2026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

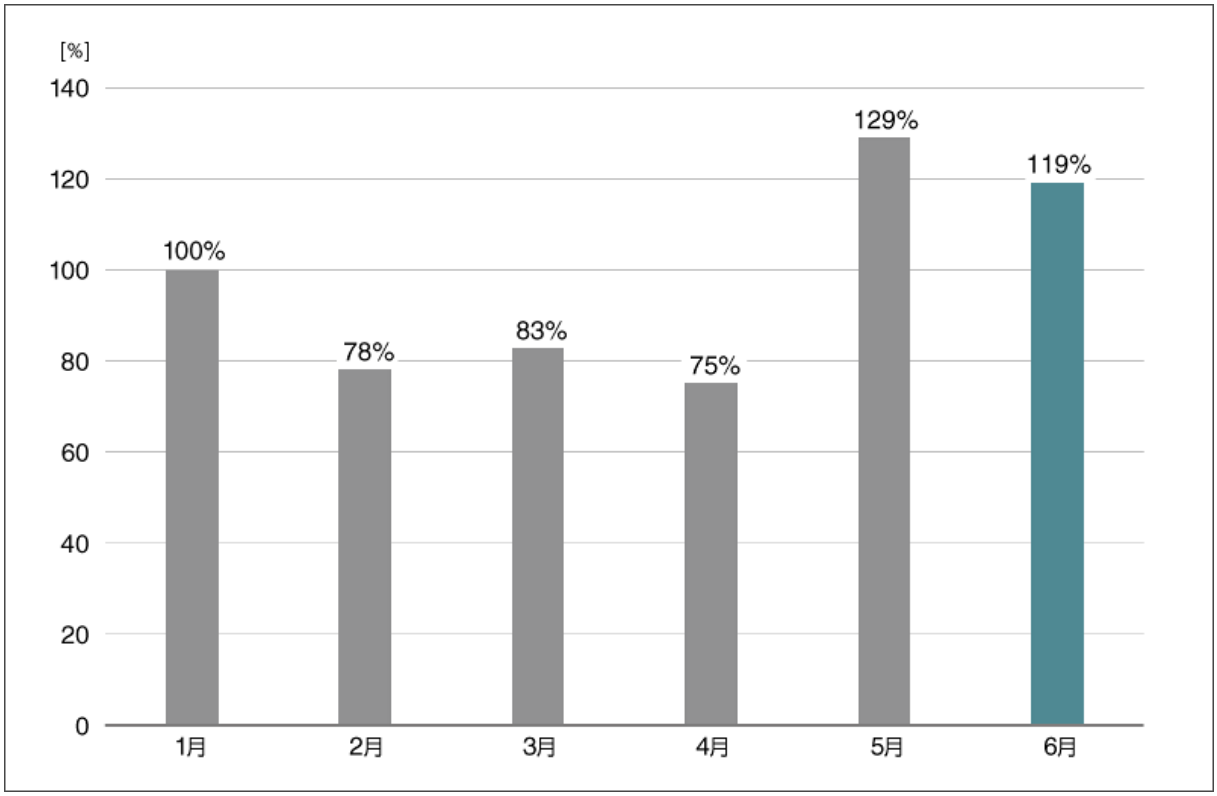
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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。

2026 年 6 月マルウェア検出状況

2026 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

(2026 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 6 月の国内マルウェア検出数は、2026 年 5 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。

