2026年
10月
OCTOBER

MALWARE REPORT

マルウェアレポート

国内のマルウェア検出状況を解説



キヤノンマーケティングジャパン株式会社

はじめに

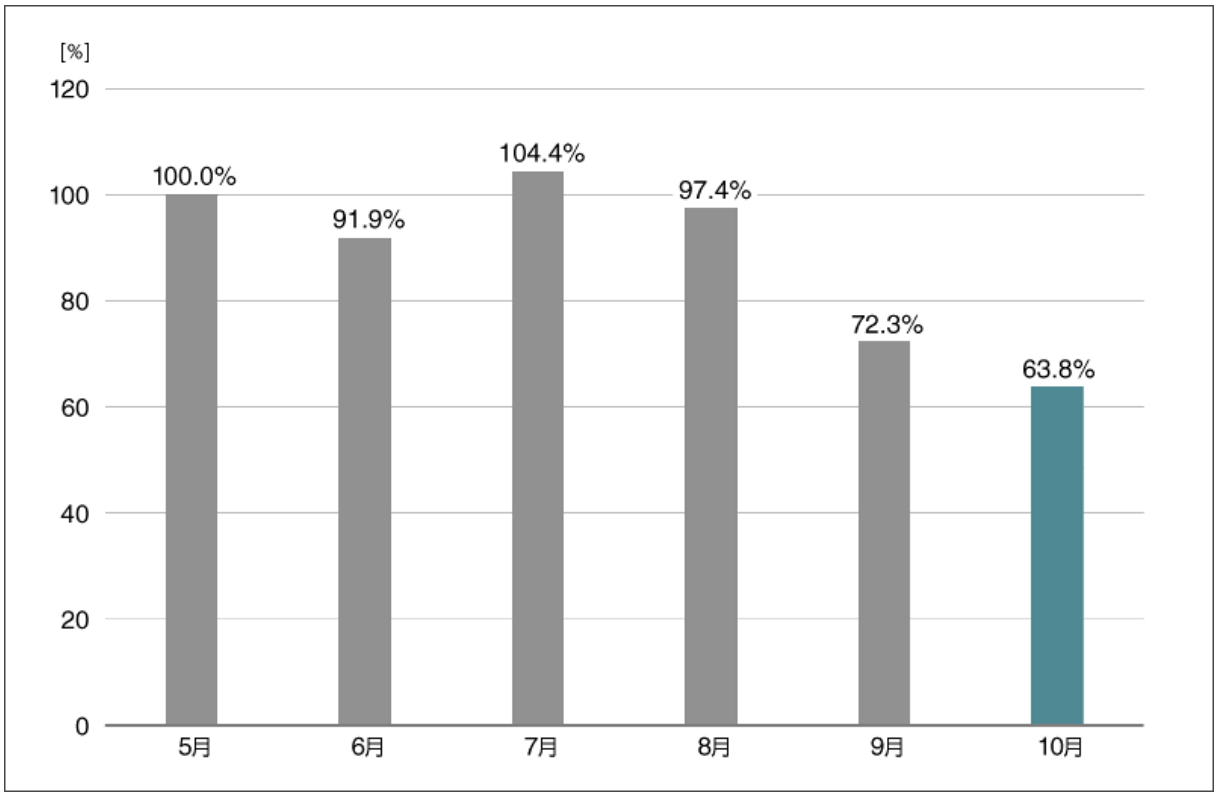
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「サイバーセキュリティラボ」が「ESET セキュリティソリューションシリーズ」の

マルウェア検出データを基に国内のマルウェア検出状況を分析し、まとめたレポートです。

2026 年 10 月マルウェア検出状況

2026 年 10 月（10 月 1 日～10 月 31 日）に ESET 製品が国内で検出したマルウェアの検出数の推移は、以下のとおりです。



国内マルウェア検出数*1の推移

(2026 年 5 月の全検出数を 100%として比較)

*1 検出数には PUA（Potentially Unwanted/Unsafe Application; 必ずしも悪意があるとは限らないが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があるアプリケーション)を含めています。

