フィッシング対策協議会
Council of Anti-Phishing Japan

フィッシングレポート 2019

2019 年 5 月

フィッシング対策協議会

技術・制度検討ワーキンググループ

フィッシング対策協議会
Council of Anti-Phishing Japan

目次

1. フィッシングの動向

1.1. 国内外の状況

フィッシング情報の届け出件数は 2018 年も高水準で移行した。銀行やカード会社を騙るフィッシングの報告も依然としてある中、宅配業者、仮想通貨交換所、映像配信事業者などを騙るフィッシングなども報告されており、攻撃者の対象とするサービスが多様化してきている。

警察庁の発表[1]によると、2018 年上半期では、サイバー空間における探索行為などに基づくアクセス件数が増加している傾向にあり、仮想通貨のネットワークを標的としたアクセスなどが認められている。

一方、インターネットバンキングの不正送金の発生件数は減少傾向にあり、これは金融機関による対策の強化による効果であると考えられる。

フィッシング対策協議会の統計では、2018 年のフィッシング届け出件数が 3 月から急激に増加し、上半期は比較的高位な水準で推移した（図 1-1）。短縮 URL を用いてメールごとに異なる URL を送付する、不正アプリのインストールを促すサイトへ誘導するといった手口が増加したことが報告されている。

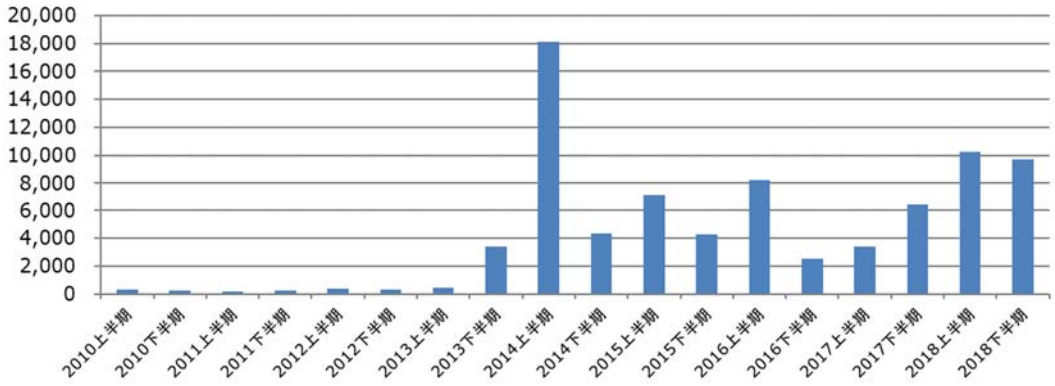

図 1-1　フィッシング情報の届け出件数

[1] 警察庁、 平成 30 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、
https://www.npa.go.jp/publications/statistics/cybersecurity/data/H30_kami_cyber_jousei.pdf

フィッシングサイトの URL 件数（重複無し）は、2018 年上半期では昨年度と比較し減少傾向にあったが、下半期に増加し（図 1-2）、ブランド名を悪用された企業の件数は増加の傾向にある（図 1-3）。

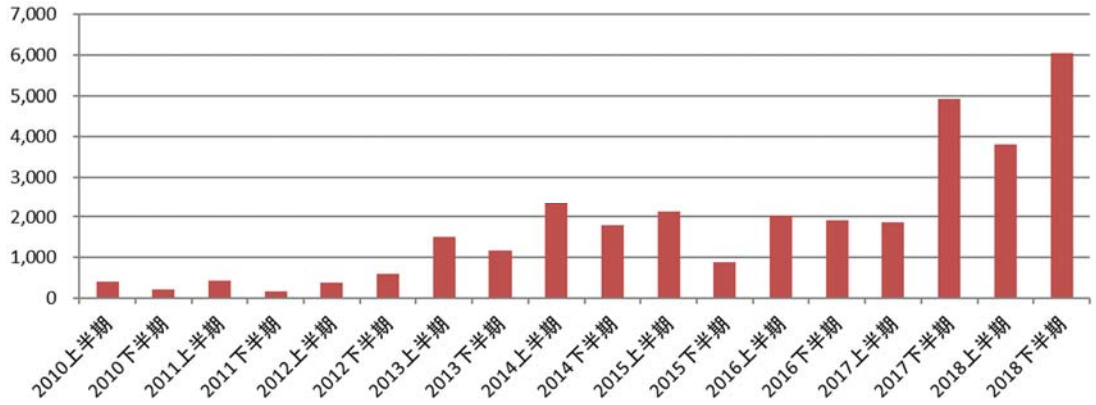

図 1-2　フィッシングサイトの件数

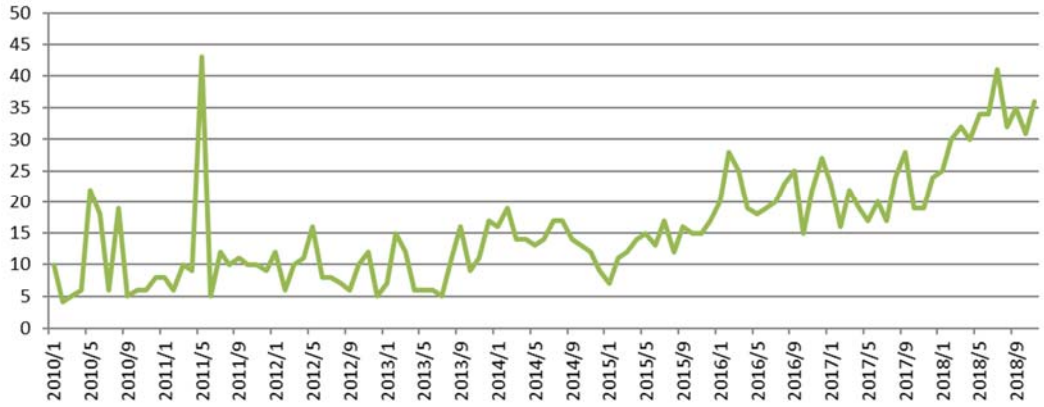

図 1-3　ブランド名を悪用された企業の件数

また、国家公安委員会・総務省・経済産業省の発表によれば、2018 年に警察庁に報告のあった不正アクセス行為のうち、識別符号窃用型不正アクセス行為（ID 窃盗による不正アクセス行為）は 2017 年に比べてやや減少した（図 1-4）。手口を見ると、2018 年におけるフィッシングは 3 件であり、前年と同様に比率は全体の 1%に満たない（図 1-5）。

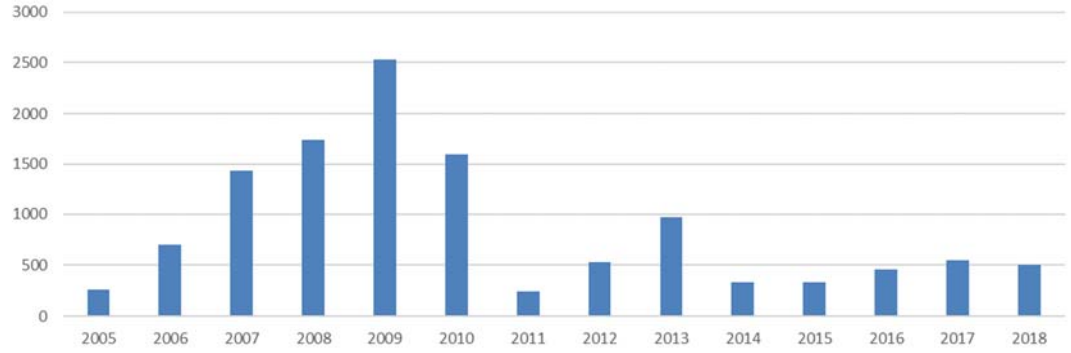

図 1-4　識別符号窃用（ID 窃盗）型不正アクセス行為の検挙件数[2]

