1 ゼロトラストとは！

迷惑メールを受信しないようにどんなに注意をしていても、さまざまなきっかけでアドレスが迷惑メール送信者に渡ってしまう可能性があります。

迷惑メール対策を行っていたとしても、迷惑メール送信者は次々と手法を変えて送信してきます。

そして、最近の迷惑メール・SMSは、本物かニセモノかを見分けることが難しく、従来から言われていた“日本語やURLがおかしくないか”などを確認する方法だけでは、見極めに限界があります。

ですから、メールを受信したときは、たとえ、公式メールだと思っても、『最初は、決して信頼せず、きちんと確認する』ゼロトラストの考え方がとても大切になります。

では、具体的にはどうしたらよいのでしょうか。

【ゼロトラスト　3つの基本】

私たちゼロトラシスターズが、だまされないコツ
「ゼロトラスト　３つの基本」を紹介します。

・スマートフォンでは、送信者と件名に、数行の本文が表示されていますから、それ以上開くことはやめましょう。
・件名で「緊急」「重要」「セキュリティ」などを強調していれば、メールを開かない方が安全です。

・リンクをタップ（クリック）してしまうと不正な詐欺サイトへ誘導されてしまう危険があります。
・公式メールだと思ったとしても、タップ（クリック）しないで、確認は、公式サイトやブックマーク、アプリから事業者サイトにアクセスするようにしましょう。

・有名企業やブランドを装って偽サイトへ誘導し、ID・パスワードを入力させてだまし盗る「フィッシング詐欺」の例もあります。
・受信したメールでクレジットカード情報や、ＩＤ・パスワードなどの重要な個人情報の入力や確認を求められても、絶対に入力しないようにしましょう。

ゼロトラシスターズ　©2025　Japan Data Communiations Association.

被害にあわないための日頃の備えと対処法

インターネットやスマートフォンを利用する以上、どれだけ気をつけていても、迷惑メールや詐欺メールにだまされるリスクを完全に避けることはできません。

ゼロトラストの３つの基本を守りながら、併せてあらかじめの対策をしておくことも重要です。

【日頃からの３つの備え】

❶迷惑メールフィルターの利用

携帯電話事業者や多くのプロバイダでは、迷惑メールフィルターを無料で提供しています。サービスを利用して迷惑メールや詐欺メールを受信しないで済むようにしておきましょう。

→詳しくは27～30ページ

❷セキュリティソフトの利用

セキュリティソフト（アプリ）を利用すれば、うっかり、メールのリンクをタップ（クリック）してしまった場合でも、偽サイトなどへのアクセスや、不正ソフト（アプリ）のインストールリスクを抑えることができます。

→詳しくは31～32ページ

❸OSは常に最新に

迷惑メールの中には、OSやソフト（アプリ）の脆弱性（ぜいじゃく）を悪用してマルウェア（悪意のあるソフトウェア）を送り込もうとするものもあります。常に最新バージョンに保ち脆弱性を塞いでおくことが重要です。

【困ったときの対処法】

詐欺の手口は高度化しています。詐欺と気づかないうちにだまされてしまったり、後になって不安に思うこともあります。困ったときは一人で悩まず、関係機関に相談してください。

❶メールのURLを開いてしまった

メールを開くだけでは危険性は低いですが、リンクをタップ（クリック）してしまうと、アクセスしたことが送信者に伝わり、迷惑メールが増えたり、他の詐欺メールが届く可能性があります。

もし、覚えのない料金請求メールが届いても支払わず、消費生活センターなどへ相談しましょう。

❷個人情報を入力してしまった

クレジットカード番号やアカウントID、パスワードなどを入力してしまうと不正利用されるおそれがあります。すぐにカード会社や金融機関、ご利用サービスの相談窓口に連絡をして対応しましょう。

問い合わせは、メールのリンクではなく、ブックマークやアプリからアクセスするようにしましょう。

❸ウイルスに感染したかも

ウイルス感染が疑われるときは、まず、スマートフォンを機内モードにして、インターネットに接続しないようにしましょう。その後、セキュリティアプリで不審なアプリなどがインストールされていないか確認したり、最終手段としてスマートフォンを初期化するなどの対処法があります。

