

### Gen、2024 年第 4 四半期脅威レポートを発表

2024 年第 4 四半期では、世界で 25 億 5000 万件の脅威をブロック  
日本は変わらず世界で最もテクニカルサポート詐欺の標的とされている

デジタルセキュリティのグローバルリーダーである Gen は、2024 年第 4 四半期の Avast、Norton、AVG、Avira、LifeLock を含む多様なサイバーセキュリティブランドの脅威レポートを発表しました。

本レポートによると、第 4 四半期だけで世界で 25 億 5000 万件の脅威をブロックしました。（1 秒あたり 321 件の攻撃に相当）日本では、ランサムウェアが 3 四半期連続で増加傾向にあり、テクニカルサポート詐欺の件数については前四半期に引き続き世界で最も多い結果となりました。

レポートの主なトピックは以下をご覧ください。

#### ランサムウェアは世界的にも増加傾向

ランサムウェアは 3 四半期連続で増加傾向が続いており、2024 年第 4 四半期には 50% 増という結果になりました。これは、2024 年第 3 四半期 100% 増加、2024 年第 2 四半期の 24% 増加に続くものでした。Magniber は依然として最も流行しているランサムウェアで、マルウェアシェアの 62% にも上ります。



リスクが最も上昇したのは南米諸国で、コロンビア (+400%)、ウルグアイ (+400%)、ブラジル (+370%)、アルゼンチン (+300%)、ベネズエラ (+290%)、ペルー (+270%) となりました。そのほかにもメキシコ (230% 増)、オーストリア (100% 増)、フランス (100% 増)、カナダ (100% 増) となっており、日本も 180% リスクが上昇したことがわかりました。

＜本件に関するお問い合わせ先

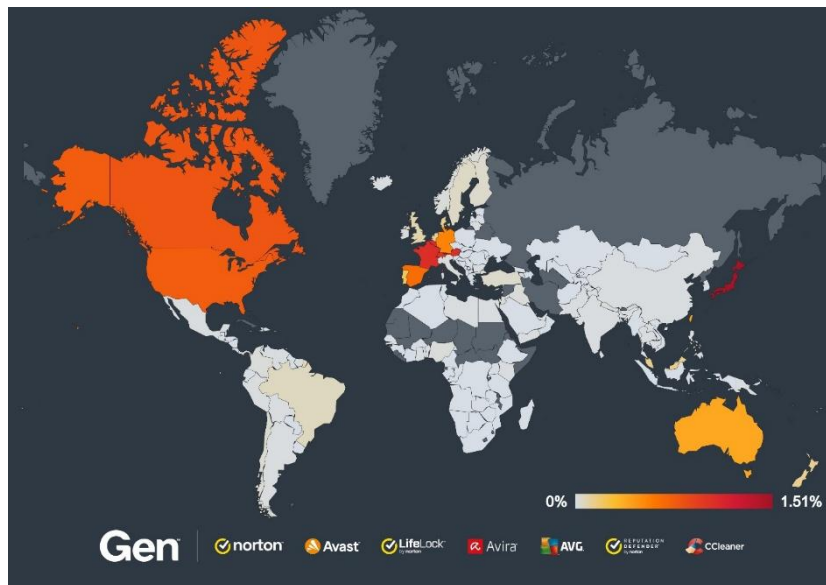
Gen PR 事務局（株式会社ブラチナム内）担当：石間、杉原、加藤、宮下  
TEL : 03-5572-6071 (PR 事務局) / Mail : norton-pr@vectorinc.co.jp

© Copyright 2025 Gen Digital Inc. All rights reserved.

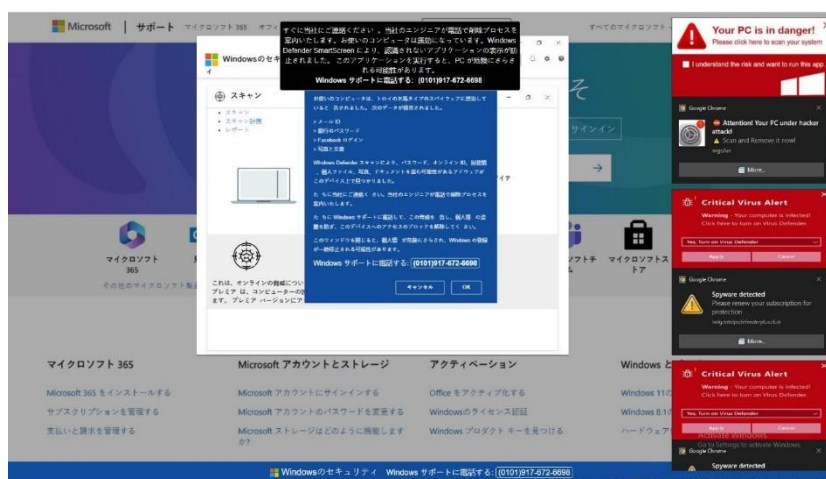
## テクニカルサポート詐欺は依然として日本が最もターゲットにされている

テクニカルサポート詐欺の脅威は、正規のテクニカルサポート担当者を装ったサイバー犯罪者が被害者のデバイスへのリモートアクセスを試みたり、クレジットカードや銀行口座の詳細情報などの機密性の高い個人情報を取得しようとしたりするものです。