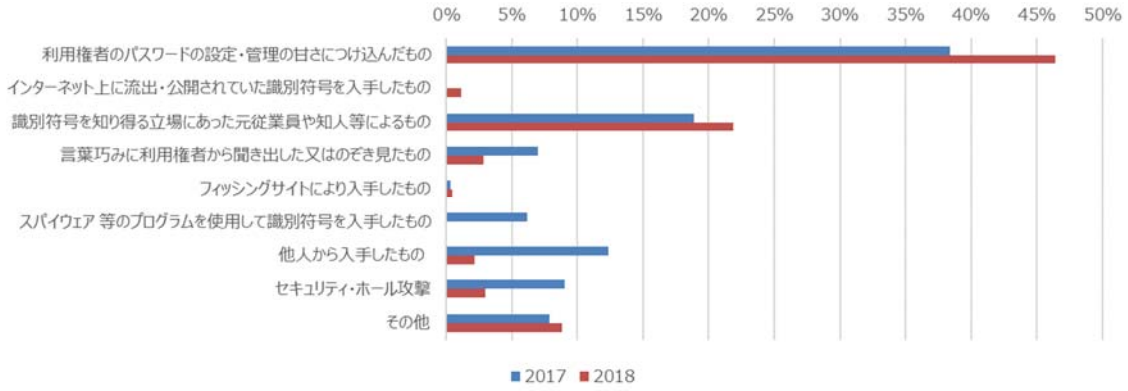

図 1-5　不正アクセス行為に係る犯行の手口の内訳（2017 年、2018 年）[3]

警察庁の発表[4]によれば、2018 年中の不正アクセス禁止法違反の検挙件数は 564 件であった。また、被疑者が不正に利用したサービスとしては「オンラインゲーム・コミュニティサイト」が 217 件を占めて最多となっている。ここ数年、利用者の銀行口座から不正送金させるインターネットバンキングを狙った不正送金事件が話題となっているが、インターネットバンキングの不正送金の被害件数（被害額）は、2016 年は 1,291 件（約 16 億 8,700 万円）だったのに対し、2017 年には 425 件（約 10 億 8,100 万円）、2018 年も 322 件（約 4 億 6,100 万円）と件数、被害額とも減少傾向が続いている。

[2] 国家公安委員会・総務省・経済産業省、「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」，http://www.soumu.go.jp/main_content/000606259.pdf よりフィッシング対策協議会が作成

[3] 同上

[4] 警察庁、平成 30 年におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/H30_cyber_jousei.pdf

1.2. 海外の状況

米国で設立されたフィッシング問題に関する国際組織 APWG(Anti-Phishing Working Group)の調査によれば、2018 年のフィッシング届け出件数は、2017 年からほぼ横ばいで推移した（図 1-6）。フィッシングサイトの件数は、2017 年上期に大幅に減少したものの、2018 年上半期では増加した（図 1-7）。フィッシングによるブランド名の悪用の件数はやや減少している（図 1-8）。

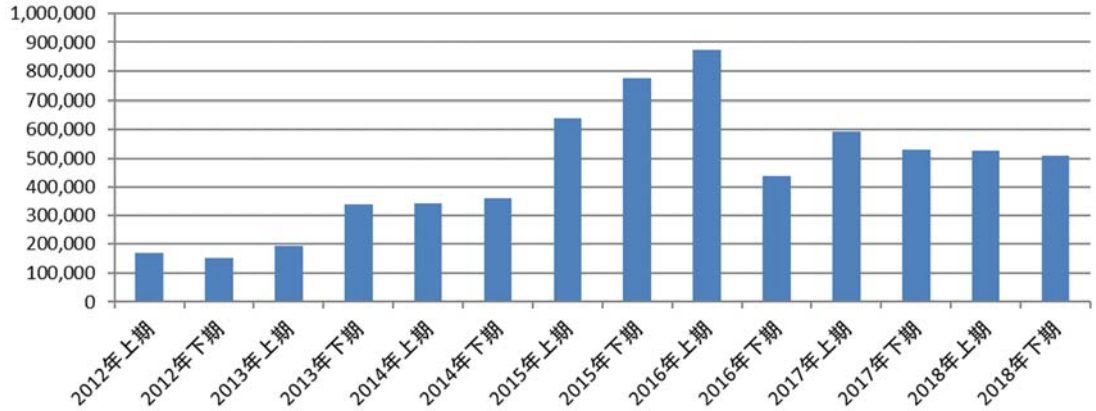

図 1-6　APWG へのフィッシングメール届け出件数[5]

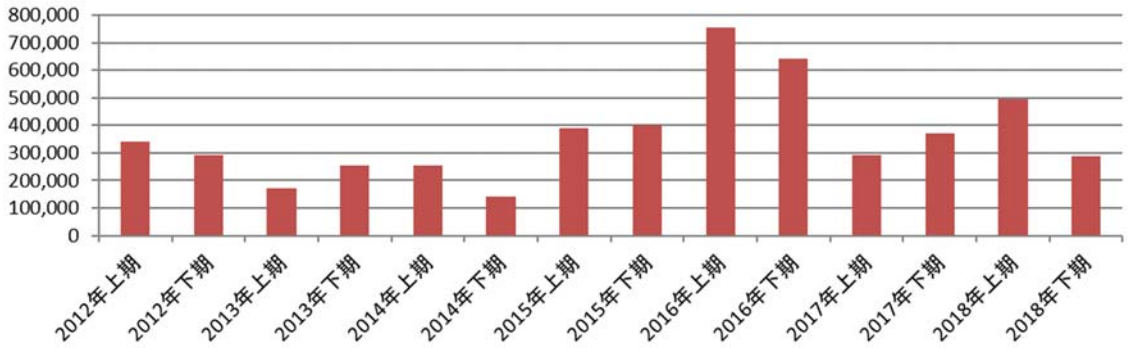

図 1-7　フィッシングサイトの件数（APWG）[6]

[5] APWG（Anti-Phishing Working Group)、"Phishing Activity Trends Report"、https://www.antiphishing.org/resources/apwg-reports/、よりフィッシング対策協議会にて作成
[6] APWG (Anti-Phishing Working Group)、 "Phishing Activity Trends Report"、https://www.antiphishing.org/resources/apwg-reports/、よりフィッシング対策協議会にて作成

図 1-8　フィッシングによりブランド名を悪用された企業の件数（APWG）[7]

[7] APWG (Anti-Phishing Working Group)、"Phishing Activity Trends Report"、https://www.antiphishing.org/resources/apwg-reports/、よりフィッシング対策協議会にて作成

1.3. フィッシングこの一年

2018 年 1 月から 12 月までのフィッシング報告件数は 19,960 件で、2017 年に比べ約 2 倍に増加した。2017 年はクレジットカード情報を詐取するフィッシングが多く報告されたが、2018 年も同様の傾向が続いた。クレジットカード会社、Apple や Amazon などのメジャーブランドをかたってクレジットカード情報の詐取を目的とするフィッシングサイトが多く確認されている。一般社団法人日本クレジット協会の発表[8]によると、2018 年 1 月から 9 月までのクレジットカードの番号盗用による被害額は 131 億円を超えており、2017 年の同時期に比べて約 1.5 億円増加している。この背景にはフィッシングによるクレジットカード情報の不正詐取があるとみられる。

