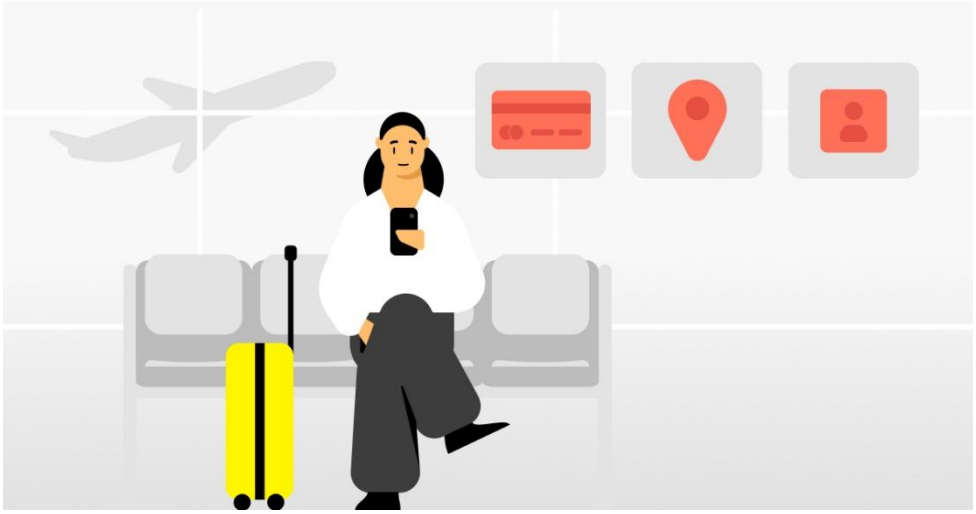
報道関係者各位

2025 年 7 月 23 日

# 日本のパスポート情報がたったの 1,500 円から売買されている？！
# NordVPN と Saily がダークウェブで売買される旅行データの実態を調査！
## ～夏休みの旅行前に確認すべきサイバーリスクと対策をご紹介～

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、グローバル eSIM サービス「Saily」と共同で、ダークウェブでのパスポートやロイヤリティアカウントの売買について調査を実施しました。また、旅行予約時における不正アクセスや個人情報の悪用を防ぐための対策もあわせてご紹介します。



**調査背景**

夏休みに向けて海外旅行の需要が高まる中、旅行者を標的としたサイバー犯罪が急増しています。サイバー犯罪者は、航空会社や旅行代理店になりすました偽サイトや偽の SMS 送信など、さまざまな手口で旅行者を狙っています。こうした状況を受け、NordVPN と Saily はダークウェブ上で旅行者の個人情報の売買に関する実態を調査しました。

**調査概要**

NordVPN は、グローバル eSIM サービス「Saily」と共同で、情報漏えい管理プラットフォーム「NordStellar」を使用し、ダークウェブ上で旅行関連データに関する取引について調査を実施しました。

調査期間：2025 年 6 月 10 日～6 月 20 日

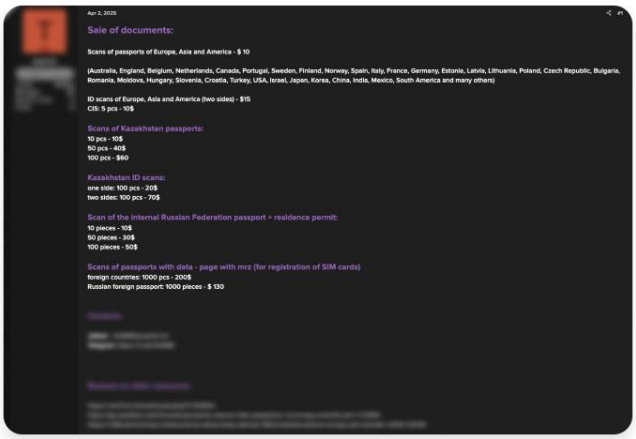
調査対象：ダークウェブ上のマーケットプレイスやハッカーフォーラムに掲載されている盗まれた旅行書類および関連データの売買情報

分析項目：パスポート、ビザ、ロイヤリティアカウント、旅行予約情報などの出品状況や価格など

調査機関：NordVPN、Saily

## ■パスポートが 1,500 円から？驚くほど安価で売買されている旅行者の個人情報

今回の調査では、ダークウェブ上で旅行者の個人情報がいかに安価かつ大規模に取引されているかが浮き彫りになりました。例えば、スキャンされた日本などアジアのパスポートはわずか 10 ドル(約 1,500 円)から売買されていますが、認証済みの EU パスポートとなると、その価値は 5,000 ドル（約 75 万円）以上に跳ね上がります。さらに、偽造された銀行の取引明細やビザステッカー、数百万マイルを保有するハッキングされた航空会社のロイヤリティアカウントは数百ドルで売買されていました。また、主要な旅行予約プラットフォームでのホテルや航空券の予約情報については、250 ドル(約 38,000 円)以上の、割引価格で売買されています。




