



ホワイトペーパー

macOS の セキュリティの強化

組織のセキュリティを維持し、常に最新の macOS を 安心してご利用いただくために

セキュリティに対するニーズはあらゆるオペレーティングシステムで高まっており、macOS も例外ではありません。Apple ではネイティブのプライバシー機能とセキュリティ機能に集中的に投資してきましたが、企業内での Mac プラットフォームの市場が拡大するにつれ、マルウェアや侵害、脆弱性発見が増えています。従業員が自分でコンピューターを選べる企業では、macOS の使用を許可している企業がこれまでにないほど増えています。そのなかで、他のプラットフォーム同様、macOS でもセキュリティを強化して詳細な管理が求められています。

複数のセキュリティベンダーが Mac を保護するためのソリューションを提供しています。しかし、ほとんどのソリューションでベンダー固有、または自社の Windows 向け製品のセキュリティモデルを使用しており、macOS の最新のフレームワークには対応していません。これにより、変化し続けるオペレーティングシステムを最新の状態に保つことが難しくなっています。そのため、既存の macOS セキュリティモデルを拡張してセキュリティを強化し、組織を脅威から効果的に守るためにセキュリティ部門が必要とする macOS 固有のメリットを活用する必要があります。

このホワイトペーパーでは、macOS セキュリティの現状の概要、および効率的かつ効果的でユーザに影響の少ない方法で Apple のセキュリティ機能を強化する方法についてご紹介します。

このホワイトペーパーで取り上げる内容

- ・ Mac に組み込まれているセキュリティ機能の詳細
- ・ 企業向けにセキュリティ機能を強化する仕組み
- ・ 署名や組み込み機能よりも強力な脅威検出の実現
- ・ Apple のセキュリティモデルを高度なエンタープライズセキュリティへと拡張する方法

macOS におけるアプリケーションの信頼

Apple ではユーザと、実行されるサードパーティアプリケーションの間の信頼を構築するセキュリティ機能の設計に多大な努力を払ってきました。このセクションではこうした機能の一部を紹介して、戦略的に強化および拡張する方法について説明します。Apple のセキュリティ機能の詳細については、Apple プラットフォームのセキュリティ (<https://support.apple.com/guide/security/>) を参照してください。

Gatekeeper による信頼の検証

Apple が推奨しており、最も信頼性の高い形でサードパーティアプリケーションをインストールする手段が App Store です。Apple は App Store 上のアプリが、プライバシーやセキュリティ、ユーザエクスペリエンスの標準を満たしているか確認を行います。ただし、Apple では、App Store のアプリケーション機能を制限しており、ビジネスに必要なアプリケーションにとって App Store のような配信方法は最適でない場合もあります。

App Store からの配信ができない場合のために、Apple では macOS 開発者が自分でホスティングしているダウンロードサイトや従来の配信方法でアプリケーションを配信できるようにしています。こうした「特別

な配信方法をサポートするために、Apple ではオペレーティングシステムに追加のチェックを導入することで、macOS デバイス間で信頼されていないソフトウェアが蔓延するリスクを軽減しています。Gatekeeper は Apple の信頼性チェックと認証チェックの中心的な役割を果たす機能です。当初は信頼レベルに基づいてプログラムの実行を許可する macOS の機能としてスタートしましたが、現在は幅広い範囲をカバーする厳しい要件と緩和の両方を提供する形へと進化しています。基本的な信頼レベルでは、今でも「App Store」または「App Store と身元確認済みの開発者」からアプリをダウンロードできますが、信頼されていないコードを実行するオプションに対して厳格な対応がなされていない状況が続いています。

こうしたチェックはインターネットからダウンロードされたアプリケーションにのみ適用されます。Apple では、ダウンロードされたファイルに隔離属性と呼ばれる追加のメタデータを添付することで、こうしたアプリケーションを追跡しています。プログラムが実行されると、隔離属性を検証してプログラムが実行可能か判断するなど、Gatekeeper によってさまざまなチェックが実行されます。最も基本的なチェックの 1 つが、さきほど説明した設定に従って、アプリケーションが正当な開発者によって署名されているか、App Store を通じて配信されているかを確認することです。

