5V-03

OAuth 認証を利用する SNS の認可リスクに関する考察

吉田 達司†　　関 良明‡

東京都市大学†‡

1. はじめに

Twitter や Facebook は，ユーザが情報や意見を簡便に発信できる SNS（Social Network Service）である．SNS の機能を拡充するために，OAuth 認証[1]を使ってスマートフォン上で連携するアプリケーション（AP）が多数存在する．連携した AP はユーザの同意を確認した上で，Twitter で 3 種類，Facebook で 40 種類以上の権限を獲得することができる．ユーザがこれらの権限を悪意のある AP に対して不用意に認可すると，リスクが発生する．

2. OAuth 認証と認可の仕組み

OAuth 認証は，ユーザのクレデンシャル情報（ユーザ ID，パスワードなど）を AP に渡すことなく，AP が SNS に限定的にアクセスすることを可能にする仕組みである．図 1 に示すように，OAuth 認証は，①～⑤の一連の手順で認証を行い，その中の③で「アクセス認可画面」を表示して，認可を行っている．この認可は，AP がユーザの SNS リソースにアクセスする権限を許可することであり，SNS 提供者が API を公開している．OAuth 認証を使用する際，この認可の部分で，ユーザが不用意に同意してしまうと，いくつかのリスクが生じることが考えられる．

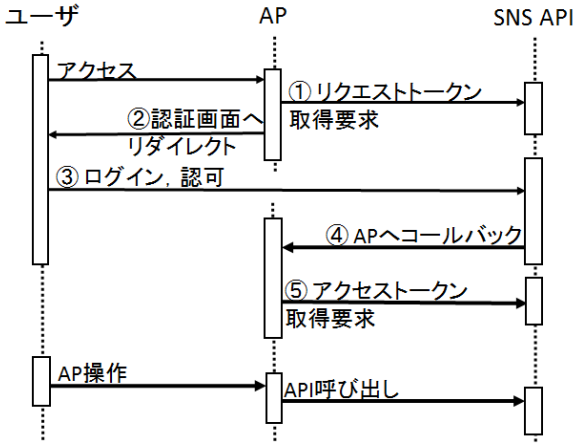

図 1 OAuth 認証シーケンス図の例

Consideration about Risk of Authorization with OAuth Authentication in SNS

†Tatsuzi Yoshida・Tokyo City University

‡Yoshiaki Seki・Tokyo City University

3. SNS における認可の悪用

SNS には，ユーザの情報をフォロワーに知らせる投稿，パーソナル情報の保管，ユーザとフォロワーが 1 対 1 で交信するダイレクトメッセージなどの機能がある．これらの機能において認可を悪用した事例を以下に挙げる．

3.1 自動投稿

Facebook には，連携した AP が獲得できる権限の中に，ユーザの代わりに投稿できる”publish_actions”という権限がある．図 2 に示すように，悪意のある AP がこの権限を設定し，ユーザが連携を許可した場合，ユーザの信頼性を損なわせるような記事を AP がユーザになりすまして投稿することができる．投稿内容はウォール（掲示板）やニュースフィールドなどに表示され，情報が拡散しやすい．

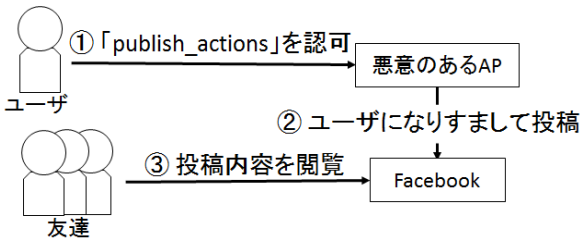

図 2 Facebook の自動投稿

3.2 パーソナル情報取得

Facebook では，ユーザ登録の際にユーザの名前や誕生日などのパーソナル情報を入力する．パーソナル情報は後に項目ごとに公開，非公開を選択できる．連携した AP は，このパーソナル情報を取得する権限を得ることもできる．図 3 に示すように，ユーザがパーソナル情報を非公開にしていても，OAuth 認証の際，ユーザが認可すれば，AP はパーソナル情報を取得できる．

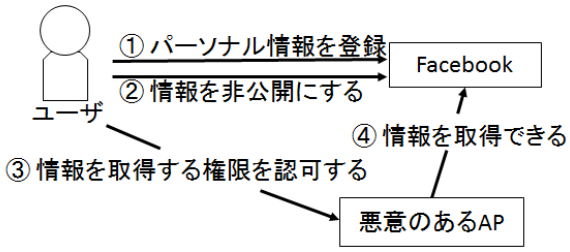

図 3 Facebook のパーソナル情報取得

Copyright ©2016 Information Processing Society of Japan.
All Rights Reserved.

