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 2021

2021 年 6 月

フィッシング対策協議会

技術・制度検討ワーキンググループ

フィッシング対策協議会
Council of Anti-Phishing Japan

目次

1. フィッシングの動向 1
1.1. 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. 狙われているターゲット 6
1.3.2. フィッシングメールの大量配信 6
1.3.3. 誘導先 URL の多様化 6
1.3.4. スミッシングの継続 7
2. WG の活動について 8
2.1. 今年度の WG 活動について 8
2.2. フィッシング対策協議会　各 WG の活動について 9
2.3. 認証方法調査・推進ワーキンググループでの報告について 14
3. フィッシングの被害について 18
3.1. 攻撃のトレンドや被害 18
3.1.1. 電子決済サービス不正引き出し被害および今後とるべき対策について 18
3.1.2. フィッシングサイト詐欺　個人のクラウドサービスの被害についての可能性 20
3.2. SMS 関係 22
3.2.1. 二段階認証を用いるスマホアプリケーション開発における推奨 API、およびブラウザーにおける将来的な対応 22
3.2.2. 正規の SMS と同一スレッドに偽装 SMS を紛れ込ませるフィッシングについて 24
4. フィッシングの対策について 27
4.1. 最新の動向 27
4.1.1. フィッシングと FIDO と最新動向 27
4.1.2. よりアグレッシブなフィッシング対策 29
4.2. ドメイン関連 31
4.2.1. ドメイン名を狙ったインシデント 31
4.2.2. ドメイン名の廃止にあたっての注意 32
5. まとめ 36

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、2020 年上半期では、新型コロナウイルス感染症に関連したサイバー攻撃として、医療機関や研究機関などに対する攻撃が確認されている。また、警察によるサイバー犯罪の検挙件数は、年間の検挙件数が最多となった前年の同期と同水準となり、令和２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 235 件であった。このうち 222 件が識別符号盗用型（アクセス制御されているサーバーに、ネットワークを通じて、他人の識別符号を入力して不正に利用する行為）であったことが報告されている。

インターネットバンキングの不正送金の被害件数（被害額）は、発生件数 885 件、被害額約 5 億 1,200 万円となり、前年同期と比べて大幅に増加した。被害の多くは、SMS や電子メールを用いて金融機関を装ったフィッシングサイトへ誘導する手口によるものと報告されている。

フィッシング情報の届け出件数について、2020 年は前年と比較して著しく増加した。（図 1-1）。金融機関や Amazon、楽天のなりすまし送信が多く報告されている。

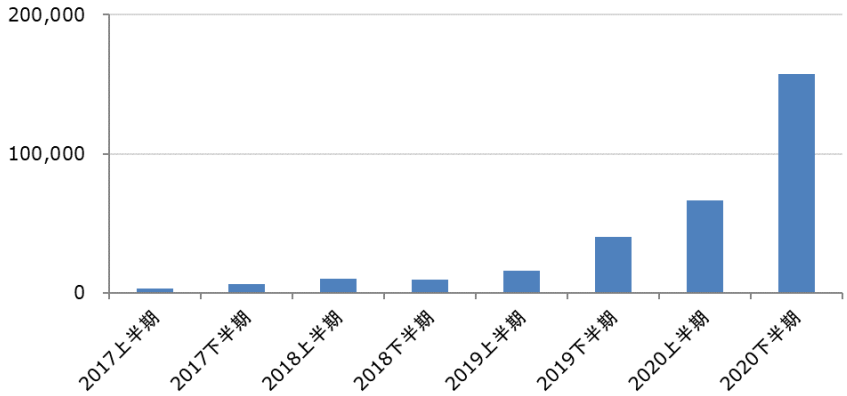


図 1-1　国内のフィッシング情報の届け出件数[2]

フィッシングサイトの URL 件数は、2020 年上半期、下半期ともに増加した（図 1-2）。ブランド名を悪用された企業の件数も、2019 年と比較しても増加

[1] 警察庁、 令和 2 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/R02_kami_cyber_jousei.pdf
[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）より作成
https://www.antiphishing.jp/report/monthly/

の傾向にある（図 1-3）。

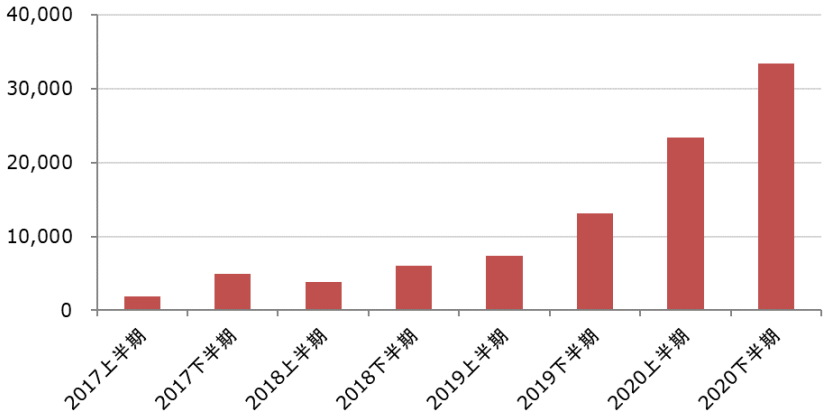


図 1-2　国内のフィッシングサイトの件数[2]

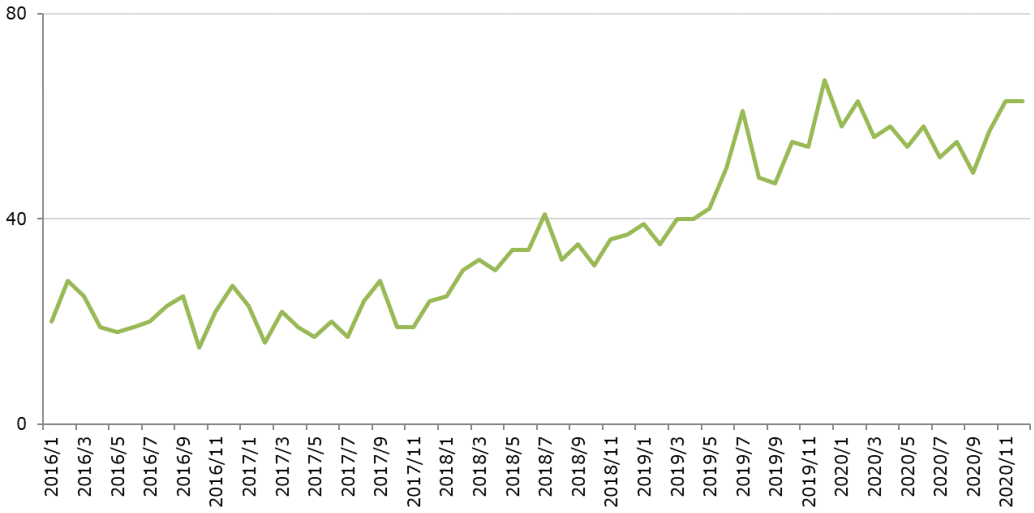


図 1-3　国内のブランド名を悪用された企業の件数[2]

また、国家公安委員会・総務省・経済産業省の発表によれば、2020 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 2019 年に比べてやや減少した（図 1-4）。しかしながら、2020 年の手口別内訳では、フィッシングサイトにより入手したものの割合が最も高く、前年比で 172 倍の増加となった（図 1-5）。

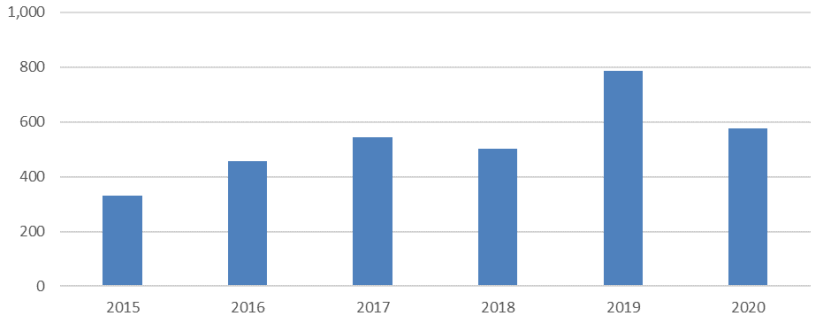


図 1-4　識別符号窃用（ID 窃盗）型不正アクセス行為の検挙件数 [3]

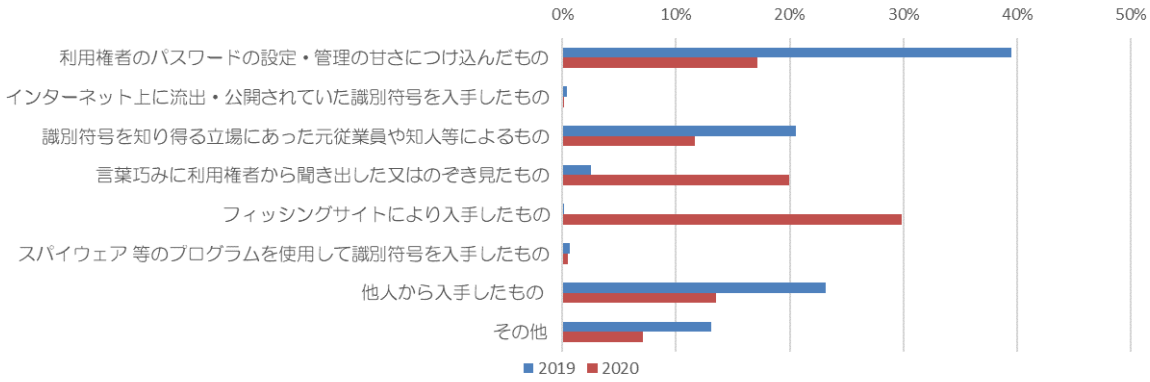


図 1-5　識別符号窃用型不正アクセス行為の手口別検挙件数の内訳（2019 年、2020 年）[4]

