Information-technology
Promotion
Agency, Japan

第 13-16-284 号
2013 年 3 月 1 日
独立行政法人情報処理推進機構

今月の呼びかけ

「 公式マーケット上の不正なアプリに注意！ 」
～　不正なアプリをインストールしないために　～

2012 年 4 月、スマートフォン（Android OS）アプリの公式マーケットである Google Play から、端末情報や電話帳の中身を外部サーバーに送信するなど、不審な動きをする不正なアプリが多数発見され問題となりました。そのほとんどが「（商標などを含む単語） the Movie」という名称のもので、当時 7 万回以上ダウンロードされていました。

このたび IPA では、同じ Android OS 向けの公式マーケットから、50 万回以上もダウンロードされていた不正なアプリを発見しました。その不正なアプリには、個人的嗜好をくすぐるようなアイコンやキーワードが含まれていました。この不正なアプリを実行することで、スマートフォン内の位置情報やメールアドレスなどの情報が外部に送信されてしまうことを確認しています。流出した情報が必ずしも悪用されるとは限りませんが、当然、悪質な行為に利用される危険性はありますので、インストールするべきではありません。

IPA は、Google Play から「ポルノセクシーなモデルの壁紙」という不正なアプリを入手し、解析しました。なお、これはかつて Google Play で無料公開されていましたが、現在は削除されています。

ここでは、50 万回以上もダウンロードされたこのアプリの手口と動作を明らかにし、被害にあわないための対策を解説します。

（1） 不正なアプリをインストールさせる手口

Google Play におけるアプリの紹介画面では、各アプリの「評価」と「レビュー数」も同時に表示されます。IPA で確認した時は、この不正なアプリの評価が 5.0 満点中 4.4、レビュー数が 7,830 と比較的良い評価で、さらにダウンロード数が 50 万を超えていました（図 1 参照）。その評価とダウンロード数に安心してインストールしてしまった利用者が多いと思われます。また、アプリのアイコンが、個人的嗜好をくすぐるものであったことも、ダウンロード数が伸びた一因と考えられます。

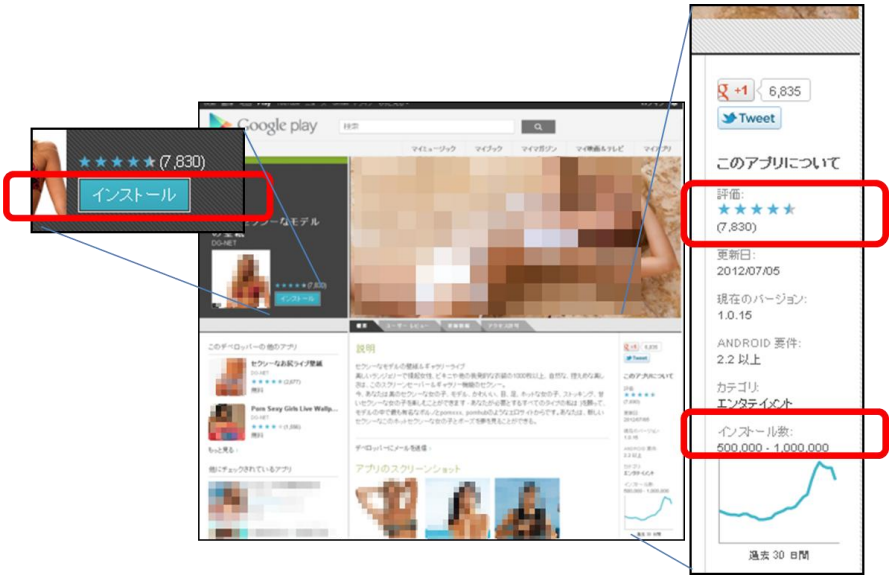

図 1：Google Play に表示されていた評価とレビュー数

※　一部画像処理を施しています。

（2） 不正なアプリの動作

① 図１の「インストール」をタッチすると、インストール前の確認として、当該アプリが要求するアクセス権限※が表示され、インストール開始の有無を聞いてきます（図２参照）。**<u>ここで注意しなければならないことは、このアプリは Wallpaper（壁紙）を謳っているにもかかわらず、端末情報の読み取りなど、アプリの機能としては不自然な許可などを求めていることです。</u>**

