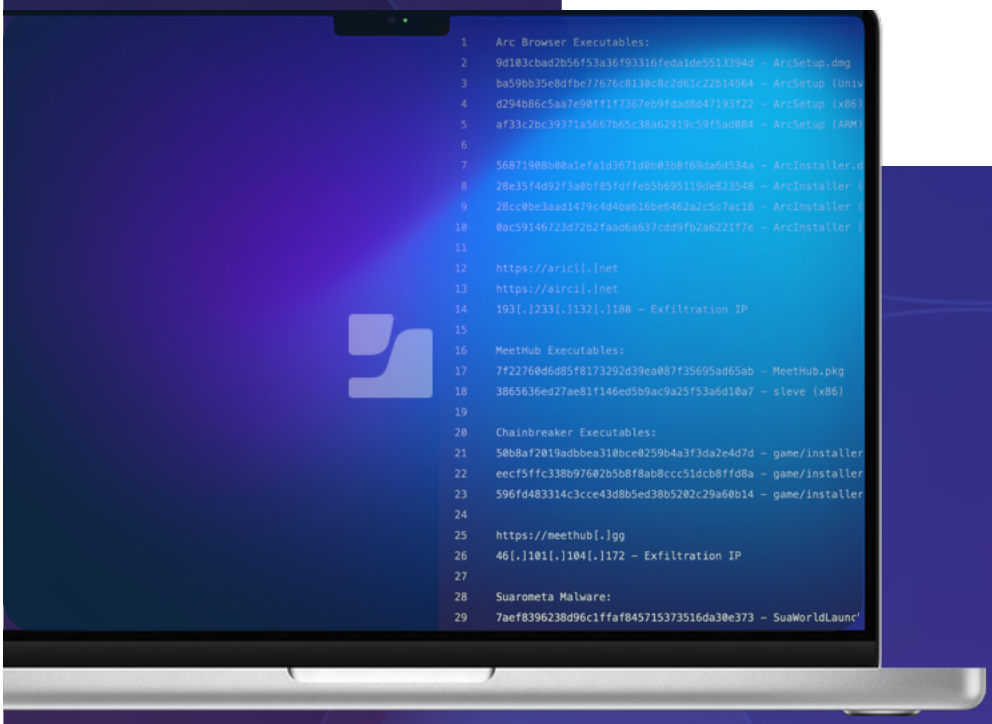
jamf

セキュリティ360：
最新トレンドレポート
Mac



序文

Jamfは、Macの大ファンです。私たちが最初に開発したソフトウェアはMac向けであり、現在でも多くのJamf社員がMacに強い情熱を注いでいます。Jamfは**macOSセキュリティコンプライアンスプロジェクト**の公式コントリビューターとしても活動しており、創業以来、**Macが業務環境においてますます重要な役割を担うようになる過程**を、現場の最前線で見つめ続けてきました。初めはクリエイターやエグゼクティブ向けのマシンでしたが、今やエンジニアなどの職種の日常業務にも浸透しつつあります。しかし、職場でのMacの普及が進むにつれ、脅威アクターから狙われる攻撃対象領域も広がっています。

Macを標的とした脅威はかつてないほど多様化し、巧妙なMacの侵害方法が多数編み出されています。Jamfは「お客様のApple製品による成功をお手伝いする」というミッションの下、お客様、そしてAppleコミュニティ全体のために、Macデバイスを狙う脅威の現状を注意深く監視しています。

– Jaron Bradley、
Jamf Threat Labsディレクター

はじめに

Jamfセキュリティ360は、昨年実際に起きたお客様のインシデント、脅威の調査、業界の出来事を分析した結果を基に作成されるレポートです。本レポートでは、組織が直面しているリスクを明らかにするため、現在のMacを取り巻く環境を調査しています。

本書では、ユーザを騙し、デバイスを侵害して組織に侵入するうえでよく用いられている各種攻撃ベクトル（マルウェア、脆弱性、ソーシャルエンジニアリングなど）を分析評価しました。この分析は、デバイス脆弱性やWeb脅威、マルウェアなどのトピックを対象としています。

さらに、こうした脅威の最新事情に関する分析結果に加え、ユーザ、デバイス、アプリケーション、ネットワークの各レベルでのMacデバイスの保護に関するセキュリティリーダーの知見を踏まえた、Jamf CISOからの助言も提供します。

調査方法

本レポートで特定するセキュリティトレンドが現実社会に及ぼす影響を把握、定量化するために、Jamf製品によって保護されているデバイス140万台をサンプルとして分析しました。分析対象は過去12ヶ月間、世界90ヶ国で、実施時期は2025年第1四半期です。

プライバシーを守り、データの収集・取り扱いに関する最高の基準を維持するため、調査で分析され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。

調査の目的

この分析の目的は、組織やユーザ向けに、高度化するサイバーセキュリティの最新のトレンドを解説し、リスクを軽減するための手法を紹介することです。また、マルウェアや脆弱性の発見など、Jamf Threat Labsが成し遂げた調査結果の中でも特に影響の大きかったものについても概説します。

Macのセキュリティ強化については、「信頼できるソース以外からはソフトウェアをダウンロードしない」など、ユーザであれば誰でもできる行動がいくつかあります。一方で、組織として実践できる以下のようなベストプラクティスも存在します。

