報道関係者各位

2025 年 10 月 8 日

セキュリティに自信があるビジネスパーソンの約 7 割が実は危険な行動

NordVPN が“無意識な行動に潜むセキュリティリスク”を調査

～知識はあっても実践できない？ セキュリティ行動のギャップが顕在化～

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、全国のビジネスパーソン 1,000 名を対象に「ビジネスパーソンの無意識な行動に潜むセキュリティリスクに関する調査」を実施しました。

本調査は、IT 専門職以外の 20～60 代のビジネスパーソンで、直近 1 年に業務で PC を利用している方を対象としています。今回は、ビジネスパーソンの日常に潜む“無意識のセキュリティリスク”に着目。誰もがつい行いがちなセキュリティリスクが潜む 8 つの行動シーン（生成 AI の利用、公共 Wi-Fi の利用、自宅 Wi-Fi ルーターのセキュリティ非設定、ブラウザの自動保存利用、個人クラウドへ業務データの保存、二要素認証（2FA/MFA）非設定、フィッシングメール、OS やアプリの未更新）を取り上げ、それぞれについて 「リスクを自覚しているかどうか」と「実際の行動傾向（1～5 段階で自己評価）」 を調査しました。

さらに、年齢・残業時間・職種といった属性ごとの傾向も分析。その結果、特定のシーンにおける行動だけでなく、属性によっても“認識と行動のギャップ”に大きな差があることが明らかになりました。

【エグゼクティブサマリ】

●属性別

・ビジネスパーソンの半数（47.1%）が“無意識のセキュリティリスク”にさらされており、セキュリティに自信がある層の約 7 割が危険な行動を取っていることが判明

・年代別では、20 代のフィッシングメールによるリスク行動が 17.0%と、全体平均（10.2%）の約 1.7 倍に達し、他世代と比べても突出

・残業時間別では、月間 40 時間以上の残業層が公共 Wi-Fi で機密資料を扱う割合が 13.0%に上り、全体平均（5.7%）の約 2.3 倍と高水準

・職種別では、「企画・マーケティング職」の生成 AI の利用リスクが全体の約 2.2 倍、
「人事・労務職」では公共 Wi-Fi の利用やブラウザの自動保存機能など複数のリスクが平均を大きく上回る結果に

●セキュリティリスクが潜む 8 つの行動シーン

・調査全体を通じて「セキュリティの知識があっても実践できない」というギャップが顕在化。無意識のうちに利便性を優先してしまうことが、リスク行動に繋がっていることが判明

・公共 Wi-Fi の利用（40.9%）、自宅 Wi-Fi ルーターの初期設定放置（43.7%）、ブラウザの自動保存利用（54.4%）が、主要なリスク要因として浮き彫りに

