マルチメディア通信と分散処理　54－5
（1992. 3. 5）

SNMPを利用したエキスパートネットワーク管理システム AIMSの実現と利用

村田眞人† Glenn Mansfield† 時庭康久†
Krishnamachari Jayanthi† 樋口謙一† 和泉宏明‡

†AIC ‡日立ソフトウェアエンジニアリング(株)

インターネットワークの大規模，複雑化に伴い，その高信頼，高効率を維持するネットワーク管理の重要性が十分認識されるようになってきた．

本論文では，先ず現状のインターネットワークを対象とした現実的なネットワーク管理モデルを提案し，提案モデルに基づいて設計・開発を行なっているエキスパートネットワーク管理システム **AIMS**(AICs Internet Management System)の実現方法について述べる．特に時間を導入した管理を実現するための方法については詳しく述べる．また，**AIMS**の利用例についても紹介する．

Implementation & Operation of an SNMP-based Expert Network Management System **AIMS**

Makoto Murata† Glenn Mansfield† Yasuhisa Tokiniwa†
Krishnamachari Jayanthi† Kenichi Higuchi† Hiroaki Izumi‡

†Advanced Intelligent Communication Sys. Lab.
‡Hitachi Software Engineering Co-Ltd.

6-6-3, Minamiyoshinari, Aoba-ku, Sendai 989-32, Japan

As internetworks become larger and more complex, the importance of network management that supports high reliability and high efficiency increases.

In this paper we propose a realistic network management model that is useful in the present internetwork environment and then describe **AIMS**(AICs Internet Management System) designed by our group in accordance with the proposed model. We talk in detail about practical management using various time related aspects and also introduce some of the operations of **AIMS**.

1 はじめに

日本のインターネットワークもWIDE[1]やJAIN[2]などの活動によってますます大規模，複雑化しており，その高信頼，高効率を実現するためのネットワーク管理の重要性が十分認識されるようになってきた．また，ISOやIAB (Internet Activities Board)では，ベンダやアーキテクチャに依存しない管理を実現するために，ネットワーク管理プロトコルの標準化が進められており，SNMP (Simple Network Management Protocol)のように既に標準化が終了したプロトコルに関しては，そのプロトコルを利用した管理システムの製品も出始めている．

インターネットワーク管理の現状を見てみると，例えばトラヒック解析[1][3]やRTT (Round Trip Time)に関する検討[4]が行なわれ，利用状況や性能が調べられている．しかし，障害に対しては，検出されてから対処するという管理が依然として中心であり，障害の自動検出や自動診断の例は少ない[5][6]．

次に管理者について見てみると，大規模広域ネットワークの多くは実験や研究のためのネットワークであり，その管理は研究プロジェクトの関係者や一部のボランティアによって行なわれている．管理者はその仕事を専門としているわけではなく，研究の一貫あるいは副業として携わっている人がほとんどである．そのため，商用ネットワークのように専任の管理者が24時間管理を行うような体制にはなっていない．また，ネットワーク管理を行なうためには，ネットワーク構成，各種通信プロトコルなど，ネットワークとその管理に関する深い知識と多くの経験が必要であり，管理者が実際に管理を行なえるようになるまでには時間を要する．

筆者らは，このような現状の管理体制にマッチし，様々なレベルのネットワーク管理者の支援を可能とする管理システムとして，専門家の管理知識を知識ベースに持つエキスパートネットワーク管理システムAIMS(AICs Internet Management System)の研究及び開発を行なっている[7][8]．

本論文では，2章で従来のネットワーク管理モデルを考察した上で，現状のインターネットワーク管理を目的とした現実的なネットワーク管理モデルの提案を行なう．次に3章で提案モデルに基づいて設計したAIMSの実現方法について述べた後，4章で時間を導入した管理を可能とするための実現方法について詳しく説明する．そして5章で本システムを利用して筆者らがどのようにネットワーク管理を行なっているかを紹介する．

