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 2023

2023 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

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. 国内の状況

警察庁の発表[1]によると、2022 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前年の同期と比べ増加しており、令和 4 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 233 件であった。このうち 217 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 144 件、被害額約 3 億 1,571 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。

フィッシング情報の届け出件数について、2022 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。

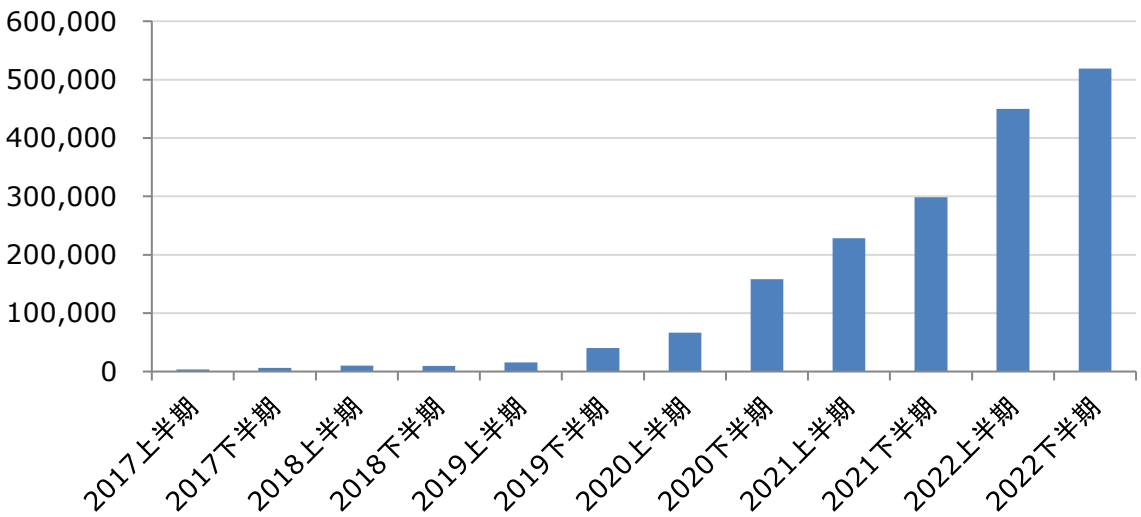


図 1-1　国内のフィッシング情報の届け出件数[2]

[1] 警察庁、令和４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/R04_kami_cyber_jousei.pdf）（閲覧日：2023年2月14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：2023 年２月６日）より作成

フィッシングサイトの URL 件数は、2022 年度下半期は 2021 年下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、2021 年と比較して増加の傾向にある（図 1-3）。

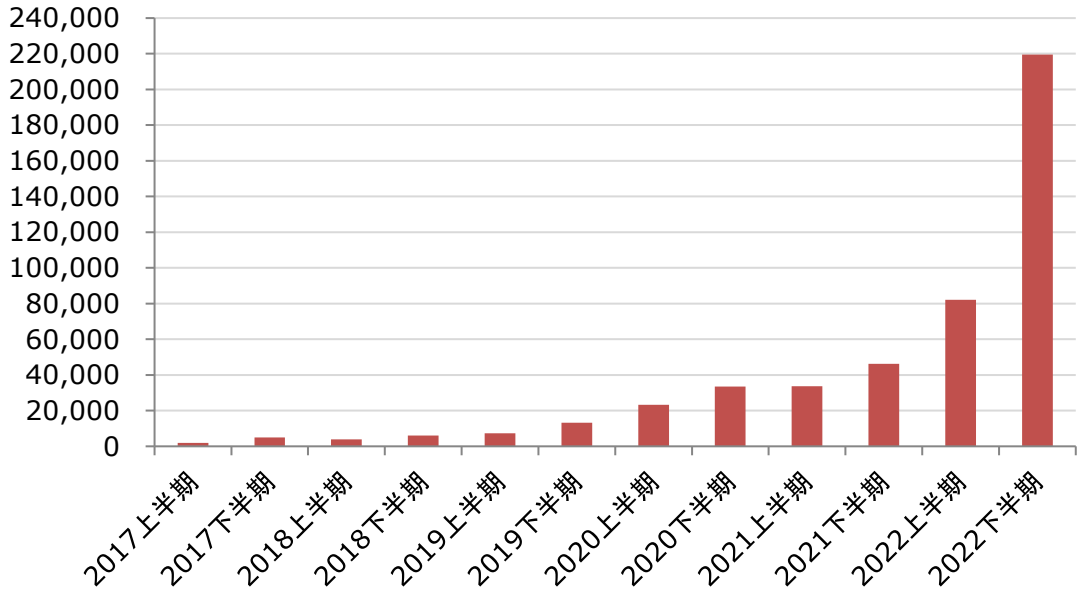


図 1-2　国内のフィッシングサイトの件数 [2]

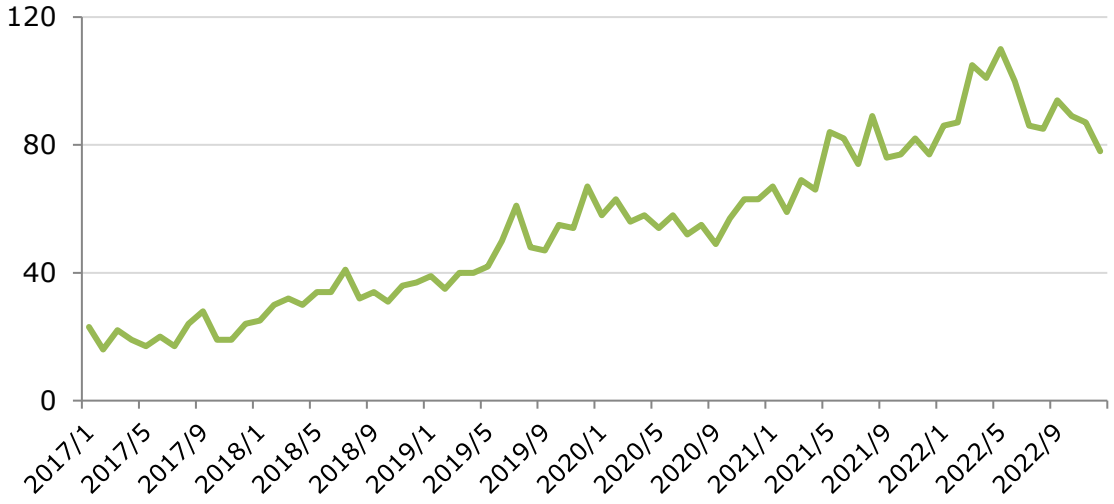


図 1-3　国内のブランド名を悪用された企業の件数 [2]

また、警察庁・総務省・経済産業省の発表[3]によれば、2022 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 2021 年に比べて増加した（図 1-4）。2022 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、5 割弱を占める（図 1-5）。

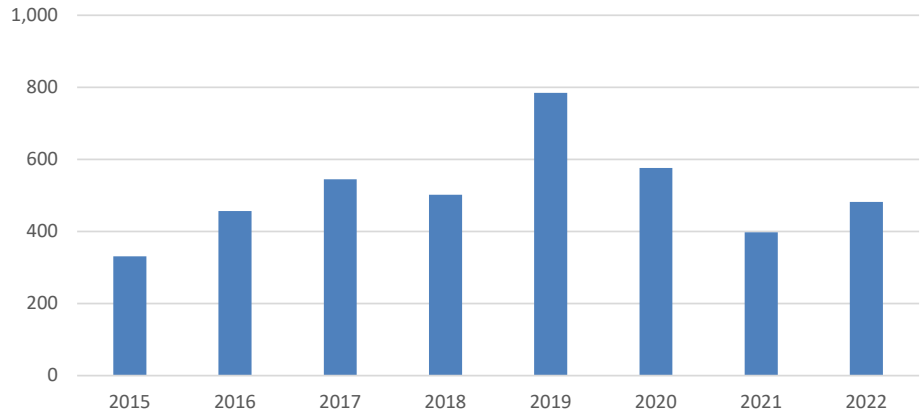


図 1-4　識別符号窃用（ID 窃盗）型不正アクセス行為の検挙件数[4]

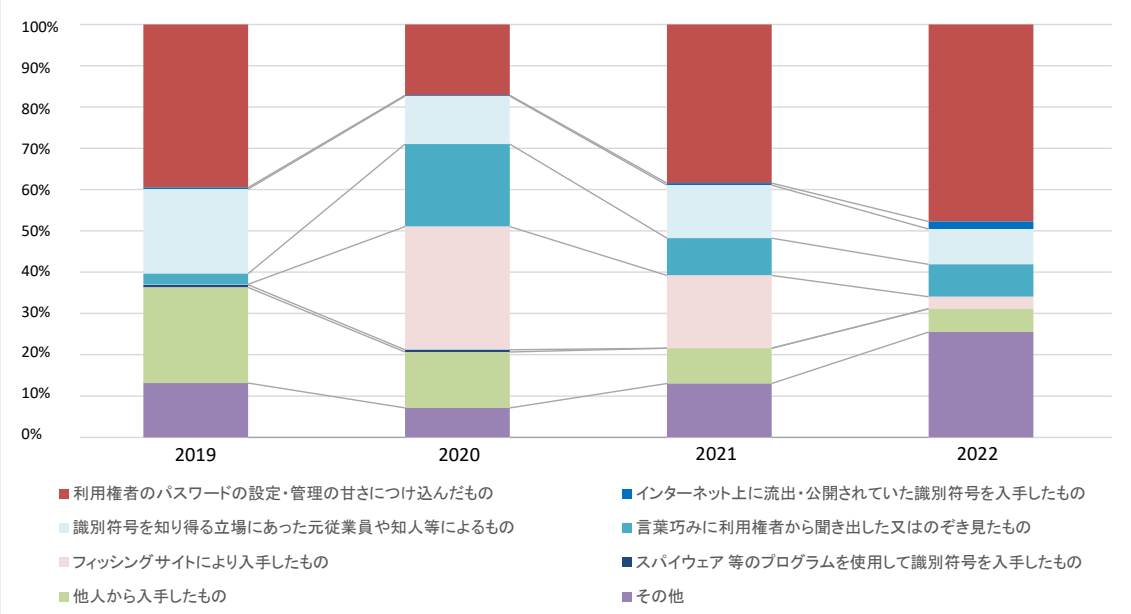


図 1-5　識別符号窃用型不正アクセス行為の手口別検挙件数の内訳（2019 年～2022 年）[5]

【エム・アール・アイリサーチアソシエイツ株式会社】

[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/000868634.pdf）（閲覧日：2023 年 3 月 23 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、2021 年のフィッシング届け出件数は、2020 年から減少した（図 1-6）。フィッシングサイトの件数は、2022 年上半期は前年から増加した（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 の報告によると、2022 年の第 3 四半期には金融機関に対するフィッシングが全体の 23.2%を占めていることが報告されている[6]。全体のフィッシングの動向としては、Business Email Compromise のフィッシングが引き続き増加していることが示されている。

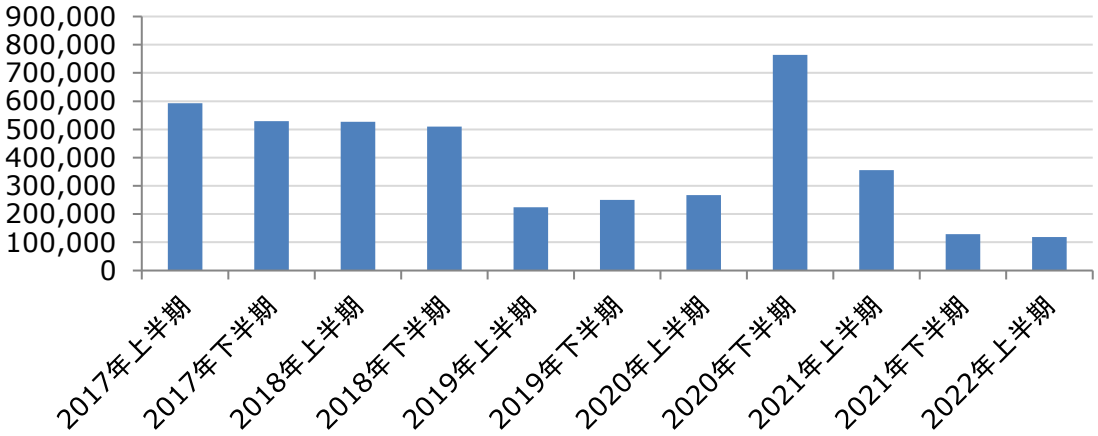


図 1-6　APWG へのフィッシングメール届け出件数[7]

[6] APWG（Anti-Phishing Working Group）、"Phishing Activity Trends Report"（https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf）（閲覧日：2023 年 2 月 6 日）

[7] APWG（Anti-Phishing Working Group）、"Phishing Activity Trends Report"（https://apwg.org/trendsreports/）（閲覧日：2023 年 2 月 6 日）

