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 2024

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

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]によると、2023 年上半期は、ランサムウェア被害の件数が高水準で推移している。また、フィッシング被害等に伴うクレジットカード不正利用被害やインターネットバンキングに係る不正送金被害も急増している。2023 年上半期のインターネットバンキングに係る不正送金被害は、年間の被害件数と比較しても過去最多、被害総額も過去最多に迫る状況である。

警察によるサイバー犯罪の検挙件数は、1,181 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 188 件（前年同期比で 19.3%減少）であった。このうち 157 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。

フィッシング情報の届け出件数について、2023 年は前年と比較して増加した（図 1-1）。EC サイト大手、クレジットカード会社のほか、マイナポイント事務局など公共サービス、交通系サービスのなりすましが報告されている。

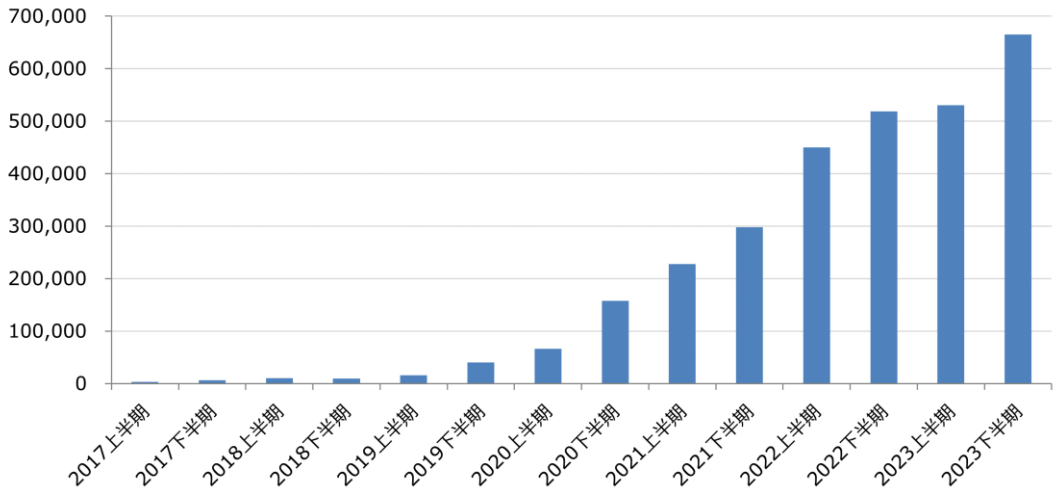


図 1-1 国内のフィッシング情報の届け出件数[2]

1 警察庁、令和 5 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/R05_kami_cyber_jousei.pdf）（閲覧日：2024 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：2024 年 2 月 20 日）より作成

フィッシングサイトの URL 件数は、2023 年は上半期・下半期とも 2022 年上半期より増加しており、2022 年下半期の突出した件数を除き、全体的に増加傾向が続いている。（図 1-2）。ブランド名を悪用された企業の件数も、2022 年と同程度の件数で高止まりしている（図 1-3）。

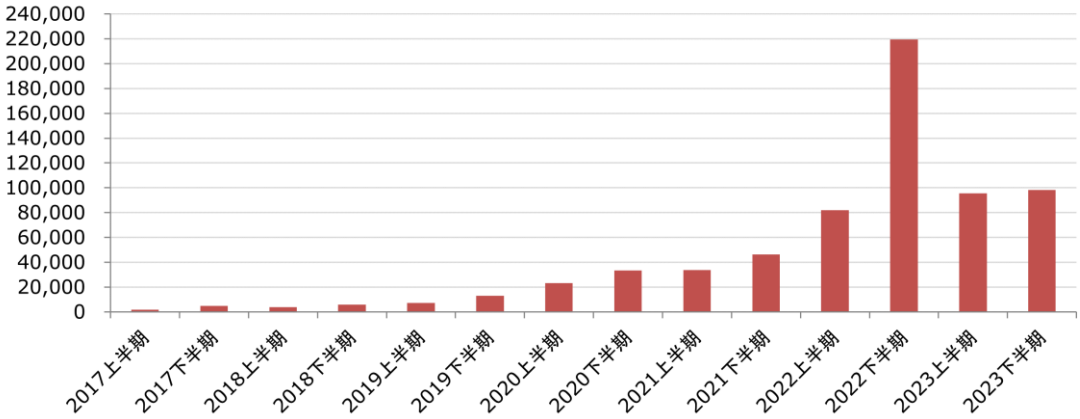


図 1-2　国内のフィッシングサイトの件数

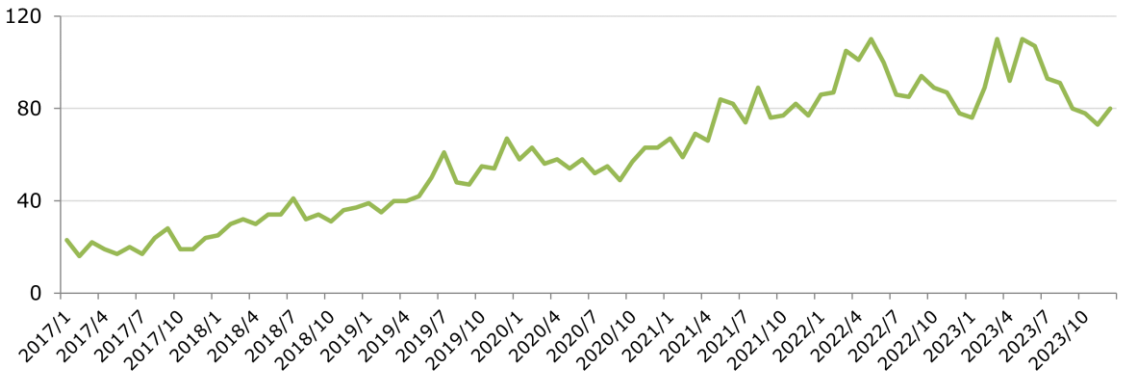


図 1-3　国内のブランド名を悪用された企業の件数

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 年と同程度であった（図 1-4）。2023 年の手口別内訳では、2022 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、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.soumu.go.jp/main_content/000935209.pdf）

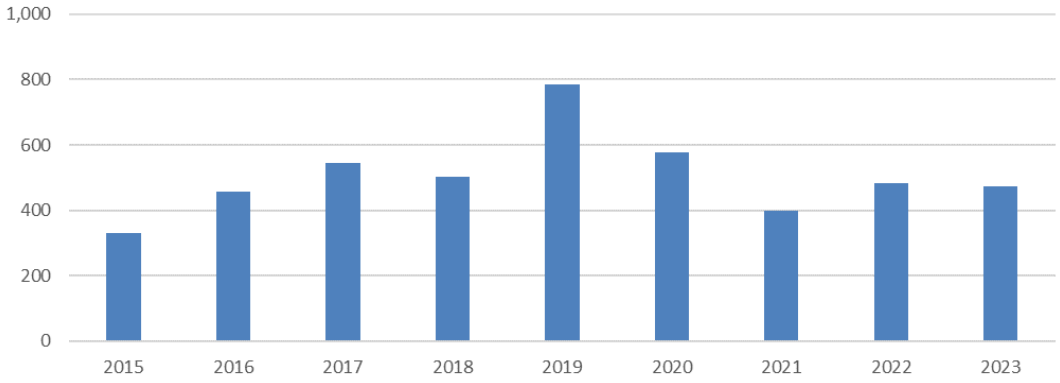


図 1-4　識別符号窃用（ID 窃盗）型不正アクセス行為の検挙件数[4]

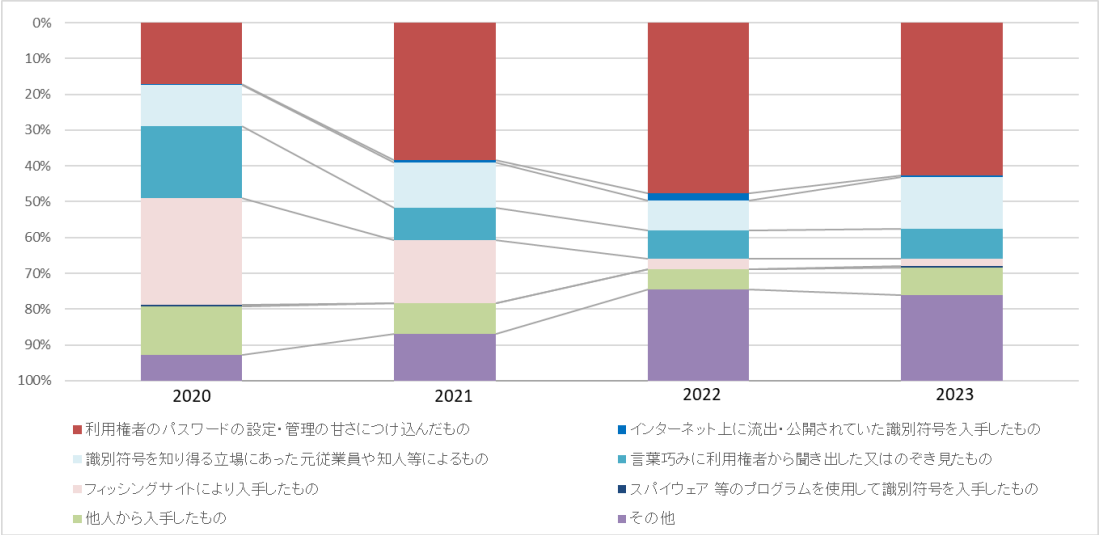


図 1-5　識別符号窃用型不正アクセス行為の手口別検挙件数の内訳
（2020 年～2023 年）[5]

【株式会社三菱総合研究所】

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、2023 年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たが 2022 年下半期に増加した。2022 年下半期以降は減少傾向にある（図 1-6）。フィッシングサイトの件数は、2023 年上半期までは増加傾向であったが、2023 年下半期は減少に転じたものの依然として高い水準にある（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 年に入って減少傾向にある。（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 1 四半期にはフィッシング攻撃全体の 37.4%が標的となったことが報告されている。また 2024 年第 1 四半期の Business Email Compromise 攻撃で要求された平均送金額は 84,059 ドルで、前四半期の平均から約 50%増加した。

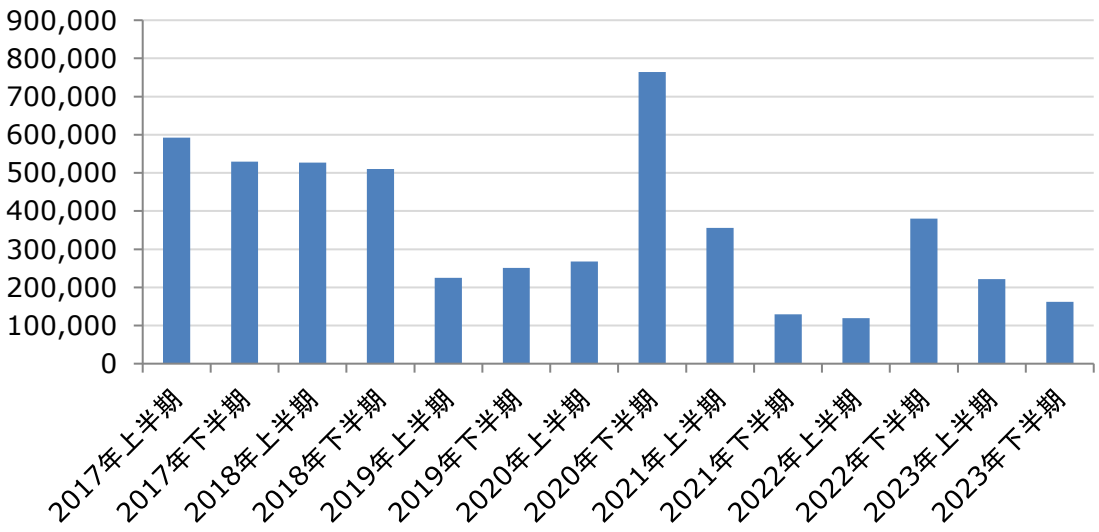


図 1-6　APWG へのフィッシングメール届け出件数[7]

6 APWG（Anti-Phishing Working Group）、"Phishing Activity Trends Report"（https://apwg.org/trendsreports/）（閲覧日：2024 年 5 月 17 日）

7 APWG、"Phishing Activity Trends Report"（https://apwg.org/trendsreports/）のデータに基づき三菱総合研究所が作成（閲覧日：2024 年 5 月 17 日）

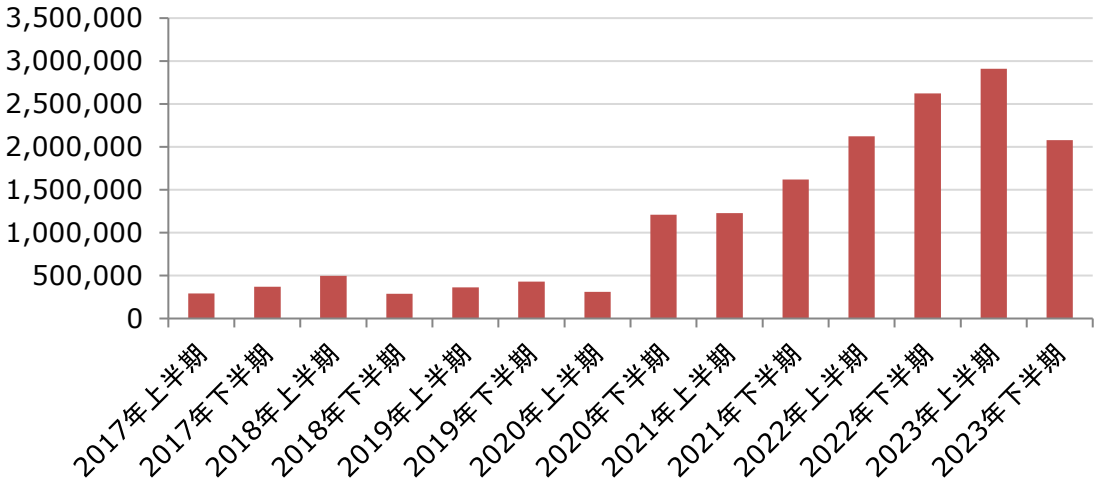


図 1-7　フィッシングサイトの件数（APWG）[8]

