※フィッシング対策には最新版ガイドラインをご活用ください

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

2013 年度版

平成 25 年 6 月

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

※フィッシング対策には最新版ガイドラインをご活用ください

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等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、オンラインゲーム等の登録会員制 Web サイトを運営するサービス事業者及び情報セキュリティ関連団体等も、利用者に対してフィッシング詐欺に関する注意喚起とともに被害を避けるための対策方法の啓発を行っている。

フィッシング対策は、利用者向けの対策とサービス事業者向けの対策があるが、サービス事業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、サービス事業者の信用を高め、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、多くのサービス事業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 ガイドライン策定ワーキンググループでは、利用者及びサービス事業者を読者と想定したフィッシング対策ガイドラインを策定することとした。

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

フィッシング対策協議会

ガイドライン策定ワーキンググループ

※フィッシング対策には最新版ガイドラインをご活用ください

目 次

1. はじめに 1

1.1. 本ガイドラインの想定読者及び目的 1
1.2. 本ガイドラインの対象としない領域 1
1.3. 用語解説 1

2. フィッシングに関する基礎知識 3

2.1. フィッシング詐欺の手口 3

3. サービス事業者におけるフィッシング詐欺対策 6

3.1. サービス事業者におけるフィッシング詐欺の被害とは 6
3.2. 利用者を守るためのフィッシング詐欺対策とは 6
3.3. フィッシング詐欺被害の発生を抑制するための対策 7
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 7
3.3.2. 利用者が正規サイトとフィッシングサイトを判別可能とする対策 10
3.3.3. フィッシング詐欺被害を拡大させないための対策 12
3.3.4. ドメイン名に関する配慮事項 15
3.3.5. 組織的な対応体制の整備 17
3.3.6. 利用者への啓発活動 18
3.4. フィッシング詐欺被害の発生を迅速に検知するための対策 19
3.5. フィッシング詐欺被害が発生してしまった際の対策 19
3.5.1. フィッシング詐欺被害状況の把握 22
3.5.2. フィッシングサイトテイクダウン活動 22
3.5.3. フィッシングメール注意勧告 23
3.5.4. 関係機関への連絡、報道発表 24
3.5.5. 生じたフィッシング詐欺被害への対応 24
3.5.6. 事後対応 24

4. 利用者におけるフィッシング詐欺対策 25

4.1. フィッシング詐欺への備え 25
4.1.1. 怪しいメールを見分ける 25
4.1.2. 電子メール本文中のリンクの扱い 27
4.1.3. パソコンを安全に保つために 30
4.1.4. アカウント情報の管理 31
4.2. フィッシング詐欺に遭ってしまった時 32
4.2.1. 詐取された情報の識別 32
4.2.2. 関連機関への連絡 32

5. 付録 35

付録 A－サービス事業者が考慮すべき要件一覧 35
付録 B－利用者が考慮すべき要件一覧 36
付録 C－参考情報 36
C.1 【被害にあわないための 5 か条】 37
C.2 【情報サイト】 37
C.3 【業界団体と各省庁のサイト】 37
C.4 【安全な Web サイトの利用】 37
C.5 【サイトの脆弱性対策】 37

※フィッシング対策には最新版ガイドラインをご活用ください

C.6　【送信ドメイン認証】 38
C.7　【CSIRT への支援要請】 38
C.8　【Web ブラウザのフィッシングサイト対策機能】 38
C.9　【フィッシング 110 番】 38
C.10　【国民生活センター・消費生活センター】 38
C.11　【フィッシング対策協議会】 38
付録 D–プロバイダへのテイクダウン要請文例 39
付録 E–事業者における NG 集 40
6.　検討メンバ 42

※フィッシング対策には最新版ガイドラインをご活用ください

1. はじめに

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

1.1. 本ガイドラインの想定読者及び目的

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サービス事業者及び一般消費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。

- サービス事業者における機密性、完全性、可用性の保証
- 利用者におけるウイルス、スパイウェア等のマルウェア対策（フィッシング詐欺に悪用されるものについては考慮している）

サービス事業者における、サービス、サーバ機器、ネットワーク等に関する安全管理の詳細については、（独）情報処理推進機構の情報セキュリティ対策コンテンツ[1]等を参考にしていただきたい。

1.3. 用語解説

本ガイドラインで扱う用語の意味を以下に示す。

【フィッシング（phishing）】

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

【フィッシャー（phishier）】

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等、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。

【フィッシングサイト（phishing site）】

金融機関、クレジットカード会社等、金銭に関連するアカウント情報を持つサイトを模倣して設置されたおとりサイトのこと。

【ファーミング（pharming）】

---

[1] 「情報処理推進機構：情報セキュリティ：システム管理者の方」
http://www.ipa.go.jp/security/sysad/index.html

正規サイトへのアクセスを誘導してフィッシングサイトにアクセスさせる手法のこと。スパイウェア等により PC 上のホスト名と IP アドレスの対照表[2]を改ざんする攻撃、及び、PC が参照している DNS キャッシュサーバ、標的サイト（模倣している元のサイト）の IP アドレスを提供している DNS サーバのデータを改ざんする攻撃が知られている。フィッシングメール等を使わずとも、被害者が正規サイトにアクセスするだけでフィッシングサイトに誘導することができるため、注意深い利用者でも対策は難しいとされる。

【フィッシング被害】

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

【テイクダウン（take-down）】

フィッシングサイトを閉鎖することを指す。シャットダウン又はサイトクローズともいう。

【CSIRT（シーサート、Computer Security Incident Response Team）】

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

【URI（Uniform Resource Identifier）】

RFC3986, “Uniform Resource Identifier (URI): Generic Syntax”で規定されるリソースを識別するための単純かつ拡張性の高い記法である。Web の世界ではコンテンツアドレスを表記するために URL（Uniform Resource Locator）と呼ばれていた記法である。現在でも URI という言葉が多く使われているが、URI は URL を内包する上位概念であることから、本ガイドラインでは URI に表記を統一する。

[2] hosts ファイルと呼ばれる

2. フィッシングに関する基礎知識

本章では、フィッシング詐欺の主要な手法等についての基礎的な知識を示す。

2.1. フィッシング詐欺の手口

フィッシング詐欺の単純な例を図 1 に示す

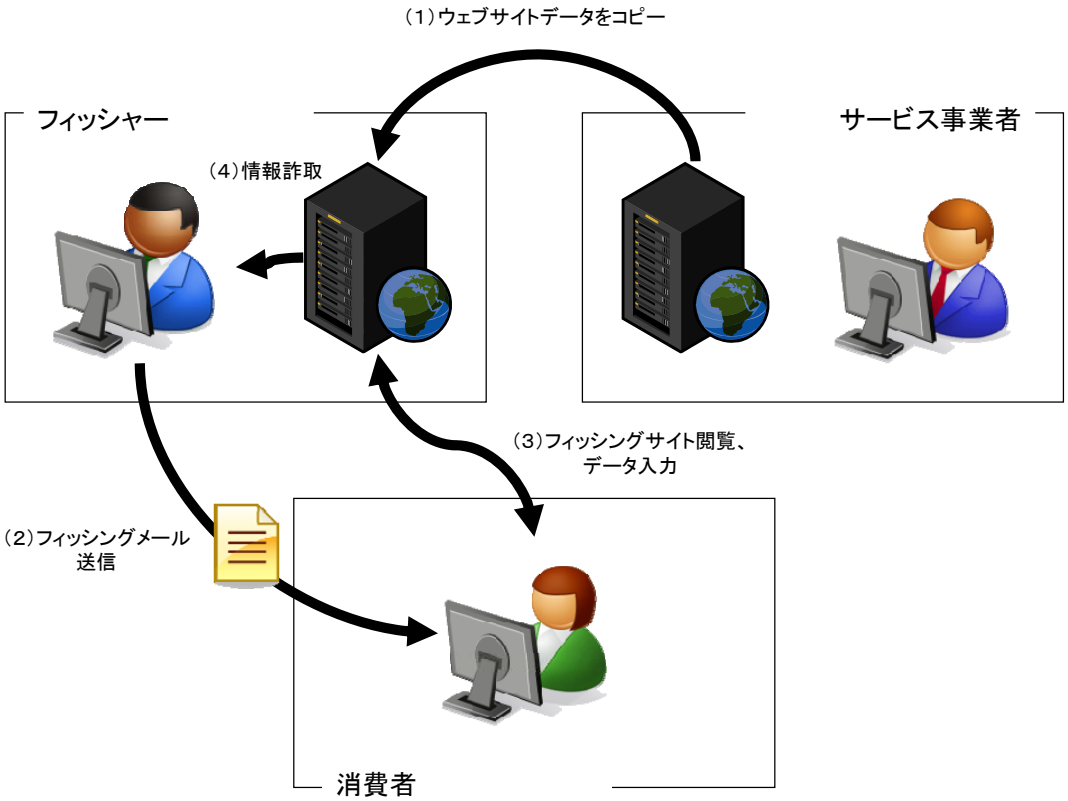


図 1 フィッシング詐欺の単純な例

まず、フィッシャーはターゲットとするサービス事業者の 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 URI 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、クレジット番号等を入力することでフィッシャーが情報を手に入れる。

なお、フィッシング詐欺のひとつの手法として、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等を送付するなど、最適化されているため、成功率は一般のフィッシングよりも高いと考えられる。ただし、スピアフィッシングは、その目的からするとフィッシング詐欺というよりも、標的型攻撃（ターゲテッドアタック）の一種に分類する方が適当かもしれない。

