**デジタル署名者** : Council of Anti-Phishing Japan
DN : c=JP, st=Tokyo, l=Chuo, serialNumber=AATL20241016370915, o=Council of Anti-Phishing Japan, cn=Council of Anti-Phishing Japan, email=antiphishing-sec@jpcert.or.jp
**日付** : 2025.06.03 14:38:52 +09'00'

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 2025

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

1.1 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 フィッシングで使用された多様な手法 ..... 7
1.3.3 「なりすまし」送信メールの状況について ..... 8

2. WG の活動 ..... 9

2.1 今年度の WG 活動 ..... 9
2.2 フィッシング対策協議会　各 WG の活動 ..... 10
◆被害状況共有 WG＜主査：角谷 沙歩子氏（株式会社マクニカ）＞ ..... 10
◆認証方法調査・推進 WG＜主査：加藤孝浩氏（TOPPAN エッジ株式会社）＞ ..... 12
◆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）＞ ..... 12
◆STC 普及啓発 WG＜主査：林 憲明氏（トレンドマイクロ株式会社）＞ ..... 13
◆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）＞ ..... 13
◆詐欺サイト対処机上演習タスクフォース＜主査：林 憲明氏（トレンドマイクロ株式会社）＞ 14

3. フィッシングの被害 ..... 15

3.1 QR コードを悪用したフィッシングメール ..... 15

4. SMS を用いたフィッシング詐欺についての意識調査 ..... 16

5. ドメイン名関連 ..... 26

5.1 ドメイン名の廃止・利用終了にあたっての注意 ..... 26
5.1.1 ドメイン名廃止のリスク ..... 26
5.1.2 ドメイン名を廃止する前に注意して欲しいこと ..... 26
5.1.3 ドメイン名の管理ルール・手順の確立 ..... 27
5.1.4 誤ってドメイン名を廃止してしまった場合の対処 ..... 27
5.1.5 自組織のサブドメインを利用終了する際の注意 ..... 27

6. トピック ..... 28

6.1 送信ドメイン認証技術 DMARC 導入ガイドラインの公開について ..... 28
6.2 送信ドメイン認証技術「DMARC」の導入状況について ..... 29
6.3 NIST SP 800-63 と PCIDSS 4.0 のパスワード要求事項の違いについて ..... 31

6.4 パスワードマネージャーの利用について ..... 34
6.4.1 利点 ..... 34
6.4.2 サービス提供者側にとっての要検討事項 ..... 34
6.4.3 考察 ..... 34
6.5 進化したワンタイムパスワード ..... 36
6.5.1 SMS OTP の国防上の必要性 ..... 36
6.5.2 リアルタイム・フィッシング攻撃対策技術：Unicode OTP ..... 36
6.6 パスキーとフィッシング耐性 ..... 38
6.6.1 パスキーはパスワード不要の便利な認証方式 ..... 38
6.6.2 パスキーとフィッシング耐性について ..... 39
6.6.3 パスキーの浸透状況 ..... 39
7. まとめ ..... 41

本レポートの改定および公開は、一般社団法人 JPCERT コーディネーションセンターが経済産業省より委託を受けた「サイバー攻撃等国際連携対応調整事業」の一環として実施したものです。

# 1. フィッシングの動向

## 1.1 国内の状況

警察庁の発表[1]によれば、2024 年上半期は、サイバー攻撃の前兆ともなる脆弱性探索行為等の不審なアクセス件数およびランサムウェアの被害報告件数が前年同期から増加しました。また、フィッシング報告件数は前年同期比で約 10 万件増加し、不正送金被害総額についても前年同期比で減少しているものの、未だ高水準で推移しています。

警察によるサイバー事案の検挙件数は、1,396 件であり、2023 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 190 件（前年同期比で 1.1%増加）でした。このうち 170 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ます。

フィッシング情報の届け出件数について、2024 年は特に下期において前年と比較して著しく増加しました（図 1-1）。キャッシュレス決済サービス、クレジットカード会社のほか、消費者金融、交通系サービス等のなりすましが報告されています。

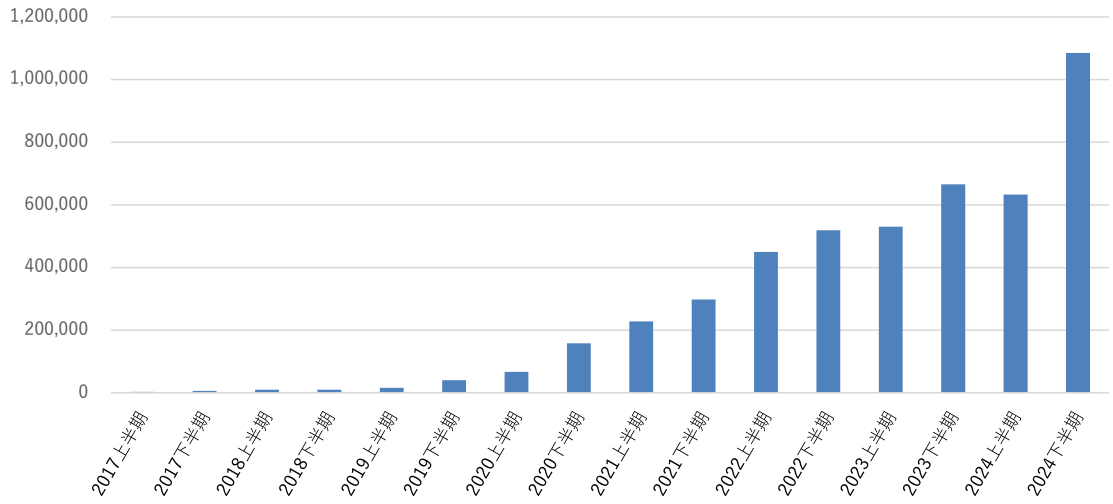



図 1-1 国内のフィッシング情報の届け出件数[2]

フィッシングサイトの URL 件数は、2024 年は上半期・下半期とも 2023 年より著しく増加しており、全体的にも増加傾向が続いています。（図 1-2）。ブランド名を悪

1 警察庁、令和 6 年上半期における サイバー空間をめぐる脅威の情勢等について（https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf）（閲覧日：2025 年 2 月 12 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：2025 年 2 月 12 日）より作成

用された企業の件数は、2023 年下期以降で若干の減少傾向がみられたものの、2024 年下期以降再び増加しています（図 1-3）。

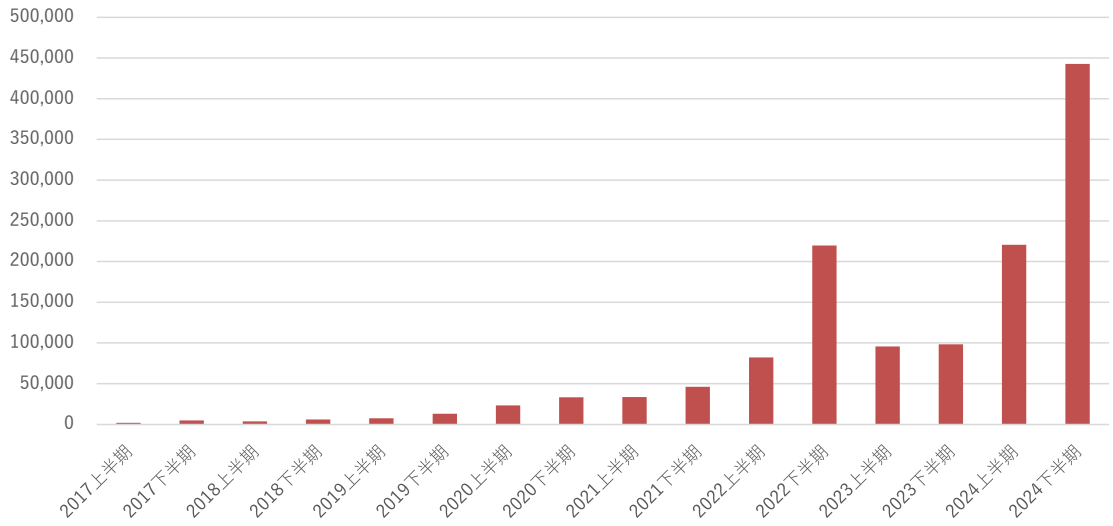



図 1-2　国内のフィッシングサイトの件数


図 1-3　国内のブランド名を悪用された企業の件数

また、警察庁・総務省・経済産業省の発表[3]によれば、2023 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 2022 年と同程度であした（図 1-4）。2023 年の手口別内訳では、2022 年に比べ

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/000935209.pdf）

て、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は減少し、識別符号を知り得る立場にあった元従業員や知人等による犯行が増加しました（図 1-5）。

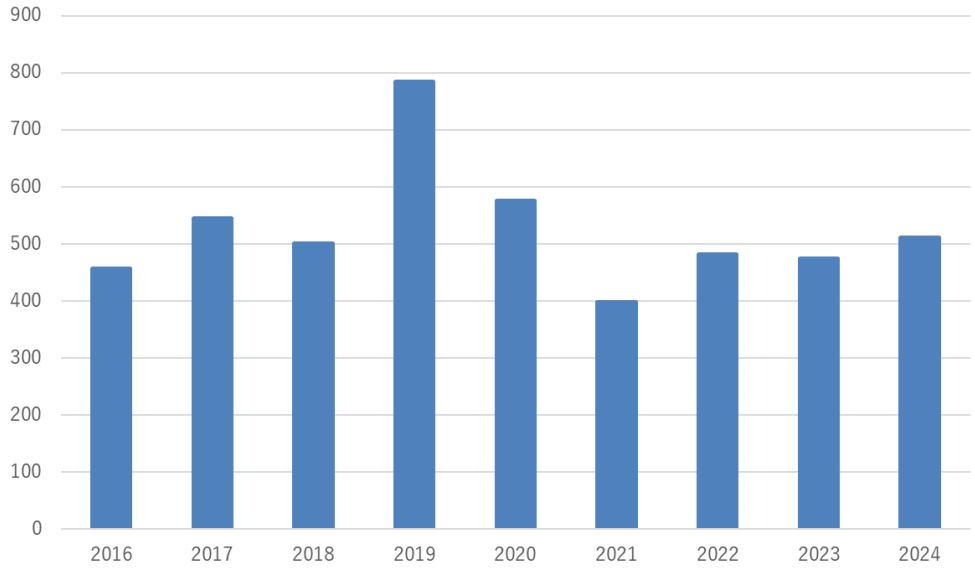



図 1-4　識別符号窃用（ID 窃盗）型不正アクセス行為の検挙件数[4]

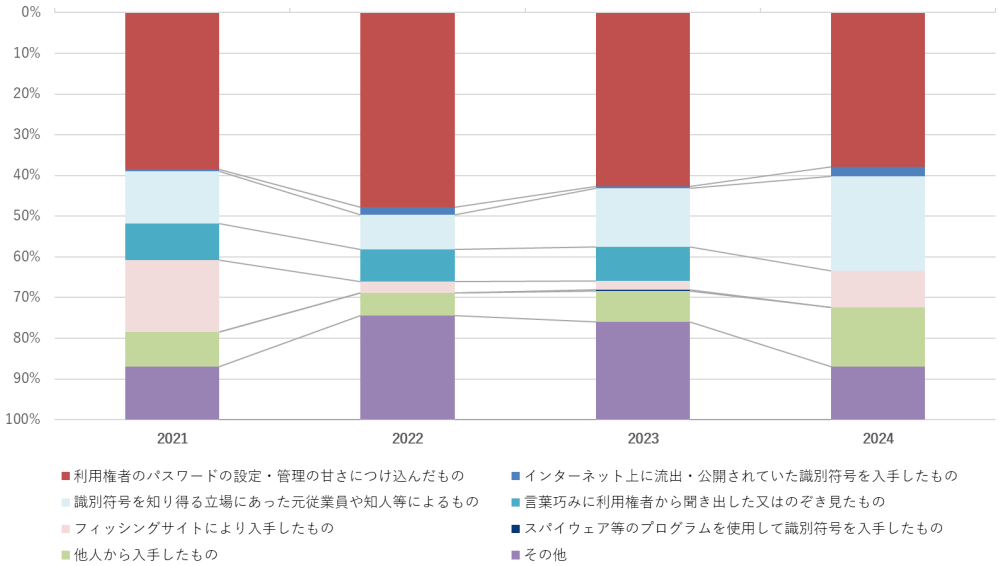



図 1-5　識別符号窃用型不正アクセス行為の手口別検挙件数の内訳
（2021 年～2024 年）[5]

【みずほリサーチ＆テクノロジーズ株式会社】

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、半期毎のフィッシング届け出件数は、2020 年下半期をピークに減少していましたが 2022 年下半期に増加しました。2022 年下半期以降は減少傾向にあるものの、下げ止まりの状況となっています。2024 年上半期のフィッシング届け出件数は 2023 年上半期と同程度となりました（図 1-6）。フィッシングサイトの件数は、2023 年上半期をピークに減少傾向となっています（図 1-7）。フィッシングによるブランド名の悪用の件数は 2023 年に入ってから減少傾向にありますが、2024 年は同水準で推移しており、下げ止まりの状況となっています（図 1-8）。APWG の報告[6]によると、ソーシャルメディア・プラットフォームは最も頻繁に攻撃されたセクターであり、2024 年第 3 四半期にはフィッシング攻撃全体の 30.5%が標的となったことが報告されています。また、SMS やテキストメッセージで宣伝されるフィッシングであるスミッシングは、前四半期から 22%以上増加しました。

