Information-technology
Promotion
Agency, Japan

第 14-09-314 号
2014 年 5 月 1 日
独立行政法人情報処理推進機構

今月の呼びかけ

「 あなたのスマートフォン、のぞかれていませんか？ 」

2014 年 4 月、元交際相手のスマートフォン（Android OS）に無断で紛失・盗難対策用アプリをインストールし、端末内の情報の覗き見や端末を不正操作した容疑で男性が逮捕されたとの報道がありました。

これまで IPA では、スマートフォンにおける不正なアプリについて“今月の呼びかけ[1]”で取り上げるなどして注意を呼び掛けてきました。不正なアプリとは、実際の機能と利用者に説明している機能が異なっているものなどを指します。この事件はそのような**不正なアプリによる被害ではなく、スマートフォンの紛失・盗難対策用アプリの悪用によるものでした。またこのアプリは公開されていました。**不正なアプリであれば、公式マーケットから削除されるなどの対応が行われます。しかし、今回の場合、アプリの機能に問題はなく、使い方に問題がありました。そのため、アプリが公式マーケットから削除されることはなく、今後も同様の被害が発生する可能性があります。

今月の呼びかけでは、本来の目的以外の用途でアプリが悪用されることで発生した今回の事件の概要と、同様の被害に遭わないための対策について説明します。

（１） 紛失・盗難対策用アプリの仕組みと今回の事件の概要

今回の事件では、以前から公式マーケットで公開されていたスマートフォンの紛失・盗難対策用アプリが悪用されました。スマートフォンの紛失・盗難対策用アプリとは、事前にスマートフォンに当該アプリをインストールし設定を行っておくことで、スマートフォンの紛失・盗難時にも、他のパソコンやスマートフォンから当該アプリをインストールしたスマートフォンを遠隔操作できるというものです。遠隔操作では、スマートフォンの位置情報の取得や画面のロック、データの削除などが可能です。

今回の事件では、容疑者は被害者のスマートフォンを遠隔操作できるようこの紛失・盗難対策用のアプリを無断でインストールしておき、スマートフォン内のデータや位置情報といったプライバシーに関

---

[1] 2013 年 3 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　～
http://www.ipa.go.jp/security/txt/2013/03outline.html
2012 年 9 月の呼びかけ「情報を抜き取るスマートフォンアプリに注意！」
～　スマートフォンの中の個人情報が狙われています　～
http://www.ipa.go.jp/security/txt/2012/09outline.html
2012 年 5 月の呼びかけ「あなたを狙うスマホアプリに要注意！」
～不正なアプリをインストールしてしまわないために～
http://www.ipa.go.jp/security/txt/2012/05outline.html
2012 年 2 月の呼びかけ「スマートフォンでもワンクリック請求に注意！」
http://www.ipa.go.jp/security/txt/2012/02outline.html

