2025年
12月
DECEMBER

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

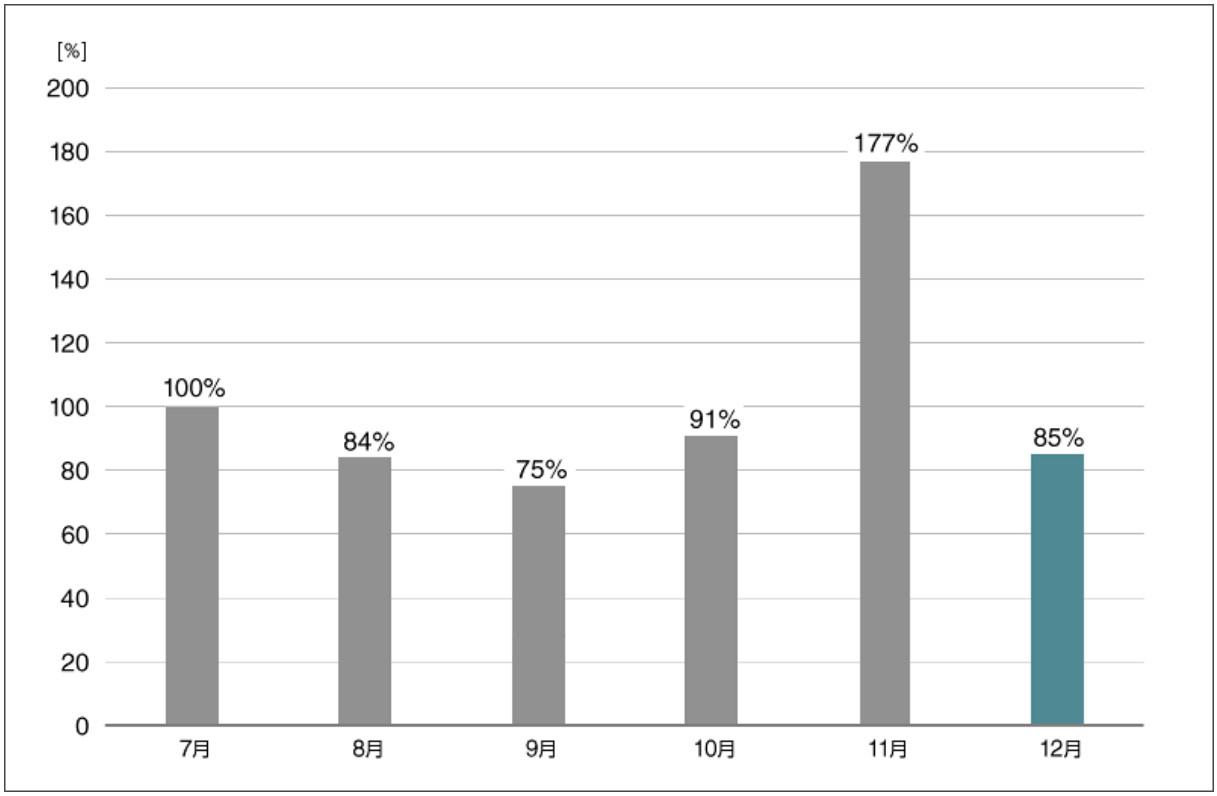
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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 12 月マルウェア検出状況

2025 年 12 月（12 月 1 日～12 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 7 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 12 月の国内マルウェア検出数は、2025 年 11 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。

