Press Release

Avast PR 事務局
2025 年 4 月

SNS を活用した詐欺では、半数以上（56%）が Facebook

Avast が“SNS 詐欺の実態”についての調査結果を公開

SNS を活用した詐欺のうち、マルバタイジングは 27%も占めることが判明

デジタルセキュリティおよびプライバシー製品のグローバルリーダーで、Gen 傘下のアバストは、日本を含む 12 カ国の消費者を対象に「サイバーセキュリティに関する調査」[*1] を実施し、その結果の一部を公表いたします。

サイバー犯罪のトレンドとして、特に近年ではソーシャルメディアを通じた詐欺の急増が挙げられます。ソーシャルメディアには、動画共有プラットフォーム、メッセージングアプリなど、幅広いプラットフォームが含まれており、それらの普及とともに詐欺手法もますます巧妙かつ多様化しています。ま代表的な手法として、メッセージングアプリを使用してフィッシングリンクへの誘導、従来のソーシャルネットワークの偽プロフィールなどがあります。

さらに、人工知能（AI）の台頭により、犯罪手法もより巧妙になり、詐欺ということに気づきづらくなってきています。本レポートでは、最新の SNS 詐欺の実態と、消費者の皆様ができる対策について紹介いたします。

* 1：調査対象国（12 カ国）：日本、オーストラリア、ブラジル、チェコ共和国、フランス、ドイツ、香港、イタリア、メキシコ、ニュージーランド、イギリス、アメリカ

ソーシャルメディア詐欺の近年の変化

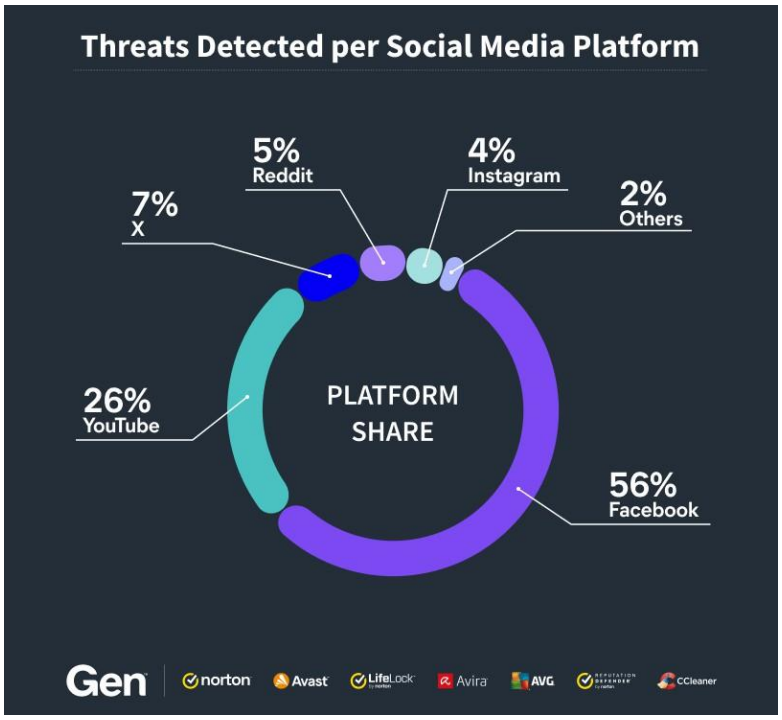
今日、サイバー犯罪の脅威はマルウェアだけにとどまらず、日々さまざまな形態の詐欺が発生しています。トロイの木馬やワームといった昔から有名な脅威は依然として存在していますが、これらがオンライン上のユーザーにおけるセキュリティ上の最大の懸念であった時代は終わりつつあります。最近の脅威は技術的な面だけでなく、人々の心理的な面にも働きかけるものが増え、より多くの注意と対策が必要になりつつあります。

