2026年
5月
MAY

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

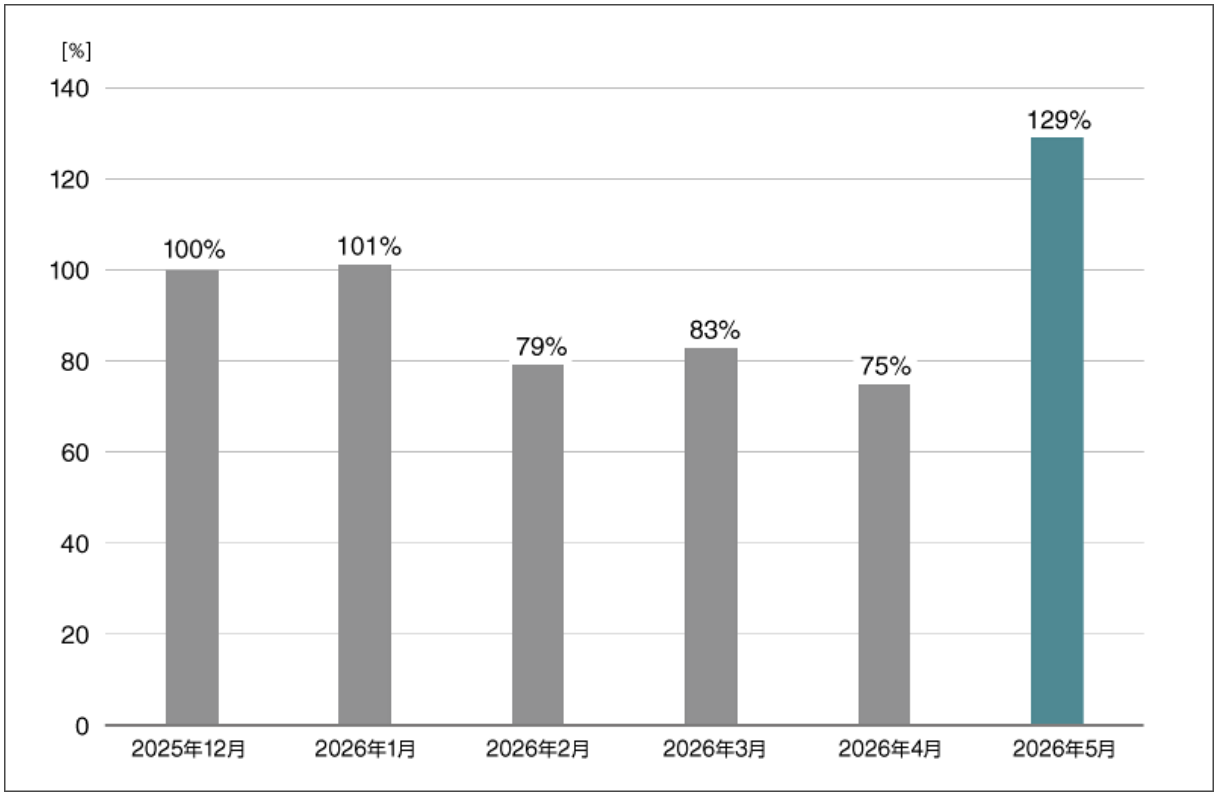
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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 5 月マルウェア検出状況

2026 年 5 月（5 月 1 日～5 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 12 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 5 月の国内マルウェア検出数は、2026 年 4 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。

