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

目次

はじめに

Jamf Security 360 は、絶えず変化し続ける脅威の現状を深く考察したレポートです。本レポートは、お客様の環境で実際に確認されたセキュリティ事案、Jamfの脅威リサーチチームによる新たな発見、そして世界情勢や業界動向から得られた知見に基づいています。今回のレポートでは、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。

ここでは、多岐にわたる深刻な攻撃経路を検証します。攻撃者がどのように侵入の糸口を掴み、システム間を移動し、最終的にデータの窃取や実害を引き起こすのか、そのプロセスを詳しく紐解きます。攻撃者は自らの目的を達成するため、デバイスやソフトウェアの脆弱性を突き、アプリやWeb通信に悪意あるコードを混入させます。さらに、組織最大の弱点であるユーザも標的にし、あらゆる手段を講じてきます。

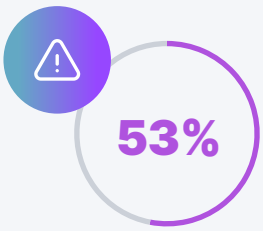
脅威トレンドの分析のみならず、JamfのCISOによる専門的な考察も盛り込み、モバイル管理を担うセキュリティの責任者やIT担当者の皆さまにとって、実務に役立つ洞察をご提供します。

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170万台を超えるiOSおよびAndroidデバイスをサンプルとして匿名性を確保した形で分析しました。調査は2025年末に実施され、過去12か月間の動向を振り返るとともに、世界各国の多岐にわたる地域を対象としています。

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。

主な調査結果



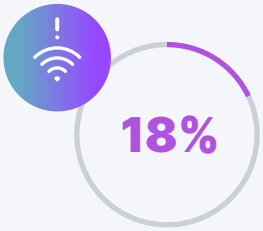
OSのバージョンが古く、危険な状態のデバイスを1台以上使用している組織の割合

最新バージョンでないOSは、パッチが適用されておらず、脆弱性が悪用できる状態です。アップデートの自動化と強制がデバイスの保護に非常に効果的です。

1台/850台

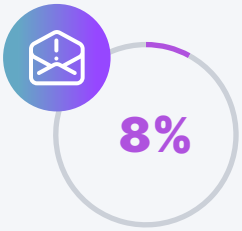
ジェイルブレイクされている業務用デバイスの数

Jamfによるデバイス検知とコンテキストベースのアクセス制御により、重要なリソースは侵害から守られました。



セキュリティリスクのあるWi-Fiに接続している従業員がいる組織の割合

危険なWi-Fiスポットは、偽装アクセスポイントや中間者攻撃（AiTM）といったインフラへの脅威を招く要因となります。特に、こうしたリスクへの対策がデバイスに施されていない場合は、その危険性がさらに高まります。



ユーザがフィッシングリンクをクリックしたデバイスの割合

手口こそ毎年少しずつ変わってはいるものの、フィッシング攻撃はアカウント侵害を試みる攻撃者が依然としてよく使う方法です。適切な対策を取らない場合、甚大な影響が発生するおそれがあります。

ゼロクリック攻撃とブラウザ攻撃

これまで同様、よく使われる効果的な手法

OSとソフトウェアのどちらも、脆弱性の発見が後を絶ちません。脆弱性は多様なスパイウェアファミリーで攻撃者が機密情報を収集するための鍵となっています。本レポートでは、モバイルデバイスのリスクを戦略的に軽減する重要性を説明します。

企業における主要なセキュリティトレンド

モバイルデバイスは、場所を選ばない柔軟な働き方と、業務の効率化の両立を支えています。どのようにデバイスを活用・管理し、どのような脅威にさらされているか。その実態に合わせて、セキュリティも進化させる必要があります。

攻撃者に隙を与えないよう、多くの組織がアタックサーフェス（攻撃対象領域）縮小に向けた戦いを繰り広げています。コントロールやポリシーを実装し、IT環境に最高のセキュリティソフトウェアをインストールして対策してはいるものの、攻撃は高度化し、いつまでもなくなりません。

攻撃対象領域には多数の構成要素があります。本レポートでは、多くの組織が管理に苦慮し攻撃者が頻繁に悪用する主要なリスクを詳しく解説します。あわせて、壊滅的な被害を未然に防ぐための具体的な対策についても提示します。

1. ソフトウェアとデバイスの脆弱性：避けて通れないビジネス上のリスク

モバイルデバイスのOSは細心の注意を払って開発されていますが、それでも完璧はありえません。2025年には、48,000件以上のCVEレコードが公開されました。これほど膨大な数の脆弱性をすべて把握し、対処するのは容易なことではありません。

しかし、開発者側もこの状況を理解しているからこそ、セキュリティパッチを次々とリリースしているのです。こうした最新の保護策を現場のデバイスへ迅速に届けることが、管理チームの重要な役割です。そのパッチを適用していますか？OSを最新の状態に保っていますか？セキュリティのベストプラクティスに従っていますか？重要なのは、デバイスをどのように構成するかです。

攻撃者は欠陥を悪用します。こうして攻撃対象領域は拡大します。

2. モバイルアプリ：利便性の向上と表裏一体の脅威

モバイルデバイスを使う仕事にはアプリが欠かせません。皆さんの会社でも、デバイスに数十、数百のアプリがインストールされていることでしょう。アプリそれぞれに固有のリスクがあります。モバイルマルウェアの発生自体は比較的稀ですが、プライバシーの侵害、サプライチェーンの脆弱性、そして不適切なデータ取り扱いといったリスクは、依然として潜在的な脅威となっています。

最新状態に保つ必要があるのはアプリも同じです。開発者も脆弱性のパッチ修正に取り組んでいます。アプリのライフサイクル管理が極めて重要です。同じく、セキュリティと従業員のプライバシーのバランスを取ることも大切です。

アプリは潜在的なリスクを何倍にも増やします。こうして攻撃対象領域は拡大します。

3. ネットワークとWebのリスク：堅牢なデバイスをも脅かす死角

保存されたデータであれ、転送中のデータであれ、その保護は基本中の基本です。保護を確実にするには、ネットワークインフラとユーザの行動を理解する必要があります。従業員は、AitM攻撃を受けるおそれのある、保護されていないWi-Fiスポットに接続しがちです。デバイスを適切に構成しないと、データが無防備になります。

フィッシングやその他のWebリスクは、今なお猛威を振るい続けています。攻撃者は、エンターテインメント、ビジネス、公共サービス、金融など、さまざまな分野のオンラインコンテンツで人気サイトを模したサイトを作成しています。また、攻撃者の手口が生成AIで巧妙化していることもあり、偽サイトに騙されるユーザが後を絶ちません。

ユーザの誤操作や外部ネットワークの利用は、制御不能な侵入口となり、アタックサーフェス（攻撃対象領域）を拡大させる要因となります。

4. 複合的なリスクの増大と高度な脅威の出現

デバイスやアプリの脆弱性、ネットワーク構成、ユーザのリテラシーといったさまざまな要因が、セキュリティ体制の弱点となり、侵害の入り口となります。攻撃対象領域が大きくなるほど、対策が難しくなります。ここに挙げた3種類のリスクは、標的型攻撃によく悪用されます。

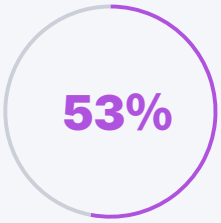
こうしたリスクの拡大は、持続的標的型攻撃（APT攻撃）やスパイウェアといった、より深刻な攻撃への入口を開く可能性があります。2025年、Jamf Threat Labsではゼロクリック攻撃とワンクリック攻撃を足掛かりにした継続的なエクスプロイトを観測しました。企業の経営層や政治家、活動家、ジャーナリストが特に狙われやすい傾向にあります。

2025年に発生した中で非常に悪質度の高いゼロクリック攻撃やワンクリック攻撃をいくつか調査したところ、それらの攻撃は機密情報を盗み出すことを目的とし、デバイスの複数のコンポーネントを悪用したものでした。この調査結果については、後ほど説明します。

デバイスの脆弱性

安全も危険も、モバイルOSが基礎となる

デバイスのOSを支えるコードベースは膨大かつ複雑で、常に潜在的な脆弱性を孕んでいます。人間は誤りを犯しがちであることから、コードにはどうしても脆弱性が入り込みます。しかし、人間は賢くもあります。知恵の働く攻撃者は悪用できそうなものを常に探し回っています。