・一方で、フィッシングメールによる情報漏洩（10.2%）や OS やアプリの未更新（13.0%）は、他のリスク行動に比べて低水準

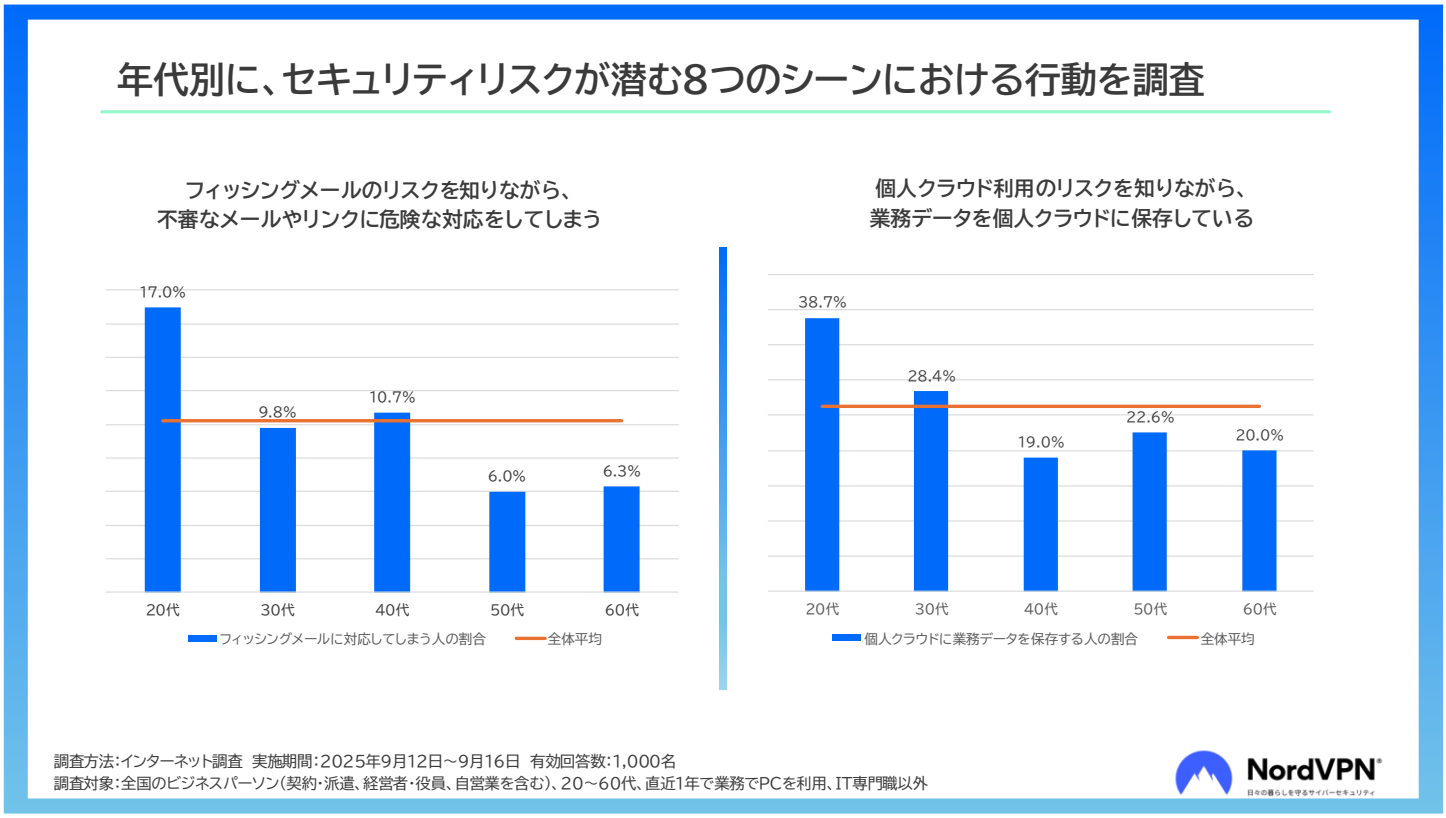
●属性別

今回の調査では、ビジネスパーソンの半数（47.1%）が“無意識のセキュリティリスク”にさらされており、セキュリティに自信がある層の約 7 割が危険な行動を取っていることが判明しました。

【Topic1：20 代、30 代は全般的にセキュリティリスクが高く、特に 20 代のフィッシングメールに対するリスクは平均の 1.7 倍】

調査の結果、20 代、30 代は全般的に無意識のセキュリティリスク行動が高い傾向が見られました。中でも、フィッシングメールに対するセキュリティリスクについて知っていると答えた 20 代のうち、リスク行動を取っている人は 17.0%と、全体平均（10.2%）の約 1.7 倍に達し、他の年代と比べても高い水準を示しています。

