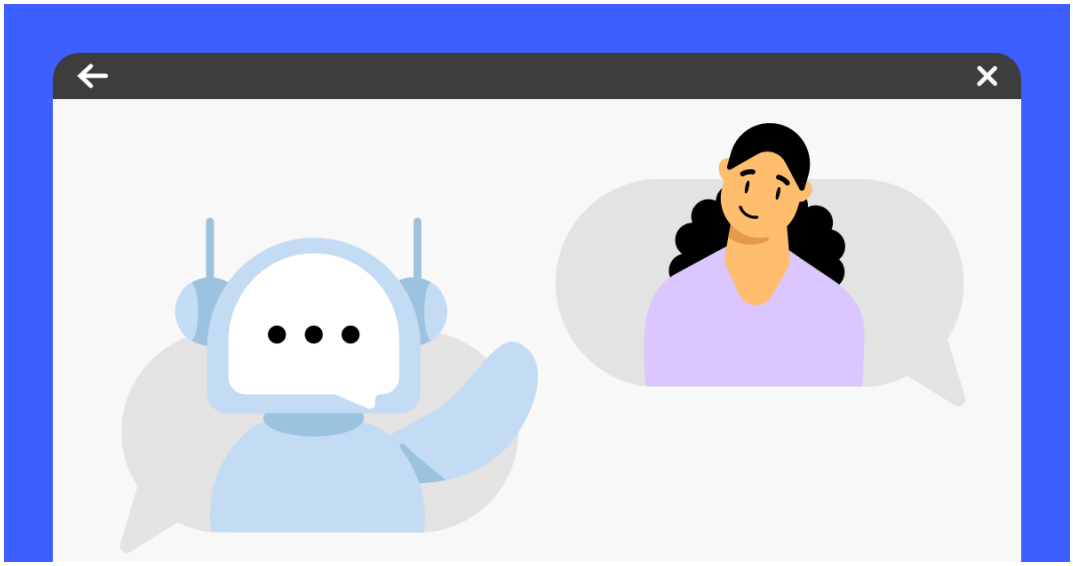
報道関係者各位

2025 年 8 月 6 日

9 割の日本人が「生成 AI のリスク」を正しく理解していない？！
NordVPN が「AI への相談」が引き起こす無意識な情報漏洩を調査！

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、生成 AI の利用とプライバシー意識に関する調査を実施しました。また、生成 AI を安全に利用するための 3 つの対策をご紹介します。



調査背景

世界の約 10%、およそ 8 億人が ChatGPT などの生成 AI を利用しています。日々生成 AI にオンラインプライバシーの保護や安全なデジタルライフに関する相談がされていますが、多くのユーザーが自覚のないまま個人情報を開示している実態があります。

本調査では、AI に寄せる最も一般的かつ時に「奇妙な」サイバーセキュリティに関する質問を掘り下げるとともに、利用者が無意識のうちに公開してしまう情報についても詳しく調査しました。

調査概要

NordVPN は、500 人以上の日本人を対象に生成 AI のセキュリティ意識について、調査しました。

調査期間：2024 年 1 月 1 日～12 月 31 日

調査人数：526 人

調査対象：全国のインターネットユーザー

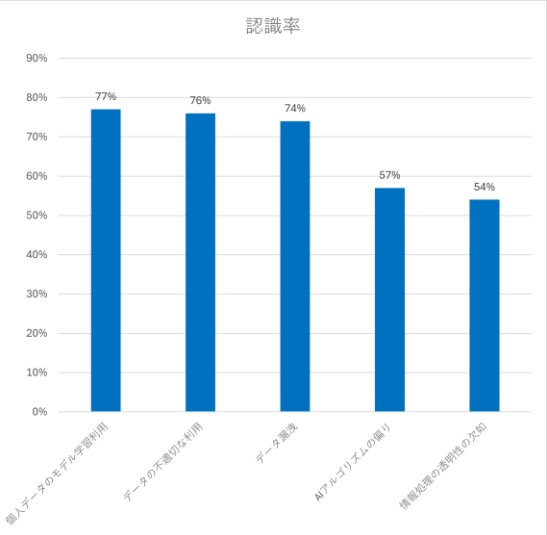
調査機関：NordVPN

■ 日本における「理解しているつもり」のリスク

日本国内で実施された調査では、「業務で AI を活用する際のプライバシーリスクを正しく理解している」と回答した人はわずか 10%にとどまりました。しかし、個別のリスク項目に関しては比較的高い認識率が見られ、たとえば「個人データが AI の学習に利用されるリスク」は 77%、「提供データの不適切な利用」は 76%、「データ漏洩の可能性」は 74%の人が把握していると回答しました。