- オペレーティングシステム(OS)のアップデートを速やかかつ継続的に適用する
- ユーザに教育とトレーニングを提供する
- アプリケーションを審査する
- 多要素認証を実装する
- ゼロトラストセキュリティフレームワークを実装する
- 社内データの利用ポリシーを定める
- 全ユースケースでAppleに最適な業務フローを適用する

こうしたベストプラクティスの中にはすべての組織で実践すべきものもありますが、一部組織だけのデバイスセキュリティ要件もあります。たとえば、規制の厳しい業界で活動する組織の場合、業界ベンチマークやフレームワーク(CISベンチマークやHIPAAなど)への準拠が必要になります。

今年のレポートでは、世界中の組織にとって最優先事項と考えられる以下の3つのリスクカテゴリに分けて分析結果を紹介します。

I. アプリケーションリスクとマルウェア

II. 脆弱性管理

III. ソーシャルエンジニアリング

モバイルデバイスに関するセキュリティ360レポートも公開していますので、ぜひ**こちら**からご覧ください。

本レポートの分析の大部分は、Jamf Threat Intelligence、独自の脅威調査で得た幅広い知見、現実の使用状況に関する指標に加え、ニュース分析とデータフィードもベースとしています。Jamf Threat Intelligenceは、Jamf Threat Labsとデータサイエンスチームによる実践的かつ高度な調査に裏打ちされています。これらの専門チームが、デバイス・アプリ・ネットワークトラフィックを常時監視し、リスクや脅威、ゼロデイ脆弱性を特定・分析しています。

企業のMacデバイスの重要トレンド

セキュアなプラットフォームでも、マルウェアのリスクは存在

Appleは**プラットフォーム設計の中核にセキュリティを据えています**。この方針は、プラットフォームそのものだけでなく、Appleユーザに対するセキュリティの伝え方にも現れています。たとえば、**Appleプラットフォームのセキュリティサイト**には、Appleユーザ向けにmacOSでのマルウェア対策を紹介するページが設けられています。さらに、App Store、XProtect、Gatekeeperなどの各種テクノロジーを組み合わせることで、アプリのライフサイクルの各段階にわたり複数の層で悪意あるアプリを阻止しています。

Macデバイスの業務利用において、セキュリティとは、リスクの可能性があるアプリへのアクセスを禁止しながら、作業に必要なアプリをユーザに提供する行為を指します。Macアプリはネイティブ Macアプリ、Webアプリ、ハイブリッドアプリのようにタイプもサイズもさまざまであり、作成・設計した開発者の想定する用途も多種多様です。しかも、昨今の**一般的なMac用ビジネスアプリの多くは**、Mac App Store経由ではなく、開発者から直接パッケージとして配布されています。その上、ユーザはアクセス可能なサイトであればどこからでもアプリをダウンロードできます。

たった一つの脆弱性が、システム全体を危険にさらす

事実として、私たちが日常的に使用しているソフトウェア（OSおよびアプリケーション）には脆弱性が存在します。

米国立標準技術研究所（NIST）によると、「一般的なソフトウェアの場合、エラーおよび脆弱性の推定発生頻度はコード1,000行あたり約25個」とされています。また、同研究所のNational Vulnerability Database（NVD）で公開されている共通脆弱性識別子（CVE）では、次の情報が公に提供されています。

- CVEの情報
- 影響を受ける製品またはベンダー
- 脅威の説明

脆弱性が発見され、パッチで修正されるまでの間に、被害が生じる可能性があります。また、パッチが公開された場合でも、該当のデバイスにインストールしなければ意味はありません。どのような脆弱性が存在し、最も深刻であるかなどを把握可能なセキュリティツールを導入することで、IT部門や情報セキュリティ部門では最も緊急性の高いパッチを最優先で適用し、パッチ適用プロセスを効率化できます。

巧妙化するソーシャルエンジニアリングによるユーザの被害が続発

今回の調査でも、フィッシングなどのソーシャルエンジニアリングが脅威アクターの攻撃手法として非常に多く使われており、脅威ランドスケープにおける影響力は従来と同程度でした。2024年9月に**Appleはブログ記事を投稿**し、Appleユーザ向けに「詐欺に引っかからないためのヒントや、疑わしいメールやその他のメッセージを受信したり、そうした電話がかかってきたりした場合の対処法」を紹介しました。攻撃者の手口は巧妙化しており、採用担当者や家族、実績ある企業などを騙るようになっています。プラットフォームやオペレーティングシステムのセキュリティがどれほど強固であっても、ソーシャルエンジニアリングはデバイスの最も脆い部分、つまりユーザを突いて社内データを侵害するのです。

パート1:Macに特化したマルウェア

本レポートでは、実際に確認された種類、組織に対する影響、発生頻度など、Macを標的としたマルウェアの情報について解説することを目的としています。企業でのMacの利用が拡大し、より重要なアプリケーションにMacからアクセスするようになるにつれ、組織全体のユーザが攻撃の標的となりつつあります。

Appleのマルウェア対策は、以下の3層構造になっています。

1. **マルウェアの起動と実行の防止**
2. **ユーザシステムでのマルウェア実行のブロック**
3. **実行されたマルウェアへの対処**

AppleはApp Store、GateKeeper、XProtect、公証など、脅威を軽減するための各種ネイティブテクノロジーをユーザ向けに提供しています。たとえば、XProtectは、内蔵のウイルス対策機能です。さらにマルウェアが発見された場合、Appleはデベロッパ ID を無効化するなどの対処を講じます。

