報道関係者各位

2025 年 2 月 28 日

NordVPN、偽装の危険性が高いサイトを調査！サイバー攻撃の最新の手口とは？

～日本はアジアで最もマルウェアの影響を受けた国であることが判明～

個人向けセキュリティサービスを提供する NordVPN（本社：オランダ・アムステルダム、日本代表：小原拓郎）は、無料動画サイトや偽装サイトに関するセキュリティリスクを分析した最新調査を発表しました。

■調査内容について

近年、無料動画ホスティングサイトの利用者が急増する一方で、これらのサイトがマルウェアやフィッシング攻撃の温床になっていることが懸念されています。NordVPN は 2024 年 1 月から 2025 年 1 月にかけて、Threat Protection Pro™を通じたサイバー脅威データを分析し、最も危険なウェブサイトの種類となりすまし被害の多いブランドを特定しました。
Threat Protection Pro™は、マルウェアのブロック、フィッシングサイトへのアクセス遮断、侵入型広告やトラッカーの防止などを行う NordVPN のセキュリティ機能です。
※NordVPN は、言及したブランドの所有者によって承認、管理、スポンサー提供されておらず、提携や関連性も一切ありません。ブランドは、マルウェアを拡散するためになりすまされる可能性が最も高いブランドに関連する情報を正確に報告する目的でのみ表示しています
本調査全文：https://nordvpn.com/ja/research-lab/online-threats-statistic/

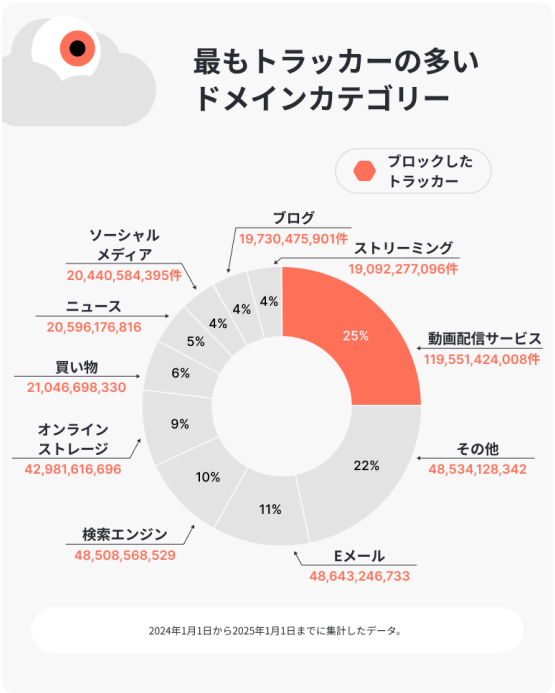
フィッシングの標的となったブランド

フィッシング詐欺の標的として最も多く利用されているのは、Google、Facebook、Microsoft の 3 大ブランドです。
特に Google は最多の偽装サイトが確認されており、その数は 85,000 件以上。Google アカウントの認証情報を盗むために、正規のログインページに似せた偽サイトが作られています。Facebook は約 6,000 件の偽サイトが確認され、ユーザーのアカウント情報や個人データを抜き取る手口が多発。Microsoft は約 5,000 件の偽サイトが発見され、特に企業向けアカウントの乗っ取りが狙われています。
その他、AT&T、Yahoo!、Netflix といったブランドも偽装の対象となっており、それぞれ約 4,000 件のフィッシングサイトが確認されています。

マルウェア感染リスクが高いサイトカテゴリ

マルウェア感染のリスクが最も高いのは無料動画サイトで、NordVPN の Threat Protection Pro™は 2024 年、15 億件以上のマルウェア感染をブロックしました。悪質な広告を通じて、閲覧するだけで感染するリスクがあります。
次いでエンターテインメントサイトが約 10 億件、スポーツ関連サイトが 1.2 億件、アダルトサイトが 1.09 億件と続きます。
ファイル共有サイトも 7,400 万件の感染が確認されており、特に違法ダウンロードを扱うサイトは注意が必要です。

