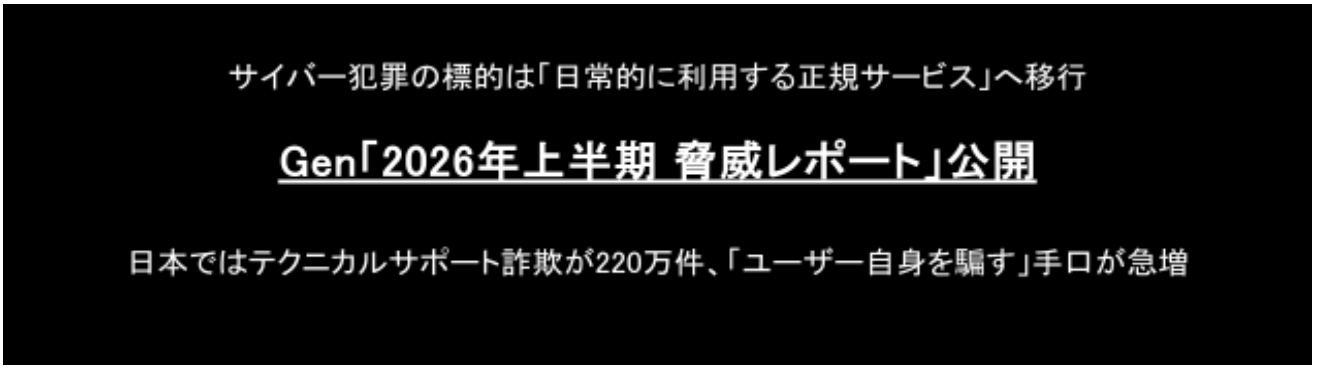
ノートン 広報部

2026年8月吉日

Press Release



ノートンやアバストなど、信頼のブランドを擁し、デジタルの自由を推進するグローバルリーダーであるGenは、2026年上半期（2026年1月～6月）の「脅威レポート」を発表しました。

本レポートにおいて、サイバー攻撃の手法に明確な変化が起きていることが明らかになりました。サイバー犯罪者は、システムの技術的な脆弱性を突いたり、一目で不審とわかるようなマルウェアを無差別に拡散したりする手法から、ユーザーが普段から利用し、安全だと信じているプラットフォームやサービスを巧みに悪用する手口へとシフトしています。宿泊施設の予約サイトや家族間のメッセージアプリ、実在するブランド、ソフトウェアの更新システム、広告プラットフォーム、さらには自律的に動くAIエージェントに至るまで、私たちの日常的なデジタル生活の基盤そのものがサイバー犯罪者に狙われています。

グローバルにおける脅威の傾向：日常のオンライン行動に紛れ込む詐欺手口

2026年上半期において顕著だったのは、普段利用しているプラットフォームに巧妙に偽装するサイバー犯罪です。ホテルの予約サイトを通じて実際の予約情報を参照しながら詐欺メッセージが届いたり、SNSで「すぐに現金が手に入る」と誘い込まれた実在する人物の口座を経由して不正資金が移動したりするケースが確認されています。

●オンラインストア詐欺

偽のショッピングサイトを用いた攻撃のブロック数は1億1,420万件に達し、前期比で109%増加しました。

●公的機関や家族へのなりすまし

公的機関を装って金銭や情報を騙し取る手口が387%増加したほか、家族を装うなりすましも454.2%増加しまし

た。特にメッセージアプリでは、パスワードのハッキングではなく、デバイスの連携機能を悪用してユーザーを騙し、サイバー犯罪者のブラウザを連携させてアカウントへの永続的なアクセス権を奪う手口も確認されています。

●プライバシー侵害とデータ流出の連鎖

個人の行動を追跡するトラッキングの試みは約19億回ブロックされました。また、ノートンおよびLifeLockのデータ侵害通知は628.1%増の330万件に達し、総計で1,000万件以上の通知が送信されています。メールアドレスを含む個人情報の流出が1,570万件以上確認されたほか、銀行口座に関連する不審なアクティビティの警告は734%増加しており、データ流出から金融被害へと急速に連鎖している実態が浮き彫りになっています。

