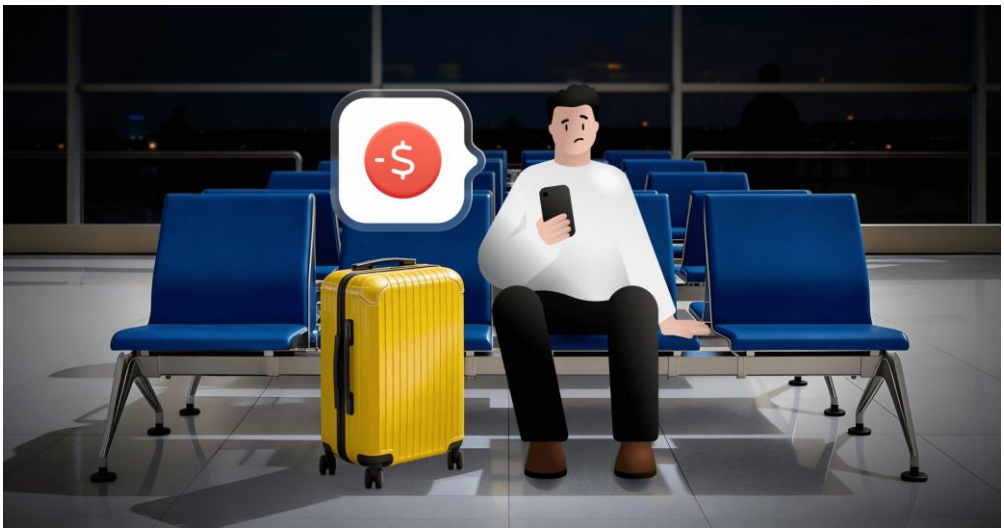
報道関係者各位

2025 年 12 月 24 日

年末年始に狙われるマイルアカウント、ダークウェブでは 115 円から売買
NordVPN と Saily が共同で過去 5 年間のダークウェブ投稿を分析
～旅行業界を狙うサイバー犯罪の実態が明らかに～

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、グローバル eSIM サービス「Saily」との共同で、過去 5 年間にダークウェブ上で投稿されたコンテンツを分析し、ダークウェブ上における航空会社のマイレージプログラムやホテルの会員ポイントなど、優良顧客向け特典が付与される会員アカウントの売買実態を調査しました。マイルやホテルポイントは換金性が高く、直前の旅行予約やギフトカードへの交換にも利用できることから、サイバー犯罪者にとって収益性の高い標的となっています。

調査の結果、盗まれたアカウントがわずか 115 円から取引されているほか、ダークウェブ上で確認された航空会社を狙ったサイバー犯罪に関する議論のうち、54%以上が大手航空会社 8 社に集中していることが明らかになりました。こうした不正行為は、航空会社やホテル側の対応負担が増すだけでなく、旅行者が気づかないうちにマイルやポイントを失ってしまうケースも少なくありません。
年末年始の旅行シーズンを迎える中、NordVPN では、こうした被害を防ぐために個人が取るべき対策についてもあわせて紹介します。



