jamf

Mac管理における最重要セキュリティ対策

はじめに

米国の大企業では働き方の変化、セキュリティニーズの高まり、デバイスの従業員選択制の普及を受けて**Macの採用**が広がっており、導入率が76%増加しました。Computerworldが紹介した調査によれば、「IT専門家の10人中9人が職場でのMac、iPhone、iPadの利用にはビジネス面のメリットがあると評価」しています。この結果は、従業員にも組織にも喜ばしいものです。従業員にとっては、テクノロジーの選択肢が広がるため、最も使いやすいハードウェア/ソフトウェアを利用して生産性を高めやすくなります。

IT部門やセキュリティ部門の観点では、変化というものは、放置するとリスクにつながりかねない要素を生み出すものです。しかし企業にとって幸いなことに、macOS特有のリスクには対処法があります。それは、プロアクティブかつ多層的な戦略でモバイルデバイス管理（MDM）ソリューション、ID・アクセス管理ソリューション、エンドポイントソリューションのすべてを導入し、インフラストラクチャ全体にわたりデバイス、データ、ユーザを進化する脅威から保護することです（詳細は次セクションで解説します）。

複数のソリューションを統合することで、きめ細かなセキュリティ対策を実践し、必要十分なエンドポイントの健全性を確保できます。これによりコンプライアンスを強化し、従業員の生産性を損なうことなくIT部門の手間を減らして、業務に役立つワークフローの開発にかける時間を増やすことができます。本資料では、以下をはじめとする重要なセキュリティ対策について解説します。

- パッチとアップデートの管理
- 脅威検出とインシデント対応
- データの保護と暗号化
- ネットワークとアプリケーションのセキュリティ

Macの管理とセキュリティの土台

重要なセキュリティ対策を見る前に、Macの管理プロセスおよびワークフローを支える土台が強固であることの重要性について理解しておきましょう。例えば、あるソリューションが拡張性に優れていても、最新パッチにリリース初日に対応できない場合、デバイスと組織両方のセキュリティに穴が開くおそれがあります。この理由は主に、最新macOSに対するサポートを開発者がすぐに実装できないか、重要な機能に対するサポートに制限があることです。

モバイルデバイス管理（MDM）

2024年に、macOSはOSごとのCVE（共通脆弱性識別子）検出数ランキングで上位50種中9位（個別の脆弱性508件）となり、注目を集めました。2025年5月時点では、macOSで検出された**個別の脆弱性は243件**（2024年の約半分）に達し、同ランキングで上位10種中2位に浮上しています。ただし、このランキングは年が経つにつれて変動する可能性があり、時期によってCVE数と順位が変化する場合があることに注意してください。

上記の調査結果を見れば、デバイスのOSとアプリを最新の状態に保つことの重要性は明らかです。宣言型デバイス管理（DDM）のような最新の機能を使用すれば、デバイスに設定を自律的に適用させ、状態の変化をリアルタイムで報告させられます。このメリットは、MDMソリューションにかかる負荷の軽減だけではありません。アップデートの速度と確実性を高めるとともに、デバイス状態の重要な変化をIT部門が即座に把握できるようになります。

また、MDMの機能はパッチ管理にとどまらず、業務を簡素化し意思決定を効率化する機能も備えています。これは、Mac管理の他の主要素を一元的に運用する機能と同様に不可欠です。MDMの基本的性質を直接物語る機能としては、次のものが挙げられます。

- セキュアな構成および設定の導入
- 管理対象アプリケーションのインストール
- ポリシーベースでのコンプライアンス管理
- 現在のアセットインベントリの維持

IDとアクセス

データを保護することと従業員が生産性を維持するために必要なリソースへアクセスできるようにすることは、一見すると別々の課題のように見えます。しかし、よく見るとその両者は「アクセス許可」という共通の要素で本質的につながっているのです。**Verizon社の2024年度Data Breach Investigations Report**によれば、「データ侵害の68%には人的要素が関わっていた」とされています。この調査では悪意ある内部者は考慮されておらず、アクセス許可の設定ミス（最小権限）に起因するインシデント、および認証情報に関するエンドユーザのミスに起因するインシデントのみが対象とされています。

セキュリティの観点から見ると、脅威の検出と報告について学ぶセキュリティ意識のトレーニングを義務付けたところで、このようなミスに対処できるものではありません。企業としてこうしたインシデントや関連するセキュリティ問題に対処するには、クラウドベースのIDの活用だけでなく、以下の機能も備えたソリューションが必要です。

- リスクを考慮したアクセスポリシー：侵害されたデバイス/アカウントへのアクセスを拒否
- 高度なスプリットトンネリング：業務関連の通信を暗号化し、業務に関係のない通信でもユーザのプライバシーを保護
- 多要素認証（MFA）：リソースを要求したユーザの身分を検証

