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

フィッシング対策ガイドライン

2020 年度版

2020 年 6 月

フィッシング対策協議会
https://www.antiphishing.jp/

序

最近、国内でもフィッシング被害が増加している。これは、従来、英語によるフィッシングメールやおかしな言い回しの日本語によるものが多かったため、必ずしも十分な対応がなくても、被害が増加しなかったものと思われる。しかしながら、最近は、完璧な日本語表現によるフィッシングの増加やスマートフォンなどでの利用が増加しているため、多くの利用者が被害を受けやすくなっている。

金融機関（オンラインバンキング）、インターネットショッピング、インターネットオークション、オンラインゲームなどの登録会員制 Web サイトを運営する事業者および情報セキュリティ関連団体なども、利用者に対してフィッシング詐欺に関する注意喚起とともに被害を避けるための対策方法の啓発を行っている。

フィッシング対策は、利用者向けの対策と Web サイト運営者向けの対策があるが、Web サイト運営者の立場からみると、フィッシング被害を防止するための措置を講じることは、Web サイト運営者の信用を高め、利用者からの信頼・安心を得ることになる。

フィッシング対策事項を集約し、利用者が被害にあわないために行うべき対応や不幸にして被害を受けた時に行うべき対応を、ガイドラインとして整理し、周知・啓発を行うことで、利用者の被害を最小限に抑えることができる。

フィッシングを未然に防ぐための予防措置や、フィッシング被害にあってしまった場合の対応を、ガイドラインとして整理し、多くの Web サイト運営者がガイドラインに従い対策に取り組むことにより、インターネットを活用したサービス業界全体のフィッシング被害の対応レベルの向上が期待できる。

この様なことから、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では、利用者および Web サイト運営者を読者と想定したフィッシング対策ガイドラインを策定することとした。

本ガイドラインを活用することにより、フィッシング詐欺被害を未然に防ぎ、また被害が発生した場合の被害拡大を効果的に抑止するために役立てていただければ幸いである。

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. はじめに

本章では本フィッシング対策ガイドラインの目的、適用範囲など本ガイドラインに関する概要を記す。

1.1. 本ガイドラインの想定読者および目的

本ガイドラインは、フィッシングによる被害を受ける可能性のある Web サイト運営者および利用者がフィッシングの手法により不正に利益を得ようとする者に対して講じておくべき対策について、適切かつ有効であるという観点から選択・整理し、提示することを目的とする。

1.2. 本ガイドラインの対象としない領域

本ガイドラインでは、フィッシング対策に焦点を絞るため、以下の領域については言及しないこととする。

・Web サイト運営者における安全性、機密性、完全性、可用性の確保

・利用者におけるウイルス、スパイウエアなどのマルウエア対策（フィッシング詐欺に悪用されるものについては考慮）

Web サイトの安全性については、(独) 情報処理推進機構「安全なウェブサイトの作り方」[1]など、Web サイト構築に関するセキュリティガイドラインを参照しつつ、外部専門機関などを活用して、正規サイトの安全性を確保・検証することが不可欠である。

また、サービス、サーバ機器、ネットワークなどに関する安全管理の詳細については、同機構のシステム管理者向け情報セキュリティ関連情報[2]などを参考にしていただきたい。

1.3. 用語解説

本ガイドラインで扱う用語の意味を以下に示す。

【フィッシング（phishing）】
実在する組織を騙って、ユーザネーム、パスワード、アカウント ID、ATM の暗証番号、クレジットカード番号といった個人情報を詐取すること。

【フィッシャー（phisher）】
フィッシング行為は、おとりとなる電子メールを起案する者、電子メールを送信する者、フィッシングサイトを設置する者など、複数の行為者で構成される。フィッシャーとは、それら一連の

[1] https://www.ipa.go.jp/security/vuln/websecurity.html
[2] https://www.ipa.go.jp/security/sysad/index.html

行為者の全体を意味する。

【フィッシングサイト（phishing site）】
金融機関、クレジットカード会社など、金銭に関連するアカウント情報を持つサイトを模倣して設置されたおとりサイトのこと。

【フィッシング被害】
事業者がその社名やサービス名などブランドを不正に第三者に騙（かた）られたり、そのログイン画面などを真似られたりすることによりフィッシング行為に悪用されること。または、そのフィッシング詐欺により利用者や従業員が個人識別情報を詐取されること。または、そのフィッシング詐欺により利用者や事業者が金銭的な損害を被ること。

【テイクダウン（take-down）】
フィッシングサイトを閉鎖することを指す。シャットダウンまたはサイトクローズともいう。

【CSIRT（シーサート、Computer Security Incident Response Team）】
コンピュータおよびコンピュータネットワークで発生したセキュリティインシデントに関する報告を受け取り、精査した後に、適切な対応を行うことを目的に組織されたチームのことを指す。特定の企業、大学など比較的大規模な教育機関、地域あるいは国家、研究ネットワークなどのために組織される。

【SMS（Short Message Service）】
携帯電話同士で電話番号を宛先にして短いテキスト（文章）によるメッセージを送受信するサービス。開封率の高さから企業から利用者への連絡手段として利用されている。

2. フィッシングに関する基礎知識

本章では、フィッシング詐欺の主要な手法などについての基礎的な知識を示す。

2.1. フィッシング詐欺の手口

フィッシング詐欺の単純な例を図 1 に示す。

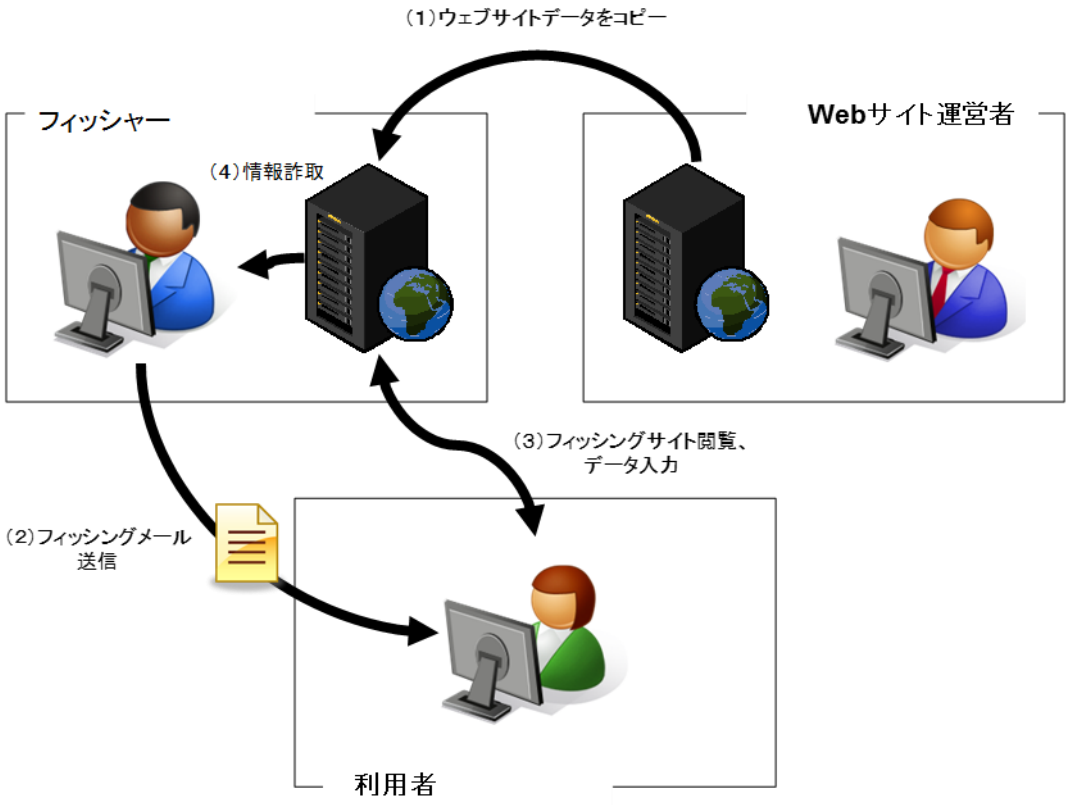


図 1 フィッシング詐欺の単純な例

まず、フィッシャーはターゲットとする事業者の Web サイトのデータをコピーしてフィッシングサイトを設置する。次に、フィッシングサイトをリンク先とした URL を文面に含めたフィッシングメールを利用者にばら撒く。リンク先にアクセスした利用者が個人情報、アカウント情報、クレジット番号などを入力することでフィッシャーが情報を手に入れる。

なお、フィッシング詐欺のうち、「標的（誰をだますのか)」に注目した事例として、スピアフィッシング というものがある。これは、特定の人間の個人情報やパスワードを窃取することを目的とした攻撃である。特定の人間向けにカスタマイズされたフィッシングメールなどを送付するなど、最適化がされている。このため、成功率は一般のフィッシングよりも高いと考えられる。ただし、スピアフィッシングは、その目的からするとフィッシング詐欺というよりも、標的型サイバー攻撃の一種に分類する方が適当かもしれない。

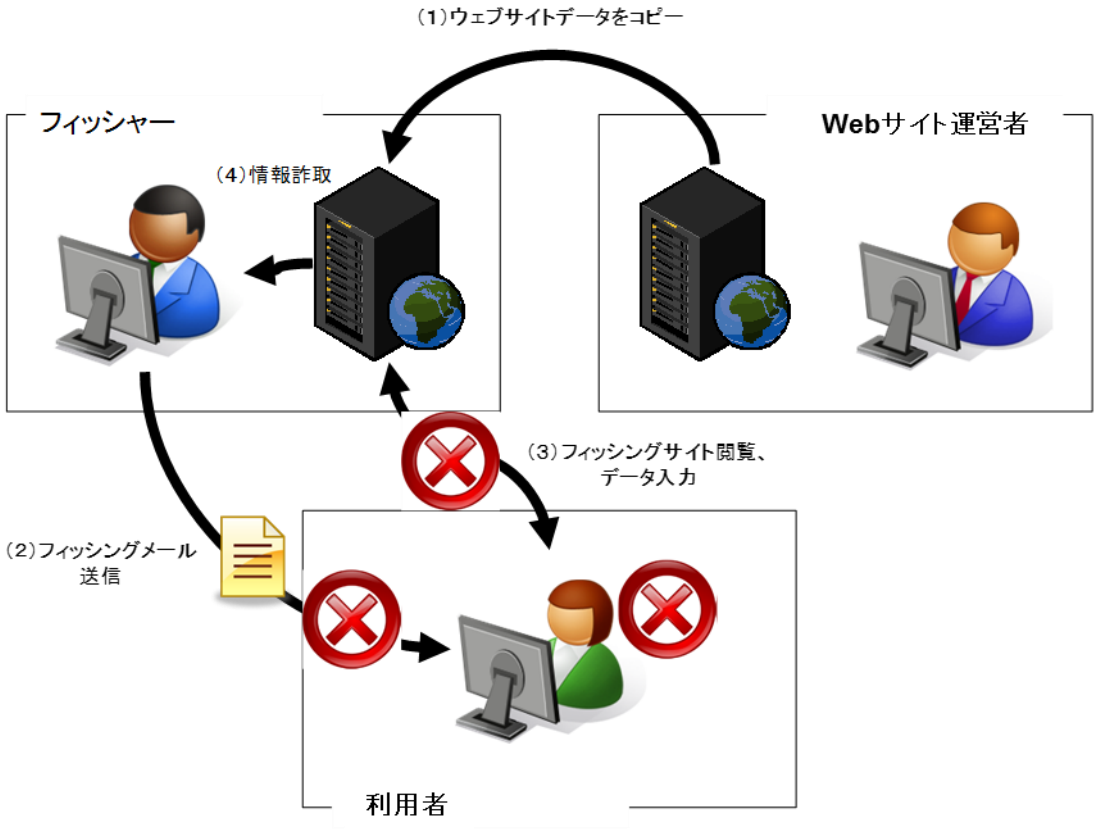


図 2 フィッシング詐欺被害の抑止ポイント

フィッシング詐欺の被害を抑制するためには、図 2 に示すような抑止ポイントで対処する必要がある。つまり、フィッシングメールが利用者に届かないこと、届いたフィッシングメールを読まないこと、フィッシングメールを読んでしまった利用者がフィッシングサイトを閲覧しないこと、フィッシングサイトを閲覧してしまった利用者が個人情報などを入力しないことといった抑止ポイントで対処する必要がある。

