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

# 利用者向け

# フィッシング詐欺対策ガイドライン

2024 年度版

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

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

# 目次

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

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

## 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が講じておくべき対策について、昨今のフィッシング事例をもとに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。

## 2. フィッシングとは　～あなたの「情報」が狙われている～

フィッシング（Phishing）とは、「魚を釣る（Fishing）」フィッシングになぞらえて、人をだまして情報を盗み、最終的に金銭的な利益を得ようとする不正行為のことを意味します。フィッシングにより、例えば、あなたのクレジットカード情報やインターネットバンク、ショッピングサイトの登録情報（ID、パスワード）が盗まれ、勝手にお金が引き出されたり、物品を購入されたりする恐れがあります。

魚釣り（Fishing）と紛らわしいので、「フィッシング詐欺[1]」と呼ばれることもあります。その定義はさまざまですが、本ガイドラインでは次のように定義しています。

> フィッシング（Phishing）とは、実在する組織をかたって、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個人情報を詐取すること。

魚釣りにたとえると、魚を集めるための撒き餌として電子メール（フィッシングメールと呼びます）を大量に送りつけ、魚を釣るための釣り針として正規 Web サイトの模倣サイト（フィッシングサイト）を設置し、魚、つまりインターネットユーザーがかかるのを待つという一連の行為となります。

犯罪者は利用者が気付きにくい手口や、思いもよらない新しい手口を次々と編み出してくるため、これまでの知識だけでは、被害を防ぐことが困難になっています。

被害に遭わないようにするためには、つねに関心と警戒意識を維持することが大切です。

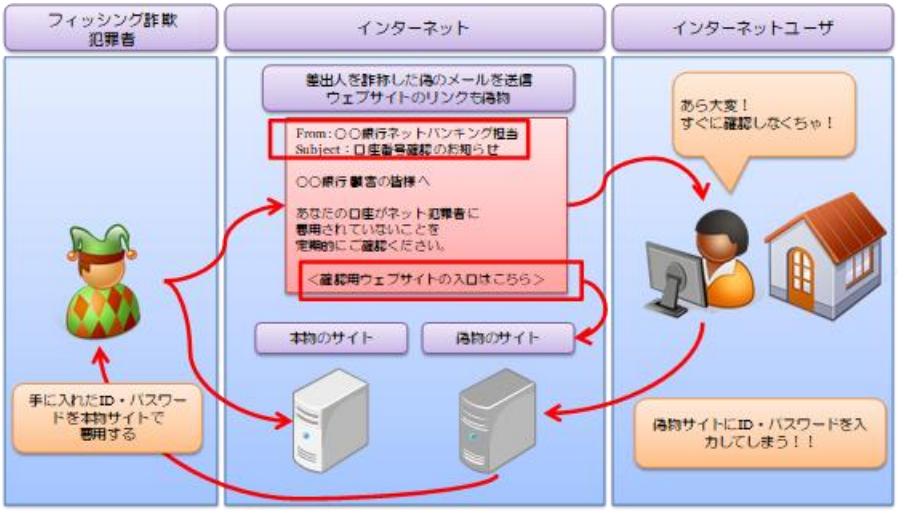


図 2-1　典型的な「フィッシング」行為

[1] 2012 年 3 月に不正アクセス禁止法が改正され、2012 年 5 月に改正法が施行されたことにより、フィッシング行為が処罰対象となりました。

## 2.1 類似手法　～フィッシングだけではありません～

2022 年時点では[2]、国内におけるインターネット利用率は約 85%となっており、その 7 割以上がスマートフォンを利用しています。以前は PC をマルウェアに感染させ犯罪者が使用するネットワーク（ボットネット）の支配下に置き、遠隔操作でフィッシングメールなど不正メールの配信を行わせたりしていましたが、近年はひと昔前のパソコン並みに性能が向上したスマートフォンが狙われるようになってきました。本ガイドラインで対象とするフィッシングだけでなく、このようなだましの手法にも十分な注意が必要です。

### 2.1.1 スマートフォンの個人情報等を狙う不正アプリ

不正アプリをインストールさせる代表的な手口としては、宅配便の不在連絡を装う SMS からの誘導が最も多く、2018 年から現在に至るまで続いています。SMS 内のリンクへアクセスすると、Android 端末は再配達申請を行うための正規アプリや、セキュリティ対策アプリをインストール・更新するよう促されます。また、iPhone などの Apple 端末は不正アプリのインストールではなく、同一のリンクからモバイルキャリアや銀行、Apple などをかたるフィッシングサイトへ誘導されます。

