IPA Technical Watch

2011 年 6 月 22 日
独立行政法人情報処理推進機構

IPA テクニカルウォッチ：『スマートフォンへの脅威と対策』に関するレポート

～ IPA 自らの検査に基づくアンドロイド端末における脆弱(ぜいじゃく)性対策の実情と課題の考察 ～

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、スマートフォンのうち「Android（アンドロイド） OS」を搭載したスマートフォン（アンドロイド端末）に対して、IPA 独自でセキュリティ上の弱点（脆弱性）への対策状況を検査し、その結果に基づきアンドロイド端末の脆弱性対策の実情と課題の考察をまとめて、技術レポート（IPA テクニカルウォッチ 第 3 回）として公開しました。

スマートフォンは、従来の携帯電話と異なり、アプリケーションソフトをインストールすることにより、機能の追加や拡張を行える点がパソコンと類似しており、“電話機能付きのパソコン”と表現しても過言ではありません。

米国 Google（グーグル）社が提供する OS（基本ソフト）「アンドロイド」は、オープンソースソフトウェア (*1) の「Linux (*2)」などを基に開発され、世界各国で多数のメーカーに採用されています。スマートフォンのうち、アンドロイド端末の市場占有率は、米 Apple（アップル）社の「iPhone」や米 Research In Motion（RIM）社の「BlackBerry（ブラックベリー）」に比べて高い割合を占めつつあります (*3)。

今回の検査は、昨今、このアンドロイド OS における脆弱性の存在が指摘されていることから、脆弱性対策の実情と課題を把握する必要があると判断したため、IPA 独自で、国内で流通しているアンドロイド端末を入手し対策状況の検査を実施したものです。

検査時期は今年 3 月で、対象機種は、3 月の時点で市販されていたアンドロイド端末 14 機種です。検査は、「ドロイド・ドリーム」というウイルスを構成するプログラムの一部を用いて実施しました。この「ドロイド・ドリーム」は、2010 年 8 月に発覚した脆弱性などを悪用するもので、検査では、このウイルスが悪用の対象とする 2 件の脆弱性への対応状況を確認しました。

3 月の検査時点で、アンドロイド OS 自体は対策済みとなっていましたが、検査の結果、3 月の実験では、これらの脆弱性に対策できていない機種が、14 機種中 11 機種（約 79%）に上りました。間隔をおき、6 月に各機種の対策状況をアンドロイド端末販売元に確認したところ、対策できていない機種は、2 機種残っています（詳細：別紙 1 参照） 。

このように、**脆弱性が発覚してから 10 か月以上経過しても、脆弱性対策できないアンドロイド端末がある**ように、アンドロイド端末はパソコンと比べて (*4) 脆弱性対策に時間を要します。アンドロイド OS 自体に脆弱性のセキュリティパッチ (*5) が提供された場合も、アンドロイド端末のメーカーは機種それぞれにおいて、アンドロイド OS に独自の仕様を加えて搭載しているため、それぞれの機種に対応させ

(*1) 「開発情報（ソースコード）が公開されており、再配布の自由が可能なソフトウェア」を指します。
(*2) パーソナルコンピュータ上で利用される OS の 1 つで、ウェブサーバーや DNS サーバーなどのサーバーOS として広く使われています。
(*3) 2010 年全世界におけるスマートフォンの出荷台数のうち、アンドロイド端末は 22.7%で第 2 位のシェア（第 1 位は Symbian）を占めています（米ガートナーの調査報告）。国内では、57.4%で第 1 位（MM 総研の調査報告）
(*4) ウイルスなどに悪用されるパソコン向け OS「Windows」の脆弱性 CVE-2010-3970 を例にとると、この脆弱性は発覚から 1 か月で修正されています。
(*5) 脆弱性を修正するソースコードの変更箇所や修正を適用するプログラムを指します。ソースコードの変更箇所の場合、この情報を基にソフトウェアのソースコードを変更することで、脆弱性を解消できます。

るまで時間がかかる傾向にあると言えます。

また、アンドロイド OS の基となっているオープンソースソフトウェアにおいて、多数の脆弱性が確認されていますが、アンドロイド端末メーカーが独自の仕様を加えているため、どの脆弱性がアンドロイド端末に影響を及ぼすのか実態を把握しにくく（詳細：別紙 2 参照）、情報もほかのスマートフォンに比べて少ないため、アンドロイド端末メーカーごとの対策を難しくしていると言えます。

アンドロイド OS は、世界的に広く普及していること、オープンソースソフトウェアを基に開発されていること、アプリケーション配布の自由度が高いことから、脆弱性を狙われやすい傾向にあると言えます。アンドロイド端末メーカーが個々に対策の充実、向上を行うのではなく、メーカー全体やセキュリティソフト企業を含めた迅速な情報の共有が不可欠です。国内においては、すでにこのような取り組みが始められつつあり (*6)、IPA としても、これらの課題解決に向けて、今後はスマートフォンに関連する企業・組織などに情報提供や意見交換していく方針です。

なお今後 IPA では、スマートフォンのほかに、脆弱性対策状況の実態把握が難しいと考える組込み機器などに対しても、独自に脆弱性検査などを実施していくことを検討しています。

■ 本件に関するお問い合わせ先
IPA セキュリティセンター　小林／金野／勝海
Tel: 03-5978-7527　Fax: 03-5978-7518　E-mail: vuln-inq@ipa.go.jp
■ 報道関係からのお問い合わせ先
IPA 戦略企画部広報グループ 横山／大海
Tel: 03-5978-7503　Fax: 03-5978-7510　E-mail: pr-inq@ipa.go.jp

(*6) 2011 年 5 月 25 日に日本スマートフォンセキュリティフォーラム（JSSEC）が発足し、IPA もオブザーバーとして参画しています。