2 ネットワーク管理モデル

本章では従来のネットワーク管理モデルについて考察し，新たな管理モデルの提案を行なう．

2.1 従来モデルの考察

2.1.1 モニタモデル

ネットワーク管理の初期から現在に至るまで広く利用されているモデルである．ネットワークにネットワークアナライザ等のデータ収集・解析機器を接続し，障害解析やトラヒック解析を行なう．ここで，接続した機器が行なうのはデータ収集と低レベルなデータ解析だけであり，障害解析等を実際に行なうのは管理者である．

本モデルには，構成が単純，既存のネットワーク要素の変更が不要といった利点がある反面，接続するネットワークセグメントの情報しか収集できない，管理は受身的なものに限定され，管理対象に対する制御は不可能等の問題点がある．本モデルを利用した管理形態例を図1に示す．

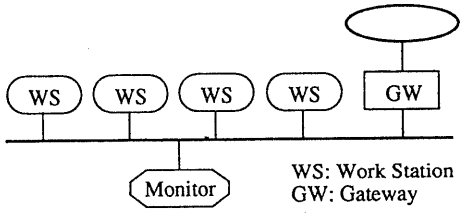


図1: モニタモデルによる管理形態例

2.1.2 マネージャ・エージェントモデル

本モデルにおいてはネットワーク要素は管理ステーションとその他の管理対象とに分類される．マネージャ(プロセス)は管理ステーション上に存在し，管理対象に実装されているエージェント(プロセス)と通信を行なって，管理対象のモニタや制御を行なう．マネージャ・エージェント間通信にはネットワーク管理プロトコルが使用される．

本モデルには，管理対象に対して制御が可能，他のネットワークセグメントの管理も容易という利点があるが，マネージャ・エージェント間通信自体が機能しなくなるような障害時には管理不能となる．本モデルを利用した管理形態例を図2に示す．

2.1.3 従来モデルの問題点

現状のインターネットワークを対象として，ネットワーク管理システムを実際に開発，運用していく立場に立つ

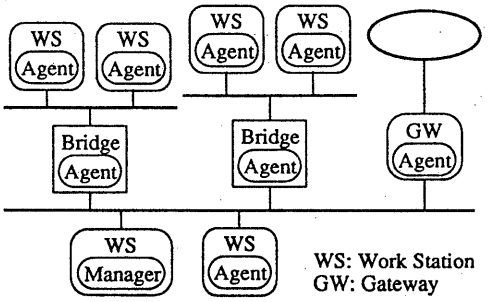


図 2: マネージャ・エージェントモデルによる管理形態例

と，従来の管理モデルには個々のモデルの問題点以外に次のような問題が考えられる．

1. 大規模ネットワークを管理対象にする場合，そのネットワークを構成する全ネットワークセグメントにデータ収集機器を接続したり，全ネットワーク要素にエージェント機能を持たせることは，費用，インストールの手間，ネットワーク構成の流動性等から考えて現実的ではない．しかし，ネットワーク全体のトラヒック情報を収集，解析，評価することは重要である．
2. 従来の管理モデルでは“時間”が考慮されていない．ネットワーク管理において，時間は重要な意味を持つ．常に変化するネットワークの状態を正確に解析するには，マネージャ及び全管理対象間での時間の一致や，各エージェントが決められた時間から決められた間隔で情報を収集する能力が不可欠である．

2.2 提案するネットワーク管理モデル

以上の問題を解決するため，モニタモデルとマネージャ・エージェントモデルを融合し，さらに時間を導入したネットワーク管理モデルを提案する (図 3).

