

★撃退! 迷惑メール

だまされないコツ📢 教えます

🔒 ゼロトラスト



最新! 迷惑メール対策情報 BIMI (ビミ) で見分ける!

電気料金などの請求をかたる偽メールに注意
ドコモ・au・ソフトバンク・楽天の迷惑SMS対策

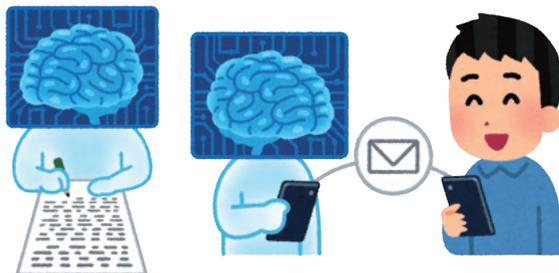
はじめに

近年、迷惑メールは、スマートフォンの普及にともない大きな質的变化を遂げています。

そして、コロナ禍を経て、リモートワークやオンライン教育の導入などにより私たちの生活のオンライン化は、ますます加速しています。

オンライン化を狙ったフィッシング詐欺による情報の窃取や金銭被害など、迷惑メールをきっかけとしたさまざまな詐欺被害も目立ちます。迷惑メールはインターネット犯罪を試みる者たちの重要なツールになっていると考えなければなりません。

従来は、文章が不自然だったり、ワンパターンな内容だったりしましたが、最近では、あらゆるデータを学習し、簡単に色々なパターンが作成できる生成AIの登場により、様々な企業をかたり、受け取り手の関心を引きやすい内容にカスタマイズされた、本物と区別のつかない詐欺メールや詐欺SMSが届くようになりました。そのため、誰でもだまされる危険にさらされているといえるわけです。



皆さんは、「ゼロトラスト」という考え方をご存知でしょうか。セキュリティ分野の考え方で「最初は決して信頼せずにきちんと確認を行う」とする考え方です。

本物か二セモノか見分けることが困難な詐欺メールがあふれているとすると、“メールのあやしい点に気づいてだまされないようにする”という発想では、対応が難しいといえます。

ですから、私たちは受信メールに対するこれからの姿勢をゼロトラストという考え方へと転換する必要があります。

インターネットやスマートフォンはとても便利ですが、便利さにはリスクを伴います。インターネット時代のあふれる情報に振り回されず、安全に利用できるように、あらかじめそのリスクを小さくしておくことが大切です。

この冊子では、メールを受け取った時の対応の基本、スマートフォンを安全に使うための設定、トラブルを避けるための工夫などを紹介しています。これらをよく理解し、あらかじめ対策し、ICTリテラシーを養って安全で楽しくインターネットを利用しましょう。



INDEX

特集 最新! 迷惑メール対策情報 BIMi(ビミ) 1

- (1) BIMi(ビミ) で見分ける! 公式メールはロゴをチェック 1
- (2) BIMiに対応したメールアプリで見てみよう 2
- (3) BIMiに対応した企業の一例 2

★1 だまされないコツゼロトラスト 3

- 1 ゼロトラストとは! 3
- 2 被害にあわないための日頃の備えと対処法 5
- 3 フィッシングのしくみ 7
- 4 だましのテクニックとキーワード 9

★2 迷惑メール・詐欺メールの手口を知る 11

- 1 フィッシング詐欺SMS 11
- 2 大手ECサイトになりすました偽メール 13
- 3 宅配便業者になりすました偽メール・SMS 15
- 4 金融機関やクレジットカード会社になりすました偽メール 17
- 5 電気料金などの請求をかたる偽メール 19
- 6 利用した覚えのない架空請求メール 21
- 7 ビットコインを要求するセクストーション(性的脅迫)メール 23
- 8 友人・知人から届くチェーンメール 25

★3 被害にあわないためのセキュリティ対策 27

- 1 迷惑メール対策 27
- 2 迷惑SMS対策 29
- 3 セキュリティ対策 31
- 4 有害サイト・有害アプリ対策 33
- コラム** 子どもの安全なスマートフォン利用のために 35
- 5 迷惑メールは法律違反 37

6 情報提供のお願い 39

★4 STOP!ネットトラブル 41

1 ネット社会の危険 41
 2 情報発信は慎重に行いましょう 43
 3 意図しない情報の流出を防ぎましょう 45
コラム SNSアカウントが乗っ取られる被害が増えています！ 47
 4 緊急時の情報発信 49

ネット・メールトラブル防止 理解度チェック 51

問題 51
 正解と解説 53

ご案内 55

1 トラブル別相談窓口 55
 2 迷惑メール相談センターのご案内 57

最新! 迷惑メール対策情報 BIMI (ビミ)

大量に届く迷惑メールにより、受信トレイは本物か偽物かわからないメールであふれかえっていませんか? どんなにフィルターを設定してもすり抜ける迷惑メールが原因で、大切なメールを見逃してしまったり、詐欺メールを開いてしまったり、お困りの方も多いと思います。そこで、最近メールサービスで導入が進んでいるBIMI(ビミ)の便利な機能を紹介します。



(1) BIMI(ビミ)で見分ける! 公式メールはロゴをチェック

BIMI (Brand Indicators for Message Identification) は、メールのなりすまし対策の一つで、正規のメールと認証されたメールに送信側の企業のロゴアイコンが表示されます。

例えば、auからのメールを受信したときに、メールアプリの受信一覧にauのロゴが表示されることで、ひと目で公式のauからのメールと判断することができます。もしauをかたった詐欺メールだった場合はauのロゴは表示されません。

このBIMIの機能を知っていれば、企業や銀行、クレジットカード会社などをかたった詐欺メールを受け取ったとしても、ロゴが表示されているかどうかを確認すれば、正規のメールかを一目で見分けることができます。



Android auメールアプリ



iPhone/iPadメールアプリ

<メールアプリでのau/KDDIロゴ表示イメージ>

※出典: auメール、なりすましメールの抑止と送信元のアイコン表示でフィッシング詐欺への対策強化 (au) <https://www.au.com/information/topic/mobile/2023-024/>

(2) BIMIIに対応したメールアプリで見てみよう

それでは、実際にBIMIIに対応したメールアプリの例を紹介します。下の画像は同じメールを、違うアプリで表示したときのものです。左の画像はBIMIIに非対応のメールアプリで見た場合で、右の画像はBIMIIに対応した「Yahoo!メール」アプリで同じメールを見た場合です。ロゴがあるだけで見やすさがずいぶん変わります。



BIMIIに対応したGmailアプリや「Yahoo!メール」アプリでは複数のメールアドレスを設定することができるので、もし現在利用しているメールアプリがBIMIIに対応していないときはメール受信アプリを変更することもおすすめです。

参考：Gmail アプリにメール アカウントを追加する (Gmail)
<https://support.google.com/mail/answer/6078445>
 「Yahoo!メール」アプリについて (Yahoo! JAPAN)
<https://support.yahoo-net.jp/SaaMail/s/article/H000012116>

(3) BIMIIに対応した企業の一例

BIMIIに対応したメールを利用するためには、送信側と受信側企業両方での対応が必要なため、導入はまだ一部の企業に限られています。現状BIMIIに対応したメールよりも、対応していないメールの方が多いため、右のメール受信画面の例のように、①BIMII対応メール、②BIMII非対応メール、③詐欺メールが一覧に表示され、まだまだ必要なメールを見分けにくい印象があります。

そのため、間違って詐欺メールを開いてしまう可能性もありますので、メールを確認するときは、次のページで紹介する「ゼロトラスト」の心構えがあると安心です。なお、BIMIIに対応した企業ブランドの一覧は以下のページで紹介されていますのでご参考ください。

参考：BIMII対応組織リスト (ナリタイ)https://www.narital.jp/enterprise_bimii.html



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。

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】



①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



②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



③OS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。



①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。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。



②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へ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。



③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。

アカウントの異常の詳細を確認して、異常を解除してください。

お客様の会員情報

ご登録いただいたユーザ ID: [REDACTED].jp

異常を確認し、解除する → **詐欺サイトへのハイパーリンク**
※実際に接続されるサイトURLは表示されていません

※ アカウントの異常を削除しないと、アカウントの使用と販売活動を停止する可能性があります。

※ 画面の指示に従って解除を続けてください。



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> **【XXXXXX】** 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。

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。



フィッシング詐欺SMS

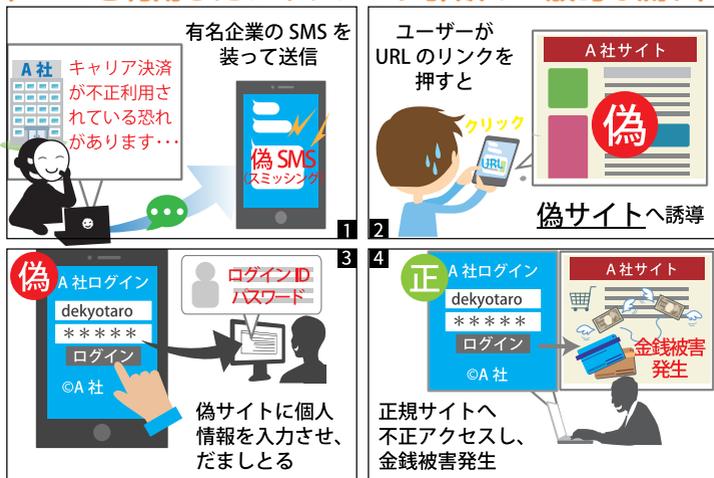
最近、本人確認の2段階認証や企業・自治体からの情報配信用としてなど、さまざまなシーンでSMSが利用されるようになりました。

SMSは電話番号を利用してメッセージをやりとりするサービスで、一般的に受信者がメッセージに気づきやすく、開封率が高いといわれています。便利になった反面、こうしたSMSの特徴を悪用した詐欺が最近急増しているため注意が必要です。

有名企業・ブランドになりすます

SMSを利用したフィッシング詐欺の事例が急増しています。よくある手口としては、宅配便業者、携帯電話事業者、通販会社などの有名企業になりすましてSMSを送るものです。このSMSにより、偽サイトへ誘導した上で、ID・パスワードなどの個人情報盗み取り、最終的に金銭をだまし取るものです。

<SMSを利用したフィッシング詐欺の一般的な流れ>



●新しい手口にも注意が必要です

スマートフォンの中にはアプリのログイン情報、ショッピングサイトやオンラインバンクのアカウント情報など、重要な情報が大量に保存されています。

そして、こうした情報は悪意のある攻撃者にとっての格好のターゲットとなっています。

ID・パスワードなどの個人情報を盗み取る手口だけではなく、不正なアプリをインストールさせ、そのスマートフォンから同じ内容のSMSを他の宛先に多数送信させる悪質な手口も報告されています。

不審なSMSにも十分注意するようにしましょう。



迷惑メール・詐欺メールの手口を知る

もしフィッシング詐欺SMSにだまされて入力してしまったら

●アカウントID／パスワード、名前や住所を入力してしまった

すぐにアカウントID／パスワードを変更し、サイトへ登録した住所、連絡先メールアドレスなどが変更されていないか確認しましょう。身に覚えのないログイン通知が届いたときは特に注意しましょう。