エンドポイントセキュリティ

2024年には、**macOSを標的としたマルウェア**の総数は世界の全プラットフォームにおけるマルウェア検出数の約11%に達しています。検出数の大多数は他OSが占めているものの、IT部門もセキュリティ部門もこの傾向には留意すべきです。なぜなら、この検出数は2年前と比較して倍増しているからです。さらに、MaaS（Malware-as-a-Service）やAIを利用した高度なマルウェアの登場を受け、インフォスティーラーマルウェアキャンペーンでMacを標的とする脅威アクターは**大幅に増加**しています。

進化する脅威からデバイスを保護するには、macOS内蔵のコード署名対策を回避するトロイの木馬や、APT（持続的標的型攻撃）のような悪意あるコードに加え、マルウェアも防御することが絶対的に必要です。さらに、デバイスと組織のセキュリティ体制を強固に保つため、以下のような対策も欠かせません。

- 行動分析により未知の脅威を特定
- 不審なアプリや検出済みの脅威を隔離し削除
- デバイスの詳細な健全性データ（テレメトリ）をアクティブに監視し、警告および報告
- 危険なウェブコンテンツへのアクセスを制限（ゼロデイフィッシング攻撃のURLなど）

Mac管理における最重要セキュリティ対策

このセクションで扱うべき事柄は多数あるため、特に重要なセキュリティ対策に絞ってリスト形式で紹介します。このようにすることで、IT部門およびセキュリティ部門で対策を講じるうえで必要な情報を柔軟に示すことができます。以下の形式ではIT担当者向けに、前述の3種の基礎ソリューションを統合することで対応可能な7つのカテゴリに分けて、セキュリティ対策のポイントの概要を示しています。

デバイスの登録とプロビジョニング

- MDM登録によりデバイス導入を安全かつゼロタッチで実施する
- システム設定を自動化する（管理対象アプリや構成のプロビジョニングなど）
- デバイスのオーナーシップ（会社所有およびBYOD）にかかわらず社内共通の基準とセキュリティポリシーを適用する

エンドポイント保護とコンプライアンス

- macOSのセキュリティ設定を強化する（FileVault、Gatekeeper、XProtect）
- カスタムアナリティクス機能でデバイス上およびネットワーク内の脅威対策を調整する
- 業界のフレームワークや基準に基づく独自のセキュリティベースラインを構築するうえで必要なコンプライアンスレベルに合わせ、エンドポイントを構成するためのセキュリティ指針を策定する

ID・アクセス管理（IAM）

- 役割ベースのアクセス制御（RBAC）を設定し最小権限アクセスを実装する
- SSOやパスワード認証を導入して認証関連のリスクを最小化する
- ゼロトラストアーキテクチャでデバイスおよび認証情報の健全性を検証する

パッチとアップデートの管理

- OSやアプリケーションのアップデートを簡素化し、既知の脆弱性を自動的に軽減する
- テレメトリデータを追跡し、統合ソリューションとリアルタイムでセキュアに共有する
- コンプライアンス違反の検出時にトリガーされるポリシーベースの自動修復ワークフローを実装し、コンプライアンスを確保する

脅威検出とインシデント対応

- 機械学習を活用して脅威情報の収集と分析、およびデータに基づく助言と勧告を自動的に行う
- シームレスなEDR（エンドポイントの検出・対応）ツールでインシデントの解決を迅速化する
- AIやポリシーベースのワークフローで脅威ハンティングを強化し、修復を自動化する

データの保護と暗号化

- デバイスレコード内に復旧キーを安全に保存・更新する仕組みを整え、FileVault暗号化を適用しキー収集を自動化する
- インフラ全体にゼロトラストネットワークアクセス（ZTNA）を包括的に展開し、保護対象のビジネスリソースへのアクセスはデバイスと認証情報の健全性の検証後に許可する
- データ損失防止（DLP）ツールを使用し、データの保護対象ボリュームへの保存を徹底するとともに不正な共有や認可されていない場所へのコピーを制限する

ネットワークとアプリケーションのセキュリティ

- 全ネットワーク接続を対象として常時暗号化を実装し、ファイアウォールポリシーを管理して、ネットワーク全体でセキュリティ体制を整える
- サードパーティアプリの権限およびmacOSのセキュリティベースラインを管理する
- リソース要求を個別のマイクロトンネルにルーティングしてネットワークトラフィックをセグメント化し、ネットワークベースの攻撃（中間者攻撃）を防止する

