2026年
1·2月
JAN / FEB

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

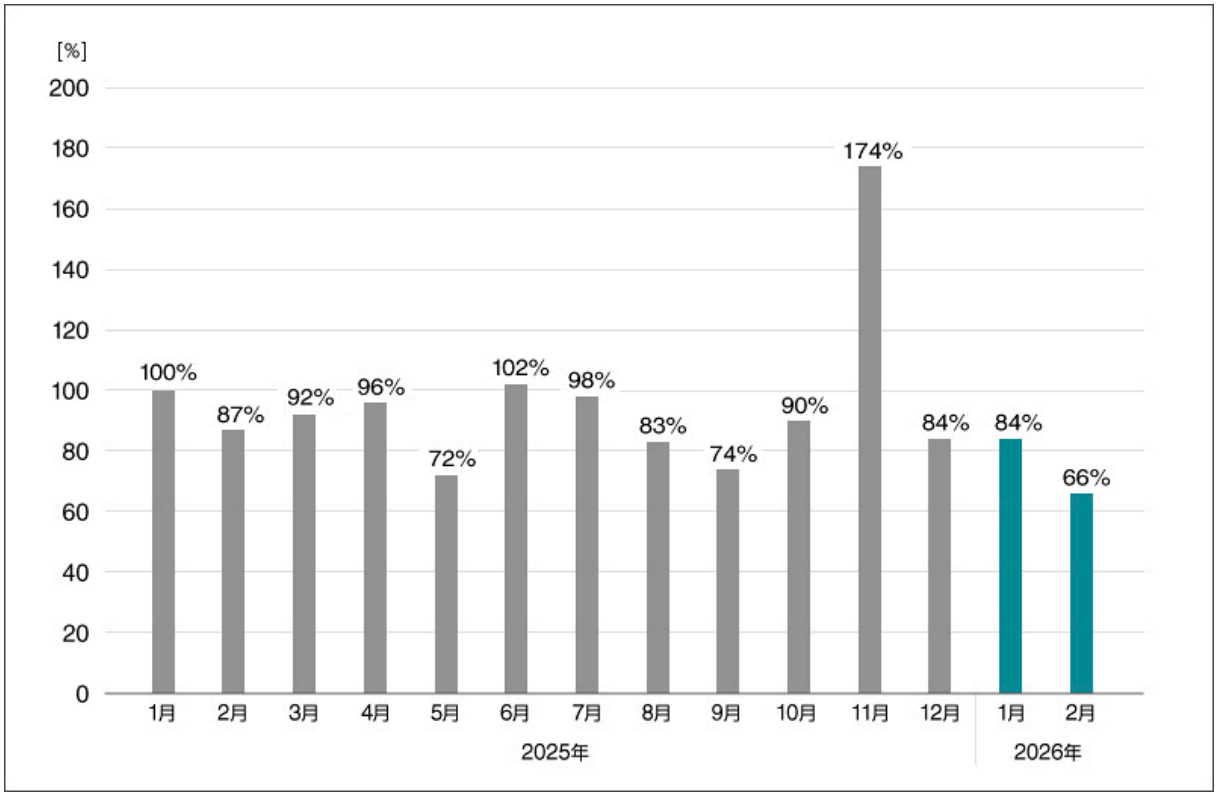
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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 1 月･2 月マルウェア検出状況

2026 年 1 月（1 月 1 日～1 月 31 日）と 2026 年 2 月（2 月 1 日～2 月 28 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。

2026 年 1 月の国内マルウェア検出数は 2025 年 12 月と比較して微増しました。また 2026 年 2 月の国内マルウェア検出数は、1 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 1 月･2 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	31.8%	アドウェア
2	HTML/Phishing.Agent	15.4%	メールに添付された不正な HTML ファイル
3	Win32/PSW.Amatera	6.9%	情報窃取を目的としたマルウェア
4	DOC/Fraud	6.2%	詐欺サイトのリンクが埋め込まれた DOC ファイル
5	JS/TrojanDownloader.Agent	2.1%	ダウンローダー
6	JS/Danger.ScriptAttachment	1.7%	メールに添付された不正な JavaScript
7	JS/Agent	1.1%	不正な JavaScript の汎用検出名
8	HTML/Phishing	0.9%	フィッシングを目的とした不正な HTML ファイル
9	HTML/FakeCaptcha	0.8%	偽の CAPTCHA を表示させる HTML ファイル
10	Win64/Aotera	0.8%	ローダー型のマルウェア

国内マルウェア検出数*2 上位（2026 年 1 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	34.3%	アドウェア
2	Win32/PSW.Amatera	12.3%	情報窃取を目的としたマルウェア
3	HTML/Phishing.Agent	9.9%	メールに添付された不正な HTML ファイル
4	DOC/Fraud	8.2%	詐欺サイトのリンクが埋め込まれた DOC ファイル
5	JS/TrojanDownloader.Agent	2.0%	ダウンローダー
6	JS/Danger.ScriptAttachment	1.5%	メールに添付された不正な JavaScript
7	JS/Agent	1.1%	不正な JavaScript の汎用検出名
8	HTML/FakeCaptcha	1.0%	偽の CAPTCHA を表示させる HTML ファイル
9	HTML/Phishing	0.9%	フィッシングを目的とした不正な HTML ファイル
10	VBA/TrojanDownloader.Agent	0.6%	ダウンローダー

