

学校内ネットワークにおける多機能ゲートウェイサーバの実現

牧野晋[†] 大塚秀治[†] 松本彰夫[†] 久保美和子[†] 林英輔[†]

[†]麗澤大学国際経済学部 [†]麗澤大学情報システムセンター

概要

教育の情報化を推進する流れの中で、各地で学校 LAN の構築と運用が進められている。校内 LAN の構築は、自治体行政の教育設備計画によって進められている他に、校内の教員の手による配線作業やボランティアによる、所謂、ネットデイ活動によっても進められている。その場合に必要となるのが可能な限り周到に考慮されたネットワーク設計である。柏インターネットユニオン (KIU) ではその活動の中で、学校教育用ネットワークの構築と運用を支援してきたが、ネットワーク設計において教室系と職員室系のネットワークを互いに独立なサブネットとして構成する重要性に注目し、これを実現するための経済性が高く、多機能なゲートウェイサーバのプロトタイプを開発した。現在、その運用経験からシステムに改良を加え、運用の更なる安定性を目指している。本報告では、当該ゲートウェイサーバの機能と運用データについて論じた。

Multi-function Gateway Server for School Education Network

Susumu MAKINO, Hideharu OHTSUKA, Akio MATSUMOTO,
Miwako KUBO and Eisuke HAYASHI

Reitaku University

Abstract

In the activity that promotes educational computerization, construction and management of school network are advanced in every place. Construction of the network in a school is advanced by the educational equipment plan of a local government and administration, by the teacher, by the volunteer on the NetDay activity and so on. However, when building a school network, the network design fully taken into consideration is required. Kashiwa Internet Union (KIU) has supported construction and management of the network for school education. In the network design, it is important to divide mutually the network for student and teacher as an independent sub network. In order to realize this, the prototype system of a multi-function gateway server was developed. In this paper, we describes the design, function and implementation of this gateway server. We also discuss about the management data of this server on the school education network environment in Kashiwa area.

1. はじめに

柏インターネットユニオン (KIU) では、柏市との協力関係のもと、1997 年より学校用ネ

ットワークの構築と運用を支援してきた。この活動を通して、我々は、学校ネットワークの構築と運用に関する実証実験に取り組み、教育用ネットワークの現状分析とそのあり方につい

て検討してきた。

柏地区は、平成 10 年度からの学校インターネット高度化モデル地域事業¹の地区センターに指定され、CATV をアクセス網として使い市内 20 校が接続されている[1]。また、平成 11 年度からの学校インターネット²プロジェクトでもサブセンター指定を受け 2 校が同様の形態で接続された。並行して、自治体の整備計画に基づきシステムの導入が進められ、今年度中に市内の公立学校 50 校すべての接続を完了する予定となっている。当初、ISDN を利用した間欠 LAN 間接続が多かったが、現在では、ほとんどの学校が専用線、CATV などの常時接続へ移行しつつある。

「教育の情報化」推進の流れの中で、学校でのコンピュータやインターネットの活用は実運用段階へと徐々に移行している。各地で学校 LAN の構築と運用が進められている[2]が、校内 LAN の構築は、自治体行政の教育設備計画によるもの、校内の教職員や生徒らの手でケーブル敷設作業を行い構築・拡張されたもの、ボランティアによる所謂ネットデイ活動によって進められたものなど、その形態はさまざまである。多くはない予算規模の中でインターネットの教育利用を考えると、まず考慮されるのはインターネットへの接続性そのものである。各種の実験プロジェクトでも整備されるのは外部への接続点までであることが多い。校内 LAN の構築については各自自治体や学校等にまかされるケースがほとんどである。このような場合、構築された校内ネットワークに十分なセキュリティが確保されないこともあり問題となる。

筆者らは、ISDN 間欠接続時における問題を中心に議論した報告[3]の中で、校内にキャッシュサーバを置く必要性、複数サブネットに分割する校内 LAN の構築方式等についても触れた。本論では、これを実現するためのプロトコ