スイスでは今四半期にテクニカルサポート詐欺が最も急増し、リスク比率は前期比 114%増の 1.05%となった。一方、日本では依然としてテクニカルサポート詐欺の標的として最も重要視されており、リスク比率は 1.51%で、前期比 14%増となりました。オーストリアも大幅な増加が見られた国で、同様に増加が見られました。リスク比率は 1.06%で、68%増となりました。同様に、香港は 43%増の 0.96%、カナダは 35%増の 0.80%でした。



全体として、日本は引き続きホットスポットであることに変わりはありません。一方で、スイス、オーストリア、香港、カナダ、フランスでの大幅な増加は、テクニカルサポート詐欺の脅威がより広範囲に拡大していることを示しています。



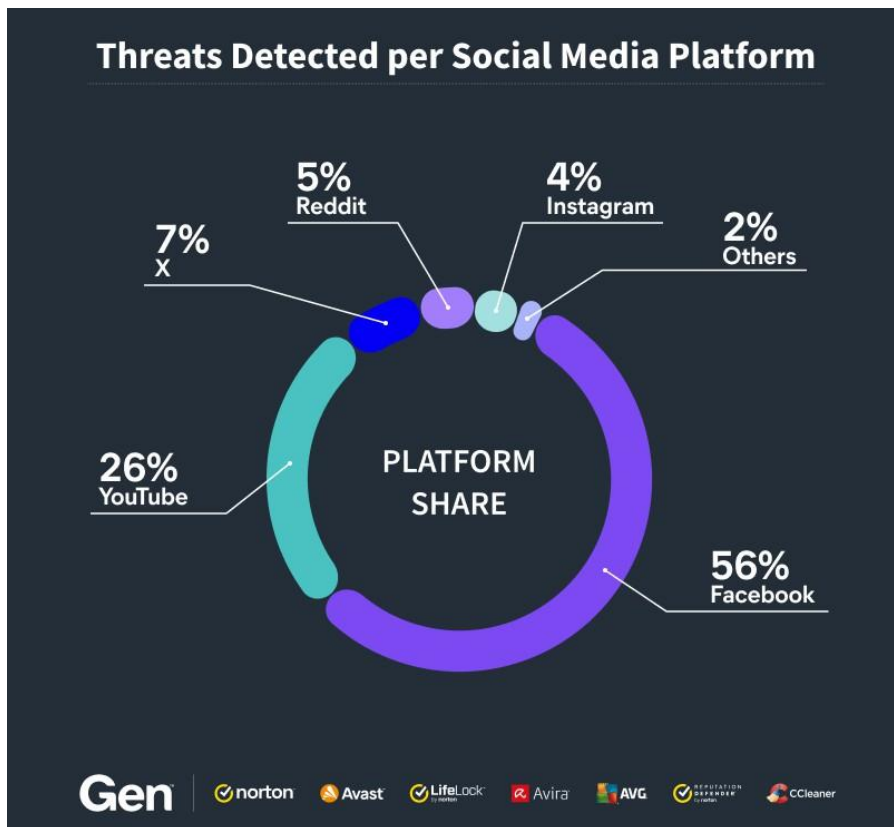
△日本のテクニカルサポート詐欺の画面

## ソーシャルメディアの脅威とその内訳

詐欺に関連する攻撃は、世界的な広がりや適応力が見られました。2024 年末時点でも、ソーシャルメディアプラットフォームは詐欺やサイバー犯罪の主な現場であり続けています。

ソーシャル・メディア・プラットフォーム全体で検出された脅威を分析すると、Facebook が全体の 56% を占め、圧倒的な存在感を示している。次いで YouTube が 26%、X が 7%、Reddit が 5%、Instagram が 4% となっていました。この分布は、ユーザーベースの規模、エンゲージメントパターン、プラットフォーム固有の特性により、一部のプラットフォームで不均衡なリスクをもたらしていることを浮き彫りにしています。

ソーシャルメディア上で人々を狙う脅威には、さまざまな手法があります



#### 1. マルバタイジング (26.95%)

サイバー犯罪者は、不正なオンライン広告を通じてマルウェアを拡散したり、ユーザーを悪意のあるウェブサイトにリダイレクトさせたりします。これらの広告は、多くの場合、あたかも本物のような広告を装って有害なコンテンツを配信したりします。

#### 2. EC サイト詐欺 (23.47%)

攻撃者は本物のように見える偽のオンラインショップを作り、ユーザーを騙します。被害者は、偽の商品を受け取ったり、商品が届かないことがあります。そのため、お金を失ったり、個人情報が漏れてしまう可能性があります。

