ファイアウォールを用いたWebサーバへの同時アクセス数制御機構の設計と機能テスト

09T214　大川 昌寛　（最所研究室）

安定的にサービスを提供したい特定のサービスに対して，ファイアウォールを利用してアクセス制御を行なうシステムの開発を目指す．提案するサービス対象を制限したWebシステムの設計と，実現性を確かめるための簡易実装および機能テストについて述べる．

1　はじめに

Webを利用したサービスの中には，ある特定の対話的な処理を高い優先度で処理したいという要求がある．そのような場合サーバの過負荷によって応答性が低下することが問題になる．ユーザ認証などにより同時サービス数を減らす対策が考えられるが，DoS攻撃を防ぐことはできない．この攻撃はファイアウォールによって防ぐことができる．この方法は，脆弱性を狙った攻撃に対しても有効である．

本研究室では，通常アクセスと優先アクセスのキューを別にして，優先アクセスを実現するWebサーバの開発を行っている[1]．このシステムでもDoS攻撃を防ぐことはできない．本研究では，安定的に提供したい特定のサービスに対して，ファイアウォールを利用してアクセス制御を行なうシステムの開発を目指す．

2　サービス対象を制限したWebシステム

本システムの構成を図1に示す．特定サービスサーバはFWサーバによって保護されており安定的にサービスを提供する．WEBサーバは，通常のWebサービスを行いながら，特定サービスの要求を受けると，FWサーバに対して，そのクライアントがサービスを受けられるように指示を出す．FWサーバはファイアウォール，クライアント数管理機構，アクセス許可機構をもつ．特定サービスの利用開始を検知する方法として，ユーザ認証を利用しログインによって検知する方法と，特定のURLへのアクセスを検知する方法を考えている．

特定サービスをログインによって開始する手順を以下に示す．クライアントはWEBサーバ上の認証機構へアクセスし，ユーザ認証する(1)．認証に失敗した場合，認証機構はクライアントに認証失敗の旨を通知し，再入力を促す．認証に成功した場合，セッション情報をDBへ保存し(2)，FWサーバにフィルタリングルールの変更を指示する(3)．指示を受けたFWサーバは，クライアントのアクセスを許可するためにフィルタリングルール変更と，セッションDBを参照したクライアントリストの更新を行い(4)，結果をWEBサーバに返す(5)．WEBサーバは，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

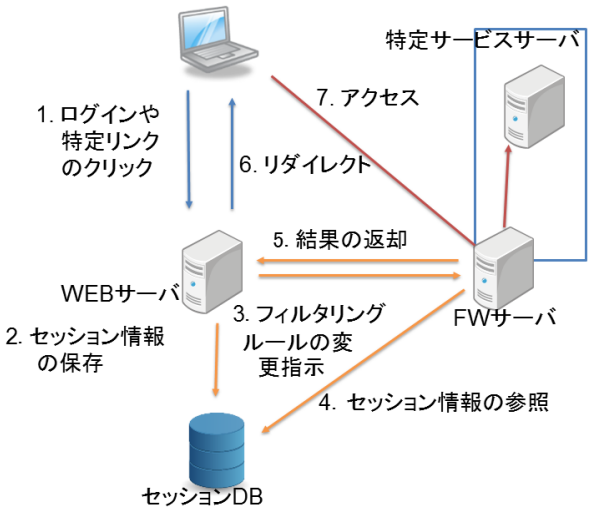

図1: システムの構成

クセス許可機構は，特定サービスへのクライアントのアクセスを監視する．許可されたクライアントからの場合は何もせずにアクセスを通す(7)．そうでない場合は，アクセスが許可されないことを通知するため，クライアントをWEBサーバへリダイレクトする．

特定リンクのクリックに対しては，(1)で認証を行わないこと以外は同じである．ただしセッション情報の作成と保存は行う．

Webサーバは認証機構を，FWサーバはクライアント数制御機構とアクセス許可機構を持つ．認証機構は，特定サービスの開始の検知やクライアント数制御機構への通知などの機能を持つ．クライアント数制御機構は，同時アクセス数に基づいたクライアントリストの管理や定期的なアクセス許可の失効などの機能を持つ．アクセス許可機構は，接続元IPアドレスやクライアントのもつcookieによるフィルタリング機能を持つ．