アプリケーションが開発者によって署名されている場合は、取り消された署名が登録されているデータベースとアプリケーションの証明書を照合して、署名者が過去

にマルウェアに関係していないことを確認します。このようにして、Apple は証明書を迅速に失効させ、マルウェアの蔓延を防いでいます。

macOS Catalina 以降、Gatekeeper のセキュリティチェックを通過するには Apple のノータリゼーション（公証）が必要になっています。アプリケーションがセキュリティチェックを通過するには、アプリケーションをアップロードして Apple に分析してもらう必要があります。分析に問題がなければ、公証データがアプリケーションと関連付けられて、この追加の調査に合格したという記録が残されます。

最終的な信頼はユーザに依存

使い勝手を優先するために、macOS ではさまざまな場面でエンドユーザが Gatekeeper を「オーバーライド」することができます。ユーザはアプリケーションを右クリックして、「開く」または「プログラムから開く」をクリックするだけでアプリケーションを開くことができます。アプリケーションの起動を一律で拒否する代わりに、信頼されていないアプリケーションを起動しようとしていることを警告する新しいダイアログが表示されますが、Gatekeeper ではこうしたアプリケーションを実行することができます。XProtect によって特定されたマルウェアについてはユーザが実行することができません。

アプリケーションを初めて実行したときに隔離コンポーネントが更新されるので、次にアプリケーションを開いたときに Gatekeeper が同じ動作を繰り返すことはありません。

XProtect と MRT による脅威のブロック

Gatekeeper には、XProtect と Malware Removal Tool (MRT) と呼ばれる Apple の署名ベース検出メカニズムなど、さまざまなテクノロジーが使われています。こうしたテクノロジーを組み合わせることで、オペレーティングシステム上のファイルをスキャンしたり、既知のマルウェアと関連しているファイルにある特徴を見つけます。XProtect がアプリケーションの起動時にトリガーされるのに対して、MRT は定期的にファイルシステムをスキャンします。

XProtect は Yara と呼ばれるバイナリ署名スキャンエンジンを使って動作します。Yara は柔軟性が高く強力なバイナリ署名定義と効率的な実行エンジンをサポートしています。アプリケーションの信頼性を検証するために、XProtect は初回起動時にのみ実行可能な各ダウンロードファイルをスキャンします。一致する署名が検出されるとプログラムの実行は許可されません。既知の不正な署名が含まれるファイルは、Apple から macOS 用の個別の更新プログラムとして提供されます。Apple では、Yara 実行エンジン自体とは別に、適切と思われる署名の定義と配信を行っています。Gatekeeper 同様、アプリケーションの最初の実行が成功した後に更新された適切な隔離拡張属性をアプリケーションが保持している場合にのみこのスキャンが実行されます。

一方、MRT はプログラムの実行時ではなくあらかじめ設定されたスケジュールに沿って実行され、過去のマルウェアと関連がある特定のファイル名や中間ファイルを見つけるためにファイルシステムをスキャンして、こうしたファイルが検出された場合には削除します。この機能の主な目的は、世間で使われている macOS ですでに実行されている可能性がある既知の脅威を検出して修復することです。

Gatekeeper の企業での利用

Gatekeeper 自体は本来の役割を十分に果たしています。Gatekeeper は信頼されていないアプリケーションの起動をブロックして、疑わしい、または悪意のあるアプリケーションを検出するとユーザに通知します。IT 担当者や情報セキュリティ担当者は社内アセット上で信頼されていないソフトウェアが実行されようとしていないかを把握する必要があります。また、ユーザが企業のセキュリティコントロールをうまく回避して、右クリックメニューからアプリケーションを起動するようなケースも把握しなければなりません。企業のこうしたニーズに応えるために、Mac 専用エンドポイントセキュリティソリューションである Jamf Protect では、Gatekeeper のアクションの兆候を監視して、結果を一元管理することで、IT 部門とセキュリティ部門がリスクを正確に評価して情報に基づいた意思決定をできるようにします。

