VLAN 機能による研究室単位の多様なセキュリティポリシーの実現

大塚秀治[1)], 久保美和子[1)],牧野晋[1)], 山戸田芳雄[2)],林英輔[1)]

[1)] 麗澤大学国際経済学部・麗澤大学情報システムセンター
[2)] 伊藤忠テクノサイエンス株式会社ネットワークソリューション推進第１部

概要

大学のような多様な研究機関の集合体では、情報セキュリティポリシーの実現が困難である。これは、一般的に研究者によって異なるニーズをもつためである。このような研究教育機関において、一定のセキュリティを実現するためには、構成員の最小単位である、研究者ごとのセキュリティニーズを実現する環境が必要となる。本報告では、すべての研究室に設置される複数の情報コンセントを VLAN で構成し、ルーティングモジュールにより、LAN 間の通信を行う。これにより、すべての VLAN にセキュリティルールを実装可能とした。また、研究室単位の LAN 内の Windows の共有フォルダを、隠蔽する対策を行った。セキュリティ対策として、研究室単位でトラフィック傾向を観察することにより、セキュリティを維持する運用を提案し、その実装結果の一部を報告した。

Implementation of Varying Laboratory Security Policies through the Use of VLAN Functions

Hideharu OHTSUKA[1)], Miwako KUBO[1)],Susumu MAKINO[1)], Yoshio Yamatoda[2)],Eisuke HAYASHI[1)]

1)The International School of Economics and Business Administration.Reitaku University
Reitaku University Information System Center
2)ITOCHU TECHNO-SCIENCE Corporation, Network Solution Assistance Center.

Abstract

Implementation of policies related to information security for an assortment of research facilities in an institution such as a university poses a real challenge. In general, the difficulty arises from the diverse needs of researchers. Achieving a certain level of security for such academic organizations requires an environment that facilitates satisfying the security needs of each researcher, since the individual researchers are the smallest elements of the organization.

In this report, we explain a system in which multiple information wall jacks were installed in each laboratory and connected through a virtual local area network (VLAN). Communication between LANs was implemented through Cisco Catalyst routing modules (RSM/MSFC). Such a design enabled the implementation of a set of security rules for each VLAN. In addition, as a security measure, shared Windows folders within each laboratory's LAN were hidden. An operation for maintaining security by monitoring the movement of each laboratory's traffic was also proposed. The results of implementing that measure are also reported.

1. はじめに

2000 年 1 月、主要官公庁のホームページがクラッカーにより改竄されるという事件以来、急速にセキュリティ問題がフォーカスされるようになってきた。この事件では当時の科学技術庁や総務庁統計局のサーバが含まれており、政府機関に大きな衝撃を与えた。このような状況下で、2000 年 7 月には、政府 IT 戦略本部に設置されている情報セキュリティ対策推進会議において「情報セキュリティポリシーに関するガイドライン」が策定され、2000 年度末までに全省庁でセキュリティポリシーの整備が求められた[1]。また、大学等においてもセキュリティポリシーの策定が急がれている[2]。しかしながら、大学のような研究機関においては、ネットワークの利用目的がさまざまであり、多様なニーズを満足させ、一定のセキュリティを維持するポリシーの策定は多くの利用者の合意形成を伴うため、非常に困難な作業となる。とりわけ、情報ネットワークを研究する利用者がいる場合、ファイアウォールの設置は運用の複雑さを増すことにつながる場合も多い。本研究では、多様なニーズを満たし、一定のセキュリティを確保するためのネットワークの構成事例を示し、運用状況について報告する。

