ノートン 広報部
2026年7月吉日

Press Release

Gen「2026年第1四半期 脅威レポート 日本版」公開

漫画閲覧サイト、アニメ配信サイトなど、日本市場を標的としたテクニカルサポート詐欺が145%増加

フィッシング攻撃の被害を将来の不正送金やアカウント乗っ取りへとつなげる「インフォスティーラー」も270%急増

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1四半期（2026年1月～3月）の脅威レポート 日本版を発表しました。日本市場では、フィッシング攻撃やテクニカルサポート詐欺、偽 EC サイト、SMS 詐欺など、人間の心理や行動を悪用する「ソーシャルエンジニアリング攻撃」が拡大していることが明らかになりました。特にフィッシング攻撃は前四半期比で約2倍に増加し、1,068万件を超える攻撃がブロックされました。

また、漫画・アニメ配信サイトなどを経由したテクニカルサポート詐欺や、楽天を装う偽ショッピングサイト、Android 端末を標的とした SMS 詐欺など、日本のユーザーを狙った攻撃も確認されています。

ブラウザ、SMS、オンラインショッピング、動画・漫画・アニメ配信サイトなどを横断し、攻撃者は楽天や Amazon などの正規サービスに見せかけた警告表示、割安な商品ページ、不審なリンクを通じて、認証情報の入力、リンクのクリック、電話連絡、決済情報の入力といったユーザー自身の行動を誘導していました。

フィッシング攻撃が急増、依然として消費者にとっての大きな脅威に

フィッシング攻撃は引き続き、日本の消費者を狙う脅威の中で最も多く確認された攻撃手法となりました。フィッシング攻撃では、利用者が信頼するサービスと見分けがつかないログイン画面が表示され、わずかに異なるドメインへ誘導されることで、ID やパスワードなどの認証情報が窃取されます。2026年第1四半期にはフィッシング攻撃を1,068万件ブロックし、223万人のユーザーを保護しました。前四半期の556万件から約2倍の増加。

攻撃の80%は Windows 環境で確認された一方、モバイル環境を狙う攻撃も増加しており、iOS 端末だけでも124万件のフィッシング攻撃が確認されました。フィッシング攻撃は個人情報を窃取するだけでなく、その後のアカウント乗っ取りや金銭詐欺の入り口となるケースも多く、引き続き警戒が必要な脅威となっています。

日本市場を狙うテクニカルサポート詐欺が145%増加

「あなたのデバイスはウイルスに感染しています」などの警告画面を表示し、利用者に電話での連絡や遠隔操作の受け入れを促すテクニカルサポート詐欺も大きく増加しました。2026年第1四半期にはテクニカルサポート詐欺を115万件ブロックしました。これは、前四半期比145%の増加となります。

これらの攻撃では、全画面の警告表示や警告音、Windows を模倣した画面デザインなどを利用し、利用者の不安を煽ることで冷静な判断を妨げます。利用者が表示された番号へ電話すると、遠隔操作ソフトのインストールや不要なサポート費用の支払いを要求されるケースが確認されています。

また今回の調査では、日本の利用者を標的とした組織的な攻撃キャンペーンも確認されました。攻撃者は海賊版サイトや漫画閲覧サイト、アニメ配信サイト、ファイル共有サイトなどを悪用しており、日本語コンテンツを利用した誘導が行われていました。

偽ショッピングサイトが67%増加、楽天を装う攻撃も確認

オンラインショッピング利用者を狙う偽ショッピングサイトも増加傾向にあります。これらのサイトは正規 EC サイトと見分けがつかない外観を持ち、市場価格より30～50%安い商品を掲載することで利用者を誘導します。しかし、商品が届かないだけでなく、入力したクレジットカード情報などが窃取される危険性があります。2026年第1四半期には偽ショッピングサイト関連の攻撃を196万件ブロックしました。これは、前四半期比67%の増加となります。また、モバイルショッピング利用者を狙う傾向も強まっており、iOS ユーザーだけでも50万人以上が攻撃対象となりました。
さらに調査によると、このような攻撃で使われた Web ドメインには、楽天など特定のブランド名を含み、ユーザー側の判断を迷わせるものも確認されました。