3　実装

提案手法の実現性を確認するために簡易的な実装を行っている．認証機構，クライアント数制御機構，アクセス許可機構の実装状況を表1に示す．

実装済みを○，未実装を×，部分的に実装されてい

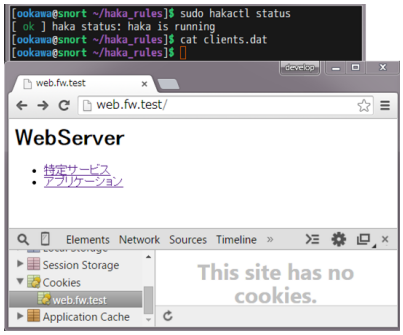

図 2: アクセス前の状態

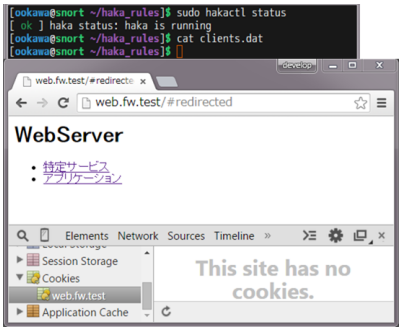

図 3: cookie 無しのアクセス

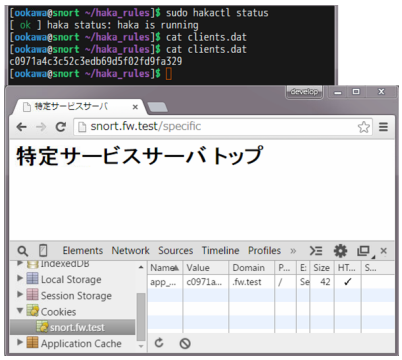

図 4: cookie 有りのアクセス

表 1: 実装状況

機能	実装状況
認証機構	
ユーザ認証	○
特定 URL へのアクセス通知	×
cookie の発行と DB への保持	△
クライアント数制御機構への通知	○
ログアウト時のアクセス許可失効	×
クライアント数制御機構	
クライアントリストの保持	○
定期的なアクセス許可の失効	×
同時アクセス数に基づいた クライアントリストへの追加	×
アクセス許可機構	
cookie によるフィルタリング	○
接続元 IP アドレスによるフィルタリング	×

るものを△で表記している．全ての機構において，認証を利用しない機能を実装できていない．

4 機能テスト

cookie によるフィルタリングで，認証済みのクライアントに対してアクセス許可とリダイレクトを切り替えできるかどうかの機能テストを行った．行った機能テストの手順を以下に示す．

1. 機構の起動状態を確認する
2. クライアントリストが空であることを確認する
3. ブラウザに cookie がないことを確認する
4. 特定サービスへのアクセスを試みる

結果を図 2，図 3，図 4 に示すが，上部に機構の起動状態とクライアントリストを，下部に Google Chrome のデベロッパーツールによる cookie の詳細表示を示す．

特定サービスへのアクセス前の状態を図 2 に示す．上部から，クライアントリストが空であることがわかる．下部を見ると，URL は”web.fw.test”となっており，WEB サーバへアクセスしていることわかる．また，デベロッパーツールの表示よりブラウザが cookie を持っていない状態であることが確認できる．

次に，未認証状態のクライアントから特定サービス (http://snort.fw.test/specific) へアクセスした状態を図 3 に示す．下部の URL を見ると，ドメイン名はリンクと異なっており，リダイレクトされていることわかる．

最後に，認証状態のクライアントから特定サービスへアクセスした状態を図 4 に示す．下部より，ブラウザの URL を見ると特定サービスサーバへアクセスできていることが確認できる．また，上部のクライアントリストを見ると，クライアントリストに cookie が追加されており，ブラウザが同じ cookie を持っていることがわかる．

5 おわりに

本研究室で開発している，特定のサービスを安定的かつセキュリティを確保しながら提供するために同時アクセスできるユーザ数を制限するシステムの設計について述べた．また，システムの実現性を確認するためにユーザ認証を利用する場合に限定した実装を行った．さらにその機能テストを行い，実現可能であることが確認できた．

今後の課題として，発行したアクセス許可を失効させる機能の実装が必要である．また，認証を利用しない場合の特定 URL へのアクセス検知や cookie の発行機能の実装も必要である．

参考文献

[1] 山田 茂和，”NAP-Web の時間予測に関する評価と優先アクセス機構の設計”， 香川大学，修士論文, 2012