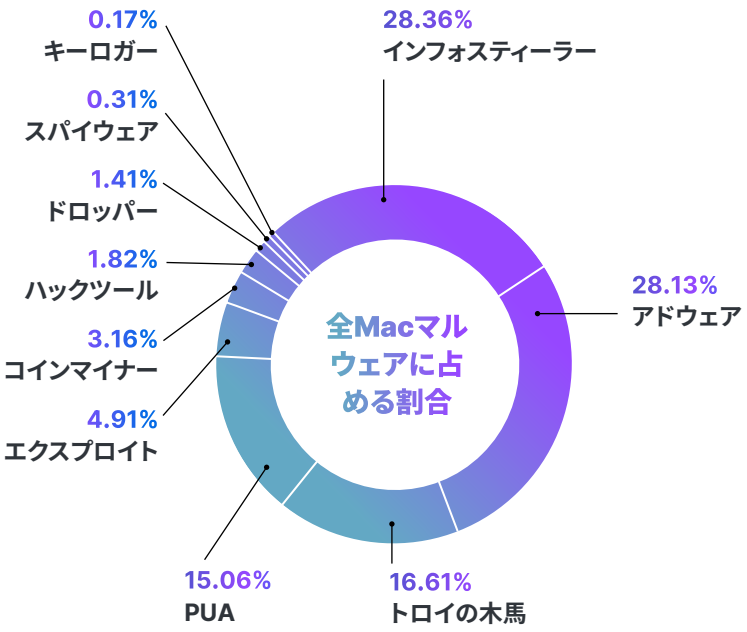
macOSは強力なセキュリティメカニズムをシステムに内蔵していますが、マルウェアと無縁というわけではありません。**今年3月**、Jamf Threat Labsチームとデータサイエンスチームはマルウェアとは無縁という通説について論じた記事を共同で執筆し、既知のマルウェアとともに新種のマルウェアを解説して、Titan（Jamf Threat Labs開発の3D可視化ツール）でmacOSのマルウェアベクトルを紹介しました。Titanを活用することで、状況を詳しく示し、関連するマルウェアサンプルを提供しています。さらに、複数のマルウェアファミリが発見されたことで、macOSを狙う「新種の特化型マルウェアの数が増え続けている」こともわかりました。これが意味するのは、「Macを狙うマルウェアが存在し、この種のマルウェアには複数のファミリがあり、このマルウェアを利用する脅威アクターが増加している」ということです。

今年、Jamf Threat Labsは、北朝鮮（DPRK）との関連が疑われるマルウェアが**Flutterベースのアプリケーションに組み込まれている**ことを発見しました。Flutterはクロスプラットフォーム対応であるため、アプリケーション開発にこのフレームワークが使われるのはめずらしくありません。しかし、Jamf Threat Labsチームの知る範囲ではmacOSデバイスへの攻撃にFlutterが使われた事例はこれが初めてであることから、この攻撃は注目に値します。同チームはこのマルウェアおよびPython版とGo版の亜種について解説し、「このマルウェアはより強力な攻撃の開発を目的としたテスト用である可能性が高い」理由を明かしています。また、コード開発にFlutterを使用することで、自然と構造がわかりにくくなる点も特筆に値します。

Macマルウェアのファミリ

以下に、2024年に調査した新規Macマルウェア事例の内訳を示します。

このデータからわかることは、昨年のマルウェアレポートと比べるといくつかの一貫性が見られることです。たとえば、アドウェア、トロイの木馬、潜在的に迷惑なアプリケーション（PUA）、エクスプロイト（エクスプロイトを利用していると判明したアプリケーション）は、今年もマルウェアカテゴリの上位を占めています（昨年はトロイの木馬が17%で最多でしたが、今年は16.6%とやや減少しました）。ただし、今年のトップはインフォスティーラーでした。それどころか、調査対象となったマルウェア全体に占める割合について、インフォスティーラーは28.08%もの増加を見せています。



インフォスティーラーが存在している点は、Jamf Threat Labsの昨年の調査結果と一致しており、macOS環境はこの種のマルウェアの攻撃に絶えずさらされている状況です。この手口で興味深い点は、攻撃者が目的のデータを不正に入手するうえで、インフォスティーラーだけでなく先述した別の手法である「ソーシャルエンジニアリング」も利用していることです。このことからわかるように、脅威アクターは被害者を騙すために、複数の攻撃手法を組み合わせるようになっています。そのため、クリプト産業のように注目度の高い業界で活動する従業員や組織にとっては、トレーニングとセキュリティツールの両方の観点で警戒心を維持することが重要と言えます。攻撃は偶然に受けるものではなく、仕組まれたものなのです。

調査事例：PyInstallerを利用してmacOSにインフォスティーラーを送り込む

2025年4月、Jamf Threat Labsは、PyInstallerを利用してMach-O形式の実行可能ファイルにPythonコードをバンドルする、これまで検出されていなかったmacOS狙いのインフォスティーラーサンプルを発見しました（Jamf Threat LabsはVirusTotal上で未検出のインフォスティーラーを3種発見しました）。

