フィッシングレポート 2020

2020 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

目次

1. フィッシング対策ガイドライン　重要５項目 1
   1.1. 今年度の WG 活動について 1
   1.2. フィッシング対策ガイドライン 2020 年版　重要 5 項目 2
2. フィッシングの動向 7
   2.1. 国内外の状況 7
   2.2. 海外の状況 10
   2.3. フィッシングこの一年 12
      2.3.1. 犯罪者が狙うターゲットの変化 12
      2.3.2. スミッシングの増加 13
3. フィッシングの被害について 17
   3.1. フィッシング詐欺の被害状況 17
   3.2. 金融機関（銀行）をかたるフィッシングが急増 19
   3.3. SMS を使ったフィッシング 20
   3.4. フィッシングサイトの URL の傾向 23
4. フィッシングの対策について 26
   4.1. 個人認証の状況と背景 26
   4.2. 認証技術関連 28
      4.2.1. リスクベース認証 28
      4.2.2. FIDO を使用した生体認証 31
   4.3. SMS を使ったフィッシングへの対策 32
5. まとめ 37

1. フィッシング対策ガイドライン　重要５項目

フィッシング対策協議会の技術・制度検討ワーキンググループでは、本レポートのほか、事業者向けの「フィッシング対策ガイドライン」および「利用者向けフィッシング詐欺対策ガイドライン」を Web にて公開しており、毎年内容を見直し、必要な改定を行っている。

今般、最近のフィッシングの傾向等をふまえ、ガイドラインの対策要件の中でも、ユーザがフィッシング被害に遭うリスクを減らすために事業者が特に重点的に取り組むべきものを５ つにまとめ、本レポートに掲載することとした。

1.1. 今年度の WG 活動について

技術・制度検討ワーキンググループの 2019 年度の活動において、「フィッシング対策ガイドライン」の 2020 年版への改定にあたり、事業者における対策の内容をかなり改定する方向で議論を進めた。その理由として以下の二つがあった。

- 改定の度に追加項目が増えることにより、本当に重要な対策が分かりにくくなってきた。

- インターネットの利用者の使う機器の主流がパソコンからスマートフォンに移るとともに、利用者の高度な IT リテラシーに頼る対策は、難しくなってきた。

その結果として、ガイドラインの項目の集約や削減により項目数をガイドライン作成以来、初めて削減した。また、新たに「重要 5 項目」というのを作成した。

この「重要 5 項目」は、ID/パスワードを利用者から預かるサービス事業者として、フィッシング被害を防ぐための最低限必要な対策として取り上げた。

現状では、この 5 項目すべての対策を提供しているサービス事業者は、かなりの少数だと思われる。

まずは、ID/パスワードを利用者から預かるサービス事業者のすべてがこの 5 項目の対策に早期に対応することを期待したい。

1.2. フィッシング対策ガイドライン 2020 年版　重要 5 項目

- 利用者に送信するメールには「なりすましメール対策」を施すこと
- 複数要素認証を要求すること
- ドメインは自己ブランドと認識して管理し、利用者に周知すること
- すべてのページにサーバ証明書を導入すること
- フィッシング詐欺対応に必要な組織編制とすること

以下に、各 5 項目を解説する。

利用者に送信するメールには「なりすましメール対策」を施すこと

外部送信用メールサーバを SPF（Sender Policy Framework）と DKIM（Domain Keys Identified Mail）の送信ドメイン認証と電子署名による S/MIME を導入し、送信元アドレスの偽称検知と送り主の身元証明、配信途中の改ざん検知を可能とすることが必要である。さらに DMARC（Domain-based Message Authentication, Reporting & Conformance）を活用し、受信制御ポリシにて受信を拒否する「reject」を設定し、フィッシングメールを利用者に届けない制御を施すことが望ましい。

また、メールに使用していないドメインに DNS の MX レコードと DMARC レコードを記述し、DMARC の受信制御ポリシを reject にすることはスパムやフィッシングメールの未然防止につながる。

「フィッシング対策ガイドライン 2020 年度版」の参照箇所

利用者が正規メールとフィッシングメールを判別可能とする対策については、以下を参照。

【要件 1】 ◎：利用者に送信するメールには電子署名を付与すること

【要件 2】 ◎：外部送信用メールサーバを送信ドメイン認証に対応させること

また、SMS を利用する場合については、以下を参照。

“2.2. SMS（Short Message Service）を利用したフィッシング詐欺”

複数要素認証を要求すること

フィッシャーが不正に知りえたログインアカウント情報でログインできないようにするためには、ログイン認証時に乱数表やワンタイムパスワード、生体認証などの複数要素認証を求めるようにすることが必要である。

特に資産の移動機能（他金融機関への振込み、商品の購入など）を提供

している場合には、資産の移動操作実行時にも再認証や複数要素認証を求めるようにすることが望ましい。複数要素認証の一手法としてワンタイムパスワードを発行する場合には、第一の認証とは異なる経路（例：第一の認証を ID・パスワードで求めたとすれば、ワンタイムパスワードをユーザのメールアドレスに送るなど）を利用することが望ましい。また、利用者が法人の場合、申請者とは異なる承認権限者による承認を求めるなどの対策も考えられる。

「フィッシング対策ガイドライン 2020 年度版」の参照箇所

フィッシング詐欺被害を拡大させないための対策については、以下を参照。
【要件 12】 ◎：複数要素認証を要求すること

ドメインは自己ブランドと認識して管理し、利用者に周知すること

利用するドメイン名は、自社のブランドとして大切に管理することが必要である。また、正しいドメイン名について繰り返して利用者に示す必要がある。

企業においてドメイン名の登録・利用を行う場合、ドメイン名の管理を担当する部門・要員、および管理のためのルール・手順を社内で確立しておくことが必要である。組織内の複数の部門からそれぞれの利用目的のために勝手に複数のドメイン名管理サービスが利用されるような状況であると、その全容把握ができず、セキュリティ配慮に欠けた運用がなされたり、管理が放置されたりする。

「フィッシング対策ガイドライン 2020 年度版」の参照箇所

ドメイン名に関する情報については、以下を参照。
【要件 21】 ◎：使用するドメイン名と用途の情報を利用者に周知すること
【要件 22】 ◎：ドメイン名の登録、登録、利用、廃止にあたっては、ドメイン名を自己のブランドとして認識して管理すること

すべてのページにサーバ証明書を導入すること

すべての Web ページで HTTPS でのアクセスを提供することが必要である。サーバ証明書を使った HTTPS による暗号通信では、機密性保護に加え、アクセスしている Web サーバの正当性（ドメイン名を含めたサーバ名と運営者との関係について認証局が確認を取っているというこ

と）を確認できる。ブラウザによっては、HTTPS を使っていないと安全でないという警告が出される。検索エンジンでは HTTPS のページが優先されており、検索によるフィッシングサイトへの誘導を防ぐうえでも効果的である。

なお、Web サイトで用いるサーバ証明書の種類については、DV（Domain Validation）、OV（Organization Validation）、EV（Extended Validation）があり、特に、EV は証明書発行機関により Web サイト運営者の実在確認を厳格に実施したうえで発行されるため、組織としては高い信頼性を得ることができる。

「フィッシング対策ガイドライン 2020 年度版」の参照箇所

正規サイトを判別するためのサーバ証明書に関する情報については、以下を参照。

【要件 7】 ◎：すべてのページにサーバ証明書を導入すること

フィッシング詐欺対応に必要な組織編制とすること

フィッシング発生時には、さまざまな事項を同時並行的にすみやかに処置していくことが必要になるので、組織に応じた事前準備、役割分担、連絡・レポート体制を明確化しておくことが必要である。また、運営しているサイトの不正操作や不正取引の被害により利用者に多大な被害が及ぶサービス、キャッシュカード、クレジットカード、デビットカードの発行を行っているサービスの場合は紛失や盗難などの事故の被害を報告できる 24 時間受付窓口を設置する必要がある。