また、2018 年には、新たに「キャリア決済」を狙ったフィッシングが報告された。「キャリア決済」とは、携帯電話の各キャリアの 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で商品等の代金を支払える決済サービスである。MySoftbank や佐川急便などのブランドをかたってこのサービスにログインするための 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（図 1-9）。

[8] 一般社団法人日本クレジット協会（クレジットカード不正利用被害の集計結果について）
https://www.j-credit.or.jp/download/news20181228b.pdf

図 1-9　MySoftbank のフィッシングサイト

長期にわたって発生しているフィッシングでは、その手法も手がこんできている。2018 年 5 月~6 月の約 2 ヶ月間にわたり発生した MyEtherWallet をかたるフィッシングでは、メールフィルタを回避するために、フィッシングメールにさまざまな文をランダムに埋め込む手法が使われていた（図 1-10）。また 2018 年 8 月から 2019 年 2 月現在まで約半年間にわたり、次々とフィッシングサイトが報告されている佐川急便をかたるフィッシングでは、2018 年 7 月までは Android 端末に不正アプリ（マルウエア）をインストールさせるように作られていたサイトが、8 月頃より、Android 端末以外の場合には、キャリア決済を不正利用するための情報（電話番号と認証コード）を詐取するフィッシングサイトとして動作するように作り替えられた（2.3 参照）。

HTMLメール

様々な文をランダムに埋め込んだメール例

図 1-10　断片的な文字列が入っているメール画像

フィッシング報告件数は増加の一途を辿っている。攻撃者の主たる狙いは依然としてクレジットカード情報であるが、キャリア決済も狙うなど、新たなターゲットも登場している。仮想通貨関連サービスをかたるフィッシングなどにおいては、攻撃パターンの変化も確認されている。今後も、変化するフィッシング動向を注視し、対策を講じる必要があるといえる。

2. 近年の攻撃の動向

2.1. フィッシングの国内外での定義、取り巻く環境について

セキュリティ関連の用語は、定義が明確に定まっていないことも多い。本協議会で扱う「フィッシング」についても、国内では比較的類似の定義がなされているが、グローバルで見ると同じとはいえない。

国内では、

① 送信者を詐称した電子メールを送りつけたり、偽の電子メールから偽のホームページに接続させたりするなどの方法で、クレジットカード番号、アカウント情報（ユーザ ID、パスワードなど）といった重要な個人情報を盗み出す行為のこと（総務省）

② 実在する組織を騙って、ユーザネーム、パスワード、アカウント ID、ATM の暗証番号、クレジットカード番号といった個人情報を詐取する（フィッシング対策協議会）

と定義されており、大きな違いはない。

一方、米国を拠点にしている APWG(the Anti-Phishing Working Group)の定義では、かなり広い定義がされている[9]。即ち、フィッシングは、個人識別データや金融機関の口座情報を搾取することを目的としている点は変わらないが、搾取手段として、「ソーシャルエンジニアリング」と「技術的な詐欺行為」の両方で行われていると述べている。

ソーシャルエンジニアリングの利用は国内の定義と基本的に同じであるが、技術的な詐欺行為では、犯罪目的の「マルウエア」を被害者のパソコンなどに挿入（導入）して、重要情報を搾取する方法であると述べている。

APWG の定義を考えると、搾取手段を、ソーシャルエンジニアリングと技術的な詐欺行為としているが、誰を騙すかを考えると、

①「人間を騙す」⇒ ソーシャルエンジニアリング

②「機器（PC など）を騙す」 ⇒ 技術的な詐欺行為

と考えることもでき、騙す対象が、人間か機械の違いだけで、基本は同じだと考えることもできる。

【内田 勝也　情報セキュリティ大学院大学】

[9] APWG の定義は、「Phishing Activity Trends Report」（四半期ごとに公表している）より引用

2.2. ソーシャルエンジニアリングの課題について

「フィッシングレポート 2017」では、ソーシャルエンジニアリングを以下の様に定義した。

人間の心理的な弱さを利用したり、他人になりすましたりして、必要な情報を盗み見したり、盗取するもので、いくつかの方法を組み合わせたり、複数の人から情報収集を行うこともある。

今回は、この考えを少し拡張して考えてみたい。前項 2.1 では、
“「人間を騙す」⇒ ソーシャルエンジニアリング”
と考えているが、誰が人間を騙すかを考えると、フィッシングでは、電子メールを送付して騙すと考えられ、実際には、“【攻撃者＋電子メール】で、【電子メール＋被害者】を騙している”と考えることができる。

そこで、これをそれぞれに分解して考えると、攻撃側も被害者側も

(a)人間、

(b)人間＋機械（コンピュータなど）、

(c)機械（コンピュータなど）

と考えることができる。ここで、人間単独の場合、電話や FAX などの単純な機器を利用するケースも「人間」と考える。

攻撃・防御の全体を示したものが、図 2-1 で、ソーシャルエンジニアリングを広義に考えてみることが可能になる。

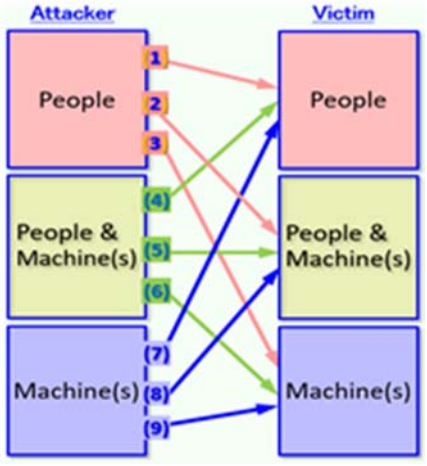

図 2-1 攻撃・防御の考え方

以下に、図中に矢印で示す攻撃のうち主なものを説明する。

(1)「人間」⇒「人間」:

対面や電話などを利用して、情報を窃取するもので、被害者を脅したり、騙したりする。2012 年 11 月に神奈川県下で発生した「ストーカー殺人事件」では、加害者男性が調査会社の経営者に依頼し、経営者は被害女性の夫になりすまし、言葉巧みに被害女性の住所を聞き出した。

(3)「人間」⇒「機械」:

生体認証（指紋、静脈など）を偽造し、生体認証装置を騙す。

(5)「人間＋機械」⇒「人間＋機械」:

電子メールを送付し、埋込 URL をクリックさせ、偽の Web で、アカウント

情報やクレジットカード情報などを窃取する。通常のフィッシングはこれに該当する。

(7)「機械」⇒「人間」:

2015 年 7 月に、カナダの出会い系サイトがハッカー攻撃を受け、大量の個人情報が漏えいしたが、その内容の調査で、女性会員アカウントの多くはニセモノ（ボット）で、ボットが多くの男性会員を騙していたことが判明した。

(9) 「機械」⇒「機械」:

インターネットにおける TCP 接続は、クライアントとサーバ間で３ウェイハンドシェイク（①SYN、②SYN ACK、③ACK）によって通信が始まる。クライアントが「③ACK パケット」を送らないと３ウェイハンドシェイクが完成しない。 このため、サーバは最後の「③ACK」パケットを待ち続ける。大量の「①SYN」パケットを送付すれば、サーバは大量の「③ACK」を待つことになり、サーバの処理能力が大幅にダウンする。

最近の AI の発展を考えると、騙されるのは人間だけでなく、機械（コンピュータ）なども騙される、あるいは、機械に人間が騙されることもあり、従来のソーシャルエンジニアリングやフィッシングなどの定義では対応できない現象がある、ということを考える必要がある。