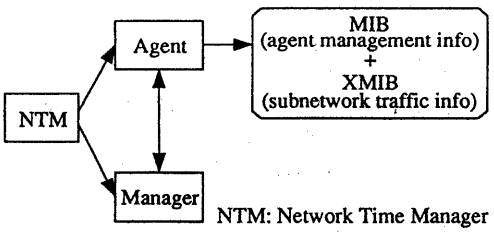


図 3: 提案するネットワーク管理モデル

本提案モデルにおいて，エージェントは標準 MIB (Management Information Base) の管理情報だけでなく，モニタモデルにおけるデータ収集機器が収集するのと同様な情報として，接続しているネットワークセグメントのトラヒック情報も拡張 MIB (XMIB: eXtended MIB) の管理情報として収集，保持する．この拡張によって，大規模ネットワークを構成する各ネットワークセグメントに最低一つのエージェントが存在すれば，マネージャはネットワーク全体のトラヒック情報を入手できることになる．また，NTM (Network Time Manager) によってネットワーク要素間の時間が同期しており，複数のエージェントから入手した情報から，ある時刻におけるネットワーク全体の負荷状態を再現することが可能となる．本モデルを利用した管理形態例を図 3に示す．

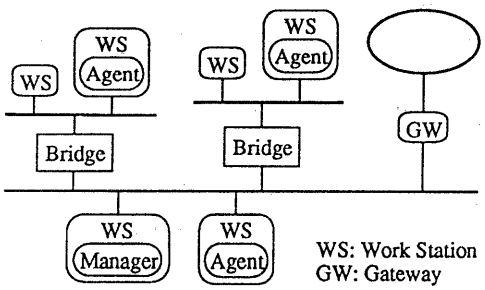


図 4: 提案モデルによる管理形態例

3 AIMS の実現

本章では AIMS で採用したネットワーク管理プロトコル，システム構成とその実現について述べる．

3.1 ネットワーク管理プロトコル

提案したモデルにおいては，マネージャ・エージェント間通信が必要となる．以下に代表的なネットワーク管理プロトコルを示す．

- CMIP(Common Management Information Protocol)
- CMOT(CMIP over TCP/IP)
- SNMP(Simple Network Management Protocol)

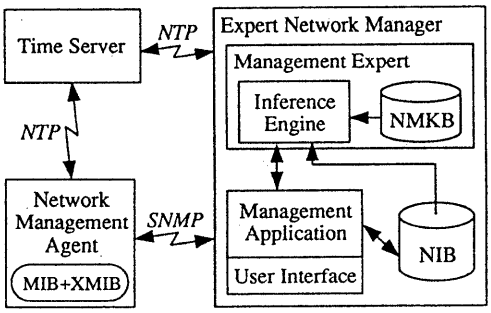
CMIP[9] は ISO で標準化された OSI 管理で使用されるプロトコルである．

CMOT[10]，SNMP[11][12] は IAB で標準化されている管理プロトコルである．CMOT は TCP/IP ネットワークを OSI 管理によって管理するプロトコルであり，高機能なこともあり将来的には主流となると思われるが，まだ標準化が終了していない．

筆者らは，現在管理対象としているTCP/IPネットワーク上で動作する，標準化が既に終了し業界標準となりつつある，構造が比較的簡単で移植性が高い，小規模から大規模なネットワークにまで幅広く適用可能という理由からSNMPを管理プロトコルに採用した．

3.2 システム概要

図5に本システムの構成を示し，以下にコンポーネントのいくつかについて説明する．



NMKB: Network Management Knowledge Base
NIB: Network Information Base
NTP: Network Time Protocol

図 5: システム構成

3.2.1 管理アプリケーション,NIB (Network Information Base)

実装した管理アプリケーションを，管理目的毎にまとめてみると次のようになる．

構成管理	• コンフィグレーションモニタ
性能管理	• MIB ブラウザ
	• トラヒックモニタ
	• ルーティングモニタ
	• 各種リポート作成ツール
障害管理	• ネットワークインタフェース監視モニタ
	• プロトコルアナライザ

NIBにはマネージャがこれらのアプリケーションを用いて各エージェントから収集した管理情報が蓄積される．

3.2.2 ネットワーク管理エキスパート

ネットワーク管理エキスパートは，管理の専門家の知識が格納されているNMKB とNIBに蓄積された管理情報から推論を行ない，管理者の支援を行なう．NMKBに格納される管理知識には，ネットワーク監視，異常の自動検出，障害対策，ユーザインタフェースの制御等がある．

