SSL 暗号通信の通過制御に関する一考察

5N－6

佐久間 剛*　河田 悦生**
NTT 第一法人営業本部*　NTT 情報通信研究所**
e-mail : t.sakuma@ntt.co.jp , kawada@dsa.isl.ntt.co.jp

1. はじめに

インターネットの利用は、近年急激に増加して、その利用方法も研究開発のみでなく企業の業務・一般家庭での利用と広範囲に利用されるようになってきている。企業で社内ネットワーク(内部 LAN)をインターネットに接続する場合、不正なアクセスなどによる重要情報の漏洩・破壊を防ぐためファイアウォール(防火壁)を設け通過するデータを制御している。しかし、暗号通信(SSL 暗号通信など)の場合、OSI モデルの上位レイヤー部分が暗号化されているため、平文での通信に比べファイアウォールで十分な通過制御を行うことができずこの結果、内部サーバが直接外部に曝されやすい問題点がある。

本稿では、この問題点を解決するために、ファイアウォールが持つパケットフィルタリング機能・アプリケーションゲートウェイ機能を活かした暗号通信の通過制御技術について検討した。

2. 暗号通信時の問題点

ファイアウォールは、パケットフィルタリング機能・アプリケーションゲートウェイ機能でデータの通過制御を行い許可されたアクセスのみを内部 LAN に接続することでインターネットからの不正アクセスなどの攻撃を防御している。しかし、暗号通信の場合データが暗号化されているためファイアウォールではパケットフィルタリング機能である IP アドレスの通過制御しかできず、DoS 攻撃や不正データの侵入を防ぐことができない。

3. モデル考察

WWW で広く使用されている HTTPS の通信方法であり、サーバ・クライアント間を１対１で暗号通信する SSL 暗号通信におけるファイアウォールの効率的な通過制御方法のモデルを考察した。

ファイアウォールのサブネット上に、SSL 接続要求をするクライアントに対して、サーバに代わり暗号・復号応答する「SSL 代理応答システム」を考案した。このシステムによりクライアントからの暗号通信データは、サーバまで直接送信されずにいったん代理応答システムで受けて平文に復号化した後にファイアウォールを再度通過させてサーバに送信される。これによりファイアウォール上でアプリケーション層の通過制御が可能となる。(図１)

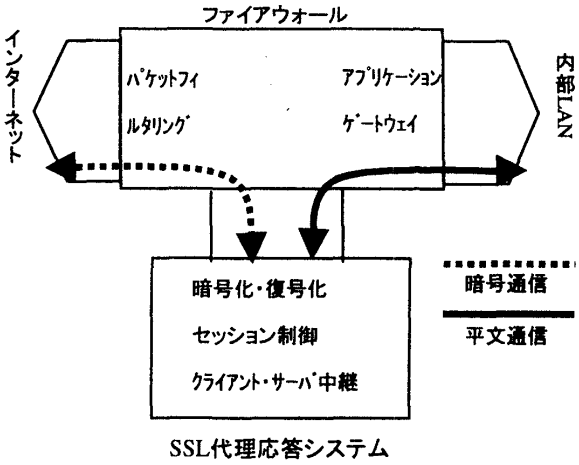

図１　SSL 代理応答システムモデル図

4. モデル実装

本モデルのプロトタイプを開発し実装した。プロトタイプは、クライアントからの接続要求が SSL であることを確認しセッションが確立してからサーバへコネクションを行いデータを転送する。(図２、３)

主な特徴は、以下の通りである。

A study on Access Control for SSL communications
Tsuyoshi SAKUMA*, Etsuo KAWADA**
NTT Business Communication Headquarters I*
NTT Information and Communication Systems Labs. **

・１プロセスにサーバの IP アドレスと代理応答用の IP アドレスを設定する。複数プロセスを起動することで複数サーバに対応できる。
・インターネット側には代理応答システムの IP アドレスのみを公開する。
・クライアントからサーバへのアクセス毎に子プロセスを起動して通信状態を制御する。
・クライアントから送信されてきた暗号データを復号化してサーバへ送信する
・サーバからクライアントに送信する場合データを暗号化して送信する。
・SSL 代理応答システムはサーバの証明証、秘密鍵を譲り受け暗号認証通信をする。
・許可した（プロセスで設定した）IP アドレス、ポート番号以外への接続は拒否する。

