平成 13 年度

修士学位論文

ネットワークポリシに基づいた
校内ネットワークの構築

Policy-based Design of School Networks

1045023　　田鍋潤一郎

指導教員　　情報システム工学科　清水明宏

2001 年 12 月 28 日

高知工科大学大学院 工学研究科 基盤工学専攻

情報通信ネットワークコース

要 旨

ネットワークポリシに基づいた
校内ネットワークの構築

田鍋潤一郎

学校は急速な勢いで情報化が進んでおり，学校のいたるところにコンピュータが置かれ，校内ネットワークが整備されようとしている．どのようなネットワークを構築し，運営・管理していくかという学校におけるネットワークポリシの策定は急務である．

本稿では，学校と企業のネットワークポリシの違いについて述べ，教育用ネットワークの特性を明らかにし，校内ネットワークにおけるネットワークポリシの基本的要求項目について提案する．そして，ネットワークポリシに基づいた校内ネットワークを構築する上で，児童・生徒に個人環境を持たせるための具体的な方法と，サーバへの個人認証の問題を解決する一方法を示す．また，校内ネットワークを運用・管理していく上で欠かせない，ネットワークモニタリングシステムの概要について述べる．

キーワード　ネットワークポリシ, ネットワーク管理システム，モニタリング，学校ネットワーク

Abstract

Policy-based Design of School Networks

Tanabe Junichiro

In today's schools, computerization is progressing quickly. Computers tends to be set up throughout schools and connected to Local Area Networks. As a consequence, it is necessary for us to urgently propose a school network policy on what kinds of networks should be installed and how they should be managed.

In this report, we propose the concrete method of protecting students' individual environment in building school networks based on network policy. Further, we present the outline of a network monitoring system that is essential for manageing the networks at schools.

key words Network Policy, Network Management, Monitoring, School Networks

目次

図目次

図目次

表目次

第 1 章

序　論

1.1　研究の背景

平成 9 年 11 月 4 日に文部大臣により「全国のすべての国公立私立学校を対象に，2001 年までに中・高等学校および特殊教育学校，2003 年までに小学校をインターネットに接続する」方針が表明された [1]．続いて政府は平成 11 年 12 月，ミレニアムプロジェクト [2] と題し，新しい千年紀に向けて新産業を生み出す技術革新への取り組みをスタートさせた．このプロジェクトの中には，教育の情報化プロジェクトも含まれており，具体的な整備計画としては，すべての普通教室に 2 台ずつ，その他の特別教室用に各学校 6 台ずつを整備し，併せて小学校のコンピュータ教室を 2 人 1 台から 1 人 1 台体制に充実させるというものである．また，すべての公立学校について，2001 年度末までにインタネットへの学校接続を目指し，2004 年度末までに校内 LAN(Local Area Network) を整備することとしている．学校は，急速な勢いで情報化が進み，学校のいたる所にコンピュータが置かれ，校内ネットワークが整備されようとしている．

企業では，数年前から，セキュリティや管理ポリシを中心に，ネットワークポリシの重要性が言われ，ポリシに基づいたネットワークの構築が進んでいる．今では，それを一歩進め，ポリシベースネットワークとして，システム化されようとしている [3]．

業務の効率化を図るために設計された，専門の管理者によって運営されている企業のネットワークと，児童・生徒の教育のために活用される専門の管理者不在の学校のネットワークでは，ネットワークポリシの違いは明らかであり，それをそのまま学校へ適用させることはできない．

1.2　研究の目的

校内ネットワークの導入が急速に進む一方で，解決されていない大きな問題として,「校内ネットワークを誰が管理するのか」ということが挙げられる．最近の IT 関連ニュースでも「学校の IT 現場も人材不足」の中で「管理者がいない」[4] として連載の第 1 回で取り上げられているほどである．このことは，学校に，確固たるネットワークポリシがないために，ネットワークの管理は誰がするのか，どのようなネットワークを構築するのか，どのようにネットワークを活用し，どのように運用していくのかという明確なポリシのないことが原因の一つであると言える．そこで本研究では，ポリシに基づいたネットワークの構築が進んでいる企業のネットワークと，学校のネットワークの違いを明らかにした上で，校内ネットワークポリシの必須項目について検討し提案する．そして，ネットワークポリシに基づいた校内ネットワークと，現状の校内ネットワークを比較検討し，具体的な改善の手法を示すのが本研究の目的である．

1.3　本論文の構成

本論文の以下の構成は次のようになっている．第 2 章では，本研究の位置づけについて述べる．第 3 章では校内ネットワークのポリシの策定を行い，ポリシに基づいた現状の校内ネットワークの具体的な改善点を述べる．第 4 章では，策定したネットワークポリシに基づいた校内ネットワークの構築および改善について述べる．第 5 章では，改善したネットワークの評価を行う．最後に，第 6 章で本論文の結論を述べる．

第 2 章

研究の位置づけ

2.1　ネットワークポリシとは

都丸によると，ネットワークポリシとは,「情報ネットワークの利用条件や運用条件の規定がポリシーであり，ポリシーに従って情報ネットワークを設計し，あるいは構成要素の運用条件を決めるといったことを意味している」と述べ，ネットワークポリシの構成要素として「サービス品質ポリシー」「性能設計ポリシー」「信頼性ポリシー」「拡張性ポリシー」「ルーティングポリシー」「セキュリティポリシー」「ネットワーク管理」の 7 項目を挙げている [5].

ネットワークポリシとは，ネットワークを安全に運用・利用する上での指針として「誰が」「何を」「どのように」「どの程度」行うかを目標やガイドラインとして明確に示したものである．それらを参考にし，ネットワークポリシの構成要素を，大きく三つのカテゴリに分類した.

ネットワークポリシの構成としてあげられる要素を図 2.1 に示す.

校内ネットワークポリシの策定は，早急な課題である．筆者の校内ネットワーク運営の経験を踏まえ，ネットワークポリシのそれぞれの構成要素について，積極的な提案を試みる.

2.2　学校と企業のネットワークポリシの違い

企業と大学のネットワーク利用形態の違いについて述べ，そのセキュリティ対策について論じたものとして「セキュリティと利便性を考慮したシステム構築の一考察」[6] がある．研究機関として位置づけられる大学のネットワークと，児童・生徒が授業で活用する学校ネッ

2.2　学校と企業のネットワークポリシの違い

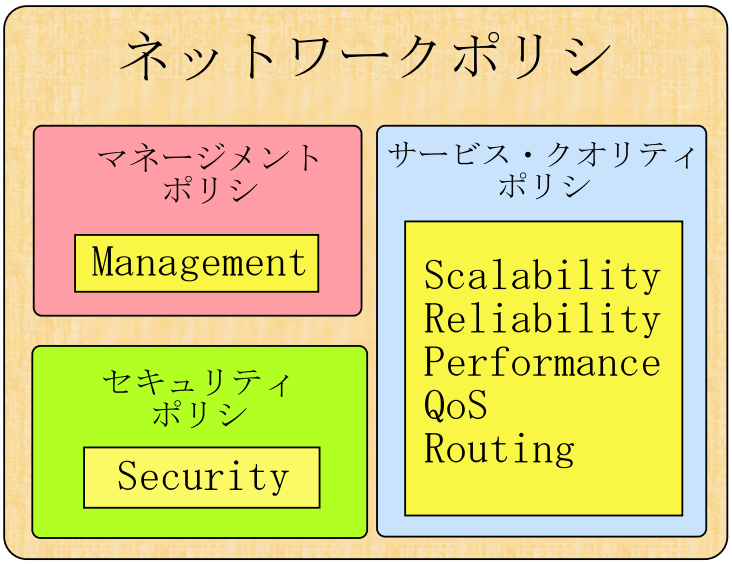

図 2.1　ネットワークポリシの構成要素

トワークとは自ずと利用形態が違ってくる．また，利用者が成人に限定される大学ネットワークと，発達段階・学習履歴の異なる学校ネットワークでは，運用方法にも違いがある．しかし，企業と学校のネットワークポリシの違いについて論じているものはなかった．そこで，筆者の校内ネットワーク運用の経験を基にして，ネットワークポリシの構成要素ごとに違いを述べる．

- マネージメントポリシ

  ネットワーク内での管理すべき対象を明らかにし，誰がどのように管理するのかを決めるのが，マネージメントポリシである．企業では，専門のネットワーク管理者がおかれ，規模によっては，管理部門が置かれている所も多い．学校には，専門のネットワーク管理者もおらず，クラス担任や教科担任が掛け持ちでやっているのが実情である．数百人のアカウントを一人で管理し，ネットワーク内での振る舞いを見守るというのは容易にできるものではない．管理者の負担の分散が必要である．

- セキュリティポリシ

  セキュリティポリシは，守るべき対象をどのようにして守るのかを決めるものである．企業の場合は，利益に関わる機密情報や顧客の情報等をターゲットにした外部から

の脅威が問題になる．また，内部からの脅威も無視できないものがある．このような内外からの脅威に対するセキュリティ対策としてファイアウォールを設置して防衛することが一般的である [6]．一方，校内ネットワークにおいては，専門のネットワーク管理者がいないことから，外部からの脅威に対処することは難しい．学校単独で高度なセキュリティを確保するよりも，外部機関のファイウォールによって守られていることが望ましい．

また，コンピュータの利用形態の違いについて比較してみると，企業の場合は，一般に１人に１台のコンピュータが配置されており，個人の使うコンピュータは固定されている場合が多い．学校では，児童・生徒数に対するコンピュータの数が極端に少なく，不特定多数の児童・生徒が同じ端末を使うことになる．そのために，特定の端末のデスクトップに複数の児童・生徒の作品が散在し，個人情報が，他の児童・生徒に漏洩するだけでなく，教師が扱うべき情報が児童・生徒の目にとまるようなことも起こりうる．

さらに，個々の端末にもセキュリティに関る様々な設定が必要である．企業では専門のネットワーク管理者がガイドラインを定め，設定を行っている．学校では，ガイドラインすらない場合が多く，導入された状態のまま使っている場合が多い．どこまで，児童・生徒が自由に端末を使えるかという，個々の端末のセキュリティポリシは考慮しなければならない問題である．ネットワークの設定一つを変更されても，その端末はネットワークに繋がらなくなってしまう恐れがある．

- サービス・クオリティポリシ

ネットワークには，どの程度のパフォーマンスが必要であり，ネットワーク全体の品質基準は，どの程度必要かということを決めることがサービス・クオリティポリシである．企業では，拡張性やルーティングも重要になってくるが，校内ネットワークでは，これらの２つは必然的に決まってくることであり，考察の対象とはしないことにする．企業ではコストに見合ったパフォーマンスや品質が望まれ，学校では，限られた予算の中で，ネットワークをどのように活用するかを第一に考えて決めなくてはならない．教育用ネットワークにおいて，特に重要度の高いサービスは何であるかを事前に明らか

にする必要がある．そして，具体的にどのような使われ方をするかを想定したうえで，サービス実現のためにはどのようなシステムが必要であり，また，どの程度の帯域が必要であるかを見極めることが重要である．

2.3　校内ネットワークの現状及び問題点

2.3.1　プライバシの保護とセキュリティ対策

個人の使う端末が固定されていない学校では，共同端末で個人環境を確立することが必要であるが，一部を除いてほとんどの小・中学校で個人環境が確立されていないのが現状である．「マイドキュメント」や「デスクトップ」に複数の児童・生徒の作成したファイルが入っていることも多い．そのような状況では，不用意に他人のファイルを書き換えたり削除したりする危険性がある．また，個人のファイルを他人が自由に閲覧できるので，児童・生徒のプライバシはないといってよい．そのような状況では，児童・生徒は安心してコンピュータを使うことはできない．サーバ・クライアント環境でない共同端末でメールサービスを行った場合，個人宛てのメールをいとも簡単に第三者が見ることができてしまう．

また，児童・生徒のプライバシを守るためには，ネットワーク内での児童・生徒の動きを見守ることが必要である．そのためには，サーバの各種ログの管理や閲覧をしなければならない．自ずから，サーバ保守用の知識が必要となり，ネットワーク管理の専門家ではない学校の先生にとっては無理がある．

2.3.2　個人認証の問題

共同端末での児童・生徒の個人環境を確立するための最も現実的な方法として，サーバ上に個人ディレクトリを持つことが考えられる．しかし，そのためには，サーバへの個人認証はさけては通れない．ローマ字の学習が小学校４年生であることを考えると，小学校や中学校のように，学習段階・発達段階の違う児童・生徒に，一般的なキーボードによる認証を強制することは現実的ではない．

マイクロソフトより学校向け BackOffice ツールキットとして，ログイン時のユーザ名やパスワードで文字や数字の入力を一切排除し、マウス操作のみの絵合わせでコンピュータにログオンできるツールが配布されている [7]．しかし，このような GUI による認証システム