「フィッシング対策ガイドライン 2020 年度版」の参照箇所

組織的な対応体制の整備については、以下を参照。

【要件 23】 ◎：フィッシング詐欺対応に必要な機能を備えた組織編制とすること

【要件 24】 ◎：フィッシング詐欺に関する報告窓口を設けること

コラム【ドメイン名の廃止にあたっての注意】[1]

◆ 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つながるリスクもある。

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したり、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。

◆ 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

[1] ※本コラムの内容は以下の Web サイトの内容をもとに作成しています。 詳細な情報へのリンクなどは Web サイトをご覧ください。
ドメイン名の廃止に関する注意 https://jprs.jp/registration/suspended/

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[2]。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ほしい。

◆ 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ほしい。

【宇井 隆晴　株式会社日本レジストリサービス】

[2] 「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

2. フィッシングの動向

2.1. 国内外の状況

フィッシング情報の届け出件数について、2019 年は 2018 年と比較して大きく増加した。

警察庁の発表[3]によると、2019 年上半期では、サイバー空間における探索行為などに基づくアクセス件数が増加している傾向にあり、IoT 機器等の脆弱性を狙ったアクセスなどが認められている。また、不正アクセス禁止法違反の検挙件数は 182 件であった。このうち 159 件が識別符号盗用型（アクセス制御されているサーバに、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、2017 年には 425 件（約 10 億 8,100 万円）だったのに対し、2018 年は 322 件（約 4 億 6,100 万円）と件数、被害額とも減少した。2019 年上半期も発生件数 182 件、被害額約 1 億 6,500 万円で、2018 年上半期と比較して減少した。

しかし、2019 年 9 月以降はインターネットバンキングに係る不正送金事犯による被害が急増しており、11 月には発生件数が 573 件、被害額は約 7 億 7,600 万円にのぼったことが報告されている[4]。

フィッシング対策協議会の統計では、2019 年のフィッシング届け出件数が毎月増加し、年間を通して非常に高位な水準で推移した（図 2-1）。金融機関をかたるフィッシングのほか、無料の DDNS (ダイナミック DNS) サービスを使い、短時間で URL を変えるものが確認されたことが報告されている。

図 2-1　フィッシング情報の届け出件数

[3] 警察庁、 令和元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/R01_kami_cyber_jousei.pdf
[4] 警察庁サイバー犯罪対策プロジェクト、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（全銀協等と連携した注意喚起）
http://www.npa.go.jp/cyber/policy/caution1910.html

フィッシングサイトの URL 件数（重複無し）は、2019 年上半期、下半期ともに増加した（図 2-2）。ブランド名を悪用された企業の件数も、2018 年と比較しても増加の傾向にある（図 2-3）。

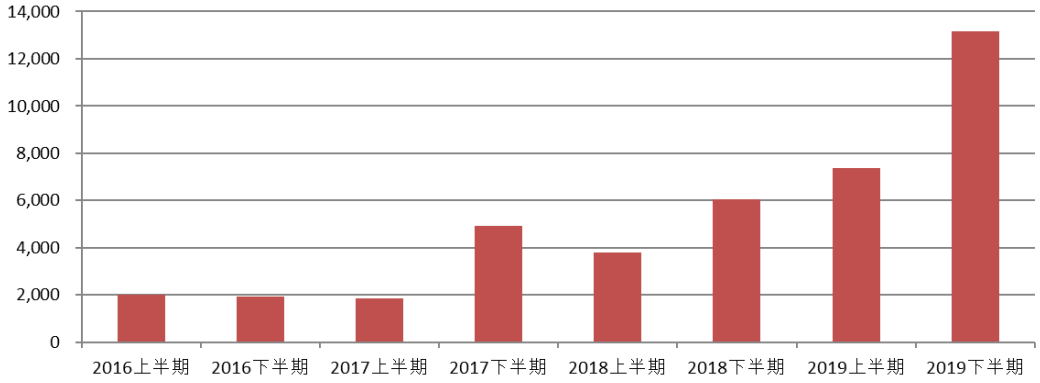

図 2-2　フィッシングサイトの件数

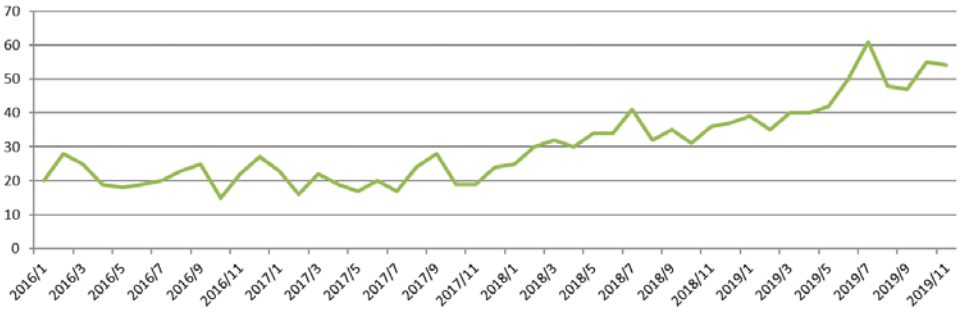

図 2-3　ブランド名を悪用された企業の件数

また、国家公安委員会・総務省・経済産業省の発表によれば、2019 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 2018 年に比べて増加した（図 2-4）。手口を見ると、2019 年におけるフィッシングは 1 件であり、前年と同様に比率は全体の 1%に満たない一方、他人から入手したものの割合が大きく増加した（図 2-5）。

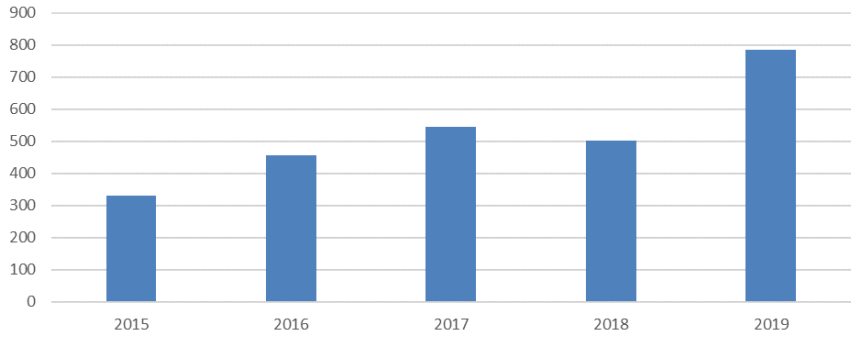

図 2-4　識別符号窃用（ID 窃盗）型不正アクセス行為の検挙件数 [5]