Jamf Protect では、Gatekeeper のアクティビティ



が把握できるだけでなく、企業環境において信頼されていない追加の署名情報を登録することで、企業が開発者の信頼モデルを管理できるようにします。Apple の最新のエンドポイントセキュリティフレームワークを利用することで、Jamf Protect は企業が設定したブロックリストに載っているアプリケーションの実行を先回りしてブロックします。ブロックリストはアプリケーションレベル（アプリケーション ID）でもベンダーレベル（開発者チーム ID）でも定義できます。macOS には、好ましくない行動や侵入を試みる行動を起こす数多くのアドウェアや暗号通貨マイニングアプリケーションなど、さまざまなグレイウェア（望ましくない、または許可されていないソフトウェア）の署名やブロック機能が用意されていません。多くの場合、こうしたプログラムは Apple の開発者によって合法的に署名されており、ユーザは通常、気付かないままインストール時に情報収集やリソース使用の許可に同意しています。そのため、多くの場合、Apple はこうしたアプリケーションの動作を妨げません。

しかし、企業によってリスク評価方法も異なっているため、より厳格での絞ったアプローチが必要になります。そのため、Jamf Protect では独自に管理する Yara ルールやバイナリ署名、信頼されていない開発者の証明書を充実させて、隔離拡張属性の有無にかかわらず実行時のプロセスのスキャンに使用しています。これにより、新しい署名が追加されて企業がセキュリティ体制を更新したときに、既存のアプリケーションは、初回だけでなく、その次の実行時にも再スキャンされます。



Jamf では、macOS を標的にした脅威に関する広範な独自調査と、サードパーティから提供された Mac の脅威に関する情報を元に、Mac を標的にした既知のマルウェアに関する情報を選別します。自社環境内で実行するソフトウェアをより細かく制御したい場合は、バイナリハッシュやチーム ID などのリストを Jamf Protect がブロックするアプリケーションのリストに加えて拡張することができます。macOS 10.15 (Catalina) 以降の既知のマルウェアの挙動や署名と一致するアプリケーションが実行されると、Jamf Protect によってプ

ロセスの実行が阻止されて、問題を起こしているファイルを隔離し、マルウェアが阻止されたことを示すアラートが登録されます。この操作は Gatekeeper/XProtect のアクションとは別に実行され、Gatekeeper/XProtect の機能のスーパーセットとして設計されています。Jamf Protect は、安全ではない可能性があるバイナリを特定する隔離ビットを使わずに既知のマルウェアを検出し、マルウェアに関する幅広い知識を保持します。



Self Service によって App Store の信頼モデルを拡張

IT 部門が承認したリソースがあらかじめ用意されたセルフサービス型のアプリカタログを活用して、ユーザがインストールできるプログラムを用意するのが適切な場合もあります。

Jamf Self Service では、IT ヘルプチケットを登録しなくてもユーザが App のインストール、構成の更新、よくある問題のトラブルシューティングを自分で実行できる独自の企業用アプリカタログを IT 部門が作成できるようにすることで、安全でスピーディーなリソースへのアクセスを実現します。

アプリケーションの動作の制御と監視

アプリケーションの動作を制限および許可するためのプライバシーコントロール

macOS Mojave ではシステムのプライバシーコントロールが導入されました。プライバシーコントロールでは、ユーザ（または企業）がアプリケーションごとに特定の操作やフォルダへのアクセスを許可する必要があります。特定の操作を実行する権限が一度アプリケーションに付与されると、今後同じアプリケーションがその操作を実行するときに許可を求められなくなります。この機能により、OS の機密性が高い部分（ウェブカメラ、マイク、キーボード入力、ダウンロードしたファイル）にアプリケーションがアクセスする際に明示的な許可を求めることでユーザを思いとどまらせ、プライベートなデータへのアクセス権をアプリケーションに付与しようとしていることを気付かせることができます。

制御を強化してアプリケーションの監査と分析を実現

プライバシーコントロールによってアプリケーションが実行可能なことを制限できますが、ユーザは間違いを犯したり、認証が悪用されることがあります。ここまで、Jamf Protect が Apple の組み込みのセキュリティ機能が実行する操作と、従来型のマルウェア / アドウェア防止機能の動作を可視化することにより、企業が必要な情報を得てセキュリティを確保するための方法についてご紹介してきました。しかし、Jamf は、エンドポイントセキュリティソリューションがそれだけで終わるべきではないと考えています。Jamf Protect には、従来はエンドポイント検出・対応（EDR）製品にしかない監査・監視機能も搭載されています。さらに、