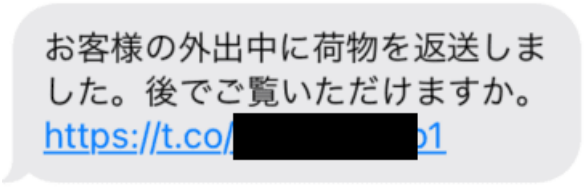


図 2-2　メール・SMS の文面例 1


図 2-3　メール・SMS の文面例 2

[2] 総務省：令和 5 年　情報通信に関する現状報告の概要
第 2 部 情報通信分野の現状と課題 第 11 節 デジタル活用の動向
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/html/nd24b120.html


図 2-4　フィッシングサイトまたは不正アプリのインストールへ誘導される例[3]

不正アプリをインストールすると、遠隔操作で自分のスマートフォンから不正な SMS を配信させられるため、問い合わせや苦情の電話が殺到したり、SMS 配信料金で高額な請求がくることで、初めて異変に気が付くケースが多いようです。アプリをインストールする際には「4 .6. 正規アプリをインストール」も参考に、正規のアプリストアからのみインストールするよう心がけてください。

『フィッシングレポート 2024』「不正アプリ検知ツールで検知した直近の「悪性アプリ」」にも事例が掲載されておりますので、ご参照ください。

[3] フィッシング対策協議会：ソフトバンクをかたるフィッシング (2022/12/01)
https://www.antiphishing.jp/news/alert/softbank_20221201.html より

## 3. フィッシング対策３つの心得

フィッシングの被害は世界中で発生しており、年間の被害額は数千億円ともいわれており、日本でも多数の被害が出ています。ここでは、フィッシングに遭わないための 3 つの心得（STOP. THINK. CONNECT.）を示します。STOP. THINK. CONNECT.は、全世界共通のサイバーセキュリティキャンペーン（https://stopthinkconnect.jp/）です。

### STOP.　立ち止まって理解する

インターネットは便利ですが、一般社会と同様、そこには危険もあります。どのような危険があるかを知り、解決策をどのように見つけるかについて、一旦、立ち止まって調べましょう。

### THINK.　何が起こるか考える

さまざまな警告の見極め方を知る必要があります。警告を確認したら、これからとろうとする行動がコンピューターやあなた自身の安全を脅かさないか考えましょう。

一般にフィッシングは、クレジット会社やネットショッピングサイトであるかのように、差出人を偽装、文面を工夫した電子メールなどを被害者に送りつけるところから始まります（餌を撒く）。この段階で疑いを持ち、信憑性を確認できれば被害を受けずにすませることができます。もし、電子メールを疑わずに、リンクをクリックしてしまった場合、ウイルスに感染させられたり、偽の入力フォームに個人情報を入力させられるなどにより重要な情報（ユーザーID、パスワード、クレジットカード番号、金融口座番号、個人情報など）を盗まれる可能性があります。リンクをクリックする前に、「もしかして怪しい？」と感じることができれば、被害を避けることができます。

### CONNECT.　安心してインターネットを楽しむ

危険を理解し、十分な対策をとれば、インターネットをより信頼できるようになるでしょう。

上記の心得を忘れずに、インターネットを楽しんでください。

# 4. 今すぐできるフィッシング対策

ここでは、フィッシングに遭わないために日ごろから心がけること、フィッシング対策を解説します。

## 4.1 フィッシングメール対策をする

### 4.1.1 迷惑メールフィルターを使う

フィッシングメールは迷惑メールの一種であり、迷惑メールフィルターでその多くが検知、分別、削除できます。ほとんどのメールサービスでは迷惑メールフィルターが利用できますが、標準では設定が無効となっていることが多いため、設定を確認し、有効にしましょう。メールアプリやセキュリティ対策ツールの迷惑メールフィルター機能も併用すると効果的です。

### 4.1.2 メールアドレスを新しく作る

フィッシングメールや迷惑メールは、一度届きはじめると、止まることはありません。大量にそのようなメールが届いている場合は、そのメールアドレスが広くインターネット上に漏えいしてしまっていることを意味します。漏えいした情報は完全に消すことはできません。同時にパスワードも漏えいしている可能性もあるため、安全のためメールアドレスを新しく作り、利用中のオンラインサービスに登録し直しましょう。

### 4.1.3 不正メール対策が充実したメールサービスを使う

メールサービスによって、不正メール対策機能に差があります。メールサービスを選ぶ際には、フィッシング対策に有効な以下の要件に対応しているか、確認すると良いでしょう。

- メールの認証（送信ドメイン認証）に対応している
- 認証された正規メールにアイコンやマークが付く（「4.4.2 正規メールに付くアイコンやマークの確認」を参照）
- すり抜けた不正メールを報告するための、メールサービスの窓口がある

### 4.1.4 スマートフォンでは SMS フィルターを使う

スマートフォンでは Email 以外に SMS（ショートメッセージサービス：電話番号宛に短いメッセージを送る機能）を使ったフィッシングが流行しています。これを防ぐには、①アドレス帳以外の人からの SMS を受信しない機能、②通信キャリアが提供し