2026 年 10 月の国内マルウェア検出数は、2026 年 9 月と比較して減少しました。検出されたマルウェアの内訳は以下のとおりです。

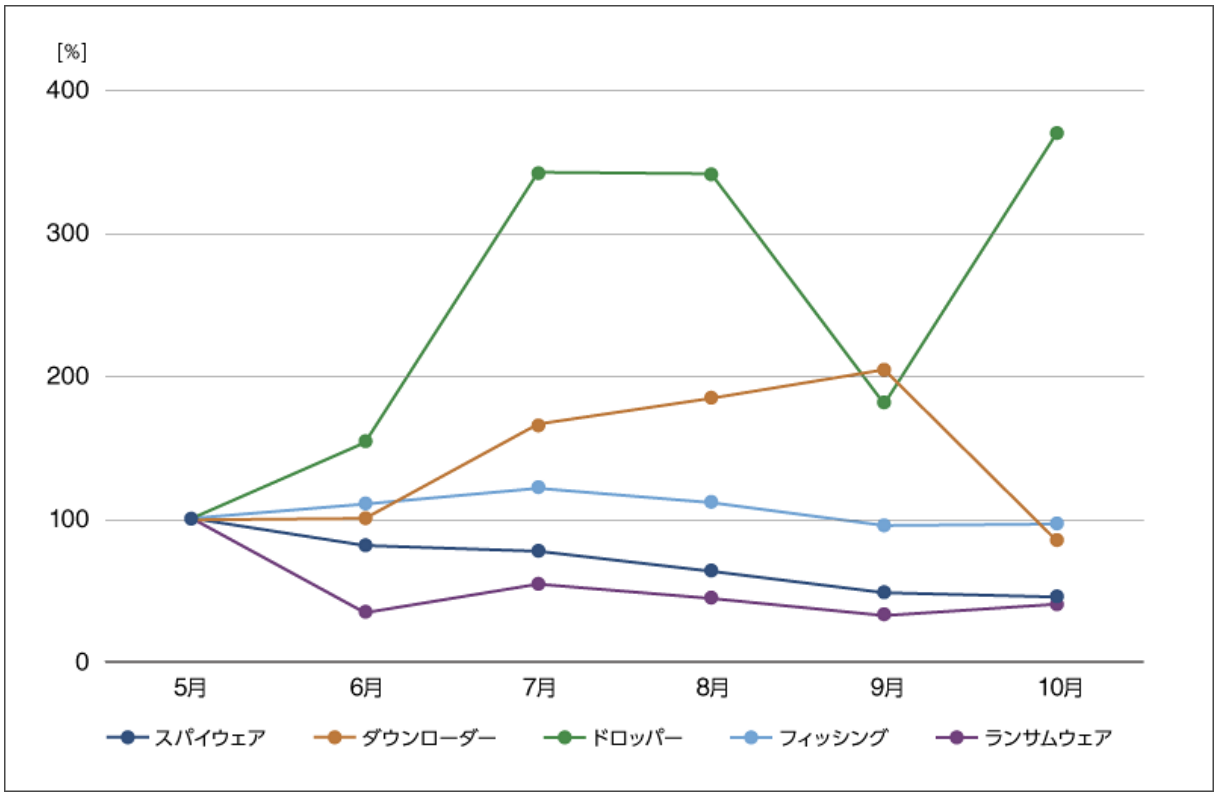
国内マルウェア検出数*2 上位（2026 年 10 月）

順位	マルウェア	割合	種別
1	DOC/Fraud	29.1%	詐欺サイトのリンクが埋め込まれた DOC ファイル
2	HTML/Phishing.Agent	8.6%	メールに添付された不正な HTML ファイル
3	JS/Adware.Agent	7.9%	アドウェア
4	JS/TrojanDropper.ModiLoader	3.5%	ドロッパー
5	JS/Danger.ScriptAttachment	3.4%	メールに添付された不正な JavaScript
6	Win32/Exploit.CVE-2017-0199	3.0%	脆弱性を悪用するマルウェア
7	Win64/Valley	2.3%	PC の遠隔操作を目的としたマルウェア
8	PDF/Phishing.A.Gen	0.9%	メールに添付された不正な PDF ファイル
9	JS/Obfuscated	0.9%	難読化された不正な JavaScript
10	JS/Agent	0.8%	不正な JavaScript の汎用検出名

*2 本表には PUA を含めていません。

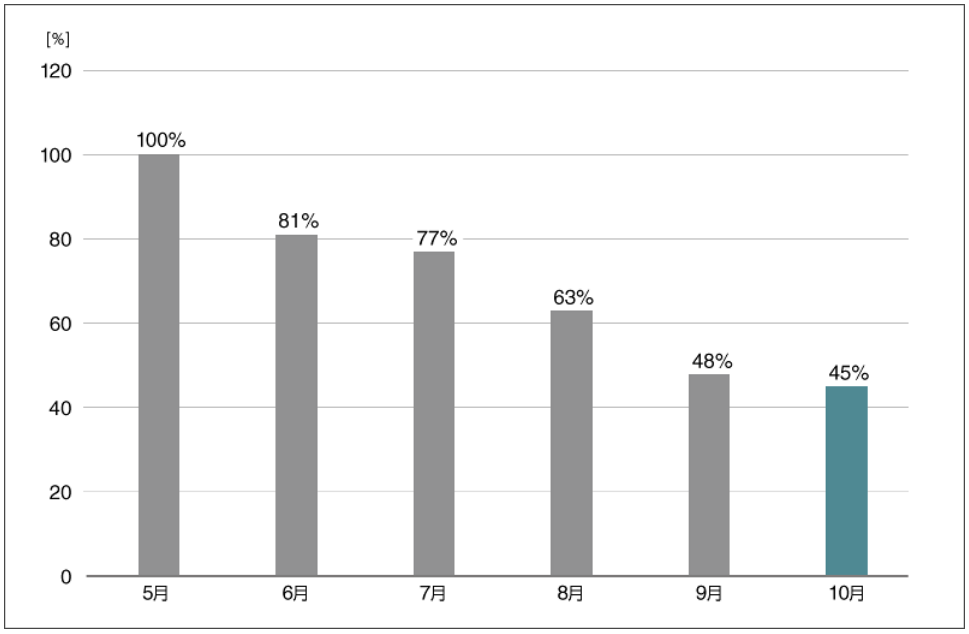
10 月に国内で最も多く検出されたマルウェアは、DOC/Fraud でした。
DOC/Fraud は、詐欺サイトへのリンクまたは詐欺を目的とした文章が書かれている Word ファイルの検出名です。主にメールの添付ファイルとして確認されており、ファイル内に記載されている内容に従ってしまうと詐欺や個人情報の窃取といった被害に遭う可能性があります。