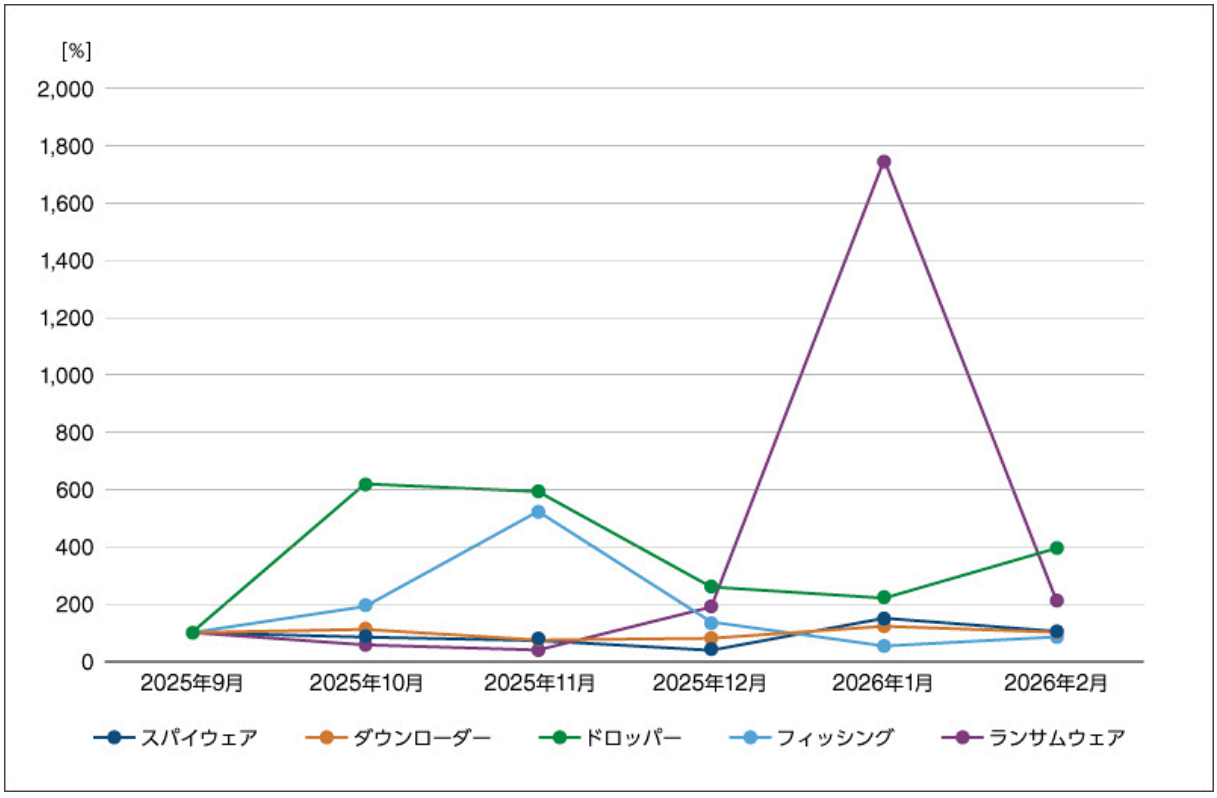
国内マルウェア検出数*2 上位（2026 年 2 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	28.6%	アドウェア
2	HTML/Phishing.Agent	22.4%	メールに添付された不正な HTML ファイル
3	DOC/Fraud	3.5%	詐欺サイトのリンクが埋め込まれた DOC ファイル
4	JS/TrojanDownloader.Agent	2.2%	ダウンローダー
5	JS/Danger.ScriptAttachment	1.9%	メールに添付された不正な JavaScript
6	JS/Agent	1.3%	不正な JavaScript の汎用検出名
7	Win64/Aotera	1.2%	ローダー型のマルウェア
8	JS/Adware.Subprop	1.0%	アドウェア
9	DOC/TrojanDropper.Agent	1.0%	ドロッパー
10	HTML/Phishing	0.9%	フィッシングを目的とした不正な HTML ファイル