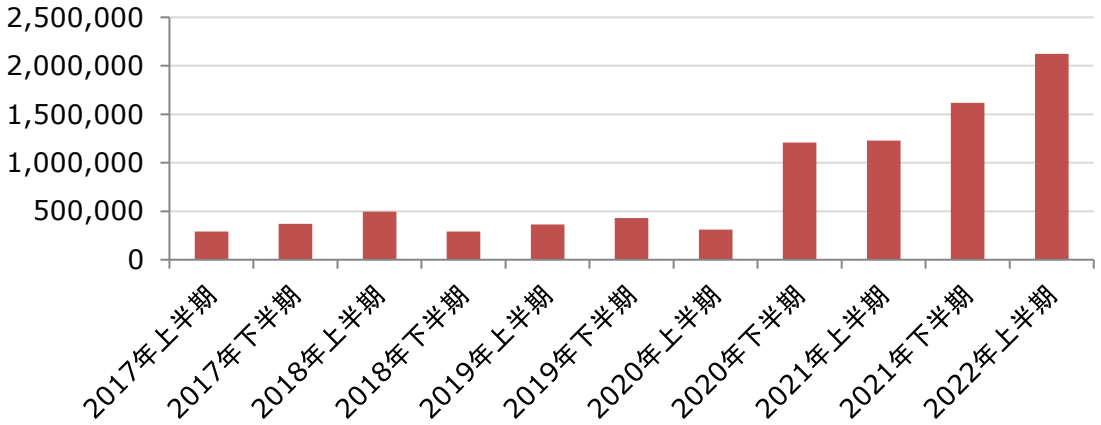


図 1-7　フィッシングサイトの件数（APWG）[8]

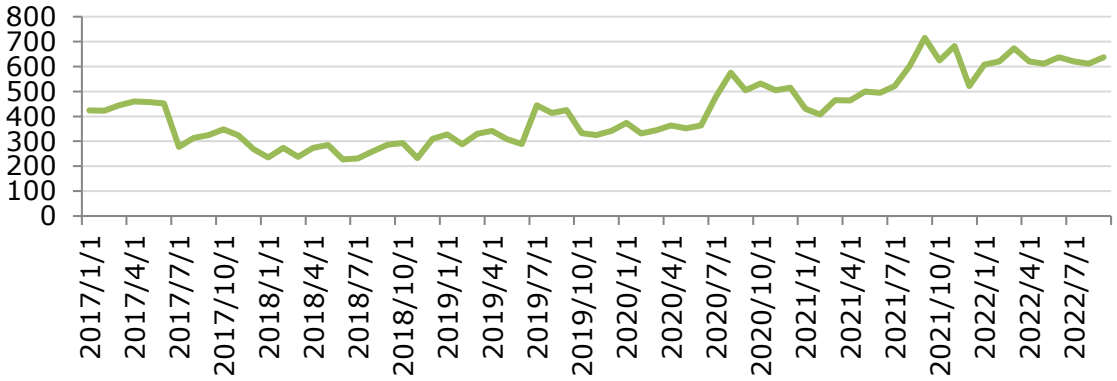


図 1-8　フィッシングによりブランド名を悪用された企業の件数（APWG）[9]

【エム・アール・アイリサーチアソシエイツ株式会社】

[8] APWG（Anti-Phishing Working Group）、"Phishing Activity Trends Report"（https://apwg.org/trendsreports/）（閲覧日：2023 年 2 月 6 日）より作成
[9] 同上

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 2022 年 1 月から 12 月までのフィッシング報告件数は 968,832 件で、2021 年と比較して約 1.8 倍となった。

7 月には、報告件数が 10 万件を超え過去最高となった。これは、大量のドメインとサブドメインを組みあわせたフィッシング URL が報告されたことが影響しているが、10 月以降は減少している。

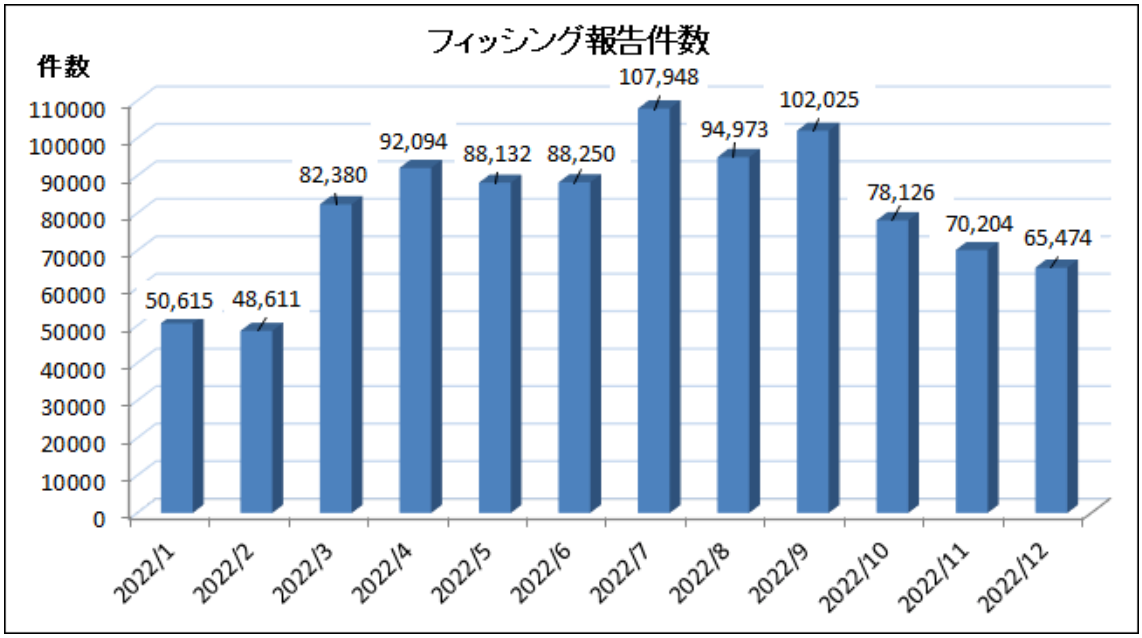


図 1-9　2022 年フィッシング報告件数の推移

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

2022 年は、クレジットカードをかたるフィッシングの報告件数が最多となり、その割合は全体の約 42.6%、そのブランド数は 39 ブランドであった。EC 系（インターネットショッピングなど）をかたるフィッシングも継続に行われていて、その割合は約 30.0%であった。

クレジットカード情報を狙うことに加えて、キャッシュレス決済サービスをかたるフィッシングも発生した。これはスマートフォンによるキャッシュレス決済サービスの利用率が増加していることからターゲットにしていると考えられ、詐取した情報をもとに不正に決済サービスを利用して利益を得るものである。キャッシュレス決済サービス側が対策すると、別のブランドへ移行する動きもあった。

前年度から発生していた ETC 利用照会サービスや交通系サービスをかたるフィッシングは、コロナ禍で止まっていた交通往来再開をターゲットに定常的に発生するようになっている。また、政府による全国旅行支援が発表されると旅行予約サイトをかたるフィッシングも発生した。

省庁関連では国税庁をかたるフィッシングが多く発生した。誘導方法としては、電子メール、SMS 両方で行われていて定番化している。その他では警察庁や金融庁をかたるフィッシングも発生している。

1.3.2. フィッシング URL 数の増加

冒頭でも取り上げた大量にドメインとサブドメインを組みあわせたフィッシング URL を取得し、不正サイトへ誘導する手法により URL 件数が増加した。誘導メールでは複数のブランドがかたられていて、同一デザインのフィッシングサイトへ誘導された。これは、複数の URL を使用することにより、URL フィルターの検知率を低減させるためと考えられる。10 月以降減少したものの、その代わりに短縮 URL や DDNS サービスを使用した誘導が増加している。

1.3.3. フィッシングで使用された多様な手法

フィッシングサイトへの誘導方法として、翻訳サービスの正規 URL を経由した誘導や QR コードを使用した誘導が行われた。また、スマートフォンや通信キャリアのネットワーク網からのアクセスしか許可しないフィッシングサイトも増加してきている。このような手法やアクセス制限は、いずれも URL フィルターの検知を逃れたり、フィッシングサイトの調査行為を妨害したりするためのものと考えられる。翻訳サービスを利用した誘導手法以外は、いずれも過去にも使われている手法であるが、犯罪者は常にその有効性を試していて効率的に利益の得られる手段を模索している。

1.3.4. 「なりすまし」送信メールの継続

2021 年に引き続き、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」送信メールが継続していて、観測している受信メールアドレスで受信したフィッシングメールの内、平均約 71.6%、最大で 89.9%が「なりすまし」送信メールであった。ドメインフォルダーである事業者には、利用者保護のため送信ドメイン認証技術（DMARC）を導入するとともに、DMARC レポートによる「なりすまし」送信メールの把握から、隔離・拒否へとステップを

進めてもらいたい。また、そのような「なりすまし」送信メールを大量に受信している利用者は、正規メールにブランドアイコンが表示されるなどのフィッシング対策機能が強化されているメールサービスを使用することも検討してもらいたい。

【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

今年度は、多くの新しいメンバーの参加があり、フレッシュな意見を多くいただけました。事業者向けガイドラインについては、フィッシングの報告受付窓口を行っている JPCERT/CC の平塚様より、実際の窓口での対応からフィードバックをいただき、冗長な要件の削除などを行った。それにより、34 件あったガイドラインの要件を 29 件に削減した。

報告を受けたフィッシングメールの調査の中で、なりすましメールが半数以上を占め、なりすましメールの 8 割は「DMARC」で検出可能と、「DMARC」の重要性をあらためて再認識した。「DMARC」の対応状況も大手の携帯通信キャリアも対応するなど、多くのメール受信利用者が「DMARC」によるなりすましメールの検知が可能になり、2022 年は、送信側の企業の「DMARC」の導入もかなり進んだ。それをさらに進めるためにも今回のガイドラインでは DMARC に関する記述について、報告受付窓口を行っていただいている平塚様の意見を入れ、さらなる追加を行った。

一方で、フィッシングは、検知が難しい SMS の増加がみられているが SMS については、国内直接接続による配信、または RCS 準拠サービスの利用以外のいい対応がなく、RCS 準拠サービスの導入および利用者の利用が望まれる。

【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ーを通じて被害状況の共有を図っている。

2022 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。

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。

2022 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。

2022 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。

・Web サイトのサーバー証明書種類の確認方法（2022/09/06） 公開のお知らせ
https://www.antiphishing.jp/news/info/certificate_checker_20220906.html

・【更新】 各ブラウザーによる SSL / TLS サーバー証明書の表示の違い (2022/09/06) 公開のお知らせ
https://www.antiphishing.jp/news/info/_ssl_20220906.html

◆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 [10]。

2022 年の活動としては、『第 18 回 IPA「ひろげよう情報モラル・セキュリティコンクール」 2022』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。[11]

◆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。

2022 年の活動としては、マルウェア対策研究人材育成ワークショップ 2022 で発表した。講演資料を以下サイトにて公開している。

講演タイトル：フィッシング対策研究 101

発表者：加藤 雅彦氏（フィッシング対策協議会 学術研究 WG・長崎県立大

[10]フィッシング対策協議会、STOP THINK CONNECT Web サイト（https://stopthinkconnect.jp/）STOP. THINK. CONNECT. とは（https://www.antiphishing.jp/pdf/about_StopThinkConnect.pdf）（閲覧日：2023 年 2 月 14 日）

[11]フィッシング対策協議会、『第 18 回 IPA「ひろげよう情報モラル・セキュリティコンクール」2022』の優秀賞を選出（https://www.antiphishing.jp/news/info/ipa_competition2022.html）（閲覧日：2023 年 2 月 14 日）

学 情報システム学部 情報セキュリティ学科 教授）
詳細は・発表資料（MWS2022 のサイト）
https://www.iwsec.org/mws/2022/mws20221025.html

【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 による調査結果（インターネットサービス利用、認証への利用者意識の変化について）

認証方法調査・推進 WG では 2020 年に実施した【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】の追跡調査として、2022 年 12 月に同様の調査を実施した。新型コロナ感染や東京オリンピックの開催などを経て、インターネット利用も変化しており、利用者の状況や意識にどの様な変化があったかを確認した。その結果についてダイジェストを紹介する。

今回の調査結果によると、2020 年以降コロナ禍の影響でインターネットサービスの利用が増加したこと、パソコンよりもスマホでの利用比率が上がっていることが確認された。それに伴いログインの方法やパスワードの管理などに変化が見られた。また、安全利用の意識についても変化が確認された。

以下、調査の概要と特徴的な結果について紹介する。

＜調査概要＞

実施期間　2022 年 12 月 7 日（水）～2022 年 12 月 12 日（月）

調査方法　調査会社による Web システムでアンケート調査を実施

調査対象　インターネットにてサービス利用を経験したことがある者

回答者数　533 名　（男性 264 名、女性 269 名）

	男性	女性	計
18歳～29歳	53	54	107
30歳～39歳	51	52	103
40歳～49歳	50	52	102
50歳～59歳	55	54	109
60歳～69歳	55	57	112
合計	264	269	533