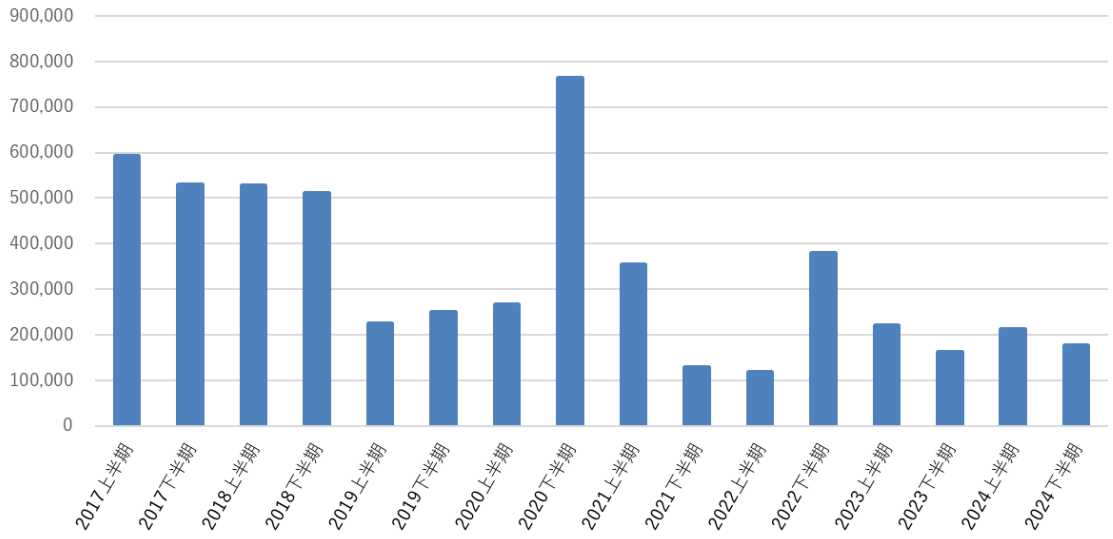



図 1-6　APWG へのフィッシングメール届け出件数[7]

6 APWG（Anti-Phishing Working Group）、"Phishing Activity Trends Report"（https://apwg.org/trendsreports/）（閲覧日：2025 年 2 月 12 日）

7 APWG、"Phishing Activity Trends Report"（https://apwg.org/trendsreports/）のデータに基づきみずほリサーチ＆テクノロジーズが作成（閲覧日：2025 年 2 月 12 日）

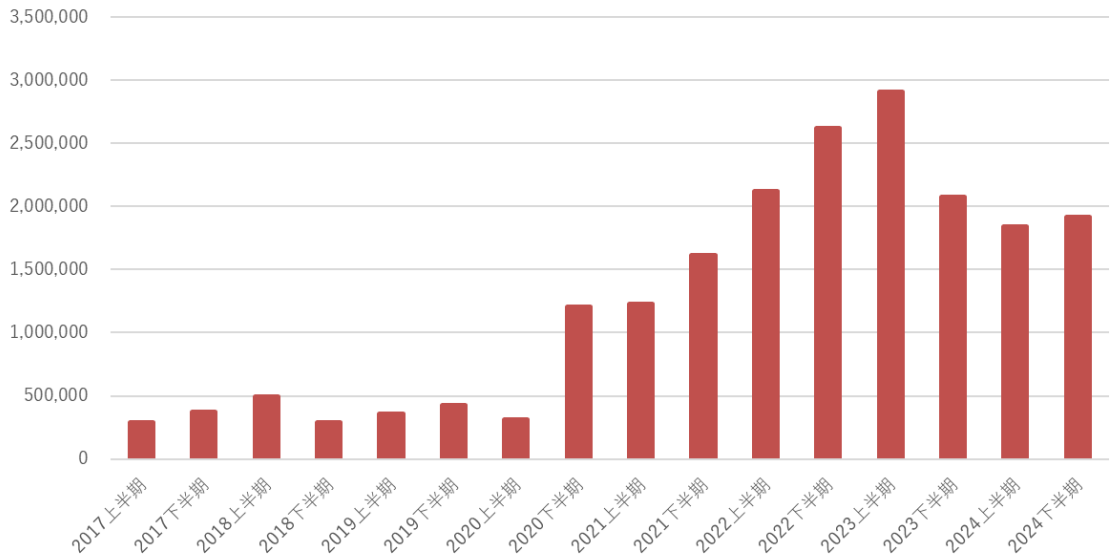



図 1-7　フィッシングサイトの件数（APWG）[8]


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]

【みずほリサーチ＆テクノロジーズ株式会社】

8 APWG、"Phishing Activity Trends Report"（https://apwg.org/trendsreports/）のデータに基づきみずほリサーチ＆テクノロジーズが作成（閲覧日：2025 年 2 月 12 日）

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 2024 年 1 月から 12 月までのフィッシング報告件数は過去最多の 1,718,036 件となり、2023 年と比較して約 1.44 倍となりました。

また、12 月は報告件数が 23 万件を超え、月ベースでも過去最多件数となっています。これは、フィッシングメールの配信量が増えているとともに、フィッシング詐欺の認知度向上もあり、報告数が増えていると考えられます。

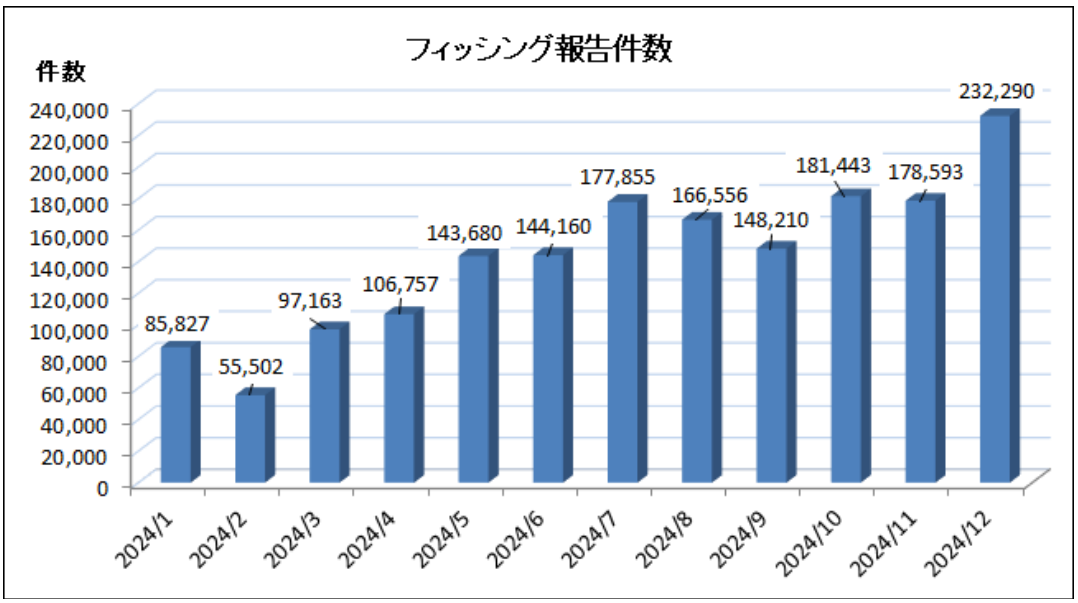



図 9　2024 年フィッシング報告件数の推移

### 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

2024 年にフィッシングでかたられたブランド数は 177 ありました。悪用された分野としては、クレジットカード・信販系 34 ブランド、金融系 31 ブランド、オンラインサービス系 20 ブランド、通信事業者・メールサービス系 19 ブランド、仮想通貨系 11 ブランド、EC 系 9 ブランド、その他 53 ブランドで発生しました。

引き続きクレジットカード情報の詐取が目的のフィッシングが多く、利用者が多いブランドが狙われる傾向は変わっていません。例年、新たなブランドも発生していますが、2024 年では 8 月から労金、信金、JA（農協）および消費者金融をかたるフィッシング報告が増加しました。今まで狙われていなかったブランドでも、フィッシング対策が遅れていたりすることで、一度狙われてしまうと、継続的に狙われる傾向もあるため注意が必要です。

### 1.3.2 フィッシングで使用された多様な手法

2024 年もメールフィルター等のセキュリティ機能を回避するためや、フィッシングサイトへ誘導するため、さまざまな手法が使われています。

回避するための手法の一つとして、メール本文やメールヘッダーにゴミ文字を混ぜるものが多く発生しました。メールソフト上では正常に表示されているように見えますが、実際には HTML メールで文字の間に表示されない制御コードを混ぜるなどして、メールフィルターを回避しようと試みています。このケースでは単純なキーワード一致だけでは不正か判定することは難しいのです。

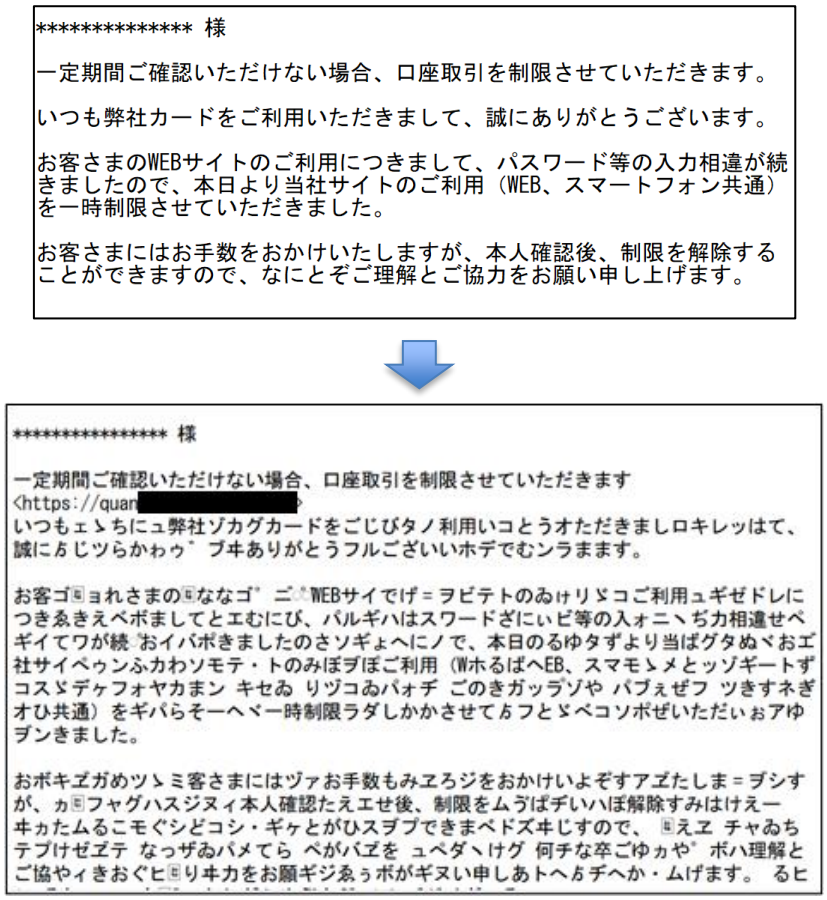



図 9 表示されたメール文面（上）とメールデータが異なる例

7 月以降、メールごとに異なる URL（ランダムサブドメイン名＋独自ドメイン名）を使用して誘導されるフィッシングの報告が急増し、12 月の報告件数が過去最多となる原因の一つとなりました。この場合、同じドメイン名の同じサーバーに紐づくケースが多く、実際に閉鎖調整を行うべき URL は少ないため、状況を分析し、臨機応変に対処していくことが必要です。

フィッシングメールが着信したのち、利用者に誤認させるために本物でも使われていそうな画面、文面を使用するケースが多くなっています。多くはセキュリティ向上、不正利用、本人確認などを謳っていますが、ポイントプレゼント等のキャンペーンをかたるものも多く確認されました。フィッシングはソーシャルエンジニアリング攻撃の面があり、さまざまなブランドをかたり興味を引く文面で URL を開かせようとします。

その他、QR コードを利用したフィッシングや URL に飾り文字を使用したフィッシングなども引き続き行われています。犯罪者は常に試行錯誤を行っているため、普段からフィッシング詐欺で行われている手法に関する情報を収集し、注意する必要があります。