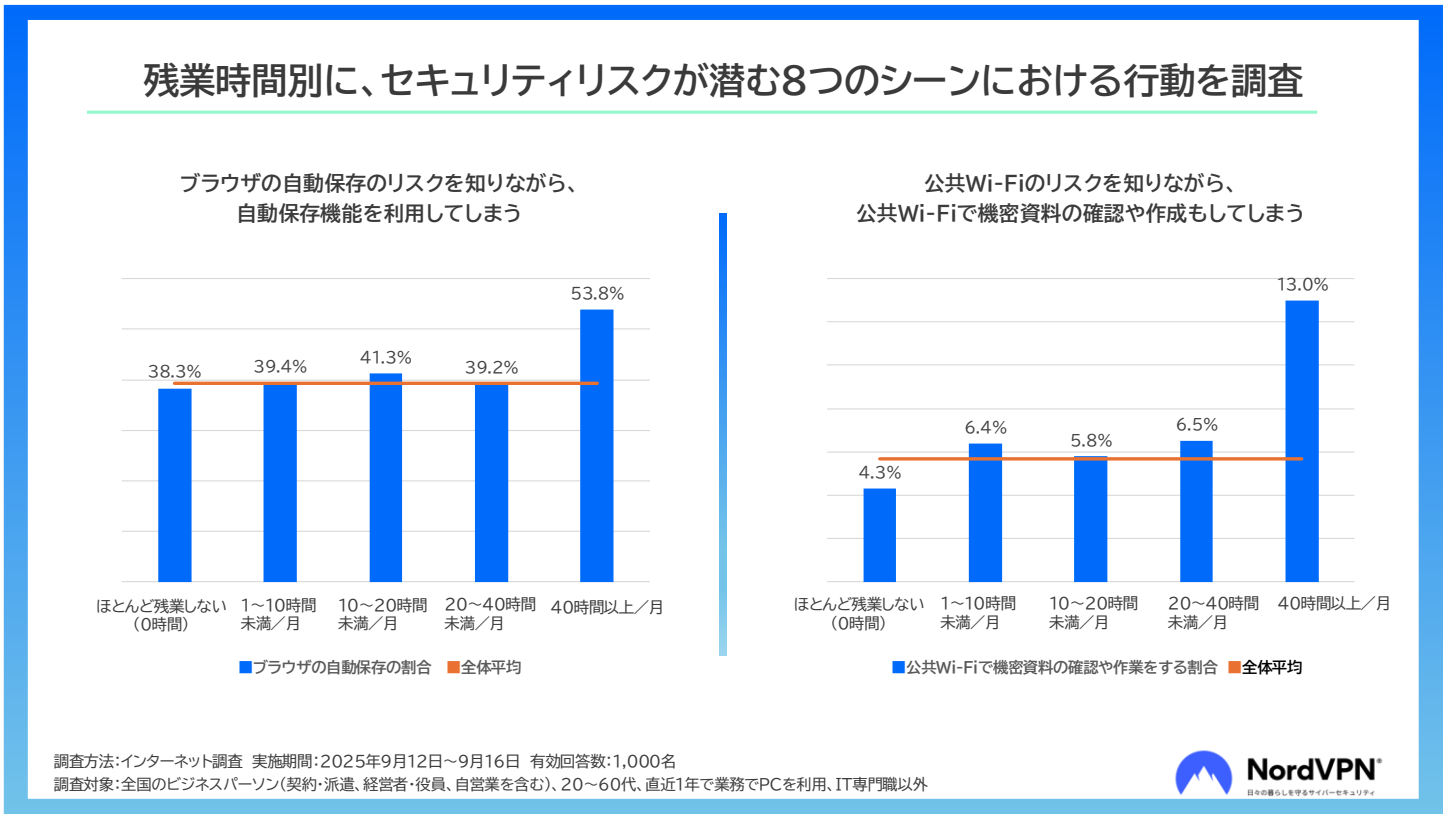
また、個人クラウドに業務データを保存するリスクについては、個人クラウドのセキュリティリスクについて知っていると答えた 20 代のうち、リスク行動を取っている人は 38.7%、30 代は 28.4%と、全体平均（26.3%）と比べて高い数値を記録しました。こうした偽メールに騙されると、個人情報の盗難や金融詐欺、マルウェア感染といった深刻な被害につながる危険があります。



【Topic2：月間 40 時間以上の残業層はリスク行動が全般的に高水準、公共 Wi-Fi の利用に対するリスクは平均の約 2.3 倍】

調査の結果、月間 40 時間以上の残業層は、ブラウザの自動保存利用（53.8%）や個人クラウドへの業務データ保存（42.3%）など、全般的にリスクの高い行動を取る割合が他の層と比べて高い傾向が見られました。中でも、公共 Wi-Fi のリスクについて知っていると回答した月間 40 時間以上の残業層のうち、13.0%が外出先で公共 Wi-Fi を利用し、機密資料の確認・作成を行っていることがわかりました。この割合は、全体平均（5.7%）の約 2.3 倍に達しています。