■よく利用するインターネットサービスについて

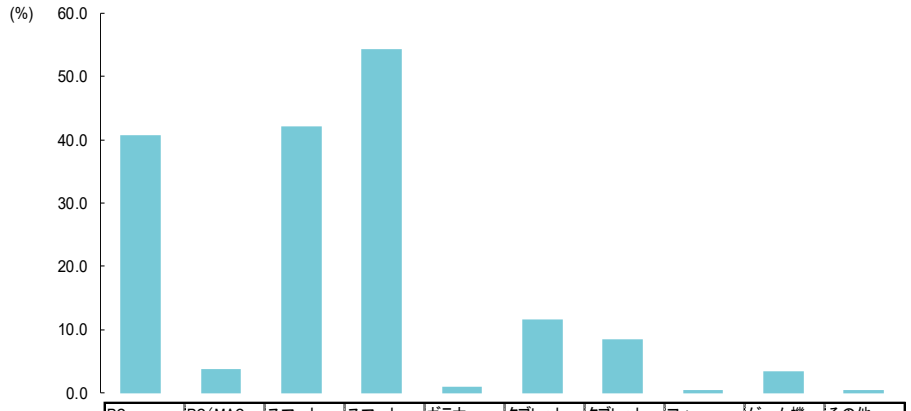
コロナ禍前と比べ、SNS が 51.4%から 62.3%へ、動画配信が 32.2%から 52.5%へ増加、オンライン上でのコミュニケーションが活発化したと思われる。

オンラインショッピングも 35.4%から 40.3%へと増加、今回新たに確認したオンライン決済が 41.1%と利用が活発である。

インターネットバンキングが 36.8%から 26.1%と減少しているが、これはオンライン決済の普及が進み、銀行振り込み決済が減少したためと思われる。

■インターネットサービスを利用するデバイス（機器）について

PC の利用が前回 66.2%から 40.7%へ大幅に減少している。インターネットサービス利用の多くがスマートフォン内で完結できることで、スマートフォン利用だけを想定したサービスが増加したためと思われる。



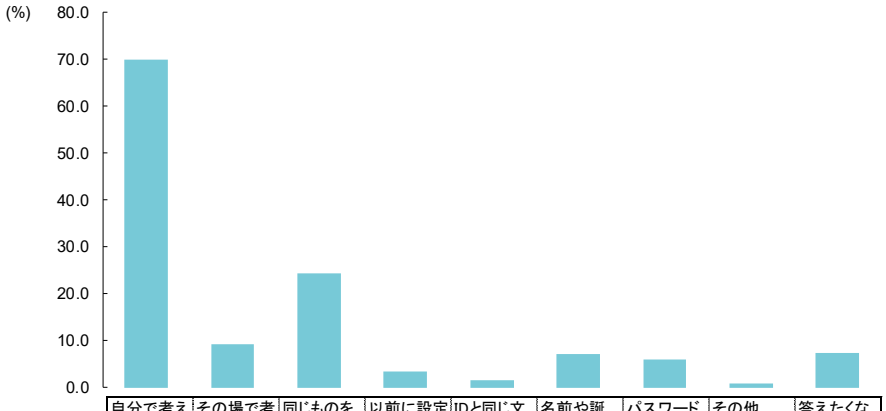
	n=	PC（Windows）	PC（MAC：Macintosh）	スマートフォン（iPhone：iOS）	スマートフォン（Android）	ガラホ（Android）＊携帯電話（ガラケー）形状スマートフォン	タブレット（iPad：iOS）	タブレット（Android）	フィーチャーフォン（ガラケー）	ゲーム機	その他
TOTAL	533	40.7	3.8	42.2	54.4	0.9	11.6	8.4	0.4	3.4	0.4

■パスワード文字列の文字数について

前回は 11 文字以上が 29.9%あったが、今回は 10.2%（6.4%＋3.8%）と 3 分の 1 程度まで下がっている。長めのパスワードが嫌われている傾向がある。

■パスワード設定での、パターンやルールについて

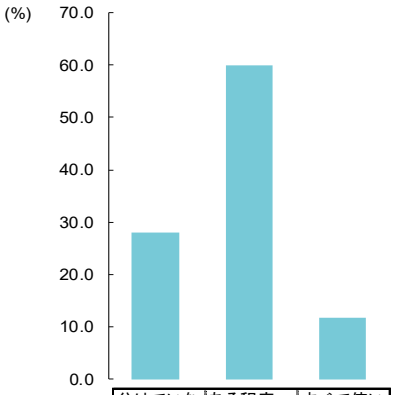
前回とは違った傾向となっており、前回その場で考えて決めるが 40.7%あったが、今回は 9.2%と大きく減少しており、パスワードの決定が計画的に実施されるようになったと思われる。記憶しやすいものも 16.0%から 7.1%へ減少しており、パスワード設定について安全意識が高まっていると思われる。



	n=	自分で考えた規則（パターン、ルール）で決定する	その場で考えて決める（不規則）	同じものを使いまわす	以前に設定したものを時期をあけて再使用	IDと同じ文字列	名前や誕生日など記憶しやすいものにしている	パスワード入力欄で表示される強度評価を参考に決める	その他	答えたくない
TOTAL	533	70.0	9.2	24.4	3.4	1.5	7.1	6.0	0.8	7.3

■パスワードの使い分けについて

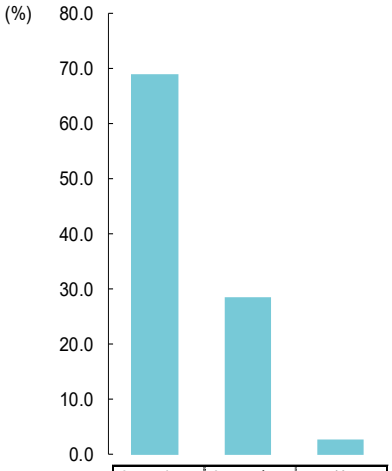
前回と同様の傾向ではあるが、一つを使いまわしているが 17.4%から 28.1%へ増加しており、使いまわしの危険度が増している。これは、多くのサービスを利用するようになり、利便性から同じパスワードを使いまわす機会が増えていると思われる。



	n=	分けていない。一つを使いまわしている	ある程度、インターネットサービスによって使い分けている	すべて使い分けている
TOTAL	533	28.1	60.0	11.8

■安全性を重視した面倒なサービスと、便利な利用を重視したサービスでは、どちらを利用したいと思うか。

少し面倒でも安全性を重視が 58%から 68.9%へ増加、少し不安でも簡単重視が 39.5%から 28.5%へ減少と変化があった。安全重視傾向が強まった。



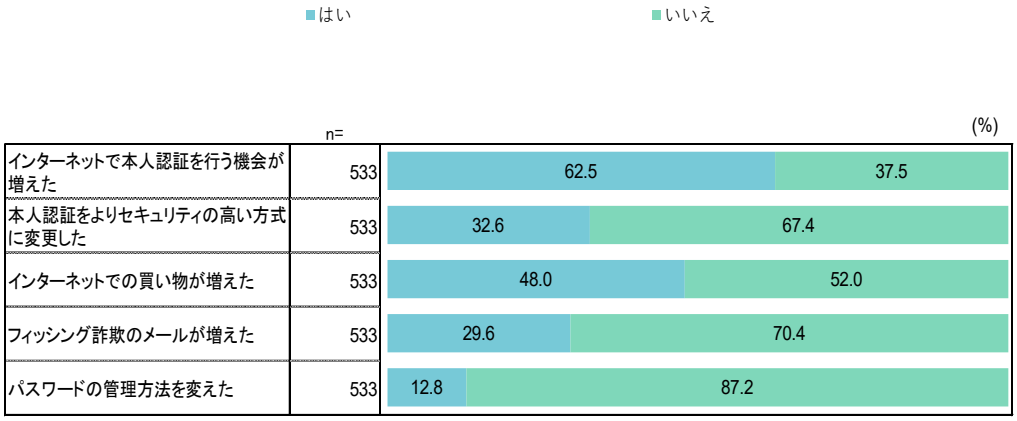
	n=	少し面倒でも安全性が重視されたサービス	少し不安でもログインが簡単で使いやすいサービス	その他
TOTAL	533	68.9	28.5	2.6

■コロナ禍以前と比べた、インターネット上のサービスの使い方や本人認証の方法などの変化について。

比較のために今回の調査で設けた質問。

認証機会が増えた、買い物が増えたとの回答が多く、サービス利用の量、幅が広がったと思われる。

フィッシングメールの増加に反応がないことについては危惧するところである。



スマホでのサービス利用が大きく進んだ結果、アプリでのサービス提供も増加し、初期設定で実施した認証の情報で継続利用している状況が増えているようだ。その結果、認証への意識が低くなっていると思われ、アカウントの管理など安全利用への注意が薄れている可能性について心配な状況である。インターネットサービス利用増加に伴いフィッシング詐欺などに遭う機会も増加し、利用に際し不安な状況は広まっていることから、安全への意識は高まっているようである。

【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. フィッシングの被害

3.1. 保険会社を狙った新しいフィッシング被害

2021 年 11 月以降、明治安田生命、住友生命、アフラック、朝日生命など、複数の生命保険会社をかたったフィッシング報告を受けている。登録された個人情報の再確認を求めるフィッシングメールから保険契約者専用サイトを装ったフィッシングサイトに誘導し、専用サイトの ID とパスワード、さらに保険証券番号の入力が求められる。このフィッシングは保険の契約者貸付制度（解約返戻金の一定範囲内で必要資金を用立てする制度）を悪用した可能性がある。詐取した会員 ID を使って振込先を偽装口座に変更し、貸付金を不正に受け取る詐欺である。フィッシング対策ガイドラインでは、「登録情報を変更するページへの移動には再度認証を要求すること」として、本人識別の精度を上げるため、単一の情報（パスワードのみ）ではなく、複数の情報を求めるようにすることが望ましいとしている。事業者は会員 ID が詐取された場合の影響範囲を調査し、複数要素認証などの認証強化を検討することが望ましい。

図 3-1　明治安田生命をかたるフィッシングサイト

【加藤 孝浩　トッパン・フォームズ株式会社】

3.2. ブランド名だけを差し替えるパターン化したフィッシングメール

クレジットカード会社やキャッシュレス決済事業者などをかたるフィッシングの報告が増した。クレジットカードの利用確認に関する通知を装うフィッシング内容であるが、フィッシングメールの文面はほぼ同じ内容となっており、ブランド名のみを差し替えて作成されていて、利用者はブランド名だけ変更となった複数通数のフィッシングメールを受信している場合もある。攻撃者は本物と同じメール文面を使う攻撃からブランド名のみを差し替える手法に変化し、フィッシングメールの量を増加させている。

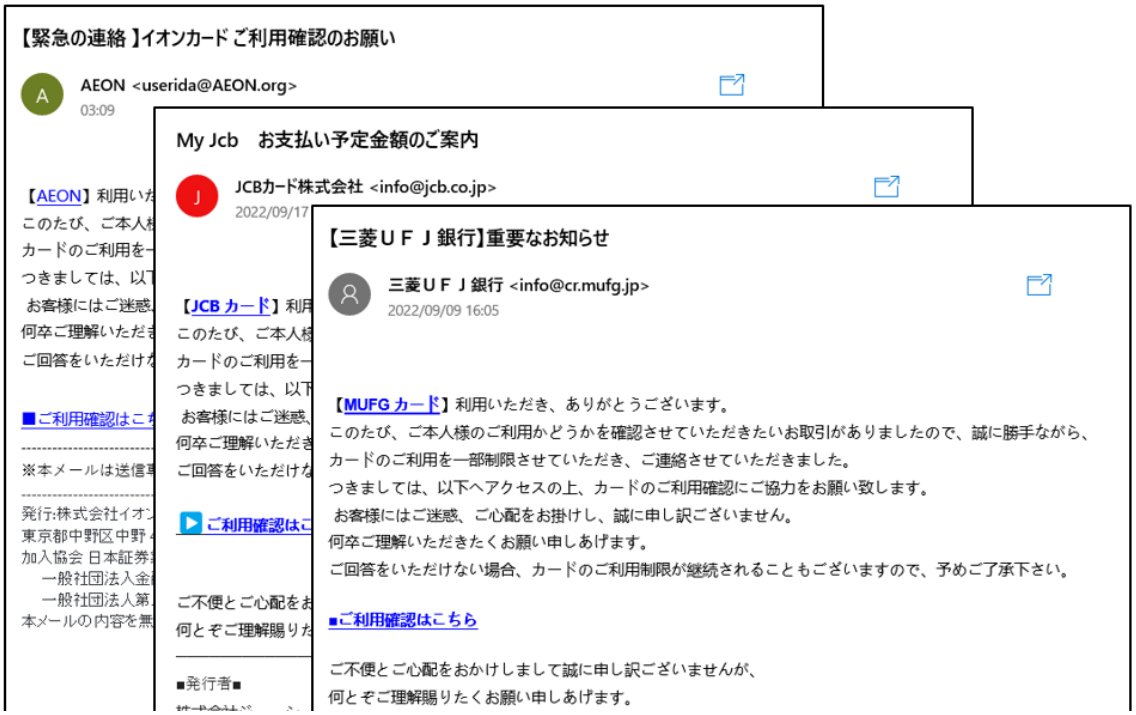


図 3-2　パターン化したフィッシングメールの例

【加藤 孝浩　トッパン・フォームズ株式会社】

3.3. それでもなぜ人は騙されるのか～被害者の視点・詐欺犯の視点～

そもそもフィッシングは利用者をだますソーシャルエンジニアリングである。手口は古くからある現実の詐欺と同じく、人の心理を突くものであり、これを日常のインターネット利用シーンに応用したものである。ネット利用者という広いターゲットに対し、対象の人数、場所に縛られず、数々の詐欺文面や詐欺サイトを使って活動できるため被害は広がっている。