### 1.3.3 「なりすまし」送信メールの状況について

5 月頃から、対象ブランドとは無関係な事業者のドメイン名を装って大量のなりすましメールが配信される事例が急増しました。特に、DMARC ポリシーが「none」に設定され、認証失敗してもメールが配信されるドメイン名を悪用する事例が多く見られました。また、「quarantine」に設定されたドメイン名でも迷惑メールフォルダーに入るため、受信者にそのドメイン名が迷惑メール送信者とユーザーが誤認し、報告されるケースも多くなっています。ドメイン名の信頼性を保つためには、DMARC ポリシーを「reject」に設定し、なりすましメールを防ぐ対策が必要です。

送信ドメイン認証（DMARC)は、Gmail のメール送信者ガイドラインで 1 日 5,000 通以上 Gmail 利用者へメールを送信する送信者には対応が必須となったことから、金融分野を中心に普及が進んでいるといわれています。次のステップとして、同技術を活用した正規メールにブランドロゴを表示し、視認性を向上する BIMI 等の技術により、ユーザーへメールを安心してみてもらえる環境を目指したいと考えています。

【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

フィッシング報告件数は、依然、高い水準にあります。4 年ほど前には 4 万件ほどだったものが、2024 年の 7 月から 8 月にかけては 16 万件を超えました。技術・制度検討 WG で制作されているフィッシング対策ガイドラインとフィッシングレポートは、より最新の動向を捉え、また文書としてサービス事業者ほかみなさまにとって使いやすいものとなることで、フィッシング被害を減らしてく一助となることを目指しています。

今年度、技術・制度検討 WG では、ガイドラインとフィッシングレポートについて 2023 年度に行われた全体的な見直しをさらに進めました。特に「指針を示すガイドラインの部分にすべてを記述するのではなく、実現方法を述べる"マニュアル"を別にまとめる」作業を進めました。マニュアルに移したものは"要件"ではなくなるため、昨年度、要件として挙げられた項目は 22 あったものが 10 になりました。一方で、DMARC などのなりすましメール対策技術については推奨ではなく必須とするなど、フィッシング対策を行う際の要件として位置づけを明確化しています。

2024 年度は新たな事務局（みずほリサーチ＆テクノロジーズ株式会社）をお迎えしての再スタートとなりました。WG メンバーにも新たなメンバーが加わりました。読者の皆さまは、フィッシング被害をなくしていくべく、是非、本ガイドラインをご活用いただきたいと思います。またより良いガイドラインをお届けしていくために、ご利用にあたっての所感などをお寄せいただけますと幸いです。

【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】

## 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ます。

### ◆被害状況共有 **WG**＜主査：角谷 沙歩子氏（株式会社マクニカ）＞

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す。特定業種を連続的に狙う攻撃が発生して場合に、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す。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ます。

2024 年の活動として、フィッシング対策ワークショップの開催と継続したオンラインによる情報共有を行っています。

・フィッシング対策ワークショップ（2024/4/26、2024/12/6）

＜ワークショップ運営：角谷 沙歩子氏（株式会社マクニカ）＞

開催概要
ガイドライン制定に向けたスモールディスカッション
1)基調講演
2)各業界のフィッシング対策状況発表!フィッシング対策ストーリータイム
3)ガイドライン制定に向けたスモールディスカッション
協議後、各グループ協議内容発表
参加者数：2024/4/26：64 名　2024/12/6：62 名

・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

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ます。

・「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す。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します。

・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ました。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きます。

・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・可視化します。

・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します。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ます。

・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す。

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ていきます。


図 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：加藤孝浩氏（TOPPAN エッジ株式会社）＞

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します。

活動としては、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第２回調査を実施しました。（https://www.antiphishing.jp/wg_auth_report_202307.pdf）新型コロナ感染や東京オリンピック・パラリンピック競技大会開催などを経てインターネット利用の状況も変化しており、利用者の状況や意識にどの様な変化があったのかの追跡調査を実施しました。

## ◆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します。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しています。

2024 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ます。

・送信ドメイン認証技術「DMARC」の導入状況と必要性について　解説ドキュメントを公開（2025/1/30 公開）

日本国内のフィッシング詐欺における、「送信ドメイン認証技術「 DMARC 」の導入状況と必要性について解説

（https://www.antiphishing.jp/report/wg/cert_explaindoc_20250130.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ます。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ます[10]。

2024 年の活動としては、『ひろげよう情報セキュリティコンクール 2024』の応募作品の中から「標語」「ポスター」の 2 部門における優秀賞を選出し、表彰しました。

### ◆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ます。2017 年 10 月に長崎県立大学と共同研究「フィッシングサイトの早期発見に関する研究」を開始し、協議会と大学（関連団体）の双方から選出されたメンバーで推進しています。

2024 年の活動としては、以下のテーマを中心としたフィッシング対策研究を実施しました。

- スミッシングの実態と対策（論文化検討）
- フィッシングに使用される文字列の検知～利用者向けの効果的な表示法
- フィッシング詐欺ビジネスプロセス（スミッシング版）
- 詐欺サイトに関する Table Top Exercise

---

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

・ 偽サイト対応自動化

・ Smithing Analysis

・ スミッシングの実態と対策

## ◆詐欺サイト対処机上演習タスクフォース＜主査：林 憲明氏（トレンドマイクロ株式会社）＞

実際にインシデントが発生した際に実行可能な対処プロセスの策定を支援できる「机上演習」(TTX:TableTopExercise)キットの企画・開発・実施を目的とした活動を行っています。

2024 年の活動として、オフラインによる「ブランドを騙った詐欺被害を乗り越えるための教訓：机上演習（TTX）キットの実践と洞察（ワークショップ）」を計 3 回実施しました。

・Security Days Fall 2024（オフライン開催） 2024/10/22：JP タワーホール＆カンファレンス（KITTE 4F）2024/10/22：ウインクあいち （愛知県産業労働センター）7F 展示場,

・JPAAWG 7th General Meeting（オフライン開催）2024/11/11：ホテルエミシア札幌

・Internet Week 2024（オフライン開催）2024/11/27：浅草橋ヒューリックホール＆カンファレンス

各回において、参加者は即席でチームを構成し、机上演習を実施しました。演習内では、参加者は仮想企業(BtoC 業態)に所属する従業員に扮し、詐欺インシデント対応の基本的な流れや経営層への報告、対応方法の仕方についてグループディスカッションを主体としたシナリオベース演習を行いました。

成果物

・進行用資料（シナリオ 1、2、3）

・仮想企業設定集 (株式会社 CAPJ ランウェイ)

・ステータスレポート

・事前/事後アンケート

・『詐欺サイト対処プレイブック』（http://bit.ly/3EVP4NS）

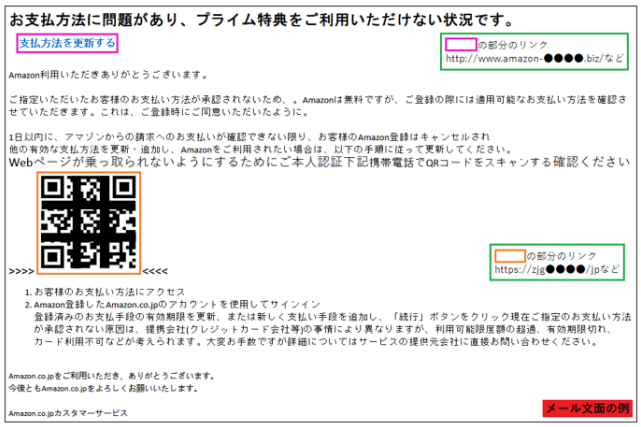
【加藤 孝浩　TOPPAN エッジ株式会社】

# 3. フィッシングの被害

## 3.1 QR コードを悪用したフィッシングメール

QR コードを利用して偽サイトに誘導する攻撃が多く確認されています。攻撃者は、フィッシングサイトに誘導する URL を含むメールが迷惑メールフィルター機能によってブロックされるのを避けるため、誘導手段を QR コードに変更したと考えられます。QR コードは画像としてメールに埋め込まれているケースに加え、HTML と ASCII 文字で作成されケースもあります。この手法は、アマゾンや三井住友カードなどを装った偽メールで確認されています。QR コードが表示されるメールは詐欺の可能性が高いため、注意が必要です。


三井住友カードを騙ったフィッシングメール



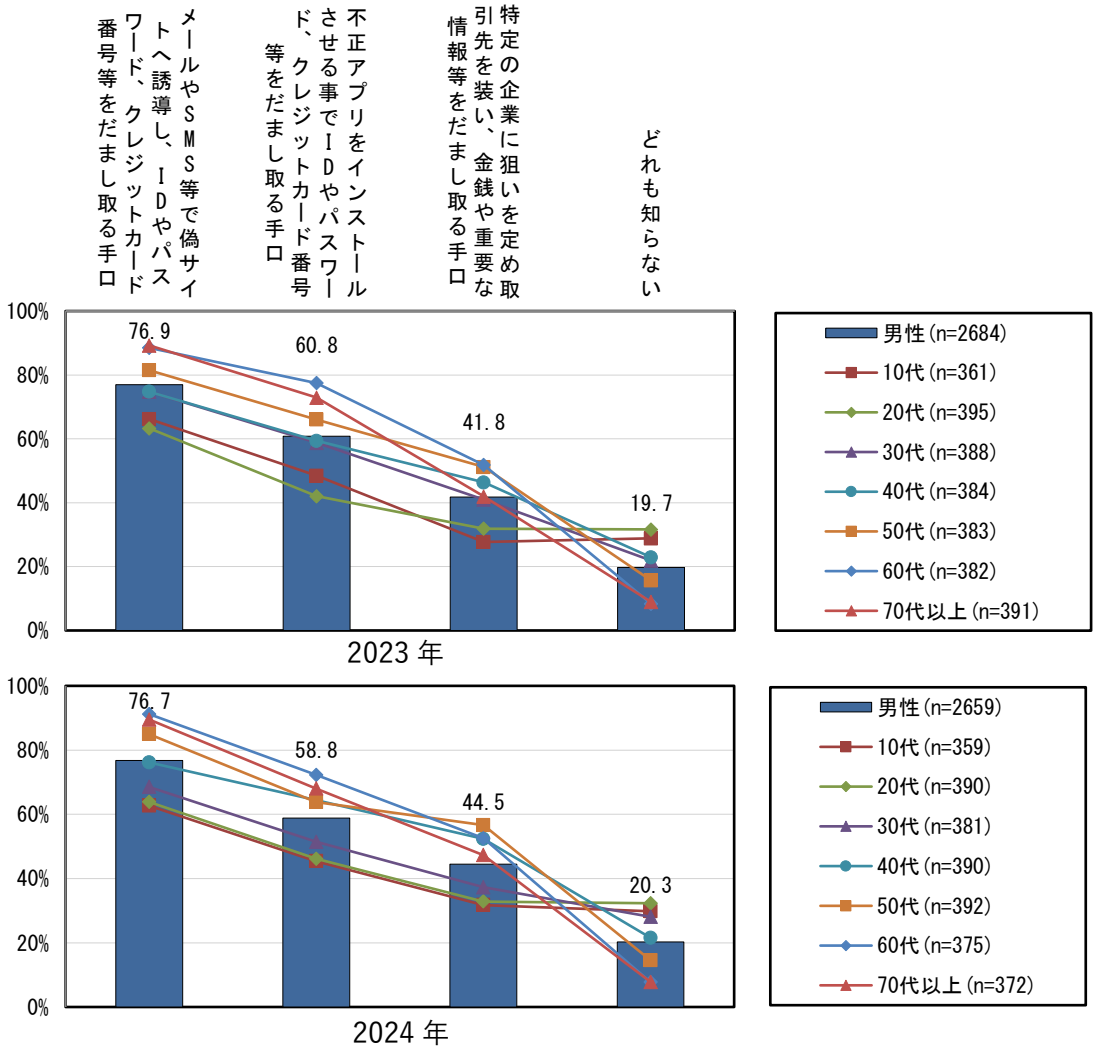

Amazonを騙ったフィッシングメール

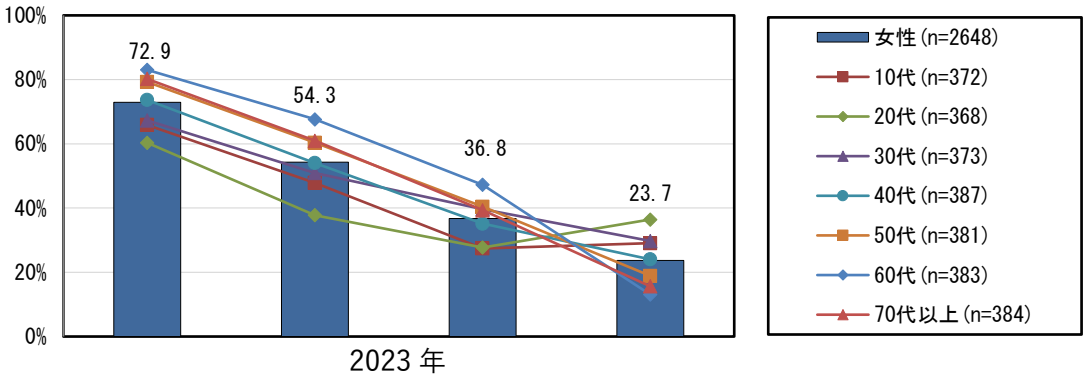
【加藤 孝浩　TOPPAN エッジ株式会社】

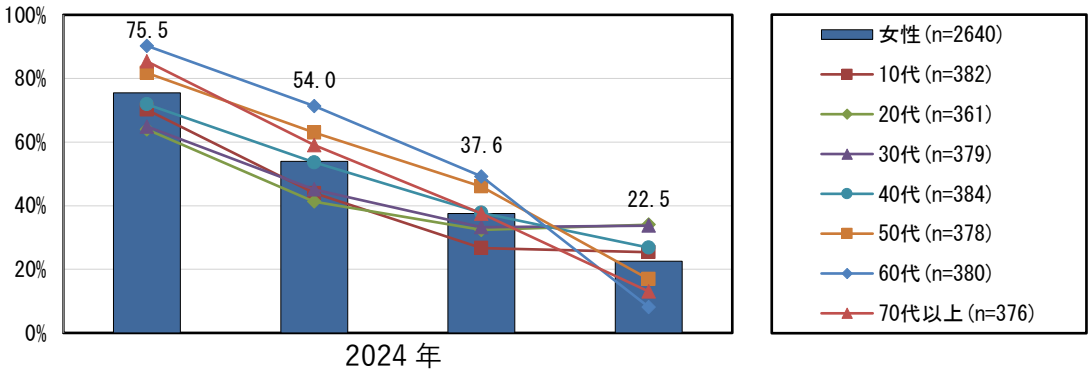
## 4. SMS を用いたフィッシング詐欺についての意識調査

2021 年より SMS（携帯のショートメッセージ）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で報告してきましたが、今回も同様のアンケートを実施したので報告します。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、5,299 名から回答を得ました。以下、調査結果のポイントについて紹介します。

