システムソフトウェアと
オペレーティング・システム 84−11
（２０００．５．２５）

WAN環境下における遠隔分散管理システムの提案

知念 眞也 † 長田 智和 † 谷口 祐治 ‡ 河野 真治 † 玉城 史朗 †

†琉球大学 理工学研究科 ‡琉球大学 情報処理センター

〒 903-0213 沖縄県 中頭郡 西原町 千原１番地

E-mail: fukuyama@ads.ie.u-ryukyu.ac.jp

あらまし 近年，インターネットの普及により，企業や大学などのネットワークは大規模化・多様化してきている．そのため，大規模ネットワークにおける管理には多くの管理ツールが必要となり，ネットワーク管理は複雑化してしまう．さらに，ネットワーク管理者の絶対数は低く，少数のネットワーク管理者に負担（障害の発見と復旧，未知なる障害に対する情報収集など）が集中しているというのが現状である．そのような現状における問題を解決すべく本研究では，WANを介すような大規模ネットワークにおいて，WEBベースでの遠隔管理を行い，管理者の負担軽減を目的とした遠隔分散管理システムを提案する．

キーワード： ネットワーク，管理システム，分散システム

A Proposal of Remote Distributed Management System under WAN environment

Shinya CHINEN † Tomokazu NAGATA †
Yuji TANIGUCHI ‡ Shinji KONO † Shiro TAMAKI †

†Graduate School of Science and Engineering, University of the Ryukyus
‡Center for Integrated processings, University of the Ryukyus

1, Senbaru, Nishihara, Nakagami, Okinawa, 903-0213 JAPAN

E-mail: fukuyama@ads.ie.u-ryukyu.ac.jp

Abstract In recent years, by the spread of Internet, the networks such as a company or a university become large scale and diversification. Therefore a lot of management tools become necessary for management in a large-scale network, and network management has become complicated. Futuremore, becouse of the number of network administrator is small, a burden (discovery of obstacle and resolution, gethering information for an unknown obstacle) concentrates on the few network administrator.
In this paper, to solve such probrems, we propose a remote distributed management system by a Web based under WAN environment.

Key Words : Network, Management system, Distributed system

1 はじめに

近年，インターネットの普及により，企業や大学などのネットワークは大規模化し，組織の構内ネットワークにはFDDI，ATM，Gigabit Ehernetなどの様々な回線網が混在する形態が増えてきた．このようにネットワークシステムが大規模化，多様化するに伴い，効率的な運用・管理のためのネットワーク管理システムの重要性がますます高まってきている．

従来型のネットワーク管理は，ネットワーク管理者が管理対象となる機器に直に，またはリモートから間接的にアクセスし，出力される膨大なログを見て経験的に行うというものである．しかし，このような管理方法では，管理対象機器が増えるに従い管理者へかかる負荷は増大していく．また，管理対象機器に障害が発生した場合，管理者の判断可能である障害に対してはその検知と対応を行うことができるが，管理者の知識にない未知の障害に対しては，障害の発見は困難であり，障害を発見することができた場合でも，管理者の障害に対する知識不足，及びスキル不足により対応不可能であった．

更に，基本的には，各機器は独立して機能しているため，オペレーティングシステムなどに障害が発生しても，管理者がその機器に直接アクセスしていなければ障害状況などをリアルタイムで知ることはできない．

機器によってはSNMPやRMONをサポートしているものもあり，トラップ機能によって障害をほかの管理機器へ連絡することができるが，トラップによる障害通知はMIBに基づいてるため限定的なものにしか対応しておらず，様々な障害要因を事前に察知するといった予防的な障害対策や，障害発生時に自立的に復旧処置を行うなどの制御はできない．

このようなことから，従来のネットワーク管理では，大規模なネットワークにおいて管理者への負担(障害の発見と復旧，未知なる障害に対する情報収集など)が非常に大きくなってしまうのである．

