第 14-15-320 号
2014 年 9 月 1 日
独立行政法人情報処理推進機構

今月の呼びかけ

「 非公認のスマートフォンアプリに不用意にアカウント情報を登録していませんか？ 」

2014 年 1 月頃、App Store や Google Play のような公式マーケットで、サービス事業者非公認のスマートフォンアプリが公開され、一部報道などによって騒がれたことがありました。**これらの非公認アプリは、サービス事業者の公式サイトに接続する仕組みを持っており**、非公認とは気付かずに実際にダウンロードしたスマートフォンユーザーもいました。IPA でもサービス事業者の公式サイトに接続する非公認アプリの出現に懸念を抱いていましたが、特に具体的な被害は確認されていませんでした。

ところが、2014 年 8 月、App Store 上でゲームアプリを公開していた作者が、その所有権を、不正に奪われてしまうという事件が発生しました。この事件は**非公認アプリを使用していたため、ID とパスワード情報を悪意ある第三者に窃取された**ことが原因と言われています。

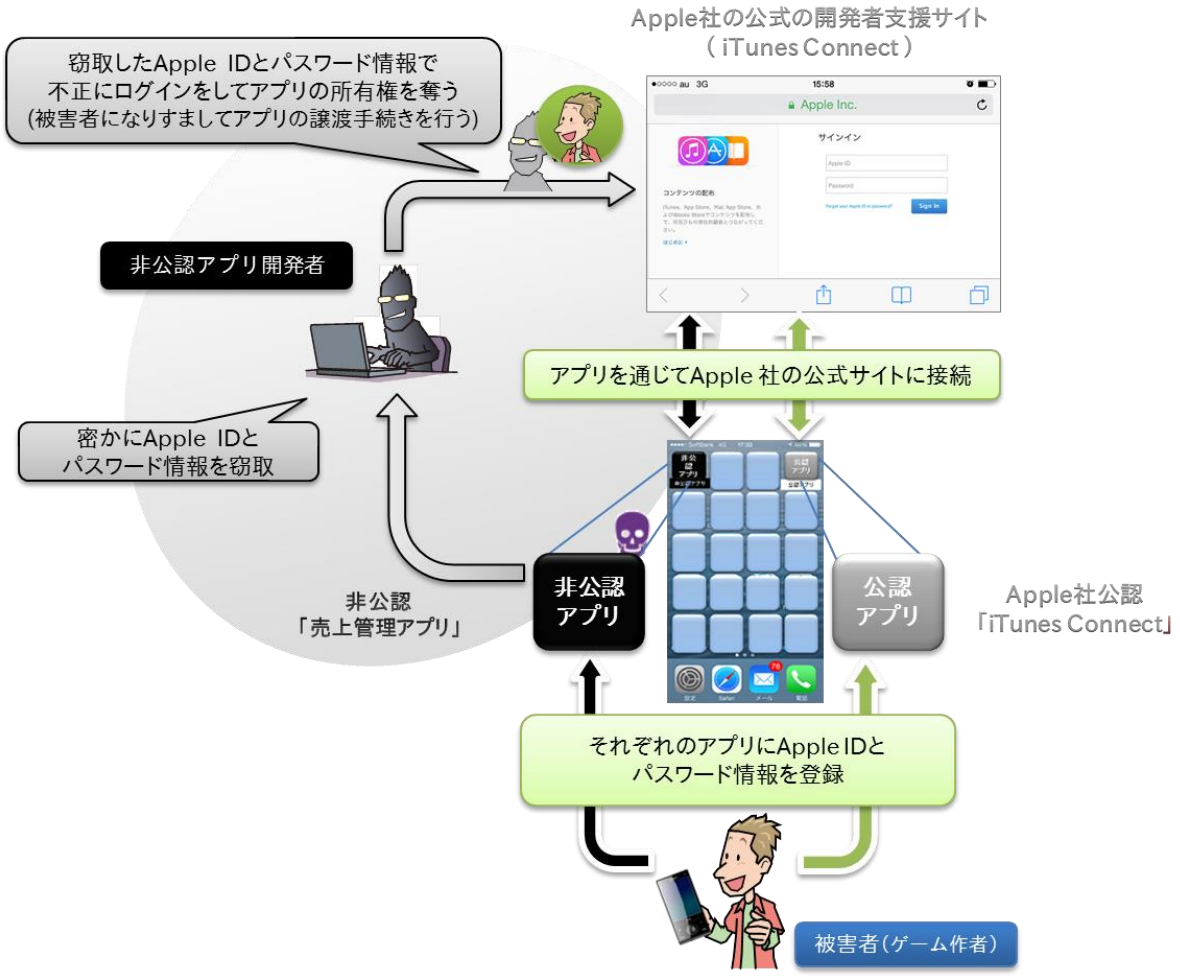

図 1：ゲームアプリの権利が奪われる事件の概要

図 1 のように、被害者であるゲーム作者は Apple 社が提供する開発者支援の公認アプリ「iTunes Connect」に加えて、ゲームアプリの売上管理のために、Apple 社ではない第三者が提供する非公認の売上管理アプリを利用していました。いずれのアプリも Apple 社のサイトに接続するために、Apple ID とパスワードの情報が必要になりますが、非公認アプリに登録した Apple ID とパスワードが第三者に窃取されてしまったと考えられます。