PyInstallerは、開発者がPythonスクリプトをスタンドアロンバイナリにパッケージするための正式なオープンソースツールです。しかし、今や攻撃者はこのツールを利用し、macOSでスムーズに実行される悪意あるペイロードを配布するようになっています。同チームはこのマルウェアの主要機能を検証し、その正体がインフォスティーラーであると確認しました。マルウェアの主な機能は次のとおりです。

- 偽りのパスワード入力画面を表示し、ユーザの認証情報を収集する
- 攻撃者サーバから送られた任意のAppleScriptペイロードを実行する
- 保存済みの認証情報や機密情報をmacOSキーチェーンから直接抽出する
- 既知の暗号通貨ウォレットのファイルシステムをスキャンし秘密鍵を流出させ、暗号資産を盗む

インフォスティーラーがmacOS狙いの脅威として広がり続けるにつれて、これらを配布する新たな手段が脅威アクターにより編み出されていくでしょう。しかし、上記のマルウェアから組織を守るための実用的な対策もあります。例えば：

- ソフトウェアの実行をAppleおよび確認済みの開発元により署名されたアプリのみに限定する
- 正規のITプロセスに使用するosascriptプロンプトを自社ブランドにするとともに、認証情報の入力前にその自社ブランドを確認するようスタッフを教育する

注意すべきマルウェア

POOLRAT

POOLRATは3CXのサプライチェーンの侵害に関与したことで知られるmacOSバックドアで、攻撃者が重要なシステムデータを収集し、ファイル操作と同時にコマンドを実行できるようにします。最近、このマルウェアをスリム化したPondRATも見つかっています。

PondRAT

PondRATはAppleJeusおよびPOOLRATとの類似点があるバックドアで、悪意あるPyPiパッケージを通じて配布されました。インストールされると、コマンド&コントロールサーバ（C2）との接続を確立して、ファイルのアップロードとダウンロードの円滑化や所定期間にわたる動作の一時停止、任意コマンドの実行を行います。

NotLockBit

悪名高いLockBitの亜種を装った、Goベースのランサムウェアです。このランサムウェアは最初の事例以来、暗号化された公開鍵を使用して、ハードコードされた拡張子のリストを列挙し、暗号化しています。最新版の亜種は、攻撃者の管理するS3バケットにデータを流出させ、osascriptを使用してデスクトップ壁紙を変更します（LockBit 2.0と同様）。現在、NotLockBitの開発は積極的に進められているものと考えられています。

Thiefbucket

Thiefbucketは北朝鮮のLazarus Groupとの関連があるマルウェアファミリで、高度なソーシャルエンジニアリングキャンペーンを通じて標的を狙います。第2段階のペイロードとして、偽のコーディング問題を通じて配布されていることが観察されました。このバックドアには複数の機能があり、中でも注目すべきは自動インフォスティーラー機能です。他の機能としては、永続化メカニズム、プロセスの終了、ファイルの削除、ファイルのダウンロード／アップロード、自己削除、シェルコマンドの実行、Spotlightによる迅速なファイル検索、コマンド&コントロールサーバとの通信などがあります。

HZ Rat

HZ RatはmacOSバックドアであり、元々はWindowsユーザを標的としていましたが、その後正規ソフトウェアインストーラーの偽物でmacOSユーザを標的とするように変更されました。インストールされると、コマンド&コントロールサーバ（C2）との接続を確立し、攻撃者がコマンドを実行したり、ファイルを盗んだり、WeChatおよびDingTalkから機密情報（ユーザ名、メールアドレス、電話番号などの個人情報）を抽出したりできるようになります。

Banshee Stealer

Banshee StealerはTelegram上で宣伝された、攻撃者用のWebインターフェースを備えたMaaS（Malware-as-a-Service）です。情報窃取に特化し、アカウントパスワード、ブラウザデータ、セッションクッキー、暗号通貨ウォレットなど、さまざまな機密データを流出させることができます。他のインフォスティーラーと同様にAppleScriptのダイアログ機能を悪用し、ユーザを騙して認証情報を提供させます。ユーザのパスワードが入力されると、macOSキーチェーンからさらに追加の機密データを盗み出します。アンチ仮想マシンやアンチデバッグなどの分析を妨害する回避手段が複数搭載されており、ロシア語のシステムを検出する機能も備えています。

InvisibleFerret

InvisibleFerretはPythonベースのトロイの木馬で、偽装アプリケーションに組み込まれたマルウェアにより使用されていました。最も注目すべき点は、ステージ2のインプラントとしてBeaverTail InfoStealer（一部はDPRKの仕業とされる）により投下される事例が確認されたことです。複数プラットフォームに対応した悪意あるPythonスクリプトであり、攻撃者は偵察やデータの流出、クリップボードのコピー、リモートコマンドの実行を行えます。また、追加のリモートコントロールが必要な場合には、AnyDeskソフトウェアをインストールすることも可能です。

BeaverTail

BeaverTailはインフォスティーラーであり、ソーシャルエンジニアリングキャンペーンで標的に送られる前に正規アプリケーションを偽装していることが確認されました。他のインフォスティーラーと同様に、標的のキーチェーン、ブラウザクッキー、暗号通貨ウォレットなどの重要な情報を収集し、攻撃者の管理するサーバにアップロードします。また、InvisibleFerretバックドアなど、標的のシステム上で別のリモートペイロードを実行する機能も備えています。DPRKが関与しているとされています。