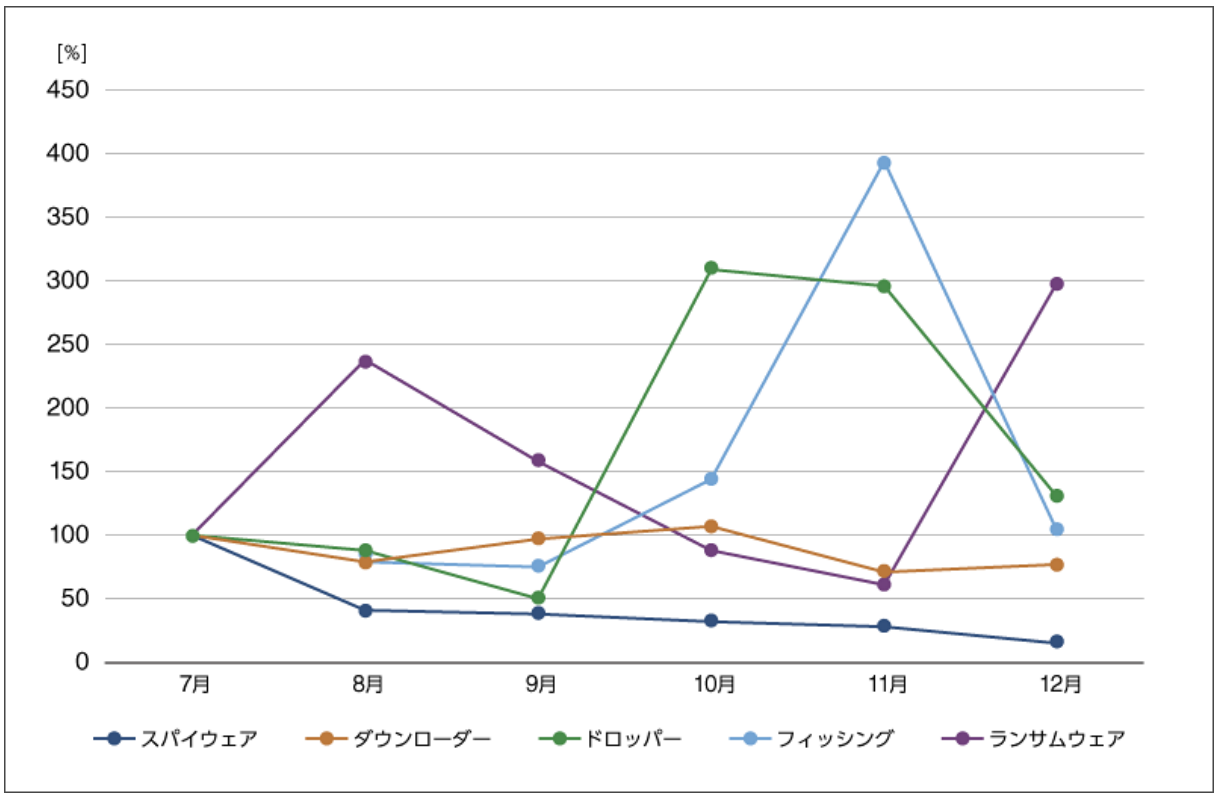
国内マルウェア検出数*2 上位（2025 年 12 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	34.4%	アドウェア
2	HTML/Phishing.Agent	29.4%	メールに添付された不正な HTML ファイル
3	DOC/Fraud	3.7%	詐欺サイトのリンクが埋め込まれた DOC ファイル
4	JS/Agent	1.4%	不正な JavaScript の汎用検出名
5	HTML/Phishing.Gen	0.8%	フィッシングを目的とした不正な HTML ファイル
6	JS/Danger.ScriptAttachment	0.7%	メールに添付された不正な JavaScript
7	DOC/TrojanDropper.Agent	0.6%	ドロッパー
8	JS/TrojanDownloader.Agent	0.6%	ダウンローダー
9	VBA/TrojanDownloader.Agent	0.6%	ダウンローダー
10	Win32/TrojanDownloader.ModiLoader	0.6%	ダウンローダー

*2 本表には PUA を含めていません。

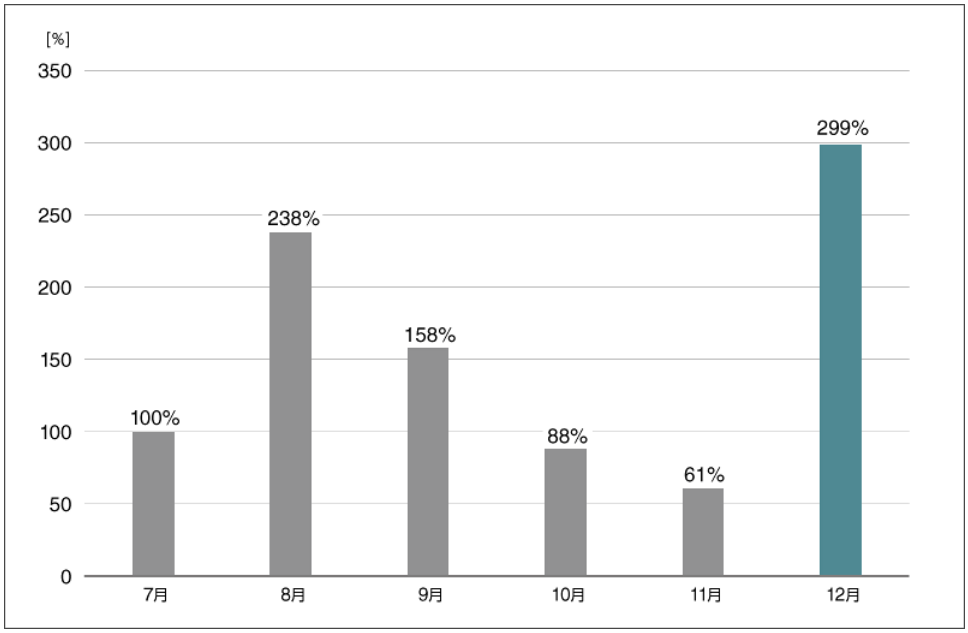
12 月に国内で最も多く検出されたマルウェアは、JS/Adware.Agent でした。
JS/Adware.Agent は、悪意のある広告を表示させるアドウェアの汎用検出名です。Web サイト閲覧時に実行されます。