Apple を第一に考えたアプローチと、macOS ユーザが求めるプライバシー標準とセキュリティ標準も組み込まれています。

Jamf Protect の検出メカニズム

Jamf Protect エージェントで中心的な役割を果たすのが、Apple 独自のロジック実行エンジンの 1 つである GameplayKit を活用した、軽量のユーザモードセンサーです（Kernel Extension を使用していません）。ゲームエンジンを使ってセキュリティイベントを分析するのは一般的ではありませんが、これを利用することで Apple エコシステムとの緊密な統合を維持しながら収集やレポートが必要になるまでデバイス上のデータを分析できるようになります。このゲームエンジンは大量のイベントをリアルタイムに処理できるようにも設計されているため、デバイスで発生したアクティビティを即座に分析するのに最適です。当初は Windows プラットフォーム専用として開発されてから macOS に移植された多くのセキュリティソリューションや、クラウドにすべての情報を集めて分析する必要があるソリューションと比べると GameplayKit には大きなメリットがあります。

Yara 同様、GameplayKit には、検出定義から実行エンジンを切り離すことで、コアエージェントを更新することなく検出の更新と拡張ができるというメリットがあります。検出定義については、Apple が開発した、従来のクエリ構文と正規表現をサポートする強力なロジッククエリメカニズムである NSPredicate を使用します。Jamf Protect のデータモデルは、ネイティブ関数の呼び出しやデータモデルの連携など、NSPredicate の豊富な機能を活用できるよう特別な設計がされています。これにより、他の従来の方法では複雑でコンピューターリソースを多く必要とする機能を利用することができます。たとえば、Jamf Protect のデータモデルと NSPredicate を使うことで次のことができます。

- ・ 痕跡を隠すためによく使用される、ファイルの自動削除が発生した場合アラートを出します。このシンプルなユースケースでは、コストのかかる結合演算やハードコーディングされた検出を使用せずに、削除されたファイルと削除を実行したプロセスを分析します。

- ・署名がない、または疑わしい署名済みバイナリが起動デーモンとして存在している場合にアラートを出します。この処理では、構成ファイルを解析し、埋め込まれたバイナリパスをコンテンツから抽出して、そのバイナリファイルのメタデータを分析に使用します。
- ・Microsoft Office アプリケーションが予期しない子プロセスを作成した場合にアラートを出して、Office マクロの悪用を検出します。これは、アプリケーション機能の悪用を発見するために子 / 親の関係を理解する能力が Jamf Protect にあることを示す例です。
- ・攻撃の兆候を示唆する方法で「環境寄生型 (Living off the Land)」アクティビティが使われている場合にアラートを出します。このタイプのアクティビティでは、一見無害にも見えるアクティビティ (curl、ssh、python など) の悪用を検出するために、子 / 親や、プロセスグループの関係性、コマンドラインパラメータにアクセスする必要があります。
- ・企業全体で USB の使用状況を追跡して、リムーバブルメディアに書き込まれるファイルのメタデータをレポートします。

こうした種類の検出の影響を簡単に理解できるようにするために、Jamf Protect は特定した攻撃を MITRE ATT&CK (TM) フレームワークにマッピングします (該当する場合)。現在、Jamf Protect では以下のカテゴリーの検出方法を含む、フレームワーク全体のユースケースに対応しています。

- ・永続化 (Persistence)
- ・初期アクセス (Initial Access)
- ・C&C (Command and Control)
- ・防御の回避 (Defense Evasion)
- ・検出 (Discovery)
- ・権限昇格 (Privilege Escalation)
- ・認証情報アクセス (Credential Access)

シンプルな統合ログの収集とレポート機能

大半のセキュリティアナリストと IT 管理者が、コンプライアンス監査の一環として、または他のセキュリティ制御のギャップを埋めるためにエンドポイントログを強く必要としています。macOS が syslog ファイルから統合ログに移行したことで、企業全体でこの情報の収集、保管、調査を行うことが難しくなりました。macOS の Console.app を使えばローカルの Mac の統合ログインフラストラクチャに簡単にアクセスして詳細を把握できますが、組織でそのデータを一元管理するのは簡単ではありません。

Jamf Protect は、統合ログに書き込まれたクライアントのログを即座にシステムにストリーミングできます。目当てのデータだけが収集されるようにするために、Jamf Protect の管理者は組み込みの `log stream` コマンドラインユーティリティと同じ述語フィルター言語 (NSPredicate) を利用します。これにより、マシンごとにデータを集めるという面倒な作業が不要になって Mac のログデータ記録システムの構成がシンプルになります。たとえば、ログインやログオフ、ssh、AirDrop、認証イベントなどに利用できます。データが統合ログに書き込まれると Jamf Protect はそれを収集することができます。