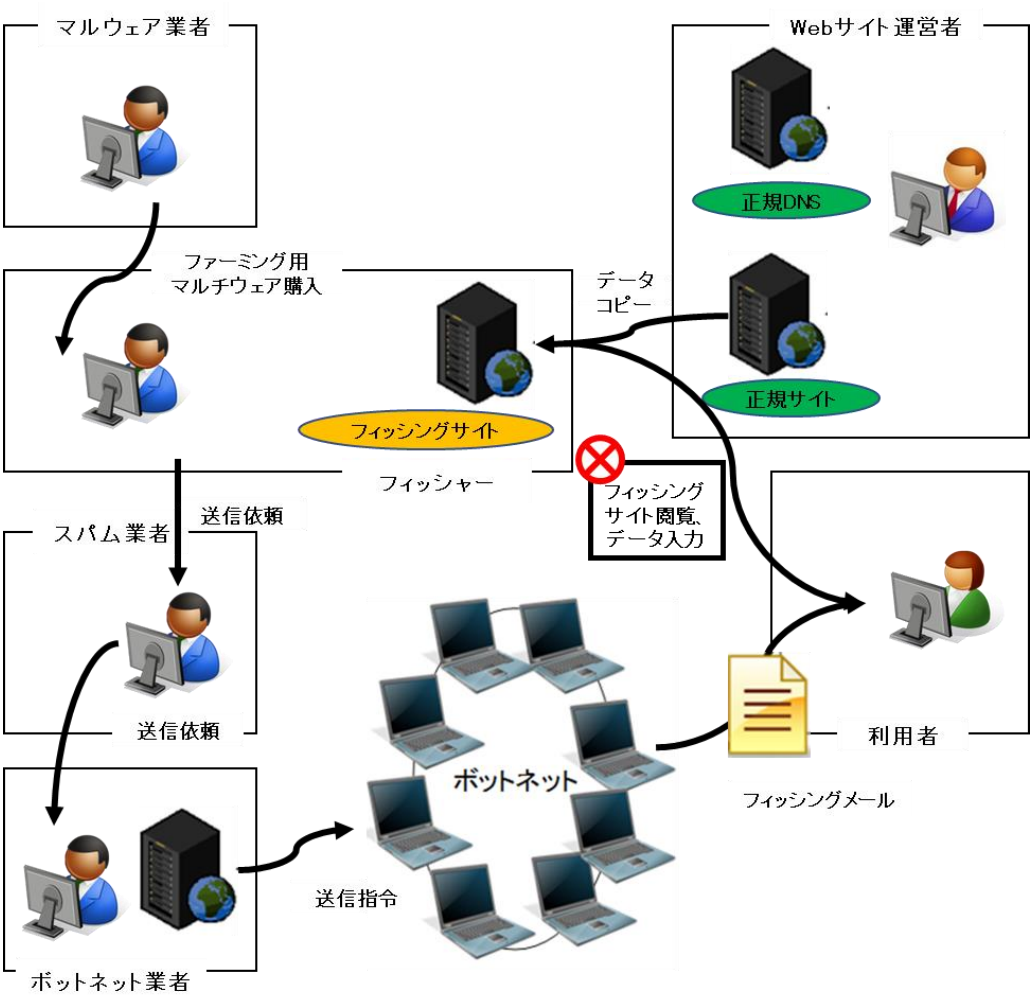


図 3 フィッシング詐欺の複雑な例

近年確認されているフィッシング詐欺においては、工程ごとの専門分業体制が確認されている。計画、調達、構築、誘導、詐取、収益化、強化拡大の 7 つの工程において別々の犯罪者による請負・仲介・誘引が行われている。こうした分業体制が実現している要因のひとつとして、犯罪者コミュニティにおけるサービスやツールの氾濫があげられる。

フィッシングサイトを設置して利用者の情報を集めるフィッシャー、フィッシングメールの作成と大量送信を請け負う迷惑メール配信業者、送信元を隠すためボットネットの貸し出しを行う業者、本人確認が緩く発信者情報の開示要求や警察からの捜査協力依頼に対して非協力的なホスティングサービス（Bulletproof Hosting）などは「サイバー犯罪のためのサービス（Crime as a Service）」として調達、構築することが可能である。

また、ファーミング[3]用にカスタマイズされたマルウェアや、複数の流出情報をまとめた「漏洩アカウント情報リスト（Anti Public Combo List）」、フィッシャーがフィッシングサイトを設置する際に、設置の簡略化と詐取情報の一元管理を実現する「フィッシングキット」、「パスワードリスト攻撃ツール（Credential Stuffing Attack Tool）」など、フィッシング行為ならびに詐取した個人情報の悪用、収益化を手助けするツールの売買が行われていることも確認している。

なお、フィッシングにおける調達、構築において濫用されている認証局より取得した証明書の悪用によるフィッシングサイトの HTTPS 化（TLS/SSL 化）などが問題となっている。（図 3）。

フィッシャー側の構造が複雑になることで事件として捜査する際には支障が発生する可能性があるものの、フィッシング詐欺に対抗するための Web サイト運営者、利用者サイドの対策に大きな変化を求めるものではなく、本ガイドラインにて説明する要件に配慮して、Web サイト運営者においては信頼できるサービスの構築に努め、利用者においてはフィッシング詐欺被害に関する知識、騙されないための知識を身に付けていただきたい。

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

SMS を利用したフィッシングでは、メールアドレス宛のフィッシングメールと同様、フィッシングサイトへ誘導する手口に加え、電話をかけるように誘導し、利用者本人と電話で話したうえ、金銭を詐取する手口が使われる事が多い。

まず、フィッシャーは有名な Web サイト運営者を装って未納料金があると偽り、指定した電話番号へ連絡を求める内容の SMS を送る。要求に従わない場合は法的措置をとる事をほのめかし、心理的な圧力をかけるケースが多い。 SMS 送信の際には、本文中で Web サイト運営者名を騙ることに加え、発信者番号をアルファベットで自由に表記できることから、国際網経由の SMS 配信を利用し、Web サイト運営者名を騙るケースがある。

次に、電話をかけてきた利用者に対して、架空の未納料金を請求し、自ら指定する方法で送金するよう要求する。フィッシャーにとっては、相手の反応にあわせ会話を工夫することで、成功率を高められる、直接金銭を詐取できるといったメリットがあるが、一般のフィッシングとは別の技術や労力を要する手法だといえる。

また SMS は携帯電話端末で受信される事と、文面に電話番号が含まれる場合、発信を容易にするためのリンクが自動で生成される機能が、ほぼ全ての機種にあり、通話へ誘導する詐欺に利用されやすいと考えられる。

[3] 「ファーミング（Pharming）」とは、フィッシング詐欺と同様に個人情報の詐取を行う詐欺行為である。犯罪者のもとへ誘導する手口にフィッシングとの違いがある。被害者へ何らかのアクションを要求することなく、犯罪者が用意したウェブサイトへ誘導するのがその特徴として挙げられる。犯罪者が「不正な転送の種（しかけ）」を撒き、被害者が正規の URL を正しく入力したとしても、否応なしに偽のウェブサイトへ転送させ、個人情報などを不正に詐取される（刈り取る）。この一連の様を「Farming（農場経営）」になぞらえ、ファーミングと呼ばれている。

SMS を利用したフィッシング詐欺の被害を抑制するためには、利用者が受信した SMS について、フィッシングの可能性が高いと判断した場合に慎重な行動ができるようにする事が必要である。

Web サイト運営者においては、フィッシングに利用される可能性が低い国内直接接続の SMS 配信を利用し、事前に発信者番号をウェブサイト等で告知する事が対策としてあげられる。

利用者においては、国際網経由の SMS についてはフィッシングの可能性を疑い慎重に行動する事が対策としてあげられる。心当たりがある場合でも、自身で調べた Web サイト運営者の正規の窓口に問い合わせるなどして、記載されている電話番号へ直接連絡するのを避けるべきである。仮に記載されている電話番号へ連絡してしまい、困惑するような要求があった場合でも、第三者に相談するなどして、拙速な判断で相手の要求に従う事のないよう注意が必要である。

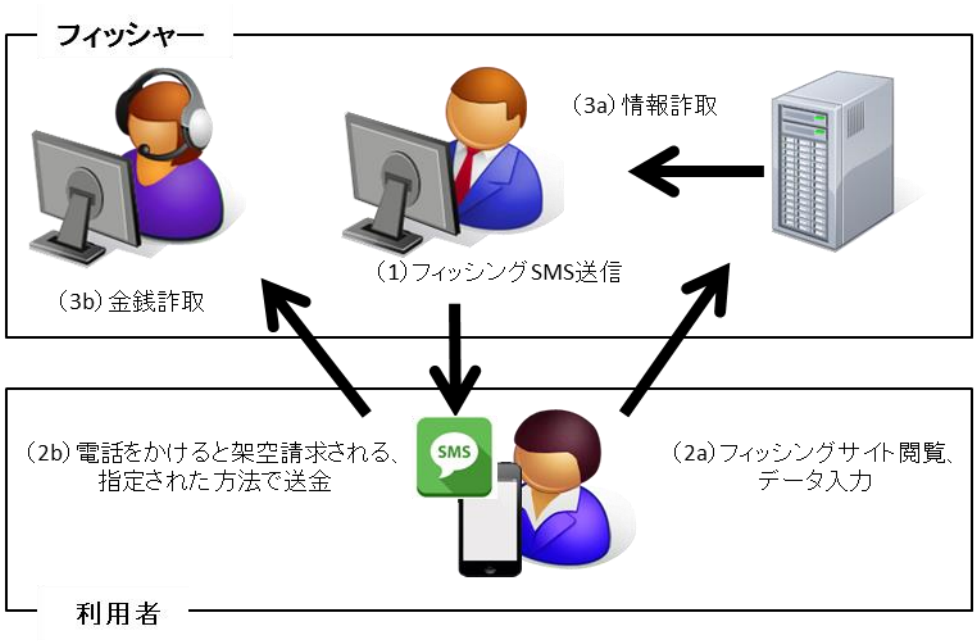


図 4 SMS を利用したフィッシング詐欺の例

	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。

図 5 SMS 配信経路ごとの特徴

3. Web サイト運営者におけるフィッシング詐欺対策

本章では、フィッシング詐欺の標的、つまり、フィッシングサイトを設置され、利用者のアカウント情報などを窃取されるリスクを負っている Web サイト運営者にとって、被害が発生する前に心がけて置くべき対策、および、被害が発生した際の対応事項について記述する。

なお、本ガイドラインで提示する対策事項では、実施必要性について以下のような優先度を設定している。

◎：実施すべきと考えられるもの

○：実施を推奨するもの

△：必要に応じて実施すべきもの

3.1. Web サイト運営者におけるフィッシング詐欺の被害とは

Web サイト運営者のフィッシング詐欺による被害を考えてみると、事業者職員がフィッシング詐欺により情報を詐取される状況を除けば、直接的な被害は利用者（登録会員）サイドで発生し、Web サイト運営者にとっては、間接的に発生する利用者の信頼喪失および利用者に対する損害補償の二点になる。

さらに、自らのサイトを模倣したフィッシングサイトの設置により、利用者に多大な被害が発生した場合、Web サイト運営者の過失が実際にあったのかどうかに関わらず、利用者の間では Web サイト運営者のサイト利用に不安が生じ、利用者離れ、ひいては利益の損失につながることになる。

相手の姿が直接見えることのないインターネットの性質上、Web サイト運営者と利用者の信頼を築くことは容易なことではない。利用者保護、信頼確保の視点を持ち、Web サイト運営者においても、十分なフィッシング詐欺対策を実施すべきであろう。

3.2. 利用者を守るためのフィッシング詐欺対策とは

利用者がフィッシング詐欺被害にあう際の事象の流れを図 6 に示す。

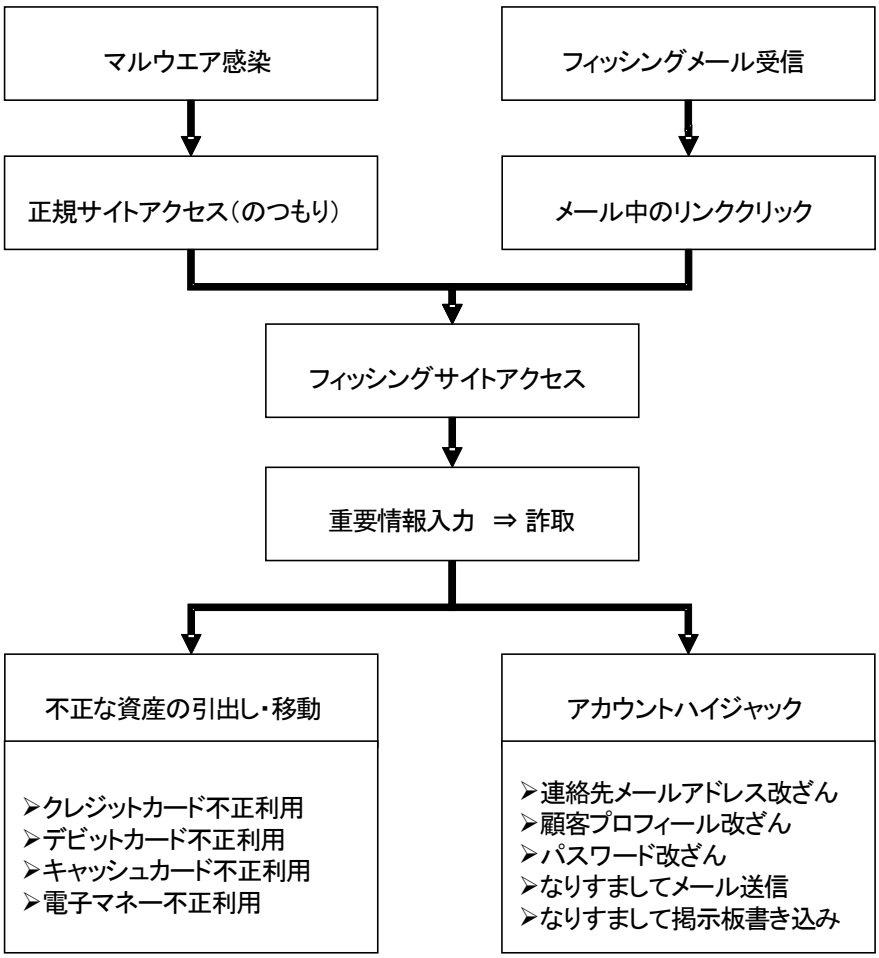


図 6 利用者サイドでのフィッシング被害発生フロー

利用者のフィッシング被害を抑制するためには、利用者自身の対策、心構えなどに付いて啓発することが最も重要であるが、Web サイト運営者サイドにおいて実施すべき対策がある。フィッシング詐欺被害の発生を抑制するための対策、フィッシング詐欺被害の発生を迅速に検知するための対策、フィッシング詐欺被害が発生してしまった際の対策などである。

