第21部

地域活動(東北地区)

第１章　教育用ネットワークの設計における要件と問題点

1.1 概略

文部省は、平成十三年度 (2001 年) までにすべての学校を対象にしたインターネット接続整備計画を明示しており、今回の学習指導要領改訂でも、情報ネットワークを活用した学習が大きな柱となっている。これを踏まえ、県域での教育用のネットワークを構築する。ここでは県域の教育用ネットワークを構築するにあたり、他のネットワークと比べて留意しなければならなかったことを「教育用ネットワークの要件」と「運用上の技術課題」に分けて述べる。

1.2 学習指導要領とネットワーク構築上の目標

インターネットは、学習活動の場を教室や外の世界に拡大し、学習活動を深めるものと言われており、インターネット利用環境の整備は、国際化や情報化を重視した新しい教育課程の実施と深い関係がある。インターネットを学習に活用できる環境を整備することは、重要な課題である。

また学習指導要領の改訂の主な内容として、

- すべての児童生徒に情報活用能力を育成する。
- 小、中、高等学校段階を通じてコンピュータ等を積極的に活用する。
- 小学校段階では、総合的な学習の時間を中心に情報教育を実施する。
- 中学校段階では、技術・家庭科の「情報とコンピュータ」を必修に、発展的内容は生徒の興味・関心等に応じて選択的に学習する。
- 高等学校段階では、新教科「情報」を設け、「情報 A」「情報 B」「情報 C」の 3 科目から 1 科目選択必修とする。
- 特殊教育諸学校では、小、中、高等学校に準ずるほか、盲学校等において情報機器の活用を明確に位置づけ、知的障害者を教育する養護学校の高等部に選択教科として「情報」を設置する。

となっている。

上記の内容を実現するため、以下の目標を掲げる。

目標

- 児童生徒が安全に学ぶことができる
- 現場の教員の持つ専門的な知識を有効に活用できる。
- 社会教育に携わる専門または一般の多くの人々が参加しやすい。
- ネットワーク上のコミュニケーションによって得られた知識を再利用できる。

この中でもっとも大きな特徴は１番目の「児童生徒が安全に学ぶことができる」である。その他のものはどのようなネットワークでも多かれ少なかれ似たようなことを考えなければならないことである。しかしながら児童生徒からなる参加者の自己責任という点では、参加者が学習途上であるため大きな保護を必要としている。よって、構築するネットワークは、全体としてある程度インターネットに似ていて、インターネット上の安全な部分にはアクセスできるが危険な部分にはアクセスできないようなネットワークである必要がある。インターネットの魅力はそのネットワークが非常に大きく多種多様な人々が参加している点にある。一方これは逆に欠点でもあり、危険もまたこの点にある。具体的には、豊富さ多様性という点で十分魅力あるコミュニケーションを行えるような程度の大きな規模の学校間をつないだイントラネットを構築する。このようなイントラネットを構築した上でインターネットへのゲートウェイを設ける。このゲートウェイからはインターネットの安全な部分にのみアクセスできるようにする。

1.3 教育用ネットワークの利用者

1.3.1 教育用ネットワークの利用者構成と規模

目標を達成するための具体的なネットワークを構成する行政単位として、市町村レベル、都道府県レベルあるいは国レベルが考えられる。どのレベルで教育用イントラネットを実現すべきであろうか？市町村レベル特に町村では豊富で多様な参加者を得る

ためには十分ではないと思われる。豊富で多様な参加者といえるためには児童生徒を除いたアクティブな参加者の数が 1000 人を超える必要があると考えられる。そうすると、何らかの理由で非アクティブな参加者の割合を考えると 1 万人以上の参加者が必要になる。この規模の参加者を得るためには都道府県レベルのイントラネットが必要になる。しかし学校教育の関係者のみが参加しても多様性には限りがある。

一方で、教育とは学校教育のみを指すわけではない。社会教育もまた教育の一環であり、このためのネットワークも必要である。ここでは詳しく触れないが、社会教育用のネットワークもこの教育用イントラネットに含んでいる。

社会教育用のネットワークを含むことで、多様性はいっきに拡大し学校教育関係者のみの限界をある程度超えられると考える。

これによりインターネットなしでもある程度魅力あるネットワークが構築できると考える。しかし、県域で完全に閉じるのではなく更なる安全性を備えた多様性の確保のため都道府県間交流等を考慮していく。

1.3.2 利用者クラス

対象は県域教育用ネットワークとして

1. 県内の小中高校特殊学校の教職員
2. 県内の小中高校特殊学校の児童生徒
3. 県内の社会教育に携わる (不) 特定多数の人々
4. 県内の教育行政に携わる人々

となり、上記に該当する人員は下記のようになる。

メールアドレス、クローズドな BBS 等アカウントを必要とするもの

1. 小中高校特殊学校の教員 20,000 人
2. 児童生徒等 100,000 人
3. どの程度の規模になるか予想が付かないが社会教育関係者の一部

WWW の閲覧、BBS への書き込み、メーリングリストへの参加等アカウントを必要としないもの

最終的にはアカウント数 10 数万程度の大規模なものとなることが予想されるため、予め規模の拡大を想定して設計する必要がある。

最終的にネットワークが魅力的になるかどうかは「アクティブ」な参加者にかかっている。システム的にこれを増やしていけるシステムでなければならない。

1.4 教育用ネットワークの要件

1.4.1 使いやすいアプリケーション

操作性を上げる

教育用ネットワークでは、そもそも、ネットワークを利用するのが始めてであるという人も珍しくない。よって、メールが使えることを前提にできない。そこで、WWW 上に CGI で作成した BBS を設け、メーリングリストと連動させる。