●クレジットカード番号や口座番号を入力してしまった

すぐにクレジットカード発行会社や金融機関に連絡しましょう。

●身に覚えのないセキュリティコードのSMSが届いた

実際に不正アクセスが行われている可能性もあります。

公式アプリやブックマークなどでログイン履歴などを速やかに確認し、不正アクセスの事実があった場合には、ID／パスワードを変更してください。

●身に覚えのない料金請求が届いた

公式アプリや公式サイトからサービスを提供している会社へ連絡し、請求内容を確認しましょう。確認はSMSやメールのリンクから行うのはやめましょう。





迷惑メール・

詐欺メールの手口を知る

2

大手ECサイトになりすました偽メール

●本物そっくりの詐欺メール・フィッシングサイトに要注意

スマートフォンのアプリやブラウザから気軽にオンラインで買い物をする機会が増えています。

普段からお知らせや購入確認などのメールを受け取る機会が多いため、送信者は、受信者が思わずメールを開封してしまうことを狙っています。

メールの件名や本文には「アカウントを凍結する」「不正利用されている」などと、緊急性の高い言葉を記載してあわてさせ、本物そっくりのフィッシングサイトへ誘導する巧みな手口です。

「すぐに対応しなければいけない」と指示されたフィッシングサイトで、アカウント情報などを入力してしまうと、クレジットカードの不正利用や、サイトでの不正購入などの被害にあうおそれがあります。

決してメールのリンクをタップ（クリック）したり、個人情報を入力したりしないようにしましょう。

実在の企業と無関係に送信された偽メールの例



ポイント

- ✓ 大手ECサイトでは顧客へ未納料金を督促するSMSを送信することはありません。また、登録のアカウント情報の開示をメールやSMSで求めることもありません。
- ✓ もし、アカウント情報を入力してしまった場合は、すぐにカスタマーサービスに連絡してください。購入履歴の確認、キャンセルや、パスワードの変更などの措置が必要です。

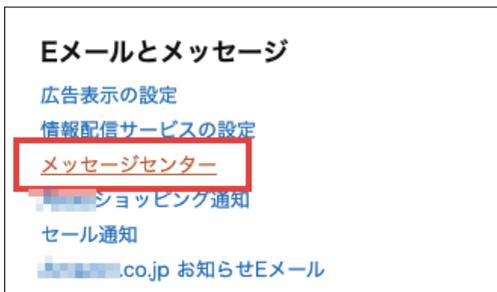
本物のメッセージかを確認するには？（Amazonの場合）

本物のお知らせかどうか迷ったときは、「メッセージセンター」を確認しましょう。

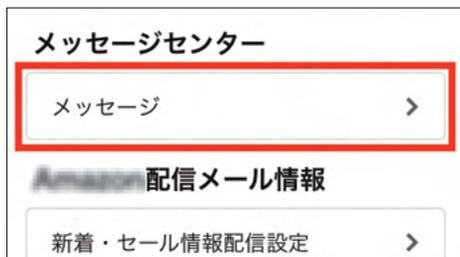
確認するときは受信したメールのリンクからではなく、「検索」や「アプリ」からログインし、「アカウントサービス」→「メッセージセンター」を開くとメールで送られたすべての内容を確認することができます。

ログイン>アカウントサービス>メッセージセンター>メッセージ>すべてのメッセージ

パソコンでの表示



アプリの表示





宅配便業者になりすました 偽メール・SMS

郵便局や佐川急便、ヤマト運輸などの宅配便業者になりすました偽メール・SMSによる詐欺被害が継続して報告されています。

この手口は、荷物の不在通知や発送完了などのお知らせを装い、偽メール・SMSに記載されたURLから、偽サイトへ誘導して、Android向けの不正アプリをインストールさせたり、iPhone端末では「Apple ID」や「パスワード」をだましとろうとするものです*。

また、被害にあったスマートフォンのアカウントが不正利用され、身に覚えのない携帯電話事業者の提供するキャリア決済の請求が発生したり、Google Playアカウント、端末に紐づくSNSなどのサービスのアカウントへの不正ログインも報告されています。



※(独)情報処理推進機構 (IPA) 2021年12月22日掲載 宅配便業者に加えて通信事業者をかたる偽ショートメッセージサービス(SMS)が増加中～偽SMSから不正アプリのインストールやフィッシングの被害にあう手口に引き続き注意!～



メール・SMSの特徴

- ・SMSで届くことが多い
- ・荷物の不在通知や発送完了メールなどを装う
- ・アプリのインストールを要求する（Android端末）
- ・「Apple ID」と「パスワード」の入力を要求する（iOS端末）

対処法

- ✓身に覚えのない不在通知やお知らせのSMSは無視をしましょう。
- ✓本文内のURLは絶対にタップ（クリック）しないようにしましょう。サイトを表示してしまったときは、ブラウザを閉じて、アカウント情報などの入力はしないようにしましょう。
- ✓公式サイト以外からアプリをインストールするのはやめましょう。Android端末は「Google Play」、iOS端末は「App Store」からのみ、アプリをダウンロードするようにしましょう。
- ✓間違っても不審なアプリをインストールしないように、Android端末は「提供元不明のアプリ」のインストールを許可（ON）しないように設定しておきましょう。



迷惑メール・詐欺
メールの手口を知る

相談窓口：

■ 消費者ホットライン188

電話番号：（局番なし）188（通話料有料）
お近くの消費生活相談窓口等につながります。
※接続先により受付時間が異なります。
※一部のIP電話などからはつながりません。



消費者庁
消費者ホットライン
188キャラクター
イヤホン

■ 情報セキュリティ安心相談窓口

【IPA（独立行政法人 情報処理推進機構）】

電話番号：03-5978-7509
受付時間：平日10：00～12：00、13：30～17：00
（年末年始・祝祭日は除く）

■ 各携帯電話事業者（詳しくは56ページ）

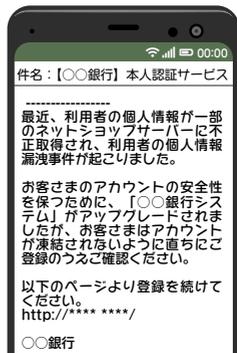
金融機関やクレジットカード会社 になりすました偽メール

● あなたの預金やクレジットカード番号が狙われています

金融機関になりすまし、ネットバンキングやクレジットカード利用者へのお知らせメールを装ったフィッシング詐欺の事例もあります。

「安全性向上のためにパスワードを変更してください」「カードの利用確認」などと緊急性を強調して、本物そっくりの偽サイトへ誘導し、利用者のアカウント情報（口座番号、契約者番号、クレジットカード番号、暗証番号など）を入力させてたましとろうとする手口です。

犯罪者に、この方法でたましとったアカウント情報を使われて、正規のサイトにログインされ、銀行口座からの不正送金や不正なクレジットカード利用をされてしまうなどの被害が報告されています。



メールの特徴

- ・「不正に利用される懸念がある」「漏洩した名簿にあなたが含まれている」「セキュリティ強化に必要」「カードの利用確認」などと緊急を装う内容

対処法

- ✓ 金融機関やクレジットカード会社がメールで個人情報を求めることはありません。メールに記載されたリンクをタップ（クリック）したり、メールの問い合わせ先へ連絡したりするのはやめましょう。
- ✓ 偽サイトは本物そっくりに作成しているため、本物と見分けるのは困難です。本物かどうか確認する必要がある場合には、普段使用しているブックマークやアプリからアクセスするか、公式サイトから連絡するようにしましょう。
- ✓ フィッシング詐欺の被害にあった時は、速やかにご利用の金融機関やクレジットカード会社の窓口へ連絡してください。また、金銭被害にあった場合には、最寄りの警察署へ相談してください。
- ✓ 偽サイト対策には、「100%安心」といった対策を示すことは困難ですが、セキュリティ対策ソフトを最新の状態にアップデートして、「提供元不明のアプリ」のインストールを許可しないといった設定も有効です。



迷惑メール・詐欺
メールの手口を知る

相談窓口

警察相談ダイヤル

電話番号：#9110（通話料有料）

受付時間：平日8：30～17：15（各都道府県警察本部で異なります）
（土日・祝日及び時間外は、一部の県警を除き、当直または音声案内での対応となります）

もっと
知りたい

フィッシング対策協議会ではフィッシングに関する緊急情報やフィッシング事例の紹介を行っています。

フィッシング対策協議会

<https://www.antiphishing.jp/>





迷惑メール・

詐欺メールの手口を知る

5

電気料金などの請求をかたる 偽メール

架空の電気・ガス・水道などの料金請求に要注意

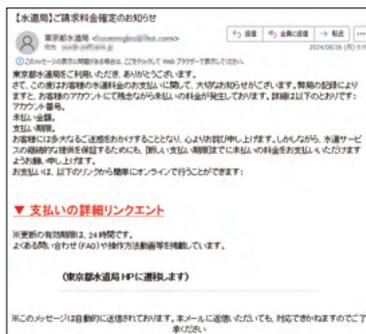
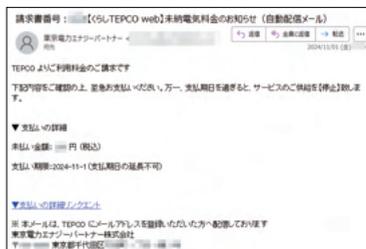
電気やガス、水道料金の未払いの請求など、誰もが生活する上で利用している会社を装った偽メール・偽SMSが多く送られています。

カードの引き落としが失敗した、支払いが確認できないなどの言葉で気を引き、期日までに支払いがないと電気が止まるなどと不安にさせて、本物そっくりのホームページへ誘導し、個人情報をだましとろうとします。

こうしたインフラ会社がかたられるのは、サービスが止まると日常生活に支障をきたすのが明白であることから、受信者の関心や反応を得られやすい点にあります。

真偽がわからない場合は、慌ててリンクからサイトにアクセスしないようにしましょう。

もし不審なメールを受け取ったときは、メールのリンクではなく、企業の公式サイト・アプリや普段の請求書などから連絡先を確認するようにしましょう。



メールの特徴

- ✓ 正規のロゴやイラストが入っている本物そっくりのメールが送信されています。
- ✓ 偽メールから誘導された詐欺サイトでは、未払い料金の支払いとして電話番号やクレジットカード情報の入力を求められます。
- ✓ 料金の支払いは電子マネーのみ可能として、コンビニで電子マネーを購入させて、コード番号の入力を求める場合もあります。
- ✓ 3日以内に支払いがないと送電を停止するなど受信者を脅します。

対処法

- ✓ 不審な料金請求やサイトに誘導するメールは無視しましょう。
- ✓ 一般的に、電気やガス、水道会社から、支払期日を過ぎるとただちに供給を停止すると記載したメールや、ただちにこのリンクから支払うようにと記載したメールを送ることはありません。
- ✓ 個人情報やクレジットカード番号を入力してしまった場合は、すぐにご利用中のサービス、カード会社へ連絡し、トラブルが心配なときは最寄りの消費生活センターに相談してください。

相談窓口：

■ 消費者ホットライン

電話番号：(局番なし) 188 (通話料有料)

