jamf

ビジネス環境におけるMacの管理とセキュリティ

働き方が大きく変化するなか、成長中の組織は柔軟に対応しながら、生産性の向上とセキュリティ強化を両立させる方法を模索しています。その鍵を握るのが、どのテクノロジーを選択し、いかに活用するかという「意思決定」に他なりません。デバイスの選択権が従業員の満足度や生産性を高めることは、数々の調査で証明されています。自身のポテンシャルを最大限に引き出すためにMacを選ぶビジネスパーソンが、これまで以上に増えています。

IT部門にとって、この変化はチャンスでもあり課題でもあります。どのようにして、ユーザが好むテクノロジーを利用できるようにしながら、シームレスな管理、最大限のセキュリティ、最小限の運用リスクを実現すればよいのでしょうか。

macOSには強固なセキュリティ機能が内蔵されていますが、現代の環境では管理、コンプライアンス、セキュリティに対してシンプルで一貫したアプローチが必要です。管理デバイス数が増加の一途をたどるなか、IT部門にとってセキュリティの確保とユーザ利便性の維持はますます困難な課題となります。macOSネイティブではないツールに頼ることで、監視体制や事後対応に限界が生じている組織は少なくありません。適切な戦略を採用すれば、ワークフローの合理化、生産性の向上、セキュリティリスクの低減を実現できるとともに、セキュリティ部門がMacデバイスに対して必要な可視性を確保し、効果的な予防対策を講じられるようになります。

jamf

本ガイドは、Macの大規模な導入・運用において、管理とセキュリティを両立させるための戦略的な指針をIT部門に提供します。主な内容は次のとおりです。

Mac管理の基本– シームレスな導入、構成、管理の基本原則

高度なセキュリティ戦略 – macOSネイティブ機能よりも広い範囲で保護することで、進化する企業リスクを軽減

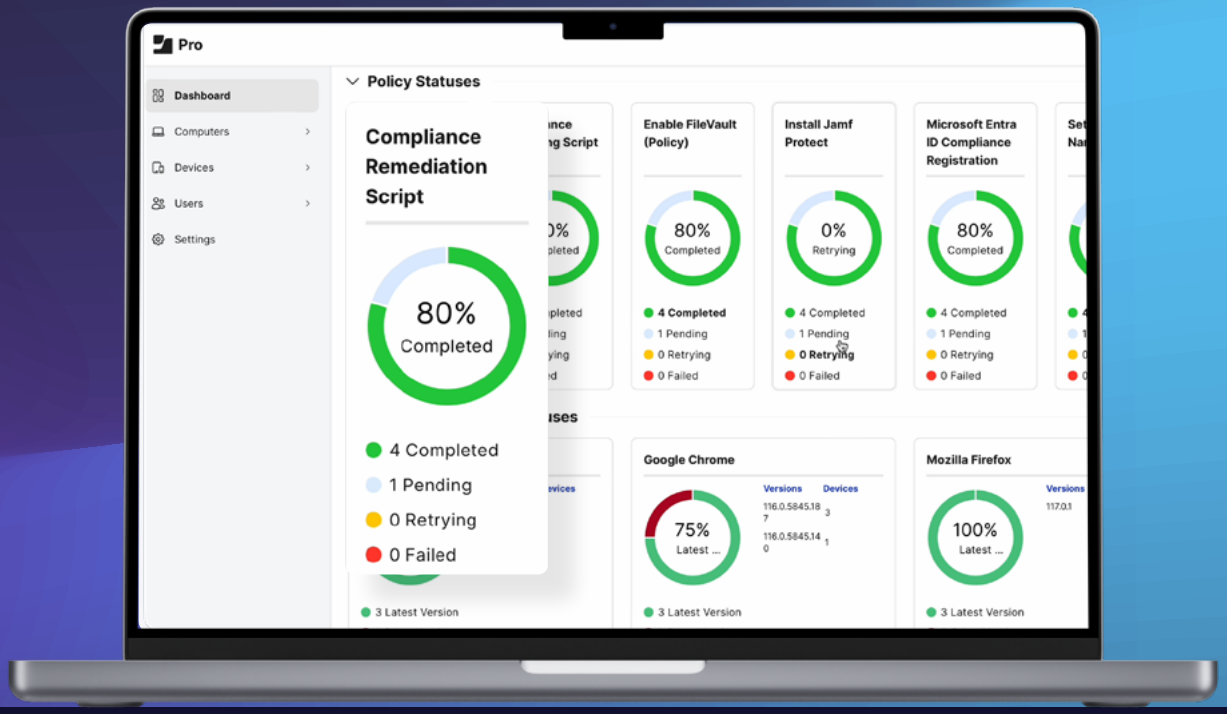
ライフサイクル管理 – ゼロタッチ導入による即戦力化から確実なデバイス回収・初期化の実現まで、Macのエクスペリエンスを最適化

インフラの統合 – Windows環境や企業のITエコシステムとのスムーズな共存を実現

エンタープライズセキュリティのベストプラクティス – Macに最適化されたツールで企業のデータ、デバイス、ユーザを保護

従来のWindows主体の組織にMacを導入する場合でも、既存のAppleデバイス環境を拡張する場合でも、ITの効率化と簡素化を進め、セキュリティを強化し、Macへの投資利益率を最大化しながら運用リスクを最小限に抑えるのに必要な情報や知見を紹介します。

最新のMac管理の概要：基本原則とテクノロジー



ビジネス環境におけるMac管理の進化

現代のビジネスシーンにおいて、Macは戦略的な基盤としての地位を確立しました。セキュリティとパフォーマンス、さらには卓越したユーザ体験を兼ね備え、企業の成長を支えます。かつては主にクリエイティブの専門職が使用するニッチな製品と考えられていましたが、今や現代のIT環境にとっては欠かせない存在です。Macの普及が進むにつれて、IT管理者はシームレスな統合とセキュリティを確保するために、より高度な管理戦略を採用するようになり、Mac管理の効率化と自動化を実現するモバイルデバイス管理（MDM）ソリューションに目を向け始めました。