また、議論の場は多様性がありすぎても議論が収束せず、なさ過ぎても議論にならない。例えば参加者が少ないうちは、「理科」の議論をする場でよかったのが増えていくと「物理」「化学」「生物」などに議論の場を分けていく必要があるなどである。そこで，メーリングリストや BBS を最適規模に分割できることを予めシステム化しておく

教育ネットワークにおいては、教育のしやすさが常に問われるので、エンドユーザの使用する部分は操作方法が一定していることが望ましい。よって構築するシステムも、特定メーカの独自プロトコルを避け、業者の気まぐれによる操作方法の変化を最小限にとどめる必要がある。

- インターネットと互換であること。これは TCP/IP を用い一般に用いられるインターネット用のツールを活用できること。メーカによる独自プロトコルを排除。
- コアのシステムは smtp、ftp、http、nntp、ntp、telnet、pop3、imap4、ldap 等インターネットで一般的に使用されているものを使用する。これを達成するために、少なくとも API だけでなくプロトコル仕様が公開されていて使用する機能を提供するプロトコルを使用したプロダクトが 2 製品以上あることが必要である。特定の企業の特定のアプリケーションに強く依存したものはなるべく使用しない。real system 等すでに重要なサービスであると考えら

れているが代替製品がない場合は例外とする。

- アプリケーションが変更になった場合でもデータの互換性を維持できること。現在において使用するデータフォーマットを扱えるプロダクトが 2 製品以上あるかソースコードが公開されていること。ユーザが使用する OS は現状では Windows95/98/NT/2000 及び MacOS8.0 以上を予定。

- すでに敷設されている各公所、学校等のプライベート、グローバルアドレスを使用した IP ネットワークと互換性をもつこと。これは既存の所内プライベートアドレス部、及び各学校のグローバルアドレスのネットワークが相互に http/smtp/nntp レベルで接続できることを意味する。できれば real system 等ストリーム系のプロトコルが通るように設計する。またこれはいわゆる「extra–net 問題」を含む。この問題を解決するために NAT や proxy を用いることになるが、この場合、stream 系のプロトコルの一部が通らない場合が考えられる。

- 人員増になっても、一貫した操作性を保持できること。人員増によるサーバの分割などを予め視野に入れておく必要がある。

蓄積情報を増やし再利用可能にする

ネットワークシステム全般にいえることだが、ネットワークの主役は人であり、ネットワーク上のコンテンツとはある意味人そのものである。しかしながら一度ネットワーク上に載せられた情報は蓄積し検索可能にしておくことで有限なリソースであるところの人への負担を減らすことになる。一度ネットワーク上に投入された情報は再利用可能でなければならない。再利用可能でなければ、如何に情報を蓄積しても利用可能な情報は増えない。公開可能なすべての情報は蓄積し検索可能にしておく。これはメーリングリストや BBS の書き込み内容も含む。

熟練者の知識を活用する

適宜コーディネータを立てて運用をスムーズに行えるようにする。

- 必要があれば議論が途切れないように議論の取りまとめ役/話題振り役を置きコーディネータとする。

- 参加したものの議論にならなかったり、回答が得られなかったりするのを防ぐ必要があるので、コーディネータが、議論に埋もれた発言を確認しやすいようにする。

- 議論の場を分割するときに、積極的に参加している参加者からコーディネータを立てる。

既存システムから取り込む

教育や行政において、ネットワーク化を推進したり、参加のリテラシーを向上させるため、既存システムをネットワーク化していく必要がある。現段階では、ネットワークの必要性を問う声があることもまた確かであり、これらの声に答えるため学習ではなく「実際に動いている」システムの実例を示すこともまた重要なことと考える。そこで

- 既存業務のうちネットワーク化した方が効率がよいものの積極的に取り込み。

- 電話と紙文書通知等の既存のコミュニケーション手段の可能な限りの置換。

などを行い、ネットワーク化のによる効率アップの実例としていけるようにする。

1.4.2 教育的安全性

通常ネットワークの参加者は自己責任で行動するが、教育用ネットワークにおいては、児童生徒を悪意から守る義務が生ずる。しかし、児童生徒の個人情報保護は各市町村の個人情報保護条例に左右されるので、県が構築するシステムは柔軟なシステムでなければならない。

- 児童生徒のプライバシーを守ることができる。

- 万が一悪意あるアクセス者にシステムのコントロールの全部又は一部が奪われたとき、それを発見できる。

- システムの管理者とコンテンツの運営者が別であり、ネットワーク的な安全性を確保する上での基準が明確である。

- 侵入を意図する、または侵入準備を意図するアクセスによるユーザの不安を取り除くことができる。
- 相互につながったネットワークのうち相互に安全であるネットワークとそうでないネットワークを区別し、個人情報を強く守るためのセキュリティを確保できる。

上記を解決するため、「教育用県域ネットワーク」を閉鎖空間で構築し、「教育用県域ネットワーク」からインターネットへのゲートウェイを持つようにする。すべての参加学校/機関は、「教育用県域ネットワーク」に接続する。ここはインターネットから直接アクセスできないネットワークであり、いくつかのセキュリティ装置によって守られている。「教育用県域ネットワーク」は一般公開をしないことから、「個人情報保護条例」の制約からある程度自由である。よって、児童生徒の実名による会話や発表を行うことができる。これにより、教育効果の濃い交流が行える。

