jamf

セキュリティ360：
最新トレンドレポート
モバイルデバイス

序文

小売業務から医療現場の運用まで、さまざまな業界やユースケースにおいて、ビジネスリーダーはモバイルデバイスの使い方を一新し、従業員の働き方を改革し、組織としての成果の最適化を推進しています。業界を問わず、仕事に使用する機器がモバイルデバイス（スマートフォンやタブレット）だけという従業員は少なくありません。さらに現代の職場においては、従業員が場所や時間を問わず、希望するデバイスを用いて業務にアクセスできる環境の整備が重要視されています。

モバイルワーク普及の大きな要因のひとつは、業務におけるモバイルデバイスの利活用が本格化したことにあります。モバイルデバイスは、これまでの補助的な役割から、業務を遂行するための主要なアクセス手段として位置づけられつつあります。職場におけるモバイル活用はすでに一般化しており、現在では主要な業務プロセスへの統合がかつてない速度で進んでいます。現代の職場では、働く場所を問わず従業員の生産性を最大化するために、優れたユーザ体験と**高いセキュリティ**を両立したデジタル環境が不可欠です。

– Josh Stein、
製品管理担当VP

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、現在のモバイルデバイスを取り巻く環境を調査しています。

ユーザを騙し、モバイル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さまざまな攻撃ベクトルを分析評価しました。これらの攻撃対象はデバイスの脆弱性に限定されないため、分析対象には危険なアプリやWeb脅威も含めています。

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モバイル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。分析は2025年第1四半期、直前の12ヶ月間を対象に、90の国と複数のプラットフォーム（iOS、iPadOS、Androidデバイス）にわたって実施しました。

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、調査で見つかった脅威や脆弱性など、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。世界の実情を読者の皆さんに伝えることで、誤った通説を打ち払い、ユーザとデータを保護する手段の導入方法を広められれば幸いです。組織向けの一般的なベストプラクティスには以下のようなものがあります。

- 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
- コンプライアンスベースラインを設定および管理する
- 社内データの利用ポリシーを導入する

本レポートでは、世界中の組織にとって最優先事項と考えられる以下の4つのリスクカテゴリに分けて分析結果を紹介します。

I. モバイル狙いのフィッシング

II. 脆弱性管理

III. アプリのリスク

IV. マルウェアとスパイウェア

本レポートの分析は、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、デバイス、アプリ、ネットワークトラフィックのリスク監視および脅威とゼロデイ脆弱性の監視を担当するJamf Threat Labsチームおよびデータサイエンスチームが実施した、人間主体の調査の結果をまとめたものです。

本レポートの統計にはAppleデバイスとAndroidデバイスが含まれます。

Mac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。

モバイルの主要トレンド

I. 今年もフィッシングが企業の課題

フィッシングはいまだに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、iOS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。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、フィッシングなどの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。

II. 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、現在世界に存在しているCVEについての情報が公に提供されています。アップデートは不可欠ですが、組織で活用するにはパッチを適用しなくてはなりません。

AppleとGoogleでは、脆弱性が発見されると重要な情報を提供し、どのオペレーティングシステムアップデートでその脆弱性を修正できるかを知らせています。たとえば2025年には、Appleから **CVE-2025-24201**（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iOS 18.3.2がリリースされました。また、**GoogleはAndroidのセキュリティに関する公開情報** で、重大なゼロデイ脆弱性2件を含む43のセキュリティ脆弱性について説明しています。