【エム・アール・アイリサーチアソシエイツ株式会社】

[3] 国家公安委員会・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/000735800.pdf より作成
[4] 同上

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、2019 年のフィッシング届け出件数は、2018 年から大幅に減少した。(図 1-6)。フィッシングサイトの件数は、2019 年上半期以降僅かに増加傾向であったが、2020 年上半期は減少した(図 1-7)。フィッシングによるブランド名の悪用の件数は増加傾向にある。(図 1-8)。APWG の報告書によると、新型コロナウイルス感染症(COVID-19)の拡大に伴い医療施設や失業者に対するフィッシングやマルウェア攻撃が急拡大したことが報告されている。全体のフィッシングの動向としては、Business Email Compromise のフィッシングが増加していることが示されているほか、フィッシングサイトの 7 割以上が SSL 保護されていることが示されている。

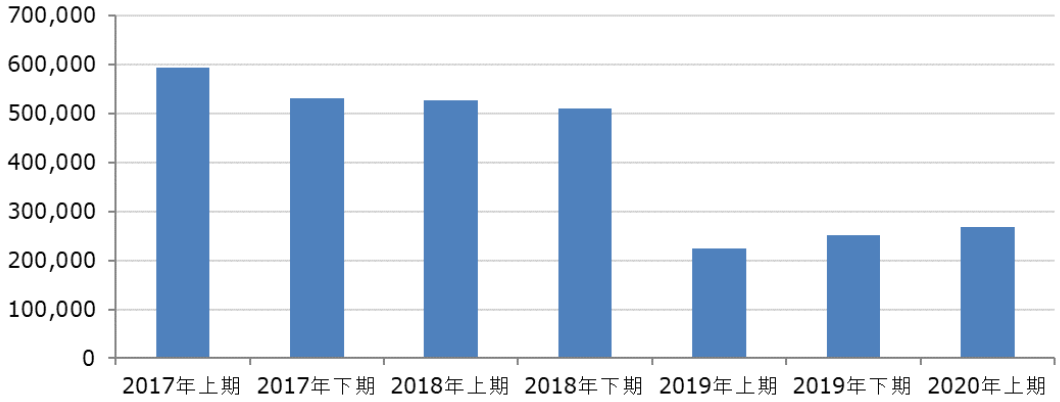


図 1-6　APWG へのフィッシングメール届け出件数 [5]

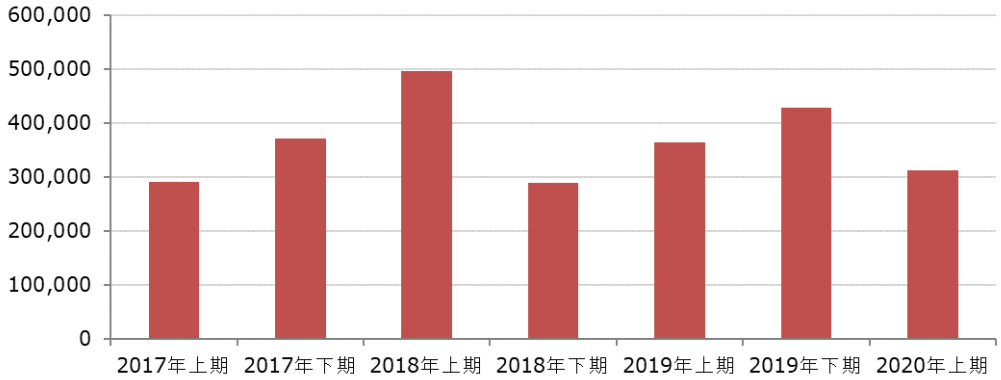


図 1-7　フィッシングサイトの件数（APWG）[5]

[5] APWG（Anti-Phishing Working Group)、"Phishing Activity Trends Report"、https://www.antiphishing.org/resources/apwg-reports/、より作成

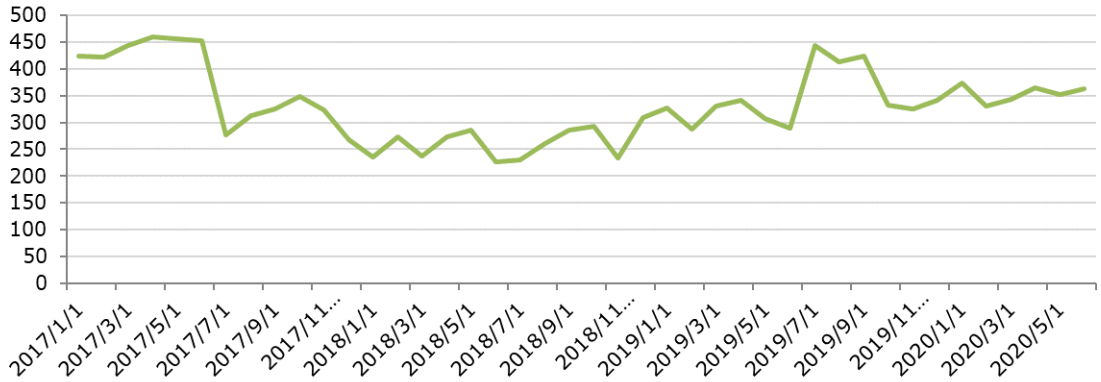


図 1-8　フィッシングによりブランド名を悪用された企業の件数（APWG）[5]

【エム・アール・アイリサーチアソシエイツ株式会社】

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 2020 年 1 月から 12 月までのフィッシング報告件数は 224,676 件で、2019 年と比較して約 4 倍となった。

1.3.1. 狙われているターゲット

クレジットカード情報の詐取を目的としたものが多いのは、例年通りであるが、2020 年に最も多くの割合を占めたのは、インターネットショップ・EC サイトであった。その割合は、全報告件数の約 68%を占めており、報告件数増加の要因となっている。原因としては、このコロナ禍において、インターネットショッピング需要が高まっていることが背景にあると考えられ、その利用者を標的としてフィッシングメールや SMS の大量配信が行われている。また、特別定額給付金の通知を装うフィッシングが発生したタイミングなどに注視すると、攻撃者は日本の状況をよく観察していることがわかる。その他、銀行やクレジットカードをかたるフィッシングも継続して行われていて、年末には、さまざまな地方銀行、クレジットカードをかたるものが多く報告されており、新たなターゲットを求め、詐欺の裾野を広げているように見える。

1.3.2. フィッシングメールの大量配信

2018 年頃からフィッシングメールの配信インフラが整ってきたと見られ、フィッシングメールの大量配信が行われるようになってきた。2020 年は、さらに配信の頻度が増えているが、ボットネットを使用したものから、国内事業者、海外事業者を経由したもの、正規のメール配信サービスを利用するなど、さまざまな方法で大量配信された。その大量配信系の配信先としてメールアドレスが登録されてしまうと、日に何件もフィッシングメールを受信することになるため、一人の報告者から数十通もフィッシングメールが添付されて報告されるケースも多かった。また、フィッシングメールの送信者メールアドレスが詐称された、なりすましメールも多く大量配信されており、それを阻止するためには、送信ドメイン認証技術（SPF / DKIM / DMARC）の更なる普及が望まれる。

1.3.3. 誘導先 URL の多様化

前述の大量配信頻度とあわせて、フィッシングサイトも短時間で誘導先 URL を次々と変えて構築されている。これは、攻撃者がブラウザーやセキュリティアプライアンス／サービスの監視・検知機構を回避するためと考えているが、ブラックリストによる検知を逃れるため、2020 年もさまざまな方法で行われている。

このようなサイトは、何度もアクセスするとアクセス不能となったり、短時間で停止したりするケースが多い。

【報告のあった誘導先 URL のパターン】
- 独自ドメイン大量に取得（ランダムな文字列＋正規サイトのドメインなど）
- 無料の DDNS (ダイナミック DNS) サービスを使用
- SNS サービスなどで使われる短縮 URL を使用
- メール配信サービスのトラッキング用 URL から誘導
- ドメインを取得せず、IP アドレスを直接使用した URL

1.3.4. スミッシングの継続

2018 年頃から増え始めたショートメッセージ（SMS）を使用したフィッシングも、引き続き行われている。宅配便の不在通知を装うものが多いが、誘導先が銀行やクレジットカードのサイトをかたるケースの報告もある。また、EC サイトをかたるスミッシングも新たに発生している。送信元情報を詐称する（海外発信）ケースの報告では、正規のスレッドに詐欺メッセージが混入するため注意が必要である。また、国内の携帯電話番号が送信元である場合は、前述の宅配便の不在通知を装うショートメッセージ内のリンクへアクセスし、不正アプリケーションのインストールを行ってしまった被害者のスマートフォンが遠隔操作されて送信された可能性が高いため、電話をかけたり、返信したりしないよう、注意や配慮が必要である。

【一般社団法人 JPCERT コーディネーションセンター】

2. WG の活動について

2.1. 今年度の WG 活動について

今年度の活動はコロナ禍ということもあり、活動をすべてオンラインによるコラボレーションツールとオンライン会議の仕組みを使って行った。オンライン会議は、対面での会議と異なり、インタラクティブな議論がやりづらい点があったが、事前のある程度の議論をコラボレーションツールで行うとともに、オンライン会議で議論をまとめるという方法を使うことにより対面での会議以上の議論もできたのではないかと思われる。すべてをオンラインで行うことにより、地理的な制約を受けずに会議ができるので、今後できれば、本 WG の活度に地方からの参加も期待できるのではないかと思った今年度の活動だった。

