

平成16年度
産業教育内地留学生

研究のまとめ(資料)

研修場所 : 九州大学大学院 システム情報科学研究院
研修期間 : 平成16年4月1日~平成17年3月31日

福岡県立宇美商業高等学校

教諭 笹野 明裕

はじめに

平成11年に高等学校学習指導要領の改訂により、教科「情報」が平成15年4月1日から年次進行により段階的に適用され、各学校で「情報」の授業が開始された。情報教育に関しては、専門高校をはじめ普通高校にも教科「情報」が新設され必修となり、各学校にパソコン教室が設置された。そのため、各学校において本格的な校内ネットワークの運用及び管理体制が求められるようになった。そういった背景のもと、福岡県においては、福岡県教育センターを情報拠点とする「福岡県教育情報ネットワーク」(県内を2.4ギガビットの大容量光ファイバで結ぶ高速ネットワーク情報幹線)を構築し、平成13年度より段階的に整備し、平成15年度までにすべての県立学校への接続を完了した。

本校では、平成9年度よりパソコン室内のLANを構築し、それから段階的に校内LANの規模を拡張していき、平成14年にパソコン教室以外(職員室・事務室・校長室・進路指導室・各種準備室等)の場所からも校内ネットワークへの接続ができる環境を構築していった。そういった中、本校においては、校内ネットワークの管理体制や運用する環境などにおいて、いくつかの問題点が明らかとなった。それらの問題点を調査・分析し、快適なネットワーク環境を実現することは急務である。本校の抱える校内ネットワークの問題点については、専門高校をはじめ、同じ県立高校において同様の問題を抱えていると考えられた。そのため、その問題点を解決するためのシステムや環境構築に関して調査及び研究を行うことが本務にとって有益であると判断し、今年度1年間の研修における研究主題とした。また、教育用情報システムの構築に伴い、ネットワークを利用する生徒・教員のマナーと意識の改善が必要とされるが、ネットワークにおける機密性(認可されたものだけが情報にアクセスできること)、完全性(正確であること、及び完全であることを維持する)、可用性(許可されたものが必要なときに情報にアクセスできること)の3つの面を考え、セキュリティ面を強化することを副主題として掲げ、よりよい校内ネットワークの管理運営と情報教育環境のあり方について考察を行った。

本研修における各概要については、以下のとおりである。

第1章 高等学校における校内ネットワーク

各学校における校内ネットワークの現状および、管理運営体制における問題点を明らかにするために、インターネットを用いて県内高等学校のホームページ閲覧調査と県内の高等学校15校に対して学校訪問を行った。そこでは、各学校における様々な問題点を抽出するとともに、先進校における先進的な取り組みのうち他校でも実施可能な事例を収集して、これからの校内ネットワークの運営およびそのあり方について検証を行い、校内ネットワークの管理・運用に関するモデルケースを作成した。

第2章 校内ネットワーク接続技術

校内ネットワークの利用者およびコンピュータを管理するために、多数のパソコンから構成される情報システムにおいて、利用者が属するグループに応じてアクセス権限を設定できる利用者管理技術に関して調査を行い、その導入について検討を行った。ここでは、Windows ネットワークにおける利用者管理方式であるワークグループ、ドメインネットワーク方式を取り上げた。

また、生徒と職員のパソコンのトラフィックを分離するために、単一のネットワークを仮想的に職員用と生徒用のネットワークに分けるVLAN技術について調査および、その導入と効果について検証を行い、VLAN技術を用いた構築例を作成した。VLAN技術を実現するための機器であるスイッチの機能およびそれを用いたLAN構築については、麻生塾におけるシスコ・ネットワークングブリッジ研修を並行して受講し、より効果的な研修を行うことができた。その他に、同じ分野を扱う経済産業省テクニカルエンジニア(ネ

ットワーク)の出題範囲と、これまで出題された問題とその解答について理解を深めた。

第3章 学校環境におけるセキュリティ

学校には、生徒の個人情報をはじめ多くの機密データが存在しており、そういったデータを外部からの不正アクセスや侵入から守り、安心して校内のネットワークを活用することができるように、セキュリティ技術について調査し理解を深めた。ここでは、ネットワークを介して攻撃を行う攻撃者からの攻撃パターン、ウイルス感染の仕組み、外部にサーバを安全に公開するための方法、暗号化メール等の基盤となるPKI(公開鍵暗号基盤)と電子署名について実習を通し理解した。また、校内ネットワークにおける管理・運用のために、その利用状況を視覚化するMRTGの導入について検討を行った。

第4章 PCサーバの構築と活用

近年各高校には、生徒実習用パソコンの他に管理運用等に係るネットワークサービス提供のためにLinuxサーバ計算機が導入された。そのため、Linuxオペレーティングシステムに関する理解とその運用、さらにサーバ構築のための知識の習得を行った。ここでは、企業や大学などで多く利用されるLinuxサーバについて、普及状況とその利用方法などについて調査を行なった。また、学校におけるLinuxサーバ利活用を想定した運用と管理について検討し、その構成例を作成した。サーバ構築実習においては、Linuxのインストールからファイル共有サービスを提供するSambaサーバ、IPアドレスの自動割り当てを行うDHCPサーバ、ウェブサーバなどの各サーバの構築を行い、その構築までの手順を示した教員用のマニュアルを作成した。

第5章 システム開発

個人所有パソコンを校内ネットワークに接続させるための利用者における不正なIPアドレスの設定(誤ったデータの入力や重複したIPアドレス等の入力)を避けるとともに、利用者側の負担軽減とネットワーク管理者の作業軽減のために、あらかじめ登録された端末へのIPアドレスの自動割当機構を実現するためのシステムを設計した。そのシステムを開発するにあたり、Linuxサーバの開発環境を整え、端末登録を行うための入力画面を、専門知識を有しない者であってもGUIで簡単に操作できるように設計した。DHCPサーバの設定ファイルは難解で、編集にあたっては専門的知識が必要となり、また文法ミスがあると正常に稼働しないため、このようなシステムを企画し設計を行なった。

ソフトウェア開発にあたっては、CGIプログラミング言語とPerlを用いたプログラミングについて研修を行った。また、開発したシステムは、入力画面から入力されたデータおよび、更新された設定ファイルの定期的なバックアップを自動で行う機能を備えている。

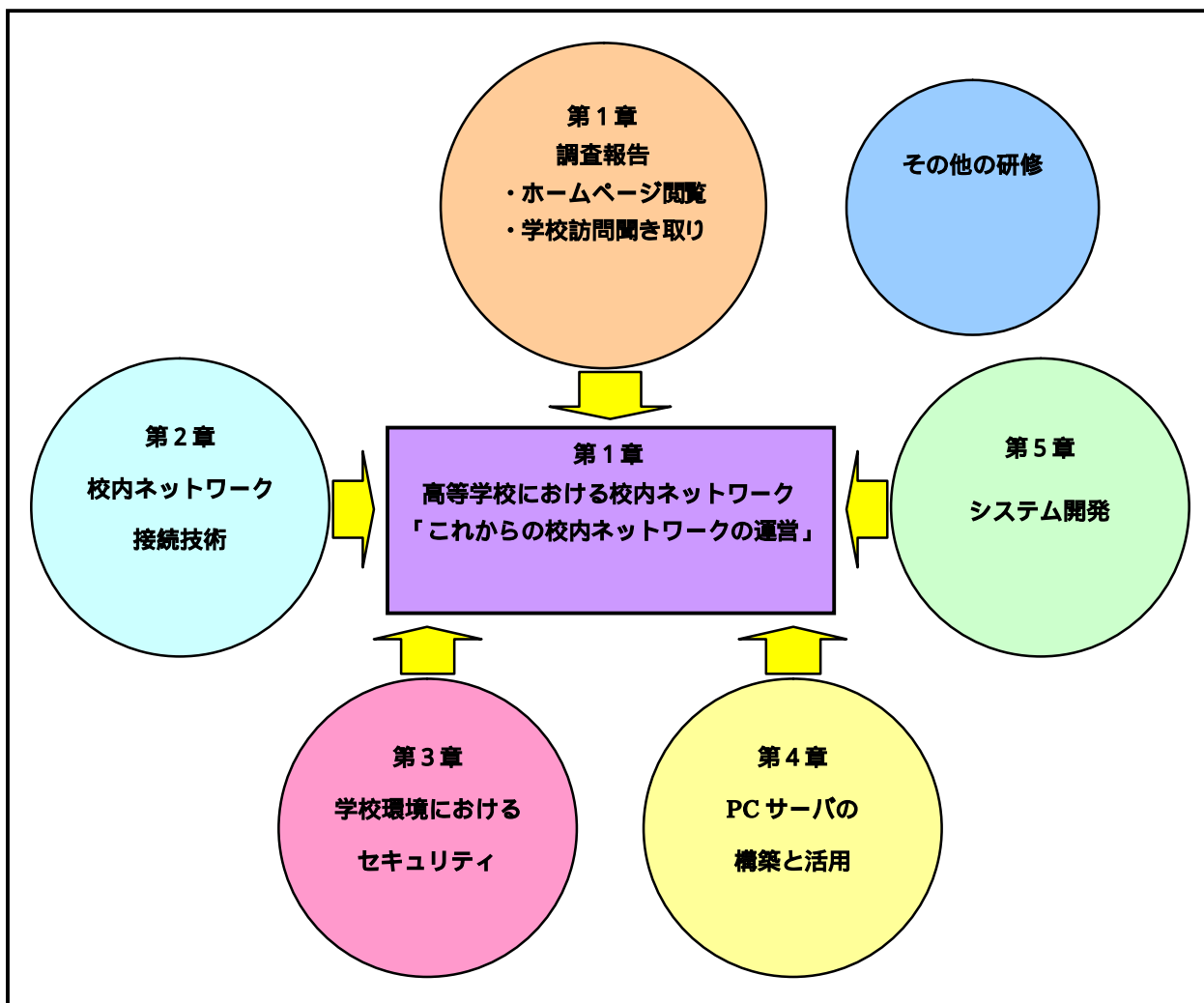
第6章 その他の研修

九州大学工学部電気情報工学科目から、前期では4科目、後期では2科目の講義を聴講させていただいた。それぞれの情報システムに関する講義で、現代のコンピュータの動作原理とそれを実現する構成要素の動作と構造や、ハードウェアとソフトウェアのインタフェースとしてのコンピュータアーキテクチャの概念を理解することができた。また、授業補助を行うことで、様々な到達度を有する受講生に対する指導について、実践を通してその指導法を習得することができた。

その他に、校務における基本的な技術として、共同作業における実践的な手法と文書作成のための方法論について学ぶことができた。

研究のまとめ（資料）の構成

研究のまとめ（資料）は、大きく6つの章から構成される。本研修の研究主題である「高等学校における教育用情報システムの構築と運営」および、副主題である「校内ネットワークにおけるセキュリティとUNIXの活用」を実現するために以下の内容を研修した。また、それぞれの章は「これからの校内ネットワークの運営」についてモデルケースを検討するための様々な技術について研修した内容である。



「研究のまとめ」構成のイメージ図

「これからの校内ネットワークの運営」の構成について

背景

調査の実際

- 1 ホームページ閲覧調査
- 2 学校訪問による調査

明らかになった問題点

- 1 ホームページ閲覧調査
 - (1) 県立高校における掲載内容の不統一について
 - (2) ホームページの定期的な更新
- 2 学校訪問による調査
 - (1) 校内ネットワーク構築状況の不統一
 - (2) 校内ネットワークの管理運営体制
 - (3) セキュリティ対策
 - (4) 生徒の個人情報保護

項目を対応

問題点への対応策

- 1 ホームページ閲覧調査
 - (1) 県立高校における掲載内容の不統一について
 - (2) ホームページの定期的な更新
- 2 学校訪問による調査
 - (1) 校内ネットワーク構築状況の不統一
 - (2) 校内ネットワークの管理運営体制
 - (3) セキュリティ対策
 - (4) 生徒の個人情報保護

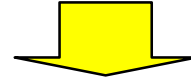
まとめ

< 構成の流れ >

背景

調査の実際

実際にどのような調査を行ったか



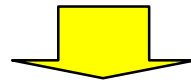
明らかになった問題点

調査を実施することにより、明らかとなった問題点について説明

- ・ ホームページ閲覧による調査
- ・ 学校訪問による調査

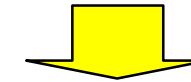
2つの調査から問題点を抽出

- ・ 問題提起



問題点への対応策

明らかになった問題点についての対応策・改善策



学校ホームページと校内ネットワークのあり方について、モデルケースの提案

まとめ

「福岡県教育情報ネットワーク利用規程」追加に関する提言等

研修の記録

第1章 高等学校における校内ネットワーク	Page 7
1 これからの校内ネットワークの運営	Page 8
2 調査報告	
(1) 県内高等学校ホームページ閲覧調査報告	Page 23
(2) 学校訪問聞き取り調査のまとめ	Page 27
第2章 校内ネットワーク接続技術	Page 40
3 Windows ネットワーク	Page 41
4 ワークグループとドメインネットワーク	Page 44
5 校内ネットワークを支える仕組み（ドメイン管理の導入）.	Page 50
6 スイッチとVLAN	Page 52
第3章 学校環境におけるセキュリティ	Page 69
7 インターネットセキュリティ	Page 70
8 PKI（Public Key Infrastructure：公開鍵暗号基盤）の活用	Page 85
9 MRTG（ネットワーク監視システム）について	Page 103
第4章 PC サーバの構築と活用	Page 105
10 Linux とは	Page 106
11 Linux の導入と活用例	Page 110
12 Linux サーバ構築例	Page 115
第5章 システム開発	Page 151
13 システム開発のまとめ	Page 152
14 資料	
(1) 構築手順書	Page 169
(2) 使用説明書	Page 180
(3) プレゼン資料	Page 183
(4) 開発したシステムの有用性について	Page 193
その他の研修	Page 195
15 情報システムに関する研修について	Page 196
16 情報処理演習における指導法に関する研修について	Page 197
17 専門的研修以外で学んだこと	Page 199
参考文献	Page 200

第1章 高等学校における校内ネットワーク

各学校における校内ネットワークの現状および、管理運営体制における問題点を明らかにするために、インターネットを用いて県内高等学校のホームページ閲覧調査と県内の高等学校15校に対して学校訪問を行った。そこでは、各学校における様々な問題点を抽出するとともに、先進校における先進的な取組みのうち他校でも実施可能な事例を収集して、これからの校内ネットワークの運営およびそのあり方について検証を行い、モデルケースを作成した。これをもとに、本校をはじめ各学校における校内ネットワークのあり方について議論していただき、再検討していただければ幸いである。

これからの校内ネットワークの運営について考察し、検証するにあたり、まず、インターネットを用いて県内の高等学校ホームページ閲覧調査(7月27日～9月3日)を実施した。この閲覧調査では、各学校のウェブページ掲載内容の不統一性、ウェブページの定期的な更新、校内ネットワークの管理運営体制などの課題が明らかになった。各学校のウェブページでは、作成した担当者の個性がそのままウェブページに反映されている傾向や、自校のウェブページを作成した担当者が転勤になり、更新することができなくなったというような傾向が見られた。そういったことを防ぐためにも、いくらかの予算を投じてウェブページの作成を専門業者に委託し、ウェブ作成に関する専門的な知識がなくとも、誰もが更新ができるようなものにする必要があるように思われる。

次に、県内の高等学校15校(県立11校・私立4校)を訪問(12月10日～12月22日の7日間)し、校内のネットワーク環境の現状について調査を行った。調査対象の15校については、北九州地区4校・福岡地区5校・筑豊地区3校・筑後地区3校の普通高校および専門高校とし、地域・校種に偏りが無いよう配慮し調査を実施した。この訪問による聞き取り調査では、校内ネットワークシステムの状況をはじめ、教員用のパソコンの状況、情報教育の実施状況、遠隔授業の取り組み、個人情報保護について実施した。その中で、以下のような様々な問題等が浮上してきた。

各学校における校内ネットワークの構築状況に統一性がなく、各学校の状況に合わせたネットワークとなっていた。

校内のネットワーク化が進んでいる学校とそうでない学校の格差があった。

教員用パソコンの設置台数が十分でないため、個人所有のパソコンが校内に持ち込まれ、ネットワークに接続されていた。

校内のデータが、持ち込まれたパソコンや記録媒体によって校外に持ち出されていた。

このような問題点をどう解決し、これからの校内ネットワークがどうあるべきか検証を行った。

校内のネットワークでは、各学校のネットワーク管理者を中心に運営組織を設置し、校内における運営・管理を行う必要がある。校内のネットワークを安全かつ快適に活用しようとするのであれば、片手間でできるような業務ではない。特にセキュリティ対策については十分な措置を行わなければならない。校内のネットワークに関するガイドラインの見直しと、教員・生徒の情報リテラシーの強化、セキュリティポリシーの確立を早急に校内で協議し、ネットワーク利用に関する意識を高める必要がある。また、各学校のネットワーク管理者を明確にし、各学校のネットワーク管理者同士で相談できる横のつながりを作る必要があるように感じる。それと同様に、教科「情報」の担当者についても各学校が独自に進めているような傾向が見受けられるため、定期的に担当者が集い、進捗状況や問題点等が話せるような場を設ける必要があるように感じられる。

今後ますます校内のネットワーク化が進む状況の中で、校内ネットワークの管理体制を決して軽んじてはならず、全職員に対する意思徹底を図らなければならない。

これからの校内ネットワークの運営

背景

コンピュータやインターネットをはじめとする情報通信ネットワークなどの IT の発達に伴い、現代社会ではあらゆる分野の情報化が進んでいる。文部科学省においては、このような状況を踏まえ、21世紀を担う子どもたちを育てる学校教育においても、IT を積極的に活用できるように学習活動の充実を図るため、平成17年度を目標に、全ての小中高等学校等からインターネットにアクセスでき、全ての学級のあらゆる授業において教員及び児童生徒がコンピュータを活用できる環境を整備するとしている。

そういった中、本県では、福岡県教育センターを情報拠点とする「福岡県教育情報ネットワーク」が平成13年度より段階的に整備され、平成15年度までにすべての県立学校への接続を完了した。それを受けて各学校では、急ピッチに校内ネットワークの構築が行われた。それから1年が経過した現在、各学校における校内ネットワークの管理運営とその問題点、および情報教育環境のあり方と指導上の問題点に関する調査を実施し、よりよい校内ネットワークの管理運営と情報教育環境のあり方について考察を行った。

なお、この調査については平成16年度長期派遣研修員（産業教育）として九州大学大学院システム情報科学研究院でコンピュータネットワークに関する研修を行っている私の研究活動の一部として実施するものであり、各学校におけるコンピュータネットワークシステムの構築とその管理・運営についての提案を行うためのモデル作成を研修項目の一つに掲げている。そこで、この研修の機会を活かし、この場を借りてこれからの校内ネットワークのあり方について提案させていただきたい。

調査の実際

これまでに福岡県内の各高等学校のネットワーク環境およびその管理運営体制について、インターネットを用いて各学校のホームページ閲覧調査を実施した。しかし、ほとんどの学校のホームページからは校内ネットワーク環境およびその管理運営体制について情報が公開されておらず、閲覧することができなかった。そのため、ウェブでの調査では限界と判断し、実際に高等学校へ訪問して校内のネットワーク運用とその問題点、改善点、効果的な工夫等について聞き取り調査を実施した。

1 ホームページ閲覧調査

この調査の目的は、現在の県内高等学校の状況を把握するというのではなく、情報教育が今後どのように行われていくべきかを念頭に置き、校内ネットワークの設置状況および管理運営組織の有無、校内ネットワークの運営状況を調査することである。そのことにより、今後の福岡県内の高等学校における情報教育が円滑に遂行していくための方向性を見出せると考えた。また、先日文部科学省の「文部科学白書」が公表され、その中で校内 LAN の整備率が発表されていた。残念なことに福岡県はワースト10に入っており、その要因を探りたいと考えウェブによる調査を行った。この調査の結果から、今後の教科「情報」を含めた情報教育の体制・環境について議論できればと考えている。

この調査を進めていく中で、各県立高校のホームページにおける掲載項目の不統一さや更新状況の不定期化等が浮上してきた。そこで、この掲載項目の統一化や更新の時期と回数を統一するような対策と意義を提案したいと考えた。何のためのホームページであるか、何のための情報公開であるのかをここでもう一度確認する必要がある。

2 学校訪問による調査

この調査の目的は、現時点における学校現場の問題点（校内ネットワーク）を集約し、その調査結果よ

り、普通高校をはじめ専門高校における情報教育環境の調査・考察を行うことにより、更なる研修の充実に努め、研修の成果として各学校へ校内ネットワークの構築および管理運営について提案できるものを作成する。また、今後社会の状況が変化していくことにどう対応していくか結び付け、各学校でどのような対応策を講じる必要があるか検討するためである。

学校訪問を行うにあたり、地域・校種に偏りがないよう配慮し県内の高等学校15校(県立11校・私立4校)を訪問し、校内のネットワーク環境の現状について調査を行った。調査対象の15校については、北九州地区4校・福岡地区5校・筑豊地区3校・筑後地区3校の普通高校および専門高校とした。

調査方法としては、各学校のネットワーク管理者または、校内ネットワーク担当者に対する聞き取り調査とし、調査項目を以下のように設定し調査を行った。

- (1) 各学校における校内ネットワークシステムの状況
 - ・ 技術面における校内ネットワークの調査
 - ・ 管理運用面における体制、規定(ガイドライン)など
 - ・ 現在の問題点とその解決のための方法
- (2) 校内における教員用パソコンの状況
 - ・ 設置済み教員用パソコンとその利用状況
 - ・ 個人所有パソコンの持ち込み状況
 - ・ 現在の問題点とその解決のための方法
- (3) 情報教育環境と指導上の問題点
 - ・ 普通教科「情報」と専門教科「情報」の実施状況
 - ・ 教室の状況に関する調査
 - ・ 実施上の問題点とその解決のための方法
- (4) 遠隔授業(テレビ会議等)の取り組みについて
 - ・ 遠隔授業の実施について
 - ・ 遠隔授業が活用されない原因について
- (5) 個人情報保護について
 - ・ 重要書類等の管理の状況
 - ・ 成績データ等の管理の状況
 - ・ ネットワーク管理者の業務について

明らかになった問題点

インターネットにおける各学校のホームページ閲覧と学校訪問による聞き取り調査の2つから、様々な問題点が浮上してきた。

ホームページ閲覧調査では、各県立高校のホームページにおける掲載内容の不統一さや更新状況の不定期化といった問題点、学校訪問による調査では、校内ネットワーク構成の不統一や管理運営体制、ウイルスに対するセキュリティ対策とセキュリティポリシーの策定、個人情報保護に対する危機感などの問題点が浮上してきた。そういった問題点を抽出し、その経緯について検証した。

1 ホームページ閲覧調査

- (1) 県立高校における掲載内容の不統一について

各学校のホームページを閲覧調査した中で、掲載内容のばらつきや掲載するべき項目の有無といった不統一性が見られた。また、それぞれの学校ホームページでは、作成した担当者の個性がそのままホー

ムページに反映されている傾向が見られ、学校ホームページのあり方についてもう一度見直す必要性を感じた。

(2) ホームページの定期的な更新

各学校のホームページを閲覧していると、古い内容のものが掲載されていたり、どう見ても昨年度のものであろうと思われるものがそのまま掲載されているといった状態で、定期的に更新されていないと思われる学校が数多く見受けられた。どのようなことが原因で更新されないままであるかは、きちんとした情報を得ることができなかったが、外部に対して一般公開している限り、ホームページの定期的な更新と掲載内容については責任を持って管理維持しなければならない。また、誰に対する情報公開かをもう一度見直す必要があるように思われる。

2 学校訪問による調査

(1) 校内ネットワーク構築状況の不統一

県立高校では、校内ネットワークの設計および構築において、県から予算が付き業者へ外注されるといったこともなく、パソコンやネットワークに関して他の教員より詳しい教員や、パソコンのリース更新と併せて業者へ依頼し構築されていたなど様々である。そのため、ネットワークの利用形態や構成に統一性がなく、各学校での格差が生じている。特に県立高校の職員においては、毎年人事異動等により職場が変わるため、統一されたネットワーク環境を構築し、どこかの学校に異動しても同じ操作、あるいは同じ環境で利用できるようにする必要があるように思われる。

(2) 校内ネットワークの管理運営体制

ネットワークの保守や管理を行うための体制については、約半分の学校で校務分掌や委員会が設置され、そういった部署で管理されているようであった。しかし、そういった部署に配置されている教員は、他の校務分掌との兼務であり、ネットワークの管理体制が十分とは言い難い状況であった。その部署の業務のほとんどは、学校ホームページの更新や生徒用パソコンの故障を保守契約業者へ連絡するという内容である学校が目立った。そういった管理体制の見直しと、ネットワークの管理・運営のための業務を明確にする必要性を強く感じた。

(3) セキュリティ対策

本来であれば、各学校のウェブページを公開用サーバに置き、外部からのアクセスを許可する必要があり、そこに重点を置いたセキュリティ対策が必要となるが、幸い県立高校の場合は教育センターでウェブサーバとメールサーバが一括管理されている。そのため、県立高校においては外部からの侵入などに対する危機意識が低いように思われる。

ウイルス対策においては、半分近くの学校でウイルス対策ソフトを導入し管理がなされていたが、個人所有のパソコンについては、ウイルス対策ソフトの導入を強要されているものの、その確認までは十分行われていないことや、校内のネットワークに接続する際ウイルス対策がなされていることを確認したが、その後どのようにウイルス対策を行っているかまでの確認ができていないという学校が見られ、まだ不十分な状況と思われた。パソコンに詳しい職員であればそう問題ではないが、そうでない職員はウイルス対策ソフトを購入し、インストールしたままの状態ですべてのアップロードが行われていないや、利用可能な期限が過ぎていたりするということが考えられる。また、セキュリティポリシーを作成しているという学校はほとんど見られなかった。

(4) 生徒の個人情報保護

生徒の個人情報漏洩などに関する記事が、毎月のようにマスコミにより報道されている。先日も、毎日新聞に「学校現場は個人情報保護に関する意識が希薄で、無防備といえる状態」といった内容が報道されていた。私が実施した学校訪問による調査では、各学校において生徒の個人情報が掲載されている書類や成績データなどについては、しっかりとした管理が行われていたが、その管理について盲点と思われる箇所が浮上してきた。

問題点への対応策

前節で明らかとなった様々な問題点について検証し、その改善策として以下のような手立てを考えた。

1 ホームページ閲覧調査

(1) 県立高校における掲載内容の不統一について

県立高校におけるホームページの掲載内容の統一を図るためには、県から各学校に対して統一した最低限掲載すべき内容を示すといった指導が必要になると思われる。しかし、これについては14教高指第149号（平成14年6月7日付）の「福岡県立学校ホームページ公開指針」が既に示されており、各学校でその確認が十分にできていないように思われた。早急にその文書の確認を行い、自校のホームページと照らし合う必要がある。また、いくらかの予算を投じて学校ホームページの作成を専門業者に委託し、ウェブ作成に関する専門的な知識がなくとも、誰もが更新ができるようなものにする必要があるように思われる。

各学校が統一した掲載内容とするために、ホームページはどうあるべきかについて提案させていただきたい。

広報的な役割を果たす学校ホームページ

現在の高等学校ホームページのほとんどが広報的な機能として作成されている。ホームページを作成する際、掲載すべき内容ばかりに捉われており、誰に対する情報公開かをもう一度見直す必要がある。また、掲載項目の不統一から、今後県立高校における各学校のホームページによる公開すべき項目を統一する必要性を強く感じた。そのためにも、県からの文書にある「福岡県立学校ホームページ公開指針」をもう一度各学校で確認し、それに沿った項目を掲載する必要がある。その文書にある公開すべき情報を以下に挙げる。

- ・ 学校名、住所、電話番号、FAX番号、代表メールアドレス
- ・ 学校の紹介（高等学校においては『展望』等に掲載している内容）
- ・ 年間行事予定と主な行事の内容
- ・ 教育課程等（教育課程表、学校時制、総合的な学習の時間の取組）
- ・ 部活動の状況、課外授業の実施状況、土曜日の活用状況、ボランティア活動
- ・ 授業料、入学料及びその他校納金等（入学時、例月）
- ・ 学校自己評価に伴う情報（目標、目的達成のための中間評価、学年末評価）

教材的な機能を果たす学校ホームページ

県内の高等学校では、小中学校と比べ校内向け、および学習に関する情報が公開されていない。教育実践の情報などを公開すると、外部からの批評を得る機会ができる。さらに教員自らの名前と責任のもとで教材や授業実践を公開し、より良い授業作りのきっかけとして位置づける必要を感じる。そのためには、校内でのホームページを管理運営する組織を設置し、より良い学校ホームページを作成することが望まれる。

(2) ホームページの定期的な更新

学校ホームページが更新されていない学校は、教育活動の活発性に欠け、魅力を感じない学校に思われがちである。そういったイメージを打破するためにも、定期的な更新が必要となる。そのためにも各学校できちんとした組織を設置し、その運営と管理を行う必要がある。本調査できちんとした情報を得ることができなかつたが、ホームページの作成を一部の技術を持つ教員に依頼し、ホームページの管理・運営を組織化していない学校があるように思われる。その一部の教員がホームページを作成し、アップロードしたままで更新されていないという状況も見られた。その原因として考えられることは、校内で組織化されておらず作成した教員が転勤となり、その引継ぎが行われず更新されないままの状況となっているのではないかと思われる。

ホームページの更新は、それだけ大切なことであり、外部から学校を見られているという意識を十分に持つておく必要があると思う。更新の目安としては、1ヶ月に1回程度でどこかのページが更新されていけば問題ないように思われる。その際、更新履歴を明記し、新しく更新した箇所をはっきりわかるようにする必要がある。

2 学校訪問による調査

(1) 校内ネットワーク構築状況の不統一

今回訪問させていただいた15校のほとんどが、学校独自に校内ネットワークを構築されており、当然利用形態やネットワークの構成が異なっていた。そういった学校独自のネットワーク構成とその利用方法を統一し、どこの学校に異動しても同じ操作、あるいは同じ環境で利用できるようにしなければならないように思われる。また、学校の規模や校種によってネットワーク環境は異なるが、基本となる環境については統一する必要があるように思う。そこで、そのための手段として図1のようなネットワーク構成の例を挙げる。

校内ネットワークについて

校内ネットワークの基本構成として、県立高校はふくおかギガビットハイウェイでイントラネット化されており、福岡県教育センターから各学校にプライベートアドレスが割り当てられている。さらにそのアドレスを職員用と生徒用とに分けられ、生徒用のアドレスからは有害情報にアクセスできないようフィルタリングされるという設定がなされている。

各学校へ割り当てられているアドレスとその詳細

生徒用	*.*.*.1	~	*.*.*.127	フィルタあり
職員用	*.*.*.128	~	*.*.*.254	フィルタなし

ネットワークの構成例(図1)では、校内のルータに職員用のアドレスの1つを与え、職員用のネットワークと生徒用のネットワークとに分ける。職員用は教育センターから割り当てられた職員用のアドレスの1つをLinuxサーバに割り当て、それをアドレス変換して職員用のネットワークアドレス(192.168.0.0/24)としている。そのため、職員用として利用するパソコンや周辺機器については、192.168.0.1~192.168.0.254のアドレスを使用する。

生徒用では、教育センターから割り当てられた生徒用アドレスのうちの1つを生徒用サーバに割り当て、それをアドレス変換して生徒用のネットワークアドレス(192.168.1.0/24)としている。そのため、生徒用として利用するパソコンと周辺機器については、192.168.1.1~192.168.1.253のアド

レスとし、パソコン室が2室以上ある場合は連番で使用する。ただし、複数のパソコン室にアドレスを割り当てる場合は、必ずしもこの通りでなくてもよい。これは基本構成ということで、専門高校(工業・商業)のように生徒用パソコンの台数が多い学校においては、生徒用サーバの下位に位置するスイッチなどから分岐させるといったように、それぞれ対応させる必要がある。

職員用のサーバは、ファイルサーバと認証サーバ、DHCPサーバ、Sambaサーバ、ウェブサーバとして利用する。そのため、職員用ではDHCP機能を用いることから各パソコンにIPアドレス等の設定を行わない。また、ネットワーク接続の際にユーザ認証が必要となる。その他として、校内用のウェブを利用できるようにする。

生徒用のサーバとしては、ファイルサーバとプロキシサーバ、認証サーバとして利用する。そのため、生徒用では各パソコンにIPアドレスを固定で割り当て、プロキシサーバである生徒用サーバをデフォルトゲートウェイ(192.168.1.254)とする。また、ネットワーク接続のためにユーザ認証が必要となる。その他に、生徒用サーバをプロキシサーバとして、クライアントからのパケット監視を行えるようにし、授業でインターネットを利用しない場合は外部へのアクセスを禁止するというような設定をサーバ上で行う。(例:フリーソフト Black Jumbo Dog の利用)

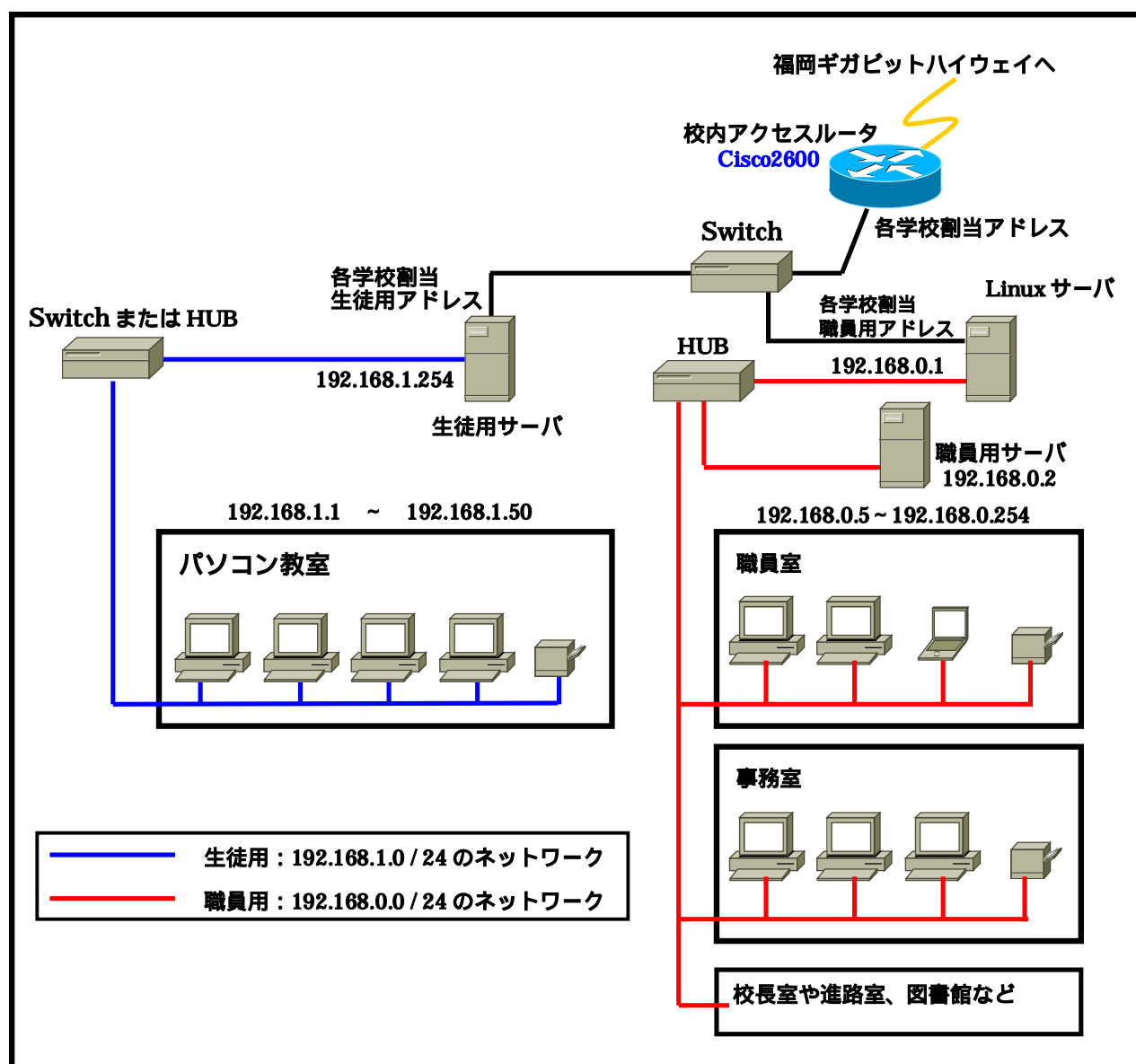


図1 ネットワーク構成例(基本部分)

校内ネットワークの利用

ア 生徒用

a パソコンの設定

パソコン教室のパソコンに対しては、固定の IP アドレス等を割り当て、生徒全員にユーザ ID とパスワードを配布し、ユーザ認証を行うようにしたい。そうすることにより、生徒へ個人情報の大切さやリテラシーを学ばせるといった教育的効果が得られるように思われる。また、生徒用のファイルサーバ上に個人用のフォルダを作成し、ネットワークドライブの割り当てを行うことにより、他の生徒のフォルダに対するアクセスやいたづらを防止するようにすることが理想的である。

b パソコンの管理

予算があればパソコンを起動する都度、初期状態へ戻す機能をもつソフトウェア（例：ハードディスクキーパ）などの導入を薦めたい。そういったソフトを導入することで、生徒によるパソコンへのいたづら（デスクトップの壁紙やスクリーンセーバの画面を変える）や、ゲームソフトをダウンロードし、ハードディスクに保存するといったことを防止することができる。それ以外にも、生徒各自が作成したファイルについては必ずファイルサーバに保存させ、1台のパソコンを複数で利用するためのマナーを身に付けさせることができる。

イ 職員用

a 職員の利用について

職員全員に対し、ユーザ ID とパスワードを配布する必要がある。特に学校に設置済みの職員用のパソコンを複数で利用している場合、使用する職員が自分のユーザ ID とパスワードでログインし、利用後は必ずログアウトするように周知徹底する必要がある。また、データの保管場所として職員用のサーバに職員全員分のフォルダを用意し、そこに保存するように徹底する。

個人所有のパソコンを校内のネットワークに接続する場合は、事前に管理者に申し出て、DHCP サーバを利用した固定 IP アドレス等の自動割当（システム開発 使用説明書参照）を利用する。また、個人所有のパソコンで作成した生徒の個人データ等については、ハードディスクや他の記録媒体への保存を禁じ、必ずファイルサーバに保存することを周知徹底する必要がある。ただし、このことについては、バックアップとして各自保管することを認め、自宅への持ち帰りを禁止し、個人情報流出の可能性を阻止するようにしたい。

b 校務における活用

校務における活用としては、サーバ上の設定になるが、校内のネットワーク管理形態をドメイン管理にして、アクセス権を設定することにより利用できる権限のレベルを変える。これにより、権利のないユーザに対して不用意に情報を与えてしまうということを防ぐことができる。このように設定すると、校務分掌ごとの独立した利用が可能となり、次年度への引継ぎなどがスムーズに行われる。

c 成績処理等のネットワーク化

成績管理についても、各学校で様々な成績入力用のシステムを作成されているため、そのファイルをサーバに置き、管理者によって一時的に入力可能状態にするような手立てを行う必要がある。それには、上記（校務における活用）で述べたように、サーバ上でアクセス権を一時的にユーザ全員としておき、成績締め切り後はユーザにアクセス権を与えないようにするなどの方法が考えられる。

d 校内用のウェブページ

現在、本校において職員への連絡として用いられている方法では、

- ・職員朝礼で一斉にアナウンスを行う
- ・職員全員にプリント紙を配布する
- ・職員室内の黒板等に連絡事項を板書する

といったことがなされている。そこで、職員用としての Linux のウェブサーバを利用し校内用のウェブページを作成し、職員への連絡事項や研修の案内などを表示するといった活用が望まれる。そうすることにより、連絡等の聞き漏らしや職員朝礼時の不在、プリント類の紛失などに対処することができる。また、校内用のウェブページを職員の掲示板として利用するといった活用も考えられる。

このように校内用ウェブページを作成し活用することにより、職員のパソコン活用能力の向上を図ることができ、校内用ウェブページの管理側でも連絡事項の管理や保管を行うことができる。各学校の状況によるが、こういった業務を行うためには、他の分掌と掛け持ちではなく、この業務への専従者を数名配置する必要がある。

これからの校内ネットワーク

校内でネットワークの活用を推進することにより、すべての教科でネットワークを活用した授業も可能となる。また、全職員のパソコン活用能力の向上につながり、校務の電子化を図ることが可能となる。これからの校内ネットワークでは、教職員間での情報の共有をはじめ、ネットワークの利便性を追及し、十分なセキュリティ対策を行うことが必要である。

ア 職員に対する連絡について

a 校内ウェブページの利用

教員は授業で教室にいる時間が多く、職員室にいる時間が少ない。教職員全員が目を通す文書などは、電子掲示板や校内用ウェブページを使って確認すると、ペーパーレスになるばかりでなく、後に記録として利用できる。また、そのまま保護者向けのウェブページ作成に転用することもできる。また、生徒の欠席の電話連絡や、保健室などのあらゆる場所からリアルタイムで正確に情報を把握できるようになる。また、これまでは校内でどのような情報が流通しているのかを教職員が確認しにくい状況にあったが、校内ネットワークによって校務が情報化することにより、校内を流通する情報が教職員全体に見えるようになる。

b 電子メール・チャットの利用

職員室不在というケースが多い教員にとっては、不在時の連絡等がメモで行われる。教育センターから全職員に配布されているメールアドレスを使うことにより、不在時の連絡を確実に受け取ることができ、もちろん外部に対して連絡用としても用いることができる。また、各自のメールアドレスを使い、学年内や教科内、または職員間でチャットを用いた連絡のやり取りが可能になる。

イ 校内サーバの利用

a 校務情報の共有

校務分掌で、これまでの行事関係の書類、各種検査、保護者への連絡、式次第など、毎年繰り返されるものについては、それまでの関係書類を校内サーバに保存しておき、それぞれの係りが呼び出して修正、そして更に更新という作業で完了する。これによって校務の共有化と透明性の確保、効率的な管理などが実現する。

b 個人データの保存

パソコンを使って作成したファイルについては、サーバ上の個人用のフォルダに置き、ファイルの紛失を防ぐ。また、フロッピーディスクやCD-Rなどの記録媒体がかさばらず、個人での管理面負担が緩和される。

c 職員用パソコンの利用

職員に配布済みのユーザIDとパスワードでログインすることにより、複数で使用するパソコンを各自の環境で利用することができる。

d 個人所有のパソコンの利用

個人のパソコンを学校に持ち込んだ場合、各自でネットワーク接続のための設定を行わなくても、DHCPサーバでIPアドレス等が割り当てられるため、簡単に校内ネットワークに接続することができる。

ウ 職員研修会

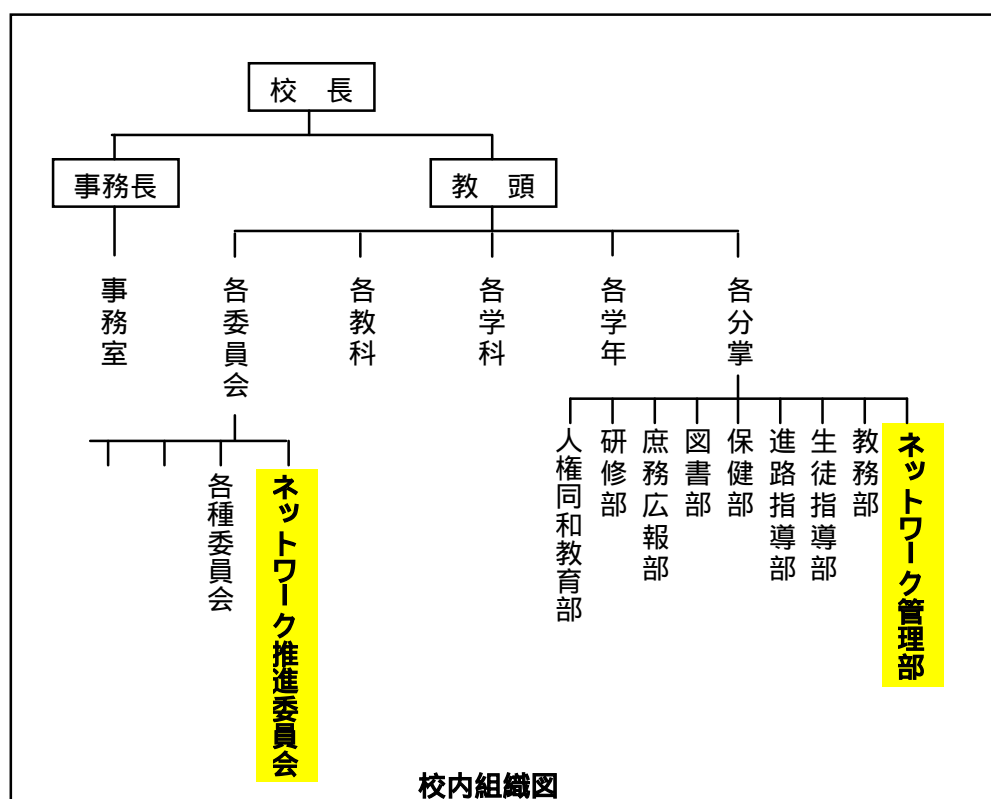
定期的実施される職員研修会に参加することにより、パソコンの活用技術も向上し、授業でネットワークの活用も可能になる。

(2) 校内ネットワークの管理運営体制

校内ネットワークの管理運営組織について

現在、校内ネットワークが導入されている学校のほとんどでは、何らかの形で管理運営組織が設置されている。しかし、校内ネットワークの在り方が今後ますます重要視される傾向にあるため、管理運営組織を他の分掌との兼務ではなく一つの分掌と位置付け、校内の業務に従事する必要があるように思われる。

管理運営体制では、校内のネットワークを管理・運営するための組織と、校内ネットワークの活用を推進し、発展させていくための組織の二つを設置する必要性が強く感じられる。



具体的な組織とその業務について

管理・運営・保守・開発系と利用推進系の2系統の業務内容を構成する分掌および委員会組織を設置する。

ア ネットワーク管理部（管理・運営・保守・開発系）

校内ネットワークの管理運営の全般を行う。また、校務に関わるデータ処理をスムーズに行うためのネットワークシステムの開発を行う。このネットワーク管理部（仮称）は、校務分掌としてきちんと位置付ける必要がある。構成人数としては3,4名程度とし、そのうち1名をネットワーク管理者とする。

私立学校の場合、日常のネットワーク管理者を雇う学校が増えているが、公立の場合では専任のネットワーク管理者を置くことは難しく、しかも人事異動や校内の都合で担当者が変わる可能性があるため、何の作業でも管理者一人で行わないようにする必要がある。

校内のネットワークを運営する中で、業務を分担するのが望ましい。全体の指南役を主担当であるネットワーク管理者が行い、日常の作業を分担する。システム全体にかかる作業やログ（コンピュータの出力するエラーメッセージなどのファイル）の解析とユーザ登録や端末の登録、ネットワークがつながらなくなった時の対応など、日頃行っている作業をリストアップし、それを係分担する。また、保守的な作業や何らかのトラブルが発生した時などの作業は複数で行い、管理技術を組織内の担当者全員で共有することにより、作業の引継ぎや中心となる教員の負担を軽減することが可能となる。

ネットワーク管理部における業務内容としては、以下のようなものが考えられる。

a ネットワーク運用

- ・ サーバの運用・保守
- ・ サーバの定期的なバックアップ（ファイルサーバとは別のサーバにバックアップする）
- ・ 職員用ネットワークのメンテナンス
- ・ 生徒側ネットワークの利用・保守
- ・ ネットワーク環境の保守
- ・ 職員のユーザ登録とIPアドレスの割り当て・ウイルス対策の確認（個人所有パソコン）
- ・ システムのログ確認 など

b 校務データのメンテナンスとシステム化

- ・ 生徒データの維持管理
- ・ 生徒名簿・成績・出欠等のデータ提供
- ・ 成績処理
- ・ 校内連絡用掲示板の運営
- ・ メーリングリストの作成

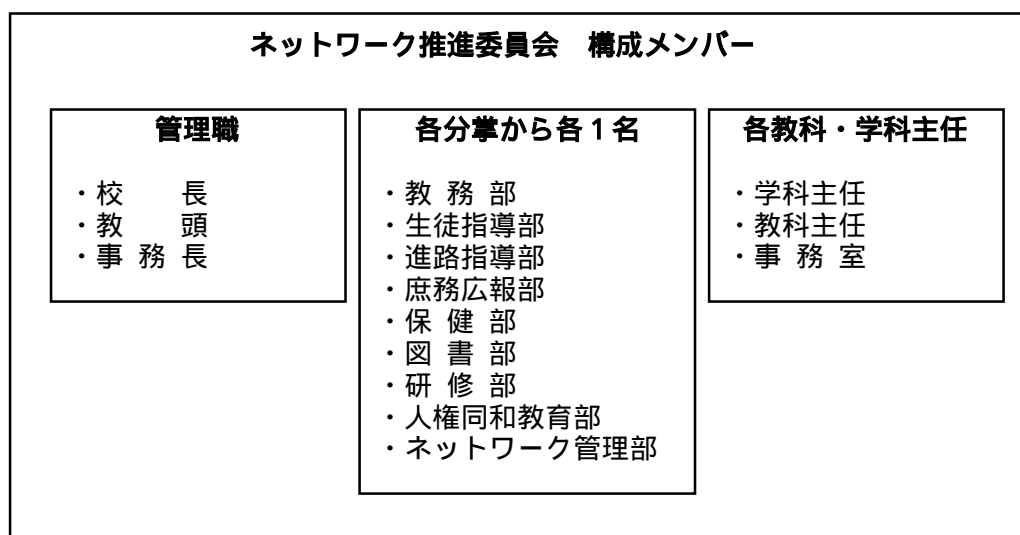
イ ネットワーク推進委員会（利用推進系）

このネットワーク推進委員会（仮称）については、校務分掌として位置付けず、各校務分掌の代表者1名と各教科主任で構成し、校内における様々な立場から意見を出し合えるようにし、校内ネットワークの推進的な役割を果たす委員会とする。

「情報教育」・「教育の情報化」などにおけるネットワークの活用についての提案を行う。また、校内ネットワークにおける利用規定等のガイドラインを策定し、情報リテラシー（コンピュータ活

用のための基礎的・基本的な知識・技術)の浸透化を図る必要がある。

「情報教育」全般については、ネチケツト(ネットワークエチケツト)を基盤においた情報の抽出・収集・利用・加工・発信のあり方についての方向性を示し、推進していく必要がある。また、「教育の情報化」については、ネットワークを活用した教材・授業展開の提案と実現に向けたサポートが必要である。その他に、個人情報保護の観点から、生徒データの流出を防ぐための校内規定などの検討が必要となる。以上のような内容を実施するにあたり、定期的に委員会を開催し、職員に対してネットワーク活用の推進およびサポートを行う。このように各校務分掌と兼ねた職員で構成することにより、ネットワーク管理だけでなく、情報教育を推進する上でも合理的であるように思われる。



ネットワーク推進委員会における業務内容としては、以下のようなものが考えられる。

a 校内ネットワークの在り方

- ・ 校内ネットワークの利用に関する基本的事項の検討
- ・ ウェブページ運用と公開情報の検討
- ・ 授業におけるネットワーク活用に関する検討
- ・ ネットワーク利用形態の見直しと改善点をネットワーク管理部へ提案
- ・ ガイドラインとセキュリティポリシーの策定と見直し
- ・ 情報リテラシーの浸透化を図る
- ・ ネットワークを活用した教材・授業展開の提案
- ・ 個人情報保護に関する校内規程の検討
- ・ 校内の利用規程の策定

b 職員研修の企画・実施

- ・ 月に1回～2回、希望者を対象に研修会を実施

テーマ例：成績入力手順、インターネットの活用、電子メールの利用、メッセージャーの利用、アプリケーションソフト(Microsoft Word・Excel・PowerPoint・Access等)の活用など
ネットワーク管理者における異動時の対策について

校内ネットワークの運営にあたっては、すべてをマニュアル化することが一番良い方法であるが、毎日の業務に追われ、マニュアルを作成する余裕がないと思われる。そのため、何らかの作業が発生

した際は一人で行わず、校内ネットワーク管理組織の構成員と一緒に実施することが望まれる。また、後継ぎを育てるためにもその方法が最も有用であると思われる。

しかし、全くマニュアル化されていないということも問題であるように思われるため、重要な業務または校内のネットワーク構成図などについてはマニュアルを作成しておく必要がある。

(3) セキュリティ対策

外部から電子メールの配信によるウイルスやウェブページ閲覧によるウイルス感染、内部からの記録媒体などによるウイルス感染や校内データの漏洩といった危機を想定しての対策が必要である。そのため対策として以下のような対策を講じる必要がある。

ウイルス対策

ウイルス対策については、どの学校においてもウイルス駆除ソフトが導入されている。その導入例の一つとして、パソコンのリース契約は通常5年であるため、その導入の際に併せてウイルス駆除ソフトも導入し、複数年契約(5年)を行う。例えば、トレンドマイクロ社のウイルスバスターコーポレートエディションでは、学校に設置されているパソコンのすべてにインストールすることが可能なため、ネットワーク管理部で手分けしてインストール作業を行い、定期的なアップデートも自動で行うよう設定する必要がある。ただし、トレンドマイクロ社との使用許諾については、十分熟知しておく必要がある。また、Windows マシンにおいては、定期的なアップデートを行い、常に最新の状態にしておく。

個人所有のパソコンについては、福岡県教育情報ネットワーク利用規程の第6条(セキュリティの確保)第4項の「ウイルス対策がなされていないコンピュータを教育情報ネットワークに接続しない。」を遵守し、校内のネットワークに接続する前に必ずネットワーク管理組織で手分けし、その対策がなされているかの確認を行う。また、ウイルス対策ソフトなどにおいては、定期的なアップデートを行うよう徹底させることや、利用可能期限を過ぎアップデートができない状況でないかなど、定期的に調査する必要がある。

その他の対策としては、Proxy サーバの活用が有用である。教育センターから割り当てられた生徒用のアドレスでは、教育センターの Proxy サーバでフィルタリングされているが、さらに校内でも生徒に悪影響を及ぼすサイトへは接続させないといった手立てが必要であると思われる。

セキュリティ対策

セキュリティ対策で最も重要なことは、校内ネットワークの利用者に対するリテラシー教育である。教員に対しては、校内研修会などを通じてリテラシーに対する考えを身につけてもらう。生徒においては、パソコンを活用した授業を通じてリテラシー教育を実施する。

技術的対策としては、校内ネットワークへの参加時にユーザ認証を行うとともに、ユーザまたはグループごとにデータのアクセス制御を行い、データを保護する。また、校内ネットワークへのログイン記録やデータのアクセス記録を定期的に点検し、許可された範囲外からのアクセスが試みられていないかを監視する。

情報セキュリティポリシー

校内ネットワークを管理運営していく中で、ネットワークのセキュリティポリシーの策定は急務である。問題がめったに起こらないのであれば、起こったときに個別に判断すればよいが、急激に増えて来たウイルス感染から個人情報流出に至るまでの様々な事件が発生する今日では、あらかじめ方針を立てておかなければ対処することができない。その方針をセキュリティポリシーと呼ぶ。ここでいうセ

セキュリティとは直訳すると安全性だが、情報の漏洩防止（機密性）、情報やそれらの処理が正確であること（完全性）、そして正当な利用者がいつでもシステムを使えること（可用性）の3つを維持することである。人為的な攻撃だけでなく、地震や落雷などの天災も安全性に対する脅威となることを忘れてはならない。

セキュリティポリシーを策定するときに、ネットワークだけを対象とする場合と情報システム全体を対象とする場合がある。後者を情報セキュリティポリシーと呼び、情報とその取り扱い、情報を蓄積・加工するコンピュータ、そして情報を伝送するためのネットワークのすべてを対象に含むので、できれば各学校では情報セキュリティポリシーの方を策定する必要がある。

セキュリティポリシーは、結局文書として表現されるものであるが、作文すれば終わりではなく、各学校でどう運営していくかが重要である。その文書は、学校長はもとより全職員が認めるものでなければならない、さらに実際に運用できる体制も整える必要がある。したがって、予算や人員も関係してくるので校長を含めた委員会組織で検討する必要がある。この体制も含めた一連のシステム、すなわち「情報セキュリティマネジメントシステム（ISMS）」を構築することが重要といわれており、国際標準、認証システムなどもできつつある。

学校の情報を守るためにしっかりとした情報保護計画を策定することによってセキュリティポリシーを確立し、それに従ってシステムの構築・運用におけるセキュリティ確保を実現する。セキュリティ対策と管理については既に作成されている基準・ガイドラインに基づき、ネットワーク推進委員会で十分に検討を行い全職員に示す必要がある。また、ネットワーク推進委員会において定期的にセキュリティポリシーの見直しと改訂を行い、校内における実施手順書を作成する必要がある。

(4) 生徒の個人情報保護

生徒データの管理

各学校で十分な管理が行われている生徒の成績データとは、各授業担当者が生徒を評価し、結果として算出された最終的な成績である。その前段階である考査の成績や授業における記録などは教員個人が管理している。そういったデータが個人所有のパソコンや個人の記録媒体の中に保存されて、校外に持ち出され盗難などに遭うというケースが考えられる。個人情報漏洩の原因として最も多いのは、帰宅途中におけるパソコンや記録媒体などの盗難からである。そのため、その可能性をなくすためにも生徒のデータは、校内のファイルサーバに保存し、自宅には持ち帰らないといった校内規程やセキュリティポリシーを策定するようにしたい。

ア 個人所有のパソコンについて

校内に個人所有のパソコンを持ち込まないということが最も理想であるが、学校に設置されているパソコンの台数から考えると現実的に難しい。だからといって個人所有のパソコンの持ち込みを奨励し、それを校外への持ち出すことを禁止するというような制限をかけることはできない。そこで、個人所有のパソコンで作成された生徒データの保存場所を職員用のファイルサーバとし、そのパソコンのハードディスクには生徒情報を保存させないようにする必要がある。そうすることによって、生徒データを校外に持ち出し盗難などに遭う可能性をなくすることができる。

イ 個人の記録媒体について

記録媒体といっても、フロッピーディスクからCD-R/RW、MO、DVD-R/RW、フラッシュメモリなど、多くの媒体がある。最近校内でよく利用される記録媒体として、CD-Rやフラッシュメモリなどがあるが、それについてはサーバ以外にバックアップデータを保存するためのものとし、

校外への持ち出しを禁止するようになる必要がある。ただし、これについては個人が管理するため、鍵がかかる個人の机等で十分な管理をおこなうよう職員へ周知徹底しなければならない。

ウ その他の対応策

現在企業などで多く利用されている機器として、パソコンに鍵をかけ、パソコンの不正使用や情報漏洩を防止するために開発された USB ハードキー（サンワサプライ）がある。もし、学校に予算があればそういった機器を導入し、個人所有のパソコンを持ち込まれた職員に貸し出すといった方法や、各自で準備してもらうことを前提に個人のパソコンを校内に持ち込めるようにするという方法が考えられる。

その他書類の管理

学校には、職員個人で管理しなければならない生徒の個人情報にかかるデータがいくつも存在する。例えば、生徒指導票や考査の解答用紙などがある。こういったものについても個人の記録媒体の管理と同じように、校外への持ち出しの禁止について徹底し、その保管については鍵がかかる場所での管理を徹底する必要がある。

ア 生徒指導票

家庭訪問などで生徒の自宅地図や連絡先等が必要で、生徒指導票を持ち出すケースが考えられるが、その際該当箇所のみコピーし、訪問終了後確実に処分するようになる必要がある。

イ 考査の解答用紙等

考査における生徒の解答用紙や小テストなどについても自宅に持ち帰らないようにする必要がある。勤務時間内に採点が終わらないため、自宅に持ち帰って採点するといったケースが考えられるが、校内から解答用紙を持ち帰らないでいいように工夫するための手立てを各学校で検討する必要がある。その手立てとして、教務部へ提出する小票等の締め切り日の配慮や、勤務時間中に採点する時間を確保するといった配慮が必要になる。こういったことが、生徒の個人情報を保護することと自分自身を守るといったことにもつながる。

職員に対する研修会の実施

個人情報保護に関して職員に周知徹底するためには、生徒情報を遵守する強い意志が必要である。そういった遵守しようという強い意志を職員一人ひとりが持つためには定期的な校内の研修会が必要となる。職員全員に校内の何を守るのかを明確に示し、今後校内ネットワークを運営していかなければならない。

まとめ

本県の県立高校においては、校内ネットワーク化が進み、各校様々なネットワーク形態で構築されている。こうした学校独自の校内ネットワーク化を進めるのではなく、すべての県立高校で統一されたネットワーク形態を推進していくようになる必要がある。また、県立高校では、福岡県教育情報ネットワークに接続し、福岡県教育情報ネットワーク利用規程に基づいてネットワークの利用を行っている。学校訪問による調査から、各学校における個人所有のパソコンのセキュリティ対策が十分に行われていなかった。そこで、「福岡県教育情報ネットワーク利用規程」のセキュリティに関する項目に追加する必要性が感じられた。まず、利用規程の第4条（ネットワーク活用委員会の設置）において、ネットワーク活用委員会で行う事務について5項目挙げられている。そこに、「校内のセキュリティポリシーの策定に関すること。」というような1項目を追加する必要性を感じた。次に、第6条（セキュリティの確保）の第4項では、「ウイルス対策がな

されていないコンピュータを教育情報ネットワークに接続しない。」と述べてあるが、各学校の現状から一旦接続したコンピュータへの調査がほとんどなされていなかった。教育情報ネットワークに接続する時はウイルス対策ができていても、その後ウイルス対策について何の手立ても講じていなければ、ウイルス対策がなされていないコンピュータと同様になる。そのため、その部分を明確にするために、「教育情報ネットワークに接続されたコンピュータのウイルス対策においては、常に最新の状態に保つこと。」といった内容を加える必要があるように思われる。そうすることによって、各学校のネットワーク活用委員会で十分検討され、定期的なアップデートを促す連絡や、個人所有のパソコンへの確認が行われたり、そのための校内規程が設けられると思われる。

福岡県教育情報ネットワークの利用により、校内の情報化が進みインターネットの教育への活用や、日常の業務の中での電子データの取り扱いなどの比重が日増しに大きくなってきている。そのように便利になってきた反面、生徒の個人情報漏洩に関する問題も出てきており、校内ネットワークの整備に併せて、セキュリティ対策や不正アクセス等のトラブル発生時の対応方針を明確にし、具体的な対応手順を整備することが緊急の課題である。

各学校に即したセキュリティポリシーの策定をネットワーク活用委員会等で話し合い、校内のセキュリティ・レベルを断続的に向上させ、学校からの情報漏洩を阻止できるような環境を構築しなければならない。また、今後情報通信機器の発展に伴い変化していく校内ネットワークにおいても、常に校内の情報保護を念頭に置き、柔軟に対応していかなければならない。

この調査の目的は、現在の県内高等学校の状況を把握するというのではなく、情報教育が今後どのように行われていくべきかを念頭に置き、校内ネットワークの設置状況および管理運営組織の有無、校内ネットワークの運営状況を調査することである。そのことにより、今後の福岡県内の高等学校における情報教育が円滑に遂行していくための方向性を見出せると考える。また、先日文部科学省の「文部科学白書」が公表され、その中で校内LANの整備率が発表されていた。残念なことに福岡県はワースト10に入っており、その要因を探りたいと考えウェブによる調査を行った。この調査の結果から、今後の教科「情報」を含めた情報教育体制・環境について議論できればと考えている。

調査を進めていく中で、各県立高校のウェブページにおける掲載内容の不統一や更新状況の不定期化等が浮き彫りになった。そこで、この掲載内容の統一化や更新の時期と回数を統一するような対策と意義を提案したいと考えた。何のためのウェブページであるか、何のための情報公開であるのかをここでもう一度確認する必要がある。

1 県立高校における掲載内容の不統一について

この調査については、当初各学校における情報教育の実施状況と校内ネットワークの管理運営体制の2点に焦点を絞り、ウェブによる閲覧調査を実施した。情報教育の実施状況については、教育課程表を基に実施科目とその単位数、何年生で実施しているかについて調査した。ほとんどの県立高校では教育課程表が掲載されていたが、掲載されていない学校もあった。また、掲載されている教育課程表が14年度のものや15年度というように、古いものが掲載されたままのところが多く目立った。

教育課程表の掲載については、2通りの掲載が考えられる。まず、今年度実施の教育課程表として3つの学年が掲載されているもの、もう一つは当該年度に入学した生徒の3年間の教育課程表を3学年分掲載することである。ここで、ウェブ上に公開する教育課程表は、今年度実施するものでいいと思うが、詳細のページを作成し各学年に対応した3年間の教育課程を掲載してもいいように感じられる。それ以外にも、中学生が閲覧することを目的に作成されたウェブページであれば、来年度入学生の教育課程表を掲載することにより、中学生が高校入学後に学習する内容を知ることができ、受験する高校を選択する際に役立つのではないかと思う。こういった情報提供を校内で検討する必要があるように思われる。

次に、校内ネットワークの管理運営体制については、学校自己評価表を基に校内の組織と課題になっているところを調査した。ここでは、ほとんどの学校において掲載されておらず、校内のネットワーク化が図れていないのか、またそういった組織がないのかよくわからない状況であった。校内のネットワークの管理運営組織については掲載されていなかったが、学校ウェブページの管理運営組織については多くの学校で組織化されていることがこの調査で知ることができた。しかし、この調査についても、学校自己評価表が新しいものに更新されていない学校が多く、古いもので14年度計画段階のままのものが掲載されているという状況であった。

学校自己評価については、平成15年度の文部科学白書に「自己評価の努力義務化」ということで、「学校評価と情報提供の実施を促進し、開かれた学校・信頼される学校づくりを推進している」と明記されている。さらに、自己評価を実施して結果を公表する努力義務が課されている。また、「自己評価だけではなく、保護者や地域住民、学校評議員が評価を行うなど、外部評価の取組も期待されている。」と明記されている。

このことから、各学校における学校自己評価の掲載を軽んじてはならず、学校ウェブページを定期的に更新し、常に最新のものを公開する必要性を強く感じた。

2 私立高校におけるウェブページのあり方

私立高校においては、全般的に受験生に対して学校の特色を強くアピールすることに主眼が置かれる傾向にあり、校内ネットワーク等の運営や教科「情報」に対する教育体制等を調査するには情報不足であった。

ウェブページの作成については、県立高校では現場の先生方の労力に拠っていると思われるのに対し、私立高校では明らかに、専門業者に外注しているものが多く見られた。ウェブページの作成については、県立高校のようにゼロから現場にたまたま居合わせた教員の技術や能力に頼るのではなく、構成の見直しや、いくらか予算を投入しての、専門知識が無くとも更新すべき情報が更新される枠組みの確立は重要であると思われる。

3 学校ウェブページのあり方

学校ウェブページが本来持つべき機能としては、校外に対する広報的な機能と、校内向けの教材的な機能に分けることができる。今回、各学校のウェブページの閲覧調査では、ほとんどの学校が前者の広報的な役割であることがわかった。それぞれの特徴としては、様々な閲覧対象を想定し、社会一般向けであったり、卒業生と在校生、その保護者向けであったり、中学生や中学校の教員・保護者向けであったりと、それぞれの学校の地域的な関りや学校の状況から、そういったページが作成されているようであった。

広報的な役割を果たす学校ウェブページ

現在の高等学校ウェブページのほとんどが広報的な機能として作成されている。ウェブページを作成する際、掲載すべき内容ばかりに捉われており、誰に対する情報公開かをもう一度見直す必要がある。また、掲載内容の不統一から、今後最低でも県立高校における各学校のホームページによる公開内容を統一する必要性を強く感じる。そこで掲載内容の統一を図るため、最低限掲載すべき必須の基本事項として以下にあげる。