また、学校からインターネットへのゲートは「教育用県域ネットワーク」のインターネットのゲートからのみであり、有害コンテンツのフィルターやウィルスのチェックもこのゲートで行う。

上記を満たすように各学校が「教育用県域ネットワーク」へ接続するため、以下の方法のうち 1 つをとる

- FR/ATM/digital leased line の直接接続
- インターネット経由の VPN

ダイアルアップを用いない理由は、県下には 1000 校の学校がありこれをすべてダイアルアップで収容することはできないことである。学校におけるインターネットの使用状況を見ると 13 時から 15 時に利用が集中しており、ダイアルアップの口も利用時間の分散を当てにはできないので 1000 校分のダイアルアップの口を設ける必要がある。しかしこれは非現実的である。また、学校側からしても、県北地方にあるサーバセンターに直接ダイアルアップを行うのは電話代がかかりすぎる。学校によってはサーバセンターから 30km 以上離れている。このため、サーバセンターにダイアルアップをせず、FR/ATM/digital leased line による直接収容か最寄りのインターネット プロバイダにダイアルアップか OCN のような常時インターネット接続サービス経由の VPN でサーバセンターにアクセスする。

これにより、すべての関係機関を「教育用県域ネットワーク」の内側に接続させることが可能になる。

1.5 運用上の技術課題

1.5.1 障害対策体制

コンピュータ ネットワークの宿命としてコンピュータのトラブルがある。しかしこのようなトラブルの解決は、情報化教育とはコンピュータの操作を覚えることではないので情報化教育にとって関係のないことである。このようなトラブル時においては速やかに外部のスタッフが問題の解決をし、システムのダウンタイムを最小にする必要がある。

以下の要件を満たす専任のヘルプデスク及び SE を活用する

- トラブルがあった場合、早急に原因を切り分けし、ネットワーク上のトラブルであればすばやく対応し、結果報告を出せること。
- 設定変更等が生じた場合早急に規格化されたレポートを出せること。
- ユーザサイドでは基本的にトラブル時に問題の切り分けをする知識はないのでこれに対処するよう対応できること。
- いわゆるインターネットプロバイダ サービスで提供されるサービス（smtp,pop3,http, ユーザの ftp) をイントラネット用に用いたときは、ISP とはまた違った制限が付くが、よく知っているユーザほど制限に馴染んでもらえないことが予想されるのでこれらをうまく説明できること。

具体的には Windows, Macintosh, Unix で

- interface の生き死を確認できる (ifconfig, netstat)。
- IP layer の接続確認ができる (ping)。
- ip foward の様子を trace できる (traceroute)。

- DNS の解決を確認できる (nslookup, resolver)。
- NVT でサーバの生き死を確認できる (telnet)。
- NAT の動きを理解している。
- routing table を読める。
- syslog を読める。
- サーバのプロセスを確認できる。
- super daemon の役割を理解している。
- netbios(over IP と over NetBEUI) の動きを理解している。
- appletalk の動きを理解している。
- TCP/IP, NetBEUI, AppleTalk, その他の切り分けができる。
- IP filtering/TCP wrapper の動きを理解している。
- 特定のプロトコルだけ到達できないことがある proxy の働きを理解している。
- HUB, Switching HUB, Router の違いを理解している
- 上記の知識を元に総合して、問い合わせもとのユーザにわかりやすい質問をして

client OS の Network 以外の部分に問題があるのか	ユーザで対処、納入業者で対処
client OS の Interface の設定に問題があるのか	ユーザで対処、納入業者で対処
client OS の routing table に問題があるのか	ユーザで対処
client OS の DNS の設定に問題があるのか	ユーザで対処
client の proxy の設定に問題があるのか	ユーザで対処
Windows の NetBIOS の設定に問題があるのか	ユーザで対処
Windows の NetBEUI の設定に問題があるのか	ユーザで対処
Macintosh の AppleTalk の設定に問題があるのか	ユーザで対処
Router の Routing Table に問題があるのか	納入業者で対処、サポートで対処
Router の IP Filter の設定に問題があるのか	納入業者で対処、サポートで対処
Router の NAT の設定に問題があるのか	納入業者で対処、サポートで対処
Ethernet の設定に問題があるのか	納入業者で対処
HUB 等の故障ではないか	納入業者で対処
Server に問題があるのか	サポートで対処
電話に問題がある	納入業者で対処、プロバイダで対処

の切り分けができる。

以下、関係機関の役割をまとめると

ヘルプデスクの役割 上記切り分けを行い、client の設定に問題がある場合には修正案をユーザに出す。下記分類に応じて適切な解決者に連絡する。

プロバイダの役割 ヘルプデスクの切り分けにより、ppp, routing, 電話がつながらないなどの問題解決をする。

ハードウェア納入業者の役割 ヘルプデスクとサポート委託業者の切り分けにより、納入した機器に問題がある場合の問題解決をする。

サポート委託業者の役割 ヘルプデスクの切り分けにより、センター内のネットワークに問題がある場合の問題解決をする。

サーバに問題がある場合のハードウェア障害かソフトウェア障害かの切り分け、ハードウェア障害の場合はハードウェア納入業者に連絡、ソフトウェアの場合は問題の解決、各学校がネットワークを構築する場合のコンサルタントにより障害からの回復を早急に行える体制を整える。

