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

2024年はフィッシング詐欺報告件数の増加に加え、新たな手口の拡大によってインターネットバンキングに係る不正送金被害も増加。ウェブサービス側の認証強化となりすましメール対策が急務。

■フィッシング詐欺被害の現状

●増え続けるフィッシング詐欺報告

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）や偽のSMS（ショート・メッセージ・サービス）、さらに偽サイト（フィッシングサイト）を用いてユーザーをだまし、クレジットカードの番号やインターネットバンキングのID・パスワード、さらに氏名や住所などの個人情報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、2024年12月に23万2290件、2024年の年間累計は171万8036件と、前年から約1.4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

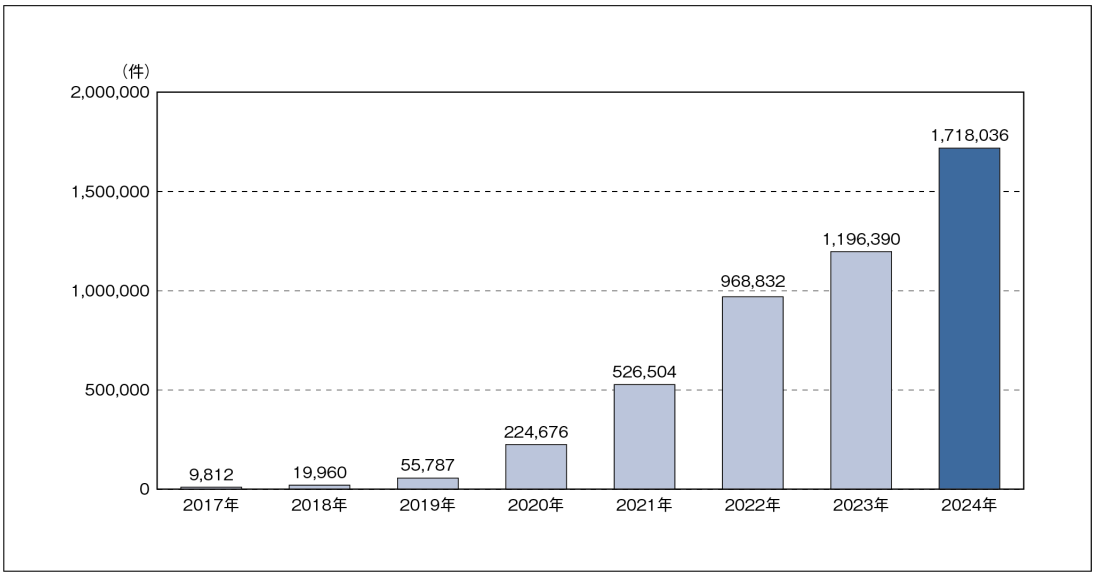
インターネットバンキングにおける不正送金事案は引き続き増加している。警察庁の発表によると、2023年の不正送金被害額は前年比約5.7倍の約87億3000万円に達し、過去最多を更新した[1]。被害の多くは、フィッシング詐欺が原因とみられる。

増加の理由としては、主に次の2点が挙げられる。1つめは、偽メールや偽サイトが正規のものと区別しづらくなっていることである。これには、攻撃者がAI技術などを活用している可能性がある。2つめは、ワンタイムパスワードを利用した2段階認証を突破する新たな手口が増加していることである。この手口は「リアルタイム型フィッシング詐欺」と呼ばれる。具体的には、偽サイトにIDとパスワードを入力させ、それを盗んだ攻撃者が正規サイトに不正ログインを試みる。その直後に、正規サイトからユーザーに送信されるワンタイムパスワードも、再び偽サイトに入力させることで盗み取る手法であり、このような新たな攻撃により被害が拡大している。

