

# スマホを安心安全に使うために

急速に普及しているスマートフォンですが、従来の携帯電話とは様々な点が異なり、インターネットを利用するパソコンと同等の機能を備えていると言えます。情報セキュリティ対策を行って使わないと、思わぬトラブルに巻き込まれることもあります。利用の際は、しっかりと対策を行きましょう。

## ■インターネットとアプリが特長

スマートフォンは、携帯電話よりも大きな画面でインターネットコンテンツをスムーズに操作できたり、便利なアプリケーション（「アプリ」。地図検索、ショッピング、画像編集、ゲームなど、利用者が作業の目的に応じて使うソフトウェアのこと）を自由にインストールしたり、多彩な機能を自分が使いやすいように設定して利用できる点が人気を呼んでいます。

しかし、その反面、その中にはコンピューターウイルス（不正アプリ）が混じっている場合や、パソコン同様にフィッシングサイトへの誘導などの危険性もあります。

## ■架空請求や電話帳データを抜き取られる被害も

スマートフォンは、パソコンと同じようにウイルスに感染することがあります。しかし、利用者の中には、今までの携帯電話を単に買い換えただけという感覚の方もいて、スマートフォンの情報セキュリティ対策を十分に取っていない方も多いのではないのでしょうか。

近年、スマートフォンを狙った架空請求詐欺や個人情報を不正に収集するアプリなどによる様々な被害が発生しています。



### 事例 1：架空料金請求例

動画を再生するアプリを装ったもので、インストールの指示に従って操作すると、架空の利用料金の請求画面を繰り返し表示させるウイルスを含むアプリが確認されています。いわゆる「ワンクリック詐欺」を行うアプリです。

このアプリは、アダルト動画サイト上で公開されており、インストールすると、そのスマートフォンから、利用者の電話番号やメールアドレスといった個人情報を抜き取って、請求画面に表示する機能を備えていました。

### 事例 2：個人情報不正収集例

電話帳情報を外部に送信するアプリが確認されています。これは人気ゲームを動画で紹介するアプリで、公式の提供サイトで無料配布されていました。インストールする際に、「連絡先データの読み込み」などについて、利用者に許諾を求め、「同意する」ボタンを押すことでインストールが実施されます。起動すると、動画が再生されますが、同時にスマートフォン所有者の電話番号とともに電話帳に登録された個人名、電話番号、メールアドレスなどが外部のサーバーに送信されてしまう機能を持っていました。

（このようなアプリによって数百万人の個人情報が流出した可能性があります）

自分自身が被害に遭わないために、また、大事な友人の個人情報を流出させてしまうことのないように、スマートフォンを利用する際には、利用者自身も、普段から情報セキュリティ対策とスマートフォンに蓄積された利用者情報の取り扱いに関する注意が必要です。