# 高速キャンパス情報ネットワークシステムの導入について
## －現状の問題点と新システムの設計－

建設・機械系（情報メディア教育センター）　高木　稔

## 1　はじめに

本学に LAN（以下「MITnet」という。）が導入されて７年が過ぎようとしている。当初高速と思われた FDDI バックボーン（100Mbps）も、今ではパソコン自身が 100Base-TX で接続できる環境になってきている。昨年暮れ、これまで要求していた MITnet の更新が今年度（2000 年）補正予算で高速キャンパス情報ネットワークシステム（以下「新 MITnet」という。）として実現する運びとなり、本年９月１日には稼動する予定となった。

本報告は、MITnet の現状と問題点を明らかにし、新 MITnet が何を目指しているかについて報告する。

## 2　MITnet の現状と問題点

MITnet は FDDI（100Mbps×3 ループ）を幹線とするネットワークに、学科内を巡る 10Base-5（10Mbps×3 ライン）を支線として接続した形態でスタートした。現在の構成を図１に示す。MITnet は本学最初の LAN として、必要な補強・改良を繰り返しながら、教育研究の高度化、情報化、国際化並びに事務処理の合理化及び効率化に寄与してきた。

しかし、情報通信分野での急速な発展と普及は、現状の MITnet では対応しきれない問題点を抱えるようになった。以下、主な問題点を考察する。

### 2.1　セキュリティ問題

昨今、インターネットを通じて組織内 LAN への攻撃は日常茶飯に行われており、昨年（2000 年）１月の政府機関のホームページ改竄が大きく話題となったが、その２月には本センターの教育システムに対するクラッキング攻撃被害が明らかとなり、全ユーザ ID のパスワード変更を余儀なくされた。同じく他学科内サーバのクラッキング、メールサーバの脆弱性を突いた攻撃などがこの年末を挟んで急増しており、インターネットの普及が多くの違法なクラッキング行為をも増長させつつある（図２参照）。また、パソコンのウィルス汚染もますます拡大し、大きな社会問題として捉えられつつある。現在の MITnet の抱える第一の問題は、こうした攻撃や弱点からファイアウォールなど学内のネットワーク環境を守る手段を何１つ用意していないということである。

もちろん、個々のサーバに対し、その管理者が必要な防御手段を講ずべきことは言うまでもないが、組織のネットワークを守るという観点から考えるとき、「ネットワーク・セキュリティ」という概念がごく当然のこととなってきた。

### 2.2 利用管理問題

MITnet へ接続するには申請が必要である。しかし、現状では、申請なしに勝手に接続することも可能である。このことが、IP アドレスの二重割当によるネットワークの混乱を引き起こす場合がある。また、SINET を通じた学外との通信スピード（当初64Kbps）が遅く、6Mbps（2000 年 2 月）になる以前には、たった 1 台の負荷の高い通信が他の接続を停止していると思わせるほど遅延させることが頻発した。この場合、原因となったコンピュータが分かればすぐに対処もできるが、未申請のものであると、混雑解消は困難となる。また、図書館など学内には利用者が特定できない利用を前提としたパソコンがあり、不正なメールの発信等が問題になった場合もあった。こうしたネットワークを「誰が」使ったか特定できない現状は、そろそろ見直す必要があるのではないだろうか。

### 2.3 通信速度問題

問題というより、当たり前のことではあるが MITnet の提供する通信スピードが遅く時代に対応できなくなってきている。MITnet へのコンピュータの接続数は約 350 台から約 2300 台と劇的に増加した。これにより、学科によっては 10Mbps の支線に 100 台を超えるコンピュータが接続され、支線自体がコリジョン過多になって接続困難をもたらすこととなった。また、パソコンの高性能低価格化とマルチメディア技術の急速な発展は、通信される情報の質を変え、情報量そのものを大きくした。現状のスピードでは最早対応はできない。

