

Press Release

ブロックされたディープフェイク関連攻撃の98%が日本語で生成されたことが判明

YouTube や Google 広告を悪用した新たな詐欺手口も増加

Gen「2026年第2四半期 脅威レポート 日本版」公開

ノートンやアバストなどの信頼あるブランド群を擁するグローバル企業 Gen は、「2026年第2四半期（2026年4月～6月）の脅威レポート 日本版」を発表しました。日本では、サイバー攻撃全体のブロック件数が前期比7.7%減少した一方で、フィッシングや詐欺、リモートアクセス型の攻撃など、利用者を狙って行動を促す脅威が大きく増加しました。フィッシング攻撃は45.0%増の1,566万件、詐欺攻撃全般では27.0%増の2,062万件がブロックされています。

中でも顕著な増加があったものとしてはディープフェイク動画に関連する攻撃が挙げられ、ブロック件数が前期比約9倍に急増しました。そのほか、宅配便の通知を装う SMS 詐欺、YouTube や Google 広告など、日常的に利用するサービスを入口とした詐欺、日本のニュースサイトを模倣した攻撃なども確認されています。攻撃者が動画、広告、SMS、ニュースサイトなど、利用者が日常的に接するチャネルへと活動範囲を広げている実態が明らかになりました。

攻撃者が端末を遠隔操作するために利用するリモートアクセス攻撃は2026年5月以降に確認された攻撃活動の活発化を背景に、714.9%増加しました。その一種である RAT（Remote Access Trojan）は、同時期に1,427.7%増加しました。RAT は、端末への侵入後に攻撃者が遠隔から操作を行い、情報の窃取やさらなるマルウェアの導入などにつながる可能性のある脅威です。

ディープフェイク動画関連の攻撃ブロック件数は日本で約9倍に急増 日本語コンテンツが最大の割合に

ディープフェイク動画に関連する世界全体のブロック件数は、2026年第2四半期に前期の約3倍に増加しました。一方、日本では前期の約9倍に急増し、世界全体と比較して顕著な増加が見られました。

さらに、日本でブロックされた攻撃の約51,600件のうち、日本語コンテンツは約43,200件と最大の割合を占めました。Gen では、日本語を含む多言語の脅威に対するブロック精度の向上に注力しており、日本語によるディープフェイク動画の増加は、脅威が単に世界的な動向として日本に流入しているだけでなく、日本の利用者に合わせてローカライズされたコンテンツが拡大している可能性を示しています。

ブロックした攻撃の言語別内訳

日本語

43,190件をブロック（全体の約80.2%） | うち詐欺は3.5%

最多のセグメント

英語

3,754件をブロック（全体の約7.0%） | うち詐欺は5.3%

その他・不明

1,107件をブロック（全体の約2.1%） | うち詐欺は77.0%

※「その他・不明」には、言語情報を特定できなかったものが含まれます。そのため、合計は全体の件数と一致しない場合があります。

＜本件に関するお問い合わせ先＞

Gen PR 事務局（株式会社プラチナム内） 担当：石間、加藤、宮下
TEL：03-5572-6071（PR 事務局）／Mail：norton-pr@vectorinc.co.jp
© Copyright 2026 Gen Digital Inc. All rights reserved.

AI エージェントの活用拡大に伴う新たなセキュリティリスクも

生成 AI の活用が広がる中、AI が質問に答えるだけでなく、自ら情報の収集やファイルの操作、外部サービスとの連携などを実行する「AI エージェント」においても、新たなセキュリティリスクへの注意が必要です。

AI エージェントは、外部から読み込む指示や設定ファイルに不正な命令が含まれていた場合、意図しない操作を実行するリスクがあります。また、AI エージェントがコマンドの実行やファイルのダウンロード、認証情報へのアクセスなどが、悪意のある動作につながる可能性もあります。

こうしたリスクに対応するには、AI が生成する回答だけでなく、AI エージェントが読み込む指示や設定、実際に実行する操作、アクセス先の Web サイトやネットワーク環境まで含めた、多層的なセキュリティ対策が重要となります。

宅配便を装う SMS 詐欺が7,370.9%急増 被害対象は Android 端末が中心に

宅配便や荷物の配送通知を装う SMS 詐欺も、第2四半期に急増しました。いくつかの標的型攻撃の活発化を背景に、前四半期と比較して大幅な増加が確認されました。

このタイプの詐欺では、「荷物を届けられなかった」「配送状況を確認してください」など、日常的に受け取る配送通知を装った SMS を送り、利用者にリンクをクリックさせることで、偽サイトへの誘導や個人情報・認証情報の入力を促します。

また、ブロックされた攻撃の99.22%が Android 端末を標的としていました。前四半期の攻撃件数が少なかったことに加え、6月に攻撃が集中していたことから、今後も継続的な動向の監視が必要です。



テクニカルサポート詐欺の入口は、YouTube・Google 広告へ

「端末がウイルスに感染した」などの偽の警告を表示し、サポート窓口への電話や遠隔操作を促すテクニカルサポート詐欺では、YouTube や Google 広告を入口とした新たな攻撃活動が日本で確認されました。

