Memoirs of the Faculty of Science
Kochi University (Information Science)
Vol. 26 (2005), No. 5

高知学園短期大学における LAN 監視システム構築

Local Area Network Monitoring System in Kochi Gakuen College

濱田　美晴[†]　菊地　時夫[††]
Miharu Hamada[†]　Tokio Kikuchi[††]

要　旨

高知学園短期大学においては，平成 11 年度から 12 年度にかけて構内ネットワークの導入・整備が行われた．しかし，その後端末の増加に伴い順次必要箇所へ HUB とケーブルを増設していったため，多段接続となりその構造が複雑化していた．このため，問題点の多かった旧ネットワークを改善し，平成 15 年度末にはスター型の光ケーブル配線による新ネットワークへと移行した．

本研究では，新ネットワークについてパケット流量計測による監視システムを構築した．システム構築監視の基本目的は，(1) ネットワーク構成機器のパケット流量を測定すること，(2) ネットワークに障害が発生した場合や接続不良の要因を特定すること，(3) ネットワーク構成機器の障害や故障に迅速に対応すること，(4) 管理者の負担を軽減することである．

ネットワークシステムを管理するためのツールとして一般的に SNMP（Simple Network Management Protocol）が用いられている．SNMP はネットワークを構成する機器（エージェント）に内部情報を保持し，監視サーバ（マネージャ）からネットワークを通じてその情報を管理する仕組みであり，本研究ではこの SNMP を利用した監視システムを構築した．

システム構築にはデータベース部に PostgreSQL を，データベースとの連携を図るため Python プログラム言語と Apache ウェブサーバを用いた．本システムの最大の利点は，データベースの検索機能を付加したことでグラフ表示に自由度を持たせたことである．管理画面は，パケット流量の大きさや異常を，数値のみでなく画像で表現できる仕組みを備えた．また，メール通知システムの導入により障害発生時にメールで異常を知らせる機能を持つため，迅速な対応が可能となっている．

1. はじめに

情報・通信ネットワークの急速な拡大とともに，教育活動や商業活動などにおいてもその重要度は増し，情報化社会の新しいインフラストラクチャとなっている．そうした中で，ネットワークに障害や機能低下が発生すると，様々な業務にも影響を及ぼす問題にもなりかねない．今や，効率的なネットワークの運用・管理は，企業や教育現場においても重大な課題となり，ネットワークを構成する中継機器（ハブやルータ）の障害発生に即座に対応できるような仕組みが必要であると考える．

† 高知大学大学院理学研究科数理情報科学専攻
Department of Mathematics and Information Science, Kochi University
高知学園短期大学
Kochi Gakuen College
†† 高知大学理学部
Faculty of Science, Kochi University

しかし，現在では，ネットワークを構成する機器の数が多くなり，インテリジェントハブや，ルータの数が数十を超えてくると，各機器を 1 台 1 台管理することは困難な状況となった．そこでネットワークに接続された機器の情報をネットワーク経由で収集・管理する仕組みが考えられてきた[1]．それが SNMP (Simple Network Management Protocol)[2] と呼ばれるネットワーク管理を行なうための基本プロトコルである．監視サーバ（マネージャ）はネットワークを構成する監視対象機器（エージェント）が持つ MIB (Management Information Base) と呼ばれる機器の状態を表す管理情報のデータベースにアクセスし，それによってネットワーク上のノードやサービスの設定状況，あるいは稼動状況を管理することが可能となっている．