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]

【株式会社三菱総合研究所】

8 APWG、"Phishing Activity Trends Report"（https://apwg.org/trendsreports/）のデータに基づき三菱総合研究所が作成（閲覧日：2024 年 5 月 17 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 2023 年 1 月から 12 月までのフィッシング報告件数は過去最高の 100 万件を超えて 1,196,390 件となり、2022 年と比較して約 1.23 倍となった。

また、10 月は報告件数が 15 万件を超え、月ベースでも過去最高件数となっている。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る。

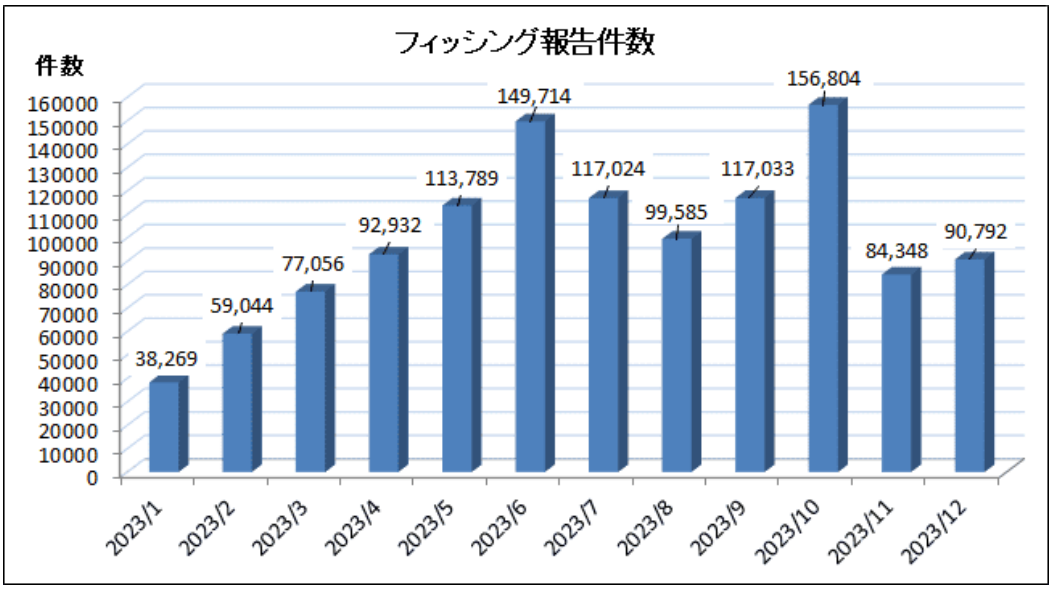


図 9　2023 年フィッシング報告件数の推移

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

2023 年もさまざまなブランドをかたり、フィッシング行われており、そのブランド数は 212 となった。悪用された分野としては、金融系 41 ブランド、クレジットカード・信販系 34 ブランド、通信事業者・メールサービス系 25 ブランド、EC 系 18 ブランド、オンラインサービス系 15 ブランド、仮想通貨系 12 ブランド、公共サービス系 10 ブランド、官公庁系 9 ブランド、決済サービス系 8 ブランド、その他 34 ブランドが発生した。

さまざまなブランドをかたるフィッシングが発生している背景には、今まで狙われていた事業者がフィッシング対策を進めていることにより、対策が遅れている事業者や、今までフィッシングが発生していない分野が狙われていることが考えられる。

1.3.2 フィッシングで使用された多様な手法

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る。

以前からセキュリティ機能を回避するための手法として、QR コードを使用したり、正規サービスのリダイレクト（転送）機能を悪用して、フィッシングサイトへ誘導したり、ランダムな文字列を組み合わせて多数の URL を生成して誘導したりする手法が行われていたが、対策が進み、報告数（メール配信数）が減り始めた 10 月中旬以降、新たに URL に飾り文字（囲み英数字等）や 16 進や 8 進数を取り混ぜた IP アドレス表記を使用するフィッシングが発生した。

飾り文字の例：https://example.🄲🄾🄼/
IP アドレスの例：http://●●●●.0x1c.071763/

また、フィッシングサイトへ誘導するために正規メールと誤認させる手法として、そのメール文面を盗用されることが多いが、その信ぴょう性を高めるための方法として、偽の S/MIME 署名ファイル「smime.p7s」を添付したフィッシングメールが発生した。これは、S/MIME 検証ができないメーラーで、署名されたメールを受信した場合に電子署名を添付ファイルの形で表示する動作を模倣したものであり、ユーザーが署名付きの正規のメッセージであると誤認することを狙っている。そのため、S/MIME を使用したメールセキュリティ対策をしている場合の利用者への啓発については、今後注意が必要である。

過去最高となった不正送金被害額（80.1 億円）[10]急増の要因としては、リアルタイムフィッシングと呼ばれる手法が多く使用されていることが影響していると見られる。この手法では、犯罪者がフィッシングサイトで情報を詐取すると同時に、バックグラウンドで正規サイトを操作し、ワンタイムパスワードや認証コードをも入力して不正送金操作を完了してしまう。この手法は、2019 年頃から使用されているが、被害者が本物と信じて情報を入力してしまい、セキュリティ対策の効果も低下してしまうことから対策も難しい状況である。

1.3.3 「なりすまし」送信メールの状況について

2023 年も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る。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

[10] 警察庁、フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について（注意喚起）（https://www.npa.go.jp/bureau/cyber/pdf/20231225_press.pdf）（閲覧日：2024 年 2 月 29 日）

のうち、平均約 74.9%、最大で 91.9%が「なりすまし」送信メールであった。「なりすまし」送信メールを排除するためには、正規に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）が有効である。ドメインホルダーである事業者やメールサービス提供事業者には、DMARC の正式運用（認証失敗したメールは隔離、受信拒否というポリシーを宣言し、ポリシーに法ったメール配信を行う）と、その技術を利用して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（BIMI: Brand Indicators for Message Identification 等）の実装を進めてもらいたい。

【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

フィッシング対策ガイドラインの冒頭に書かれております通り、フィッシング報告件数はこれまでにも増して高い水準にあります。4 年ほど前の 2020 年 4 月から 2021 年 3 月にかけては 1 万件から 4 万件に増加していたのが、2023 年は 4 月の段階ですでに 9 万件を超え、2023 年 10 月には 15 万件に達しています。技術・制度検討 WG で毎年作成されているフィッシング対策ガイドライン（以下、ガイドライン）の重要性もまた高まっていると言えます。

2023 年 10 月にフィッシング対策協議会で行われたフィッシング対策ワークショップでは、奇しくも、ガイドラインに関する意見交換が行われる時間が設けられ、一参加者であった私としても読み手の率直なご意見に触れる機会となりました。

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改めて全体を見直す活動を行いました。従来の良さを残しつつ、読み手の観点で、読みたい節にたどり着きやすくするとともに、内容の明確化を通じて対策を取りやすくするためです。まず従来の記述項目の中で「情勢の変化を受けて、削除できる項目がないか」「指針を示すガイドライン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”として別記できないか」といった点について WG メンバーからすべての節についてご意見を集めました。今年度のガイドラインとレポートはこれを受けた結果として、執筆されたものです。

今後も改善を図っていくとともに、ガイドラインの内容が検索結果にヒットするなどオンラインで参照しやすくしていく、ご説明の機会を設けるなどしてガイドラインを活かしていくことも重要と考えられます。

今年度、トレンドマイクロ株式会社の野々下幸治様より主査を引き継ぎ、例年よりも活動期間が短い中、新たな事務局ご担当の田中則通様（三菱総合研究所）をお迎えしてのスタートとなりました。引き続き WG メンバーとして活躍されている野々下様と WG メンバーとで取り組んで参りたいと思います。読者の皆さまにおかれましても、ご協力を賜りたく、よろしくお願いいたします。

【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。

2023 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 1 フィッシング詐欺被害状況ダッシュボード「Phish Trends」

・フィッシング対策ワークショップの開催（2023/10/2）

＜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. ガイドラインの項目検討
2. ガイドラインへの追加項目
3. ガイドラインの簡略化・優先度
4. フィッシング啓発活動

参加者数：65 名

◆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。

2023 年の活動として、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を追跡調査を実施した。

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第 2 回調査結果 (2023/07/21)

（https://www.antiphishing.jp/wg_auth_report_202307.pdf）

◆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。

2023 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。

・フィッシングメール詐欺：手口と対策　解説ドキュメント（2024/2/20 公開）

日本国内におけるフィッシング詐欺における、なりすましメールの手口とその対策方法について解説

（https://www.antiphishing.jp/report/wg/cert_explaindoc_20240220.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[11]。

[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/）

2023 年の活動としては、『第 19 回 IPA「ひろげよう情報モラル・セキュリティコンクール」 2023』の応募作品の中から「標語」「ポスター」「4 コマ漫画」の 3 つの部門における優秀賞（協力企業・団体賞）を選出し、表彰した。12

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

フィッシングサイトの早期発見に関する研究を推進し、よりプロアクティブなフィッシング詐欺対策の確立を目指している。2017 年 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、協議会と長崎県立大学の双方から選出されたメンバーで推進。

2023 年の活動としては、以下のテーマを中心にフィッシング対策研究を実施。

- サブドメイン悪用調査
- 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
- 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る。

2023 年の活動として、オフラインまたはオンラインによる『詐欺サイト対処机上演習』を計 3 回実施し、延べ参加者数は 134 名となった。

・（オフライン開催）2023/5/30, フィッシング対策協議会『詐欺サイト対処机上演習（プロトタイプ版）』, 参加者 14 名

12フィッシング対策協議会、『第 19 回 IPA「ひろげよう情報モラル・セキュリティコンクール」2023』の優秀賞を選出（https://www.antiphishing.jp/news/info/ipa_competition2023.html）

・（オンライン開催）2023/9/16, ISACA 名古屋 2023 年 9 月度 月例会『詐欺サイト対処机上演習（mini 版）』, 参加者 31 名

・（オフライン開催）2023/10/30, 日本シーサート協議会 インシデント対応演習訓練 WG『フィッシング対策協議会 連携特別会～詐欺サイト対処机上演習を体験しよう～』, 参加者 89 名

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。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った。

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 国税庁、東京都水道局、マイナポータル等をかたるフィッシング

2023 年 12 月以降、e-Tax に関するフィッシングサイト、水道料金の未納や滞納を通知するフィッシングメールや SMS、給付金の支給を知らせるフィッシングメールやサイトが報告されている。いずれもメールや SMS からフィッシングサイトに誘導され、ログイン情報やクレジットカード番号などの入力が求められる。

これらのフィッシングサイトは本物のサイトの画面をコピーして作成されることが多く、見分けることは非常に困難になっている。

フィッシング対策ガイドラインでは、「利用者が安全にサービスを利用する環境を整えるように促すこと」において、新たに「メールや SMS に記載された URL もしくは検索結果の URL を利用しない、提供者側がそれを前提としない形を取る」さらに「メールや SMS に記載された URL を直接利用することの常態化を避ける」記述を追加した。いわゆるメールや SMS といったエントリーポイントは利用者の観点では正規かどうかの見わけがつきにくいため、ブラウザーのブックマークやアプリといった、ユーザー側のアクションで確保される導線を利用する方法である。多数のサービスを利用するユーザーはどのサービスが URL を含むメッセージを送ってくるかを覚えることが難しいため、より多くのオンラインサービスにおいて、正規の導線をより早くユーザーに提供できるかが重要になる。

