［2024年度版］

メールde詐欺 あなたのお金と情報が危ない

そのメール、詐欺サギカモ!?

最初はメール・SMSを信用しないゼロトラスト

迷惑メール相談センター

サギかもファミリー
迷惑メール詐欺被害防止啓発キャラクター

最初はメール・SMSを信用しない

ゼロトラスト3つの基本

最近の迷惑メールは、本物か偽物か見分けることが難しくなっています。フィッシング詐欺メール・SMSにだまされないために、メール受信した場合には、本物を含めて、すべてを『最初は決して信頼せず、きちんと確認する』**ゼロトラスト**の考え方を紹介します。

フィッシング詐欺とは：
①有名企業やサイトになりすましてメールやSMSを送り、②偽のサイトにアクセスさせて、③だまされた受信者から個人情報やパスワードなどを入力させて盗む詐欺の手口。

Point! だまされないための3つの基本

開かない

あやしいメール、身に覚えのないSMSは、最初から開かないほうが安全です。

リンクをタップしない

フィッシング詐欺メール・SMSは、偽サイトにつながるリンクが埋め込まれています。

入力しない

個人情報や銀行口座、カード番号の入力を求められたら、まず詐欺を疑いましょう。

Check! 被害にあわないための日頃の備え

迷惑メールフィルター

迷惑メール・SMSフィルターで、あらかじめ受信しない設定にしておきましょう。

セキュリティソフト

セキュリティソフトやアプリの利用で、詐欺サイトへのアクセスなどを抑えられます。

OSは常に最新に

ＯＳやアプリのアップデートは更新通知を見逃さず必ず最新にしておきましょう。

● より詳しく知りたいときの続きは、こちらをチェック！

迷惑メール相談センターでは、フィッシング詐欺メール・SMSの被害にあわないために、だまされないコツを紹介していますので参考にしてください。

撃退!詐欺メール＆SMS｜https://www.dekyo.or.jp/soudan/mb/index.html

メール de 詐欺とは

お金や情報をだましとる目的で送りつけられる迷惑メールです。

詐欺被害では、電話の「オレオレ詐欺」「振り込め詐欺」がとても有名ですが、実はメールやSMSを使った詐欺被害も数多くあります。最近の迷惑メールは、悪質化、巧妙化していて、気をつけないとお金や情報をだましとられる被害につながるケースが多くなっています。

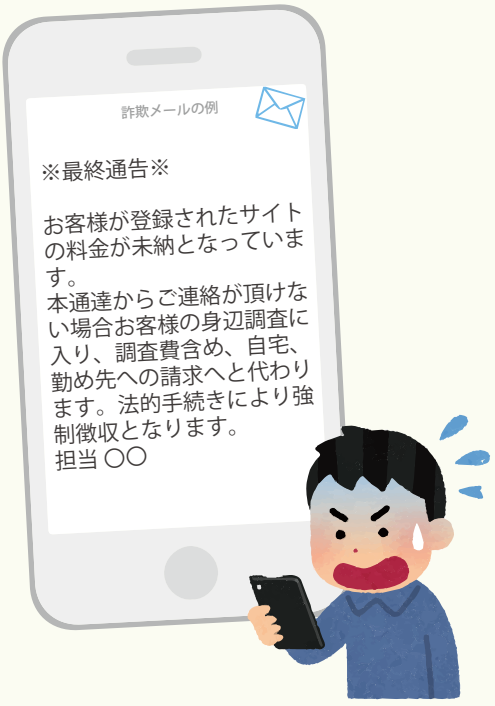
● より詳しく知りたいときは、こちらもチェック!

迷惑メール相談センターでは、様々な詐欺メールの実例を随時掲載していますので参考にしてください。右のQRコードからぜひご覧ください。

要注意メール一覧｜https://www.dekyo.or.jp/soudan/contents/news/alert.html

架空請求メール・SMS

● “架空(でたらめ)”の請求に支払いの必要はありません!



