3F-3

OAuth 2.0を利用したメール送信者制御手法の検討

城間　政司†　　長田　智和‡　　谷口　祐治††　　名嘉村　盛和‡　　玉城　史朗‡
†琉球大学大学院理工学研究科　　‡琉球大学工学部情報工学科　　††琉球大学総合情報処理センター

1　はじめに

インターネットの普及により電子メールが広く利用されており，日常生活や業務で必要不可欠なものとなっている．一方，メールアドレス所有者の意図しない多量のスパムメールの存在が問題となっている．マイクロソフト社のセキュリティインテリジェンスレポート [1] によると，当社の Forefront Online Protection for Exchange サービスでチェックしたメールのうち約 8 割がスパムメールとして送信されている．このため，広告，フィッシング目的のメールやマルウェアを含んだメールなど，多量のスパムメールの中に重要なメールが埋もれてしまうケースがあり，さまざまなスパムメール対策が講じられている．

本稿では，SNS における交友関係やユーザの属性情報などを利用した認証方法をメール送信者制御に活用する手法を提案する．本手法は，OAuth 2.0[2] および OpenID Connect[3] を利用しており，メールアドレスの所有者が当該メールアドレスへのメール送信を認可したユーザに対してアクセストークンを発行し，そのアクセストークンが添付されたメールが正当なメールであることを判別する．

2　ID 連携技術を利用したメール送信者制御手法

本節ではメールアドレスの所有者が認可した相手からのメールであることを確認してスパムメールと区別するため，OAuth 2.0 および OpenID Connect を利用したメール送信者制御手法を提案する．本手法はメールアドレスの所有者が設定したポリシーや認証方法によってメール送信者を認証し，認証が成功したメール送信者に対してアクセストークンを発行する．メール送信者はアクセストークンを添えたメールを送信することで，宛先アドレスへのメール送信が認可されていることを証明する．

本手法のメール送信手順は図 1 および以下の通りである．

†Tadashi SHIROMA　joma@ns.ie.u-ryukyu.ac.jp
‡Tomokazu NAGATA　nagayan@ie.u-ryukyu.ac.jp
†Graduate School of Science and Technology, University of the Ryukyus.
‡The Department of Information Engineering, University of the Ryukyus.

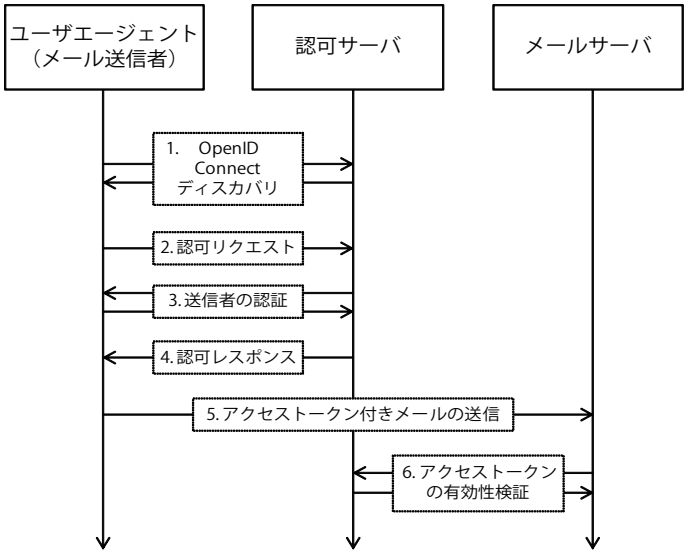

図 1: 提案手法におけるメール送信手順

1. メール送信者は宛先のアドレスに対して OpenID Connect ディスカバリを実行し，認可リクエストに必要な情報を取得する．
2. メール送信者は認可サーバに認可リクエストを送信する．
3. 認可サーバはメールアドレス所有者が事前に設定した認証手順でメール送信者を認証する．
4. 認可サーバは認可レスポンスをメール送信者へ送信する．
5. メール送信者は認可レスポンスに含まれるアクセストークンを添付したメールを作成し，宛先アドレスへメールを送信する．
6. メールサーバまたはメールアドレス所有者は，受信したメールに含まれるアクセストークンの有効性を認可サーバに問い合わせて検証する．