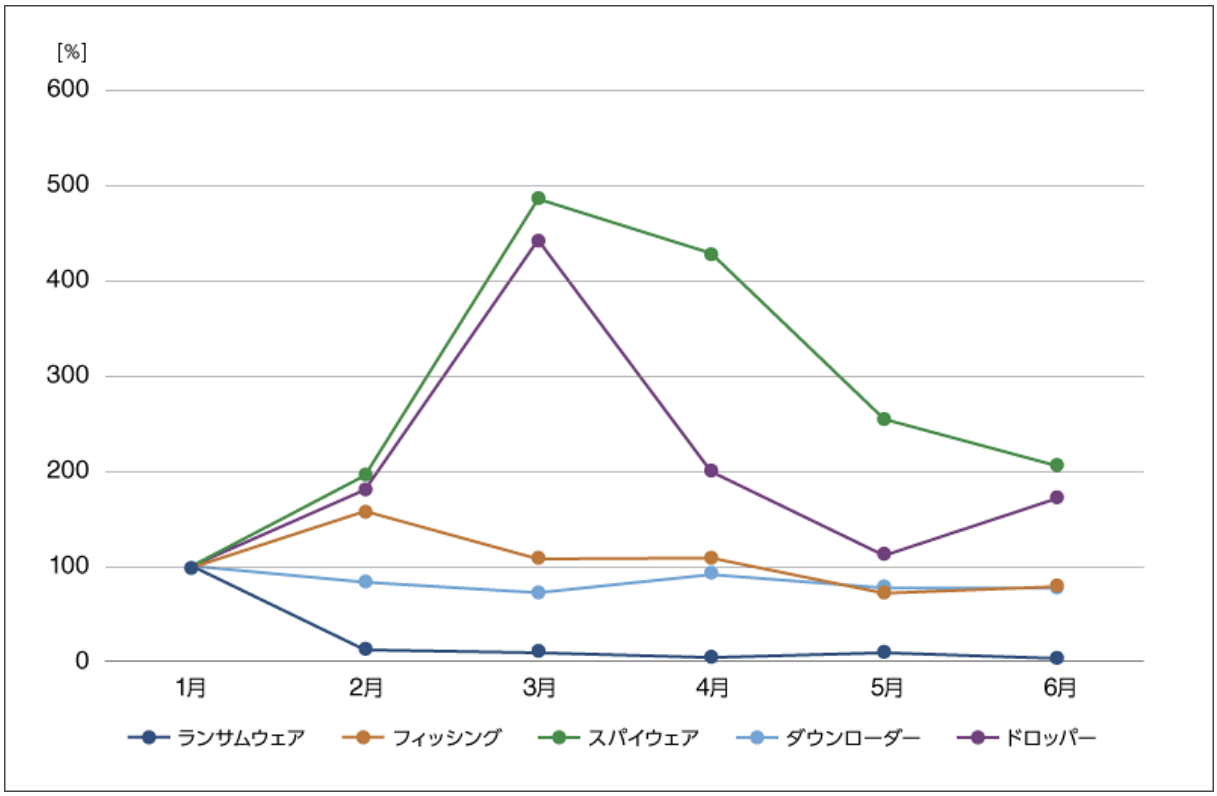
国内マルウェア検出数*2 上位（2026 年 6 月）

順位	マルウェア	割合	種別
1	DOC/Fraud	47.8%	詐欺サイトのリンクが埋め込まれた DOC ファイル
2	JS/Adware.Agent	7.3%	アドウェア
3	HTML/Phishing.Agent	6.7%	メールに添付された不正な HTML ファイル
4	JS/Agent	4.8%	不正な JavaScript の汎用検出名
5	JS/Danger.ScriptAttachment	2.6%	ダウンローダー
6	Win32/Exploit.CVE-2017-0199	2.5%	脆弱性 CVE-2017-0199 を悪用するプログラム
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	JS/TrojanDropper.Agent	1.0%	ドロッパー
9	JS/TrojanDownloader.Agent	0.8%	ダウンローダー
10	PDF/Phishing.Gen	0.5%	メールに添付された不正な PDF ファイル