本研究ではこの SNMP の仕組みを利用し，高知学園短期大学 LAN におけるネットワーク監視システムを構築しパケット流量の計測を行った結果を報告する．

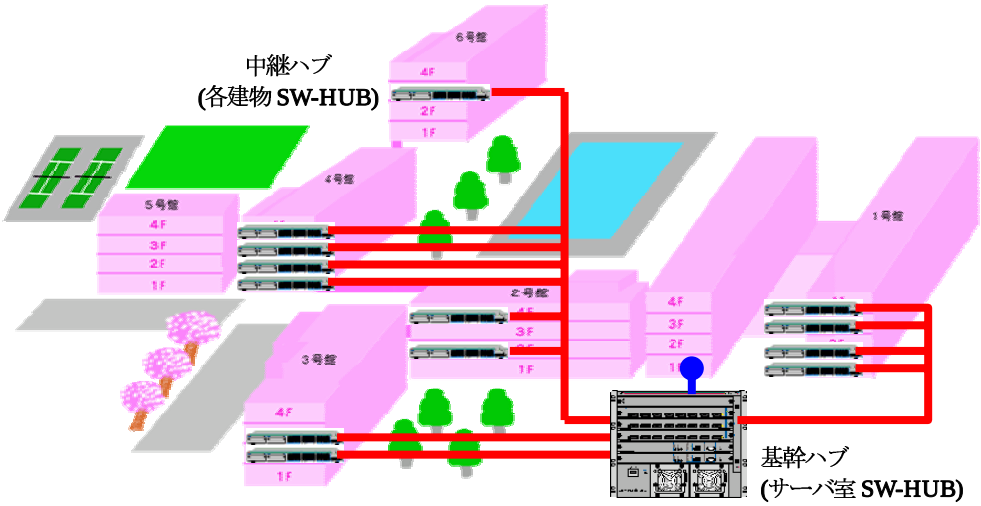

図 1　光ケーブルによる基幹ネットワーク

高知学園短期大学では，快適に利用できる理想的な構内ネットワークシステムを目的とし，セキュリティ問題，使用状況・場所による回線の混雑等，旧ネットワークにおけるいくつかの課題となる点を改善し，平成 15 年度末に新ネットワークに移行した．しかし，いずれの場合もネットワークを監視するシステムが導入されていなかった．中継機器などに障害が発生した場合，その発生箇所を特定することがとても困難な状況であり障害復旧に多大な人的労力が必要とされていた．

そこで，本研究では LAN におけるネットワーク監視システムを構築することでネットワーク内のパケット流量を計測するとともに，障害発生時に対応できるシステムを構築したいと考えた．ネットワークを構成する中継機器が内部に保持する情報のうち，パケット流量を SNMP の仕組みを利用して取得することにした．筆者の一人による先行研究[3]では，旧ネットワークにおいて SNMP のマネージャにオープンソースソフトウェアである MRTG (Multi Router Traffic Grapher)[4] を利用して計測を行い，一定の成果をあげることができた．

新ネットワークにおいては，高知学園短期大学独自の SNMP 監視システムを構築することで，より一層ネットワークの運用・管理をスムーズに行うことを目的としている．本システムの大きな特徴は，SNMP から得られた情報をデータベース (PostgreSQL[5]) に蓄積し，過去ログの検索機能を装備したことである．検索機能を付加することで，グラフ表示にも自由度をもたせることが可能となった．Web サーバ (Apache[6]) からは，Mod_Python[7] によりファイルの入出力を行うことでデータベースサーバや Web ブラウザとの連携を行っている．また本システムの最大の特徴として，管理者の負担をできるだけ軽減したいという観点から，十分な視覚化を行ったシステム構築となっている．

2.　ネットワーク構成

高知学園短期大学新ネットワークは，光ファイバーを基幹とする高速ネットワークで構築している．図 1 に示すように，サーバ室の Switching Hub（基幹ハブ）から各建物の Switching Hub（中継ハブ）へとスター型に接続される基幹ネットワーク部を光ファイバーによって構築し，Giga-bit での接続を可能としている．

中継ハブの各ポートからは，直接それぞれの研究室，事務室または教室の情報コンセントにつながり非常にシンプルなネットワーク構成である．このことは，障害発生時の原因と箇所を特定する場合においても発見容易であるといった利点を持ち，ネットワーク管理を行う上で重要な要素となっている．

また，基幹ネットワークを構成する基幹ハブと中継ハブには全てインテリジェントハブを導入し，SNMP に対応しているため，リモートからのネットワーク管理が可能である．基幹ハブのレイヤー3 スイッチ（アライドテレシス SwitchBlade4000）は，中継ハブとの接続用に 13 個の 1000BaseSX と，学生・教員・短大事務・本部事務・共通の各ネットワークのサーバ用に 5 個の 1000BaseT 端子を提供する．また，中継ハブ

にはレイヤー2 スイッチ（アライドテレシス CenterCOM 8224SL）を用い 100BaseTX 24 ポートと 1000BaseSX 1 ポートを持っている．