【内田 勝也　情報セキュリティ大学院大学】

2.3. SMS から不正アプリに誘導し攻撃を行う事例について

企業から消費者への SMS 送信が日常的になる事に伴い、SMS を利用したフィッシングも増加傾向にある。消費者に馴染みのある大手の銀行や通販会社、運送会社などを騙り、情報や金銭を詐取することが目的のフィッシングが主である。SMS は携帯電話番号を宛先としてメッセージを送るサービスのため、スマートフォンを対象としたフィッシングを企む攻撃者にとっては好都合であると言える。

2018 年に新たに確認された手口として、7 月中旬頃から急増した佐川急便を騙ったフィッシングの事例を紹介したい。

当初は Android 端末を対象として不審アプリをインストールさせるための偽サイトへ誘導する SMS が送られていた。攻撃者は佐川急便を装い偽の不在通知を送り URL をタップさせる事によって偽サイトから不審アプリのダウンロードとインストールを誘導する。不審アプリをインストールした端末からは情報詐取や不正に遠隔操作をする事を可能になる。被害としてはキャリア決済サービスの不正使用や受信した偽の SMS と同様の内容を、自身の端末から見知らぬ電話番号宛に多数送信される事例などが報告されている。Android 端末は iPhone 端末と違い公式のアプリマーケット以外のサイトから提供元不明のアプリであってもユーザが許可する事でインストールが可能である事を利用した攻撃である。

8 月に入るとそれまでの Android 端末に対象を限定した手口だけではなく、iPhone 端末を対象とした手口も確認されるようになった。攻撃者は偽サイトへアクセスしてきた端末を自動的に iPhone 端末か Android 端末かを識別する。iPhone 端末に対して iPhone 端末用のページに誘導し、電話番号と認証コードの入力画面が表示される。利用者が画面の指示に従い入力すると攻撃者が当該電話番号に紐付いたキャリア決済サービスを不正使用する事が可能となる。8 月以降、実際に入力してしまいキャリア決済サービスによる身に覚えのないコンテンツなどの請求が発生したケースが確認されている。（図 2-2）

佐川急便だけでなく、12 月にはヤマト運輸を装った偽の不在通知 SMS が送られてくる事例も新たに確認された。佐川急便のケースと同様の手口であり、同じく不正に情報の詐取やキャリア決済の不正使用などの被害が懸念される。

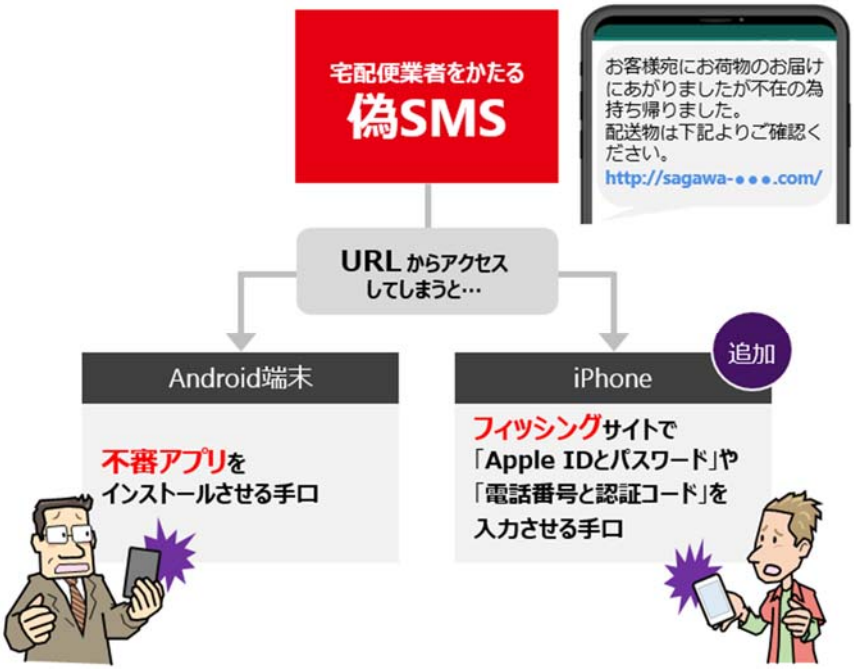

図 2-2 アクセスする端末種類ごとの手口分類[10]

SMS を利用したフィッシング詐欺のほとんどは、携帯電話端末もしくは国際網を経由した SMS 配信サービスを利用している。攻撃者は身元を特定される事を避けるため、比較的匿名での利用がしやすいこれらの送信手段を用いている事が多い。国内直接接続の SMS 配信サービスでは利用審査や契約手続きなどがあり、匿名での利用が困難なためである。

この点に着目すると、企業からの通知 SMS と攻撃者が送る詐欺 SMS を見極めることが消費者側の対策となる。具体的には発信者番号が 090 などから始まる国内の携帯電話番号で届いた SMS および海外の電話番号もしくはアルファベット表記で届いた SMS は、内容に関わらず詐欺の可能性を考慮して対応するのが有効である。フィッシングサイトの URL は本来のドメインと類似したドメインが用いられる事が多いため、上記のとおり発信者番号が疑わしい場合は安易に URL をタップせず真偽を確認する事が望ましい。

SMS を業務に利用する企業側の対策としては、消費者がフィッシング SMS と明確に区別できるよう国内接続の SMS 送信サービスを用いる事と、SMS を送信する際の発信者番号を自社ドメインの Web サイト上に掲載し、受信した SMS に疑いを持った消費者が容易に真偽を確かめられるよう事前に準備する

[10] IPA 情報処理機構　安心相談窓口だより
https://www.ipa.go.jp/security/anshin/mgdayori20181129.html

事が考えられる。SMS 配信経路ごとの特徴については、表 2-1 に整理した。

スマートフォンを利用した送金や決済の利便性が向上し一般に普及することは、同時に攻撃機会も増えることであり、より金銭的な被害が広がりやすい状況にある。SMS を業務に利用する企業側も消費者が被害にあわないための対策や注意喚起など対応が求められる。

表 2-1　SMS 配信経路ごとの特徴（フィッシング対策ガイドライン 2018 年度版より抜粋）

	国内直接接続の SMS 配信	国際網を経由した SMS 配信	携帯電話端末からの SMS 配信
発信者番号表示	日本の電話番号 （例：03-0000-0000） 携帯キャリア毎の特別番号 （例：50000）	海外の電話番号 （例：+1 000-000-0000） アルファベット （例：FOOBAR）	携帯電話番号 （例：090-0000-0000）
発信者番号登録・変更	契約者が自由には登録・変更できず、事前申請が必要	契約者が任意のタイミングで自由に登録・変更することが可能	携帯キャリアからの払い出しのみ
利用審査の厳格性	現在、審査をしないまま偽名や匿名での申込者に提供している事業者が存在しない	審査がなく偽名や匿名での申込者へ提供する事業者が存在する	端末レンタルサービス等で十分な審査を実施しないまま提供する事業者が存在する
Web サイト運営者の対策	自社が送信する SMS の発信者番号を利用者に対しウェブサイト等に記載し事前に通知したうえで利用する	フィッシャーに利用されやすく、利用者にとって自社が送信する SMS と判別しづらい事から、極力利用を避ける	フィッシャーに利用されやすく、利用者にとって自社が送信する SMS と判別しづらい事から、極力利用を避ける
利用者の対策	発信者番号は Web サイト運営者が事前に告知している番号と異なる SMS を受信した場合、フィッシングの可能性を疑い慎重に行動する	Web サイト運営者を騙ったフィッシングの可能性を疑い、慎重に行動する	Web サイト運営者を騙ったフィッシングの可能性を疑い、慎重に行動する
発信者番号の表示イメージ			