III. セキュアなプラットフォームでも、アプリからリスクが生じる

AppleのApp StoreおよびGoogleのGoogle Playストアはともに、誕生以来ユーザや組織の保護を実施しています。Appleユーザの場合、Appleが「**ユーザの安全、セキュリティ、プライバシーに影響を及ぼす可能性のあるマルウェアやその他のソフトウェアがないことを確認するため、各アプリを検証**」しているので、App Storeから安全にアプリをダウンロードして利用できます。Androidユーザの場合、Google PlayストアがGoogle Playプロテクトを展開しています。それでもなお、脅威アクターの完全な排除には至っていません。過去5年間にわたりAppleは90億ドル以上の不正取引を防止してきましたが、**欧州連合（EU）デジタル市場法**（DMA）で代替のアプリストアの設立が認められ、「ゲートキーパー」に対しウォールドガーデン（閉鎖的なデジタルエコシステム）の開放が義務付けられました。このような代替アプリストアで配布されるアプリに課されるガイドラインは、AppleのApp Storeアプリに対するものとは異なるため、ユーザのセキュリティ、プライバシー、安全が脅かされるおそれがあります。Apple App Store外でユーザがアプリをダウンロードしたり他の決済システムを利用したりすることで生じるリスクとしては、ソーシャルエンジニアリング（フィッシングなど）やランサムウェア、消費者向けスパイウェアなどが挙げられます。

Androidデバイスについては、今年前半に**Googleが新種のトロイの木馬に関する警告を出し**、「750個以上の正規の銀行アプリやショッピングアプリが被害を受けた」と公表しました。EU圏内では、今やこれら2つの有名アプリストアはユーザによるアプリのサイドローディングを許可するよう義務付けられたため、脅威アクターが攻撃可能な領域が広がってしまっています。

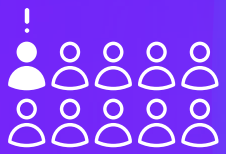
IV. モバイルデバイスには標的型攻撃のリスクがある

モバイルデバイスは、場所を問わず業務を行える柔軟性を提供します。特に、経営幹部やグローバルに活動するビジネスリーダーにとっては、業務遂行に不可欠なツールとなっています。しかし、保有するデバイスに知的財産や財務データなどの重要情報が含まれていることから、**こうした立場のユーザはサイバー攻撃の主要な標的となりがちです。**攻撃者は、より高い見返りを期待して、社会的なつながりが多く影響力のある人物を標的にする傾向があります。特に恐喝行為においては、そのような個人が狙われやすいのです。

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

I. モバイル狙いのフィッシング

現在、組織が特に頻繁に被害を受けている脅威はフィッシングです。米国サイバーセキュリティ・社会基盤安全保障庁（CISA）によると、「成功したサイバー攻撃の90%以上は**フィッシングメールから始まっていた**」とされています。

フィッシングは、モバイルデバイスのさまざまなチャネルから行われます。攻撃はもはやメールだけにとどまらず、テキストメッセージ（スミッシングと呼ばれる手法）、SNS、さらには偽のWebサイトへのリンクなど、さまざまな手段で行われています。

しかし、モバイルデバイスを狙ったフィッシング攻撃の成功率が高いのはなぜなのでしょうか。

まず押さえておくべきは、現在、**世界中のWebページ閲覧の62%以上**がモバイルデバイスから行われているという事実です。つまり、現在のインターネットトラフィックの大部分はモバイルデバイスがかかわるものであり、脅威アクターにとっては脆弱性を探す標的候補が増えているということです。

その反面、モバイルデバイスはコンパクトで、画面も小さいものです。この特性、つまりどこにでも持ち運べるサイズであるために、ここまでの人気を博しているとも言えます。さらに、このサイズのおかげで、組織では以下のような業務にモバイルデバイスを組み込むことも可能になっています。

- 小売業界（POSシステムや在庫管理）
- 医療業界（巡回看護や患者ベッドサイドでのケアを含む）
- 製造業界（オペレーターや機械への指示）
- 航空業界（電子フライトバッグやグランドスタッフ用機器）

しかし、このように便利なデバイスであるからこそ、ユーザは悪意あるフィッシング攻撃につい引っかかってしまうと言えます。モバイルデバイスは本質的に安全であるという認識はいまだに根強く残っていますが、これまでの事例が示すとおり、たった1つのリンクでデバイスが危険にさらされる現実があります。

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

モバイルデバイスは、新たな業務フローの導入や顧客との接点の効率化、ユーザエクスペリエンスの向上を可能にします。現代の働き方では、モバイルデバイスを補助あるいは主要機器として利用するのが当たり前になっています。職場でも家庭でも、私たちの暮らしとモバイルデバイスは切っても切り離せません。攻撃者はこの事実を基に、悪意ある活動を行っています。