ルとして構築したゲートウェイサーバの機能について概要した。PC-UNIX を用いた学校サーバの構築事例はある[4]が、運用に関する定量的データに関する報告は少ない。この点について、本報告ではさらに、運用を通して得られた知識についても報告する。

2. 学校内 LAN の現状

柏地区では、自治体の整備計画に基づき校内 LAN の設置が進んでいるが、それでもすべての教室に情報コンセントが設置される状況にはない。全国的にも校内 LAN は未整備である場合が多い。文部省資料[5]でも、2004 年度末までに全教室まで校内 LAN が整備される予定なのは、全国の公立小中高等学校等約 4 万校のうち約 20%の大規模校（約 8,000 校）のみであり、これ以外の小中規模校における教室接続については、ボランティア等の手により各学校独自に校内コンピュータの相互接続を行うことが想定されている。

このような状況下、現状では、仮に校内 LAN があつたとしても、コンピュータ教室に構築された LAN がつぎはぎ的に拡張され、教室や職員室、教材準備室などまで延長されるという形態が多い。すなわち、LAN のトポロジーにかかわらず、校内が一つのサブネットとして構成されているケースである。この状態は以下のような問題点を持つ。

学校ではいわゆる「学校サーバ」として Windows 系のサーバが使用されている場合が多い。このサーバは、主にファイルサーバ、プリンターサーバなどに使用されている。Windows 系のネットワークを構築する場合、ワークグループ名を独自に設定したり、ユーザ認証に関する項目を正しく設定せねばならない。これらをきちんと管理・運用するには、ネットワーク管理に関する基礎知識を持つ管理者が必要になるが、必ずしもそういった人材が校内にいるとは限らない。また、NetBIOS を使った Windows の「共有」機能を用いてファイル共有などが行われている場合もあるが、不用意な共有を行うことで、教師用 PC 上に作成された成績データ等の重要な個人データを生徒用 PC から参照できてしまうということも起こり得る。

¹ プロジェクト正式名称は、「先進的教育用ネットワークモデル地域事業」。柏地区では「のぞみプロジェクト」と称する。

² プロジェクト正式名称は、「マルチメディア活用学校間連携推進事業」。柏地区では「やまびこプロジェクト」と称する。

3. 校内 LAN に必要な構成

こうした問題に対応するためには、校内 LAN の構築に対して可能な限り周到に考慮されたネットワーク設計が必要となる。KIU では、ネットワークの設計において教室系（生徒用）のネットワークと職員室系（教員用）のネットワークを互いに独立なサブネットとして構成する重要性に注目した。現在の柏市内の学校で構築されている校内 LAN の概要を図 1 に示す。このようにしてネットワークをセグメント分割しても、Windows 上に lmhosts ファイルを記述すればルータを越えての共有は可能³であり、完全なセキュリティが実現されているわけではないが、教員が安易に設定したファイル共有によって「教室で生徒が Windows のネットワークコンピュータを開き、そこに表れたアイコンをクリックしたら成績データが見えた」というような事故は未然に防げる。

設計では、対外ルータと同一セグメントには教室系を置き、別のルータを介して職員室系を配置した。IP アドレスは、KIU からアドレス付与する学校については原則として 1/4C のグローバルアドレスを付与し、これを校内で 2 分割して使用した。各 PC にはグローバルアドレスを付与しているが、これは教育用に使用されるストリーミング系アプリケーションへの配慮⁴である。前述のモデル地区事業に該当する学校では、プロジェクトにより付与されたプライベートアドレス（各校 2C ずつ）を使用している。プロジェクトは、全対象校と地区センターを包含する巨大なイントラネット形態と