OSバージョンが古く、危険な状態のデバイスを1台以上使用している**組織**の割合

CVEとは？

共通脆弱性識別子（CVE）プログラムは、サイバーセキュリティコミュニティが発見した脆弱性をデータベース化したものです。CVE項目それぞれに、影響を受けたソフトウェアやライブラリ、重大性スコア、考えられる悪用方法が記載されています。

2025年の注目すべき事例を見てみましょう。いずれも、実際の攻撃での悪用が確認されています。これらのCVEはiOS 18.4.1でパッチが適用されました。

CVE-2025-31200

重大度：9.8（重大）

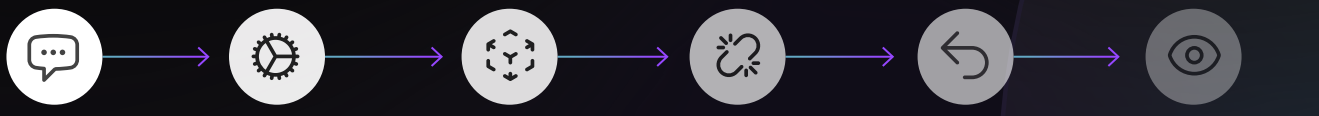
悪意を持って作成されたメディアファイルに含まれるオーディオストリームを処理するとコードが実行される可能性がある。

CVE-2025-31201

重大度：9.8（重大）

任意に読み書きできる権限を持つ攻撃者がポインタ認証を回避できる可能性がある。

攻撃者はこれらの脆弱性を連鎖的に悪用してデータを盗み取り、スパイウェアを導入させます。あるシナリオを想定してみましょう（説明のために大幅に簡略化しています）。



社会的影響力の高い特定の標的に対し、悪意のある音声ファイルを含む、巧妙に作り込まれたメッセージが届く

ユーザが一切操作せずとも、デバイスがプレビュー表示のために音声メッセージを自動的に処理

処理中のメモリ破壊により、データの任意読み書き（本来許可されない操作）が可能になる

ポインタ認証を回避することで、攻撃者は偽造した正規のコードポインタを作成できるようになる

攻撃者はプログラムの実行フローを書き換え、悪意のあるペイロード（実行コード）へと誘導

デバイスが完全に乗っ取られ、密かな監視活動が開始される

解説

- **標的型ゼロクリック攻撃：**ユーザが何もクリックしなくてもデバイスが侵害されます。標的となるのは、ジャーナリスト、政治家、経営幹部など、注目を集める個人であることが多いです。
- **脆弱性の積み重ね：**攻撃者は悪用できそうな脆弱性を注意深く探しており、その発見に長けています。
- **パッチが重要：**これらの脆弱性はiOS 18.4.1で修正されています。デバイスをアップデートしていない場合、データが保護されていません。

デバイスをアップデートする重要性をおわかりいただけたでしょうか。アップデートの実施が簡単なわけではありません。ユーザがデバイスのアップデートを躊躇する背景には、さまざまな理由があります。

- 新機能/インターフェイスを使用したくない
- 新しいOSバージョンに対するアプリの互換性
- 業務フローの阻害/リソースの制約

これまで見てきた通り、古いバージョンのソフトウェアが放置されているケースは非常に多く、常に最新の状態を維持することは容易ではありません。最新OSへの強制アップデートやバージョン管理を行うことは、2025年にJamf Threat Labsが分析したような、深刻な影響を及ぼす脆弱性からデバイスを保護することに直結します。

攻撃者は脆弱性を悪用し、ゼロクリック攻撃ベクトル（画像や音声ファイルの解析など）やワンクリックブラウザ攻撃を成立させます。セキュリティパッチやベンダーによる対策があるとしても、攻撃者は侵害に使える新しい脆弱性を発見して悪用できるため、脆弱性からユーザを守るにはモバイルデバイスの定期的なアップデートが非常に重要です。以下に、2025年に発見された脆弱性のうち非常に影響が大きいもののレビューを示します。

2025年の注目すべき脆弱性（iOS）

CVE-2025-24201 | 重大度：10.0（重大）

説明：

悪意を持って作成されたWebコンテンツがWebコンテンツサンドボックスの外部で実行されるおそれがある。

影響：

この脆弱性は、範囲外（本来想定されたバッファの末尾を超えて、または先頭より前）にデータを書き込めるようにするものです。メモリ破壊を引き起こしたり、意図しないコードを実行させるためのコード改ざんを可能にしたりします。

パッチが適用されたOS：

iOS 18.3.2およびiPadOS 18.3.2

CVE-2025-43300 | 重大度：10.0（重大）

説明：

悪意のある画像ファイルを処理することで、メモリ破壊が発生するおそれがある。

影響：

この脆弱性も、範囲外（本来想定されたバッファの末尾を超えて、または先頭より前）にデータを書き込めるようにするものです。

パッチが適用されたOS：

iOS 18.6.2およびiPadOS 18.6.2

CVE-2025-31201 | 重大度：9.8（重大）

説明：

任意に読み書きできる権限を持つ攻撃者がポインタ認証を回避できる可能性がある。

影響：

この脆弱性には、セキュリティ上重要なコンポーネントへの不正アクセスを可能とする不適切なアクセス制御が含まれます。結果として、攻撃者によるメモリの改ざんと読み取りや、不正コード実行のおそれがあります。

パッチが適用されたOS：

iOS 18.4.1およびiPadOS 18.4.1

Jamfが2025年に悪用を確認した他の脆弱性を次の表に示します。

iOS

パッチが適用されたIOSのバージョン	公開時期	脆弱性スコア	コンポーネント
18.3.1	2025年2月	CVE-2025-24200 CVSSスコア:6.1 | 重大度:中	アクセシビリティ
18.3.1	2025年2月	CVE-2025-43200 CVSSスコア:4.2 | 重大度:中	メッセージ
18.4.1	2025年4月	CVE-2025-31200 CVSSスコア:9.8 | 重大度:重大	CoreAudio
26.2	2025年12月	CVE-2025-43529 CVSSスコア:8.8 | 重大度:高	WebKit
26.2	2025年12月	CVE-2025-14174 CVSSスコア:8.8 | 重大度:高	WebKit

2025年の注目すべき脆弱性(Android)

CVE-2025-10585 | 重大度:9.8(重大)	CVE-2025-48543 | 重大度:8.8(高)	CVE-2024-53104 | 重大度:7.8(高)
説明:		
Google ChromeのV8のタイプ混乱脆弱性により、特製のHTMLページを介してリモート攻撃者がヒープ破損を悪用できる可能性がありました。	複数の場所で、Use After Freeが原因でChromeサンドボックスを回避してAndroidのsystem_serverを攻撃できる状態になっています。その結果、追加の実行権限を必要とせずに、ローカルで実行権限が昇格されるおそれがあります。この攻撃の実行に、ユーザの操作は一切必要ありません。	メディア:UVCビデオ:uvc_parse_format内でUVC_VS_UNDEFINEDタイプのフレームの解析がスキップされます。uvc_parse_streamingでフレームバッファのサイズを計算する際にこのタイプのフレームが考慮されないため、境界外の書き込みが発生する可能性があります。
影響:		
ポインタなどのリソースは特定のタイプとして宣言されていますが、後で互換性のないタイプのリソースにアクセスします。その結果、メモリの書き換え、クラッシュ、場合によってはコード実行が発生するおそれがあります。	過去に解放されたメモリを使用して、有効なデータが破損させられるおそれがあります。メモリを統合する前に攻撃者が悪意のあるデータを送り込んで、任意のコードを実行できる可能性があります。	バッファ境界外へのデータ書き込みにより、メモリ破損やデータの改ざんを招き、最終的に攻撃者による任意のコード実行を許す危険性があります。
パッチが適用されたOS:		
Chrome 140.0.7339.155	Android 13、14、15、16	アップストリームLinuxカーネル、2025年2月

Android

パッチが適用されたANDROIDのバージョン	公開時期	脆弱性スコア	コンポーネント
12、12L、13、14、15	2025年3月	CVE-2024-43093 CVSSスコア:7.3 | 重大度:高	フレームワーク
セキュリティに関する公開情報*	2025年3月	CVE-2024-50302 CVSSスコア:5.5 | 重大度:中	カーネル
セキュリティに関する公開情報	2025年9月	CVE-2025-38352 CVSSスコア:7.4 | 重大度:高	カーネル

