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

2026 年度版

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

序

2025 年度は、フィッシング対策協議会に寄せられたフィッシング報告件数が、月によっては 20 万件を超える状況となった。3 年前には月間 10 万件を下回る水準で推移していたことを踏まえると、被害の裾野はこの数年で大きく拡大していると言える。報告件数の増加は攻撃の活発化を示すとともに、社会全体におけるフィッシングの脅威が常態化している現状を浮き彫りにしている。

また、本年度は証券口座の乗っ取りにより高額な被害が発生する事案が相次いだほか、生成 AI を活用した自然な文章表現や個別最適化されたメッセージによる攻撃の巧妙化も顕著となった。従来の不自然な日本語や明らかな誤りを手掛かりに判別することが難しくなり、この点についての注意喚起のみでは被害を防ぎきれない状況になっている。

制度面においても重要な動きがあった。2025 年 9 月には総務省より「フィッシングメール対策の強化に関する要請」が公表され、同年 10 月には日本証券業協会において「インターネット取引における不正アクセス等防止に向けたガイドライン」が改定された。フィッシング対策は、個々の事業者の自主的な取り組みにとどまらず、業界横断的な枠組みの中で強化されつつある。

本ガイドラインは、こうした情勢の変化を踏まえ、フィッシング対策協議会 技術・制度検討 WG において検討を重ね、改定を行ったものである。2025 年度において項目構成の整理を行ったことを受け、2026 年度版ではその枠組みを基礎として各項目の内容を精査・更新した。

- 前年度に整理した項目構成に基づき、各事項の詳細説明を更新
- 特定の技術や方策の単なる推奨よりも、それらが必要とされる背景や想定リスクの説明を簡潔に記述

フィッシング対策は、技術的措置のみならず、組織としてのリスク認識を含む総合的な取り組みである。本ガイドラインが、オンラインサービスを提供する事業者にとって、現状を見つめ直し、対策を強化するための一助となれば幸いである。

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 1

1.1 本ガイドラインの想定読者および目的 1
1.2 本ガイドラインの対象としない領域 1
1.3 本ガイドラインの構成と使い方 1
1.3.1 Web サイト運営者が考慮すべき要件一覧 2
1.4 付録について 3

2. フィッシング対策ガイドライン重要 5 項目 4

3. WEB サイト運営者におけるフィッシング対策 7

3.1 Web サイト運営者におけるフィッシングの被害とは 7
3.2 利用者を守るためのフィッシング対策とは 7
3.3 フィッシング被害の発生を抑制するための対策 8
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 9
3.3.2 利用者が正規サイトを判別可能とする対策 10
3.3.3 フィッシング被害を拡大させないための対策 11
3.3.4 ドメイン名に関する配慮事項 11
3.3.5 フィッシングへの備えと発生時の対応 12
3.3.6 利用者への啓発活動 13
3.4 フィッシング被害の発生を迅速に検知するための対策 13

4. フィッシング対策マニュアル 14

4.1 利用者がフィッシングを識別可能にするための対策 14
4.1.1 送信ドメイン認証への対応 14
4.1.2 利用者宛メールに関するガイドラインの策定・遵守 15
4.1.3 ドメイン名の管理 16
4.1.4 利用者への周知 18
4.1.5 利用者への注意喚起・環境整備の推奨 22
4.2 フィッシング被害を拡大させないための対策 23
4.2.1 多要素認証の採用 23
4.2.2 資産の移動における限度額設定と通知 25
4.2.3 追加のセキュリティ要求 25
4.2.4 フィッシングサイトへの対応体制の整備 25
4.2.5 フィッシング検知に有効なサービスの活用 26
4.2.6 Web サイトに対する不審なアクセスの監視 26
4.2.7 DMARC レポートやバウンスメールの監視 26

4.2.8 フィッシングに関わる最新情報の収集 27
4.3 フィッシング被害が発生してしまった際の対応と対策 27
4.3.1 フィッシング被害状況の把握 29
4.3.2 URL フィルターへ登録 29
4.3.3 フィッシングサイトのテイクダウンまたは無効化 29
4.3.4 フィッシングメール注意勧告 30
4.3.5 関係機関への連絡、報道発表 33
4.3.6 生じたフィッシング被害への対応 33
4.3.7 事後対応 33
5. 利用者におけるフィッシング対策 34
6. 付録 35
付録 A－フィッシングに関する基礎知識 35
付録 B－SMS（ショート・メッセージ・サービス）を利用したフィッシング 39
付録 C－用語集 42
付録 D－参考情報 45
【マンガでわかるフィッシング対策 5 ヶ条】 45
【情報サイト】 45
【業界団体と各省庁のサイト】 45
【安全な Web サイトの利用】 46
【サイトの脆弱性対策】 46
【送信ドメイン認証】 46
【CSIRT への支援要請】 47
【Web ブラウザーのフィッシングサイト対策機能】 47
【フィッシング 110 番】 47
【国民生活センター・消費生活センター】 48
【その他の一般向け相談先】 48
【STOP. THINK. CONNECT. キャンペーン】 49
【フィッシング対策協議会】 49
付録 E－プロバイダーへのテイクダウン要請文例 50
付録 F－事業者における NG 集 51
付録 G－作成・送信に関するガイドラインに含めるべき内容 53
付録 H－フィッシング対策チェックリスト 54
7. 検討メンバー 57

本ガイドラインの改定および公開は、一般社団法人 JPCERT コーディネーションセンターが経済産業省より委託を受けた「サイバーセキュリティ経済基盤構築事業（サイバー攻撃等国際連携対応調整事業）」の一環として実施したものです。

1. はじめに

本章では、本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。本ガイドラインで用いられているフィッシングの基本的な概念や用語については付録を参照いただきたい。

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利用者および Web サイト運営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している。

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。

- 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 Web 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 本ガイドラインの構成と使い方

本ガイドラインは第 2 章に本 WG メンバーによって特に重要として選ばれた項目が挙げられている（表 1-1）。Web サイト運営者など、フィッシングに対する対策を事前に行うためには第 2 章の「重要項目」が守られているかをまず確認いただきたい。その詳細やより強い対策を講じるためには第 3 章の各項目を参照いただきたい。フィッシング被害が発生してしまった際についてまとめられているのは第 4 章である。

[1] https://www.ipa.go.jp/security/vuln/websecurity/about.html

[2] https://security-shien.ipa.go.jp/

表 1-1 フィッシング対策ガイドライン重要項目（第 2 章）

重要項目 1	利用者に送信するメールでは送信者を確認できるような送信ドメイン認証技術等を利用すること
重要項目 2	利用者に送信する SMS においては、国内の携帯キャリアに直接接続される送信サービスを利用し、事前に発信者番号等を Web サイトなどで告知すること
重要項目 3	フィッシング耐性を有する多要素認証を要求すること
重要項目 4	ドメイン名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
重要項目 5	フィッシングについて利用者に注意喚起すること

1.3.1 Web サイト運営者が考慮すべき要件一覧

第 3 章に書かれている要件項目を以下に示す。「◎」は考慮を必須とする項目であり「〇」は考慮を推奨する項目である。

【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	◎	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 2	◎	利用者へのメール送信では、作成・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 3	◎	利用者に送信する SMS には国内直接接続の配信、ならびに携帯キャリア共通番号（0005）を利用すること

【フィッシング被害を拡大させないための対策】

要件 4	◎	フィッシング耐性を有する多要素認証を要求すること
要件 5	◎	アクセス履歴参照機能を利用者に提供すること

【ドメイン名に関する配慮事項】

要件 6	◎	ドメイン名を自社のブランドとして認識し、利用者への周知と維持に継続的に取り組むこと

【フィッシングへの備えと発生時の対応】

要件 7	◎	フィッシングに対応できる組織を編制すること
要件 8	◎	フィッシング被害に関する対応窓口を明記すること

【利用者への啓発活動】

要件 9	◎	利用者が実施すべきフィッシング対策に向けた啓発活動を行うこと

【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 10	〇	フィッシングの発生を検知できるように監視すること

1.4 付録について

付録には利用者への注意喚起に利用しやすいサイトや最新情報のリンク集「参考情報」もある。

付録 A	フィッシングに関する基礎知識
	… フィッシングの手口やそのメカニズムが解説されている。
付録 B	SMS（ショート・メッセージ・サービス）を利用したフィッシング
	… 架空請求などのメカニズムや発信番号の違いが解説されている。
付録 C	用語集
付録 D	参考情報
付録 E	プロバイダーへのテイクダウン要請文例
付録 F	事業者における NG 集
付録 G	制作・送信に関するガイドラインに含めるべき内容
付録 H	フィッシング対策チェックリスト

