Information-technology
Promotion
Agency, Japan

第 12-26-261 号
2012 年 10 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 におけるサービス連携に注意！ 」
～　あなたの名前で勝手に使われてしまいます　～

はじめに

（ご案内）
2012 年 9 月まで毎月公表しておりました「コンピュータウイルス・不正アクセスの届出状況」につきましては、2012 年 10 月より、四半期毎の公表とさせていただくことになりました。2012 年の第 3 四半期分の届出状況公表は、10 月中旬を予定しております。
なお、「今月の呼びかけ」につきましては、従来通り、毎月の公表を予定しております。

最近、インターネット上のサービスである“Twitter（ツイッター）”などのミニブログサービスや、“mixi（ミクシィ）”、“Facebook（フェイスブック）”、“Google+（グーグルプラス）”などの SNS（ソーシャルネットワーキングサービス）が人気です。これらのサービスは、今の自分の行動や考えを簡単にインターネット上に発信できることや、同じ趣味や考えを持つ利用者同士の交流の場として利用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。その反面、悪意ある者からサービス利用者が狙われるようになりました。例えば、「自分では何もしていないのに、Twitter 上で勝手に投稿された」といった相談などが複数寄せられています。Facebook では悪意あるサイトへのリンクを含む投稿が確認されています。

IPA で調査した結果、SNS 間のサービス連携機能を悪用された場合に、こうした被害が発生し得ることを確認しました。ここでは、サービス連携機能とそれを悪用した被害の実例を説明するとともに、解消方法についていくつかの SNS の実際の画面を用いて説明します。

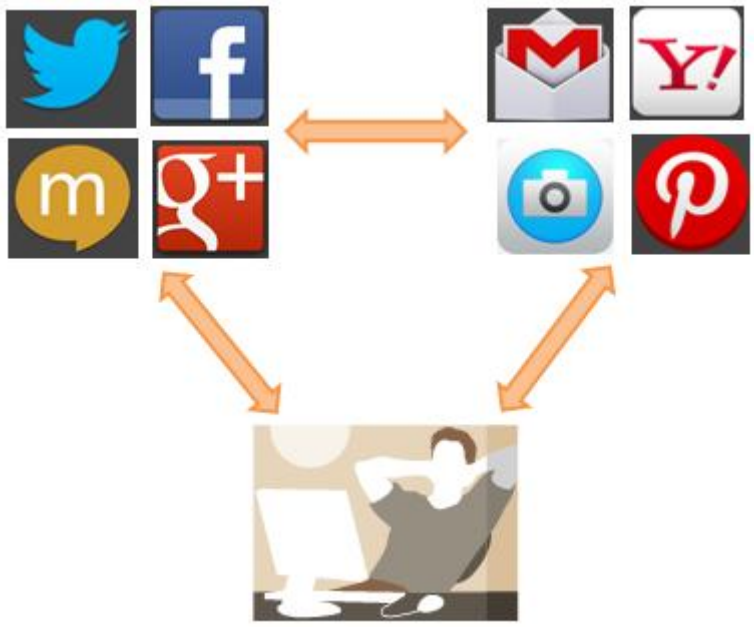

図 1-1：サービス連携のイメージ図

（1） SNS 間のサービス連携例

SNS 間における、典型的なサービス連携の例を示します。

●Twitpic と Twitter の連携

Twitpic によってアップロードした画像を、Twitter のツイートを通じて簡単に共有することができます。

●mixi と Twitter の連携

mixi 上でのつぶやき（mixi ボイス）を、自分の Twitter でのツイートに反映することができます。またその逆も可能です。

●Facebook と Yahoo! Mail の連携

Yahoo! Mail 内のアドレス帳を、Facebook 側が読み取ることを許可することにより、Yahoo! Mail のアドレス帳に含まれる知人に対して Facebook への招待状を送信することができます。

●Facebook と Gmail の連携

Gmail 内のアドレス帳を、Facebook 側が読み取ることを許可することにより、Gmail のアドレス帳に含まれる知人に対して Facebook への招待状を送信することができます。

●Pinterest と Twitter の連携

Pinterest 上で画像をアップロードした時に、画像の URL とメッセージを、自動的に Twitter 上でツイートすることができます。

上記の連携は、画面表示をよく読まずに操作すると、本人が意図しないまま開始してしまうことがあります。**意図しないサービス連携に注意してください**。
連係解除の方法は「(3) 対策」の中で説明します。
例）