ガイドラインということでは、今年度は、SMS を使ったフィッシングのかなりの増加が目立ち、SMS について【要件 5】を追記した。また、日本においても DNS ハイジャックによる事案が発生したこともあり、【要件 22】のドメイン名自社のブランドとして認識して管理することについて、具体的な対策を分かりやすく書いていただいた。今年度はコロナ禍によりテレワークが進んだことにより、一般消費者のみならず企業ユーザーのフィッシングの危険性も高まったと思われる。このガイドは、一般消費者へのサービスを提供している事業者と一般消費者向けのガイドとなっているが、企業ユーザーにも適用できる部分もあると思われる。テレワークが進んでいる中、企業ユーザーも自社の IT 利用のユーザーのフィッシング被害を防ぐために活用していただけるとありがたい。

【野々下 幸治 トレンドマイクロ株式会社】

2.2. フィッシング対策協議会　各 WG の活動について

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。

2020 年の活動として、WG メンバーに対するオンラインによる情報共有に注力している。

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、二つの機能強化を行った。

- 「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。

また、2020 年度は従来のフィッシング詐欺に関する枠組みに限った活動から、「資格情報の奪取（credential harvesting）」までその範囲を拡張し、新たに三つのプロジェクトを開始した。

- 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。2020 年度は特に「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に注力した。

・ Carding Forums Meta Search

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

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

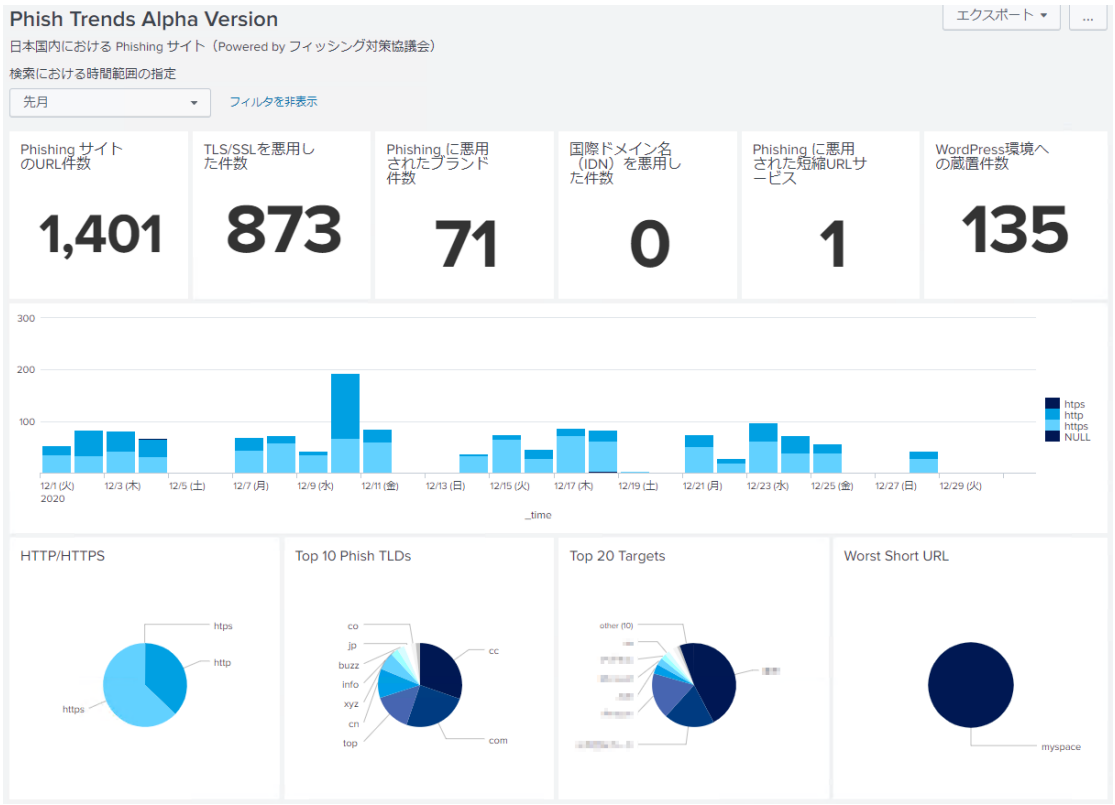


図 2-1　フィッシング詐欺被害状況ダッシュボード「Phish Trends」

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

フィッシング詐欺と関係性が深いインターネットサービスの認証について調

査を行い、より安全なサービス利用、より安全なサービス提供に向けた認証方式関連の情報を提供することでフィッシング詐欺対策を支援する。

2020 年の活動として、2019 年 2 月に実施したインターネットサービス提供事業者に対する 認証方法に関するアンケート調査に続き、インターネットサービス利用者に対する アンケート調査を実施し、結果報告書を公開。今回の調査によるインターネットサービス提供者側との意識の違いについて確認し、安全利用へ向けた意見をまとめる予定[6]。

◆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。

2020 年の活動として、各ブラウザーによる SSL/TLS サーバー証明書の表示の違いや主要ブラウザーのセキュリティ強化に対する施策、サーバー証明書の有効期限の短縮について情報提供を実施。

図 2-2 各ブラウザーによる SSL/TLS サーバー証明書の表示の違い[7]

[6] インターネットサービス利用者に対する 「認証方法」に関するアンケート調査結果報告書を公開 (2020/09/09) https://www.antiphishing.jp/news/info/20200909.html

[7] 【更新】主要ブラウザのセキュリティ強化に対する施策について（2020/8/24） https://www.antiphishing.jp/news/info/2020824.html
サーバ証明書の有効期限の短縮について https://www.antiphishing.jp/news/info/20200714.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。

STOP. THINK. CONNECT. とは
https://www.antiphishing.jp/pdf/about_StopThinkConnect.pdf
https://stopthinkconnect.jp/

2020 年の活動としては、『第 16 回 IPA 「ひろげよう情報モラル・セキュリティコンクール」 2020』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 [8]。

◆学術研究プロジェクト＜主査：唐沢 勇輔(Japan Digital Design 株式会社 / ソースネクスト株式会社)＞

フィッシングサイトの早期発見に関する研究を推進し、よりプロアクティブなフィッシング詐欺対策の確立を目指している。2017 年から長崎県立大学と共同で研究を進めている。

2020 年の活動としては、さまざまな手法があるフィッシング詐欺を一つの物差しで分析できるよう、フィッシング詐欺をビジネスプロセスとしてとらえて整理する手法についてまとめた。（情報処理学会第 92 回コンピュータセキュリティ研究会にて口頭発表予定）

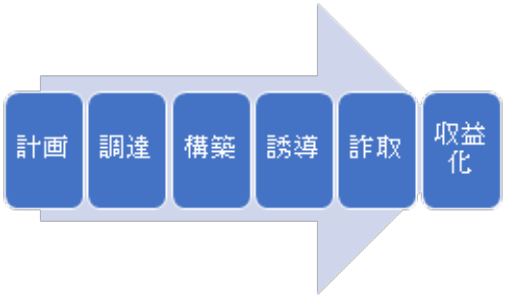


図 2-3 フィッシング詐欺ビジネスプロセス

[8] フィッシング対策協議会、『第 16 回 IPA「ひろげよう情報モラル・セキュリティコンクール」2020』の優秀賞を選出
https://www.antiphishing.jp/news/info/ipa_competition2020.html

2021 年度は参加メンバーで複数のテーマを担当し、研究を進める予定である。（テーマ例：フィッシングハンティング、スミッシング対策、フィッシングテイクダウンプロセス分析）

【加藤 孝浩 トッパン・フォームズ株式会社】

2.3. 認証方法調査・推進ワーキンググループでの報告について

認証方法調査・推進ワーキンググループは、フィッシング対策と関連の高いインターネットサービスの利用者認証について、サービス利用者へアンケート調査を 2020 年 3 月に実施し、その調査結果を報告書として公開した。

報告書全文をご覧になりたい方は、以下の URL よりダウンロード可能となっている。＜https://www.antiphishing.jp/news/info/20200909.html＞

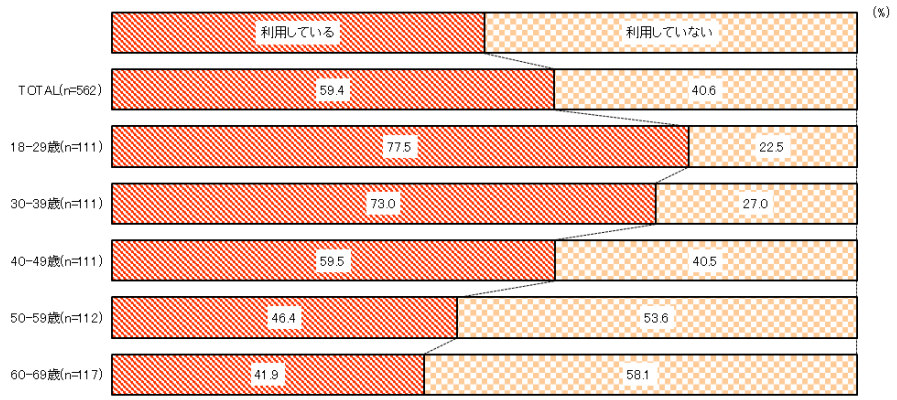
また、2019 年に実施した、インターネットサービス提供事業者に対する調査は、以下の URL よりダウンロード可能となっている。
＜https://www.antiphishing.jp/news/info/wg_auth_report_20190701.html＞

調査は、インターネットサービスの利用者（匿名）に対して、インターネットリサーチにより 46 問実施。年代ごと、男性、女性の比率などが同等になるよう配慮し、562 名から回答を得た。