そこで本研究では，管理者の負担を軽減させ，少ない人数でも効率的に大規模ネットワークを管理できる分散型リモート管理システムを提案する．

本稿では，2章で提案する管理システムの構成について説明し，3章でそのシステムを構成する管理コントローラと管理デーモンの機能について説明する．4章では本システムの監視実験例をいくつか示し，5章で残された課題と今後の展開を述べ，6章でまとめを行う．

2 管理システム概要

2.1 システム概要

実装したシステムは，管理コントローラと管理デーモンから構成され，両者はそれぞれ独立して実行される(図1)．両者は独立しているため，管理コントローラが停止した場合でも，管理デーモンは継続して監視を行うことが出来る．また，管理デーモンが得た情報は一定時間ごとに管理コントローラに送付される．

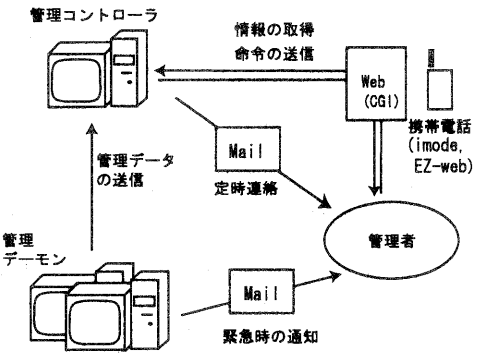


図1: システムの構成

様々なOSが混在する大規模ネットワーク上で動作する管理システムを構築するため，使用する言語には，マルチプラットフォームであるJAVA，およびPerlを用いる．

管理コントローラと管理デーモンの作成にはJAVAを使用し，管理デーモンが制御する

監視プログラム群は，文字列操作に長けた言語であるPerlを使用した．

管理者が管理対象のシステムに接続していなくとも管理データを得ることが出来るよう，本システムのインタフェースは基本的にWebを用いる．Web上で管理データの閲覧や管理プログラムの制御ができるため，携帯電話上でWebを見ることができるサービスであるiモードやEZWeb等を利用することで，管理者は携帯電話の電波が届く範囲でシステムの管理が可能となる．Web上での管理では，主にiモードを使用した管理を行った．

管理者には，管理システムから定期的に管理データが送信される．また，管理上重要なデータが得られた場合は，即座に管理者へ連絡する．連絡方法には電子メールを利用したPUSH型情報発信を活用している．このように本システムでは，比較的長い間隔で管理対象機器にpollingを実施して管理情報を取得し，機器に何か障害が起きたときにはTrapを送る，という二つの機能を利用した管理方法である"Trap-Directed Polling" [3] を採用している．ゆえに，管理対象機器の増加によるポーリングで消費されるバンド幅の節約と，管理コントローラでの処理の増加を抑えることができる．

2.2 管理コントローラ

管理コントローラは，Javaで作られたマルチスレッドサーバである(図2)．このサーバのメインとなるServerクラスでは，複数のポート上に複数のサービスを提供する．そのサービスが実現する機能を以下で示す．

(1) 管理者からの要求処理
　管理コントローラは，コンソール上，及びWeb上からの管理者の要求を処理する．要求内容としては，管理者の指定する管理データの表示，定時連絡内容・周期設定等である．

(2) 管理者から管理デーモンへの指令送信
　管理デーモンで制御している管理プログラムの起動・停止・設定ファイル変更等の指令を管理デーモンへ送信する．

(3) 管理デーモンから送付された情報の処理
　1日ごとに管理デーモンから送られてくる管理データを，管理者がスムーズに検索できるように，各管理デーモンごと，各データごとに分類して保存する．また，Web上閲覧できるようにHTMLへの変換を行う．

