報道関係者各位

2026 年 1 月 6 日

～ 2026 年を「AI リスク認識元年」へ ～
マルウェア検知 2.3 億件超、日本が「アジア・ワースト 1 位」の標的
AI 悪用で顕在化する新たな脅威

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、自社のセキュリティ機能「脅威対策 Pro™」で検知されたデータの分析をもとに、AI 技術の悪用によって個人を狙うサイバー脅威が新たな局面に入っている実態を明らかにしました。本リリースでは、年初という節目にあたり、AI を巡る代表的な脅威の傾向を整理し、注意すべきポイントを解説します。

■ 法律改正の推進と個人の意識のギャップ

日本は昨年、サイバーセキュリティ政策において大きな変革が起き、2025 年 7 月には内閣府に「国家サイバー統括室」が新設されました。法制度においても攻撃サーバーへの無害化措置等を含む「能動的サイバー防御」へと改正され、サイバーセキュリティの「国家の壁」が厚くなりました。

一方、個人ユーザーレベルでは、AI の利用が急速に広がる一方で、そのリスクに対する認識が十分に追いついていない状況が続いています。実際、日本人を対象とした調査でも、生成 AI の利用経験が広がる一方で、個人情報の取り扱いやセキュリティリスクを十分に意識しないまま利用している実態が指摘されています。こうしたギャップを背景に、情報漏洩やそれに伴う詐欺被害は拡大を続けています。

アメリカ連邦取引委員会（FTC）のデータによると、個人の資産を狙う詐欺による被害総額は、2024 年に 57 億ドル（約 8,500 億円）規模に達しました。AI によって「本物そっくりの投資サイト」が大量に生成されたり、チャットボットへの信頼を逆手に取った情報窃取が行われたりするなど、AI 悪用による詐欺手口は進化を続けています。

さらに、NordVPN が 2024 年 1 月から 2025 年 9 月にかけて集計したデータによると、日本国内でブロックされたマルウェアの総数は 232,077,563 件に達し、アジア地域で突出して多い結果となりました。AI によって自動化・巧妙化された攻撃が、すでに日本の個人ユーザーの身近な環境にまで及んでいることを示しています。NordVPN は、こうした個人のリスク認識と実際の被害状況とのギャップが、被害拡大の一因になり得ると考え、AI を起点とする代表的な脅威を以下の 3 つに整理しました。

■ NordVPN が特定した、特に注意すべき 3 つの主要な AI 脅威

脅威① AI に預けた情報や前提が裏切られるリスク

AI の利用が広がる中、AI に信頼して預けた情報や、無害であると前提されていた条件が、想定外の形で侵害されるリスクが指摘されています。これらのリスクは、大きく 3 つの形で確認されています。

会話データが守られないケース

AI との会話はデジタル記録として保存されます。過去には、AI の共有機能に関する欠陥により、本来は非公開であるはずの会話記録や機密情報が、第三者から閲覧可能な状態となっていた事例が報告されました。信頼して打ち明けた内容が、想定とは異なる形で外部に露出する可能性があります。

機能を通じて情報が取得されるケース

会話内容に限らず、サービスの機能を起点として情報が扱われるリスクも存在します。カレンダーへの招待機能に関連する脆弱性を悪用し、攻撃者が会議のリクエストを通じてユーザーデータを不正に取得できる可能性があることも報道されました。利用者が特定の情報を共有した認識がなくても情報が扱われる可能性がある点には注意が必要です。

「無害な前提」を突く新たな攻撃（LegalPwn）

近年では、「LegalPwn（リーガルポーン）」と呼ばれる攻撃手法も確認されています。これはユーザーがサービスを利用する際に同意する利用規約やプライバシーポリシなど、AI が一般的に無害と判断する法的な文章を利用し、AI の判断を誤らせる手法です。こうした文章のなかに、意図的に AI への指示が自然な形で含まれることによって、従来の AI コード解析やセキュリティチェックをすり抜けることができます。危険なマルウェアを「安全」と誤認させてしまう可能性があり、その結果、AI への相談内容が本来想定されていない第三者に閲覧されたり、悪意ある操作に利用されたりするリスクが生じます。

これらの事例は、AI に預けた会話内容、利用機能を通じて扱われる情報、そして無害であると前提されていた判断条件のいずれもが、攻撃の起点となり得ることを示しています。

脅威② AI が生み出す「本物らしさ」を悪用した詐欺の拡大 “8 ヶ月で 450 万件の偽サイトを確認”

