2025年
6月
JUNE

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

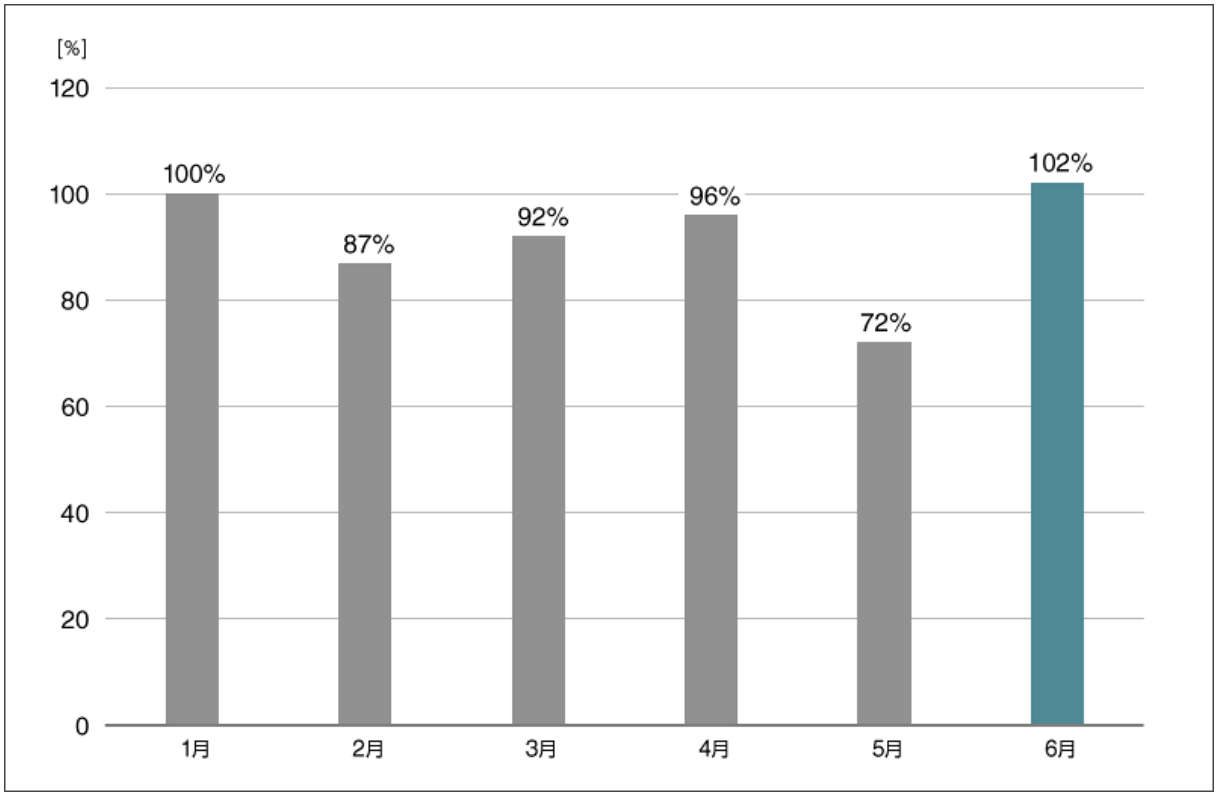
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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。

# 2025 年 6 月マルウェア検出状況

2025 年 6 月（6 月 1 日～6 月 30 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 1 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。

2025 年 6 月の国内マルウェア検出数は、2025 年 5 月と比較して増加しました。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（2025 年 6 月）**

| 順位 | マルウェア | 割合 | 種別 |
|---|---|---|---|
| 1 | DOC/Fraud | 28.5% | 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 | 19.9% | メールに添付された不正な HTML ファイル |
| 3 | JS/Adware.Agent | 12.2% | アドウェア |
| 4 | HTML/Phishing.MetaMask | 6.4% | 特定ブランドを騙ったフィッシングサイトの検出名 |
| 5 | HTML/Phishing.Gen | 1.8% | フィッシングを目的とした不正な HTML ファイル |
| 6 | JS/Agent | 1.2% | 不正な JavaScript の汎用検出名 |
| 7 | MSIL/TrojanDownloader.Agent | 1.1% | ダウンローダー |
| 8 | HTML/Phishing.WeTransfer | 1.0% | 特定ブランドを騙ったフィッシングサイトの検出名 |
| 9 | HTML/Fraud | 0.7% | 詐欺サイトのリンクが埋め込まれた HTML ファイル |
| 10 | MSIL/Spy.AgentTesla | 0.7% | 情報窃取型マルウェア |

