

フィッシング対策

○ フィッシングとは

フィッシングとは、実在のサービスや企業、官公庁等をかたり、偽の電子メールやSMS（ショート・メッセージ・サービス）を送付し、偽サイト（フィッシングサイト）に誘導した上で、IDやパスワード、クレジットカード番号等の情報を窃取したり、マルウェアに感染させたりする手口です。

情報を盗まれると、IDを乗っ取られて不正送金され（金銭を奪われ）たり、インターネット通信販売サイト等でクレジットカードを不正利用されたりします。また、マルウェアに感染してしまうと、スマートフォンに保存している電子メールや電話帳等の情報が盗まれたり、自分のスマートフォンがフィッシングSMSの発信源になってしまうこともあります。

<入力を求められる情報の例>

- ・ 金融機関の口座番号、クレジットカード番号、暗証番号（ワンタイムパスワード、乱数表の番号等）
- ・ 住所、氏名、電話番号、生年月日
- ・ 電子メール、インターネットバンキング、SNSアカウント等のID、パスワード等
- ・ 運転免許証、マイナンバーカード、乱数表等の画像情報

○ よくある相談

<相談事例1>

ネット口座を開設している銀行から「重要なお知らせ」という件名のメールが届いたので、記載されたURLにアクセスし、口座番号、暗証番号等を入力した。その後、知らない口座に対して、身に覚えのない多額の送金をされていることが分かった。

<相談事例2>

クレジットカード会社から「クレジットカード情報の確認」という件名のSMSが届いたので、記載されたURLにアクセスし、カード情報を入力した。後日、クレジットカードの支払い明細を見ると、身に覚えのない支払いがあった。

<相談事例3>

大手通販サイトから、「アカウントで不正なログインが確認されたため、アカウントをロックしました。解除するには下記のURLから手続きしてください。」というSMSが届き、慌ててURLに接続し、当該大手通販サイトのIDとパスワードを入力してしまった。

<相談事例 4 >

携帯電話に宅配業者から「お荷物のお届けにあがりましたが、不在でしたので持ち帰りました。」という不在通知（SMS）を受信したので、記載されていたURLにアクセスし、荷物追跡のアプリをインストールしてしまった。そうしたところ、知らない間に携帯電話に登録されている電話番号に、荷物追跡の内容のSMSが大量に送信されていることが判明した。

○ フィッシングの手口

フィッシングサイトに誘導する

携帯電話会社、宅配業者、金融機関をかたって電子メールやSMSを送信し、本物そっくりの偽サイト（フィッシングサイト）に誘導する事例が多数確認されているほか、検索サイトの広告から誘引する方法など、様々な誘導方法が確認されています。

電子メール等の文面は、「個人情報の漏えい」、「不正アクセス検知」、「取引の停止」等、切迫感を煽り、ログインさせようとするものが多数確認されています。

<電子メール等の文面例>

- ・ あなたのアカウントに不正アクセスがありました。至急以下のサイトからアクセスしてログインしてください。ログインしないとあなたのアカウントは安全のため失効します。
- ・ ○○に関する申告の参考となる情報について、メッセージボックスに格納しましたので、内容をご確認ください。
- ・ お客さまのアカウントは○○サービスを更新できませんでした。カードが期限切れになった可能性があります。

フィッシングサイトへの誘導手段や手口は日々変化しています。最新の手口については、[「フィッシング対策協議会～フィッシングに関するニュース」](#)を参考にしてください。

送信元情報を偽装する

電子メールは、仕様上、受信者から見える「送信元名称」や「送信元メールアドレス」を変更することが容易であるため、実在の企業等になりすますことができます。したがって、メールソフトに表示される「送信元名称」や「送信元メールアドレス」だけを見てメールの真偽を判断することは困難です。

また、スマートフォンのメールアプリで表示される「送信元名称」や「送信元メールアドレス」は、パソコンに比べて表示項目が少ない場合もあり、メールの真偽の判断はより一層困難となります。

※ 送信元情報の見え方の画像（省略）

○ **フィッシングの被害に遭ったら**
サービス提供会社に相談する（被害の補償等）

フィッシングによって、不正送金の被害に遭った場合は金融機関が、クレジットカードの不正利用の被害に遭った場合はクレジットカード会社が、それぞれ補償制度を設けていたり、トラブルに関する相談窓口を設けているところもあります。被害に遭ったサービスを提供している会社に相談してください。

【不正送金への対応】

一般社団法人全国銀行協会

[金融犯罪に遭った場合のご相談・連絡先](#)

