ノートン 広報部
2025年9月吉日

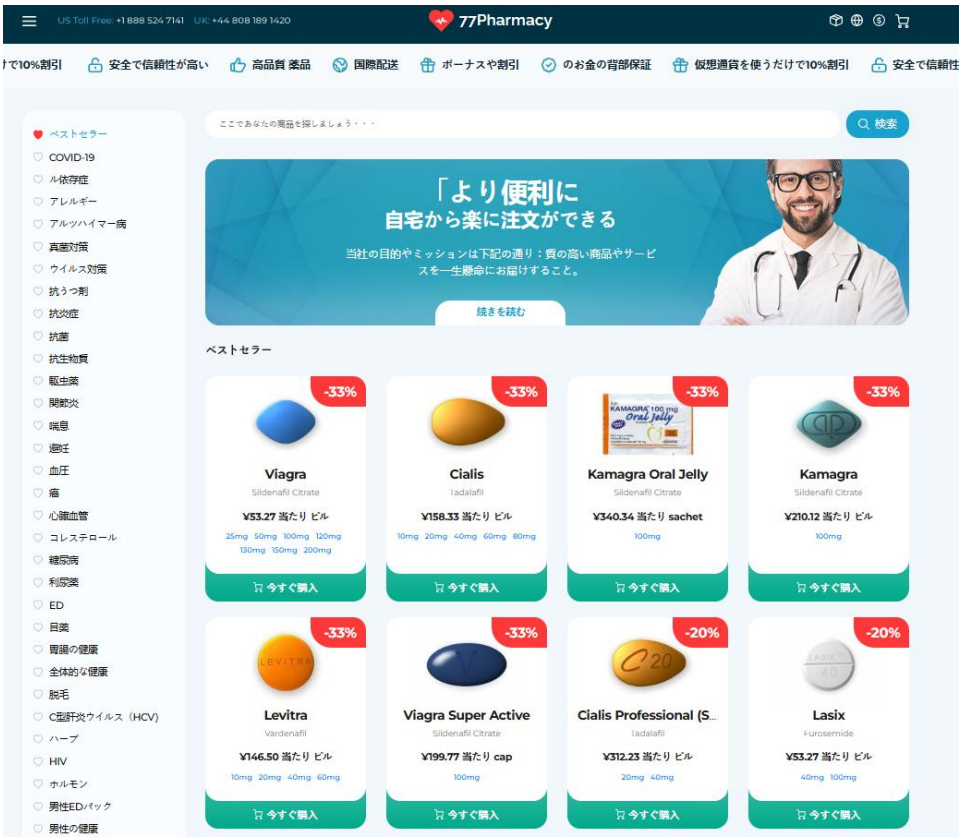
Press Release

サイバー攻撃の総数は減少するものの、AI を活用してより巧妙に進化

Gen「2025年第2四半期 脅威レポート」公開

世界で検出された偽オンライン薬局の実態を解明

ノートンやアバストなどのブランドを擁し、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、2025年第2四半期（2025年4月～6月）の「脅威レポート」を発表しました。



今回のレポートの大きなトピックスとしては、世界的に個人情報や金融情報を詐取するために処方薬を販売する5,000以上の偽オンライン薬局（通称 Pharma Fraud）の大規模ネットワークが明らかになりました。