※接続先により受付時間が異なります。

※一部のIP電話などからはつながりません。

■ 参考サイト

当社を装った電気料金支払いを促す不審なメール等について (東京電力エナジーパートナー)

<https://www.tepco.co.jp/ep/archive/20240315.html>

東京ガス社員などを装った訪問や不審メール・電話等にご注意ください(東京ガス)

https://www.tokyo-gas.co.jp/news/notice/notice_01.html

水道料金に関する不審メールについて (東京都水道局)

<https://www.waterworks.metro.tokyo.lg.jp/press/r05/231213-02.html>



消費者庁
消費者ホットライン
188キャラクター
イヤヤン



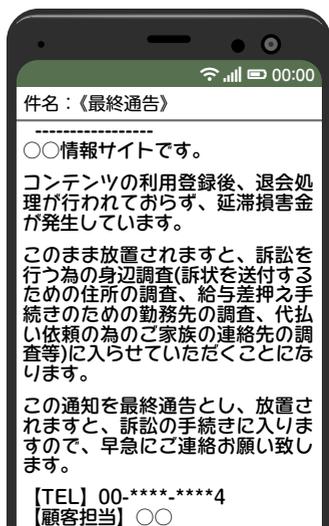
利用した覚えのない架空請求メール

架空請求メールは、「情報料の請求」「有料動画の未納料金の請求」といった身に覚えのない架空の請求をし、払わないと訴訟するなど脅迫的な内容で脅して、お金をだましとろうとする詐欺の手法の一つです。

● 連絡しないで！相手はあなたのことを知りません

悪質な業者は、法律用語や脅迫的な内容で受信者を不安な気持ちにさせて、受信者があわてて連絡してくるのを待っています。支払わなければ「自宅を調べて取り立てに行く」と書かれているものもありますが、多くの場合、相手はあなたのメールアドレス以外知らずにランダムに不特定多数へ請求メールを送っているだけです。

相手に連絡してしまうと、その他の個人情報聞き出される危険があります。絶対に連絡しないようにしましょう。



● 「払えば終わり」ではありません！更なる請求が……

少額ならば払ってしまおうと一度でもお金を支払ったり、業者の要求に支払いそうな様子を見せてしまったらすると、だましやすい「カモ」だと思われ、更なる請求が続くおそれがあります。「払えば終わり」にはなりませんので、決して支払ってはいけません。



メールの特徴

- ・「情報サイト」「総合コンテンツ料」などあやふやなサービス名の料金を請求
- ・「すぐ」「至急」「最終」などの言葉で時間的に急がせる
- ・「料金を払わなければ取り立てにいく」「裁判を起こす」などと脅している

対処法

- ✓ 身に覚えのない請求は「詐欺」。メールに対応せず、無視をしましょう。
- ✓ 架空請求メールが続いてわずらわしいときは、迷惑メールフィルターを利用して受信拒否を設定しましょう。(詳しくは27～30ページ)
- ✓ 架空請求メールの一部には、個人情報などがどこかから漏れて、実際に名前などが記載されているものもあります。トラブルが心配なときは最寄りの消費生活センターに相談してください。
- ✓ もし支払いをしてしまったときは、二次被害をさけるためにも、必ず消費生活センターや警察相談ダイヤル(#9110)で相談してください。

相談窓口：

■ 消費者ホットライン188

電話番号：(局番なし) 188 (通話料有料)

お近くの消費生活相談窓口等につながります。

※接続先により受付時間が異なります。

※一部のIP電話などからはつながりません。



消費者庁
消費者ホットライン
188キャラクター
イヤホン

■ 警察相談ダイヤル

電話番号：#9110 (通話料有料)

受付時間：平日8：30～17：15

(各都道府県警察本部で異なります)

(土日・祝日及び時間外は、一部の県警を除き、当直または音声案内での対応となります)



ビットコインを要求する セクストーション (性的脅迫) メール

セクストーション (性的脅迫) メールは、「アダルトサイトを閲覧している様子の性的動画・写真を入手したので、それを友人・知人にばらまく」と脅して金銭を要求する手口のメールです。

「パソコンをフルアクセスしている」「セキュリティソフトでは検出不可」「メールやSNSの連絡先すべてにばらす」などと強い言葉で脅して、ビットコインで48時間以内に送金するようになどと強要します。

家族や知り合いに誤解されたくない、とあせって支払ってはいけません。一連の脅迫内容はすべて虚偽です。あわてて支払いをしてくるのを待っているだけです。メールには反応せず無視してください。



〈セクストーションメールの例〉

……貴方のアカウントに最近メールをお送りしましたが、お気づきになりましたでしょうか？……私は貴方のデバイスに完全にアクセスできるのです。……訪問されたアダルトサイトに付いていたマルウェアに感染されていらっしゃるからです。……トロイの木馬ウイルスにより、私は貴方のパソコンや他のデバイスに完全にアクセスが可能です。これは、貴方のスクリーンに搭載されたカメラやマイクをオンにするだけで、貴方が気づくことなく、私が好きな時に貴方を見ることが可能となることを意味します。……私のマルウェアは……4時間毎に署名を更新するため、ウイルス対策ソフトでは検出不可能なので通知が送られないのです。……貴方がマスタベーションを行い、……閲覧していた動画が再生されるビデオを私は所有しています。……私がマウスを1度クリックするだけで、貴方のソーシャルネットワークやメールの連絡先全てへと送信されます。……この状況を回避するために出来ることは、\$1000相当のBitcoinを私のBitcoinアドレスへと送金するだけです……2日(48時間)の猶予がございます。このメールが開封されると同時に私は通知を受信し、タイマーが起動します。……このメッセージについて誰かに話したことを私が感知すると、先ほども申し上げた通り、ビデオはすぐに共有されます。

※上記文面は、途中省略して記載しています。ほかにも、文面の異なるメールが多数ありますが、朱書き部分の特徴は同じです。

メールの特徴

- ・「アダルトサイトを閲覧している姿を撮影し、連絡先情報を収集した」などと脅す
- ・「パスワードを傍受」「トロイの木馬を仕込んだ」などハッキングを信じさせようとする記述がある
- ・ビットコインでの支払いを要求する
- ・「48時間以内」「至急」などの言葉で時間的に急がせる
- ・送信元が自分のアドレスになっていたり設定したことのあるパスワードが記載されている場合がある

対処法

- ✓ メールには対応せず、無視をしましょう。
- ✓ メールに記載されていたパスワードを現在も使用している場合は、パスワードの変更をしましょう。
- ✓ トラブルが心配なときは最寄りの消費生活センターか都道府県のサイバー犯罪相談窓口にご相談ください。
- ✓ もし支払いをしてしまったときは、二次被害をさけるためにも、必ず消費生活センターや警察相談ダイヤル(#9110)で相談してください。

相談窓口：

■ 消費者ホットライン188

電話番号：(局番なし)188 (通話料有料)
お近くの消費生活相談窓口等につながります。
※接続先により受付時間が異なります。
※一部のIP電話などからはつながりません。



消費者庁
消費者ホットライン
188キャラクター
イヤマン

■ 警察相談ダイヤル

電話番号：#9110 (通話料有料)
受付時間：平日8:30~17:15
(各都道府県警察本部で異なります)
(土日・祝日及び時間外は、一部の県警を除き、当直または音声案内での対応となります)

参考サイト

独立行政法人情報処理推進機構 (IPA)
性的な映像をばらまくと恐喝し、仮想通貨で金銭を要求する迷惑メールに注意
<https://www.ipa.go.jp/security/anshin/mgdayori20181010.html>



友人・知人から届くチェーンメール

●迷惑の連鎖、チェーンメール

チェーンメールは、受信者に対して「誰かに送らなければ不幸になる」「危害を加える」などと怖がらせたりして転送させるものや、転送したら受験がうまくいく、恋愛成就祈願になるなど良いことが起こるといった内容もあります。

また、献血のお願いやペットの飼い主探し、節電協力などを呼びかけるメールなどもあり、大人でも善意の気持ちからチェーンメールと自覚せずに転送してしまうこともあるようです。

これはホントだから回してください。10月5日、僕の彼女が突然姿を消しました。警察に調べてもらいましたが、すぐ捜査は打ち切りになってしまいました。僕はその犯人が憎くてたまりません。そのためにこのメールを作りました。このメールを1週間以内に20人以上に回してください。僕はPAmw-B38という機械を開発しました。メールを届いてから8日までに20人以上に送信すれば、このプログラムは自動的に削除されます。しかし、もしこのメールを20人以上に送信しなければ、その人を犯人と見なしてメールが届いてから10日目に殺しに行きます。これ以上犠牲者を出すのは悲しいのです。このメールはただのチェーンメールではありません。



●どうしてチェーンメールを回してはいけないの？

送る内容にあなたは責任が持てますか？

チェーンメールは、出所も、真偽もわからない情報です。途中で簡単に書き換えることもできます。転送される中で、危険なサイトへのリンクが付け加えられていることもあります。伝言ゲームのように、次々と変化してしまう不確かな情報を広めてしまうのはやめましょう。

誰かに送るように、などと押し付けないで！

突然送りつけられた上に、転送まで強制されて、“回さないと不幸になる”、なんてすいぶん勝手な話だと思いませんか？自分が受け取った時の嫌な気持ちを、さらに転送する相手に押し付けるチェーンメールは迷惑そのものです。転送してしまえば今度はあなたが迷惑メールの加害者になってしまいます。



●メールからLINE、X(旧Twitter) などSNSへも広がっています

スマートフォンでSNSアプリが広く利用されるにつれ、チェーンメールはSNSアプリ内のメッセージでも送られるようになりました。

メールと比べてやりとりが簡単なため、「1分以内に転送して!」「タイムラインに書きこんで!」などと急がされたりします。また、既読機能で受信者が反応したかどうか、送り手にすぐわかってしまうものもあるため、よりやっかいなものになっています。チェーンメールと同じく、転送を促す内容は無視して、迷惑な送信者とならないよう冷静に対応することが重要です。

●不安なときは迷惑メール相談センターへ

「殺しにいく」「呪われる」などの言葉が書かれていると、どうしても不安で無視できず、友人たちに送ってしまいたくなる場合があります。

迷惑メール相談センターでは、そんな不安を解消するため、チェーンメールの捨て場所となる転送先アドレスを提供しています。

どうしても不安な場合は、友人・知人にチェーンメールを送ってしまう前に迷惑メール相談センターへ転送するようにしてください。

※内容が犯罪予告のような場合には、念のため警察などにも相談してください。



キャリアメール・フリーメール問わず、どのアドレスからでも転送できます!

risu1@ezweb.ne.jp
risu2@ezweb.ne.jp
risu3@ezweb.ne.jp
dakef1@docomo.ne.jp
dakef2@docomo.ne.jp
dakef3@docomo.ne.jp
dakef4@docomo.ne.jp
dakef5@docomo.ne.jp
kuris1@t.vodafone.ne.jp
kuris2@t.vodafone.ne.jp

sun@dekyo.or.jp
mercury@dekyo.or.jp
venus@dekyo.or.jp
earth@dekyo.or.jp
moon@dekyo.or.jp
mars@dekyo.or.jp
jupiter@dekyo.or.jp
saturn@dekyo.or.jp
uranus@dekyo.or.jp
neptune@dekyo.or.jp



