デジタル署名者 : Council of Anti-Phishing Japan
DN : c=JP, st=Tokyo, l=Chuo, serialNumber=AATL20251120423868, o=Council of Anti-Phishing Japan, cn=Council of Anti-Phishing Japan, email=antiphishing-sec@jpcert.or.jp
日付 : 2026.05.29 13:41:22 +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 2026

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 3
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 検知回避テクニックと誘導のバリエーション 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 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）＞ 14
◆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 17

3.1 ボイスフィッシングの増加と脅威について 17

4. SMS を用いたフィッシング詐欺についての意識調査 19

5. ドメイン名関連 32

5.1 ドメイン名の廃止・利用終了にあたっての注意 32
5.1.1 ドメイン名廃止のリスク 32
5.1.2 ドメイン名を廃止する前に注意して欲しいこと 32
5.1.3 ドメイン名の管理ルール・手順の確立 33
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 33
5.1.5 自組織のサブドメインを利用終了する際の注意 33
5.2 ICANN による gTLD 追加募集 33
5.2.1 gTLD の追加募集とは 34
5.2.2 gTLD 追加募集のスケジュール 35
5.2.3 申請条件 36
5.2.4 RSP 評価プログラム 36

6. トピック 37
6.1 DNSSEC, DMARC によるドメイン名の信頼性の向上～.BANK の事例～ 37
6.2 日本証券業協会によるフィッシング詐欺防止に向けた取り組みについて 39
6.2.1 証券業界における「インターネット取引における不正アクセス等防止に向けたガイドライン」（2021 年 3 月）制定までの経緯 39
6.2.2 2025 年初に発生した不正アクセス・不正取引等を受けての業界としての対応 39
6.2.3 改正ガイドライン（2025 年 10 月）の主な改正点（技術面） 40
6.2.4 改正ガイドライン（2025 年 10 月）におけるメール等の取り扱いについて（フィッシング詐欺等被害未然防止のための措置） 41
6.3 「今すぐできるフィッシング対策」のコンテンツ紹介 43
7. まとめ 44

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「サイバーセキュリティ経済基盤構築事業（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、2025 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依然として高水準で推移しました。また、フィッシングの報告件数も前年上半期比で約 56 万件（約 89%）増加したほか、インターネット上には犯罪実行者募集情報が氾濫するなど、極めて深刻な情勢が継続しています。2025 年上半期におけるフィッシング報告件数は 119 万 6,314 件、インターネットバンキングに係る不正送金事犯の被害総額は約 42 億 2,400 万円に及んでいます。

フィッシング情報の届け出件数について、2025 年は 3 月にこれまでで最大の報告件数を記録するなど、年間を通じて多くの報告がありました（図 1-1）。広く報道のあった証券会社のほか、キャッシュレス決済サービス、クレジットカード会社、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。

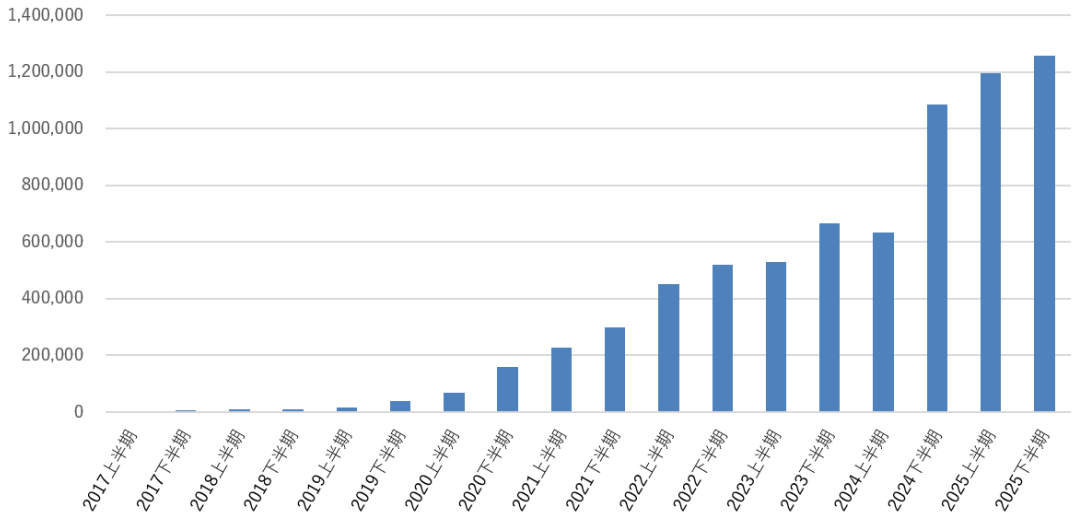


図 1-1 国内のフィッシング情報の届け出件数 [2]

フィッシングサイトの URL 件数は、2025 年は上半期・下半期ともピークより下回っているものの高止まりの傾向が続いています。（図 1-2）。ブランド名を悪用され

1 警察庁、令和 7 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/R7kami/R07_kami_cyber_jyosei.pdf）（閲覧日：2026 年 2 月 20 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 5 月 22 日）より作成

た企業の件数は、2024 年に若干の減少傾向がみられたものの、2025 年は再び増加傾向となっています（図 1-3）。

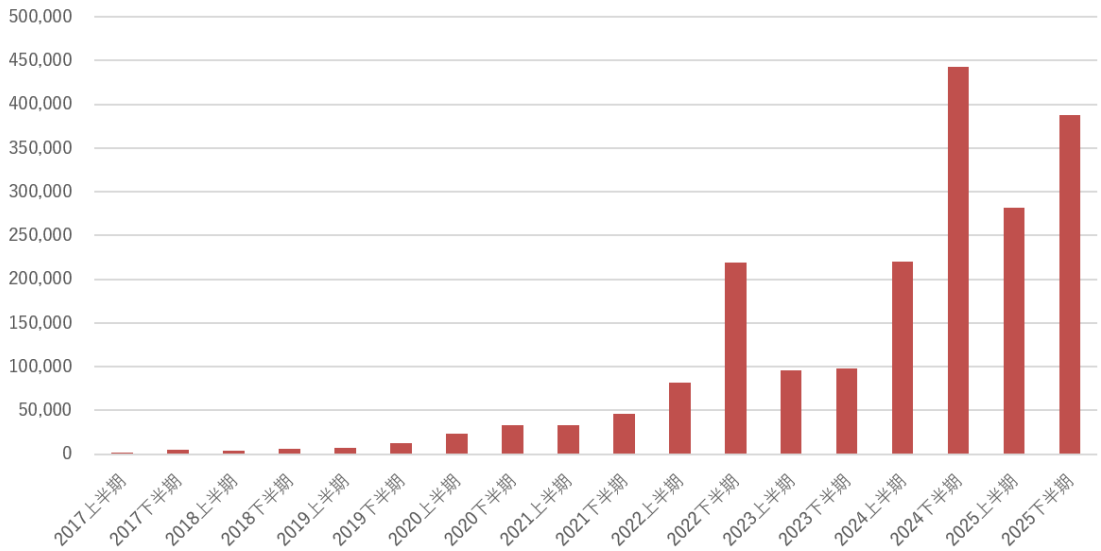


図 1-2　国内のフィッシングサイトの件数

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、2025 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 2024 年と比較して減少しました（図 1-4）。2025 年の手口別内訳では、2024 年に比べて、「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、「フィッシングサイトにより入手」が増加しました（図 1-5）。

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.npa.go.jp/bureau/cyber/pdf/R080312_access.pdf）

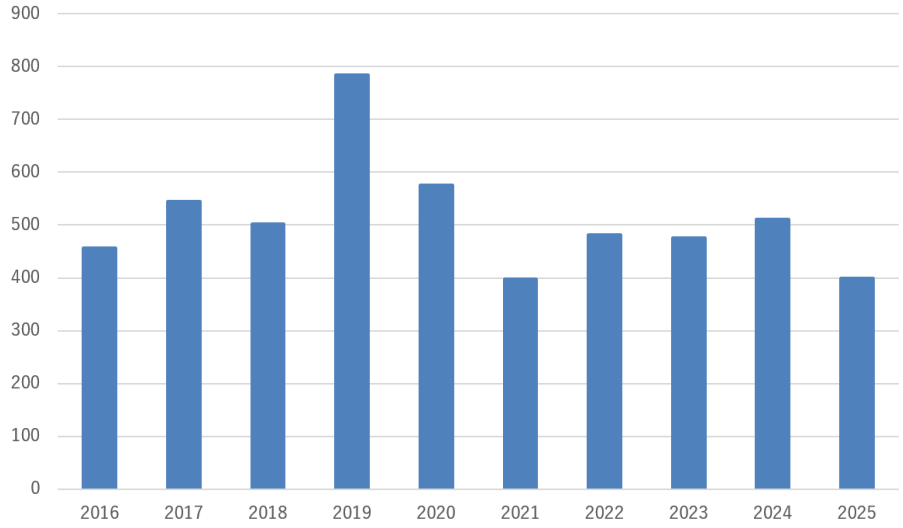


図 1-4　識別符号窃用（ID 窃盗）型不正アクセス行為の検挙件数 [4]

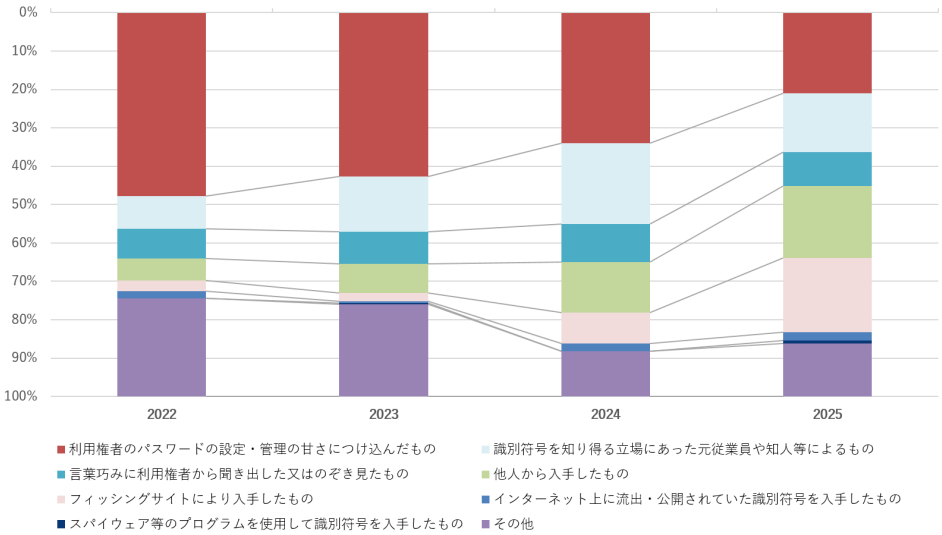


図 1-5　識別符号窃用型不正アクセス行為の手口別検挙件数の内訳
（2022 年～2025 年）[5]

【みずほリサーチ＆テクノロジーズ株式会社】

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

4 同上より作成
5 同上より作成

ものの、下げ止まりの状況となっています。2025 年のフィッシング届け出件数は 2024 年と比較して若干減少となりました（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、2025 年は下期に増加へ転じています（図 1-8）。APWG の報告 [6]によると、ソーシャルメディアおよび SaaS/Web メールが 2025 年に最も頻繁に攻撃されたセクターであり、2025 年第 4 四半期にはフィッシング攻撃全体の 20.3%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、四半期ごとに 30～40%の安定した増加を示しているとしています。