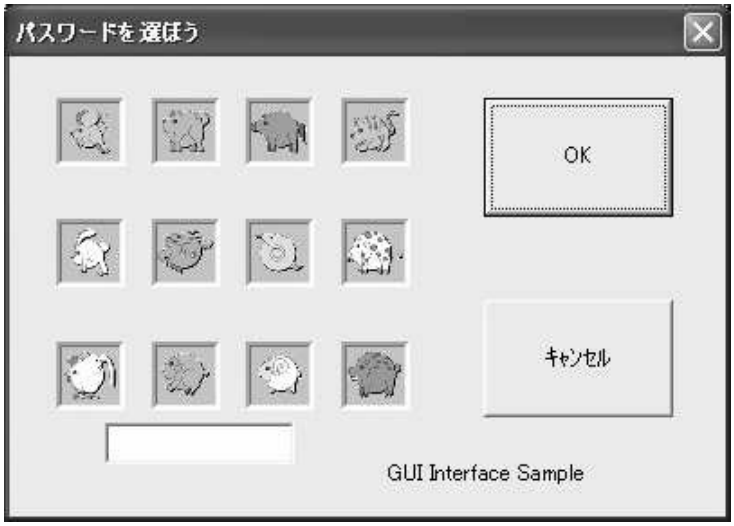

図 2.2　GUI インタフェースの例

では (図 2.2)，パスワードの入力に時間がかかるばかりでなく，第三者によって入力中にパスワードを見られる恐れがあり，セキュリティ上好ましくない．また，必要なシステム，ソフトウェアとして，

サーバー側	Windows NT Server 4.0 + Service Pack 5 以上
クライアント側	Windows NT Workstation 4.0 + Service Pack 5 以上

が挙げられており，多数の学校現場に入っている OS が Windows98/95 であるという現状では，使用できる学校は限られる．また，新たにサーバソフトウェアを購入する必要があり，コストもかかる．

2.3.3　導入済みコンピュータの問題

現在の学校に導入されているコンピュータは，OS として Windows95 または Windows98 が採用されているのが主流である．これらの OS は，パーソナルユースで利用するには比較

的使いやすいが，不特定多数のユーザがコンピュータを共有して使う教育現場では，サーバ上に個人環境を持ち，電子メール環境を構築するためのクライアントマシンの OS としては，最適なものであるとはいい難い．問題点としては次のようなものがあげられる．

- マルチユーザで使えない．Microsoft Network サービスを利用することで，起動画面表示後にログインウィンドウが表示されるが，キャンセルすることで誰でもそのコンピュータにログインすることができる．
- 擬似マルチユーザ環境のため，キャンセルでログインし，他人のパスワードファイルを簡単に消去できる．パスワードを消去し，他人の ID でログインすればその人になりすますことができる．
- ファイル，ディレクトリにおけるセキュリティが貧弱である．ファイル単位の細かいセキュリティの設定には対応しておらず，ディレクトリ単位のセキュリティも利用者のレベルでの管理ができない．
- ログインした利用者のデスクトップ環境などの情報を利用者ごとに管理することは可能であるが，複数台のコンピュータを一括管理することができない．

以上のような問題を解決するためには，Windows NT（または 2000）でのサーバ・クライアント環境を構築しなおすことである程度解決できるが，学校におけるコンピュータは旧機種となったからと言って簡単に買い換えることは難しく，数年間は既存の機種を用いなければならない．また，サーバ単独での導入では，後に電子メールサーバを構築することを考えると，コスト的に見合わない．また，クライアントマシンが Windows95 または Windows98 である場合には，NT 上に個人ディレクトリを持つことは簡単にはできない．

第 3 章

校内ネットワークポリシの策定

3.1　校内ネットワークポリシとは

「校内ネットワークポリシ」とは，企業におけるネットワークポリシの考え方を，校内ネットワークに適用しようとするものである．学校ネットワークの特性を踏まえ，学校におけるネットワーク構築と運用の指針とするためのものである．具体的には，どのような目的を持って校内ネットワークを構築すればよいか，誰が，どのように管理し，どのように運営をしていくかを明確に述べたものである．ポリシの策定は，個々の校内ネットワークに関わる項目は省き，基本的な要求項目にのみとどめた．

3.2　マネージメントポリシ

まず初めに考えなければならないことは，校内ネットワークを誰が管理すべきかを明確にすることである．専門の管理者のいない学校では，コンピュータにある程度詳しい者が管理者になる場合が多いが，自分の仕事をしながら，その合間に校内ネットワークを一人で管理・運営していくのは困難である．

そこで，手間のかかる煩雑な管理業務は保守管理業者に実施してもらい，報告を受けられる体制にしておくことが大切である．その上で数人の管理者グループを組織し，ネットワークの保守や，バックアップを担当し，個々の児童・生徒のことを最も知っている学級担任が，アカウント管理を行うのが望ましい．このような管理者組織モデルを図 3.1 に示す．

そのためには，コンピュータやサーバ管理に詳しくない教職員でも，ログ管理や閲覧がで

き，ネットワーク内での児童・生徒の振る舞いを見守っていけるシステムが必要である．

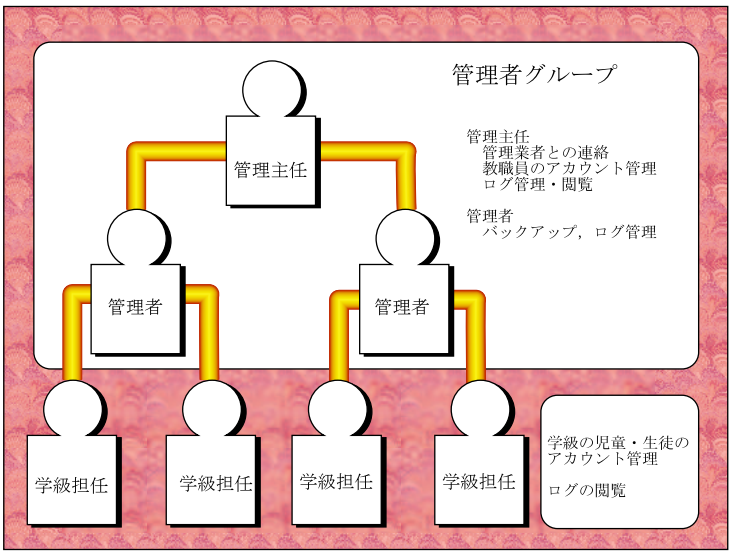

図 3.1　ネットワークの管理組織

3.3　セキュリティポリシ

児童・生徒の個人情報を守り，一人ひとりのプライバシを保護することはたいへん重要なことである．個人専用の端末が存在しない学校で，上記のことを実現するためには，サーバに個人ディレクトリを持つことが必要となる．また，ゲストやグループアカウントでの端末へのログインは，個人の匿名性を強め，ネットワーク内での児童・生徒の振る舞いを把握することができなくなる危険性がある．今後，コンピュータがコンピュータ室だけでなく，学校のあらゆるところに置かれるようになるという前提では [2]，どの端末からログインしても個人環境が実現できるような校内ネットワークシステムにする必要がある．

このような環境を実現するためには，サーバ・クライアント方式にすればよいが，ログイン時に，サーバへの ID とパスワードによる個人認証が必須となる．しかし，前章でも述べたように，現状の認証システムは，キーボードからの英数字の入力が必要であり，発達段階の違う小・中学校の児童・生徒全員に使えるものではない．また，ID やパスワードを覚えることがコンピュータを使うことの必要条件になっては，本末転倒である．導入されている

機器に大幅な変更の必要のない，新しい認証の仕組みが必要とされている．

また，有害情報へのフィルタリングも必要である．日々増殖するインターネットですべての有害情報を遮断することは難しいが，必要な時に容易に設定できる方法が必要である．外部機関でのフィルタリングも必要であるが，実際の運用現場でのタイムリなフィルタリングがより効果的である．

さらに，データへのセキュリティも考慮しなければならない．UNIX システムのファイルやフォルダのパーミションは比較的強固であり，グループ機能と併用すれば，校内ネットワークでは実用的なレベルのセキュリティが確保できる．

加えて，端末のセキュリティも大事な要件である．ログイン時にキャンセルで入り，他人のパスワードを消すことはいとも簡単にできてしまう．また，ネットワークの設定を一箇所変更しただけでも，コンピュータはネットワークにつながらなくなってしまう．教師用と児童・生徒用のコンピュータの端末のセキュリティレベルを変更し，児童・生徒用のコンピュータはネットワークコンピュータなどのプロパティにアクセスできないようにしておく必要がある．

表 3.1　セキュリティポリシ

端末へのログイン方法	誰でも使える新しい認証方式が必要
アカウント発行	匿名性をなくすため個人アカウント発行
個人環境の構築	サーバ上に個人ディレクトリを持つ
アクセス権の設定	グループにより設定する
端末のセキュリティ	グループ毎にセキュリティレベルを分ける
有害情報のフィルタリング	運用現場でのフィルタリング
ウィルス対策	端末にウィルス駆除ソフトを入れる
	端末に共有フォルダを作らない

3.4　サービス・クオリティポリシ

まず初めに，校内ネットワークをどのような目的で構築し，どのように活用していくのかを明確にする必要がある．今後のネットワークの使われ方の一つの指針として参照すべきものに,「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』」[2] がある．その中で動画コンテンツの重要性を指摘し,「これまでの授業をわかりやすくするための動画コンテンツ」としてその教育的効果について述べられている．これからの学校ネットワークは,教材として使える品質の動画がストレスなく再生できるだけの帯域の確保が必要となる．

しかし，実際に流通する教材コンテンツの容量は明らかになっていない．実際の流通コンテンツに見合った，教育用ネットワークに必要な帯域幅の調査の必要がある．

ネットワーク構築の目的に関わるサービスの優先順位としては，大阪教育大学の調査 [8] でもマルチメディアリソースとしての Web[*1]の利用と，交流・共同学習がインターネットの教育利用の二つの柱として位置づけられているように，Web ブラウジングと，メール環境を整えることが最も優先しなければならないサービスであると言える．

しかし，この調査の中でも明らかなように，交流・共同学習の経験の有無では，54%の学校が無いと回答している．実施できない要因として，第 1 位がメールアカウントの不足で,全体の 40%を占め，次いで児童・生徒のプライバシ保護の問題が続いており，これらで全体の 76%を占めている．メールアカウントの不足については，校内にメールサーバを設けることにより解決できるが，児童・生徒のプライバシの保護には，サーバ上に個人ディレクトリを持つことと併せてメールの送信履歴を確認する必要がある．

校内にメールサーバを設置し，児童．生徒にメールアカウントを持たせることについては，様々な議論がある．電子メールでのコミュニケーションにおいて，しばしば攻撃的なメール，非礼なメールや感情的なメールを送ってしまうという事例も報告されている [9].

しかし，四国総合通信局の統計情報 [10] によると，携帯電話・PHS の人口普及率（契約数を総務省「国勢調査速報による人口」で除した値）は，平成 13 年 10 月で全国で 56.4%,

[*1] Web(World Wide Web)

四国で 50.9%となっており，携帯端末による IP 接続の契約数の人口普及率は全国で 36.4%，四国で 36.2%となっていることからも，もはやメールについては，教育利用での効果の大きさや，リテラシ教育の必要性も含めて，学校では無視できない状況になっている．

また，高知県では，子どもたちの悩み事を電子メールで受け付ける「E メール相談」が平成 13 年 11 月 1 日から開始され，たくさんの相談が寄せられているように [11]，子どもたちの日常生活の中にも深く浸透していることも明らかである．

最後に，教育用ネットワークのトラヒックの特性について，考察してみた．特徴として，カリキュラムに準じた一斉授業を行うことから，次のようなトラヒック特性があると考えられる．

1. 時間的なバースト性

   教師の指導のもとに一斉にアクセスを行うことから，一定時間内にバースト的なトラヒックが発生する．
2. アクセス対象の類似性

   一斉授業で活用される場合には，アクセスする対象となるコンテンツが類似している事が多い．特定のサーバに負荷が集中することがある．
3. カリキュラムに応じたトラヒックの再現性

   カリキュラムに従って授業が進んでいくことから，同一学年の異クラスで，類似のトラヒックが次々と発生する場合が考えられる．
4. 時間的なトラヒックの特性

   トラヒックが平日の昼間に集中し，夜間や休日は極端に少ない．

以上のことから，一度アクセスしたコンテンツはローカルでキャッシングし，二度目からは，ローカルで配信することのできるキャッシュサーバを設置することにより，網内を流れるトラヒック量を大幅に軽減し，ユーザへの応答速度を向上させる可能性がある [12]．

また，カリキュラムに従って計画的に授業が進んでいく点と，時間的なトラヒック特性を考慮すれば，教材コンテンツのミラーリングや，事前配信技術の手法も効果的である．

表 3.2　サービス・クオリティポリシ

必要な帯域	動画コンテンツが参照可能であること
優先するサービス	Web サービス Mail サービス
校内 LAN 配線	10/100BASE-TX
トラヒック改善	キャッシュサーバの設置
	ミラーリングまたは事前配信

第 4 章

ネットワークポリシに基づいた校内ネットワークの構築

4.1　ネットワーク構成モデル

一般的な小・中学校における，ネットワーク構成モデルを図 4.1 に示す．学校に一度導入された機器は，簡単には買い換えることは難しく，数年間は既存の機種を用いなければならないのが普通である． そのために，既存の機器を活用していく方向で，現実的なモデルを提案している．