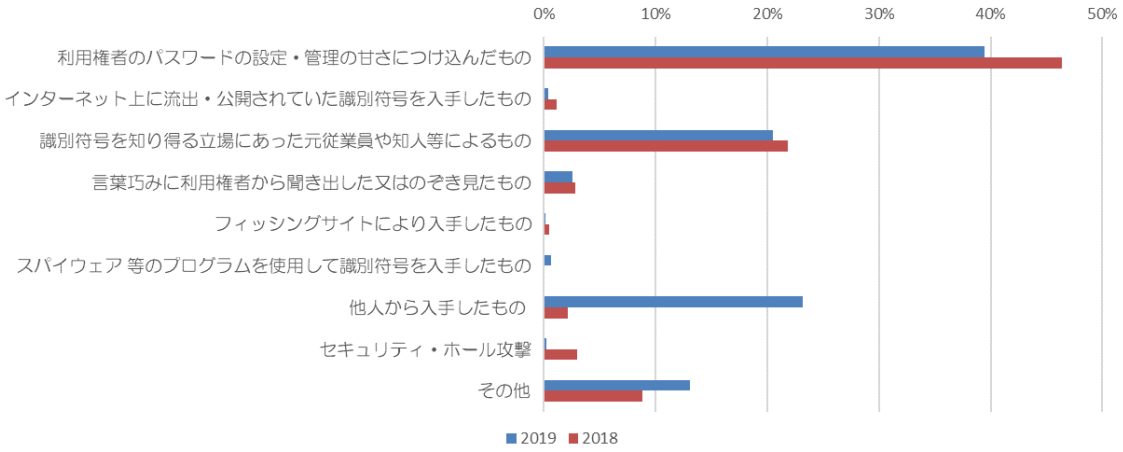

図 2-5　不正アクセス行為に係る犯行の手口の内訳（2018 年、2019 年）[6]

[5] 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/000671872.pdf よりフィッシング対策協議会が作成

[6] 同上

2.2. 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 2-6）。フィッシングサイトの件数は、2018 年下期に大幅に減少したものの、2019 年上半期では増加した（図 2-7）。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 2-8）。APWG の報告書によると、Web メールや SaaS（Software-as-a-Service）のユーザを対象としたフィッシングが多いことや、フィッシングサイトの 4 分の 3 が SSL を使用していることが報告されている。フィッシングサイトの SSL 利用は 2015 年の調査開始以降最も高い割合となっていることが示されている。

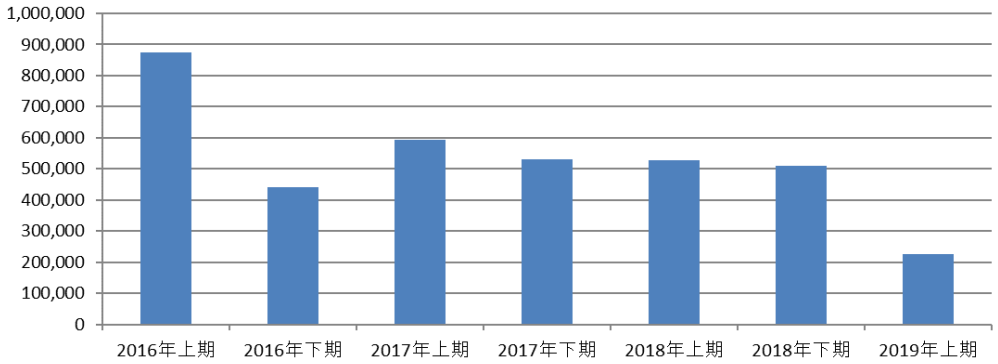

図 2-6　APWG へのフィッシングメール届け出件数 [7]

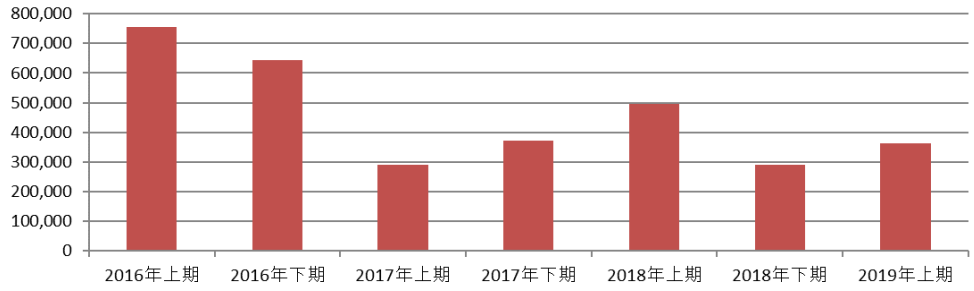

図 2-7　フィッシングサイトの件数（APWG）[8]

[7] APWG（Anti-Phishing Working Group)、"Phishing Activity Trends Report"、https://www.antiphishing.org/resources/apwg-reports/、よりフィッシング対策協議会にて作成
[8] APWG (Anti-Phishing Working Group)、 "Phishing Activity Trends Report"、https://www.antiphishing.org/resources/apwg-reports/、よりフィッシング対策協議会にて作成

図 2-8　フィッシングによりブランド名を悪用された企業の件数（APWG）[9]

［エム・アール・アイリサーチアソシエイツ株式会社］

[9] APWG (Anti-Phishing Working Group)、"Phishing Activity Trends Report"、https://www.antiphishing.org/resources/apwg-reports/、よりフィッシング対策協議会にて作成

2.3. 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 2019 年 1 月から 12 月までのフィッシング報告件数は 55,787 件で、2018 年と比較して約 2.8 倍となった。

2.3.1. 犯罪者が狙うターゲットの変化

2019 年に受領した報告の中で最も多くの割合を占めたのはクレジットカード情報の詐取を目的としたフィッシングである。その一方で、2019 年は国内の銀行かたり不正送金を狙うもの、携帯電話の契約に自動付帯している「キャリア決済」の不正利用を狙うものなど、多様なフィッシング報告も多く受け、より広範な金融・決済サービスがターゲットになっている状況を確認した。

クレジットカード情報の詐取を目的としたフィッシングについては、最も報告件数が多く、この傾向は例年と変わらない。大手のクレジットカード会社はもちろんのこと、クラウドコンピューティングサービスやネットショップ・EC サイトをかたり、クレジットカード情報の詐取を試みるフィッシングサイトを多く確認した。一般社団法人日本クレジット協会の発表によると、2019 年 1 月から 9 月までのクレジットカードの番号盗用による被害額は 167 億円を超え、2018 年の同時期に比べて約 35.1 億円増加していることから、犯罪者にとって現在もっとも狙いやすい対象であることは疑いない。

国内の銀行をかたるフィッシングについては、5 月頃より報告が増え始めた。このフィッシングは、ワンタイムパスワード導入等の銀行側の対策により 2014 年以降、報告数は減少していたが、2019 年 8 月頃にワンタイムパスワードを詐取して即時に不正送金を行う手法による金銭的被害が顕在化した。11 月には 1 ヵ月で約 7.7 億円の被害（警察庁発表）が出たことから、多くのメディアが驚きをもって取り上げた。

キャッシュレス決済のひとつである、「キャリア決済」の不正利用を目的としたフィッシングについては、通信キャリア（携帯電話会社）装うもので、多くはメールではなく SMS（ショート・メッセージ・サービス）からフィッシングサイト等に誘導されるものであった。

2.3.2. スミッシングの増加

2019 年は、フィッシングサイトへの誘導に SMS を使う「スミッシング」の報告が増え、スマートフォン利用者が明確なターゲットとなっている状況が鮮明になった。

国内の銀行、通信キャリア、宅配便の不在通知などをかたったスミッシングが確認されたが、これらの不正な SMS は海外の SMS 事業者や電話番号から送信されたものも多くあった。

前項に記載したとおり、国内の銀行をかたるフィッシングは 5 月頃より報告が増え始めた。この時点ではメールからのフィッシングサイト誘導がほとんどであったが、年末ごろに、メールのみならず海外から送信された不正な SMS からのフィッシングサイト誘導が確認された。