■ 日本における脅威の傾向：突出するテクニカルサポート詐欺と、利用者を誘導して感染させる手口の急増

日本国内においては、詐欺型攻撃が依然として最大の脅威となっており、世界的な傾向と比較しても特定の手口が集中していることが明らかになりました。

●利用者を誘導して自身の端末に感染させる手口が急増

日本での特筆すべき傾向として、コンテンツや動画、ページデザインなどを駆使し、利用者を誘導して自身の端末に感染させる手口の急増が挙げられます。特に、信頼できるソフトウェアなどに偽装する一般的な「なりすまし（Fake）」コンテンツの検知は前期比942%増と爆発的な伸びを記録しました。正規の解説動画を装う「偽チュートリアル」型詐欺（39%増）などとあわせて、ユーザーの不安や学習意欲といった心理的弱点を突くアプローチが広がっています。

●深刻な被害をもたらすマルウェア関連の脅威も増加

日本国内では以下の通り、マルウェア関連の脅威も軒並み高い増加率を記録しました。

- **ドロッパー（183%増）**：ユーザーの気づかないうちに、コンピュータへ密かに他の悪意あるアプリケーションをインストールする脅威です。
- **トロイの木馬（177%増）**：画像や文書など正規の安全なファイルに見せかけてユーザーを騙し、実行させることでコンピュータを感染させます。
- **遠隔操作ツール等（114%増）**：感染したコンピュータへの長期的なアクセス権を確保し、サイバー犯罪者がデバイスを遠隔操作してユーザーを監視したり、コンピュータの機能を不正利用したりします。
- **情報搾取マルウェア（16%増）**：パスワードや銀行の認証情報、暗号資産のウォレットキーなど、機密情報を端末から盗み出します。

■新たな脅威の最前線：エージェント型AIへの攻撃

本レポートは、自律的に動作する「エージェント型AI」が新たなセキュリティの脅威となりつつあることも指摘しています。AIシステムがユーザーに代わってウェブを検索し、ソフトウェアをインストールし、様々なサービスと連携する能力を持つようになるにつれ、サイバー犯罪者はAIに与えられた「権限」そのものを標的にし始めています。 ノートンやアバストのAI

エージェント保護機能の基盤となっている、Genのプラットフォーム「Sage」の初期の調査によると、AIエージェントが関与する高リスクな振る舞いとして以下が確認されています。

- 危険なシステムコマンドの実行の試み
- サイバー犯罪者がシステムを制御できる可能性のあるリモートコマンド（遠隔操作）の経路を開こうとする試み
- インターネットからの不正なコードのダウンロードと実行
- 権限のない認証情報ファイルの読み取り
- 信頼されたキーの追加など、永続的なリモートアクセスの作成の試み
- エージェントへの指示を上書きしようとする試み

より詳細な情報については、レポート（英語）をご覧ください：

https://www.gendigital.com/blog/insights/reports/threat-report-h1-2026

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は、パソコン、スマートフォン、タブレットなどのデバイスを幅広いサイバー脅威から守る、オールインワンのセキュリティソフトです。AIを活用した「Scam Protection（詐欺対策機能）」により、オンライン上の詐欺だけでなく、テキストメッセージやディープフェイク動画などに潜む詐欺の検知をサポートします。

また、統合型AIアシスタント「Norton Genie」が、怪しいメッセージやオンライン上の情報についてリアルタイムでアドバイスを提供するほか、「Deepfake Protection（ディープフェイク対策）」などの機能を通じて、巧妙化するオンライン詐欺から利用者を守ります。

さらに、詐欺サイトやウイルスなどの脅威を検知・防御する機能、パスワードを安全に管理するパスワードマネージャー、通信を暗号化するVPNなども搭載し、オンライン上でより安全に過ごせる環境を提供します。

※製品やプランにより、利用できる機能が異なる場合があります。

■個人情報の流出を検知し、メールとアプリで通知、被害時に365日電話でサポート！

ノートン™ IDアドバイザー：https://jp.norton.com/products/identity-advisor

流出した個人情報は、ダークウェブ等で売買され、不正利用される可能性があります。ノートンはインターネットをパトロールし、お客様の個人情報が流出した場合、メールとアプリでお知らせします。また、SNSアカウントの乗っ取り、フィード内の危険なリンクや不適切コンテンツを警告します。個人情報の不正利用被害にあった場合は、365日復旧支援スペシャリスト(日本拠点）がトラブル解決をサポートします。関連機関と三者通話を行い、サポートさせていただく場合もございます。

*対象SNS等、機能の詳細はHPをご確認ください。

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です。Genの消費者向けブランドは、Genは消費者向けブランドとして、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、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。