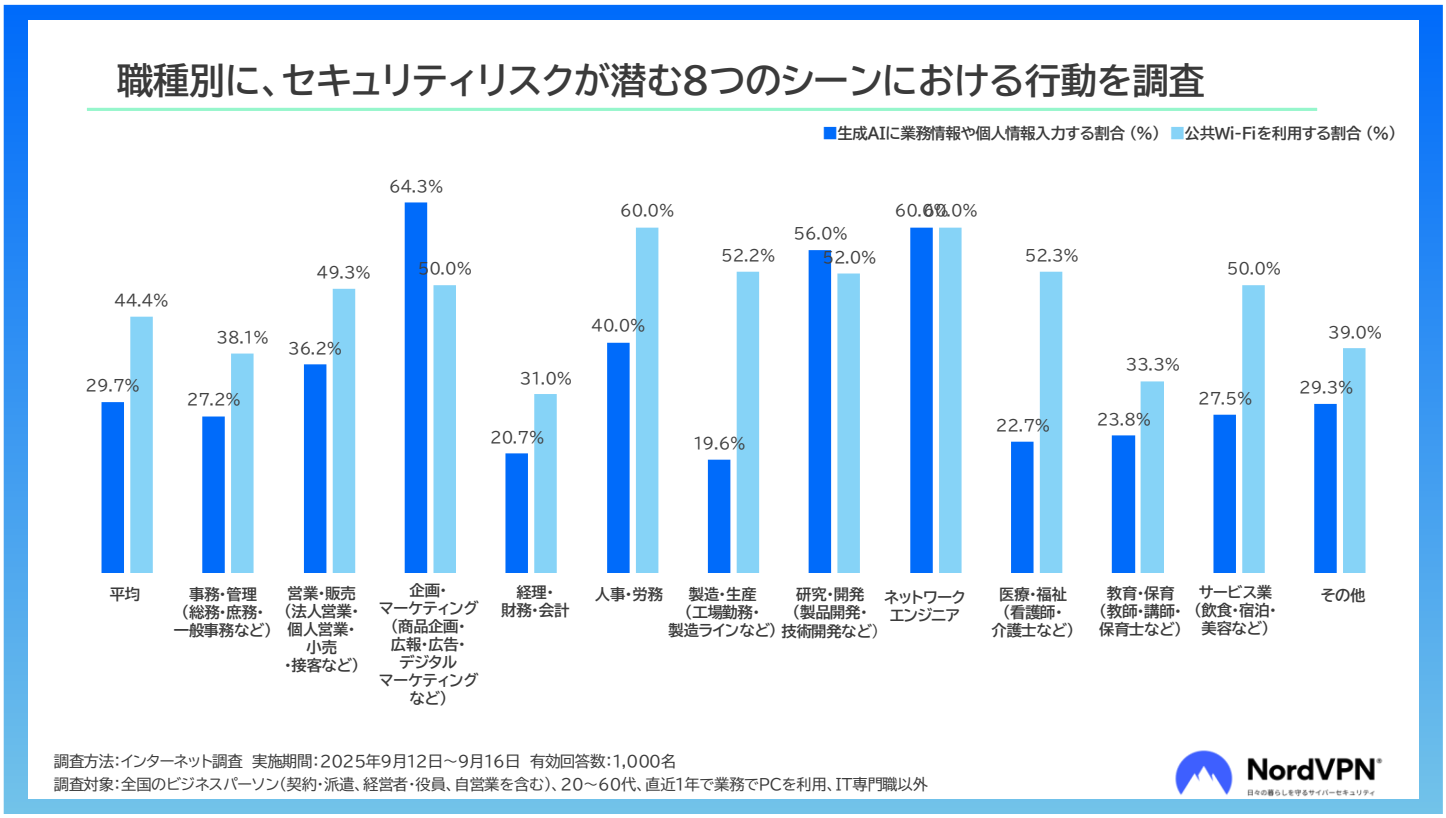
公共 Wi-Fi は通信傍受や偽 Wi-Fi への接続など中間者攻撃の危険が高く、ブラウザの自動保存はパスワードや銀行情報などが簡単に盗まれる恐れがあります。また、個人クラウドの業務利用も共有設定の不備や MFA 未設定によって情報流出のリスクを抱えます。



【Topic3:「企画・マーケティング職」は生成 AI の利用が平均の約 2.3 倍、「人事・労務職」は公共 Wi-Fi の利用が平均の 12.7 ポイント増】

調査の結果、職種別にみると「企画・マーケティング職」と「人事・労務職」で特に高いリスク行動が明らかになりました。「企画・マーケティング職」では、生成 AI のリスクについて知っていると回答した人のうち、生成 AI に業務情報や個人情報を入力する人は 64.3%に達し、全体平均（29.7%）の約 2.2 倍と突出しています。