3. SNMP 監視システムの構成

高知学園短期大学の基幹ネットワークにはリモート管理を可能とするため, SNMP を利用して監視システムを構築した．SNMP 監視システムの構成機器には, UNIX 系 OS 搭載 PC (CPU Celeron2.0GHz，ハードディスク 60GB，メモリ 256MB，OS FreeBSD-4.8[8]) を使用した．

システム全体のプログラミング言語には，プログラミングしやすいこと，後で読みやすいこと，ライブラリが豊富であることなどを考慮し Python[9] を使用した．エージェントの持つ MIB のオブジェクト変数を取得する際には, pysnmp-3.4.2[10] のモジュールを使用し，エージェントに対して snmpget リクエストを送る．本システムでは，MIB の情報として各ポートの入力と出力のパケット流量の値を取得している．また，SNMP から得られた情報をデータベース (PostgreSQL-7.4[5]) に格納し，過去ログの検索機能を装備している．データベース化することでグラフ表示にも自由度をもたせることが可能となっている．Web サーバ (Apache HTTPD-2.0.50[6]) からは，Mod_Python-3.1.3[7] によりファイルの入出力を行うことで, データベースサーバや, Web ブラウザとの連携を行っている．データベースへのアクセスには psycopg-1.1.11[11] を，グラフ表示には gnuplot-py-1.6[12] を使用ており，システム全体として Python で統一しているところにも特徴がある．

SNMP エージェントの対象機器には，基幹ハブ (SwitchBlade4000) と中継ハブ (CenterCOM 8224SL) を設定した．

本研究に用いたシステム構成を図 2 に示す．

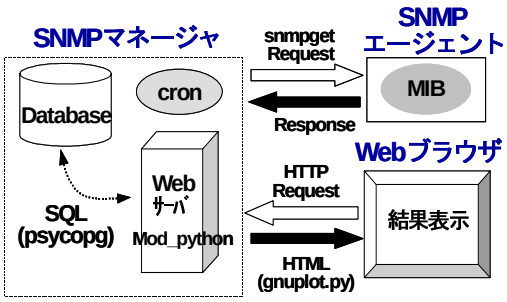

図 2　システム構成

3.1 データベース作成

データベースサーバ構築のソフトウェアとしてオープンソースである PostgreSQL を利用することとした．PostgreSQL は MVCC（Multi-Version Concurrency Control）を提供し, ほとんど全ての SQL の構文（サブセレクト，トランザクション，ユーザ定義型と関数を含む）をサポートし, 幅広い言語バインド (C, C++, Java, Perl, Python) が可能である等の特徴を持つ[12]．

Web 上からデータベースへの入力, 検索を行うための DBMS インタフェース用言語として Python を使用し，データベースと Web との連携には Psycopg を用いた．検索の情報源となるパケット流量値は，エージェントごとにデータベースを作成した（表 1）．

エージェント	データベース名
サーバ室 SW-HUB	snmp
1 号館 1F SW-HUB	build1floor1
1 号館 2F SW-HUB	build1floor2
1 号館 3F SW-HUB	build1floor3
1 号館 4F SW-HUB	build1floor4
2 号館 1-2F SW-HUB	build2floor1_2
2 号館 3-4F SW-HUB	build2floor3_4
3 号館 1-2F SW-HUB	build3floor1_2
3 号館 3-4F SW-HUB	build3floor3_4
4-5 号館 1F SW-HUB	build4_5floor1
4-5 号館 2F SW-HUB	build4_5floor2
4-5 号館 3F SW-HUB	build4_5floor3
4-5 号館 4F SW-HUB	build4_5floor4
6 号館 1-4F SW-HUB	build6floor1_4

表 1　データベース一覧

3.2 テーブル作成

基幹ハブのデータベース（snmp）は，各中継ハブにつながるインタフェースごとにテーブルを作成し，テーブル名を中継ハブの設置箇所（例えば build1floor1）とした（表 2）．中継ハブのデータベースも，24 ポート分のテーブルを作成し，テーブル名を port1，port2…port24 とした．それぞれのテーブルには，日付，入力パケット流量，出力パケット流量をデータに持つ（表 3）．

データ入力には，インタフェースのパケット流量を 5 分間ごとに cron で取得し, データベースに蓄積する．エージェントの持つオブジェクト変数を取得する際, IP アドレス，Community Name，OID の 3 つの引数を snmpget コマンドに送ることで値が返される．また，各インタフェースの入出力オクテット（バイト）数をそれぞれ表す inoctets と outoctets の値は，MIB