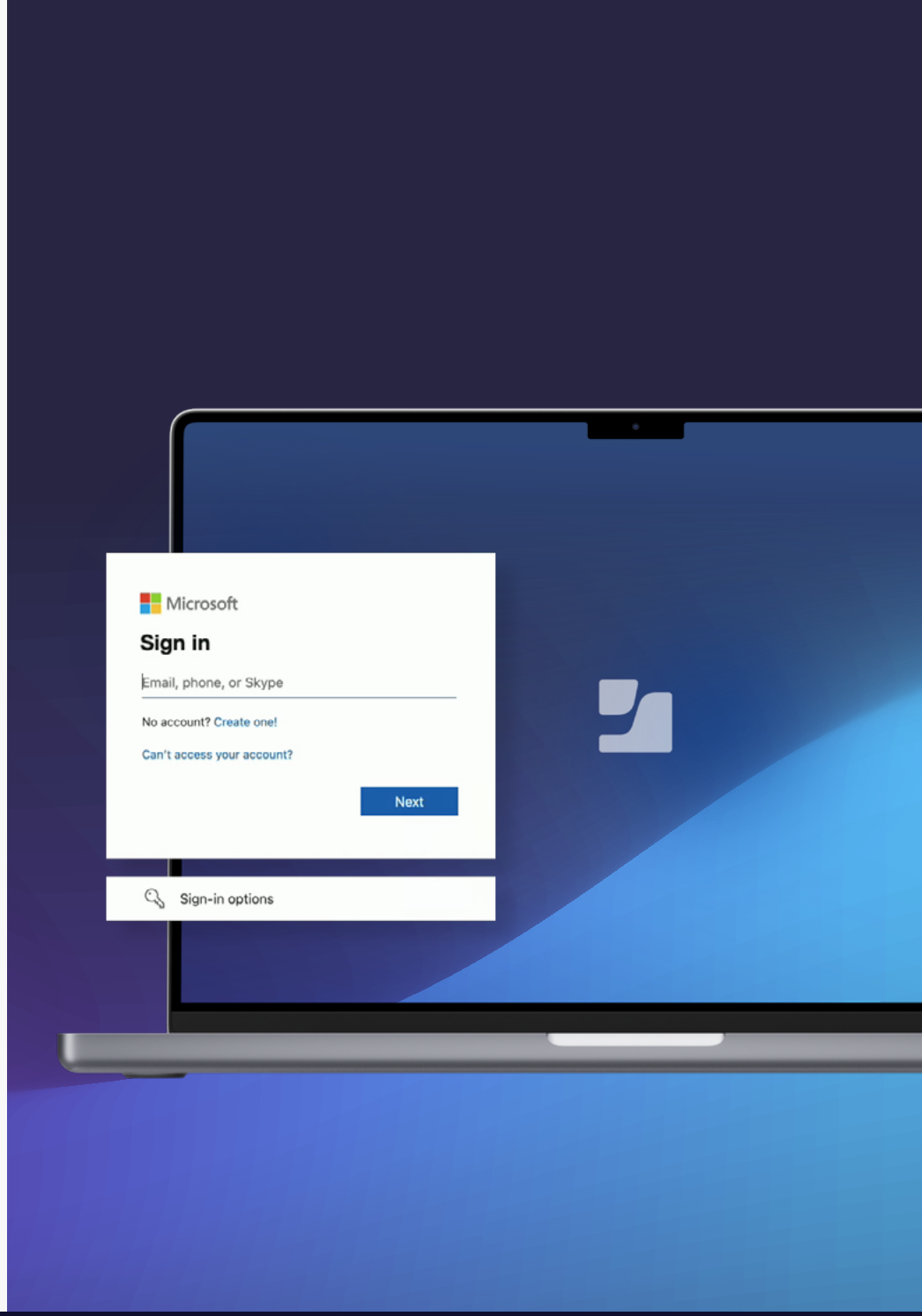
その一方で、Macの普及が進むとともに、レガシーなMDMソリューションでは対応しきれない課題が浮き彫りになっています。従来のソリューションは主にWindows向けに設計されているため、急速に進化するAppleのエコシステムに十分に適合させることが難しいのです。macOSのアップデートとのシームレスな統合、セキュリティ機能や新しい機能のリリース初日からのサポート、Appleネイティブのワークフローとの互換性を確保することが課題となり、それらにはAppleに特化したソリューションを使用することでしか実現できない、的を絞ったアプローチが求められます。

このような課題からは、IT部門が2つのプラットフォームのシームレスな統合、効率的な拡張、セキュリティの強化を実現しながら、違和感のないユーザエクスペリエンスを維持できる最新の管理ソリューションを必要としている理由がうかがえます。Windowsベースの管理手法に熟知しているITエンジニアにとって、Macの管理は一見異質に思えるかもしれません。しかし、Mac本来の生産性を損なうことなくセキュリティを最大化するためには、macOSに最適化された手法を取り入れることが最善の道です。組織では、Windows主体の戦略からの脱却が進むにつれて、Macが効率性と従業員満足度を高める推進力となるという認識が広がっています。これらのメリットを最大限に引き出すには、成長する組織のニーズに対応できるよう設計された、プロアクティブで拡張性に優れたAppleネイティブの管理戦略を採用することがIT部門に求められます。