*Androidではカーネルアップデートのための OSバージョンはリリースされていません。詳細は、該当のAndroidのセキュリティに関する公開情報をご覧ください。

Chrome

パッチが適用されたCHROMEのバージョン	公開時期	脆弱性スコア
136.0.7103.125	2025年5月	CVE-2025-4664 CVSSスコア:4.3 | 重大度:中
137.0.7151.72	2025年6月	CVE-2025-5419 CVSSスコア:8.8 | 重大度:高
138.0.7204.63	2025年6月	CVE-2025-6554 CVSSスコア:8.1 | 重大度:高
138.0.7204.157	2025年7月	CVE-2025-6558 CVSSスコア: 8.8 | 重大度:高
142.0.7444.175*	2025年12月	CVE-2025-13223 CVSSスコア:8.8 | 重大度:高
143.0.7499.109	2025年12月	CVE-2025-14174 CVSSスコア:8.8 | 重大度:高

*言及したバージョンは、デスクトップ版Chromeのものです。

デバイスの構成方法こそが、セキュリティの成否を分ける鍵

現代のモバイルOSが備える多彩で強力な機能は、わずか5年前の想像を遥かに超える進化を遂げています。そして、大いなる力には何が伴うのかはご存じでしょう。

皆さんは、デバイスをモバイルデバイス管理（MDM）に登録してデバイスの構成を適切に行っていることと思います。デバイス運用において、利便性や生産性、セキュリティ、そしてユーザのプライバシーのバランスを保つことは不可欠ですが、最適な構成を見極めるのは、極めて困難な課題です。

最適な対策は組織のリスク許容度や業界によって異なりますが、多くのリスクを誘発するため、一律に制限を検討すべき標準機能や設定がいくつか存在します。

- ジェイルブレイクされているデバイス：Appleのセキュリティ制限を回避して、ユーザがデバイスを危険/不安定な方法で変更できるようになったデバイス。攻撃者がシステムに侵入するバックドアが存在する可能性があります。
- 非公式アプリストア：App StoreやGoogle Playといった公式ストア以外のチャネルからユーザがアプリをインストール可能。公式ストアと同等のセキュリティ要件やプライバシー要件に準拠しているわけではないため、アプリに悪意や問題があるリスクが高くなっています。

これらのリスクがあるにもかかわらず、JAMF THREAT LABSの調査で以下が判明：

1台 /850台
の業務用デバイスが
ジェイルブレイク状態

2%
の組織に非公式アプリストア
を使用しているデバイスが存在

Jamf CISOの見解

スパイウェア、侵害されたアプリや悪意のあるアプリ、脆弱性が放置されたアプリ — これらは企業の機密データを密かに流出させる恐れがある極めて危険な存在です。以下に示す包括的な対策が極めて有効な抑止力となります。

- **すべてのモバイルデバイスをMDMに登録**し、承認済みのOSバージョン・アップデートを適用し、セキュリティベースラインを満たしていることを確認する。コンプライアンス違反のデバイスは、修復されるまで自動的に企業リソースから隔離する。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。
- ジェイルブレイク、悪意のあるふるまい、OSレベルの脅威を監視する**エージェントベースのセキュリティを実装**する。テレメトリをSIEMに連携させ、SOCがモバイルの脅威を他の環境と同様に可視化できるようにする。
- Eメールに限らず、すべてのデバイスとアプリを対象とした**DNSフィルタリングおよびフィッシング保護を有効に**する。不正なWi-FiとAitM攻撃の検出も行います。

アプリのリスク

モバイルアプリは業務を円滑に進める上で不可欠なツールとなっています。貴社に導入されているモバイルアプリはいくつあるでしょうか。サードパーティ製であれ、内製であれ、アプリは機密データへの入口となります。

1%未満

の組織でしか **モバイルマルウェアの被害** は発生していない

モバイルマルウェアは珍しい存在です。存在はしますが、コンピュータを標的としたマルウェアほどではありません。大きな理由は、主要なモバイルOSで使われている最新アーキテクチャにあります。サンドボックス化と管理の行き届いたアプリストアによって、悪意のあるコンテンツがデバイスに到達するリスクが小さくなっているのです。

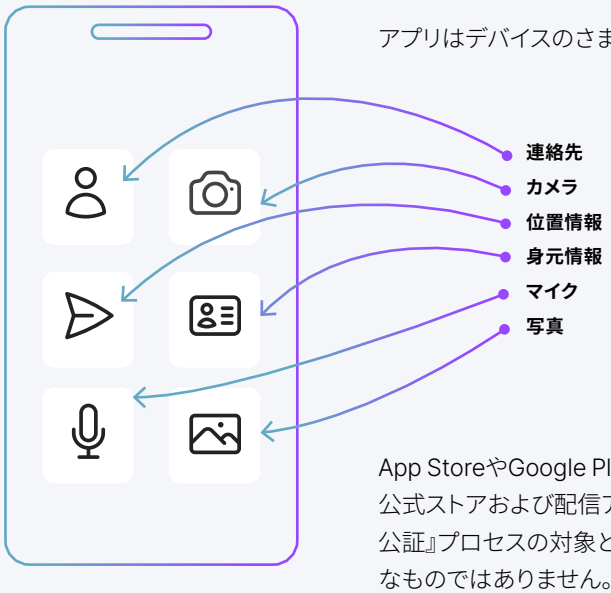
しかし、アプリを導入するほど、攻撃対象領域は拡大していきます。そのため、以下に注意してください。

- **アプリにおけるデータの保存方法と転送方法**
- **アプリが収集するデータとアプリのプライバシーポリシー**
- **サプライチェーンの懸念事項（アプリのベースとなっているライブラリは何か、など）**

攻撃者はアプリの脆弱性を利用して、APT攻撃を行ったり、スパイウェアを仕込んだりします。そのため、使用しているアプリを深く理解することが重要です。また、アプリがネットワーク経由でデータを転送する方法によっては、リスクが生じる場合もあります。これについては、後ほど詳しく説明します。

データの取り扱いはプライバシーポリシーで決まる

アプリはデバイスのさまざまな要素にアクセスできます。その中には、機密性の高い要素もあります。



App StoreやGoogle Playのアプリは、収集するデータを開示するよう求められています。すべての非公式ストアおよび配信アプリは、安全性とプラットフォームの整合性を維持するため、Appleによる『公証』プロセスの対象となります。ただし、その承認プロセスは公式App Storeのレビューほど厳格なものではありません。

セキュリティとプライバシーの両立は難しい

従業員にモバイルデバイスを支給するか、私用デバイスの業務利用（BYOD）を許可するかにかかわらず、企業リソースとデータへのアクセスを許可する際はセキュリティとプライバシーのどちらにも十分に配慮する必要があります。セキュリティは、データを守るために必要です。プライバシーは、ユーザを守るために必要です。

もっとも、両者のバランスを取るのには苦労することもあります。具体的には、以下のとおりです。

- **DLP（データ損失防止）**対策がプライバシー侵害的な行為に踏み込んでしまう可能性がある
- セキュリティ優先で**デバイスを過度に制限**すると、生産性が低下する
- **不適切なポリシー**はシャドーITを誘発し、ユーザが特定の業務のために未承認のアプリをダウンロードする原因となる

これらの問題に対処するために組織ができることを以下に挙げます。

- 企業リソースへのアクセスには**MDM**への登録を必須にする
- BYODデバイスにおいて、堅牢なコンテナやパーティションによって個人データと会社データを分離し、データ損失防止（DLP）ポリシーを徹底する。これにより、個人データへのアクセスを遮断しユーザのプライバシーを保護する
- 企業のネットワークトラフィックを暗号化されたトンネル経由で送信し、機密性とデータの整合性を保証する
- ユーザに対して、セキュリティのベストプラクティスとポリシーに関する教育を行う

補足：アプリのセキュリティ分析

JamfはNowSecureと連携して、モバイルアプリのリスクについて（特に、企業で導入されることの多いアプリについて）広範な分析を行いました。分析対象としたのは、人気が高く、幅広く配布されている135種類の業務用および個人用モバイルアプリで、モバイルアプリリスクのベースライン評価としてOWASP標準を使用しています。

