2026年
3月
MARCH

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

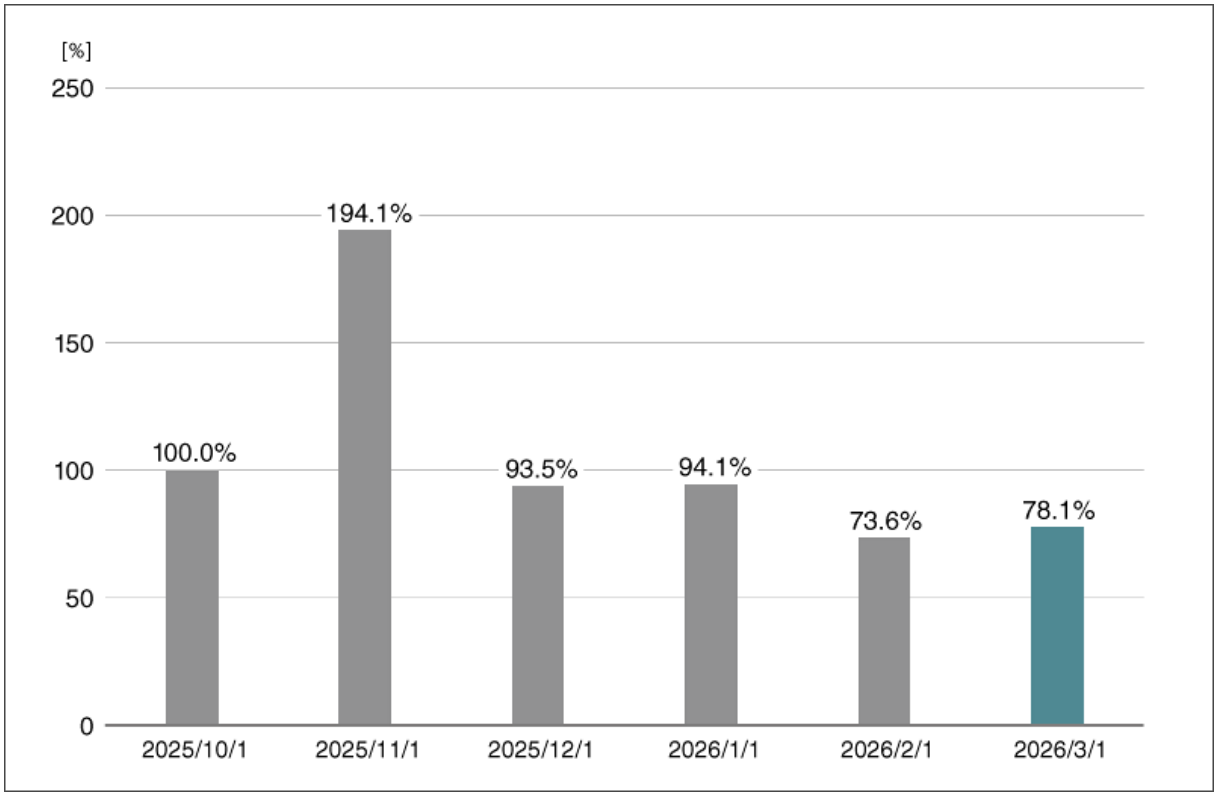
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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 3 月マルウェア検出状況

2026 年 3 月（3 月 1 日～3 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

(2025 年 10 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 3 月の国内マルウェア検出数は、2026 年 2 月と比較して微増しました。検出されたマルウェアの内訳は以下のとおりです。