対策として、システム（テクノロジー）による防御、啓発・注意喚起が行われているが、いずれも道半ばである。このような中、だます／だまされる対象がシステムではなく人であるため、啓発・注意喚起は重要なアプローチと言える。

啓発・注意喚起の課題は、届けたい相手に適切に届いていないことである。届けたい相手とは、IT に関して特別な関心を持たない一般利用者である。例えば企業・団体がホームページに掲載するケースを考えても、一般利用者が、日々の生活動線の中で自発的に当該ページを見る機会は皆無であることは容易に想像できる。企業で行われるフィッシング訓練など啓発機会から切り離されている利用者も詐欺ターゲットである。TV など公共メディアと繋がりはネット世代と言われる若年層ほど薄い。学校教育における啓発の有無・内容・対象学年もバラつきがある。

啓発は、フィッシング詐欺の存在と脅威を一般に知らしめ、慎重な行動を促す・用心深くなっていただくことが期待値である。注意喚起は、発生中のフィッシング詐欺をタイムリーに広くお知らせし、詐欺メール・詐欺サイトに対して利用者が反応するのを思いとどまらせることが期待値である。

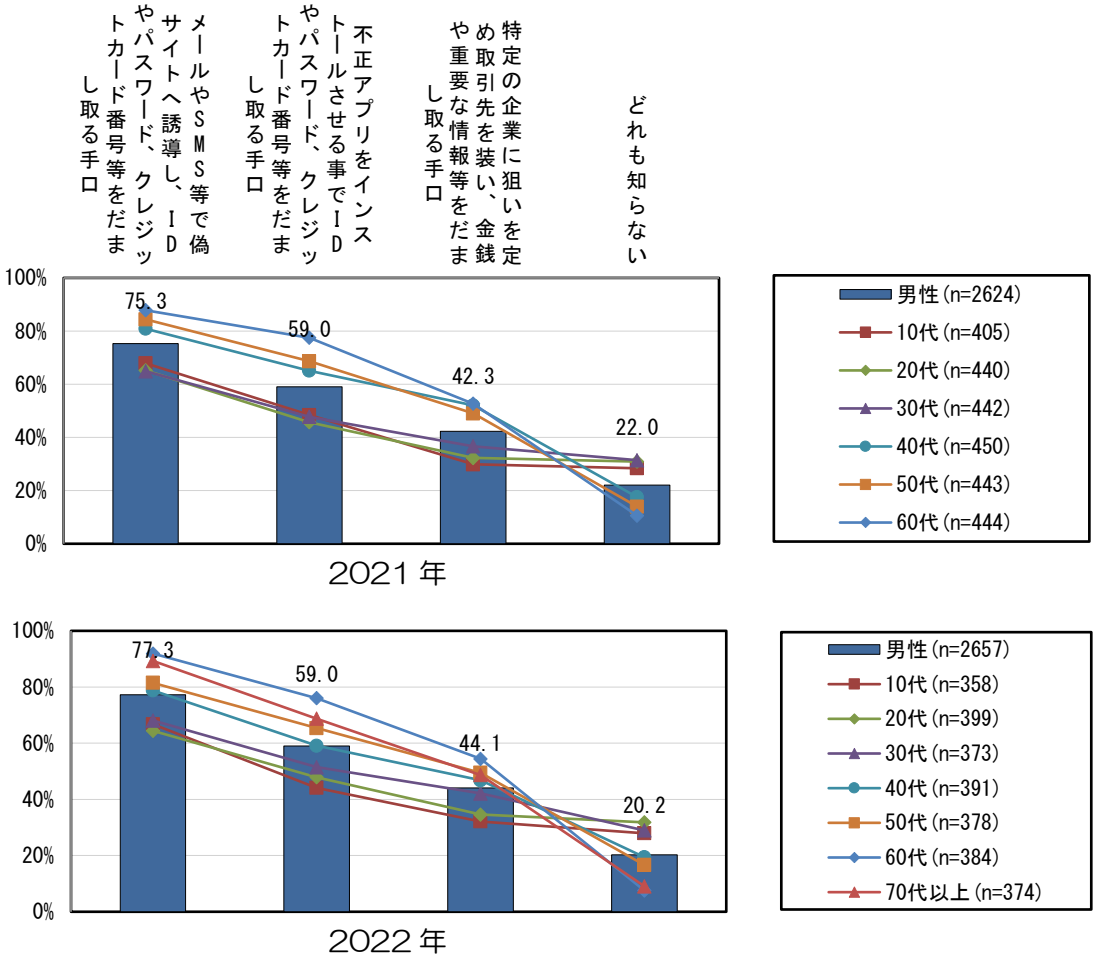
騙される人を減らすには、上記の期待値をしっかり踏まえ、一般利用者の日常のネット動線に沿った情報発信、ネット経済圏への新規参入者が常にいることなど年齢構成や利用者動態なども加味した啓発や注意喚起が必要である。どうすれば一般利用者へ届くか、アプローチ方法を考え改善し続けることが求められる。

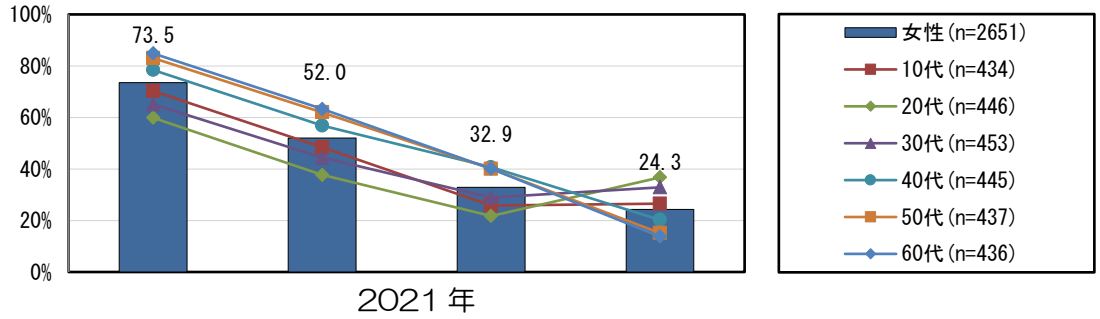
【塚田 晴史,鈴木 一実　株式会社マクニカ】

4. SMS を用いたフィッシング詐欺についての意識調査

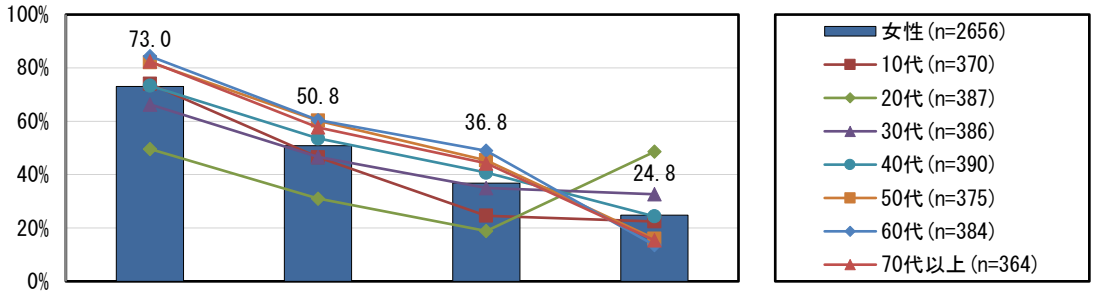
2021 年に SMS を用いたフィッシング詐欺について消費者の意識や被害の実態を調査するアンケートを実施し、その結果をフィッシングレポート 2022 で報告したが、今回も同様のアンケートを実施したので報告する。アンケートは、インターネットリサーチにて対象者を年代ごと、男性、女性の比率などが同等になるよう配慮し、5,313 名から回答を得た。前回は 60 代までを対象にしていたが、今回は 70 代以上も対象としている。以下、調査結果のポイントについて紹介する。

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





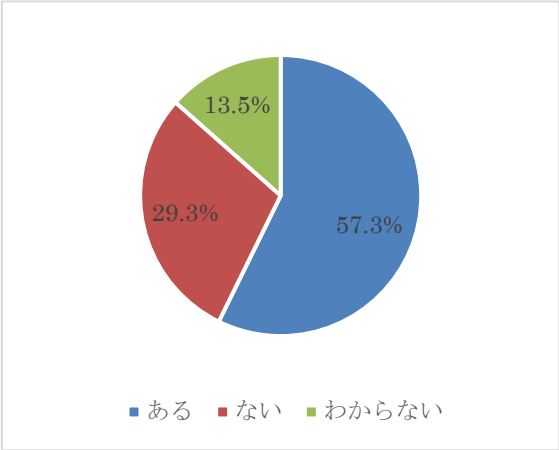
2021 年



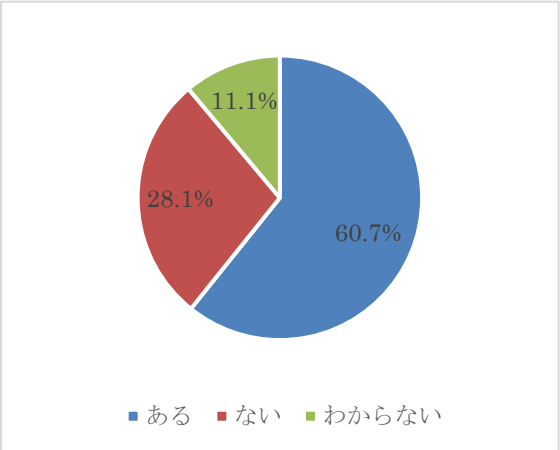
2022 年

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で、男女ともにシニア層の方が手口に詳しい。前回との比較では女性 20 代で「どれも知らない」の回答割合が増えた。

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？



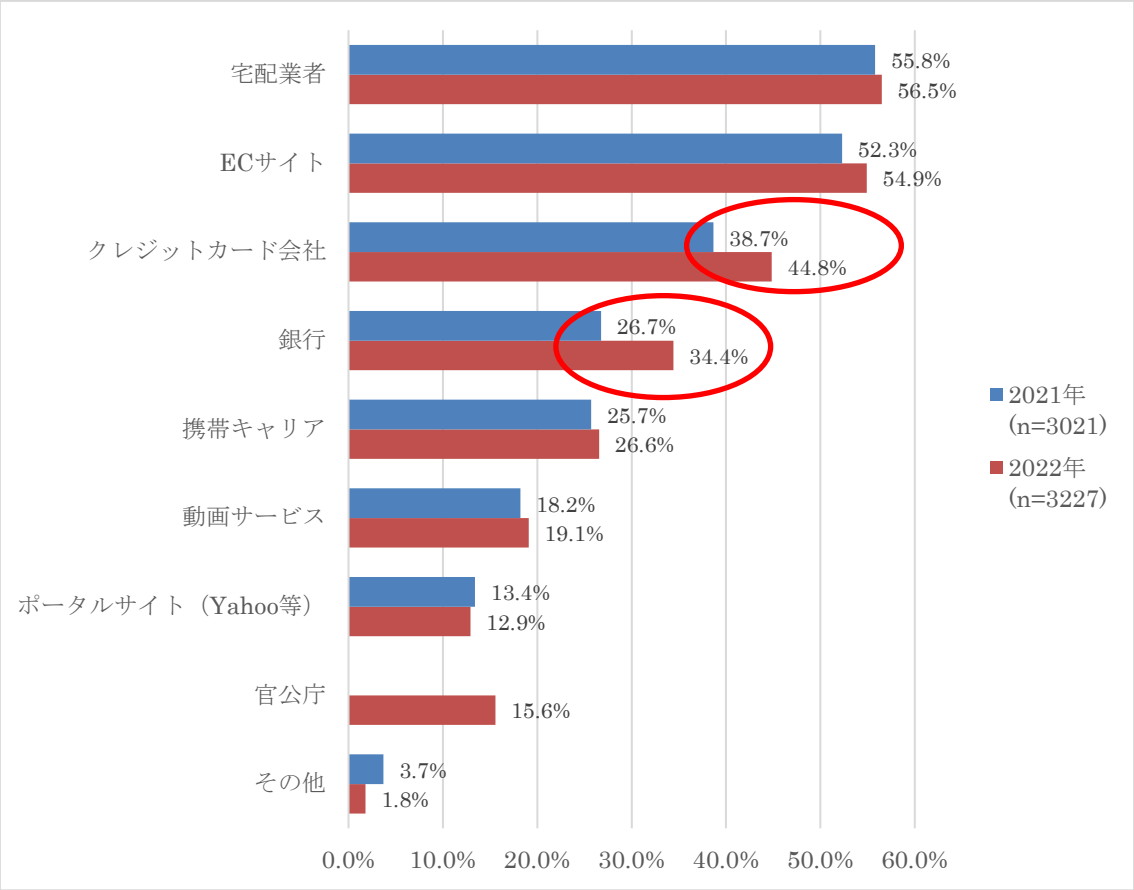
2021 年(n=5275)



2022 年(n=5313)