の情報をそのまま取り出しておりいずれも統計値として値が蓄積される．日付は timestamp 型に変換し，表示している．

Port No.	Table Name
Port. 2.1	build1floor1
Port. 2.2	build1floor2
Port. 2.3	build1floor3
Port. 2.4	build1floor4
Port. 2.5	build2floor1_2
Port. 2.6	build2floor3_4
Port. 2.7	build3floor1_2
Port. 2.8	build3floor3_4
Port. 3.1	build4_5floor1
Port. 3.2	build4_5floor2
Port. 3.3	build4_5floor3
Port. 3.4	build4_5floor4
Port. 3.5	build6floor1_4

表 2　テーブル一覧

date	inoctets	outoctets
2005-01-04 14:35:01	1092940046	1145234151
2005-01-04 14:30:00	1092749968	1144184306
2005-01-04 14:25:01	1092474659	1142607753

表 3　テーブル

3.3　データ検索

Web 上から実行要求があると Apache で Mod_python により PostgreSQL との連携を行い，データベース検索 SQL を生成する（図 3）．

```
""" SELECT * FROM %s WHERE date >= '%s%%'
    AND date <= (SELECT cast('%s%%' as timestamp)
    + cast('%s%%' as interval))
    ORDER BY date DESC
""" %(buildno, start_time, start_time, period)
```

図 3　データベースへの問い合わせ

Mod_python は Apache のサーバーサイド処理（ハンドラ）を Python で書くことができるようにする Apache モジュールである．また，Mod_python は，インタプリタがサーバと一緒に動いているので実行速度が早い．そのため，データベースに頻繁にアクセスするようなアプリケーションでは一般に利用される CGI と比べて有効であると考えられる．本システムでは，その Mod_Python を使用してデータベースサーバと Web ブラウザとの連携を行っていることが大きな特徴の一つとして挙げられる．Mod_Python のハンドラ関数の引数は，buildno，日付，期間であり，Web でリクエストがあると必要な処理を行い HTML 文書またはグラフ（画像）にしてブラウザに返す．このように，要求と応答が全て Web ブラウザで行われているため，原理的にはネットワークに繋がれているどの PC からでもアクセスが可能である．ただし，セキュリティ上学内のネットワークを VLAN でセグメントが分割しているため，管理用グループ IP アドレスでアクセス許可して本システムの使用を管理者に限定している．

また，本システムでは過去データを参照する仕組みを備え，Web ブラウザの検索入力フォームから問い合わせ可能である（図 4）．検索フォームの各値が引数となり，図 3 の SELECT 文にわたされることでデータが抽出される．この検索フォームはグラフ表示やログ表示の機能として備えられている．データ取得時には値が定期的（5 分ごと）に入力されているとは限らない．そのため，date 項目を秒数で計算し「前回の値－今回の値／計測時間間隔」でこの間の平均毎秒パケット流量を返すようにする．

実行要求により抽出されたデータは plot.dat, plot2.dat または plot_select.dat として/tmp に置かれ，次に示すグラフ表示のためのファイルとなる．

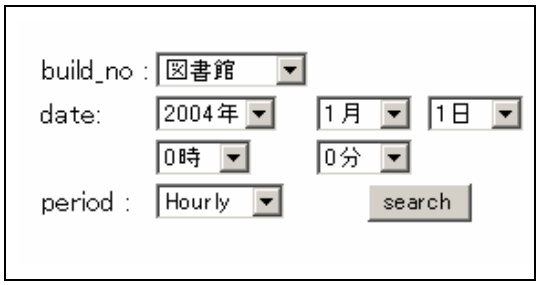

図 4　検索入力フォーム

3.4　グラフ表示

Gnuplot は２次元や３次元のグラフを描くツールである．多くの数学関数を標準に持ち，解りやすいコマンドを使って対話的にグラフを作成することができる．また，出力形式は png，gif など標準的な画像形式がサポートされているため，本ツールを使用することとした．

