2026年5月19日

Jamf Japan 合同会社

Jamf、「2026年版セキュリティ360レポート」を公開：モバイルデバイスおよび Mac の最新セキュリティリスクを分析

～脆弱性を抱えたアプリやバージョンの古い OS が企業・組織にとって大きなリスクに～

企業・組織における Apple デバイスの管理とセキュアな運用のための業界標準ソフトウェアを提供する Jamf Japan（本社：東京都千代田区、カントリーマネージャー：岡 学）は、モバイル環境および macOS 環境を分析した最新の「セキュリティ360レポート」の日本語版を公開しました。本調査レポートでは、2025年の業界動向や実際のインシデント、各種セキュリティリスクの調査データをもとに、攻撃者が使用する主要な攻撃ベクトルを分析し、セキュリティおよび IT 担当者が、Mac やモバイルデバイスを企業・組織内で安全に運用するために取り組むべき重要な対策や知見を提示しています。

モバイルデバイス版

Mac 版

「セキュリティ360レポート」の調査概要

■セキュリティ360レポートとは

企業におけるモバイル環境および macOS 環境のセキュリティリスクを分析し、実データに基づく洞察と戦略的な対策指針を提供するレポートです。
モバイルデバイス環境と macOS 環境それぞれに特化した2本のレポートで構成され、複雑化するリスクを包括的に可視化し、より高度なセキュリティ対策について紹介しています。

■調査目的

企業・組織に影響を及ぼすモバイルデバイスおよび Mac のセキュリティリスクへの理解を深め、適切な脅威検出、コンプライアンス管理、インシデント対応の実現を支援することを目的としています。お客様の環境を守るだけでなく、Mac やモバイルデバイスのセキュリティ強化、導入成功に役立つ知見をセキュリティコミュニティ全体に提供するために、Jamf は最新のセキュリティトレンドを調査しています。

■調査方法

以下のサンプルにて、2025年末に世界各地の過去12ヶ月間のデータを対象に調査を実施しました。

・モバイルデバイス：Jamf のお客様が利用している iOS および Android 計170万台以上
・Mac：15万台以上の Mac デバイス※
※マルウェア調査においては米国を拠点とするデバイスを対象とし、脆弱性調査では世界各国のデータを使用しています。

プライバシーを守り、データの収集および取り扱いに関する最高の基準を維持するため、すべて匿名性を確保した形で分析を実施し、今回の調査で分析したメタデータは個人情報や組織を特定する情報を含まない集約されたログから得られたものを使用しています。

モバイルデバイス・macOS 環境の最新セキュリティリスク動向

■モバイルデバイスが直面するセキュリティリスクの動向

モバイルデバイスは、従業員が場所を問わず業務を行うための基盤として、その重要性を増しています。多くの組織がセキュリティソフトウェアを導入し、各種機能やポリシーを活用して

管理や保護を行っているものの、一方で、サイバー攻撃は年々高度化・巧妙化しています。そのため、モバイルデバイスが直面するセキュリティリスクへの意識を高めるとともに、頻発する脅威からデバイスを守るための具体策を講じることが不可欠です。
2026年版レポートでは、モバイルデバイスを標的とした脅威を、組織にとって特に優先度の高い以下の4つのカテゴリに分類し、詳細に分析しています。

(1)デバイスの脆弱性 ～2社に1社が脆弱性を放置したままのデバイスを保有～

企業・組織において、プログラム実行、データ処理の基盤としてモバイルデバイスの重要性は高まっていますが、多くの企業では PC ほどセキュリティ管理が十分に行われていません。実際に、今回の調査では過去1年間に53%の組織において、OS のバージョンが古く、リスクの高い状態のデバイスが見つかっています。
脆弱性が放置されたデバイスから機密データなどが流出するリスクの対策として、すべてのデバイスを MDM に登録し、包括的で綿密な管理体制を整えることが重要となります。

(2)アプリケーションのリスク ～95%のアプリに中リスク以上の脆弱性が存在～

モバイルアプリは、モバイルデバイスで業務を行う上で欠かせないものである一方、組織の攻撃対象領域を拡大させる要因となりえます。今回の調査で評価対象となったアプリのうち、95%で「中」レベル以上の脆弱性が1件以上確認され、モバイルアプリのほとんどが攻撃者の対象となりうることを示唆しています。
また、危険な権限を要求したアプリは62%、プライバシーに影響を及ぼす可能性のある動作が含まれるアプリは21%に上っています。
モバイルアプリをきっかけとした情報漏洩の危険性が増加している現在、業務で使用するアプリを統制し、脆弱性を常時把握していくことが企業に求められています。

(3)ネットワークと Web のリスク ～1/4の企業でフィッシングリンクをクリック～

フィッシング攻撃は、依然として主要な攻撃手法として用いられています。今回の調査では、25%の企業・組織でフィッシングリンクをクリックしたユーザが確認されました。さらに、18%の企業・組織では、危険な Wi-Fi スポットに接続したユーザが存在しており、安全性の低い公共ネットワークが企業のデータにおけるリスクとなっていることが示されています。
デバイスの技術的な管理による対策だけでなく、従業員自身がリスクとして認識し、迅速に対応できるようにセキュリティ訓練を企業として適切に実施することも重要です。