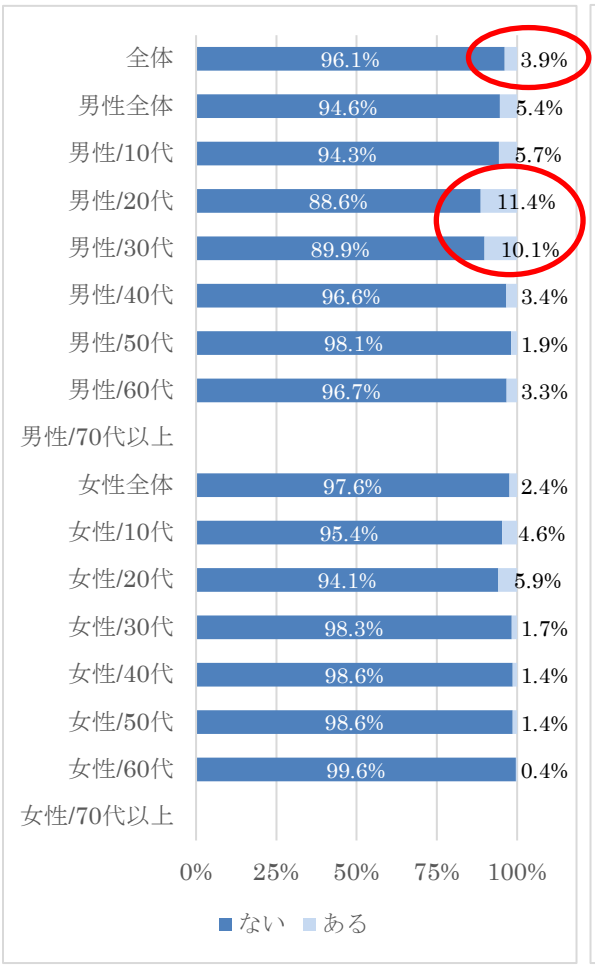
半数以上の方は受け取ったことがあると回答しており、前回調査より 3.4pt 増えている。SMS を用いたフィッシング詐欺は身近に迫るものとなっており、増加傾向にあることがうかがえる。

Q3. 何を装ったフィッシング詐欺でしたか？ ※複数回答可

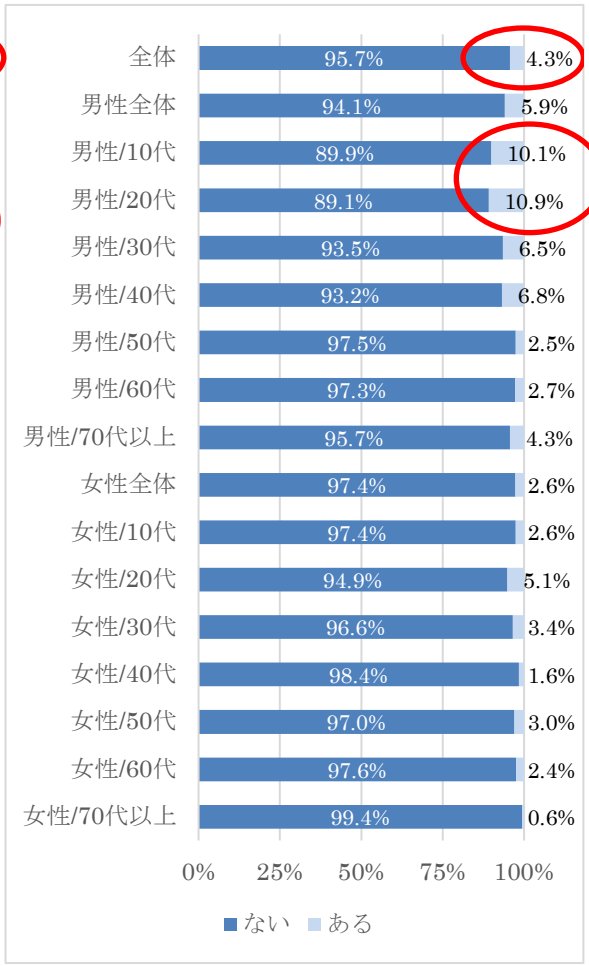


2022 年に国税庁をはじめとした官公庁を装ったフィッシング詐欺の報告が目立ったことから、今回より「官公庁」を項目として追加した。結果から「官公庁」と回答した割合は相対的には低いことがわかった。宅配業者や EC サイトなど消費者が日常的に利用する接点の多いサービスを装う手口の割合が多いのは、前回調査と同様だったが、銀行やクレジットカード会社を装う手口の増加率が大きい。攻撃者にとって、より直接的に金銭の詐取につながりやすい手口を用いる傾向が強くなっていると想定される。

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？



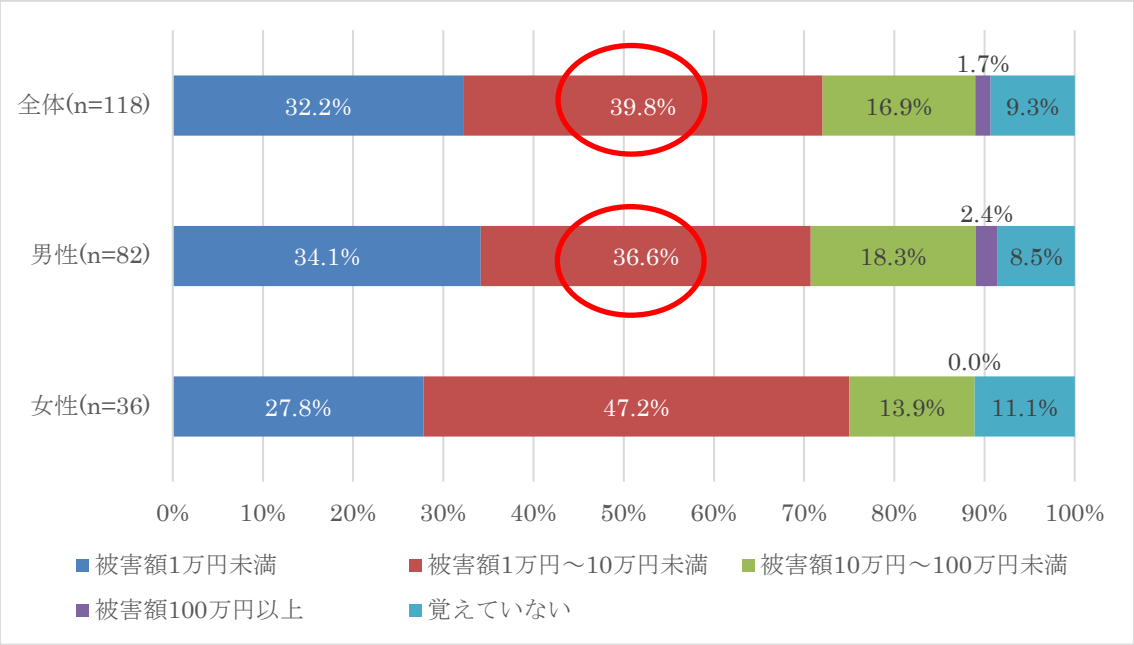
2021 年(n=3021)



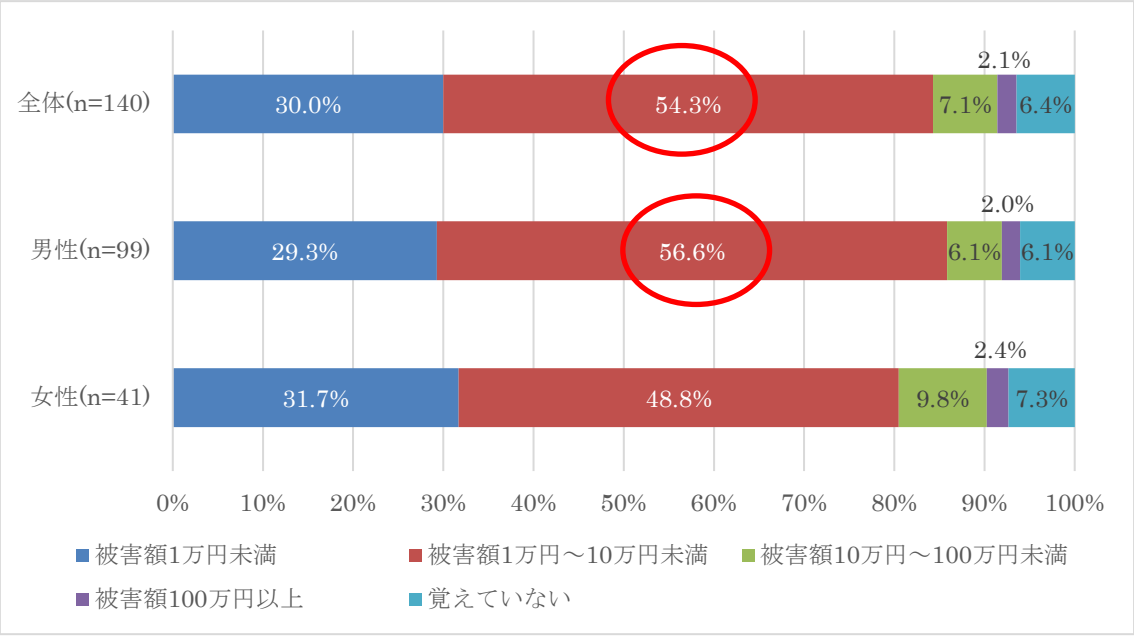
2022 年(n=3227)

前回の調査では全体で金銭的被害にあった方の割合は 3.9%のところ、今回は 4.3%と拡大傾向にある。前回の特徴的な点として、男性の 20 代、30 代は 10%超と全体の 2 倍以上多い点があった。今回は、男性の 30 代は 10%を下回る結果となり、男性の 10 代、20 代が 10%超と、一部に変化が見られた。2022 年 4 月より成人年齢の引き下げにより、18～19 歳が親権者の同意なしにクレジットカードなどの契約ができるようになったが、今後、このことによる被害増加も懸念される。属性として攻撃者のターゲットに選ばれやすい可能性があるため、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。



2021 年

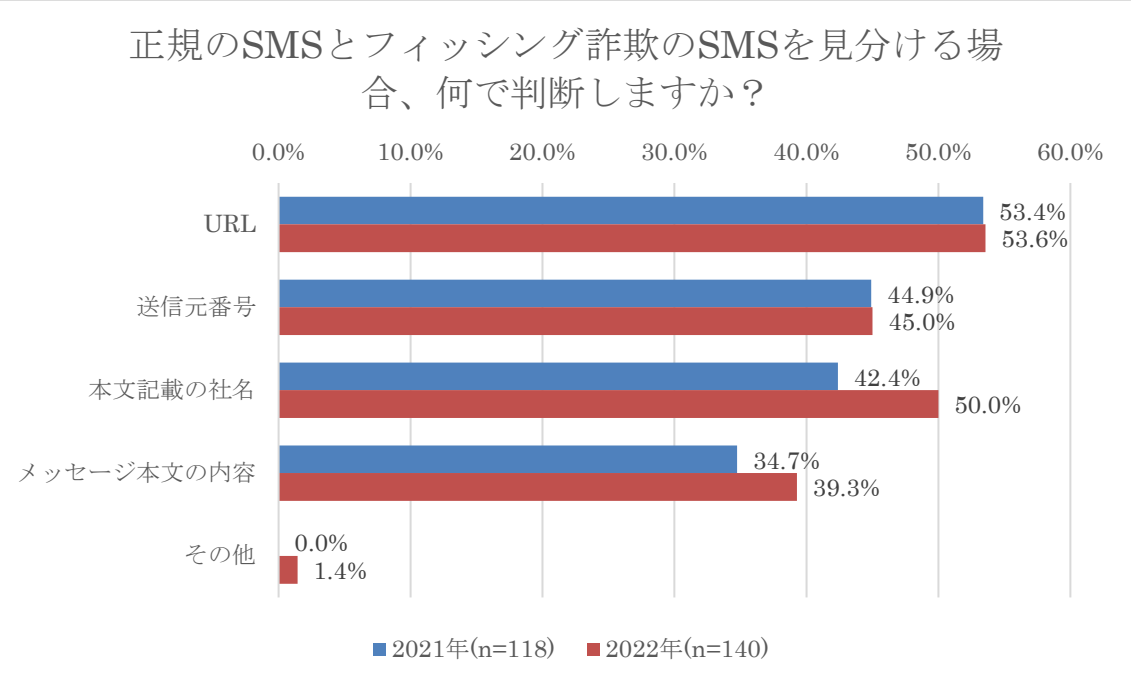


2022 年

前回の調査では、全体での「被害額 1 万円～10 万円未満」の割合が、39.8%

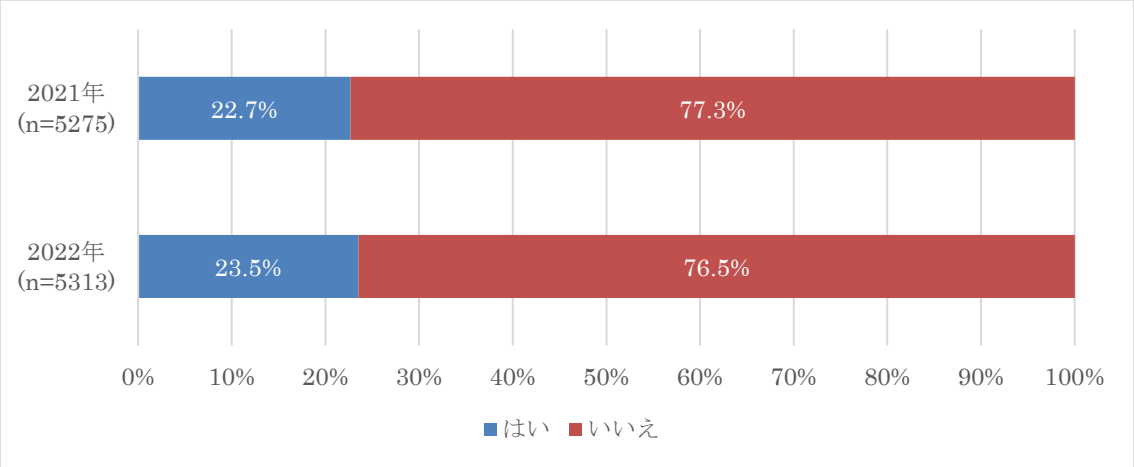
だったが、今回は 54.3%と 14.5pt 増えている。男性の「被害額 1 万円～10 万円未満」の割合が増えていることが影響している。今回の調査で最大額は 252 万円で 20 代の男性からの回答だった。