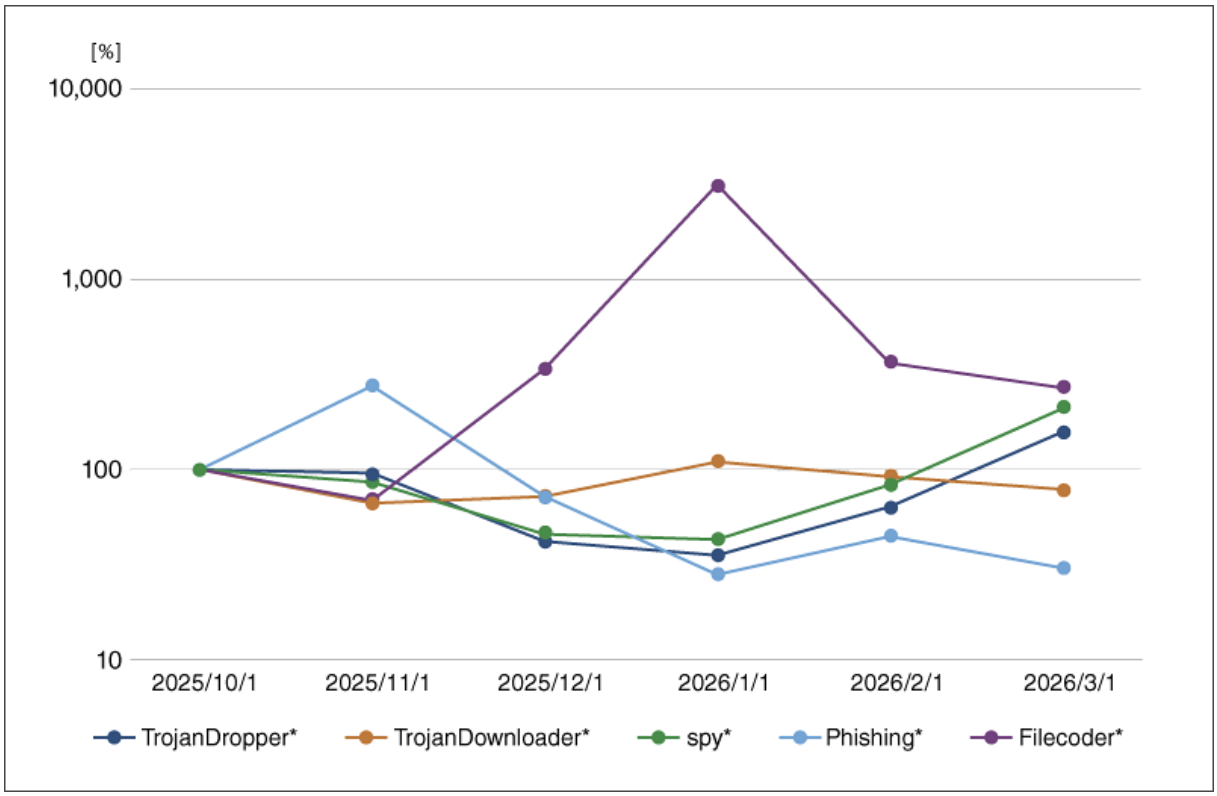
国内マルウェア検出数*2 上位（2026 年 3 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	19.8%	アドウェア
2	HTML/Phishing.Agent	13.1%	メールに添付された不正な HTML ファイル
3	DOC/Fraud	11.0%	詐欺サイトのリンクが埋め込まれた DOC ファイル
4	JS/Danger.ScriptAttachment	3.3%	ダウンローダー
5	DOC/TrojanDropper.Agent	2.2%	ドロッパー
6	MSIL/Agent	2.1%	不正な.NET プログラムの汎用検出名
7	HTML/Fraud	1.8%	詐欺サイトのリンクが埋め込まれた HTML ファイル
8	Win64/Agent	1.7%	不正な 64bit プログラムの汎用検出名
9	JS/TrojanDownloader.Agent	1.7%	不正な JavaScript の汎用検出名
10	JS/Agent	1.5%	不正な JavaScript の汎用検出名

*2 本表には PUA を含めていません。

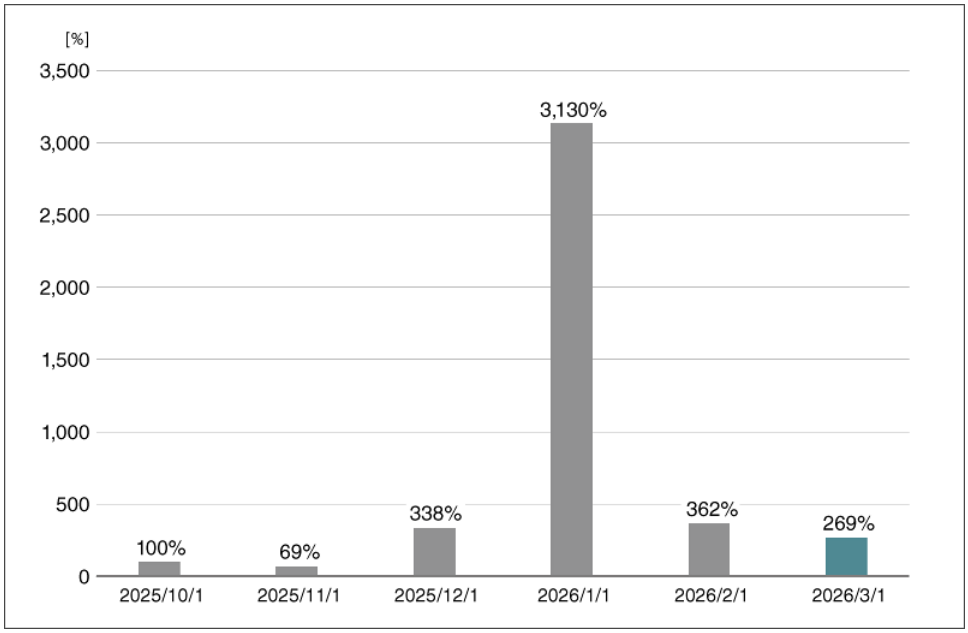
3 月に国内で最も多く検出されたマルウェアは、JS/Adware.Agent でした。
JS/Adware.Agent は、悪意のある広告を表示させるアドウェアの汎用検出名です。Web サイト閲覧時に実行されます。

