

フィッシングレポート 2022

2022 年 6 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

目次

1. フィッシングの動向	1
1.1. 国内の状況	1
1.2. 海外の状況	4
1.3. フィッシングこの一年	6
1.3.1. ...フィッシングのターゲットとなっているブランド	6
1.3.2. ...「なりすまし」送信メールの継続	7
1.3.3. ...スミッシングで狙われるキャッシュレス決済	7
2. WG の活動	8
2.1. 今年度の WG 活動	8
2.2. フィッシング対策協議会 各 WG の活動	9
2.3. 認証方法、調査・推進 WG による意見	14
3. SMS を用いたフィッシング詐欺についての意識調査	17
4. フィッシングの対策	25
4.1. 最新の動向	25
4.1.1. ...FIDO とフィッシング耐性への期待	25
4.1.2. ...フィッシング関連情報の収集・共有による効果と課題	27
4.1.3. ...フィッシング対策のシフトレフト	29
4.1.4. ...フィッシングサイトの短時間化と被害発生状況の推移からの課題	32
4.1.5. ...携帯キャリアによる SMS に関する施策・フィッシング対策	35
4.1.6. ...IT サービス認証における推奨事項	37
4.2. ドメイン関連	39
4.2.1. ...ドメイン名の廃止にあたっての注意	39
4.2.2. ...ドメイン名を廃止する前のリスク判定	41
5. まとめ	47

1. フィッシングの動向

1.1. 国内の状況

警察庁の発表¹によると、2021 年上半期では、国内外でランサムウェアによる攻撃が多発している。また、警察によるサイバー犯罪の検挙件数は、年間の検挙件数が最多となった前年の同期と比べ増加しており、令和 3 年上半期における不正アクセス禁止法違反の検挙件数は 146 件であった。このうち 123 件が識別符号盗用型（アクセス制御されているサーバーに、ネットワークを通じて、他人の識別符号を入力して不正に利用する行為）であったことが報告されている。

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、発生件数 376 件、被害額約 4 億 7,900 万円となり、前年同期と比べて発生件数、被害額ともに減少した。被害の多くは、前年から継続している SMS や電子メールを用いて金融機関を装ったフィッシングサイトへ誘導する手口によるものと報告されている。

フィッシング情報の届け出件数について、2021 年は前年と比較して著しく増加した（図 1-1）。EC サイト大手、クレジットカード会社などのなりすまし送信が多く報告されている。

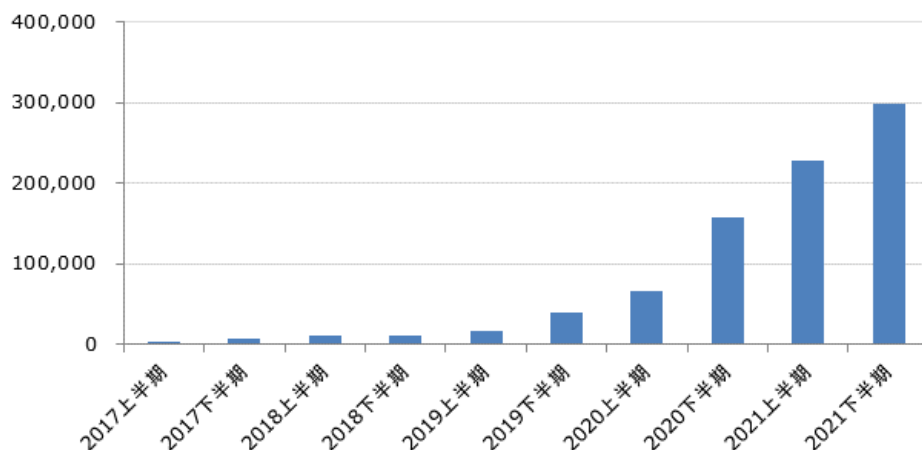


図 1-1 国内のフィッシング情報の届け出件数²

¹ 警察庁、令和 3 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/R03_kami_cyber_jousei.pdf) (閲覧日：2022 年 2 月 21 日)

² フィッシング対策協議会、フィッシング報告状況（月次報告書）
(<https://www.antiphishing.jp/report/monthly/>) (閲覧日：2022 年 2 月 21 日) より作成

フィッシングサイトの URL 件数は、2021 年度下半期は 2021 年上半期よりも増加している。(図 1-2)。ブランド名を悪用された企業の件数も、2020 年と比較して増加の傾向にある(図 1-3)。

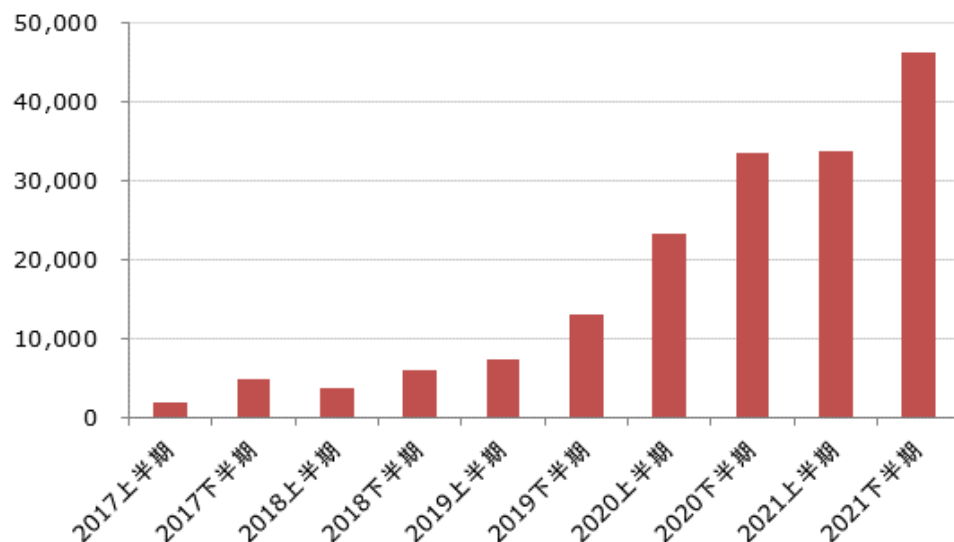


図 1-2 国内のフィッシングサイトの件数²

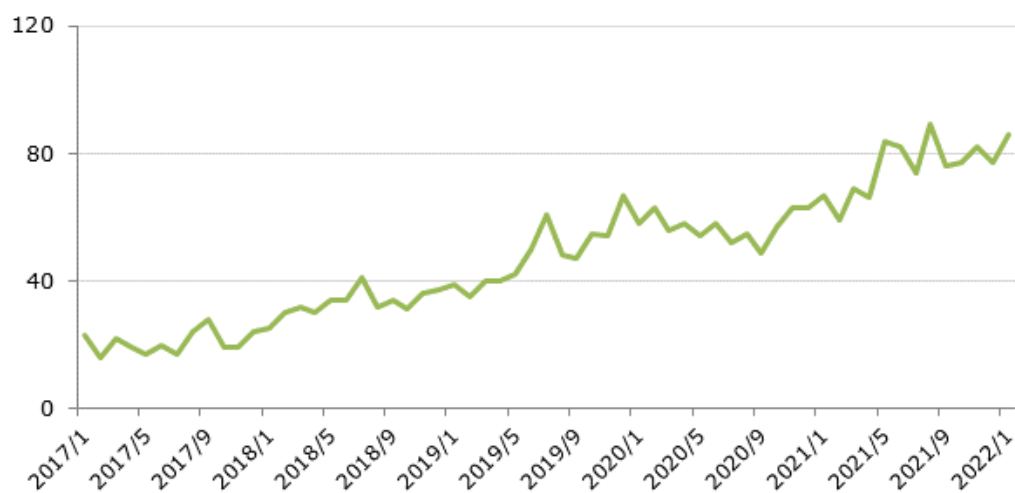


図 1-3 国内のブランド名を悪用された企業の件数²

また、警察庁・総務省・経済産業省の発表³によれば、2021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2020年に比べて減少した（図 1-4）。しかしながら、2021年の手口別内訳では、利用権者のパスワードの設定・管理の甘さにつけ込んで入手したものの割合が最も高く、前年比で約 1.5 倍の増加となった（図 1-5）。

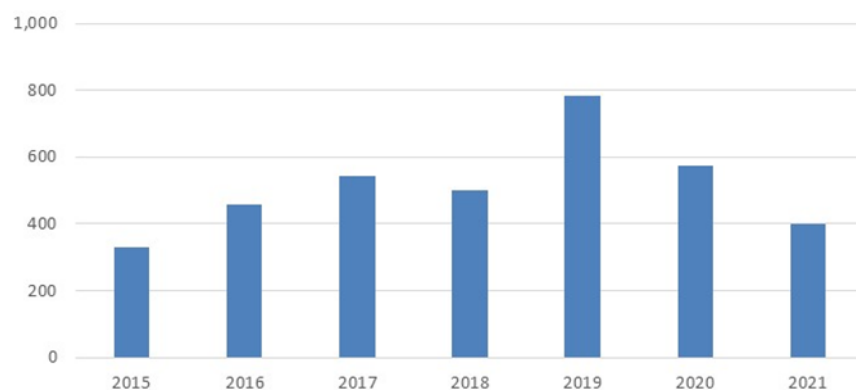


図 1-4 識別符号窃用（ID 窃盗）型不正アクセス行為の検挙件数⁴

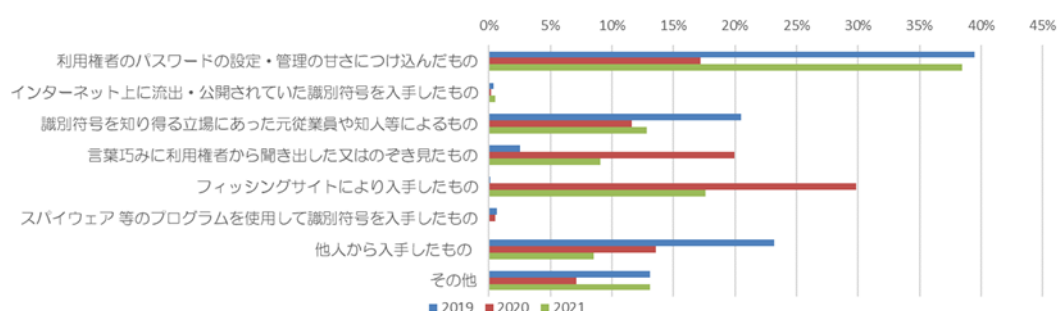


図 1-5 識別符号窃用型不正アクセス行為の手口別検挙件数の内訳
（2019年～2021年）⁵

【エム・アール・アイリサーチアソシエーツ株式会社】

³ 警察庁・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（https://www.soumu.go.jp/main_content/000807446.pdf）（閲覧日：2022年4月11日）

⁴ 同上より作成

⁵ 同上より作成

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、2020 年のフィッシング届け出件数は、2019 年から大幅に増加した (図 1-6)。フィッシングサイトの件数は、2020 年上半期には減少傾向であったが、2020 年下半期、2021 年上半期は大幅に増加した (図 1-7)。フィッシングによるブランド名の悪用の件数は増加傾向にある。(図 1-8)。APWG の報告⁶によると、金融機関に対するフィッシングが拡大したことが報告されている。全体のフィッシングの動向としては、Business Email Compromise のフィッシングが増加していることが示されている。

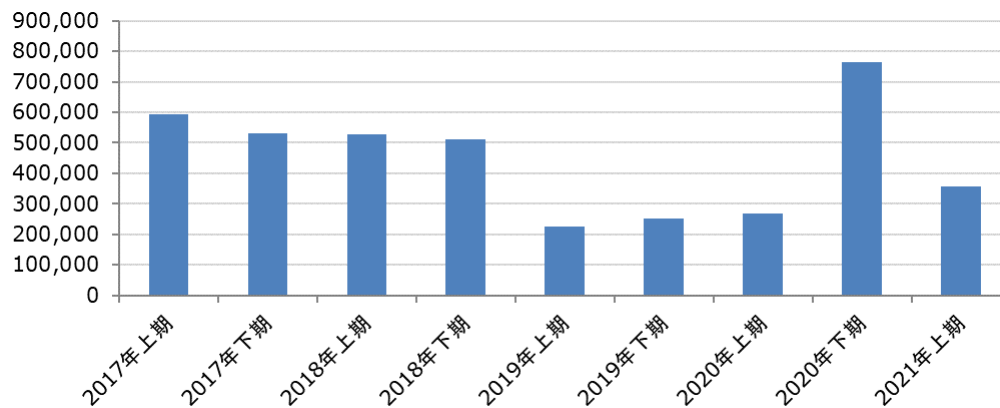


図 1-6 APWG へのフィッシングメール届け出件数⁷

⁶ APWG (Anti-Phishing Working Group)、"Phishing Activity Trends Report"
(https://docs.apwg.org/reports/apwg_trends_report_q2_2021.pdf?_ga=2.108698310.537511705.1644904958-1869577878.1641523189&_gl=1*268s0q*_ga*MTg2OTU3Nzg3OC4xNjQxNTIzMTg5*_ga_55RF0RHXSr*MTY0NDkwNDk1OC4yLjEuMTY0NDkwNTk4Ny4w)
(閲覧日：2022 年 2 月 21 日)

⁷ APWG (Anti-Phishing Working Group)、"PHISHING ACTIVITY TRENDS REPORTS"
(<https://www.antiphishing.org/resources/apwg-reports/>) (閲覧日：2022 年 2 月 21 日) より作成