サポート委託業者は、システムの構築に関わった全体を熟知している特定の SE である。委託した場合の問題点として、システム提案時に提案を行った SE と実際に構築を行った SE に力量の差があり提案はよかったが構築時に提案がうまく反映していないなどということが無いように、提案、構築、サポートの SE は同一技術者とした。あくまで業者ではなく技術者と話し合うようにした。

ヘルプデスクも業者ではなくヘルプデスク本人とよく話し合い、こちらが要求した水準がある人物かどうか判断する。

1.5.2 セキュリティ対策

セキュリティ対策として、いわゆるファイアウォールは採用しなかった。これは、buffer over flow がアタックの中心になっている現在では、単純なフィルタリングではセキュリティ的に軟弱である、と判断したからである。そこで、ルータによる port 毎のフィルタと個別サーバの TCP wrapper は使用するが、フィルタリングはそれのみとし、全体的な対策は IDS (Intrusion Detection Systems) を使用することにした。

IDS として Cisco 社の Net Ranger を使用した。これは、例えば buffer over flow によって、管理者権限が奪われても、侵入者が不審な動き、例えば、/etc/shadow を cat で開こうとしたりすると、発信元と受信先に TCP RST を送り TCP セッションを切断する。また、アタックが長期に及んだときは、ルータのフィルタを書き換えアクセス不能にする。また、IDS を使用することにより、ルータのフィルタやファイアウォールによる、速度の低下を防ぐことができる。

1.6 教育用県域ネットワークの構築と運用

1.6.1 ネットワーク構成

提供するサーバ環境としては

- WWW 情報提供/公開
- 参加者のメールの送受信
- BBS システム
- Internet News
- ldap を利用したディレクトリサービス
- ntp による時刻同期

を想定し、上記を使用するために必要なサービス（例えば DNS）も当然用意する。その他のユーザ−ユーザ間のサービスは安全なネットワークの要件を満たす限り妨げない。

1.6.2 ユーザ管理

行政・教育従事者の大部分は、コンピュータシステムの秘密情報保持能力に大きな不安を持っている。このことの大部分は、コンピュータのセキュリティに関する無理解が原因であるが、一方で、セキュリティホールが次から次へと発見されていることもまた確かであり、不安ももっともなことだと考えられる。当初、ldap ディレクトリに多くの情報を登録して汎用ディレクトリとして用いようと考えていたが、上記のような理由で、登録可能な情報はごくわずかになってしまった。つまり、個人にかかわる情報のうち個人の業務以外の生活が特定できる情報（性別、年齢、住所、電話番号）などはもちろん、業務上の管理番号なども載せられないという結果になった。よって、当初においては、機関の住所、電話番号、機関用メールアドレス、個人の名前、所属、メールアドレス、メールサーバ、WEB/ftp サーバのアカウントとパスワードのみを登録し、イントラのユーザからのメールアドレスの検索と、web/ftp/pop3/imap4 の認証及びメール転送の virtual user table にのみ使用する。

1.6.3 メールアカウント管理

概要

メールシステムは、人事異動、改姓や個人情報保護などを考慮したシステムとし、以下のカテゴリをもつ

- 職員用メールアドレス
  - 学校非依存アドレス
  - 学校依存アドレス
- 機関用メールアドレス
- 児童生徒用アドレス

– インターネット用アドレス
– 教育ネットワーク用アドレス

職員用メールアドレス

メールアドレスは自分の責任で管理しなければならないことを認識するため、馴染み深いものでなければならない。また各職員は 3 年から 5 年で異動になるため、異動を考慮したメールアドレス体系にしなければならない。また、改姓による氏名の変化もあるので、これも考慮しなければならない。

よって、メールアドレス中 user@domain の user は記号の羅列ではなく意味のある、使用者に identify できるようなものである必要がある。そこで、システム的には user 部分は任意に設定できるようにする。しかし、完全任意ではなく、使用者の氏名と何らかの関連性があるものとすることをポリシーとしてもった。つまり、メールシステムとしては完全にどのようなものでも設定できるが、氏名と関連性の無い物は登録しない（申請を受けつけない）こととした。

上記を達成するため、センター側で 4th level domain 部分にユニークな id を設定しサブドメインとした。DNS の MX は当然「*」となる。

よって

`ANYTHING@UNIQ.3rd-level.ed.jp`

という形をとる。これをもって「学校非依存メールアドレス」とした。このアドレスはすべての教職員のうち臨時ではないものにアサインされる。

また、教師が授業で児童生徒とやり取りを行う場合、学校名がついていた方が親しみ易いと考えられるので、「学校非依存メールアドレス」の他に「学校依存メールアドレス」を用意した。これは

名前@学校名.3rd-level.ed.jp

という形を取るもので、「名前」の部分は学校内でユニークであることが保証される必要がある。このユニーク性の保証は学校内で調整してもらう。このアドレスは異動により破棄される。このアドレスはすべての教職員にアサインされる。

学校非依存アドレスと学校依存アドレスの関係は同じ local アカウントに alias される 2 つのアドレスという関係である。

この実装であるが、学校非依存アドレスは、1 ドメイン 1 ユーザ状態になる。このため、user unknown と host unknown をどのようにして返すかが問題となる。今回は sendmail の K マクロによる virtual user table によって実装した。本格稼動時にはアカウントが ldap に登録されるため、K マクロから ldap を引くことになるが、ldap がまだ稼動していないので、K マクロから、BerkeleyDB を引いた。