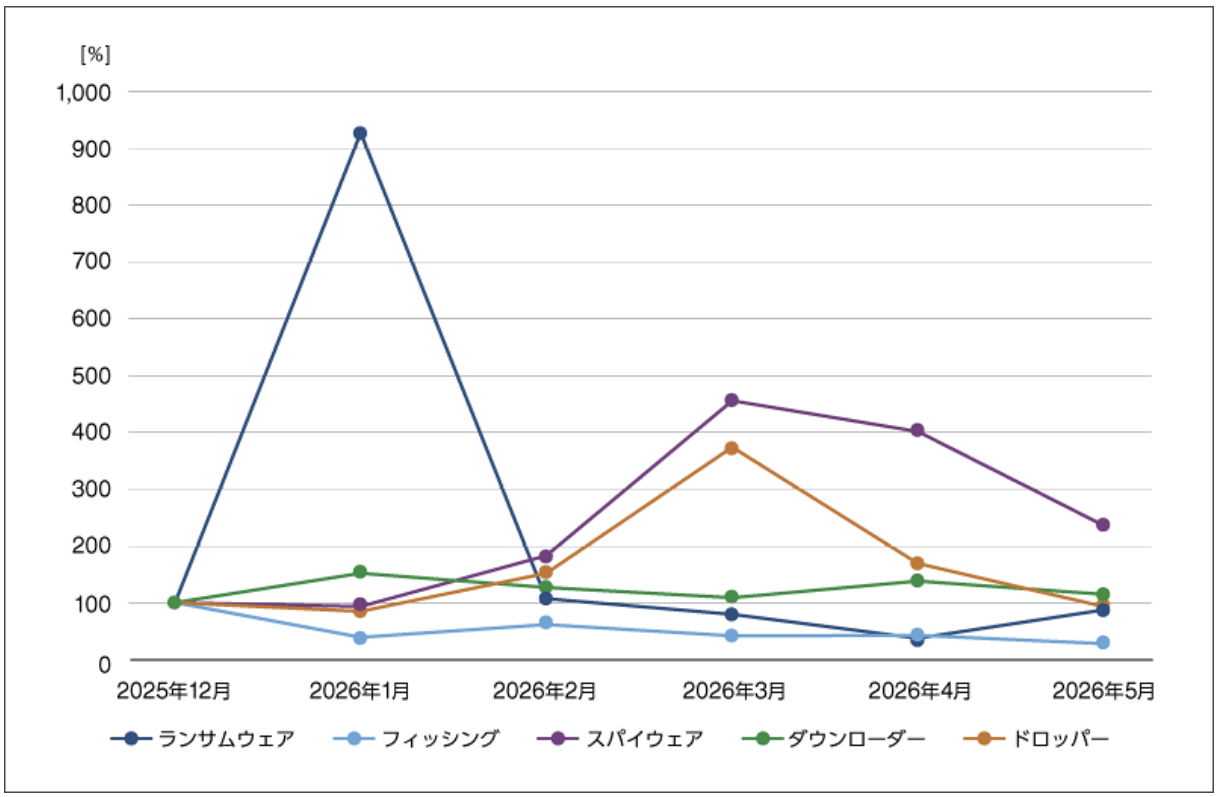
国内マルウェア検出数*2 上位（2026 年 5 月）

順位	マルウェア	割合	種別
1	DOC/Fraud	48.1%	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	12.5%	アドウェア
3	HTML/Phishing.Agent	5.4%	メールに添付された不正な HTML ファイル
4	JS/Agent	2.4%	不正な JavaScript の汎用検出名
5	Win32/Exploit.CVE-2017-0199	1.6%	脆弱性 CVE-2017-0199 を悪用するプログラム
6	JS/Danger.ScriptAttachment	1.4%	ダウンローダー
7	BAT/Obfuscated	1.0%	難読化された不正な BAT ファイル
8	JS/TrojanDownloader.Agent	0.8%	ダウンローダー
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	HTML/Phishing.Gen	0.5%	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。

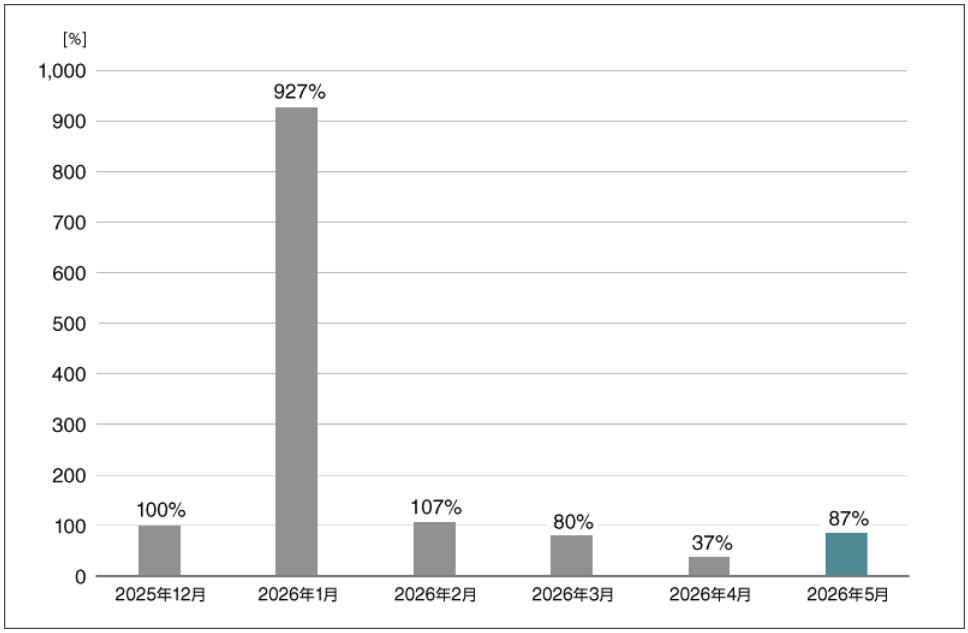
5 月に国内で最も多く検出されたマルウェアは、DOC/Fraud でした。
これは詐欺サイトのリンクが埋め込まれた DOC 形式のファイルとして検出され、ユーザーがリンクをクリックすると、個人情報が窃取されたり、さらなるマルウェアがダウンロードされたりする可能性があります。