*2 本表には PUA を含めていません。

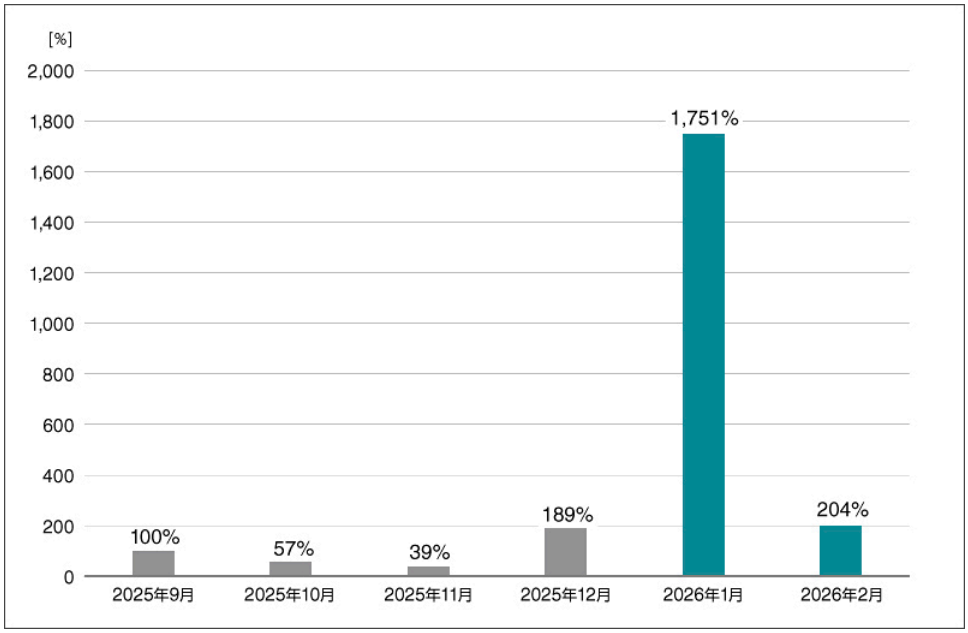
1 月と 2 月に国内で最も多く検出されたマルウェアは、HTML/Phishing.Agent でした。
HTML/Phishing.Agent は、メールに添付された不正な HTML ファイルの汎用検出名です。HTML ファイル内に埋め込まれた URL に接続すると、個人情報の窃取、マルウェアのダウンロードといった被害に遭う可能性があります。

2026 年 1 月と 2 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。



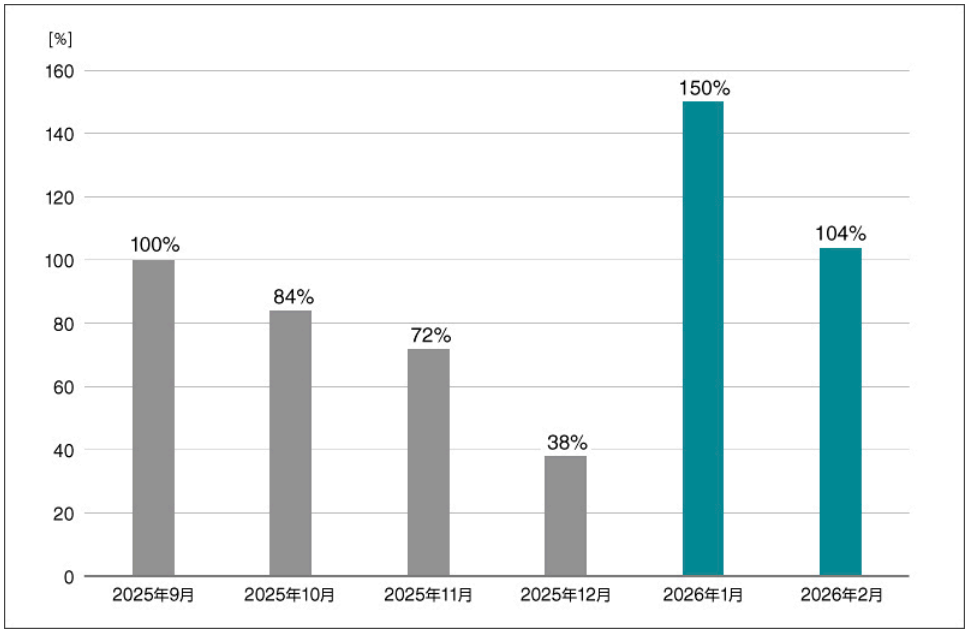
国内マルウェアの種類別検出数の推移
（2025 年 9 月の各検出数を 100%として比較）

2026 年 1 月はランサムウェアの検出数が大きく増加しました。しかし 2026 年 2 月になるとランサムウェアの検出数は減少して平均的な水準に戻りました。また 2 月はドロッパーの検出数の増加が観測されました。