### 2.4 サービス問題

これは前項の問題とも関係するが、MITnet の有効利用を図るためのサービスの問題である。MITnet は先にも延べたが、単にインターネットへの接続を目的に設計されたものではなく、これを学内の文書処理や情報利用にも有効に生かすよう設計された。具体的には、学内文書システムとしての MR メールシステムであり、学生向け電子掲示板としての情報表示装置であった。これらは、学内の情報化を図る上で当時の制約（MS-DOS も対象にした等）を受けながらも学内情報化にとって貴重な役目を果たしたが、ほとんどが文字中心の内容にならざるを得なかった。MR メール自身は 2000 年 1 月より、Web サービスを利用した業務文書配布システム（VWS）に置換えたが、今後はインターネット上を含めて高品位な画像、音声、映像を含むマルチメディア通信が主役となる。もちろん、これには学外との通信スピードの向上を抜きには無理であるが、

少なくとも学内においてこれを前提としたサービスのあり方を検討しなければならない。同じく、情報表示装置に変えて学生への情報発信の質的な向上も目指す必要がある。また、すでに当初からのEメール、WWW、ニュース、FTPの各サービスもより充実する必要がある。

## 3　新MITnetの概要

次に、前節で述べた現状の問題点が新MITnetでどのように改善されようとしているのか、その仕様書に沿って報告する。新MITnetの構成を図3及び図4に示す。

### 3.1　ネットワークの構成

新MITnetは、学内の主要施設3ヵ所（専門棟、図書館、情報メディア教育センター）にバックボーンスイッチを分散配置し、8Gbps以上の伝送路を有する高速幹線ネットワークを構築する。また、各施設にスイッチを分散配置し、幹線ネットワークと1Gbps以上の伝送路を有する支線ネットワークを構築する。さらに、支線ネットワークのスイッチから各室内まで100Mbpsで接続するためのネットワークケーブルが敷設される。これにより、研究室にコンピュータが1台のみの場合は、100Mbpsの接続が可能になる。研究室内に複数のコンピュータがあればハブにより複数のコンピュータを接続することもできる。この高速化は3.3に述べる映像配信システムを利用する上で十分な速さと品質が得られるよう考慮されたものである。

上記のスイッチは、IPアドレスなどによるフィルタリング機能や、帯域制御機能を持っており、ネットワーク監視装置の導入と併せて未申請な接続への利用制限や、場合によっては負荷の高い利用に対する帯域制限を行うことも可能である。また、これまでグループ支線については専用線を引き、ルータを介して学科支線に接続する形態をとっていたが、スイッチがVLAN機能を持っており、原則として物理的位置関係を考慮することなくグループ支線を構築することが可能である。

セキュリティの関係では、ファイアウォールを導入し、学外、DMZ、及び学内のネットワークを区分し、学外からの不正アクセスに水際で対応する。このDMZ（DeMilitarized Zone）には学外向けの通信サービスを専門とするサーバが置かれる。また、ウィルスの侵入を防ぐためのウィルス対策サーバの導入、及びDMZ内のサーバを監視するためのセキュアシステムも導入される。もちろん、これで全ての不正アクセスなどがなくなり接続されたコンピュータが安全になるわけではない。個々のコンピュータに対する防御はやはり個々に必要であることは言うまでもない。

### 3.2　ネットワークサーバ

DNS，メール，ニュース，WWW，proxy，ftp等のネットワーク基本サービスを行

うサーバを強化し、充実を図る。メールサーバはPOPとIMAPをサポートし、ネットワークディスクアレイと連携して、メールをサーバ上に保存できるようにする。WWWサーバはメインサーバの他に部局用のサーバを用意し、設置・管理上の学科の負担を軽減する。

### 3.3 映像配信システム

既設の衛星受信設備やビデオ撮影設備等による受信映像又は撮影映像をリアルタイムにエンコードし、新MITnetを通して学内へライブ同報配信する。これにより、研究室などに居ながら講演会などの内容をテレビ中継のようにネットワークを経由して視聴することが可能になる。また、撮った映像などをネットワークディスクアレイに蓄積し、好きなときにオンデマンドによるビデオ視聴を行うことができる。