- ・ 校長あいさつ、沿革、教育方針、校章、校歌
- ・ 学校自己評価
- ・ 教員紹介
- ・ 学科・コース紹介、各学科コースの教育課程表、取得可能な資格（専門学科を有する学校のみ）
- ・ シラバス（将来的に）
- ・ 卒業生の進路
- ・ 施設設備紹介
- ・ 制服紹介
- ・ 所在地（アクセス方法・周辺地図など）、問い合わせ先、更新情報

教材的な機能を果たす学校ウェブページ

県内の高等学校では、小中学校と比べ校内向け、および学習に関する情報が公開されていない。教育実践の情報などを公開すると、外部からの批評を得る機会ができる。さらに教員自らの名前と責任のもとで教材や授業実践を公開し、より良い授業作りのきっかけとして位置づける必要を感じた。そのためには、校内でのウェブページを管理運営する組織を設置し、より良い学校ウェブページを作成することが望まれる。

4 ウェブページの更新について

学校ウェブページが更新されていない学校は、教育活動の活発性に欠け、魅力を感じない学校に思われがちである。そういったイメージを打破するためにも、定期的な更新が必要となる。そのためにも各学校できちんとした組織を設置し、その運営と管理を行う必要がある。本調査できちんとした情報を得ることができなかったが、ウェブページの作成を一部の技術を持つ教員に依頼し、ウェブページの管理・運営を組織化していない学校があるように思える。その一部の教員がウェブページを作成し、アップロードしたままで更新されていないという状況も見られた。その原因として考えられることは、校内で組織化されておらず作成した教員が転勤となり、更新されずにそのままの状況となっているのではないかとと思われる。

ウェブページの更新は、それだけ大切なことであり、外部から学校を見られているという意識を十分に持つておく必要があると思う。更新の目安としては、1ヶ月に1回程度でどこかのページが更新されていれば問題ないように思われる。その際、更新履歴を明記し、新しく更新した箇所をはっきりわかるようにする必要がある。

5 校内ネットワーク設置について

本調査では、校内のネットワークに関する事項を閲覧することができなかった。しかし、各学校のウェブページに掲載されている内容から校内をネットワーク化されているように読み取れた。施設設備の紹介で、「本校のパソコン室のどこからもインターネットが使用可能」や「生徒データベースの構築」、「生徒成績データの管理」、「図書館の貸し出し状況をパソコンから見るができる」などから、校内ネットワークが運営されている。しかし、そのネットワークを管理・運営する組織のことがほとんど記述されておらず、組織的に行われず一部のネットワークの知識を有した教員によって管理されているのか、またネットワーク障害発生時における対応はどのような危機管理体制を設定しているのかが不明であった。

校内ネットワークの運営については、今後重要な役割となるため早急な対応が必要であると考え。さらに、生徒個人情報を多く持つ学校では十分なセキュリティ対策を講じなくてはならない。情報の重要性について職員に周知徹底を促す必要がある。

6 まとめ

今回のウェブによる閲覧調査では、各学校のウェブページ掲載内容の不統一性、ウェブページの定期的な更新、校内ネットワークの管理運営体制などの課題が明らかになった。

各学校のウェブページでは、作成した担当者の個性がそのままウェブページに反映されている傾向や、自校のウェブページを作成した担当者が転勤になり、更新することができなくなったというような傾向が見られた。そういったことを防ぐためにも、いくらかの予算を投じてウェブページの作成を専門業者に委託し、ウェブ作成に関する専門的な知識がなくとも、誰もが更新ができるようなものにする必要があるように思われる。

校内ネットワークについては、各学校のネットワーク管理者を中心に運営組織を設置し、校内における運営・管理を行う必要がある。校内のネットワークを安全かつ快適に活用しようとするのであれば、片手間でできるような業務ではない。特にセキュリティ対策については十分な措置を行わなければならない。校内のネットワークに関するガイドラインの見直しと、教員・生徒の情報リテラシーの強化、セキュリティポリシーの確立を早急に校内で協議し、ネットワーク利用に関する意識を高める必要がある。また、各学校のネットワーク管理者を明確にし、各学校のネットワーク管理者同士で相談できる横のつながりを作る必要があるように感じる。それと同様に、教科「情報」の担当者についても各学校が独自に進めているような傾向が

見受けられるため、定期的に担当者が集い、進捗状況や問題点等が話せるような場を設ける必要があるように感じられる。

今後ますます校内のネットワーク化が進む状況の中で、校内ネットワークの管理体制を決して軽んじてはならず、全職員に対する意思徹底を図らなければならない。

学校訪問聞き取り調査におけるまとめ

はじめに

平成16年12月10日から12月22日の間、7日間で県内の高等学校15校（県立11校・私立4校）を訪問し、校内のネットワーク環境の現状について調査を行った。調査対象の15校については、北九州地区4校・福岡地区5校・田川筑豊地区3校・筑後地区3校の普通高校および専門高校とし、地域・校種に偏りがないよう配慮し調査を実施した。

各学校における校内ネットワークシステムの状況

各学校において校内ネットワークの設計に教員が携わっており、特に県立高校では、平成14年度に構築された「ふくおかギガビットハイウェイ」によって各学校にネットワーク管理者を配置し、校内ネットワーク化の推進が図られた。しかし、校内ネットワークの設計および構築においては、県から予算が付き業者へ外注されるわけでもなく、パソコンやネットワークに関して他の教員より詳しい教員によって構築されていたようである。そのため、各学校における校内ネットワークの構築状況に統一性がなく、各学校の状況に合わせたネットワークとなっている。そのため、校内のネットワーク化が進んでいる学校とそうでない学校の格差があり、その状況も様々であった。

1 ネットワークの概要

(1) 構想・設計に携わった職員

各学校における校内ネットワークの設計に携わった職員は、教員という回答が最も多く、次に事務職員という状況であった。特に県立高校では、平成14年度より「ふくおかギガビットハイウェイ」の構築により、各学校にネットワーク管理者を配置し校内ネットワーク化の推進がなされた。それを機に、普通高校では校内のネットワークの構築と教科「情報」を実施するためのパソコン室のネットワーク化が図られていった。そういった校内のネットワークの構想や設計に携わった職員については、県からそのための予算がつくといいこともなく、各現場で対応せざるを得ないといった状況となり、パソコンやネットワークに関して他の教員よりも知識がある教員の手によって構築されていたようである。この弊害として、たまたま各現場にそういった教員が居合わせていた学校については職員室内のネットワーク化が図られたようであるが、そういった教員が不在の学校では、ネットワーク化が十分に進んでいないようであった。

また、専門高校である工業と商業では、「情報」に関する科目が以前より実施されていたこともあり、情報の専門教員が校内ネットワークの設計に携わり、外部業者に依頼するのではなく自分達で構築したといった状況であった。そのため、普通高校よりも校内ネットワーク化が進んでいるように思われた。

私立高校では、各学校の独自予算で校内のネットワーク整備がなされている学校もあったが、そうでない学校も見受けられた。これは、現在のところ校内のネットワークの必要性に迫られていない学校ほどそういった傾向に見られた。

(2) 導入時期

導入時期については、各学校様々といった状況であった。私立高校では平成6年度といった早い時期にネットワークが導入され、少しずつ問題点などを改善しながら再構築されていったという状況であった。次に導入されたのが県立の工業・商業高校で、パソコン室のネットワーク化が図られ、職員用のネ

ットワークが作られていったようである。

県立の普通高校では、ふくおかギガビットハイウェイの導入と普通教科「情報」の実施から、校内ネットワークの導入時期がほぼ同時期で、平成14年度に集中している。また、単位制高校では教育支援システム稼働に伴い、平成10年度頃に導入されている。

(3) ネットワーク接続状況

現在では、今回調査を行った学校全てが職員室および事務室がネットワークに接続されており、進路室や図書室などでは独立したネットワークを構築されている学校が多かった。また、広範囲に接続されている学校では、校内全てネットワークに接続できている学校もあり、教室に情報コンセントが設置され、教員が授業を行う際にパソコンとLANケーブルを持参することにより、教室からもインターネットに接続することができる学校もあった。

2 校内ネットワークの保守・管理

ネットワークの保守や管理を行うための体制については、約半分の学校で分掌や委員会が設置され、そういった部署で管理されているようであった。しかし、そういった部署に配置されている教員は、他の分掌との兼務であり、ネットワークの管理体制が十分とは言い難い状況であった。その部署の業務のほとんどは、ホームページの更新や生徒用パソコンの故障について保守契約業者へ連絡するといった内容であった。

ネットワークの保守等で係りが活動する時間帯については、どの学校も放課後から夜間、または休日に行うといった学校が多く、他の業務との兼務でこのような状況になっているのか、またはネットワークに接続している利用者が帰宅しないと作業ができないのかわからなかった。

3 ガイドラインについて

ガイドラインを作成している学校は、私が想像していたよりも少なく、その内容もネットワークに接続するためのマニュアル的なものが多かったように思われる。

生徒によるパソコン室の使用に関するガイドラインや、職員のネットワークに接続するためのガイドラインなどをきちんと作成し、職員研修などを通じて職員に徹底させる必要があるように感じられた。また、セキュリティポリシーを作成している学校はほとんどなく、ウイルス発生時の対応や不正アクセスが発生した際の対応などについても、きちんと文書化し職員に周知徹底する必要性を感じた。

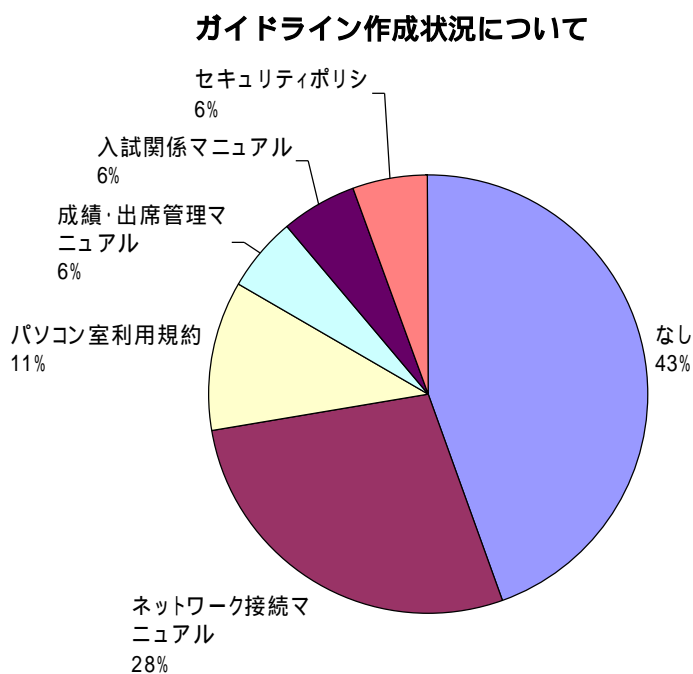


図 1

4 運用例

(1) 職員室および教員用のネットワーク

教員用のネットワークには様々な形態があった。まず、職員室内にサーバを置いて認証用とファイルサーバとして利用し、各自のファイルは共有できるようにしている学校がある。これについては各利用者にユーザ権限を与え、ファイルサーバのユーザしか利用できない箇所しか触れないように設定されていた。それ以外には、職員室内の数台のパソコンを接続し、成績データ入力用として利用されているといった形態や、ネットワークに接続しプリンタサーバしか利用させず、ファイルは各自のパソコンのハードディスクに保存させるといった形態など、何のためのネットワークかわからないような学校も見られた。しかし、どの学校も成績管理の形態については十分に検討されており、学校独自の方法で工夫されていた。教員による成績入力は個人のパソコンから入力できないようにされており、学校に設置されているパソコンから入力しなければならないようにされている学校もあった。

当然のことであるが、全ての学校が生徒用のネットワークと教員用のネットワークを分離しており、VLAN やレイヤ3以上のスイッチ、ルータを用いて生徒用と教員用の独立したネットワーク環境を構築されていた。

(2) パソコン教室

半分以上の学校では生徒各自にIDとパスワードを持たせ、パソコンを利用する際に各自のIDでログインするようにされていた。また、ファイルの保存場所として、生徒用のファイルサーバを設置されていた。生徒用のファイルサーバの利用については、各生徒用パソコンにネットワークドライブが割り当てられており、他の生徒のファイルが見られないように工夫されており、教材配布用のフォルダには共有がかけてあるという状況であった。

インターネットの利用については、ほとんどの学校が自由に使えるようにされており、県立高校のほとんどは、ふくおかギガビットハイウェイに接続し福岡県教育センターで設定されているフィルターを使いフィルタリングされている。そのため、生徒によるインターネットの接続制限がされていた。私立高校や一部の県立高校においても、各学校独自にProxyサーバを立てフィルタリングされていた。

生徒へのパソコン室の開放については、基本的にどの学校も放課後等に教員が監督に就いての開放といったところが多く、生徒だけでの利用といった形態は取られていなかった。また、一部の私立高校では、放課後大学生をアルバイトで雇い監督業務を行わせているという学校もあった。

(3) 校内用サーバ

校内用のサーバの利用状況については、圧倒的にファイルサーバとしての利用が多かったが、一部の学校ではProxyサーバや認証サーバ、DHCPサーバ、メールサーバとして活用されていた。サーバをデータの記憶場所として利用されている学校が多く、このことからネットワークの知識を持つ教員や係りが十分でないことがうかがえた。また、教員用のファイルサーバとして活用されていない学校もあり、ネットワーク構築の不十分さを調査することができた。教員用のファイルサーバとして利用されていない学校では、1台のパソコンのハードディスクに共有をかけて、そこにファイルを保存したり、大容量の外付けハードディスクをネットワーク上に置き、そこにファイルを保存しているといった状況が見られた。

5 ネットワーク管理

(1) 問題点および工夫点

教員用として設置されているパソコンのネットワークに接続するための設定については、校内ネットワークの係りまたは管理者によって設定されているが、個人の教員によって持ち込まれたパソコンの設定については、半分近くの学校では校内ネットワークの係りまたは管理者によって設定されているといった状況であった。また、そういったパソコンの保守や問い合わせについては、知識を持つ教員が対応している学校もあれば、利用者から管理者や係りに連絡があり対応しているという学校もあった。それ以外では、個人所有のものについては対応しないという学校もあった。

個人所有のパソコンの校内ネットワークへの接続許可については、ほとんどの学校が許可されており、その設定は基本的に各自で行うようになっているが、どうしても上手く接続できないものについては、管理者や係りが設定の手伝いを行うといった状況であった。こういったパソコンの設定といった業務について、県立高校では明確にされていない学校が多かった。

そういった業務の工夫点として、私立高校で行われている方法によると、個人で持ち込まれたパソコンを校内のネットワークに接続させる場合、パソコンを事務に持参し、そこで設定をしてもらうといった方法を取られていた。こういったように、ネットワーク接続業務の窓口を一本化する必要性を強く感じた。

(2) ウイルス対策とセキュリティについて

半分近くの学校では、ウイルスバスターコーポレートエディションが導入され、校内に設置されたパソコンにインストールされていたり、それをサーバに置いて利用者がネットワークに接続する都度、ファイルのアップデートや更新を自動で行うといった方法を取られていた。

このコーポレートエディションには、Client/Server Suite エデュケーションパックがあり、校内で1年間無制限で使用できるようになっているため、校内に設置済みのパソコン（教育目的利用）すべてにインストールすることができるが、校内に持ち込まれた個人所有のパソコンについてはインストールすることができないように規定されている。（トレンドマイクロ

持込パソコンへのウイルス対策について

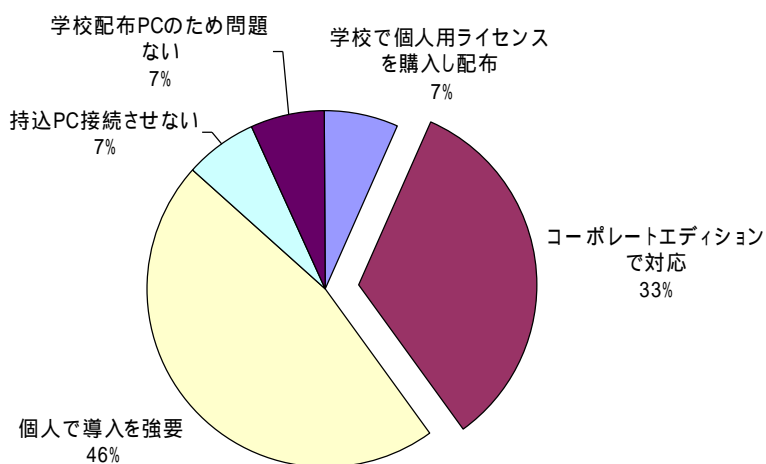


図2

ウイルスバスターコーポレートエディション エデュケーションパックに関する FAQ 参照 <http://www.trendmicro.com/jp/purchase/edu/faq.htm#040>)

このことを十分理解されている学校もあったが、理解されていない学校が何校も見られ、訪問時に個人所有のパソコンにインストールできないことをお知らせしたところ、知らなかったという返答があり早急に対応する必要があった。

それ以外の学校では、個人所有パソコンへのウイルス対策ソフトの導入強要について、どこも苦労されていたが、一人ひとりのパソコンのチェックまではできていないという状況であった。

ウイルス発生時の対応については、全体にアナウンスして各自で確認・対応してもらったり、該当者を

巡回戦術で探しワクチンソフトを配布するといった手立てを行われていた。しかし、半数近い学校では、ウイルス対策ソフトに頼りきっているといった状況であった。また、個人用のインターネットメールの使用を禁止したりしている学校もあった。

ウイルス対策とセキュリティについては、どの学校も十分な対応ができていないように感じられた。これもウイルスに対するセキュリティポリシーが作成されていないということが原因であり、管理者やネットワーク運営組織の係りに十分な知識が不足しているように思われた。

(3) ファイルサーバのバックアップについて

ファイルサーバを設置されている学校では、バックアップが定期的に行われている学校と、サーバ上でミラーリングされているため、ほとんどバックアップを行わない学校とに大別された。

また、バックアップについても、タイマーで自動バックアップを行っている学校と、手動で行っている学校があった。バックアップを行っているファイルについては、いずれも生徒の成績データが保管されているもので、生徒作品などの生徒用ファイルサーバについてはバックアップされていなかった。

バックアップについては、ファイルサーバ内の異なるドライブに行うといった学校が多く、他のサーバへバックアップされている学校が少なかった。ここでも、ファイルの危機管理について管理者が十分に考慮していないのか、知識が不十分のように思われた。

ファイルサーバのバックアップについて

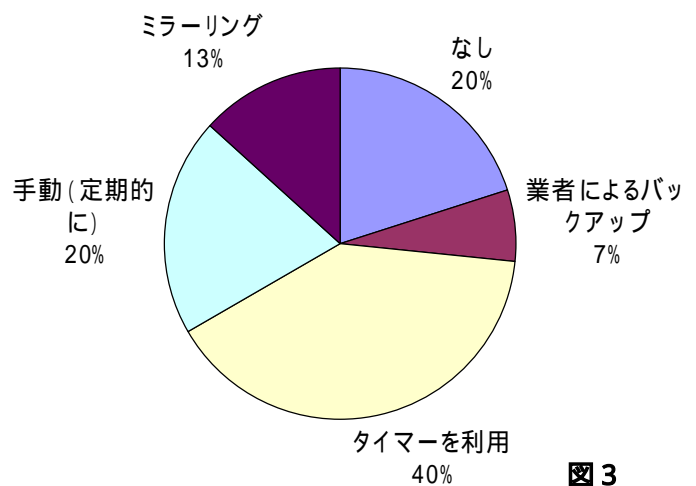


図 3

6 校内ネットワークにおける問題点と改善策

校内ネットワークにおける問題点として、以下のようなことを聞き取った。以下のような問題点については、県からの予算措置を行っていただくか、あるいは各学校で努力するしかないように思われる。

- ・ 生徒実習用パソコン室のパソコン更新に伴い、新たにサーバを追加導入したが、導入されたままの状態となっており校内のネットワークを最新の状態に再構築したい。
- ・ 職員用のファイルサーバがあまり活用されていないため、ファイルサーバ活用推進のための研修会を行う必要がある。
- ・ 無線 LAN のセキュリティを高めたい。現在 2 系統のネットワークに 1 台のパソコンを接続している利用者がいて、その 1 台のパソコンがブリッジの働きをしてしまい、2 系統のネットワークが接続されるといったことが度々起こる。そのためにも利用者に対するスキルアップと利用モラルを身につけるための研修会を行う必要がある。
- ・ 教員用のパソコンの OS が異なり、設定が困難である。
- ・ ネットワークに関する専門の教員がいないため、専任の教員が欲しい。
- ・ サーバの OS が様々で管理が難しい。(OS 導入の予算がない。)
- ・ 管理者からの連絡が徹底できていない。

校内における教員用パソコンの状況

各学校におけるパソコンの設置状況においては、教員数に対して十分と言える台数が設置されていなかった。そのため、どの学校でも個人所有のパソコンが多く持ち込まれていた。そのパソコンの持ち込みや管理に関する規定、校内ネットワークへの接続について、県が予算措置を行っていないため具体的な指導ができないといった状況であった。そのため、各学校の自由な解釈で学校に持ち込まれ、校内のネットワークに接続されているという状況であった。個人所有のパソコンを校内のネットワークに接続することで、ウイルスをはじめデータの校外持ち出しなど、様々な問題が浮上してきた。

1 教員用のパソコンの実態

各学校に設置されている教員用のパソコンについては、各学校で台数の差が目立った。一番多かった回答は、職員室に数台しかなく、成績処理などで待ち行列ができるといった状況であった。こういった状況であることから、個人のパソコンを学校に持ち込むといった状況が生まれてくるように思われた。また、各自のデータの保管場所が確保されていない学校については、デスクトップにデータを貼り付けられ、整理するための業務まで必要になるとのことであった。また、ファイルサーバに教員各自のフォルダを用意していても使用されていない、またはファイルサーバ内がゴミ箱状態になっているといった学校もあった。

学校設置の教員用パソコンについては、すべての学校がネットワーク接続されており、インターネットの閲覧も自由にできるといった状況であった。

2 利用形態

利用形態については、教員に対してIDとパスワードを配布し、教員用のパソコンを使用する際にログインし使い終わったらログアウトするといった学校もあれば、職員で共通したIDとパスワードを使い、パソコンを起動したらログオンした状態で複数人が使用するという学校もあった。

教員用パソコンの利用形態について

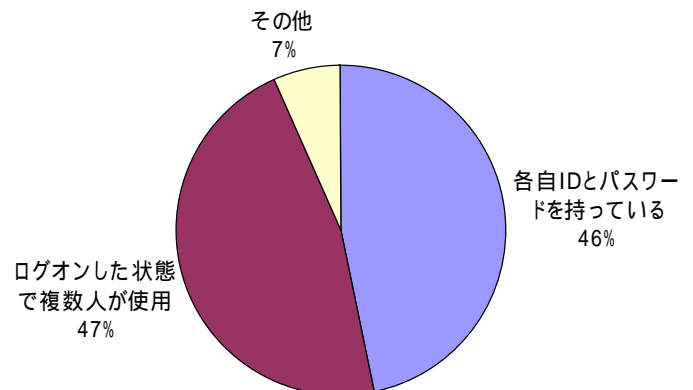


図4

3 個人所有のパソコンの持ち込みについて

個人所有のパソコンの持ち込みについては、すべての学校で許可されていたが、校内のネットワークへの接続には制限を設けている学校があった。個人所有のパソコンが持ち込まれ校内ネットワークに接続するための要因としては、授業の教材を作成しネットワークプリンタで印刷するために利用されていることが多く、必ずしもファイルサーバにデータを保管し、データ管理を行ったりファイルを共有するためのものではなかった。また、一部では成績データを入力するためにネッ

個人所有パソコン持込率(校種別)

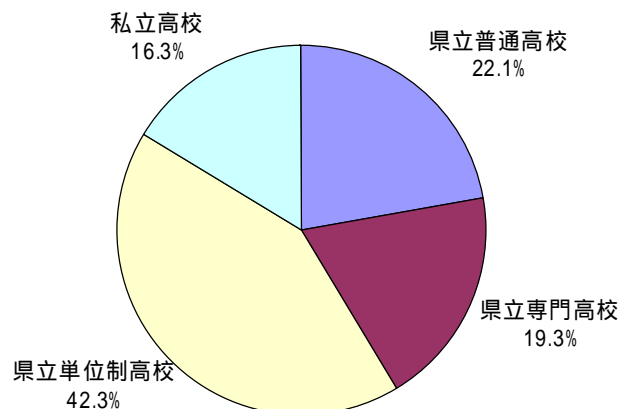


図5

トワークに接続するといった状況であった。逆に、一部の私立高校では、職員にパソコンを配布しているにも関わらず、使い勝手が悪いや使いたいソフトがインストールされていないことから、個人のパソコンを持ち込んでいるといった状況をうかがうことができた。

今回調査を行った学校全体に対する教員のパソコン持ち込み率は、40.6%となり、そのうち校内のネットワークに接続しているパソコンが約 60%であった。そのうちのほとんどが、プリンタを使用する目的で接続されており、ファイルサーバやインターネットを利用するためにネットワークに接続しているパソコンの台数は更に下がるであろうと思われる。

4 問題点および改善策

個人所有のパソコンを校内に持ち込むことについては特に問題ないが、そのパソコンを校内のネットワークに接続することで様々な問題が浮上してくる。まず、パソコンを持ち込んだ本人が、校内ネットワークへの接続設定を行うことができればよいが、その設定ができないためネットワーク管理者や係りの手を煩わすことになる。また、個人所有のパソコンを持ち込まれることにより、校内のネットワークにウイルスが侵入する可能性が出てきたり、校内のデータを校外へ持ち出される心配も出てくる。しかし、校内の重要データに対するセキュリティと、そういったデータを外部に持ち出せない仕組みをどの学校も施されていたためその心配はないように思える。最良の策としては、個人所有のパソコンを校内のネットワークに接続させないことが一番であるように思えるが、教員用のパソコンの設置台数からするとそうともいえない状況であった。

情報教育の実施状況

高等学校指導要領の改訂により、教科「情報」が平成15年度から年次進行により段階的に導入され、各学校における現在の実施状況について調査を行った。まず、普通高校および普通科での普通教科「情報」では、「情報A・B・C」の選択を各学校の裁量や生徒の状況に合わせ選択することができる。そこで、それぞれの選択理由を調査したところ「情報A」については、情報に関する基礎的な内容、実習中心で生徒の状況に合っている、リテラシーの向上を目指すため、といった回答であった。「情報B」では、コンピュータサイエンスや工学の基礎、認知心理学の内容であったため、「情報C」では、課題研究で発表を実施するため、「数学C」での図形作成の実習ができるからといった回答を得ることができた。

その他に、「情報」の授業担当者における他教科との掛け持ち状況、パソコンの台数についての状況、生徒の授業に対する反応について聞き取ることができた。

1 現在の実施状況

高等学校学習指導要領の改訂により、教科「情報」が平成15年4月1日から年次進行により段階的に適用され、各学校で「情報」の授業が行われている。今回訪問した15校のうち、普通教科「情報」を実施している学校に対して、A～Cのどれを実施し、どういった理由で設定したのかを伺った。また、専門高校のうち工業高校は、「情報技術基礎」と「プログラミング」で、商業高校は、「情報処理」と「プログラミング」で専門教科「情報」の代替をされていた。

(1) 普通教科「情報」

普通高校および普通科での普通教科「情報」の授業では、「情報A・B・C」の選択を各学校の裁量

や生徒の状況に合わせて、自由に選択することができる。
そこで、情報A・B・Cの実施割合を算出すると以下のようになった。

- ・情報A : 62%
- ・情報B : 15%
- ・情報C : 23%

普通教科「情報」実施状況

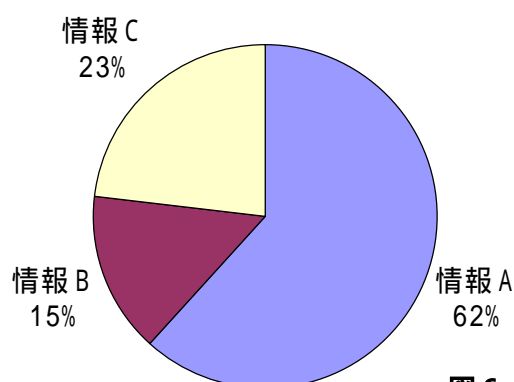


図6

(2) 「情報A～C」を選択した理由について

「情報A」

- ・以前より「情報流通基礎」を実施しており、その内容に最も近かった
- ・生徒の実態から、生徒が最も入りやすいと思われた
- ・情報モラルやソフトウェアの基本操作など、情報に関する基礎的な内容と思われた
- ・生徒が最も興味を持つ内容と思われた
- ・パソコンを多く使用する科目であったため
- ・実習中心の内容が、生徒の状況に合っていると判断した
- ・中学校の地区によって生徒のスキルに差があり、「情報C」を実施するには難しい
- ・リテラシーの向上を目指すため

「情報B」

- ・コンピュータサイエンスや工学の基礎、認知心理学の内容であった
- ・学校独自で検討している内容に最も近い

「情報C」

- ・課題研究で発表を実施するため、その内容に最も近い
- ・数学Cでの図形作成を手書きで行うには困難なため、N88Basicで図形作成を行わせるため

2 指導上の問題点とその改善策

(1) 担当者について

専門高校では、「情報」の授業に掛かる専門の教員が配置されているが、普通高校では、ほとんどが他教科との掛け持ちといった状況で、専属で指導にあたるという形態は取られていなかった。

(2) パソコンの台数について

専門高校では、パソコン教室が多い学校で7教室という学校もあったが、普通高校ではほとんどが1教室(42台)であった。しかし、訪問した80%の学校ではパソコンの台数は十分ということであった。ほとんどの学校は、1年次に2単位で実施しているため、「情報」の授業を全てパソコン教室で実施したとしても、1年生が8クラスであれば、16時間パソコン教室が利用されるということになる。そのため、十分といった回答を得られたように思われる。逆に、専門高校において不十分といった回答が多かった。

(3) 授業を受けての生徒の反応

「情報」の授業は、入試科目と関係ないことから、生徒の取り組み状況について危惧していたが、それとは逆に興味を持って取り組む生徒が多く、中には検定にチャレンジするといった生徒もいるということを知ることができた。しかし、入学してくる生徒のパソコンの活用能力に関するスキルの差が大きく、スキルの高い生徒にとっては遊びの延長であるようにも伺った。その解決策として、ティームティーチング(TT)制を導入し、各生徒に応じた対応を行っている学校も見られた。また、一部の学校では、大学生をティーチングアシスタント(TA)として、専属の教員3名プラス大学生(TA)1名の、合計4名で実施されている学校もあった。

現在、入学してくる生徒のスキルの差があり、指導するのが困難という意見もあったが、中学校学習指導要領の改定により、中学校での情報教育が平成14年度の入学生から導入されたため、来年度(17年度)の高等学校への入学生からそういった問題も解消されると思われる。

遠隔授業(テレビ会議等)の取り組み

福岡県の小・中学校では、遠隔授業やテレビ会議を積極的に活用し、学校間交流や共同学習を実施している学校が多い。しかし、高等学校でその取り組みがほとんどなされていない。その原因については、授業時間を確保することが精一杯で時間的な余裕がないという回答が最も多かった。その他としては、実施したことがある教員が身近にいないため、イメージが湧かないといった回答であった。

遠隔授業の必要性については、直接行くことができないところとの交流や、大学や専門学校からの遠隔授業の実施導入について、半分以上の学校が必要性を感じるということであった。

1 遠隔授業の実施について

遠隔授業の実施状況について伺ったところ、1校を除いた14校では実施したことがないという回答であった。その14校に対して、その必要性について尋ねたところ、直接行くことができないところとの交流や、大学や専門学校からの遠隔授業を導入したいなどから、半分の学校が必要性を感じるという回答であった。さらに、遠隔授業の実施導入について尋ねたところ、実施したいという回答が半分であった。その理由としては、以下のような内容が挙げられた。

- ・中学校に出前授業として活用したい
- ・外部からの教育協力をお願いしたい
- ・生徒の学習への動機付け
- ・総合学習で意見交換やリポート大会などを実施したい
- ・eラーニングの実施
- ・教員として資質を伸ばすために様々な経験をしたい
- ・ネットミーティングなどを実施したい

また、実施していない理由として、

- ・学校の機器の整備が整っていない
- ・遠隔授業に関する知識がない
- ・準備を行うための時間的な余裕がない
- ・実施したことがない
- ・外部向けで宣伝効果を期待しているように見える

といった意見をいただいた。

2 高等学校で活用されない理由について

福岡県の小・中学校では、遠隔授業やテレビ会議を積極的に活用し、学校間交流や共同学習を実施している学校が多いが、高等学校による活用が積極的でないように思われたため、活用されない理由について伺った。一番多かったのは、時間的な余裕がないという回答で、次に実施したことがないためイメージが湧かないや、テレビ会議を行うための機器が整備されていないという状況であった。その他の回答としては、高校間での交流がない、相手の探し方がわからない、普通教室で行えない、回線の速度が遅く使用に耐えることができない、良さがわからない、生徒は携帯電話で体験しているといった回答であった。

個人情報保護について

各学校において、重要書類の取り扱いや生徒の成績データなどについては、しっかりとした管理がなされていた。しかし、個人所有のパソコンの持ち込みや個人の記録媒体の取り扱いについては、十分な管理ができていないように思われた。特に生徒の成績データにおいては、各授業担当者が生徒を評価し、結果として算出された最終的な成績というデータを学校が十分に管理しているのであって、その前段階である考査の成績や授業における記録などは教員個人が管理している。そういったデータが個人所有のパソコンや記録媒体の中に保存されて、校外に持ち出され盗難などに遭うというケースが考えられる。そのような状況がこの調査によって明らかになった。

1 重要書類の取り扱いについて

(1) 生徒指導要録

全ての学校で持ち出しが禁止されており、特例（管理職の許可）も認められていない。また、どの学校も生徒指導要録を担任が記入する時期が決められており、その期間以外は金庫等鍵がかかる場所で保管されている。

(2) 生徒指導票

生徒指導票は、各学校でばらつきがあった。持ち出しを禁止している学校では、担任が家庭訪問等行う際に、生徒自宅地図などをコピーするといった工夫がなされていた。特に指定されていない学校では、原則禁止という学校もあったが、それ以外の学校では生徒指導票を持ち出す際に十分注意している（移動の途中、どこにも立ち寄らないなど）とのことであった。また、取り扱いの注意として、管理職からアナウンスがなされていた。

(3) 生徒成績データ

全ての学校で持ち出しを禁止しているが、あくまで観点別評価により平常点を加味した後の成績であ

生徒指導票の持ち出し

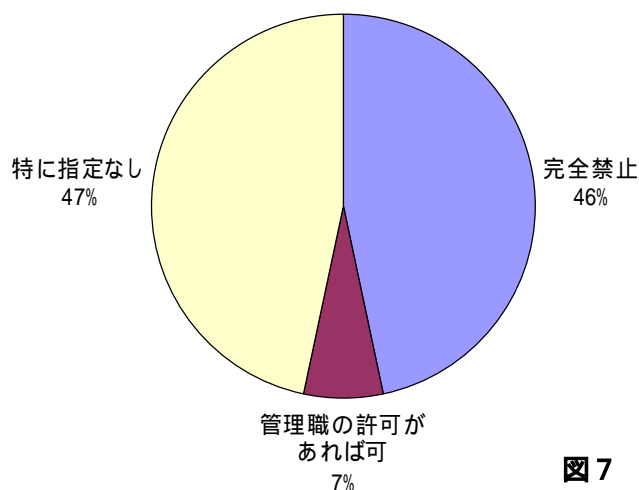


図7

り、考查点の成績については個人が管理しており、それが個人情報流出の原因と考えられる。

また、ほとんどの学校では、成績管理システムとしてデータベース化されており、全てのデータが入った成績データを個人の記録媒体に保存して持ち出せないといった状況であったが、それでも十分な管理ができているようには思えなかった。

(4) 考查等の解答用紙

考查等の解答用紙では、勤務時間内に採点できないことから、自宅に持ち帰り採点するといった学校が多く見られた。持ち帰る際は、十分注意するよう管理職からアナウンスがあり、各教員も帰宅途中にどこにも立ち寄りないようにしているとのことであった。

持ち出しを禁止している学校では、採点時間への配慮として成績締切日を遅らせ、学校で採点できるように工夫されていた。しかし、学校では他の業務がありなかなか採点する時間を確保できないことから、勤務時間外に遅くまで学校に残り採点を行ったり、休業日に出勤し採点を行うという状況であった。

考查等の解答用紙の持ち出し

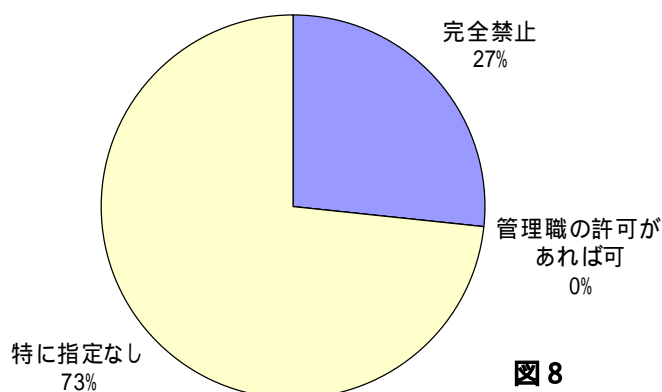


図 8

2 個人所有のパソコンの持ち込みについて

上記でも述べたように、個人のパソコンを学校に持ち込み、校内のネットワークへ接続することに関しては、ほとんどの学校で許可されていた。しかし、使用者のデータを保存する場所は特に指定されておらず、校内の業務に関するデータも各自のパソコンに保存されるケースが考えられる。そのパソコンについては、個人のものだからということで、持ち帰りについては特に指定されていない。こういったことから、個人情報流出する可能性が考えられる。

このことについては、早急にセキュリティポリシーの作成や、データの持ち帰りに関する規約などを作成し、職員に対する研修会を行い、周知徹底する必要があるように思われる。

3 システム管理者について

(1) システム管理者の業務について

全ての学校のシステム管理者は他の分掌や係りと兼務で、それ以外にも多くの業務を行っていた。システム管理者が行っている業務としては、情報システム構築と今後の運用についての検討や LAN の整備、ネットワークの保守・管理、機器トラブルの対応、ウイルス監視、プロファイルのログ確認、個人所有パソコンの対応、設定の補助、ファイルサーバのバックアップ、委員会開催の呼びかけ、ネットワーク保守、ドメインへ参加のマニュアル作成、年度初めのデータ入力というように、かなり多くの作業を行われていた。このことから、システム管理者については、負担軽減しなければ校内のネットワークに関する業務が十分に行えないように思える。

(2) 校内研修会について

ほとんどの学校が、年度当初に転入された職員に対してネットワーク接続や利用方法、ログイン方法、

成績入力の方法などについての研修会を実施されていた。それ以外にも、全職員を対象として定期的にソフトの使い方をはじめ、セキュリティや著作権、出席・成績入力方法、情報機器の授業での活用法などについて実施されていた。

(3) 担当者の異動に対する対応について

システム管理者が転勤することにより他の職員に引継ぎを行わなければならないが、伝える内容が多く時間的制約もあり、それをマニュアル化することが困難であることから、異動時の対応についてはほとんどの学校ができていないという状況であった。引き継ぐための工夫として多くの学校が行われていたことは、システム管理者としての作業を行う際、一人で行わず委員会のメンバーやその業務に携わっている職員と一緒にいき、いつでも引き継げるような環境を作っているという状況であった。

(4) 運用・管理で期待されること

全ての学校のシステム管理者に「システム管理者への期待」について伺ったが、半分以上の学校が校内ネットワークシステムの安定稼働に重点を置いており、セキュリティ面の強化と答えた学校が少なかった。こういったことから、教員における個人情報保護についての危機意識が低かったように感じられた。

また、普通高校では、専門教科が普通科目という教員がほとんどで、システム管理者として専門的な知識が十分でないことから、管理者という専属の人員を配置して欲しいといった意見を聞くことができた。

開発したシステムの有用性について

各学校への訪問の際、15校に対して私が作成したシステム（登録端末へのDHCPによる自動アドレス割り当て機構）を紹介し、各学校での有用性または必要性について調査を行った。その結果、図9のようになった。

1 必要と答えた学校（4校：県立3校、私立1校）

必要と回答していただいた学校では、校内ネットワークへの接続設定を手動で行っているか、あるいはDHCP機能を用いて自動でIPアドレス等を配布しているため、配布先のパソコンが把握できないという問題点を抱えていた。そこで、私が作成したシステムを紹介させていただいたところ、非常に興味を持っていただき、Linuxサーバの導入についても検討したいというご意見をいただくことができた。この4校のネットワーク接続設定の状況および、その問題点については、所属校と非常によく似た状況であった。

2 必要ないと答えた学校（6校：県立4校、私立2校）

必要ないと回答頂いた学校のネットワークへの接続設定は様々な状況であった。そのうちの5校は、他校

と比べ進んでいると思われ、現在のままで不自由していない、または私の設計したシステムと同じような

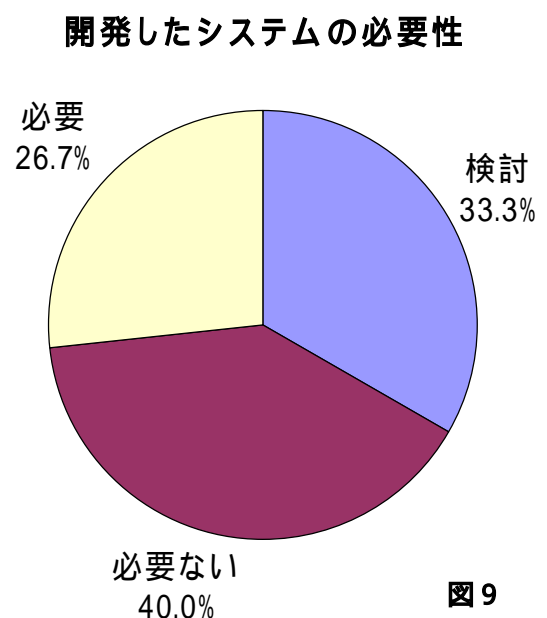


図9

ことが可能なシステムを導入しているということであった。残りの1校については、現在個人所有のパソコンを校内のネットワークに接続させていないため必要ないとのことであった。

3 検討と答えた学校（5校：県立4校、私立1校）

検討とは、今後の検討課題ということであり、5校のうちの4校については、他校と比べ比較的校内ネットワークの構築状況が遅れているといった学校であった。そのため、システム自体には興味を持っていただくことができたが、Linuxサーバの導入については考えていないといった回答であった。また、校内のネットワークの構築がまだ十分でなく、登録端末への自動アドレス割り当てについては今後の話といった意見を聞くことができた。その他の1校は、現在固定IPアドレスを割り当てているため、そういったシステムを導入するかについて今後検討したいといった回答であった。

このシステム（登録端末へのDHCPによる自動アドレス割り当て機構）については、本研修において開発したものであり、この研究のまとめ（資料）にプログラムコードと構築手順書、使用説明書を収録させていただいている。それを見ていただき、必要とされる学校については導入していただければ幸いである。

第2章 校内ネットワーク接続技術

校内ネットワークの利用者およびコンピュータを管理するために、多数のパソコンから構成される情報システムにおいて、利用者が属するグループに応じてアクセス権限を設定できる利用者管理技術に関して調査を行い、その導入について検討を行った。ここでは、Windows ネットワークにおける利用者管理方式であるワークグループ、ドメインネットワーク方式を取り上げた。

Windows は、今まで専門的な知識がなければ不可能だったネットワークの設定などを可能な限りユーザから隠蔽し、ネットワークに関する深い知識を持たないユーザでも、気軽にネットワークを使えるようにした。そういった「Windows ネットワーク」の仕組みについて調査を実施した。

次に、単一の LAN に仮想的に複数のネットワークを実現する VLAN 技術について、調査および校内 LAN への導入とその効果について検討をおこなった。学校で校内 LAN を構築する際、校内のネットワークを生徒用と職員用のネットワークに分離しなくてはならない。その手法としてネットワークアドレスで分離するという方法も考えられるが、スイッチを用いて単一のネットワークを職員用 LAN および教室用 LAN（生徒用）として利用する手法において、特に両者の相互接続を条件付きで実現する手法について検討しそのまとめを行った。また、VLAN の構築例として所属校の校内ネットワークへの導入例を作成した。

Windows ネットワーク

Windows ネットワークは、OS をインストールする際にホスト名とワークグループ名の設定さえすれば構築できる。極端に言えば、Ethernet ケーブル (LAN ケーブル) をつなげるだけでネットワーク環境が構築できる。これは、Windows 独自のネットワークプロトコルを使って、接続マシン同士が互いに通信できる環境が整えられるためである。このシンプルさが、Windows ネットワークの基本といえる。

こうして相互につながった Windows マシンは、「マイネットワーク」アイコンをクリックすることで一覧表示され、ここで表示されるコンピュータの名称は「NetBIOS 名」と呼ばれている。

これで、接続マシンでファイル共有が設定されていれば (アクセス権限があれば) ファイル共有が簡単に行えるようになる。また、共有プリンタもその設定はウィザード形式で行えるので利用は簡単である。こうしたファイルやプリンタ共有は、アプリケーション層で動作する SMB (Server Message Block) と呼ばれるプロトコルによって可能になっている。

SMB は、マイクロソフトが開発したプロトコルであり、この仕様は公開されているので、現在 UNIX 系 OS の「Samba」と呼ばれるソフトウェアを使えば、UNIX マシンも Windows ネットワークに参加できるようになっている。



このように NetBIOS 名を持つホスト同士を接続するだけで利用できる Windows ネットワークを、「ワークグループ」という。ワークグループは、各マシンごとに管理されたユーザ名とパスワードといったユーザ情報を元にリソース (ファイルやプリンタ) の共有を行なう。ワークグループはドメイン環境と異なり、専用のサーバを必要としない。ただし、各コンピュータの名前 (NetBIOS 名) を確認 (名前解決) するための仕組みが必要である。これを提供するマシンが「マスタブラウザ」 (本校ではサーバとしている) である。

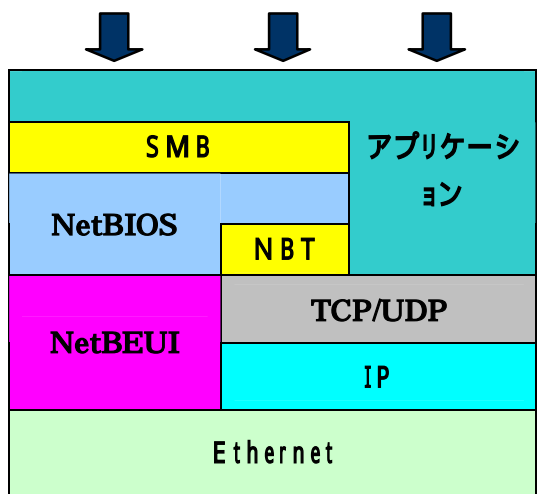
マスタブラウザは、一定のルールに従って選ばれたワークグループ内のマシンが担当する。マスタブラウザは 12 分ごとにブロードキャスト通信を行い、ワークグループ内にどんなマシンが接続されているかという情報を収集する。そこで得られた情報を元に、各コンピュータの名前とワークグループ名のリストを作成しているのである。したがって、同一ブロードキャストドメインであれば、特定のサーバを必要とせずに、Windows ネットワークを運用できる。つまり、本校の校内ネットワークではワークグループ (教師用と生徒用) ごとに Windows ワークグループを形成し、Windows マシン同士がファイルやプリンタを共有できるようにしているわけである。

前に述べた「マイネットワーク」アイコンをクリックすると、接続マシンの一覧が見えるが、これはそのコンピュータがブロードキャストを送信し、それに対してマスタブラウザが収集したリストを提供するようになっている。

マスタブラウザは、校内ネットワーク内で最初に起動したマシンがなるようになっている。これは、「Server系 OS > クライアント系 OS」という優先順位に基づく。たとえば Windows 2000 であれば、Windows 2000 Professional よりも Windows 2000 Server が優先的にマスタブラウザになる。また、OS は最新バージョンのものが優先されるので Windows2000 よりも Windows XP が優先される。したがって、最初に Windows 95 を搭載したコンピュータがマスタブラウザになっていても、次に Windows 2000 を搭載したコンピュータが起動すれば、そちらが優先的にマスタブラウザとなる。また、同じ OS であれば、NetBIOS 名のアルファベット順で選ばれる。

このように本校の校内ネットワークでは、自動的にマスタブラウザが必ず 1 台用意されるが、同一ブロードキャストドメインで 32 台以上のコンピュータが接続されている場合は、33 台目のマシンが 2 代目のマスタブラウザになる。

このマスタブラウザの仕組みにより、Windows ネットワークのワークグループでは、簡単にネットワークが構築できる。これは Windows 独自のネットワークプロトコルである。Windows ネットワークはもともと、「NetBEUI (ネットビュー)」と呼ばれる独自のプロトコルを利用し、BIOS (Basic Input Output System) の機能拡張プログラムである「Net BIOS」を介して通信を行っていた。これらのプロトコルは OS のインストール時に自動的に組み込まれるので、Windows マシン同士であれば接続が簡単にできるようになっている。しかし、NetBEUI をベースとしたワークグループには、いくつかの問題点がある。例えば、アクセス権をマシン単位で設定しなければならない。また、マスタブラウザがうまく機能しないこともある。さらに、マスタブラウザがブロードキャストを頻繁に流すため、ネットワークの効率も悪い。



現在は、TCP/IP を使ったネットワークが主流である。NetBEUI は「小規模な部内ネットワーク」を想定したもので、IP のようにルータを越えるための「中継機能」を持たない。そこで現在では、下位層に TCP/IP を使った「NBT (NetBIOS over TCP/IP)」がメインで利用されている。これにより、Windows ネットワークは、リソースやユーザ情報を一括で管理したうえで複数のサブネットをつなげて利用することも可能になっている。それが「ドメイン」である。

Windows ネットワークのドメイン環境では、ワークグループと異なり専用のサーバで、共有リソース、ユーザのアクセス権限、接続ホストを一括管理する。このサーバは「ドメインコントローラ」と呼ばれる。ドメインコントローラは、ドメイン環境の「要」として、ドメイン全体で最低 2 台以上で運用され、Windows 2000 Server 以上の Windows が使われている。

ドメインのメリットは、職員室にはないパソコン室の高価なカラーレーザープリンタなどを学校内で共有できることである。そういったプリンタを共有サブネットに置いておけば、複数のパソコン教室からはもちろん、職員室や事務室からも利用できるようになる。また、ユーザ情報を一元的に管理することもできる。ワークグループのようにホストごとに「このユーザはアクセスできるが、あのユーザはできない」といった不具合を解決できる。

このユーザ情報は、管理者によってユーザごとに登録されたユーザ名とパスワード (ホスト単位で設定する

ユーザアカウントとは別のもの)である。ユーザがコンピュータにログオンする際には、まずドメインコントローラにユーザ情報が照会される。ユーザ名とパスワードが正しければログオンでき、各ユーザに与えられた「アクセス権限」で、共有ファイルやプリンタが利用できる。

また現在の Windows ネットワークでも、TCP/IP を利用した NBT が使われている。大規模な環境では、複数のブロードキャストドメインでネットワークが構築されており、NetBIOS 名を IP アドレスとマッピングして、TCP/IP ベースで管理できると便利である。そこで、NetBIOS 名と IP アドレスの名前解決を行なうために、WINS (Windows Internet Name Server) という仕組みも用意されている。

WINS は、TCP/IP ネットワークでいうところの「DNS」の役割を果たす。IP アドレスと NetBIOS 名の解決のために、ドメイン環境では WINS も導入されているケースがほとんどである。WINS は、現在校内ネットワークの主流である TCP/IP ネットワークと Windows ネットワークを相互運営するうえで、非常に重要な機能を提供している。

マイクロソフトの最新 OS である Windows XP は、TCP/IP ネットワークを前提に作られている。NetBEUI は、デフォルトではインストールされない。また、マイクロソフトは、Windows2000 までで NetBEUI のサポートを打ち切っている。Windows XP では、NetBEUI は「非サポートプロトコル」となっている。つまり、今後の Windows ネットワークは、これまでのように「TCP/IP を追加する」というスタンスではなく、最初から TCP/IP を利用する形になっている。

これまでの NetBEUI を使った Windows ネットワークは、主に Windows NT 時代からネットワーク環境を利用しているユーザが使っているところも多い。そこで Windows XP では、あとから追加インストールをして、これまでの Windows ネットワークにも参加できるようになっている。Windows XP では、従来の「TCP/IP」と「NetBEUI」の位置付けが、全く逆になっているというわけである。

ワークグループとドメインネットワーク

ネットワーク上に複数のコンピュータが存在すると、アクセスしたい相手を示すために名前を付ける必要がある。つまり、ネットワーク上に接続されているコンピュータにそれぞれ名前をつけて区別するという必要がある。コンピュータに名前を付けることで、どのコンピュータにアクセスしたいのかがはっきりとわかる。しかし、多くのコンピュータがつながっていた場合は、その名前を探すのに時間もかかり非常に不便であり効率もよくない。そこで、ネットワークをグループ分けする方法があげられる。

ネットワークのグループ管理には、大きく分けてワークグループで管理する方法とドメインで管理する2つの方法があり、その方法について詳しく述べていきたい。

ワークグループ

ネットワークで作業を行うコンピュータに、ワークグループ名をつけてグループングすることで、管理をやすくしようというのがワークグループの考え方である。

1 ワークグループの特徴

(1) 独立した SAM (Security Account Manager) データベースをもつ

それぞれのコンピュータごとに専用の SAM データベースを持ち、ユーザアカウントやグループアカウント情報を構成していく。すなわち、所属するコンピュータが独立した存在として、それぞれが資源の管理を行う。各コンピュータの管理をユーザが担当するために、ネットワーク管理者が不要である。

(2) 分散型のリソース管理を行う

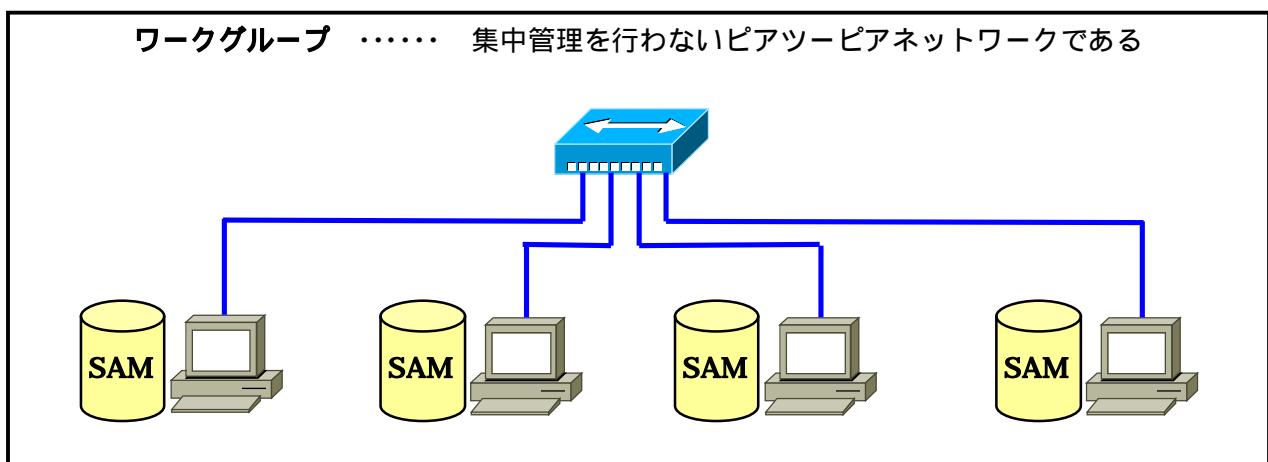
リソース管理やユーザ認証は、それぞれのコンピュータごとで実行される。

(3) 容易で低コストな構築

ワークグループ環境では、サーバを必要とせずクライアントコンピュータだけで構築が可能である。また、構築も容易かつ安価でできる。

(4) 小規模環境向け

分散型のリソース管理を行うため、ユーザ数やクライアントコンピュータの数が増加すると管理がだんだんと困難になる可能性がある。よって、ワークグループに属するコンピュータを同じ設定にするには、全てのコンピュータを設定しなければならない、変更が生じたら全てのコンピュータに同じ設定を行わなければならない。



ドメイン管理

ドメイン管理はユーザを一元管理するために専用のサーバが必要となる。ドメインを設定することにより、ネットワークのユーザアカウントやセキュリティの原則を一元的に管理することができ、個々のコンピュータでこれらの管理を行う方法（ワークグループ）に比べて、ネットワーク管理の効率化が図れる。

ネットワークに接続しているそれぞれのユーザは一度認証を受けると、どのコンピュータへアクセスしてもパスワードを要求されることなく作業を続けることができる。

しかもユーザ管理を一元化しているため、ユーザの権限変更等が非常に簡単になり、信頼性も高まる。

1 ドメインの特徴

(1) ドメイン情報を保持する Active Directory データベース

ドメインの情報を保持するためにアクティブディレクトリが必要である。

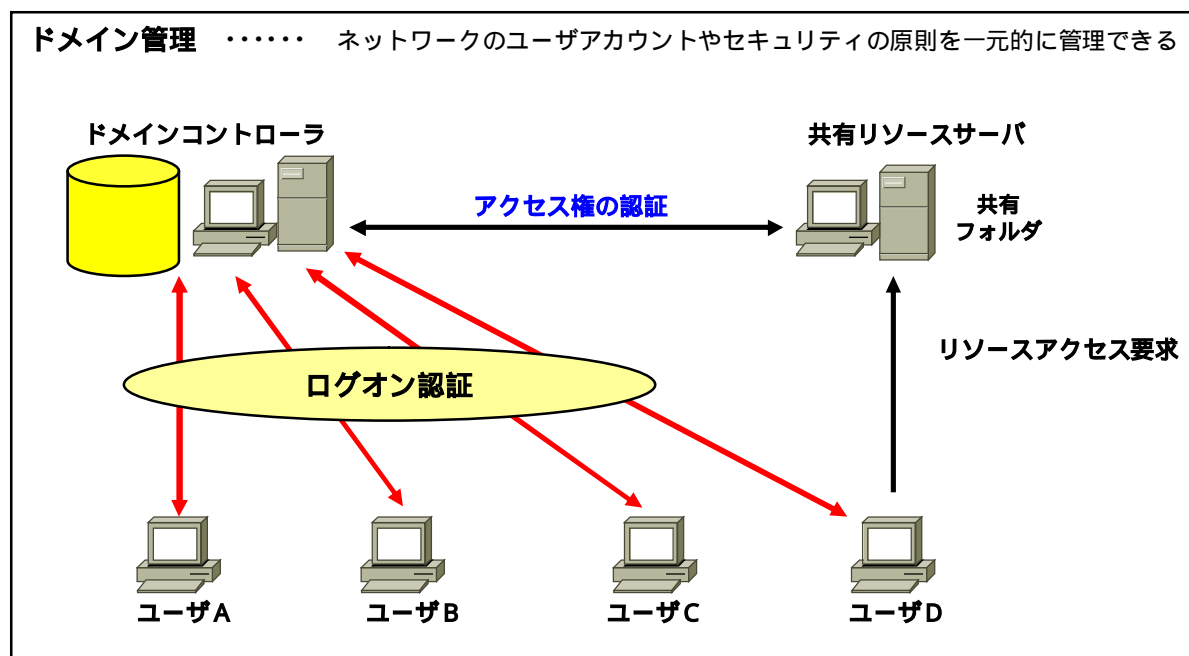
(2) リソースやアカウントの集中管理

リソースやアカウントを集中管理することが可能である。

(3) 高い拡張性

(4) Windows 2000 Server 以上の製品が必要

ドメイン環境を構築するためには、ドメインコントローラというアクティブディレクトリデータベースを保持するコンピュータが必要になる。そのためには、1台以上の Windows 2000 Server 以上のサーバが必要となる。また、ドメイン環境を構築することによって、大規模なネットワークも容易に管理作業を行うことができる。それ以外にも、アクティブディレクトリのグループポリシーなどの機能を使用した一元管理、およびセキュリティ設定やアプリケーションの配布といった作業が簡単に行える。



ドメイン内のユーザアカウントを一元管理

2 ドメインの管理

(1) ドメインコントローラ

ドメインコントローラは、Windows 2000 Server 等を使用してドメインを構成する際に、ドメイン内にユーザアカウントデータベースを一元的に保持する役割を果たす。

(2) ユーザ登録

ドメインが構築されている環境では、ネットワーク上の資源を利用したいユーザは、ドメインコントローラにユーザ登録をしなければならない。登録される内容は、ユーザアカウントとパスワードなどである。ユーザがドメインに参加しているコンピュータにログオンしたい場合は、ログオン画面でユーザ名とパスワード、参加するドメインを入力する。入力された情報は、参加を希望するドメイン内のドメインコントローラに受け渡され、認証を受けドメインに参加することができる。

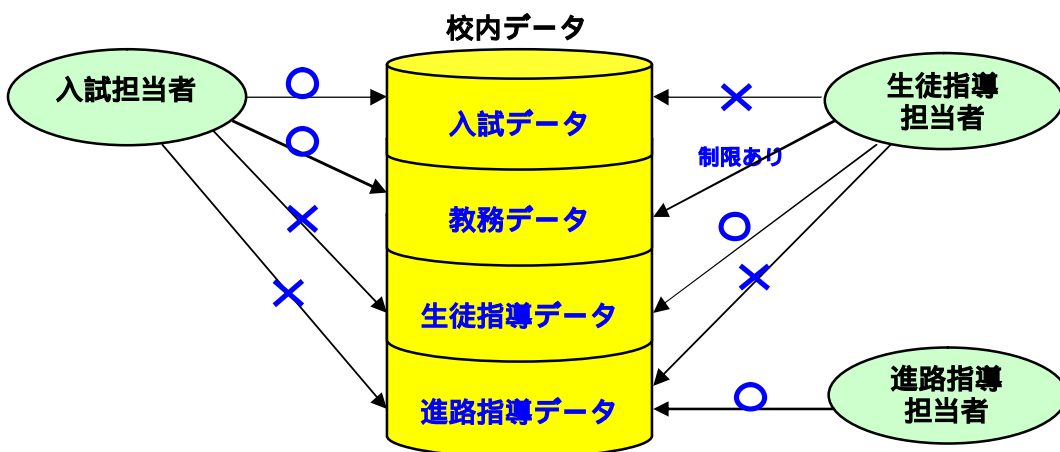
共有リソースを使用する場合には、ユーザ名やパスワードはリソースを管理するサーバに渡されるが、そのユーザに許可されているリソースのアクセス権の認証はドメインコントローラに受け渡され認証が行われる。

(3) ユーザグループ

Windows 2000 Server では、通常ユーザをグループに分け、そのグループに権限を与えることにより、グループに属するユーザは同一の権限を持つことができる。ユーザごとに異なる権限を与えることもできるが、管理上の面からグループを設定する方が効率的である。

(4) アクセス権の設定

個人またはグループに対して、ファイルやフォルダごとにアクセス権を設定することにより、利用できる権限のレベルを変えることができる。これにより、権利のないユーザに対して不用意に情報を与えてしまうことを防ぐことができる。



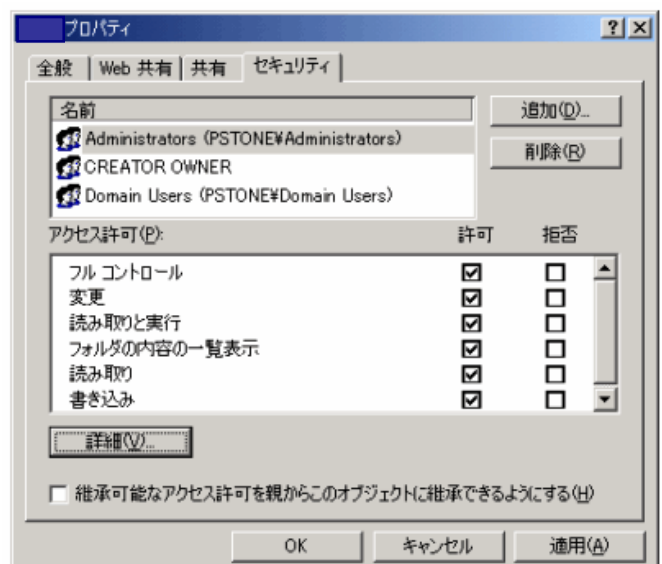
(5) サーバ上でのアクセス権設定

Windows 2000 Server の場合、右図 (アクセス許可欄) を用いて設定を行う。

Windows のファイルシステムには、

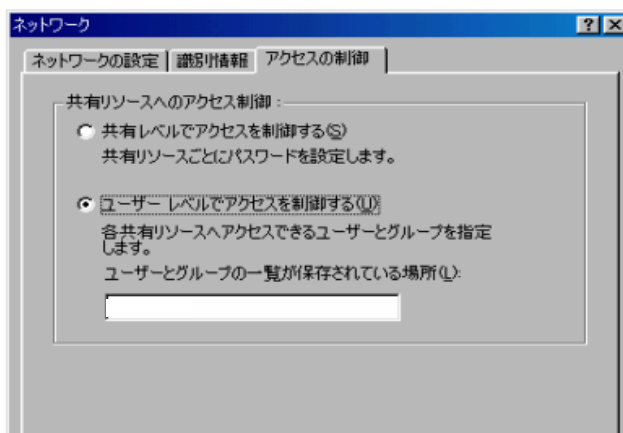
- ・ FAT (File Allocation Table)
- ・ FAT32
- ・ NTFS (NT File System)

の 3 種類がある。



(6) クライアントでのアクセス権設定

クライアントのPCにもアクセス権を設定することができる。ドメインに参加している場合には、ドメインコントローラ内のユーザアカウントの単位でアクセス権を設定することができる。



校内ネットワークの管理形態の移行（ワークグループからドメイン管理へ）

現在、本校のネットワーク管理形態はワークグループで管理しており、教員用と生徒用にそれぞれ「NT-DOMAIN」と「NT-SERVER」というグループ名を付けている。このようにすればコンピュータの数が多くても比較的運用しやすくなる。

しかし、このような場合、それぞれのコンピュータはワークグループ名で単純にグループ分けされているだけで、それぞれのコンピュータは独立した動きをしている。コンピュータが独立した動きをしているとコンピュータAがコンピュータBにアクセスしようとした場合、コンピュータBはユーザ名とパスワードを要求する。その逆も同様で、それぞれのコンピュータが独立してユーザを管理しているため、このような煩雑な作業が発生する。

そこで、本校のネットワークの管理形態についてはドメイン管理に移行する必要がある。ただ単にパソコンの接続台数が多いからという理由ではなく、セキュリティ面の強化のためにもドメインで管理を行った方がより安全で信頼性も高まる。

それでは、どのようなグループを作り、どのような管理が望ましいのか、以下に説明していく。

1 ドメイン名とユーザグループ（一例）

教員用

ドメイン名	グループ名	校務分掌等	係り	アクセス権
教員	admin		ネットワーク管理者	フルアクセス
	kanri	管理職		管理職用
	kyomu	教務部	教務主任	教務主任・教務全般・入試・成績データ・個人用
			入試係	教務全般・入試・成績データ・個人用
			成績	教務全般・成績・個人用
			時間割	教務全般・個人用
	seito	生徒指導部	生徒指導主事	生徒指導主事・生徒指導全般・個人用
			生徒会・その他	生徒指導全般・個人用
	shinro	進路指導部	進路指導主事	進路指導主事・進路指導全般・個人用
			進学・就職・その他	進路指導全般・個人用
kojin	教員用	全教員用	個人用	