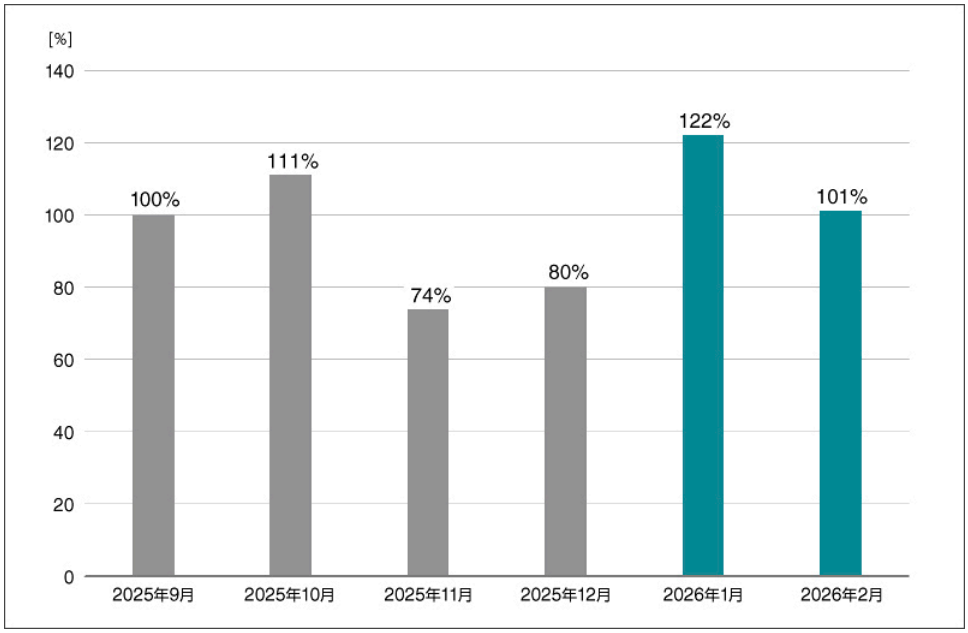
ランサムウェア検出数の推移（国内）

（2025 年 9 月の検出数を 100%として比較）



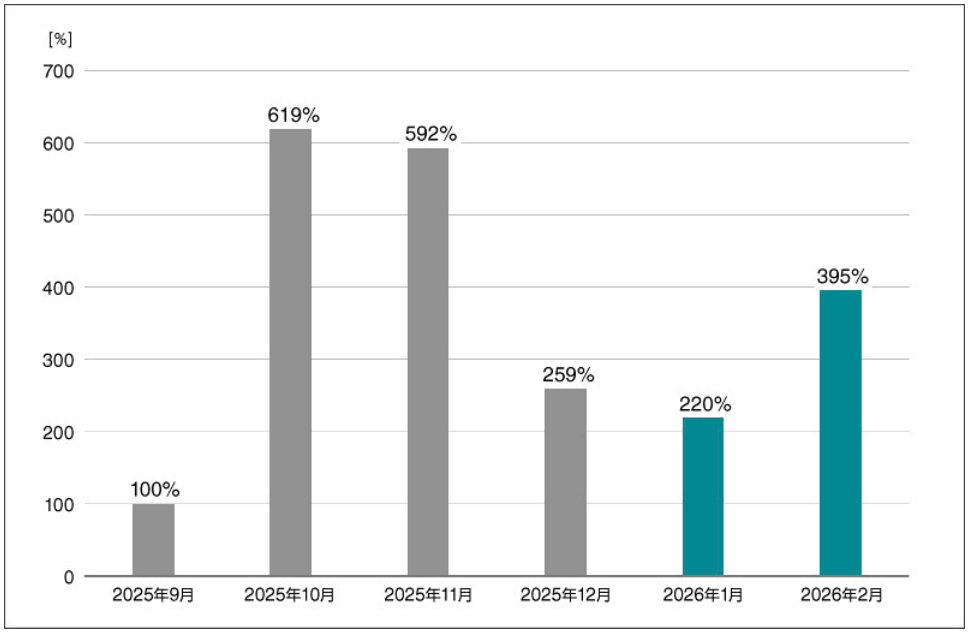
スパイウェア検出数の推移（国内）

（2025 年 9 月の検出数を 100%として比較）



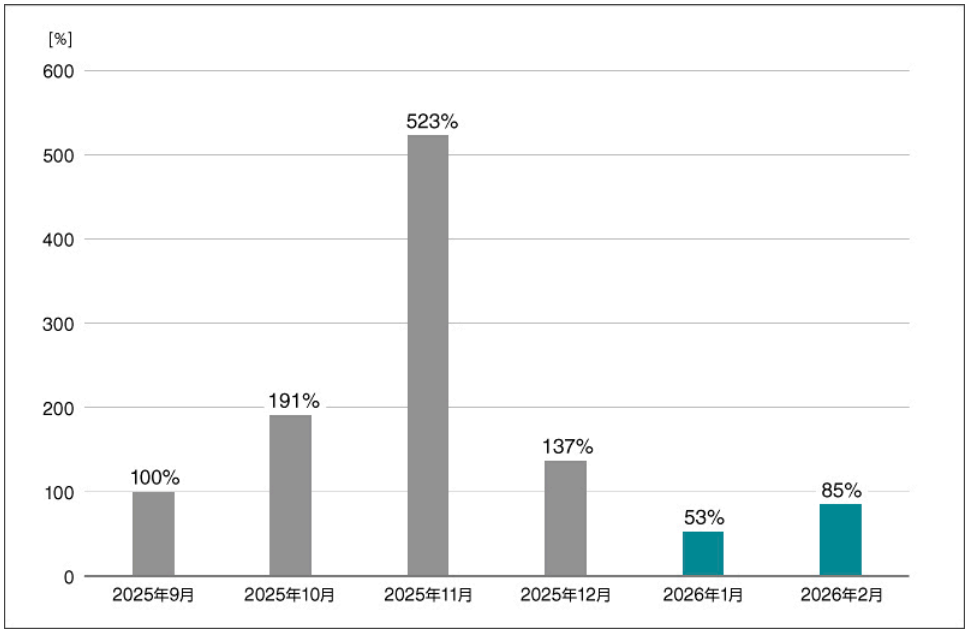
ダウンローダー検出数の推移（国内）

