報道関係者各位

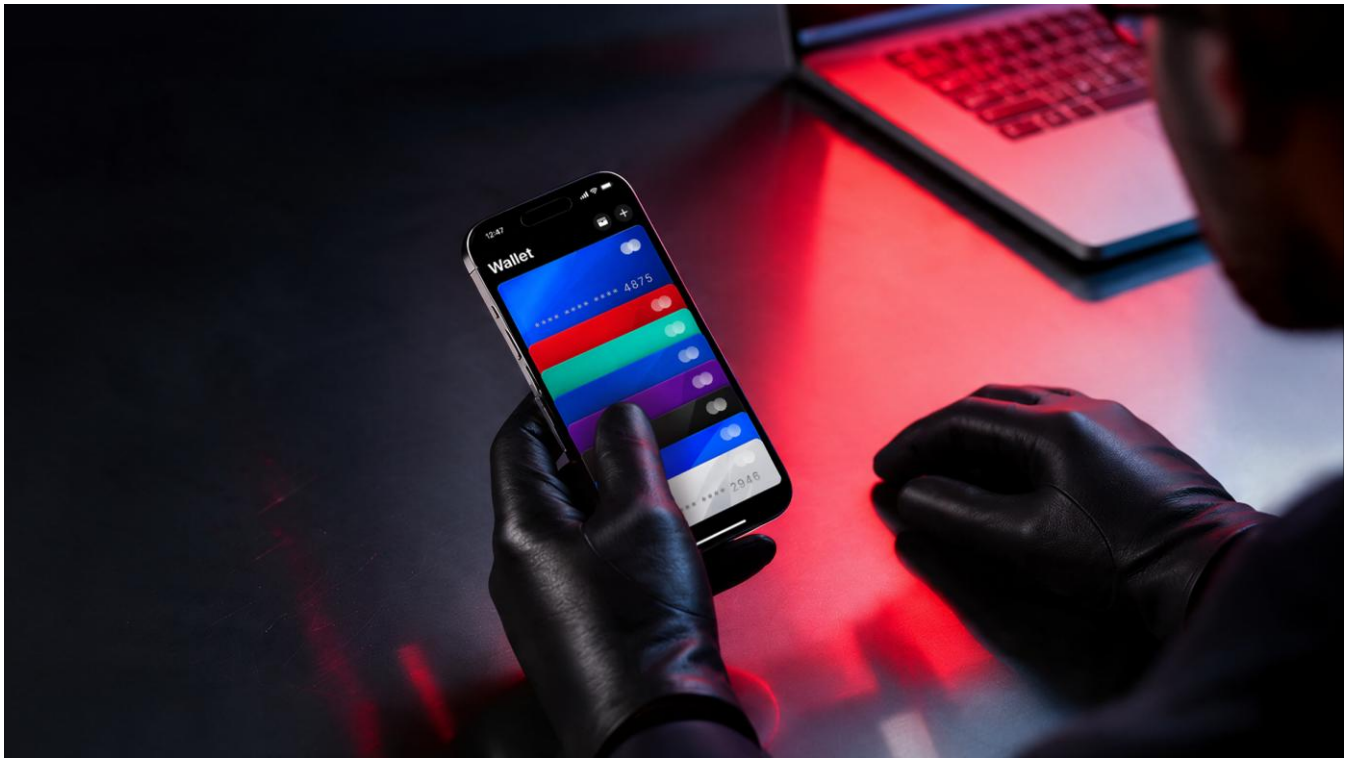
2026 年 11 月 5 日

犯罪者が盗んだカードを「スマホ決済」に入れたがる 4 つの理由　ダークウェブでの関連する話題は 1 年で約 3 倍　NordVPN 調査

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、国内で年間 510.5 億円※1 の被害が出ているクレジットカードの不正利用について、盗まれたカードの使われ方に関する調査結果を発表しました。NordVPN の脅威分析チームがダークウェブ上の議論を分析したところ、盗んだカードを Apple Pay や Google Pay などのスマホ決済に登録する手口に関する話題が、この 1 年で約 3 倍に増え、カード不正の中で最も急速に拡大している手口の 1 つとなっていることが分かりました。