［インストール］をタッチすると、不正なアプリがインストールされてしまいます。

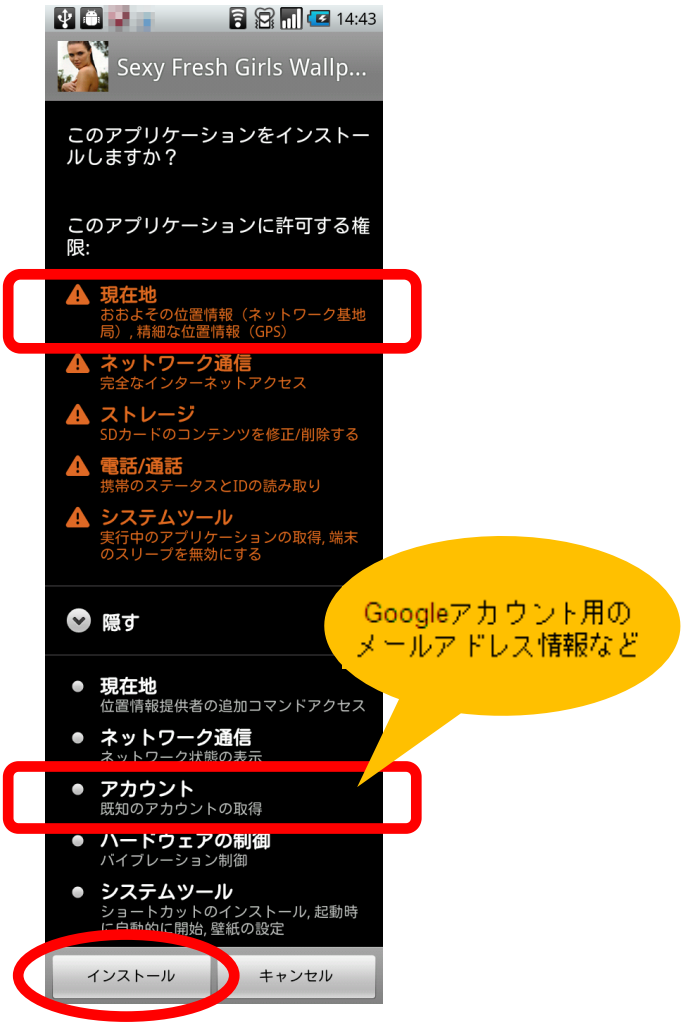

図２：インストール画面（一部加工しています）

※：Google Play から直接インストールする際には、白地の画面となります。

※：アクセス権限の表示内容は、同じアプリでも、端末の機種や Android OS のバージョンによって異なる場合があります。

② インストールが完了すると、アプリを起動するための開くボタンが現れ、またスマートフォンのアプリー覧画面にアイコンが表示されます（図３参照）。開くボタンをタッチするか、このアプリアイコンをタッチするとアプリが起動します。