以降では、この三種の対策について具体的に述べていくことにする。

3.3. フィッシング詐欺被害の発生を抑制するための対策

利用者が正規 Web サイト運営者とフィッシャーの区別を確実に行うことができれば、フィッシング被害を大きく抑制することができると考えられる。

3.3.1. 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

通常フィッシングメールは、Web サイト運営者の送信している正規メールの文面を模倣した自然な文面となっていることから、正規のメールとの見分けることが難しくなっている。

【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

電子メールでは From:に記載される差出人アドレス（通常、メーラ上に表示される差出人）は容易に詐称できるため、本当は誰が作成した文章で、誰が送信したのか確認する手段が無い。この性質がスパムメール、フィッシングメールの氾濫を招いているといえる。誰が送信したのかを確認する手段には後述の送信ドメイン認証（SPF、DKIM など）が利用でき、誰が文面を作成したのかを確認する手段として電子署名[4]が利用できる。電子署名は公開鍵暗号技術を使って文面を作成したものが誰であるのか（作成したものが署名する）を検証する手段を提供する。

一般的に使われているメールソフトウエアでは S/MIME 形式による電子署名がサポートされており、利用者の多くは特段の意識をしなくても電子署名を適切に扱うことができる（利用者を惑わせるエラーなどが表示されないという意味）と考えられるが、いまだ電子署名をサポートしていないメールソフトウエアやメールサービス（Web メール）も存在すること、Web サイト運営者から送付されたメールにおいては電子署名を必ず検証することなどについて、わかりやすい説明文書を作成し、利用者に配布することが必要である。

電子署名は利用者に送信する全てのメールに付与することが望ましい。電子署名の付与を利用者により選択できるように配慮することも考えられるが、自らの利用者層における電子署名付与による影響を評価し、妥当な範囲であれば、全てのメールへの電子署名付与を検討すべきである。なお、どの範囲に電子署名を付与しているか（全て、あるいは特定サービスのみなど）を利用者が分かるように明示する必要がある。

【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

外部送信用メールサーバは SPF、DKIM の送信ドメイン認証に対応すること。

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に対応させ、送信元を詐称したスパムメールやフィッシングメールを検出できるようにすることが必要である。SPF と DKIM、S/MIME は検知範囲が異なるため、組み合わせて補完することが望ましい。

さらにフィッシングメールの対策に SPF や DKIM の認証結果を用いた DMARC（Domain-based Message Authentication, Reporting & Conformance）を活用することも有効である。DMARC は SPF や DKIM の認証結果（または両方の認証結果）からメールの配送制御を行うフレームワークであり、認証が失敗した場合に Web サイト運営者は以下の 3 つの受信制御ポリシを選択することができる。

[4] 独）情報処理推進機構「電子メールのセキュリティ ”電子メールの安全性を高める技術の利用法”（H19 年 3 月）」等を参考にすること

1.そのまま受信させる（none）
2.隔離させる（quarantine）
3.受信を拒否する（reject）

例えば正規メールの差出人アドレスになりすましたフィッシングメールが送信された場合、SPF、または、DKIM の認証が失敗した情報から、プロバイダは指定された受信制御ポリシに従って受信を拒否（reject）することができる。フィッシングメールを利用者に届けない制御が可能となる。

また、DMARC はプロバイダ側から Web サイト運営者に詳細な認証結果のレポートを送る仕組みを有しており、フィッシングメールの発生状況の把握やなりすましメールの送信元の特定などが可能となる。

事業者は受信に影響のない、受信制御ポリシ「none」にした DMARC を設定し、なりすましメールの発生状況の把握から開始することが望ましい。加えて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。

【要件3】 ◎：利用者へのメール送信では、制作・送信に関するガイドラインを策定し、これに則って行うこと

Web サイトの模倣を防ぐことができないことと同様、メールを模倣されることを防ぐことはできないが、メール作成に関するガイドラインを策定し、これに社内・組織内が統一的に則って作成・送信することで、利用者がフィッシングメールに対して「いつもと何か違う」と気づきやすくすることができる。

ガイドラインには、差出人、件名の書き方、本文の構成や段落の使い方、表現や用語の統一、本文下部の問い合せ先や配信停止等の定型フッタ様式、配信時間帯など多岐に渡る。

【要件4】 ○：Web サイト運営者が利用者に送信するメールはテキスト形式とすること

フィッシングメールの多くは被害者に意識させずリンクを踏ませるため HTML 形式で作成されている。HTML 形式では、フィッシングサイトのリンクを無害なリンクに見せかけることが容易であり（例：無害なリンク）、古典的とは言えフィッシングメールの常套手段である。利用者に無用なリスクを負わせないためにも、Web サイト運営者が利用者に送信するメールはテキスト形式で作成することが望ましい。テキスト形式以外で作成する場合には、フィッシングメールと混同する可能性や、フィッシングメールを作成・悪用されるリスクを理解したうえで送付するべきである。

宣伝広告を目的とするメールに画像表示やボタン型リンクを用いるため HTML 形式を採用する場合には、利用者がテキスト形式か HTML 形式かを選択できるように配慮することが望ましい。

【要件5】 ◎：利用者に情報発信する手段および内容を周知すること

ユーザに周知・連絡する場合には、Web サイト運営者が利用者に対して情報発信を行うケースや手段（メール、SMS、郵送など）について示すとともに、メールや SMS では ID およびパスワードの確認を行わないことなどを明確にしておくことが重要である。

3.3.2. 利用者が正規サイトを判別可能とする対策

様々な巧妙な手法により、利用者がどれほど注意をしていてもフィッシングサイトを閲覧してしまうリスクをゼロにすることはできない。正規サイトに工夫を施すことで、利用者が閲覧しているサイトがフィッシングサイトであることに気が付くように配慮すべきである。

【要件6】 ◎：Web サイトの正当性に係る情報を十分に提供する画面とすること

利用者が正規の Web サイトであることを確認するための情報を十分に提供するためコンテンツデザインに配慮しなくてはならない。Web サイトの全てのページにおいて次の原則に準拠すること。

- ページの URL がアドレスバーに表示されていること（アドレスバーを隠さない）
- 異なるドメイン名を URL に持つページが混在しないよう frameset を使わないこと
- JavaScript、Adobe Flash など、HTML 以外の要素が利用できることを前提とした画面設計としないこと

利用者情報が詐取される前、つまりログイン前に正規サイトであることを確認できなければならないことに十分、配慮することが望ましい。

【要件7】 ◎：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必要がある。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と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上で発行されるため、組織としては高い信頼性を得ることができる。

【要件8】 ◎：正規 Web サイトのドメイン内設置サーバの安全性を確認すること

フィッシングサイトを信用させる手段として、模倣したサイトのドメイン名を調査し、管理が行き届いていないサーバを見つけて、そこのコンテンツを改ざん、または不正アクセスにより Web サービスを起動して、正規 Web サイトと同じドメイン名を持つフィッシングサイトを設置する行動が見られる。例えば、example.co.jp に test01.example.co.jp という何らかのテスト用サーバがあり、単純な ID/パスワードでログインできる状態にあったのならば、コンテンツを書き換えて、www.example.co.jp のフィッシングサイトとしてしまう。ドメイン名が同じであるため、容易に信頼してしまう利用者もいるであろう。

このような状況が発生しないように、正規 Web サイトが利用しているドメイン内に管理状況の

悪いサーバ（脆弱性の存在が報告されているソフトウエアなどが放置されている、ログの監視が行われていないなど）が設置されていないことを定期的に確認すること。

サービス提供正規サイトを含め、管理が行われているサーバにおいては、Web サーバ、メールサーバ、ネームサーバなど、サービスそれぞれの特性、利用ソフトウエアに応じた安全管理を徹底し、OS、アプリケーションなどの脆弱性対応、定期的な脆弱性検査などを綿密に行うこと。

【要件9】 ○：認証システムが許容するポリシを利用者に示すこと

Web サイト運営者は利用者がパスワードを登録または変更する際に、入力されたパスワードの強度を知らせ、システムが許容する範囲でより強固なパスワードを求まるようにする。パスワードは長さ、複雑さ、変更、禁止事項などを明確にしたパスワードポリシを定め、ポリシを下回る場合は注意を表示、または受け付けない仕組みとすること。またポリシを満たしている場合でもパスワードの強度を評価し、数値化やビジュアル化するなどして強度をリアルタイムに表示することが望ましい。パスワードの強度は、使用する文字の種類と複雑さ、パスワード全体の長さ、パスワードが辞書に記載されているかどうかなどをスコア化して評価する。

【要件10】 ○：色々なチャネルで利用者に対する脅威の状況を提供する

フィッシング詐欺被害発生、送信者を Web サイト運営者に偽装したウイルスメール、スパムメールなど、サービス提供上の脅威の状況を正規サイトに表示するなどして、利用者の状況判断を容易にすること。正規サイトの利用者に注意喚起するため、SNS やメルマガ等、様々なチャネルを利用して脅威の状況を提供できるよう工夫することが望ましい。

3.3.3. フィッシング詐欺被害を拡大させないための対策

利用者がフィッシング詐欺被害にあい、アカウント情報、個人情報を詐取されるなどの被害に遭った場合でも、詐取された情報が悪用される被害を最小限に食い止めるための対策を実施しておく必要がある。

【要件11】 ◎：利用者に端末を安全に保つよう、注意を促すこと

不正なポップアップが表示されインターネット・バンキングの情報を盗み取ろうとするフィッシング手口では、利用者の端末がマルウエアなどに感染することによって発生している。Web サイト運営者は利用者が端末の脆弱性を放置しないよう、利用者にパソコンやスマートフォン等を安全に保つよう、注意を促す必要がある。

注意項目としては次にあげる内容を含める必要がある。

- 「Windows などの OS や Web ブラウザ、アプリケーションソフトウエアは、最新の状態に保つこと」
- 「Flash や Java などのプラグインソフトウエアをアップデートし、常に最新の状態を保つこと」
- 「セキュリティ対策ソフトウエアをインストールし、機能を有効にして最新状態に保つこと」

- 「フィッシング対策に有効なツールを活用すること」
- 「発行元不明のソフトウエアはインストールしないこと」
- 「アプリやソフトウエアは公式サイトや信頼できるサイトからインストールすること」

なお、Web サイト運営者は、マルウエア対策ソフトウエアやマルウエア対策サービスを利用者に提供することを検討すると共に、提供している場合はその利用を促進するため利用者に周知する必要がある。

【要件12】 ◎：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は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。

【要件13】 ◎：資産の移動に限度額を設定すること

フィッシャーによる利用者資産の窃盗被害を抑制するため、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、移動資産の限度額を設定できるようにする。この場合、一回の操作の上限とともに、一日あたりの上限を設け、制限に達した利用者には緊急に連絡を行い、利用者自身の操作であるかどうか確認をとること。限度額を変更する場合などには複数要素認証などを活用することが望ましい。

【要件14】 ◎：資産の移動時に利用者に通知を行うこと

資産の移動が小額であっても、移動が行われるたびに、電子メールなどによる通知を行うこと。この種の通知がフィッシング被害の発生を検出する機会となることが考えられるため、携帯電話向けの通知配信を行うことが望ましい。

利用者 PC のマルウエア感染など、中間者攻撃による利用者資産の窃盗被害を抑制するためには、携帯電話に別途認証コードを送るなどの別経路を使った資産移動確認手続きを検討することが望ましい。

【要件15】 ○：利用者の通常とは異なるアクセスに対しては追加のセキュリティを要求すること

フィッシャーによる不正なログインを抑制するため、利用者の通常とは異なるログインが行われた場合には、第二認証や第三認証を求めるようにし、次の操作に進めないようにする。

複数要素認証はフィッシングによる不正なログインを抑制するためには効果的であるが、利用者の利便性は損なわれる。利用者の通常のログイン行動パタンを分析し、それと異なるログイン行動パタンを検知した場合に追加の認証手段を求めるリスクベース認証を導入することが望ましい。

