

年末商戦を狙う偽配送サイト急増！

NordVPN が「宅配詐欺」に関する調査を発表

～なりすましの偽配送サイトが 1 ヶ月で 86% 増、日本でも大手物流会社が注意喚起～

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、年末年始の商戦に伴い、配送追跡を装うなど宅配関連のサイバー攻撃に関する最新の調査を発表しました。また、詐欺被害から身を守る 4 つのポイントもあわせて紹介します。



■実施背景

年末年始はクリスマスやお歳暮、福袋などでオンラインショッピングの利用が急増し、それに伴い宅配便の配送需要もピークを迎えます。多くの消費者は、複数の荷物を待つ状況では、個々の配送状況を正確に把握することが難しく、正規の通知と偽装メッセージの判別が困難になる傾向があります。こうした状況を踏まえ、NordVPN はセキュリティツール「脅威対策 Pro」のデータをもとに、配送業者を装ったフィッシング詐欺の最新動向を分析しました。

■調査概要

調査機関：NordVPN「脅威対策 Pro」

データ収集時期：2025 年 8 月 1 日～10 月 31 日

調査方法：対象期間内に「脅威対策 Pro」が検知した匿名化データを分析

※本文中に記載しているブランド名は、模倣被害が多かった傾向を正確に伝えるためのもので、NordVPN はいずれのブランド所有者とも関係していません。

■配送業者を装う偽サイトが1ヶ月間で86%増、SMS詐欺(スミッシング)経由の被害が多数

NordVPN「脅威対策 Pro」のデータによると、配送業者を装った悪質なウェブサイト数は、9月と比べて、10月では先月比86%増加しました。最もなりすまし被害が多かったブランドはDHLで、偽サイトは前月比206%増を記録しています。

NordVPNが実施した意識調査では、回答者の38%が配送関連の詐欺に遭遇した経験があり、その多くがSMS経由という結果も明らかになりました。米国連邦取引委員会(FTC)のデータによると、メッセージ詐欺による損失額は2024年に4億7,000万ドルに達し、2020年の5倍以上の規模に拡大しています。



■日本でも配送系フィッシング詐欺に警戒を、年末を前に昨年水準超え

配送業者を装った詐欺の手口は、日本国内でも多数確認されています。こうした詐欺は、「お荷物をお届けにあがりましたが、不在の為持ち帰りました」といった不在通知を装い、偽のサイトへ誘導する「フィッシング」と呼ばれる手口を起点とするケースが多くみられます。主要物流各社も、自社を装った不審なSMSやメール、電話などについて公式に注意喚起を行っています。

フィッシング対策協議会が毎月公表している月次報告書によると、宅配便の不在通知などを装った「配送系」フィッシングは、前年同月にあたる2024年12月時点で全体の約9.8%を占めていました。

さらに、最新の2025年10月時点では、配送系フィッシングが全体の約10%に達しており、年末を迎える前の段階ですでに昨年末の水準を上回っていることが確認されています。特に宅配便の「不在通知」を装ったSMS(スミッシング)が継続的に報告されています。

近年は生成AIの悪用により、SMSごとに異なる文面が作成されるケースも確認されており、従来のように同一文面を手がかりに真偽を見分けることが難しくなっています。年末セールなどに伴い配送関連の通知が増える時期には、こうした手口による被害の拡大が懸念されています。

■ NordVPN 最高技術責任者(CTO) マリウス・ブリエディスが推奨する、配送詐欺被害を防ぐためのチェックポイント

① 追跡リンクはクリックしない

テキストやメール内のリンクは避け、配送業者の公式サイトやアプリに追跡番号を直接入力するほうが安全です。

② 「緊急」のメッセージをまず疑う

「即時の対応が必要」など催促のある言葉は詐欺に繋がりがちです。正規の業者がメッセージ内のリンクを経由して即時の支払いを求めることは通常ありません。

③ 送信者の詳細を細かく確認する

詐欺師は電話番号やウェブサイトを実物に見せる「スプーフィング」を使用し、ウェブアドレスの文字や記号を1つだけ変えて騙そうとする手口があります。そのためきちんと細部まで確認する必要があります。

④ 再配達手数料や個人情報の要求に応じない

「荷物を配達するために情報や手数料が必要」などメッセージが届いた場合でも、リンクを開いたり返信したりしないことが重要です。不審なメッセージを受け取った際は、配送業者の公式サイトや公式窓口で事実確認を行い、必要に応じて報告してください。

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

「年末のショッピングピークに合わせて、スミッシングやなりすましによる配送詐欺が急増しています。近年注目される企業へのサイバー攻撃なども、基本的な情報さえあれば、簡単に標的型フィッシングが実行できてしまうかを改めて確認しました。不審なリンクをクリックしないことはもちろんですが、強力なパスワードの設定、二要素認証の利用、そしてVPNによる保護を有効にするなど、基本的なセキュリティ対策を徹底することが日々の生活においても非常に重要です。」

■ 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。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/>