わる情報を不正に取得していたというものです。被害者は、元交際相手に日常生活を覗き見されていたのです。

以下が紛失・盗難対策用のアプリを使用した際のイメージ図です。

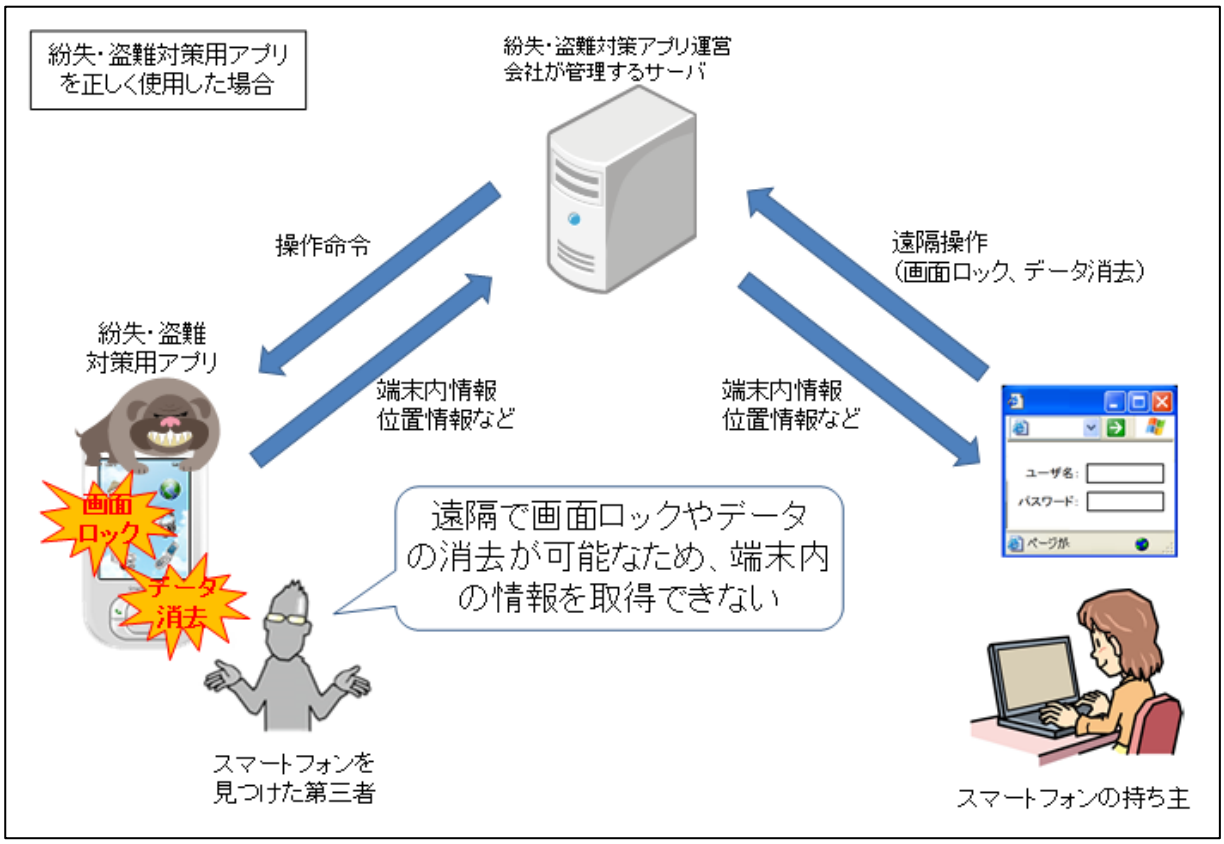

図 1：紛失・盗難対策用アプリを正しく使用した場合のイメージ

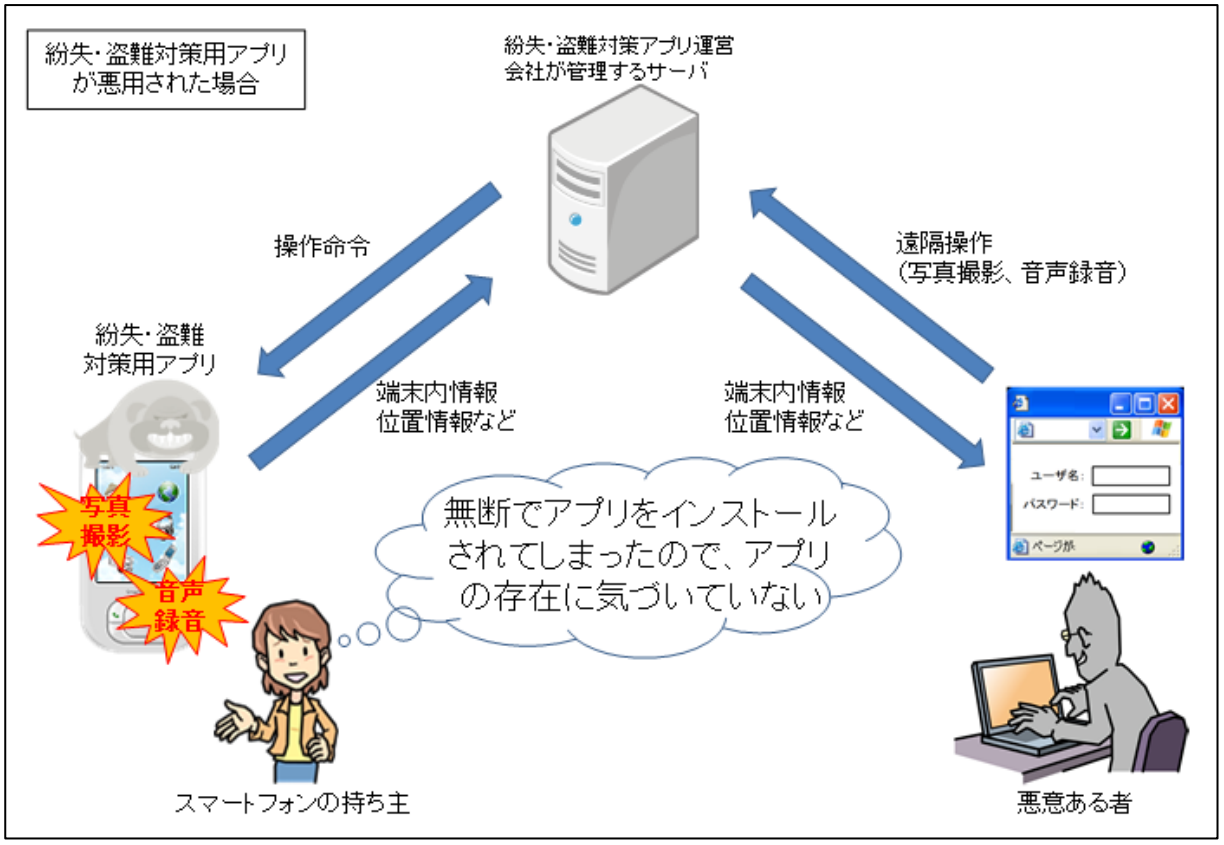

図 2：紛失・盗難対策用アプリが悪用された場合のイメージ

（２） 今回の事件での問題点

【１】 本来は自分がスマートフォンにインストールすることで紛失・盗難対策となるアプリが、他人にインストールされたことで、いわゆるスパイアプリとして悪用されることとなった

