ファイアウォールを用いた同時アクセス数制御機構の試作

12T230　杉本 亮太 （最所研究室）

特定のサービスを安定して提供するために，ファイアウォールを利用したフィルタリング機能とアクセス数制御を行う機構の実装と評価について述べる．

1　はじめに

アクセスの集中などにより，サーバが過負荷状態になるとサービスの応答性が低下するという問題が発生する．ある特定のサービス (特定サービス) に対して応答性を維持したまま処理したいという要求がある．当研究室では，特定サービス以外をファイアウォールを用いて，遮断する機構の開発を行っている．先行研究 [1] では全体の設計と，cookie を用いたフィルタリング機能の実装が行われたが，IP レベルでのフィルタリングを用いる部分は実装されていなかった．本研究では，IP レベルでのフィルタリングを用いた部分の実装と，その評価を行った．

2　ファイアウォールを用いた同時アクセス数制御機構

ファイアウォールを用いたアクセス数制御の概要を図 1 に示す．クライアントが認証に成功すると，認証サーバは FW サーバにアクセス可否を問合せる．FW サーバのアクセス数制御機構は，現時点でのアクセス許可数によりアクセスの可否を決定し，その結果を認証サーバに返す．認証サーバはアクセス許可の場合，リダイレクトによりクライアントに特定サービスサーバにアクセスさせる．認証を行わないクライアントが特定サービスサーバへ直接アクセスしてもアクセス許可機構により拒否される．アクセス許可機構は接続元 IP アドレスによるフィルタリング機能と，cookie によるフィルタリング機能の 2 つの機能から構成される．本研究では，接続元 IP アドレスによるフィルタリング機能とアクセス数制御機構の実装を行った．

3　接続元 IP アドレスによるフィルタリング機能の実装と評価

IP アドレスレベルのフィルタリングには iptables を用いた．認証サーバは，FW サーバからアクセス許可を受け取ると，クライアントの IP アドレスをリストに追加し，FW サーバに送る．FW サーバはそのリストから同一 IP アドレスを排除したサブリストを作成し，それを基に iptables に登録するように実装を行った．実装した機能が設計通りに動作するかテストを行った．

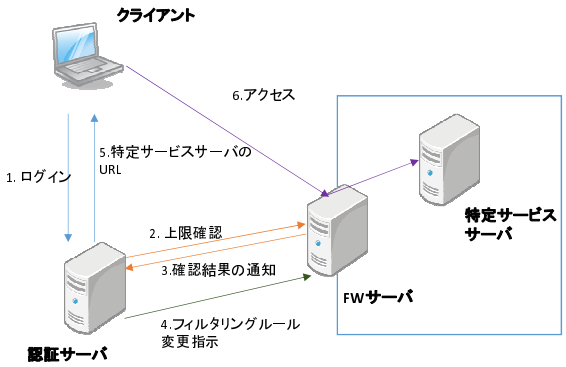

図 1: ファイアウォールを用いたアクセス制御

認証を行わずに特定サービスサーバへアクセスした時の結果を図 2 に示す．図左上赤枠に iptables に登録された通過可能な IP アドレスを，図右上緑枠にクライアントの IP アドレスを，図下部にクライアントのブラウザを表示させている．クライアントの IP アドレスは，iptables にはなく，ブラウザもアクセスができていないことがわかる．次に，認証を行った時の結果を図 3 に示す．クライアントの IP アドレスは iptables に登録され，ブラウザにも特定サービスサーバのトップページを表示され，アクセスできていることがわかる．最後に，Google Chrome と Firefox を用い，図 4 に両方で認証を行った時，図 5 に Google Chrome のみで認証を行った時の結果である．両方で認証を行った場合は青枠に示すように，同じ IP アドレスが 2 つ登録されており，両方で認証されていることがわかる．片方で認証を行った場合は 1 つのみ認証されている．いずれの場合も両方のブラウザで特定サービスサーバへアクセスできていることがわかる．

4　アクセス数制御機構の実装と評価

以下に，アクセス数制御機構の手順を示す．

1. 認証サーバから上限確認がきた時に，FW サーバは，許可を出した IP アドレスの数を見る．
2. その数が上限未満であれば認証サーバに接続許可通知を，上限であれば接続不許可通知を出す．