例えば外部ネットワークに低速度の回線で接続しているサイトに，「一般ユーザがビジネスタイムに外部ネットワークに対してFTPを行なってはいけない」というローカルルールがあったとすると，それを監視するための知識は以下のような知識として記述することができる．

```
if Gateway.tcpConnLocalPort = FTP   and
   time is between 9 am and 5 pm    and
   today is not holiday             and
   remoteMachine is not PrivilegedMachine
then send warning to remoteMachine
     send notice   to systemAdminstrator
     send notice   to Logbook.
```

3.2.3 ユーザインタフェース

システムの操作や，収集した情報を表示するグラフィカルユーザインタフェースに加えて，管理者に異常を通知するためのポケットベル，FAX，電話等の通信機器もインタフェースとして持つ．管理者は，マネージャが実装されている計算機の前にいつも座っているわけではない．したがって，異常あるいは異常の兆候が検出された時にだけ管理者に通報するユーザインタフェースは，管理を確実なものとし，管理者の負担を軽くする上で大変有効である．

ネットワーク管理エキスパートは，これらのインタフェースの利用に関する知識も有しており，障害のタイプと管理者のスケジュールに応じて適切な通信機器を選択して管理者に通知する．

3.2.4 拡張MIB(XMIB)

拡張定義したXMIBは現在次に示す5つの管理オブジェクトグループからなる．

The extended System Group

標準MIBにおけるSystemグループの拡張．エージェントが動作している計算機のCPU負荷やディスクの残量等に関するグループ．計算機がダウンする原因の多くがディスクフルによることから，ディスクの残量を知ることは特に重要である．

The Statistics Group

エージェントが接続するネットワークセグメントのトラヒック統計情報に関するグループ．標準MIBのThe Interfaces Groupに相当する情報に加えて，プロトコル毎やアプリケーション毎の統計情報を持つ．これらの情報はネットワークインタフェースから直接Etherフレームを読むことによって収集している．

The Time Labeled Object Group

上記The Statistics Groupの管理情報を測定時間情報に基づいて収集するグループ．詳細は4章で述べる．

The Packet Dump Group

プロトコル毎にパケットのヘッダ部分のダンプリストを持つ．マネージャがプロトコルアナライザを用いてパケットの詳細分析を行なう際に利用される．

The Alarm Group

ディスクの残量や異常トラヒックに対して，警告を発するための閾値を設定するグループ．例えばこのグループのalarmIcmpPkts というオブジェクトに整数値 n を設定すれば，1分間に n パケットを越える ICMP パケットがネットワークに流れた場合には，エージェントからマネージャに対して snmp-trap メッセージが送られる．

4 時間を導入した管理の実現

本章では，提案したネットワーク管理モデルの2つ目の特徴である“時間を導入した管理”の AIMS における実現方法について述べる．

4.1 必要とされる機能とその実現

正確なネットワークの状態解析，性能評価，障害対策を行なうためには，単に管理情報にタイムスタンプを付加するだけでなく，時間に関する次の2つの機能が必要であると考える．

1. マネージャ及び全管理対象間での時間の一致．
2. 指定時間から一定間隔で管理情報を測定する機能．

1番目の機能はネットワーク上の計算機の時間を同期させるプロトコルである NTP (Network Time Protocol)[13] を利用して実現した．

2番目の機能を実現するに当たってはいくつかの問題が生じた．この機能を実現する最も単純な方法は，マネージャが自らが持つ時計に従って，一定時間間隔でエージェントにポーリングを行なう方法である．しかしこの方法では，ネットワーク負荷によるエージェントへの要求メッセージの到着時間のずれや，エージェントの CPU 負荷による要求メッセージに対する処理時間のずれにより，測定時間間隔は正確なものではなくなる．特にマネージャとエージェントが1対多の関係になった場合には，同一時刻にポーリングを行なうことは不可能であるため，エージェント間での測定時間の一致は実現できない．さらに，ポーリングにはトラヒックを増大させてしまう欠点がある．

