スマートフォンやパソコンのトラブルにご注意

事例１　スマートフォンに携帯電話会社を騙り「料金未納」という SMS（※）が届いた。添付の URL をタップすると本物そっくりのフィッシングサイトにつながり、ID、パスワード、クレジットカード情報等を入力してしまった。

事例２　スマートフォンに宅配業者を騙り、「不在なので荷物を持ち帰った」という SMS が届いた。添付の URL をタップすると偽サイトにつながり、誘導されるままアプリをインストールすると、スマートフォンのアドレス帳にある連絡先宛に SMS が勝手に大量に送信された。更にフリーマーケットサービスのアカウントを勝手に作成され不正使用された。

（※）SMS：電話番号を宛先に設定して送受信するショートメッセージサービス

これらは実在する事業者を装う**偽の SMS** です。

○携帯電話会社や宅配会社など利用者が多い企業名を騙る手口が多発しています。**決してメール内の URL をクリックしたり連絡したりせず無視しましょう。**判断に迷うときは事業者の公式サイトなどで真偽を確認してください。

○AppStore や GooglePlayストア以外で配信される提供元不明のアプリには危険なものもあります。公式アプリをインストールするようにしましょう。

○フィッシングサイトに、パスワード、認証コード、クレジットカード情報などを入力してしまった場合は、すぐにクレジットカード会社や携帯電話会社に不正な請求が発生していないか確認し、パスワードを変更してください。

事例３　スマートフォンで無料のアダルト動画を再生しようと年齢確認ボタンを押すと、画面に「登録完了、登録料 40 万円を支払ってください」と表示が出た。解約しようと電話をすると、名前や生年月日を聞かれ「一旦支払えば調査して全額返金する」と言われ、コンビニに行き電子マネーで支払った。

これは典型的な**ワンクリック請求**の手口です。

○ 有料の契約であることが事前にわかりやすく書かれていなければ、契約は成立しておらず、料金を支払う必要はありません。

○ **「退会はこちら」などのボタンがあってもタップせず決して連絡しないようにしましょう。**電話をしてしまうと相手に着信履歴が残ります。知らない電話番号からの電話には出ないでください。メールアドレスを知られてしまった場合は、アドレスを変えるのも対策のひとつです。

事例４　パソコンでインターネットを利用中、突然画面に「警告」「ウイルスに感染」とメッセージが出て警報音が鳴った。慌てて表示された業者連絡先に電話しオペレーターに指示されるままに遠隔操作ソフトをインストールした。サポート代金として 5 万円のプリペイドカードをコンビニで買って番号を連絡したが「無効コードだ」などと言われ、繰り返しカードを購入させられて総額 30 万円を支払った。

これは偽のセキュリティ警告です。

○実際には異常がないにもかかわらず、パソコンにトラブルが起きているかのような表示をして不安をあおります。

○電子マネーを購入させて、そのコード番号を連絡させるのは、典型的な詐欺の手口です。絶対に応じないでください。

○遠隔操作中にインターネットバンキングの画面を開かせ、振込に誘導する事例もあります。

スマートフォンやパソコンで被害が発生し、**不安があれば早急に消費生活センターに相談してください。**

下記のホームページも参考になります。

独立行政法人　情報処理推進機構（IPA） →

https://www.ipa.go.jp/security/anshin

契約している携帯電話会社やプロバイダ、パソコンメーカーに相談してもよいでしょう。