Gnuplot によりデータベースに蓄積された値からある一定期間（hourly, daily, weekly, monthly）を取り出しグラフ化する場合の python プログラムを図 5 に，またそれにより得られたグラフを図 6 に示す．

```
g=Gnuplot.Gnuplot()
g('set terminal png medium')
g('set size 0.50,0.40')
g('set title "%s %s"' %(buildno,date))
g('set xdata time')
g('set timefmt "%s"' % timefmt)
g('set xlabel "hour"')
g('set format x "%H"')
g('set output "/tmp/plot.png"')
f = Gnuplot.File('/tmp/plot.dat', using='1:3',
    title='In:%s'%h[0], with='lines linetype 9
    linewidth 3')
w = Gnuplot.File('/tmp/plot.dat', using='1:4',
    title='Out:%s'%l[0], with='lines linetype 3')
g.plot(f, w)
```

図 5　gnuplot によるグラフ処理

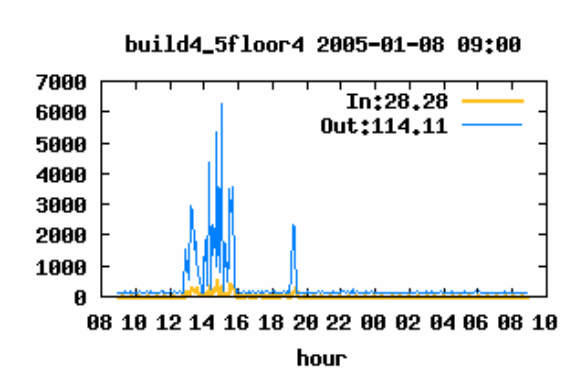

図 6　gnuplot により処理されたグラフ

4.　実験結果

4.1　Web ユーザインタフェース

本学のネットワーク構成は図 1 のようになっており，SNMP のエージェントとして基幹ネットワークを構成する基幹ハブと全ての中継ハブをエージェントに設定した．ただし，基幹ハブにおけるインタフェースのパケット流量を計測することで，学内ネットワーク全体の異常なパケットあるいは，停止状態を把握することが可能と考えられる．そこで，中継ハブのデータは補足的に使用するものとし，主に基幹ハブ（SwitchBlade4000）の計測を行うことにした．

オープンソースソフトウェアの MRTG のように，ポートごとの管理方式の場合は，管理対象が多ければ多いほど管理者側の負担が増大する [3]．そこで本研究では，管理者の負担をできるだけ軽減できるようなユーザインタフェースを作成した．

SNMP 監視システムのインデックス画面では，各エージェントとログ管理ファイルへのリンクボタンの一覧が表示される（図 7）．

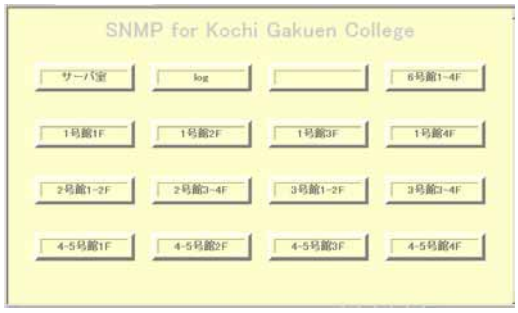

図 7　インデックス画面

インデックス画面から基幹ハブ管理画面へのリンク（サーバ室）を選択することで図 8 が表示される．通常値の場合，各建物のパケット流量が 3 種類の矢印で示されると同時に 5 分ごとの値が表示される仕組みとなっている．このように一目で学内すべてのおおよそのパケット流量が確認できることは，管理者の手間を大いに省いてくれると考えられる．また，右側のグラフは，上部は建物の図を選択することで変化するようになっている．例えば，左画像の 1 号館 1 階をクリックすると，その階の 1 日の入出力パケット流量値をグラフとして表示する仕組みである．下のグラフは検索オプションから過去データを参照することが可能となっている．

管理画面は建物の配置と中継機器の設置箇所を具体的に示した図になっていることから，学内の誰が見てもその仕組みが理解できるようになっており，これも本監視システムの特徴のひとつである．

検索オプションでは，場所，日時，期間などの選択肢があり，期間は hourly, daily, weekly, monthly のグラフの閲覧が可能となっている．各項目を選択後，search ボタンをクリックすることで過去データがグラフとして表示される仕組みになっている．そのため，下のグラフには daily で過去のグラフを表示することで，上部の現在の値と比較することなどにも応用が可能である．