※フィッシング対策には最新版ガイドラインをご活用ください

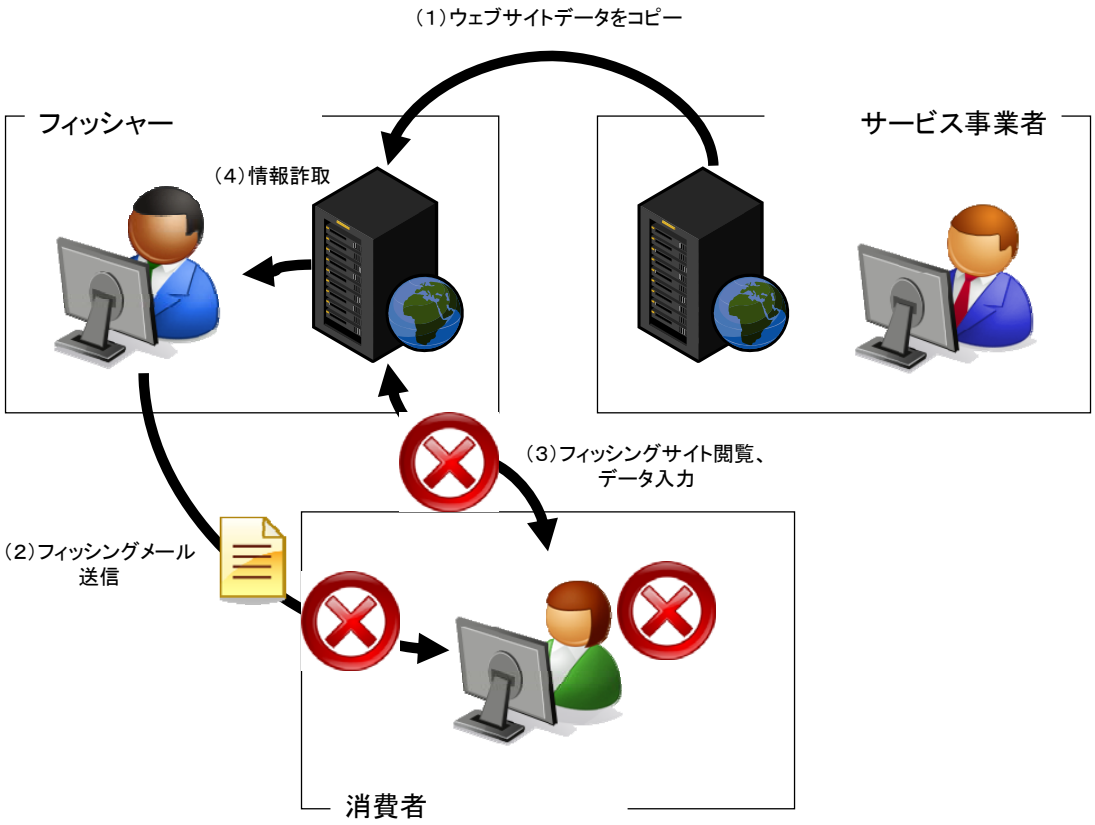


図 2 フィッシング詐欺被害の抑止ポイント

フィッシング詐欺の被害を抑制するためには、図 2 に示すような対策ポイント、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等を入力しないこと、といったポイントで対処する必要がある。

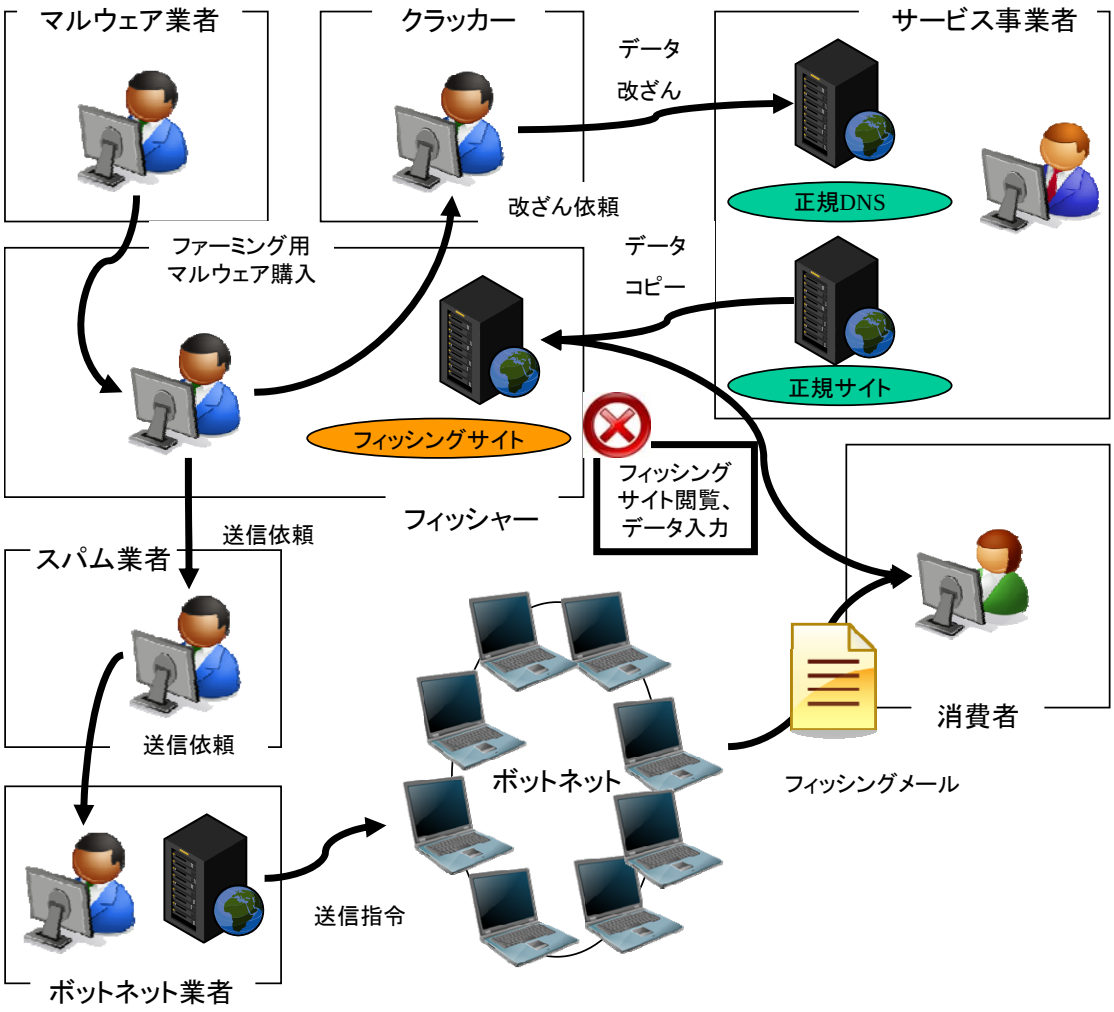


図 3 フィッシング詐欺の複雑な例

フィッシング詐欺においては、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スパム業者、送信元を隠すためボットネットを貸し出すボットネット業者、ファーミング用にカスタマイズされたスパイウェアを製造・販売するマルウェア業者、標的サイトの DNS サーバのデータを改ざんする職業クラッカー等の分業性が進んでいるとされる（図 3）。フィッシャーサイドの構造が複雑になることで事件として捜査する際には支障が発生する可能性があるものの、フィッシング詐欺に対抗するためのサービス事業者、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、サービス事業者においては信頼できるサービスの構築に努め、利用者においてはフィッシング詐欺被害に関する知識、騙されないための知識を身に付けていただきたい。

3. サービス事業者におけるフィッシング詐欺対策

本章では、フィッシング詐欺の標的、つまり、フィッシングサイトを設置され、利用者のアカウント情報等を搾取されるリスクを負っているサービス事業者にとって、被害が発生する前に心がけて置くべき対策、及び、被害が発生した際の対応事項について記述する。

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

◎：実施すべきと考えられるもの

○：実施を推奨するもの

△：必要に応じて実施すべきもの

3.1. サービス事業者におけるフィッシング詐欺の被害とは

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

全銀協のアンケート調査[3]によれば、インターネット・バンキングによる貯金等の不正払戻し事件は平成 23 年度に 87 件発生しており、払戻金額は 1 億 3 千万円に達している。87 件の内、銀行が補償を行ったのが 80 件であり、補償率は 96.4%であった。このうちの多くはフィッシング詐欺事件と考えられる。

その他の国内サービス事業者がフィッシング詐欺被害の補償をどの程度行っているのかは不明であるが、銀行同様に補償するということであれば、サービス事業者にとってもフィッシング詐欺の金銭的被害は無視できるものではないであろう。

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、サービス事業者の過失が実際にあったのかどうかに関わらず、利用者の間ではサービス事業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、サービス事業者と利用者の信頼を築くことは容易なことではない。利用者保護、信頼確保の視点を持ち、サービス事業者においても、十分なフィッシング詐欺対策を実施すべきであろう。

3.2. 利用者を守るためのフィッシング詐欺対策とは

利用者がフィッシング詐欺被害にあう際の事象の流れを図 4 に示す。

[3]一般社団法人全国銀行協会、「インターネット・バンキングによる預金等の不正払戻し」等に関するアンケート結果、http://www.zenginkyo.or.jp/news/entryitems/news241248_4.pdf