2. フィッシング対策ガイドライン重要 5 項目

以下に、重要 5 項目を解説する。

重要項目[1] 利用者に送信するメールでは送信者を確認できるような送信ドメイン認証技術等を利用すること

悪質なフィッシングメールの中に送信者（From:）を騙ったものがある。利用者等がフィッシングメールを判定可能にするためには DMARC 等の送信ドメイン認証技術を利用し、メールにおける送信者のドメイン名を詐称されないようにすることが対策の第一歩となる。具体的には DMARC ポリシーの設定において、「p=reject」（排除）を設定することを推奨する（要件 1 および 4.1.1 参照）。これにより利用者に正規メールのドメイン名を確認させることの効果が担保できるようになる。

なお、送信者が正規かどうかを分からないようなメールのドメイン名を利用すると、この技術導入の効果は期待できなくなる。重要項目 4 を参照のこと。

送信ドメイン認証技術の導入によって、スマートフォン等においてブランドのマークが表示される認証マーク証明書（VMC）やブランドアイコンが表示される Web メールのサービスが利用可能になる。これらによってドメイン名の知識のない利用者にも送信者が確認できるようになるため、本ガイドラインではこれらの導入も推奨する。

【フィッシング対策ガイドラインの参照箇所】
◎要件 1　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
マニュアル 4.1.4　利用者への周知 (1) 利用者への周知の良い例・悪い例

重要項目[2] 利用者に送信する SMS においては、国内の携帯キャリアに直接接続される送信サービスを利用し、事前に発信者番号等を Web サイトなどで告知すること

Web サイト運営者は、SMS を使って利用者にメッセージを送る際、フィッシングに利用されることが少ない国内直接接続の SMS 配信や携帯キャリア共通番号（0005）、RCS 準拠サービス等を利用し、事前に発信者番号や送信内容等を Web サイトなどで告知することが重要である。これにより SMS の受信側での判別が容易になることで到達率が高まるほか、発信側でもキャリアごとに異なる番号を伝える必要がないため管理負荷が軽減されるメリットがある。

【フィッシング対策ガイドラインの参照箇所】
◎要件 3　利用者に送信する SMS には国内直接接続の送信、ならびに携帯キャリア共通番号（0005）を利用すること

付録 B　「SMS（ショート・メッセージ・サービス）を利用したフィッシング」

重要項目[3] フィッシング耐性を有する多要素認証を要求すること

「フィッシング耐性」とは、中間者攻撃によるフィッシングの影響を受けることなく認証を行うことができる能力のことをいう（用語集参照）。フィッシングを行う者（フィッシャー）が不正に知り得たログイン情報（クレデンシャルと呼ぶ）だけでログインできないようにすることは、フィッシング被害が起きないようにするために重要である。そのためには、ユーザー認証を行う際にフィッシング耐性を持つ多要素認証（パスキー、生体認証、耐性を有するワンタイムパスワード等）で本人確認を行うようにすることが必要である。

あわせて、これらの認証方式を利用できない場合の代替手段についても、フィッシング耐性を有する認証方式を用いることが適切である。【フィッシング対策ガイドラインの参照箇所】
◎要件 4　フィッシング耐性を有する多要素認証を要求すること
マニュアル 4.2.1　フィッシング耐性を有する多要素認証の採用

重要項目[4] ドメイン名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。特に、十分な管理がなされず失効した自社ドメインが悪用される事例が絶えず発生しており、自社ブランドの毀損を招くことからも留意が必要である（要件 6 参照）。

また管理下のドメイン名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）ドメイン名や、保有しているだけのパークドメイン名は、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】
◎要件 6　ドメイン名を自社のブランドとして認識し、利用者への周知と維持に継続的に取り組むこと
マニュアル 4.1.3　ドメイン名の管理
マニュアル 4.1.4　利用者への周知

重要項目[5] フィッシングについて利用者に注意喚起すること

フィッシングが定常的に発生している場合は、利用者がいつでも情報にたどり着けるよう、トップページなどにリンクを掲載しておく。フィッシング被害が急増したり、手法が変化したりした場合は、新たに情報を掲載して注意を呼びかけることも検討すること。

【フィッシング対策ガイドラインの参照箇所】
◎要件 8　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 9　利用者が実施すべきフィッシング対策に向けた啓発活動を行うこと
マニュアル 4.1.5　利用者への注意喚起・環境整備の推奨

3. 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。

【対策事項の実施必要性】
◎： 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。

3.2 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示す。

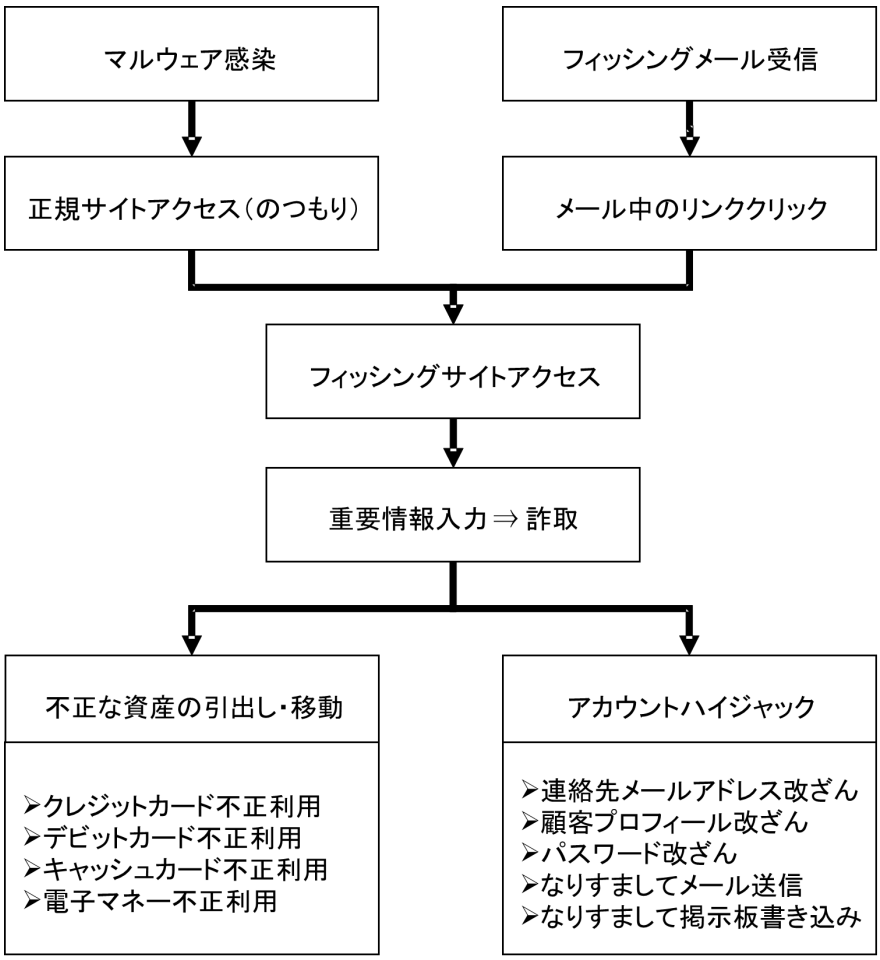


図 3-1　利用者サイドでのフィッシング被害発生フロー

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。

3.3 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。

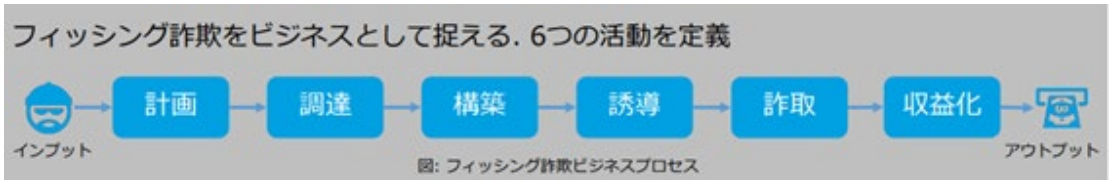


図 3-2　6 つの活動

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）

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】　◎：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（Sender Policy Framework）、DKIM（Domain Keys Identified Mail）、DMARC の送信ドメイン認証に対応し、さらに DMARC（Domain-based Message Authentication, Reporting & Conformance）による、なりすましメールに対する受信制御ポリシーを“reject”に設定することが望ましい。