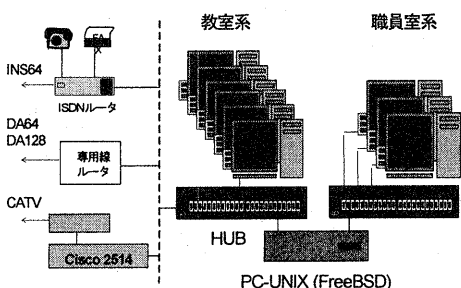


図 1 柏市学校のネットワーク概念図

なっており、地区センターに設置された FireWall によりアドレス変換されてインターネットと接続される。

4. 多機能ゲートウェイサーバの構築 1 (プロトタイプ 1)

校内ネットワークを分割するにはローカルルータが必要になるが、構築当初、安価なローカルルータを入手することは困難であった。例えば、Cisco 社の 1600 シリーズなどでも IOS を含めて高性能な PC 以上の価格となり、学校単位でこれを購入するのは難しい状況がある。また、学校インターネットプロジェクトにおいても、複数のイーサネットインターフェースを持つルータは整備されなかった。

KIU では、ISDN 間欠 LAN 間接続が行われていたネットワークの構築初期からキャッシュサーバの必要性を示唆していた。低速な回線を使用した場合の Web を使った一斉授業への対応や、従量料金の ISDN での通信コスト削減のためにもキャッシュサーバは必須である[3]。1.5Mbps の上位回線を持つプロジェクト校では、当初、キャッシュサーバは不要との考えもあったが、授業環境のように、同一コンテンツへのアクセス頻度が高い場合には、運用上有効性が高いことが示されている。同時に、間欠接続時における予期しない発呼を避けるために、校内に Primary DNS サーバを置くという方法を採用したので、学校には FreeBSD を実装した PC-UNIX を配置していた。さらに、異常発呼等が発生した場合には、校内ネットワークの状態を監視する必要がある、

- 遠隔から操作できるシステムが学校内にあること。
- tcpdump 等のパケット監視ツールが実装されていること。

などは障害の原因特定に不可欠であった。すなわち、PC-UNIX は、一種のネットワーク監視装置としても利用されていたことになる。

プロトタイプ 1 では、この PC-UNIX にインターフェースカードを増設したモデルを学校数分用意し、校内 LAN を分割するローカルル

³ NetBIOS を TCP/IP にバインドする。

⁴ CU-SeeME や NetMeeting など。NAT や Proxy ではうまく動作しないことがある。

ータとして使用することとした。

プロトタイプ1は、以下の機能を有する。

- 1) IP ルータ
- 2) キャッシュサーバ (squid)
- 3) ネームサーバ (bind8)
- 4) メールサーバ (sendmail、qpopper)
- 5) ユーザ登録用ツール (独自開発)
- 6) アクセス制御・ネットワーク監視 (tcp-wrapper、tcpdump、syslog 等)

このうち、4)については、独自に校内メールサーバを運用したい場合のオプションとなっている。5)は、4)を運用するにあたり、Excelで作成された CSV データから一括して ID 登録・削除を行うものである。

学校インターネットプロジェクトの実施と並行して、小学校では年次計画によってコンピュータの入れ替えが行われていたので、これに合わせ PC-UNIX 用の H/W は柏市が調達した。一方、中学校については新規の H/W の用意ができなかったが、リース切れの PC などを転用するなどの処置を行った。別途、NE2000 互換の ISA タイプの NIC を必要枚数新規購入した。これには構築時等の作業性を考慮⁵して、IRQ や I/O Port アドレスをジャンパーピンで設定できるものを採用した。NIC は当時の価格で千数百円/枚程度であった。

構築した PC-UNIX ルータの転送能力について図2に示す。ここでは、他のサーバ機能は動作させていない。他のシステムを接続しない単純な LAN 環境で一定サイズのファイルを30回ずつ ftp した時の平均転送速度である。