3.3 ダイレクトメッセージ送信

Twitter には，連携した AP が獲得できる権限として，ダイレクトメッセージ（DM）を見る権限がある．図 4 に示すように，悪意のある AP がこの権限を設定し，連携した場合，ユーザになりすまして，フォロワーに DM を利用したメッセージを送ることができる．フォローしている相手から届くメッセージは，文中のリンクを信用してクリックする可能性が高まる．

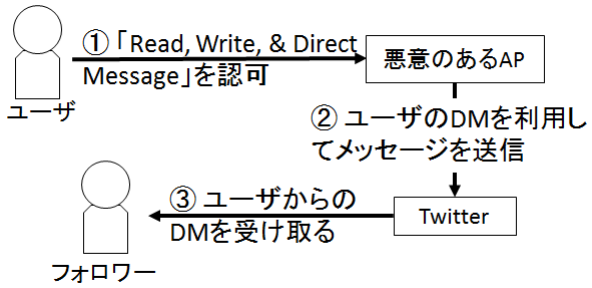

図 4 Twitter のダイレクトメッセージ送信

4. 現状の対策

OAuth 認証の認可を悪用する AP に対する SNS 提供者とユーザの現在の対策を以下に挙げる．

4-1 SNS 提供者の対策

Twitter や Facebook は，SNS 提供者として以下の対策を講じている．

1) ユーザによる確認

SNS 提供者は，AP と連携する際，ユーザに「アクセス認可画面」を表示している．ここで，ユーザは権限一覧を確認した上で，連携の可否を判断している（図 1 参照）．

2) AP の審査

Facebook は，AP が要求する認可権限が AP 内で適切に使用されていることを審査している．その際，AP の動作の内容，権限を要する理由，個人情報保護方針も AP 開発者に提出させている．これにより権限の不正使用を抑止している．

3) ユーザへの告知

Twitter や Facebook は AP の連携によって起きる問題の対策をヘルプサイトに掲載している[2][3]．具体的には，アプリの解除やスパム報告の方法を掲示している．

4-2 ユーザの対策

IPA では以下の対策を推奨している[4]．

1) 不要な連携の解消

SNS の設定において，連携しているサービスや AP を確認し，不要な連携は取り消すこと．

2) AP の評判

よく知らない AP と連携する際には，インターネット上で掲載されている AP の評判を確認し，連携の可否判断の参考にすること．

3) 不要な連携の防止

他者の投稿に書かれている URL を容易にクリックしないこと．

5. 考察

悪意のある AP が出現する要因を以下に考察する．

5-1 SNS 提供者の責任

スマートフォン利用年齢の若年化と高齢化に伴い，PC 利用経験のない初心者が増加している．SNS 提供者は，操作や表示を簡略化することで，これらのユーザへ利用拡大を図っている．しかし，認可に関する表示の簡略化は，説明責任を十分に果たさず，悪意のある AP と連携してしまうリスクをユーザに転嫁するものである．

5-2 ユーザの意識低下

持ち運びが容易なスマートフォンは，何らかの作業や移動中に片手間で操作することが多い．このような状況で AP との連携処理を行うことは，認可の内容をユーザが十分に確認して，実行しているとは考えにくい．

5-3 AP の開発環境

SNS 提供者は，連携する AP の開発環境や API 仕様の公開を積極的に推進している．API 仕様によっては，複数の認可権限を 1 つにまとめている場合がある．AP は余分な認可権限も得ることができ，AP 開発者に悪用を助長させてしまうことになりかねない．

6. おわりに

SNS 提供者が認可項目を適切に設定し，AP の審査を実施することにより，SNS 提供者の責任において，悪意のある AP を抑止し，安全な AP だけを市場に提供することができると考える．

参考文献

[1] The OAuth 2.0 Authorization Framework
http://tools.ietf.org/html/rfc6749
[2] Twitter ヘルプセンター
https://support.twitter.com
[3] Facebook ヘルプセンター｜Facebook
https://www.facebook.com/help
[4] SNS におけるサービス連携に注意！
https://www.ipa.go.jp/security/txt/2012/10outline.html

Copyright ©2016 Information Processing Society of Japan.
All Rights Reserved.