今回の調査では、モバイルデバイスのエンドユーザを標的としたソーシャルエンジニアリング攻撃で、特定の人気ブランドが悪用されていることがわかりました。これらのブランドを、エンドユーザの信頼を悪用するためによく使われている**4つのカテゴリ**に分類しました。

仕事のメールにアクセスする、日用品を注文する、個人の銀行を利用するなど、モバイルデバイスを使う理由は無数にあるため、脅威アクターはよく必要とされる一般的な用途を悪用して、データへのアクセスを得ています。以下の表は、ソーシャルエンジニアリングで悪用されたブランドの上位20社を、4つのカテゴリで示したものです。

1. エンターテインメント	2. ビジネス	3. 公共サービス	4. 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.

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。その信頼度から、正規のコミュニケーションを装った悪意あるコンテンツにユーザが騙されやすくなります。

このリストには昨年最も悪用されたブランド20社を記載していますが、決して網羅的なものではありません。攻撃者は常に状況に応じて変化しており、模倣するブランドはいつでも変わる可能性があるからです。そのため、このリストから読み取るべきなのは、攻撃者はこうしたブランドが長年かけて築き上げた信頼を利用し、ユーザを騙して搾取しているということです。

現代では、個人情報は絶えず危険にさられています。日常および仕事に使われるモバイルデバイスが増えるにつれ、攻撃者の手が及ぶ範囲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。

II. 脆弱性管理

脆弱性とは、セキュリティ、完全性、可用性の侵害に悪用されかねないシステム、アプリケーション、またはプロトコルの弱点や欠陥を指します。**Apple** および**Google** は、それぞれのオペレーティングシステムに影響する既知の脆弱性のリストを公開しています。しかし、これは同時に、AppleまたはGoogleからアップデートやセキュリティパッチが提供される前にこうした脆弱性が「世に出てしまう」ことを意味します。2024年1月1日から2025年4月1日の期間に、Appleは**29件のセキュリティアップデート** と、iOSのメジャー／マイナーバージョンに関連するCVEを公開しています。同じ期間に、Googleは「Androidのセキュリティに関する公開情報」で**39件のシステム脆弱性**と関連するCVEを公開しています。

また、AppleとGoogleはともに、ソフトウェアアップデートの合間に単独のセキュリティパッチも提供しています（Appleは**緊急セキュリティ対応**、Googleは**Androidセキュリティパッチ**）。このパッチが有益である理由は、時期に応じたアップデートであることです。つまり、組織からすれば、大規模アップデートを待つことなくアップデートを自動で適用できます。

巧妙かつ複雑化する現代の**サイバー脅威**に対しては、個人も企業もデバイスの更新を怠らず、常に警戒を続ける必要があります。デバイスを**アップデート**するだけでなく、そのアップデートが**本物かどうか**をきちんと確認することも大切です。

Jamf Threat Labsは、攻撃で使われる手法の1つである「永続化」について詳しい調査を行いました。その結果、「攻撃者はiOSの設定インターフェースを悪用し、iOSのアップデートがあると伝えるプロンプトや通知ごとシステムアップデート設定を改ざんできる」ことがわかりました。

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
iOS 18.4.1およびiPadOS 18.4.1	2025年4月	CVE-2025-31200 CVSS – スコア：7.5	深刻度：高	CoreAudio
iOS 18.4およびiPadOS 18.4	2025年4月	CVE-2025-30430 CVSS – スコア：9.8	深刻度：緊急	Authentication Services
iOS 18.3およびiPadOS 18.3	2025年1月	CVE-2025-24085 CVSS – スコア：7.8	深刻度：高	CoreMedia
iOS 18.3およびiPadOS 18.3	2025年1月	CVE-2025-24154 CVSS – スコア：9.1	深刻度：緊急	WebContentFilter

アップデート対象のAOSP*バージョン	日付	脆弱性スコア	影響
13、14、15	2025年4月	CVE-2025-26416 重大度：重大	権限昇格
15	2025年3月	CVE-2025-22403 重大度：重大	リモートコード実行
15	2025年2月	CVE-2025-0096 重大度：高	権限昇格
12、12L、13、14、15	2025年1月	CVE-2024-43771 重大度：重大	リモートコード実行

