フィッシング詐欺被害の現状と対策

加藤 孝浩 ●フィッシング対策協議会 運営委員長

フィッシング詐欺の報告件数が前年の2倍以上に急増した2021年。悪用されるブランド数も増加しており、すべての業種で対策が必要となっている。

■フィッシング詐欺被害の現状

フィッシング詐欺は、金融機関などを装ったメール（フィッシングメール）を利用者に送り、メール内のリンクから偽サイト（フィッシングサイト）に誘導して氏名や住所などの個人情報、銀行口座番号、クレジットカード番号、さらに会員サイトのIDとパスワードなどを詐取する詐欺行為である[1]。

フィッシング対策協議会は、一般の方からフィッシング詐欺に関連する報告を受け付けている。2021年12月は6万3159件の報告を受け、2021年の年間累計は52万6504件となった（資料4-1-3）。フィッシング詐欺の報告件数は2020年に対前年4倍、2021年はさらに同2倍以上に増加し、深刻な状況となっている。

●多くのブランドでフィッシング詐欺が発生

フィッシング詐欺に悪用されたブランド数は80を超え、これも増加の傾向にある。アマゾンをかたるフィッシング詐欺は報告数全体の約3割で、次にメルカリをかたるフィッシング詐欺が多い。2021年11月は三井住友カード、楽天、ETC利用照会サービスが続き、これら上位5ブランドで報告数全体の約7割を占めている。2021年は新たにコロナワクチンナビ（厚生労働省）や特別定額給付金の申請サイト（総務省）をかたったフィッシング詐欺が発生し、さらに生命保険会社、電子マネーサービス、家電量販店、コンビニエンスストア、インターネットプロバイダー、旅行予約サイトなどにも広がっている。

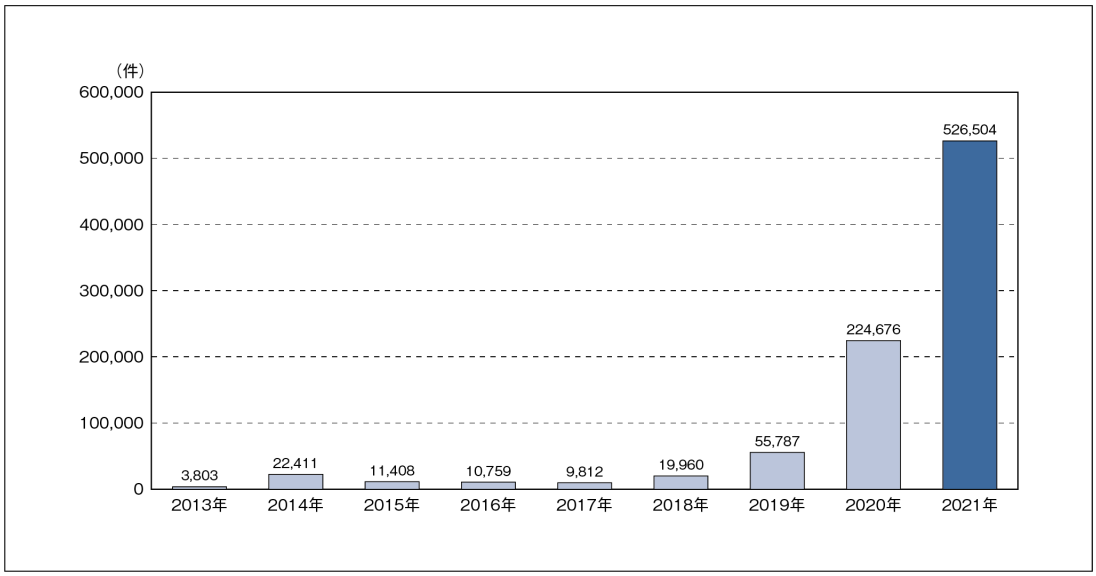
■フィッシングの標的はクレジットカード情報

クレジットカード情報の詐取を目的としたフィッシング詐欺は最も報告件数が多い。この傾向は、以前から続くものである。アマゾンやアップルなどのメジャーブランドに加え、日本郵便や家電量販店、インターネットプロバイダーをかたったフィッシング詐欺も、目的はクレジットカード情報の詐取となっている。日本クレジット協会の発表によると、クレジットカードの番号盗用による被害額は2020年に223.6億円まで拡大し、2021年は9月段階で前年を上回る223.9億円となっている（資料4-1-4）。

●無関係にカード情報の入力が求められる

上述のように、コロナワクチンナビをかたるフィッシング詐欺が2021年8月に報告された。これは、予約サイトを装った偽サイトに誘導し、ワクチン接種予約に必要のないクレジットカード

資料4-1-3　フィッシング情報の届け出件数（年別）



出所：フィッシング対策協議会

情報の入力が求められるというものである。ワクチン接種の予約に当たり、公的機関がクレジットカード情報を求めることはない。同様に、日本郵便をかたるフィッシング詐欺でも、再配達登録に必要のないクレジットカード情報の入力が求められる。