今回悪用されたアプリは、本来であれば利用者が自分のスマートフォンにインストールしておき、紛失・盗難時にスマートフォンを探したりするために利用するアプリです。正しく使えば便利なアプリですが、今回の事件では、悪意ある者がこのアプリを無断で他人のスマートフォンにインストールしておき、本来の用途以外に使ったことが問題です。

【２】 他人にスマートフォンを操作させてしまいアプリをインストールさせてしまった

現在のスマートフォンの仕組みでは、アプリが勝手にインストールされることはなく、基本的に必ず人の手によってインストールされるようになっています。つまり、自分のスマートフォンを他人に操作させると、何かしらアプリをインストールされてしまう可能性があります。悪意のある者にスマートフォンを操作されれば、不正アプリなどをインストールされてしまう点が問題です。

【３】 紛失・盗難対策用アプリを悪用されることによりスマートフォンの持ち主は自分の日常生活を監視されることとなった

紛失・盗難対策用アプリの具体的な機能はアプリにより様々ですが、今回悪用されたアプリは位置情報の取得だけではなく、周囲の音声録音や写真撮影ができる機能がありました。そのため、日常生活を監視される被害へと発展してしまったことが問題です。

今回は上記【１】～【３】により、持ち主に無断でスマートフォンに紛失・盗難対策用アプリがインストールされ、本来の目的外に悪用された結果、最終的にプライバシー情報が漏えいすることとなりました。なお、Android OS や iOS の端末では、端末の設定時に登録した Google アカウントや Apple ID を用いることで、設定によっては今回悪用されたアプリと同様の紛失・盗難対策機能が利用できます。その場合、特にアプリなどインストールしなくても、その ID とパスワードさえ分かればパソコンなどからログインすることで、第三者にプライバシー情報などが取得されてしまいますので、注意が必要です。

（３） 対策

【１】 スマートフォンを他人に操作させない

今回の事件では、紛失・盗難対策用アプリが持ち主のスマートフォンに知らないうちにインストールされてしまったことが一番の原因と言えます。スマートフォンは、他人に操作させないようにするのが基本です。もし操作させる場合でも、操作内容を持ち主が確認するなど、注意が重要です。

【２】 スマートフォンには画面ロックをかけておく

実際には、24 時間 365 日スマートフォンを他人に操作させないよう常に注意を払うことは難しいといえます。スマートフォンには画面ロックの機能がありますので、以下の手順を参考にして設定を行ってください。なお、パスワードは複雑なものを設定してください。

■Android 4.2.2 の場合

ホーム画面の「設定」→「セキュリティ」→「画面のロック」→「パスワード」の順にタップします。

図 3：端末ロックの設定方法（Android 4.2.2）

■iOS 7.1.1 の場合

ホーム画面の「設定」→「パスコード（場合によっては、「Touch ID とパスコード」）」→「パスコードをオンにする」の順にタップします。「簡単なパスコード」を「オフ」にすることで、複雑なパスワードを設定することができます。

図 4：端末ロックの設定方法（iOS 7.1.1）

【３】　重要な情報の閲覧時や画面ロック解除の時は周りの目に注意する

スマートフォンを操作している時に画面の表示内容を覗かれてしまえば、アプリを悪用されなくても、情報が漏えいしてしまう可能性があります。また、画面ロック解除のパスワードが知られてしまえば、第三者に勝手に操作されてしまう可能性があります。そのため、入力内容や画面の表示を覗き見されないように特に注意する必要があります。

【４】　他人にアプリをインストールしてもらう際は、何のアプリなのかを事前に確認する

スマートフォンのアプリの中には、今回の事例のようにスパイ行為に悪用できるものもあるということを認識してください。場合によっては、他人にスマートフォンを操作してもらいアプリをインストールしてもらうことがあるかもしれません。その場合は、アプリの機能などを事前に確認しておくことが重要です。

【５】　スマートフォンに登録するアカウントを適切に管理する

スマートフォンに設定したアカウント（Android OS であれば Google アカウント、iOS であれば Apple ID）を使うと、単にアプリのダウンロードだけではなく、設定によっては端末の位置情報や端末内の情報の取得など紛失・盗難対策機能が利用可能です。アカウント情報（ID とパスワード）を他人に悪用されると、自分の行動が筒抜けになってしまいます。パスワードは、推測されにくいものにするとともに、他人に知られることがないように適切に管理してください。

■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／田中
Tel:03-5978-7591　Fax:03-5978-7518
E-mail: isec-info@ipa.go.jp