これらの問題点を解決するために以下の方針をとった．

- 管理オブジェクト毎に測定開始時間，測定間隔，測定回数を設定できるように MIB を拡張し，これらの情報によりエージェントに自律的に情報収集を行なわせる．
- 測定した管理情報は，測定終了後マネージャが一括して回収することにより，通信の回数を減らす．

ポーリングによる方法と，本提案方法のアクセスシーケンスを比較してみると図6のようになる．

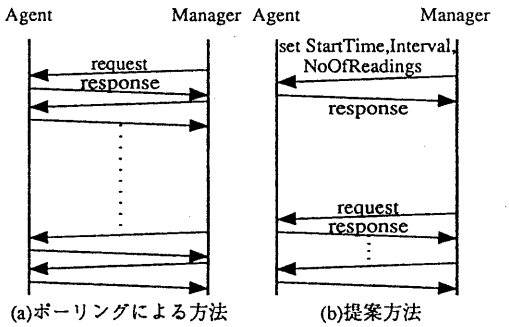


図 6: アクセスシーケンス

この方式は，マネージャ・エージェント間のトラヒックを軽減できるばかりでなく，次のような長所を持つ．

- 管理のための通信の影響を受けないネットワークの状態を測定可能．
- 通信処理のために要していたマネージャ，エージェント双方の CPU 負荷の軽減が可能．
- 通信とその処理時間が無くなるため，ポーリングによる方法に比べてより短い測定間隔の設定が可能．

図7に本提案方式を実現するために採用したエージェントの構成を示す．

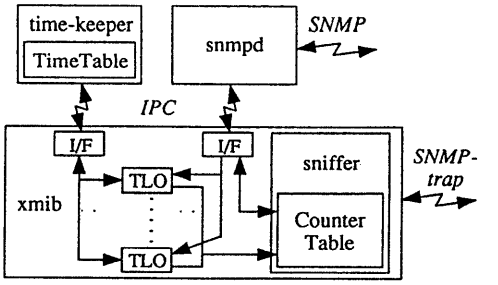


図 7: エージェントの構成

エージェントは3プロセスから構成されており，それぞれがプロセス間通信を用いて相互に通信を行なう．

snmpd　マネージャとのSNMP通信を行ない標準MIBを持つ.

xmib　拡張MIBに定義されたオブジェクトの値を収集する. snifferは接続するネットワークセグメントから拡張MIBにおけるThe Statistics GroupとThe Packet Dump Groupの管理情報を収集する. TLOにはプロトコルやアプリケーション毎に測定時間情報やその情報に基づいて収集された管理情報, アラームに関する情報が保存されている.

time-keeper　測定時間情報をテーブルに持ち, 測定時間になった場合にxmibにその旨通知する.

例えば, 測定時間情報に基づいて情報収集を行なう場合には次のような処理手順となる. 先ずsnmpdはマネージャからの測定時間情報のset要求を受けとるとそれをxmibに伝え, それらの情報は該当するTLOに保存されると同時にtime-keeperにも送られTimeTableに登録される. time-keeperは常にTimeTableを監視しており, 測定時間になったオブジェクトが存在した場合には, xmibにどのオブジェクトが測定時間になったか通知する. xmibはその通知に基づいてsnifferのCounterTableから該当オブジェクトの値を取りだしTLOに保存していく. マネージャは測定終了後に要求した個数分のget要求を出し, snmpdを経由してTLOから保存されている管理情報を一括回収する. この時, 測定個数分のGetRequest-PDU (Protocol Data Unit), GetResponse-PDUが生成されるのではなく, 複数個のオブジェクトが1つのPDUにまとめられて通信が行なわれる.

4.2 評価

NTPの性能に関しては文献[14]において, 約90%の計算機が時間差 10 msec 以内に, 約99%が時間差 50 msec 以内に一致できたことが報告されている.

次に, 提案方法(図6(b))と, ポーリングによる方法(図6(a))とのマネージャ・エージェント間のトラヒックの比較結果を表1に示す.

