スマートフォンの企業導入検討ガイド

東京システムハウス株式会社
日本スマートフォンセキュリティ協会（JSSEC）技術部会ネットワーク WG
佐藤　導吉

スマートフォンの企業導入について、検討すべきセキュリティ項目を説明します。

セキュリティを検討するうえで、先に考慮すべき点をあげます。

	考慮すべき点	概要
1	目的	スマートフォンを導入する目的によって、リスクや対策が変わります。例えば、社内メールを利用しない場合は、それに伴うリスクは発生しなくなります。また、業務改善が目的の場合、運用ルールを複雑にしすぎると、使いづらくなり業務改善に繋がらないケースもあります。
2	守るべき情報	何を守らなければならないのかをはっきりさせることにより、無駄な対策を省くことが出来ます。例えば、Web で公開されている製品情報であれば、流出による被害は少ないと考えられます。
3	利用端末	会社支給の端末を利用する場合と、個人利用端末を利用する場合では、リスクや対策が異なります。例えば、個人利用端末であれば、利用するアプリケーションの制限などが行えないケースが多いです。
4	コスト	企業の場合は、スマートフォン導入の最終的な目的は、利益の増加に繋げることです。リスクが小さい脅威に対して、対策に高いコストをかけることは本末転倒になります。リスクの大きさと、対策にかかるコストのバランスが大切です。
5	利便性	脅威から守ることばかりに専念し、機能を制限したり、ガチガチな運用ルールを制定することにより、利便性が損なわれます。使いにくいものは、使われなくなる可能性があります。

ここに挙げている内容については、答えというものはありません。業務内容によって異なったりします。以降では、特に利用シーンに拘らず、より一般的な脅威とリスク、対策について述べます。

セキュリティの対策を行う上で、まずはどのような脅威とリスクがあるのかを把握する必要があります。以下に、スマートフォンを利用する上での主な脅威とリスクを挙げます。

	脅威	リスク
1	盗難、紛失	・ デバイスに保存されている情報の漏洩 ・ イントラネットへのアクセス
2	故障	・ データの消失
3	覗き見	・ 情報の漏洩 ・ パスワードの漏洩
4	誤操作	・ メールの誤送信 ・ 不正サイトアクセスによる情報漏洩
5	脆弱性	・ 脆弱性を突いた不正アプリケーションによる情報情報漏洩
6	不正アプリケーション	・ 不正アプリケーションによる情報漏洩
7	不正サイト	・ 架空請求 ・ パスワードの漏洩
8	利用者の知識不足や悪用	・ OS の改造 ・ 運用ルール外利用による情報の漏洩

各脅威について、主な対策です。

	脅威	対策
1	盗難、紛失	・ データを暗号化する ・ 端末へデータを保存しない ・ 盗難、紛失時にデータの遠隔削除を行う ・ 端末の画面ロックを有効にする
2	故障	・ データを定期的にバックアップする
3	覗き見	・ 覗き見防止シートを装着する ・ 画面ロック用パスワードは、他のパスワードとは異なるものにする
4	誤操作	・ 慎重に操作するよう注意を喚起する
5	脆弱性	・ 使用するデバイスや OS の種類を絞り込む ・ 端末を常に最新の状態にする（バージョンアップは必ず実施する）
6	不正アプリケーション	・ 信頼できるマーケットからアプリケーションを入手する ・ インストール時にアクセス許可を確認する ・ ホワイトリスト、ブラックリストによる制限をかける ・ ウイルス対策ソフトを利用する

7	不正サイト	・ ホワイトリスト、ブラックリストによる制限をかける ・ 不用意にメールやSNSに張られているURLへ接続しない ・ セキュリティ対策ソフトのウェブフィルタリング機能を利用する
8	利用者の知識不足や悪用	・ 運用ルールを設定する ・ 定期的な教育を実施する ・ ルール違反時の罰則を設ける