・画像共有サービスと Twitter との連携を許可している場合、画像をアップロードすると、その画像が Twitter に自動的にツイートされることになります。
・Facebook とウェブメールサービスとの連携を許可している場合、本人が意図していなくても、ウェブメールサービスのアドレス帳に記載しているメールアドレス宛てに、自動的に招待状メールが送られることになります。

（2） ミニブログサービスの特徴と被害の実例

ここでは、ミニブログサービスの一つである Twitter の特徴と、サービス連携による被害の一例を示します。

▼Twitter の特徴

Twitter では、利用者がそれぞれ思いついた事などを「ツイート（つぶやき、投稿）」しています。Twitter には、他の利用者の「ツイート」を見るための「フォロー」という仕組みがあります。（図 1-2）。例えば、自分の好きな芸能人を「フォロー」しておけば、 その芸能人の動向「ツイート（つぶやき）」を、自分の「タイムライン（「ツイート」の一覧表示機能）」からすばやく知ることができます。

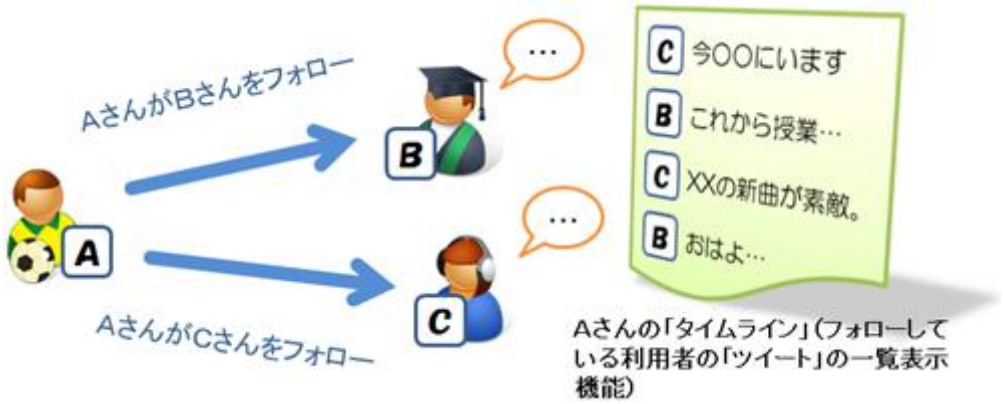

図 1-2：Twitter の仕組みのイメージ図

悪意ある攻撃者は、これらの仕組みを悪用して、利用者を攻撃しようとします。次に、Twitter における具体的な被害の実例を、IPA で検証した結果を踏まえた上で示します。（図 1-3）