このようなフィッシングサイトにカード番号、カード名義人、有効期限、セキュリティコードなどを絶対に入力しないよう、注意が必要である。

■フィッシング詐欺の傾向と新たな手口

2021年のフィッシング詐欺には、以下の傾向があった。今後も変化するフィッシングの動向を注視し対策を講じる必要がある。

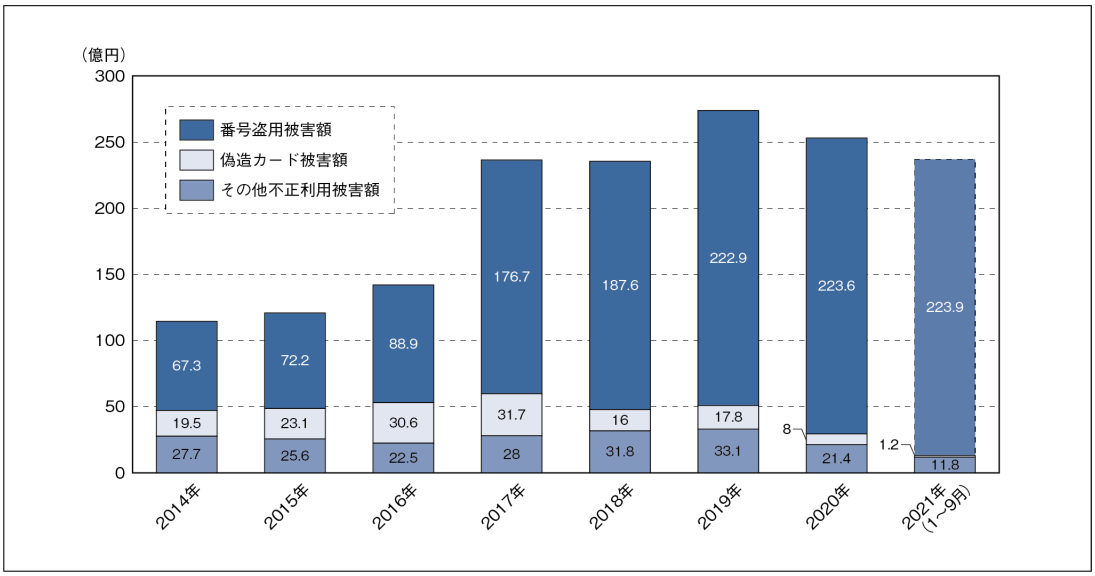
・悪用されたブランド数の増加
・短期間に運用されるフィッシングサイトの増加
・クレジットカードブランドの詐称が増加
・同じ文面でブランドだけを変更
・CN事業者からの発信が増加

●生命保険会社をかたったフィッシング詐欺の発生

2021年11月以降、明治安田生命、住友生命、アフラックをかたったフィッシング詐欺の報告を受けている。これは、登録された個人情報の再確認を求めるフィッシングメールから契約者専用サイトを装ったフィッシングサイトに誘導し、契約者専用ページのIDとパスワード、さらに保険証券番号の入力を求めてくるものである。このフィッシング詐欺は、保険の契約者貸付制度（解約返戻金の一定範囲内で必要資金を用立てする制度）を悪用した可能性がある。詐取したIDを使って振込先を偽装口座に変更し、貸付金を不正に受け取るというものだ。

利用者（契約者）の対策としては、保険会社のウェブサイトのドメインが正規のものかを確認するようにし、契約者ページには保険会社のウェブ

資料4-1-4　クレジットカードの不正利用被害額



出所：日本クレジット協会

サイトまたはスマートフォンアプリを経由してアクセスし、ログインすることが望ましい。

●SMSによるフィッシング詐欺が継続

SMS（ショート・メッセージ・サービス）によるフィッシング詐欺は「スミッシング」と呼ばれており、2021年も宅配便の不在通知やアマゾン、NTTドコモ、auなどをかたるスミッシングの報告を受けている。宅配便の不在通知のスミッシングでは、無関係な金融機関のフィッシングサイトへ誘導され、オンラインバンキングのIDやパスワードなどの入力が求められる。

■インターネットバンキングのフィッシング詐欺被害状況

インターネットバンキングを狙ったフィッシング詐欺は、減少傾向にあるものの継続している。警察庁によると、不正送金被害のピークは2015年に1495件・約31億円であるが、2016年からは減少傾向となり、2018年には約4億6100万円まで下がっている。この減少傾向は、ウイルス対策ソフトの導入やOS最新化などの利用者側の基本的な対策に加え、ワンタイムパスワードを使った複数要素認証など、各金融機関のフィッシング対策が進んだことによる。2019年に再度件数・被害額共に増加しているが、さらなる対策により、2020年からは減少傾向となっている。