*2 本表には PUA を含めていません。

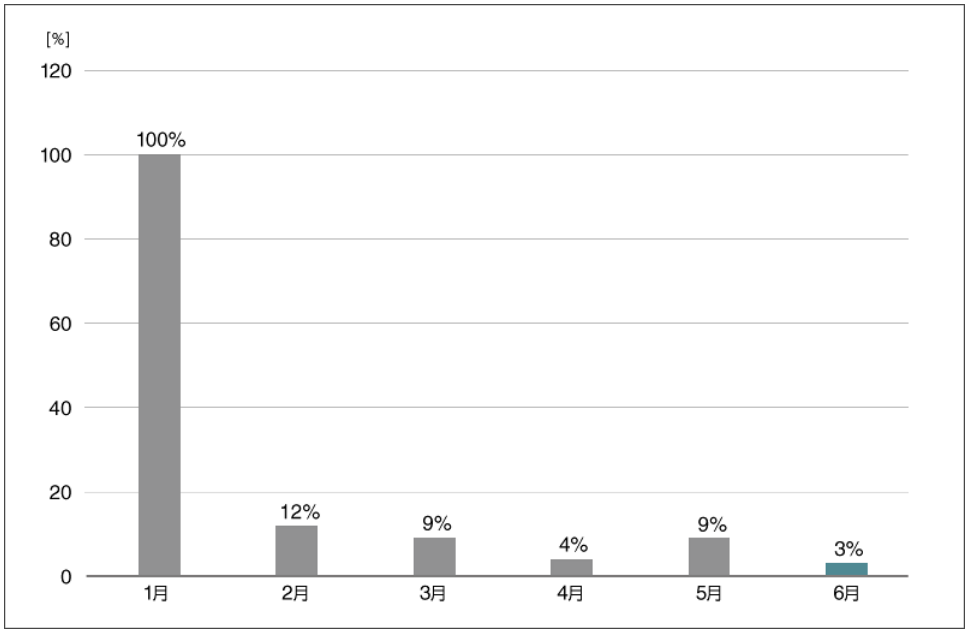
6 月に国内で最も多く検出されたマルウェアは、DOC/Fraud でした。
DOC/Fraud は、詐欺サイトへのリンクまたは詐欺を目的とした文章が書かれている Word ファイルの検出名です。感染すると、不正な金銭の要求や個人情報の窃取といった被害に遭う可能性があります。

2026 年 6 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。



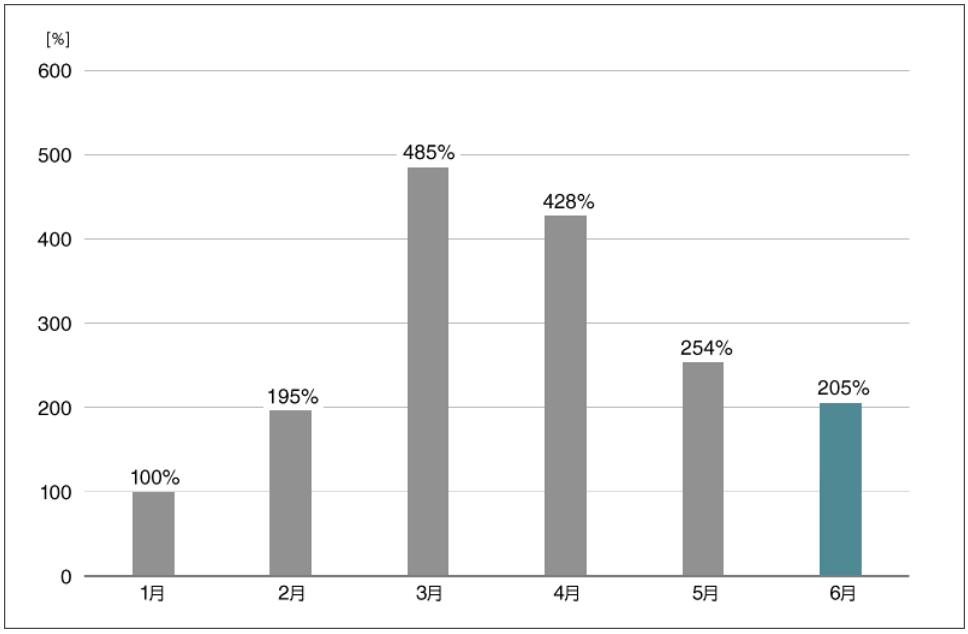
国内マルウェアの種類別検出数の推移
（2026 年 1 月の各検出数を 100%として比較）

