Council of Anti-Phishing Japan
**デジタル署名者** : Council of Anti-Phishing Japan
DN : c=JP, st=Tokyo, l=Chuo, o=Council of Anti-Phishing Japan, cn=Council of Anti-Phishing Japan, email=antiphishing-sec@jpcert.or.jp
**日付** : 2023.05.31 16:14:20 +09'00'

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

2023 年度版

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、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と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機密性、完全性および可用性の確保

・利用者におけるウイルス、スパイウェアなどのマルウェア対策（フィッシング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、サーバー機器、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、ユーザーネーム、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、それら一連の行為者の全体を意味する。

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

【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、金銭など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、そのフィッシングにより利用者や従業員が個人に関わる情報を詐取されること。または、そのフィッシング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）】
コンピューターおよびコンピューター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。SMS を利用して、個人情報を抜き取るフィッシングサイトへと誘導するフィッシングはスミッシングと呼ばれている。

【錠前マーク】
Web ブラウザーのアドレスバーの近くに表示されるアイコンのことで、Web ブラウザーと、アクセスしている先の Web サーバーとの間でやり取りされる通信データが暗号化されていることを示している。途中で盗聴されてもデータの内容を読み取られないが、安価なもしくは無料のサーバー証明書を使ったフィッシングサイトが増加しており、錠前マークが表示されているだけではフィッシングに対して安全とは言えなくなりつつある。鍵マークと呼ばれることもある。

【フィッシングメール】

クレジットカード会社や銀行からのお知らせと称したメールなどで、巧みにリンクをクリックさせ、あらかじめ用意した本物のサイトにそっくりな偽サイトに利用者を誘導する。そこでクレジットカード番号や口座番号などを入力するよう促し、入力された情報を盗み取る。

【ファーミング】

ファーミング（Pharming）とは、フィッシング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 Web 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 Web 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。

【SPF（Sender Policy Framework）】

電子メールの送信元ドメインが詐称されていないかを検査するための仕組みであり、仕様は、RFC4408 で定められている。

【DKIM（DomainKeys Identified Mail）】

電子メールにおける送信ドメイン認証技術の一つであり、メールを送信する際に送信元が電子署名を行い、受信者がそれを検証することで、 送信者のなりすましやメールの改ざんを検知できるようにするものである。

【DMARC（Domain-based Message Authentication, Reporting, and Conformance）】

電子メールにおける送信ドメイン認証技術の一つであり、SPF、DKIM を利用したメールのドメイン認証を補強する技術で、RFC7489 で標準化されている。

【S/MIME（Secure/Multipurpose Internet Mail Extensions）】

電子証明書を用いた電子メールのなりすまし対策技術の一つ。主要なメールソフトは S/MIME に対応しており、「電子署名」と「暗号化」機能を提供している。

【パークドメイン】

ドメインを取得後、コンテンツが掲載されることなく、ドメインを維持するための Web ページ、もしくはそのドメイン自体を指す。

【BIMI（Brand Indicators for Message Identification）】

DMARC による送信ドメイン認証で認証された正規メールをブランドロゴや公式マークで視覚的にわかりやすく表示する技術やサービスを指す。

【FIDO2】

窃取あるいは漏えいする元となる記憶認証（Something You Know）であるパスワードを使用せず、スマホなどの認証器（Something You Have）となるデバイスに組み込まれた認証機能（生体認証（Something You Are）や PIN など）または外部（またはローミング）認証器（FIDO セキュリティキー、モバイルデバイス、ウェアラブルなど）を使用した認証規格である。