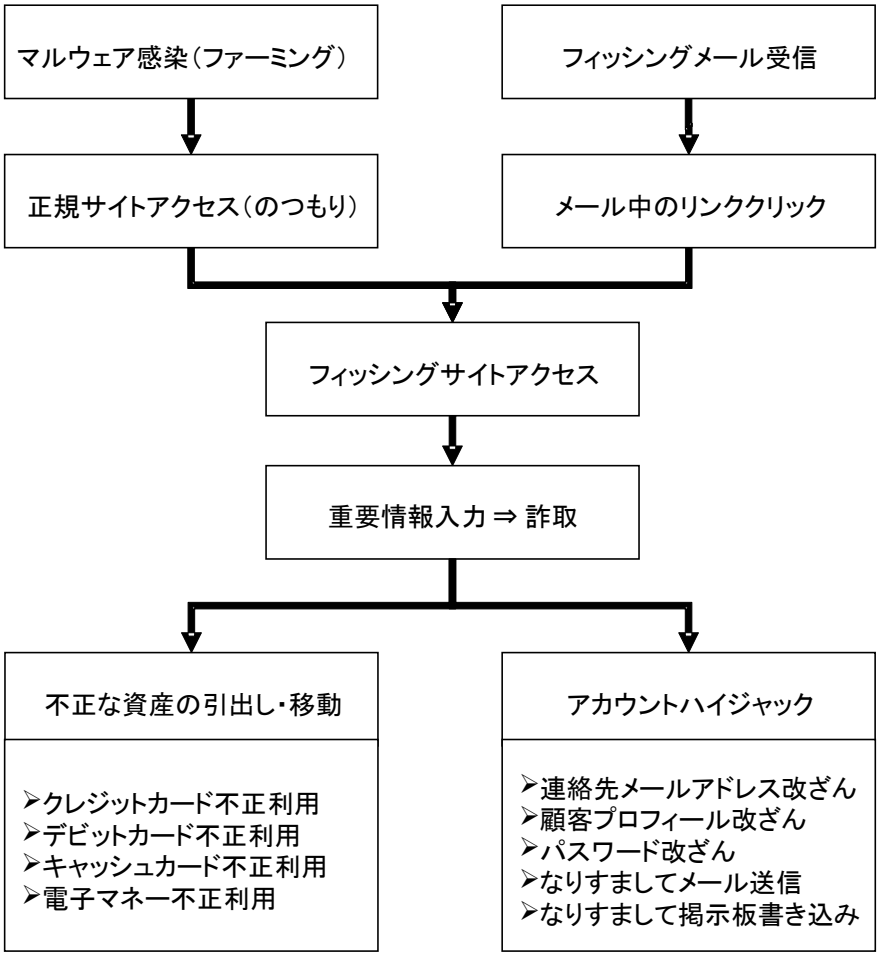


図 4 利用者サイドでのフィッシング被害発生フロー

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、心構え等に付いて啓発することが最も重要であるが、サービス事業者サイドにおいて実施すべき対策がある。フィッシング詐欺被害の発生を抑制するための対策、フィッシング詐欺被害の発生を迅速に検知するための対策、フィッシング詐欺被害が発生してしまった際の対策等である。

以降では、この三種の対策について具体的に述べていくことにする。

3.3. フィッシング詐欺被害の発生を抑制するための対策

利用者が正規サービス事業者とフィッシャーの区別を確実に行うことができれば、フィッシング被害を大きく抑制することができると考えられる。

3.3.1. 利用者が正規メールとフィッシングメールを判別可能とする対策

通常フィッシングメールは、サービス事業者の送信している正規メールの文面を模倣していると思われる自然な文面となっていることから、正規のメールとの見分けることが難しくなっている。

【要件1】 ◎：利用者に送信するメールには電子署名を付与すること

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

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

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

【要件2】 ◎：外部送信用メールサーバを送信ドメイン認証に対応させること

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

スパムメールにおける送信元詐称に対処する技術として、SPF（Sender Policy Framework）が定められている[5]。SPF は当該ドメインから SMTP コネクションを張ることが許可されたメールサーバのリストを DNS レコードとして提供することで、スパマー及びフィッシャーが送信元アドレスを偽ってメールを送信しようとする行為を検出することができる技術である。ただし、SPF をサポートしていないメール中継サーバは検査を行わないため送信元アドレスを偽ったメールでも中継してしまう。よって、SPF を導入したからといって、当該ドメイン名を偽ったメールを完全に廃絶することにはならないが、国内主要 ISP 等は SPF による送信元 SMTP サーバの検査を行っているため、利用者の多くをフィッシングメールから救うことができると考えられる。

なお、当該ドメインの SPF 登録 SMTP サーバにアクセス権を持つ者あるいは機器から送信されるフィッシングメールを止めることはできないので、サービス事業者内にボット感染 PC がある、サービス事業者内機器に侵入される等の状況では、対策漏れが生じてしまうことから、サービス事業者ネットワーク内の脅威を排除する活動と合わせて SPF 対応を行うことが望ましい。さらに、SPF の設定を間違えると、当該ドメインから外部にメールを送信できない状態にもなりうるため、SPF の導入時には十分な検討、試験を実施することが求められる。

---

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

[5] RFC 4408, ”Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1”

SPF に加えて、送信者及び送信ドメインを支援するフレームワークとして、より包括的な DKIM（DomainKeys Identified Mail）も規定されている[6]。DKIM については、S/MIME や SPF を機能面で補い、スパムメールやフィッシングメールを検出、破棄できる機能を有している。

DKIM は電子署名を元にしてメールの改ざんの検知とメール送信者（From:）のドメインの正当性を確認でき、転送されたメールも検証できるなど、SPF の欠点を補う機能がある。S/MIME はメールソフトウエアでメールの電子署名を検証するのに対し、DKIM はプロバイダが電子署名を検証する。また、DKIM には DKIM-ADSP（Author Domain Signing Practices）[7]という規格があり、DKIM 署名（作成者署名）の検証に成功しなかったメールをどのように取り扱うかを、あらかじめ送信者側がポリシとして宣言することができる。

表 1　DKIM-ADSP ポリシ概要

値	概要
all	このドメインから送信されるメールは、すべて DKIM 署名（作成者署名）が付いている。
unknown	このドメインから送信されるメールのいくつか、またはすべてに、DKIM 署名（作成者署名）が付いている。
discardable	このドメインから送信されるメールは、すべて DKIM 署名（作成者署名）が付いている。もし DKIM 署名（作成者署名）が付いていないメールや、不正な内容の DKIM 署名がされているメールが届いたら、受信者はメールを破棄してもかまわない。

利用者にログインを行わせるための通知メールなどには、送信ドメイン認証の SPF と DKIM に対応させ、さらに DKIM-ADSP として「discardable」を宣言し、差出人アドレス（From:）を詐称したフィッシングメールを受信者に届けない（または迷惑メールボックスに入るなど通常とは違う受信処理が行われる）対策を行うことが望ましい。

ただし、受信者は利用しているプロバイダが DKIM および DKIM-ADSP に対応していることを事前に確認する必要がある。

送信ドメイン認証に関する参考情報を C.6 [送信ドメイン認証]に示す。

【要件3】　◎：利用者に送信するメールでは定型的な様式を用いること

Web サイトの模倣を防ぐことができないことと同様、メールの様式を模倣されることを防ぐことはできないが、サービス事業者固有の様式を用いた文面とすることで、情報セキュリティ上の重要な通知等がスパムとして利用者に届かないことを避けることができる。

フィッシングメールでは受信者に冷静に判断されないよう「緊急」であることを煽る文面を用いるものがある。このようなフィッシングメールと正規の通知メールを判別するため、また、利用者が被害にあわないよう、フィッシング被害発生時の通知手段として電子メールを用いる場合にはリンクアドレスを含まない様式とし、その様式を利用者に説明しておくこと。

[6] RFC4871, “DomainKeys Identified Mail (DKIM) Signatures”
[7] RFC 5617, “DKIM-ADSP（Author Domain Signing Practices）”

【要件4】 ◎：サービス事業者が利用者に送信するメールは TEXT 形式とすること

フィッシングメールの多くは被害者に意識させずリンクを踏ませるため HTML 形式で作成されている。HTML 形式では、フィッシングサイトのリンクを無害なリンクに見せかけることが容易であり（無害なリンク）、古典的とは言えフィッシングメールの常套手段である。利用者に無用なリスクを負わせないためにも、サービス事業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。

利用者への通知に画像表示、リンクを含めるため等の理由で HTML 形式としている場合には、利用者が TEXT 形式か HTML 形式か選択できるように配慮し、デフォルトは TEXT 形式とすることが望ましい。

【要件5】 ◎：利用者にメール送信する状況及び内容を周知しておくこと

多くのフィッシングメールでは ID 及びパスワードの確認を行うよう求めている。利用者がアカウント登録を行う際に、サービス事業者がメールを送信するケース、送信するメールの種類と用途について示し、メールでは ID 及びパスワードの確認を行わないことを明確にしておくことが重要である。

3.3.2. 利用者が正規サイトとフィッシングサイトを判別可能とする対策

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

【要件6】 ◎：Web サイトの安全性を確保すること

フィッシング詐欺の手法として、正規サイトのクロスサイトスクリプティングぜい弱性を悪用するものがある。このぜい弱性は多数のサイトで発見されており、ユーザセッションハイジャック等にも使われるものであることから、最も注意が必要なものといえる。

（独）情報処理推進機構「安全なウェブサイトの作り方 改訂第 3 版」[8]等、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、外部専門機関等を活用して、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。

【要件7】 ◎：Web サイトの正当性に係る情報を十分に提供する画面とすること

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

[8] http://www.ipa.go.jp/security/vuln/websecurity.html

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

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

【要件8】 ◎：重要情報を入力するページは SSL/TLS で保護すること

利用者にユーザ ID 及びパスワード等の認証情報を入力させるページ、及び認証された状態で閲覧するページの全てにおいて認証情報保護のため、SSL/TLS を使用して、盗聴のリスク及び第三者中間者攻撃のリスクを避けること。

また、用いるサーバ証明書に関しては、次の原則に準拠すること。

- SSL/TLS を運用する際には多くの Web ブラウザでサポートされている認証局から発行されたサーバ証明書を用いること
- 認証局がオンライン証明書失効確認プロトコル（OCSP、Online Certificate Status Protocol）に対応、あるいは CRL リポジトリを提供していることを確認すること
- 個人情報を入力させるサイトでは、サービス事業者の実在確認を厳格に実施した上で発行される EV SSL[9]証明書を導入し、サービス事業者及び Web サイトについて高い信頼を提供することが望ましい