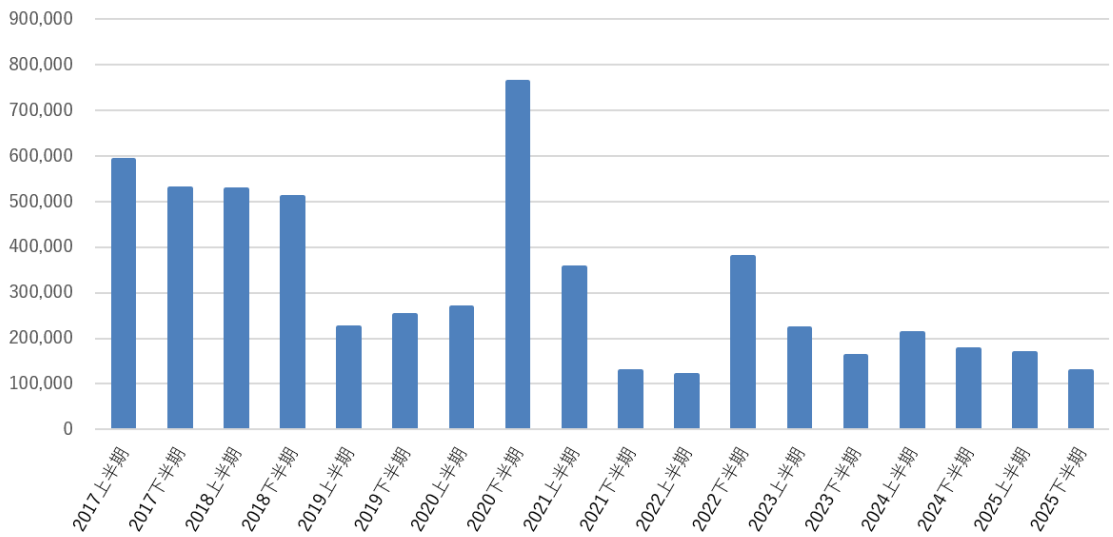


図 1-6　APWG へのフィッシングメール届け出件数 [7]

6 APWG（Anti-Phishing Working Group）、"Phishing Activity Trends Report"（https://apwg.org/trendsreports/）（閲覧日：2026 年 5 月 22 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：2026 年 5 月 22 日）

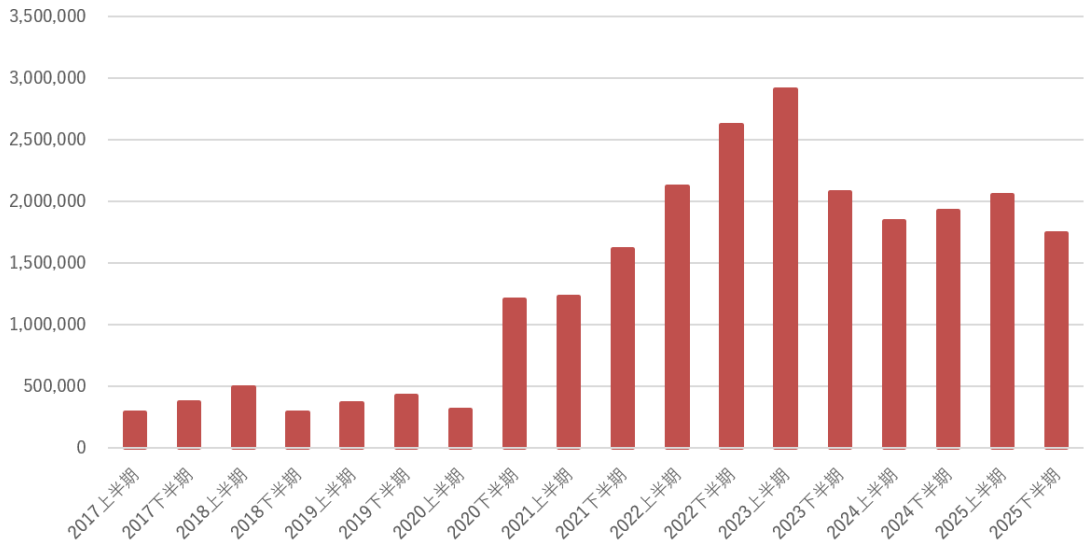


図 1-7　フィッシングサイトの件数（APWG）[8]

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：2026 年 5 月 21 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 2025 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 2,454,297 件となり、2024 年と比較して約 1.43 倍となりました。

また、3 月は報告件数が約 25 万件となり、月ベースでも過去最多件数を更新しました。報告件数は高止まりしており、引き続き注意が必要です。

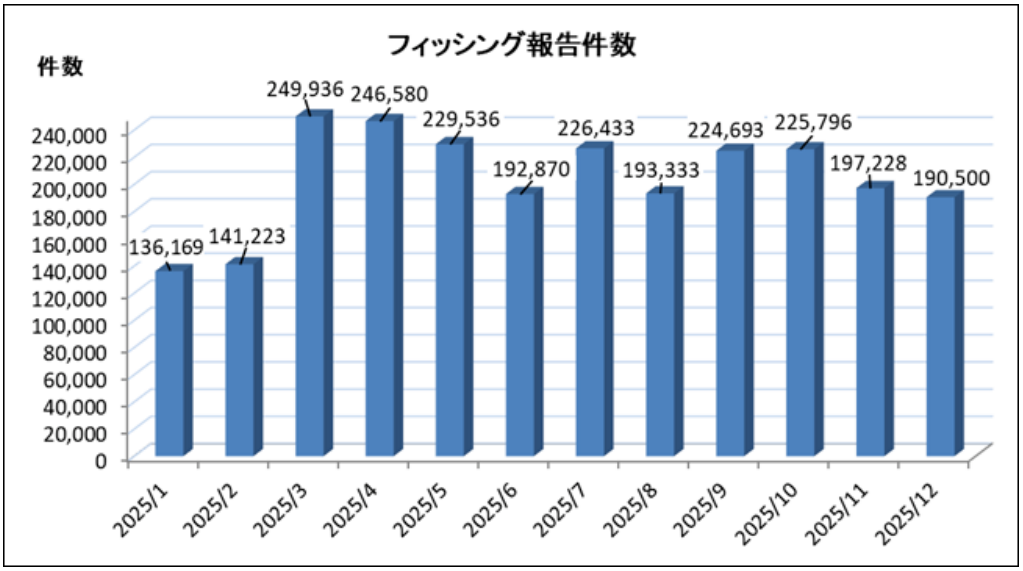


図 9　2025 年フィッシング報告件数の推移

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

2025 年にフィッシングでかたられたブランド数は 229 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 37 ブランド、金融系 36 ブランド、証券系 21 ブランド、通信事業者・メールサービス系 20 ブランド、オンラインサービス系 20 ブランド、EC 系 16 ブランド、決済サービス系 13 ブランド、仮想通貨系 10 ブランド、配送系 7 ブランド、その他 49 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。2025 年では、証券会社をかたるフィッシングで詐取した情報を使用して証券口座を乗っ取り、株価操縦を行うことで利益を得るという手口により、不正取引被害額は約 7,393 億円規模 [10]となりました。事業者が多要素認証の設

[10] 金融庁「インターネット取引サービスへの不正アクセス・不正取引による被害が急増しています」
https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html

定必須化を決定するなど対策を進めた 6 月以降は減少したものの、引き続き発生しています。

1.3.2 検知回避テクニックと誘導のバリエーション

2025 年も、メールフィルターなどのセキュリティ機能による検知を回避するため、またフィッシングサイトへ誘導するための件名や本文の工夫など、さまざまな手法が確認されています。攻撃者は複数の回避手法を組み合わせつつ、効果が確認された手法を繰り返し使用しています。

（1） 正規サービスを悪用したリダイレクト

Google 翻訳の URL をリダイレクト元として利用し、セキュリティ製品による URL スキャンを回避しようとする手法が確認されています。さらに、amazonaws.com（AWS）や sendgrid.com／sendgrid.net など、信頼性の高いドメイン名を URL に含めることで、不審性を低減させるケースも見られます。

（2） 文字列の細工

URL やメール本文に「〇」「□」などの囲み文字や、Unicode 文字（斜体、太字など）を混在させるほか、GBK など日本語以外の文字コードを意図的に使用することで、解析ツールの文字列パターンマッチングを回避する手法です。

（3）URL およびメール文面の難読化

URL における BASIC 認証形式の悪用や、HTML 内への大量の非表示文字列（いわゆるゴミ文字）の挿入により、解析を妨害する手法が確認されています。また、一部のメールアプリでは不完全な書式の URL であっても自動的にリンク化される仕様を悪用する事例も見られます。

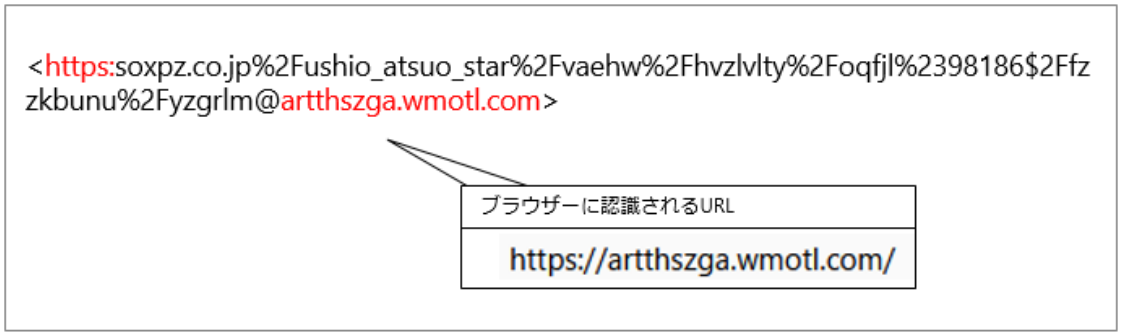


図 9 不完全な書式が使われていてもリンクとして扱ってしまう例

フィッシングメールの受信後、利用者に誤認させるため、実在のサービスで使用されていそうな画面や文面を用いるケースが増加しています。多くは「セキュリティ向上」「不正利用への対応」「本人確認」などを名目としていますが、「ポイントプレゼント」といった文面では、利用者のお得感につけ込み、警戒心を緩めることを狙っています。また、証券会社をかたる事例では、事業者側の対策状況に応じて「多要素認証の再設定」や「補償手続き」など、実際に事業者が発信する案内に酷似した文面を用い、その信頼性を逆手に取って誘導しています。

1.3.3 「なりすまし」送信メールの状況について

2 月には、なりすまし送信メールが全体の約 69.0%に急増し、3 月も高水準で推移した結果、過去最高の報告件数を記録する一因となりました。これらの攻撃では、DMARC ポリシーが「none（監視のみ）」に設定されている、あるいは未設定のドメインが選別され悪用されていました。しかし、10 月以降はその割合が約 27.0%まで大幅に減少しました。これは、9 月に総務省が通信事業者に対して DMARC 対応を要請したことを受け、攻撃者が DMARC 認証の失敗による検知を回避する動きを強めた可能性があります。その結果、年後半には独自ドメイン（非なりすまし）を用い、DMARC 認証を通過させることで迷惑メールフィルターを回避しようとする試みが急増しました。12 月には、この手法が全体の約 75.3%を占めるに至っています。

2025 年は、なりすまし送信メールが増加する一方で、DMARC や BIMI といった技術がメールセキュリティの基本要件として改めて強く求められた年となりました。攻撃者が検知回避のため独自ドメインへと手法をシフトさせる状況を踏まえると、今後は単に送信ドメイン認証技術を実装するだけでなく、BIMI などを活用して「正規メールの視認性を高める」取り組みが、事業者にとってブランド保護の観点から不可欠になると考えられます。

【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、月間 20 万件を超える水準で推移するなど、引き続き極めて高い状況にあります。証券口座の乗っ取りといった高額被害の発生や、生成 AI を活用した巧妙な攻撃の増加など、脅威の質も変化しています。技術・制度検討 WG で制作しているフィッシング対策ガイドラインおよびフィッシングレポートは、こうした最新の動向を的確に捉え、サービス事業者をはじめとする関係者の皆さまにとって実践的かつ活用しやすい内容とすることで、被害低減に資することを目指しています。

今年度、技術・制度検討 WG では、ガイドラインの内容をより多様な読者層に届けるための工夫として、利用者向けガイドラインの中から、特にわかりやすさと伝わりやすさに配慮したコンテンツ「今すぐできるフィッシング対策」を新たに作成しました。運営副委員長の唐沢勇輔氏が中心となってまとめられています。

