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

2023年は、フィッシング詐欺の報告件数がさらに増加した。不正送金とクレジットカード情報の盗用被害も増加しており、なりすましメール対策と認証強化がすべてのインターネットサービスで必要である。

■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、さらに銀行口座番号やクレジットカード番号、会員サイトのID・パスワードなどを詐取する詐欺行為である。

フィッシング対策協議会に寄せられたフィッシング詐欺に関連する報告は、2023年12月に9万792件、2023年の年間累計は119万6390件と、前年から約1.2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年から毎年増加が続き、深刻な状況となっている。

●フィッシング詐欺による不正送金の急増

インターネットバンキングに係る不正送金事犯が急増している。警察庁と金融庁の発表によると、2023年12月8日時点の同年11月末における被害件数は5147件、被害額は約80.1億円と、過去最多を更新した[1]。被害の多くはフィッシング詐欺によるものとみられ、金融機関（銀行）を装った偽メールが多数確認されている。メールやSMS（ショート・メッセージ・サービス）に記載されたリンクから偽サイトに誘導され、そこでID・パスワードに加えワンタイムパスワードや乱数表等の情報が詐取されることが要因とされている。

●クレジットカード情報詐取が主目的

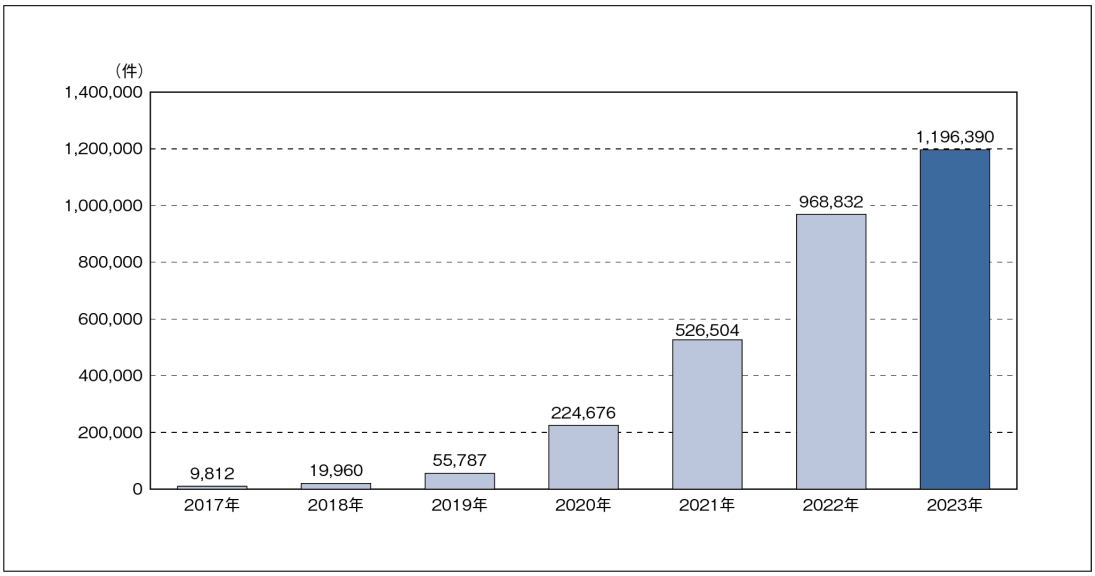
フィッシング詐欺の報告で最も多いのが、偽サイトに誘導されてクレジットカード情報を盗もうとする内容である。継続して悪用されているアマゾン・ドット・コムやアップル、楽天に加え、総務省、国税庁、国土交通省などをかたったフィッシング詐欺でも、クレジットカード情報の詐取が行われている。日本クレジット協会の発表によると、クレジットカードの番号盗用による被害額は2022年に411.7億円まで拡大し、2023年9月までに376.3億円と、増加傾向となっている（資料4-1-4）[2]。