2026 年 5 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。



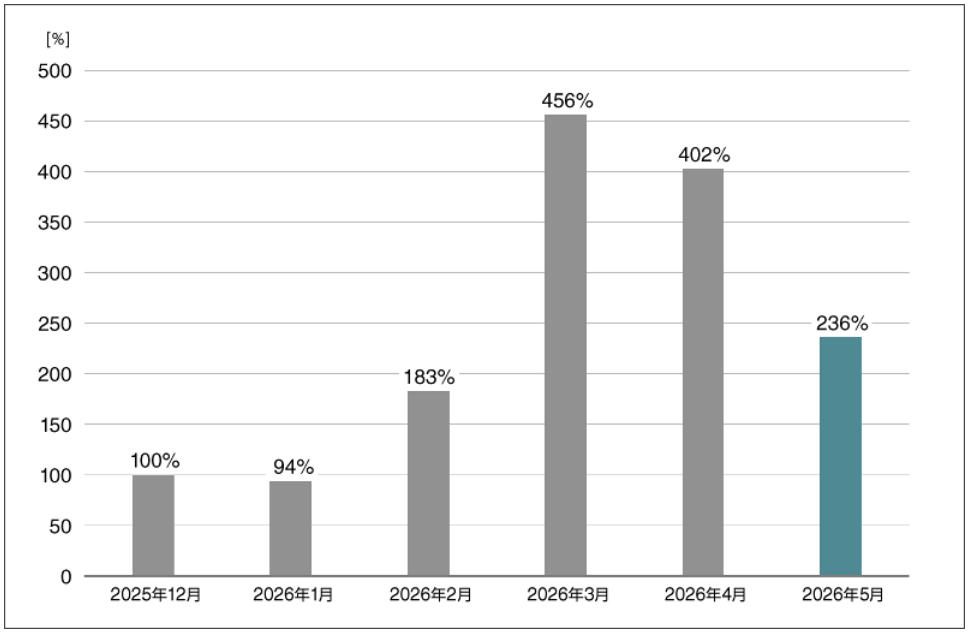
国内マルウェアの種類別検出数の推移
（2025 年 12 月の各検出数を 100%として比較）