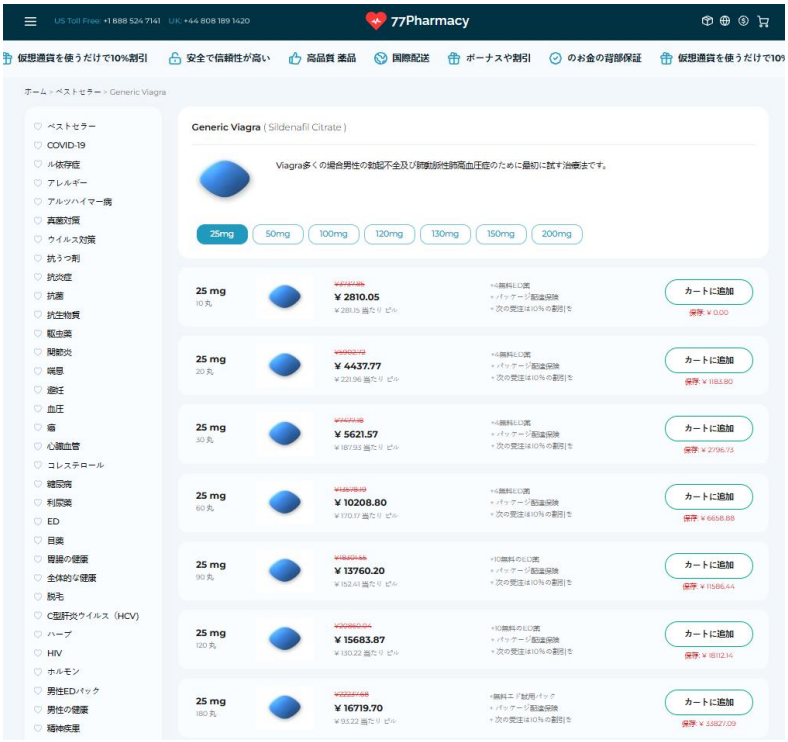
他にも今回のレポートにおける世界的な特徴は、AI を利用して開発された初のランサムウェアの摘発、データ侵害の21%増加、金融詐欺の340%増加などが挙げられます。さらに Gen のリサーチチームは、セクストーション詐欺（性的脅迫詐欺）の100%増加や、Facebook 上で拡大するテクニカルサポート詐欺の急増も確認しました。

日本では、前四半期と比較して詐欺のリスク比率が1.8%増加し、詐欺は依然として脅威のほぼ半数を占めています。デスクトップでは約半数、モバイルデバイスでは脅威の63%以上が詐欺であり、これは前四半期から29%以上の増加となっています。レポートの主なトピックは以下をご覧ください。

偽オンライン薬局：医薬品を装った巧妙な詐欺が発見

世界中でオンラインでの医薬品購入が一般化する中、サイバー犯罪者がこの新たな市場に目をつけています。抗生物質、人気の減量薬、ED 治療薬などを迅速かつ匿名で入手できる利便性の裏で、個人情報や金融情報を狙う詐欺が急増しています。Gen の研究者たちは、この偽オンライン薬局サイトによる詐欺を「PharmaFraud」と呼び、需要の高い抗生物質、減量薬、ED 治療薬などの薬を扱う5,000以上のドメインを含む大きなネットワークを特定しました。

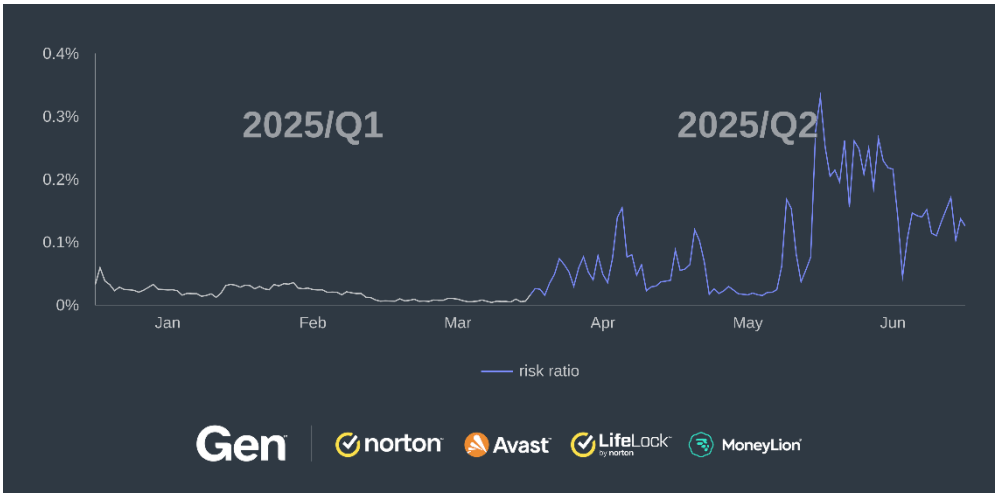
これらの偽オンライン薬局サイトはさまざまな手口を使ってアクセスを集めます。正規の医療系サイトにのコードを埋め込んだり、検索結果を操作したり、AI 生成の健康ブログや偽レビューサイトを活用したりします。見た目は本物らしく、整ったレイアウト、偽のカスタマーサポート、詳細な商品ページも備えています。しかし裏側では、不自然に安価な処方薬、連絡先情報の欠如、暗号通貨での支払い要求、セキュリティの欠如した決済プロセスに加えて、個人情報・医療情報・金融情報の入力を促す仕組みなど、多くの危険信号が潜んでいます。表面的に正規に見えても、実際は精巧に作られた詐欺サイトであり、金融詐欺や個人情報盗難を目的としています。



