通信制限システムの Web 経由での安全な遠隔操作

2006MI096 松永 龍太朗
指導教員　後藤 邦夫

1　はじめに

近年，インターネットでは，DoS 攻撃や迷惑メール等の迷惑行為が増加している．

後藤研究室では，この問題の対策手段として「段階的通信制限システム」(以下，既存手法または GK とする [4]) の開発をしてきた．本研究では，GK へのアクセス時の認証方法とフィルタリングルールの操作方法を改良することで，外部ホストから GK への Web を経由した安全確実な遠隔操作の実現を目標とする．

既存手法ではパスワードで外部ホストの認証をしているが，パスワードの入力は最初の通信時のみで，ホストの識別もできない．本研究では SSL クライアント認証を利用し，毎回の SSL 通信時にホストを認証することで安全性を高めることができると考えた．また，XML で操作情報を記述し，サーバでデータの妥当性を検証することで，正確な操作を実現できると考えた．

2　システムの概要

本節では, 既存手法と本研究で提案する手法の概要, 本研究で利用する SSL クライアント認証について述べる．

2.1　既存手法の構成と処理の流れ

既存手法の構成を図 1 に示す．GK では受信したパケットに任意の通信制限を起こすことができる．外部ホストは Commander にアクセスし，フィルタリングルール操作の依頼をすることで，任意の通信制限を起こす．

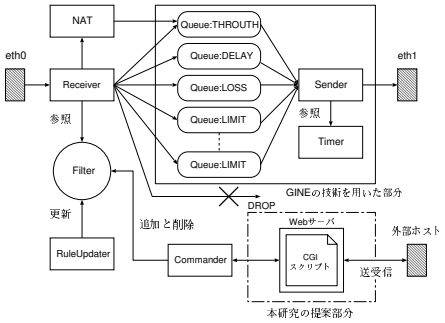

図 1　GK の構成

2.2　提案する手法の概要

本研究では一台の PC に Web サーバと私設の認証局 (以下 CA(CertificateAuthority)) を構築し，それらを利用して SSL クライアントを認証する．GK も同 PC で稼働させ，外部ホストから GK の Commander へは Web サーバから呼び出した CGI スクリプトを介してアクセスする． そのさい，本研究では GUI 環境がないホストからの Web サーバへのアクセスは wget を利用する．

以下に本研究の全体の処理の流れを示す．

1. 外部ホストは Web ブラウザや wget で Web サーバにアクセスし GK の操作情報を送信.
2. Web サーバは正規のクライアント証明書をもったホストが https アクセスした場合のみアクセスを許可し，CGI スクリプトに操作情報を送信.
3. CGI スクリプトで XML を検証し，妥当な XML であれば GK の Commander に操作情報を送信. 定義に違反していたらエラーメッセージを出力.
4. GK の Commander は受け取った操作情報にしたがいフィルタリングルールを操作.

2.3　SSL クライアント認証

SSL クライアント認証とは，サーバに SSL で接続するさい，特定の CA が発行した証明書を提示したクライアントに対してのみサーバへのアクセスを許可する仕組みである．それぞれの関係図を図 2 に示す．

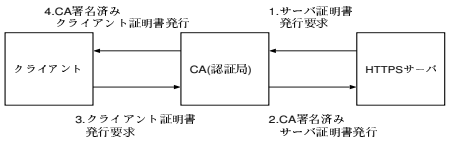

図 2　認証局等の関係

図 2 のようにクライアントとサーバが同一の CA によって認証される．これにより，毎回の通信時に，サーバが信用する認証局が署名した証明書をクライアントが提示した場合のみ，SSL 接続が確立する．また，クライアント証明書ごとに CommonName(以下, CNAME) を指定し，この CNAME でクライアントを識別する．クライアントが Web ブラウザでのアクセス時に証明書を利用する場合は，ブラウザに読み込ませて利用する．また，wget でのアクセス時はコマンドオプションで証明書ファイルを指定して利用する．

3　システムの実現

本研究で提案するシステムを実現するための Web サーバの設定，XML タグでの操作情報の定義，CGI スクリプトについて述べる．

3.1　Web サーバ

本研究では Apache2[1] を用いて Web サーバを構築した．本研究で Web サーバを構築する際に重要な設定は SSL 通信に関する設定である．SSL に関する設定はすべて '/etc/apache2/sites-available/default-ssl' 内で VirtualHost ディレクティブを利用した．

3.2　XML によるコマンド定義

本研究では，外部ホストは XML タグで記述した操作情報を CGI スクリプトに送信し GK を操作する．本研究で XML タグで定義した操作情報例を以下に示す．

```
<filtering_rule>
  <add>
```

```
    <direction></direction>
    <action></action>
    <protocol></protocol>
    <src_info></src_info>
    <dst_info></dst_info>
    <option></option>
  </add>
</filtering_rule>
```