NordVPN は、この手口が広がる背景を 4 つの理由に整理するとともに、カードの持ち主ができる対策を公開しました。

※1 日本クレジット協会の集計による 2025 年（1～12 月）のクレジットカード不正利用被害額。このうち 93%を番号盗用が占める



■ 盗んだカードがスマホ決済に登録される 4 つの理由

NordVPN は、この手口が広がる背景として、次の 4 つを挙げています。

1. **ネット通販では、カード番号だけでは使いにくくなった**
   ネット通販では、カード会社による本人確認（3D セキュア）の導入が進み、カード番号だけでは決済が完了しない場面が増えています。国内でも、2025 年 3 月末までにネット通販事業者への導入が原則として求められました。
2. **スマホ決済なら、本人確認は登録時の 1 回だけ**

スマホ決済では、カードを登録する際にカード会社の本人確認を通過すれば、その後の支払いは登録したスマホの顔認証や指紋認証で行われます。登録時の確認を一度突破すれば、同じカードを繰り返し使うことができます。

3. **カード本体がなくても、店頭で使える**
   IC チップの普及により、磁気ストライプを複製した偽造カードは使いにくくなっています。スマホ決済に登録すれば、カード本体がなくても店頭のタッチ決済で買い物ができます。ダークウェブ上でも、磁気ストライプの複製や古いカード番号帯に関する話題は重要性を失いつつあります。
4. **現金に換えやすい**
   登録したカードで店頭の商品やギフトカードを購入し、転売することで、現金に換えることができます。

■ 狙われるのは「登録時の 1 回」──持ち主に届く確認コード

カードをスマホ決済に登録する際には、通常、登録しようとしている人が正当なカードの持ち主であることをカード会社が確認します。確認には、SMS で届くコードやアプリでの承認などが使われます。

犯罪者はこの確認を突破するため、カード会社や銀行の担当者を装って持ち主に連絡し、確認コードを聞き出す、フィッシングや携帯電話番号を乗っ取る「SIM スワップ」でコードを横取りする、スマホ決済で使えることが分かっているカードを入手する、といった方法を用いています。ダークウェブ上では、確認コードの窃取に関する話題も増えているほか、スマホ決済への登録に成功しやすいとうたう「ウォレット対応」カードも販売されています。