2026 年 3 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。



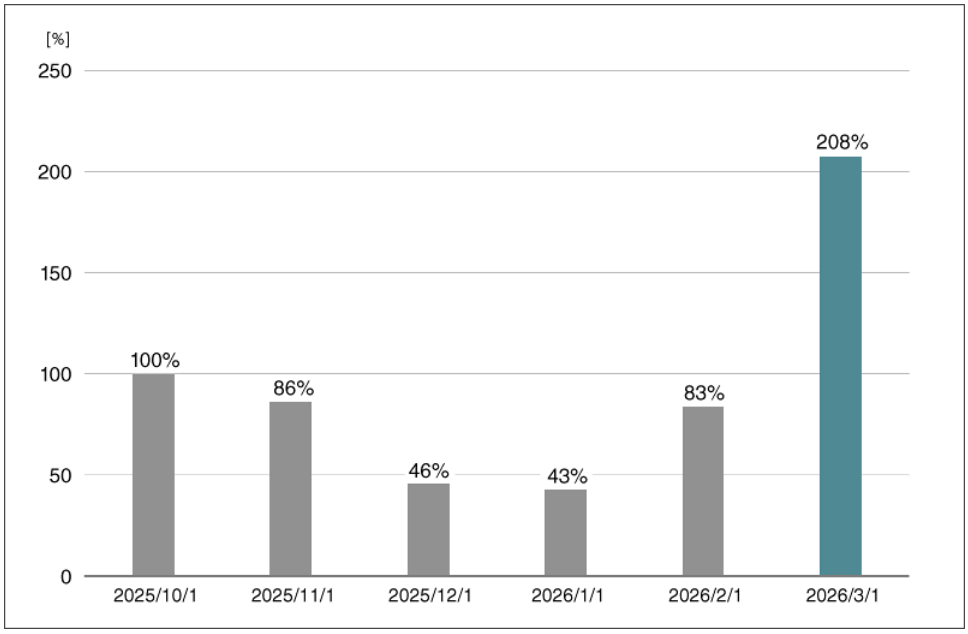
国内マルウェアの種類別検出数の推移
（2025 年 10 月の各検出数を 100%として比較）