2026 年 10 月に ESET 製品が国内で検出したマルウェアの種類別の推移は、以下のとおりです。以降のグラフには PUA が含まれています。



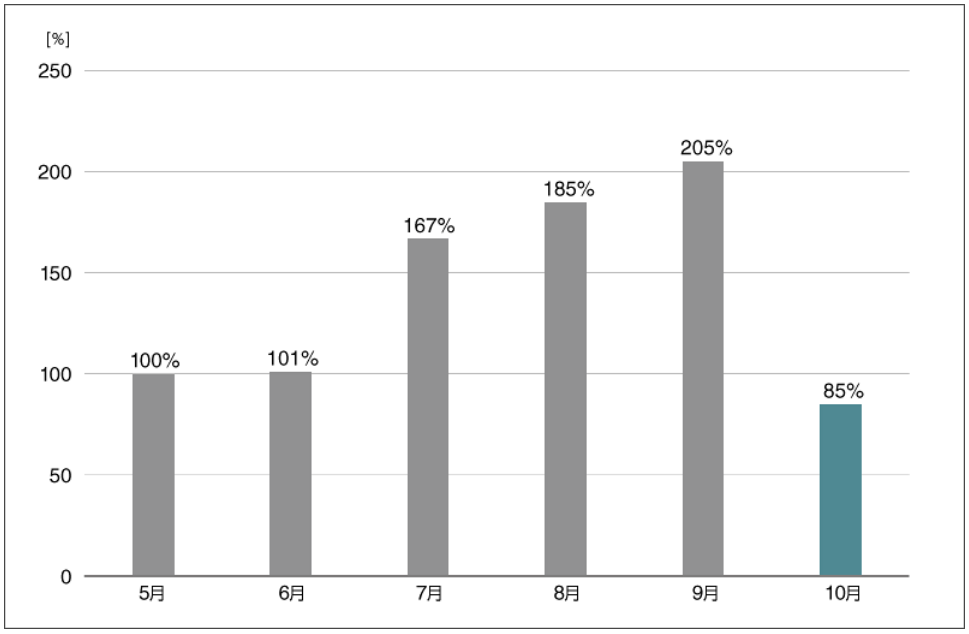
国内マルウェアの種類別検出数の推移
（2026 年 5 月の各検出数を 100%として比較）