【福地雅之　NTT コム オンライン・マーケティング・ソリューション株式会社】

3. 対策の動向と課題

3.1. QR コードを利用したサイバー犯罪とフィッシング対策

キャッシュレス推進の目玉として注目されている QR コードを利用する決済について、QR コードの特徴である目視による視認性が低いことを悪用した手口が確認されている。QR コードのフィッシングには、アナログ的な手口と巧妙な手口が存在し、QR コードの読み取り方法によっても違った犯罪手口が存在する。なお、QR コードの読み取り方法は、QR コードを利用者の端末で読み取る方式（Merchant Presented Model。以下、MPM とする。）と、 利用者が端末に QR コードを表示して機器にかざす方式（Consumer Presented Model。以下、CPM とする。）がある。

MPM のアナログな手口の代表例は、本物の QR コードの上にフィッシング用の QR コードのシールを貼ってしまう手口である（図 3-1 上）。利用者は、視認性が低い QR コードではフィッシング用の QR コードとは気づかずに利用者の端末でフィッシング用 QR コードを読み取り、誘導されたまま決済をしてしまう。中国ではすでにこの手口の被害が発生しており、印刷された固定の QR コードの場合は利用金額の制限が設けられるなどの運用が開始されている。

CPM のアナログな手口の代表例は、ショルダーハッキングによる QR コードの盗撮被害である。店頭で利用者が端末に QR コードを表示しようと待機している後ろから悪意のある者が利用者の QR コードを撮影し、撮影した QR コードを店員に読み取らせるという手口である。利用者の QR コード自体が不変で固定の場合はこの被害を防ぐことが困難である。

最後に、MPM と CPM 両方に起こりうる巧妙な手口の代表例は、偽装 QR[11]を使った手口である（図 3-1 下）。偽装 QR を使った手口とは神戸大学大学院の森井昌克教授が提唱している本物の QR コードに微少なドットを 1 個混入させただけで識別子を変えるフィッシング攻撃の手法のことである。巧妙なことに、QR コードの誤り訂正技術の裏をかき、10 回に 9 回は正常な識別子として、1 回だけ偽の識別子として動作させることもできてしまう。

紹介した 3 つの手口の対策としては、固定の QR コードではなく都度ダイナミックに生成されるワンタイム QR コードを利用すること、QR コードの生成および表示側と読み取り側は証明書などを使って信頼関係を構築すること、固定

[11] Nikkei Fintech 2018.8 偽装 QR コードの脅威 神戸大学大学院 森井 昌克教授

の QR コードを利用せざるをえない状況であれば上限金額の制限をすることなどが有効である。

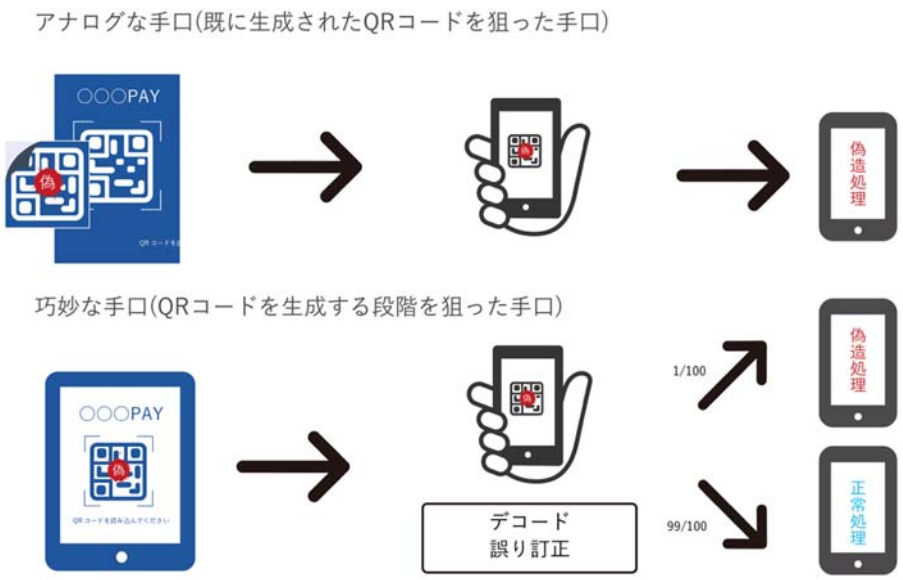

図 3-1 MPM のアナログな手口の代表例

【前澤 俊樹　株式会社 ISAO】

3.2. FIDO によるフィッシングへの対策

生体認証の導入はフィッシングへの対策として期待されている。生体認証を使用することで、フィッシングサイトから ID とパスワードを窃取された場合でも、攻撃者は生体認証を突破することができないためアカウントを保護することができる。以前は、ユーザが生体認証を利用するために専用端末を購入し、場合によっては持ち歩かなければならなかったが、近年は多くのスマートフォンで指紋認証や顔認証ができるようになり、生体認証がより身近になったと考えられる。

生体認証を実装する認証技術の一つとして、次世代の標準化されたオンライン認証技術として注目されている FIDO（Fast IDentity Online）という仕様がある。FIDO 自体はオンラインの認証基準に関する仕様のため、必ずしも生体認証を行うものではないが、生体認証と親和性が高く度々生体認証の導入で使用されている。

FIDO による認証の流れを図 3-2 に示す。

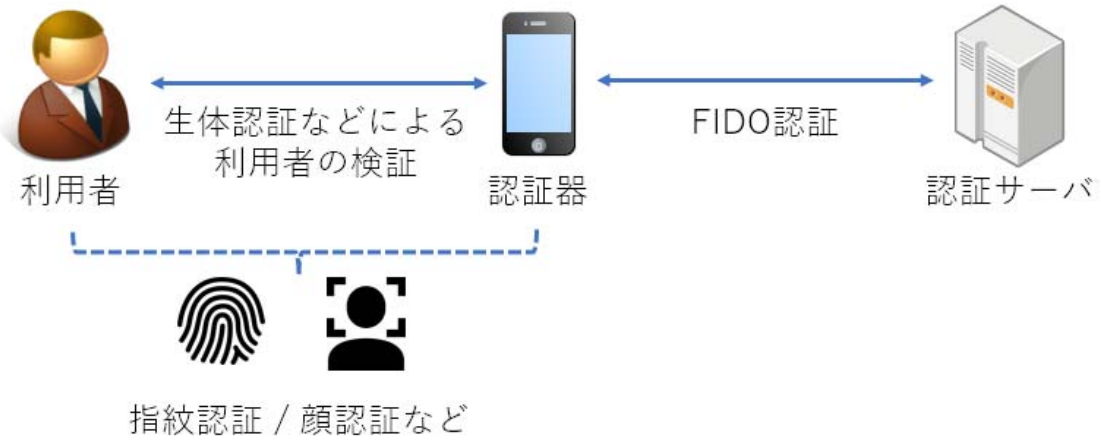

図 3-2 FIDO による認証の流れ

認証器（生体認証機能が付いたスマートフォンなど）が生体情報などで利用者を検証する。認証器は利用者が正常に検証されると、スマートフォンのアプリケーションなどを介して認証結果を認証サーバに送付する。認証サーバでは、識別したユーザ情報と認証結果を照合することで認証を完結させる。ここで注目すべき点は、生体認証は各ユーザの認証器で行っており、生体情報がネットワーク上に送受信されないということである。このため、万が一認証サーバが攻撃の被

害を受けたときや、ネットワークが盗聴された場合でも生体情報自体が漏えいすることがなく、安全に生体認証を行うことができる。

FIDO に準拠した認証方法で生体認証を行うためには認証器が必要であるが、FIDO に準拠している端末だけでなく、一部のスマートフォンの生体認証機能でも使用できることから利便性も高いと言われている。

