

# 情報ネットワーク運用上の問題点\*

情報処理センター **今 泉 重 夫**

1995年7月より、奈良大学では、ATM方式による仮想ネットワーク・システム（VPN）を導入して、4年間余り情報ネットワークを利用して来た。1999年4月よりクライアント機（HP Kayak）を65台から140台に増設し、情報利用環境を再整備した。また、カリキュラムの充実（情報基礎、2単位を全学生必修化にした）もはかった。クライアント機の増設に伴ないATMスイッチとその周辺部の設備更新も行い、過去4年間の運用実績にもとづいて、本学で発生した情報ネットワーク上での問題点およびその対処法など整理した。

## 1. はじめに

1991年に教育研究支援統合ネットワーク・システム（SS-NET）の導入に始まり、1992年には、スーパーミニコンピュータ（Convex）、ワークステーション（Sun）、パソコンなどによるLANの構築、1995年には、仮想ネットワーク方式によるキャンパス情報ネットワーク（NUICE）を構築してきた。<sup>(1)</sup> 翌年には、この情報環境の点検を行い、新情報システムとして再構築を行った。<sup>(2)~(4)</sup> 現在、使用している新情報ネットワークシステムを第1図に示した。この様に本学では、情報利用環境を年次計画により整備してきた。

本稿では、過去4年余り運用して来た情報ネットワーク管理方法とそこで発生したトラブル、その解決方法、問題点など整理したので、これらについて報告する。

## 2. 発生した問題点とその対策

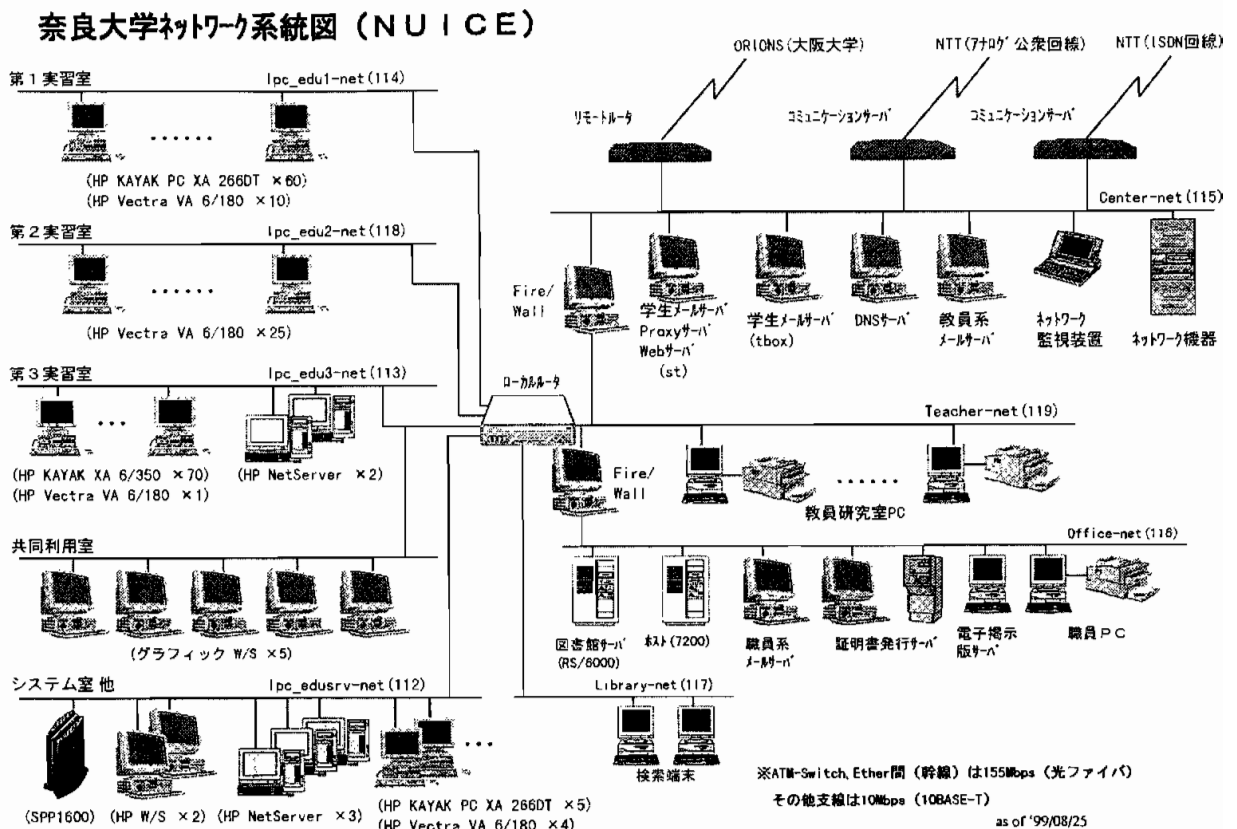
### 2・1 ネットワーク管理

本学のネットワーク管理については、専任の職員（ネットワーク管理者）が配置されていなくセンター付き教職員が仕事の合間に手分けして、その任に当たっている。少人数でしかも片手間の作業になるので、十分なネットワーク管理が行われていないのが現状である。ネットワーク・セキュリティーについては基本的に集中防御方式を採用している。<sup>(5)</sup> すなわち、教育系システムなどは、ファイヤー・ウォールによりセキュリティーを確保し

\* 本稿の内容の一部については、平成11年度 情報処理教育研究集会（主催 文部省・東北大学、平成11年11月12日～13日）にて発表した。同上論文集「文科系大学における情報ネットワーク運用上の問題点」P155（1999）に掲載。