グループ・フォルダレベルで制限をかける。

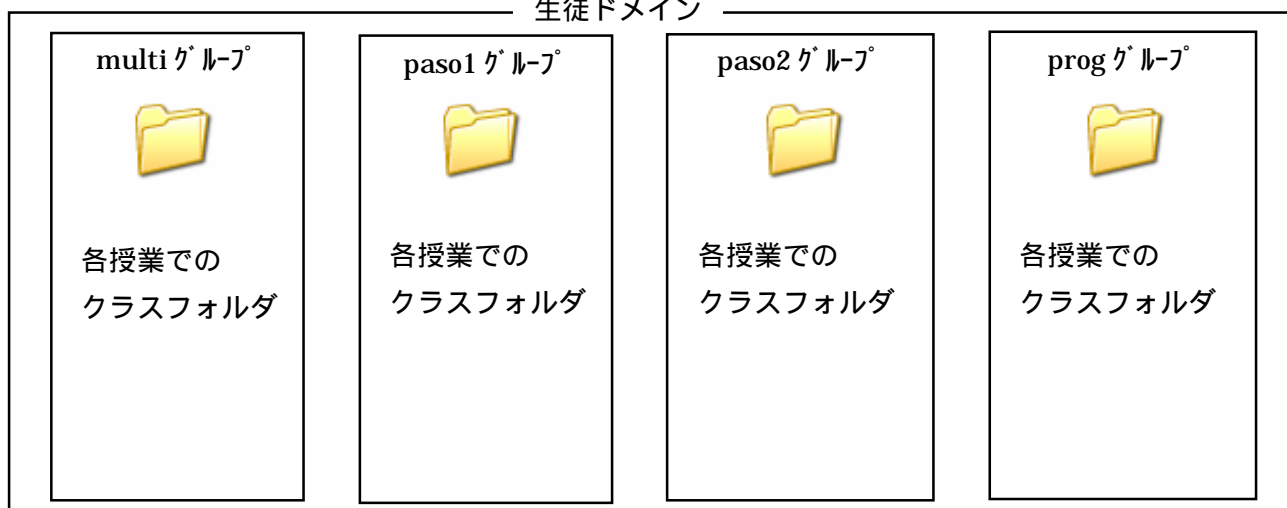
生徒用

ドメイン名	グループ名	アクセス権	ドメイン名	グループ名	アクセス権
生徒	multi	マルチ生徒用	生徒	paso2	パソ2生徒用
	paso1	パソ1生徒用		prog	プログ生徒用

教員ドメイン



生徒ドメイン

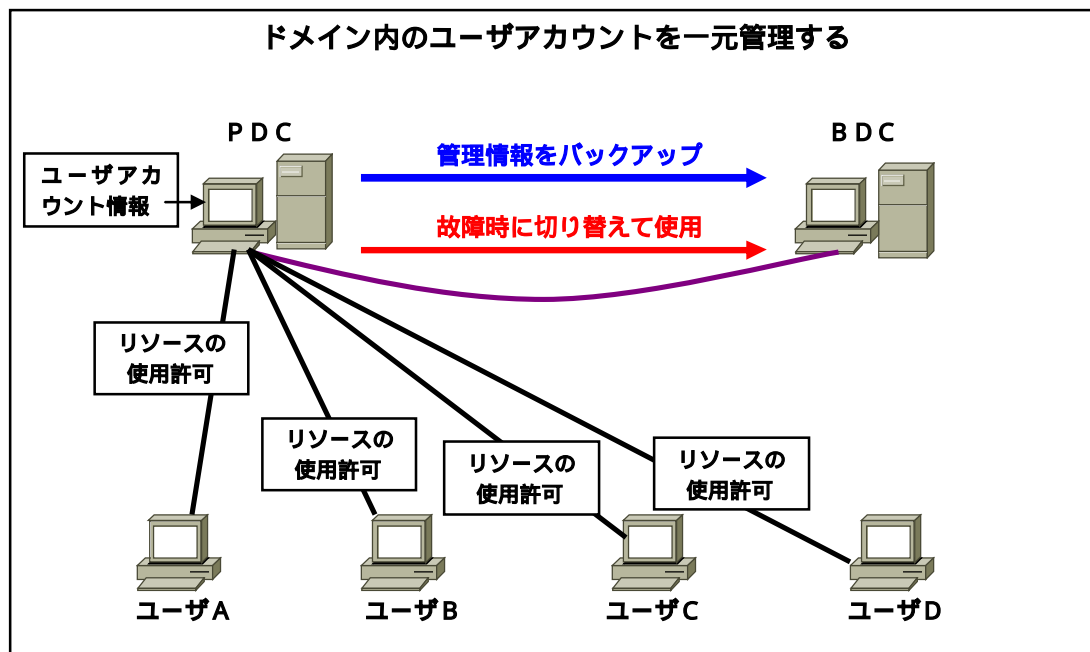


2 ドメイン管理の欠点に対する手立て

ドメインで管理することにより、一元化による管理作業工程最小化による管理コストの削減や作業工程の増大による人為的ミスが解消できる。しかし、集中型システムではドメインコントローラの故障、あるいはドメインコントローラの故障や通信不能時に、クライアントのコンピュータが使用できなくなるという欠点がある。

そこで、現在本校では教員用ファイルサーバとして Windows NT Server、生徒用として Windows 2000 Server を使用している。稼動していないサーバが2台 (Windows 2003 Server) あり、その2台についてユーザアカウントを管理する PDC (プライマリドメインコントローラ) と PDC に障害が発生した場合に PDC に代わってユーザアカウントの管理をする BDC (バックアップドメインコントローラ)

を設定するように考えている。こうすることにより、クライアントはPDCもしくはBDCの認証(リソースの使用許可)を受けてログオンすることになる。



クライアントの設定

コンピュータの管理者の権限を持つユーザとして、Windows XP Professional にログオンする。

- 1 [スタート] ボタンをクリックし、[マイ コンピュータ] を右クリック。
- 2 [プロパティ] をクリックする。
- 3 [コンピュータ名] のタブで、[変更] ボタンをクリックする。
- 4 [ドメイン] をクリックし、使用しているコンピュータが所属するドメインの名前を入力し、次に [OK] をクリックする。(ドメイン名が不明の場合は、ネットワーク管理者に問い合わせること)
- 5 画面の表示に従い、ドメイン ユーザ名とパスワードを入力し、[OK] をクリックする。
完了したら、[OK] をクリックし、再度 [OK] をクリックして、[プロパティ] ウィンドウを閉じる。
- 6 コンピュータはドメインに加わり、ドメインへの参加を通知するメッセージが表示される。
新しい設定が適用されるようにするためにコンピュータを再起動し、ユーザ名とパスワードを入力してドメインにログオンする。

校内ネットワークを支える仕組み（ドメイン管理の導入）

校内のネットワークは構築すれば終わりということではなく、利用者側からすれば、ネットワークはいつでも使えて当たり前である。つまり、「いつでも使える」という状態を維持するとともに、障害が発生した場合でもできるだけ早く復旧させなければならない。以上のようなことから、ネットワーク管理者はネットワークの障害対策や監視を行わなければならない。そのための仕組みについて以下に述べていきたい。

トラブルの発生を未然に防ぐには、1「ユーザが行う設定をできるだけ少なくする」、2「回線などを冗長化して信頼性を高めておく」、3「障害発生時にもすぐに対処できる体制をとっておく」というようなことが大切になる。では、ユーザが行う設定を少なくするにはどうするか、特にネットワークに関する知識を持たないユーザで考えるなら、パスワードの管理以外のことを可能な限り自動化する。特にデフォルトゲートウェイやDNSサーバのアドレスなど、設定しなければならない項目がいくつかあるため、誤った設定をする可能性が非常に高い。誤って入力した場合に一番厄介なのはIPアドレスの重複である。誤って設定したIPアドレスが他のユーザに割り当てられたものであれば、本人はネットワークにつながるのに、正規のユーザがどこにも接続できなくなってしまう。このようなトラブルを避けるためにも、校内のネットワークにはユーザの環境に必要な設定を自動化する仕組みが取り入れられている。それがDHCP（Dynamic Host Configuration Protocol）である。

DHCPを導入すると、管理者の立場からIPアドレスの管理がしやすくなるというメリットがある。どの教室（パソコン室等）でどれくらいのIPアドレスを必要としており、また実際にどれくらいの数のIPアドレスが使用されているのか、といったことが集中的に管理・把握できる。そのうえ、「どのクライアント（ユーザ）がどのIPアドレスを使用するのか」まで設定できるので、何かトラブルが発生した際の原因の追及にも役立つ。

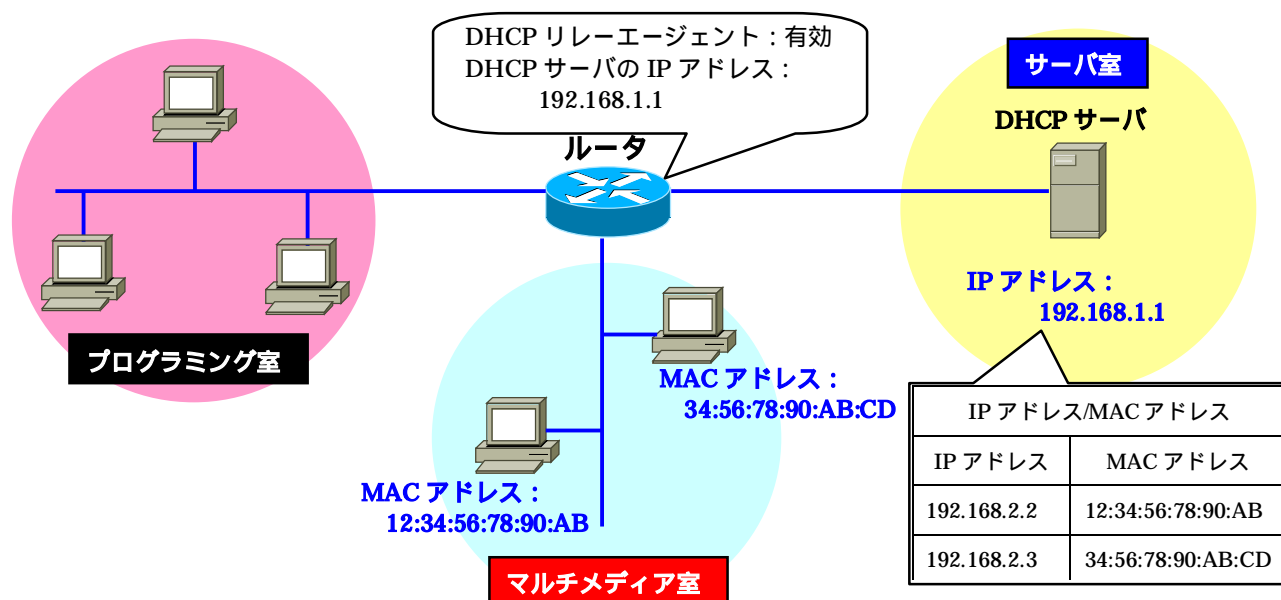
DHCPを使用するためには、TCP/IPのプロパティで「IPアドレスを自動的に取得する」「DNSサーバのアドレスを自動的に取得する」を選択するだけである。

IPアドレスを取得したいDHCPクライアント（ユーザのパソコン）はIPアドレスを自動で設定してくれるDHCPサーバに問い合わせるためにブロードキャストフレームを送信する。自分自身にIPアドレスが設定されていないので、サーバが受け取れることを期待してブロードキャストでやり取りを行う。

これを受けたDHCPサーバは「このIPアドレスでどうか」とオファーを返す。これもブロードキャストである。オファーを受け取ったDHCPクライアントは「これをお願いします」とIPアドレスを要求する。最後にDHCPサーバから「正式にIPアドレスを貸し出します」と回答が戻ってきた時点で、クライアントはIPアドレスやデフォルトゲートウェイなどの設定値を取得できる。

IPアドレスはDHCPサーバから貸し出され、使い終わると返却するという仕組みである。貸し出し可能な範囲のことを「アドレスプール」と呼ぶ。この範囲はサブネットごとに設定が可能である。また、管理者によるDHCPサーバ側の設定で、IPアドレスとあらかじめ登録したMACアドレスを1対1で対応付けることもできる。

DHCPサーバはIPアドレスを貸し出す際に、有効期限も同時に通知している。IPアドレスは無限にないため、使っていないIPアドレスは回収され、別のクライアントに割り当てられる。そのための有効期限を「リース期限」と呼ぶ。



ブロードキャストフレームはルータを越えることはできない。本来であれば、異なるサブネットにある DHCP サーバとは通信できない。これが可能となるのは、ルータに搭載された「DHCP リレーエージェント機能が使われているためである。リレーエージェントは DHCP の要求・応答フレームをユニキャストに変換し、DHCP サーバとやり取りする機能である。1 台の DHCP サーバで複数のサブネットに IP アドレスをリースできるのは、この機能があるからである。

本校では DHCP 機能を使っておらず、ネットワーク担当者は割り当て可能な IP アドレスとネットワークに接続するためのマニュアルを本人に渡し、各自でネットワーク接続設定を行ってもらうという形態をとっている。各自で設定できるユーザはいいが、そうでないユーザはネットワークの知識がある職員に頼むというのが現状である。そういったユーザが少数であれば即対応することができるが、本校職員のほとんどがネットワークの担当者へ頼むという状況である。そういった問題を解決するためにも DHCP を活用していきたいと考えている。

スイッチと VLAN

スイッチ

LAN の中継機器として製品化されているスイッチには、様々なカテゴリのものが存在する。低価格化が進み、現在のネットワーク環境の基本である「レイヤ 2 スイッチ」、ルータに取って代わりつつある「レイヤ 3 スイッチ」、e コマースや高人気の Web サイトで必須のアイテムとなった「レイヤ 4 / レイヤ 7 スイッチ」などである。そこで、現在の LAN 環境に定番のスイッチについて述べていきたい。

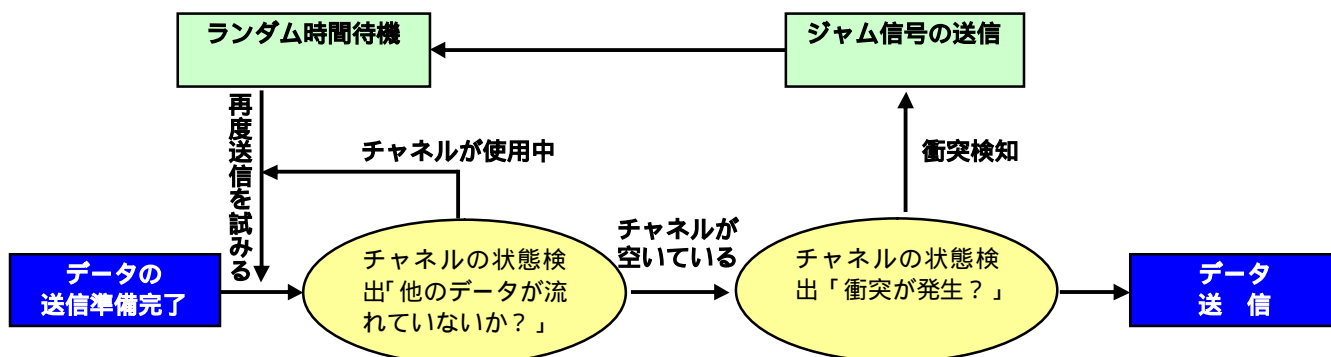
1 Ethernet と CSMA/CD

現在、LAN で最も利用されている通信方式は Ethernet で、事実上の世界標準となっているといっても過言ではない。Ethernet の中核技術は CSMA/CD であったが、スイッチ（スイッチング技術）の開発によって過去の遺物となりつつある。しかし、スイッチのことを知るうえで、CSMA/CD についての知識は必要となる。CSMA/CD について解説する。

CSMA/CD は、

- Carrier Sense : 話す前に聴け
- Multiple Access : 静かなら話せ
- Collision Detection : 話しながら聴け

の 3 つのルールを頭文字を並べたものである。理論的には 1 本の伝送路（メディア）を複数のノード（通信端末）で共有しながら、ある瞬間には同時に 1 台のノードしかデータフレームを発信できないように制御するための仕組みである。（下図）



CSMA/CD では各ノードは通信を開始する前に、他のノードがケーブル上にフレームを送出していないことを確認する。その際、他のノードが送信したフレームが流れていると、それが消えてからランダムに時間待機して送信を開始する。フレームが電気信号として流れるため非常に高速に伝搬されるが、それでもネットワーク全体に信号が伝わるには一定の時間がかかる。このため、複数のノードが同時にケーブル上に信号を送出してしまうことがある。そして複数のノードが同時に送信を行うと、ケーブル内で信号のコリジョン（衝突）が発生してフレームが破壊され、データが正確に伝送されなくなる。これに対処するため、各ノードはコリジョンを検知したら送信を取り消し、再度データフレームを送信することになっている。コリジョンが発生するとケーブル内の電圧が上がりケーブルに沿って発信源まで戻ってくる（ジャム信号）ので、各ノードはデータの送信中でもケーブル上の電気信号をチェックしている。

CSMA/CD が確実に機能するためには、送信側ノードがフレームの送出を完了する前にコリジョンを検出できなければならない。そのため、電気信号がネットワーク内を往復する時間よりも長く、フレームを送出し続けることが要求される。そこで Ethernet では、データが少ない場合でも一定時間信号を流し続けるよう、フレームの最小長を 64 バイトと定めている。

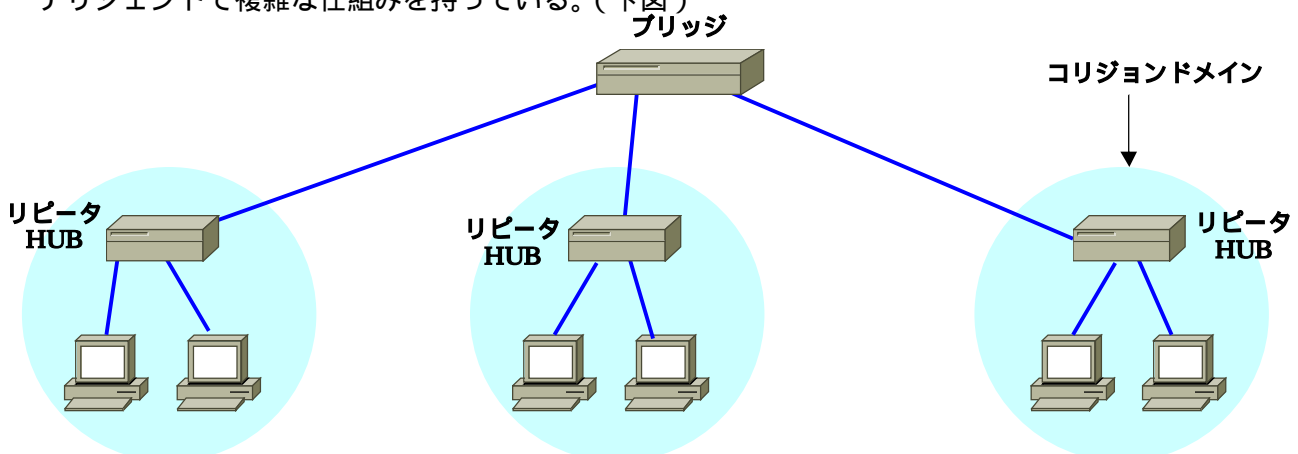
2 リピータとコリジョンドメインの問題

Ethernet では、伝送メディアとして同軸ケーブルやツイストペアケーブル（STPやUTP）、光ファイバなどを利用しているが、伝送路内で信号が減衰することを考慮して、メディアごとに最大長が定められている。しかし、現実にはその最大長以上にネットワークを拡張する必要がある。ネットワークを拡張するための最も単純な中継機器が「リピータ」である。リピータは、2本のケーブルの中継点として設置され、減衰した信号を増幅、整形して転送を行う。また、ツイストケーブルを使った 10BASE-T や 100BASE-TX など、スター型のトポロジーを利用する Ethernet では HUB を使ってネットワークを構築する。HUB は多数のポート間でリピータの機能を持った中継装置（マルチポートリピータ）である。リピータや HUB の動作の特徴は、任意のポートに接続されたノードから送信されたフレームが、他の全てのポートに流される。8ポートのリピータ HUB であれば、1つのポートに送信されたフレームは、他の7つのポート全てに流される。リピータやリピータ HUB で構築されたネットワークでは、論理的には1本の伝送路に全てのノードが接続されている以前の同軸ケーブルを使った Ethernet と同じである。つまりネットワーク全体でコリジョンが発生するために、同時に1台のノードしかデータを送信できない。この CSMA/CD 方式で利用するコリジョンを検知できる範囲（ドメイン）は「コリジョンドメイン」と呼ばれ、1つのコリジョンドメイン内で同時にデータを送信できるノードは1台だけなので、狭いコリジョンドメインの方がネットワークの効率はよいことになる。先で記述したリピータ HUB でネットワークを拡張すると、ノードが増加することによりコリジョンドメインが膨張する。これによりコリジョンが発生する確率が増え、伝送効率が低下する。

3 ブリッジからスイッチへ

インターネットの普及、ファイルサーバやプリントサーバの導入などにより、校内 LAN や社内 LAN へ接続される機器が増加し、ネットワーク内を流れるデータ量は加速度的に増えている。データ量が増えるということは、コリジョンが発生する確率も増えるということである。伝送効率を上げるには、コリジョンドメインを分割する中継機器を用いる必要がある。

コリジョンドメインを分割する中継機器として、「ブリッジ」が Ethernet と同じくらい前から存在する。リピータが電気信号を単純に中継するのに対して、ブリッジは Ethernet 上の他のノードと同じように CSMA/CD の手順を踏み、データフレームが確実に送受信されるように働く。ブリッジは、中継先のネットワークで別のノードがデータを送信中であれば、それが終了するまで送信を待つ。このためブリッジには、送信待ちのデータフレームを一時的に格納するバッファメモリが搭載されている。ブリッジは複数のネットワークを別々のコリジョンドメインとして相互接続するために、リピータよりもはるかにインテリジェントで複雑な仕組みを持っている。（下図）



ブリッジの中には、フレームを受信するたびに送信元の MAC アドレスを記憶する「ラーニング機能」を備えた「ラーニングブリッジ」と呼ばれる製品がある。ラーニングブリッジは、学習した MAC アドレス情報に基づいて、任意のポートで受信した Ethernet フレームを、どのポートへ中継するかを判断する。

このラーニングブリッジを進化させたものが「スイッチ」である。最初のスイッチはマルチポートブリッジの一種で「スイッチングハブ」とも呼ばれていた。古典的なマルチポートブリッジは、同時に 1 対の 2 ポート間の中継しかできないのに対し、スイッチングハブでは同時に複数対のマルチポート間の中継が可能になった。

また、スイッチングハブは、製品アーキテクチャがブリッジとは大きく異なり、ブリッジの実態は汎用マイクロプロセッサ（パソコンなどの CPU に使われるチップ）の上で動く、フレーム解析ソフトウェアである。これに対しスイッチングハブは、ロジックが組み込まれた専用チップを利用している。つまり、フレームの解析と転送を、ソフトウェアではなくハードウェアで行っている。このため、処理速度は桁違いに向上した。専用チップを採用し、ハードウェア的にフレーム解析と転送処理を行うアーキテクチャは、現在「スイッチ」と呼ばれる製品群の特徴である。

4 スwitchの基本はレイヤ2スSwitch

スイッチは送信元と宛先の MAC アドレスを見て特定のポートにのみフレームを転送し、複数の伝送路を同時に利用できる。また、スイッチは OSI 参照モデルのデータリンク層での中継機能を担っているため、レイヤ2スSwitchと呼ばれている。

5 スwitchの転送機能

スイッチの Ethernet フレーム転送(フォワーディング)方法は、大きく分けて次の3種類が挙げられる。

カットスルー

カットスルー方式は、フレームを宛先アドレスまで受信したら宛先ノードの接続されたポートへ転送する。有効なアドレスが宛先に指定されているフレームは全て転送され、遅延はほとんど発生しない。ただし、壊れたフレームも転送するという問題が生じる。

修正カットスルー

修正カットスルー方式は、Ethernet フレームの先頭 64 バイトを受信するまでは転送を開始しない。64 バイトは Ethernet フレームの最小長であり、コリジョンにより発生するエラーフレームのほとんどは、64 バイト以下であることが知られている。すなわち、最初の 64 バイトを検査すれば、ほとんどのエラーフレームを除去できる。この方式は、遅延対策とエラー検査を両立させたものである。

ストア&フォワード

ストア&フォワード方式は、受信したフレーム全体をバッファに全て格納してから別のポートへ送り出す。フレーム全体を受信するため、Ethernet フレームの最後に付属するエラーチェック用の FCS を確認でき、エラーが存在する「壊れたフレーム」を破棄できる。しかし、他の方式と比較すると遅延が大きくなる。

Ethernet の伝送速度が 10Mbps のころは、遅延が大きな問題であった。しかしこれまで、スイッチに搭載されるバッファメモリの性能が向上してきたことにより、遅延は無視可能なレベルとなった。さらに、10/100Mbps 対応など伝送速度が異なるポートをもつスイッチでは、速度差を吸収するためにストア&フォワード方式が事実上の業界標準となっている。

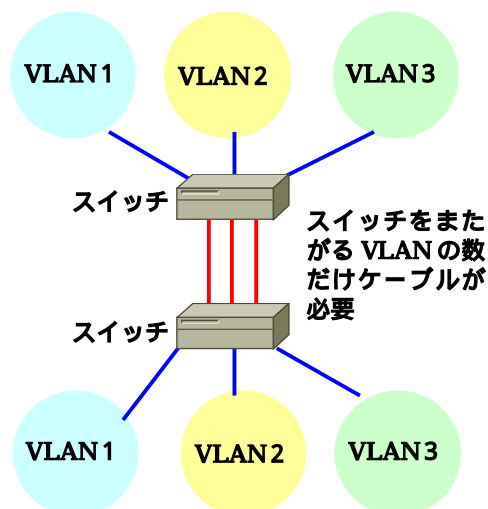
6 異なる LAN に分割する VLAN 機能

VLAN (Virtual LAN : 仮想 LAN) とは、物理的に同一のスイッチに接続されているノードを、論理的に (仮想的に) 異なる LAN に分割する機能である。VLAN 機能はレイヤ 3 の代表的な機能として紹介されることが多いが、VLAN 自体はレイヤ 2 スwitch の機能だけで実現できる。

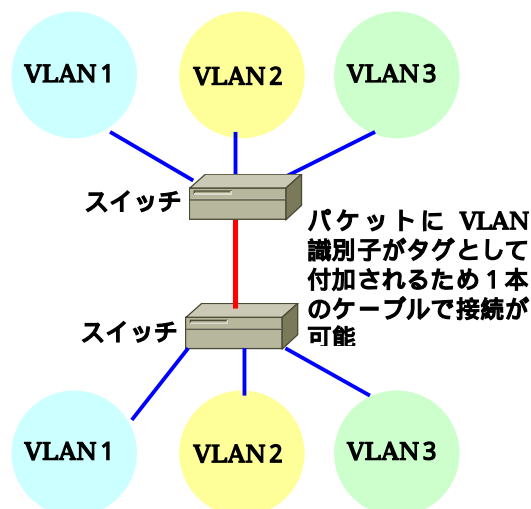
レイヤ 2 スwitch で VLAN を構築する場合、最もよく使われるのは「ポートベース VLAN」と呼ばれる機能である。これは単純にレイヤ 2 スwitch のポート単位で VLAN を分けるものである。

また、複数のフロアや建物に分散したワークグループを構築するといったことも、レイヤ 2 スwitch の「VLAN タギング」機能を使えば可能である。VLAN タギングとは、Ethernet フレームに VLAN 識別子として 4 バイトの「タグ情報」を付加する仕組みである。VLAN タギングに対応したスイッチ間では、タグ情報の付加された Ethernet フレームが送受信される。受信側のスイッチは VLAN 識別子を見て、目的の VLAN (ポートグループ) にのみフレームを転送ようになる。これにより、複数のスイッチで VLAN を構築する際にメリットが生まれる。ポートベース LAN では、複数のスイッチで VLAN 情報を共有する場合、VLAN の数だけ接続ケーブルが必要になる。しかし、VLAN タギングを利用すれば接続ケーブルは 1 本ですむ。(下図)

VLAN タギング未対応のスイッチの場合



VLAN タギングに対応したスイッチの場合



VLAN

本校の校内ネットワークを教員用と生徒用のセグメントに分ける手法として VLAN でセグメントを分ける方法が考えられる。そこで、校内ネットワークを VLAN で教員用と生徒用とにセグメント分けする方法について記述していく。

1 VLAN (バーチャル LAN) とは

VLAN とは、スイッチングハブの各ポートを複数のグループに分け、それぞれのグループを独立したサブネットとして機能させる仕組みのことである。

スイッチングハブでは全てのポートが 1 つのネットワークに属しており、どのポートからでもほかのポートにパケットを送ることができる。これに対して VLAN 機能を持つスイッチングハブでは、仮想的な複数のサブネットを 1 台のスイッチングハブに設定することができる。例えば、8 ポートの VLAN 対応スイッチングハブの 1~4 ポートを VLAN 1 に、5~8 ポートを VLAN 2 に設定するといったことが簡単

にできる。このように設定すると、片方の VLAN 内のパケットはもう片方の VLAN には中継されることはない。これにより、1つのスイッチングハブを利用するだけで、1つのネットワークを2つのネットワークに分けて利用することができる。つまり、複数のポートを論理的なグループにまとめ、グループ内だけの通信を可能にすることができる。

2 VLANの種類

VLAN には以下のような種類がある。それぞれの特長について説明する。

ポート VLAN

パケットを受信したポートにより VLAN を決める方式

タグ VLAN

パケット内のタグに指定された番号により VLAN を決める方式

MAC アドレス VLAN

送信元の MAC アドレスにより VLAN を決める方式

プロトコルベース VLAN

プロトコルの種類 (IP、IPX、AppleTalk 等) により VLAN を決める方式

レイヤ3 ネットワーク VLAN

レイヤ3のネットワーク情報により VLAN を決める方式

3 VLANの考え方

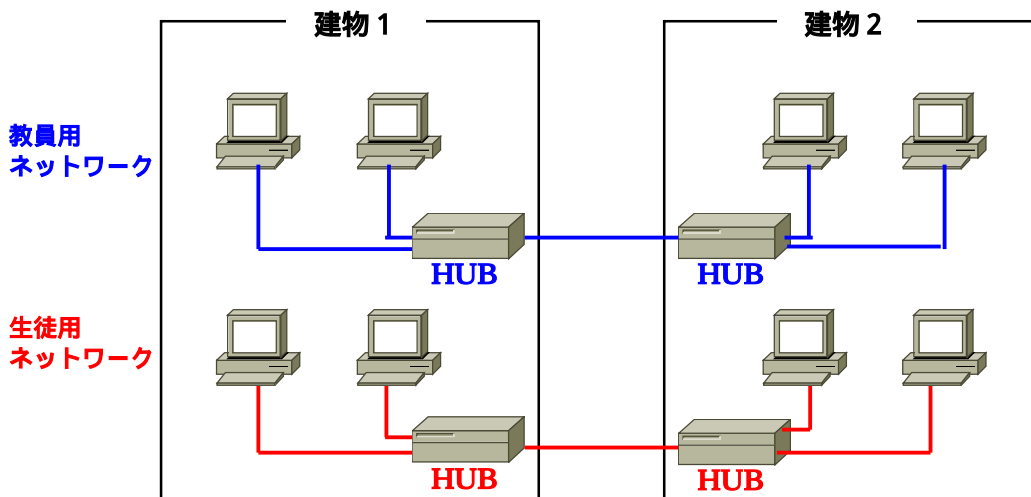


図 1

HUB を用いて全教員用のパソコンと生徒用のパソコンを接続する。(教員用と生徒用のネットワークを別々にする)しかし、この場合は建物間の接続用として2本の LAN ケーブルと4台の HUB が必要となる。

上記の図1では教員用のネットワークと生徒用のネットワークは物理的に独立している。次の図2では、VLAN を使った物理的構成である。

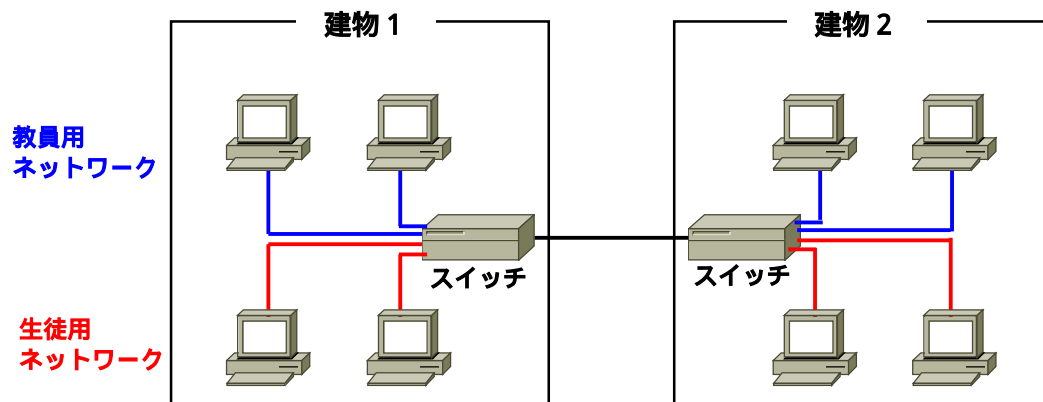


図 2

図 2 では建物間の LAN ケーブルが 1 本になり、図 1 の HUB がスイッチングハブに変更されている。これだけでは物理的に全てのパソコンが 1 つのネットワーク上に存在しているようになる。しかし、HUB をスイッチングハブに変更することにより、物理的構成を論理的構成に変更できる。また、スイッチングハブを使うことにより、VLAN ごとにポート分けができる。その構成を図 3 に示す。

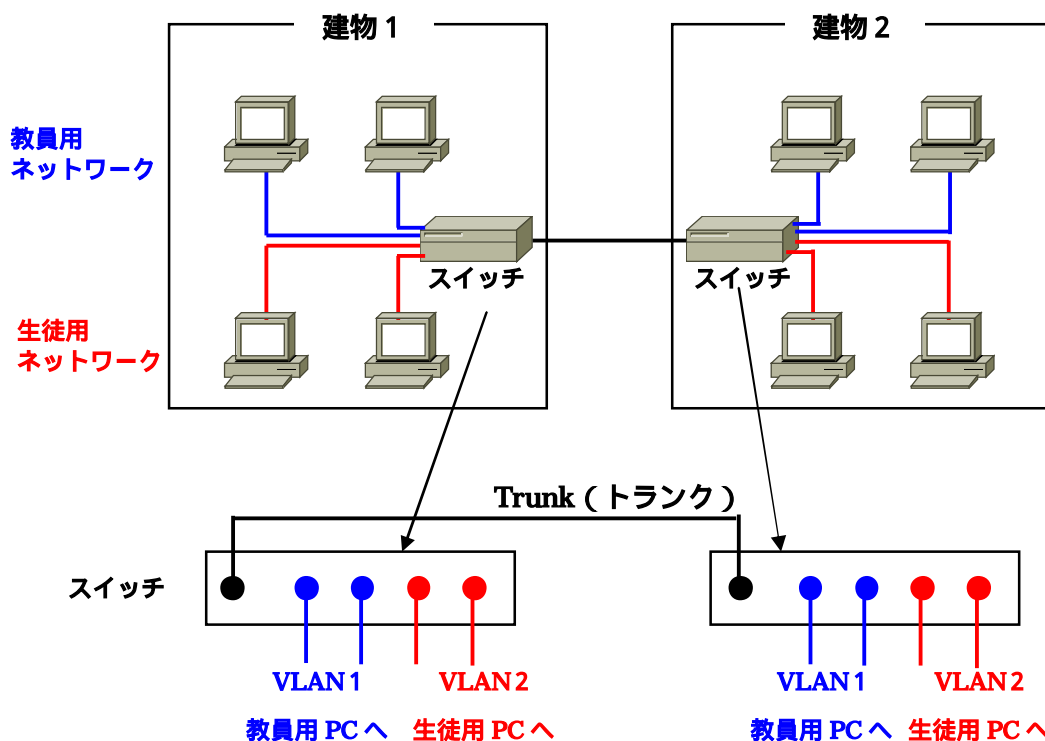


図 3

このように、2つのスイッチングハブの Trunk (トランク) を LAN ケーブルで結び、VLAN 1 を教員用のパソコンに、VLAN 2 を生徒用のパソコンに接続すればよい。ここでは、スイッチとスイッチを結ぶため、LAN ケーブルはクロスケーブルを使う。

VLAN の設定は、スイッチでソフトウェアを介して行う。VLAN は標準化されていないため、スイッチ・ベンダー独自のソフトウェアを使うことになる。

3 VLAN の作成

スイッチの設定は、シリアルポートに管理用コンピュータを接続し、そこからハイパーターミナルなどのターミナルソフトを使って行うのが一般的である。VLAN の作成については製品によって若干異なるが、およそ次のようになる。

まず、新しい VLAN の名前（ここでは生徒用を「Students」）を定義し、そこに識別番号の VID を設定する。VID に使える番号は、スイッチがサポートしている VLAN 数だけであり、すでに割り当てられていないものであれば、基本的に何を割り当ててもよい。ここでは「2」を割り当てている（1はデフォルト VLAN の VID）。あとは、その VLAN グループに属するポートを番号で指定する。ここでは「1 3」を指定している。

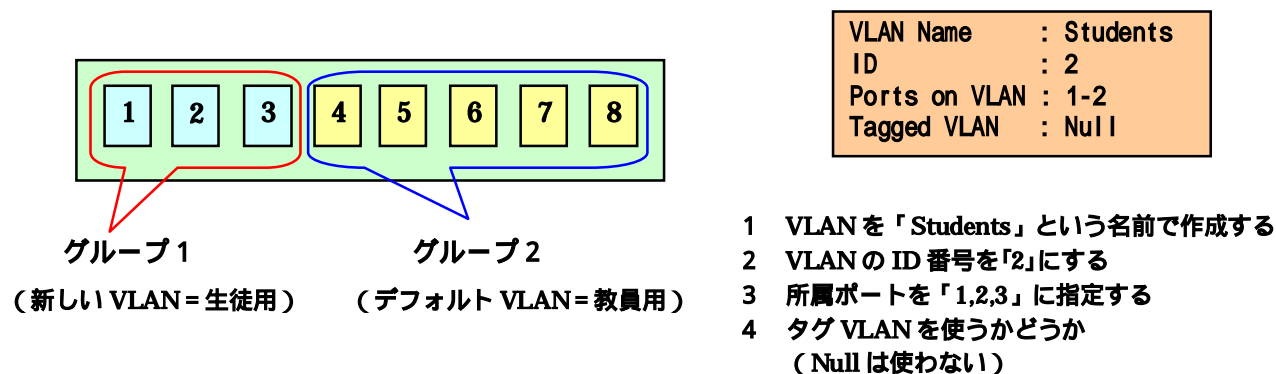


図 4

新しい VLAN グループを1つ作成すると、1台のスイッチを2台に分割したのと同じ状態になる。同じ VLAN グループに属するポート同士は直接通信できるが、異なる VLAN グループに属するポート間はルータでルーティングしなければ通信できない。

図4では、スイッチごとにグループを作成するので特に「ポート VLAN」と呼ばれる。ポート VLAN では、ポートごとに VLAN グループを割り当てていく。そのため複数のスイッチをまたぐような VLAN を作る場合、スイッチ間を接続する回線は VLAN グループの数だけ必要になる。例えば、スイッチ1とスイッチ2にそれぞれ VLAN-A 用と VLAN-B 用の2本の回線をつなげなければならない。このようなスイッチ間の回線は、ポート VLAN を発展させた「タグ VLAN」(トランク VLAN、IEEE802.1Q)を使うことで1本に束ねることができる。

タグ VLAN は、Ethernet のデータ (フレーム) に「タグヘッダ」と呼ばれる独自情報を挿入し、それに基づいてスイッチングすることで実現される。タグヘッダは4バイトの情報で、この後半に VID が収められている。タグ VLAN 対応スイッチはこの情報を認識することができるので、同じ回線に複数の VLAN のフレームが混在しても正しいあて先に中継される。

タグ VLAN の設定は VLAN の作成時に行う。具体的には、特定のポートを複数の VLAN グループに属するように設定した後、そのポートをタグヘッダ付きのフレームを送受信できるポートとして指定する。

図5でいえば、スイッチ1の「ポート8」は VLAN グループ「Teacher」(教員)と「Students」(生徒)の両方に属するようにして、「Tagged VLAN」でタグ VLAN 対応ポートに指定している。同様にスイッチ2では「ポート1」をタグ VLAN に対応させている。以上の設定で、スイッチ1のポート8とスイッチ2のポート1は、Teacher VLAN のフレームも Students VLAN のフレームも送受信できるようになるので、このポートでスイッチ同士を接続すればよい。

ポート VLAN とタグ VLAN を同時に使うことで、配線をシンプルに、かつ柔軟にできるようになる。

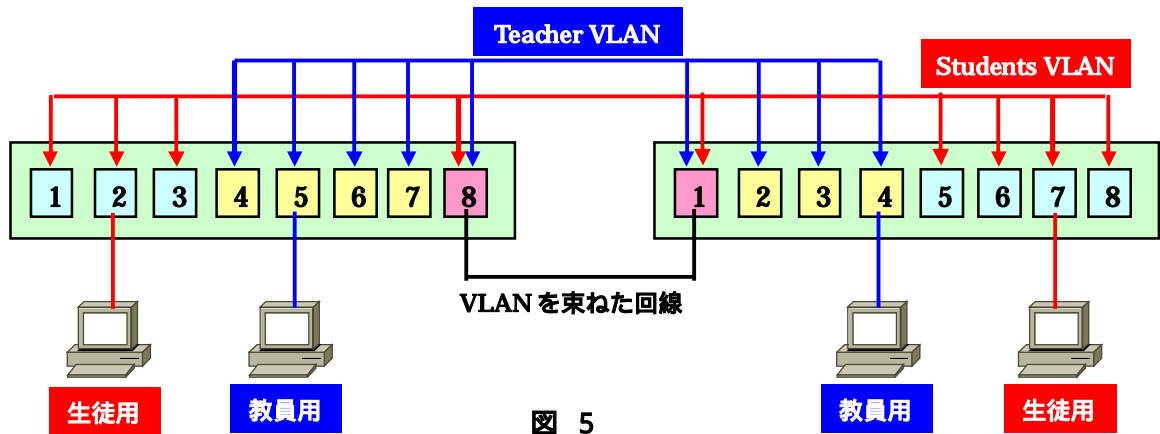
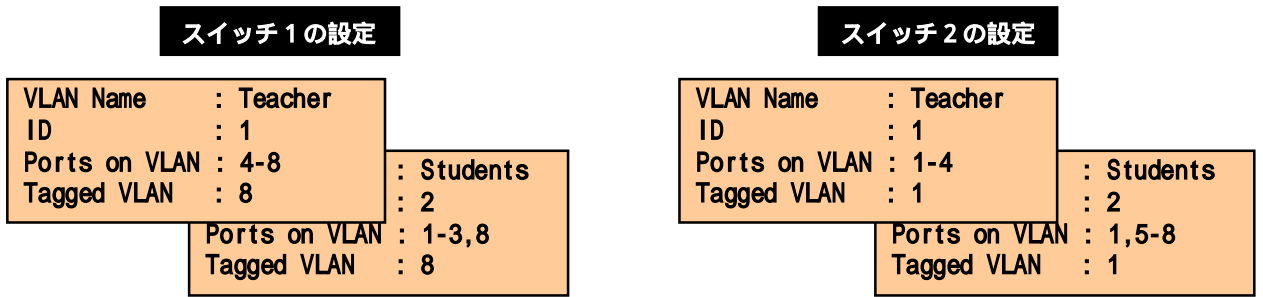


図 5

4 本校の校内ネットワークへの導入案

本校の校内ネットワークに VLAN を導入する際、教員用のセグメントと生徒用のセグメントが存在するが、2つのセグメントが混在する建物として、パソコン室がある産業教育振興棟（以下 産振棟）があげられる。そこで、産振棟を例に上げ構築例を記述していく。

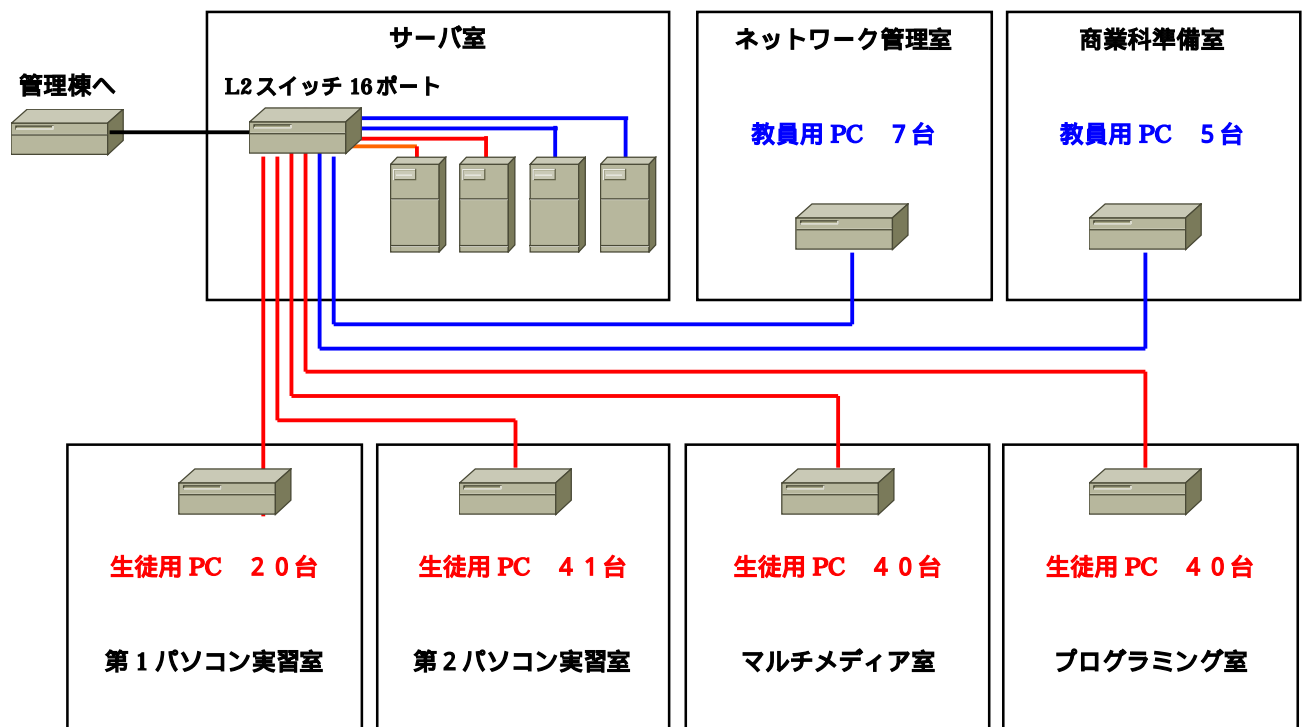


図 6

図6は本校の産振棟内の状況である。管理棟から光ファイバケーブルが産振棟のサーバ室まで来ており、メディアコンバータを経由してスイッチへ入り、そのスイッチから各パソコン室とネットワーク管理室、商業科準備室へ接続されている。インターネットに接続するためには管理等にあるルータから、VPN経由で福岡県教育センターへ接続し、そこからWebの閲覧ができる。

サーバについては産振棟のサーバ室に設置し、2台を生徒用とし1台をファイルサーバ、もう1台をDHCPサーバとしている。残りのサーバについては教員用のファイルサーバとして活用している。

今回はそのスイッチのVLAN機能を使いVLANを構築する。図7はサーバ室にあるレイヤ2スイッチの接続状態を示している。

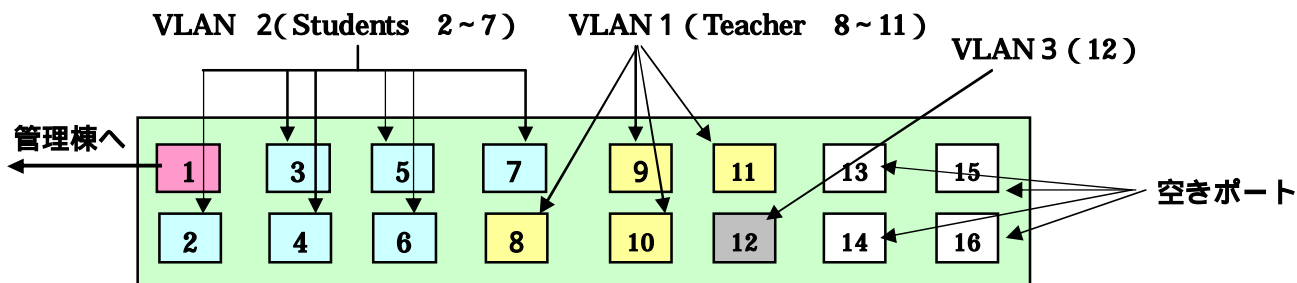
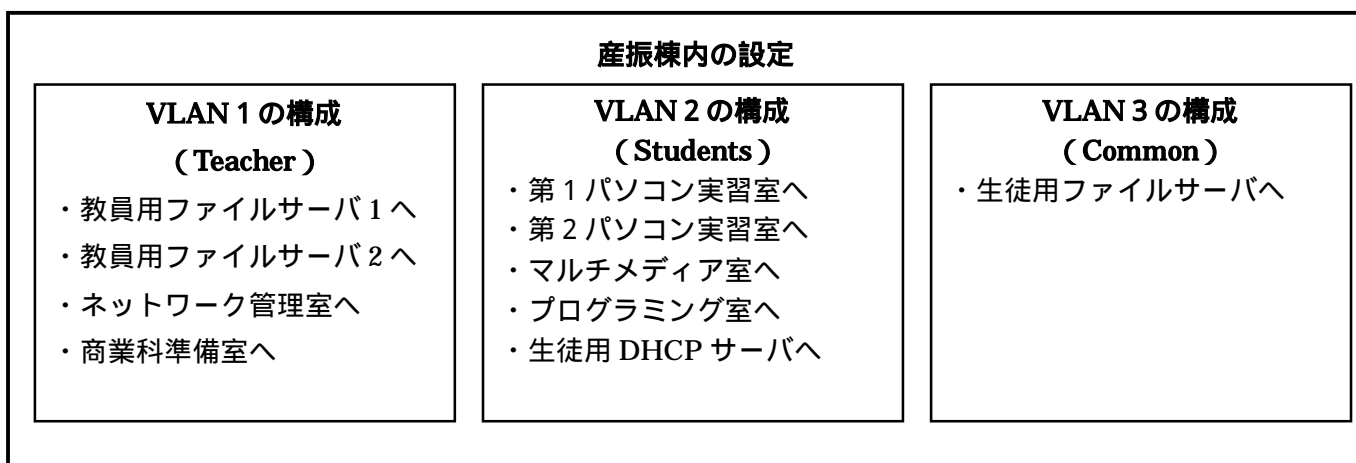


図7 タグVLAN

産振棟側スイッチの設定		
VLAN Name : Teacher ID : 1 Ports on VLAN : 1,8-11 Tagged VLAN : 1	VLAN Name : Students ID : 2 Ports on VLAN : 1-7 Tagged VLAN : 1	VLAN Name : Common ID : 3 Ports on VLAN : 1-12 Tagged VLAN : 1

上の図は産振棟側のスイッチの設定（タグVLAN）
左から VLAN 1、VLAN 2、VLAN 3 の設定例

図8

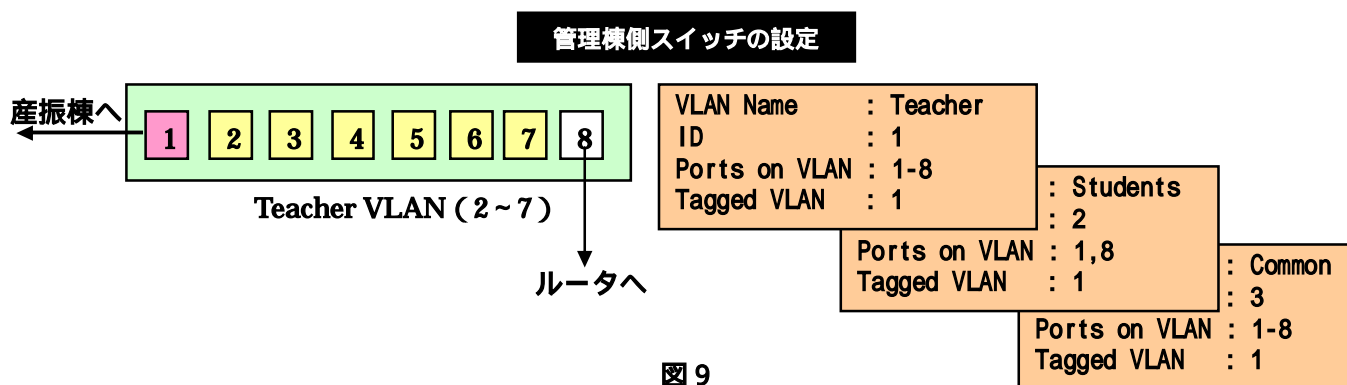


図 8 は産振棟サーバ室のスイッチの設定と図 9 が管理棟にあるスイッチの設定である。管理棟には生徒用のポートは必要ないが、インターネットができなくなると困るのでタグ VLAN をポート 1 に設定し、ポート 8 はルータへとつなげるために設定する必要がある。また、職員室内から生徒用のファイルサーバにアクセスできるようになる。

空きポートについてはスイッチのメーカーによるが、ほとんどがデフォルトで VLAN 1 となっている。そこで空きポートを使用する際は、スイッチの設定を再度行う必要がある。

本校の VLAN によるセグメント分割をまとめると以下のようなになる。

- ・ VLAN 1 を教員用のセグメントとする。
- ・ VLAN 2 を生徒用のセグメントとする。
- ・ VLAN 3 を教員用と生徒用の共通セグメントとする。
- ・ VLAN 1 と VLAN 2 は通信が行えないため、生徒側から教員側へはアクセスできない。
- ・ VLAN 3 を VLAN 1 と VLAN 2 の両方に所属させることにより、どちらからも生徒用ファイルサーバにアクセスでき、生徒はファイルの保存用に、教員は授業に利用する教材などをサーバに保存することができる。
- ・ 管理棟のポート 8 がルータに接続しているため、すべての VLAN に所属させる。

これで VLAN による生徒用と教員用ネットワークセグメントが分けられたことになり、セキュリティにおいても確保できる。

本校の例では複雑なネットワーク環境になっているため、VLAN 環境で生徒用と教員用ネットワークセグメントを分ける簡単な例を図 10 に示す。

ここでは、生徒用パソコン教室を「VLAN 1」、教員用を「VLAN 2」、全校用サーバやルータを「VLAN 3」に分割する。ただし、「VLAN 3」については VLAN 1, 2 の両方に所属させることにより、パソコン教室からも、職員室の教員用パソコンからもインターネットを利用でき、パソコン教室の生徒用のパソコンからは職員室の教員用ネットワークにはアクセスできない環境が構築できる。

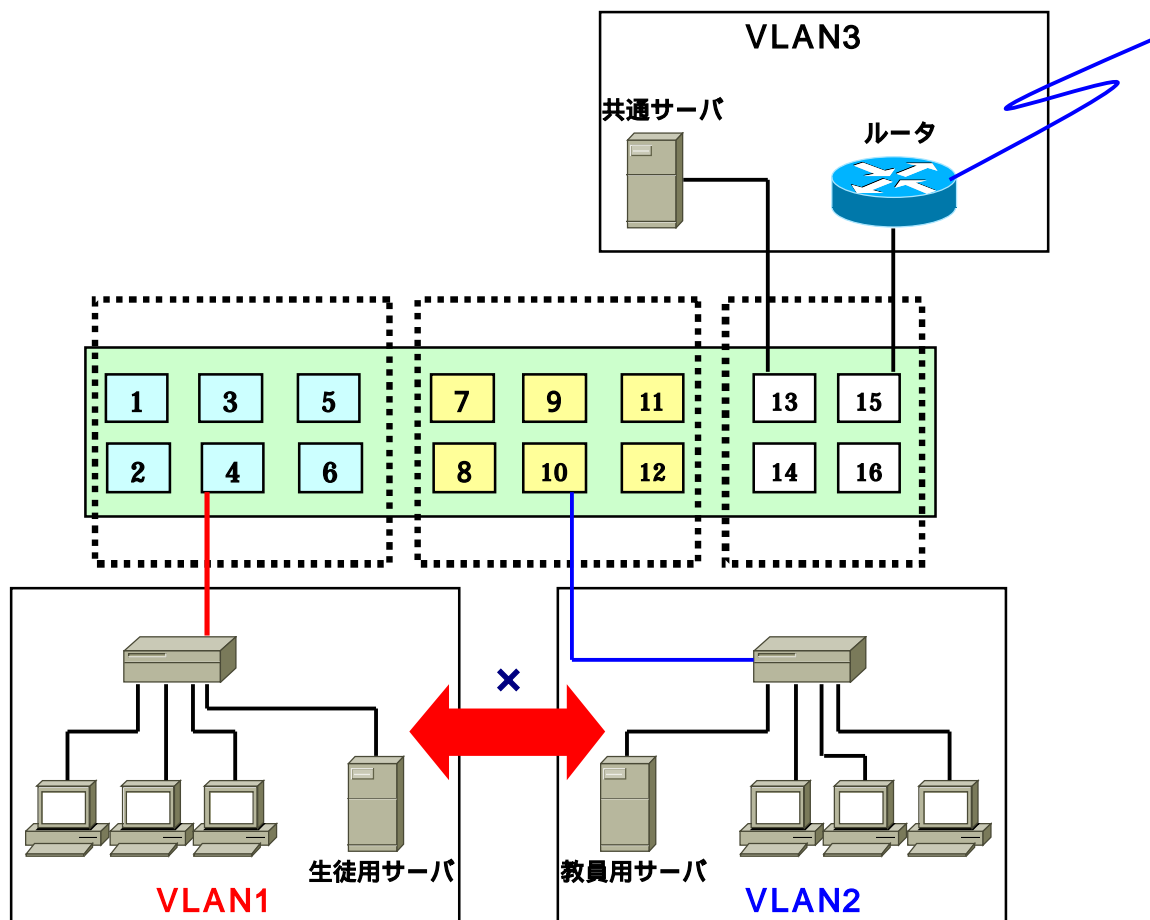


図 1 0

VLAN で生徒用と教員用ネットワークセグメントを分割する方法以外に、ルータを用いて2つのセグメントを分ける方法がある。その方法の一つはルータにもよるが、プライマリアドレスとセカンダリアドレスといったように、2つのネットワークアドレスを設定できるものがあり、1つの物理的なネットワーク（同一セグメント）を2つの論理的なネットワークに分割することも可能である。ただし、TCP/IP プロトコルのみで、NETBEUI などのプロトコルは対応できない。

もう一つの方法は Cisco 製品のルータになるが、ACL（アクセス・コントロール・リスト）を活用する方法がある。これは Cisco 独自の言語である IOS を使ったプログラムのような記述が必要になる。次にその設定方法について述べていく。

5 アクセス・コントロール・リスト (ACL : Access Control List)

アクセス・コントロール・リスト（以下、ACL という）とは、ルータのインタフェースに適用する指示のリストである。それは、どのパケットを許可し、どのパケットを拒否するかをルータに伝える。具体的には、送信元アドレス、宛先アドレス、ポート番号などの仕様に基づいて、パケットを許可または拒否することができる。ルータのインタフェースに ACL を適用すると、それによりトラフィックを管理し、特定のパケットをスキャンすることができる。どのトラフィックもインタフェースを通過するときに、ACL の条件と照合されてテストされる。

ACL は Internet Protocol (IP: インターネット・プロトコル) や IPX (Internetwork Packet Exchange) など、すべてのルーティング対象ネットワーク・プロトコルに対して作成でき、ルータを通過する際にパ

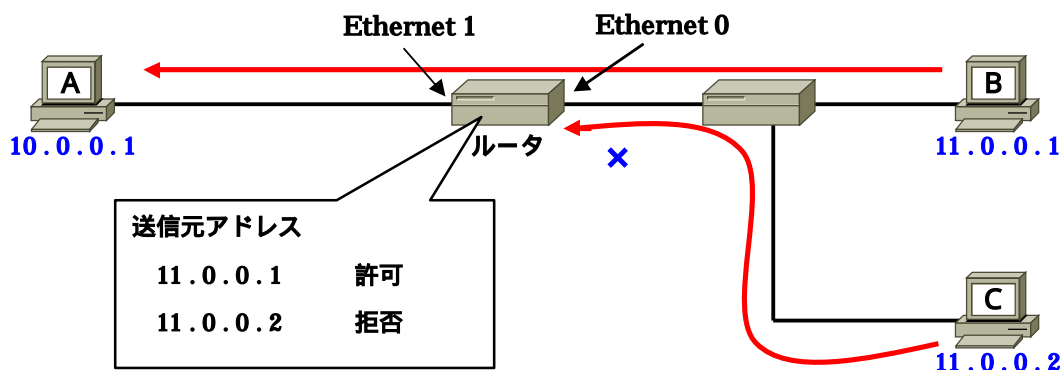
ケットをフィルタリングする。ルータで ACL を設定すると、ネットワークまたはサブネットへのアクセスを制御できる。そこで、学校における校内 LAN では ACL を使って生徒のトラフィックが教員用ネットワークに侵入するのを防止することができる。

ACL はルータのインタフェースでルーティング対象パケットを転送するか、ブロッキングするかを制御することによってネットワーク・トラフィックをフィルタリングする。ルータは ACL に指定された条件に基づいて各パケットを調べ、パケットを転送するか廃棄するかを決める。ACL の条件には、トラフィックの送信元アドレス、トラフィックの宛先アドレス、上位層のプロトコルなどの情報がある。

ACL はプロトコル単位で定義しなければならない。つまり、特定のインタフェースのトラフィック・フローを制御する場合は、そのインタフェースで使用できるすべてのプロトコルに対して ACL を 1 つずつ定義する。(プロトコルによっては ACL のことをフィルタという場合もある。)たとえば、IP、AppleTalk、IPX 用に設定されたルータ・インタフェースの場合は、少なくとも 3 つの ACL を定義する。ACL をネットワークの管理用ツールとして使うと、ルータのインタフェースに到着または送信するパケットのフィルタリングに柔軟性が加わることになる。

(1) 標準アクセス・リスト

標準アクセス・リストは、送信のみの制御を行い、IP アドレスの送信元をチェックする。たとえば、ホスト B からホスト A へのパケットの送信については許可し、ホスト C からの送信は拒否するとする。そうすると、ルータにパケットが入ってくる時にチェックすればよい。



では、どのように上記のような制御を行うかということ、ルータのインタフェース (Ethernet 0) に入力パケットをチェックし、ホスト B の PC は通信を許可してホスト C の PC は通信を許可しないという例を記述する。

基本的な ACL

```
Router # access-list 1 permit host 11.0.0.1
Router # access-list 1 deny host 11.0.0.2
Router(config-if)# ip access-group 1 in
```

アクセスリスト番号 → 1

許可 → permit host 11.0.0.1 「B」の IP アドレス

拒否 → deny host 11.0.0.2 「C」の IP アドレス

入力パケットをチェック → in

アクセスリスト番号は 1~99 が標準で 100~199 までが拡張として使われる。

ルータのコンソールに Cisco 専用のケーブルを接続して IOS を起動し、このように入力するとホスト B の PC からホスト A へのパケット送信が許可され、ホスト C から拒否される。しかし、このようにホスト数が少なければいいが、ホストの台数が複数台ある場合、ホストすべてを記述するのは面倒である。そういった面倒を解消するためにワイルドカード・マスク・ビットを使い指定するとよい。

ワイルドカード・マスク・ビットとはビットごとに指定し、1 のところをチェックする。例えば、10.0.0.0 のネットワークアドレスはすべて送信を許可しないとすると、0.255.255.255 と指定する。このようにネットワークアドレスごとに許可するかしないかを指定することができる。

標準 ACL 以外にも、拡張 ACL と名前付き ACL がある。ACL は 1 つのインタフェースの 1 つのプロトコルに 1 つしか指定できないことから、上記のような種類がある。標準 ACL は送信元のみの制御で、拡張 ACL は送信先も制御できる。名前付き ACL は、標準 ACL および拡張 ACL に番号ではなく名前をつけることができる。

6 Cisco のスイッチによる VLAN の設定例

< 3 個の VLAN の作成 >

```
Switch_A#vlan database
Switch_A(vlan)#vlan 10 name Accounting
Switch_A(vlan)#vlan 20 name Marketing
Switch_A(vlan)#vlan 30 name Engineering
Switch_A(vlan)#exit
```

< VLAN 10 へのポートの割り当て >

```
Switch_A#conf t
Switch_A(config)#int fa0/4
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 10
Switch_A(config-if)#int fa0/5
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 10
Switch_A(config-if)#int fa0/6
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 10
Switch_A(config-if)#end
```

< VLAN 20 へのポートの割り当て >

```
Switch_A#conf t
Switch_A(config)#int fa0/7
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 20
Switch_A(config-if)#int fa0/8
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 20
Switch_A(config-if)#int fa0/9
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 20
Switch_A(config-if)#end
```

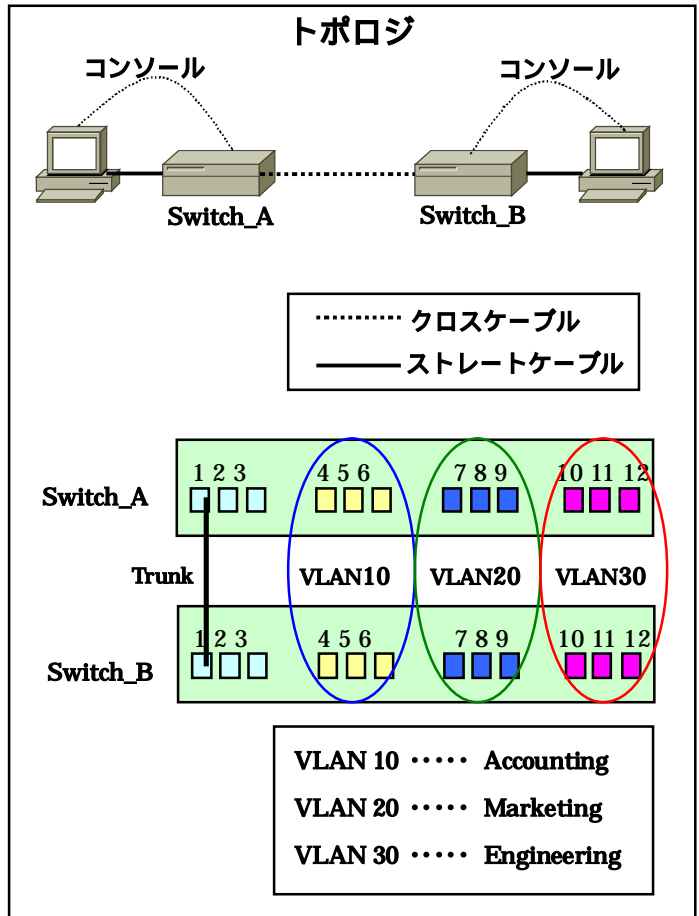
< VLAN 30 へのポートの割り当て >

```
Switch_A#conf t
Switch_A(config)#int fa0/10
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 30
Switch_A(config-if)#int fa0/11
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 30
Switch_A(config-if)#int fa0/12
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 30
Switch_A(config-if)#end
```

< トランクの作成 >

```
Switch_A(config)#int fa0/1
Switch_A(config-if)#switchport mode trunk
Switch_A(config-if)#end
```

```
Switch_B(config)#int fa0/1
Switch_B(config-if)#switchport mode trunk
Switch_B(config-if)#end
```



複数のポートを一度に設定する方法

```
Switch_A(config)#int range fa0/10 – 12
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 30
```

• VLAN 設定の確認

```
Switch_A#show int fa0/10 switchport
```

• VLAN メンバーシップの確認

```
Switch_A#show vlan
```

• VLAN の削除

```
Switch_A#vlan database
Switch_A(vlan)#no vlan 30
```

• トランクの確認

```
Switch_A#show int fa0/1 switchport
```

< V T P の設定 >

```
Switch_A#vlan database
Switch_A(vlan)#vtp server
Switch_A(vlan)#vtp domain group1
Switch_A(vlan)#exit
```