なお、https://を利用する際には、cookie に secure 属性を使うこと[10]。

【要件9】 ◎：Web サイト運営者の連絡先及びガイダンス等、利用者に間違いなく情報を伝える必要のあるページは SSL/TLS で保護すること

SSL/TLS には、機密性保護に加え、アクセスしている Web サーバの正当性（ドメイン名を含めたサーバ名と運営者との関係について認証局が確認をとっているということ）を検証する機能が備わっている。Web サイト、Web サービスに関する緊急時の連絡先及びガイダンス等、Web サイト運営者から正しく情報を伝える必要のあるページは SSL/TLS でのアクセスを可能とし、利用者が Web サイト運営者からページコンテンツが提供されていることを確認する手段を提供することが望ましい。

【要件10】 ◎：正規 Web サイトのドメイン内設置サーバの安全性を確認すること

フィッシングサイトを信用させる手段として、模倣したサイトのドメイン名を調査し、管

[9] Extended Validation SSL、CA/Browse Forum（http://www.cabforum.org/）にて規定されているガイドラインに従って、組織の実在確認を厳密に行った後に発行される SSL サーバ証明書のこと。この証明書を使っているサイトにアクセスすると、一部の Web ブラウザではアドレスバーが緑色に変化して、安全性が高いサイトであることを表現する。

[10] 理由については http://www.ipa.go.jp/security/ciadr/20030808cookie-secure.html を参照

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

このような状況が発生しないように、正規 Web サイトが利用しているドメイン内に管理状況の悪いサーバ（ぜい弱性の存在が報告されているソフトウエア等が放置されている、ログの監視が行われていない等）が設置されていないことを定期的に確認すること。

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

【要件11】 ○：認証システムが許容するポリシを利用者に示すこと

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

【要件12】 ○：正規サイトの全てのページに利用者に対する脅威の状況を表示する

フィッシング詐欺被害発生、送信者をサービス事業者に偽装したウイルスメール、スパムメール等、サービス提供上の脅威の状況を正規サイトに表示することで、利用者の状況判断を容易にすること。正規サイトにアクセスしている利用者の全てに通知するため、全てのページに脅威の状況を表示するよう工夫することが望ましい。

【要件13】 △：認証画面には利用者個別のマーク等を表示できるようにする

フィッシングサイトでは ID・パスワード等の認証情報を入力させる画面（認証画面）を悪用することが多い。この認証画面に利用者が事前に登録した文字列あるいは画像等を表示させるようにして利用者ごとに異なる画面を構成すると、フィッシングサイトとの違いをはっきりさせることができる。

3.3.3. フィッシング詐欺被害を拡大させないための対策

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

実施しておく必要がある。

【要件14】 ◎：資産の移動に限度額を設定すること

フィッシャーによる利用者資産の窃盗被害を抑制するため、資金の移動機能（他金融機関への振込み、商品の購入等）を提供している場合には、移動資産の限度額を設定できるようにする。この場合、一回の操作の上限とともに、一日辺りの上限を設け、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。

【要件15】 ◎：資産の移動時に利用者に通知を行うこと

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

利用者 PC のマルウェア感染など、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資産移動確認手続きを検討することが望ましい。

【要件16】 ○：正規 Web サイトにアクセス可能な端末を制限すること

フィッシャーによる不正なログインを抑制するため、利用者が通常利用している端末以外の端末からログインを行った場合には、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。

コスト面で妥当であれば利用者に電子証明書を発行し、SSL/TLS の相互認証（クライアント認証）を行うことで、効果的なアクセス端末の制限を実現することができる。フィッシングによる ID/パスワードの詐取が直接、金銭的損害に結びつくサービスの場合には利用者に対する電子証明書の発行を検討することが望ましい。

【要件17】 ○：携帯電話によるサービス利用は利用者の選択制とすること

一般に携帯電話からのアクセスを安全に保つことには制約がある。サービス事業者が携帯電話でのサービスを提供している場合、携帯電話からサービスを利用しない、したくない利用者のために、携帯電話からのログインを制限（停止）する機能を提供する。また、携帯電話の個体識別情報を利用できる場合にはユーザ ID と個体識別情報を紐付けて特定の端末からのログインだけを認めるようにすることが望ましい。

【要件18】 ○：機微情報を変更するページへの移動には再度認証を要求すること

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

【要件19】 ○：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四桁など一部だけの表示に留めることが望ましい。

【要件20】 ○：パスワードのブラウザへの保存ついては禁止する

オンライン銀行、オークションなどの重要なサイトでは、利用者に対してパスワードのブラウザへの保存を禁止する。

【要件21】 ◎：アクセス履歴の表示

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

【要件22】 △：特別な認証方法を採用する場合には、その方式に特有のぜい弱性対策を行うこと

例えば乱数表を第二認証要素として用いる場合、フィッシャーが乱数表の一部を不正取得したとすると、取得した乱数表の一部から知ることのできる乱数値が認証要素として要求されるまで認証画面をリフレッシュし続けるという攻撃方法が知られている。この場合、認証ページの連続表示回数を制限することにより不正行為を防止する等の対策が必要となる。

別の例としては、トークンの真正性を認証する情報を使い捨てにする手法が広範に使用されているが、こうしたトークン認証情報を使い捨てにする、いわゆる「ワンタイムパスワード」は当該のトークンを手にしている人物が正規ユーザであるのか、あるいは攻撃者であるのかを知らせるものではないので、別途パスワード・暗証番号の入力を要求することが望ましい。

このように、特別な認証方法を採用する場合には、その方法のメリットだけでなく、デメリットとなりうるぜい弱性等について十分に調査し、適切な対策を実装すること。

【要件23】 ○：正規サイトログイン時の認証には複数要素認証を利用すること

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、ID,パスワード以外の認証を加えた複数要素認証を利用しておくことが効果的である。実際にネットバンクでは、ワンタイムパスワードを生成するハードウェアトークンの配付や、マトリックス認証用のカードを配付している事例がある。事業者・利用者双方に多大な影響があるサービスについはワンタイムパスワードを利用することが望ましい。

ワンタイムパスワードはパスワードの盗聴に対抗する手段として強力な対策となりうる。しかし、利用者にとって、ある程度の不便を要求するものでもあり、安全と利便性のトレードオフについて、十分な理解を求めることが望ましい。

ただし、トークンによって生成されるワンタイムパスワードはトークンが本物であることは示すが、アクセス時点でのトークン保持者が本人であるか否かの証明には関わらないので別途本人認証情報としてパスワード・暗証番号入力を要求することが望まれる。トークン認

証情報ではなく本人認証情報そのものをワンタイムパスワードとする手法の場合にはこうしたパスワード・暗証番号の併用は不要である。

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サービス事業者の管理運営するサイトであることを明確にするための方策を示す。なお、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 等、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。

【要件24】 ◎：利用者の認知しているサービス事業者名称から連想されるドメイン名とすること

Web サイトは SSL/TLS を利用することで、電子証明書によるドメインの正当性の検証手段を利用者に提供することができるが、電子メールについては S/MIME 等、あまり一般的ではない手法を用いない限りは、送信元アドレスを目視確認してもらう手段を提供することができない（もちろん送信元アドレスは詐称可能であるため目視確認を行っても有効な手段にはならない）。このため、サービス事業者は利用者に送信するメールのドメイン名（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、サービス事業者の一般呼称をそのまま使ったもので、かつ“co.jp”ドメイン[11]、あるいは“jp”ドメインであるようなものを指す。

“com”、“org”、“net”といった特定の国に依存しないドメイン名[12]をオフィシャルなドメイン名として利用している国内企業、サービスもあるが、これらのドメイン名では取得申請者に対する実在確認を行わないことが多いことから類似のドメイン名使用権利をフィッシャーが手に入れたり、何らかの原因でドメイン名使用権利が失効した際に他の事業者にドメイン名使用権利を奪われたりするケースがある等、安定したサービスを提供する上での問題がある。

客観的に見てサービス事業者にとっては“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、可能な限り、“co.jp”ドメイン名にてサービスを提供するべきといえる。

なお、企業名称及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。

---

[11] 同様に“ac.jp”、“go.jp”等があり、属性型 JP ドメイン名と呼ばれる。

[12]特定の国に依存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。

【要件25】 ◎：悪用される可能性の高い類似ドメイン名を登録しておくこと

フィッシャーは正当ドメイン名であると誤解されやすいドメイン名を取得して悪用する場合がある。例えば、サービス事業者のドメイン名が example.co.jp の場合は、example.jp や example.com、example.net、exampleco.jp、wwwexample.co.jp 等である。これらの紛らわしいドメイン名の内、少なくとも、“example.jp”、“example.com”については悪用を防ぐために登録しておくことが望ましい。既に登録者が存在する場合には、ドメイン名の委譲交渉を行う、委譲を考える際には優先的に交渉してもらえるよう協議しておくことが望ましい。

類似ドメイン名を他事業者が既に取得している場合には、登録事業者に対して、ドメイン名委譲の交渉を行うことになるが、転売目的でドメイン名を登録している事業者も世の中には存在し、不当な高値を提示してくるケースがある。このような場合の紛争処理に関しての情報が（社）日本ネットワークインフォメーションセンターの Web サイトでまとめられているので参考にすること（http://www.nic.ad.jp/ja/drp/index.html ドメイン名紛争処理方針（DRP））。なお、“jp”ドメインに関しては日本知的財産仲裁センターに対して紛争処理の申し立てを行うことができる。

【要件26】 ◎：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

ドメイン名には日本語などを使用すること（ドメイン名[13]）も可能となっており利用も始まってはいるものの、まだ十分に普及している状況とは言えない。わが国では、組織名称やサービス名称は日本語の漢字や仮名で表記されることが多いが、現状ではそれらを、アルファベット、数字及びハイフンによる表現に変換してドメイン名として利用している例が多い。この際、ローマ字変換する、英文呼称を設けて英語表記する、略語により表記する等、いくつかの方法が考えられる。