※SNSメッセージの場合は、本文をコピー＆ペーストしてメールで送ってください。



迷惑メール対策

迷惑メールを受信しないようにするには、メールアドレス提供事業者の迷惑メールフィルターを使う方法とセキュリティソフトやアプリを利用する方法があります。

各携帯電話事業者やプロバイダの多くは無料で迷惑メールフィルターを提供していますので、利用スタイルにあわせて自分の環境にあった設定をしましょう。

キャリアメール

2024年12月現在



迷惑メールフィルター
@docomo.ne.jp



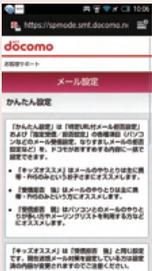
My docomoへ
ログインして
設定

おすすめ：「かんたん設定」

「携帯・PHS／パソコンなどのメール設定」・「特定URL付メール拒否設定」を、ドコモがオススメする設定値に一括で変更することができます。

2024年10月より、フィッシング詐欺の可能性のある不審なメールについて警告を表示する「なりすましメールの警告表示機能」が導入されました。

設定手順：迷惑メール対策のかんたん設定
https://www.docomo.ne.jp/info/spam_mail/spmode/easy_setup/index.html





迷惑メールフィルター
@au.com/@ezweb.ne.jp



My auへ
ログインして
設定

おすすめ：「オススメ設定」

迷惑メールに多く見られる「なりすまし」メールや迷惑メールの疑いのあるメールをブロックします。

設定手順：オススメ設定
<https://www.au.com/support/service/mobile/trouble/mail/email/filter/recommend/>





迷惑メールフィルター
@softbank.ne.jp/
@i.softbank.jp



My SoftBankへ
ログインして
設定

おすすめ：「迷惑メールフィルター」

なりすましメールや、未承諾広告メール、悪意のあるウェブサイトへ誘導するような迷惑メールを受け取らないように設定する方法です。

蓄積されたスパム（迷惑メール）データベースをもとにメールの内容を機械的に判断し、スパムと判断されたメールの受信をブロックします。

設定手順：迷惑メールフィルター
<https://www.softbank.jp/mobile/support/mail/antispam/email/i-spammailfilter/>





迷惑メールフィルター
@ymobile.ne.jp



My Y!mobileへ
ログインして
設定

おすすめ：「迷惑メールフィルター」

迷惑メールデータベースを元に迷惑メールの受信を拒否することができます。また、メールの件名欄に「! 広告!」などが記載されているメールを未承諾広告メールとし受信を拒否することもできます。

設定手順：迷惑メール対策
https://www.ymobile.jp/support/relief/trouble_mail/



迷惑メールフィルター
@uqmobile.jp

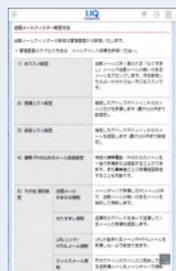


My UQ mobile
へログインして
設定

おすすめ：「おススメ設定」

迷惑メールに多く見られる「なりすまし」メールや迷惑メールの疑いのあるメールをブロックします。何を設定したらよいか分からない方におすすめです。

設定手順：メールサービス設定方法/迷惑メールフィルター
<https://www.uqwimax.jp/mobile/support/guide/mail/>



フィルター設定機能
@rakumail.jp

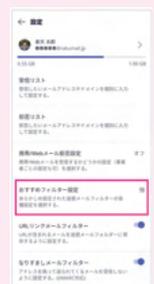


Rakuten Linkアプリより設定可能

おすすめ：「おすすめフィルター設定」

あらかじめ設定された迷惑メールフィルターの各種設定を「オフ・標準・強」から選んで設定できます。

※デフォルトはおすすめフィルター設定（強）になります。
設定手順：おすすめのメールフィルターを設定する
https://network.mobile.rakuten.co.jp/guide/rakumail/filter_2/#setting01



被害にあわないための
セキュリティ対策

※操作方法や詳細は56ページの各窓口からお問い合わせください。

プロバイダメール・フリーメール

プロバイダ・フリーメールのメールアドレスで受信する迷惑メール対策としては、各種サービスが提供する迷惑メールフィルターを利用しましょう。一部をのぞき、無料で提供されています。メールサーバー上で迷惑メール判定を行うため、受信トレイに迷惑メールが届きにくくなります。詳しくは各種サービス窓口にお問い合わせください。



迷惑SMS対策

迷惑SMSを受信しないように、携帯電話事業者が提供している迷惑SMSフィルターを利用しましょう。不審なSMSや架空請求SMSなどを事前に届かないようにブロック設定することができます。自分の利用スタイルにあわせて選択して設定しましょう。

携帯会社のSMS(ショートメッセージ・Cメール)2024年12月現在

docomo



My docomoへ
ログインして
設定

5G (ahamo)
も同様

- **SMS一括拒否**：すべてのSMSを拒否
- **危険SMS拒否**：フィッシングSMSと判定されたSMSを拒否
- **非通知SMS拒否**：非通知のSMSを拒否
- **国際SMS拒否**：海外事業者から送信されたSMSを拒否
- **国内他事業者SMS拒否**：ドコモ以外の事業者からのSMSを拒否
- **個別番号拒否**：個別に指定した電話番号からのSMSを拒否
- **個別番号受信**：個別に指定した電話番号からのSMSのみを受信
- **なりすましメールの警告表示機能 (2024年10月より提供開始)**：フィッシング詐欺の可能性がある不審なメールに警告を表示

au



設定の詳細は
各HPをご覧
ください

**UQ
mobile**



- **SMS(Cメール) 国内他事業者ブロック機能**：
au、UQ、povo以外の事業者からのSMS(Cメール) を拒否
- **SMS(Cメール) 海外事業者ブロック機能**：
海外事業者から送信されたSMS(Cメール) を拒否
- **SMS(Cメール) オプションの停止**：
すべてのSMS(Cメール) を拒否 (SMS(Cメール) の送信も
できなくなります)
- **迷惑SMSブロック**：
迷惑SMSの疑いのあるSMSを自動判定しブロックします。

SoftBank



My SoftBankへ
ログインして
設定

LINEMOも同様

Y!mobile



My Y!mobileへ
ログインして
設定

・なりすましSMSの拒否：

差出人をSoftBankなどになりすましたSMSを拒否

・すべての電話番号、または特定の電話番号から送られてくるメールを「許可／拒否する」：

すべてのSMSを拒否

・特定の電話番号（SMS）で送られる迷惑メールの拒否設定：

個別に指定した電話番号からのSMSを拒否

・URLリンク付きのSMSを拒否：

携帯電話番号から送られるSMS本文にURLリンクが含まれているSMSを拒否

・迷惑SMSフィルター：

受信したSMSを機械的に迷惑メールかどうか検知し拒否。悪意あるウェブサイトへ誘導するSMSに有効。

Rakuten Mobile



拒否設定を利用しない場合は、Rakuten Linkアプリより設定可能

・迷惑SMS拒否設定（2024年7月より提供開始）：

フィッシング詐欺対策として、有害なサイトのURLや電話番号が含まれるSMSを自動で拒否。

※拒否設定については申し込み不要で、自動適用

※操作方法や詳細は56ページの各窓口からお問い合わせください。



セキュリティ対策

●スマートフォンはパソコンと同じ！セキュリティ対策は必須です

スマートフォンの機能はパソコン同等とも言われます。ウイルスや不正アプリでの被害を避けるため、セキュリティ対策を行うことが必要です。

●スマートフォンを狙うウイルス

パソコン同様のセキュリティを！

スマートフォンはパソコンと同じようにOS（基本ソフト）が搭載され、さまざまなアプリをインストールすることができる一方で、セキュリティ対策を怠るとウイルスに感染するおそれがあります。このため、パソコンと同様にセキュリティ対策を行っていくことがとても重要です。

また、ウイルスはインストールしたアプリ内にも仕込まれスマートフォン内で不正行為を働く場合もありますので、不正なアプリのインストールをしないよう注意する必要があります。

ウイルスに感染したらこんな事態も…

- ・アドレス帳や写真、個人情報などの重要な情報が抜き取られてしまう。
- ・抜き取られた情報を使われて、クレジットカードやオンラインの決済サービスを不正利用されてしまう。
- ・SNSやWebサービスのアカウント情報が抜き取られ不正利用されてしまう。
- ・スマートフォンが外部から遠隔操作されて知らない間に迷惑メールの大量送信をされ、迷惑行為を行う加害者となってしまう。
- ・端末に保存したデータが消えてしまう。



● 携帯電話事業者が提供するセキュリティサービス

2024年12月現在

<p>NTTドコモ あんしんセキュリティ</p>	<ul style="list-style-type: none"> ・アプリをインストールする際、ウイルスが混入していると検出する ・設定で、定期的にウイルスの検出を行うことができる ・ウェブサイトの安全性を判定して、フィッシングサイトなど危険なサイトへのアクセスを警告しブロックする ・危険なWi-Fiスポットに接続すると、警告を出す
<p>au ウイルスバスター™ for au/ウイルスブ ロック</p>	<p>Android端末を対象に</p> <ul style="list-style-type: none"> ・ウイルスを検知、侵入をブロックする ・不正サイトへのアクセス規制および警告表示を行う ・決済アプリの保護機能 ・アプリをインストールする際にリアルタイムでセキュリティの脅威をチェックする ・フィッシング詐欺やワンクリック詐欺など危険なWebサイトへのアクセスをブロックする
<p>SoftBank・ ワイモバイル セキュリティOne</p>	<ul style="list-style-type: none"> ・危険サイトチェック 悪意のある詐欺サイトを検知し、警告する ・危険Wi-Fiチェック 危険なWi-Fiへの接続や不正アクセスを検知し、警告する ・迷惑電話チェック 振り込め詐欺などの迷惑電話からの着信時に警告する ・迷惑メッセージチェック 「メッセージSNSアイコン」に届いた迷惑メールを自動で検知し振り分ける
<p>UQ mobile ウイルスバスター モ バイル for UQ mobile</p>	<ul style="list-style-type: none"> ・不正なアプリのダウンロードやインストールをブロックする(不正アプリ対策(ウイルス対策)) ・Webサイトの安全性を判定し、不正アプリの配布元サイトや、フィッシングサイト、不正アプリの情報送信先サイトなどへのアクセスをブロックする(Web脅威対策)
<p>楽天モバイル ノートン™ モバイル セキュリティ</p>	<ul style="list-style-type: none"> ・Web保護：悪質なサイトや詐欺サイトなど、危険なWebサイトへのアクセスの際に警告 ・Wi-Fiセキュリティ：安全でないWi-Fiネットワークに接続の際に警告 (Android版) アプリアドバイザー：アプリの危険性を判定し警告 (iOS版) デバイスセキュリティ：OSが古くなっているとユーザーに通知し、その影響について警告

※サービスの詳細は、ご利用中の携帯電話事業者へお問い合わせください。

被害にあわないための
セキュリティ対策

● セキュリティベンダーが提供する対策ソフトの利用

セキュリティ対策ソフト提供会社でも、スマートフォン用のセキュリティソフトを発表しています。盗難・紛失対策、Web脅威対策などの機能を搭載しているものもありますので、スマートフォンの機種毎の対応状況を確認して利用するとよいでしょう。