ここでは、最近話題にあがることが多い不正アプリケーションについて、もう少し詳しく説明していきます。以下では、Android OS について説明いたします。

不正アプリケーションは、日に日に増加傾向にあります。以下は、2012 年 10 月にトレンドマイクロ社から発表された不正アプリケーションの数です。

（出典：トレンドマイクロ社）

2012 年 4 月以降、約半年間で 16 万以上の不正アプリケーションが発見されました。予想を上回るペースで不正アプリケーションが出回っていることがわかります。

数多い不正アプリケーションですが、主に次の 2 つに分類されます。

(1) 不正に情報収集

(2) プレミアムサービスを悪用する

日本においては、プレミアムサービスに該当するものが存在しないため、(2)については考える必要はありません。 (1)について詳しく見ていきます。

2012 年に日本で話題になった不正アプリケーションについて、いくつか紹介していきます。

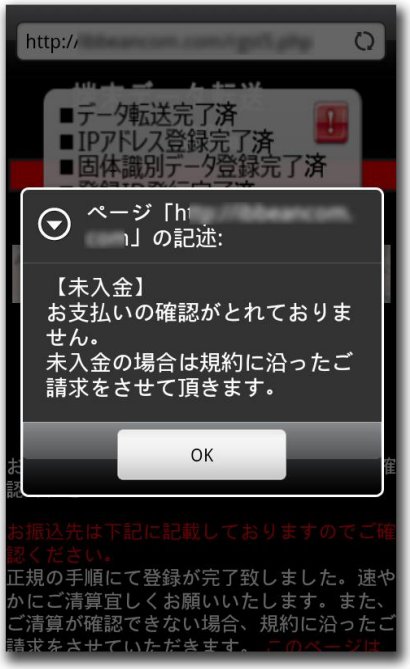
■ 架空請求へ誘導するアプリケーション

2012 年 1 月に確認されたアプリケーションです。

アダルトサイトで動画を閲覧しようとしたときに、アプリケーションのインストールを促されます。インストールしたアプリケーションを起動すると、右図のような振り込め詐欺のサイトへ繋がります。

パソコンの場合と比べ注意が必要な点は、電話番号やメールアドレスが表示されているところです。電話番号やメールアドレスによる繰り返しの請求がある場合は、消費者センターへ連絡してください。

この件では、アダルトサイトからの入手となりましたが、今後は、アダルトサイトに限らず、このようなアプリケーションは増えていくと予想されます。自分はアダルトサイトには接続しないからといって、安心してはいけません。



（出典：トレンドマイクロ社）

■ 電波改善、電池長持ち

2012 年の 8 月に確認されたアプリケーションです。

電波改善、電池長持ちなどの便利ツールを装っている点が特徴です。実際は、電話帳のデータを盗み取り、外部サーバーへ送信するアプリケーションでした。

2012 年当初までは、不正アプリケーションはアダルト系が圧倒的に多かったです。しかし、現在では、このようにアダルト系に限らず、いろいろなアプリケーションが出回っています。

（出典：IPA）

（出典：IPA）

■ わんこアプリ

2012 年の 8 月に確認されたアプリケーションです。

SNS の愛犬家コミュニティのページに投稿されていました。愛犬家の人には思わずインストールしたくなるようなコメントが添えられていることが特徴です。このときに、実際にインストールされたアプリケーションは、電池長持ちアプリでした（先ほどの電話帳を盗み取るアプリケーションです）。

このように、SNS を利用して不正アプリケーションをインストールさせるケースが増えてきています。また、特定のユーザー（この場合は愛犬家）を対象にするケースも合わせて増えています。

■ the Movie

2012 年の 4 月ごろに話題となったアプリケーションです。

「the Movie」の名前が付いた約 30 種類のアプリケーションで、見かけ上は人気アプリケーションの使い方を説明したり、人気コンテンツをまとめて紹介する動画です。一見すると、普通に動画の再生を行っているアプリケーションのように見えますが、裏でこっそりと、利用者の名前と電話番号、電話帳に登録されている人の名前、電話番号、メールア