ているが、今までのところ大きな問題は起きていない。時間の許す限り、ネットワーク情報（不正侵入、不正使用等の痕跡の追求、ロギング情報の解析、ユーザー管理、ファイル管理など）を点検、検討しているが充分とは言えない。

情報ネットワークを管理する上で、日々どのように利用されているか概要を知ることが大切なことである。すなわち、何らかの方法で、トラフィック管理を行う必要がある。この最適な方法として、パブリック・ドメイン・ソフトウェア（PDS）のMRTG（The Multi Router Traffic Grapher）があり、本学では、これを利用している。MRTGはSNMPエージェント（たとえば、ルーター）で処理したトラフィックを調べ、その結果をグラフ化するツールである。このMRTGの採用によりトラフィックの様子や過去の履歴を一目で知ることが出来情報ネットワーク管理に関する有用な情報を知ることが出来る。<sup>(6)</sup> 1999年の春休みに、ATMを設備更新して、調整中であった3月30日22時10分のMRTGの様子を示したのが第2図である。上の図から、日、週、月、年のトラフィックの平均値をBytes/Sの単位でグラフ化したものであり、奈良大学より出入りする（流入をグリーン、流出を青で表している。しかも、流入に比べて、流出が常に上回っている。）トラフィックを示している。本学の場合、昼間はネットワークが良く利用されているが、夜間はあま



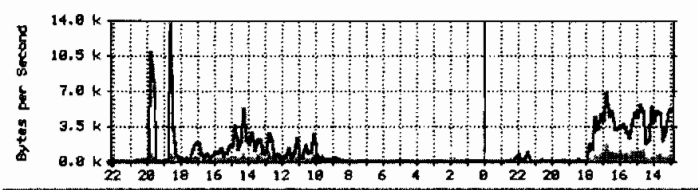
第1図 奈良大学情報ネットワーク・システム図

# Traffic Analysis for Ethernet0

System: router.nara-u.ac.jp in  
 Maintainer:  
 Interface: Ethernet0 (1)  
 IP: No hostname defined for IP address  
 Max Speed: 1250.0 kBytes/s (ethernetCsmacd)

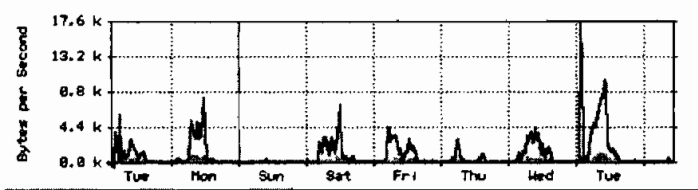
The statistics were last updated Tuesday, 30 March 1999 at 22:10 ,  
 at which time 'router.nara-u.ac.jp' had been up for 5 days, 8:37:53.