Mac管理を効果的に行うには、以下のような主要なビジネス目標に沿ったものであることが必要です。

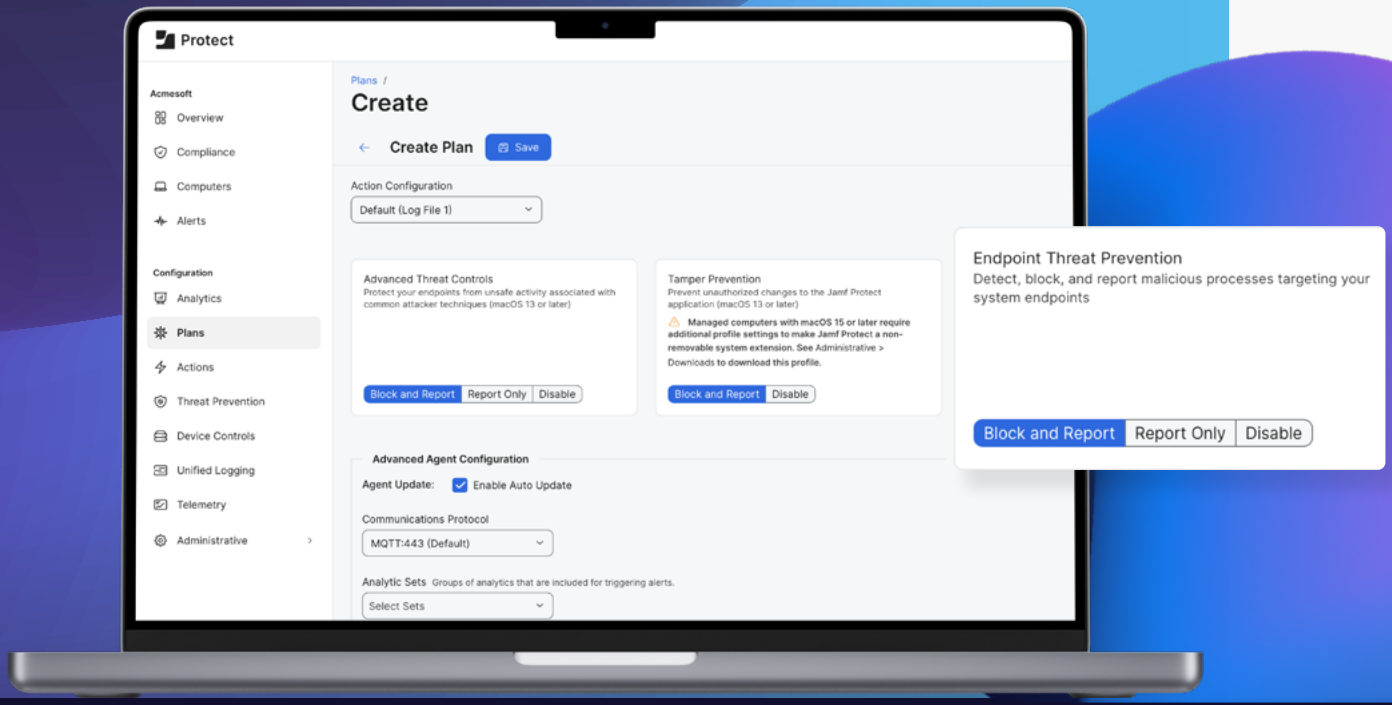
- **生産性の向上：**デバイスのセットアップ、アップデート、サポートを効率化することで、ダウンタイムを削減し、従業員が効率的に働ける体制を整える。
- **リスクの軽減：**エンドポイントを常時監視し、セキュリティポリシーを活用してコンプライアンスを維持し、修復タスクを自動化することで、企業・組織に対する脅威を最小限に抑える。

このような原則が念頭に置かれた最新のMac管理戦略は、AppleのMDMとセキュリティのフレームワークを中心に策定されており、組織の成長に合わせてMacデバイスの導入、保護、保守を行うための体系的なアプローチが採用されています。



Mac管理の基本：**成長する組織のための戦略的アプローチ**

IT部門は、以下の基本原則を採用することで、Macのシームレスな導入、構成、管理を実現し、従業員が求めるユーザエクスペリエンスを保ちながら、ユーザのプライバシーを損なうことなく強固なセキュリティを維持できます。



ゼロタッチ導入：自動化で拡張性を向上

効率、セキュリティ、ユーザ満足度を高めるには、合理的なオンボーディングプロセスが欠かせません。ゼロタッチ導入を採用すれば、IT部門はデバイスが開梱される前にMacの構成と初期設定を行えるため、手作業のセットアップが不要になり、IT部門の負担を軽減できます。このようなメリットは以下の要素で実現できます。

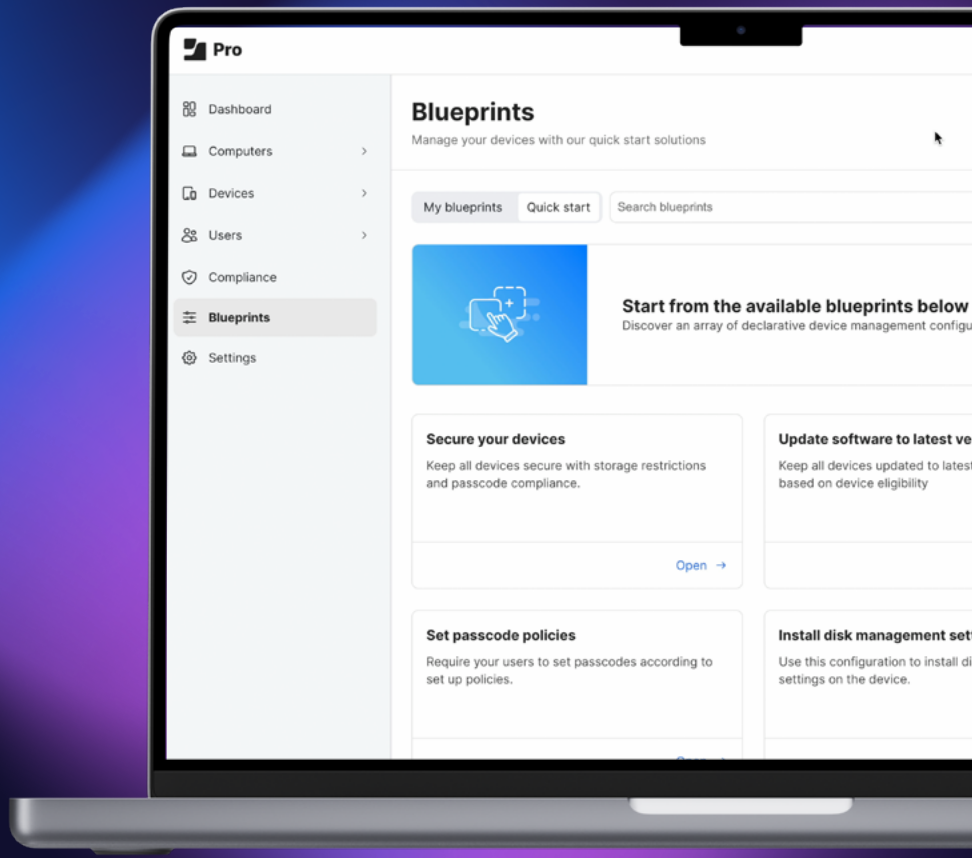
- **自動登録とカスタマイズ**
- **アカウントのプロビジョニングと管理**
- **ジャストインタイムのmacOSオンボーディング**