< V L A N の作成 >

```
Switch_A#vlan database
Switch_A(vlan)#vlan 10 name Accounting
Switch_A(vlan)#vlan 20 name Marketing
Switch_A(vlan)#vlan 30 name Engineering
Switch_A(vlan)#exit
```

< VLAN 10 へのポート割り当て >

```
Switch_A#conf t
Switch_A(config)#int fa0/4
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 10
Switch_A(config-if)#int fa0/5
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 10
Switch_A(config-if)#int fa0/6
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 10
```

< VLAN 20 へのポート割り当て >

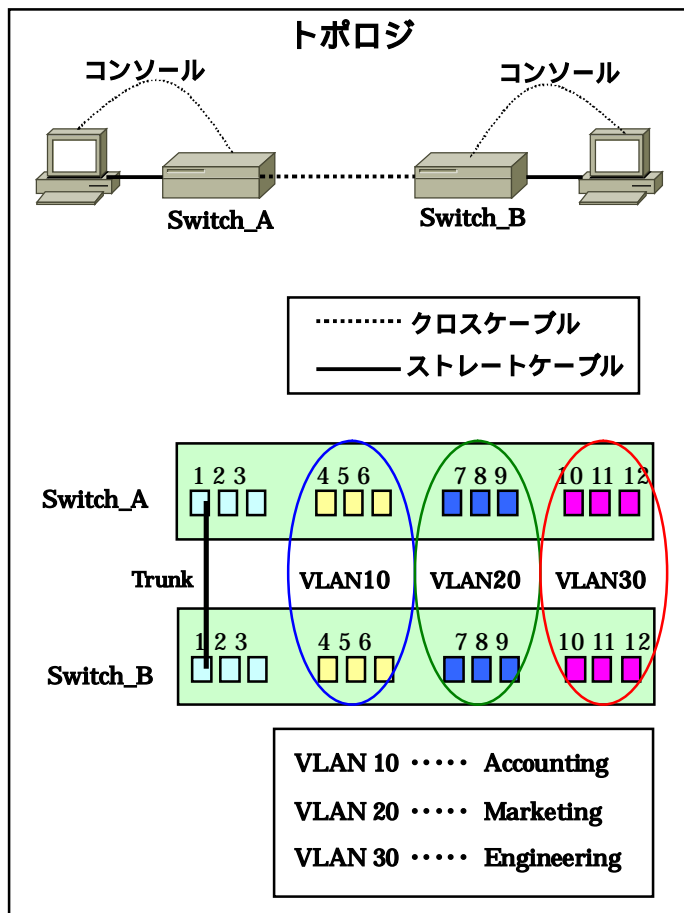
```
Switch_A#conf t
Switch_A(config)#int fa0/7
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 20
Switch_A(config-if)#int fa0/8
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 20
Switch_A(config-if)#int fa0/9
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 20
Switch_A(config-if)#end
```

< VLAN 30 へのポート割り当て >

```
Switch_A#conf t
Switch_A(config)#int fa0/10
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 30
Switch_A(config-if)#int fa0/11
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 30
Switch_A(config-if)#int fa0/12
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 30
Switch_A(config-if)#end
```

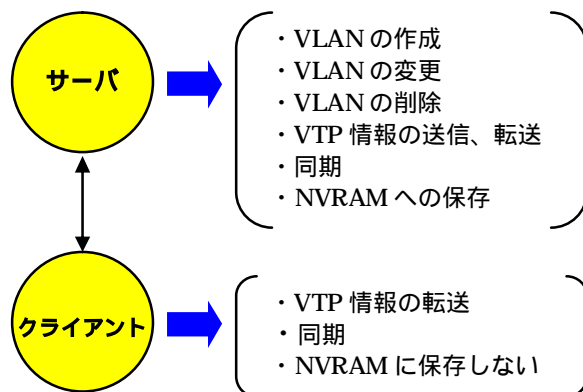
< V T P クライアントの設定 >

```
Switch_B#vlan database
Switch_B(vlan)#vtp client
Switch_B(vlan)#vtp domain group1
Switch_B(vlan)#exit
```



・ VTP (VLAN Trunking Protocol)

VLAN 構成情報を通知して同期させるメッセージプロトコル。



- ・ VTP の通知は5分ごと、あるいは変更があるときに送られる。
- ・ VTP サーバと VTP クライアントは、最新のリビジョン番号で同期される。
- ・ VTP 設定の確認
Switch_A#show vtp status

< トランクの作成 >

```
Switch_A(config)#int fa0/1
Switch_A(config-if)#switchport mode trunk
Switch_A(config-if)#end
```

```
Switch_B(config)#int fa0/1
Switch_B(config-if)#switchport mode trunk
Switch_B(config-if)#end
```

< VLAN 10 へのポート割り当て >

```
Switch_B#conf t
Switch_B(config)#int fa0/4
Switch_B(config-if)#switchport mode access
Switch_B(config-if)#switchport access vlan 10
Switch_B(config-if)#int fa0/5
Switch_B(config-if)#switchport mode access
Switch_B(config-if)#switchport access vlan 10
Switch_B(config-if)#int fa0/6
Switch_B(config-if)#switchport mode access
Switch_B(config-if)#switchport access vlan 10
Switch_B(config-if)#end
```

< VLAN 20 へのポート割り当て >

```
Switch_B#conf t
Switch_B(config)#int fa0/7
Switch_B(config-if)#switchport mode access
Switch_B(config-if)#switchport access vlan 20
Switch_B(config-if)#int fa0/8
Switch_B(config-if)#switchport mode access
Switch_B(config-if)#switchport access vlan 20
Switch_B(config-if)#int fa0/9
Switch_B(config-if)#switchport mode access
Switch_B(config-if)#switchport access vlan 20
Switch_B(config-if)#end
```

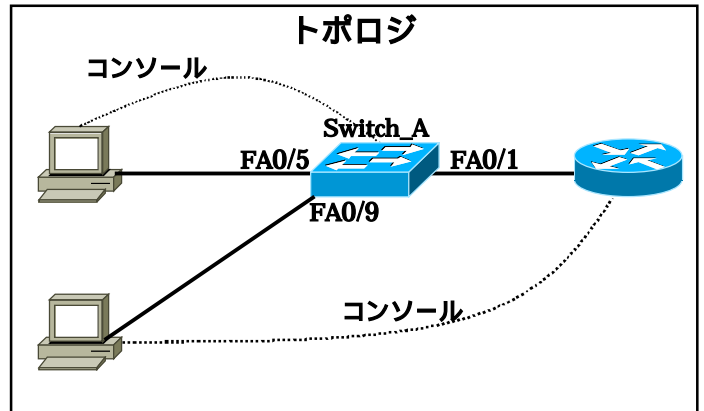
< VLAN 30 へのポート割り当て >

```
Switch_B#conf t
Switch_B(config)#int fa0/10
Switch_B(config-if)#switchport mode access
Switch_B(config-if)#switchport access vlan 30
Switch_B(config-if)#int fa0/11
Switch_B(config-if)#switchport mode access
Switch_B(config-if)#switchport access vlan 30
Switch_B(config-if)#int fa0/12
Switch_B(config-if)#switchport mode access
Switch_B(config-if)#switchport access vlan 30
Switch_B(config-if)#end
```

「VLAN 間ルーティングの設定」

```
< VLANの作成および命名 >
Switch_A#vlan database
Switch_A(vlan)#vlan 10 name Sales
Switch_A(vlan)#vlan 20 name Support
Switch_A(vlan)#exit
```

```
< VTPプロトコルの設定 >
Switch_A#conf t
Switch_A(config)#int fa0/5
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 10
Switch_A(config-if)#int fa0/6
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 10
Switch_A(config-if)#int fa0/7
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 10
Switch_A(config-if)#int fa0/8
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 10
Switch_A(config-if)#end
```



```
Switch_A#conf t
Switch_A(config)#int fa0/9
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 20
Switch_A(config-if)#int fa0/10
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 20
Switch_A(config-if)#int fa0/11
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 20
Switch_A(config-if)#int fa0/12
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 20
Switch_A(config-if)#end
```

```
< トランクの作成 >
Switch_A#conf t
Switch_A(config)#int fa0/1
Switch_A(config-if)#switchport mode trunk
Switch_A(config-if)#end
```

```
< ルータの設定 >
router>enable
router#conf t
router(config)#hostname Router_A
Router_A(config)#enable secret cisco
Router_A(config)#line con 0
Router_A(config-line)#password cisco
Router_A(config-line)#login
Router_A(config-line)#line vty 0 4
Router_A(config-line)#password cisco
Router_A(config-line)#login
Router_A(config-line)#exit
Router_A(config)#int fa0
Router_A(config-if)#no shutdown
Router_A(config-if)#int fa0.1
Router_A(config-subif)#encapsulation dot1q 1
Router_A(config-subif)#ip address 192.168.1.1 255.255.255.0
Router_A(config-if)#int fa0.2
Router_A(config-subif)#encapsulation dot1q 10
Router_A(config-subif)#ip address 192.168.5.1 255.255.255.0
Router_A(config-if)#int fa0.3
Router_A(config-subif)#encapsulation dot1q 20
Router_A(config-subif)#ip address 192.168.7.1 255.255.255.0
Router_A(config-subif)#end
```

第3章 学校環境におけるセキュリティ

学校には、生徒の個人情報をはじめ多くの機密データが存在しており、そういったデータを外部からの不正アクセスや侵入から守り、安心して校内のネットワークを活用することができるように、セキュリティ技術について身につけネットワークを構築していきたいと考えている。

セキュリティに関する基礎的な学習として、クラッカーと呼ばれる攻撃者からの攻撃パターンを知ることから行った。攻撃パターンには、IPアドレスを収集（ICMP エコーを使った方法）、ポートスキャン（開いているポートを探す）、アプリケーションバナーを調査（バグを探しセキュリティパッチを適用していないプログラムを探す）、バッファオーバーフロー攻撃（プログラムの不具合を利用して OS のメモリをあふれさせたうえ、任意のプログラムを実行する）、踏み台を使った DoS 攻撃（特定のホストに大量の packets を送りつけることで本来のサービスを妨げ、それによって被害をもたらす攻撃）、なりすまし（通信先ホストになりすまして、あるホストを騙す）があり、そういった脅威について学習を行った。

次に、インターネットからの脅威に対応するための手段、そして防衛のための一般的な手段として利用されているファイアウォール、そしてファイアウォールを実現するための技術であるパケットフィルタリング（あらかじめ設定したルールに照らしてそのパケットを通すか通さないかを判断する）、アプリケーションゲートウェイ、アドレス変換することによりネットワーク内を守る NAT と IP マスカレードの技術についての学習を行った。

それ以外にも、ウイルス感染の仕組みや外部にサーバを安全に公開するための方法や盗聴を防ぐための通信、PKI（公開鍵暗号基盤）と電子署名について学習した。

以上のように、ネットワークにおける脅威とその防御の両面から、ネットワークにおけるセキュリティ、各ホストにおけるセキュリティ、通信にかかるセキュリティについて広く調査し、セキュリティに関する暗号通信技術およびその知識を身に付けるための研修を実施した。また、このような研修を通して、校内における安全なネットワーク構築が行えるよう必要なスキルを身に付け、セキュアな環境を実現したいと考えている。また、認証局ソフトウェア（Easy Cert：名古屋工業大学電気情報工学科の岩田研究室で開発された認証局ソフトウェア）を使い、実習を通して PKI（Public Key Infrastructure：公開鍵暗号基盤）の理解を深めた。

所属校では、ネットワークの監視やログの確認を行うことがほとんどなかった。そこで、ネットワーク接続装置から得られるトラフィック情報を、LAN を介して収集しそれを視覚化するシステムについて調査を行い、ネットワークの監視を行うためのツールとして MRTG の導入について検討を行った。MRTG（The Multi Router Traffic Grapher）とは、ネットワークの負荷を監視するツールである。監視対象のルータに対して、SNMP を用いてトラフィックの処理量を定期的にお問い合わせ、その値をグラフ化する。ネットワークの調子が悪くなったときや、どのルータで混雑しているかを調べたりするのに使用する。監視結果は HTML 形式のページとして出力され、Web ブラウザ経由で参照することができる。MRTG は、その使い勝手のよさから、大学のキャンパス・ネットワークの運用や ISP における簡易管理ツールとして広く利用されている。

インターネットセキュリティ

最近では ADSL や CATV インターネットの利用など、学校内外においてもインターネットに常時接続される環境が一般的になってきた。このため、外部から自分のパソコンにアクセスされてしまう例も珍しくなくなってきている。個人のパソコンに侵入されることも困るが、学校のパソコンにアクセスされ、生徒の個人データが外部に漏れるようなことはあってはならない。そのためには、セキュリティに関する知識を十分に身に付け、インターネットからの脅威に対応するための手段を整えておく必要がある。そこでインターネットセキュリティに関して詳しく述べていく。

攻撃パターンを知る

セキュリティ対策の第一歩は「敵を知る」ことである。クラッカーと呼ばれる攻撃者がどのようにネットワークセキュリティを侵害し、それによってどのような被害を与えるのか。セキュリティ対策とは、クラッカーの侵害行為に対して予防線を張ることといえる。侵害の手法はパターン化しており、そのパターンを理解し、ターゲットにされないようにすることが大切である。

インターネットに接続している限り、クラッキング(クラッカーによる侵害行為)の対象になるのは仕方がない。クラッカーはインターネットに接続するホストを無差別にターゲットにしている。つまり、インターネットに接続するホストから幅広く調査して、適当なものがあればそれを攻撃対象にする。自分の PC をそのまま使ってクラッキングするクラッカーはおらず、第 3 者のホストを「踏み台」にして最終ターゲットを攻撃する。踏み台とは、クラッカーに操られて攻撃に加担するホストのことで、ターゲットとは、こうした踏み台に使うホストのことである。

1 IP アドレスを収集

インターネットで通信するためにはグローバル IP アドレス(以下 IP アドレス)が必要となる。クラッキングのほとんどは、インターネットを介した通信として行われるため、IP アドレスはクラッカーにとって非常に重要な情報である。約 4 3 億個の IP アドレスのうち、日常的に稼働している IP アドレスを収集することがクラッキングの最初の段階となる。

有効な IP アドレスは、様々な方法で収集される。最も頻繁に採られるのは、ICMP エコーを使った方法である。ICMP (Internet Control Message Protocol) とは、パケット配送を担当する IP と同じネットワーク層に属するプロトコルであり、IP レベルで通信が可能かどうか、可能でなければどんな状況なのかを報告する働きをする。そのうち ICMP エコーは、通信先のホストが稼働しているかどうか、稼働している場合どのくらい応答時間がかかるかを調べるものである。これは、「ping」コマンドで送ることができる。あるホストに対して ping を発行すると、IP レベルでホストが稼働しているかどうかを識別できる。稼働していれば応答時間とともに ICMP エコー応答のパケットが戻ってくるし、稼働していなければエラーメッセージが表示される。

ping は基本的に 1 台のホストに対して発行されるが、専用ツールを使えば連続したアドレス範囲で ping を送ることもできる。さらに、掲示板サイトなどに不用意に表示された IP アドレスも収集の対象になる。掲示板の書き込みから、ユーザが常時接続していることや、あまりネットワークに詳しくなさそうだということがわかれば「踏み台にしてやろう」と考えるクラッカーがいるのである。

2 ポートスキャン

ICMP エコーを使ってホストの稼働状況がわかって、まだ IP レベルで接続できることが判明した

けである。ある住所を入手して行ってみたら、そこに家が建っていることがわかったのと同じ程度である。次に必要な作業は、そのホスト（家）へ侵入する入口を探すことである。ネットワーク通信では、すべて「ポート」にパケットを受け渡すことで実現している。ポートにパケットを受け渡すのは TCP と UDP（トランスポート層）であり、ポートには 0~65,535 番までの番号が振られている。Web やメールサーバは、このうち 1023 番以下の特定ポート（ウェルknownポート）を使って、パケットを待ち受けしている。つまり、サーバプログラムは通常、クライアントからの接続要求を受け付けてサービスを提供するため、いつでもポートを開けてパケットの到達を待っていないなければならない。そのため公開サーバなど、ネットワーク上の他のホストに対して何らかのサービスを提供するホストは、必ずいくつかのポートを開けていなければならない。この開いているポートを探す行為が「ポートスキャン」である。

ポートスキャンは、ホストの各ポートに順番に接続要求（SYN パケット）を送ることで可能になる。特定のポートでサーバが待ち受けしていれば、その確認（ACK）と、クライアントに対するサーバからの接続要求（SYN）がセットになった「SYN+ACK」パケットが送られてくる。これが戻ってきたら、ポートが開いていることが判断できる。

ポートスキャンは、TCP が通信路であるコネクションを確立する「3ウェイハンドシェイク」を利用している。したがって、ポートスキャンを防御することは、TCP の仕組み上できない。では、コネクションを使わない UDP ではポートスキャンされないかといえば、そうでもない。UDP の通信には 3ウェイハンドシェイクはないが、サービスが稼動していなければ即座に ICMP エラーが返される。そこから UDP を使うサーバの待ち受け状態がわかる。

<ポート番号>

ビルでイメージする。 IPアドレスはビルの住所、ポート番号は各部屋番号
ビルの 25 号室（ポート番号 25 = SMTP）では手紙を 1 通ずつ受けたり出したりするサービスを行っている。
ビルの 110 号室（ポート番号 110 = POP3）では、誰からの要求によってその人物あてに届いた手紙を一括して送り出すサービスを実施している。

ポート番号は、ネットワーク経由で任意のサービスを受ける際に、そのサービスを識別するために用いられる。

IPアドレスはIPが対応するレイヤ3（ネットワーク層）で、ポート番号はTCP/UDPが対応するレイヤ4（トランスポート層）で機能する。

<パケットフィルタリング>

ビルの部屋なら鍵をかけておかなければ不審者が部屋に入り込んで何か悪さをするかもしれない。ポートも同様、使用/不使用に関わらず、鍵をかける必要がある。

パケットフィルタリングには、2種類のポリシーベースがある。

「初期状態では全てのパケットを通しておき、必要に応じてパケットをフィルタリングするための規則を設定するという」ポリシーと、「初期状態ではすべてのパケットを通さずに（リジェクトし）必要なものだけ通すように設定する」というポリシー。現在は後者のポリシーを採用している場合が多い。（デフォルトとなっている）

3 アプリケーションバナーを調査

どんなプログラムにも「バグ」と呼ばれる実装上の不具合がある。そのバグが悪用され、ホストへの侵入を許してしまうことがある。バグがセキュリティホールとなる可能性はきわめて高い。そこでクラッカーは、ポートスキャンで得られた待ち受けポートで稼動するサーバプログラムの種類やバージョン（アプ

リケーションバナーという)を調べる。ここからセキュリティホールがあるかがわかるからである。アプリケーションバナーを見てセキュリティパッチ(バグの修正プログラム)を適用していないプログラムが動作していることがわかれば、そのホストを手中に収めたのも同然である。バッファオーバーフロー攻撃を使って、実際にホストに侵入することができる。

アプリケーションバナーの取得には、リモートログインプロトコルの「Telnet」を使う。Telnet は通常、Telnet サーバ(TCP23 番ポートで待ち受け)に接続して、遠隔のホストからコマンドを送るのに使われる。しかし、Telnet 接続時に別のポート番号を指定すれば、Telnet サーバ以外のサーバにコマンドを送ることができる。

4 バッファオーバーフロー攻撃

ここまでのプロセスは、クラッキングまでの前調査である。実際に何か被害を被るわけではないが、通常の通信にはまったく不要の行為で、明らかにクラッキングの予兆と見ることができる。もし、この段階でセキュリティホールが発見されたら、攻撃を受ける可能性がきわめて高いといえる。

セキュリティホールに対する実際の攻撃には、「バッファオーバーフロー攻撃」がよく使われる。バッファオーバーフロー攻撃とは、プログラムの不具合を利用して OS のメモリをあふれさせたうえ、任意のプログラムを実行することをいう。

バッファオーバーフロー攻撃は、手法としては古典的ともいえる。そのため多くの場合、セキュリティパッチをまめに適用し、セキュリティホールを作らないことで防ぐことができる。

5 踏み台を使った DoS 攻撃

クラッカーが最終的に被害をもたらそうとしているホストは、個人的な思惑によって決められている。(ニュースになるのを期待して世界的に著名なサーバなど)しかし、こうした著名なサーバはきちんとした運用がなされているため、バッファオーバーフロー攻撃が通用しないことが多い。そこで、管理の甘いホストを探しそれを踏み台にして「防ぎようのない」方法で攻撃する。その一つが「DoS 攻撃」である。

DoS とは「Denial of Service」を意味し、「サービス不能」攻撃などと訳される。特定のホストに大量のパケットを送りつけることで、本来のサービス(通信機能)を妨げ、それによって被害をもたらす攻撃である。

DoS 攻撃にはいくつかの種類があるが、「スマーフ攻撃」や「SYN フラッド攻撃」が有名である。スマーフ攻撃は、ICMP エコー(ping)を悪用してホストの接続回線の帯域を食い潰す DoS 攻撃である。方法としては、あるネットワークに対して ICMP エコー要求をブロードキャストし、要求を受け取ったホストは送信元へ ICMP エコー応答を返すが、要求はブロードキャストで行われているため、何十、何百というホストから同時に応答が戻される。ICMP エコー要求の送信元 IP アドレスを別の IP アドレスに書き替えておけば、膨大な量の応答を別のホストへ向けられるという仕組みである。

もう一つの SYN フラッド攻撃は、TCP の 3 ウェイハンドシェイクを悪用してホストを応答不能に陥れる DoS 攻撃である。方法としては、ターゲットに対して端時間に膨大な量の接続要求(SYN)パケットを送りつける。SYN を受け取ったホスト(ターゲット)は SYN+ACK を返して、通信相手(クラッカー)から最後の ACK が戻ってくるのを一定時間待機するが、その間ホストのリソース(メモリ)は消費される。もしこのとき、最後の ACK を送り返さないまま、次々に大量の SYN を送ればホストはいずれリソースを使い果たして、応答不能に陥ってしまう。

こうした攻撃はいわば物量攻撃なので、たくさんのホストから一斉に仕掛けたほうが効果的である。しかし、1 箇所から連続して大量のパケットを送ると、相手のファイアウォールが遮断することもある。そこで多くの場合、DoS 攻撃は複数の踏み台から同時に行う。

6 なりすまし

バッファオーバーフローや DoS 攻撃のように「力づく」でホストを攻撃する以外にも、「こっそり」と情報を盗み出すクラッキングもある。代表的なものが「なりすまし」で、これは文字通り、本来の通信先ホスト（サーバ）になりすまして、あるホストを騙すことである。

実際の方法としては、DNS サーバの情報を書き替える「DNS スプーフィング」が有名である。DNS サーバはドメイン名に対応する IP アドレスを回答するサーバであり、同時に自分が保持していない情報は、別のサーバに尋ねるといった機能を持っている。そこで、ある DNS サーバが別の DNS サーバに問い合わせをしたときに、その通信を途中で横取りし（セッションハイジャック）嘘の IP アドレスを答える。嘘の IP アドレスを教えられた DNS サーバは、それを元の問い合わせ先（クライアント）に回答する。その結果、クライアントは知らずも別のサーバに接続し、そのまま通信してしまうというわけである。

ファイアウォール

インターネットからの脅威に対応するための手段、そして防衛のための一般的な手段として利用されるのがファイアウォールである。クラッカー（攻撃者）の攻撃にはいくつかのパターンがあり、前準備の段階ではホストへ侵入する入り口を探している。その入り口よりも前に設置し、不正な侵入を前もって防御するための機能がファイアウォールである。ファイアウォールは、「安全でないネットワーク」であるインターネットと、社内ネットワークなどの「安全を確保したいネットワーク」との境界に唯一の出入口として設置する、文字通り「壁」のような存在である。

インターネットの脅威として、以下の表のようなことがあげられる。

脅 威	意 味	現実に例えた場合
乗っ取り	外部からの侵入者（クラッカー）がシステムの最高の利用権限を得てしまう状態。	泥棒に自宅に侵入された状態。自宅にあるすべてのものが危険にさらされる。
ポートスキャン	システムの弱点を探し出す。情報収集であり、直接的な被害に直結するものではない。	泥棒が侵入口を探してドアや窓を丹念に調べている状態。
物量作戦	無意味なデータを大量に送りつけることで通信を阻害する。	暴走族が深夜に自宅の周りを走り回るとか、街宣車に乗り付けられるという状態。
一撃必殺	あるポートに特定のデータを送りつけるとシステムがダウンするといった類のもの。	現実の家屋にたとえれば放火に近い。
メールウイルス	メールに添付したマクロなどにウイルスを仕込むメールウイルスによる攻撃。	剃刀入り封筒や爆弾が自宅に送られてくるといったイメージ。

インターネットの脅威

現実の家屋に対してはそうそう簡単に生じるものではないが、コンピュータネットワークの世界では、現実世界よりも罪悪感が薄くなりがちである。こうした行為を犯した場合のクラッカー側が負うリスクも、現実世界の犯罪に比べれば少ないので、被害に遭う可能性も高い。そのため何らかの防御手段を考えておくことが必要である。そのためにまず利用される一般的な方法が、ファイアウォールである。

外部からの脅威の侵入を食い止めるための防御手段一般を指す。ファイアウォールの実装手段には何種類もあり、実装方法によって防御できるもの、向き不向きがある。

パケットフィルタリング

ファイアウォールを実現する技術で基本となるのが、「パケットフィルタリング」である。パケットフィルタリングとは、パケットに含まれるさまざまなヘッダ情報を参照し、あらかじめ設定したルールに照らしてそのパケットを通すか通さないかを判断する。

1 パケットフィルタ

パケットをフィルタリングする機能。パケットを一つずつチェックして、事前に設定された条件に従って通過させたり遮断したりする機能。ただし、一般的には IP および TCP/UDP のヘッダまでしかチェックしない。パケットフィルタの判断材料には、送信元 / 受信先それぞれの IP アドレス、ポート番号やプロトコル、そして最初のパケットか、既存のセッションに属する応答かなどがある。これを適宜組み合わせることで、内部から外部への通信は許可するが、外部から内部への通信は、内部から開始された通信の応答以外は遮断するといった機能が実現できる。また、ポートを条件として利用すれば、通信に必要なポート以外への着信をすべて遮断することが可能となる。そういった場合、NAT が非常に有効である。

一方、通信自体は正当だが、データに不都合があるというケースにメールウイルスがある。メール自体がそのユーザに送られてきたものであり、ユーザ自信が POP などを利用してメールをサーバから転送してくる場合、そのパケットのヘッダなどに不正な点がないし、当然 NAT による隠蔽も意味をなさない。こうした「正当な通信に混入される不正な情報」を遮断するのはパケットフィルタでは困難である。また、物量作戦に関してもパケットフィルタに限らず有効な対策はない。

2 アプリケーションゲートウェイ（最近ではプロキシサーバと呼ばれる）

アプリケーションレベルで中継を行い、その過程で詳細なチェックを行うことができる。単純に言えば、クライアントの代わりに、まずファイアウォールが全データを受信し、チェックしたあとクライアントに渡すという手順になる。Web アクセスの際に使われる HTTP プロキシなどがその例である。ただし、プロキシサーバには様々な用途があり、必ずしもファイアウォールとしてのみ利用されるとは限らない。HTTP プロキシの場合も、実際キャッシュサーバとして利用される例が目立つ。メールに添付されてくるウイルスをチェックするウイルスチェックなどでは、一度ファイアウォールがメールを受け取ってウイルスチェックをかけたあと、本来のメールクライアントに再度データを渡すという処理をするものが多いが、これもアプリケーションゲートウェイの実装だといえる。

ファイアウォールの実装場所にも様々な例が考えられる。最近目立つのは、PC 以外のハードウェアに組み込まれる例である。ISDN ダイアルアップルータや、ケーブルモデムに接続することを想定した「ブロードバンドルータ」のほとんどすべてには、パケットフィルタの機能やアドレス変換の機能が組み込まれている。こうした組み込み型のファイアウォールでは、機能面では拡張性に欠ける面があるが手軽に利用でき、PC よりも安定して動作することが期待できる。一般家庭や小規模な組織では、こうしたパケットフィルタ内蔵のデバイスを利用するのが簡単でよい。

ソフトウェア製品として実装されているファイアウォールでは、高価なものから OS 標準の機能として提供されるものまで様々なものがある。高機能なものでは、アプリケーションゲートウェイとパケットフィルタを組み合わせるほか、LDAP (Lightweight Directory Access Protocol) などのディレクトリサービスや認証メカニズムと連携して高度なセキュリティ機能を提供するのが一般的である。

ファイアウォールを組み込んだ OS としては Linux がよく知られているが、Windows 2000 にも簡単なパケットフィルタ機能は提供されている。したがって、外部ネットワークとの接続点にこうした OS が稼

動するマシンを設置しておくだけでも小規模環境では有用である。さらに、Windows95以降では、クライアント上で直接動作する「パーソナルファイアウォール」があり、1台しかPCを所有していないホームユーザには有用である。

3 パケットフィルタリング

ビルの部屋なら鍵をかけておかなければ不審者が部屋に入り込んで何か悪さをするかもしれない。ポートも同様、使用/不使用に関わらず、鍵をかける必要がある。

パケットフィルタリングには、2種類のポリシーベースがある。「初期状態では全てのパケットを通しておき、必要に応じてパケットをフィルタリングするための規則を設定するという」ポリシーと、「初期状態ではすべてのパケットを通さずに（リジェクトし）必要なものだけ通すように設定する」というポリシー。現在は後者のポリシーを採用している場合が多い。（デフォルトとなっている）

アドレス変換の必要性

最近では、LAN 内部などではプライベートアドレスを利用する方が一般的である。個々のマシンにグローバルアドレスを割り当てるのは、例外的なケースになってきている。プライベートアドレスを利用するには、NAT（Network Address Translation）またはIP マスカレードと呼ばれる機能を利用してアドレスを変換する。NATは1対1の対応で、IP マスカレードは1対多の対応となる。最近では、NATと単純に呼びつつも、実体としては1対多のIP マスカレードであるという例が多い。NAT/IP マスカレードの機能は、最近ではISDNダイヤルアップルータやブロードバンドルータ、そして一般的なOSに実装されている。クライアントOSでも、Windows98 Second Edition以降で実装されている「インターネット接続共有」という機能は、実体としてはIP マスカレードである。

NATとIP マスカレードは「単一のグローバルアドレスを複数のマシンで共有できる」という点に関しては共通だが、セキュリティ面からは重要な違いがある。単純なNATの場合、グローバルアドレスとプライベートアドレスが単純に変換されるだけなので、LAN内に複数のPCがある場合「グローバルアドレスがどのプライベートアドレスにマッピングされているか」はわからないが、そのPCに対して外部からアクセスすることは可能である。この場合、グローバルアドレスを指定してポートスキャンをかけると、実際にはプライベートアドレスを利用しているPCのポートが走査される。マッピングが変更されれば状況が変化るとはいえ、セキュリティが強化されることはない。

一方IP マスカレードでは、グローバルアドレス+ポートがプライベートアドレス+ポートに変換される。このように、ポート番号も含めて変換されるため、ポートスキャンは実質上意味をなさなくなる。つまり、IP マスカレードを利用するだけでポートスキャン対策になる。

セキュリティを考えた場合、IP マスカレードを利用するだけで簡易ファイアウォールと見なせるレベルのセキュリティが実現できる。特に、ブロードバンドルータなど、デバイスのみグローバルアドレスが割り当てられている状態であれば、乗っ取りやポートスキャン、一撃必殺型攻撃に関してはほぼ保護される。

さて、このようにセキュリティ面での効果も期待できるIP マスカレードだが、一方ではセキュリティを強化するためには利用が必須というわけではない。ファイアウォールを適切に設定すれば、グローバルアドレスを利用していたとしても外部からのアクセスを個々のPCごとに制御することは可能である。また、プロキシサーバを経由して接続することで個々のPCに外部から直接接続できないような環境を構築することもできる。

NAT と NAPT

NAT (Network Address Translation) と NAPT (Network Address Port Translation : I P マスカレード) の違いについて、NAT も NAPT も、企業などの組織内で使用できるアドレス (ローカルアドレス) と、インターネット上のアドレス (グローバルアドレス) を透過的に相互変換し、1 つのグローバルアドレスを複数のコンピュータで共有する技術である。相違点は、NAPT ではアドレスだけでなく TCP / UDP のポート番号も動的に変換されるので、1 つのグローバルアドレスで複数のコンピュータからの同時接続を実現できる。NAT は「 1 : 1 のアドレス変換」で、NAPT は「 1 : 多のアドレス変換」である。

I P マスカレード	NAT による IP アドレスの変換だけでなく、その上位プロトコルである TCP / UDP のポート番号も識別することで、異なる通信ポートを利用するものについては、1 つのグローバル IP アドレスを利用して、複数のローカルノードが外部と通信できるようにしたソフトウェア。UNIX システムの 1 つである Linux 上で最初に開発された。「masquerade」は「仮面舞踏会」という意味。
-------------------	--

ウイルス感染の仕組み

ウイルスといっても様々なパターンがあり、当然その仕組みや目的も異なるし対策も変わってくる。そこで、ウイルスとは何かというところから記述していく。

国内のウイルス届出窓口となっている政府機関の IPA (Informaion-technology Promotion Agency : 情報処理振興事業協会) によると、コンピュータウイルスは「 プログラムに寄生する極めて小さなプログラムであり、 自分自身を他のプログラムファイルにコピーすることで増殖し、 コンピュータウイルス自身に組み込まれたユーザの予期しない動作を起こすことを目的とした特異なプログラム」とされている。

現状では、 の特徴をもつプログラムをひとくくりにして「ウイルス」と呼ぶ場合が多い。しかし、厳密な意味でのウイルスは不正プログラムの 1 つの形態なので、他の不正プログラムである「ワーム」や「トロイの木馬」とは別ものである。ワームやトロイの木馬は、それ自身が 1 つの独立したプログラムとして動作する点で の特徴を持つウイルスとは異なる。ワームは自分自身の増殖が主目的であり、作成者はどれだけ広範囲に広がるかに焦点を当てて作成している。一方トロイの木馬は、ターゲットになる PC に潜ませておいて、あとからクラッキングするために利用する仕掛けである。この 2 つのウイルスはユーザの知らないところで勝手に動作して被害をおよぼすという点は共通している。また、現在はメールが普及したことで、以前に比べて短時間で広範囲に不正プログラムが行き渡りやすくなっている。また、「Code Red (コードレッド)」のような、ウイルス、ワーム、トロイの木馬が連携するタイプの不正プログラムが増加している状況もある。

ウイルスの正体はプログラムであり、ウイルスを実行することで他のプログラムにウイルスが埋め込まれたりする。一般にウイルスが埋め込まれているプログラムを「ウイルスに感染しているプログラム」と呼ぶ。ウイルスがいつ活動を始めてもおかしくない状況を「感染」というのである。このことから、ウイルスに感染するのは「ウイルス作成者が送り込んできたウイルスプログラムを実行する」ことが前提となる。裏を返せば、ウイルスを実行しなければ感染しないということである。

以前は、ウイルスはフロッピーなどの物理的な媒体を経由して運ばれることが多かった。メールを介して次々にウイルスが広まる現状では、悪循環に陥る可能性が高い。誰かがどこかで止めなければ、永久にループしてウイルスの被害はなくなる。

また最終的な目的はどうであれ、ウイルス作成者はウイルスが広範囲に広がることを期待し、自分の能力

を誇示したい場合もあるだろうし、DoS 攻撃の攻撃元に利用する場合は、攻撃元が多ければ多いほど効果的である。現在のようにこれだけメールが普及していれば、それを使わない手はない。つまり、狙った相手にウイルスプログラムを実行させれば、後はメールに乗って広範囲に広がることは明らかなのである。

先に「ウイルスプログラムを実行しなければウイルスには感染しない」と述べたが、よくクラッカーに狙われる Outlook Express では、プレビューする際に Internet Explorer のプログラムモジュールを呼び出すようになっている。このため、ActiveX や JavaScript など書かれたプログラムを Outlook Express でプレビューすると、Internet Explorer が実行環境（シェル）として呼び出されてしまう。「Nimda（ニムダ）」や「Klez（クレズ）」などは、この方法を利用して爆発的に広がった。

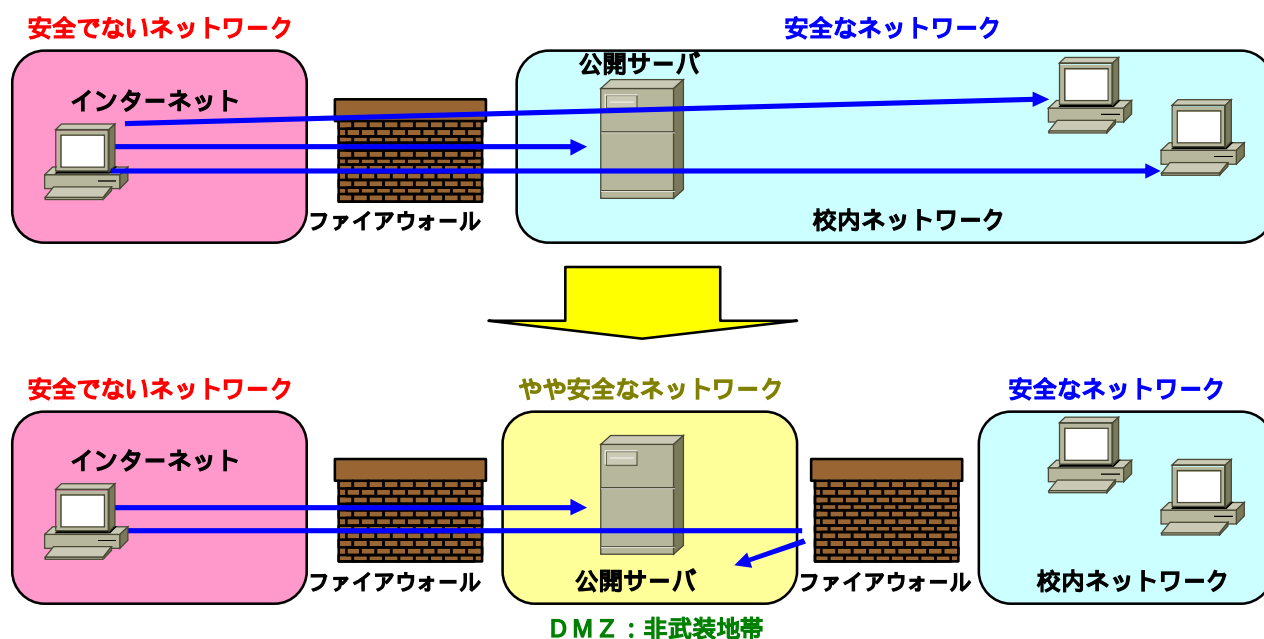
具体的には、セキュリティホールを利用するため、バッファオーバーフローを起こすような特定のコマンドやスクリプトをメールの本文に記入し、最後に添付ファイルを実行するようにしておく。すると、メールをプレビューした時点でスクリプトが実行され、そのまま添付ファイルも実行されてしまう。

これらの対策として、Outlook Express や Internet Explorer を使わなければいいという意見もあるが、一番の対策は、セキュリティパッチをこまめに当てたうえでメールクライアントの「自動的にプレビューを表示する」機能をオフにすることである。

DMZ とホストの要塞化

1 外部にサーバを安全に公開する

外部にサーバを公開するということは、安全でないインターネットにサーバを公開するということである。そのためにはそれなりの工夫が必要となる。ファイアウォールの内側（校内ネットワーク内）に公開サーバを設置すると、インターネットからの通信をすべて遮断してしまい、サーバを公開できない。かといってサーバへの通信を許可すれば、外部からの接続を校内に入れてしまうことになる。つまり、他のホストの安全性が公開サーバと同じレベルまで下がってしまう。そこで、もう一つ別のネットワークでサーバを公開する。1台のファイアウォールでは、ルールが一つしか決められないため、「安全な校内ネットワーク」と「そうでないインターネット」の2つにしか切り分けられない。しかしファイアウォールを2台設置すれば、ルールは2つ決められる。そうすると3つのセグメントができ、1つ目は安全でないネットワーク、2つ目はやや安全なネットワーク、3つ目が安全なネットワークとなる。この3つ目のセグメ



ントに、校内ネットワークと異なるセキュリティポリシー（パケット通過のルール）を適用すれば公開サーバを安全に運用できる。この3つ目のセグメントのことをDMZ（DeMilitarized Zone：非武装地帯）という。DMZは、2台のファイアウォールにはさまれた中間のセグメントのことを指す。インターネットとDMZ間は「やや安全」に、DMZと校内ネットワーク間を「絶対安全」というポリシーを作れば、校内ネットワークのセキュリティを下げずにサーバを公開できるようになる。

2 DMZを介したパケットの流れ

3つのセグメント間でのパケットの流れにおいて、基本的にパケットは「否定」「必要なポートのみ許可」「問い合わせに対する応答のみ許可」の3種類のルールに基づいてネットワーク内を流れる。

ファイアウォールの設定			
接続元		あて先	動作
インターネット		DMZ	必要な通信のみ許可
		校内ネットワーク	拒否
DMZ		インターネット	問い合わせに対する応答のみ許可
		校内ネットワーク	問い合わせに対する応答のみ許可
校内ネットワーク		インターネット	拒否
		DMZ	必要な通信のみ許可

インターネットと校内ネットワークの間は、パケットを通さない「拒否」になっており、双方とも直接通信できない。つまり、インターネットから直接校内ネットワークにアクセスできず、逆に校内ネットワークからインターネットにも直接出られない。これで校内ネットワークは「絶対安全なネットワーク」として守られる。

「必要なポートのみ許可」は、インターネットと校内ネットワークが、DMZにアクセスする際のルールである。DMZにメールサーバ、Webサーバ、DNSサーバの3台を設置すると、プロトコルとしては、SMTP（25番）、HTTP（80番）、DNS（53番）の3つのみがDMZに出入りする。つまり、DMZに設置した公開サーバにアクセスさせるためには、この3つの宛先のルールポートに対する通信を許可すればよいことになる。逆に、これ以外はアクセス拒否にしておけば、ファイアウォールに必要最低限のポートを開けることになるので、一定レベルのセキュリティが保たれる。

「問い合わせに対する応答のみ許可」は、先のルールとは逆にDMZから他の2つのセグメントに向けた通信に適用される。公開されたメールやWeb、DNSサーバへの問い合わせに対する応答のみ許可される。具体的には、それぞれの送信元ポートが25、80、53番だった場合は通信を許可し、それ以外は拒否されるということになる。

3 ファイアウォールの機器

ファイアウォールを構築する機器として最も原始的なものは、ルータである。ルータはパケットフィルタリングを使ったファイアウォールである。あるいは、1台のPCサーバにNICを2枚挿してインターネットと校内ネットワークを接続し、OSのパケットフィルタリング機能やプロキシソフト、ファイアウォール専用ソフトを使って構築することもある。DMZは2台のルータで構築したり、PCサーバにもう1枚のNICを取り付けることで作ることができる。しかし、いずれの方法でも、複数のルータ

を適切に設定したり、ゼロからマシンを構築するなどの手間がかかる。

そこで最近主流なのが、ファイアウォール専用機（アプライアンス）を利用するケースが多くなってきている。

4 サーバの要塞化

公開サーバを設置するための DMZ は、インターネットからの接続を直接受け付けるための「やや安全なネットワーク」にすぎず、校内ネットワークよりも危険度が高いといえる。少なからず、攻撃される危険性がある。そこで公開サーバには、サーバ自体を強固なものにする「サーバの要塞化」というセキュリティ対策も欠かせない。サーバの要塞化は、複数の手法を組み合わせで行う。

セキュリティパッチの適用

サーバで稼動している OS やアプリケーションを、常に最新のものにしておくという方法がある。インターネットでは、日々新しいセキュリティホールが発見され、それに追従する形で各ベンダーから最新のセキュリティパッチ（修正プログラム）が提供される。

不要なサービスの停止

サーバで動作している不要なサービスを止める。Windows や UNIX 系 OS に限らず、OS はインストール直後の状態で、何らかの機能を提供するための「サービス」と呼ばれるプログラムが動作している。不要なサービスとして、外部からホストにリモートログインするための Telnet が挙げられる。Telnet では、ユーザ名とパスワードが判明してしまえば、そのマシンにログインできる。また、通信は平文で行われるため、盗聴されてしまえばパスワードの情報が漏れてしまう。そこで現在では、暗号化通信が可能な SSH（Secure SHell）が使われることが多い。

強固なパスワードの設定

管理者用のパスワードを強固なものにする。クラッカーがサーバに侵入しようとする際は、とりあえず考えられる文字の組み合わせをすべて試したりするからである。

ログの管理

最後に、サーバのログをきちんと管理することも要塞化につながる。もちろんログを収集するだけでは意味がないので、きちんとした解析が必要となる。ログの解析ツールを使えば、システムの状態だけではなく、攻撃を受けた形跡をビジュアル的に調査できる。また、ログを数ヶ月保存しておく必要がある。これは攻撃を受けたら、その痕跡を数ヶ月に遡って調べる場合もあるからである。さらにログは、安全な場所に保管し、syslog を使って他のマシンにログを定期的に転送しておくことも要塞化の有効な方法である。

盗聴を防ぐための通信

1 暗号化通信

インターネットで送られるデータは、郵便の「はがき」に書かれた文字と同じで、データはホストが作成したままの状態配送される。テキストデータであれば、生のテキストがネットワークに流れ、相手に届くまでのルートもあらかじめ決められていないため、どこをどう通るのかわからない。つまりインターネットは、データの中身が誰の目に触れてもおかしくない状態で通信されている。はがきが大事な用件の伝達に不向きなように、インターネットでも機密性の高い情報のやり取りには向いていない。しかし現在では、インターネットが生活や仕事の一部になっているため、平文で送らないようにする方法を取る必要がある。それを行うのが暗号化通信である。

暗号化通信は、送信元で平文のデータを加工する「暗号化」を行い、受信先で元のデータに戻す「復号化」をすることで実現される。

2 暗号鍵の共有方法

暗号鍵の共有には2通りの方法がある。1つ目は、送信ホストと宛先ホストで同一の暗号鍵を共有する方法である。この方法は「共通鍵暗号方式」と呼ばれ、暗号化通信するホスト同士で共通の鍵を共有する。暗号化通信したい相手に自分の鍵を渡すことにより実現できる非常にシンプルな方法である。しかし、共通鍵暗号方式の課題として、暗号鍵の受け渡しをどのように行うかである。離れている相手に鍵を渡すために、メールの添付ファイルとして送れば、その鍵自体が盗聴される恐れがある。安全を期すためには、暗号鍵をフロッピーディスクに入れて手渡しするしかない。そこで、もっと手軽にかつ安全に暗号鍵を受け渡せる方法が考え出された。それが2つ目の「公開鍵暗号方式」である。公開鍵暗号方式では、暗号鍵を2つに分けて、1つを一般に公開する（公開鍵）。そして、もう1つの鍵は自分だけで管理する（秘密鍵）。暗号化はどちらの鍵を用いても行えるが、復号化できるのは他方の鍵だけとなる。つまり、公開鍵を使って暗号化してもらえば、それを復号化できるのは秘密鍵を持つ「自分だけ」ということになる。

公開鍵暗号方式なら、共通鍵暗号方式の課題である鍵の受け渡しの問題はなくなる。しかし、公開鍵暗号方式にも問題がある。それは、公開鍵を配布している人が「本当に通信しようとしている相手」かどうか何の保証もないことである。もし、公開鍵の持ち主が他人になりすました悪意の第三者であれば大変なことになる。そのため公開鍵暗号方式では、公開鍵の所有者の身元を確認したうえで通信できる仕組みが不可欠である。これは現在、PKI という技術によって実現されている。

また公開鍵暗号方式は、身元の確認や、512ビットや1024ビットの長い鍵長のため重く、処理に時間がかかるという問題がある。そこで実際の暗号化通信では、最初に公開鍵暗号方式を使って共通鍵を送受信し、そのあとは処理の軽い共通鍵方式を使うという「2つの方式の組み合わせ」で行う場合がほとんどである。

3 さまざまな暗号化技術

暗号化技術とは、暗号アルゴリズムを機能として使えるようにするものである。これは通信のレイヤ（層）ごとにいくつか開発されている。

TCP/IPでの通信は、4つの階層に分かれて機能している。下から順番に、ホストの物理的な接続を提供する「データリンク層」、IPアドレスに基づいてデータ（パケット）を送受信する「ネットワーク層」、パケットをアプリケーションに受け渡す「トランスポート層」、アプリケーション同士でデータを解釈する「アプリケーション層」である。暗号化技術はこの各層ごとにあり、中でも上位3層のものは馴染み深い。

最上層のアプリケーション層には、メールの暗号化を行う「PGP (Pretty Good Privacy)」や「S/MIME (Secure MIME)」、ホストの遠隔操作を暗号化する「SSH (Secure SHell)」がある。

その下のトランスポート層の暗号化では、Web通信でよく利用される「SSL/TSL (Secure Sockets Layer / Transport Security Layer)」がある。

ネットワーク層で暗号化する「IPsec (IP security)」では、IPレベルで暗号化するため、すべてのアプリケーションの通信を丸ごと保護する。実際にパケットを暗号化/復号化するのは、ルータなどネットワーク層で動作する機器である。つまりIPsecを使うと、アプリケーションは暗号化のことを考えなくても暗号化通信できる。またホストやネットワーク全体を暗号化の対象にするため、インターネットを介し

たりリモート接続や LAN 間接続にも利用しやすい。

4 SSL の仕組み

現在最も普及している暗号化技術では SSL (Secure Sockets Layer) である。これは、一般に利用されるほとんどの Web ブラウザで使用することができる。SSL では、共通鍵暗号方式と公開鍵暗号方式の組み合わせで暗号化通信を行う。

SSL ではまず、公開鍵暗号方式を使ってクライアントとサーバ間で安全な通信路を確立する。この通信路を使ってやり取りされるのは、実際のデータ通信の暗号化に使う共通鍵の「元データ」である。この元データは、「プレマスターシークレット」と呼ばれる 48 バイトのランダムな数値である。

公開鍵暗号方式による通信は、具体的に次のようになる。クライアントがサーバへ接続要求を送ると、それに対する応答が戻ってくる。応答には、サーバの公開鍵が含まれている。クライアントは公開鍵の所有者を確認したあと、プレマスターシークレットを生成する。これをサーバの公開鍵で暗号化して送り返す。サーバがプレマスターシークレットの暗号文を受け取ったら、自分の秘密鍵で複合化する。この時点でクライアントとサーバは「同じデータ」を共有できたことになる。しかし、このデータから直接共通鍵が作られるわけではない。クライアントとサーバ間のセッションが途中で横取りされていないとも限らないので、共通鍵の生成には 2 つのランダムデータ (最初の要求 - 応答時に送られている) を加える。これによって、クライアント - サーバごとに固有で、セッションごとに固有な共通鍵を共有できる。共通鍵の共有ができれば、あとはその鍵を使った共通鍵暗号方式で暗号化通信を行う。

5 IPsec とは

SSL 以外にも、最近では IPsec (IP security) も徐々に普及の兆しを見せている。ネットワーク層で暗号化をする IPsec はネットワーク自体を対応させる必要があるため、他の暗号化技術に比べて導入の敷居が高い。具体的には、パケットの出入口にあたる 2 点間を IPsec の暗・複合化する「VPN ゲートウェイ」で接続しなければならない (LAN 間接続の場合)。しかも、IPsec の実装は VPN ゲートウェイベンダーによってばらつきがあり、相互接続性が乏しいのが現状である。

IPsec はもともと、IP レベルで広くセキュリティを確保するために開発されて技術である。IPsec でできることは、暗号化通信に限らず、あるプロトコルのネットワークに別のプロトコルパケットを通す「トンネリング」や、パケットの改ざんを防止する「パケット認証」、通信先の正当性を確認する「サーバ認証」といった、安全な通信に欠かせない機能が盛り込まれている。そのため、IPsec の構造はとても複雑である。

PKI と電子署名

現在のインターネットでは、公開鍵暗号方式と共通鍵暗号方式の組み合わせによって暗号化通信が行われている。ただし公開鍵暗号方式では、公開鍵の所有者が「本当に通信する相手」であることが保証されなければ、安全な通信はできない。例えば、あるショッピングサイトで買い物をして、買い物時に入力する氏名や住所、クレジットカード番号といった情報は、SSL を使った暗号化通信によって保護されている。しかし、暗号化に利用した公開鍵は、本当にショッピングサイトのものかどうか分からない。そしかするとショッピングサイトになりすました悪意の第三者かもしれない。そうになると、送信した個人情報別の誰かに知られてしまう。そこで、公開鍵暗号方式を利用した通信を行う場合、クライアントが公開鍵の所有者を確認できるようにするのが「PKI」である。

1 PKI (公開鍵暗号基盤) で身元証明

PKI は公開鍵暗号方式を利用して、ネットワーク上のセキュリティを確保するために考えられた仕組みである。PKI はインターネットがビジネスや生活にすっかり浸透した現在、これまで「紙ベース」で進めていた様々な処理をオンラインで安全に行うために必要になる。具体的には、顔が見えないネットワークで、相手の身元を確認し(なりすまし防止)、データが途中で書き替えられていないかを調べ(改ざん防止)、内容の食い違いをなくす(否認防止)ための技術が盛り込まれている。

前に挙げたショッピングサイトの例で考えれば、ショッピングサイトで安心して買い物するためには、ネットワーク上で配布された公開鍵の所有者の身元を証明しなければならない。加えて、その証明が正当なものであることの保証も必要となる。これを実現するために、PKI では「電子証明書」(公開鍵証明書)と、「電子署名」という2つの技術を使う。

Web ブラウザからショッピングサイトと SSL 通信する際、実はサーバから公開鍵といっしょに電子証明書も送られてきている。サーバから送られてきた電子証明書は、SSL のページにアクセスしている Web ブラウザ (Internet Explorer) の右下にある「鍵」のアイコンをダブルクリックすれば表示される。これを見れば、暗号化に使う公開鍵の所有者を確認できる。

実際に電子証明書を見てみると、「発行先」としてショッピングサイトの名前、「発行者」として何らかの組織名が記されていることがわかる。発行先は、公開鍵の所有者である。また発行者は、この証明書を作成した組織を示す。つまり、発行先の名前がサイトの名前と同じであれば、発行者によって公開鍵は発行先のサイトのものであることが証明されている。

発行先は何らかの組織名が記されていると前述したが、この組織は「認証局 (CA : Certificate Authority)」と呼ばれる。もし、この認証局が怪しい組織であれば、確かにその証明書は疑わしいが、認証局がユーザにとって「信頼できる組織」であれば、送られてきた証明書は信頼できることになる。しかし、認証局を信頼できるかどうかはユーザ自身の問題であるため、PKI では一般に「著名な組織」か、「自分に関連する組織」であれば信頼できることを前提にしている。それは、電子署名という仕組みによって、証明書を改ざんすることや偽造することが非常に困難になっているからである。

認証局には、2つの種類がある。1つは第三者的な立場で、様々なサイトに電子証明書を発行する専門の認証局 (パブリック CA)。もう1つは、特定の関係者だけで利用するネットワーク用に専用の構築ソフトを使って自前で運営する認証局 (プライベート CA) である。パブリック CA は、ベリサインなどいくつかの有名なセキュリティ事業者によって運営されている。こうした名の知れた認証局であれば信頼できる。

PKI の用途

PKI では以下のような幅広い用途が考えられる。

ア 電子商取引のインフラ構築

安全な電子商取引を行うためには、企業間あるいは事業者内で専用線を使ってセキュリティを保つことが考えられるが、将来の本格的な企業間の取引ではインターネットを介したセキュアな取引が必須となる。また、オンライン販売のような販売事業者対消費者の場合では、インターネットでクレジットカードを使ったオンライン決済が必要となる。ここに PKI を適用すれば、相手が誰であるかを確実に確認でき、しかも情報が漏洩する不安のない電子商取引が円滑に行えるようになる。

イ イン트라ネットのアクセスコントロール

企業や組織でイントラネットを構築し情報の提供や共有を行なう場合、部署や役職等に応じてアク

セスできる情報に制限を設けたい場合がある。PKI を使えば、このような情報のアクセス制御が容易になる。PKI が提供するセキュリティの特徴は、外敵の侵入を防ぐのではなく、対象物（エンティティ）を守るセキュリティを提供するところにある。イントラネット上の重要な文書は意図したユーザだけに閲覧（復号化）を可能にし、かつ、その文書が正しい人物によって作成されたことを証明するため、文書の改ざんの危険からも回避できる。

高等学校で PKI の活用

PKI は、電子商取引等のアプリケーションを構築するためのインフラであるため、高等学校での活用については考えていない。しかし、将来的には校内ネットワークのアクセスコントロールという方向で検討し、導入する価値があるようにも感じられる。

2 電子証明書の記載内容

電子証明書に記載されている情報は、発行先（公開鍵の所有者）と発行者（認証局）だけではない。Web ブラウザでどこかの電子証明書を開けるなら、ウィンドウのタブを「全般」から「詳細設定」に切り替えるとその中身を見ることができる。

あるショッピングサイトの電子証明書の詳細設定を開いて確認すると様々なことが記述されている。PKI で使われる電子証明書は、「X.509（バージョン3）」という形式に基づいて記述される。この形式では、発行先や発行者情報の他にも、証明書の有効期限など様々な情報が記載されている。ここで注目すべき点は、証明書に公開鍵が埋め込まれていることである。

PKI では、公開鍵は電子証明書の一部として送られている。これは、証明書で単に公開鍵の「所有者の身元」を示しているのではなく、「公開鍵と所有者の結び付き」を証明しているためである。つまり、証明書が発行されたあとに、勝手に鍵を変更できないようになっている。また、証明書の最後に付けられた認証局の電子署名にも注目しておく。電子署名はよく、デジタルの印鑑などと言われるが、単なる「確認印」ではない。実はもっと重要な役割を担っており、公開鍵を含めた電子証明書のデータが1ビットでも改変されると、証明書を受け取った側ですぐにわかるようにしている。これによって、証明書の改ざんを防止している。

3 メッセージダイジェストと電子署名

電子署名で改ざん防止が実現するのは、署名データが証明書の「メッセージダイジェスト」から生成されているからである。メッセージダイジェストとは、「ハッシュ関数」という特殊な関数（SHA1 や MD5）を使って生成された文字列である。ハッシュ関数は「不可逆的な一方向の関数」ともいわれ、生成したメッセージダイジェストから元のデータを取り出せないようになっている。また、同一のメッセージダイジェストを持つ、2つの異なるデータを作ることもできない。

このメッセージダイジェストの性質を利用すると、2つのデータの同一性を確認できる。例えば2つのデータが「ネットワークに送信する前のデータ」と、「送信後、相手が受け取ったデータとする。データを送るとき、あらかじめ生成しておいたメッセージダイジェストを添付すれば、受け取った側はデータから生成したメッセージダイジェストと比較できる。比較した結果、2つのメッセージダイジェストが一致すれば、データが送信中に改ざんされていないこと（データの同一性）が保証される。

電子署名を使った改ざん防止は、このような仕組みを利用する。送信側（認証局）で、証明書全体のデータを元データとしたメッセージダイジェストを生成し、証明書に添付しておけば、受信側で証明書の内

容を検証できる。加えて、メッセージダイジェストを認証局の秘密鍵で暗号化すれば、これを生成したのはその認証局であることを証明することにもなる。これを「本人認証」という。

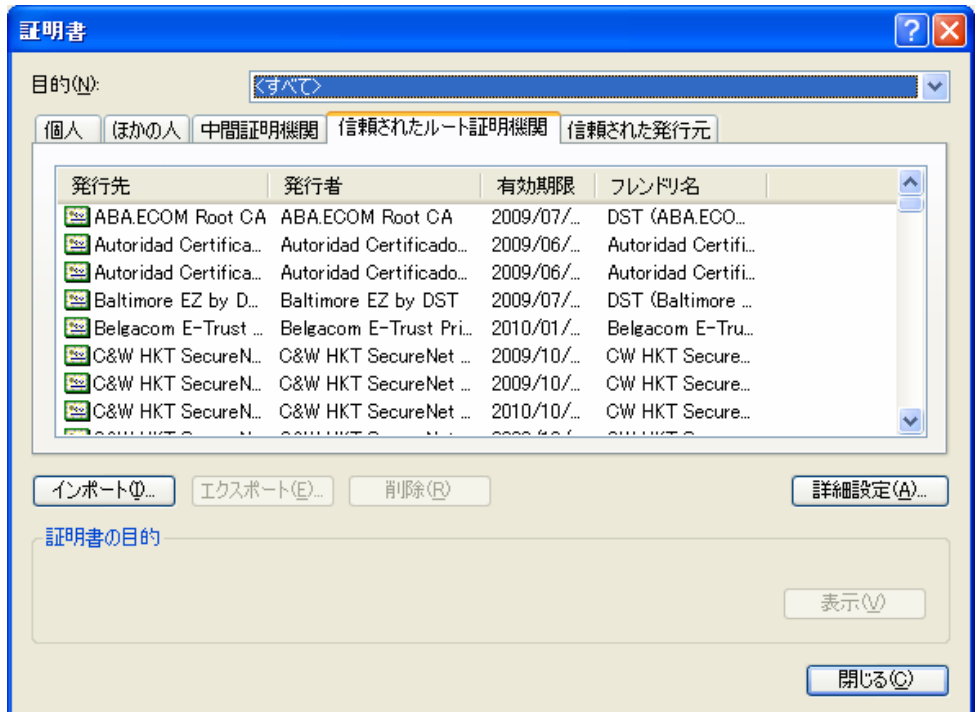
ネットワークを介して電子証明書を受け取った側（ユーザ）は、次の手順で正当性を検証する。まず、証明書全体のデータを元データとしてメッセージダイジェストを生成する。同時に、電子署名の部分だけを「認証局の公開鍵」（サイトの公開鍵ではない）で復号化し、認証局が生成したメッセージダイジェストを取り出す。この2つのメッセージダイジェストが一致すれば、証明書全体は改ざんされていないことがわかる。認証局が証明書を発行したあとに、もしその一部でも改変されていれば、2つのメッセージダイジェストは一致しないからである。

4 認証局の公開鍵

電子署名を使った改ざん防止のプロセスでは、認証局の公開鍵が必要である。証明書にはサイトの公開鍵が含まれているが、認証局の公開鍵は含まれていない。多くのパブリック CA の公開鍵は、証明書という形で Web ブラウザにあらかじめ登録されている。例えば Internet Explorer では、「ツール」「インターネットオプション」「コンテンツ」「証明書」から登録されている認証局の証明書を見ることができる。また、登録されていない認証局（特にプライベート CA）の証明書を別途登録することも可能である。こうして Web ブラウザにあらかじめ認証局の公開鍵を持たせておくことで、証明書に付けられた電子署名を復号化できるようになっている。上記の Internet Explorer に登録してある証明書の認証局には、「中間証明機関」と「信頼されたルート証明機関」の2種類がある。

認証局に2種類あるのは、PKI では認証局自体の身元を別の認証局によって階層的に証明しているためである。これにより、「信頼の連鎖」を構築することができる。前で、認証局を信頼できるかどうかはユーザ自身の問題で、著名なパブリック CA や自分と関連するプライベート CA であれば信頼できると述べた。認証局の信頼が階層構造になっていれば、ユーザは間接的に多くの認証局を信頼できるようになる。

階層の頂点に立つのがルート認証局である。これは、別の認証局に電子証明書を発行する（＝署名する）役割を担う。また、ルート認証局から署名され、各サイトに証明書を発行するのが中間認証局である。例えば、あるサイトの証明書がどこ



かか中間認証局 A から発行されているとする。この場合、ユーザが認証局 A を信頼できなくても、その認証局がペリサインといった信頼できるルート認証局から署名されていれば、必然的に A を信頼できる。この理屈から、ルート認証局を信頼すれば、大半の認証局を信頼できることになる。すなわち、PKI は「ルート認証局を信頼する」という前提で成り立っているのである。

PKI (Public Key Infrastructure : 公開鍵暗号基盤) の活用

1 認証局ソフトウェアで証明書を発行する

認証局ソフトウェア (Easy Cert) で認証局を構築する手順を示す。この「Easy Cert」は名古屋工業大学電気情報工学科の岩田研究室で開発された暗号ライブラリをベースにして開発された認証局ソフトウェアである。証明書と失効リストの発行を主眼にしており、登録局やリポジトリの要素は省略されている。

Easy Cert のダウンロード

岩田研究室の Web サイトからダウンロードする。

<http://mars.elcom.nitech.ac.jp/security/download.html>

ダウンロード可能な最新バージョン 0.91 Beta2 (EasyCertSetup091b2e.lzh)

ダウンロードしたファイルは圧縮されているため、解凍する必要がある。解凍後、setup.exe.を実行するとインストールが始まる。



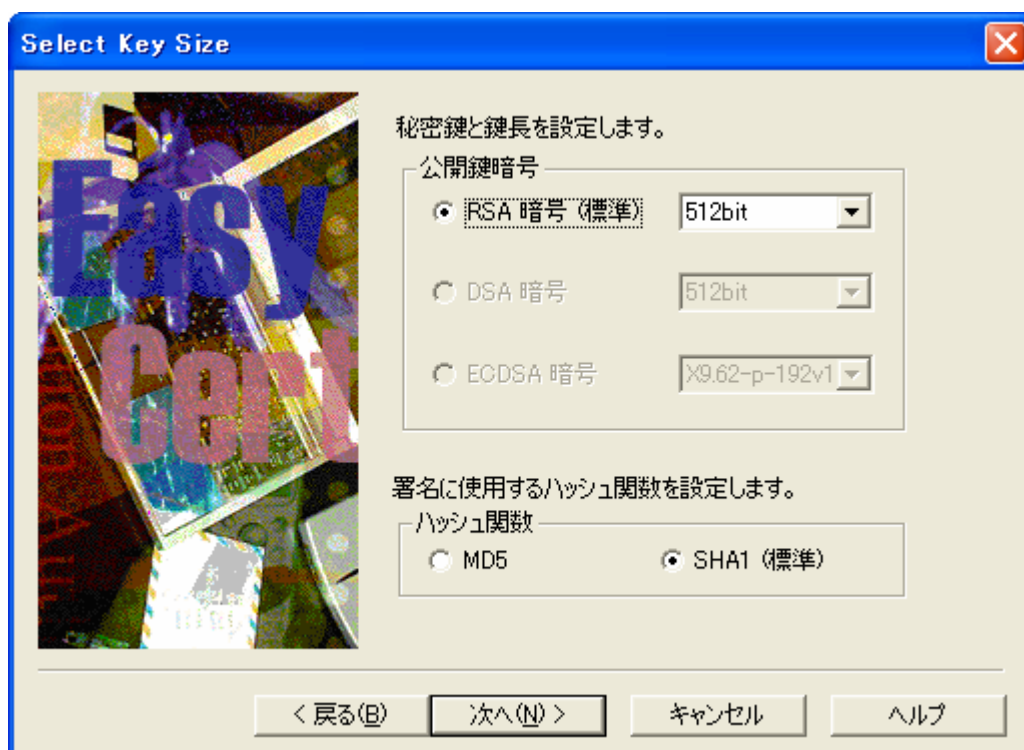
EasyCert v0.91
Copyright (C) 2000-2002 T.Okuno
AiCA, AiCrypto (C) 1998-2002
A.Iwata Lab in N.I.T.
このアプリケーションは強度な暗号アルゴリズムを含んでいます。無断転載・配布は日本国の輸出制限に抵触するため、堅く禁じます。

乱数初期化
擬似乱数の初期化を行いません。
Window内でマウスを移動してください。

Input CA Name
新しいCA(認証局)を構築します
CAの名前を入力してください。
テストCA

認証局 (CA) に名前をつける。この名前は証明書の中の発行者とは別に扱われる。

次に、構築するCAの公開鍵と秘密鍵の鍵ペアに関する指定を行う。ここでは、「証明書と秘密鍵を新規に作成する。」を選択する。証明書の電子署名はここで生成した秘密鍵で行うことになる。

