【第２部　ワークショップ②】

スマホを取り巻く脅威とセキュリティ対策

話題提供者

加賀谷　伸一郎

独立行政法人　情報処理推進機構 IPA セキュリティ調査役

司会

成　田　秀　樹

社会安全・警察学研究所　所員

京都産業大学法学部　教授

はじめに

スマホを取り巻く脅威の一つとして、パソコンを利用したスマホの遠隔操作がある。情報処理推進機構 IPA セキュリティ調査役の加賀谷　伸一郎氏をお迎えし、パソコンのインターネットエクスプローラーを利用し、スマホを遠隔操作する様子をデモンストレイションして頂きながら、問題点と対策について解説頂いた。

（1）不正なアプリをダウンロードしてしまい、遠隔操作される場合

インターネットを使える環境とホームページを見る端末があれば､世界中どこからでもスマホの遠隔操作が可能である。その際に、スマホに不正なアプリをインストールさせることが、スマホの遠隔操作の前提となる。

スマホに不正なアプリをダウンロードしてしまう状況は、パソコンの場合とほとんど同じである。

パソコンでウイルスに感染すると、ID やパスワードを盗まれ、本人の同意を得ずに勝手に買い物をされる等の被害にあう場合がある。スマホの場合も、不正なアプリをダウンロードした場合に、様々な情報を盗み取られることがある。

ただ、パソコンの場合は、サイトを見てクリックしただけでウイルスに感染する場合があるが、スマホの場合は、まず、騙してスマホにアプリをダウンロードさせなければならない。この点が、重要な違いである。

スマホは、パソコンを使えない高齢者や中高生でも利用できるので、ウイルスという概念を知らないままスマホを利用することがあり、この点で被害拡大に結び付きやすい傾向がある。

手口としては、自分のサイトまたは他人のサイトを勝手に改造し、メール等でそこに誘導する等が典型的である。そのメールを受領者の 0.1％しか騙されないが、数億通のメールを発信した場合、相当数が騙されることになる。

（グーグルに似せて造られたサイトから、「時計」のアプリをダウンロードする様子を見せる）

アンドロイドのアプリをダウンロードする場合は、必ず利用者に確認を求めるルールになっている。この不正なアプリの場合、同意を求める画面に、このように、電話番号、写真･動画を送る、電話帳を読み取るとの表示が出ている。「時計」には、このような機能が必要ないので、何も考えずにインストールするのは、危険であることだとわかる。

（アプリを動かす）

この不正アプリに感染すると、すぐ通信を開始し、端末が何処にあるか、緯度、経度情報が、パソコン側に示されている。

遠隔操作をすると、このように、盗聴や盗撮も可能になる。また、コマンドを送って、アドレス帳を盗むことができる。

対策としては、不正なアプリをダウンロードしないようにすることが重要である。

第１に、アプリをダウンロードする際に、同意画面でどのような機能のアプリなのかを確認する必要がある。スマホは、パソコンと異なり、あるサイトをクリックしただけで勝手にアプリがダウンロードされることはない。

第２に、自分で同意画面をチェックするには、一定の知識が必要なので、信頼できるサイト（店）を選んで利用することが大事である。

（2）クラウド

スマホは、データを自分のスマホではなく、インターネット上に保存するクラウドを利用することが多い。スマホは、電池の容量との関係で、パソコンより処理機能を落としているからである。クラウドを利用している場合は、ID とパスワードが判明すれば、他人の ID とパスワードを使用して他人の情報を見ることができる。これは、不正アクセス禁止法違反の行為となる。たとえば、メール、スケジュール、連絡先、位置情報等を ID とパスワードを盗んだ第３者に見られる可能性があり、ストーカー行為に利用されることがある。

これらの様子が、デモンストレイションされた。

（3）対策および質疑応答のまとめ

子どもが被害に会わないようにするためには、親に対策を理解してもらうことは重要である。スマホの特徴として、自分で不正なアプリをダウンロードしなければ、被害に会わない。　子どもを保護するためには、ペアレンタル・コントロールを使って、親がアクセス制限をしたり、子どもがアプリをインストールしようとすると親に承認を求める設定にしたりするのは有効である。

クラウドを利用する場合、ID とパスワードの管理がまず重要である。被害の拡大を予防するためには、特に、パスワードの使い回しを避ける必要がある。

また、ユーザーに落ち度がなく、サービスサイトが攻撃されて、情報が盗られることが実際に起きている。

このような事態を想定すると、まず、ユーザー側が、情報を保存する際に、そこに情報を保存してよいのかを考えることが大事である。情報の重要度は人それぞれ異なるので、その情報が知られた場合何が起こるのかを考えなくてはならない。

サービス提供側が、セキュリティ対策を確実に行うこと、公的機関が、セキュリティ対策の基準を設け、その基準を充足するサービス提供側を公表するシステムを検討することも重要だと思われる。