報道関係者各位

2026 年 9 月 17 日

# なりすまし詐欺は「見た目」から「信用」の偽装へ
# NordVPN、“本物らしさ”を多重に作り込む 2 つの大規模詐欺キャンペーンを確認
## ～有料広告、高評価レビュー、公式ストア風ページ、政府機関――「安心材料」そのものが詐欺の手口に～

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）の脅威インテリジェンスチームは、著名ブランドや公的機関への信頼を悪用した、2 つの大規模な詐欺を確認しました。

今回の調査で特徴的だったのは、名称やロゴ、ウェブサイトの外観を模倣する従来のなりすましにとどまらず、利用者が正規のサービスだと判断する際の“安心材料”まで悪用されていた点です。複数の要素を組み合わせることで“本物らしさ”を補強し、利用者の警戒心を下げる手法が確認されました。

**■ 確認された詐欺①：Facebook・Instagram の有料広告から、無許可オンラインカジノへ誘導**

**【手法】**

被害者との最初の接点は、Facebook・Instagram 上に配信される有料広告です。

広告には、Google Authenticator、Capital One、Disney+、Duolingo、デルタ航空など、実在する有名ブランドが使用されています。広告をタップすると、そのブランドの正規アプリを装った偽の Google Play ページが表示されます。

偽ページにはブランドロゴや偽の開発者名に加え、「4.9」の星評価や数千件の捏造レビューまで掲載されています。

本物の Google Play ページとの重要な違いの一つは、アドレスバーの URL が「play.google.com」ではない点です。ページ上の「インストール」をタップしても、通常のアプリはダウンロードされません。代わりにブランド名とアイコンを装った PWA（プログレッシブウェブアプリ）がホーム画面に追加され、そこから無許可のオンラインカジノへ誘導されます。

**【今回のポイント】広告審査をすり抜けるための「クローキング」**

この詐欺では、偽サイトの見た目だけでなく、利用者がそこへたどり着くまでの過程にも“本物らしさ”が作り込まれていました。入口となる SNS の有料広告から、ブランドの知名度、高評価や多数のレビュー、公式ストアを模したページまで、利用者が安心しやすい要素が一連の導線上に配置されています。

さらに、広告審査をすり抜けるための「クローキング」と呼ばれる仕組みも確認されました。アクセスしてきた相手を判別し、広告審査などに使われる自動スキャナーには無害なページを表示する一方、実際のターゲットには無許可カジノへの誘導ページを表示します。つまり、広告をチェックする側と実際の利用者とで異なるページを表示し、詐欺広告を発見されにくくする仕組みまで組み込まれていました。

**【数字で見る規模】**

- **400 以上**：なりすましに悪用されたブランド
- **約 1,000 人**：偽広告キャンペーンを運用するアフィリエイト
- **250 以上**：アフィリエイトが所属する広告運用グループ
- **7,261 回**：実際のユーザーに無許可カジノへの誘導ページが表示された回数

NordVPN の調査では、偽ページの作成や広告審査を回避する機能を提供するプラットフォーム、その仕組みを利用して広告を運用するアフィリエイト、さらに登録や入金に応じて報酬を支払う無許可カジノや CPA ネットワークが存在し、複数の役割に分かれた運営構造も確認されています。

**■ 確認された詐欺②：航空会社や政府機関になりすまし、不正アプリでスマートフォンを遠隔操作**

**【手法】**

被害者には、SMS、WhatsApp、SNS などを通じて、実在する航空会社や政府機関を装ったメッセージが送られます。内容は、航空会社の求人、税金の還付、身分証の更新、年金の確認、大幅に割引された航空券などです。

リンクをタップすると、なりすました組織の公式サイトそっくりに作られたウェブサイトが表示され、Android アプリのインストールを求められます。しかし、そこでインストールされるのは正規アプリではなく、攻撃者がスマートフォンを遠隔操作するための不正アプリです。不正アプリはバックグラウンドで動作し続け、端末を再起動しても停止しません。SMS や連絡先、通話履歴の読み取り、画面のキャプチャ、音声の録音、カメラの起動などの権限を要求します。

特に危険なのが SMS の読み取りです。銀行などから送られるワンタイムコードを攻撃者が取得することで、二段階認証を突破し、被害者の銀行アプリへのログインや取引の承認に悪用される可能性があります。

**【今回のポイント】サイトだけでなく、「実際に届きそうな用件」まで作り込む**

この詐欺では、航空会社や政府機関のサイトを本物そっくりに模倣するだけでなく、被害者に最初に届くメッセージの内容まで、なりすました相手に合わせて作り込まれています。

政府機関であれば税金の還付や年金確認、航空会社であれば求人や割引航空券など、その組織から実際に届いても不自然ではない用件を利用しています。さらに、誘導先の偽サイトもターゲットとなる地域の言語に合わせて作られており、メッセージを受け取ってからアプリをインストールするまで、違和感を抱きにくい導線が作られていました。