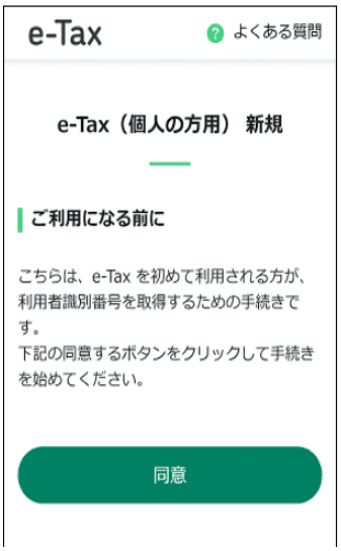


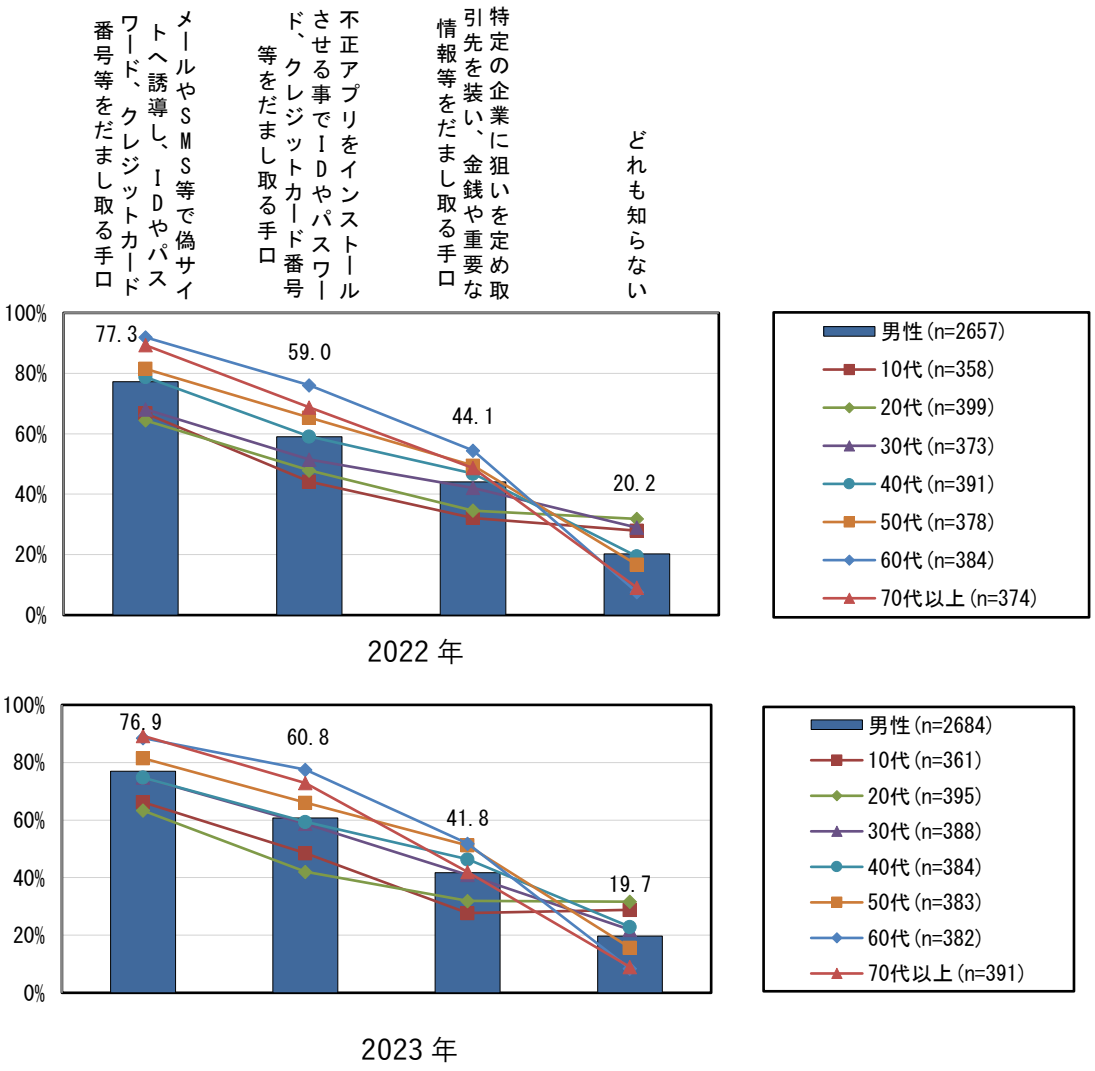
図 3-1　国税庁の e-Tax かたるフィッシングサイト
（フィッシング対策協議会 緊急情報より）

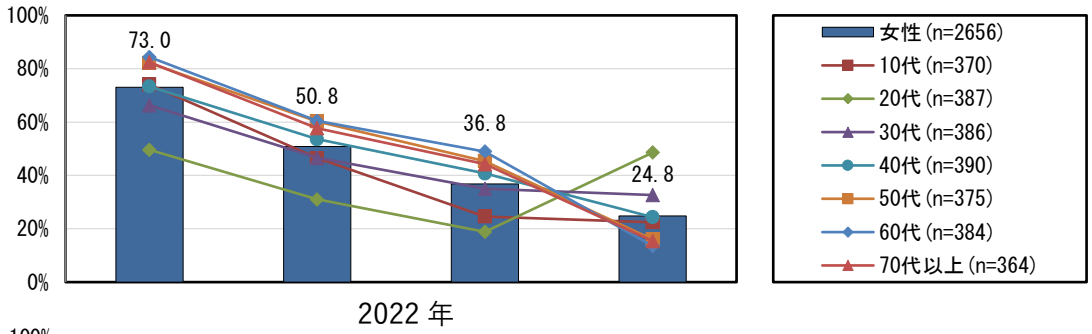
【木村 泰司 一般社団法人日本ネットワークインフォメーションセンター】

4. SMS を用いたフィッシング詐欺についての意識調査

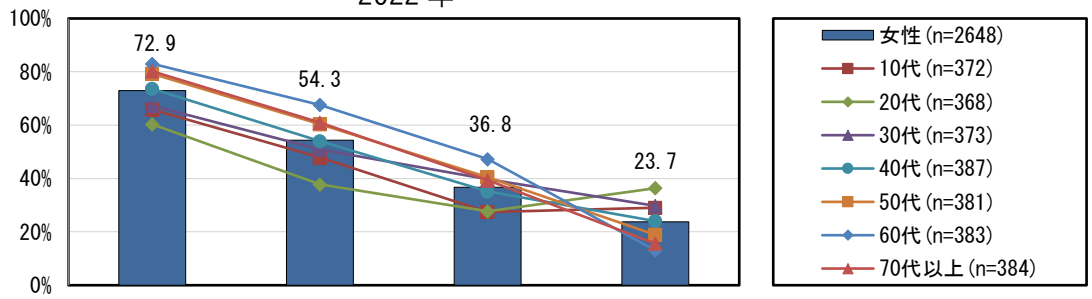
2021 年より SMS（携帯のショートメッセージ）を用いたフィッシング詐欺について消費者の意識や被害の実態を調査するアンケートを実施し、その結果をフィッシングレポートで報告してきたが、今回も同様のアンケートを実施したので報告する。アンケートは、インターネットリサーチにて対象者を年代ごと、男性、女性の比率などが同等になるよう配慮し、5,332 名から回答を得た。以下、調査結果のポイントについて紹介する。

Q１フィッシング詐欺の手口で知っている手口を選んでください。※複数回答可





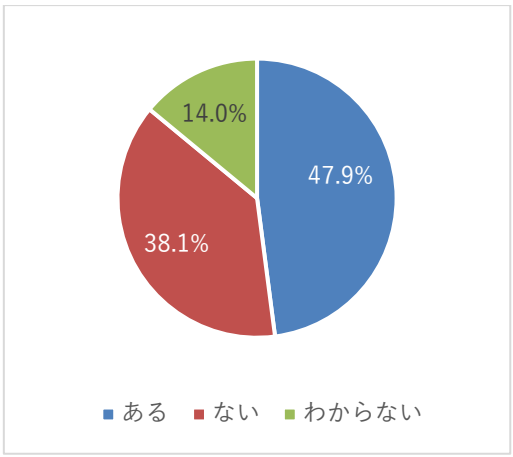
2022 年



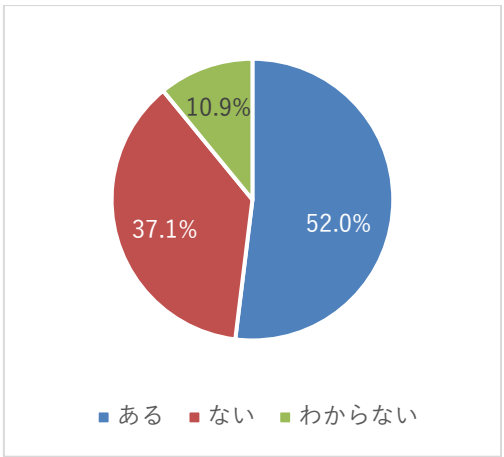
2023 年

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」の回答割合が減った。

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？(n=5332)



この 1 年間 n=5332
（2022 年 12 月～2023 年 11 月）

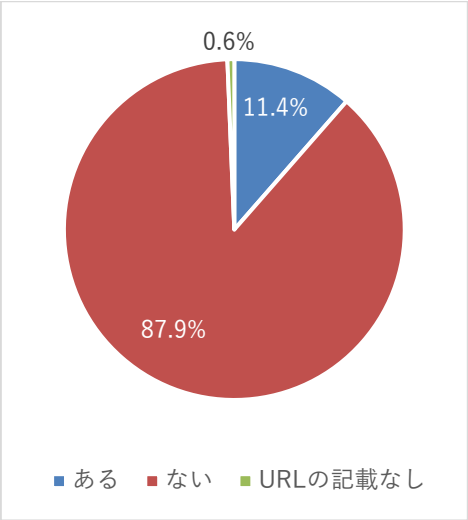


この 1 年間よりも前 n=5332
（2022 年 11 月以前）

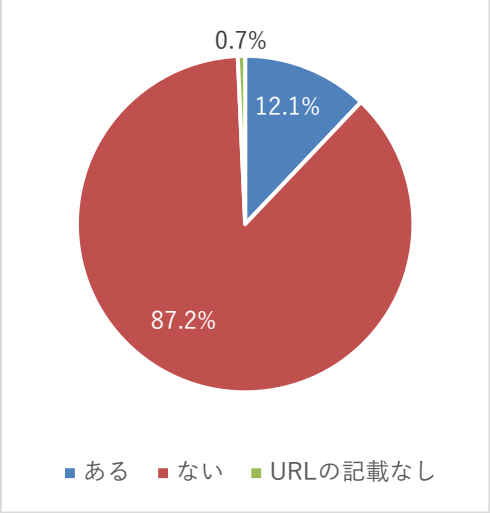
今回の調査では、フィッシング詐欺 SMS の受信やその被害について、この一年間（2022 年 12 月～2023 年 11 月）とこの 1 年間よりも前（2022 年 11 月以前）に対象期間を分けて質問した。

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、半数以上の方は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、4.1pt 増え、「わからない」が 1pt 減っていた。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る。

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



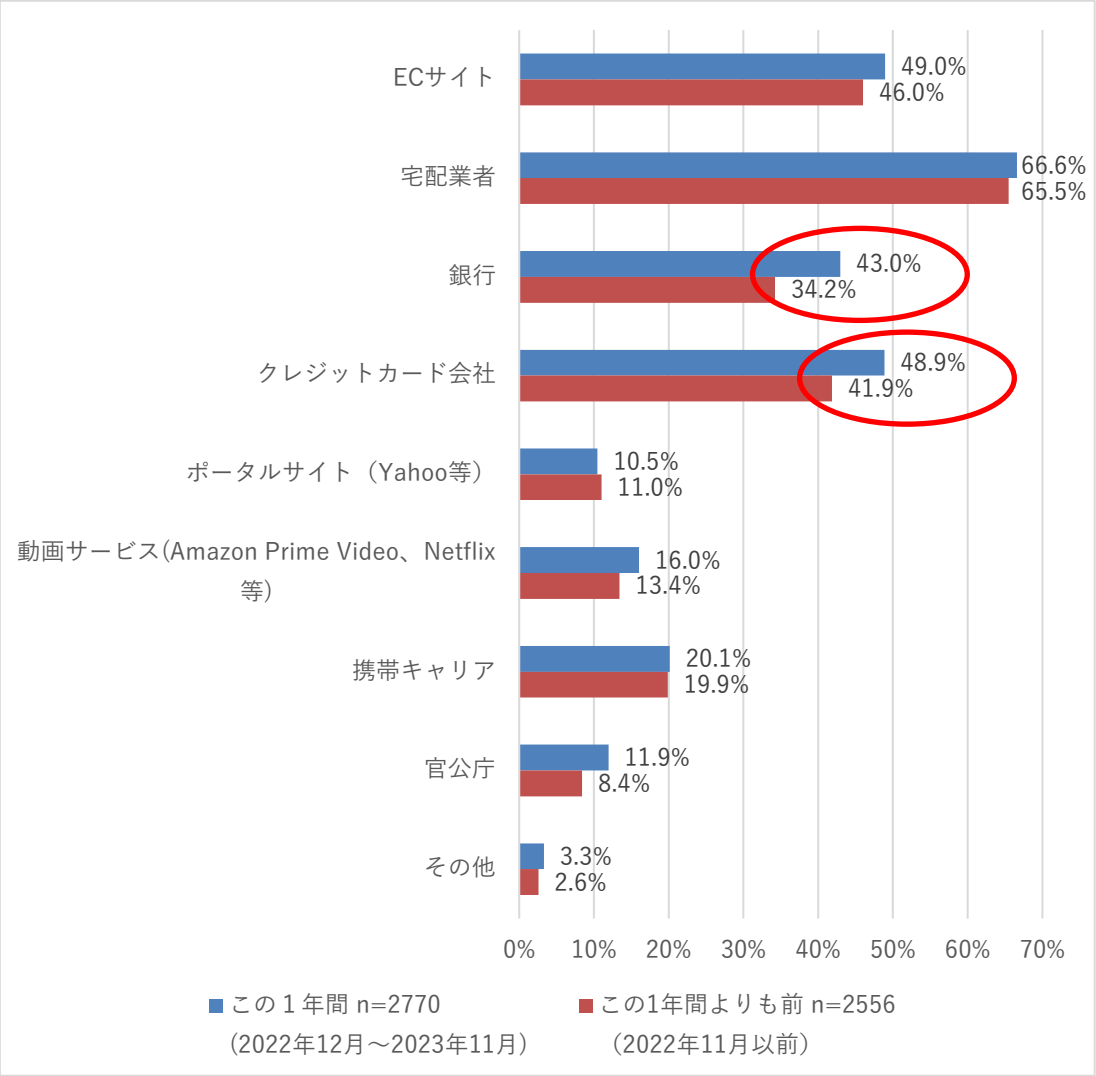
この 1 年間 n=2770
（2022 年 12 月～2023 年 11 月）