2026 年 3 月は 2 月から引き続きスパイウェアとドロッパーの検出数が増加しました。



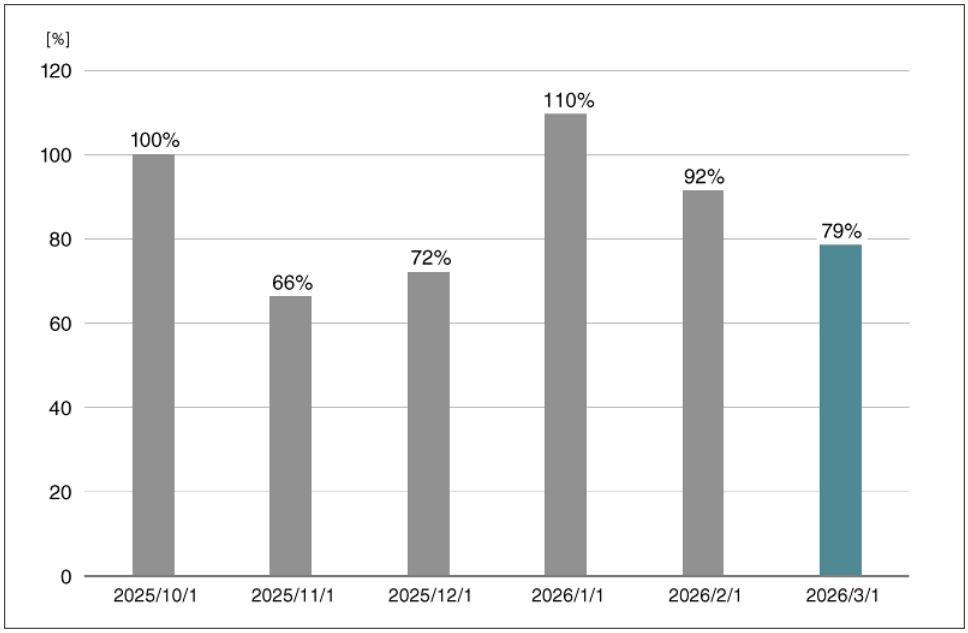
ランサムウェア検出数の推移（国内）

（2025 年 10 月の検出数を 100%として比較）



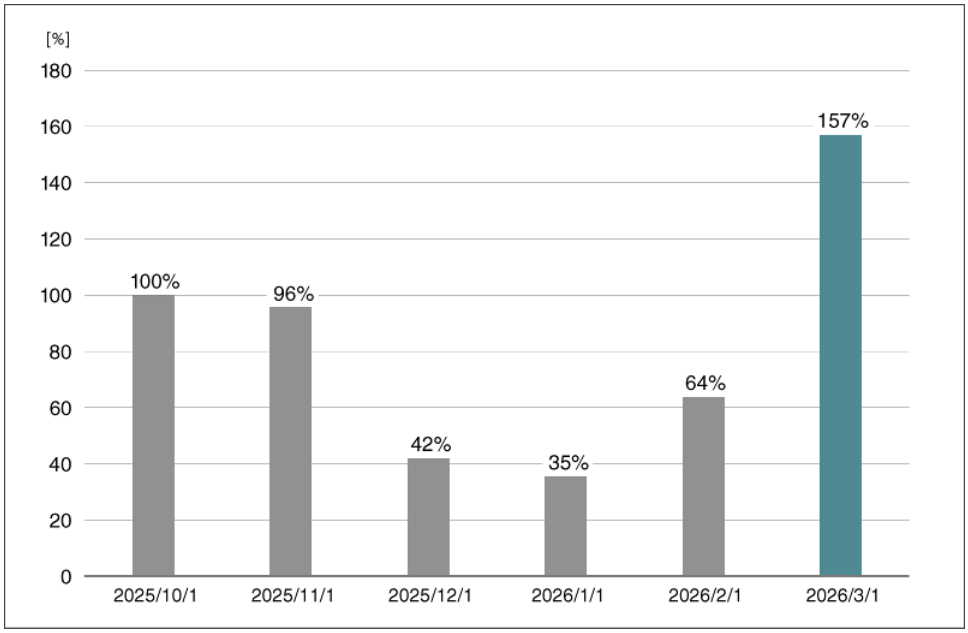
スパイウェア検出数の推移（国内）

（2025 年 10 月の検出数を 100%として比較）



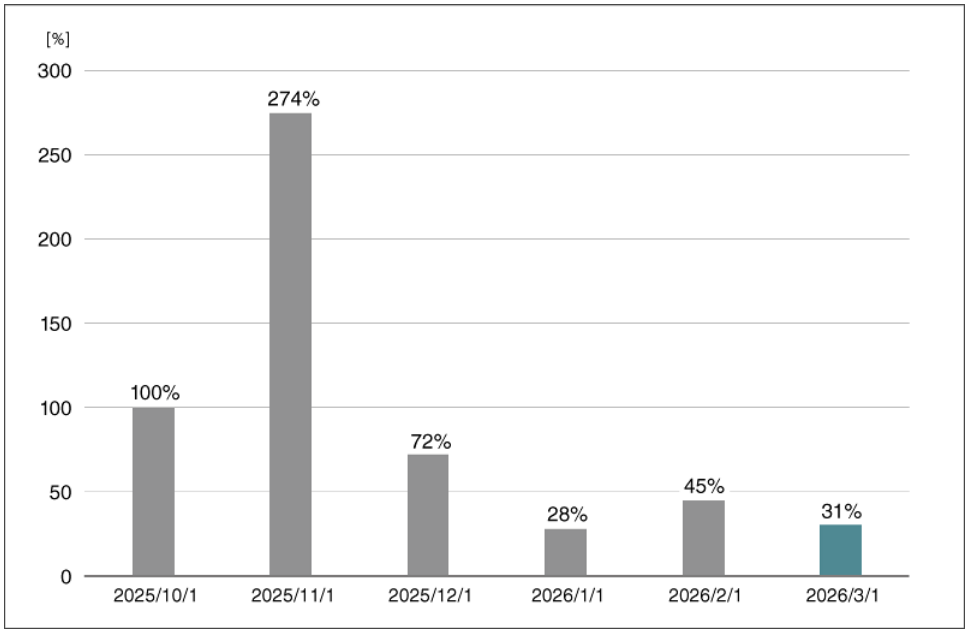
ダウンローダー検出数の推移（国内）

（2025 年 10 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）

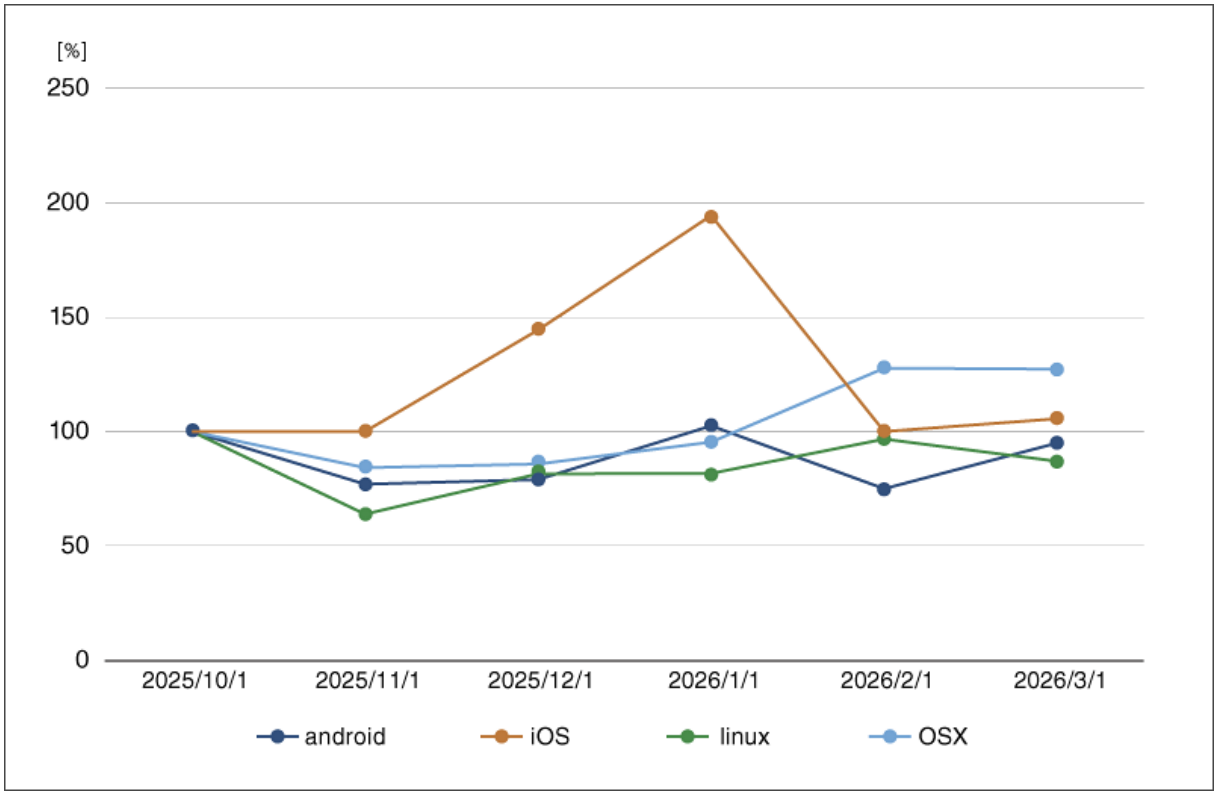
（2025 年 10 月の検出数を 100%として比較）