## ■サイバー犯罪者も AI を悪用！偽のチェックインサイトなど手口も巧妙化

近年、パスポートや旅行に関する個人情報が狙われるケースが増えており、デバイスをスキャンするマルウェアや、航空会社・旅行代理店からの情報漏洩など、様々な手口があります。特に注意が必要なのは、AI 技術を悪用したフィッシング詐欺です。偽の航空会社のチェックインサイトで本人確認用の顔写真と IDを要求され、空港ラウンジやフリーWi-Fi の偽登録ページに誘導されるケースが多発しています。AI が犯罪者に悪用されることで、これらの詐欺が自然な文章やデザインで構成され、見抜くことが一層困難になっています。

これらの不正行為により、盗まれた氏名やパスポート番号、連絡先などの個人情報が悪用される危険も高まっています。盗んだ情報を使って他人になりすまし、銀行口座の開設や各種ローンの申し込みを行うなど、深刻な金銭的被害につながるケースも報告されています。

## ■今からでも間に合う！NordVPN 最高技術責任者 マリユス・ブリエディスが推奨する、夏休みの旅行前に押さえたい 5 つの「デジタル防御策」

**① 機密書類は暗号化して保管**

パスポートや運転免許証などの重要書類のコピーは、ただデジタル化するだけでなく、万が一の漏洩に備えて厳重に保管しましょう。例えば、保護機能付きのフォルダや、高機能なパスワード管理アプリのセキュアストレージを活用することで、万が一アカウントに不正アクセスされた場合でも、ファイルが暗号化されているため情報漏洩のリスクを低減できます。さらに、二要素認証を設定し、セキュリティを一層強化することもおすすめです。

**② フィッシング詐欺に警戒**

巧妙化するフィッシング詐欺から身を守るには、安易に情報を入力せず、公式サイトであるかを慎重に確認することが大事です。メールや SMS のリンクを直接クリックせず、公式のウェブサイトやアプリ経由でアクセスする習慣をつけましょう。特に、「緊急」や「重要」といった言葉で不安を煽るメッセージや、不自然な日本語が含まれている場合は注意が必要です。URL や送信元のメールアドレスに違和感がないか、常にチェックすることが大切です。

**③ 公共 Wi-Fi 利用時は VPN を利用**

カフェや空港の公共 Wi-Fi は便利ですが、通信内容が第三者に傍受されるリスクも潜んでいます。VPN は、デバイスとインターネットの間に暗号化された安全な通信経路を確立し、悪意のある傍受やマルウェアの侵入から情報を保護できるため、こうしたネットワークを利用する際は、VPN を使用するよう意識してください。

**④ アカウントを定期的に確認**
銀行口座やクレジットカード、ポイントサービスのアカウントは、定期的に確認することが不正利用の早期発見につながります。メールやプッシュ通知を有効にすることで、身に覚えのない取引があった際にすぐに気づくことができます。また、月に一度はログイン履歴や利用明細に目を通す習慣をつけることにより、ポイントの不正利用といった見逃しがちな被害も防ぐことができます。

**⑤紛失・盗難時の対応は迅速に**
重要書類やスマートフォンを紛失・盗難した場合は、ただちに関係各所への届け出を行いましょう。クレジットカードや携帯会社にはサービスの利用停止手続き、警察への遺失届・盗難届の提出をしましょう。よりスムーズに対応するために、事前に各種連絡先をリスト化し別保管することもおすすめです。

**■NordVPN 最高技術責任者 マリユス・ブリエディスのコメント**
「ダークウェブで確認された取引価格からも明らかになるように、旅行者の個人情報には非常に高い価値があります。同時に、それらの情報は脆弱であり、ハッカーにとって “金のなる木”です。比較的簡単な手口で個人情報に直接アクセスできてしまうため、盗まれた情報は取引され、多くの犯罪に悪用されています。個人情報の保護は、旅行時においても極めて重要です。」

パスポート情報の漏えいや売買については、こちらもご覧ください：https://nordvpn.com/ja/blog/stolen-travel-document-research-nordvpn-saily/

**■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/