基本的な動きは以下のようになる sendmail.cf の S0 内で

メールアドレス ⟹ 学校非依存の virtual user table

あれば local のアカウントに変換して local へ

メールアドレスのドメイン部 ⟹ 学校非依存の virtual user table

あれば user unknown で error

メールアドレス ⟹ 学校依存の virtual user table

あれば local のアカウントに変換して local へ

メールアドレスのドメイン部 ⟹ 学校依存の virtual

あれば user unknown で error、なければ host unknown で error

機関用メールアドレス

連絡用として以下のアドレスを定義する。これは、業務連絡用に担当者を探さずに済むようにである。一般に、校長宛の文書は、学校機関を意味するところであり、通常事務で開封され受け付けられる。しかし校長宛の電話は校長個人によって処理される。このようなことを考えるとメールは文書とも電話ともいえないもののように思える。よって上記による混乱を避けるため、機関用アドレスとして校長/分校長、教頭/副校長、ネットワーク/情報教育担当者の個人に着信するメールと学校という機関に着信するメールを分ける必要がある。しかし、機関に着信とはいっても最終的に誰かが処理するのであるので、機関として校長/分校長、教頭/副校長、ネットワーク/情報教育担当者全員を当てた。

`head@学校名.3rd-level.ed.jp`
　校長/分校長

`assist@学校名.3rd-level.ed.jp`
　教頭、副校長

`netmaster@学校名.3rd-level.ed.jp`
　ネットワーク/情報教育担当

`school@学校名.3rd-level.ed.jp`
　上記のすべて（学校宛文書）

これらは、各学校依存アドレスに alias される。

児童生徒用メールアドレス

今後の「情報」と「教育」を考えるとき児童生徒はメールを使用できるべきであり教育はこれをサポートしなければならない。児童生徒用にメールを使用するに当たって、次のことに注意する

- 受信者である児童生徒が望まない内容（中傷、誘惑、spam 等）のメールが直接児童生徒に届かないようにする必要がある場合がある
- 送信者である児童生徒が受信者が望まない内容（中傷、誘惑、spam 等）のメールを出さないようにする。

一方、児童生徒は、即時性、直接性、強い自己責任性、使い方によっては強い匿名性などのメールの特徴も学ばなければならないのでメールを教師がすべてモデレートするわけにはいかない。よって、メール環境をクラス分けする。

- メールソフトの操作を学ぶ場合、インターネットに接続された環境は必要なく、同一教室内の相手に出せればよい。児童生徒が教師の目の届く範囲で活動している限り強い匿名性が現れることはない。
- 情報交換ツールとしての即時性、直接性などを学ぶ場合でも初期においては教師によるコーディネートが必要であり、インターネット上のアドレスでも宛先は限られる。よって送信先、着信先を限定したメール環境によって望まないメールを食い止めることができる。

上記を踏まえて

- 教育ネットワーク用アドレス　メールアドレスを児童生徒個人に割り当てある程度自由に使えるが送受信先は、所属学校の同一教室、同一学年あるいは共同研究校のみとする。
- インターネット用アドレス　クラス、サークルや行事の実行委員会などに与え、教師のコーディネート下に置くようにする。

の 2 つを設定する。

メールデリバリエージェント

学校のコンピュータ環境の現状は、未だコンピュータの共有状態である。これは、児童生徒においてもそうであるが、教師もまた、コンピュータを共有して使用している。しかし、メールアドレスを共有したり、メールがプライバシーの保てない状態でやり取りされるは防がなければならない。また、クライアント機に資源が希少であるのでメールの使用が制限されるというようなことがあってはならない。メールアドレスを共有すると、いわゆる浄書された文書のみがメールで流れ作業段階のメールが流れなくなる。このことにより、メールの持つ即時性、直接性が失われ、単なる通信ツールとなり、思考補助のツールとはなりにくくなる。

しかし、一方でコンピュータが共有であるというのは事実であり、メールの持つメリットを生かしつつコンピュータを共有しなければならない。

このため、特定のコンピュータでなければ作業できないというような事態が無いように、メール環境は imap として、どのコンピュータからもメール環境は同一である様にする。このことによって、職員室でもコンピュータ室でも同じように作業できるようになる。また児童生徒にとっても、コンピュータの数が少ないことによるアカウント共有を防ぐことができる。

共有アドレス帳

メールアドレスの検索をするため ldap ディレクトリを活用する。この ldap は、ユーザ管理で使用している ldap である。

1.6.4 WWW システム

WWW による情報の公開は、教育において個人情報保護との兼ね合いで難しい問題をはらんでいる。インターネットの不特定の訪問者への公開という点では、制限される必要があるが、一方で交流という点では、制限されたくない。当該県域教育ネットワークはイントラネットであるのでアクセス制限をかけるのは容易である。ただし、インターネット向けとイントラネット向けのサーバに全く同じページをもつというのも無駄である。公開範囲は、インターネットに公開してもよいものは、イントラネットに公開してもよい、逆は不可という関係なので、これを階

層構造とする。

あるサーバのディレクトリ `~/www/pref/internet` を定義して

- internet 以下のディレクトリは、すべてに公開
- pref 以下のディレクトリはインターネット以外に公開
- www 以下は校内のみに公開

となる。

ここで internet は www に含まれるので、internet においたものは、自動的にインターネット以外や校内のみにも公開されることになる。

よって、同一 URL、例えば `http://www.学校名.3rd-level.ed.jp/` をアクセスした場合、インターネットからとイントラネットからと所属の学校からでは見え方が変わることになる。