この 1 年間よりも前 n=2556
（2022 年 11 月以前）

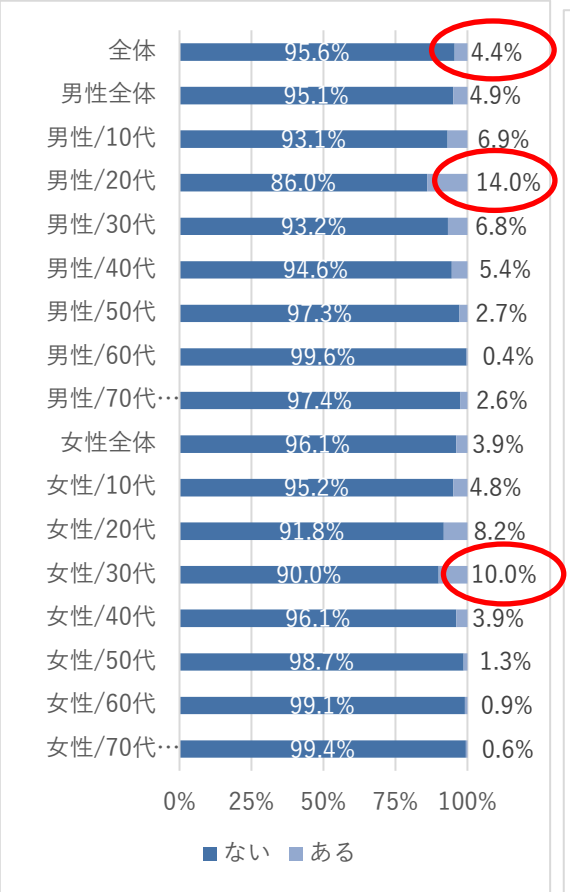
今回の調査より、フィッシング詐欺と考えられる SMS を受け取ったことがあると回答した方を対象に、メッセージ内の URL をタップし、サイトにアクセスした事があるかを新たに質問した。「この一年間」で「ある」と回答した方は「この 1 年間よりも前」と比較し、0.7pt 減少していた。フィッシング詐欺を警戒し、詐欺サイトへのアクセスを未然に回避する方が増えた可能性がある。

Q4. 何を装ったフィッシング詐欺でしたか？　※複数回答可

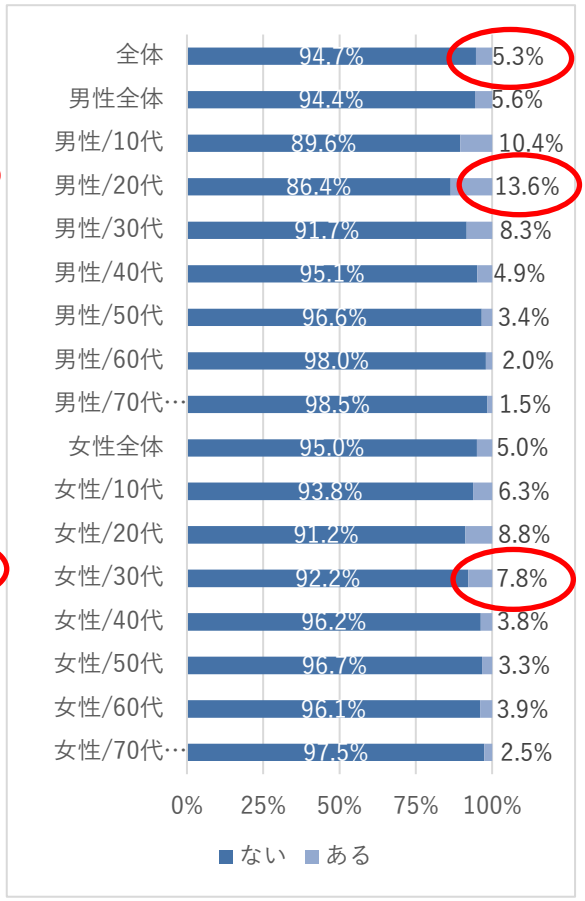


宅配業者や EC サイトなど、消費者が日常的に利用するサービスを装う手口の割合が多いのは、前回調査と同様だった。「この 1 年間」と「この一年間よりも前」を比較すると、銀行やクレジットカード会社を装う手口の増加率が大きい。攻撃者にとって、より直接的に金銭を詐取する手口を用いる傾向が強まっていると想定される。

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？



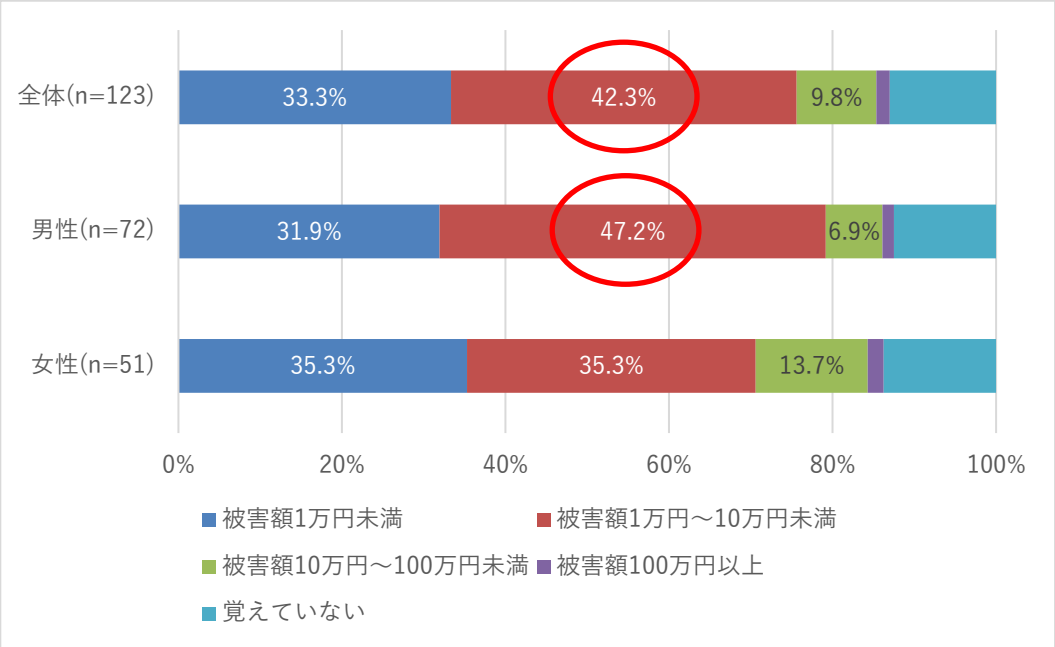
この 1 年間 n=2770
（2022 年 12 月～2023 年 11 月）



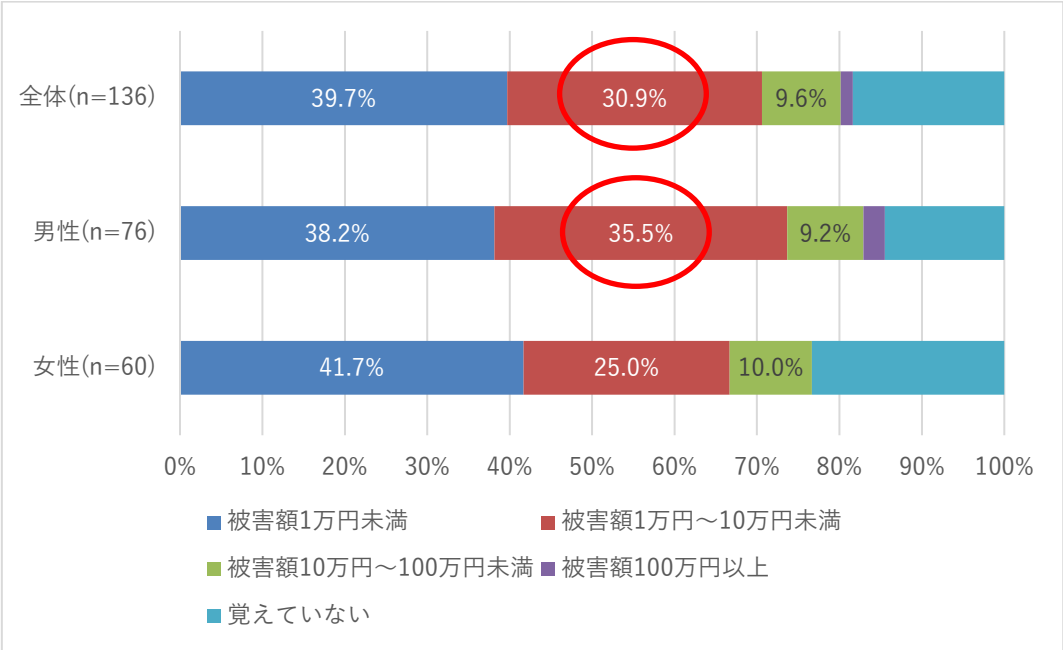
この 1 年間よりも前 n=2556
（2022 年 11 月以前）

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 5.3%、「この 1 年間」では 4.4%だった。「この 1 年間」の特徴的な点として、男性の 20 代が 14%、女性の 30 代は 10%と全体での割合を大きく上回り、いずれも「この 1 年間より前」よりも増加していた。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。

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
（2022 年 12 月～2023 年 11 月）

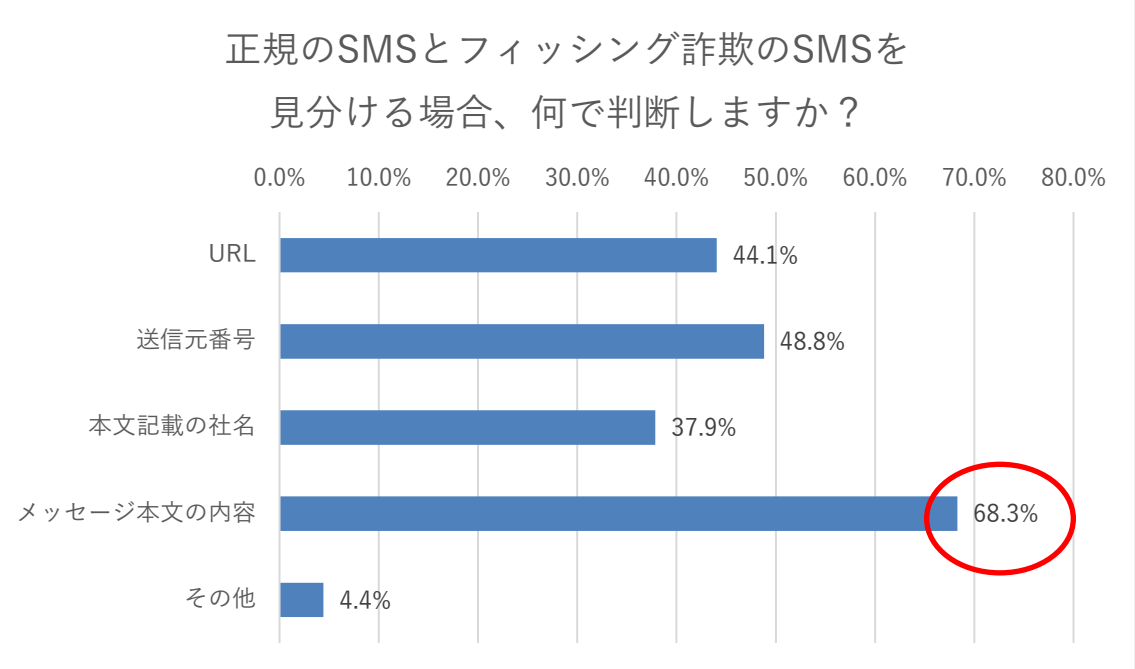


この 1 年間よりも前
（2022 年 11 月以前）

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、30.9%だったが、「この 1 年間」では 42.3%と 11.4pt 増えている。特に男性の「被害額 1 万円～10 万円未満」の割合が大きく増えていた。「この一年間」の被害の最大額は 250 万円で、30 代の女性からの回答だった（不正アプリをインストールさせる手口）。「この一年間よ

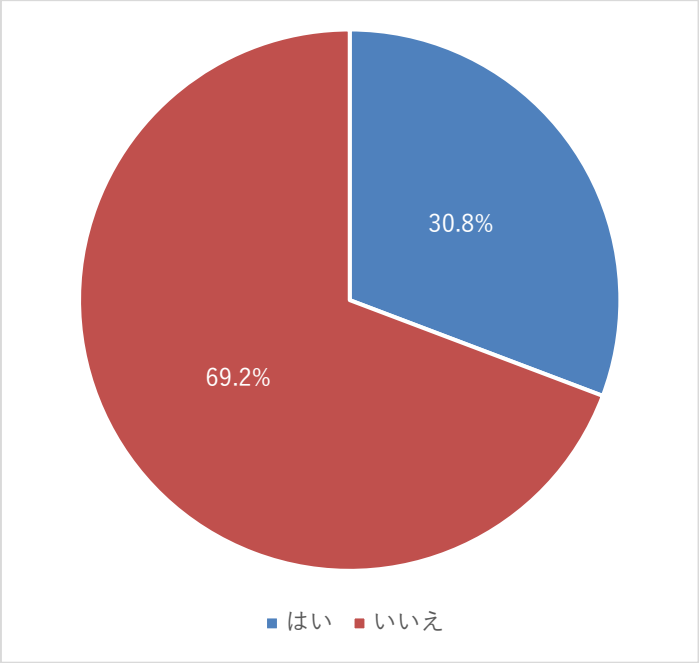
り前」での被害の最大額は 30 代の男性からの回答で 500 万円だったが、この方は「この一年間」でも同様の手口で「被害額 1 万円～10 万円未満」の被害にあったと回答していた。「この一年間より前」で被害にあった方は 136 人、その内「この一年間」でも被害にあったと回答したのは 73 人で、「この一年間より前」に被害にあった方の約半数が「この一年間」で再度被害にあっている事がわかった。一度被害にあった方は、繰り返し被害に合う可能性が高いと考え、日頃からフィッシング詐欺に関する情報収集を行い、慎重な行動を取るなど自衛の対策が必要である。

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=5332)