*Androidオープンソースプロジェクト

AppleおよびGoogleのウェブサイトに記録されているこれらの脆弱性を見ると、脆弱性はソフトウェアを開発すれば必ず生じることがわかります。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。

そのためには、OSを常に最新の状態に保ち、アップデートを展開できるツールを活用することが有効な手段のひとつです。

オペレーティングシステムをアップデートしてセキュリティポスチャを確保する

企業にとって、脆弱性を軽減しコンプライアンスを維持する最善の方法は、デバイスのオペレーティングシステムをアップデートすることです。前ページに示したように、AppleおよびGoogle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。

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一般的な手段は、モバイルデバイス管理（MDM）ソリューションを利用することです。MDMを導入すれば、各管理対象デバイスにインストールされているOSも詳細に把握できます。しかし、ほとんどの組織では多数のデバイスがさまざまな用途に使用されており、ユーザによって使用するアプリも異なります。そのため、組織内の全デバイスのオペレーティングシステムを最新に保つことは困難（かつ、導入前にアプリをテストする場合などは往々にして実現不可能）です。

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

55.1%

の業務用モバイルデバイスのOSに脆弱性あり

調査により、最新のセキュリティパッチを適用せずにモバイルデバイスを運用している組織があると判明しました。調査データでは、脆弱性のある全Androidデバイスの**4.8%**が社内リソースへのアクセスに使用されていました。

モバイルデバイスの活用によって、働き方を自由に選べるようになります。車の中で仕事の電話を受けたり、現場作業員や接客担当者の業務フローの拡充まで、モバイルデバイスによりさまざまな仕事の可能性が広がります。しかし、他のコンピューティングデバイスと同じく、モバイルデバイスのシステムも脅威アクターの攻撃には脆弱です。組織がモバイルデバイス全体の脅威を軽減するためにできる対策としては、使いやすさとセキュリティを両立したツールを導入する、従業員向けのトレーニングを行う、その時点で一般的な脅威を把握することが挙げられます。

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。

III. アプリのリスク

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、攻撃者が脆弱性を悪用してできることを含め、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、組織の従業員および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ケーション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

アプリを「危険」にする要素について考えてみると、危険なアプリの特徴としては以下のようなものがあります。

- 異常な特性
- 悪意のあるコードパターン
- 危険なアクセス許可
- 危険な動的挙動
- 疑わしい開発者のプロファイル

組織はアプリのバージョンやデータ漏えいアプリなどを可視化することで先手を打ち、リスクを迅速に調査および修正する準備を整えられます。

企業にとって重要なのは、アプリケーションの健全性を完全に把握することです。危険なアプリを特定し修復するために、組織が注意すべきデータポイントの一例を以下に示します。

- 最新版でないアプリをインストールしているユーザの数
- 特定のアプリバージョンを使用しているユーザの数
- 暗号化の実装に問題があり、機密データを保護されていないネットワーク流出させてしまうアプリのリスト
- デバイスの別の部分に保存されているデータにアクセスする権限を求めるアプリ

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が実装されており、ユーザは個々のアプリの機密データ（写真、連絡先、位置情報など）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。そのため、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、iOS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iOS 18.0パッチで対処されました。CVE-2024-44131のようなCVEが見つかるたびに、組織のデバイスを最新に保つことが必須であると強く認識されるでしょう。

App Storeのセキュリティと実際の不正未遂

前述のとおり、Appleは過去5年間で90億ドル以上の不正取引を防止しました。2024年だけでも、同社が防止した不正取引の額は20億ドルを超えています。さらに、同年には次のような成果も上げています。

- 14万6,000個以上のデベロッパアカウントを不正行為の疑いで停止
- デベロッパとして登録済みの13万9,000人を追加で却下
- 隠された機能や文書化されていない機能を有しているとして4万3,000本以上のアプリの登録を却下
- 他のアプリを模倣しているか、スパムと判明したか、ユーザを誤解させる32万件以上のアプリ登録を却下
- 海賊版アプリストアで配布されていた違法なアプリ1万本以上を検出およびブロック