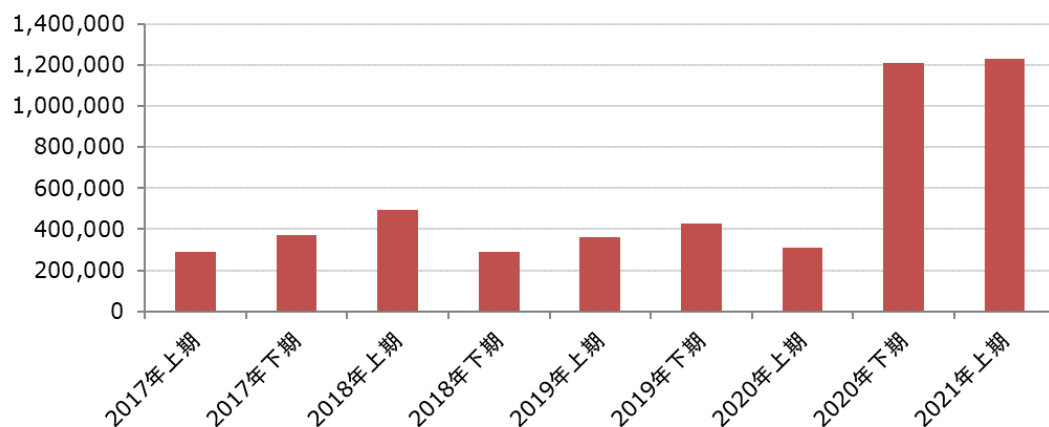


図 1-7 フィッシングサイトの件数（APWG）⁸

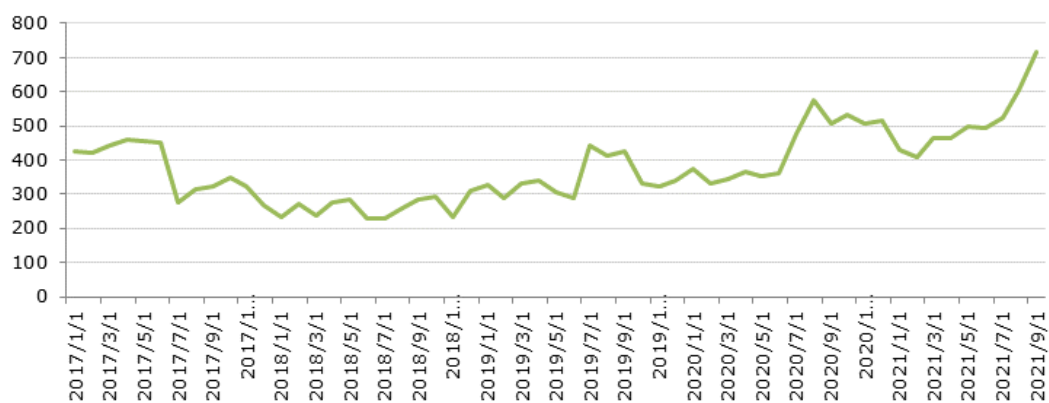


図 1-8 フィッシングによりブランド名を悪用された企業の件数（APWG）⁹

【エム・アール・アイリサーチアソシエーツ株式会社】

⁸ APWG (Anti-Phishing Working Group)、"Phishing Activity Trends Report"
(<https://www.antiphishing.org/resources/apwg-reports/>) (閲覧日：2022 年 2 月 21 日) より作成

⁹ 同上より作成

1.3. フィッシングこの一年

フィッシング対策協議会で受領した 2021 年 1 月から 12 月までのフィッシング報告件数は 526,504 件で、2020 年と比較して約 2.3 倍となった。

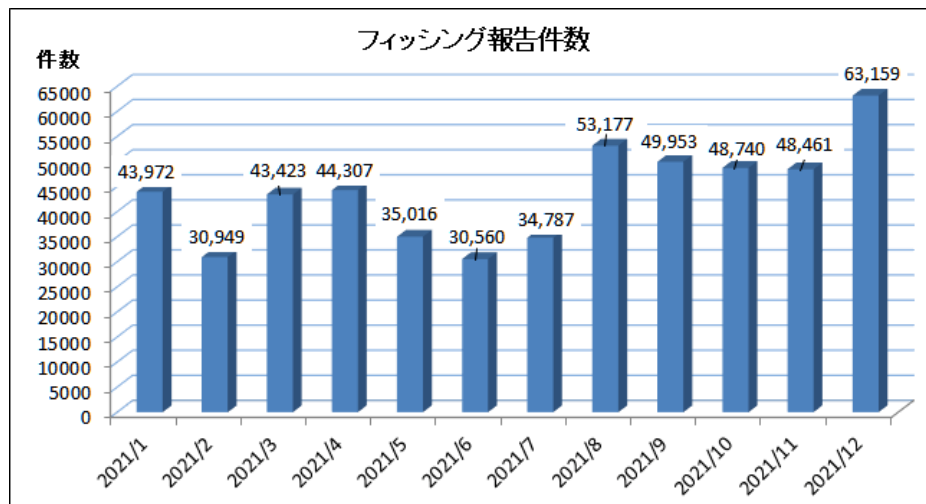


図 1-9 2021 年フィッシング報告件数の推移

1.3.1. フィッシングのターゲットとなっているブランド

昨今のフィッシングは、基本的にはクレジットカード情報狙いであるが、前年に引き続き、EC 系（インターネットショッピング、フリーマーケットなど）ブランドの報告件数が最多で、その割合は全体の約 53.6%であった。クレジットカードブランドをかたるフィッシングも継続的に行われていて、さまざまなブランドをかたり（40 ブランド）、その割合は約 35.2%であった。その他、年末には、これまで報告がまったくなかった保険会社をかたるフィッシングも発生している。

ISP やホスティング事業者、メールサービスをかたるフィッシングも発生¹⁰しているが、これはアカウント情報を詐取して、不正メールの踏み台発信に利用していると考えられている。

新型コロナウイルス関連では、厚生労働省をかたるものや、特別定額給付金をかたるものなども発生している。犯罪者は常日頃から経済、社会状況を観察し、利用者の多いサービスや生活状況からついアクセスしてしまいそうなものをフ

¹⁰JPCERT/CC、Web メールサービスのアカウントを標的としたフィッシングに関する注意喚起」
(<https://www.jpccert.or.jp/at/2021/at210049.html>)（閲覧日：2022 年 2 月 21 日）

フィッシングの対象として選択していることから、今後も新たなブランドを対象としてフィッシングが行われる可能性があり、引き続き注意が必要である。

1.3.2. 「なりすまし」送信メールの継続

大量配信されるフィッシングの内、送信元メールアドレスに正規サービスのドメインを使用した「なりすまし」送信メールは、現在も多く発信されている。この「なりすまし」送信メールの検出には、送信ドメイン認証技術（SPF/DKIM/DMARC）の内、特に DMARC が有効であるが普及率が低い状況である。事業者は最低限 SPF と DMARC でドメインを保護し、DMARC レポートで本物のメールが届いていることを確認することから、「なりすまし」送信メールの検知をはじめてもらいたい。

1.3.3. スミッシングで狙われるキャッシュレス決済

スミッシング＝ショートメッセージ（SMS）から誘導されるフィッシングについては、宅配便の不在通知をかたるものに加えて、EC 系や通信キャリアをかたるものが多く報告された。スミッシングで入手した情報をもとに、キャリア決済やキャッシュレス決済を不正利用するという事例も報告されている。SMS で受信した認証コードを入力する際は、一度立ち止まり、その入力先サイトが本物かどうか、本当に必要な手続きなのかどうかを確認するようにしたい。また、身に覚えがないタイミングで認証コード通知 SMS などが届いた時は、裏で不正利用されている可能性があり、パスワード変更や、決済サービスの使用履歴を確認して問題がないか確認して欲しい。

【一般社団法人 JPCERT コーディネーションセンター】

2. WG の活動

2.1. 今年度の WG 活動

昨年度は、事業者におけるフィッシング対策の重要な対策をわかりやすくするために、「重要5項目」というのを策定させていただいた。一方、現状のフィッシングの状況については、2020 年の後半からユーザーからの報告も大幅に増加している。フィッシングサイトへの誘導方法は SMS による方法が増えてきている。さらに、攻撃対象についてはわざわざスマホユーザーのみを狙ったものも出てきている。また、ユーザーをだます手口は高度化し、ワンタイムパスワードさえもユーザーを騙してユーザーから直接ワンタイムパスワードを詐取し、それを裏で悪用する方法も出てきている。

そのような傾向からもっと幅広い議論の必要性を感じ、これまでの技術主体の議論から人間系の議論も加えるため、2020 年度の活動においては、学術分野からの参加が必要だと考え、長崎県立大学の加藤雅彦教授と情報セキュリティ大学院大学の稲葉緑准教授にご参加をお願いした。

まだ、議論は始まったばかりであるが、そもそもフィッシング攻撃自体を減らすために、攻撃者がフィッシングを計画する段階での対策方法はないか、また、ユーザーがフィッシングサイトのリンクのクリックする前に、冷静に考えるチャンスと与える方法はないかなどのこれまでとは異なる議論も出てきた。今後の議論の中で具体的なアイデアが出てくれば、ガイドラインに反映することもできると期待している。

【野々下 幸治 トレンドマイクロ株式会社】

2.2. フィッシング対策協議会 各 WG の活動

フィッシング対策協議会ではワーキンググループ活動やプロジェクトを通じてフィッシング対策を推進している。

◆被害状況共有 WG<主査：林 憲明氏（トレンドマイクロ株式会社）>

フィッシング詐欺は他社や他業種の被害状況を把握することが困難である。特定業種を連続的に狙う攻撃が発生した場合に、自社に被害が及ぶ前に状況を共有し、対策につなげることが有効である。本 WG ではブランドを悪用される可能性のあるサービス事業者を中心としたコミュニティを通じて被害状況の共有を図っている。

2021 年の活動として、WG メンバーに対する継続したオンラインによる情報共有を行っている。

発足当初より提供しているフィッシング詐欺被害状況に関するデータを統計・可視化することを目的としたダッシュボード「Phish Trends」の運営は継続（2018 年 10 月より観測開始）するとともに機能強化を行っている。

・「HazardInfoWG API」の提供を開始

被害状況共有 WG が提供する情報を REST API 形式により、HTTP 標準のメソッドを使ってデータ取得を可能とする機能である。本機能により円滑なデータ取得、加工整形作業の自動化を図り、発信情報の利活用を推進する。

・リアルタイムフィッシング URL の特徴抽出

URL の長さ、URL のスラッシュやドットの数などの統計を行う機能を実装した。特徴量の定点観測を通じて、正規サイトの運営上の注意すべき事項を明確にしていく。

・ダッシュボード「FakeStore Trends」（2019 年 9 月より観測開始）

一般財団法人日本サイバー犯罪対策センターの協力を得て、実在する企業のサイトに似せた、または、そのままコピーした「偽サイト」や、ショッピングサイトでお金を振り込んだにもかかわらず商品が送られてこない「詐欺サイト」に関する状況を統計・可視化する。

・ダッシュボード「Databases Leaks Trends」（2020 年 4 月より観測開始）

アンダーグラウンドマーケット、アンダーグラウンドフォーラムにおける国内組織に関連する資格情報の漏えいや売買に関する情報を収集し、統計処理から可視化する。特に「二重脅迫型（または暴露型）ランサムウェア」による被害情報の収集している。

• Carding Forums Meta Search

盗まれたクレジットカード情報やログイン情報などが売買されるアンダーグラウンドフォーラム『カーディングフォーラム』を対象にした検索に最適化された検索エンジンである。2021 年 1 月現在、32 件のカーディングフォーラムを対象とした検索機能を提供している。

引き続き、更なる活用方法の検討を中心とした活動を推進していくとともに、信頼できる関係を築き、連携して全体セキュリティレベルの向上につなげる。



図 2-1 フィッシング詐欺被害状況ダッシュボード「Phish Trends」

◆認証方法調査・推進 WG<主査：長谷部 一泰氏（アルプス システム インテグレーション株式会社）>

フィッシング詐欺と関係性が深いインターネットサービスの認証について調査を行い、より安全なサービス利用、より安全なサービス提供に向けた認証方式関連の情報を提供することでフィッシング詐欺対策を支援する。

2021 年の活動として、2019 年、2020 年に結果報告書を公開した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、ならびにインターネットサービス利用者に対するアンケート調査によるインターネットサービス提供者側との意識の違いについて確認し、安全利用へ向けた意見をまとめる。

◆証明書普及促進 WG<主査：田上 利博氏（サイバートラスト株式会社）>
電子証明書の有効性などをサイト運営者や事業者に説明するための資料を作成。EC サイトなどの利用者向けに信頼できる安全な Web サイトに関する啓発コンテンツを提供する。