IT部門は自動化を活用することで、従業員のオンボーディング時間を短縮し、デバイスの電源を初めて入れたときからセキュリティを強化できます。影響力の大きいIT業務に時間を割きつつ、すぐに生産性向上につながる理想的なオンボーディングエクスペリエンスを実現できます。

設定と構成の一元化：大規模環境で一貫性を維持

増加するMacデバイス全体でセキュリティとコンプライアンスを確保するには、ポリシーを使用した一元的アプローチが必要です。IT部門には、ビジネスニーズをサポートしながら一貫性を維持する構成を確立して適用することが求められます。これを実現する手段には次のようなものがあります。

- **ブループリント**
- **スマートグループ**
- **リモートセキュリティコマンドと制限**
- **Apple Business Manager（ABM）との統合**



アプリケーションとパッチ管理：リスクの軽減と生産性の向上

ソフトウェアの導入とパッチの管理を標準化することで、IT部門はセキュリティの脆弱性を軽減し、ダウンタイムを最小限に抑えながら、ユーザの生産性向上に寄与する新しい機能をサポートできます。ユーザがアプリを最大限に活用できるよう支援する機能には以下のようなものがあります。

- **アプリの自動導入**
- **パッチの適用**
- **App カタログ**
- **コンテンツとデバイスのオンデマンドセキュリティ**

セキュリティとコンプライアンスの基本：重要な資産を保護

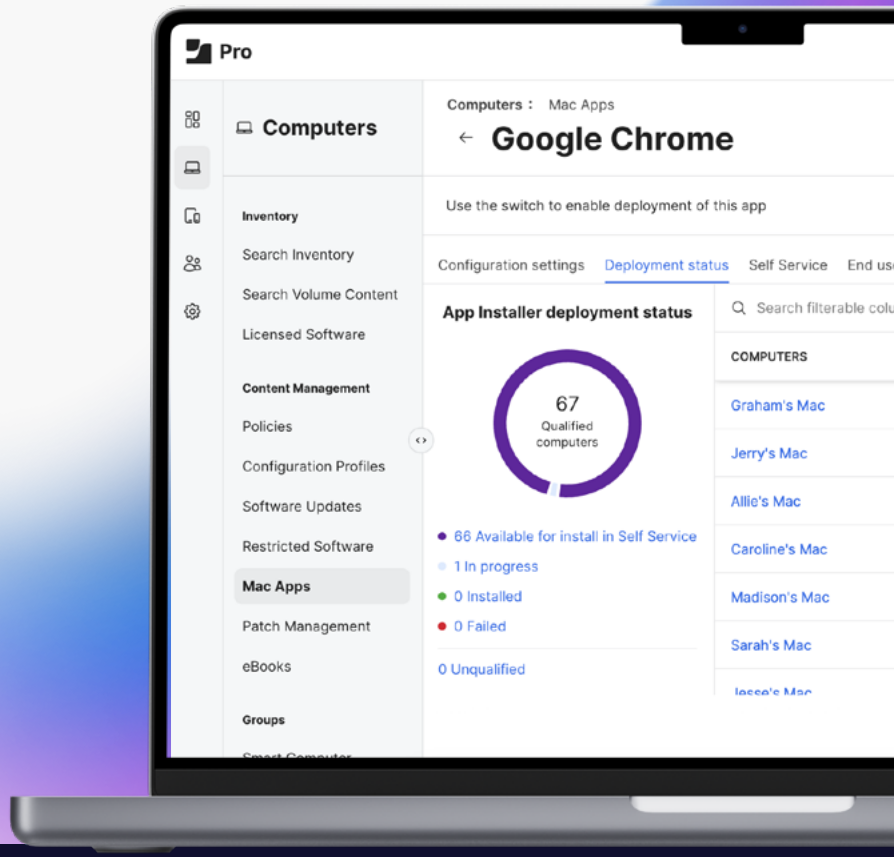
macOSには強力なセキュリティとプライバシーの機能が搭載されていますが、組織のセキュリティ基準や必須のコンプライアンス要件を満たすためには、追加の保護対策が必要です。最新のMacセキュリティ戦略には、以下の機能が含まれています。

- **エンドポイントセキュリティとコンプライアンス**
- **アイデンティティベースのアクセス管理（IAM）**
- **脅威検出とインシデント対応**
- **ネットワークベースの脅威対策**
- **ゼロトラストネットワークアクセス（ZTNA）**

