マルチメディア通信と分散処理 77－11
（1996．7．12）

SNMPを用いたファイアウォール管理エージェントの構築

泉 裕 井上博之 山口 英

奈良先端科学技術大学院大学

内容梗概

インターネット接続ではファイアウォールを導入することが一般的になっており、様々なプロダクトが使われるようになってきた。しかしながら、現在のファイアウォールには、不正侵入等の異常状態の発見と検出、その報告の機能が不足している。これらの機能は、より安全なファイアウォールの運用に必須の機能であり、これらの機能の実現が求められてきた。本研究では、これらの機能を既存のファイアウォールに付加するシステムを提案する。このシステムは、ファイアウォールの設定と、異常状態の検出を行うファイアウォール・エージェントとして実現されている。さらに、異常状態の報告にはSNMPの機構を採用しており、既存の管理システムとの親和性を高めている。本論文では、ファイアウォール・エージェントの設計・実装と、SNMPインタフェースを実現するために開発したファイアウォールMIBの概要について報告する。

Design and Implementation of Firewall Agent using SNMP for Firewall Management

Yutaka Izumi Hiroyuki Inoue Suguru Yamaguchi

Nara Institute of Science and Technorogy,Ikoma, Nara, JAPAN

Abstract

It becomes popular to use "firewall" to set up the Internet connection. Various kinds of both commercial products and freewares of "firewall" are available. However, many of these products do not have vital functions for network management: detection of attacks such as intrusions and reporting them to network management stations. In order to add these functions to firewalls, we propose an add-on system called "firewall agent." Without any modifications on firewalls, the firewall agent provides functions for both detection and reporting of attacks against firewalls. For its reporting fuction, we developed firewall MIB and its SNMP interface in the agent, therefore, it is easy to integrate the agent into the current Internet management architecture. In this paper, design and implementation of the firewall agent are shown.

1 はじめに

インターネットは、計算機能力の向上や通信回線の高速化および異機種間の通信技術の発展を背景として急激な成長を遂げ、将来においても、インターネットに接続するホスト台数は指数関数的な増加が予想されている。インターネットの発展とともに、インターネットにおいて提供されるサービスにも変化が見られる。従来の電子メールやニュースシステムなどのテキストベースのサービスだけでなく、WWW(World Wide Web)などのマルチメディア情報(映像,音声)を主流とした、様々なサービスの利用、提供が増加している。これらの情報発信の技術を有効に利用しようと、企業も商用目的としてインターネットに積極的に接続するようになった。

インターネットに接続する際、企業や研究機関は、組織内の重要な情報を守るために防火壁(以下、ファイアウォールと呼ぶ)を構築し運用する。現在のファイアウォールは、組織において外部と接続を持つ計算機の数とサービスを制限し利便性をいくぶん犠牲にすることで、セキュリティの向上とセキュリティ確保の労力の低減を実現している。

現在ファイアウォールを構築するためのプロダクトには様々なものがあり、ファイアウォールを構築することは、これらのプロダクトに対応したソフトウェアを個別にインストールし、管理運用するこ

とで実現されている。しかし、このことはファイアウォールの管理者にとってオーバヘッドとなる。経路制御、IP パケット転送機能、プロキシー等のフィルタリングなどのファイアウォールプロダクトは、統一された管理インタフェースを持っておらず、管理者は、これらの膨大な設定に対応することを強いられるからである。

さらに、現在のファイアウォールは異常の検出や管理者への報告機能が不足しており、管理者への負担を大きくしている。管理者の設定のもと通信の制限を行い、必要ならば通信の記録を管理者に電子メール等で通知する。管理者は膨大な記録の中から、不正なアクセスがないかをチェックし、あれば設定の変更を検討する。すなわち、侵入者からの不正なアクセスや異常発生の判断は管理者によって行われるため、オーバヘッドとなる。

我々は、ファイアウォールを構築する様々なプロダクトを、統一されたインタフェースで管理運用すること、異常検出ができることがファイアウォールに求められる要素であると考える。本稿では、ファイアウォール技術の仕組みと特徴について説明する。次に問題点の考察と、これを解決する手法すなわちファイアウォール管理技術として、SNMP[1]を用いたエージェントシステムを提案し、その構成と機能の実装および今後の課題について述べる。

2 研究背景

2.1 ファイアウォール技術

ファイアウォールとは、企業や研究機関において、組織内部の、ネットワークの危険にさらされる計算機の数やサービスを制限し、セキュリティを向上させる技術の総称である。図 1に、一般的なファイアウォールの概念図を示す。

図 1は、外部につながっているネットネットワークと内部のネットワークを専用ルータでつないだファイアウォールの一般的な構成である。外部側にはサービスホストという特定のサービスを提供するホストが存在し、外部から、あるいは外部への特定のサービスを許可している。