2021 年の活動として、以下の情報をまとめ協議会ホームページから公開している。

・ Google Chrome における混在コンテンツのブロック（2021/04/01）

https://www.antiphishing.jp/news/info/Chrome_MixedContents_20210401.html

・ 通信プロトコル「QUIC」が標準化 ～ HTTP/3 によるウェブサイト表示速度の更なる高速化 ～（2021/08/27）

https://www.antiphishing.jp/news/info/quic_http3_20210827.html

・ S/MIME のメーラー別対応状況の調査結果を公表

（一般財団法人日本情報経済社会推進協会 JIPDEC と協力）

<https://www.antiphishing.jp/news/info/smimeppap.html>

メーラー名	OS	メーラーのバージョン/ Webブラウザのバージョン	S/MIME電子署名		S/MIME暗号化	
			受信(検証)	送信	受信(復号)	送信
Outlook (アプリ)	Windows10 Pro	2008	○	○	○	○
Outlook (Webブラウザ)	Windows10 Pro	(edgeのバージョン:91.0.864.59)	○	○	○	○
Outlook (アプリ)	iOS 14.6	4.2124.0	○	○	○	○
Outlook (アプリ)	Android 11	4.2123.2	○	○	○	○
Thunderbird (アプリ)	Windows10 Pro	78.11.0	○	○	○	○
Gmail (Webブラウザ) 無料版	Windows10 Pro	(Chromeバージョン:91.0.4472.114) (Firefoxのバージョン:89.0.2)	○	×	×	×
Gmail (アプリ) 無料版	iOS 14.6	6.0.210530	○	×	×	×
Gmail (アプリ) 無料版	Android 11	2021.05.16.380255809	○	×	×	×
Yahoo!メール (アプリ)	Android 11	4.11.2	×	×	×	×
Yahoo!メール (アプリ)	iOS 14.6	8.6.0	×	×	×	×
Yahoo!メール (Webブラウザ)	Windows10 Pro	(Firefoxのバージョン:89.0.2)	×	×	×	×
iPhone標準メール (アプリ)	iOS 14.6	—	○	○	○	○
対応数			9	6	6	6
対応割合			75.0%	50.0%	50.0%	50.0%

図 2-2 メーラーの S/MIME 対応状況調査結果

・ 国の行政機関が発行するメールマガジンのなりすまし対策状況の調査結果を公表（2021/12/21）

（一般財団法人日本情報経済社会推進協会（JIPDEC）、株式会社 TwoFive と協力）

◆STC 普及啓発 WG<主査：林 憲明氏（トレンドマイクロ株式会社）>
インターネットを安全に使うための消費者向けセキュリティ普及啓発キャンペーンを日本国内で推進している。インターネットや Web サイトにアクセスす

る前に「ちょっと立ち止まって、（例えば、その Web サイトにアクセスすることで）何が起こるか考える」意識を持つよう呼びかけている¹¹。

2021 年の活動としては、『第 17 回 IPA「ひろげよう情報モラル・セキュリティコンクール」 2021』の応募作品の中から「標語」「ポスター」「4 コマ漫画」の 3 つの部門における優秀賞（協力企業・団体賞）を選出し、表彰した。¹²

◆学術研究 WG<主査：唐沢 勇輔（Japan Digital Design 株式会社／ソースネクスト株式会社）>

フィッシングサイトの早期発見に関する研究を推進し、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。2017 年から長崎県立大学と共同で研究を進めている。

2021 年の活動としては、長崎県立大学との共同研究活動成果の 1 つとして、学術論文「フィッシング詐欺のビジネスプロセス分類」を公開した。

2 つの事例分析を実施し、実際のフィッシング詐欺を特定するためのプロセスとして適用可能であることを確認。フィッシング詐欺におけるプロセスを体系的に理解し、フィッシング詐欺の脅威を予測することが容易となった。¹³

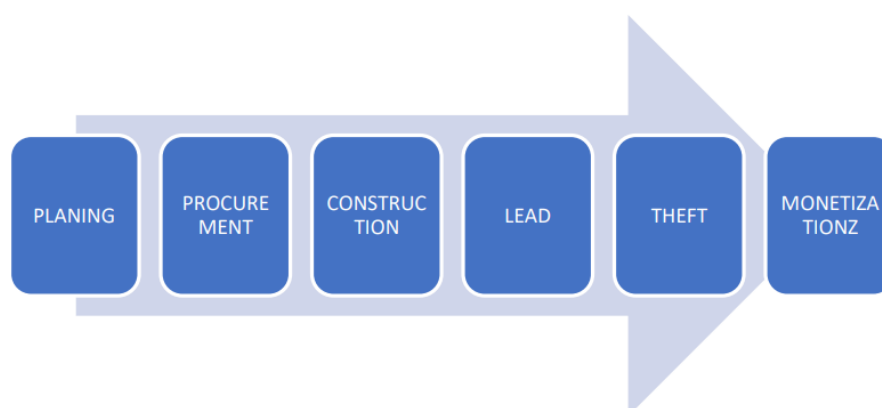


図 2-3 フィッシング詐欺ビジネスプロセス

¹¹ フィッシング対策協議会、STOP. THINK. CONNECT. とは（https://www.antiphishing.jp/pdf/about_StopThinkConnect.pdf）（閲覧日：2022 年 2 月 21 日）

STOP THINK CONNECT Web サイト

（<https://stopthinkconnect.jp/>）（閲覧日：2022 年 2 月 21 日）

¹² フィッシング対策協議会、『第 17 回 IPA「ひろげよう情報モラル・セキュリティコンクール」 2021』の優秀賞を選出（https://www.antiphishing.jp/news/info/ipa_competition2021.html）（閲覧日：2022 年 2 月 21 日）

¹³ フィッシング対策協議会、「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/news/info/collabo_20210316.html）（閲覧日：2022 年 2 月 21 日）

• JANOG48 Meeting（2021 年 7 月 15 日開催）にて、学術研究 WG および事務局が講演

<https://www.antiphishing.jp/news/info/20210820.html>

• スミッシングについて本気出して考えてみた～ビジネスプロセス的観点から～

発表者：唐沢 勇輔（フィッシング対策協議会 副運営委員長・学術研究 WG/Japan Digital Design 株式会社）

• 増え続けるフィッシング被害に今、我々ができること

発表者：平塚 伸世（フィッシング対策協議会 事務局/JPCERT/CC）

【加藤 孝浩 トッパン・フォームズ株式会社】

2.3. 認証方法、調査・推進 WG による意見

認証方法 調査・推進 WG（以下認証 WG と略す）では、前述でご紹介いただいたとおり、フィッシング詐欺と関係性が深いインターネットサービスの認証について調査を行いレポートしている。

本 WG における活動との連携として、過去の調査レポートによる年代ごと利用実態や意識の傾向と、フィッシング詐欺被害の年代ごとの傾向について関連性を確認し、今後の対策への一助となるように情報を整理する。

認証 WG は、東京オリンピック開催へ向けて、増加するであろうフィッシング詐欺被害に対応すべく、WG を立上げ、調査、レポートを進めてきたが、新型コロナウイルス感染という想定外の事態による、社会活動の制限への対応としてのインターネット利用の促進が進み、インターネットサービスは想定外のスピードで拡大した。それに従いフィッシング詐欺の被害も増大している。

現在のインターネット利用状況の背景にあること、それはコロナ禍による外出の自粛、集会の制限これら活動制限に対して、以前同様に目的を実現する手段としてのインターネットの活用がある。

併せてスマートフォンの普及による、インターネットサービス利用機会の拡大もあり、より身近にインターネットサービスを利用することができるようになったことが挙げられる。

その状況下に置いて、被害増大となっている要因を年代における傾向で考察した。

最初にパスワードの使いまわしについてである。当たり前のことだがパスワードが使いまわされていると、フィッシングされた ID、パスワードをもとに使いまわし先での被害拡大が安易に予想される。

2020 年実施の認証 WG レポート「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報告書」（以下 WG レポートと略す）によると、パスワードの使いまわしは、年代ごとの傾向があり、高年齢であるほうが、使い分けが進んでおり、低年齢の方が使いまわしている傾向があった。

同時に、SNS や総合サービスのアカウントでのログインについて、（18 歳から 20 歳代）の利用が 77.5%と SNS 利用度の高い若い世代での利用が高く、60 歳代以上は、29%と低い状況が確認されている。このように SNS などのアカウントによる認証を利用しているのが、低年齢に多いことから、これは、パスワードを使い分けているのではなく、SNS サービス認証でのシングルサインオンを利用していることを指していることから、パスワードを使い分けしていないとの回答が多いことも想定される。

また、認証について面倒と感じているとの回答が低年齢に多い状況からも、低年齢の利用者になるべく簡単に認証をすましてサービスを利用したいと思っているようである。

次に「インターネットのサービスを利用して不安に感じることは何ですか」との回答では、「特に不安と感じていない」と回答した（18 歳から 20 歳代）の回答が 43%と大きく、（60 歳代以上）での 20%の倍以上となっている。「本人認証の方法について不安に感じたことはありますか」との問いにも、「不安に感じたことはない」と（18 歳から 20 歳代）の回答が 45%と大きく、（60 歳代以上）での 24%と大きく差がある。低年齢においては、生まれたときからインターネット環境が身近にあり、インターネット利用について当たり前の感覚があるために不安は無いと言っていると思われる。60 歳以上では、i-モード開始などによるインターネット利用が一般化されたときには 40 歳代となっており、その年代から恐る恐る利用してきた年代にとっては、不安要素が多く感じていることと思われる。

もう一つ、働き盛りで資産の移動を活発に行う年代と思われる、30 歳代から 50 歳代においては、認証に対して慎重な対応を求め実施しているようである。この年代では、70%以上が「より安全と思われる本人認証の方法がオプションで用意されていた場合、利用する」と回答している。40 歳代においては、47%が「サービス事業者からの、より安全な本人認証についての案内（二段階認証などの案内や、セキュリティ設定の推奨事項など）や推奨事項を見て推奨事項に従った」と回答している。

これら利用者の年齢傾向に対して、フィッシング詐欺被害の年齢傾向についての正確な情報は、現在のところ見当たらないが、幾つかのサービスへのヒアリングや、事件の状況から見てみると、被害の年齢傾向からは、若年層、老年層が多く、次いで中年層の順になると想定される。

その要因は、多角的にあると思われるが、上記のように利用者調査からの傾向から幾つかの要因が見えると思われる。

ID、パスワードの管理については、慣れすぎている低年齢には油断をさせず、面倒がらせずに安全な認証を勧めたり、高年齢には、分かり易い説明と手順でより安心感を持てる認証を利用してもらう努力を惜しまないことが大事だと思われる。

現在においては活発な活用をしている 30 歳代から 50 歳代についても、高齢化した際には、同じ要領で安全な対応ができるか心配なところも出てくるため、

不安を感じた際の対応について案内を行う準備が必要かもしれない。

利用するインターネットサービスの内容は同じでも、年代ごとにサービスで扱う資産の大きさが違ったり、時代背景によるリテラシーの差や感覚の差など、利用者の年代による傾向があることは事実のようである。

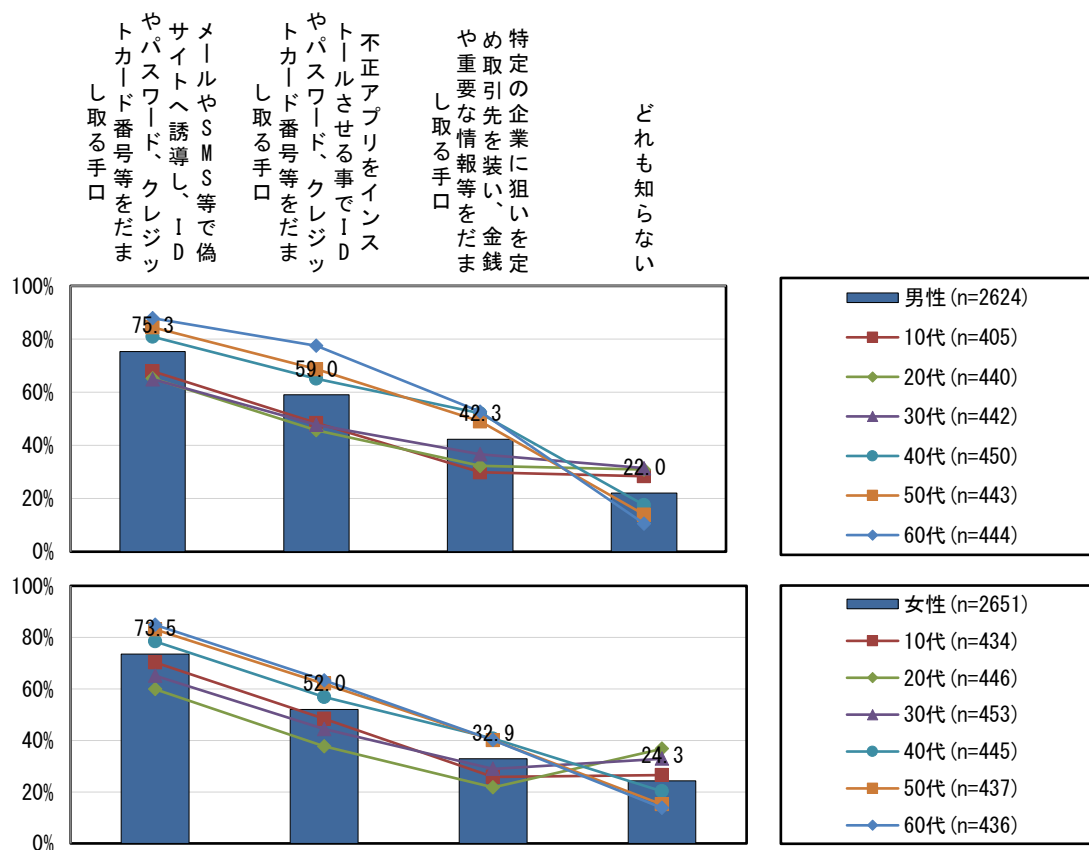
これら利用傾向が年代ごとに違うことを意識した認証設計や注意喚起を行うことが大事であると言える。