### 3.4 キャンパスインフォーメーションシステム

これまでの情報表示装置に代わり、学生の呼び出し、授業異動、お知らせ等のキャンパス情報を掲示する情報掲示システムを設置する。これらのお知らせは、インターネットを介して自宅のパソコンや携帯電話で見ることも可能である。

また、教室の利用予約状況を閲覧し、学期途中の教室利用について予約や取り消しのできる教室管理システムを導入する。

## 4 おわりに

新MITnetは、セキュリティと速さにこだわって構成された。ただし、それゆえ未体験の装置・システムが多いが、果たして狙い通りに行くのかその効果に注目したい。また、紙面の都合で紹介しきれなかったが、新MITnetでは、接続確保を重視した機器の安全面も前回と比較にならないほど網羅されている。例えばファイアウォールの二重化や、幹線スイッチの電源の二重化などである。

今回市場を調査する中でつくづく感じたのは、セキュリティには莫大とも言える予算が必要となるということである。しかもこれは年間保守料であるから年度ごとに負担が掛かる。7年前には想定していなかった負担である。考えてみれば不正アクセスのような犯罪はやる方が悪いに決まっているが、摘発が難しいせいかやる方よりやられる方が非難される理不尽な世界だ。それだけに本当に有意義な利用が望まれるし、学生教育においても啓蒙教育の充実が切に望まれるところである。

## 謝辞

本稿を執筆にあたり、本センターの石田純一教官、石坂徹教官および技術室の諸氏

より貴重なアドバイスをいただいた。心から感謝申し上げる。

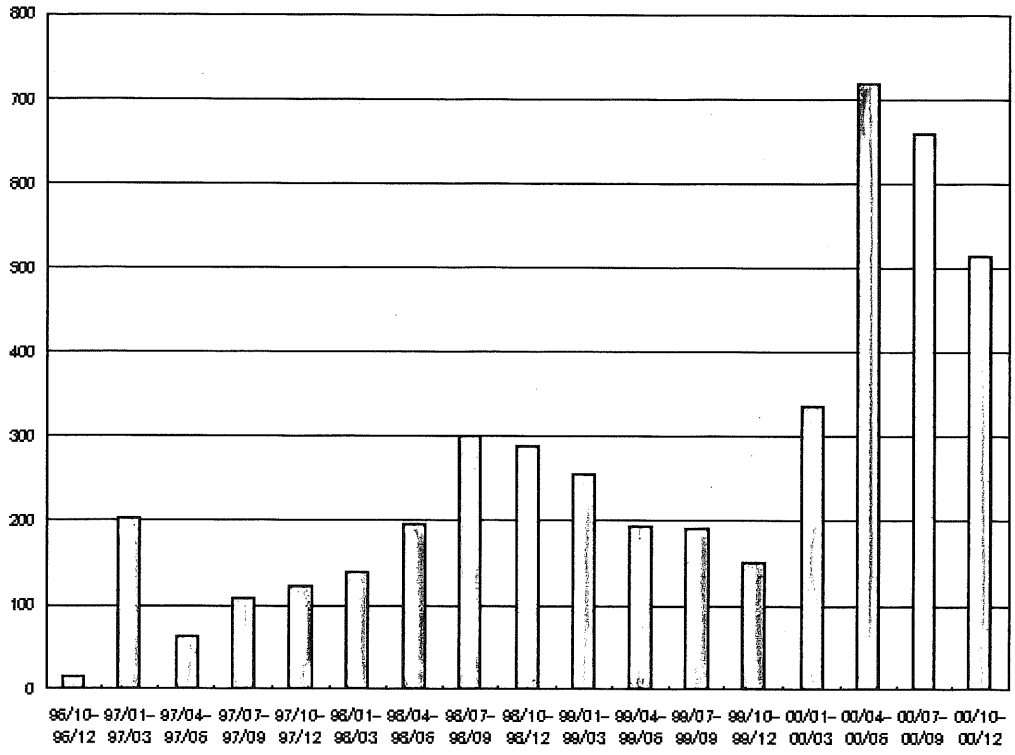


**図 2　インシデント報告件数の推移**

注: ここにあげた件数は、インシデント報告を JPCERT/CC が受理した件数であり、不正アクセスやアタック等に関して実際の発生件数や被害件数を直接類推できるような数値ではありません。