2. 本学の情報ネットワークの変遷と現状

著者らの所属する麗澤大学[1]では、国際経済学部新設にともない 1991 年末に TokenRing を基幹とし、Ethernet を支線とするマルチプロトコルのキャンパス LAN を整備した。その後、逐次 Ethernet を増設し、Wellfleet[2]社製のマルチプロトコルに対応する高速ルータ BLN を基幹としたスター型のネットワークへ移行した[3]。これらの運用結果から、管理コストを下げるために、1）運用プロトコルを整理すること、2）スター型接続を採用すること、3）Ethernet を採用することを決め、1997 年にネットワークの再整備を行った。再整備では、UB Networks 社製の GeoLAN/500 を基幹としたネットワークが採用された。この製品は 1 筐体で 100/10Mbps の Ethernet スイッチポートを最大 168 個取り出すことが可能で、さらに VLAN 機能とトランク機能を持つ。また、ルーティングモジュールを導入することで、最大 40GBit のバックプレーンを用いて IP ルーティングが可能な製品である。この製品を 5 台用いて、キャパス内の主要な建物間をトランクした 2 系統の光ケーブルで接続し、小規模な建物については GeoRim と呼ばれるボックス型スイッチングハブで接続することとした。2 つある研究棟の各研究室については、各室 2 個の情報コンセントを配置した。スイッチングハブを用いることで、他の研究室間の通信をキャプチャすることを抑止するようにした。2 個の情報コンセントは、必要に応じて異なる VLAN に属すことが可能で、かつ設定変更を容易にするためパッチパネルを経由して、各情報コンセントへ接続された。教室内の全ての PC も、この方法で直接 GeoLAN/500 から接続する方式とし、教室内にはハブを設置しない方式を採用した。

しかし、施工段階で GeoLAN/500 用の 12 ポートスイッチモジュールの発熱問題で出荷が遅れたため、32 ポートの 10Mbps グループスイッチモジュールで代用せざるを得なかった。また、ルーティングモジュールも出荷が遅れ、筐体外にマルチポートの Cisco4500 ルータを設置して経路制御を行うという代替策をとった。さらに、この作業遅延のなかで UB Networks 社が ATM 交換機を主力とする NewBrige 社[3]に買収されたため、IP ルーティングモジュールの出荷自体が停止される事態となった。このため、全ての GeoLAN/500 をキャンセルし、その時点で出荷可能となっていた Cisco Catalyst5500 シリーズに全てを置き換え、ルーティングモジュール(RSM)

[1] 千葉県柏市。学生数約 3,000 人の小規模な大学。現在、情報システムセンターが管理する PC は約 600 台（Macintosh を含む）である。http://www.reitaku-u.ac.jp/

[2] Wellfleet 社は BayNetworks 社に買収され、BLN シリーズおよびその後継機種は BayNetworks 社によりサポートされている。

[3] 当初、Ethernet 製品が不足するカナダの大手ネットワーク機器メーカの NewBrige Networks 社が UB Networks 社の製品構成により自社製品の強化をはかるものと思われたが、翌年旧 UB 部門は業績不振のためリストラ対象となり、当該製品は扱われなくなった。更に、2000 年 2 月には会社自体がフランスの Alcatel 社に買収された。

を導入し、当初の計画通りの構成となった。しかし、PC の導入が終了しており、サブネットワークの構成の変更に工数を要することから、研究室の高速化とスイッチ化が行われたにとどまった。

その後、1998 年から 1999 年に国際産業情報学科増設に伴う、ネットワークの構成変更が行われ、キャンパス内のモバイル環境の整備、マルチメディアコンテンツ作成環境に伴う、一部の LAN のトランク数変更によるネットワーク速度の強化等が行われた。

2000 年に、1997 年に導入したネットワークの再構成が行われ、Catalyst6500 シリーズへの更新および、建物間の GigaBitEther 化が行われた。この際に、全ての研究室について、/28 のサブネット化が行われ教員数分のサブネットワークが増設（全154サブネット）された。教育系ネットワークでは、大学院棟の個人ブースを除く全てのポートが VLAN 対応のスイッチ化が行われた。

同時に、ウィルスメール対策、学生用メールクライアントの Web 化、NTP stratum 1 サーバの新設等、クライアントの多重ログオン抑止[4]などの構成変更が行われた。2001 年度からは IDS として RealSecure 社の ISS が導入された。