2026 年 5 月はランサムウェアの検出数が増加しました。一方で、ランサムウェア以外の検出数は減少しています。



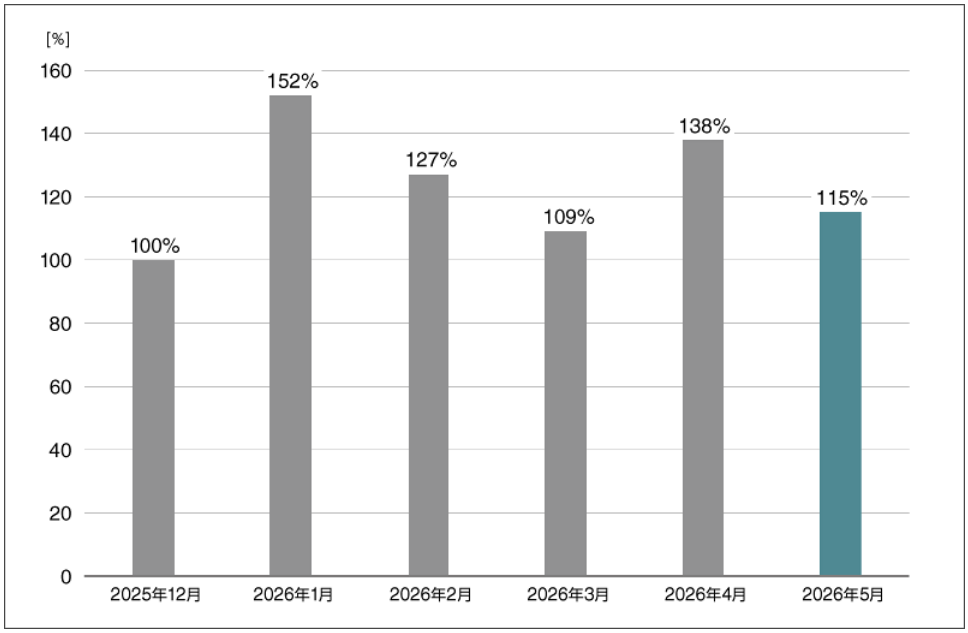
ランサムウェア検出数の推移（国内）

（2025 年 12 月の検出数を 100%として比較）



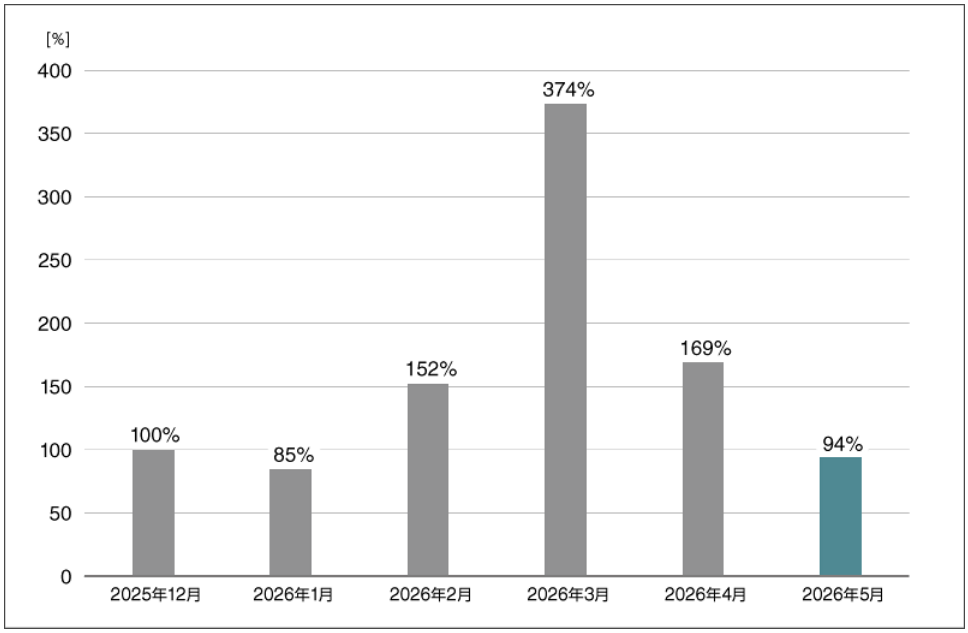
スパイウェア検出数の推移（国内）

（2025 年 12 月の検出数を 100%として比較）



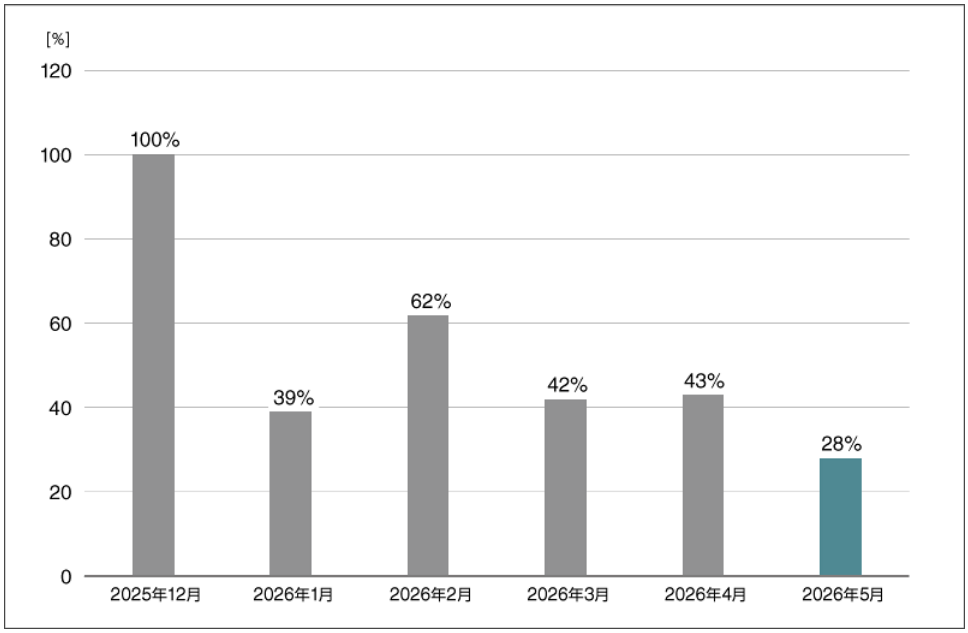
ダウンローダー検出数の推移（国内）

（2025 年 12 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）

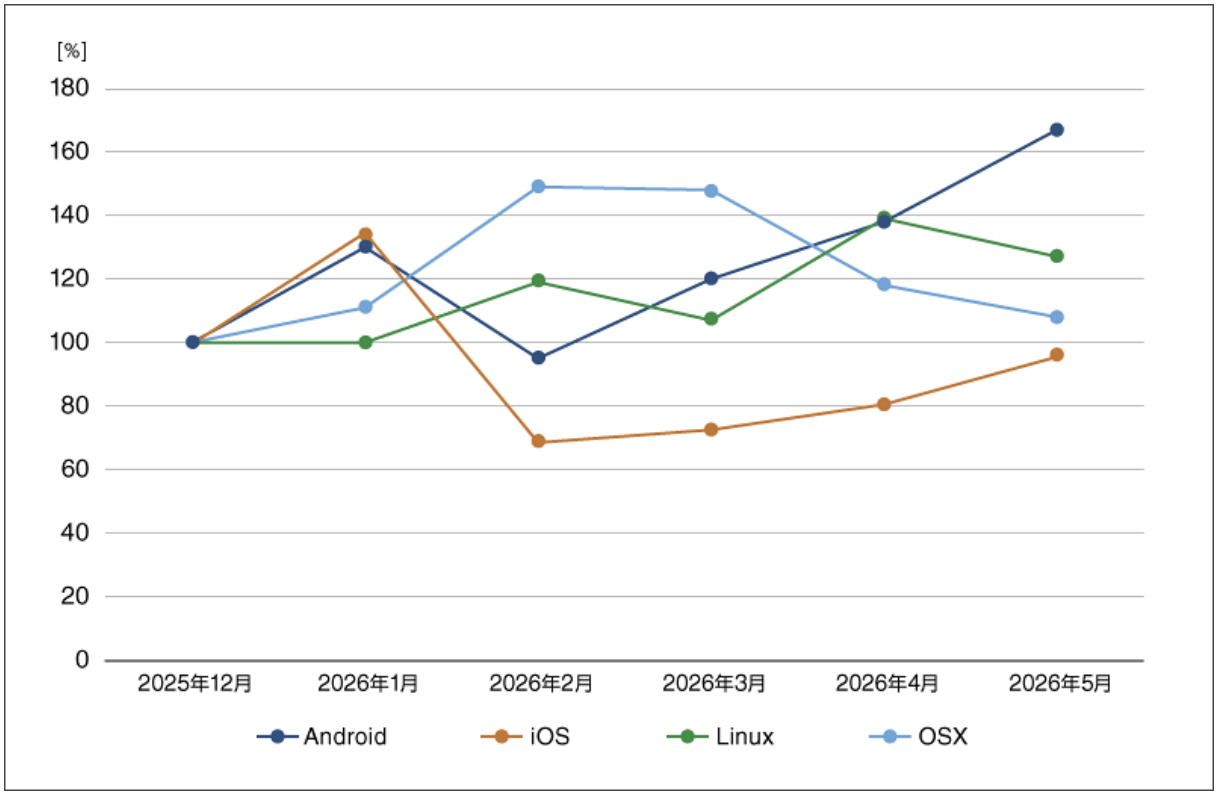
（2025 年 12 月の検出数を 100%として比較）



フィッシング検出数の推移（国内）

（2025 年 12 月の検出数を 100%として比較）

2026 年 5 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 12 月の各検出数を 100%として比較）

2026 年 5 月は Android や iOS を狙ったマルウェアが増加しました。一方で、Linux や OS X を狙ったマルウェアは減少しました。

正規の生成 AI 共有リンクを悪用する LLMShare キャンペーン

近年、ChatGPT や Claude をはじめとする生成 AI サービスの利用が急速に拡大しています。企業では業務効率化や情報収集、文書作成などに活用される機会が増え、個人利用においても日常的なツールとして定着しつつあります。