【バウンスメール】

メール配信の結果としてエラーとなった場合に、相手サーバーから通信メッセージによる応答ではなく、別途メールによってエラー応答されるメールを指す。

【テイクダウン】

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。

【Abuse】

Abuse（あびゅーず）とは、「不正行為」や「乱用」を意味し、インターネット上での迷惑行為や不正行為、または通報する窓口を指す。

# 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. フィッシングの手口

フィッシングの単純な例を図 1 に示す。

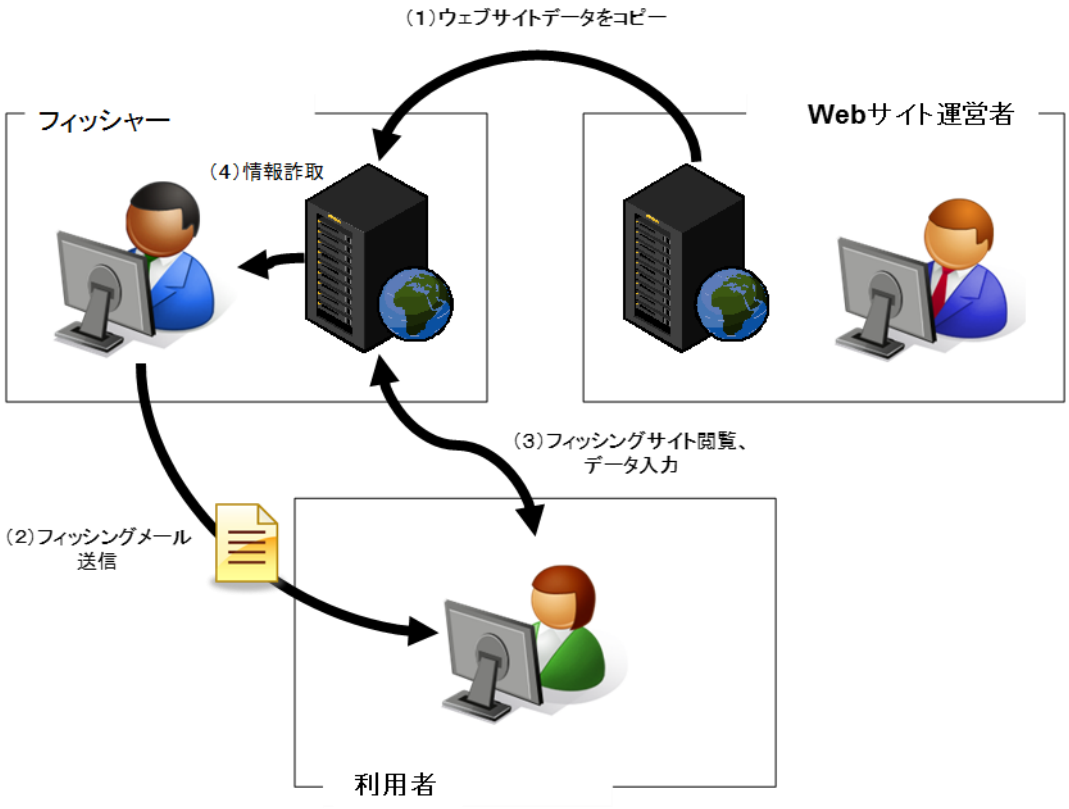


**図 1　フィッシングの単純な例**

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切と考えられる。

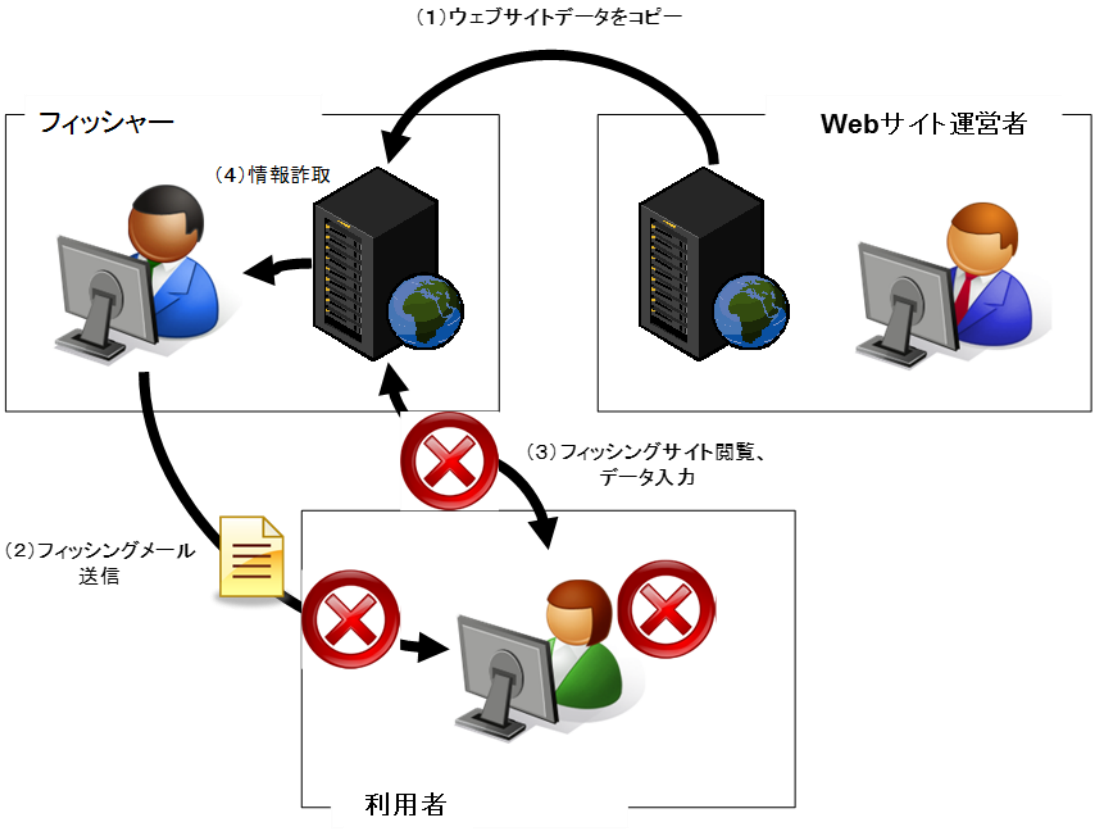


**図 2　フィッシング被害の抑止ポイント**

フィッシング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（図 2 中の赤バツの部分）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。

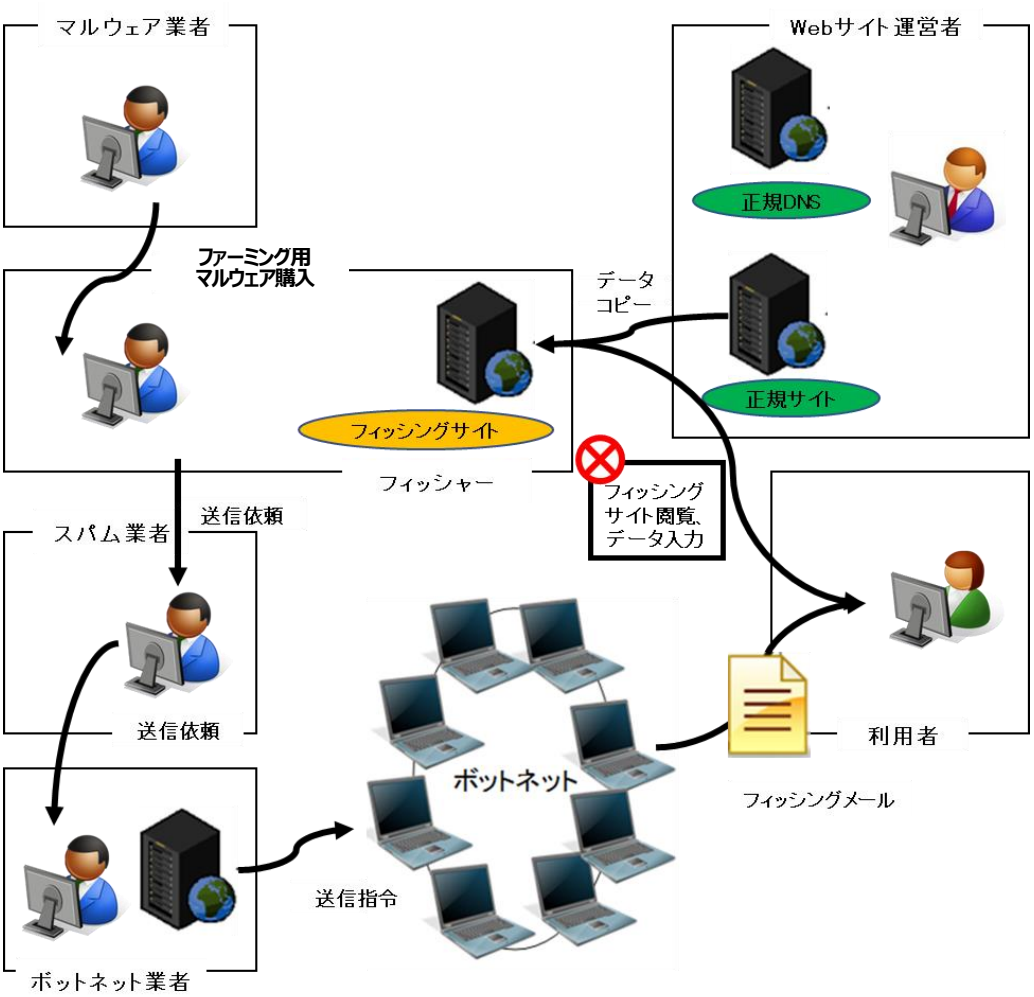


**図 3　フィッシングの複雑な例**

近年確認されているフィッシングにおいては、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、収益化および強化拡大の 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一つとして、犯罪者コミュニティー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「漏えい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ていただきたい。

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

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ことが多い。

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ことをほのめかし、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 サイト運営者名をかたることに加え、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 サイト運営者名をかたるケースがある。

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ことと、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、ほぼすべての機種にあり、通話へ誘導する詐欺に利用されやすいと考えられる。

SMS を利用したフィッシング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ことが必要である。

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 Web サイトなどで告知することが対策としてあげられる。

昨今では、宅配便の不在通知を装う不正な SMS も頻出している。これらは主に国内の携帯電話番号から送信されており、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。一般に、海外からの SMS 受信拒否を設定することが対策となり得るが、それだけでは被害／加害を十分に防げない状況ともなっている。