## 'Daily' Graph (10 Minute Average)



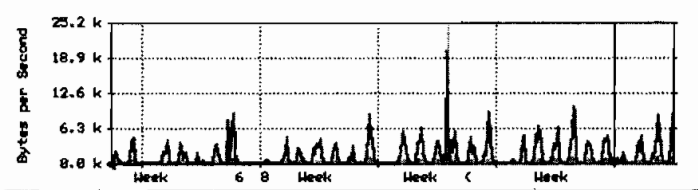
Max In 1880.0 B/s (0.2%) Average In 292.0 B/s (0.0%) Current In 13.0 B/s (0.0%)  
 Max Out 13.7 kB/s (1.1%) Average Out 1139.0 B/s (0.1%) Current Out 17.0 B/s (0.0%)

## 'Weekly' Graph (30 Minute Average)



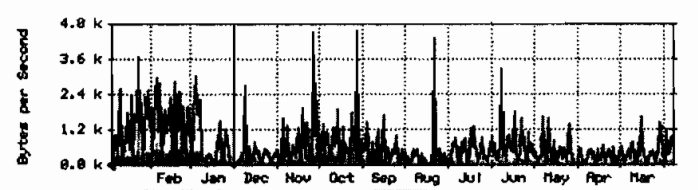
Max In 1417.0 B/s (0.1%) Average In 223.0 B/s (0.0%) Current In 59.0 B/s (0.0%)  
 Max Out 17.3 kB/s (1.4%) Average Out 947.0 B/s (0.1%) Current Out 22.0 B/s (0.0%)

## 'Monthly' Graph (2 Hour Average)



Max In 24.9 kB/s (2.0%) Average In 386.0 B/s (0.0%) Current In 182.0 B/s (0.0%)  
 Max Out 19.9 kB/s (1.6%) Average Out 1292.0 B/s (0.1%) Current Out 1655.0 B/s (0.1%)

## 'Yearly' Graph (1 Day Average)



Max In 3689.0 B/s (0.3%) Average In 188.0 B/s (0.0%) Current In 266.0 B/s (0.0%)  
 Max Out 4558.0 B/s (0.4%) Average Out 641.0 B/s (0.1%) Current Out 1193.0 B/s (0.1%)

GREEN ### Incoming Traffic in Bytes per Second  
 BLUE ### Outgoing Traffic in Bytes per Second

り利用されていないことがわかる。また、回線速度が1.5 Mb/Sであるため、昼間でもまだ回線利用に余裕があることがわかる。この一般化されたスペクトラムを知っていれば、不規則なスペクトラムを示した時、その内容をさらに詳しく調べて不正利用を推測することが出来る。過去に、この方法で不正使用を止めたことがある。

## 2・2 情報ネットワーク・トラブル

本学の情報ネットワークの運用開始(1995.7)から4年間(1999.8)までにネットワーク運用上で発生したトラブルは、全部で29件であった。これは2ヶ月間に1件の割合で何らかのトラブルが発生したことになる。原因別に整理したものを第1表に示した。予想される通り、ATM、サーバー関係のトラブルが多い。

第1表 情報ネットワーク運用上で発生したトラブル ('95.7 - '99.8)

ATM 関係	11件
サーバー関係	9
周辺装置 (ルーター、ハブ等)	3
Fire/Wall	2
その他	4
合 計	29件

この内容をさらに詳しく分析したのが、第2表、第3表である。ここに番号は、トラブルの発生順に付けたシーケンス番号、症状は、トラブルの具体的な内容を表し、期間はネットワークが止まった期間(VPN方式のため、全面的な停止はなく、ほとんどが部分的な停止である)、トラブルの原因とそれに対して取った対策例を表にしたものである。これらの結果をまとめると、

- ① 一時的にトラブルが発生すると、同じような箇所で、集中してトラブルが起こる。
- ② 次元の低い不注意(ケアレスミス)で発生するトラブルによるネットワーク停止も結構ある。
- ③ トラブルが複合している場合、原因を特定するのに時間が必要で、そのため、ネットワーク復旧に時間がかかる。
- ④ また、原因が容易に分からない時や原因を特定できない場合も復旧に時間がかかる。

などである。

情報ネットワーク上で発生するトラブルを無くし、いつも快適なネットワークとして利用して行くためには、日頃の情報ネットワーク管理と保守、関係者の日々の技術力の向

第2表 トラブルの原因と対策 (I)