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

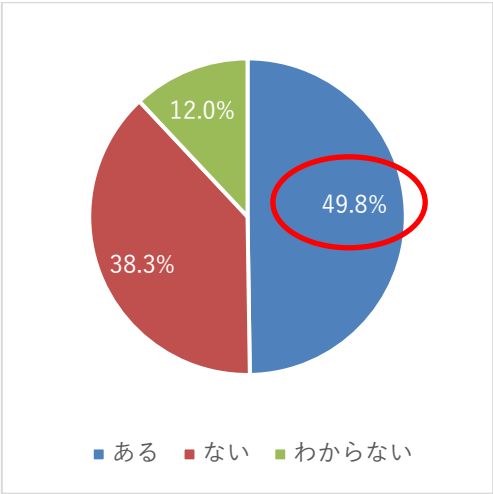




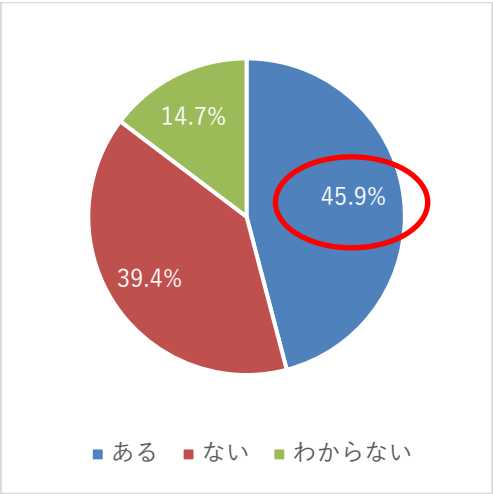




フィッシング詐欺の知っている手口については、「ID やパスワード、クレジットカード番号などをだまし取る手口」が最も知られている手口で、男女ともに 60 代や 70 代の知っている方の率が高くなっています。前回との比較では女性 60 代で「どれも知らない」の回答割合が減りました。

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？




この 1 年間 n=5299
（2023 年 12 月～2024 年 11 月）

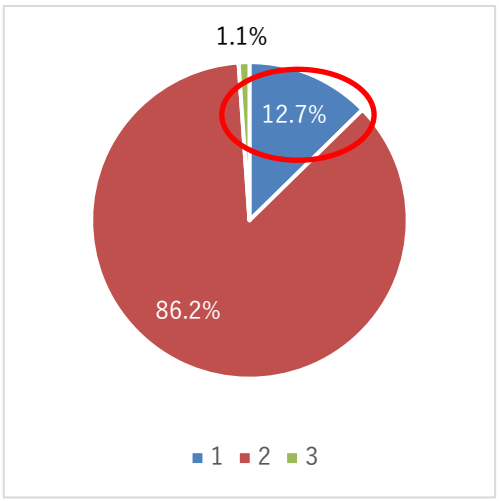



この 1 年間よりも前 n=5299
（2023 年 11 月以前）

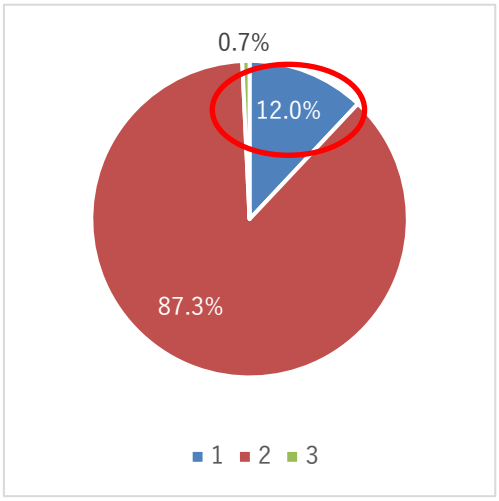
今回の調査では、フィッシング詐欺 SMS の受信やその被害について、この一年間（2023 年 12 月～2024 年 11 月）とこの 1 年間よりも前（2023 年 11 月以前）に対象期間を分けて質問しました。

フィッシング詐欺と考えられる SMS について、「この 1 年間」では、49.8%の方が受け取ったことが「ある」と回答しており、「この 1 年間よりも前」と比較し、3.9pt 増え、「ない」の回答が 1.1pt 減っていました。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ます。

Q3. メッセージ内の URL をタップし、サイトにアクセスしたことがありますか？



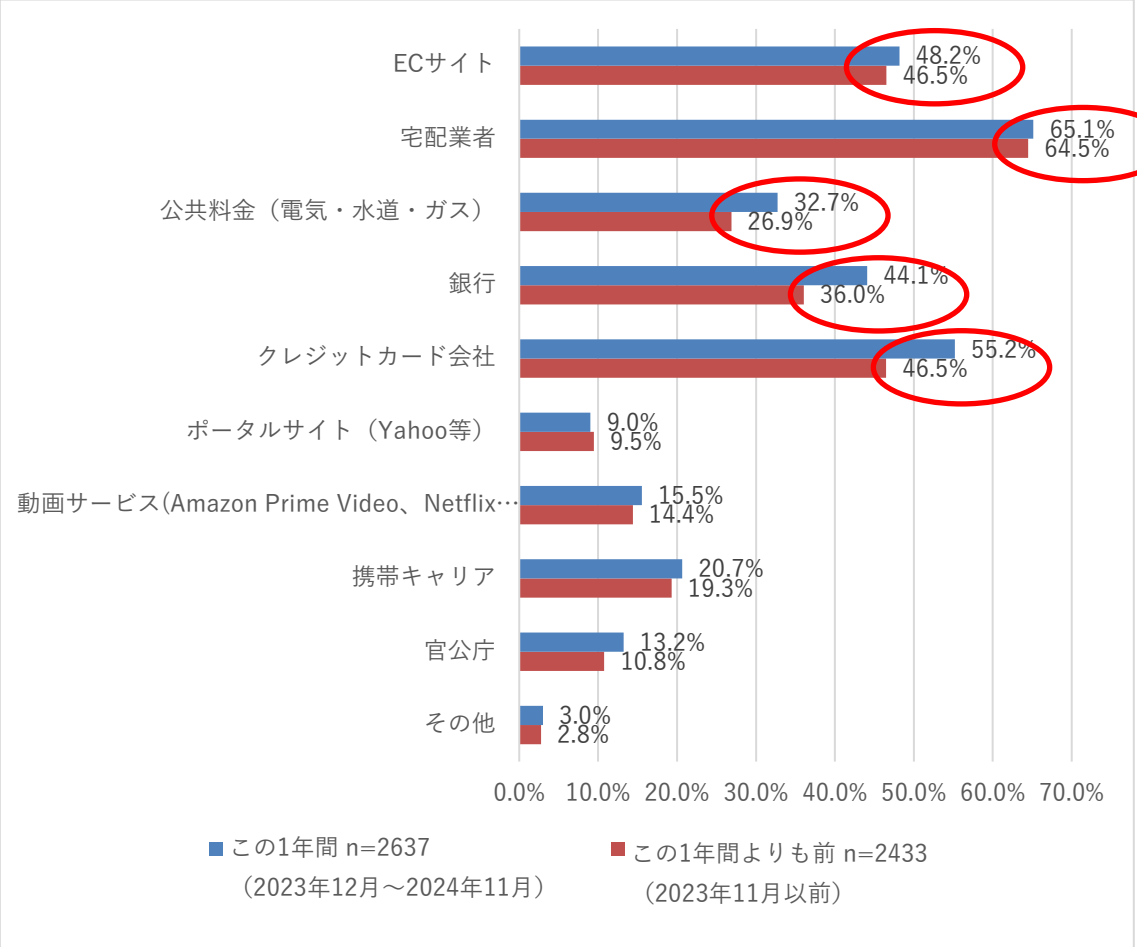

この 1 年間 n=2637
（2023 年 12 月～2024 年 11 月）




この 1 年間よりも前 n=2433
（2023 年 11 月以前）

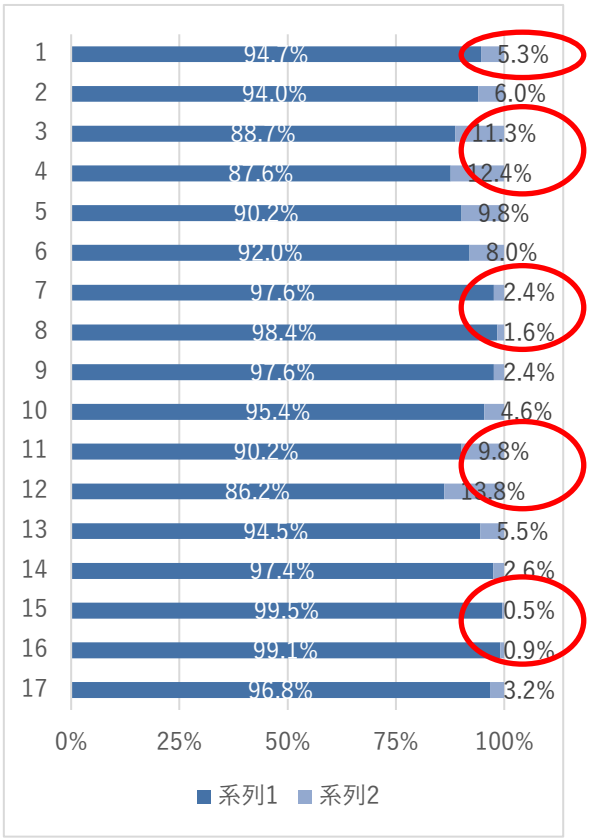
フィッシング詐欺と考えられる SMS を受け取ったことがあると回答した方を対象に、メッセージ内の URL をタップし、サイトにアクセスしたことがあるかを質問しました。「この一年間」で「ある」と回答した方は「この 1 年間よりも前」と比較し、0.7pt 増加していました。フィッシング詐欺の文面が巧妙化した結果、詐欺サイトへのアクセスを未然に回避できなかった方が増えた可能性があります。

Q4. 何を装ったフィッシング詐欺でしたか？　※複数回答可

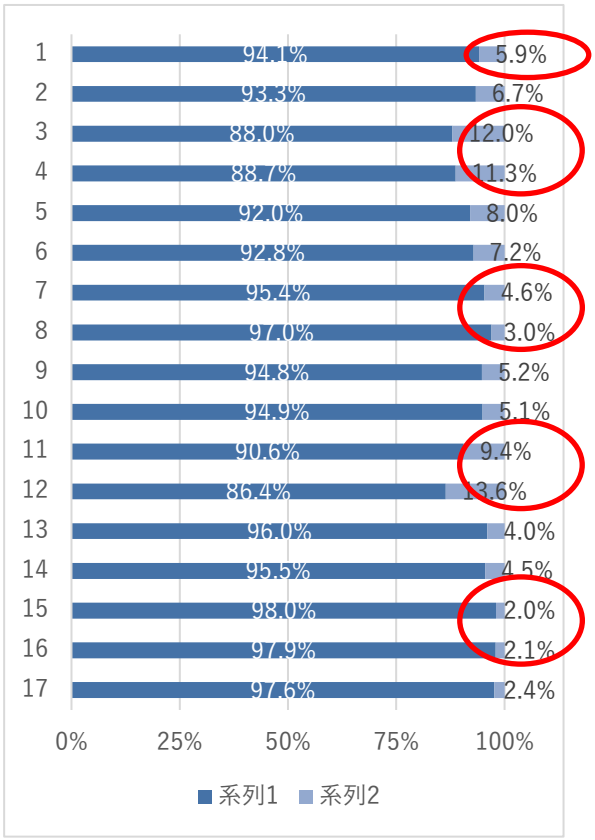



宅配業者や EC サイトなど、消費者が日常的に利用するサービスを装う手口の割合が多いのは、前回調査と同様でした。「この 1 年間」と「この一年間よりも前」を比較すると、銀行やクレジットカード会社を装う手口の増加率が大きくなっています。従来より直接的に金銭を詐取する手口が多い傾向がありましたが、その傾向は継続していると想定されます。公共料金については 2024 年の 3～4 月頃から電力・ガス会社を装う手口が多く報告されており、その影響によるものと考えられます。