Apple の標準に準拠

リリース当日からサポート

macOS とのインタフェースやセキュリティ上の意思決定に必要なデータを収集するために、Jamf Protect では Apple のネイティブテクノロジーを活用しています。こうしたテクノロジーには、Catalina 以降に搭載されているエンタープライズセキュリティフレームワーク (ESF) や、それ以前の macOS に搭載されている OpenBSM 監査フレームワークなどの新しいフレームワークが含まれています。こうしたメカニズムを使うことで、Jamf Protect はデバイスへの影響を最小限に抑えて、パッチや OS のメジャーリリースによって導入される macOS への変更と競合しないようにしています。セキュリティ対策として一般的に最も推奨されているのが、リリースされたパッチを頻繁かつ早めに適用することです。この方法を実際に行うには、リリース当日からサポートするセキュリティツールの存在が不可欠です。

機能としてのユーザエクスペリエンス

Jamf Protect は潜在的な脅威がないか、アプリケーションとユーザのアクティビティを常に監視する一方で、休止状態にあるマルウェアや Microsoft Windows に関連するマルウェアはあえてスキャンしません。ユーザエクスペリエンスを低下させる主な要因としてよく挙げられるのが、多岐にわたるマルウェアの署名を見つけるためにファイルシステム内のファイルをスキャンすることです。Jamf Protect のこのアプローチは、実行時に脅威を検出することでユーザエクスペリエンスとユーザの生産性への影響を最小限に抑える Gatekeeper/XProtect と同様です。

プライバシー

Jamf Protect はデバイス上のデータを分析して、通常は悪意のある可能性があるアクティビティや特に注意が必要なアクティビティがリアルタイムで検出されたときなど、指定した設定に一致する場合のみ関連する情報を収集します。これによって、デバイスから取り出されてクラウドに保管されるユーザデータが少なくなるため、ユーザのプライバシーを確保しながら企業のニーズを満たすことができます。悪意のあるアクティビティが特定された場合は、特定されたアクティビティと関連データが Jamf Protect のクラウドコンソール、またはあらかじめ設定したセキュリティ情報イベント管理 (SIEM) システムに渡されます。他にも、明示的にリクエストしたデータも Jamf Protect や SIEM に送られます。不必要なデータをすべて除外することで、インシデントの監視と調査を担当しているセキュリティアナリストには本当に必要なデータだけを集めたものが表示されます。

