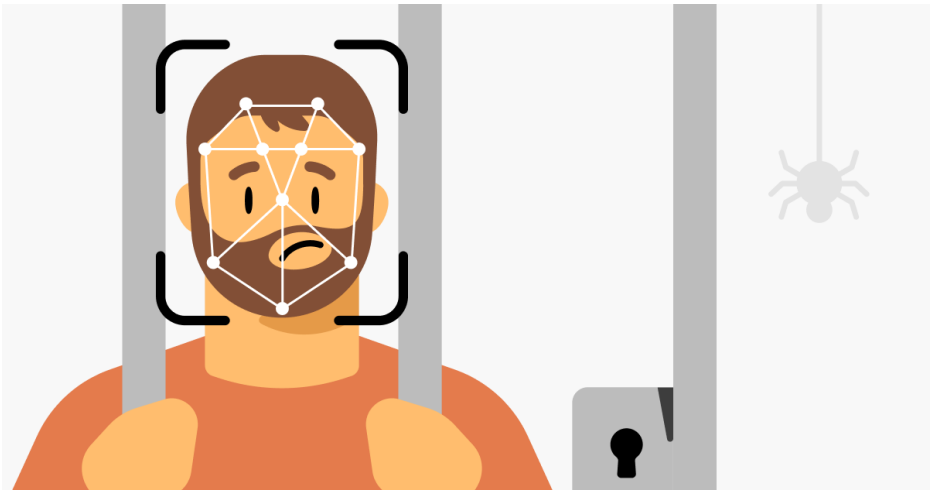
報道関係者各位

2025 年 5 月 16 日

Z 世代の約 5 人に 1 人が「虹彩認証」を活用し始めている！？
NordVPN が生体認証の利用に関する調査結果を発表

～「なりすまし」を防ぐ 5 つの対策をご紹介～

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、生体認証システムの普及に伴い利用者数が急増していることを受け、生体認証の利用実態に関する調査を実施しました。あわせて、生体データを悪用した「なりすまし」による不正認証や情報漏えいを防ぐための、8 つのセキュリティ対策をご紹介します。



調査概要

NordVPN は、日本、ドイツ、イタリア、ブラジルの 4 カ国 4,000 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

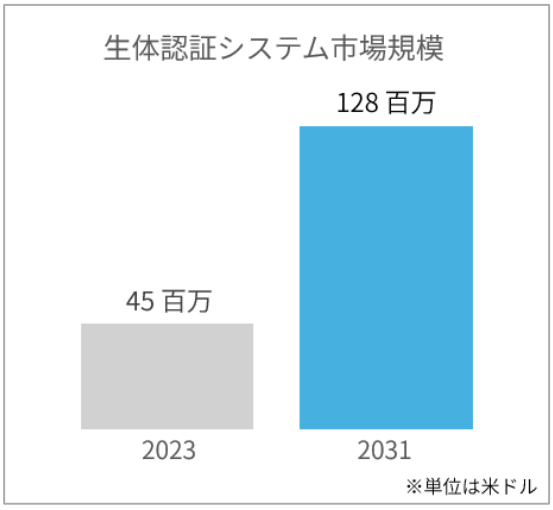
調査人数：各国約 1,000 人

調査対象：18～74 歳の成人

調査機関：NordVPN

生体認証とは、顔や指紋、目の虹彩など、人間の身体的特徴を用いて個人を特定する認証方法です。近年、この技術を活用したサービスを提供する企業が増加しており、DATA BRIDGE によると、世界の生体認証システム市場は年間平均約 14%のペースで成長しており、8 年でおよそ 3 倍に拡大すると予測されています。

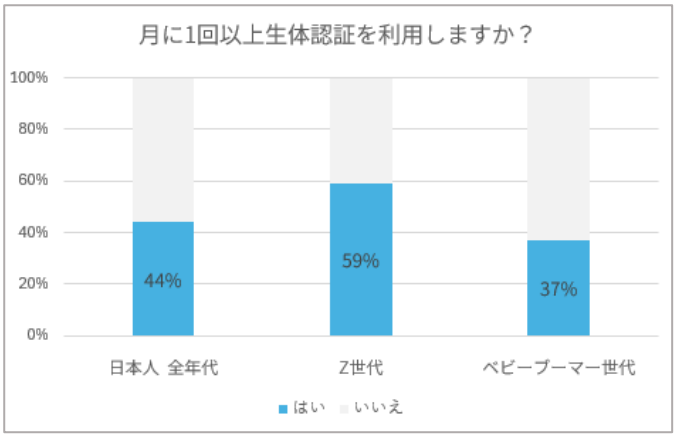
こうした背景を受け、NordVPN は生体認証の利用実態に関する調査を実施しました。あわせて、生体データを悪用して本人になりすまし、不正認証や情報漏えいを引き起こすリスクに備えるための、8 つのセキュリティ対策もご紹介します。



■日本人の約 44%が「少なくとも月 1 回以上生体認証を利用する」と回答

生体認証の利用頻度に関する調査では、日本人の約 44%が「少なくとも月に 1 回以上生体認証を利用している」と回答しました。さらに年代別に見ると、「月に 1 回以上利用している」と答えた人の割合は、Z 世代（18～27 歳）で約 59%、ベビーブーマー世代（60～78 歳）では約 37%にのぼり、60 代以上でも約 3 人に 1 人が生体認証を利用していることが明らかになりました。

