2Z-7

OpenID Connectにおけるセキュリティ脅威モデルの検討

渡邉 貴文† 大丸 雅人‡ 磯 有斗 ‡ 今野 真希‡ 齋藤 孝道†
明治大学† 明治大学大学院‡

1. はじめに

近年，インターネット上でサービスを提供する Web アプリケーションが普及している．Web アプリケーションの多くは，エンドユーザに個別のサービスを提供することを目的として認証・認可を行う．認証には，ID とパスワードが用いられる場合が多い．従来，複数の Web アプリケーションを利用する場合，エンドユーザは Web アプリケーション毎にアカウントを管理しなければならず，認証と認可を切り離すことはなかった．そのような課題を解決する標準仕様の一つに OpenID Connect[1]がある．

OpenID Connect は，OAuth 2.0[2]をベースに拡張された，OpenID 2.0[3]の後継仕様である．Web アプリケーションは OpenID Connect を利用することで，他の運営主体からエンドユーザの認証情報及び属性情報を取得できる．しかし，OpenID Connect では，その仕様書の Security Considerations[4]で言及されているように，多くの課題が存在する．

本論文では，OpenID Connect において脅威となる攻撃手法に対して，影響や対策について検討する．

2. OpenID Connect

2.1 概要

OAuth 2.0 は，認可のためのプロトコルであり，認証情報及び属性情報を取り扱うための規定は含まれていない．これに対し，OpenID Connect では，OAuth 2.0 の機能を引き継ぎながらエンドユーザの認証情報及び属性情報のやり取りや，異なるドメイン間でシングルサインオンを実現できる．

2.2 OpenID Connect の関連用語

OpenID Connect の関連用語を説明する．

OP（OpenID Provider）

OP はエンドユーザのアカウント情報を管理し，RP に対して，エンドユーザの認証情報及び属性情報を提供する主体である．

RP（Relying Party）

RP は OP にエンドユーザの認証を委託し，エンドユーザにサービスを提供する主体である．

エンドユーザ

RP を利用するために，OP によって認証を受ける主体である．Web ブラウザで RP や OP にアクセスする．

認可コード

OP が RP に提供するランダムな文字列である．RP は OP に認可コードを送信することで，後述する ID トークン及びアクセストークンを取得する．

ID トークン

エンドユーザの識別子や認証日時などの認証情報が記載されたトークンである．

アクセストークン

OP が RP に提供するランダムな文字列である．RP は OP にアクセストークンを送信することで，エンドユーザの属性情報を取得する．

2.3 OpenID Connect のフロー

OpenID Connect の認可コードグラントと呼ばれる方式のフローについて説明する（図 1）．

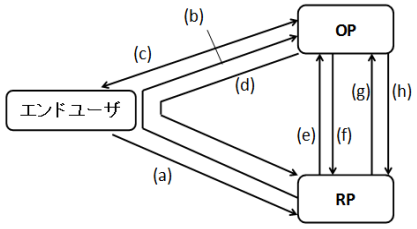

図 1 OpenID Connect のフロー

(a) エンドユーザは RP へリソースを要求する．
(b) RP は OP に認可要求を HTTP リダイレクトで送信する．
(c) OP はエンドユーザを認証する．認証後，エンドユーザは RP に認可をする．
(d) OP は RP に認可応答として，認可コードを URI に含め，HTTP リダイレクトで送信する．
(e) RP は OP から提供された認可コードを HTTP POST メソッドで，OP に送信する．
(f) OP は認可コードを検証し，正しいものであ

OpenID Connect threat models and security considerations
†Takafumi WATANABE
‡Masato OMARU，Yuto ISO，Maki KONNO
†Takamichi SAITO
Meiji University (†)，Meiji University Graduate School(‡)

