分類に基づいたスマートグループを作成すれば、アップデートの対象を絞り込むことも、全体に適用することも可能です。

基礎的要素 その5 アプリケーションのセキュリティ確保とパッチ適用

パッチのタイムリーな適用とアプリケーションの安全性確保

アプリケーションの安全性

アプリケーションにマルウェアやその他の悪意のあるコードが含まれていないことを確認することは非常に大切です。アプリケーションのソースが信頼できない場合、セキュリティの確保は難しくなります。

アプリの安全なダウンロードおよび使用のために、Appleは以下の機能を提供しています

- 各アプリケーションに独自の空間を与えて他のアプリケーションとのインタラクションを防ぐための**サンドボックスモデル**を採用。他のアプリの共有データの読み込みや書き込みを許可するには、ユーザまたは管理者の承認が必要になります
- セキュリティリスクを軽減するため、**App Store**のすべてのアプリは審査されます。審査に通らなければiOSデバイス用のアプリは提供できないため、セキュリティが担保されます。また、Mac用アプリはApp Storeでしか入手できないため、管理者にとってもデバイス全体のセキュリティを管理しやすくなります
- **macOS向けGatekeeper**は、ユーザが自分で選択するか、管理者がJamfのようなMDMを利用してすべてのデバイスに対して構成することができる機能です。ユーザまたは管理者は、3つのGatekeeperオプションから選択し、以下の場所からダウンロードしたアプリを許可することができます。
  - Mac App Store
  - Mac App Storeと確認済みの開発元
  - 指定なし

独自のアプリケーションを作成したり、アプリケーションを再パッケージ化する場合には、Mac App Storeと確認された開発元のアプリのみを許可するのがベストです。Gatekeeperに信頼されるよう、自身で署名することをお勧めします。

許可するダウンロード元を指定しない選択肢も用意されていますが、送信中に何者かによって手が加えられた場合に備えて、アプリがどこから来たのか、また信頼できる開発者によって署名されているのかを確認することが重要です。

Gatekeeperのオプションを手動で設定する場合

1. [環境設定] → [セキュリティとプライバシ] > [一般]
2. 3つのオプションから選択
3. 組織内のすべてのデバイスに対して以上の手順を繰り返す

JamfでGatekeeperのオプションを設定する場合

これまでのパターンと同じで、構成プロファイルを設定し、すべてのデバイスに導入します。

それだけです。

アプリケーションのセキュリティ確保とパッチ適用

パッチの適用

すべてのソフトウェアは人間の手で作られます。よってバグが存在します。ヒューマンエラーを避けることは、人間が人間である限り無理と言えます。

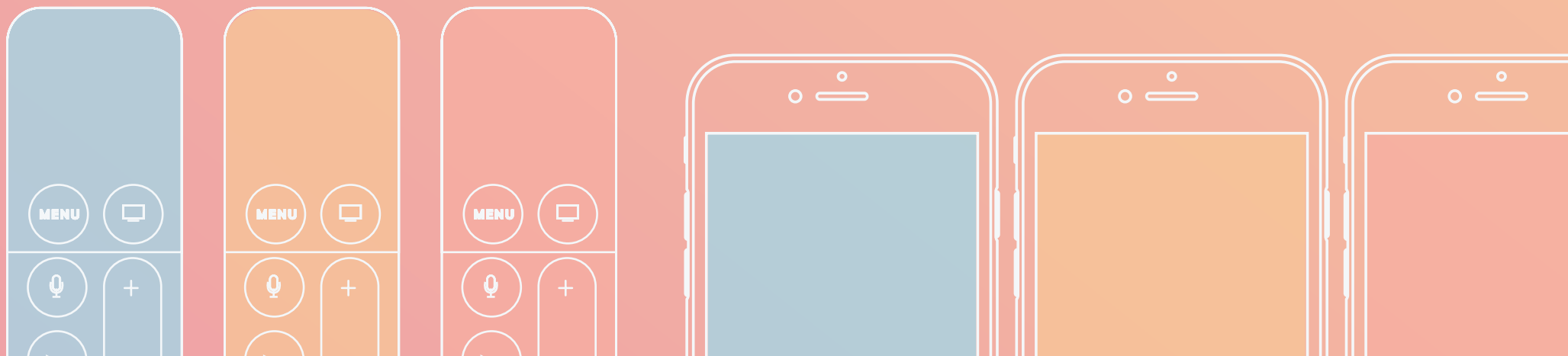
そのため、組織ではバグ修正をできるだけ早く実装する戦略を取ることが不可欠です。バグがセキュリティの脆弱性になり得る場合は特に注意が必要です。

パッチ管理を手動で行う場合

- デバイスにアップデートに関する通知が届いたらすぐに自分でアップデートを行うようユーザを教育
- アプリの新しいパッチがリリースされたらすべてのデバイスを回収し、手動でダウンロード
- 手動によるコンプライアンス監視の実施中にパッチが適用されていないデバイスを検出

パッチ管理をJamfで行う場合

- アップデートとパッチに関する通知と、組織内のすべてのデバイスにパッチを導入するためのツールが自動でJamfに送信されるため、パッチを見逃すことはありません
- Jamfのアプリカタログ「Self Service」を利用すると、アプリの使用を続ける前にアップデートを行うようユーザに通知を送ることができるため、ユーザ側で簡単にアップデートを行うことができます
- または、個人によるアップデートの実施を禁止して、ポリシーですべてのデバイスにパッチを配布したり、スマートグループに対して配布することもできます



基礎的要素 その6 セキュアな導入

AppleのDevice Enrollment ProgramとJamfを活用したデバイスとソフトウェアのセキュアな導入

すべてのデバイスのセキュアな導入を実現するための第一歩は、Appleが無料で提供しているDevice Enrollment Programへの登録です。

このプログラムでは、組織が所有するすべてのデバイス、および組織が選んだMDMでそれらを管理することをAppleに通知します。このプログラムに登録されたデバイスが初めて起動すると、自動的に組織のMDMに登録されます。これにより、より厳格なセキュリティコントロールと迅速なセキュリティアップデートが可能になり、同時にすべての構成プロファイルを適用することができます。これにより時間の節約やセキュリティの確保が実現され、憶測で物事を進める必要がなくなります。

jamf

Jamfで得られるもの

ゼロタッチ登録

拡張可能な導入プロセス

セキュアな構成

Mac、iPad、iPhone、Apple TVに対応

デバイスとデータのセキュリティを軽視すると痛い目に遭います

組織はAppleを通じてできるだけ強力なセキュリティ対策を実施し、将来起こりうる攻撃や盗難に対して先手を打つことができます。これにJamfを組み合わせることで、手動によるセキュリティプロトコルよりもさらに簡単かつ迅速、そして安全なセキュリティ管理が可能になります。

jamf

実際に何かが起こってしまってから慌てるのではなく、デバイスとデータのセキュリティを積極的に確保し、組織とそれを構成する個人の安全とセキュリティを維持しましょう。

最適なセキュリティオプションをお探しの方は、ぜひJamf製品の無料トライアルにお申し込みいただくか、当社のスペシャリストまでお気軽にお問い合わせください。

トライアルに申し込む　お問い合わせ

または、お近くのApple認定販売代理店経由でトライアルにお申し込みいただくこともできます。