ドレスを取得し、外部のサイトに送信していました。

このアプリケーションですが、公式マーケット「Google Play」から入手可能でした(*1)。7 万件以上のダウンロードがあった人気のアプリケーションです。

2012 年の 10 月に、このアプリケーションの開発に携わっていた 5 人が逮捕されました。

次に、不正アプリケーションの脅威から守るための対策を挙げていきます。

(1) 不正なアプリケーションをインストールしない
  (1-A) 信頼できないサイトからはダウンロードしない
  (1-B) インストールするときはアクセス許可を確認する
(2) 不正なアプリケーションをインストールしても、被害を受けないようにする
  (2-A) 重要なデータは保存しない
  (2-B) 重要なデータは暗号化して保存する

(1-A) 信頼できないサイトからはダウンロードしない

簡単に出来る対策です。不正なアプリケーションの多くは、海賊版マーケットと呼ばれる非公式なマーケットで配信されています。したがって、アプリケーションをダウンロードする場合は、公式のマーケットである Google Play や、各通信キャリアが提供しているマーケットから入手しましょう。ただし、「the Movie」の件でもわかるとおり、Google Play では、不正なアプリケーションが存在しないというわけではありません。これだけでは防ぎきれないのが現状です。

(1-B) インストールするときはアクセス許可を確認する

アプリケーションをインストールするときは、図のようにアクセス許可が表示されます。このアクセス許可とは、アプリケーションがどのような情報、機能を必要としているものかを示すものです。例えば、アドレス帳など連絡先データを読み取る場合は「個人情報」、外部のサイトに情報を送信する場合は「ネットワーク通信」というアクセス許可が必要になります。このアクセス許可を確認することにより、安全なアプリケーションなのかどうかの判断が出来ます。しかし、上記のアクセス許可があれば、直ちに不正アプリケーションというわけではありません。「安全でない可能性がある」と「危険である」は同じではありません。本当に危険があるのかどうかの判断は難しいものとなります。

このように、完璧に不正アプリケーションをインストールしないようにするのは、至難の業となります。したがって、「(2) 不正なアプリケーションをインストールしても、被害を受けないようにする」必要があります。

(2-A) 重要なデータは保存しない

盗まれてはまずいものを、スマートフォンに保存しないという方法です。重要なファイルは保存しない、アドレス帳にはデータを保存しないなどです。盗まれるものがなければ安全ですね。しかし、それでは便利な機能が多いスマートフォンが、かえって不便なものになってしまいます。ある程度のデータは保存する必要が出てきます。

(2-B) 重要なデータは暗号化して保存する

不正なアプリケーションは、保存されているデータをそのまま外部サイトへ送信しています。したがって、暗号化されたものは暗号化されたまま送信されます(*2)。これにより情報を入手した側は、解読しなければ、どんな情報かがわからなくなります。この解読に何十年とかかるようなものであれば、それは安全といっていいものです。それに、わざわざ解読してまでデータを入手したいと考える人は少ないです。

参考までに、暗号化アプリケーションとして K2filemanager Enterprise Edition をご参照ください。データを自動で暗号化することで、不正アプリケーションからも大切なデータを守ります。簡易トライアル版では自動暗号化機能を無料で体験していただけますので、ぜひお試しください。

(*1)現在は、Google Play から削除されています。
(*2)Android に標準で搭載されている暗号化機能の場合は、復号されて送信されます。これは、システム側で自動的に復号してしまうためです。

参考サイト

1．Android の不正アプリが累計 17 万 5 千種に 全世界で最も検出数が多かった不正プログラムは「ZACCESS」
（トレンドマイクロ株式会社）
http://jp.trendmicro.com/jp/about/news/pr/article/20121022005943.html

2．スマホを狙ったワンクリックウェアを確認。執拗に請求画面を表示し、電話番号の流出も
（トレンドマイクロ株式会社）
http://blog.trendmicro.co.jp/archives/4714

3．コンピュータウイルス・不正アクセスの届出状況[8 月分]について
（IPA 独立行政法人 情報処理推奨機構）
http://www.ipa.go.jp/security/txt/2012/09outline.html