トピックス

高校生がスマートフォンを使用するにあたり知っておきたいこと

独立行政法人　情報処理推進機構(IPA)
技術本部　セキュリティセンター　加賀谷　伸一郎

1．スマートフォンの概要

ここ2，3年の間で，利用者が自由にアプリケーションをインストールし，様々な用途に利用できる，「スマートフォン」と呼ばれる携帯端末の普及が進んでいます。

スマートフォンを，主な基本ソフト（OS）で分類すると，以下のようになります。

・Android
・iPhone / iPad
・BlackBerry
・Windows Phone

スマートフォンは，見た目は携帯電話に似ていますが，その中身（機能）はほぼパソコンと同等と言っても過言ではありません。実際は「スマートフォン＝パソコン＋携帯電話（常時インターネット接続）＋システム手帳（アドレス帳や予定表など)」であり，パソコンよりも取扱いに注意すべきものであると言えます。

2．スマートフォンの特徴

従来型の携帯電話と比較しながら，スマートフォンの特徴を解説していきます。

従来型の国内の携帯電話は，機種ごとに異なる仕様となっているほか，アプリケーションのインストールについて利用者の自由度が制限されていたこともあり，セキュリティは強固になっていました。このため，悪意のある者によるウイルスの作成が難しく，またウイルスに感染しにくいという特徴がありました。例えば2004年頃から海外の一部の携帯電話においてウイルス感染の事例が複数ありましたが，それらウイルスの国内の携帯電話への感染事例はごく少数となっています。

一方，スマートフォンは，従来の携帯電話と異なり，全世界的に共通の仕様であることに，注意が必要です。海外でウイルスが発生した場合，日本にいても感染の危険があるということです。このことからも，スマートフォンは，パソコンと同様の脅威にさらされているということを自覚すべきです。

さらにスマートフォンでは，アプリケーションのインストールについても従来と異なり，自由度が高くなっています。さらにアプリケーション開発についても，開発ツールが公開されていることもあり，開発は容易になっています。そのため，パソコンと同様に，ウイルスなど悪意のあるプログラムに狙われやすい状況となっています。

3．スマートフォンのウイルスの脅威

2011年から，スマートフォン，特にAndroid端末を狙ったウイルスが次々と発見されるようになりました。スマートフォンがウイルスに感染してしまった場合に想定される被害例として，以下が考えられます。

・スマートフォン内のアドレス帳，位置情報など，個人情報を含む重要な情報が悪意ある第三者に送られてしまう。
・悪意ある第三者にスマートフォンを乗っ取られて，自由自在に操られてしまう。

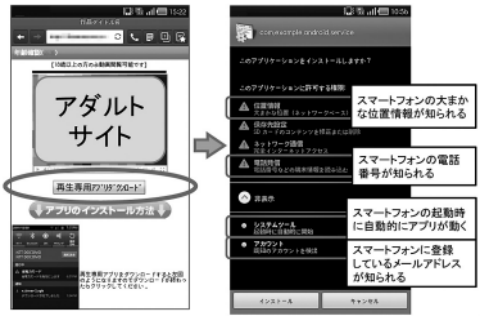
これらの他，パソコンで起こり得るウイルス感

染被害はそのほとんどがスマートフォンにおいても起こる可能性が高いという認識で間違いはありません。

4．ウイルス感染被害の実例

IPAに寄せられる相談で最も多いのは，いわゆる「ワンクリック請求」の被害で，月あたり数百件にのぼります。これは，アダルトサイトで動画を見ようとして画像をクリックしただけで勝手に会員登録され，利用料金請求画面が数分おきに出てきて消えないというものです。感染したウイルスが，料金請求画面を数分おきに出すのです。2012年に入ってから，ウイルスを悪用したワンクリック請求の被害が，パソコンのみならずAndroid端末でも起こるようになっています。

以下に，Android端末でワンクリック請求の被害に遭う様子を紹介します。



検索などでたどり着いた上記左側のサイトで「再生専用アプリのダウンロード」を押すと，アプリのファイルがダウンロードされます。ファイルをタッチすることで上記右側のようにインストール画面に移行します。よく見ると，動画再生アプリとしては不必要と思われる権限を要求されているのが分かります。ここで「インストール」ボタンを押すと，ウイルス入りアプリのインストールが完了してしまいます。

ウイルス感染後は，左下のような料金請求の画面になります。右側の図をよく見ると，自分のスマートフォンの電話番号とメールアドレスが表示されていることが分かります。つまり，業者側に自分の情報が伝わってしまったということになります。