通常の再ログイン時は、ID/パスワードのみで認証し、リスクベース認証機能により、通常と異なるログインを検知した場合にのみ、第二認証や第三認証を求めるようにすることで、利便性を犠牲とせずフィッシャーによる不正なログインを防ぐことが可能となる。

【要件16】 ○：登録情報を変更するページへの移動には再度認証を要求すること

フィッシャーによる利用者情報の変更、削除を抑制するため、登録情報の変更を行うページへ移動するときには、ログイン状態であっても再度認証を求めること。その際本人識別の精度を上げるため、単一の情報（パスワードのみ）ではなく、複数の情報を求めるようにすることが望ましい。

【要件17】 ○：重要情報の表示については制限を行う

ログインアカウント情報を手に入れたフィッシャーに重要情報が漏れないよう、クレジットカード番号やデビットカード番号は下 4 桁など一部だけの表示に留めることが望ましい。

【要件18】 ○：認証情報は厳格に管理すること（アカウントは不必要に発行しない）

ID・パスワードを含む認証情報は個人情報であるので厳格に管理する必要がある。またアカウントの管理運用は高いセキュリティ技術を要するため、厳密な本人確認やアカウント発行自体が必須でないサービスについては、外部の認証機構を活用することも考慮すること。

【要件19】 ◎：アクセス履歴の表示

利用者がそのサイトへの過去のアクセス履歴（複数回）を確認できるようにする。アクセス履歴には接続時刻、時間、アクセス元 IP アドレスを含むこと。

3.3.4. ドメイン名に関する配慮事項

ドメイン名は利用者が安全性を判断するために最も重要な要素である。ドメイン名は混乱のないことはもとより、フィッシャーに簡単に利用されないための対策が必要である。ドメイン名に関して Web サイト運営者の管理運営するサイトであることを明確にすることが求められる。

【要件20】 ◎：利用者の認知している Web サイト運営者名称から連想されるドメイン名とすること

Web サイト運営者は、Web サイトで用いるドメイン名および利用者に送信するメールの送信者アドレスで用いるドメイン名（送信者のメールアドレスの@から右の部分）について、誤解の無いドメイン名を使う必要がある。誤解の無いドメイン名とは、Web サイト運営者の一般呼称をそのまま使ったものを指す。

ドメイン名の種類には様々なものがあるが、"com"、"net"、"org"などの特定の国と関連しないド

メイン名[5]は、登録申請者に対する実在確認を行わないことが多いことから類似のドメイン名使用権利をフィッシャーが手に入れたり、何らかの原因でドメイン名使用権利が失効した際に他の事業者にドメイン名使用権利を奪われたりするケースがあるなど、Web サイト運営者が安定したサービスを提供する上では注意が必要である。

"co.jp"や"jp"[6]は登録にあたって日本国内に住所が必要なドメイン名である。特に"co.jp"は日本国内での法人登記が必要というルールとなっており、グローバルにも日本企業が利用するドメイン名として認知されている。

既に広く認知されているドメイン名がある場合にはそれを継続利用するのが望ましいが、Web サイト運営者が日本企業で、新たにドメイン名の登録を検討する場合、"co.jp"ドメイン名が利用者に信頼を与えうる最も望ましいドメイン名であり、先述の「Web サイト運営者の一般呼称をそのまま使った」"co.jp"ドメイン名でサービスを提供することを、まずは検討すべきである。

なお、企業名称およびサービス名称が長い場合には、適度に省略したドメイン名とすることも利用者の利便性を重んじる観点からは許される。この場合には後述する利用者へのドメイン名の十分な周知方法に従うこと。

【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

わが国では、組織名称やサービス名称は日本語の漢字や仮名で表記されることが多いが、現状ではそれらを、アルファベット、数字およびハイフンによる表現に変換してドメイン名として利用している例が多い[7]。この際、ローマ字変換する、英文呼称を設けて英語表記する、略語により表記するなど、いくつかの方法が考えられる。

いずれの方法にせよ、利用者にとっての紛らわしさを完全に払拭することは困難であることから、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。周知の手段として、利用者に対して案内や連絡などを行う際には、電子メールではなく郵便を用いること（電子メールを読まない関心を持たない利用者のため、および印象づけるため）、封筒自体にドメイン名をはっきりと示す（開封しない利用者もいるため）、フィッシング詐欺、振り込め詐欺など、サービス利用上の注意を示した利用者カードを配布し、ドメイン名をはっきり示すなどが考えられる。機会があれば、新聞、テレビ（CM）などでサービスのキャンペーンを行うことが効果的と思われる。また、サーバ証明書を利用することで、ドメイン名の正当性を示すことも重要である。

なお、一度、サービスを開始したドメイン名については、特別の理由が無い限りは変更しないようにすること。

利用者の混乱を避けるため、Web サイトのドメイン名と、利用者に送信する電子メールアドレスのドメイン名は共通とすること。例えば、Web サイトが www.example.co.jp であれば、電子メールアドレスは customer-support@example.co.jp とする（下線部分を同じとする）。また、Web サイトが netbanking.example.co.jp など、特定のサービス名称を含んでいる場合、電子メールアド

[5] 特定の国に関連しないドメイン名を gTLD（generic Top Level Domain）と呼ぶ。対して.jp のように国ごとに割り当てられたドメイン名を ccTLD（country code Top Level Domain）と呼ぶ。
[6] JP ドメイン名の種類と対象：https://jprs.jp/about/jp-dom/spec/
[7] ドメイン名には日本語などを使用することも可能となっており（国際化ドメイン名）利用も始まってはいるものの、まだ十分に普及している状況とは言えない。（https://www.nic.ad.jp/ja/dom/idn.html）

レスは support@netbanking.example.co.jp とすることも考えられる。また、一般的な役割をもつメールアドレス名については、RFC2142[8]に準拠すること。

【要件22】 ◎：ドメイン名の登録、利用、廃止にあたっては、自社のブランドとして認識して管理すること

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。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ドメイン名が発生してしまうリスクが高くなる。

ドメイン名管理サービスからは、登録中のドメイン名に関して、ドメイン名の移転、更新／廃止、レジストラ変更など、ドメイン名の登録者の意向を確認するための重要な連絡が来ることがある。企業はドメイン名の登録者として、その連絡を正しく受け取ることができるように、届け出ている連絡先情報を常に最新に保ち、登録しているドメイン名に関する連絡があった場合には、必ず内容を確認し、適切な対応を行うことが必要である。

利用を終えたドメイン名についても、ドメイン名の廃止には慎重な検討が必要である。廃止されたドメイン名は一定期間後に第三者による登録が可能となるため、悪意ある第三者が当該ドメイン名を新たに登録してフィッシングサイトを運営するリスクがある。利用終了後もすぐには廃止せず、数年単位でのクールダウンタイムを確保するなどの対策が考えられる。

なお、新たなドメイン名を登録するのではなく、サブドメイン名やサブディレクトリなどを活用することも考えられるが、この場合、URL 全体が長くなることで利用者の利便性・視認性を下げてしまうことにもなる。個別の事例ごとにメリット・デメリットを検討し、判断することが必要である。

以上のようなことを組織のポリシーとして定め、共有することが重要である。

【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

企画・運営と情報セキュリティの技術的内容の分かる人材を含めたメンバによる体制構築が望まれる一方、広報、コールセンターなど関係部門との連携も重要である。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。

【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

サービス提供に際しては、フィッシング詐欺被害あるいはフィッシングサイト出現の報告窓口を設けておく必要がある。サービス提供 Web サイトおよび、Web サイト運営者のコーポレート Web サイトなどに、フィッシング詐欺を含めた問い合わせ窓口情報をわかりやすく記載すること。

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

[8] RFC2142 "MAILBOX NAMES FOR COMMON SERVICES, ROLES AND FUNCTIONS"

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。

【要件25】 ◎：フィッシング詐欺発生時の行動計画を策定すること

フィッシング詐欺発生時の行動計画を策定する必要がある。策定すべき行動計画の例を示す。

- 不正操作、不正取引の被害があった場合
- フィッシングサイトの報告があった場合、あるいは発見した場合
- 報道発表を行う準備も整えておく、事象発生前に発表文面のテンプレートなどを用意し、そのレベルで事前に関係者・役員などに了解を得ておくなどして速やかに発表できる仕組みにしておくことが望ましい。

【要件26】 ◎：フィッシング詐欺および対策に関わる最新の情報を収集すること

情報サイトのセキュリティコーナーやウイルス情報のサイトを確認する。

情報サイトを付録 C に示す。

【要件27】 ◎：フィッシングサイト閉鎖体制の整備をしておくこと

フィッシングサイトの閉鎖は、自社にて対応することもできるが、通常フィッシングサイトは海外にホストされているケースが多く、自社に専門スタッフや専門部署が無い場合には専門業者などへの対応要請が推奨される。あわせて「フィッシング対策協議会」に相談すること。なお、届出窓口を設置し、早期に認知できるような体制を構築することが望ましい。

【要件28】 ○：フィッシングサイトアクセスブロック体制の整備をしておくこと

利用者がフィッシングサイトへアクセスし個人識別情報などを入力しないように、アクセスを防止あるいは抑止する措置をとるようセキュリティソフトウエアや Web ブラウザのベンダに要請できるように準備しておく。

フィッシングサイトを発見した場合は、セキュリティベンダ等の窓口に報告する。各セキュリティソフトウエア／Web ブラウザベンダの Web サイトなどにその報告の方法が掲載されている。文書による協力要請を行う場合には事前に要請書のテンプレートを作成しておくことが望ましい。

3.3.5. 利用者への啓発活動

フィッシングに留まらず、セキュリティの脅威全般についての注意喚起を行う。また、顧客対応窓口を告知し、事件が発生した場合の対処をスムーズに行えるようにする。

【要件29】 ◎：利用者が実施すべきフィッシング詐欺対策啓発活動を行うこと

利用者への啓発資料（コンテンツ）を作成する際にはその作成者は「利用者向けフィッシング詐欺対策ガイドライン」や付録 C.4「安全な Web サイト利用の鉄則」などを参考に作成することが望ましい。また啓発資料の作成に当たっては、一般の利用者が理解できる内容にすると同時に、内容の正確性確保のため技術的内容が分かるメンバも企画の最初の段階から参画する必要がある。

【要件30】 ◎：フィッシング詐欺発生時の利用者との通信手段を整備しておくこと

フィッシング詐欺が発生した時点では速やかに利用者への連絡を行わなければならない。通信手段としては、電話（SMS 含む）、電子メール、郵便、マスメディアなどが考えられる。過去に発生したインターネット上のインシデントの例を見ると、被害状況の把握までに一定の時間を要している。フィッシング詐欺においても、フィッシングメールがどれだけ流通しているのか、利用者の何割がフィッシングメールを受け取ったのか、すでに被害を受けた利用者はどれだけいるのかなど、被害発生を認識した時点で把握することは難しいと思われるため、被害の拡大を抑制するためには、可能な手段を全て使って利用者に被害発生を通知すべきと考えられる。

利用者登録時には、緊急通知用[9]の電子メールアドレス、携帯電話番号を登録してもらうこと、金融サービスなど、深刻な被害が想定される Web サイト運営者においては、電話番号、住所も合わせて把握しておくこと。更にマスメディアを活用した通知手段を整備しておくことが望ましい。

3.4. フィッシング詐欺被害の発生を迅速に検知するための対策

フィッシング詐欺が発生した際に利用者の被害を最小限に抑えるためには、発生から発見までのタイムラグを短くすることが重要である。

【要件31】 ○：Web サイトに対する不審なアクセスを監視すること

サーバやファイアーウォールなどのログなどを監視し、例えばログインの失敗が多発するなど不振なアクセスを監視し、兆候を早めにキャッチすれば、早期に適切な対処を行える体制をとることが可能になる。

【要件32】 △：フィッシング詐欺検出サービスを活用すること

フィッシング詐欺発生について、利用者からの問い合わせ、第三者の連絡などで発見される事例もあるが、インターネット上の不正活動を 24 時間体制でモニタリングする商業サービスが存在するため、これらのサービスを活用して、迅速に被害発生を検出することが望ましい。

【要件33】 △：端末の安全性を確認すること

スマートフォンでサービスを提供している場合、端末の安全性を確認することが望ましい。例えば、デバイスのルート化（ジェイルブレイク）を検知し、必要な場合はサービスへのアクセスを禁止することが望ましい。

【要件34】 △：バウンスメールを監視すること

フィッシャーが送信元を偽装したメールを存在しないアドレスに送信した場合、受信先のメールサーバで配信不能となったメールがバウンスメールとして偽装に使われた正規の送信者に差し戻されることがある。バウンスメールを監視し、フィッシングの兆候を検出することが望ましい。

[9] 通常連絡用アドレスでも良いが件名を工夫して緊急通知であることがわかるようにすること。

3.5. フィッシング詐欺被害が発生してしまった際の対策

Web サイト運営者のフィッシングサイトが設置された場合、Web サイト運営者の利用者にフィッシング詐欺の被害が発生した場合には迅速に対応活動を実施することが必要である。この対応活動は一種のインシデントハンドリング活動であるが、フィッシング詐欺被害特有の対応活動がある、それは、被害の拡大を防ぐため、フィッシングサイトのテイクダウン（閉鎖活動）[10]を行うことにある。