以下、調査結果のポイントについて抜粋で紹介する。

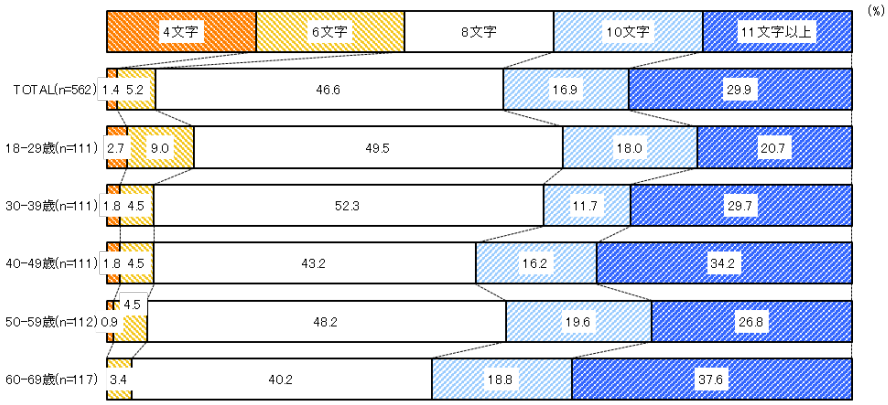
利用者認証において若年層で利便性重視の傾向があり、SNS 利用度の高い若い世代で SNS を中心としたアカウント管理が進んでいるほか、「ログインした状態にしておく」設定にするとの回答は、18 歳から 20 歳代が 49.5%と半数を占めていた。

Q26　SNS（LINE、Facebook、Twitter など）や総合サービス（Google、Yahoo！など）のアカウントを利用して、他のサービスに会員登録・ログインするサービスを利用していますか。



パスワード文字数については、半数以上の 53.2%が 8 文字以下で安全と思っており、8 文字では安全性が足りていない状況下において、事業者は 10 文字以上、可能であれば 12 文字以上を目指して設定をルール化してほしいところである。また、パスワードの管理については、専用のパスワード管理ソフトを利用している利用者は少なく、ブラウザーへパスワードを記憶させている利用者が 78.0%と多い状況であった。

Q11 パスワードの文字列について、安全と思う文字数を選択してください。



「二段階認証」を利用できる場合、どのようなサービスに利用したいと思っているか確認したところ、ネットバンキングに二段階認証を利用したいとの回答が 59.1%と 6 割近い結果を得た。ついでクレジットカード会員サービスとの回答が 45.6%と、資産を扱うサービスで二段階認証を利用したいとの傾向を確認した。これは、2019 年に実施したサービス事業者側の調査結果と同じ傾向でありサービス提供者と利用者の考えが合致している状況である。しかしながら、本人認証での不満点について、二段階認証が面倒との回答が 22.8%あり、二段階認証の手順のさらなる改善が必要と思われる。

Q44 パスワードに加えて、SMS やメール、ワンタイムパスワードなどの何らかの認証を行う「二段階認証」を利用できる場合、どのようなサービスに利用したいと思いますか？

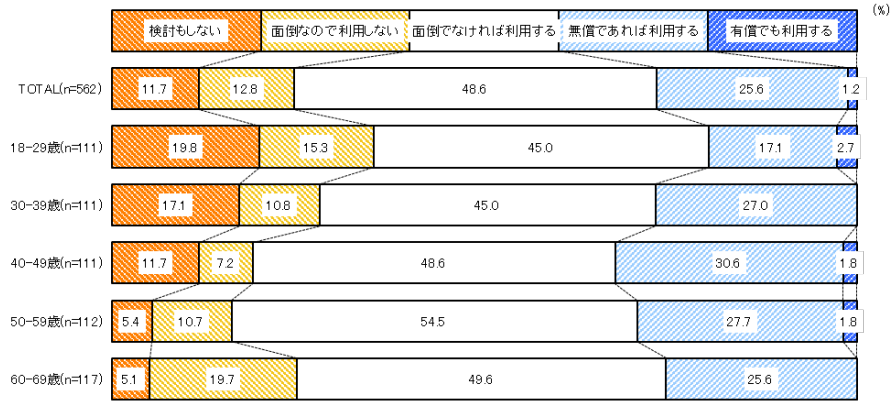
Q44：回答結果概要

ネットバンキングとの回答が 59.1%
クレジット会員サービスとの回答が 45.6%
証券との回答が 19.4%
通販（EC）との回答が 18.9%
保険との回答が 15.8%

SNS との回答が 14.1%
通信との回答が 11.9%
メールとの回答が 10.0%
特になしとの回答 24.4 が%
その他に、お金に関わるものとの自由回答もあった。

オプションでの追加認証については、面倒でなければ利用するが 48.6%と半数近くあり、無償であれば利用、有償でも利用とあわせて 75.4%は利用すると回答。面倒でなければ利用する 48.6%と、面倒なので利用しない 12.8%と合わせると、面倒か否かでの利用判断が 61.4%となり、6 割以上が面倒かどうかでオプション利用を判断している。

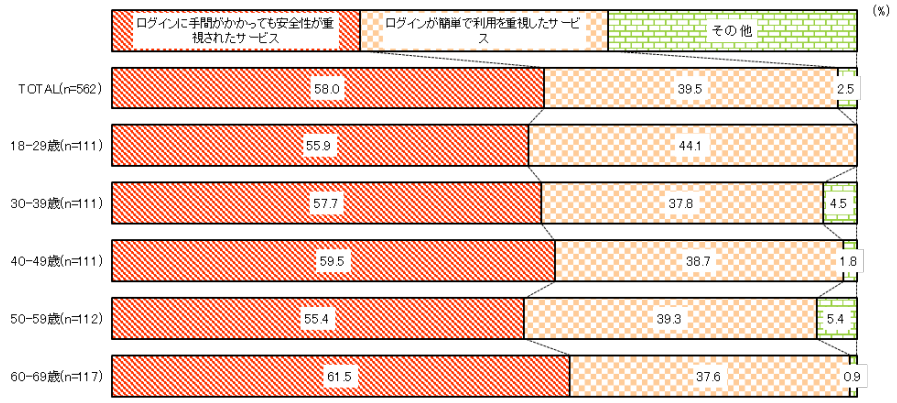
Q43 通常のパスワードより安全と思われる本人認証の方法がオプションで用意されていた場合、利用しますか。



認証に対する意識として、何となく不安である、不安を感じつつもログインしているとの利用者が 44.7%と半数近い状況。これらの「何となく」を解消するために認証の安全性について説明を強化するなど、不安を解消し安心して利用してもらうための施策が必要である。また、32.7%が不安は感じていないと回答しているが、この中には油断をしている利用者も含まれている可能性があり、より安全性の高い認証の利用に対する啓発も引き続き必要である。

安全性を重視したサービスと、便利な利用を重視したサービスでは、どちらを利用したいかとの問いに、58%は手間がかかり面倒でも安全性が重視されているサービスを求めている。反面、利便性を優先しており、安全性よりも便利な利用を重視した利用者が 39.5%あり、こちらは心配な状況である。

Q46 安全性を重視したサービスと、便利な利用を重視したサービスでは、どちらを利用したいと思いますか。



2019 年のサービス提供事業者向け調査では、「ユーザービリティー」よりも、「セキュリティ」を求める安全性重視の回答が 75%と高くあったが、今回の利用者調査では、面倒でも安全としたい回答は 58%にとどまり差が出ている。他の設問回答からも利用者は、安全性よりも利便性を優先し、便利な利用を重視しているため、これらの差を埋めるためにも安全確保にいっそうの工夫が必要である。

【長谷部一泰　アルプス システム インテグレーション株式会社】

3. フィッシングの被害について

3.1. 攻撃のトレンドや被害

3.1.1. 電子決済サービス不正引き出し被害および今後とるべき対策について

キャッシュレス化が進んでいる中、2020 年 8 月、NTT ドコモの「ドコモ口座」を経由して銀行預金が不正に引き出されるという事件が起こった[9]。不正利用の流れは下図のように、他人名義でドコモ口座を開設し、被害者の銀行口座から本人が知らない間に口座連携・チャージを行い、ドコモ口座から商品購入の代金を支払ったと推測される。

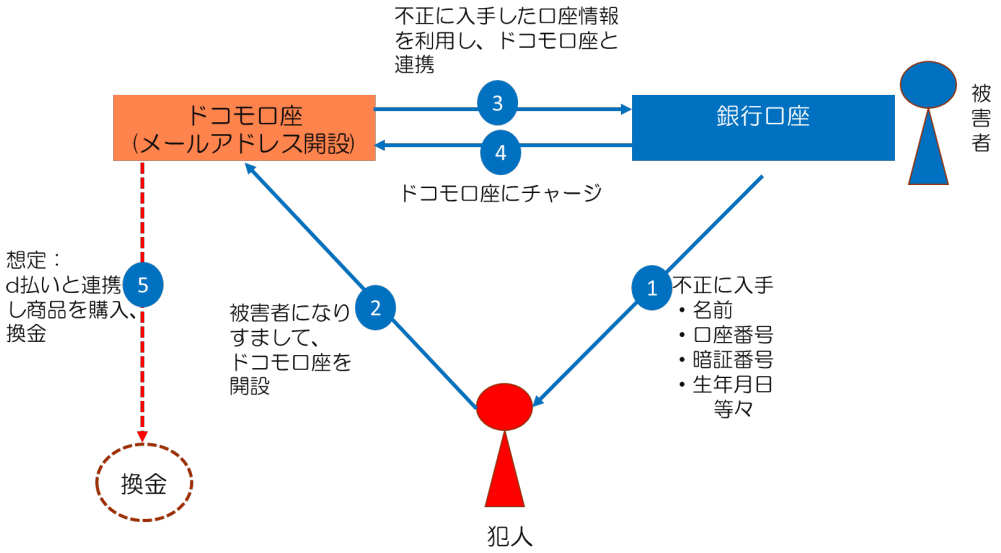


図 3-1　不正利用の流れ

銀行口座からの不正引き出しの窓口として利用された「ドコモ口座」への非難が集中したが、のちに銀行側の不備も認識され業界全体の問題としてとらえられるようになった。問題点を整理すると、二つ挙げられる。第一に決済サービス口座開設時の本人確認が不十分だった点が考えられる。一般的に決済が可能な口座開設時の本人確認は、免許証や住基カードなど写真付き ID の提示や、登録された住所に開設に必要な情報を郵送することで完結すべき手続きである。モバイル番号紐づけのような認証を通さずとも、メールアドレスさえあれば、口座