番号	症状	期間	原因	対策
1	ATM トラブル	2日	ハード・エラー	故障カードの交換
2	ATM トラブル	7日	ATM駆動ソフトのバグ	リセットして復旧
4	ATM トラブル	0.5日	ATM駆動ソフトのバグ	リセットして復旧
6	ATM トラブル	0.5日	ATM駆動ソフトのバグ	駆動ソフトのバージョン・アップ
7	ATM トラブル	1日	ハード・エラー	部品の交換
16	ATM-Ether	0.5日	ハード・エラー	本体の交換
17	ATM-Ether	0.5日	ハード・エラー	本体の交換
24	ATM-Ether	1日	ハード・エラー	本体の交換
25	ATM トラブル	0.5日	リセットのタイミング不適	設定ファイルの再構築
27	ATM トラブル	1日	異常ハングアップ	リセット後、コンフィグの再設定
29	ATM トラブル	0.5日	ハード・エラー	本体の交換
3	電子メール・サーバーの不動	1日	動作不安定(?)	リセットして復旧
5	ネーム・サーバーの不動	2日	磁気ディスクのクラッシュ	ディスクの交換
8	サーバー機のトラブル	5日	磁気テープ装置(DAT)故障	磁気テープ装置の交換
19	サーバー機の不動	2日	磁気ディスクのクラッシュ	ディスクの交換と再設定
20	電子メールの送受信不能	2日	設定のミス	ソフト(sendmail)の改良
22	電子メールの送信不能	0.5日	設定の不備	ソフトの改良と再設定
23	ネーム・サーバー機の不調	1日	ディスプレイの故障	ディスプレイの交換
26	サーバー機の不調	—	動作不安定(?)	リセットして復旧
28	リモート・ルータの故障	1日	落雷による停電	ルータ電源、メモリーの交換、UPSの増設

第3表 トラブルの原因と対策 (II)

番号	症状	期間	原因	対策
9	事務系ネットの動作緩慢	約1月	(トラフィック) 過負荷	SW-HUBの増設
10	事務用オフコンと不通	1日	オフコンの設定不十分	リポートにより復旧
11	一部ネットワークの不通	5日	光ケーブルの接触不良	再設定
12	F/Wの動作不安定	2日	ソフト・エラー (バグ)	ソフトのバージョン・アップ
14	F/Wの動作不安定	1日	(増設による) 設定ミス	再設定とメモリー増設
13	一部ネットワークの不安定	約1月	IPアドレスの重複	IPアドレスの再設定
15	一部機器の未動作	約1週	hosts ファイルの削除	hosts ファイルの復元
18	ネットワークの停止	1日	落雷による瞬間停電	ソフト等の再設定
21	ネットワークの動作緩慢	約1週	IPアドレスの一斉取得	時差立ち上げで対応(DHCP)