一方で、利用者基盤が拡大したサービスは、攻撃者にとっても魅力的なツールとなります。生成 AI サービスも例外ではなく、攻撃者が正規の生成 AI サービスを装った偽サイトや広告を用いて、利用者をフィッシングページや不正なアプリへ誘導する手口が確認されています。

こうした中、2026 年 5 月に ChatGPT や Claude の共有リンク機能を悪用する「LLMShare」と呼ばれる攻撃キャンペーンが確認されました。LLMShare は、正規の ChatGPT や Claude の共有リンクを悪用して利用者をマルウェア感染に誘導します。

- **LLMShare とは**

LLMShare とは、ChatGPT や Claude などの生成 AI サービスが提供する「共有リンク機能」を悪用し、マルウェア配布につなげる攻撃手法です。

共有リンク機能とは、AI との会話内容や生成結果を URL として他者に共有できる機能です。本来は、回答内容を共有したり、業務上のナレッジを共有したりするための便利な機能です。しかし LLMShare では、攻撃者が ChatGPT や Claude の共有リンクを作成し、そのリンクを開いた先の共有ページ内に、偽の障害通知やインストール案内を表示します。

利用者には、正規の AI サービス上で公式の案内が表示されているように見えますが、実際には攻撃者が作成した会話内容であり、ボタンや手順に従うと不正なダウンロードページやマルウェア実行へ誘導されます。

攻撃者はさらに検索広告を悪用し、利用者をこれらの共有リンクへ誘導します。

利用者から見ると、「検索結果の広告をクリックしたら、ChatGPT や Claude の正規ページが開いた」ように見えるため、不審に感じにくい点が特徴です。つまり LLMShare は、生成 AI サービスへの信頼と、正規ドメインであることの安心感を悪用した攻撃といえます。