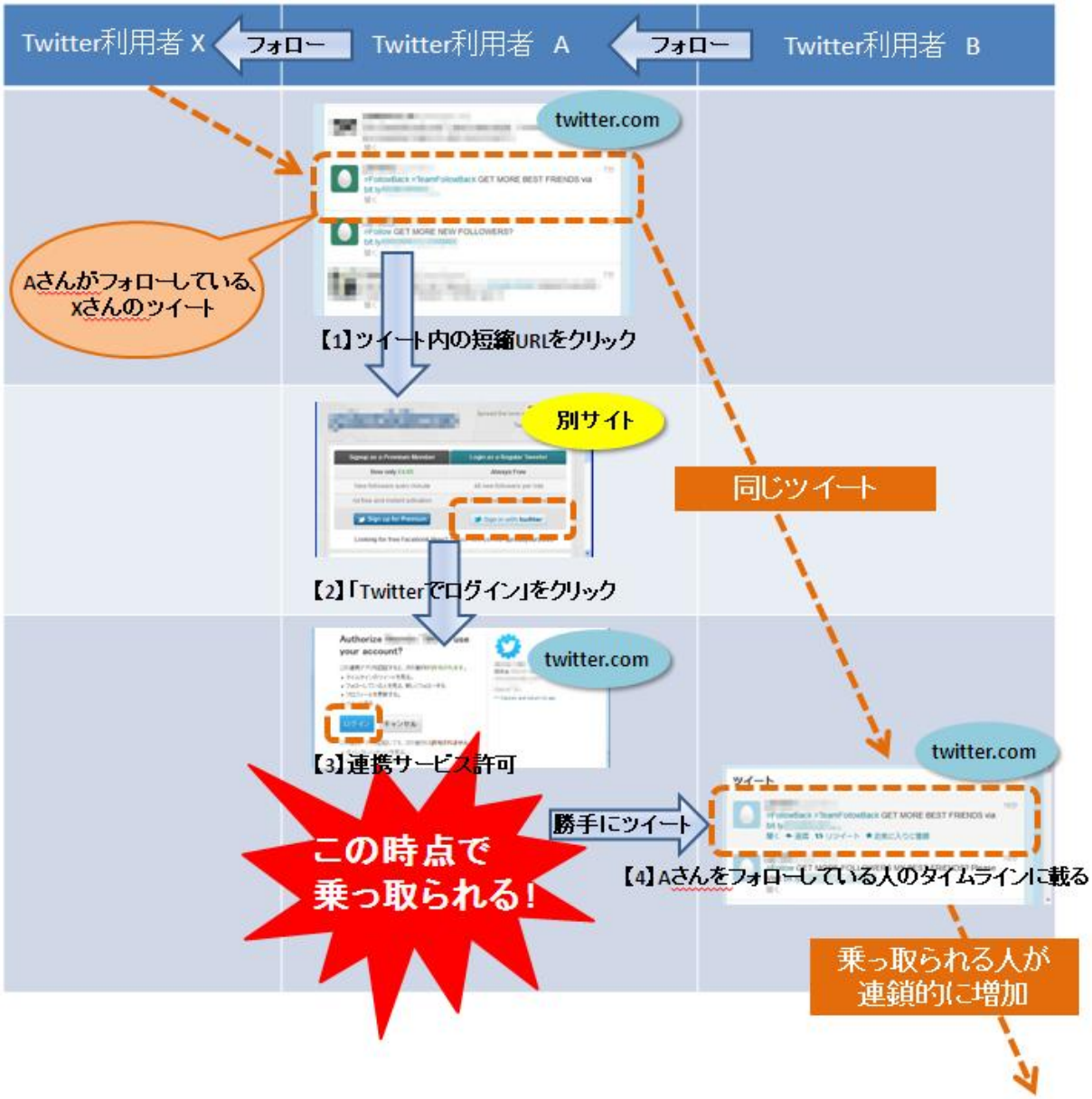

図 1-3：Twitter における被害実例のイメージ図

▼被害の実例（図 1-3 の解説）

【1】A さんが、自分が「フォロー」している X さんの「ツイート」があったことを、A さん自身のツイート一覧画面（タイムライン）で知ります。A さんは、自分が「フォロー」している相

手の「ツイート」なので信用して、その「ツイート」内の URL をクリックします（図 1-3 の【1】）。

【2】URL をクリックすると、新規フォロワー※1 を得られることをうたうようなページが表示されます。ここで「Twitter でログイン」というボタンをクリックします（図 1-3 の【2】）。

【3】「連携サービスを A さんの権限で動作させてもよいか？」という内容のページが表示されます。ここで「ログイン」をクリックしてしまうと、**Twitter の ID とパスワードを入力していないにも関わらず、A さんの権限をその連携サービスに対して許可することになります。つまり、A さんの Twitter アカウントがその連携サービスに乗っ取られた状態になってしまいます**※2。今回 IPA で検証したケースでは、**連携サービスが A さんの代わりに勝手に、**【1】で受け取ったものと同じ内容の「ツイート」をしてしまうことを確認しました（図 1-3 の【3】）。

【4】A さんをフォローしているユーザー（例えば B さん）のツイート一覧画面に、連携サービスが A さんの代わりに勝手に書き込んだ「ツイート」が載ります（図 1-3 の【4】）。

「フォロー」という信頼関係が仇となり、連携サービスに各ユーザーの権限利用を許可してしまうという被害が連鎖式に広がる恐れがあります。

勝手に「ツイート」されるだけであれば、それほど大きな実害ではありませんが、問題は**連携サービスにアカウント利用権限を乗っ取られてしまうという点**です。

一度連携してしまうと、自分で連携を解除しない限り、連携は基本的に継続します。そしてこの罠に騙された利用者がある程度の人数になった時点で、連携サービス側からの悪意ある URL※3 を含むツイートを一斉に行う攻撃による二次被害が発生するという脅威が想定されます（図 1-4）。