また、フィッシング対策に関わる制度的な取り組みについて詳しい松本泰氏をお招きし、EU におけるフィッシング対策の動向や取り組みについてお話を賜り、ディスカッションを行いました。国際的な視点を取り入れながら議論を深めたことは、本 WG の活動にとって大きな意義があったと考えています。

事務局については、昨年度に引き続き、みずほリサーチ＆テクノロジーズ株式会社にご担当いただきました。円滑な WG 運営と資料作成が実現しております。

今後も、技術動向や制度環境の変化を踏まえつつ、実効性のある情報発信を行ってまいります。読者の皆さまにおかれましては、フィッシング対策ガイドラインおよびフィッシングレポート、そして「今すぐできるフィッシング対策」をご活用いただき、フィッシング被害の抑止に向けた取り組みにお役立ていただければと思います。

【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】

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。

2025 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（2025/7/4、2026/4/17 開催）

＜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：2025/7/4：66 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をしています。

・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 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。

これまでの活動としては、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。

2025 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。

・SSL/TLS サーバー証明書における WHOIS 情報を利用したドメイン名使用権確認方法の廃止について を公開（2025/5/8 公開）

SSL/TLS サーバー証明書発行に必要な手続きとして一般的であった WHOIS 情報の利用が廃止されるため、SSL/TLS サーバー証明書の継続的な利用にあたり、本変更内容の詳細について解説

（https://www.antiphishing.jp/report/wg/cert_explaindoc_20250508.html）

・SSL/TLS サーバー証明書における 有効期間短縮化について を公開（2025/8/19 公開）
サーバー証明書の有効期間を短縮する目的について解説
（https://www.antiphishing.jp/report/wg/cert_explaindoc_20250819.html）

・送信ドメイン認証技術導入実施状況について を公開（2025/9/16 公開）
一般財団法人日本データ通信協会の迷惑メール相談センターが実施した「送信ドメイン認証実施状況」をもとに、各プロバイダー（ISP）、CATV（ケーブルテレビ）、モバイル事業者、フリーメール事業者における導入・設定状況について集計した結果
（https://www.antiphishing.jp/report/wg/cert_20250916.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 [11]。

2025 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 2025』の応募作品の中から「ポスター」部門における優秀賞を選出し、表彰しました。

[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）
STOP THINK CONNECT Web サイト
（https://stopthinkconnect.jp/）

◆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。

2025 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。

- Phishing as a service
- フィッシング報告状況
- 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
- 「スミッシングの実態と対策」から論文化
- フィッシング詐欺/対策への AI 導入
- 先行研究論文の調査
- フィッシング対策勉強会（2026 年 1 月 28 日開催）
  - 「証券業界を狙うフィッシンググループ動向について」
  - 「証券口座乗っ取り事案における分析観点について」
  - 「証券業界での絵文字認証の一般的効果」

◆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。

2025 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。

・詐欺サイト対処机上演習 WG サポート詐欺対応演習を開催（2025 年 7 月 30 日）

「詐欺サイト対処机上演習　実際の詐欺音声を使ったサポート詐欺対策編」を、Daigas グループにて開催。実際のサポート詐欺の通話音声を用いた体験型の演習。「家族がフィッシングメールに騙されて情報を提供してしまった」、「フィッシングサイトに表示された電話番号へ電話してしまった」という設定で、講師からの説明と、グループでの議論・発表を行いました。

・Security Days Fall 2025 登壇（2025 年 10 月 23 日）
題目：「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」
講演者：林 憲明 氏（詐欺サイト対処机上演習 WG 主査 / トレンドマイクロ株式会社 プリンシパルエンジニア）
会場：JP タワーホール＆カンファレンス（KITTE 4F）

・Internet Week 2025｜詐欺サイト対処机上演習を開催（2025 年 11 月 26 日）
題目：詐欺サイト対処机上演習＋社内セキュリティ意識向上と行動変容へ向けた皆様
み
講演者：
林 憲明(フィッシング対策協議会／トレンドマイクロ（株），詐欺サイト対処机上演習 WG 主査／ プリンシパルセキュリティアナリスト)
中西 拓実(明治安田生命保険相互会社 リスク管理統括部（サイバー・システムリスク統括担当））
会場：KFC Hall＆Rooms

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）

◆フィッシング詐欺啓発活動企画＜主査：加藤孝浩氏（TOPPAN 株式会社）＞

・協議会設立 20 周年記念セミナー、記念式典の開催

フィッシング対策協議会は、2005 年にフィッシングをはじめとするオンライン犯罪の増加を予見し、関係者が情報交換を行い、また被害状況に応じた対策を推進するという目的で発足し、今年で 20 周年を迎えました。この節目を記念し、関係者の皆さまへ感謝をお伝えするとともに、これからのフィッシング対策に向けて新たな一歩を踏み出すための記念セミナーと記念式典を開催いたしました。

記念セミナーでは、20 年の協議会活動の振り返りとこれからの 10 年についてのパネルディスカッションを行い、フィッシング詐欺に関連する法執行機関、金融機関、学術機関などから有識者をお招きし、フィッシングの傾向と、その対応策などを紹介しました。また、会場にはフィッシング対策サービスや各種ソリューションのブース展示も行いました。

・フィッシング対策協議会 20 周年記念セミナー　（2025 年 11 月 14 日開催）
　会場：赤坂インターシティコンファレンス　the Air　＋　Webex ウェビナー
　参加者数：合計 595 名（会場参加 179 名、オンライン参加 416 名）
　（https://www.antiphishing.jp/news/event/antiphishing_seminar2025.html）

【加藤 孝浩　TOPPAN 株式会社】

3. フィッシングの被害

3.1 ボイスフィッシングの増加と脅威について

フィッシング詐欺の手口は多様化・巧妙化していますが、特に 2024 年秋頃から「ボイスフィッシング」が増加しています。

ボイスフィッシングはビッシング（Vishing = Voice（ボイス）+ Phishing（フィッシング））とも呼ばれ、電話を悪用する詐欺手口です。代表的なケースでは、銀行を装った偽電話を企業の代表電話にかけ、「インターネットバンキングの電子証明書の更新が必要」「更新用のリンクを送りたい」などともっともらしい口実を用いて、担当者のメールアドレスを聞き出し、個別のフィッシングメールを送り付けます。個別のメールには聞き出した担当者自身の名前や部署名の記載があり本物の案内のように見えてしまい、さらに、フィッシングメール（SMS 含む）を起点として偽の電話番号へ誘導され、電話で信用させながらフィッシングサイトに認証情報などを入力させるため、正規の手続きだと誤認しやすくなります。

■手口の概要（一例）

1. 攻撃者が、銀行や金融関係団体を騙り、企業の代表電話をかけ、担当者のメールアドレスを聞き出す。
2. 攻撃者が担当者にフィッシングメールを送信し、電話で指示しながらフィッシングサイトに誘導し、インターネットバンキングのアカウント情報等を入力させて盗み取る。
3. 電話で指示しながらリアルタイムにワンタイムパスワードもフィッシングサイトに入力させて盗み取る。
4. フィッシングサイトに入力させたアカウント情報とワンタイムパスワード等を使って、攻撃者が法人口座から資産を不正に送金する。

この手口の危険性は、フィッシングメールが担当者への個別のメールであることに加え、音声というコミュニケーション手段の特性にあります。電話では相手の声や話し方から「実在の担当者らしさ」を感じやすく、緊急性を強調されることで冷静な判断が難しくなり、直接会話を通じて心理的に追い込まれるため、だまされやすい状況が生まれやすくなっています。

対策としては、「SMS やメールに記載された電話番号には絶対に電話をかけない」ことです。緊急性を強調されても、まずは落ち着き、自身が実際に利用しているサービスの公式サイトを確認し、そこに掲載されている正規の連絡先へ問い合わせる必要があります。また、「電話で認証コードを教えて欲しい」と求められた場合は、詐欺を強く疑うべきです。正規の事業者が電話でワンタイムパスワードや暗証番号を尋ねることはありません。

万が一、インターネットバンキングの認証情報やカード情報を伝えてしまった場合は、速やかに金融機関やカード会社などへ連絡し、利用停止等の措置を講じることが不可欠です。さらに、不審に感じた時点で警察など第三者へ相談することも有効な被害防止策となります。

フィッシング詐欺は、ブランドの悪用拡大や手口の高度化により、今後も形を変えて継続することが予想されます。ボイスフィッシングもその一環として、利用者の心理的隙を突く攻撃であることを認識しなければなりません。利用者一人ひとりが「電話であっても安易に信用しない」という意識を持ち、公式情報を自ら確認する習慣を徹底することが被害防止の鍵となります。

【加藤 孝浩　TOPPAN 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、5,338 名から回答を得ました。今回の調査より、回答者のインターネット利用環境（主に使用する端末や利用時間）に関する設問を新たに追加しています。以下、調査結果のポイントについて紹介します。

Q1. インターネットを利用する場合に最もよく使用する端末はどれですか？

		スマートフォン（iPhone）	スマートフォン（Android）	タブレット（iPad など）	ノート PC	デスクトップ PC	その他
全体(n=5338)		30.1	35.4	2.3	20.2	11.9	0.0
男性(n=2657)		25.6	35.3	1.6	21.2	16.3	0.0
	10 代(n=366)	32.2	59.0	1.1	4.4	3.3	0.0
	20 代(n=379)	49.9	35.9	2.4	5.0	6.9	0.0
	30 代(n=388)	31.2	38.7	1.8	15.2	13.1	0.0
	40 代(n=387)	26.1	34.1	2.8	18.6	18.3	0.0
	50 代(n=385)	16.6	32.5	1.6	28.1	21.0	0.3
	60 代(n=377)	15.1	26.0	0.8	31.3	26.8	0.0
	70 代以上(n=375)	8.0	21.9	0.8	45.3	24.0	0.0
女性(n=2681)		34.7	35.5	3.1	19.2	7.5	0.0
	10 代(n=386)	47.2	49.0	2.1	1.3	0.5	0.0
	20 代(n=383)	66.3	29.0	2.1	0.8	1.8	0.0
	30 代(n=389)	47.6	39.6	2.3	6.9	3.6	0.0
	40 代(n=372)	28.2	48.1	2.2	15.1	6.5	0.0
	50 代(n=391)	22.5	32.7	3.6	32.0	9.2	0.0
	60 代(n=378)	18.8	27.8	3.7	36.5	13.2	0.0
	70 代以上(n=382)	11.5	22.8	5.5	42.4	17.8	0.0

インターネットを利用する際のメイン端末について調査したところ、「スマートフォン（iPhone）」が 30.1%、「スマートフォン（Android）」が 35.4%となり、あわせて 65.5%がスマートフォンを主たる利用端末としていることが分かりました。年代別に見ると、10 代、20 代の若年層ではスマートフォンの利用比率が圧倒的に高く、特に 10 代女性では iPhone と Android を合わせると 9 割を超えています。SMS を用いたフィッシング詐欺は、スマートフォン利用者を主な標的としています。PC と比較して画面が小さく

