オーム社 技術総合誌「OHM」2013 年 1 月号　掲載

Android の不正アプリで情報流出が続発

酒井　寿紀（Sakai Toshinori）　酒井 IT ビジネス研究所

不正アプリによる情報流出が続発

2012 年 7 月号の本コラム「プライバシー問題に新時代到来！・・・スマートフォンで」(1)に、Android のスマートフォンはプライバシー侵害のリスクが高いので注意が必要だと記した。その後、下記にように本問題にからんだ事件が続発しているので、再度 Android のどこに問題があり、どう改善すべきかを考えてみよう。

2012 年 10 月 30 日、警視庁は「不正指令電磁的記録に関する罪（通称：ウィルス供用罪、など)」の疑いで 5 人を逮捕した。約 50 種の、一見ゲームのような不正アプリを作成し、Android 用アプリの提供サイトである「グーグル・プレイ」に登録したという。これが延べ約 9 万回ダウンロードされ、スマートフォンの「連絡先」からメールアドレスや電話番号を合計 1,000 万件以上読み取って外部のサーバーに送出したということだ。

11 月 20 日には、京都府警が同じ罪状で 4 人を逮捕した。5 種類の、有益なソフトに見せかけた不正アプリを作成し、それが約 18,000 回ダウンロードされて、連絡先などから約 400 万件のデータが流出したという。

これらの事件の背景には、現在の Android の基本的な問題があるように思う。

根本原因と改善策は？

第 1 の問題は、Android ではどのアプリでも、ユーザーが許可すればオペレーティング・システム(OS)のいろいろな機能を使えるようになっていて、この許可の仕組みに問題があることだ。

今回の不正アプリも、Android の標準機能である、連絡先を読み取る機能とインターネットでデータを送受信する機能を、ユーザーの許可を得て使っている。

個人情報のうちウェブの閲覧履歴などは、行動ターゲティング広告（ユーザーの行動にマッチした広告を掲載することにより広告の効率を上げるもの）の掲載のために、どのアプリでも使う可能性があり、たとえ流出しても被害は限られる。しかし、連絡先はメール、ソーシャル・ネットワークなど、ごく一部のアプリしか要らないはずで、流出したら大問題だ。にも関わらず、現在の許可を取得する画面では、これらは「個人情報」という大項目の下にまとめられているので、問題を見落とす危険性が大きい。

連絡先のように、必要とするアプリが限られていて、かつ犯罪者にとって価値が高いものは、他の個人情報とは別にして、一般のユーザーが判断を誤らないようにすべきだ。

また、連絡先のように危険性が高いファイルについては、ファイル側でもアクセスを許可するアプリを限定して、他のアプリからのアクセスを禁止できるようにすることも考えられる。

第 2 の問題は、グーグルのアプリ配信サイトが無審査で、今回の事件のアプリのように、ちょっと調べればすぐに変だと分かるものが堂々と登録されていることだ。不正アプリか否かの判断をすべてユーザーにゆだねるのは、ユーザー間のレベル差が非常に大きいスマートフォン

では無理がある。

最近は、通信事業者やセキュリティ会社が、アプリの安全性を審査するサービスを提供している例もある。しかし、公害の垂れ流しは元を断つのが最も効率がいいので、最低限の審査はアプリの配信元が行うべきだ。

そして第 3 の問題は、ウィルス対策ソフトによる監視が不十分なことだ。

今回の事件を起こしたアプリのように、OS の標準機能だけを使って不正を働くものは厳密な意味でのウィルスではなく、従来のウィルス対策ソフトの対象外である。もちろん、判明した不正アプリはリストに登録して排除できるが、不正アプリの名前はいくらでも変えられるので、こういう方法だけではいたちごっこが永久に続く。そこで、別の方法での対策が必要になる。

例えば、連絡先などのファイルは、あらかじめユーザーが許可したアプリ以外からのアクセスがあったら警告を発するなどの方法が考えられる。

いずれにしても、現在の Android はセキュリティ面がまだ不完全で、今後改善が必要であろう。

自衛手段は？

では、現状ではどういう自衛手段があるのだろうか？

第 1 に、新しいアプリをインストールするときは、「許可」のリストを調べて、必要がない機能の許可を求めるアプリは使わないことだ。これをきちんと実行していれば、今回の事件の被害者にならないで済んだはずだ。

ただ、アプリ自身では不要なはずの情報の取得を要求するものもあるから注意を要する。例えば、広告を掲載することで無料にしているアプリはインターネット通信の許可を求める。また、行動ターゲティング広告を利用するサイトは、現在地、ウェブ閲覧履歴などの取得も要求することがある。そういう場合、これらの情報の取得を許可するか、それとも拒否して有料ソフトを選ぶかはユーザーの判断だ。

第 2 に、できるだけ名の通ったベンダーのアプリを使い、聞いたこともないベンダーのものは極力避けることだ。また、アプリの紹介サイトでの評判も参考になる。ただし、1 つの紹介サイトが世の中の平均的評価を反映しているとは限らないので、必ず複数サイトを調べる必要がある。

(1) 「プライバシー問題に新時代到来！・・・スマートフォンで」、OHM、2012 年 7 月号、オーム社
(http://www.toskyworld.com/archive/2012/ar1207ohm.htm)