差の主な原因は通信回数の差によるものである. 例えば測定オブジェクトが1個の場合, ポーリングによる方法では測定回数100回でrequestとresponseで合計200回の通信が行なわれる. これに対して提案方法では, 測定時間情報をsetするのに応答含めて2回, 1PDUで扱かえるカウンタオブジェクト数は最大24個であるから, 収集された100個の管理情報を回収するのに10回(requestとresponseそれぞれ24個ずつ4回と残り4個を1回)の合計12回で済む. つまり, その差188回分の通信に必要とされるプロトコルヘッダの分だけトラヒックを削減できる. しかし, 測定オブジェクト数が, 1PDUで扱える

【比較条件】
- 測定はCounter Objectだけで, 測定回数は100回.
- コミュニティは"public".
- 通信エラーは無いものとする.
- 1個のPDUで扱えるCounter Objectは最大24個とする.

object数(個)	pollingによる方法(byte)	提案方法(byte)	差(byte)
1	20,300	4,492	-15,808 (-77.9%)
6	37,600	25,284	-12,316 (-32.8%)
12	57,400	50,560	-6,840 (-11.9%)
24	97,800	100,950	+3,150 (+3.2%)
30	135,400[1]	117,638	-9,166 (-6.8%)

[1] 1個目のPDUで24個, 2個目で6個のオブジェクトを扱う.

表1: マネージャ・エージェント間のトラヒック比較結果

オブジェクト数に一致した(上記の条件では24個)場合には, 提案した方法でも情報回収時にポーリングによる方法と同じ回数分の通信が必要となり, 初めに測定時間情報をセットする通信の分だけトラヒックは大きくなる.

以上より, 提案方法によれば, 測定オブジェクト数が1PDUで扱えるオブジェクト数に一致する場合以外は, トータルなトラヒックをある程度軽減できることが分かった. しかし, ネットワークの状態を正確に調べたい場合には, 管理情報を収集するための通信は排除されるべきであり, ポーリングによる方法よりトラヒックが増えてしまうとしても, 本方法は有効であると思われる.

5 AIMSの利用

本章では, 筆者らがAIMSを利用してどのようにネットワークの管理を行なっているかを紹介する.

図8にAICのネットワーク構成を示す. このネットワークを管理するために, マネージャをWIDEインターネットへのゲートウェイであるaic-wideに, エージェントをWNOC (WIDE Network Operations Center)であるwnoc-snd, 外部とISDNで接続しているaic-isdn, そして3つのサブネットワークのそれぞれに1台づつ実装している. さらに, モデム監視用の管理アプリケーションをaic-uucpに実装している.

ネットワークインタフェイスの監視

ネットワーク管理における最も基本的な管理は, ネットワークをダウンさせないことである. そこで, WNOCとゲートウェイのネットワークインタフェースの状態(MIBのifOperStatusの値), 具体的にはwnoc-sndのWNOC-SFC, 東北大学, 当社向けの各インタフェースとaic-isdn

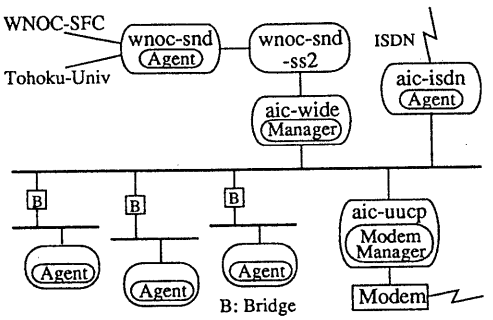


図 8: AIC のネットワーク構成

の ISDN インタフェースの状態を監視し，ダウンした場合には管理者に通知するとともにログに記録している．wnoc-snd のネットワークインタフェース監視ログの例を図 9 に示す．

```
**********************************************************
# Error Log on host.name [ wnoc-snd ] for Jan 10 1992 #
**********************************************************

    Polling Start Time =   00:01:01
    Polling Interval   =   60 sec

 17:18:01  ifOperStatus.8 changed from  Up    to  Down
 17:19:01  ifOperStatus.8 changed from  Down  to  Up
 19:24:01  ifOperStatus.8 changed from  Up    to  Down
 19:26:01  Error Occurred. No Response.
 19:28:01  Returned to Normal.
 19:28:01  ifOperStatus.8 changed from  Down  to  Up
                    === OVER ===
```