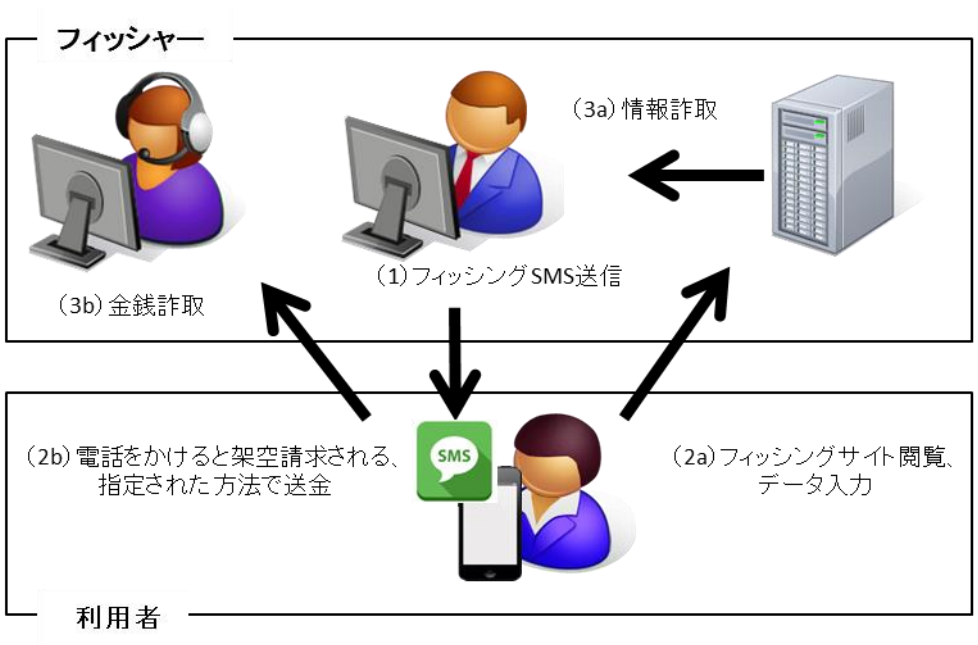


図 4　SMS を利用したフィッシングの例

| | 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<br>（例：03-0000-0000）<br>携帯キャリアごとの特別番号<br>（例：50000） | 海外の電話番号<br>（例：+1 000-000-0000）<br>アルファベット<br>（例：FOOBAR） | 携帯電話番号<br>（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 Web サイトなどに記載し事前に通知した上で利用する | 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. フィッシング対策ガイドライン重要 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ー証明書を導入すること**
- **フィッシングについて利用者に注意喚起すること**

以下に、上記の 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ーに、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と、DMARC（Domain-based Message Authentication, Reporting & Conformance）を設定し、受信制御ポリシーを受信拒否の「reject」を選択することが必要である。また、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および配信途中の改ざん検知を可能と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 の受信制御ポリシーを 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。

SMS（Short Message Service）の配信には、国内直接接続の SMS 配信を利用し、事前に発信者番号を Web サイトなどで告知することが必要である。

フィッシング対策ガイドラインの参照箇所

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】◎:利用者が確認できるように利用環境と分かりやすい説明に配慮した上で、どのように確認すればいいのかを分かりやすく端的に説明すること。
【要件 2】◎:外部送信用メールサーバーを送信ドメイン認証に対応させること
【要件 4】◎:利用者に送信する SMS には国内直接接続の配信、または、RCS 準拠サービスを利用すること

### 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得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ー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の参照箇所

**フィッシング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 10】◎: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・要員を決め、管理のためのルール・手順を社内で確立し十分に共有・周知しておくことが重要である。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。

また管理下のドメインはなりすましメール送信などに不正利用されないよう、DMARC で保護する。特にメールを送らない（Web サービスでのみ利用など）ドメインや、保有しているだけのパークドメインは、reject ポリシーにする。

フィッシング対策ガイドラインの参照箇所

**ドメイン名に関する情報については、以下を参照。**
**【要件 19】◎: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 20】◎: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**

## すべてのページにサーバー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。サーバー証明書を使った 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 サーバーの正当性（ドメイン名を含めたサーバー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。ブラウザーによっては、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上でも効果的である。

フィッシング対策ガイドラインの参照箇所

**正規サイトを判別するためのサーバー証明書に関する情報については、以下を参照。**
**【要件 6】◎:すべてのページにサーバー証明書を導入すること**

## フィッシングについて利用者に注意喚起すること

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、役割分担および連絡・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、クレジットカードおよび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。

フィッシングは、事業者を模倣したメールやサイトと利用者との間で発生する。それは事業者から離れたところで行われることとなり、フィッシングメールの到着やフィッシングサイトへのアクセスを阻止することは困難である。したがって事業者はフィッシングの発生有無に関わらず、利用者に対しフィッシングに関する注意喚起を行うことが重要である。また、フィッシングに遭ってしまった場合の報告窓口の事前案内も必要である。利用者への注意喚起には、「利用者向けフィッシング対策ガイドライン」や「安全な Web サイト利用の鉄則」などを参考にすることが望ましく、啓発資料の作成にあたっては、一般の利用者が理解できる内容にすると同時に、内容の最新化や正確性確保のため技術的内容がわかるメンバーも企画の段階から参画する必要がある。

注意喚起は「難しい」や「専門すぎる」と伝わる場合がある。利用者のパソコンやインターネットの知識や経験の差を考慮し、用語説明の追加や漫画などで分かりやすく表現するなど工夫することが必要である。例えば「ドメイン」が理解できない状態で、なりすまし手口やフィッシング対策は伝わらない。顧客からの問い合わせ状況などを参考にして注意喚起を複数パターン用意することが望ましい。

フィッシング対策ガイドラインの参照箇所

**利用者への注意喚起については、以下を参照。**

**【要件 21】◎:フィッシング対応に必要な機能を備えた組織編制とすること**

**【要件 22】◎:フィッシング被害に関する対応窓口を明記すること**

**【要件 25】◎:利用者が実施すべきフィッシング対策啓発活動を行うこと**

**【要件 26】◎:フィッシング発生時の利用者への連絡手段を整備しておくこと**

# 4. Web サイト運営者におけるフィッシング対策

本章では、フィッシングの標的、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

## 4.1. Web サイト運営者におけるフィッシングの被害とは

Web サイト運営者のフィッシングによる被害を考えてみると、事業者職員がフィッシング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。利用者保護および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対策を実施すべきであろう。