れば RP に ID トークン及びアクセストークンを送信する．

(g) RP は提供されたアクセストークンを HTTP POST メソッドで，OP に送信する．

(h) OP はアクセストークンを検証し，正しいものであれば RP にエンドユーザの属性情報を送信する．

3. OpenID Connect における脅威

3.1 攻撃例

OP はエンドユーザを認証後，RP に認可コードを提供する．その際，OP は認可コード，エンドユーザ，及び，認可コードを提供した RP の識別子を紐付けて管理しなければならない．OP は RP から認可コードを受け取ると，その認可コードと紐付いているエンドユーザの ID トークン及びアクセストークンを送信する．

攻撃者は攻撃者のフローで利用される認可コードを，何らかの方法で取得した攻撃者以外のエンドユーザ（以下，別のエンドユーザとする）の認可コードに置き換えることで別のエンドユーザの ID トークン及びアクセストークンを取得することができる（図 2）．

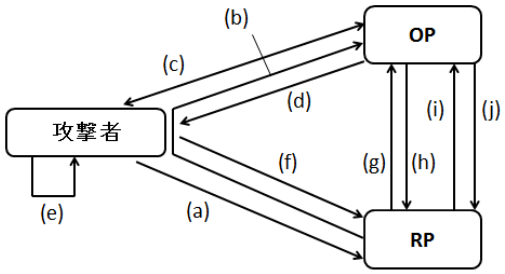

図 2　攻撃例のフロー

(a) 攻撃者は RP へリソースを要求する．

(b) RP は OP に認可要求を HTTP リダイレクトで送信する．

(c) OP は攻撃者を認証する．認証後，攻撃者は RP に認可をする．

(d) OP は RP に認可応答として，攻撃者の認可コードを URI に含め，HTTP リダイレクトで送信する．

(e) 攻撃者は，HTTP リダイレクトを停止し，URI における認可コード部を別のエンドユーザの認可コードに書き換える．

(f) 攻撃者は書き換え済みの認可コードを RP に送信する．

(g) RP は提供された認可コードを HTTP POST メソッドで，OP に送信する．

(h) OP は認可コードを検証し，別のエンドユーザの ID トークン及びアクセストークンを送信する．

(i) RP は提供されたアクセストークンを HTTP POST メソッドで，OP に送信する．

(j) OP はアクセストークンを検証し，RP に別のエンドユーザの属性情報を送信する．

仮に，攻撃者が別の RP に提供された認可コードを置き換えた場合，OP は認可コードと提供した RP の識別子を紐付けているので，図 2 における(h)での検証時に検知することができる．しかし，図 2 のように，RP を同じとして，ある攻撃者用の認可コードを別のエンドユーザ用の認可コードとして置き換えた場合，OP は認可コードを提供した RP が一致しているので，検証時に検知することができない．そのため，攻撃者に別のエンドユーザの認証情報及び属性情報が利用され，なりすましや個人情報の漏えいにつながる．

3.2 対策

この攻撃は，RP がエンドユーザの識別子と認可コードを紐付け，それをプロトコルの実行において検証することで防ぐことができる．たとえば，RP は認可要求（図 2 の b）で乱数をチャレンジとしてエンドユーザの識別子に付加し，OP に送信する．OP は受け取った乱数，RP の識別子，OP の識別子，認可コード，及び，OP と RP 間で予め共有している文字列をハッシュ化した値を認可コードと紐付け，認可応答（図 2 の d）でレスポンスとして返信する．RP は，チャレンジに対するレスポンスが期待する値であることを確認することで，認可コードがプロトコルの該当実行において送信されたことを検証できる．また，RP は受け取ったハッシュ値と認可コードを図 2 における(g)で同時に送信することで，OP でも認可コードの置き換えを検知することが可能である．

4. まとめ

本論文では，OpenID Connect において脅威となる攻撃についての例を挙げ，影響や対策について検討した．

5. 参考文献

[1]OpenID Connect Standard 1.0
http://openid.net/specs/openid-connect-standard-1_0-21.html

[2]OAuth 2.0 Authorization Framework
http://openid-foundation-japan.github.io/rfc6749.ja.html

[3]OpenID Authentication 2.0
http://openid.net/specs/openid-authentication-2_0.html

[4]OpenID Connect Messages 1.0
http://openid.net/specs/openid-connect-messages-1_0-20.html