いずれのアプリも2025年12月31日時点における最新バージョンを分析し、実際の企業が現在利用できるアプリビルドを反映しています。

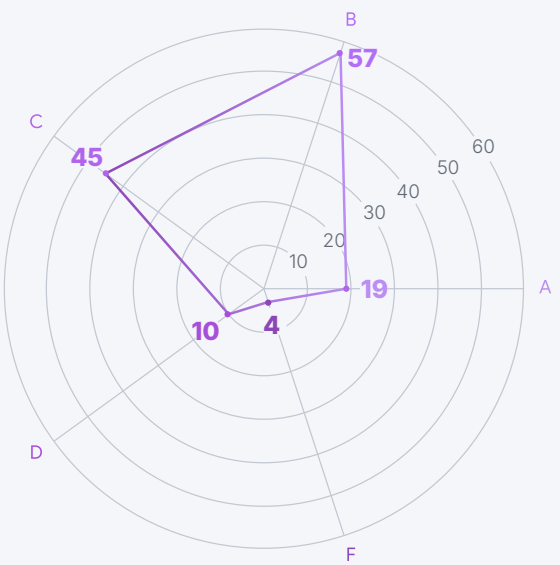
NowSecureは、モバイルアプリの脆弱性やデータ漏洩が各種インシデントに発展するのを予防する製品・サービスを展開する企業です。社内製とサードパーティ製両方のモバイルアプリを継続的に監視し、結果をセキュリティ、IT、リスクワークフローで考慮することにより、組織がモバイルデバイスのリスクに大規模に対処するうえで必要な可視性、証拠、ガバナンスを提供しています。

NowSecureの詳細はこちら

アプリのセキュリティスコア

NowSecureでは、モバイルアプリのセキュリティスコアを0〜100（スコアが高いほど良好）、リスク評価を**A**〜**F**（**A**=リスク最小、**F**=リスク重大）で示しています。これらのスコアは、脆弱性・データ漏洩・安全性に問題のあるコーディング慣行・暗号化方法の弱点・ネットワークの欠陥を評価する自動テストに基づいて付けられています。

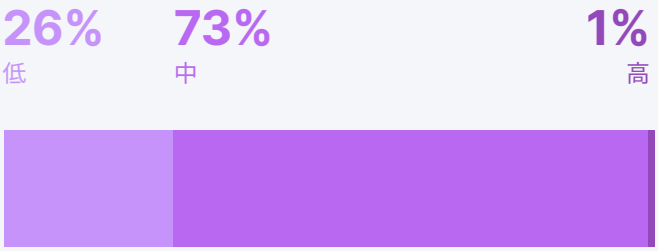
人気アプリのセキュリティスコア



A — F
リスク最小 — リスク重大

調査対象となった135のアプリのうち、約**86%**で既知のセキュリティ欠陥が確認され、リスクが最小限であると評価されたのは、わずか**14%**でした。この結果は、私たちが日々利用する主要なアプリには、たとえ最新の状態であっても、セキュリティリスクが広く潜在していることを物語っています。

脆弱性の分布



分析で見つかった脆弱性は、大半が重大度「中」に分類されました。後ほど示しますが、脆弱性の数は分析したアプリの数を上回っています。複数の脆弱性を抱えたアプリが数多く存在していることを示しています。

アプリの脆弱性評価

1つのアプリに複数の脆弱性が見つかった場合のリスクの影響を評価することが重要です。評価の時点で、アプリの**95%**に重大度「中」の脆弱性が1つ以上ありました。135種類のアプリの**2%**には重大度「高」の脆弱性があり、いつ攻撃を受けてもおかしくない状態でした。

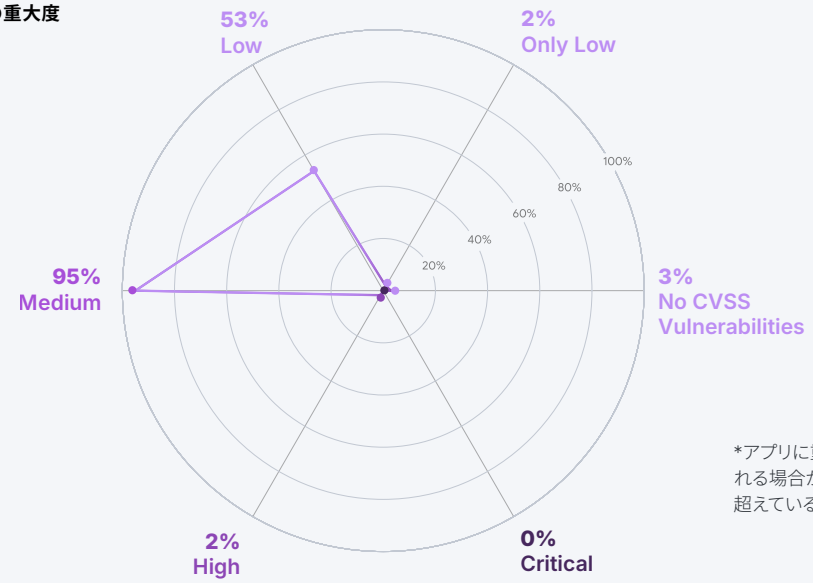
ソフトウェアメーカーがアプリの脆弱性を修正するのは当然の責務ですが、一方でそれを利用する企業側にも、リスクを把握し、タイムリーな更新管理を行う責任があります。パッチ適用のサイクルについては、CISAが緊急の脆弱性を15日以内、重要度の高いものを30日以内に修復するよう推奨するなど、いくつかの基準が存在します。しかし、今回の調査結果が示唆しているのは、基準の如何にかかわらず、アプリを常に最新の状態に保つための運用体制を構築すべきであるということです。

前述のように、NowSecureが評価したアプリは最新バージョンでしたが、それでもなお、大半のアプリに複数の脆弱性が見つかりました。アプリのリスクへの対処は絶え間なく進化する課題であり、継続的な監視と実施が必須です。

次の対策を講じることで、効率的な管理体制を築くことができます。

1. 脆弱性とプライバシー問題の特定を継続的に行う
2. 業務への影響に基づいて修復の優先順位を付ける
3. MDMツールを通じてポリシーを適用する
4. サードパーティ製アプリの動作を長期間監視する

脆弱性の重大度

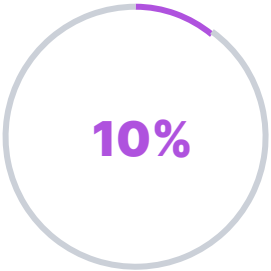


*アプリに重大度が異なる複数の脆弱性が含まれる場合があるため、パーセンテージが100%を超えている可能性があります。

サプライチェーン

モバイルアプリはサードパーティ製SDKやライブラリを利用していることが多く、それが隠れたリスクを招きます。

アプリのデータ収集ポリシーとプライバシーポリシーが要件を満たしていても、使われているサードパーティ製SDKやライブラリに重大な欠陥がある可能性があります。
アプリによるデータ漏洩とコンプライアンス違反の責任を取るのはそれを利用する企業なので、企業はソフトウェアのサプライチェーンリスクを確認する必要があります。



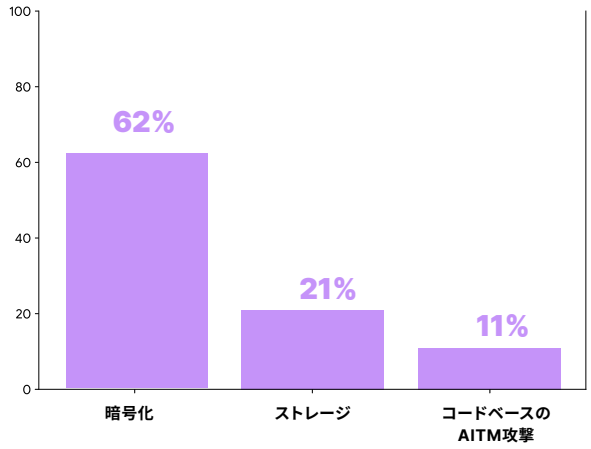
の**アプリ**に
脆弱なライブラリ

データのセキュリティ

アプリからのデータ漏洩にはいくつかのパターンがあります。

- **暗号化方法の問題:** アプリ開発者にとって、データの安全確保・通信の保護・ユーザの本人確認は難しい課題であり、多くの開発者がサードパーティ製ライブラリを利用します。NowSecureの調査によると、分析対象となったすべてのアプリにおいて、すでに脆弱性が確認されている2つのライブラリ（OpenSSLおよびlibpng）の使用が特定されました。
- **安全性に問題のある保存方法:** 保存データの管理方法によって、データの機密性・整合性・可用性が損なわれることもあります。ストレージ保護が脆弱な場合、データ窃取のリスクが高まります。
- **AitM攻撃リスク:** 転送中のデータの扱いも重要です。例えば、通信が適切に暗号化されていない場合、攻撃者は転送中の機密情報の盗聴や改ざんができます。
- **データアクセス:** モバイルアプリには、攻撃者が求めるクラウドデータや企業データへのアクセス権があります。アクセス方法がどうであれ、データ損失はデータ損失です。