（2025 年 9 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）

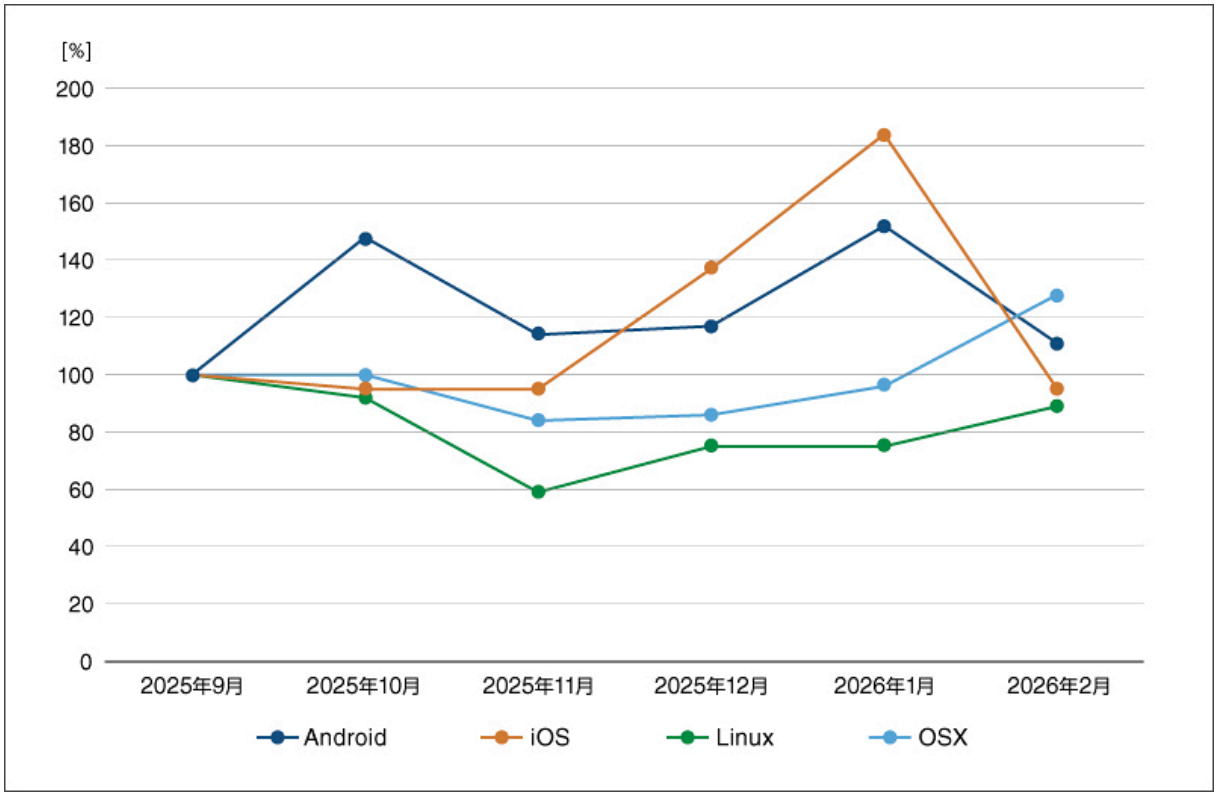
（2025 年 9 月の検出数を 100%として比較）



フィッシング検出数の推移（国内）

（2025 年 9 月の検出数を 100%として比較）

2026 年 1 月と 2 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 9 月の各検出数を 100%として比較）

