報道関係者各位

2026 年 7 月 14 日

# NordVPN 調査：日本の約 3 人に 1 人が「個人情報を共有していない」と回答、20 カ国で最多

## ～予約・会員登録も個人情報の共有にあたり、自己認識と実態に乖離～

サイバーセキュリティ企業の NordVPN（本社：オランダ・アムステルダム、日本代表：小原拓郎）は、20 カ国のインターネット利用者 20,054 名を対象とした調査「Life online 2.0」の結果をもとに、日本の利用者に特有の“個人情報の共有に関する認識のギャップ”を明らかにしました。日本で「オンラインで個人情報を共有したことがない」と回答した人は 34%と、20 カ国で最も高く、平均（10%）の 3 倍以上にのぼりました。しかし実際には、会員登録や予約、本人確認といった日常的な操作自体が個人情報を渡す行為であり、「自分は出していない」という認識は実態と一致していません。日本は個人情報の流出を心配する人の割合も 20 カ国で最も低く、こうした「自分は大丈夫」という意識が広がる一方で、偽サイトの手口は正規店と見分けがつかないほど巧妙化しています。両者が重なることで、被害に遭うリスクはむしろ高まっているといえます。

**■ 3 人に 1 人の“誤認識”──「出していない」つもりで、実は入力している**

日本で「オンラインで個人情報を共有したことがない」と答えた人は 34%と、20 カ国平均（10%）の 3 倍以上、2 位のフランス・ドイツ（各 14%）を大きく上回り、最も高くなりました。一方で、「共有したことがある」と答えた人が実際に入力した情報を見ると、生年月日（52%）、氏名（48%）、住所（42%）が上位に挙がっています。これらの共有率自体は、他の 19 カ国と比べれば低い水準です。しかし、会員登録や予約、配送先の入力といった操作はいずれも個人情報を渡す行為であり、日本だけ「共有したことがない」人がこれほど多いという結果は、共有しているという自覚のないまま情報を入力している人が少なくないことをうかがわせます。

■ 危機感も、20 カ国で最も薄い──「自分は大丈夫」という思い込み

「出していないつもり」は、危機意識の低さとも重なります。日本で「自分の個人情報が知らないうちにネット上に出ているのではないか」と心配する人は 15%と、20 カ国で最も低く、平均（28%）の約半分にとどまりました。「必要以上にアプリやサイトを信用しすぎているかもしれない」と考える人は 9%、「個人情報を共有して後悔したことがある」人は 5%と、いずれも平均（14%、10%）を大きく下回り、最も低い部類となっています。「心配していない」「信用しすぎていない」「後悔もない」という自己認識が、偽サイトへの警戒を弱める要因になりかねません。

■ 「見ればわかる」は通用しない──お礼状まで送る、精巧な偽サイト

こうした「自分は大丈夫」という意識とは裏腹に、偽サイトの手口は年々高度化しています。NordVPN の脅威分析チームは海外で、人気トレーディングカードゲームに便乗し、正規販売店になりすます偽ショップ網を特定しました。偽店は Shopify 上に構築され、正規店のデザインを精巧に模倣。Instagram や Facebook、Google の検索連動型広告で、収集家が特定のカードを検索した際に上位に表示されるよう誘導します。手口の中心は 2 つの心理操作で、「在庫残りわずか」といった偽の品薄表示で購入を急がせ、レイアウトや商品画像まで正規店をコピーするブランドなりすましで信用させます。

この詐欺の特徴は、決済後にあります。一部の事例では、被害者の自宅に紙の「お礼状」が郵送され、正規の店と取引したかのような印象を与えることで、不審に思ってカードの利用停止（チャージバック）を申し立てるまでの時間を遅らせます。次回使えるクーポンやおまけを同封し、最初の商品を待っている間に“リピーター”に仕立てる狙いです。

