



## 巧妙化するフィッシング詐欺にご注意!

実在するクレジットカード会社や大手通販会社などを装って電子メールなどを送りつけ、偽サイトに誘導し、クレジットカード情報や ID・パスワードなどのアカウント情報・個人情報を盗み取るフィッシングによるトラブルが多発しています。

不正な盗み取りで二段階承認を突破する新たな手口の「リアルタイムフィッシング詐欺」も起こっています。利用者が偽サイトに個人情報を入力すると、犯罪者がその情報を使って正規サイトに本人になりすましてログインします。さらに、正規サイトから利用者へ送信されるワンタイムパスワードも偽サイトを通じて盗み取り、正規サイトで不正利用を行います。この場合、クレジットカードは本人の利用とみなされクレジットカード会社から補填されないため、注意が必要です。

### ■相談事例

「還付金のお知らせ」のメールが送られてきた。記載された URL を開き、メールアドレスなどの個人情報やクレジットカード情報を入力し、SMS で送られてきたワンタイムパスワードも入力した。不審に思いすぐにカード会社に連絡をすると、高額な2件の覚えのない決済があった。

### ■消費者へのアドバイス

- ・ メールや SMS の URL リンクを安易にクリックしないようにしましょう。
- ・ 不審なメールに添付されたファイルは安易に開封しないようにしましょう。
- ・ パスワードはできるだけ長く、複雑なものを設定し、複数のサービスでパスワードを使いまわさないようにしましょう。
- ・ ワンタイムパスワードを入力する際は、偽サイトではないことをよく確認し、不審な場合は認証しないようにしましょう。
- ・ スマートフォンの生体認証（顔認証や指紋認証）で所有者確認を行い、パスワードの代わりにスマートフォンで作成したパスキー「電子署名」を使用するようにしましょう。

千代田区消費生活センター

TEL:03-5211-4314(相談専用)

月曜日～金曜日 9:00～16:30

(土日祝、年末年始除く)

分からないことがあれば、  
消費生活センターに  
ご相談ください。