2025 年 12 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。



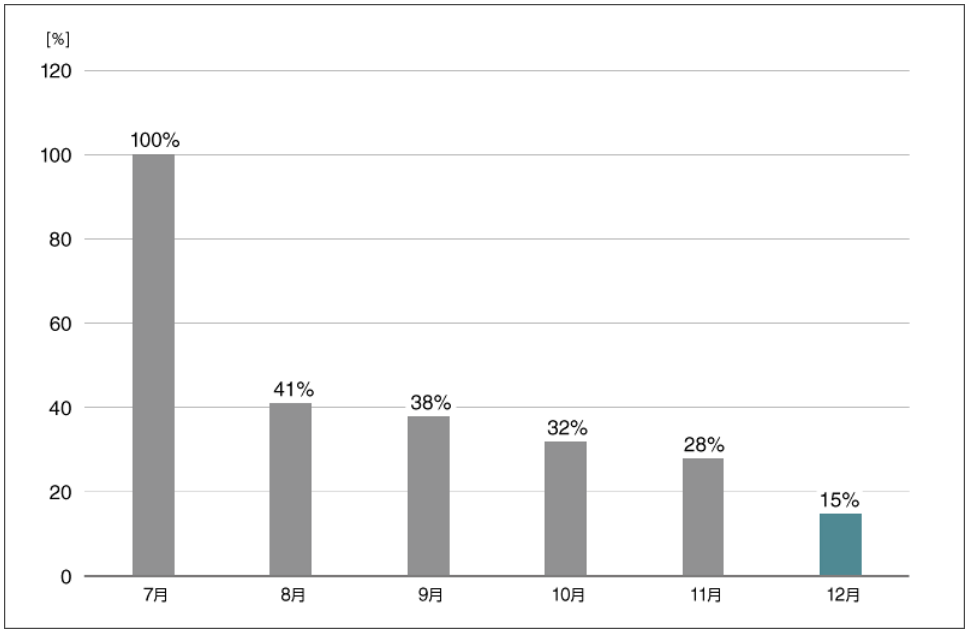
国内マルウェアの種類別検出数の推移
（2025 年 7 月の各検出数を 100%として比較）