ifOperStatus.8 は WNOC-SFC へのインタフェースを示す．

図 9: ネットワークインタフェース監視ログの例

モデムの監視

aic-uucp にはモデムを監視する管理アプリケーションが動作しており，モデムに何らかの異常が検出された場合には snmp-trap メッセージをマネージャに送る．マネージャはメッセージを受けとるとネットワークインタフェースの場合同様，管理者に通知するとともにログに記録する．現在は 一つの管理アプリケーションとして実現しているが，将来的にはモデムを管理する代理エージェント (Proxy Agent) として実装する予定である．

トラヒック情報の収集及びリポート作成

ネットワークの負荷や利用状況を調べるため，wnoc-snd から各種管理情報を 1 分間隔で収集し，1 日，1 週間，1ヶ月単位のリポートを自動作成している．これらのリポートは上記の目的以外に，監視のための情報を得るためにも利用している．例えば，通信エラーに関係するものとして，入力パケットエラー数 (ifInErrors) や，ICMP のパケット数 (icmpInMsgs) の平常時におけるおおよその最大値を導き出し，その値を拡張 MIB の The Alarm Group のオブジェクトにセットすることによって，通信エラー関係のパケットが特に多く流れた場合には，異常の兆候としてマネージャに通知するようにしている．図 10 に，月間リポートより作成した wnoc-snd における入力パケット数の変化を示す．

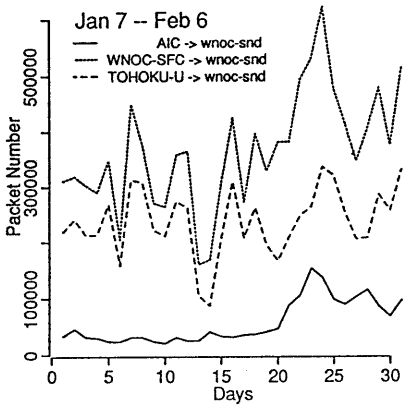


図 10: wnoc-snd における 1 カ月間の入力パケット数

ポケットベルによる管理者への異常の通知

現在，管理者への異常の通知にはポケットベルを多用している．この時，マネージャである aic-wide には電話インタフェースがないため，snmp-trap メッセージが届いた場合には，aic-isdn 上のプロセスを起動して isdn インタフェースからポケットベルをコールする．仙台地区ではユーザが作成する自由な文章をポケットベルに表示するサービスはまだ提供されていないため，あらかじめ登録したいくつかの文節を組み合わせることによって，例えば「WNOC の mcp がダウンです」程度のメッセージを管理者に伝えるようにしている．

図 11 に AIMS の画面例を示す．

6 おわりに

本論文では，現状のインターネットワークの管理を目的としたネットワーク管理モデルを提案し，そのモデルに基づいて我々が設計したエキスパートネットワーク管理システム AIMS の実現方法及びその利用例について述べた．

AIMS のエージェントは標準 MIB に加えて，接続するネットワークセグメントのトラヒック情報を収集する機能も持っており，1 ネットワークセグメントに最低 1 つのエージェントが存在すれば，ネットワーク全体のトラヒッ

クに関する管理が可能となっている．また，管理情報に測定時間情報を付加することにより，時間を導入した管理が可能である．

今後は，AIMS を利用してより多くの管理を実際に行ない，そこから得られる知見をもとに知識ベースの高度化を行なっていく予定である．

謝辞

本研究に対し，有益な御助言をいただいた東北大学野口正一教授，白鳥則朗教授，AIC 緒方常務，ならびに多くの議論，ご指導をして頂いた秋田大学坂田真人教授に深謝致します．また，貴重な意見を聞かせて下さった WIDE プロジェクトメンバーの皆様に感謝の意を表します．

参考文献

[1] 村井 純ほか,"WIDE プロジェクト 1990 年度研究報告書",1991.

