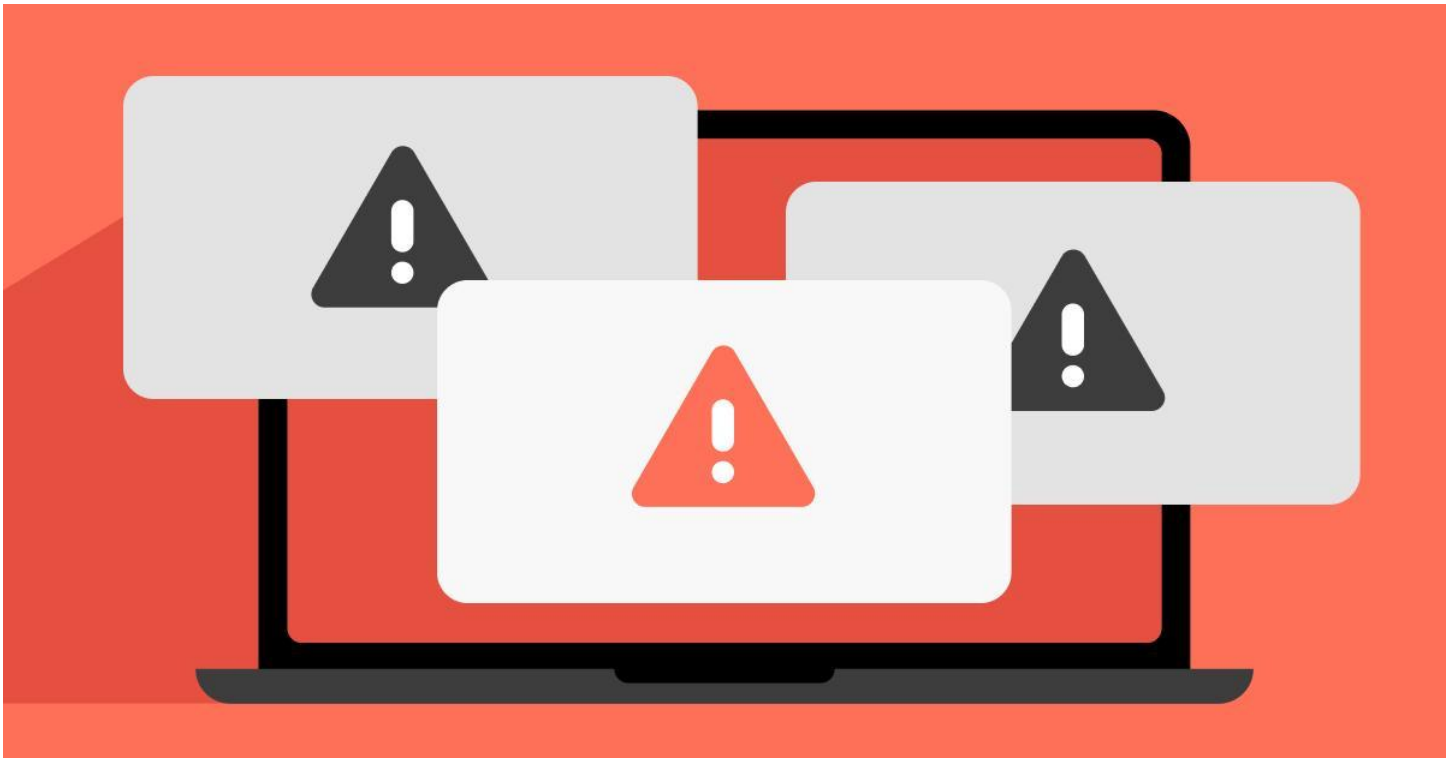
報道関係者各位

2026 年 4 月 23 日

# AI 時代に巧妙化する採用詐欺に注意！
# NordVPN が大手企業を装う新しい手口を公開
## ～偽の求人メール 1 通で SNS 乗っ取り・情報流出に～

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、同社の脅威インテリジェンス研究部門の調査により、世界的な大手企業を装い、求職者を標的に SNS アカウントの認証情報を窃取する新たな採用詐欺の手口を発表しました。

本調査では、Meta、Disney、Coca-Cola、Spotify などの著名企業の採用担当者を装ったメールを起点に、本物と見分けがつかない偽求人サイトへ誘導し、最終的に Facebook アカウントを乗っ取る多段階型の攻撃の実態が明らかになっています。こうした手口は世界的に確認されており、日本の求職者にも広がる可能性があります。



**■調査背景**

近年、生成 AI の普及などを背景に、フィッシング詐欺をはじめとするサイバー攻撃は、実在する企業を精巧に模倣した多段階型の攻撃へと巧妙化しています。

こうした中、企業の Web サイトや採用情報、メール文面などを自然に再現した詐欺も増えており、見分けが難しくなる傾向が指摘されています。特に就職・転職活動中の求職者は、見知らぬ相手からの連絡に応じやすく、個人情報を提供することへの警戒心が緩みやすい傾向があります。攻撃者はこうした状況を悪用し、採用プロセスに見せかけた手口で SNS アカウントの認証情報を狙っています。こうした実態を明らかにするため、NordVPN の脅威インテリジェンス研究部門は調査を実施しました。

