

Views

急増するフィッシング詐欺 中国闇市場で高値売買される個人情報

2022.8.2



八巻 高之

企業の偽サイトに誘導し、個人情報を抜き取る「フィッシング詐欺」。国内の報告件数は、1年で約3倍に増えた。急増の背景には、クレジットカード番号など日本人の個人情報を売買する海外の闇市場という存在があるようだ。



メルカリは不正利用をなくすためユーザーへの注意喚起やセキュリティー強化を進める

7月までに、中国人グループが神奈川など複数の県警による合同捜査本部に逮捕された。フリマアプリ大手メルカリの電子決済サービス「メルペ

イ」で、他人のアカウントを不正に利用してコンビニエンスストアで商品を購入したなどの疑いがあった。

容疑者らはフィッシング詐欺などで入手した他人のアカウントに不正アクセスして決済を繰り返したもようだ。

被害は深刻だ。メルカリは2022年1～3月期にユーザーへの補填金など総額16億円の費用を計上した。「画面を見ただけで偽物と見破ることは困難」「メルカリのログイン画面が表示されたらまずは疑って」と、同社は利用者に注意を促す。情報配信だけでなく、認証機能をアプリに追加するなど、様々な手段で不正利用防止を急ぐ。

カード不正利用被害額が最高

監視団体のフィッシング対策協議会（東京・中央）によると、22年6月の報告件数は8万8250件と前年同月比で約3倍に増えた。さらに、日本クレジット協会（東京・中央）の調査では、全国のクレジットカード不正利用の被害額は21年に330億円と過去最高を記録。フィッシング詐欺で抜き取られたカード情報が悪用されていると疑われる。

ネット通販や電子決済が普及する中、企業になりすまして巧妙に情報をだまし取る手口が広がる。メールやSMS（ショートメッセージサービス）で偽サイトのリンクを送信し、ウェブページでは有名企業のロゴを盗用して信用性を演出する。ログインを誘い込み、個人情報やクレジットカード番号、アカウントIDやパスワードを盗む。



(背景写真 = PIXTA)

[画像のクリックで拡大表示]

サイバー対策大手トレンドマ

イクロの岡本勝之氏は「新たな標的がネット通販や電子決済になっている。これまでの標的はネット銀行だった」と語る。不正検知のノウハウが蓄積されてきたネット銀行と違い、電子決済は特に歴史が浅い。利用者の防犯意識の低さに、事業者側の対策の不完全さが重なり合い、サイバー犯罪者の格好の標的となった。

さらに、フィッシング被害急増の背景には、国境をまたいだ詐欺犯罪者網の広がりがある。

セキュリティー会社サウスプルーム（東京・新宿）の協力で、盗まれた個人情報を買取る中国のネット上のブラックマーケット（闇市場）をのぞいた。

中国の闇市場に大量の個人情報

同社と提携する韓国のセキュリティー会社、CNSECURITY（シエンセキュリティー）の調査員が潜入するチャットアプリを開くと、日本人のものとみられる個人情報が大量に売りに出されていた。サウスプルームの篠田律社長は「毎日、数千件の個人情報が売りに出ている」と説明する。

アプリ上で「無料サンプル」というテキストファイルを選ぶと、ある日本人女性のフルネームや携帯電話番号、住所、クレジットカード情報が表示された。端末情報など他の項目に並んで、生年月日も写し出されている。見ると、彼女はまだ19歳にすぎない。

彼女の個人情報の後にも次々と投稿が続く。こうしたチャットルームは他にも数多く存在していた。

日本人のカード情報が高額で売買



IDやパスワードなど日本人の個人情報が狙われている（写真=PIXTA）

篠田社長によれば、フィッシングで取得された日本人のクレジットカード情報は最も高額に売買されるそうだ。フィッシングの情報は、他の情報の3倍以上の値が付くこともある。個人情報は企業へのハッキングなどの手段でも不正に入手されるが、本人が実際に入力するフィッシング情報が一番『使える』と判断されるという。

闇市場には、フィッシング専用のツールも売られていた。通販サイトの運営企業、金融機関や航空会社など大手企業を巧妙に模倣したウェブページのHTMLファイルだ。このファイルをネット上に公開し、多数の日本人にメールやSMSで送りつけて、引っかかった一定数の個人情報を抜き取る手法のようだ。ツールの操作手順を解説する動画まで闇市場で共有されていた。

指示役は海外で野放しのケースも

国内で摘発された犯罪者は、「受け子」や「買い子」など末端メンバーの場合が少なくない。グループの指示役は、依然として中国など本拠地から、日本の別の末端メンバーに指示を送り続けている場合もあるようだ。

海外の捜査機関が捜査に協力的でない場合もあり、国際捜査のハードルは高い。「『とかけのしっぽ切り』で、本当に悪いやつは痛くもかゆくもないという状態が続いているのだろう」。京都府警でサイバー犯罪を捜査した経験を持つNECサイバーセキュリティ戦略統括部の木村公也氏は、こう指摘する。

企業は不正利用対策を急ぐが、犯罪の手段も巧妙化し、被害増加に歯止めがかからない。「日本経済の損害は大きい」（篠田社長）。官民を挙げてネット犯罪を防ぐセキュリティー対策の強化が求められている。



Copyright © Nikkei Business Publications, Inc. All Rights Reserved.