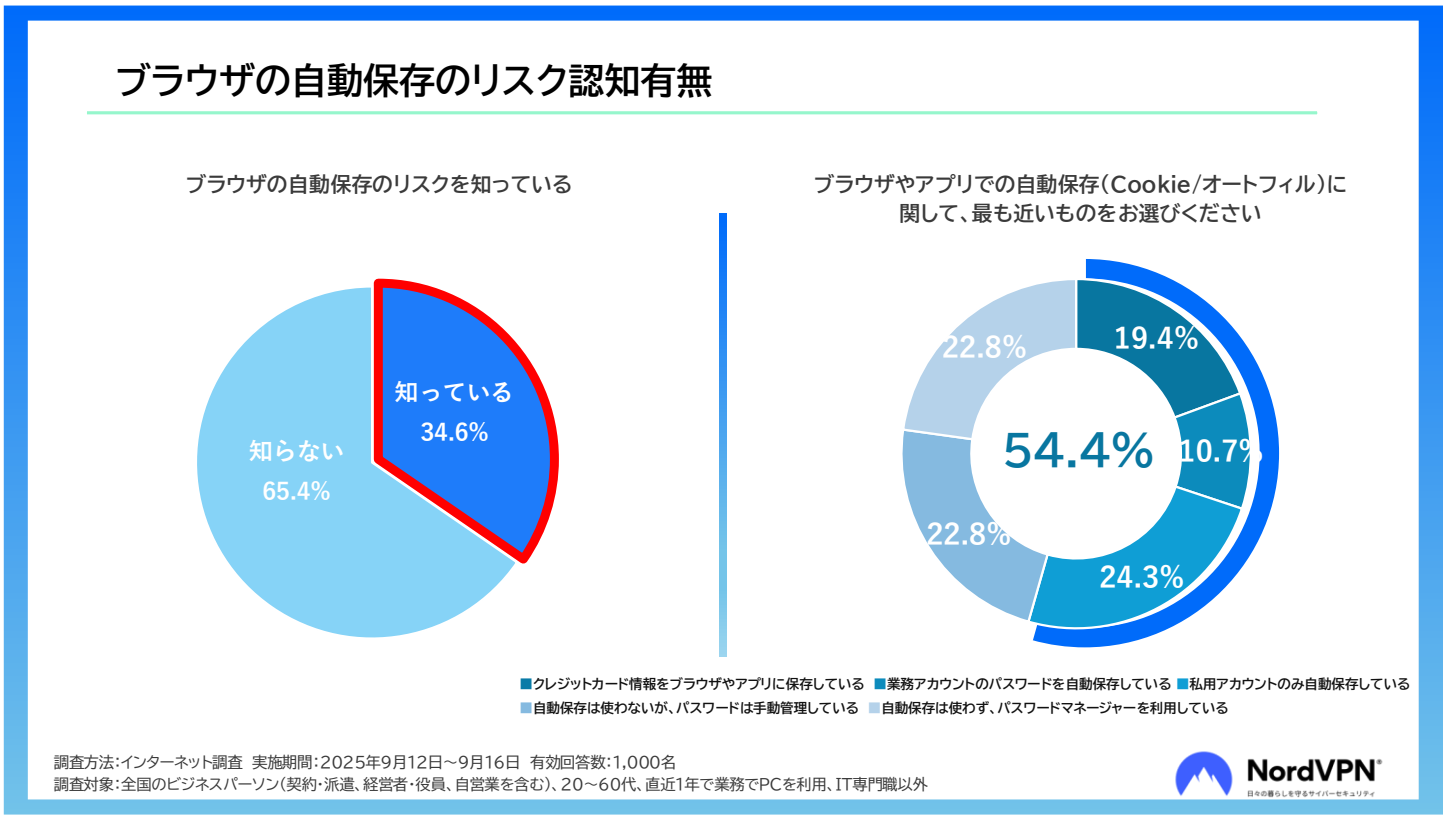
一方、「人事・労務職」では公共 Wi-Fi のリスクについて知っていると回答した人のうち、公共 Wi-Fi を利用している人は 60.0%と、全体平均（44.4%）を 12.7 ポイント上回りました。さらに生成 AI の利用（40.0%）やブラウザの自動保存機能（53.3%）など複数の項目で平均を大きく上回っています。生成 AI の利用は便利ですが、機密情報を誤って入力すれば、ログに保存され外部漏洩の危険があります。