2025年上半期、日本は偽オンライン薬局詐欺のブロック件数で世界第6位となりました。

日本で増加傾向にある主要な詐欺脅威

2025年第2四半期、日本における詐欺脅威は全体的に拡大傾向を示しました。特に金融詐欺やテクニカルサポート詐欺が大幅に増加しており、セクストーション詐欺や偽ショッピングサイト詐欺についても引き続き確認されています。こうした動きは Facebook を中心とした SNS 上でも顕著で、Facebook 上でブロックされた脅威の14%がテクニカルサポート詐欺によるものでした。また、活動範囲は日本国内にとどまらず、ドイツ、オーストリア、フランスといった欧州地域にも広がりを見せています。



●セクストーション詐欺（性的脅迫詐欺：Sextortion Scam）
攻撃ブロック件数が22.77%増加。性的脅迫を利用した恐喝型の詐欺が拡大。

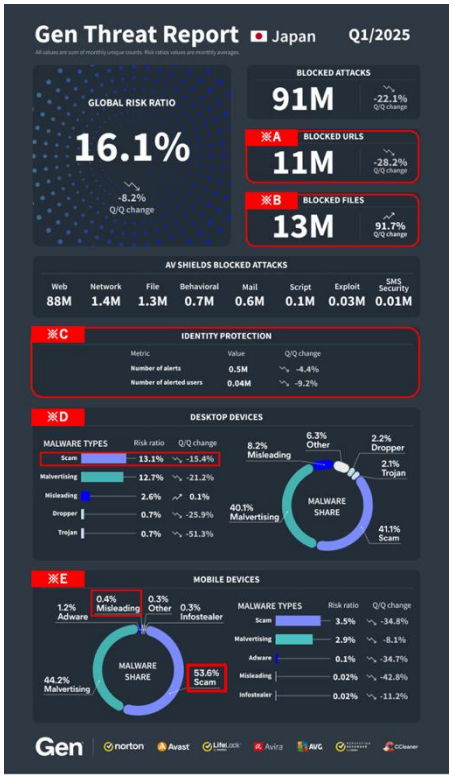
●偽ショッピングサイト詐欺（E-shop Scam）
攻撃ブロック件数が4.34%増加。比較的緩やかな伸びだが、依然としてオンライン購入者を狙った詐欺が継続。