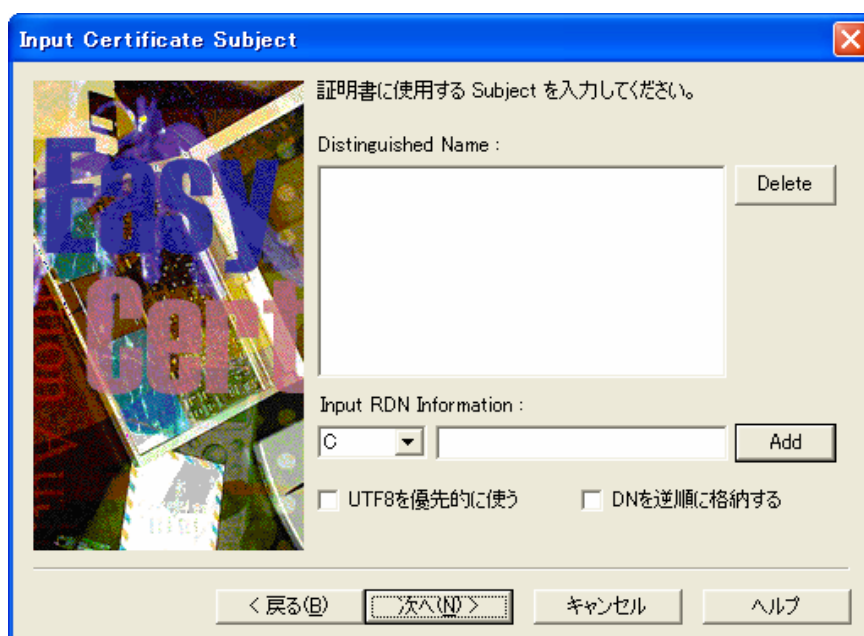


Easy Cert は輸出規制に対応しているため RSA 暗号の鍵長が制限されている。本来であれば、安全性の観点からは、1,024 ビットを選ぶのが望ましい。ハッシュ関数については、MD5 は衝突を起こす可能性があることが報告されているため、「SHA1」を選択する。

次に鍵の生成を行う。「鍵生成」ボタンをクリックしてしばらく待つと鍵生成が完了する。

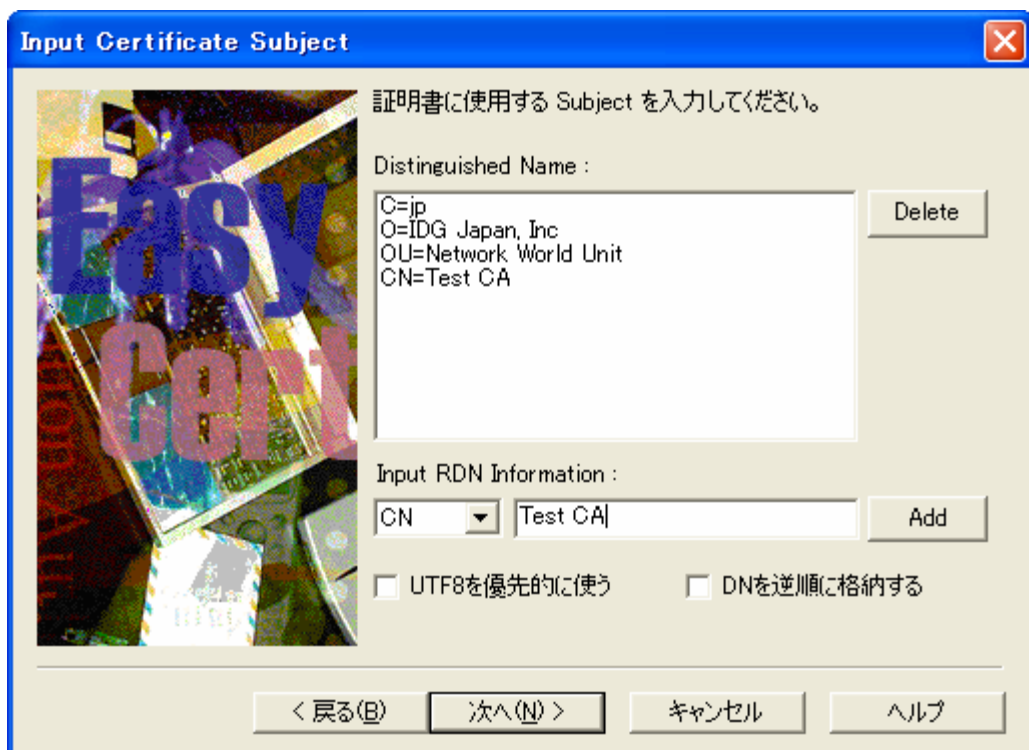


証明書のサブジェクトとなる識別名を入力する。

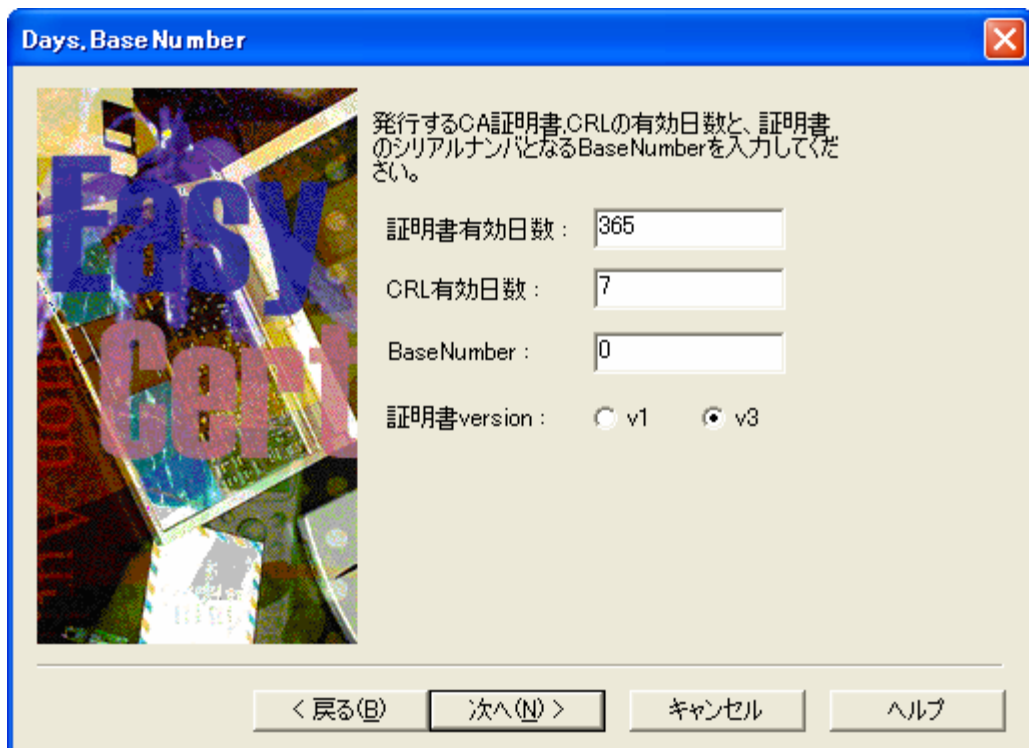


証明書の DN (Distinguished Name) フィールドの項目名と概要

項目名	説明
C	国 (Country) の名称。必ず半角 2 文字のアルファベットを入力する。
S T	州名 (State) の名称。入力する必要はない。
L	位置 (Location) の名称。これも特に入力の必要はない。
O	組織 (Organization) の名称。半角 64 文字まで入力可。日本語入力も可能。
O U	下位組織 (Organization Unit) の名称。半角 64 文字まで入力可。日本語入力も可能。
C N	一般的な名前 (Common Name)。半角 64 文字まで入力可。日本語入力も可能。
EMAIL	電子メールアドレス (EMAIL)。半角 64 文字まで入力可能。



続いて、証明所に記載される有効期間と失効リスト（CRL）を発行する間隔をそれぞれ日数で指定する。（いずれの項目もデフォルト値）

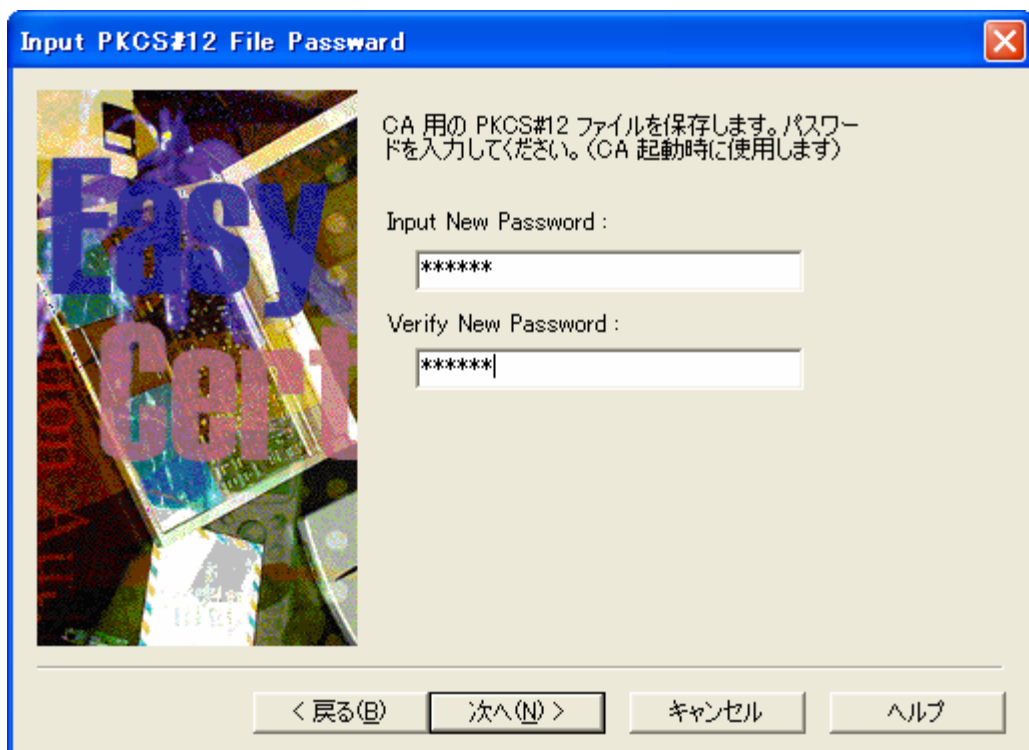


続いて、必要な証明書の拡張情報を指定する。「詳細設定」ボタンをクリックすると、拡張情報の値を詳細に指定できる。ここもデフォルトのまま、「次へ」をクリックする。



最後に、PKCS#12 ファイルのパスワードを設定する。PKCS#12 形式は作成した証明書と秘密鍵をペアでファイルに保存できる。その場合、秘密鍵などを保護する必要があるので、パスワードを使って暗号化してから保存する。このパスワードは、Easy Cert 起動時や「ファイル」メニューの「CA を開く」コマンド実行時などに確認されることになる。

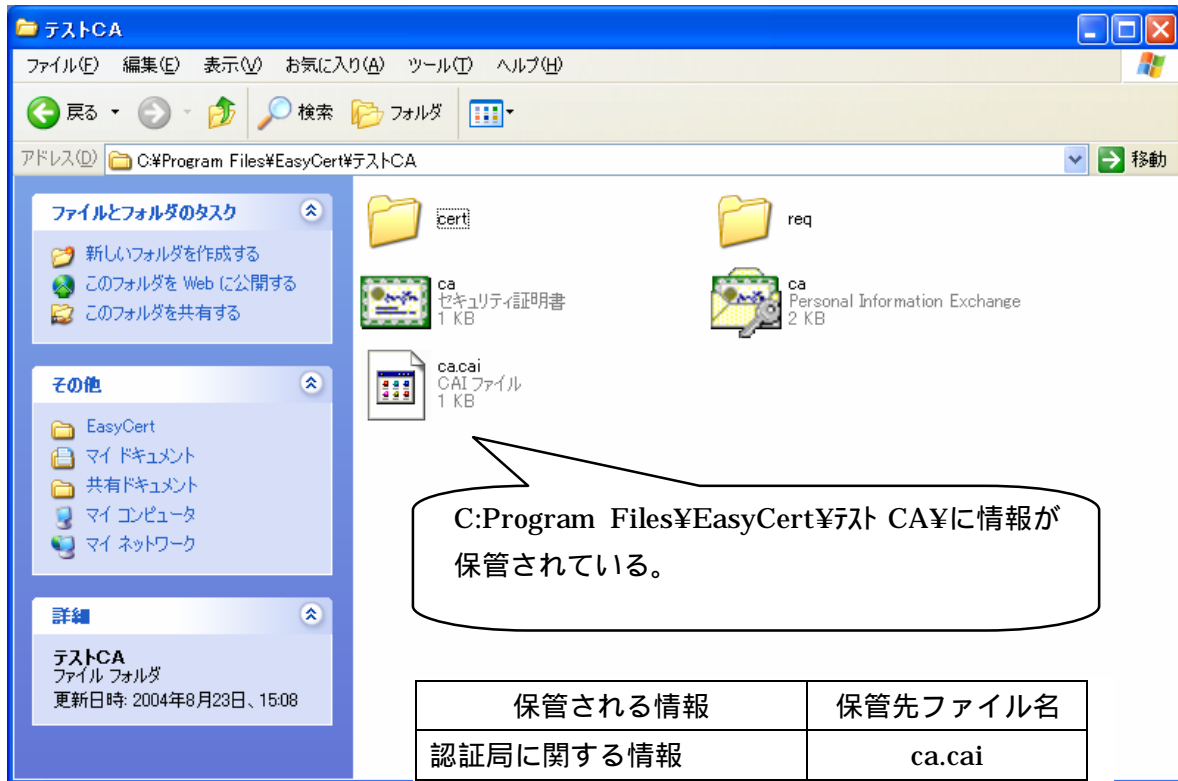




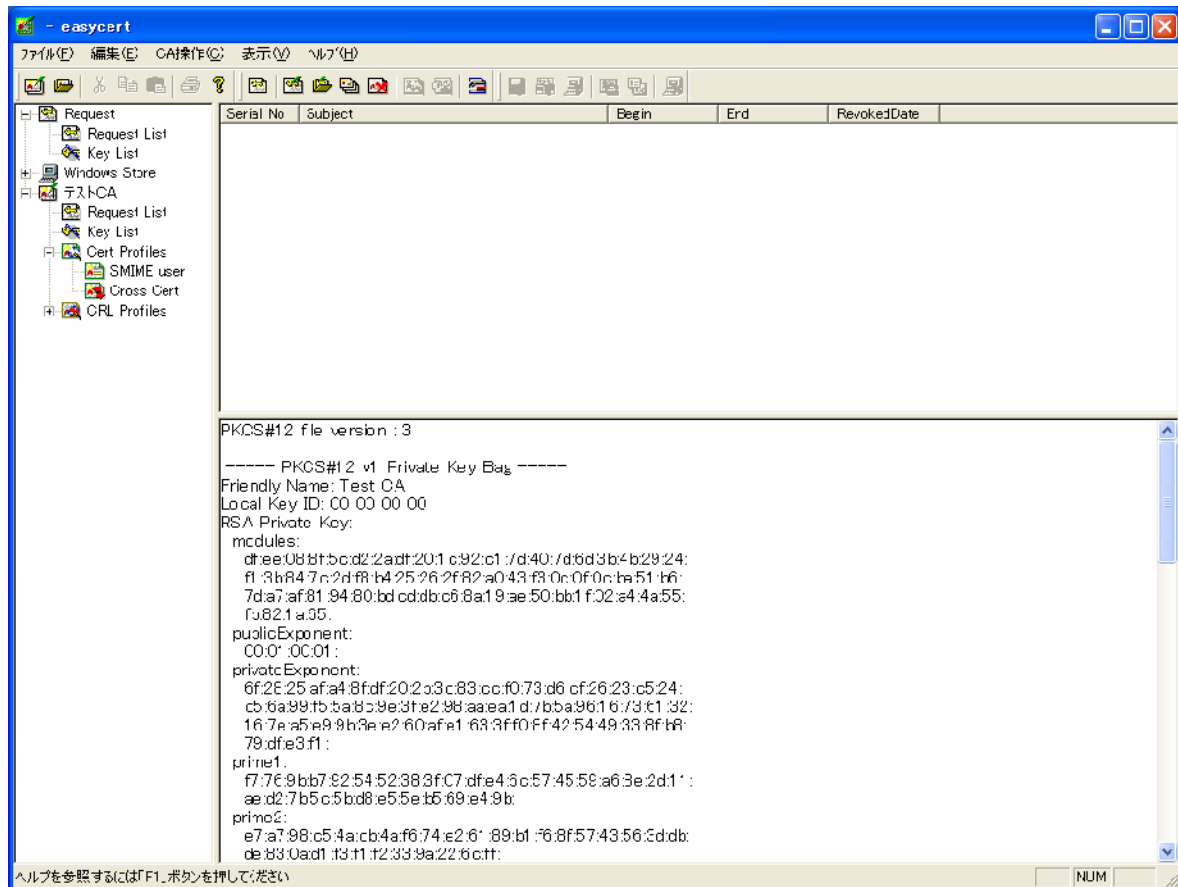
以上で認証局の構築が完了するので、「完了」ボタンをクリックして作業を終了する。

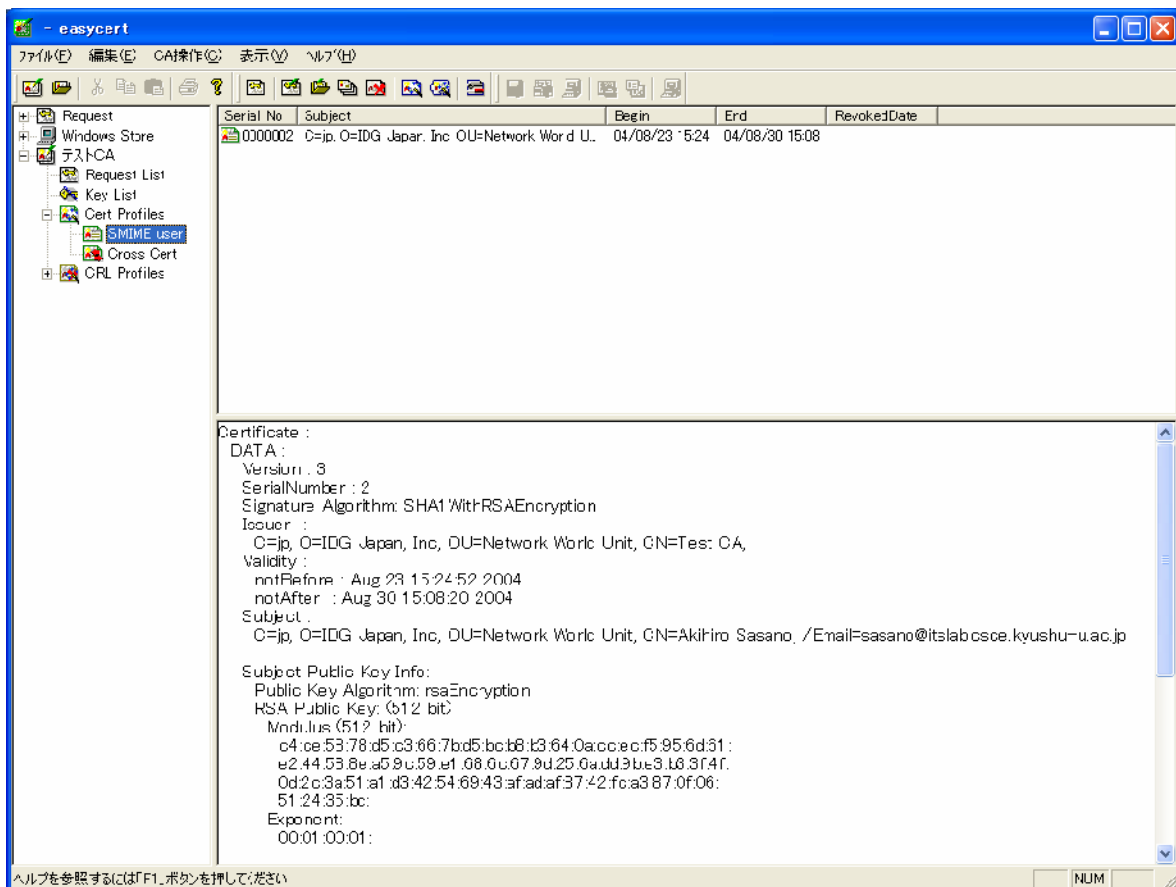
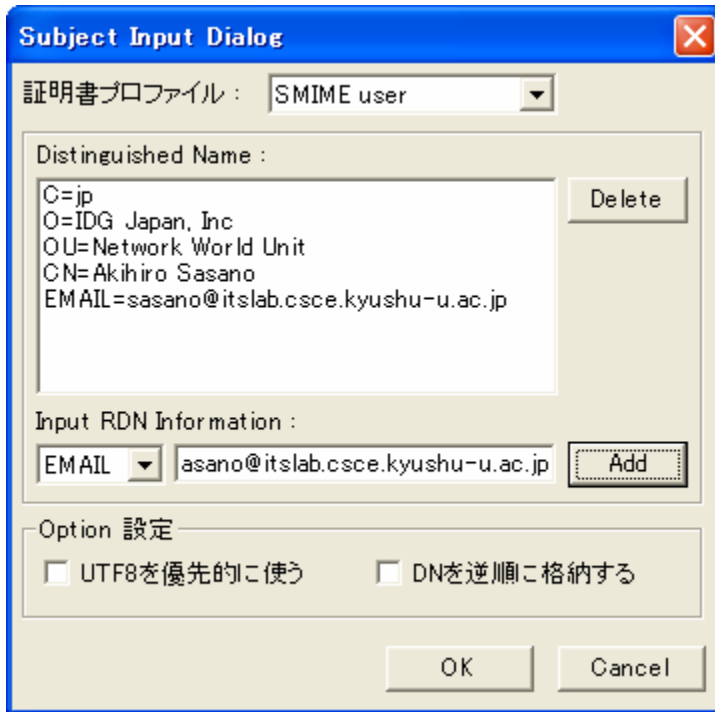


作成したファイルは、< インストール先 > ¥ < 認証局の名前 > ディレクトリに保管される。



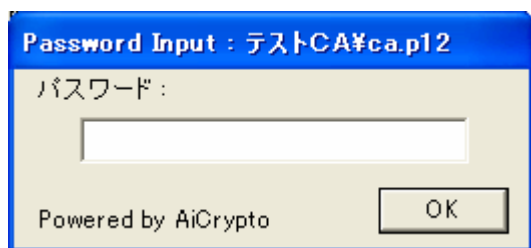
保管される情報	保管先ファイル名
認証局に関する情報	ca.cai
認証局の証明書と秘密鍵のペアの PKCS#12	ca.p12
認証局の証明書	ca.cer



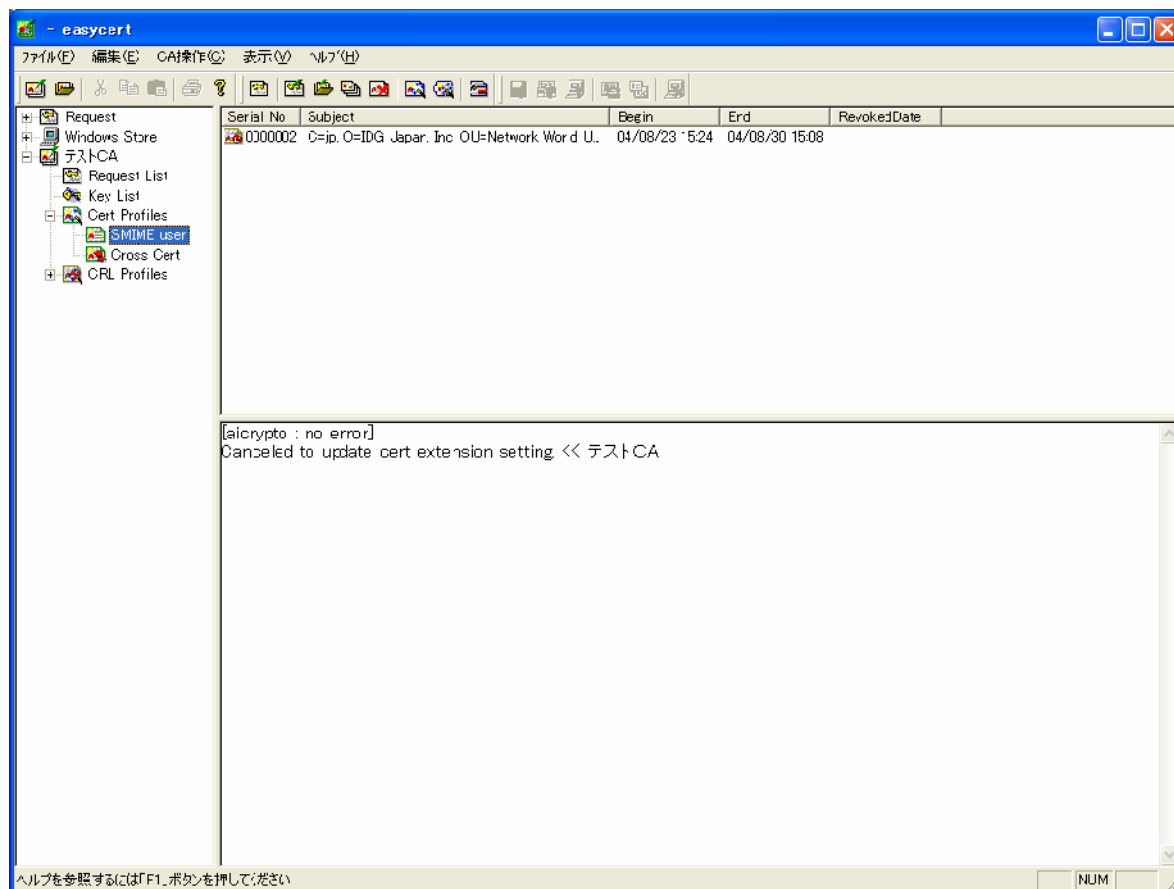


2 認証局を開いて証明書プロファイルを設定する

認証局に関する操作は、起動画面の「ファイル」の「CAを開く」から行う。「CAを開く」では、認証局に関する情報を得るために「ca.cai」を選択すると、その認証局のPKCS#12ファイルのパスワードを聞かれる。パスワード欄を空白のまま「OK」ボタンをクリックするとキャンセルできる。認証局の表示が不要な場合には、「CAを閉じる」を選択する。



発行する証明書のプロファイルを設定する。ツリービューで「SMIME user」のコンテキストメニューの「プロファイルの設定」から証明書の基本領域を設定する。



「拡張情報設定」では、証明書拡張領域の設定を行う。ここで設定した内容が、これ以降に発行する証明書に反映される。基本領域として、証明書の有効期限や証明書のバージョンなどの項目を設定する。デフォルトでは有効期間が7日となっている。

基本制限 (Basic Constrains)

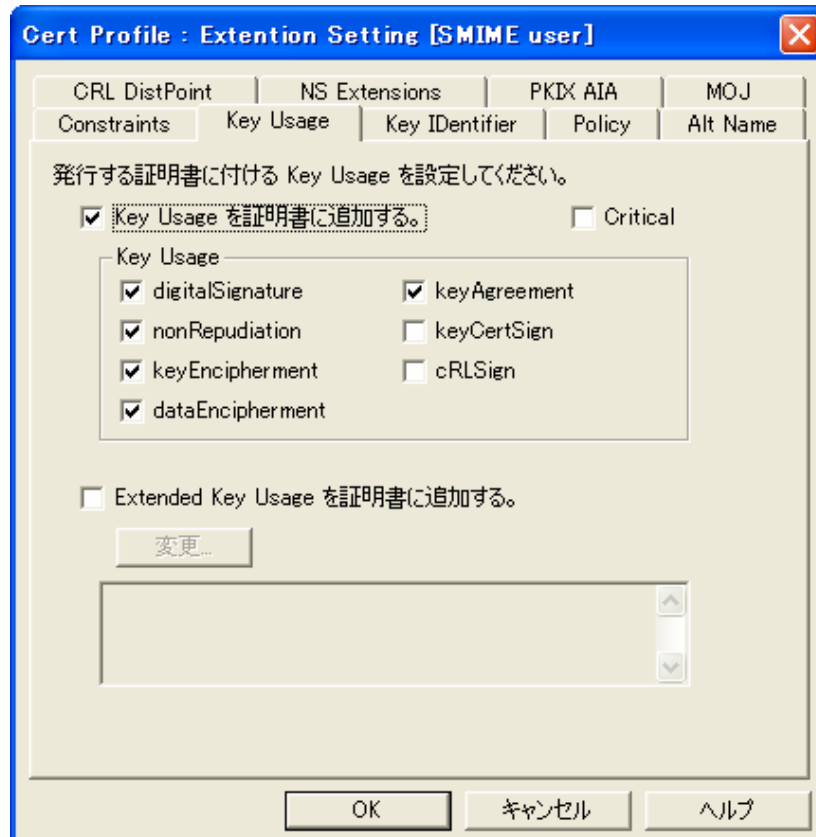
「Constraints」タブで指定する。認証局か否かを示す。「Basic Constrains」はどのような場合にもほ

ば必須と考えてよい。メニューの「Basic Constrains を証明書に追加する。」をチェックする。



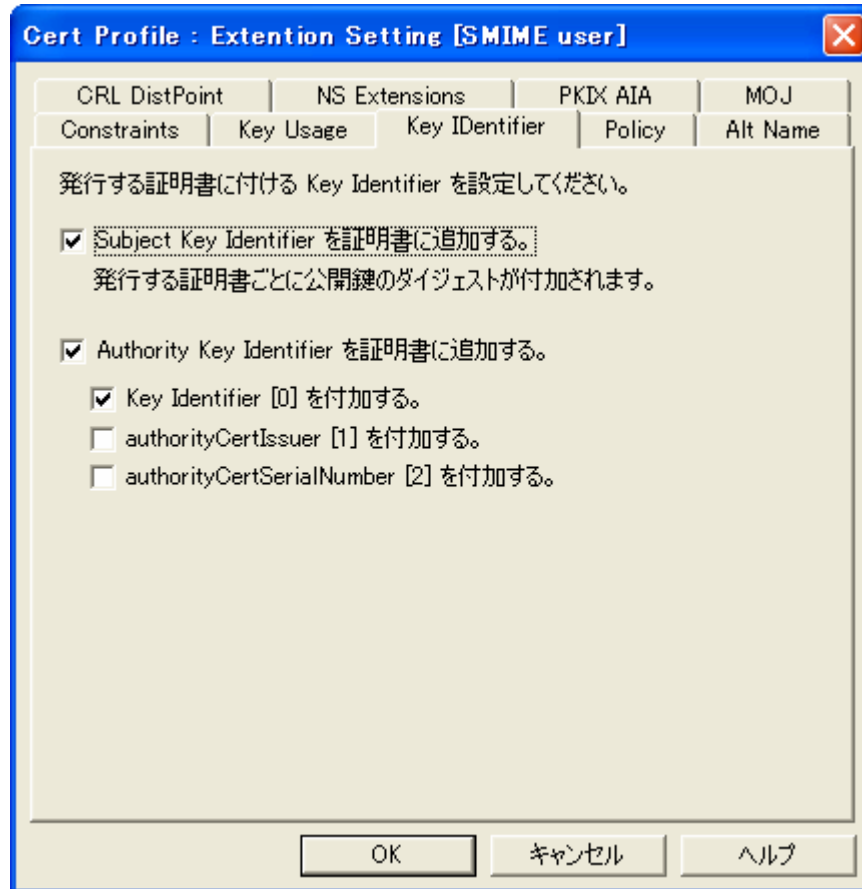
鍵使用法 (Key Usage)

「Key Usage」タブで、許可する鍵の用途を指定する。RSA 暗号の鍵を電子メールに使う場合には、「digitalSignature」(電子署名)と「nonRequidiation」(否認防止)「keyEncipherment」(鍵の暗号化)をチェックしておく。



サブジェクトキーID (Subject Key Identifier) と発行元キーID (Authority Key Identifier)

サブジェクトキーIDは「Key Identifier」画面で指定する。サブジェクトIDキーとは、サブジェクトの公開鍵の識別子、つまり証明書に含まれている公開鍵を識別するための値で、発行元キーIDは証明書を発行した認証局の公開鍵の識別子である。公開鍵の識別子には、公開鍵のハッシュ値などを使う。発行元キーIDでは発行元DNとシリアル番号の組み合わせを使うこともある。



項目の重要性 (Critical)

証明書の拡張領域のそれぞれの項目には、「重要」か「非重要」かを指定する。「重要」となっている項目については、アプリケーションはその項目を仕様に基づいて解釈し、処理しなければならない。アプリケーションが解釈および処理できない項目が「重要」であった場合、アプリケーションはその証明書を無効なものとして扱う。

サブジェクトの固定値

「CA 操作」メニューの「CA のプロパティ」で、証明書のサブジェクトの一部に標準で使用する値を決める。デフォルトでは認証局証明書のサブジェクトから、C、O、OUの値が採用されている。

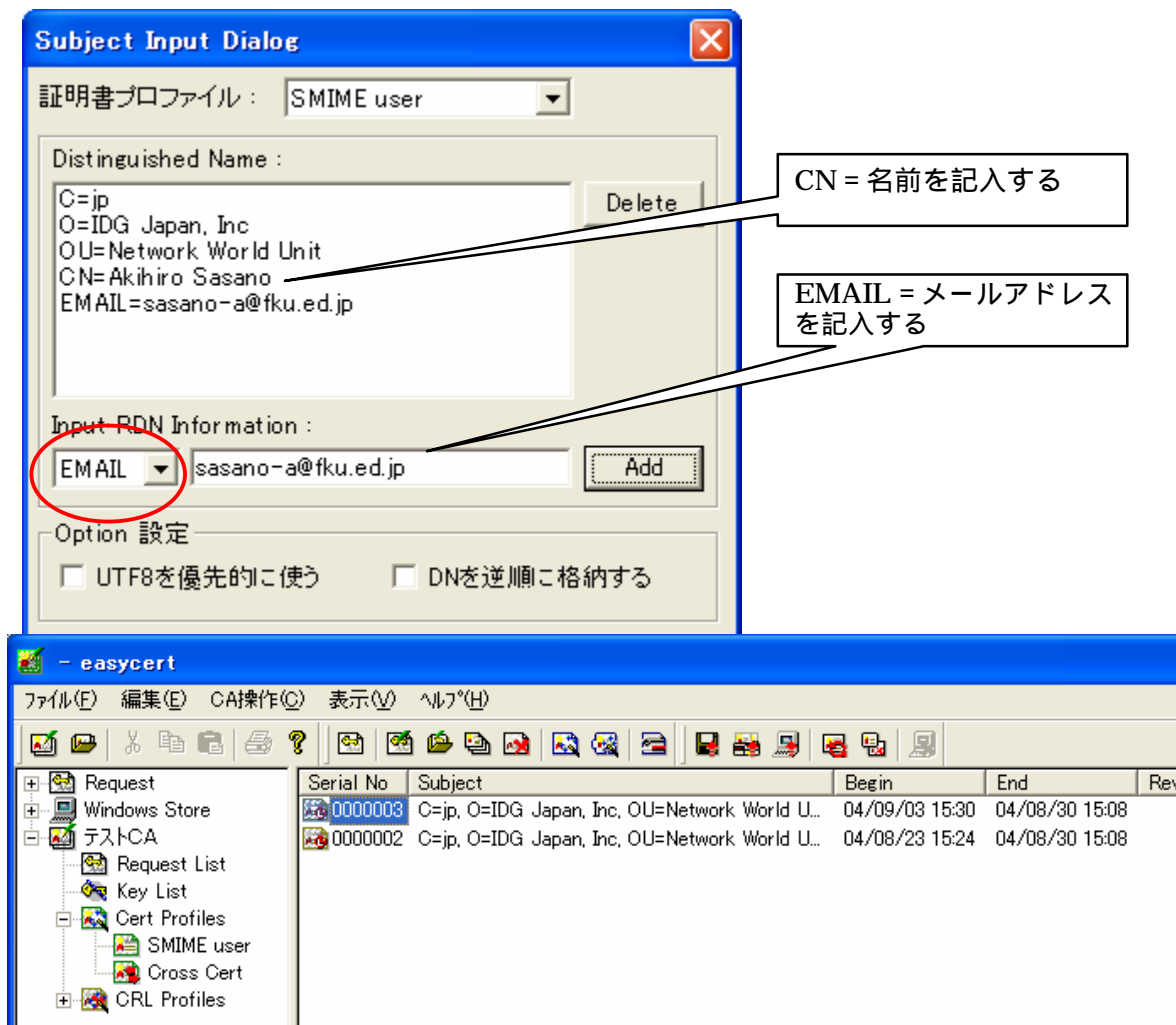
プロファイルの追加

「CA 操作」メニューの「プロファイルの追加」を選択すると、新たに証明書プロファイルを定義したり追加したりできる。

3 証明書を発行して利用者に配布する

利用者のそれぞれが使う秘密鍵と公開鍵のペアを生成し、証明書を作成する。作成した証明書はファイルに保管して利用者ごとに証明書を発行して渡す。

サブジェクトを入力する。標準の DN があらかじめ設定されているので、「CN」に名前を、「EMAIL」にメールアドレスを追加する。(CA 操作 証明書発行)



作成した証明書は、利用者に配布し、目的のアプリケーションで行うことになる。そのために、証明書を扱うための標準的なフォーマットのファイルに保存して受け渡しをする。Easy Cert では、証明書は拡張子が .cer であるようなファイルに、秘密鍵と証明書をペアでファイルにする場合は PKCS#12 と呼ばれるフォーマットに従ったファイルにそれぞれ保管可能である。

Easy Cert では、PKCS#12 に保存する場合、秘密鍵と証明書とその発行元の証明書をいっしょに保存している。これにより、目的のアプリケーションで証明書の信頼性を確認できる。

ツリービューで「SMIME user」を選択すると、右上のペインに作成した証明書が一覧表示される。証明書を選択し、コンテキストメニューを開くと「保存」と「PKCS#12 で保存」コマンドがある。「保存」では、証明書をファイルに保存する。送信相手の証明書は「保存」でファイルを



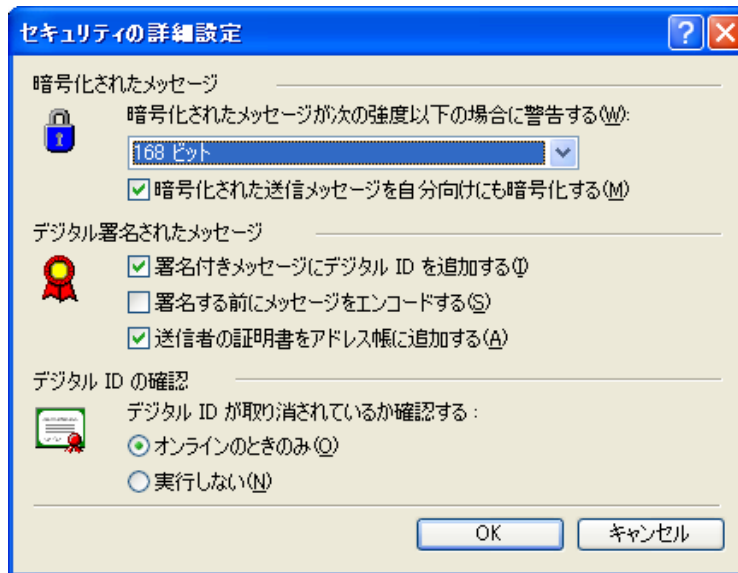
作成し、自分の証明書は「PKCS#12 で保存」を使って秘密鍵と証明書がペアになったファイルを作成する。作成には秘密鍵を保護しているパスワードと PKCS#12 を保護するパスワードが必要になる。

4 Microsoft Outlook Express で証明書を使う

証明書と秘密鍵をセットで保存したファイル（拡張子が「.p12」となっている PKCS#12 ファイル）と、証明書のみを保存したファイル（拡張子が「.cer」となっている証明書ファイル）を上で作成したこの2つのファイルを電子メールソフトウェアで使うことで、電子署名や暗号化が可能となる。

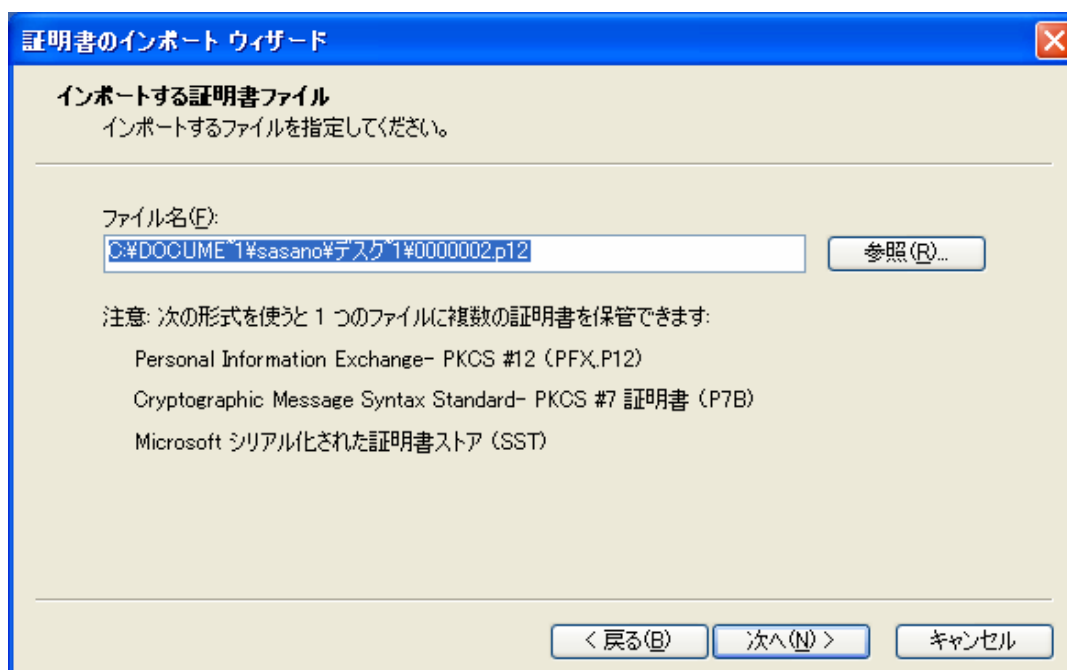
Outlook Express では、電子署名や暗号化に関する設定は「ツール」メニューの「オプション」で「セキュリティ」のタブを開いて行う。詳細な設定は、「セキュリティ」タブの「詳細設定」から行う。

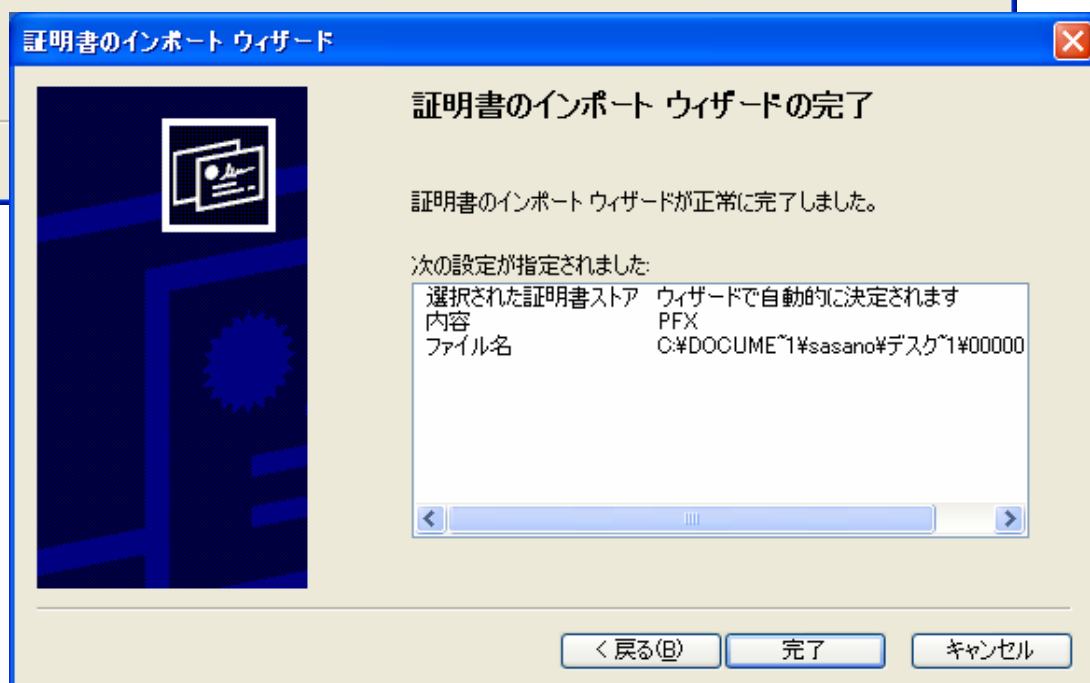
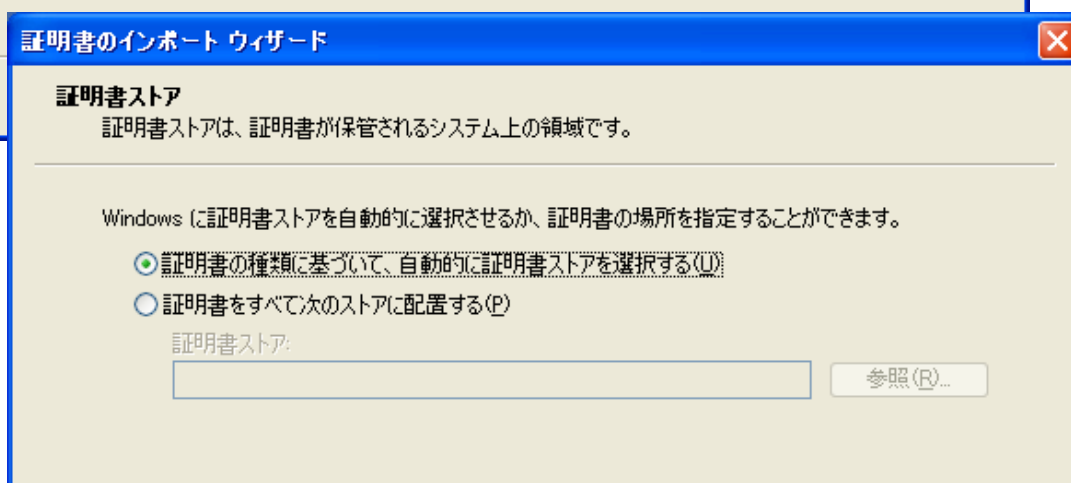
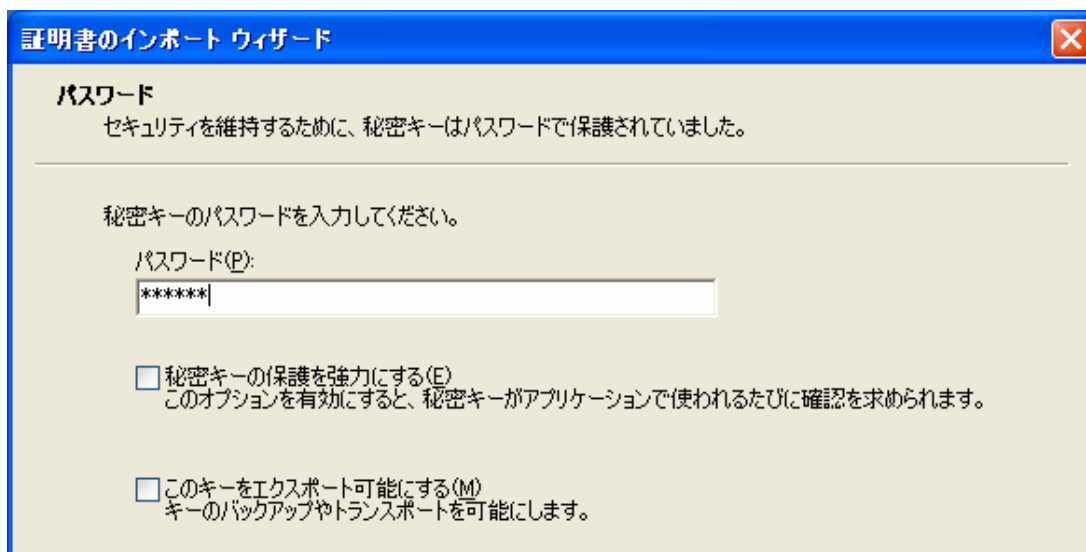
「セキュリティの詳細設定」画面では、標準で電子署名や暗号化を行うかどうかを指定する。ここでは、暗号の強度や電子署名に関するプロトコルのオプション、証明書の有効性の確認などを設定する。



ウィザードに従って PKCS#12 ファイルをインポート

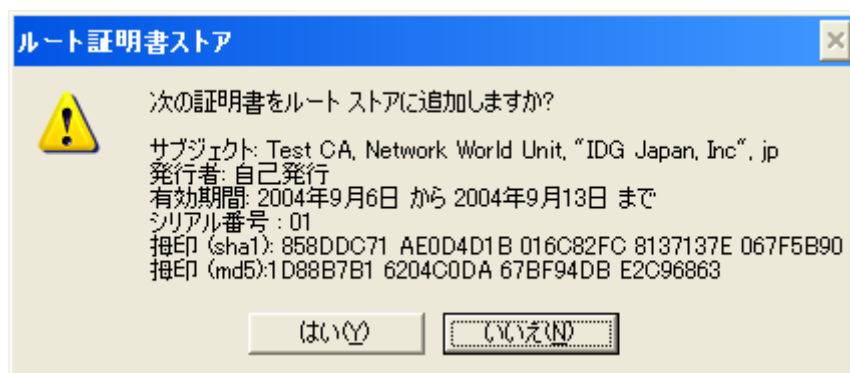
PKCS#12 ファイルをダブルクリックすると、「証明書のインポートウィザード」が開始される。このウィザードに従って操作を進めると、Windows が標準で持つ証明書の保管場所である「証明書ストア」に証明書が保管され、Outlook Express でも秘密鍵や証明書が利用可能になる。





途中で「秘密キーのパスワード」の入力が要求されるので、PKCS#12 ファイルを保護する際に用いたパスワードを入力する。「証明書のインポートウィザードの完了」画面で「完了」をクリックすると、認証局の証明書をルート証明書ストアに追加することを確認するメッセージが表示される。「はい」をクリ

ックするとインポートは完了する。



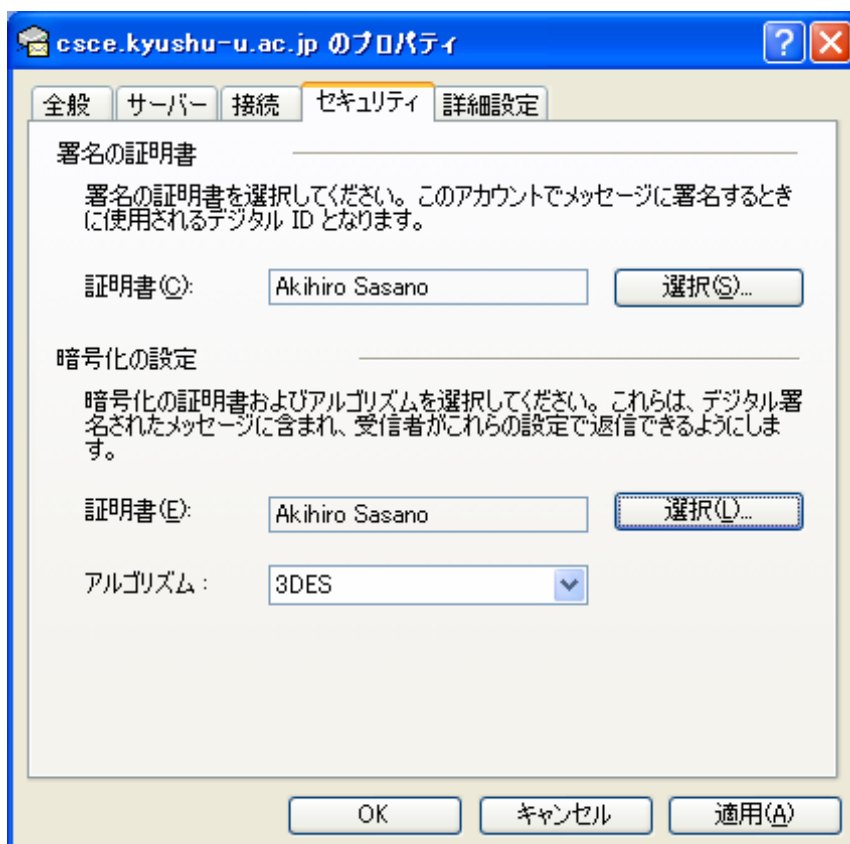
このメッセージは、PKI において、ルート証明書を信頼の基点として信頼性を検証するため、自己署名の証明書をインポートする際に、信頼できるものであるか否かを確認するために表示されるものである。利用者は、表示された「拇印 (sha1)」または「拇印 (md5)」を基に、自分の信頼性を確認しなければならない。拇印とは、証明書のバイナリデータを入力値としたハッシュ値のことである。自己署名の証明書の場合には、拇印を参照して、証明書が信頼できるものかどうかを確認する。ハッシュ関数には sha1 を使うケースと md5 を使うケースがあるので注意が必要である。Windows では、証明書ファイルのコンテキストメニューの「開く」コマンドで表示される「証明書」ダイアログの「詳細」ページで確認できる。

また、拇印は何らかの安全な経路を介して認証局の管理者から利用者に伝える必要がある。保護された Web サイトなどに記載するなどの方法が採られることもあるが、それ自身が同じルート証明書を基点にしている場合にはこの方法も意味がないため注意する。

メールアドレスの設定を「プロパティ」画面で行う

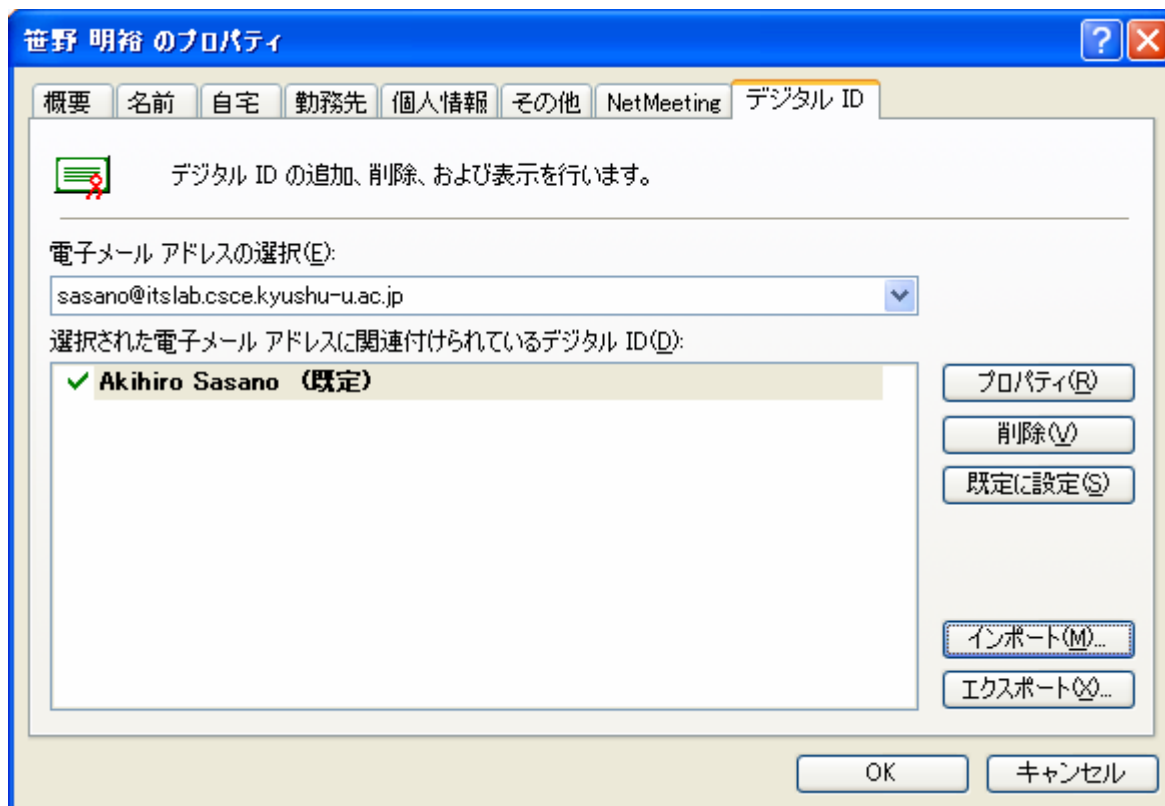
電子署名に使う証明書の指定と、暗号化に使う証明書の指定は、メールアドレスの「プロパティ」の「セキュリティ」タブで行う。

「選択」ボタンをクリックすると利用可能な証明書が表示されるので、この中から選択する。このとき、メールアドレスと証明書の電子メールアドレスが一致している必要がある。また、「暗号化に使う証明書」が、自分宛の暗号化に使われる証明書となる。



「アドレス帳」から証明書をインポート

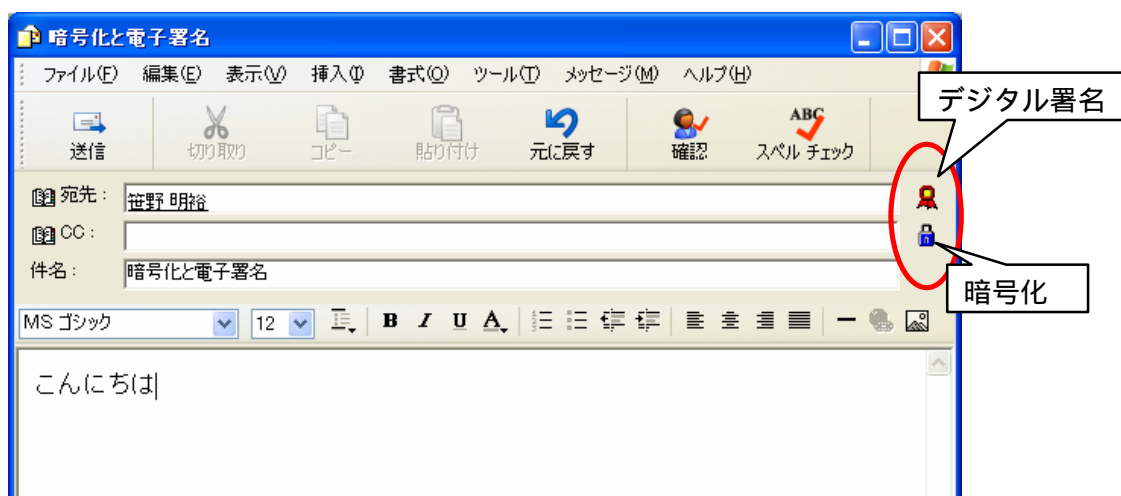
暗号化する相手は連絡先としてアドレス帳に登録されている必要がある。「ツール」メニューの「アドレス帳」から証明書をインポートして、メールの送受信に証明書を使えるように設定する。「アドレス帳」を選択し、右ペイントで通信相手を右クリックして「プロパティ」を開き、「デジタル ID」タブの「インポート」ボタンをクリックして、作成した証明書ファイルを選択する。



ここでいう「デジタル ID」とは証明書のことである。ここでも、証明書に指定されている電子メールアドレスと選択する電子メールアドレスが一致している必要がある。

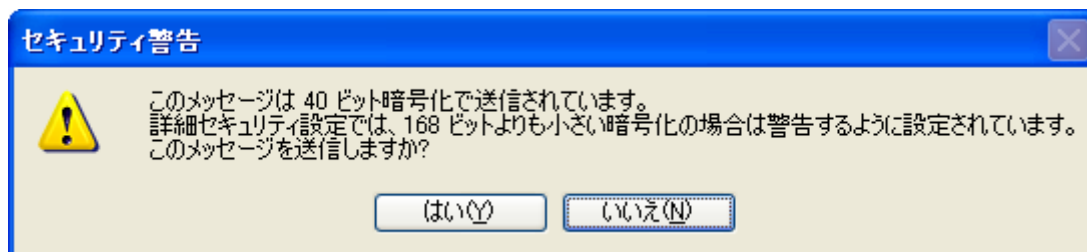
メッセージの暗号化

インポートした証明書を使って電子メールメッセージを暗号化して送信する。メールの作成画面で連絡先を選択し、「ツール」メニューで「暗号化」と「デジタル署名」を選択する。



「デジタル署名」にはリボンのアイコンが、「暗号化」には錠前のアイコンが対応する。なお、Outlook Express では電子署名を「デジタル署名」と呼んでいる。一般的には、電子的に行われる署名一般を「電子署名」と呼び、「電子署名」のうち、PKI の枠組みにおいてなされるものは「デジタル署名」と呼んで使い分けられる傾向がある。

「送信」をクリックすると、下図のような「セキュリティ警告」が表示される。暗号化アルゴリズムに 40 ビットの RC2 が利用されることになる。



この警告メッセージが表示される理由については、Outlook Express が暗号化アルゴリズムを決定するにあたって、相手からの電子署名のデータから、利用可能な暗号化アルゴリズムの通知を参照している。しかし、電子署名されたメールを一度も受信していない時点では、40 ビットの RC2 を利用することになる。これと「ツール」メニューの「オプション」コマンドの「セキュリティ」タブの「セキュリティの詳細設定」で指定されている「暗号化されたメッセージが次の強度以下の場合に警告する」で設定されているビット長とを比較して、40 ビットの RC2 では指定に満たないため安全性が不十分と判断される。

5 PKI の構成要素

PKI を大別すると次の 4 つの要素で構成される。

利用者

PKI の枠組みの中では「エンドエンティティ」と呼ばれる。エンドエンティティは、公開鍵と対応づけられた、公開鍵の持ち主である人間であったり、サービスを提供するサーバのサービスそのものであったりする。

登録機関

証明書を発行するにあたって、利用者の本人性を確認する役割を担う。

証明書発行機関

この機関自身が証明書を持ち、公開鍵とその持ち主の情報に電子署名を行って証明書を発行する。また、失効した証明書のシリアル番号のリストに電子署名を行い、証明書失効リストを発行する。

リポジトリ

証明書や証明書失効リストを格納し、それらを公開、配布することを目的として設置される。通常 LDAP ディレクトリサーバが用いられる。

認証局は、登録機関、証明書発行機関、リポジトリの役割を一括してサービスを提供したり、登録局やリポジトリを外部に持ち、証明書発行機関のみサービスを提供したりといった形態を取る。この 3 つの要素の管理と運営が認証局の業務である。認証局は CPS (Certification Practice Statement) という形で運営方針などを規定する文章を公開し、利用者に明示する義務がある。

6 3種類の暗号化アルゴリズム

PKI（公開鍵基盤）は、暗号化アルゴリズムとして公開鍵暗号のみを用いて成立しているのではなく、次に示す3種類のアルゴリズムを組み合わせで使っている。

ハッシュ関数（一方向性関数）

入力データを基にして一定の長さのデータを作る処理を行う。出力データからもとの入力データを算出することはできない。

共通鍵暗号（秘密鍵暗号）

暗号化と復号化に同じ鍵を使用する。この鍵を「共通鍵」または「秘密鍵」と呼ぶ。

公開鍵暗号

暗号化に使う鍵と復号化に使う鍵が異なり、一方の鍵を公開してももう一方の鍵を割り出すことはできない。公開する鍵を「公開鍵」、秘密にする鍵を「秘密鍵」または「私有鍵」「非公開鍵」と呼ぶ。上記の共通鍵暗号における共通鍵も「秘密鍵」と呼ぶことが多い。

公開鍵証明書などに使われている電子署名では、ハッシュ関数と公開鍵暗号を組み合わせで使う。署名したいデータのハッシュ値を、秘密鍵を使った公開鍵暗号で暗号化して相手に渡す。

電子メールでメッセージを暗号化する場合などは、共通鍵暗号と公開鍵暗号を組み合わせで使う。共通鍵暗号の処理の高速性を生かして、メッセージを公開鍵暗号ではなく共通鍵暗号で暗号化し、その鍵を公開鍵暗号で暗号化し、暗号化したメッセージとともに通信相手に送るという手法が取られている。

MRTG (Multi Router Traffic Grapher : ネットワーク監視システム) について

The Multi Router Traffic Grapher (MRTG)はネットワークの負荷を監視するツールである。MRTG は現在のネットワークのトラフィックの状態を示すグラフィックイメージを含む HTML ページを生成する。

MRTG は Perl と C で記述されており、UNIX と Windows NT で動作する。MRTG はネット上の多くのサイトで使用されている。

1 特徴

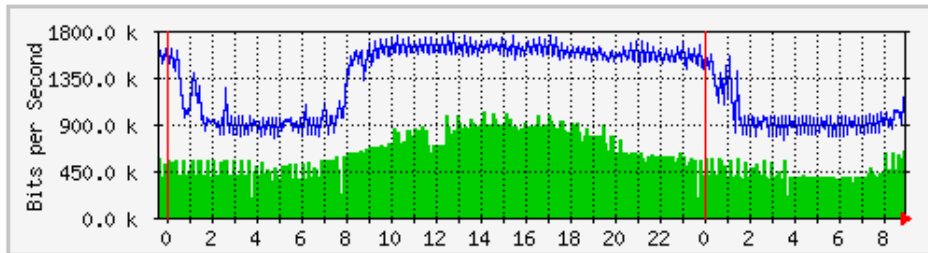
MRTG は、SNMP を使用してルータ上のトラフィックカウンターを読み取る Perl スクリプトと、トラフィックデータを収集して監視しているネットワークのトラフィックを見た目のいいグラフにする高速な C のプログラムで構成されている。これらのグラフはどんな Web ブラウザからでも読めるように、WEB ページに埋め込まれる。

MRTG は日ごとの詳細なグラフに加えて、それぞれ過去 7 日間、4 週間、12 ヶ月のトラフィックを視覚化する。これは、MRTG がルータから収集してきた全てのデータをログとして保持するため可能となっている。このログは自動的に整理されるため、時間の経過とともに肥大することがないだけでなく、過去 2 年間におけるトラフィックに関するデータを保持する。これらの作業はすべて効率的に行われるので、200 を超えるネットワークリンクを比較的 low スペックの UNIX で監視することができる。

MRTG はトラフィックの監視だけに限らず、あらゆる SNMP 変数を監視することが可能である。また、他の外部プログラムを使用して、MRTG で監視されているデータを集約することもできる。MRTG を使って複数のデータを 1 つのグラフにまとめることもできる。

2 MRTG のグラフ (<http://www.stat.ee.ethz.ch/mrtg/>)

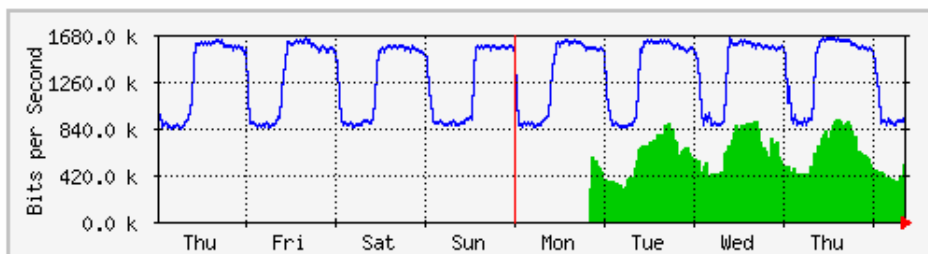
'Daily' Graph (5 Minute Average)



Max In:1035.7 kb/s (0.1%) Average In:585.5 kb/s (0.1%) Current In:665.0 kb/s (0.1%)
Max Out:1789.9 kb/s (0.2%) Average Out:1290.7 kb/s (0.1%) Current Out:1201.7 kb/s (0.1%)