## 4.2. 利用者を守るためのフィッシング対策とは

利用者がフィッシング被害に遭う際の事象の流れを図 6 に示す。

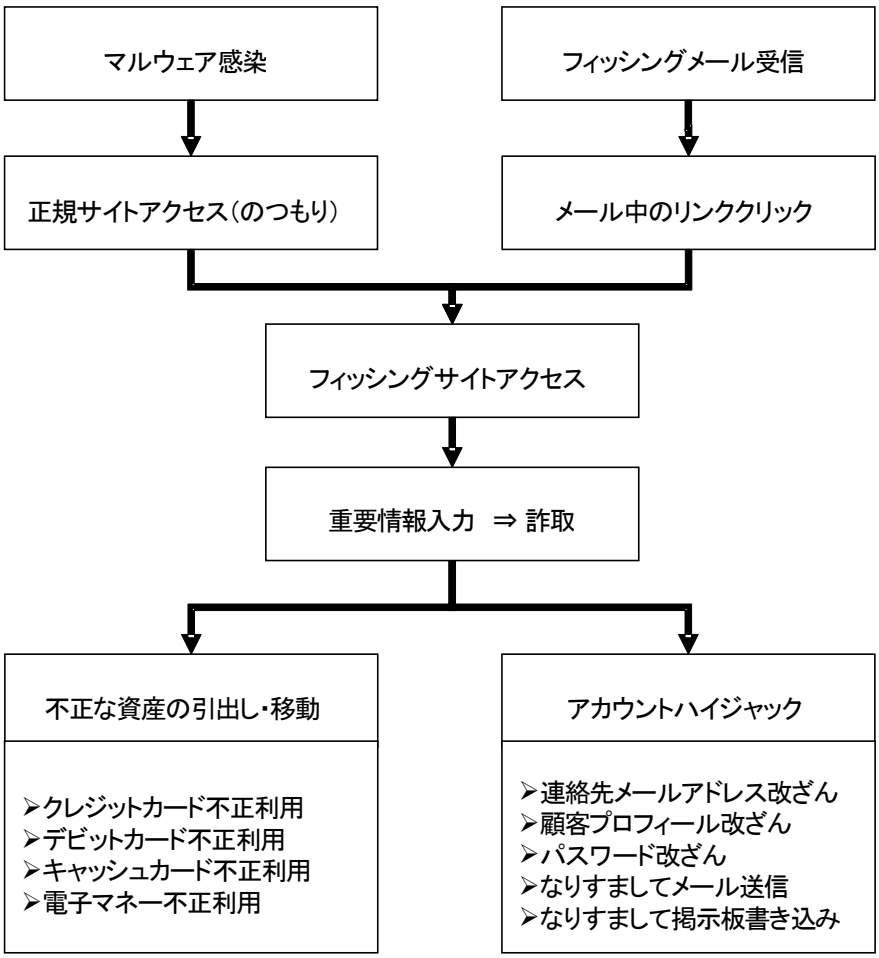


**図 6　利用者サイドでのフィッシング被害発生フロー**

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。フィッシング被害の発生を抑制するための対策、フィッシング被害の発生を迅速に検知するための対策、フィッシング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。

## 4.3.　フィッシング被害の発生を抑制するための対策

フィッシングは、計画→調達→構築→誘導→詐取→収益化の 6 つの行動によって行われる（フィッシング対策協議会 学術研究 WG　フィッシングのビジネスプロセス分類より）。事業者は、この行動に沿った対策を行うことが望ましい。

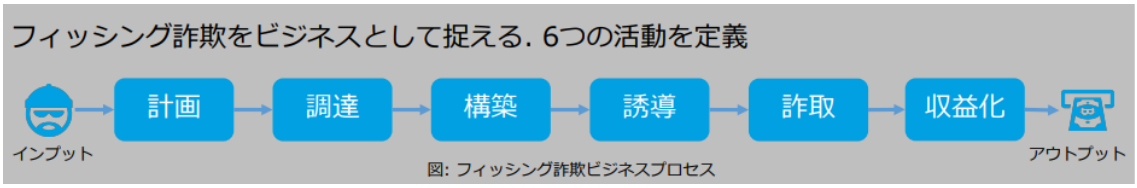


**図 7　6 つの活動**

①計画：フィッシングの計画を立てる（フィッシング対象となる組織の選定、組織の調査など）

②調達：フィッシングを行うために必要なツールや情報を調達する（Phishing Kit の購入、フィッシングメールの送信先一覧の取得など）

③構築：フィッシングに必要なシステムを構築する（フィッシングサイトの構築など）

④誘導：フィッシングサイトなどへ誘導する（フィッシングメール/SMS の送信など）

⑤詐取：フィッシングサイトに入力させ、情報を騙し取る（ID やパスワード、複数要素認証などの認証情報の詐取。クレジットカード情報の詐取など）

⑥収益化：犯罪者が騙し取った情報をもとに金銭的な利益を得る（正規サイトへの不正ログインにより別口座に現金を振り込む。盗んだ情報を転売するなど）

### 4.3.1.　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】 ◎：利用者が確認できるように利用環境と分かりやすい説明に配慮した上で、どのように確認すればいいのかを分かりやすく端的に説明すること。**

ドメインから送信された正規メールに表示されるブランドのロゴや公式マーク、メールに付与する電子署名は、メールを使って利用者をフィッシングサイトに誘導する手法に対する技術的な対策として位置づけられる。しかし技術による対策を取っていても、そのことが利用者に伝わらなければ意味がなくなってしまう。

2022 年現在、国内で利用者が多い大手メールサービスは、BIMI に対応しており、S/MIME もまたスマートフォン標準のメールアプリで確認できるため、このような正規メールの確認に必要な技術に対応し、その確認方法を周知する。

例えば、〇〇銀行を名乗るメールが届いたときにそれが正規のメールであるか否かことが判別できるように、ブランドのロゴや公式マークが表示された本物メールと表示されない偽物メールの違いを掲載する、S/MIME の電子署名が正しいかどうか確認する方法を掲載する、など考えられる。

また、S/MIME による電子署名は、送信元のメールアドレス単位で署名を行うため、連絡内容（メールアドレス）によって、電子署名をつけたりつけなかったりすると、利用者は電子署名が施され

ていないことがあると認識してしまい、効果が半減する。したがってS/MIMEによる電子署名を行う際には、送信に使用するすべてのメールアドレスで電子署名を施すことが必要となる。

## 【要件2】 ◎：外部送信用メールサーバー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ーはSPF、DKIMの送信ドメイン認証に対応し、さらにDMARCによるなりすましメールに対する受信制御ポリシーを設定すること。

SPF（Sender Policy Framework）は送信元メールサーバー（IPアドレス）の認証を、DKIM（Domain Keys Identified Mail）はメールヘッダーや本文への電子署名によりメール本体の認証を行う技術であり、DMARC（Domain-based Message Authentication, Reporting & Conformance）は、送信ドメイン認証技術のSPFやDKIMを補強する技術であり、なりすましメールで発生するSPF、DKIMの認証失敗状況から、そのメールを利用者に届く前に、プロバイダー側で受信を拒否、または、迷惑メールボックスに入れるなどの制御が可能となる。

DMARCの「メールの受信制御ポリシー」は、以下の3つの受信制御ポリシーを選択することができるが、なりすましメールの対策としてDMARCのポリシー“reject”を設定することが重要である。

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、プロバイダーは指定された受信制御ポリシーにしたがって受信を拒否（reject）することができ、なりすましメールを利用者に届けない制御が可能となる。また、DMARCはプロバイダー側から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、受信制御ポリシー「none」による現状把握から開始し、正規メールが認証されて届いていることを確認したのち、次に「quarantine（隔離させる）」「reject（受信を拒否する）」の受信制御（DMARC Enforcement）を行う。ポリシーが「none」のまま運用を続けると、なりすましメールは受信者へ素通しで届き続けるため、被害抑制にならず、フィッシングで狙われる続ける要因となる。

またさらに、正規ドメインから送信される認証済みメールの視認性を向上させるBIMI（Brand Indicators for Message Identification）を活用することも有効である。事業者がBIMIを設定すると、利用者側のBIMIに対応するメールソフトにて、組織のブランドロゴなどを表示することができる。これにより、受信者は正規のメールであることを確認することができる。

## 【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」と気付きやすくすることができる。ガイドラインは、付録 E を参考にすることが望ましい。

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、本文下部の問い合わせ先や配信停止などの定型フッター様式、配信時間帯、メール形式、情報発信手段（SMS、メール、SNS）など多岐に亘る。

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る（例：<a href=”フィッシングサイトのリンク”>無害なリンク</a>）。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、メール全文をコピーし、リンクだけを差し替えた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上で送付する。

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。

また、メール送信の際は、送信ドメイン認証 DMARC で保護されたドメインのメールアドレスから送信する。DMARC で保護されていない場合、正規メールと同じメールアドレスやドメインを使って「なりすまし」メールを送ることが可能であり、利用者は本物か否か判断ができないため、被害が発生しやすくなる。