FIDO は当初 U2F と UAF の 2 つの仕様で構成されていた。U2F (Universal 2nd Factor) では、認証器を用いた二要素認証を実現する。パスワードで最初の認証を行い、ハードウエアトークンなどで二要素目の認証を行う。一方、UAF (Universal Authentication Framework) では、スマートフォンの UAF に準拠した認証器を用いて生体認証を行い、パスワードの代替として認証を行うことができる。

現在では、U2F と UAF を統合した「FIDO2」と呼ばれる仕様が提案され、Web サービスの認証への応用などが期待されている。FIDO2 の中で特に注目されているものとして、WebAuthn (Web Authentication) がある。WebAuthn はブラウザ上で FIDO を実装する API である。WebAuthn が実装されている Web サイトに、FIDO に準拠した認証器と WebAuthn をサポートするブラウザでアクセスすると、パスワードの代替として FIDO を使用することが可能になる。WebAuthn は Web 関連の技術の標準化を行っている W3C と FIDO の標準化を行っている FIDO Alliance により策定され、すでに複数の大手ブラウザがサポートしており、これからの普及が期待されている。

【松本悦宜 Capy 株式会社】

3.3. DKIM と DMARC について

DKIM（DomainKeys Identified Mail）は送信ドメイン認証技術の一つで、他に SPF（Sender Policy Framework）がある。フィッシングメールは正規のメールサーバを経由せずにドメイン名（メールアドレスの@より右側部分）を偽って送信される場合があり、送信ドメイン認証技術はメールが正規なメールサーバから送信されたものであることを判別する機能となる。

3.3.1. DKIM の国内普及率

DKIM 署名の付与率は、総務省統計データによると 2017 年に 50%、2018 年 3 月には 60%を超え、DKIM の普及は進んでいると言える。DKIM の普及はフィッシング対策として事業者の取り組みによるものであるが、一部はメールクラウドサービスによる自動付与も含まれている。DKIM はフィッシングメールの対策の一つであることと、メールの改ざんを電子署名不一致により検知することもできため、メールクラウドサービスが安全のため自動付与することが進んでいる。

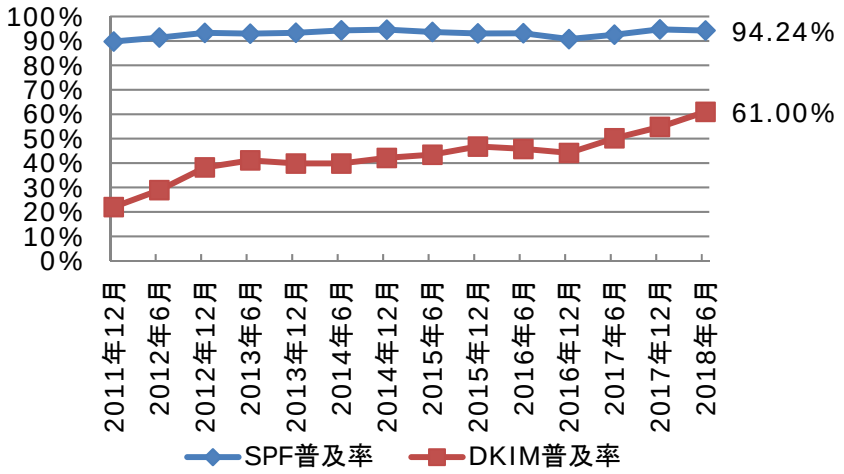

図 3-3 送信ドメイン認証普及率

3.3.2. DMARC の動向

DMARC （ Domain-based Message Authentication, Reporting & Conformance）は、SPF や DKIM の認証結果を元にメールヘッダ上の送信者情報（From:ヘッダ）のドメインとの関係性を比較して DMARC としての認証を行い、あらかじめ決めたポリシーにより送信者側がメールの挙動を管理することを可能とした仕組みである。DMARC の機能である DMARC レポートは、メールの送信元 IP、Header-From、Envelope-From、送信ドメイン認証の結果など、主になりすましの判定に使用された情報がレポートされる。送信事業者はレポートの状況から徐々に認証失敗したメールをフィッシングメールとして利用者に届けないようにする「受信拒否」のポリシー設定が可能であり、フィッシングメール対策として期待できる。DMARC レポートは XML 形式であるが、レポートを可視化するクラウドサービスがあり、導入を支援する環境も整ってきている。

2018 年の DMARC の設定状況は、JP ドメインにおいて 0.96%（2018 年 12 月末時点の総務省発表）と少ない。しかし海外では米国政府が DMARC 義務化を実施し、国内でもなりすましメール被害を受けた企業への導入が行われており、国内の普及が期待できる。

3.3.3. DKIM 普及に伴う新たな課題

DKIM 普及拡大の一方で DKIM 署名の認証失敗も発生しており注意が必要である。たとえば DKIM 署名後に、添付ファイルを ZIP 化するとメールの改ざんと同じことになってしまい、通信事業者の受信段階で DKIM 認証失敗となってしまう。添付ファイルの ZIP 化以外にも、マルウエア検知結果の情報付与や文字コード変換なども影響する場合がある。これはメールクラウドサービスの DKIM 自動付与機能の認識不足から発生する場合もあり、事業者側はクラウドサービスの機能を理解し、DKIM 署名実施の順番や実施個所を最適化する必要がある。DMARC 拡大につなげるためにも正しい DKIM 署名を推進する必要がある。

【加藤孝浩　トッパン・フォームズ株式会社】

3.4. ドメイン名の乗っ取りを防止するために

ドメイン名の乗っ取り（ドメイン名ハイジャックとも呼ばれる）は、ドメイン名の管理権限を持たない第三者が、不正な手段で他者のドメイン名を自身の支配下に置く行為である。

企業が利用しているドメイン名が乗っ取られた場合、

- インターネット利用者が正しい URL で Web にアクセスしているのに、偽の Web サイトが表示される
- 企業宛ての電子メールが盗まれ、機密情報や顧客情報が流出する
- ドメイン名の名義が第三者のものに書き換えられてしまう

といった企業の信頼に直結する被害が発生する。

ドメイン名の乗っ取りの手法としては、主に以下の 2 つの手段が用いられる。

- DNS サーバを狙い、不正な応答を返すようにする
- ドメイン名を管理するサービスに不正アクセスして登録情報を書き換える

企業の Web 担当者など、ドメイン名の管理に関わる立場においては、特に後者によるドメイン名の乗っ取りを防ぐために適切な管理を行う必要がある。

1. ドメイン名管理サービス利用のための適切な認証情報の設定

   ドメイン名管理サービスを利用するためのパスワードが安易であったために第三者による不正なログインが行われ、ドメイン名の登録情報や DNS 情報が書き換えられてしまうという事例が発生している。

   オンラインサービスに一般的な注意事項ではあるが、類推されにくいパスワードの設定とその適切な管理、二要素認証などによるセキュリティレベルの高い認証手段の選択肢があればその利用を検討することなどがあげられる。

2. 社内におけるドメイン名管理体制の確立

   企業など組織においてドメイン名の登録・利用を行う場合、組織内の複数の部門からそれぞれの利用目的のために勝手に複数のドメイン名管理サービスが利用されるような状況であると、その全容把握ができず、セキュリティ配慮に欠けた運用がなされたり、管理が放置されたりするドメイン名が発生し、ドメイン名の乗っ取りに繋がるリスクが大きくなる。組織としてドメイン名の管理を担当する部門・要員、および管理のためのルール・手順を社内で確立しておくことが必要である。