*2 本表には PUA を含めていません。

6 月に国内で最も多く検出されたマルウェアは、前月に引き続き 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 ファイルです。主にメールの添付ファイルとして確認されており、不正な金銭の要求や個人情報の詐取といった被害に遭う可能性があるため、引き続き注意が必要です。
また、HTML/Phishing.MetaMask の検出が上位に入り、暗号資産を標的としたフィッシング攻撃が多く確認されました。

## ボイスフィッシングについて

**■ボイスフィッシング概要**

フィッシング詐欺は実在する組織を騙り被害者から個人情報や金銭を不正に入手する詐欺です。近年では、フィッシング詐欺の一種として「ボイスフィッシング」と呼ばれる音声を利用した詐欺が増加しています。ボイスフィッシングとは、電話や自動音声ガイダンスなどの音声を用いて被害者から個人情報や機密情報を不正に入手する手法です。音声（Voice）とフィッシング（Phishing）を合わせて、ビッシング（Vishing）と呼ばれることもあります。現在確認されている事例では主に 2 パターンの手口があります。

①直接個人情報を聞き出す手口
行政機関や金融機関を装って、被害者に電話をかけ、口座番号や暗証番号などの個人情報を聞き出す手口です。
例：「口座に不正アクセスがありました。本人確認のために口座番号と暗証番号を教えてください」

②フィッシングサイトに誘導する手口
行政機関や金融機関を装って、被害者に電話をかけ、メールアドレスを聞き出します。その後、偽のメールを送信し、オンラインバンキングなどの認証情報を入力するフィッシングサイトに誘導することで、個人情報を窃取します。

本レポートでは、現在被害が増加しているパターン②について解説していきます。
以下は、ボイスフィッシングの手口を時系列に沿って図示したものです。


**ボイスフィッシングの流れ**

2025 年には国内企業でボイスフィッシングによる被害が多数発生しており、警察庁や銀行から注意喚起が行われています。電話で聞き出したメールアドレスに対してフィッシングサイトの URL を送信し、フィッシングサイトから法人口座の認証情報を窃取する事例が確認されています。被害規模も大きく、1 組織あたり 1 億円以上の被害が出た事例がありました。
ボイスフィッシングは、以下の 4 つのフェーズに分けることができます。

①被害者に接触する
攻撃者は行政機関や金融機関といった実在する組織を騙り、ユーザーへ架電します。最初に自動音声ガイダンスからの着信があり、ガイダンスに従って応答すると攻撃者に直接繋がるケースも確認されています。

②被害者からメールアドレスを聞き出す
攻撃者は依頼した操作を Web 上で実施するために URL を送付するといった話から、メールアドレスを聞き出します。現在確認されている中では、攻撃者は電子証明書や法人口座情報の更新が必要という話を出し、メールアドレスを聞き出すことがありました。

③被害者をフィッシングサイトへ誘導する
聞き出したメールアドレスに対して、フィッシングサイト URL が記載されたメールを送信します。更新作業を行うために、フィッシングサイト URL へのアクセスを促します。

④被害者から情報を窃取する
ユーザーがフィッシングサイトと気づかずに対応すると、オンラインバンキングの認証情報をフィッシングサイトへ入力してしまう恐れがあります。入力してしまった場合、攻撃者に法人口座から攻撃者の口座へ不正送金が行われます。

**■攻撃者がボイスフィッシングを選ぶ理由について**
攻撃者の意図を知ることは、攻撃者の狙いや被害が増えている要因の理解を深め、ボイスフィッシング対策向上に繋がります。ここでは、攻撃者が一般的なフィッシング詐欺ではなく、ボイスフィッシングを選ぶ理由を考えます。

・従来のフィッシング詐欺と比較して情報を窃取しやすい
電話で直接働きかけ、実在する組織の担当者だと誤認させることで、被害者がフィッシングサイトへ認証情報を入力しやすくなっていると考えられます。メールなどの文章によるやり取りと異なり、声色や話すスピード、抑揚を変化させることでユーザーに対してさまざまな印象を与えることができます。場合によっては、緊急を要する対応といった緊迫感や緊張感を与えることも可能です。ほかにも、メールと比較して、返答に使える時間が短い点も情報の窃取しやすさに影響を与えています。電話ではリアルタイムに返答する必要があるため、被害者に詐欺かどうかを考える時間を与えずに会話を進めることが可能です。