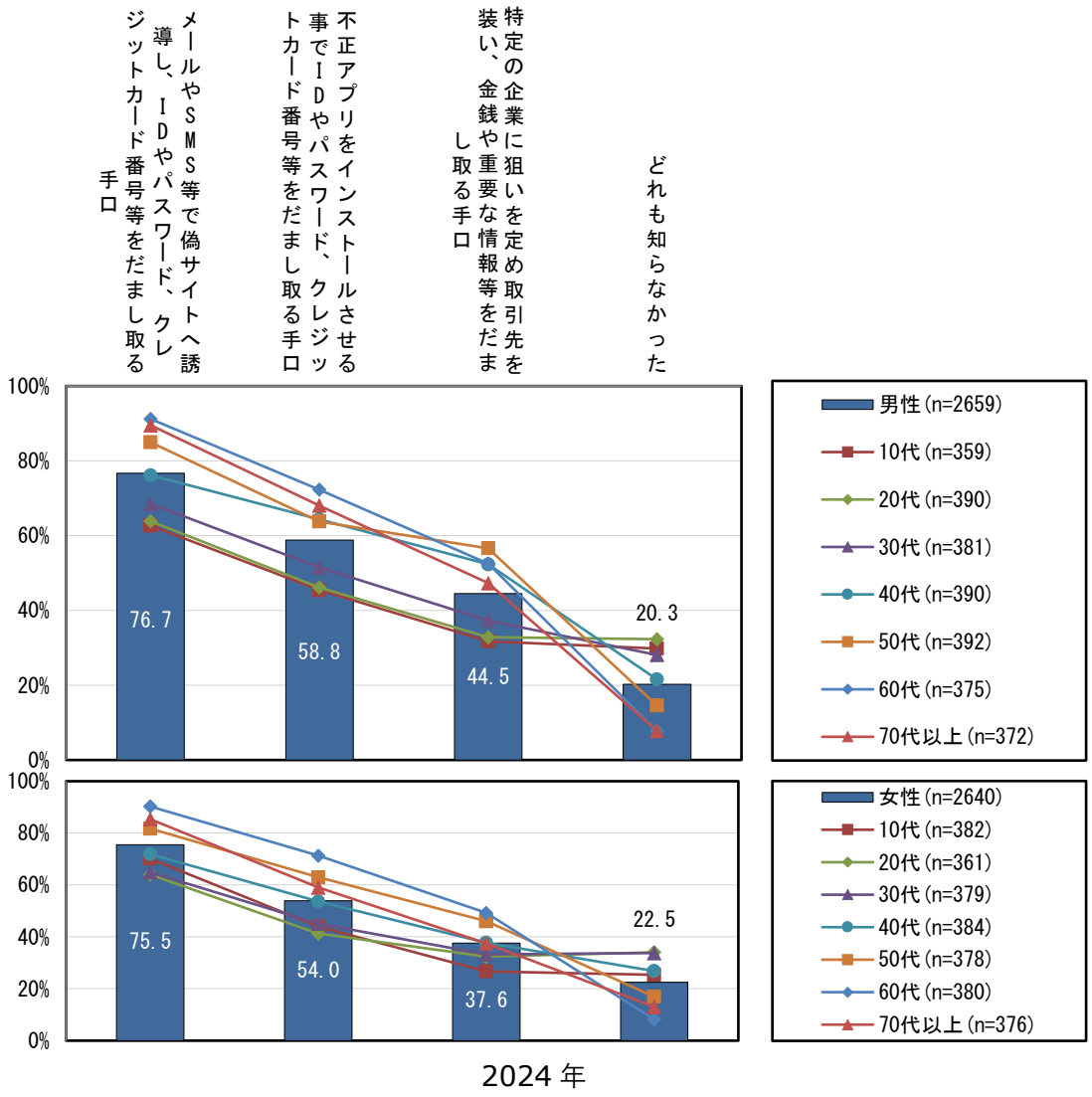
URL の全体像を確認しづらい点や、SMS 通知から即座にアクセスしやすい環境にあることが、フィッシング詐欺の脅威を高める背景の一つとなっています。

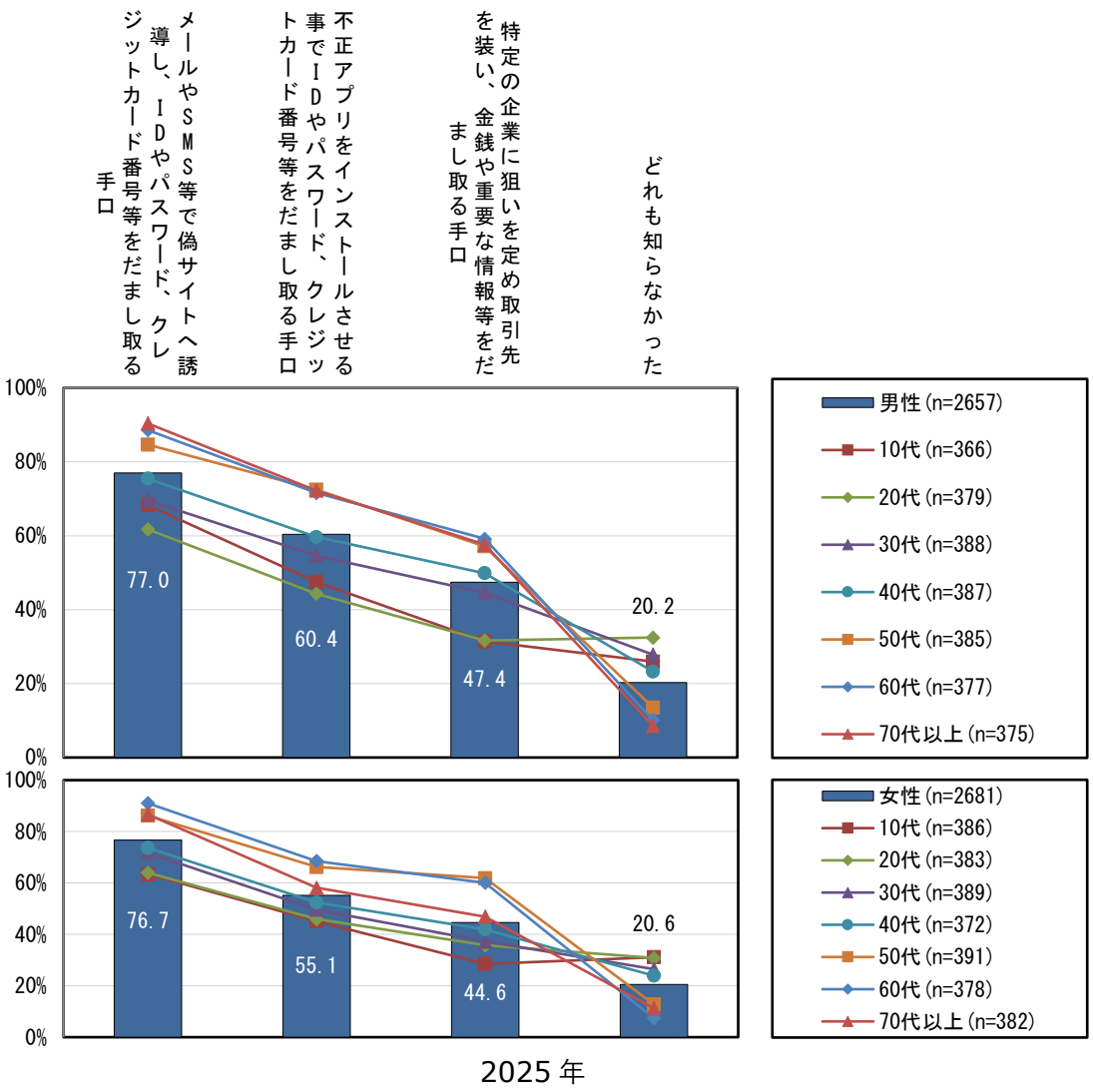
Q2. 1 日あたりの平均的なインターネット利用時間をお聞かせください。

			全体	1 時間未満	1～3 時間未満	3～5 時間未満	5～8 時間未満	8 時間以上
全体(n=5338)		%	100.0	13.4	36.2	25.4	14.0	11.0
男性(n=2657)		%	100.0	13.5	35.2	25.1	13.3	12.9
	10 代(n=366)	%	100.0	7.4	21.0	34.4	20.8	16.4
	20 代(n=379)	%	100.0	9.8	31.1	28.0	14.5	16.6
	30 代(n=388)	%	100.0	11.6	31.7	23.7	17.3	15.7
	40 代(n=387)	%	100.0	15.8	35.4	23.8	11.9	13.2
	50 代(n=385)	%	100.0	17.7	43.1	18.7	9.6	10.9
	60 代(n=377)	%	100.0	15.9	41.4	23.3	9.0	10.3
	70 代以上(n=375)	%	100.0	16.0	41.9	24.5	10.1	7.5
女性(n=2681)		%	100.0	13.3	37.3	25.7	14.7	9.0
	10 代(n=386)	%	100.0	7.3	18.9	31.3	28.2	14.2
	20 代(n=383)	%	100.0	8.9	30.3	29.2	17.2	14.4
	30 代(n=389)	%	100.0	16.7	36.2	25.4	11.8	9.8
	40 代(n=372)	%	100.0	16.7	41.9	19.9	12.1	9.4
	50 代(n=391)	%	100.0	12.3	43.2	25.3	12.5	6.6
	60 代(n=378)	%	100.0	13.0	46.6	25.7	10.1	4.8
	70 代以上(n=382)	%	100.0	18.6	44.5	22.5	10.5	3.9

1 日あたりのインターネット利用時間（SNS、動画視聴、ブラウザー、アプリ、ゲーム等含む）については、「1 時間～3 時間未満」が 36.2%で最も多く、次いで「3 時間～5 時間未満」が 25.4%となりました。「5 時間以上」（「5 時間～8 時間未満」と「8 時間以上」の合計）のヘビーユーザー層も 25.0%存在し、1 日の起きている時間の多くをインターネット利用に費やしている実態が明らかになりました。

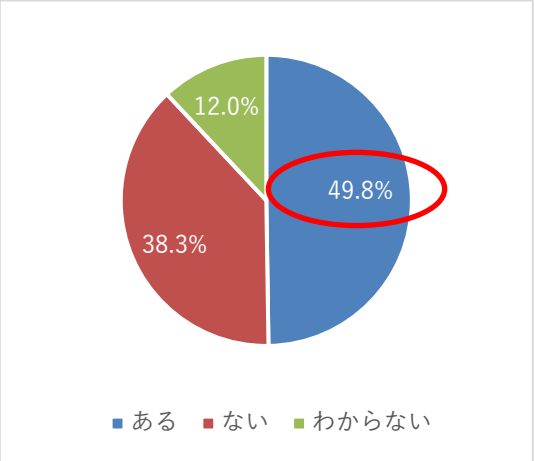
Q3. フィッシング詐欺の手口で知っている手口を選んでください。※複数回答可



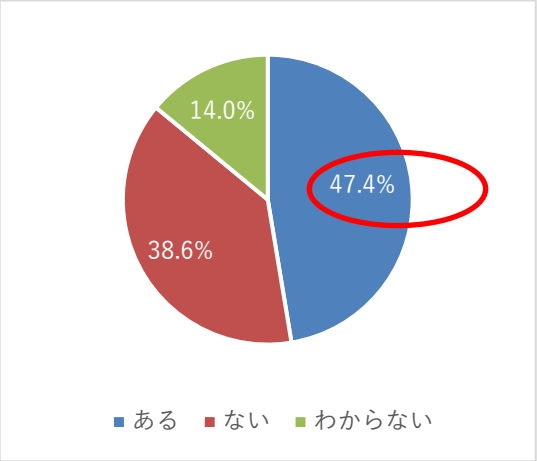


フィッシング詐欺の知っている手口については、「メールや SMS 等で偽サイトへ誘導し、ID やパスワード、クレジットカード番号等をだまし取る手口」が最も知られている手口で、前回調査と同様ですが、男女ともに 60 代や 70 代で知っている方の率が高くなっています。また、「特定の企業に狙いを定め取引先を装い、金銭や重要な情報等をだまし取る手口（ビジネスメール詐欺等）」は男女ともに増加しています。2025 年はランサムウェア被害に遭う企業が相次ぎ、大きく報じられました。この一連の報道により、企業をターゲットとした巧妙な詐欺全般への関心が高まったことがうかがえます。