2025 年 12 月はランサムウェアの検出数が大きく増加しました。その一方でフィッシングとドロッパーは検出数が大きく減少しました。



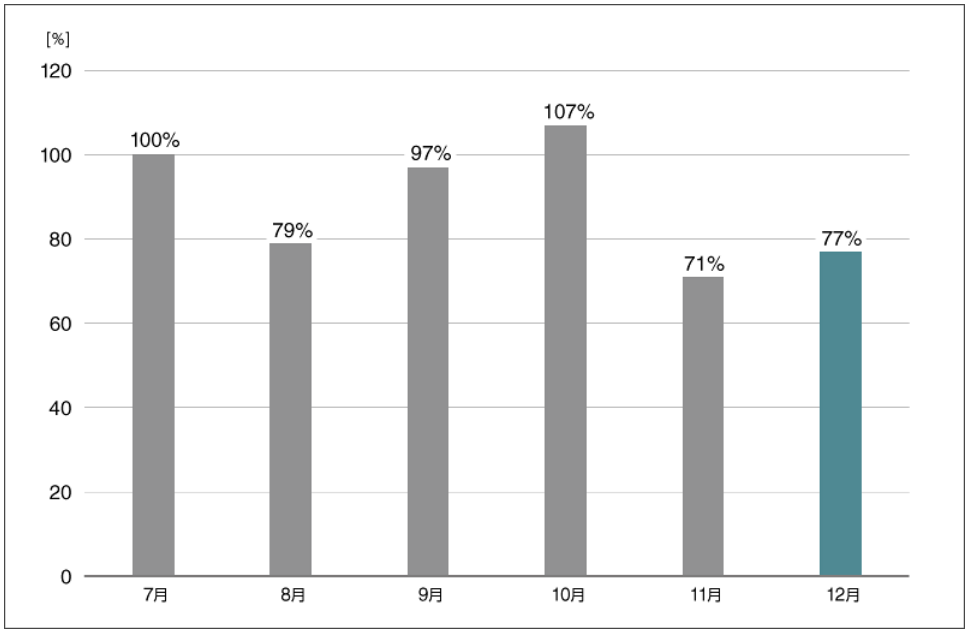
ランサムウェア検出数の推移（国内）

（2025 年 7 月の検出数を 100%として比較）



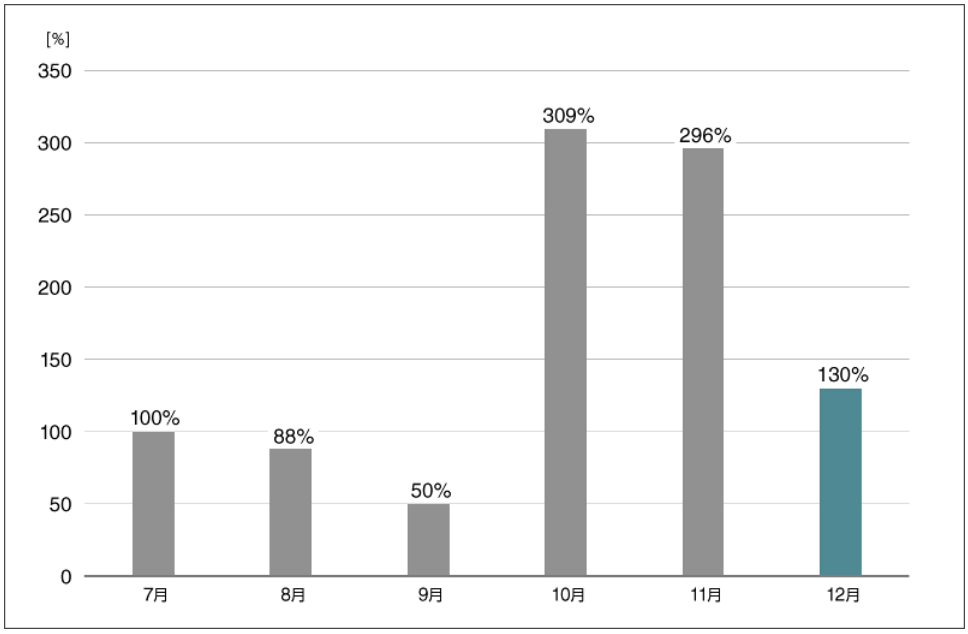
スパイウェア検出数の推移（国内）

（2025 年 7 月の検出数を 100%として比較）



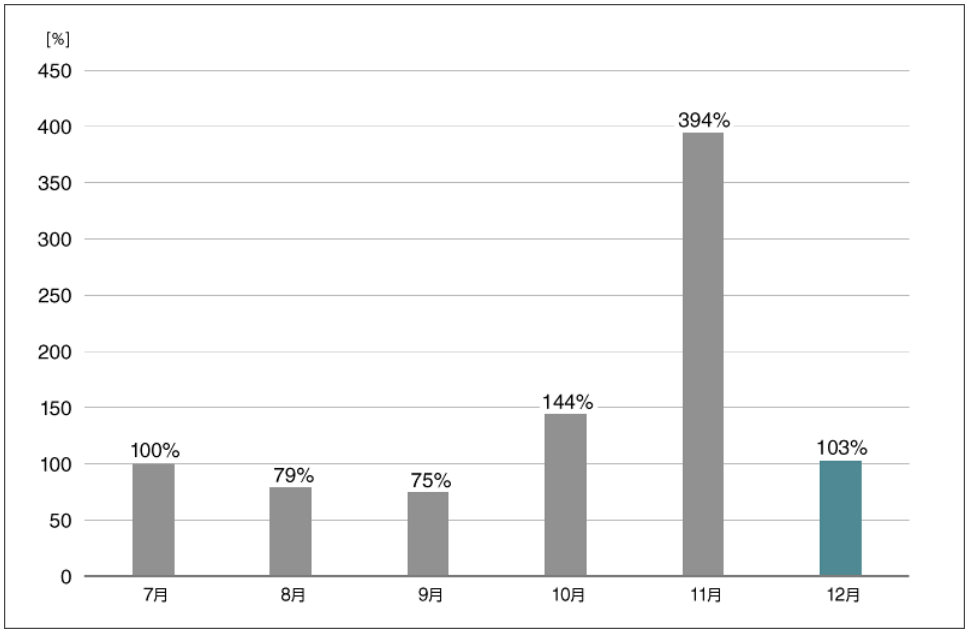
ダウンローダー検出数の推移（国内）

（2025 年 7 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）

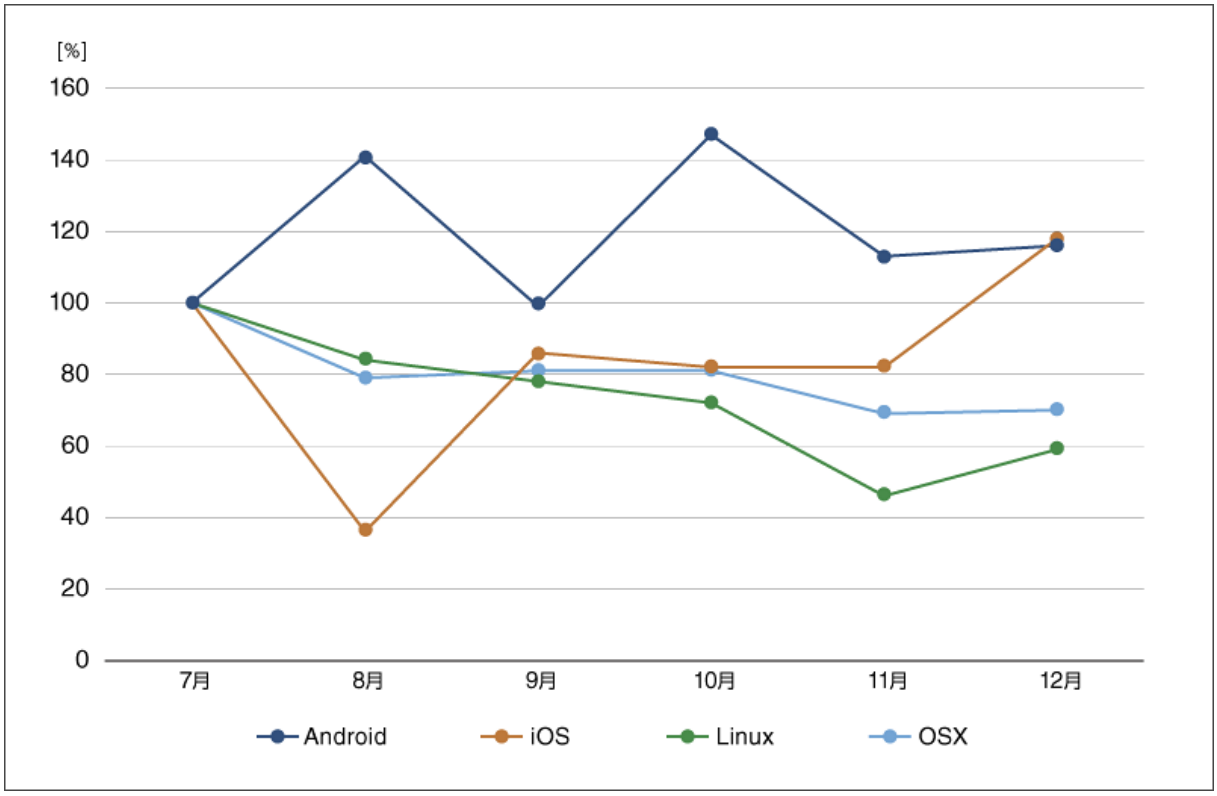
（2025 年 7 月の検出数を 100%として比較）



フィッシング検出数の推移（国内）

（2025 年 7 月の検出数を 100%として比較）

2025 年 12 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。



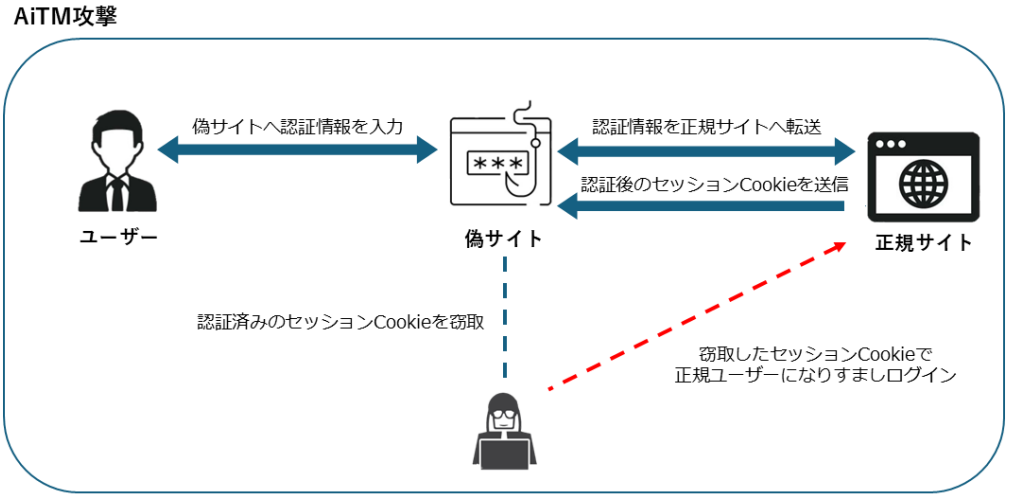