ている迷惑メールフィルターサービスや③リンク付きSMS拒否機能など、ご自身にとって好ましくないSMSをフィルター（遮断）する方法が複数あります。利用している通信キャリアによってサービス内容は異なりますが、いずれも積極的に使うことでフィッシング詐欺に遭遇する可能性を減らせます。

## 4.2 Webフィルターを活用する

パソコンやスマートフォンに入っている標準のWebブラウザーはWebフィルター機能があります。フィッシングサイトや危険なサイトを閲覧しようとすると、警告画面を表示してブロックしてくれます。ブラウザーによって警告が表示されるまでの時間に差があるため、早く警告が出るブラウザーを使ったり、セキュリティ対策ツールのフィルターも併用すると良いでしょう。

例）

- Google セーフブラウジング （対象ブラウザー: Chrome、Safari、Firefox）
- マイクロソフト SmartScreen （対象ブラウザー: Edge）

## 4.3 正しいURLや正規のアプリケーションを用いてアクセスする

### 4.3.1 ブックマークや正規のアプリケーションを活用する

オンラインサービス初回利用時にはそのドメイン名を利用者カード／請求書などで確認し、直接入力してください。初回利用時にブラウザー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す。事業者が提供している正規のスマホアプリを利用することも有効です。スマホアプリをダウンロードする際は正規の提供元（Google Play や App Store）から入手してください。偽のバナー広告や検索結果からフィッシングサイトに誘導される事例もあり、特によく利用するオンラインサービスについては、ブックマークや正規のスマホアプリを活用するようにしてください。また、定期的にブックマークが正しいものかを確認し、更新するようにしてください。

ただし、ブックマークを作成する際やアプリをダウンロードする際には、タイポスワッピング（似たような文字列のドメイン名を利用した詐欺）に特に注意が必要です。ドメイン名やアプリ名を入力する時には、文字の一つ一つを慎重に確認してください。

### 4.3.2 正規メール以外のメール中のリンクからはアクセスしない

正規メールであると認証(「4.4.2 正規メールに付くアイコンやマークの確認」を参照)されていないメール中のリンクはアクセスすると危ないサイトに行く可能性があるため、安易にアクセスしないでください。もしアクセスする必要がある場合は、ブラ

ウザーに登録したブックマークや正規アプリからアクセスして、状況を確認してください。

マウスカーソルをリンクに重ねたり、スマートフォンの場合はリンクを長押しするとリンクの内容が表示されるので、文字列としてフィッシングで無いことを確認してからアクセスするように心がけてください。なお Apple 端末の場合は、リンク長押しでプレビューを表示するとサイトへアクセスしてしまうため、あらかじめ安全なサイトでリンクを長押しして、プレビューを非表示にすることもできます。

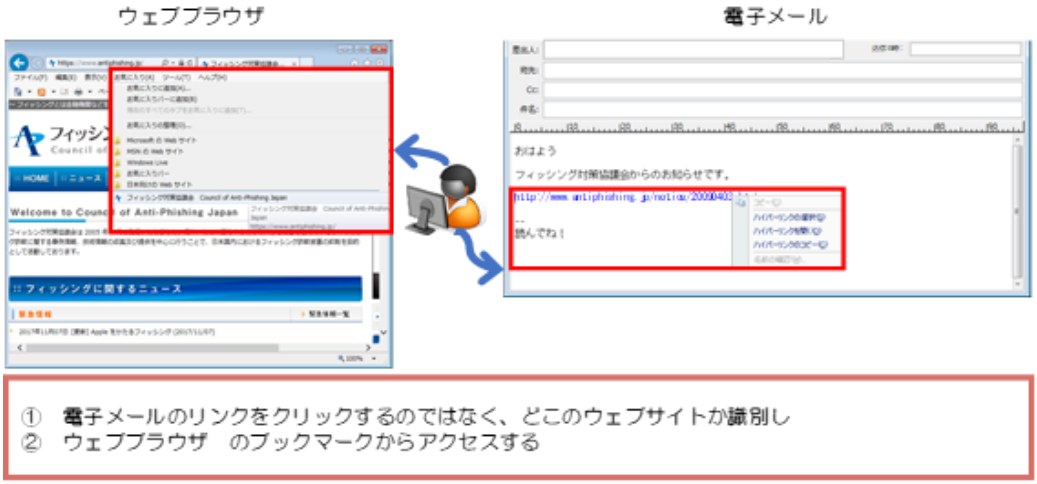


図 4-1　Web ブラウザーのブックマークの活用

### 4.3.3 Web サイトに不審な点がないかを確認する

フィッシングサイトはそのサービスの正規の Web サイトをコピーして作られることが多く、その Web サイトが本来アクセスしようとしている Web サイトなのか、それとも見た目がそっくりに作られているだけの偽の Web サイトなのかを見分けることは非常に困難です。