### 【要件4】 ◎：利用者に送信する SMS には国内直接接続の配信、または、RCS 準拠サービスを利用すること

SMS（Short Message Service）を利用したフィッシングでは、発信元をアルファベットで自由に表記できる国際網経由の SMS 配信を利用し、Web サイト運営者名をかたるケースが多い。そのため、利用者に配信する SMS には、第三者のなりすましが困難な国内直接接続の SMS 配信を利用し、事前に発信者番号を自社の Web サイトなどで、告知する対策が有効である。また、SMS の次世代版といえる RCS（Rich Communication Service）に準拠したサービスを利用することも有効な対策となり得る。RCS に準拠した国内サービス「＋メッセージ」では、事業者が携帯キャリアから認証を得たことを示す「認証済みマーク」を発信元に表示する仕組みが用意されている。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ていることから、安全なコミュニケーションツールとして切り替えを進めることが望ましい。

### 【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

ユーザーに周知・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。

### 4.3.2. 利用者が正規サイトを判別可能とする対策

さまざま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】 ◎：すべてのページにサーバー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。サーバー証明書を使った 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 サーバーの正当性（ドメイン名を含めたサーバー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。

また、昨今、HTTPS を使用していないサーバーは「安全ではない」と表示され、ブランドイメージが損なわれる。HTTPS を有効にしたサーバーでは、HTTP は無効にして、HSTS （HTTP Strict Transport Security）により常に HTTPS を使うよう設定し、暗号通信で保護する。

**【要件7】 ○：パスワード強度に関するポリシー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めるようにする。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ーを定め、ポリシー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。またポリシー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8】 ○：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 やメルマガなど、さまざま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。

### 4.3.3. フィッシング被害を拡大させないための対策

利用者がフィッシング被害にあい、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9】 ◎：利用者に端末を安全に保つよう、注意を促すこと

警告画面を表示し、アプリのセキュリティアップデートなどを装って、スマートフォンを遠隔操作する不正アプリをインストールさせる事例が 2018 年頃から急増し、被害が続いている。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などを安全に保ち、危険なサイトへ誘導する不正なメールを排除するよう、注意を促す必要がある。

注意項目としては次に挙げる内容を含める必要がある。

- 「OS、Web ブラウザーおよびアプリ、ソフトウェアは、最新の状態に保つこと」
- 「セキュリティ対策ソフトウェ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」
- 「URL フィルターを活用すること」
- 「アプリやソフトウェアは公式サイトや信頼できるサイトからインストールし、発行元不明のアプリ、ソフトウェアはインストールしないこと」
- 「オンラインサービスを利用する場合は、公式アプリを利用すること」
- 「なりすましメール対策、迷惑メール対策が強化されているメールサービスを使うこと」
- 「迷惑メールフィルターを利用すること」

なお、Web サイト運営者は、つねに正規サイトに接続してサービスが利用できるよう、公式アプリの提供や、マルウェア対策アプリを利用者に提供することを検討するとともに、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10】 ◎：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。

特にポイントや資産の移動機能（商品の引換、他金融機関への振込みなど）を提供している場合には、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ー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。

一方、昨今では複数要素認証のワンタイムパスワードも窃取される事例が増えてきており、以下のような対策をサービスの内容に応じて実施することが望ましい。

対策 1：ワンタイムパスワードが必要となるのは、サービスへのログイン、パスワードなどの重要情報の変更、振込みなどの複数の目的があることから、その目的をメッセージに含めることで、本人に心当たりがない場合、意図に反した処理が進んでいること（＝ワンタイムパスワードが窃取さ

れようとしていること）を認識できる。

対策 2 : サービス提供事業者は FIDO2 の WebAuthn による認証の導入も是非検討したい。FIDO2 では、生体認証（Something You Are）と認証機（Something You Have）の二要素を使い、窃取あるいは漏えいする元となるパスワードやワンタイムパスワードなどの記憶認証（Something You Know）を使用しないスマホだけ認証が完結する最新の認証規格である。最新のブラウザーはほとんどサポートされており、Web サーバー側の認証仕様である WebAuthn も実際に導入する企業やサービスが増えてきている。

### 【要件11】 ◎ : ポイントや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のポイントや資産の窃盗被害を抑制するため、ポイントや資産の移動機能（ポイント交換や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。また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12】 ◎ : ポイントや資産の移動時に利用者に通知を行うこと

ポイントや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 のマルウェア感染など、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移動確認手続きを検討することが望ましい。

### 【要件13】 〇 : 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ーンを分析し、それと異なるログイン行動パター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。

### 【要件14】 〇 : 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や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、複数要素認証を求めるようにすることが望ましい。

### 【要件15】 ○：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16】 ○：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17】 ◎：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、接続時間およびアクセス元 IP アドレスを含むこと。

#### 4.3.4. 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18】 ◎：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さまざまなものがあるが、"com"、"net"、"org"あるいは”xyz”、”site”などの特定の国と関連しないドメイン名[3]は、登録申請者に対する実在確認を行わないことも多いことから類似の文字列のドメイン名の登録をフィッシャーが行いやすく、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"[4]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。

すで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

[3] 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。
[4] JP ドメイン名の種類と対象：https://jprs.jp/about/jp-dom/spec/

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19】 ◎：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

一般消費者がドメイン名を見て判断することは非常に困難だが、正規サービスで使用しているドメイン名はオンライン上以外でも利用者が確認できるよう示す必要がある。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（電子メールを読まない・関心を持たない利用者のため、およびドメイン名を印象づけるため）、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、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。そのような確認が苦手な層に対象を絞り、確認しやすい内容にすることも検討する。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、サーバー証明書を利用することで、ドメイン名の正当性を示したり、送信ドメイン認証でドメインを不正利用から保護することも重要である。

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、一般的な役割を持つメールアドレス名については、RFC2142[5]に準拠すること。また BIMI やブランドアイコン、公式マークのような技術を使い、メール送信元のドメイン名の確認を不要にすることも検討する。

### 【要件20】 ◎：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

企業において登録・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ため、ドメイン名管理のためのルール・手順を社内で確立することが重要である。具体的には、ルール・手順として以下の内容を定める必要がある。

- ドメイン名の管理を行う部門・担当者
- ドメイン名の登録に関する留意事項

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

- ドメイン名に関する各種連絡先情報に関すること
- ドメイン名の廃止・Web サービス利用終了時の注意事項

- ドメイン名の管理を行う部門・担当者

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、自社で登録しているドメイン名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するリスクが高くなる。このような事態を避けるため、あらかじめドメイン名管理を行う部門・担当者を定めておく必要がある。

- ドメイン名の登録に関する留意事項

新たなドメイン名を登録・利用する際は、その目的を明らかにし、サブドメイン名やサブディレクトリなどの活用と、メリット・デメリットを比較検討する必要がある。例えば、サブドメイン名やサブディレクトリの活用は URL 全体が長くなり、利用者の利便性・視認性を下げてしまう可能性がある。個別の事例ごとに比較検討し、ドメイン名登録の要否を判断することが必要である。

また、登録中のドメイン名管理におけるセキュリティ向上の手段として、意図しないレジストラー変更を防ぐためのサービスや、ドメイン名の登録情報が意図せず書き換えられることを防ぐためのサービスを提供しているレジストラーがある。これらのサービスは、悪意ある第三者からドメイン名の乗っ取りを防ぐための対策として有効である。ドメイン名の登録・利用目的に応じて、これらのサービス利用を検討することも必要である。