DMARC を導入していても、ポリシーが「p=none」では意味をなさない。送信ドメイン認証の条件を満たせない電子メールが存在するなどにより、直ちに「p=reject」に設定することが困難な場合は、まず「p= quarantine」（隔離）の設定とし、最終的に「p=reject」を目指すことが適切である。

【要件2】　◎：利用者へのメール送信では、作成・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。

【要件3】	◎：利用者に送信する SMS には国内直接接続の送信、ならびに携帯キャリア共通番号（0005）を利用すること

SMS（Short Message Service）を利用したフィッシングでは、SMS の送信元がアルファベット、海外国番号を含むものが過去から使われてきたが、最近ではマルウェアに感染した個人のスマホなどから 090、080、070 で始まる 13 桁の携帯電話番号が送信元として利用されるケースが急速に増えている。そのため、企業活動として利用者に配信する SMS には、第三者のなりすましが困難な国内直接接続の SMS 送信サービスを利用し、事前に発信者番号や送信内容等を自社の Web サイトなどで、告知する対策が有効である。

しかしながら、受信した利用者のすべてが Web サイトを確認することは期待できないため、利用者による判別が容易な送信元として、2023 年 1 月から全携帯キャリア対応となった 0005 で始まる 10 桁の番号を利用することも有効である [3]。加えて、SMS の次世代版といえる RCS（Rich Communication Service）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」を送信元に表示する仕組みが用意されている。利用者にとって、より詐欺の判別がしやすい UI であることから、あわせて活用することが有効である。

3.3.2 利用者が正規サイトを判別可能とする対策

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。

[3] 携帯キャリア共通番号を活用している企業が以下のページで確認できる。
SMS 共通番号/共通ショートコード情報　https://japansms.com/

3.3.3 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4】　◎：フィッシング耐性を有する多要素認証を要求すること

フィッシングを行う者（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、ユーザー認証を行う際に、リアルタイムフィッシング攻撃などの高度な脅威に対抗するため、フィッシング耐性を持つ多要素認証（パスキー、生体認証、耐性を有するワンタイムパスワード等）で本人確認を行うようにすることが必要である。また、フィッシャーが被害者になりすましてパスキー等の登録をすることを防ぐため、初期登録の際は本人であることの確認を厳格に行うことが望ましい。

あわせて、これらの認証方式を利用できない場合（例：パスキーを登録したデバイスの紛失、怪我等で生体認証を利用不可の場合等）の代替手段についても、フィッシャーによる悪用を防ぐためにフィッシング耐性を有する認証方式を用いることが適切である。

【要件5】　◎：アクセス履歴参照機能を利用者に提供すること

利用者が気付かないうちにサイトを勝手に利用された痕跡を知るために、利用者がそのサイトへの過去のサービス利用履歴（複数回）を確認できるようにする。アクセス履歴にはユーザーアクション、接続時刻、接続時間、接続端末（PC、スマートフォンなど）情報を含めること。

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6】　◎：ドメイン名を自社のブランドとして認識し、利用者への周知と維持に継続的に取り組むこと

Web サイト運営者は、ドメイン名を自社のブランド戦略の一貫として考え、自社のブランドガイドラインに含めるとともに、内部統制のプロセスの中に含めることを関

係部署等に要求することを推奨する。また、名前については社名や認知されているブランド名など利用者が認知しやすいドメイン名を使うこと。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）は、同一のドメイン名の利用が推奨される[4]。一度登録したドメイン名は広く認知してもらうため、長く継続利用するのが望ましい。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。

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。特にドメイン名廃止は、廃止後に悪意のある組織に再登録（ドロップキャッチ）され、悪用される可能性があるので、廃止は慎重な判断が求められる。

3.3.5 フィッシングへの備えと発生時の対応

【要件7】　◎：フィッシングに対応できる組織を編制すること

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。

「4.3 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）を策定した上で、この対応が可能な体制を構築する。

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8】　◎：フィッシング被害に関する対応窓口を明記すること

[4] やむを得ず異なるドメインを利用する場合の対策は、4.1.4 を参照のこと。

自サービスに関するフィッシングメールやSMSの配信やフィッシングサイト発見に関する情報をいちはやく収集するため、利用者からの情報提供を受けるフィッシング報告窓口（コールセンターや他目的の窓口との兼用で差し支えない）を設けておくことが望ましい。

また、フィッシングで盗まれた情報の不正利用により、利用者に多大な被害が及ぶサービス（金融系、クレジットカード系、キャッシュレス決済サービス等）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。

3.3.6 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9】　◎：利用者が実施すべきフィッシング対策に向けた啓発活動を行うこと

利用者は正規のメールおよびSMSか否かを判断する必要があるため、その助けとなるようフィッシングに関する注意喚起や啓発を行うことが重要である。また、フィッシング手法は日々変化しているため、掲載後の内容は少なくとも毎年見直しを行い、啓発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参画することが望ましい。

3.4 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10】　○：フィッシングの発生を検知できるように監視すること

例えば、Web サイトに対する不審なアクセス、DMARC レポートやバウンスメールを監視することが挙げられる。フィッシング検知に有効なサービスを活用することも考えられる。

4. フィッシング対策マニュアル

本節は前節までに述べたガイドライン項目を実施するために必要な手順や情報について述べます。

4.1 利用者がフィッシングを識別可能にするための対策

4.1.1 送信ドメイン認証への対応

利用者に届く前にフィッシングを制御する方法として、SPF、DKIM、DMARC、BIMI といった送信ドメイン認証への対応が有効である。

SPF は送信元メールサーバー（IP アドレス）の認証を、DKIM 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、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 認証を満たすためには、SPF 認証と SPF アライメント、または DKIM 認証と DKIM アライメントのいずれかを満たす必要がある。SPF アライメントを満たすためには、From:ヘッダーのドメイン名と return-path ヘッダーのドメイン名の一致、DKIM アライメントを満たすためには、ヘッダーFrom のアドレスが、DKM 署名の「d=」で指定したドメイン名と一致する必要がある。

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。

<table>
<tr><th colspan="6">送信ドメイン認証技術</th></tr>
<tr><th colspan="2">SPF</th><th colspan="2">DKIM</th><th colspan="2">DMARC</th><th>BIMI</th></tr>
<tr><td colspan="2">正規のサーバー（IPアドレス）から送信されたかを検証</td><td colspan="2">電子署名でメールを検証。メールヘッダー情報やメール本文も署名対象にできる</td><td colspan="2">SPFとDKIMの検証結果を使って検証。認証に失敗したメールの挙動を定められる</td><td>正規メールであることをユーザーが視認できる

適切に認証されたメッセージの横にブランド固定のインジケーターを表示するための規格</td></tr>
<tr><td>アライメント
不一致</td><td>アライメント
一致</td><td>第三者署名</td><td>アライメント
一致</td><td>監視モード</td><td>制御モード</td><td rowspan="2">DMARCポリシー
quarantine または reject</td></tr>
<tr><td>ヘッダ From ドメイン：企業ドメイン

エンベロープ From ドメイン：配信サービスドメイン</td><td>ヘッダ From ドメイン
＝
エンベロープ From ドメイン</td><td>ヘッダ From ドメイン：企業ドメイン

DKIM署名ドメイン：配信サービスドメイン</td><td>ヘッダFromドメイン
＝
DKIM署名ドメイン

（DKIMヘッダのd=タグ）</td><td>DMARCポリシー
p=none

DMARC レポートを定期的に検証して、メールがどのように認証、配信されているかを確認</td><td>DMARCポリシー
p=quarantine
隔離させる

p=reject
受信を拒否する</td></tr>
</table>

図 3-1　送信ドメイン認証技術の比較

4.1.2 利用者宛メールに関するガイドラインの策定・遵守

利用者宛メール関するガイドラインを策定し、社内・組織内がガイドラインに則ってメール作成・送信を行うことで、利用者がフィッシングメールに気付きやすくなる。

メール作成・送信に関す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、多岐に亘る内容を盛り込むことが望ましい。

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：無害なリンク）。

利用者に無用なリスクを負わせないとの観点から、Web サイト運営者が利用者に送信するメールにはリンク URL を記載しない、もしくはテキスト形式で作成することで利用者による識別を容易に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名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名を使って「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。