校内ネットワーク構成モデルの概要を，図 4.1 に基づいて説明する．

- 校内ネットワークは，管理上の問題からも外部機関のファイアウォールによって守られていることが望ましい．
- セキュリティの観点から，外部公開用の Web サーバはファイアウォールの外に設置し，必要に応じてファイル転送する．校内ネットワークとしては，内部の Web サーバを最大限活用する．
- キャッシングと，有害情報フィルタリングのため Proxy Server を設置し，必要に応じて Mail Server, DNS Server を設置する．
- 校内 LAN は，レイヤー 3 スイッチまたはマルチプル VLAN スイッチで三つのセグメントに分け，アクセス制限をかけ，児童・生徒エリアからは教職員エリアへのアクセスはできないようにする．

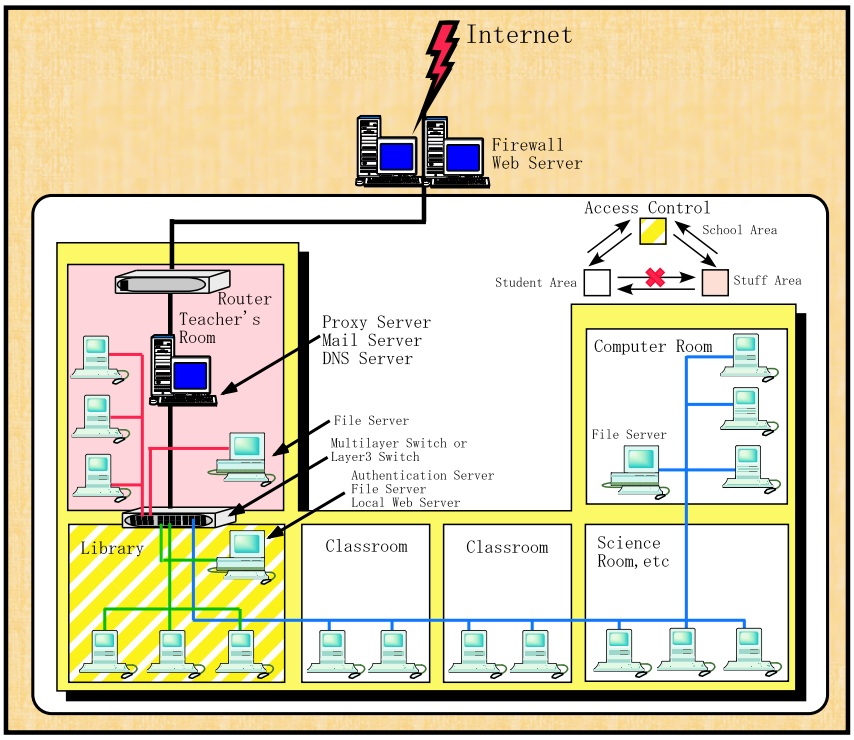

図 4.1　校内ネットワーク構成モデル

- 児童・生徒の個人情報（成績や家庭環境）を保護するためには，教職員エリアの入り口にファイアウォールを置くことも必要となる場合もある．
- LAN は，10/100BASE-TX とすることにより，ローカルキャッシングと，ローカル Web サーバのパフォーマンスを生かすことができる．

ネットワークポリシに基づいた校内ネットワークシステムを構築することで，安全で，管理しやすく，使いやすい校内ネットワークの構築が可能となる．

4.2　校内ネットワーク運用における問題点の改善

校内ネットワークの構成モデルに準じてネットワークを構成し，適切な機器を導入すれば，ネットワークポリシに基づいたネットワークが構築できるが，学校は一度導入された機器は簡単にリプレイスすることは難しく，今ある機器やネットワークを数年間は使わなければならない．けれども，児童・生徒のプライバシの保護やセキュリティの問題一つを取ってみて

も，早急に解決しなければならない問題である．

そこで，策定したネットワークポリシに基づいて，現状の校内ネットワークを比較・検討し問題点を明らかにした．その結果，次のような提案が必要となることが明らかとなった．

- 児童・生徒のプライバシを守るため，移動端末における個人環境を確立するための方法の提案
- 発達段階・学習履歴の違う児童・生徒でも使える個人認証の仕組みの提案
- 専門の管理者でない先生が，ネットワーク内での児童・生徒の振る舞いを見守るためのシステムの提案

以下の項で，それぞれの問題点を解決する具体的な方法を述べる．

4.3　個人環境の確立

先行研究として，長谷川らの実践事例がある [13]．この事例では，Windows95 をクライアントとし，Windows NT サーバを導入し，サーバ上に個人ディレクトリを持たせる試みを取り上げている．

個人ディレクトリ設定のためにはレジストリを書き換えたり，スクリプトファイルを設定したりしなければならず，構築・管理面で不便な点も多いことが報告されている．また，セキュリティの面を考慮するとシステムポリシの機能を使い，ユーザの権限を制限する必要があることも報告されている．本研究では，サーバ OS として Linux[*1] を導入することにより，問題のいくつかを解決する．

- UNIX のファイルシステムが使えるため，個人毎にファイルやディレクトリ単位でセキュリティの設定が可能である．
- Samba[*2] を使うことにより，Windows 端末でも比較的簡単に Linux サーバ上に個人お

[*1] 元ヘルシンキ大学の Linus B. Torvalds 等が開発推進したオープンソースで配布されている UNIX 系 OS

[*2] UNIX および UNIX クローンのオペレーティングシステムが動作しているマシンにおいて，Microsoft ネットワーキングプロトコルを使用したサービスを提供できるようにするためのプログラム群

よび共有ディレクトリを持つことができる.

- メールサーバを含めると，導入コストを低く抑えることができる.

Samba をプライマリ・ドメイン・コントローラとして機能させることにより，サーバ上の個人ディレクトリ内にユーザプロファイルを保存するようにし，ログオンスクリプトにより，ログイン時に共有ディレクトリと，個人ディレクトリをドライブとしてマウントさせることにした．これにより，ネットワークコンピュータを開くことなく，サーバ上のディレクトリを活用できるようになった． また，サーバ上の個人ディレクトリ内にメールボックスを設置することにより，一箇所の端末で設定すれば，どこの端末でも個人のメールアカウントが使えるようになった．端末に，一度ログインすれば，そのまま個人アカウントでメールができるのである．管理者の側からみても，メールアカウント設定の労力の大幅な軽減になるはずである.

さらに，UNIX のグループ機能を生かして，ユーザを，ゲストグループ，児童・生徒グループ，教師グループ，管理者グループ，の 4 グループに分け，それぞれのグループによって，最適なポリシファイルが適用されるようにした.

具体的な方法としては，ログオン時に読み込まれる，BAT ファイルを作成する．この中で，実際にマウントドライブの設定を行い，net time コマンドにより，端末の内蔵時計をサーバの時計に合わすように設定する.

次に，ポリシファイル（この場合のポリシーファイルは，Windows 環境での，端末の環境設定用のファイル）を作成する．端末で，ポリシエディタを起動し，児童・生徒用のアクセスなら，ネットワークプロパティを非表示にするなどの必要な設定を行った．主な端末のセキュリティポリシは表 4.1 のように設定した.

この設定作業は非常に難解で，詳しくは解説書[*3]を参照されたい.

作成した，二つのファイルをサーバ上のグループディレクトリのポリシファイル用のディレクトリに置く．samba サーバの設定に，グループ環境変数を使えば，管理者グループ以外

[*3] Windows98 リソースキット 日経 BP 社,Windows95 リソースキット アスキー出版局

表 4.1　端末のセキュリティ設定の例

		管理者	教職員	児童・生徒	ゲスト
制限事項	ネットワーク変更	○	×	×	×
	デスクトップ変更	○	○	○	×
	ファイル名で起動	○	○	×	×
	共有プリンタの使用	○	○	○	×
	MS-DOS プロンプト	○	×	×	×
ポリシファイルの配布受付		×	○	○	○
マウントディレクトリ	ホーム	○	○	○	×
	児童・生徒	○	○	○	×
	教職員	○	○	×	×
	管理者	○	×	×	×

でログインした場合ネットワークの変更はできないように (図 4.2)，ログイン時のユーザアカウントの所属グループによって適切な端末ポリシが適応される．

ログインするユーザにより，端末の環境を変えることが可能となり，端末毎のセキュリティが大幅に上がった．ポリシファイル配布の概要を図 4.3 に示す．

4.4　フロッピディスク利用による認証システム

サーバ上に個人ディレクトリを持つためには，サーバへの個人認証はさけては通れない．小学校や中学校のように，発達段階の違う児童・生徒に，一般的なキーボードによる認証を強制することは無理があることは，既に述べた．

そこで，誰でも簡単にログインができ，大幅なシステムの変更の必要がない，フロッピディスクによる認証を提案する．

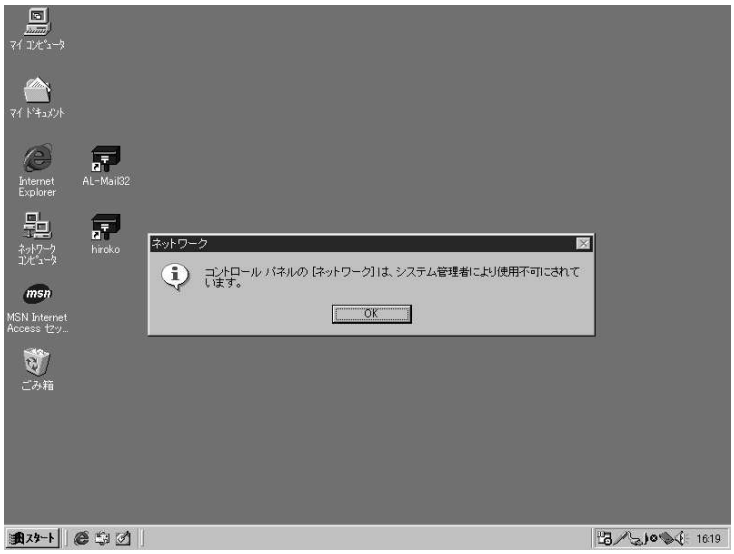

図 4.2　ポリシファイルの適用例

ディスクログインシステム (図 4.4) として開発したこのアプリケーションは，ID とパスワードを暗号化してフロッピディスクの中に保存しておき，ログイン時には，通常のログイン画面を出さずに，ディスク挿入を促す画面を出し，その後フロッピディスクを入れると，認証が完了するというものである．複数の端末に対応するため，端末への新規ログインでも，パスワードの再入力が必要のないものになっている．

管理者は，ログインディスクの管理をすれば，児童・生徒の使用をある程度制限でき，使用状況も把握できる．学校においては，一部のネットワーク管理者にまかされていた児童・生徒のアカウント管理を学級担任に委ねることができる．また，ログインディスクがなければ，ログインできないため，学校内でのプライバシの保護もできる．

通常の，ログインウィンドウが表示されないため，キャンセルでログインし，不明のユーザがアカウントを操作したりすることも不可能となる．ログインディスクとしては，現在ほとんどのコンピュータに内蔵されているフロッピディスクをメディアとして利用したが，よりセキュアな JAVA CARD[14] なども将来的な選択肢として検討する必要がある．

また，より強固なセキュリティが必要とされる場合や，校内ネットワークが外部機関でのファイアウォールによって守られていない場合には，清水らによる SAS（Simple And