フィッシング検出数の推移（国内）

（2025 年 10 月の検出数を 100%として比較）

2026 年 3 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。

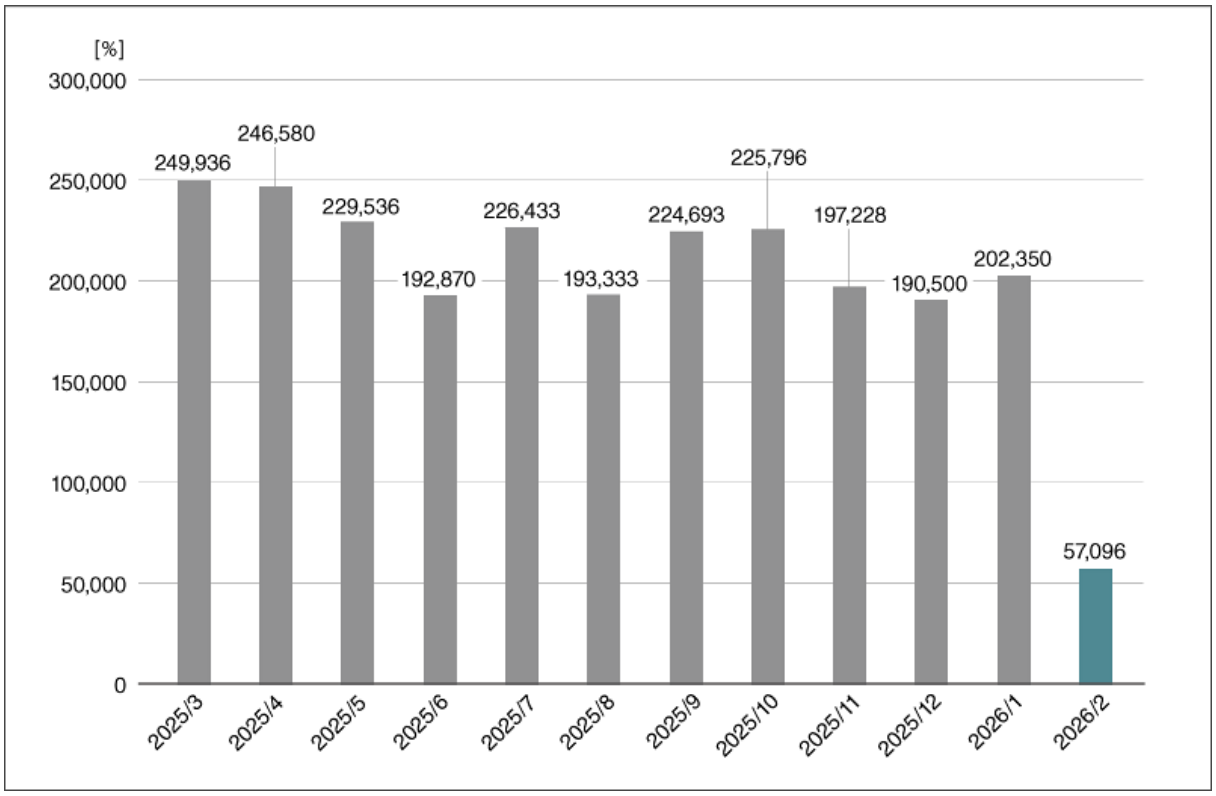


国内マルウェアの OS 別検出数の推移（Windows を除く）
（2025 年 10 月の各検出数を 100%として比較）

2026 年 3 月は Android を狙ったマルウェアが増加しました。一方で、Linux を狙ったマルウェアは減少しました。

フィッシング統計の変化から見る最新のフィッシング手法

日本国内におけるフィッシング詐欺被害の抑制を目的として活動するフィッシング対策協議会は、寄せられたフィッシング報告に関する統計情報を毎月公開しています。同協議会が公表した 2026 年 2 月のデータによると、フィッシング報告件数は 57,096 件となり、前月から 145,254 件の減少となりました。



2026 年 2 月のフィッシング報告件数
（フィッシング対策協議会が毎月公開しているデータから作成）

上記グラフからもわかるように、2026 年 2 月のフィッシング報告件数は先月比で大幅減少となっています。過去のデータから、年初にあたる 1 月 2 月は報告件数が減少する傾向にあることがわかりますが、70%に近い減少は過去に例を見ない水準です。
2026 年 3 月のマルウェアレポートでは、フィッシングに関する最新の統計を紹介し、フィッシング手法の近年の変化について分析を行います。

統計データから見る傾向

改めてフィッシング対策協議会の統計データを確認し、フィッシング報告件数の減少について分析を行います。また、レポート前半で紹介している ESET の統計データからフィッシングに関するものを抜き出し、フィッシング対策協議会の統計データと比較します。