- **攻撃の流れ：ChatGPT と Claude の事例**

LLMShare では、ChatGPT と Claude の両方で類似した手口が確認されています。ただし、利用者をだます方法には違いがあります。

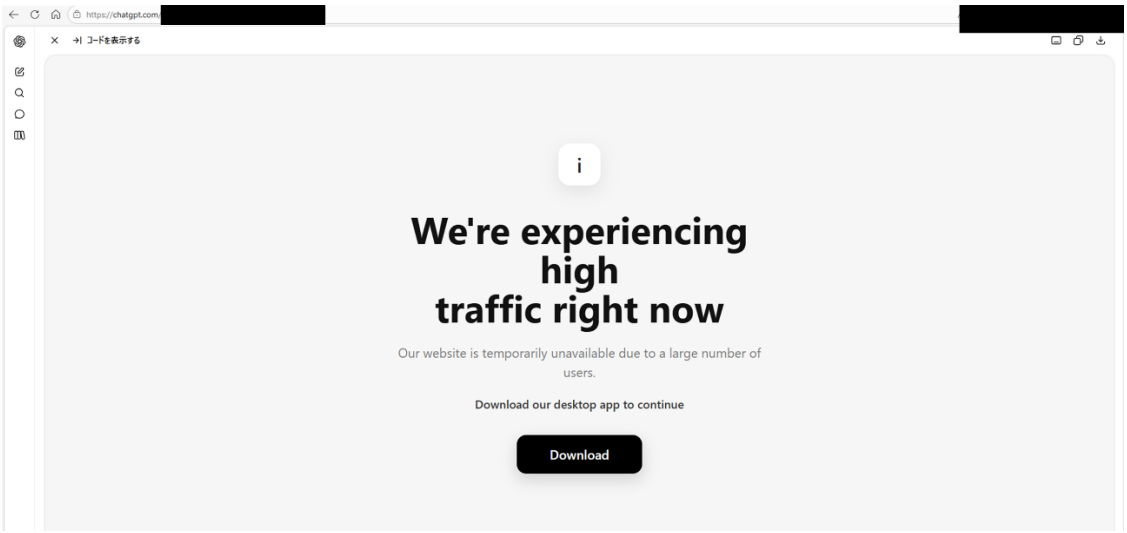
■　ChatGPT の共有リンクを悪用した事例

ChatGPT を悪用した事例では、利用者はまず検索エンジンで ChatGPT 関連のキーワードを検索します。攻撃者は「chatgpt」「chatgpt free」「chat gpt」などの検索語句や、入力ミスを狙ったキーワードに広告を表示し、利用者を共有リンクへ誘導していました。

この事例では、ChatGPT の共有リンク上で、HTML などのコードを画面として表示できるコードレンダリング機能が悪用されていました。これにより、共有ページ内に本物の障害通知のように見える画面が表示されます。

攻撃の流れは次の通りです。

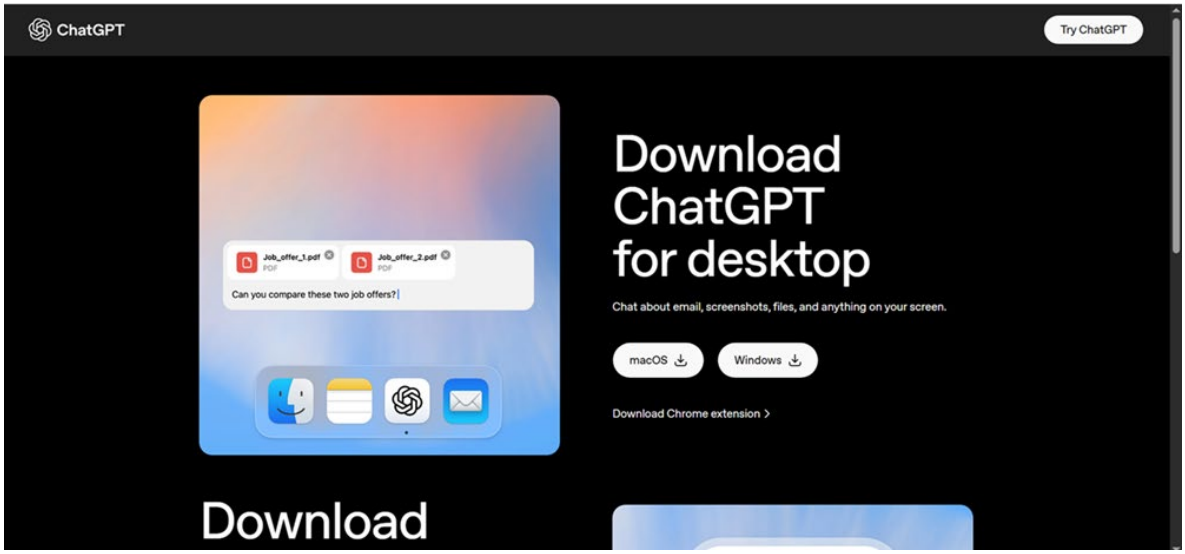
1. 利用者が検索広告をクリックする
2. chatgpt.com の正規共有リンクへ遷移する
3. コードレンダリング機能で作成された偽の障害通知が表示される
4. 「デスクトップアプリをダウンロードしてください」と案内される
5. 偽の ChatGPT ダウンロードページへ誘導される
6. 偽インストーラーを実行するとマルウェア感染につながる