メッセージ本文の内容が 68.3%と最も多い回答割合となった。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、正規の SMS とフィッシング詐欺の SMS を見分けることは難しい。URL については、ドメイン名によって見分ける事が可能だが、正規のドメイン名と似たドメイン名を用いられる事が多い事から、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ある。

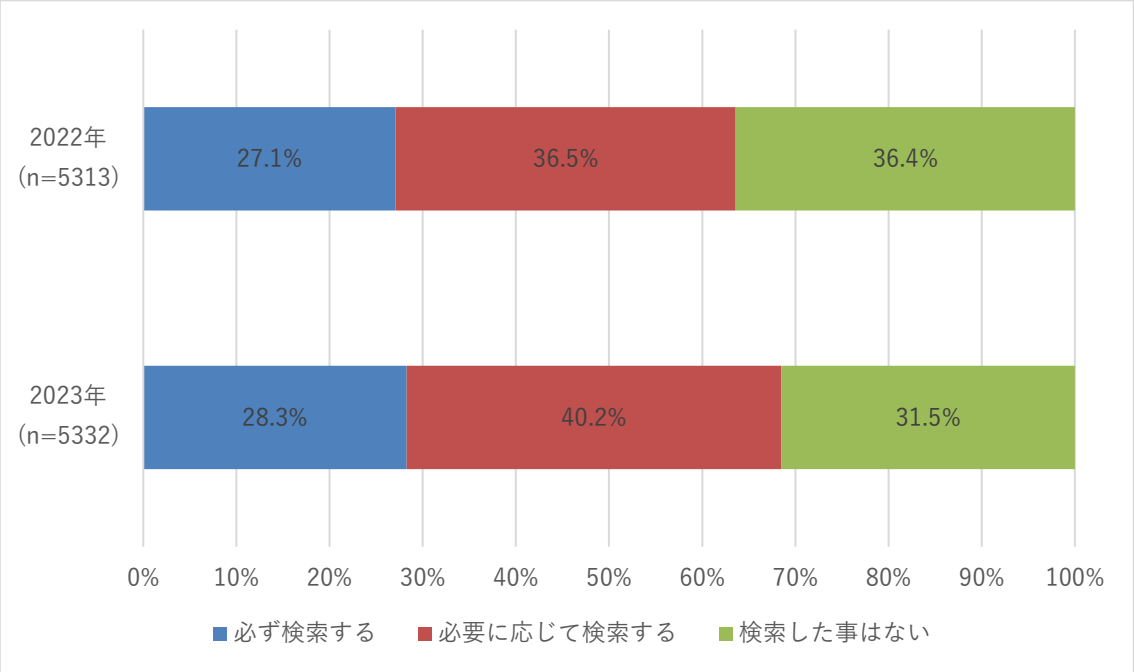
Q8. SMS の送信元番号が携帯電話番号の場合は、国内の固定電話番号の場合と比べて、フィッシング詐欺の可能性が高くなる事をご存知でしたか？(n=5332)



不正アプリに感染させた携帯電話端末を利用して、フィッシング詐欺の SMS を送信する手口が増えている事や携帯電話回線(SIM)を利用した SMS 送信サービスを提供している事業者が、利用者の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使われやすい事から、今回の調査から、質問に追加した。

回答者のうち約 3 割の方が、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たが、大半の方には、認識されていない状況だった。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る。利用者へ注意喚起を行っていく事に加えて、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る。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る。

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だが、「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 4.9pt 増加した。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る。

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事がフィッシング詐欺への対策になり得る。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、速やかに公表する事を強く推奨したい。

＜まとめ＞

SMS を使ったフィッシング詐欺が増えるにつれて、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る。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た。また今回の調査で新たに追加した「この 1 年間」と「この 1 年間以前」の比較や前回調査との比較によって傾向把握することができた。

「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 52%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 4.4%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。最近のSMSを利用したフィッシングでは、携帯キャリアの不正対策フィルタリングを回避するためか、携帯電話回線を利用したSMS配信や企業名やブランド名を騙らないフィッシングも増えている。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る。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」を参照いただきたい。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ない。今後も利用者向けの周知を強化していく必要がある。

＜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：2023/12/01 ～ 2023/12/07
有効回答者数：5,332 名
回答者の属性：
【性別】男性：50.3%　女性：49.7%
【年代】10 代：13.7%、20 代：14.3%、30 代：14.3%、40 代：14.5%、50 代：14.3%、60 代：14.3%、70 代以上：14.5%
※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 ドメイン名廃止にあたっての注意

昨年（2023 年）は、公共機関などによって登録された新型コロナウイルス感染症(COVID-19)関連のドメイン名が廃止され、第三者によって登録されるというニュースがいくつか報じられた。毎年本レポートで取り上げているテーマであるが、本年も注意喚起の意味を込めて、ドメイン名の廃止に関する注意事項をご紹介する。

5.1.1 ドメイン名廃止のリスク

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・利用できなくなるだけでなく、一定期間後に第三者が登録・利用できるようになる。これにより、まったく関係のない Web サイトを作られる可能性がある。さらに、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、ブランド悪用などの行為につながることも考えられる。

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すると、メール経由でパスワードを再設定され、アカウントが乗っ取られ、機密情報が盗まれる恐れもある。

5.1.2 ドメイン名を廃止する前に

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する

◆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検討して欲しい。

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：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 ドメイン名を登録する制度がある。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、積極的な利用検討を勧めたい。この制度の利用についての詳細は、登録中のドメイン名を管理している事業者に相談して欲しい。

◆廃止前には十分な時間をかけた準備を行う

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。

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」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。

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ある。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ある。

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。

【松尾佳彦 株式会社日本レジストリサービス】

5.2 DMARC, DNSSEC によるドメイン名の信頼性を上げよう

Google が発表した「メール送信者のガイドライン」により突然 DMARC への対応を急ぐ企業が増えた。また、「高校出願システムから送信されたメールが Gmail に届かない」というニュースが大きな話題になり、普段からメールは相手に届いて当たり前と思っていたものが、突然、いかにメールを相手に届けるかに関心が高まりました。2022 年のメールの世界での流量の内、ユーザーが必要としないのに勝手に送られてくる SPAM メールの割合は、いろいろな組織の統計値があるが、おおよそ約半数が SPAM メールとなっています。2011 年は、8 割が SPAM メールだったようなので、いろいろな努力によってかあるいは、SMS や SNS 等への移行によるものか不明ですが、減少傾向にはあるようです。ただし、この統計数値はシステムで SPAM と自動で判定された割合で、実際のユーザーが不要と判断したメールではありません。もし、実際のユーザーによる判断で数値を取った場合、重要でないメールの割合はかなりのものだと想像できます。そうだとすると、迷惑メールと判断できるものをシステムで選別するのではなく、その逆で信頼できるメールをユーザーに届けることが重要になってきていると思われます。そのためには、メールを送信するドメイン名の信頼を上げて、このドメイン名から送信されるメールは信頼できるものであるという仕組みも求められてくると思います。その仕組みの一つが DMARC だと考えていただいた方がいいと思います。DMARC を迷惑メール対策の数ある技術の一つと考えるのではなく、逆のアプローチで信頼できるメールをユーザーに確実に届けるための仕組みと考える必要があると思います。

DMARC を数ある迷惑メール対策の一つとして考えた場合、その導入コストと効果で考えると、あまりコスト対効果を感じないかもしれません。しかし、自組織で送信するメールを信頼してもらい確実にユーザーに届けるという方向で考えると、特に信頼を必要とする組織にとっては重要性が上がってくるかと思います。

ドメイン名に信頼を与えるということでは、「.BANK」および「.NISURANCE」の二つのトップレベルドメインを運営する fTLD の活動はドメイン名の信頼性を上げるということでは参考になると思われます。fTLD は、「.BANK」「.INSURANCE」ドメイン名を「オンラインにおける信頼の証 (online stamp of trust)13」と位置付けており、それが信頼されるようにするためにドメイン名の取得に下記のような条件が含まれており、EV 証明書の取得より厳しい条件を求められています。

- ドメイン名と組織の正式な名前またはブランドとの一致
- DNSSEC の実装
- TLS 1.2 以降の実装を Web およびメールに適用

[13] https://www.bankrate.com/banking/what-is-dot-bank-domain/

・ DMARC の実装

これにより、ユーザーは、「.bank」または「.insurance」に属するドメイン名は、信頼してメールを受信することができるし、Web サイトも安心して接続することができる。ユーザーは、最後が「.bank」まはた「.insurance」で終わるドメイン名かどうかを確認すればいいことになる。「.bank」「.insurance」では、類似したドメイン名を取得することはできないため、「.bank」「.insurance」さえ確認すれば、金融機関を騙った詐欺サイトへ誘導されることもなくなる。

DMARC は、DNS レコードの中に書かれるため、これが改ざんされる可能性があるとDMARC の信頼性が落ちてしまいます。DNSSEC は、DNS レコードの改ざんによるドメイン名のなりすましを防ぐという目的もありますが、DNS レコードの中に記述される SPF, DKIM, DMARC のような重要なレコードを防ぐためにためにも重要性がかなり増してきていると思います。今後も DNS のレコード中には、BIMI や DANE など信頼に必要な情報が追加されてくると思われます。その DNS のレコードを保護するためには、DNSSEC が重要になってきていると思います。

最後に、電子証明書により技術的な信頼を上げても、大元のドメイン名の使い方がずさんになると人がそれを信頼できなくなってしまいます。受信するメールのドメイン名とそのメールの中に書かれているサイトのドメイン名が異なれば、技術的には改ざんの可能性が極めて少なく信頼できるとしても、ユーザーはアクセスに不安を覚えると思います。これまでドメイン名は IT の問題だと考えられて、IT に任せられていましたが、「ドメイン名が信頼の証」としてユーザーにその組織を認知してもらうためには、ドメイン名に対する一貫したポリシーが必要で、組織のブランド戦略の一貫として考える必要が出てきていると思います。

【野々下幸治　トレンドマイクロ株式会社】

【コラム】アカウント回復処理は、アカウント管理の最も脆弱な部分になる可能性が

2014 年 1 月初めに GitLab にユーザーの操作なしにアカウントが乗っ取られる可能性があるパスワードリセットの脆弱性(CVE-2023-7023)が見つかり、1 月末の段階でも 5,300 以上のインスタンスにパッチが未適用になっており、ニュースなりました14。

上記は、アプリケーションにおけるパスワードリセットの脆弱性ですが、多くのアカウント回復処理は、アカウント管理の運用の中で行われており、アカウントの新規開設に比べ、アカウント作成後は、クレジットカード情報の登録を含め、個人情報を登録した後にアカウントが乗っ取られる可能性があり、アカウント作成以上に本人確認を含め、強固なセキュリティが求められ、アカウントの回復処理は、システムの最も脆弱な部分になる可能性があります。

昨年 9 月以降に Amazon アカウントの不正アクセスが急増し、不正アクセスの被害は 2 段階認証を設定しているアカウントでも報告されており、何らかの方法で 2 段階認証がする抜けられ、ギフトカードなどを無断購入される被害が多く SNS などに報告されていました。実際の方法は、アマゾン社からの報告もなく、不明です。ただし、Amazon の MFA の回復処理は、Amazon の MFA の回復処理のヘルプ15を見ると十分なのか疑問が持たれます。回復のためには、身分証明書の画像をアップロードすることが求められていますが、アカウント作成時には、身分証明書を求められていないので、アップロードされた画像が本人であるかの確認は難しいのではないかと思います。もし、Amazon に登録されているメールアカウントも同時に ID/パスワードが攻撃者に取られている場合、MFA の回復と同時に送信されるメールは攻撃者に取られてしまい、MFA のリセットされたことを利用者が知ることなく、アカウントがとられてしまう可能性があります。

アカウント回復処理の問題で、システム侵害を受け大きな被害を受けた事例としては、昨年 9 月に大きなニュースになったラスベガスの MGM ホテルの事例があります。MGM を攻撃した「Scatterd Spider」と呼ばれる組織は、あらかじめ SNS の LinkedIn の情報を使って、従業員に成りすまし、MGM のヘルプデスクへ電話を掛け、担当者をソーシャルエンジニアリングで騙し、パスワードのリセットを依頼し、成りすました従業員のアカウントを乗っ取りました。MGM のヘルプデスクは、パスワードのリセットに従業員の名前と、社員番号、生年月日の基本的な情報のみで実施していたということです。Octo Tmpest と呼ばれる金融犯罪グループも同様の手口で、IT 管理者を騙し、初期アクセスのための従業員のアカウントを入手していたようです。

このように認証に関して、多要素認証等でいくらアカウントセキュリティを強化していても、アカウント回復処理に問題がある場合、重大なサイバー侵害につながる可能性があり、既存のアカウントがとられるため、気が付くのも遅れがちになります。よって、パスワード回復処理は、慎重に実装されるべきですが、多くの場合、緊急対応となるため、本人確認が甘くなりがちです。

できれば、人が介在せず、本人自身でアカウント回復処理ができるセルフパスワードリセットが望ましいですが、最初に挙げた Gitlab の件を含め、アプリケーションで提供されるアカウント回復処理にも脆弱性は見つかっており、２０２３年も２５件が報告されています。数としては、少ないですが、アカウント回復処理の機能を持っているアプリはそれほど多くはないと思われます。

したがって、アカウントの回復処理は、多要素認証を使用する要件がバイパスされる可能性があり、人が介在ケースやアプリで完結するケースに限らず、パスワードの変更・リセットに対する検討事項を列挙し、考えうるケースで抜けがないかしっかり検討すべきだと思われます。

【野々下幸治　トレンドマイクロ株式会社】

[14] https://news.mynavi.jp/techplus/article/20240127-2870306/

[15] https://www.amazon.co.jp/gp/help/customer/display.html?nodeId=GU3SL3GTHLHPDQ2H