Jamfの実績：お客様の声

デバイスのプロビジョニングにかかる時間を削減し効率を向上

「ノートパソコン1台あたり、手動のプロビジョニングに比べて1日以上の時間を節約できました」

– 電子署名・文書自動作成プラットフォーム企業、プロダクトオーナー様

Macを多数導入した企業は、**大幅な効率向上**とセキュリティ体制の強化を実現しています。

反復作業を減らしてイノベーションにかける時間を拡大

「マシン1台あたりにかかる時間をわずか10分にまで削減できています」

– 財務管理・会計プラットフォーム企業、IT担当マネージャー様

自動ゼロタッチ導入ワークフローには、**目に見える時短効果とリソース最適化効果**があります。

包括的なリスク対策によりデータのセキュリティとユーザの生産性を両立

「リアルタイムの脅威検出機能、コンプライアンス監視機能、ポリシーの一元適用機能は、資産の保護と規制への準拠に役立っています」

– デジタル公共図書館、IT担当マネージャー様

Mac管理ソリューションを利用すると**セキュリティ体制と規制コンプライアンスを強化**でき、特にリアルタイム脅威検出機能とポリシーの一元適用機能の効果は絶大です。

デバイスのライフサイクル全体で組織のコンプライアンスを確保

「この構造はSOC 2 Type IIやISO、HIPAAなどの厳格な基準を満たすだけでなく、遵守の取り組みも促進してくれました。このことから、Jamf製品なら組織のセキュリティを強化するとともに主要な業界規制の遵守も実現できるとわかります」

– デジタルヘルス企業、IT担当シニアマネージャー様

コンプライアンスベンチマークとの整合性を能動的に改善し、業界公認の基準やフレームワークに基づいて**セキュリティベースラインを実装**できます。

まとめ

企業におけるMacの導入率が高まっている今、Macデバイスを管理・セキュアに運用するためのプロアクティブな統合型アプローチを最優先で導入する必要があります。進化する脅威に加えて、ハイブリッド／リモートワークを含む複雑化する業務環境においては、ビジネスの運用と整合しつつ、利用者の状況に柔軟に対応できる、明確な焦点を持ったセキュリティ戦略が大きな効果を発揮します。

しかし、そのためには汎用的なソリューションでは力不足です。

むしろ、デバイスやアプリのライフサイクル全体を通じて、Macをネイティブにサポートする多層的なソリューションが求められます。まずは、モバイルデバイス管理（MDM）、ID・アクセス管理（IAM）、エンドポイントセキュリティの3つの組み合わせて強固な土台を構築しましょう。この土台が完成すれば、セキュリティとユーザプライバシーのどちらも犠牲にすることなく、自信を持ってユーザの選択の自由をサポートできます。

簡単に言えば、以下のすべてを実現できます。

- **デバイスのコンプライアンス**
- **データの保護**
- **ユーザの保護**

本資料では、エンドポイントの完全性を維持し規制コンプライアンスを確保するうえで必要となる重要なセキュリティ対策について解説しました。これらの対策を講じることで、セキュリティ部門は脅威に速やかに対応するためのツールを揃え、IT部門は関係者に最高レベルのサポートを提供しながらイノベーションに注力できます。さらに、従業員は業務に支障をきたすことなく最大限の生産性を発揮できるようになります。

複数のソリューション同士がシームレスに連携することで、企業はWindows PCと共存する、安全で拡張性の高いMacエコシステムを構築できます。これにより、生産性・使いやすさ・セキュリティのバランスが取れた環境が実現し、働く場所を問わず、イノベーションと強靭性への道が開かれます。

本資料の要点

従業員の希望と生産性向上のメリットを受け、米国企業におけるMacの導入率は**76%**増加しています。

現在はインフォスティーラーやAIを利用したマルウェアなど、マルウェアの脅威が高まっており、macOS用のエンドポイントセキュリティが重要さを増しています。

IT専門家の**90%**が、職場へのAppleデバイス導入にはビジネス面のメリットがあると評価しています。

コンプライアンスを維持しながら脅威を検出し、対応時間を削減するには、ゼロトラストアーキテクチャと自動化が肝要です。

複数の基盤ソリューションを統合することで、ユーザへの影響を最小限に抑えながらコンプライアンス管理を自動化・効率化できます。

セキュリティ侵害の**68%**には人的要素が関わっているため、権限とアクセスの管理対策が最優先事項となっています。

ソリューションの包括性を高めるには、MDM、ID・アクセス管理（IAM）、エンドポイントセキュリティを統合する必要があります。

IT部門とセキュリティ部門はMacの導入で生じる新たな要素に対応し、リスク対策として多層的な統合戦略を導入する必要があります。

Mac用の包括的な統合セキュリティ戦略を導入することで、ユーザの生産性を最大限に高めながら安全に環境を拡張できます。

企業全体でmacOS特有のリスクを最小限に抑えるには、多層型の戦略が重要です。

jamf

www.jamf.com/ja/

Jamf for Macを無料でお試しください