最近はパソコンやスマートフォンの Web サイトに関する表示の方法がさまざまになっているので、まず、ご自身が使っているブラウザーやスマートフォンでドメイン名や鍵マークが、普段、どのように表示されるのかを確認しておきましょう。その後、次の方法を使って確認しましょう。

Web サイトに不審な点がないかを確認する方法：

（1） ドメイン名が正しいか、不審なサイトではないかを確認する

正規のドメイン名が分かっている場合には、ブラウザーの上部または下部に表示されている Web サイトの URL のドメイン名が一致しているかどうかを確認します。ドメイン名は「https://（ドメイン名）/」もしくは「（鍵マーク）（ドメイン名）」の

ように表示されます。ドメイン名が分からない場合は、表示されたドメイン名をネットで調べて、フィッシングや詐欺の情報がないか、確認しましょう。

また、ドメイン名の表示についてブラウザーごとに表示が変わるように注意が必要です。以下に例を示します。

Microsoft Edge、Safari では「https://」のサイトではドメインの左に鍵マークが表示されます。

Google Chrome 「https://」のサイトでは鍵マークは表示されません。一方で「https://」で暗号化されていないサイトにアクセスすると「保護されていない通信」と表示されます。


図 4-2　PC 版 Safari の場合


図 4-3　PC 版 Google Chrome の場合


図 4-4　スマートフォン(iOS)版 Safari の場合


図 4-5　スマートフォン(Android)版 Google Chrome の場合

（2） Web サイトを運営している組織の表示を確認する
－組織の名称が表示されている場合－

URL が表示されるところに Web サイトを運営している会社などの組織の名称が表示されている場合には、その名称が、アクセスしようとしている Web サイトの会社名と一緒になっていることを確認します。

（3） 証明書の内容を確認する

「https://」から始まる URL にもかかわらずフィッシングサイトであるケースが増えています。当該サイトでは、Web サイトとの通信が暗号化されているという意味と、Web サイトを運営している組織が実在しているといった全く異なる意味がありますが、いずれも同じように表示されています。「https://」から始まるサイトだけで安心せず、より詳しく、もしくは他の方法と組み合わせて確認しましょう。

確認のポイント：

- 発行先／証明書の発行先
  - Web サイトを運営している法人などの組織の名称になっているかどうかを確認します。特に、銀行、オンラインショッピング、電子申請の Web サイトでは、その Web サイトを運営している会社の名称になっていることを確認します。

Web サイトが正しいかどうかの確認ができないときには、利用を止めます。特に、銀行、オンラインショッピング、オンラインの電子申請の Web サイトにアクセスするときには注意が必要です。

どうしても利用したい時や、初めてアクセスする Web サイトであって、偽サイトかどうかが分かりにくい場合には、URL がフィッシングサイトのものでないかどうかを調べることが考えられます。その方法として、そのサービスを提供している事業者によって提供された Web 以外の情報、例えば新聞や広告を使って正しい URL を知ることが考えられます。厳密さが問われる場合にはサポート窓口に電話で確認する方法もあります。この他には、初めて利用する URL であれば、その URL をいくつかの検索サイトで検索して、偽サイトであるという発言があるかどうかを調べる方法も考えられます。

## 4.4 なりすましメールに注意しましょう

### 4.4.1 銀行やショッピングサイトなどのサービス内容を確認しましょう

メールの差出人情報などは簡単に詐称ができ、差出人情報などを頼りにメールの真偽を見抜くことは不可能です。銀行やショッピングサイトなどからどのようなタイミングで、どのようなメールが届くかを事前に理解し、それに当てはまらないものはすべて怪しいと考えることが大切です。電子メールだけでなく、SNS（Social Networking Service）や SMS（Short Message Service）による連絡においても同様です。


図 4-6　怪しいメールの例[4]

[4] フィッシング対策協議会: ゆうちょ銀行をかたるフィッシング (2022/11/08)
https://www.antiphishing.jp/news/alert/japanpostbank_20221108.html


図 4-7　怪しい SMS の例[5]

例えば、国税庁（国税局、税務署を含む）、各配達業者では SMS による案内は送信していない、と注意喚起しています。国内のある銀行では Web サイト上で、第二認証カードの番号すべての入力を求めることはないとしています。また別の事業者ではメールにてパスワードの変更を依頼することはないとしています。このように各社のサービス内容を事前に確認しておくことで、本来あり得ない問い合わせを見抜くことが可能です。

### 4.4.2 正規メールに付くアイコンやマークの確認

「送信ドメイン認証」という技術を使い、認証された正規メールにブランドアイコンやマークを表示するメールサービスが増えています。アイコンが表示されるためには厳しいセキュリティ要件を満たす必要があり、2023 年現在では、以下のメールサービスが対応しています。