※1 フォロワー：Twitter 上で自分を「フォロー」するユーザーのこと。

※2 乗っ取られた状態：実際に行われているのは「認可情報の委譲」で、アカウントの乗っ取りではありませんが、便宜上「乗っ取り」としています。

※3 悪意ある URL：ウイルス配布サイト、フィッシングサイト、など。

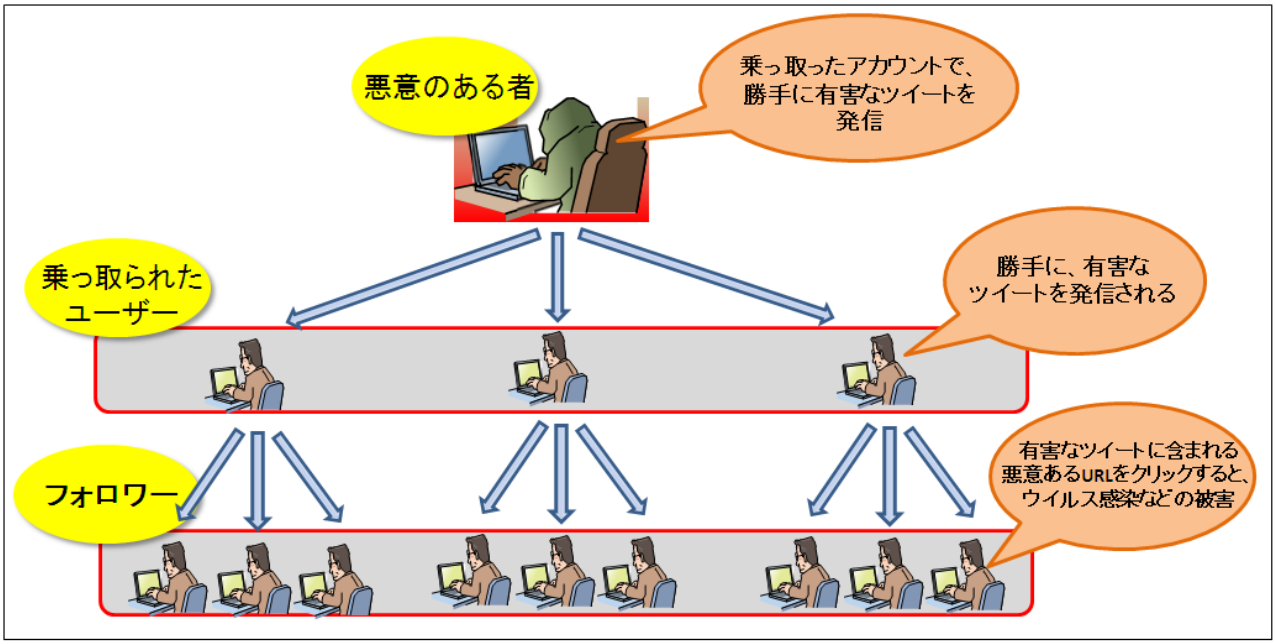

図 1-4：ユーザー乗っ取り後の二次被害のイメージ図

（3）対策

対策１　<u>不要な連携サービスの取り消し</u>

SNS にログインした状態で設定を確認すると、当該 SNS と連携しているサービスやアプリを確認することができます。明らかに不要なものや、身に覚えのないものがあれば削除してください。削除の判断に迷う場合は、各サービスのヘルプをご覧ください。

●Twitter の場合

自分のアカウントで Twitter にログインした後、「設定」→「アプリ連携」で確認することができます。現在連携中のアプリやサービスが表示されますので、不要なものは「許可を取り消す」をクリックして連携を取り消してください。

図 1-5：Twitter における連携サービス表示画面の例（2012 年 9 月 15 日時点）

●Facebook の場合

自分のアカウントで Facebook にログインした後、「ホーム」→「アカウント設定」→「アプリ」で確認することができます。現在連携中のサービスがすべて表示されますので、不要なものは右端の「×」をクリックして連携を取り消してください。

図 1-6：Facebook における連携サービス表示画面の例（2012 年 9 月 15 日時点）

●Yahoo! Japan の場合

自分のアカウントで Yahoo! Japan にログインした後、トップページ内の「登録情報」をクリックして「登録情報の確認」画面を表示させます（図 1-7 左）。

そこで「外部アカウント連携/解除」をクリックすると、現在連携しているサービスの一覧が表示されます（図 1-7 右）。

現在連携中のサービスについては「解除」と表示されます。その中で不要なものは「解除」をクリックして連携を取り消してください。

図 1-7：Yahoo! Japan における連携サービス表示画面の例（2012 年 9 月 15 日時点）

対策 2　<u>他者の投稿（ツイートなど）に書かれている URL を安易にクリックしない</u>

他者の投稿やツイートに書かれている URL を簡単にクリックすると、悪意あるサービスのサイトに転送されて、知らないうちにそのサービスと連携してしまう恐れがあります。

知り合いによる投稿（ツイート）でも安易にクリックしないようにしてください。

手口として“短縮 URL”※4 が使用されることも多いようです。特に Twitter は、1 回で入力できる文字数の制限があり、長い URL が収まりきらないことがあるため、リンクを提示する際に短縮 URL が頻繁に使われます。短縮 URL は、クリックするまでどのようなウェブサイトに誘導されるかわからず、悪意あるサイトへ誘導される可能性があります。