2026 年 10 月はドロッパーの検出数が大きく増加しました。
一方で、ダウンローダーの検出数は大きく減少しました。



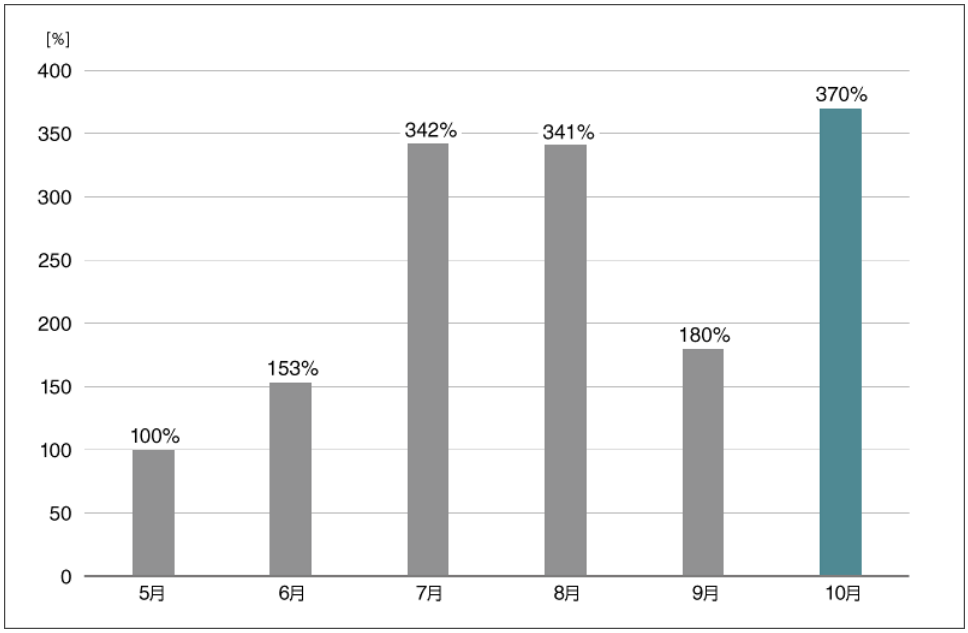
スパイウェア検出数の推移（国内）

（2026 年 5 月の検出数を 100%として比較）



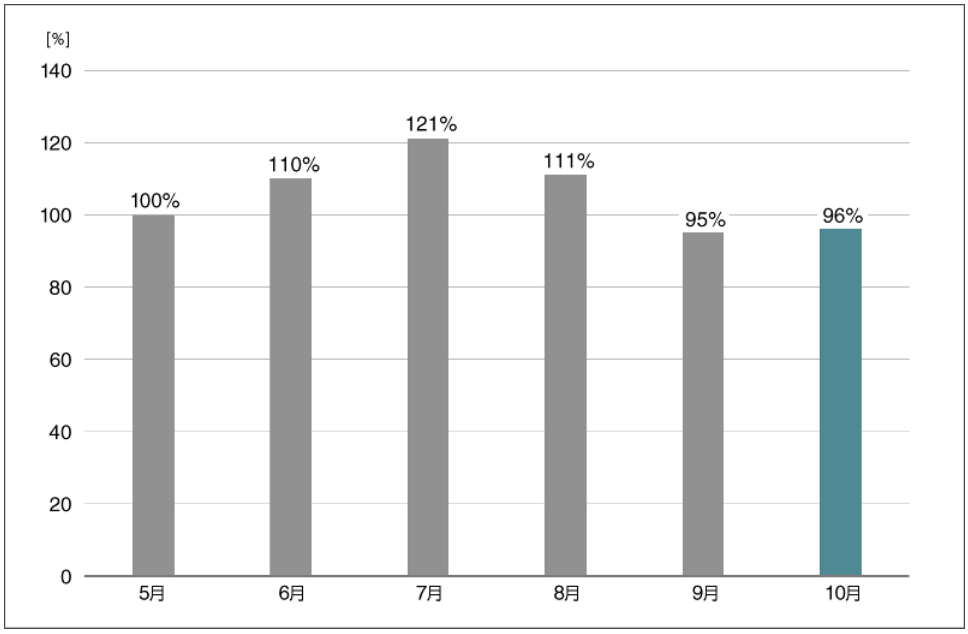
ダウンローダー検出数の推移（国内）

（2026 年 5 月の検出数を 100%として比較）



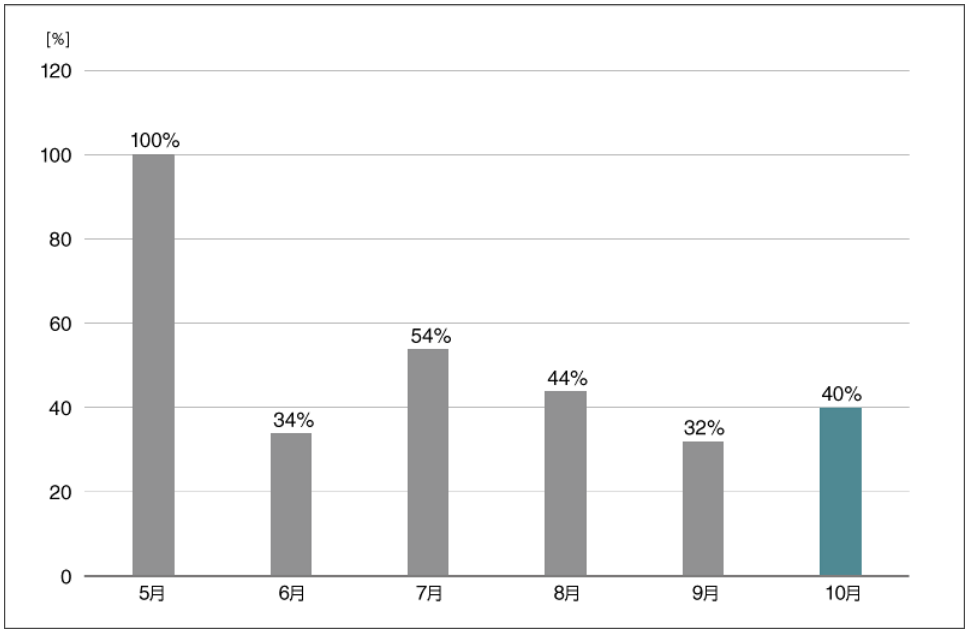
ドロッパー検出数の推移（国内）

（2026 年 5 月の検出数を 100%として比較）



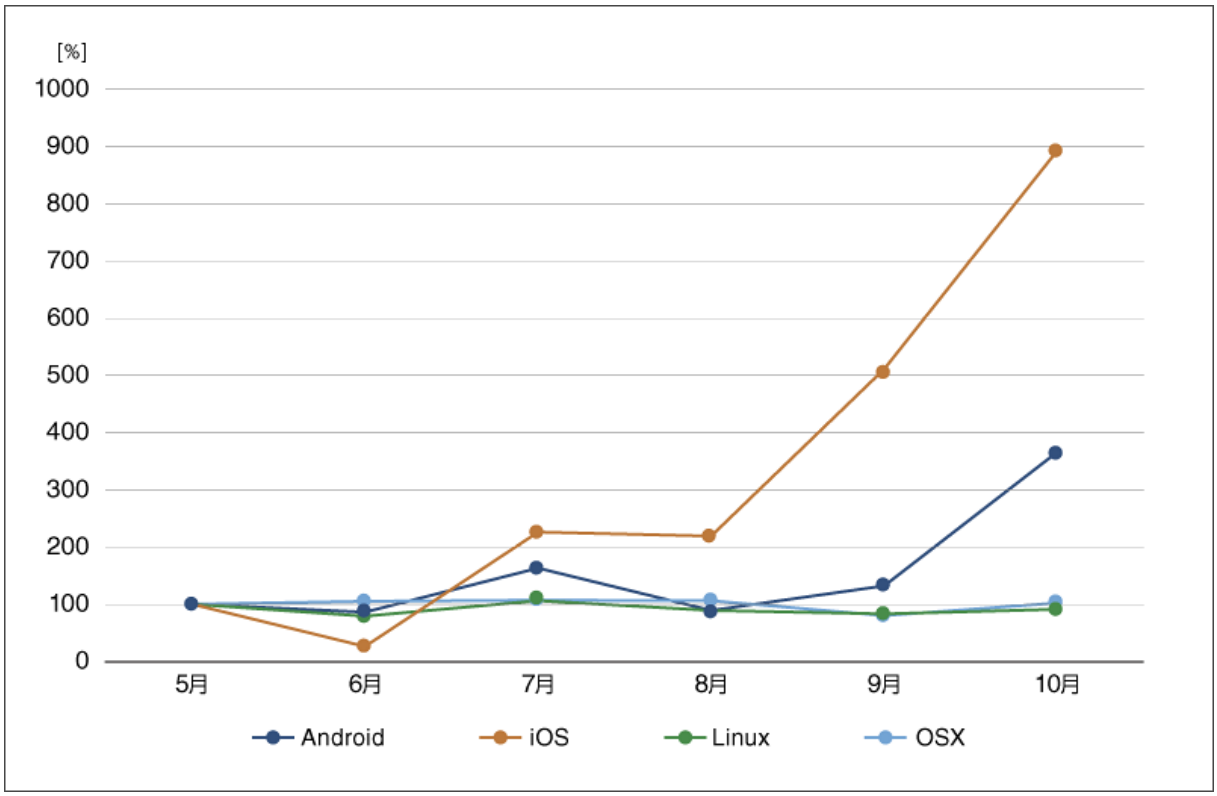
フィッシング検出数の推移（国内）

（2026 年 5 月の検出数を 100%として比較）



ランサムウェア検出数の推移（国内）
（2026 年 5 月の検出数を 100%として比較）