2026 年 6 月はドロッパーの検出数が増加しました。スパイウェアの検出数は、2026 年 3 月をピークに、減少傾向にあります。



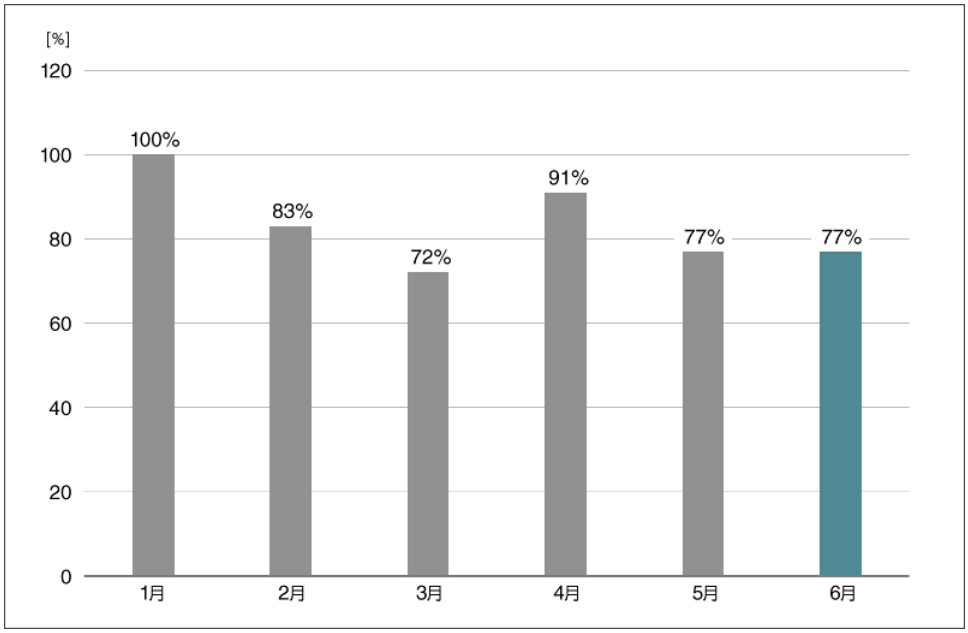
ランサムウェア検出数の推移（国内）

（2026 年 1 月の検出数を 100%として比較）



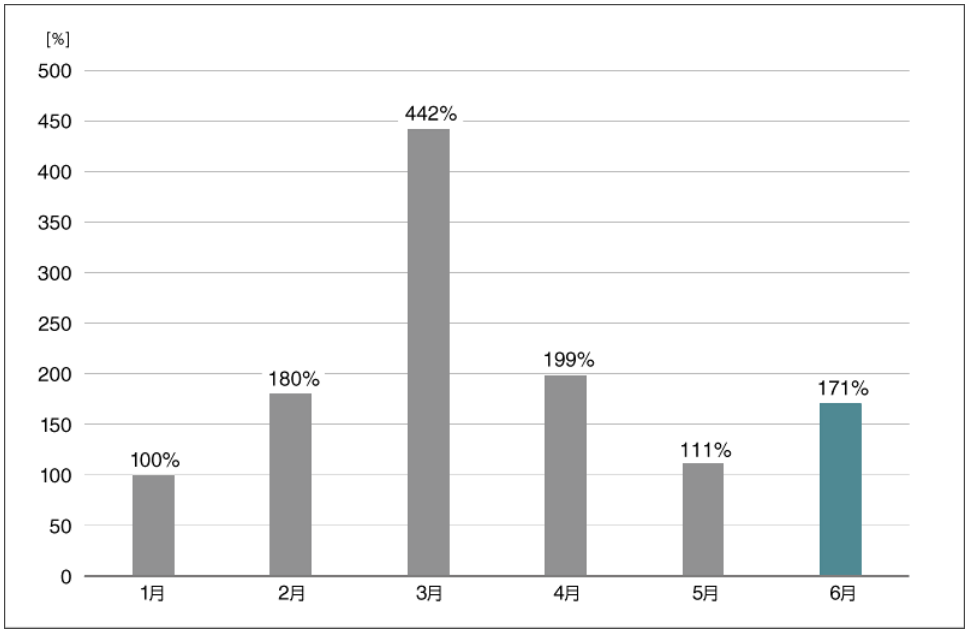
スパイウェア検出数の推移（国内）

（2026 年 1 月の検出数を 100%として比較）



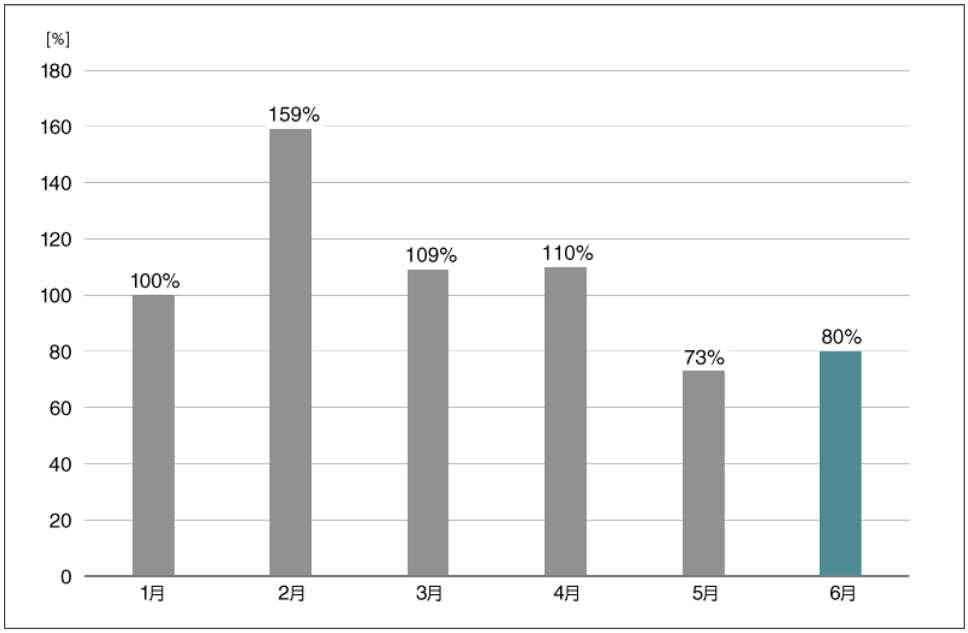
ダウンローダー検出数の推移（国内）

（2026 年 1 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）

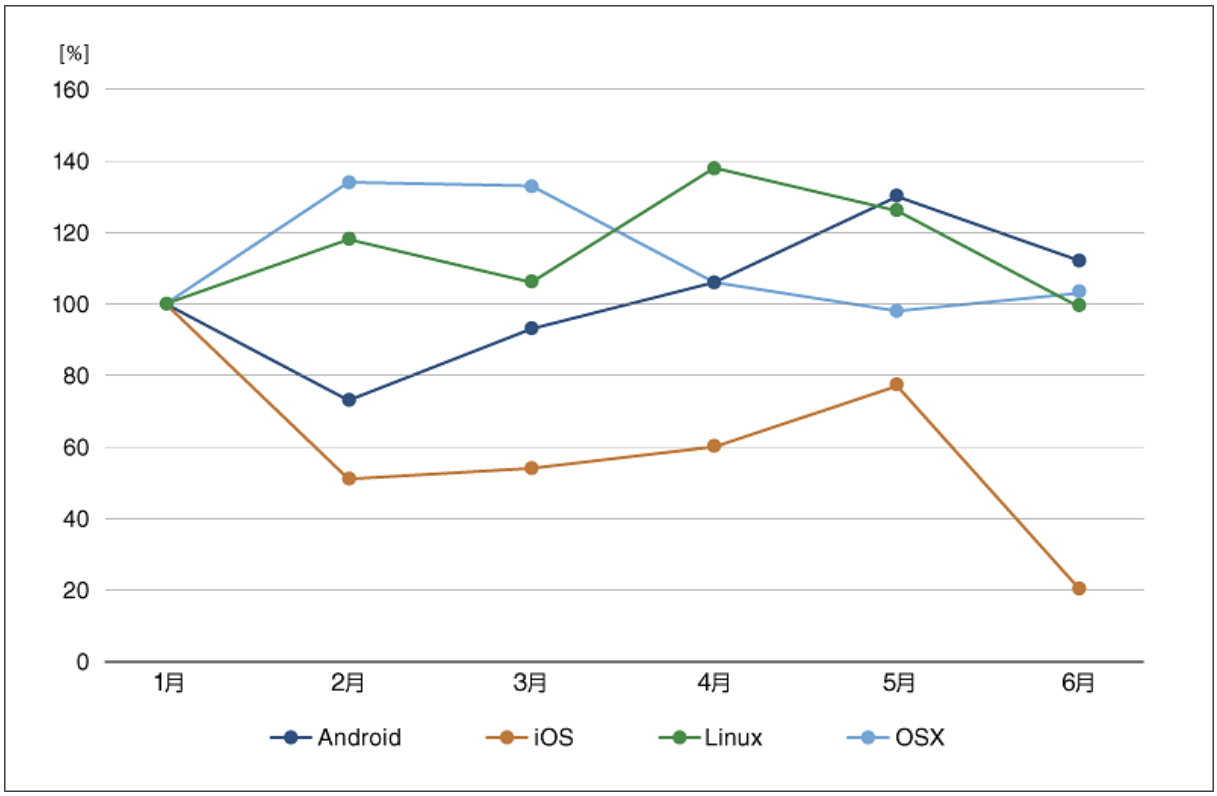
（2026 年 1 月の検出数を 100%として比較）



フィッシング検出数の推移（国内）

（2026 年 1 月の検出数を 100%として比較）

2026 年 6 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 別の推移（Windows を除く）
（2026 年 1 月の各検出数を 100%として比較）

2026 年 6 月は OS X を狙ったマルウェアが増加しています。一方で、それ以外の OS を狙ったマルウェアは減少しています。iOS を狙ったマルウェアは大きく減少しています。

USB メモリーの悪用手法について

2026 年 6 月、公的機関で使用されていた USB メモリーからマルウェアが検知された事例が、各種メディアで報道されました。