Android ユーザーを狙う SMS 詐欺が急増

SMS を通じた詐欺も急速に拡大しています。2026年第1四半期には、Android ユーザーを狙い、アンケート回答を装う SMS 詐欺が前四半期比で6,637%増加したほか、宝くじ当選を騙る SMS 詐欺も3,056%増加しました。確認されたメッセージには、LINE の当選通知、銀行口座の利用制限、配送通知、ショッピング関連の案内など、日常的に受け取るメッセージを模倣した内容が含まれていました。

SMS は利用頻度が高く、利用者が警戒心を持ちにくいコミュニケーション手段であることから、攻撃者にとって有効な攻撃経路となっています。特に Android 端末を中心に攻撃が確認されており、リンクを開く前に送信元や内容を慎重に確認することが重要です。

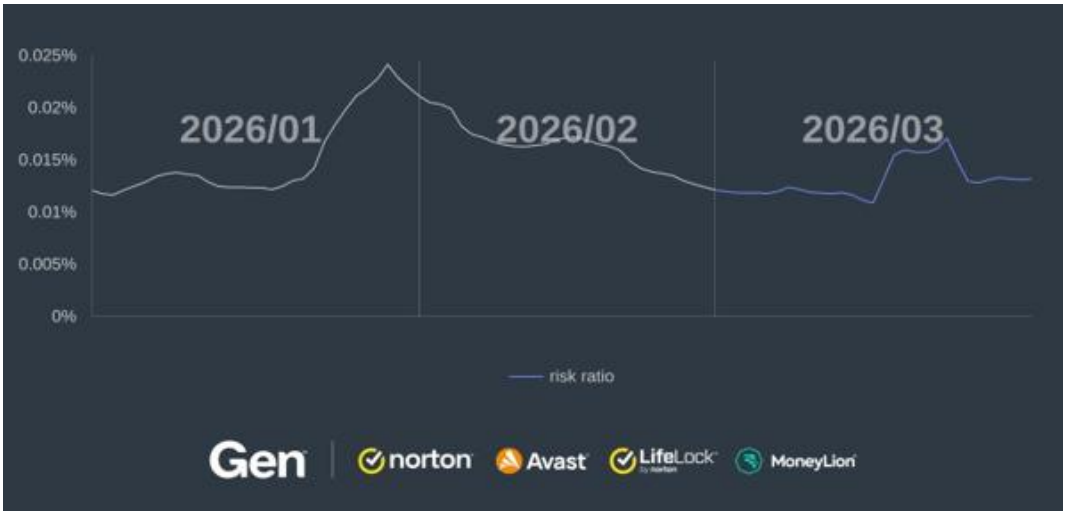
詐欺を超えるマルウェアの脅威、汎用的なインフォスティーラーは270%増加

Gen のサイバーセーフティ研究チームによると、ソーシャルエンジニアリング攻撃が拡大する一方で、それに比べて被害規模が甚大になりやすいマルウェアも急増しています。2026年第1四半期、日本では、スパイウェア（+419%）、ワーム（+414%）汎用的なインフォスティーラー（+270%）ドロッパー（+164%）、など複数のマルウェアカテゴリで大幅な増加が確認されました。

これらの脅威は詐欺のように目立つものではありませんが、一度デバイスが感染すると、認証情報や個人情報、金融情報などが継続的に窃取される可能性があります。さらに、端末上の操作を監視されたり、攻撃者にデバイスへのアクセスを許可してしまったり、別のマルウェアを追加でインストールされるリスクもあります。

特に汎用的なインフォスティーラーは被害者に気づかれないまま保存済みパスワードや Cookie、暗号資産ウォレット情報などを窃取することから、サイバー犯罪者による不正アクセスや金銭詐欺の入り口として利用されています。2026年第1四半期にはインフォスティーラーを30,377件ブロックし、そのうち3分の1以上はモバイルデバイスを標的とした攻撃でした。前四半期比270%の増加。これらの攻撃は保存済みパスワードやブラウザセッション、クレジットカード情報などを密かに窃取することを目的としており、利用者が異変に気付きにくいことが特徴です。

汎用的なインフォスティーラーは、今日のフィッシング攻撃による被害を将来の不正送金やアカウント乗っ取りへとつなげる“橋渡し役”として機能しており、日本市場においても無視できない脅威となっています。



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ーフ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 のサイバーセーフ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、Norton、Avast、LifeLock などのブランドを支えるセキュリティ技術に知見を提供しています。