スマホ時代のセキュリティ

元農林水産省　技術会議事務局
研究計算センター　システム専門官
西　田　信　博

◆略　歴◆
2000年　農水省研究計算センター　システム専門官
2004年　同情報センター　リモートセンシングDB担当

1. はじめに

世界的IT企業の某CEOは、「ユーザーは、自分の個人情報よりも利便性を優先する」と断言して、ひんしゅくを買ったことがあります。街から公衆電話が消え、会話や動画、キャッシュレス決済まで、あらゆることがスマートフォン(以下スマホ)一台で済んでしまう時代になると、ビッグデータと呼ばれるグローバルなデータが、企業の競争力や開発力に直接影響するようになりました。

マーケティングの観点からみても、詳細な個人情報は“宝の山”ですから、それだけにセキュリティに関してはしっかり考え、対策しないと、思わぬ損害や巻き添えを食うことになりかねません。

2. インターネットは危うい？

「製品」というのは、本来完成品で販売されるものです。しかし、IT機器は違います。「バグ(欠陥)は必ずある。だけど今は見つからないから、一応完成品として売ります。欠陥については追々修正します」ということを前提に販売されています。

それがスマホやPCで頻繁に行われるソフトウェアの「アップデート」です。つまり、アップデートをやらずに、そのまま放置するということは、欠陥品のまま製品を使用する、ということになるのです。

製品だけではありません。スマホやPCが接続するインターネットは、本来閉じられた領域で可動するように設計されたネットワークでした。いわば性善説で構築されているため、もともと悪意ある者からの攻撃には脆弱にできています。

もちろん内部からの攻撃にはさらに弱くなります。技術が進んで、様々なセキュリティがソフトもハードも構築されるようにはなりましたが、基本的な部分は変えようがありません。

皆さんはまず、毎日そのような器械を利用しているということを認識してください。

3.「盗まれるものなんてないし～」

古い落語に、長屋の熊さんが、「俺のところなんざ盗まれるものなんてねぇよ～」と油断していたら、泥棒にフンドシを盗まれて困った、なんて話があります。一見つまらないようなものでも、失くしてみると困ることもたくさんあると思います。

ハッカー（侵入者・攻撃者）は、なにもあなた個人を狙っているわけではありません。技術を駆使して、不特定多数の機器にアタックをかけ、セキュリティの甘いところに侵入＝**盗める人から盗もうとしている**のです。

ウイルス付きのメールも、誰かが安易に開けてくれることを狙っています。例えば、「怪しげなサイトを閲覧したら料金を請求された」、「メールを開いたらPCやスマホがロックされて動かなくなり、金銭を要求された」なども、

あなたを個人として狙ったわけではありません。

ですから慌てて個人で対応しないでください。閲覧の料金請求は無視するか、心配ならば、地域の「消費生活センター」に相談しましょう。スマホがロックされたら、メーカーに修理を依頼してください。

4. 自分の情報は自分で管理

利用者は常に、**自分の情報は自分で守る**、という姿勢が一番のセキュリティ対策になります。様々なアプリをインストールする際、「規約に同意」のボタンを押しますが、この規約を最後まで読む人はめったにいません。読まなくてはと分かってはいても、「To be or not to be, that is the question」ですよね。

規約の中には第三者への情報提供を明記してあるものも多々あります。利用者は利便性の代わりに、自分の情報をどこまで提供できるか、いま一度よく考えてみてください。

ネットワークでは大事な原則があります。**一度ネット上に流れた情報は、ほとんど回収・削除は不可能**ということです。

5. 知らないうちに流れ出る情報

本人が知らないうちに流れ出ている情報もあります。その代表的なものが「位置情報」です。位置情報は意外なアプリでも利用されています。例えば、あなたがスマホで撮った写真には、緯度経度の位置情報と時刻が記録されています。

また、「Facebook」などSNSにアップした写真には、あなたが何時何分に世界のどこで写真を撮ったかが記録されています。調べようと思う人は、インターネットを巡るプログラムを利用し、自動的に情報を収集します。「わたしの情報なんか、誰も集めないし」と思うのは油断でしかありません。ですので、**位置情報は必要なときにOnにしましょう**。

フリーのWi-Fiも危ないもののひとつです。感知したWi-Fiへ自動的に接続するように設定していませんか？悪意のある第三者には、罠のフリーWi-Fiを開放している人もいるのです。自動的に接続したら、自動でウイルスをダウンロードさせようとするかもしれません。スマホの設定を見直して、Wi-Fiは必ず接続時に確認画面が出るように設定しておきましょう。

6. IoTと上手に付き合うために

セキュリティの話を始めたら、何時間話しても足りません。そこで最後に家庭でインターネットを利用する際の話をいたします。

近頃、「IoT」という話題がよく流れます。エアコンやテレビ、冷蔵庫などをネットに繋げて制御でき、利便性が高まります。すでに監視カメラなどで利用している人も多いかと思います。そこで一番大切なのは、**家庭用ルーターを購入して、インターネットに接続すること**です。

接続業者が設置していったルーターに直接繋いだり、無線HUBなどに直接接続したりせず、間に家庭用ルーターを挟むことでセキュリティは向上します。ルーターの設定は、素人にはチンプンカンプンですが、今は出荷時に最低限のフィルターが施してあるので安心です。もちろん、管理用パスワードは変更しましょう。ルーターに侵入されたらアウトです。その際、**パスワードは忘れても大丈夫なもの、絶対忘れないものに設定しましょう**。例えば、家族の頭文字の羅列、ペットの誕生日、毎日使っている物に書かれた番号や文字列などに別の数字や文字を少し混ぜて使えば、類推できませんし、忘れないと思います。

7. 最後に

ペット用の監視カメラが、ぐるりと回ってあなたを見ている、なんて悪夢になりませんように。**パスワードの変更と、ソフトウェアの更新**は、常日頃忘れず、手を抜かないように気をつけましょう。

■このコーナーは、つくば市が２００８年度から推進している「つくば市ＯＢ人材活動支援事業」に登録されている研究者・教育者の方々より寄稿を受けて作成しています。現役を一旦引退されてもいつまでも社会発展の牽引力となってご活躍をされている方々の研究実績や業務経験の一端をご紹介させていただくものです。