脆弱性の種類



AIの使用

AI（特に生成AI）は、昨今注目の話題です。Deloitteは2026年1月のレポートで、承認されたAIの利用は1年で50%増え、業務にAIツールを使っている従業員の割合は60%であると報告しています。

オンデバイスAIとクラウドAIの双方が便利な機能を数多く提供している状況を踏まえれば、当然の結果です。例えば、以下の両方を取り入れているモバイルアプリが増えてきています。

- **オンデバイスAI:** LLMでテキスト生成や予測入力などの自然言語処理タスクが可能になります。また、機械学習モデルで画像認識、リアルタイム物体検出、バーコードスキャナ、拡張現実などの機能が実現します。
- **クラウドAI:** 処理や計算に外部インフラを使い、高度なタスクを実行します。

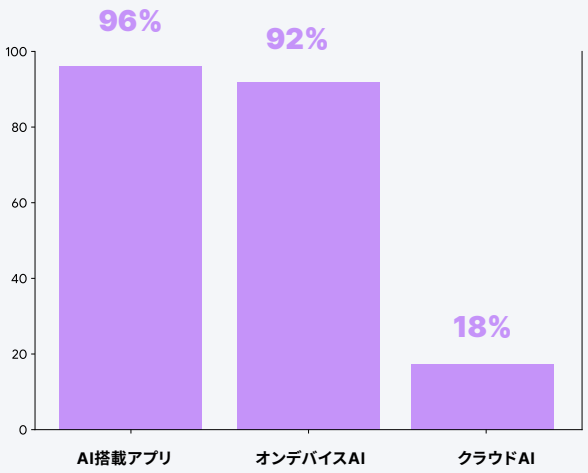
生成AIの導入が急速に進む一方で、その進化のスピードに合わせるかのように、新たなセキュリティリスクも次々と出現しています。

特に注意が必要なリスク

- ユーザがシャドーAIを利用する可能性があります。管理されていない未承認のAIが**企業の機密データ**などにアクセスし、ポリシーに違反する可能性があります。外部インフラを利用するクラウドAIの場合、**データ漏洩**などの**潜在的なリスク**を組織がはっきりと把握できないおそれがあります。
- AIエージェントに**自律動作をさせる**と、意図しない動作をするおそれがあります。

一般的なアプリの多くでAIが利用されていますが、その実情を企業がはっきりと把握できない形になっていることも少なくありません。

アプリのAI機能



プライバシー

私たちは今、どこへ行くにもモバイルデバイスを持ち歩いています。その中には、写真・連絡先・機密データ・金融書類・専有情報など、プライベートや仕事に関する多数の情報が格納されています。

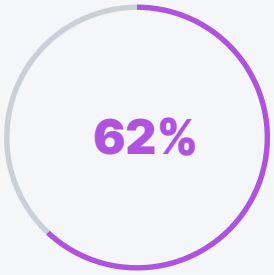
そのため、ユーザも雇用主もプライバシーを重視します。さらに、各種プライバシー法の対象となる可能性もあります。

しかし、開発者の意図であれ、単なる不注意であれ、これがアプリに反映されていないことがあります。アプリが機微データを収集するための危険なアクセス許可を要求してくる場合があります。例えば、次のような対象へのアクセスです。

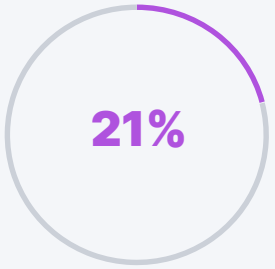
- デバイス位置情報
- マイク
- カメラ
- 連絡先

情報の要求以外にも、アプリでの情報処理方法はどうなっているでしょうか。アプリの機能に必要であるという理由で収集されるデータもありますが、必要性がさほど大きくないのに収集されるデータもあるのです。アプリの機能によってはプライバシーを侵害します。プライバシーにかかわる問題としては、例えば以下があります。

- トラッキングとプロファイリング
- サードパーティとのデータ共有
- 連絡先の収集/ターゲティング広告



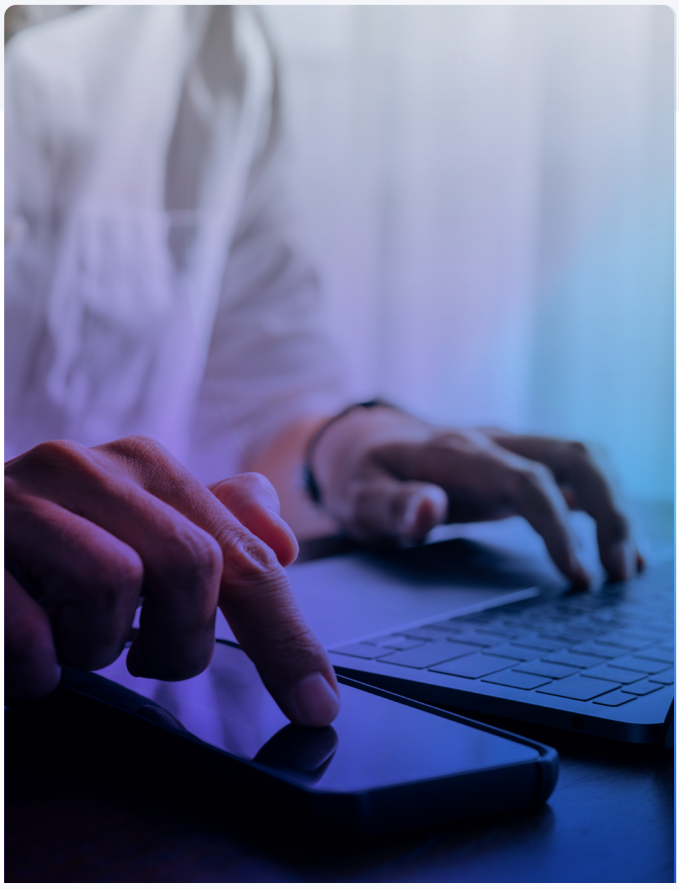
のアプリが危険なアクセス許可を要求



のアプリにプライバシーにかかわる動作

Jamf CISOの見解

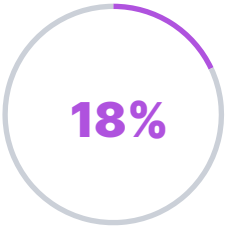
モバイルアプリは企業の機密データへの入口です。このリスクに対処するために、組織はデバイスにインストールしてもよいアプリを統制し、ネットワークで転送されるデータを保護し、デバイスで使われているアプリの脆弱性を常時把握する必要があります。BYODの場合、目標は分離です。企業データをコンテナ化して、個人のプライバシーを侵害することなく保護しましょう。このようにして、セキュリティチームによる確実な統制と、従業員のプライバシー保護を両立。バランスの取れた運用を実現します。



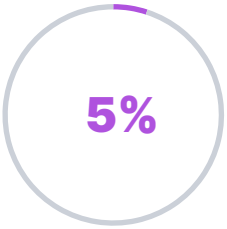
ネットワークとWebのリスク

不変の真理が一つあります。それは、攻撃者は常にセキュリティにおける『最大の弱点＝人間』を悪用し続けるということです。攻撃の手口は巧妙さを増しており、生成AIを駆使して、より信憑性の高い攻撃を仕掛けてくるようになっています。その一方で、ユーザがフィッシングリンクを誤ってクリックしたり、安易に危険なWi-Fiに接続してしまったりと、セキュリティ意識の『隙』を突かれるケースが後を絶ちません。