[2] 平原正樹, "X.25 網を利用した IP ネットワークの構築", 情報処理学会研究報告, マルチメディア通信と分散処理 51-3,1991.

[3] Tania Volochine,G.S.Subramanian,Ronald W. Toth, "Network Management and Traffic Analysis for CICNet", IEEE Network Magazine,Vol.5,pp.41-50,1990.

[4] 中村修, 北島剛, 村井純, "大規模広域ネットワークにおける RTT に関する考察", 情報処理学会研究報告, マルチメディア通信と分散処理 51-6,1991.

[5] 菅原俊治, "大規模インターネットワーク診断 / 監視エキスパートシステムについて", 電子情報通信学会論文誌,Vol.J73-D-I,No.12,pp.990-996,1990.

[6] 菅原俊治, "TCP/IP によるインターネットワークにおけるある障害の自動発見方法について", 情報処理学会研究報告, マルチメディア通信と分散処理 49-1,1991.

[7] G.MANSFIELD et al., "An SNMP-based Expert Network Management System", 電子情報通信学会研究会資料,CS91-69,1991.

[8] 村田眞人, 時庭康久ほか, "SNMP を利用したエキスパートネットワーク管理システム (1)(2)", 情報処理学会第 43 回全国大会論文集 (1),pp.275-278,1991.

[9] ISO/IEC 9596 (1989).

[10] RFC-1189 (1990).

[11] Marshall T.Rose, "The Simple Book - An Introduction to Management of TCP/IP-based Internets", Prentice Hall,1991.

[12] RFC-1155,1156,1157,1158 (1990).

[13] RFC-1119,1128 (1989)

[14] David L.Mills, "On the Accuracy and Stability of Clocks Synchronized by the Network Time Protocol in the Internet System", Computer Communication Review,Vol.20,pp.65-75,1990.

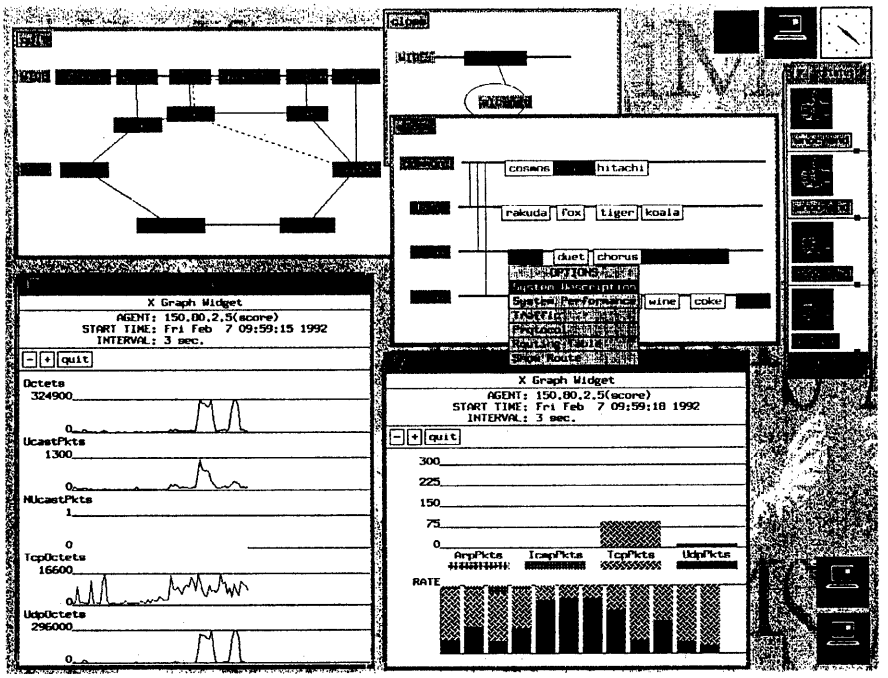


図 11: AIMS の画面例