[9] NTT ドコモ株式会社 2020 年 9 月 10 日報道会見
NTT ドコモグループサステナビリティレポート 2020（サステナブルメッセージ）
https://www.nttdocomo.co.jp/binary/pdf/corporate/csr/about/pdf/csr2020w_000.pdf#page=9

の開設ができてしまったことは犯罪を可能にした大きな要因であった。もう一つは、連携する銀行口座の認証プロセスにあった。口座番号、暗証番号、生年月日など、フィッシングが横行する昨今の情勢を考慮すると、こうした静的な情報のみで行われる認証は、決済を許可する認証としては十分とはいえない。銀行側で送金などの決済をオンラインで受け付ける時と同等以上の強度で認証することが必要である。

今回のような事案が二度と発生しないように、決済サービスの提供者、銀行側ともにも対策とる必要がある。対策ポイントは以下のとおりである。

- 口座情報などの情報を詐取する自社のフィッシングサイト発生をいち早く検知し封鎖活動を行う。また、フィッシングサイトに入力されてしまった被害者口座情報の取得や、ダークウェブも含めたネットの監視を行い漏えいした口座情報を特定し利用を停止する
- 決済サービス口座開設時の本人確認の強化
  郵送不要、専用アプリケーションで写真付き証明書と容貌を撮影して、送信する非対面の本人確認 eKYC が注目されている。
  ただし、証明書の偽装などで犯人を正当化してしまうリスクがあるため、今後は住基システムや免許システムなどへの照合が可能になると、より信ぴょう性の高い本人確認が期待できる。
- 銀行口座連携時の本人確認の強化
  口座番号、暗証番号、生年月日など、フィッシングが横行する昨今の情勢を考量すると、こうした静的な情報のみで行われる認証は不十分であり、銀行側で確信を持てる別経路での追加認証を導入する（携帯電話や銀行アプリケーション、登録住所への郵送によるアクティベーションのためのワンタイムパスワード発行など）

【胡　敏　Appgate】

3.1.2. フィッシングサイト詐欺　個人のクラウドサービスの被害についての可能性

フィッシング詐欺による被害は、主に個人の金銭被害であるケースが多い。しかし在宅ワークも広がりなどの環境の変化により、業務データの漏えいリスクも懸念されるようになって来ている。そこでフィッシング詐欺により業務データが外部に漏えいするリスクはどのくらいあるのだろうか。有り得るリスクのパターンを FTA[10]で分析をした解析例を図 3-2 に示す。

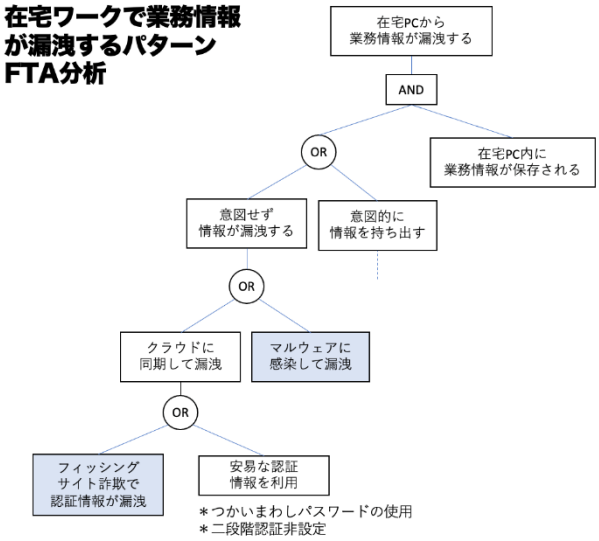


図 3-2　起こりうるリスクパターン

昨今在宅パソコンデータのバックアップにクラウドのストレージサービスを同期させるユーザーは少なくない。その場合、ユーザーが業務データを在宅パソコンに保存させると、そのまま個人のクラウドストレージにアップロードされることとなる。業務データが個人のクラウドサービスに同期されることも問題であるが、フィッシング詐欺サイトなどで、ユーザーのアカウントが悪意のあるハッカーに漏れてしまうと、クラウドに上がった業務データが外部に漏れるリスクがある。

[10] FTA（Fault Tree Analysis＝故障の木解析）とは信頼性工学の手法で不具合が起きる条件を洗い出す手法である。

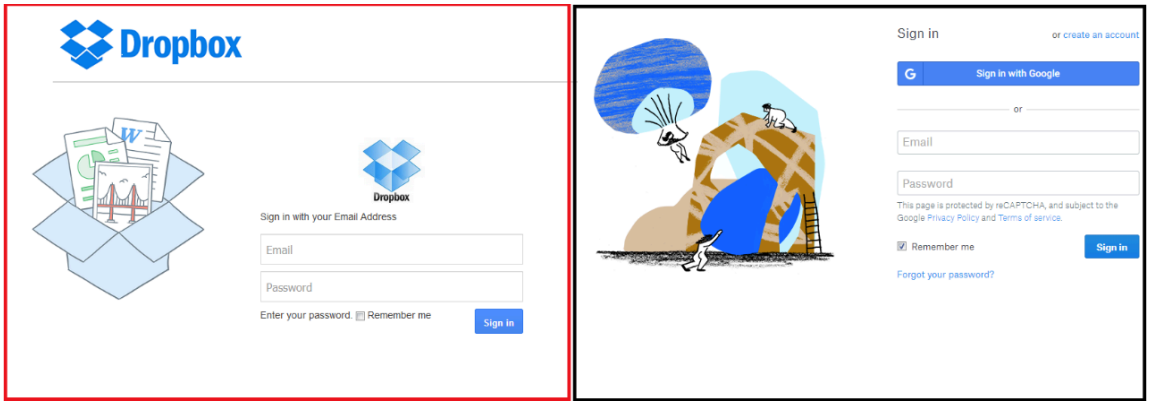


図 3-3　左側がフィッシングページ、右側が本物の Dropbox ログインページ [11]

この情報漏えいを防ぐには、やはり在宅パソコンに業務データを保存させない対策が有効であることが、FTA からわかる。特に、情報漏えいが企業に大きなダメージを与える、顧客の個人情報や取引先の NDA 対象データなどを取り扱う場合は、仮想デスクトップやセキュアブラウザーなどの対策は有効である。

どうしてもそれらのセキュリティ対策の導入が難しい場合は、せめて
- 在宅パソコンのマルウェア対策の徹底
- 業務データのパソコン保存禁止の徹底
- 個人のクラウドサービスの認証ポリシーの強化
- フィッシング詐欺への注意の徹底

という運用ルールの厳格化が情報漏えいのリスクを低減させることがわかる。

システム管理者の目の行き届かない個人のパソコン環境においては、マルウェアの感染対策と同じように、フィッシング詐欺対策への教育が重要である。

【吉田 晋　株式会社コネクトワン】

[11]Fortinet フォーティネットセキュリティブログ「偽の Dropbox に隠されたフィッシングネットワークを掘り起こす」（2018 年 10 月 8 日）https://www.fortinet.com/jp/blog/threat-research/bindweed--digging-down-to-a-root-of-a-hidden-phishing-network

3.2. SMS 関係

3.2.1. 二段階認証を用いるスマホアプリケーション開発における推奨 API、およびブラウザーにおける将来的な対応

企業による SMS 利用のユースケースとしては、スマホアプリケーション・Web サイトにおける二段階認証が典型的であるが、昨年に入り、フィッシング SMS から被害者を偽サイトに誘導し必要な情報を入力させ、それを加害者が正規サイトで利用して不正送金を行う手口が報告されている。

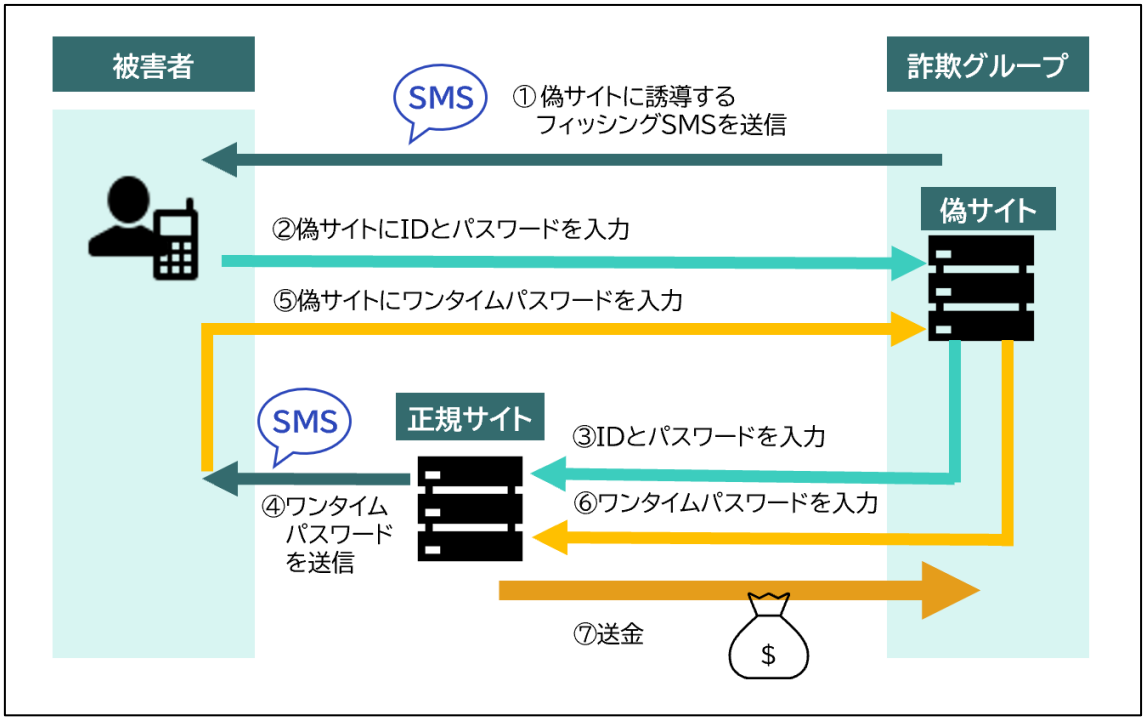


図 3-4　SMS から偽サイトに誘導した不正送金の流れ

このケースの加害者は、SMS で受信したワンタイムパスワードをサイト利用者が正規サイトに「手作業で入力」する点に着目し、偽サイトを用意してその「手作業で入力」させることにより、被害者から必要な情報を入手する。