レポートと可視性

調達から廃棄までMacのライフサイクル全体を管理することで、長期的なコスト削減と運用効率の向上を実現できます。また、機器の紛失によるデータ漏洩リスクの軽減にもつながります。このようなメリットは以下の要素で実現できます。

- **インベントリ管理**
- **App レポート**
- **スマートターゲティング**



ビジネス面のメリット：**IT部門が移行を主導すべき理由**

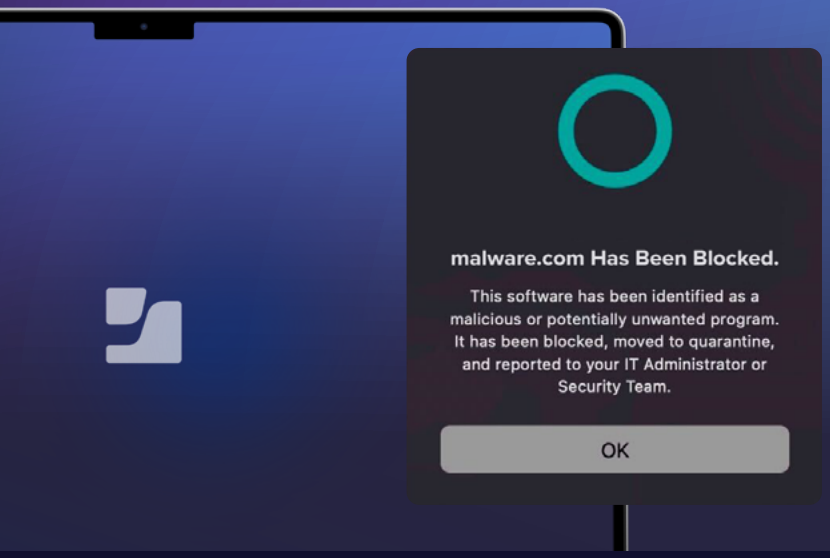
職場におけるMacの普及は、IT部門にとって管理戦略を捉え直す絶好の機会です。Appleネイティブの予防型・自動化アプローチを採用すれば、以下のことを実現できます。

- セキュリティを強化し、コンプライアンスを確保しながら、複雑さを最小限に抑える。
- Macエクスペリエンスを損なうことなく、シームレスなワークフローを通じてユーザの生産性を向上させる。
- 運用の自動化と効率化を通じてIT部門の負荷を軽減する。

このようなMac管理の基本原則を採用することで、IT部門はMacの導入を戦略上の強みへ変革することができ、組織は以下のような付加価値を得られるようになります。

- 事業運営をサポートしながら、効率とセキュリティを向上させる。
- 他のハードウェアベンダーに比べて総所有コスト（TCO）を大きく削減できる。
- 組織の成長に合わせてMacを管理・保護することで投資利益率（ROI）を向上 させる。

高度なセキュリティ戦略：**macOSネイティブ機能よりも広い範囲で保護することで、組織の リスクを軽減**



Mac管理における セキュリティの重要性

組織全体でMacの導入が進むにつれて、多拠点・多様化する従業員の管理に伴うセキュリティの課題も増えています。macOSには強力な保護機能が内蔵されていますが、特にMacを狙う脅威アクターが増えている今は、組織のデータを保護するのにデフォルトのセキュリティ対策に頼るだけでは不十分です。IT部門は以下の要素のある包括的なセキュリティアプローチを採用することでニーズを満たすことができます。

- **エンドポイントセキュリティ**
- **アイデンティティベースのアクセス管理**
- **ベースラインセキュリティ構成**
- **アクティブな監視とレポート**
- **コンプライアンスの徹底**

組織はパッチ適用の自動化、ゼロトラストフレームワーク、リアルタイムの脅威検出でMacを予防的に保護することで、リスクを軽減し、コンプライアンス要件を遵守し、企業リソースを保護することができます。セキュリティ戦略の明確な定義は、IT部門の優先事項であるだけでなく、セキュリティ状態を強化し、事業継続性を支える基盤を構築するうえで欠かせない要素なのです。

デバイスライフサイクル管理：死角のないセキュリティ

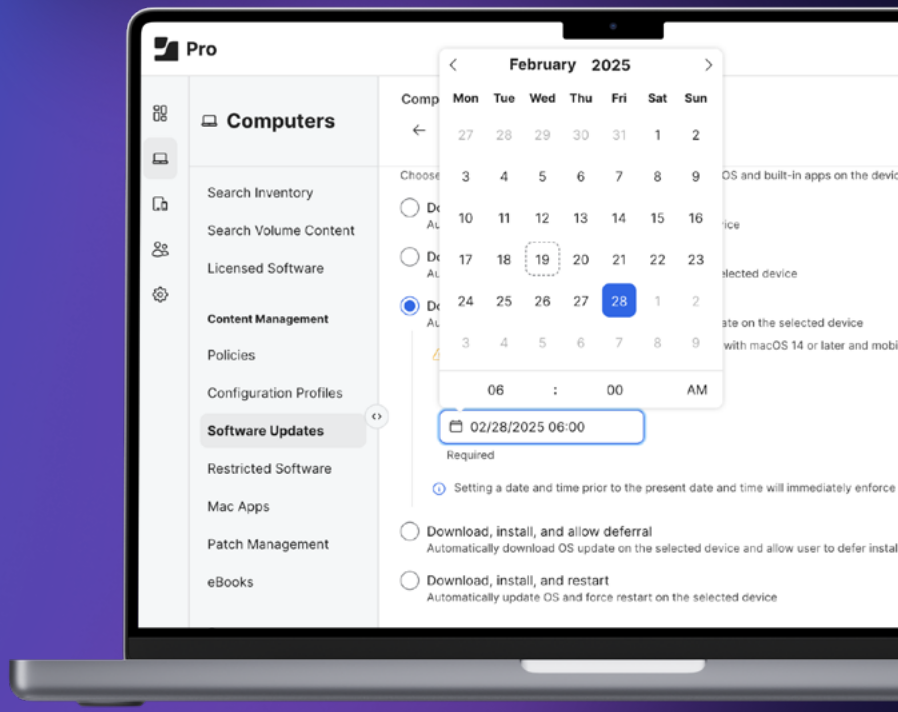
効果的なセキュリティを実現するには、組織のリソースに及ぼすリスクの観点から、リソースに接続するすべての業務デバイスを同等に扱う必要があります。その際に鍵となるのは、デバイスのライフサイクル全体にわたる一貫性です。調達からオンボーディング、構成の展開、コンプライアンスの監視、継続的なパッチ管理、次のデバイスのライフサイクルが始まる廃棄に至るまで、セキュリティにギャップが生じないようにすることが重要です。一貫性を保つこと、IT部門は以下のようなメリットを達成できます。