有害サイト・有害アプリ対策

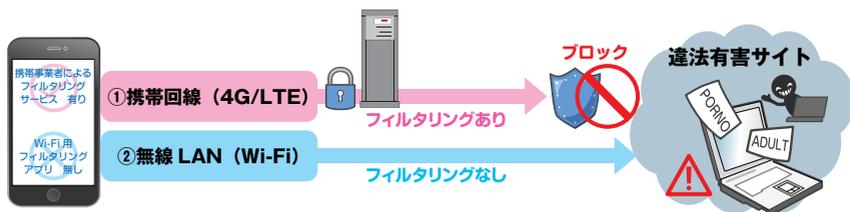
スマートフォンを利用して、いつでも・どこでも膨大なインターネットの情報にアクセスできるようになりました。しかし、インターネット利用で、思いがけず危険な情報へアクセスしてしまいトラブルに巻き込まれる可能性が高くなっています。

特に、スマートフォンの利用が低年齢化し、小学生が利用することもめずらしくなくなった現状では、子どもたちが知らないうちに有害な情報へアクセスしてしまう危険性が高くなっています。

詐欺サイトなどの危険なサイトや出会い系・アダルト系などの性的な表現を含むもの、違法情報などを表示させないように、あらかじめフィルタリングを設定しましょう。

フィルタリングの特徴

1. スマートフォンから有害サイトへのアクセスを制限できます
2. アクセスを制限しても閲覧が必要なサイトは個別に許可することができます
3. 一般向け、小学生向け・中学生向けなど、年代や利用スタイルにあわせて設定できます
4. 専用アプリを利用することで、無線LAN (Wi-Fi) 利用時にも有害サイトへのアクセス制限ができます



ポイント

- Wi-fi接続時は、携帯回線のフィルタリングが適用されません。
- スマホ本体へのフィルタリングアプリのインストールが必要です。

● 携帯電話事業者が提供するフィルタリングサービス

2024年12月現在

		①Web利用	②Wi-Fi利用	③アプリ利用
NTTドコモ	iPhone※ 2	あんしんフィルター for docomo ※ 1 ※ 4		端末本体の「機能制限」設定により制限可能
	Android	あんしんフィルター for docomo※ 3		
au・UQ mobile	iPhone※ 2	あんしんフィルター for au※ 1 ※ 4		端末本体の「機能制限」設定により制限可能
	Android	あんしんフィルター for au (Android™) ※ 6		
SoftBank・ワイモバイル	iPhone※ 2	あんしんフィルター※ 1 ※ 5		端末本体の「機能制限」設定により制限可能
	Android	あんしんフィルター※ 3		
楽天モバイル	iPhone※ 2	あんしんコントロール by i-フィルター※ 5		端末本体の「機能制限」設定により制限可能
	Android	あんしんコントロール by i-フィルター※ 3		

- ※ 1 iOS端末の場合、フィルタリングアプリの利用と併せて、Safari（標準搭載ブラウザ）を「OFF」にしておく必要があります。
- ※ 2 携帯電話事業者で回線契約したiPadを含みます。
- ※ 3 AndroidOS 6以上が対象です。
- ※ 4 iOS 9.0以上が対象です。
- ※ 5 iOS 13以上が対象です。
- ※ 6 AndroidOS 5.0以上が対象です。
- ※ サービスの詳細は、各携帯電話事業者へお問い合わせください。



被害にあわないための
セキュリティ対策

● セキュリティベンダーが提供するフィルタリングサービス

セキュリティベンダーでも、スマートフォン用のセキュリティソフトを提供しています。盗難・紛失対策、Web脅威対策などの機能を搭載しているものもありますので、スマートフォンの機種毎の対応状況を確認して利用するとよいでしょう。

※ サービスの詳細は、各セキュリティベンダーへお問い合わせください。

子どもの安全なスマートフォン 利用のために

子どもがスマートフォンを利用する際には、親子で話し合いながら、使う時間、対処の仕方、ルールを守れなかった場合の対応などのルールを決めておきましょう。

【中学生向けルールの例】（スマートフォン利用の注意点チェックリストとしてもご利用ください）

使い方のルール	✓
利用してもいい時間【平日 : ~ : 休日 : ~ : 】	
アプリに使える金額は1ヶ月に_____円までとする	
ルールを守れなかったときは「一時利用停止」する	
トラブルにあったらすぐに保護者か先生に相談する	
有害サイト・迷惑メールのトラブルを防ぐために	✓
Web（Wi-fi利用時も）・メール・アプリの3つのフィルタリングを設定する	
アダルト系や犯罪・違法情報などを掲載している不適切なサイトは利用しない	
不用意に電話番号やメールアドレスを教えない	
知らない人からのメールやメッセージに返信しない	
ネットで知り合った人に誘われても会いに行かない	
迷惑メールやメッセージは開かない、返信しない	
料金請求メールが突然届いてもあわてて支払わない	
誰かに転送を促すチェーンメールやメッセージは無視して転送しない	
SNS（ソーシャルネットワーキングサービス）でのトラブルを予防するために	✓
ネット上に名前や住所など個人情報に関する書き込みをしない	
情報を公開する範囲は友人のみなど「必要最低限」に設定する	
誹謗中傷や犯罪予告、悪ふざけなどは絶対に書き込まない	
ネット上に写真を掲載する時は肖像権や位置情報に注意する	
オリジナルルール	✓
歩きながらや自転車で乗りながらスマートフォンを使わない	

参 考

- スマホ・ケータイファミリーガイド on WEB（au）
<http://www.kddi.com/family/rules/>
- 家族で話そう！お子さまの携帯電話利用のルール（SoftBank）
<https://www.softbank.jp/mobile/support/3g/protect/kids/rule/>

●こんな時どうする？保護者のお悩みにお答えします

子どもから「あのアプリが使えないからフィルタリングを外して！」って言われて困っています。

➤ アプリ起動のフィルタリングを設定したままでも、利用したいアプリがある場合には、そのアプリを個別に起動できるように設定変更することができます。

例えば、フィルタリング設定で起動できなくなっているアプリをどうしても利用したいのであれば、一覧からそのアプリを選んで起動できるようにしてください。

アプリの起動制限を外すと、そのアプリはフィルタリングサービスによる保護がなくなります。制限を外した後は、子どもが安全に使っているか、保護者の方がしっかり見守ってください。

子どもがスマートフォン依存にならないか心配です。 22:00

➤ フィルタリング機能のカスタマイズで、サイトアクセス可能時間帯の制限やWeb毎に起動可能時間帯の設定をして使い過ぎを防止することができます。



iPhoneで子ども向けの安全なアプリを知りたい！

➤ App Storeで配信されるアプリには、アプリ毎に対象年齢が設定されています。iPhone本体で「許可するAppのレート設定」を行うことで、まとめて対象年齢外のアプリのダウンロードを制限することができます。対象年齢は4+（4歳以上9歳未満）、9+（9歳以上12歳未満）、12+（12歳以上17歳未満）、17+（17歳以上）から選択できるので、お子様の年代に応じてレートを設定すると、対象外のアプリは表示されないようになります。



「設定」>スクリーンタイム>コンテンツとプライバシーの制限>コンテンツ制限の「App」の順にタップ。許可するAppのレートに対象年齢を選んでください。

例えば、「12+」に設定すると【App Store】から「17+」のレーティングがかけられたアプリはダウンロードすることが出来ません。





迷惑メールは法律違反

● 広告宣伝メールの送信は法律で規制されています

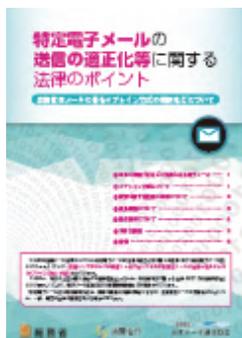
平成14年（2002年）4月に広告宣伝メール送信のルールを定めた「特定電子メールの送信の適正化等に関する法律」（以下、「特定電子メール法」といいます。）が成立し、同年7月1日から施行されました。

その後、メール送信手法の悪質化および巧妙化が進んだことから、平成17年5月（同年11月1日施行）と平成20年6月（同年12月1日施行）に法律の改正が行われ、平成20年の改正では、広告宣伝メールは、原則としてあらかじめ同意した者に対してのみ送信が認められることとなっています。

同意を得て広告宣伝メールを送信する場合でも、次の表示が義務づけられています。（右ページの図を参照してください）

- ① メール本文に、送信者などの氏名又は名称
- ② メール本文に、受信拒否の通知を受けるための電子メールアドレス又はURL
- ③ 受信拒否の通知先の直前又は直後に、受信拒否の通知ができる旨
- ④ 任意の場所に、送信者などの住所
- ⑤ 任意の場所に、苦情・問合せなどを受け付けることができる電話番号・電子メールアドレス又はURL

また、送信者情報を偽って送信することは禁止されています。
詳しい法律のポイントについては以下の資料をご覧ください。



特定電子メールの送信の適正化等に関する法律
のポイント

— 広告宣伝メールに係るオプトイン方式の規制
などについて —



健康サプリが特別価格!

差出人: soushinsya@example.xx
 送信日時: 2018.7.10(Tue) 00:01
 To: 総務次朗[jiro@soumu-syo.xx]
 件名: 健康サプリが特別価格!

【このメールの送信者】
 △△株式会社

<配信停止手続はこちらから↓>
<http://www.example.com/xx/teishi@example.xx>

【製品の販売事業者】
 ☆☆株式会社

<配信停止手続はこちらから↓>
<http://www.jigyosya.example/xx/teishi@jigyosya.xx>

! キャンペーン実施中!
 ☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆
 忙しいあなたに
 健康サプリが特別価格!
 ☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆

■商品の購入はこちらから↓
<http://www.kenko/xx/x>

■送信者の住所はこちらに記載↓
<http://jyuso/example>

■各種問合せはこちらから↓
<http://toiawase/example>

送信者情報(送信に用いた電子メールアドレス、IPアドレス、ドメイン名)を偽って送信することは禁止されています。

✓送信者など(※1)の氏名または名称

✓受信拒否の通知ができる旨
 受信拒否の通知先の直前または直後に表示する必要があります。送信に用いられた電子メールあてに送信することで通知できる場合は、その旨を電子メールの中の受信者が容易に認識できる場所に表示する必要があります。

✓受信拒否の通知を受けるための電子メールアドレスまたはURL(※2)
 URLとする場合は、リンク先において、受信拒否に必要な情報が明確かつ平易に提供され、受信拒否の通知が容易に行うことができるよう、必要な措置が講じられている必要があります。

特定商取引法上の販売業者などと送信者などが異なる場合

✓販売業者などの氏名または名称
 ✓相手方が電子メール広告の提供を受けない旨の意思を表示するための電子メールアドレスまたはURL(※2)

特定商取引法に基づくその他の表示事項はリンク先での表示とすることも可能です。

✓送信者などの住所
 ✓苦情・問合せなどを受け付けることができる電話番号、電子メールアドレス、URL(※2)
 リンク先での表示とすることも可能です。その場合は、表示場所を示す情報を電子メールの中に表示する必要があります。