●クレジットカード情報の番号盗用被害は減少

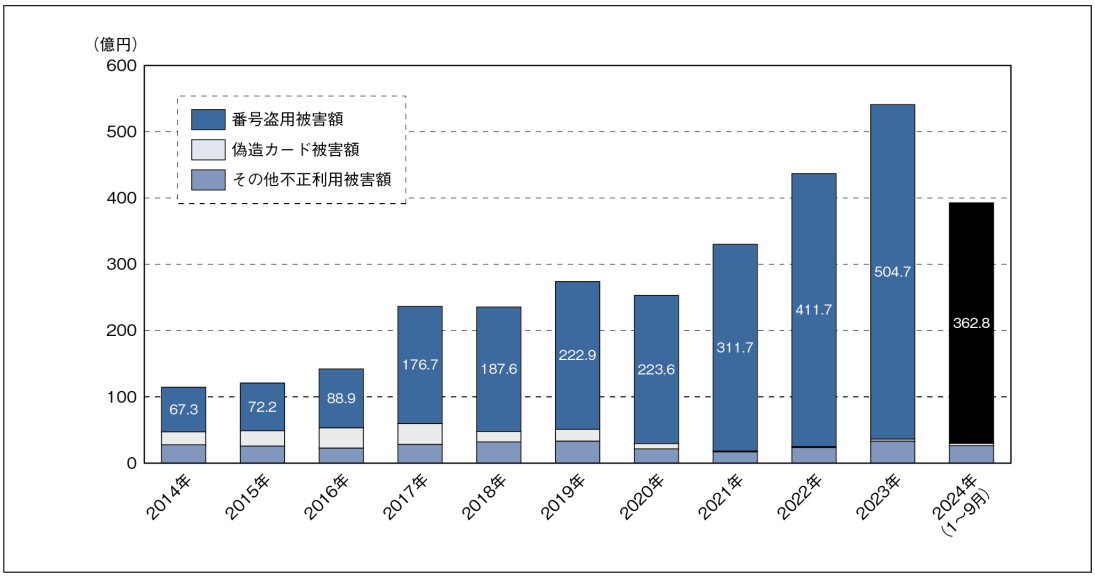
クレジットカード情報の番号盗用被害は、2023年に504.7億円まで拡大したが、2024年9月までに362.8億円、2024年第3四半期には121.4億円となり、前年同四半期の130.6億円から減少した（資料4-1-4）[2]。しかし、フィッシング詐欺の報告ではクレジットカード情報を盗もうとする手口が最も多く、2022年第4四半期以降、8四半期連続で被害額が100億円を超える深刻な状況が続いている。特に、JCBやMastercardなどのクレジット・信販系を装うフィッシングが約23.1％、ア

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」

マゾン・ドット・コムや楽天などのEC系を装うフィッシングが約21.7％を占めている[3]。

■巧妙な手口でフィッシング詐欺が拡大

●2次元コードを使った偽サイトへの誘導

2次元コードを利用して偽サイトに誘導する攻撃が多く確認されている。攻撃者は、偽サイトの

URLを含むメールが迷惑メールフィルタ機能によってブロックされるのを避けるため、誘導手段を2次元コードに変更したと考えられる。この手法は、三井住友カードやアマゾン・ドット・コムなどを装った偽メールで確認されている（資料4-1-5）[4]。2次元コードが表示されているメールは詐欺の可能性が高いため、注意が必要である。

●URLフィルタを回避するリダイレクトの悪用

偽サイトのURLをクリックした際に警告を表示するセーフブラウジング機能は、無料で提供されている。フィッシング対策協議会に寄せられたフィッシング報告情報もこの機能と連携しており、これがフィッシング目的の偽サイトへのアクセス防止につながっている。しかし、この機能を回避する攻撃も確認されている。攻撃者はURLの転送を行うリダイレクトサービスなどを悪用し、ランダムな文字列をサブドメインに付加した「リダイレクトURL」を大量に作成して、セーフブラウジングに登録された偽サイトのURLとの一致を避けている。このケースは全体の約47.4％を占めており、増加傾向にある[5]。

●差出人に悪用される正規ドメイン

正規の差出人ドメインになりすました偽メールも、引き続き確認されている。新たなパターンとして、ゲーム会社A社の正規ドメインを差出人に使用しながら、メール本文には全く別のクレジットカード会社を装った内容が記載されているというものがある。これは、攻撃者が単に取り違えているのではない。A社のドメインにおいて、送信ドメイン認証技術のDMARC（Domain-based Message Authentication, Reporting, and Conformance）ポリシー設定（なりすましメールを届かなくする度合い）が拒否設定ではなく調査用設定または隔離設定になっていることを悪用し、差出人のアドレスとして使い回しているのである。この手口は、なりすましメールを多くのユーザーに届けることを狙っている。ユーザーは差出人のドメインと、本文の内容やブランドが一致しないことに気付いた時点で詐欺であると認識することが重要である。