【Topic4：リスク認知は 3 割止まり、54.4%が危険と知りながら自動保存機能を利用】

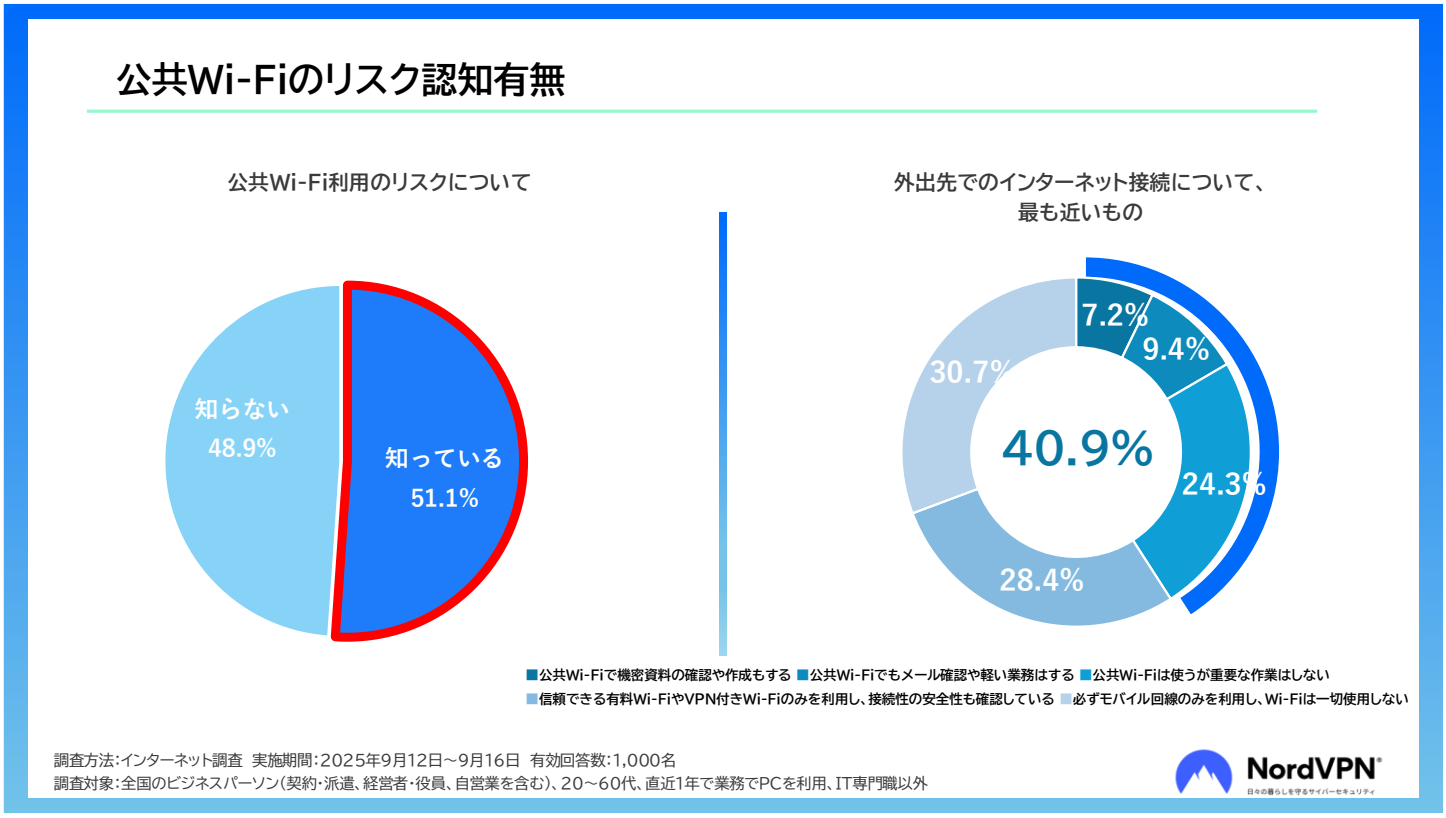
調査の結果、ブラウザやアプリの自動保存機能（Cookie/オートフィル）に潜むリスクを認識している人はわずか 34.6%にとどまりました。さらに、リスクを理解しながらも利用している人は 54.4%と「2 人に 1 人」が利用していることがわかりました。また、パスワードマネージャーを活用する人は 24.1%にとどまりました。