この問題の背景としては、スマホアプリケーションにおいては過去に Android OS では、ユーザーがパーミッションさえ与えればあらゆるアプリケーションでユーザーが受信したすべての SMS を参照でき、それを悪用してユーザーの個人情報を取得するアプリケーションが数多く市場に出回ったことから、「手作業での入力」を行わせることがスマホアプリケーションの二段階認証ではスタンダートな UX となった時期がある。

一方で Apple/Google としては UX を改善するために、該当の正当なアプリケーションだけが、必要な SMS 内のワンタイムパスワードを参照できる仕組み

を、現時点ではそれぞれ用意している。

特に Google は、過去に悪用された API の利用に厳しい制限を設けた上で、新たな API を用意し、悪用されていた API は申告と Google による承認が必要としているため、悪用していたアプリケーションはすでに Google Play から削除されている。

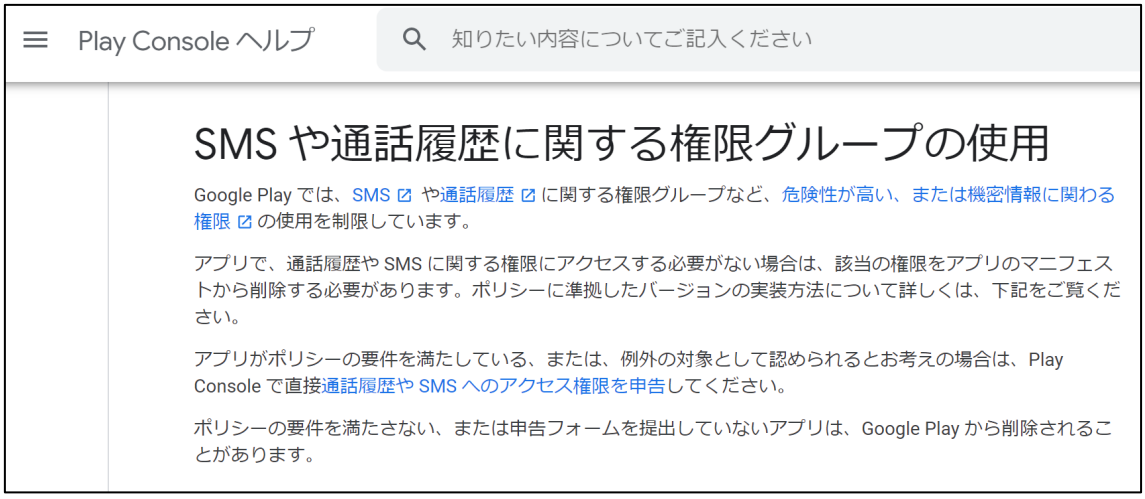


図 3-5　Google による Android アプリケーション開発者向けの説明内容 [12]

Android の場合は、Google が用意した新しい API（SMS Retriever API）による SMS での二段階認証を用いることで、「手作業での入力」を避け、より良い UX を提供することが可能となる。

図 3-6　Google による OTP（ワンタイムパスワード）における新しい API の説明 [13]

iOS の場合は、Apple が Password AutoFill[13]という API を提供しており、下記が実際の利用事例で、ワンタップで 4 桁のパスワードがアプリケーションに自動入力される。

[12] Google 社の Play Console ヘルプ　https://support.google.com/googleplay/android-developer/answer/10208820

[13] Apple 社の開発者向けドキュメント https://developer.apple.com/documentation/security/password_autofill/about_the_password_autofill_workflow

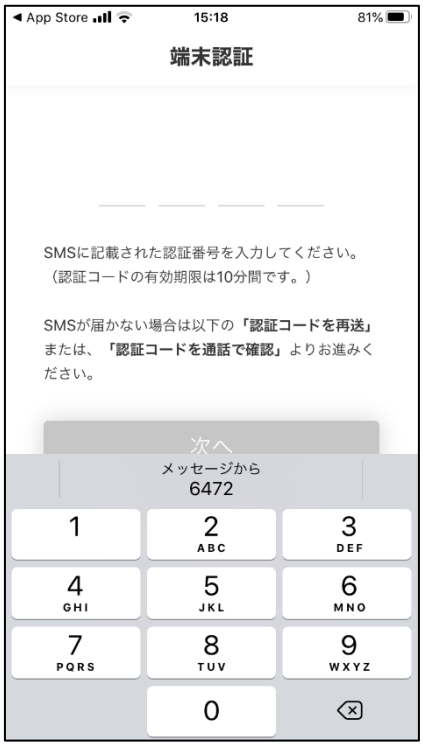


図 3-7　Google による OTP（ワンタイムパスワード）における新しい API の説明

一方、Web サイトにおける同様の機能は、Apple の Webkit エンジニアによる「不正サイトにワンタイムパスワードを手入力した場合に警告を出して入力を防ぐこと」も含めた提案を Google が受け入れたと報じられており [14]、Apple のエンジニアが GitHub 上にて情報を更新 [15]していることから、将来的には Safari、Chrome などのブラウザーにて同様の UX が実現される可能性が高いと考えられる。

【浦田泰裕　株式会社アクリート】

3.2.2. 正規の SMS と同一スレッドに偽装 SMS を紛れ込ませるフィッシングについて

2019 年 6 月に NTT ドコモをかたり、偽サイトへ誘導する不審な SMS が確認され、同社からは注意が呼びかけられた。この事例が特徴的だったのは、不審な SMS の送信元は NTT ドコモの公式 SMS と同じ「NTT DOCOMO」となっており、NTT ドコモ公式の正規 SMS とフィッシング SMS が同じスレッドに表示

[14] engadget 日本版　2020 年 2 月 1 日掲載　https://japanese.engadget.com/jp-2020-02-01-sms-google.html
[15] GitHub における Apple エンジニアの共有内容　https://github.com/wicg/sms-one-time-codes

される事象が発生したことである。受信したスマートフォンの画面上では正規のメッセージに紛れてフィッシングのメッセージが表示されるため、利用者は受け取ったメッセージが不正な SMS であることに気付くのは難しい。

この事象が発生する要因は、攻撃者が送信元を公式 SMS と同じ文字列に偽装していることである。SMS は送信元に Sender ID と呼ばれる文字列を指定することができる。端末側の SMS アプリケーションでは受信した SMS の送信元（Sender ID、以下「送信元」とする）が同じ場合、同じスレッド内で表示されるケースが多い。（図 3-8）

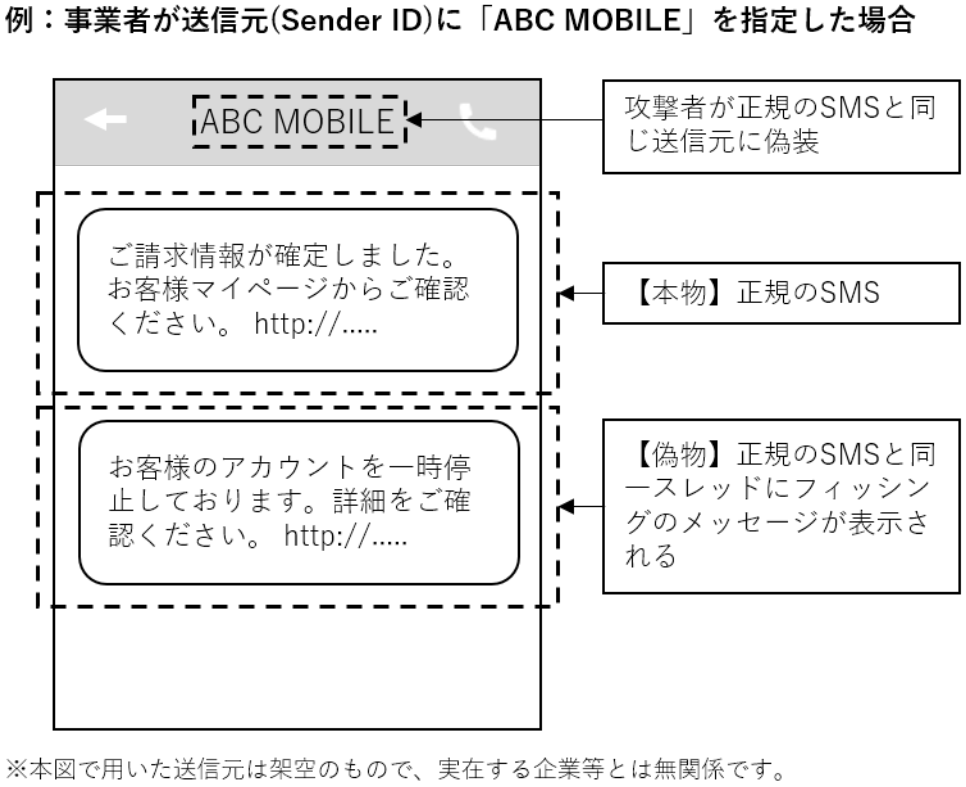


図 3-8　正規の SMS と同一スレッドに紛れ込む偽装 SMS

問題は送信者の判別に送信元を使用しているにもかかわらず、自社が使用している送信元を第三者が特に制約なく自由に使用可能であることだ。国際網を経由した SMS 配信サービスの多くでは送信元に任意のアルファベットを指定することができる。利用審査や契約手続きも厳格に実施しない事業者が存在し、そのような事業者が提供するサービスがフィッシングに利用されやすい。