通信キャリアをかたる不正な SMS も同じく海外から送られていたものを確認した。SMS の仕様により、受信者側のスマートフォンでは実在する通信キャリアからのメッセージと同じスレッド上に不正なサイトに誘導するメッセージも表示されてしまったため、多くの人が通信キャリアからの通知と信じてしまい、被害の拡大につながった。

一方、宅配便の不在通知を装う不正な SMS は、主に国内の携帯電話番号から送信されていた。Android スマートフォンの利用者の場合、SMS 内のリンクにアクセスすると、不正なアプリのインストールするよう誘導され、その後、インストールした人自身のスマートフォンから、さらに不正な SMS が大量に見知らぬ番号宛てに送信されており、被害が広がっていった。

前述の海外から送られた SMS については、海外からの SMS 受信拒否を設定することが対策となりうるが、それだけでは被害/加害を十分に防げない状況となっている。

【一般社団法人 JPCERT コーディネーションセンター】

■コラム【パスワードの使いまわしサイトを簡単に調べる方法】

複数のサイトで同じパスワードを使いまわすのは、非常に危険な行為であることは分かっていても、ついつい使いまわしてしまいがちである。

昨年 Google 社と世論調査会社の Harris Poll 社が共同で、米国に在住する 18 歳以上の 3,419 名にパスワードの利用状況を調査するアンケートを行った結果でも、３分の２の 66%の回答者がパスワードの使いまわしを行っているという調査結果が報告されている[10]。別のオンラインサービスでのユーザのパスワードの再利用について調査した結果でも 52%のユーザでパスワードの使いまわしが確認されている[11]。

多くのサイトが ID としてメールアドレスを使っているため、パスワードの使いまわしは、もし、パスワードの使いまわしをしている一つのサイトでパスワードが漏えいした場合、複数のサイトで悪用される可能性が出てくる。

パスワードが漏洩していないか調査してくれるサービスはよく知られているが、パスワードの使いまわしはついうっかり行っているため、自分がどのサイトでパスワードの使いまわしをしているのかは、把握している人は少ないと思われる。Google の Chrome ブラウザは、最近パスワードのチェック機能を実装した。その機能を使えば、下記のように簡単にパスワードの使いまわしを行っているサイトをチェックできる。

1. Chrome を起動する。
2. https://passwords.google.com/ のサイトを開く

[10] https://www.gizmodo.jp/2019/10/200210.html
[11] https://people.cs.vt.edu/gangwang/pass

3.　「パスワードチェックアップ」の「パスワードの確認」をクリック

4.　「パスワードを確認」をクリック

5.　「次へ」でパスワードの分析結果を表示し、サイトの一覧を確認できる。

ただし、この機能を使うためには、Google の Chrome ブラウザのパスワード管理機能を利用する必要がある。昔のブラウザのパスワード保存機能は、安全性が低く、ブラウザのパスワード保存データベースを盗まれるとパスワードが復元できていた。したがって、フィッシング対策協議会のガイドラインでも利用しないことを推奨していた。しかし、最新のブラウザのパスワード管理機能は、ユーザ固有の暗号化により安全になっているため、ガイドラインでもブラウザのパスワード管理機能は、容易なパスワードを利用しないためにも利用することを推奨するように変更した。

最新のブラウザを活用してパスワードの上手な管理をすることでフィッシングの被害のリスクを少しでも減らそう。

【野々下 幸治　トレンドマイクロ株式会社】

3. フィッシングの被害について

3.1. フィッシング詐欺の被害状況

一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）では、フィッシング対策協議会と連携し、フィッシング対策製品・サービスを提供する事業者等にフィッシングサイトの URL 情報を提供している。

フィッシング対策協議会では、2019 年度よりこのフィッシングサイトの URL 情報を活用して、被害状況データの蓄積と統計化、また、ダッシュボード等によるデータの可視化を「被害状況共有ワーキンググループ」の活動の一環として開始した。これにより自社がフィッシングの標的となり被害が及ぶ前の段階から、同業種や異業種における被害状況等を把握し、未然の対策につなげることを目指している。

本データセットによれば、2019 年もトレンドは上昇傾向となっており、標的ビジネス領域の上位は、クラウド事業者、オンライン通販事業者、銀行業となっている。また、特定のブランドを標的としたフィッシング詐欺サイトが数多く確認されており、上位 3 ブランドだけで全体の 52.2%（6,285 件）を占める結果となった。

表.3-1　2019 年のフィッシング URL の標的ビジネス領域

順位	標的ビジネス領域	URL 件数
1	クラウドコンピューティングサービス	2,106 件
2	ネットショップ・EC サイト	1,256 件
3	銀行	882 件
4	通信事業者	421 件
5	クレジットカード	350 件

※上位 5 つの標的ビジネス領域にて全体の 79.8%（5,015 件）を占める。

2019 年被害状況データの分析結果から以下の傾向もある。

・フィッシングサイトにおける暗号化（HTTPS 化）の傾向

　フィッシングサイト全体の 50.4%（3,167 件）は HTTPS にて運用されていることが判明した。フィッシャーは利用者を油断させる手口として、暗号化を組み込む傾向が高まっていると言える。

・フィッシングサイトの設置手口の傾向

フィッシャーが第三者の Web サイトをフィッシングサイトのコンテンツ蔵置先として確保している傾向が確認された。その確保手段は Web アプリケーションが使用するソフトウェアの脆弱性を悪用した Web サイトの改ざんとなっている。特に、オープンソースの CMS（Contents Management System）である「WordPress」の URL パスの特徴をもつケースが目立っている。その数は全体の 5.4%（341 件）を占める結果となった。

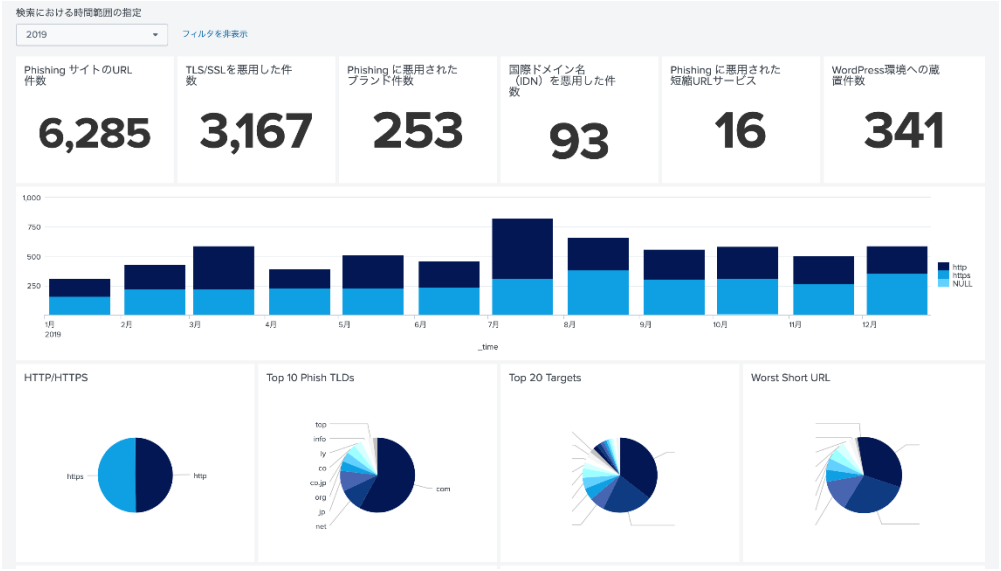

図.3-1　2019 年被害状況データ　ダッシュボード（イメージ）

このような傾向を踏まえた利用者への啓発の必要性とサイバー空間に接続する個々の機器を健全な状態に保つことが重要と言える。

【林 憲明　トレンドマイクロ株式会社】
【加藤 孝浩　トッパン・フォームズ株式会社】

3.2. 金融機関（銀行）をかたるフィッシングが急増

2019 年に急増した国内の金融機関（銀行）をかたるフィッシングには以下のような特徴があった。

１）2 要素認証の突破

- ワンタイムパスワード自体を詐取する手法によるフィッシングが急増。

２）日本または国内の特定地域にターゲットを絞ったフィッシング攻撃が発生

- 沖縄や北海道の携帯番号の特性を利用したスミッシングが発生し、地銀をターゲットとした攻撃が発生。
- これまでは.com や.co といったドメインの利用が見受けられたが、jp ドメインの悪用が見受けられる。不正送金口座に関してもこれまで外国人名義のものが大半だったのに対し、日本人名義のものが急増。