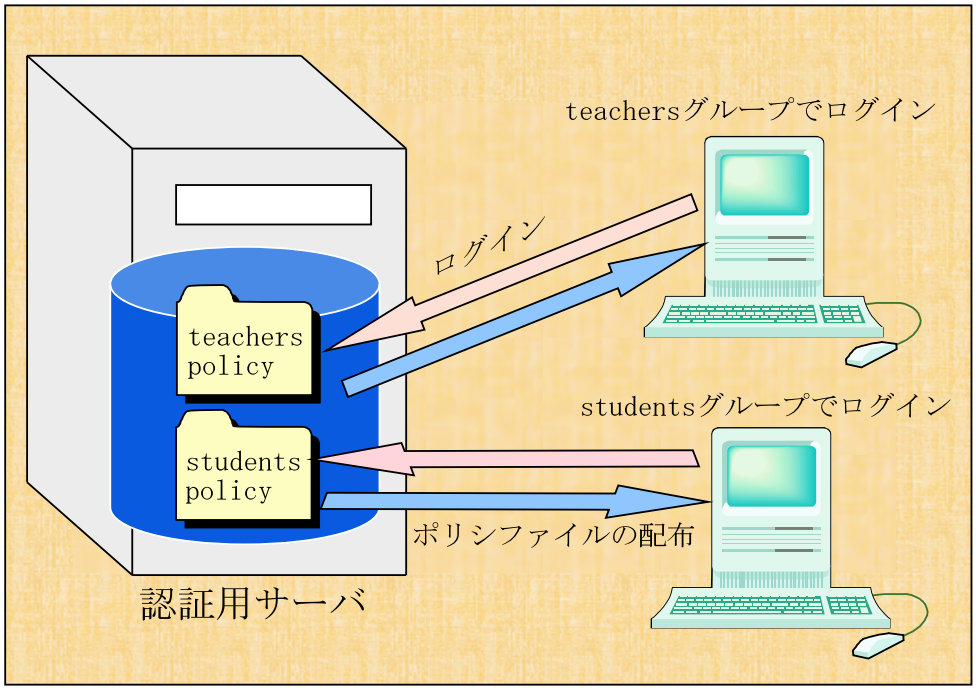

図 4.3　ポリシファイル配布の概要

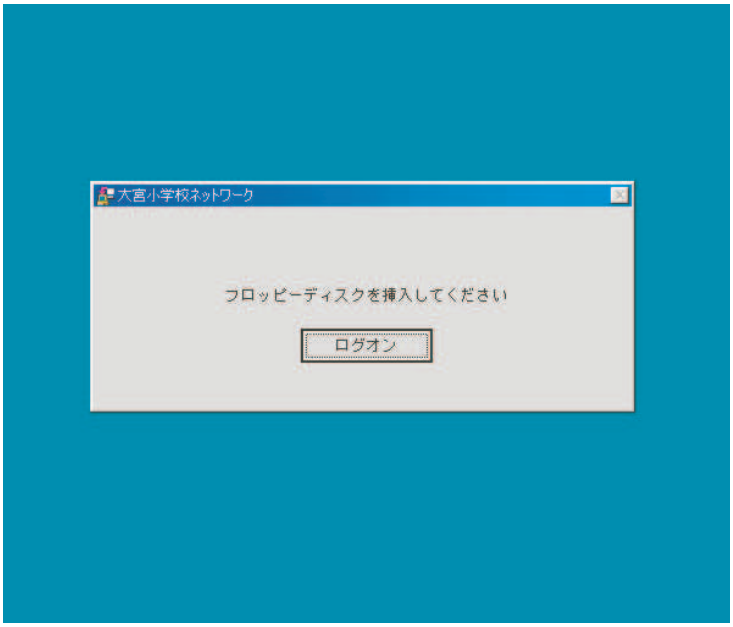

図 4.4　ディスクログインシステム起動時の画面

Secure) 暗号通信方式 [15] を HTTP プロキシに応用した，SASProxy[16] を使う方法も検討する必要がある．SAS は，次回認証情報予告型ワンタイムパスワード方式であり，毎回異なった認証情報を生成し，安全，且つ，極めて少ない計算量で認証を実現することができる．この特性から，フロッピディスクや，記憶容量の限られた外部メディアでの認証にも対応できる．SASProxy の概要を図 4.5，暗号処理方式を図 4.6 に示す.

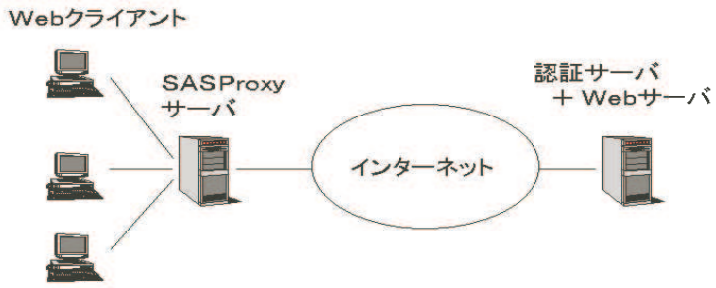

図 4.5　SASProxy の概要

4.5　Web Based 校内ネットワークモニタリングシステム

4.5.1　モニタリングシステムの概要

Web ブラウザを使ったネットワークの監視ツールや設定ツールは，市販されているものや [17]，実践的な研究の中から様々なものが生まれている [18]. しかし，ほとんどのものが，ネットワークの障害やセキュリティ面の不安を監視・管理するものであったり，サーバの設定を容易に行おうとするものである.

これらは非常に有用なツールであるが，学校において，一教師である管理者や学級担任にとっては，セキュリティの監視やシステムの障害状況を常々監視することは時間的にも，また，スキル面でも非常に困難な状況である．むしろ，校内ネットワークでは，児童・生徒がどのような場所から，どのように使っているかを知ることが重要であり，ネットワーク内での児童・生徒の動きこそが欲しい情報だと言える.

このようなネットワークのモニタリングシステムの研究例としては，IP アドレスとユー

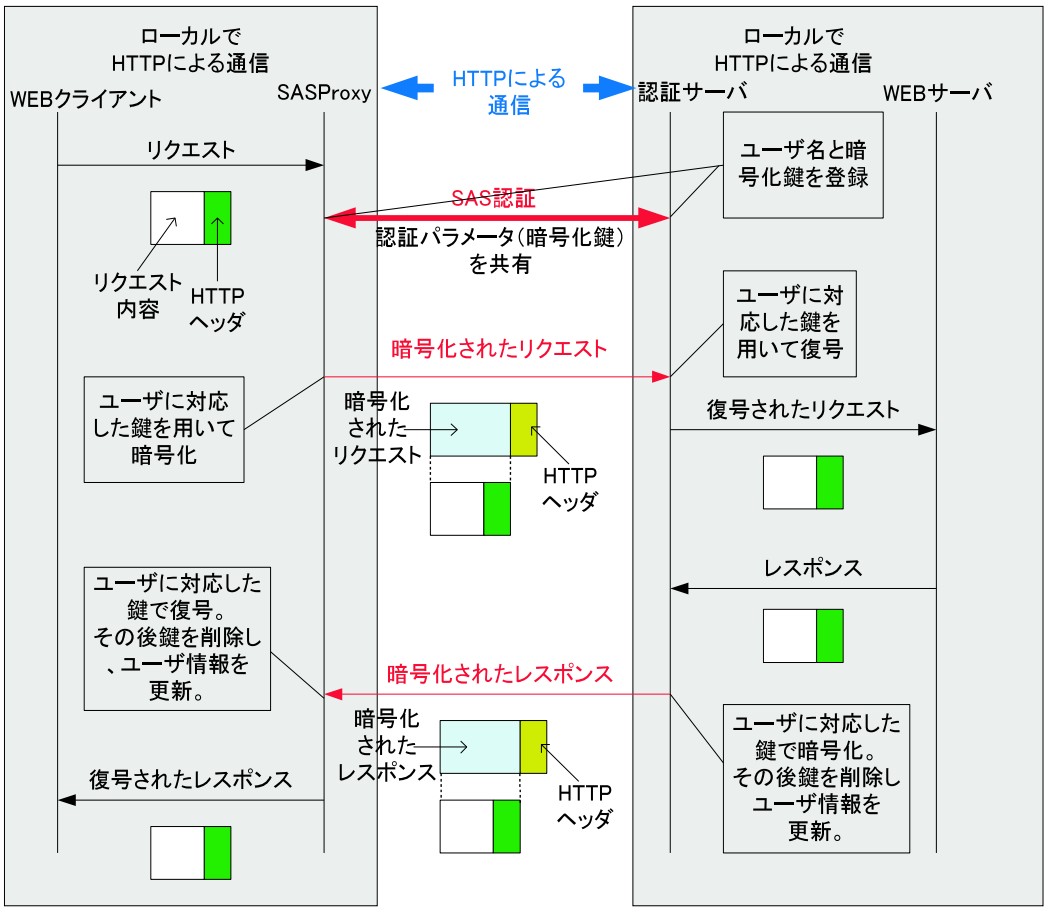

図 4.6　SASProxy の暗号処理方式

ザ属性を関連付けて，実際の氏名を表示させることができるものがあるが [19]，グループウェアベースとなっており，既存のネットワークにマージすることは難しい．そこで，現在運用されているネットワークにアドオンする形で実装でき，Web ブラウザを用い，ネットワーク上のどこの端末からでも容易にアクセスできて，簡単な操作で必要な情報が得られるシステムが必要となる．実験協力校の情報担当の先生からのアドバイスも受け，モニタリングの必要な情報としてリストアップしたものは，次のような項目である．

- 現在のネットワークの利用者情報と利用端末
- 今までの児童・生徒のネットワーク利用履歴
- メール利用状況（送信履歴及び受信履歴）
- ホームページの閲覧履歴

モニタリングシステム構築に関しては，各種情報を Web ブラウザで表示できることが前提となる．しかし，Linux システムのコマンドで得られる情報やログファイルを一覧できるだけでは意味がない．一般的にサーバのログファイルは英語である．詳細に報告されていることでログファイルが膨大になる傾向があり，Linux システムの知識がないと見たい情報を見逃してしまう恐れがあるからである．そこで，児童名簿や，端末の情報をデータベース

表 4.2　モニタリングシステムの必要条件

Web ブラウザで閲覧できること
日本語で表示できること
アカウント名ではなく，児童名で表示できること
使用している端末の設置場所がわかること
必要とされる最小の情報しか表示しないこと

に登録しておき，ログインしたユーザアカウント情報と端末名や IP アドレスによりデータベースに問い合わせをし，個人名や，マシンの配置場所を特定できるようにすれば，学級担任や情報担当教職員でも見やすいものになる．実装の際のプラットフォームとしては，端末側の処理の軽減と今後の拡張性とネットワークとの親和性を考慮して，JAVA Servlet と JSP で構築した．図 4.7 に概要を示す．データベースシステムとの連携については次項で詳しく述べる．

4.5.2　データベースシステムとの連携

管理コマンドの出力やログを参照する際に，前もって児童・生徒名簿データベースと端末データベースを作っておき，それらを参照することで，より見やすい出力とすることを目指した．データベースシステムとしては，PostgreSQL を採用した．

データベースシステムの操作は，psql コマンドを直接入力する必要がないように，Web ブラウザから操作可能なようにしている．

アカウント名と，ドメイン名を登録すれば，メールアドレスは自動で登録されるように

4.5　Web Based 校内ネットワークモニタリングシステム

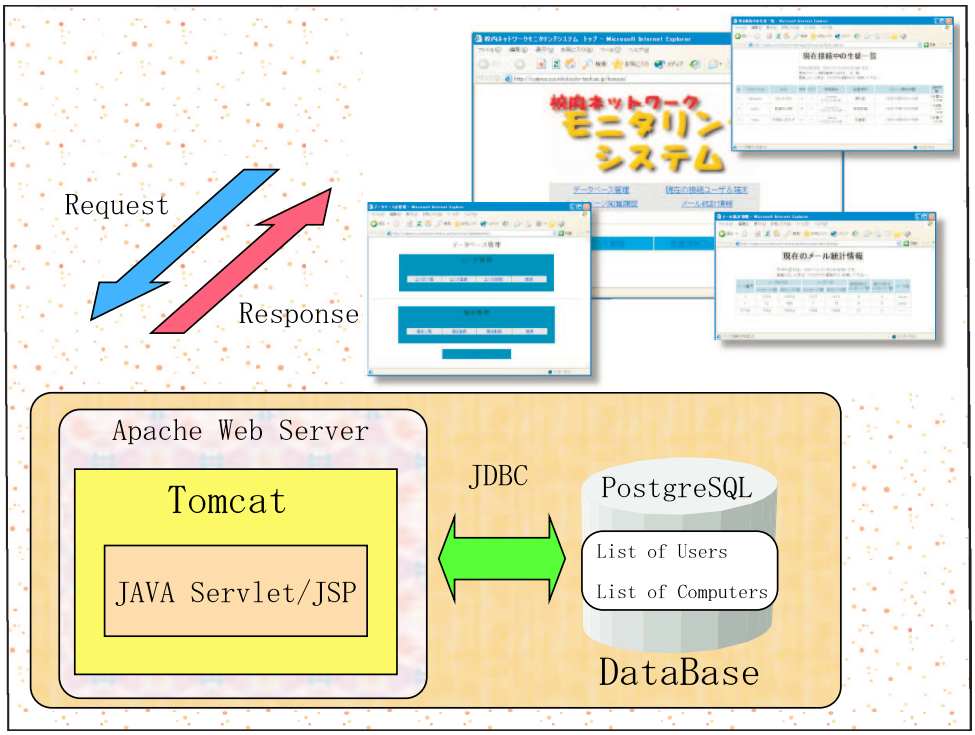

図 4.7　モニタリングシステムの概要

なっている．EXCEL などで児童・生徒名簿を作成している場合には，保存形式を変更すればそのまま読み込めるので，改めて入力する必要はない．ユーザアカウント情報の登録画面と，登録結果を図 4.8, 図 4.9 に示す．

図 4.8　データベースへの登録画面

データベースシステムとの連携の例を smbstatus コマンドの出力を例に取りながら説明する．通常のシステムで，smbstatus コマンド出力情報を得るためには，次のような手順が