特にその要因としては、人工知能（AI）の台頭があげられます。AI を搭載した詐欺ツールの普及により、サイバー犯罪者は、ディープフェイクビデオや音声合成、パーソナライズされたフィッシング・メッセージといった受け手が納得してしまうような内容や、人ごとにカスタマイズされた内容で詐欺を働きかけられるようになっています。さらに手法の増加だけでなく、AI を活用した詐欺手法は今まで以上に発見が難しくなっています。

そして今日のサイバー犯罪者にとって、格好の活動場所となっているのがソーシャルメディアです。ソーシャルメディアは従来のテキストと写真をかけ合わせたものから、動画共有プラットフォーム、メッセージングアプリなど、幅広いプラットフォームが増えています。各ソーシャルメディアは、利用者、コンテンツ、機能性の面で個別の特徴を持ち、こうした多様性がサイバー犯罪者にとって悪用される要因となっています。昨年では動画投稿が可能な TikTok での「イーロン・マスク詐欺」が話題となりました。この事件では、サイバー犯罪者たちがディープフェイク技術でイーロン・マスクになりすました動画を作成し、偽の暗号通貨をプレゼント、リターンが 2 倍になるから送金するように促した事件になります。多くの人が被害にあった背景としては、ディープフェイク動画のなりすましが巧妙だったことに加え、イーロン・マスク自体の影響力の高さ、若年層の TikTok の高い利用率が相まって、多くの被害が出たと考えられます。

ソーシャルメディアで脅威は Facebook が半数以上

ソーシャルメディア全体で検出された脅威を分析すると、フェイスブックが全体の 56.19%を占め、次いで YouTube が 25.92%、X、Reddit、Instagram がそれぞれ 6.91%、4.65%、3.79%ということが判明しました。各プラットフォームにはそれぞれ特性を利用したサイバー犯罪が存在しています。特に日本での利用の高い Facebook 、YouTube、X、Instagram の特徴とサイバー犯罪を以下でご紹介します。



<Facebook／偽オンラインショップ詐欺>
フェイスブックで最も蔓延しているサイバー犯罪は、偽オンラインショップ詐欺であり、偽の出品物を作ったり、売り手になりすましたりするもので、他のソーシャル・プラットフォームではあまり見られません。これは、以下のようなプラットフォームの特性によるものと考えられます

・フェイスブックのマーケットプレイスが商品の売買に広く利用されているため
・TikTok や Instagram のような、デジタルネイティブ向けのプラットフォームと対照的に、テクノロジーに疎く、詐欺に遭いやすい人々を含む、幅広い年齢層が利用しているため。
・フェイスブックでは、正規の EC サイトを忠実に再現したページ、グループ、プロフィールを作成することができ、本物のサイトと見分けるのが難しいため。
・フェイスブックがコミュニティ・グループや地域交流に重点を置いている特性から、特定の都市や地域をターゲットにした偽店舗など、地域密着型の詐欺が発生しやすいため

＜本件に関するお問い合わせ先＞
Avast PR 事務局（株式会社プラチナム内） 担当：石間、杉原、加藤、宮下
TEL：03-5572-6071（PR 事務局）／Mail：norton-pr@vectorinc.co.jp

＜YouTube／不正広告＞
YouTube では、不正広告が最も多い詐欺手法となっています。

・YouTube は広告収入に大きく依存しているプラットフォームであり、広告が一般なものとなっています。その状況下で視聴者に配信される広告に有害なリンクやマルウェアを埋め込むマルバタイジングが使用されています。

・YouTube の月間アクティブユーザー数は約 25 億人にのぼる大規模なプラットフォームであり、動画コンテンツ自体の特性としてユーザーを長時間留まらせることができるため、悪質な広告への接点を増加させる可能性があります。

・YouTube 広告は、ユーザーの興味、視聴履歴、デモグラフィックに基づいて高度にターゲティングすることができます。不正広告キャンペーンはこの機能を悪用して、有害な広告を特定の視聴者に向けて配信しています。

