セキュリティトレンド

スマートフォンアプリケーションを提供する企業が考慮すべき利用者情報の収集と取り扱い

iPhoneの登場を契機に、スマートフォンが世界中で急速に普及している。企業は自社サービスをアプリで提供し、顧客の利便性向上を図るだけではなく、企業イメージ向上やプロモーションにも活用している。金融業界でもアプリ提供が増加しているが、安全性の配慮は万全だろうか。

昨今、様々な企業がスマフォアプリ[1)]を盛んに開発し、一般配布している。金融業界も同様の傾向にあり、自社の金融関連サービスや付加価値を提供するためのアプリ開発が急増している。当社では金融機関から様々な相談を受けているが、スマフォアプリの開発／提供におけるセキュリティ上の問題として質問が多いのが、スマフォアプリ特有の情報収集の問題である。

スマフォアプリ特有の情報収集の問題

従来のブラウザベースで行うサービスでは、利用者が「自ら入力する情報」だけをウェブサイトの管理者は取得できる[2)]。利用者が入力しない限り、メールアドレスや電話番号等の個人情報が収集されることはない。また、企業のウェブサイトでは、収集した個人情報の利用目的を記載した利用規約やプライバシーポリシーに利用者が同意した上で、個人情報を収集するのが常である。

しかしスマフォアプリは、利用者が「情報を入力する」という動作や「利用者の承諾」がない状態で、個人的な情報を収集できる。アプリがインストールされるスマートフォン端末は、電話帳、通話記録、スケジュール、写真、音声等に加え、リアルタイムに取得できる位置情報等も格納された、極めて個人的な情報の塊である。インストールされた後、アプリがこれらの情報にどのようにアクセスするのか、十分な知識なしにアプリを開発・配布すると、たびたびニュースにもなっているように、企業責任を追及される可能性を孕む。例え外部にアプリ開発を委託する場合でも、発注する企業は、適切な対策・配慮がされているか、委託先に常に確認をとる必要がある。

OSごとに異なる情報へのアクセス権の付与プロセス

スマートフォン端末に蓄積された情報へのアクセス権[3)]がアプリに付与されるプロセスには、Android OSとiOSで以下のような違いがある。

- Android OS：アプリのインストール時に、端末内の情報へのアクセス権の付与を利用者に要求する。利用者が承諾すると、アプリはアンインストールされるまで端末内の情報を自由に取得できる。
- iOS：インストールされたアプリには端末内の情報へのアクセス権が平等に付与され、利用者の承諾は不要。位置情報等へのアクセスはその都度、利用者の承諾が必要だが、電話帳等[4)]、承諾が不要な情報もある。

上記の違いは、利用者の視点で見ると、図表のようなメリット／デメリットとして現れる。ここにあるデメリットのとおり、両OSともアプリが端末から収集する情報の「利用目的」を記載する機能を提供しておらず、利用者は何の目的で自分の情報が利用されるのか知ることができない。さらにiOSでは、収集する情報の内容についても知ることができない。この点は、ウェブサイト上でのサービスと大きく異なる。

図表　OSにより異なる利用者のメリット・デメリット

OS	メリット	デメリット
Android OS	・利用者がアプリごとに端末内の情報へのアクセス権を設定できる	・アプリがアクセスする情報の利用目的が記載されていない
iOS	・アプリが端末内の特定の情報にアクセスする際、明示的な承諾を求める機能がOSにより提供されている	・利用者の承諾なしに、アプリが電話帳等の個人情報にアクセスすることができる ・アプリがアクセスする情報やその利用目的が記載されていない

（出所）NRIセキュアテクノロジーズ

NOTE

1) スマフォアプリ：スマートフォンアプリケーション
2) リモートホスト、IPアドレス、ブラウザ・OSのバージョン等は個人情報には繋がらない。
3) 情報へのアクセス権：パーミッション
4) iOS6以降では、電話帳情報にアクセスする際には、利用者の許可が必要になった。
5) NRIセキュアテクノロジーズでは、スマフォアプリの開発・設計における考慮すべきセキュリティ要件の策定を支援する「スマートフォンアプリケーション開発・設計ガイドライン」や、スマフォアプリのセキュリティ対策状況を確認するサービス「スマートフォンアプリケーション診断」を提供しており、情報収集が適切に行われているか、収集した情報は端末内において適切に管理されているかについて確認している。
・スマートフォンアプリケーション開発・設計ガイドライン
http://www.nri-secure.co.jp/service/assessment/guideline.html
・スマートフォンアプリケーション診断
http://www.nri-secure.co.jp/service/assessment/smartphone.html

第三者のモジュールによる情報収集

スマフォアプリでは、第三者が開発／提供しているモジュールを自身が開発するアプリに組み込むことが可能だ。非常に便利ではあるが、そのモジュールがどのような情報を収集するか、利用目的は何かをあらかじめ確認しておくことが必要である。利用者の視点では、モジュール側で行われる情報収集の実態と、アプリの利用規約やプライバシーポリシーに記載されている内容に乖離があった場合、そのアプリが不正な情報収集を行っていると認識するだろう。故に、企業がモジュールを利用する場合、自社アプリと同様に、収集する情報の内容と利用目的、第三者への情報提供の有無等を、アプリ内で個別に表現・実装し、利用者の承諾を得る必要がある。

収集した情報の取り扱い

スマフォアプリで収集した情報は、送信先であるサーバだけではなく、スマフォ端末内においても適切に保護・管理しなければならない。端末内に情報を保存しておく必要性がないならば、むしろ保存しないほうが良い。保存しておく必要があるなら、適切に保護・管理するために、以下のような対策を講じる必要がある。

・収集した情報を公開ディレクトリに保存しない
・収集した情報に対して適切なアクセス制御を行う
・収集した情報を平文ではなく、暗号化して保存する

対策が不十分な場合、収集した情報に端末内の他のアプリがアクセスし、情報が漏洩する危険がある。これが判明すると、そのアプリは脆弱性情報サイトに登録され、半永久的に掲載され続ける。実際、収集した情報を公開ディレクトリに平文で保存していたアプリが脆弱性情報サイトに登録された事例（CVE-2012-2640）も存在する。

企業としての責任：適切な情報収集と取り扱い

スマートフォンは人々の生活に浸透しており、アプリの活用により大きなビジネスチャンスが見込めるが、開発・提供するには慎重にならなければならない。セキュリティ上の脆弱性の有無以外に、情報収集の適切さについても企業責任が求められる。特にセンシティブ情報を扱う金融機関にとっては重要な問題であり、その対処を間違えば、企業の信用を傷つける事態になりかねない。

バージョンの更新頻度が高く、OSごとに特性も違うスマフォアプリの開発には、常に細心の注意が必要である。収集する情報やその利用目的、第三者提供の有無等を明示した利用規約やプライバシーポリシー等を提示した上で利用者の同意を取得すること、収集した情報については第三者からの不正アクセスを防ぐため適切に保護・管理すること、そして何より、情報の収集は適切かつ最低限にすることが必要である。

こうした問題を解決するには設計・開発のガイドラインの策定や、完成したアプリのセキュリティ診断など、常に最新のセキュリティ情報を持つセキュリティ専業ベンダーに委託することも選択肢となるだろう[5)]。

Writer's Profile
藤原 健 Takeshi Fujiwara
NRIセキュアテクノロジーズ　コンサルティング事業本部
セキュリティコンサルタント
専門はサイバーセキュリティ
focus@nri.co.jp