さらに，通常値の場合は矢印の大きさを変化させ表示していたが，ある一定の値を超えた場合には赤い矢印として表示される為，一目で現在の状態と異常を知ることができるようになっている．

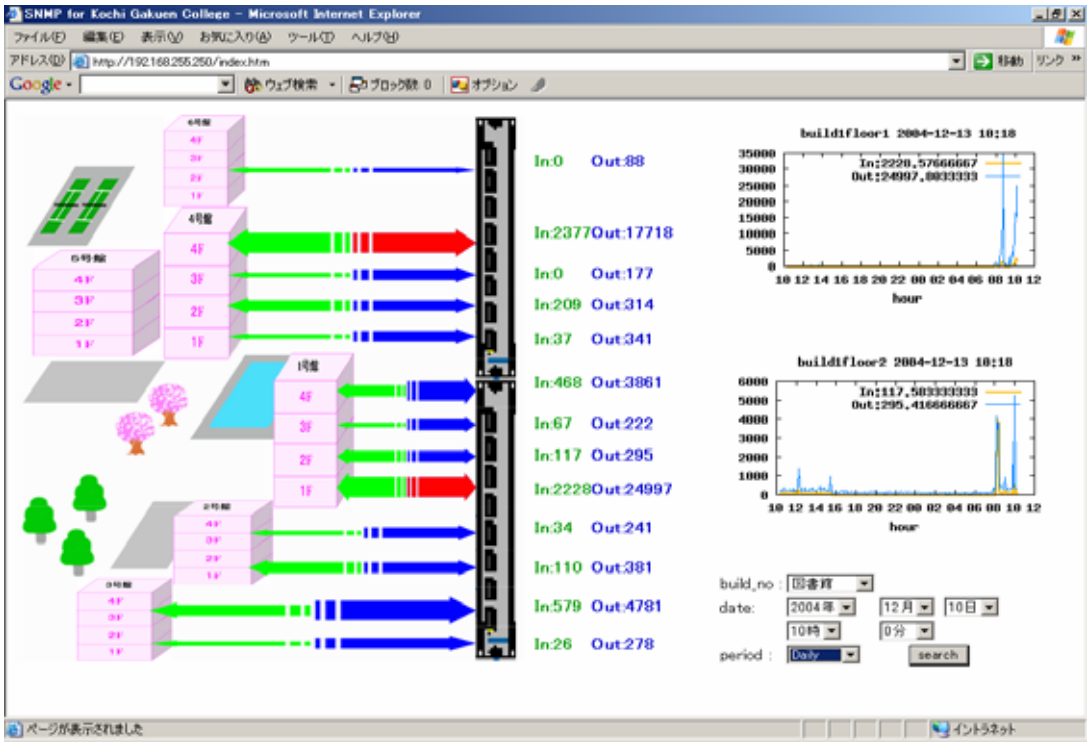

図 8　サーバ室エージェントの管理画面

中継ハブのパケット流量は，各研究室または事務室や教室に直接接続されているポートからの情報を取得したい場合，補足的に使用することがあると考えられ，各々エージェントとして設定することとした（図 9）．

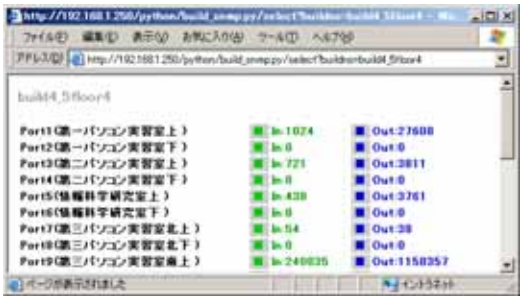

図 9　各建物のエージェント管理画面

これは図 8 で異常値が検出された場合，建物内のどの部分にパケットの異常値が現れているのか詳細を調べることができる．図 9 のインタフェースを使用し，各研究室，事務室または教室に直接繋がるポートの値を見ればその特定が可能となる．

本システム以外のフリーのネットワーク監視ツールには，パケット流量を IP アドレスや Mac アドレス，またはコンピュータ名で表示するツールなどもあるが，高知学園短期大学の場合 DHCP で自動的に IP が割り当てられており，コンピュータ名も登録制でないことからどの部屋に設置されているかの判断ができない．本システムでは直接部屋に接続されたポートを管理するため，こういった状況においても対処可能である．