6. トピック

6.1 SMS を用いたフィッシング、それに対する携帯キャリアの対策状況

SM S を用いたフィッシングでは、携帯電話番号が宛先となることから、不特定多数への送信等で利用される中、携帯キャリアも不審な SMS をブロックする等の対策を順次実施している状況が続いている。

2022 年 3 月～　危険 SMS 拒否設定（NTT ドコモ）

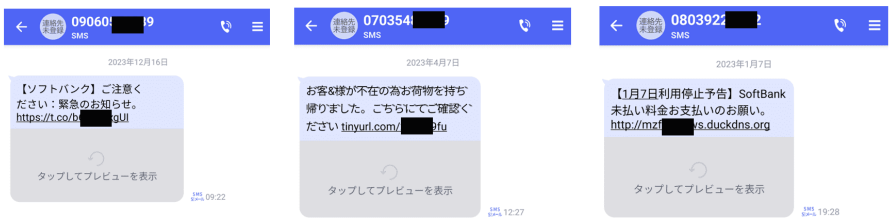
2022 年 6 月～　迷惑 SMS フィルター（ソフトバンク）

2023 年 2 月～　迷惑 SMS ブロック（KDDI）

SMS を受信した人は、メッセージの内容に加えて、SMS の送信元を確認することにより、フィッシングを疑う状況の中、疑わしい送信元としては主に下記 3 つのパターンがある。数年前は②のアルファベットを用いて、銀行や IT サービスの会社の名前を使うケースが多数を占めたが、近年ではマルウェアのスマホアプリをインストールさせられた人の携帯電話番号から①のパターンで送信される方法が主流となっている。

1	090、080、070 で始まる 13 桁の携帯電話番号【最近の主流】
2	アルファベットの文字列　（例）info、その他企業名等
3	国番号から始まる番号　（例）+1XXXXXX

① 090、080、070で始まる13桁の携帯電話番号からのフィッシングSMSの例



② アルファベットの送信元からのフィッシングSMSの例

図 6-1　実際のフィッシング SMS のメッセージ内容と送信元の例

受信する人にとって、①の送信元で送られてくるSMSには、フィッシングの他に、Ⓐ携帯キャリアが認めた正当な企業による双方向SMS、　Ⓑ携帯キャリアが推奨しないSIMファーム※1を利用する企業によるSMSも存在することから、従来は送信元でフィッシングを判別することが困難となっていた。

そのような状況の中、2023年1月に楽天モバイルがNTTドコモ、KDDI、ソフトバンクの連携に加わることにより、Ⓐにおいて携帯電話番号ではないショートコードを使用して、企業がSMSを送受信することが可能となった。※2　本件のショートコードは0005で始まる10桁の番号であり、かつ、他社によるなりすまし送信が不可能なため、正規な企業による SMS と考えることができるサービスとして、SMS アグリゲーター各社から提供されている。2024 年 1 月現在、アクリート社では約 100 社の顧客企業、約 200 件のサービスが本ショートコードを利用中であり、今後さらに利用企業とSMS配信数の増加、および受信する人々への認知度向上が期待される。

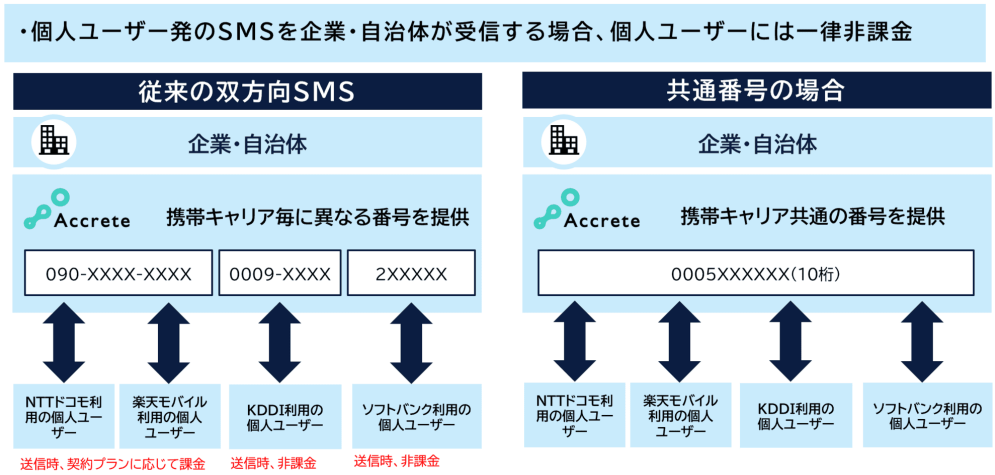


図 6-2　4 キャリア共通ショートコードによる双方向 SMS

一方で携帯キャリアはSMSの送信元をよりわかりやすくするための協議を続けており、Ⓐにおける携帯電話番号の利用を 2024 年 4 月以降認めないという決定をしている。加えて、Ⓑの SIM ファームについても、利用企業の管理ができないことから、携帯キャリアは非推奨という立場を継続している。そのため、企業から送信される正規のSMSにおいて、携帯電話番号で送信されるケースは今後減少していく見通しである。

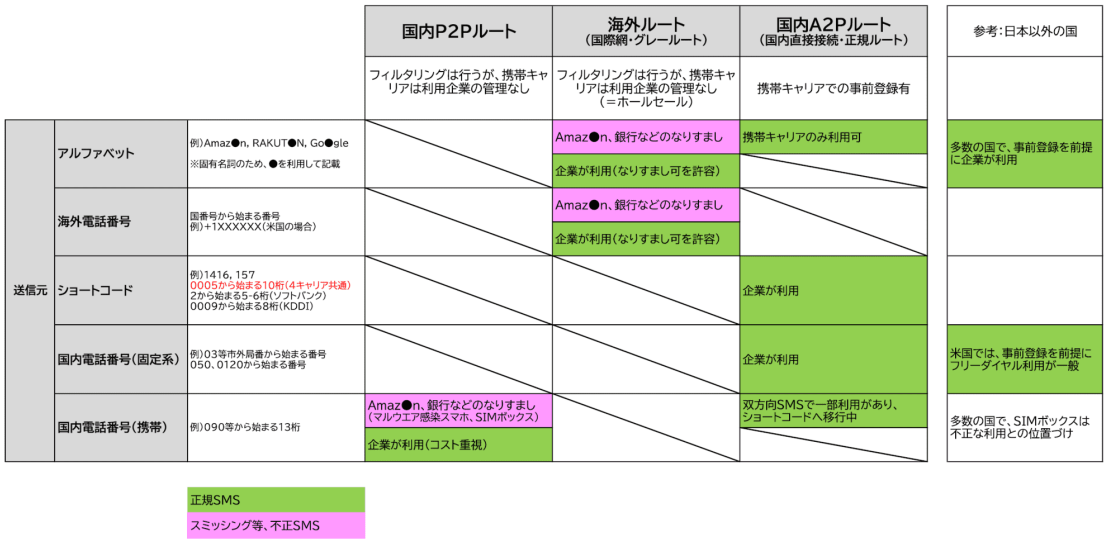


図 6-3　企業から送信される SMS の送信元

また、SMS と同様に GSMA で国際標準化されている RCS （Rich Communication Service）は、2019 年に国内携帯キャリア 3 社により、「＋メッセージ」としてサービスを開始した。2023 年 9 月末現在、3,800 万人が利用登録しているが、携帯電話ユーザー全体における普及率では約 2 割、そのほとんどが Android という点が、企業による利用が進まない理由となっているところ、Apple 社がメディアを通じて、iPhone の自社メッセージアプリにおける 2024 年後半の RCS 対応を公表した。※3

RCS 規格では企業の公式アカウントに認証済みマークが付くことから、メッセージを受信した人が容易に正規な企業からか否かを認識できる。そのため、今後は料金督促などの用途において「＋メッセージ」を利用する企業が増加することも想定される。

図 6-4　＋メッセージにおける公式アカウントの UI

【浦田泰裕　アクリート】

※1　SIM ボックスと呼ばれることもある（https://www.accrete-inc.com/reason/activity/）

※2　https://corp.mobile.rakuten.co.jp/news/press/2023/0110_01/

※3　https://9to5mac.com/2023/11/16/apple-rcs-coming-to-iphone/

6.2 Google と米 Yahoo が迷惑メール対策を強化

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」を発表した。（2023 年 10 月）

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、これらの対策は迷惑メールの一種であるフィッシングメールにも非常に有効である。

◆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る。つねに英語版とも比較しながら確認することを推奨する。

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

＜すべての送信者の要件＞

2024 年 2 月 1 日以降、Gmail アカウントにメールを送信するすべての送信者は、以下の要件を満たしている必要がある。

（以下 Google サイトより抜載。）

- ドメイン名に SPF または DKIM メール認証を設定します。
- 送信元のドメイン名または IP に、有効な正引きおよび逆引き DNS レコード（PTR レコードとも呼ばれます）があることを確認します。
- メールの送信に TLS 接続を使用します。
- Postmaster Tools で報告される迷惑メール率を 0.10% 未満に維持し、迷惑メール率が決して 0.30% 以上にならないようにします。
- Internet Message Format 標準（RFC 5322）に準拠する形式でメールを作成します。
- Gmail の From: ヘッダーのなりすましはしないでください。Gmail では、DMARC の検疫適用ポリシーの使用が開始されます。Gmail の From: ヘッダーのなりすましをした場合、メール配信に影響する可能性があります。
- メーリングリストや受信ゲートウェイを使用するなどして、メールを定期的に転送する場合は、送信メールに ARC ヘッダーを追加します。ARC ヘッダーによって、メールが転送されたことが示され、送信者が転送者と見なされます。メーリング リ

ストの送信者は、メーリング リストを指定する List-id: ヘッダー送信メールに追加する必要があります。

＜1 日当たり 5000 件以上の送信者の要件＞

2024 年 2 月 1 日以降、Gmail アカウントに 1 日あたり 5,000 件を超えるメールを送信する送信者は、以下の要件もあわせて満たしている必要がある。

（以下 Google サイトより抜載。）

- ドメイン名に SPF および DKIM メール認証を設定します。
- 送信ドメインに DMARC メール認証を設定します。DMARC 適用ポリシーは none に設定できます。
- ダイレクト メールの場合、送信者の From: ヘッダー内のドメイン名は、SPF ドメインまたは DKIM ドメインと一致している必要があります。これは DMARC アライメントに合格するために必要です。
- マーケティング目的のメールと配信登録されたメールは、ワンクリックでの登録解除に対応し、メッセージ本文に登録解除のリンクをわかりやすく表示する必要があります。

◆DMARC 認証を満たす必要がある

メールが DMARC 認証を満たすためには、SPF 認証と SPF アライメント、または DKIM 認証と DKIM アライメントのいずれかを満たす必要がある。SPF アライメントを満たすためには、From:ヘッダーのドメイン名と Return-Path アドレスのドメイン名の一致、DKIM アライメントを満たすためには、From:ヘッダーに含まれるドメイン名が、DKIM 署名の「d=」で指定したドメイン名と一致する必要がある。

◆正規メールとなりすましメールが区別可能となる

正規メールのドメイン名をなりすました偽メールは、DMARC 認証を満たすことができないため、フィッシングメールの多くを占める「なりすましメール」の対策として有効な対策と言える。また、BIMI(Brand Indicators for Message Identification)のような正規メールの視認性向上技術を併せて使うことで、利用者が正規メールのみを安心して読める環境が実現可能となる。

【加藤 孝浩　TOPPAN エッジ株式会社】
【平塚 伸世　一般社団法人 JPCERT コーディネーションセンター】

6.3 FIDO/Passkey に関して

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。中でもパスキーと呼ばれるオンライン認証の仕組みが多くのシステムで使用されている。パスキー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

パスキーでは FIDO(Fast Identity Online)の仕様をもとに制定されており、公開鍵認証方式を使用している。そのため、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が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。

パスキーではクレデンシャルとともに、当該サイトのドメイン情報をメタデータとして保存し、認証時にはメタデータにあるドメイン名が一致しないと失敗するようになる。フィッシングサイトではドメイン名が正規なものではないため、ここのチェックが失敗しフィッシングの被害を防ぐことが可能になる。併せて、パスワードを無効化することにより、パスワードに起因するフィッシング被害も起こりにくくなる。

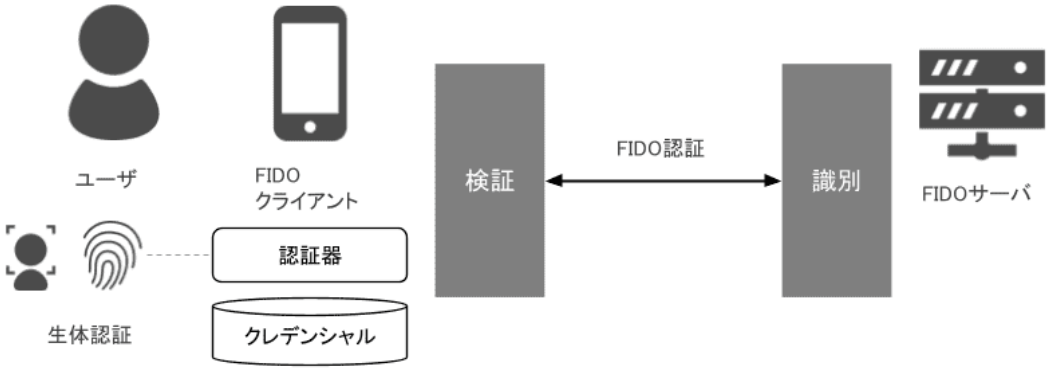


図 6-5　FIDO の認証モデル

パスキーでは、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。従来の FIDO と比較して、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。

