ファイアウォールを用いた同時アクセス数制御機構における アクセス権管理機能の実装

13T232　近藤 裕基　（最所研究室）

1　はじめに

Web を利用したサービスの中には, 特定のサービスに対する要求を, 一定の応答性を維持したまま処理したい場合がある. このとき, サーバに対して過剰のアクセスが集中すると, 応答性が低下するという問題が発生する.

当研究室では、特定のサービスを安定的に提供するために, ファイアウォールを用いた同時アクセス数制御機構の開発を行っている. 先行研究では, システム全体の設計と cookie を用いたフィルタリング機能の実装 [1], IP アドレスを用いたフィルタリング機能とアクセス数制御機能の実装 [2] が行われた. しかし, 特定サービスの URL やサービス名などのサービス情報を登録・保持する機構が存在しないため, オンラインでサービス情報を登録できないという問題や, ユーザが自発的にログアウトしない限り, アクセス権が失効しないという問題があった. これらの問題を解決するために, 本研究では, 特定サービスの情報を管理するサービス情報管理機能と, タイムアウトによるユーザのアクセス権失効機能を実装する. また, 実装したシステムが実用に耐えうるものかを確かめるために, 複数のクライアントを用いた同時アクセス実験を行い, システムのオーバヘッドを評価する.

2　システム構成

この機構は, 認証サーバ (Auth サーバ) 上のユーザ認証機能, IP フィルタリングサーバ (IPF サーバ) 上のアクセス数制御機能と IP アドレスによるフィルタリング機能, クライアント識別サーバ (CI サーバ) 上の cookie を用いたフィルタリング機能から構成される. 以下に, 特定サービスサーバ (SS サーバ) への最初のアクセスまでの同時アクセス数制御機構での処理の流れを示す.

(1) ユーザが Auth サーバにアクセスし, ログインを行なう. Auth サーバは, 認証に成功した場合は次に進み, 失敗した場合は認証失敗の通知を出して, 再入力を促す.

(2) Auth サーバは, IPF サーバに現在のアクセス数を確認する.

(3) IPF サーバは, 現在のアクセス数が上限に達していないか確認し, Auth サーバにアクセスの可否を返す.

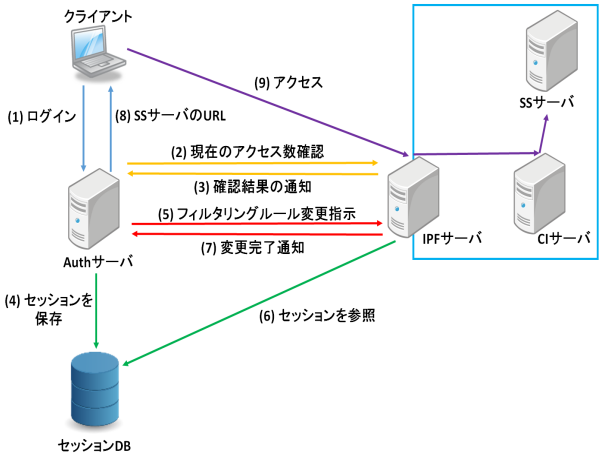

図 1: 同時アクセス数制御機構の構成

(4) Auth サーバは, アクセス許可が返ると, クライアントのセッション情報をセッション DB に保存したあと次に進み, アクセス不許可が返ると, クライアントにアクセス上限通知を返す.

(5) Auth サーバは, IPF サーバにフィルタリングルールの変更指示を出す.

(6) IPF サーバは, セッション DB の登録情報に基づいてフィルタリングルールを変更して, クライアントのアクセスを許可する.

(7) IPF サーバは, Auth サーバに変更完了通知を返す.

(8) Auth サーバは, クライアントに対して, 許可を示す cookie を生成し, セッション DB に保存したあと, SS サーバの URL とともにクライアントに返す. これによりクライアントは渡された cookie を伴って SS サーバにリダイレクトする.

(9) IPF サーバは, クライアントからのアクセスを通過させる. CI サーバでは, セッション DB を参照し, クライアントからの cookie が許可されたものであることを確認して, SS サーバにリダイレクトする.

3　サービス情報管理機能

サービス情報管理機能は, 特定サービスのサービス情報の閲覧, 登録, 及び編集を行なうための機能である. この機能は, 特定サービスの管理者と本機構の管理者 (root) のみが利用できる. 特定サービスの管理者が自分のサービスに対する操作しかできないのに対して, root は全てのサービスに対する操作ができる.