4.2　ログ管理画面

ログ管理画面は，グラフからは読み取りにくいような細かい値を参照したい場合に使用する（図 10）．

build_no : 図書館
date: 2005年 1月 14日
8時 0分
period : Daily search

date	In Octets	Out Octets
2005-01-15 08:00	15.08	80.8
2005-01-15 07:55	14.68	95.02
2005-01-15 07:50	15.93	84.4
2005-01-15 07:45	14.04	104.95
2005-01-15 07:40	15.31	89.78
2005-01-15 07:35	14.85	114.32
2005-01-15 07:30	15.31	85.82
2005-01-15 07:25	14.68	72.7
2005-01-15 07:20	15.3	102.01
2005-01-15 07:15	15.13	74.77
2005-01-15 07:10	14.63	70.74

図 10　ログ表示画面

通常 MIB の情報はパケットの積算値でデータが保存されているが，本システムのログ管理画面は単位時間当たりのパケット流量（octets/sec）で示されるようになっている．また，ログも指定日時と期間が選択できるようになっており，過去ログの参照も容易である．

4.3 エラー通知システム

さらに，障害発生に迅速に対応するために閾値を超えた場合のメール通知システムを付加した（図 11）．しかし，この場合の問題点は，閾値を超えた時の値は通知するものの，機器の停止時に対する通知システムを備えていないことである．もし停止を知らせる通知システムを作成する場合は，パケット流量値以外の MIB 情報を取得する方法を考えなければならない．

5. システムの利点と今後の課題

以上のように本稿で作成した Web の管理ユーザインタフェースは，ネットワーク管理における負担の軽減を目的としている．今回，高知学園短期大学 LAN の Switching Hub を SNMP 管理対象機器として設定し，計測を行った．基幹ハブと各中継ハブのインタフェースのパケット流量は 5 分間ごとに cron で取得し，データベースに蓄積されている．メイン画面においてはスター型ネットワークの中心に配置された基幹ハブの状況を示し，通常値では 5 分毎の最新情報を表示している．障害発生時や過去データを参照する際には，管理画面の検索フォームから検索キーを入力することで必要な情報を取り出すことが可能である．

また，管理画面はパケット流量の大きさやエラーを数値のみでなく，画像で表現できる仕組みを備えている．これは数値を解析し判断する手間を省き一目でおおよそのパケット流量が監視できるため，管理負担の軽減につながる．

実際，被害の多かったウィルス W32.Welchia.Worm は，ICMP（TCP/IP プロトコルにおいて，その機能を補助するために用意された制御用のプロトコル [14]）エコーを送信することによって現在動作中のコンピュータを探して感染するため，このワームの動作中は ICMP トラフィックが増大する [15]．一つのネットワーク内で感染台数が多くなると，ルータのトラフィックが異常に増加し，停止してしまうといった被害が生じるようである．こういった障害発生の場合にも本システムを使用することで迅速に障害を検知し，対処できると考えられる．

しかし，現在のシステムではパケット流量を測定するのみとなっており，ネットワーク内を流れるパケットの内容までは判断できない。そこで，どういったパケットを監視対象にしていくのかを踏まえ，今後の検討課題としていきたい．また，ネットワーク停止時についても機器の設定内容の履歴管理によって，機器が正常に動作しているかどうかのチェックを行う [16] など，パケット流量計測以外の SNMP 管理手法について様々な仕組みを備えたシステムに改善していきたい．