※1 電子メールの送信を委託している場合は、送信者または委託者のうち送信に責任を有するもの

※2 ハイパーリンクとすることも可能

★表示義務には一定の例外があります(例えば、受信拒否の対象とならない広告宣伝メールにおいては、受信拒否の通知ができる旨や受信拒否の通知先を表示する必要がないなど)。

もっと
知りたい

詳しくは、総務省のホームページをご覧ください。

https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html

情報提供のお願い

●「特定電子メール法」に違反して 広告宣伝メールを配信すると処罰されます

広告宣伝メールについては、「特定電子メール法」によって「原則としてあらかじめ送信の同意を得た者以外の者への送信禁止」「一定の事項に関する表示義務」「送信者情報を偽った送信の禁止」「送信を拒否した者への送信の禁止」などが定められています。

これらのルールを守っていないメールは違法となり、総務大臣及び内閣総理大臣は、メールの送受信上の障害を防止するため必要があると認める場合、送信者に対しメールの送信方法の改善に関し必要な措置をとるよう命ずることができます。

送信者情報を偽って送信した場合や、送信者が総務大臣及び内閣総理大臣の命令に従わない場合には、1年以下の懲役または100万円以下の罰金（法人の場合は、行為者を罰するほか、法人に対して3000万円以下の罰金）に処せられます。



●違反メールの情報提供にご協力を！

「特定電子メール法」に違反していると思われる迷惑メールを受け取られた場合は、以下の方法で迷惑メール相談センターまで情報提供をお願いします。

ご提供いただきました違反情報につきましては、総務大臣及び内閣総理大臣による違反送信者への措置に活用させていただきます。

注意!

- ※情報提供に際しては、個人情報が必要としないので、氏名・住所・電話番号などの個人情報は入力しないで下さい。
- ※個々の情報や送信者への措置状況などについての照会には対応いたしませんので、あらかじめご了承ください。

法律に違反していると思われるメールの情報提供は、以下のいずれかの方法によりお願いします。送信者情報を偽ったメールの情報提供の際には、ヘッダ情報の添付をお願いします。

メール

モバイルやPCから

メールを転送
送信先アドレスmeiwaku@dekyo.or.jp



ウェブから

フォームへの入力
https://www.dekyo.or.jp/bingo/mail_ghan_meiwakuform/



近畿大学警察 近畿大学情報センター
迷惑メール相談センター

違反メール情報提供

オプトイン通知、禁止義務通知、なりすましメールの情報提供
受信記録に添付された迷惑メールの通報受付と対応を行います
上記の対応に関する情報は下記をご覧ください。

違反メールについて

発信日時	送込先: 近畿大学情報センター
違反メールの送信者アドレス(氏名)	送込先: 1111111111111111
違反メールの件名	送込先: 1111111111111111

被害にあわないための
セキュリティ対策

SMS(ショートメッセージサービス)

モバイルから

フォームへの入力
https://www.dekyo.or.jp/bingo/mail_ghan_meiwakuform/



近畿大学警察 近畿大学情報センター
迷惑メール相談センター

違反SMS情報提供

特定電子メール法に違反しているSMSの情報提供となります。

発信日時 送信日時を選択し送信日時を入力してください。
(例: 2024-04-18)

発信者氏名 送信日時を選択し発信者氏名を入力してください。
(例: 近畿大学情報センター 近畿大学情報センター 1111111111111111)

発信元電話番号 送信日時を選択し発信者氏名を入力してください。
(例: 03-XXXX-XXXX)

ネット社会の危険

インターネットは、現在の私たちのくらしに、もはや欠かせないものとなっています。モバイル端末の普及に伴い、いつでも・どこでも、さまざまな情報を手に入れられるようになりました。しかし、便利になった反面、インターネットを通じて、詐欺被害、個人情報の流出、掲示板での炎上など、さまざまな問題・事件が起こるようになってきました。



スマートフォンが、小学生から高齢者まで幅広い世代に浸透したいま、インターネットにある多くの危険から身を守るため、利用者のICTリテラシーを向上させることが重要となっています。

● ICTリテラシーを学んでトラブルを避けよう

ICTとは、Information（情報）、Communication（通信）、Technology（技術）の略で情報通信技術を意味します。ICTリテラシーは、インターネットの情報を読み解く能力やスマートフォン、クラウドサービスなどのツールを安全・安心に活用してコミュニケーションを行う能力のことです。

インターネットを安全・安心に利用するには、パソコンやスマートフォンの操作ができるだけでなく、ネット社会において危険なトラブルをさけるために必要となる知識やスキルを学ぶことが必要です。

スマートフォンやSNSをもっと楽しむために、ICTリテラシーを身につけましょう。

ICTリテラシーを学ぶには？

多くの分野において、ICTリテラシー向上のためのさまざまな取組が進められています。

「ICTメディアリテラシーの育成」

総務省では、子どもから高齢者まで安全に安心してインターネットや携帯電話などのICTを活用できるようホームページで学習コンテンツ等を公開しています。教材は、無料で利用することができます。

https://www.soumu.go.jp/main_sosiki/joho_tsusin/kyouiku_joho-ka/media_literacy.html



「インターネットトラブル事例集」

総務省では、インターネット、スマートフォンを始めとするデジタル機器、SNSなどのコミュニケーションツールについて「賢く活用する知識・知恵」「ルールを守って使える健全な心」「安全に利用するための危機管理意識」を育む一助として、インターネットトラブル事例集を作成し、その予防法と対処法を紹介しています。

https://www.soumu.go.jp/use_the_internet_wisely/trouble/



「インターネットルール＆マナー検定」

(一財)インターネット協会では、インターネットを安全・安心に利用するためのルールやマナーに関する無料のWeb検定試験を行っています。「ビジネス版」、「こどもばん」、「こどもばんふりがな」、「大人版」の四種類があり、サイトから24時間受検することができます。

<https://rm.iajapan.org/>



情報発信は慎重に行いましょう

● インターネットで発信した情報は消えません

インターネットは、世界中の人々へ個人でも発信できるメディアです。発信した情報は基本的に全世界に公開されることになり、簡単に複製され、短時間で広まると削除することもできなくなります。

そして、発信した内容によっては意図しない想定外の反応が起こることもあります。

● その書き込み、本当に大丈夫？

以前からSNSなどでの発言をきっかけに、個人や企業への批判や誹謗中傷が、不特定多数から集中して寄せられる事象が起こっています。いわゆる“ネット炎上”です。

批判や誹謗中傷の対象とされた方が、無関係の第三者だった場合、問題はさらに深刻になります。

2019年8月に高速道路で発生したあおり運転に関連して男女が逮捕された事件がありました。この際に、暴行の様子を撮影する女の動画が拡散したことをきっかけに、ネット上では、事件とはまったく関係のない女性の名前や写真、会社名が投稿され、多くの事実無根の誹謗中傷を受けることとなりました。

「誤った情報を発信するとその責任を問われます。他人を傷つけるような投稿は自分に跳ね返ってきます」書き込みなどの情報発信をきっかけに、警察に逮捕されたり、相手から損害賠償を請求されたり、学校や職場から処分を受ける事例もあります。情報発信する際は、個人情報を含んでいないか、人を傷つけるような内容が含まれていないか、真偽不明の情報でないか、などを必ず確認するよう心がけましょう。



● 個人情報の公開は最小限に

SNSの利用にあたっては、インターネット上に、氏名、メールアドレス、写真といった情報を公開することの危険性についても、きちんと認識しておかなければなりません。不用意に個人情報を書き込んでしまうと、さまざまなトラブルを呼び込むきっかけとなります。

トラブルから身を守るため、投稿する内容は最小限にし、むやみに個人情報を公開しないようにすることが大切です。

SNSは、利用者の使い方にあわせて投稿内容やプロフィール閲覧の公開範囲が制限できますから、トラブルや情報をとられることを避けるため、少なくとも「投稿公開範囲」、「アカウントの検索可能範囲」を次のように設定しておくといよいでしょう。

2024年12月現在

	投稿公開範囲	アカウントの検索可能範囲
LINE	設定>LINE VOOM>新しい友だちに自動公開>OFF 設定>LINE VOOM>友だちの公開設定>友だちごとに公開・非公開を設定	設定>友だち>友だち自動追加>OFF 設定>友だち>友だちへの追加を許可>OFF 設定>プライバシー管理>IDによる友だち追加を許可>OFF
Facebook	メニュー>設定>設定とプライバシー>共有範囲と公開設定>投稿>今後の投稿のプライバシー設定>友達	メニュー>設定>設定とプライバシー>共有範囲と公開設定>検索と連絡に関する設定>あなたから提供されたメールアドレスまたは電話番号を使って私を検索できる人>友達
X (旧Twitter)	設定とサポート>設定とプライバシー>プライバシーと安全>オーディエンスとタグ付け>ツイートを非公開にする	設定とサポート>設定とプライバシー>プライバシーと安全>見つけやすさと連絡先>メールアドレスまたは電話番号の照会と通知を許可する>OFF 見つけやすさと連絡先>アドレス帳の連絡先を同期>OFF
Instagram	設定>設定とアクティビティ>アカウントのプライバシー>非公開アカウント>OK	設定>設定とアクティビティ>アカウントセンター>あなたの情報とアクセス許可>連絡先をアップロード>連絡先をリンク>OFF

※設定方法はOSや機種、アプリのバージョンにより異なります。

また、公開範囲を友だちに限定していてもその友だちが内容を転載してしまうこともあり得ます。ネット上に書きこんだ文章・写真は決して取り消すことはできませんから、普段から不特定多数に読まれたり見られたりしても困らない内容かどうか十分注意をして投稿するようにしましょう。

意図しない情報の流出を 防ぎましょう

● 知らないうちにあなたのいる場所を公開していませんか

いろいろな利用者との日常的な会話から情報収集までできるSNSは便利で楽しいサービスですが、一方で、SNSに掲載されたこれらの情報を狙う犯罪者が増えていることにも注意が必要です。

SNSでは、アプリの位置情報利用をONに設定にしておくと、投稿に位置情報が付けられ、自分の所在地を不特定多数へ知られることにもなりかねません。頻繁に位置情報を公開していると住所や学校などの個人情報が特定されるおそれもありますので注意してください。

スマートフォンのプライバシー設定で位置情報サービスの設定を利用しないこともできますので、一度設定を見直しましょう。

2024年12月現在

	位置情報OFF設定
LINE	スマートフォンの設定でLINEの「位置情報利用」権限をOFFにする
Facebook	スマートフォンの設定でFacebookの「位置情報利用」権限をOFFにする
X (旧Twitter)	「設定」>「設定とプライバシー」>「プライバシーと安全」>「位置情報」>正確な位置情報をもとにカスタマイズをOFFにする
Instagram	スマートフォンの設定でInstagramの「位置情報利用」権限をOFFにする

※設定方法はOSや機種、アプリのバージョンにより異なります。



● 写真から自宅の場所がわかってしまうこともあります

スマートフォンで撮影した写真に、撮った場所が記録されているって知っていますか？

スマートフォンには、GPS機能がついているので、カメラアプリの設定が位置情報機能ONになっていると、撮影した写真に位置情報が記録されています。

ということは、位置情報機能をONにしたまま、自宅で写真を撮って、その写真をそのままインターネットへ公開してしまうと、自宅の場所が特定できてしまうことになってしまいますね。

トラブルを避けるためにも、カメラアプリの位置情報機能はOFFにしておきましょう。



● 位置情報機能をOFFにしても場所がわかってしまう？

写真に写り込む情報から、その場所がわかってしまうこともあります。電信柱などに書いてある住所が写真に写っているかもしれませんし、お子さんの入学式の写真だったらその学校がわかってしまうかもしれません。

SNSの中には、投稿するときに付近のお店などのスポット情報を「位置情報」として追加することもできるものもありますが、自宅や学校などで撮影した写真にその「位置情報」をつけてしまうと、おおよその場所がわかってしまいます。自宅周辺などからの投稿では「位置情報」を追加するのはやめましょう。



STOP!
ネットトラブル

カメラの位置情報利用をOFFにしても、決して安心はできません。写真をインターネットへ公開する際は、事前によく確認するようにしましょう。

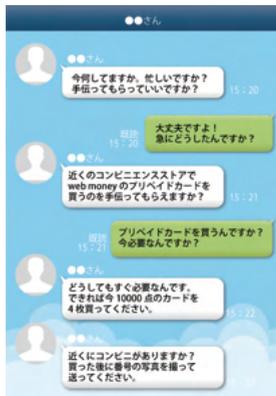
SNSアカウントが乗っ取られる被害が増えています!