Q4. 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？



2024 年 n=5299
（202 3 年 12 月～202 4 年 11 月）

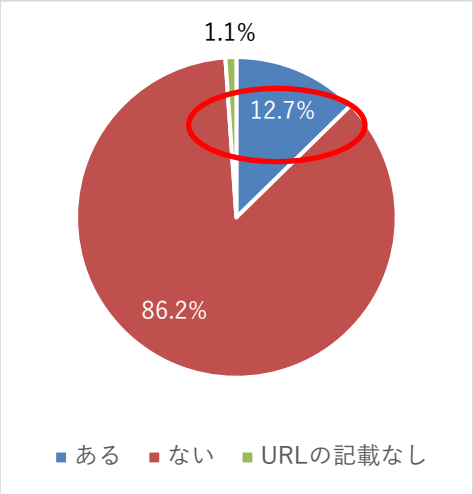


2025 年 n=5338
（2024 年 12 月～2025 年 11 月）

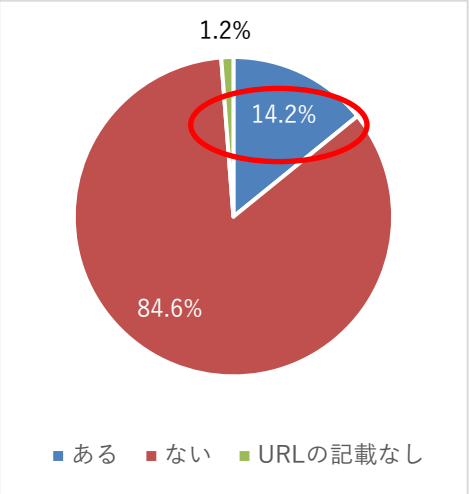
前年の調査と比較するため、2024 年 12 月から 2025 年 11 月を対象期間とし、フィッシング詐欺 SMS の受信および被害状況について質問しました。

フィッシング詐欺と考えられる SMS について、47.4%の方が受け取ったことが「ある」と回答しました。前回の調査と比較すると 2.4 ポイント減少しているものの、依然として半数近くがフィッシング SMS を受信しており、脅威は継続しています。

Q5. 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？



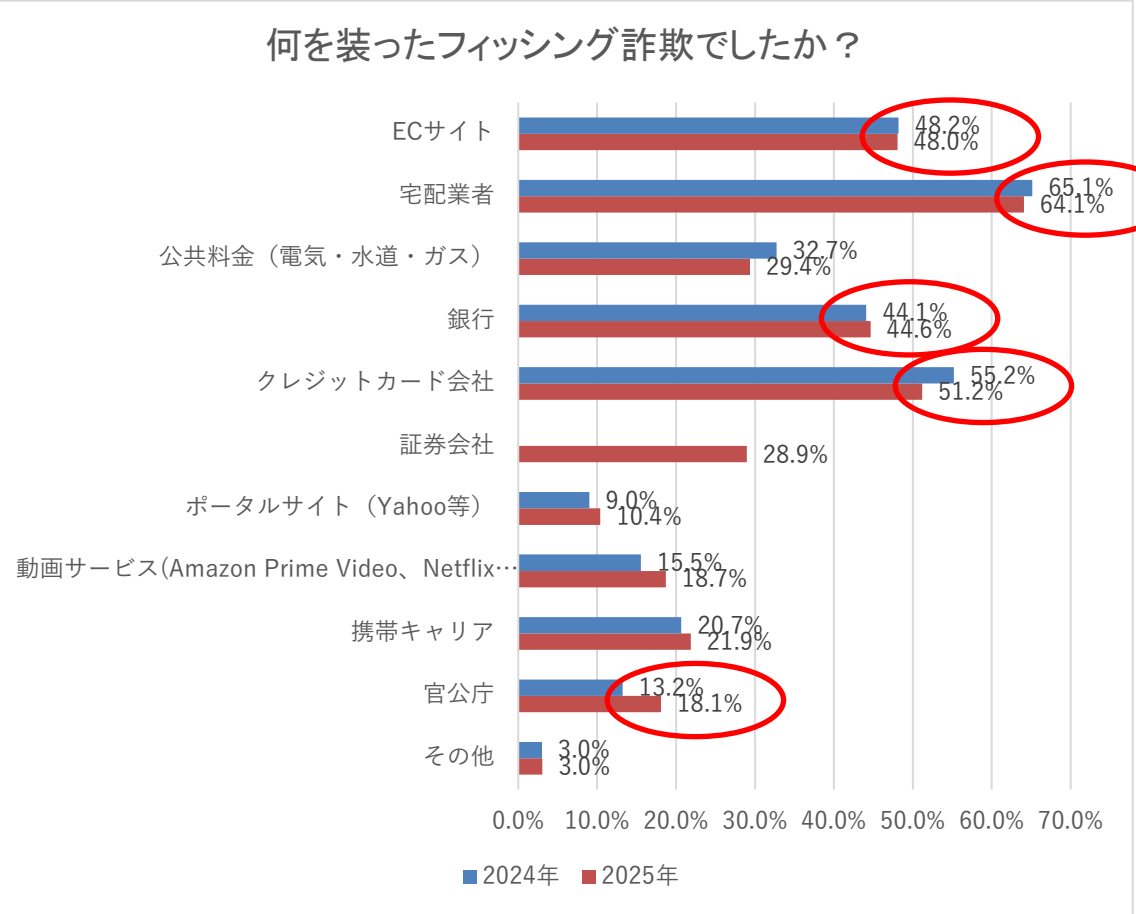
2024 年 n=2637
（202 3 年 12 月～202 4 年 11 月）



2025 年 n=2529
（2024 年 12 月～2025 年 11 月）

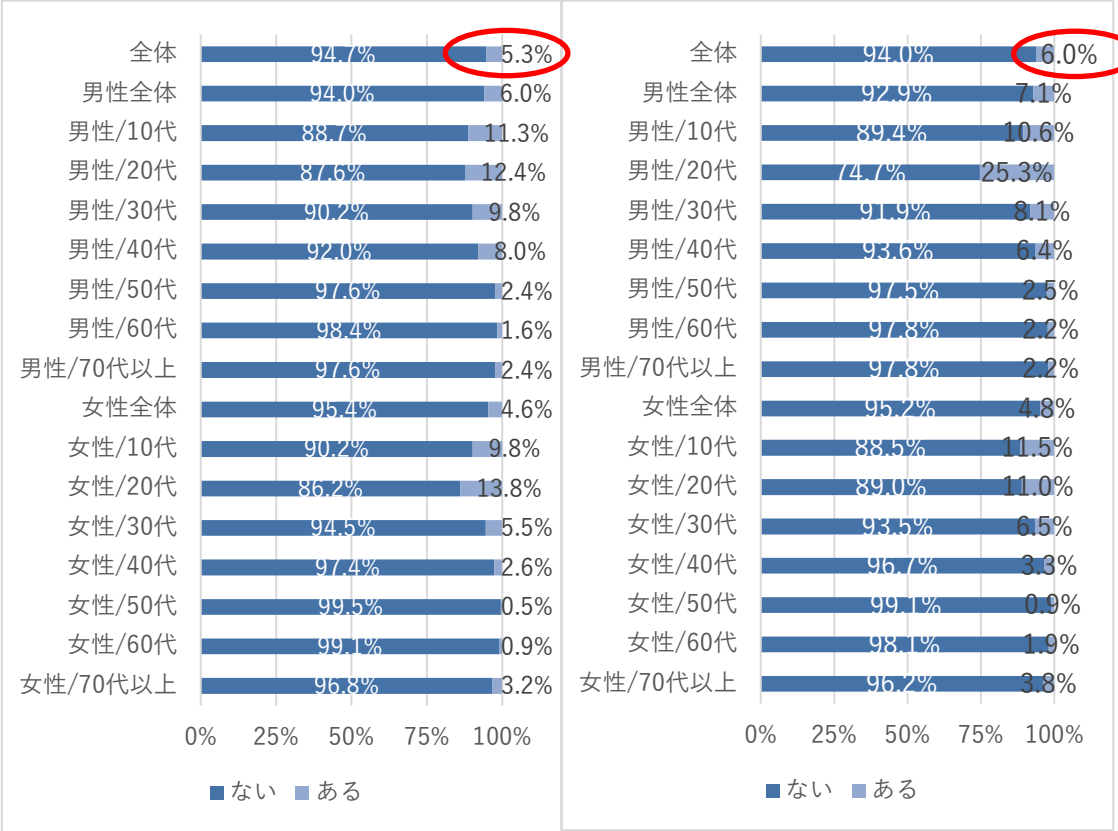
フィッシング詐欺と考えられる SMS を受け取ったことがあると回答した方を対象に、メッセージ内の URL をタップし、サイトにアクセスしたことがあるかを質問した。「ある」と回答した方は 14.2 でした。前回の調査結果（12.7%）と比較し、1.5 ポイント増加している。フィッシング詐欺 SMS の受信率自体はわずかに減少傾向にあるものの、URL をタップしてしまう割合は増加しており、文面の巧妙化などにより、詐欺サイトへの誘導を回避できないケースが増えている可能性があります。

Q6. 何を装ったフィッシング詐欺でしたか？　※複数回答可



受け取ったフィッシング詐欺 SMS において、何を装っていたかを聞いたところ、「宅配業者」が 64.1%で最も多く、次いで「クレジットカード会社」が 51.2%、「EC サイト」が48.0%となりました。前回調査と比較して顕著な変化が見られたのは「官公庁」を装う手口です。前回の 13.2%から、今回は 18.1%へと大幅に増加しています。国税庁やマイナポータルをかたるフィッシングの増加が影響していると考えられます。また、「銀行」を装う手口も 44.6%と高い水準を維持しています。