ChatGPT のコードレンダリング機能によって表示される偽の障害通知のイメージ

上記の画像において、ブラウザーのアドレスバーには正規の ChatGPT ドメインが表示されています。そのため、利用者は「公式の案内」と判断してしまう可能性があります。

利用者がダウンロードボタンをクリックすると、ChatGPT の公式ダウンロードページに似せた外部サイトへ誘導されます。

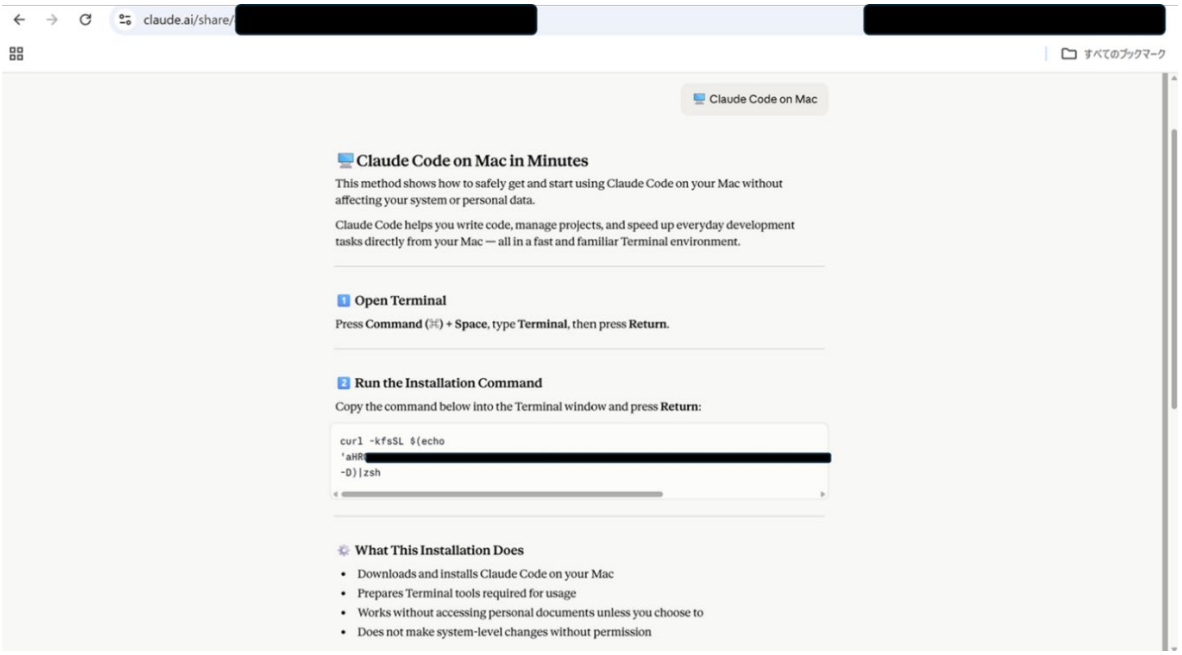


偽の ChatGPT ダウンロードサイト

この偽サイトでは、正規アプリに見せかけたインストーラーのダウンロードが促されます。
最初に表示されるページが ChatGPT の正規共有リンクであるため、利用者は不審に感じにくく、そのまま偽インストーラーを実行してしまうおそれがあります。実行してしまった場合、端末内の情報や認証情報が盗まれたり、社内システムへの不正アクセスにつながる可能性があるため注意が必要です。

■ Claude の共有リンクを悪用した事例

Claude を悪用したケースでは、ChatGPT の事例とは異なり、偽のダウンロードページには遷移させず、共有リンク機能を使い、インストールガイドを装ったページを表示させる手法が確認されています。
claude.ai の共有リンク機能を使い、「Claude Code on Mac」のインストールガイドを装ったページが確認されています。このページでは、利用者にターミナルを開かせ、表示されたコマンドをコピーして実行するよう促していました。



Claude の共有リンクに表示された偽のインストール手順

Claude の場合の特徴は、偽のインストール手順によって、利用者自身に危険な操作を実行させる点です。攻撃の流れは次の通りです。

1. 利用者が検索広告やリンクから Claude の共有リンクへアクセスする
2. Claude のページ上に、偽のインストール手順が表示される
3. ターミナルを開くよう指示される
4. 表示されたコマンドをコピー＆ペーストするよう促される
5. コマンド実行により、不正なスクリプトやマルウェアが実行される