2026 年 10 月に ESET 製品が国内で検出したマルウェアの OS 別推移は、以下のとおりです。

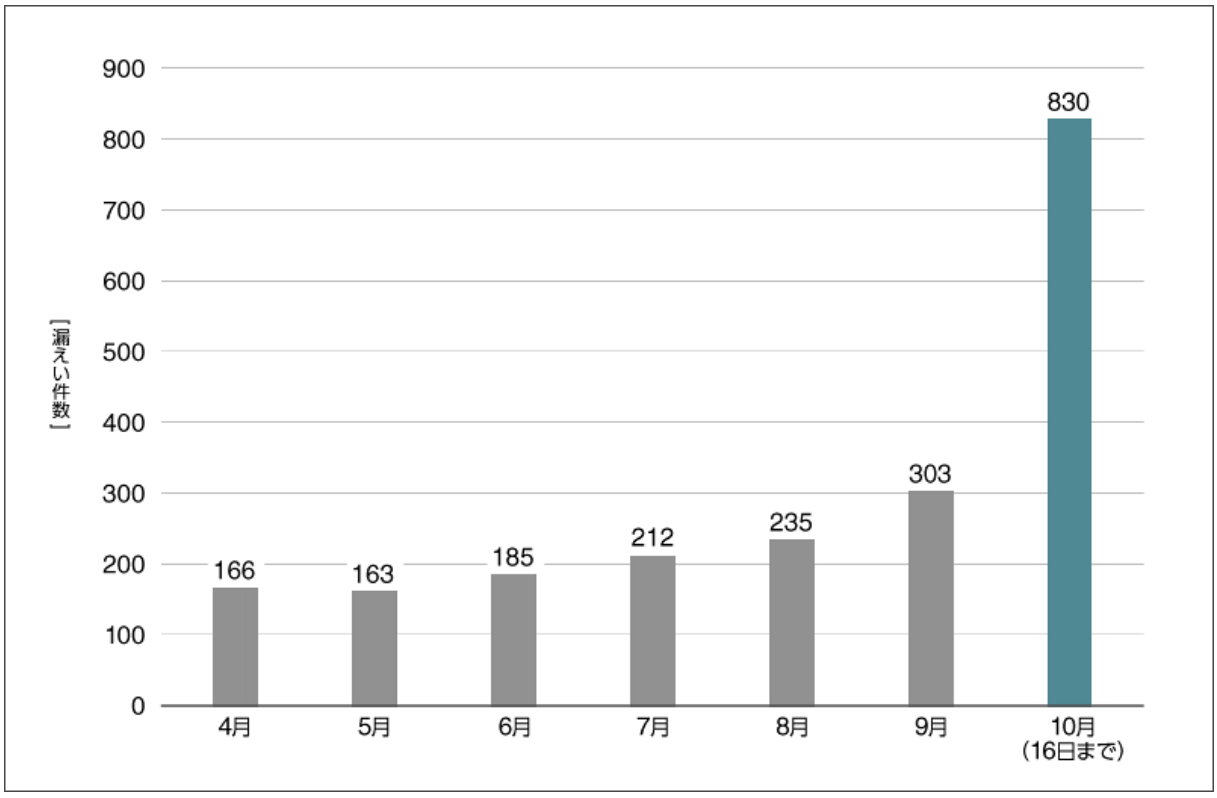


国内マルウェアの OS 別検出数の推移（Windows を除く）
（2026 年 5 月の各検出数を 100%として比較）

2026 年 10 月は iOS と Android を標的としたマルウェアの検出数が大きく増加しました。

頻発する情報漏えいについて

個人情報保護委員会によると、2026 年 4 月 1 日から 10 月 16 日までに、事業者から同委員会に直接報告された不正アクセスによる個人データの漏えい等の報告件数は 2,094 件に上りました。これらの報告によると、漏えいした個人データの対象者は延べ約 2 億 6,000 万人に達しています。
特に 10 月は報告件数が急増しており、9 月の 303 件に対し、10 月は 16 日までのわずか半月で 830 件と、前月の約 2.7 倍に達しました。