操作に必要な情報は既存手法と同じだが，必ずしも必要でない情報は<option>要素とし，省略可能とした．

また，本研究ではデータの構造を定めるスキーマ言語の DTD で XML の構造を定義した．DTD では XML 文書中で使われるタグの登場回数や，位置，要素の種類等を定義できる．次節で説明する CGI スクリプト中でこの DTD で XML データを検証する．この DTD の定義通りの XML でなくては検証を通過できない．

3.3 CGI スクリプト

本研究では Perl で CGI スクリプトを記述し，XML 解析用 parser には Perl のアーカイブ CPAN[2] よりインストールした XML::libXML モジュールを使用した．

以下に大まかな処理の流れを示す．

1. 外部ホストから送信された XML を取得.
2. XML 検証用 parser を指定し，XML を読み込み検証.
3. DTD の定義に反していたらエラー文を出力，満たしていたら各要素を抽出し変数に代入.
4. 操作の種類ごとに場合分けし，それぞれの仕様に合わせた文字列に変換.
5. TCP ソケットを使い GK の Commander に接続し，変換した文字列を送信.
6. Commander からの返信文を受け取り，出力.

4 実験

本節では本研究で提案したシステムの動作実験をし，その結果を述べる．

4.1 実験環境の構成

図 3 に実験環境の構成を示す．本研究では Ubuntu Linux8.10(32bit OS) をインストールした PC を 2 台用意し，1 台は GK や Web サーバをインストールしたシステムホストとし，1 台はシステムにアクセスする外部ホストとした．また，後藤研究室のネットワークエミュレータ GINE[3] の仮想ホスト機能で HostA，HostB を構築し，HostA と HostB の間で GK を動作させた．

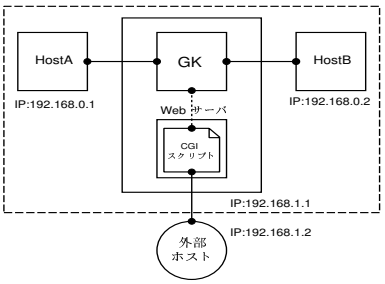

図 3　実験環境の構成

4.2 実験結果

前節で構築した実験環境にて実験をする．まずは，アクセス実験である．この実験で正規の外部ホストのみが CGI スクリプトにアクセスできることを確認する．この実験では，サーバで登録済みの CNAME の証明書を持つホストが HTTPS アクセスした場合のみアクセスに成功した．それ以外の場合はエラーメッセージが表示され，Web サーバや CGI スクリプトにアクセスすることはできず，期待どおりの結果となった．

次に CGI 動作実験で，CGI スクリプトで正しく XML の検証がされ，GK を操作できるか確認する．

表 1　CGI 動作実験結果

XML	結果
妥当な XML	GK の操作成功
要素名ミス	エラー行とエラー要素の出力
必要な要素の欠如	エラー行と欠如要素の出力
要素の順番ミス	エラー行と取得した順番の出力
option 要素の省略	GK の操作成功

表 1 は実験結果である．DTD の定義を満たしていない XML の場合はエラー箇所と原因が出力され，GK の操作をすることはできず，期待どおりの結果となった．

5 おわりに

本研究は GK を外部ホストから Web を介して安全に遠隔操作することを目的とした．そのために外部ホストの認証に Web サーバを利用した SSL クライアント認証を実装し，フィルタリングルールの操作情報は XML で定義した．これらにより，外部ホストからの GK の遠隔操作時の安全性と確実性の向上が見込めた．しかし，本研究で Web サーバの構築に利用した apache はソフトウェアの規模が大きく，本研究の使用用途では無駄になる部分もある．よって今後は，GK に専用のコンパクトなサーバを組み込み，本研究で apache を利用して実装した機能を追加すれば，より良いシステムになると考えられる．

参考文献

[1] The Apache Software Foundation (Accessed June 2009). http://www.apache.org.

[2] Comprehensive Perl Archive Network (Accessed November 2009). http://www.cpan.org.

[3] Sugiyama, Y. and Goto, K. (Eds. Zhang, S. e. a.: Design and Implementation of a Network Emulator using Virtual Network Stack, *Proc. of the Seventh International Symposium on Operations Research and Its Applications (ISORA2008)*, World Publishing Corporaiton, pp. 351–358 (2008).

[4] 中西忠夫，坂口由佳：段階的通信制限システムの拡張 (卒業論文)，南山大学数理情報学部 情報通信学科 (2009).