このように、偽のインストール手順を表示し、利用者自身にコマンドを実行させる手口は、ClickFix や InstallFix と呼ばれる攻撃手法と共通しています。特に AI 関連ツールや開発ツールでは、コマンドラインでのインストール手順に見慣れている利用者もいるため注意が必要です。

ChatGPT と Claude で行われた LLMShare キャンペーンの比較

項目	ChatGPT 版	Claude 版
悪用される機能	共有リンク＋コードレンダリング	共有リンク
表示内容	偽の障害通知	偽のインストール手順
外部サイトへの誘導の有無	有	無
標的 OS	Windows、macOS	macOS
マルウェア感染方法	偽インストーラーのダウンロード・実行	偽インストールコマンドの実行

対策

LLMShare への対策では、「URL が正しいか」だけでなく、そのページで何を求められているかを確認することが重要です。
chatgpt.com や claude.ai のような正規ドメイン上のページであっても、次のような操作を求められた場合は注意が必要です。

- アプリやインストーラーのダウンロード
- 外部サイトへの遷移
- ターミナルや PowerShell でのコマンド実行
- エラー解消やインストールを理由にした操作指示

■ 利用者向け

生成 AI サービスの共有リンクは、本来、会話内容や回答結果を閲覧するためのものです。しかし、正規ドメイン上に表示されたページであっても、アプリのダウンロードやコマンド実行を求められた場合は注意が必要です。利用者からは通常の公式ページに見える場合でも、実際には共有機能や共有コンテンツを悪用したページである可能性があります。URL だけで判断せず、そのページが何を求めているかを確認することが重要です。
利用者が意識したい基本ルールは次の通りです。

- AI サービスのアプリは、検索広告や共有リンク内のボタンからダウンロードしない
- URL に「/s/」「/share/」「/shared/」などが含まれる場合は、共有リンクの可能性があるため注意する
- ページ遷移が発生した場合は、都度 URL を確認する
- 共有リンク内の「Download」「Install」「Fix」などのボタンを安易に押さない
- Web ページや AI の回答に表示されたコマンドは、意味を理解しないまま端末で実行しない
- 不審な案内が表示された場合は、情報システム部門に確認する

特に注意したいのは、「アクセスが集中しているためアプリを入れてください」「不具合を直すためにこのコマンドを実行してください」といった案内です。一見正当な理由が示されていても、確認すべきは URL ではなく、求められている操作内容です。正規ドメイン上のページであっても、ダウンロードやコマンド実行を求められた場合は、すぐに従わないことが重要です。

■ 情報システム部門向け：ルール整備と端末側の対策を組み合わせる

情報システム部門では、利用者が迷わず判断できるように、生成 AI サービスの利用ルールを明確にしておくことが重要です。
特に、LLMShare では正規ドメイン上の共有リンクが悪用されるため、「URL を確認しましょう」だけでは十分ではありません。社内では、次のような内容を周知すると効果的です。

- 利用を許可しているサービスやツールを一覧化し、そのダウンロードページを社内ポータルなどに掲載する
- 検索広告経由でソフトウェアをダウンロードしないよう周知する
- 共有リンク内のインストール案内や障害通知を安易に信用しないよう教育する

技術的な対策としては、EDR（Endpoint Detection and Response）の活用が有効です。LLMShare では、最初のアクセス先が正規ドメインであるため、URL フィルタリングだけでは危険性を判断しにくい場合があります。そのため、端末上で発生する不審な挙動を検知できる体制を整えておくことが重要です。
EDR では、次のような挙動を検知・調査できるようにしておくとよいでしょう。

- インターネットからダウンロードされた実行ファイルの起動
- PowerShell やターミナルを使用したコマンド実行
- 不審なプロセスがブラウザーや OS に保存された認証情報・セッション情報など、通常アクセスする必要のない領域にアクセスする挙動
- 不審なプロセスが外部サーバーへ通信する挙動

LLMShare は、正規ドメインを経由するため、入口だけを見て安全かどうかを判断するのが難しい攻撃です。情報システム部門では、利用者への周知と EDR による端末監視を組み合わせて備えることが重要です。

まとめ

2026 年 5 月のレポートでは、ChatGPT や Claude の正規共有リンクを悪用する「LLMShare」と呼ばれる攻撃キャンペーンを取り上げました。LLMShare は、正規ドメイン上の共有リンクに偽の障害通知やインストール手順を表示し、利用者をマルウェア感染に誘導する手口です。
特に注意すべき点は、chatgpt.com や claude.ai といった正規ドメインが使われるため、「URL が正しいから安全」と判断してしまいやすいことです。
正規のサービス上に表示されている案内であっても、すべてが安全とは限りません。ファイルのダウンロードやコマンド実行を求められた場合は、一度立ち止まって確認することが重要です。

■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

●LLMShare: how attackers are turning AI chatbot pages into malware delivery platforms | Push Security
https://pushsecurity.com/blog/llmshare-malvertising-campaign

Canon

キヤノンマーケティングジャパン株式会社