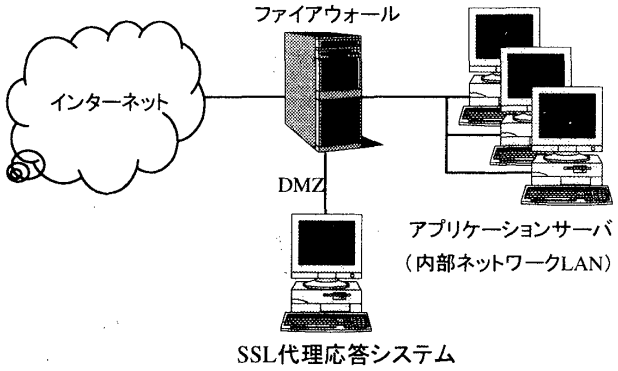

図２　ハードウェア構成図

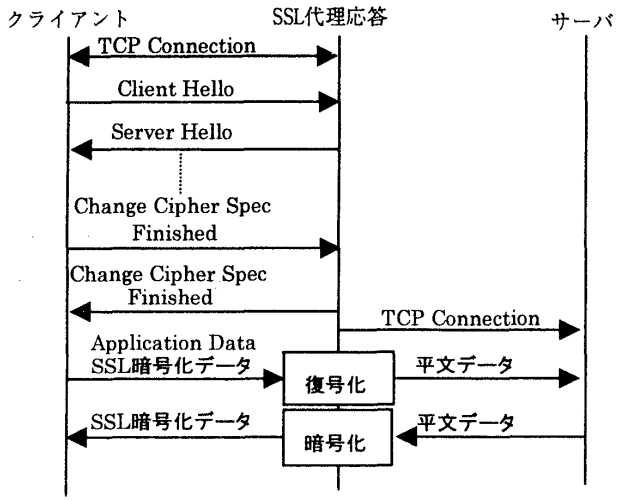

図３　データ処理フロー図

5. モデル評価

本モデルにより今まで暗号により通過制御できなかったセッション層の通過制御ができる。さらにファイアウォールの機能を利用することでアプリケーション層の通過制御ができる。（図４）

また、SSL 暗号通信機能を持たないサーバも本システムにより外部に対して SSL 暗号通信が可能になる。

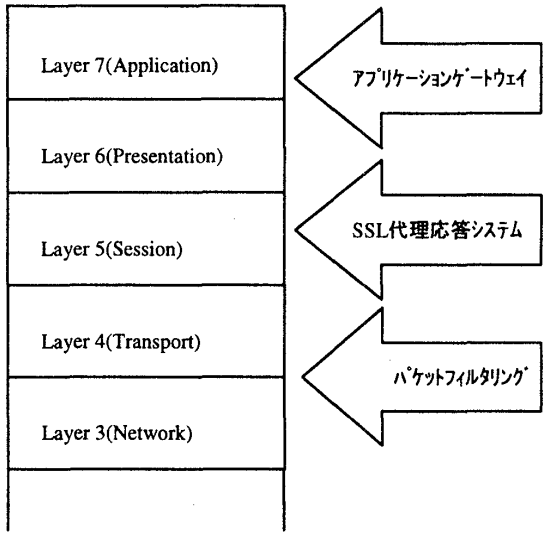

図４　各機能の通過制御部分

6. まとめ

本論文では、SSL 通過制御方式の一考察として SSL 代理応答システムについてモデルを提案した。本モデルにより SSL 暗号通信におけるファイアウォールの機能を効率的に活用した通過制御が可能となる。

今後の課題として、実環境などにおける性能検証および機能確認を行う。さらに内部ネットワークで平文に復号化するためトータル的なネットワークセキュリティとしてのトレードオフを検討（ネットワーク構成との関係）する必要がある。

7. 謝辞

本研究は、通信・放送機構（TAO）委託研究「電子マネーの伝送技術に関する研究開発」の課題イ「電子マネーの伝送特性に着目したファイアウォール通過制御技術の研究開発」の一環で行われたものである。