（※JPCERT/CC ホームページより承認を受けて転載）

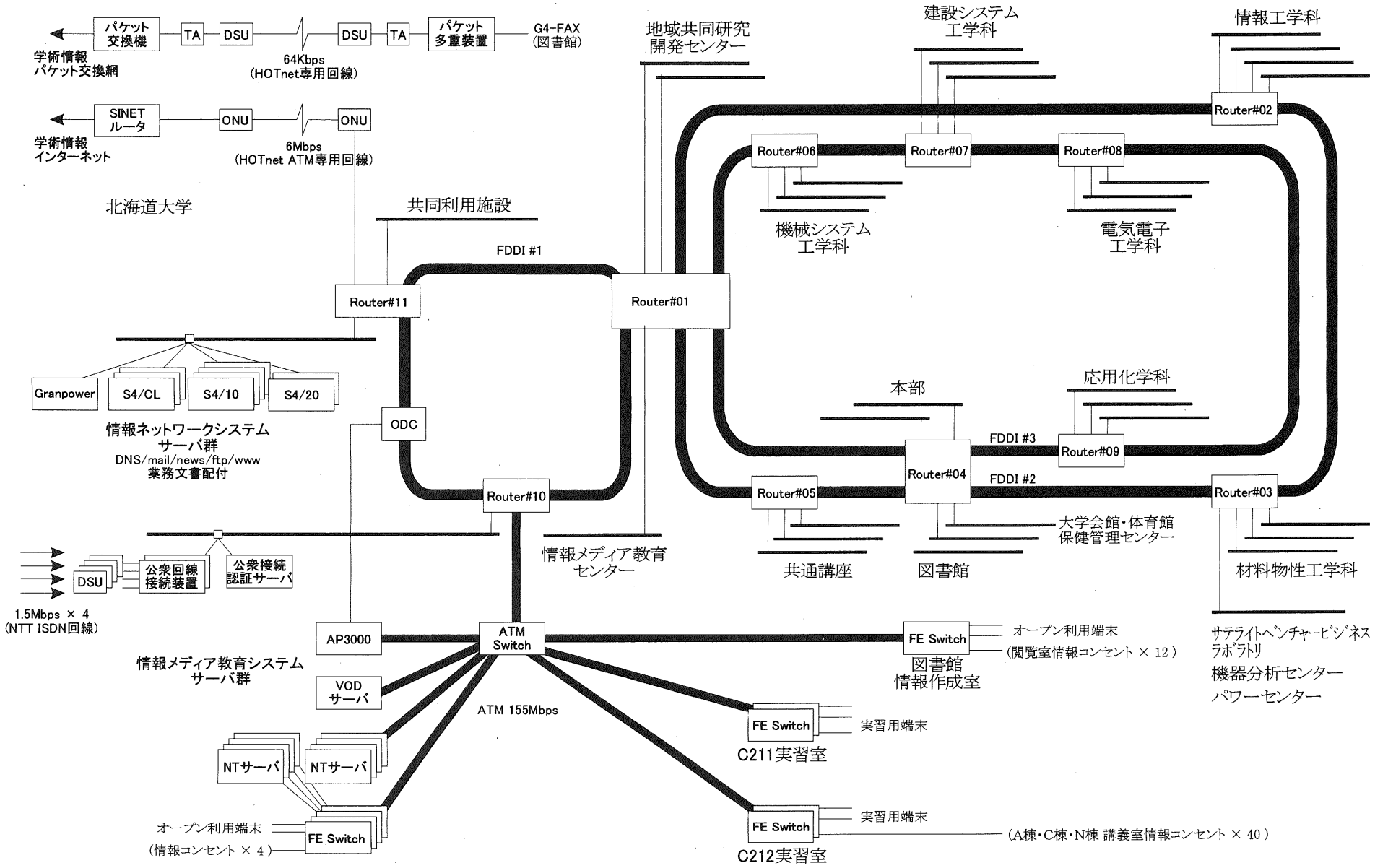