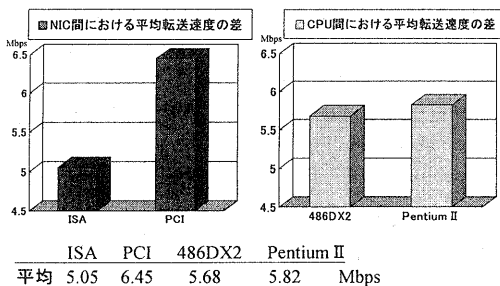


図2 PC-UNIX の転送能力

⁵ EPROM に焼き付けるタイプでも問題はないが、DOS から専用ツールを起動する必要があり、設定に時間がかかる。

NIC の違い (左図) では、CPU が Pentium II の場合、CPU の違い (右図) では NIC を ISA バスの場合で比較している。CPU の能力よりもむしろ NIC が ISA か PCI かというバスの違いが大きく影響していることが見てとれる。Windows を使用できなくなった CPU : i486 (100MHz)、メモリー : 16~24MB、HDD : 500MB 程度の PC でも 5Mbps 程度の IP forwarding 能力を有し、他のサーバ機能を搭載しても充分実用可能である。

20 台以上のシステムを一時期に構築するのは大変で、作業を分担するための導入手引き書の作成、現場に設置するにあたって個別情報を設定するための設置手引き書の作成などまで含めると、作業コストはそれなりにかかるが、全体として経済性の高いシステムを構築できた。

5. プロトタイプ1の運用と問題

プロトタイプ1の設置は、学校インターネットプロジェクトの実施とほぼ同時期、1999/10~11 頃からである。約1年間の運用を通じて得られたデータと生じた問題点についてまとめた。

当初は、障害が発生した場合、学校から柏市立教育研究所へ電話連絡→KIU NOC へ電子メール等で連絡といった手段を用いていたが、今年1月ら Watch-dog システムを導入して PC-UNIX 等の監視を行っている。これは、

```
Date: Fri, 30 Jun 2000 09:29:59 +0900 (JST)
From: Super-User <root@pluto.kiu.ad.jp>
To: net-admin@kiu.ad.jp
Subject: [KIU ALERT] HOST==dai4-e+dai4-e+dai4-e

CHECK START: Fri Jun 30 09:10:00 JST 2000 Check ON pluto

Domain dai1-e TEL:73-0000          -> 発生場所
09:13:19 Cisco2514-OUT 10.108.51.24 STATUS=1  -> ルータ非疎通

Domain dai4-e TEL:73-0001
09:13:19 Cisco2514-OUT 10.108.49.24 STATUS=0  -> ルータ疎通
09:16:37 Unix host 10.108.66.2 Port Num 21 STATUS=1  -> UNIX 非疎通
09:19:55 Unix host 10.108.66.2 Port Num 23 STATUS=1  -> UNIX 非疎通
.....

Domain dai5-e TEL:73-0021          -> 正常
09:19:55 Cisco2514-OUT 10.108.50.16 STATUS=0
09:19:55 Unix host 10.108.68.2 Port Num 21 STATUS=0
09:19:55 Unix host 10.108.68.2 Port Num 23 STATUS=0

PORT -----
21:FTP 23:telnet 25:SMTP 70:Gopher 80:HTTP
106:POPpasswd 110:POP 119:NNTP
8080:Squid
-----
KIU Watch-Dog ver2.00 (C) KIU Tech 1999.
```

図3 Watch-dog メール

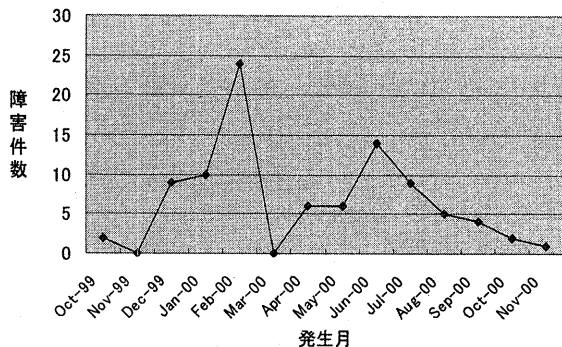


図4 障害記録

NOC 側から学校側ルータ、PC-UNIX の特定 port への疎通確認を cron で定期的に行うという単純なものであるが、障害の早期発見には有用である。障害が発生すると、図3のようなメールが管理者あてに届く。