#### 3. フィッシング (18.07%)

サイバー犯罪者は、偽のメッセージ、電子メール、ウェブサイトを使用して、クレジットカード番号、銀行情報、パスワードなどの機密情報を盗みます。これらは本来、あたかも信頼できる本物の連絡かのように見せかけて行われることがほとんどです。

#### 4. 金融詐欺 (10.68%)

サイバー犯罪者は人々を騙し、金銭や重要な金融情報を提供させます。よくある例としては、偽の投資や詐欺的な融資の申し出などがあります。

## 5.一般的な詐欺 (10.24%)

この大きなカテゴリには、サイバー犯罪者が被害者を騙して個人情報の共有や金銭の要求を目的とした詐欺が含まれます。

## 6.テクニカルサポート詐欺 (5.43%)

サイバー犯罪者が正規のテクニカルサポート担当者になりすまし、被害者のコンピューターやデータにアクセスする。これらの詐欺は通常、偽のエラーメッセージに対して助けを求める迷惑電話から始まります。

## 7.デート詐欺 (2.93%)

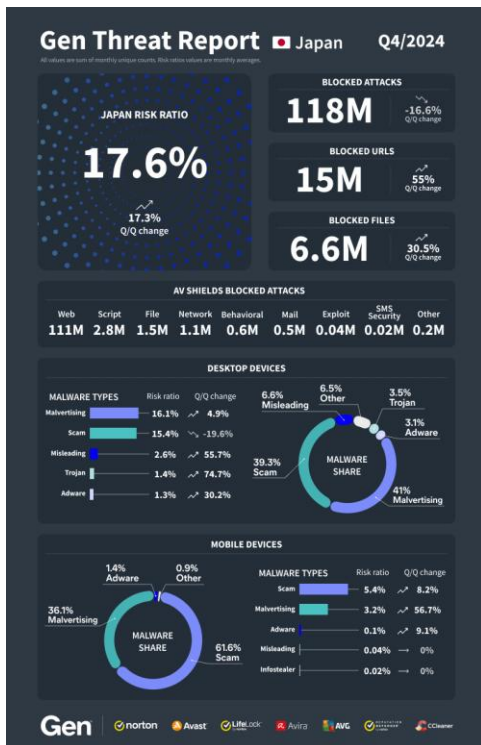
サイバー犯罪者が偽の恋愛関係を構築し、被害者を騙して金銭を送金させたり、偽のプロフィールを使って出会い系プラットフォームやソーシャルメディアで個人情報を共有させたりするのが一般的です。

## 8.その他 (2.24%)

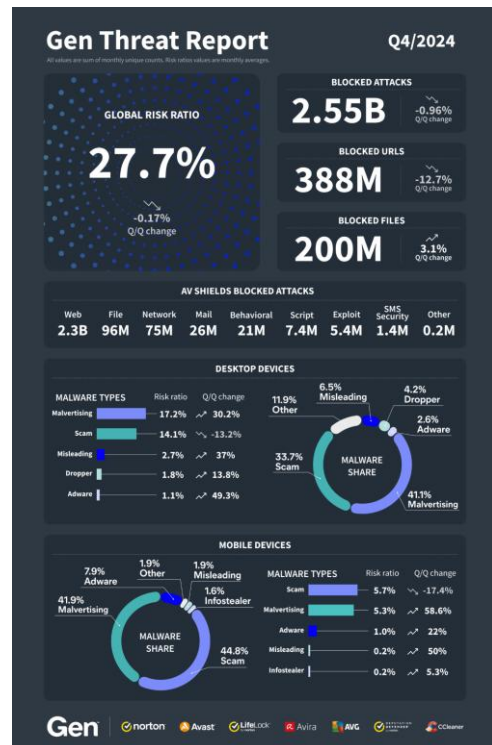
ソーシャルメディアを様々な方法で悪用する。あまり一般的ではないが、それでも重要な脅威の種類を集めたものです。

### 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。



△日本のレポート



△全世界のレポート

### <比較サマリー>

- ・全体的なブロックされた URL の件数は減少しているが、日本では増加傾向にある
- ・スクリプトシールドは、日本では依然としてセキュリティにおける重要な要素となっている
- ・マルウェアの傾向は、世界的な統計と同じである



- ・日本ではモバイルプラットフォームにおける詐欺が深刻な問題となっている

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/insights/reports/threat-report-q4-2024>

## Gen について

Gen™ (NASDAQ: GEN) は、信頼性の高いサイバーセキュリティブランドであるノートン、アバスト、ライフロック、Avira、AVG、ReputationDefender、CCleaner 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ファミリーは、デジタル世代の安全の確保を第一に考えています。現在、Gen は、人々が今日、そして将来にわたってデジタルライフを安全に、プライバシーを保護しながら、自信を持って送れるようサポートしています。Gen は、サイバーセキュリティ、オンラインプライバシー、ID 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](https://www.gendigital.com) をご覧ください。