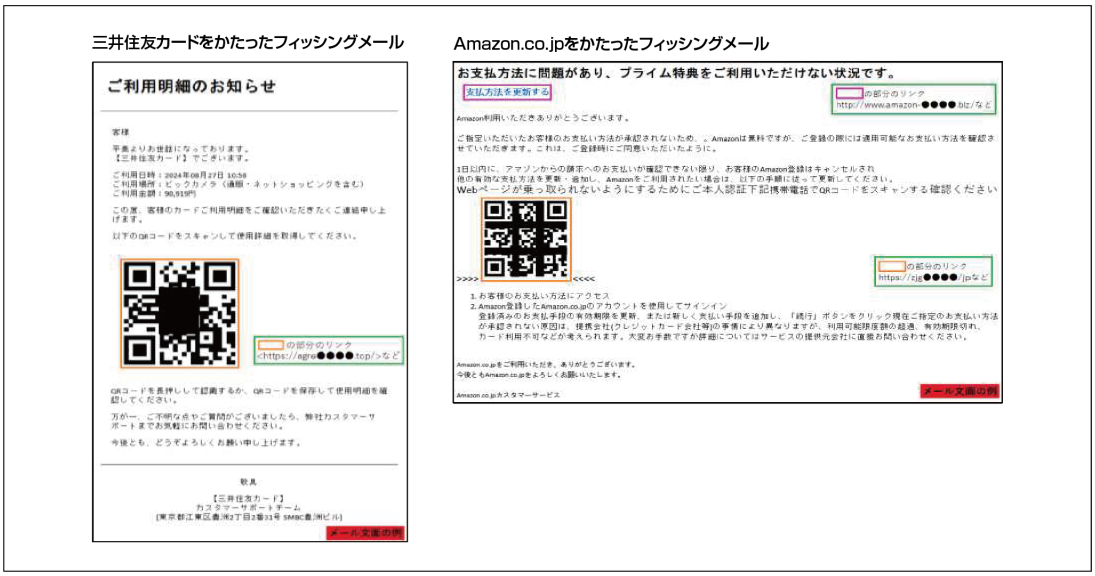
■事業者側のフィッシング対策

●パスワードが要らないパスキー認証が効果的

パスキー（FIDO2）認証は、パスワードを使用せず指紋や顔認証などの生体情報を用いる、新しい認証方式である。フィッシング詐欺では、偽サイトに誘導されてIDとパスワードが盗まれ、それを使って攻撃者が正規サイトに不正ログインを行うが、パスキー認証はパスワードを使わないことから認証詐取の防止に効果的である。パスキー認証では、ランダムな文字列である「チャレンジコード」を送信する仕組みを採用し、また、送信する際にはドメインを確認する仕様となっていることから、本物に似せた偽サイトに情報が渡ることはない。これらにより、フィッシング耐性が高い認証方式として注目されている。さらに、パスワードを使用しないため複雑で多くの文字列を覚える必要がなく、利便性も向上する。

2022年以降、アップル、グーグル、マイクロソフトの3社がパスキー認証に対応したことで、スマートフォンを使って安全かつ簡単にウェブサービスへログインできる運用が可能となった。これを受けて、三菱UFJ銀行、三井住友銀行、みずほ銀行、LINEヤフー、ソフトバンク、NTTドコモ、メルカリ、トヨタ自動車など、多くの日本企業もパスキー認証を導入した。ウェブサイトの運営事業者は、フィッシング詐欺への耐性向上とユーザーの利便性向上の両方を実現できるパスキー認証の導入を積極的に検討すべきである。

資料4-1-5　2次元コードを使った新たな手口



出所：フィッシング対策協議会、「緊急情報」

●なりすましメールを届かなくする対策が重要

フィッシング詐欺対策では、偽サイトへ誘導するなりすましメールをユーザーに届かないようにすることが重要である。その対策がDMARCである。フィッシング対策協議会の調査では、実在するサービスのメールアドレス（ドメイン名）を差出人としたなりすましメールが9割を超える月もあり、平均で66％と、この手口が依然として多く確認されている。