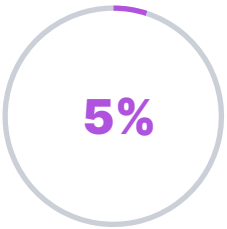
脆弱性が存在するのはデバイスだけではありません。理想的な構成で完璧に保護されたデバイスでさえ、転送中のデータ盗聴の脅威には脆弱です。ネットワークはエクスプロイトでよく利用される手段です。エクスプロイトは、以下のように複数の方法で行われます。



の**組織**に**危険なWi-Fiスポット**に接続するユーザが存在



の**組織**に**インフラベースのAitM攻撃**を受けたユーザが存在



の**組織**に**クリプトジャッキング攻撃**を受けたデバイスが存在

ネットワークインフラ

自社ネットワークの構成は制御できても、ユーザが組織の外部で接続するサードパーティのネットワーク（モバイルデータ通信ネットワークを含む）まですべてを制御することはできません。条件付きアクセスの適用・業務用ネットワークの分離・ゼロトラストネットワークアクセスポリシーの適用は必ず行うようにしましょう。

これらが実施されていなければ、データはリスクにさらされています。ユーザが公共のフリーWi-Fiネットワーク（暗号化が弱い/認証不要の可能性がある）に接続すると、セッションCookieを盗む・証明書検証を回避するなどの手法で攻撃者に利用されるおそれがあります。

Webプロトコルは、デバイス、ブラウザ、サーバが情報をやり取りする方法を規定するもので、データセキュリティの重要な要素です。攻撃者は、プロトコルを旧式のセキュリティが弱いバージョンにダウングレードさせることで、転送中のデータの暗号化を解除して盗みやすくします。これがきっかけとなり、組織にAitM攻撃が始まります。

このようなAitM攻撃は、OSやアプリが持つコードベースの脆弱性ではなく、ネットワークインフラの脆弱性を悪用しています。

Webのリスク

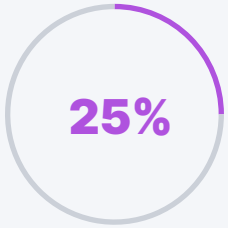
安全な接続を使用していても、インターネットの閲覧が安全とは限りません。必ずしもデバイスの侵害が原因で問題が起こるわけではないのです。悪意のあるリンク/広告をクリックしたり、問題のあるWebサイトにアクセスしたりすると、フィッシングによるクリプトジャッキングや認証情報窃取につながるおそれがあります。クリプトジャッキングとは、攻撃者がデバイスのCPU処理能力やメモリを不正に利用して暗号資産のマイニングを行う手法です。被害に遭うとデバイスのパフォーマンスが著しく低下し、業務に支障をきたすほど動作が不安定になる恐れがあります。

フィッシングは長らく定番の攻撃です。生成AIによって、本物らしいフィッシングメッセージを作るのがこれまで以上に簡単になっています。もはや、悪意のあるメッセージは、従来のようにわかりやすい特徴（誤字脱字など）を含むものだけではありません。

フィッシング攻撃に悪用されたブランド上位30社

攻撃者はよく、人気のブランドを模倣します。これは、普段から使っている馴染みのあるサービスのリンクなら、ユーザがクリックする可能性が高まる傾向にあるためです。つまり、攻撃者はそのようなサービスにユーザが寄せる信頼を利用するのです。彼らが特に狙うのは、銀行と金融サービスです。侵害されたアカウントには財産と機密情報の両方が含まれている可能性が高いからです。

ここに挙げるブランドは何も悪意のある行為を行っていないことに留意してください。その機関が積み上げた信頼を、疑いを抱かないユーザをフィッシングするために攻撃者が利用しているのです。



の**組織**に
フィッシングリンク
を踏んだユーザが存在

エンタテインメント/ネットワーク	ビジネス	公共サービス	銀行/金融サービス
Netflix	Microsoft	Optus	Allegro
Facebook	Apple	AT&T	U.S. Internal Revenue Service
Steam	Adobe	Amazon	楽天
eBay, Inc.		DHL	Coinbase
WhatsApp		British Telcom	PayPal
		Orange	イオンカード
		Comcast	三井住友銀行
		JR東日本	Navy Federal Credit Union
			Bradesco
			Bank of America Corporation
			HSBC Group
			Raiffeisen Bank
			American Express
			ING Direct

Jamf CISOの見解

技術的管理策のほかに重要なのは、従業員がフィッシングなどのソーシャルエンジニアリングの脅威を認識して報告できるように、意識向上プログラム・トレーニング・フィッシング訓練を通じて積極的に備えることです。フィッシング訓練では、AIを活用してユーザの能力に合わせてカスタマイズした訓練を提供することをお勧めします。また、脅威の最新状況と多様性を反映して常に訓練内容を見直すことも重要です。

リスクの拡散：持続的標的型攻撃

ここまでに、以下に関連するリスクについて説明しました。

- デバイスのOSと構成
- モバイルアプリ
- ネットワークとWeb閲覧

OSの脆弱性・モバイルアプリの不適切なデータ処理・ユーザの公共Wi-Fi接続といったリスク1つだけでも、データセキュリティに甚大な影響を及ぼす可能性があります。
リスクを抑えられるかどうかは、構成・ポリシー・ユーザトレーニング次第です。

こうしたリスクが高まれば、やがて問題に変わります。先進的な攻撃者集団は脆弱性を組み合わせて巧妙なエクスプロイトを作り出します。こうした高度な攻撃を仕掛ける攻撃者は、これまでは「価値の高い標的」に絞って行動を抑制してきました。しかし現在、彼らが使用するツールキットがより広範囲に流出し始めており、一般の市民までもがその脅威にさらされようとしています。

高度な脅威の被害を防ぐには、そのような脅威に対する理解が欠かせません。Jamf Threat Labsでは、ジャーナリスト・企業幹部・政治家・活動家などのリスクの高いユーザからインテリジェンスデータを取得するための複数のエクスプロイト実施メカニズム（ゼロクリック攻撃、ワンクリック攻撃を含む）と、標的型監視活動で使用される攻撃展開モデルを評価しました。この分析は、OSとサードパーティ製アプリの脆弱性・ベンダーの対応などのトピックを対象としています。これからは、その分析結果を紹介します。

ゼロクリック攻撃が引き続き大きな課題

2025年もAppleおよびAndroidデバイスに対するゼロクリック攻撃が、引き続き活発な脅威ベクトルとなっています。とりわけ標的となっているのはジャーナリストと経営幹部です。実際、画像解析の脆弱性（CVE-2025-43300）を悪用した、WhatsAppユーザに対する攻撃 が発見されています。

このことからわかるのは、攻撃者が今後も従来の意識ベースの対策を回避して、ユーザインタラクションなしでコードを実行させてくるという点です。この種の攻撃は一般的に、特定対象を狙った監視活動や情報収集活動が付随します。

ゼロクリック脆弱性の実際の悪用事例が続いていることから、コストのかかるエクスプロイトの開発に投資する能力と意志の両方を兼ね備えた攻撃者が今なお存在することは確実です。

組織を守る方法：
ユーザインタラクション制御だけに頼るのではなく、ポストエクスプロイト（侵入後）検出・行動テレメトリ・異常ベース監視を実装します。

なくならないブラウザ攻撃。広告経由で知らぬ間に行われることも

AppleとGoogleは1年を通じて多数のブラウザセキュリティパッチを公開しました。Chromeには250、Safariには75以上のセキュリティパッチが提供されており、手の込んだWebコンテンツを原因としたメモリ安全性に関する問題が相次いで発見されていることがわかります。

このような脆弱性は攻撃者にとって特に魅力的です。悪意のあるWebサイトや広告でJavaScriptを使って脆弱性を兵器化して、攻撃コストを抑えられるからです。脅威インテリジェンスレポートでは、商用スパイウェアベンダーが引き続き、デバイス全体を侵害するために、発見した脆弱性とサンドボックス回避を組み合わせたワンクリックエクスプロイトチェーンを利用していることを確認しています。

Intellexaの活動の発見は、インテリジェンス組織がこのようなエクスプロイトを盛んに使用していること、また、**エクスプロイトが広告ネットワークを通じてゼロクリック攻撃として配信されうる**ことを浮き彫りにしました。

組織を守る方法：
セキュリティスタックを調整して、管理されたモバイルデバイス環境内でWebトラフィック調査・エクスプロイト動作検出・迅速なOS/ブラウザアップデートを行うようにします。