特に無料動画サイトには、さまざまなセキュリティとプライバシーの脅威が含まれている傾向があります。マルウェアだけでなく、侵入的な広告やトラッカーも含まれます。過去 1 年間で Threat Protection Pro™は無料動画サイトだけで約 70 億の広告と 1,190 億を超えるトラッカーをブロックしました。これは、2024 年に Threat Protection Pro™によってブロックされたすべてのトラッカーの 25%に相当します。



日本は、アジアで最もマルウェアの影響を受けた国であり、合計で 106,139,174 件、1 デバイスあたり月間 1,315 件のマルウェア感染が確認されています。

■NordVPN のサイバーセキュリティ専門家であるエイドリアナス・ワルメンホーフェンのコメント

実際、フィッシング攻撃の大半は、約 300 のサイト名を使って詐欺を働きます。サイト自体に非はありません。こうした偽物はサイトの評判も傷つけるため、企業は対策を取らざる負えなくなります。しかし、サイトの認知度が高いと、被害者は誤った安心感を抱き、警戒を緩めてしまう可能性があります。特に無料の動画サイトには、さまざまなセキュリティとプライバシーの脅威が含まれている傾向があります。マルウェアだけでなく、侵入的な広告やトラッカーも含まれます。過去 1 年間で、Threat Protection Pro™は動画ホスティング サイトだけで約 70 億の広告と 1,190 億を超えるトラッカーをブロックしました。これは、2024 年に Threat Protection Pro™によってブロックされたすべてのトラッカーの 25%に相当します。

■サイバー攻撃の手口とリスク

サイバー犯罪者は巧妙な手口でユーザーを欺き、個人情報やデバイスを狙っています。正規のサービスを装ったフィッシング詐欺や、閲覧するだけで感染するマルウェア広告など、その手法は年々進化。一見安全そうなサイトやメールも、クリックひとつで被害につながる危険があります。代表的なサイバー攻撃の手口とリスクを紹介します。

フィッシング詐欺

偽装サイトに誘導して個人情報を盗み取る手口です。メールや SNS で「当選通知」や「特別オファー」を装い、ユーザーにリンクをクリックさせることで情報を収集します。

マルウェア感染

動画視聴やファイルダウンロード時にウイルスを仕込み、デバイスを乗っ取ります。特にランサムウェアによる攻撃では、重要なデータが暗号化され、身代金を要求される危険があります。

侵入型広告とトラッキング

強制的なポップアップ広告で悪質なサイトへ誘導し、マルウェア感染を引き起こすことがあります。また、トラッカーによりユーザー情報が収集され、第三者に販売されるリスクも高まります。

■安全なネット利用のための 5 つの対策

①無料動画サイトを避ける

マルウェアを仕込んだ広告が多く、閲覧するだけで感染のリスクがあります。

②不審なメールやリンクをクリックしない

「当選通知」や「アカウント確認」などの誘導はフィッシング詐欺の可能性大。送信元や URL を確認しましょう。

③ダウンロードは公式サイトから

非公式サイトのファイルはウイルス感染のリスクが高いため、必ず正規サイトを利用しましょう。特にサイトの URL の綴りは確認しましょう。

④個人情報の公開を最小限に

SNS での無防備な情報公開は危険。プライバシー設定を見直しましょう。

⑤OS やアプリを最新に保つ

古いソフトは攻撃の標的になります。定期的にアップデートを行いましょう。

■NordVPN について

NordVPN は、世界中で何百万人のユーザーをもつ先進的な VPN サービスプロバイダーです。7,000 台以上のサーバーを 111 カ国で提供し、専用 IP や Double VPN、Onion Over VPN サーバーなど、多彩な機能を備え、トラッキングなしでオンラインプライバシーを強化します。主要機能の一つである「脅威対策 Pro」は、悪質なウェブサイトやトラッカー、広告のブロックに加え、マルウェアのスキャンが可能です。さらに、最新の製品であるグローバル eSIM サービス「Saily」を展開しています。「Saily」は海外旅行者向けに設計されており、現地で SIM カードを購入する必要がなく、簡単にデータ通信が利用可能です。

【会社概要】

会社名：NordVPN
本社：Fred. Roeskestraat 115 1076 EE Amsterdam, Netherlands
日本代表：小原拓郎
NordVPN ウェブサイト：https://nordvpn.com/ja/
VPN について：https://nordvpn.com/ja/what-is-a-vpn/