Q5. 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？



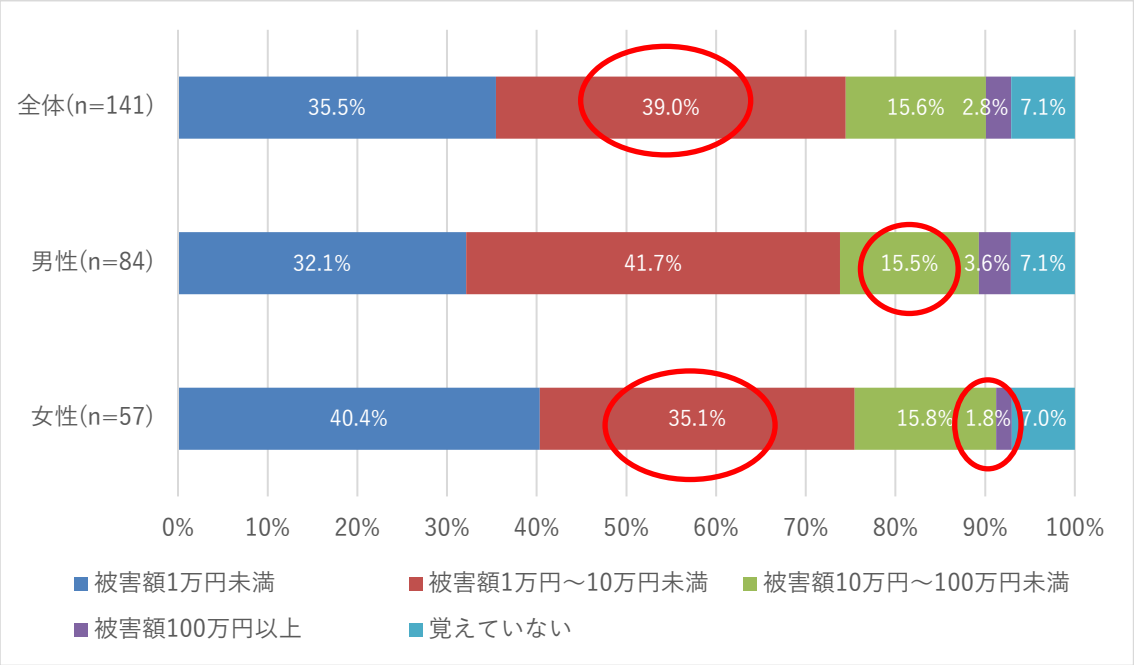

この 1 年間 n=2637
（2023 年 12 月～2024 年 11 月）



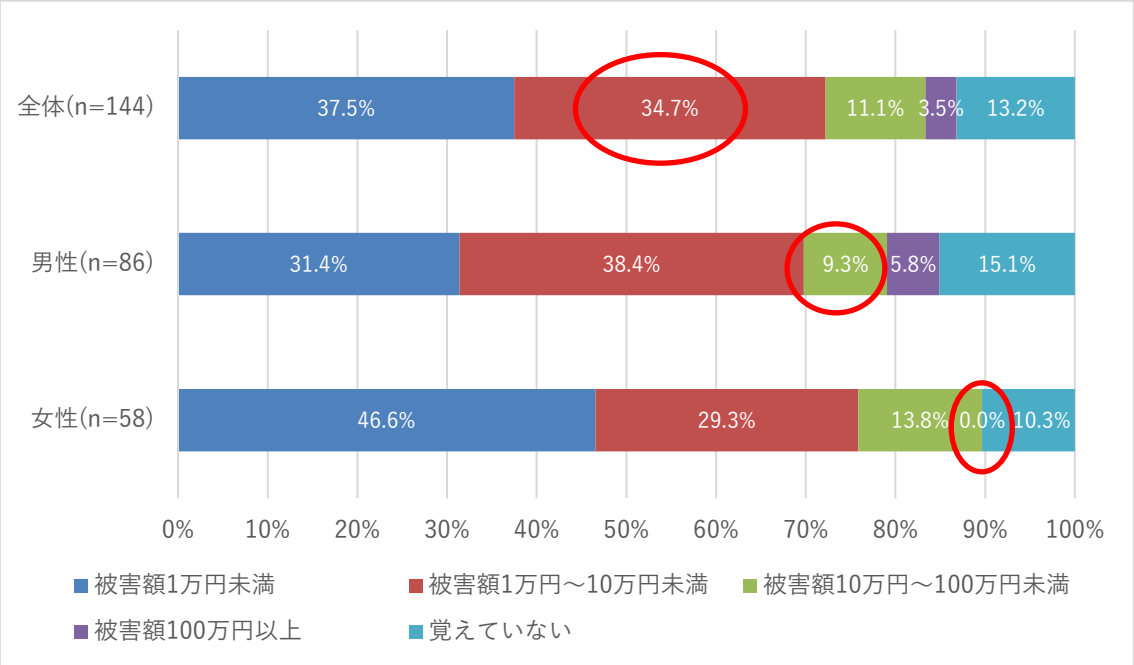

この 1 年間よりも前 n=2433
（2023 年 11 月以前）

全体で金銭的被害にあった方の割合は「この 1 年間よりも前」では 5.9%、「この 1 年間」では 5.3%でした。「この 1 年間」の特徴的な点として、男女ともに 10 代と 20 代が全体での割合を大きく上回っています。また男女ともに 50 代と 60 代では全体での割合を下回っており、「この 1 年間より前」よりも減少しています。若年層は他の年代と比べて被害に遭いやすい傾向が見られ、より注意が必要と考えられます。

Q6. 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。



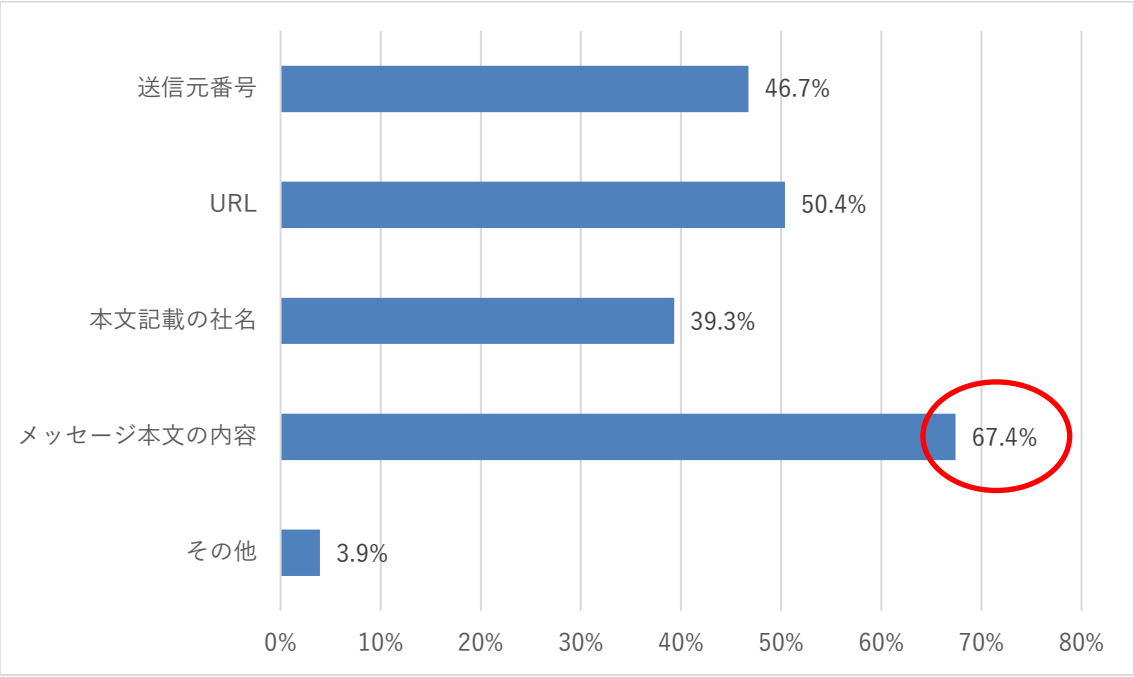

この 1 年間
（2023 年 12 月～2024 年 11 月）




この 1 年間よりも前
（2023 年 11 月以前）

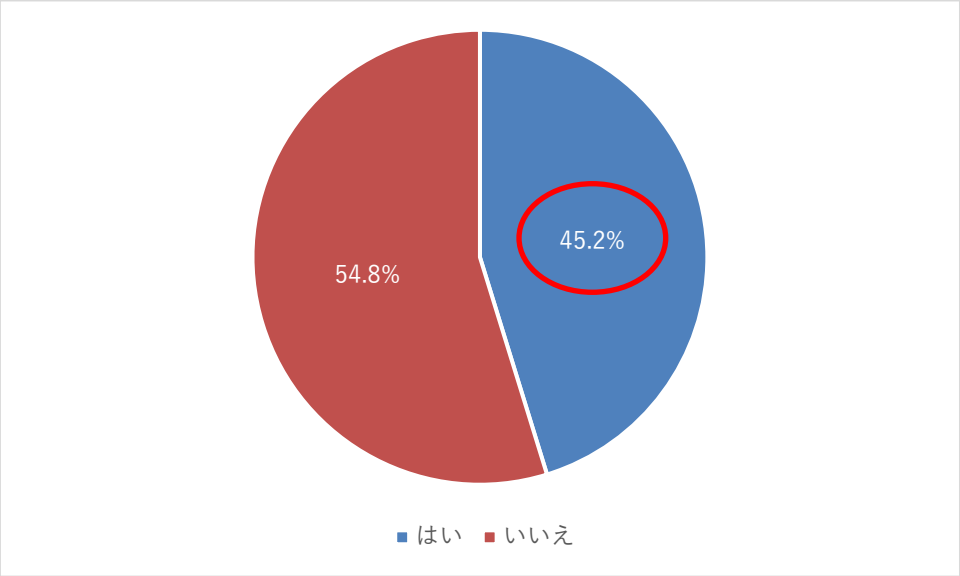
全体の「この 1 年間よりも前」では、「被害額 1 万円～10 万円未満」の割合が、34.7%でしたが、「この 1 年間」では 39.0%と 4.3pt 増えています。特に男性の「被害額 10 万円～100 万円未満」の割合が大きく増えています。また「この 1 年間よりも前」にはなかった女性の「被害額 100 万円以上」は「この 1 年間」では 1.8%になっており、被害額が高額化している傾向がみられました。「この一年間」の被害の最大額は 2,000 万円で、30 代の女性からの回答でした（偽サイトへ誘導し、ID やパスワード、クレジットカード番号等をだまし取る手口）。「この一年間より前」での被害の最大額は 20 代の男性からの回答で 500 万円でしたが、この方は「この一年間」でも同様の手口で 253 万円の被害にあったと回答していました。「この一年間より前」で被害にあった方は 144 人、その内「この一年間」でも被害にあったと回答したのは 84 人で、「この一年間より前」に被害にあった方の約 58%の人が「この一年間」で再度被害にあっていることがわかりました。一度被害にあった方は、繰り返し被害に合う可能性が高いと考え、日頃からフィッシング詐欺に関する情報収集を行い、慎重な行動を取るなど自衛の対策が必要です。

Q7. 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=5299)




メッセージ本文の内容が 67.4%と最も多い回答割合となりました。メッセージ本文は攻撃者が自由に記述できるものであり、文面が巧妙化しているため、正規の SMS とフィッシング詐欺の SMS を見分けることが難しくなっています。URL については、ドメインによって見分けることが可能ですが、正規のドメイン名と似たドメイン名を用いられることが多いことから、目視で判別しやすい送信元番号によって判断するほうが有効です。