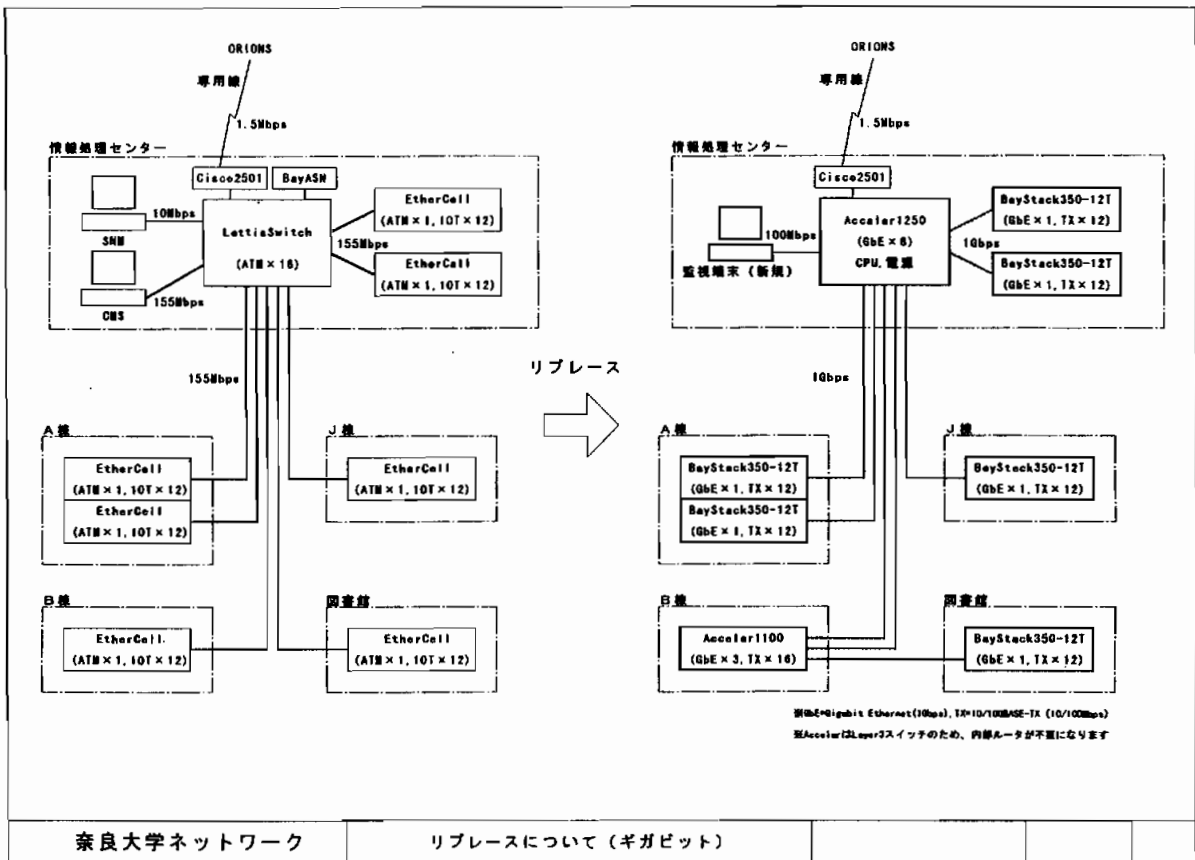
上などが必要である。

## 2・3 情報ネットワークのトラブル対策

### 2・3・1 ネットワーク機器（ATMスイッチ、ATM-Etherなど）の更新

第1表～第3表から、情報ネットワークの要であるATM関係のトラブルが、ハードウェア、ソフトウェア共に多いことがわかる。導入時（1995年の始め）には、ATM装置も初期の製品であり、3年間の使用経験により、昨年末に情報ネットワーク全体の見直しを行った。その結果、ATM装置本体、ATM-Ether、周辺装置など全面的な改善が必要となった。設備更新にあたり、

- ① 情報ネットワーク駆動方式の改良、ネットワーク監視設備関係の効率の向上などシステム全体を改善すること。
- ② ボトルネックの解消、情報ネットワーク全体の信頼度の向上、セキュリティーの向上
- ③ ATM本体で単独稼働し、ローカル・スイッチング処理を行って、故障時でも、ネットワーク全体に影響を与えないこと。



第3図 ATMシステム図

- ④ ネットワーク全体のパフォーマンスの向上
- ⑤ 二重化電源の採用

などに留意し、実際に更新したシステムを第3図に示した。ATM本体は、Bay Network System 社の Lattis シリーズを Centillion シリーズに更新し、回線速度も155 Mb/S から 1 Gb/S と高速にした。また、監視装置もワークステーション2台から、使い易いノート型パソコンに変えて、監視による負荷の軽減をはかった。学内各棟の Ether Cell も更新して、パフォーマンスの向上に努めた。

新ATM装置に設備更新した後、現在まで情報ネットワーク上のトラブルはまったく発生していない。

### 2・3・2 ネットワーク・セキュリティ

大学のインフララインとなった情報ネットワークを安定に、効率よく運営して行くためには、そのハードウェア、ソフトウェアの管理だけでなく、情報ネットワーク・セキュリティの日頃の管理も重要である。基本的には、それに携わる者が日常業務の点検、分析、検討およびこれらの対策を充分に行うことである。少人数で運営している場合、これらの事項は、格別に難しい仕事になる。中小規模システムの場合、次の各点に注意して情報ネットワークを運用する必要がある。

- ① コンピュータ・ウィルス対策 大学の場合、(悪意が無く)無意識の内に混入するケースが多い。大半は既知のウィルスであるから、適切な対策を講ずれば、被害を最小限にすることが出来る。また、利用者には、適宜、注意を喚起することも大切であり、最近では、予算さえゆるせば、良いウィルス・チェッカー、ウィルス駆除のソフトウェアも市販されている。
- ② システム運営管理 情報ネットワーク・システムのセキュリティを確保する手段として、ファイヤー・ウォールを設置することは、比較的手軽でしかも有効である。しかし、この設定は詳細に行う必要がある。また、内部からの攻撃に対しては無効である。重要な箇所には二重にファイヤーウォールを設置する必要がある。