Poseidon Stealer

Poseidon Stealer（Atomic Stealerの競合種）はTelegram上で宣伝された、攻撃者用のWebインターフェースを備えたMaaS（Malware-as-a-Service）です。情報窃取に特化し、アカウントパスワード、ブラウザデータ、セッションクッキー、暗号通貨ウォレットなど、さまざまな機密データを流出させることができます。Atomic Stealerと同様にAppleScriptのダイアログ機能を悪用し、ユーザを騙して認証情報を提供させます。ユーザのパスワードが入力されると、macOSキーチェーンからさらに追加の機密データを盗み出します。このマルウェアは正規アプリケーションを装って配布され、Google Ads上のマルバタイジングを通して配信されていることが確認されています。

Kuiper

KuiperはGoで書かれたRaaS（Ransomware-as-a-Service）で、アンダーグラウンドフォーラムにおいてRobinhoodという名のユーザにより宣伝されました。RSA、ChaCha20（600 MB以下のファイル用）、AES（600 MB以上のファイル用）を組み合わせてファイルを暗号化します。大部分の機能はWindowsを標的としたものですが、macOS狙いの亜種は「/dev/urandom」を使用してランダムキーとランダム初期化ベクトル（IV）を生成し、脅迫文を復号し、標的を再帰的に暗号化（「.kuiper」拡張子を付加）し、キーとIVをメモリから消去して、システムを再起動します。

Macマルウェアの確認結果

カスタマー環境において確認されたMacマルウェアをより詳しく見ると、以下のマルウェアファミリがトップ10にランクインしていました。

ファミリ名	カテゴリ	パーセント
Genieo	アドウェア	13.63
Imobie	PUA	10.96
Multiverze	アドウェア	9.44
Mackeeper	PUA	7.19
Tnt	PUA	6.07
Jailbreak	PUA	5.74
Ccleanmac	アドウェア	4.33
Puagent	トロイの木馬	3.07
Macinformer	PUA	2.33
Pirrit	アドウェア	2.33

上記の数字から、数量の観点ではインフォスティーラーをはじめとする多くの種類のマルウェアが大幅に増加しているものの、ユーザに最も頻繁にダウンロードおよびインストールされているアプリケーションは前年同様アドウェアとPUAであることがわかります。アドウェアは対象範囲が広く、インフォスティーラーは標的が絞られていることを踏まえると、この傾向はすべてのOSプラットフォームに共通するものと考えられます。

Jamf Threat Labsは、**クリプト業界の個人を標的としたインフォスティーラー**に関するブログを公開しました。こうした攻撃者の目標は、認証情報とさまざまな暗号通貨ウォレットのデータを収集することです。Jamf Threat Labsでは、被害者のシステムにインフォスティーラーを投下する以下の2つの攻撃手法を追跡しました。

1. Google広告経由：「Arc Browser」を検索してGoogle広告をクリックしたユーザを、悪意のあるサイトに誘導します。
2. バーチャル会議経由：攻撃者は、求人面接やビジネスチャンスを装ってターゲットに接触し、Meethubなどのバーチャル会議ツールを用いてユーザを偽のミーティングへ誘導します。

どちらの事例でも、ユーザはGatekeeperをバイパスしてアプリケーションをダウンロードし、macOSのログインパスワードを入力するよう求められました。

今回調査したマルウェアファミリと提供したサンプルから、以下のように基本的なセキュリティ原則が必要であることがわかります。

- アプリケーションは正規ソースから取得する
- 審査プロセスを適用する（Mac App Storeなどの信頼できる第三者を利用するか、デバイス管理ベンダーから調達する）
- 最新のセキュリティソフトウェアを実行する

Jamf CISOからのアドバイス

- **Macに特化した専用EDRソリューションを導入する：**企業向けの多くのソフトウェアは依然としてWindowsファーストの設計となっており、Appleデバイスは後回しにされがちです。しかし、特にセキュリティに関しては、このような考え方はもはや時代遅れです。脅威ランドスケープが発達している今、初めからApple製品のために開発されたセキュリティ製品を選ぶ必要があります。
- **堅牢なMDMソリューションを導入する：**
  デバイスを保護するには、それらの管理が不可欠です。ユーザの自由度と手にする可能性のあるアクセス権を考えると、マルウェアの大規模感染を未然に防ぐためには、デバイスと各デバイスのユーザを管理できる堅牢なフレームワークを用意することがきわめて重要です。
- **強力なコミュニケーション戦略を確立する：**
  セキュリティ部門とIT部門の連携や、セキュリティ部門による社内広報、トレーニングプログラム、エンドユーザ向けの啓発活動、経営陣の社内連絡など、運用しているセキュリティプログラム、ツール、現在の戦略について効果的に伝える仕組みをつくることで、社員全員の認識を揃え、共通の目標に注力させられます。

パート2：脆弱性管理

脆弱性はどれも同じというわけではありません。その深刻度はさまざまであり、ほとんどのものには個別のスコアが割り当てられています。**Apple** は、macOSに影響するパッチ修正済みのセキュリティ脆弱性と、各脆弱性を修正したオペレーティングシステムの一覧を公開しています。たとえば、2024年には、**CVE-2024-44308** および**CVE-2024-44309**（Webコンテンツに悪意ある工夫を施すとWebコンテンツのサンドボックスを抜け出せる脆弱性）に対応したmacOS 15.1.1がリリースされました。これらのCVEの深刻度スコアは「高」でした。一方で、Appleからはスコアの低いCVEに対するセキュリティアップデートもリリースされています。これが意味するのは、「優先順位付けが重要」ということです。IT部門とセキュリティ部門が、システムやアプリケーションも含めて社内デバイスの脆弱性を完全に把握できれば、最も緊急性の高いものに正しく対処できるようになります。