4.5　Web Based 校内ネットワークモニタリングシステム

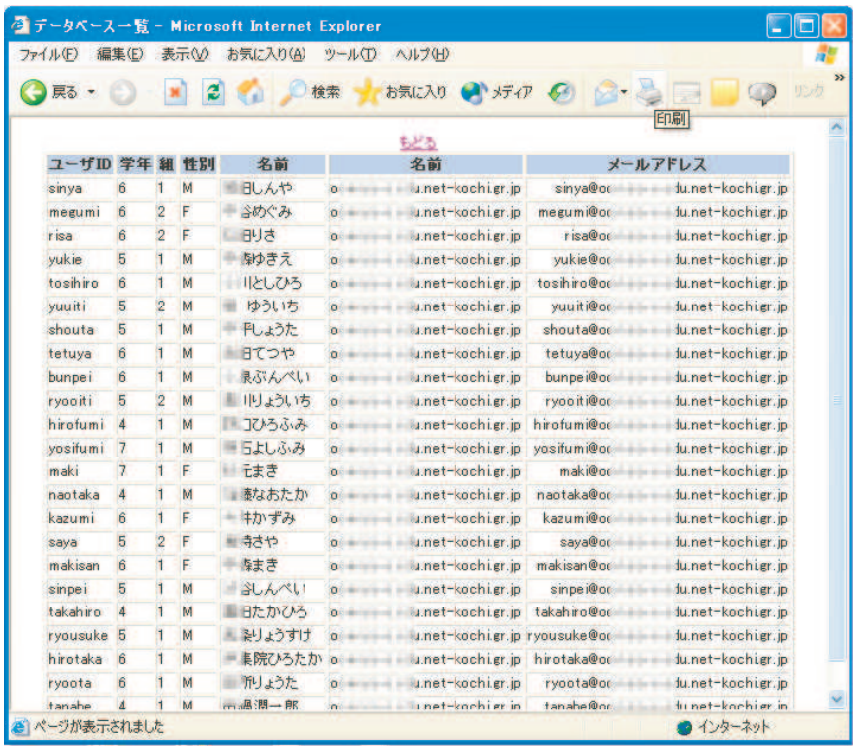

図 4.9　ユーザ一覧の画面

必要となる．

1. 管理者アカウントでログインする．
2. 端末で telnet を起動する．
3. ホスト名を入れる．
4. ID とパスワードを入力する．
5. smbstatus のコマンドを入力する．
6. 表示

実際に表示された出力は次のようなものである (図 4.10)．telnet でのログインは一般的ではない上に，キーボードからのコマンド入力が必要であるので，日常的に行う操作としては適していないことは明らかである．ログインしている端末が少ない場合は，ユーザアカウントから個人名を特定できるが，端末の数が多くなると即座に把握できない．端末名と IP アドレスだけではどこの端末からログインしているかわからない．

4.5 Web Based 校内ネットワークモニタリングシステム

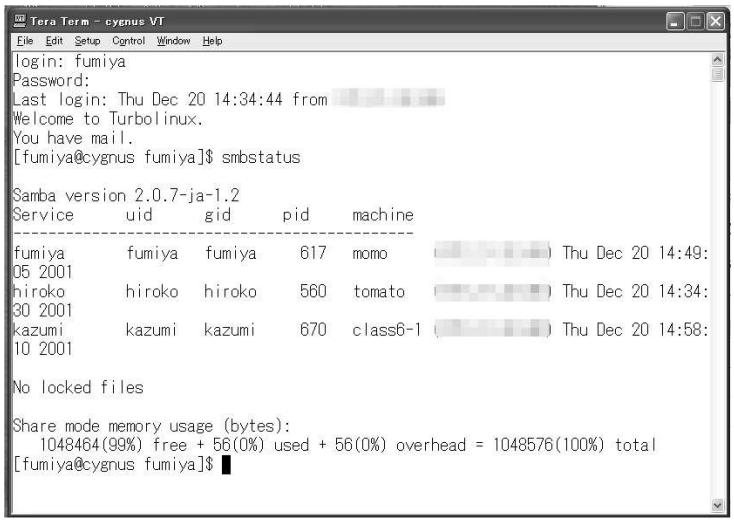

図 4.10　コンソールでの表示の例

そこで，smbstatus コマンドの出力結果をデータベースと照合させることにより，より視認性のよい出力とした．また，結果を JSP で受け取ることにより，Web ブラウザへの出力を可能とした．

この評価用システムでの，実際のモニタへの出力結果は図 4.11 のようになる．

図 4.11　モニタリングシステムによる表示例

4.5.3　メールログの監視

校内にメールサーバを設置し，個人アカウントでログインすれば，そのままメールが使える環境の構築が可能となったが，実際に運用していく上では，子どもたちのメールの使用状況をどのように見守っていくのかが課題である．一番確実な方法は，ロギングである．しかし，学級担任が sendmail のログを見て，その中から問題点を見つけ，児童・生徒の利用状況を把握することは困難である．

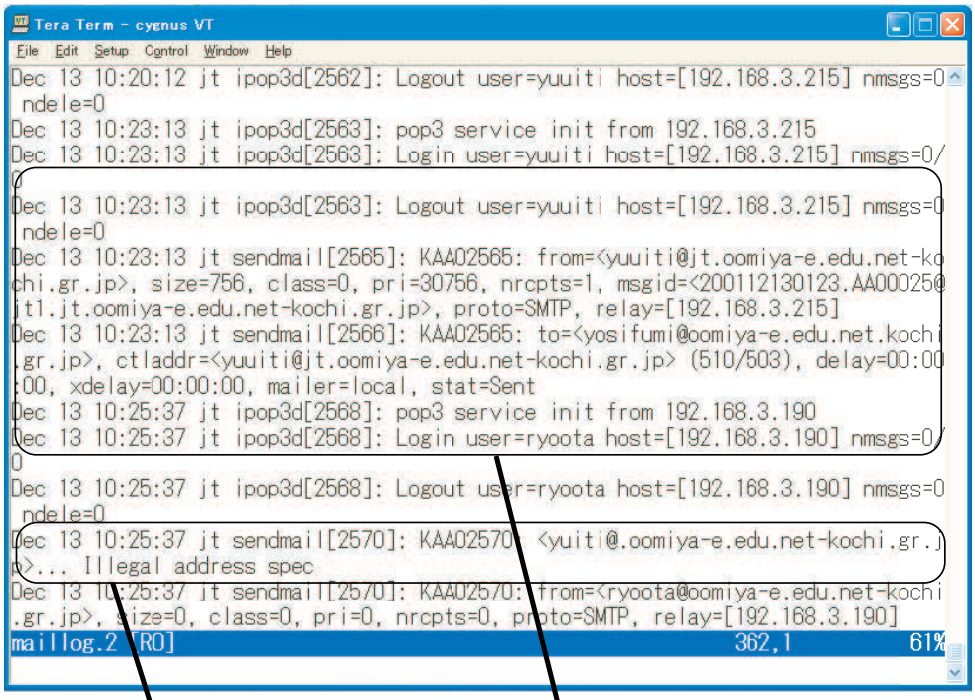

図 4.12　送信履歴のログの例

そこで，sendmail のログから必要な部分を抽出するフィルタプログラムで処理したあと，加工・整形したログファイルをデータベースに登録するシステムを考案した．特徴を以下に述べる．

- メールの送受信履歴は，ある程度の期間保存する必要があり，データベースに登録しておくことで，確実な保存が可能となる．

- データベース化することで，様々な角度から閲覧・検索が可能となる．
- 児童・生徒名簿データベースとリンクすることで，メールアドレスから，名前を調べたり表示させることも可能となる．
- データベースへの登録量を軽減するために，前処理として必要な部分のみ抽出し，集計処理も行うようにした．

sendmail ログの処理手順は図 4.13 のようになっている．

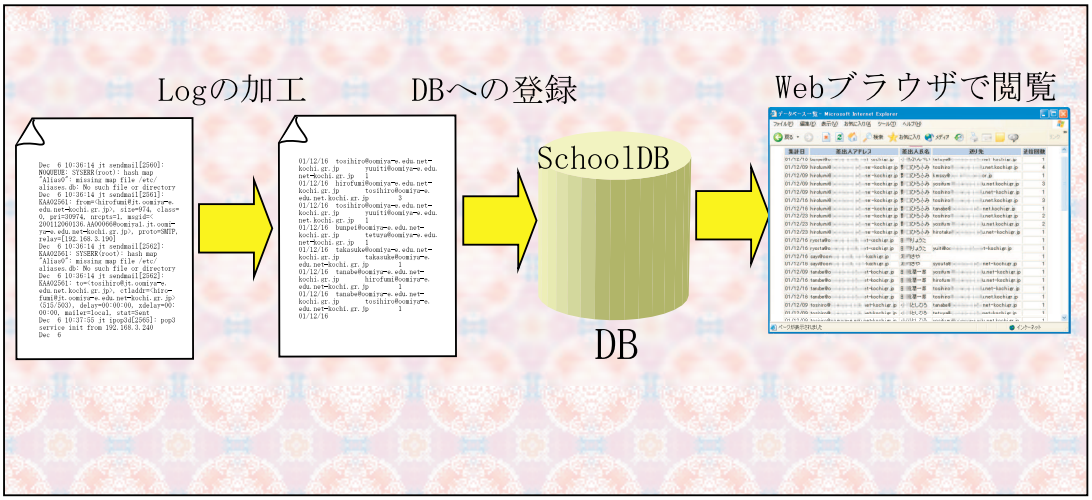

図 4.13　評価システムによる sendmail ログの処理の流れ

sendmail のログ処理は，日曜日の深夜に自動に行うように設定をしたので，管理者は Web ブラウザで管理画面にアクセスするだけでよく，容易に送受信のログのチェックができると思われる．データベースに登録してあるので，ユーザアカウントで絞り込んだり，日付で絞り込んだりと様々な観点から閲覧可能である．ユーザアカウントによる表示は，図 4.14 のようになる．

4.5.4　有害情報のフィルタリング

児童・生徒への有害情報のフィルタリングは個人情報の保護の問題と併せて，教育でインタネットを活用していくうえで，解決しなければならない大きな問題である．フィルタリングソフトは，市販されている物の他に，様々な実践的な研究が行われており [20]，その必要

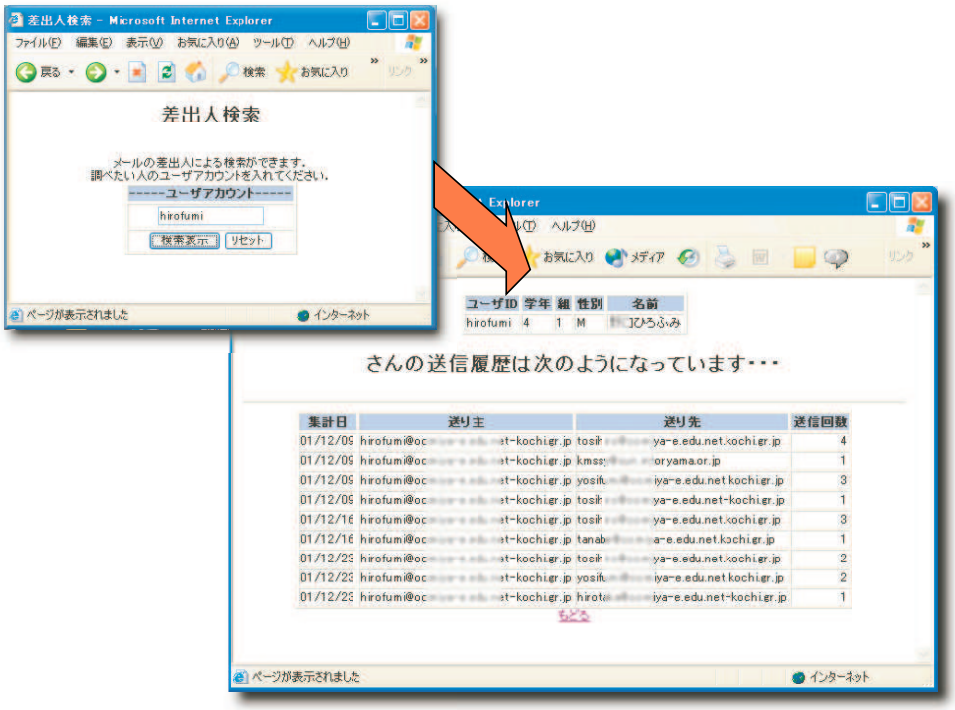

図 4.14　ユーザアカウントで検索した場合の表示

性を裏付けている．技術的な面での有害情報のへの規制として，次の３つの段階で行うことが可能である．

- 情報発信者側での規制

  アクセスする利用者の年齢を特定することで，対象年齢者未満の情報発信を制限する方式であるが，アクセスする者の年齢を特定できる有効な方策はないので，発信者側のモラルにかかっていると言える．

- 受信者側での規制

  受信するクライアント側で有害情報をフィルタリングする方法で，一般にフィルタリングソフトを使うことになる．また，Internet Explorer や Netscape Navigator などの Web ブラウザにも規制する機能が付加されているが，使用者が設定を変更してしまえばフィルタリングの効果はなくなる．

- 情報中継経路中での規制

主にプロキシサーバで様々なアクセス制限をかける方法である．アクセス制限をかけすぎると，サーバに繋がっている多数の端末が必要なコンテンツにアクセスできない事になってしまう恐れもあり，一般に強固なアクセス制限はかけられない．

校内ネットワークという視点から，受信者側での規制，情報中継経路中の規制に絞って考える．受信者側での規制は，受信する端末にフィルタリングソフトウェアを導入することになる．端末毎のインストールや設定が必要であり，導入コストもかかる．そこで，情報中継経路でのフィルタリングについて考察した．

一般にとられているフィルタリングの手法として，２つの方式がある．一つは，アクセスを制御する URL の一覧をデータベース化し，一覧の中の URL には，アクセスを制限する方法であり，もう一つは，利用者がアクセスしたコンテンツの内容をチェックし，不適切な単語や語句が含まれているコンテンツにはアクセスを制限するという方式である．URL チェック方式は，登録された URL へのアクセスを確実に回避できるが，適切なページへのアクセスができなくなるという報告もある [21].