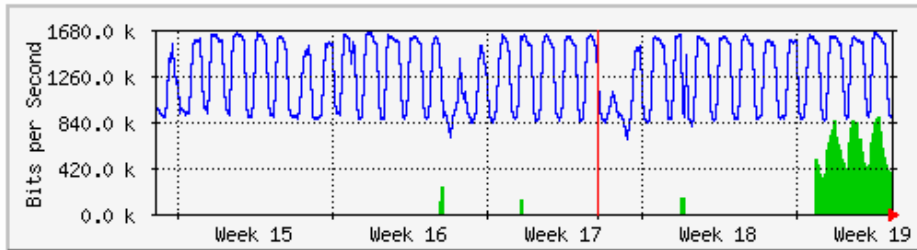
1 日間のネットワーク上のトラフィック(5分毎の平均)をグラフ化したもの

'Weekly' Graph (30 Minute Average)



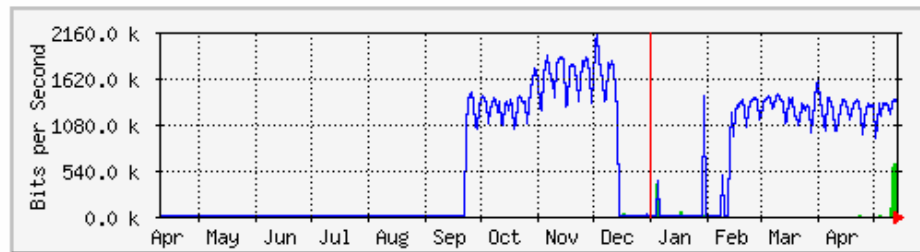
1 週間のネットワーク上のトラフィック(30分毎の平均)をグラフ化したもの

Monthly Graph (2 Hour Average)



ひと月間のネットワーク上のトラフィック(2時間毎の平均)をグラフ化したもの

Yearly Graph (1 Day Average)



Max In:646.4 kb/s (0.1%) Average In:11.7 kb/s (0.0%) Current In:646.4 kb/s (0.1%)
Max Out:2155.8 kb/s (0.2%) Average Out:1038.9 kb/s (0.1%) Current Out:1402.3 kb/s (0.1%)

1年間のネットワーク上のトラフィック(2時間毎の平均)をグラフ化したもの

GREEN ### Incoming Traffic in Bits per Second (入ってくる情報量をビット/秒で表したもの)

BLUE ### Outgoing Traffic in Bits per Second (出て行く情報量をビット/秒で表したもの)

3 導入について

現在本校において、ネットワークの監視やログのチェックを行う機関がない。そこでMRTGを用いてネットワークのトラフィックを監視できれば、グラフ化されているため非常に見やすくログからデータを読む手間が省かれ効率アップを図ることが可能である。

MRTGの導入については今後検討していく必要がある。

第4章 PC サーバの構築と活用

本校では、生徒用パソコンのリース契約の際、Linuxとして活用するためのパソコンを1台導入した。現在の状況としては、Linuxに関する知識を有した教員が私を含め本校に在籍しておらず、Linuxが導入されていないといった状況である。そのため、本研修でLinuxに関する知識を身につけ本校にLinuxサーバを導入したいと考えた。

まず、はじめにUNIX・Linuxとは何か、UNIXの歴史、オープンソースOS、Linuxを取り巻く環境などについて調査を行なった。また、どういった経緯で企業や大学がLinuxサーバを導入しているのかなどについて調査を実施した。

次にUNIXの流れを汲むOSとして広く利用されているLinuxについて、具体的に調査を行い、本校に導入することを想定しながら、どういったことをLinuxサーバで行い、運用していくかについて検討し、その運用例を作成した。ここでは、Linuxに関して技術的なものではなく、導入目的と活用例について検証した。ウェブサーバを校内用として構築し、諸連絡等のページを作成してどのように活用していくかについて検討し、Linuxにおける基本的なコマンドについての学習を実施した。

実習については、Red Hat Linuxの後継種であるFedora Core2のインストールおよびサーバ構築（ファイルサーバ、ウェブサーバ）を実施した。また、Linuxサーバ導入から構築までの一連の流れと、各サーバの設定方法についてのまとめを行い、「Linuxサーバ構築例」を作成した。

今回研修した内容を私一人のスキルアップのためのものとはせず、「Linuxサーバ構築例」としてまとめたものについては、今後Linuxサーバの導入を検討している学校のネットワーク管理者へ配布できるよう考慮しながら作成していった。

Linux とは

1 Linux とは

(1) Linux の誕生

Linux は、フィンランドのヘルシンキ大学の学生だったリーナス・トーバルズ氏 (Linus B. Torvalds) によって開発され、1991 年に一般公開された UNIX クローンの OS である。Linux は、ソースコードを含めてすべてインターネットでフリーソフトウェアとして公開され、当初はボランティア・ベースのみで付属ツール開発や多言語対応などが行われた。

インターネット上の Web サーバやメールサーバなどとして十分実用に耐えることが分かったと、Linux をベースとするシステム・インテグレーションや、Linux 対応のアプリケーション開発などが活発化した。

(2) オープンソース

オープンソースとは、ソフトウェアの設計図にあたるソースコードを、インターネットなどを通じて無償で公開し、誰でもそのソフトウェアの改良、再配布が行なえるようにすることである。ソースコードがあれば、そのソフトウェアの類似品を作成したり、そのソフトウェアで利用されている技術を転用することが容易であるため、企業などでは自社の開発したソフトウェアのソースコードは極秘とし、他社に供与するときにはライセンス料を取ることが多い。

それに対し、オープンソースの考え方は、ソースコードを公開して有用な技術を共有することで、世界中の誰もが自由にソフトウェアの開発に参加することができ、その方が素晴らしいソフトウェアが生まれるはずだという思想に基づいている。Linux がはじめてインターネットに公開されたとき、このオープンソースという形式をとって公開されたため、世界中の優秀な技術者がボランティアで Linux の改良を行い、これまでにない速さで安定した堅牢な OS が誕生した。

(3) オープンソースによるメリットとデメリット

メリット

- ・オープンソースは無料のためコスト削減が可能
- ・セキュリティの観点からソースコードが公開されているため透明性が高い
- ・多くの技術者が開発に携わるため、質の高いプログラムが仕上がる

デメリット

- ・商用ソフトでは当たり前前のサポートが受けられない
- ・ユーザに Windows のように浸透していないため実績が少ない
- ・技術者の育成におけるノウハウの蓄積が困難

(3) カーネル

Linux とは、厳密に言うとハードウェアと密接に関わりのある「カーネル」という部分を指す。インターネットに公開されたばかりのときは、ほとんどカーネルの状態のままであったため、より完成度の高い OS にするには多くのユーティリティ・プログラムが必要であった。

Linux は GNU GPL (GNU General Public License) と呼ばれるライセンスに基づいて無料で配布されている。これは Linux の大きな特徴である。しかし本来の Linux として提供されるのは、OS のカーネルのみで、シェルやツールなどの付属ソフトウェアは、ほかのソフトウェアを組み合わせる必要がある。

1つのコンピュータシステムとして使うには、カーネルだけでは何もできないため、GNU ソフトウェアなど、他のソフトウェアと組み合わせる必要がある。さらに日本語環境では、追加の日本語フォントや、「かな漢字変換ソフト」も必要となる。このため、Linux カーネルと、標準的な追加ソフトウェアをパッケージ化したものが配布されるようになった。これが Linux ディストリビューション・パッケージである。ディストリビューション・パッケージは、世界に数百種類以上あるといわれており、その多くが無償で配布されている。Linux が実用性を増すとともに、営利目的でディストリビューション・パッケージを販売する企業が誕生した。これがいわゆる商用 Linux ディストリビュータである。

商用ディストリビュータは、Linux ディストリビューション・パッケージの一部として商用ソフトウェアなどを提供するだけでなく、各種サポートを準備して、インストール時やトラブル発生時にユーザが「サポートを受ける権利」を提供している。

このように、日本語フォントや、かな漢字変換ソフトのような商用ソフトウェアが不要で、かつサポートは一切あてにすることなくインストールやセットアップ、運用が可能な技術とノウハウがあるというのでなければ、Linux であっても有償のディストリビューション・パッケージを購入しなければならない。

2 Linux の種類

Linux といっても、日本で販売されている主要な製品だけでも、Red Hat Enterprise Linux、Vine Linux、SUSE Linux、Turbo Linux、MIRACLE Linux など、多数の種類がある。これらはいずれも Linux の異なるディストリビューション・パッケージである。

前述したとおり、厳密に言えば、Linux は OS のカーネルの部分だけを指す。このため各ディストリビューション・パッケージの供給元は、Linux をベースに、シェルやインストーラ、アプリケーション・ソフトなどを、独自にパッケージ化して販売している。パッケージの内容が異なれば、当然それは機能差や使い勝手の差となって表れてくる。

ディストリビューション・パッケージの差が最も顕著に表れるのが、システム管理ツールである。例えば Red Hat Linux と SUSE Linux、Vine Linux では、まったく異なるシステム管理ツールがパッケージングされている。どれが使いやすいかは一概にいえませんが、どのディストリビューション・パッケージを選択するかで、管理の手順や、管理にかかる工数がかかなり変わってくるはずである。このためユーザは、各ディストリビューション・パッケージの違いを正しく認識し、適切なパッケージを選択する必要がある。

3 UNIX

(1) UNIX の歴史

最初の UNIX は、1969 年に AT&T のベル研究所でアセンブリ言語により開発された。当時 Multics と呼んでいたものが、UNIX と名称が改められ、その後の何回かの改版によって様々な機能が追加された。

1973 年の第 5 版では、OS の中核部分のカーネルが C 言語で書き直され、1974 年には大学で使用されるようになり、実験室、ソフトウェア開発プロジェクトチーム、電話局の業務支援システム等に導入されるようになる。

1978 年の第 7 版で現在の UNIX の主な機能が装備された。この時期にカリフォルニア大学バークレイ校で UNIX の改造が始まる。従って、AT&T 版とバークレイ版 (BSD: Berkley Software Distribution) という 2 つの流れができた。

1980 年代に、AT&T の System とバークレイの 4.2BSD が発表されている。その後両方の良いところを合わせた System Release 4.0 をサンマイクロシステムズが開発する。これに対して IBM、HP など

どが OSF (Open Software Foundation) という団体を設立し、OSF/1 という UNIX を提供するようになった。その後世界中に広がって何十万ものシステムに搭載され、その範囲はマイクロコンピュータから大型メインフレームにまで及んでいる。

(2) UNIX の特徴

UNIX は非常に優れた OS であり、特にサーバとして利用するには最適のシステムである。また、UNIX はサーバ・ワークステーション用 OS として一番古くからあった OS である。UNIX を動かすには大規模なハードウェアが必要であり、個人ユーザ向けとしては不適切であった。そこで考案されたのが PC-UNIX である。これは一般にパソコンと呼ばれているコンピュータで UNIX を動かすために開発された OS である。(厳密に言えば Linux は UNIX ではなく、本来 Linux とは UNIX のカーネルを指す。その他にも FreeBSD などの無償 OS の他に Sun Microsystems が開発する商用 (有償でサポートの整ったもの) UNIX・SunOS や同じく商用 UNIX の Hewlett Packard 開発による HPUX 等がある。

当時はパソコンがとても高価で、今のように個人が一台を所有することができなかつたことから、複数の人が一台のパソコンを利用できるマルチタスク、マルチユーザを実現した OS であった。UNIX は当時、独占禁止法によってコンピュータ産業に参入することができず、格安の値段でさまざまな教育機関に配布されていた。

マルチタスク

複数の処理を同時に実行できる。(タスク コンピュータで実行される処理の単位) UNIX は優れたメモリ管理機能を有している。(異なる処理が同時に進行しても、お互いのデータを破壊しない)

サーバは他のコンピュータから同時にアクセスされる。複数のプログラムを同時に実行しても UNIX マシンであれば安定した動作が可能

マルチユーザ

UNIX は 1 台のマシンを複数のユーザが同時に利用できるよう設計されている。他のユーザのファイルやプロセスに危害を加えることができないようになっている。異なる OS (Windows や Mac OS) からでもサーバを利用できる。

仮想記憶

実装しているメモリ (RAM) の中から使用頻度の少ないデータをハードディスクに書き出し、使用頻度の高いデータのみを RAM に保存することで、効率よくデータ処理を行う技術。UNIX では、プロセス (マルチタスク環境で現在実行中のプログラムを指す) の実行に応じて必要な時点で必要な部分だけをメモリに読み込む要求時ページングという技法により、実メモリよりも大きな容量を持つプログラムでも実行可能。

パイプライン

複数のプログラムを連結して動作させる機能。

4 ファイルサーバとしての Linux

ファイルサーバはファイルを管理するためのサーバである。部署内でファイルを共有する場合や異なる OS 間でファイルを受け渡す場合などに、Linux で構築したファイルサーバが役立つ。ファイルサーバとして Windows や MacOS を使う方法もあるが、Linux によるファイルサーバはこれらと比較して動作が軽く (速く)、安定しているため、多数のユーザが同時にアクセスするような環境でも快適に利用できる。また、ファイルサーバの構築に必要なツールがフリーで配布されていることも魅力である。

5 Linux をサーバとして利用するための条件

ネットワークサーバに必要なハードウェア構成は、それほどハイスペックではない。基本的にはネットワークカードと必要なだけのディスク容量さえあればよい。マシンのパフォーマンスを大きく左右するのはCPUとメモリであるが、パシフィック・ハイテックによる推奨動作環境は以下のとおりである。

C P U : Pentium 233MHz 以上

メモリ : 64MB 以上

ハードディスク : 2 GB 以上

ネットワークサーバのパフォーマンスは、動作させる各種サーバーソフトの構成や設定、アクセス頻度などにより変化する。

Linux の導入と活用例

1 導入の目的（実践的目的）

Linux を導入するにあたって、教員間での校内情報の共有を目指す。

校内での連絡などは全て紙による印刷物である。そこで、印刷物等を紛失して見ることができなくなることや、連絡の徹底が図れなくなることを防ぐ。また、そのデータを pdf ファイルとして管理すれば、パソコン操作が苦手な教員からの操作ミスによるファイルの消去や改ざんを防ぐことができる。

以前職員に対する情報機器の活用について調査をおこなった。その調査の結果から、パソコンを自在に使うことはがきない教員が 35%いたが、インターネットによる Web の閲覧ができないと答えた教員はいなかった。そのことから、教員全員がファイルを共有するためには Web 上に共有できる情報を保管しておくことが一番良いと考えた。

2 学校現場で必要なものとして（どういうサーバをセットアップするか）

Webサーバとファイルサーバを構築する。

- ・Webサーバ …… 福岡県教育センターの Web サーバを自由に使えない(本校の HP も教育センターで管理されている)ため、校内用の Web サーバとし教職員でのファイルを共有する。職員会議の資料をはじめ、校内で配布されたプリント類を pdf 形式で Web サーバに保存し、全職員が簡単に閲覧できるようにする。
- ・ファイルサーバ …… 校務分掌別のフォルダをはじめ、係りごとのファイルを置き、ファイルの共有を図る。また、個人用のファイルについては別のファイルサーバを置き、個人用のフォルダを作りファイルの共有を図る。

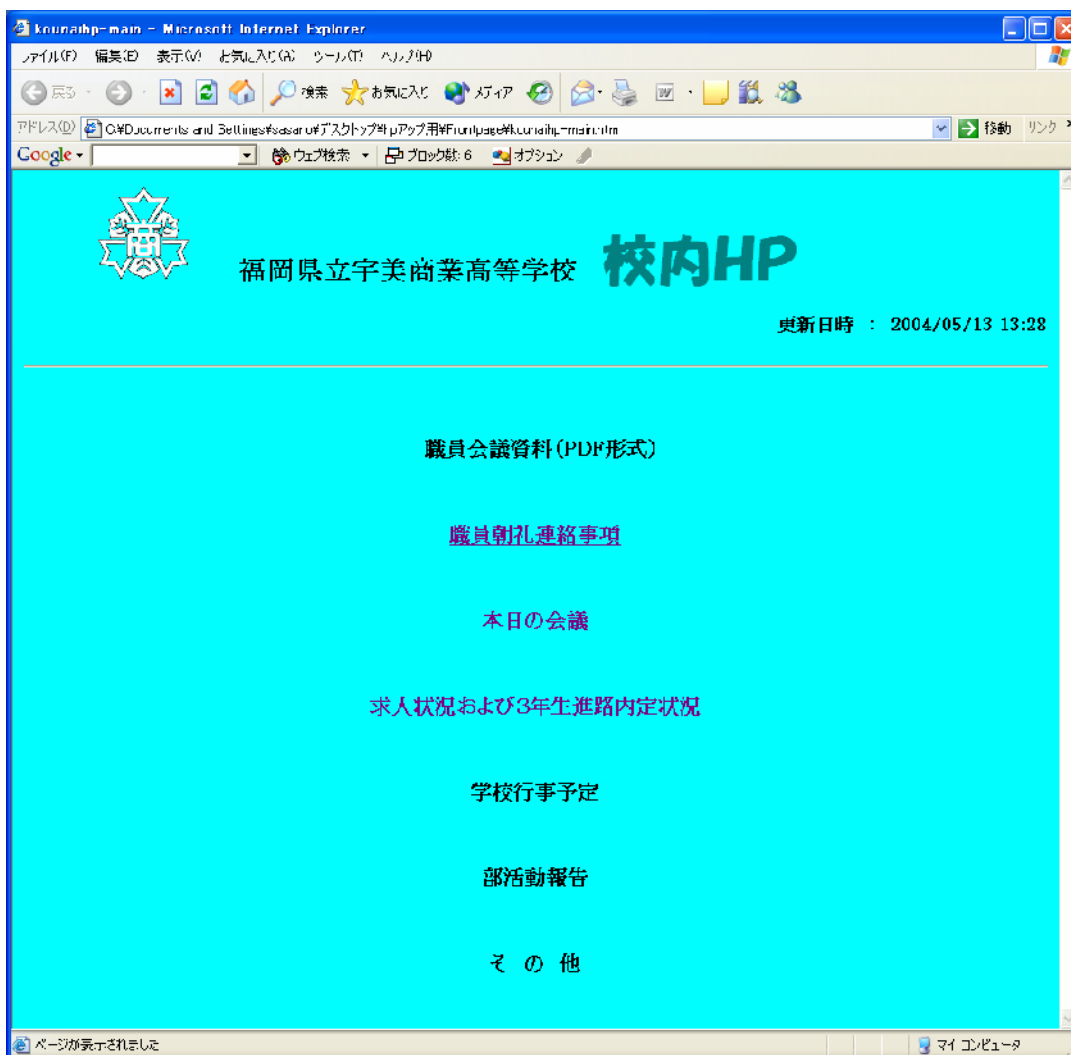
3 構成

Webサーバでは校内用のHPをアップロードし、全職員に本校の状況等逐一閲覧できるように配慮する。現在会議の連絡や朝礼での連絡は全て職員室のホワイトボードに記入されている。職員室に不在で各準備室や教官室に常駐している教員に対する連絡を校内のネットワークに接続されているパソコンからいつでも確認できるようにしたい。また、本校の職員全員で共通のデータを共有したいということから、以下に掲げる項目を校内用HPとして毎日更新していきたい。

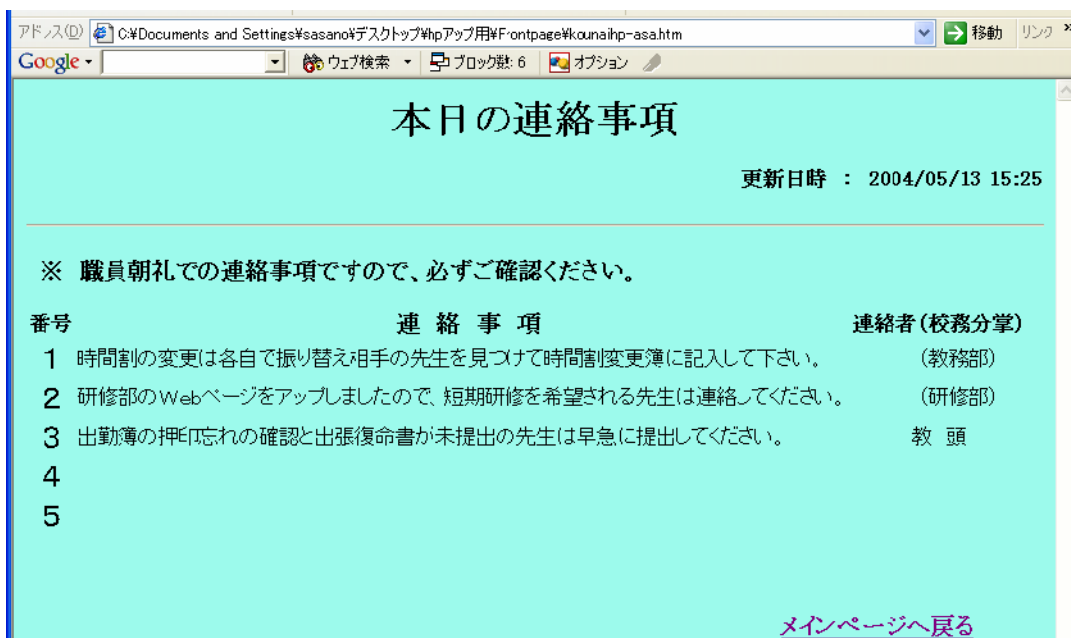
- ・職員会議資料 …… 職員会議の資料をはじめ、職員に公開可能なものを置き、閲覧に制限をかけない。
- ・職員朝礼連絡事項 …… 朝礼に出席できない教員のために、毎朝の連絡事項を閲覧できるようにする。現在ホワイトボードに連絡事項を記入していることをWebで閲覧できるよう工夫する。
- ・学校行事等の連絡 …… 学校行事の日程の掲載を行う。
- ・部活動等の連絡 …… 部活動（運動部・文化部）の試合報告や国家試験合格者などを掲載し、職員全体に本校の活動状況を把握させる。
- ・進路情報の掲載 …… 求人状況や内定状況を職員に知らせる。今までは3年生の進路状況をリアルタイムに確認する場所がなかったため、Webにより公開する。
- ・会議の連絡 …… どの場所からでも会議の時間と場所が確認できるようにする。

校内用ホームページの例 (<http://itslab.csce.kyushu-u.ac.jp/~sasano/actest/kounaihp-main.htm>)

メイン画面



職員朝礼連絡事項の画面



本日の会議の連絡用画面

本日の会議予定

更新日時 : 2004/05/13 15:38

※ 本日の会議の予定です。場所・時間等の変更については適宜アップします。

会議名	時間	場所
職員会議	16:10~17:00	会議室
商業科会議	職員会議終了後	会議室
運営委員会	4時間目	小会議室

[メインページへ戻る](#)

求人状況および進路内定状況の画面

求人情報および進路内定状況 進路指導部

更新日時 : 2004/05/13 15:47

○生徒の進路状況

・就職内定者

組氏名	企業名	職種	内定日
7組 山田 花子	宇美商事株式会社	一般事務	9月18日
6組 鈴木 一郎	糟屋物産株式会社	営業事務	9月19日

・進学先決定者

組氏名	学校名	学部・学科名
1組 宇美 太郎	宇美情報大学	情報学部 情報科学学科
3組 福岡 次郎	須恵簿記情報専門学校 福岡校	マルチメディア科

○求人状況

受付番号	企業名	受付日時
16001	糟屋物産株式会社	7月25日
16002	福岡商事株式会社	7月25日
16003	福岡硝子販売株式会社	7月25日
16004	糟屋物産株式会社	7月25日

[メインページへ戻る](#)

4 ネットワークコマンド（目的別調査一覧）

コマンド	説明	使用目的
Ping	パケットを送りネットワークの状況をチェックする。	指定したホストからの応答を調べる。通信ができない時や指定したホストまでの通信が可能であるかなどを調べる。
Ping-q	結果は表示されない。ping のオプション。	ppp 接続などで常にアクティブでないといけないうきに便利なコマンドである。
Ping-s	送信するパケットサイズを指定する。ping のオプション。	送信するパケットサイズを調べるときに使用する。
ifconfig	指定したネットワークインタフェース情報を表示する。	ローカルホスト上で promiscuous モードで動作しているインタフェースを検出することができる。
ifconfig-a	全てのネットワークインタフェースの状態を表示する。ifconfig のオプション。	デバイス名がわからない場合に使用する。
traceroute	目的のノードまでのポップ数や、その経路について調べる。	目的のノードまでのポップカウントや経路情報、各部での遅延時間などを調べたいときに使用する。
netstat	マシンが認識しているネットワークに関する設定情報を表示する。	ネットワークの状態を調べる際に使う。
nslookup	指定したホストコンピュータの情報を表示する。	指定したホストコンピュータの情報を見たいときに使う。
ftp	指定したホストとの間でファイルのやり取りを行う。	ネットワーク上でのファイル転送を行う際に使用する。

5 命令だけでなく ping でどういうデータが流れているか

TCP/IP の IP レベルで通信できるかどうかを確認するために、ping コマンドを使う。ping は ICMP パケットを送信し、相手からの応答を要求するプログラムである。

ping コマンドは、まずアドレスにエコー要求パケットを送信し応答を待つ。ping は、次の場合にだけ成功する。

エコー要求が宛先に到達する場合。

宛先が送信元へエコー応答を戻すことができる場合。

ping や traceroute では一般に、ICMP (Internet Control Message Protocol : RFC792 / RFC1812) と呼ばれる特別なプロトコルを用いてネットワークの疎通を確認している。

もともと ICMP は、ネットワークに障害があり正常な通信が行えない場合に、経路に位置するルータやホストが送信元ホストへその障害を知らせるためのプロトコルである。そのため、**エラー報告プロトコル**とも呼ばれる。IP 自体は到達信頼性の低いプロトコルだが、仮に途中でパケットが破棄されたとしても、再送などによりエラーをハンドリングすることは可能だ。しかし永続的な障害などの場合には、非常に効率が悪い結果となる。そこで、ICMP によってエラーを通知することで、復旧やエラーハンドリングの効率を上げる目的を持っている。ICMP は IP 上で動作するプロトコルであり、TCP や UDP と同一階層と考えてよ

い。IP ヘッダにおける Protocol フィールドは 1 が設定される。こうした障害時通知など特殊な目的のためには、通常の TCP や UDP に比べ、より詳細な情報が通知できるように設計されている。

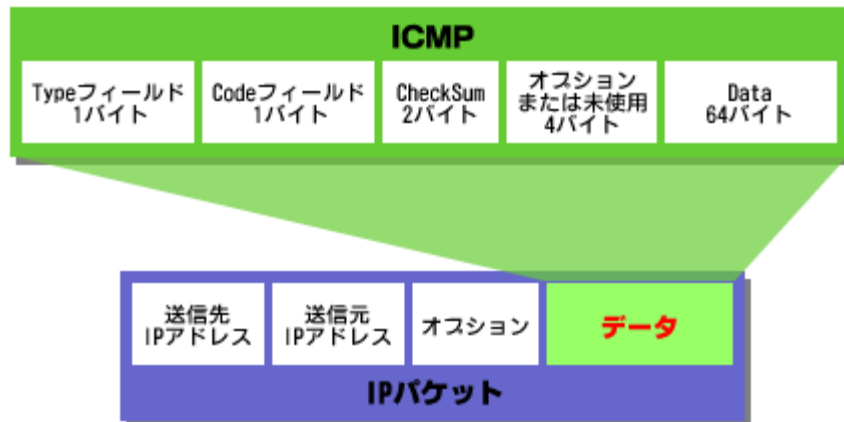


図1 ICMP のプロトコルフォーマット

Linux サーバの構築

Linux サーバを構築するにあたり、最初にどのディストリビューションを導入するかを考えなければならない。現在世界には、無数のディストリビュータがいて、様々なディストリビューションが存在する。そして、その数は今も増え続けている。

現在一般に普及しているディストリビューションには、OS の稼動に必要なプログラムだけでなく、便利なアプリケーションやツール、各種デバイスドライバが大量に収録されている。ディストリビューションによっては、ワープロや表計算といったオフィス系ソフトをはじめ、画像処理ソフト、音楽再生ソフト、プログラミングの開発環境など、コンピュータ上で使われるありとあらゆるソフトを網羅したものもある。

こうしたディストリビューションのほとんどが、オープンソースの考えに則り、インターネットや雑誌付録の CD-ROM などを通じて無償で公開されている。そのため、メーカーの作ったものであっても、その会社の FTP サイトなどからダウンロードすれば簡単に入手することができる。なおメーカーでは、自社のディストリビューションに関して有償によるサポートを行ったり、パッケージとして販売するなどの方法で収益を得ている。

Linux のディストリビューションには様々な種類があるが、基本的には同じカーネルを使っている。従って、本来ならばディストリビューション間におけるソフトの互換性があるはずだが、現実にはそうになっていない。各ディストリビューションは、おおよそ「Red Hat 系」・「Slackware 系」・「Debian 系」の 3 つの系統に分かれている。また、日本国内でよく利用されているディストリビューションは、Red Hat Linux・Turbolinux・Vine Linux・LASER5 Linux・Linux MLD 6 が挙げられる。

これ以降の説明として Red Hat 系のディストリビューションである Fedora Core2 について述べていく。

1 Linux のインストール

- (1) 以下の URL から、Fedora Core2 のソースプログラムをダウンロードし、ライティングソフトで CD-R 等のメディアに書き込む。650MB 以上の CD-R が 4 枚必要となる。

<http://download.fedora.redhat.com/pub/fedora/linux/core/2/i386/iso>

- (2) Linux のインストールを行う前に、BIOS の設定を一部変更しておく。

設定の必要な項目は、BIOS のトップメニュー上の「Advanced BIOS Features」(旧バージョンでは「BIOS FEATUERS SETUP」)を選択し、「Anti-Virus Protection」を「Disabled」にする。これはウイルス対策を無効にするということで、BIOS が行うウイルス対策の実体は、とかくウイルスが付着しやすいハードディスクの MBR を書き込み禁止にするというものである。

次に、コンピュータを CD-ROM から起動するため CD-ROM の起動順序を変更する。設定を保存して終了する。

- (3) インストール CD のテストを行う。

インストールは CD-1 から行う。インストーラの最初の画面が表示され、ここでインストールの方法を選択する。ここでは操作が簡単なグラフィカルモードでのインストール方法を行う。グラフィカルモードでのインストールを始めるには、そのまま「Enter」キーを押す。インストール CD が正規の Fedora Core2 であることをテストするかどうかを選択する。初回だけ「OK」ボタンを選択しテストへ進む。

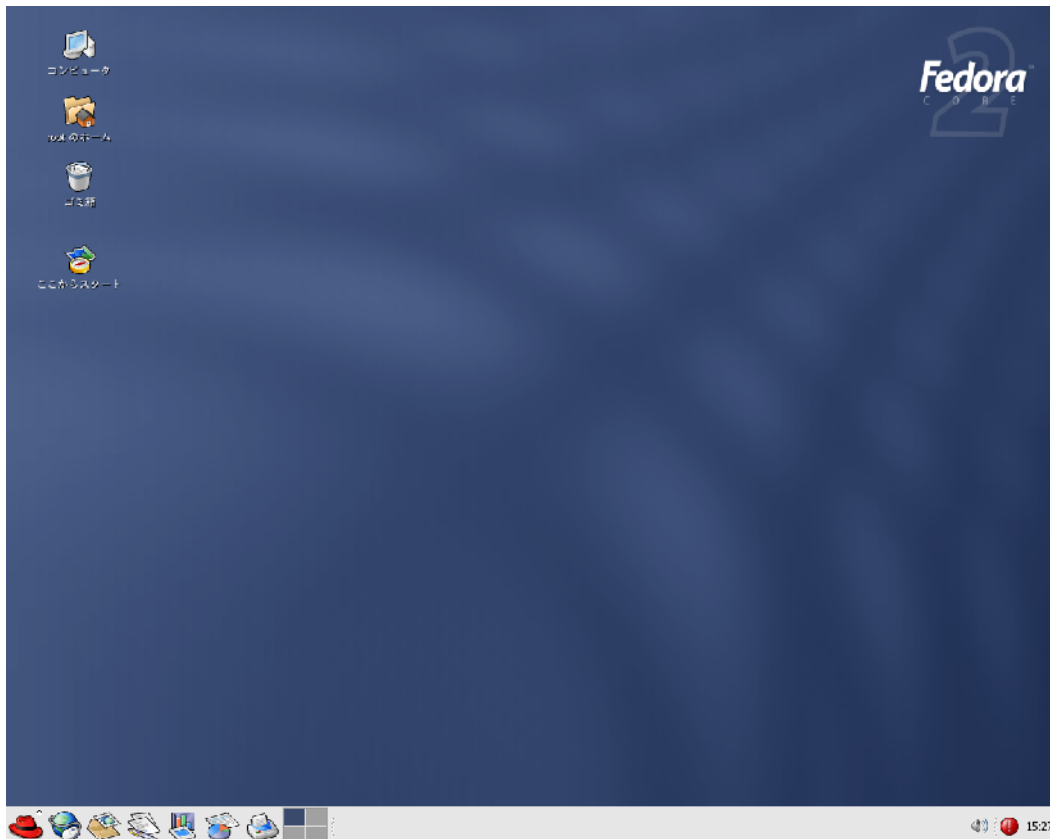
- (4) 作成した 4 枚の CD がすべて合格となることを確認したらテストを終了し、インストールへ進む。インストール CD1 をセットし、「Continue」ボタンを押しインストールを行う。言語を選択する画面では、「Japanese」すると、次の画面から表示が日本語となる。キーボードを設定、モニターを設定し

て進んでいくと「パーティションを正しく調整できない」という「警告」の画面が出てくるが、「無視」のボタンをクリックし、そのまま作業を続ける。

(5) インストール完了後再起動する。

Linux の起動後、ライセンス同意書が英文で表示されるので、それに同意できれば「同意する」を選択する。日付と時刻、ディスプレイの表示の仕方を設定し、一般ユーザのアカウントを一つ設定する。このアカウントは、管理者が日常の作業のためにログインするときに使う。しかし、メンテナンスにあたる操作は禁止される。

(6) ユーザ名 (root) とパスワードを入力して起動する。

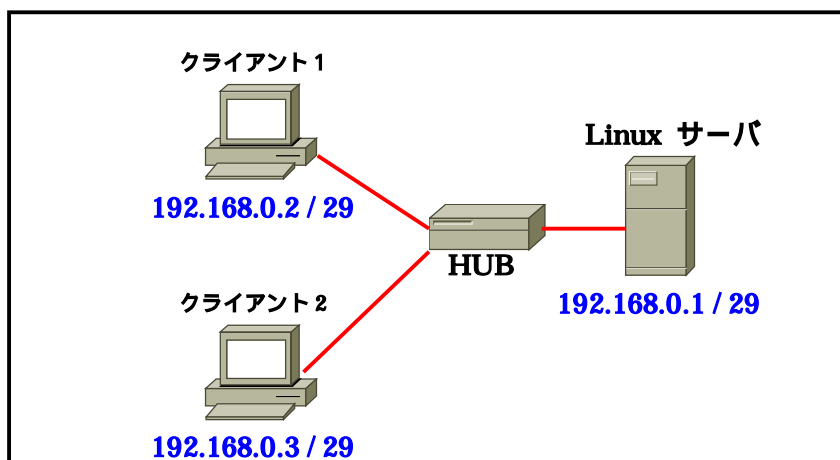


【Fedora Core2 の画面】

2 Linux サーバ構築計画

Linux サーバを構築するにあたり、練習を兼ねて段階的に設定作業を進めていった。

(1) 独立したネットワークの作成



準備物

- ・HUB 1 (3ポート以上)
- ・LANケーブル 3
- ・クライアントPC 2
- ・Linuxサーバ 1

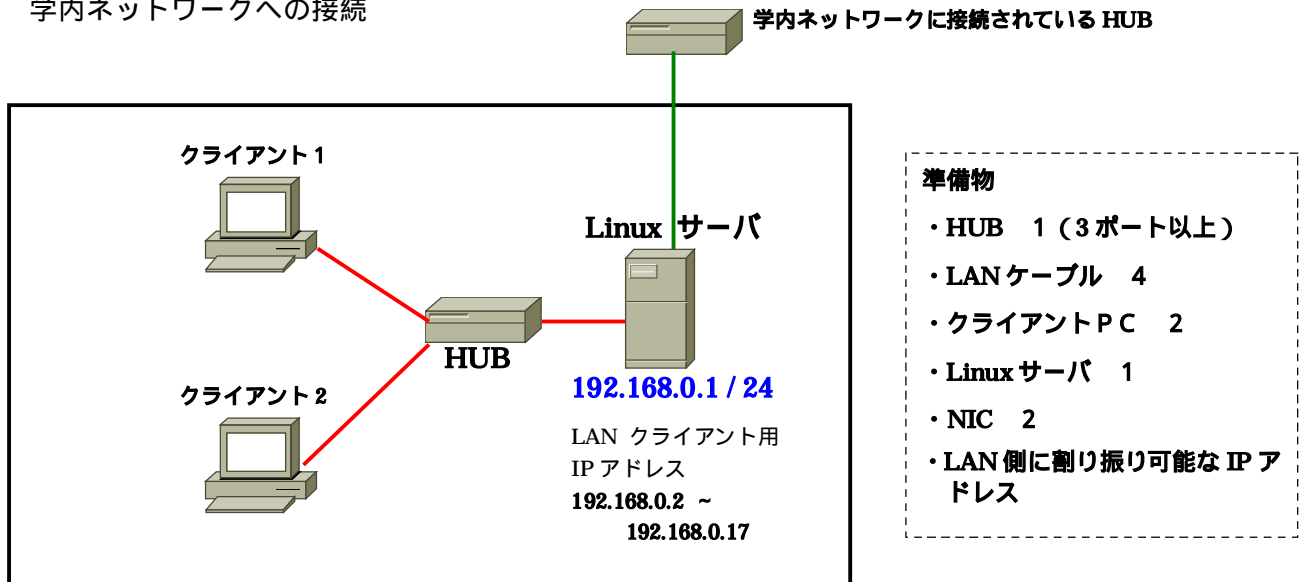
設定手順

機器の物理的な接続

Linux サーバの構築

- ・ Windows 用のファイルサーバ samba
- ・ クライアント (ユーザ) 登録
- ・ プライベート IP アドレスの設定
- ・ クライアントのネットワーク設定

(2) 学内ネットワークへの接続

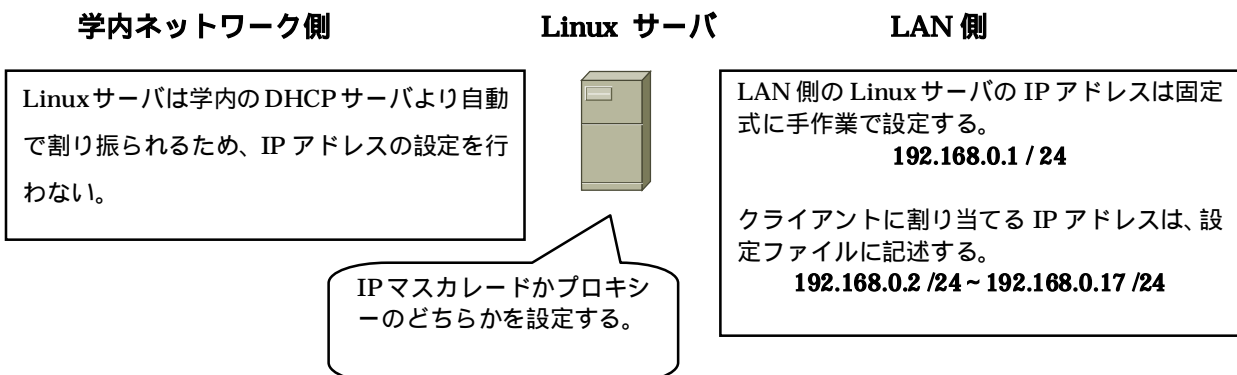


設定手順

Linux サーバの構築 (DHCP サーバ・DNS サーバ)

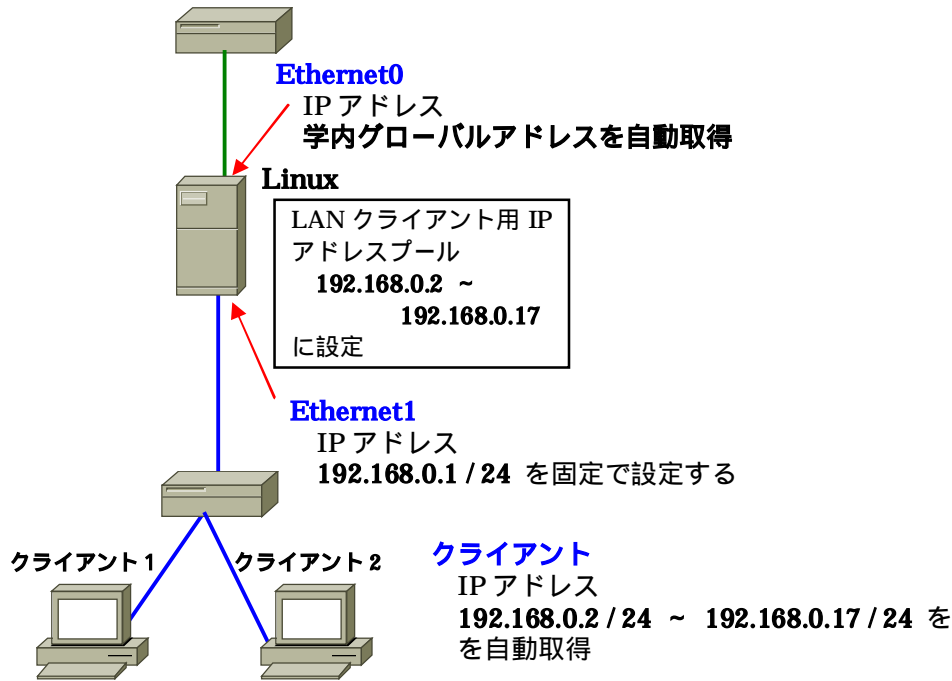
- ・ Linux サーバには、学内ネットワーク側と LAN 側の二つの IP アドレスを割り当てる。学内の DHCP サーバから Linux サーバは DHCP クライアントでグローバルアドレスを受け取り設定される。(GNOME で ifconfig コマンドを使い確認する)
 - ・ Linux サーバの DHCP サーバで LAN 側にプライベート IP アドレスを自動で割り振る。
- クライアントの設定
- ・ クライアントは自動で IP アドレスを受け取るため、「IP アドレスを自動的に取得する」にする。

Linux サーバ設定の詳細



(3) 各設定の詳細

学内ネットワークに接続されている HUB



```
root@csce:~
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(T) ヘルプ(H)
[root@csce root]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:01:80:31:EC:
          inet addr:          Bcast:          Mask:255.255.255.0
          inet6 addr: fe80::201:80ff:fe31:ece7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:37098 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4926 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7411977 (7.0 Mb)  TX bytes:511804 (499.8 Kb)
          Interrupt:11 Base address:0xc000

eth1      Link encap:Ethernet  HWaddr 00:90:CC:51:AF:11
          inet addr:192.168.0.1 Bcast:192.168.0.255 Mask:255.255.255.0
          inet6 addr: fe80::290:ccff:fe51:af11/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5448 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6217 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:584477 (570.7 Kb)  TX bytes:5122019 (4.8 Mb)
          Interrupt:10 Base address:0x3000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2487 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2487 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1950289 (1.8 Mb)  TX bytes:1950289 (1.8 Mb)

[root@csce root]#
```

【GNOMEでifconfigコマンドを使い確認したところ】

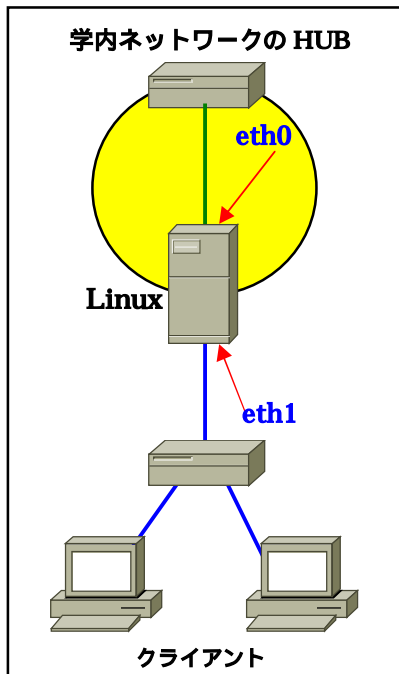
3 ネットワークへの接続

ここでは、今回構築する Linux サーバを九州大学内のネットワークに接続し、さらに小さなネットワークを作成する例を示す。一般にサーバは、IP アドレスを固定して運用するのが原則である。しかし、本研

修では学内ネットワーク内にあるDHCPサーバから自動的にIPアドレス等を取得するための設定を行なう。

(1) 学内ネットワーク側の接続

学内ネットワークに接続されているHUBとLinuxサーバに設置しているイーサネットカード(eth0)をLANケーブルで接続する。Linuxのeth0では、自動的にIPアドレス等を取得するように設定しなければならない。

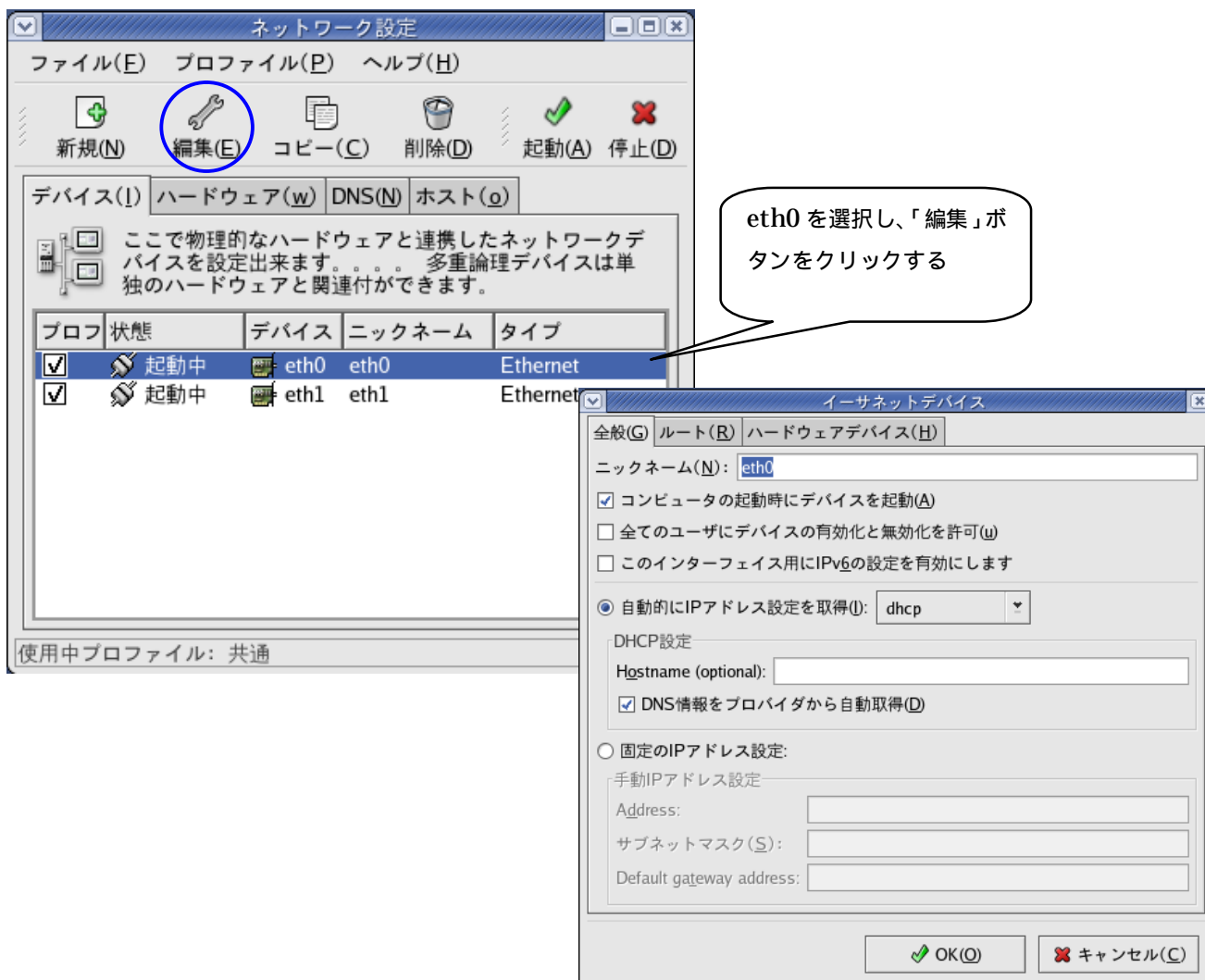


左に示すネットワーク機器構成図の黄色部分の設定について以下に示す。

Linuxサーバeth0の設定

メインメニューで「システム設定」「ネットワーク」を選択し、ネットワーク設定画面を開く。「デバイス」タブに装着されているすべてのイーサネットカードが表示される。ここで学内ネットワーク側のイーサネットカードを選択する。

次に「編集」ボタンをクリックし、選択したイーサネットカードの基本的な設定を行なうダイアログが開く。ここで、学内ネットワーク側のイーサネットカードeth0の設定を行なう。



イーサネットデバイスの設定

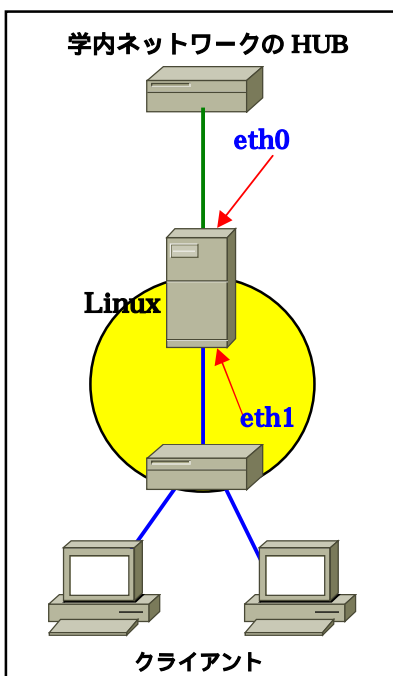
イーサネットデバイス画面で設定が必要なのは、「全般」タブだけである。まず、「コンピュータの起動時にデバイスを起動」の項目にチェックマークを入れる。次に、「自動的に IP アドレス設定を取得」をクリックし、「dhcp」とする。最後に、「DNS 情報をプロバイダから自動取得」にチェックマークを入れ、「OK」ボタンをクリックする。その後、メニューバーで「ファイル」「保存」と選択し、確認のダイアログで「OK」ボタンをクリックする。

この設定は、Linux サーバを再起動したあと有効となるため、それまでの間、動作が不安定となるためすぐに再起動を行なう必要がある。

項目	設定
コンピュータの起動時にデバイスを起動	オン
自動的に IP アドレス設定を取得	オン (dhcp を選択)
DNS 情報をプロバイダから自動取得	オン

(2) LAN 側の設定

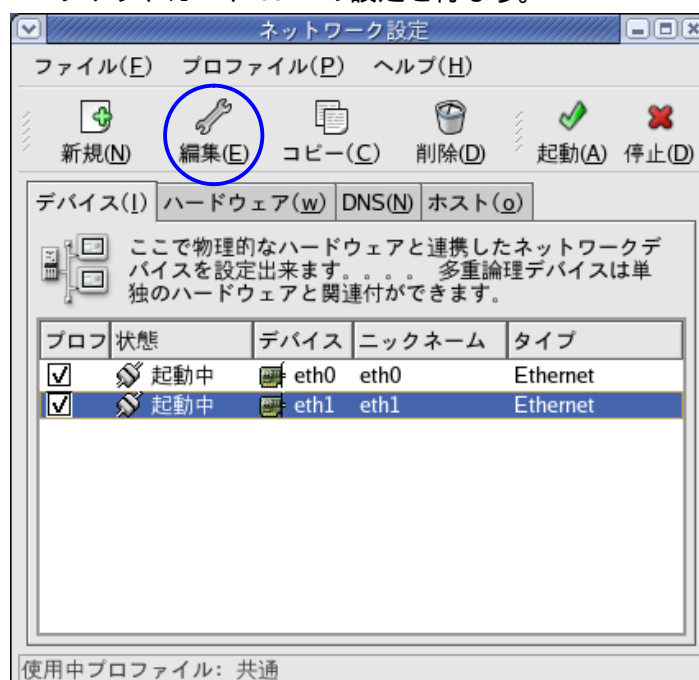
LAN 側では、Linux サーバの eth1 の IP アドレスをプライベートアドレス (192.168.0.1) に固定し、合わせて関連の設定を行なう。左に示すネットワーク機器構成図の黄色部分の設定について以下に示す。

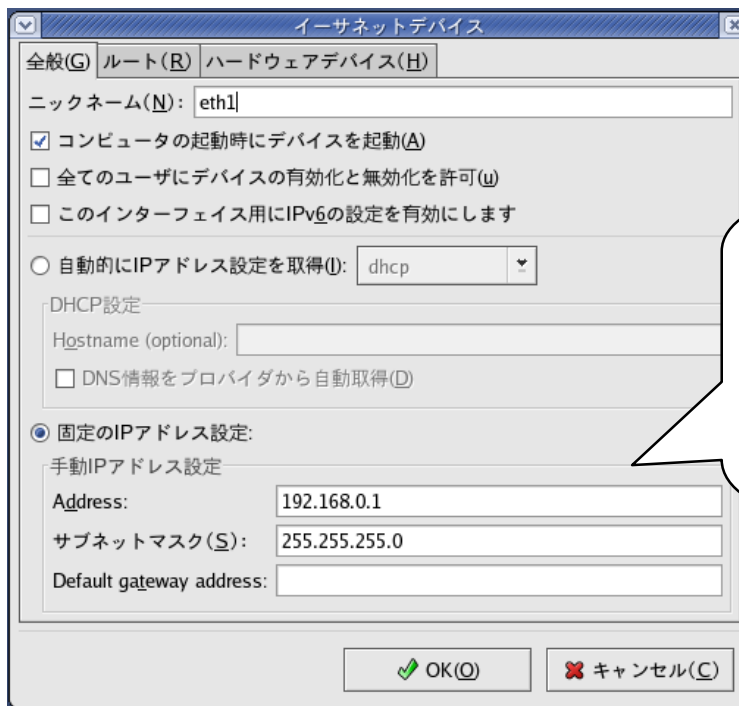


Linux サーバ eth1 の設定

メインメニューで「システム設定」「ネットワーク」を選択し、ネットワーク設定画面を開く。「デバイス」タブに装着されているすべてのイーサネットカードが表示される。ここで LAN 側のイーサネットカードを選択する。

次に「編集」ボタンをクリックし、選択したイーサネットカードの基本的な設定を行なうダイアログが開く。ここで、LAN 側のイーサネットカード eth1 の設定を行なう。





「コンピュータの起動時にデバイスを起動」をオンにする。「固定の IP アドレス設定」をオンにし、「手動 IP アドレス設定」の各欄に IP アドレスを設定。「OK」ボタンをクリックし、ダイアログを閉じる

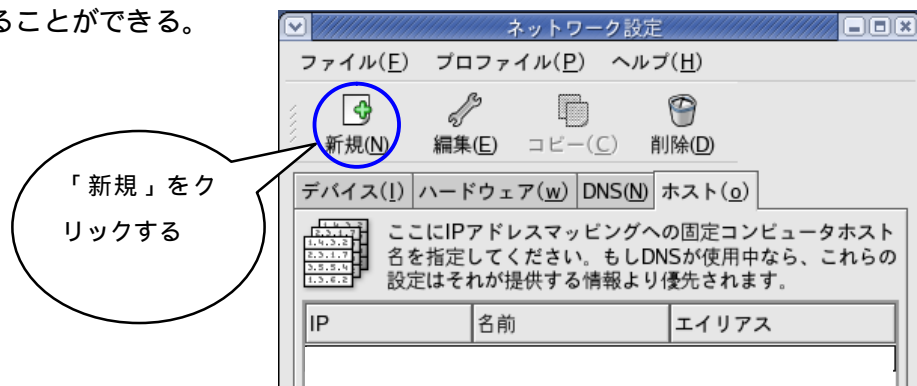
項目	設定
コンピュータの起動時にデバイスを起動	オン
固定の IP アドレス設定	オン
Address	192.168.0.1
サブネットマスク	255.255.255.0
Default gateway address	空欄

イーサネットデバイスの設定

イーサネットデバイス画面で設定が必要なのは、「全般」タブだけである。まず、「コンピュータの起動時にデバイスを起動」の項目にチェックマークを入れる。次に、「固定の IP アドレス設定」をクリックし、IP アドレスとサブネットマスクを入力し、「OK」ボタンをクリックする。

「ホスト」タブで対照表に追加する

「ホスト」タブをクリックしてホスト設定画面を開く。ここは、IP アドレスとドメイン名の対照表となっている。実物の対照表は、/ etc ディレクトリの hosts であるが、ここにその内容が反映されており、ここで編集することができる。



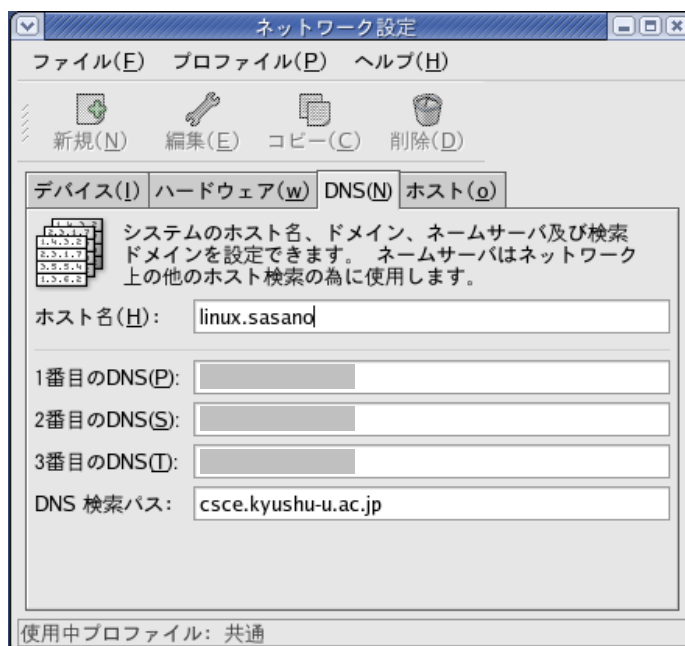
「新規」ボタンをクリックすると、追加のためのダイアログが開く。



ダイアログの各欄に、左に示す内容を設定する。IP アドレスは左に示すとおり、あとは自分で決める。設定後、「OK」ボタンをクリックし、ダイアログを閉じる。

DNS の設定

「DNS」のタブを開き、ホスト名を入力する。このホスト名は、 で設定したホスト名と同一のものでなければならない。「1 番目の DNS」～「3 番目の DNS」欄には、学内ネットワークから取得した DNS サーバの IP アドレスが設定されている。通常 2 つ設定されるが、そうでない場合もある。少なくとも一つ設定されていれば正常な状態である。



設定後、メニューバーで「ファイル」 「保存」と選択し、確認のダイアログで「OK」ボタンをクリックする。新しい設定は、Linux サーバを再起動後有効になる。

4 Linux サーバの構築

(1) Samba サーバの構築

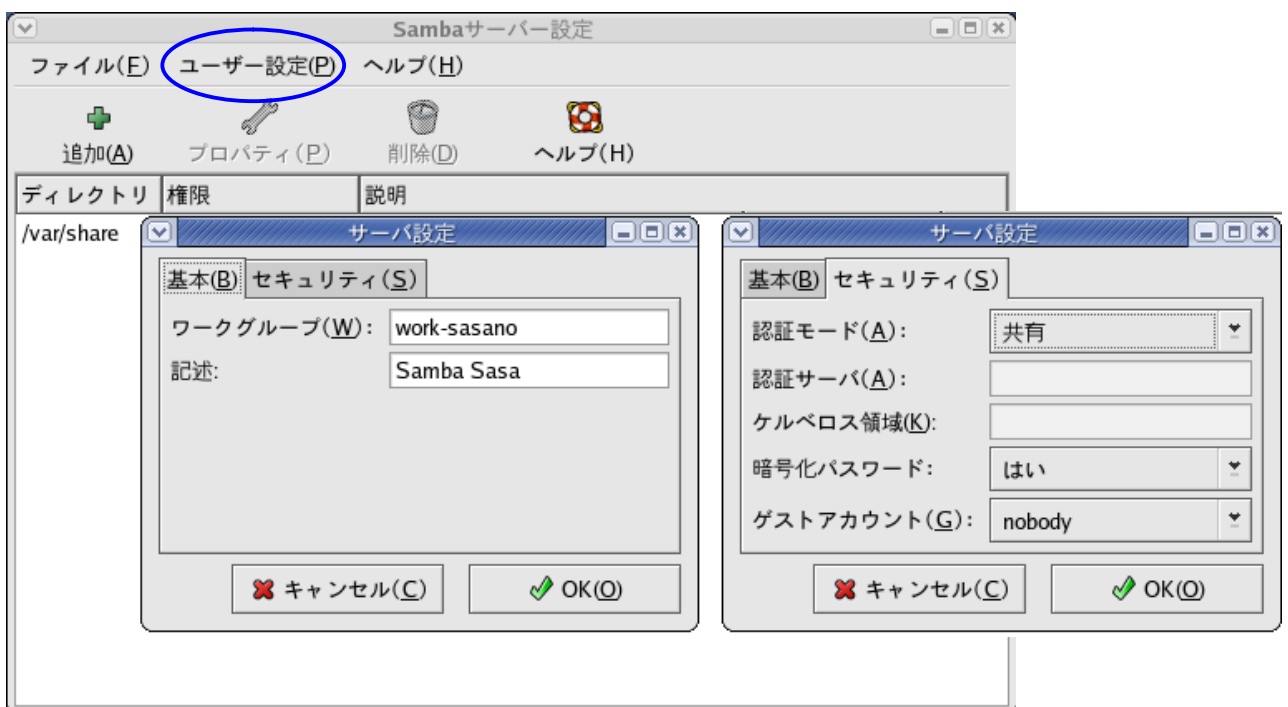
Samba サーバの設定ファイルを編集し、基本的な機能の設定と正規ユーザの登録を行う。設定ファイルの初期値により、ホームディレクトリの共有も有効になる。

基本的な機能を設定する

メインメニューで「システム設定」 「サーバ設定」 「Samba」と選択し、Samba サーバの基本的な機能を設定する。Samba サーバ設定画面のツールバーから、「ユーザ設定」 「サーバ設定」と選択し、ダイアログの各項目を設定する。このうち、「基本」タブの「ワークグループ」欄は、現在 Windows

に設定されているワークグループの名前と一致させる必要がある。設定を終えたら「OK」をクリックする。この時点で、Samba サーバが起動あるいは再起動され、新しい設定が有効になる。

項目	設定
ワークグループ	Windows のワークグループに相当する名前
記述	Windows のコメントに相当する記述
認証モード	「ユーザ」を選択
認証サーバ	空欄
ケルベロス領域	空欄
パスワードを暗号化	「はい」を選択
ゲストアカウント	「nobody」を選択



正規ユーザを登録する

Samba サーバの正規ユーザを登録する。「ユーザ設定」、「Samba ユーザ」と選択し、正規ユーザの一覧を開く。次に、「ユーザの追加」をクリックし、ダイアログの各項目を設定する。

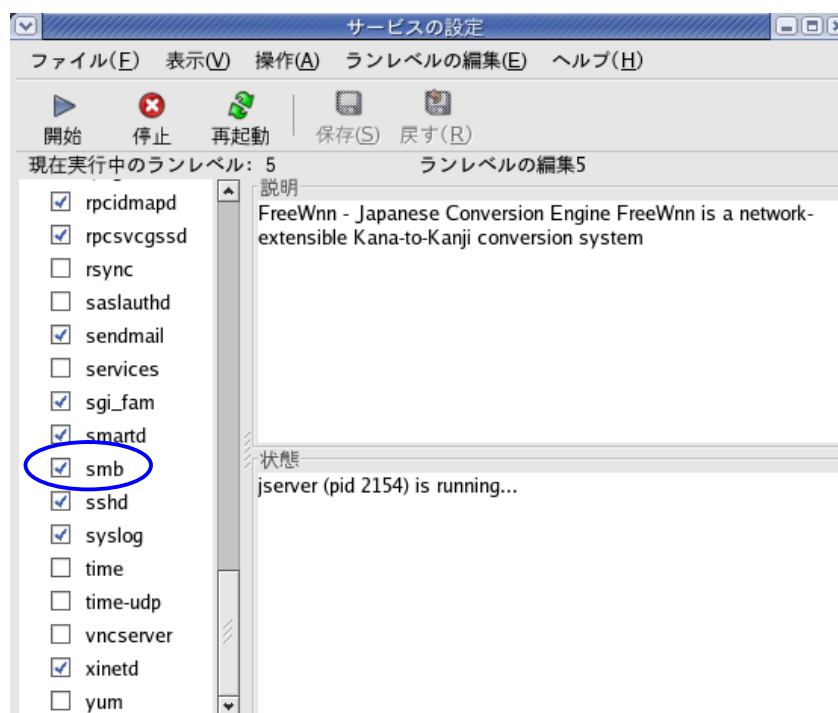
設定を終えたら、「OK」をクリックし一覧に戻る。正規ユーザはこの時点で登録される。Samba サーバとの接続には、ここで設定した「Unix ユーザ名」と「Samba のパスワード」が必要となる。

項目	設定
Unix ユーザ名	Linux サーバのアカウントのユーザ名
Windows ユーザ名	Windows のユーザ名 (使われない)
Samba のパスワード	Samba のパスワード
Samba のパスワードの確認	上記と同じパスワード



メインメニューで「サービス」を選択する

設定ツールで起動した Samba サーバは、Linux を終了すると同時に終了してしまう。ここでは、次に Linux を起動したときにも Samba サーバが自動的に起動するよう設定しておく。メインメニューで「システム設定」「サーバ設定」「サービス」と選択する。現在、Linux にインストールされているサーバの一覧が開く。Samba は「smb」と表示され、この一覧で、オンになっているサーバが Linux とともに起動する。Samba サーバをここでオンにし、「保存」ボタンをクリックし、新しい設定を保存する。



(2) DHCP サーバの構築

DHCP サーバを構築することにより、LAN に接続したコンピュータ (Linux サーバに接続されているクライアント) は、DHCP サーバが設定されたアドレスプール内の IP アドレスを自動的に割り当てるこ

とができる。したがって、手作業でクライアントの IP アドレスや DNS、デフォルトゲートウェイ等を設定する必要がない。

DHCP サーバをインストールする

インストール CD 3 を CD-ROM ドライブにセットする。ウィンドウシステムは、CD-ROM がセットされるとデスクトップ上に CD-ROM のアイコンを配置し、これをダブルクリックするとその内容を見ることができる。

DHCP サーバのパッケージは、インストール CD 3 の Fedora フォルダに dhcp-3.0.1rc12-4.i386.rpm という名前で保存されている。そのパッケージを選択し、メニューバーで「ファイル」「アプリケーションから開く」「アプリケーション」と選択する。アプリケーションを選択するためのダイアログが開くので、「Install Packages」を選択し、「OK」をクリックする。これで、インストールの処理が始まる。システムの準備が完了したことを示すウィンドウが表示され、「続ける」をクリックする。