- ドメイン名に関する各種連絡先情報に関すること

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、レジストラー変更など、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。

- ドメイン名の廃止・Web サービス利用終了時の注意事項

利用を終えたドメイン名を廃止する際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。

最も有効な対策は、一度登録・利用したドメイン名は、その後も登録を継続し続けることである。止むを得ず利用終了後にドメイン名を廃止する際は、すぐに廃止するのではなく、他の参照されているサイトでの対応や利用者の対応を考慮し、数年間は確保した後に廃止するなどの対策が考えられる。なお、廃止したドメイン名と同じ文字列が第三者によって登録された場合、当事者同士の話し合いや訴訟を通じて、ドメイン名を取り戻す（＝「ドメイン名の移転」を行う）道もあるが、多額の費用や時間がかかってしまう可能性が高いこと、また、確実に取り戻せる保証はない点に留意が必要である。また、「ドメイン名紛争処理方針（DRP）」に基づく申立を行い、その紛争処理を通じて、ドメイン名を取り戻す（＝「移転裁定」を得る）方法もあるが、過去に当該文字列のドメイ

ン名の登録者であったことをもって移転裁定を得ることは、極めて難しい点にも留意が必要である。

加えて、外部の Web サービスを利用してドメイン名を運用しているケースで、そのサービス利用を終了する際には、DNS の設定を適切な状態にした上でサービス利用を終了することが必要である。

例えば、CDN サービスの利用を終了する場合、利用終了後も DNS の CNAME レコードが残っていると、悪意ある第三者がサブドメインを乗っ取り（Subdomain Takeover）、フィッシングサイトを運営するリスクがある。CDN サービスの利用終了時には、DNS の CNAME レコードを削除する必要がある。

### 4.3.5. フィッシングへの備えと発生時の対応

**【要件21】 ◎：フィッシング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わかる人材を含めたメンバーによる体制構築が望まれる一方、広報、コールセンター、サービス運用部門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、被害抑制のため、さまざまな事項を同時並行的にすみやかに連携、対処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、役割分担および連絡・レポート体制を明確化しておくことが必要である。

「4.5 フィッシング被害が発生してしまった際の対応と対策」に基本的なフローを解説しているので、これを参考に、フィッシング発生時の行動計画（対応フロー）を策定する。

フィッシングは一時的なものではなく、一度発生するときちんと対策がなされるまで、継続する傾向がある。このフローを参考に組織内（グループ内）でスムーズな連携がとれるよう、準備する。

またフィッシング被害を減らすためには、対応するだけではなく、サービス運用部門と協力し、ログなどの分析結果からの状況把握と対策の効果測定を行うことは重要である。

**【要件22】 ◎：フィッシング被害に関する対応窓口を明記すること**

サービス提供に際しては、フィッシング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、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。

不正操作や不正取引により利用者に多大な被害が及ぶ金融系サービス、キャッシュカード、クレジットカードおよびデビットカードの発行を行っているサービス、オンライン決済サービスの場合はアカウントの利用制限（停止）依頼や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23】 ◎：フィッシングの手法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 B に示す。

**【要件24】 ◎：フィッシングサイトへの対応体制の整備をしておくこと**

URL フィルターでアクセスをブロック、警告表示をすると、フィッシングサイトが稼働していても、被害を抑制することができる。フィッシングサイトの閉鎖には時間がかかるため、まずは URL フィルターへの登録を優先する。

各セキュリティソフトウェア／Web ブラウザーベンダーの Web サイトなどにその報告方法が掲載されているので、フィッシングサイトの URL を迅速に共有できるように準備しておく。

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」にも情報共有し、被害規模など状況を鑑みて注意喚起の掲載や有効な対策について相談する。なお、外部組織へ連携の際には、組織内 CSIRT またはそれに代わる窓口を設け、セキュリティ外部組織へ連携の際には、その窓口から連絡を行い、組織内の関連部門へ展開することが望ましい。

### 4.3.6. 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25】 ◎：利用者が実施すべきフィッシング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 B.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あたっては、「難しい」や「専門すぎる」と思われる場合がある。利用者のパソコンやインターネットの知識や経験の差を考慮し、用語説明の追加や漫画などで分かりやすく表現するなど工夫することが必要である。例えば「ドメイン」が理解できない状態で、なりすまし手口やフィッシング対策は伝わらない。顧客からの問い合わせ状況などを参考にして注意喚起を複数パターン用意することが望ましい。

**【要件26】 ◎：フィッシング発生時の利用者への連絡手段を整備しておくこと**

フィッシングが発生した場合は、速やかに情報収集し、発生する被害を把握した上で、Web や SNS などに注意喚起を掲載する。またメールで注意喚起を行う場合は、注意喚起メール文面をコピーしたフィッシングメールを送信される可能性を想定し、S/MIME で電子署名を施したり、送信ド

メイン認証 DMARC で保護されたドメインのメールアドレスで送信する。BIMI やブランドアイコン、公式マークなどの正規メール視認性向上対策が行われていることが望ましい。

利用者登録時には、緊急通知用[6]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、住所もあわせて把握しておく。また、公式アプリ内での通知は、利用者が安全に連絡を受け取ることができる手段であるため、利用を推奨し、環境を整備しておくことが望ましい。

## 4.4. フィッシング被害の発生を迅速に検知するための対策

フィッシング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27】 〇：Web サイトに対する不審なアクセスを監視すること

サーバーやファイア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審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。

また、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以下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。

- favicon.ico（ホームページのシンボル（アイコン）として使われる、画像ファイル）
- 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

### 【要件28】 ◎：フィッシング検知に有効なサービスを活用すること

フィッシング発生について、利用者からの問い合わせや第三者からの連絡、また、SNS（Twitter など）による投稿などから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し、URL フィルターへの登録やテイクダウンを行う商業サービスが存在するため、組織内に専門的に対応を行う人員を配備できない場合は、これらのサービスを活用して迅速に被害発生に対応することが望ましい。また、フィッシング発生を早期に検知する目的で、事業者特有の文字列を含むドメイン名の事業者以外からの登録状況のモニタリングや検知・通知サービスを活用することも有効である。

[6] 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。

**【要件29】 ◎：DMARC レポートやバウンスメールを監視すること**

送信ドメイン認証 DMARC 対応済ドメインのメールアドレスに偽装したなりすましメールを送信すると、DMARC 検証に対応済メールサービスから集約レポート（Aggregate Report）や失敗レポート（Failure Report）が送られてくることがある。利用者が多い大手メールサービスは DMARC 集約レポートの返送を行っているため、これらを収集、分析することによって、なりすましフィッシングメール送信元のサーバーや配信規模を把握することができる。また、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ー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。DMARC 未対応の場合は、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。

## 4.5. フィッシング被害が発生してしまった際の対応と対策

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、および Web サイト運営者の利用者にフィッシング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、URL フィルターへの登録と、フィッシングサイトのテイクダウン（閉鎖活動）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。テイクダウンは時間を要するが、フィッシング被害はフィッシングメールが配信されてから数時間以内に多く発生しており、間に合わないケースが多い。また短時間で稼働を停止し、次の新たなサイトに切り替えるフィッシング手法も一般的となっている。そのため、フィッシング発生時の事後対応においてはフィッシングサイトへのアクセスをブロックする URL フィルターへの登録をいかに迅速に行えるかが、被害抑制の鍵となっている。