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



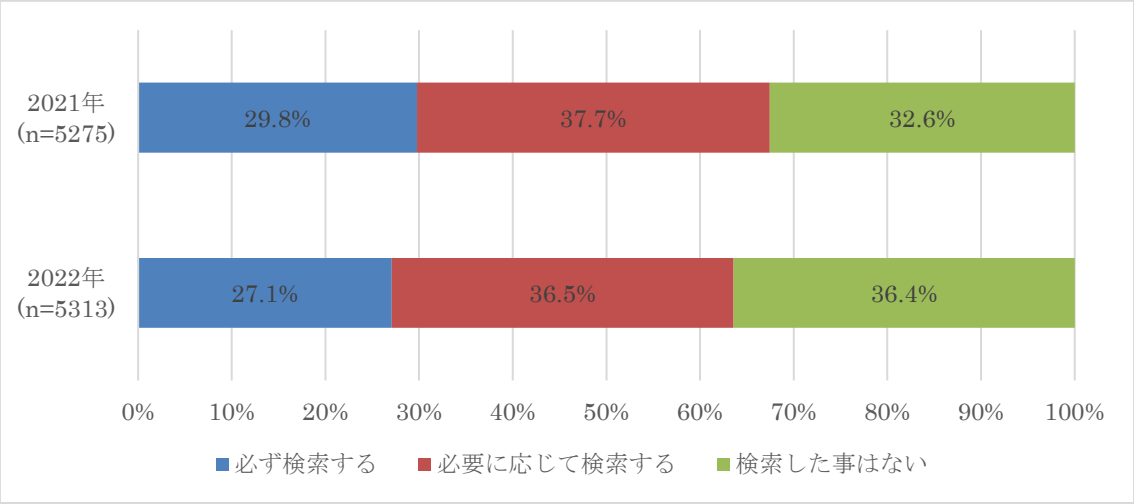
本文の記載内容だけでは正規の SMS とフィッシング詐欺の SMS を見分けることはできないが、URL や送信元番号は見分ける根拠となり得る。今回の調査では URL や送信元番号と回答した割合は前回とあまり変わらない一方、本文の記載の社名や内容で判断するという回答の割合が増加していた。

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)



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。前回調査から、若干改善しているものの、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 45%あり、一定程度注意が払われているようだったが、送信元がアルファベットの場合の危険性について、十分認知されていない状況と言える。送信元がアルファベットの場合の注意喚起をより一層行っていく必要がある。

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？



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」という回答が前回調査よりも 3.8pt 増加した。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、1 年前との比較によって傾向把握することができた。

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 60.7%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 4.3%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。SMS を利用したフィッシングでは、送信元をアルファベットで自由に表記できる国際網経由の SMS 配信を利用し、Web サイト運営者名をかたるケースが多い。送信元がアルファベットや海外電話番号の国際網経由と判断できる SMS についてはフィッシングの可能性を疑い、慎重に行動することが対策となる。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。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：2022/11/30 ～ 2022/12/02
有効回答者数：5,313 名
回答者の属性：
【性別】男性：50.0%　女性：50.0%
【年代】10 代：13.7%、20 代：14.8%、30 代：14.3%、40 代：14.7%、50 代：14.2%、60 代：14.5%、70 代以上：13.9%
※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】

5. フィッシングの対策

5.1. 最新の動向

5.1.1. フィッシングキットについて

フィッシング攻撃では、認知度の高い有名ブランドを装った偽サイトを用意し、被害者を偽サイトに誘導することで、個人情報の窃取やマルウェア感染などを行う。このような偽サイトを構築するには、専門的な知識が必要で偽サイトの構築にも時間がかかる。また、セキュリティ対策ソフトの検知を回避するために偽サイトの IP アドレスやドメインなどを頻繁に変更する必要もある。そのため、攻撃者は、「フィッシングキット」と呼ばれる、高度なスキルを必要とせず、簡単にフィッシングサイトを構築できるツールを利用する場合が多い。

「フィッシングキット」はダークウェブ上で販売されており、フィッシング攻撃に必要な各種機能を備えた高度なものから、偽サイトを ZIP 形式で圧縮した簡単なものまでさまざまである。

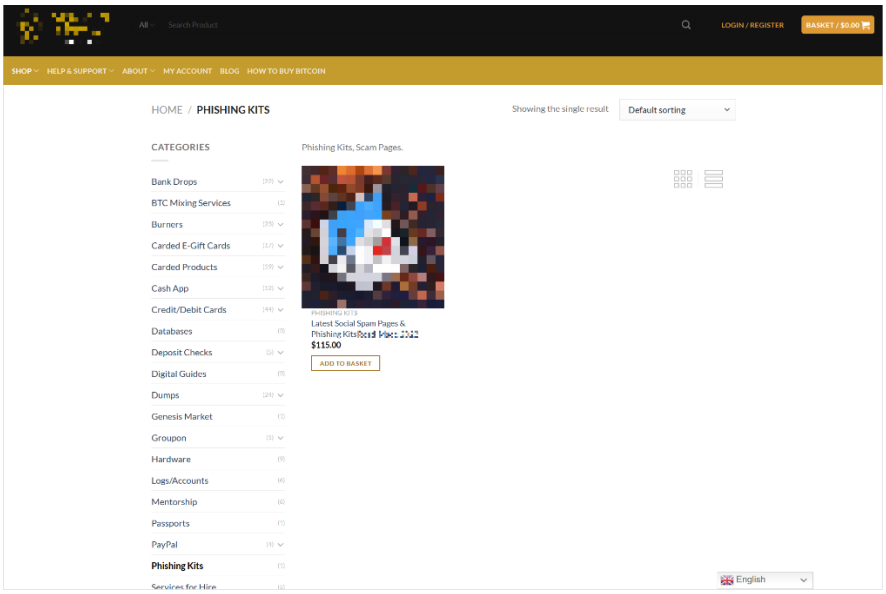


図 5-1　フィッシングキット販売サイト例

また、フィッシング攻撃に必要なツールなどをまとめサービスとして提供する PhaaS (Phishing as a Service)も広まってきており、フィッシング攻撃の参入障壁が下がってきている。

フィッシング攻撃で収集した情報は、ダークウェブ上で販売されており、

PhaaS の中には、フィッシング攻撃で収集した個人情報を売買できる機能を提供しているサービスもある。

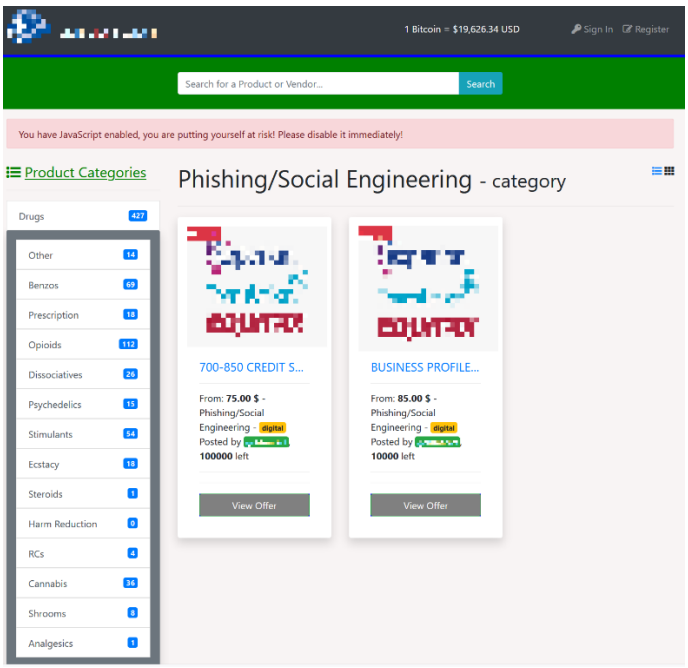


図 5-2　収集データ販売サイト例

　このようにプログラミングなどの特別な技術を必要とせず、比較的簡単にフィッシング攻撃を行うことができるフィッシングキットや PhaaS は、攻撃者にとって非常に魅力的である。これらの利用の広まりによりフィッシング攻撃が今後さらに増えていくことが見込まれており、フィッシング対策の重要性は増していく。個人利用者においては、このような脅威があることを認識し、各種対策を実施していく必要がある。また、事業者においては、「シフトレフト」[12]に着目し、利用者保護の強化につなげていく必要がある。

【長谷川 智久,村田 充昭　キヤノン IT ソリューションズ株式会社】

[12] フィッシング対策協議会、フィッシングレポート 2022（https://www.antiphishing.jp/report/phishing_report_2022.pdf）（閲覧日：2023 年 2 月 14 日）

5.1.2. 企業による認証テクノロジーの採用と普及に関して

IT サービスを提供する企業が、ユーザーを認証する場合の認証テクノロジーは、新旧さまざまな手段が存在するなかから費用対効果を踏まえて適宜選択し提供されている状況にある。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。最新のテクノロジーの一例としては、パスキー（Passkey）[13]が挙げられる。公開鍵暗号を用いてパスワードの漏えいリスクがなく、かつ UX としても優れた認証が、iOS/Android の該当バージョンのユーザー向けに、対応済みの IT サービスですでに利用可能となっている。

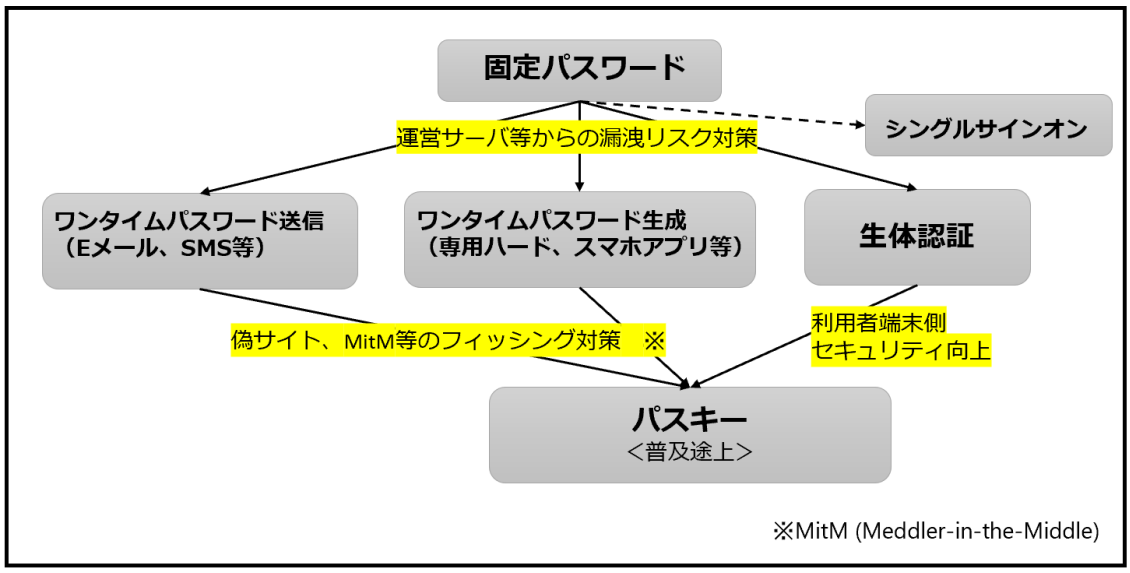


図 5-3　認証テクノロジーの変遷

その一方で、普及している IT サービスの提供企業にとっては、最新のテクノロジーにキャッチアップできないエンドユーザーへの対応も必要となることから、既存の方式も併存させることが必要であり、また場合によっては、導入コストなどの理由で最新テクノロジーの導入が先延ばしになる場合もある。そのため、既存方式のセキュリティリスクの改善は、最新テクノロジーの導入とあわせて必要とされている。

既存の方式のセキュリティリスクとしては、この数年、フィッシング SMS・E メールから被害者を偽サイトに誘導し必要な情報を入力させて、それを用いて

[13] 日経クロステック、ニュース解説「iOS や Android に相次ぎ搭載、「パスキー」はパスワードレス普及の切り札になるか」（https://xtech.nikkei.com/atcl/nxt/column/18/00001/07497/）（閲覧日：2023 年 2 月 14 日）