いずれの方法にせよ、利用者にとっての紛らわしさを完全に払拭することは困難であることから、正しいドメイン名について繰り返して利用者に示す必要がある。周知の手段として、利用者に対して案内や連絡等を行う際には、電子メールではなく郵便を用いること（電子メールを読まない関心を持たない利用者のため、及び印象づけるため）、封筒自体にドメイン名をはっきりと示す（開封しない利用者もいるため）、フィッシング詐欺、振り込め詐欺等、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等が考えられる。機会があれば、新聞、テレビ（CM）等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、SSL 証明書を利用することで、ドメイン名の正当性を示すことも重要である。

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

【要件27】 ○：ドメイン名に見た目が紛らわしい文字を含めないこと

“co.jp”ドメイン名は、一法人に一つと決められているので、サービスの種別毎に Web サイトを設置する場合には、サーバのアドレスが“www.service.example.co.jp”あるいは“service.example.co.jp”といったように、比較的長いアドレスになってしまう。このため、

[13] http://www.nic.ad.jp/ja/dom/idn.html

特に携帯電話向けサイトなど、長い文字列の入力が好まれない場合等には“co.jp”ドメイン名ではなく“example.jp”といったサービス名＋“jp”ドメイン名といった短いアドレスを用いることも、利用者の利便性を考える上では止むを得ない。

この場合には、誤解の無いようにサービス名を工夫することが求められる。ローマ字に直した時に紛らわしい、あるいは複数の書き方が存在するようなサービス名を用いると、利用者がフィッシングメールに騙されやすい場合が考えられる。例えば、“l（エル）”と“1（数字の一）”、“O（オー）”と“0（数字のゼロ）”、“shi”と“si”といった紛らわしい文字が含まれている場合等である。他にも英語を使ったサービス名の場合に、つづりがわかりにくい場合、例えば、フィッシング対策協議会のドメイン名は“antiphishing.jp”であるが“antiphising.jp”、“antifishing.jp”等は、利用者にとっては区別がつきにくいものと考えられる。紛らわしいドメイン名にならないようにサービス名には十分に配慮すべきであろう（既に紛らわしさの残るドメイン名でサービスを行っている場合には、そのリスク、悪用される可能性のあるドメイン名等について利用者に十分に周知すること）。

3.3.5. 組織的な対応体制の整備

必要なフィッシング詐欺対応要件の整理や脅威の想定とリスク評価を行い、対策を実施するため、組織的な対応体制の整備が必要となる。

【要件28】 ◎：フィッシング詐欺対応に必要な機能を備えた組織編制とすること

フィッシング詐害対策に留まらず情報セキュリティ対策全般を受け持つ専門部署の設置、企画・運営と情報セキュリティの技術的内容の分かる人材を含めたメンバの確保が望まれる一方、広報、コールセンタ等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、様々な事項を同時並行的にすみやかに処置していくことが必要になるので、組織に応じた事前準備、役割分担、連絡・レポート体制を明確化しておくことが必要である。

【要件29】 ◎：フィッシング詐欺に関する報告窓口を設けること

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

運営しているサイトの不正操作や不正取引の被害により利用者に多大な被害が及ぶサービス、キャッシュカード、クレジットカード、デビットカードの発行を行っているサービスの場合は紛失や盗難などの事故の被害を報告できる 24 時間受付窓口を設置する必要がある。

【要件30】 ◎：フィッシング詐欺発生時の行動計画を策定すること

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

- 不正操作、不正取引の被害があった場合
- フィッシングサイトの報告があった場合、あるいは発見した場合

- 報道発表を行う準備も整えておく、事象発生前に発表文面のテンプレートなどを用意し、そのレベルで事前に関係者・役員等に了解を得ておくなどして速やかに発表できる仕組みにしておくことが望ましい。

【要件31】 ◎：フィッシング詐欺及び対策に関わる最新の情報を収集すること

情報サイトのセキュリティコーナーやウイルス情報のサイトを確認する。

情報サイトを付録 C に示す。

【要件32】 ◎：フィッシングサイト閉鎖体制の整備をしておくこと

フィッシングサイトの閉鎖は、自社にて対応することもできるが、通常フィッシングサイトは海外にホストされているケースが多く、自社に専門スタッフや専門部署が無い場合には専門業者などへの対応要請が推奨される。

【要件33】 ○：フィッシングサイトアクセスブロック体制の整備をしておくこと

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

フィッシングサイトを発見した場合は、ウイルス対策ソフト、フィルタリングソフトなどのセキュリティソフトベンダや Web ブラウザベンダに、該当サイトアクセスをブロック対象とするよう要請または事象報告する。各セキュリティソフト／Web ブラウザベンダの Web サイトなどにその報告の方法が掲載されている。文書による協力要請を行う場合には事前に要請書のテンプレートを作成しておくことが望ましい。

3.3.6. 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34】 ◎：利用者が実施すべきフィッシング詐欺対策啓発活動を行うこと

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

【要件35】 ◎：フィッシング詐欺発生時の利用者との通信手段を整備しておくこと

フィッシング詐欺が発生した時点では速やかに利用者への連絡を行わなければならない。通信手段としては、電話、電子メール、携帯メール、郵便、マスメディア等が考えられる。

過去に発生したインターネット上のインシデントの例を見ると、被害状況の把握までに一定の時間を要している。フィッシング詐欺においても、フィッシングメールがどれだけ流通しているのか、利用者の何割がフィッシングメールを受け取ったのか、既に被害を受けた利用者はどれだけいるのか等、被害発生を認識した時点で把握することは難しいと思われるため、被害の拡大を抑制するためには、可能な手段を全て使って利用者に被害発生を通知すべきと考えられる。

利用者登録時には、緊急通知用[14]の電子メールアドレス、携帯メールアドレスを登録してもらうこと、金融サービス等、深刻な被害が想定されるサービス事業者においては、電話番号、住所も合わせて把握しておくこと。更にマスメディアを活用した通知手段を整備しておくことが望ましい。

3.4. フィッシング詐欺被害の発生を迅速に検知するための対策

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

【要件36】 ○：Web サイトに対する不審なアクセスを監視すること

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

【要件37】 △：フィッシング詐欺検出サービスを活用すること

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

3.5. フィッシング詐欺被害が発生してしまった際の対策

サービス事業者のフィッシングサイトが設置された場合、サービス事業者の利用者にフィッシング詐欺の被害が発生した場合には迅速に対応活動を実施することが必要である。この対応活動は一種のインシデントハンドリング活動であるが、フィッシング詐欺被害特有の対応活動がある、それは、被害の拡大を防ぐため、フィッシングサイトのテイクダウン（閉鎖活動）[15]を行うことにある。

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

[14] 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。
[15] 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。

からは保有組織がフィッシャーであるのか、第三者であるのか、の判別が難しいことがある。

フィッシング詐欺被害の発見から対応、事後対応までのフローを示す。

（1） フィッシング詐欺被害の発見

（2） フィッシング詐欺被害状況の把握

（3） フィッシング詐欺被害対応活動

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

（4） 生じたフィッシング詐欺被害の回復措置

（5） 事後対応

以降では各ステップの詳細を記述する。

※フィッシング対策には最新版ガイドラインをご活用ください

フィッシング詐欺被害対応フロー

（1）フィッシング詐欺被害の発見

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

（2）フィッシング詐欺被害状況の把握

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

（3）フィッシング詐欺被害対応活動

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

（4）生じたフィッシング詐欺被害への対応

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

（5）事後対応

・事後処理含め、改善、再発防止策などを体制や対応手順書などに反映する。

3.5.1. フィッシング詐欺被害状況の把握

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

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

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

3.5.2. フィッシングサイトテイクダウン活動

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

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

テイクダウン要請をサービス事業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）、更に海外の ISP であれば現地の CSIRT に支援要請を行うことが望ましい。多くの ISP はインシデント対応機関とのチャンネルを持っており、サービス事業者からの連絡よりもインシデント対応機関からの連絡の方がスムーズに受入れられることが理由である。

（2）専門機関にテイクダウン依頼を行う

国内においては JPCERT/CC にてフィッシングサイトのテイクダウン依頼を受け付けている。支援要請の際には、「インシデント報告の届出[16]」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 URI 情報(必須)、確認した日時・場所等をインシデント届出様式[17]に記載して送信する。また、既にサービス事業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、警察等に連絡を行っている場合には、連絡日時と連絡先、連絡内容等もインシデント届出様式に記載するとよ

[16] https://www.jpcert.or.jp/form/
[17] https://www.jpcert.or.jp/form/form.txt

いだろう。

（3）フィッシング詐欺被害対応サービス事業者にテイクダウン依頼をする

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

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

3.5.3. フィッシングメール注意勧告

フィッシング詐欺被害の発生をサービス事業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、サービス事業者自身による発見、第三者による問い合わせ等が考えられる。

サービス事業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

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

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

（2）利用者への通知を行う

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

まず、フィッシングサイトにアクセスしないように注意を促す必要がある。この場合、広く利用者へ連絡するためには、電子メールによる通知に加え、正規サイトでの掲示、報道機関等各種メディアへの告知等、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、郵便等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、既に被害にあってしまった利用者が相談できる窓口・情報も記載しておくことが重要である。

3.5.4. 関係機関への連絡、報道発表

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

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

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

3.5.5. 生じたフィッシング詐欺被害への対応

報告窓口に寄せられる利用者からの被害報告、及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 の詐取等）の発生状況を把握する。クレジットカード番号、オンラインバンキングアカウントの詐取等、金銭的被害の発生する危険性があれば、被害拡大抑制のための活動を実施すること。

3.5.6. 事後対応

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

4. 利用者におけるフィッシング詐欺対策

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

脅威：フィッシングメール中のリンクを正規リンクと間違える

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

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

4.1. フィッシング詐欺への備え

常日頃からの心がけとして、フィッシング対策協議会では「被害にあわないための 5 カ条」を定義して公開している。中でも、以下の三項目が重要である。

- 怪しいメールに注意する
- 電子メール本文中のリンクはクリックしない
- パソコンを安全に保つ

基本的には、この三項目であるが、フィッシングの手口は益々巧妙となり「怪しいメール」であることを判定することは容易ではなく、企業からの主な連絡手段が電子メールとなっていることから「電子メール本文中のリンク」をクリックせざるを得ない場合もあり、脅威は次々に現れることから「パソコンを安全に保つ」ことも容易ではない。