国内マルウェアの OS 別検出数の推移（Windows を除く）
（2025 年 7 月の各検出数を 100%として比較）

2025 年 12 月は iOS を標的としたマルウェアの検出数が増加しました。一方、iOS 以外では大きな変化は見られず、先月とほぼ同水準を維持しています。

多要素認証を回避する AiTM 攻撃とは

● AiTM（Adversary-in-the-Middle）攻撃の概要

AiTM（Adversary-in-the-Middle、以下 AiTM）攻撃は、中間者攻撃（Man-in-the-Middle、以下 MITM）の一種です。
MITM 攻撃とは、通信を行いたい二者の間に第三者が通信相手になりすまして割り込み、通信内容の盗聴や改ざんを行う攻撃の総称です。
一方、AiTM 攻撃は、この MITM 攻撃の中でもユーザー認証の窃取に特化した手法です。攻撃者は本物そっくりのフィッシング（リバースプロキシ）サイトを用意し、ユーザーが偽サイトへ入力した ID／パスワードや多要素認証（Multi-Factor Authentication、以下 MFA）コードを正規サイトへ中継します。これにより、Web サービス側では正規利用者のアクセスとして認証が進み、認証成功時に発行されるセッション Cookie が攻撃者に窃取されます。
その結果、攻撃者は MFA を回避し、正規ユーザーになりすまして継続的にアクセスできるようになります。



