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

2022年は、フィッシング詐欺の報告件数が倍増した。実在するサービスのメールアドレスが差出人となっているケースも非常に多く、“なりすましメール”の対策は急務となっている。

■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本物そっくりの偽メール（フィッシングメール）や偽サイト（フィッシングサイト）を用いてユーザーをだまし、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の活動では、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。2022年12月は6万5474件の報告を受け、2022年の年間累計は96万8832件と、前年から約2倍に増加している（資料4-1-3）。このフィッシング詐欺は、2020年から毎年倍増する深刻な状況となっている。

●標的となるブランドが多様化

フィッシング詐欺の標的となるブランド数も増加している。月に100ブランドを超え、業種もさまざまである。アマゾン・ドット・コムをかたるフィッシング報告が全体の約3割を占めており、受信者のメールボックスを埋め尽くしている場合もある。auとえきねっと（JR東日本）も継続されている上、複数のクレジットカード会社をかたってカードの利用確認を装うフィッシングも増加している。

2022年はさらに、国税庁、金融庁、警察庁、日本年金機構（ねんきんネット）、資源エネルギー庁などをかたるフィッシング詐欺が発生した。2021年に厚生労働省のコロナワクチンナビや総務省の特別定額給付金の申請サイトが標的となったが、行政機関をかたったフィッシングが拡大したことになる。

■狙いはクレジットカード情報の詐取

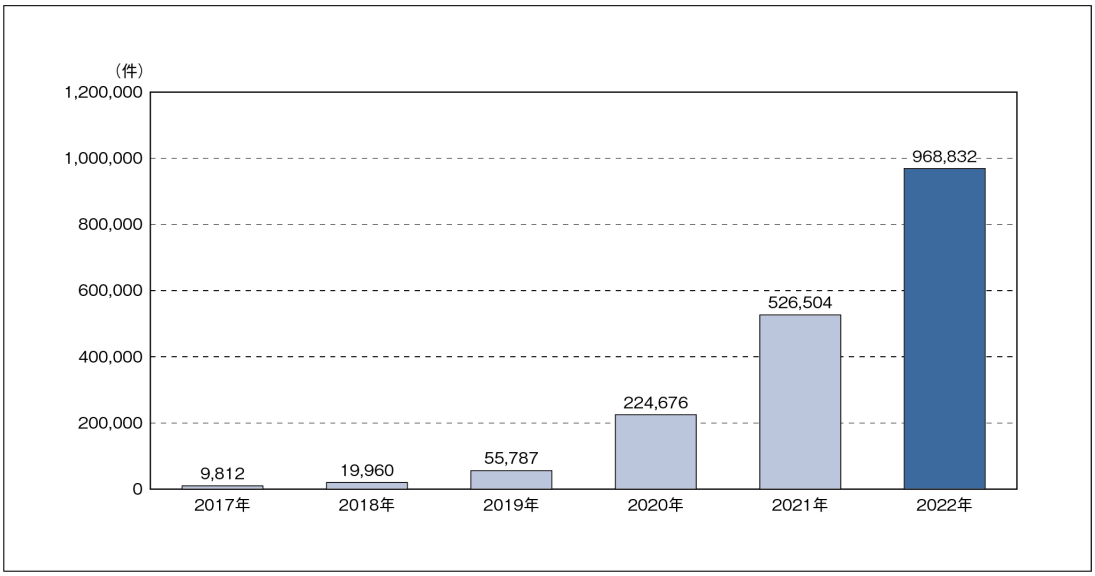
一般の方からの報告では、フィッシングサイトに誘導され、クレジットカード情報を盗もうとする内容が最も多い。また、アマゾン・ドット・コムやアップル、楽天、えきねっとなどのブランドが、クレジットカード情報の詐取ではよく見られる。日本クレジット協会の発表によると、クレジットカードの番号盗用による被害額は2021年に311.7億円まで拡大し、2022年は9月段階で前年同月を上回る291.3億円と、増加が続いている（資料4-1-4）。

