チェックリスト：セキュリティギャップの特定

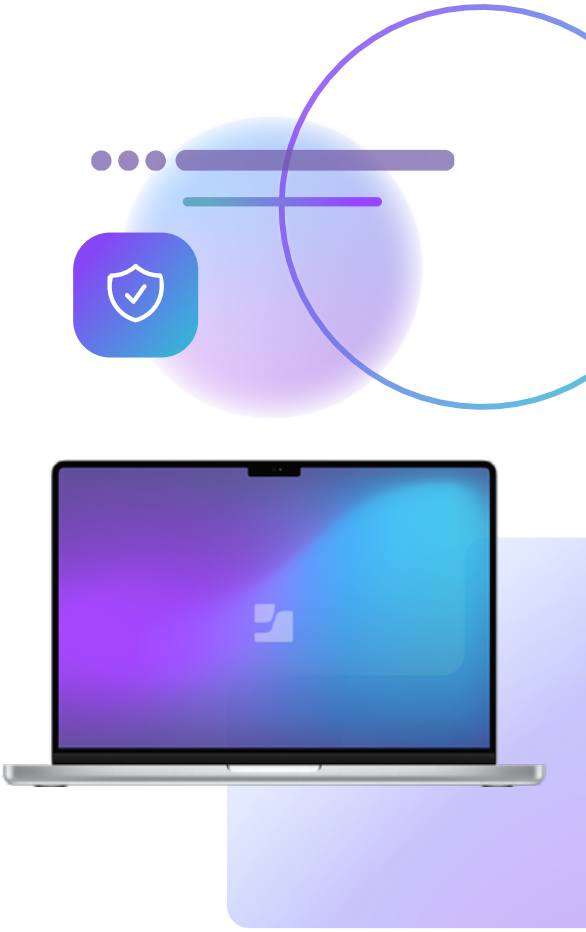
Macを管理するIT管理者とセキュリティ部門向けの要点ガイド

エンジニア、マーケティング担当者、経営陣、クリエイティブチームなど、Macは既に様々な部署で業務に使用されています。Macの人気は高まり続けていて、2025年第2四半期には前年同期比で21.4%の成長率を記録しました。これは、他のどのコンピュータベンダーよりも高い伸び率です。

これは驚くべきことではありません。**Macの使いやすさ**が、仕事の快適さにつながっており、企業におけるMacの導入が進むことで、好みのデバイスを仕事でも使用する環境が整いつつあり、従業員の満足度や生産性の向上が期待できます。しかし、ITおよびセキュリティ担当者にとっては、この状況が新たな課題を意味することもあります。

MacとWindows PCは根本的に異なるデバイスです。OSはもちろんのこと、ハードウェア戦略やアーキテクチャ、設計思想にも違いがあります。当然ながら、それぞれに適したセキュリティ対策も異なるアプローチが求められます。これまでWindowsを主に扱ってきた管理者にとっては、特に多数のデバイスを管理する際に、既存の戦略では対応しきれないギャップを感じるかもしれません。MacはハードウェアもソフトウェアもAppleが一貫して設計・開発しているため、管理者にはAppleのエコシステムに最適化されたツールの活用が必要です。

このチェックリストは、Macのセキュリティに特化した戦略の要点を把握し、潜在的なセキュリティギャップを理解するのに役立ちます。IT担当者やセキュリティ担当者向けに作成したチェックリストを通じて、初期設定、IDとアクセス、エンドポイント保護、コンプライアンスの概要を解説します。



より詳しくお知りになりたい場合は、こちらのホワイトペーパーをご覧ください：

多層防御：ソリューションを多層的に統合してセキュリティギャップを解消

IT管理者向けのセキュリティギャップチェックリスト

ゼロタッチ導入とデバイスの初期設定

検討すべきこと：

- Apple Business Managerをモバイルデバイス管理（MDM）プラットフォームと併用する
- 自動デバイス登録を使用してペイロードと制限を定義する
- Macで設定アシスタントを実行する前に、最小OSバージョンを適用する

ユーザ認証とIDプロバイダの統合

検討すべきこと：

- プラットフォームシングルサインオンをIDプロバイダ（IdP）およびMDMと連携する
- 拡張シングルサインオン構成をサポートするMDM
- 初回ログイン後の特権操作に対する追加認証の要求

Apple OSアップデートの導入

検討すべきこと：

- 自動アップデートと年次ソフトウェアアップグレードを導入する（Windowsデバイスとは頻度が異なる）
- macOSの最新バージョンに対応するための、管理・セキュリティベンダーによる検証作業（特にメジャーアップデート前のベータ版テストを含む）
- ユーザの生産性を損なわない迅速なセキュリティアップデートの展開

32%の組織がパッチで修正可能な重大な脆弱性のあるデバイスを1台以上運用

360レポート

セキュリティオペレーション管理者向けのセキュリティギャップチェックリスト

コンプライアンス フレームワークへの適合

検討すべきこと：

- macOS Security Compliance Project（mSCP）との連携により、デバイスのセキュリティ強化を自動化
- CISレベル1およびレベル2やNIST 800-171などのベンチマークとベースラインに対応する
- 特定のセキュリティポリシーを全社のMacに適用するための管理設定を構成・維持し、自動化

Macに特化した脅威向けのエンドポイントセキュリティ

検討すべきこと：

- ゼロデイ脅威を含む、Macに特化した高度な攻撃を防御するために開発されたツール
- XProtect、Gatekeeper、Notarization（認証）などのmacOSの標準機能を活用したリアルタイムエンドポイント保護の実装
- 専門家による最新の調査結果を参考にした、Mac特化型マルウェアに対する脅威ハンティングの実施

既存のSIEM/SOARへのmacOSテレメトリデータのストリーミング

検討すべきこと：

- エンドポイントセキュリティAPI から直接テレメトリを取得するツール
- 既存のSIEMデータモデルにmacOSテレメトリを整合させるツール
- すぐに使用できるようにテレメトリをコンテキスト化するツール
- GatekeeperのバイパスやXProtectによるマルウェアへのフラグ設定時など、macOSセキュリティイベントのリアルタイム分析

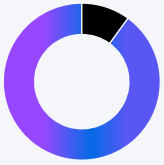
主なMacマルウェア：

インフォスティーラー**28.36%**

アドウェア**28.13%**

トロイの木馬**16.61%**

360レポート



サイバー攻撃の90%以上は、フィッシングが起点です。

360レポート

アプリケーションのインストールと監視

検討すべきこと：

- 環境内のサードパーティmacOSソフトウェアを最新に保つツール
- Macアプリのバージョンと使用状況のレポート
- 管理対象アカウントと開発者証明書によるアプリ配信チャネルの制御

ユーザとデバイスによる業務リソースへのアクセス

検討すべきこと：

- Network Relay などのAppleテクノロジーを活用したゼロトラストネットワークアクセスの実現
- Secure Enclave を活用したハードウェアベースのデバイス認証による条件付きアクセス制御の実装
- macOSプラットフォームに特化したゼロトラストモデルの構築

多層防御戦略に向けた取り組みの第一歩として、このチェックリストをぜひお役立てください。

jamf

www.jamf.com/ja/

さらに詳しく知りたい場合は、
ぜひ、こちらのホワイトペーパーをご覧ください