

トップ VPN に選出された個人向けセキュリティ会社 NordVPN 2025 年最新のサイバーセキュリティリスクの動向予測を発表

～来年増加する可能性がある 5 つのサイバー脅威とは～

個人向けセキュリティサービスを展開する NordVPN(本社: Amsterdam, Netherlands、日本代表: 小原拓郎)は、2025 年のサイバーセキュリティ予測を発表しました。NordVPN は自社が運営する情報漏えい管理プラットフォーム NordStellar Analytics を活用し、詐欺情報が横行する大規模なダークウェブフォーラムを分析しました。話題となっている最新のトピックを調査し、2025 年に増加すると予測される 5 つのサイバー脅威や脆弱性を発表しました。



当社は、毎年 12 月に、NordStellar Analytics を活用して翌年のサイバーセキュリティリスクの動向に関する予測を発表しています。今年は調査した結果、2025 年サイバーリスクとして予測される 5 つの脅威や脆弱性が明らかになりました。

2025 年サイバーリスクとして予測される 5 つの脅威や脆弱性

① アカウントの乗っ取り被害が拡大

ダークウェブ上で多く議論されているスレッドには、2024 年 1 月 1 日～11 月 1 日までに、135,000 件を超えるインターネット上で流出したユーザー名やパスワード、個人情報などを一覧化したリストである「コンボリスト」に関するコメントがありました。また、このデータを悪用した「アカウントの乗っ取り」に言及したコメントが、26,000 件近く寄せられています。近年では、複数のサイトで同じパスワードを使い回すことが一般的になっていることから、ハッカーにアカウント情報を盗まれることで、詐欺の被害を受けたり、アカウントの不正利用が行われたりするだけでなく、個人情報盗まれるリスクも大幅に高まっています。

② スマートホームシステムに関連するセキュリティの悪用が増加

ダークウェブ上で、スマートホームシステムやアプリケーションのセキュリティの脆弱性に焦点を当てたコメントは、約 21,000 件寄せられており、脆弱性を突いた具体的な詐欺手順もダークウェブ上に記載されています。2024 年の IoT [セキュリティラウンドスケープレポート](#)の約 5,000 万件の IoT デバイスの調査によると、世界中で 91 億件を超えるセキュリティに関するトラブルが起きていることが明らかになりました。平均すると、ホームネットワークではネットワークに接続されたデバイスに対して、毎日 10 件を超えるサイバー攻撃が発生していることがわかります。この数は 2025 年も増加することが予想されます。

③ 個人情報の盗難

詐欺に関するトピックは、ダークウェブ上でコメント数の多いスレッドのトップ 10 にランクインするほど話題となっているトピックであり、詐欺を実行させるためのヒント、ツール、そして戦略が共有されています。クレジットカード詐欺や保険金詐欺については、頻繁に会話されていますが、ハッカーにとって、個人情報の盗難は高い収益性から、依然として注目度が高くなっています。実際に個人情報の盗難については、約 13,000 件のコメントがあり、詐欺に関するトピックの中では、最も議論されているものになります。今後も、ハッカーが個人情報を悪用して、銀行口座に不正ログインすることやクレジットカード情報を盗むこと、脱税を行うことなど、個人情報の盗難手法はますます巧妙化することが予想されます。

④ 偽情報がサービスとして拡散

[グローバルエコノミックフォーラムの 2024 年グローバルリスク報告書](#)によると、AI が生成した偽情報は、今後 2 年間で 2 番目に深刻な世界的リスク(53%)として選ばれており、異常気象がトップ、サイバー攻撃が 5 番目に選出されています。ダークウェブ上には、SNS アカウントやプロパガンダを広めるための多数のスパムメールが使用されているなど、偽情報を広めるための手法が複数紹介されています。また、偽情報を大規模に拡散するための偽情報ボットファームが開発されています。

⑤ AI によるソーシャルエンジニアリングの高度化

AI を活用したソーシャル エンジニアリングは、今後さらに高度化することが予想されます。ソーシャルエンジニアリングとは、マルウェアなどを用いずにパスワードなどの情報を盗む手法です。このトピックは広く議論されているわけではありませんが、ダークウェブ上には、この手法を活用する方法やチュートリアル、実例が飛び交っています。重要なトレンドとして、システムの脆弱性の検出に AI を使用するというものがあります。また、情報収集のために人間の行動を真似て、効果的なフィッシングメールを作成するように設計されたツールが登場するなど、システムの複雑さが増しています。

NordVPN のサイバーセキュリティ専門家としてオランダ初のサイバー犯罪対策組織設立の経験もある、エイドリアナス・ワルメンホーフ氏コメント

「パスワードの使い回しがなくなる限り、サイバー攻撃はハッカーの間で続くことが予測されます。個人情報の盗難は進化しており、来年には新たな手法が出現すると予想します。その一つである流出した個人情報を使って架空の身元(アイデンティティ)を作る合成 ID 詐欺は、その精度を高めるために、AI を用いて人物の動画や音声を人工的に合成するディープフェイク技術が組み込まれることがよくあります。その他にも、進化している手法として、なりすまし詐欺があります。これは、個人が他人の個人情報を金銭的利益のためではなく、日常生活でその人になりすますために行われるもので、就職の優遇、保険適用、法的責任の回避などを目的としています。これらの戦略は、目先の金銭的利益よりも長期的な目的で行われています。

また、現在のダークウェブの傾向を振り返ると、来年は偽情報を提供するサービスが脅威として浮上することが予想できます。サイバー犯罪者は、偽情報の作成と拡散から利益を得ています。自由にカスタマイズ可能で適応性が高いサービスは、人口統計やプロフィールを正確にターゲットにし、SNS のアルゴリズムを操作して影響を最大化します。さらに、新たな個人情報の流出によって、ハッカーに認証情報が提供されるため、2025 年は、こうした活動が増加することが予測されます。さらに、詐欺師が企業を騙して、あらゆる理由を付けて返金や代替品をもらう『企業への詐欺と搾取』と呼ばれる脅威に注意が必要です。ダークウェブ上には、Amazon、ASOS、Walmart などの大企業をターゲットにして、これらの計画を上手く実行するために、企業を分析する方法が提供されています。」と説明します。

■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。6,400 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、最新製品グローバル eSIM サービス「Saily」を展開しています。

【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/>