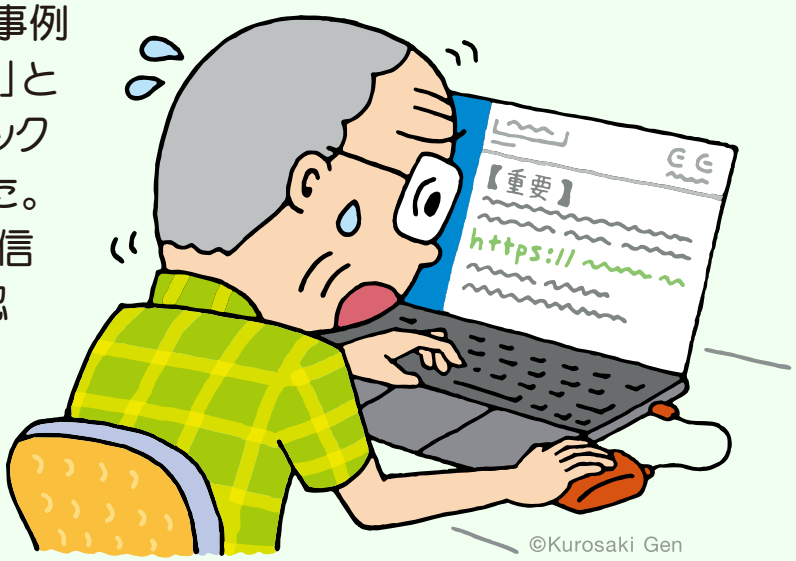
見守り新鮮情報

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）



©Kurosaki Gen

実在する組織をかたる フィッシングメールに注意！

ひとこと助言

- 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フィッシングの手口が多く発生しています。
- 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てはいけません。
- 困ったときは、すぐにお住まいの自治体の**消費生活センター**等にご相談ください（消費者ホットライン 188）。

本文イラスト：黒崎 玄

見守り新鮮情報　第420号（2022年5月24日）発行：独立行政法人国民生活センター