5U-04

ファイアウォールにより同時アクセス数を動的に制御するWebシステムの設計

大川昌寛† 最所圭三‡
香川大学

1. はじめに

対話的処理を必要とする特定サービスではサーバの過負荷などによって応答性が低下することが問題になる．この問題は，ユーザ認証などにより同時サービス数を減らすことで，対策することができる．しかし，DoS 攻撃を防ぐことはできない．これはファイアウォール(FW)によるフィルタリングによって防ぐことができる．この方法は脆弱性の狙った攻撃に対しても有効である．

本研究では，対話的な処理を行うサーバに対し，FW を利用してアクセス制御を行うシステムを開発している．特定サービスサーバが過負荷になる前に，アクセスを遮断することができるためである．

本システムでは，特定サービスにアクセスを行うリクエストにより，FW サーバのフィルタリングルールを動的に変更することで特定サービスサーバへアクセスできるようにする．特定サービスサーバへアクセスできるクライアント数を制御することによって安定的なサービスと，セキュリティの確保ができる機構の実現を目指す．

本稿では，特定サービスサーバへのアクセスを許可する機構について述べる．

2. 提案システム

本研究で提案する機構を図 1 に示す．特定のサービスを提供するサーバ(特定サービスサーバ)，フィルタリングルールの変更や，ルールに応じてアクセスを制御するサーバ(FW サーバ)，クライアントの誘導や，ユーザの認証など通常の Web サービスを提供するサーバ (Web サーバ) というそれぞれの役割を持つ 3 種類のサーバを用いる．

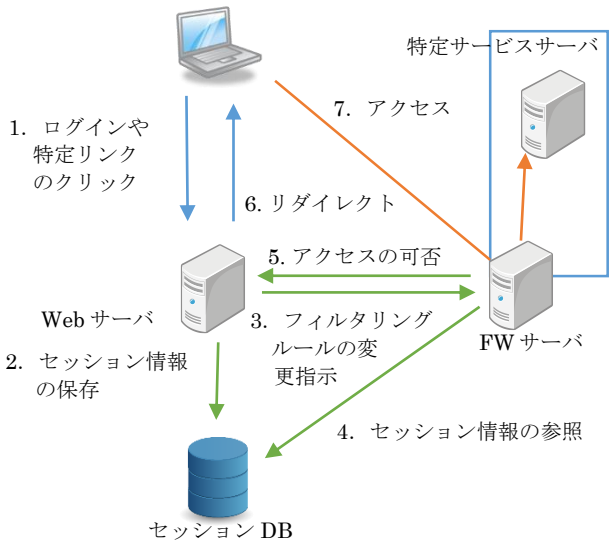

図 1 提案するシステムの構成図

FW サーバは，同時アクセス可能なクライアント数の制御，アクセス許可が失効したクライアントのフィルタリングルールの削除，アクセス許可が発行されたクライアントのフィルタリングルールの追加，特定サービスサーバを FW 内に設置するためのネットワーク機能を持つ．Web サーバからの指示により，フィルタリングルールの追加を行なう．特定サービスサーバからの指示や，定期的な各クライアントの接続時間のチェックにより，アクセス許可を失効させ，クライアントからのアクセスを遮断する．

特定サービスサーバは FW サーバ上に構築されたファイアウォールの内側に存在する．Web サーバは特定ユーザへのサービス，あるいは特定サービスサーバで行うサービスを検知した場合，FW サーバへフィルタリングルールの変更を指示し，クライアントへ特定サービスサーバの URL を返却する．クライアントは返却された URL にアクセスする．

3. 特定サービスサーバへのアクセス制御

3.1 認証を必要とする場合

FW サーバのフィルタリングルールは初期状態では，特定サービスサーバへのすべてのアクセスを許可しないように設定されている．ユーザ

Design of Access Control Mechanism Controlling Simultaneous Access Number for Web Server Using Firewall.
Masahiro OKAWA, Kagawa University, Faculty of Engineering
Keizo SAISHO, Kagawa University, Faculty of Engineering

Copyright ©2015 Information Processing Society of Japan.
All Rights Reserved.