フィッシングサイトのテイクダウンは一般的に難しいとされる。フィッシングサイトは犯人を突き止める足がかりとならないよう第三者が運営する既存のサーバに対する不正アクセスにより設置されることが多く、Web サイト運営者が直接の交渉を行う上で、いくつかの障害がある。まず、フィッシングサイトの保有組織が判明した場合において、Web サイト運営者からは保有組織がフィッシャーであるのか、第三者であるのか、の判別が難しいことがある。

フィッシング詐欺被害の発見から対応、事後対応までのフローを示す。

（1） フィッシング詐欺被害の発見

（2） フィッシング詐欺被害状況の把握

（3） フィッシング詐欺被害対応の活動

- フィッシングサイトテイクダウン活動
- フィッシングメールに対する注意勧告
- 関係機関への連絡、報道発表

（4） 生じたフィッシング詐欺被害の回復措置

（5） 事後対応

以降では各ステップの詳細を記述する。

[10] 情報セキュリティの文脈においては、フィッシングサイトを閉鎖することを「サイトのテイクダウン」あるいは単に「テイクダウン」と表現する。

フィッシング詐欺被害対応フロー

(1) フィッシング詐欺被害の発見

□発見状況、通知内容の記録（担当者：　　）
□緊急連絡網の把握
□対応役割の把握

(2) フィッシング詐欺被害状況の把握

・フィッシングサイトを調査し、実際に被害が出る危険性はどれぐらいなのかを判断する。
□調査・判断（担当者：　　）
　□調査内容、フィッシング詐欺判断の内容記録
　□フィッシング詐欺発生の確定、関係者への連絡（第一次連絡先：　　）

(3) フィッシング詐欺被害対策活動

・フィッシングサイトテイクダウン活動
□IPアドレスブロックを管理しているISPへの依頼（連絡先：　　）
□専門機関へのテイクダウン依頼
　□JPCERT/CCへの依頼（連絡先：http://www.jpcert.or.jp/form/ ）
　□フィッシング対策協議会への連絡（連絡先：info@antiphishing.jp ）
　□フィッシング詐欺被害対策サービス事業者への依頼（連絡先：　　）
　□サービス事業者テイクダウン依頼受付時間（　　時　　分　～　　時　　分　土日祝日対応：有　無　）
・フィッシングメールに対する注意勧告
□顧客からの問い合わせ窓口設置（担当者：　　）
□基本的な質問事項、応答事項の準備（担当者：　　）
□顧客への通知
　□フィッシングメール、フィッシングサイトの特徴情報まとめ（担当者：　　）
　□正規サイトでの注意喚起掲示（担当者：　　）
　□注意喚起通知メール配信（担当者：　　）
　□報道機関等各種メディアへの告知等（担当者：　　）
・関係機関への連絡、報道発表（顧客の被害が発生している場合）
□都道府県警察のサイバー犯罪相談窓口への連絡（連絡先：　　）
□その他関係機関への報告（連絡先：　　）
□報道機関等各種メディアへの告知等（連絡先：　　）

(4) 生じたフィッシング詐欺被害への対応

・詐欺被害（金銭的被害、ID詐取等）発生状況の把握（連絡先：　　）
□クレジットカード番号、オンラインバンキングアカウントの詐取等の状況把握
□金銭的被害の状況把握
□被害拡大抑制の活動実施

(5) 事後対応

・事後処理含め、改善、再発防止策などを体制や対応手順書などに反映する。

3.5.1. フィッシング詐欺被害状況の把握

フィッシングサイトとフィッシングメールはセットと考え、どちらかだけの報告、発見であっても、双方の状況を確認する必要がある。流通範囲の広さから、通常はフィッシングメールの発見がフィッシング詐欺被害の発見の機会となるであろう。この場合には、メールの中にフィッシングサイトのリンクが含まれているので、フィッシングサイトの発見はただちに行うことができる。

フィッシングサイトを調査し、実際に被害が出る危険性はどれくらいなのかを判断する。やはり、見た目の類似性が一つの判断基準となるだろう。フィッシングメールにおいては、「3.3.1」で示した Web サイト運営者が利用する定型様式との類似性、定型様式を認知していない利用者に対する信憑性の高さなどから危険性を判断する。

加えて、フィッシングメールの流通量を把握する必要があるが、この作業には時間を要することと、作業自体が難しいことから、「3.5.4」で示す関係機関への連絡の際に合わせて事態把握に協力を求めることとして、被害対応作業に進むべきであろう。

3.5.2. フィッシングサイトテイクダウン活動

（1）Web サイト運営者自身でテイクダウンを行う

フィッシングサイトのテイクダウンを Web サイト運営者自らが行う場合には、フィッシングサイトの管理者に直接連絡をとるのではなく、フィッシングサイトが属している IP アドレスブロックを管理している ISP に連絡をとることが望ましい。なぜなら、フィッシャーが第三者の Web サーバに不正アクセスをしてフィッシングサイトを設置している場合もあり、フィッシングサイトの管理者に連絡を直接行っても、相手からは第三者から突然の連絡を受けたことになるので、場合によっては難しい交渉になってしまうことが考えられるためである。

ISP が国内の事業者であれば、迅速な対応のため、電話にて対応依頼を行うことが望ましいが、海外の事業者の場合には、時差の問題があることから電話ではなく、電子メールにて連絡することも考えるべきであろう。その場合の例文を付録 D として示しておく。

テイクダウン要請を Web サイト運営者自ら行う場合でも、並行して JPCERT コーディネーションセンター（以下、JPCERT/CC）、フィッシング対策協議会、更に海外の ISP であれば現地の CSIRT に支援要請を行うことが望ましい。多くの ISP はインシデント対応機関とのチャネルを持っており、Web サイト運営者からの連絡よりもインシデント対応機関からの連絡の方がスムーズに受入れられることが理由である。

（2）専門機関にテイクダウン依頼を行う

国内においては JPCERT/CC にてフィッシングサイトのテイクダウン依頼を受け付けている。支援要請の際には、「インシデント報告の届け出[11]」を参照し、電子メールの件名に『サイト停止希望』と明記した上で、フィッシングサイトの URL 情報（必須）、確認した日時・場所などをインシデン

[11] https://www.jpcert.or.jp/form/

ト届け出様式[12]に記載して送信する。また、すでにWebサイト運営者自身でフィッシングサイトが属しているIPアドレスブロックを管理するISPや、警察などに連絡を行っている場合には、連絡日時と連絡先、連絡内容などもインシデント届け出様式に記載するとよいだろう。

(3) フィッシング詐欺被害対応サービス事業者にテイクダウン依頼をする

フィッシング詐欺被害の備えとしてフィッシング詐欺被害対応サービス事業者と契約を持っておくことも検討すべきであろう。このような契約を行っている場合には、その事業者にテイクダウン依頼を行う。

事業者を選定するポイントとして、テイクダウン依頼受付時間が24時間365日であること、どのような地域にフィッシングサイトが設置されていても対応してくれること、機密保持に関する体制が検証されていること（定期的に監査を受けていることが望ましい）、フィッシングサイト監視サービスを提供していること、などが考えられる。

3.5.3. フィッシングメール注意勧告

フィッシング詐欺被害の発生をWebサイト運営者が認識するきっかけとして、フィッシングメールを受け取った、あるいはフィッシングサイトの設置を発見した利用者からの問い合わせ、Webサイト運営者自身による発見、第三者による問い合わせなどが考えられる。

Webサイト運営者のフィッシングサイトが設置され、大量にフィッシングメールが配送された場合、利用者から不審なフィッシングメールに関する多数の問い合わせが殺到し、緊急対応を迫られる場合がある。利用者を守るために偽サイトの存在を速やか、かつ、適切に伝達することも必要である。ここではそれらについて記載する。

(1) 利用者からの問い合わせ対応窓口の準備

すでに利用者からの問い合わせ窓口などが設置されている場合には、直接利用者と接する担当員に対応方法・手順などを周知徹底しておく。「フィッシングとは何か」「コンピュータウイルスではないのか」「今後はどうしたら良いのか」といった基本的な質問事項、応答事項については事前に作成するなどの準備をしておくとよい。

利用者からの問い合わせ窓口が設置されていない場合は、早急に設置し、窓口の存在、アクセス方法を利用者に周知すること。

(2) 利用者への通知を行う

フィッシングサイトの出現を確認次第、被害発生、拡大を防ぐため、フィッシングサイトのテイクダウン作業を開始すると同時に、利用者に対してフィッシング詐欺被害の発生と対処事項について早急に通知しなくてはならない。

まず、フィッシングサイトにアクセスしないように注意を促す必要がある。この場合、広く利用者へ連絡するためには、電子メールによる通知に加え、正規サイトでの掲示、報道機関など各種メディアへの告知など、複数の伝達経路を用いること。被害の深刻度、例えばクレジットカード番号

[12] https://www.jpcert.or.jp/form/form_v4.01p.txt

の詐取による不正利用が疑われる時などは、電話、郵便などの利用も考慮すべきである。

利用者に対して送付する電子メールや、正規サイトに掲載する情報の内容としては、告知文以外にも、対応窓口などを併記し、すでに被害にあってしまった利用者が相談できる窓口・情報も記載しておくことが重要である。

3.5.4. 関係機関への連絡、報道発表

すでに利用者の被害が発生している場合など、必要に応じて、警察に届け出を行う。この場合、Web サイト運営者からの連絡は、Web サイト運営者の所管の都道府県警察のサイバー犯罪相談窓口に対して行うこと。この窓口への連絡方法は前もって調べておくこと

利用者に提供しているサービスの種別によっては所管官庁への報告が必要な場合があるので、報告窓口へのアクセス方法を前もって調べて置くこと。

また、被害の拡大が予測される状況であれば、利用者に対する迅速な注意喚起として報道発表を利用することが考えられる。ただし、報道する情報によっては、類似の方法による他サイトのフィッシング詐欺、便乗詐欺などかえって被害を拡大させてしまうリスクもあるため、報道発表をどのタイミングで、どのような内容で行うのかについて、慎重な対応が求められる。

3.5.5. 生じたフィッシング詐欺被害への対応

報告窓口に寄せられる利用者からの被害報告、およびフィッシングメール報告を情報として、詐欺被害（金銭的被害、ID の詐取など）の発生状況を把握する。クレジットカード番号、オンラインバンキングアカウントの詐取など、金銭的被害の発生する危険性があれば、被害拡大抑制のための活動を実施すること。

3.5.6. 事後対応

フィッシング詐欺被害対応から学んだこと、改善すべき点、などの事後処理含め、改善、再発防止策などを体制や対応手順書などに反映する。

4. 利用者におけるフィッシング詐欺対策

フィッシング詐欺対策において、利用者の負う役割は、Web サイト運営者よりも大きなものである。フィッシング詐欺の特異な構造として、Web サイト運営者はコンテンツを複製されるだけで、詐欺行為自体にはほとんど関与しない（できない）ことがある。つまり、フィッシャーと被害者となる利用者だけで構成されるため、被害の抑制は利用者自身にかかってくる。

脅威：フィッシングメール中のリンクを正規リンクと間違える

脅威：フィッシングサイトを正規サイトと間違える（サイトに記載されている虚偽の情報を信用する）

脅威：フィッシングサイトの情報入力ページを正規ページと間違える（サイトを信用して個人情報などを入力してしまう）

なお、フィッシング対策協議会は利用者向けのガイドラインとして「利用者向けフィッシング詐欺対策ガイドライン」および「インターネットバンキングの不正送金被害にあわないためのガイドライン」を作成している。利用者への普及啓発に際しては併せて参照することが望ましい。

4.1. フィッシング詐欺への備え

常日頃からの心がけとして、フィッシング対策協議会では「被害にあわないための 5 ヶ条」を定義して公開している。

① パソコンやモバイル端末は、安全に保ちましょう。

② 不審なメールに注意しましょう。

③ 電子メールにあるリンクはクリックしないようにしましょう。

④ 不審なメールやサイトは報告しましょう。

⑤ 銀行やクレジットカード会社の連絡先リストを作りましょう。

中でも、①～③が重要である。基本的には、この三項目であるが、フィッシングの手口は益々巧妙となり「不審なメール」であることを判定することは容易ではなく、企業からの主な連絡手段が電子メールとなっていることから「電子メールのリンク」をクリックせざるを得ない場合もあり、脅威は次々に現れることから「パソコンやスマートフォン等を安全に保つ」ことも容易ではない。

また、メールだけでなく SMS によるフィッシング詐欺にも注意が必要である。

ここでは、これらの三項目を遵守するため、具体的にどうしたら良いのかについて、一定の方針を示すものとする。

4.1.1. パソコンやモバイル端末は、安全に保つ

パソコンやモバイル端末を安全に保つためには、最新のソフトウエアを利用するだけではなく、スパイウエア、ボットなど、情報を盗み出すマルウエアの侵入を防ぐための対策を考慮することが必要である。また、フィッシング詐欺の手法は進化を続けていることから、利用者の心がけだけでは完全に対処することは難しい。ここでは、フィッシング対策を徹底するために有益なツールおよび、その有効な使い方について紹介する。