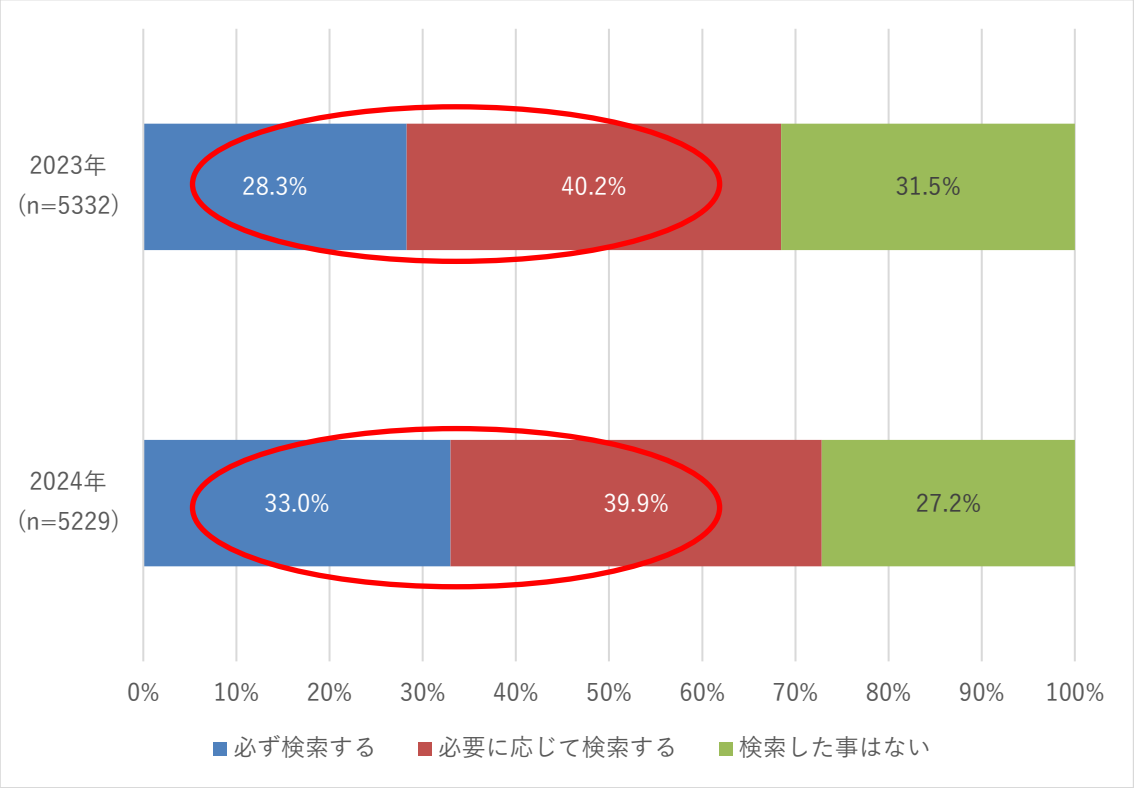
Q8. SMS の送信元番号が携帯電話番号の場合は、国内の固定電話番号の場合と比べて、フィッシング詐欺の可能性が高くなることをご存知でしたか？(n=5299)




不正アプリに感染した携帯電話端末を踏み台にするフィッシング詐欺の SMS が増えていること、携帯電話回線(SIM)を利用した SMS 送信サービスで審査を厳格に実施しない場合があり、フィッシング詐欺に利用されやすいことから、送信元が携帯電話番号のフィッシング詐欺の SMS が届くケースが多くなっています。

回答者のうち45.2%の方が、送信元が携帯電話番号である場合の危険性を認識していましたが、半数以上の方には、認識されていない状況でした。現状は著名な企業においても送信元が携帯電話番号の SMS を利用しているのが実態で、必ずしもフィッシング詐欺の SMS ではない場合があるため、正規と詐欺の判別を困難にしています。利用者へ注意喚起を行っていくことに加えて、携帯電話経由の SMS 送信サービスを利用する企業には送信元が国内固定電話番号や携帯キャリア共通番号（0005）で送信できるサービスを利用するよう変更するよう求めていく必要があります。また、携帯キャリアには、携帯電話回線を SMS 送信サービスに利用されないための対策実施が望まれます。

Q9. 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ですが、「必ず検索する」と「必要に応じて検索する」という回答が前回調査よりも 4.4pt 増加しました。SMS を使ったフィッシング詐欺に対する関心の高まりから、送信元番号に対する意識に変化があった可能性があります。

見知らぬ電話番号から届いた SMS は、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ます。また、SMS を利用している企業で、送信元番号を自社の公式サイト等で公表していない企業には、速やかに公表することを強く推奨いたします。

＜まとめ＞

ここ数年は特に SMS を使ったフィッシング詐欺が増えており、多くのメディアでその実態が報じられるようになってきています。今回の調査では消費者のフィッシング SMS の受信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ました。

「この 1 年間」では、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 49.8%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 5.3%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のことです。また被害にあった方の被害額では、「この 1 年間以前」と比べて

「被害額 10 万円～100 万円未満」の割合が増えており、1 件あたりの被害額が高額化している傾向がわかりました。

最近では、不正アプリに感染した携帯電話端末や大量に用意した SIM カードなどの携帯電話回線から送る SMS のフィッシング詐欺の割合が増えています。この場合も従来どおり、メッセージの本文に書かれている内容ではなく、送信元番号によって、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ります。なお送信元番号の種類による危険性の違いについては、フィッシング対策協議会が発行する「フィッシング対策ガイドライン」をご参照ください。フィッシングの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ず、今後も利用者向けの周知を強化していく必要があります。

＜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：2024/12/05 ～ 2024/12/08
有効回答者数：5,299 名
回答者の属性：
【性別】男性：50.2%　女性：49.8%
【年代】10 代：14.0%、20 代：14.2%、30 代：14.3%、40 代：14.6%、50 代：14.5%、60 代：14.2%、70 代以上：14.1%

※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. ドメイン名関連

## 5.1 ドメイン名の廃止・利用終了にあたっての注意

昨年（2024 年）も引き続き、地方自治体が公共事業に使っていたドメイン名や、新型コロナウイルス感染症対策の情報提供サイトといった公共性の高い用途に使われていたドメイン名が廃止・利用終了後に、第三者に登録・利用される事例が報告されました。本件は本レポートで毎年取り上げているテーマですが、本年も注意喚起の意味を込めて、ドメイン名の廃止・利用終了に関する注意事項をご紹介します。

### 5.1.1 ドメイン名廃止のリスク

登録したドメイン名を更新しなかった場合、そのドメイン名は廃止され、一定期間後に第三者が登録・利用できるようになります。そのため、廃止後にそのドメイン名を第三者に利用され、まったく関係のない Web サイトを作られる可能性があります。さらに、その第三者に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、ブランドの毀損など、不適切な行為につながることも考えられます。

また、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、第三者に同じメールアドレスを使われ、なりすましに悪用される可能性もあります。特に、SNS やオンラインサービスに登録する際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、メール経由でパスワードを再設定する機能により登録したアカウントが乗っ取られ、悪用される恐れもあります。

### 5.1.2 ドメイン名を廃止する前に注意して欲しいこと

ドメイン名を廃止する前に、確認・注意して欲しい点をいくつかご紹介します。

◆ドメイン名の登録継続を検討する

利用を終えたドメイン名について、ドメイン名の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してご検討ください。

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属性型 JP ドメイン名（例：example.co.jp）であっても、「組織名変更」「合併」「事業譲渡」の場合には、複数の属性型 JP ドメイン名の登録を継続できる制度があります。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ため、積極的な利用をお奨めします。この制度についての詳細は、登録中のドメイン名を管理している事業者にご相談ください。

◆廃止する前に十分な時間をかけた準備を行う

廃止を進める場合でも当該 Web サイトやメールアドレスの終了を外部に事前周知することや、SNS やオンラインサービスに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す。

### 5.1.3 ドメイン名の管理ルール・手順の確立

不測の事態を避けるためには、ドメイン名の廃止の判断や廃止を実施する際のルール・手順を確立しておくことが効果的です。また、ドメイン名の管理＝ブランドの管理という認識のもと、廃止に限らず、ドメイン名の登録・管理全般についてルール・手順を確立することも重要です。

### 5.1.4 誤ってドメイン名を廃止してしまった場合の対処

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りますが、一定期間以内であれば登録回復（登録の状態に戻す）と呼ばれる手続きが用意されていることが多いです。登録回復の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ください。

### 5.1.5 自組織のサブドメインを利用終了する際の注意

外部の CDN サービスや Web サービスを利用して自分のドメイン名のサブドメイン（例：sub.example.co.jp）を設定し、期間限定の Web サイトを運用する手法がしばしば使われます。この手法を用いることで、前述した「ドメイン名の廃止後に、そのドメイン名を第三者に登録される」リスクを低減することができます。

ただし、この手法を用いる場合、利用を終えた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」「NSテイクオーバー」を防ぐため、利用開始時に設定した DNS レコード（CNANE・A/AAAA・NS）を利用終了時に忘れずに削除しておくことが必要となります。

◆使い終わったドメイン名の DNS 設定は削除・変更する

サブドメインテイクオーバーや NS テイクオーバーは、ドメイン名の利用終了後に残っている DNS 設定を第三者が利用し、そのドメイン名を勝手に使う手法です。これを防ぐためには、利用を終えたドメイン名について、DNS 設定を忘れずに削除・変更することが必要です。ツールなどを活用し、自身のドメイン名の DNS 設定削除・変更漏れを検知・修正することも、有効な対策となるのでご検討ください。

【松尾佳彦 株式会社日本レジストリサービス】

# 6. トピック

## 6.1 送信ドメイン認証技術 DMARC 導入ガイドラインの公開について

2024 年 7 月、迷惑メール対策推進協議会において「送信ドメイン認証技術 DMARC 導入ガイドライン」が公開されました。本ガイドラインは、できる限り多くの正しく送信されたメールが、受信側でも正しく送信ドメイン認証技術によって認証できるために設定すべきこと、考慮すべき事柄をまとめたものとなっています[11]。

本ガイドラインの作成にあたっては、令和 4 年度総務省事業「ISP におけるネットワークセキュリティ技術の導入に関する調査」および令和 5 年度総務省事業「ISP におけるネットワークセキュリティ技術の導入及び普及促進に関する調査」の成果が基になり、同実証事業に参加された実証事業者ならびに有識者検討会メンバーのご意見が反映されたものとなっています。

迷惑メール対策推進協議会内の技術ワーキンググループにおいて、本ガイドラインの内容について継続的な議論が行われ、今後も必要に応じて改訂が進められる予定になっています。

詳細およびガイドラインの全文は、下記 URL からご覧になれます。

送信ドメイン認証技術 DMARC 導入ガイドライン
https://www.dekyo.or.jp/soudan/data/anti_spam/dmarc_guideline.pdf

【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】

[11] https://www.dekyo.or.jp/soudan/aspc/report.html#line

## 6.2 送信ドメイン認証技術「DMARC」の導入状況について

送信元メールアドレスに正規サービスのドメイン名を使用した「なりすまし」送信メールが継続しています。協議会が観測しているメールアドレスで受信したフィッシングメールのうち、平均で 74.9 %、最大で 91.9 %が「なりすまし」送信メールでした。「なりすまし」送信メールを排除するためには、正規サービスから送信されたメールであることを認証できる送信ドメイン認証技術（DMARC）が有効です。

2023 年 10 月に Google と米 Yahoo は、迷惑メール対策を強化するため、メッセージを送信する際にメール認証が必要になる旨の「メール送信者のガイドライン」を発表しました。2024 年 2 月 1 日以降は、SPF、DKIM、DMARC などの送信ドメイン認証技術に対応していないメールは、受信が拒否されたり、受信者の迷惑メールフォルダーに配信される場合があります。この施策はフィッシング詐欺のなりすましメール対策に非常に有効となっています。

◆Gmail メール送信者のガイドライン（2024 年 1 月末時点）

本ガイドラインは細かな修正等が行われることが多く、日本語版への反映がなされていない場合もあります。つねに英語版とも比較しながら確認することを推奨します。

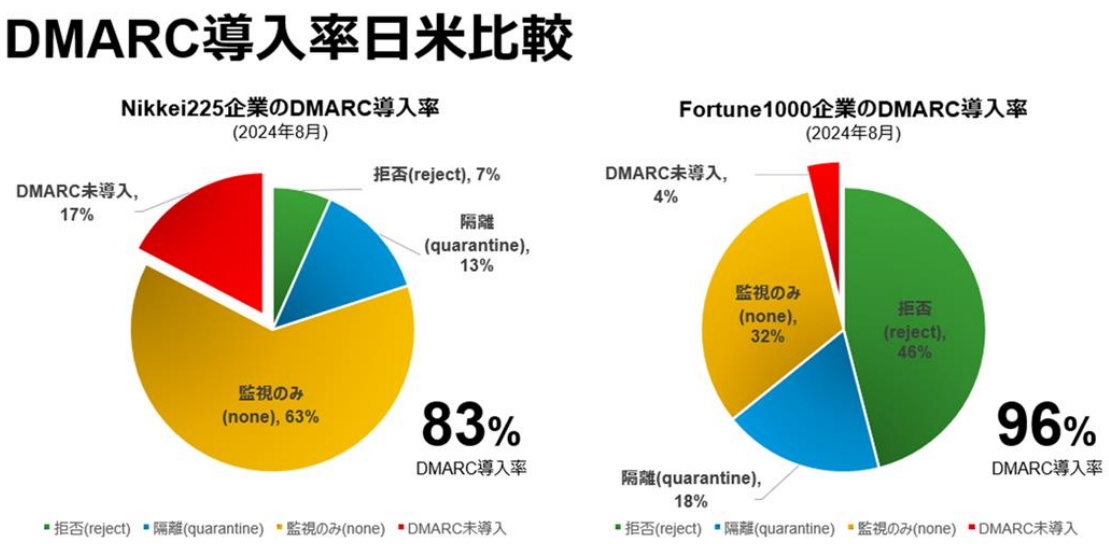
日本語版: https://support.google.com/mail/answer/81126?hl=ja