(4) 管理者への定時連絡
　管理者が指定した管理データを，定期的に電子メールで通知する．

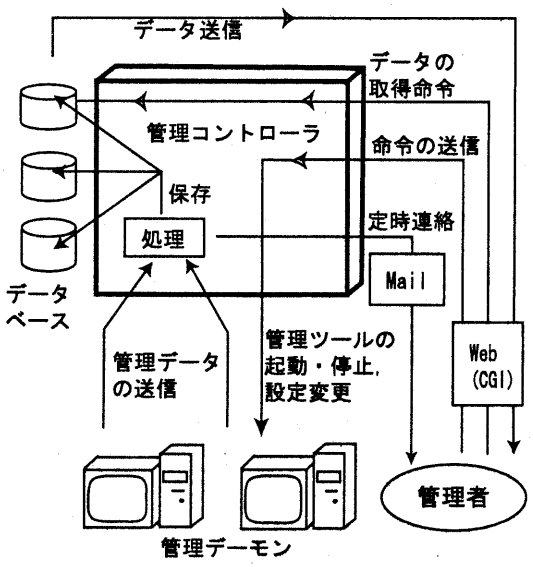


図 2: 管理コントローラの構成

2.3 管理デーモン

管理デーモンはJavaで作成されたサーバである．管理デーモンは，基本的に一つのサブネット上に一つ配置し，主に各種管理プログラムによるネットワーク管理データの収集を行う．その構成を図3で示す．

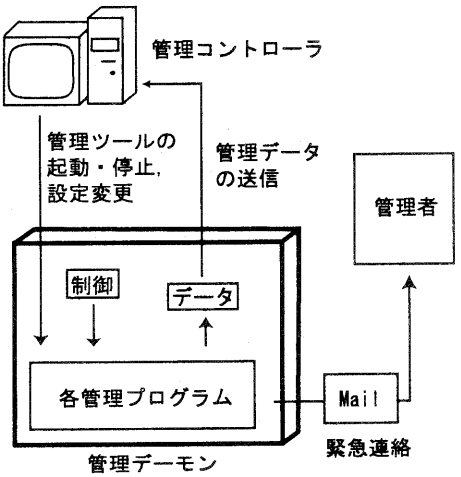


図 3: 管理デーモンの構成

管理デーモンは次のような機能を持つ.

(1) ネットワークの監視・測定

(a) PC の電源 ON/OFF 監視

PCの電源監視には, pingを使用する. 基本的に, 管理デーモンはサブネット単位で設置するので, ping だけで PC の生存確認は可能である. ルータなどを隔てたPCも監視する場合は, pingの反応が返ってこないPCに対して traceroute で経路上の機器が正常であるかも調べる. その結果より pingが返ってこない原因が対象PC自身であるのか, PCまでの経路上の機器およびネットワークケーブルなどであるのかを判定する.

(b) パケット量・データ量測定

パケット量·データ量の測定には, tcpdumpを利用する. tcpdumpでは, -eオプションをつけ, リンクレベルヘッダ情報も付加させた出力を利用する. イーサネットにおいて, リンクレベルヘッダには, 時間, 送信元の MAC アドレス, 送信先の MAC アドレス, プロトコル, パケット長が必ず含まれる.

この計測では, リンクレベルヘッダ情報の測定, その後に出力されるプロトコルごとの出力結果から, プロトコルを判別し, その出現回数及び合計パケットサイズの測定を行う. もしプロトコルごとの出力結果の中に送信先と送信元のドメインが含まれている場合は, その測定も行う.

トラフィック統計の結果から, ネットワークの特性 (どのようなサービスが多く利用されてるか, どの時間帯のトラフィックが多いか) の把握や, 出現ホストの統計からの不審ホストの発見が行える. また, ホストとポート番号を対で調べることで, ポートスキャン攻撃の発見も行える.

(c) 入出力パケットエラー率測定

パケット不良は, ネットワークにより大きな負荷を与える. 本システムでは, netstat を利用して, 一定時間ごとに各ネットワーク・インタフェースでの入力パケットエラー率, 出力パケットエラー率を測定する. この測定を長期的に続けることで, 常にパケットエラー率が高い場合は, ネットワークを構成するハードウェアに問題があることが分かる.