また、「AI アルゴリズムの偏り」や「情報処理の透明性の欠如」についても、それぞれ 57%、54%と一定の理解が示されています。

この結果から、ユーザーの間ではリスクの存在自体は認知されているものの、「どのように対応すべきか」についての理解が追いついておらず、認識と行動のギャップが明らかになりました。



■ChatGPT が「情報漏洩の相談窓口」に？

世界中で約 8 億人が利用している ChatGPT などの AI ツール。日々多くのユーザーが「セキュリティの相談相手」として頼りにしていますが、本調査によると、多くのユーザーが個人情報を含む内容をそのまま入力している実態があります。

・位置情報：地域のおすすめ検索やトラブルシューティングの際に、都市名、住所、GPS 座標などを共有することがあります。

・SNS のプロフィール：アカウントの安全性について相談する際、プロフィールリンクやユーザー名を貼り付けるケースもあります。

そのほかにも氏名や連絡先、金融情報、アカウントログイン情報などがあり、様々なサポートを求める中で、ユーザー名、パスワード、二段階認証コードなどを不本意に開示してしまうことがあります。一見、無害に見える質問であっても、これらの情報が AI のログに残ることでサイバー犯罪の標的となるリスクが生じます。

■ AI に寄せられた「本気」のセキュリティ質問

NordVPN は、日本国内の ChatGPT ユーザーによるセキュリティ関連の質問を独自に分析しました。その結果、AI に最も多く寄せられていたのは、フィッシング詐欺の見分け方やスミッシング（SMS 詐欺）への対処法、公共 Wi-Fi の安全性、LINE アカウントのハッキング対策、スマートフォン向けのウイルス対策ソフトの選び方など、実用的で日常生活に密着した不安や疑問でした。

さらに、VPN の合法性と安全性、マルウェア感染の確認方法、オンラインバンキング利用時のセキュリティ対策、パスワード管理の最善策、オンラインショッピング時の安全性なども頻繁に相談されていました。これらの傾向から、日本でも生成 AI が「デジタル生活の相談窓口」として活用されている実態が見えてきます。

こうした相談内容からは、ユーザーの関心がセキュリティ対策に向いていることがわかります。一方で、AI に質問することで生じる「情報開示リスク」への理解は、まだ十分とは言えず、課題として浮き彫りになっています。

■ NordVPN 最高技術責任者マリユス・ブリエディスが推奨する、AI 活用が進む中で最低限実践すべき 3 つの対策

① 個人情報を含んだまま質問しない

生成 AI はあくまで外部サービスであり、入力された内容が学習や記録の対象となる可能性があります。直接的または推測可能な個人情報は入力しないように注意しましょう。質問文の中に、意図せず自分の情報や取引先の情報が含まれていないかを、送信前に一度見直す習慣をつけることが大切です。

② AI ツールの「学習利用オフ」設定を活用する

多くの生成 AI ツールは、入力された情報を今後のサービス改善や学習モデルに活用する場合があります。「チャット履歴が保存されることを前提に使う」という意識を持ち、機密性の高い相談は避け、学習利用をオフにしましょう。

③ VPN を使って通信内容自体を暗号化する（第三者からの傍受を防止）
AI ツールへのアクセス時に、公共 Wi-Fi やセキュリティが不十分なネットワークを利用すると、通信内容が第三者に傍受されるリスクが高まります。こうしたリスクを回避するために、VPN を活用し、通信経路を暗号化することが有効です。VPN を使用することで、自身の IP アドレスや位置情報も保護されるため、より安全な状態で AI ツールを活用できます。

■NordVPN 最高技術責任者 マリユス・ブリエディスのコメント
「AI は利便性の高いツールである一方で、ユーザー側の理解が不十分な場合、「相談そのものが新たなリスク」になりかねません。どのような情報を AI に提供しているのかを意識することは、今後のデジタル社会において不可欠なセキュリティ対策の一つです。安全な活用のためには、AI とのやり取りにおいても、プライバシー保護の視点を常に持つことが求められます。」

■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。7,600 台以上のサーバーを 118 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/