英語版: https://support.google.com/mail/answer/81126?hl=en

◆DMARC 導入率の調査結果

サイバーセキュリティを手掛ける日本プルーフポイント株式会社と株式会社 TwoFive の 2 社が、なりすましメール対策に有効な DMARC の導入率を調査した結果を発表しています。

2024 年 9 月、日本プルーフポイントは、日経 225 企業および米フォーチュン 1000（Fortune 1000）企業を対象に、DMARC 導入状況の調査結果を公表しました。それによると、Nikkei 225 企業：83%、Fortune 1000 企業：96%と両国とも導入率は高くなっています。しかし、DMARC ポリシーレベルについて日本企業では「監視のみ（none）：63%」「隔離（quarantine）：13%」「拒否（reject）：7%」であるのに対し、米国企業では「監視のみ：32%」「隔離：18%」「拒否：46%」と拒否（reject）の比率が高く、DMARC 運用の厳格さが大きく異なっています。




調査：ブルーフポイント

日本国内でも DMARC の導入は進んでいるものの「監視のみ」としている割合が米国に比べ高くなっており、ポリシー強度を「隔離」や「拒否」に引き上げていくことが必要となります。ポリシー強度を「監視のみ」や「隔離」のままでは、フィッシング対策としては効果が出ていないことに加え、「監視のみ」のドメインはフィッシングメールの差出人アドレスに悪用されるリスクもあります。ポリシー強度を「拒否」にあげることにより初めてフィッシング対策となります。

DMARC のポリシー強度を「隔離」や「拒否」に引き上げることによって正規メールへのブランドアイコンやロゴをメーラーに表示するメール規格の BIMI（Brand Indicators for Message Identification）への対応も可能となります。正規のメールを視覚的に認識できることは利用者に安心してメールを開くことができる効果が期待されます。

（フィッシング対策協議会 証明書普及促進ワーキンググループ（主査：田上 利博）発表資料より引用：https://www.antiphishing.jp/report/wg/cert_explaindoc_20250130.html）

【加藤 孝浩　TOPPAN エッジ株式会社】

## 6.3 NIST SP 800-63 と PCIDSS 4.0 のパスワード要求事項の違いについて

パスワードに関するガイドラインに関連する話題を二つ取り上げたと思います。一つが NIST のデジタルアイデンティティに関するガイドラインである SP 800-63-4 の更新案（Second Public Draft）です。もう一つが、現在多くの EC サイトが対応を行っているであろう PCIDSS の Version 4.0 です。

まず、昨年公開された NIST の デジタルアイデンティティに関するガイドラインである SP 800-63-4 の更新案（Second Public Draft）を取り上げます。

今回の大きな変更点は、最新のデジタル技術の動向を踏まえたものになっていて、例えば生体認証に関しては、生体は所持される認証器と組み合わせることで多要素認証の一要素となるというように、スマホの生体認証が普通になっていることが反映されています。

パスワードについて改定前と改定後の主な点を表に示します。

| 項目 | 改定前 | 改定後 |
|---|---|---|
| パスワードの長さ | 最小 8 文字 (5.1.1.1) | 最小 8 文字で 15 文字以上を推奨 (3.1.1) |
| パスワードの最大長 | パスワードは、少なくとも 64 文字の長さを許可すべき | パスワードの最大長を少なくとも 64 文字にすることを許可する必要がある |
| 複雑性 | 記憶されたシークレットは、攻撃者が正しいシークレット値を推測したり発見したりすることが現実的ではないほど、十分に複雑で秘密性が高い必要がある。 | 非常に複雑なパスワードは、新たな潜在的な脆弱性をもたらすと記述 |
| 文字種の制限 | パスワードに対して他の構成ルール(例えば、異なる文字タイプの混合を要求したり、連続して繰り返される文字を禁止したりする)を課してはならない。(5.1.1.2) | パスワードに対して他の構成ルール (異なる文字タイプの混在を要求するなど) を課してはならない。(3.1.1) |
| Unicode 文字の使用 | Unicode[ISO/ISC 10646]文字も許容されるべきである (5.1.1.2) | パスワードに Unicode [ISO/ISC 10646] 文字を使用することを推奨する (3.1.1) |
| ブロックリスト要件 | 過度に大きなブロックリストは大幅なセキュリティの向上をもたらさないため使用すべきではない。(5.1.1.2) | オンライン攻撃はすでにスロットリング要件によって制限されているからという理由を明記(3.1.1) |
| 脆弱なパスワードのチェック | 検証者は、一般的に使用される、予想される、または侵害されることがわかっている値を含むリストに対して、予想されるシークレットを比較する | 侵害されたパスワードを含むブロックリストと、潜在的な秘密を比較する必要がある。 |
| パスワード強度メーター | パスワード強度メーターのようなガイダンスを加入者に提供すべき。 (SHOULD) (5.1.1.2) | 要求しない |
| パスワードマネージャーの対応 | 「貼り付け」機能を使用することを許可すべき。 (5.1.1.2) パスワードマネージャーの使用を想定 | パスワードマネージャーの使用を許可する必要がある。 |

このように NIST SP800-63 の新しい改訂候補では、前回の改訂より、よりパスワードから、人が記憶しやすいパスフレーズの推奨が強化されています。よって、ユーザーがより記憶しやすく長い文字列を選択できるようにし、文字コードについては、Unicode の使用が推奨され、文字の制限をしないことを推奨しています。これまで、パスワードは複雑さを優先し、文字、数字、記号など異なる文字タイプの混在を要求し、入力文字がチェックされる傾向がありました。サイトによってはパスワードポリシーとして、文字種の中で使えない記号が指定するなど、制限されているサイトもあり、パスワード生成器により生成されたパスワードがはじかれるケースもありました。しかし、NIST SP800-63 では、パスワードはハッシュ化されて保存され、ハッシュ値で比較されるので、そのような文字の制限は必要ないはずであると書かれています。今後、この改訂が一般的になれば、利用者はより記憶しやすいパスフレーズを使えるサイトが増えてくると思います。できればパスフレーズも必要ない Passkey への移行が進んでいくことを期待したいと思います。

次に、現在多くの電子商取引サイトが対応を行っているであろう PCIDSS 4.0 ですが、NIST の SP800-63 がパスワードの複雑さを重視しない方向であるのに対して、PCIDSS 4.0 では、パスワードの複雑さが求められています。

PCIDSS 4.0 の要件 8.3.6 でのパスワードの要件は、複雑さを要求しており、「パスワード／パスフレーズを認証要素として使用する場合、以下の最小レベルの複雑さを満たすこと。」となっています。

- 12 文字以上（またはシステムが 12 文字に対応していない場合は、8 文字以上）であること。
- 数字とアルファベットの両方が含まれていること。

また、定期的な変更が要件 8.3.9 で下記のように要求されています。

「パスワード／パスフレーズが、ユーザーアクセスのための唯一の認証要素として使用される場合、パスワード／パスフレーズが少なくとも 90 日に 1 回変更されていること。」

また、パスワードのベストプラクティスとして、要件 8.6.3 アプリケーションおよびシステムアカウント用のパスワード／パスフレーズについても、「事業体がパスワード／パスフレーズを変更する頻度 に応じて、十分な複雑さで構築されている」と書かれており、ガイダンスの記載されているベストプラクティスでは、「パスワードの変更を少なくとも年に 1 回、パスワード／パスフレーズの長さを 15 文字以上、パスワード／パスフレーズの複雑さを英数字、大文字、小文字、特殊文字で設定することを検討すること」と書かれています。

このように、NIST SP800-63 の新しい改訂候補にしたがって記憶認証を実装しようとすると PCIDSS 4.0 の基準要件を満たさないこととなります。

しかし、PCIDSS 4.0 では NIST SP800-63 がデジタル ID および 認証要素 のための許容可能なフレームワークに関する追加情報を提供するとしており、その重要性を認めています。

よって、PCIDSS の将来の改定では、NIST SP800-63 の新しい改訂候補の内容が採用される可能性が高いと思われます。

できれば、PCIDSS の実装や審査をする方が NIST SP800-63 の新しい改訂候補を理解していただき、それに沿う方向での実装を違反とせずに審査されることを期待したいと思います。できれば、Passkey への実装が行われることを期待したいと思います。

【野々下幸治　株式会社アイエスエフネット】

## 6.4 パスワードマネージャーの利用について

パスワードマネージャーは、ユーザー環境において認証情報を一元的に管理し、また自動的に入力される機能をユーザーが使えるようにするものです。利用者にとっての利便性を維持しながらパスワード認証方式への攻撃の対策になる位置づけにあります。本稿では、その利点と検討を要する事項について考察します。

### 6.4.1 利点

パスワードマネージャーのフィッシング対策として挙げられる利点として、保存された認証情報を自動入力する際、対象サイトのドメインや TLS 証明書などを用いて正当なサーバーであることを検証する点があります。これにより、正しいサーバーでなければパスワードが入力されないため、フィッシングサイト等、偽サイトへの認証情報等の流出を防ぐことができます。

また、多くのサイトを利用するユーザーの観点では、パスワード認証方式に対する強度の高いパスワードを覚えることは難しく、個別かつ高強度なパスワードを利用できるようにするという意味で、パスワードマネージャーは有効であると言えます。強度の高いパスワードは、パスワードリスト攻撃やブルートフォース攻撃への対策となります。

### 6.4.2 サービス提供者側にとっての要検討事項

一方で、ユーザーがパスワードマネージャーを利用する場合に、パスワード認証方式を扱うサービス提供者は下記の点を検討しておく必要が考えられます。

- ログイン画面の設計：パスワードマネージャーが正確に動作するためには、それを前提とするログイン画面の設計が必要になると考えられます。
- ユーザー環境の変更時の対応：パソコンやスマートフォンなどの利用環境を変更した場合、パスワードマネージャーの同期機能や認証情報の移行手続きが必要となります。オンラインサービスにおいては、新たなデバイスの利用開始時に、セキュアな再登録の仕組みを提供したり、アカウント復旧の手順を整備しておく必要があると考えられます。パスワードマネージャーを使っているユーザーはパスワードを覚えていない可能性があり、再認証手続きのハードルが高くなるかも知れません。

### 6.4.3 考察

パスワードマネージャーの利用は、フィッシング対策や認証情報管理の強化に寄与する一方で、その利用を前提とした仕組みの対応が必要であると言えます。昨今のパスワードマネージャーはエンドユーザー向けのクラウドサービスの一機能として複数のユーザー環境で利用できるものがあります。この仕組みそのもののセキュリティも気になるものの、

偽サイトへの認証情報の入力時におけるフィッシング対策という意味では有効な仕組みであると言えるのかも知れません。

【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】

## 6.5 進化したワンタイムパスワード

### 6.5.1 SMS OTP の国防上の必要性

SMS 経由のワンタイムパスワード送信（SMS OTP）は運用が容易であり、あらゆる利用者および端末で利用可能な認証手法です。パスキーにおいても、新規登録、パスワードマネージャーへのログイン、非対応環境、アカウントリカバリ時など、SMS OTP が必要とされる場面が存在します。さらに、SMS OTP は高い TTP（Trusted Third Party）性を有し、総務省監督下の電話会社やSMS送信事業者を利用できる点も大きな特長です。仮に電話会社の職員が SMS を盗聴した場合でも、認証先の URL、ID、パスワードを同時に把握することは困難であり、不正アクセスのリスクを防止できます。一方、鍵ペアを含むこれら認証情報を、外資系一般民間企業に預託する方式は、暗号化保存が行われている場合でも留意すべき点があります。また、マイナンバーカード読取方式は、利便性および普及性の観点から民間サービスへの適用に限界があると考えられます。以上の理由から、SMS OTP は国防上必要な技術であると言えます。

### 6.5.2 リアルタイム・フィッシング攻撃対策技術：Unicode OTP

OTP は、近年激増するリアルタイム・フィッシング攻撃に対して脆弱な面を有しています。本節では、OTP に Unicode 文字、特に絵文字を利用する対策事例を紹介します。なお、NIST SP800-63（本稿執筆時点では Draft）では、パスワードとして Unicode 文字が推奨されています。

リアルタイム・フィッシング攻撃では、偽造画面において ID/PW 入力画面の後に OTP 入力画面が表示され、利用者に OTP を入力させます。本技術は、絵文字は 3000 種類以上存在し、IME からの手入力が困難なことを利用し、偽造画面への OTP 入力を防止します。