**■調査概要**

調査名称　：　NordVPN 脅威インテリジェンス研究部門

調査機関　：　NordVPN・NordStellar

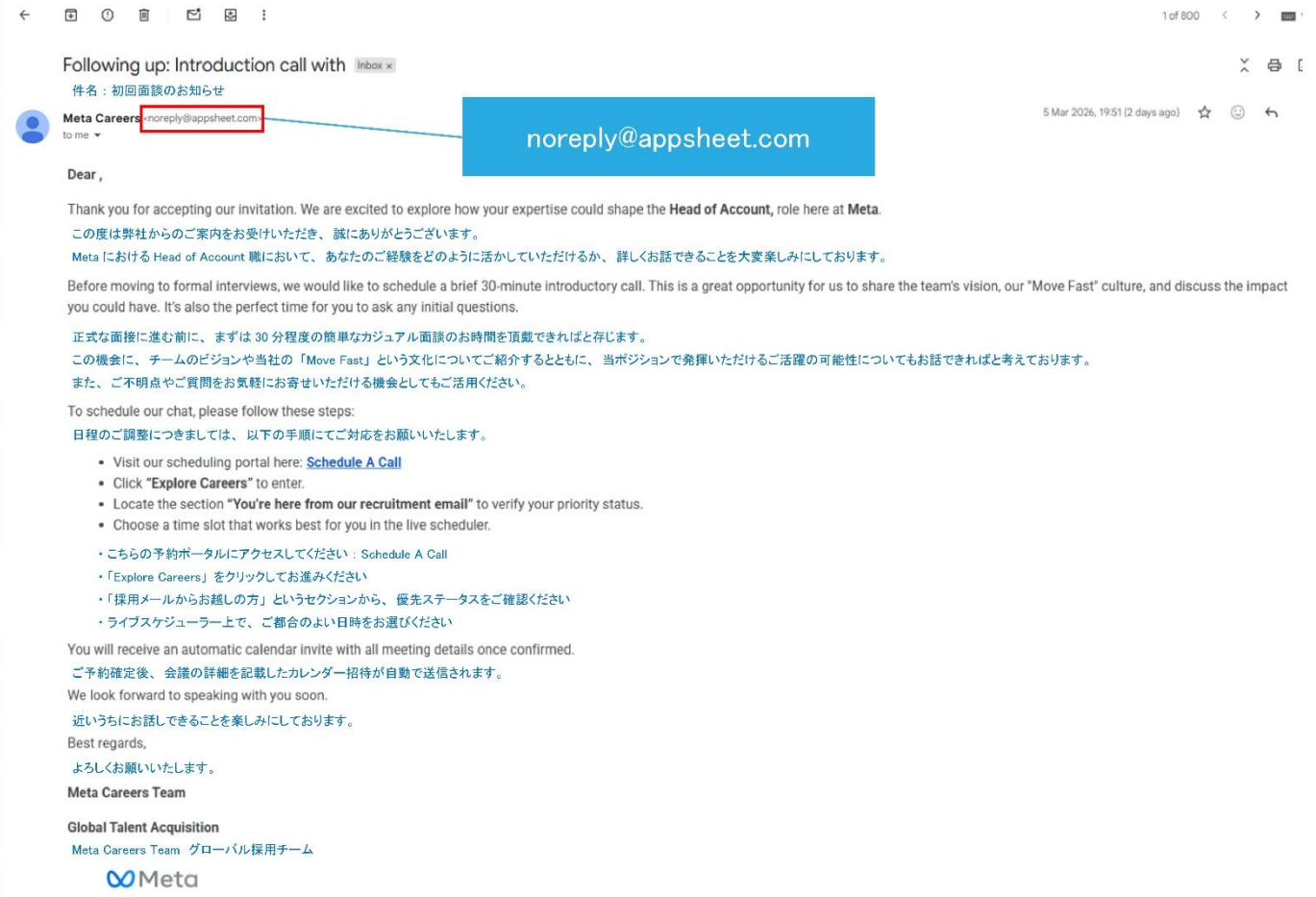
調査日　　：　2026 年 3 月 31 日

調査方法　：　主要検索エンジンへの高度な検索文字列の適用、および IoT 検索エンジン・Fofa.io・Shodan.io などを活用したドメイン・サービス・ポートの特定

**■採用メールから始まる、3 段階の詐欺の手口**

今回確認された詐欺は、複数のステップを経て巧妙に被害者を誘導する手口です。一見すると通常の採用プロセスと区別がつかず、注意深いユーザーでも気づきにくいのが特徴です。

