報道関係者各位

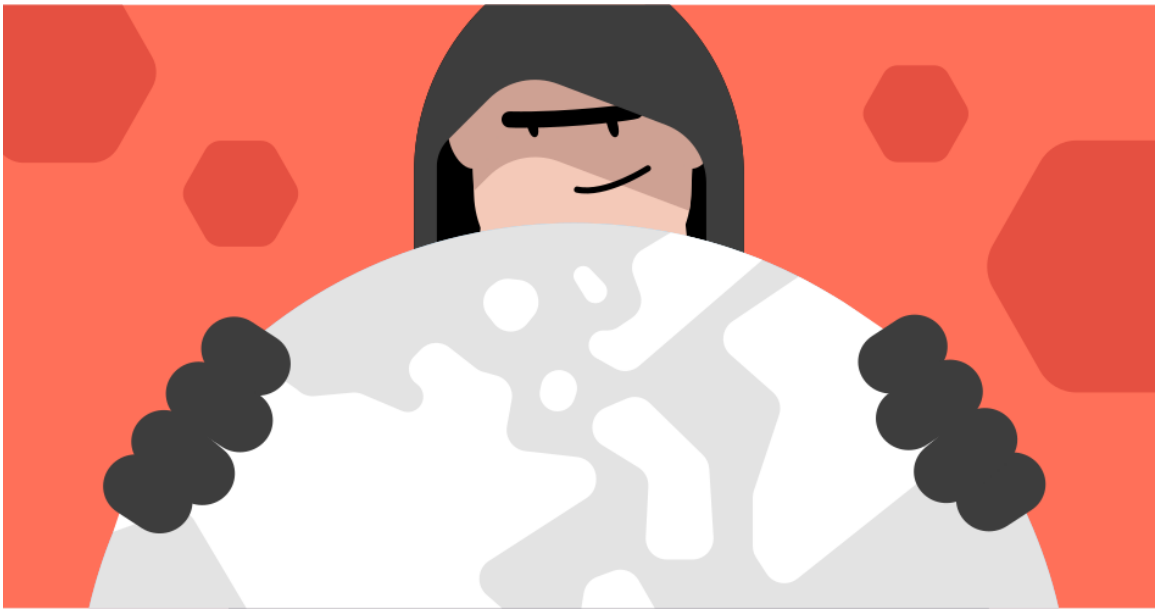
2025 年 12 月 9 日

NordVPN、2026 年のサイバーセキュリティ脅威予測を発表

～専門家が指摘する一般ユーザーを狙う 5 つの新興サイバー脅威～

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 年に予想される主要なサイバーセキュリティリスクについて発表しました。人工知能(AI)を悪用した攻撃手法や量子コンピューター技術の進展により、サイバー犯罪は新たな段階に入ろうとしています。

デジタルサービスやスマートデバイスへの依存度が高まる中、一般ユーザーが直面する脅威は規模・複雑性ともに拡大しています。NordVPN の専門家が指摘する 5 つの新興脅威を解説します。



2026 年における 5 つの主要なサイバーセキュリティリスク

1. インターネット・モノカルチャーのリスク

現在、世界中の多くの人が同じサービスを利用しています。クラウドサービスなら AWS、オフィスソフトなら Google や Microsoft Office といったように、特定の大手企業のサービスに集中している状態です。この「インターネットの単一化（モノカルチャー）」は、便利である一方で重大なリスクをもたらしています。

一つのサービスに障害が発生すると、そのサービスを利用している数百万人のユーザーが一斉に影響を受け、インターネット全体の回復力を低下させる可能性があります。

さらに、このモノカルチャー化はハッキングの収益性を大幅に向上させています。犯罪者にとって、単一のプラットフォーム上にいる数百万人のユーザーを一度に攻撃できることは、一人当たりの利益が小さくても、トータルでは大きな収入源となります。かつて、企業や個人がバラバラのシステムを使っていた時代には、攻撃者は標的ごとに異なる手法を用意する必要がありコストがかかりましたが、現在はその必要がなくなっているのです。

2. SNS 上で増加する誤情報―セキュリティ軽視を煽る組織的な動き

2025 年を通じて、SNS や掲示板などのオンラインプラットフォームにおいて、パスワードを複雑にすることや二段階認証などのセキュリティ対策を「やりすぎ」「意味がない」と嘲笑する投稿が目立つようになりました。