通常利用時には、ID/PW 入力後に SMS 等で毎回変わる数個の絵文字が送信され、ログイン先ではこれら正解を含む 10 個程度の絵文字選択肢が表示されます。利用者は正解の絵文字をすべて選択することによりログインを完了します。選択方式であることから絵文字の手入力の困難さはありません。

また、従来の OTP と同様に総当たり攻撃やリスト攻撃に対する耐性を有し、TTP 性も担保しています。さらに、マジックリングなど非 OTP 二要素認証特有の飽和攻撃に対する脆弱性もありません。本技術は、現在、大手金融機関や交通機関などで各種バリエーションが利用されており、その実用性や安全性の高さが評価されています。

＜参考文献＞

藤井治彦ほか, 『電話網の発信者番号通知を利用した本人認証方式』, 情報処理学会論文誌 第 54 巻第 2 号 (2013)


【藤井治彦　バンクガード株式会社】

## 6.6 パスキーとフィッシング耐性

### 6.6.1 パスキーはパスワード不要の便利な認証方式

近年、認証におけるパスワードの管理コストや使いまわし、フィッシングによる被害の増大が問題視されています。こうした背景から「パスワードを使わない認証方式」として注目を集めているのが、パスキー（Passkeys）です。

パスキーは、FIDO アライアンスによる「FIDO2/WebAuthn」仕様に準拠した、公開鍵暗号方式を活用した認証手法の総称です。従来のようにパスワードをサーバーに保存したりユーザーが入力したりするのではなく、図 1 のように、秘密鍵は利用者端末の安全な領域（Secure Enclave や TPM など）に保持し、サーバーには対応する公開鍵のみを保存します。

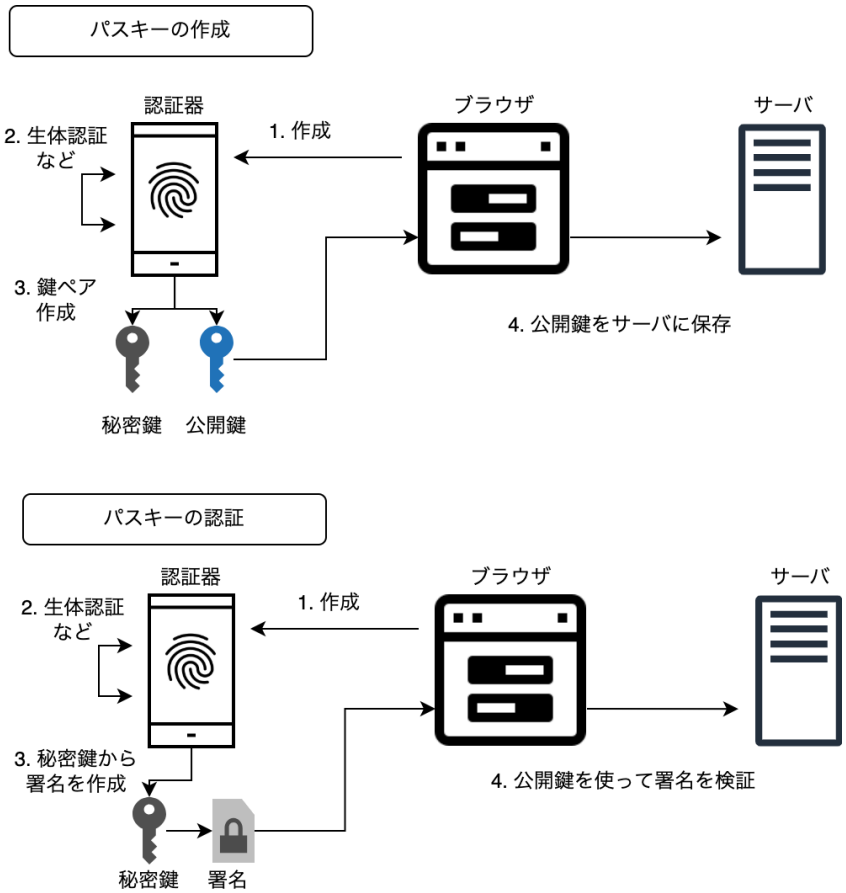



図 1. パスキーの利用フロー

パスキーでは、端末に保存された秘密鍵を利用できる状態にするために、指紋や顔認証などの生体認証や PIN ロックなどが用いられます。ユーザーは「指紋を当てる／顔を向ける」といった簡単な操作で本人確認を行い、その上で秘密鍵によって署名を作成すること

でログインが成立するため、「覚えなくてもいい」「入力しなくてもいい」 という利便性の高さが特徴です。

パスワードによる認証と大きく異なるのは、サーバー側に「秘密鍵」が残らない設計です。仮にサーバーが攻撃を受けたとしても、漏えいリスクは「公開鍵のみ」なので、ユーザーが使う秘密鍵が盗まれることはありません。そのためパスワードリスト攻撃や総当たり攻撃も成立しにくく、根本的に安全性を高められます。

### 6.6.2 パスキーとフィッシング耐性について

パスキーはフィッシング攻撃にも非常に強い耐性を持っています。その理由の一つとして、認証器（端末）に登録されたクレデンシャルが「当該サイトの正規ドメイン」と紐付いている点が挙げられます。具体的には、パスキー登録時にメタデータとしてドメイン情報を保持し、認証時にはアクセス先のドメインが一致しない限り署名が行われません。この仕組みにより、不正なドメインへのアクセスでは認証が拒否されるため、攻撃者がフィッシングで情報を盗むことが困難になります。

例えば、フィッシングサイトが正規サイトに似せたデザインを用意していたとしても、URL（ドメイン名）が異なるため、パスキーの認証フローでは簡単に弾かれてしまいます。結果として、誤ったドメインへのアクセスでは認証処理が失敗し、ユーザーが万が一リンクをクリックしてしまった場合でも、パスワードや認証情報を入力させられるリスクを大幅に減らすことが可能です。

従来のフィッシング攻撃では、ユーザーにパスワードや認証情報を入力させ、それを盗み取る手口が主流でした。しかしパスキーでは、ユーザーが何らかの文字列を入力する場面自体が存在せず、端末内に保存された秘密鍵を使用して署名を行う仕組みになっています。この構造上、そもそも盗まれるべきパスワードが存在しない状態を作り出しており、フィッシング攻撃の成立可能性を大幅に低下させています。

さらに、Yahoo! Japan ではパスワード認証を無効化する機能を導入しています。これにより、パスキー認証と組み合わせてより強固な認証環境を実現しています。このように、パスキーの導入に加えて、既存のパスワード認証を排除する施策を同時に進めることで、ユーザー体験の向上とセキュリティの強化を両立する取り組みが広がっています。

### 6.6.3 パスキーの浸透状況

パスキーの普及が進んだ背景には、OSやブラウザーなど各プラットフォームによる標準対応が挙げられます。Windows、macOS、iOS、Android といった主要 OS がパスキーをネイティブでサポートし、Google Chrome、Safari、Firefox といったブラウザーでも利用可能になりました。これにより、多くのユーザーがパスキーを身近な認証手段として利用できる環境が整備されつつあります。

さらに、スマートフォン同士やスマートフォンと PC との間でパスキーを同期できる仕組みも、普及を後押ししています。例えば、Apple の iCloud や Google パスワードマネージャーを活用することで、複数の端末間でシームレスにログインが可能となり、ユーザーの利便性が大幅に向上しました。これに加えて、1Password や Dashlane などのサードパーティ製パスワードマネージャーもパスキーの保存と同期をサポートするようになり、異なるプラットフォームを利用するユーザーでも統一的な体験が得られるようになっています。

こうした技術的進化に加え、iOS や macOS のエコシステムでは、ログインフォームに自動的にパスキーを入力する Passkey Autofill 機能が導入されています。この仕組みにより、ユーザーはフォーム上に自動的に表示される候補からパスキーを選択するだけで、簡単にログインを完了することができます。このような直感的な体験が一般ユーザーにも広がり、パスキーの利便性がさらに高まっています。

一方で、Google のプラットフォームでも、Google Password Manager を通じてパスキーの保存と同期が可能となり、Android 端末や Chrome ブラウザーを利用するユーザーにも同様の利便性が提供されています。これらの進化により、異なるプラットフォーム間であっても一貫したログイン体験が少しずつ実現されつつあります。

すでに海外の大手 SNS や EC サイト、国内の金融系サイトなどでも、パスキーを用いたログインを導入する動きが見られます。NTT ドコモ社およびメルカリ社などが報告しているように、パスキー実装後はなりすましや不正アクセス被害が大幅に減少したという事例もあり、ユーザー体験とセキュリティを両立できる手段として注目されています。

さらに、認証器がない PC でもスマートフォンのパスキーを活用する「Hybrid」方式（QR コードと BLE の組み合わせ）を用いることで、シームレスにログインできる仕組みが整備されています。これらの技術的な進化と UI/UX の洗練が進むことで、ユーザーが「パスワードを入力しない」体験が当たり前になる未来が、すでに現実のものとなりつつあります。

＜参考文献＞

えーじ, 倉林 雅, 小岩井 航介著:『パスキーのすべて』, 技術評論社, 2025.

『ドコモが「パスキー」を導入してフィッシング被害報告が 0 件に　パスワードレス認証の効果』（ITmedia）
https://www.itmedia.co.jp/mobile/articles/2312/09/news060.html

『メルカリ FY202. 6 インパクトレポート』（株式会社メルカリ）
https://pj.mercari.com/impact-report/FY2024_6_ImpactReport_JP.pdf

【松本 悦宜　Capy 株式会社】

# 7. まとめ

毎年作成される本フィッシングレポートは、フィッシング対策協議会 事務局や技術・制度検討 WG メンバーによる寄稿をもとに、フィッシングの動向や関連する最新情報をまとめたものです。本年度も注目すべきトピックが多数掲載されています。

3 章「フィッシングの被害」では、QR コードを利用した偽サイトへの誘導手法について紹介されています。また、4 章では SMS を用いたフィッシング詐欺に関する意識調査の結果を解説しており、現状を把握する上でぜひご一読いただきたい内容です。

利用が終了したドメイン名の悪用については、2024 年にも報道されました。本レポートでは、5 章においてドメイン名の廃止・利用終了に関する注意点をまとめています。

6 章「トピック」では、送信メールドメイン認証技術「DMARC」に関するガイドラインや導入状況の調査結果を取り上げています。また、ユーザー認証に関しては、米国 NIST の「SP 800-63-4」や「PCI DSS」などの基準がパスワード要件の検討に有益である点に触れています。さらに、パスワードマネージャーのメリットや注意点、新たなワンタイムパスワードの方式、パスキーのフィッシング耐性に関する議論など、注目すべきテーマも多く掲載されています。

本レポートが、フィッシング対策に取り組む企業・組織の担当者のみならず、フィッシング対策に関心を持つすべての方に届き、現状の理解を深めるとともに、総合的な対策やその在り方についての議論の一助となることを願います。末筆ながら、ご寄稿くださった技術・制度検討 WG メンバーの皆さま、また取りまとめに尽力された事務局の方々に深く感謝申し上げます。

【木村泰司　技術・制度検討 WG 主査】

# 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・五十音順）

【主査】

| | |
|---|---|
| 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 |

【構成員】

| | |
|---|---|
| 阿部 巧 | 株式会社三井住友銀行 |
| 植松 太郎 | 株式会社クリーマ |
| 大石 哲生 | 株式会社クリーマ |
| 大谷 昭彦 | 株式会社三菱 UFJ 銀行 |
| 小椋 陽平 | 株式会社クリーマ |
| 笠間 英宏 | NTT コミュニケーションズ株式会社 |
| 加藤 孝浩 | TOPPAN エッジ株式会社 |
| 加藤 雅彦 | 順天堂大学 |
| 金井 孝三 | Sky 株式会社 |
| 唐沢 勇輔 | Japan Digital Design 株式会社 |
| 杉山 明男 | 株式会社クローバーネットワークコム |
| 鈴木 伸吾 | 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 |
| 鈴木 智也 | LRM 株式会社 |
| 竹内 司 | 株式会社みずほフィナンシャルグループ |
| 塚田 晴史 | 株式会社マクニカ |
| 坪井 祐一 | エヌ・ティ・ティ・コミュニケーションズ株式会社 |
| 野々下 幸治 | 株式会社アイエスエフネット |
| 平塚 伸世 | 一般社団法人 JPCERT コーディネーションセンター |
| 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 |
| 藤井 達朗 | 株式会社クリーマ |
| 藤井 治彦 | バンクガード株式会社 |
| 逸見 智弘 | 株式会社クローバーネットワークコム |
| 星加 匡人 | 株式会社みずほフィナンシャルグループ |
| 増田 亮 | KDDI 株式会社 |
| 松尾 佳彦 | 株式会社日本レジストリサービス |
| 松本 悦宜 | Capy 株式会社 |
| 森 三千代 | 株式会社みずほフィナンシャルグループ |
| 八子 浩之 | 株式会社みずほフィナンシャルグループ |
| 尹 慈明 | SBI EVERSPIN 株式会社 |

【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
みずほリサーチ＆テクノロジーズ株式会社