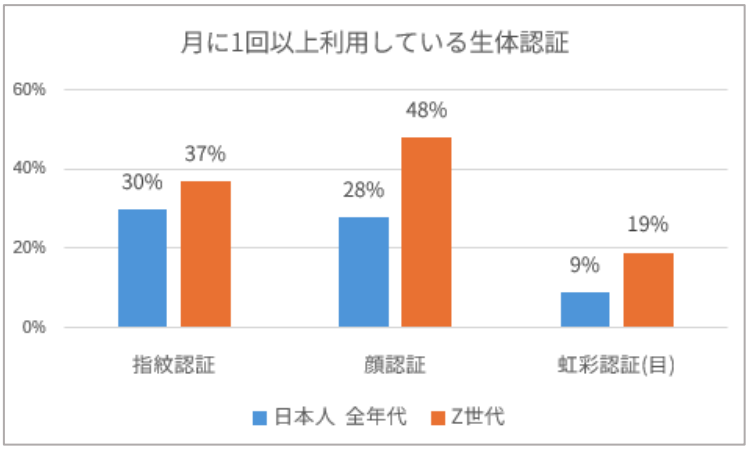
パスワードを記憶する必要がなく、指や顔をかざすだけで簡単に認証ができる利便性から、生体認証は幅広い世代に浸透していると考えられます。



■Z 世代は「顔認証」を最も利用していることが判明。「虹彩認証」を活用する Z 世代も。

項目別の生体認証の使用率に関する調査では、日本人全体では「指紋認証」の利用者が最も多い一方で、Z 世代においては「顔認証」の利用が最も多いことが明らかになりました。マスクを着用したままでも顔認証が可能なスマートフォンが登場しているほか、近年では銀行の ATM にも顔認証が導入されています。

また、「虹彩認証」と呼ばれる、目の虹彩（模様）を読み取る認証方式についても調査を実施。その結果、「月に 1 回以上虹彩認証を利用している」と回答した Z 世代は約 19%にのぼり、およそ 5 人に 1 人が利用していることが分かりました。虹彩認証はゴーグルやマスクを着用した状態でも認証が可能なため、工場や医療現場などでの入退室管理に活用されています。



以上の結果から、日本人の約半数が生体認証を利用しており、顔や目など、さまざまな認証手段が広く活用されていることが分かりました。スピーディーで利便性の高い生体認証ですが、その一方で、生体データを悪用して認証を突破する「なりすまし」のリスクも潜んでいます。パスワードとは異なり、生体データは個人の身体的特徴そのものであるため、一度登録すると変更が困難です。そのため、万が一流出した場合、「なりすまし」などの悪用リスクに対して、より慎重な対策が求められます。

■生体認証を狙った代表的な「なりすまし」手口

①偽造指紋によるロック解除

グラスやスマートフォンに付着した指紋を採取し、シリコンやゼラチンで偽の指を作成する方法です。スマートフォンのロックや本人確認を突破される事例があり、セキュリティコンテストや実験でも実際に成功したケースが報告されています。

②高精細な顔写真や 3D マスクによる顔認証の突破

SNS に投稿された高画質の正面写真を利用し、顔認証システムを欺く手口です。さらに高度な手法として、3D マスクやディープフェイク動画を用いて本人になりすますケースも確認されています。

③虹彩画像を使った偽装アクセス

高精度なカメラで撮影した虹彩画像を認証カメラに提示し、不正にアクセスを試みる方法です。画像処理技術の進化により、より精巧な偽造が可能になってきています。

■NordVPN 最高技術責任者マリユス・ブリエディスが提案する「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可能性があることを意識し、慎重に判断しましょう。

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。

⑤生体情報は多要素認証で使用するのが安心
生体情報だけに頼った認証は避け、パスワードや物理的なデバイスなどと組み合わせた多要素認証（MFA）を導入することで、安全性を高めることができます。

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新しいサービスには慎重に生体情報を提供する
新たに登場したアプリやデバイスに生体情報を登録する際は、セキュリティ対策や情報の取扱い体制が十分であるかを事前に確認するようにしましょう。

■NordVPN 最高技術責任者マリユス・ブリエディスのコメント
「生体認証は、デジタル社会における“新たな鍵”として急速に普及しています。従来のパスワードや PIN コードに代わり、多くの人が生体認証を選ぶようになりました。スムーズで時間の節約にもつながる一方で、利便性とリスクが表裏一体である点には注意が必要です。セキュリティ強化に有効である反面、顔や指紋などが詐欺の標的になるケースも増えています。
指紋、虹彩スキャン、顔認証などの生体データは、個人を特定する“デジタル上の身元”を示すものであり、ネットバンキングや Apple Pay、Google Pay など、幅広いサービスの認証に利用されています。万が一、生体情報が悪用された場合には、個人情報の不正アクセスや、なりすましによる金銭的被害につながる恐れがあります。リスクを最小限に抑えるためにも、生体情報の扱いには日頃から十分な注意と対策が必要です。」

■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/