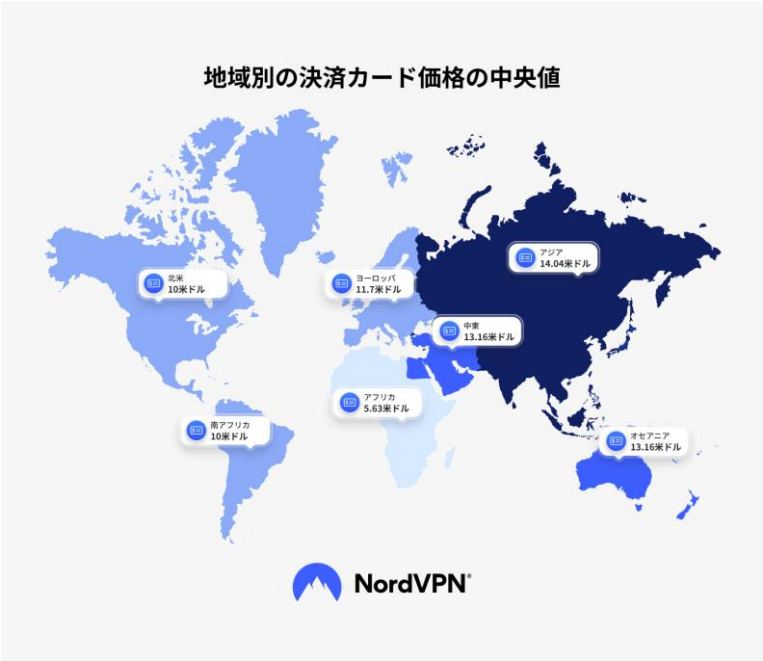
■ 格付けや保証付きで売られる盗難カード

ダークウェブでは、盗まれたカードが「まだ使えるかどうか」で格付けされて売られています。販売者が今後も使えると見込むカードは約 22 ドル（約 3,300 円）※2、「新鮮」とうたうカードは約 35 ドル（約 5,300 円）、「残高 5,000 ドル以上」とうたうカードは約 38 ドル（約 5,700 円）で売られる一方、止められている可能性が高い古いカードは、まとめ売りで 1 枚約 2 ドル（約 300 円）です。販売者の約 8 割は、使えなかった場合の返金や交換の保証を付けています。



カード情報そのものは安価で、分析した出品全体の平均価格は約 10 ドル（約 1,500 円）でした。出品の 7 割以上を占める米国のカードは約 10～12 ドルで、日本のカードは中央値 27 ドル（約 4,000 円）と高い水準でした。分析した中で最大のマーケットプレイスでは、米国の社会保障番号と生年月日が付いたカードの価格の中央値が 18.85 ドルと、これらがないカード（11.70 ドル）より約 6 割高く、氏名や住所、電話番号など本人の情報が 3 つ以上付くと 23 ドルを超えました。カードが使えなくなった後も、本人の情報が残っていれば「デッド・フルズ」と呼ばれ、1 件約 1 ドル（約 150 円）で取引されています。

※2 1ドル=150 円で換算



https://nordvpn.com/ja/research-lab/stolen-payment-cards-wallet

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

「アンダーグラウンド市場では、単に誰かのカード情報を持っていることよりも、その情報を実際にお金に換えられるかどうかが重視されるようになっています。犯罪者は、本人確認やアカウントへのアクセス、カードにひもづく個人情報など、カードの周辺にある最も弱い部分を狙うようになっています。」

「カードの不正と、個人情報の不正利用は重なり合うようになっています。決済カードはすぐに止めることができますが、生年月日や住所、社会保障番号といった個人情報は、カードが使えなくなった後も長く出回り続けるおそれがあります。」

■ カードの持ち主ができる対策

NordVPN は、カードの不正利用を防ぐため、次の対策を推奨しています。

1. **利用通知を有効にする**
   不審な支払いにすぐ気づけるよう、カードの利用通知を有効にしてください。
2. **確認コードは、予期せぬ連絡の相手に教えない**
   相手がカード会社や銀行を名乗っていても、突然の電話やメッセージで求められた確認コードは伝えないでください。
3. **「新しい端末に追加されました」という通知を軽視しない**
   身に覚えのない登録の通知は、カードが他人のスマホに登録されたサインの可能性があります。
4. **見覚えのない登録があれば、すぐにカード会社に連絡する**
   カードの停止とあわせて、そのカードにひもづくスマホ決済の登録（トークン）を無効化できるか確認してください。

■ 調査概要

調査主体：NordVPN 脅威分析チーム（脅威エクスポージャー管理プラットフォーム「NordLayer Intelligence」のデータを使用）

調査対象：9 つのダークウェブマーケットプレイスにおける 24,000 件以上のカード出品、犯罪者のフォーラムおよび Telegram チャンネルにおける 14 テーマ・約 3,900 件の投稿

調査期間：マーケットプレイスのデータは 2026 年 2 月に収集。議論の推移は 2025 年第 3 四半期～2026 年第 3 四半期（途中まで）を分析

注：価格は比較のため米ドルに換算しています。議論の増減は、会話量全体の増加と比較して算出しています。重複する出品や再投稿された広告は除外しています。

■ NordVPN について

NordVPN は、世界中の何百万人ものインターネット利用者から信頼されている、オールインワンのデジタルプライバシー・セキュリティアプリです。NordVPN アプリは、世界最先端の VPN と次世代型アンチウイルス、ダークウェブモニター™（Dark Web Monitor™）などのセキュリティ機能を組み合わせ、利用者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。フィッシング、詐欺、悪質なウェブサイト、トラッカー、迷惑な広告、マルウェアからの保護に役立ち、オンラインプライバシーの強化を支援します。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/