“短縮 URL”をクリックする前に、“短縮 URL”を本来の URL で表示するツールやサービスを使用し、URL の信頼性を確認してください。

また“短縮 URL”の文字列全体をインターネット検索することで、ある程度その内容と危険性を確認できる場合があります。

※4 短縮 URL：長い URL 文字列を短縮して利用できるサービス。例えば
「http://www.ipa.go.jp/security/personal/yobikake/index.html」を短くすると
「http://〇〇〇〇/5G5G3g」となります。（「〇〇〇〇」は短縮サービスを行うサイト名）

対策 3　連携先のサービスの評判を確認する

特に不正なサービスの場合はインターネット上で情報が見つかる場合があります。よく知らないサービスと連携する前には、事前に口コミなどで評判を確認することを勧めます。

（4）こんなときは…

怪しいツイートや DM（ダイレクトメール）が届いた、怪しいリンク先が書かれている SNS やブログなどの投稿文を見つけた、などがありましたら、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

■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

OAuth に関する技術的解説

「(2) ミニブログサービスの特徴と被害の実例」の実例は、連携先のサービスに ID とパスワードを教えることなく連携可能な「OAuth（オーオース）」の仕組みを巧みに利用したものです。

OAuth を活用して連携先のサービスと連携することで、多くの便利なサービスがおこなわれていますが、この仕組みを悪用されると、ID とパスワードを誰にも教えていないのに、勝手に SNS 上で悪事をされてしまいます。

前述の実例において発生するやり取りの技術的解説を、以下に示します（図 1-8）。

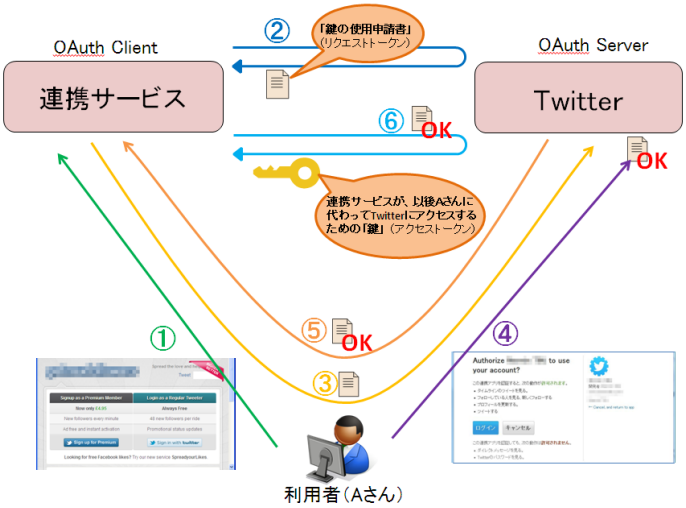

図 1-8：サービス連携時に発生するやり取りの概要

① A さんが、前述(2)【2】の画面上で「Twitter でログイン」をクリックします。実はこの行為は、「連携サービス」側に対して、「Twitter」と連携する手続きを開始するように指示する行為となります。

② 「連携サービス」側が「Twitter」に対して、鍵の使用申請書に匹敵するもの（正式には「リクエストトークン」）を要求し、受け取ります。

③ 「連携サービス」側が、A さんを「Twitter」上のページにリダイレクトさせます。その際、鍵の使用申請書も同時に転送※5 します。

④ A さんが、③で転送されたページ上で、「ログイン」をクリックします。これは、鍵の使用申請書に A さんが許可のサインをすることに相当します。

⑤ 「Twitter」が、A さんを「連携サービス」側のページにリダイレクトさせます。その際、A さんサイン済の、鍵の使用申請書も一緒に転送されます。

⑥ 「連携サービス」側が「Twitter」と通信し、A さんサイン済の、鍵の使用申請書と、鍵（正式には「アクセストークン」）を交換します。以後「連携サービス」側は、この鍵を持っていることで、**Twitter 上で A さんしかできないことを、A さんの代わりに実行することができます。**

※5 鍵の使用申請書も同時に転送：実際には、リクエストトークンを URL パラメータとして URL に付加します。

以上の①～⑥の過程を踏むことにより、「連携サービス」が A さんの権限で、Twitter 上でツイートしたり、第三者をフォローしたりすることができます。逆に A さんから見ると、その「連携サービス」に権限を委譲したつもりは無いのに、何気なくクリックしただけで、勝手にツイートされたり、第三者を勝手にフォローされたりすることになります。