情報ネットワーク・システムのハード、ソフトともに、何時か、何処かで必ず故障が起きる。そのバックアップ体制は、常に取っておかないと、故障時に、利用者に迷惑を掛けることとなる。特に、デスク・クラッシュが起きた場合、復旧に時間が掛かるので、ファイルのバックアップは、必ず収集する必要がある。しかも、日、週、月など、こまめにバックアップを取っておかないと、システムが元に戻らない事になる。

その他、システムの管理と保守は、日々、正確に行う事が事故を未然に防ぐことになる。これらの諸点をマニュアル化して、常に誰でもが、対応できる体制にすることが大切である。あわせて、セキュリティ方針の策定〈セキュリティ・ポリシーの策定〉も重要な事項である。

③ 認証システム 大学の場合、認証システムとして、一般的に普及しているのは、ユーザー名とパスワードである。学生の場合、ユーザー名としては学籍番号を基本としたものを利用することが多い。そのため、認証としてのパスワードは、非常に重要であるにもかかわらず、その理解が十分に浸透していなく、初期設定のパスワードをそのまま使い続けたり、誕生日、電話番号など推測されやすいものをそのまま使っている例が多い。また、長期休暇時には、パスワードを忘れて、休み明け、または、締め切り日などにコンピュータが利用できなくなることもある。いずれの場合も教育でパスワードの意義、重要性を理解させることが大切である。最近、個人情報を取り扱うケースが増えて来て、(たとえば、就職活動など)、文書の暗号化や本人であることを認証するデジタル署名などの教育も必要となった。セキュリティーを確保する面では、好ましい傾向といえる。

⑤ 電源管理 情報ネットワーク運営上、盲点になっているのは電源関係である。トラブルの原因別に整理した第2表～第3表を見ると、電源関係のトラブルは結構ある。例えば、落雷、停電、瞬間停電、人為ミス(うっかり、電源を切断するケース)などがある。主要部に無停電電源装置(UPS)を設置すれば良いが、数が多くなり、全体では高額の出費になるので要注意である。また、電池も時々、交換する必要がある。15分以上の停電に対しては、システムを停止するほかない。この事を含めて、停電時の対処手続きをマニュアル化して、システム運用者に周知徹底をはかる必要がある。

以上の他、いま、情報ネットワーク上で何が起きているのかを知ることも大切で、常にネットワーク回線を監視し、制御ツールを利用するだけでなく、ネットワーク・セキュリティーを継続的に改善する必要がある。情報ネットワークを携わる者はネットワークに関する知識、その脆弱性に関する情報を取得し、常に、その対策を講じて行くことが重要である。

### 3. あとがき

文科系大学特有な問題として、全学的に情報ネットワーク、情報(処理)教育の意義、必要性が十分に理解されていなく、どうしても少ない予算(経費)で、しかも少人数で運営されている場合が多い。そのため、情報ネットワークに関する諸問題も多く、その解決には多くの時間がかかる。これを克服するには、関係者の地道な努力しかない。



## 参考文献

- (1) 今泉重夫、湊敏、横田浩：”文科系大学における情報システムの構築と運用”  
平成8年度情報処理教育研究集会講演論文集（文部省、名古屋工業大学  
主催） P142 （1996）。
- (2) 湊敏：”新システムの概要—平成9年度導入システム—”奈良大学情報処理  
センター年報 No.8 P1 （1997）。
- (3) 今泉重夫、湊敏、横田浩：”文科系大学における情報システムの構築と運用Ⅱ”  
平成9年度情報処理教育研究集会講演論文集（文部省、室蘭工業大学主  
催） P535 （1997）。
- (4) 今泉重夫、湊敏、横田浩：”文科系大学における情報システムの構築と運用Ⅲ”  
平成10年度情報処理教育研究集会講演論文集（文部省、九州工業大学主  
催） P130 （1998）。
- (5) 湊敏：”学内ネットワークのインターネットへの接続”第12回私情協大会資料  
P130 （1998）。
- (6) 原耕司：”奈良大学ネットワークシステムのMRTGを利用したトラフィック分  
析”奈良大学情報処理センター年報 No.9 P47 （1998）。