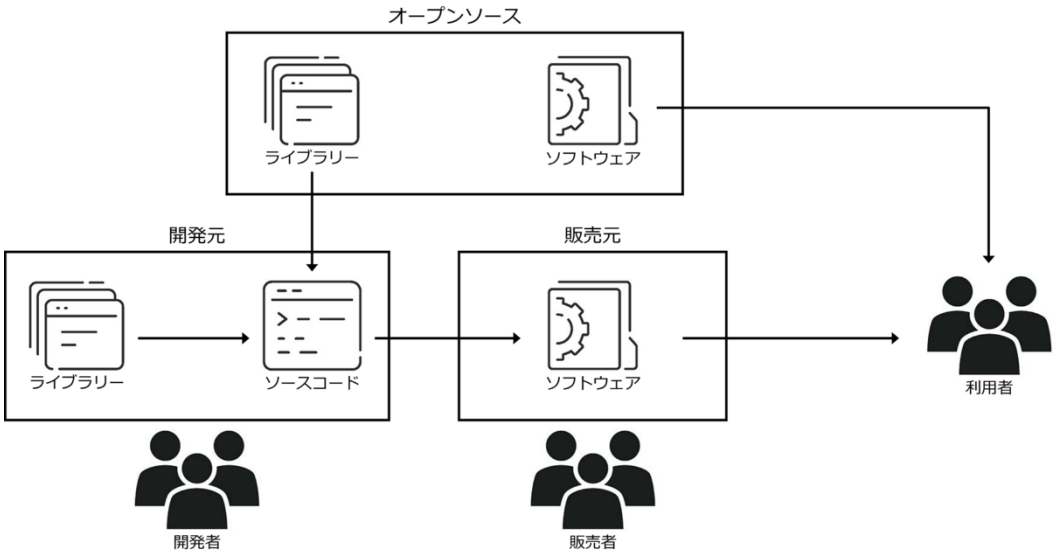
2026 年 1 月は 2025 年 12 月と比較すると、Linux 以外の OS を標的としたマルウェアの検出数が増加しました。一方で 2026 年 2 月になると Android と iOS を狙ったマルウェアの検出数は大きく減少し、Linux については増加に転じました。なお、OSX を狙ったマルウェアの検出数については引き続き上昇しています。

・外部リソースの利用によるインシデント

2025 年 12 月、掲示板運営や広告配信などを行う A 社は、同社が利用するシステムについて不正アクセスを受けたことを公表しました。さらに 2026 年 1 月には不正アクセスに関する調査結果を発表しました。
この調査結果によると、社内の開発環境が不正アクセスされ、その環境に保存されていた情報の一部が外部からアクセス可能な状態となっていたとのことです。この不正アクセスについては、不正なコードが混入していた外部プログラムを自動ビルドの処理によって開発環境に取り込んだことが原因であると報告されています。
上記のインシデントは、組織の管理外にある侵害された外部リソースによって生じました。これはソフトウェアサプライチェーン攻撃と呼ばれる手法の一種です。現代において、組織内部で利用される外部リソースは、把握しきれていないものも含めると非常に数が多く存在します。これらは業務プロセスに深く組み込まれており、切っても切り離せない存在となっています。ソフトウェアサプライチェーン攻撃は自組織の外部で発生した事案の影響を受けることから、組織のセキュリティ対策を考えるうえで見落としがちな脅威のため、改めて攻撃の概要や対策について紹介します。

・ソフトウェアサプライチェーン

ソフトウェアサプライチェーンとは、ソフトウェアの開発、製造、提供といった一連の工程や、その工程の中で関連するソフトウェアや組織など、ソフトウェアを取り巻く相互関係のことです。ソフトウェアサプライチェーンの簡易的な関係図の例を以下に示します。



ソフトウェアサプライチェーンの例

利用するソフトウェアとしては、企業や公的機関などが提供しているソフトウェアのほか、開発元が不明確な場合もあるオープンソースソフトウェア（OSS）が挙げられます。これらのソフトウェアを開発する際、開発環境の内部で作成するコードに加え、外部から取得するライブラリーやツールなどを使用することが一般的です。上記の図は簡易的に表していますが、複数の組織が協力しながら開発する、自社開発のソフトウェアが存在するなど、実際のソフトウェアサプライチェーンはより複雑なものとなっています。
このように、利用者のもとに届くソフトウェアは多くの要素が複雑に絡み合いながら開発されています。サイバー犯罪者は、この開発工程の中でセキュリティ的に脆弱な部分が存在しないかを常に探し、攻撃の機会をうかがっています。

・ソフトウェアサプライチェーン攻撃

ソフトウェアサプライチェーン攻撃とは、上述のソフトウェアサプライチェーンに対して攻撃者が介入し、悪意のあるコードやマルウェアを混入させる攻撃手法のことです。過去に発生したインシデントを交えながら、攻撃の例を紹介します。

■OSS のライブラリーの侵害

ソフトウェアが利用する外部のライブラリーに対する改ざんの事例が、これまでにいくつか確認されています。例えば、プログラミング言語である Python の PyPI（Python Package Index）[*3] にホストされている「ctx」ライブラリー[*4] の改ざんが挙げられます。
SANS Internet Storm Center による 2022 年の報告では、「ctx」ライブラリーのアップデートにより、AWS の認証情報やコンピューター名などを含む環境変数の値を窃取する機能が追加されていました。この事象は、開発者の PyPI アカウントが何らかの方法で乗っ取られ、不正にライブラリーが改ざんされたことにより生じたと考えられています。
Python の PyPI に限らずプログラミング言語で利用されるサードパーティ製のライブラリーは、開発者にとって容易に導入することができ、開発にかかるコストを大きく削減することが可能です。しかしライブラリーの更新履歴や更新内容を精査せずに利用すると、上述のような事例に巻き込まれる可能性があります。