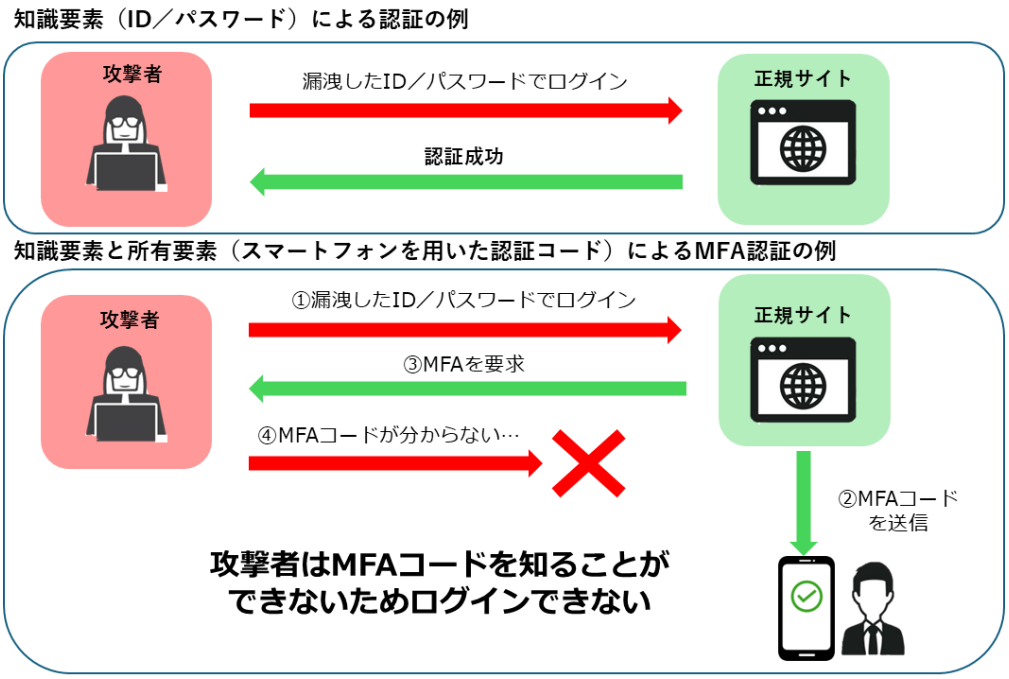
AiTM 攻撃の概要

AiTM 攻撃は、強固な認証を前提とした金融サービスやクラウドサービスへの攻撃が確認されており、近年その危険性が注目され警戒が高まっています。
2025 年初頭には、国内の証券口座で乗っ取り被害が多発しました。多くの口座で ID／パスワードのみに依存した認証方式が依然として利用されていたこともあり、認証が突破されやすい状況が続いていたと考えられます。また、この一連の被害の中には MFA を有効にしていたにもかかわらず侵害されたケースもあり、その背景として AiTM 攻撃を含む複数の手口が悪用されていたと思われます。
こうした状況を受け、金融庁は 2025 年 7 月に「金融商品取引業者等向けの総合的な監督指針」の改正案を公表し、同年 10 月に改正を実施しました。これにより、ログインや出金などの重要操作において、フィッシング耐性のある多要素認証の実装が必須化されました。その結果、証券会社を中心に認証強化が進み、乗っ取り被害は大きく減少しています（2025 年 12 月時点）。
しかし、クラウドサービスや SNS を狙った AiTM 攻撃は依然として活発であり、2026 年以降もこうした攻撃は高度化・多様化する可能性が高く、引き続き警戒が必要です。

● AiTM 攻撃による MFA の回避

MFA は、不正アクセス対策として広く導入されていますが、AiTM 攻撃ではこの仕組みをすり抜けることが可能です。まずは、MFA の基本的な仕組みを説明します。

■MFA（多要素認証）の仕組み
MFA は、ユーザーの本人確認を強化するために複数の認証要素を組み合わせる仕組みです。一般的には、「知識要素（ID、パスワードなど）」「所有要素（スマートフォンや認証アプリなど）」「生体要素（指紋や顔認証など）」のうち、2 つ以上の要素を用いて認証を行います。これにより、仮に ID やパスワードが漏えいしても、追加の認証要素がなければログインできないため、不正アクセスのリスクを大幅に軽減できます。