情報コンセントは VLAN により、情報コンセント系としてまとめられ、ファイアウォールにより隔離し、認証を受けなければ、外部との通信が行えないように変更された。また、VPN 装置を導入し、外部ISP経由などのインターネットから

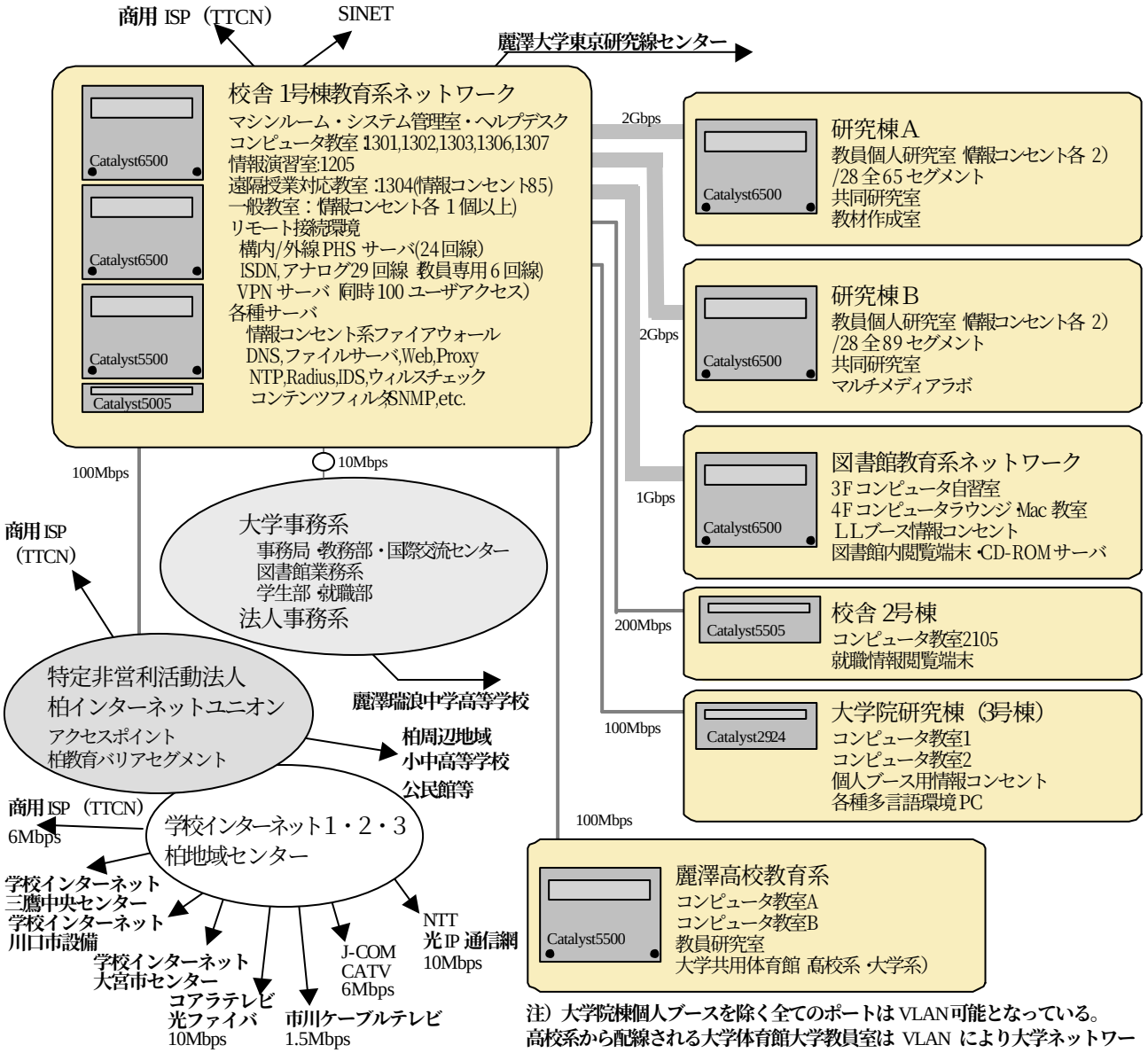


図１教育系ネットワーク概要図

注）大学院棟個人ブースを除く全てのポートは VLAN可能となっている。高校系から配線される大学体育館大学教員室は VLAN により大学ネットワークに所属する。

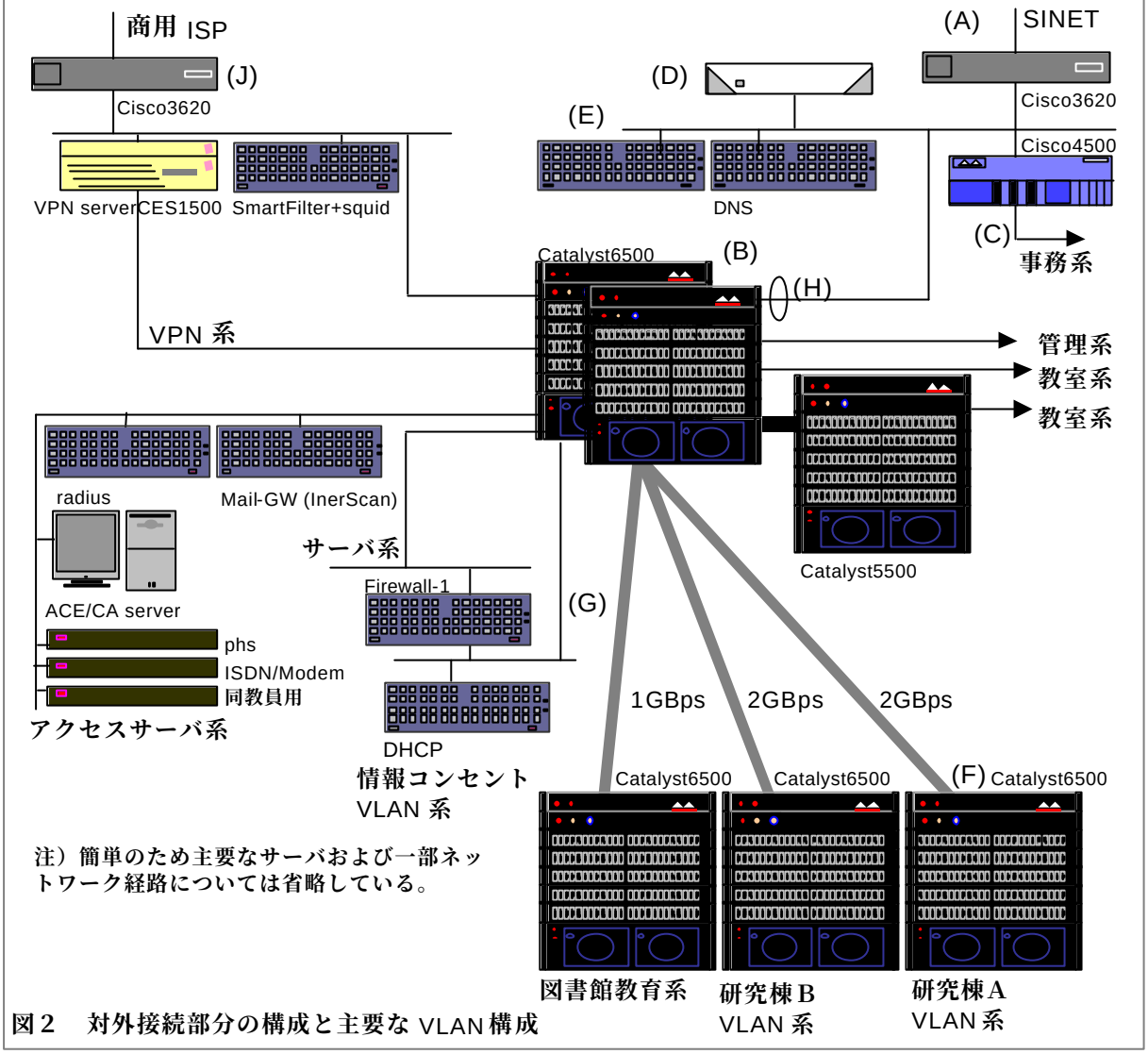


図２　対外接続部分の構成と主要な VLAN 構成

のアクセスを可能とした[4]。図１は、現在のネットワーク構成のうち、教育系について示したものである。各個人研究室に Winodws2000 または Mac が 1 台配布される[5]。

[4] FireWall-1 のセッション認証機能を採用した。このため、情報コンセントを使用する学生はユーザ登録を行う必要がある他、専用のクライアントを導入しなければならない。