SSL フェイルオーバの提案

島崎 聡史† 中澤 昌史† 金田 健太郎†† 黒羽 秀一†† 齋藤 孝道†
†明治大学 ††明治大学大学院

1 はじめに

インターネットの普及に伴い，Web を通じて電子商取引など様々なサービスが提供されるようになった．その一方で，Web 上を流れる個人情報の盗聴や改竄，ユーザの成りすましなどの脅威も多数存在している．そこで，その対策として SSL (Secure Socket Layer) やその後継にあたる TLS (Transport Layer Security) (以降, 併せて SSL と呼ぶ) が広く利用されている．その依存が高まる一方で，例えば，サーバ停止によってシステムが停止してしまうと，電子商取引では商業機会を逸することになりかねない．そこで，予め，本番稼動機とは別にバックアップ機を用意しておき，サーバが 1 台停止したとしても，システム全体としての停止は回避できる方法の一つとして，フェイルオーバと呼ばれる技術がある．

しかしながら，SSL 通信では，暗号アルゴリズムや，暗号化や復号に用いる暗号鍵などのセッション情報をサーバ，クライアント間で共有する必要があり，既存のフェイルオーバの技術では，そのセッション情報をサーバ間で共有できないため，フェイルオーバ後に改めてセッション情報を構築する必要がある．

そこで，本論文では，SSL のセッション情報を複数のサーバ間で共有することにより，フェイルオーバを行うシステムの提案と実装を示す．

2 OpenSSL におけるセッション再開

2.1 セッション再開

セッション再開とは，サーバとクライアントとの間で以前に確立したセッションがある場合に，その際のセッション情報を利用して，再度通信を再開することをいう．はじめからセッション情報を構築する FullHandshake に比べ，以前に共有したマスターシークレットを利用しているので，マスターシークレットを生成する分の処理を省略することができ，処理コストが小さくて済む．

2.2 SSL_SESSION 構造体

OpenSSL[2][3] では，SSL_CTX 構造体，SSL 構造体や SSL_SESSION 構造体などからなる構造体群で通信の状態や構築したセッション情報などを管理している．その構造体のうち，SSL_SESSION 構造体は，セッション ID やマスターシークレット，セッション ID コンテキストなどセッション再開を行うのに必要な情報を格納している．

3 提案システム

3.1 概要

提案システムでは，平常時にクライアントからの HTTPS リクエストに応答する Active サーバと，Active サーバの停止時に応答する Standby サーバとの間で，セッション情報*を共有する．Active サーバの停止時も Fullhandshake をすることなく，セッション再開により Standby サーバがクライアントに応答することができる．

3.2 主体構成

提案システムは，上述の Active サーバと Standby サーバからなり，図 1 に示すネットワークトポロジで構成した．

Active サーバ

本番系の SSL-Web サーバである．クライアントとの間でセッション情報を構築した際に，Standby サーバにそのセッション情報を通報し，共有する．Apache1.3.39-mod_SSL2.8.30[1] を修正して実装した．

Standby サーバ

Active サーバが停止した際に応答をする待機系の SSL-Web サーバである．平常時は，Active サーバからの通報を受信し，格納する．Active サーバが停止したときは，処理を引き継ぎ，応答をする．同じく Apache1.3.39-mod_SSL2.8.30 を修正して実装した．

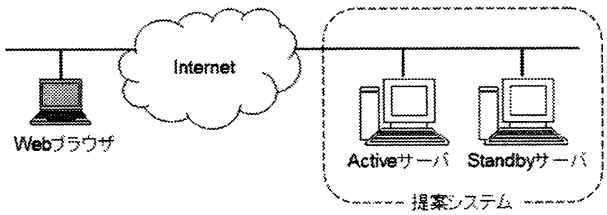

図 1: 提案システムのネットワークトポロジ

3.3 提案システムの詳細

3.3.1 Apache のセッションキャッシュモード

Apache mod_SSL では，プロセス間でセッション情報を共有するために，それをデータベースファイルに書き出すモードと，共有メモリに書き出すモードの 2 種類がある．今回はそのうち，データベースファイルに書き出すモードを用いた．