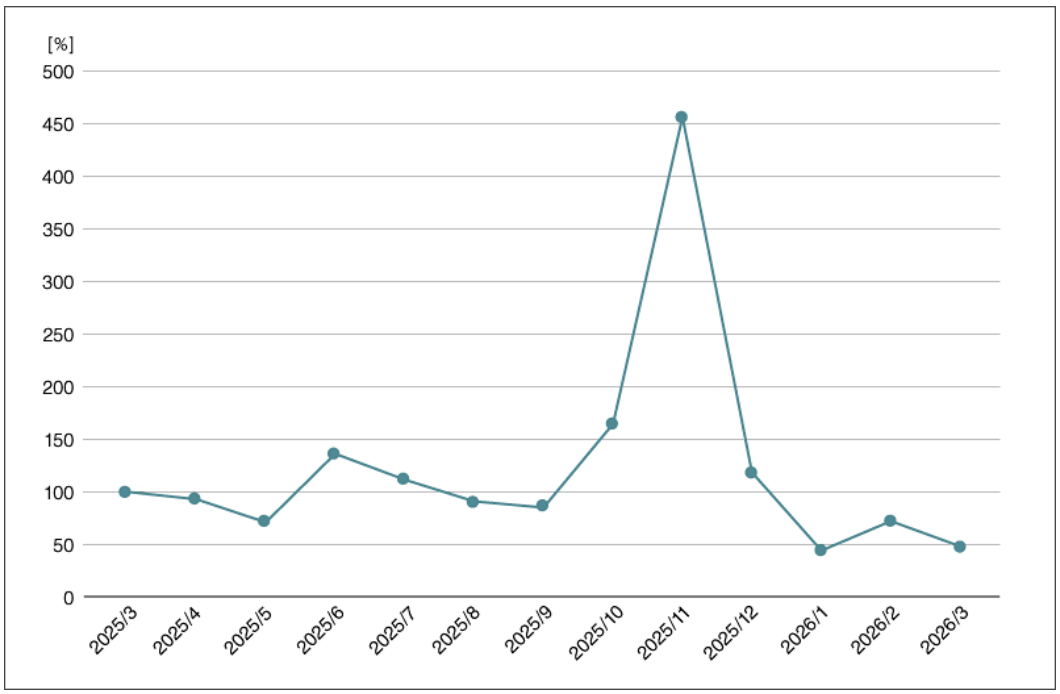
フィッシング対策協議会が公開している統計データは、

- フィッシング報告件数
- フィッシングサイトの URL 件数
- フィッシングに悪用されたブランド件数

の 3 種類です。また、これらのほかにフィッシングメールの送信元に関するデータも公開しています。

3 種類のデータのうち、大幅な減少を記録したのは、フィッシング報告件数とフィッシングサイトの URL 件数の 2 種類でした。フィッシングに悪用されたブランド件数は先月比で微減していますが、ほかの 2 種類と比べると誤差の範囲に収まる減少となっています。
これらのデータから、特定のブランドを悪用する攻撃が減少したわけではなく、幅広くフィッシングの報告が減少したものと推測できます。
フィッシング報告件数の減少の要因として、フィッシング対策協議会は「1 月末に行われた海外におけるレジデンシャルプロキシやボットネットの無力化等の影響」「2 月半ば以降の旧正月休暇期間には報告が 1 月と比較して大幅に減少したこと」の 2 点を挙げています。

フィッシング件数の減少は歓迎するべきことです。しかし、フィッシング対策協議会が公開しているデータは、一般ユーザーや企業などから寄せられた通報件数に基づくものであり、実際の被害状況の全体像を反映しているとは限りません。
そのため、特定の指標のみに依拠するのではなく、複数の観点から状況を捉えることが重要です。ここでは、フィッシング対策協議会のデータに加え、ESET が保有する統計データもあわせて確認し、より多角的にフィッシングの動向を分析していきます。



ESET が保有するフィッシングのマルウェア検出数の推移（国内）
（2025 年 3 月の検出数を 100%として比較）

ESET の統計データからは以下の傾向を読み取ることができます。

- 2025 年 11 月の検出数が突出して多かったこと
- 2026 年 2 月は 2025 年の平均値と比較すると低水準であるものの、極端な減少は記録していないこと
- 直近の 2026 年 1 月と比較すると、2026 年 2 月はむしろ検出数が増加していること

このように、ESET の統計データはフィッシング対策協議会の統計データとは異なる傾向を示しています。また、ESET の統計データにおけるフィッシング検出数の大部分を HTML/Phishing.Agent が占めており、2025 年 11 月は同検出が特に多かった月となっています。

これらの 2 種類の統計データは、いずれか一方が正しく、もう一方が誤っているというものではありません。ただ、単純にフィッシングの攻撃が減少していると判断することは適切ではないと、本分析から示唆されます。また、2 種類の統計データの差異を踏まえると、フィッシングの攻撃手法がよりユーザーに気づかれにくい巧妙な形に変化しているのではないかと推測できます。

最新のフィッシング手法

ここからは最新のフィッシング手法について紹介していきます。

- AI 技術を悪用したフィッシング
- ディープフェイク技術を悪用したフィッシング
- フィッシングのマルチチャネル化

上の 3 手法について順番に取り上げます。

- **AI 技術を悪用したフィッシング**

AI 技術が活用されるシーンは日常の中でも増えてきていますが、それと比例するように AI 技術が攻撃者に悪用されるケースも増加しています。

AI 技術はフィッシングメールの文面をより自然なものにするだけでなく、過去のやり取りを踏まえた自動応答により、あたかも実在の相手と会話しているかのように振る舞うことも可能にしています。また、フィッシングサイトについても、単に見た目を模倣するだけでなく、ログイン後の画面や購入フローなどの機能面まで再現され、本物と区別がつきにくくなっています。

アメリカのサイバーセキュリティ企業である Vectra AI は、「AI 技術の登場で、フィッシングサイトやフィッシングメールの作成にかかるコストは従来の 10 分の 1 以下に減少し、ターゲットのクリック率は 4 倍以上に増加した」という統計データを公開しています。

AI を悪用したフィッシングは質と量の両面で脅威と捉えることができます。今後、フィッシングに AI を組み合わせる手法は攻撃者のスタンダードになっていくことでしょう。