【瀬古 敏智　株式会社三菱 UFJ 銀行】

3.3. SMS を使ったフィッシング

1） 被害状況

2018 年に引き続き、2019 年も SMS を利用したフィッシングは増加傾向の中、不正サイトに誘導された国内のモバイル利用者数が 4 月以降増加傾向にあり、10 月～11 月では 2 カ月間の合計で全四半期を越えているという調査結果が存在する。

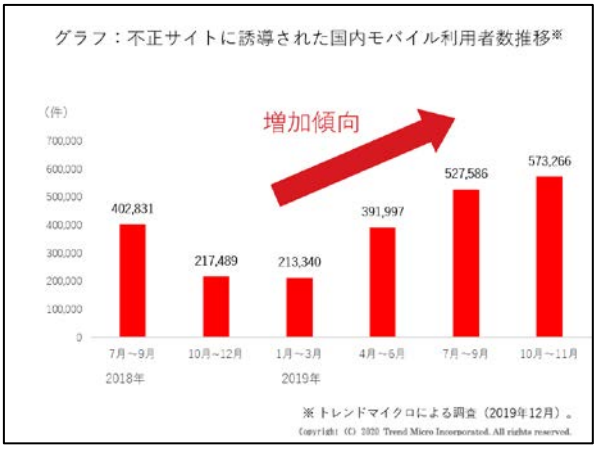

図 3-1 不正サイトに誘導された国内モバイル利用者推移 [12]

被害報告についても、下記の警視庁発表データの通り増加トレンドの中、フィッシング対策協議会の統計によると銀行系の不正送金狙いが 10 月以降急増していることが特徴の 1 つである。

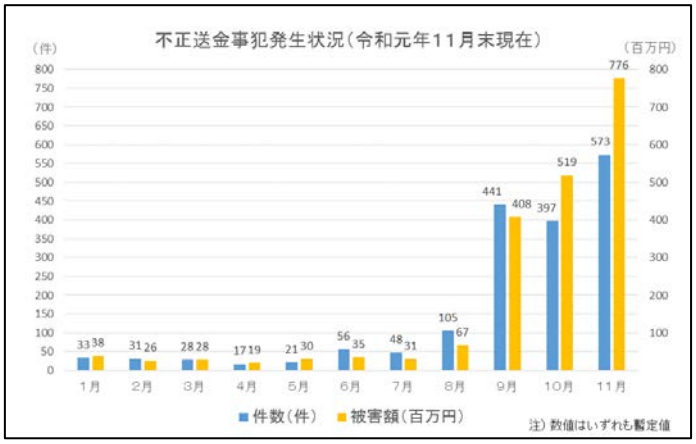

図 3-2 不正送金事犯発生状況（令和元年 11 月末） [13]

---

[12] トレンドマイクロ社より提供資料（「2019 年の主に個人を標的とするサイバー犯罪の動向を解説するセミナー（2020 年 1 月 7 日）」より）

[13] 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 警視庁発表 2019 年 12 月 19 日

表 3-1　SMS フィッシング被害報告件数 [14]

2019年	6月	7月	8月	9月	10月	11月	12月
銀行	2	0	4	11	68	63	12
クレジットカード	0	1	0	0	2	2	0
物販・EC	5	3	0	2	3	1	1
物流	8	25	16	5	6	19	20
携帯キャリア	3	5	0	0	0	0	0
計	18	34	20	18	79	85	33

携帯電話会社のキャリア決済については、被害増加の一方、不正利用の補償制度が存在しなかったことから、被害者や国民生活センター、報道機関による改善要求に応える形で、大手 3 社が利用規約を改定し、全額補償をすることを 8 月末以降、順次決定した。

２）　フィッシング SMS の特徴

SMS でのフィッシング目的に悪用される SMS の送信元番号は、従来通り、国際網（+を含む国番号から始まる番号、またはアルファベット）、携帯電話端末（090 から始まる番号等）が使用されていることが下表の通り報告されている。

正規な SMS を配信する企業側の対策としては、従来通り国内網直接接続（03 から始まる番号等）を利用することだが、一部の SMS 配信事業者が携帯電話端末を用いたサービスを特定の携帯キャリアの料金プランを利用して提供していることが報告されている。

このような利用形態は携帯キャリアが想定していたものではなく、携帯キャリアが SMS の法人利用に課している利用審査ができないという課題もあり、キャリアは利用規約の変更、および該当料金プランの受付終了という対策をしていることから、フィッシングに対するリスクだけでなく、サービスの安定提供に対してもリスクがあると考えられる。

[14] フィッシング対策協議会提供資料

種別	発信元電話番号	報告件数
国際網	国際電話番号（+国番号から始まる）	93
国際網	アルファベット文字列	52
国際網	電話番号以外の数字	2
国内携帯	携帯電話番号（090 等から始まる）	128
	番号不明	41
総計		**316**

図 3-3　フィッシング被害が報告された SMS 送信元（6～12 月）[15]

【浦田泰裕　株式会社アクリート】

[15] フィッシング対策協議会提供資料（6～12 月）

3.4. フィッシングサイトの URL の傾向

フィッシングサイトの URL については以下の手口を確認している。いずれも消費者に正規サイトと誤認させフィッシングサイトへ誘導している。

同一文面のフィッシングメールでも、複数のフィッシングサイトを用意しているケースがある。

1）トップレベルドメインを複数用意
2）類似する URL を複数用意
3）短縮 URL を使用
4）正規 URL を偽装してフィッシングサイトへ誘導

注：以下は例であり記載のトップレベルドメインや英数字記号が、必ずしもフィッシングサイトで使用されているものではありません。

1）トップレベルドメインを複数用意
（正規〇）http://●●●.jp
（不正×）http://●●●.xyz
（不正×）http://●●●.ltd

2）類似する URL を複数用意
（正規〇）http://●●●.aa.jp
（不正×）http://●●●-aa-jp.com
（不正×）http://aa.●●●.jp

3）短縮 URL を使用
http://▲▲.▲▲/●9●6
→ （不正×）http://●●●-jp.top へリダイレクト

4）正規 URL を偽装してフィッシングサイトへ誘導
http://●●●. jp （表記上は正規）
→ （不正×）http:// ●●●-jp.online へリダイクト

事業者においては、このような傾向を認識し、1 件のフィッシングサイトが閉鎖となっても安心することなく、消費者が同種のフィッシングサイトで被害に合わないよう、継続して情報収集に努めることが必要である。

また、消費者においてはメールに記載されている URL を送信事業者の正規 URL と見極めることは困難であることから、メールに記載されている URL はクリックしないで、予め正しい URL を登録したブックマークからアクセスすることが必要である。