Q7. 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？

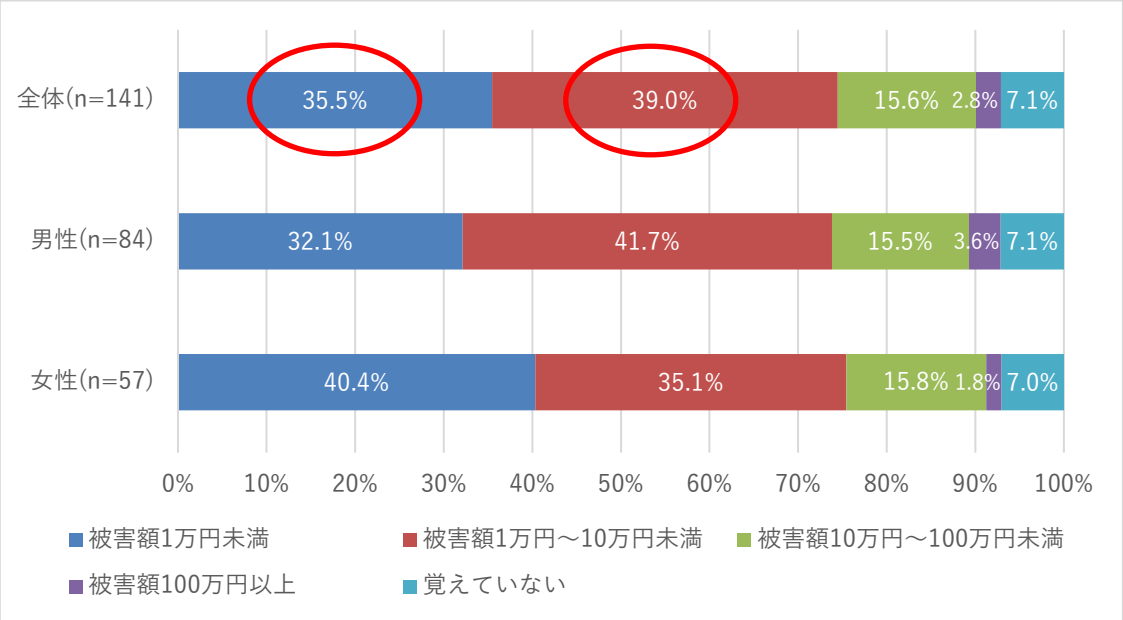


2024 年 n=2637
（202 3 年 12 月～202 4 年 11 月）

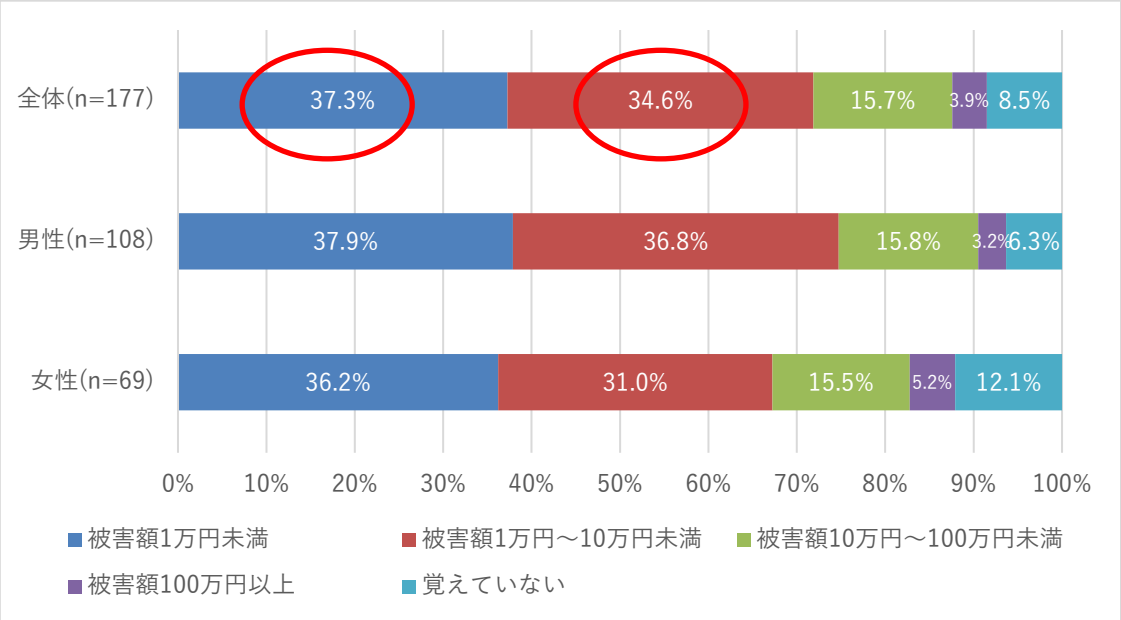
2025 年 n=2529
（2024 年 12 月～2025 年 11 月）

全体で金銭的被害にあった方の割合は、6.0%でした。前回の調査における 5.3%と比較して 0.7 ポイント増加しています。受信率は低下しているにもかかわらず、URL クリック率および金銭被害発生率が上昇しており、フィッシング詐欺の手口がより悪質化・巧妙化し、実被害に結びつきやすくなっている状況が懸念されます。

Q8. 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。



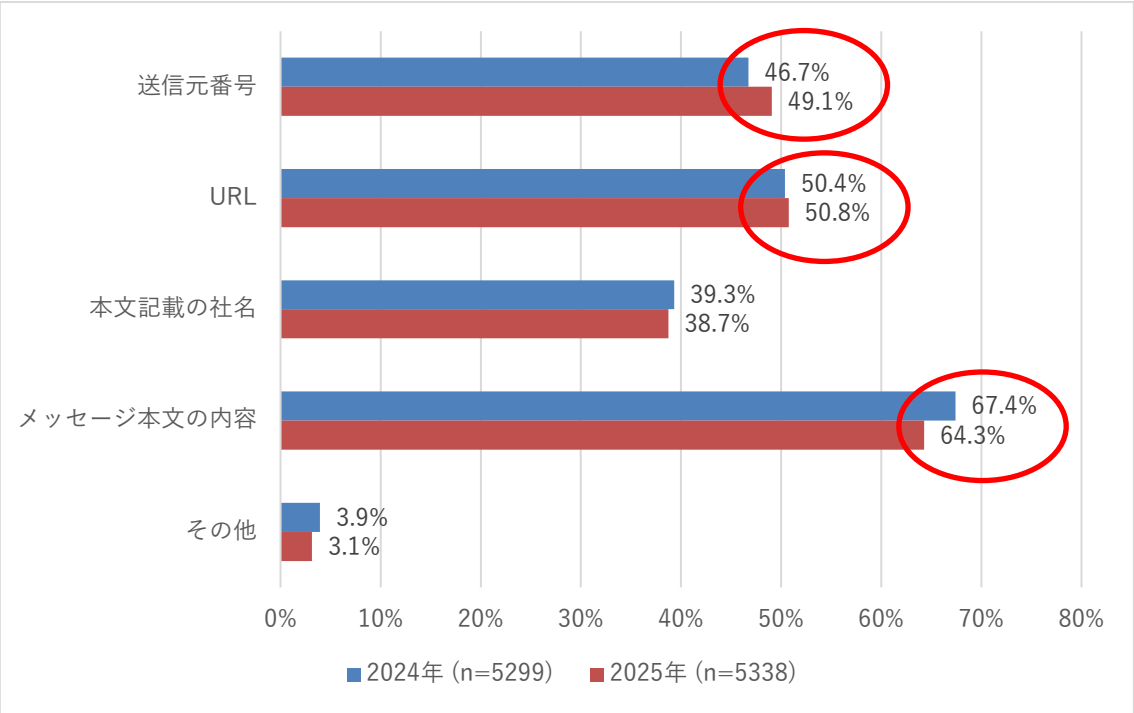
2024 年
（202 3 年 12 月～202 4 年 11 月）



2025 年
（2024 年 12 月～2025 年 11 月）

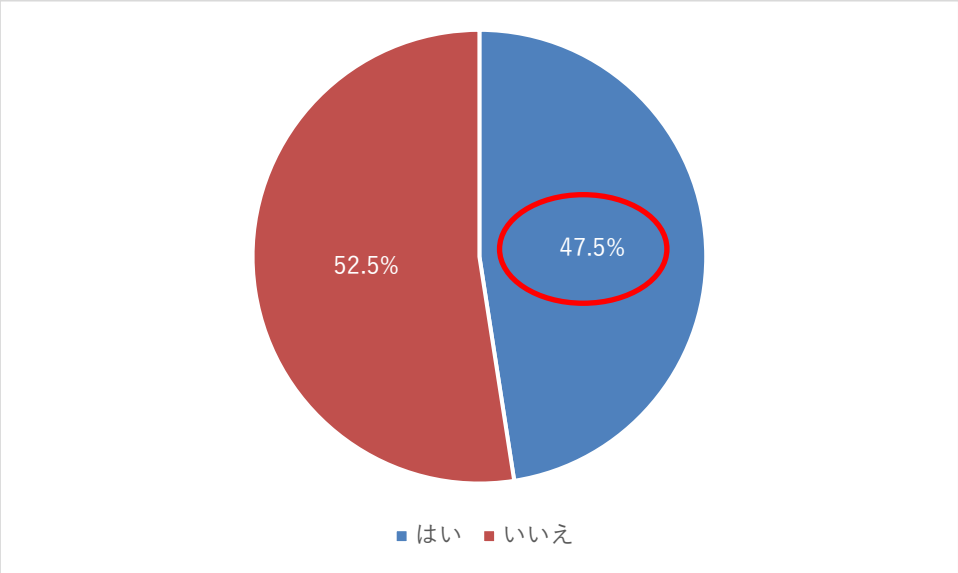
被害額は前回調査と比較し「1 万円未満」が 1.8 ポイント増加しましたが、「1 万円～10 万円未満」が 4.4 ポイント減少しました。被害額の分布を見ると、少額被害が依然として多い一方で、数百万円単位の高額被害も確実に発生しており、二極化の傾向が見られます。今回の調査で被害の最大額は 400 万円で 30 代の男性でした。

Q9. 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



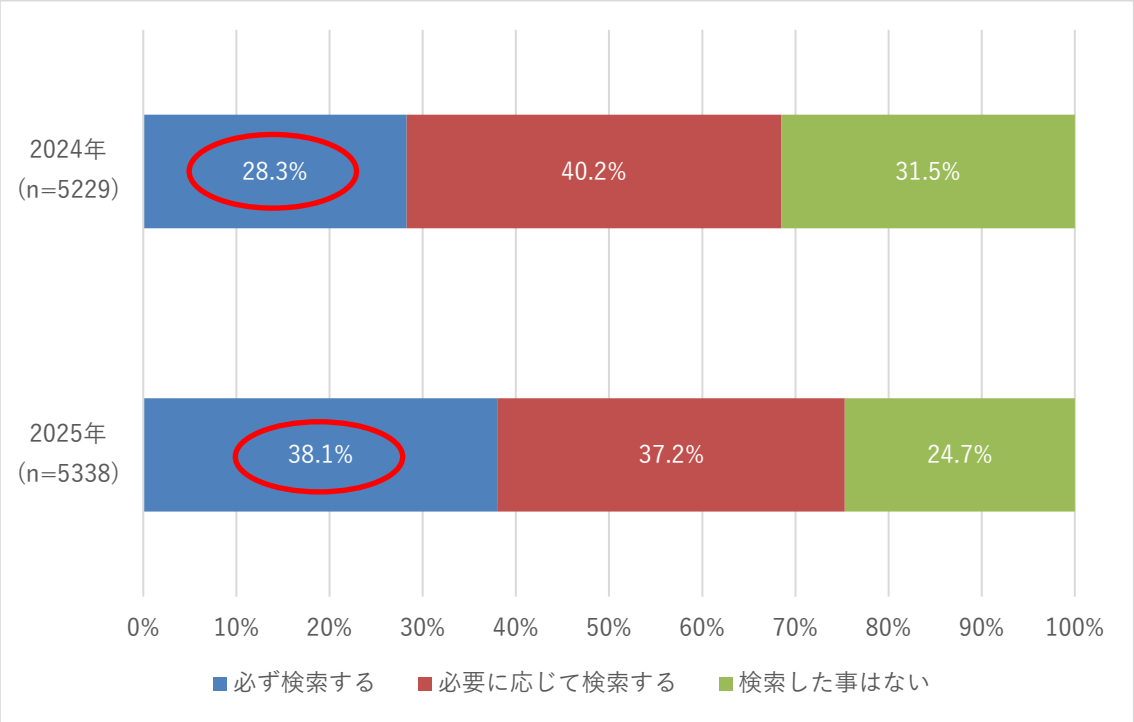
「メッセージ本文の内容」が 64.3%と最も多い回答割合となりましたが、前回の 67.4%からは減少しました。一方で、「送信元番号」で判断すると回答した割合は 49.1%となり、前回の 46.7%から 2.4 ポイント増加しました。「URL」で判断する割合も 50.8%と約半数が回答しています。メッセージ本文は攻撃者が容易に偽装できるため、送信元番号や URL（ドメイン）といった、より客観的な指標への意識が徐々に高まっていることがうかがえます。メッセージ本文は攻撃者が自由に記述できるものであり、文面が巧妙化しているため、正規の SMS とフィッシング詐欺の SMS を見分けることが難しくなっています。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。

Q10. 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=5338)



不正アプリに感染した携帯電話端末を経由した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 47.5%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。利用者へ注意喚起を強化していく必要があります。

Q11. 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、見知らぬ電話番号からの SMS に対して、「必ず検索する」と回答した割合は 38.1%となり、前回の 28.3%から 9.8 ポイント増加した。「必要に応じて検索する」（37.2%）と合わせると、7 割以上が検索行動をとっていることになります。フィッシング詐欺への警戒感の高まりから、SMS を受信した際に即座に反応せず、送信元を確認するという慎重な行動が定着しつつあると言えます。

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、フィッシング SMS の受信率自体は 47.4%と前回よりわずかに減少したものの、URL をタップしてしまう割合（14.2%）や、実際に金銭被害に遭う割合（6.0%）は前回よりも増加していることが明らかになりました。特に「官公庁」を装う手口の急増が目立っており、公的機関を騙ることで、サイトへ誘導する手口が横行しています。また、今回新たに追加したインターネット利用環境に関する調査からは、スマートフォン利用の常態化（主端末としての利用率 65.5%）と、長時間利用の実態が明らかとなりました。スマートフォンは UI の特性上、URL の全体像を確認しづらいことや、SMS 通知から即座にアクセスしやすい環境にあるため、PC 利用時以上にフィッシング詐欺への警戒が必要です。