身に覚えのないサイトから登録料や情報料などの利用料金を請求されるのが「架空請求メール・SMS」です。

あわてて連絡をしてしまうと、何度も督促を受けたり、おどされる被害にあう可能性があります。

身に覚えがなければ、支払いの必要はありません。

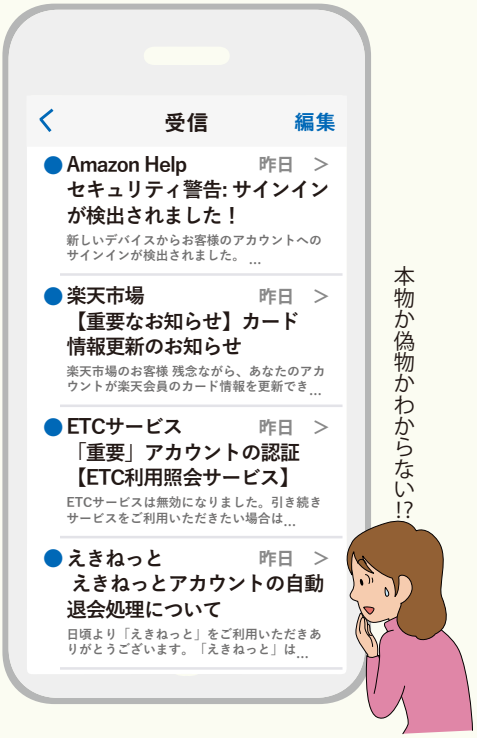
被害にあってしまったときは、すぐに最寄りの消費生活センターや警察にご相談ください。

⇒ 消費者ホットライン **188**(いやや!)(通話料有料)

※お住まいの地域の最寄の消費生活センターへ繋がります。接続先により受付時間が異なります。

⇒ 警察相談ダイヤル **#9110**(通話料有料)

有名通販企業をかたるメール・SMS



● Amazon・楽天などの有名通販企業をかたる詐欺が急増

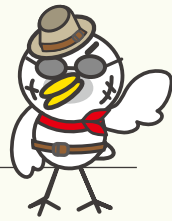
Amazonや楽天などの注文メールや発送、アカウントの確認などをかたるメール・SMSが急増しています。アカウントを停止・凍結するなどの不安をあおる内容で偽の詐欺サイトへアクセスさせ、ログイン情報をだましとるなどの手口です。

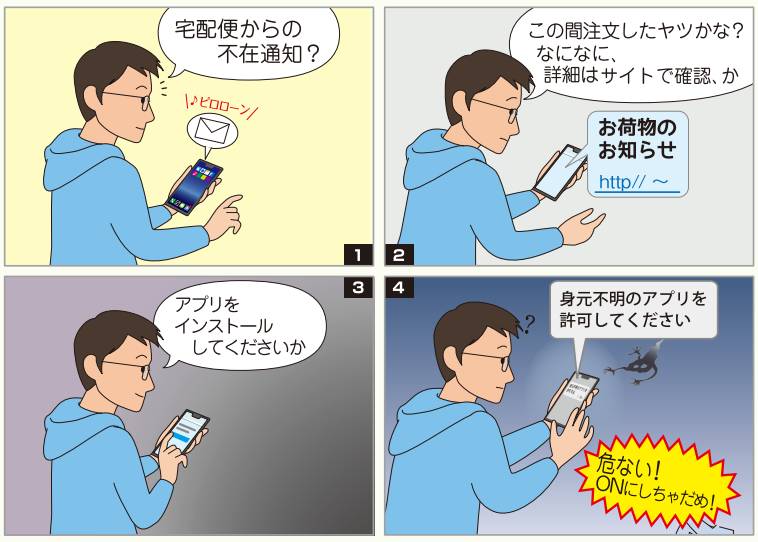
心当たりのないメール・SMSなら無視できても、普段利用している宅配便、ネットショッピング、携帯電話会社などからのメールで、思わず開けてしまうことを狙っています。アクセス先の偽の詐欺サイトも、本物そっくりに作られ、偽物を見分けるのが大変難しく、詐欺と気づかず被害にあう人が増えています。

サイトへのリンクを含むメール・SMSは、詐欺かもしれないと常に注意し、リンクを開いてアクセスするのはやめましょう。

公式からのお知らせが気になるときは、メール・SMSではなく、公式サイトやブックマーク、アプリから確認するようにしましょう。

宅配の不在通知を装うメール・SMS





● 荷物の配達を装う偽メール・SMSに注意

宅配便業者や郵便局になりすました詐欺のメール・SMSによる被害が多く報告されています。

荷物の不在通知や発送完了などのお知らせを装い、記載されたリンクを開かせて、Android向けの不正なアプリをインストールさせたり、個人情報を入力させようとするものです。

さらに、スマホを外部から操られたり、身に覚えのない携帯キャリア決済による請求が発生するなどの被害も報告されています。

アプリのインストールは、必ず公式サイト（Google Play、App Store）から行い、メール・SMSのリンクからアプリをインストールするのはやめましょう。