一方，コンテンツの内容をチェックする方法では，あらかじめ単語を登録しておくことにより，アクセスのあったコンテンツの内容をチェックするので，更新や登録の作業は必要がない．しかし，登録された単語が適切でなかったり，自動判別アルゴリズムの不十分さから制限する必要のないページまでアクセス制限をしてしまうという問題がある．また，アクセスしたページ毎にコンテンツをチェックするために，処理スピードの面からも不利である．

そして，上記の二つの方法に共通する大きな問題がある．それは「誰がフィルタリングポリシを決めるか」ということである．本論文では，学校ネットワークのマネージメントポリシでも明らかにしたように，校内ネットワークを見守っていくのは学校の先生であり，学級担任である．すべての有害情報を児童・生徒から遮断することは事実上不可能である．そこで，最も教育現場で現実的に起こりえる場面として，児童・生徒が偶然そのようなページを見つけ，その情報を共有しあっているという事実があった場合を想定してみた．

その場合，学級担任がそのページを実際に確認したうえで，アクセス制限をかけることが必要であるか判断し，必要であればフィルタリング処理を行うことが望ましい．

そこで，学級担任がユーザである児童・生徒のアクセス履歴をチェックし，自らの判断で簡単にフィルタリングのできる環境が必要となる．そこで，使いやすさ，パフォーマンス，実装面のシンプルさを考慮して，次のような仕様で有害情報のフィルタリングを実装することにした．

- フィルタリングは，校内ネットワークのプロキシサーバで行う．
- 処理速度の面と，実装の容易さを考慮し，URL フィルタリング方式とする．
- フィルタリングは学校の情報担当教職員または，学級担任が行うものとする．
- Web ブラウザで操作できるインタフェースにする．
- フィルタリングの基礎データとして，児童・生徒の URL のアクセス履歴を取得できるようにする．

プロキシサーバとして，squid[*4]を導入する．すべての端末をプロキシ経由にすれば，児童・生徒がアクセスした URL 情報は，squid のログに残る．そのログを加工し，集計すればどのようなホームページを見ているかという詳細な情報が得られる．評価用システムでは，squid.log の集計・加工ツールとして webalizer[22] を使った．実際の小学校で運用し集計したものを図 4.15 に示す．

実際の学校現場での有害情報のフィルタリングプロセスは，次のような流れとなる．

1. webalizer での集計処理データから，URL 履歴情報を得る．(図 4.16)
2. アクセス履歴の多いものから順に，チェックをする．
3. フィルタリング処理が必要な URL が見つかったら，フィルタリングウィンドに URL をコピー・ペーストする．(図 4.17)

[*4] FTP や gopher，HTTP データオブジェクトに対応した，web クライアントの ための高性能な代理キャッシュサーバ

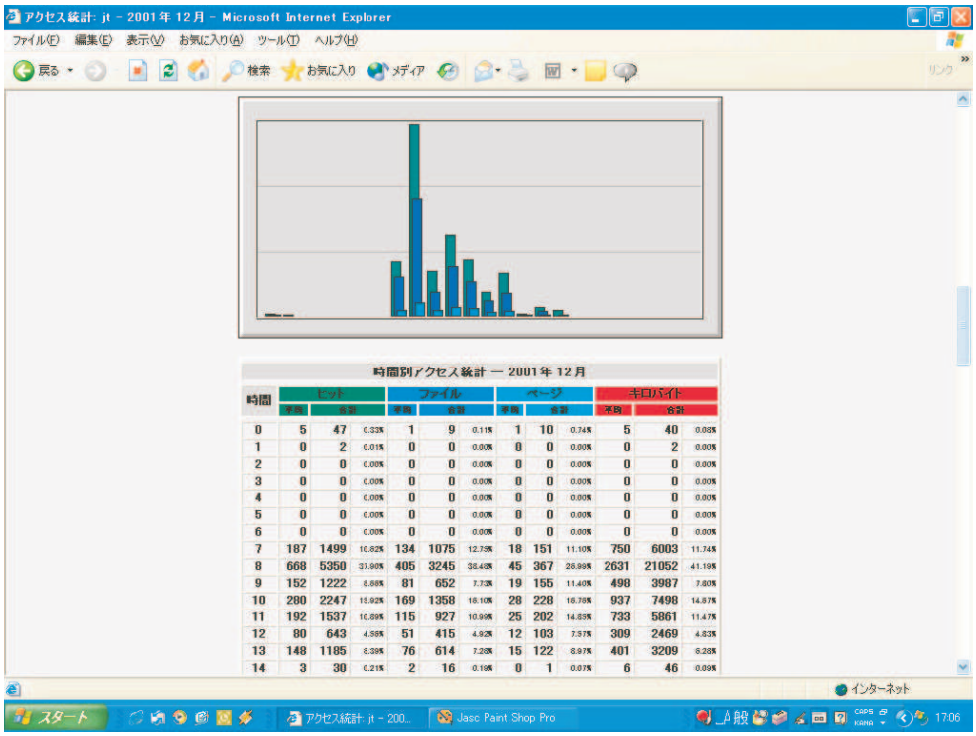

図 4.15　webalizer の出力例

4. 送信ボタンをクリックすると，squid のアクセス拒否リストに URL が登録される．(図 4.18)
5. squid を再起動すれば，登録した URL にはアクセスができなくなる．(図 4.19)

4.5　Web Based 校内ネットワークモニタリングシステム

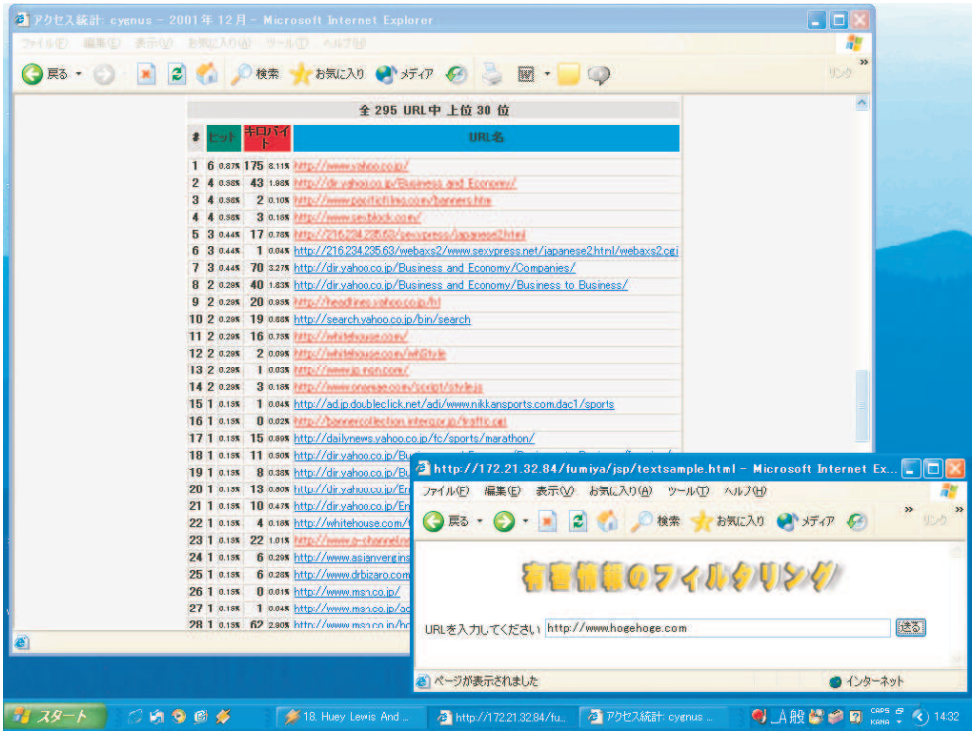

図 4.16　URL 閲覧履歴をチェックする

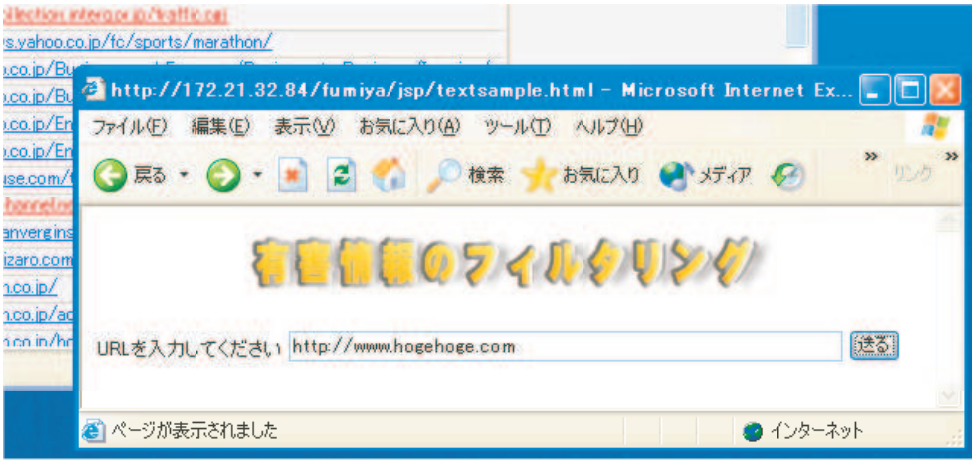

図 4.17　フィルタリングする URL の入力

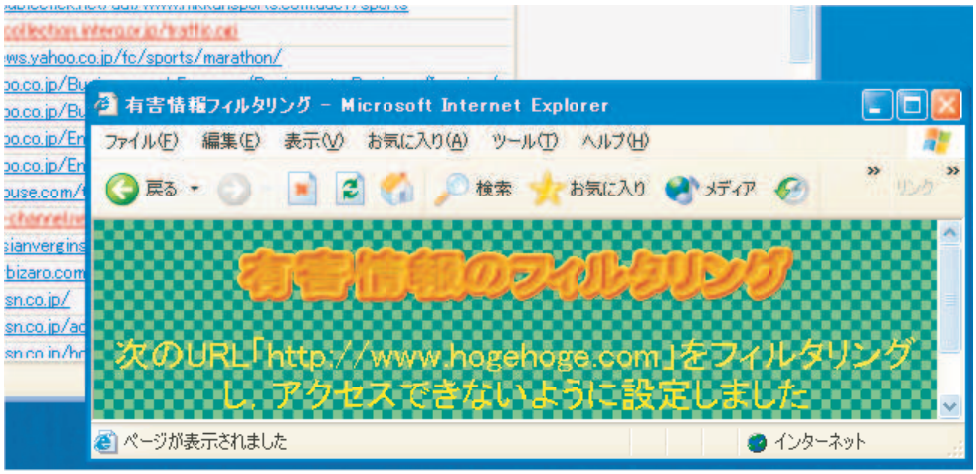

図 4.18　フィルタリング処理

図 4.19　アクセス制限のかかった URL へ接続した例

第 5 章

評　価

5.1　個人環境の確立とディスク認証システムの評価

構築したネットワークシステムを，香北町立大宮小学校の校内ネットワークに付加する形で実験を行った．大宮小学校は，校内 LAN が整備されており，ファイル共有用のサーバが設置されているが，個人環境の構築はできていない．

実験用のサーバ 1 台と，実験用の端末を特別教室に 2 台，図書室に 1 台設置し，休み時間や放課後などに自由に使ってもらう形をとった．

被験者はパソコンクラブを中心に希望者を募り，小学校 4 年生から 6 年生の 22 名の児童にメールアカウントを発行し，ログイン用のディスクを作成し，3 週間実験を行った．

実験後，アンケートとログの解析により評価を行った．アンケートの回答数は 15 名である．複数回答によるものだが，児童が自分の個人環境が持てることのよさを実感できたといえる．