USB メモリーを悪用した脅威によるリスクは古くから確認されており、報道されているように依然として脅威によるリスクは解消していないため、採用する攻撃者も存在しています。
今回は周知を目的として、想定被害の観点から悪用手法を紹介します。加えて、脅威への対策についても取り上げます。

■ USB メモリーの悪用によって想定される被害

想定される被害としては、主に 3 つ挙げられます。

- マルウェア感染
- 任意のコマンド実行
- 端末破壊

ここからは、上記の想定被害を発生させる恐れがある悪用手法を紹介します。

■ USB メモリーを悪用する主な手法

想定被害：マルウェア感染

- AutoRun 機能の悪用

AutoRun 機能は、USB メモリーや DVD などの記憶媒体を Windows 端末に接続した際に、インストーラーなどのアプリケーションを自動で起動する機能です。この機能を悪用することで、ネットワークに接続されていない PC に対しても感染を広げることが可能となります。攻撃者はインターネットに接続されていないエアギャップ環境[1]へのサイバー攻撃でこの手法を採用してきました。実際にサイバー攻撃で利用されたマルウェア Stuxnet は、USB メモリーを媒介して感染を拡大しました。ほかにも、ワームの 1 つである Conficker も USB メモリーによって感染を広げます。
一方、この機能を無効化する更新プログラムが 2009 年に配布され、2011 年に Windows XP や Windows Vista といった対象バージョンを広げるアップデートが行われました。現在もデフォルト設定で AutoRun 機能は無効化されています。

1 エアギャップ：インターネットや安全でない LAN などのネットワークから物理的に隔離して、最も機密性の高いネットワークを保護するために使用されるセキュリティ対策の 1 つ