＜X＞
X では特定の手法に限らず多岐にわたる詐欺が見られます。その背景としては X がもつ下記のような特徴が関係しているからと予測されます。

・X は、厳格な本人確認なしに、手軽にアカウントを作成することができることから、サイバー犯罪者は、影響力のある個人やブランド、組織になりすました偽アカウントを作成しやすいため。

・信頼性の証明でもあった認証済みアカウントのバッジを、有料のサブスクリプションで入手することが可能になったことで、サイバー犯罪者が安全なアカウントを装うことが簡単になっているため。

・X のオープンなプラットフォームの特性から、サイバー犯罪者はツイート、リプライ、リツイートを通じて何百万人ものユーザーと直接アプローチすることができるためです。また X では注目されている人気のあるツイートに悪意のあるリンク埋め込んでリプライするといった手法も見られました

＜Instagram／偽のオンラインショップ詐欺＞
偽のオンラインショップ詐欺がインスタグラムでも多発しています。要因としては下記が考えられます

・Instagram はビジュアル重視のコンテンツが中心のため、サイバー犯罪者が偽の商品の魅力的な画像や動画を投稿することで、偽のオンラインショップに誘導しやすい特性があるからです。

・Instagram には、Instagram Shopping という機能があり、ストーリーズや投稿内のリンクを通じてオンラインショップへアクセスでき、サイバー犯罪者たちにこうした機能を悪用されるリスクが高まっています。

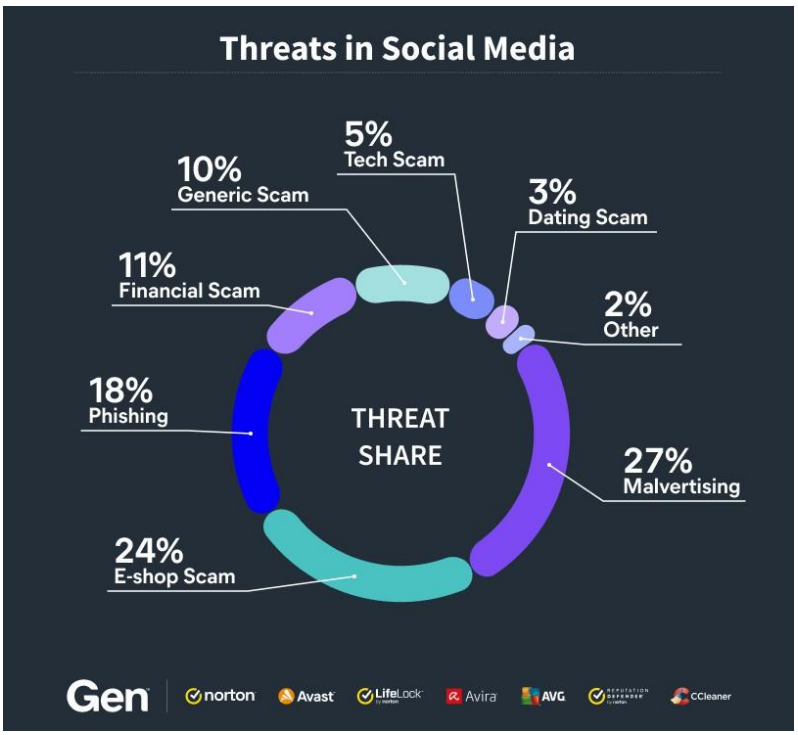
・企業を装ったアカウントを簡単に作成することができ、詐欺行為が行われやすい環境であるため

・Instagram の広告はターゲティングすることもでき、サイバー犯罪者がユーザーの興味関心や購買行動に基づいて特定の層にリーチすることができるため。

＜本件に関するお問い合わせ先＞
Avast PR 事務局（株式会社プラチナム内） 担当：石間、杉原、加藤、宮下
TEL：03-5572-6071（PR 事務局）／Mail：norton-pr@vectorinc.co.jp

ソーシャルメディア全体における詐欺はマルバタイジングが最多

ソーシャルメディア全体における、詐欺の種類としてはマルバタイジングが 27%と最も多いことがわかりました。さらに偽のオンラインショッピング詐欺も 24%と高く、フィッシング詐欺（18%）、投資詐欺（11%）と続きました。以下では最も多かった 3 つの詐欺手法について紹介します。