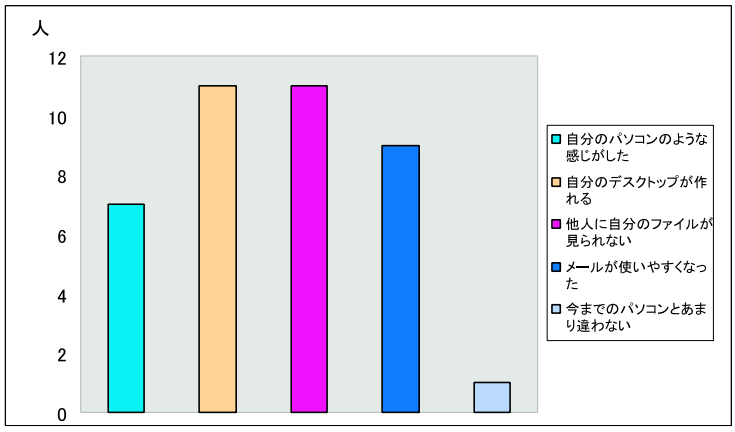

図 5.1　実験用ネットワークの良かったところ

また，実験用ネットワークを管理側の先生からも自由記述で評価をしてもらった．

- 今までのネットワーク（インターネット接続とファイルサーバのみ）では，メールの設定を端末毎にしなけらばならず，児童一人ひとりにアカウントを持たせることは困難であった．今度のネットワークなら端末１台で設定すれば，学校内のどこの端末からでも個人アカウントでメールができるようになるので，設定も簡単であるし，全校児童にメールアカウントを持たせることもできそうである．
- 児童の作ったファイルをサーバ内に保存できるので，セキュリティの面でも，プライバシの面でも安全である．デスクトップもすっきりした．
- 児童ごとにデスクトップをカスタマイズできるので，ログインしたときに，自分のコンピュータのような感じがしたのではないだろうか．どこの端末から入っても同じデスクトップが再現できるので驚いた．
- 教師のアカウントで入った場合はネットワークの設定が変更可能であり，児童の共有フォルダと教師の共有フォルダにアクセスできるが，児童のアカウントで入った場合はネットワークのプロパティにアクセスできないようになっており，共有フォルダも児童用しか見えないようになっている．安心して使わせることができそうである．
- アカウントの追加や変更は行うことができたが，ネットワークのことを詳しく知らないので，何らかの障害が起こったときに対処できるか不安である．

次にディスク認証システムの評価を行った．小学校６年生の児童５人に使ってもらい，従来のキーボードによるログイン認証方式との認証時間の比較実験を行った．

キーボードによる認証とフロッピによる認証による，ログイン終了までの時間を比較したものが表 5.1 である．キーボードによるログインは，時間のバラつきがあるのに対して，ディスクログインは，認証にかかる時間が一定で，早いこともわかる．また，キーボードによる入力で時間のかかった原因として，パスワードの入力ミスがあげられる．また，認証方式の比較のために，３週間の実験のうち，最初の２週間をディスク認証システムを用い，あとの１週間を通常のログイン方法で行ってもらった．　ログを調査してみると，最初の２週

図 5.2　ディスクログインの様子

表 5.1　ディスクログインとの比較

	キーボードよりの入力 (単位 秒)					
	被験者 A	被験者 B	被験者 C	被験者 D	被験者 E	ディスク
1	10.3	13.8	23.6	15.8	18.6	10.5
2	10.6	12.6	25.3	14.9	19.3	11.4
3	15.8	13.6	22.8	13.9	17.9	12.4
4	43	13.5	14.3	20.6	15.4	10.2
5	12.9	12.5	14.9	21.8	17.6	11.5
平均	18.52	13.2	20.18	17.4	17.76	11.2

間の一日あたりの平均ログイン数はそれぞれ 36.25 回，30.33 回となっているのに対して，第 3 週のキーボードからのログインによる一日あたりの平均ログイン数は 13.8 回と半分以下になっており，入力ミスによるログイン不可の総数が 31 回となっている (表 5.2)．2 人の児童は，何度かログインに失敗し，その後，一度もネットワークに入っていない．日常的にログインしている児童は ID やパスワードを覚えているが，時々しか使わない児童は忘れてしまう．担当の先生にも，何度かパスワードの問い合わせがあったという．

表 5.2　1 日の平均ログイン回数

	ログイン方式	1 日平均ログイン回数
第 1 週	ディスクログイン	36.25
第 2 週	ディスクログイン	30.33
第 3 週	キーボードによるログイン	13.8

実験終了後の，アンケート調査によると，15 名中 13 名の児童がディスクログインを支持している．ディスクログインを支持する理由としては,「パスワードを覚える必要がない」「ディスクを入れるだけなので簡単」などがあった．一方，キーボードからのログインを支持する理由としては「慣れているから」「むずかしいけど，やっているとなれると思う」というのがあった．小学校の高学年を対象とした実験で上記のような結果が得られたということは，小・中学校で使える有効なログイン方式であると言える．

管理する側の先生の意見として,「ディスクログインは，児童にとっては使いやすく，教師側もある一定の制限のもとに自由に使わせることができるのでよい」という意見をいただいた．ログイン用のディスクも一括して作成できるため，負担も大きくはなかったそうである．

また，実験校に隣接した中学校から「個人アカウントを発行し，全員にメールアドレスを持たせたいが，自由に使えることで管理が行き届かなくなるという不安があった．しかし，ディスクログインなら生徒の利用の制限ができそうなので，関心がある」という意見を聞かせていただいたことを付け加えておく．

ID やパスワードを覚えなくても，プライバシが守られセキュリティが確保され，児童・生徒のアカウントが管理しやすいディスクログインシステムは，校内ネットワークにおいて有効な認証方式であると言える．

5.2　校内ネットワークモニタリングシステムの評価

本評価の目的は，試作システムの有用性や操作の容易さを現職の教職員の立場から明らかにすることである．大宮小学校の先生方を中心に，10 名の現職の教職員がモニタリングシステムの評価を行った．初めに，従来のモニタリング（ロギング）との比較のため，TELNET でサーバにログインし，UNIX コマンドによる smbstatus の操作を行って現在のログイン一覧を見てもらった．その後，Web ブラウザで本モニタリングシステムを用い，自由に操作した後，その必要性と使用感を 5 段階で評価してもらった．その結果を表 5.3 に示す．

結果より，次のことが明らかになった．

- 調査者全員が，校内ネットワークでのモニタリングの必要性を感じている．
- 校内ネットワークの管理経験がある先生ほど，より必要性を感じている．
- 日常的にコンピュータを使わない先生は，必要性は感じていながらも，操作にはあまり自信がなく，進んで使うことには消極的である．

表 5.3　モニタリングシステムの有用度と操作性の評価

	自分でも使えると思う	モニタリングは必要だと思う	使ってみようと思う
全体 (10 名)	4.4	4.5	4.3
情報担当経験者 (3 名)	5	5	5
情報担当経験なし (7 名)	4.1	4.3	4
コンピュータを日常的に使わない (3 名)	3.5	4	3.5

感想の主なものは次のようなものであった．

- ブラウザでホームページを見る感覚で操作ができるため，迷うことなく操作できた．
- 表示も日本語なのでわかりやすく，内容がつかみやすかった．

- メールの配送履歴については，アカウントを持たせる上で，大切な情報であると思う．
- どこの端末からでも閲覧できるので，便利である．
- これからコンピュータを使った教育を行っていく上で，何らかのモニタリングシステムは必要である．
- 早くこのようなシステムを実現してほしい．コンピュータに興味を持つ児童が多いが，授業でしか使えないので，児童の興味が薄れていく．いつでも自由に使えるようにしてやるためにも必要．

同時にデータベースへのユーザの登録も操作してもらった．同じくブラウザインタフェースなので，簡単に登録ができた. エクセルで学級名簿を作成している場合は，保存形式を変えるだけでそのままデータベースに読み込むことができるので，登録の手間は大幅に軽減できる．

情報担当の経験のない先生にも操作してもらったが，操作自体はできるのだが，表示される情報が何であるのか説明をしないと理解できなかった．実際の運用では，操作マニュアルとともに，表示される情報がどういったもので，何のために閲覧するのかを記述しておく必要を感じた．

有害情報のフィルタリングについても，フィルタリングソフトを導入したことがあったが，設定が難しく，必要なコンテンツにアクセスできなくなり，使用を取りやめた経緯があるという．実際の児童・生徒のアクセス履歴を見て，必要な時に簡単にフィルタリングができるので，有効な方法であるという意見をいただいた．

5.3　マルチメディア教材配信実験

これまで，教育の分野において，ネットワークでマルチメディアコンテンツを配信するという試みは少なく，教育効果を持ったマルチメディアコンテンツは，どのくらいの容量になるかよくわからないという実態があった．

そこで，今回の実験で使用するコンテンツは，教育効果という点から品質を分析，これか

ら流通するであろう教育コンテンツの容量を検討した．例えば，1 時間の授業でコンテンツを利用することを考えた場合，品質の悪い動画を使用すると，子供たちの集中力が欠けたり，興味をなくすことが考えられる．授業で利用するのに十分な品質を維持するため，今回使用するコンテンツの作成には，情報教育の実践経験のある学校の先生に協力していただき，次のような条件で作成した．

- 児童の集中力を考慮し，各動画は 1 分前後で閲覧可能
- 児童の興味を引き出すため，動画は最低 320 × 240 の解像度を確保
- 先生の説明時間，発表時間等を考慮しコンテンツ全体を 20 〜30 分で閲覧可能に構成
- 動画の圧縮率は細部まで閲覧できる様に制作者 (教諭) が調整

制作したコンテンツは小学校三年生社会科の農業に関するコンテンツであり，メロン栽培をテーマとしている．コンテンツは，総再生時間 18 分の 16 動画中心で構成されており，動画を MPEG-1 で構成した場合は 158MB ，RealVideo で構成した場合は 84.2MB の容量となる．図 5.3 に制作したコンテンツの概観図を示す．以下本コンテンツを流通の単位コンテンツ例として実験を実施する．

図 5.3　作成したマルチメディアコンテンツ

実証フィールドとしては，高知学校インタネットシステムの簡易モデルを構築し行っ

た．学校インタネットシステムは中央センタを中心として各地の地域センタが接続しており，各地域センタが学校に接続した階層構造となっている．各地域は CATV 等を利用した 10Mbps の高速回線をアクセス網としており，各地域センタと中央センタは 1.5Mbps の専用線で接続されている．今回想定している実験は，コンテンツを中央センタへ配置した場合の 1.5Mbps の帯域と，地域センタへ配置した場合の 10Mbps でのコンテンツ閲覧における品質調査を目的としている．高知学校インタネットシステムのモデルを図 5.4 に示す.

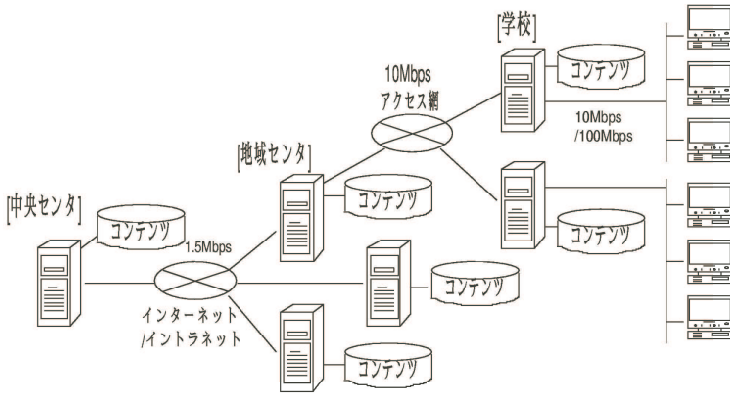

図 5.4　高知学校インタネットシステム

コンテンツの品質評価については，都丸 [5] による「画像の主観的評価尺度」によった.

表 5.4　画像の主観的評価尺度

評点	品質尺度	説明
5	非常によい	劣化が全く認められない
4	よい	劣化が認められるが気にならない
3	まあよい	劣化がわずかに気になる
2	悪い	劣化が気になる
1	非常に悪い	劣化が非常に気になる

MPEG-1 コンテンツ，ストリーム形式コンテンツを中央センタ，地域センタに配置した場合の学校からの品質評価を行った.

