Information-technology
Promotion
Agency, Japan

第 13-35-302 号
2013 年 11 月 1 日
独立行政法人情報処理推進機構

今月の呼びかけ

「 SNS の友達申請に注意！ 」
～ Facebook で乗っ取り被害に遭わないために ～

近年、“Facebook（フェイスブック）”、“Google+（グーグルプラス）”、“mixi（ミクシィ）”などの SNS や、“Twitter（ツイッター）”などのミニブログサービスが人気です。これらのサービスは、同じ趣味や考えを持つ利用者同士の交流の場として活用できることや、いま現在の自分の行動や考えを簡単に発信できることが特徴となっており、多くの利用者を集めています。

その一方で、これらのサービスが悪意ある者から狙われるようになりました。IPA の安心相談窓口※1にも「第三者に自分の SNS アカウントが不正ログインされ、勝手に投稿された」、「不正ログインされ、自分になりすまして友達申請された」といった相談が続いており、特に Facebook に関する相談が多い状況です（図 1 参照）。実際に、Facebook においてアカウントを乗っ取られたという相談は 2013 年 7 月から 9 月に 4 件寄せられています。

情報セキュリティの一部の専門家の間では、2 年ほど前から、Facebook の偽アカウントを 3 つ用意して乗っ取りに用いる方法が話題となっていました。それに対して、Facebook 社は「信頼できる連絡先」機能※2 で対策を講じていますが、利用者がうっかりしていると、依然として同じような方法で被害に遭う恐れがあります。

そこで今月の呼びかけでは、乗っ取られた場合の被害例とともに、3 つの偽アカウントを用いる仕掛けと、それを防ぐための注意点を解説します。

※1 ：IPA が国民に向けて開設している、コンピューターウイルスや不正アクセスに関する総合的な相談窓口。
URL：http://www.ipa.go.jp/security/anshin/

※2 ：Facebook 特有の方法で、予め 3 つ以上（5 つ以下）の「信頼できる連絡先」登録しておきます。パスワードをリセットしたい時に、その「信頼できる連絡先」から 3 つの情報を揃えると、確かに本人からのリセット申請であると認証される仕組みです。従来、本人確認は本人しか知らないはずの情報で認証するのが一般的でしたが、この仕組みは本人が認めた「信頼できる連絡先」を身元保証人として本人の認証を行う方法です。しかし、この身元保証人も SNS 上の友人関係を前提として行うものである、という点に落とし穴があります。

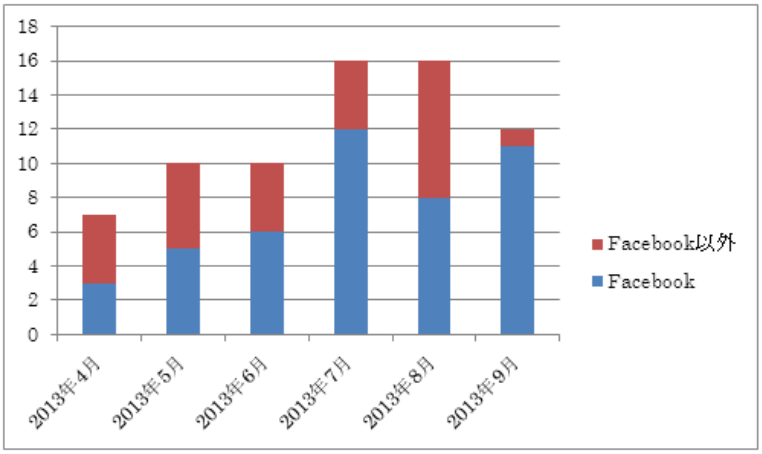

図 1：SNS に関する相談件数の推移（Facebook とそれ以外）

(1) Facebook アカウントを乗っ取られた後の被害の例

Facebook のアカウントが乗っ取られると、どのようなリスクに繋がるのか、例を挙げて示します。
アカウントを乗っ取られると、自分自身だけでなく、Facebook 上の友達にまで被害が及ぶ恐れがあります。

【1】情報を窃取される

乗っ取られたアカウントのプロフィールに設定している居住地・職歴・学歴などの個人情報が盗み見されてしまいます。また友達とのメッセージのやり取りも見られてしまうため、そこから友達に関する情報も盗み見されてしまいます。

【2】勝手に「いいね！」をクリックされて、悪意あるサイトの宣伝や誘導に加担させられる

自分のアカウントが乗っ取られた A さんは、悪意あるサイト上で自分をかたって勝手に「いいね！」※3 をクリックされてしまいます。すると、「いいね！」をクリックしたことが当該アカウントの友達（例えば B さん）に伝わり、B さんは“友達 A さんが勧めている”と思い、クリックしてしまうことで悪意あるサイトに誘導される恐れがあります。

※3 ：Facebook 内の投稿記事や Facebook 外のコンテンツで面白いと思ったものを、Facebook の友達に勧めたい時に「いいね!」をクリックします。