App Store は、一般的に、安全かつ簡単にアプリを入手する手段として、最も信頼性が高く、操作性に優れ、プライバシー保護にも配慮されたプラットフォームとされています。iOS向けのApp Storeはサンドボックスとユーザからの権限リクエストを利用しており、デバイス上で署名済みコード以外が実行されることはありません。しかし、上記データからわかるとおり、脅威アクターは後を絶たず、不正行為はいまだに試み続けられています。2008年のApp Storeのサービス開始以来、Appleはこのストアを安全かつ信頼できるアプリの入手先とするべく取り組み、ユーザと開発者を保護してきました。しかし、「サイドローディングアプリ」、つまりApple以外のアプリストア（AltStoreなど）で配布されるアプリに、このような保護は適用されません。

Jamf CISOからのアドバイス

モバイルセキュリティの効果を発揮させるには、多層的なアプローチが必要です。信頼できるベンダー製の最新ハードウェアと最新のオペレーティングシステムを組み合わせるだけでは、組織や機密資産を侵害から守りきれません。アプリケーションも含む技術スタックの各層に、適切なセキュリティ対策を施す必要があります。

- **組織の機密度の高いモバイルアプリを対象としたアプリ審査プログラムを導入する：**
  まず最も重要なアプリを対象として、組織全体で最新かつセキュアなバージョンを運用していることを定期的に確認しましょう。次第にプログラムの対象を広げ、エンタープライズアプリストアに登録するすべてのアプリを審査するようにします。
- **望ましくないアプリケーションがインストールされたデバイスを「コンプライアンス違反」扱いにするポリシーを策定する：**
  危険なアプリが更新または削除されるまでは、こうしたリスクのあるデバイスからSaaSアプリケーション、重要なデータセンター、リモートワークロードへのアクセスを禁止します。
- **トレーニングプログラムでモバイルアプリのセキュリティについて指導する：**ユーザが仕事で持ち歩くデバイスでアップデートが必要になった際に各自で導入できるようにして、ユーザもセキュリティ対策の一員に組み込みます。
- **組織に代替のアプリストアが必要ない場合**は、業務用デバイスから代替ストアへのアクセスを禁じるポリシーを定めます。さらに、正規ソースのアプリ以外がデバイスで使用されないように、サイドローディングアプリも禁止します。

Jamf Threat Labsチームは、サイドロードしたソーシャルメディアアプリにより写真を監視し、攻撃者のサーバへアップロードできると示すデモを公開しました。このアプリは「既存のものを改変しているが、機能は完璧」です。同チームは以下のような、明確なセキュリティ強化策を提示しています。

- アプリプライバシーレポートを有効化し、定期的に確認する
- アプリの権限を注意深く選択する
- 機密情報を保存しないようにする

アプリのダウンロードは信頼できるソース（App Storeなど）からのみ行う

ネイティブアプリとクラウドホスト型Webアプリのどちらにも、リスクは存在します。
クラウドホスト型アプリの方が攻撃対象領域が広いため、リスクにさらされやすいと言えます。しかし、適切な可視化機能、制御機能、修復機能を用意すれば、危険なアプリが職場に持ち込まれても、そのリスクを軽減できます。

IV. 標的型攻撃および高度なスパイウェア

2021年以降、**Appleは150ヶ国以上のユーザに脅威の通知を送っています**。この通知は、金銭目当てのスパイウェア攻撃の標的となっているユーザ（大部分はジャーナリストや政治家、外交官などの著名人）にその旨を知らせ、サポートするためのものです。また2025年4月下旬に、Appleは「政府機関の関与するスパイウェアの標的になったと思われる人物に通知を送った」とされています。しかし、攻撃者の標的はAppleだけではなく、あらゆる種類のオペレーティングシステムやアプリも狙われています。**The Citizen Labは、**「AndroidデバイスのWhatsAppや他のアプリにスパイウェアが組み込まれていた」と伝えています。

Appleの脅威の通知で扱われるようなマルウェアやスパイウェアは、現在組織と個人が直面している最も高度な脅威の一種です。しかし、こうした高度な脅威についても、組織のあらゆる階層のユーザを守る手段はあります。