4.1.3 ドメイン名の管理

（1）ドメイン名に関する基本情報

自社のドメイン名を登録するトップレベルドメイン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[5]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"[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。

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であるが、知識のある利用者や、フィッシング対応を行う国内外のベンダー、調査機関、事業者、アナリスト等に正規ドメインと用途（サービス名）を示すことは、誤判定や不明と判断されることを防止できる。

（2）適切なドメイン管理のための留意事項

企業において登録・利用するドメイン名を適切に管理するためのルール・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
- ドメイン名に関する各種連絡先情報の管理
- 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】

---

[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/

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、サブドメイン名は一般的に親ドメイン名の管理に統合し集中管理しやすいが、設定が複雑になり、親ドメイン名の設定状況に影響を受ける可能性がある。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の管理】

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。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。他サイトに掲載されているリンク等は、もれなく削除または変更依頼を行う必要がある。廃止されたドメイン名は一定期間後に第三者が当該ドメイン名を新たに登録することが可能となり、これを狙って登録を行う行為はドロップキャッチと呼ばれる。特に正規サービスで使用されていたものは「優良中古ドメイン名」としての価値があるため、オークションにかけられたり、不審なサイトを運営されたりするリスクがある。近年。ドロップキャッチされたドメイン名を高額で買い戻し、注意喚起を行うなどの事例も発生した。

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、サービス終了後、最低 10 年程度は継続手続きを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、ドメイン名更新よりもはるかに高額の費用や時間がかかってしまう可能性が高く、また、確実に取り戻せる保証はない。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名を乗っ取り（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。

4.1.4 利用者への周知

(1) 利用者への周知の良い例・悪い例

実施した対策を有効に機能させるためには、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必要がある。説明の仕方によっては利用者が誤解し、逆に攻撃者に悪用されるリスクを高める恐れもある。

ここでは、利用者にどのような情報をどのように伝えればよいのかについて、具体的な文面例を示しながら、わかりやすい伝え方を解説する。これにより、事業者が利用者への注意喚起をより効果的に実施し、フィッシング詐欺による被害を軽減できることを目指している。

【良い例 1】 公式サイトや正規アプリへの正しい導線を明確に提示する

フィッシングメールや不正サイトは、本物そっくりの URL やアプリを使って利用者を騙そうとする。利用者が「どれが本当の正規サイトやアプリなのか」をひと目でわかるように導線を用意することで、誤って偽物にアクセスするリスクを減らすことができる。また、不審なリンクが拡散されるリスクを考慮して、あえて URL を記載しない手法も有効である。

記載例

本システムではフィッシング対策の一環として、特定の URL を直接掲載しておりません。詳細につきましては、XXX 銀行の Web サイト内「YYY メニュー」からご確認いただけます。安全にアクセスするためには、事前にブックマークを設定しておくことをおすすめします。

【良い例 2】アカウント情報（ID やパスワード）の取り扱いに注意を促す

フィッシング詐欺の狙いは、利用者の ID やパスワードなどの認証情報を盗み取ることにある。メールや SMS で届く URL に利用者を誘導し、ログイン情報を入力させる手口は多くの被害をもたらしている。そこで、「パスワードは他人に絶対に教えない」「パスワードを使い回さない」「リンクを踏む際は本当に正規サイトかを確認する」といった基本的な注意喚起を徹底することが大切である。

記載例

当社がメールやSMSでお客さまのパスワードをお尋ねすることは一切ございません。万が一、不審なメッセージを受け取った場合は、リンクをクリックせずにご自身でブックマークした公式サイトから再度ログインし、状況をご確認ください。ID やパスワードは家族や友人であっても他人と共有しないようお願い申し上げます。当社以外のサービスに同じパスワードを設定することも避けてください。

【良い例 3】実際に確認された攻撃被害の発生事実を紹介しつつ、具体的な手口や注意点を分かりやすく示す

実例を交えて注意喚起をすることで、フィッシングが巧妙に行われ得ることを利用者が理解し、「自分も被害に遭うかもしれない」と認識しやすくなる。ただし、被害に使われたフィッシング URL や送信元アドレスをそのまま掲載すると、不用意にクリックされる恐れや二次拡散のリスクがあるため、一部加工（伏せ字など）を施すなどの配慮が必要となる。

記載例

偽の銀行ロゴを使用したフィッシングメールが多数確認されています。件名には「ご本人確認のお願い」という文言が含まれ、本文から偽サイトへ誘導される手口が確認されました。リンク先の URL は本物と見分けがつきにくいため、必要以上にクリックしな

いようご注意ください。少しでも不審に感じる場合は、普段からご利用の正規サイトに直接アクセスしてご確認ください。

【良い例 4】 外部の公的機関や業界団体が発行する注意喚起情報・公式資料を適切に参照する

フィッシング詐欺は手口が絶えず変化しており、公的機関や業界団体が最新の対策情報を随時更新している。事業者独自の情報提供だけでなく、第三者機関の公式情報を案内することで、利用者が追加の知識を得やすくなる。これらの正規サイトへのリンクを示す際には、利用者がアクセス先を間違えないようアドバイスすることが重要である。

記載例

フィッシング対策に関する最新の手口や注意点については、警察庁や金融庁などの公的機関でも詳しく案内しています。ご不安な場合は、XXX 銀行だけでなく、フィッシング対策協議会の公式情報もあわせてご覧いただくと、より詳細な対策を確認できます。リンクの正否を確かめるためにも、検索エンジンを使う、あるいは公的機関の名称を正しく入力して公式サイトへアクセスする方法をおすすめします。

【悪い例 1】「URL が正しいかどうかを自分で確認してください」と呼びかける

URL を目視でチェックするのは難しく、攻撃者の巧妙な偽装を見破るのは容易ではない。HTML メールなどでは表示されている URL と実際のリンク先が違うケースも多いため、利用者に「自分で正しいか判断してからクリックして欲しい」と伝えるだけでは被害を防ぎきれないことを認識する必要がある。

悪い記載例

最近、不審なメールが多数報告されています。怪しいと思ったら、まずは本文に記載の URL が「https://www.a-bank.example.com/」など、当行の正しい URL になっているかどうかをよく確認してください。もし表示されている URL が当行のドメインと似ていれば、そのままクリックしていただいて構いません。

【悪い例 2】「メールアドレスや送信元が正しいか確認してください」と呼びかける

攻撃者はメールの送信元（From）を偽装できるため、同じ組織でも複数の正規アドレスを使う可能性がある。利用者が「送信元アドレスが合っていれば本物」と思い込むと、似たドメインや文字列を使った詐欺メールを見抜けないリスクが高まってしまう。

悪い記載例

当社では、公式メールアドレスとして「info@a-bank.example.com」「support@a-bank.example.com」のみを利用しております。もし届いたメールの送信元が当行のドメイン（@a-bank.example.com）を含んでいれば、正真正銘当社が発信したものです。疑わしいメールを受け取った際も、送信元をチェックするだけで本物かどうかの判別が簡単にできます。万が一、このドメインと違う場合はフィッシングメールの可能性が高いので、削除していただくようお願いいたします。

【悪い例 3】「正規ドメインから始まる URL なら安全です」と案内する

https://a-bank.example.com/ という文字列が含まれていても、それが実際にサブドメインに埋め込まれた偽サイトの可能性がある。利用者が「正規ドメイン部分を見つければ OK」と思い込むと、攻撃者の巧妙なトリックに引っかかりやすくなる。

悪い記載例

当社の正規サイトは「https://a-bank.example.com/」というドメインを利用しています。メールや Web サイトで、この URL が最初に表示されていれば基本的に安全です。例えば下記のように、URL が「a-bank.example.com」で始まっていれば当社のサービスページですので、安心してログイン情報を入力していただいて構いません。

https://a-bank.example.com/users/login

https://a-bank.example.com/account/info

もし似たようなドメインを見かけた場合は、その場で判断して大丈夫です。少しでも違う文字列が混じっていなければ、当社公式サイトと考えられます。

【悪い例 4】「トップレベルドメイン（.com や .jp など）で安全かどうか判断する」と呼びかける

トップレベルドメイン（TLD）が「.com」や「.jp」などであっても、攻撃者は正規登録を偽装したり、似た企業名でドメインを取得して悪用することが可能なことに留意する必要がある。