AI 技術の進化により、「本物そっくりの投資サイト」や「著名人のなりすまし広告」の作成コストが低下し、サイバー攻撃の規模が拡大しています。また、デザインや文章の精度が高く、見た目や表現だけで真偽を判断することは困難になっています。

NordVPN「脅威対策 Pro™」は 2025 年 3 月から 10 月の 8 ヶ月間で、詐欺の疑いのある偽サイトを 450 万件以上ブロックしました。ハッカーは、AI を使って信頼性の高い大手 EC サイトや金融機関を模倣したサイトを量産するだけでなく、知人や家族の声を模倣する「ディープフェイク音声」を用いた詐欺も確認されています。これにより、「本人の声だから」「公式サイトのように見えるから」といった直感的な判断が通用しなくなっています。

このように、AI が生み出す高い再現性と説得力によって、利用者の警戒心をすり抜ける詐欺が拡大しています。見た目や雰囲気が「本物らしい」こと自体は、もはや安全性の判断材料にはなりません。

脅威③ AI の回答そのものは「正しい」とは限らない

AI は、質問に対して自然で説得力のある回答を返しますが、その内容が必ずしも正確であるとは限りません。実在しない情報を事実のように生成してしまうことがあり、この現象は「AI ハルシネーション（幻覚）」と呼ばれています。こうした特性が新たな攻撃手法に悪用されています。

近年確認されている「スロップスクワッティング」と呼ばれる手法では、AI が誤って提示しそうな実在しない URL や架空のソフトウェア名を攻撃者が予測し、あらかじめ偽サイトやマルウェアを用意します。利用者が AI の回答を信じてリンクにアクセスしたり、推奨されたソフトウェアをダウンロードしたりすると、正規のサービスを利用しているつもりでも、実際には攻撃者の用意したサイトに誘導されてしまう可能性があります。有名ブランド名に似せた URL も多く、違和感に気づくことは容易ではありません。

このように、AI の回答であること自体が信頼の根拠になってしまう状況が、新たなリスクを生んでいます。AI の「おすすめ」や「回答」を無条件に正しいものとして受け取ることは、利用者自身が攻撃の入口に近づくことにつながります。

■ NordVPN 最高技術責任者（CTO） マリユス・ブリエディスが推奨する、AI リスクから身を守る 4 つの対策

① AI 利用における「情報の非秘匿性」を認識する
AI システム自体が安全であっても、会話ログの取り扱いやアクセス範囲が常に利用者側から明確に見えるとは限りません。クレジットカード番号や機密情報は入力しないようにし、AI との会話は「第三者に共有される可能性のある情報」として扱う意識を持つことが大切です。入力ボタンを押す前に、「これが世界中に公開されても問題ないか？」と自問する習慣をつけましょう。

② 業務とプライベートのアカウント利用を厳格に分離する
個人用と業務用の AI アカウントは可能な限り使い分け、チャット履歴を定期的に削除することをお勧めします。システム上に保存されるデータを最小限に留めることで、万が一のアカウント侵害やデータ流出時のリスクを抑えることができます。

③ AI 生成情報の真偽確認を徹底する
AI が提示した URL やソフトウェア名については、わずかなスペルミスやドメインの違いにも注意を払いましょう。特にソフトウェアをダウンロードする際は、AI の回答にあるリンクをそのまま使用せず、必ず検索エンジンなどで公式サイトや一次情報を確認し、正規のルートから入手するように心がけましょう。

④ セキュリティツールによる多層的な防衛策を講じる
人による確認には限界があります。「脅威対策 Pro™」のような、悪意あるウェブサイトやトラッカーを自動で検知、ブロックするツールの活用も有効です。あわせて、多要素認証（MFA）や ID 監視アラートを有効にすることで、不正アクセスやデータ侵害の兆候を早期に察知し、被害を未然に防ぐことが期待できます。

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

「AI ツールが急速に普及した背景には、多くの人がそれを『自分だけのパーソナルアシスタント』のように感じ、無防備に信頼しているという実態があります。しかし、日本がアジア最大の標的となっている現状において、その『安心感』こそが脆弱性になり得ます。だからこそ、AI は便利な存在である一方で、『攻撃の入り口にもなり得る』という認識を持つことが重要です。AI や有名ブランドを騙る攻撃を常に疑う『ゼロトラスト』の姿勢は、皆様の大切な資産を守るうえで、有効な防御策となるでしょう。」

■ 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/