加害者が正規サイトにログインするというケースがある。IT リテラシーの高いエンドユーザーは、偽サイトの URL やメッセージの送信元から疑うことは可能ではあるが、IT リテラシーの高くないエンドユーザーの被害は依然として存在している。

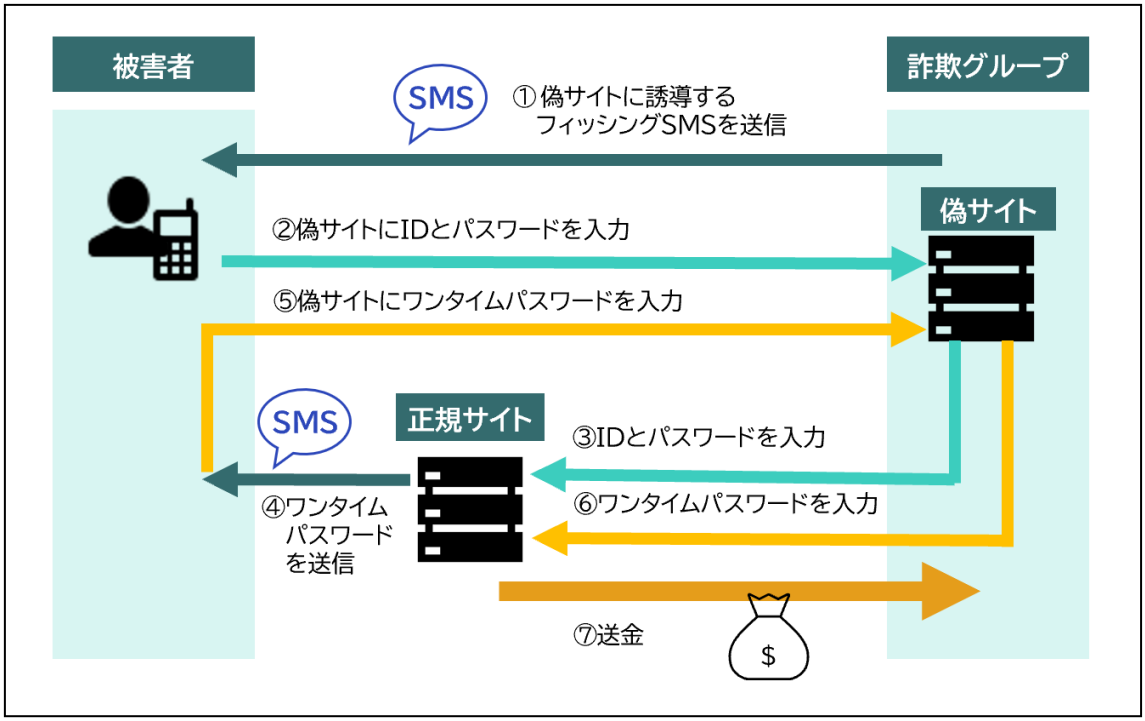


図 5-4　SMS から偽サイトに誘導した不正送金の流れ

この問題の背景としては、スマホアプリにおいては過去に Android OS では、ユーザーがパーミッションさえ与えれば、あらゆるアプリがユーザーが受信したすべての SMS を参照できる API が提供されており（現在は提供終了）、それを悪用してユーザーの個人情報を取得するアプリが数多く市場に出回ったことから、「手作業での入力」がスマホアプリの二段階認証ではスタンダートな UX となった時期があるため、「手作業での入力」において偽サイトが介在する余地を与えている。

一方、その後、Apple/Google は該当の正当なスマホアプリだけが、必要な SMS 内のワンタイムパスワードを参照・自動入力できる仕組みを、2018 年以降提供している。[14]　2021 年にはスマホブラウザー上で、対象サイトのドメインが正しい場合のみに当該 Web ページに SMS で受け取ったワンタイムパスワ

[14] フィッシング対策協議会、フィッシングレポート　2021　3.2.1 章（https://www.antiphishing.jp/report/phishing_report_2021.pdf）（閲覧日：2023 年 2 月 14 日）

ードを自動入力できる WebOTP も利用可能となっているものの、それらを活用できているのは一部の企業に留まる。

自動入力の仕組みは自社で技術調査・開発する代わりに、サードパーティーのサービスの活用も可能である。具体的には、SMS でワンタイムパスワードを送付する場合に、ランダムにパスワードを生成して、エンドユーザーが入力後に認証する機能について、Twilio 社の Authy、Vonage 社の Verify API、アクリート社の認証 API[15]などを利用すると、その IT サービスにおいては、スマホアプリおよびスマホブラウザーにおける自動入力に対応可能となる。下記図 5-5 が認証 API を用いて送信される SMS の例である。自動入力の可否だけではなく、認証コードの桁数や有効期限などのセキュリティに関する他の項目も簡易なパラメーターで設定可能となっているため、現在自動入力に対応できていない企業には、このようなサードパーティーのサービス活用が推奨される。

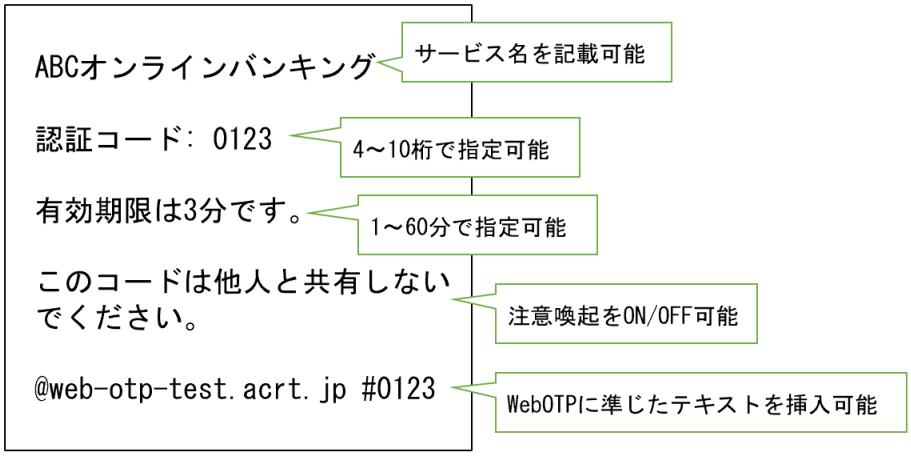


図 5-5　アクリート社認証 API にて送信される SMS の例

[15] 株式会社アクリート、選ばれる理由（https://www.accrete-inc.com/reason/）（閲覧日：2023 年 2 月 14 日）※認証 SMS 配信機能、および認証コード検証機能を提供。利用企業が図 5-5 のようなメッセージを送信することが可能。

図 5-6　アクリート社認証 API による Chrome および Safari での自動認証の例

【田中 優成,浦田 泰裕　株式会社アクリート】

5.1.3. フィッシングメールを利用者に届けないための事前対策　DMARC の reject 設定

協議会の調査用メールアドレス宛に届いたフィッシングメールのうち、約85.7%がメール差出人に実在するサービスのアドレス（ドメイン）が使用された「なりすまし」フィッシングメールであり、多い状況が続いている。

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。フィッシングメールは「誘導」に該当し、次にフィッシングサイトなどで情報が盗まれる「詐取」段階につながるため、フィッシングメールの対策は、情報が盗まれる前段階の対策として大変重要である。

実在するアドレスをなりすましたフィッシングメールを利用者に届かなくする対策に DMARC がある。DMARC は、送信ドメイン認証技術の SPF や DKIM を補強する技術であり、なりすましメールで発生する SPF、DKIM の認証失敗状況から、そのメールを利用者に届く前に、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。

DMARC の「メールの受信制御ポリシー」は、1.そのまま受信させる（none）、2.隔離させる（quarantine）、3.受信を拒否する（reject）から選択することができる。フィッシング被害に遭った事業者のみならず、なりすましメールの対策として DMARC のポリシー “reject”の設定を進めることが重要である。DMARC のポリシー宣言は、監視モード（1.そのまま受信させる（none））から開始し、取得した DMARC レポートから自ドメインのなりすまし状況を把握することが重要である。レポートでは業務で使用しているクラウドサービスから配信される自ドメインを使ったメールが、SPF や DKIM の設定不備により、なりすましメールとレポートされる場合がある。DMARC レポートから正規に使用しているサーバーやクラウドサービスからの配信を精査し、その完了をもって DMARC のポリシー “reject”の設定に進むことが望ましい。

【加藤 孝浩　トッパン・フォームズ株式会社】

5.1.4. フィッシング詐欺の収益化を阻止する対策　クレジット決済の本人確認、複数認証義務化を検討

フィッシング詐欺で詐取されたクレジットカード情報は、本人になりすまして悪用され、不正な物品購入などによる「収益化」に使われる。この「収益化」段階の対策として、経済産業省は 2022 年 10 月にクレジットカード番号等不正利用対策の強化として、クレジット決済の本人確認、複数認証の義務付けの検討を発表している。本人確認、複数認証では、認証規格「EMV-3D セキュア」が検討されており、現在のセキュリティコード・静的パスワードなどによる認証から、非対面取引における本人認証の原則化と、生体認証・ワンタイムパスワードなどといった強力な本人認証方法が検討されている。

【加藤 孝浩　トッパン・フォームズ株式会社】

5.1.5. フィッシングメール情報の利用者周知方法について

フィッシングの手口が高度化して判別が難しくなり、被害も増加している。こうした状況において、システムによる防御だけでは被害を防ぐことは困難であり、フィッシングが発生した際にタイムリーに利用者に通知して注意喚起を行うことは、重要な対策の一つになっている。

利用者通知の目的は、フィッシング詐欺の存在を伝えて、脅威を認識してもらうことで、慎重な行動を促すことである。通知を届けたい相手は、フィッシング詐欺の対象となるサービスの一般利用者で、必ずしも IT に詳しかったり、特別な関心を持っているとは限らない。そこで、通知を効果的に行うために留意する点を３つにまとめた。

１．フィッシング発生時の対応を決めておく

- ✓ 発見した場合に取るべき対処をあらかじめ準備して、発見後に迅速な対応が取れるようにする。
- ✓ 詐欺の手口は短時間で変わることが多いので、準備が大切となる。

２．より多くの利用者に届く方法で発信する

- ✓ できるだけ多くの利用者に通知を届けるため、複数のメディアを活用する。
- ✓ ホームページだけではなく、Twitter、SNS など複数の方法を合わせることで、利用者が通知を認識する機会が増える。

３．わかりやすさを重視する

- ✓ 通知内容を簡潔で分かりやすいメッセージにする。
- ✓ 利用者にどんな内容が届くかを具体的に示すことで、被害軽減につなげることができる。

フィッシング対策ワークショップでは、利用者通知において推奨すること、逆にすべきでないことの声を集め、集約して意見を事業者ガイドラインに反映している。

【塚田 晴史,鈴木 一実　株式会社マクニカ】

5.1.6. FIDO とフィッシング耐性への期待

パスワード認証の要件や管理の煩雑化が課題としてあげられるようになり、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。中でも FIDO(Fast IDentity Online)と呼ばれるオンライン認証の仕様が多くのシステムで使用されている。FIDO を使用するとスマートフォンなどの生体認証を使用して個人認証を行うことができる。FIDO を使用することにより、パスワードリスト攻撃やフィッシング詐欺の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がやり取りされているため、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 5-7）。

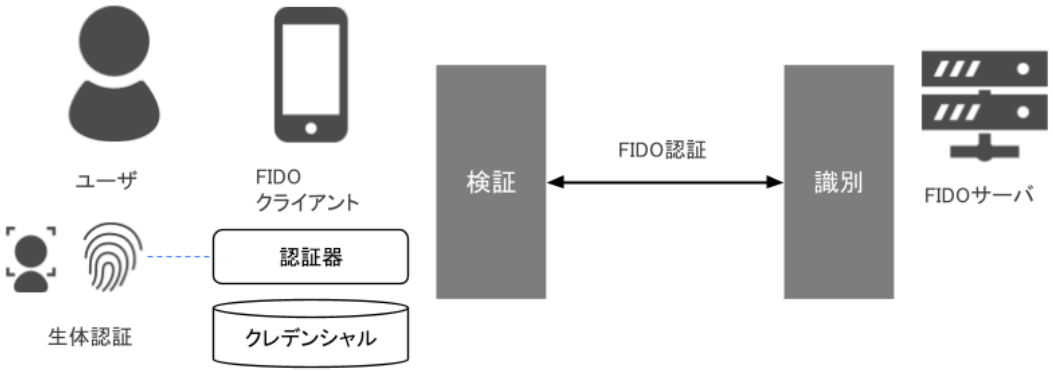


図 5-7　FIDO の認証モデル

初期の FIDO 認証では仕様に準拠したハードウェアトークンなどの認証器や、スマートフォン OS のアプリケーションなどを使用することが必要だったが、FIDO2 として新たに策定された仕様では、WebAuthn (Web Authentication API)をサポートしたブラウザーを使用することで FIDO 認証を行うことができるようになった。FIDO2 は Microsoft Edge、Google Chrome、Firefox などの大手ブラウザーや、Touch ID、Face ID などのさまざまなデバイスで FIDO2 認証がサポートされ、すでに国内のサイトにおいてサポートが開始されている。