Appleは、より特別なセキュリティアップデートである「緊急セキュリティ対応」で、ソフトウェアアップデートの合間に**セキュリティに関わる重要な改善** も配信しています。このパッチが有益である理由は、軽量のアップデートであるため、組織では社内システムを止めることなく自動的に適用できる点です。たとえば、2024年6月から2025年4月には、AppleはmacOSのメジャー／マイナーバージョンに関連するCVEについて、**20件のセキュリティアップデート**をリリースしています。

脆弱性の実例：TCC（透明性、同意、制御）バイパス

Appleのオペレーティングシステムでは、重要なセキュリティフレームワークとしてTCC（透明性、同意、制御）が実装されており、ユーザは個々のアプリの機密データ（マイク、Webカメラ、フルディスクアクセスなど）へのアクセス要求を承認または拒否するよう求められます。TCCバイパスという脆弱性は、この制御に問題が生じ、アプリケーションがユーザに知られることなく同意なしで機密情報にアクセスできる状態を指します。この場合、攻撃者はユーザに通知することなく、ファイルやフォルダ、健康データ、マイク、カメラなどに不正にアクセスできます。

Jamf Threat Labsは、MacデバイスのFile Providerに影響する**TCCバイパスの脆弱性CVE-2024-44131**を発見しました。この脆弱性は、直ちにAppleのmacOS 15パッチで対処されました。このCVE-2024-44131のようなCVEが存在することから、組織に予期せぬ動作を検出しブロックできるツールを導入する必要性が高まっています。積極的にアプリの動作を監視し、不正なデータアクセスを禁止する体制を整えれば、脆弱性が見つかった場合でも、その修正前に先手を取って対応できます。

最近のAppleのリリース（注：本レポートは2025年4月に執筆されました）から、注目すべき脆弱性を以下に示します。

AppleのCVE修正リリース	日付	脆弱性スコア	影響
macOS Sequoia 15.4.1	2025年4月	CVE-2025-31200 CVSS – スコア：7.5 | 深刻度：高	CoreAudio
macOS Sequoia 15.4	2025年3月	CVE-2025-24234 CVSS – スコア：7.8 | 深刻度：高	AccountPolicy
macOS Sequoia 15.4	2025年3月	CVE-2025-24180 CVSS – スコア：8.1 | 深刻度：高	Authentication Services
macOS Sequoia 15.3	2025年1月	CVE-2025-24085 CVSS – スコア：7.8 | 深刻度：高	CoreMedia

前述のとおり、脆弱性はソフトウェア開発に付き物です（エラーの発生頻度はコード1,000行あたり約25個）。そのため、セキュリティ担当者にとって重要なのは、これらの脆弱性を監視し、データを保護するための対策を講じることです。オペレーティングシステムを最新の状態に保てない場合（アプリケーション/エージェントのテスト時など）もありますが、組織は常に注意を怠らず、保護を維持する必要があります。

問題は、単にオペレーティングシステムに脆弱性があることではありません。2024年11月下旬に、米国サイバーセキュリティ・社会基盤安全保障庁（CISA）から、**2023年において最も頻繁に悪用された脆弱性に関するレポート**が発表されました（リンク先のレポートは執筆時点での最新版です）。このレポートでは、CVEおよび脅威アクターの各脆弱性の利用方法を含め、上位15件の脆弱性が詳しく解説されています。これらの脆弱性は、企業の従業員や学生が日常的に利用するコンピューティングプラットフォームやアプリで発生していました。レポートによると、「2023年は、悪意あるサイバーアクターが企業ネットワークの侵害に利用できるゼロデイ脆弱性が2022年に比べて増加し、優先度の高いターゲットに攻撃を仕掛けることが可能になっていました」。CISAはさらに、開発者やエンドユーザ組織向けの脆弱性の軽減手段も提示しています。このレポートで示された、エンドユーザ組織向けの対策は次のとおりです。

- ソフトウェア、OS、アプリ、ファームウェアを速やかにアップデートする
- 自動アセット検出を定期的に実行する
- 堅牢なパッチ管理プロセスを導入する
- セキュアなベースライン構成をドキュメント化する
- セキュアなシステムバックアップを定期的に実行する
- サイバーセキュリティインシデント対応計画を定期的に更新する

上記のように、AppleはOSに脆弱性が認められた場合、定期的にアップデートを提供しています。そのため、繰り返しになりますが、ソフトウェアのアップデートは不可欠です。組織がOS（と従業員が日常的に使用するビジネスアプリ）をアップデートする最も一般的な手段は、モバイルデバイス管理ソリューション（MDM）を利用することです。しかし、サイバー防衛の層はこれだけではありません。インシデント対応計画の策定、テレメトリの収集および分析、社内パッチ適用プロセスの確立などもすべて、組織が問題を未然に防ぐ手段と言えます。これらの手段を実行することで、ソフトウェア脆弱性レベルの特定や、脅威ハンティングワークフローによるエンドポイントに潜むリスクの発見など、サイバー防衛層を拡充し、組織のリスク軽減を促進できます。