- 偽装ファイルの悪用

USB メモリー内にアイコンや拡張子を偽装した LNK ファイル（ショートカットファイル）や実行ファイルを書き込み、ユーザー自身に実行させることでマルウェアに感染させる手法も存在します。AutoRun 機能が無効化された環境においても感染可能であることから、現在も攻撃者に採用されています。実際に、USB メモリー内の LNK ファイルがクリックされると、USB メモリー内に隠されたマルウェア PlugX が実行される事例が確認されています。

想定被害：任意のコマンド実行

- 接続端末に対する認識の偽装

USB メモリーは記憶媒体として利用されることが一般的であるため、保存するデータだけが格納されていると認識されがちですが、実際には USB メモリーを制御するためのファームウェア（書き換え可能な実行コード）も格納されています。このファームウェアを改ざんし、キーボードなどの Human Interface Device（HID）として端末に認識させることで、悪意のあるコマンドをセキュリティ製品やユーザーに気づかれずに実行することができます。この手法を用いた USB メモリーは、BadUSB と呼ばれています。一般的に、USB メモリーの接続を禁止している場合であっても、利便性の観点から HID は接続可能となっていることがあります。攻撃者はこの設定を悪用し、本来接続できない USB メモリーを HID として接続することでコマンド実行を行います。悪意のあるコマンドが実行されると、マルウェアの追加ダウンロードや認証情報の窃取、キーロギングの被害に遭う恐れがあります。過去には、攻撃者グループ「FIN7」が米国企業に対して官公庁からの送付物やギフトボックスに偽装した荷物で BadUSB を送付していた事例が報道されています。