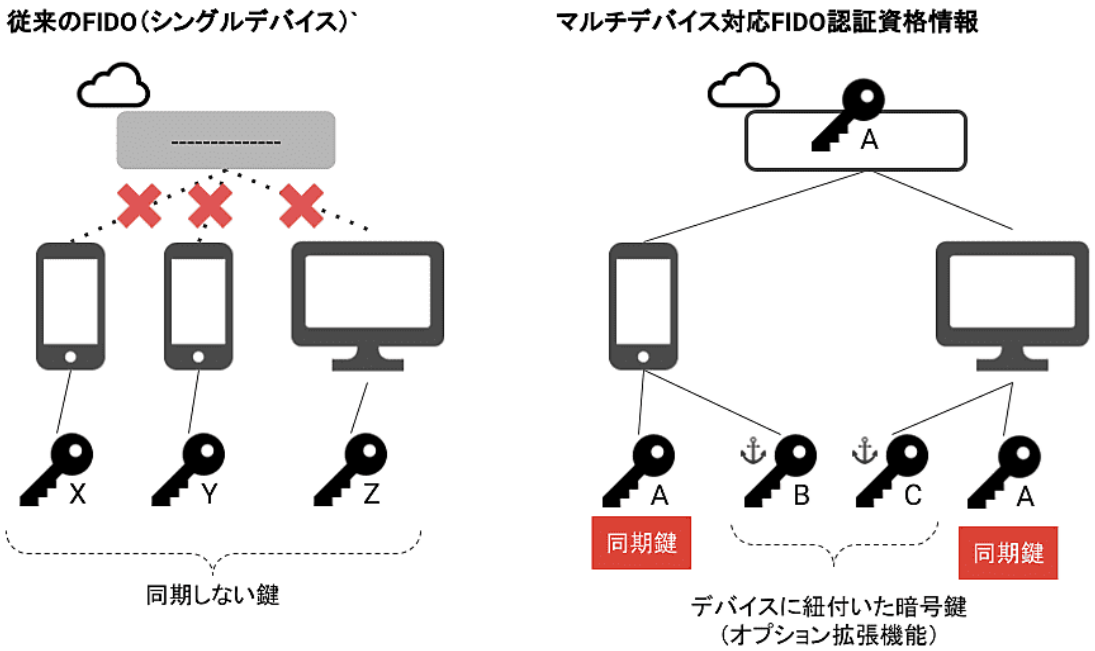


図 6-6　マルチデバイス対応 FIDO 認証資格情報

加えて Hybrid と呼ばれる機能で、二次元コードと BLE を経由して使って必要な認証器がないデバイスでもパスキーを使用することができる。ユーザーがパスキーを使用するとブラウザーが認証器の選択肢に二次元コードが表示される。ユーザーはパスキーで認証済みのスマートフォンを使用して二次元コードをスキャンし、BLE が使用できるようパソコンの近くで操作することでパスキーを使用することができる。

実際のパスキーのユースケースとして、例えば、スマートフォンで登録や認証を行っている場合、タブレット端末でも鍵が同期され、同じアカウントでログインすることができる。また、認証器がないパソコンでも先に解説した Hybrid を使用することにより、スマートフォンを使用してパソコンでも同じアカウントでログインすることができる。

以上のことからパスキーを使用することにより、セキュリティと利便性を両立させ、フィッシング対策としても期待できるため、安全なシステムを作ることができる。ログインの機能を持っている Web サービスでは是非パスキーの導入を検討することをお勧めする。

【松本 悦宜　Capy 株式会社】

6.4 不正アプリ検知ツールで検知した直近の「悪性アプリ」

スマートフォンの普及に伴い、不正アプリによる被害も増加している。不正アプリとは、不正な意図で開発されたアプリのことで、便利なアプリケーションをよそってユーザーにダウンロードさせ、端末内の電話帳の内容や位置情報などの個人情報を抜き取ったり、フィッシングＳＭＳを大量に送信するなどの不正な活動を行うアプリのことである。正規のアプリストアは事業者によって不正アプリかのチェックをされているが、そのチェックをすり抜けてしまうアプリも中にはある。セキュリティベンダーから不正なアプリのブラックリスト16やホワイトリスト17を使ったアプリフィルターが提供されており、これらのサービスを使うことにより安全に安心してアプリを使うことも可能である。

下記は、ホワイトリストを使った AI 基盤の不正アプリ検知ツール「Fake Finder」にて 2023 年 9 月から 12 月まで検知した悪性アプリの例である。

6.4.1 2023 年 9 月検知結果

（1） 悪性アプリ情報および検知時間

事例	PACKAGE_NAME	検知時間
①	あんしんセキュリティ	2023-09-13 15:48:40
②	Softbank セキュリティ	2023-09-13 15:57:11
③	KDDI セキュリティ	2023-09-27 12:03:10

（2） 悪性アプリの特徴

a. 基本事項

デフォルト SMS アプリとして設定を誘導

b. 動作事項

セキュリティアプリを偽装し、アドレス帳、SMS、電話記録等の個人情報を窃取

c. UI 特徴

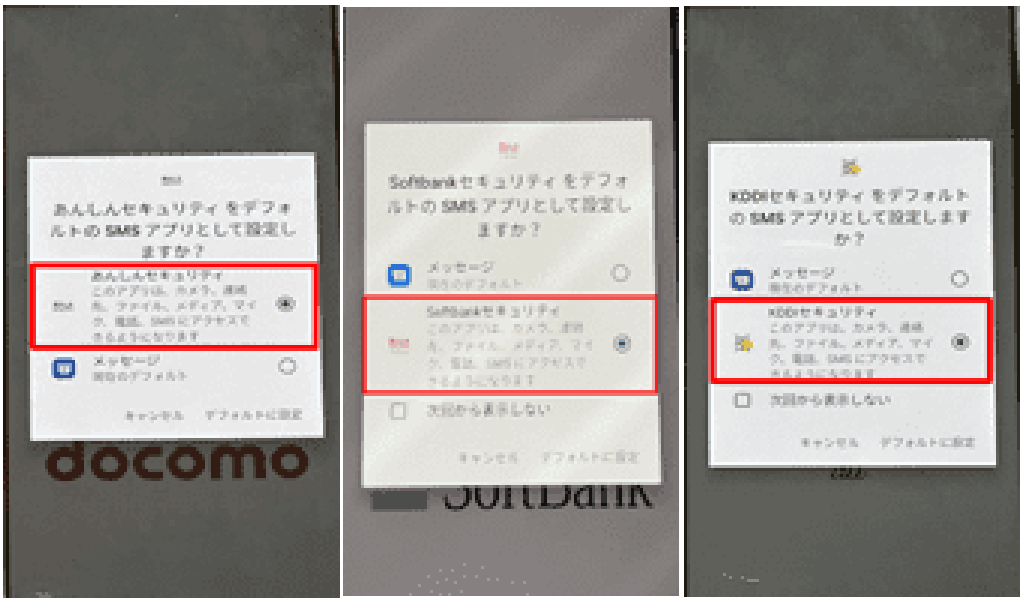
端末管理セキュリティアプリ（メモリ最適化、WIFI セキュリティ等）の UI 形態を偽装しているが、実際に操作を行っても動作しない

16 あらかじめ「危険な対象」を定義したリスト
17 あらかじめ「安全な対象」を定義したリスト

（3） 悪性アプリの動作について

a. インストール後の初期画面でデフォルトの SMS アプリとして設定を誘導

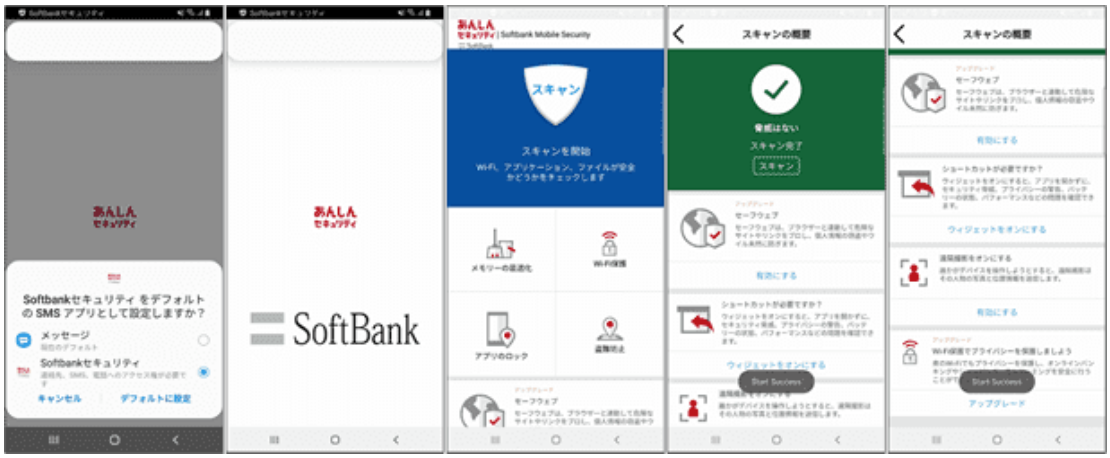
事例①　　事例②　　事例③



b. 悪性アプリの実行画面

【事例① あんしんセキュリティの偽アプリ】

【事例② Softbank セキュリティの偽アプリ】



【事例③ KDDI セキュリティの偽アプリ】

6.4.2 2023 年 10 月検知結果

（1） 悪性アプリの概要

a. 種類

金融機関または公共機関等を詐称する偽アプリ

b. 説明

該当機関の名称やアイコンを盗用するなど、悪意的な目的で作成されたアプリ、または、セキュリティプログラム、本人認証等の金融アプリの機能アップデートおよびその他 追加プログラム等になりすました偽アプリ

c. 事例

当該アプリがインストールされるとアプリ開発者のサーバーに自動的に繋がり、スマート フォンに他の悪性アプリを自動的にダウンロード・インストール

（2） 悪性アプリ情報および初回検知時間

事例	PACKAGE_NAME	初回検知時間
①	JPpost	2023-10-13 18:32:25
②	Chrome	2023-10-23 18:31:36

（3） 悪性アプリの特徴（Chrome を詐称した事例）

a. 基本事項

Chrome の偽アプリで「r」に見た目はほぼ同様だが通常とは異なるフォントとしてユニコードを使用（ユニコード情報：U+0433）- 電話、ファイルとメディア、SNS、連絡先へのアクセス権限要求（※1）