【要件35】 ◎：ソフトウエアは信頼できるサイトからインストールする

偽アプリケーションなどをインストールすることで端末内の重要情報を不正に窃取されるなどの危険性がある。特にスマートフォンの場合はメーカーやキャリアが提供する信頼できるサイトからインストールする。

【要件36】 ◎：最新のソフトウエアを利用する

パソコンやスマートフォン等にセキュリティ上の脆弱性があると、利用者が気づくことなくマルウエアへの感染や脆弱性を利用した攻撃を受けることになる。最新の OS やアプリケーションには自動的に最新のセキュリティパッチを適用する機能が備えられていることが多いので、できるだけその機能を有効にするとともに、サポートの切れた OS は使わないなどにより、最新のソフトウエアを利用することが重要である。

【要件37】 ◎：セキュリティ対策ソフトウエアの機能を理解し適切に用いる

セキュリティ対策ソフトウエアは自動更新を行い、常に最新のエンジンおよびパタンファイルを利用すること。また、セキュリティ対策ソフトウエアを過信しないこと。

また、Web サイト運営者がセキュリティ対策ソフトウエアを提供している場合は、その利用を検討すること。

【要件38】 ○：端末の利用には一般ユーザアカウントを利用する

コンピュータのログオン時には、システム管理者アカウントを使わず、一般ユーザアカウントを利用すること。

【要件39】 ○：URL フィルタリングを活用すること

統合型セキュリティ対策ソフトウエアや URL フィルタリングソフトウエアにはフィッシングサイトへのアクセスを遮断する機能があるので、これを活用することで被害を避けることができる。

利用に関しては、フィルタリングソフトウエアのフィッシング対策機能が有効となっている事を確認する。また、ソフトウエアによっては「判定レベルの設定」がある為適切に選択する事を勧める。

4.1.2. 不審なメールに注意する

メールでID/パスワード、銀行口座番号、クレジット番号の再確認など、直接、個人情報を問い合わせるメールは怪しいものとされている。

【要件40】 ◎：個人情報の入力を求めるメールを信用しない

- 貴方のアカウントは再認証が必要です、パスワードの入力をお願いします
- 貴方のアカウントに怪しい操作が行われました、確認して下さい
- 特別なプレゼントが貴方を待っています、サイトにログインしてお確かめ下さい

これらの表題およびメッセージにより、フィッシングサイトへのログインを行わせ、ID/パスワードを詐取しようとするものである。

【要件41】 ◎：メールに記載される差出人名称は信用しない

このところ見られる攻撃の一つは標的型攻撃（Targeted Attack）と呼ばれている。前述のフィッシングメールは大多数にばら撒いて、一定数の犠牲者が現れれば、投資が回収できるという戦略で作られたものであるが、より効率的かつ大規模な被害を起こすため、特定の利用者向けに文面を編集した以下のようなメールを、特定組織に集中して送信する攻撃である。

> **○△□株式会社の皆さまへ**
>
> **こちらは○○トラベル、○△□様担当××です。**
> **ただいま、特別キャンペーンとして貴社の皆さまだけに、沖縄ツアーを特別料金で御提供しております。いますぐ、以下のリンクをクリックして特設サイトで御応募下さい。**
>
> http://www.△△.jp/○△□/special.html
>
> ―
> **○○トラベル○△□様担当××より**

これまで、スパムメール、フィッシングメールは機械的にばら撒かれ、このように特定組織の名称が文面に記載されることは無かったので、知識のある利用者は、知識が逆効果となって、犠牲者となってしまうことがある。

更には、特定ドメイン名のメールアドレスを収集し、実在の内部アカウントを偽装してフィッシングメールを送信する目標型攻撃の事例も報告されている。会社の総務部門のアカウントになり済まし、文面に該当アカウントの氏名までも記載されていたら、少々、怪しい内容であっても「まさかフィッシングメールでは無いだろう」と考えてしまっても不思議ではない。

【要件42】 ◎：怪しいメールの判断基準を知る

どうしたら怪しいメールを判別できるのだろうか。それには一定の判断基準と冷静な対応が必要

である。

- 自分と取引のある事業者か
- いつも受け取る内容と比較して、書式や言い回し・トーンなどに違いや違和感はないか
- メールの内容が、「緊急」「重要」「セキュリティ」などを強調し、該当事業者の Web ページにログインする情報の確認や入力を求めていないか
- メール文中にある Web サイトへのリンク先 URL に見覚えがない
- 電子署名が付与されていない
- 送信ドメイン認証が施されていない（送信企業、組織が送信ドメイン認証を導入している場合）

差出人が誰であろうと、誰宛てと書かれていようと、「何をさせようとしているのか」だけに着目して、上記のような怪しい特徴を判別しようと心がけることである。

送信者に確認をとり、確認がとれないリンクはクリックしないことが重要である。

【要件43】 ◎：安全なメールサーバを活用したり、類似性評価によるフィッシングメール判別機能を活用すること

さまざまな事業者が提供しているメールサービスの中には、アドレス詐称されたメールを自動的に迷惑メールに分類するような機能をもったサービスもある。このようなサービスを利用することで、怪しいメールの相当部分について機械的に判断することが可能になる。ただし、完全な技術ではないため、振り分けに失敗することもあるため 100%信用することはできない。加えて、機密性の高い情報をメールで扱う場合にはこのようなサービスを用いない方が良いことがある。

また、スパムメールを判別して特別なフォルダに配送するメールフィルタは、多くの主要なメールソフトウエアおよびセキュリティ対策ソフトウエアに実装されている。単純なフィッシングメールの多くはスパムメールとしても判別できるため、メールソフトウエアおよびセキュリティ対策ソフトウエアでスパムメール判別機能を有効にすることは、欠くことのできない対策といえる。スパムメール判別機能には、ベイズ理論を応用して文面から判別するもの、スパムメールデータベースとの類似性により判別するもの、送信者、送信元サーバアドレスなどのブラックリストにより判別するものなどが広く使われている。

しかし、フィッシングメールは、Web サイト運営者が実際に利用者に送信しているメールを模倣している場合があるため、ベイズ理論によるスパムフィルタはフィッシングメールの判別に特別有効とはいえない。ばらまき型のフィッシングメールの場合には、セキュリティベンダなどでも同時期にメールを捕獲しているため、スパムメールデータベースとの類似性により判別する方式が有効である。

問題は標的型フィッシングメールである。文面は標的組織で使われている文面を模倣しているためベイズ理論によるフィルタは効力が薄く、限定された組織だけに配送されるためスパムデータベースにも登録されていない。もし、他の組織も標的としているフィッシャーであれば、送信者、送信元サーバアドレスがブラックリストに登録されている場合も考えられるが、スパムフィルタの技術を熟知しているフィッシャーであれば、それらのデータを標的ごとに使い分けるような対策をと

っているだろう。このように標的型フィッシングメールに対抗するには、ツールに頼るのではなく、メールが求めている行為（メール中のリンクをクリックするなど）の怪しさを自ら判別することに尽きる。

【要件44】 ◎：リンクにアクセスする前に正規メールかどうか確認する

フィッシング詐欺メールか正規メールかによらず、メール本文中に URL が記載されている場合が多い。その場合、その URL にアクセスする前に、正規メールかどうかを十分に確認する必要がある。

4.1.3. 電子メールにあるリンクはクリックしないようにする

フィッシングメールは図 7 に示すように HTML 形式で送られてくるケースが多い。この例では、HTML フォームをメール本文中に記述し、フィシングサイトに誘導せずに口座番号、暗証番号を詐取しようとしている。

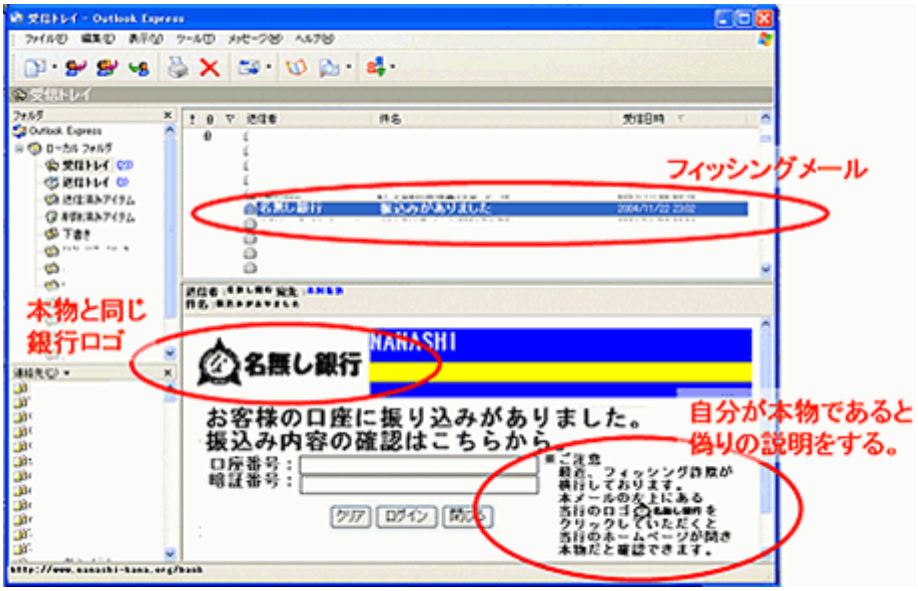


図 7 HTML 形式のフィッシングメールの例

もちろんテキスト形式のフィッシングメールも存在するので、形式だけの問題ではないが、HTML 形式の場合にはリンクをフィッシングサイトでは無いように偽装できるため、テキスト形式よりも注意が必要になってくる。

【要件45】 ◎：正しい URL を確認する

オンラインサービス初回利用時にはその URL を利用者カード/請求書などで確認し、直接入力することが望ましい。なお、初回利用時にブラウザのブックマークに登録などすることで、以後入力を省くことが可能である。

【要件46】 ◎：電子メール本文中のリンクには原則としてアクセスしない

フィッシングメールの手口は本文中のフィッシングサイトへのリンクをクリックさせることなので、フィッシングメールであろうと無かろうと、電子メール本文中のリンクをクリックしない慣習とすることが望ましい。しかし、電子メールにリンクを記述することは一般的に行われており、現実問題として、全てのメールにおいてリンクにアクセスしないということはできないだろう。

このため、電子メール本文中のリンクにアクセスする際には、次にあげる条件を全て満たしていることを確認すること。

- 電子メールをテキスト形式で閲覧していること
- アクセスする先の URL は https:// で始まっていること
- アクセスする先の URL が既知の正規サイトのものであること

HTML 形式の電子メールを閲覧する場合、リンクにはアドレス自体が表示される訳ではないので、安易にクリックすると予想外のサイトにアクセス、あるいは予想外のコンテンツにアクセスしてしまうことが考えられる。Web ブラウザの多くは実際のアクセス先リンクを Web ブラウザ上に表示する機能を持っているので、偽装したリンクを見破ることができる。しかし、メーラで HTML 形式の電子メールを表示している場合に、そのような実際のアクセス先を確認する機能が提供されていないものがあることから、リンクを直接クリックして閲覧するのではなく、コピー&ペーストして、実態としてのリンク先を確認することが必要である。

URL スキーマにはさまざまなものが定義されているが、電子メールで送られるリンクとして https://以外のスキーマを指定することは一般的とは言いがたく、既知の問題も報告されているため、そのような不審なスキーマが現れた時には、その段階で操作を停止し、ブラウザのアドレスバーから削除、閲覧していた電子メールについても、破棄する、あるいは注意が必要というマークをつけるなどの対策を実施することが望ましい。

【要件47】 ◎：正しい URL と錠前マークを確認する

Web サイトにアクセスした際に、ブラウザ上で錠前マークが表示されていれば、その通信は適切に暗号化されているため、特にパスワードなどの入力の前には

①ドメイン名が正しいかどうか

②Web サイトを運営している組織の表示

③鍵前マークをクリックして証明書の内容を確認

の 3 点を確認することが望ましい。

URL のドメイン名については、1 文字だけ違わせた類似ドメインを使い、錠前マークが表示されたフィッシングサイトが確認されており、注意深く確認する必要がある。両者を確認出来た場合にのみ入力を行うことが必要である。

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上で発行されるため、組織としては高い信頼

性を得ることができる。また、サーバ証明書の種類は Check website security のサイト[13]で確認することができる。

【要件48】 ○：Web サイト運営者からの通知メール形式をテキスト形式に設定する

Web サイト運営者への利用者登録時に通知メール形式を選択できる場合には HTML 形式ではなく、テキスト形式を選択すること。HTML 形式のみが提供されている場合には、本章で示す要件に従って、フィッシング詐欺被害のリスクを低減することが望ましい。

4.1.4. アカウント情報の管理

フィッシング詐欺で詐取されるものは、口座番号、クレジットカード番号など、直接、金銭的被害に結びつくものと、Web サイト運営者サイトのアカウント ID/パスワードなどのアカウント情報に大別される。ここでは、フィッシング詐欺被害に備えたアカウント情報管理について示す。