- **組織全体へのセキュリティの展開**
- **制御のバラつきの回避**
- **ワークフローの保護**
- **継続的なデバイス認証**

セキュリティ状態のベースラインの確立

事業の正常な運営レベルのボーダーラインを引くことで、検証された責任分界点を設定できます。さらに、IT部門は、デバイス自体と、保護対象のデータタイプをデバイスで扱う従業員とを、データの保護方法を定めた社内ポリシーや外部の要件に確実に準拠させることが求められる場合があります。コンプライアンスの確保は以下の要素で実現できます。

- **標準やフレームワークへの準拠**
- **コンプライアンスレポートの生成**
- **リアルタイムの通知**
- **ポリシーベースの適用**



AI/MLによる脅威防御とデバイス上のセキュリティ

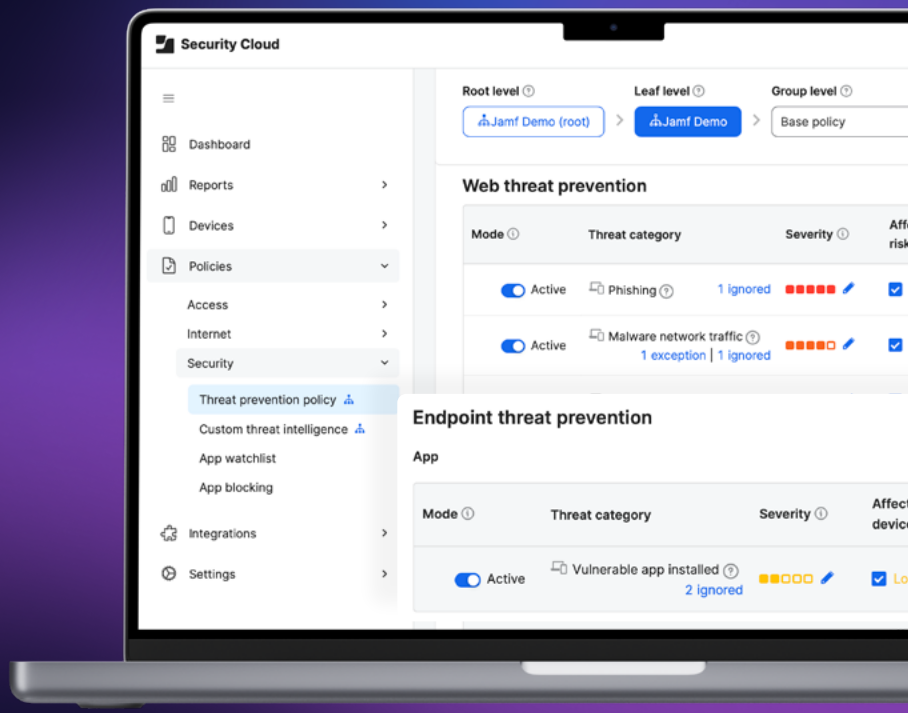
脅威アクターは絶えず戦術を進化させており、IT部門が先手を打つことは容易ではありません。AIと機械学習を活用したリアルタイム分析を利用すれば、異常な動作を特定し、既知や未知の脅威を防御し、ユーザの生産性に影響が出る前に悪意のあるアクティビティをブロックできます。また、EDRツールを使用すれば、脅威の調査と対応に役立つ可視性が得られ、IT部門は発生した問題を把握し、素早い是正措置を講じやすくなります。

- **リアルタイムの脅威検出**
- **AI/MLを活用した防御**
- **デバイス上の保護対策**
- **調査に役立つ可視性**

ゼロトラストの原則

たった1台のデバイスが侵害されただけでリスクが発生することは多くの組織が理解しています。ゼロトラストは、アイデンティティ、デバイスの健全性、アクセスの意図を継続的に検証することでセキュリティを強化するアプローチです。ゼロトラストを採用すれば、コンテキストに基づいたアクセス権の適用が可能になり、ネットワーク上でもリモートでも、信頼性が確認されたユーザとデバイスのみに機密情報へのアクセスを許可できます。

- **アイデンティティとデバイスの継続的なチェック**
- **コンテキストベースのアクセス**
- **ネットワーク内外を問わないデータ保護**
- **攻撃対象領域の縮小**



コンプライアンスの適用：ITの安全性の確保

組織は事業運営を組織の標準や業界の規制に適合させながら行うことで、デバイス、データ、ユーザ、プロセス、ワークフローが安全性維持のために確立された指針に準拠しているという確証を得ることができます。IT部門はコンプライアンスを徹底することで、エンドポイントが適切に構成され、セキュリティ対策が確立されていることを示す価値ある証拠を手にできます。具体的には以下のようなものがあります。