専用クライアントには Macintosh 用のものが無いため、情報コンセントを利用できる PC は Windows 系に限定される。これは VPN 装置についても同様で、Macintosh 用の VPN クライアントが無いため Macintosh ユーザは VPN を利用することはできない。

[5] 一部の教員については、複数台の PC またはワークステーションが配置される他、研究室には教員が個人的に持ち込む PC や研究費で整備される PC がある。教員がネットワークに機器を接続する場合には、機器接続申請を行わなければならない。しかし、/28 のアドレス空間が割り当てられているため、知識のあるユーザの場合には、申請しないで接続を行うケースも散見される。Windows の場合には管理サーバで検知可能となっている。

3.　セキュリティ環境

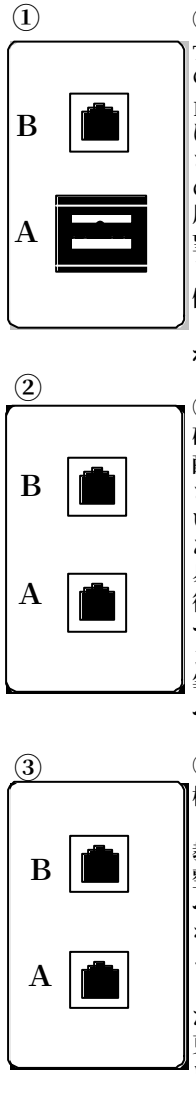
図２に対外接続部分と基幹部分の構成について示す。基本的に(A),(J)のルータでパケットフィルタリングが行われる。事務系のポリシーと教育系のポリシーの異なる部分については、(B),(C)でフィルタリングが行われる。(D)の部分で、このセグメント中のパケットがキャプチャされ、一定期間保存される。また、(E)の部分で IDS のセンサーの一つが稼動しており、攻撃を検知するとネットワーク管理者のコンソールに警告を表示する。事務系については独自のファイアウォールを(C)の下に持つ。

本学では、インターネット側からの telnet や FTP, POP 等は原則的に禁止されている。このた

め、商用プロバイダーからのアクセスは VPN 装置を介して行われることになる。認証は Radius を使って行われる。

情報コンセント系からのアクセスは、キャンパス内に散在する情報コンセントを 1 つの VLAN(G)に収容し、他の VLAN 間との通信を抑止する。DHCP で配布されるデフォルトの経路でのみ通信可能で、FireWall-1 を認証を受けて通過しなければならない。

研究室内で、Windows のファイル共有を行った場合には、ブロードキャストドメイン内に PC の所在を露見することになる。ファイル共有を行う場合、デフォルトではすべてのユーザが読み書き可能となっている。このため、セキュリティの変更を忘れると非常に危険な状態となる。