- Gmail
- Apple iCloud メール
- Yahoo！JAPAN メール
- ドコモメール
- au メール

---

[5] ソフトバンクをかたるフィッシング (2022/12/01)
https://www.antiphishing.jp/news/alert/softbank_20221201.html
au および KDDI をかたるフィッシング (2021/11/26)
https://www.antiphishing.jp/news/alert/au_kddi_20211126.html
国税庁をかたるフィッシング (2022/08/15)
https://www.antiphishing.jp/news/alert/nta_20220815.html
宅配便の不在通知を装うフィッシング (2020/12/18)
https://www.antiphishing.jp/news/alert/fuzaiSMS_20201218.html
NTT ドコモをかたるフィッシング (2022/02/10)
https://www.antiphishing.jp/news/alert/nttdocomo_20220210.html

モバイル環境での対応率が非常に高く、セキュリティ意識の高いサービスはこのような正規メールの視認性向上に対応しています。そのようなサービスは安心して利用することができるとも言えます。

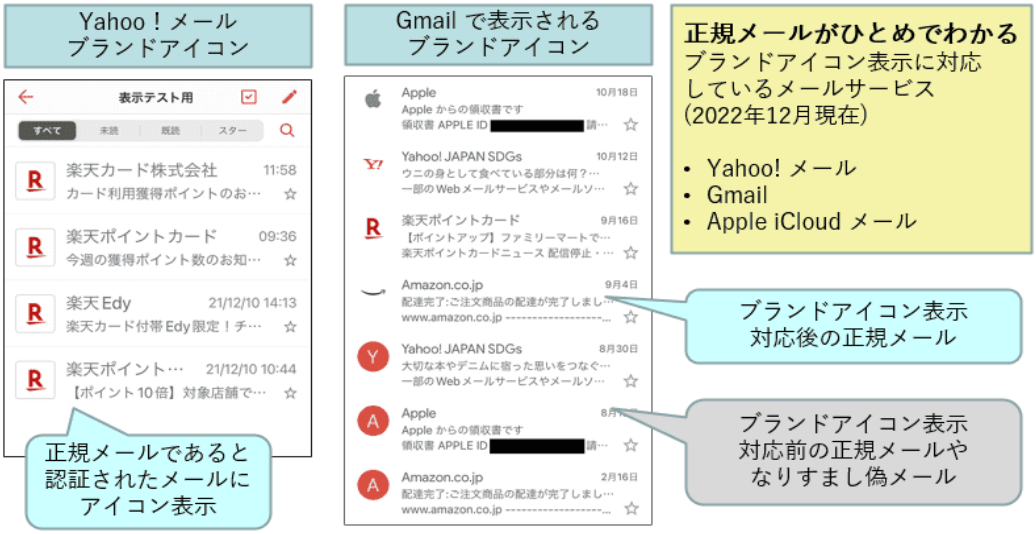


図 4-8　各社のアイコンやマークの例

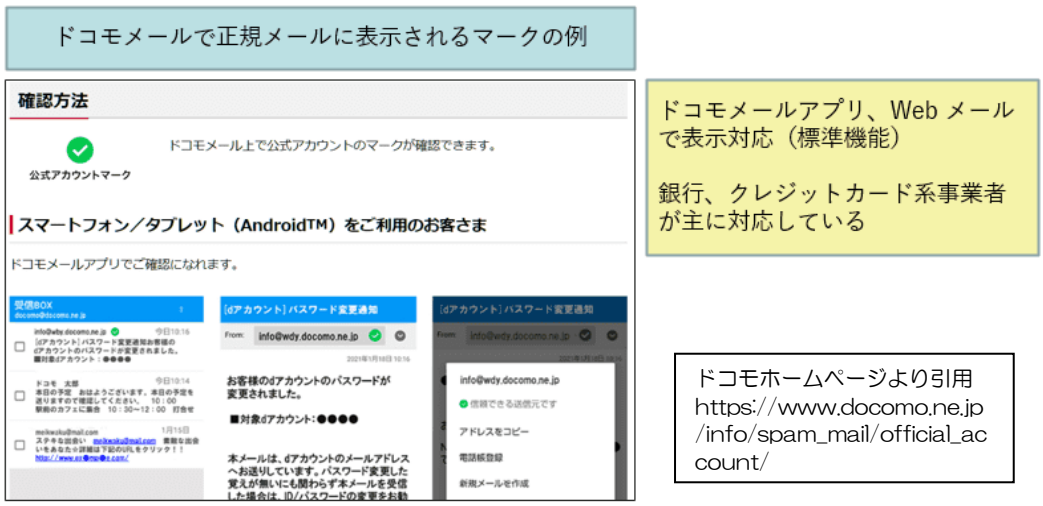


図 4-9　各社のアイコンやマークの例[6]