図1　現在のMITnet 構成図

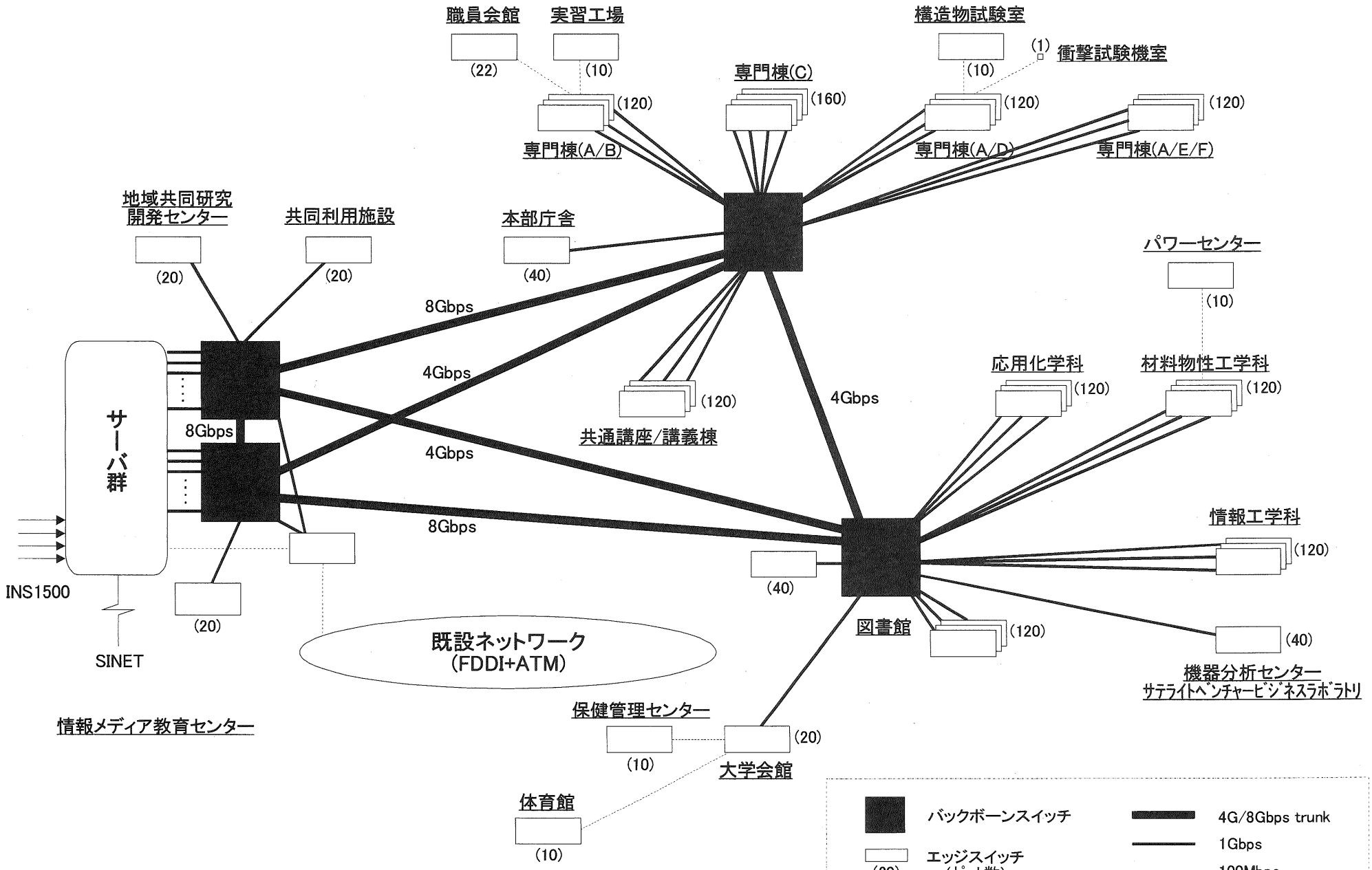