しかし、ファイアウォールには、ネットワークの

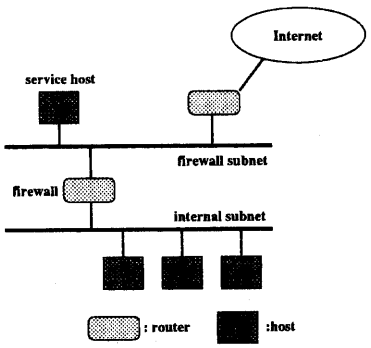

図 1: 一般的なファイアウォールの形態

利便性の向上とセキュリティ強化の点でトレードオフが生じる。ネットワーク管理者は、どのサービスを利用可能にするか検討しファイアウォールを構築する。ファイアウォールを構築するプロダクトには様々なものがある。以下に、ファイアウォールプロダクトについて述べる。

- 外部からの IP パケットの到達を制限する経路制御および IP の転送制限 (IP フィルタリング)

  特定のマシンからのアクセスや特定のマシンへのアクセスを許可する方法、内部のネットワーク構成を外部に広告しない方法等がある。一般的には専用ルータによる設定で実現される。

- アプリケーションゲートウェイ

  サービスホストでサービスの中継を行う方法。フィルタリングとの違いは、プロトコルの持つサービス名を理解し、中継処理を行う点である。中継処理を行うものをプロキシーサーバと呼ぶ。代表的なアプリケーションとして、proxy httpd,DeleGate,TIS Firewall Tool Kit などがある。

- アドレス変換 (NAT[2])

  組織内部の IP アドレスを、グローバルなアドレスに動的に変換する方法で、組織内部のネットワーク構成を隠蔽できるという特徴を持つ。

[1]Simple Network Management Protpcol の略。文献 [1] 参照

[2]Network Address Translattion の略

上記のプロダクトを用いることでファイアウォールを構築できるが、現実にファイアウォールを管理運用すると、いくつかの問題点が生じる。次項で問題点について述べる。

2.2 ファイアウォール管理の問題点

前項で述べたファイアウォール構築のプロダクトは個々に存在している。そのため、ファイアウォールの管理者は、ファイアウォールのためのソフトウェアを個別にインストールし、設定したうえで管理を行なう。個々のプロダクトは、ファイアウォールを構築する上で重要な役割を持つが、ファイアウォール全体を管理運用するには、以下の問題点が生じると考える。次項でこれら問題点について詳しく言及する。

- ファイアウォールの集中管理が困難
- 異常検出 (Trap) 機能の不足

2.2.1 ファイアウォール集中管理の困難

前述のファイアウォールプロダクトにはそれぞれ特性があり、制限や設定の対象が異なる。つまり、管理者がそれぞれのファイアウォール技術を集中して管理するインタフェースがないため、管理者に人的労力のオーバヘッドが生じる。

2.2.2 異常検出 (Trap) 機能の不足

現在のファイアウォールは、外部からの不正アクセスや異常を検出する機能が不足している。管理者は、膨大な記録の中から不正アクセスを見つけ出し、対応を考えることになる。さらに、不正アクセスを行なった侵入者への対応は皆無で、アクセス元のチェック (リバースアタック) や侵入方法、被害報告等は行なわれない。

このように、異常検出 (Trap) 機能がないことは、管理者への負担を大きくする要因となっている。

2.3 エージェントによる管理

上記の問題点を解消する方法として、本研究では、エージェントによるファイアウォールの集中管理を目指した管理プラットフォームを設計し、SNMP を用いて開発を行った。エージェントとは、存在する

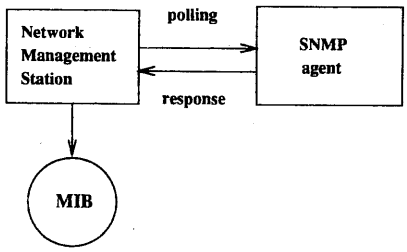

図 2: SNMP による管理環境

個々のファイアウォールプロダクトにおいて、設定や変更、モニタリングを容易にし Trap 機能およびカウンター機能を容易に付加させて強力かつ柔軟性をもったファイアウォールを実現するものである。

次章では、SNMP エージェントのモデルを説明し、その後ファイアウォールエージェントのモデルを提示する。

3 モデル

3.1 SNMP エージェント

SNMP(Simple Network Management Protocol) とは、ネットワーク管理を支援するために開発された、プロトコルを含む一連の仕様を示したものである。SNMP を用いた管理環境を図 2に示す。

