

[2026年度版]

そのメール、 詐欺かも!?

フィッシング詐欺にだまされないために
ゼロトラスト3つの基本

実際にあった詐欺の事例を掲載

有名企業をかたるメール・SMS

金融機関をかたるメール・SMS

社長・代表をかたるメール・SMS

警察官をかたるメール・SMS

最初は
メール・SMSを
信用しない
ゼロトラスト

めいわく そうだん
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 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法。

Point!

だまされないための3つの基本

ひら 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。

にゅうりよく 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

めいわく 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・SMS de 詐欺とは



お金や個人情報^{かね こじん じょうほう}をだまし^{もくてき}とする目的^{おく}で送りつけられる迷惑メール^{めいわく}です。

「オレオレ詐欺^{さぎ}」や「振り込め詐欺^{ふ こ さぎ}」などの電話^{でんわ}を使った詐欺^{さぎ}はよく知られていますが、実はメールやSMSを使った詐欺^{さぎ}被害^{ひがい}も急増^{きゅうぞう}しています。最近^{さいきん}の迷惑メール・SMSは、手口^{てぐち}が巧妙^{こうみょう}かつ悪質^{あくしつ}になっており、油断^{ゆだん}すると金銭^{きんせん}や個人情報^{こじん じょうほう}をだまし取^とられる危険性^{きけんせい}があります。



こうした詐欺^{さぎ}から身^みを守るためには、表面^{おもてめん}に記載^{きざい}されている「ゼロトラスト」の考え^{きょうえ}方が重要^{じゅうよう}です。これは、たとえ本物^{ほんもの}に見えるメールやSMSであっても、最初^{さいしょ}から信用^{しんよう}せず、必ず内容^{かなら}を確認^{ないよう かくにん}するという姿勢^{しせい}です。

近年^{きんねん}では、海外^{かいがい}から日本人^{にっぽんじん}をターゲットにAIを使って作成^{さくせい}された詐欺メール^{さぎ}も増^ふえています。日本語^{にほんご}が自然^{しぜん}で見分け^{みわけ}がつきにくいケースも多^{おほ}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^{もっと あんぜん}な対策^{たいさく}です。

■安全のために

公式アプリ^{こうしき}の利用^{りよう}：銀行^{ぎんこう}・宅配業者^{たくはいぎょうしゃ}・通販サイト^{つうはん}などは、必ず公式アプリ^{かなら こうしき}を使うこと。

セキュリティソフトの導入^{どうにゅう}：スマホにもウイルス対策アプリ^{たいさく}を入れておくことと安心^{あんしん}です。

■被害^{ひがい}にあってしまったときは、すぐ^{かぞく}に家族^{かんけい}や関係機関^{きかん}にご相談^{そうだん}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^{じつれい}を随時掲載^{ずいじ けいさい}していますので参考^{さんこう}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。



本物が偽物かわからない!?

社長・代表をかたるメール・SMS



ニセ社長からのメール・SMSに注意

主な手口・特徴

- 自社や団体の代表者名を装う
- LINEグループの作成、QRコードで招待させる
- 経理担当の責任者を参加させる
- 会社の銀行口座の残高などを尋ねる
- 具体的な送金口座を示し、送金を指示
- 何度もリマインドを送り、不安をあおる



普段から詐欺メールへの対応を社内で共有・周知しましょう。緊急の送金指示には特に注意し、SNSのやりとりではなく、既知の電話番号などで直接確認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

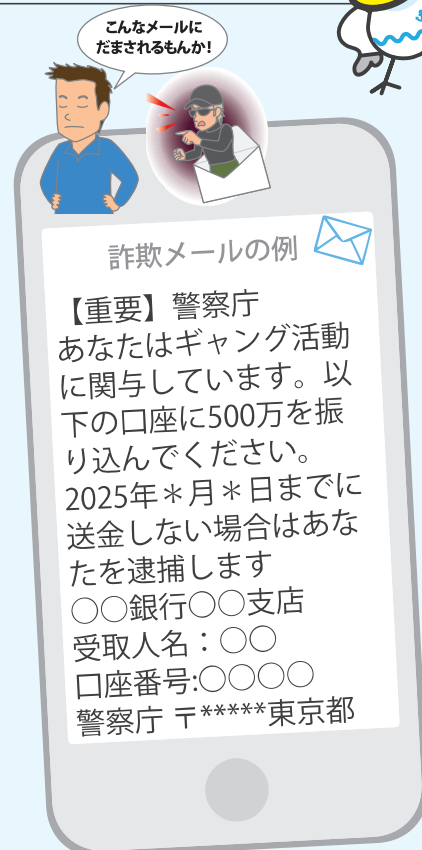


日本全国で警察官をかたる詐欺が多発中

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で個人情報や金銭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。



めいわく
迷惑メールでお困りの方は相談窓口へ
めいわく
迷惑メール相談センター
そうたん
そうたんまどぐち

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

けんさく
検索



さき
詐欺メール対策リーフレット
そのメールは詐欺かも!?

2026年 6月 第12版 第1刷 発行

デ協 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。

©2026 Japan Data Communications Association