【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】

3. SMS を用いたフィッシング詐欺についての意識調査

SMS を用いたフィッシング詐欺について消費者の意識や被害の実態を調査するアンケートを実施した。アンケートは、インターネットリサーチにて対象者を年代ごと、男性、女性の比率などが同等になるよう配慮し、5,275 名から回答を得た。以下、調査結果のポイントについて紹介する。

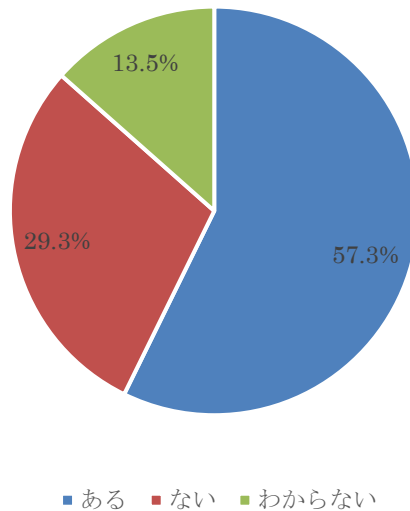
Q1 フィッシング詐欺の手口で知っている手口を選んでください。※複数回答可 (n=5275)



一般的なフィッシング詐欺の手口について知っている手口についての質問では、ID、パスワード、クレジットカード番号などをだまし取る手口が最も知られている手口となった。男女ともにシニア層の方が手口に詳しい。

Q2. フィッシング詐欺と考えられる SMS（携帯のショートメッセージ）を受け取ったことがありますか？ (n=5275)

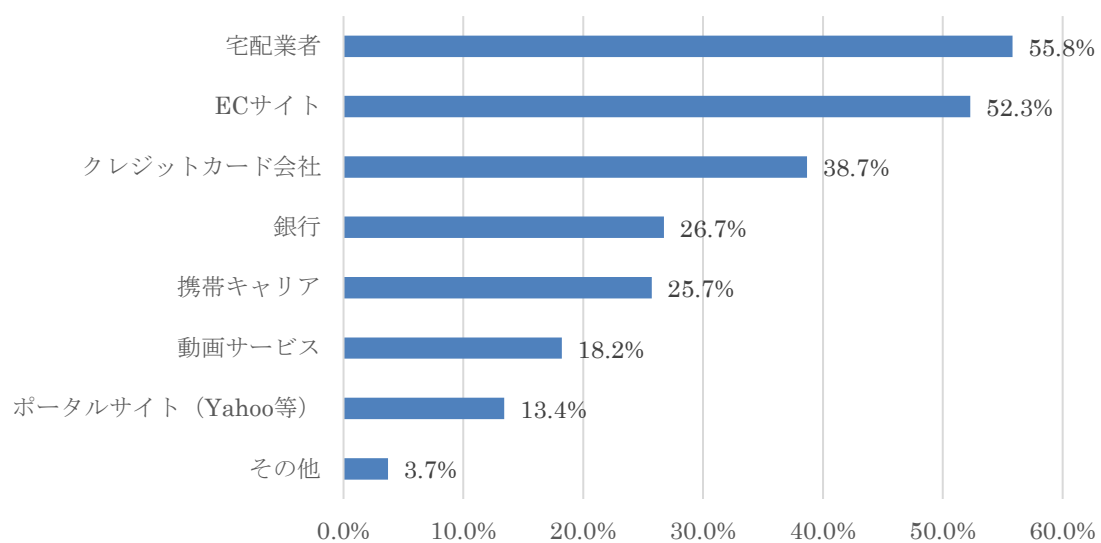
フィッシング詐欺と考えられるSMSを受け取ったことがありますか？



半数以上の方は受け取ったことがあると回答しており、SMS を用いたフィッシング詐欺が、身近に迫るものとなっていることがわかる。

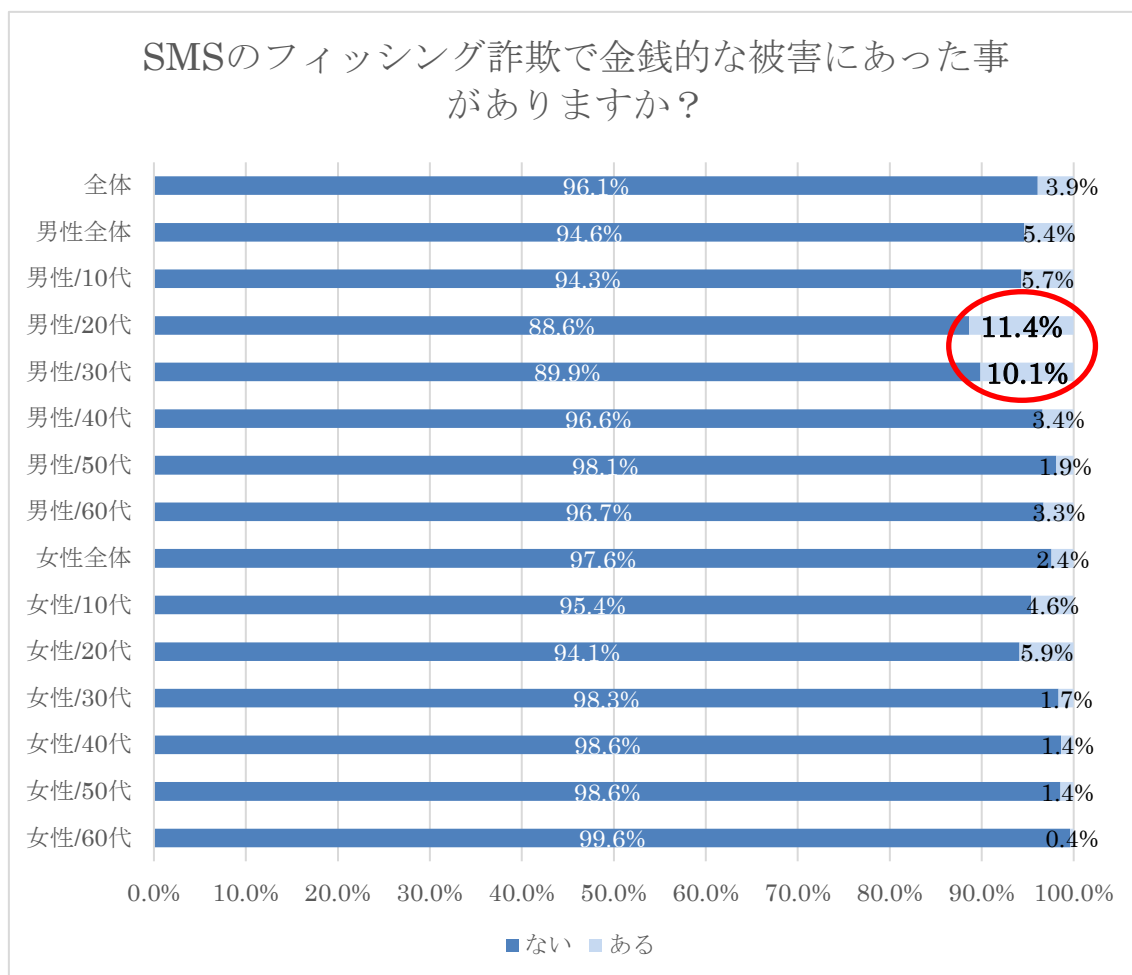
Q3. 何を装ったフィッシング詐欺でしたか？※複数回答可（n=3021）

何を装ったフィッシング詐欺でしたか？



金融機関を装う手口よりも、宅配業者や EC サイトなど消費者が日常的に利用する接点の多いサービスを装う手口が多いことがわかった。

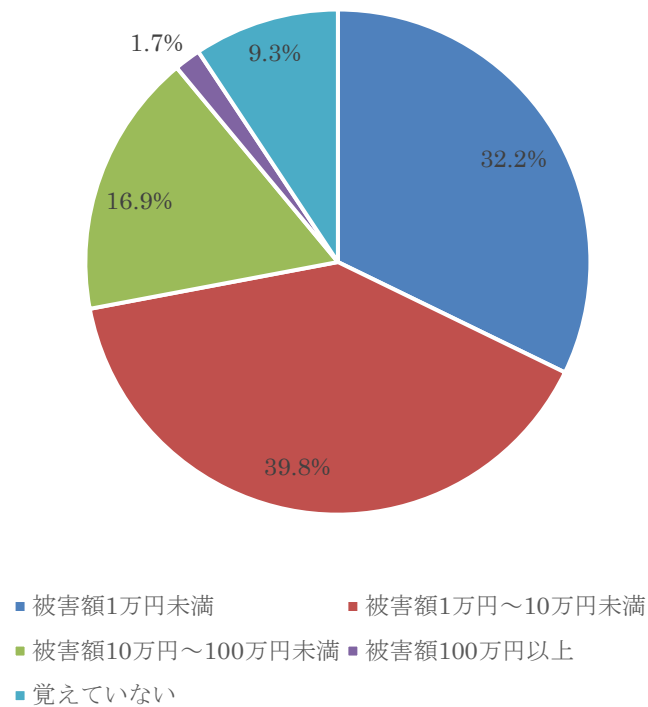
Q4. SMS のフィッシング詐欺で金銭的な被害にあったことがありますか？
(n=3021)



全体で金銭的被害にあった方の割合は 3.9%のところ、男性の 20 代、30 代は 10%超と全体の 2 倍以上多い結果となった。攻撃者がターゲットとして選ばれやすい属性である可能性があるため、被害を防ぐには女性や他の年代の男性に比べてより注意が必要と考える。

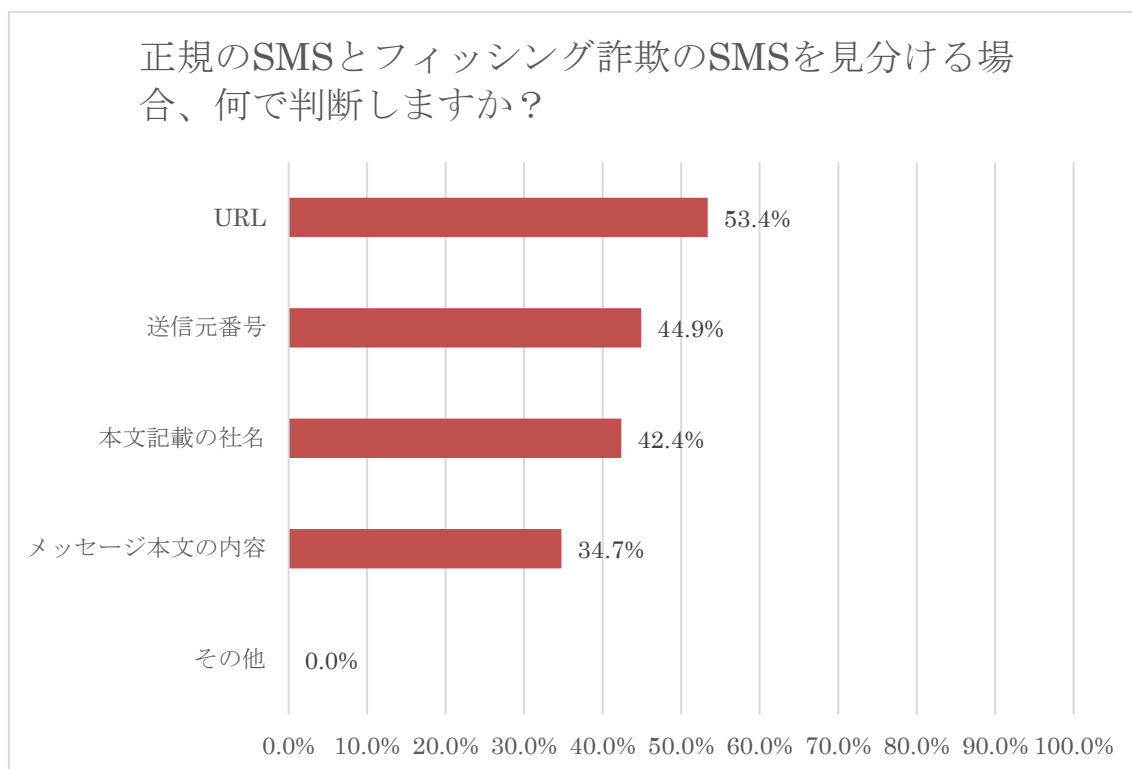
Q5. SMS のフィッシング詐欺での被害額はいくらでしたか？複数回ある方は一回あたりの最大額をお答えください。(n=118)

SMSのフィッシング詐欺での被害額はいくらでしたか？



被害にあわれた方の 72%が被害額 10 万円未満という結果だった。最大額では 382 万円と高額な被害もあった。

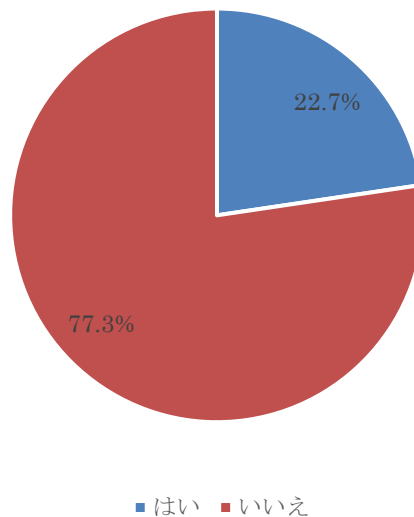
Q8. 正規の SMS とフィッシング詐欺の SMS を見分ける場合、何で判断しますか？※複数回答可（n=118）