MFA を導入することによるセキュリティ強化のイメージ

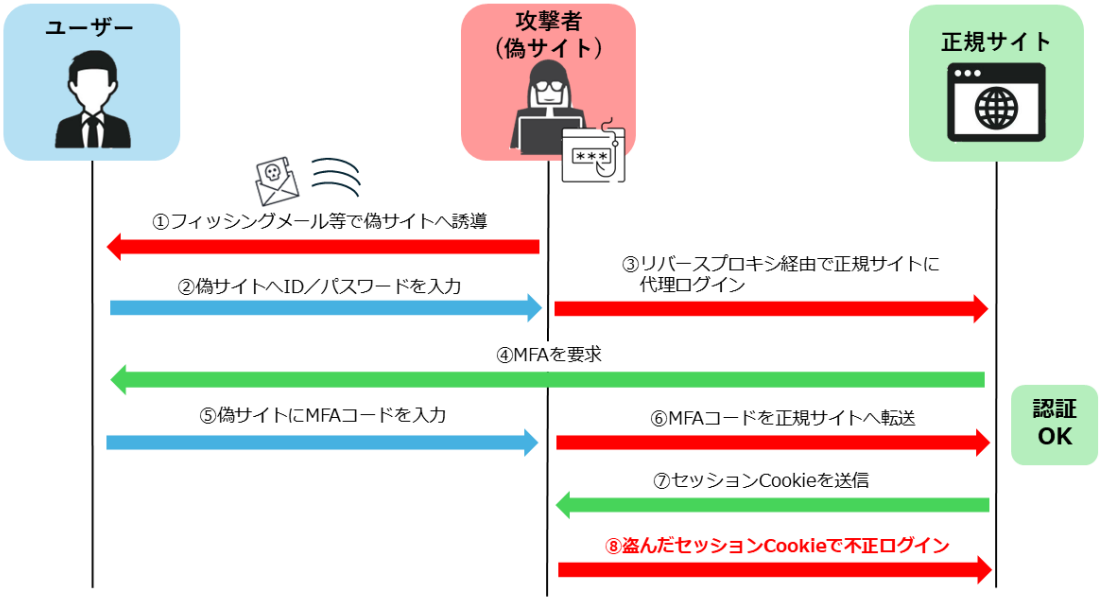
続いて、AiTM 攻撃が MFA を回避する具体的な手口について解説します。

■AiTM 攻撃の流れ

AiTM 攻撃では、攻撃者が正規の認証ページを模倣した偽サイトにユーザーを誘導し、通信を中継することで認証情報を窃取します。この手法により、ユーザーが偽サイトに入力した認証情報（ID、パスワードなど）と認証成功時のセッション Cookie 情報はすべて攻撃者に渡ることになります。

その結果、攻撃者は窃取したセッション Cookie を悪用し認証済みユーザーになりすますことができます。

以下は、攻撃の手口を時系列に沿って図示したものです。この図をもとに、攻撃の流れを 4 つのフェーズに分けて詳しく解説します。



AiTM 攻撃の流れ

1．フィッシングの下準備と誘導

攻撃者は、正規サイトを模倣した偽サイトを構築します。この偽サイトには、ユーザーが入力した情報をリアルタイムで正規サイトに転送する仕組み（リバースプロキシ）が組み込まれています。

次に、攻撃者は用意した偽サイトにユーザーを誘導します。例えばフィッシングメールで誘導する場合、巧妙な文面で偽サイトへのリンクをクリックさせるようなメールを作成して標的ユーザーに送信します。

2．偽サイトへ認証情報を入力

このページは、見た目や動作が正規サイトとほとんど変わらないため、ユーザーは疑うことなく ID・パスワード・MFA コードなどの認証情報を入力してしまいます。

3．攻撃者による通信の中継・窃取

ユーザーが偽サイトに入力した認証情報は、攻撃者によって正規サイトにリアルタイムで中継されます。正規サイト側からは、通常のユーザーアクセスと区別がつかないため、攻撃者経由の通信も正規のアクセスとして認識され、認証が成功してしまいます。

その結果、ログイン状態を維持するためのセッション Cookie が発行され、攻撃者はこれを取得して保存します。

4. 攻撃者によるセッション乗っ取り
攻撃者は、偽サイト経由で取得したセッション Cookie を使い、正規サイトにログイン済みのユーザーとしてアクセスすることができます。
その結果、攻撃者は正規ユーザーになりすまし、情報の閲覧・送金・設定変更などを継続的に行うことができます。

AiTM 攻撃への対策

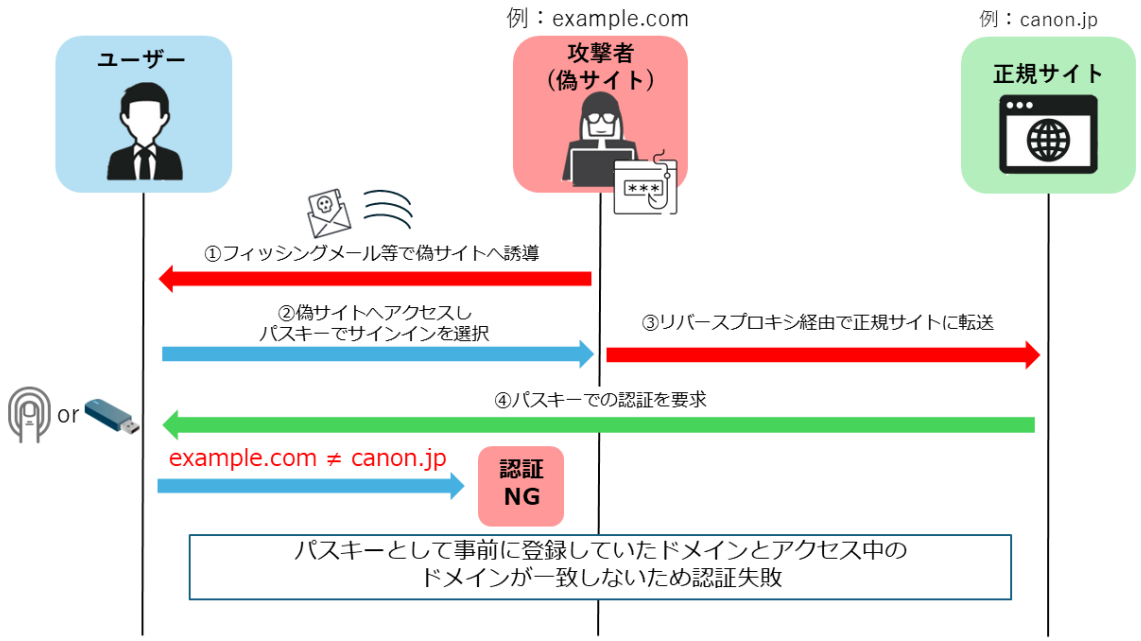
本レポートで紹介した AiTM 攻撃は、従来のフィッシング対策である MFA では防ぎきれない高度な手法です。社内のセキュリティ体制を見直し、技術的対策・教育的対策の 2 つの観点から多層的な対策を講じることが求められます。