プロジェクトの開始から現在(2000/11)までで約100件の障害記録があった(図4)。また、障害の内訳を図5に示した。

PC-UNIX をサーバとして用いた場合、必ずしも対障害性が高くないことは過去の報告にもある[6]が、障害のうち約半数は PC-UNIX に関連したトラブルとなっている。PC-UNIX 障害のうちの多くは、停電などによって電断が発生し、システム再起動がかかったようなケースである。必ずしも正しい運用とは言えないが、最近の PC-UNIX は突然の reboot が発生しても概ね正常に起動する。

最も深刻なのが HDD 障害である。本実験による PC-UNIX は、校内 LAN を分割するためのルータの他、前述した通りキャッシュサーバとしても動作するため、これが故障すると「教室から Web が参照できない」といった問題が発生する。その場合、緊急を要するときには、教室の各 PC に設定された Proxy の値を変更する等を行えば利用できるが、学校 PC には reboot による自動リカバリーシステムが導入されていることもあり運用が難しい。これについては、予備のマシンを用意しておき、障害が発生した場合には、柏市立教育研究所の要員が設置手順書に従って交換・復旧を行うことになっている。しかし、H/W 障害によってシステム交換を余儀なくされる場合、停止時間が2~10数時間に及んでしまう場合が多い。運用中、

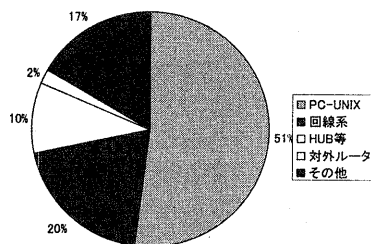


図5 障害の内訳

このようなトラブルが15件程度⁶発生した。

特に、使用期間約4年の中古PCを利用した中学校マシンで、運用開始から約4ヶ月のほぼ同一時期に HDD トラブルが頻発した。また、マザーボード上にあるリチウム電池が消耗しており、再起動すると CMOS 情報がクリアされてしまうような事態も発生した。このため、HDD と電池を別途購入して予防交換処置を行った。中古 PC を活用する場合、HDD だけでも新品を使うことが推奨される。ただ、HDD は 1GB 程度の容量があれば充分であるのだが、市場で入手可能な HDD は大容量化しており、適当な H/W の入手が困難である。古い PC の場合、BIOS と整合しないこともあるので注意が必要である。さらに、新規に導入したマシンであっても、運用から約半年で HDD の障害が発生することもあった(2件/12台)。稼動部分にトラブルが発生しやすいことは予想できたが、学校環境ではいわゆるマシンルームなどは存在せず、エアコンすら整備されていないことが多い。また、現場の教員はこの PC に触れることは少ないので PC-UNIX にとっては厳しい環境に置かれることが少なくない。

その他、実験的な CATV 接続であったことに起因する回線系の障害や、落雷等による障害、HUB の障害、運用に関連する障害(帰宅時に HUB 等の電源を落とされてしまう等)などが主な障害の原因となっている。一方、専用ルータの障害は非常に少ない。

⁶ 同じマシンでの HDD 障害だが reboot により一時的に回復させて運用を続けた場合もあるので、実質は 10 件程度。15 件には、HDD 予防交換による停止を含む。

6. 多機能ゲートウェイサーバの構築2 (プロトタイプ2)

約1年間の運用経験から、HDD等のH/W障害に対する復旧についての対応が特に重要であることがわかった。期間中、CATVの高速性を利用して、NOC内のサーバに夜間ネットワーク経由でバックアップを行う実験も行った。過去の研究[2]にもある通り、1組織あたり約2時間でバックアップは完了したが、将来、50組織を接続した状況での運用は難しいと判断した。

