報道関係者各位

2026 年 9 月 10 日

【NordVPN 2026 年上半期サイバー脅威レポート】
日本はマルウェア攻撃の検知件数で世界 10 位、26.8 万件
～生成 AI の普及で高度化するサイバー犯罪、「システムの脆弱性」から「人の信頼」を突く攻撃へ～

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、2026 年 1 月から 6 月までの脅威インテリジェンスデータを分析した初の消費者向けサイバーセキュリティレポート「Consumer Cybersecurity Report: Dismantling the Evolving Threat Landscape（消費者向けサイバーセキュリティレポート：変化するサイバー脅威の実態を読み解く）」を発表しました。
2026 年上半期、日本では 26.8 万件のマルウェア攻撃が確認され、国別で世界 10 位となりました。世界的にも、フィッシングや個人情報の流出など、消費者を取り巻くさまざまなサイバー脅威が確認されています。本レポートでは、上半期に観測されたデータの中から、特に消費者への影響が大きい脅威や、新たに見られた攻撃手法の変化を取り上げています。

■ 身近なブランドへの「信頼」を悪用、フィッシングの 99%が 300 ブランドへのなりすまし

NordVPN は、2026 年上半期に 440 万件を超えるフィッシング接続をブロックしました。そのうち 99%が、わずか 300 ブランドへのなりすましだったことが確認されています。ブランド別では、Microsoft へのなりすましが 16.12%と最も高く、Roblox が 12.32%、Google が 9.94%、Netflix が 5.99%と続きました。
攻撃者は、利用者が普段から目にしている企業やサービスへの信頼を悪用します。今回の結果は、フィッシングが「知らない相手」から届く不審な連絡だけではなく、日常的に利用するブランドを装うことで、認証情報や個人情報を入力させる手口として広がっていることを示しています。

■ 氏名や住所などの流出情報を組み合わせ、より個人を狙った攻撃へ

NordVPN のダークウェブモニタリングツールでは、わずか 90 日間で 840 万件の情報漏えいが確認されたアカウントが見つかりました。2026 年上半期には、流出データの確認件数が前月比 33%増加しており、サイバー犯罪の産業化に伴って流出データの規模も拡大しています。

さらに、流通しているデータの 47%以上に住所と氏名が含まれていました。攻撃者がデジタル上の認証情報と現実世界の個人を特定できる情報を組み合わせることで、被害者についてより詳細なプロフィールを構築し、個人に合わせた攻撃に悪用する可能性があります。

このほか、2026 年 1 月から 5 月には 940 億件の Cookie がオンライン上に流出し、そのうち 12 億件は、パスワードを使わずにアカウントを乗っ取るために悪用される可能性のあるセッション Cookie でした。

■ 生成 AI で「違和感から見抜く」ことが困難に、詐欺の参入障壁も低下

本レポートが示す 2026 年の大きな変化は、サイバー犯罪の手口が、大量配信型で粗い攻撃から、より精巧で標的を絞った攻撃へと移行していることです。生成 AI の進歩により、自然な文章などのコンテンツを短時間で作成できるようになり、従来の検知方法だけでは、その生成スピードや品質に対応することが難しくなっています。

さらに、すぐに利用できる詐欺キットや制限の少ない AI モデルの登場によって、高度な専門知識や大きな資金を持たない攻撃者でも詐欺を仕掛けやすくなっています。NordVPN は、こうした変化によって、技術的な脆弱性だけでなく、緊急性、焦り、身近なブランドへの信頼といった人の心理そのものが、攻撃に利用されるようになっていると指摘しています。

■ 日本も例外ではなく、マルウェア攻撃 26.8 万件で世界 10 位

マルウェアは、今回のレポートで確認された脅威の中でも件数が最も多いカテゴリーです。2026 年 1 月には、NordVPN が 500 万件を超えるマルウェア攻撃をブロックしました。国別では、米国が 489 万件超、英国が 200 万件超。日本は 26.8 万件で 10 位となっています。

中でも、端末に保存されたパスワードや Cookie、クレジットカード情報などを盗み出す「インフォスティーラー」は、引き続き主要な脅威となっています。NordVPN は 1 日あたり 1,200 万件を超えるユニーク URL を処理し、月間では約 3 億 6,000 万件の異なるウェブアドレスを分析しており、悪意のあるページへのアクセスを 1 日平均約 13 万件ブロックしています。

※インフォスティーラー：パスワードや Cookie など、端末内の個人情報を盗み出すことを目的としたマルウェア。

■ NordVPN 最高技術責任者（CTO） マリユス・ブリエディスのコメント

「悪意のある攻撃者は、私たちが目にしたものや耳にしたものを信じようとする、人間の自然な心理を武器にしています。こうした攻撃には、もはや高度な技術や大きなリソースは必要ありません。インターネット接続さえあれば、誰でも仕掛けられる状況になっています。たった一度の人的ミスでも、以前より深刻な被害につながる可能性が高まっています。」

■ 「見た目」ではなく「確認方法」を変える、生活者が意識したい 5 つの対策

1. 緊急性をあおるメッセージほど、すぐに行動しない

「今すぐ確認」「アカウント停止」「返金期限」など、急いで対応するよう求める連絡を受け取った場合は、その場でリンクを開かず、公式アプリや公式サイトから情報を確認してください。

2. 送信元の名前だけで信用しない

実在する企業やサービス名が表示されていても、送信元アドレスや URL を確認し、不審なドメインや表記の違いがないか確認してください。

3. パスワードの使い回しを避け、多要素認証を利用する

サービスごとに異なるパスワードを設定し、利用可能な場合は多要素認証を有効にすることで、認証情報が流出した際の被害拡大を抑えられます。

4. OS、ブラウザ、アプリを最新の状態に保つ

セキュリティ更新を適用し、不要な拡張機能やアプリを整理することで、マルウェアや情報窃取型攻撃の侵入口を減らしてください。

5. 不審なサイトや流出情報を検知するセキュリティ機能を活用する

悪意のあるウェブサイトやマルウェアを検知する機能、ダークウェブ上で認証情報の流出を確認できる機能などを活用し、異常を早期に把握してください。

■ 調査概要

NordVPN の専門家が、2026 年 1 月から 6 月までの社内セキュリティシグナルを分析し、関連する外部の脅威インテリジェンス情報と比較しました。すべての分析は集計されたデータを用いて実施され、個々のユーザーを特定できる情報は使用していません。

■ NordVPN について

NordVPN は、世界中で何百万人ものインターネットユーザーに利用されている、デジタルプライバシーとセキュリティのためのオールインワンアプリです。NordVPN アプリは、世界最高水準の VPN、次世代アンチウイルス、Dark Web Monitor™をはじめとするセキュリティ機能を統合し、ユーザーがオンライン上でより安全かつプライベートに過ごせるようサポートします。また、フィッシング、詐欺、悪質なウェブサイト、トラッカー、迷惑広告、マルウェアなどの脅威からユーザーを保護し、オンラインプライバシーの強化にも貢献します。詳細は nordvpn.com をご覧ください。

【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/