### 4.4.3 電子署名の確認

銀行によっては電子メールに電子署名を付与してメールを送っています。その理由は電子署名を付けることにより、電子メールの送信元の確認と改ざんされてないこと

[6] ドコモホームページより引用
https://www.docomo.ne.jp/info/spam_mail/official_account/

を確認することができるためです。多くの銀行は電子署名に S/MIME[7]という規格を採用しており、S/MIME を使用した電子署名付き電子メールは、メール本文と電子証明書に電子署名が付加され、添付ファイルとしてユーザーに送信されます。ユーザーは電子署名を確認することで、正規の事業者から送られているものや改ざんされてないことを確認することが可能ですので、怪しいメールが届いた際には電子署名を確認するようにしましょう。

※S/MIME の確認にはメールソフトが対応している必要があります。

### 4.4.4 SMS（Short Message Service）の発信者番号表示の確認

SMS を使ったフィッシングは増加する中、手法も多様化しています。SMS の配信には以下の 3 種類があり、国際網経由の SMS についてはフィッシングの可能性を疑い、慎重に行動することが大切です。SMS が届いた際には発信者番号表示の電話番号が海外の電話番号やアルファベットになっていないことを確認しましょう。また、近年は不審な SMS のリンクから不正アプリをインストールしてしまい、乗っ取られた一般利用者のスマートフォンからのスミッシング[8]配信が非常に多いので、発信者番号が携帯電話番号の場合は、正規の発信者であるか、事業者のホームページを確認しましょう。事業者名が判らない場合は、リンクにアクセスしないようにしましょう。

SMS の送信元には、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事業者も増えてきています。この番号を利用する事業者は携帯キャリアからの認証を得ているため、事業者になりすまして怪しいメッセージが送信される可能性は低いと考えられます。

| SMS 配信方式 | 発信者番号表示 |
|---|---|
| 国内直接接続 | 日本の固定電話番号　（例：03-0000-0000）<br>携帯キャリア 4 社の共通番号（例：0005-000000）<br>携帯キャリアごとの特別番号（例：50000,240000） |
| 国際網を経由 | 海外の電話番号　（例：+1 000-000-0000）<br>アルファベット　（例：info, その他企業名等） |
| 携帯電話端末または SIM カードを用いたシステム | 日本の携帯電話番号　（例：090-0000-0000） |

[7] S/MIME は PKI を利用した電子証明書を用いる手法で、電子メールの暗号化や電子署名を行うことができます。

[8] 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のこと。


図 4-10　SMS 配信経路の種類と怪しい SMS の例

また、SMS の次世代版である RCS（Rich Communication Service）に準拠したサービス「＋メッセージ」では企業が携帯キャリア 3 社それぞれの審査を受け、認証を得たことを示す「認証済みマーク」が表示される仕組みがあります。「+メッセージ」で企業からのメッセージを受信した場合は「認証済みマーク」を確認しましょう。


図 4-11　認証済みマークのイメージの例[9]

[9] 出典：NTT ドコモ
https://www.nttdocomo.co.jp/info/news_release/2019/04/23_00.html より

## 4.5 パソコンやモバイル端末を安全に保ちましょう
## ～パソコンやスマートフォンを安心して使うために～

パソコンやスマートフォンを使っているとき、気付かないうちにフィッシングにあってしまうかも知れない、そのような不安を持つことは実は大切なことです。ただ、不安をそのままにしていては意味がありません。本節では、パソコンやスマートフォンの利用にあたって、日頃から気を付けておくことでフィッシング対策につながる事柄についてまとめます。

### 4.5.1 ソフトウェアを最新の状態にする

パソコンやスマートフォンのようなモバイル端末にセキュリティ上の脆弱性があると、利用者が気付くことなく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ります。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やモバイル端末を利用することが重要です。

また、セキュリティのサポートがされなくなった古いパソコンの基本ソフト（OS）、新しい基本ソフト（OS）を使いましょう。また、スマートフォンも数年でサポート対象外となってしまうため、注意が必要です。

### 4.5.2 サービス事業者が提供するセキュリティ機能を積極的に利用する

サービス事業者は利用者の安全を目的にさまざまなセキュリティ機能を提供しています。オプションとして手続きが必要な機能もありますが、積極的にセキュリティ機能を利用するようにしましょう。サービス事業者が提供するセキュリティ機能例としては、以下のものがあります。

- ワンタイムパスワード
- アプリ生体認証
- メール認証、ＳＭＳ認証
- 利用状況メール通知
- ソフトウェアキーボード
- ウイルス対策ソフト
- フィッシングサイト検知ソフト

SMS 認証やワンタイムパスワード認証などの多要素認証を利用することが、攻撃者による不正ログインと「収益化」を阻止するために有効です。

ID とパスワード認証だけではフィッシング対策として十分とは言えないため、各 Web サービスで提供されているセキュリティ機能は積極的に利用するようにしましょう。

