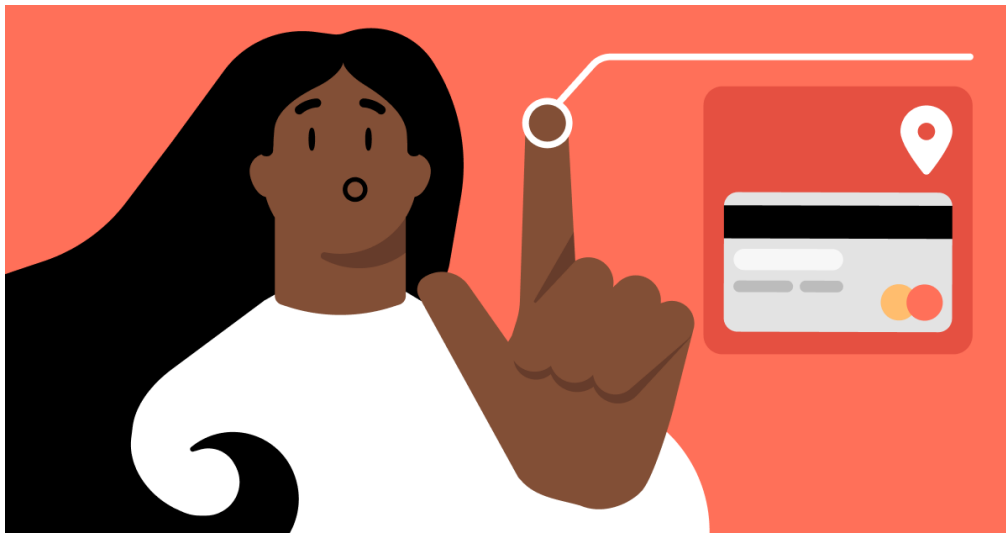


日本人の 3 人に 1 人が「生体認証データの悪用」を懸念！ NordVPN が生体認証の利用実態に関する調査結果を発表 ～生体認証時代におけるプライバシー対策のヒントとは～

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、日本における生体認証技術の利用実態と意識に関する調査結果を発表しました。

また、生体認証をより安全に活用するためのポイントや、日常生活で実践できる具体的な対策も合わせてご紹介します。



調査概要

NordVPN は、日本人 1,000 名以上を対象に、生体認証の利用に関する調査を実施しました。

調査期間:2024 年 11 月 18 日～11 月 28 日

調査人数:1,004 人

調査対象:18～74 歳の成人

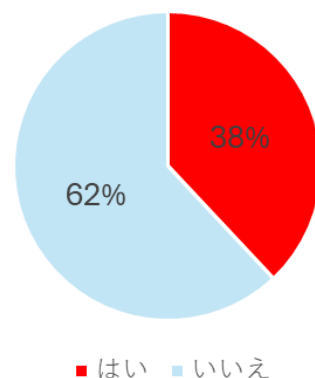
調査機関:NordVPN

■約 4 割の回答者が、生体認証を週 1 回以上使用

近年、スマートフォンのロック解除や決済認証など、日常生活のあらゆる場面で生体認証の利用が広がっています。

Nord VPN が実施した生体認証の使用実態に関する調査では、約 4 割の人が週 1 回以上の頻度で生体認証を使用していることが明らかになりました。

生体認証（指紋・フェイス・アイスキャナー）
を週 1 回以上使用していますか

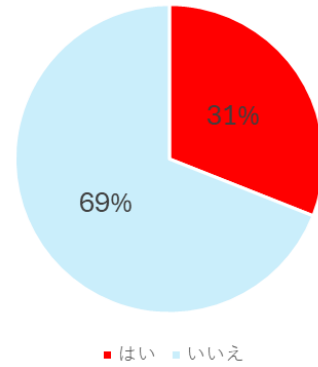


■31%の回答者が「サイバー犯罪者による生体認証データの悪用」に懸念

サイバー犯罪者に生体認証データを悪用されることを懸念

生体認証は、パスワードの入力を省略でき、SNS や銀行アプリへのアクセスをワンタッチで行えるなど、高い利便性を備えた技術です。

その一方で、31%の回答者が「サイバー犯罪者による生体データの悪用」に懸念を抱いているということも、調査から明らかになっています。



その背景には、生体情報の流出や、なりすましによる個人情報の盗難、さらにはダークウェブでの売買といった現実的なリスクの存在があります。特に、指紋や顔、虹彩といった情報は、一度漏洩するとパスワードのように変更できず、長期的に悪用される危険があります。