■フィッシング詐欺の傾向と新たな手口

●なりすましメールの増加が続く

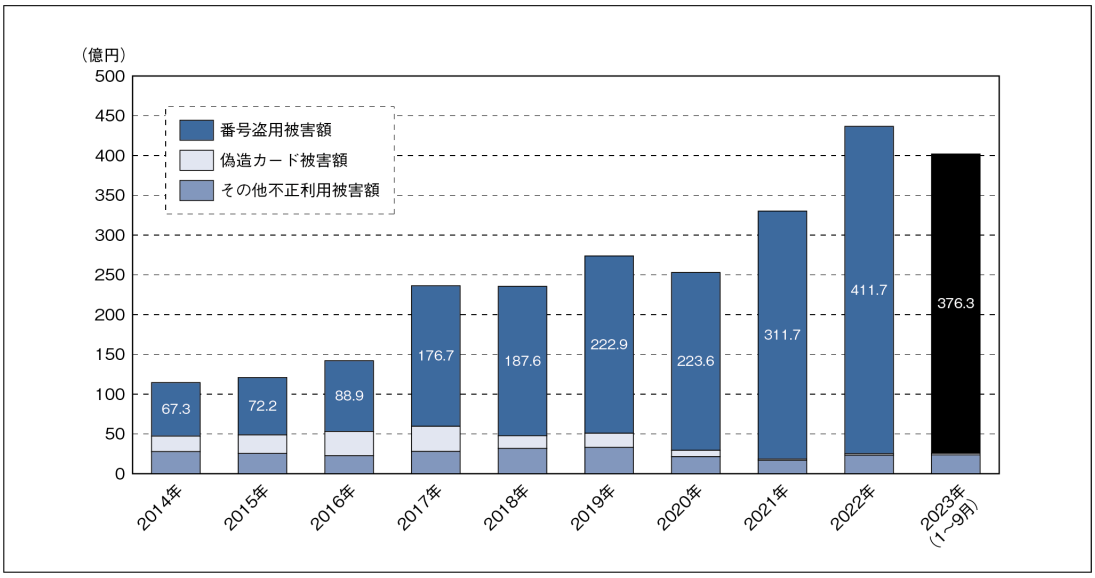
フィッシングメールの約65.5％が、メール差出人として実在するサービスのメールアドレス（ドメイン）を使用した“なりすまし”メールとなっている[3]。実在するサービスのドメインを使用することで受信者に本物のメールと認識させる目的がある。

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、「月次報告書：フィッシング報告状況」

資料4-1-4　クレジットカード不正利用被害額



出所：日本クレジット協会、「クレジットカード不正利用被害の発生状況」

●マイナポイント事務局も標的に

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。具体的には、アマゾン・ドット・コムなどのEC系が約38.2％、ETC利用照会サービスなどのオンラインサービス系が約32.2％、続いてクレジット・信販系が約13.1％となっている[4]。

2023年はさらに、マイナポイント事務局をかたるフィッシング詐欺の報告が複数発生した（資料4-1-5）[5]。「お早めに回収してください」と受信者を焦らせる偽メールからフィッシングサイトへ誘導し、クレジットカード情報（番号、名義人、有効期限、セキュリティコード）、さらに3-Dセキュアの認証情報を盗む詐欺となっている。

●受信者を焦らせるメッセージ

「銀行口座の取引を停止」や「カードのご利用を一部制限」などの偽のメッセージで受信者を焦らせ、冷静な判断をできなくする偽メールが多い。サービス事業者が不審な利用を検知した際に送信するお知らせメールから、クレジットカードの番号、暗証番号、セキュリティコード等の入力を求めることはないので、落ち着いて、電話などでサービス事業者に確認することが重要である。

●スミッシングがさらに巧妙に

「ご不在のためお荷物を持ち帰りました」などの偽のSMSによるスミッシングが続いている。スミッシングはSMSによるフィッシング詐欺であるが、iPhoneとAndroid端末で異なった手口になっている場合がある。iPhoneからクリックした場合はクレジットカード情報を詐取するフィッシング詐欺が展開されるが、Android端末では、まず不正アプリのダウンロードが行われ、マルウエア感染に進む。次に、そのマルウエアがスマートフォンの連絡先・電話帳の宛先に偽のSMSを発信するという“踏み台”が増殖する――というものである。こういった、個人が差出人になっている偽SMSの増加が深刻な状況にある。

■フィッシング対策のポイント

●なりすましメール対策のDMARC導入が急務

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[6]。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」段階で発生する偽メールを利用者に届かなくする対策を講じることが重要となる。

その対策の一つが、DMARC（Domain-based Message Authentication, Reporting, and Conformance）である。2023年2月に経済産業省、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た。DMARCは、送信ドメイン認証技術のSPF（Sender Policy Framework）やDKIM（DomainKeys Identified Mail）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が可能となる。