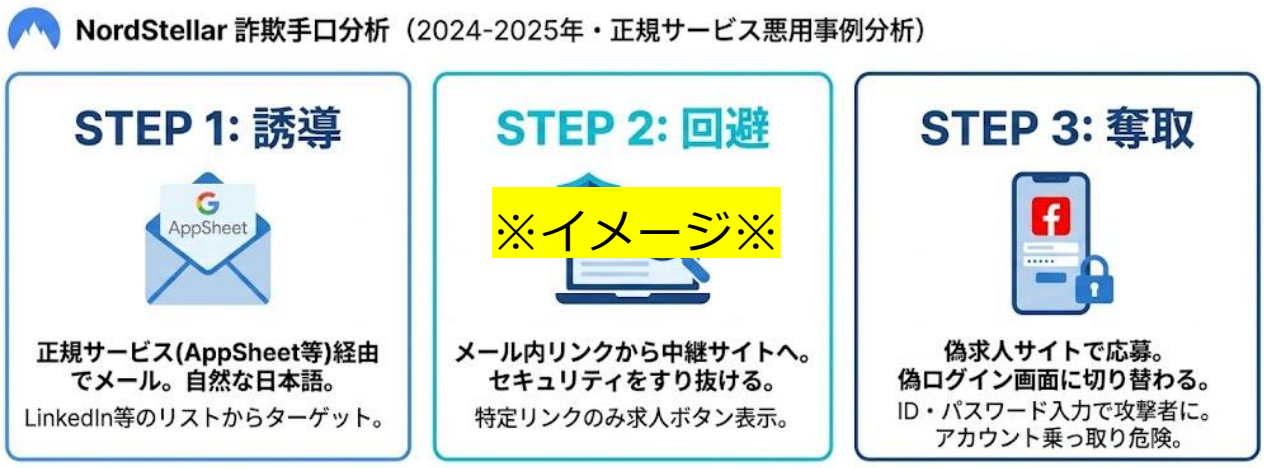
詐欺は Google AppSheet など正規サービスを経由して送られてくる採用メールから始まります。文面は自然な日本語で書かれており、実際の採用連絡と見分けがつきません。AppSheet とは Google が提供する正規のサービスであるため、送信元アドレスが「appsheet.com」となり、スパムフィルターに検知されにくく、受信者も疑いを持ちにくい点が悪用されています。




送付先のリストは LinkedIn などから収集されたか、過去の情報漏洩データを利用したものと考えられます。

メール内のリンクをクリックすると、中継サイト（例：careers.meta-findyourjob[.]com）に誘導されます。このサイトにはセキュリティ対策をすり抜ける仕組みが組み込まれており、ウイルス対策ソフトや検索エンジンのクローラーが直接アクセスしても無害なページしか表示されません。詐欺メール内の特定のリンクを経由した場合にのみ「求人を検索

する」ボタンが現れる仕掛けになっています。
ボタンをクリックすると、各企業に合わせてつくられた偽の求人サイトに誘導されます。一見すると本物の採用ページと変わらず、実際の求人情報まで掲載されています。求職者が応募ボタンを押した瞬間、偽の Facebook ログイン画面に切り替わり、入力した ID とパスワードが攻撃者に渡る仕組みです。




**確認された偽サイトの例**

・Meta ：plus.jobfusion-mt[.]com ／ official.professionlaunch-mt[.]com
・Coca-Cola：careers.coca-contactnow[.]info
・Spotify：connect.spotifycareerapply[.]com
・Disney：jobquest.wdcfutureste ps[.]com

**■NordVPN プロダクトディレクター ドミニンカス・ヴィルビツカスが推奨する、採用詐欺から身を守る 3 つの対策**

**①ログイン前に URL を必ず確認する**

正規の企業は自社の公式ドメインで採用ページを運営しています。見慣れない外部サイトへの誘導や、「Facebook でログイン」を求める画面が出たときは、その URL が本当に facebook.com かどうかを確認してください。少しでも違和感があれば入力を止めることが重要です。

**②すべての SNS アカウントで二要素認証（2FA）を有効にする**

パスワードが漏れても、二要素認証が設定されていれば不正ログインを防ぐことができます。設定に数分かかるだけで、被害を大きく減らせます。

**③突然の求人連絡には慎重に対応する**

メールや SNS で突然届く求人オファー、とりわけ急いで応募するよう促すものは要注意です。気になる場合は、その企業の公式サイトから採用情報を直接調べる習慣をつけてください。

**■NordVPN プロダクトディレクター ドミニンカス・ヴィルビツカスのコメント**

「求職活動中は、知らない相手からの連絡に応じることが珍しくありません。攻撃者はその状況を利用し、本物と見分けがつかないほど精巧な偽サイトを使って個人情報を詐取しています。今回の手口で特に注意が必要なのは、セキュリティ対策ソフトをすり抜けるように設計されている点です。URL の確認と二要素認証の設定を習慣にすることが、自分を守るうえで最も確実な方法です。

また、生成 AI の進化により、攻撃者は本物のように見える採用メールや偽の求人ポータルを簡単に作成できるようになっています。これらのツールがより身近になるにつれ、採用詐欺はよりスケーラブルに、よりターゲットを絞った形で広がり、正規の採用プロセスとの区別が一層難しくなるでしょう。だからこそ、ブランド名や見た目だけを信頼するのではなく、正確な URL を確認することがこれまで以上に重要になっています。」

**■ 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 135 カ国 209 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/

ナショナル・プライバシー・テスト（National Privacy Test）について: https://nationalprivacytest.org/jp