①1991 年～1996 年
TokenRing Type1 ケーブルにより A のデータコネクタを使って研究室内 PC との接続が行われた。TokenRing に接続できる PC は全て IBM 製に限定された。Ethernet の使用を希望するものは B のポートに UTP を接続して使用した。Mac で localtolk の使用を希望するものは、アタッチメントを利用して B ポートへ接続した。ノード装置側で、パッチパネルを利用して B ポート側へ配線を切り替える方法が採用された。

②1997 年～1999 年
研究室には A,B の Ethernet ポートが配布された。2 つの研究棟は/24 で運用されており、GeoLAN/500 が使われている間はパケットキャプチャが可能であり、パスワードやデータの盗聴は容易であった。1998 年に Catalyst 変更後はキャプチャは不能となったが、1 つの研究棟がブロードキャストドメインであったため、Windows の共有設定等で他の研究室のファイルやプリンタへ容易にアクセス可能であった。

③2000 年～
標準で A,B ポート共通の/28 セグメントに割り当てられる。一部の情報系の教員には 4 個以上の情報コンセントが整備され、それぞれ異なるセグメントへの VLAN へ接続を行う。例えば、A を教育系へ、B を実験系や KIU 系といったセグメントへ割り当てる。ブロードキャストドメインが研究室内になるため Windows2000 サーバの設定を変更することで、特定のホストしかブラウズできなくなる。

図 3 研究室情報コンセントの変遷

VLAN でブロードキャストドメインを研究室内に限定すると、通常はこのような状況とはならないが、Windows2000/NT のドメイン環境では、ブロードキャストドメインとかかわりなく、ドメインコントローラが一括して Windows ドメイン内の PC の所在をネットワーク内にアナウンスする。さらに Windows2000/NT の場合は所在が分かるだけではなく、各クライアントへのアクセスも可能である。このため、本学では研究室の WindowsNT/2000 クライアントについて、Windows ドメイン内のブラウズ一覧に表示させない設定を行った。一方、コンピュータ教室や自習室などは稼動状態の確認のため、この設定はおこなっていない。

このように、VLAN に依存した構成の場合 Catalyst のルーティングモジュール(MSFC)が故障すると通信不能となる範囲が大きい。このため、(B)の部分の異なる筐体に MSFC を冗長配置し、一方の MSFC がダウンした場合、他方がルーティングを代行する構成としている(H)。研究棟のセグメント分割は研究棟側に配置される Catalyst によって行われる。2 つの研究棟に合計 154 セグメント追加定義し、それぞれの MSFC に VLAN インターフェースを定義し、このインターフェースを使ってルーティングを行う。従って、各研究室毎に定義されるインターフェースの in バウンド、out バウンドのそれぞれアクセスリストを定義することが可能となる。上述のブラウズ問題もアクセスリストで制限することも可能となる。

4. セキュリティポリシーの検討と適用

本学のキャンパスワイドなネットワーク管理と計画は大学の情報システムセンターが担当するが、図書館、事務系、高校や学校法人事務系にネットワーク運用部門がある。このため、セキュリティ上の脅威に対しては円滑に対応が可能となっている。情報システムの利用規則や利用ガイドラインは整備されているが、明文化された情報セキュリティポリシーの作成は今後の課題となっている。この合意形成の過程で、教員が希望する利便性とセキュリティ上の脅威とのトレード

オフの調整に困難が予想される。また、情報系学科を持つため、アプリケーションゲートウェイによるファイアウォールの導入に抵抗が大きい。

本方式では、研究室単位でアクセスリストを設定することが可能であるため、教員の管理能力に応じて、外部へのアクセス制限を段階的に設定することが可能となる。今後、この基盤に基づいて情報セキュリティガイドラインの構築行う予定である。図 3 に 1991 年から現在に至るまでの研究室内の情報コンセントの機能についてまとめて示した。

