

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

フィッシング詐欺情報の届け出件数が前年の2倍以上に急増。新たな手口で被害範囲が拡大しており、金融以外でも対策が必要になっている。

■フィッシング詐欺被害の現状

フィッシング詐欺（Phishing）とは、主に銀行やクレジットカード会社といった金融機関を装ってメール（フィッシングメール）を送り、住所や氏名、銀行口座やクレジットカードの番号などの個人情報を詐取する行為である¹。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、そこで個人情報を入力させる手口が多い。

フィッシング対策協議会では、フィッシング詐欺に関連する情報提供を受け付けている。2020年9月は2万8575件で、2020年は同月までの累計で13万2811件となった（資料4-1-4～4-1-5）。これはすでに2019年通年の2倍以上の件数であり、急増していることが分かる。

ブランド名を悪用された企業の件数も、増加の傾向にある。特にアマゾン、楽天、三井住友カード、LINEをかたるフィッシングメールが繰り返され大量配信されており、これらの上位4ブランドで届け出件数全体の約9割を占めている。さらに、2020年には総務省の特別定額給付金に関するフィッシングメールも発生した²。

■インターネットバンキングのフィッシング詐欺被害

被害者の銀行口座から攻撃者の口座に不正送金させる、インターネットバンキングを狙った

フィッシング詐欺被害は、2015年に1495件・約30億7000万円まで拡大した（資料4-1-6）。不正送金ウイルスによる被害が多数を占めていたが、2016年から減少傾向となり、2018年には322件・約4億6000万円まで減っている。

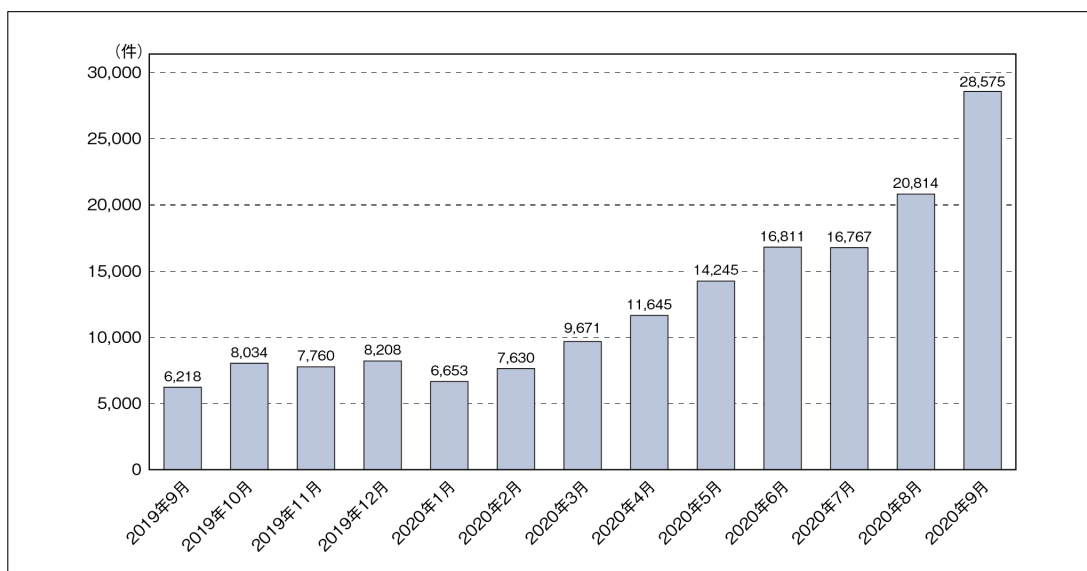
この減少はウイルス対策ソフトの導入やパターンファイルの更新、基本ソフト（OS）の更新など、利用者側の基本的な対策に加え、金融機関のフィッシング詐欺対策が進み、例えばワンタイムパスワードなどを使った複数要素認証などの普及によるところが多い。