●金融詐欺（Financial Scam）
攻撃ブロック件数が33.03%増加。今回の中で最も大幅な伸びを示し、投資や金融関連の偽装詐欺が顕著。

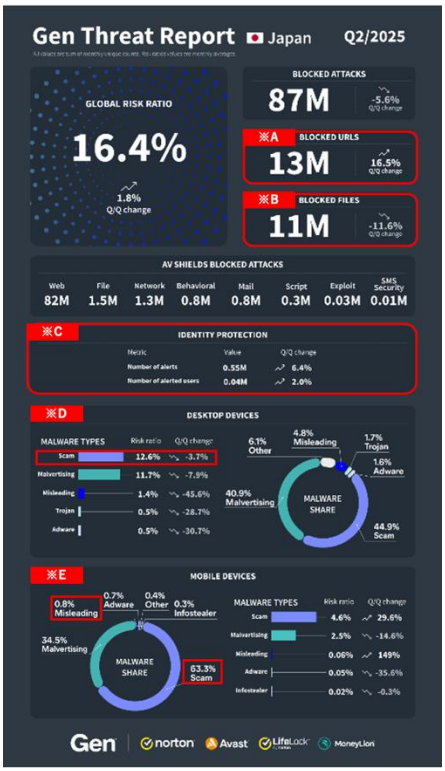
●テクニカルサポート詐欺（Tech Scam）
攻撃ブロック件数が30.24%増加。偽のサポート画面やヘルプデスクを装い、利用者をだます攻撃が急増。

日本における脅威の傾向｜前四半期比較

2025年第2四半期の日本における脅威情勢は、第1四半期と比較していくつかの顕著な変化が見られました。全体のリスク比率は上昇し、特にブロックされた URL 数が増加するなど、攻撃の入り口が多様化していることが示されています。一方で、ブロックされたファイル数は減少傾向にあり、検知される脅威の種類にも変化が表れています。詐欺関連の脅威が、デスクトップおよびモバイルの両方で増加傾向にある点も大きな特徴です。



△2025年第1四半期 結果



△2025年第2四半期 結果

●URL ブロック数の増加(※A)

第1四半期の 1,100万件 から、第2四半期には 1,300万件 に増加。前四半期より+16.5%の増加傾向が見られました。

●ファイルブロック数の減少(※B)

ブロックしたファイル数は 1,300万件（第1四半期）→1,100万件（第2四半期） と -11.6% 減少。第2四半期は、ファイルよりも URL からのブロック数が多いことがわかりました。

●個人情報の監視機能における通知件数が増加(※C)

確認した通知件数は 50万件（第1四半期）→ 55万件（第2四半期）と +6.4% 増加。個人情報の流出やアカウント不正利用の通知が含まれます。

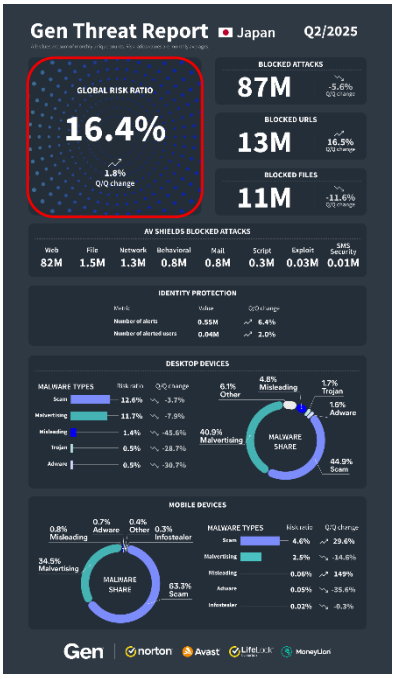
●デスクトップの主要脅威の順序は変わらず(※D)