対策として、送信元番号を確認する意識や、番号を検索するといった行動は年々向上しています。企業側には正規の送信元番号の公表や、携帯キャリア共通番号（0005）等の信頼できる送信手段の活用が求められるとともに、利用者に対しては「本文だけで判断せず、送信元番号や URL を必ず確認する」という基本動作の啓発を継続していく必要があります。

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。フィッシング詐欺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：2025/12/05～2025/12/08
有効回答者数：5,338 名 回答者の属性： 【性別】男性：49.8% 女性：50.2% 【年代】10 代：14.1%、20 代：14.3%、30 代：14.6%、40 代：14.2%、50 代：14.5%、60 代：14.1%、70 代以上：14.2%

※調査結果をご利用の際は、「NTT ドコモビジネス X 調べ」と明記ください。

【福地 雅之　NTT ドコモビジネス X 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（2025 年）も引き続き、地方自治体や企業が閉鎖したホームページに使っ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。

5.2 ICANN による gTLD 追加募集

本年のレポートでは、ICANN（Internet Corporation for Assigned Names and Numbers）が 14 年ぶりに実施する gTLD 追加募集について取り上げます。この募集により、新しいト

ップレベルドメイン（例:「.com」や「.org」のようなドメイン名の末尾部分）が数多く誕生する見込みです。フィッシング対策の観点では、まず、トップレベルドメインの種類が増える点について認識しておくことが重要です。また、フィッシング対策ガイドラインで重要項目である『ドメイン名を自社のブランドとして認識し、利用者への周知と維持に継続的に取り組むこと』を実現する手段としても注目されます。具体的には、自社のブランド名を冠したトップレベルドメインを設立することで組織のドメイン名の管理を強化し、前セクションでご紹介したドメイン名の不適切な廃止を防止することが期待されます。

5.2.1 gTLD の追加募集とは

ICANN は、ドメイン名、IP アドレス、プロトコル、ルート DNS サーバーなどのインターネットの基盤となる資源に関する調整を行うために、1998 年に米国で設立された民間の非営利法人です。新しく gTLD を創設するためには、ICANN の審査を経て、ICANN と契約を締結する必要があります。これまでに、ICANN では、「革新(Innovation)」「競争(Competition)」「消費者選択(Consumer Choice)」の促進を目的として、2000 年、2003 年、2012 年に gTLD の追加募集を行ってきました。前回の 2012 年には大々的な募集が行われ、一般名称や地理的名称に加え、企業名やブランド名での申請も可能となり、全世界から 1,930 件（日本からは 71 件）の申請がありました。（図 1、図 2）

順位	国名	申請数	順位	国名	申請数	順位	国名	申請数
1	アメリカ合衆国	884	21	南アフリカ	13		ノルウェー	3
2	ケイマン諸島	91	22	ブラジル	11		マレーシア	3
3	ルクセンブルク	85		スウェーデン	11		パナマ	3
4	イギリス領ヴァージン諸島	72	24	トルコ	10		バーレーン	3
5	日本	71		デンマーク	10	45	タイ	2
6	ドイツ	70	26	ロシア連邦	8		ポルトガル	2
7	ジブラルタル	62	27	ウルグアイ	6		エジプト	2
8	フランス	54	28	韓国	5		クウェート	2
9	スイス	51		サウジアラビア	5		ニュージーランド	2
10	香港	42		フィンランド	5		キプロス	2
11	オーストラリア(豪州)	41		シンガポール	5	51	マン島	1
12	中国	41		カタール	5		モナコ	1
13	イギリス	40	33	バミューダ諸島	4		コロンビア	1
14	アラブ首長国連邦	36		バチカン市国	4		ギリシャ	1
15	アイルランド	36		台湾	4		イスラエル	1
16	カナダ	27		ウクライナ	4		チェコ	1
17	インド	21	37	オーストリア	3		フィリピン	1
18	オランダ	19		リヒテンシュタイン	3		イラク	1
19	イタリア	16		メキシコ	3		モーリシャス	1
20	スペイン	15		ベルギー	3		ガンビア	1
						計		1,930

図 1 前回 2012 年募集における国、地域別申請数

TLDとして創設され、2026年2月調査時点で存在するトップレベルドメイン

一般名詞	地理的名称	サービス名、組織名等			文字列が競合したため未創設（もしくは別の申請組織により創設）	申請後に申請取下
.earth .moe .shop（*1）	.kyoto .nagoya .okinawa .osaka（*1） .ryukyu .tokyo .yokohama	.able .bridgestone .brother .canon .chintai .datsun .dnp .epson .firestone .fujitsu .ggee .gmo .goldpoint .hisamitsu .hitachi	.honda .infiniti .jcb .jprs .kddi .komatsu .lexus .lotte .mitsubishi .nec .nhk .nico .nikon .nissan .nissay	.ntt .otsuka .panasonic .pioneer .playstation .ricoh .sakura .sharp .softbank .sony .suzuki .tdk .toshiba .toray .toyota .yodobashi	.blog .inc .mail .osaka（*1） .shop（*1）	.design .docomo .gree .olympus .site .普利司通 TLD創設後に廃止 .goo .konami .lixil .mtpc
3	7	46			5	10

（*1）日本国内から同一文字列に対して複数の申請あり

図 2 2012 年募集における日本からの申請と 2026 年 2 月調査時点の状況

2026 年より開始する新たな募集においても、国内外から多様なトップレベルドメインが追加される見通しです。

5.2.2 gTLD 追加募集のスケジュール

ICANN が発表したスケジュールによれば、本レポートが公開される 2026 年 6 月時点では、申請の受付が行われている予定となります。そして、早ければ 2027 年に審査や契約手続きが完了し、2028 年には新しいトップレベルドメインを使用した Web サイトが登場している可能性があります。

ICANN が公開しているスケジュール（本レポートを執筆した 2026 年 2 月時点）は次のとおりです。

- 2026 年 4 月～8 月：TLD 申請受付期間
- 2026 年 10 月：申請文字列公開、代替文字列変更期間（2 週間）
- 2026 年 10 月～2027 年 4 月：文字列審査
- 2026 年 11 月：申請者／申請の審査順の抽選実施
- 2027 年 5 月～：審査順に申請者／申請の審査開始
- 審査合格後：Registry Agreement（RA）締結
- RA 締結後：ルートゾーンへの委任（TLD 利用開始）

5.2.3 申請条件

申請可能な文字列には制約があり、ASCII（英数字）の場合は 3 文字以上、非 ASCII（IDN）の場合は原則として 2 文字以上が必要です。申請資格は企業、組織、または機関に限定されており、個人による申請は認められていません。さらに、ICANN が定めた技術的および財務的要件を満たす必要があります。

申請に際しては、ICANN に対して最低でも US$ 227,000 の支払いが求められ、TLD 運用開始後についても ICANN に対して年間で最低 US$ 25,750 の維持費の支払いが必要となります。

5.2.4 RSP 評価プログラム

トップレベルドメインを運営するには、登録情報の管理や DNS の運用をはじめとする高度な専門技術が求められます。前回の gTLD 追加募集以降、これらの技術や支援を提供する「レジストリサービスプロバイダー（RSP）」と呼ばれる組織が登場しました。

RSP の登場を受け、ICANN は今回の追加募集に際し、各 RSP の技術力を評価し、その結果を公開する「RSP 評価プログラム」を開始しました。この評価プログラムを通じて技術力が認められた RSP は「評価済み RSP」として公式に公開されています。

参考：https://newgtldprogram.icann.org/en/application-rounds/round2/rsp/rsp-applications/evaluated-rsps

今回の gTLD 追加募集では、申請者が「評価済み RSP」を指定することで、ICANN による技術評価プロセスが免除されるため、簡便かつ安心して申請することができます。

【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 DNSSEC, DMARC によるドメイン名の信頼性の向上～.bank の事例～

フィッシング対策ガイドラインに記載しているように、ドメイン名は、組織やサービスのブランド価値やお客様からの信頼と直接結びついています。そのため、ドメイン名をブランドとして認知させ、その信頼性を高めることが重要です。

ドメイン名をユーザーに認知してもらい、そのドメインからのメールやサイトは信頼できると利用者に安心してもらうアクセスしてもらう必要があります。ドメインの認知と信頼が上がれば、ユーザーは偽のサイトや偽のメールの識別が容易になり、フィッシング詐欺にかかりにくくなります。そのため、ドメイン名の適切な管理と保護は、インターネット上でのブランド力を持続的に高めるために欠かせない要素となっています。

そのようにドメイン名をブランドとして厳しくその信頼を構築している事例として、2014 年 9 月から".bank"ドメインを運用している fTLD レジストリーサービスが求める技術的な管理と保護は大いに参考になります。fTLD レジストリーサービスは、".bank"ドメインのブランドの信頼を守るため、".bank”を取得のために厳しいセキュリティ対策を求めています。具体的には、".bank"ドメインの信頼が損なわれることが無いように次のような対策をドメイン取得金融機関に求めています。

- 厳格な登録者認証：登録できるのは、政府当局によって認可・監督されている銀行などの金融機関に限定
- DNSSEC による DNS の保護：DNS レコードの改ざんや毒入れを防ぐため、.bank ドメインを取得する組織は、DNSSEC を導入することが求められる。
- HTTPS の強制と TLS1.2 以上の使用
- DMARC の導入：SPF, DKIM を使っての DMARC の導入が求められ、ポリシーは、reject。
- レジストリ・レジストラーのシステムへのアクセスには MFA が必須

上記のような厳しいセキュリティ対策により、「.bank」信頼を担保し、ユーザーがアドレスバーで「.bank」で終わる URL を見ることにより、信頼できる銀行のドメインであると認知し、安心してアクセスできます。特に、上記の中の技術的な対策である DNSEC と DMARC は、ドメインの信頼を上げるためには、必須の技術です。fTLD は、上記のような対策によって、銀行のドメインの乗っ取りや大規模な詐欺を防止することで、金融システムのデジタルサービス全体の信頼を守っています。2024 年 10 月時点の報告に基づくと世界中で 860 以上の金融機関が".bank"ドメインを使用しています。

「.bank」の利用については、民間主導で実施されていますが、インドは、2025 年 4 月に、国として銀行のドメイン名の信頼を上げるため、インド準備銀行（RBI）が主導して、2025 年 4 月に「.bank.in」立ち上げました。インドのすべての銀行は、2025 年 10 月 31 日までにデジタルバンキングサービスのドメインを「.bank.in」に移行することが義務付けられています。そこに求められるセキュリティ機能は、「.bank」と同様に、DNSSEC, HSTS, DMARC などの技術的な要件が求められています。

このように金融機関は、ドメイン名のブランドとしての信頼を確かにすることにより、ユーザーがフィッシングなどのオンライン詐欺にかかるリスクを減らす活動が行われています。ただ、一般の業種においても、gTLD を取得して、ドメイン名をブランドとして認知を上げていけば同様のことが可能だと思います。また、gTLD を取得できなくても、自組織のドメイン名をブランドとしてきちんと管理し、ユーザーの認知を上げていけば、信頼できるドメイン名かどうかユーザーが認識しやすくなります。ドメイン名は気軽に取得できるため、これまでは、新しいサービスを立ち上げるとドメイン名を容易に取得する傾向がありました。一つの組織が複数のドメイン名を取得していることは、珍しくありません。また、中には、短期間で利用されなくなるドメイン名もあります。これでは、ユーザーは、ドメイン名でその組織を認知することが難しく、ドメイン名を信頼することができません。インターネット上でのブランド力を持続的に維持するためには、ドメイン名の一貫した利用、適切な管理と保護が必要とされています。

【野々下 幸治　株式会社アイエスエフネット】

6.2 日本証券業協会によるフィッシング詐欺防止に向けた取り組みについて

証券会社をかたるフィッシング被害の多発を踏まえ、日本証券業協会「インターネット取引における不正アクセス等防止に向けたガイドライン」の改正を含む、利用者への電子メールでの連絡に関する事項について紹介します。