これに代わる仕組みとして、同一タイプのHDDを2本実装したプロトタイプ2・システムを考案した。あらかじめ起動可能なHDDをslaveディスクとして装着しておく。夜間、cronにて2本目のディスクをmountし、masterディスクのフルダンプを行う。バックアップ後は、mountが切り離されるので、2本目のディスクが駆動することではなく、バックアップ側HDD総駆動時間を短縮できる。1本目のディスクに障害が発生した場合には、HDDのみを交換することで同一環境を再現できる。PCが古いと、master、slaveのジャンパー切替を行ったのち、IDEケーブルを差し替える必要があるので多少の技術を必要とする。しかし、最近のマザーボードはHDDのcable selectモードに対応するので、ケーブル差し替えのみで作業完了できることもある。目標は「PC-UNIXの復旧を現場の教員が行えるようになること」であり、これに向けて講習会の実施等も予定している。

また、PC利用率の高い学校ではIPアドレスが不足するという問題も発生した。これについては、職員室系ネットワークをプライベートアドレスへ移行することで対応することとした。ストリーミング系アプリケーションは主に教室で利用されると判断したためである。ただ、職員室系でのこれらのアプリケーション利用も考慮し、static NATへの対応も行っている。さらに、持込みPCへの配慮から、DHCPサーバ機能を追加した。

柏地区では、運用当初より各学校毎のトラフィック状況をMRTGにより収集し蓄積している。これは対外用ルータからの情報である。今

後、校内の利用状況調査のため、プロトタイプ2にはSNMPの実装も行っている。

運用経験に基づいて以上のような改良を加え、プロトタイプ2はプロトタイプ1の機能に加え、以下の機能を有する。

- 1) HDD×2 (2本目HDDより起動可能)
- 2) NAT (ip-firewall)
- 3) DHCP (ISC dhcp)
- 4) SNMP (UCD snmp)

プロトタイプ2は、今年度のプロジェクト校、及び、柏市の整備計画に基づきネットワーク整備が行われる学校へ10月より導入が始まり、運用を開始したところである。

7. まとめ

学校内ネットワークの構築にあたり、校内LANを分割することの意義と、これを実現するためにKIUで用いた多機能ゲートウェイサーバを使った実践事例について報告した。学校用ネットワークのあるべき姿については、まだ議論が始まったばかりであり、運用データも少ない。今後、プロトタイプ2を用いた運用・管理面からのデータを蓄積し、校内LANのあり方についてさらに検討したい。

引用・参考文献

- [1] 大塚秀治・林英輔：CATVをアクセス網とした地域ネットワークの展開—地域における学校ネットワークの高速化—, 情報処理学会誌, Vol.41, No.1, pp.14-19 (2000.1).
- [2] 田口裕・相原玲二：分散管理を有する教育情報ネットワークシステムの基本構想について, 情報処理学会研究報告 2000-DSM-18, Vol.2000, No.62, pp.19-24 (2000.7).
- [3] 牧野晋・大塚秀治・林英輔：学校教育用ネットワーク運用における諸問題, 情報処理学会分散システム/インターネット運用技術 シンポジウム 2000 論文集, Vol.2000, No.2, pp.63-68 (2000.2).
- [4] 相原玲二・石川真由美・西村浩二：初等中等教育現場を対象としたインターネットサーバ, 情報処理学会研究報告 99-DSM-13, Vol.99, No.44, pp.25-30 (1999.5).
- [5] 文部省学習情報課：「ミレニアム・プロジェクト」により転機を迎えた「学校教育の情報化」(2000) http://www.manabinet.gr.jp/it_ed.pdf
- [6] 大野浩之：遠隔地に設置されたPC UNIXサーバを安定運用するための手法 第1報, 情報処理学会研究報告 2000-DSM-17, Vol.2000, No.47, pp.13-18 (2000.5).