5. ネットワーク分割の効果と諸問題

研究室単位にネットワークを分割すると、研究室単位のトラフィック量を測定可能となる。ルータのトラフィック量を継続的に測定できる MRTG はセキュリティ監視のツールとしても有用である。しかし、ルータ上（MFSC）のネットワークインターフェースは仮想インターフェースであり、そのアドレスから SNMP でトラフィックを測定することはできない。Catalyst 内でのルーティングは Cisco Express Forwarding によりスイッチされる。この機能を抑止するとスイッチの性能が大きく低下する。このため、全てのポート単位で MRTG を用いてトラフィックデータを採取することとした。しかし、ポート側で測定を行う場合、通常のトラフィックの in/out の記録が逆転する。また、各研究室でのトラフィックを表示するには、設置されている 2 つのポートを合算処理する必要がある。このため、in/out の逆転と合算を行うスクリプトを平行して動作させることで、研究室ごとのトラフィック監視を可能とした。図 4 に測定例を示す。

本方式では、アクセスリストを MFSC に記述可能である。しかし CiscoIOS の場合、拡張 IP アクセスリストは 100 から 199 番までしか設定できない。このため、約 150 の研究室 VLAN 毎に異なる in/out のアクセスリストを定義することは、不可能である。従って、アクセスリストは共用化できるよう工夫する必要がある。また、アクセスリストを各インターフェースに付けることにより、パフォーマンスの低下が予想される。このため、in バンウンドに 10 行、out バウンドに 20 行のアクセスリストを記述し、アクセスリストの有無の比較を netperf を使って行った。前述の通り、Cisco Express Forwarding 機能により、ルーティングが行われるため、通常の利用では転送速度の劣化はまったく認められなかった。これは一旦、ルールを通過した接続は継続するパケットでチェックを受けないためで、netperf のテストでは妥当な結果と言える。従って、さらに詳細な分析が必要である。

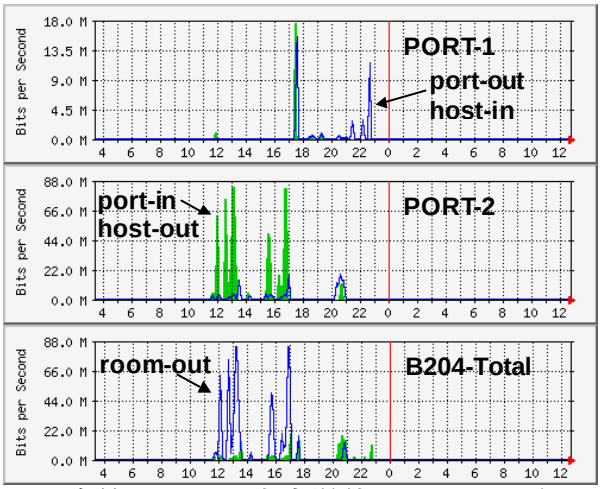


図 4 合算による研究室単位の MRTG 記録

6. まとめ

本方式では、シャーシ型高速スイッチングハブを用いて、スター型に配線し VLAN 機能により研究室単位で独立したネットワークとして構成した。この方法により、多様なセキュリティを実装することが可能となった。

参考文献

[1] 総務省・情報通信に係わるセキュリティ保護に関する検討会,「情報通信利用に係わるセキュリティ保護に関する検討会報告書」,2000 年,12 月.
http://www.joho.soumu.go.jp/policyreports/japanese/group/tsusin/Pdf/001205d55101.pdf
[2]大塚秀治,大学におけるネットワークセキュリティ,平成 13 年度「教育の情報化フォーラム」,私立大学情報教育協会,2001 年,6 月.
[3]大塚秀治,マルチプロトコルネットワーク環境における教育システムの運用と問題点,情報処理学会分散システム運用技術グループ資料,DSM-9505036,1995 年,5 月.
[4]久保美和子,大塚秀治,牧野晋,林英輔,システム利用マナー教育のためのアクセス管理,情報処理学会分散システム/インターネット運用技術研究会,2001-DSM-22,2001 年 7 月,pp.63-68.