(d) ネットワーク混雑測定

管理デーモンの動作しているセグメントの混雑を判断する指標として衝突率がある. 本システムでは, netstat を利用して一定時間ごとの各ネットワーク・インタフェースでの衝突率を調べる.

また, リモートホストとの通信経路の混雑を判断する指標として RTT がある. リモートホストに対して 100~1500bytesのパケットを送信し, RTT を測定する. これらの各パケットサイズの RTT の値が単調増加していない場合, リモートホストとの通信経路で混雑が発生していることがわかる. 混雑を発見し, 自ホストからリモートホストとの間にある各ルータに対して同様の測

定を行うことで，通信経路のどこで混雑が発生しているかを調べることができる．

もし衝突率が常に高い場合は，ネットワークを分割してネットワーク・トラフィックの負荷を下げる必要がある．また，常に通信経路で混雑が発見される場合は，現在のネットワーク機器に性能的なボトルネックが起きている可能性があるので，ネットワークの再構築を行う際にこの結果が利用できる．

(e) パケット損失率統計

ここでは，指定されたリモートホスト間でのパケット損失率を調べる．パケット損失率が高い場合，TCP パケットのウインドウフィールドの統計や入力パケットエラー率を見ることで，リモートホスト間のパケット損失がデータリンクレベルでの損失なのか，又はＩＰレベルでの損失なのかを判断できる．

(f) 外部センサによる温度，湿度測定

シリアルポートに繋げるセンサを利用することで，温度や，湿度などの物理的な情報も測定する．この測定情報を利用し，ある一定温度を超えると管理者に通知を送るように設定することで，マシン室の温度上昇によるトラブル等を未然に防ぐことができる．また，その他様々なセンサと組み合わせることでより多角的な管理情報を収集することができる．

(2) 各プログラムの制御

管理デーモンは，Perl で作成された各プログラムの制御 (起動・停止・生存確認・設定変更等) を行う．起動・停止・設定変更は，管理者から管理コントローラを通して行われる．生存確認は，各プログラムのプロセス ID を収めたファイル中の，プログラム名とプロセス ID の値と，UNIX の ps コマンドで出力されるプログラム名とプロセス ID の値を比較して行う．

(3) 管理コントローラへの管理情報の送信

管理デーモンは，管理者の設定した期間で管理コントローラへ管理情報を送信する．デフォルトの周期は 1 日に 1 回である．

(4) 緊急時の管理者への連絡

管理データの値が管理者の指定したしきい値を超えた場合，または主要 PC への ping が届かなかった場合等には，即座に管理者へメールで通知する．通知内容は，障害メッセージと緊急通知の原因となったデータである．この PUSH 型通知により障害への迅速な対応が可能となる．

3 実装ネットワーク

琉球大学キャンパスネットワーク RAINS(Ryukyu Academic Information Network System: 以下 RAINS と称す) の学内基幹ネットワークは，ATM と FDDI，Gigabit Ethernet で構成されている．ATM は 12 台の ATM 交換機が各学部と総合情報処理センターに設置され，OC12(622Mbps) で PVC により接続されている．一方，FDDI は事務系の通信網として運用されている．また，双方のネットワークと相互に接続している Gigabit Ethernet は，附属図書館と総合情報処理センターを 2Gbps で結び，キャンパスネットワークの主軸として運用されている．