本文の記載内容だけでは正規のSMSとフィッシング詐欺のSMSを見分けることはできないが、URLや送信元番号は見分ける根拠となり得る。URLや送信元番号で判断するという回答が本文の記載の社名や内容で判断するという回答を上回っていたが、大きな差はついておらず、少なからず本文の社名や内容が判断に影響を及ぼしていることがわかった。

Q9. SMSの送信元番号がアルファベットの場合は、国内電話番号の場合と比べて、フィッシング詐欺の可能性が高くなることをご存知でしたか？(n=5275)

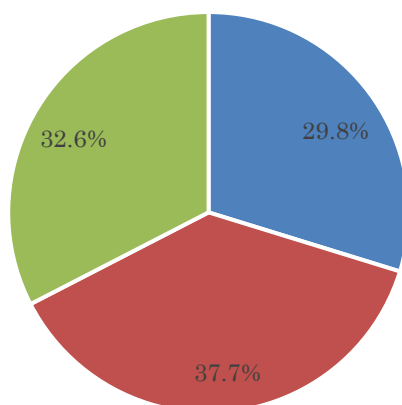
SMSの送信元番号がアルファベットの場合は、国内電話番号の場合と比べて、フィッシング詐欺の可能性が高くなる事をご存知でしたか？



送信元がアルファベットの場合は、国際網を経由した SMS である。海外には利用審査や契約手続きも厳格に実施しない事業者が存在するため、フィッシングに利用されやすい。海外からの SMS の危険性について 8 割弱の方は認識がなかったと回答している。Q8 では送信元番号で正規の SMS と詐欺の SMS を見分ける判断材料とする回答が 44.9%あり、一定程度注意が払われているようだったが、一方でこの質問の結果を見ると送信元がアルファベットの場合の危険性について、十分認知されているとは言えないことがわかった。

Q10. 見知らぬ電話番号から SMS を受け取った場合、検索サイトで該当の電話番号を検索しますか？（n=5275）

見知らぬ電話番号からSMSを受け取った場合、検索サイトで該当の電話番号を検索しますか？



■ 必ず検索する ■ 必要に応じて検索する ■ 検索した事はない

前述のとおり、送信元番号は正規のSMSと詐欺のSMSを見分ける手段になり得るものだが、「検索したことはない」という回答が29.8%と3割近くにのぼった。見知らぬ電話番号から届いたSMSには、すべて取り合わないという場合は、問題ないが、正規のSMSとして扱う必要があれば、企業側が公表している送信元番号を調べて、届いたSMSの送信元番号と照合してから扱うことがフィッシング詐欺への対策になり得る。

<まとめ>

フィッシング詐欺でSMSが使われる事例は多くのメディアでも報じられるようになってきているが、今回の調査では消費者のフィッシングSMS受信の状況や金銭的な被害の状況、消費者の意識などの情報を得ることができた。

実際にフィッシング詐欺と考えられるSMSを受け取ったことのある人は57.3%にも上り、SMSに記載されたURLを開かないなどの被害を防ぐ行動を取っている方も多い一方で、全体の3.9%が実際にSMSによるフィッシング被害に遭ったことがあるという。またフィッシング手口を知っていても、正規のSMSと詐欺のSMSを見分ける手段については、まだ広く認知されているとは言えないため、今後も利用者向けの周知を強化していかなければならない。

<調査概要>

調査対象者：インターネットモニター会員を母集団とする 10 代から 60 代のスマートフォンを所有する男女

調査方法：NTT コム リサーチによるインターネットアンケート

調査期間：2021/12/03～2021/12/05

有効回答者数：5,275 名

回答者の属性：

【性別】 男性：49.7% 女性：50.3%

【年代】 10 代：15.9%、20 代：16.8%、30 代：17.0%、40 代：17.0%、50 代：16.7%、60 代：16.7%

※調査結果をご利用の際は、「NTT コム オンライン調べ」と明記ください。

【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】

4. フィッシングの対策

4.1. 最新の動向

4.1.1. FIDO とフィッシング耐性への期待

近年のサービスではフィッシングやパスワードリスト攻撃などのパスワード認証に関わるセキュリティ事故から防ぐため、パスワード認証の要件や管理の煩雑化が課題として挙げられるようになった。一方でパスワード認証のセキュリティ対策によりユーザビリティが損なわれユーザーが離脱することも懸念され、認証にパスワードを使用しないパスワードレスの技術が注目されている。

FIDO (Fast Identity Online) と呼ばれるオンライン認証の仕様が策定され、採用するサービスが注目されている。FIDO を活用することで、認証器と認証サーバー間で高度なオンライン認証を実現することができる。認証方法として生体認証などが使用され、現在流通している多くのスマートフォンでも使用できることから、フィッシング詐欺やパスワードリスト攻撃の根本的な対策を行うことが可能になる。

認証情報であるクレデンシャルは端末内で安全に管理されており、インターネット上では、クレデンシャルの検証を成功したかどうかだけがやり取りされており、生体情報はデバイスで安全に保管されているため、セキュリティリスクを大幅に軽減できるという点もある (図 4-1)。

FIDO の最新の仕様に基づいて提供されている WebAuthn の API は Android7 以降および iOS14 以降のスマートフォンで対応されており、スマートフォン内の Web ブラウザーで FIDO による認証を行うことができる。また、FIDO2 に対応した Web ブラウザーと USB 型の認証デバイスなどの組み合わせでも使用できることから多くのデバイスでの活用が可能になる。

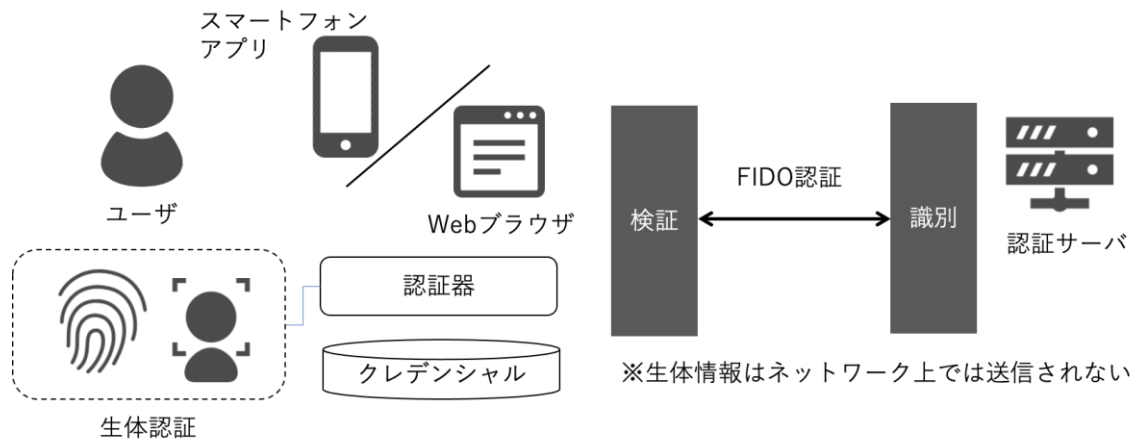


図 4-1 FIDO の認証モデル

ユーザー体験としては普段使用している生体認証を使用できることから、認証にかかる操作も少なく、パスワード認証と比較してもユーザビリティも良くなり、セキュリティ向上と両立することができる。¹⁴

【松本 悦宜 Copy 株式会社】

¹⁴ Yahoo! JAPAN Tech Blog、WebAuthn を用いたパスワードレス生体認証のユーザビリティ調査 (<https://techblog.yahoo.co.jp/entry/2020122330052970/>) (閲覧日：2022 年 2 月 21 日)

4.1.2. フィッシング関連情報の収集・共有による効果と課題

フィッシング被害を減らすためにさまざまな取り組みがあるが、その中のログ（フィッシング関連情報）を収集することによる犯行グループの特定・逮捕と、被害者の特定・被害の食い止めへのアプローチ、またその課題について記載する。

犯罪の高度化も進んでいるが、不正対策ソリューションもまた進化しているため、最新動向を把握し、対策も高度化し続ける必要がある。

■犯行グループの特定・逮捕へのアプローチ

犯行グループの特定・逮捕においては、フィッシングサイトや、犯行に利用された ATM や PC・スマホ端末、利用ネットワークなどの手がかりのログを取得し、調査を行う必要がある。フィッシング被害が各事業者で多く発生しているという背景もあり、ログを取得し調査を行うという取り組みは以前に比べかなり進んでおり、犯行グループの特徴を捉え、逮捕につながった例もある。

ログを取得し調査を行うことは、即時フィッシング被害を食い止めるという結果には直結しないが、各事業者にとっても、これらを実施することでより有効な検知ルール策定や、対策を講じる上で大変有効であるし、金融庁の各種ガイドラインにもモニタリングの重要性は説かれているため、引き続きログ取得強化を進める必要がある。

■被害者の特定・被害の食い止めへのアプローチ

犯罪の高度化（OTP 突破や被害者の情報入力から送金の短時間化など）が進んでいるが、不正対策ソリューションも進化している。

ログ取得による早期の被害者特定や、その情報を用いた早期のアカウント凍結によって被害を食い止めるような対策も打てるようになってきている。

さらには、犯人や被害者の情報を自社内のみで利用するのではなく、各事業者で共有することにより、犯罪を未然に防ぐといったことも可能となっている。

■課題

一方、各種情報の商用利用も進む中、プライバシー保護の観点で情報が取得しにくくなるような取り組み（iOS15 から利用可能となったプライベートリレーという IP 情報を秘匿するような機能や、広告用 Cookie の利用制限など）も進んでおり、今後犯罪調査の難易度が上がってしまう懸念もある。

令和 3 年版警察白書によると、令和元年の捜査の課題として匿名化技術の悪用が最多となっており、個人が容易に匿名化できる技術の発展は、捜査の難易度

をさらに上げてしまうと考えられる¹⁵。

図表特2-13 サイバー犯罪捜査における事後追跡上の課題

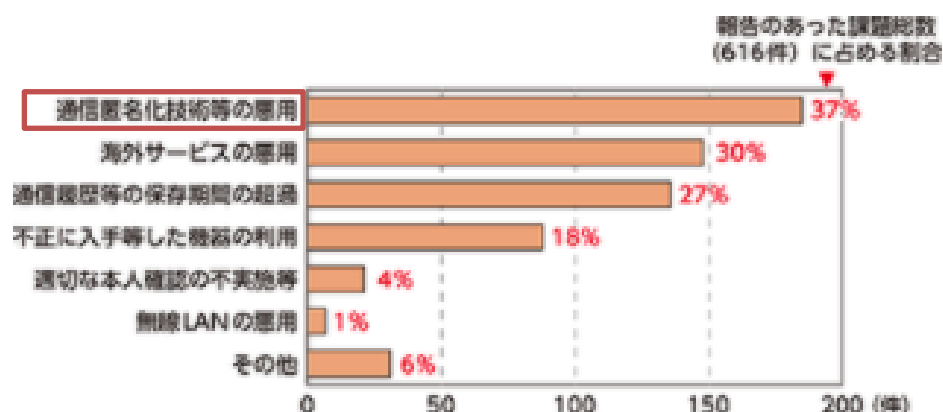


図 4-2 サイバー犯罪捜査における事後追跡上の課題

また、各事業者においてはモニタリング体制を構築したからといって慢心せず、外部環境の変化による不正対策の抜け穴を作らぬような対策が必要である。そのために最新ソリューションの導入や情報収集を継続的に行う必要があるが、ソリューション導入に関してはベンダーロックインの影響もあり、導入に多くの時間と費用がかかってしまうという課題もある。

不正情報や被害者情報を各事業者間で共有し被害を食い止めるという点に関しては、各々の情報の取り扱いなどに関するルールや基準が存在しているためルール整備の難しさという課題もある。

解決すべき課題は複数あるが、不正対策ソリューションの導入や、各事業者間の情報共有が進むことはフィッシング対策において有効であるため、それらの推進を引き続き実施していく必要がある。

【島田 美奈 株式会社カウリス】

¹⁵ 警察庁、令和3年度版警察白書 第2節 サイバー空間の脅威への対処「サイバー犯罪捜査における犯人の事後追跡上の課題」
(<https://www.npa.go.jp/hakusyo/r03/honbun/html/xf221000.html>) (閲覧日：2022年2月21日)

4.1.3. フィッシング対策のシフトレフト

巧妙化や悪質化が進むフィッシング詐欺手口に対し、新たな対策の追加は必要不可欠であるが、フィッシング詐欺発生 の阻止、また、初期段階に検知する早期対策の検討も必要である。フィッシング対策協議会の学術研究 WG<主査：唐沢 勇輔（Japan Digital Design 株式会社／ソースネクスト株式会社）>では、長崎県立大学との共同研究活動の中で、フィッシング詐欺におけるプロセスを「計画」「調達」「構築」「誘導」「詐取」「収益化」の 6 つの活動に分類することができた。フィッシング対策を、このプロセスのより計画に近い段階での行う「フィッシング対策のシフトレフト」を検討していく必要がある¹⁶。