予想された事であるが，中央センタ (1.5Mbps) に配置した場合は，１台のみ閲覧可能で

あった．地域センタへ配置した場合は，高品質で３台まで閲覧可能であったが，４台以上になるとフリーズを起こす結果となった．実験を行った学校の校内 LAN が 10BASE-T であったため，10Mbps の帯域を活かせない結果となった．

表 5.5　MPEG1 コンテンツ (1.5Mbps)

同時閲覧台数	1 台	3 台	4 台	5 台
品質評点	5	閲覧不可	閲覧不可	閲覧不可

表 5.6　MPEG1 コンテンツ (10Mbps)

同時閲覧台数	1 台	3 台	4 台	5 台
品質評点	5	5	閲覧不可	閲覧不可

次にストリーム形式について，実験を行った．

表 5.7　ストリーム型コンテンツ (1.5Mbps)

	同時閲覧台数	1 台	5 台	10 台	15 台	20 台
動画帯域幅（台）	主観的評価	5	4〜5	3〜4	1〜2	不可
	220kbps	1	0	0	3	-
	150kbps	0	2	1	0	-
	100kbps	0	3	2	0	-
	100kbps 未満	0	0	7	12	-

ストリーム形式は，中央センタ（1.5Mbps）に配置した場合でも，10 台までなら，教育コンテンツとしての品質を保てることがわかった．地域センタ (10Mbps) に配置した場合には，２０台同時に閲覧してもある程度の品質を保った動画を再生することができた．コンテンツ配置用のサーバが外部にある場合でも，ストリーム形式では地域センタにコンテンツを配置してもある程度の品質が得られた．

表 5.8　ストリーム型コンテンツ (10Mbps)

	同時閲覧台数	1 台	5 台	10 台	15 台	20 台
	主観的評価	5	5	5	4〜5	4〜5
動画帯域幅（台）	220kbps	1	5	10	14	15
	150kbps	0	0	0	1	0
	100kbps	0	0	0	0	0
	100kbps 未満	0	0	0	0	0

実験結果からも明らかなように，教育用マルチメディアコンテンツを閲覧するためには，1.5Mbps では，明らかに帯域不足である．ストリーム形式の動画が 20 台での受信を可能とするためには 10Mbps は必要である．MPEG-1 形式では，学校サーバに置いても学習に必要な台数での閲覧が不可能だった．校内にコンテンツ配置用のサーバを置き，校内 LAN を 100Mbps にすれば MPEG-1 コンテンツを 20 クライアントで実行することも可能であるが，管理等の作業が発生するために，コンテンツは地域センタに事前配信し，学校ではキャッシュサーバ等を利用することが望ましい．

5.4　キャッシュサーバ設置によるトラヒック改善

学校は，複数の端末から同じコンテンツにアクセスする確立が高いことからキャッシングやミラーリングの手法が効果的である [12]．キャッシュサーバの性能目標や，設定項目を具体化するために，次のような条件を設定した．

- 授業時間内に生徒 1 人が平均的にブラウズする Web ページ数を 30 ページとする．
- 1 ページあたりのデータ量を 100KByte とする．
- 動画の利用が増えることから，1 時間に一つの動画ファイルを閲覧するとする．
- 1 クラス 40 人で，1 日 6 時間の授業で使用されるものとする．
- カリキュラムへの考慮から 2 週間分のキャッシングを実現する．

MPEG1 形式のクオリティの高い動画データは，1 分間のプレビュー時間のものが 10MByte であるとすると，２週間分（10 日間）で必要な記憶容量は 32.2GByte となった．以上の予測をもとに，構築したキャッシュサーバの詳細と主な設定項目を表 5.9 に示す.

表 5.9　キャッシュサーバのスペックと主な設定

CPU	Celeron 1.0GHz
Memory	640MB
HardDisk	40GB
OS	Linux　version:2.2.18-2
Software	squid 2.3.STABLE4-1
cache_mem	128 MB
maximum_object_size	20480 KB
cache_dir ufs	/var/spool/squid　2000 16 256
cache_peer	****.****.****.**** parent **** 0 no-query

比較的大きな動画ファイルもキャッシング可能なようにオブジェクトサイズは 20MB とした．Squid の場合，メモリ上にキャッシングすると大幅なアクセス速度の改善が望まれることから [23]，キャッシュメモリを増やしている.

校内ネットワークにキャッシュサーバを設置し，Web 利用時のトラヒック改善の調査を行った．実験用ネットワークの運用により採取したホームページのアクセス履歴から上位に入っているものを１０箇所選び，ランダムな順でリンク集を作成し，Web ページのロードが完了すると次のページに進み，１０箇所をすべて見終わった時間を端末毎に計測した.

実験結果は図 5.5 にあるように，コンテンツアクセス時間は約 $\frac{1}{2}$ となりトラヒックの改善につながった．また，パケットキャプチャリングによるスループットの比較でも，平均スループットは，114KB/秒 (キャッシュ無) から 224KB/秒 (キャッシュ有）へと改善され，キャッシュサーバの有効性が明らかとなっている (表 5.10)．また，上位ネットワークの HUB のデータの流れをキャプチャリングした結果を見ると (表 5.11)，受信パケット数，受信バイ

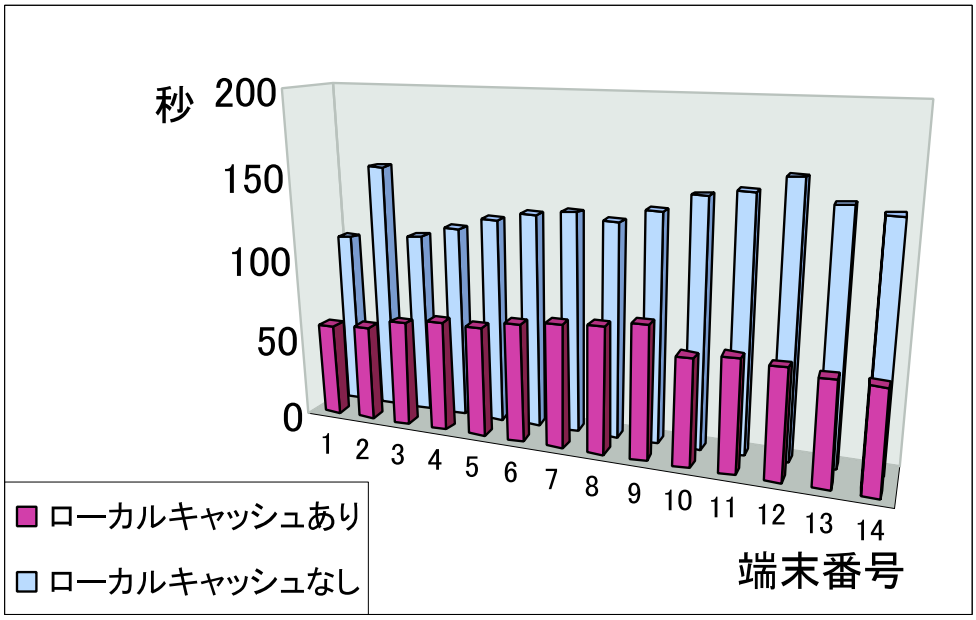

図 5.5　アクセス速度の調査結果

ト数ともに，少なくなっていることからもキャッシングが有効に機能していることが伺える．実験校の端末は，CPU クロックが 200MHz と比較的古いものであったが，サーバのメモリ上にキャッシングするため，高速にアクセスが可能となっている．

表 5.10　キャッシュサーバ有無によるスループットの比較

	キャッシュ無し	キャッシュ有効
全バイト数 (KB)	20,977	19,077
全パケット数	43,418	23,832
バイト数 (KB)/秒	114.6	224.4
パケット数/秒	237	280

キャッシュサーバの設置は，校内ネットワーク内のスループットを向上させるだけでなく，外部ネットワークへのトラヒック改善につながり，結果として所属する網ネットワーク全体のトラヒック改善にもつながる．同じ時間に同じコンテンツが同時にアクセスされることの多い，特徴あるトラヒック特性を持つ学校という環境において，有効であることが明らかと

表 5.11　上位ネットワークの HUB のデータの流れ

	キャッシュ無し	キャッシュ有効
受信パケット数	19,332	7,677
受信バイト数 (KB)	2,045	1,224

なった.

校内ネットワークに，比較的管理負担のかからないキャッシュサーバを設置すれば，ネットワーク全体のトラヒック改善につながり，限られた帯域の有効利用が可能となる．より細かな設定のチューニングにより，まだまだパフォーマンスの向上の余地もありそうである.

第 6 章

結　論

6.1　本研究の成果

本研究では以下のことを提案，実現，確認した．

- 校内ネットワークポリシの必要性について述べ，ネットワークポリシの提案を行った．
- ネットワークポリシに基づいた校内ネットワークモデルを提案した．
- ネットワークポリシに基づいて，現状の校内ネットワークの問題点を明らかにした．
- 発達段階，学習履歴の異なる児童・生徒でも容易に認証が行える，ディスクログインシステムを提案し, 実際の学校現場で評価を行い，有効な方法であることを確認した．
- 機器の購入や入れ替えが簡単にできない学校の環境下で，既存の機器を生かしながら，児童・生徒のセキュリティを守り，個人情報を保護するために，サーバ上に個人ディレクトリを持つ方法を提案し，実証実験を行った．
- 校内ネットワークの管理者を明らかにし，ネットワークを見守っていくために必要なモニタリングシステムを実装し，評価した結果，有効なシステムであることを確認した．
- 流通単位としてのマルチメディア教材を作成し，配信実験を行い，教育ネットワークに必要な帯域を明らかにした．
- 特殊なトラヒックを持つ校内ネットワークに有効なキャッシュサーバを設置し，実証実験を行い，有効性を確認した．

6.2　今後の課題と展望

校内ネットワークポリシを策定し，導入されている機器を生かしながら改善点を指摘し，その改善の施策を実際の学校現場で行ってきた．改善されなければならない問題点を置き去りにしたまま，学校への情報機器の導入は進んでいる．それらの機器をどのように使い，管理・運用していくかは，早急に成されなければならない議論である．

本研究で行ったネットワーク改善の手法は，実際の教育現場で運用実験を行い，評価したものであり，実運用に耐えることのできるものである．しかし，モニタリングシステムについては，インタフェイスの見直しや，基本的なデータベースの設計などについて，若干の手直しが必要であり，今後も改良を加えていきたい．

本研究が児童・生徒にとってセキュアで使いやすく，管理者である先生にとっても安心できる校内ネットワーク構築の参考となることを願っている．

謝辞

本研究の遂行および本論文に関して，多大なるご指導，適切なご助言をいただいた高知工科大学情報システム工学科清水明宏教授に心よりお礼申し上げます.

本論文に関して，適切なご助言を頂戴した高知工科大学情報システム工学科島村和典教授，高知工科大学情報システム工学科岩田誠教授に心から感謝致します.

本論文および本研究において，数々の有益なご助言，ご指導をいただいた高知工科大学情報システム工学科妻鳥貴彦助手に心から感謝致します.

本研究において，ご助言を下された高知工科大学情報通信ネットワークコース岡田実氏，三菱電機株式会社の横里純一氏，NTT アドバンステクノロジ株式会社の真島大介氏，本実験にご協力下さった香美郡香北町立大宮小学校の児童の皆さん，先生方に心からお礼申し上げます．最後に，ディスクログインシステムの共同制作者である難波二郎氏に感謝いたします.

参考文献

[1] http://www.monbu.go.jp/news/00000307/

[2] http://www.www.kantei.go.jp/jp/mille/index.html

[3] 関口敦二 他, ”ポリシィ制御型ネットワーク”, 2000 年電子情報通信学会総合大会, SB-5-4, pp.665-666, 2000

[4] http://www.atmarkit.co.jp/fengineer/rensai/edu01/edu01.html

[5] 都丸敬介, ネットワークポリシー設計, ソフト・リサーチ・センター,2000.6

[6] 木下広揚　他, ”セキュリティと利便性を考慮したシステム構築の一考察”, 信学技法, Vol.100, No.67, pp.1-6,2000.05

[7] http://www.microsoft.com/japan/BackOffice/BOT/UserAuthentic/default.asp

[8] http://shigi.cc.osaka-kyoiku.ac.jp/educ/

[9] 大谷　尚,”電子メールが利用者の情意的・認知的な態度におよぼす影響の検討-感情的なメールをうむメディアとしての電子メールの特性の分析-”, 日本科学教育学会　年会論文集 22,pp.61-62,1988

[10] http://www.shikoku-bt.go.jp/news/2001press/200111/2001112004.htm

[11] 高知新聞夕刊 平成 13 年 12 月 18 日 p.6

[12] 横山浩之　他,”教育用インターネットに適したキャッシング手法およびミラーリング手法に関する一考察”, 信学技報, Vol.100, pp1-6, 2000.04

[13] 長谷川勝一，”小規模校における電子メール環境の構築　”，美作女子大学短期大学部紀要４２号

[14] http://www.sun.co.jp/software/consumer-embedded/card/

[15] 上岡　隆, 清水明宏,”ワンタイムパスワード認証方式 SAS の安全性に関する検討”, 信学技報 Vol.101 No.435,pp.53-58,2001.11.19

[16] 真島大介，羽田友義, 田鍋潤一郎, 清水明宏, ”SAS 暗号通信方式を利用した HTTP ベー

スの安全，簡便な認証方式”, 情報処理学会全国大会 (第 63 回後期) 分冊 3, pp.535-536, 2001

[17] http://www.hde.co.jp/lc/standard/demo/

[18] 川幡太一　他　”コンポーネント指向 Ops における XML の利用”, 信学技法, Vol.98, No.544, pp.25-30, 1999.01

[19] 相澤淳平　他,”Web によるネットワーク管理支援ツールの開発”, 信学技報 Vol.101 No.435,pp.11-16,2001.11.19

[20] 井ノ上直己　他,”文書分類手法を用いた有害情報フィルタリングソフトの開発”, 電子情報通信学会論文誌,D-2, Vol.J84-D-2, No.6 pp.1158-1166,2000.6

[21] http://www.watch.impress.co.jp/internet/www/article/1999/0531/filter.htm

[22] http://www.mrunix.net/webalizer/

[23] 梶田朋己　他,”メモリベース・キャッシング代理サーバの実装”, IC’ 99:インターネットコンファレンス’99, 1999.12.15