IPA Technical Watch

2012年6月13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：『Androidアプリの脆弱性』に関するレポート
## ～簡易チェックリストで脆弱（ぜいじゃく）性を作り込みやすいポイントを確認～

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、IPAに届け出られるAndroidアプリの脆弱性関連情報が2011年後半から増加していることを踏まえ、それらを分析して脆弱性を作り込みやすいポイントをまとめ、技術レポート「IPAテクニカルウォッチ」として公開しました。

近年、Android端末の利用者の増加に伴い、多くのAndroidアプリが提供されるようになりました。そのような状況の中、2011年後半からIPAに届け出られるAndroidアプリの脆弱性関連情報も増加しており、2012年5月末までの累計で42件の届出がありました。届出を分析した結果、その7割超が「アクセス制限の不備」の脆弱性であることがわかりました。

「アクセス制限の不備」の脆弱性は、制限が適切に実施されていないために、非公開または公開を限定すべき情報や機能に対するアクセスを第三者に許してしまう問題です。

Androidアプリにおける「アクセス制限の不備」の脆弱性の原因箇所を分類すると、ファイルアップロードやデータ共有などのAndroidアプリの「機能（コンポーネント）」に対するアクセス制限不備と、Androidアプリが生成する「ファイル」に対するアクセス制限不備の2つに分けられます。どちらもAndroidの仕組みを理解し、適切にアクセス制限の設定をしていれば防ぐことのできる脆弱性ですが、多くの届出があったという事実から、このAndroid特有の設定の内容が開発者に周知できておらず、結果的に、アクセス制限の不備の脆弱性を作り込んでしまっているのではないかとIPAでは推測しました。

本レポートでは、より多くのAndroidアプリ開発者にAndroid特有のアクセス制限の必要性についての理解を促進するために、Androidの仕組みについて説明した上で、届出の多かったAndroidアプリの脆弱性の例を5件紹介しています。

- ファイルのアクセス制限不備の脆弱性
  - （1） SDカードに機微な情報を保存
  - （2） ファイルが不正なアプリからアクセス可能
- 機能（コンポーネント）のアクセス制限不備の脆弱性
  - （1） 不正なアプリに機能を悪用される
  - （2） ファイルが不正なアプリからアクセス可能
- ログ出力に関する情報漏えい
  - （1） 機微な情報をログに出力

また、脆弱性を作り込みやすい7つのポイントを確認できる簡易チェックリストを掲載しています（本レポートP.22参照）。

- Androidアプリが生成するファイルのアクセス制限
  （1） SDカードに保存
  （2） ファイルの生成
- Androidアプリの機能（コンポーネント）のアクセス制限
  （1） ファイルアップロード等の機能の提供
  （2） データ共有機能の提供
- Androidアプリが出力するログの内容
  （1） デバッグログの出力
  （2） アプリの機能呼び出し時のログの出力
- Androidアプリが取得する権限
  （1） 権限の要求

IPAとしては、本レポートがAndroidアプリに作り込みやすい脆弱性の把握と対策方針の参考のために活用され、セキュリティを考慮したAndroidアプリの開発に寄与することを期待します。

■ 本件に関するお問い合わせ先
IPA　技術本部　セキュリティセンター　小林／金野／谷口
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