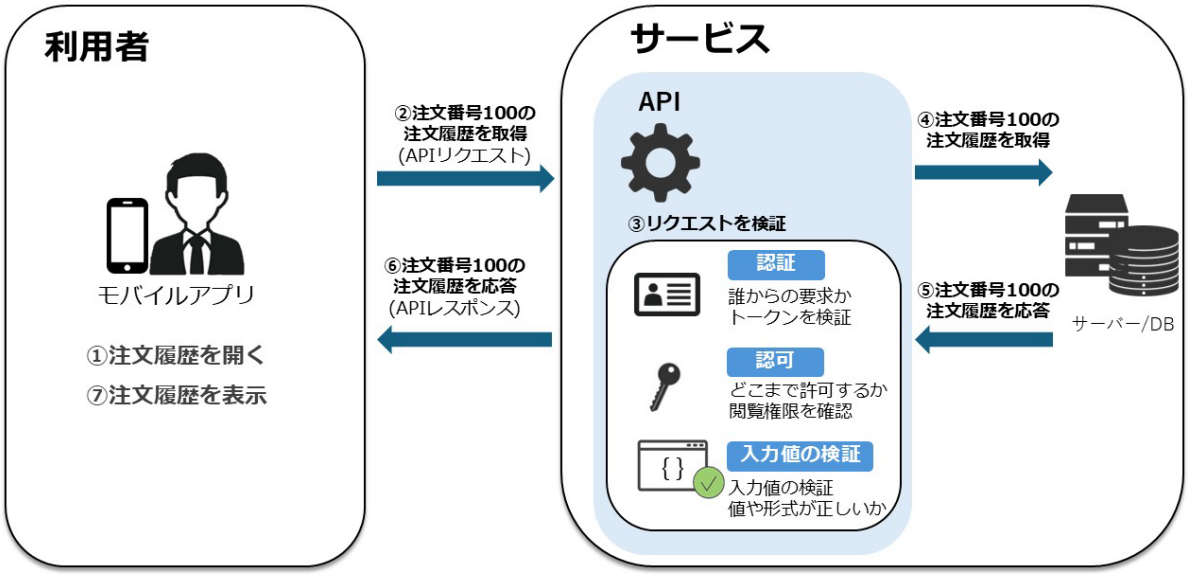
不正アクセスによる個人データの漏えい等の報告件数
（個人情報保護委員会の資料をもとに作成）

情報漏えいにつながる要因はさまざまですが、情報通信研究機構（NICT）は 10 月 13 日、その 1 つとなり得る攻撃手法として「A2B 攻撃」への注意を呼びかけました。これを受け、総務省も事業者に対してセキュリティ対策の徹底を求めています。

A2B 攻撃（App-to-Backend Attack）とは

スマートフォンのアプリは、ログインや情報の表示など、さまざまな処理をアプリの裏側にあるサーバーと連携して行っています。このとき、アプリがサーバーの機能や情報を利用するための窓口となるのが API（Application Programming Interface）です。

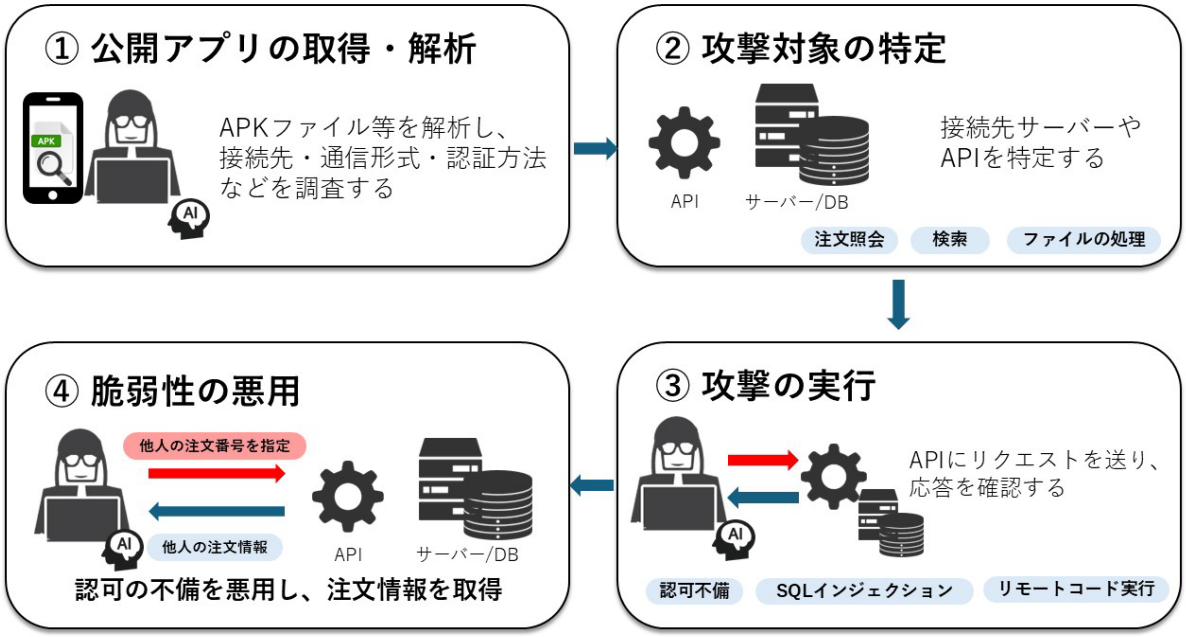
A2B 攻撃は、こうしたアプリとサーバーの連携に着目した攻撃手法です。攻撃者は一般に公開されているアプリを解析し、アプリが利用している API の接続先や通信方法などを調べます。そして、アプリを経由せずに API へ直接リクエストを送り、サーバー側のセキュリティ上の不備を探して悪用します。そのため、アプリ自体に脆弱性がなくても、API やサーバー側に脆弱性があれば、情報の不正取得などにつながる恐れがあります。



注文照会システムを例にした API による処理の流れ

攻撃の流れ

ここでは注文照会 API を例に、攻撃者が公開アプリを解析し、自身のアカウントを用いて他人の注文情報へのアクセスを試みるまでの流れを説明します。



A2B 攻撃の流れ（概念図）

1. 公開アプリの取得･解析

攻撃者は、ストアなどで公開されているアプリを入手し、解析ツールなどを使って内部の処理を解析します。プログラムの処理を調査することで、サーバーの接続先や API へのリクエスト形式、認証方法などの情報を収集します。