・対策の難しさ
従来のフィッシング詐欺では、不特定多数のユーザーにフィッシングサイトの URL を送信します。多くのユーザーにフィッシングサイトの存在が認知されるため、悪意のあるサイトとして通報される確率が高くなり、結果としてフィッシングサイトの稼働期間が短くなる可能性があります。一方、ボイスフィッシングでは、限られたユーザーにフィッシングサイト URL を送るため、従来のフィッシング詐欺よりも通報されにくいです。第三者による通報がされにくい状況は、フィッシングサイトが長期間稼働しやすいといった利点があります。

また、近年の生成 AI 技術の進化がボイスフィッシングの手口を巧妙化させています。より自然な日本語文章の作成や特定の人物の音声に変換するボイスチェンジャーなどのツールに利用されています。音声を取り巻く生成 AI 技術の進化が、ボイスフィッシングの更なる増加につながる可能性があるため、今後も動向に注意が必要です。

**■ボイスフィッシング対策について**

本レポートで紹介したボイスフィッシングによる被害に遭わないためにも対策は欠かせません。ここでは、ボイスフィッシングに特化した対策を紹介します。

・脅威情報の組織内共有

ボイスフィッシングは電話応対が攻撃の起点となるため、特徴や手口を組織内で共有することが重要です。例えば、契約中の金融機関を名乗る着信があった場合、事前に担当者間で情報共有しておくことで、特徴や手口に照らし合わせてボイスフィッシングであるかを確認できます。

・不審な電話に対する応対ルールの整備

組織の情報セキュリティポリシーに則りながら不審な電話への応対手順や応対方法を確立することで、組織としての防御体制を強化します。具体的な対応手順としては、「電話応対時に電話番号確認を行う」が挙げられます。攻撃者が使用する電話番号は、海外から発信しているケースや実在する組織の電話番号ではない番号から発信しているケースがあります。電話応対時に発信先番号を確認することで、明らかな詐欺電話を防ぐことができます。ほかにも、電話口で個人情報や機密情報を求められた場合は、組織内での確認を経た上で、正規の電話番号を確認し、折り返し電話で対応すると決めておくことも効果があると考えます。また、これらの手順や応対方法が実際に実行できるかを定期的に訓練することも効果を高めます。

・着信拒否設定の活用

ボイスフィッシングなどの電話による脅威に対しては、着信設定の見直しが一定の効果を発揮します。例えば、電話番号の先頭に「184」をつけて非通知発信した場合や、一部の転送サービスを利用した場合のように電話番号が表示されない着信を拒否する設定を行うことで、攻撃者からの接触を減らすことができます。ほかにも、海外からの着信が不要な場合、海外番号からの着信を拒否することも可能です。ただ、これらの設定変更を行う際には、顧客からの発信を拒否するといった支障が出ないかどうかを検討する必要があります。

## まとめ

今月は増加傾向にあるボイスフィッシングについて紹介しました。ボイスフィッシングが増加している背景には、電話というリアルタイムコミュニケーションゆえの対策の難しさがあるのかもしれません。また、近年の生成 AI 技術の向上は、ボイスフィッシングの手口を巧妙化させています。今後もボイスフィッシングの動向に注意が必要です。
今一度組織における電話機器設定や電話応対手順を見直し、ボイスフィッシングなどの脅威に備えてください。

■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。

※ESET は、ESET, spol. s r.o.の登録商標です。Windows は、米国 Microsoft Corporation の、米国、日本およびその他の国における登録商標または商標です。

---

引用・出典元

●ビッシング | サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/term/detail/00194.html
●サイバー警察局便り R7Vol.1「銀行から電話・・・はたして本物？企業の資産が危ない！」| 警察庁
https://www.npa.go.jp/bureau/cyber/pdf/R7_Vol.1cpal.pdf
●中小企業狙う「ボイスフィッシング」、金融機関装う電話で「偽サイト」誘導…不正送金２８億円 | 読売新聞
https://www.yomiuri.co.jp/national/20250531-OYT1T50100/
●地銀装う「ボイスフィッシング詐欺」各地で猛威　企業口座狙い電話、億単位の実害も | ITmedia NEWS
https://www.itmedia.co.jp/news/articles/2504/07/news094.html

Canon

キヤノンマーケティングジャパン株式会社