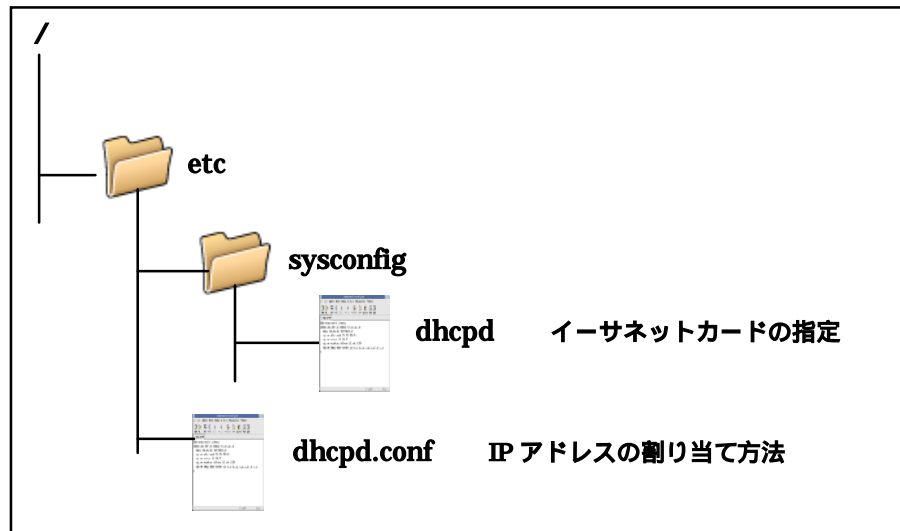
インストールが上手くいけば、何も表示されずに処理が終了する。CD-ROM アイコンを右クリックし、コンテキストメニューで「取り出し」を選択し CD 3 を取り出す。



設定ファイルの位置と役割を確認する

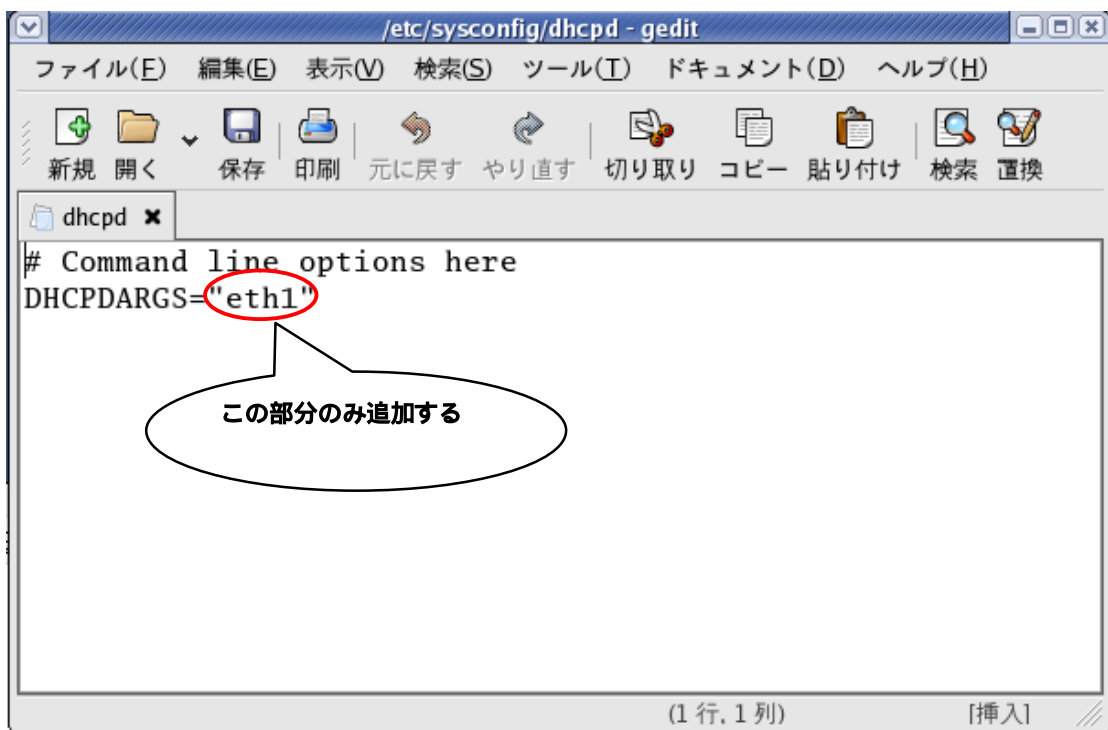
DHCP サーバを適切に動作させるためには、下に示す設定ファイルを編集または作成する必要があります。

る。dhcpd はサービスを提供する側のイーサネットカードを指定するもので、それを編集する必要がある。dhcpd.conf は IP アドレスの割り当て方法を決めるもので、新規に作成する必要がある。



dhcpd を編集する

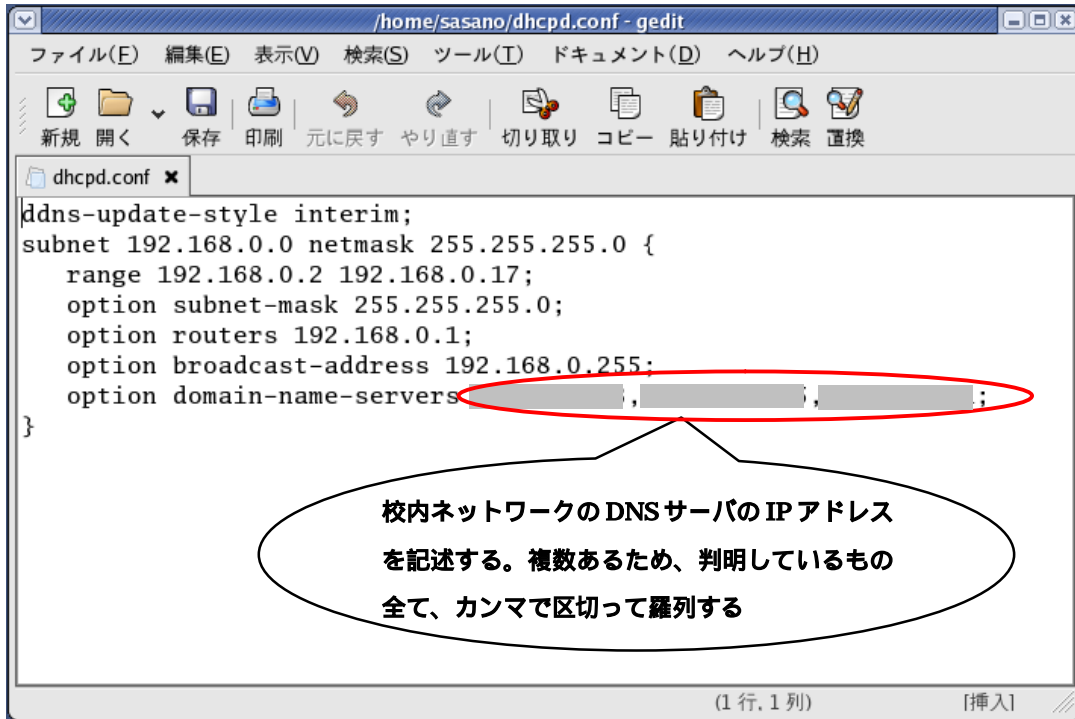
/etc/sysconfig ディレクトリの設定ファイル dhcpd には、DHCPDARGS という変数が記述されている。この変数は、サービスを提供する側のイーサネットカードを定義するものである。現在、DHCPDARGS には何も定義されていないため、サービスは初期値に従い全てのイーサネットカードに提供される。しかし、本来は LAN 側のイーサネットカード eth1 だけに提供されなければならないため、「DHCPDARGS="eth1"」となるように編集する。



dhcpd.conf を作成する

IP アドレスの割り当て方法は、dhcpd.conf に記述し、/etc ディレクトリに保存する。この設定ファ

イルは新規に作成を行なう。下に記述例を示す。

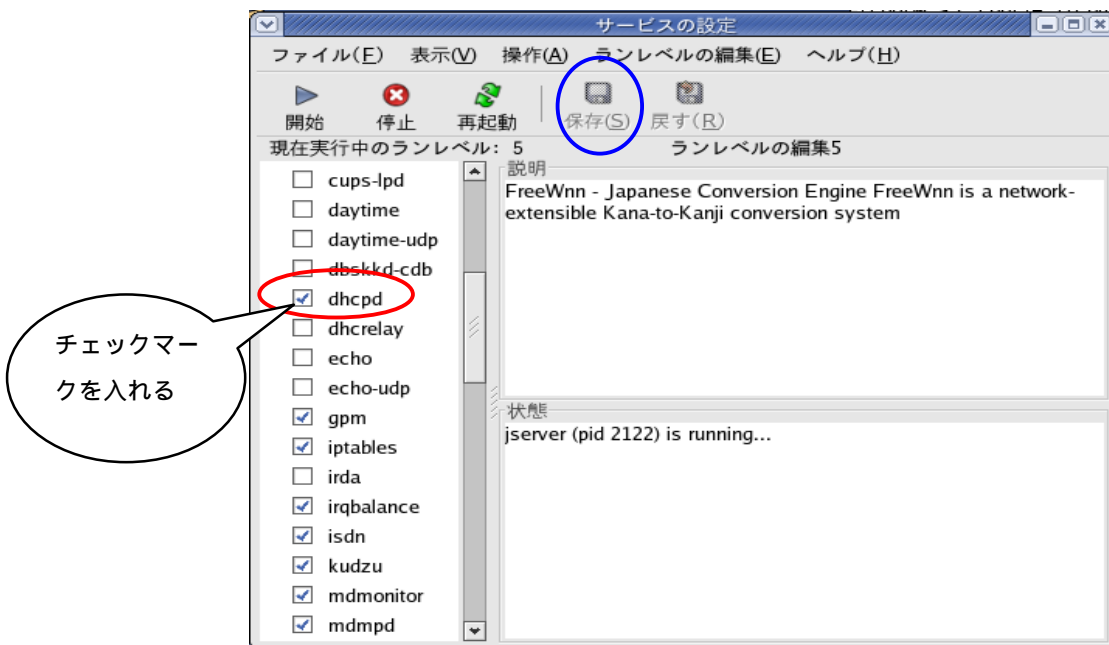


アドレスプールを 192.168.0.2~192.168.0.17 までの 16 個のプライベートアドレス

上記の dhcpd.conf を記述するのは、メインメニューの「アクセサリ」 「GNOME テキスト・エディタ」を開いて作成し、保存先を間違えないように注意する。

メインメニューで「サービス」を選択する

DHCP サーバが Linux とともに起動し、自動的にサービスを開始するよう設定する。操作については、メインメニューで「システム設定」 「サーバ設定」 「サービス」と選択する。

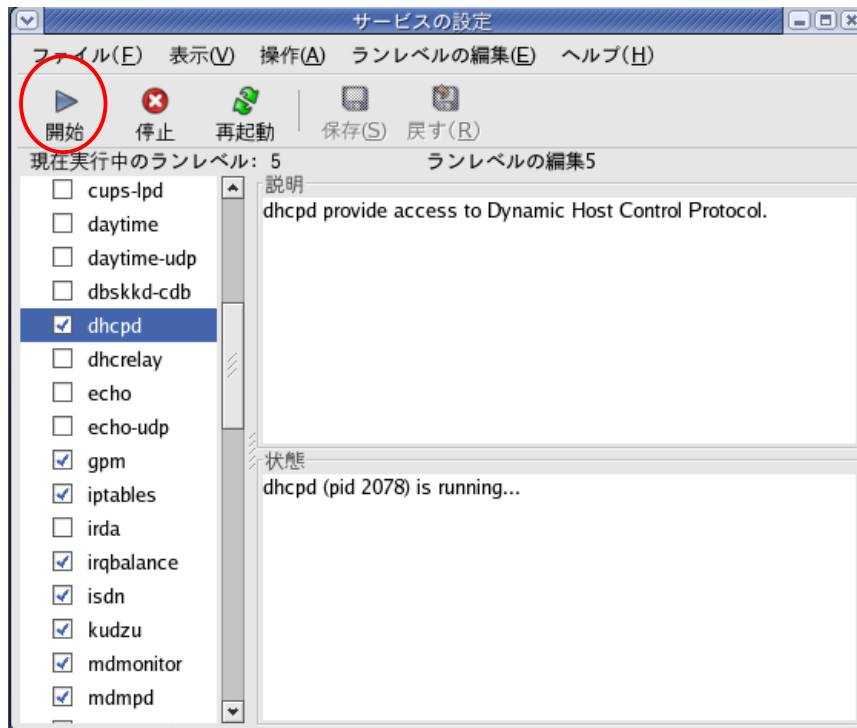


サービスの設定の一覧で、オン (チェックマークがついている) になっているサーバが Linux とともに起動する。DHCP サーバは「オフ」になっているため、ここでは「オン」にし、「保存ボタン」を

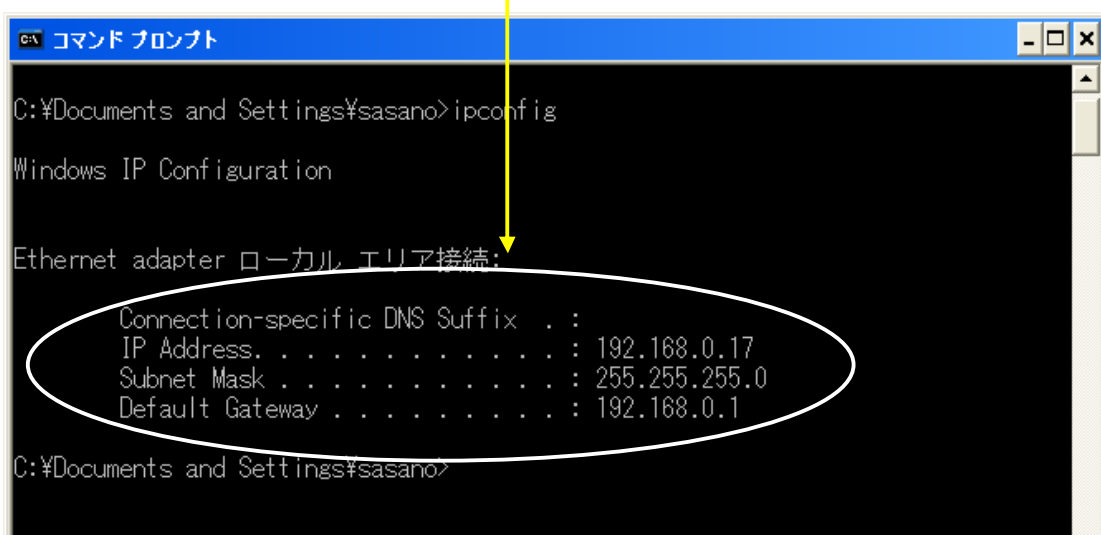
クリックし、新しい設定を保存する。これで、次に Linux を起動したとき DHCP サーバも起動し、自動的にサービスを開始する。

サービスを開始する

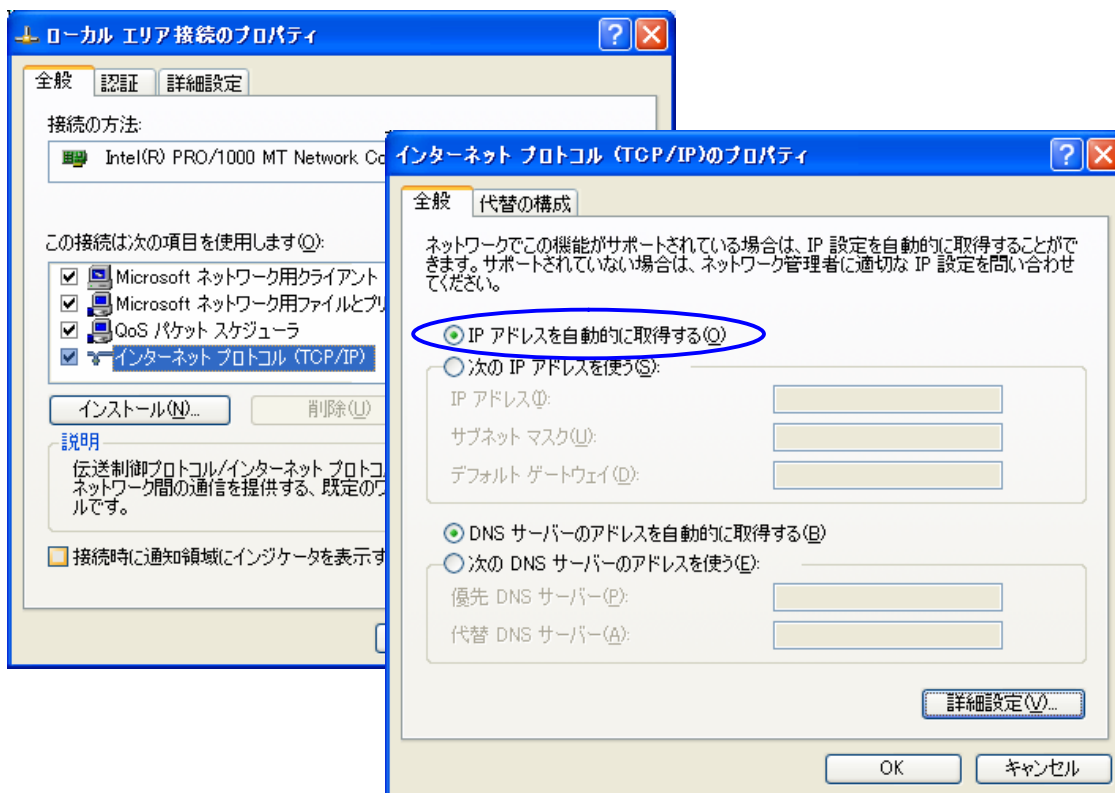
Linux サーバは、インストールしたあとわざわざ再起動しなくても起動することができる。DHCP サーバを起動するには、サーバの一覧で「dhcpd」を選択し、「開始」ボタンをクリックする。その後ダイアログが開き、起動に成功したことが通知されるので、「OK」ボタンをクリックする。



DHCP サーバが構築されれば、Linux サーバに接続されているクライアントは自動的に IP アドレスとサブネットマスク、デフォルトゲートウェイが設定される。



クライアントの設定については、マイネットワークのプロパティで設定を行なう。インターネットプロトコル (TCP/IP) のプロパティ画面の「全般」で、「IP アドレスを自動的に取得する」にしておけばよい。



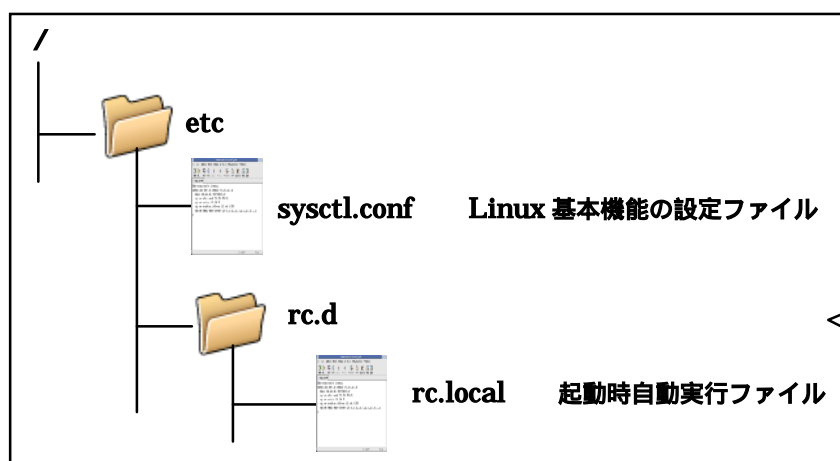
(3) IP マスカレードの設定

Linux サーバで IP マスカレードを行い、インターネットと LAN をつなくよう設定する。これで、LAN に接続した Linux サーバ以外のコンピュータでインターネットを利用できるようになる。

IP マスカレードを有効にする

IP マスカレードは「サービス」ではなく「処理」のため、設定ファイルはないが、Linux の設定ファイルともいべき一部のファイルの編集が必要になる。

Linux の初期値では、IP マスカレードの実行を禁止する設定になっている。IP マスカレードを実行するには、この設定を解除しなければならない。/etc ディレクトリにある `sysctl.conf` を以下に示すような変更を行なう。

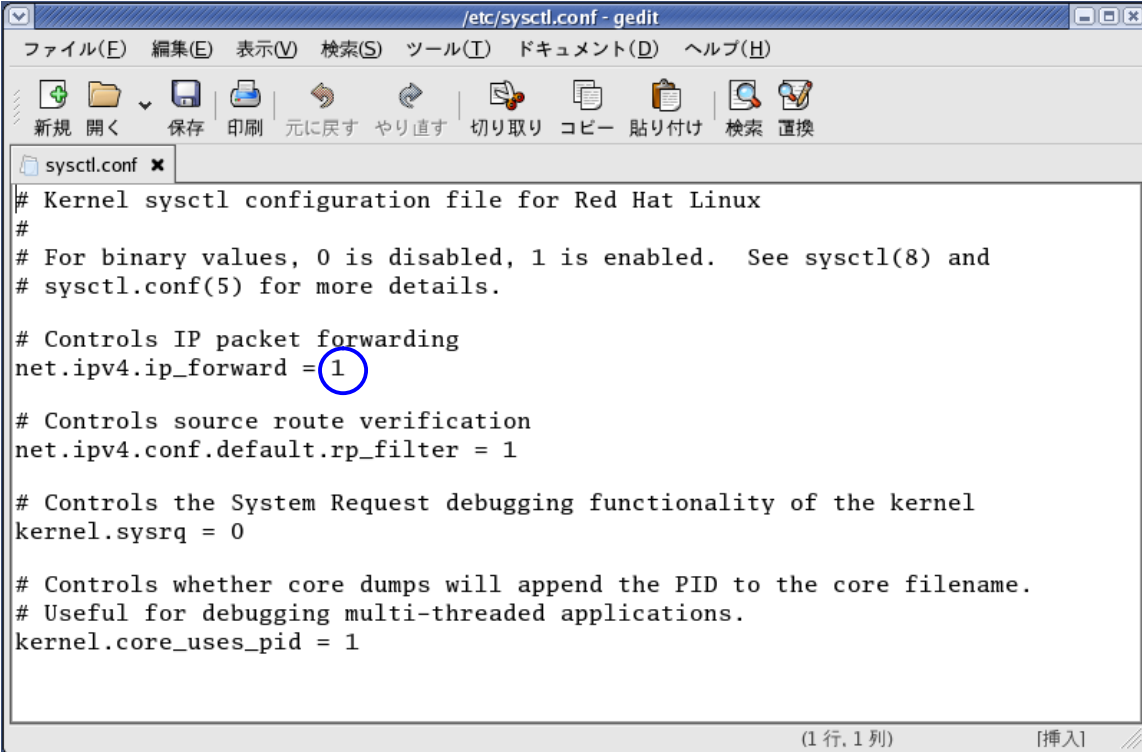


IP マスカレードを実行するために編集が必要となるファイル。いずれも Linux の設定ファイルに相当する。IP マスカレードそのものの設定ファイルはない。

`sysctl.conf` で IP マスカレードを有効にする

以下に `sysctl.conf` の編集例を示してしるが、青い で囲んでいる箇所 1 文字だけの書き替えになる。

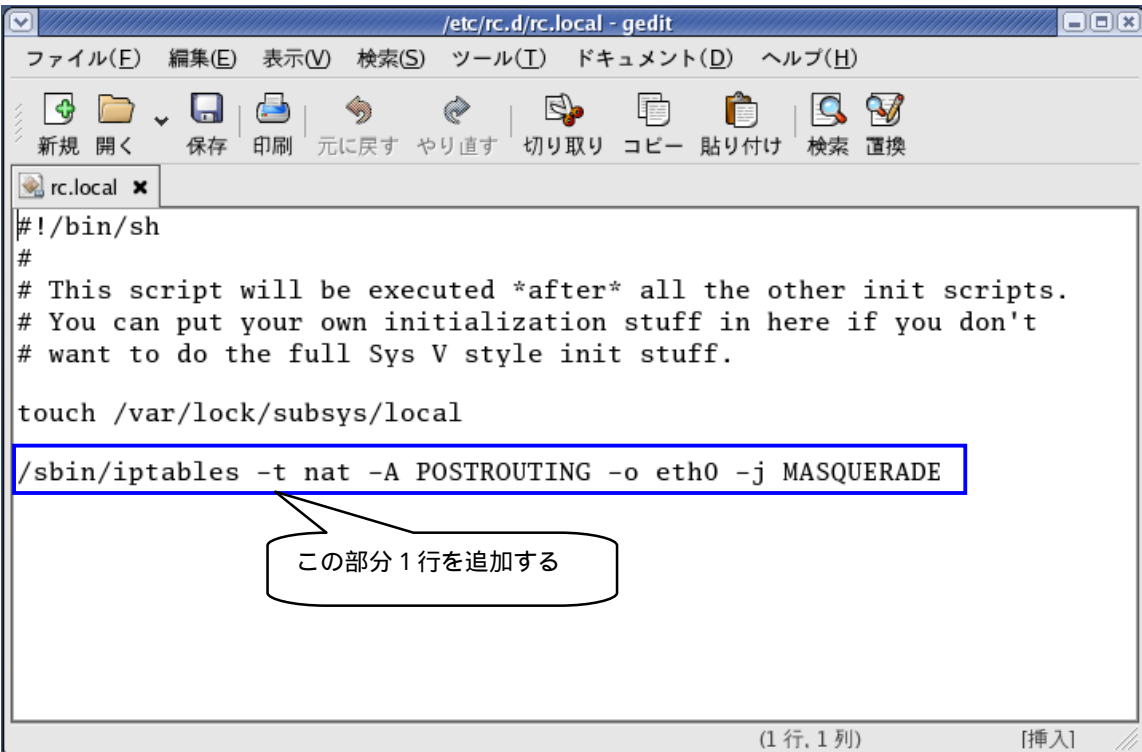
その他の記述はいっさい編集しない。これで IP マスカレードを実行できる設定に変更された。



```
etc/sysctl.conf - gedit
ファイル(E) 編集(E) 表示(V) 検索(S) ツール(T) ドキュメント(D) ヘルプ(H)
新規 開く 保存 印刷 元に戻す やり直す 切り取り コピー 貼り付け 検索 置換
sysctl.conf x
# Kernel sysctl configuration file for Red Hat Linux
#
# For binary values, 0 is disabled, 1 is enabled.  See sysctl(8) and
# sysctl.conf(5) for more details.
# Controls IP packet forwarding
net.ipv4.ip_forward = 1
# Controls source route verification
net.ipv4.conf.default.rp_filter = 1
# Controls the System Request debugging functionality of the kernel
kernel.sysrq = 0
# Controls whether core dumps will append the PID to the core filename.
# Useful for debugging multi-threaded applications.
kernel.core_uses_pid = 1
(1行, 1列) [挿入]
```

rc.local にコマンドを追加する

IP マスカレードは、iptables コマンドで実行する。また、そのコマンドは、/etc/rc.d ディレクトリにある rc.local に追加しておく。rc.local は Windows の「スタートアップ」フォルダに相当し、このファイルに記述したコマンドは Linux が起動した直後、自動的に実行される。



```
etc/rc.d/rc.local - gedit
ファイル(E) 編集(E) 表示(V) 検索(S) ツール(T) ドキュメント(D) ヘルプ(H)
新規 開く 保存 印刷 元に戻す やり直す 切り取り コピー 貼り付け 検索 置換
rc.local x
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.
touch /var/lock/subsys/local
/sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
(1行, 1列) [挿入]
```

(4) ファイアウォールの設定

ファイアウォールは Linux サーバを不正アクセスから守るが、正しいアクセスまで否定することがある。多くのサービスは、アクセスを許可する設定が必要となる。

セキュリティレベルの設定

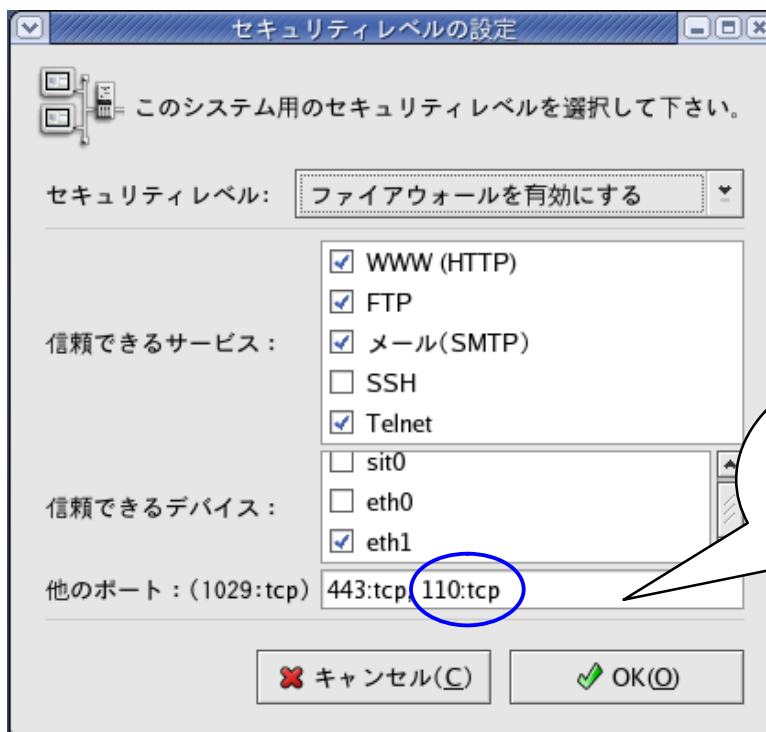
現在、ファイアウォールはほとんどのアクセスを拒否している。いわばクライアント向きの設定になっており、Linux サーバとしては不都合である。そこで、Linux サーバ向きに設定を行なう。

メインメニューで、「システム設定」、「セキュリティレベル」と選択する。

アクセス権の設定

ファイアウォールを設定するためのウィンドウで、学内ネットワーク側からはサービスごとにアクセスの許可・禁止を設定し、LAN 側は無条件にアクセスを許可する。その設定については下の表に示す。

項目	設定
セキュリティレベル	「ファイアウォールを有効にする」を選択
信頼できるサービス	実現するサービスにより設定する（下の表参照）
信頼できるデバイス	「eth1」をオンにする
他のポート	実現するサービスにより設定する（下の表参照）



「他のポート」欄に複数の記述が必要となる場合、カンマで区切って羅列する

設定を終えたら、「OK」ボタンをクリックし、これまでの設定に上書きするという警告が表示されるため、「はい」ボタンをクリックする。設定はこの時点から有効になる。

サービス	設定
DHCP	設定不要
プロキシ	設定不要 (LAN 側からのアクセスのみ許可)
Telnet	「信頼できるサービス」欄の「Telnet」をオン
VNC	設定不要 (LAN 側からのアクセスのみ許可)
FTP	「信頼できるサービス」欄の「FTP」をオン
sendmail	「信頼できるサービス」欄の「メール (SMTP)」をオン
POP3	「他ポート」欄に「110:tcp」と入力
ウェブ	「信頼できるサービス」欄の「WWW」をオン
Samba	設定不要 (LAN 側からのアクセスのみ許可)
Netatalk	設定不要 (LAN 側からのアクセスのみ許可)

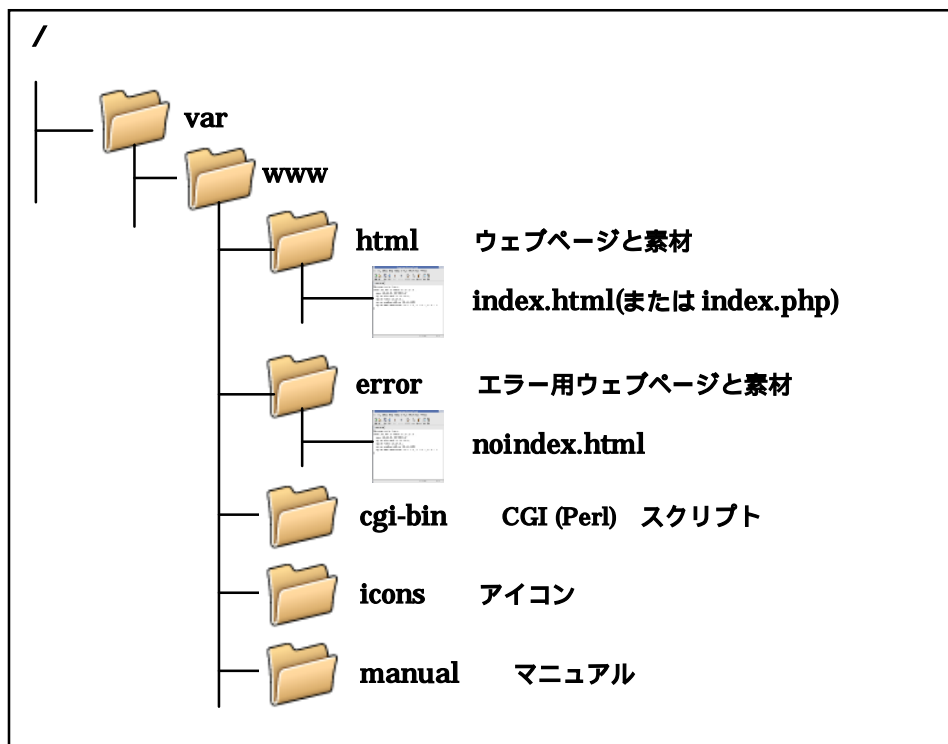
サーバ等で設定した箇所のみ設定を行なう

(5) ウェブサーバの構築

ウェブサーバの基本的な役割はウェブページの送付である。ウェブページは、あらかじめ作成し所定のディレクトリに保存しておく方法がある。Perl や PHP のスクリプトで状況にあわせて作成することもできる。

実ディレクトリの構成

ウェブページをはじめとするコンテンツは、/var/www ディレクトリの下の各ディレクトリに分類して保存する。各ディレクトリは、下に示す性質を持っている。これを踏まえ、適切に分類し保存を行なう。ファイル名には初期値があり、トップページから index.html、PHP スクリプトを含むトップページが index.php、エラーページが noindex.html である。これらは、URL を指定するときファイル名を省略することができる。また、Perl で記述した CGI スクリプトは拡張子を .pl としておくのが無難である。



仮想ディレクトリの構成

ウェブサーバは、実際のディレクトリを仮想ディレクトリに変換する。ブラウザで閲覧したり、ウェブページにリンクを設定する場合、実際のディレクトリではなく、仮想ディレクトリを使う。ウェブサーバの URL は仮想ディレクトリの / ディレクトリ、実際の /var/www/html ディレクトリにあたる。クライアントは仮想ディレクトリを使うため、どのように指定しても実際の /var/www ディレクトリより上に移動できない。

rpm コマンドの操作方法の確認

通常、インストールの作業にウィンドウシステムのユーティリティ Install Packages を使うが、パッケージがたくさんあれば操作が煩雑になる。そこで、ここでは能率的なテキストモードの rpm コマンドを使いパッケージのインストールを行なう。

ウェブサーバのインストール

ウェブサーバは、最低限 5 パッケージ、機能を欲張れば 20 パッケージの構成となるが、ここでは 10 パッケージを選択して適度な機能を実現する。

インストール CD 1 を CD-ROM ドライブにセットする。これ以降は、テキストモードで操作を行なう。テキストモードでは、CD-ROM を /mnt/cdrom ディレクトリで操作する。

```
[root@linux sasano]# cd /mnt/cdrom/Fedora/RPMS
[root@linux RPMS]# rpm -i apr-0.9.4-11.i386.rpm
[root@linux RPMS]# rpm -i apr-util-0.9.4-14.i386.rpm
[root@linux RPMS]# rpm -i distcache-1.4.5-2.i386.rpm
[root@linux RPMS]# rpm -i gd-2.0.21-3.i386.rpm
[root@linux RPMS]# rpm -i httpd-2.0.49-4.i386.rpm
[root@linux RPMS]# rpm -i mod_perl-1.99_12-2.1.i386.rpm
[root@linux RPMS]# rpm -i mod_ssl-2.0.49-4.i386.rpm
[root@linux RPMS]# rpm -i --nodeps php-4.3.4-11.i386.rpm
[root@linux RPMS]# rpm -i --nodeps php-pear-4.3.4-11.i386.rpm
-----
[root@linux RPMS]# cd
[root@linux sasano]#
```

途中「警告」が表示されるが、気にせず進める

【ディレクトリを移動し、パッケージをインストールする操作】

インストール CD 1 の取り出し

インストールを終えたら、「cd」と入力し、初期値のディレクトリに戻す。ディレクトリが CD-ROM に移動していると、CD を取り出すことができない。CD-ROM アイコンを右クリックし、コンテキストメニューで「取り出し」を選択する。または、テキストモードで、# umount /mnt/cdrom と入力し、CD を取り出す。

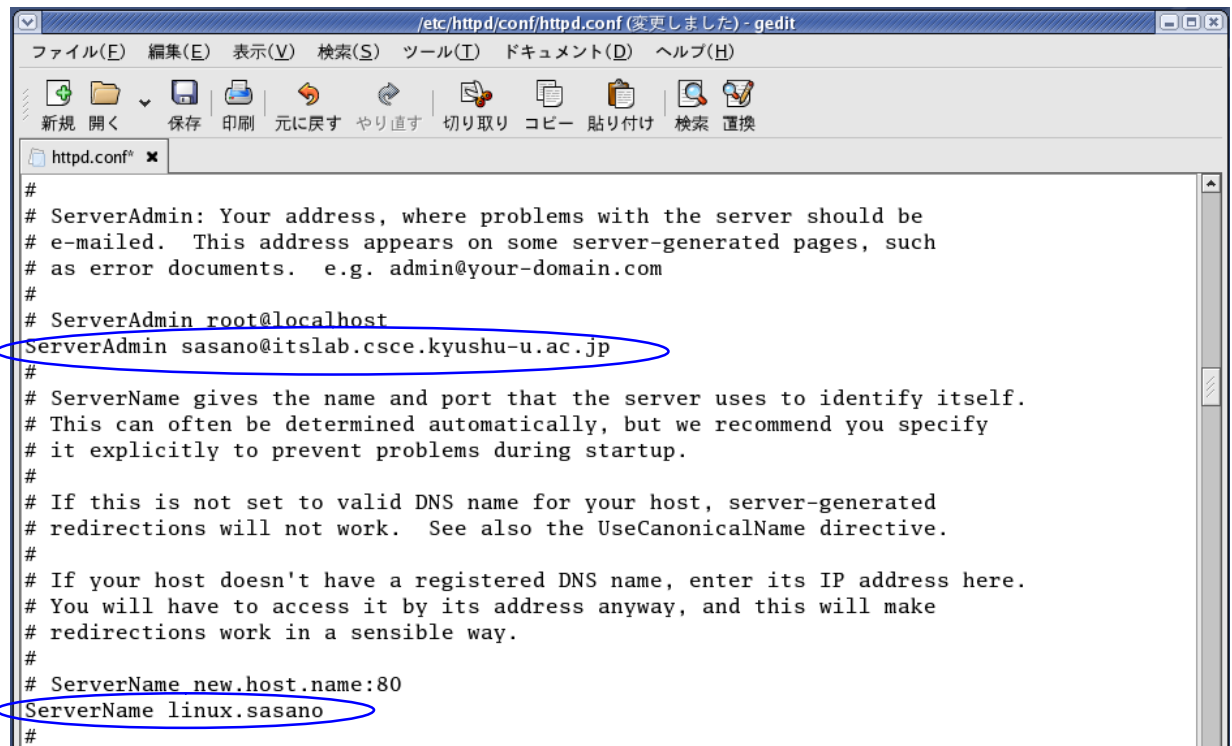
ウェブサーバの設定 1 (httpd.conf の編集)

ウェブサーバの設定ファイルを編集し、正しく動作させるとともに、関連機能を有効にする。この設定で、ウェブページの公開はもちろん、Perl や PHP のスクリプトが実行できる。

ウェブサーバの設定ファイルは、/etc/httpd ディレクトリの下の各ディレクトリに分類して保存され

ている。ウェブサーバの主要な機能は、/etc/httpd/conf ディレクトリの設定ファイル httpd.conf で設定する。この設定ファイルには多くの記述があるが、設定に必要となるのは次の二つだけである。

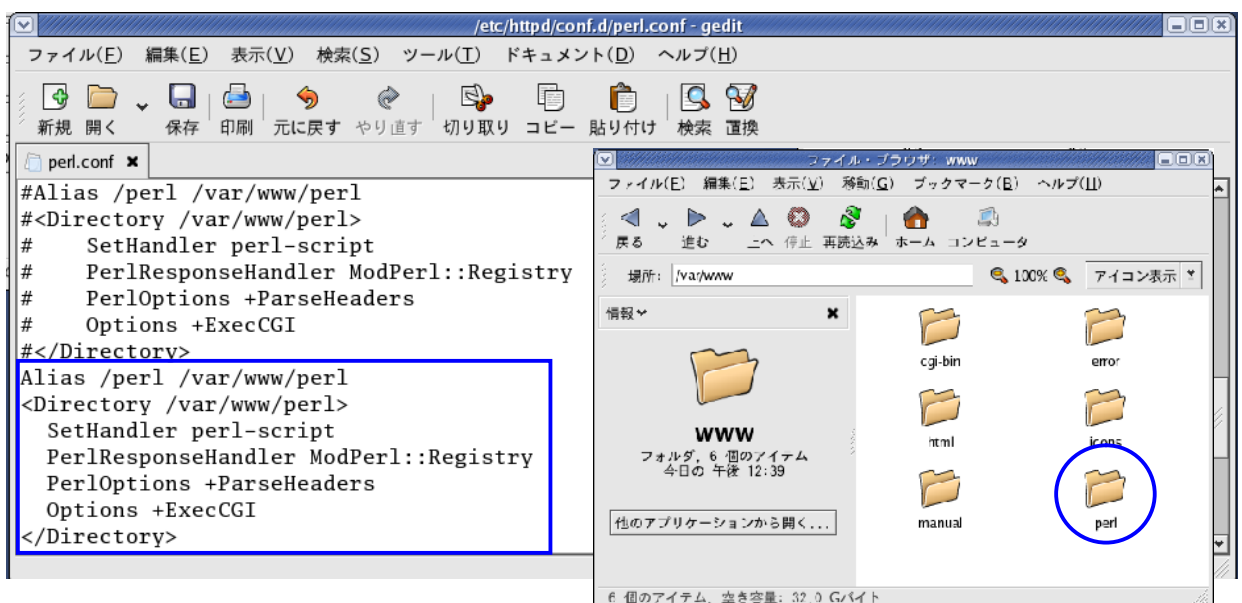
記述子 ServerAdmin には、ウェブサーバ管理者の電子メールアドレスを設定する。これは、エラーを通知する表示に埋め込まれる。記述子 ServerName は、サーバの完全修飾ドメイン名を設定する。



```
#
# ServerAdmin: Your address, where problems with the server should be
# e-mailed. This address appears on some server-generated pages, such
# as error documents. e.g. admin@your-domain.com
#
# ServerAdmin root@localhost
# ServerAdmin sasano@itslab.csce.kyushu-u.ac.jp
#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If this is not set to valid DNS name for your host, server-generated
# redirections will not work. See also the UseCanonicalName directive.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
# You will have to access it by its address anyway, and this will make
# redirections work in a sensible way.
#
# ServerName new.host.name:80
# ServerName linux.sasano
#
```

ウェブサーバの設定 2 (perl.conf の編集)

/etc/httpd/conf.d ディレクトリには、ウェブサーバの関連機能の設定ファイルがある。これらのほとんどはそのまま使えるが、Perl の設定ファイル perl.conf だけは、安全性を確保するため実行しない設定になっているため編集が必要である。下に示す記述を追加し、実行させる。



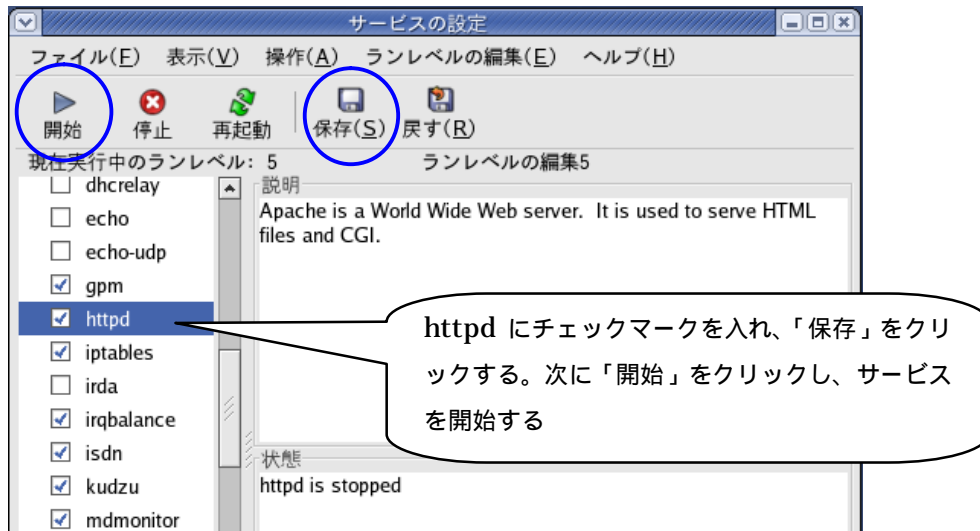
```
#Alias /perl /var/www/perl
#<Directory /var/www/perl>
#   SetHandler perl-script
#   PerlResponseHandler ModPerl::Registry
#   PerlOptions +ParseHeaders
#   Options +ExecCGI
#</Directory>
Alias /perl /var/www/perl
<Directory /var/www/perl>
  SetHandler perl-script
  PerlResponseHandler ModPerl::Registry
  PerlOptions +ParseHeaders
  Options +ExecCGI
</Directory>
```

追加した記述は、/var/www/perl ディレクトリに保存する。ただし、このディレクトリは存在しないため、作成する必要がある。

ウェブサーバの起動

ウェブサーバを起動し、サービスを開始する。これでウェブサーバは所定のディレクトリを公開する。ただし、まだそこにコンテンツを作っていないため、ブラウザで接続しても意味のある内容は表示されない。この時点では、エラーページが表示される。

メインメニューで「システム設定」「サーバ設定」「サービス」を選択する。



(6) Telnet サーバの構築

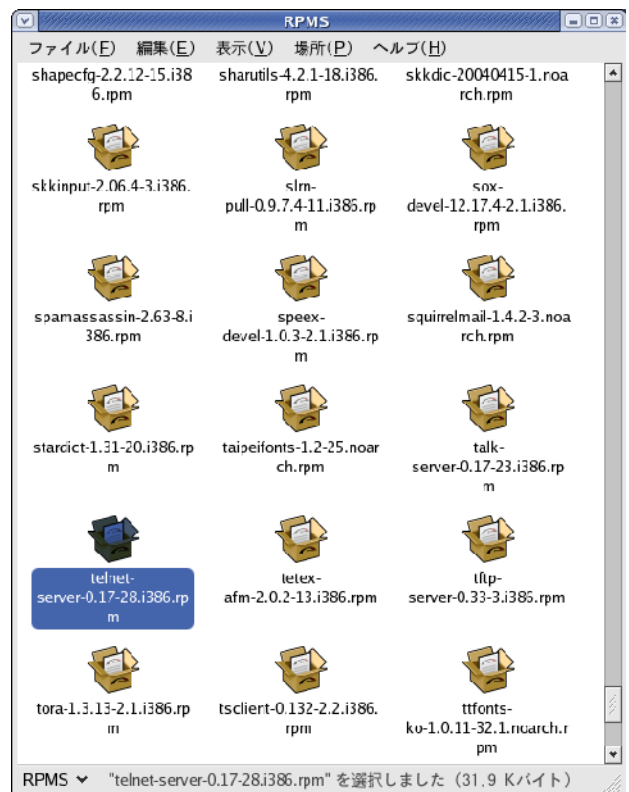
Telnet サーバは、クライアントにテキストモードでの操作を認める。クライアントは、通常 telnet コマンドで接続し、接続したあとの操作は直接の操作と同じとなる。ただし、「root」のユーザ名ではログインできない。

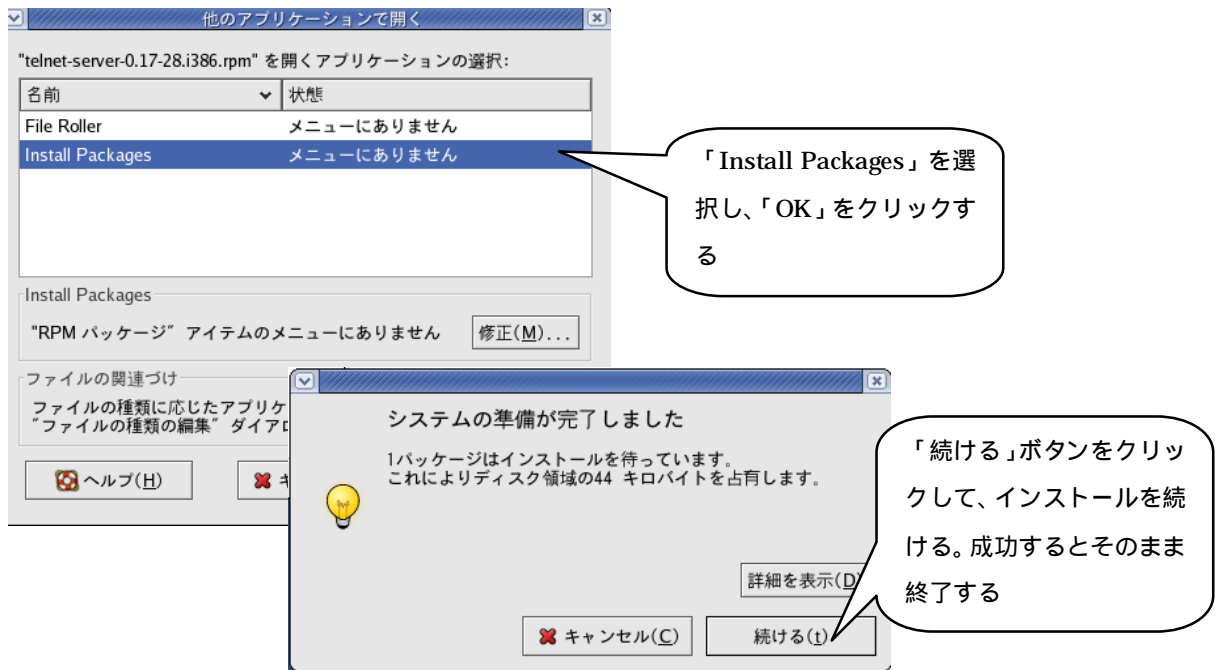
Telnet サーバのインストール

インストール CD 3 を CD-ROM ドライブにセットし、デスクトップに CD-ROM アイコンを配置する。そのアイコンをダブルクリックするとウィンドウが開き内容が表示される。

Telnet サーバのパッケージは、インストール CD 3 の Fedora フォルダの RPMS のフォルダに、teinet-server-0.17-28.i386.rpm という名前で作保存されている。

メニューバーで「ファイル」「アプリケーションから開く」「アプリケーション」と選択する。アプリケーションを選択するためのダイアログが開くので、「Install Packages」を選択して「OK」ボタンをクリックする。これで、インストールの処理が始まる。



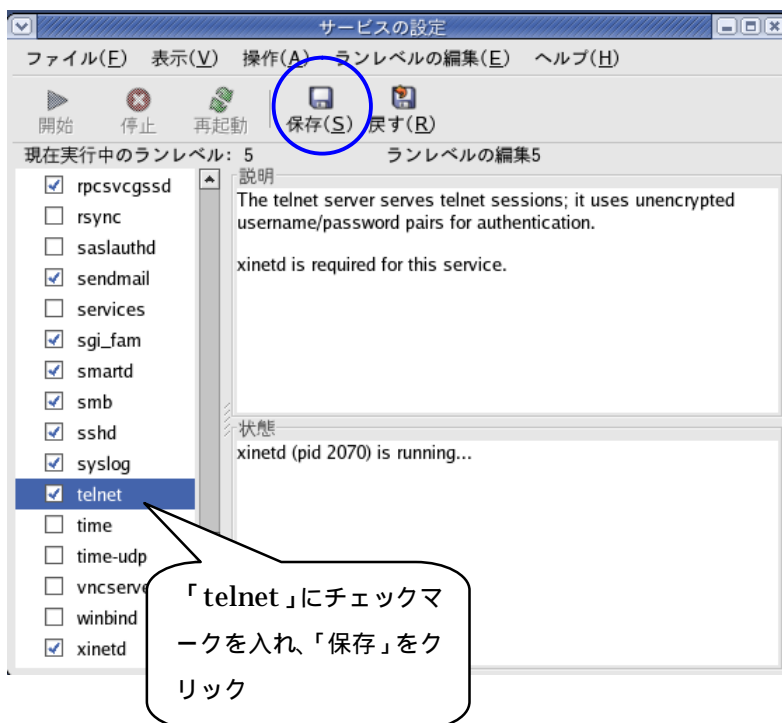


インストールが終了したら、CD-ROM アイコンを右クリックし、コンテキストメニューで「取り出し」を選択して、インストール CD3 を取り出す。

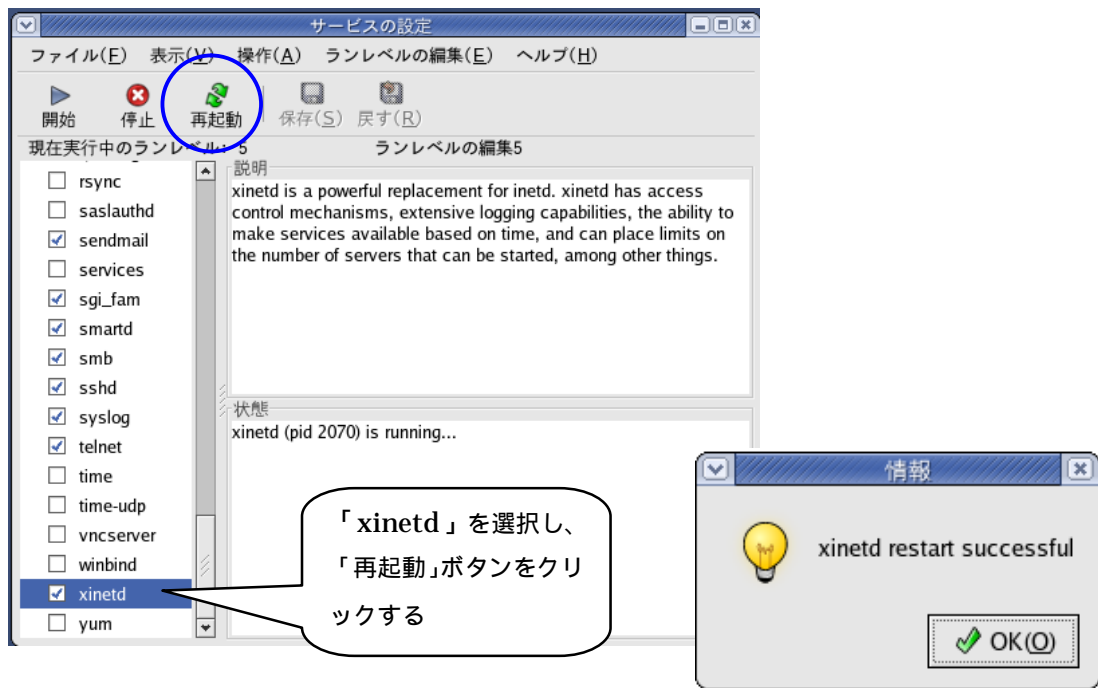
Telnet サーバの起動

Telnet サーバは、現在スーパーサーバの管理下におかれているが、まだその存在が認識されていない。そこで、スーパーサーバを再起動し、Telnet サーバの存在を認識させる。その結果、Telnet サーバが起動し、Telnet クライアントに対するサービスが開始される。

メインメニューで「システム設定」「サーバ設定」「サービス」と選択する。



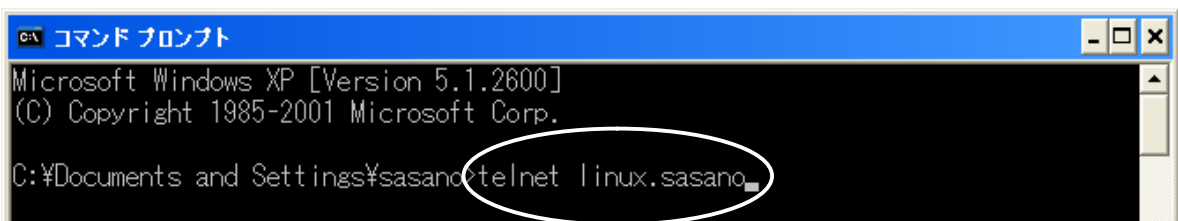
telnet をオンにして保存をクリックし、新しい設定を保存する。これで次に Linux を起動したとき Telnet サーバも起動し、自動的にサービスを開始する。しかし、この時点ではまだ起動しない。



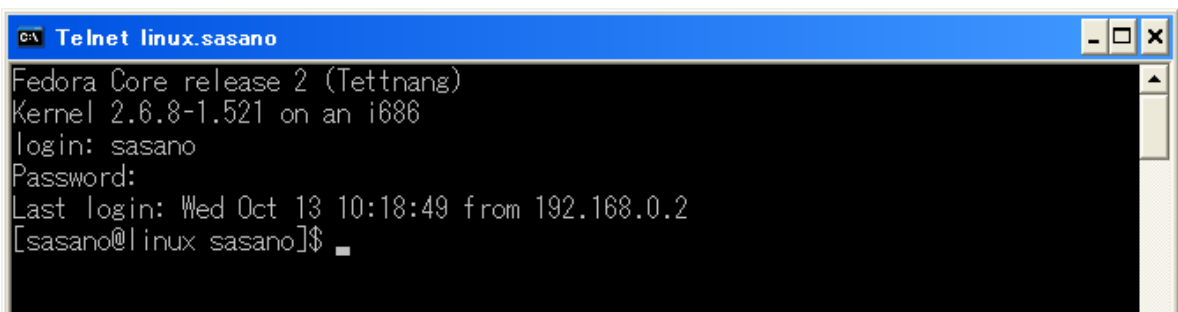
Telnet サーバは、スーパーサーバ xinetd の管理下にあるため、スーパーサーバを再起動しなければならない。サーバの一覧で「xinetd」を選択し、「再起動」ボタンをクリックする。数秒してダイアログが開き、再起動に成功したことを通知するので、「OK」ボタンをクリックして閉じる。これで Telnet サーバが起動し、サービスを開始したことになる。

Telnet コマンドでの接続

Telnet サーバへの接続には、通常テキストモードの telnet コマンドを使う。WindowsXP であれば「コマンドプロンプト」、WindowsMe であれば「MS-DOS プロンプト」を使う。

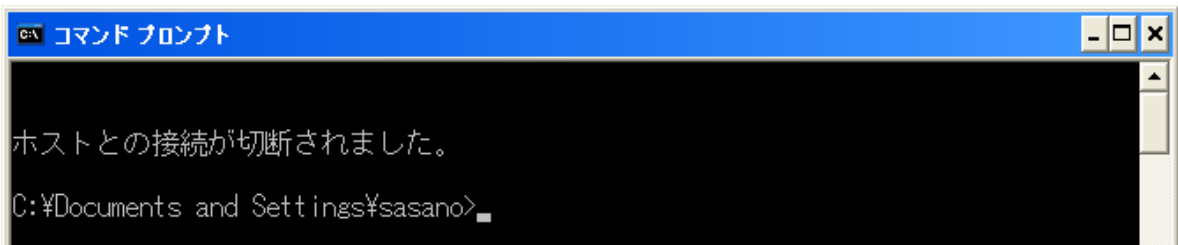


【WindowsXP から接続】

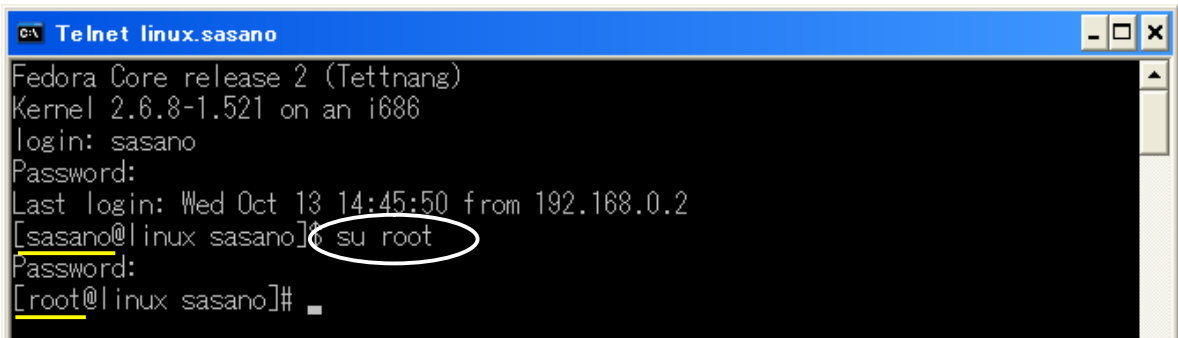


【一般ユーザのアカウントでのみログインできる】

正常に接続すると、Telnet サーバがログインの手続きを求める。安全性を確保するため、一般ユーザのアカウントでのみログインできるようになっている。一般ユーザのユーザ名を入力し、パスワードを入力する。以降、テキストモードでの操作が認められる。ログインからあとの操作は、直接操作するのとほぼ同じで、作業を終えたら「exit」と入力してログアウトする。



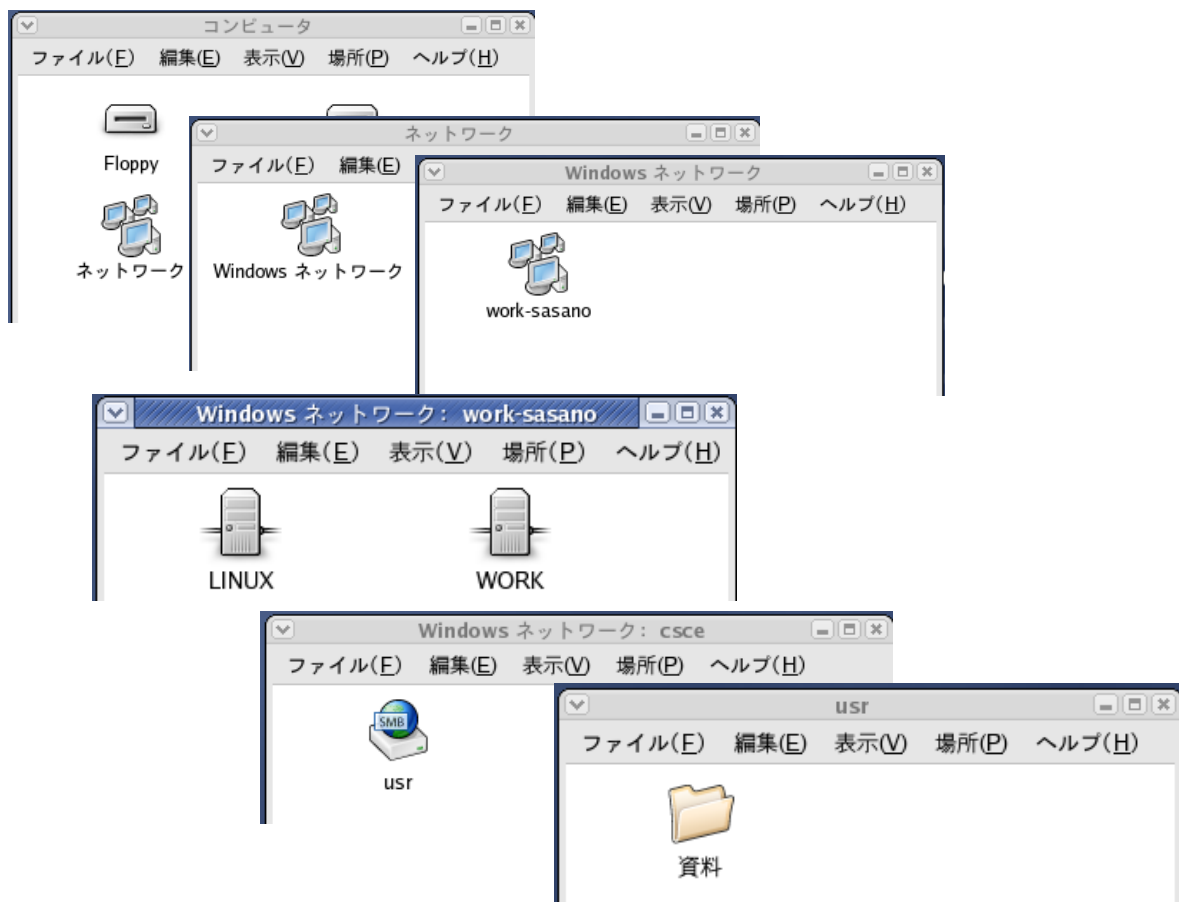
Telnet サーバは、よくクライアントからメンテナンスをするために使われる。この作業には root (管理者) の権限が必要であるが、「root」のユーザ名ではログインできない。そこで、一般ユーザのアカウントでログインしたあと、su コマンドで root の権限を取得する。



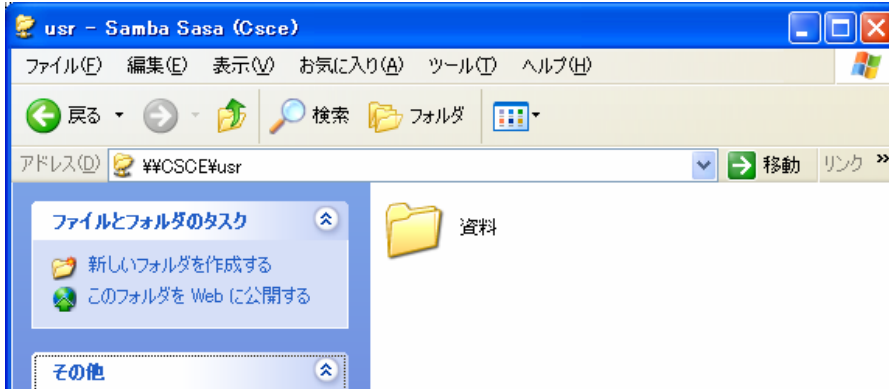
5 Windows 形式のネットワークの確認

Samba サーバ/クライアントをインストールし、Windows 形式のネットワークの構築を行なった。Linux サーバと Windows が、あたかも Windows 同士のネットワークのように接続し、ファイル等を共有している状況を確認する。

(1) Linux サーバからのネットワーク



(2) クライアント (Windows) からのネットワーク



「資料」のフォルダを共有できていることがわかる

6 ウィンドウシステムとテキストモード

Linux は現在、優秀なウィンドウシステムが登場したおかげで Windows のように操作できるようになった。とりわけ、Fedora Core 2 のウィンドウシステム GNOME は、Windows の長所を積極的に取り入れており、コンピュータを Windows で覚えたユーザに好評を博している。

そのウィンドウシステムを使わない本来の Linux は、DOS のように文字だけの画面になる。この環境をテキストモードと呼ぶ。テキストモードではコマンドを使って操作することになり、マウスによる直感的な操作ができないが、かえって能率的なこともある。例えば、拡張子 tmp のファイルをすべて削除する場合、ウィンドウシステムであれば該当するアイコンを一つずつゴミ箱へドラッグしたり、Delete キーを押して削除するが、テキストモードであれば「rm*.tmp」と入力するだけである。また、経験を積むことにより様々な技法を身に付けることができる。テキストモードで複雑な操作を一瞬のうちにこなすことが、年季を積んだユーザの誇りであると思われる。

ウィンドウシステムでテキストモードの操作をする際、メインメニューで「システムツール」「GNOME 端末」を選択し、ターミナルを起動する。このターミナルが仮想的なテキストモードとなる。そこで、Linux をテキストモードで使いたい場合は、テキストログインに変更することができる。/etc ディレクトリにある設定ファイル inittab を編集し、最初の有効行 (行頭に # がついていない行) の「5」を「3」に書き換えることにより本来のテキストモードに変えることができる。また、これをもとどおり書き換えればグラフィカルログインに戻る。

純粋なテキストモードでも、「startx」と入力するとウィンドウシステムが起動する。また、ウィンドウシステムをログアウトするとテキストモードに戻る。こうして、双方の環境を使い分けることができる。

```
# Default runlevel. The runlevels used by RHS are:
# 0 - halt (Do NOT set initdefault to this)
# 1 - Single user mode
# 2 - Multiuser, without NFS (The same as 3, if you do not have
networking)
# 3 - Full multiuser mode
# 4 - unused
# 5 - X11
# 6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:
```