【内山裕延　三菱 UFJ ニコス株式会社】

■コラム【広告を利用した新たなフィッシング手法】

フィッシングサイトへ誘導するための手法として、メールや SMS を利用したプッシュ型のものが広く知られているが、2019 年より検索エンジンの広告を利用した手法も確認されるようになった。ユーザが検索エンジンで社名やサービス名などのキーワードを検索すると、検索エンジンの広告枠に攻撃者が事前に出稿していた広告が表示され、誤ってクリックすると攻撃者が用意したフィッシングサイトへ誘導されるという仕組みだ。広告枠の仕様上、検索結果よりも広告が優先されるため、場合によっては公式サイトよりもフィッシングサイトが上部に表示される。そのため、ユーザはより一層の注意が必要となる。

検索エンジンの広告を利用したフィッシングサイトの場合、広告を削除するとフィッシングサイトへ誘導する際の証跡が残らないため、いつ攻撃が行われていたかを特定することが困難となる。さらに、攻撃者にとってはメールや SMS のようにいつアクセスされるのか予想しづらい誘導手法とは異なり、攻撃者の意図した時間枠で攻撃（広告出稿）を行うことができる。そのため、ユーザがフィッシングサイト上で認証情報やワンタイムパスワードを入力した際に、そのワンタイムパスワードの有効期限内に攻撃者がリアルタイムかつ手動で正規サイトへログインし不正を働くというケースにつながりやすい。攻撃者にとって２要素認証の突破は必須となりつつある昨今、効率の良い攻撃手法の一つである検索エンジンの広告を利用したフィッシングサイトは今後増加することが予想される。

【松岡　晋矢　株式会社 bitFlyer】

4. フィッシングの対策について

4.1. 個人認証の状況と背景

フィッシング詐欺とは、インターネット上でサービス利用に関する情報を詐取する詐欺行為であるが、その主たるものは、個人認証に関する情報である。銀行取引や商品購入、ゲームのアイテム管理など個人の資産に関するサービスにおいて、本人と偽ってサービスを利用し、その資産を詐取するなどのために本人の認証情報を詐取するのである。

サービス提供者側では、利用者を守り、安心利用できるサービスを提供するために、個人認証については、フィッシング詐欺で情報を詐取されても大丈夫な個人認証の提供を出来る限り心掛けている。そして、提供サービスに関連する個人資産の価値に比例して厳格な認証システムが用意されるが、厳格であればあるほど安全性は上がるが、利便性が下がることが多く、これら安全性と利便性は反比例する関係であり、守られるべき資産の価値に合わせた、厳格性・利便性とのバランスが求められる。

このような背景の中、単純な ID とパスワードの認証から、それに他の要素の認証を加えた二段、もしくはそれ以上の多要素認証が提供されている。それぞれの認証技術については、後述の内容に任せることにして、ここではどのようなサービスにおいて、どのような認証が提供されているかを調査した結果があるので、それを元に状況を伝える。

以下は、2019 年 2 月にフィッシング対策協議会 認証方法調査・推進ワーキンググループが実施したアンケート調査「インターネットサービス事業者が採用している認証方法について」の結果からの考察である。

全体として、75%以上のサービスが ID、パスワードのみの認証しか行っていなかった。特に通信、保険、交通機関のサービス、また、ID 数が少ないサービスほど ID//パスワードのみの比率が高く、多要素認証への対応が遅れていると考えられる。銀行では、ID//パスワード以外に 10 種以上の認証方式の採用が確認されており、資産移動などの場面で新たな要素の認証を行うなどの対応が進んでいる。また、インターネット販売、ゲーム業界では、30%以上が多要素認証を取り入れている。

認証方式の選択にあたっては、銀行が圧倒的な比率で手間を減らすよりも、安全性を重視しており、クレジットカード業界では半々、ゲーム業界では手間の少ない方式を優先している傾向がある。

そして、認証技術に「セキュリティ」と「ユーザビリティ」のどちらを求める

かという、どうあるべきかの質問に対しては、金融関連の 80%が「セキュリティ」と回答しており、資産の重要度と求める安全性が比例していることが見られた。他、すべての業種においても「ユーザビリティ」よりも、「セキュリティ」を求める回答が上回っており、フィッシング被害対策への関心が高いことが確認された。

調査の詳細な結果については、以下にて参照可能。

【報告書公開のお知らせ】

https://www.antiphishing.jp/news/info/wg_auth_report_20190701.html

【報告書】

https://www.antiphishing.jp/news/pdf/wg_auth_report01_20190701.pdf

利用者の資産を守るために多要素認証の採用や、FIDO などユーザビリティも同時に向上させるような認証方法も登場しているが、フィッシング詐欺の手口も巧妙化しており、二段階認証も突破するフィッシング詐欺も確認されるなど、より強固で厳格、かつ利便性も確保された認証技術が求められている。

【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】

【吉田晋　株式会社コネクトワン】

4.2. 認証技術関連

4.2.1. リスクベース認証

オンラインのサービスにアクセスしたときにユーザのなりすましが起きるリスクに応じて複数の認証方式を組み合わせる、「リスクベース認証」が注目されている。これは、従来の方式、例えばパスワードで認証が行われた後、それでも正しいユーザかどうかがあやしいときに、別の認証方式で認証が行われるようにする仕組みである。どういうものなのかを紹介したい。

◆ 認証したのに正しいユーザではない？

パスワード認証は「パスワードを知っている」というユーザの特徴を利用した認証方式である。従ってパスワードが漏洩してしまうと、それを知っている人であれば、通常ではありえないような別の国や別の会社からのアクセスであっても認証に成功してしまうことになる。

一方、正しいユーザかどうかを判断する材料には「パスワードを知っている」という他にもある。例えば、先ほどの別の国や別の会社からのアクセスである場合、アクセス元である IP アドレスがまったく異なり、また正しいユーザの利用環境を知らずにパスワードだけを知っている人がアクセスしている場合には、Web ブラウザの種類が違うといったことが挙げられる。パスワード以外で、アクセスしているユーザの正しさ、あやしいかどうかを判断する材料は意外に多い。

◆ あやしいときに追加で認証する

何をもって「あやしい」と判断するのかについては、リスクベース認証として何か定めがあるわけではなく、認証を行う側すなわちリスクベース認証を行う者が決められるようになっている。追加の認証をどの方式で行うかについても同様である。

リスクベース認証を行うときには、まずユーザに、パスワードなどの他に秘密の質問と回答や SMS の送信先番号といった追加の情報を登録してもらう。ユーザがアクセスをしたときに、始めにパスワードなど、予め定めておいた共通の方式でユーザ認証が行われる。その認証に成功し、かつ普段通りのアクセスであれば、そのままサービスを利用いただく。認証には成功したが普段とは異なるアクセスだった場合には、最初に登録してもらった秘密の質問に答えてもらう、CAPTCHA を解いてもらう、といった追加のチェックを行っていく。それらにも成功したときにはサービスを利用できるようになる。ユーザ認証を行うサーバ

の設定によって、この順序や条件は変えることができる。

◆ 普段通りかどうかの判定

普段通りのアクセスなのか普段とは違ったアクセスなのかの判断はどのように行われるのだろうか。それには「リスクスコア」が使われる[16]。アクセス元の特徴が、予め定めておいた範囲におさまっていない場合、スコアが加算されていく仕組みである。

（スコアの計算に使われる要素）

- アクセス元の IP アドレス
- Web ブラウザの種類
- Web ブラウザの言語の設定
- IP アドレスに基づいて検索した地理的な情報（国など）

スコアが普段よりも高い場合には、SMS を使って番号を入力するように促したり CAPTCHA を解くように促したりといった、追加の認証が行われる。明らかに不正と認められるような高いスコアである場合には、アクセスをブロックすることもできる。