フィッシング被害の発見から対応、事後対応までのフローを示す。

（1） フィッシング被害の発見

（2） フィッシング被害状況の把握

（3） フィッシング被害対応活動

- 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被害への対応

（5） 事後対応

下記に各ステップの詳細を記述する。

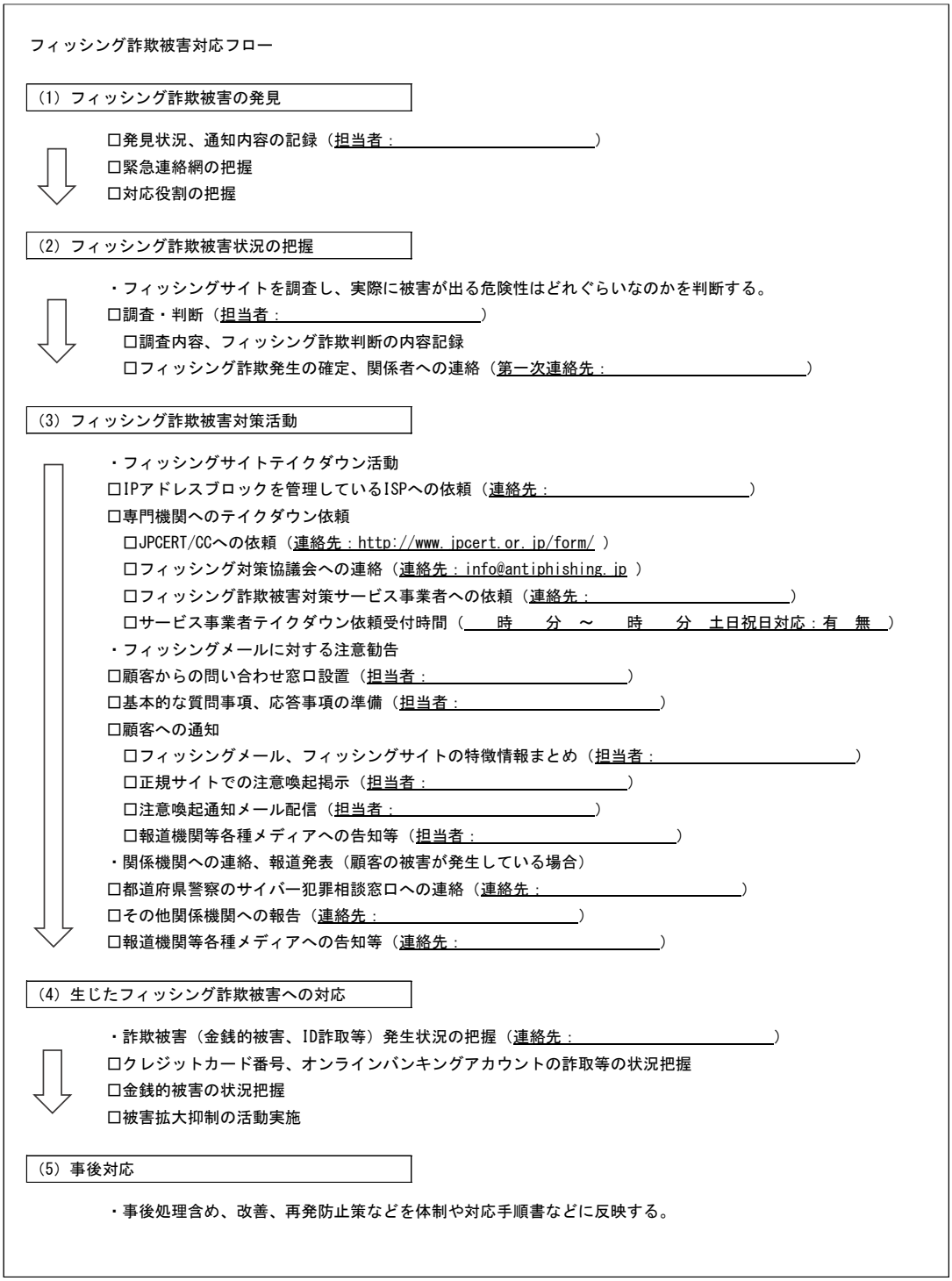


図 8　フィッシング被害対応フロー

### 4.5.1. フィッシング被害状況の把握

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や発見であっても、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、「4.3.1」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や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。近年では管理しているドメイン名をメールアドレスに使用した「なりすましメール」については DMARC 集約レポートの集計、分析により送信規模の把握が可能となっている。管理していないドメイン名を使用したフィッシングメールの場合は、問い合わせ窓口に届いた報告を確認、集計する他、「4.5.5」で示す関係機関への連絡の際にあわせて、一般消費者からの報告数など、状況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。

### 4.5.2. URL フィルターへ登録

URL フィルターでアクセスをブロック、警告表示をすると、フィッシングサイトが稼働していても、被害を抑制することができる。フィッシングサイトの閉鎖には時間がかかるため、まずは URL フィルターへの登録を優先する。

各セキュリティソフトウェア／Web ブラウザーベンダーの Web サイトなどにその報告方法が掲載されているので、フィッシングサイトの URL を迅速に共有できるように準備しておく。

### 4.5.3. 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。

ISP やホスティング事業者は不正行為の報告を受け付ける Abuse 連絡窓口を用意しているので、報告用の Web フォームや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 C 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へ情報共有することが望ましい。また、連絡をしても 1 週間以上フィッシングサイトが停止しない場合は、JPCERT/CC や現地の

CSIRT に支援要請を行う。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可能性があることが理由である。

(2) フィッシング被害対応サービス事業者にテイクダウン依頼を行う

フィッシング被害の備えとしてフィッシング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検知サービスを提供していること、などが考えられる。

(3) 専門機関にテイクダウン支援依頼を行う

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に向けての調整支援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[7]」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ト届け出様式[8]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。

### 4.5.4. フィッシングメール注意勧告

フィッシング被害の発生を 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」「コンピューター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や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、窓口の存在およびアク

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

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、被害発生と拡大を防ぐため、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、公式アプリ内での通知、SNS 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。

利用者への注意喚起を行う際の推奨事項と逆にやってはいけない NG 事項をまとめる。

[注意喚起時の推奨事項]

- いつの情報なのかを明記 : 利用者にとって、検索結果は古い情報もあり、日付をつけることで最新情報であることを明記
- 簡潔に分かりやすく
- 具体例を示しつつも、被害が拡大しないように注意 : 利用者にとって、どんな内容が手元に届くのか、具体的に示すことで、詐欺被害を軽減できる。被害の拡散を抑制するため、詐欺文面のコピーが容易にできない工夫をする（画像掲載）
- 困ってアクセスするユーザー目線で情報提供（たらい回しにしない）

[注意喚起時の NG 事項]

- ユーザーに「URL が正しいかを判断させる」は困難
- 「正しいメールアドレス・送信元の確認」も偽装できるため、NG
- 「正しいドメインから始まる URL だから大丈夫」ではない
- 利用者が誤ってクリックしないよう、フィッシングサイトの URL をそのまま掲載せず、無害化・画像化する


【作成ポイント】

- **掲載日**を明記
- **SMS＝ショートメッセージ**も解説
- どうなる：**情報搾取**
- どうする：**無視**
- **問い合わせ窓口と対象を明確化する**
- **重要情報のみ**掲載（その他は別ページへ）