想定被害：端末破壊

- サージ電圧による電子回路破壊

USB 接続した PC に対して、瞬間的に高電圧をかけることでマザーボードなどの内部パーツを破壊する USB キラーと呼ばれる脅威があります。本来、USB キラーは異常に高電圧がかかるサージ電圧をテストする目的で販売されている機器ですが、攻撃者によって悪用されています。この機器は USB ポートから給電した電力を蓄積し、高電圧をかけて繰り返し放電しますが、高電圧への耐性がない端末では、内部の電子回路が破壊されてしまいます。実際に、米国の大学において、学生が学内端末に対して USB キラーを使用し、有罪判決となった事例が確認されています。

USB メモリーの悪用手法まとめ

想定被害	悪用手法	ユーザー側の操作 [1]	実際に悪用された事例
マルウェア感染	AutoRun 機能の悪用	不要	マルウェア 「Stuxnet、Conficker」
	偽装ファイルの悪用	必要	マルウェア 「PlugX」
任意の コマンド実行	BadUSB	不要	攻撃者グループ 「FIN7」
端末破壊	USB キラー	不要	アメリカの大学での 学生による悪用

1 ユーザー側の操作には USB メモリーを端末に接続することは含めていません。
USB メモリー接続後にユーザー側の操作が必要かどうかを記載しています。

USB メモリーの悪用手法への対策

今回紹介した USB メモリーの悪用手法による被害に遭わないために日頃から取り組んでおくべき対策について、簡単に整理しました。
運用、技術、教育の観点で改めて組織における対策状況の見直しを実施してみてください。

■適切なセキュリティ運用の策定
・ OS やセキュリティソフトのセキュリティアップデート
・ USB メモリー利用ポリシーの策定／実施
■技術的対策の導入
・ EDR などのセキュリティ製品による USB 接続の監視
・ セキュリティ機能付き USB メモリーの利用
・ USB キラー対策としてプロテクターの導入
■利用者のセキュリティ意識向上
・ 定期的なセキュリティ教育の実施
・ ポリシーや運用ルールの周知

上記の対策の中でも、「USB メモリー利用ポリシーの策定／実施」は欠かせない対策です。実施するにあたって意識すべきポイントを紹介します。
USB メモリーによるデータ移動が頻繁に行われている組織では、ポリシーによる制限によって、作業の遅延などといった効率性が犠牲になる可能性があります。現場の実態を無視した過大な制約を課した場合、利用者がポリシーの抜け道を見つけようとしたり、ポリシー違反の隠ぺいが常態化するなどして、結果的に想定外のインシデントを招いてしまう恐れもあります。組織内における USB メモリーの利用実態を正確に把握した上で、業務効率とセキュリティリスクのバランスを考慮した現実的で実効性のあるポリシーの策定と運用を心掛けましょう。

まとめ

2026 年 6 月マルウェアレポートでは USB メモリーを悪用する脅威と対策を紹介しました。
USB メモリーを悪用する脅威では、マルウェア感染、任意のコマンド実行、端末破壊といった被害に遭う恐れがあります。まずは、組織内での USB メモリーの利用実態を把握し、利用ポリシーを策定することを推奨します。
策定されている場合は、ポリシーに沿った運用が行われているかを確認してください。

■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

●USB キラー？USB メモリー利用時のリスクと安全な利用方法を考える ｜ サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/special/detail/210603.html
●Replication Through Removable Media | MITRE ATT&CK
https://attack.mitre.org/techniques/T1091/
●USB デバイスに潜む―中国の PlugX マルウェアは今も現役 | UNIT42
https://unit42.paloaltonetworks.com/ja/plugx-variants-in-usbs/
●FBI: FIN7 hackers target US companies with BadUSB devices to install ransomware | The Record
https://therecord.media/fbi-fin7-hackers-target-us-companies-with-badusb-devices-to-install-ransomware
●USB を悪用したサイバー攻撃を解説 ～AutoRun、BadUSB、Stuxnet～ | Trend Micro
https://www.trendmicro.com/ja_jp/jp-security/26/g/trendnews-20260702-01.html

Canon

キヤノンマーケティングジャパン株式会社