2. 攻撃対象の特定

解析した情報をもとに、アプリが通信するサーバーのうち、利用者情報や注文情報を扱う API など、狙う対象を絞り込みます。あわせて、検索機能やファイル処理機能など、不備が潜んでいそうな機能に目星を付けます。この段階では、まだサーバーへの攻撃は行いません。

3. 攻撃の実行

攻撃者は、絞り込んだ API の仕様に合わせてリクエストを作成し、サーバーへ直接送信します。リクエストの内容を変えながら応答を確認し、認可の不備や SQL インジェクション、リモートコード実行につながる脆弱性がないか

を検証します。

4.　脆弱性の悪用

API に認可や入力値の検証に関する不備がある場合、攻撃者はその不備を悪用し、本来許可されていない情報の取得や操作を試みます。

注文照会 API の例では、要求された注文情報を閲覧する権限があるかを適切に確認していない場合、他人の注文情報が返される可能性があります。その結果、攻撃者は他人の購入履歴や配送先などを不正に取得する恐れがあります。

どのような脆弱性が狙われるか

前述の例では、注文履歴へのアクセスを許可してよいかを確認する「認可」に不備があるため、攻撃者が他人の注文情報を取得できてしまいます。

攻撃者が狙うのは、このような認可の不備だけではありません。アプリを解析して、検索機能やファイル処理機能などを見つけ、サーバー側に不備がないかを調査します。ここでは、A2B 攻撃で狙われる脆弱性の例を紹介します。

■　認可不備（IDOR／BOLA）

IDOR（Insecure Direct Object Reference）や BOLA（Broken Object Level Authorization）は、注文番号などを指定して情報を取得する際に、その利用者に閲覧する権限があるかを適切に確認していないことで、他人の情報にアクセスできてしまう脆弱性です。情報を更新する API に同様の不備があれば、他人の登録内容を書き換えられる可能性もあります。

■　SQL インジェクション

SQL とは、データベースに検索や更新を指示するための言語です。アプリが外部から入力された検索語などを不適切な方法で SQL 文に組み込んでいると、攻撃者が細工した入力によって、開発者が意図しない SQL 文が実行されてしまいます。その結果、本来は閲覧できない情報を取得される恐れがあります。

■　SSRF（Server-Side Request Forgery）

サーバーから別のシステムへアクセスする機能を悪用する脆弱性です。例えば、URL を指定して画像を取得する機能で、接続先が適切に制限されていない場合、攻撃者は外部から直接アクセスできない内部システムなどに、サーバーを通じてアクセスできる恐れがあります。

■　リモートコード実行につながる不備

攻撃者が、離れた場所からサーバー上でコードやコマンドを実行できてしまう不備です。例えば、ファイル変換機能が外部から受け取った値を不適切に OS コマンドに組み込むと、攻撃者がサーバー上のアプリケーションと同じ

権限で任意のコマンドを実行できる場合があります。

なぜ今、A2B 攻撃が注目されているのか

公開アプリを解析し、接続先の API を狙う攻撃は、生成 AI の登場以前から存在しました。従来は、攻撃者が長い時間をかけてアプリのコードを読み解き、通信方法やサーバーの脆弱性を調べる必要がありました。
例えば、大量のコードから API に関係する処理を探したり、API へのリクエスト形式や認証方法を読み解いたりする作業や、得られた情報をもとに攻撃コードを作成して、検証する作業などが必要で、この攻撃を実現するためには高い技術力と人間の労力を必要としました。しかし、最近は生成 AI を悪用することで、こうした作業は自動化・効率化できるようになっています。
これまで A2B 攻撃を実現する上で必要とされた技術力や人的労力のハードルが生成 AI によって大幅に下がれば、攻撃者がより頻繁に攻撃を試すであろうことは容易に想像できます。
A2B 攻撃の対象となり得るアプリは数多く存在しますが、これまで実質的被害が少なかったために対策が手薄になっている可能性があります。脆弱性を放置すれば、類似の攻撃が今後ますます拡大する恐れもあります。このような背景から注意喚起と対策の推進が広く呼びかけられています。

アプリを公開する企業ができること

A2B 攻撃では、公開アプリを解析し、そこで得た情報をもとにサーバーの脆弱性が狙われます。そのため、アプリの通信方法を知られることを前提に、サーバー側の安全性を確保することが重要です。
まずは、公開中のアプリからアクセスできる API やサーバーを洗い出しましょう。現在使用しているものだけでなく、旧バージョンのアプリや開発用の API も確認してください。アプリの開発やサーバーの運用を外部に委託している場合は、委託先にも A2B 攻撃への注意を呼びかけ、API やサーバーの利用状況を確認したうえで、以下の対応を委託先と協力して進めましょう。

1. 侵害の確認

API やサーバーのログを確認し、不審なアクセスや情報の不正取得がないかを調査します。
例えば、注文照会 API では、同じアカウントから短時間に多数の注文番号が照会されていないかを確認します。認可に不備がある場合、不正なリクエストでも正常に処理されることがあるため、エラーの記録だけでなく、成功したリクエストも確認してください。
不審なアクセスが見つかった場合は、照会したアカウントと注文を行ったユーザーを確認し、どの情報が取得された可能性があるかを、残されているログなどから調査します。

2. 脆弱性の点検

公開アプリから利用できる API やサーバーに、認証・認可や入力値の検証などの不備がないかを確認します。例えば、検証用に 2 つのアカウントを用意し、一方のアカウントで他方の注文情報を閲覧できないことを確認します。

また、検索機能やファイル処理機能などに、SQL インジェクションや OS コマンドインジェクションなどの脆弱性がないかを調査します。外部サービスへのアクセス権を持つ API キーや秘密鍵が、アプリに埋め込まれていないかも確認しましょう。