Jamf Threat Labsは、macOSのGatekeeper脆弱性（CVE-2023-41067）を発見しました。この脆弱性はLaunchServicesに影響するものであり、ユーザに適切なセキュリティプロンプトが表示されることなく、未署名、未公証のアプリケーションが実行される可能性があります。Gatekeeperは、インターネットからダウンロードされたアプリについて、有効なデベロッパIDで署名されていない場合に実行を禁止する第一防衛線です。このCVEは速やかにAppleのパッチで修正されたものの、脆弱性がどのようなシステムにも発生することの証拠となりました。管理とトレーニングを適切に行うことで、Jamf Threat LabsがGatekeeperに見つけたような脆弱性で引き起こされるリスクを軽減できます。

過去12ヶ月間の調査結果：

32%

の組織が重大な（パッチで修正可能な）脆弱性のあるデバイスを1台以上運用

Jamf CISOからのアドバイス

- **組織全体の脆弱性を可視化する：**
  エンドユーザのデバイスやインフラに存在する脆弱性を把握することは、セキュリティ対策の出発点として非常に重要です。まずは、どこにリスクが潜んでいるのかを可視化し、全体像をつかむことが効果的な対応の第一歩となります。こうして得られたデータを足がかりとして、アプリごとのフットプリントや潜在的なリスク、影響範囲などを分析できます。こうすることで、データに基づいた脆弱性の優先順位付けを始められます。
- **確実なパッチ適用プログラムを導入する：**
  MDMの視点に戻ると、環境の安全性と健全性を保つうえでは、常にソフトウェアやOSを最新バージョンまたはサポート対象のN-Xバージョンに維持できるツールを導入することが最も重要です。エンドユーザへの影響をゼロもしくは最小限に抑えてこのプログラムを進めることで、社内の協力を得やすくなります。
- **リスクベースのアクセス制御を導入する：**
  コンプライアンスに違反したデバイスが企業リソースへアクセスしようとした場合、そのアクセスは一時的に制限すべきです。エンドユーザには、最小限の手間でデバイスを再び準拠状態に戻せるような仕組みを整えることで、セキュリティとユーザ利便性のバランスを保つことができます。

パート3：ソーシャルエンジニアリング

ソーシャルエンジニアリングとは、攻撃者が個人をたくみに騙して、機密データや認証情報を提供させる行為です。世界経済フォーラムの**Global Cybersecurity Outlook 2025レポート**によると、「昨年ソーシャルエンジニアリング攻撃の被害を受けた組織は42%に上る」とされています。

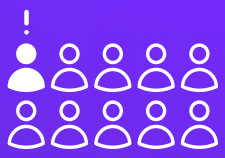
現在、組織が特に頻繁に被害を受けている脅威は、ソーシャルエンジニアリングの一種であるフィッシングです。モバイルデバイスは画面が小さく、持ち運びが容易で社外で使われることからフィッシングの主な標的になっていますが、Mac（およびすべてのデスクトップやPC）も脅威アクターにとっては格好の攻撃対象です。なぜなら、Macなどのデバイスを使用しているのは、サイバーセキュリティ上もっとも脆弱な要素である「ユーザ」だからです。

攻撃者の手法が巧妙化し、真実味を増している今、私たちの個人情報や業務上の情報の安全性は常に脅かされています。企業でのMacデバイス活用の普及に伴い、攻撃対象領域は拡大の一途をたどっています。攻撃者は無防備な被害者を騙すため、手口を工夫し、本物らしいインターフェースやユーザエクスペリエンス、コミュニケーション手法を駆使するようになっています。しかし、組織にも、継続的に従業員をトレーニングする、脅威防御ツールを導入するなど、ユーザとデータを保護するための安全策はあります。

過去12ヶ月間の調査結果：

25%

の組織がソーシャル
エンジニアリング攻撃に遭遇



1/10人

のユーザが悪意ある
フィッシングリンクをクリック

ました。記事においてJamf Threat Labsチームが着目したのは、「LinkedInでテック企業の人事部門の採用担当者を装ってユーザに接触する」という攻撃です。この攻撃では、まず攻撃者がユーザに、スキルを測るためと言ってコーディング問題のzipファイルを送信します（現代の開発職の求人ではよくある手順です）。ユーザがこのファイルを開くと、マルウェア（実際の例ではインフォスティーラー）が実行されるという仕組みです。今後も、ソーシャルメディアの利用およびソフトウェアのダウンロードについて従業員にトレーニングすることが、あらゆる組織で実践すべき重要なトピックと言えるでしょう。

フィッシングキャンペーンに悪用されたブランド上位20社

Jamfの調査により、フィッシング攻撃では特定の有名ブランドが頻繁に悪用されていることがわかりました。これは、これらのブランド名がユーザにとってわかりやすく、信頼を得ているからと考えられます。これらのブランドは以下の4つのカテゴリに分けられます。

1.	2.	3.	4.
エンターテインメント	**ビジネス**	**公共サービス**	**個人向けサービス**
Netflix	Outlook	United States Postal Service	Amazon.com Inc
Bet365	Microsoft 365	Gazprom	Telegram
Steam	Allegro	AT&T Inc	Meta Platforms, Inc
	InterActive Corp	Orange S.A.	Chase
	Tencent	DHL	WhatsApp
		BT Group	Yahoo, Inc.