† Satoshi SHIMAZAKI, Masashi NAKAZAWA, Takamichi SAITO
†† Kentaro KANEDA, Shuichi KUROBA
Meiji University (†)
Graduate School of Meiji University (††)
1-1-1, Higashimita, Tama-ku, Kawasaki-shi, Kanagawa, 214-8571, Japan

* 以下，マスターシークレットなどセッション再開に必要な情報をセッション情報と呼ぶことにする．

データベースファイルには，セッションIDを検索キーとして，ASN.1フォーマットのSSL_SESSION構造体と当該セッションの有効期限を格納している．

3.3.2 通報

提案システムでは，セッション情報を共有するため，Activeサーバから Standbyサーバへ，以下の通報を送信する．

```
Struct{
    Session_id
    SSL_SESSION ASN.1 converted
}
```

ただし，SSL_SESSION ASN.1 convertedとは，SSL_ASN.1フォーマットのSSLSESSION構造体であり，セッションID，マスターシークレット，セッションIDコンテキストなどを含む．

3.3.3 生存確認と仮想IP

Standbyサーバは，Heartbeat[4]を用いて，定期的にActiveサーバの生存を監視している．Activeサーバが生存している間は，Activeサーバが，仮想IPを利用してクライアントからのリクエストを待ち受け，Activeサーバの停止時は，Standbyサーバが，代わりにその仮想IPを利用してクライアントからのリクエストを待ち受ける．

3.3.4 mod_SSLの変更点

Activeサーバ

Apache mod_SSLがクライアントとの間で構築したセッション情報をデータベースファイルに格納する部分に，通報を送信する処理を追加した．

当該部分では，格納しようとするSSL_SESSION構造体から情報を抜き出して通報を作成し，Standbyサーバに送信する．

Standbyサーバ

Apacheを親プロセスとした，通報受信専用のプロセスを用意し，Activeサーバからの通報を待ち受けるようにした．受信プロセスは，通報を受信すると，セッションIDを検索キーに，SSL_SESSION ASN.1 convertedをデータベースファイルに格納する．

3.4 動作例

提案システムの障害発生時の動作例を図2に示す．なお，図中の番号は以下の説明のそれに対応しており，破線はHeartbeatによる生存確認の様子を表している：

(1) WebブラウザがHTTPSリクエストを送信する
(2) Activeサーバは FullHandshake後，セッション情報をStandbyサーバに送信する
(3) Standbyサーバは，受け取ったSSL_SESSION構造体の情報をデータベースファイルに格納する
(4) Activeサーバから Webブラウザへレスポンスを送信する

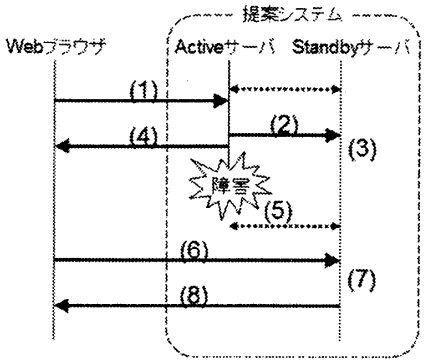

図 2: 提案システムの動作例

(5) Activeサーバに障害が発生した場合
Standbyサーバは，Heartbeatによって Activeサーバの生存を確認できなくなると，仮想IPによって Webブラウザに応答サーバとなる
(6) Webブラウザが再び HTTPSリクエストを送信する
(7) 格納していた情報を利用し，セッション再開を行う
(8) Webブラウザへレスポンスを送信する

4 まとめ

本論文では，SSLのセッション情報を複数のサーバ間で共有することにより，セッションの再構築を経ずにフェイルオーバを行うシステムの提案と実装を示した．

提案システムでは，FullHandshakeの完了後に，そのSSL_SESSION構造体の情報を Standbyサーバに通報するため，その通報が完了するまでに Activeサーバが停止した場合，フェイルオーバを行うことができない．そこで，今後の課題として，任意のタイミングでフェイルオーバができるように発展させることなどが考えられる．

参考文献

[1] The Apache Software Foundation, http://www.apache.org/

[2] The OpenSSL Project, http://www.openssl.org/

[3] John Viega,Matt Messier,Pravir Chandra 共著 齋藤孝道 監訳 "OpenSSL 暗号・PKI・SSL/TLS ライブラリの詳細" オーム社

[4] The High Availability Linux Project, http://linux-ha.org/ja/HomePage/