- **構成の堅牢化**
- **セキュリティの分析**
- **ベースラインの確立**
- **コンプライアンスのレポート**

緊密な統合によるソリューションの強化

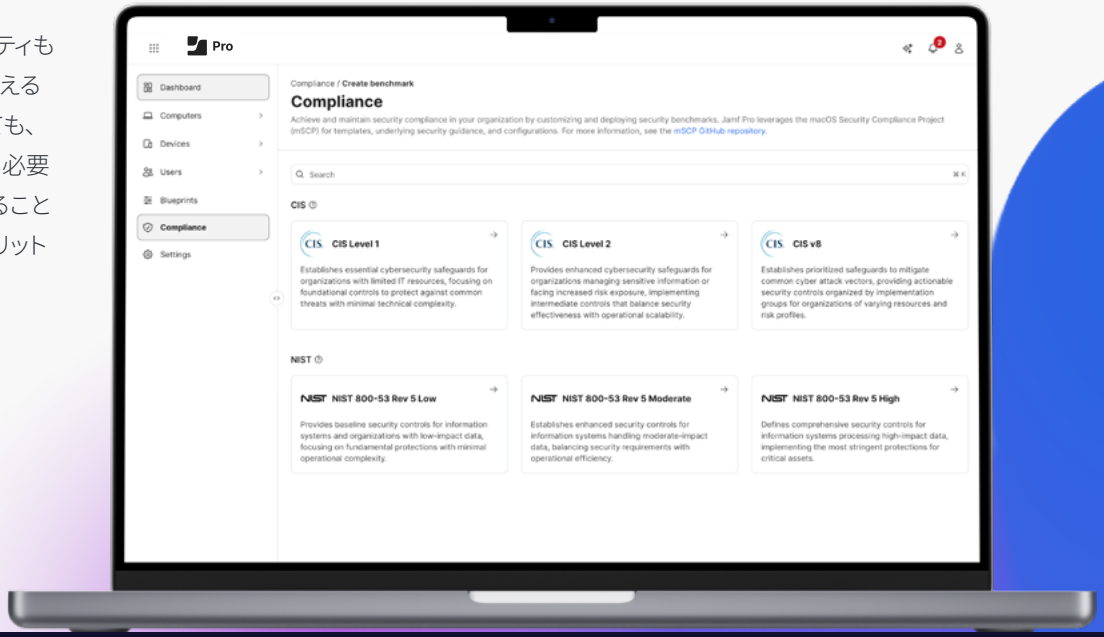
意思決定が孤立無援の状態で下されることはほとんどありません。セキュリティも同様です。OSの機能をネイティブにサポートしながら今日の企業に影響を与える多様な脅威を阻止することは、それがどんなに強力なソリューションであっても、単独では不十分です。それぞれのニーズに対応するソリューションがどちらも必要であり、企業独自のニーズを満たすために追加のソリューションが必要になることも少なくありません。ソリューションの統合によって組織が得られる大きなメリットには、以下のものがあります。

