報道関係者各位

2025 年 11 月 6 日

日本のカード情報は 22.80 ドル、世界最高値で取引されることが判明！
NordVPN がダークウェブ上の 50,000 件超のデータを分析
～支払いカードを安全に利用するために実践すべき 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、情報漏えい管理プラットフォーム「NordStellar」を活用し、ダークウェブ上で売買される 50,705 件の盗難カード情報を分析しました。また、支払いカードを安全に利用するために実践すべき 5 つの対策もあわせてご紹介します。

実施背景

近年、オンラインショッピングやサブスクリプションなどのキャッシュレス決済が急速に拡大する一方で、支払いカード情報を狙った不正アクセスや情報漏えいが世界的に増加しています。こうした状況を受け、NordVPN では、ダークウェブ上で実際にどのようなカード情報が売買されているのか、その規模と傾向を明らかにするために調査を実施しました。

調査概要

調査機関：NordVPN（情報漏えい管理プラットフォーム「NordStellar」）
データ収集時期：2025 年 5 月
調査対象：ダークウェブ上のマーケットプレイスにおける盗難カード出品データ（合計 50,705 件）
調査方法：カード番号・有効期限・価格帯・国籍別データなどをメタデータ分析
備考：本調査では、研究者が実際の支払いカード情報や利用者の認証情報にアクセスしたり、購入したりすることは一切ありません。分析の対象としたのは、ダークウェブ上の出品情報に含まれるメタデータのみです。

■アメリカが支払いカードの盗難件数最多を記録

他国と比較すると、アメリカの利用者が支払いカード詐欺の被害を最も多く受けていることがわかりました。被害を受けた支払いカードのうち、60%以上がアメリカ発行のカードで、続いてシンガポールが約 11%、スペインが約 10%と、上位 3 か国で全体の約 8 割を占めています。

■日本の支払いカード情報が世界最高値で取引されていることが判明

被害件数が多いことが必ずしも高価格につながるわけではありません。盗まれた米国のカード情報はダークウェブ上で約 11.5 ドル程度と、価格帯のほぼ中間に位置しています。

一方、最も高値で取引されているのは日本の支払いカード情報で、平均約 23 ドル（約 3,400 円）。次いで、カザフスタン・グアム・モザンビークのカード情報がいずれもおよそ 16 ドル前後で取引されていました。

その一方で、コンゴ共和国、バルバドス、ジョージアなどでは、わずか 1 ドル（約 150 円）程度で販売されるケースもあり、国や地域によって盗難データの「市場価値」に大きな差があることが明らかになりました。

■なぜ日本の支払いカードが高値で取引されるのか

NordVPN は、「データ供給の少なさ」と「不正検知システムの厳しさ」が、日本のカード情報が高値で取引される主な理由と分析しています。ダークウェブ上での盗難カード価格は、基本的に需要と供給のバランスによって決まります。つまり、盗まれにくい国ほど希少性が高まり、犯罪者は高額を支払ってでも入手しようとする傾向があります。一方で、米国やスペインのように大量のカード情報が流出している国では、価格が安価に抑えられ、まとめ売りされるケースも多いため、1 枚あたりの取引価格は低くなります。

さらに、有効期限が長いカードほどプレミアが付くことも確認されました。今回の調査対象では、全体の約 87%が 12 か月以上有効な状態で販売されており、犯罪者が再利用や再販を容易に行える点が、価格上昇の一因と考えられます。

■犯罪者の「カーディング」実態：カード情報が“現金”になるまで

ダークウェブでは、単なるカード番号にとどまらず、氏名・住所・メールアドレス・電話番号・セキュリティコードなどがセットになって販売されるケースが一般的です。これらの情報を用いて、犯罪者はオンライン決済やギフト券購入などを通じて不正に現金化する「カーディング（carding）」という手法を行います。犯罪者は数ドルを投じるだけで、他人の資金を直接現金化するためのルートを手に入れ、小額のテスト課金を繰り返して有効なカードを特定した後、自動化された仕組みでギフトカードや旅行予約を大量に購入し、それらを転売・資金洗浄することで利益を上げます。

カーディングの運用は分業化されており、主に次のような役割が存在します。

・ハーベスター（harvesters）：カード情報を盗み出す／収集する。

・バリデーター（validators）：ボットを用いて大量のカード情報を自動で照合・検証し、有効なカードを選別する。

・キャッシュアウター（cash-outers）：有効と判定されたカードでギフト券や暗号資産を購入し、それを換金して利益を得る。

■ NordVPN サイバーセキュリティ専門家 アドリアヌス・ワーメンホーフェンが推奨する、支払いカードを安全に利用するために実践すべき 5 つの対策

① 利用明細を定期的に確認する

利用明細は少なくとも週に 1 回確認し、リアルタイム通知（取引アラート）を有効にしましょう。身に覚えのない請求を見つけたら、カード会社へ速やかに異議申し立てを行い、不正利用の拡大を防ぎます。

② 強力なパスワードを設定する

英字・数字・記号を組み合わせた推測されにくいパスワードを使用し、同じパスワードを複数のサイトで使い回さないでください。

③ ブラウザの自動保存を無効にする

ブラウザにカード情報や住所などを保存すると、マルウェアによりその情報が盗まれるリスクが高まります。自動入力機能はオフにして、重要情報は手入力または安全な管理ツールで管理しましょう。

④ 多要素認証（MFA）を導入する

パスワードだけでなく、デバイス認証、生体認証などを組み合わせることで、不正ログインのハードルを大幅に上げられます。

⑤ ダークウェブ監視ツールを活用する

自分のメールアドレスやカード番号がダークウェブで流出していないかを定期的にチェックしましょう。NordVPN の「Dark Web Monitor™」のような監視サービスを利用すれば、漏洩が確認された際に即時通知を受け取り、被害を早期に食い止めることができます。

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

「たとえ盗難カード情報の価格が上昇しても、カードデータは入門レベルの犯罪者にとって依然として十分に安価です。主要なマーケットプレイスでは、盗まれたカード情報が映画のチケットとほぼ同程度の価格で取引されており、カードはまとめ売りされることも多く、有効期限が長いものは現地で現金化されやすいのが実情です。つまり、犯罪者は数ドルの出費で『映画に行く』か『詐欺やアカウント乗っ取り、他人の資金を現金化するための手段』のいずれかを容易に手に入れられます。

今回の価格上昇は、犯罪者がリスクを負ってでも日本のカードを狙う価値があると判断していることの表れです。しかし、VPN の利用、多要素認証の導入、ダークウェブ監視といった対策を講じれば、被害の多くは防ぐことが可能です。サイバー犯罪者にとってのコストを引き上げることが、最も効果的な防御策です。」

■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。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/