また、Whois（ドメイン名の登録情報をオンライン確認するサービス）での定期的な登録状態の確認や、ドメイン名管理サービスからの登録情報変更通知メールを一元的に確認することは、ドメイン名の乗っ取りなどの意図しない情報変更を迅速に検知するための手法として有効である。

3. ドメイン名乗っ取りを防ぐサービスの利用

ドメイン名の乗っ取りはドメイン名の登録情報が第三者により不正に変更されることで発生する。ドメイン名の種類やドメイン名管理サービスによってはこれを事前に防ぐためのサービスが提供されていることがある。サービスによって名称や手続きの詳細が異なることもあるが「ドメインロック（レジストリロック/レジストラロック）」と呼ばれ、これらを利用することでドメイン名の登録情報をオンラインの手続きで変更できないようにロックすることができる。

ロックされたドメイン名の登録情報を変更するためには電話による本人意思確認などの特別な手続きでロックを解除することが必要であり、パスワード漏洩などが発生した場合でも第三者により登録情報が不正に変更されることを防ぐことができる。

ドメイン名登録者本人の利便性を下げることにもなるが、セキュリティの確保が求められるドメイン名については積極的な利用を検討すべきである。

【宇井隆晴 株式会社日本レジストリサービス】

4. まとめ

4.1. フィッシングに対する対策の変化

フィッシング対策協議会は、2005 年 4 月に設立された。技術・制度 WG の活動は、2007 年から活動を開始し（途中、ガイドライン作成 WG と改称し、今年から技術・制度 WG）、その年度に「フィッシング対策における技術・制度調査報告書」を公開した。当時この中で攻撃技術と技術的対策と法・制度面を中心とした対策についてまとめているが、今回改めて最新の情報で更新し、表 4-1 のようにまとめた。

なお、2007 年にまとめたものを表 4-2 に掲載する。

攻撃手法については、SMS や MMS のようなメッセージングサービスが広く使われるようになった以外は、それほど大きな変化はないと思われる。

一方で、対策技術については、フィッシング準備段階の対策として、類似ドメインの取得があげられており、ガイドラインにも類似ドメインの取得が対策として推奨されていた。メール送信に対する対策としては、送信者認証が提案はされていたが、標準が定まっておらず、導入できる段階ではなかった。よって、精度に問題がある迷惑メールフィルタリング技術が唯一の技術的対策であった。

フィッシング対策の識別については、フィッシング対策ツールバーに対策が依存していて、サイトの実在を証明する EVSSL の技術が、フィッシングサイト識別技術として、特に信頼が必要とされるサイトについては、強く推奨されていた。

また、法・制度面での対策については、迷惑メール法と偽装 Web サイトへの著作権法の適用や盗んだ認証情報を悪用したときに不正アクセス禁止法の適用など、既存の法・制度の適用による対応で、積極的にフィッシングを防止するための法・制度は、整備されていなかった。

表 4-1　技術的対策と法･制度面での対策のまとめ（2019 年改訂版）

ステップ	内容	技術的対策方法	法･制度面での対策
0:フィッシングの準備	攻撃ターゲットの選別や電子メール送信のためのアドレス収集。類似ドメインの取得	信頼できる gTLD(.BANK の fTLD など)の利用 利用者に ID/Pass を与えずに、ID プロバイダーに認証を任せる ・任せられる IdP の数が少ない	課題：サービスプロバイダーがフィッシングの対象とならないために、容易な ID/Pass の提供の禁止。侵害時の迅速な公開の義務化
1：メールや SMS,MMS の送信	フィッシングサイトに誘導するために詐欺メールの送信	ISP によるメールフィルタリング技術 送信者認証、メールの電子署名 DKIM さらに DMARC の導入	不正アクセス行為の禁止等に関する法律の第 7 条（識別符号の入力を不正に要求する行為の禁止） 課題： DMARC 技術を推進する制度が必要とされる。
2:ユーザがメールや SMS,MMS に反応	届いたメールまたはメッセージングを開封し、URL をユーザが実行	証明書付き電子メール DMARC の MUA での確認の仕組み	不正アクセス行為の禁止等に関する法律の第 7 条（識別符号の入力を不正に要求する行為の禁止） 教育・啓発活動によるユーザの教育
3:フィッシング攻撃の実行	偽装サイトにユーザが訪れる	クロスサイトスクリプティングの脆弱性の除去 ユーザが容易にフィッシングサイトを見分けられるようにするための技術 ・フィッシング対策ツールバー ・実在性も保証する厳密な証明書(EVSSL) ・サイト画像認証	不正アクセス行為の禁止等に関する法律の第 7 条（識別符号の入力を不正に要求する行為の禁止）
4:機密情報の送信	偽装サイトにユーザが個人識別情報を入力する	ID プロバイダーを使うなど、そもそもユーザ認証を求めない技術の導入	不正アクセス行為の禁止等に関する法律の第 6 条（他人の識別符号を不正に保管する行為の禁止） 課題：制度面での技術の普及の後押しが必要
5:機密情報の入手	偽装サイト上の収集された個人識別情報をフィッシャーが取得	マルウエアによる識別情報の盗み取りを防止するための技術 ・ソフトキーボード、キーロガー検知	不正アクセス行為の禁止等に関する法律の第 6 条（他人の識別符号を不正に保管する行為の禁止）
6:機密情報の利用	個人識別情報を利用してユーザになりすましてサービスを利用	盗み出した個人識別情報を利用してもなりすましを出来ないようにするための技術 ・二要素認証 ・帯域外認証 ・トランザクション署名	不正アクセス禁止法 課題：制度面での技術の普及の後押しが必要 コスト面での課題は低くなったが、普及が問題
7:不正行為の実行	クレジットカードの利用や預金の引き落としなど不正行為の実行	トランザクションの不正検知	現行の刑法に順ずる 課題：国際的な犯罪に対する国内法の限界

表 4-2　技術的対策と法･制度面での対策のまとめ（旧 2007 年版）

ステップ	内容	技術的対策方法	法･制度面での対策
0:フィッシングの準備	攻撃ターゲットの選別や電子メール送信のためのアドレス収集。類似ドメインの取得	類似ドメイン取得の監視	類似ドメイン取得の禁止 JPRS による類似ドメイン取得に関する注意喚起の提供
1：メールの送信	フィッシングサイトに誘導するために詐欺メールの送信	ISP によるメールフィルタリング技術 送信者認証、メールの電子署名 課題:迷惑メール用フィルタのため、フィッシングの場合フィルタの誤検知のとの見分けが付かない	迷惑メール法、偽装メールに対する著作権法の適用 課題： 送信者認証や電子署名の技術を推進する制度が必要とされる。
2:ユーザがメールに反応	届いたメールを開封し、URL をユーザが実行	証明書付き電子メール	教育・啓発活動によるユーザの教育 フィッシング対策協議会の Web によるフィッシングの啓発活動
3:フィッシング攻撃の実行	偽装サイトにユーザが訪れる	クロスサイトスクリプティングの脆弱性の除去	偽装 Web に対する著作権法の適用
4:機密情報の送信	偽装サイトにユーザが個人識別情報を入力する	ユーザが容易にフィッシングサイトを見分けられるようにするための技術 ・フィッシング対策ツールバー ・実在性も保証する厳密な証明書(EVSSL) ・サイト画像認証 ・画像を利用したユーザ認証	課題：制度面での技術の普及の後押しが必要
5:機密情報の入手	偽装サイト上の収集された個人識別情報をフィッシャーが取得	マルウエアによる識別情報の盗み取りを防止するための技術 ・ソフトキーボード、キーロガー検知	課題：個人識別情報の入手を罰する手段がない
6:機密情報の利用	個人識別情報を利用してユーザになりすましてサービスを利用	盗み出した個人識別情報を利用してもなりすましを出来ないようにするための技術 ・二要素認証 ・帯域外認証 課題：コスト	不正アクセス禁止法 課題：制度面での技術の普及の後押しが必要
7:不正行為の実行	クレジットカードの利用や預金の引き落としなど不正行為の実行	トランザクションの不正検知	現行の刑法に順ずる 課題：国際的な犯罪に対する国内法の限界

