

ネットワーク遠隔管理システムの実装に関する検討

Remote Management System and Mounting Examination for LAN

佐島 敬真

石井 啓之

Yoshimasa Sajima

Hiroshi Ishii

東海大学大学院工学研究科電気工学専攻

Course of Electrical Engineering, Graduate School of Engineering, Tokai University

1. まえがき

インターネットの発展により、個人運営による WEB サーバやメールサーバ等のインターネット上のサービス提供が増えてきている。そのような現状において、ユーザーからネットワーク管理者の予想を超えた利用をされたり不正な利用をされ、サービスを提供することが困難となり、停止をせざるを得ない状況が多く発生するようになった。そのような問題を回避するため、個人においてもネットワークを管理することが重要となった。しかし、ネットワークにおける障害の種類は非常に多く、また障害を回避するためのシステムやツールは一般的に高価であり、それぞれの目的にあったツールを個別に管理することは難しいと思われる。

そこで、本検討では安価で複数のネットワーク管理ツールを統合管理するシステムを構築し、ネットワーク内のトラフィック量からネットワーク障害を検知するシステムを提案することを目的とした。

2. ネットワーク管理ツール

ネットワーク管理ツールには、ネットワークの規模や用途によって様々な種類のもが存在している。以下に代表的なツールを挙げる。

- ・ ICMP (Internet Control Message Protocol)

端末間通信の可否を調べ、パケットの送信元に異常を知らせるために使われる。

- ・ SNMP (Simple Network Management Protocol)

SNMP が実装されている機器同士が情報を管理し、遠隔地から機器設定の更新を行ったり修復をすることができる。また、管理者に対する報告機能や独自のカスタマイズができる。

- ・ パケットキャプチャリング

ネットワーク内に流れるパケットを収集し、障害発見や不正パケットの検出などに用いられる。

上記のほかにも製品版を含め数多くのネットワーク管理ツールが世の中には存在している。しかし、それらのツールは個別に動作するため管理労力が必要とされる。本検討ではそれらの管理ツールを統合し、一元的に、かつ遠隔操作ができるシステムを構築した。

3. システム構成

本検討では図1に示すように LAN 内に Linux がインストールされた端末をネットワーク管理サーバとして設置し、図2で示すようにサーバ内に Perl 言語で記述されたネットワーク管理ツールを統合するシステムを導入した。また、LAN 外から携帯端末を用いて LAN 内のネットワーク管理システムを使用できるように WEB ブラウザ上からもネットワーク管理ツールを操作できるようにした。外部からサーバ内の HTTP を利用するためにはポートを開けなければならない等のセキュリティの問題が生じる。そのような問題を回避するため、ルータにおけるパケットフィルタリングや、暗号化の一種である SSL の利用、そして必要なホストのアドレスしか公開しない NAT 機能の利用などの対策をとる必要がある。

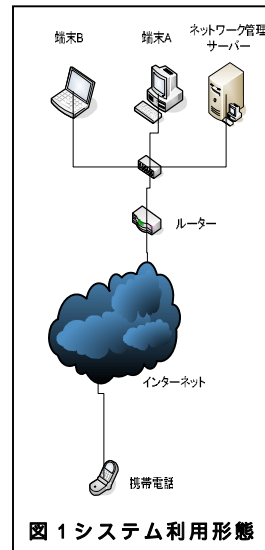


図1 システム利用形態

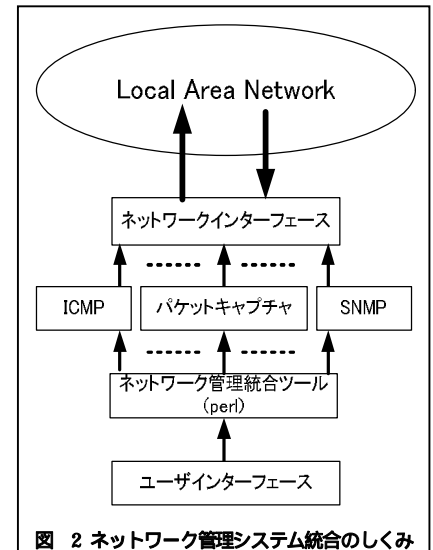


図2 ネットワーク管理システム統合のしくみ

4. 考察

図1、および図2のシステムを携帯端末から実行することにより、遠隔地から管理する LAN 内に対して ICMP、パケットキャプチャリング、SNMP を実行し、状況を把握することができた。SNMP では一定期間の情報を集約した結果を表示するため、瞬間的なネットワーク内の状況変化に対して迅速に対応ができないという問題がある。しかし、パケットキャプチャリングを常時実行し、同時にデータの分析を行うことにより上記の問題は解決できると考えられる。しかし、管理ツールの実行結果の中には膨大なデータ量になるものがあり、携帯端末を使用した管理にはデータ圧縮などの対策を行う必要がある。具体的な対策として、実行結果の中から管理者が必要なデータのみを抽出し、サーバ側でデータの加工をして携帯端末に表示する方法が考えられる。

5. まとめ

本検討では既存のネットワーク管理ツールを統合し、安価で、かつ一元的に管理するシステムを構築してその可用性を確認した。今後の課題として、ネットワーク管理ツールの種類の充実を行い、ネットワーク管理者が必要とされるツールを組み合わせる実行ができるように拡張をすることである。

また、収集したデータを分析し、ネットワーク内の障害を自動で予測・修復をするシステムを構築し、管理者の更なるネットワーク管理労力の低減を目指すことである。

参考文献

1. Northcutt 「Intrusion Signatures and Analysis」 Pearson Education
2. サーバ構築研究会 「FedoraCore1 で作るネットワークサーバ構築ガイド」 秀和システム
3. Douglas R. Mauro 「Essential SNMP」 O'REILLY