◆ リスクベース認証を行うには

リスクベース認証は 2006 年頃に出てきたもので[17]、2010 年頃にオープンソース・ソフトウェアが現れた[18]。サーバ側でリスクベース認証に対応するための実装には、アクセス管理に関する、以下がある。各々商用版がある。

- OpenAM

OpenAM コンソーシアム
https://www.openam.jp/
GitHub-openam-jp/openam
https://github.com/openam-jp/openam/

---

[16] "Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild", Stephan Wiefling1, Luigi Lo Iacono1, and Markus D¨urmuth, ICT Systems Security and Privacy Protection. IFIP Advances in Information and Communication Technology. Springer International Publishing: 134–148.
https://epb.bibl.th-koeln.de/frontdoor/index/index/docId/1369

[17] US patent 9021555, Takaya Kato(BANK OF TOKYO MITSUBISHI UFJ [JP])
https://worldwide.espacenet.com/patent/search/family/038540891/publication/US20130811 07A1?q=pn%3DUS9021555

[18] ForgeRock Extending Sun's OpenSSO Platform - InternetNews.
http://www.internetnews.com/dev-news/article.php/3881681/ForgeRock+Extending+Suns+OpenSSO+Platform.htm

- Keycloak
  Keycloak
  https://www.Keycloak.org/
  GitHub-keycloak/keycloak
  https://github.com/keycloak/keycloak

リスクベース認証の特徴として、普段通りのアクセスであれば追加の認証は必要ないため、正しいユーザが普段通りに利用する分には利便性が損なわれない点が挙げられる。また正しいユーザが普段と異なる Web ブラウザを使ってアクセスしたときに、認証手続きが増えるだけで、利用することができる点は利便性を補完していると言える。

パスワード認証だけでは心もとない、ユーザのパスワードが偽のサーバ等を通じて漏洩してしまっているのではないか、といった不安があるときに、リスクベース認証は改善策の一つとして位置づけられるものではないだろうか。

【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】

4.2.2. FIDO を使用した生体認証

近年では、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注目を浴びている。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できる。

FIDO はパスワードの変わりにオンライン認証を行う UAF と、二要素認証として使用する U2F が策定されていた。UAF や U2F を FIDO 認証で使用する場合は、FIDO に準拠したハードウェアトークンなどの認証器や、スマートフォンでは認証を要求するアプリケーションなどを提供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、対応する Web ブラウザのみで FIDO 認証を行うことができる。

FIDO2 では WebAuthn (Web Authentication API)をサポートしたブラウザを使用すると FIDO 認証を行うことができる。WebAuthn は 2019 年 3 月に W3C により勧告され Web の標準機能になり、Microsoft Edge、Google Chrome、Firefox に加え、Safari でも一部サポートが開始されている。

2019 年 11 月には国内で初めて FIDO UAF、U2F、および FIDO2 の相互接続性テストを開催し、自社サービスの認証に FIDO を対応させるなどの普及が進んでいる。

【松本悦宜　Capy 株式会社】

4.3. SMS を使ったフィッシングへの対策

◆ フィッシング詐欺で利用される国際 SMS

SMS を利用したフィッシング詐欺のほとんどは、携帯電話端末もしくは国際網を経由した SMS 配信サービスを利用している。攻撃者は身元を特定されることを避けるため比較的匿名での利用がしやすいこれらの送信手段を用いていることが多い。国内直接接続の SMS 配信サービスでは利用審査や契約手続きなどがあり匿名での利用が困難なためである。

◆ 消費者側の対策　～国内企業から国際 SMS が届いた場合に詐欺を疑う～

この点に着目すると企業からの通知 SMS と攻撃者が送る詐欺 SMS を見極めることが消費者側の対策となる。具体的には発信者番号が 090 等から始まる国内の携帯電話番号で届いた SMS および海外の電話番号もしくはアルファベット表記で届いた SMS は、内容に関わらず詐欺の可能性を考慮して対応するのが有効である。フィッシングサイトの URL は本来のドメインと類似したドメインが用いられることが多いため、上記の通り発信者番号が疑わしい場合は安易に URL をタップせず真偽を確認することが望ましい。

◆ 事業者側の対策　～消費者が判別できる手段を提供する～

受信した SMS に詐欺の疑いをもった消費者に対し、真偽を判別するための手段を提供することが重要である。携帯電話端末や国際 SMS は前述の通り、攻撃者が詐欺に利用しやすくかつ、企業が通知 SMS でそれらを利用した場合、消費者は判別できない。企業が消費者に SMS を送る場合は、発信者番号で判別が可能な国内接続の SMS 送信サービスを利用する必要がある。さらに発信者番号は自社ドメインのウェブサイト上に掲載することが望ましい。受信した SMS に詐欺の疑いをもった消費者に対し、確認の手段を提供することができるからである。SMS 配信経路ごとの特徴については、表 4-1 に整理した。

表 4-1　SMS 配信経路ごとの特徴
（フィッシング対策ガイドライン 2020 年度版より抜粋）

	国内直接接続の SMS 配信	国際網を経由した SMS 配信	携帯電話端末からの SMS 配信
発信者番号表示	日本の電話番号 （例：03-0000-0000） 携帯キャリアごとの特別番号 （例：50000）	海外の電話番号 （例：+1 000-000-0000） アルファベット （例：FOOBAR）	携帯電話番号 （例：090-0000-0000）
発信者番号登録・変更	契約者が自由には登録・変更できず、事前申請が必要	契約者が任意のタイミングで自由に登録・変更することが可能	携帯キャリアからの払い出しのみ
利用審査の厳格性	現在、審査をしないまま偽名や匿名での申込者に提供している事業者が存在しない	審査がなく偽名や匿名での申込者へ提供する事業者が存在する	端末レンタルサービス等で十分な審査を実施しないまま提供する事業者が存在する
Web サイト運営者の対策	自社が送信する SMS の発信者番号を利用者に対しウェブサイト等に記載し事前に通知したうえで利用する	フィッシャーに利用されやすく、利用者にとって自社が送信する SMS と判別しづらいことから、極力利用を避ける	フィッシャーに利用されやすく、利用者にとって自社が送信する SMS と判別しづらいことから、極力利用を避ける
利用者の対策	発信者番号は Web サイト運営者が事前に告知している番号と異なる SMS を受信した場合、フィッシングの可能性を疑い慎重に行動する	Web サイト運営者を騙ったフィッシングの可能性を疑い、慎重に行動する	Web サイト運営者を騙ったフィッシングの可能性を疑い、慎重に行動する
発信者番号の表示イメージ			

※国内直接接続の SMS 配信においても双方向サービスでは、利用審査を経た携帯電話番号を用いる場合がある。

◆ 将来的な展望について

SMS の次世代版として世界的に注目が高まっているのが RCS（Rich Communication Service）である。RCS は、携帯電話番号宛てのテキストの送受信に加え、写真や動画などの送受信やグループチャットといった、リッチなコミュニケーションとして利用可能な機能を備えている。携帯キャリアの国際的業界団体 GSMA により SMS の後継のメッセージサービス規格として標準化され、全世界で採用事業者が拡大している。