6.2.1 証券業界における「インターネット取引における不正アクセス等防止に向けたガイドライン」（2021 年 3 月）制定までの経緯

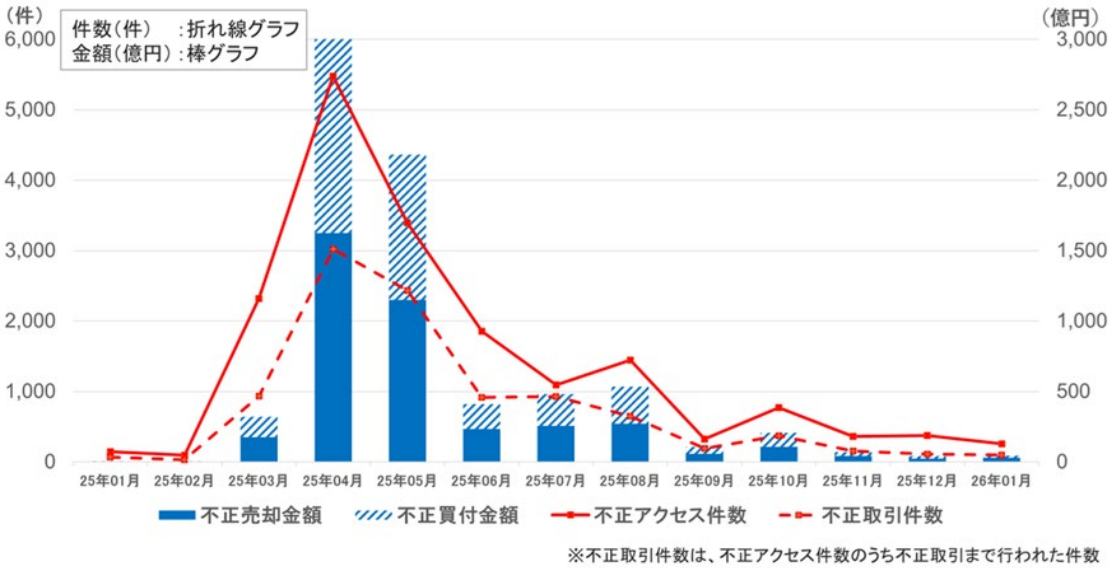
2020 年にインターネット取引サービスを顧客に提供する証券会社システムへの悪意のある第三者による不正アクセスの発生、顧客の証券取引口座にある有価証券の売却、第三者の銀行口座への不正出金等が複数発生しました。

証券業界の不正アクセス等防止に向けた対策として、日本証券業協会（以下、「日証協」）は、2021 年 3 月、インターネット取引における証券取引口座開設時からの出金に至る各段階における不正防止、脆弱性対策や情報管理、不正利用時の対応等についての具体的な留意事項を「インターネット取引における不正アクセス等防止に向けたガイドライン」（以下、「ガイドライン」）として取りまとめました。

6.2.2 2025 年初に発生した不正アクセス・不正取引等を受けての業界としての対応

- 2025 年 1 月頃より、フィッシングおよびマルウェアによる顧客情報（ID、パスワード等）の窃取、インターネット取引における不正アクセス・不正取引等の事案が発生しました。従来の証券口座から銀行口座を経由した不正出金を行うという手口ではなく、不正アクセスによる有価証券の売却代金を投資資金とし、犯罪者が事前に別口座にて低い値段で購入していた銘柄の株価の不正つり上げに悪用されていました。
- 2025 年 3 月、日証協は証券会社各社に対して、自社における必要なセキュリティ対策の実施および顧客に対してセキュリティ対策を促すよう注意喚起を行うとともに、不正取引の監視を行うように注意喚起を実施しました。
- 同年 4 月、電子メール等にて日証協や証券会社の名を騙り「フィッシング詐欺の安全確認等」と称した新たなフィッシング詐欺等が発生したことを受けて、再度、証券会社各社に対して、注意喚起を実施しました。
- 同年 4 月～5 月、日証協は被害拡大防止策として、以下の①～②を実施しました。
  ① インターネット取引におけるログイン時の多要素認証の設定必須化を決定した証券会社名の公表
  ② ガイドラインの見直しの検討
- 同年 7 月～8 月、ガイドライン改正（案）のパブリックコメント実施
- 同年 10 月 15 日、改正ガイドライン公表

〔インターネット取引サービスでの不正アクセス・不正取引の被害状況〕



不正取引が発生した証券会社数(社)												
25年1月	25年2月	25年3月	25年4月	25年5月	25年6月	25年7月	25年8月	25年9月	25年10月	25年11月	25年12月	26年1月
2	2	5	10	16	7	6	7	7	8	7	7	7

出典：金融庁ホームページ
https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html

6.2.3 改正ガイドライン（2025 年 10 月）の主な改正点（技術面）

以下、2025 年 10 月に公表された改正ガイドラインにおける主な改正点について紹介します。文中の記載内容の意味は次のとおりです。

> ガイドラインにおけるスタンダードとベストプラクティス
> 【スタンダード】：証券会社各社において、対応が必要とされる事項
> 【ベストプラクティス】：証券会社各社の規模・サービス内容や顧客特性、並びに犯罪手口の巧妙化・複雑化を踏まえた上で、対応することが望ましいとされる事項

(1) フィッシングに耐性のある多要素認証の実装及び必須化

✓ ログイン時、出金時、出金先銀行口座の変更時など、重要な操作時 におけるフィッシングに耐性のある多要素認証 （例：パスキーによる認証、PKI（公開鍵基盤）をベースとした認証）の実装及び必須化（デフォルトとして設定）する。【スタンダード】

【参考】「フィッシング耐性のある多要素認証」に関するパブリックコメントの回答（要約）

2025 年 7 月に実施したガイドライン改正のパブリックコメントの募集において、「新しい技術仕様を実質的に強制とすることは個人投資家にとっても大きな負担」、「フィッシング耐性さえあれば被害に遭わない、といった誤った主観を植え付けてしまう恐れもある」といった意見が寄せられました。

日証協としては、今般、フィッシング等により窃取された顧客情報により、インターネット取引サービスでの不正アクセス・不正取引（第三者による取引）の被害が急増したことを踏まえて、フィッシングへの対策を強化するために、本ガイドラインの改正において、ログイン時等における「フィッシングに耐性のある多要素認証」の実装および必須化を【スタンダード】※としました。

「フィッシング耐性のある多要素認証」の考え方として、パスキーによる認証や PKI （公開鍵基盤）をベースとした認証は、現時点においてフィッシングに耐性があると考えられる認証方式であり、「国民を詐欺から守るための総合対策 2.0」（令和 7 年 4 月 22 日犯罪対策閣僚会議決定）において、次世代認証技術の一つである、「パスキーの普及促進」が掲げられています。

なお、今後の認証技術の進展を踏まえて、その他の技術を用いた認証の実装を妨げるものではないことも併せて付しております。

（2） 不正ログイン・不正売買等を防止するための対策（顧客への通知等）

- ✓ 身に覚えがない第三者による不正なログイン・取引（売買注文もしくは約定）、出金、出金先口座変更について、顧客自らが早期の被害認識を可能とするため、通知先として登録されている電子メールや SMS 等に対して、通知を送信する機能を提供する。なお、顧客自らが通知（する・しない）を設定する機能を設けることができるものとする。【スタンダード】
- ✓ 第三者が不正にアクセスし、重要な顧客情報の窃取や改ざんが行われないよう、通知を送信する機能を提供する。【スタンダード】

6.2.4 改正ガイドライン（2025 年 10 月）におけるメール等の取り扱いについて（フィッシング詐欺等被害未然防止のための措置）

改正ガイドラインでは、フィッシング詐欺等被害未然防止のため、電子メール等の取り扱いに関して次の内容が規定されました。

（1） DMARC の計画的な導入／メールや SMS へのログインリンク記載禁止

- ✓ 顧客へ送信する電子メールのドメインを特定し、DMARC 等の送信ドメイン認証技術の計画的な導入を行う。また、DMARC レポート等の確認等を行った上で、ポリシーは「reject」にする。【スタンダード】
- ✓ メールや SMS（ショートメッセージサービス）内にパスワード入力を促すページの URL やログインリンクを記載しない（法令に基づく義務を履行するために必要な場合など、その他の代替的手段を採り得ない場合を除く）。【スタンダード】

【参考】
「メールや SMS への URL の記載」に関するパブリックコメントの回答（要約）
2025 年 7 月に実施したガイドライン改正のパブリックコメントの募集において、「メールや SMS 内にパスワード入力を促すページの URL やログインリンクを記載しないこと」とした場合の業務影響等を想定した意見が寄せられました。
日証協としては、インターネット取引を行うツールにログインを行うことができるパスワードが存在する、あるいはパスワードの取得ができる状況にある顧客がいる場合には、URL ・ログインリンクを記載することはできないと考えられます。
例外事項として、法令に基づく義務を履行する行為に該当する場合や、顧客の状況に応じてサービス提供にあたり代替的手段を採り得ないと判断されている場合には、URL ・ログインリンクを記載することは問題がないと考えられます。

（2） 顧客が各社からの正規のメールだと判断できるような措置

- ✓ 電子メールにブランドのロゴや公式マークが表示されるよう、BIMI への対応を行う。【ベストプラクティス】
- ✓ 顧客へ何らかの通知を行う場合のメールについて、S／MIME による電子署名を付与する。【ベストプラクティス】

【日本証券業協会】

6.3 「今すぐできるフィッシング対策」のコンテンツ紹介

フィッシング対策協議会のホームページでは、消費者向けにフィッシング詐欺から身を守るために今すぐできる対策と、被害にあったかもしれないサインとその対処法をまとめた「今すぐできるフィッシング対策」を公開しています。対策の紹介では、必須か否かであったり、対策の難易度を分かり易く明示しています。また、被害にあった場合の相談先や簡単な用語集も付けています。ぜひご活用ください。

今すぐできるフィッシング対策
https://www.antiphishing.jp/consumer/antiphishing-for-users.html

7. まとめ

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られたものです。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 章では、巧妙化しつつある手口の一つ「ボイスフィッシング」の解説です。手口や対策を把握する上でぜひご一読いただきたい内容です。4 章は、2021 年から行われている SMS を用いたフィッシング詐欺についての意識調査の解説です。年代・男女・利用環境(端末)のほか、フィッシングの手法、被害にあったことがあるか、といったアンケート調査の結果が分析されています。5 章はドメイン名関連の話題です。ドメイン名廃止に関する対処の仕方のほか、ICANN による gTLD の追加募集についてまとめられています。6 章「トピック」では、DNSSEC や DMARC の制度面での事例として、.bank について紹介されています。TLD である.bank では DNSSEC 導入が求められており、また DMARC 導入においては reject のポリシーが求められています。また、日本証券業協会によるフィッシング詐欺防止に向けた取り組みとして、2025 年 10 月に公表された「インターネット取引における不正アクセス等防止に向けたガイドライン」の経緯や改定点などについて解説されています。

フィッシングを巡る脅威は年々変化しています。本レポートが、その変化を的確に捉え、継続的な対策の見直しや高度化を検討する際の指針となれば幸いです。ご多忙の中、専門的知見をご寄稿くださった技術・制度検討 WG メンバーの皆さま、ならびに全体の取りまとめに尽力された事務局の皆さまに、あらためて深謝いたします。

【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
笠間 英宏	NTT ドコモビジネス株式会社
加藤 孝浩	TOPPAN 株式会社
加藤 雅彦	順天堂大学
金井 孝三	Sky 株式会社
上川 佳一	株式会社アクリート
栢森 亮輔	明治安田生命保険相互会社
唐沢 勇輔	Japan Digital Design 株式会社
鈴木 伸吾	NTT ドコモビジネス X 株式会社
高山 寛史	日本証券業協会
竹内 司	株式会社みずほフィナンシャルグループ
多田 憲治	日本証券業協会
田中 優成	株式会社アクリート
張 作庭	レジル株式会社
塚田 晴史	株式会社マクニカ
野々下 幸治	株式会社アイエスエフネット
半戸 祐次	BC Signpost 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
福地 雅之	NTT ドコモビジネス X 株式会社
藤井 治彦	バンクガード株式会社
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

【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