

Press Release

【調査レポート】

アバストが一般家庭の通信ネットワークを悪用した サイバー攻撃を2,080万件ブロック

～「帯域幅の共有」アプリの危険性と、日本国内のユーザーが知っておくべきリスク～

Gen (NASDAQ: GEN) の消費者向けサイバーセーフティブランドであるアバストは、一般消費者の家庭用インターネット回線が、本人の気づかないうちにサイバー犯罪者の通信に悪用されている実態についての最新調査結果を発表しました。

Gen Threat Labs の調査によると、2026年1月から9月中旬にかけて、当社製品が Windows 上でレジデンシャルプロキシ（住宅用プロキシ）のトラフィックに関連する2,080万件ものサイバー攻撃を確認し、ブロックしました。

■ レジデンシャルプロキシとは

レジデンシャルプロキシとは、一般家庭向けのインターネット回線に接続されたパソコンやスマートフォン、IoT 機器（ルーター、ネットワークカメラなど）が、第三者の通信を中継する仕組みのことです。サイバー犯罪者は、自身の IP アドレス（インターネット上の住所のようなもの）を隠すために、パソコンやスマートフォン、IoT 機器を「踏み台」にして攻撃を行います。通信先のサーバーには踏み台となった機器の IP アドレスしか記録されず、攻撃元の特定が困難になるため、こうした悪用が増加しています。

■ 日本国内でも警視庁が注意喚起：あなたの家電も「踏み台」に？

現在、ユーザーが使用していないインターネットの帯域幅を共有することで、現金や特典、プレミアム機能などを提供すると謳うアプリが存在します。また、無料の VPN や海賊版ソフトウェアの裏で密かにインストールされるケースもあります。これらのアプリを介してユーザーのホームネットワークから出ていくトラフィックが、ユーザーの意図しないところで、悪意のある攻撃や不正行為に利用される危険性が高まっています。さらに、AI ツールによる大規模な Web の解析も、このレジデンシャルプロキシの需要を押し上げる大きな要因となっています。

日本国内においても、デバイスを悪用するレジデンシャルプロキシの脅威が高まっており、警視庁が注意喚起（※1）を行っています。警視庁によると、レジデンシャルプロキシ化される手口として、以下のような事例が確認されています。

1. プロキシ化ソフトウェアのインストール等によるもの

- プロキシ化マルウェア（不正なソフトウェア）やアプリ
- 収益をうたう通信帯域提供サービスやアプリ

2. IoT 機器自体に仕込まれたマルウェアによるもの

- 製造過程又は流過程で仕込まれたマルウェア
- IoT 機器の脆弱性等の原因から侵入され仕込まれたマルウェア

高いインターネット普及率を誇る日本市場においても、一般家庭の IP アドレスはサイバー犯罪者にとって非常に価値が高く、知らず知らずのうちに日本のユーザーの回線がサイバー攻撃の踏み台にされかねません

■ ブロックされた攻撃と脅威のデータ

Gen が2026年1月から9月中旬にかけてブロックした2,080万件の攻撃には、以下の脅威が含まれています。

- 最も一般的な脅威は「フィッシング」であり、515万件に上る。
- 次いで「悪意のある広告（マルバタイジング）」が126万件検出
- 「トロイの木馬」による攻撃も66万7,000件ブロック
- 攻撃がブロックされた件数の上位国は、インド、ブラジル、ベトナム、米国、フランス

■ 米国における意識調査：正しく理解している人はわずか8.8%

2026年7月に米国の成人1,000人を対象に実施された調査では、消費者の意識と実態の間に大きなギャップがあることが浮き彫りになりました。レジデンシャルプロキシの仕組みを正しく理解している回答者はわずか8.8%に留まりました。一方で、回答者の17.2%が「未使用の帯域幅を共有する代わりに報酬を提供するアプリ」を現在使用していると答えています。

このレジデンシャルプロキシの仕組み（第三者が自分のホームネットワーク経由でインターネットにアクセスすること）を説明された後では、76.5%の回答者が「懸念がある」と答えました。

■ 被害に遭っている可能性を示す兆候

これらのソフトウェアはバックグラウンドで静かに動作するため、多くの人は自分の回線が利用されていることに気づきません。以下の兆候がある場合、注意が必要です。

- 説明のつかない CAPTCHA（画像認証）が頻繁に表示される。
- WEB サイトから VPN を使用していないのに「VPN を使用しています」という警告プロンプトが出る。
- 明確な理由がないのに、ログインやセキュリティ確認でエラーになる。
- インターネットサービスプロバイダーから不正利用に関する通知が届く。
- 通信速度が低下する。

Gen（ノートン、アバスト等）は、日本の消費者の皆様に向け、安全なデジタルライフ（サイバーセーフティ）の実現をサポートするための継続的な啓発活動と技術提供を行ってまいります。

※1：家庭用 IoT 機器を悪用するレジデンシャルプロキシ

(<https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/notes/iot.html>)

アバストについて

アバストは、デジタルセキュリティとプライバシーのリーダーであり、信頼できる消費者向けブランドを通じてデジタルの自由の実現を目指すグローバル企業 Gen（NASDAQ: GEN）の一員です。アバストは、モバイル、PC、Mac 向けの製品・サービスを通じて、世界中の何億人ものユーザーをオンライン上の脅威から保護しています。

アバストの製品・サービスは、VB100、AV-Comparatives、AV-TEST、SE Labs などの第三者評価機関から高い評価や認証を受けています。また、アバストは Coalition Against Stalkerware、No More Ransom、Internet Watch Foundation のメンバーです。詳しくは、アバスト.com をご覧ください。