管理システムの実験運用は，総合情報処理センター内の OSN(Open System Network) で行った．

4 ネットワーク監視実験

前章で説明したネットワークにおける本システムの監視・測定実験例を示す．

(1) パケット量・データ量測定例

1 時間ごとのプロトコルデータ量の棒グラフ表示例 (図 4)．この図より，データ量の全体的な推移や，ネットワークの特

性などが分かる．

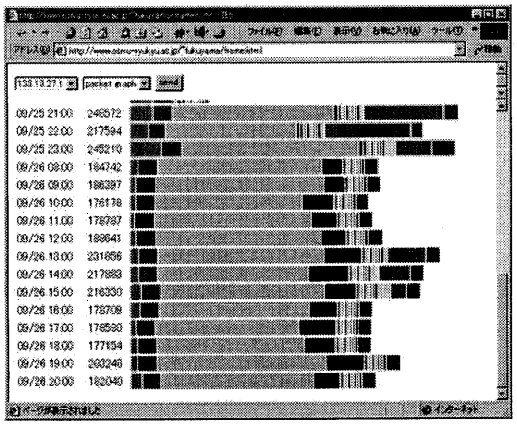
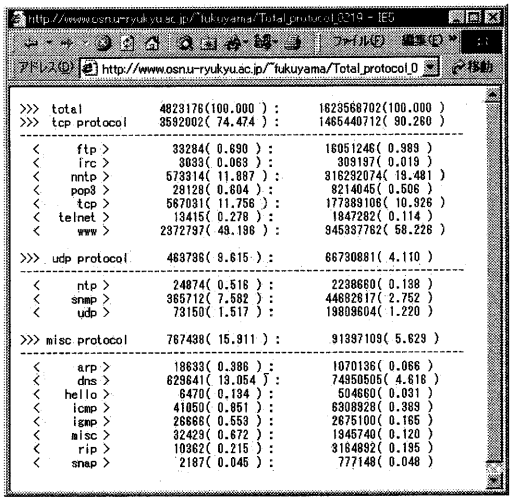


図 4: パケット量・データ量測定（グラフ）

上グラフの，数値によるより詳細な表示例 (図 5)．上図のより詳細なデータ表示である．



>>> total	4823176(100.000) :	1623568702(100.000)
>>> tcp protocol	3592002(74.474) :	1465440712(90.260)
< ftp >	33284(0.690) :	16051246(0.989)
< irc >	3033(0.063) :	309197(0.019)
< nntp >	573314(11.887) :	316292074(19.481)
< pop3 >	29128(0.604) :	8214045(0.506)
< tcp >	567031(11.756) :	177389108(10.926)
< telnet >	13415(0.278) :	1847282(0.114)
< www >	2372797(49.196) :	945337762(58.226)
>>> udp protocol	463736(9.615) :	66730881(4.110)
< ntp >	24874(0.516) :	2238660(0.138)
< snmp >	365712(7.582) :	44682617(2.752)
< udp >	73150(1.517) :	19809604(1.220)
>>> misc protocol	767438(15.911) :	91397109(5.629)
< arp >	18633(0.386) :	1070136(0.066)
< dns >	629641(13.054) :	74950505(4.616)
< hello >	6470(0.134) :	504660(0.031)
< icmp >	41050(0.851) :	6308828(0.389)
< igmp >	26666(0.553) :	2675100(0.165)
< misc >	32429(0.672) :	1945740(0.120)
< rip >	10362(0.215) :	3184892(0.196)
< snap >	2187(0.045) :	777148(0.048)

図 5: パケット量・データ量測定（数値）

(2) i モード表示例

パケット量・データ量測定の，i モードでの表示例 (図 6)．

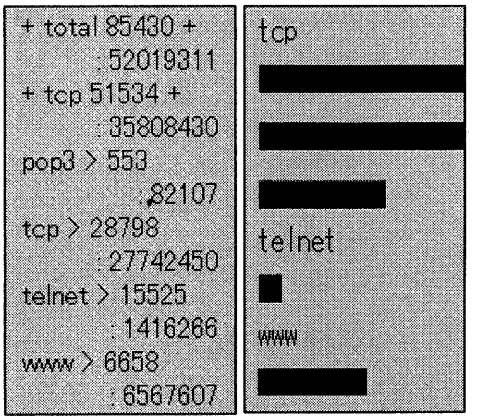


図 6: i モード表示例

(3) PC の電源 ON/OFF 監視

監視対象 PC の電源が OFF になった場合の電子メール通知 (図 7)．監視対象 PC は，システムの設定ファイル内に IP で記述しておく．

```
Date: Sat, 8 Apr 2000 00:09:44 JST
From: Shinya CHINEN <fukuyama@oix1.oix.u-ryukyu.ac.jp>
To: fukuyama@osn.u-ryukyu.ac.jp
Subject: Host Unreachble

04/14 08:45

133.13.27.239
133.13.27.238
```