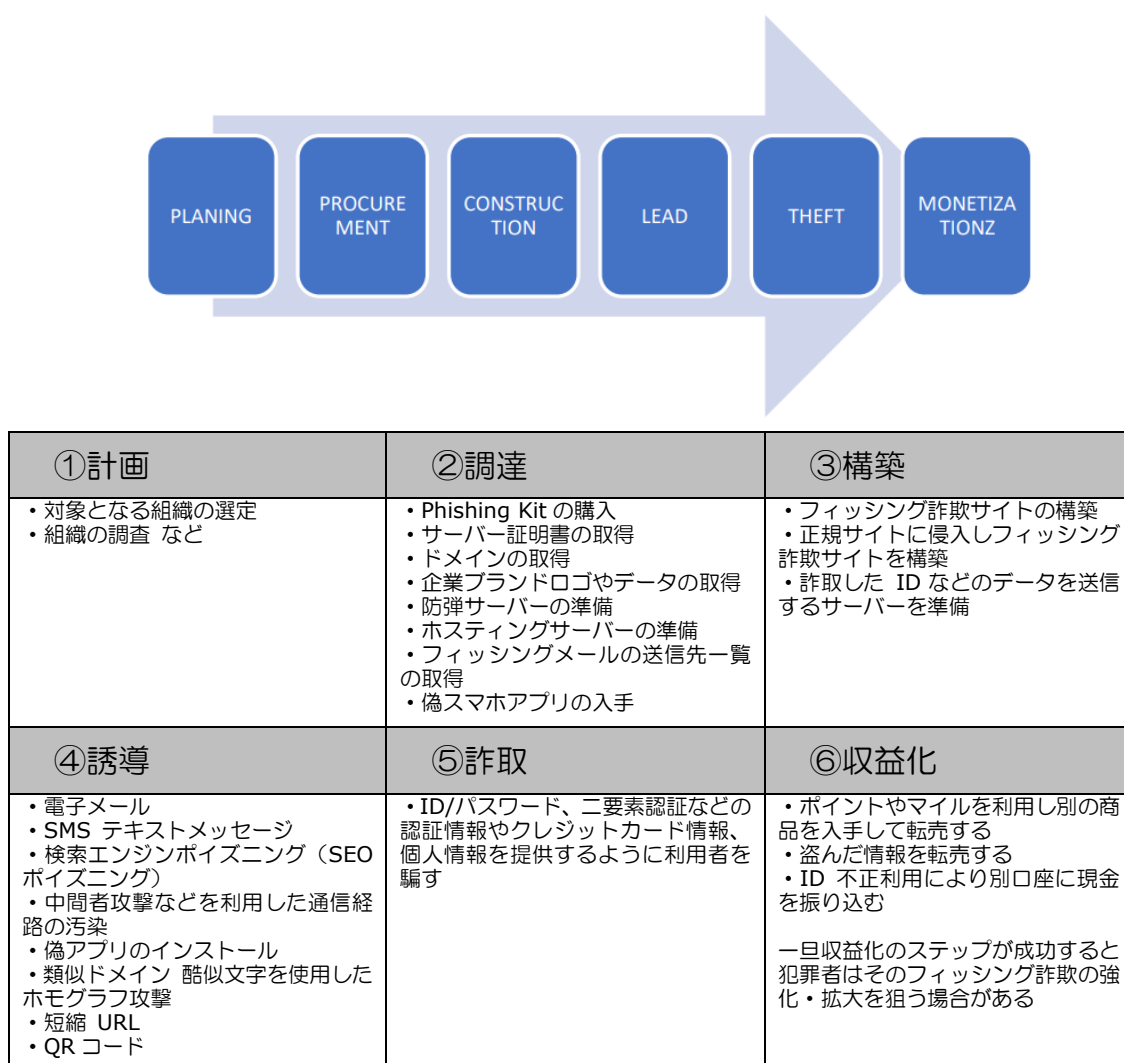


図 4-3 フィッシング詐欺におけるプロセス

¹⁶ フィッシング対策協議会、フィッシング詐欺のビジネスプロセス分類（論文）
https://www.antiphishing.jp/news/info/collabo_20210316.html（閲覧日：2022 年 2 月 21 日）

協議会が発行している事業者向けのフィッシング対策ガイドラインの項目をこのプロセスに沿って分類すると、ほとんどが4番目の「誘導」以降となっている。これはフィッシング詐欺の特異な構造が関係している。フィッシング詐欺は、事業者を模倣したメールやサイトに利用者を誘導し、攻撃者と利用者の間のみで行われる。すなわち事業者から離れたところで行われ、この段階では事業者対策より利用者本人の対策となってしまう、現在の事業者対策は、「④誘導」「⑤詐取」「⑥収益化」に対し本物と区別できるようにする対策、また、「⑥収益化」に対してID/パスワードやクレジットカード情報を詐取されたとしても、攻撃者が収益を得にくくする対策が中心となるためである。

表 4-1 フィッシング対策ガイドライン 2021 のプロセスに沿って分類

			①計画	②調達	③構築	④誘導	⑤詐取	⑥収益化
Web サイト運営者が考慮すべき案件一覧	【利用者が正規メールとフィッシングメールを判別可能とする対策】	【案件1】○	○			○		
		【案件2】○	○			○		
		【案件3】○	○			○		
		【案件4】○	○			○		
		【案件5】○	○			○		
	【利用者が正規サイトと判別可能とする対策】	【案件6】○	○			○		
		【案件7】○	○			○		
		【案件8】○	○			○		
		【案件9】○	○			○		
		【案件10】○	○			○		
	【フィッシング詐欺被害を拡大とせたいの対策】	【案件11】○	○			○		
		【案件12】○	○					○
		【案件13】○	○					○
		【案件14】○	○					○
		【案件15】○	○					○
		【案件16】○	○					○
		【案件17】○	○					○
		【案件18】○	○					○
		【案件19】○	○					○
		【案件20】○	○					○
	【ドメインに関する取組事項】	【案件21】○	○					○
		【案件22】○	○					○
		【案件23】○	○					○
	【フィッシング詐欺対策のための組織体制】	【案件24】○	○					○
		【案件25】○	○					○
		【案件26】○	○					○
		【案件27】○	○					○
		【案件28】○	○					○
	【利用者への啓発活動】	【案件29】○	○					○
		【案件30】○	○					○
		【案件31】○	○					○
	【フィッシング詐欺被害の発生も当該は防衛するための対策】	【案件32】△	△					○
		【案件33】△	△					○
		【案件34】△	△					○
		【案件35】○	○					○
利用者が考慮すべき案件一覧	【パソコンやモバイル端末は、安全に使う】	【案件36】○	○					○
		【案件37】○	○					○
		【案件38】○	○					○
		【案件39】○	○					○
		【案件40】○	○					○
	【不審なメールは注意する】	【案件41】○	○					○
		【案件42】○	○					○
		【案件43】○	○					○
		【案件44】○	○					○
		【案件45】○	○					○
	【電子メールにあるリンクはクリックしないようにする】	【案件46】○	○					○
		【案件47】○	○					○
		【案件48】○	○					○
	【アカウント情報の管理】	【案件49】○	○					○
		【案件50】○	○					○

これらの対策は、フィッシングを繰り返さないためにも重要な対策であり、手を緩めるわけにはいかないが、利用者にフィッシングが及ぶ前に対策する方向がフィッシング対策のシフトシフトと言える。今後のガイドライン改定検討においては、「計画」「調達」「構築」に分類される対策の追加を技術と制度の両面で行っていく必要がある。

フィッシング対策ガイドライン 2022 では「③構築」の対策につながる以下の 2 点を強化している。

- 【要件 22】◎：ドメイン名の登録、利用、廃止にあたっては、自社のブランドとして認識して管理すること
- 【要件 32】○：フィッシング詐欺検知に有効なサービスを活用すること

事業者側においても、今後、「フィッシング対策のシフトレフト」に着目していただき、利用者保護の強化につなげていただきたい。

【加藤 孝浩 トッパン・フォームズ株式会社】

4.1.4. フィッシングサイトの短時間化と被害発生状況の推移からの課題

フィッシング詐欺が発生してから、そのフィッシングサイトにアクセスできなくなるまでのアクティブである時間は、傾向として年々短くなっている。2004年のある分析では5～6日であり、2012年では1～3日、2017年では24時間以内や4～8時間といった分析がされており、現在でも多くのケースで同程度ではないかと想定される。

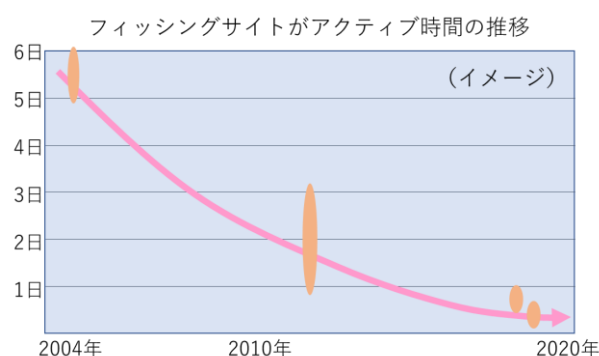


図 4-4 フィッシングサイトがアクティブ時間の推移

また、フィッシング詐欺発生後の被害の時間推移では、2012年と2019年のある分析は概ね同様で、最初の1時間が最も多く、順次減少してロングテールとなるものの24時間もすればほぼ被害は収束する。フィッシングメールやSMSは着信直後が最も利用者が反応してしまうであろうことを推測すると、現在のフィッシング詐欺の多くも概ね似たような傾向となっているのではないだろうか。

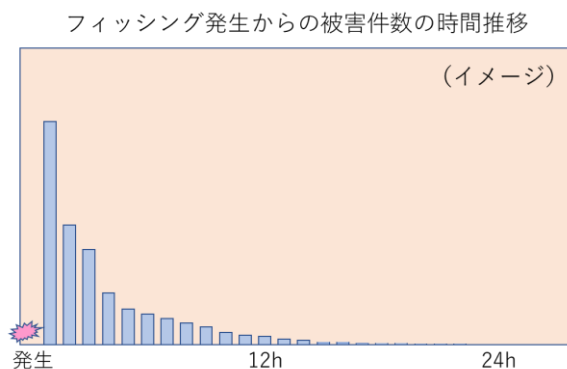


図 4-5 フィッシング発生からの被害件数の時間推移

つまり、現在のフィッシングサイトは、効率の悪いロングテール部分は捨て、効率の良い冒頭数時間のみ稼働させ、代わりに回数を増やすことで、より多くの利用者情報を詐取する状況となっている。

フィッシングの短時間化・高頻度化

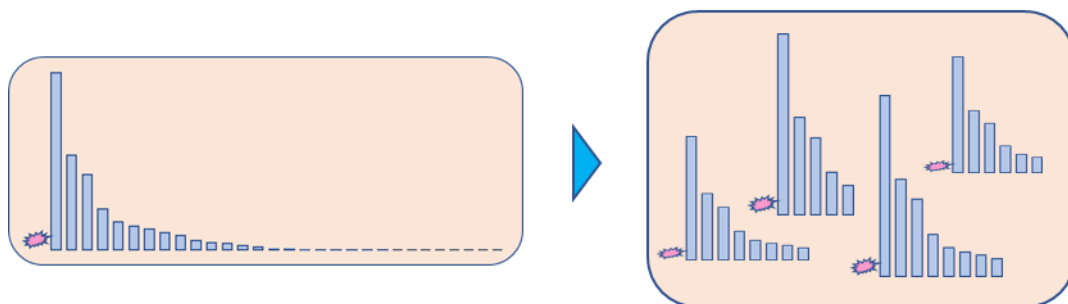


図 4-6 フィッシングの短時間化・高頻度化

フィッシング詐欺に対抗する手段の一つとして、「ブラウザやセキュリティソフトなどによるフィッシングサイト URL のフィルタリング」があり、現在も有効な手段として広く利用されている。しかし、昨今のフィッシングサイトの短時間化に伴い、フィッシングの発生から URL の反映まで何時間も要してしまうと、フィルタリングによる利用者保護がまったく間に合っていないケースもあるものと考えられる。

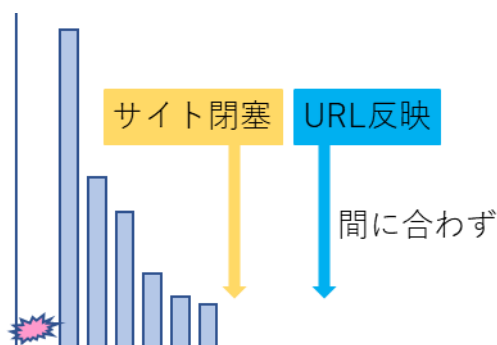


図 4-7 フィルタリングによる利用者保護

お客様サービスを提供する各組織は、①一刻も早く発生を認識する。②一刻も早く対処する。ことが一層重要となっている。「①認識」においては、お客様から連絡をいただきやすくするため、日ごろのお客様コミュニケーションを密とするとともに、連絡先窓口をわかりやすく明示し、またフィッシングサイトを検出する機能やサービスの導入なども検討したい。「②対処」においては、フィッシング対策協議会への報告や Web などでのお客様周知などを迅速に行うための、

社内体制やフローなど仕組みづくりを整備したい。「①認識」「②対処」において、数分～数十分滞留するだけで、お客様被害がより広がり、場合によっては対処が一切間に合わなかった、という事態は避けたい。

【早川 和実 NTT コミュニケーションズ株式会社】

4.1.5. 携帯キャリアによる SMS に関する施策・フィッシング対策

最近一年間において各携帯キャリアから下記のプレスリリースがされている。

2021年6月：SMS 送受信番号の共通化

2021年9月：+メッセージを各社の MVNO で利用可能に

2022年1月：フィッシング SMS 拒否機能の提供開始

SMS 送受信番号の共通化は、企業が個人のユーザーと SMS で双方向のコミュニケーションをする場合に、従来、日本ではユーザーが利用している携帯キャリアごとに異なる送信元番号で企業が SMS を送受信していたが、今後はユーザーが利用する携帯キャリアに関係なく共通番号で企業が SMS を送受信することが可能となるものである。