まず手順 1 では，メール送信者は，宛先のアドレスに対して OpenID Connect ディスカバリ [4] を実行し，当該アドレスに関する認可サーバの情報を収集する．OpenID Connect ディスカバリは Simple Web Discovery をベースとしたディスカバリプロトコルであり，メールアドレスや URI を元にして認可サーバの URI やサ

ポートする認証ポリシーなどのコンテキスト情報を取得できる．

手順2では，メール送信者が認可サーバに認可リクエストを送信する．このとき，OAuth 2.0 および OpenID Connect の認可リクエストでは，要求するアクセス範囲を scope パラメータで指定することができる．そこで本手法では，mailto スキームで宛先アドレスを指定して認可リクエストを送信する (例：`scope=mailto:taro@example.com`)．

手順3では，メールアドレス所有者が事前に設定した認証方法を用いて認可サーバがメール送信者を認証する．認証方法には，CAPTCHA によるテストや合言葉の入力，Facebook や Twitter とサービス連携してメールアドレス所有者とメール送信者が交友関係にあることを認証する方法などが考えられる．

手順4では，手順3の認証が成功した場合に認可サーバはアクセストークンを発行し，認可レスポンスにアクセストークンを含めて送信する．

手順5では，メール送信者は認可レスポンスに含まれるアクセストークンを添付したメールを作成し，宛先アドレスにメールを送信する．

最後に手順6では，アクセストークン付きのメールを受信したメールサーバまたはメールアドレス所有者は認可サーバにアクセストークンの有効性を問い合わせてその有効性を検証し，受信したメールが認可したメール送信者から送信されたものであることを判別する．

以上の手順により，宛先アドレスの所有者が認可したメール送信者によるメールであることを確認して正当なメールの判別が可能となる．

3 考察

3.1 アクセストークンの盗聴対策

SMTP を用いて送信するメールは基本的に平文のデータであるため，送信経路の途中でアクセストークンが盗聴される可能性がある．さらに，アクセストークンが不正利用され，スパムメールや不正なメールを認可されたメールとして送信されるリスクが生じる．

OAuth 2.0 ではアクセストークンと共にリフレッシュトークンを発行できる．通常，アクセストークンは盗聴や不正利用の対策のため有効期限が短く設定されており，リフレッシュトークンを用いると認可手続きなしに新しいアクセストークンを取得できるようになっている．前述のケースにおいても，アクセストークン付きのメールを検証後にアクセストークンを無効化し，メール送信者はリフレッシュトークンを用いてアクセストークンを再度取得することで，盗聴や不正利用に対策可能である．

3.2 アクセストークン添付方法の検討

本手法では，アクセストークンを添えたメールを送信する．このとき，受信したメールのどの情報がアクセストークンであるかを判別しなければならない．

OAuth 2.0 の従来の方法では，HTTP ヘッダ内の Authorization ヘッダにアクセストークンを指定する方法が規定されている．SMTP におけるメールにもヘッダ部分があるため，メールのヘッダに Authorization ヘッダとアクセストークンを追加する方法が考えられる．ただし，メールのヘッダを追加するにはメールクライアント側の本手法への対応が必要となるため，この方法では任意のメール送信者のメールクライアントを用いたメール送信に対応できない．

また，拡張アドレスを用いる方法が考えられる．拡張アドレスとは，メールアドレスのユーザ名の部分を+記号のデリミタと任意の文字列で拡張することで，同一ユーザが複数のメールアドレスを持つことを可能にする (例：taro+jiro@example.com)．2 節の手順 5 で述べたように，アクセストークンを拡張部分に指定してメールを送信することでアクセストークンを添えたメールを送信可能である．

4 まとめ

本稿では，スパムメールと正当なメールを判別するための手法として，メールにアクセストークンを添付する手法を提案した．アクセストークンの発行手続きでは，ID とパスワードによるユーザ認証以外にも CAPTCHA テストや SNS における交友関係を用いた認証方法を利用することで柔軟な認可ポリシーの設定が可能である．

今後の展望として，本手法を実装する上で必要となる詳細なプロトコルの検討や，プロトタイプによる利便性などの評価を行う予定である．

参考文献

[1] Microsoft Corporation. Microsoft security intelligence report - volume 13, 2012.

[2] Dick Hardt. The oauth 2.0 authorization framework.

[3] OpenID Foundation. Openid connect specs, 2012.

[4] Nat Sakimura, John Bradley, Michael B. Jones, and Edmund Jay. Openid connect discovery 1.0, 2012.