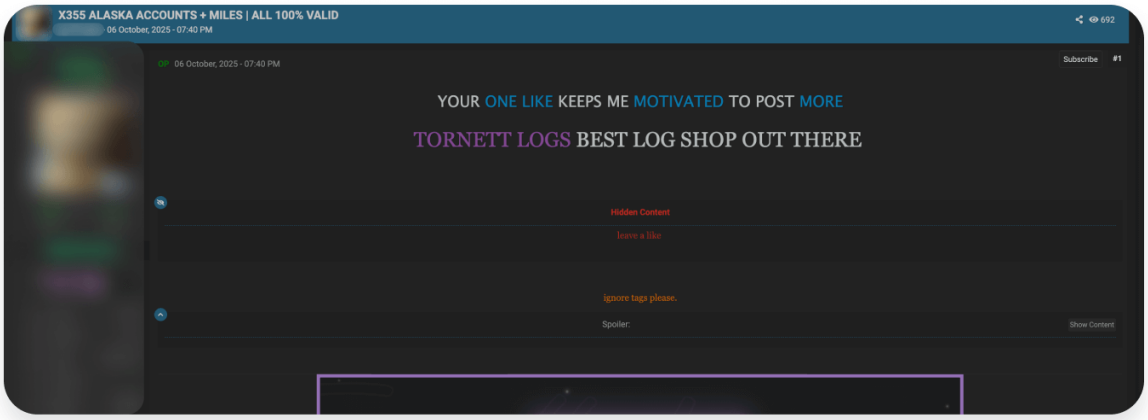
調査概要

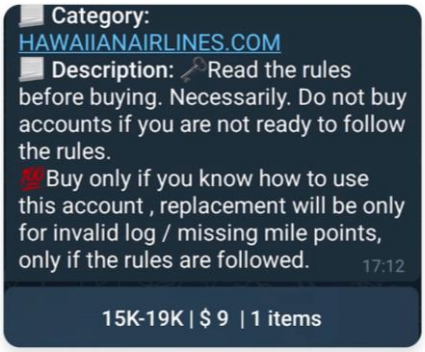
本調査は、NordVPN のサイバーセキュリティ専門家が、eSIM アプリ「Saily」のチームと共同で実施したもので、ダークウェブ上におけるロイヤリティ関連データの露出状況に焦点を当てています。調査にあたっては、NordStellar の「Dark Web Search」ツールを使用し、AI を活用したフィルタリング技術によって、過去 5 年間に投稿されたデータを収集・分析しました。データ収集は、ダークウェブ検索の設定、航空会社関連投稿の分析、ホテル関連投稿の分析、旅行関連データベースの流通状況の分析といった複数の工程を通じて行われました。なお、サンプル数が限られていることや、ダークウェブのデータ環境が断片的であるという特性を踏まえ、本調査は包括的な統計データではなく、旅行およびロイヤリティプログラム関連データの露出実態を示す参考情報（示唆）として位置づけられます。

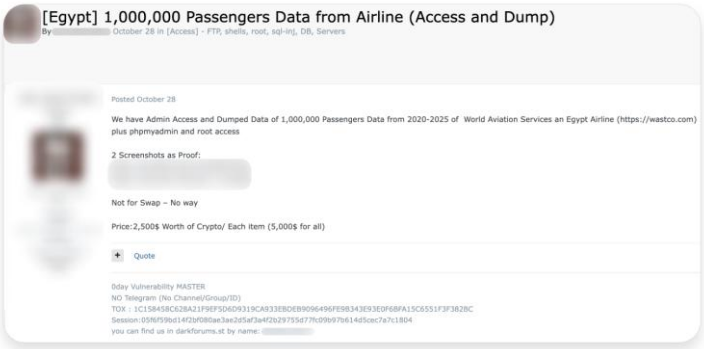
調査対象：ダークウェブ上で議論・取引されている主要な航空会社およびホテルチェーンのデータ
分析項目：航空会社のマイレージプログラムやホテルの会員ポイントなど、優良顧客向け特典が付与される会員アカウントの出品価格、サイバー犯罪の標的となっている企業ブランドの傾向など
調査期間：2025 年 11 月 19 日から 2025 年 12 月 4 日
調査機関：NordVPN、Saily

■調査結果：航空会社のマイレージアカウント売買について
「travel」「airline」といったキーワードを用い、ダークウェブ上で航空会社への不正行為や、会員アカウント・データ侵害に関連する投稿を調査しました。収集した投稿には、スパムや重複投稿、調査対象と無関係な内容も多く含まれていたため、AI を活用してこれらを除外しました。その結果、航空会社を標的としたサイバー犯罪に関する議論が行われている投稿が、1,045 件確認されました。
これらの投稿や取引情報によると、航空会社のマイレージアカウントは、数十万マイルを保有している場合であっても、0.75 ドル～200 ドル（約 115 円～3 万円）という低価格で取引されています。また、ダークウェブ上で確認された航空会社を巡るサイバー犯罪に関する投稿や議論を分析した結果、その 54%以上が、米国・アジア・中東を拠点とする大手航空会社 8 社に関する言及であることが判明しました。これは、航空関連の不正行為について、特定の企業名が集中的に話題に上っている状況を示すものです。実際にダークウェブ上では、航空会社名や保有マイル数、取引条件などを明示した形で、ロイヤルティアカウントが売買されている投稿が確認されています。

以下は、NordVPN と Saily の調査過程で確認された投稿例です。







<u>※これらの画像は、NordVPN と Saily の調査過程で確認されたダークウェブ上の投稿例をもとに、個人情報や特定可能な要素を加工・削除したものです。特定の航空会社や個別事案の被害を示すものではありません。</u>

これらの投稿は、航空会社の会員アカウントが偶発的に流出しているのではなく、一定の手口によって継続的に不正取得されている可能性を示しています。調査で確認された、主なアカウント情報の流出手口は以下の通りです。