Cookie に保存されたパスワードや個人情報は、攻撃者に悪用されればアカウント乗っ取りや不正購入、二要素認証回避に繋がるため、注意が必要です。



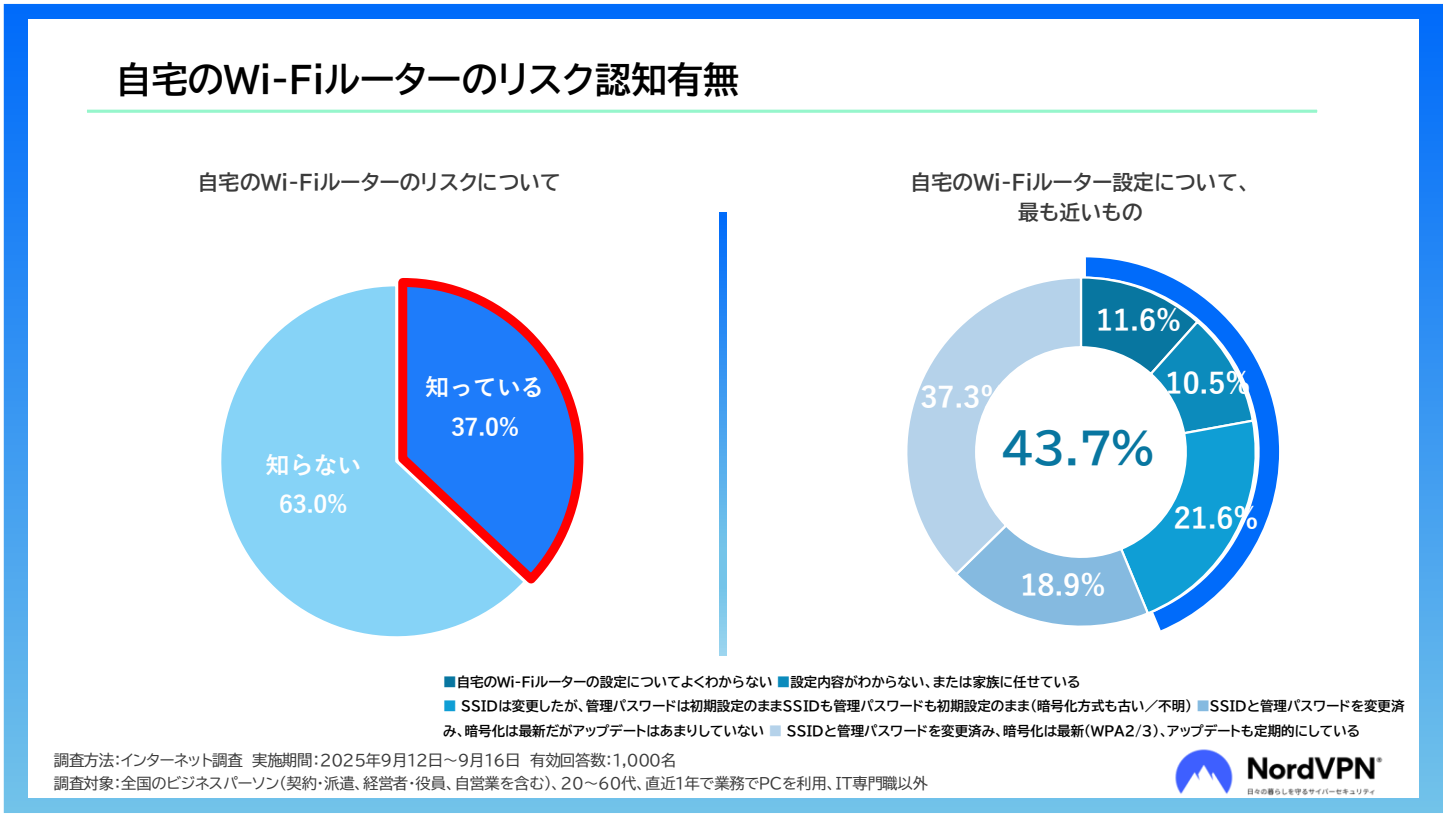
【Topic5：危険と知りつつ、40.9%が公共 Wi-Fi を利用】

調査の結果、危険と知りつつ外出先で公共 Wi-Fi を利用している人は全体の 40.9%に上ることが明らかになりました。内訳を見ると、「機密資料の確認・作成を行う」人が 7.2%、「メール確認や軽い業務を行う」人が 9.4%、「重要作業は避けつつも利用する」人が 24.3%と、危険性を理解しながらも多くのビジネスパーソンが公共 Wi-Fi を利用している実態が浮き彫りとなりました。しかし、公共 Wi-Fi は通信傍受、中間者攻撃、偽 Wi-Fi による窃取など、企業の情報資産に直接影響するリスクがあります。



【Topic6：自宅 Wi-Fi のリスク認識不足、6 割以上が対策不十分】

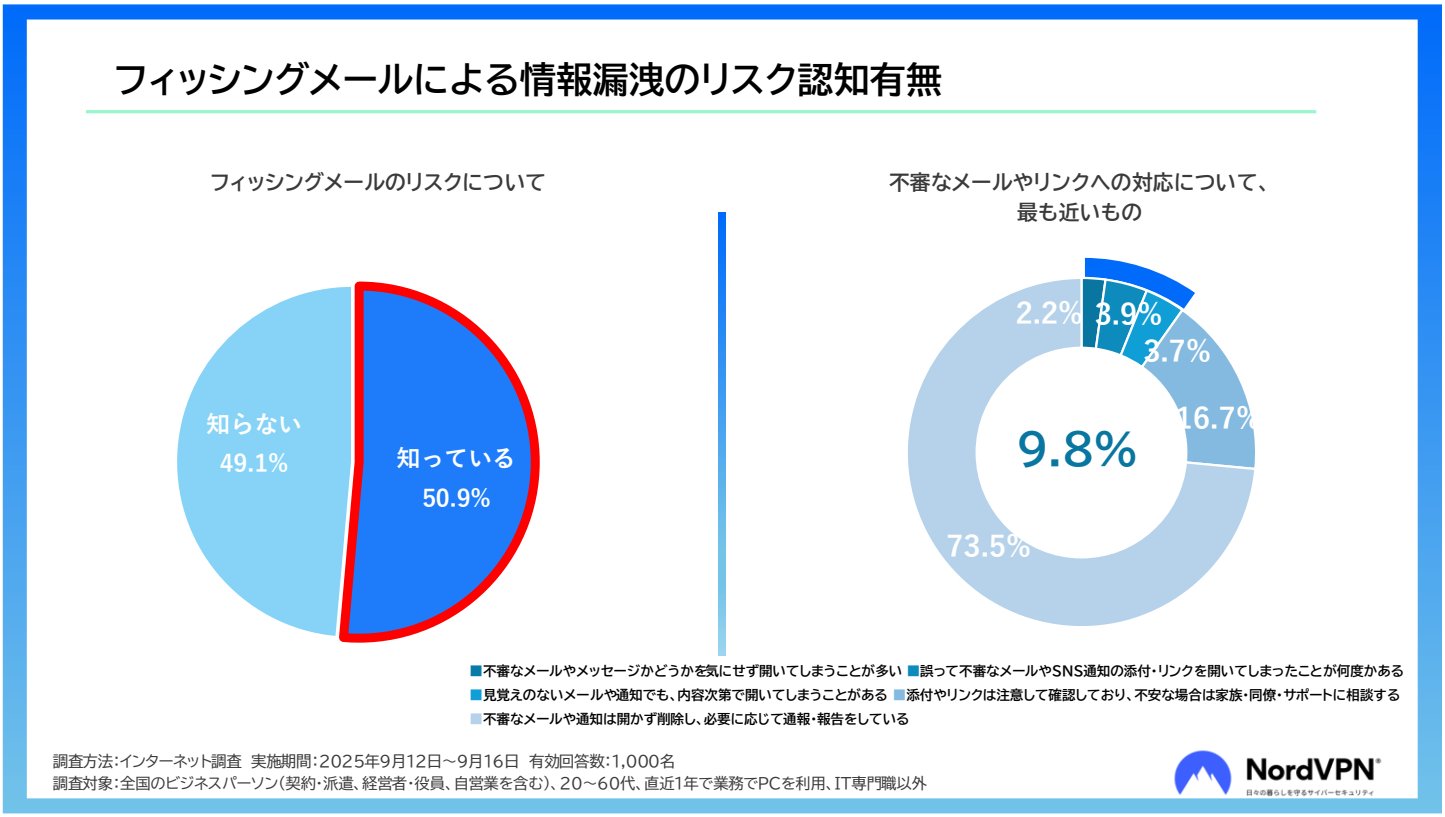
自宅の Wi-Fi ルーターについては、「リスクがある」と認識していない、または設定方法が分からないまま利用している人が全体の 6 割以上にのぼりました。具体的には、「設定内容が分からない／家族に任せている」人が 10.5%、「SSID や管理パスワードを初期設定のまま利用している」人が 21.6%など、セキュリティが不十分な状態が目立ちます。自宅の Wi-Fi ルーターが侵害されると、通信傍受、フィッシングリダイレクト、家庭内デバイスへのマルウェア感染といったリスクに直結します。