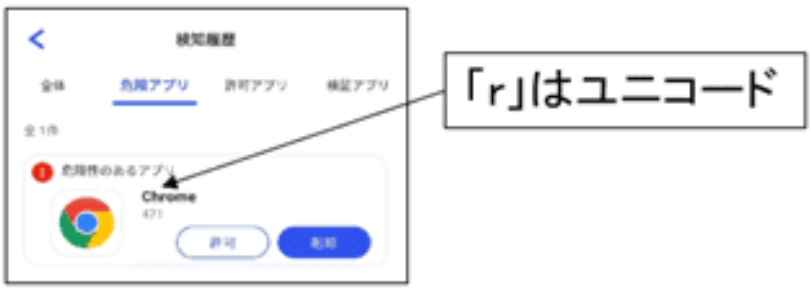
b. 動作事項

Android バージョン問題で強制終了後、目に見えない「悪性アプリ」を追加インストール（※2）

c. UI の特徴

アイコンが隠れて見えなくなる

※1「Fake Finder」悪性アプリ検知画面の再現

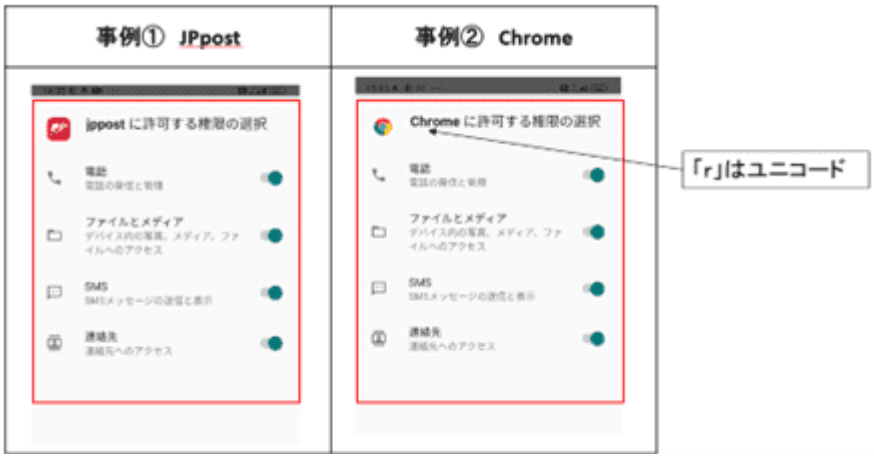


※2 アプリ強制終了時のエラーメッセージ

（4） 悪性アプリの動作について

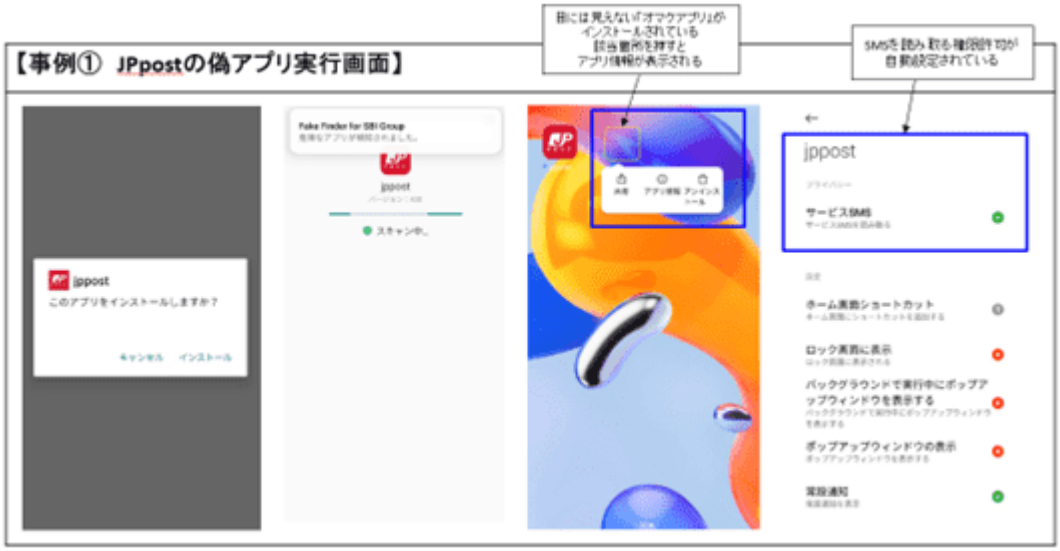
a. インストール後の初期画面

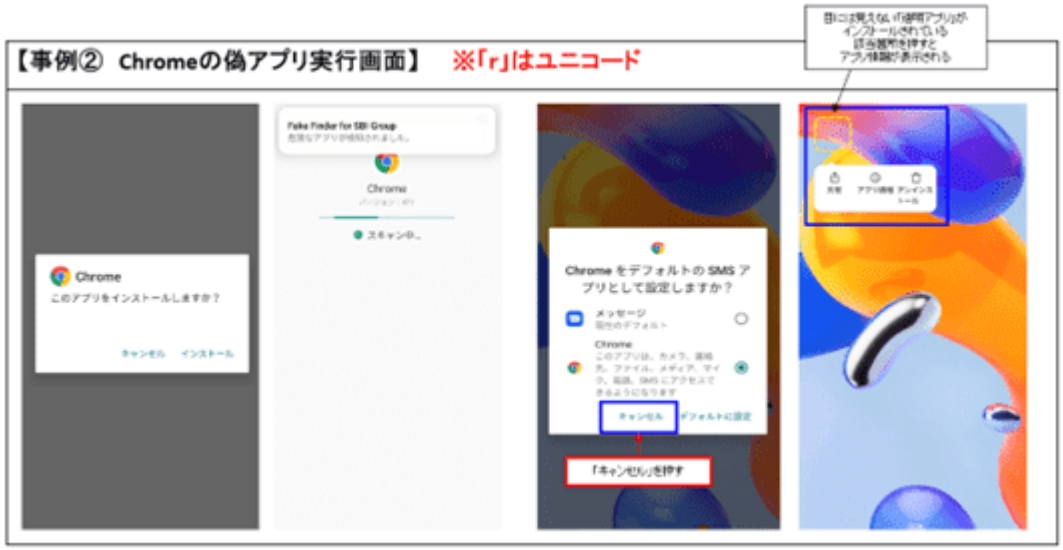
電話、ファイルとメディア、SMS、連絡先へのアクセス権限要求



b. 悪性アプリの実行画面

目に見えない「悪性アプリ」が追加でインストールされる


【事例① JPostの偽アプリ実行画面】
目には見えない「オマケアプリ」がインストールされている
該当箇所を押すとアプリ情報が表示される
SMSを読み取る権限許可が自動設定されている
jppost
このアプリをインストールしますか？
キャンセル
インストール
スキャン中。
サービスSMS
ホーム画面にショートカットを追加する
ロック画面に表示
バックグラウンドで実行中にポップアップウィンドウを表示する
ポップアップウィンドウの表示
常駐通知


【事例② Chromeの偽アプリ実行画面】 ※「r」はユニコード
目には見えない「偽物アプリ」がインストールされている
該当箇所を押すとアプリ情報が表示される
Chrome
このアプリをインストールしますか？
キャンセル
インストール
スキャン中。
Chrome をデフォルトの SMS アプリとして設定しますか？
メッセージ
Chrome
キャンセル
デフォルトに設定
「キャンセル」を押す

6.4.3 2023 年 11 月・12 月検知結果

（1） 悪性アプリの概要

a. 種類

個人情報を搾取する不正アプリまたは、金融機関または公共機関等を詐称する偽アプリ

b. 説明

該当機関の名称やアイコンを盗用するなど、悪意的な目的で作成されたアプリ

c. 事例

スマートフォンをフルコントロールするために、過剰な権限を要求。スマートフォンに他の「悪性アプリ」を自動的にダウンロード・インストール

（2） 悪性アプリ情報および初回検知時間

事例	PACKAGE_NAME	初回検知時間
①	Chrome	2023-11-28 15:24:10
②	SyncService	2023-12-08 16:33:48
③	Chrome	2023-12-15 14:42:31

（3） 悪性アプリの特徴（Chrome を詐称した事例、SyncService(アプリ名 hoverwatch)を詐称した事例）

a. 基本事項

- 事例①③：Chrome の偽アプリで「C」「e」に見た目はほぼ同様だが通常とは異なるフォントとして ユニコードを使用
- 事例②：「hoverwatch（監視アプリ名）」を詐称する偽アプリ

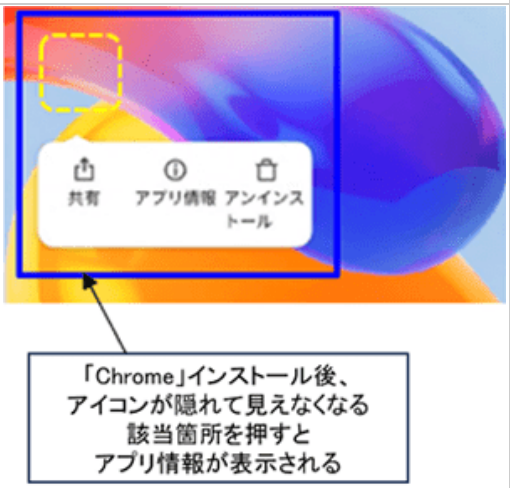
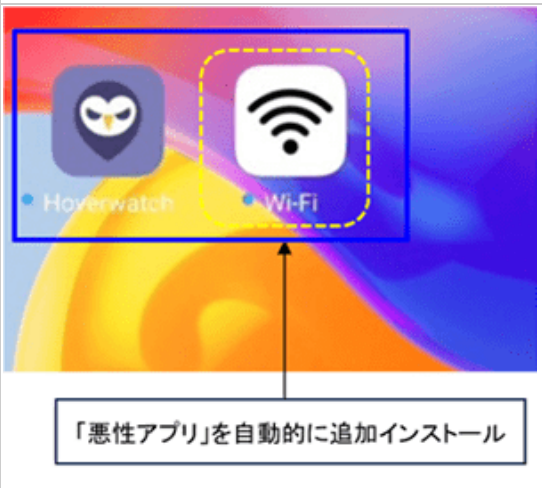
b. 動作事項

- 事例①③：個人情報を搾取するため、過剰な権限を要求
- 事例②：目に見えない「悪性アプリ」を追加インストールするとともにスマートフォンをフルコントロールするため、過剰な権限を要求

  - 電話、ファイルとメディア、SNS、連絡先等へのアクセス権限要求

c. UI の特徴

アイコンが隠れて見えなくなる、または「悪性アプリ」を追加インストール

「Chrome」詐称アプリのインストール後、アイコンが隠れて見えなくなる	「hoverwatch」詐称アプリのインストール後、「悪性アプリ」を自動的に追加インストール
	

(4) 悪性アプリの動作について

電話、ファイルとメディア、SMS、連絡先へのアクセス権限要求

（5） その他、同期間中の「Fake Finder」における遠隔操作アプリ（※）の検知結果について

集計期間	遠隔操作アプリ検知件数
2023 年 11 月～12 月	1,482 件

（※）遠隔操作アプリ：遠隔地にあるスマートフォンを監視または操作するアプリ

2023 年 11 月～12 月において、遠隔操作アプリの検知件数は 1,500 弱であった。昨今、インターネット閲覧中に偽のセキュリティ警告等を表示し、ユーザーの不安を煽り、画面に記載されたサポート窓口に電話をかけさせ、遠隔操作ソフト（アプリ）をダウンロード・インストールさせたり、サポートの名目で金銭を騙し取ろうとする、いわゆる「サポート詐欺」が全国的に多発している18,19,20が、「サポート詐欺」も遠隔操作を悪用した被害事例の一つとなる。遠隔操作が一度許可され接続が確立している間では、悪意のある第三者にスマートフォンの遠隔操作を受けながら、対面しているかのようなきめ細かな指示や案内を受けやすく、口頭では説明しにくい情報も画面越しに伝わり、見られたくない情報も画面に映し出されていれば相手に伝わってしまう恐れがある。Android 端末においては、遠隔操作の接続が確立している間において、端末内にあるアプリの起動や操作など

18 警察庁、サポート詐欺対策（https://www.npa.go.jp/bureau/cyber/countermeasures/support-fraud.html）（閲覧日：2024 年 2 月 22 日））

19 警視庁、スマホによる詐欺「偽警告音編」（https://www.keishicho.metro.tokyo.lg.jp/about_mpd/joho/movie/cyber/cs_anime/personal/300.html）（閲覧日：2024 年 2 月 22 日）

20 IPO 独立行政法人情報処理推進機構、遠隔操作を他人に安易に許可しないで（https://www.ipa.go.jp/security/anshin/attention/2020/mgdayori20201125.html）（閲覧日：2024 年 2 月 22 日）

を「操作する側」で行うことが可能な状態になり、Android 端末・iOS 端末においては「操作される側」の画面表示がリアルタイムに「操作する側」へ転送されているため、画面を覗かせているのと同じ状態になる。

図 6-7　遠隔操作アプリによる遠隔操作のイメージ

遠隔操作が許可され接続が確立している間は、画面に表示された ID,PW などの重要な情報が「操作する側」に伝わってしまう恐れ[21]があり、個人情報を窃取する手段になり得ること[22,23]を認識した上で「操作する側」に遠隔操作を安易に許可しないよう細心の注意を払う必要がある。

また、悪性アプリは、公式マーケット以外の場所で配布されることが多く、Android 端末では、Google Play 以外の提供元からもアプリを入手できるため、これを悪用して不正アプリが配布されている。昨今、スマートフォンにおけるアプリは、さまざまな開発者から数多く提供され、利用者がアプリをインストールすることが日常的になっている状況に乗じて、攻撃者は不正アプリへ誘導しようとする。そのため、不用意にアプリを入手して

---

21 令和 5 年 2 月時点の SBI EVERSPIN 社による検証では第三者の遠隔操作による Android 端末・iOS 端末でのバンキングアプリ等に登録された個人情報（ID・PW.・住所等）の閲覧および、あらかじめ遠隔操作の過程において奪取した ID・PW 等の個人情報を流用することにより Android 端末において遠隔操作による不正送金が可能であることを確認できた。

22　令和 5 年 12 月 25 日　警察庁・金融庁　フィッシングによるものとみられるインターネットバンキングに係る 不正送金被害の急増について（注意喚起）
（https://www.npa.go.jp/bureau/cyber/pdf/20231225_press.pdf）（閲覧日：2024 年 2 月 22 日）

23 警察庁、フィッシング対策
（https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html）（閲覧日：2024 年 2 月 22 日）

いると、思わぬ被害につながる恐れがある。不正アプリによる被害を回避するためには、原則としてアプリは公式マーケットから入手し、アプリを選ぶ際は、開発元の信頼性やアプリの機能、利用規約等を慎重に確認することが必要と考える。

【尹　慈明　SBI EVERSPIN 株式会社】

7. まとめ

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、フィッシングの動向やフィッシングに関わる動向について寄稿いただいてまとめられたものである。

1.3節で述べられているように、フィッシングのターゲットになっているブランドの数は 212 に上り、依然多い状況にある。手法もまた多様化している。送信元メールアドレスに正規のドメイン名を使用した「なりすまし」メールも多く、フィッシングメールのうち、平均約 74.9%はなりすましメールであるとの調査もある。この状況を受けてか、なりすましメールに対して、Google や米 Yahoo においてなりすましメールの対策が強化された。詳細は 6 章で取り上げられている。

2023 年度に取り上げられたドメイン名の管理について、本レポートでは 5 章でより具体的な解説がある。今後、ドメイン名の管理や将来的な廃止が想定される企業等の担当者の方には是非ご一読いただきたい。

本レポートが、フィッシング対策を行う企業等の担当者のみならず、フィッシングへの対策に関心を寄せる方にお届けでき、動向や情勢の認知を広げるとともに総合的な対策やそのあり方の議論の醸成に資するものであることを願う。末尾になるが、寄稿くださった技術・制度検討 WG メンバー、取りまとめに尽力された事務局の方々にお礼を申し上げたい。

【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】

明尾　洋一	サイボウズ株式会社
猪野　裕司	株式会社リクルート
梅野　祐太	ソフトバンク株式会社
浦田　泰裕	株式会社アクリート
遠藤　淳	株式会社日本レジストリサービス
掛谷　勇治	株式会社マクニカ
加藤　孝浩	TOPPAN エッジ株式会社
加藤　雅彦	長崎県立大学
狩野　耕太	株式会社みずほフィナンシャルグループ
川口　祐介	かっこ株式会社
熊沢　明生	ソフトバンク株式会社
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
小頭　秀行	KDDI 株式会社
鈴木　一実	株式会社マクニカ
鈴木　壮	OpSec Online Limited
関根　健太郎	かっこ株式会社
高田　加菜江	楽天グループ株式会社
田中　優成	株式会社アクリート
塚田　晴史	株式会社マクニカ
中村　翔太	KDDI 株式会社
野々下　幸治	トレンドマイクロ株式会社
早川　和実	NTT コミュニケーションズ株式会社
星加　匡人	株式会社みずほフィナンシャルグループ
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
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
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
株式会社三菱総合研究所