- **ディープフェイク技術を悪用したフィッシング**

分類としては上の AI 技術を悪用したフィッシングに近いですが、より標的型攻撃の性質が強いことから、本レポートでは個別に取り上げます。

ディープフェイクとは、AI 技術を用いて作成された偽の画像や音声、映像などを指します。昨今のフィッシングでは、ディープフェイク技術で作成された著名人や被害者の身近な人の顔や声を用いてターゲットを騙す事例が確認されています。中には、ビデオ会議に参加したものの、ほかの参加者が全員ディープフェイクで作られた偽物であり、騙された結果、攻撃者に多額の送金を行ってしまったというケースもありました。

こうしたフィッシング攻撃は、従来の不特定多数をターゲットにしたものとは異なり、特定のターゲットに対して事前準備を行った上で実行されます。そのため、対策についても従来のフィッシングとは異なる観点から行う必要があります。

- **フィッシングのマルチチャネル化**

従来のフィッシング攻撃では、フィッシングサイトやフィッシングメールといった単一のチャネル（媒体）を介して情報を窃取する手法が主流でした。近年では、複数のチャネルや段階を経由して情報を窃取するマルチチャネル型のフィッシング攻撃が増加しています。
マルチチャネル型フィッシングの例を以下に示します。

- メールで最初の接触を行い、誘導先の Teams のチャットで信頼関係を構築し、マルウェアをインストールさせる
- Google カレンダーでイベントを送信し、会議に参加したユーザーを偽のログインページへ誘導する

このように複数の要素を介することで、ユーザーが設定したセキュリティを回避できるほか、ユーザーが攻撃者を信頼してしまう状況が生まれます。

フィッシングに対する対策

ここまで紹介してきたように、近年のフィッシング攻撃は AI 技術の発展により高度化し、単純な注意喚起だけでは防ぐことが難しくなっています。そのため、従来の対策に加え、技術的対策・運用的対策・人的対策を組み合わせた多層防御が重要となります。
それぞれの対策から代表的なものを紹介します。

- 技術的対策：多要素認証（MFA）・パスキーの導入
- 運用的対策：重要操作における承認プロセスの徹底
- 人的対策：フィッシングに対する認識のアップデート

技術的対策としては、やはり MFA の導入が重要になります。ID とパスワードのみで認証を行っていると、それらが流出した際に無防備になってしまいます。容易に流出しない要素、すなわち本人に依存する要素を認証に組み込むようにしましょう。また、「機密情報を取り扱うサービスでは MFA を必須とする」といった形でルール化し設定漏れがないか定期的に確認する必要があります。
加えて、近年はパスワードそのものに依存しない認証方式として「パスキー」が注目されています。パスキーは端末や生体認証と紐づいた仕組みであり、フィッシングサイトに対して認証情報が送信されない設計となっています。そのため、従来のパスワード＋MFA による認証方式と比較して高い安全性が期待できます。

また、運用的対策としては、権限を個人で完結させずに、重要操作における承認プロセスを徹底することが大切です。ユーザーがフィッシングに騙されてしまうと、技術的な対策が困難になってしまうため、判断に第三者の承認を求める必要があります。複数人による承認や、異なるチャネルでの再確認（電話や対面確認など）を行うことで、不正な操作の実行を防ぐ効果が期待できます。
さらに、人的対策としては、フィッシングに対する認識のアップデートが不可欠です。従来の「不審な日本語」や「怪しい URL」といった判断基準は、AI 技術の発展により通用しなくなりつつあります。そのため、ユーザー個人の判断に依存する対策には限界があることを前提とし、「誤って操作しても被害が拡大しない設計」を行うことが重要です。
具体的には、認証情報の入力先を限定する仕組みや異常なログイン・操作を検知する監視、重要操作に対する追加認証や承認フローの導入などが挙げられます。

まとめ

今月の月次マルウェアレポートでは、フィッシング対策協議会の統計データと ESET の統計データを比較し、統計データの変化について考察しました。また、データの変化に基づき、近年のフィッシング手法の変化について紹介しました。
フィッシング対策協議会の統計データにおけるフィッシング報告件数の減少は、必ずしもフィッシング攻撃の件数の減少を意味しません。そのため、複数の観点からフィッシングの現状を理解しておく必要があります。
AI 技術の悪用やディープフェイクの悪用、さらにマルチチャネル化によって、フィッシング手法はますます巧妙なものに変化しています。特に標的型攻撃の要素を持つフィッシングには注意が必要です。
技術的対策・運用的対策・人的対策を組み合わせた多層防御を構築して、フィッシング攻撃の被害を受けない体制を構築してください。

■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。

引用・出典元

●2026/02 フィッシング報告状況 | フィッシング対策協議会
https://www.antiphishing.jp/report/monthly/202602.html
●AI phishing explained: How artificial intelligence is transforming social engineering attacks | VECTRA
https://www.vectra.ai/topics/ai-phishing

Canon

キヤノンマーケティングジャパン株式会社