(4)持続的標的型攻撃（APT）～高度な手法を用いたリスクの存在～

高度な技術を有するサイバー攻撃者組織は複数の脆弱性を組み合わせ、ゼロクリック攻撃やブ

ラウザ攻撃など高度な手法を用いています。2025年には、Apple 製品の画像解析の脆弱性（CVE-2025-43300）を悪用した WhatsApp ユーザを狙う攻撃や、スパイウェアグループによる JavaScript を使ったワンクリック攻撃の事例が確認されています。
高度化する攻撃から重要データを守るために、厳格なデバイス管理と迅速なセキュリティアップデートが重要になります。

■macOS 環境が直面するセキュリティリスクの動向

ビジネスシーンにおける Mac デバイスの導入拡大に伴い、macOS を標的としたセキュリティリスクも多様化しています。Mac デバイスの市場シェアは、全世界で2024年から2025年にかけて16.4%拡大し、2025年の Mac デバイスの出荷台数は270万台を超えました。今や、Mac デバイスはあらゆる場所で活用されていると言っても過言ではありませんが、その多様化するリスクへの対策は非常に重要になっています。

Mac を狙うマルウェアと脅威 ～トロイの木馬による攻撃の増加～

Mac を含む Apple 製品には Gatekeeper やシステム整合性保護（SIP）、Transparency, Consent, and Control（TCC）などのセキュリティ機能が備わっていますが、それでも Mac を狙った攻撃は増加しています。実際に、悪意のあるネットワークトラフィックが検出されたデバイスは44%、デバイスを不正利用するクリプトジャッキング被害を受けた組織は26%に上りました。2025年に Jamf Threat Labs※が新たに登録したマルウェアサンプルは26,000件以上に達しています。
2025年の調査では Mac デバイスを標的とした攻撃では、約90%がトロイの木馬、インフォスティーラー、アドウェア、潜在的に迷惑なアプリケーション（PUA）の4種類で占められています。2025年に最も多く確認された攻撃はトロイの木馬で、全体の約50%を占めました。2024年はトロイの木馬の攻撃割合は16.6%であり、インフォスティーラーとアドウェアが主流であったことを踏まえると大幅に増加していることがわかります。

※データアナリストおよびサイバーセキュリティの専門家で構成された、モバイル・Mac の脅威調査を行う専門チーム

Mac を標的とした主なマルウェアファミリー ～多種多様なマルウェアによる脅威～

Mac デバイスを標的とするマルウェアファミリーは多種多様で、明確な主流は存在していません。2025年の調査では、ブラウザを改ざんし、ユーザの行動を追跡する PuAgent が全体の16.4% を占め、最も多く確認されたマルウェアファミリーとなりました。
一方で、2023年および2024年に最も多く検出されていた Web ブラウザを乗っ取り、ユーザ情

報を収集する Genio アドウェア（13.6%） は、2025年には 7.19% に減少し、第4位に順位を下げています。これらの結果は、Mac を取り巻く脅威が固定化されたものではなく、年々変化していることを示唆しています。
このような脅威に対し、macOS 環境においては、Windows 優先のアプローチではなく、Apple エコシステム専用に構築されたセキュリティソリューションを活用し、適切な対策をとっていくことが重要になります。

アプリおよび OS の脆弱性 ～モバイルデバイスを上回る数値～

本調査では、58%の組織で OS バージョンが古くリスクのある Mac デバイスが確認されており、モバイルデバイスを上回る数字となりました。また、評価対象のデバイスの73%から脆弱性を含むアプリケーションが1件以上検出されています。
モバイルデバイス同様に Mac においても、定期的なソフトウェアアップデートの適用、デバイス状態の可視化、脆弱性への迅速な対応が重要です。

これらの結果から、モバイルデバイスおよび Mac 双方において、脆弱性管理やデバイス状態の可視化、ユーザ教育を含めた包括的なセキュリティ対策の重要性が明らかになりました。本レポートでは、こうした脅威の詳細な数値や課題解決に向けた具体的な対策を提示しています。

■レポートのダウンロード
「2026年版セキュリティ 360 レポート」の日本語版はこちらからダウンロード可能です（「PDF をダウンロード」をクリックください)。

セキュリティ360 ：モバイルデバイス 最新トレンドレポート
セキュリティ360 ：Mac デバイス 最新トレンドレポート

Jamf について

Jamf は、エンドユーザから愛され、企業・組織から信頼される Apple エクスペリエンスの管理、セキュアな運用、業務の簡素化を目指しています。また Jamf は、デバイス管理、セキュリティ対応、AI による自動化が統合された Apple 特化型プラットフォームを提供する業界唯一の企業です。IDC Market Scape や Gartner®においても、複数の部門でリーダとして選出され、業界をリードしています。
Jamf Japan 合同会社は2017年の設立以来、日本国内の企業だけでなく、教育機関や医療機関

など幅広い業界において、Apple デバイスの統合エンドポイント管理を支援してきました。
Jamf Japan は、グローバルで培ったノウハウを活かし、日本市場に特化したサポート体制を構築。導入から運用、セキュリティ強化まで、組織の規模や業種に応じた柔軟なソリューションを提供しています。
Jamf に関する詳細は公式 Web サイトをご覧ください。

■報道関係者様のお問合せ先■
Jamf Japan 広報事務局（株式会社小田急エージェンシー内）
メール：jamf_press@odakyu-ag.co.jp