DMARCは2024年6月以降、グーグルやヤフーでメール送信の条件となったことから、日本国内の導入率も向上している。2024年7月の調査結果では、日経225銘柄企業での導入率が約80％に達している[6]。しかし、なりすましメールを届かなくするDMARCポリシーの拒否の設定率を見ると、米国（Fortune 1000企業）の46％に対し、国内（日経225銘柄企業）はわずか7％と低い[7]。このため、日本国内ではDMARCの効果が十分に発揮されていない。拒否以外のポリシーを設定しているドメインはなりすましメールの差出人として悪用されるリスクも高いため、事業者は拒否設定を推進し、自社ドメインのなりすましを防ぐことが重要である。

●スミッシング対策は、キャリア共通番号「0005」

SMSを使ったフィッシング（スミッシング）は配送物の不在通知をかたった手口が多いが、他の業界にもSMSが悪用されている。このスミッシングの対策として、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。

スミッシングは、偽サイト誘導による情報詐取

だけでなく、不正アプリのインストールが行われユーザー自身が偽SMSを送信するという攻撃加担につながる場合もある。そのため、事業者は安全なSMSを導入し、それを周知していくことが重要である。

■ユーザー側のフィッシング対策

●メールやSMSのURLをクリックしない

フィッシング詐欺では、本物のアドレスを使用したなりすましメールや、AIを使った流ちょうな日本語の偽メール、さらに、本物のウェブサイトを模倣した偽サイトが利用されるため、見抜くことが非常に困難である。そこで、偽物が混入する可能性を認識し、メールやSMSの本文内に記載されたURLをクリックしないことが重要である。

安全な行動としては、ECサイトなどのウェブサービスにはトップページからアクセスしたり、正規のアプリを利用したりすることがある。また、ウェブサービスが提供している安全機能を積極的に活用することも推奨される。特に、新しい認証方式であるパスキー認証は安全性が高く利便性も向上するため、積極的に利用してほしい。

●頻繁にフィッシングメールが届く場合の対策

頻繁に偽メールが届く場合は、使用しているメールアドレスが攻撃者に漏えいしている可能性が高い。漏えいしたアドレスは攻撃者間で売買され、その結果、複数の攻撃者から偽メールが送られることになる。このような状況では偽メールを止めることは難しく、メールアドレスを変更することが有効な対策となる。メールアドレスを変更する際は、なりすましメール対策としてDMARCに対応したメールサービスを選ぶことが望ましい。

●偽サイトに重要な情報を入力してしまったら

偽サイトに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、また、その可能性がある場合は、被害を最小限に抑え二次被害を防止するために、速やかに関係機関などに連絡・相談を行っていただきたい。その際は、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」が参考になる。

これらのユーザーの対策は、事業者側から注意喚起等で広く伝えていくことも重要である。フィッシング詐欺対策は、事業者側、ユーザー、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公式サイトで発信している緊急情報やフィッシング対策ガイドライン、啓発コンテンツなどを、ぜひご活用いただきたい。

●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/

1. 警察庁、「令和6年上半期におけるサイバー空間をめぐる脅威の情勢等について」、2024年9月19日
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.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」、2024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：2024/12 フィッシング報告状況」、2025年1月17日
https://www.antiphishing.jp/report/monthly/202412.html
4. フィッシング対策協議会、「緊急情報：QRコードから誘導するフィッシング」、2024年8月28日
https://www.antiphishing.jp/news/alert/qr_20240828.html
フィッシング対策協議会、「緊急情報 Amazonをかたるフィッシング」、2023年1月5日)
https://www.antiphishing.jp/news/alert/amazonQR_20230105.html
5. 注釈3に同じ
6. TwoFive、「国内DMARC統計とその傾向2024年12月版」
7. 日本プルーフポイント、「プルーフポイントの調査により、日経225企業および日本政府の「なりすましメール詐欺」対策は加速するも、米国水準には達していないことが判明」、2024年9月5日
https://www.proofpoint.com/jp/newsroom/press-releases/Nikkei225-Firms-and-Japanese-Gov-Accelerating-Measures2Combat-Email-Spoofing-Fraud

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～2025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