この実装は、実際の WWW サーバはイントラネットからのみ直接アクセスできるようにすることによって、行った。DNS の指す WWW サーバは、この実際に ftp するサーバではないサーバを指すようにするると、インターネット用とイントラネット用の DNS は実際には異なったサーバを指すことになるので、それぞれのサーバから、異なったディレクトリに proxy pass を張ることで実現する。

WWW サーバの ftp アカウントは、各学校の net-master 毎に作成し、uid は学校毎に作成、ftp アカウントと実際に login する uid は ldap により認証/変換する。

1.6.5 アクセス制御

教育用ネットワークは VPN で接続された VPN である。VPN の実現方法は多種多様である。ここでは以下の方法を検討した。

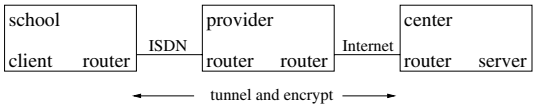
前提 1 学校側の負荷を減らすため、VPN は、router-router か router-server で行って欲しい。クライアント 1 台 1 台に設定はできない。20 台× 1000 校で 2 万台。クライアントが増えるたびにはできない。

前提 2 通信は暗号化して欲しい

前提 3 センター側で最低 100 セッション同時に処理して欲しい

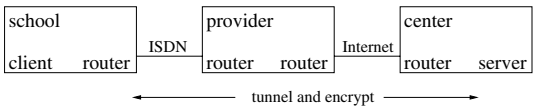
前提 4 なるべく学校側に金銭的な負担が出ないようにする

ルータ–ルータでの暗号化



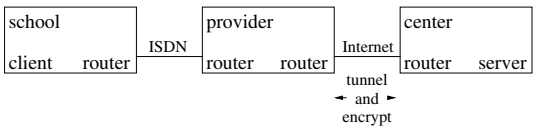
あるいは、

ルータ - サーバでの暗号化



あるいは、

ISDN の部分は覗き見不可能と仮定してプロバイダのルータ - ルータでの暗号化



となって欲しい。

候補として

- PPTP
- IPSec
- ppp over udp など
- クライアント/サーバ ベースの VPN
- L2TP

が上げられる。以下個別に検討する。

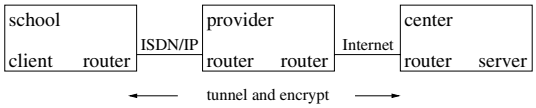
PPTP

学校　–　センター
router　–　router
mn-128　–　mn-128
router　–　server
mn-128　–　PopTop
client　–　router
いろいろ　–　mn-128
いろいろ　–　いろいろ
client　–　server
いろいろ　–　PopTop
いろいろ　–　WindowsNT

のパターンがある。

router–router の場合

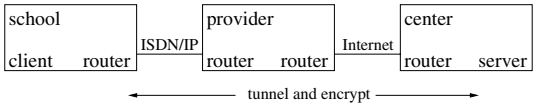
user 側の router は安価なものがある（mn128-soho-*)。center 側は、多くのセッションをさばけ、且つ user が使用する暗号化と互換のものはない (mn128-soho-*は 2 セッションまで)。



前提 3 を満たさないので不可。

router–server の場合

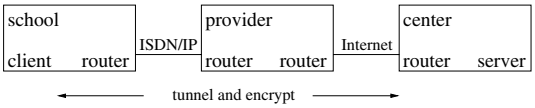
user 側の router は安価なものがある（mn128-soho-*)。center 側は、多くのセッションをさばけ、且つ user が使用する暗号化と互換のものはない (PopTop は、mppe 互換の暗号のみサポート)。



暗号化できない。前提 2 を満たさないので不可。センター側でどれだけ処理できるかわからない。前提 3 を満たさないので不可。

client–router の場合

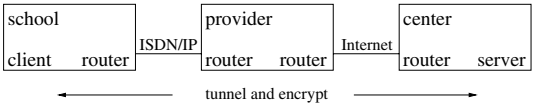
user 側の client は、無料のものがあるが、すべてのマシンには入れる労力は払えない。center 側は、多くのセッションをさばけ、且つ user が使用する暗号化と互換のものはない (mn128-soho-*は 2 セッションまで)。



ユーザの労力的負荷が大きい。センター側でどれだけ処理できるかわからない。前提 3 を満たさないので不可。前提 1 を満たさないので不可。

client–server の場合

user 側の client は、無料のものがあるが、すべてのマシンには入れる労力は払えない。center 側は NT の RAS を使用した。



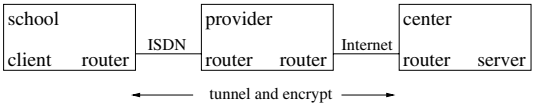
ユーザの労力的負荷が大きい。前提 1 を満たさないので不可。センター側でどれだけ処理できるかわからない。前提 3 を満たさないので不可。

全体として PPTP は有効な解ではない。

IPSec

router　–　router
学校　–　センター
Cisco router　–　Cisco router
yamaha RT103i　–　yamaha RT140p
FreeBSD+KAME　–　FreeBSD+KAME