しかし、新たな手口としてワンタイムパスワードを詐取するフィッシング詐欺などが発生したことから2019年、件数・被害額共に再度増加に転じている。

●ワンタイムパスワードを詐取して即時に不正送金を行う手法による金銭的被害が顕在化

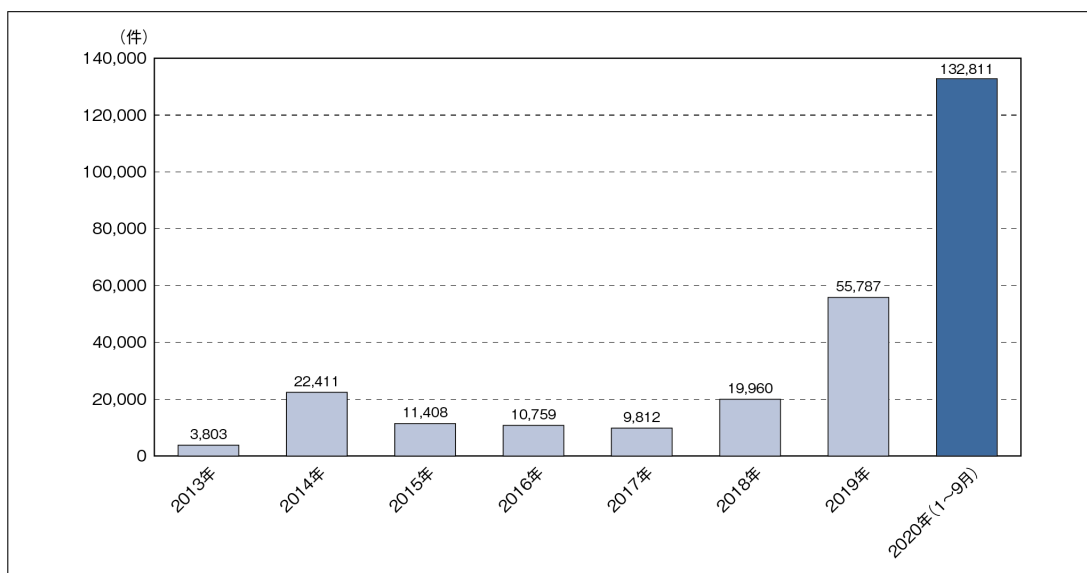
ワンタイムパスワードは、インターネットバンキングからの送金など重要な処理のときに求められるフィッシング詐欺対策の一つである。60秒ほどの短い時間で内容が変わる一度きりのパスワードを、あらかじめ登録したスマートフォンや専用の機械（トークン）に表示するものだが、攻撃者は本物そっくりのフィッシングサイトを用意し、このワンタイムパスワードの入力を待ち構え

資料4-1-4 フィッシング詐欺情報の届け出件数（月別）



出典：フィッシング対策協議会

資料4-1-5 フィッシング詐欺情報の届け出件数（年別）



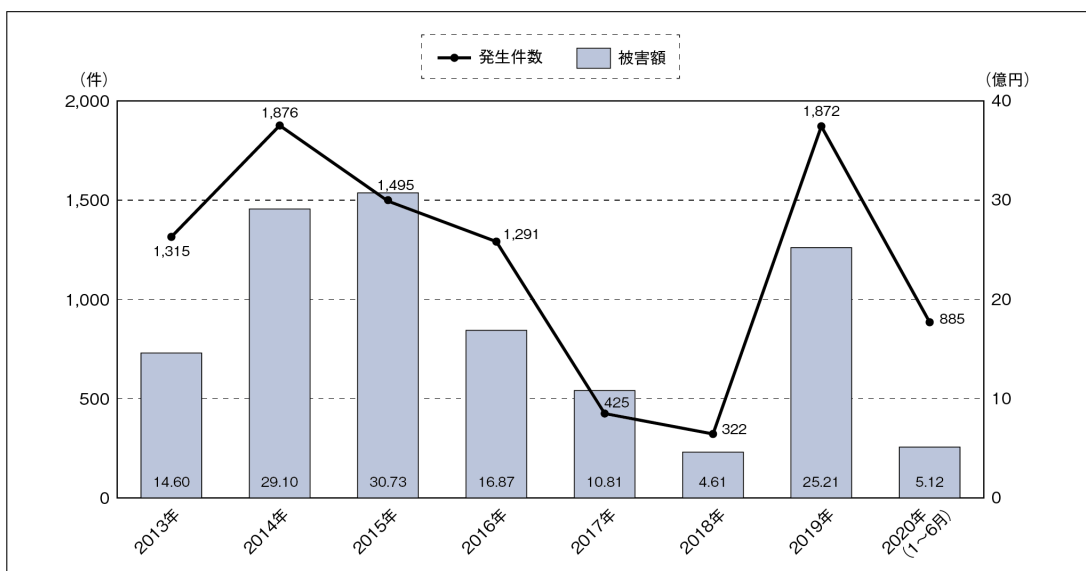
出典：フィッシング対策協議会

る。そして、パスワードの短い有効時間内に不正送金操作を完了させる。

決してワンタイムパスワードのセキュリティが危殆化したわけではなく、オーソドックスな

フィッシング詐欺の手口でワンタイムパスワードが突破されたのである。

資料 4-1-6 インターネットバンキングに係る不正送金事犯の発生状況



出典：警察庁

■クレジットカード情報が狙われている

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く、現在までの傾向は続いている。

アマゾンやアップルなどのメジャーブランドをかたったフィッシング詐欺の目的は、クレジットカード情報の詐取である。大手のクレジットカード会社はもちろん、2020年にはクラウド・コンピューティング・サービスやECサイトをかたりクレジットカード情報詐取を仕掛けたフィッシングサイトが多く発生している。クレジットカード情報の盗用による被害額は2017年から増加傾向にあり、2019年には約223億円まで拡大している（資料4-1-7）。