3. 暫定的な緩和策

不要になった旧バージョンの API や開発用 API は、利用状況を確認したうえで停止しましょう。また、漏えいが疑われる API キーや認証情報は、影響を確認したうえで無効化し、必要に応じて再発行を実施してください。

脆弱性が見つかり、すぐに修正できない場合は、対象機能の利用やアクセス元を制限します。また、不審なアクセスを早期に発見するため、ログの監視を強化します。短時間の大量アクセスに対しては、リクエストの回数を制限するレート制限も有効です。

これらの対策で被害のリスクを抑えつつ、確認された脆弱性を修正しましょう。

利用者が情報漏えいに備えてできること

どのようなサービスでも、情報が漏えいしてしまう可能性はあります。A2B 攻撃のように利用者側では対策が難しい攻撃もありますが、日頃から情報漏えいの可能性を想定し、被害の拡大に備えることが大切です。

例えば、パスワードをサービスごとに変えておけば、あるサービスからパスワードが漏えいしても、同じ情報を使って別のサービスに不正ログインされるリスクを抑えられます。また、多要素認証を利用できる場合は、有効にしておきましょう。

利用しているサービスで情報漏えいが公表された場合は、事業者の公式サイトなどで、漏えいした可能性のある情報と対応方法を確認します。パスワードが漏えいした可能性があれば、案内に従って変更し、同じパスワードを使っているほかのサービスでも変更しましょう。

また、氏名やメールアドレス、注文情報などが漏えいした場合は、それらを悪用した偽のメールや配送通知が届く可能性があります。メール内のリンクから手続きを行う前に、公式アプリや公式サイトから直接確認しましょう。

まとめ

A2B 攻撃は、公開アプリを解析し、得られた情報をもとに接続先のサーバーを狙う手法です。アプリ自体に脆弱性がなくても、サーバー側の認証・認可や入力値の検証に不備があれば、情報漏えいなどの被害につながる恐れがあります。生成 AI の活用によって、こうした不備を探す作業が効率化され、攻撃の対象が広がることも懸念されています。

アプリを提供する企業は、アプリが解析されることを前提に、API やサーバーの脆弱性を点検し、不審なアクセスがないかを確認することが重要です。開発や運用を委託している場合は、委託先と協力して対応を進めましょう。

また、利用者は、情報が漏えいする可能性を踏まえ、パスワードの使い回しを避けるなど、日頃から被害の拡大に備えることが大切です。

■常日頃からリスク軽減するための対策について

各記事でご案内しているようなリスク軽減の対策をご案内いたします。下記の対策を実施してください。

1．セキュリティ製品の適切な利用

1-1. ESET 製品の検出エンジン（ウイルス定義データベース）をアップデートする

ESET 製品では、次々と発生する新たなマルウェアなどに対して逐次対応しています。最新の脅威に対応できるよう、検出エンジン（ウイルス定義データベース）を最新の状態にアップデートしてください。

1-2. 複数の層で守る

1 つの対策に頼りすぎることなく、エンドポイントやゲートウェイなど複数の層で守ることが重要です。

2．脆弱性への対応

2-1. セキュリティパッチを適用する

マルウェアの多くは、OS に含まれる「脆弱性」を利用してコンピューターに感染します。「Windows Update」などの OS のアップデートを行ってください。また、マルウェアの多くが狙う「脆弱性」は、Office 製品、Adobe Reader などのアプリケーションにも含まれています。各種アプリケーションのアップデートを行ってください。

2-2. 脆弱性診断を活用する

より強固なセキュリティを実現するためにも、脆弱性診断製品やサービスを活用していきましょう。

３．セキュリティ教育と体制構築

3-1．脅威が存在することを知る

「セキュリティ上の最大のリスクは“人”だ」とも言われています。知らないことに対して備えることができる人は多くありませんが、知っていることには多くの人が「危険だ」と気づくことができます。

3-2．インシデント発生時の対応を明確化する

インシデント発生時の対応を明確化しておくことも、有効な対策です。何から対処すればいいのか、何を優先して守るのか、インシデント発生時の対応を明確にすることで、万が一の事態が発生した時にも、慌てずに対処することができます。

４．情報収集と情報共有

4-1．情報収集

最新の脅威に対抗するためには、日々の情報収集が欠かせません。弊社を始め、各企業・団体から発信されるセキュリティに関する情報に目を向けましょう。

4-2．情報共有

同じ業種・業界の企業は、同じ攻撃者グループに狙われる可能性が高いと考えられます。同じ攻撃者グループの場合、同じマルウェアや戦略が使われる可能性が高いと考えられます。分野ごとの ISAC（Information Sharing and Analysis Center）における情報共有は特に効果的です。

※ESET は、ESET, spol. s r.o.の登録商標です。Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。OS X は、米国およびその他の国で登録されている Apple Inc. の商標です。

引用・出典元

●最近の不正アクセスによる個人データの漏えい等の傾向 | 個人情報保護委員会
https://www.ppc.go.jp/files/pdf/261028_sankoushiryou-2.pdf
●【注意喚起】相次ぐ情報漏洩、その原因の一つは「アプリ解析からのサーバ攻撃」 | 情報通信研究機構(NICT)
https://cynex.nict.go.jp/library/261013-01.html
●不正アクセスによる情報漏えい等の事案を踏まえた対応について（公開アプリの解析情報を悪用した攻撃への注意喚起） | 総務省
https://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000680.html
●直近で相次いでいる国内組織における不正アクセスに関する注意喚起 | JPCERT/CC
https://www.jpcert.or.jp/at/2026/at260030.html

Canon

キヤノンマーケティングジャパン株式会社