標的企業は懸命に応戦しているが、依然として防御対策範囲は不十分

プラットフォームベンダーと大規模IT企業は2025年、標的型スパイウェア攻撃に対抗するための取り組みを、法的、技術的、アーキテクチャ的手段を含め、はっきりと増やしました。MetaがNSO Groupを告訴するなどの法的措置が注目を集めましたが、これは技術による純粋な防御から法的手段による長期的な抑止に対策がエスカレートしている証です。

Appleでは、そのような対策と同時に、Memory Tagging Extension（MTE）やロックダウンモードの改善など、プラットフォームレベルの軽減措置にも投資を続けています。しかし、こうした防御策を講じてもなお、複数の脆弱性を組み合わせた『エクスプロイト・チェーン』による攻撃の成功事例は後を絶ちません。

先進的な攻撃者は、新しい軽減措置が施された状況で活動するために、ツールと手法を適応させ続けています。例えば、非公開のカンファレンスで最近、攻撃者が取りうる回避策が実演されました。

組織を守る方法：
ベンダーレベルの保護を補うために、標的型攻撃シナリオに合わせた独立検出・フォレンジック可視性・インシデント対応機能を導入します。

注意すべきスパイウェア

Predator | 開発：Intellexa

Predatorは主にWebベースのワンクリックエクスプロイトを利用します。多くの場合、悪意のあるリンクやWebコンテンツ（広告を含む）を通じて配布されます。Appleが繰り返しパッチを配布していることからわかるように、WebKitの脆弱性を激しく悪用しています。このモデルは拡張性は高いものの、攻撃の成否がパッチ適用の早さに大きく左右されます。Predatorはワンクリック攻撃が依然として通用することを示しています。

Graphite | 開発：Paragon

Graphiteは高度なiOSエクスプロイトに関連した商用スパイウェアプラットフォームで、ゼロクリック攻撃とワンクリック攻撃の両方に対応していると評価されています。2025年、**パッチが万全に適用されたiPhoneでゼロクリックiMessageエクスプロイトの成功**が確認されました。これは、Graphiteがユーザインタラクションなしでデバイスを侵害できることを意味しています。複数の感染が同一オペレータのインフラに起因することが判明しており、出来心による活動ではなく、組織的かつ計画的に標的を設定していることは確実です。この調査結果は、スパイウェアベンダーに対する規制や法的圧力が強まっているにもかかわらず、Graphiteがスパイウェア市場内で実質的な後継の地位を固めたことを示していると言えます。

Landfall | 開発者：N/A

Landfallは、今まで知られていなかった商用グレードのAndroidスパイウェアファミリで、Samsung Galaxyデバイスに対する標的型モバイルスパイ活動に使用されていました。オペレータは**Samsungの画像処理ライブラリに存在する重大なゼロデイ脆弱性を悪用**し、悪意を持って作成した画像ファイルを通じてスパイウェアを配布しました。このファイルは、WhatsAppなどのメッセージアプリを通じて送信されたと見られます。

攻撃活動は少なくとも2024年半ばから2025年4月にSamsungが脆弱性にパッチを適用するまで行われ、攻撃者は音声録音・位置追跡・連絡先・写真・通話ログ取得など、広範な監視機能を利用できました。Landfallの事例からは、ゼロデイ脆弱性を突くAndroidスパイウェア活動は一般に把握できない状態で進化を続けていることがわかります。防御の観点から、モバイルプラットフォーム全体にわたって積極的なパッチ対応・異常検知・長期的なデバイステレメトリの実施が重要です。

Pegasus | 開発：NSO Group

Pegasusは、ゼロクリックと一部ワンクリックを利用したエクスプロイトチェーンを利用して**デバイス全体を侵害**できる、iOSおよびAndroidに対応した高度なスパイウェアプラットフォームです。少人数の価値の高い個人を標的とし、隠密性と持続性に最適化されています。2025年、NSOは輸出規制の対象に指定されたほか、訴訟により賠償金の支払い義務が課せられました。その後、同社は**投資家集団に買収**されましたが、同社のテクノロジーは（おそらく別のブランドを冠して）引き続きインテリジェンス組織に利用されると見られます。

Dante | 開発：Memento Labs

Memento Labsはイタリアを拠点とする監視テクノロジーベンダーであり、2019年の買収を経て再編された、かつての『Hacking Team』の後継会社です。2025年、Memento Labsとつながりのあるツールが、Chromeサンドボックスを回避できるゼロデイ脆弱性（CVE-2025-2783）を突いた**高度なサイバースパイ活動キャンペーン**「Operation ForumTroll」に利用されました。同社CEOによると、同社はWindowsを対象としたソリューションのサポートを終了し、モバイルプラットフォームに重点を移したといいます。そのため、このマルウェアファミリと脆弱性は、Androidデバイスで発見されることが見込まれます。

Spyrtacus | 開発：SIO

Spyrtacusは商用監視スパイウェアファミリで、2025年にAndroidデバイスを標的とした活発な活動が報じられています。悪意のあるリンクとアプリケーション層のソーシャルエンジニアリングを通じて配布されました。Spyrtacusはデバイスに侵入すると、**データ窃取・位置追跡・メッセージと連絡先の取得**など、典型的なスパイウェアの挙動を示します。

PegasusやGraphiteなどのゼロクリックスパイウェアとは異なり、Spyrtacusは通常、インストール開始までにある程度のユーザインタラクションかソーシャルエンジニアリングを必要とします。実際の攻撃にSpyrtacusが使われた事例から、標的型モバイルスパイウェアのすべてがゼロデイ脆弱性を悪用したものとは限らず、ソーシャルエンジニアリングと便利なスパイウェアフレームワークが併用される場合もあることが明らかになりました。

Jamf CISOの見解

ベンダーがプラットフォームレベルでかなりの対策とセキュリティ強化を実施しているにもかかわらず、2025年も攻撃者は重大な脆弱性を見つけ、悪用しています。なかでも、ブラウザ（Chrome、Safari）とメッセージアプリなどは攻撃者にとって価値の高いコンポーネントと言えます。これらは複雑に構築されており、信頼できないコンテンツに頻繁に接し、ユーザの毎日の業務フローで中心的な役割を果たすため、魅力的な標的なのです。

標的型攻撃の度重なる成功事例から、どのような対策をしても（豊富なリソースを持つ攻撃者が相手であればなおさら）完全にリスクを除去できないことは明らかです。結果的には、厳格なデバイス管理と強力なアップデート適用が引き続き組織の取りうる最も効果的かつ制御可能な防御策であることは変わりません。

このように、MDMは補助というよりむしろ中核的なセキュリティ対策です。セキュリティアップデートの迅速な適用、セキュリティベースラインの強制、デバイスの可視性の確保、攻撃に晒される期間の短縮が、新しく発見された脆弱性の影響を抑えるうえで決定的な要因となります。