■NordVPN サイバーセキュリティ専門家 アドリアヌス・ワーマンホーフェンのコメント

「生体認証技術は、従来のパスワードよりも安全と見なされていますが、すべてのデータは依然としてハッキングのリスクにさらされています。これまでに、何万件もの指紋や顔画像がダークウェブ上で売買されていることが確認されています。特に懸念されるのは、パスワードと異なり、生体情報は一度漏洩すると変更ができないという点です。一度漏洩すれば、そのデータは悪用され続ける可能性があります。さらに、AI やディープフェイクなどの進化により、生体認証のなりすましも身近な脅威となりつつあります。SNS などから取得された画像や音声をもとに、サイバー犯罪者が“なりすまし用データ”を生成するケースも少なくありません。

こうした背景から、生体情報は極めて機密性の高い個人情報の一つとして慎重に扱う必要があります。また、生体認証を利用する際は、強固なパスワードや多要素認証などを併用することで、悪用のリスクをより確実に下げることができます。」

■NordVPN サイバーセキュリティ専門家 アドリアヌス・ワーマンホーフェンが推奨する生体認証使用時にプライバシーを守るための8つの対策

①生体情報が写る SNS 投稿には注意を

顔、指紋、虹彩などが映り込んだ画像や動画を SNS に投稿する際は、不特定多数に閲覧されるリスクを認識し、慎重に判断することが重要です。ハッカーが SNS 上の高解像度画像から指紋などを抽出し、ディープフェイクのモデル作成やダークウェブ上での売買に悪用している事例があります。

②画質を調整し、個人情報が特定されやすい部分を隠す

画像や動画を公開する際は、解像度を下げたり、顔・指先・目元などの生体情報が含まれる部分をぼかす・隠す加工を行うことで、情報の悪用リスクを抑えることができます。

③第三者に取得されにくい生体認証手段を選ぶ

顔認証や指紋認証よりも、虹彩や網膜スキャンなど、他人に容易に取得されにくい生体情報を使った認証方法を選ぶことで、なりすましなどのリスクを軽減できます。

④自分の画像がどう使われているかを定期的に確認する

インターネット上で自分の顔写真などがどのように使われているかを定期的に検索し、不適切な掲載が見つかった場合は速やかに削除依頼などの対応を行いましょう。

また、情報の取扱い体制が十分であることを事前に確認することも重要です。

⑤生体情報は多要素認証(MFA)で使用するのが安心

生体情報のみを使った認証は避け、パスワードや物理デバイスなどと組み合わせた多要素認証(MFA)の導入が推奨されます。たとえ生体情報が流出した場合でも、他の要素との組み合わせにより、悪用のリスクを大幅に下げることが可能です。安全性を高めるためには、強固なパスワードを設定し、信頼性の高いパスワードマネージャーで管理することも重要です。

⑥ハードウェア認証デバイスでセキュリティを強化

FIDO (Fast IDentity Online) 対応のハードウェアトークンなどを併用することで、安全性がさらに高まり、不正アクセスからの保護が強化されます。

⑦生体情報の代わりに、強力なパスワードを使う選択も

生体認証を使わないアカウントでは、推測されにくい強力でユニークなパスワードを設定し、信頼できるパスワードマネージャーで安全に管理しましょう。

⑧新しいサービスに生体情報を登録する際は慎重に

新たに利用するアプリやデバイスに生体情報を登録する際は、データの保存場所や取り扱い方針が明示されているか確認しましょう。一般的に、端末内のローカル保存の方が安全性は高く、クラウド上に保存される場合は、大規模な情報流出リスクが伴います。漏洩した生体情報は変更ができず、ダークウェブ上で売買される可能性もあります。

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 개국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/>