FIDO のセキュリティレベルを保ったまま利便性の向上も継続して検討されている。FIDO アライアンスでは従来の FIDO の仕様から、マルチデバイス対応 FIDO 認証資格情報（マルチデバイス FIDO クレデンシャル）という機能のアップデート（図 5-8）を行い、本アップデートにより次の変更点があると解説している。

- ユーザーの携帯電話（FIDO 認証器となる）と、ユーザーが認証を行おうとしているデバイスとの間で通信するためのプロトコルを定義し、携帯電話をローミング認証器として使用できるようにすること。
- FIDO 認証資格情報をユーザーのすべてのデバイスで広く利用できるようにし、デバイスの紛失に耐えられるようにし、異なるデバイス間でも同期できるようにすること。

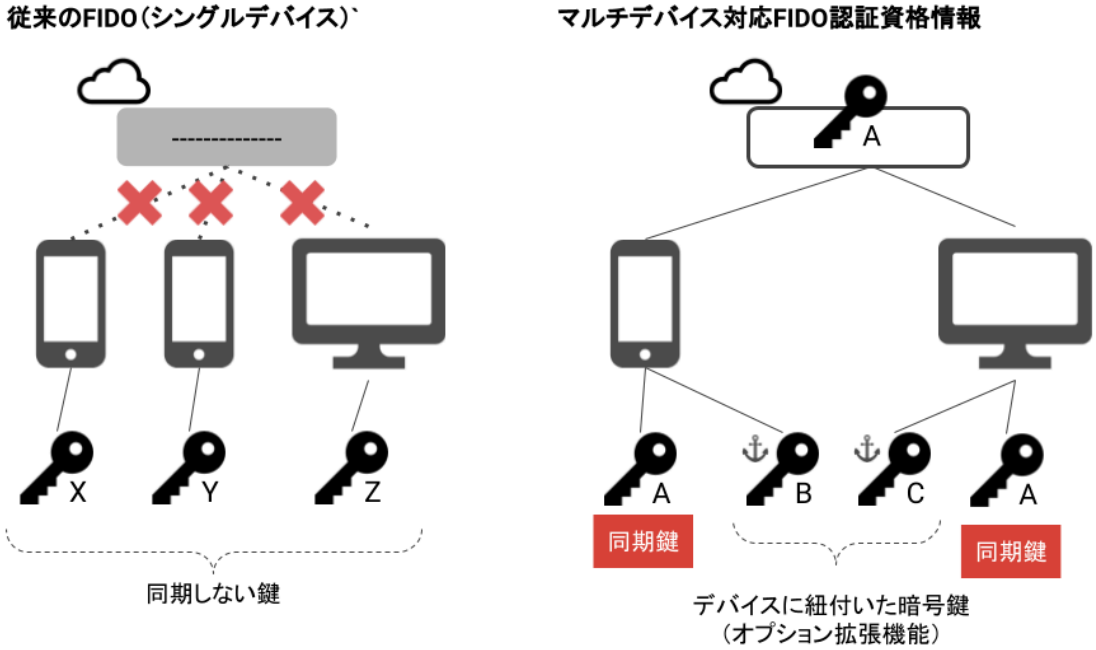


図 5-8　マルチデバイス対応 FIDO 認証資格情報

各ベンダーも実装が進んでおり、例えば Apple 社では「パスキー」という名前で発表し、 iCloud のアカウントと連携し、複数端末にて FIDO のクレデンシャルを扱うようにしている。

パスワードレス認証の普及を加速させる取り組み
https://fidoalliance.org/charting-an-accelerated-path-forward-for-passwordless-authentication-adoption-jp/?lang=ja

さまざまなユースケースへの FIDO の対応に向けて （国際版の日本語訳）（PDF）
https://media.fidoalliance.org/wp-

content/uploads/2022/04/%EF%BC%88%E5%9B%BD%E9%9A%9B%E7%89%88%E3%81%AE%E6%97%A5%E6%9C%AC%E8%AA%9E%E8%A8%B3%EF%BC%89How-FIDO-Addresses-a-Full-Range-of-Use-Cases-rF2.pdf

【松本 悦宜　Capy 株式会社】

5.2. ドメイン関連

5.2.1. 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 [16]」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、外部の CDN サービスや Web サービスを利用し、自分のドメイン名にサブドメインを設定して期間限定の Web サイトを運用する場合、利用を終えた

[16]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。

サブドメインを第三者に勝手に使われる「サブドメインテイクオーバー」[17] を防ぐため、利用開始時に設定した DNS レコード（CNANE・A/AAAA）を利用終了時に忘れずに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、と思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 [18]。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問い合わせて欲しい。

【遠藤 淳　株式会社日本レジストリサービス】

[17] CDN サービスや Web サービスの利用開始時に設定したサブドメインの DNS 設定が残ったままになっていることを利用し、管理権限を持たない第三者がそのサブドメインの乗っ取り（テイクオーバー）を図る攻撃手法。

[18] 株式会社日本レジストリサービス、「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：2023 年 2 月 14 日）

5.2.2. 悪用されたドメインの対応について

悪用されたドメインに対しては、多くのケースでは Web サイトやメールサーバーなどのコンテンツやサーバーのレベルでの対応が考えられるが、ドメイン名での対応も可能である。このドメイン名の対応は ICANN（Internet Corporation for Assigned Names and Numbers）によって制定された UDRP（Uniform Domain Name Dispute Resolution Policy／ドメイン名紛争処理方針）に沿って対応がなされ、権利者からの申立てに基づいて、ドメイン名の取り消しや移転を行う仕組みである。

この UDRP は悪用されたドメイン名が社名やブランド名と一致するようなケースに適用される。UDRP 処理方針によれば、紛争処理手続は、ドメイン名が悪意をもって登録されている疑いのある紛争についてのみ利用することができる。（詳しくは参考 URL①参照）

例えば、社名が「Example 株式会社」、公式 URL が「www.example.jp」で、悪用ドメインが「example.***（TLD が異なるドメイン）」の場合、UDRP の申立てが可能となる。ただし、UDRP はすべての TLD を網羅しているのではなく、gTLD と一部の ccTLD が対象である。JP ドメイン名については JPNIC が JP-DRP（JP ドメイン名紛争処理方針）を制定している。なお、すべての TLD において、UDRP 等ではなく、訴訟の提起によって解決を図る道を選択することもできる。

この UDRP はドメイン名がブランド名や社名など権利を保有している場合に、手続きが有効となるため、ドメイン名の侵害対応の一つのオプションとして考慮する余地がある。

参考 URL

① WIPO、WIPO によるドメイン名紛争統一処理方針（処理方針）についてのガイド
https://www.wipo.int/amc/ja/domains/guide/

② JPNIC、ドメイン名紛争処理方針（DRP）
https://www.nic.ad.jp/ja/drp/

【加藤 恭久　GMO ブランドセキュリティ株式会社】

■ コラム 標的型フィッシングメール教育に関する課題と今後の展開

フィッシングメールの中でも検知が最も困難とされる標的型フィッシングメールへの対策の１つに、教育がある。標的型フィッシングメールとは、組織を対象とした標的型攻撃の最初のステップで従業員に送りつけられるメールを指すことが多い。メールにはマルウェアを含むファイルが添付されていたり、悪意のある接続先へのリンクが本文中に挿入されていたりする。これに対して従業員への教育では、添付ファイルを開く、また、リンクをクリックする（以後、「反応する」という）ことへの注意を喚起する。また、差出人アドレスのドメインをよく見るなど、フィッシングメールを見抜くための手がかりを教えることも多い。加えて、標的型攻撃訓練を実施する組織も増加している[1]。この訓練では、情報システム担当部署などが標的型フィッシングメールに関する知識を提供した後、各従業員に標的型フィッシングメールを模した訓練用のメールを送付する（このメールに反応した従業員に対し、さらなる教育を提供することもある）。従業員が教えられた知識を活用できるかについて評価し、また、従業員の攻撃に対する意識を高めることを目的とする。

しかし、学術研究によっては、標的型攻撃訓練を含む、従来の教育の効果が不十分であることが示唆されている。訓練において多くの従業員は訓練用メールに反応しないが、反応する従業員も、一定数存在する。前者の反応しなかった従業員については、習得した知識を活用したことによるケースもあると考えられる。この点では教育の効果があると推測される。一方、後者、反応した従業員について教育の効果があるなら、この後に届く訓練用メールには反応しないだろう。訓練用メールに反応したことを伝えれば、彼らはメールへの警戒心をそれまで以上に高め、知識を活用するようになると期待される。この期待に反し、訓練用メールに反応した従業員が、その後も同様の訓練用メールに繰り返し反応するという報告は少なくない[例えば2]。

そこで研究者の中では、従来の教育の改善が必要であるという認識が共有されつつある。例えば、メールと自身との関連性を適切に判断する力をいかに伸ばすかという課題が挙げられる。精巧に作成された訓練用メールに反応する従業員と反応しない従業員との違いの 1 つは、そのメールが自身に関連しているかについての判断の適切性にある[3]。この判断は、メールの文脈や内容のほか、本人の性格や経験、価値観などによって左右される。言い換えれば、一般化して教えることが難しい部分である。現状、我々は「メールが自身に関連があるものか、よく考える」といった注意喚起しかできて

いない。一方、この適切に判断する力を伸ばすことができれば、標的型フィッシングメールの検知精度を構造的に向上させることができるかもしれない。すなわち、各従業員が反応しない確率を高めるというだけでなく、スイスチーズモデルにおけるリスク低減が期待できる。スイスチーズモデルとは、視点やアプローチの異なる対策を組み合わせて実施することによる多層防御のモデルである（情報セキュリティの文脈では入口・内部・出口対策のことのみを指す場合もあるようだが、元々の safety に関する文脈[4]では上述の考え方を指す）。自身との関連性という、技術的な検知基準とは異なる視点によってメールが検証される機会を増加させることは、検知の多層化につながる。

もちろん、教育によって全ての従業員がいかなる標的型フィッシングメールも検知する、および、このメールに反応しないよう目指すことは現実的ではない。そのために従業員が当該メールに反応した場合のレジリエンスも重要である。しかし、システム内での攻撃が始まることの予防、すなわち、標的型フィッシングメールの検知が防御の基本であることは疑いようがない。また、このメールの検知については技術的な対策の限界も指摘されており、従業員による検知や適切な対応が鍵を握る[5]。この確実性を今以上に高めるための教育について明らかにすることは、研究業界にとっての急務であると筆者は考えている。

引用文献

[1] 日本シーサート協議会(2022)『メール訓練手引書一般公開版(ver.1.0)』

[2] Caputo, D.D. et al.(2014)”Going spear phishing: Exploring embedded training and awareness” IEEE Security & Privacy.

[3] Greene, K. K. et al.(2018)”User context: An explanatory variable in phishing susceptibility” NDSS Symposium.

[4] リーズン(2014)『ヒューマンエラー 完訳版』海文堂出版

[5] フィッシング対策協議会(2022)『フィッシング対策ガイドライン 2022 年度版』

【稲葉緑　情報セキュリティ大学院大学】

6. 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、引き続きフィッシングは増加傾向である。金融機関へのフィッシングの対象も従来の銀行だけでなく、保険会社の契約者貸付を狙ったと思われるフィッシングも出現した。フィッシングの注意喚起もかなり行われているにもかかわらず、ユーザーはフィッシングのメッセージに相変わらず騙されており、周知方法についても工夫が必要と考えられる。

技術的な対策では、「最新の動向」で紹介しているように新しい認証である FIDO の利便性が向上する技術が進んだ。しかし新しい技術は中小のサービス提供事業者にとっては、導入にハードルがあるが、サードパーティーによるサービスの提供によって容易に導入できることを期待したい。

企業によるドメインの管理については、引き続き問題が存在している。2022 年もサービス提供事業者が廃止したドメイン名が悪用されるケースが確認された。企業にとってインターネットでのビジネスの重要性が上がっている現在、ドメイン名はコーポレート・アイデンティティのイメージ形成の重要な要素と考えられるが、現状では、容易な取得や廃棄がみられる。

被害は増えておらず、一時落ち着いた銀行のフィッシングによる被害も 2022 年 8 月にまた増加した。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。

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と思う。

【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】

林 憲明	トレンドマイクロ株式会社
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
松本 悦宜	Capy 株式会社
加藤 恭久	GMO ブランドセキュリティ株式会社
加藤 孝浩	TOPPAN エッジ株式会社
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
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
熊沢 明生	ソフトバンク株式会社
長谷川 智久	キヤノン IT ソリューションズ株式会社
村田 充昭	キヤノン IT ソリューションズ株式会社
塚田 晴史	株式会社マクニカ
鈴木 一実	株式会社マクニカ
大川 哲	株式会社ボーグテクノロジー
崎山 康平	株式会社 ranryu
大野 真理	株式会社 ranryu
大谷 なすか	合同会社 DMM.com
寺西 一平	合同会社 DMM.com
沖 真也	NRI セキュアテクノロジーズ株式会社
大塚 淳平	NRI セキュアテクノロジーズ株式会社
平塚 伸世	一般社団法人 JPCERT コーディネーションセンター

【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）