**【数字で見る規模】**

**・65 以上**：なりすましに悪用されたブランド・組織

**・100 以上**：キャンペーンに関連するドメイン

**・10 件**：NordVPN が分析した不正アプリ

**・2025 年 8 月以降**：少なくとも確認されている活動期間

**・世界 7 地域**：アジア、アフリカ、オーストラリア、中東、中南米、欧州などで確認

なりすましの対象には、フィリピン航空、マレーシア航空、エア・インディアなどの航空会社のほか、インドネシアの税務当局「Coretax」、フィリピンの社会保障制度、タイの社会保障制度、ベトナムの社会保険機関・保健省などが含まれています。

**■ 2 つの詐欺に共通するのは、「本物」と判断する手がかりの悪用**

今回確認された 2 つの詐欺は、誘導方法や最終的な被害は異なります。一方で共通しているのは、企業や公的機関の名称や見た目を模倣するだけでなく、利用者が「これは本物だろう」と判断するまでの過程そのものに働きかけている点です。

一つの偽物を精巧に作るだけではなく、そこへ至るまでに「信用する理由」を積み重ねる。今回の 2 つの調査では、そうした“本物らしさ”の作り込みが確認されました。

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

「私たちが目にしているのは、いわば“信頼のロンダリング”です。犯罪者は、正規企業が長年かけて築いてきた信頼を横取りし、自分たちの目的のために利用しています。被害者が異変に気づいたときには、既に聞いたこともないカジノに入金してしまっているのです。

また、航空会社や政府機関を装い不正アプリをインストールさせる詐欺が危険なのは、餌があまりにも“普通”であることです。税還付や航空券の割引は脅威には感じられず、むしろ良い知らせのように感じられます。一度インストールしてしまえば、そのスマートフォンはもう自分のものではありません。攻撃者は画面を見て、SMS の認証コードを読み取り、内部から口座を空にしていきます。」

**■「安心材料」を鵜呑みにしないために、今日からできる 3 つの自己防衛策**

今回のような詐欺では、「怪しいサイトを避ける」だけでは十分とは限りません。一見すると安心できそうな要素が複数揃っていても、一つの情報だけで安全性を判断せず、別の経路から確認することが重要です。

**1. 広告やメッセージのリンクから、そのまま手続きを進めない**

知っている企業や公的機関からの案内に見えても、広告やメッセージに記載されたリンクからそのままログインやインストールを行わないでください。企業や公的機関の公式サイト・公式アプリを自分で開き、同じ案内が掲載されているか確認しましょう。

**2. アプリは公式ストアを自分で開いて検索する**

ウェブサイト上に公式ストアのようなページが表示されても、そこにある「インストール」ボタンをそのまま押さず、Google Play や App Store を直接開いてアプリを検索してください。ブラウザ上で Google Play に見えるページが表示された場合は、URL が正規のものか確認することも重要です。

**3. 一つの“安心材料”だけで安全だと判断しない**

知っている企業名が使われている、評価が高い、サイトがきれいに作られているといった一つの要素だけでは、安全性を判断できません。送信元、URL、公式サイト上の情報、アプリが要求する権限など、複数の情報を別々に確認してください。

## ■ 調査概要

### 偽広告から無許可オンラインカジノへ誘導する詐欺

NordVPN の脅威インテリジェンスチームは、偽のアプリストアページ群に共通するテンプレートの特徴を特定し、稼働中のネットワークを調査しました。ネットワークトラフィック解析や JavaScript の分析を通じ、個々のアフィリエイトアカウントと広告キャンペーン、誘導先のカジノ、Facebook ビジネス広告ピクセルとの関連を調査。ドメイン登録記録やホスティング事業者データ、コード上の手がかりなどを用いてネットワークの構造を分析しました。

### 航空会社・政府機関を装い不正アプリをインストールさせる詐欺

NordVPN の脅威インテリジェンスチームは 10 件の不正アプリを分析し、署名証明書をもとに 7 つのグループに分類しました。また、2025 年 8 月以降に使用された 100 以上の関連ドメインを特定。各アプリが要求する権限や内部コード、ドメイン登録・ホスティングのパターンなどを分析し、詐欺に使用されるインフラとなりすまし対象を調査しました。

## ■ NordVPN について

NordVPN は、世界中で何百万人ものインターネットユーザーに利用されている、デジタルプライバシーとセキュリティのためのオールインワンアプリです。NordVPN アプリは、世界最高水準の VPN、次世代アンチウイルス、Dark Web Monitor™をはじめとするセキュリティ機能を統合し、ユーザー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。また、フィッシング、詐欺、悪質なウェブサイト、トラッカー、迷惑広告、マルウェアなどの脅威からユーザーを保護し、オンラインプライバシーの強化にも貢献します。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/ |