この共通化によりユースケースの拡大が期待され、例えば、テレビ番組を見た視聴者がクイズなどの勝者を予想し正解者にプレゼントを送付すること、コロナ対策としてレストランやイベント会場に行った人が自治体などにその日時を報告¹⁷することが SMS のみで可能となる。従来、同じことをするには音声通話などと SMS を併せて利用する必要があったため、手順が複雑で時間がかかりプロセスを完了できないユーザーが存在したと考えられる。

また、フィッシング対策として、企業は利用する SMS の送信番号を個人のユーザーに告知し、異なる送信元の SMS を疑う旨の案内をしているが、その告知内容がよりシンプルになることで、フィッシング SMS の区別が比較的容易になるという効果も今後の利用拡大とともに期待される。

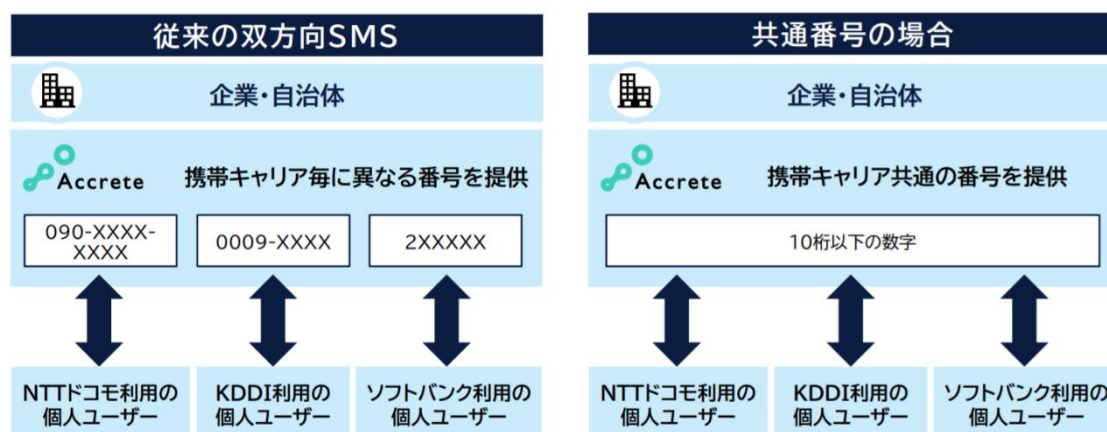


図 4-8 SMS 送受信番号の共通化

¹⁷ 株式会社ディー・エヌ・エー、プレスリリース「ワクチン・検査パッケージ」の技術実証の一環として 二次元コード、SMS を活用し クラスター対策を目的とした情報連携調査を実施
(<https://dena.com/jp/article/3681>)（閲覧日：2022 年 2 月 21 日）

＋メッセージは SMS の後継のメッセージサービス規格であり、企業のアカウントに「認証済みマーク」が表示されることから、メッセージを受信したユーザーがフィッシング詐欺をより判別しやすい環境にあるが、MVNO ユーザーおよび各携帯キャリアでもフィーチャーフォンなどの一部の端末では＋メッセージが利用できなかった。今回の MVNO とフィーチャーフォンへの拡大により、＋メッセージ利用者2,500万人（2021年7月現在）の更なる増加がフィッシング詐欺の判別にも貢献すると考えられる。



図 4-9 ＋メッセージのサービス拡大¹⁸

フィッシング SMS を拒否する機能は、今年1月にドコモとソフトバンクから発表された。両社の提供内容は若干異なり、他の携帯キャリアの公式な発表は現時点（2022年2月）ではないものの、携帯キャリア4社による情報共有は継続的に行われ、協力することでの相乗効果が見込まれる。ユーザーに届く前の最後の砦として、フィッシングと特定される SMS を携帯キャリアが防ぐことの意義は大きく、フィッシング被害の減少が期待される。

このような機能は海外携帯キャリアでは一般的だが、日本では電気通信事業法第四条「通信の秘密」の適用範囲を巡り慎重な検討が行われた結果として、今回提供可能となったという背景も存在する。

【田中 優成, 浦田 泰裕 株式会社アクリート】

¹⁸ KDDI 株式会社、ニュースリリース「＋メッセージ」が携帯3社すべてのブランドと MVNO で利用可能に (<https://news.kddi.com/kddi/corporate/newsrelease/2021/09/02/5363.html>) (閲覧日：2022年2月21日)

4.1.6. IT サービス認証における推奨事項

IT サービスを提供する企業は、ユーザー認証を必要とするケースが多く、現在はさまざまな手段から適宜選択し、採用している状況にある。以前からフィッシング対策ガイドラインにおいても「複数要素認証を要求すること」を重要5項目に含めており、金融資産の移動などの重要なトランザクションにおいては、複数要素として生体認証の FIDO2 などを推奨してきたが、企業のコスト負担、アカウントのリカバリの簡便さとのトレードオフとなる側面がある。

下記にて現状の主な IT サービスのアカウント認証について調査を実施したところ、日々のログイン（金融資産の移動などの重要なトランザクションを含む）においては各サービスで生体認証や利用者の住所登録に基づき物理的な認証キーを送付するなど、費用対効果に則った方式を採用している一方、アカウントの作成・リカバリについては E メールと携帯電話番号による SMS を利用している状況が一般的である。

	アカウントの 作成・リカバリ	日々のログイン	他サービスのシングルサインオン・OTP生成
LINE	携帯電話番号 (機種変更時はEメール必須)	ユーザが選択可 (パスコード、生体認証等)	○
携帯キャリアID	携帯電話番号	ユーザが選択可 (パスコード、生体認証等)	○
Google Apple Microsoft	Eメール (電話番号等の多要素も 選択可)	ユーザが選択可 (パスコード、生体認証等)	○ OTP生成機能も有
金融等オンライン サービス	Eメール (携帯電話番号)	Eメール&パスワード (OTP、生体認証等で 多要素化)	○ ※三菱UFJ銀行のIDで他社サービスログインを2021年10月に開始

図 4-10 主な IT サービスのアカウント認証

E メールによる認証は、サービスを提供する企業にとって極めてコスト負担が少ない方法であることと、重要事項の告知などのユーザーへのコンタクト手段として有効であることから、複数要素認証の1つとしてはスタンダードである一方、配信経路のインターネット上で傍受されるリスクが存在する。

携帯電話番号による SMS 認証は、コスト面では E メール以上のコストが必要となるものの、郵送コストよりも低コストである点、受信者が最新のスマートフォン・携帯電話端末でなくても受信でき、受信者が気付き易いか否かの観点では、SMS はプッシュ通知オフに設定されていることが稀であり、受信するアプリをほとんどのユーザーが認識していることから、E メールに加えた複数要素として

SMS 認証がベストプラクティスとして、一般に推奨される方法である。なお SMS の配信形態としては、いくつか方法があるが、最近金融機関や大手企業を中心に普及が進んでいるのは SMS の送信元番号を国内の携帯電話事業者に事前登録が義務付けられる国内直接接続¹⁹である。

一方で、海外においては SMS 認証に影響を与える SIM カード不正複製・取替が報告されており、米国 NIST のレポートなど SMS 認証の安全性に懸念する意見が存在していることから、複数の国内携帯キャリアにヒアリングを実施したところ、「海外で報告されている正常な利用者²⁰に対しての SIM カード不正複製・取替は日本の携帯キャリアでは発生しないシステム・運用となっていること」が確認された。そのため、日本では携帯電話番号の安全性は、海外よりも比較的高いと考えることができる。

【田中 優成, 浦田 泰裕 株式会社アクリート】

¹⁹ 詳細はフィッシング対策協議会のフィッシング対策ガイドライン、フィッシング対策セミナー 2020 の当社提供資料に記載

²⁰ パスワードなどが他者に漏えいしていない利用者を指す。

4.2. ドメイン関連

4.2.1. ドメイン名の廃止にあたっての注意

◆ドメイン名廃止のリスク

合併や事業譲渡に伴う組織名の変更、サービス／キャンペーンの終了などにより、Web サイトや電子メールで使っているドメイン名を「別のドメイン名に切り替える」「今後は利用しない」と判断することがある。

この時、自組織におけるドメイン名の利用の終了をもって、すぐにそのドメイン名を廃止（登録終了）してしまってよいかを判断するにあたっては、いくつか注意しなければならないことがある。

まず、ドメイン名を廃止した場合、そのドメイン名が自組織による登録状態でなくなる、というだけでなく、一定期間後に第三者が登録・利用できるようになる、ということに留意が必要である。

廃止したドメイン名には、他の Web サイトからのリンクや、検索エンジンによるドメイン名の評価に関する情報が残っている場合がある。そのため、リンクや検索エンジンを経由したアクセス数の増加を見越し、第三者によりドメイン名が「ドロップキャッチ²¹」され、まったく関係のない Web サイトを作られてしまう可能性がある。また、悪意がある場合にはそのドメイン名を利用したフィッシング詐欺や誹謗中傷、ブランド悪用などの行為につながるリスクもある。

さらに、そのドメイン名をメールアドレスとして使っていた場合、ドロップキャッチした第三者が同じメールアドレスを作り、なりすましに悪用する可能性もある。特に、SNS やオンラインサービスに登録したメールアドレスとして利用されているドメイン名を廃止してしまうと、メール経由でパスワードを再設定されてアカウントを乗っ取られたり、機密情報を盗み見られたりするリスクもある。

そのため、利用を終えたドメイン名については、ドメイン名廃止に伴うリスクを考慮し、ドメイン名の登録を継続することも選択肢とすべきである。また、廃止を進める場合でも該当の Web サイトやメールアドレスの終了を外部に周知することや、SNS アカウントなどの削除や設定の削除、登録されているメールアドレスの変更など、事前に十分に時間をかけた準備を行うことが必要である。

また、利用を終えたサブドメインや廃止後の第三者による再登録に起因するアクセスの乗っ取り（テイクオーバー）リスクへの対策も必要である。該当するサブドメインやドメイン名が、他のサブドメインやドメイン名から参照先として設定されている場合には、サブドメインの利用終了やドメイン名の廃止前に、参照元となる DNS や外部の CDN サービスなどで設定中の不要な DNS レコー

²¹廃止したドメイン名が一時凍結期間を経て、誰でも登録できる状態になる瞬間を狙って再登録を図る行為。

ド（A/AAAA・CNAME）・転送設定などを削除しておくことが必要である。

◆属性型 JP ドメイン名における 1 組織 1 ドメイン名の制限緩和

co.jp などの属性型 JP ドメイン名は、原則として 1 組織につき 1 ドメイン名しか登録できないため、別の属性型 JP ドメイン名を利用したい場合に、これまで使っていたドメイン名を廃止しなければならない、ということもあるかもしれない。

しかし、「組織名変更」「合併」「事業譲渡」の場合には、複数の属性型 JP ドメイン名を登録することができる、制限緩和が利用可能である²²。この制度を利用することで、これまで利用していたドメイン名の登録を維持しながら、新しいドメイン名を登録・利用できるようになる。ドメイン名の廃止には前述のようなリスクがあるため、この制度の積極的な利用検討を勧めたい。利用にあたっては所定の手続きが必要になるため、詳細は登録中のドメイン名を管理している事業者にご相談して欲しい。

◆誤ってドメイン名を廃止してしまった場合への対処

その意図がないのに誤ってドメイン名を廃止してしまった場合、ドメイン名の種類によっても異なるが、一定期間以内であれば登録回復（登録状態に戻す）などと呼ばれる手続きが用意されていることが多い。対応期間や手続きについてはドメイン名登録をしていた事業者にお問い合わせで欲しい。

【佐々木 俊博 株式会社日本レジストリサービス】

²² 株式会社日本レジストリサービス(JPRS)、「属性型（組織種別型）・地域型 JP ドメイン名登録等に関する規則」の改訂について（<https://jprs.jp/whatsnew/notice/2014/20140217-rule.html>）
（閲覧日：2022 年 2 月 21 日）

4.2.2. ドメイン名を廃止する前のリスク判定

第三者が新規にドメイン名を取得してフィッシングサイトを立ち上げる事例には枚挙にいとまがないが、公式サイトで利用していたドメイン名が廃止された後に再利用される事例も増えている。

Web サイトやメールで利用していたドメイン名を使わなくなって廃止するのは維持コストからは合理的と言えるが、リスクの観点からはドメイン名の廃止はリスクが潜在していることを頭に置いておく必要がある。

ドメイン名の用途は大きく2つの Web サイトとメールが挙げられる。

一つ目の Web サイトでは外部サイトから被リンクが張られ、昨今ではソーシャルメディアからの被リンクも増えている。このような外部サイトからの被リンクを削除することは現実的に不可能と言える。これらの被リンクの残り続けると考えられ、ドメインを廃棄することは、第三者に自社サイトへの被リンクを明け渡すリスクがある。実際には利用者が被リンクから発見してサイトオーナーに通報されて発覚している。

二つ目のメール用途では社員個人のメールアドレスで機密情報のやり取りが日常的に行われている。たとえメールサーバー閉鎖の前に、サーバー移行やメールアドレス変更のお知らせを送っていたとしても、受信者が認知するとは限りません。社員メールで利用していたドメイン名を廃止することは、第三者になりすましを許容することになり、Web 用途よりもリスクが高い状況と言える。

いずれの場合も、使用していたドメイン名を廃止することは間接的に利用者や取引先をリスクにさらすことにつながる。そのリスクヘッジ対策の一つがドメイン名の利用状況の記録で、現在の使用状況だけではなく、過去の使用履歴を記録することが重要となる。