1.マルバタイジング（27%）：
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、悪質なウェブサイトへ誘導したりする詐欺。正規の広告のように見せることでユーザーの警戒心を下げ、有害なコンテンツを配信する詐欺手法。

2.偽のオンラインショップ詐欺（23%）：
サイバー犯罪者が偽のオンラインショップを作り、実際にはない商品を販売してユーザーを騙す詐欺です。
被害者は偽の商品が届いたり、商品が届かずにお金だけを失うだけでなく、さらには個人情報までも流出してしまう詐欺になります。

3.フィッシング詐欺（18%）：
サイバー犯罪者が実在する企業やサービスを装い、偽のメールや SMS を送り、偽のウェブサイトに誘導して、個人情報（ID、パスワード、クレジットカード情報など）を盗み取る詐欺。

＜本件に関するお問い合わせ先＞
Avast PR 事務局（株式会社プラチナム内） 担当：石間、杉原、加藤、宮下
TEL：03-5572-6071（PR 事務局）／Mail：norton-pr@vectorinc.co.jp

SNS 詐欺を防ぐにはどうすれば良いのか

SNS 詐欺はプラットフォームごとの特性や詐欺手法の多さがあるものの、以下のような基本的な対策を実施することで、未然に被害を防ぐ可能性が高まります。

■SNS 詐欺を防ぐための 5 つの対策

1. プライバシー設定の見直し
   └個人情報を守るための設定を行いましょう。
2. 怪しいリンクは絶対にクリックしない
   └フィッシング詐欺にかからないために、リンクをクリックしないことを徹底しましょう。
3. 送金を要求されたら疑う
   └送金を求めるものは典型的な詐欺のパターンのため、送金を求められたらまず疑いましょう、
4. 二段階認証の活用
   └アカウント乗っ取りを防ぐ方法として、二段階認証を設定することも重要です。
5. 最新のサイバーセキュリティ対策を学ぶ
   └SNS がサイバー犯罪者にとって格好の標的であることを理解し、合わせてセキュリティの知識つけることが重要です。

まとめと今後の展望

ソーシャルメディアは、交流だけでなく、取引、娯楽のためのプラットフォームへと進化しましたが、同時にサイバー犯罪者にとっては詐欺を行いやすい環境になりつつあります。今回の調査では各プラットフォームが持つ固有の機能と、季節的トレンドとの連動性が確認され、現代の詐欺手法が非常に高い適応性を持っていることが明らかになりました

今後、ソーシャルメディアにおけるサイバー犯罪は進化し続けると予想されるため、それに対抗するセキュリティも革新的かつ、適応力が求められてます。プラットフォームがより多くの機能を持ち、ユーザーがオンライン上でより多くの情報を共有するようになるほど、より機能性と安全性のバランスが重要になります。

安全にソーシャルメディアを使用するためにも、プラットフォームの提供者、それを利用するユーザー、そしてセキュリティの専門家が協力して、日々増加するデジタル上の脅威に対抗することが重要です。

Avast 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、信頼できる消費者ブランドで、デジタル化が進んだ世界においてもサイバー犯罪などの危険を心配せず、自由にデジタルを使いこなせる環境「デジタルフリーダム」の実現に力を注ぐグローバル企業の Gen（NASDAQ: GEN）のブランドです。アバストは数億人ものユーザーをインターネット上の脅威から守り、モバイル、PC、Mac 向けのセキュリティ製品は、著名な第三者機関である VB100、AV-Comparatives、AV-Test、SE Labs 等によって授賞を受けています。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 Avast.com をご覧ください。

<本件に関するお問い合わせ先>
Avast PR 事務局（株式会社プラチナム内） 担当：石間、杉原、加藤、宮下
TEL：03-5572-6071（PR 事務局）／Mail：norton-pr@vectorinc.co.jp