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

4.1.1. 怪しいメールを見分ける

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

【要件38】 ◎：機微情報の入力を求めるメールを信用しない

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

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

【要件39】 ◎：メールに記載される差出人名称は信用しない

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

> 〇△□株式会社の皆様へ
>
> こちらは〇〇トラベル、〇△□様担当××です。
> ただいま、特別キャンペーンとして貴社の皆様だけに、沖縄ツアーを特別料金で御提供しております。いますぐ、以下のリンクをクリックして特設サイトで御応募下さい。
>
> http://www.△△.jp/〇△□/special.html
>
> --
> 〇〇トラベル〇△□様担当××より

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

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

【要件40】 ◎：怪しいメールの判断基準を知る

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

- 「緊急、今すぐ、明日まで」等、対応を急がせる文面
- 「素晴らしい、あなただけに、特別な」等、欲望を掻き立てるフレーズ
- なんらかの秘密情報を聞き出そうとする
- 日本語として妙なところがある（外国人が作成したもの）
- 電子署名が付与されていない（現状は、ほとんど付与されていないので効果がない）
- 送信ドメイン認証が施されていない（送信企業、組織が送信ドメイン認証を導入している場合）

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

送信者に確認をとり、確認がとれないリンクはクリックしない。

【要件41】 ◎：安全なメールサーバを活用したり、類似性評価によるフィッシングメール判別機能を活用すること

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

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

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

問題は標的型フィッシングメールである。文面は標的組織で使われている文面を模倣しているためベイズ理論によるフィルタは効力が薄く、限定された組織だけに配送されるためスパムデータベースにも登録されていない。もし、他の組織も標的としているフィッシャーであれば、送信者、送信元サーバアドレスがブラックリストに登録されている場合も考えられるが、スパムフィルタの技術を熟知しているフィッシャーであれば、それらのデータを標的毎に使い分けるような対策をとっているだろう。このように標的型フィッシングメールに対抗するには、ツールに頼るのではなく、メールが求めている行為（メール中のリンクをクリックする等）の怪しさを自ら判別することに尽きる。

【要件42】 ◎：リンクにアクセスする前に正規メールかどうか確認する

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

4.1.2. 電子メール本文中のリンクの扱い

フィッシングメールは図 5 に示すように HTML 形式で送られてくるケースが多い。この例では、HTML フォームをメール本文中に記述し、フィシングサイトに誘導せずに口座番号、暗証番号を詐取しようとしている。

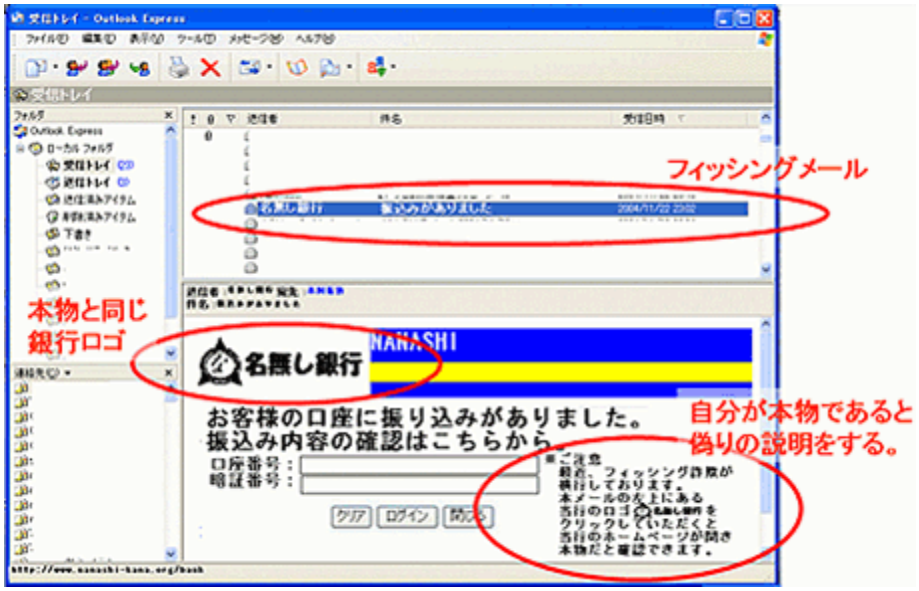


図 5 HTML 形式のフィッシングメールの例

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

【要件43】 ◎：正しい URL を確認する

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

【要件44】 ◎：電子メール本文中のリンクには原則としてアクセスしない

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

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

- 電子メールを TEXT 形式で閲覧していること
- 表示されたアドレスは http:// あるいは https:// で始まっていること
- 表示されたアドレスが既知の正規サイトのものであること

HTML 形式の電子メールを閲覧する場合、リンクにはアドレス自体が表示される訳ではないので、安易にクリックすると予想外のサイトにアクセス、あるいは予想外のコンテンツにアクセスしてしまうことが考えられる。ウェブブラウザの多くは実際のアクセス先リンク

をウェブブラウザ上に表示する機能を持っているので、偽装したリンクを見破ることができる。しかし、メーラで HTML 形式の電子メールを表示している場合に、そのような実際のアクセス先を確認する機能が提供されていないものがあることから、リンクを直接クリックして閲覧するのではなく、コピー&ペーストして、実態としてのリンク先を確認することが必要である。

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

【要件45】 ◎：錠前マークを確認する

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

①正しい URL にアクセスしているか？

②錠前マークが表示されているか？

の 2 点を確認することが望ましい。両者を確認出来た場合にのみ、入力を行うようにしてください。なお、EV-SSL サーバ電子証明書が使われている場合には、電子証明書自体を確認しなくても、サイトの運営者がウェブブラウザのアドレスバー付近に表示されるため 、確認が確実かつ容易になるよう工夫されている。

【要件46】 ○：サービス事業者からの通知メール形式を TEXT 形式に設定する

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

【要件47】 ○：リンク先で機微情報の入力を求められた場合には、電話等でサービス事業者に真偽を確認する

サービス事業者から送信されたと判断した電子メール中のリンクにアクセスしたところ、ID/パスワード（ログイン要求ということ）、口座番号、暗証番号、個人情報等の機微情報の入力を求められたのならば、フィッシングサイトである危険性が高いので、情報を入力せず、ウェブブラウザ画面はそのままにして、サービス事業者に電話等で問い合わせを行い、本当に情報を入力させる目的でメールを送ったのかどうか確認すること。

この確認の電話がフィッシング詐欺被害発生の契機となる可能性があるので、ウェブブラウザの画面をそのままにしておいていただきたいが、ウェブブラウザにてサービス事業者の問い合わせ電話番号を調べることが難しくなる場合があるため、事前に問い合わせ電話番号等を記録しておくことが望ましい。

4.1.3. パソコンを安全に保つために

パソコンを安全に保つためには、セキュリティパッチを適用するだけではなく、スパイウェア、ボット等、情報を盗み出すマルウェアマルウェアの侵入を防ぐための対策を考慮することが必要である。また、フィッシング詐欺の手法は進化を続けていることから、利用者の心がけだけでは完全に対処することは難しい。ここでは、フィッシング対策を徹底するために有益なツール及び、その有効な使い方について紹介する。

【要件48】 ◎：最新のセキュリティパッチを確実に適用する

パソコンにセキュリティ上の脆弱性があると、利用者が気づくことなくマルウェアマルウェアへの感染や脆弱性を利用した攻撃を受けることになる。最新の OS やアプリケーションには自動的に最新のセキュリティパッチを適用する機能が備えられていることが多いので、できるだけその機能を有効にし、最新のセキュリティパッチが確実に適用された状態でパソコンを利用することが重要である。

【要件49】 ◎：セキュリティ対策ソフトウエアの機能を理解し適切に用いる

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

【要件50】 ◎：Web ブラウザにフィッシングサイト判別機能を組込み活用すること

フィッシャーの巧妙な手口により、メール中のフィッシングサイトへのリンクをクリックしてしまうことをリスクとして想定しておかなければならない。その場合の対策として、フィッシングサイト判別機能を Web ブラウザに組み込んでおきたい。ツールバーと呼ばれるソフトウエア（アドイン、プラグイン等と呼ばれる）を Web ブラウザに組み込むことで、フィッシングサイトの疑いのあるサイトにアクセスしようとした際に警告を表示するようにできる。

なお、Firefox（バージョン 3.6 以上）、Internet Explorer 8、Opera 等の Web ブラウザはフィシングサイト判別機能を備えている。それぞれの Web ブラウザベンダの解説、ヘルプ情報等を読み、フィッシングサイト判別機能が有効になっていることを確認すること。

【要件51】 ○：PC の利用には標準ユーザアカウントを利用し、ユーザアカウント制御機能を活用すること

コンピュータのログオン時には、システム管理者アカウントを使わず、標準ユーザアカウントを利用すること。また、Windows Vista から提供されているユーザアカウント制御機能を活用し、不用意にシステムへの変更が加えられるのを防ぎ、発行元が不明のソフトウエアのインストールを行わないこと。

ユーザアカウント制御機能はデフォルトで ON のため、OFF にしないこと。

【要件52】　○：URL フィルタリングを活用すること

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

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

4.1.4. アカウント情報の管理

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

【要件53】　◎：アカウント ID/パスワードはサービス事業者別に設定すること

複数のサービス事業者で同じアカウント ID/パスワードを使っていると、一つのフィッシング詐欺で詐取された認証情報を他のサービス事業者でも悪用されてしまう危険があるため、アカウント ID/パスワードの組をサービス事業者別に設定すること。少なくともパスワードは別々のものに設定すること。