●グーグルなどがフィッシングメール対策を強化

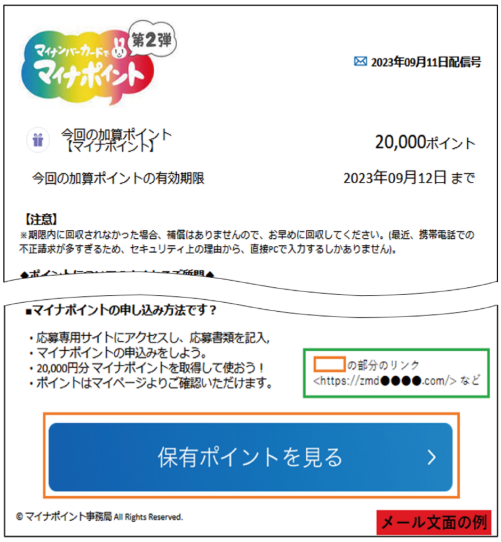
グーグルとヤフーは2023年10月、メールを送信する際の条件としてSPF・DKIM・DMARCへの対応を必須とすると発表した[7]。このように、広く国内外企業のDMARC導入が進むことで、なりすましメールの送信が困難になることが期待される。

●新しい偽SMS対策、キャリア共通番号「0005」

新たなスミッシング対策として、国内4キャリア（NTTドコモ、KDDI、ソフトバンク、楽天モバイル）が発行するキャリア共通番号の「0005」がある。各キャリアの厳格な審査を通過した法人のみに与えられる発信元番号となっており、発信元番号が「0005」から始まるSMSは「正規の企業からのSMSです。安心して受信してください」と案内することが可能となる。

加えて「＋メッセージ」との組み合わせでさら

資料4-1-5　マイナポイント事務局をかたるフィッシング



出所：フィッシング対策協議会、「緊急情報：マイナポイント事務局をかたるフィッシング（2023/09/11）」

なる対策強化が図れる。＋メッセージは次世代版であるRCS（Rich Communication Services）に準拠したSMSであり、認証を得たことを示す「認証済みマーク」が表示されるため、正規のSMSを判別しやすくなる。

●「収益化」を阻止する対策が全事業者に必要

フィッシング詐欺によって盗まれたID・パスワードは、攻撃者が本人になりすまして正規サイトにログインすることができ、さらに詐取したクレジットカード情報から不正購入などの「収益化」を達成できてしまう。この収益化を阻止する対策として、SMS認証やワンタイムパスワード認証、パスキー認証などの複数要素認証による認証強化が重要となる。

攻撃者はさまざまなブランドになりすまして、盗んだ認証情報とクレジットカード情報から、収益化の標的サービスも選定している。同じパスワードを複数サービスに設定している場合もあることから、フィッシング詐欺に遭っていないサービス事業者も収益化の標的になる可能性がある。

すべての事業者は、自社の顧客を守るためにも認証強化を実施し、詐取されたクレジットカード情報の不正利用対策[8]と組み合わせることで、盗んだ情報からは不正な収益が得られない安全なネット社会の実現を目指す必要がある。

■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ことから、見抜くのは大変困難である。そのため、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にアクセスすることをやめるとともに、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するか、企業サイトのトップページにアクセスしてから目的の

ウェブページに移動するといったことが安全な行動となる。

フィッシングサイトにID・パスワードやクレジットカード情報、インターネットバンキングの認証情報などを入力してしまったときは、フィッシング対策協議会の公式サイト内「フィッシングの相談等」を参考に、対応を急いでいただきたい。

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では公式サイトで緊急情報やフィッシング対策ガイドラインなど各種情報を発信しているので、ぜひご活用いただきたい。

1. 警察庁・金融庁、「フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について（注意喚起）」、2023年12月25日
https://www.npa.go.jp/bureau/cyber/pdf/20231225_press.pdf
2. 日本クレジット協会、「クレジットカード不正利用被害の発生状況」、2023年12月
https://www.j-credit.or.jp/information/statistics/download/toukei_03_g.pdf
3. フィッシング対策協議会、「月次報告書：2023/10 フィッシング報告状況」、2023年11月9日
https://www.antiphishing.jp/report/monthly/202310.html
4. （注釈3に同じ）
5. フィッシング対策協議会、「緊急情報：マイナポイント事務局をかたるフィッシング（2023/09/11）」
https://www.antiphishing.jp/news/alert/myna_20230911.html
6. フィッシング対策協議会、「協議会WG報告書：「フィッシング詐欺のビジネスプロセス分類」を公開（2021/03/16）」
https://www.antiphishing.jp/report/wg/collabo_20210316.html
7. グーグルは2024年2月から、ヤフーは2024年第1四半期から。
8. EC加盟店において、2025年3月末を期限に、クレジット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 3-Dセキュア」の導入が義務化される。

●参考資料

・フィッシング対策協議会
https://www.antiphishing.jp/
・フィッシングの相談等（フィッシング対策協議会）
https://www.antiphishing.jp/contact_faq.html
・フィッシング対策ガイドライン（フィッシング対策協議会）
https://www.antiphishing.jp/report/guideline/
・クレジット関連統計（日本クレジット協会）
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～2024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