悪い記載例 もし、不審なメールやサイトを見かけたときは、ドメインの末尾が「.com」や「.jp」になっていればある程度信頼できると判断していただいて構いません。逆に「.xyz」や「.info」など、あまり聞き慣れないトップレベルドメインの場合は詐欺サイトの疑いが高いので絶対にアクセスしないようお願いいたします。

(2) 利用者への周知に関する参考情報

2025 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。

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。

サービスを行っている 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、共通であるほうが利用者にも判りやすいため望ましいが、メール配信設備の都合上、サービスとは違うドメイン名を使用するケースも多いと思われる。その場合は必ず送信ドメイン認証でドメイン名を保護した上で、ドメイン名と用途を公開し、BIMI やブランドアイコン、公式マークのような技術を使い、正規メールの視認性を向上することも検討する。

4.1.5 利用者への注意喚起・環境整備の推奨

（1）利用者が安全にサービスを利用する環境を整えるように促す

利用者がオンラインのサービスの利用環境を安全に保つことはフィッシング対策につながる。注意項目としては次に挙げる内容を含めることが考えられる。

- OS、Web ブラウザーおよびアプリ、ソフトウェアは、お知らせや通知に従って最新の状態に保つこと。
- セキュリティ対策ソフトウェアがインストールされていない場合には、インストールし、機能を有効にして最新状態に保つこと。
- URL を確認することができない利用者や利用環境には URL フィルターを導入すること。
- アプリやソフトウェア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。
- なりすましメール対策や迷惑メール対策が備わったメールサービスを使うこと。そうでない場合には迷惑メールフィルターを利用すること。

なお、オンラインサービスの提供者は、利用者環境において正規サイトの URL が使われたときに正規サイトに接続されるようにしておく必要がある。そのためには DNSSEC や RPKI などのセキュリティ技術を採用している通信事業者やクラウドサービス事業者を利用する。

（2）利用者が実施すべきフィッシング対策に向けた啓発活動を行う

注意喚起や啓発資料は利用者の利用環境（パソコン、スマートフォン等）やインターネットの知識、経験の差を考慮し、正規メールのみに表示されるアイコンなど「見てわかる」方法を中心に、図やスクリーンショット、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。専門用語が入った説明や解説は正しい理解が難しいため、「より詳しく知りたい」と望む利用者への追加情報として掲載する。

「利用者向けフィッシング詐欺対策ガイドライン」や付録 D「安全な Web サイト利用の鉄則」なども参考に作成することが望ましい。

4.2 フィッシング被害を拡大させないための対策

4.2.1 フィッシング耐性を有する多要素認証の採用

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、リアルタイムフィッシング攻撃などの高度な脅威に対抗するため、フィッシング耐性を持つ多要素認証（パスキー、生体認証、耐性を有するワンタイムパスワード等）で本人確認を行うようにすることが必要である。かつてはワンタイムパスワードによる認証を行えばフィッシング耐性があると考えられていたが、利用者に送付されるワンタイム

パスワードをフィッシャーが盗んで悪用するリアルタイムフィッシング攻撃により被害が多発した結果、単にワンタイムパスワードを利用するのみではフィッシング耐性を有するとはいえなくなっている。

多要素認証においてフィッシング耐性を確保するために、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、リアルタイムフィッシングへの技術的な耐性を有する多要素認証方式の導入も検討すべきである。例えばパスキーは、FIDO2 をベースにユーザーの利便性を向上させた認証規格であり、生体認証と認証器の所有認証（スマートフォンや FIDO 認証器など）の二要素を組みあわせて、パスワードレス認証を実現している。フィッシング攻撃は、ユーザーがフィッシングサイトに対して秘密情報を送信することで攻撃が成立するが、パスキーは秘密情報をドメイン名と紐づけて認証器内に保存することから、フィッシングサイト（フィッシングドメイン）に対して正規ドメインと紐づいた秘密情報を送信することはないため、耐フィッシング性が担保される。なお、パスキーの初期登録の際は、フィッシャーによるなりすましを防ぐため、本人確認を厳格に行うことが望ましい。

このほか、フィッシャーは窃取した秘密情報を用いてログイン成功した場合、永続的なログインを可能にするために、多要素認証の無効化や、多要素認証の設定変更（例えばワンタイムパスワードの送信先をフィッシャーのメールアドレスへ変更するなど）を行うことがあるため、ユーザー情報や多要素認証の設定変更時にも同様にフィッシング耐性を有する多要素認証で本人確認するなどの考慮が必要である。また、利用者がパスワードを失念した場合や、PC やスマートフォンの紛失・盗難等で通常の認証操作を行うことができなくなった場合の代替手段（フォールバック）としての認証手段を提供する場合、フィッシャーによる悪用を防ぐためにフィッシング耐性を有する認証方式を用いることが適切である。その他、アカウントの回復手続についても、注意深く設計しないと攻撃者に悪用される恐れがある。

これらのフィッシング耐性の強化に関する対策はセキュリティの確保の上では欠かせないものであるが、一方で利用者の IT リテラシーやデバイス環境の差異により、利用者に対して利便性の観点での著しい格差を生じさせる可能性があるものでもあるため、設計時には十分な配慮が望まれる。

4.2.2 資産の移動における限度額設定と通知

フィッシャーによる利用者の資産（預金やポイントなど）の窃盗被害を抑制するため、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多要素認証などを活用することが望ましい。

資産の移動が小額であっても、移動が行われるたびに、電子メールや SMS、アプリ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。

4.2.3 追加のセキュリティ要求

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や登録情報の変更が行われる場合には、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。

多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。

4.2.4 フィッシングサイトへの対応体制の整備

下記を定め、フィッシングサイトへの対応方法を整備しておくことを推奨する。

- URL フィルターの申告方法（テイクダウンよりも即効性が期待できるため）
- テイクダウンのアプローチ方法（自社、社外業者）
- 発生中のフィッシングサイトを利用者に注意喚起する実施手順

実施方法については、フィッシングが発生してしまった際の対応と対策に関するマニュアル（4.3 4.3.4 ）を参照のこと。

4.2.5 フィッシング検知に有効なサービスの活用

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 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各種情報を 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。

4.2.6 Web サイトに対する不審なアクセスの監視

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名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

4.2.7 DMARC レポートやバウンスメールの監視

自社として【要件 2】DMARC に対応すること以外に、利用者が多い大手メールサービス等から DMARC 集約レポートが返送されてくる場合がある。これらを収集、分析することによって、自社ドメインがなりすましをされているか、また、されていた場合の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。

4.2.8 フィッシングに関わる最新情報の収集

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し、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を推奨する。情報サイトを付録 D に示す。