■フィッシング詐欺の傾向と新たな手口

●見抜くのが困難、巧妙なフィッシング手口

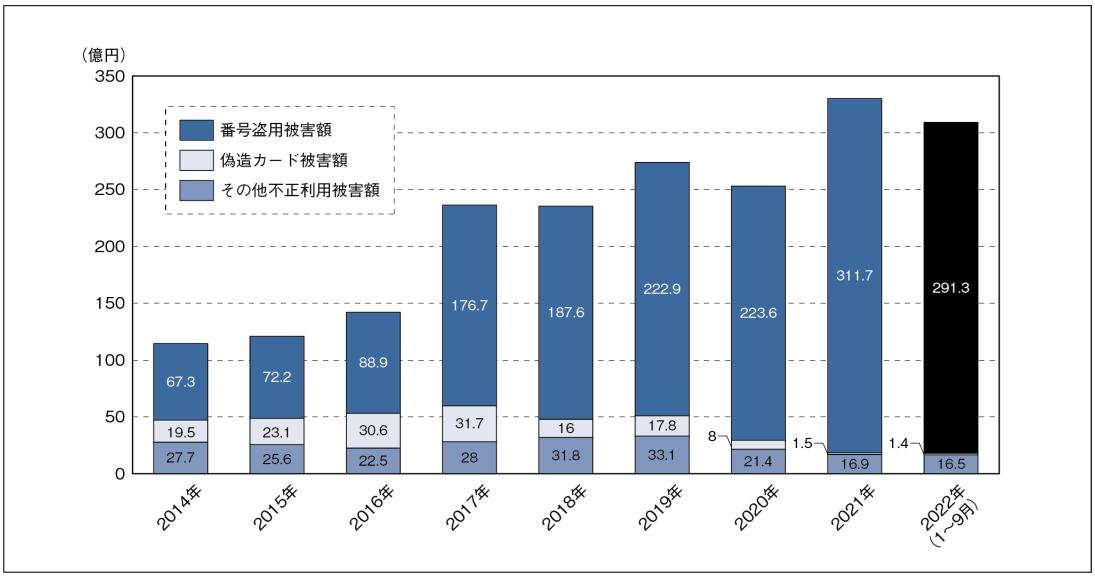
行政機関をかたったフィッシング詐欺では、クレジットカード情報詐取以外の手口が追加され

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

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

ている。警察庁をかたったフィッシング詐欺では、マルウエア感染が検知されたと偽の警告を表示し、不正アプリのインストールに誘導されている。国税庁をかたるフィッシング詐欺では、税金未納の偽メールから電子マネー（Vプリカ）の購入を案内し、その番号と電子マネーカードの写真のアップロードを要求する手口となっている。

●auをかたったスミッシングが継続

SMSによるフィッシング詐欺は、スミッシングと呼ばれている。2022年も宅配便の不在通知やアマゾン・ドット・コム、アップル、auなどのスミッシングが発生しており、国税庁をかたるSMSも観測された。中でも、auおよびau PAYをかたるスミッシングが増加している。利用者は本物のウェブサイトに酷似したフィッシングサイトに誘導され、au IDとパスワード、さらに本人確認用暗証番号の入力を求められる。攻撃者は不正に入手したau IDを使って本物のウェブサイトでログインし、au PayのQRコードを取得する。これが、他人のau Payで不正購入する手口である。

■事業者側の対策が急務のなりすましメール対策

●フィッシングメールにサービスの正規アドレスが使われる。

フィッシング対策協議会の調査用メールアドレス宛てに、2022年12月に届いたフィッシングメールのうちの約85.7％が、メール差出人に実在するサービスのアドレス（ドメイン）が使用された「なりすまし」であった。

フィッシング詐欺は、計画→調達→構築→誘導→詐取→収益化の6つの行動によって行われる(資料4-1-5)。事業者はフィッシングサイトで情報が盗まれる前の「誘導」段階に当たるフィッシングメールの抑制を強化すべきである。

●なりすましメールを利用者に届かなくする対策

実在するアドレスになりすましたフィッシングメールを利用者に届かなくする対策として「DMARC（Domain-based Message Authentication, Reporting, and Conformance）」がある。DMARCは、送信ドメイン認証技術のSPFやDKIMを補強する技術であり、なりすましメールで発生するSPFやDKIMの認証失敗状況から、そのメールが利用者に届く前にプロバイダー側で受信を拒否する、または迷惑メールボックスに入れるなどの制御を可能とする。

DMARCの「メールの受信制御ポリシー」には①そのまま受信させる（none）②隔離させる（quarantine）③受信を拒否する（reject）――があり、それらから選択することができる。フィッシング被害に遭った事業者のみならず、なりすましメールの対策としてDMARCのポリシーの「reject」の設定を進めることが重要である。