NordVPN は、広告の透明性ページや画像のハッシュ、サイトに埋め込まれた共通のトラッキング ID（Google Analytics や Meta の Pixel）を手がかりに、無関係に見える複数の店を単一の攻撃者による一連の犯行として突き止めました。ドメインを立ち上げては広告で集客し、決済を集めて閉鎖する“ヒットアンドラン”を繰り返す構造だといいます。

見た目の精巧さや購入後の“丁寧な対応”は、必ずしも正規事業者の証拠ではありません。海外で確認されたこうした手口は、国境を越えて日本の利用者が目にする可能性もあります。「怪しいサイトは見ればわかる」「自分は個人情報を出していない」という思い込みが強いほど、こうした巧妙な偽サイトの前では警戒が働きにくくなります。価格や在庫、サイトの見栄えだけで判断せず、入力の前に運営元を確認することが重要です。

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

「収集家は、自分が買おうとしているものに感情移入しています。レアなカードを追いかけている人は、立ち止まってサイトを精査するような心理状態にはありません。攻撃者はそれを分かったうえで狙っています。彼らが突いているのは、技術的な脆弱性ではなく、感情的な脆弱性なのです。」

■ なぜ今、注意が必要か──入力機会が増える時期

夏季は、旅行・宿泊予約、レジャーやイベントのチケット購入、EC のセール、限定商品の購入など、氏名・住所・生年月日・決済情報を入力する機会が一年のうちでも増える時期です。「残りわずか」「期間限定」といった表示は、利用者が内容を十分に確認しないまま入力・決済を進める一因になります。急ぐほど、運営元を確認する余裕は失われがちです。IPA（独立行政法人情報処理推進機構）をはじめとする関係機関も、旅行や長期休暇が増えるこの時期に合わせ、情報セキュリティ上の注意を例年呼びかけています。

■ 入力の前に確認したい 3 つの習慣

1. **URL・運営元を確認する：** ログイン情報や決済情報を入力する前に、URL、ドメイン、会社名、表示内容に不自然な点がないかを確認してください。少しでも違和感があれば、リンクをたどらず、公式アプリまたは公式サイトを直接開いてください。

2. **求められる情報が妥当かを確認する：** 予約や購入に不要と考えられる生年月日、本人確認書類、銀行情報などの入力を求められた場合は、そのサービスに本当に必要かを確認し、不要な入力は避けてください。

3. **「品薄」「今だけ」の表示で判断を急がない：** カウントダウンや在庫僅少の表示は購入を急がせる手法であり、それ自体が急ぐ理由にはなりません。あわせて、OS やアプリを最新の状態に保ち、多要素認証を利用してください。

**■ 調査概要**

調査名称：Life online 2.0（Lifetime online #2）
調査期間：2026 年 4 月 1 日～17 日
調査対象国：日本、米国、
英国、オーストラリア、カナダ、ブラジル、メキシコ、韓国、フランス、ドイツ、イタリア、スペイン、オランダ、スウェーデン、フィンランド、オーストリア、スイス、ポーランド、リトアニア、アイルランドの 20 カ国
対象者：各国のインターネット利用者（18～74 歳。メキシコおよび韓国は 18～64 歳）
サンプル数：合計 20,054 名。原則各国約 1,000 名、アイルランド・韓国・スペイン・スイスは各約 800 名
調査方法：年齢、性別、居住地に基づく割付を行った全国代表サンプルへのオンライン調査
調査機関：Cint、Syno International（オーストリア、スイス）、Norstat（リトアニア、ポーランド）

**■ NordVPN について**

NordVPN は、世界中で何百万人ものインターネットユーザーに利用されている、デジタルプライバシーとセキュリティのためのオールインワンアプリです。NordVPN アプリは、世界最高水準の VPN、次世代アンチウイルス、Dark Web Monitor™をはじめとするセキュリティ機能を統合し、ユーザーがオンライン上でより安全かつプライベートに過ごせるようサポートします。また、フィッシング、詐欺、悪質なウェブサイト、トラッカー、迷惑広告、マルウェアなどの脅威からユーザーを保護し、オンラインプライバシーの強化にも貢献します。詳細は nordvpn.com をご覧ください。

**【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/ |