図3　新MITnet構成図

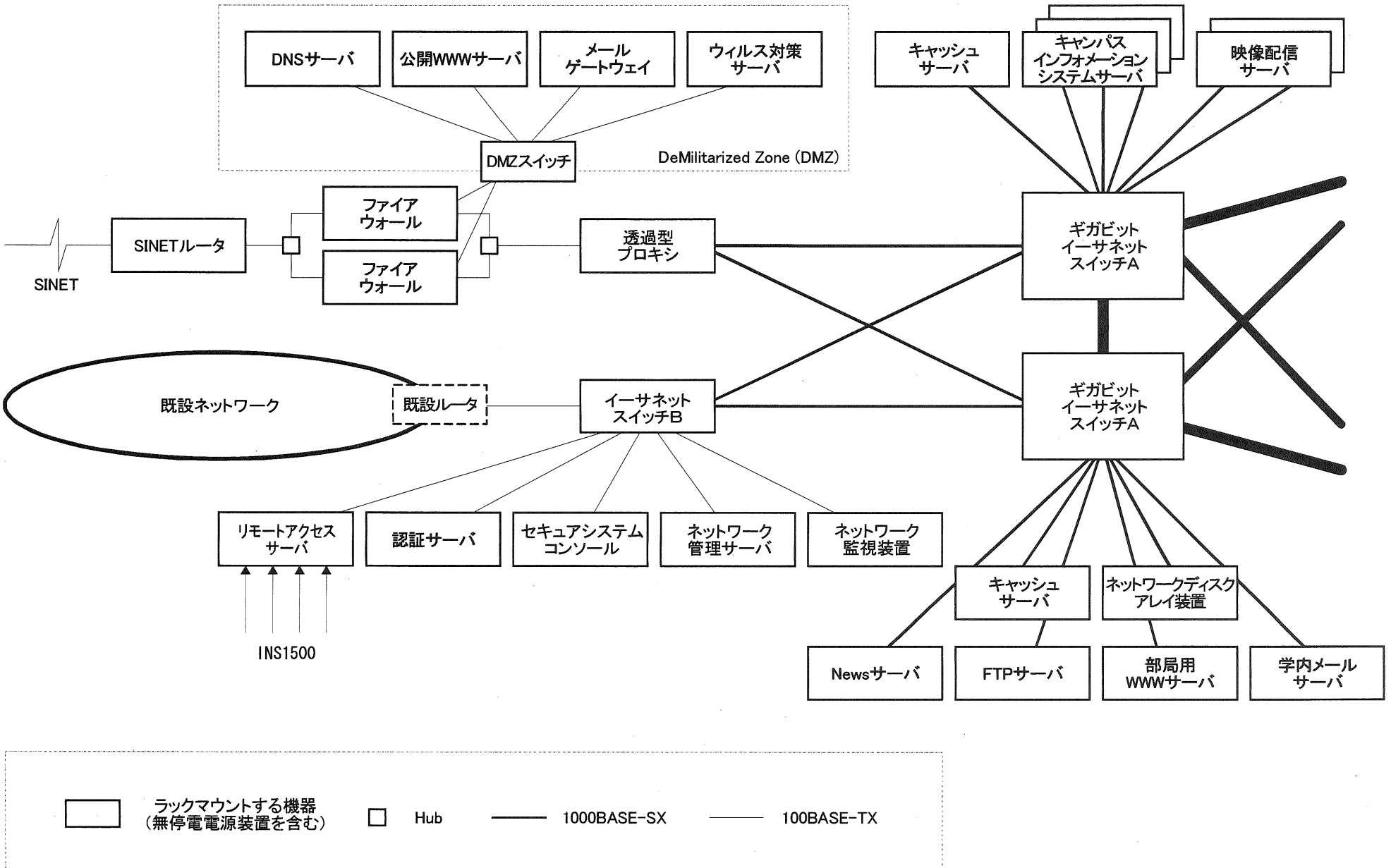


図4　新MITnetサーバ構成図