■フィッシング詐欺の実例と傾向、そして新たな手口

●宅配通知を装ったSMSの狙いはオンラインバンキングの不正送金

SMSによるフィッシング詐欺（Smishing）が

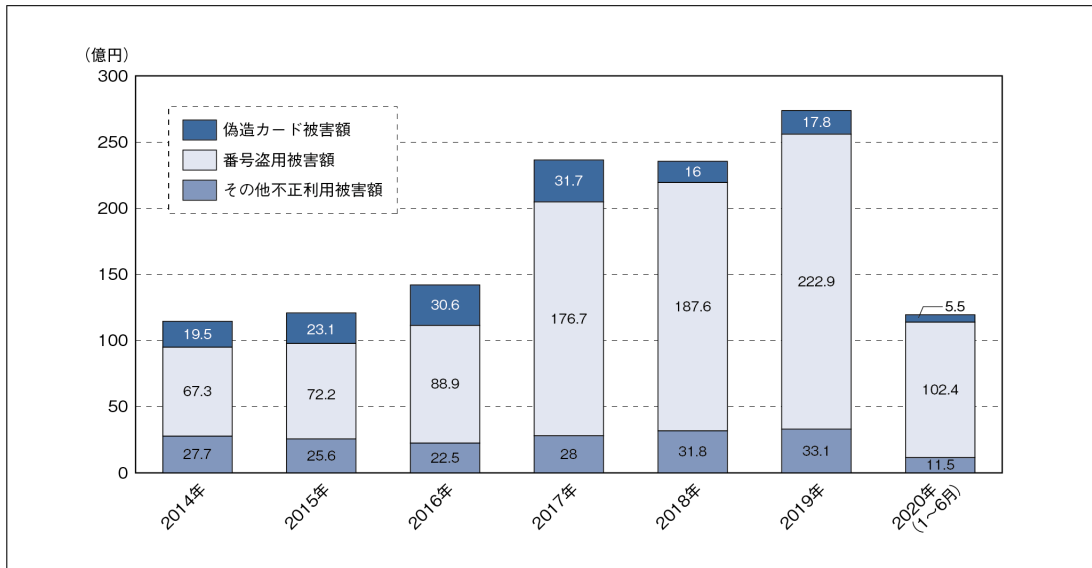
増加している。特に宅配業者の不在通知を装ったSMSは継続的に大量配信されており、不正送金を目的としたマルウェアのインストールや、金融機関やクレジットカードのブランドをかたるフィッシングサイトへの誘導が行われている。

フィッシング詐欺に使われるSMSは発信者番号をアルファベットで自由に表記できる国際網経由のものが使われていることが多いため、SMSの配信に国内直接接続の配信を利用するか、SMSの次世代版であるRCS（Rich Communication Service）に準拠したサービスを利用することが対策となる。RCSに準拠したサービスとして国内携帯3キャリアが提供を開始した「+メッセージ」（プラスメッセージ）は、2019年4月に機能が拡充されている。

●新たなターゲット「キャリア決済」「暗号資産」を狙ったフィッシング詐欺

キャリア決済を狙ったフィッシング詐欺が報告

資料 4-1-7 クレジットカードの不正利用被害額



出典：日本クレジット協会

されていることも新しい動きである。キャリア決済とは、携帯キャリアのIDとパスワード認証を利用することで、携帯電話料金と合算して商品などの代金を支払える決済サービスである。

具体的には、ソフトバンクや佐川急便などのブランドをかたってキャリア決済のIDとパスワードの不正詐取を行うフィッシングサイトが多く確認された。

さらに、暗号資産関連サービスをかたるフィッシング詐欺も報告されており、ここにきて、攻撃パターンが変化してきている。

●2020年のフィッシング詐欺の特徴

2020年のフィッシング詐欺には、以下のような特徴もあった。今後も変化するフィッシング詐欺の動向を注視し、対策を講じる必要がある。

- ・フィッシングメールが大量配信される頻度の増加（1日数回～十数回）

- ・本物と同じドメインを使ったなりすまし送信の増加

- ・国内ホスティング事業者の設備からの大量フィッシングメール配信

- ・誘導されるフィッシングサイトのHTTPS化（フィッシングサイト全体の50.4%）

■フィッシング詐欺対策は事業者と利用者の両者から

●事業者側の対策

フィッシング対策協議会は、事業者側の対策を「フィッシング対策ガイドライン」にまとめている。同ガイドラインの対策要件の中でも、利用者がフィッシング詐欺被害に遭うリスクを減らすために事業者が特に重点的に取り組むべきものをまとめたのが、以下の重要5項目である。