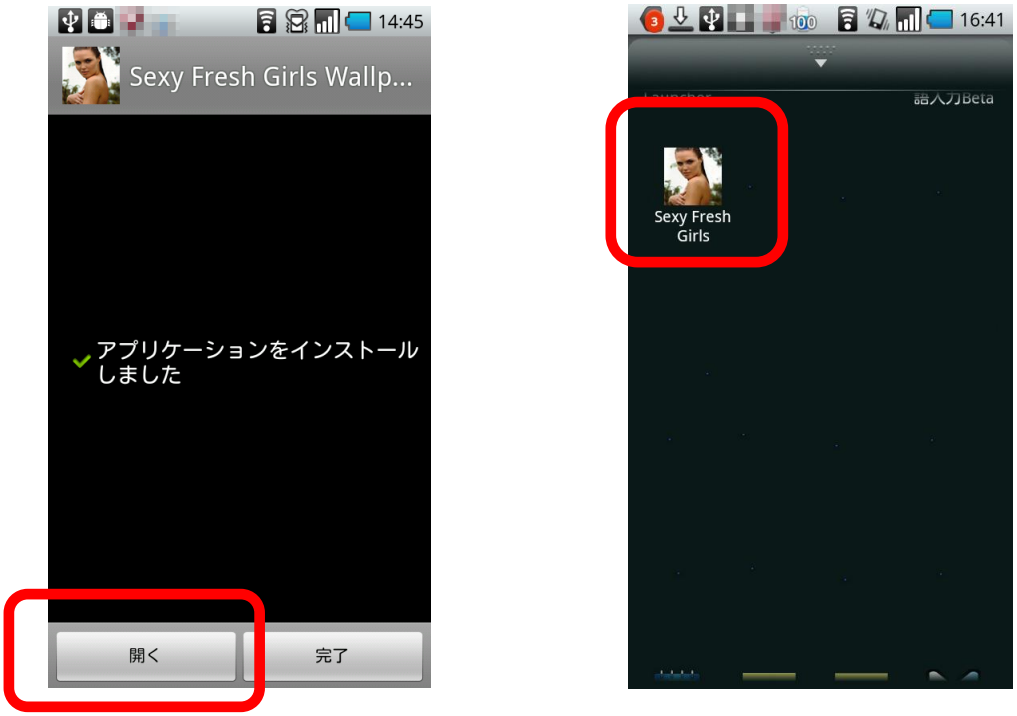

図３：インストール完了とインストールされたアプリのアイコン

③ アプリを起動すると、壁紙が表示されます（図４参照）。
<u>このアプリは、図４のような画面を表示させる裏で、メールアドレスや位置情報などの内容を窃取し、外部のサーバーへ送信します。</u>
その後「Connecting …」という表示とともに外部のサーバーに接続を試みますが、IPA で確認した時には接続に失敗したためか、「Connection error 」というメッセージが複数回表示されました。

図４：壁紙表示画面（接続中を意味するメッセージと、エラーを意味するメッセージ）

※ 一部画像処理を施しています。

不正なアプリが実行されると。図 5 に示すように、メールアドレスや位置情報を外部のサーバーに送信されます。これを見ると、「&」記号を区切りにして、メールアドレス、端末識別番号、位置情報、アプリ名、電気通信事業者識別コード、などの順となっており、これらの情報を POST メソッドという方式で送信していることが分かります。

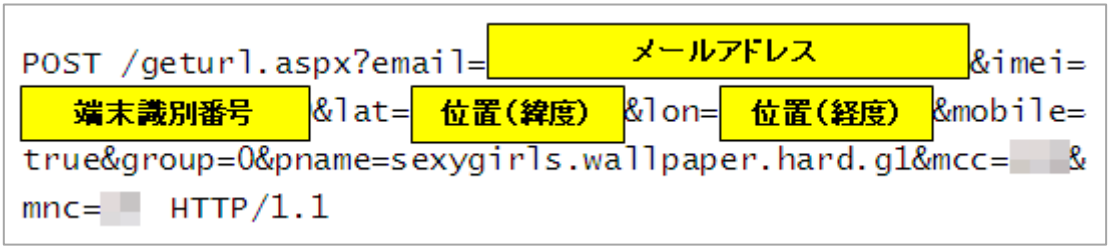

図 5：不正なアプリがプライベートな情報等を外部のサーバーへ送信する際の通信内容

このように、**このアプリは実際に壁紙を表示させる機能はあるものの、実際には端末情報などを窃取するための不正なアプリだと言えます。**2012 年 9 月の「今月の呼びかけ」で取り上げた不正なアプリ「電波改善」は、ユーザーが必要とする実用的な機能を一切持っていなかったのに対し、今回の不正アプリは利用者の目的である壁紙表示という機能を持ち合わせており、不審に思われにくくする効果を狙っているものと推測されます。

このアプリで流出してしまうメールアドレスは、Android OS のスマートフォンを初期設定する際に必要となる Google アカウント用のメールアドレスです。したがって、この Google アカウントに紐づいたメールアドレスを変更する場合、端末の初期化も必要になるため、このメールアドレス宛に大量のスパムメールが来るからといって、メールアドレスを変更することはユーザーにとって容易でないと思われます。