この傾向は 2026 年にさらに加速すると予想され、多くの人のオンライン安全とプライバシーに深刻な影響を及ぼします。

実は、この背景には犯罪組織の存在があります。一部の犯罪組織は正規の企業以上に組織化されており、ユーザーを無防備な状態に保つことを目的とした専門のマーケティング部門を持っています。潤沢な資金力を背景に、人気インフルエンサーを買収したり、一から育成したりして、「セキュリティ対策なんて面倒なだけ」「このアプリは安全だから大丈夫」といった、安全性の低い習慣や製品を宣伝させる動きが強まっています。

3. 1,500 円で誰もが買える「Evil GPT(悪の ChatGPT)」―AI 悪用時代の到来

サイバー犯罪者はすでに、人間がほとんど介入しなくても自動的にネットワークを調査し、弱点を見つけ出し、攻撃を仕掛ける「自律型 AI」の実験をしています。これらのシステムは自ら学習・改良・適応することができ、攻撃のスピードが速くなり、予測も困難になります。

さらに、「Evil GPT(悪の ChatGPT)」と呼ばれる攻撃用 AI モデルが、ダークウェブでわずか約 1,500 円で誰でも購入できる状況です。

「パスワードを忘れた」「クレジットカード番号は…」などの情報を何気なく入力していませんか？ChatGPT などの AI ツールは、会話の履歴をブラウザ内に保存することが多く、パスワードやクレジットカード番号といった機密情報を入力すると、情報を盗み取るマルウェア（悪意のあるソフトウェア）に狙われる危険性があります。

4. 信頼の崩壊―ディープフェイクと合成 ID による「なりすまし」の巧妙化

2026 年、最大のセキュリティ課題は「何も信じられなくなる」ことだと予想されています。ディープフェイク（AI による偽造コンテンツ）、音声クローニング（声の複製）、精巧な偽のプロフィール、自動化されたフィッシングメッセージ、そして個人情報を悪用した超個別化攻撃により、本物と偽物の境界線が完全に曖昧になります。

犯罪者は、実在する人物の情報と架空の情報を巧みに組み合わせ、実在しない「合成 ID」を作り出します。この偽の ID を使って、クラウドサービスのアカウントを乗っ取ったり、銀行口座を開設したり、ローンを組んだりすることが可能になり、何年も発覚せずに犯罪を続けられます。AI を駆使した詐欺は犯罪者の効率を飛躍的に高め、偽のウェブサイトや詐欺サービスを見分けることが極めて困難になります。

5. 現実味を帯びる量子コンピューター攻撃

量子コンピューターとは、従来のコンピューターとは桁違いの計算能力を持つ次世代技術です。この技術の発展により、現在「絶対に安全」とされている暗号化技術が、いとも簡単に解読されてしまう時代が近づいています。大規模な量子攻撃の実現はまだ数年先ですが、サイバー犯罪者はすでに「今のうちに盗んでおき、量子コンピューターが実用化されたら解読する」という作戦を実行中です。つまり、数年前にやり取りした暗号化メール、保存した機密ファイル、オンラインバンキングの記録などが、将来突然解読され、第三者に閲覧される可能性があるのです。

量子技術による復号化が現実になれば、数十年分の個人情報が一気に露呈する恐れがあります。企業や個人にとって、量子コンピューター時代への備えは、もはや「いつか考えるべきこと」ではなく、「今すぐ取り組むべき課題」となっています。

■ NordVPN サイバーセキュリティ専門家 アドリアナス・ワーメンホーフェンのコメント

「現在のデジタルエコシステムはモノカルチャー化が進み、オンライン上のあらゆる個人が潜在的な標的となっています。DNS レコード（ウェブサイト閲覧時に残る “アクセス履歴などの情報”）のような一見取るに足らないデータでさえ、売買・集約・悪用されるリスクが存在します。

2026 年には、AI を活用した攻撃と防御の高度化が続き、サイバー犯罪の敷居が下がる一方で、熟練した攻撃者の能力がさらに強化されると見込まれています。また、量子コンピューティング市場は 50 億ドル規模へ成長する予測があり、その商用化の進展に伴い、サイバーセキュリティは各産業でより重要なテーマとなります。加えて、物理世界とデジタル世界の境界が曖昧になる中、サイバーセキュリティは技術課題を超え、社会全体の課題へと拡大しています。これまでデジタル教育はデバイスの使い方といったリテラシーに重点が置かれてきましたが、今後は日常的な“デジタルハイジーン（デジタル衛生習慣）”の定着がより重要になります。これらの動向は、2026 年に向けて世界のサイバーセキュリティ環境が大きく変化することを示しています。」

■ NordVPN について

NordVPN は、世界中で何百万人も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。8,200 台以上のサーバーを世界 127 カ国 165 都市で提供し、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/