認証は，Web サーバ上の Web アプリケーションによって行なう(1)．ID とパスワードによってクライアントを認証する．認証に成功したクライアントごとに接続情報を記録し(2)，ユーザを一意に識別できるようにするとともに，FW サーバに対してフィルタリングルールの変更指示を行う(3)．FW サーバは現在のアクセス許可数が上限に達していない場合はクライアントがアクセスできるよう FW のフィルタリングルールを追加し，その結果を Web サーバに送る．Web サーバはアクセスが許可された場合，クライアントに対して特定サービスサーバへリダイレクトする(6)．アクセスが許可されない場合は，アクセスできないことを通知する(5)．アクセスが許可された場合は，クライアントは特定サービスサーバへアクセスする(6)．

FW サーバは，定期的に接続時間をチェックし，ある一定期間を超えた場合は，切断する．特定サービスサーバから処理の終了通知があった場合も同様に切断する．これによって特定サービスサーバへのアクセス数を制限する．

3.2 認証を必要としない場合

Web サーバ上には，特定サービスへ移行するリンクがあり，リンクがクリックされると(1)，ファイアウォールサーバへそのクライアントからのアクセスを許可するようにフィルタリングルールを変更するように指示を出す(3)(4)．以降はセッション情報の記録を除いて，認証を必要とする場合と同様である．

4. アクセス許可機構の設計

本節では，3 章で述べたアクセス制御を行うアクセス許可機構の設計について述べる．本機構は，Web サーバ部と FW 部から構成される．

Web サーバ部では，必要に応じて認証を行い，認証できない場合はクライアントに対してその旨を通知する．認証された，もしくは認証を必要としない場合は，Cookie を発行しセッション DB に格納する．ここで Cookie を使う理由は，NAPT 環境下にあるアクセス権を有するクライアントを識別するためである．アクセス許可を決定した場合は，FW 部に対してアクセス許可の指示を出す．FW 部で許可された場合は，クライアントに対する応答として生成された Cookie とともに特定サービスサーバへのリダイレクトを返す．許可されない場合は，特定サービスサーバへアクセスが集中していることを通知する．

FW 部は，Web サーバからアクセス指示を受けると，現在のアクセス許可数が上限に達していない場合は許可を，達している場合は不許可を Web サーバ部に返す．許可した場合は，セッション DB から IP アドレスと Cookie を取り出し，アクセス許可 IP アドレスのホワイトリストに追加する． Cookie はクライアントからのアクセス時に利用するため，事前に FW 部に取り込んでいる．クライアントからアクセスを受けた場合，FW 部はクライアントの IP アドレスがホワイトリストに存在するかをチェックする．存在する場合は，クライアントの送信した Cookie が FW 部の持つ Cookie リストに存在するかをチェックする．ここまでのチェックに通った場合は，アクセスを特定サービスサーバへ通す．それ以外はクライアントに対して認証失敗の旨を通知する．

Web サーバ部は Ruby on Rails[1]を用い，FW 部では Lua 言語でルールを記述することのできるセキュリティツール haka[2]を用いて実装する予定である．また，認証機能については Ruby on Rails のプラグインである devise[3]を利用する．

haka は Lua 言語で記述したルールに基づいてパケットのキャプチャやフィルタリング，ロギングなどができるツールである．プロトコルパーサを記述することで任意のプロトコルを扱うことができる．また，取得したパケットを編集する機能もある．フィルタリング機能，デフォルトで提供されている IP,HTTP のプロトコルパーサを利用して，認証済みのクライアントのみ特定サービスサーバへアクセスできる FW を構築できると考えている．

5. おわりに

ファイアウォールにより同時アクセス数を動的に制御する Web システムの概要および，そのためのアクセスを許可する機構について述べた．

今後は，FW サーバで，アクセス許可の発行されたクライアントを追加する際に，クライアント数を利用した制御の追加，特定サービスサーバへのアクセス権失効機能の追加，クライアントにブックマークを使ったアクセスを許可しない手法の検討および，設計を行う．

謝辞 本研究は ISPS 科研費 25330082 の助成を受けた．

参考文献

[1] http://rubyonrails.org/
[2] http://www.haka-security.org/
[3] https://github.com/plataformatec/devise

Copyright ©2015 Information Processing Society of Japan.
All Rights Reserved.