図 2では、管理の対象 (ホストやルータ等のマシン) に SNMP のエージェントを設置し、管理者はエージェントから管理対象の状態を知ることができる。管理対象の状態とは、通信に関するインタフェースの数や種類といった物理的な情報、IP,ICMP,UDP,TCP など各種プロトコルの実装や動作状況に関連する情報を指している。

ネットワーク管理者側では、これら情報の項目を MIB(Management Information Base) というテキスト型のデータベースを持っている。管理対象の状態において特定の情報を知りたい場合、項目名をエージェントに問い合わせることで、エージェントは項目に関する情報を管理者に返す。

情報の中には、管理者によって情報の内容 (値)

を変更できる項目もあり、エージェントは管理対象の設定を指定された値に変更することもできる。

またSNMPでは、管理対象のリブートやリンクダウン、通信負荷の過重を管理者に通知するTrap機能も備えている。

従来のSNMPは、一部のTrap機能を除いて、ポーリング主導型である。本研究では、Trap機能の強化を行うため、SNMPエージェントの改良により、新たにファイアウォールエージェントを開発した。次項で構成と機能を示す。

3.2 ファイアウォールエージェントの構成

ファイアウォールエージェントの目的には2つある。

- 統一したインタフェースとして、ファイアウォールの設定および変更が可能であること。
- 異常を定義した上でモニタリングし、異常発生時に対応できること

Trap機能やカウンター機能を充実させるには、従来のポーリング主導型だけではなく、エージェント自身も能動的にファイアウォールをモニタリング、および異常発生を認識するプロセスが必要である。ファイアウォールエージェントでは、これらのプロセスを、言語処理部において実行している。

ファイアウォールエージェントは、図3に示した各部から構成される。

- 言語処理部

  ファイアウォールのモニタリングや、異常の定義を行い対応を指示する。対応の内容や異常発生と判断する発火条件は、管理者によって記述されたファイルを参照し、モニタリングした状況と比較判定する(後述)。

- SNMP処理部

  管理者とエージェントとのインタフェースとなる部分であり、SNMPのパケットを生成する。従来のSNMPによるポーリング機能も併せ持ち、モニタリングに関する処理を行う。

- MIB処理部

  従来のSNMPが持つMIBにファイアウォール管理に必要な項目を付加したファイアウォールMIB(後述)とエージェントとのインタフェースとなる部分である。

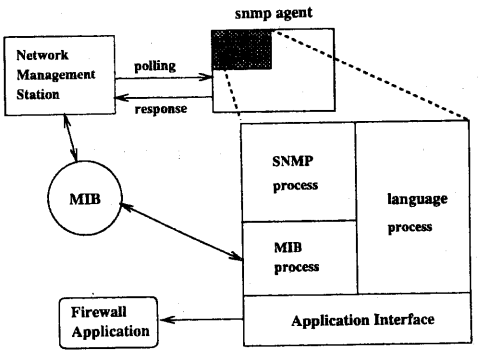

図3: ファイアウォールエージェントの構成

- アプリケーションインタフェース

  ファイアウォールを構成するアプリケーションとのインタフェースとなる。言語処理部からの設定変更の指示をアプリケーション側に渡し、実行させる。

従来のSNMPエージェントと比較した場合、ファイアウォールエージェントは言語処理部とアプリケーションインタフェースを付加している点が異なる。ファイアウォールエージェントとして必要な言語処理部とファイアウォールMIBについて、次項以降で説明する。

3.3 言語処理部

言語処理部は、ファイアウォールエージェントの対応やを記述にしたがって動作させる動作記述と、複数の動作を適切に処理するタイマ機能、および異常を検知する条件判定する機能を持つ。この機能を実現するために、イベントドリブンな関数型インタプリタ言語を開発した。

言語では、動作定義部と動作処理部、および文法処理部の仕様を定義しており、管理者は言語仕様にしたがってファイアウォールエージェントの動作を指示できる。

基本動作の定義は、以下の仕様にしたがって記述される。

```
define event <event_name> {
    SNMPtrap <trap_name> <trapID>;
    ICMPtrap <trap_name> <icmpID>
                from <IPaddress>;
    TIMERtrap <trap_name>;
}

define handle <handle_name> {
}

define object <object_name> {
    locateat <IPaddress>;
    attach <handle_name>;
    attach <handle_name> on <event_name>;
}
```

event では、どのような Trap を発生させるのかを定義する。handle は具体的な動作記述を定義する部分で、管理者への通知や、ファイアウォール側の処理等の動作を定義できる。これら個々の動作内容を特定の管理対象である object に対して実行する。

定義された動作の実行は、以下の関数を用いて記述される。

```
manage <object_name>;
unmanage <object_name>;

arm <handle_name> in <object_name>;
disarm <handle_name> in <object_name>;

poll <SNMPobjectID> in <object_name>;
set snmp <value> on <SNMPobjectID>
                    in <object_name>;
```

manage/unmanage は、管理対象に定義された動作を実行／解除する関数であり、arm/disarm は、管理対象に定義された特定の動作を実行／解除する関数である。