Macは求人への応募、アプリのダウンロード、特定業界での仕事（クリプト産業など）をはじめ、さまざまな理由で使われています。そのため、一般的かつよく必要とされる用途が、脅威アクターのデータへの不正アクセスに悪用されています。上の表では、フィッシング攻撃に悪用されたサイトのうち上位20個を、4つのカテゴリに分けて示しています。

これらのブランドは企業や個人にとって人気で、評価が高く、影響力も強いことから、悪意あるアクターがユーザにソーシャルエンジニアリング攻撃を行う際に利用されていると考えられます。これらの有名ブランドは、巧妙化するサイバー攻撃において、自らの意思とは無関係に利用されているのです。また、脅威アクターに利用されるブランドは、上表のものだけに限らないことも注目に値します。昨年は上記20社が上位を占めていましたが、来年、来月、あるいは来週にも上位が入れ替わっているかもしれません。ただ、この表を見れば、攻撃者の考えは明らかです。それは、ブランドが長年かけて得た顧客からの信頼を悪用してユーザを攻撃することです。リモートワークやハイブリッドワークの広まりに伴い、ユーザを騙してクリックさせる新しい攻撃手段が使われるようになっているのです。

現代では、個人情報は絶えず危険にさらされています。企業でのMacの普及に伴い、攻撃対象領域は拡大の一途をたどっています。攻撃者は無防備な被害者を騙すため、手口を工夫し、本物らしいインターフェースやユーザエクスペリエンス、コミュニケーション手法を駆使するようになっています。しかし、組織にも、継続的に従業員をトレーニングする、脅威防御ツールを導入するなど、ユーザとデータを保護するための安全策はあります。

Jamfは、サンプルの**デバイス140万台**に対し、過去12ヶ月間で**約1,000万件のフィッシング攻撃**が行われたことを確認しました。さらに、これらの攻撃のうち**約1.5〜2%**はゼロデイ攻撃として分類されていました。攻撃者は定期的に新しいドメインを立ち上げ、そのドメインが検出されて一般的なデータベースに悪意あるものとして登録される前にフィッシング攻撃に利用していることが確認されました。そのため、組織としてゼロデイフィッシング攻撃を特定および検証することで、まだ検出されていない新たなフィッシングサイトにユーザが騙される事態を防止できます。

Jamf CISOからのアドバイス

- **堅実なトレーニングプログラムを導入する：**
  これは、Jamfの成功の秘訣です。当社では、工夫を凝らしたフィッシングキャンペーンやゲーム的なトレーニングを展開しているほか、希望するユーザには単発のトレーニングも提供しています。また、365日にわたりユーザがフィッシングメールを報告し、報告内容についてシームレスに確認とフィードバックを受けられる仕組みも構築しています。このように、Jamfではトレーニングを「単発的な年次研修ではなく、継続的かつ実践的な教育の一環」として位置づけています。
- **新しいトレンドや戦術を把握する：**
  この対策は当たり前のように思われるかもしれません。しかし、攻撃者というのは利用できるものは何でも使う存在であり、新しく画期的なものやニュースで話題になっているものが利用されることもしばしばあります。このような状況に対処するには、トレーニングや防衛策を適応させる必要があります。適応の結果、ユーザを不安にさせてしまうこともあるため、透明性が重要になります。攻撃者は、あえてユーザの感情を揺さぶって判断力を鈍らせようとします。トレーニングでは、そうした手口に冷静に対処する力を養います。
- **アプローチを多層化する：**
  単独の手段やツールで、標的型フィッシングキャンペーンの被害を防止することはできません。複数の角度から対策を検討し、悪意あるドメインをブロックする、多要素認証（MFA）を導入する、ゼロトラスト手法を採用する、不正なパターン規制を適用するなどの手段を講じましょう。これらの手段は1つや2つでは不十分な場合もありますが、複数のセキュリティ層を設けることで、最も現実的に次のフィッシング攻撃の被害を防止できるでしょう。

まとめ

Macマルウェアは進化しています。しかし、適切な措置を講じれば、macOSマルウェアのリスクを軽減できます。たとえば、テレメトリを収集・分析することでマルウェアを特定およびレポートできます。脅威アクターは絶えずユーザやシステムを侵害する新しい方法を模索していますが、適切なツールを導入すれば、悪意あるソフトウェアによる被害を抑えられます。

適切なセキュリティハイジーンを確立することで、リスクを軽減できます。オペレーティングシステムを定期的にアップデートし、不要なコントロール（公式以外のアプリストアなど）を無効にすれば、社内ベースラインや外部フレームワークへの準拠を促進できます。社内アプリストアを構築しアプリ（特にプライベートアプリやカスタムアプリ）を継続的に審査することで、適切にアプリ脆弱性の監視、修正、パッチ適用を行えます。

ソーシャルエンジニアリングが、機密情報にアクセスする攻撃手段として広く使われるようになっています。サイバー攻撃の90%は、フィッシングが起点です。現在のフィッシングの手口はさまざまであり、メールとは限りません。ユーザと組織を守るためには、デバイス全体（ブラウザやアプリ含む）に保護対策を導入することが重要です。

jamf

Macを狙う脅威について詳しく知りたい方は、こちらから、または販売代理店までお問い合わせください。