6Y-06

米国のOAuth/OpenID Connect実装におけるセキュリティ状況の調査および日米比較

上瀧　悠輔 †i　　菊田　翼 ‡　　小芝　力太 ‡　　齋藤　孝道 †
明治大学 †　　明治大学大学院 ‡

1　はじめに

Web アプリケーションを利用する際の認証において，ソーシャルログインと呼ばれる仕組みがあり，OAuth や OpenIDConnect を用いて主に実装されている．しかし，クライアント側（サービスを提供する Web アプリケーションの構築側）の実装によっては，プライバシーの問題を引き起こすことや脆弱性を作り込むことがある．本論文では Top Sites in America-Alexa[1] における上位 500 サイト (以降，上位 500 サイトと呼ぶ) を対象として，調査した．その結果，SNS からアクセス権限を必要以上に取得している Web サイトや，実装上の欠陥，非推奨トークン発行フローの実装により脆弱性を持つ可能性のある Web サイトが確認できた．また，これらの結果と国内を対象とした既存研究 [2] における結果との比較を行った．

2　関連知識

2.1　OAuth/OpenID Connect のトークン発行フロー

Web アプリケーションにおける OAuth/OpenID Connect のトークン発行フローには主に Authorization Code Grant と Implicit Grant の 2 つが存在する．しかし，Implicit Grant の実装はアクセストークンの漏洩や再利用に対して脆弱であり，推奨されていない [3]．また，クライアントは希望するトークン発行フローの種類を認可サーバに通知するために，response_type[4] をリダイレクト URL のクエリに付与することが必須となっている [5].

3　調査方法

3.1　ソーシャルログイン実装件数の調査

上位 500 サイトで Google，Facebook，Twitter，Yahoo!のアカウントを用いたソーシャルログインが実装されているか調査した．

3.2　必要以上に取得している権限の調査

クライアントが利用者からどの程度のアクセス権を取得しているか，またその中にサービスを利用する上で必要以上に取得しているアクセス権はないかを調査した．連携に用いた Google，Facebook，Twitter，Yahoo! の各アカウントの設定ページから，連携されている Web アプリケーション名とクライアントに委譲しているアクセス権を確認した．

3.3　CSRF 脆弱性の有無の調査

OAuth/OpenID Connect における CSRF 脆弱性 [5][6] を持つ可能性のあるクライアント数を調査した．調査の際，ソーシャルログインの認可における通信を保存した．また，保存した通信から，リダイレクト URL に state パラメータ [5][6] が付与されているかを調査した．state パラメータが付与されていない場合は CSRF 脆弱性を含み，付与されている場合は CSRF 脆弱性を含まないとした．ただし，Twitter では OAuth1.0 を拡張した TwitterOAuth[7] という独自のフレームワークが存在するので，調査の対象外とした．

3.4　トークン発行フローの判別の調査

クライアントによるトークン発行フローを調査した．3.3 節で保存した通信から，response_type の値を確認し，フローを判別した．response_type の値に code が含まれていた場合は Authorization Code Grant とし，token が含まれている場合は Implicit Grant とした．また，Twitter では 3.3 節と同様の理由で，調査の対象外とした．

4　調査結果と考察

4.1　ソーシャルログインの実装状況

Google，Facebook，Twitter，Yahoo!のいずれかを用いたソーシャルログインが，上位 500 サイトにおいて，重複も含めてどの程度実装されているかを図 1 に示す．

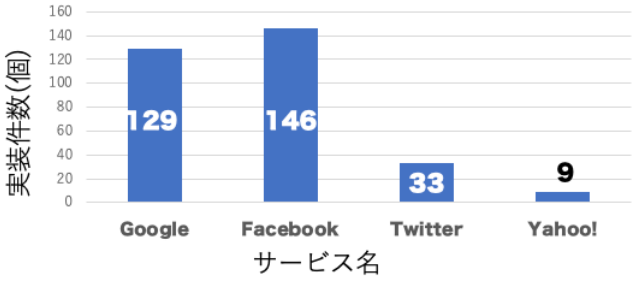

図 1: ソーシャルログインの実装状況

調査の結果，Google と Facebook を用いたソーシャルログインが実装されていたクライアントの数が突出していた．また，Google，Facebook，Twitter，Yahoo!