この問題に対する事業者側の対策は、正規の SMS の送信元にアルファベット文字列は使用せず、自社が保有する電話番号を使用することが有効である。国内

直接接続の SMS 配信サービスを利用することで、国内の電話番号を指定することができる（国際網を経由した SMS 配信サービスでは国内の電話番号を指定することができない）。さらに、利用審査や契約手続きなどがあるため、攻撃者による匿名での利用や送信元を偽装しての利用は困難であり、第三者に自社の電話番号が使用されることを防ぐことが可能だ。

上述のとおり正規 SMS の送信元にアルファベット文字列は使用せず、国内電話番号を指定するのが望ましいが、現状はアルファベットを使用している日本企業が存在する。金融機関でアルファベットが使用されるケースはほぼないが、知名度の高い大手企業で使用されるケースはあるため、今後は、金融機関以外の企業においても、この問題について広く周知がなされて、対策がとられることが望まれる。

【福地 雅之　NTT コム オンライン・マーケティング・ソリューション株式会社】

4. フィッシングの対策について

4.1. 最新の動向

4.1.1. フィッシングと FIDO と最新動向

近年では、パスワード認証の要件や管理の煩雑化が課題として挙げられるようになり、認証にパスワードを使用しないパスワードレスの技術が注目されている。中でも FIDO(Fast IDentity Online)と呼ばれるオンライン認証の仕様が多くのシステムで使用されている。FIDO を使用するとスマートフォンなどの生体認証を使用して個人認証を行うことができる。FIDO を使用することにより、パスワードリスト攻撃やフィッシング詐欺の対策を行うことが可能になる。

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

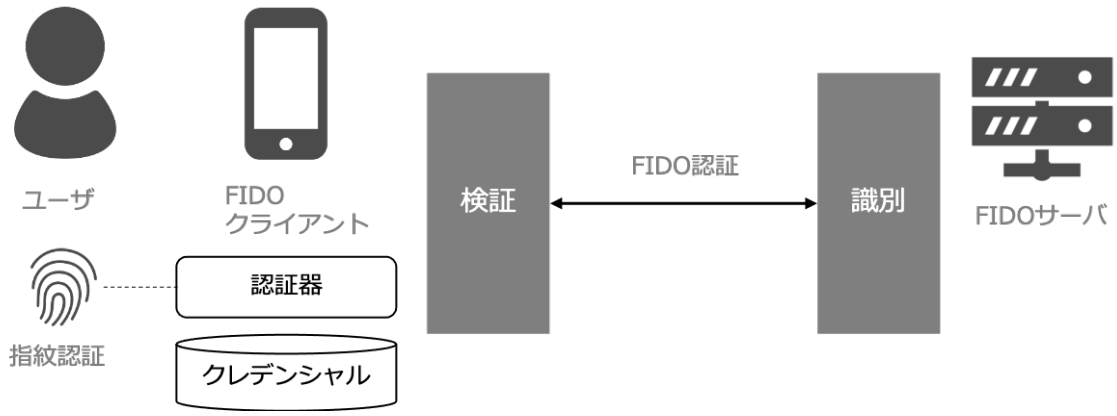


図 4-1　FIDO の認証モデル

従来の FIDO 認証では仕様に準拠したハードウェアトークンなどの認証器や、スマートフォン OS のアプリケーションなどを使用することが必要だったが、FIDO2 として新たに策定された仕様では、WebAuthn (Web Authentication API)をサポートしたブラウザーを使用することで FIDO 認証を行うことができるようになった。FIDO2 は Microsoft Edge、Google Chrome、Firefox など多くのブラウザーでサポートされていたが、iOS14 からはセキュリティトークンだけではなく、Touch ID、Face ID による FIDO2 認証がサポートされ(図 4-2)、今後多くのサイトでの使用が期待されている。

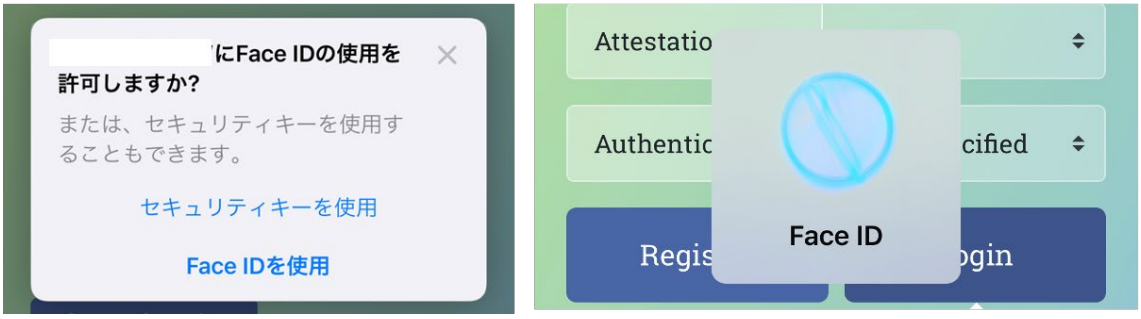


図 4-2　iOS の Face ID での FIDO 認証例

【松本悦宜　Capy 株式会社】

4.1.2. よりアグレッシブなフィッシング対策

事業者におけるフィッシング対策として、いち早くフィシングサイトの立ち上がりを検知し閉鎖依頼を行ったとしても、

- 自身が被害にあったことに気付いていない、潜在的な被害者までは捕捉できない
- フィッシングサイトが閉鎖されるまで、完全に被害は止められない

という課題が現状存在する。

フィッシングの犯行手口も以前より進化している昨今、受け身になるのではなく、

- フィッシングサイトに誘導されてしまった方に対しピンポイントに対応実施
- 出し子より上位の、主犯格の逮捕に繋がる情報を収集する

といった、防御する側としても技術/ノウハウを用いてアグレッシブなフィッシング対策を行っていくべきであると考える。

実現のための有効な手段として、多くの情報をログに残すということが第一に挙げられる。

例えば、自社サイトを構成する

- favicon.ico
- ロゴ、バナーなどの画像ファイル
- Javascript、CSS ファイルなどのスクリプト

などの資産に対するリファラーを取得、監視しておくだけでも以下のような検知/解析が可能となる。

◆ フィシングサイトの立ち上がり検知

フィッシングサイトを正規サイトに似せた構成とする目的で、バナーなど、フィッシングサイト上から直に参照されている場合があるため、自社のサイトを構成する上記の資産に対して異なるドメインからの参照が行われていないかを監視することで、フィッシングサイトの立ち上がりを早期発見することが可能となる。

◆ フィッシングサイトに誘導されてしまった方の特定

フィッシングサイト上からの画像などへのアクセス情報に含まれる、アクセス元 IP アドレス、UserAgent（OS/ブラウザーの組み合わせ情報）、設定言語などの情報を利用し、「この環境はどのアカウントが普段使いしているものか」

という観点で情報を紐付けておくことで、フィッシングサイトに誘導されてしまった方の特定が可能となる。また、特定したアカウントに対し、一時的にさらなる追加の認証をかけるなどセキュリティレベルを上げることで、被害を抑制することも可能となる。

◆　フィッシングサイトを立ち上げた犯人の情報を収集

フィッシングサイト立ち上がり直後の、上記に挙げたアクセス元 IP アドレスなどのログリファラー情報を解析することにより、犯人がどのような環境からフィッシングサイトを立ち上げているのかの追跡が可能となる。

フィッシングサイト立ち上げ後、犯人が動作確認のためフィッシングサイトに自らアクセスした後、詐取した ID/パスワード情報を使って同一環境より不正ログインを行っている形跡も、監視により捕捉できたケースも存在する。

また、自社サイトを構成する資産へのアクセス情報とは別に、ログ情報として cookie （1st party cookie）、言語設定、タイムゾーン設定、画面解像度、キーボード配列といった環境情報ログも可能な限り取得すべきである。多くの情報を取得/活用することで、検知ルール設定により一般顧客に影響がない形で犯行を抑止し、仮に被害が起こってしまった場合でもデータ解析により次の対策に活かすことができる。

金融機関においては、ほぼ毎日といっていいほど各社のフィッシングサイトが入れ替わりで立ち上がっている。犯行情報ならびに抑止成功事例など、先人にて対応してきた技術/ノウハウを業界を跨いで他事業者と密に情報共有するべきであり、それが日本全体でのフィッシング対策レベルの底上げに繋がるものと考える。

【小川秀夫　株式会社カウリス】

4.2. ドメイン関連

4.2.1. ドメイン名を狙ったインシデント

2020 年は日本企業のドメイン名登録情報（whois）が不正アクセスによって書き換えられるインシデントが発生した。その代表的な手法の一つが「ドメインハイジャック」である。この手順は被害企業のドメイン名の管理者 ID（アカウント）がドメイン名登録事業者のサイト経由で不正アクセスされ、ドメイン名登録情報のネームサーバーや登録用メールアドレスなどが第三者により不正な書き換えが行われた。結果として、被害企業の Web サーバーやメールサーバーへアクセスができなくなり、多大な影響を与えることとなった。