＊3 Python のサードパーティ製ライブラリーを扱う公式のパブリックリポジトリのことを指します。
＊4 Python における辞書オブジェクトを操作できるようにする機能を有したライブラリーです。

■ソフトウェアベンダーの開発環境やアップデートサーバーの侵害

企業が提供するソフトウェアは、OSS のものと比較すると厳格に管理されている傾向があることから、一般的に信頼性が高いです。しかしこのようなソフトウェアがマルウェア化した事例もあります。例えば、Sunburst と呼ばれるサイバー攻撃が挙げられます。

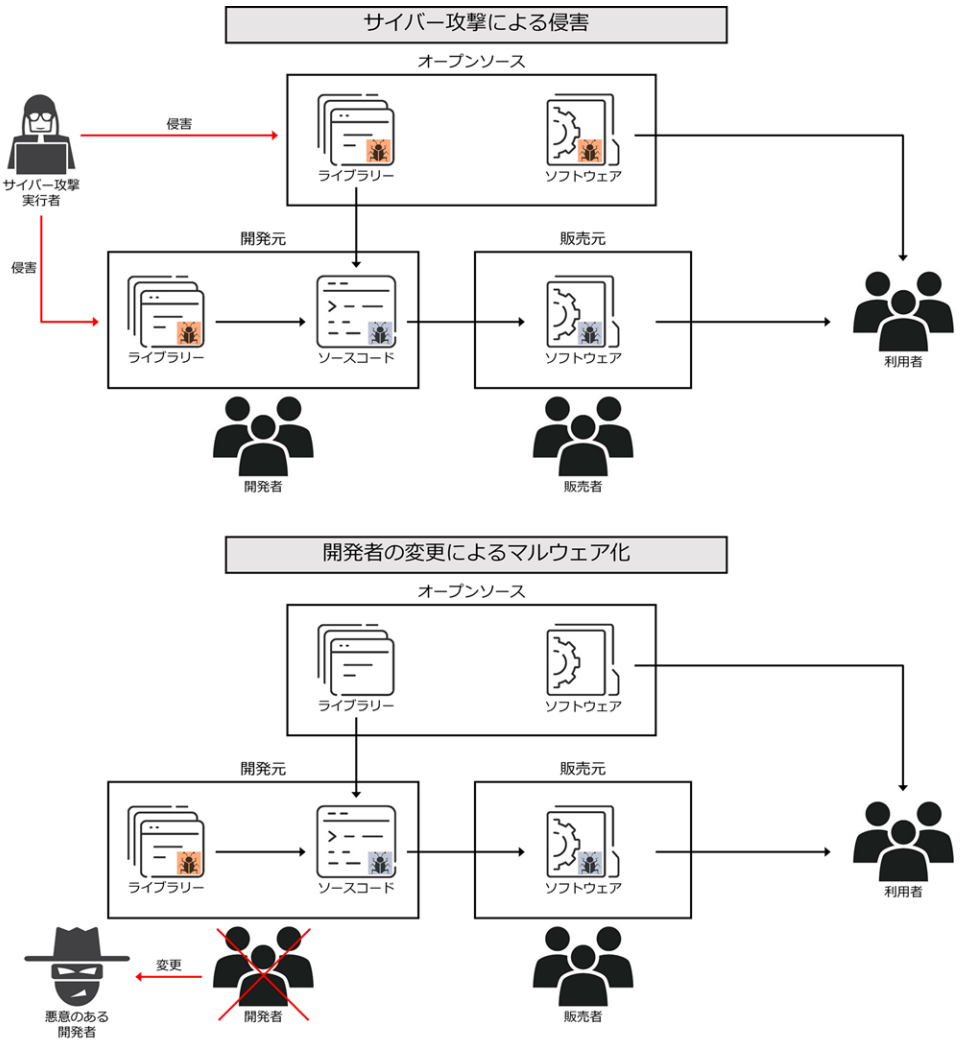
この攻撃では、ネットワーク管理ソフトなどの開発を手掛ける B 社が提供する製品のアップデートプロセスが侵害され、アップデートとして配布されたプログラムがバックドアに置き換えられました。B 社の製品は米国の企業や政府機関を中心に多くの組織で利用されていたため、広範囲に影響を及ぼしました。この攻撃で配布されたバックドアは 2 週間程度の休止期間を挟む、侵害前の製品が利用する API 通信に偽装するなど、悪意のある活動を隠ぺいする工夫が多く確認されました。このように高度なサイバー攻撃であったことから、攻撃の兆候を検知するのに時間を要しました。

■無害なソフトウェアから悪性のソフトウェアに変更

直接のサイバー攻撃とは異なる事情でソフトウェアが悪性のものとなる事例も存在します。例えば、2024 年に発生した「polyfill[.]io」[*5] 関連の事象が挙げられます。