● スマホを安全に利用するために

スマホも、パソコンと同様にセキュリティ対策を行いましょう。
「OSの更新」「セキュリティアプリの導入」などの対策も重要です。

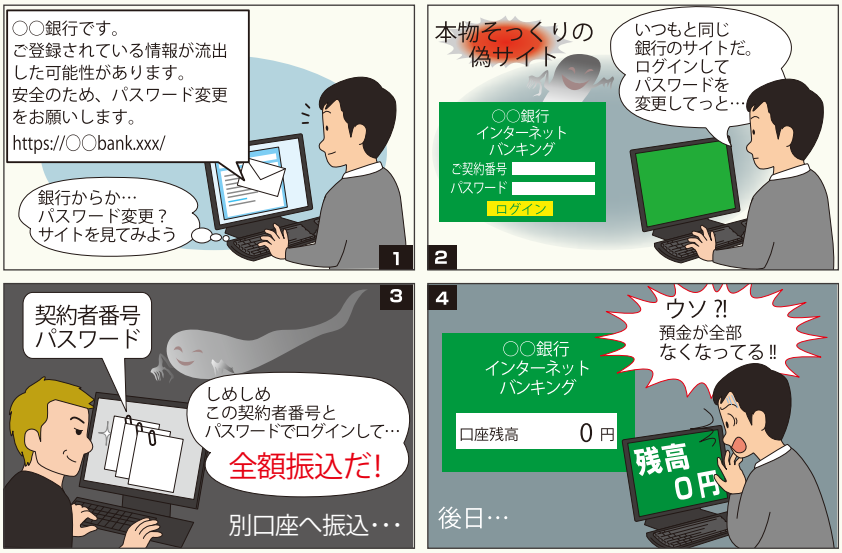
銀行やカード会社をかたるメール・SMS

● あなたのお金、狙われています

金融機関やカード会社になりすまして、個人情報をだましとるメール・SMSも数多く送られています。メール・SMSにだまされて銀行の口座番号やID、パスワードをとられてしまえば、犯罪者にあなたの口座の預金を引き出されてしまうことになります！

金融機関やクレジットカード会社ではIDやパスワード、暗証番号の入力を依頼するメール・SMSを送ることはありません。

詳しくはご利用の各社ホームページをご覧ください。



● 被害にあった時は

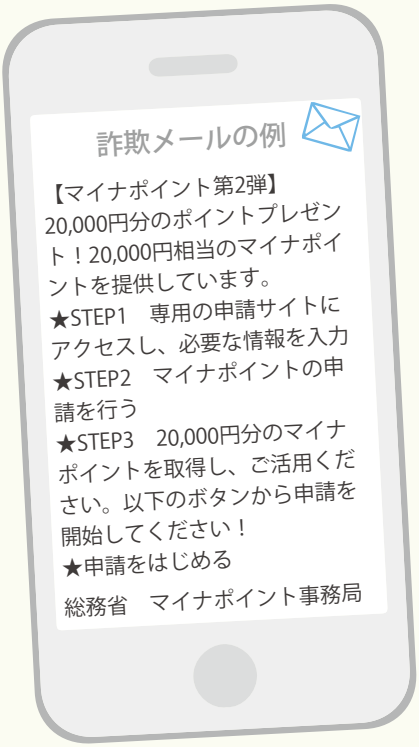
不審なメール・SMSを受け取ったときは、ご利用の銀行やクレジットカード会社等に相談してください。金銭被害が発生した場合は、最寄の警察へ相談してください。

⇒ 警察相談ダイヤル **#9110**（通話料有料）

マイナポイント事務局をかたるメール・SMS

● 詐欺のマイナポイントキャンペーンに要注意

総務省やマイナポイント事務局をかたり、本物そっくりの偽のメール・SMSから偽のホームページへアクセスさせて、お金をだましとる詐欺の手口です。ちょうど、本物のマイナポイントがもらえる第2弾キャンペーンが2023年9月に終了することから、これに乗じた詐欺メール・SMSが大量に送信されました。偽のページにアクセスすると、個人情報やクレジットカード番号を入力するように求められ、最終的に個人情報流出やクレジットカードの不正利用にも繋がります。**メール・SMSから誘導されて個人情報などを入力するのは避けて、ブックマークや検索から公式ページを確認したうえでアクセスするように**、気をつけましょう。



●トラブルにあわないために

詐欺メールは、還付金や給付金などお金をあげる内容と、税金の納付や差押えなどお金を払わせる内容などで、国や役所をかたり受信者をだまそうとします。お金に関わる不審なメールは無視し、不安なときは、下の連絡先へ相談してください。

⇒消費者ホットライン
188（通話料有料）
⇒警察相談ダイヤル
#9110（通話料有料）

迷惑メールでお困りの方は相談窓口へ

迷惑メール相談センター

03-5974-0068

10:00～12:00,13:00～17:00

（土日祝日・年末年始を除く）

https://www.dekyo.or.jp/soudan/

迷惑メール相談　検索

詐欺メール対策リーフレット

そのメール、詐欺カモ!?

2023年12月　第9版 第1刷　発行

一般財団法人 Japan Data Communications Association
日本データ通信協会
〒170-8585 東京都豊島区巣鴨 2-11-1 ホウライ巣鴨ビル 7F