Apple のセキュリティモデルを 拡張するためのその他の方法

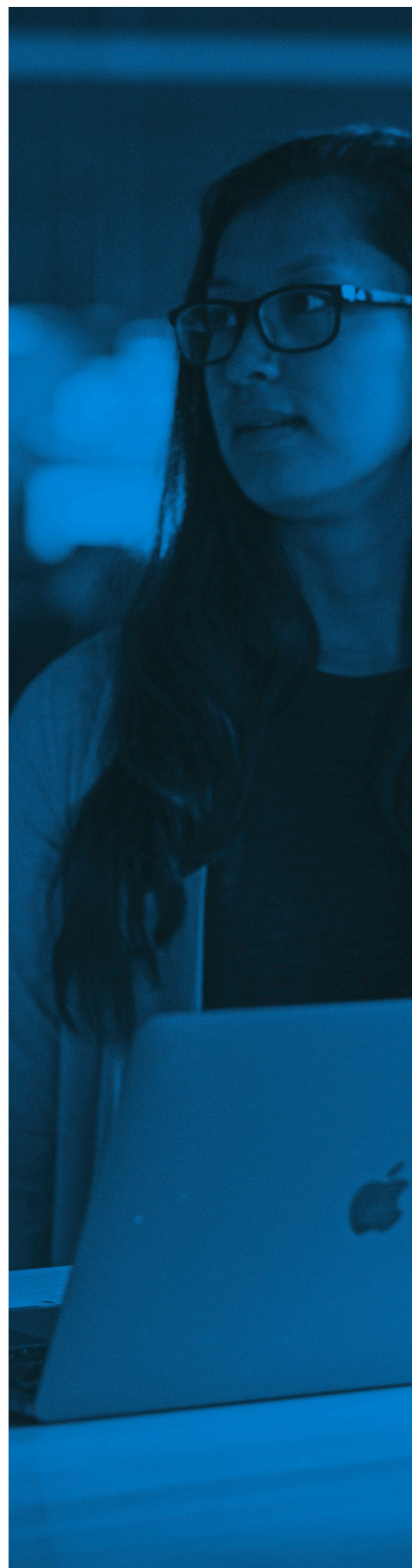
macOS のセキュリティ強化におけるベストプラクティス

Apple は最高クラスのセキュリティと信頼性を備えたオペレーティングシステムを提供してサポートしていますが、企業の環境に合う形で macOS をカスタマイズする方法に関する質問がよく挙げられます。

管理業務を大規模に自動化するには、まずは Apple のモバイルデバイス管理 (MDM) フレームワークを活用するところから始めましょう。MDM は組織を適切に保護するだけでなく、IT 部門がデバイスを管理および保護する負荷を大幅に軽減します。

OS X 10.7 (「Lion」) で導入された MDM フレームワークによって、組織固有のニーズに合わせてデバイスの機能をカスタマイズするためのさまざまなワークフローが利用できるようになりました。働く場所に関係なく従業員のセキュリティを確保するうえで、構成プロファイルと管理コマンドを使用するのが MDM の最も一般的な活用方法です。

ハードウェアの調達、管理などの自動化に役立つビジネス向け無料ソリューションである Apple Business Manager と MDM を組み合わせることで、セキュリティをさらなる高みへと押し上げることができます。



Apple が提供するセキュリティ機能

長年にわたり Apple はセキュリティを第一に考える企業としての信頼を築き上げ、macOS でそれを証明してきました。FileVault 2 暗号化や 2 ファクタ認証、リモートロック / リモートワイプ機能、そして、パスコード標準を適用する機能などのネイティブ機能は、組織の環境に新たに導入されたすべての Mac で利用できます。

Jamf Pro などの最新の管理プラットフォームでは、MDM を活用することでこうした機能をさらに一歩進めて、暗号化など有用なセキュリティツールの導入、適用、レポート機能をカスタマイズ可能なものになっています。

Jamf で組織のセキュリティを強化

MDM はあらゆる組織で威力を発揮しますが、セキュリティ体制を強化して従業員のプライバシーを高める方法が他にないものかと多くの企業が考えています。そこで Jamf の出番です。

規模がある程度大きくなると、デバイス管理に大量の人員が割かれるのは誰もが知るところです。人が多くなればハードウェアも増え、ハードウェアが増えれば IT 部門の負荷も重くなります。

少なくとも、Jamf Pro などのデバイス管理プラットフォームが登場する前までは、それが実態でした。

スマートグループなどの特許技術を有するテクノロジーにより、社内デバイスを整理して管理タスクを自動的に実行することができます。また、IT 部門がデバイス管理に費やしていた大量の時間が削減され、他の日常業務により多くの時間を使うことができます。スマートグループはデバイスのインベントリを監視して、デバイスのステータスが変わるとリアルタイムで事前定義済みグループからデバイスの追加と削除を実行します。

macOS における最新のアイデンティティ管理

最新のセキュリティの中心的な役割を果たすのが、エンドユーザを保護してアクセス権をカスタマイズするアイデンティティです。従来型の IT 部門は、名前や部門などの従業員情報を一元管理するためにローカルのディレクトリサービスを利用しています。セキュリティやデプロイメントに進化が求められるなか、企業戦略の一環としてアイデンティティに対して新しいアプローチを導入する必要があります。包括的なクラウドベースのアイデンティティソリューションを利用することで、企業はハードウェアとソフトウェアのアイデンティティを統合して眠っている機能や高度なワークフローを活用し、ビジネスの変革につなげることができます。

ディレクトリサービスの情報を活用したクラウドベースの SSO により、エンドユーザが安全な資格情報を入力して企業リソースにアクセスできるようにします。

Jamf Connect ではアイデンティティ管理におけるこうした一般的な方法をさらに拡張しています。

Jamf Connect は信頼性を損なうことなく、企業内のすべてのアプリケーション、およびユーザが使用している Mac のアイデンティティを統合します。エンドユーザは単一のクラウドアイデンティティを利用して、生産性を高めるために必要なリソースに簡単かつ素早くアクセスできます。