【要件49】 ◎：アカウント ID/パスワードは Web サイト別に設定する

複数の Web サイトで同じアカウント ID/パスワードを使い回していると、フィッシング詐欺で認証情報が詐取されたときに、アカウント ID/パスワードを使い回していた全ての Web サイトのサービスで悪用される危険がある。

少なくともパスワードは Web サイトごとに異なるものを設定することが必要であるが、多くの Web サイトのサービスを利用する場合、多くのパスワードを適切に管理することが課題となる。

アカウント ID とパスワードの組を管理する仕組みとしては、PC やスマートフォン上のアプリケーションや、クラウドサービス、ブラウザでの記憶機能（オートログイン）などがある。

これらを利用するにあたっては、自身の情報の安全性がその機能やサービス自体のセキュリティや、それらの利用環境である PC やスマホのセキュリティなどに依存するということを理解した上で、選択・利用することが大切である。

【要件50】 ◎：全てのアカウントについて緊急連絡先を把握しておくこと

後述するように、フィッシング詐欺被害の疑いを持った際に、どの Web サイト運営者のアカウント情報が詐取されたのか、はっきりしない場合には、全てのアカウントを一次停止することが望ましい。その場合、自分が利用者登録している Web サイト運営者のそれぞれの連絡先を調べている時間的余裕が無いことも考えられる。

Web サイト運営者に利用者登録を行った際には、「登録完了通知」などの名目で電子メールが送られてくることが多い。このメールには、利用者窓口の連絡先が記載されていることが多いので、これらのメールを整理しておくと緊急時の連絡に便利である。

[13] https://ssltools.digicert.com/checker/views/checkInstallation.jsp

4.2. フィッシング詐欺に遭ってしまった時

利用者がフィッシング詐欺被害を受けたことに気が付くタイミングとして考えられる状況は、正規サイトに機密情報を入力した際に不審な挙動が観られた（期待した手続き画面に進まなかったなど)、正規サイトにID/パスワードを入力したがエラーとなってログインできなかった（フィッシャーにパスワードを変更されていた)、クレジットカードの利用明細あるいは金融機関の通帳などに覚えのない取引が記載されていた（口座番号、暗証番号などが詐取されていた)、オンラインゲームのキャラクタステータスが記憶に無い状況になっている（フィッシャーがアイテムを売買してしまった）などのケースが考えられる。

このような不審な現象が起きた場合には、被害を最小限に抑え、二次被害を防止するために、以下に示す緊急対応を行うこと。

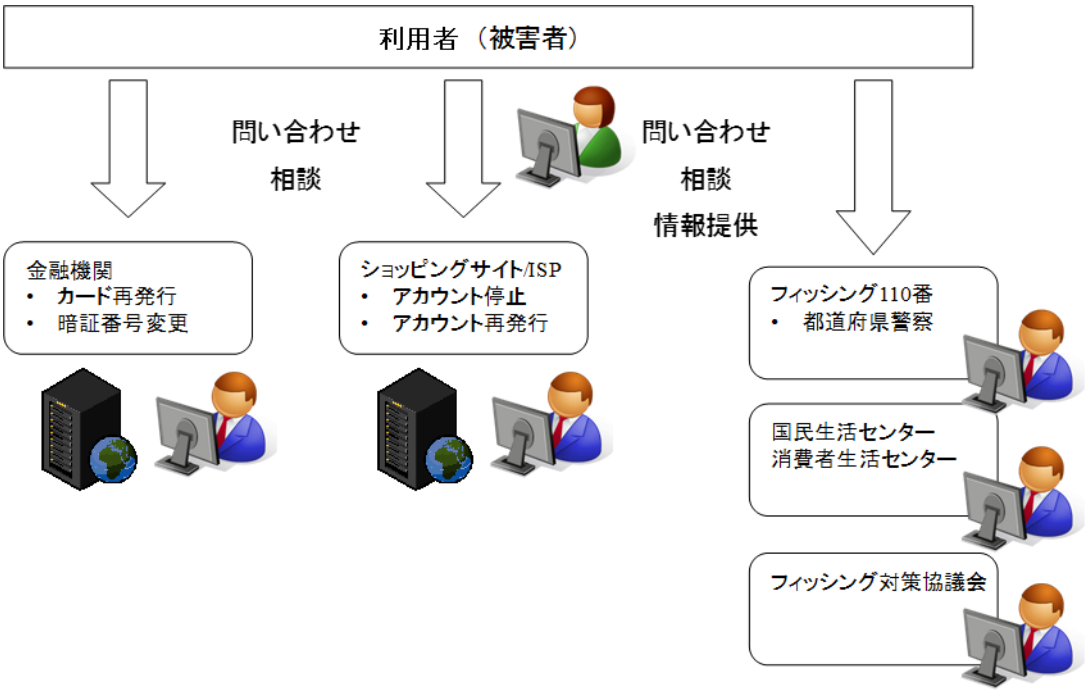
4.2.1. 詐取された情報の識別

フィッシング詐欺被害に遭った疑いを感じた場合、どの情報が詐取されたのかを把握する必要がある。しかし、フィッシングサイトに情報を入力した瞬間に気が付いたのであれば、詐取された情報について把握できても、銀行口座やクレジットカード利用履歴などに覚えの無い取引を見つけてフィッシング詐欺の疑いを持った場合においては、詐取された情報の詳細までは記憶に無いこともあるだろう。こういった場合には、該当するWebサイト運営者に直ちに連絡をとり、アカウントの停止措置を含め、対策を協議する必要がある。

また、フィッシングサイトへの情報入力だけでなく、キーロガーによるアカウント情報詐取の疑いもあることから、利用している端末上のマルウエア検出作業を行うとともに、利用者登録している全てのWebサイト運営者に連絡をとって、アカウント停止措置を行う必要性について検討することが望ましい。

4.2.2. 関連機関への連絡

詐取された情報に応じて関連する金融機関やクレジットカード会社、ショッピングサイト、プロバイダへ連絡を取り、当該アカウントの利用停止などの対応を依頼する。



フィッシング 110 番：相談/情報提供

国民生活センター/消費者生活センター：相談

フィッシング対策協議会：情報提供

図 8 フィッシング被害に遭ってしまった時の問い合わせ、相談、情報提供

（1） 被害が発生した Web サイト運営者への連絡

情報を詐取された疑いを持ったサービスを提供している事業者に、フィッシング詐欺被害の疑いがあることを伝え、指示によっては暗証番号の変更やカードの再発行、ショッピングサイトやプロバイダの ID およびパスワードの変更を行う。

この際、連絡先を探さなければならないが、Web サイト運営者の Web サイトにて被害に関する連絡先を探しやすいとは限らない。多くの Web サイト運営者では、利用者登録の際に電子メールで登録完了の案内を行っている。このメールに問い合わせ先が記載されていることが多いので、参照しやすいよう、Web サイト運営者から送られてきた電子メールを整理しておくと良いだろう。

（2） 警察への連絡

金銭的な被害など、実質的な被害が確認された場合には、被害者の居住する地区の都道府県警察サイバー犯罪相談窓口[14]へ連絡する。

（3） 国民生活センターまたは各地の消費生活センターへの連絡

国民生活センターまたは各地の消費生活センターは消費生活全般に関する苦情や問い合わせなど、利用者からの相談を専門の相談員が受付け、公正な立場で対応している。フィッシング被害に関し

[14] https://www.npa.go.jp/cyber/policy/phishing/phishing110.htm

ても苦情や相談が必要な場合には、これらのセンターに相談をする。

（4） フィッシング対策協議会への情報提供

フィッシング事象を下記サイトより情報提供する。フィッシング対策協議会では提供された情報を、事例調査や利用者への注意喚起のフィシング対策協議会ホームページ掲載に活用するとともに、対策機関との連携に活用している。

表 1 フィッシング対策協議会連絡先

Web サイト URL	https://www.antiphishing.jp/
電子メールアドレス	info@antiphishing.jp

協議会ではフィッシング詐欺報告は電子メールで受付けている。フィッシングメールに関する報告は、フィッシングメールを転送、あるいは本文に貼り付け、または以下のようにタイトル、差出人名、送信日時、概要などを記述して報告していただきたい。

Subject：フィッシングメールに関する情報提供

タイトル：緊急のお知らせ
差出人名：john@xxbank.example.co.jp
送信日時：2008 年 3 月 XX 日
概要：〇〇銀行を装ってリンクを含んだメールを送ってきた。

--
〇〇 〇〇（報告者氏名、匿名での報告も可）

図 9 フィッシングメール報告の例

ID 詐取などのフィッシング被害が発生した場合には、次のように概要などを記述して報告していただきたい。

Subject：フィッシング被害に関する情報提供

概要：〇〇銀行をかたるフィッシング（e-mail を添付します）があり、そこに ID、パスワードを入力してしまいました。 すぐ気が付いたのでパスワードを変更し、当該銀行に連絡・相談し対策を進めています。 また、警察. . .

--

〇〇 〇〇（報告者氏名、匿名での報告も可）

図 10 フィッシング被害報告の例

5. 付録

付録 A－Web サイト運営者が考慮すべき要件一覧

【 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 】
- 【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
- 【要件 3】 ◎：利用者へのメール送信では、制作・送信に関するガイドラインを策定し、これに則って行うこと
- 【要件 4】 ○：Web サイト運営者が利用者に送信するメールはテキスト形式とすること
- 【要件 5】 ◎：利用者に情報発信する手段および内容を周知すること

【 利用者が正規サイトを判別可能とする対策 】
- 【要件 6】 ◎：Web サイトの正当性に係る情報を十分に提供する画面とすること
- 【要件 7】 ◎：すべてのページにサーバ証明書を導入すること
- 【要件 8】 ◎：正規 Web サイトのドメイン内設置サーバの安全性を確認すること
- 【要件 9】 ○：認証システムが許容するポリシを利用者に示すこと
- 【要件 10】 ○：色々なチャネルで利用者に対する脅威の状況を提供する

【 フィッシング詐欺被害を拡大させないための対策 】
- 【要件 11】 ◎：利用者に端末を安全に保つよう、注意を促すこと
- 【要件 12】 ◎：複数要素認証を要求すること
- 【要件 13】 ◎：資産の移動に限度額を設定すること
- 【要件 14】 ◎：資産の移動時に利用者に通知を行うこと
- 【要件 15】 ○：利用者の通常とは異なるアクセスに対しては追加のセキュリティを要求すること
- 【要件 16】 ○：登録情報を変更するページへの移動には再度認証を要求すること
- 【要件 17】 ○：重要情報の表示については制限を行う
- 【要件 18】 ○：認証情報は厳格に管理すること（アカウントは不必要に発行しない）
- 【要件 19】 ◎：アクセス履歴の表示

【 ドメイン名に関する配慮事項 】
- 【要件 20】 ◎：利用者の認知している Web サイト運営者名称から連想されるドメイン名とすること
- 【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、利用、廃止にあたっては、自社のブランドとして認識して管理すること
- 【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
- 【要件 25】 ◎：フィッシング詐欺発生時の行動計画を策定すること
- 【要件 26】 ◎：フィッシング詐欺および対策に関わる最新の情報を収集すること
- 【要件 27】 ◎：フィッシングサイト閉鎖体制の整備をしておくこと
- 【要件 28】 ○：フィッシングサイトアクセスブロック体制の整備をしておくこと

【 利用者への啓発活動 】
- 【要件 29】 ◎：利用者が実施すべきフィッシング詐欺対策啓発活動を行うこと

【要件 30】 ◎：フィッシング詐欺発生時の利用者との通信手段を整備しておくこと

【 フィッシング詐欺被害の発生を迅速に検知するための対策 】

【要件 31】 ○：Web サイトに対する不審なアクセスを監視すること

【要件 32】 △：フィッシング詐欺検出サービスを活用すること

【要件 33】 △：端末の安全性を確認すること

【要件 34】 △：バウンスメールを監視すること

付録 B－利用者が考慮すべき要件一覧

【 パソコンやモバイル端末は、安全に保つ 】

【要件 35】 ◎：ソフトウエアは信頼できるサイトからインストールする

【要件 36】 ◎：最新のソフトウエアを利用する

【要件 37】 ◎：セキュリティ対策ソフトウエアの機能を理解し適切に用いる

【要件 38】 ○：端末の利用には一般ユーザアカウントを利用する

【要件 39】 ○：URL フィルタリングを活用すること

【 不審なメールに注意する 】

【要件 40】 ◎：個人情報の入力を求めるメールを信用しない

【要件 41】 ◎：メールに記載される差出人名称は信用しない

【要件 42】 ◎：怪しいメールの判断基準を知る

【要件 43】 ◎：安全なメールサーバを活用したり、類似性評価によるフィッシングメール判別機能を活用すること

【要件 44】 ◎：リンクにアクセスする前に正規メールかどうか確認する

【 電子メールにあるリンクはクリックしないようにする 】

【要件 45】 ◎：正しい URL を確認する

【要件 46】 ◎：電子メール本文中のリンクには原則としてアクセスしない

【要件 47】 ◎：正しい URL と錠前マークを確認する

【要件 48】 ○：Web サイト運営者からの通知メール形式をテキスト形式に設定する

【 アカウント情報の管理 】

【要件 49】 ◎：アカウント ID/ パスワードは Web サイト別に設定する

【要件 50】 ◎：全てのアカウントについて緊急連絡先を把握しておくこと

付録 C－参考情報

C.1 【マンガでわかるフィッシング詐欺対策 5 ヶ条】

・「マンガでわかるフィッシング詐欺対策 5 ヶ条」, フィッシング対策協議会
https://www.antiphishing.jp/phishing-5articles.html
（利用者にとってフィッシング詐欺にあわないための基本的対策事項を案内している）