廃止後の対応コストを考えると、維持コストのほうが安いケースも多いため、ドメイン名を廃止しない維持し続けることも一つの選択肢となる。

【加藤 恭久 GMO ブライツコンサルティング株式会社】

■ コラム ドメイン名再考：DMARC と DNSSEC の導入価値は何か～エンドユーザーの観点で～

2021 年後半のフィッシング報告件数は、フィッシング対策協議会の「2022/01 フィッシング報告状況」²³に見られるように、それ以前より多くなっています。

フィッシングサイトの URL も、2021 年以降増加してきました。2019 年の調査ではフィッシングサイトの半分以上が HTTPS を使っているという報告がある一方²⁴、利用者の多い Web ブラウザーは HTTPS に関する表示を簡素化してきており。サイトの正しさを確認するものとしては、ドメイン名が重要な位置づけにあるといえます。

フィッシング対策協議会が作成しているガイドラインでは、事業者向けとユーザー向けいずれにおいても、以前、EV 証明書の表示である緑のバーを確認しやすいように、分かりやすさを追求する説明の糸口がありました。しかし現在は、正しいドメイン名かどうかを判別してもらうという、ユーザーに知識や判断を求める方向になってきています。

それでは、そのドメイン名の確からしさは、エンドユーザーの観点で、どこで危ぶまれるものなのでしょうか。また、ドメイン名の確からしさを確認する技術の導入効果は、エンドユーザーにどのように関わってくるものなのでしょうか。これらの観点では、DMARC や DNSSEC といった技術は、そのものの効果よりも、フィッシングに関する一連の流れにおいて、どのような条件でどのような時にエンドユーザーに働きかけるものなのかという点が重要になってきます。本稿では、フィッシングの流れをいくつかのケースに分けて読み解いていき、今後の展望について考察します。

■ エンドユーザーにとってのドメイン名

フィッシングに接するユーザーにとってドメイン名と詐称への対策技術、DMARC や DNSSEC はどのような意味を持つのでしょうか。ここでは、フィッシングメールから始まり、Web ページの閲覧につながる流れについて、いくつかのケースを挙げて考察してみます。フィッシングは SMS やメールといったメッセージを通じてエンドユーザーにアプローチされます。（本稿ではドメイン名を扱うためメールに注目します。）メールの本文の中に URL が書かれていて、ユーザーがそれにアクセスし、オンラインサービスのパスワードなどを入力するとフィッシングが成立するという流れの想定です。

²³ フィッシング対策協議会、2022/01 フィッシング報告状況、
(<https://www.antiphishing.jp/report/monthly/202201.html>)（閲覧日：2022 年 2 月 24 日）

²⁴ PhishLabs、More Than Half of Phishing Sites Now Use HTTPS、
(<https://www.phishlabs.com/blog/more-than-half-of-phishing-sites-use-https/>)（閲覧日：2022 年 2 月 24 日）

この流れの中でドメイン名が現れるタイミングと、ドメイン名の確からしさに関わる DMARC や DNSSEC の効果が現れるポイントを表にまとめてみます。表は左から右に向かってひとマスずつ見ていくようになっています。ここでは、ケースを 4 つに分けてみます。

下記の表にまとめる前提となる技術導入などの状況は以下のとおりです。

- DMARC や DNSSEC は導入済みである。(DMARC の宣言がされており) ユーザーが利用するメールサーバーでは検証が行われている。ポリシーは reject もしくは none になっている。
- メールに URL が記載されており、ユーザーはその URL を使って Web サイトにアクセスする。
- Web サイトを提供する Web サーバーにはサーバー証明書が導入されており、サーバー認証に成功すると Web ブラウザーは錠前マークを表示する。

表 4-2 ドメイン名に関する 4 つのケース

	1.メール送信ドメイン認証技術の結果	2.メールアドレスのドメイン名	3.DNSSECの効果	4.Webサイトのドメイン名	5.Webサーバ認証技術の結果
A.フィッシングではないケース	• 配送される。 • (正しさの表示) 安心マーク, BIML...	• 正しいドメイン名が表示されている。	• 検証に成功し Webサイトに接続できる。	• 正しいドメイン名が表示されている。	• サーバ認証に成功する。
B.メールアドレスドメイン名が紛らわしい+サイトのURLが紛らわしい	• 配送される。	• メールのドメイン名が紛らわしく、正しいかどうかの判断が付きにくい。	• 検証に成功し Webサイトに接続できる。	• 正しいサイトかどうかの判断が付きにくい。	• サーバ認証に成功する。
C.メールサーバの詐称+サイトのURLが紛らわしい	• "reject" → 配送されない。 • "none" → 配送される。	• (配送された場合) 正しいドメイン名が表示されている。	• 検証に成功し Webサイトに接続できる。	• 正しいサイトかどうかの判断が付きにくい。	• サーバ認証に成功する。
D.メールサーバの詐称+サイトのドメイン名乗っ取り	• "reject" → 配送されない。 • "none" → 配送される。	• (配送された場合) 正しいドメイン名が表示されている。	• 検証に失敗し、Webサイトに接続できない。	• 接続できない。	• 接続できない。

各行についてみていきます。文章中の括弧はどの列かを示しています。

OA.フィッシングではないケース

ユーザーはメールを受信し (1)、メール送信者の正しいドメイン名が表示されます (2)。書かれている URL を使ってアクセスすると本来の Web サーバーにアクセスし (3)、そこで表示されているドメイン名は本来のものということになります (4)。Web のサーバー認証に成功しています (5)。

OB.メールアドレスドメイン名が紛らわしい上にサイトのURLが紛らわしいケース

フィッシングメールの例です。メールアドレスのドメイン名はユーザー

には紛らわしくても、DMARC の検証は通り、ユーザーはメールを受信します (1)。メール送信者のドメイン名は表示されていますが、ユーザーは正しいかどうかの判別がつきにくい状態です (2)。

メールに書かれている URL のドメイン名に対する DNSSEC 検証は通り (3)、Web サイトにアクセスできても正しいサイトかどうかの判断はつきにくい状態です (4)。Web サーバーの認証に成功し錠前マークは表示されています。これが現在の典型的なフィッシングの流れではないでしょうか。

OC.送信メールサーバーが詐称されていてサイトの URL が紛らわしいケース

これもフィッシングメールの例です。メールアドレスのドメイン名は正しいですが、送信メールサーバーは本来のものではありません。DMARC では検証側のポリシーに応じて、ユーザーがメールを受信するかしないかが決まります (1)。メール送信者のドメイン名は正しいものです (2)。

メールに書かれている URL はユーザーにとって紛らわしいものですが、DNSSEC の検証には通り (3)、紛らわしいドメイン名を持つ Web サイトに接続できることとなります (4)。Web サーバーの認証に成功し錠前マークが表示されています (5)。

OD.送信メールサーバーが詐称されておりサイトのドメイン名が表示されるケース

この例はメールの送信サーバーが本来とは異なるところまでは C と同じです (1) (2)。メールに書かれている URL にユーザーがアクセスすると、偽のメールサーバーが応答するなどドメイン名が詐称されているため、DNSSEC の検証に失敗し、ユーザーは Web サイトに接続できないこととなります (3)。ドメイン名は正しいものですが、接続できないためユーザーは戸惑うかも知れません (4) (5)。

■送信ドメイン認証技術と DNSSEC が導入されるとエンドユーザーの体験はどう変わるか

前述の表から読み取れることを三点にまとめます。

- ・ DMARC の検証ポリシーを reject にするとユーザーは、紛らわしいドメイン名を判別しなくて良くなる (表中の枠 X)。ただし、DMARC の検証ポリシーが none であるとメールサーバーの管理者が検知できるだけで、ユーザーに起きることは送信ドメイン認証技術の導入前と変わらない。

- ・ メールアドレスに紛らわしいドメイン名が使われると、ユーザーがフィッシングかどうかを判断するにはドメイン名が正しいかどうかを判別する必要がある（枠 Y1）。Web サイトのドメイン名についても同様である（枠 Y2）。ユーザーにとってドメイン名が紛らわしいということ自体の判定は難しい。
- ・ DNSSEC の検証で失敗し接続できなくなる挙動は、フィッシングサイトへのアクセスを抑止するという意味ではユーザーを保護する。しかしアクセスできない理由が分からなければユーザーは何とかしてアクセスしようとしてしまうかも知れない。これについては改善の方向性がある。IETF の RFC8914 に記載されている Extended DNS Error（拡張 DNS エラー）²⁵や、提案中の DNS Access Denied Error Page（DNS アクセス禁止に関するエラーページ）²⁶である。これらのエラーを受けた Web ブラウザーの表示がどうなっていくのかが注目される。

送信ドメイン認証技術と DNSSEC が偽ドメイン名に関するユーザーへの注意喚起という意味で機能していない場合、Web サイトで紛らわしいドメイン名が使われていると、サーバー認証には成功してしまいます。そのため、ユーザーは錠前マークを見て安心してしまう可能性があります（枠 Z）。十分に導入されているとは言い難い現在、ユーザーにフィッシングサイトの利用を避けていただくには、Web サイトのドメイン名が正しいかどうかを確認いただくしかないということになります。

■ 考察-現在と今後

まず前述のことからわかることは、DMARC などのメール送信ドメイン認証の検証ポリシーを"reject"にするような普及ができれば、ユーザーの判別に頼らなくて良くなるということになるということです。

Web サーバー認証技術は、サーバー証明書の種類であるドメイン検証（DV）・組織検証（OV）・拡張組織検証（EV）の違いがあり、フィッシングサイトのほとんどが DV 証明書を使っているという報告があります²⁷。しかしそうだとすると、その結果表示が変わり、その表示に応じてユーザーが、クレジットカード番号を入力しない、ユーザーID やパスワードを入力しないといった挙動を変えられるようになっていない限り、導入効果が現れにくいことになります。

DNSSEC は紛らわしいドメイン名を検出することに関して効果を発揮しま

²⁵ Extended DNS Errors(RFC8914)、(<https://datatracker.ietf.org/doc/html/rfc8914>)（閲覧日：2022 年 2 月 24 日）

²⁶ DNS Access Denied Error Page, (<https://datatracker.ietf.org/doc/draft-reddy-dnsop-error-page/>)（閲覧日：2022 年 2 月 24 日）

²⁷ USENIX, Certified Phishing: Taking a Look at Public Key Certificates of Phishing Websites, (<https://www.usenix.org/system/files/soups2019-drury.pdf>)（閲覧日：2022 年 2 月 24 日）

せんが、特定のドメイン名に対する有名なキャッシュポイズニングといった、ユーザーが気付きにくいリスクを避ける基盤的な位置づけであるといえます。その検証失敗についていかにユーザーに伝えていくのかが今後の課題ではないでしょうか。

各々の技術がユーザーの視点でどのような役割を果たすものであるかを踏まえた上で、ユーザーがフィッシングサイトを使わなくなるような効果を得られるような技術普及が望まれます。

【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】

5. まとめ

フィッシングレポートは、WG のメンバーに最新のフィッシングの動向やフィッシング対策の最新技術の動向などを書いていただいている。1. フィッシングの動向にあるように、この一年のフィッシングは急増し、手法もユーザーの反応時間が短い傾向にある SMS が増加し、それに伴いフィッシングサイトの存続時間も短くなり、フィッシング関連情報の収集・共有にも新しい取り組みが必要となっており、フィッシング URL の早期配信についても新しい取り組みが必要になっている。新しいユーザー認証技術としては FIDO が期待されているが、その一方で、既存のフィッシング対策技術をきちんと使っていただく必要もあり、IT サービス事業者が認証を行う点での推奨事項やベストプラクティスに対するさらなる理解も必要である。

一方で、技術的対策のみでは難しくなっている。また技術的対策の多くはフィッシングが実行される段階での対応となっている。そこで、フィッシングの実行前の段階での対応を考えられないかということで、シフトレフということで、実行前段階での対策や技術的対策以外の対策についても考察をしていただいた。

フィッシング対策ということで、ユーザーにわかりやすくドメインの認知してもらおうなど、ドメインの管理の問題が重要になってきている。そこで、ドメイン関連ということで、ドメイン名の廃止にあたっての注意や廃止されたドメイン名のドロップキャッチの事例についても書いていただいた。また、フィッシング対策としてのドメイン名について、ユーザー視点でどういう意味があるのかを含め再考ドメイン名ということで考察いただいた。

今年度のフィッシングレポートも WG のメンバーにいろいろな視点で文書を投稿いただき、現状のフィッシングの展望や課題について幅広く記述された内容となっていると思われる。寄稿いただいた技術・制度検討ワーキンググループのメンバーの方には、あらためてお礼を述べたい。

【野々下 幸治 トレンドマイクロ株式会社】

(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】

野々下 幸治 トレンドマイクロ株式会社

【構成員】

田中 優成	株式会社アクリート
浦田 泰裕	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
早川 和実	NTT コミュニケーションズ株式会社
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
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
島田 美奈	株式会社カウリス
福岡 省吾	株式会社カウリス
松本 悦宜	Capy 株式会社
加藤 恭久	GMO ブライツコンサルティング株式会社
加藤 孝浩	トッパン・フォームズ株式会社
遠藤 淳	株式会社日本レジストリサービス
佐々木 俊博	株式会社日本レジストリサービス
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
貞広 憲一	株式会社セブン銀行（2021 年 11 月まで）
立石 聡明	一般社団法人日本インターネットプロバイダー協会
加藤 雅彦	長崎県立大学
稲葉 緑	情報セキュリティ大学院大学

【オブザーバー】

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)