【要件54】　◎：アカウント管理ソフトウエアを導入する

フィッシング詐欺被害に遭いアカウント情報を詐取された場合を考えると、影響の拡大を防ぐため、アカウント ID、パスワード等の認証情報は、サービス事業者別に分けておくことが必要である。しかし、多くのサービス事業者を利用している場合には、記憶だけに頼っていては、全てのアカウント ID/パスワードの組を管理することは難しい。このような場合には、アカウント ID とパスワードの組について安全性を確保して管理するためのソフトウエアを利用すること。

ブラウザにもサイト毎にアカウント ID/パスワードを記憶しておく機能（オートログイン）がある。しかし、ブラウザの機能ということはブラウザにぜい弱性があれば ID/パスワードを盗まれるリスクがあるということにもなる。ブラウザのオートログイン機能は便利ではあるが、本ガイドラインでは、ブラウザ以外のアカウント管理ソフトウエアの利用を勧める。

【要件55】　◎：全てのアカウントについて緊急連絡先を把握しておくこと

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

サービス事業者に利用者登録を行った際には、「登録完了通知」等の名目で電子メールが

送られてくることが多い。このメールには、利用者窓口の連絡先が記載されていることが多いので、これらのメールを整理しておくと緊急時の連絡に便利である。

4.2. フィッシング詐欺に遭ってしまった時

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

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

4.2.1. 詐取された情報の識別

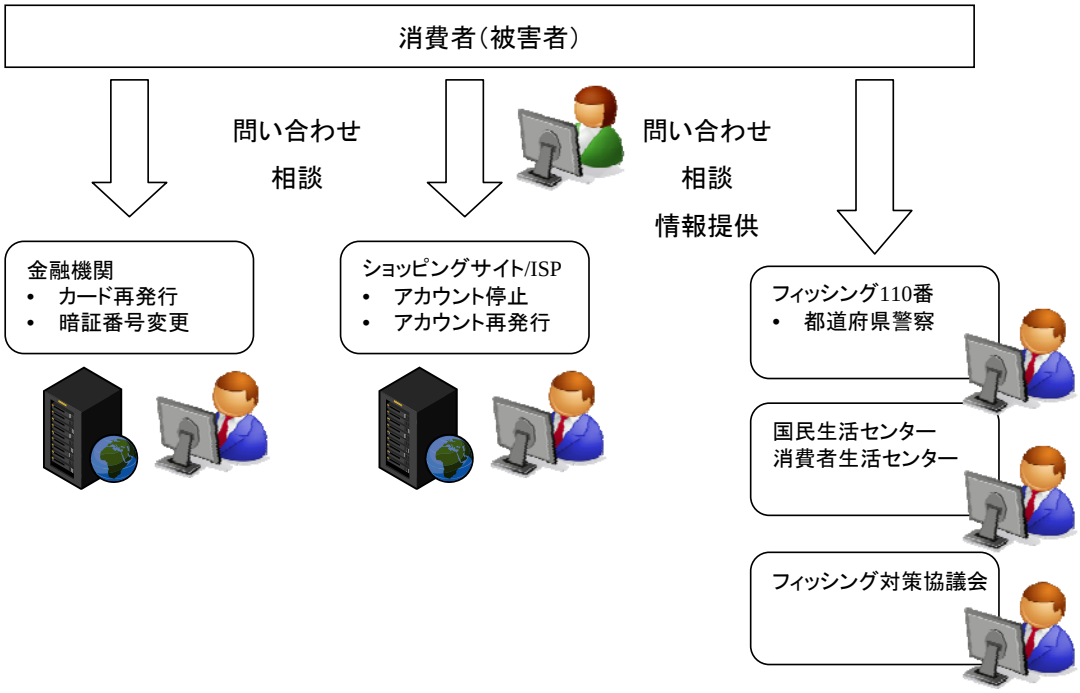
フィッシング詐欺被害に遭った疑いを感じた場合、どの情報が詐取されたのかを把握する必要がある。しかし、フィッシングサイトに情報を入力した瞬間に気が付いたのであれば、詐取された情報について把握できても、銀行口座やクレジットカード利用履歴等に覚えの無い取引を見つけてフィッシング詐欺の疑いを持った場合においては、詐取された情報の詳細までは記憶に無いこともあるだろう。こういった場合には、該当するサービス事業者に直ちに連絡をとり、アカウントの停止措置を含め、対策を協議する必要がある。

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

4.2.2. 関連機関への連絡

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

※フィッシング対策には最新版ガイドラインをご活用ください



フィッシング 110 番：相談/情報提供

国民生活センター/消費者生活センター：相談

フィッシング対策協議会：情報提供

図 6 フィッシング被害に遭ってしまった時の問い合わせ、相談、情報提供

（1） 被害が発生したサービス事業者への連絡

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

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

（2） 警察への連絡

金銭的な被害等、実質的な被害が確認された場合には、被害者の居住する地区の都道府県警察サイバー犯罪相談窓口[18]へ連絡する。

（3） 国民生活センターまたは各地の消費生活センターへの連絡

国民生活センターまたは各地の消費生活センターは消費生活全般に関する苦情や問合せなど、利用者からの相談を専門の相談員が受付け、公正な立場で対応している。フィッシング被害に関しても苦情や相談が必要な場合には、これらのセンターに相談をする。

[18] http://www.npa.go.jp/cyber/policy/phishing/phishing110.htm

（4） フィッシング対策協議会への情報提供

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

表 2 フィッシング対策協議会連絡先

ウェブサイト URI	https://www.antiphishing.jp/
電子メールアドレス	info@antiphishing.jp

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

Subject:フィッシングメールに関する情報提供

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

--
〇〇 〇〇(報告者氏名、匿名での報告も可)

図 7 フィッシングメール報告の例

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

Subject:フィッシング被害に関する情報提供

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

--

〇〇 〇〇(報告者氏名、匿名での報告も可)

図 8 フィッシング被害報告の例

※フィッシング対策には最新版ガイドラインをご活用ください

5. 付録

付録 A－サービス事業者が考慮すべき要件一覧

【 利用者が正規メールとフィッシングメールを判別可能とする対策 】
- 【要件 1】 ◎：利用者に送信するメールには電子署名を付与すること
- 【要件 2】 ◎：外部送信用メールサーバを送信ドメイン認証に対応させること
- 【要件 3】 ◎：利用者に送信するメールでは定型的な様式を用いること
- 【要件 4】 ◎：サービス事業者が利用者に送信するメールは TEXT 形式とすること
- 【要件 5】 ◎：利用者にメール送信する状況及び内容を周知しておくこと

【 利用者が正規サイトとフィッシングサイトを判別可能とする対策 】
- 【要件 6】 ◎：Web サイトの安全性を確保すること
- 【要件 7】 ◎：Web サイトの正当性に係る情報を十分に提供する画面とすること
- 【要件 8】 ◎：重要情報を入力するページは SSL/TLS で保護すること
- 【要件 9】 ◎：Web サイト運営者の連絡先及びガイダンス等、利用者に間違いなく情報を伝える必要のあるページは SSL/TLS で保護すること
- 【要件 10】 ◎：正規 Web サイトのドメイン内設置サーバの安全性を確認すること
- 【要件 11】 ○：認証システムが許容するポリシを利用者に示すこと
- 【要件 12】 ○：正規サイトの全てのページに利用者に対する脅威の状況を表示する
- 【要件 13】 △：認証画面には利用者個別のマーク等を表示できるようにする

【 フィッシング詐欺被害を拡大させないための対策 】
- 【要件 14】 ◎：資産の移動に限度額を設定すること
- 【要件 15】 ◎：資産の移動時に利用者に通知を行うこと
- 【要件 16】 ○：正規 Web サイトにアクセス可能な端末を制限すること
- 【要件 17】 ○：携帯電話によるサービス利用は利用者の選択制とすること
- 【要件 18】 ○：機微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 19】 ○：重要情報の表示については制限を行う
- 【要件 20】 ○：パスワードのブラウザへの保存ついては禁止する
- 【要件 21】 ◎：アクセス履歴の表示
- 【要件 22】 △：特別な認証方法を採用する場合には、その方式に特有のぜい弱性対策を行うこと
- 【要件 23】 ○：正規サイトログイン時の認証には複数要素認証を利用すること

【 ドメイン名に関する配慮事項 】
- 【要件 24】 ◎：利用者の認知しているサービス事業者名称から連想されるドメイン名とすること
- 【要件 25】 ◎：悪用される可能性の高い類似ドメイン名を登録しておくこと
- 【要件 26】 ◎：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 27】 ○：ドメイン名に見た目が紛らわしい文字を含めないこと

【 組織的な対応体制の整備 】
- 【要件 28】 ◎：フィッシング詐欺対応に必要な機能を備えた組織編制とすること
- 【要件 29】 ◎：フィッシング詐欺に関する報告窓口を設けること
- 【要件 30】 ◎：フィッシング詐欺発生時の行動計画を策定すること

- 【要件 31】 ◎：フィッシング詐欺及び対策に関わる最新の情報を収集すること
- 【要件 32】 ◎：フィッシングサイト閉鎖体制の整備をしておくこと
- 【要件 33】 ○：フィッシングサイトアクセスブロック体制の整備をしておくこと

【 利用者への啓発活動 】

- 【要件 34】 ◎：利用者が実施すべきフィッシング詐欺対策啓発活動を行うこと
- 【要件 35】 ◎：フィッシング詐欺発生時の利用者との通信手段を整備しておくこと

【 フィッシング詐欺被害の発生を迅速に検知するための対策 】

- 【要件 36】 ○：Web サイトに対する不審なアクセスを監視すること
- 【要件 37】 △：フィッシング詐欺検出サービスを活用すること

付録 B－利用者が考慮すべき要件一覧

【 フィッシング詐欺 】

- 【要件 38】◎：機微情報の入力を求めるメールを信用しない
- 【要件 39】◎：メールに記載される差出人名称は信用しない
- 【要件 40】◎：怪しいメールの判断基準を知る
- 【要件 41】◎：安全なメールサーバを活用したり、類似性評価によるフィッシングメール判別機能を活用すること
- 【要件 42】◎：リンクにアクセスする前に正規メールかどうか確認する