4.3 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。

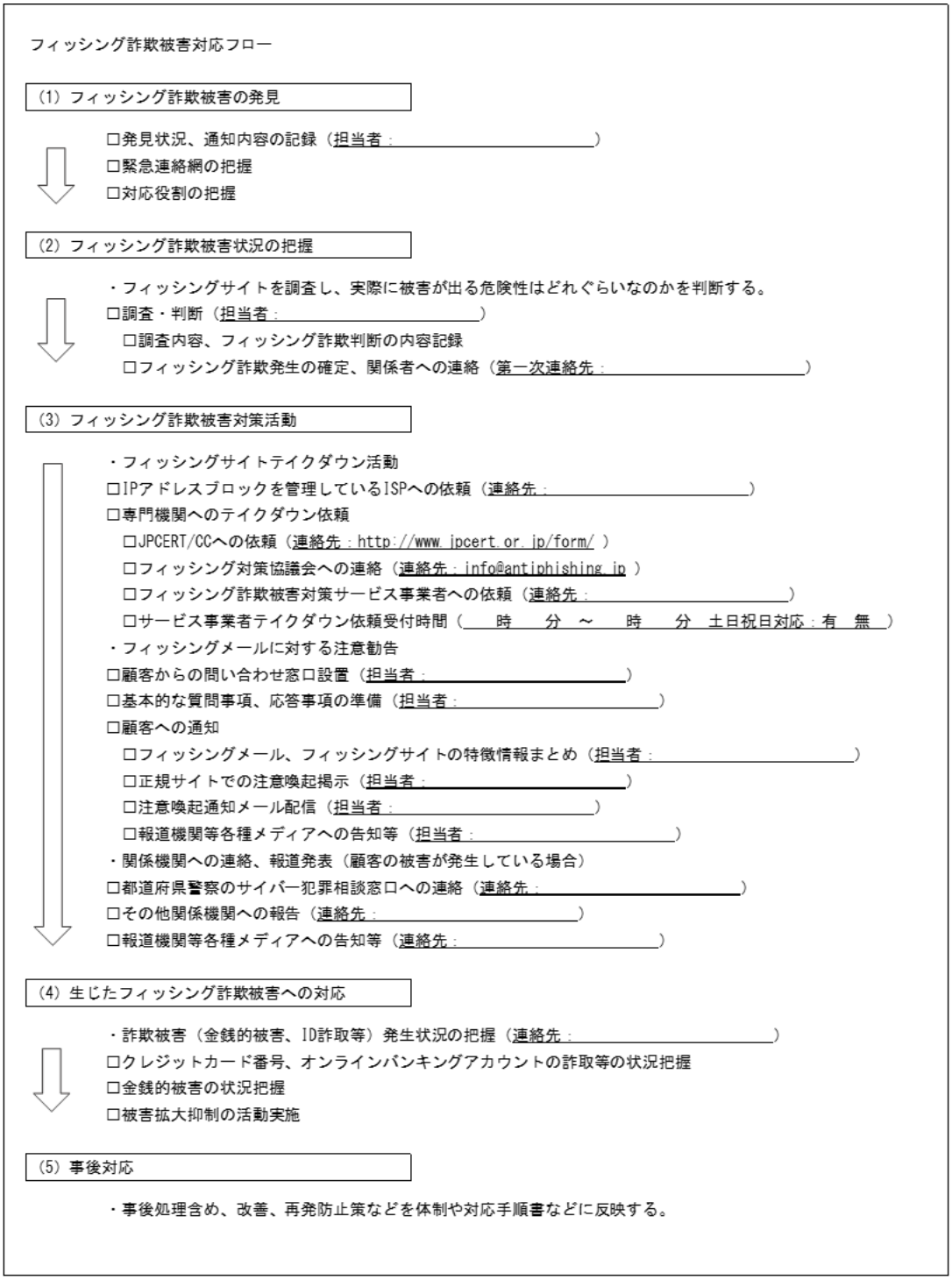


図 4-2　フィッシング被害対応フロー

4.3.1 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、4.1.2 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、4.3.5 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。

4.3.2 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（フィッシングメールの記載されている URL のリダイレクト先の URL）を迅速に共有できるように準備しておく。

4.3.3 フィッシングサイトのテイクダウンまたは無効化

（1）Web サイト運営者自身で Abuse 連絡を行う

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。

また、あわせて、当該フィッシングサイトで用いられているドメイン名の登録削除等を、ドメイン名登録事業者に連絡することも検討する。

ISP、ホスティング事業者やドメイン名登録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 E 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。

4.3.4 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。

7 https://www.jpcert.or.jp/form/

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

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]
NG　ユーザーに「URL が正しいかを判断させる」は困難
NG　「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
NG　「正しいドメインから始まる URL だから大丈夫」ではない
NG　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 4-3　Web 掲載用テンプレートの例