今回確認された攻撃では、YouTube や Google 広告から Microsoft が提供するクラウドサービスである Azure 上に設置された、使い捨ての Web サイトへ利用者を誘導していました。Web ブラウザを強制的に全画面表示にしたり、パソコンに高い負荷をかけたりすることで、あたかもパソコンに重大な問題が発生したかのように見せかけ、表示された偽のサポート番号へ電話するよう促していました。これまで不審な Web サイトなどが主な入口と考えられていた詐欺が、動画サービスや検索広告など、利用者が普段から接する環境へ入り込んでいることが、大きな特徴です。

日本の大手ニュースサイトへの信頼を悪用 Livedoor ブランドを装う攻撃も確認

第2四半期には、日本の正規ニュースポータルサイトへの信頼を悪用した攻撃も確認されました。今回確認された攻撃では、攻撃者が「Livedoor」のニュースポータルサイトを模倣した偽サイトを作成し、悪意のある広告を通じて利用者を誘導していました。この偽サイトには不正な JavaScript が埋め込まれており、アクセスした利用者のトラッキング情報を攻撃者側に送信したり、端末の処理能力を不正に利用しようとしていたりする仕組みが確認されました。



また、攻撃に使用されたドメインは登録からわずか6日しか経過しておらず、URL に「Livedoor」のブランド名を含めることで、利用者に正規サイトであると誤認させる手口が使われていました。偽サイトそのものを作るだけでなく、利用者が日常的に利用する正規サービスやブランドへの信頼を攻撃経路として利用することで、URL や画面を一目見ただけでは危険性を判断しにくくする手口が広がっています。

巧妙化するサイバー詐欺から身を守るために

AI 技術の悪用によるディープフェイク動画の拡大に加え、動画サービスや検索広告、SMS、ニュースサイトなど、利用者が日常的に接するサービスを悪用した攻撃が確認されています。こうした脅威から身を守るためには、見慣れたサービスや信頼できるブランドを装った情報であっても、その内容や発信元を慎重に確認することが重要です。

1. 動画や SNS 上の情報を鵜呑みにしない

有名人や企業関係者が登場する動画であっても、AI によって生成・加工された偽のコンテンツである可能性があります。投資や金銭の支払い、個人情報を入力を促す内容には特に注意し、公式サイトや公式アカウントなど、別の信頼できる情報源で事実を確認してください。

2. 広告や SMS 内のリンクを安易にクリックしない

広告やメッセージに表示されたリンクをすぐに開くのではなく、必要に応じて公式アプリや公式サイトから情報を確認してください。

3. 突然表示される警告画面やサポート番号を信用しない

Web サイトの閲覧中に、ウイルス感染などを知らせる警告画面が表示されても、記載された電話番号へすぐに連絡しないでください。端末の不具合やセキュリティ上の問題が疑われる場合は、正規のサポート窓口を自分で確認することが重要です。

4. セキュリティ対策を継続し、不審な動作に注意する

OS やアプリを最新の状態に保ち、信頼できるセキュリティ対策製品を活用してください。また、不審なサイトにアクセスした場合や、身に覚えのないファイルのダウンロード、認証情報の入力を求められた場合には、慎重に対応することが重要です。

Gen について

Gen™ (NASDAQ: GEN) は、信頼性の高い消費者向けのブランドであるノートン、アバスト、ライフロック、MoneyLion などを通じてデジタルの自由を推進する、グローバル企業として、デジタル社会における個人向け金融サービスの向上とサイバーセキュリティの提供に取り組んでいます。Gen は、デジタルライフを安全に、かつ前向きに、安心して歩んでいけるよう後押ししています。Gen は、サイバーセキュリティ、オンラインプライバシー、個人情報保護の分野において、受賞歴のある製品とサービスを、150か国以上で約5億人のユーザーに提供しています。詳細は、GenDigital.com をご覧ください。

Gen Threat Labs について

Gen Threat Labs は、世界中の最新デジタル脅威や詐欺を特定・分析する Gen のサイバーセキュリティ研究チームです。データ、研究、技術的専門性に基づき、進化するサイバー環境のリスクを可視化し、ノートンやアバストなどの信頼あるブランド群を支えるセキュリティ技術に知見を提供しています。

ノートン製品情報

■パソコン、スマホをオールインワンで守るセキュリティソフト

ノートン™ 360 : <https://jp.norton.com/360>

ノートン 360プレミアムは、パソコン、スマホ、タブレットなどのデバイスと Wi-Fi 通信などをオールインワンで守るセキュリティソフトです。ウイルスなどのサイバー攻撃から防御するとともに、AI で詐欺対策を行います。インターネット利用時に通信内容を盗み見されないように暗号化する VPN 機能を搭載。その他、お子様を守るための保護者機能、個人情報流出を検知するダークウェブモニタリング機能、パスワードを安全に管理するパスワードマネージャー機能など、消費者の皆様が、より快適かつ安全にインターネットを利用できるようになる機能を多数搭載しています。