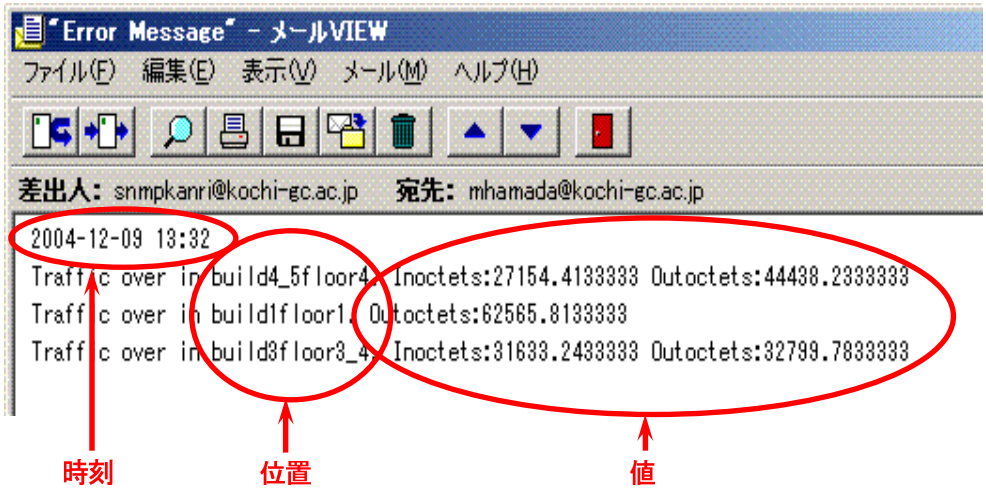

図 11 メール通知システム

6. まとめ

高知学園短期大学では，事務処理の効率化やマルチメディア情報処理を利用した新たな教育支援システムへの対応などを目的とし，旧ネットワークにおける諸問題を解決するために，平成 15 年度末にネットワークの改善を行った．

旧ネットワークにおいて MRTG によるネットワークの性能計測を行うことで，数々の問題点を顕著にした．しかし，MRTG での管理手法は，管理者にとって手間と労力を伴うものであった．そこで，高知学園短期大学の新ネットワークに移行した際，基幹ネットワークにはSNMP の機能を有する中継機器を取り入れ，また，それを管理するマネージャには独自のシステムを導入した．本システムはデータベースによる検索機能を有し，効率的で管理者の負担を軽減できる監視サーバとなっている．管理画面はパケット流量の大きさや異常を数値のみでなく，画像で表現できる仕組みを備えた．また，メール通知システムの導入により，障害発生時にメールで異常を知らせる機能を持つため常に管理画面を監視する必要がなく，迅速に対応が可能となっている．

このように本システムを用いることで，障害発生時には迅速に対応できる管理体制を築くことは，ネットワークのシステムパフォーマンスを最大限に引き出し，しいては高知学園短期大学のネットワークを利用した教育・業務活動において有益であると考えられる．今後も快適・安全，かつ可用性の高いネットワーク運用を心がけ，ネットワーク監視システムをさらに改善していきたい．

謝　　辞

本研究を進めるにあたりご支援，ご討論いただいた地球環境情報学研究室の皆様に感謝いたします．

参 考 文 献

1) Allied Telesis, ネットワーク機器講座｜ネットワーク機器管理編 http://www.allied-telesis.co.jp/library/nw_guide/device/kanri.html
2) IETF (The Internet Engineering Task Force), RFC 1157, A Simple Network Management Protocol (SNMP), http://www.ietf.org/rfc/fc1157.txt (1990)
3) 濱田美晴, ネットワーク監視システムによる高知学園短期大学 LAN のパケット流量計測, 高知学園短期大学紀要, 34:9-17pp., (2004)
4) MRTG :Multi Router Traffic Grapher http://www.mrtg.jp/doc/
5) 日本 PostgreSQL ユーザ会, http://www.postgresql.jp/
6) Japanezed Apache Server Project. http://www.apache.jp/
7) Gregory Trubetskoy, Mod_python マニュアル, http://www.netspice.co.jp/Technic/mod_python/index_html,(2003)
8) Japan FreeBSD User's Group, http://www.jp.freebsd.org/
9) Mark Lutz,David Ascber,初めての Python,オライリー・ジャパン, 432pp.,(2000)
10) Source Forge Net, The PySNMP project, http://pysnmp.sourceforge.net/
11) Zope.org, PostgreSQL Database Adapter, http://www.zope.org/Members/fog/psycopg
12) Source Forge Net, Gnuplot.py, http://gnuplot-py.sourceforge.net/
13)ブルース・モムジャン, はじめての PostGreSQL データベース問い合わせのコンセプト，ピアソン・エデュケーション, 496pp., (2001)
14) ASCII24 - アスキー デジタル用語辞典 http://yougo.ascii24.com/gh/31/003185.html
15) Symantec Security, http://www.symantec.com/region/jp/sarcj/
16) 大垣内多徳, 山下芳範, ネットワーク管理運用支援データベースの構築と運用, 情報処理学会研究報告, DSM-30:1-6pp., (2003)