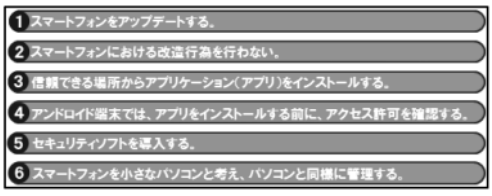
IPAで検証した際には，後日，上記のように料金を督促するSMSが届きました。IPAに寄せられた相談の中には，実際に業者から電話が掛かってきたという事例もありました。

5．スマートフォン利用の注意点

以前からパソコンを使ってきた人であれば，スマートフォンにおける脅威は比較的容易に理解できるのではないかと思います。しかしながら，特に若年層においては，パソコンの利用経験が浅いまま，従来型の携帯電話からスマートフォンに移行する人がほとんどであり，脅威に対して知識も免疫も全くないと言っても過言ではありません。つまり，スマートフォン利用者に対して，脅威についての知識を与え，パソコンと同様の対策を呼びかけることは急務と言えます。

IPAでは，スマートフォン利用者に向けた注意喚起情報を発信するとともに,「スマートフォンを安全に使用するための六箇条」を発表しています。

各項目について以下に詳しく説明します。



(1) スマートフォンをアップデートする。

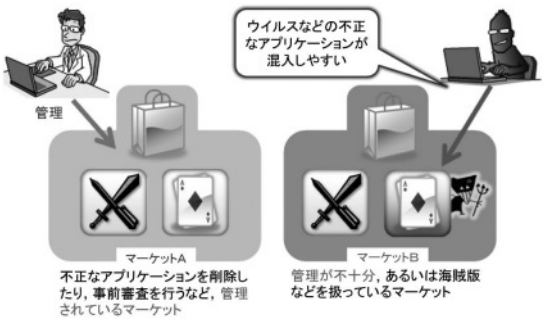
販売元からOSのアップデートが提供された場合，早めにアップデートしましょう。アップデートをしないで使っていると，パソコン同様，脆弱性を悪用した攻撃に遭う危険性が高まります。またその際，アップデート手順をきちんと理解することが重要です。アップデート手順は，販売元や製造元によって異なる場合があります。きちんとアップデートするために，取扱説明書などを確認し，正しい手順を身につけたうえでアップデートを実践しましょう。

(2) スマートフォンにおける改造行為を行わない。

スマートフォンにおける改造行為はやめましょう。ここでの改造行為とは，いわゆるiPhoneにおけるJailbreak（脱獄）やAndroid端末におけるroot権限奪取行為(root化とも呼ばれる)などのことを指します。スマートフォンで動作するウイルスの中には，改造行為を行ったスマートフォンのみに感染するものも確認されています。ウイルス感染の危険性を自ら高めてしまうことになりますので,スマートフォンの改造行為はやめましょう。

(3) 信頼できる場所からアプリケーション（アプリ）をインストールする。

スマートフォンで使用するアプリは，iPhoneであれば米Apple社の「App Store」，Android端末であればアプリの審査や不正アプリの排除を実施している場所（米Google社の「Google Play」）など信頼できる場所からインストールしましょう。



(4) Android端末では，アプリをインストールする前に，アクセス許可を確認する。

Android端末の場合，アプリをインストールする際に表示される「アクセス許可」（アプリがAndroid端末のどの情報／機能にアクセスするか定義したもの）の一覧には必ず目を通しましょう。

過去に発見されたAndroid端末を狙ったウイルスには，個人情報などを不正に盗み取るために，アプリの種類から考えると不自然なアクセス許可をユーザーに求めるものがありました。例えば，単なるゲームアプリにも関わらず，位置情報やアドレス帳の内容へアクセスするための許可を求めるなど，です。

Android端末にアプリをインストールする際に，不自然なアクセス許可や疑問に思うアクセス許可を求められた場合には，そのアプリのインストールを中止しましょう。

(5) セキュリティソフトを導入する。

スマートフォンの中でもAndroid端末では，2011年初頭以降大手ウイルス対策ソフトベンダーが続々とセキュリティソフトを発売し，その選択肢が充実してきました。Android端末では(4)に注意すればウイルスに感染する可能性を低減できますが，ゼロにはできません。ウイルス感染の可能性をより低減するためにセキュリティソフトを導入してください。

(6) スマートフォンを小さなパソコンと考え，パソコンと同様に管理する。

スマートフォンには個人情報やプライベート情報がたくさん詰まっていることを踏まえ，第三者に勝手に見られたり操作されたりしないよう，暗証番号など「端末ロック」を設定することを心掛けましょう。