## 4.6 正規アプリをインストールする

不正アプリをインストールしないために、常日頃から以下の点を意識しておきましょう！。

- 偽物の警告である可能性を疑う
- 開発元・提供元を確認する
- 不必要な権限を要求されたらインストールしない

身の覚えのないメッセージが届いたり、突然画面に警告文が表示されたりしたら、心当たりがないか考えてみましょう。特に URL のクリックやアプリのダウンロードなどを促される場合は注意が必要です。また、アプリをインストールする前に、開発元や提供元を確認するように心掛けましょう。アイコンやアプリ名だけで判断すると、本物に似せて作られた不正アプリをインストールしてしまう可能性があります。開発元が本来の企業と違っていたり、不明になっていたりする場合はインストールしない方がよいでしょう。正規のアプリストア（iOS デバイスの場合は App Store 、Android の場合は Google Play など）以外からインストールできる設定にしている場合は、特に注意が必要です。アプリをインストールする際に、不必要な権限を要求されたら、そのアプリは不正アプリの可能性があります。不審に感じた場合、権限を許可しない、または別のアプリのインストールを検討しましょう。


図 4-12　不正アプリから不必要な権限を要求される例[10]

[10] 出典：SBI EVERSPIN　プレスリリース（2024/1/11）

正規のアプリストアは事業者によって不正アプリかのチェックがされていますが、そのチェックをすり抜けてしまうアプリも中にはあります。セキュリティベンダーから不正なアプリのブラックリスト11やホワイトリスト12を使ったアプリフィルターが提供されていますので、これらのサービスを使うことでより安全に安心してアプリを使うことも可能です。

正規アプリをかたった不正なアプリだけではなく、非公認アプリによる ID やパスワードが窃取される事件が発生しています。非公認アプリとはサービス事業者が提供するアプリよりも便利な機能を提供するなどにより、広く使われている場合もありますが、悪意のある第三者が作成した非公認アプリの中には、ID やパスワードを含む個人情報を盗むものがあることに注意してください。

不正アプリをインストールしてしまった場合や、身に覚えのないアプリがインストールしていた場合は、気づいた時点で即削除しましょう。もし、電話番号やメールアドレスなどが盗まれていて、不審な業者から連絡が来たとしても、対応しないように注意してください。「クレジットカードが不正利用された」などの被害が出た場合、警察に相談しましょう。

昨今、スマートフォンにおけるアプリは、さまざまな開発者から数多く提供され、利用者がアプリをインストールすることが日常的になっている状況に乗じて、攻撃者は不正アプリへ誘導しようとします。そのため、不用意にアプリを入手していると、思わぬ被害につながる恐れがあります。不正アプリによる被害を回避するためには、原則としてアプリは公式マーケットから入手し、アプリを選ぶ際は、開発元の信頼性やアプリの機能、利用規約等を慎重に確認することが必要です。また、不正アプリは OS やアプリの脆弱性を狙って攻撃を仕掛けてくる場合もありますので被害を防ぐために、OS やアプリのアップデート、セキュリティ対策ソフトの利用なども対策として有効です。

## 4.7 履歴を確認する

普段からクレジットカードやキャッシュレス決済の利用明細を確認しましょう。また、アカウントのログイン履歴などを確認することも、不正利用の痕跡を見つけるためには有効です。

[11] あらかじめ「危険な対象」を定義したリスト

[12] あらかじめ「安全な対象」を定義したリスト

## 4.8 間違って重要情報を入力してしまったら

自分がフィッシングサイトにアクセスしていることに気付かないまま、ID、パスワード、さらにクレジットカード番号など重要な情報を入力してしまっている可能性もあります。

フィッシング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、

- 正規サイトに重要情報を入力した際に不審な挙動がみられた（期待した手続き画面に進まなかったなど）
- 正規サイトに ID／パスワードを入力したがエラーとなってログインできなかった（フィッシング犯罪者にパスワードを変更されていた）
- クレジットカードの利用明細あるいは金融機関の通帳などに覚えのない取引が記載されていた（口座番号、暗証番号などが不正利用された）
- スマホのキャリア決済やキャッシュレス決済で身に覚えのない利用履歴があった（携帯電話番号、モバイル契約管理アカウント情報が詐取されていた）
- 要求した覚えのない認証コードを受信した（認証情報が不正利用された）

などのケースが考えられます。

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、すみやかに関係機関などに報告・相談を行ってください。

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、プロバイダーへ連絡を取り、当該アカウントの利用停止などの対応を依頼します。