パスワード等を変更する

フィッシングサイト等に普段から利用しているIDやパスワード等を入力してしまった場合は、そのIDやパスワード等を利用している全てのサービスにおいて、パスワード等を速やかに変更してください。

警察に通報・相談する

フィッシングメールを受信した場合は当該フィッシングメールのメールアドレス、内容、リンクのURL等を、フィッシングサイトを発見した場合は当該フィッシングサイトのURLを、[フィッシング110番](#)に通報してください。

また、フィッシングの被害に遭った場合は、保存した通信ログ等を持参して、[最寄りの警察署](#)又はサイバー犯罪相談窓口に通報・相談してください。

なお、事前に電話で担当者と日時や持参する資料の調整をしていただくと対応がスムーズに進みます。

- ・ フィッシングメールのメールアドレス
- ・ メールの文面
- ・ フィッシングサイトのURL 等

○ **被害防止対策**

電子メールやSMSに記載されているリンクはクリックしない

電子メールに記載されたリンクは偽装可能なほか、正規サイトに類似したドメイン名を付したフィッシングサイトも多く存在することから、見た目ではリンクの真偽を判断することは非常に困難です。

電子メールやSMS内のリンクを安易にクリックせず、あらかじめ公式サイトを「お気に入り」や「ブックマーク」に登録しておいたり、公式アプリを活用するなどして正しいサイトに接続するようにしてください。

なお、**金融機関が、ID、パスワード等をメールやSMSで問い合わせることはありません。**

パソコンやスマートフォンを安全に保つ

OSやアプリ、ソフトウェアのぜい弱性や不具合を悪用し、広告などからフィ

ッシングサイトに誘導される場合があるので、OSやアプリ、ソフトウェアのアップデートを行い、パソコンやスマートフォンを安全な状態に保ってください。

携帯電話会社などが提供するセキュリティ設定を活用する

携帯電話会社などが提供する迷惑メッセージブロック機能などを活用し、フィッシングメールや不審なSMSが届きづらい設定にしてください。

IDパスワードの使いまわしはしない

複数のサイトで同じID、パスワードを登録していると、一つでもID、パスワードを盗まれたら、銀行やSNS、インターネット通信販売サービスなど全てのサービスが乗っ取られる被害に遭ってしまいます。

ID、パスワードはサイトごとに違うものを登録するようにしてください。ID、パスワードを覚えられない場合には、パスワード管理アプリなどを活用してください。

ワンタイムパスワード等を活用する

銀行やインターネット通信販売サービスでは、パスワードに加え、メールやSMSに通知されるワンタイムパスワードを入力しなければログインすることができないサービス（ワンタイムパスワードサービス）が提供されています。

IDやパスワードが盗まれた時のため、ワンタイムパスワードサービスを活用してください。

指紋や顔認証などの認証方法を活用するとより安全です。

○ 事業者における対策

フィッシングサイトへは、企業の本物のメールアドレスになりすましたメールで誘導するケースも確認されています。

事業者にあっては、自社のドメインの悪用を防止する観点で『送信ドメイン認証技術』の導入をご検討ください。

主な『送信ドメイン認証技術』

- ・ SPF：メール送信元IPアドレスの妥当性を認証するもの
- ・ DKIM：電子署名を検証することで認証するもの
- ・ DMARC：SPFとDKIMを組み合わせたもの

特に、DMARCは、認証に失敗したメールの取扱いを送信側で指定でき、「なりすまされているメールは受け取らない」といった強いポリシーを受信側に実施させることができるようになります。

なお、DMARCは、メール送信側の事業者のみならず、メール受信サービスを提供する電気通信事業者における導入も必要ですので、電気通信事業者にあっても積極的な導入を検討してください。

※ DMARCの仕組みの概要（省略）

[DMARCを含めた送信ドメイン認証に関する技術的な導入マニュアルが、迷惑メール対策推進協議会から公表されています。](#)

○ 参考リンク

- 一般財団法人日本サイバー犯罪対策センター（JC3）
JC3では、産学官の協働と国際連携を通じてサイバー犯罪の実態を解明し、その脅威を軽減・無効化する取組を推進しています。
[一般財団法人日本サイバー犯罪対策センター（JC3）](#)
- フィッシング対策協議会
フィッシング対策協議会では、フィッシングに対する情報収集・提供、注意喚起等の活動を中心とした対策を促進しています。
[フィッシング対策協議会](#)
- 独立行政法人情報処理推進機構（IPA）
IPAでは、情報セキュリティの最新情報や具体的な対策情報・対策手段等、幅広いセキュリティ関連情報を提供しています。
[独立行政法人情報処理推進機構（IPA）](#)