詳しくは、セキュリティの専門機関へ相談しましょう。

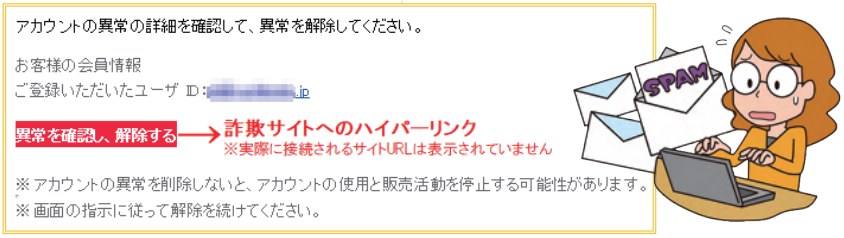
フィッシングのしくみ

くらしのオンライン化を狙い、有名企業やブランドを装って、フィッシング※1詐欺のメールやSMS(スミッシング※2)を送り、偽サイト(フィッシングサイト)へと誘導して、クレジットカード番号、アカウント情報(ユーザID、パスワードなど)といった個人情報をだましとる手口が急増しています。

私たちの不安心理などを利用して、ことば巧みに誘導していきます。フィッシングの一般的な流れを紹介しますので、あらかじめ手口を知って、だまされないように気をつけましょう。

※1　フィッシングはphishingという綴りで、魚釣り(fishing)と洗練(sophisticated)から作られた造語であると言われています。

※2　スミッシングは、スマートフォンなどのSMS(ショートメッセージサービス)を悪用したフィッシング詐欺で、“SMS” と “phishing” を組み合わせた造語です。



●フィッシングの流れ

①宅配便業者の不在通知や有名企業、ブランドになりすまして偽メールを送ります
②「重要」「緊急」「利用確認が必要」などと、受信者を不安にさせて、偽サイト（フィッシングサイト）へ誘導します。
③誘導された偽サイトは、本物そっくりに作られていて、クレジットカード番号、アカウント情報を入力させていきます。
④だました詐欺師たちは、入手した情報を不正利用して、金銭をだましとります。

フィッシングのしくみ

だましのテクニックとキーワード

●不審に思わせない手口

ネットショッピングなどの注文確認や宅配便業者の不在通知、金融機関やクレジットカード会社からの連絡を装う手法は、私たちが普段利用しているサービスに紛れ込んで、メールを受信した際に、不審に思わせないための手口です。

●不安にさせる手口

【重要】今すぐあなたのアカウントを確認してください
セキュリティ警告：お支払い方法の情報を更新するには、アクションが必要です
アカウントのセキュリティ通知
あなたのXXXXXXアカウントはセキュリティ上の理由でロックされています
XXXXXXアカウントを利用制限しています!
＜重要＞【XXXXX】異なる端末からのアクセスを確認のお知らせ

これらはすべてフィッシング詐欺メールによくある件名です。

- **重要**
- **警告**
- **アカウントロック**
- **セキュリティ**

など、いずれも受け取った人をパニックにさせ、冷静な判断力を失わせるような内容です。

いきなり、こんなメールを送りつけ、受け取った人をびっくりさせて、「えっ、どうしよう」「何とかしなきゃ！」と、とても不安な気持ちにさせる手口です。

●偽サイトへ誘導する手口

不安になって、メールを開いてしまったら、本文には

お客様のアカウントを維持するため会員個人情報を確認する必要があります。今アカウントを確認できます。 続けるには**こちら**をクリック
お客様のアカウントを維持するためアカウントの情報を確認する必要があります。下からアカウントにログインし、情報を更新してください。 ログイン
本人の確認をしてから、下記のURLで再開手続きの設定をしてください。 ※本メールは、セキュリティ強化のため、下記のURLで再開手続き https://www**********

などと、この“危機”への対応策が書かれています。受信者に「このリンクボタンやURLをタップ（クリック）すれば解決する。」と思わせるわけです。

まず、普段利用しているサービスのブランドで不審に思わせないようにし、次に「緊急」「セキュリティ」などの言葉で不安にさせ、最後に回避のための手続きを示して偽サイトに誘導していきます。これが二重三重に仕掛けられた「だましの手口」です。

このような手口があることをあらかじめ知って、いきなりのメールにあわてないことがとても大切です。