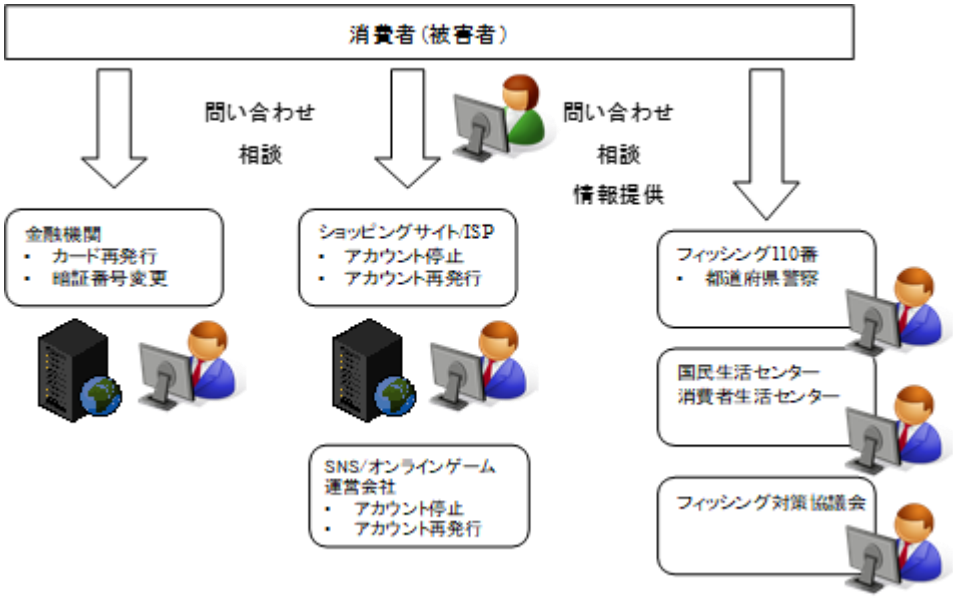


図 4-13　フィッシング被害に遭ってしまった時の問い合わせ、相談、情報提供

（1） サービス事業者（連絡）

盗まれた情報に応じて、サービスを提供している事業者に、フィッシング被害の疑いがあることを伝え、今後の対応について相談してください。例えば銀行、クレジットカード会社等への連絡は早く行ったほうが良いでしょう。また、入力してしまったパスワードは必ず変更し、メールアドレスも新しく作ったものに変更を行います。（漏えい情報の再利用を防ぐ）

（2） 警察への連絡（相談）

金銭的な被害など、実質的な被害が確認された場合には、居住する地区の都道府県警察サイバー犯罪相談窓口へ連絡してください。

| | |
|---|---|
| 都道府県警察本部のサイバー犯罪相談窓口一覧 | https://www.npa.go.jp/bureau/cyber/soudan.html |

（3） 国民生活センターまたは各地の消費生活センター（相談）

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

| | |
|---|---|
| 国民生活センター | https://www.kokusen.go.jp/ |
| 全国の消費生活センター | https://www.kokusen.go.jp/map/ |

（4） 法テラス（相談）

法テラス（日本司法支援センター）は国によって設立された法的トラブル解決のための総合案内を行っています。フィッシング被害に関して、法的トラブルに巻き込まれた場合には、法テラスへ相談してください。

| | |
|---|---|
| 法テラス | https://www.houterasu.or.jp/ |

（5） フィッシング対策協議会（情報提供）

同様の被害拡大を防ぐため、フィッシング対策協議会へ情報提供してください。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ッ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ます。

| | |
|---|---|
| フィッシング対策協議会 | https://www.antiphishing.jp/ |
| 電子メールアドレス | info@antiphishing.jp |
| Web フォーム | https://www.antiphishing.jp/registration.html |

※なりすまし EC サイト対策協議会

フィッシングではなく、なりすまし EC サイト（偽サイト）で被害を受けた場合には「なりすまし EC サイト対策協議会」に相談しましょう。

なりすまし EC サイト対策協議会

（https://www.saferinternet.or.jp/narisumashi/）

# 5. フィッシング対策協議会と本ガイドラインの位置づけ

フィッシング対策協議会は、2005 年 4 月に、フィッシングをはじめとするオンライン犯罪の増加を予見し、関係者が情報交換を行い、また被害状況に応じた対策を推進するという目的で発足いたしました。

協議会では、本ガイドライン以外に、インターネット利用者に向けた対策コンテンツを公開しております。本ガイドラインとあわせて対策を実践してください。

【緊急情報】

協議会に報告されたフィッシングメールやフィッシングサイトの実例を公開
https://www.antiphishing.jp/news/alert/

【月次報告書】

協議会に寄せられたフィッシング報告をもとに分析や調査を行い、毎月、フィッシングの傾向について情報を掲載
https://www.antiphishing.jp/report/monthly/

【マンガでわかる フィッシング詐欺対策 5 ヶ条】

https://www.antiphishing.jp/phishing-5articles.html