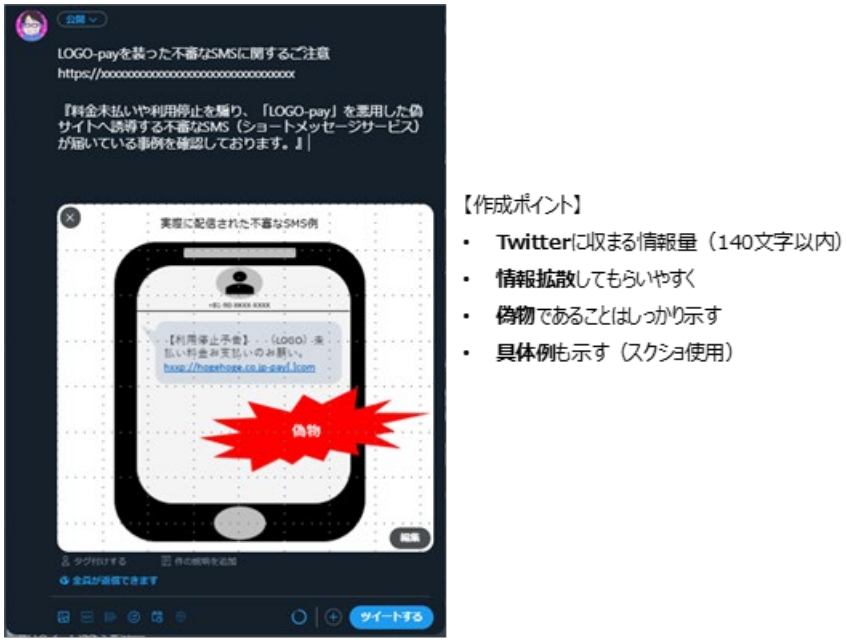


図 4-4　X（旧 Twitter）通用テンプレートの例

4.3.5 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。

4.3.6 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。

4.3.7 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あわせて参照すること。

6. 付録

付録 A－フィッシングに関する基礎知識

フィッシングの手口として、単純な例を図 1 に示す。

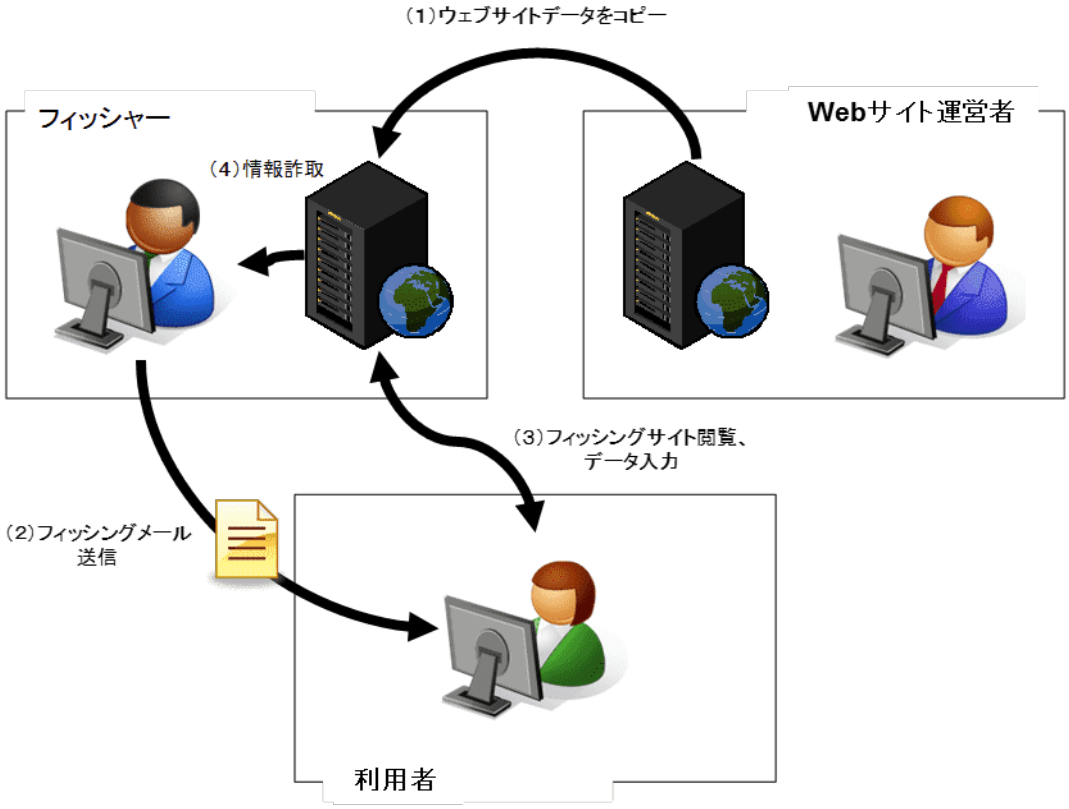


図 1　フィッシングの単純な例

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。

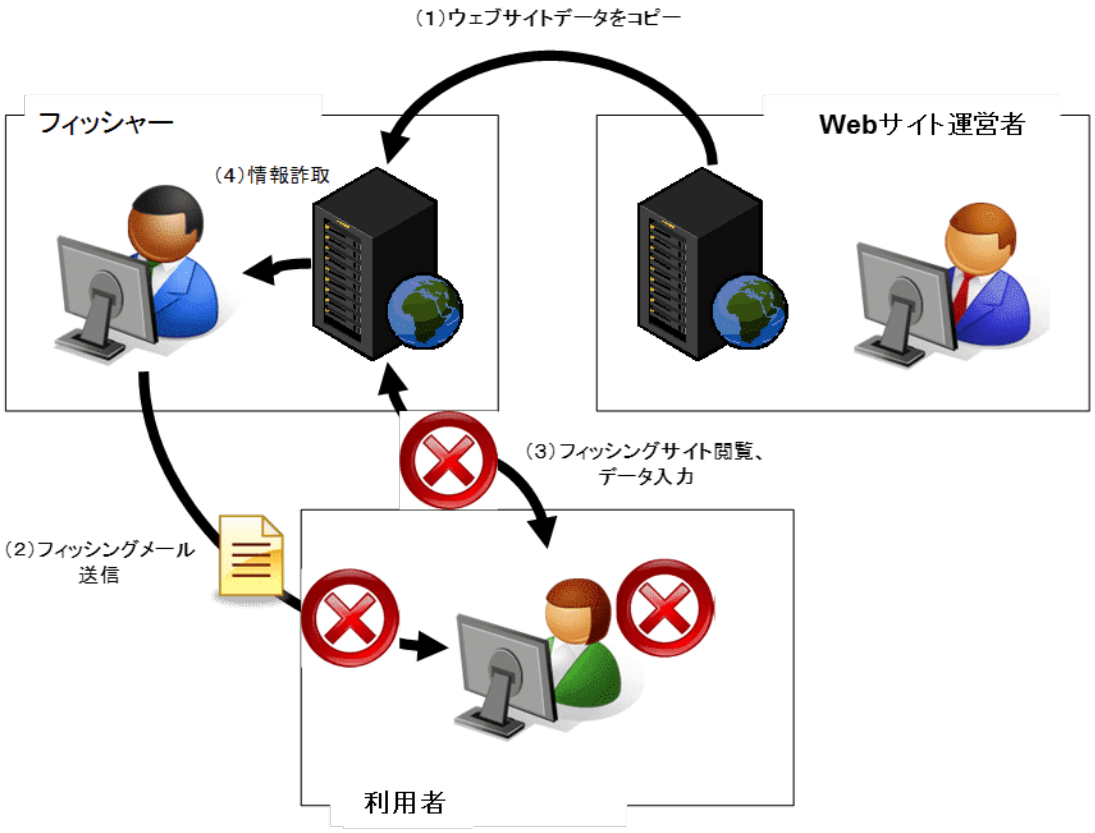


図 2　フィッシング被害の抑止ポイント

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。

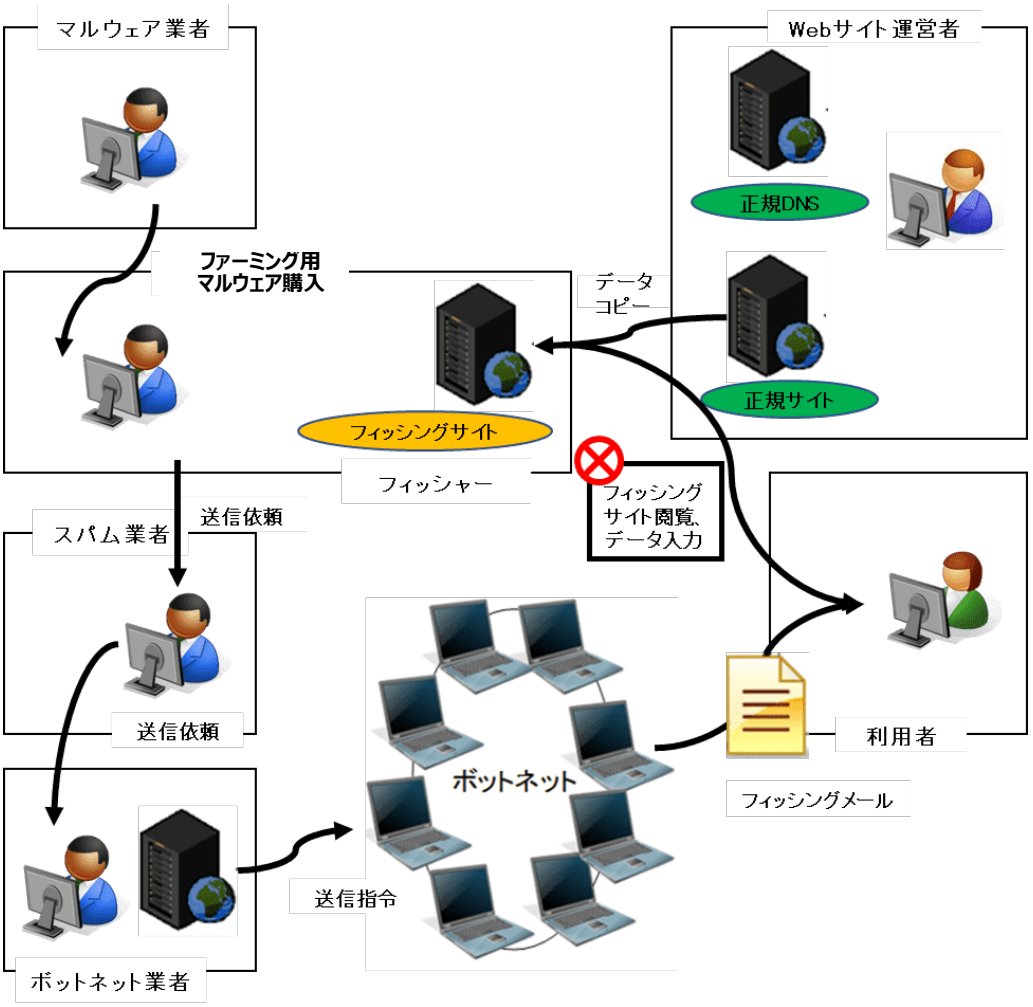


図 3　フィッシングの複雑な例

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無料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。

付録 B－SMS（ショート・メッセージ・サービス）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。

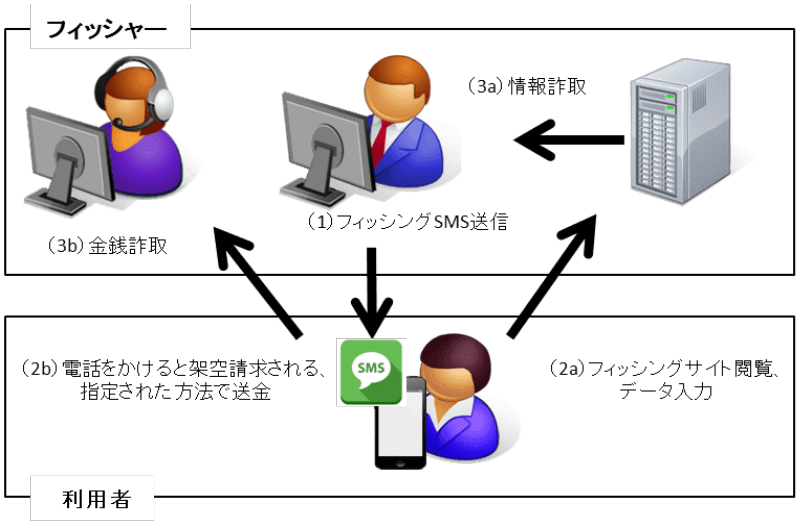


図 4 SMS を利用したフィッシングの例

	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 （例：03-0000-0000） 携帯キャリア共通番号 （例：0005-000000） 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	マルウェアに感染した端末経由も含め、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、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

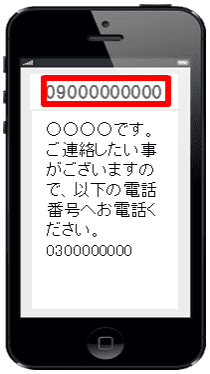
発信者番号の表示イメージ			

図 5 SMS 配信経路ごとの特徴

			国内P2Pルート	海外ルート（国際網・グレールート）	国内A2Pルート（国内直接接続・正規ルート）	参考：日本以外の国
			フィルタリングは行うが、携帯キャリアは利用企業の管理なし	フィルタリングは行うが、携帯キャリアは利用企業の管理なし（＝ホールセール）	携帯キャリアでの事前登録有	
送信元	アルファベット	例）Amaz●n, RAKUT●N, Go●gle ※固有名詞のため、●を利用して記載		Amaz●n、銀行などのなりすまし	携帯キャリアのみ利用可	多数の国で、事前登録を前提に企業が利用
				企業が利用（なりすまし可を許容）		
	海外電話番号	国番号から始まる番号 例）+1XXXXXX（米国の場合）		Amaz●n、銀行などのなりすまし		
				企業が利用（なりすまし可を許容）		
	ショートコード	例）1416, 157 0005から始まる10桁（4キャリア共通） 2から始まる5-6桁（ソフトバンク） 0009から始まる8桁（KDDI）			企業が利用	
	国内電話番号（固定系）	例）03等市外局番から始まる番号 050, 0120から始まる番号			企業が利用	米国では、事前登録を前提にフリーダイヤル利用が一般
	国内電話番号（携帯）	例）090等から始まる13桁	Amaz●n、銀行などのなりすまし（マルウエア感染スマホ、SIMボックス）		双方向SMSで一部利用があり、ショートコードへ移行中	多数の国で、SIMボックスは不正な利用との位置づけ
			企業が利用（コスト重視）			