【Topic7：フィッシングメールによるリスク行動・端末設定リスクは他項目より低水準】

調査の結果、フィッシングメールによるリスク行動は 10.2%、OS やアプリの未更新は 13.0%と、他のリスク行動に比べて低い数値にとどまりました。公共 Wi-Fi の利用（44.4%）、ブラウザの自動保存（39.9%）、生成 AI への情報入力（29.7%）など、主要なリスク行動の多くが 3～4 割にのぼるのに対し、フィッシングや端末設定関連は約 1 割と相対的に低い水準にあります。

しかし、ソフトウェアの更新を後回しにすることは見過ごせない危険を伴います。更新通知はアプリやシステムが改善され、安全性が強化されている証拠です。更新を怠れば、既知のセキュリティホールがふさがれないままとなり、攻撃の標的になりやすくなります。また、修正されるはずの不具合や潜在的な脆弱性が残るほか、場合によっては利便性を高める新機能を利用できないという不利益も生じます。



■NordVPN 最高技術責任者 マリユス・ブリエディスのコメント

「セキュリティリスクを認識していても、それが必ずしも安全な行動につながるわけではありません。公共 Wi-Fi やブラウザの自動保存が危険だと理解していても、利便性が優先されてしまうことは多々あります。たとえば、若い世代は AI ツールに過剰に情報を共有してしまいがちですし、残業時間が多いビジネスマンは個人クラウドや安全性の低いネットワークに頼ってしまうこともあります。こうした“近道”は一見無害に思えても、資格情報の窃取やデータ漏洩、マルウェアの侵入といったリスクを招く可能性があります。

サイバーセキュリティは、日々の小さな選択にかかっています。自動保存の代わりにパスワードマネージャーを使う、多要素認証を必ず有効にする、デバイスやルーターを常に更新し初期設定を変更する、公共 Wi-Fi で業務を行わない、信頼できる VPN を利用する、業務データは承認済みのクラウドに保存する、AI アカウントは仕事と私用を分ける、そして「会社の正式な文書に載せられない情報は決して生成 AI に入力しない」。こうした小さな心がけの積み重ねこそが、組織全体の安全を守る大きな力になるのです。」

■調査概要

調査名：ビジネスパーソンの無意識な行動に潜むセキュリティリスクに関する調査

調査対象：全国のビジネスパーソン（契約・派遣、経営者・役員、自営業を含む）、20～60 代、直近 1 年で業務で PC を利用、IT 専門職以外

調査方法：インターネット調査

実施期間：2025 年 9 月 12 日～9 月 16 日

有効回答数：1,000 名

※調査自体は、株式会社アクセンチュアに委託

■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/