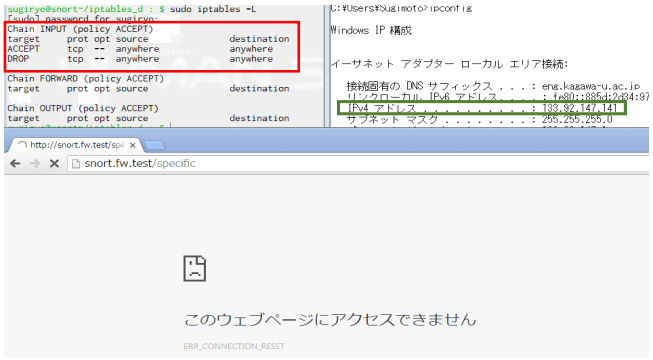

図 2: 認証無しのアクセス

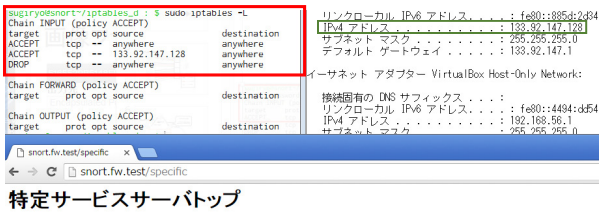

図 3: 認証有りのアクセス

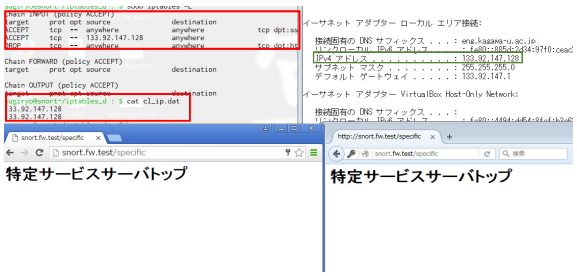

図 4: 認証有りの両ブラウザからアクセス

現時点での接続数により，接続許可，不許可通知が出され，クライアントに対して特定サービスサーバへのリダイレクトまたは接続不可の通知が行われるかのテストを行った．上限数は 5 に設定した．図 6，図 7 に結果を示す．左上部赤枠に接続許可が出ているクライアントの IP アドレスのリストを，右上部緑枠に接続要求を出しているクライアントの IP アドレスを示す．図 6 は上限である 5 台目のクライアントが認証を行った後の結果である．リストには，クライアントの IP アドレスがあり，ブラウザも特定サービスサーバの画面を出している．図 7 は，その後，6 台目のクライアントが認証を行った後の結果である．赤枠上部には認証を行う前のリストを，赤枠下部には認証後のリストを表示させているが，クライアントの IP アドレスはなく，ブラウザも上限通知が出ていることがわかる．これらより，上限数に応じてクライアント数を制御することのできる機構の実装が設計通りにできたことが

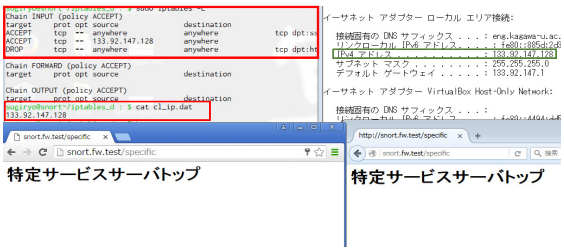

図 5: 一方のみ認証で両ブラウザからアクセス

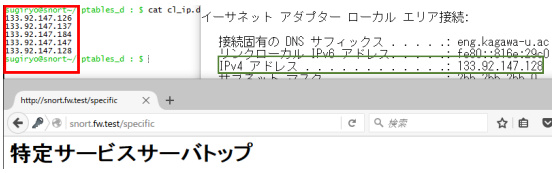

図 6: 上限未満の時のアクセス

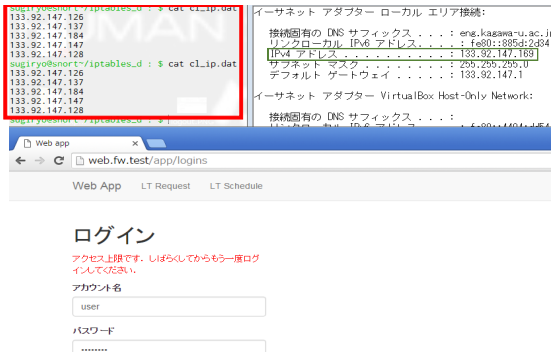

図 7: 上限時のアクセス

確認できた．

5 まとめと今後の課題

特定サービスを安定的かつセキュリティを確保するために同時アクセス数に制限をかける機構の，IP アドレスによるフィルタリング機能と，アクセス数制御機構の実装をし，動作確認を行った．その結果，設計通りの実装になっていることが確認できた．今後の課題として，IP アドレスによるフィルタリング機能と cookie によるフィルタリング機能の統合，タイムアウトによるアクセス権失効機能の実装，アクセス数制御機構の上限設定のアルゴリズムの変更が挙げられる．

参考文献

[1] 大川 昌寛，“ファイアウォールを用いた同時アクセス数制御機構の設計と機能テスト”，学士論文，2014.