

【消費生活の窓口から】

実在する組織をかたるフィッシングメールにご注意を！

～URL へのアクセスや個人情報の入力は危険です！！～

通販サイト、クレジットカード会社、フリマサービス運営事業者、携帯電話会社などの実在する組織をかたり、パスワードやアカウント ID、暗証番号、クレジットカード番号などの情報を詐取する（だまし取る）フィッシングの手口が多く発生しています。

〈事例 1〉大手通販サイトからクレジットカード番号を登録し直すようにとのメールが来たので、記載されていた URL を

クリックし名前やカード番号などを入力した。その後、約 1 万 7 千円分のカード利用がされていたことが判明し

た。（80 歳代 男性）

〈事例 2〉大手カード会社から「不正利用の事例が多いので確認するように」とメールが届き、URL をクリックし、カー

ド番号などを入力した。その後、カード会社から「通信販売で不正な利用が確認された」と連絡があった。5 万

円ほどの買い物をされていた。（70 歳代 男性）

【アドバイス】

◆メールに記載された URL には安易にアクセスせず、事業者の正規のホームページでフィッシングに関する情報がないか確認しましょう。

◆日ごろから公式アプリやブックマークした事業者のサイトにアクセスすることを習慣にしましょう。

◆メールの URL にアクセスし、個人の情報を入力してしまうと、クレジットカードや個人情報を不正利用されるおそれがあります。もし、アクセスしてしまっても、個人情報は絶対に入力しないようにしましょう。

◆困ったときは、消費生活相談窓口か消費者ホットライン^{いやや}188（局番なし）に相談しましょう。

※出典：国民生活センターホームページ「[実在する組織をかたるフィッシングメールにご注意！（PDF）](#)」

※ご相談・お問い合わせ先

中山町消費生活相談窓口（住民税務課 住民G内） ☎ 6 6 2 - 2 5 9 3