図 7: 電源 OFF メール通知

5 システムの評価

本システムを利用することで，次のような利点が考えられる．

(1) 障害の特定に有効

琉球大学で使用している SNMP を利用した管理ツールである MRTG では，入力と出力のパケット量の総量は把握することはできるが，より詳細な情報は得ることができない．本システムでは，パケットの総量以外にもプロトコル別の内訳を調べることができ，どのプロトコルがネットワー

クを圧迫しているか，等の判別を行うことができる．また，ホスト別の統計結果と照らし合わせることで，どのホストからそのパケットが流れているかという判別もできる．これらの情報を活用することで，不正パケット送信元の特定や，障害の特定に有効に活用することが可能である．

(2) 手軽な管理

本システムでは，携帯電話上からのWebアクセスを利用して管理を行うことができる．それにより，管理者は携帯電話一つで必要な管理情報を得ることができる．ゆえに，管理者はノートパソコンのようなモバイル機器を持たずとも管理情報が得られるようになり，より手軽に管理を行うことができる．

本システムでの問題点としては，まずWebを利用しているという点から，セキュリティに対する問題が挙げられる．その解決策としては，管理サイトの閲覧に関して，アクセス制限やワンタイムパスワードなどを利用することでのセキュリティ強化が考えられる．その他の問題点としては，管理コントローラ及び管理デーモンの停止時の対処が挙げられる．これに対しては，管理コントローラ及び管理デーモンの多重化による解決が考えられ，また管理デーモンにおいては，停止した管理デーモンの管理範囲ネットワークの管理を，隣接するネットワークの管理デーモンが一時的な管理範囲拡大を行うことでカバーする方法での解決が考えられる．

6 今後の課題

今後本システムに求められる機能としては，まず，SNMPとの連携が挙げられる．本システムで使用している，pingやnetstat，tcpdump等の出力結果だけでは網羅できる情報の範囲は限られている．そこで，これらのツールでは取得できない情報をSNMPを用いて取得することで，より広く管理情報を収集できるようになる．次に，障害の予測が挙げられる．本システムで収集した管理データの履歴を基に解析を行うことで，管理対象ネットワークに今後起こるであろう障害の予測を行う．最後に，モバイルエージェントを用いた管理情報収集が挙げられる [1]．管理デーモンからの集計データ送信は，管理デーモンの数に比例して増加していく．このデータ送受信処理を軽減させるために，モバイルエージェントを用いて管理情報を巡回収集する方法を用いる．モバイルエージェントを用いた収集では，管理コントローラを出入りするデータはエージェント送信とエージェント取得の最小限の回数で済むため，管理コントローラの負荷を抑えることができる．

7 まとめ

ネットワークの大規模化・複雑化によって，ネットワーク管理に要するコストは増大している．それとは対照的にネットワーク管理者の絶対数は低く，少数のネットワーク管理者に負担が集中しているというのが現状である．

その問題を解決すべく，本研究では，大規模ネットワークにおける効率的な管理システムとして管理コントローラと管理デーモンからなるリモート管理システムを提案した．今後は上記の課題をふまえ，より効率の良いシステムを構築していく．

参考文献

[1] 長田智和他，“ネットワーク管理におけるモバイルエージェントを用いた自立分散システムの適応”，計測自動制御学会第12回自立分散システム研究会，pp.59-62，2000

[2] 知念真也他，“琉球大学キャンパスネットワークにおけるリモート管理システムの提案”，第60回全国大会，pp.455-456，2000

[3] M·T·ローズ，“シンプルブック　インターネット管理入門”，株式会社プレンティスホール出版，1995