サービス情報は, サービス名・最大利用時間 (分)・最大利用間隔 (分)・サービス URL・管理者 ID の 5 つの項目で構成される. サービス名は, 本機能においてサービスを一意に識別するために用いる. 会話的な処理は図 2 に示すようにサービスを開始してから複数回のやりとりを行なう. 最大利用時間は利用時間の上限を与え, 最大利用間隔は利用間隔 (やりとり間の間隔) の上限を与え, いずれかの上限を超えるとアクセス権は失効する. サービス URL は, ユーザ認証後のリダイレクト先の URL である. さらに, サービスの情報を登録した管理者ユーザの ID を, そのサービスの管理者 ID として登録する.

図 2: サービス利用時間と利用間隔

サービス情報管理機能は, サービス情報管理ページ, サービス情報登録ページ, 及びサービス情報編集ページを通じて特定サービスの情報を管理する. サービス情報管理ページは, ログイン中の管理者ユーザが管理しているサービスの情報が一覧表示される. root でログインしている場合は, 登録されている全てのサービス情報が表示される. サービス情報登録ページは, 上記の 5 項目を入力してサービス情報を登録することができる. サービス情報編集ページは, サービスの管理者及び root のみがアクセスでき, 各項目の内容を編集することができる.

4　アクセス権失効機能

ユーザはログイン時, 認証と同時に利用するサービスを選択する. 選択されたサービスの最大利用時間 (分) を現在の時刻に加えたものが有効期限として設定され, IP アドレスや cookie と合わせてセッション情報としてセッション DB に保存される.

Auth サーバは 1 分ごとにセッション DB 内のセッション情報を確認する. 各セッション情報の有効期限と現在時間を比較し, 期限の過ぎているセッション情報を削除する. 確認後, Auth サーバは IPF サーバにフィルタリングルール変更指示を出す. IPF サーバはセッション DB の内容に従いフィルタリングルールを変更する. この変更によって, 有効期限の切れたクライアントのアクセス権は失効する.

5　システムのオーバヘッドの評価

システムのオーバヘッド (処理時間) を評価するために, クライアント 1 台〜5 台で同時アクセスを 1000 回行い, システムの処理時間を測定して比較する. 処理時間は, ユーザ認証及びフィルタリング設定の処理時間と, SS サーバへのアクセス時間の 2 つに分けて測定する. クライアントが Auth サーバにアクセスしてからリダイレクトされるまでの時間を T1, クライアントが IPF サーバにアクセスしてから SS サーバへのアクセスが完了するまでの時間を T2 とし, T1 と T2 を合計した時間 T を求める. なお, 本研究では CI サーバを研究対象としていないため, 実験では IPF サーバを通過すると直接 SS サーバにアクセスしている.

実験結果を表 1 に示す. 合計時間 T の平均時間は最大 1.6 秒ほどであり, 分散はごく小さい値を示している. これは, T が 1.0 秒〜1.6 秒に集中しているためである. また, 表 1 を見ると, T の値のうち大部分は T1 が占めていることが分かる. T1 はサービス利用開始のための認証アクセスに必要な時間である. 認証後はアクセス権が失効するまで, 認証サーバを経由せずに SS サーバにアクセスするため, 表 1 の T2 の平均値にあるように約 0.01 秒程度で SS サーバにアクセスできる. これらのことから, 本システムは実用に耐えうるものであると判断できる.

表 1: アクセスに要する時間

クライアント	1 台	2 台	3 台	4 台	5 台
T1 の平均 (s)	1.025	1.190	1.241	1.327	1.582
T2 の平均 (s)	0.008	0.010	0.012	0.012	0.010
T の平均 (s)	1.033	1.200	1.252	1.339	1.592
T の分散	0.001	0.092	0.099	0.149	0.246

6　今後の課題

現在, 固定のアクセス上限値を用いて, アクセス数制御を行っている. この設定では, サーバの負荷量によって, サーバが応答性を維持できる状態でもアクセス不可通知が出たり, 過負荷状態であるにも関わらずアクセス許可通知が出る可能性がある. そのため, サーバの負荷量に応じてアクセス可否を判断するようなアルゴリズムを実現する必要がある.

参考文献

[1] 大川 昌寛, 大川昌寛, 最所圭三 : “ファイアウォールを用いた Web サーバのための同時アクセス数を動的に制御するアクセス制御機構の設計”, 情報処理学会第 77 回全国大会講演論文集, 5X-4, pp.3-169 - 3-170, 2015.

[2] 杉本 亮太, “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”, 香川大学, 卒業論文, 2015.