



## 本物ですか？ そのメール



### ✉ フィッシングとは

実在する企業のwebサイトを装った偽のwebサイトに誘導して、インターネットバンキングの情報やクレジットカード番号、ID・パスワードなどを入力させて盗み取り、本人になりすまして不正な取引を行う犯罪行為です。

金融機関だけでなく、オンラインショッピングサイトや宅配業者を装うケースもあります。

### ☑ フィッシングの例



SMS/MMS  
今日 18:39

【重要なお知らせ】サービスは利用停止される場合がございますので必ずご確認ください。<https://>

SMS

URLをクリックすると



フィッシングサイト

危険！

### ✉ フィッシングの被害を防止するには

- **メールの送信元を信用しない！**
  - ☑ 送信元メールアドレスは二セモノかもしれません
- **メールの内容を信用しない！**
  - ☑ <重要> <緊急> と書かれていても、焦らない
- **メール記載のURLをクリックしない！**
  - ☑ メール記載のURLは簡単に偽装することができます
  - ☑ 公式サイトと同じURLでも、信用してはいけません
- **公式サイト・公式アプリから確認する**
  - ☑ 普段使用するサイトはブックマークしておきましょう
- **企業に電話で確認する**
  - ☑ 身に覚えのない内容であれば、企業のサポート窓口等に電話確認を行きましょう



サイバー犯罪対策課  
イメージキャラクター  
此花 あさひ巡査

# 詐欺サイトに 注意！



## 詐欺サイトによる被害が増えています！

- ・実在する通販サイトに似せたサイト
- ・一見して問題がないショッピングサイトで、「注文して代金を支払ったのに商品が届かない」との相談が増えています！

購入する前に、以下の点をご確認下さい。



## 詐欺サイトの見分け方(抜粋)

### サイトのURLのドメインが不審ではないか？

- ☑ 見覚えの無いドメインの場合は、注意が必要です！警察に寄せられる偽サイトの情報の多くは、「.xyz」「.shop」などのドメインが使われています！

https://○○○.xyz  
ドメイン

### 商品が大幅に値下げされていないか？

- ☑ 全品半額など、極端に値下げされている場合は偽サイトである可能性が高いです。

### 支払い方法が個人名の口座のみ？

- ☑ 支払い方法に注意しましょう！クレジットカード払いには対応せず、支払い方法が銀行振込のみの場合は、偽サイトである可能性が高いです。
- ☑ また、購入後に指定される代金振込口座が個人名の口座である場合もあります。違法に入手した口座が使われている場合があるため、注意が必要です！

### 会社情報に違和感がないか？

- ☑ ショッピングサイトには、「特定商取引法に基づく表記」として、会社名・所在地・代表社名・連絡先・支払い方法等の記載が義務付けられています。表記がないサイトは偽サイトです！
- ☑ また、正規のショッピングサイトに掲載されている会社情報を勝手に転記している偽サイトが増えています。

初めて利用するショッピングサイトは、  
会社情報（会社名・所在地等）をネット検索して下さい！

これらの情報が見つかるかもしれません！

- ・会社名・所在地がでたらめ
- ・正規のショッピングサイトでは販売していない商品を取り扱っている
- ・インターネット上に「偽サイトだ」との書き込みがある

- 偽サイトの可能性があるサイトで商品を購入し、指定口座にお金を振り込んでしまった・クレジットカード番号を入力してしまった場合は、銀行やクレジットカード会社の窓口へ速やかに連絡した上で、最寄りの警察署にご相談下さい。