2019 年 4 月に国内携帯 3 キャリアは、この RCS に準拠したサービスである「＋メッセージ」の提供開始を発表した。「＋メッセージ」では事業者が公式アカウントを取得したうえで、消費者とメッセージのやりとりをする。この公式アカウントには携帯キャリア 3 社それぞれの審査を受け、認証を得たことを示す「認証済みマーク」が表示される仕組みが用意された（図 4-1）。消費者にとって、より詐欺の判別がしやすい環境が整備されたと言える。今後、SMS から「＋メッセージ」への世代交代が進むことで、携帯電話利用者をターゲットとしたフィッシング対策の環境は大きく改善される見込みである。

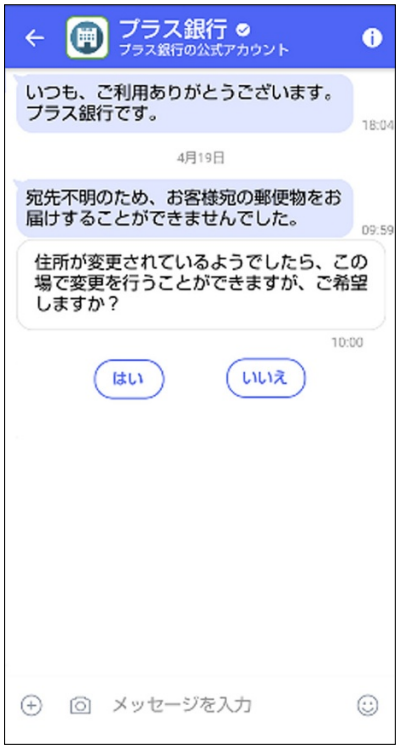

図 4-1 ＋メッセージの詳細 [19]

【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】

[19] 出典：「＋メッセージ」の機能を拡充　−携帯電話番号だけで、企業と安心・安全にメッセージのやりとりが可能に−＜2019 年 4 月 23 日＞
https://www.nttdocomo.co.jp/info/news_release/2019/04/23_00.html

■コラム【ユーザを認証するサーバの正しさ】

◆ ワンタイムパスワードが取られてしまう

2019 年後半、偽サイトによってユーザが入力したワンタイムパスワードが取られてしまい、そのまま本物のサイトで使われたという手口、そしてそれによる不正送金の被害が報道されている[20]。ユーザが入力するパスワードを複雑なものにしたり、一時的なものにしたりしても、ユーザが偽サイトでそれらを入力すると漏洩してしまい、悪意をもった第三者に使われてしまった。

これを避けるにはどうすればいいのか。これまではユーザ自身が偽サイトかどうかを判別し、あやしいサイトではパスワードやワンタイムパスワードを入力しない、というユーザの挙動に依存する対策が考えられてきた。サーバ証明書や Web ブラウザのアドレスバーの表示は偽サイトかどうかの判別に使えるものだが、先の報道は多くのユーザが偽サイトであることを見破ることができなかったことを示している。

◆ 正しいサーバでなければ認証処理を進めないという考え方

ユーザの中には、パスワードやワインタイムパスワードを入力させる、すなわちユーザを認証する処理を行うサーバが、正しいサーバかどうかを確認する人がいるかも知れない。しかし近年、Web ブラウザは鍵マークやグリーンバーの表示を変えつつあり、その動向に詳しくなければ正しいかどうかが分かりにくくなりつつあるかも知れない。またスマートフォンのように表示領域が限られているデバイスでサーバの正しさを確認するハードルは以前よりも上がっていると言える。ユーザの視点ではドメイン名を見てもそれが正しいものなのかどうかが分かりにくいことがある、という根本的な課題もある。

一方、認証の処理を正しいサーバである場合にのみ行う、その処理を自動化する、という仕組みが注目される動きがある。元来それを意図したものではなかったかも知れないが、それを含めて以下に事例を紹介したい。

- Web ブラウザのパスワード保存・入力機能

あるユーザが、検索を通じてサイトにアクセスした際、パスワードが自動的に入力されなかった。ユーザ自身はパスワードを忘れてしまっているため、手元にあるパスワードを探さざるを得なくなり、その間に、アクセスしているサイトが違うためにパスワードが入力されなかったのだと気づ

[20] ネットバンキング被害 4 倍に「ワンタイムパス」破る:日本経済新聞, https://www.nikkei.com/article/DGXMZO55313840W0A200C2MM0000/

き、パスワード漏洩を免れた。

- WebAuthn / FIDO

FIDO と共に使われる WebAuthn(W3C Web Authentication)には、認証を行うサーバを識別できる値 rpId を、Web ブラウザにおいて確認する仕組みがある [21]。

- ワンタイムコードのサーバへの関連付け [22]

ユーザに SMS で届くワンタイムコードが、本来どのサイトで入力されるべきものなのかを関連付けるフォーマットが提案されていて、実装が現れている [23]。Apple 社では SMS で届いたワンタイムコードの入力をユーザが行うのではなく自動的に行う仕組みも作られている [24]。

第三者によるユーザアカウントの悪用から、いかにユーザを守っていくかは、オンラインのサービスを提供する者の検討課題であり続けると言える。フィッシングサイトはサービス提供者としては関知し得ないところで立ち上がる状況の中でユーザを守っていくためには、本レポートなどを通じていち早く動向をキャッチし、次の手を考えていくことが重要である。

【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】

[21] Web Authentication: An API for accessing Public Key Credentials Level 1, https://www.w3.org/TR/webauthn/

[22] 株式会社アクリート 浦田泰裕氏より情報を頂いた。

[23] Delivering origin-bound one-time codes over SMS, https://github.com/WebKit/explainers/tree/master/sms-one-time-code-format

[24] iPhone で SMS のパスコードを自動入力する - Apple サポート, https://support.apple.com/ja-jp/guide/iphone/iphc89a3a3af/ios

5. まとめ

フィッシング詐欺における 2019 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、月単位の右肩上がりで急激な増加を示しており、2019 年 12 月（8,208 件）は 2018 年 12 月（1,884 件）の約 4.4 倍となっている。フィッシングに悪用されたブランド数においても、2019 年 12 月（67 件）は 2018 年 12 月（37 件）の 2.7 倍であり、より幅広い企業・組織に対する攻撃が非常に活発化していることがうかがえる。

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、高い危機意識をもって、さらなる事前あるいは追加の対応について検討・実践していく状況に既にあることを再度確認いただきたい。

来年 2021 年は、東京オリンピック・パラリンピックが開催され、世界中の攻撃者から日本が一層注目されるため、フィッシング詐欺もさらなる発生件数と被害状況となることも予想される。昨今はワンタイムパスワードの奪取を行うフィッシングも一般化しつつあり、対抗する側としては厳しい状況ではあるものの、より最新の対策技術の導入検討はもとより、お客様への啓発や情報発信、発生時に迅速な対応を行うための社内体制整備など考えること、できることは多い。

このような状況において、本協議会は引き続きフィッシングに関する最新情報を収集・分析し、フィッシングに対抗する事業者様とフィッシング詐欺のリスクに日夜接する利用者様への支援をなお一層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】

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
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
吉田　晋　　株式会社コネクトワン
加藤 孝浩　トッパン・フォームズ株式会社
林　憲明　　トレンドマイクロ株式会社
宇井 隆晴　株式会社日本レジストリサービス
内山 裕延　三菱 UFJ ニコス株式会社
山本 和輝　BB ソフトサービス株式会社
塚越 彩　　株式会社 bitFlyer
松岡 晋矢　株式会社 bitFlyer
松本 悦宜　Capy 株式会社
早川 和実　NTT コミュニケーションズ株式会社
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
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
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
瀬古 敏智　株式会社三菱 UFJ 銀行
木村 未咲　株式会社三菱 UFJ 銀行
貞広 憲一　株式会社みずほフィナンシャルグループ

【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）