正規SMS
スミッシング等、不正SMS

図 6　企業から送信される SMS の送信元

付録 C－用語集

【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。

【テイクダウン（take-down）】

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。シャットダウンまたはサイトクローズともいう。

【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。

【パークドメイン】

ドメイン名を登録後、コンテンツが掲載されることなく、ドメイン名を維持するための Web ページ、もしくはそのドメイン名自体を指す。

【パスキー】

FIDO2 をベースにユーザーの利便性を向上させた認証規格であり、生体認証と認証器の所有認証（スマートフォンや FIDO 認証器など）の二要素を組みあわせて、パスワードレス認証を実現している。

【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。

【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。

【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。

【フィッシング耐性】

中間者攻撃によるフィッシングの影響を受けることなく認証を行うことができる能力のこと。具体的な実装方法として、NIST SP800-63-4 ドラフトにおいて、クライアントの秘密鍵をサーバーによって検証するチャネルバイディング（実装例：m TLS）と、検証機の識別子を検証者の名前と結びつける検証者名前バインディング（実装例：パスキー）の 2 つが示されている。[9]

【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。

【フィッシングメール・フィッシング SMS】

実在する組織や Web サービスのお知らせと称したメールや SMS 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。そこでアカウント情報や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。

【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。

【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。

【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

[9] 米国 CISA による参考資料
http://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

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。

【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。

【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。

【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。

【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。

【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。

付録 D－参考情報

【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）

【情報サイト】

・トビラシステムズ（詐欺 SMS モニター）
　https://smon.tobila.com/
・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/
・Security Next
　https://www.security-next.com/
・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）

【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）

【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）

【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）

【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

【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）

【Web ブラウザーへの報告先】

・Microsoft
https://www.microsoft.com/en-us/wdsi/support/report-unsafe-site-guest

・Google
https://safebrowsing.google.com/safebrowsing/report_phish/?hl=ja

【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

【フィッシング 110 番】

・「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）

【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）

【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）

【STOP. THINK. CONNECT. キャンペーン】

・「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。

【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 Email 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 E－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 F－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名、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

・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 G－作成・送信に関するガイドラインに含めるべき内容

作成・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

付録 H－フィッシング対策チェックリスト

重要 5 項目（参照：2.フィッシング対策ガイドライン重要 5 項目）

重要項目 1	◎	利用者に送信するメールでは送信者を確認できるような送信ドメイン認証技術等を利用すること □ メール送信に使うドメイン名について DMARC 等の送信ドメイン認証技術を導入している(必須)。 □ VMC 等のブランドアイコンが表示される仕組みを導入している(推奨)。 □ 送信メールの送信者が正規かどうかわかるように S/MIME を導入している(推奨)。
重要項目 2	◎	利用者に送信する SMS においては、国内の携帯キャリアに直接接続される送信サービスを利用し、事前に発信者番号等を Web サイトなどで告知すること □ 使っている発信者番号を利用者に告知している(必須)。 □ なりすましが起きにくい SMS サービスを利用している(推奨)。
重要項目 3	◎	フィッシング耐性を有する多要素認証を要求すること □ 多要素認証を採用している(必須)。 □ フィッシング耐性を有する多要素認証を構成している(推奨)。
重要項目 4	◎	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 □ 自組織に割り当てられているドメイン名を把握している(必須)。 □ ドメイン名のライフサイクル管理をしている。ドロップキャッチの対策をしている(必須)。 □ ある部署もしくは発注先などによって勝手にドメイン名が設けられたり使われたりしないように管理している(必須)。 □ 利用者にサービスで使っているドメイン名を周知している(推奨)。
重要項目 5	◎	フィッシングについて利用者に注意喚起すること □ フィッシング詐欺が起きている場合にはその旨を周知している(必須)。 □ フィッシング詐欺についての注意喚起を行う Web ページ等を設けている(推奨)。

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	◎	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 □ 外部送信用のメールサーバーは SPF、DKIM、DMARC 等の送信メールドメイン認証技術に対応している。 □ BIMI を導入している。
要件 2	◎	利用者へのメール送信では、作成・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 □ 社内や組織内でメール作成に関するガイドラインを策定している。

要件 3	◎	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 には国内直接接続の配信、または、RCS 準拠サービスを利用している。

フィッシング被害を拡大させないための対策

要件 4	◎	フィッシング耐性を有する多要素認証を要求すること □ ワンタイムパスワードといった所有認証、指紋や顔認証といった生体認証を組み合わせた多要素認証を求めるようにしている。 □ フィッシング耐性を有する多要素認証を導入している(推奨)。
要件 5	◎	アクセス履歴参照機能を利用者に提供すること □ 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している。 □ アクセス履歴にはユーザーアクション、接続時刻、接続時間、接続端末（PC、スマートフォンなど）およびアクセス元 IP アドレスを含む。

ドメイン名に関する配慮事項

要件 6	◎	ドメイン名を自社のブランドとして認識し、利用者への周知と維持に継続的に取り組むこと □ ドメイン名の管理を関係部署等で内部統制のプロセスの中に含めている。 □ 社名や認知されているブランド名など利用者が認知しやすいドメイン名を使っている。 □ Web サイトで用いるドメイン名および送信するメールの送信者アドレスのドメイン名は同一である(推奨)。 □ ドメイン名管理のためのルール・手順を社内で確立している。 □ ドメイン名の廃止を慎重に判断できる。

フィッシングへの備えと発生時の対応

要件 7	◎	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 □ 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いる。 □ フィッシング被害が発生してしまった際の行動計画（対応フロー）を策定している。 □ フィッシングについて組織内で連絡や連携が取れるようになっている。 □ 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っている。
要件 8	◎	フィッシング被害に関する対応窓口を明記すること □ 利用者からの情報提供を受けるフィッシング報告窓口を設けており、利用者のために明記している。 □ 利用者に多大な被害が及ぶサービス（金融系、クレジットカード系、キャッシュレス決済サービス等）の場合、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している。

利用者への啓発

要件 9	◎	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 □ 正規のメールおよび SMS か否かを判断する助けとなるようフィッシングに関する注意喚起や啓発を行っている。 □ 掲載後の内容を毎年見直している。

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 2025 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 2026 年 2 月時点）。

【主査】

木村 泰司　　一般社団法人日本ネットワークインフォメーションセンター

【構成員】

阿部 巧　　株式会社三井住友銀行
笠間 英宏　　NTT ドコモビジネス株式会社
加藤 孝浩　　TOPPAN 株式会社
加藤 雅彦　　順天堂大学
金井 孝三　　Sky 株式会社
上川 佳一　　株式会社アクリート
栢森 亮輔　　明治安田生命保険相互会社
唐沢 勇輔　　Japan Digital Design 株式会社
鈴木 伸吾　　NTT ドコモビジネス X 株式会社
高山 寛史　　日本証券業協会
竹内 司　　株式会社みずほフィナンシャルグループ
多田 憲治　　日本証券業協会
田中 優成　　株式会社アクリート
張 作庭　　レジル株式会社
塚田 晴史　　株式会社マクニカ
野々下 幸治　　株式会社アイエスエフネット
半戸 祐次　　BC Signpost 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
福地 雅之　　NTT ドコモビジネス X 株式会社
藤井 治彦　　バンクガード株式会社
松尾 佳彦　　株式会社日本レジストリサービス
松本 悦宜　　Capy 株式会社
森 三千代　　株式会社みずほフィナンシャルグループ
八子 浩之　　株式会社みずほフィナンシャルグループ

【オブザーバー】

経済産業省商務情報政策局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
みずほリサーチ＆テクノロジーズ株式会社