【 電子メール本文中のリンクの扱い 】

- 【要件 43】 ◎：正しい URL を確認する
- 【要件 44】 ◎：電子メール本文中のリンクには原則としてアクセスしない
- 【要件 45】 ◎：錠前マークを確認する
- 【要件 46】 ○：サービス事業者からの通知メール形式を TEXT 形式に設定する
- 【要件 47】 ○：リンク先で機微情報の入力を求められた場合には、電話等でサービス事業者に真偽を確認する

【 パソコンを安全に保つために 】

- 【要件 48】 ◎：最新のセキュリティパッチを確実に適用する
- 【要件 49】 ◎：セキュリティ対策ソフトウエアの機能を理解し適切に用いる
- 【要件 50】 ◎：Web ブラウザにフィッシングサイト判別機能を組込み活用すること
- 【要件 51】 ○：PC の利用には標準ユーザアカウントを利用し、ユーザアカウント制御機能を活用すること

【要件 52】 ○：URL フィルタリングを活用すること

【 アカウント情報の管理 】

- 【要件 53】 ◎：アカウント ID/パスワードはサービス事業者別に設定すること
- 【要件 54】 ◎：アカウント管理ソフトウエアを導入する
- 【要件 55】 ◎：全てのアカウントについて緊急連絡先を把握しておくこと

付録 C－参考情報

※フィッシング対策には最新版ガイドラインをご活用ください

C.1 【被害にあわないための 5 か条】

- 「被害にあわないための 5 か条」, フィッシング対策協議会, 2006
  https://www.antiphishing.jp/stop_phishing/gokajou.html

（利用者にとってフィッシング詐欺にあわないための基本的対策事項を案内している）

C.2 【情報サイト】

- internet.com
  http://japan.internet.com/security/
- CNET ネットワークス
  http://japan.cnet.com/news/sec/
- ZDNet
  http://japan.zdnet.com/security/
- 日本経済新聞デジタルメディア
  http://it.nikkei.co.jp/security/index.aspx
- ITmedia
  http://www.itmedia.co.jp/news/security/

（フィッシング含む情報セキュリティに関するニュース/記事が掲載されている）

C.3 【業界団体と各省庁のサイト]

- 経済産業省
  http://www.meti.go.jp/policy/netsecurity/
- 総務省
  http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/
- 警察庁
  http://www.npa.go.jp/cyber/index.html
- 消費者庁
  http://www.caa.go.jp/
- 独立行政法人 情報処理推進機構（IPA）
  http://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
  http://www.jnsa.org/

（各省庁・団体における情報セキュリティ関係の情報が掲載されている）

C.4 【安全な Web サイトの利用】

- 「安全な Web サイト利用の鉄則」独立行政法人 産業技術総合研究所, 2007
  http://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及びその鉄則さえ守っていれば安全となるようなサイト作りに必要な設計の要件が記載されている）

C.5 【サイトの脆弱性対策】

- 「安全な Web サイトの作り方」独立行政法人 情報処理推進機構
  http://www.ipa.go.jp/security/vuln/websecurity.html
  （IPA への届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）

※フィッシング対策には最新版ガイドラインをご活用ください

・「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
http://www.ipa.go.jp/security/awareness/vendor/programmingv2/index.html
（ソフトウエア開発工程における上流工程（要件定義、設計）から脆弱性対策の論点を意識できるようにするための情報が記載されている）

C.6 【送信ドメイン認証】

・「送信ドメイン認証」Japan Email Anti-Abuse Group（JEAG）
http://jeag.jp/swg/senderauth/
（送信ドメイン認証に関する資料が掲載されている）
・「SPF（Sender Policy Framework）」財団法人インターネット協会(IAjapan)
http://salt.iajapan.org/wpmu/anti_spam/admin/tech/explanation/spf/
・「DKIM (Domainkeys Identified Mail)」Japan DKIM Working Group | dkim.jp
http://www.dkim.jp
・「DKIM (Domainkeys Identified Mail)」財団法人インターネット協会(IAjapan)
http://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)
http://www.dekyo.or.jp/soudan/anti_spam/report.html#dam
・「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)
http://www.dekyo.or.jp/soudan/anti_spam/report.html#auth

C.7 【CSIRT への支援要請】

・「インシデント報告の届出」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）

C.8 【Web ブラウザのフィッシングサイト対策機能】

・ 「フィッシング詐欺検出機能」
http://www.microsoft.com/japan/protect/products/yourself/phishingfilter.mspx
・「フィッシング詐欺・マルウェア対策機能」
http://mozilla.jp/firefox/phishing-protection/
（Firefox に搭載されているフィッシング詐欺・マルウェア対策機能について掲載されている）

C.9 【フィッシング 110 番】

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

C.10 【国民生活センター・消費生活センター】

・「国民生活センター」
http://www.kokusen.go.jp/
（消費者からの相談事例などが掲載されている）
・「全国の消費生活センター」
http://www.kokusen.go.jp/map/
（各居住地の相談窓口一覧が掲載されている）

C.11 【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、報告書等を公開している）

※フィッシング対策には最新版ガイドラインをご活用ください

付録 D–プロバイダへのテイクダウン要請文例

Dear Sirs and Madams,

[簡潔な企業プロファイル].

We found a fraudulent website that you appear to be providing internet services. The fraudulent website is located at the following website address.

＜当該フィッシングサイトの URI＞

Please take all necessary measures to immediately take down the fraudulent website.

We would appreciate your cooperation to terminate the fraudulent activities.

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]

※フィッシング対策には最新版ガイドラインをご活用ください

付録 E–事業者における NG 集

■サービス提供者の体制の不備

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

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

・　フィッシング発生時の対応方法が未整備
利用者からの通報などにより、フィッシング詐欺の発生を認知した場合、事前に整備・確認した手順に基づき、迅速にフィッシングサイトのテイクダウン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、セキュリティを保つ維持・運用の稼動とコストの考慮が手薄である。
フィッシング詐欺の主な対象となる認証システムのセキュリティを確保し続けるためには、開発時のみならず、日常のセキュリティ維持のための稼動とコストを伴う。Web アプリケーションの脆弱性診断、OS やミドルウェアの脆弱性対応、サーバ証明書費用等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 等による他社の 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。

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

■利用者へのメール送信

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

・　利用者にＩＤやパスワードなどの入力を求めるサービス運営を行っている。
通常のサービス運営において、ID やパスワードなどの重要情報の Web サイトへの入力を求める場合があると、利用者は、フィッシング詐欺メールとの区別がつきにくく、疑いを持たずに情報を入力してしまう。該当の運用がある場合は、運用の見直しを検討し、極力廃止するとともに、利用者に情報を入力してもらうケースは無いことを明示する。ただし、利用者に、フィッシング詐欺に遭ったことを通知し、パスワード変更を促す場合、電子証明書や EVSSL などによりそのメールや Web サイトが本物であることが判別できるよう、十分に配慮する。

■Web サイト運用

・　SSL/TLS 通信（https 通信）を正しく使用していない①
入力データの保護のみに注意が向き、SSL/TLS 通信およびサーバ証明書をフォームの送信先 Web サイトのみに導入し、入力フォーム自体を表示する Web サイトには導入していないケースが見られる。この場合、利用者に入力フォーム自体を表示するサイトの正当性を示すことができていないため、フィッシングサイトが発生した場合、利用者は偽物であることに気づきにくくなる。なお、入力フォームを表示するサイトと入力データを送信する先のサイトは極力同一とすることが望ましい。
　※通常は、同一であるサイトがほとんど。
たとえ両サイトが SSL/TLS 通信およびサーバ証明書によって正当性を証明されていても、利用者は入力フォームを表示したサイトを信頼しデータを入力するのであり、送信先サイトはデータ入力時点では確認できない。

・　SSL/TLS 通信（https 通信）を正しく使用していない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、SSL/TLS 通信を使わない通常の Web サイトのものであるなど、非 SSL/TLS 通信のパーツが混在した場合、多くのブラウザは、その旨をアラート表示し、該当画像を表示するかどうか確認を求める。ここで、表示する選択をした場合、サーバ証明書による Web サイトの正当性は証明されなくなる。（鍵マークが表示されない。）Web ページを構成する画像等の全てのパーツが、正当な SSL/TLS 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、十分検討し決定する。検討に当たっては、サービスが扱う情報の重要性や利用者のリテラシー、利用便性などに加え、利用者は同一の ID やパスワードを複数の Web サイトに設定する傾向があることから、万が一フィッシング詐欺に遭った場合、被害が他サイトにも拡大する可能性があることも十分考慮し、可能な限り厳しい基準を設ける。
　※最短文字数を長く。最低限含める文字種を多く。ID はユーザ任意ではなく、システムによる発行とする。など。

6. 検討メンバ

本ガイドラインの検討を行ったフィッシング対策協議会 平成 24 年度ガイドライン策定ワーキンググループの構成は次の通りである（所属は 2013 年 3 月時点）。

区分	氏名	所属
主査	内田 勝也	情報セキュリティ大学院大学名誉教授
副主査	野々下幸治	トレンドマイクロ株式会社
	本多 規克	アルプス システム インテグレーション株式会社
	水村 明博	EMC ジャパン株式会社
	加藤 孝浩	トッパン・フォームズ株式会社
	林 憲明	トレンドマイクロ株式会社
	早川 和実	NTT コミュニケーションズ株式会社
	八津川 直伸	日本ユニシス株式会社
	佐々木 智彦	楽天株式会社
	松田 知行	ネットスター株式会社
	山本 和輝	BB ソフトサービス株式会社
オブザーバ	経済産業省商務情報政策局情報セキュリティ政策室	
事務局	一般社団法人 JPCERT コーディネーションセンター	
	株式会社三菱総合研究所	