今回改めて、技術的対策と法・制度面での対策を整理しなおしてみて、以前と比較していろいろな点で改善が進んでいると再認識した。

【法・制度面での対策の変化】

大きく改善があったのが、法・制度面での対策である。2012 年に不正アクセス禁止法が改正され、フィッシング行為および ID・パスワードの不正取得に対する罰則が適用できるようになり、フィッシング攻撃の実行、機密情報の送信、機密情報の入手を取り締まれるようになった。

【ドメイン名に対する対策の変化】

「フィッシングの準備段階」においては、gTLD の拡大により類似ドメインの取得がほぼ無限に可能となり、あらかじめ類似ドメインを抑えるという方法は、不可能となった。一方で、gTLD として企業の企業名やサービス名などを使えるブランド TLD や fTLD（.BANK，.INSURE）などの特殊な gTLD の取得が可能となり、大手の企業においては、自ドメイン名を TLD として登録することにより、ドメイン名の認知を上げ、第三者がフィッシングサイトを類似ドメインで作成するのを難しくすることができる。

【ID・パスワードの提供に対する対策の変化】

ここ最近、杜撰なサービスプロバイダーのサイトからの ID とパスワードの大量の流出が大きな問題となっている。利用者は、一般的に同じ ID とパスワードを複数のサイトで使いがちである。そのため、いずれかのサイトで、それが漏洩した場合、利用者に迅速に通知する必要があるが、一般的には、それらが公開されないケースも多く、利用者は、自身の ID とパスワードの漏洩を知らずに、同じ ID とパスワードで他のサイトも使い続け、利用者を危険にさらしている。それらを防ぐためには、サービスプロバイダーが容易に ID とパスワードを利用者に提供するのを防ぐ制度が求められる。最近、ID プロバイダーの普及が進んできて、一部のサービスでは、サイト固有の ID・パスワードを使わずに、ID プロバイダーの認証を使うサービスも出てきてはいるが、まだまだ一般的とは言えない。また、一部では ID プロバイダーの信頼が問題となっているケースも出てきている。

【受信メールに対する対策の変化】

メールについては、技術的な対策として、送信者認証の認知が上がってきているので、今後は DKIM さらに DMARC の普及を期待したい。ただ、若者の間ではメールより、SMS や MMS の利用が多くなり、フィッシングの誘導も SMS や

MMS によるものが増加してきて、そちらに対する技術的な対策が今後必要とされる。

【多要素認証の対策の変化】

インターネット銀行については、2007 年に比べ、大きな改善があった。2007 年当時は、マトリックスカードによるワンタイムパスワードが主流で、マトリックスカードの全数字を要求するフィッシング攻撃が行われ、攻撃者にカードのすべての情報を取られるというケースが発生した。特に 2015 年は、SHIFU や VAWTRAK と呼ばれるバンキングマルウエアの被害が急増し、警察庁の発表でも不正送金被害額が過去最悪の約 30 億となった。これを機に銀行では、マトリックスカード方式から、ハードウエアトークンによるワンタイムパスワードの導入が進み、さらにトランザクション署名による送金トランザクションを保護する技術の導入が進み、インターネットバンキングの被害は、減少傾向となった。また、スマホの普及により、スマホを使った多要素認証が容易に導入でき、SNS のようなカジュアルなサービスにおいても多要素認証が使えるようになった。

上記のように、この 10 年で法・制度面でも技術面でもフィッシングを防ぐ対策は、随分進化したが、いまだにフィッシングは、サイバー攻撃の起点として、使われ続けている。フィッシング攻撃に対しては、有効な対策が出てきているので、普及や認知を進める必要があり、フィッシング対策協議会では、今後ともフィッシング対策技術の普及・啓発に努めたいと思う。

【野々下 幸治 トレンドマイクロ株式会社】

4.2. 提言

フィッシング詐欺における 2018 年の協議会への報告件数と URL 件数を見てみると、特異的に多かった 2014 年の報告件数を除き、それぞれ過去最多となった。悪用されたブランド数も 2017 年から大幅に増加しており、幅広い分野に対して、多くの URL（サイト）を高回転で使って攻撃していることがうかがえる。

インターネットで何らかのサービスを行う事業者は、フィッシングは特定分野の企業だけが狙われるのではなく、いつ自分が狙われてもおかしくない状況であると認識し、事前の対策に取り組みたい。

また、近年、フィッシングは、単に金銭目的だけでなく、企業の機密情報奪取や国家間の軍事的、政治的諜報などの足掛かりにもされることから、インターネットサービスのお客様向け取り組みだけでなく、自社・自組織ネットワークをも守るため、社員などへの啓発や自社ネットワークや利用サービスのログインセキュリティなどの強化も推進したい。

各事業者は、多種多様なフィッシングへの対抗、事前の対策として、ワンタイムパスワードの導入とともにその利用を促進するなど、より強固な個人認証の採用や利用促進のために利用者の意識を高める必要がある。昨今、ワンタイムパスワードの奪取も自動化するなどの高度化した手口も見受けられ、それらに対抗する FIDO 認証なども注目されている。フィッシングを含む多くのサイバー攻撃の起点となる標的型メールや無差別のフィッシングメールなどに高い効果が期待できる DMARC の採用についても是非検討したい。

本協議会は引き続きフィッシングに関する最新情報を収集し、新たな手法に対する対策の展開や啓発などを推進し、利用者・事業者の皆様を今後とも一層支援していくこととしたい。

【早川和実　NTT コミュニケーションズ株式会社】
【長谷部 一泰　アルプス システム インテグレーション株式会社】

（空白）

フィッシング対策協議会　技術・制度検討ワーキンググループ
構成員名簿

（敬称略・順不同）

【主査】
内田 勝也　情報セキュリティ大学院大学名誉教授
【副主査】
野々下 幸治 トレンドマイクロ株式会社
【構成員】
伊藤 彰浩　株式会社アクリート
長谷部 一泰 アルプス システム インテグレーション株式会社
加藤 孝浩　トッパン・フォームズ株式会社
林 憲明　トレンドマイクロ株式会社
宇井 隆晴　株式会社日本レジストリサービス
山本 和輝　BB ソフトサービス株式会社
松本 悦宜　Capy 株式会社
前澤 俊樹　株式会社 ISAO
山田 晃義　株式会社 ISAO
早川 和実　NTT コミュニケーションズ株式会社
黒田 和宏　NTT コム オンライン・マーケティング・ソリューション株式会社
福地 雅之　NTT コム オンライン・マーケティング・ソリューション株式会社
磯邊 良太　一般社団法人全国銀行協会
木村 泰司　一般社団法人日本ネットワークインフォメーションセンター
木村 未咲　株式会社三菱 UFJ 銀行
瀬古 敏智　株式会社三菱 UFJ 銀行
貞広 憲一　株式会社みずほフィナンシャルグループ

【オブザーバ】
経済産業省商務情報政策局サイバーセキュリティ課

【事務局】
一般社団法人 JPCERT コーディネーションセンター
エム・アール・アイリサーチアソシエイツ株式会社（株式会社三菱総合研究所）