スマートフォンの普及でSNSの利用者が増えてくると、SNSでも悪質サイトへ誘導する迷惑メッセージや詐欺被害なども発生するようになりました。知らないうちにアカウント（ID・パスワード）を乗っ取られて不正利用されるという被害もあとを絶ちません。

●アカウント管理がとても重要です

アカウントを乗っ取られるとクラウド上に保存してあるプライベートな情報が盗まれたり、詐欺サイトへ誘導しようと、つながっている友人知人にあなたのアカウントで不正なメッセージが送信されたりします。

特に、SNSアカウントとアプリの連携には注意が必要です。アプリ側がこの機能を利用できるようになると本来アカウント利用者しか行えない操作をアプリ側が外部から行えるようになってしまいます。不正なアプリだった場合、不正ログインされてアカウント情報を盗みとられてしまうわけです。



●アカウント乗っ取りでこんな被害も

IDとパスワードを不正な手段で入手した乗っ取り犯が、勝手にログインしたうえで、そのアカウントの友人・知人へ「緊急で必要だからプリペイドカードを購入して番号を知らせて」とメッセージを送り、金券番号をだましとるといった事件もありました。

全く知らない他人なら、怪しんだり警戒したりしますが、友人・知人の名前で送られてきたメッセージだったために疑うことはなく協力してしまい、多数の被害が発生してしまいました。少し不審な内容でも信じて協力してしまったようです。

●パソコンなどからはログインできないようにもできます

LINEはパソコンやタブレットからも利用することが可能です。もし、乗っ取り犯がパソコンやタブレットから不正にログインしたとしても、スマートフォンでは、いつもどおりLINEアプリが利用できるため、通知が届いても乗っ取られたことに気づかない可能性があります。

スマートフォンでの利用しかしない場合は、パソコンなどからログインできないよう設定しておくことで安全です。

「設定」→「アカウント」→「ログイン許可」をタップし、チェックを外す



乗っ取られないための対策

アカウントを乗っ取られないために、以下の点に注意し、対策をしておきましょう。

1. 複数サービスでIDやパスワードの使い回しをしない
乗っ取り犯は、入手したIDやパスワードで他のサービスにも不正ログインを試みます。同じID・パスワードにしておくで複数のSNSが乗っ取られる可能性があります。あり危険です。
2. SNSサービス間のアカウント連携を避ける
最近のSNSの多くは連携機能を利用して同時投稿などができますが、上記と同じように、1つのアカウントが乗っ取られた場合、連携機能を利用して他サービスにもアクセスされることになってしまいます。
3. 2段階認証を利用する
2段階認証は、ログイン時にSMSで届く認証コードの入力を必要とする機能です。多くのSNSサービスでは、アカウント乗っ取り対策として、いつもと異なるスマートフォンやパソコンなどの環境からログインした場合、登録しておいた携帯番号へSMSで認証コードが送られ、そのコードを入力しないとログインできない設定とすることができます。もし、IDやパスワードが流出してしまっても、これにより不正ログインを防ぐことができます。



乗っ取られてしまったときは

乗っ取り犯により不正ログインされたことに気づいたときは、すぐにパスワードを変更しましょう。もし、既にパスワードが変更されてログインできないときは、運営会社に連絡して対処してください。

参考Webサイト

LINE
ヘルプセンター



Facebook
ヘルプセンター



X(旧Twitter)
ヘルプセンター



Apple
サポート



緊急時の情報発信

● 緊急時にはデマが広がります

災害発生時や緊急時には、安否確認、緊急情報、最新の災害情報、救急救命情報の収集や支援要請の情報発信などスマートフォンなどのモバイル端末を使ったコミュニケーション手段が大きな役割を果たしています。反面、メールやX（旧Twitter）、LINEなどのSNS上では、実際に起こっていない事故や事実と異なる情報、必ずしも正確ではない情報、面白半分で載せたウソの情報などが発信されデマとして広がります。過去の震災、大型台風による災害時も、多種多様のデマ情報が発生しました。

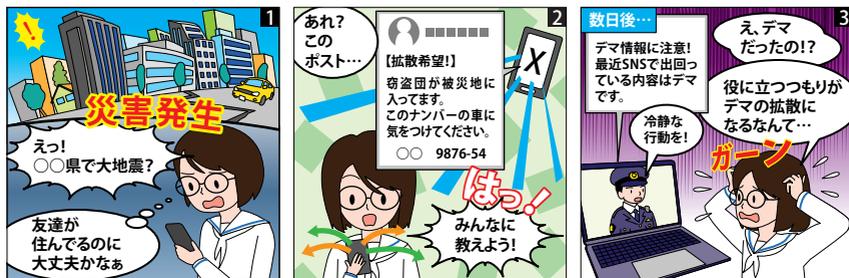


● デマが広がる理由

緊急時においては、人々は、不安な状況が続く中、少しでも役に立つ情報を得ようとします。そして、「役に立ちそうな情報」を見つけると、「みんなに伝えるべき情報」と考え、情報の信頼度にかかわらず、友人や知人へ伝えようとします。

友人や知人から得た情報は、一般的にその価値を高く見てしまうようで、チェーンメールとなったり、SNS上で拡散していきます。

SNSでは書き込み後、ボタンひとつで全世界に情報を発信することができます。災害時のこうした拡散しやすい状況と便利なツールが重なり、災害後にデマが広がりやすくなっていきます。



●デマがもたらす悪影響

1. 内容によっては混乱を引き起こしたり、被災者の不安を拡大させる

災害時や緊急時だからこそ、正確な情報が必要です。真偽を確かめないまま情報を送ることは、たとえ善意の気持ちからであってもやめましょう。

2. 誤った情報や不確かな情報は混乱や活動に支障をきたすおそれがある

刻一刻と状況が変わる中で、最初は正しかった情報だったとしても時間の経過により誤った情報になることも考えられます。不確かな情報は、現場に無用の負担を強いることになりかねず、現場が混乱し活動に支障をきたしかねません。

3. 限られた通信環境を圧迫し、必要な情報が行き届かないことにもなりかねない

デマ情報の拡散で、通信ネットワークの負荷が上昇し通信環境への深刻な影響を引き起こすことにもなりかねません。

●災害時や緊急時だからこそ、情報発信は正確に

真偽の分からない情報が拡散すると、本当に必要な情報を阻害する原因にもなりかねません。

もし、根拠の疑わしい情報・未確認の情報のメールやSNS上の情報を見たときは、もしかしたらデマかもしれないと疑い、まずは情報の真偽を確かめるようにしましょう。

情報を誰かに伝えるときは、真偽を確かめてから責任を持って発信するように心がけましょう。

- ✓ 情報の発信源は誰かを確かめる。
- ✓ いつの時点の情報かを確かめる。
→刻一刻と変わる現場では常に最新の情報が必要です。
- ✓ 複数の報道機関、媒体でも確認する。
→ネットの情報だけではなく、ラジオなど複数の情報源で確認しましょう。



ネット・メールトラブル防止 理解度チェック

● **問題** 復習も兼ねて理解度をチェックしましょう

No.	問題	回答
Q01	<p>迷惑メールにダマされないための3つの基本にないものを選んでください。</p> <ol style="list-style-type: none"> 1 メールは開かない 2 リンクをタップ（クリック）しない 3 個人情報を入力しない 4 疑わない 	
Q02	<p>いつも利用しているネットショッピングの会社から緊急のメールがきて、IDやパスワードなどの情報の入力を求められた場合の対応で、最も不適切なものを選んでください。</p> <ol style="list-style-type: none"> 1 緊急なのでその通りに入力した 2 本当かどうか、その会社のホームページで確認した 3 本当かどうか、その会社のサポートセンターに確認した 4 消費生活センターに相談した 	
Q03	<p>身に覚えがないのに「あなたがアダルトサイトを閲覧している動画を手したとして、公開回避のための金銭支払いを求めるメール」を受け取った場合の対応として、最も不適切なものを選んでください。</p> <ol style="list-style-type: none"> 1 身に覚えはなくても、本当だったら怖いのですぐに払う 2 消費生活センターに相談した 3 メールは無視して払わない 4 同じようなメールを受信しないように迷惑メールフィルターを設定した 	
Q04	<p>献血をよびかけるチェーンメールを受け取った場合の対応として、最も適切なものを選んでください。</p> <ol style="list-style-type: none"> 1 コメントを付け加えて転送する 2 献血のお願いだったので人助けのために転送する 3 記載された内容が本当か、メールに記載された病院へ確認の連絡をする 4 メールは無視して何も対応しない 	

No.	問題	回答
Q05	<p>迷惑メールにダマされないための対応には、「3つの基本」のほかに、「日頃の備え」があります。日頃の備えに含まれていないものを選んでください。</p> <ol style="list-style-type: none"> 1 迷惑メールフィルターを利用する 2 セキュリティソフトを利用する 3 最新のOSに更新する 4 メールに記載されているサイトにアクセスする場合には、いつもと同じサイトかよく確認してから行う 	
Q06	<p>SMSを受信した場合の対応として最も適切なものを選んでください。</p> <ol style="list-style-type: none"> 1 SMSにサイトへのリンクが設定されていたが、タップ（クリック）しなかった 2 送信者名が普段利用しているサービスだったので、サイトにアクセスした 3 宅配業者からのSMSだったので、指示に従いアクセスした 4 料金未納の連絡だったので、すぐに電話した 	
Q07	<p>インターネットで写真を公開する場合に、最も不適切なものを選んでください。</p> <ol style="list-style-type: none"> 1 スマートフォンカメラアプリの位置情報利用をOFFにして撮影した 2 写真に場所が特定できる情報が写っていないか確認した 3 記念に、校門の前で撮影した入学式の写真を投稿した 4 学校の制服で撮った写真だったので、インターネットへ掲載するのをやめた 	
Q08	<p>SNSを利用する際の注意点として、最も不適切なものを選んでください。</p> <ol style="list-style-type: none"> 1 掲載する内容に個人情報が含まれていないか確認する 2 公開範囲を制限しない設定のまま利用する 3 写真を掲載するとき、自宅周辺は避ける 4 親しい友人や家族であってもログイン情報を共有しない 	