● 技術的対策

■AiTM 攻撃の起点となる誘導を絶つ：フィッシング検知
AiTM 攻撃の多くは、フィッシングメールを起点としてユーザーを偽のログインページに誘導することで成立します。そのため、メールフィルターや URL フィルターを活用し、悪意あるリンクや添付ファイルを検知・遮断することが重要です。

■AiTM の認証仲介に対する直接的対策：パスキー
従来の MFA では、SMS やメールによるワンタイムパスワード（One-Time Password、OTP）が一般的でしたが、これらは AiTM 攻撃に対して脆弱です。
この課題に対し、FIDO2 に基づく次世代の認証方式「パスキー」が有効な対策となります。パスキーは、パスワードを使用せず、公開鍵暗号方式を用いた認証を実現することで、以下のような特長を持ちます。
- 認証はドメイン単位で紐づくため、偽サイト経由では認証が成立しない
- 毎回異なるチャレンジ（ランダムな値）を使用するため、認証情報の再利用ができない
- 認証情報は端末内に安全に保管され、外部に送信されない

これにより、AiTM 攻撃によるセッション乗っ取りのリスクを大幅に低減できます。



パスキーを使用している場合

■セッション乗っ取り後の被害を最小化：セッション管理

セッションの乗っ取りを防ぐためには、セッションの取り扱いに関する運用ルールの見直しが必要です。具体的には、以下のような対策が有効です。

- セッションの有効期限を短く設定する
- 一定時間操作がない場合は自動的にログアウトする
- 不審なセッションの挙動（短時間での複数ログインなど）を検知して強制的にログアウトする

これらはセッションの維持や扱いに関する対策であり、セッション乗っ取り被害を最小化する効果が期待できます。

■不正なアクセスをインフラでブロック：アクセス制限・リスクベース認証

セッション管理とは別の観点として、アクセス時点でブロックする制御も有効です。以下のような手法があります。

- 許可されたネットワーク（IP アドレス）および端末以外からのアクセスを拒否する
- 条件付きアクセスを利用し、リスクが高いアクセスには追加認証を要求する

ユーザーの行動や端末の状態に応じてアクセス制御を動的に変更する「条件付きアクセス」は、リスクベース認証の一種として有効です。例えば、通常とは異なる場所や端末からのアクセス時に追加認証を求めることで、不正アクセスのリスクを軽減できます。

- **教育的対策**

■安全なアクセス習慣の定着

AiTM 攻撃では、ユーザーが偽のログインページに誘導されることが前提となるため、ブックマークや公式アプリからのアクセスを習慣づけることが有効です。これにより、メールや検索結果経由で偽サイトにアクセスするリスクを減らすことができます。特に昨今の偽ログインページの識別は非常に困難であるため、安全な行動習慣を定着させることが重要です。

■フィッシングメール訓練の実施

定期的なフィッシングメール訓練を通じて、従業員の警戒心を維持し、実際の攻撃に対する耐性を高めることができます。訓練結果をもとに、教育内容や対策の見直しを行うことも有効です。

まとめ

今月は多要素認証をすり抜ける「AiTM（Adversary-in-the-Middle）攻撃」について紹介しました。MFA の導入が進む中でも、偽サイトを介して認証情報やセッションを盗み取るこの手口は非常に大きな脅威となっています。特に金融機関やクラウドサービスを狙った攻撃が多く確認されており、今後も注意が必要です。
今一度、フィッシング耐性のある認証方式の導入やセッション管理の見直し、ユーザー教育の強化を通じて、AiTM 攻撃への備えを進めてください。

■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

●【2025 年 4 月 マルウェアレポート】認証情報の窃取手法と対策について解説 | サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware2504.html
●インターネット取引サービスへの不正アクセス・不正取引による被害が急増しています | 金融庁
https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html
●金融商品取引業者等向けの総合的な監督指針 | 金融庁
https://www.fsa.go.jp/common/law/guide/kinyushohin/
●ユーザー認証仕様の概要 | FIDO Alliance
https://fidoalliance.org/specifications/?lang=ja
●From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud | Microsoft Security Blog
https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/

Canon

キヤノンマーケティングジャパン株式会社