Appleはユーザ全員にマルウェア対策を紹介しており、本レポートではその多くをすでに示しました。Appleが紹介する対策の具体例を以下に示します：

- デバイスのソフトウェアを最新版にアップデートする（最新のセキュリティ修正プログラムが含まれるため）
- パスコードでデバイスを保護する
- Appleアカウントに2要素認証を使用し、強力なパスワードを設定する
- アプリはApp Storeからインストールする
- オンラインでは強力なパスワードを使用し、使い回さないようにする
- 知らない人から送られたリンクや添付ファイルはクリックしない

Jamf Threat Labs：被害者に気づかれずにデバイスを侵害する

Jamf Threat Labsは、セキュリティソフトウェアのないデバイスを、被害者に気づかれることなく侵害する様子のデモを公開しました。このデモでは、攻撃者がメールや業務メッセージ、2要素認証などの個人データに不正にアクセスできることが示されました。さらに、組織および個人のデータを保護する以下の対策も紹介されています。

1. 会社所有および個人所有のデバイスの両方にコンプライアンス維持のためのセキュアな構成を適用する
2. エンドユーザのプライバシーに配慮し対象を絞った措置で、脅威の防止と監視を実現する
3. すべての管理対象デバイスにデバイス暗号化を適用する

Jamf CISOからのアドバイス

モバイルデバイスでは、他のコンピューティングデバイスほどマルウェアが蔓延していません。しかし、検出されたマルウェアの多くは、非常に高度な手口で個人を狙った攻撃を仕掛けていました。

- モバイル狙いのマルウェアの被害を組織が受けることはないと**油断してはいけません。**昨年だけでも、約100ヶ国のユーザにAppleからスパイウェアによる侵害の通知が送られています。
- **少なくとも1名のモバイルセキュリティ担当者を設置**し、組織のモバイルデバイスの健全性に関するレポートを定期的に提供してもらうべきです。電話の盗聴、標的型フィッシング、パフォーマンスの低下など、異常な挙動の兆候と見られるすべてのインシデントを一覧化します。可能であれば、デバイス管理とセキュリティツールからのテレメトリストリームを構築し、得られたデータをセキュリティ専門チームで活用します。モバイルも、他のエンドポイントと同様に扱いましょう。
- **可能な範囲でモバイルシステムのデータを収集し、ゼロデイ攻撃の痕跡や兆候の有無を調査することが推奨されます。**この場合、専門家を社内に雇用するか、外部の専門家と契約する必要があります。組織に専門のセキュリティアナリストがいるのであれば、チーム内にモバイルフォレンジックの専門家を育成しましょう。

まとめ

モバイルフィッシングは、攻撃者が機密情報へアクセスするために最も一般的に用いる手口のひとつです。教育プログラムを実施し、攻撃手法やトレンドの変化に応じて内容を柔軟に見直し、多層的なセキュリティ対策を講じている組織は、さまざまな角度から脅威に対する防御力を高めることができます。

どのようなソフトウェアにも、脆弱性は付き物です。適切なセキュリティを確立することで、脆弱性の原因となる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。

アプリの不適切な管理や利用は、セキュリティリスクを招くおそれがあります。アプリ本体に限らず、不正なネットワーク接続を行っているアプリもリスク要因となります。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。

APT攻撃とスパイウェア攻撃の頻度が増加しています。世界中の組織がこれらの脅威（たいていは国家または専門グループによるもの）の被害を受けており、多くの場合、機密データ入りのデバイスを持つ著名人が狙われています。組織として多層防御型のセキュリティ戦略を運用し、モバイルも他のデバイスと同様に扱うことで、モバイルデバイスのエコシステム、およびデバイスの接続対象となるデータを確実に保護できます。

業務用リソースへのアクセスや組織のポリシー遵守が求められる会社所有のデバイスについては、明確かつ強制力のある利用規程を策定し運用します。個人所有のデバイスについては、**Apple提供のデバイス用** プライバシー保護**など、追加のプライバシー対策も適用する必要があります。**

jamf

モバイルデバイスを狙う脅威について詳しく知りたい方は、こちらからお問い合わせください。

www.jamf.com/ja/