[ポスター発表] 研究報告

接続元認証を用いたOpenFlowによるインターネット公開サーバへのアクセス制御機構の検討

田中 健一[1,a)]　桝田 秀夫[2]　森 真幸[2]　永井 孝幸[2]

A consideration of OpenFlow-based Access Control Method for Public Servers on the Internet Using Connection Source Authentication

1. はじめに

大学や一般企業などの組織において，構成員が利用するためにインターネットで公開しているサービスは多数存在している．昨今のコロナ禍により，オンライン授業やリモートワークが急速に普及し，構成員向けのサービスの外部からの利用機会は特に高まっている．そのような中で，利用者の認証・アクセス制限を厳格に行い不正利用を防止することが求められている．

しかしながら，漏洩した認証情報を用いたパスワードリスト攻撃による不正アクセスは後を絶たない．これらの対策としては多要素認証の実施や，FIDO2 [1] によるパスワードレス認証が挙げられるが，すべてのサービスにおいて使用できるわけではない．

それらのサービスに対する不正アクセスの対策の一つとして「認証シャッター」が提案されている [2]．「認証シャッター」では，従来のサービス側での利用者認証に加え，利用者認証の可否を送信元 IP アドレス単位で行う．利用者認証の許可は，利用者自身によって申請可能であり，申請後一定時間送信元 IP アドレスからの利用者認証要求を許可することによって，「シャッター」のような動作を行う．

「認証シャッター」の具体的な実現方式は複数提案されている．本村らは，nginx[3] をリバースプロキシとして使用し，同ソフトウェアで独自の認証を行える機能を使用することにより動作を実現している [4]．佐藤らは既存のファイアウォールシステムが提供する API を使用し，特定の IP アドレスを送信元とする通信の可否を外部から動的に制御することにより動作を実現している [5]．

本研究では，シャッターの開閉動作に OpenFlow を使用し，複数のサーバに通信を分配することで機能付加できる認証シャッターについて提案する．

[1] 京都工芸繊維大学大学院 工芸科学研究科
[2] 京都工芸繊維大学 情報科学センター
[a)] m1622025@edu.kit.ac.jp

2. 提案方式

2.1 概要

本方式は，OpenFlow の特徴である通信の柔軟な制御が可能な点を活用し，シャッター開放状況に基づき異なる通信経路を選択することで認証シャッターの動作を実現可能とする．さらに，OpenFlow を用いることによってシャッター閉鎖時に届いた通信も処理可能となり，さまざまな付加機能として活用できる．ここでは，認証シャッターを適用する一つの事例として，利用者が MUA（Mail User Agent）からインターネット経由で組織の SMTP submission サービスを利用する場合を考える．

2.2 特徴

提案方式では，OpenFlow を使用することによって以下の特徴を有することができる．

(1) リバースプロキシを利用する方式と比較して多種のサービス，プロトコルに対応可能である．
(2) シャッターの開閉動作に標準化された OpenFlow 技術を用いているため，多くのベンダーのネットワーク機器で動作可能である．
(3) シャッター閉鎖時の通信を，攻撃動向の調査に用いることができる．
(4) シャッター閉鎖時に通信してきた利用者の通信を，各プロトコル上で現在シャッターが閉じている旨のエラーを送出するサーバーに転送することができる．
(5) 非利用者からの攻撃性のあるパケットを正規のサーバーに到達させないことで，正規サーバーへの攻撃の一部を減らすことが見込まれる．

2.3 想定する方式を用いたシステムの構成

今回提案する方式を用いたシステムの構成を図 1 に示す．本システムは，サービスを利用しようとするクライアント（ユーザ），通信経路の切り替えを行う OpenFlow Switch，

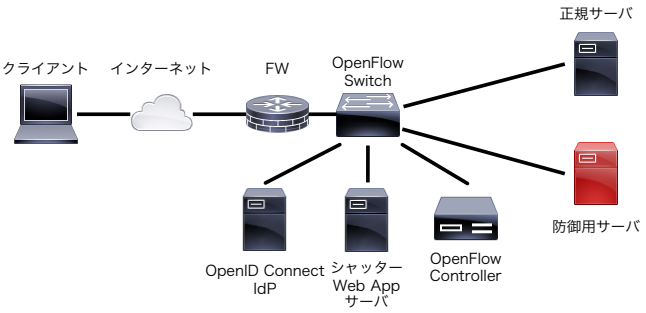

図 1 今回提案するシステムの構成
Fig. 1 Configuration of the proposed system.