正解と解説は次のページをご覧ください。



ネット・メールトラブル防止 理解度チェック

●正解と解説

No.	正解	解説
Q01	4	いきなりメールが来たら「詐欺かもしれない」と疑うクセをつけましょう。ゼロトラスト①メールを開かない②リンクをタップ（クリック）しない③入力しないの3つ基本をしっかりと覚えてください。p 1～2を参照
Q02	1	緊急性を強調して受信者をあわてさせ、アカウント情報をだましとろうとする手口のフィッシング詐欺メールが送られています。メールで個人情報やアカウント情報の入力を求められたら、詐欺を疑ってください。金融機関や企業などに問い合わせるときは、メールに記載されたアドレスや電話番号ではなく、必ずWebページなどの他の方法で調べて問い合わせをしてください。p 1～16を参照
Q03	1	「ハッキングした」と記載されていることもあります、不特定多数の方あてに一斉送信しているメールと思われる。無視して決して支払ってはいけません。心配な場合は、ひとりで悩まずに消費生活センターなどへ相談してください。p19～22を参照
Q04	4	誰かに転送を促すメールは、チェーンメールです。チェーンメールは、出所も、真偽もわからない情報です。途中で簡単に書き換えることもできます。それは、善意を装うメールであっても変わりません。伝言ゲームのような不確かな情報には反応しないで無視するようにしましょう。また、確認のためメールやメッセージに記載された電話番号へ問い合わせすることもやめてください。相手先の業務を妨害する可能性があります。p25～26を参照

問題	正解	解説
Q05	4	<p>どれだけ注意していても、迷惑メールや詐欺メールにダマされる可能性は残ります。そのため、少しでもそのリスクを抑えておくための日頃の備えもとても重要になります。詐欺メールは本物とニセモノを見分けるのは困難です。企業へ問い合わせをする必要がある場合には、普段使用しているブックマークやアプリからアクセスするか、公式サイトで確認したヘルプデスクへ連絡するようにしましょう。p1～4を参照</p>
Q06	1	<p>SMSは、受信者がメッセージに気づきやすく、自分の電話番号を知っている相手からのメッセージだと思い込みやすいためか有名企業やブランドを装った詐欺メールが増えています。送信者表示の偽装が可能ですから普段利用しているブランド名だからといって安心はできません。SMSを利用した詐欺メールが数多く送信されていることを常に意識しておいてください。SMSに表示されたURLは安易にタップ（クリック）しないようにしましょう。p5～6、9～10を参照</p>
Q07	3	<p>スマートフォンのカメラアプリで位置情報を利用していると撮影した写真に撮影場所の位置情報が記録されます。位置情報を利用したまま自宅で撮った写真を公開した場合には自宅の場所が特定されてしまうおそれがあります。また、撮影した写真に写り込む情報から個人や場所が特定できてしまう可能性もあります。写真をインターネットで公開するときは、事前によく確認するようにしましょう。p45～46を参照</p>
Q08	2	<p>SNSは、元々利用者なら誰でも投稿の閲覧ができて、コメントをつけられるサービスですから、誰でも投稿を見ることができるのが基本です。一方、インターネットには悪意を持った人間が潜んでいますので、プライバシー設定が不十分だと、投稿内容や写真などから個人が特定されてしまう可能性もあります。また、アカウント情報の管理が不十分だとSNSアカウントが乗っ取られてしまう危険すらあります。SNSを楽しく安全に利用するため公開範囲などの設定を見直しましょう。p43～48を参照</p>



トラブル別相談窓口

広告又は宣伝目的のメールのご相談

迷惑メール相談センター (一財)日本データ通信協会	<ul style="list-style-type: none"> ・03-5974-0068 ・平日10:00~12:00、13:00~17:00(年末年始を除く) ・広告・宣伝メールに関する相談
------------------------------	---

消費トラブル、情報通信に関するご相談

電気通信消費者相談センター 総務省	<ul style="list-style-type: none"> ・03-5253-5900 ・平日9:30~12:00、13:00~17:00(年末年始を除く) ・電気通信サービス(電話、電子メール)を利用している際のトラブルなどについての相談
消費者ホットライン 消費者庁・全国消費生活センター	<ul style="list-style-type: none"> ・全国统一番号188(局番なし)(通話料有料) ・IP電話など一部の電話不可 ・架空請求・不当請求などの相談 ・お近くの消費生活センターや消費生活相談窓口を案内
警察相談ダイヤル	<ul style="list-style-type: none"> ・#9110(通話料有料) ・平日8:30~17:15(年末年始を除く) ・(各都道府県警察本部で異なります) ・生活の安全や平穩に関わる困りごとの相談
情報セキュリティ安心相談窓口 (独)情報処理推進機構(IPA)	<ul style="list-style-type: none"> ・03-5978-7509 ・平日10:00~12:00、13:30~17:00(年末年始を除く) ・ウイルスや不正アクセスに関する技術的な相談窓口。メールでの相談も可能。



いじめや誹謗中傷などの人権に関するご相談

常設人権相談所 法務省	<ul style="list-style-type: none"> ・みんなの人権110番0570-003-110 ・子どもの人権110番0120-007-110(通話料無料) ・女性の人権ホットライン0570-070-810 ・いずれも平日8:30~17:15(年末年始を除く) ・IP電話など一部の電話不可 ・差別、いじめ、嫌がらせなど人権に関する相談
24時間子供SOSダイヤル 文部科学省	<ul style="list-style-type: none"> ・0120-0-78310(通話料無料) ・24時間年中無休 ・子供たちが全国どこからでも、夜間・休日を含めて、いじめの相談をすることができるよう、全都道府県及び指定都市教育委員会で実施

携帯電話事業者（フィルタリング設定・操作方法など）

 インフォメーションセンター	<ul style="list-style-type: none"> ・ドコモの携帯電話から 151（無料） ・一般電話などから 0120-800-000（無料） ・9：00～20：00（年中無休）
 総合案内	<ul style="list-style-type: none"> ・auの携帯電話から 157（無料） ・一般電話などから 0077-7-111（無料） ・9：00～20：00（年中無休） ・音声ガイダンスは24時間利用可能
au iPhoneテクニカルサポート iPhone・iPadの操作方法・各種設定方法・サービス全般	<ul style="list-style-type: none"> ・0077-7066（携帯電話・PHS可）（無料） ・上記番号が利用できない場合 0120-345-516（無料） ・平日9：00～19：00土日祝9：00～17：00
 カスタマーサポート	<ul style="list-style-type: none"> ・SoftBankの携帯電話から 157（無料） ・一般電話などから 0800-919-0157（無料） ・10：00～19：00（年中無休） ・自動音声応答サービスは24時間利用可能
スマートフォンテクニカルサポートセンター スマートフォンの操作・サービス内容に関する案内窓口	<ul style="list-style-type: none"> ・SoftBank携帯電話から 151（無料） ・一般電話などから 0800-1700-151（無料） ・平日9：00～19：00土日祝9：00～17：00
 カスタマーサポート	<ul style="list-style-type: none"> ・ワイモバイルの携帯電話から 151（有料） ・一般電話などから 0570-039-151（有料） ・10：00～19：00（年中無休）
 お客さまセンター	<ul style="list-style-type: none"> ・新規のお客様：0120-959-001（無料） ・ご契約中のお客様：0120-929-818（無料） ⇒音声ガイダンスが流れましたら【2：UQ mobile】をお選びください。 ・9：00～19：00（年中無休）
 お問い合わせ窓口	<ul style="list-style-type: none"> ・新規のお客様：0800-805-0090（通話料無料） ・お申し込み後～初期設定でお困りの方：0800-600-0700 ・楽天モバイル（Rakuten最強プラン）をご利用中の方：050-5434-4653（通話料無料） ※Rakuten Linkからの通話は、通話料無料。通話かけ放題オプションサービス加入による対象時間内の通話は、通話料が発生しません。9:00～17:00（年中無休）

迷惑メール相談センターのご案内

●それでも迷惑メールで困ったときは相談窓口へ!

迷惑メール相談センターは、皆さまからの相談を受けてその対策などのアドバイスを行うとともに、皆さまから提供いただいた特定電子メール法違反メールの情報を総務省に報告し、違反送信者に対する措置命令、ISPによる迷惑メールの送信停止措置に役立てるなど、「法違反メールを送信させない、受信しない」環境作りに取り組んでいます。

- **電話番号** 03-5974-0068
- **受付時間** 10:00~12:00、13:00~17:00
(土日祝日/年末年始を除く)

【ご注意】

- ▶ 当センターは「特定電子メール」（広告又は宣伝目的のメール）に関する相談窓口です。他のサービスやトラブルに関するご相談はお受けいたしかねることがあります。
- ▶ 特定電子メールとは、営利を目的とする団体及び営業を営む場合における個人（送信者）が自己又は他人の営業につき広告又は宣伝を行うための手段として送信するメールのことです。
- ▶ メールやFAX・郵送による相談は、承っておりません。
- ▶ 担当職員に対する罵詈雑言等により相談対応の継続が困難と判断した場合や、主張の繰り返し等により電話が長時間に及ぶなど業務に支障が生じていると判断した場合には、その時点で相談対応を終了させて頂くことがあります。予めご了承ください。



● 迷惑メール相談センターサイトのご案内

■ トップページ



迷惑メール相談

検索

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

■ 要注意メール 一覧

フィッシング詐欺と思われるメールを掲載しています（平日は毎日更新）。不審なメールを受け取ったときは、こちらのページも併せてご覧ください。



<https://www.dekyo.or.jp/soudan/contents/news/alert.html>

■ 撃退！詐欺メール&SMS



スマートフォンに届くフィッシング詐欺メールやSMSが急増しています。詐欺の被害にあわないために、だまされないコツ「ゼロトラスト」をご紹介します。

<https://www.dekyo.or.jp/soudan/mb>



最初は **信用しない!**
メールを

ゼロトラスト

3つの基本と日頃の備え

- 基本と備え**
- ① メールを開かない
 - ② リンクをタップしない
 - ③ 個人情報を入力しない
- 備え**
- ① 迷惑メールフィルター
 - ② セキュリティソフト
 - ③ OSは常に最新に



ウーノ



ドゥーエ

ゼロトラスターズ

©2025 Japan Data Communications Association

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)

デ協 一般財団法人 Japan Data Communications Association
日本データ通信協会

迷惑メール相談センター
〒170-8585 東京都豊島区巢鴨2-11-1 ホウライ巢鴨ビル7F

2025年1月 第18版 第1刷 発行

※本書の一部又は全部の転載または複写複製を禁じます。

©2025 Japan Data Communications Association