ファイアウォール MIB に基づいたモニタリングや設定の変更は、poll/ set によって行う。

文法処理に関しては、一般的な条件分岐 (if～then～else,switch～case) やループ (while,for)、算術演算子 (+,-,*, ／,mod) や関係式 (=, <, >,!=) および変数処理を定義している。

INDEX	内容
fwgatewayInfo	マシン情報
fwgatewayRegister	トラップ情報
fwgatewayControl	制御情報
reachability	ICMP ／ UDP 情報
discovery	コネクション情報
appsType	アプリケーション情報
packetType	パケット情報
packetPort	ポート情報
filter	フィルタ情報
statics	ログ情報
alarm	アラーム情報
matrix	経路情報

表 1: ファイアウォール MIB エントリ

3.4 ファイアウォール MIB

ファイアウォールを構築するマシン (ホスト, ルータ等) に対し、ファイアウォールを運用する上で必要な管理項目を作成した。ファイアウォール MIB では、従来の MIB-2 [2] 及び RMON-MIB[3]にこれらの項目を付加している。表 1にファイアウォール MIB の重要なエントリを示す。

reachability では、アクセスポイントが妥当か否かを判断するために、ICMP や UDP によるアクセスポイントへの到達可能性を示すパラメータである。ファイアウォールの制御では、ファイアウォールを構成するアプリケーションを appsType で指定し、アクセスポートやパケット情報をアプリケーション側に渡して処理を実行させる。

専用ルータでファイアウォールを構築している場合は、filter や matrix でフィルタリングおよび経路制御の設定を行う。

[3]Remote Monitoring MIB, 文献 [3] 参照

4 実装

ファイアウォールエージェントの実装環境を以下に示す。

```
[マシン]DECpc LPx
[OS]BSDI BSD/OS 2.0.1
[SNMP パッケージ]CMU SNMP Version 2
[ファイアウォール]TIS Firewall Kit
```

5 今後の課題

ファイアウォールエージェントによる管理技術には、多くの発展させるべき点があると考える。以下にその将来性について考察する。

- 様々な管理対象に対するエージェントの開発と、統一したインタフェースの提供。具体的には、情報サーバ(ファイルサーバ,WWW サーバ, FTP サーバ等) が考えられる。
- エージェントの処理の高速化。SNMP のアーキテクチャは単純なので、文字列処理等が複雑でも利用できるという利点があるが、エージェントの処理の複雑化に対して処理速度の検討を行う必要がある。
- ネットワーク環境全体の管理のための、基盤環境の整備。
- エージェントのセキュリティ強化

6 まとめ

本研究では、既存のファイアウォール管理における問題点を明らかにするとともに、これら問題点を解消する新たな試みとして、ファイアウォールエージェントによるファイアウォールプロダクトの集中管理システムの提案と開発プラットフォームの構築を行った。ファイアウォールエージェントでは、ファイアウォール管理における管理者への負担の軽減と、強力かつ柔軟性のあるファイアウォールの実現が可能となる。

今後は、ファイアウォールエージェントの管理によるファイアウォールのセキュリティ面の検討および処理速度の定量評価を行いながら、さらなる拡張について検討していく予定である。

7 謝辞

本研究を進めるにあたり、多大な御協力を頂いた奈良先端科学技術大学院大学情報科学科情報ネットワーク講座の皆さん、貴重な議論および助言を戴いた住友電工 (株) システエレ研の村瀬氏に感謝します。

参考文献

[1] Jeffrey D.Case,Martin L.Schoffstall. A Simple Network Management Protocol. RFC1157,SNMP Research, May 1990.

[2] K.Mcloghrie,Marshall T.Rose. Management Information Base for Network Management of TCP/IP-based internets:MIB-II. RFC1231, Mar 1991.

[3] S. Waldbusser. Remote Network Monitoring Management Information Base. RFC1271,Nov 1991.

著者紹介

泉　裕 (いずみ ゆたか)
奈良先端科学技術大学院大学情報科学研究科情報ネットワーク講座所属. 博士後期課程 2 年
Internet: yutaka-i@is.aist-nara.ac.jp

井上博之 (いのうえ ひろゆき)
奈良先端科学技術大学院大学情報科学研究科情報ネットワーク講座所属. 博士後期課程 2 年.
現在 住友電気工業 (株) より留学中
Internet: h-inoue@is.aist-nara.ac.jp

山口 英 (やまぐち すぐる)
奈良先端科学技術大学院大学情報科学研究科助教授
Internet: suguru@is.aist-nara.ac.jp