OpenFlow Switch を管理する OpenFlow Controller，シャッター開放の申請が行えるシャッター用 Web App サーバ，認証・認可を担当する OpenID Connect IdP，防御用 SMTP サーバ，正規 SMTP サーバからなる．

なお，現在実装中のシステムでは，OpenFlow Controller として Ryu Controller，OpenID Connect IdP として Keycloak を使用している．

2.4 想定しているユーザの動き

本方式の認証シャッターを使用した場合に想定しているユーザの動きは以下のようになる．

(1) ユーザは MUA を使用してメールを送信しようとする．このとき，シャッターは閉鎖状態であると仮定する．
(2) シャッターが閉鎖状態のため，OpenFlow Switch の経路制御によって防御用 SMTP サーバに接続される．
(3) ユーザは防御用 SMTP サーバからシャッター開放を指示するエラーメッセージを受け取る．
(4) ユーザは Web ブラウザを使用して，シャッター開放用ページを開き IdP へリダイレクトされた後ログインを実施し，シャッター開放申請を行う．
(5) ユーザは再度メールを送信する．
(6) シャッターが開放されているため，通信は正規サーバに転送され，メールの送信ができる．

2.5 各サービス構成要素の動き

2.5.1 OpenFlow Switch

基本的にはレイヤ 2 スイッチとして動作する．本 Switch には，各正規サーバの IP アドレスを宛先とするパケットについて，宛先を各防御用サーバの IP アドレスに書き換えてから送信する低優先度のフローをあらかじめ追加しておく．また，OpenFlow Controller によって動的にフローエントリが追加される．

2.5.2 OpenFlow Controller（Ryu Controller）

大きく 2 つの役割を持つ．1 つ目は OpenFlow Switch と通信し，フローエントリを追加する役割である．シャッター Web App サーバより解放指示を受けた IP アドレスに対し，各正規サーバの IP アドレスを宛先とするパケットを正規サーバに送信するフローを高優先度で追加する．逆向きの通信についても同様のフローを追加する．

2 つ目の役割は，シャッター Web App サーバとの通信である．Controller は REST API を提供し，シャッター Web App サーバから特定の IP アドレスへの解放指示を受け付け，当該 IP アドレスに対しては上述の動作を行う．

2.5.3 シャッター Web App サーバ

IdP と認証連携を行い，利用者認証を可能にする．また，利用者によるシャッター開放指示を受けて，OpenFlow Controller が提供する REST API に対して，当該 IP アドレスへのシャッター開放指示をリクエストする．

2.5.4 OpenID Connect IdP

シャッター用 Web App サーバと認証連携を行い，利用者認証を実施する．また，多要素認証などを使用し，ユーザ ID とパスワードの組のみを用いない方式によって不正ログインを防止する．

2.5.5 防御用 SMTP サーバ

シャッター閉鎖状態の送信元 IP アドレスの通信が到達する．ユーザにシャッター開放を行うよう指示するエラーメッセージを返したり，不審なクライアントの挙動を分析したりすることが可能である．

2.5.6 正規 SMTP サーバ

シャッター開放状態の送信元 IP アドレスの通信が到達する．このサーバは組織がインターネット上に公開したいサービスを提供するものである．

3. おわりに

本報告では，認証シャッターを実現する実装方式の一つとして，OpenFlow を利用したものを提案し，SMTP submission サービスへの適用を事例として説明した．OpenFlow を使用することによって，未認証の通信を防御用 SMTP サーバに転送し，正規 SMTP サーバの防御や不正な通信の分析が可能となるなど，これまでの提案方式と比べ高機能で拡張性を持たせることができる．今後，実装を行い想定通りの動作をすることや性能評価を行う予定である．

参考文献

[1] FIDO Alliance Specifications Overview - FIDO Alliance, https://fidoalliance.org/specifications/.
[2] 高田哲司：Authentication Shutter: 個人認証に対する攻撃を遮断可能する対策の提案, コンピュータセキュリティシンポジウム 2014 論文集, Vol.2004, No.2, pp.883–890 (2004).
[3] nginx, https://nginx.org/en/.
[4] 本村真一, 川村尚生：既存のサービスシステムの変更を不要とする認証シャッターの提案, 学術情報処理研究, Vol.20, No.1, pp.112–118 (2016).
[5] 佐藤 聡, 三宮 秀次, 片岸 一起, 中井 央, 亀山 啓輔：研究報告インターネットと運用技術（IOT）, 2019-IOT-46, No.4 (2019).