この「ドメインハイジャック」の予防策として最初に挙げられるのがドメイン名登録事業者のサイトアクセスに対して制限をかけることである。具体的には複数要素認証を有効にすることや、IP アドレス制限をかけることが考えられる。次に挙げる予防策はドメイン名登録情報の変更に制限をかけることである。この機能はドメイン名登録事業者によって提供されていることがあり、その機能を有効にすることができれば、より強い予防策となる。

例）jp ドメインの場合
レジストリロックサービス
https://jprs.jp/about/dom-rule/registry-lock/
指定事業者変更ロック
https://jprs.jp/about/dom-rule/transfer-lock /

上述の予防策はドメイン名登録事業者における対策だが、サービス利用者が自衛的に実施可能な対策もある。挙げられるのが「ネームサーバーのモニタリング」と「whois 情報のモニタリング」である。Web サーバーやメールサーバーのモニタリングを実施しているサービス利用者は多いが、ドメイン名のモニタリングを実施することは少ない。上述のインシデントはまさにチェックの甘いドメイン名とネームサーバーが狙われ、結果として検知に時間を要することになった。これらのモニタリングはインシデント発生時のアラートを機械的に検知する仕組みを実装することが理想である。実装が難しい場合には定期的な人為的チェックが推奨される。これらのモニタリングはインシデントの早期検知のためにも必要である。

【加藤 恭久　GMO ブライツコンサルティング株式会社】

4.2.2. ドメイン名の廃止にあたっての注意 [16]

◆　ドメイン名廃止のリスク

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

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

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

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

さらに、そのドメイン名をメールアドレスとして使っていた場合、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されているドメイン名を廃止してしまうと、メール経由でパスワードを再設定されてアカウントを乗っ取られたり、機密情報を盗み見られたりする可能性もある。

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

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

[16] 本内容は JPRS の Web ページの内容をもとに作成しています。詳細は以下のページをご覧ください。
ドメイン名の廃止に関する注意, https://jprs.jp/registration/suspended/

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

◆　属性型 JP ドメイン名における 1 組織 1 ドメイン名の制限緩和

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

しかし、「組織名変更」「合併」「事業譲渡」の場合には、複数の属性型 JP ドメイン名を登録することができる、制限緩和が利用可能である [17]。この制度を利用することで、これまで利用していたドメイン名の登録を維持しながら、新しいドメイン名を登録・利用できるようになる。ドメイン名の廃止には前述のようなリスクがあるため、この制度の積極的な利用検討を勧めたい。利用にあたっては所定の手続きが必要になるため、詳細は使用中の JP ドメイン名の指定事業者に相談して欲しい。

◆　誤ってドメイン名を廃止してしまった場合への対処

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

【佐々木俊博　株式会社日本レジストリサービス】

[17] 「属性型（組織種別型）・地域型 JP ドメイン名登録等に関する規則」の改訂について, https://jprs.jp/whatsnew/notice/2014/20140217-rule.html

■ コラム **BIMI** について

BIMI（Brand Indicators for Message Identification - メッセージの識別のためのブランド・インジケーター）は、送信者のドメイン名に関連付けられたロゴの画像イメージをさまざまなメールソフトで表示するための技術的な仕組みです。

この仕組みは 2018 年頃から BIMI グループ[18]において策定されているもので、Google、Yahoo!、Aol.においてパイロット版としてのサポートが発表されています[19]。2020 年 8 月には Gmail においてもパイロット版としてのサポートが発表されました[20]。

BIMI は、DKIM と SPF を使い、かつ DMARC の quarantine または reject ポリシーで認証が通るように設定されているドメイン名において利用できます。

技術的な動作例を説明します[21][22]。

1. (準備段階) メールの送信側において、BIMI のためのドメイン名（例：selector._bimi.example.com）の TXT レコードに、表示したいロゴの画像データの URL や VMC（Verified Mark Certificate – ロゴの画像データが入っている電子証明書）の URL を記載しておきます。
2. メールの送信側は、送信するメールに BIMI のためのヘッダー（例：BIMI-Selector: v=BIMI1; s=selector;）を入れて送信します。
3. 受信したメールサーバー（MTA）は DKIM-Signature の対象範囲に BIMI のためのヘッダーがあった場合、「selector._bimi.example.com」といったドメイン名の TXT レコードを DNS で問い合わせ、画像データを取得します。
4. 取得した画像データを BASE64 エンコードし、メールのヘッダーに

[18] BIMI Group, https://bimigroup.org/
[19] BIMI Adoption – October 2020, https://bimigroup.org/bimi-adoption-october-2020/
[20] 安全第一: G Suite に新たに 11 のセキュリティ機能を導入, https://cloud.google.com/blog/ja/products/g-suite/gsuite-security-updates-for-gmail-meet-chat-and-admin
[21] Implementation Guide | BIMI Group, https://bimigroup.org/implementation-guide/
[22] Brand Indicators for Message Identification (BIMI), https://tools.ietf.org/html/draft-blank-ietf-bimi-01

加えます（例：BIMI-Indicator: PD94bW...8L3N2Zz4K）。

5. メールを受信したメールソフトはヘッダーの画像データをデコードして表示します。

したがって、ロゴを表示するためにはメールを受信するサーバーとメールソフトが対応している必要があります。

国際的な標準化団体である IETF では、この BIMI の技術的な仕組みについて 2019 年 3 月に行われた会合（BoF）で議論されました。論点をピックアップして紹介します。

第 104 回 IETF（2019 年 3 月）の BoF での論点 [23]

- 普及の観点では BIMI をサポートしている少数の送信者と少数の受信者によってのみ利用できる状態ができる。そのため、ロゴが見えるかどうかが人によって違ってしまう。根本的な課題解決の仕組みになっているか。
- ロゴが表示されていない場合にユーザーに記述されている URL をクリックしないようにするところまで考慮されているか。
- 仕組みが複雑すぎる。

電子メールには、MUA（メールユーザーエージェント）で処理される S/MIME と、MTA（メール転送エージェント）で処理される SPF や DKIM というセキュリティ技術があります。BIMI は MTA における処理に加えて、MUA においてロゴを表示するという処理の組み合わせの技術です。したがって、Gmail のように MTA と MUA の違いをユーザーが意識しないような仕組みにおいては BIMI の導入を行いやすいかも知れません。これまで Web においては、フィッシングサイトで紛らわしいドメイン名が使われてしまったり、サーバー証明書に関する表示が Web ブラウザーによって異なってしまったりする、といったことが起きてきました。Web ページや電子メールのような情報の提供者が、ドメイン名やロゴデータの正しさを示す（assertion）技術を採用する際には、エンドユーザーがその技術を頼りに不正を見抜けるかどうかと、いうところまでデザインしていく必要があ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】

[23] Brand Indicators for Message Identification IETF104, March, 2019, https://datatracker.ietf.org/meeting/104/materials/slides-104-bimi-bimi-01

5. まとめ

フィッシング詐欺における 2020 年のフィッシング対策協議会への報告件数を見てみると、2019 年 12 月には 8,208 件だったものが 1 年後の 2020 年 12 月には 32,171 件と月間報告数が約 4 倍となっており、1 年間で月間約 24,000 件増加したことになる。昨年のレポートで「急増」と評し、月間報告件数が約 6,300 件増加して 4.4 倍となった 2019 年を大幅に上回る増加となった。

フィッシングに悪用されたブランド数においても引き続き増加の一途をたどっており、全体としてフィッシング詐欺の横行に十分な歯止めがかかっていないと考えられる。

現在、被害を受けていない。あるいは被害が止んでいる事業者や業界においても、いずれまた狙われる可能性があることを想定し、現在、被害を受けている、受けていないにかかわらず、インターネットで何らかのログインサービスを行う事業者は、引き続き高い危機意識をもって、さらなる対応策やその導入について改めて検討いただきたい。すでに従来より一段上の対策の検討が必要な情勢であり、現時点で最も有効と考えられるパスワードレス認証の FIDO2 の導入についても是非検討に加えたい。

本協議会では、現状のトレンドを反転させるべく、フィッシングに対抗する各事業者様に対して、最新情報の収集・分析・情報提供やフィッシング URL 配信事業含め、引き続きさまざまな観点での支援を推進していくこととしたい。

【早川 和実　NTT コミュニケーションズ株式会社】

（空白）

フィッシング対策協議会　技術・制度検討ワーキンググループ
構成員名簿

（敬称略・順不同）

【主査】
野々下 幸治　トレンドマイクロ株式会社

【構成員】

田中 優成	株式会社アクリート
浦田 泰裕	株式会社アクリート
胡 敏	アップゲート
長谷部 一泰	アルプス システム インテグレーション株式会社
早川 和実	NTT コミュニケーションズ株式会社
福地 雅之	NTT コムオンライン・マーケティング・ソリューション株式会社
黒田 和宏	NTT コムオンライン・マーケティング・ソリューション株式会社
小川 秀夫	株式会社カウリス
島津 敦好	株式会社カウリス
松本 悦宜	Capy 株式会社
吉田 晋	株式会社コネクトワン
加藤 恭久	GMO ブライツコンサルティング株式会社
阿部 章裕	デル・テクノロジーズ　RSA
加藤 孝浩	トッパン・フォームズ株式会社
遠藤 淳	株式会社日本レジストリサービス
佐々木 俊博	株式会社日本レジストリサービス
木村 泰司	一般社団法人日本ネットワークインフォメーションセンター
中村 健太	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情報セキュリティ課
【事務局】
一般社団法人 JPCERT コーディネーションセンター
エム・アール・アイリサーチアソシエイツ株式会社（株式会社三菱総合研究所）