デスクトップの脅威は、依然として「一般的な詐欺（Scam）」が主要な脅威であり、第1四半期の13.1%から第2四半期には12.6%へと減少しました。

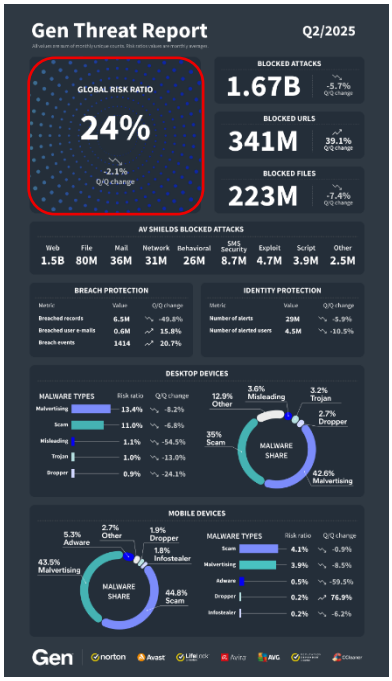
●モバイルの主要脅威は詐欺とセルフ詐欺が大幅に増加(※E)
モバイル環境でも、一般的な詐欺（Scam）が第1四半期の53.6%から、第2四半期には63.3%へと増加しました。ユーザーの身近なデバイスがより大きなリスクにさらされています。

日本とグローバルの結果比較

日本とグローバルそれぞれにて、下記図のような結果となりました。日本の全体リスク比率は 16.4%と、グローバルの 24% に比べて低いものの、世界的にリスク比率が減少している中で、日本は前四半期（16.1%）と比べて増加傾向であることがわかります。ブロックされた攻撃や URL のブロック件数など、主要な指標は世界全体のトレンドと概ね一致しています。日本市場はグローバルの動向を反映しつつも、特定の脅威分野で独自の特徴を見せています。



△日本のレポート



△グローバルレポート

●個人情報流出対策関連の統計は世界より増加傾向
個人情報保護に関する指標は、日本では世界と比べて増加傾向を示しています。ユーザーへの通知件数の増加は、個人情報流出やアカウント侵害のリスクが拡大していることを浮き彫りにしています。

●詐欺がマルバタイジングを上回る
デスクトップおよびモバイルの双方で、日本では一般的な 詐欺（Scam） が マルバタイジング（Malvertising） を上回りました。特にモバイルでは、セルフ詐欺（Scam-Yourself）を含む新たな傾向が顕著に確認されています。

●セルフ詐欺（Scam-yourself）について
ソーシャルエンジニアリングを用いて、ユーザー自身にマルウェアのインストールや情報漏洩を引き起こさせるサイバー攻撃の手法です。攻撃者は直接的に侵入するのではなく、被害者を巧妙に誘導し、自らの手でセキュリティを破らせることを目的としています。図の中ではミスリーディング（Misleading）として、ブロック数が計上されています。

●SNS 利用の裏に潜む脅威：YouTube が最多で61%

第2四半期の SNS 脅威分析によると、YouTube が全体の61%を占め、最もサイバー犯罪者に利用されている SNS プラットフォームであることが明らかになりました。次いで、Facebook が19%、X（旧 Twitter）が15%、その他５%という結果となりました。 また、SNS 上で確認された主な脅威として、偽ショッピングサイト詐欺、マルバタイジング、フィッシング詐欺、一般的な詐欺、テクニカルサポート詐欺、出会い系詐欺、金融詐欺などが挙げられており、ユーザーの安全を脅かすリスクが依然として存在しています。

●世界との比較：ドロッパーは例外的な動き

一方で、ドロッパー型マルウェア※1はこの傾向に追随せず、日本では大きな増加が見られませんでした。これは、日本市場特有のセキュリティ環境や利用状況が影響している可能性があります。

※1: ドロッパー型マルウェアとは：コンピュータにマルウェア（ウイルスやバックドアなど）をインストールするように設計されたトロイの木馬の一つである。Dropper 内のマルウェアは、ウイルス対策ソフトウェアによる検出を回避するようにパッケージ化されることがある。

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/inshts/reports/threat-report-q2-2025

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プレミアム：https://jp.norton.com/products/norton-360-premium

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 通信等をオールインワンで守るセキュリティソフトです。詐欺サイトやウイルスなどサイバー攻撃の脅威を検知し、防御する他、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機能、データ損失に対する予防的措置のクラウドバックアップ機能など、ユーザーの皆様がより快適かつ安全にインターネットが利用できるようになる機能を多数搭載しています。

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です。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。