●乱数表カードの写真アップロードが求められる

インターネットバンキングの代表的なフィッシング詐欺対策としてはワンタイムパスワードがあるが、まだ乱数表の利用も残っており、それが狙われている。フィッシングサイトでは乱数表カードの写真のアップロードを求められ、これにより、すべての乱数が盗まれてしまう。

フィッシング詐欺対策としては、スマートフォンや専用の機械（トークン）によるワンタイムパスワードへの切り替えを行うことが望ましい。

■対策は利用者と事業者の両者で必要

●利用者側の対策

フィッシング対策協議会では、利用者側のフィッシング対策を「マンガでわかるフィッシング詐欺対策5ヶ条」「利用者向けフィッシング詐欺対策ガイドライン」にまとめている。「自分は大丈夫」と過信せず、最新の情報を基にした対策を取ることが重要である。

【フィッシング詐欺対策5ヶ条】
第1条　パソコンやモバイル端末は、安全に保ちましょう。
第2条　不審なメールに注意しましょう。
第3条　電子メールにあるリンクはクリックしないようにしましょう。
第4条　不審なメールやサイトは報告しましょう。
第5条　銀行やクレジットカード会社の連絡先リストを作りましょう。

●事業者側の対策1：スミッシング対策が重要

SMSによるフィッシング詐欺であるスミッシングは継続して発生しており、悪用されるブランドも拡大傾向にある。対策には、事業者側が安全なSMS送信を行うことが重要となる。スミッシングには国際網経由のSMSが使われていることが多いため、国内の携帯電話事業者に直接接続しているSMSを利用するか、SMSの次世代版であるRCS（Rich Communication Service）に準拠した「＋メッセージ」を利用することが対策となる。＋メッセージは本人の確実性が高く、格安SIM提供会社などのMVNO利用者も利用可能となったことから、リッチコンテンツと合わせた安全なコミュニケーションツールとして切り替えを進めることが望ましい。

●事業者側の対策2：フィッシングサイトの早期閉鎖が重要

フィッシングサイトを早期にテイクダウン（閉鎖）することが重要である。そのためには、テイクダウンを遅滞なく行えるような対応体制を整えておくことが必要となる。フィッシング対策協議会は、JPCERTコーディネーションセンター（JPCERT/CC）を通じて、フィッシングサイトのテイクダウンの調整依頼も行っている。

●事業者側の対策3：すべての業種で対策が必要

フィッシング詐欺は、すべての業種で発生する可能性がある。そのため、事業者はフィッシング対策ガイドラインの重要5項目を基に、事前に対策することが必要である。

【フィッシング対策ガイドラインの重要5項目】
①利用者に送信するメールには「なりすましメール対策」を施すこと
②複数要素認証を要求すること
③ドメインは自己ブランドと認識して管理し、利用者に周知すること
④すべてのウェブページにサーバー証明書を導入すること
⑤フィッシング詐欺について利用者に注意喚起すること

事業者は利用者がフィッシング詐欺に遭わないよう、また遭ってしまったときの対処をアドバイスすることも重要である。注意喚起とアドバイスを継続し、フィッシング詐欺が発生しにくいネット社会にすることが最大の対策となる。フィッシング対策協議会のガイドラインやレポート、活動成果などをフィッシング詐欺対策に役立てていただきたい。

■参考資料

●フィッシング対策協議会
https://www.antiphishing.jp/
●フィッシング対策ガイドライン（事業者／利用者）
https://www.antiphishing.jp/report/guideline/
●警察庁 サイバー犯罪対策プロジェクト 統計
https://www.npa.go.jp/cyber/statics/
●日本クレジット協会 クレジット関連統計
https://www.j-credit.or.jp/information/statistics/
●フィッシングとは
https://www.antiphishing.jp/consumer/abt_phishing.html
●フィッシング対策協議会の活動
https://member.antiphishing.jp/about_ap/org_chart.html
●協議会からのお知らせ
https://www.antiphishing.jp/news/info/
●フィッシング報告状況 月次報告書
https://www.antiphishing.jp/report/monthly/
●協議会WG報告書
https://www.antiphishing.jp/report/wg/
●マンガでわかるフィッシング詐欺対策５ヶ条
https://www.antiphishing.jp/phishing-5articles.html
●STOP. THINK. CONNECT.
https://www.antiphishing.jp/enterprise/stc.html
●日本版「STOP. THINK. CONNECT.」
https://stopthinkconnect.jp/

1. フィッシングは phishing というつづりで、釣りの fishing を、昔のハッカーが「f」を「ph」にするのを好んでいたことから作られた造語といわれている。

インターネット白書 ARCHIVES

1996,1997,1998,1999,2000....

［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dおよび株式会社インプレスが1996年～2022年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

https://IWParchives.jp/

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、データ、URL、名称など）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真・図の作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&Dおよび株式会社インプレスと著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先　インプレス・サステナブルラボ　✉ iwp-info@impress.co.jp