経済産業省、警察庁および総務省は、クレジットカード会社等に対し、DMARCの導入をはじめとするフィッシング対策の強化を要請している[2]。

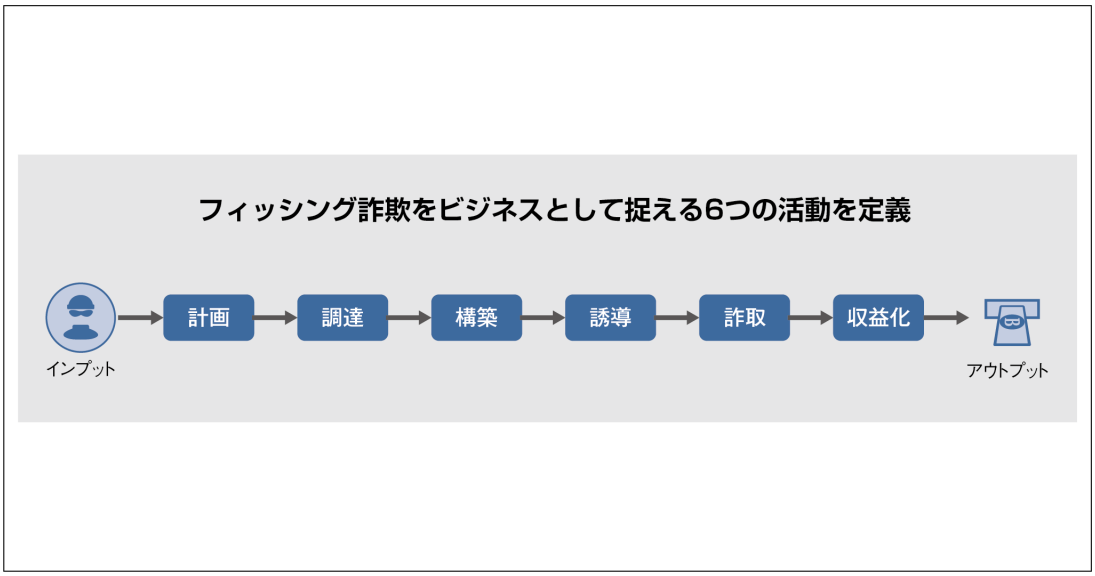
●スミッシング対策には送信側の対策が重要

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。そこで、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」を利用することがスミッシング対策となる。

●利用者へ継続した情報提供とアドバイスを

フィッシング詐欺の「誘導」と「詐取」の段階までは、被害者となる利用者と攻撃者だけで構成されているため、フィッシング詐欺への対策では利用者が負う役割が大きい。そこで、事業者は利用者に向けてフィッシング対策に関する情報を提供し、フィッシングに遭ってしまったときの対処をアドバイスし続けていくことが、信頼継続のために重要である。

資料4-1-5　フィッシング詐欺のビジネスプロセス



出所：フィッシング対策協議会 学術研究 WG、「フィッシング詐欺のビジネスプロセス分類」

■利用者の対策は「見抜こうとしない」「URLをタップしない」

フィッシング詐欺では、本物のアドレスを使ったなりすましメールと、本物のウェブサイトをコピーして作られたフィッシングサイトが使われるため、見抜くのは大変困難である。「私なんか狙われないから関係ない」「詐欺は見抜けるから大丈夫」などと過信せず、メールの参照において安全な行動を取ることが重要である。

偽物が混入することを理解し、メールやSMSの本文内にあるURLにアクセスするのをやめるとともに、ECサイトなどのウェブサービスを利用する際は正規のアプリを利用したり企業のドメインからトップページにアクセスしたりすることが安全な行動となる。

●攻撃者の「収益化」を阻止する対策

利用者は、自分がフィッシングサイトにアクセスしていることに気づかないまま、IDやパスワード、さらにクレジットカード番号など重要な情報を入力してしまっている可能性がある。クレジットカードの利用明細などから不正利用を確認することに加え、SMS認証やワンタイムパスワード認証などの複数要素認証を利用することが、攻撃者による不正ログインと「収益化」を阻止することに有効である。

IDとパスワード認証だけではフィッシング詐欺に対応することは難しいため、各ウェブサービスで提供されているセキュリティ機能を積極的に利用することも重要である。経済産業省はECサイトでのクレジットカードの不正利用防止に向け、カード所有者本人であることを複数手段で認証する国際的な認証規格「EMV-3Dセキュア」の導入義務化を検討している[3]。

■フィッシング対策協議会が発信している情報

フィッシング詐欺対策は、利用者と事業者、セキュリティ事業者の3者で行う必要がある。

フィッシング対策協議会のウェブサイトから発信している各種情報を活用いただきたい。

・緊急情報
・フィッシングに関するニュース
・フィッシング対策ガイドライン（事業者向け／利用者向け）
・利用者向けフィッシング対策コンテンツ（マンガでわかるフィッシング詐欺対策5ヶ条、インターネットを安全に楽しむための合言葉「STOP. THINK. CONNECT.」）

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。
2. https://www.meti.go.jp/press/2022/02/20230201001/20230201001.html
3. https://www.meti.go.jp/shingikai/mono_info_service/credit_card_payment/003.html

●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
https://www.antiphishing.jp/report/guideline/
・フィッシング詐欺のビジネスプロセス分類
https://www.antiphishing.jp/report/wg/collabo_20210316.html
・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/

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～2023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