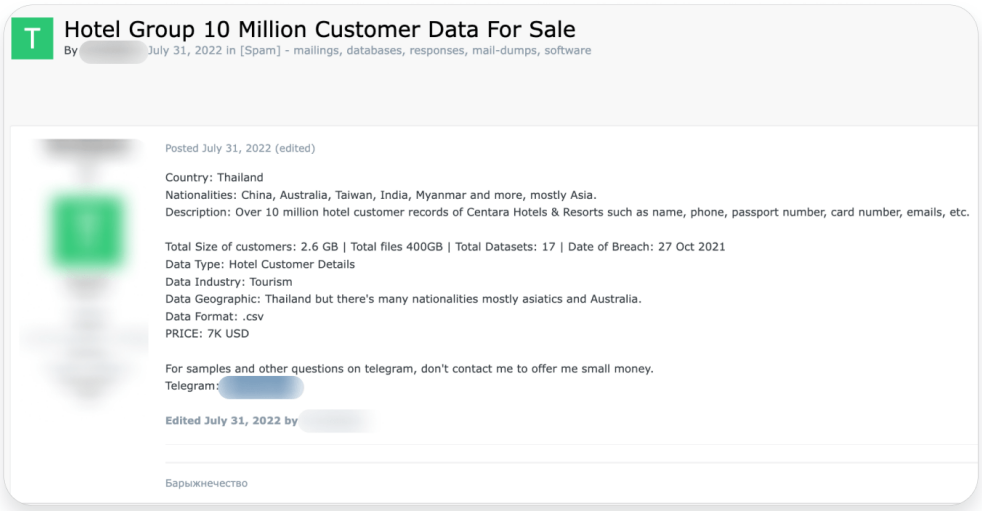
- **フィッシング詐欺**：航空会社を装った偽メールや偽サイトでログイン情報を入力させる手口
- **データ侵害**：航空会社のシステムがハッキングされ、顧客データベースが流出するケース
- **クレデンシャル・スタッフィング**：他サービスで漏洩したパスワードを使い回している利用者を狙い、不正ログインを試みる手口

不正に取得されたマイレージアカウントは、正規の利用者になりすまして、無料航空券の予約や座席のアップグレード、各種特典の利用などに使用されるケースが確認されています。これらの不正取引は正規の利用履歴に紛れ込むため、被害者が気づくまでに数週間かかることも珍しくありません。

■調査結果：ホテルの顧客データベース売買について

航空会社のマイレージアカウントに加え、ホテルに関連する顧客情報がダークウェブ上で取引されている例も確認されています。「hotel」をキーワードに、ダークウェブ上の投稿や取引情報を分析した結果、ホテルに言及した投稿は 551 件確認されました。これらの投稿や取引情報を分析したところ、ヒルトン、マリオット、IHG などの世界的なホテルチェーンに言及するケースが複数見られました。中でもヒルトンに関する言及は、ダークウェブ上で確認されたホテル関連の投稿の約 34%を占めており、特定の高級ホテルチェーンが集中的に話題に上っている状況がうかがえます。

ダークウェブで売買されているホテル関連のデータは、会員アカウント単体にとどまらず、顧客データベース単位で流通しているケースもあります。これらのデータには、宿泊客の氏名やメールアドレス、滞在履歴といった基本情報に加え、一部ではパスポート番号などの個人情報や、会員ポイント情報が含まれている例も確認されました。こうしたデータベースは、内容によっては最大 3,000 ドル（約 47 万円）で取引されている事例があります。
これらの顧客情報が不正に流通することで、会員ポイントの不正利用にとどまらず、なりすましや詐欺などの二次被害につながるリスクも指摘されています。



※本画像は、NordVPN と Saily の調査過程で確認されたダークウェブ上の投稿例をもとに、個人情報や特定可能な要素を加工・削除したものです。特定の航空会社や個別事案の被害を示すものではありません。

■NordVPN 最高技術責任者（CTO） マリユス・ブリエディスが推奨する、旅行前に押さえたい 5 つの防御策

① パスワードの使い回しを回避
複数のアカウントで同じパスワードを使用すると、個人情報盗難のリスクが高くなります。アカウントごとに強力でユニークなパスワードを設定し、多要素認証（MFA）を有効にすることで、不正アクセスのリスクを低減することが可能になります。

② アカウント履歴を定期的に確認
アカウントのログイン履歴や、ポイント利用履歴を定期的に確認することが重要です。身に覚えのない不審な操作が確認された場合は、直ちにパスワードを変更するなどの対応が必要です。

③ 旅行の前後は特に入念にチェック
旅行中は、通常とは異なるネットワーク環境からアカウントにアクセスする機会が増えるため、リスクが高まります。旅行の前後には必ずアカウントの状態を確認する習慣をつけることが推奨されます。また、ポイントの不正利用に関する通知アラートを設定することも有効です。

④ 公共 Wi-Fi 利用時は VPN を利用
空港やホテルの公共 Wi-Fi は便利ですが、すべてのホットスポットが安全とは限りません。通信内容を暗号化する VPN（仮想プライベートネットワーク）を使用することで、第三者によるデータの盗聴や傍受を防ぐことができます。

⑤ 旅行用 eSIM を活用してリスクを低減
信頼性の低い公共ネットワークへの依存を減らすために、旅行用 eSIM を活用することも一つの手段です。安全なモバイル通信環境を確保することで、セキュリティリスクを最小限に抑えることが可能です。

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

旅行業界は機密性の高い個人情報や金融データを扱っているため、ハッカーにとって収益性の高い標的になります。NordVPN の調査により、航空会社が継続的にデータ侵害に直面しており、盗まれた情報がダークウェブ上の市場で流通していることを明らかになりました。旅行需要の高まりとともに、盗まれたマイルやホテルポイントの換金手段が増えます。消費者は、特に詐欺が活発になる時期において、アカウントのセキュリティ強化により一層気を付けましょう。

■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/