図 9　Web 掲載用テンプレートの例


【作成ポイント】

- **Twitter**に収まる情報量（140文字以内）
- **情報拡散**してもらいやすく
- **偽物**であることはしっかり示す
- **具体例**も示す（スクショ使用）

図 10　Twitter 通用テンプレートの例

### 4.5.5. 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。

### 4.5.6. 生じたフィッシング被害への対応

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、決済サービスの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。

### 4.5.7. 事後対応

フィッシング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。

# 5. 利用者におけるフィッシング対策

フィッシング対策において、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。

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対策ガイドライン」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。

# 6. 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】 ◎ : 利用者が確認できるように利用環境と分かりやすい説明に配慮した上で、どのように確認すればいいのかを分かりやすく端的に説明すること。

【要件 2】 ◎ : 外部送信用メールサーバー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】 ◎ : 利用者に送信する SMS には国内直接接続の配信、または、RCS 準拠サービスを利用すること

【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】 ◎ : すべてのページにサーバー証明書を導入すること

【要件 7】 ○ : パスワード強度に関するポリシーを利用者に示すこと

【要件 8】 ○ : 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

【 フィッシング被害を拡大させないための対策 】

【要件 9】 ◎ : 利用者に端末を安全に保つよう、注意を促すこと

【要件 10】 ◎ : 複数要素認証を要求すること

【要件 11】 ◎ : ポイントや資産の移動に限度額を設定すること

【要件 12】 ◎ : ポイントや資産の移動時に利用者に通知を行うこと

【要件 13】 ○ : 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 14】 ○ : 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 15】 ○ : 重要情報の表示については制限を行う

【要件 16】 ○ : 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 17】 ◎ : アクセス履歴の表示

【 ドメイン名に関する配慮事項 】

【要件 18】 ◎ : 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 19】 ◎ : 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 20】 ◎ : 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

【 フィッシングへの備えと発生時の対応 】

【要件 21】 ◎ : フィッシング対応に必要な機能を備えた組織編制とすること

【要件 22】 ◎ : フィッシング被害に関する対応窓口を明記すること

【要件 23】 ◎ : フィッシングの手法および対策に関わる最新の情報を収集すること

【要件 24】 ◎ : フィッシングサイトへの対応体制の整備をしておくこと

【 利用者への啓発活動 】

【要件 25】 ◎ : 利用者が実施すべきフィッシング対策啓発活動を行うこと

【要件 26】 ◎ : フィッシング発生時の利用者への連絡手段を整備しておくこと

【 フィッシング被害の発生を迅速に検知するための対策 】

【要件 27】 ○：Web サイトに対する不審なアクセスを監視すること
【要件 28】 ◎：フィッシング検知に有効なサービスを活用すること
【要件 29】 ◎：DMARC レポートやバウンスメールを監視すること

## 付録 B－参考情報

### B.1 【マンガでわかるフィッシング対策 5 ヶ条】

- 「マンガでわかるフィッシング対策 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にあわないための基本的対策事項を案内している）

### B.2 【情報サイト】

- CNET Japan
  https://japan.cnet.com/news/sec/
- ITmedia
  https://www.itmedia.co.jp/news/subtop/security/index.html
- 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/top/digital/pc/pcsecurity/
- 日本サイバー犯罪対策センター
  https://www.jc3.or.jp/

（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）

### B.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/
- 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）

## B.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）

## B.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/programming/index.html（ソフトウェ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）

## B.6 【送信ドメイン認証】

・「SPF（Sender Policy Framework）」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）」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/meiwakumanual3/manual_3rd_edition.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

## B.7 【CSIRT への支援要請】

・「インシデント報告の届け出」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）

## B.8 【Web ブラウザー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

## B.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）

## B.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」
https://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」
https://www.kokusen.go.jp/map/
（各居住地の相談窓口一覧が掲載されている）

## B.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」
https://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
（マルウェ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）
・「社団法人コンピュータソフトウェ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）

## B.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ーによって、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。

## B.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 C－プロバイダー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 D－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
フィッシング発見の通報や被害に遭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 やミドルウェアの脆弱性対応、サーバー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つ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ー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付きにくくなる。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（通常は同一であるサイトがほとんどだが）極力同一とすることが望ましい。
たとえ両サイトが HTTPS 暗号化通信およびサーバー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、多くのブラウザーは、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、サーバー証明書による Web サイトの正当性は証明されなくなる（錠前マークが表示されない）。Web ページを構成する画像などのすべてのパーツが、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。検討にあたっては、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。

## 付録 E－制作・送信に関するガイドラインに含めるべき内容

制作・送信に関するガイドラインには、以下の内容を含めることが望ましい。

- 利用者に情報を発信する手段（電子メール、SMS、郵送など）
- 利用者に情報を発信するケース（事例など）
- 利用者に情報を発信する時間帯
- 利用者に情報を発信する差出人や件名の書き方
- 利用者に情報を発信する内容の書き方
- 構成や段落、ヘッダー、フッターの形式
- 表現や用語の使い方
- 問い合わせ先
- その他の注意点（ユーザー名、パスワードの確認を行わないなど）
- 利用者が配信を停止するための方法
- 電子メールや SMS で利用者に情報を送信する場合の注意点
- 電子メールを利用する場合は、テキスト形式で作成することが望ましい
- テキスト形式以外を利用する場合は、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して使用する
- 電子メール本文内で、画像表示やボタン型リンクを用いるために、HTML 形式を採用する場合、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

など

# 7. 検討メンバー

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 2022 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 2023 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 |
| 副主査 | 木村 泰司 | 一般社団法人日本ネットワークインフォメーションセンター（JPNIC） |
| | 林 憲明 | 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 |
| | 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 |
| | 島田 美奈 | 株式会社カウリス |
| | 松本 悦宜 | Capy 株式会社 |
| | 加藤 恭久 | GMO ブランドセキュリティ株式会社 |
| | 加藤 孝浩 | TOPPAN エッジ株式会社 |
| | 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 |
| | 立石 聡明 | 一般社団法人日本インターネットプロバイダー協会 |
| | 加藤 雅彦 | 長崎県立大学 |
| | 稲葉 緑 | 情報セキュリティ大学院大学 |
| | 熊沢 明生 | ソフトバンク株式会社 |
| | 長谷川 智久 | キヤノン IT ソリューションズ株式会社 |
| | 村田 充昭 | キヤノン IT ソリューションズ株式会社 |
| | 塚田 晴史 | 株式会社マクニカ |
| | 鈴木 一実 | 株式会社マクニカ |
| | 大川 哲 | 株式会社ボーグテクノロジー |
| | 崎山 康平 | 株式会社 ranryu |
| | 大野 真理 | 株式会社 ranryu |
| | 大谷 なすか | 合同会社 DMM.com |
| | 寺西 一平 | 合同会社 DMM.com |
| | 沖 真也 | NRI セキュアテクノロジーズ株式会社 |
| | 大塚 淳平 | NRI セキュアテクノロジーズ株式会社 |
| | 平塚 伸世 | 一般社団法人 JPCERT コーディネーションセンター |
| オブザーバー | 経済産業省 商務情報政策局サイバーセキュリティ課 | |
| 事務局 | 一般社団法人 JPCERT コーディネーションセンター | |
| | 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） | |