Jamf Connect は次のようなことを実現します。

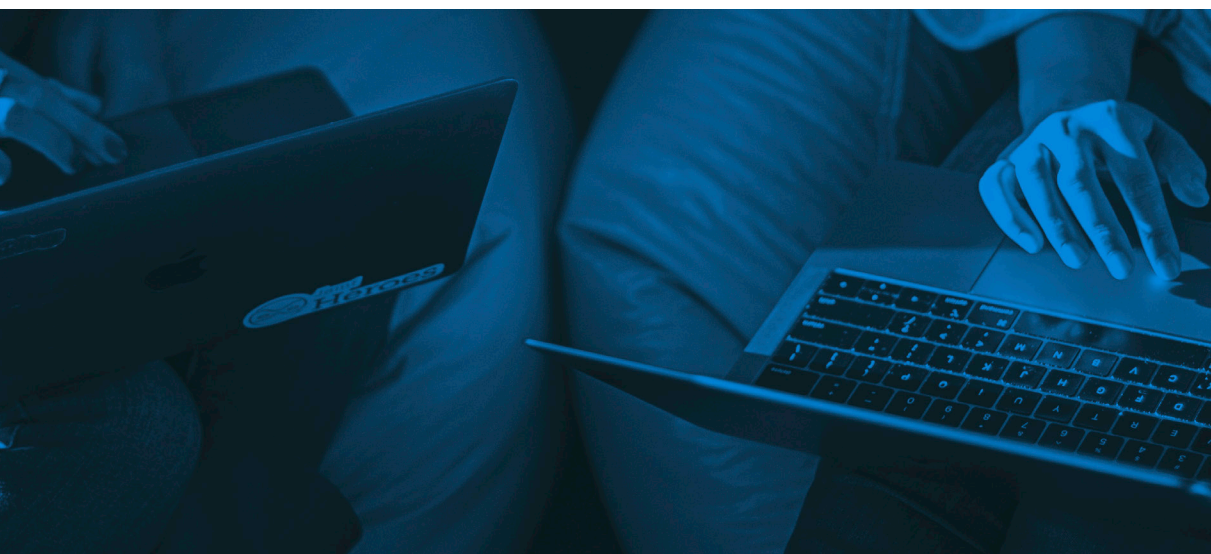
- ・ 効率化されたプロビジョニングと認証により、リモートとオンサイトの従業員をフルサポート
- ・ ユーザ ID とデバイスの資格情報を自動的に同期
- ・ IT 部門がサービスとデバイスを管理する上で必要なアイデンティティ管理機能のすべてを提供

Mac の脅威への対応と修正

Apple デバイス管理のスタンダードである Jamf Pro に用意されたダッシュボードを利用すると、Mac デバイスの状態を常に評価しながら注意が必要なハードウェアを把握できます。

特許技術を有するスマートグループ機能によって、IT 管理者は更新やパッチ適用が必要なデバイスを対象にセキュリティを強化できます。こうした作業はすべてリモートから実行可能で、自動化することもできるため、IT 担当者がデバイスを直接操作する必要がありません。

Jamf Protect と Jamf Pro を組み合わせることで、脅威への対応と修復をさらに一歩進めることができます。スマートグループの活用により、Jamf Protect から上がってくるアクティビティベースのアラート対応時に MDM と Jamf Pro のすべてのコマンドを自動化できます。これには自動化されたネットワークの分離、再イメージング、失敗した条件付きアクセス、ユーザ通知、あらかじめ設定した任意の数の対応と修正などがあります。Jamf Pro と Jamf Connect を組み合わせることで、ユーザやデバイスが攻撃を受けた時に資格情報の停止、アクセス権の変更、および ID に関するさまざまな修復が実行されます。



Mac に組み込まれた機能を強化することでもたらされるさまざまなメリット

Mac を求めるユーザが増えていることから、企業での Mac の導入も増える一方です。適切なツールを用意することで、IT 部門と情報セキュリティ部門は確実に Mac の導入を進め、セキュリティとプライバシーの基準をすべて満たした上で、必要とされているリソースとアクセス権を提供してユーザの生産性を最大限に高めることができます。

Jamf のエンタープライズソリューションを活用して、現代の組織に必要な可視性と修復機能を強化ください。

[Jamf Protect デモをリクエスト](#)