のパターンがある。この場合、user 側に、特定の router を要求する。



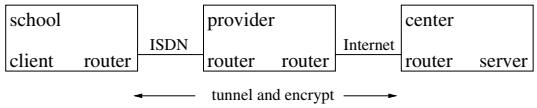
基本的にユーザ側の ip アドレスは固定でなければならない。provider の協力が必要。ユーザの金銭的負荷が大きい。ip アドレスを固定にしない方法もある。

ip アドレスを固定にしなければ有効な解になり得る。

ppp over udp など

router – router
FreeBSD – FreeBSD
+iij-ppp+KAME +iij-ppp+KAME

のパターンがある。この場合、user 側に、特定の router を要求する。

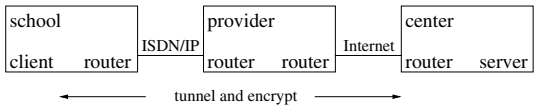


センター側でどれだけ処理できるかわからない。前提３を満たさないので不可。ユーザの金銭的負荷が大きい。

有効な解ではない。

クライアント/サーバ ベースの VPN

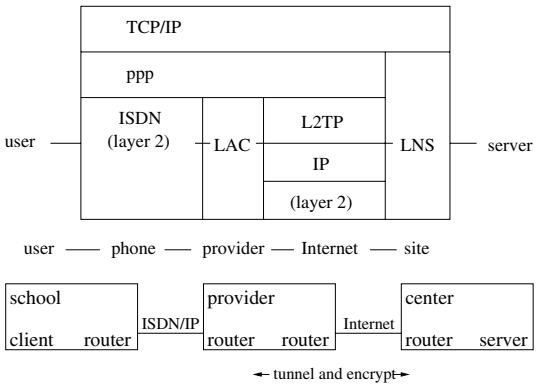
client-router



ユーザの労力的負荷が大きい。前提１を見たさないので不可。センター側でどれだけ処理できるかわからない。前提３を満たさないので不可。

L2TP

router-router L2TP とは、



となる方法で、ppp の認証と TCP/IP の取り出しは、VPN でつなぎたいサーバのある site で行われる。

ユーザからは、ppp でつなぎたい site に直接つながったように見える。site からは、自分の提供する ppp のダイアルアップの口が、あたかもプロバイダにあるように見える。

これを行うためには、provider に LAC(L2TP Access Concentrator) と呼ばれる機能をもつ dialup router が必要である。具体的には、Cisco の AS や 3600 で IOS 12.0(2a)T1、ascend の MAX で TAOS 6.0.10、3Com Total Control で ComOS 4.1 などがあり、L2TP 用の設定がされていればよい。

また、site 側には、LNS(L2TP Network Server) と呼ばれる機能を持つ router が必要である。具体的には、LAC と同じような製品が必要になる。

ここで、問題点は、provider に LAC を用意してもらえるかである。

provider の負担が大きすぎる。センター側でどれだけ処理できるかわからない。前提３を満たさないので不可。

有効な解ではない。

選択可能なもの

結果的に

IPSec で ip アドレスを固定としない方法

のみが解として残った。ここでは、Cisco 社ルータの機能によるものを採用した。

1.7 効果と現状

上記は県域教育ネットワークとして構築途上のもので、未だに実装されていないものも目立つ。現在実装を終え、運用に入ったものは、メールと WWW のみである。この中でいくつかの問題点が見えてきた。１つは、メールの設定に関して、imap と pop3 を用いる事ができるようにしてあるが、インターネットを活用してきた教師ほど pop3 を選ぶ傾向があるようである。特に imap 非対応のメールソフトを使用しているものは、継続してそのメールソフトを使用しようとするのでほとんど imap を選ぶことはない。計画段階では、今までインターネットを積極的に活用してきた教師に他の教師の補助となってくれることをもくろんでいたが、思ったほど imap の活用がなされない。imap の活用は、時間がかかる課題となっている。

WWW の階層的なアクセス制限は、概念は納得してもらえるものの、いざアップロードとなるとやはり理解しがたいらしく、なんども質問を受けた。ま

た、html エディタの制限でうまく階層を保持できないこともあるようである。例えば、どの階層からもアクセスされるアイコンなどは internet ディレクトリの下に置かなければすべてからアクセスできなくなるが、www の直下に置くことが多いためページが崩れてしまうなどである。

1.8 まとめ

更なる活用はこれからの話となるが、教育用ネットワークを設計しただけでも、その上に述べたような特殊性をいくつか思いついた。教育用ネットワークは数多く設計されたしこれからもますます設計されると思われるが、メールと WEB だけできればよいのではなく、児童生徒の安全性まで考えて設計されたものはなかったように思う。今回考えたことはまだまだ不充分な点も多く、運用上不具合も出るとは思われるが、同じような試みを行っているものに対しては、参考になると思う。

第 2 章　JB におけるネットワークトラヒック監視

2.1 成果

1. ATM レベル地図の自動生成
2. トラヒックデータの収集
3. トラヒックデータの公開

2.2 ATM レベル地図の自動生成

2.2.1 現状

JB の Web ページで公開されている VCI 情報*のみを用いて ATM レベル地図の自動生成を行ない、以下の URL で公開している。公開には、後述する NetSkate というツールを用いている。