この「polyfill[.]io」は無害な JavaScript のライブラリーを配信するドメインでしたが、ドメインと GitHub アカウントの売買に伴う開発者の変更をきっかけに、マルウェア化したライブラリーが配信されるようになりました。この結果、当該ライブラリーを使用する Web サイトにユーザーがアクセスすると、悪意のあるサイトにリダイレクトするようになりました。この状況を受けて、ドメインレジストラや CDN 事業者は「polyfill[.]io」ドメインを停止する、代替の安全な URL に接続させるといった対応に追われました。

＊5 誤接続を防止するため、「.」を「[.]」として表記しています。



事例を踏まえたソフトウェアサプライチェーンの侵害の例

上述の 3 つの事例を踏まえると、ソフトウェアサプライチェーン攻撃の特徴や攻撃者側のメリットが浮き彫りになります。攻撃の特徴としては、被害規模が大きくなるという点が挙げられます。汎用的に利用されているソフトウェアの改ざんに成功すると、広範囲に不正なコードやマルウェアを配布することが可能です。

攻撃者のメリットとしては、セキュリティが強固な標的組織に対して、直接サイバー攻撃を仕掛けることなく目的を達成しうるという点が挙げられます。強固なセキュリティを突破することは容易ではありませんが、標的組織が利用するソフトウェアに付随する外部コンポーネントの侵害であれば、より低リスクかつ低コストで実行できる場合があります。さらに、企業が提供する信頼性の高いソフトウェアへの侵害が成功した場合、検知が困難で被害の表面化までに時間を要するサイバー攻撃となり得ます。

・ソフトウェアサプライチェーン攻撃への対策

ソフトウェアサプライチェーン攻撃への対策について、代表的なものを紹介します。
まず、ソフトウェアの導入前に可能な限り精査することが重要です。ソフトウェアの開発元について、実態が明確となっているか、ISO や ISMS などの認証を取得しているか、セキュリティ向上のための修正を迅速に実施しているかなどを調査し、総合的に判断することが求められます。ソースコードが公開されている場合は、不審な処理を実装していないか確認することも重要です。コードをすべて確認することは技術的に難しく現実的ではありませんが、URL 文字列の検索による通信先の把握や、セキュリティ製品によるスキャンの実施などによって、一定のリスク低減が期待できます。さらに詳細な調査が必要な場合には、ソースコード診断サービスなどの利用を検討してください。
次に、既に組織内で利用しているソフトウェアおよびそれに紐付くライブラリーを把握することが重要です。代表的な管理方法として、SBOM（Software Bill of Materials）の利用が挙げられます。SBOM はソフトウェアを構成するコンポーネントのバージョン、ライセンス、依存関係などを一覧化したものです。経済産業省が SBOM の利用に関するガイドラインを公開しているため、これを参考に導入し、ソフトウェアの管理を徹底してください。
続いて、利用しているソフトウェアにセキュリティ上のリスクが顕在化していないか、継続的に情報収集することが重要です。ソフトウェアサプライチェーン攻撃の事例で紹介したように、利用しているソフトウェアがある時点から悪性のものに変化する可能性があります。異変にいち早く気づき、迅速な対応を進めるため、公式サイトやセキュリティ調査機関が発信する情報を継続的に確認してください。
最後に、ソフトウェアの開発者側が考慮する必要がある対策に言及します。開発者側の対策は利用者よりも広範囲に及びますが、対策の観点を体系的に捉えるうえで、OWASP Top 10 CI/CD Security Risks[*6]の参照が有用です。この OWASP の発信内容を踏まえ、セキュリティベンダーが具体的な対策を紹介しています。ソフトウェア開発を行う組織は、開発環境のセキュリティ強化に活用してください。

＊6 ソフトウェア開発で取り入れられている CI/CD パイプライン（ソフトウェアのビルド・テスト・デプロイを自動化した環境）における、重要なセキュリティリスクを 10 項目に整理したものです。

■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。

引用・出典元

●ctx Python Library Updated with "Extra" Features | SANS ISC
https://isc.sans.edu/diary/ctx+Python+Library+Updated+with+Extra+Features/28678
●Automatically replacing polyfill.io links with Cloudflare's mirror for a safer Internet | Cloudflare, Inc.
Automatically replacing polyfill.io links with Cloudflare's mirror for a safer Internet
●サイバー攻撃への備えを！「SBOM」（ソフトウェア部品構成表）を活用してソフトウェアの脆弱性を管理する具体的手法についての改訂手引を策定しました ｜ METI/経済産業省
https://www.meti.go.jp/press/2024/08/20240829001/20240829001.html
●OWASP Top 10 CI/CD Security Risks | OWASP Foundation
https://owasp.org/www-project-top-10-ci-cd-security-risks/
●OWASP Top 10 CI/CD Security Risks から考える CI/CD パイプラインのセキュリティ ｜ NEC
https://jpn.nec.com/cybersecurity/blog/240621/index.html

Canon

キヤノンマーケティングジャパン株式会社