Consideration on required skill set based on Security Incidents
†Yusuke JOTAKI　‡Tsubasa KIKUTA　‡Rikita KOSHIBA
‡Takamichi SAITO
†Meiji University
‡Graduate School of Meiji University

のいずれかを用いたソーシャルログインが実装されていたクライアントは上位500サイト中168件存在した．国内の調査結果[2]では500サイト中79件であり，2倍以上の差があった．原因として，対象の国が違うことの他に，国内の調査から約1年経過したことも原因の1つと考えられる．

4.2 利用者へ要求している権限

Google，Facebook，Twitter，Yahoo!で，クライアントが利用者に要求しているアクセス権を分類した結果を表1，表2，表3，表4に示す．

表1: Googleにおけるアクセス権の分類と件数

付与されていたアクセス権	件数
アカウントの基本情報	125件
メールアドレスの表示	124件
ユーザの個人情報の表示	122件
Googleで公開されているお客様の個人情報とお客様を関連づける	3件
Gmailの情報	2件
電話番号	1件
Googleアカウントのメールアドレスを全て表示しダウンロードする	1件

表2: Facebookにおけるアクセス権の分類と件数

付与されていたアクセス権	件数
氏名とプロフィール写真	145件
メールアドレス	140件
友達リスト	21件
生年月日	12件
ページへのいいね	6件
写真	4件
性別	2件
出身地	1件
居住地	1件
タイムラインの投稿	1件

表3: Twitterにおけるアクセス権の分類と件数

付与されていたアクセス権	件数
書き込み	31件
読み取り	19件
メールアドレスへのアクセス	11件
ダイレクトメッセージ	2件

表4: Yahoo!におけるアクセス権の分類と件数

付与されていたアクセス権	件数
プロファイル	9件
Yahoo!の連絡先	1件

調査の結果，Twitterにおいて，既存研究で指摘された「ダイレクトメッセージ」への権限を要求するクライアントが33件中2件存在した．また，Googleにおいて，「Googleで公開されているお客様の個人情報とお客様を関連づける」や「Googleアカウントのメールアドレスを全て表示しダウンロードする」といった利用者が内容を理解しにくいものが存在した．これらの権限は，サービスを利用する上で必要ないと考えられる．

4.3 stateパラメータの調査

stateパラメータが付与されていないサービスはGoogleでは129件中33件，Facebookでは146件中41件，Yahoo!では9件中2件存在し，これらのサービスはCSRF脆弱性を持つ可能性がある．国内調査ではGoogleで58件中15件，Facebookでは56件中14件と，その割合に大差はなかった．この原因の1つとして，RFC6749[5]でstateパラメータの付与が必須とされていないことが考えられる．

4.4 トークン発行フローの判別

Google，Facebook，Yahoo!で，クライアントが使用しているトークン発行フローの判別結果を表5に示す．不明と判断したものは，response_typeの値が何らかの理由で採取できなかったものである．

表5: トークン発行フローの判別結果

	Google	Facebook	Yahoo!
Authorization Code Grant	68件	58件	5件
Implicit Grant	41件	55件	0件
不明	20件	33件	4件

5 研究倫理

本論文では，特定のサービス名を明示しないなど，調査対象への悪影響を及ぼさないように配慮した．

6 まとめ

本論文では米国の上位500サイトを対象とし，ソーシャルログインの実装状況を調査した．その結果，上位500サイト中168件にソーシャルログインが実装されていた．国内の調査結果では上位500サイト中79件であったためその実装数は2倍以上であった．また，その中に，必要以上に権限を要求していると考えられるクライアントが存在した．さらに，stateパラメータが付与されていないためにCSRF脆弱性が存在している可能性のあるクライアントがGoogleでは33件，Facebookでは41件，Yahoo!では2件存在した．国内の調査ではYahoo!は対象外となっているが，Google，Facebookにおいてはその割合に大きな差は見られなかった．そして，非推奨トークン発行フローであるImplicit Grantが実装されていたクライアントが，Googleでは41件，Facebookでは58件存在し，Yahoo!では存在しなかった．

参考文献

[1] Top Sites in US - Alexa. https://www.alexa.com/topsites/countries;4/US.

[2] 菊田翼, 齋藤孝道, 小芝力太. ”OAuth/OpenIDConnect実装におけるセキュリティ状況の調査”. コンピュータセキュリティシンポジウム2019論文集, pp. 800–807, oct.

[3] OAuth 2.0 Security Best Current Practice draft-ietf-oauth-security-topics-09 section-2.1.2. https://tools.ietf.org/html/draft-ietf-oauth-security-topics-09#section-2.1.2.

[4] OAuth 2.0 Multiple Response Type Encoding Practices. https://openid.net/specs/oauth-v2-multiple-response-types-1_0.html.

[5] RFC6749 The OAuth 2.0 Authorization Framework. https://tools.ietf.org/html/rfc6749.

[6] OAuth 2.0 Threat Model and Security Considerations. https://tools.ietf.org/html/rfc6819.

[7] TwitterOAuth. https://twitteroauth.com/.