その結果、第三者は非公認アプリを悪用して窃取した Apple ID とパスワード情報を使ってゲーム作者になりすまし、ゲームアプリの所有権を不正に奪った（不正にアプリの譲渡手続きをした）と考えられています。また、被害者はゲームアプリの所有権を奪われたことで、ゲーム内でのアイテム課金による収益を受け取れなくなり、結果的に金銭的被害も受けることになりました。

この事件のように、サービス事業者の公式サイトに接続する非公認アプリの場合、そのアプリに入力した ID とパスワードの情報が窃取されてしまう可能性が否定できないため、注意が必要です。

今月の呼びかけでは、**サービス事業者の公式サイトに接続してサービスを利用するような非公認アプリに ID とパスワードの情報を登録するリスク**と、非公認アプリによる被害を防止するための方法について紹介します。

（1） スマートフォンから企業の公式サイトへアクセスする方法と問題点

スマートフォンから企業の公式サイトにアクセスするには、一般的に図 2 に示す 2 通りの方法があります。アイコンをタップするだけで企業の公式サイトに接続できるため、**スマートフォンの公認アプリは基本的にはブラウザのお気に入り機能の代替であると言えます**。また、アプリによっては ID やパスワードを事前に登録することで都度の入力が不要となるものや、スマートフォンの小さい画面向けに最適化され、見やすくかつ操作しやすいように表示するものもあり便利です。

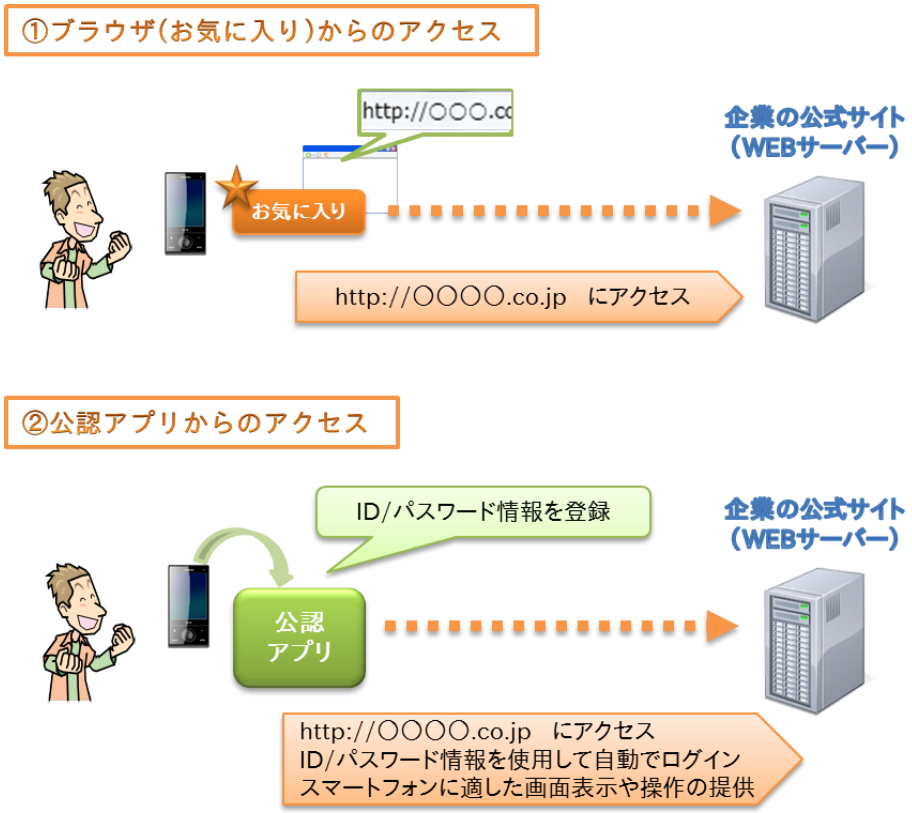

図 2：スマートフォンで企業の公式サイトにアクセスする方法

このように、スマートフォンユーザーにとってアプリは便利な存在ですが、悪意のある第三者が作成した不正な非公認アプリを利用した場合、図 3 のように登録されている ID やパスワードの情報を窃取される可能性があります。また、ブラウザからアクセスした場合、アドレスバーの情報から不正なサイトへの接続に気付くことができますが、**アプリからのアクセスではアドレスバーの表示がなく、不正なサイトに接続されていた場合でも気付くことができず危険です**。