（3）不正なアプリの被害に遭わないための対策

今回解析した不正なアプリは、Android OS 用アプリの公式マーケットサイト「Google Play」に置かれていたことを考えると、現在は「Google Play からアプリをインストールすれば安全」と必ずしも言えない状況です。このような不正なアプリの被害に遭わないためには、以下に示す対策が有効です。

●**Android 端末では、アプリをインストールする前に、アクセス許可を確認する。**

Android 端末の場合、**アプリをインストールする際に表示される「アクセス許可」（アプリが Android 端末のどの情報／機能にアクセスするか定義したもの）の一覧には必ず目を通しましょう（図 6 参照）。**過去発見された Android 端末を狙った不正なアプリには、個人情報などを盗み取るため、アプリの種類から考えると不自然なアクセス許可をユーザーに求めるものがありました。今回解析した不正なアプリも、名前は壁紙アプリを連想させるものですが、壁紙アプリと無関係と思われる「位置情報の読み取り」などの許可を求めていました。Android 端末にアプリをインストールする際に、不自然なアクセス許可や疑問に思うアクセス許可を求められた場合には、そのアプリのインストールを中止しましょう。

図 6：「アクセス許可」の表示画面の例

●**信頼できる公式アプリマーケットからアプリをインストールする。**

スマートフォンで使用するアプリの入手には、可能な限り、各携帯電話会社が運営するマーケットを利用することを勧めます。すなわち、au の「au スマートパス」、docomo の「d マーケット」、EMOBILE の「EMOBILE オススメ！アプリ」、Softbank の「Yahoo! マーケット」などです。これらのマーケットでは、運営者が独自にアプリのチェックを実施しています。

●**セキュリティソフトを導入する。**

スマートフォンにセキュリティソフト（アプリ）を入れ、かつ最新の状態に保っておくことで、このような不正なアプリのインストール時に注意を促してくれたり、インストール済みや過去にダウンロードしたまま放置したファイルからウイルスを検知してくれたりする場合があります。**不正なアプリによる被害の可能性をさらに低減するためにセキュリティソフトを導入してください。**

最近のスマートフォン向けセキュリティソフトには、「アクセス許可」の内容をチェックしてくれるものもあります。

なお、万が一このような不正なアプリをインストールして起動させてしまった場合は、すみやかにアプリをアンインストールしてください。

しかし、今回のようなアプリを**一度でも起動させると、不正アプリによって情報が窃取されてしまいます。そしてそれらの情報は取り戻すことができません。**くれぐれもアプリを安易にインストールしないよう心掛けましょう。

（ご参考）

・IPA Channel　（YouTube）

「大丈夫？あなたのスマートフォンー安心・安全のためのセキュリティー」

http://www.youtube.com/watch?v=AhiUC7X3VSg

・IPA – I Love　スマホ生活

スマホで見る連載マンガ「レイとランのスマホ事情」

http://www.ipa.go.jp/security/keihatsu/love_smartphone_life/comics/

（4）こんなときは…

不正なアプリをインストールしてしまったり、不正なアプリを発見したり、また不正なアプリを紹介するようなメールを受信しましたら、IPA 安心相談窓口までご連絡ください。

まずは、ご相談ください。

	安心相談窓口の問合せ先
電話	03-5978-7509 （オペレータ対応は、平日の 10:00～12:00 および 13:30～17:00）
E-mail	anshin@ipa.go.jp※ （このメールアドレスに特定電子メールを送信しないでください。）
FAX	03-5978-7518
郵送	〒113-6591 東京都文京区本駒込 2-28-8 文京グリーンコート　センターオフィス 16 階 IPA セキュリティセンター「情報セキュリティ安心相談窓口」宛

※：迷惑メール対策などで「メールの受信/拒否設定」が設定されている場合、IPA からのメールを受信できない場合があります。 IPA からの返信メールを受信できるように、「anshin@ipa.go.jp」や「ipa.go.jp ドメイン」からのメールを受信できるように設定をしてください。

■お問い合わせ先
IPA 技術本部セキュリティセンター 加賀谷／青木
Tel:03-5978-7591　Fax:03-5978-7518
E-mail: isec-info@ipa.go.jp