[2025年改訂版]

メールde詐欺 あなたのお金と情報が危ない

そのメール、詐欺カモ!?

迷惑メール相談センター

最初はメール・SMSを信用しないゼロトラスト

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

©2015-2025 Japan Data Communications Association All Rights Reserved.

メール・SMS de 詐欺とは

お金や個人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。

「オレオレ詐欺」や「振り込め詐欺」などの電話を使った詐欺はよく知られていますが、実は**メールやSMSを使った詐欺被害も急増**しています。最近の迷惑メール・SMSは、手口が巧妙かつ悪質になっており、油断すると金銭や個人情報をだまし取られる危険性があります。

こうした詐欺から身を守るためには、表面に記載されている**「ゼロトラスト」**の考え方が重要です。これは、**たとえ本物に見えるメールやSMSであっても、最初から信用せず、必ず内容を確認する**という姿勢です。

近年では、海外から日本人をターゲットにAIを使って作成された詐欺メールも増えています。日本語が自然で見分けがつきにくいケースも多く、**どんなメールでもリンクはクリックしないことが、最も安全な対策です。**

■安全のために

公式アプリの利用：銀行・宅配業者・通販サイトなどは、必ず公式アプリを使うこと。

セキュリティソフトの導入：スマホにもウイルス対策アプリを入れておくと安心です。

■被害にあってしまったときは、すぐに家族や関係機関にご相談ください。

消費者ホットライン 188(いやや!) ｜ **警察相談ダイヤル #9110**

※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。(通話料有料)

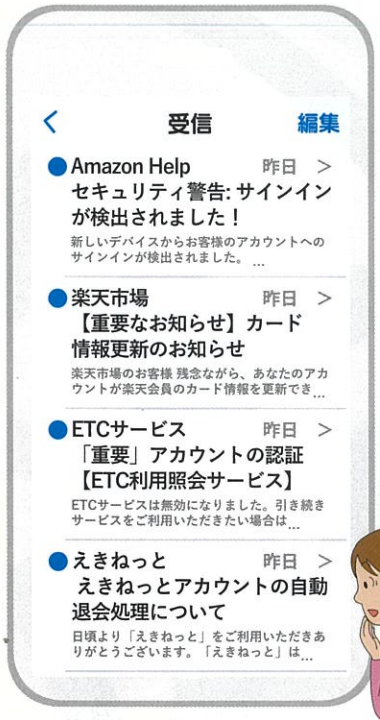
※発信地を管轄する各都道府県警察本部等の窓口に繋がります。(通話料有料)

● 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

有名企業をかたるメール・SMS



ネット通販などを装った偽のメールやSMSに注意

- 偽の高額な商品の注文・発送などで気を引く
- アカウント停止などの不安をあおり、偽サイトに誘導
- 本物そっくりのサイトでログイン情報をぬすみとる手口
- 普段使っているサービスを装うため、つい信じてしまいがち

リンク付きのメールやSMSは、詐欺の可能性を常に疑いましょう。内容の真偽が気になるときは、メールやSMSのリンクは開かず、公式アプリやブックマークから確認するのが安全です。

宅配業者をかたるメール・SMS

荷物の配達を装う偽メール・SMSに注意

- 「不在通知」や「発送完了」などを装ってリンクを開かせ、個人情報を入力させる
- Android端末に正規アプリを装って、不正アプリをインストールさせる
- スマホが遠隔操作されたり、身に覚えのない請求が発生するケースも

荷物の宅配を装う詐欺メールやSMSは特に多いため、決してメールやSMSのリンクは開かず、公式アプリやブックマークからサイトを利用するようにしましょう。

金融機関をかたるメール・SMS

偽の銀行・証券会社・カード会社をかたる詐欺メールやSMSに要注意

- 証券会社を装ったメールをきっかけに口座が不正アクセスされ、株が勝手に売却される詐欺被害が発生。
- メールやSMSから偽HPに誘導し、口座番号やID・パスワードなどを詐取。

金融機関がメールやSMSで、IDやパスワード、暗証番号の入力を求めることはありません。　リンク(URL)はクリックしないようにしましょう。

● 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）

警察官をかたるメール・SMS

日本全国で警察官をかたる詐欺が多発中

主な手口・特徴

- 「あなたの口座が犯罪に使われている」
- 「あなたの携帯電話から多数の迷惑メールが送られている」
- 「資産を保護するために口座を調査する必要がある」
- 「逮捕される可能性がある」などと不安をあおる

警察がメールやSMSで個人情報や資産の提供を求めることはありません。警察が突然ビデオ通話をしてくることもありません。警察官を名乗る不審な連絡があったら、相手の指示には従わず、最寄りの警察署か #9110 に相談しましょう。

詐欺メールの例

【重要】警察庁
あなたはギャング活動に関与しています。以下の口座に500万を振り込んでください。
2025年＊月＊日までに送金しない場合はあなたを逮捕します
○○銀行○○支店
受取人名：○○
口座番号:○○○○
警察庁 〒*****東京都

©2025 Japan Data Communications Association

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・SMSは、本物か偽物か見分けることが難しくなっています。フィッシング詐欺にだまされないために、メール・SMSを受信した場合には、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。

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

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!?
2025年11月　第11版　第6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

※本資料は、著作権法の例外を除き、無断で複写・複製することは禁じられています。
©2025 Japan Data Communications Association