【3】友達のウォール※4 に勝手に投稿されて、悪意あるサイトの宣伝や誘導に加担させられる

悪意ある第三者はアカウントを乗っ取った A さんになりすまし、A さんの友達である B さんのウォールに投稿することができます。その投稿は B さんだけでなく、他の友達も読むことができます。もし悪意あるサイトへのリンクが仕込まれた URL 等をあたかも有益な情報として投稿された場合、そうとは知らずクリックすることで B さんだけでなく B さんの友達も悪意あるサイトに誘導される恐れがあります。

※4 ：Facebook 利用者が各自持っている、自分専用の掲示板のようなものです。自分のウォールには自分だけでなく、友達も投稿できます。

【4】スパムメッセージを勝手に発信させられる

Facebook には、Facebook 利用者が Facebook 上でメッセージをやり取りする機能があります。この機能は、Facebook の任意のアカウントに対してメッセージを送信できるため、電子メールにおける「スパムメール」と同様に、Facebook 上で「スパムメッセージ」を不特定多数に送信することが可能です。

悪意ある第三者が A さんのアカウントを乗っ取ると、A さんになりすましてスパムメッセージを勝手に送信することができ、そのメッセージに悪意あるサイトに誘導させる URL 等を記述すると、それをクリックした受信者が誘導されてしまう恐れがあります。これにより A さん自身の信用が低下する恐れがあります。

(2) 乗っ取り手口の概要

SNS などの多くのサービスでは、利用者がパスワードを失念した場合の策としてパスワードリセット機能が提供されています。Facebook では 2013 年 10 月 31 日現在、次の方法でパスワードをリセットできます。

① Facebook に自身が保有するメールアドレス（Gmail, Hotmail, Yahoo! 等）でログインする
② 自分が「信頼できる連絡先」に登録した友達の助けを借りる

悪意ある第三者は 3 つの偽アカウントを作成し、以下の手順で、これらをあなたの「信頼できる連絡先」に設定させようとします。

【1】偽アカウントを使ってあなたと「友達」関係になる

悪意ある第三者は、3 つのアカウントから、あなたに対して友人申請をします。
あなたが友人として承認します（後述の「注意点その 1」参照）。
その結果 A さんのアカウントは、3 つの各偽アカウントと Facebook 上で「友達」関係になり、次のステップ【2】に移ることが可能になります。

【2】あなたに、偽アカウントを「信頼できる連絡先」に設定させる

あなたがこれらの友人申請を受諾すると、悪意ある第三者は友人となった偽アカウントで、あなたを「信頼できる連絡先」として設定します。すると、あなたの Facebook 画面上で以下の画面（図 2）が表示されます（後述の「注意点その 2」参照）。
その“お返し”として、あなたがそれぞれを「信頼できる連絡先」として設定します。

図 2：Facebook 上の「友達」が、自分を「信頼できる友達」に設定した時の通知

自分のアカウントを、あなたの「信頼できる連絡先」として設定させることに成功した悪意ある第三者は、次に、あなたになり代わってパスワードリセット機能をつかいます。このとき、必要な「信頼できる連絡先」は、悪意ある第三者が自ら 3 つ持っていますので、自在に乗っ取ることができるのです。

(3) SNS 利用時における注意点

(1)で挙げたように、Facebook 利用中に“うっかり”していると、アカウント乗っ取りの被害に遭う恐れがあります。(1)の例では“安易に友達として承認”してしまうことと“安易にその友達を「信頼できる連絡先」として承認”してしまうことが原因となります。

“うっかり”以外にも、“友達申請してくれた相手に配慮する余り、断りづらく承認”してしまう場合や、“友達の数を増やすために相手を選ばず承認”してしまう場合もあります。

他の SNS でも被害に遭わないよう、利用者として以下の点に注意してください。

① 注意点 その 1：安易に「友達」として承認しない

Facebook における「友達」や、Twitter 上で「フォロー」する人が少ないと、サービスを使う魅力が半減するかもしれませんが、確認もせず承認してしまうと悪意ある第三者を簡単に取りこんでしまう恐れがあります。実際に付き合いのある友人から「友達」申請を受け取っても、まず「その人を騙ったアカウントかもしれない」と疑ってください。

“実際に付き合いのある人、“見ず知らずの人”いずれの場合でも、そのアカウントのプロフィールや過去の投稿内容を必ず確認して、本当にその人かどうかを確認してから「友達」申請を承認してください。

② 注意点 その 2：Facebook 上で、「信頼できる連絡先」機能を正しく利用する

Facebook における「信頼できる連絡先」機能で、“お返し”程度の理由で安易に自分の「信頼できる連絡先」に登録してはいけません。事前にあなたの身元を保証でき、普段から連絡がとりやすい人のアカウントを設定しておくことが、被害を防止するために有効な対策です。

③ 友達リストを非公開にする

Facebook では、デフォルトで友達リストが公開状態になっているので、公開範囲を“誰にも公開しない”、“友達にだけ公開する”のどちらかを選択し、参照可能な範囲を限定し、自分で把握するようしてください。

Facebook 以外にも、SNS によっては友達リストを公開する機能がありますが、公開していると、悪意ある者が、友達リストの内容から共通の知人を推測して、その知人を装って「友達」申請してくる可能性があります。

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