

## 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<sup>※1</sup>詐欺のメールやSMS(スミッシング<sup>※2</sup>)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