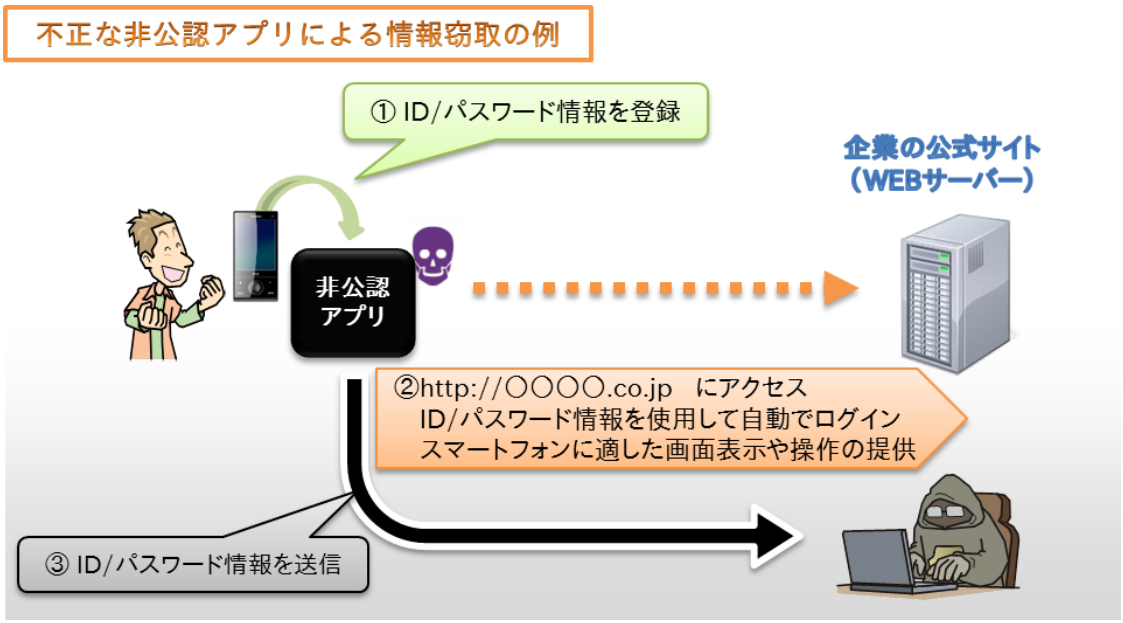

図 3：不正な非公認アプリによる情報窃取の例

ID やパスワードの情報が窃取されてしまうと、本人になりすまして当該企業の公式サイトに不正にログインされてしまい、サイト内で確認できる個人情報やファイル等の流出、ショッピングサイトであれば不正な売買手続きによる金銭的被害といった二次被害に遭う危険性があります。

（２） 被害に遭わないための心がけ

サービスを利用する際に ID やパスワード情報が必要となる場合、基本的にはサービス事業者公認のアプリを利用することを推奨します。なお、すべての非公認アプリが問題というわけではなく、非公認ながらも悪意のない第三者がサービス事業者の公式サイトにアクセスするアプリを作成、提供している場合もありますし、ID やパスワードの情報が不要で利用できる場合もあります。サービスを利用する上で ID やパスワードの情報が不要なアプリは、今回の呼びかけの対象外となります。

利用するアプリが不正なものかどうかを見極めるのは困難ですが、公認アプリについては以下のような方法で判断することができます。

【1】　Google などの検索サイトで、当該サービス事業者名で検索してサービス事業者の公式サイトにアクセスします。
【2】　サービス事業者の公式サイト内のメニューや検索機能または問い合わせ窓口に連絡してアプリの提供有無を確認します。

なお、当該サービス事業者の公式サイトにアクセスする公認アプリが見つからなかった場合は、スマートフォンからパソコンでアクセスする時と同じ URL でアクセスしたり、モバイル専用 URL にアクセスしたりすることで、当該サービス事業者が提供しているサービスを利用することを推奨します。

（３） サービス事業者側に求められること

公認アプリを望まれる人気のサービス事業者ほど、不正な非公認アプリを第三者に作成、公開されやすいという報告※1もあります。自社の不正な非公認アプリの作成、公開を防ぐだけでなく一般利用者を守る意味でも、**スマートフォン向けの会員サイトを提供している、または提供予定のサービス事業者は、自社の公認アプリを用意することを推奨します**。

もし、一般利用者が公認アプリと誤認して不正な非公認アプリを利用した場合、一般利用者の ID やパスワード情報が窃取され、その情報を悪用して自社のサイトが不正ログインの被害に遭うことも考えられます。その結果、自社のサービスやブランドイメージも損なわれ、被害はサービス事業者側にも及ぶ可能性がありますので、公認アプリを用意することは自社のサービス、ブランドを守るための対策とも言えます。

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

[1] SoLoMoLAB：人気の企業ほど狙われやすい!? ピザーラの“偽アプリ”騒動から探る背景と対策とは？
“公式アプリ未公開の国内主要チェーン「企業名+アプリ」の月間検索数(上位 15 社)”
http://solomolab.moduleapps.com/fake_apps_140618/