- **脅威分析の一元化**
- **脆弱性修復の自動化**
- **条件付きアクセスの実装**
- **サポートワークフローのカスタマイズ**

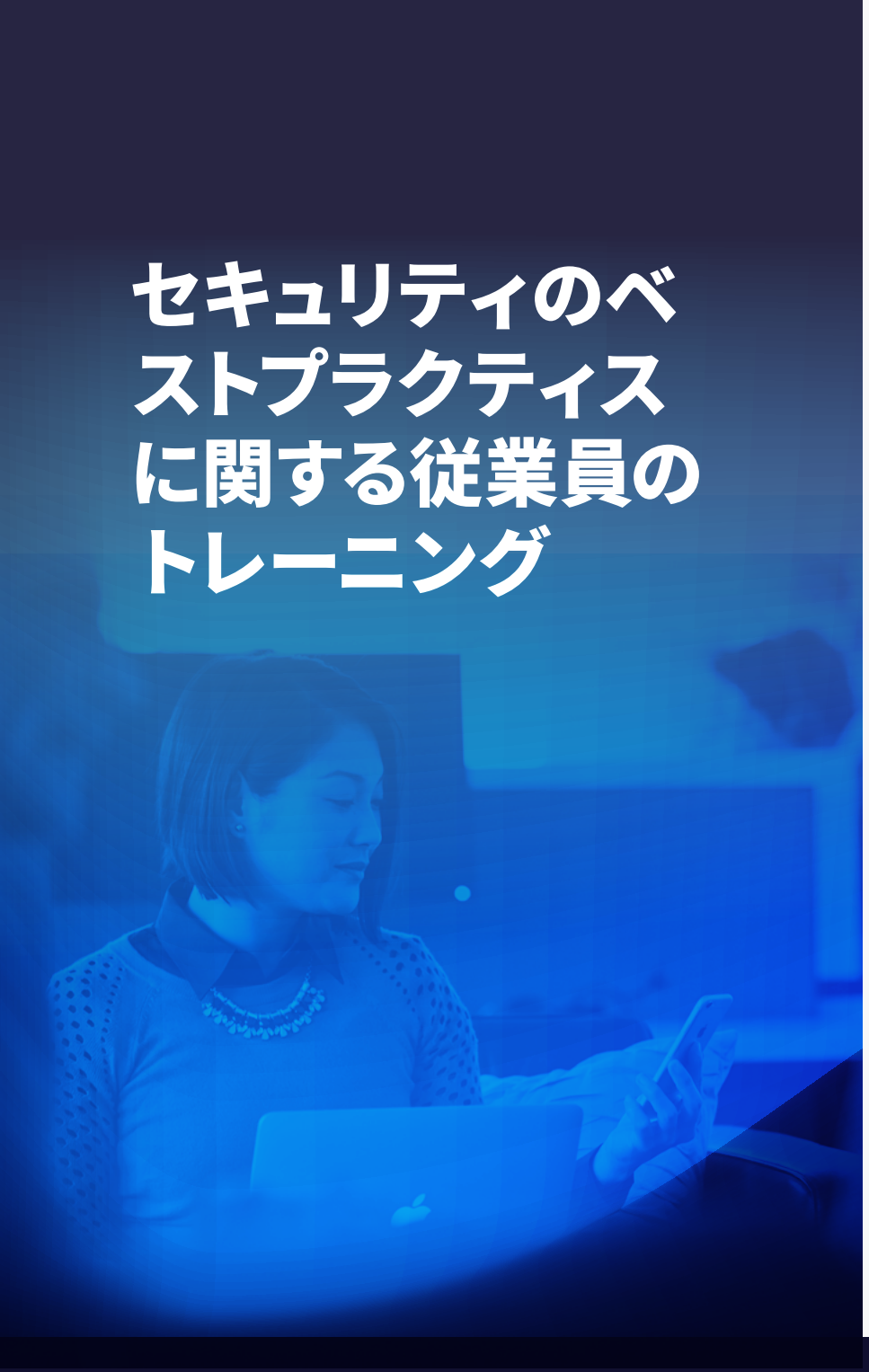
インシデント対応時間の短縮 + 脅威ハンティング = リスクの低減

セキュリティ戦略に完全無欠はありえず、脅威の侵入を許してしまうこともあります。そのような状況では、時間がきわめて重要です。時間こそが、リスクを軽減できるかデータが漏洩するかの分かれ目を決定するからです。包括的なセキュリティ計画にインシデント対応と脅威ハンティングの戦略を組み込むことで、既知のリスクを最小限に抑え、従来のエンドポイントセキュリティソリューションをすり抜けるおそれのある未知の脅威を検出できます。インシデント対応とハンティングを加速させる主な戦略には、以下のようなものがあります。

- **セキュリティベースラインの確立**
- **テレメトリデータの安全な共有**
- **トリアージと対応の自動化**
- **AI/MLテクノロジーの統合**



セキュリティのベストプラクティスに関する従業員のトレーニング



個々の対策・構成・ポリシーは、もっと大きなセキュリティというパズルのピースであることをIT部門は理解しています。パズルは企業ごとに異なり、各対策は企業の要件やリスク評価のニーズに合わせてカスタマイズされます。

多層防御戦略に不可欠な対策の1つであり、セキュリティというより管理のために行われるのが、エンドユーザトレーニングです。ユーザはセキュリティチェーンにおける脆弱性と見なされることが少なくありませんが、強力な第一防衛ラインにもなり得ます。適切なトレーニングと意識の向上を図ることで、ユーザをセキュリティ環境の強さと回復力を高める重要な要素に変えることができます。さらに、脅威が企業の防御を突破した場合でも、包括的なセキュリティ計画とセキュリティ意識向上トレーニングを組み合わせていれば、何をすべきか、何をすべきでないかを理解している従業員が断固たる行動をとることで、組織は脅威を迅速に軽減できるようになります。

IT部門はエンドユーザを対象としたセキュリティ意識向上トレーニングでセキュリティ計画を強化することで、組織の管理とセキュリティのあらゆる要素に浸透するセキュリティの文化を創造できます。このような文化があれば、特定のタイプの攻撃を未然に防ぐうえで大きな効果を発揮します。必要なのは、以下の方法を通じてユーザを強化するトレーニングだけです。

- **最新の脅威に関する情報を提供する**
- **セキュリティ対策を積極的に改善する**
- **定期的なバックアップとデータ保護を推奨する**
- **ユーザ向けのセキュリティポリシーとガイドラインを確立する**
- **インシデント対応の改善など、ユーザをソリューションの一部として組み込む**

まとめと次のステップ

Macの管理やセキュリティと同様に、IT部門の役割も進化しています。絶えず変化する状況に合わせて戦略を最適化するには、リスクに対する鋭い洞察と深い理解が欠かせません。リスクは常に変化していることを理解したうえで、macOSに特化したネイティブテクノロジーを活用して初めて、業務用Macデバイスの管理とセキュリティに最も効果的なソリューションを構築できます。

それは、組織固有のニーズや要件はもちろん、デバイス、データ、関係者のニーズや要件を、単に最低限クリアするのではなく、その上をいくソリューションなのです。

Macの管理とセキュリティに関する重要なヒントのまとめ

本書で述べたとおり、企業・組織のセキュリティ上の脆弱性を効果的に解消するためには、最新のサイバーセキュリティアプローチが必要です。管理と包括的なセキュリティ対策を重層的に展開し、インフラ全体を通じてMacデバイス、ユーザ、データの保護とプライバシーを実現することが求められます。管理、ID管理、そしてセキュリティ。これらを統合したパワフルな「多層防御」ソリューションが、組織の拡大に伴うセキュリティ基盤の強化を支えます。

Macの効果的な管理とセキュリティの鍵となるのは、以下の要素です。

- デバイスのライフサイクル全体を網羅する包括的な戦略を策定する
- 管理、アイデンティティ、セキュリティの各ソリューションを統合し、管理とセキュリティの包括的なワークフローを自動化する
- ゼロタッチ導入でデバイスオンボーディングを自動化して拡張性を高める
- 標準やフレームワークに準拠したセキュアな構成のベースラインを確立する
- アプリの導入とパッチ管理のサイクルを標準化する
- エンドポイントセキュリティとZTNAで、デバイス上とネットワークベースの脅威を阻止する
- リアルタイムの可視性でエンドポイントの健全性を監視し、既知の脅威を阻止する
- 自動化されたポリシーベースの管理ワークフローでコンプライアンスを確保する
- 共有テレメトリを活用してデータに基づいた意思決定を下し、リスクを最小限に抑える
- AI/MLベースの高度なテクノロジーと自動化で、未知の脅威を特定し、インシデント対応の時間を短縮して、脆弱性を軽減・修復する
- ユーザのセキュリティ意識向上トレーニングを、問題の原因追求ではなく、包括的なソリューションの一部として活用する

ITの効率を最大限に高め、
Macの管理とセキュリティをシンプルに。

トライアルに申し込む