同時アクセス数制御機構におけるユーザ認証機能の改良

14T241 柴原 涼 （最所研究室）

特定サービスに対して, 同時アクセス数を制御するシステムの改良について述べる.

1 はじめに

当研究室では, 特定のサービスを安定的に供給するための, ファイアウォールとクライアント毎の識別を行う機構を組み合わせたアクセス制御機構の開発を行っている. この機構により, 特定サーバ (特定サービスサーバ) への同時アクセス数を制御できるだけでなく, ファイアウォールにより許可した IP アドレスを持つクライアント以外からのアクセスを防ぐことができ、Dos 攻撃にも対応できる. また,NAT 環境からや proxy サーバを経由したアクセスでは，異なるクライアントが同一の IP アドレスからアクセスしたようにサーバでは見えるが，クライアント毎の識別機構により，許可のないクライアントからの特定サービスサーバへのアクセスをブロックできる.

先行研究では,Cookie によるクライアントの識別, 複数の特定サービスへの対応, 有効期限設定によるアクセス権執行機能が実装されているが、いくつかの管理データベースがファイアウォール外に置いたことからセキュリティ面に不安があった.

本研究では, セキュリティ向上, サービス提供の安定性の向上を目指し, サービスの応答性の評価などを行う. 本稿では, 同時アクセス数制御におけるユーザ認証機能の改良について述べる.

2 同時アクセス数制御機構

先行研究における同時アクセス制御機構の構成を図 1 に示す. ユーザ認証を行う認証サーバ (Auth サーバ),IP アドレスによるフィルタリング機能を提供するファイアウォールである IP フィルタリングサーバ (IPF サーバ), クライアントを識別し許可されていないクライアントからのアクセスを拒否するサーバ (CI サーバ), 特定サービスを提供するサーバ (SS サーバ) で構成している. SS サーバにアクセスするのは,IPF サーバと CI サーバを必ず経由する. SS サーバへのアクセス手順は以下で行う.

クライアントは Auth サーバでユーザ認証を行う. 認証に成功すると IPF サーバに同時アクセス数が上限に達していないか問合せを行う. 上限に達していなければ, セッション DB に登録を行い, フィルタリングルールの変更を行う. IPF サーバは, セッション DB を参照して許可するクライアントを設定する. 許可されたクライアントは,SS サーバの URL を受け取りアクセスをする. IPF サーバでは,IP アドレスによるフィルタリングを行い, 許可されたアクセスは IPF サーバを通過する. 通過したアクセスに対して,CI サーバは許可して良いクライアントからのアクセスであるかどうかをセッション DB を参照し,haka と呼ばれるツールを用いて判別する. アクセスを許可されたクライアントからであれば,SS サーバにアクセスし, 結果をクライアントに返す.

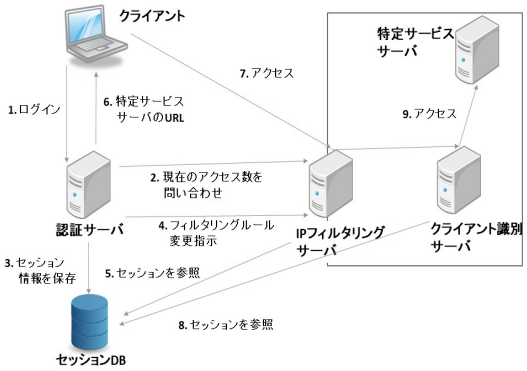

図 1: 同時アクセス数制御機構の構成

Auth サーバが持つ機能

- ユーザ認証
- Cookie の発行とセッション DB への保存
- 有効期限によるアクセス権失効機能
- クライアント数の管理

IPF サーバが持つ機能

- 同時アクセス数確認によるアクセスの可否
- IP フィルタリング

3 同時アクセス数制御機構の改良

現在の構成では, 認証情報のある DB やセッション DB が Auth サーバにあるためセキュリティ的に改善が必要である. また,Auth サーバが攻撃の対象になり

機能しなくなるとサービスを提供することができなくなってしまうため, Auth サーバの冗長化が必要である. これらの問題を解決するための手法として, 以下の 2 つの手法が考えられる.

1 つ目の手法は, 複数の認証サーバに対応するために, 同時アクセス数を一括で管理する方法である (手法 1). 認証は, 認証サーバで行うが, セッション DB をファイアウォールで保護された場所に置き, セッションの情報を一括管理することで認証サーバの冗長化に対応する.

2 つ目の手法は、ファイアウォール内に実際に認証を行う実認証サーバを置き, 従来の認証サーバを実認証サーバへのリバースプロキシサーバとして稼働する方法である (手法 2). これにより, ファイアウォール外に DB を置くことによるセキュリティ問題を解決できる. 以下, それぞれの手法の詳しい説明を行う.

3.1 手法 1

1 つ目の手法は, 今のシステムを複数の Auth サーバに対応するように改良する方法である. このまま Auth サーバを複数にしてしまうと, 他の Auth サーバと同時アクセス数を同期することができない. 同時アクセス数を,IPF 内のサーバで一括管理することで, 他の Auth サーバとの同期もとることができる.

以下に,Auth サーバと IPF サーバ内のサーバが持つ機能についてまとめる.

Auth サーバが持つ機能

- ユーザ認証

IPF サーバが持つ機能

- 同時アクセス数確認によるアクセスの可否
- Cookie の発行とセッション DB への保存
- IP フィルタリング
- 有効期限によるアクセス権失効機能
- クライアント数の管理

クライアント数の管理を一括管理することで, 複数の Auth サーバでの同期に対応することができる. しかし, 認証情報の DB が IPF サーバ外に存在することによるセキュリティに問題が残る.

3.2 手法 2

2 つ目の手法は, ファイアウォール内に実際に認証を行う実認証サーバを置き, 従来の Auth サーバを実認証を行うサーバへのリバースプロキシサーバとして使う方法である. 複数の Auth サーバ間の同期問題を解決できる. また, 実認証サーバも IPF 内に置くことで手法 1 よりもセキュリティを向上できる.

以下に,Auth サーバと IPF サーバ内の認証サーバが持つ機能についてまとめる.

Auth サーバが持つ機能

- リバースプロキシ

IPF サーバが持つ機能

- 同時アクセス数確認によるアクセスの可否
- IP フィルタリング

実認証サーバが持つ機能

- ユーザ認証
- Cookie の発行とセッション DB への保存
- 有効期限によるアクセス権失効機能
- クライアント数の管理

これにより, 複数の Auth サーバでの同期については一括管理されているので解決することができる. また, 全ての DB を IPF サーバ内のサーバに置くことができるのでセキュリティ的にも安全と言える.

4 今後の課題

提案した機能の実装

設計を行った段階なので, 実際に実装を行い正しく機能するか問題がないか確認する.

最適な手法を決定するための評価実験

2 つの手法を実際に実装して, アクセスに掛かる時間などの評価を行い, どちらが最適化について検討を行う.

同時アクセス数が上限に達しているときの対応

同時アクセス数が上限に達している場合でも,IPF サーバに問合せをしてしまい, 無駄な通信を行ってしまう. 上限に達している場合には, 問合せをしないようにする.

参考文献

[1] 利根 大樹, ” 同時アクセス数制御機構におけるクラインと識別機構の開発”, 香川大学, 学士論文, 2016

[2] 近藤 裕基, ” 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”, 香川大学, 学士論文, 2016