リスクは甚大 — だが、克服は可能

ここまで紹介してきたリスクに対処するには、周到なアーキテクチャが必要です。デバイスのセキュリティを支える柱は次のとおりです。

デバイス管理：
制限と構成を適用し、ポリシーを強制

エンドポイントセキュリティ：
潜在的な侵害に備え、デバイスの状態と動作を監視

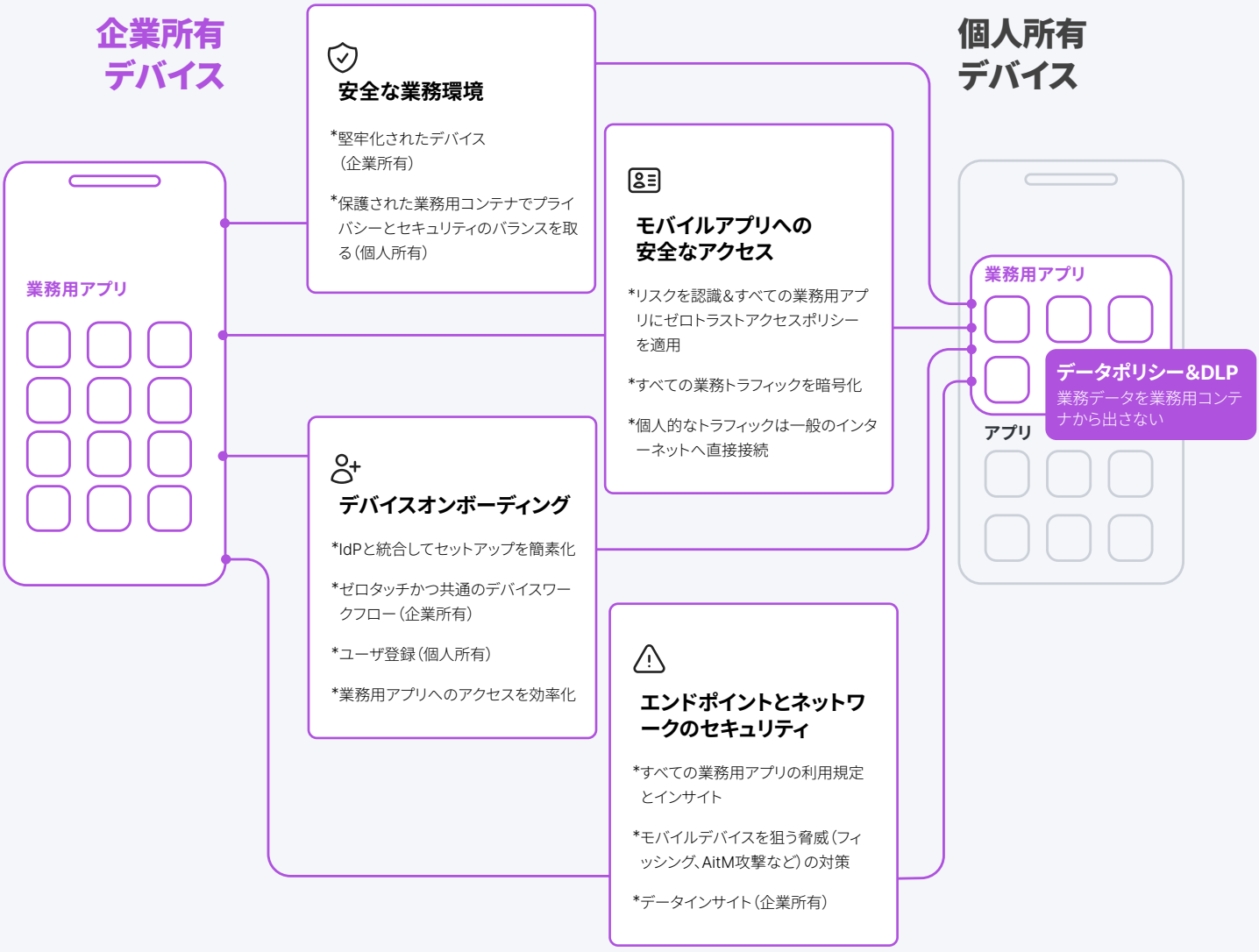
安全なリモートアクセス：
企業リソースにアクセスできる人とデバイスを管理

これらの組み合わせにより、機密データへのアクセスを要件に準拠したデバイスと許可されたユーザのみに確実に限定できます。

もっとも、この点は**デバイスが企業所有**かどうかによって状況が少し変わってくる可能性があります。

デバイスの構成は、セキュリティの弱みにも強みにもなります。アップグレード・アプリ審査・行動分析を自動化し、コンプライアンス状況に応じたアクセスポリシーを適用することが、

データ保護を成功裡に進める第一歩です。



モバイルデバイスに関してJamf Threat Labsが実施した最新の調査結果

スパイウェアPredatorがiOSの録画・録音インジケータを回避する仕組み

2026年2月

スパイウェアPredatorは、Objective-Cのnilへのメッセージ送信を悪用した高度な手法でiOSの録画・録音インジケータを回避します。その仕組みは、センサーアクティビティの更新処理すべてを単独で担うSpringBoardメソッドに介入し、selfポインタをNULLに設定して、インジケータの更新をユーザに通知せず、無視されるようにするというものです。完全に侵害を受けたデバイスでカメラとマイクへのアクセスが行われながらも、デバイスが監視されていることを示す視覚的警告が何も表示されずにデバイスが通常どおり動作するため、この手法はこれまでの手法よりも気付かれにくくなっています。

OpenClaw：便利なAIが気付かぬうちに最大のインサイダー脅威になりうる

2026年2月

OpenClawは、シェルコマンドの実行・ファイルへのアクセス・アプリの操作を行うことができる自律AIエージェントを構築するためのオープンソースフレームワークですが、セキュリティ境界が組み込まれていないため、企業に巨大なセキュリティリスクをもたらします。このフレームワークが危険なのは、システムへのアクセスに制限がなく、データ漏洩のおそれと、悪意のある命令を正規ビジネスコンテンツに埋め込む間接的なプロンプトインジェクション攻撃の脆弱性があるためです。最近公開されたセキュリティ勧告で、攻撃者がさまざまな欠陥を悪用して永続的なアクセスを取得し、OpenClawの導入が高リスクなインサイダー脅威になる仕組みが示されました。OpenClawを企業環境で安全に管理するには、包括的な検出・防止・ガバナンス戦略を導入する必要があります。

Predatorのキルスイッチ：記録になかったiOSスパイウェアの分析対策手法

2026年1月

スパイウェアPredatorには、これまでに調査結果として記録されていたもの以外にも高度な分析対策手法が搭載されています。導入失敗の理由に関する正確な診断情報をオペレータに提供するエラーコードシステムが一例です。他にも、開発者モード・ジェイルブレイクツール・セキュリティアプリ・地理的制約を検出する機能や、被害者に録音・録画インジケータを見せないようにする高度なフォレンジック回避策を実装しています。

このようなメカニズムの判明によって、標的型攻撃に失敗したときにオペレータが詳細なフィードバックを受け取っており、対策を立てて手法を調整できることや、商用スパイウェアベンダーがセキュリティ製品の回避だけでなく研究者対策に多くの労力を注いでいることがわかりました。

プレイヤー認証情報を漏洩するモバイルアプリゲームをJamf Threat Labsが発見

2025年11月

1,000万ダウンロードを超える人気のモバイルゲーム「World of Warships Blitz」でログイン時と登録時に暗号化されていないHTTP接続が使われており、プレイヤー認証情報とセッショントークンが漏洩していることが判明しました。認証情報は難読化されていましたが、漏洩によってリプレイ攻撃（認証リクエストをキャプチャして再送信することでアカウントを乗っ取る攻撃）が可能な状態でした。開発者は責任ある開示を受け、協調してバージョン8.4.0で問題を修正しました。

この調査から、人気のアプリでも重大な脆弱性を抱えている場合があり、多層セキュリティ防御と、パスワード対策に関するユーザ教育が何よりも重要であることが示されました。

認証情報を漏洩しているアプリを Jamf Threat Labsが発見

2025年9月

暗号化されていないHTTP通信により、ユーザの認証情報や個人情報（PII）を外部に露呈させている2つのアプリが発見されました。利用者数1,500万人を誇るマレーシアの医療管理アプリとインドの宝飾品ブランドによる貯蓄用アプリです。両アプリは機密データを平文のまま送信しているため、ユーザは資格情報の窃取やアイデンティティ詐取、アカウントの乗っ取りなどのリスクに直面しています。特に公共ネットワーク上では、第三者による傍受が容易であり、極めて危険な状態と言えます。

この事例は、組織による安全なデータ転送の実装が不可欠であること、そしてユーザ側もモバイル脅威対策ソリューションやZTNA、コンテンツフィルタリングなどを活用し、リスクのあるアプリを確実に遮断すべきであることを改めて示しています。

Flekst0re：サードパーティ アプリストアのセキュリティ評価

2025年8月

Flekst0reをはじめとするサードパーティ製iOSアプリストアの利用には、極めて深刻なセキュリティ上の懸念が伴います。例えば、正規のアプリを装いながら、裏では会話を密かに録音し外部サーバへ転送するよう細工された『改造版WhatsApp』の存在が、実証実験（PoC）によって明らかになっています。これらのストアは、エンタープライズ証明書によるアプリの再署名という手法を用いて、Appleのセキュリティ審査を不正に回避しています。特にFlekst0reのカスタムソース機能は、検証プロセスを経ていないアプリの導入を可能にするため、スパイウェアやマルウェア混入の温床となる極めて危険な導線となっています。

非公式ストアの利用は、改造アプリや利便性の提供と引き換えに、iOSのセキュリティアーキテクチャそのものを根本から揺るがします。特に金融・メッセージング・メールなどの機密アプリを利用する環境では危険な存在です。

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、
Jamfへお問い合わせください。