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. フィッシング詐欺対応に必要な組織編制とすること

また、認証方法調査・推進ワーキンググループでは、フィッシング詐欺対策と関連の高い利用者認証について事業者と利用者の双方にアンケート調査を行い、その結果を報告書として公開している。

フィッシング詐欺被害を防ぐためには、対応できる体制を整えフィッシング詐欺発生時の行動計画を策定することが重要である。例えば、フィッシングサイトに対しては閉鎖するための「テイクダウン」を行うが、それが遅滞なく行えるように役割や手順の明確化が必要になる。さらに、フィッシングサイトの多くが海外のサーバーに作られることから、専門機関にテイクダウンを依頼する方法を準備しておく必要もある。

フィッシング対策協議会では、コンピューター・セキュリティ・インシデントの対応組織であるJPCERTコーディネーションセンター（JPCERT/CC）を経由し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。

●利用者側の対策

フィッシング対策協議会は、利用者側の対策として「マンガでわかるフィッシング詐欺対策5ヶ条」や「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。

以下が、フィッシング詐欺対策5ヶ条である。

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。

インターネットを安全に楽しむための合言葉「STOP. THINK. CONNECT.」を活用することも有効である。

STOP＝立ち止まって理解する

THINK＝何が起こるかを考える

CONNECT＝安心してインターネットを楽しむ

■フィッシング詐欺の発生を早期に断ち切ることが必要

近年確認されているフィッシング詐欺においては、工程ごとの専門分業体制が確認されている。具体的には「計画」「調達」「構築」「誘導」「詐欺」「収益化」「強化拡大」の7つの工程があると分析されており、別々の犯罪者による請負・仲介・誘引が行われている。

この工程を断ち切ることがフィッシング詐欺発生阻止につながるとして、フィッシング対策協議会は長崎県立大学や会員事業者と連携して研究を行っており、よりプロアクティブなフィッシング詐欺対策の確立を目指している。

■参考資料

●フィッシング対策協議会

<https://www.antiphishing.jp/>

●フィッシング詐欺とは

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

●フィッシング報告状況（月次報告書）

<https://www.antiphishing.jp/report/monthly/>

●フィッシング対策協議会ガイドライン一覧

<https://www.antiphishing.jp/report/guideline/>

●フィッシング対策協議会ワーキンググループ報告書

<https://www.antiphishing.jp/report/wg/>

●「フィッシング対策ガイドライン」の改定について

https://www.antiphishing.jp/report/guideline/antiphishing_guideline2020.html

●「フィッシングレポート 2020」の掲載について
https://www.antiphishing.jp/report/wg/phishing_report2020.html

●「利用者向けフィッシング詐欺対策ガイドライン」の改定について

https://www.antiphishing.jp/report/guideline/consumer_guideline2020.html

●インターネットサービス提供事業者に対する「認証方法」に関するアンケート調査結果（2019年6月）

https://www.antiphishing.jp/news/pdf/wg_auth_report01_20190701.pdf

●インターネットサービス利用者に対する「認証方法」に関するアンケート調査結果（2020年9月）

https://www.antiphishing.jp/news/wg_auth_report_202009.pdf

●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://stopthinkconnect.jp/>

●警察庁サイバー犯罪対策プロジェクトの統計

<https://www.npa.go.jp/cyber/statics/>

●警察庁「令和2年上半年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」（2020年10月）

https://www.npa.go.jp/publications/statistics/cybersecurity/data/R02_kami_cyber_jousei.pdf

●日本クレジット協会のクレジット関連統計

<https://www.j-credit.or.jp/information/statistics/>

●「+メッセージ」の機能を拡充 — 携帯電話番号だけで、企業と安心・安全にメッセージのやりとりが可能に — <2019年4月23日>

https://www.nttdocomo.co.jp/info/news_release/2019/04/23_00.html

1. フィッシング（phishing）は、「魚釣り」（fishing）と「洗練された」（sophisticated）から成る造語であるといわれている。
2. フィッシング対策協議会、「2020/10 フィッシング報告状況」（<https://www.antiphishing.jp/report/monthly/202010.html>）



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が1996年～2021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(株式会社インプレスR&D)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(初期は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

株式会社インプレス R&D

✉ iwp-info@impress.co.jp

©1996-2022 Impress R&D