<URL:http://netskate.cysol.co.jp/>

* <URL:http://www.wide.ad.jp/wide-confidential/JB/vci-readme.html>

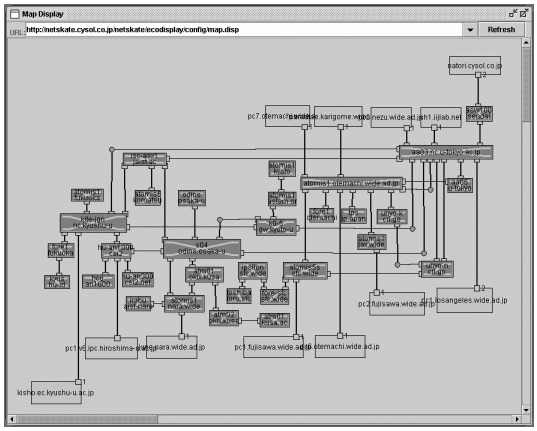


図 2.1　全体図

現在マップ上で表示可能な情報は、ATM スイッチの接続とスイッチの管理者情報、そして各ポート上の割り当て済み VPI/VCI 情報である。

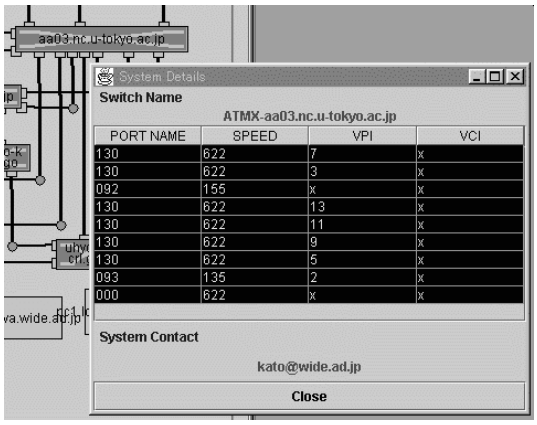


図 2.2　ATM スイッチ詳細

2.2.2 今後の課題

ATM スイッチと IP ルータの接続についての情報が公開されていないため、IP レベルの地図が生成できなかった。現在地図上に表示されている IP ルータは後述するトラヒックデータ公開システムのために便宜上追加されているもので、正確な情報に基いていないものである。

今後 IP レベルの情報が公開され次第、IP レベルの地図の生成を行ない公開する予定である。

また、自動生成の利点を活かしてネットワークトポロジの変化に即応する形で地図の更新を行なっていく予定である。

2.3 トラヒックデータの収集

2.3.1 成果

現在 JB に関係する IP ルータのトラヒック情報を SNMP により大規模に収集を行なっている。

収集には SNMPpoller というパッケージを用いた。このパッケージは Perl5 で記述され、収集頻度の正確さと管理トラヒックの極小化に主眼を置き設計されている。

実験に用いたマシンの構成を以下に示す。

CPU	Intel Pentium III 450MHz
メモリ	128 Mbytes
ディスク	20 Gbytes
ネットワーク	Intel EtherExpress Pro 10/100B Ethernet
OS	FreeBSD 2.2.8 + KAME STABLE 20000214
ソフトウェア	Perl5
	SNMP_Session (perl module)
	SNMPpoller

このシステムにより実際に収集されたデータのサマリを以下に示す。

収集期間	1999/12/14 〜 2000/3/31
収集間隔	60 秒
総データサイズ	約 2.4 GBytes
ホスト数	12 †
インタフェース数	75 †
インタフェースあたりの管理オブジェクト数	23

2.3.2 今後の課題

トラヒックデータの収集に関し、この規模であれば問題無く安定してデータの取得が行なえることを確認できた。今年度はデータの解析を行なっていないが、取得項目の再検討と併せ効果的な解析が行なえるよう研究を進めていく必要がある。

† インタフェース・ホスト動作状況に応じて変動

2.4 トラヒックデータの公開

2.4.1 成果

以下の URL で収集した情報を公開している。公開には Java 2 で記述された NetSkate というツールを用いているので、Java Runtime Environment 1.2 以上の動作する環境であれば、プラットフォームを問わず閲覧することができる。

<URL:http://netskate.cysol.co.jp/>

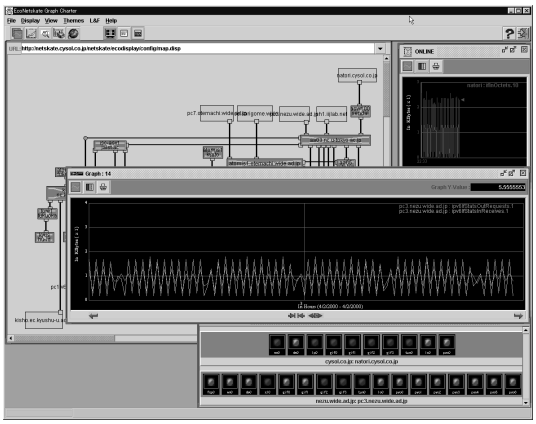


図 2.3 NetSkate 動作画面

NetSkate を用いることにより得られる情報を以下に示す。

- ネットワーク地図の表示 (前述)
  - ATM スイッチの詳細情報
- グラフ化された蓄積トラヒックデータ
- 現在のトラヒックグラフ
- 現在の IP ルータインタフェース状況

公開に用いたマシンの構成を以下に示す。

CPU	Intel Pentium III 450MHz
メモリ	128 Mbytes
ディスク	8 Gbytes
ネットワーク	Intel EtherExpress Pro 10/100B Ethernet
OS	SUN Solaris 7
ソフトウェア	Java 2
	NetSkate system
	Apache
	Perl5
	SNMP_Session (perl module)

2.4.2 今後の課題

NetSkate は未だ発展途上の段階にあり、データを処理し表示する機能に足りない部分がある。前項のデータ収集と併せ、効果的なトラヒック情報解析が行なえるよう考察を重ねていく必要がある。