C.2 【情報サイト】

- CNET Japan
  https://japan.cnet.com/news/sec/
- ITmedia
  https://www.itmedia.co.jp/news/security/
- INTERNET Watch
  https://internet.watch.impress.co.jp/
- ScanNetSecurity
  https://scan.netsecurity.ne.jp/
- ZDNET Japan
  https://japan.zdnet.com/security/
- マイナビニュース
  https://news.mynavi.jp/pc/pcsecurity/
- 読売新聞 サイバー護身術
  https://www.yomiuri.co.jp/feature/titlelist/%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E8%AD%B7%E8%BA%AB%E8%A1%93/

（フィッシング含む情報セキュリティに関するニュース/記事が掲載されている）

C.3 【業界団体と各省庁のサイト】

- 経済産業省
  https://www.meti.go.jp/policy/netsecurity/
- 総務省
  https://www.soumu.go.jp/main_sosiki/joho_tsusin/security//
- 警察庁
  https://www.npa.go.jp/cyber/index.html
- 消費者庁
  https://www.caa.go.jp/
- 独立行政法人 情報処理推進機構（IPA）
  https://www.ipa.go.jp/security/
- フィッシング対策協議会
  https://www.antiphishing.jp/
- 一般社団法人 JPCERT コーディネーションセンター
  https://www.jpcert.or.jp/
- NPO 日本ネットワークセキュリティ協会
  https://www.jnsa.org/

（各省庁・団体における情報セキュリティ関係の情報が掲載されている）

C.4 【安全な Web サイトの利用】

- 「安全な Web サイト利用の鉄則」独立行政法人 産業技術総合研究所，2007
  https://www.rcis.aist.go.jp/special/websafety2007/index-ja.html
  （Web サイトの利用者に知ってもらうべき鉄則およびその鉄則さえ守っていれば安全と

なるようなサイト作りに必要な設計の要件が記載されている）

C.5 【サイトの脆弱性対策】

・「安全な Web サイトの作り方」独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/vuln/websecurity.html
（IPA への届け出件数の多かった脆弱性や攻撃による影響度が大きい脆弱性を取り上げ、Web サイト開発者や運営者が適切なセキュリティを考慮した実装ができるようにするための資料が掲載されている）
・「セキュアプログラミング講座」独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/awareness/vendor/programmingv2/index.html
（ソフトウエア開発工程における上流工程（要件定義、設計）から脆弱性対策の論点を意識できるようにするための情報が記載されている）

C.6 【送信ドメイン認証】

・「SPF（Sender Policy Framework）」一般財団法人インターネット協会（IAjapan）
https://salt.iajapan.org/wpmu/anti_spam/admin/tech/explanation/spf/
・「DKIM (Domainkeys Identified Mail)」一般財団法人インターネット協会（IAjapan）
https://salt.iajapan.org/wpmu/anti_spam/admin/tech/explanation/dkim/
・「送信ドメイン認証技術導入マニュアル第 2 版」迷惑メール対策推進協議会（Anti-Spam mail Promotion Council）
https://www.dekyo.or.jp/soudan/data/anti_spam/201108MN_all.pdf
・「電子メールのなりすまし対策 -送信ドメイン認証でなりすましを防ぐ-」迷惑メール対策推進協議会（Anti-Spam mail Promotion Council）
https://www.dekyo.or.jp/soudan/data/anti_spam/auth_leaflet.pdf

C.7 【CSIRT への支援要請】

・「インシデント報告の届け出」一般社団法人 JPCERT コーディネーションセンター
https://www.jpcert.or.jp/form/
（インシデント報告の様式と記入の手引やガイドラインについて記載されている）

C.8 【Web ブラウザのフィッシングサイト対策機能】

・ 「Microsoft SmartScreen」
https://www.microsoft.com/ja-jp/safety/terms/smartscreen.aspx

C.9 【フィッシング 110 番】

https://www.npa.go.jp/cyber/policy/phishing/phishing110.htm
（フィッシングに関する警察関係の情報提供先や被害の相談先が紹介されている。）

C.10 【国民生活センター・消費生活センター】

・「国民生活センター」
http://www.kokusen.go.jp/
（利用者からの相談事例などが掲載されている）

・「全国の消費生活センター」
http://www.kokusen.go.jp/map/
（各居住地の相談窓口一覧が掲載されている）

C.11 【その他の一般向け相談先】

・「インターネット・ホットラインセンター」
http://www.internethotline.jp/
（日本におけるインターネット上の違法・有害情報の通報受付窓口）
・「迷惑メール相談センター」
https://www.dekyo.or.jp/soudan/index.html
（総務省より委託を受けて「特定電子メールの送信の適正化等に関する法律」に違反していると思われる迷惑メールを収集）
・「独立行政法人 情報処理推進機構 IPA ウイルス届け出」
https://www.ipa.go.jp/security/outline/todokede-j.html
（ウイルスの届け出を受け付けている）
・「独立行政法人 情報処理推進機構 IPA 情報セキュリティ安心相談窓口」
https://www.ipa.go.jp/security/anshin/index.html
（マルウエアおよび不正アクセスに関する総合的な相談窓口）
・「消費者庁 越境消費者センター」
https://www.ccj.kokusen.go.jp/
（海外から購入した商品（インターネット通販・店頭でのショッピング含む）に関するトラブルの問い合わせを受け付けている）
・「一般社団法人 コンピュータソフトウエア著作権協会不正コピー情報受付」
https://www2.accsjp.or.jp/piracy/
（著作権違反の届け出）
・「一般社団法人ユニオン・デ・ファブリカン」
https://www.udf-jp.org/
（偽物に関する情報窓口）

C.12 【STOP. THINK. CONNECT. キャンペーン】

https://stopthinkconnect.jp/
世界的なフィッシング対策ワーキンググループ「Anti-Phishing Working Group」（APWG）と アメリカ合衆国の National Cyber Security Alliance （NCSA） は 2009 年に「STOP. THINK. CONNECT.」キャンペーンを開始した。日本ではフィッシング対策協議会に参加する、情報セキュリティ対策事業者、銀行、クレジットカード会社、ショッピングサイト事業者などさまざまなメンバによって、日本国内のサイバー犯罪防止のための対策や啓発活動が行われている。

C.13 【フィッシング対策協議会】

https://www.antiphishing.jp/
フィッシング事象の情報提供先 e-mail アドレス：info@antiphishing.jp
（フィッシングの解説、事例、報告書などを公開している）

付録 D–プロバイダへのテイクダウン要請文例

To whom it may concern,

[簡潔な企業プロファイル].

The website is located at the following address:

＜当該フィッシングサイトの URI＞

For your information, the fraudulent website appears to be a forgery of this legitimate website:

<正規サイトの URL>

Please take all necessary measures to suspend services of this fraudulent site.

We highly appreciate your cooperation on this matter.

Thank you very much. Sincerely,
--
[担当者、送信者の名前]
[担当者、送信者の所属部署]
[企業名]
[国際電話番号]
[担当者、送信者のメールアドレス]

付録 E–事業者における NG 集

■サービス提供者の体制の不備

・　フィッシングを含むセキュリティ（インシデント）対応の体制が整備されていない
責任者と各人の役割を明確化し、サービスやシステムの開発とサービスの運用においても、明確な判断基準のもとセキュリティポリシーとその運用方法を策定するとともに、万が一のインシデント発生時にも迅速な対応が取れる体制を確保する。

・　利用者からの通報・相談窓口が明確でない。
フィッシング詐欺発見の通報や被害にあった場合の相談先としての窓口を開設し、利用者に明示する。サービス提供者は、利用者からの通報でフィッシング詐欺発生を認知するケースが多く、この窓口が不明確だと対応が遅れ、利用者と自組織の被害を拡大する可能性がある。他の一般サポート窓口と兼用であってもよいが、連絡先が明示されている必要がある。

・　フィッシング発生時の対応方法が未整備
利用者からの通報などにより、フィッシング詐欺の発生を認知した場合、事前に整備・確認した手順に基づき、迅速にフィッシングサイトのテイクダウン（閉鎖）や利用者への告知などを実施し、被害の最小化に努める必要があるが、これが未整備だと、対応の遅れや間違った対応により被害を拡大させてしまう可能性がある。

・　サービスやシステム開発時に、セキュリティを維持する運用稼動とコストが十分考慮されていない。
フィッシング詐欺の主な対象となる認証システムのセキュリティを確保し続けるためには、開発時のみならず、日常のセキュリティ維持のための稼動とコストを伴う。Web アプリケーションの脆弱性診断、OS やミドルウエアの脆弱性対応、サーバ証明書費用なども十分考慮する必要がある。サービス提供組織での維持運用が難しい場合、OpenID などによる他社の ID 連携サービスを活用することも検討する。ただし、将来的に自前開発の認証システムとする可能性がある場合や、セキュリティレベルをサービス提供組織でコントロールできないことは十分考慮する。

・　利用者への啓発を行っていない
フィッシング詐欺被害の軽減には、利用者の正しい知識と認識が欠かせない。フィッシング詐欺に関する知識・情報や自社・自組織の取り組みなど、Web サイトやメールを活用し、随時発信し啓発を行う。

■利用者へのメール送信

・　利用者に送信するメールの様式がバラバラ
メールの送信者アドレスおよびそのドメイン、件名、本文などの様式やトーンが送信の都度あるいは送信するメールの種類ごとにバラバラだと、利用者は、日頃送信されてくる本物のメールの特徴を把握できないため、フィッシング詐欺メールを受信しても疑いを持ちにくくなる。極力統一し、日頃から利用者に本物と偽物の判別を付きやすくする環境を整備する。また、正当なメールであることを証明するために、送信するメールへの電子署名付与の検討

を推奨する。ただし、一部のメールだけへの付与は、逆に利用者が混乱する可能性があるため注意が必要である。

■Web サイト運用

・ HTTPS による Web サイト保護が正しく行えていない①

入力データの保護のみに注意が向き、HTTPS 暗号化通信およびサーバ証明書をフォームの送信先 Web サイトのみに導入し、入力フォーム自体を表示する Web サイトには導入していないケースが見られる。この場合、利用者に入力フォーム自体を表示するサイトの正当性を示すことができていないため、フィッシングサイトが発生した場合、利用者は偽物であることに気づきにくくなる。なお、入力フォームを表示するサイトと入力データを送信する先のサイトは極力同一とすることが望ましい。

※通常は、同一であるサイトがほとんど。

たとえ両サイトが HTTPS 暗号化通信およびサーバ証明書によって正当性を証明されていても、利用者は入力フォームを表示したサイトを信頼しデータを入力するのであり、送信先サイトはデータ入力時点では確認できない。

・ HTTPS による Web サイト保護が正しく行えていない②

正当性を証明したい Web サイトのページ内の一部の画像が、HTTPS 通信を使わない通常の Web サイトのものであるなど、非 HTTPS 通信のパーツが混在した場合、多くのブラウザは、その旨をアラート表示し、該当画像を表示するかどうか確認を求める。ここで、表示する選択をした場合、サーバ証明書による Web サイトの正当性は証明されなくなる。（鍵マークが表示されない。）Web ページを構成する画像などの全てのパーツが、正当な HTTPS 通信を行う Web サイト上のものであるようページ制作する必要がある。

・ ログイン ID やパスワード文字列の制限が不用意に緩い

ログイン ID やパスワードを利用者が設定できる場合、不用意に制限が緩いＩＤやパスワードが許容されることのないよう、文字数や利用可能な文字の種類など、開発者だけの判断による基準とせず、サービスやセキュリティの担当者と十分検討し決定する。検討に当たっては、サービスが扱う情報の重要性や利用者のリテラシー、利便性などに加え、利用者は同一の ID やパスワードを複数の Web サイトに設定する傾向があることから、万が一フィッシング詐欺に遭った場合、被害が他サイトにも拡大する可能性があることも十分考慮し、適正な基準を設ける。

6. 検討メンバ

本ガイドラインの検討を行ったフィッシング対策協議会 2019 年度技術・制度検討ワーキンググループの構成は次のとおりである（所属は 2020 年 3 月時点）。

区分	氏名	所属
主査	野々下 幸治	トレンドマイクロ株式会社
	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
	山本 和輝	BB ソフトサービス株式会社
	松本 悦宜	Capy 株式会社
	塚越 彩	株式会社 bitFlyer
	松岡 晋矢	株式会社 bitFlyer
	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
	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
	内山 裕延	三菱 UFJ ニコス株式会社
	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）	