7 自動更新機能の設定

Fedora Core2 でインストールした Linux は、レッドハットが運営するレッドハットネットワークから、無料で自動更新のサービスを受けることができる。デスクトップ右下にある青いアップデートボタンは、新しいパッケージが完成すると赤に変わって通知し、以降、マウス操作だけでダウンロードから更新まで一連の処理を実行する。Windows や Mac OS にも同様のサービスがあるが、Linux はオペレーティングシステムだけでなく、Fedora Core2 に収録されたすべてのプログラムが対象となる。

(1) 自動更新の設定

はじめに自動更新の方式など関連の設定を行う。基本的に初回だけの作業になるが、設定を更新したいとき、同様に作業を行う。この時点で更新可能なパッケージがあると、そのまま自動更新に進むため、Linux サーバが完成する前に行なわないよう注意する必要がある。

自動更新の設定をはじめる

自動更新を正しく動作させるには、あらかじめ自動更新の方式など関連の設定を行っておく必要がある。メインメニューで「システム設定」「RedHat Network」と選択する。

はじめに、自動更新の方式を設定する。すべて適切な初期値が設定されているので、そのまま「OK」ボタンをクリックする。

RPM-GPG-KEY をインストールする

RPM-GPG-KEY がインストールされていないことが通知され、これをインストールするかどうか尋ねられる。RPM-GPG-KEY は、インターネット経由で入手したパッケージが偽物でないことを検証するために使われる。「はい」ボタンをクリックし、インストールを行なう。




この時点で、更新可能なパッケージがなければ、作業はそのまま終了する。更新可能なパッケージがあれば、自動更新へ進む。

(2) 自動更新の操作

Linux と関連のプログラムは、随時頻繁に改良されている。この情報はアップデートボタンに表示され、アップデートボタンから更新することができる。

アップデートボタンをクリックする

自動更新機能は、定期的にレッドハットネットワークに接続し、現在インストールしているパッケージより新しいパッケージが存在しないか調査する。その結果は、アップデートボタンの表示に反映され、ボタンが赤なら、新しいパッケージが存在する。マウスでポイントすると、チップヘルプが開き、その数を表示する。通知された情報をより詳細に表示したり、新しいパッケージで自動更新するには、まずアップデートボタンをクリックする。

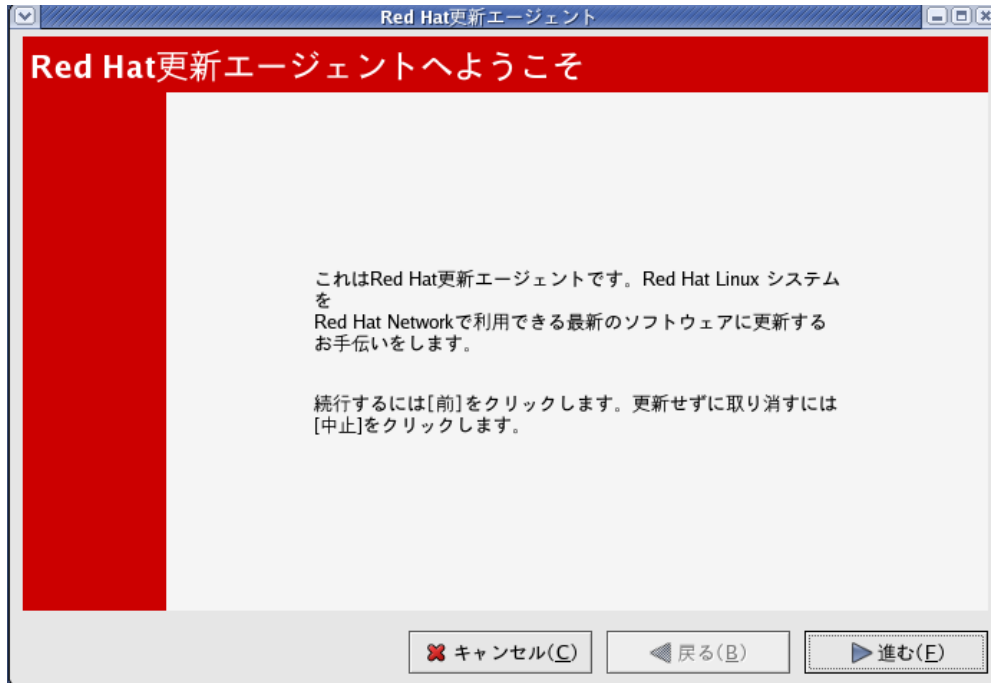
形状(色)	自動更新機能の状態
緑 	新しいパッケージが存在するかどうか調査中
青 	新しいパッケージは存在しない(最新の状態)
赤 	新しいパッケージが存在する
黄	何らかの問題が生じ、自動更新機能が働かない

【アップデートボタンの状態】

「up2date の起動」をクリックする

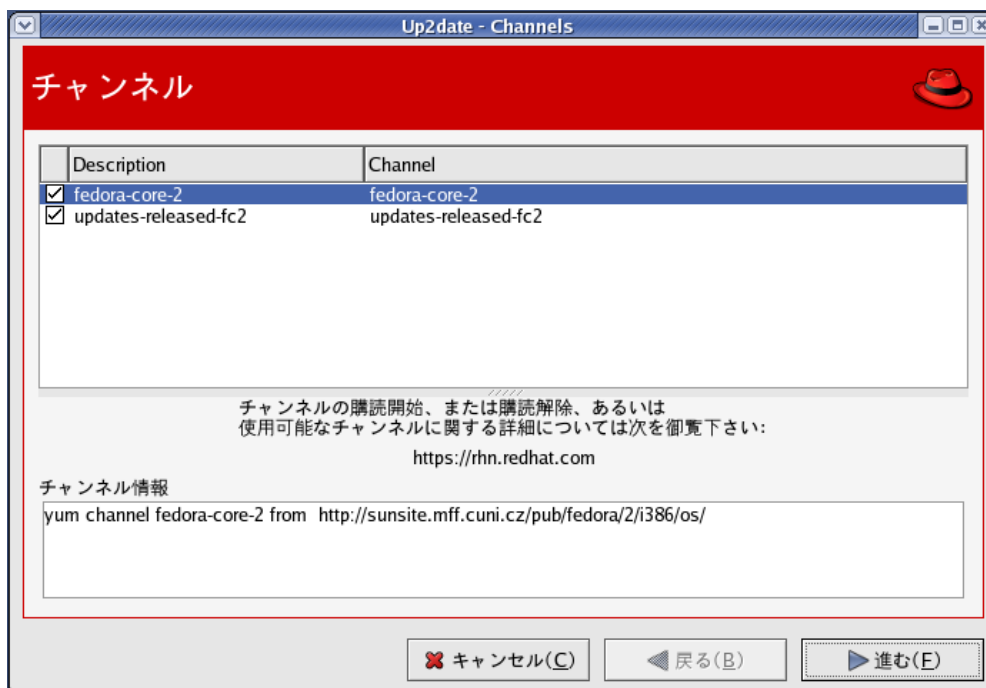
自動更新のためのウィンドウが開き、「利用可能な更新」タブ（初期値）に新しいパッケージの一覧を表示する。自動更新する場合は、「up2date の起動」ボタンをクリックする。そうすると、自動更新のためのウィザードが起動する。

最初の画面では、その確認と簡単な操作の紹介で、そのまま「進む」ボタンをクリックする。



チャンネルを選択

チャンネル（新しいパッケージの配布元）を選択する。「fedora-core-2」と「updates-released-fc2」をオンにして「進む」ボタンをクリックする。このあと新しいパッケージが検索される。

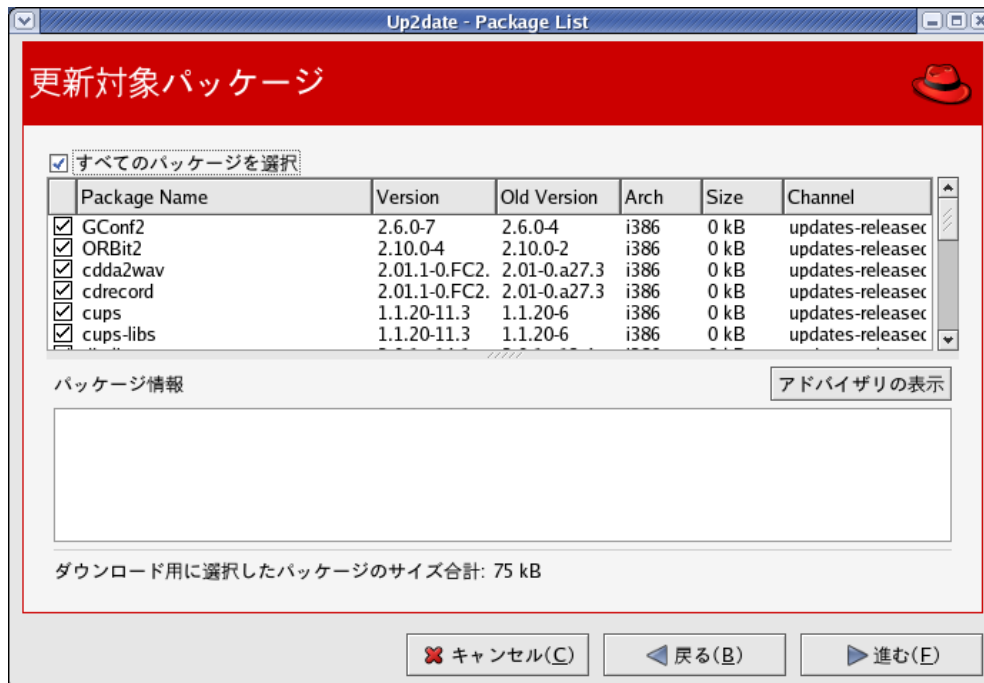


カーネルの取り扱いを決める

自動更新の設定で「除外するパッケージ」に指定されたパッケージが見つかったら、更新するかどうか判断を求められる。初期値の設定では、唯一、Linuxのカーネル(中核部分)がその対象となっている。

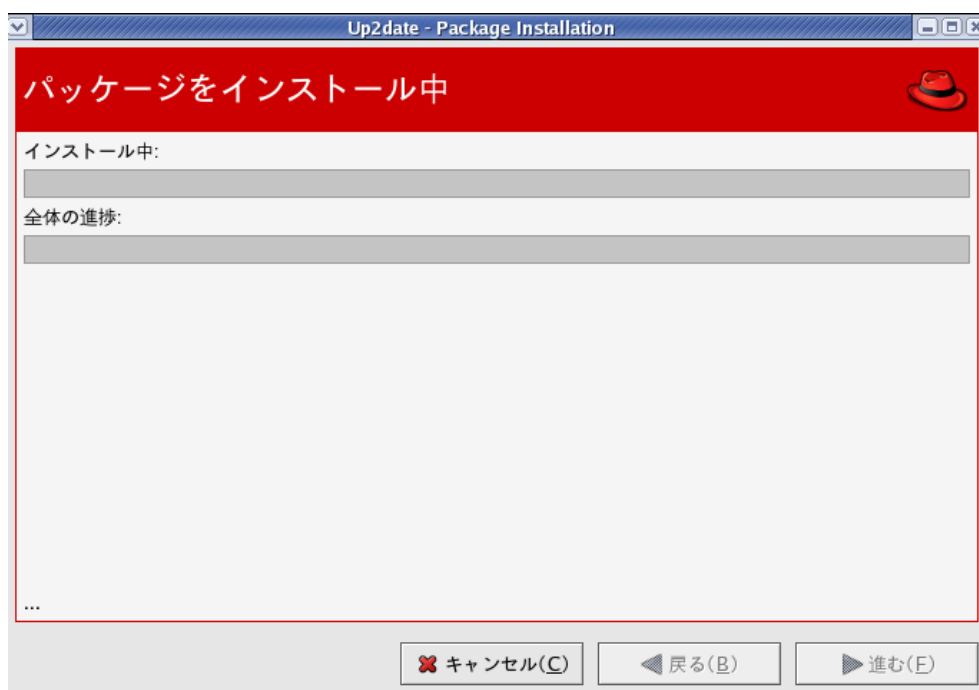
更新するパッケージを選択する

新しいパッケージが一覧に表示される。ここで、更新するパッケージを選択する。個別に選択するか、「すべてのパッケージを選択」をオンにしてすべて選択し、「進む」ボタンをクリックする。



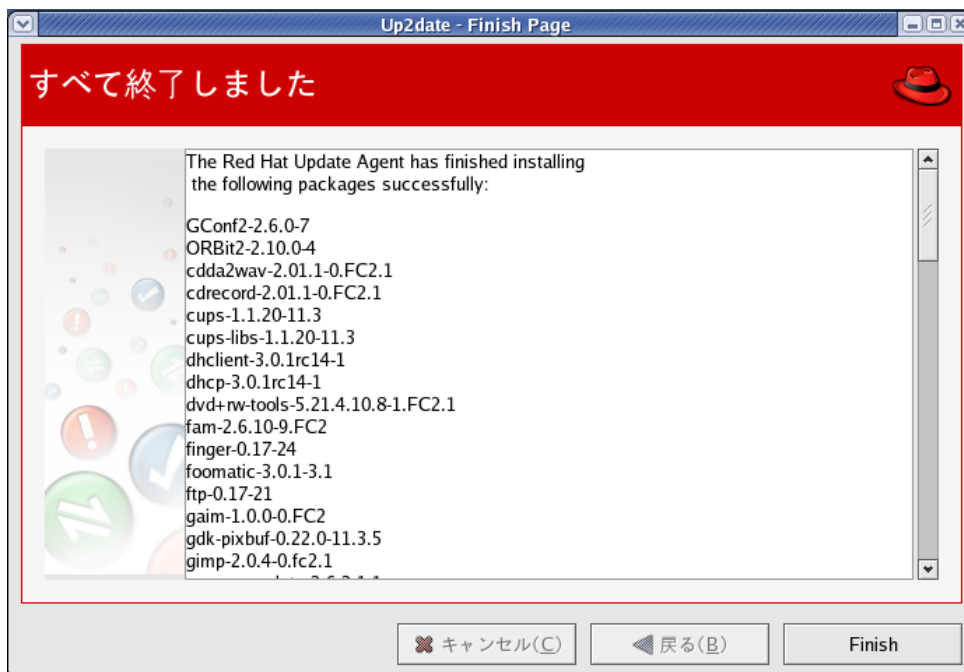
パッケージを更新する

レッドハットネットワークから、パッケージをダウンロードする。ダウンロードした新しいパッケージで、現在の古いパッケージを更新する。



ウィザードを終了する

更新されたパッケージを表示し、作業をすべて終了したことが通知される。「Finish」ボタンをクリックし、ウィザードを終了する。



(3) Linux カーネルの選択

自動更新機能により Linux のカーネルを更新したが、旧カーネルが残っている状態である。そこで、旧カーネルを残したまま新カーネルをテストし、その結果によりどちらかに決定する。

GRUB によるカーネルの選択

自動更新機能により Linux のカーネルを更新（正確に言えば追加）すれば旧カーネルが残る。この新旧二つのカーネルがある状態で Linux サーバを起動すると、GRUB が両方のカーネルを表示し、どちらで起動するか選択を求める。「」キーまたは「」キーで選択し、「Enter」キーで確定する。新カーネルは、試験的な運用期間が必要である。旧カーネルは、新カーネルの正常な動作を確認してからアンインストールするべきである。

rpm コマンドの概要

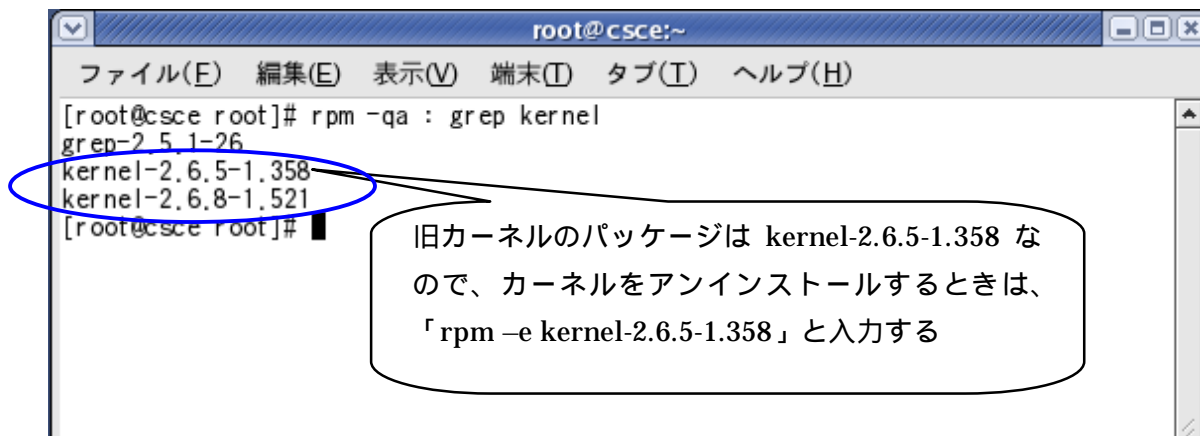
新カーネルが正しく動作することを確認できたら、必要に応じ、旧カーネルをアンインストールする。

まず、新カーネルで起動し、root（管理者）としてログインする。カーネルのパッケージは、ウィンドウシステムの設定ツールでは操作することができない。どのパッケージでも取り扱える、テキストモードの rpm コマンドを使う。

操 作	処 理
rpm -qa	インストール済みの全パッケージ名を表示
rpm -qa : grep <i>name</i>	上記のうち <i>name</i> を含むパッケージ名を表示
rpm -qi <i>package</i>	<i>package</i> の情報を表示
rpm --test -e <i>package</i>	<i>package</i> をアンインストールできるか確認
rpm -e <i>package</i>	<i>package</i> をアンインストール

旧カーネルのアンインストール

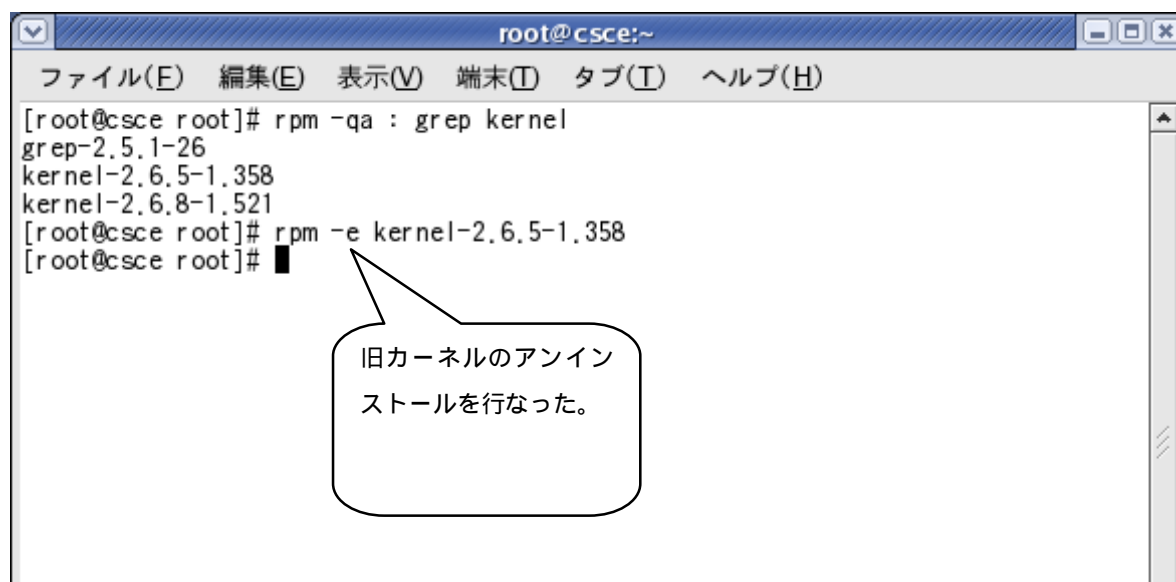
旧カーネルをアンインストールするには、そのパッケージ名を正確に知る必要がある。「rpm -qa : grep kernel」と入力し、インストールされているすべてのカーネルのパッケージ名を表示して確認を行なう。パッケージ名は、パッケージファイル名の末尾に付く「.i386.rpm」や「.noarch.rpm」を除いた名前である。



```
root@csce:~  
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(T) ヘルプ(H)  
[root@csce root]# rpm -qa : grep kernel  
grep-2.5.1-26  
kernel-2.6.5-1.358  
kernel-2.6.8-1.521  
[root@csce root]#
```

旧カーネルのパッケージは kernel-2.6.5-1.358 なので、カーネルをアンインストールするときは、「rpm -e kernel-2.6.5-1.358」と入力する

【インストールされているカーネルのパッケージ名をすべて表示】



```
root@csce:~  
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(T) ヘルプ(H)  
[root@csce root]# rpm -qa : grep kernel  
grep-2.5.1-26  
kernel-2.6.5-1.358  
kernel-2.6.8-1.521  
[root@csce root]# rpm -e kernel-2.6.5-1.358  
[root@csce root]#
```

旧カーネルのアンインストールを行なった。

【インストールされている旧カーネルのアンインストール】

アップデートボタンを確認し、新しいカーネルやパッケージがあれば適宜アップデートを行い、旧カーネルをアンインストールしなければならない。

8 その他の設定

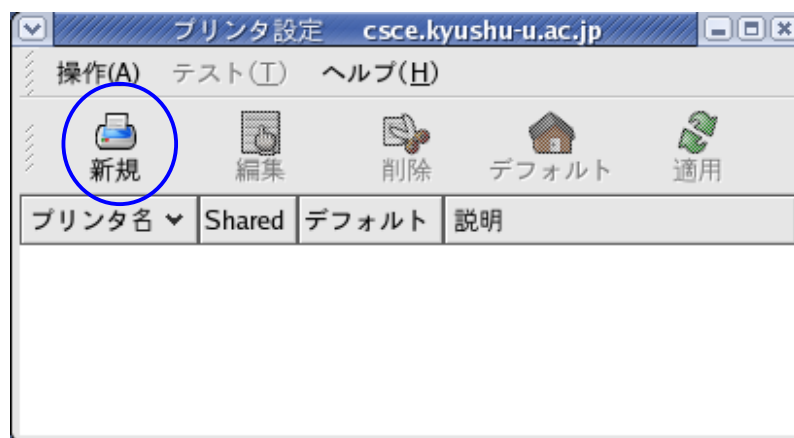
(1) プリンタの設定

プリンタの設定は、インストーラやセットアップエージェントが設定しないため、各自でこの設定を行なわなければならない。

プリンタを設定する

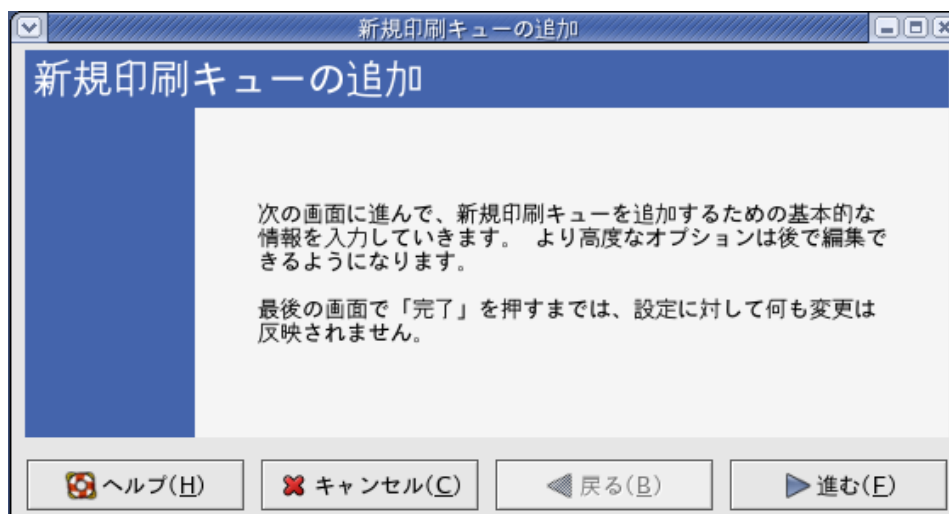
CUPS という印刷機能を設定し、プリンタの能力を最大限引き出す。メインメニューで「システム設

定」「印刷」を選択する。ここでは、設定済みのプリンタの一覧が開くが、何も設定していないため空欄となる。ここで「新規」ボタンをクリックすると、ウィザードが起動する。



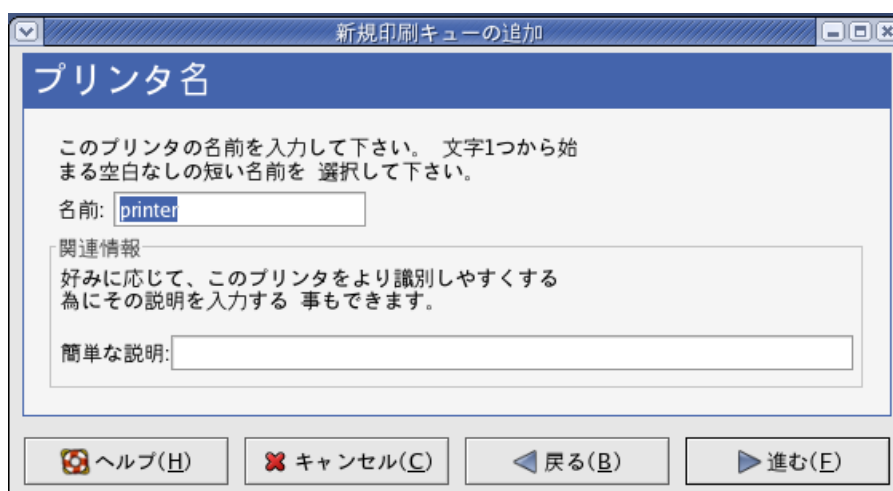
新規印刷キューの追加

最初の画面は確認を兼ねた一種の挨拶で、設定するところがないため、そのまま「進む」をクリックする。



プリンタ名

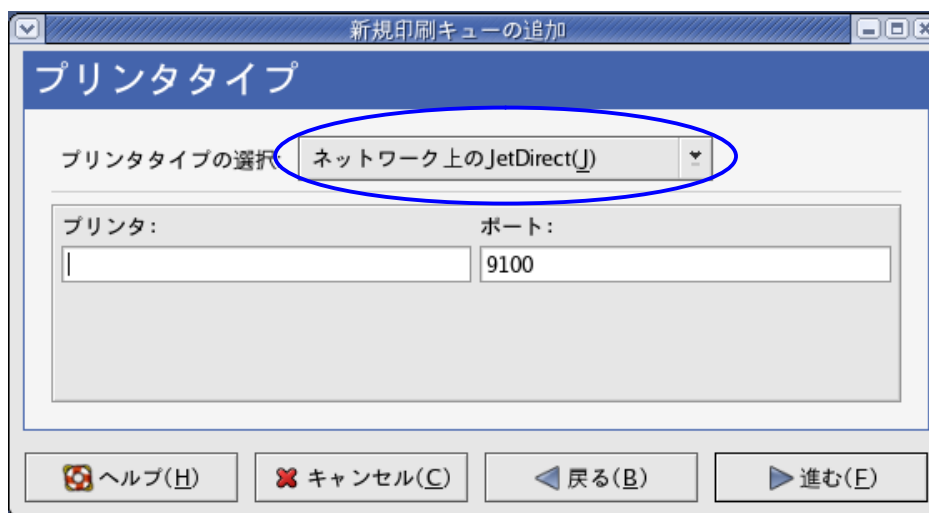
プリンタの名前を設定する。「名前」欄にできるだけ簡潔な名前を入力する。「簡単な説明」欄には、プリンタの説明を入力することができる。



プリンタタイプ

プリンタの接続先が検出され表示される。/dev/lp~はパラレルポート、/dev/usb/lp~はUSBポートで、~の部分はポートの番号である。複数のプリンタを接続していると、接続先も複数表示される。ここで、設定したいプリンタの接続先を一つ選択する。接続先が何も表示されなければ、検出に失敗したと思われる。「デバイスを再スキャン」ボタンをクリックし、再度検出を行なう。

ローカル接続ではなく、ネットワークプリンタを設定する場合は、「プリンタタイプの選択」をクリックし、「ローカル接続のプリンタ」を「ネットワーク上のjetDirect」に変更し、「プリンタ：」と「ポート：」を入力する。「プリンタ：」はプリンタホスト名またはIPアドレスを入力し、「ポート：」はIPポート番号（多くは9100）を入力する。入力が終われば「進む」をクリックする。



プリンタモデル

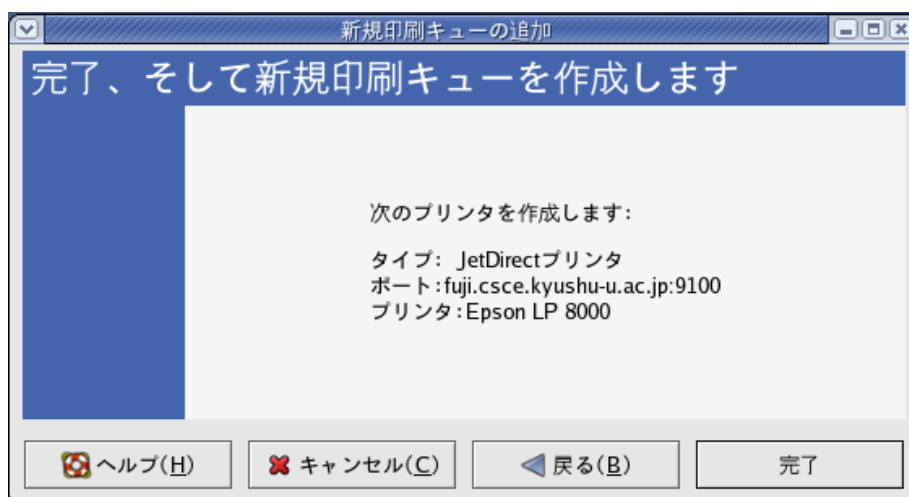
プリンタの形式を選択する。PostScript 対応型であれば「PostScript Printer」を選択する。これで、Linux の印刷機能は最高の能力を発揮する。

一般のプリンタ（PostScript 非対応）の場合、まず「汎用（クリックしてメーカーを選択します）」ボタンをクリックし、設定するプリンタのメーカーを選択する。選択肢が切り替わり、製品名を選択する。選択が終われば「進む」をクリックする。



印刷キューの作成

これまでに設定した内容が表示される。表示内容を確認し、よければ「完了」ボタンをクリックする。設定が確定し、ウィザードが終了する。ただし、プリンタ固有の機能の一部には仮の設定が適用されており、すぐ印刷できるかどうかわからない。プリンタによっては、より詳細な設定が必要となる。

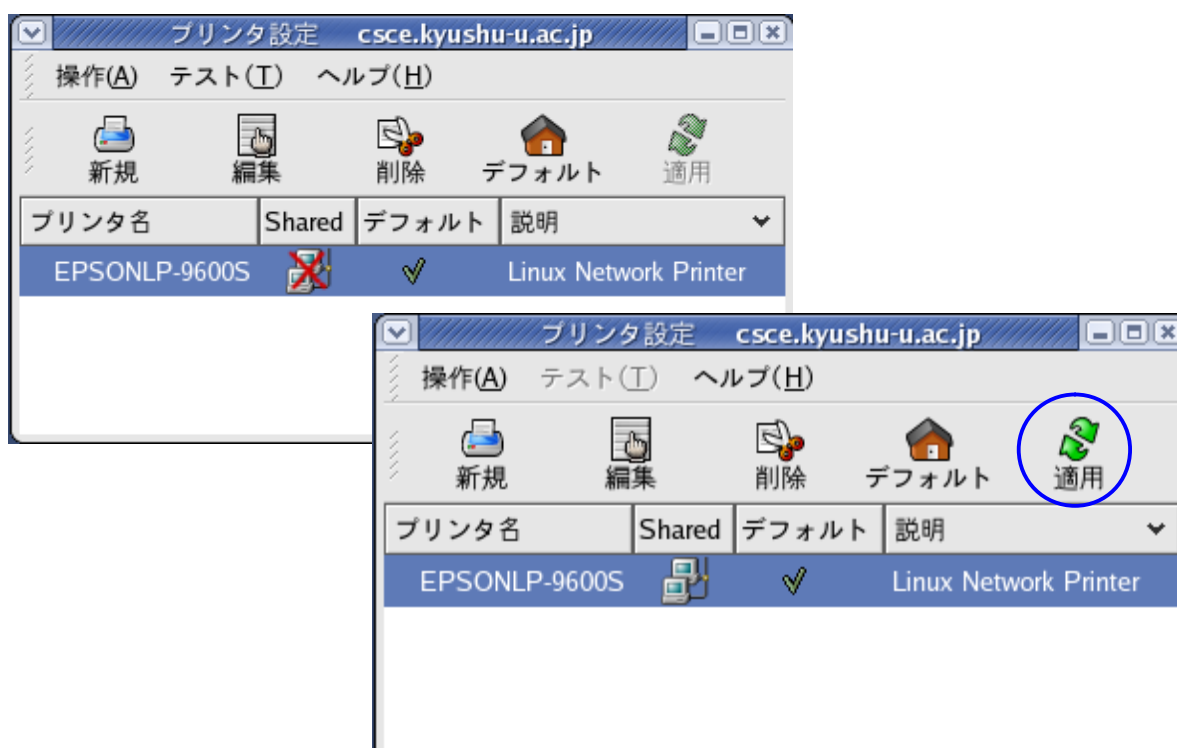


動作確認

動作確認のために、テストページを印刷するかどうかたずねられる。必要であれば「はい」をクリックして印刷の確認を行なう。

設定の終了

設定を変更した場合、「適用」ボタンをクリックして確定する。「Shared」欄に×があるのは、クライアントとの共有を認めていないということであるため、各学校における使用環境に応じて選択してもらいたい。



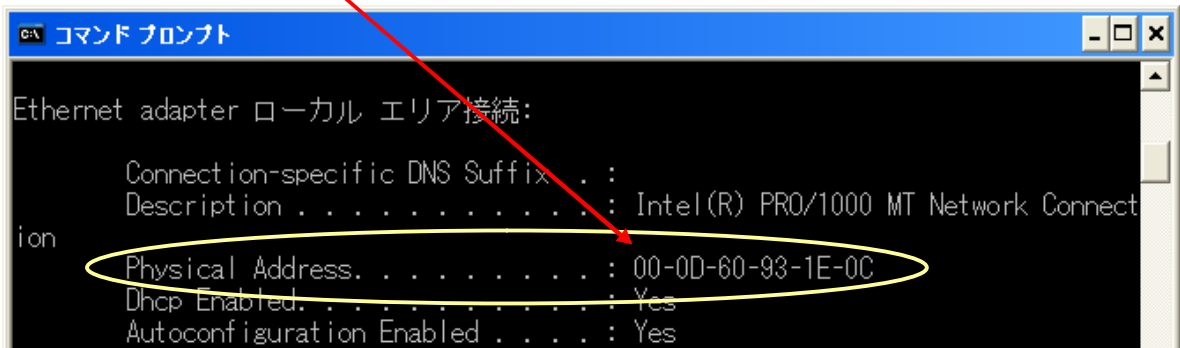
(2) 応用的な設定 (DHCP サーバによる固定 IP アドレスの割り当て)

上記の DHCP サーバ構築において、アドレスプール内のプライベートアドレスをホストに自動配布するように設定を行なった。具体的には、Linux サーバのネットワーク内にある 1 台のホストが起動した際、サーバのプール内にある 16 個の IP アドレス (192.168.0.2 ~ 192.168.0.17) のうち 1 つを自動で割り当てる。そうした場合、16 個の IP アドレスのうちどれを割り当てられたか、ネットワーク管理者は把握することができない。さらに、ホストは起動する都度違ったアドレスを取得してしまう。これでは十分な管理が行えないため、あるホストに対して常に同じアドレスを割り当てるといった設定を行なう必要がある。

その設定については、ホストの MAC アドレスに対して、あらかじめ 1 対 1 に決めておいた IP アドレスを割り当てるため、ホストの MAC アドレスを調査する必要がある。

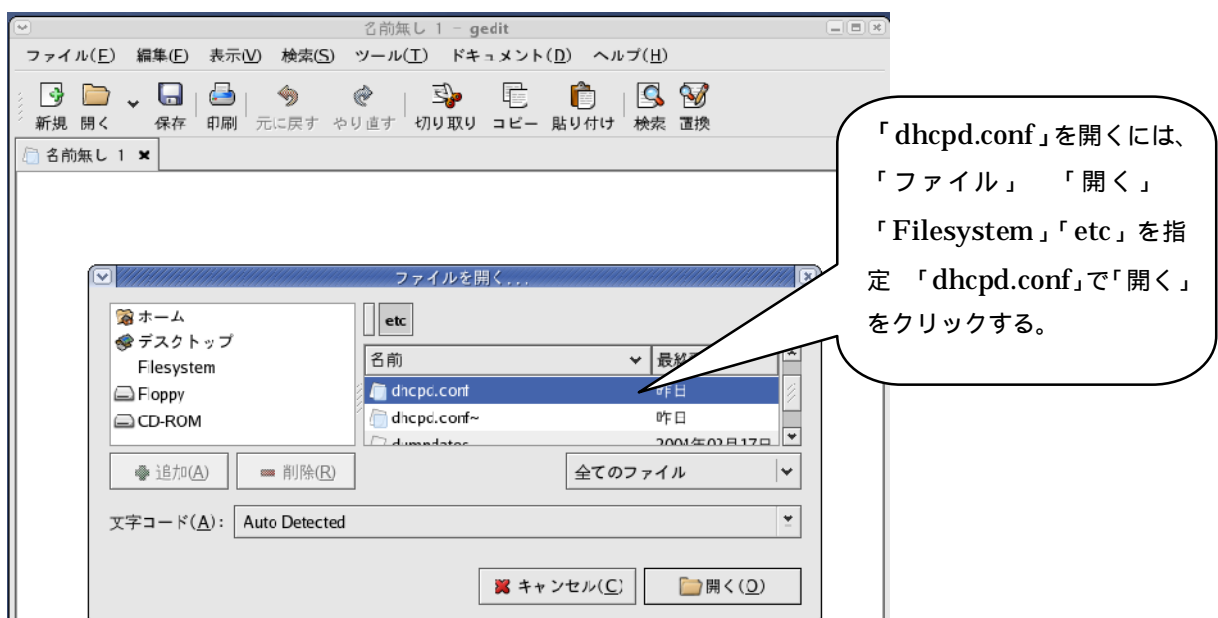
MAC アドレスの調査方法

ホストのコマンドプロンプトを使い、NIC (ネットワークインタフェースカード) の MAC アドレスを表示させ、そのアドレスをメモ帳に書きとめておく。MAC アドレスを調べるには、コマンドプロンプトを起動し、「ipconfig/all」と入力する。そうすると、現在の情報が表示され、その中の「Physical Address」の部分が MAC アドレスとなる。



dhcpd.conf の変更

ホストの MAC アドレスに対して、あらかじめ 1 対 1 に決めておいた IP アドレスを割り当てるためには、dhcpd.conf の内容を変更しなければならない。まず、メインメニューで「アクセサリ」「GNOME テキスト・エディタ」を開き、さらに「dhcpd.conf」を開く。



```
ddns-update-style interim;
subnet 192.168.0.0 netmask 255.255.255.0 {
    range 192.168.0.2 192.168.0.17;
    option subnet-mask 255.255.255.0;
    option routers 192.168.0.1;
    option broadcast-address 192.168.0.255;
    option domain-name-servers _____, _____, _____;
}
```

現在「dhcpd.conf」には、上記のように設定されている。それぞれの意味については、割り当て可能な IP アドレスが (192.168.0.2 ~ 192.168.0.17) 16 個、オプションとしてサブネットマスク、ルータ、ブロードキャストアドレス、DNS サーバのアドレスについて記述されている。この設定については、上記「Linux サーバ構築」で行なっている。これを新たに追加・編集する。

```
ddns-update-style interim;
subnet 192.168.0.0 netmask 255.255.255.0 {
    range 192.168.0.3 192.168.0.17;
    option subnet-mask 255.255.255.0;
    option routers 192.168.0.1;
    option broadcast-address 192.168.0.255;
    option domain-name-servers _____, _____, _____;
}
host work {
    hardware ethernet 00:0d:60:93:1e:0c; # IBM PC1
    fixed-address 192.168.0.2;
}
```

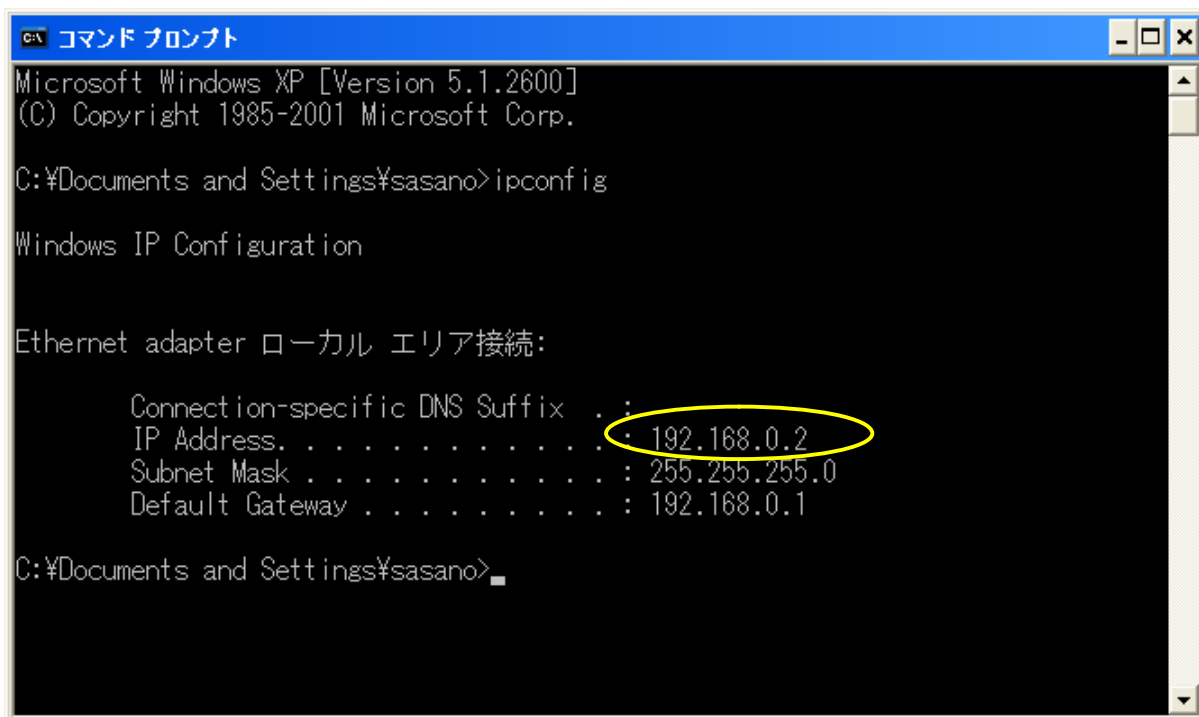
追加する内容は、MAC アドレスに対して IP アドレス (1 対 1) を対応させる。この場合、IBM の PC 側の MAC アドレス (00:0d:60:93:1e:0c) を IP アドレス (192.168.0.2) に対応付ける。そのため、自動割り当て可能なアドレスが一つ (192.168.0.2) 減るため、そこも変更しなければならない。

「dhcpd.conf」の内容を変更したら、「保存」ボタンをクリックし、この設定を/etc ディレクトリに保存する。

動作確認

上記設定が有効になっているか、ホスト側から確認を行なう。設定がきちんと動作すれば、以下のように変更され、このホストに対して DHCP サーバより固定した IP アドレスが割り当てられるようにな

る。



```
コマンド プロンプト
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\sasano>ipconfig

Windows IP Configuration

Ethernet adapter ローカル エリア接続:

    Connection-specific DNS Suffix . . . : 
    IP Address. . . . . : 192.168.0.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

C:\Documents and Settings\sasano>
```

上記の例では、1台のホストしか設定していないが、これをさらに増やし管理することが可能である。本校では、職員室内に自分のパソコンを持ってこられ、校内のネットワークに接続される先生方に対し、「ネットワーク設定マニュアル」(ネットワークに接続するための資料)を配布し、各自でIPアドレスとサブネットマスク、DNS、デフォルトゲートウェイを設定してもらっている。しかし、これではパソコンやネットワークに詳しい先生であれば自分で設定できるが、そうでない先生方には非常に難しいようである。そこで、こういった機能を用いてLANケーブルをHUBに接続するだけで、DHCPサーバから各ホストに自動割り当てによる設定を行ない、さらにどのパソコンがどのIPアドレスを使用しているかがわかり、管理する側の負担が軽減されるように思われる。校内のネットワークに参加される先生方の操作はネットワーク管理者に対し、MACアドレスの連絡のみとなり、設定する負担も軽減され、誤った設定(特に重複したIPアドレス)をされることはない。

第5章 システム開発

システム開発では、Linux サーバを所属校に導入することを前提に、現在の問題点を解決するためのシステム開発の検討を行った。現在、所属校において個人のパソコンを学校に持ち込み、校内のネットワークに接続する事例がしばしば見られる。その設定において、ネットワークに関する知識がない職員が不正な設定（誤ったデータの入力や重複した IP アドレス等の入力）することを避けるため、専門知識を有する職員が個別に対応している状況にある。そういった労力を軽減するために DHCP で IP アドレスの自動割当を行い、利用者側の負担軽減と、ネットワーク管理者側の作業軽減を目指したシステムを構築した。そのシステムは、あらかじめ登録された端末への DHCP 機能による IP アドレスの自動割当機構を実現するものであり、端末登録を GUI で簡単に操作を行うことができるようにした。DHCP サーバの設定ファイルは難解で、編集にあたっては専門的知識が必要となり、また文法ミスがあると正常に稼動しないため、このようなシステムを企画し設計した。

Linux サーバにおける DHCP 機能では、本来クライアントのパソコンに対して IP アドレスを自動的に割り当てるが、それではどのクライアントにどの IP アドレスが割り当てられているか、ネットワーク管理者では把握することができない。そこで、クライアントに対して固定した IP アドレスを割り当てる静的割り当てを計画した。その設定では、Linux 上でコマンドを使った入力となるため、その作業の簡略化を目指すとともに、マウスを使って Windows のように操作ができるようなシステムの設計を検討し、そのシステム開発に必要な CGI と Perl についての学習を併せて実施した。

開発したシステムについては、「構築手順書」と「使用説明書」を作成し、必要に応じて各学校に使ってもらうことを念頭に置き作成した。また、このシステムについては、CGI と Perl を使いブラウザ上で表示させたフォームにデータを入力し、それを `dhcpd.conf` に書き込むといった作業を自動で行うように作成している。そのため、記録媒体などでシステムの配布が行えないため、プログラムコードを文書として残している。

システム開発のまとめ

「登録端末への DHCP による自動アドレス割当機構」

Linux に関する研修とシステム設計

1 開発の概要

今回開発したシステムは、あらかじめ登録された端末への DHCP による IP アドレスの自動割当機構を実現するものである。特徴として、端末登録を GUI で行うものである。DHCP サーバの設定ファイルは難解であり、編集にあたっては専門的知識が必要であり、また文法ミスがあると正常に稼動しないため、このようなシステム開発を企画した。

2 開発の動機

宇美商業高校では、個人のパソコンを学校に持ち込みネットワークに接続する事例がしばしばみられる。その際、ネットワークに関する知識がない教員に対しては、不正な設定（誤ったデータの入力や重複した IP アドレス等の入力）を避けるため、専門知識を有する教員が個別に対応している状況にある。

このような状況における労力を軽減するために、Windows PC など多くの環境で、デフォルトとなっている DHCP を用いた IP アドレス割り当てを使用し、予め登録した端末に対して DHCP で IP アドレスの自動割当を行うシステム構築を企画した。また、個人のパソコンを持ち込む教員についても、近年ではブロードバンドの普及に伴い自宅でインターネットを行う際、ネットワークの設定を行わず DHCP 機能による自動割り当てを適用している利用者が多い。そこで、自宅と学校の設定を統一させ、学校でも自宅と同じネットワークの設定で接続できるよう考慮したシステムを企画した。

3 システム設計

当初、本格的データベース（DB）とウェブインタフェースによる GUI を考えていたが、今回の開発では DB 部分はテキストファイルを用いるものとし、本格的な DB の使用は行わないものとする。

既存のソフトウェア（dhcpd）の設定ファイルの一部については GUI を用いてブラウザ上から追加、削除、更新できるシステムとして実現する。

4 成果物の公開などについて

- ・Linux サーバの導入に関するマニュアル

作成したものを、研修成果として文書として残す。

- ・登録端末への DHCP による自動アドレス割当機構

仕様書、設計書、使用説明書および成果物（プログラムコード）を研修成果として文書として残す。必要に応じて、各学校に使っていただくことを念頭に作成する。

5 成果物の利用計画

宇美商業高校においては、H16 年 2 月に調達した Linux サーバの活用を計画しているため、その活用計画の一部に本成果物の利用を位置づけたい。

今回のソフトウェア開発環境の研修成果を生かし、ネットワーク管理を行う教員の労力を軽減するシステムを企画したい。

システム設計の計画

1 システムにおける操作の流れ

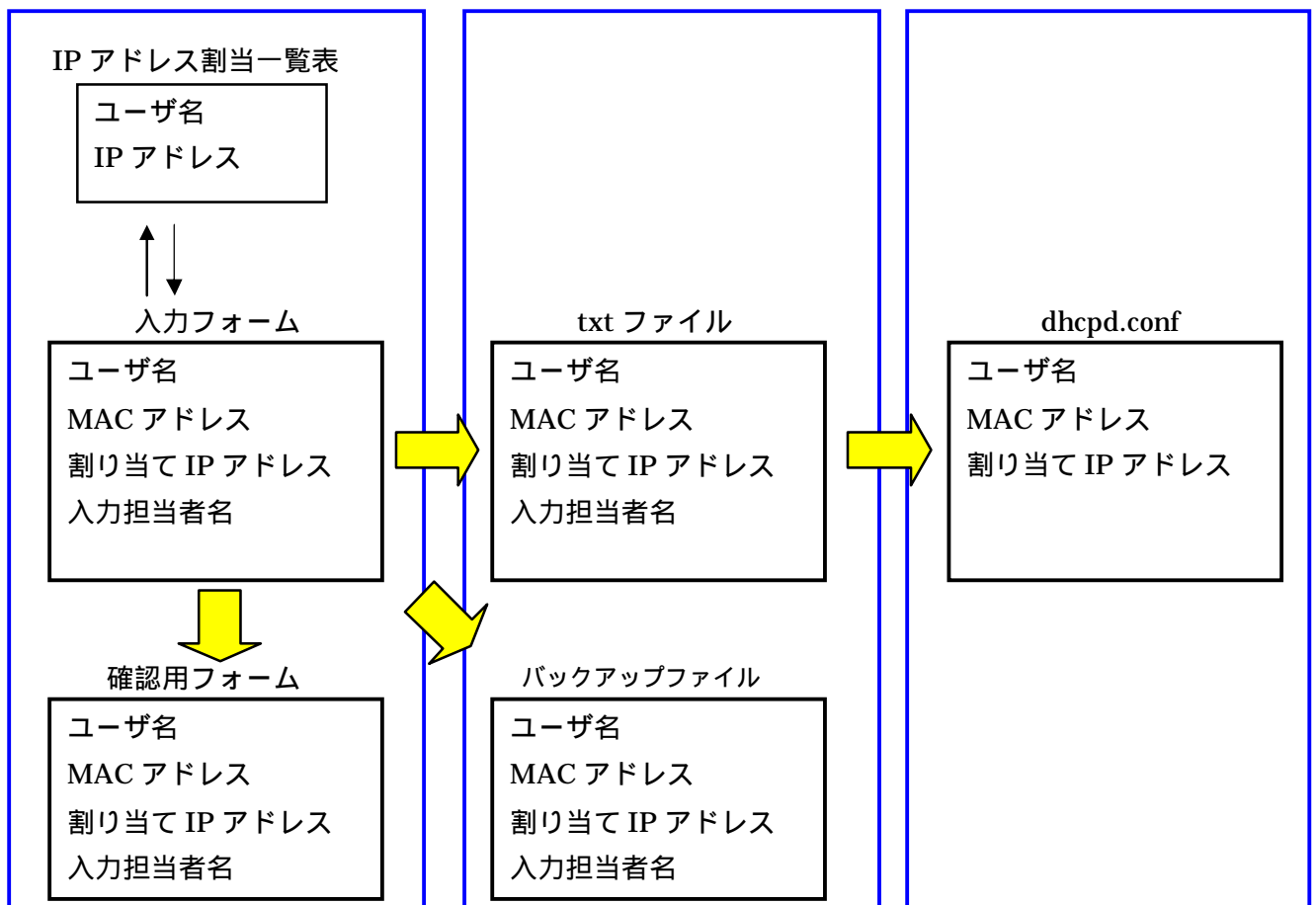
校内ネットワーク接続に掛かる業務として、ネットワーク管理者およびネットワークの係り(以下入力担当者)が行う作業のイメージを示す。

入力担当者は、利用者(個人のパソコンを校内ネットワークに接続する職員)から校内ネットワーク接続申請紙(ユーザ名と MAC アドレスが記入されたもの)を提出してもらう。

入力担当者は、利用者に貸し出し可能な校内 IP アドレス一覧表を作成しておく。

入力担当者は、利用者から受け取ったユーザ名と MAC アドレス、IP アドレス一覧表から空きアドレス、入力担当者名を入力フォームから入力する。ただし、入力フォームは Linux サーバを直接操作するのではなく、校内ネットワークに接続されているどのパソコンからでもブラウザを介して入力できるようにしておく。

入力フォームから利用者の上記情報を入力した後、「登録」ボタンをクリックすると、入力された内容が確認フォームを通じてブラウザ上に表示され、それと同時にその内容が Linux サーバ上に dhcpd.conf 書換え用のファイルとバックアップファイルして、テキストファイルに書き出され保存される。一旦、dhcpd.conf 書換え用のファイルとして保存されたテキストファイルの内容は、dhcpd.conf ファイルに書き出され保存される。



2 GUI 操作画面と各ファイル

入力フォーム

入力担当者が、利用者の提出されたデータを入力する。入力フォームは GUI で行うものとし、Linux サーバを直接操作するのではなく、校内ネットワークに接続されているどのパソコンからでもブラウザを介して入力できるようにする。また、利用者によって入力フォームからの操作や閲覧ができないようにユーザ認証を用いる。

ユーザ認証

入力者を認証する方法として、入力者のユーザ ID とパスワードを設定し、入力者以外が操作できないようにする。

確認用フォーム

入力者が入力フォーム上で入力した内容を確認させるためのフォームとする。Linux サーバへの入力が完了した旨を通知する。この動作については、CGI のプログラムで自動化する。

txt ファイル

入力フォームから入力されたデータを、一旦テキストファイルで保存する。この作業については、CGI のプログラムで自動化させる。

バックアップファイル

IP アドレスの割り当て状況を残すため、バックアップファイルとして txt ファイルとは異なるディレクトリに保存する。バックアップの操作については自動化し、タイマー機能を使い定期的にバックアップを行うようにする。また、txt ファイルとバックアップファイルの内容は全く同じものとし、dhcpd.conf に障害が発生したとき、簡単にバックアップファイルを利用できるようにする。

dhcpd.conf

dhcpd.conf の特性から、入力されたデータを dhcpd.conf に自動で書き込むことができないため、一旦テキストファイルとして保存された内容を reload (再読み込み) させる。

校内ネットワーク接続申請用紙

利用者のユーザ名と MAC アドレスを記述する用紙を作成し、それをもとに入力担当者が入力作業を行う。

校内 IP アドレス一覧表

利用者が校内ネットワークに接続するために、貸し出し可能な校内 IP アドレス一覧表を作成しておく、空きアドレスを利用者に貸し出す。

3 その他

利用者が行う作業として、校内ネットワーク接続申請用紙に MAC アドレスを記入しなければならない。その確認については、高度な操作ではないため、マニュアルを作成し各自で行わせるようにする。

システムの仕様について

設計したシステムは、Linux で動作する DHCP 機能を使ったものである。そのため、Windows 系のサーバでは動作しない。このシステムについては、CGI と Perl を使い、ブラウザ上で表示させたフォームにデータを入力し、それを dhcpd.conf に書き込むといった作業を自動で行うように作成している。そのため、記録媒体などでシステムの配布が行えないため、プログラムコードで書き残す。

システムの構築手順

1 フォームの作成

入力フォーム

入力フォームでは、管理者が利用者のユーザデータを入力しやすく、かつ入力誤りが少なくなるように配慮して作成する。「校内 IP アドレス設定フォーム」では、利用者の最低限必要データとしてユーザ名、MAC アドレスが必要となる。その他に、割り当てる IP アドレスを入力する必要がある。それ以外の情報として、登録するユーザが新規または修正なのか、誰が登録作業を行ったかといった情報を残すために、設定状況と入力担当者の欄を設けている。

ア ユーザ名

ユーザ名については、利用者を判別する際に利用されるため、ここでは半角英数字で入力するようにコメントを表示する。

イ MAC アドレス

MAC アドレスは、16 進数 12 桁で 2 桁ずつの区切りがあるため、その記述が統一した形で入力できるように半角英数字のみ入力させるようにする。

ウ 割当 IP アドレス

ここに入力する IP アドレスは、校内で決めたプライベートアドレスを利用する。別に校内割当 IP 一覧などを作成し、空きアドレスを割り当てるといったことを行う。MAC アドレス同様、半角数字のみの入力となる。

エ 設定状況

これは必ずしも必要ではないが、用途に応じて導入するか検討する。ここでは 2 つを選択するようにしているため、ラジオボタンを採用している。

オ 入力担当者

入力した係りが責任を持つように、また誰が利用者の登録を行ったかわかるように、あらかじめ入力担当の係りの名前をこのページ作成時に入力しておく。ここではプルダウンメニューを使い、入力担当者を選択するようにしている。

カ 登録ボタン

入力が完了すると、「登録」のボタンをクリックすることにより登録作業が終了する。

キ クリアボタン

入力の中止の際に利用する。

The screenshot shows a web browser window titled "IPアドレス登録 - Microsoft Internet Explorer". The address bar shows "http://linux.sasano/rensyuu/model/form6.html". The page content is titled "校内IPアドレス設定フォーム". It contains the following form elements:

- ユーザ名: [] *半角英数字で入力して下さい
- MAC アドレス: []:[]:[]:[]:[]:[] *例 00:01:80:31:EC:E7
- 割当IPアドレス: [].[].[].[] *例 192.168.0.1
- 設定状況: 新規 修正
- 入力担当者: 笹野 (dropdown menu)
- Buttons: 登録, クリア

入力フォームのソースプログラム

ここでは、CGI・Perlのプログラムを使い、入力フォームに必要事項を入力し、「登録」ボタンをクリックするとform6.cgiの画面が戻ってくるようにしている。完成したフォームの保存場所については、Linuxサーバ上の / var / www / html / に保存する。ファイル名については任意でよいが、ここではform.htmlとしている。(/ var / www / html / form.html)

```
<HTML>
<HEAD>
<meta http-equiv="Content-Type" content="text/html; charset=euc-jp">
<TITLE>IPアドレス登録</TITLE>
</HEAD>
<BODY>

<H2>校内IPアドレス設定フォーム</H2>

<FORM METHOD="POST" ACTION="/cgi-bin/form6.cgi">
ユーザ名：
<INPUT TYPE="text" name="name">
*半角英数字で入力して下さい
<P>

MAC アドレス：
<INPUT size="1.5" TYPE="text" name="mac1">：
<INPUT size="1.5" TYPE="text" name="mac2">：
<INPUT size="1.5" TYPE="text" name="mac3">：
<INPUT size="1.5" TYPE="text" name="mac4">：
<INPUT size="1.5" TYPE="text" name="mac5">：
<INPUT size="1.5" TYPE="text" name="mac6">
*例 00:01:80:31:EC:E7
<P>

割当IPアドレス：
<INPUT size="2" TYPE="text" name="ip1"> .
<INPUT size="2" TYPE="text" name="ip2"> .
<INPUT size="2" TYPE="text" name="ip3"> .
<INPUT size="2" TYPE="text" name="ip4">
*例 192.168.0.1
<P>

設定状況：
<INPUT TYPE="radio" name="jyoukyou" VALUE="new" CHECKED>新規
<INPUT TYPE="radio" name="jyoukyou" VALUE="correction">修正
<P>

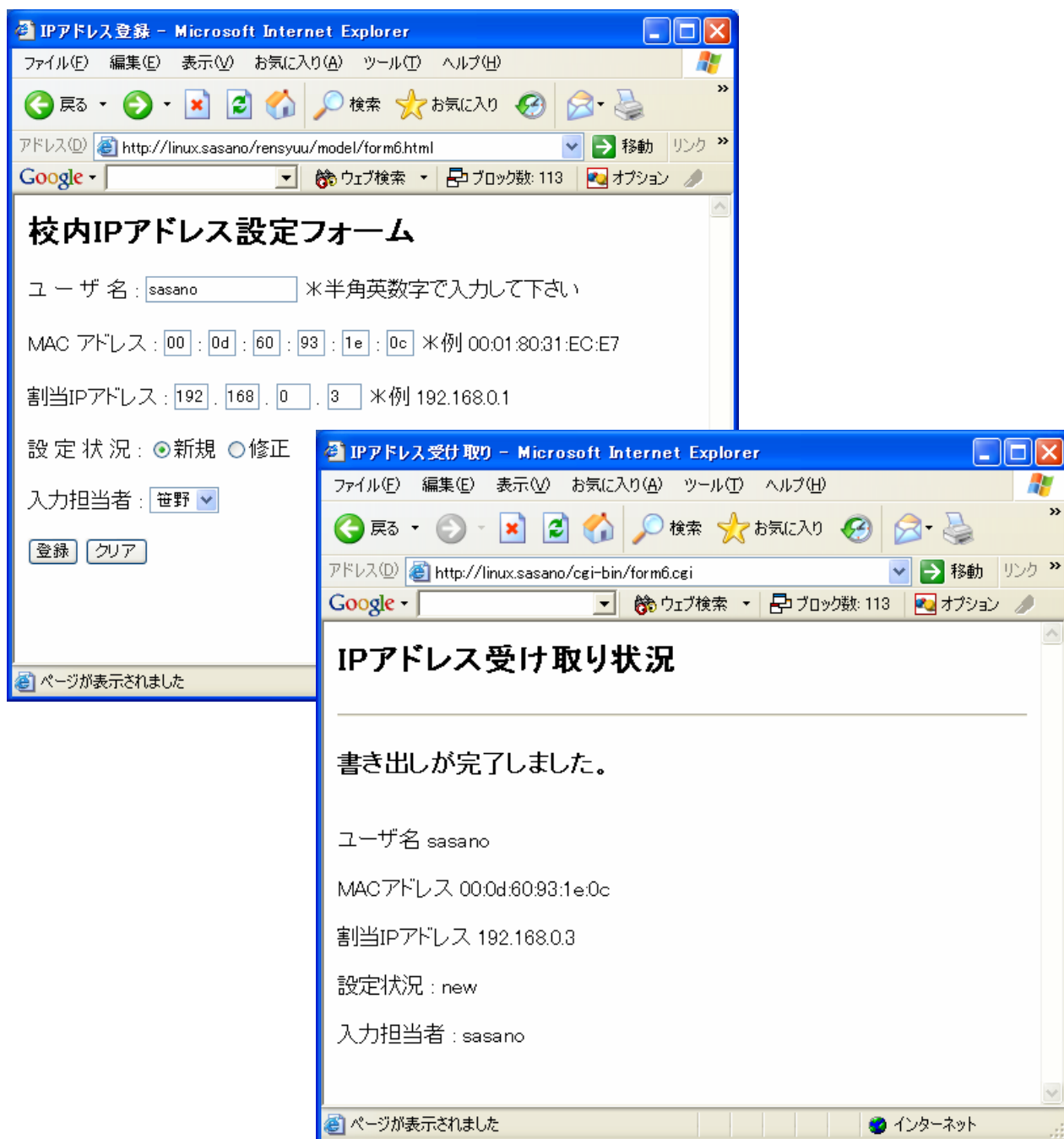
入力担当者：
<SELECT NAME="tantou">
<OPTION SELECTED VALUE="sasano">笹野
<OPTION VALUE="yasutake">安武
<OPTION VALUE="yamauchi">山内
</SELECT>
<P>

<INPUT TYPE="submit" VALUE="登録">
<INPUT TYPE="reset" VALUE="クリア">
</FORM>

</BODY>
</HTML>
```

受け取りフォーム

入力フォームに必要事項を入力し、「登録」ボタンをクリックすると「IP アドレス受け取り状況」が表示されるようにする。ここでは、ユーザ名を sasano、MAC アドレスを 00:0d:60:1e:0c、割当 IP アドレスを 192.168.0.3、設定状況を「新規」、入力担当者を「笹野」とし、登録ボタンをクリックした状態である。入力フォーム（校内 IP アドレス設定フォーム）で入力されたデータが、受け取りフォーム（IP アドレス受け取り状況）に表示される。



受け取りフォームのソースプログラム

入力フォームで「登録」のボタンをクリックすることにより、受け取りフォームにデータを返し表示させるというアクションだけではなく、ここではそれと同時に dhcpd.conf とバックアップファイルにも書き出すようにしている。dhcpd.conf とバックアップファイル作成については後で述べる。

完成した受け取りフォームの保存場所については、Linux サーバ上の /var/www/cgi-bin/ に保存する。ファイル名については任意でよいが、ここでは form6.cgi とした。(/var/www/cgi-bin/form6.cgi)

```
#!/usr/bin/perl

read(STDIN,$formin,$ENV{'CONTENT_LENGTH'});

@indata = split(/&/,$formin);
foreach $tmp(@indata)
{
    ($name,$value)=split(/=/, $tmp);
    $name{$name}=$value;
}

$macaddr="$name{'mac1'}:$name{'mac2'}:$name{'mac3'}:$name{'mac4'}:$name{'mac5'}:$name{'mac6'}";
$ipaddr="$name{'ip1'}.${name{'ip2'}.${name{'ip3'}.${name{'ip4'}}}";

#backup data
open(OUT,">>/etc/dhcpd-data/bkdata.txt");
print OUT "host ";
print OUT "$name{'name'}";
print OUT " {\n";
print OUT "    hardware ethernet $macaddr";
print OUT ";\n";

print OUT "    fixed-address $ipaddr";
print OUT ";\n";
print OUT "#tantou : $name{'tantou'}\n";
print OUT "#jyoukyou : $name{'jyoukyou'}\n";
print OUT "}\n";
close(OUT);

#dhcpd.conf data
open(OUT,">>/etc/dhcpd-data/test.txt");
print OUT "host ";
print OUT "$name{'name'}";
print OUT " {\n";
print OUT "    hardware ethernet $macaddr";
print OUT ";\n";

print OUT "    fixed-address $ipaddr";
print OUT ";\n";
print OUT "#tantou : $name{'tantou'}\n";
print OUT "#jyoukyou : $name{'jyoukyou'}\n";
print OUT "}\n";
close(OUT);

print "Content-type: text/html\n\n";
print "<META http-equiv=\"Content-Type\" text/html; charset=EUC-JP\">\n";

print "<HTML>\n";
print "<HEAD><TITLE>IPアドレス受け取り</TITLE></HEAD>\n";
print "<BODY>\n";
print "<H2>IPアドレス受け取り状況</H2><HR>\n";

print '<H3>書き出しが完了しました。</H3><BR>';
print "ユーザ名 $name{'name'} <BR><BR>";
print "MACアドレス $name{'mac1'}:$name{'mac2'}:$name{'mac3'}:$name{'mac4'}:$name{'mac5'}:$name{'mac6'} <BR><BR>";
print "割当IPアドレス $name{'ip1'}.${name{'ip2'}.${name{'ip3'}.${name{'ip4'}}} <BR><BR>";
print "設定状況 : $name{'jyoukyou'}<BR><BR>\n";
print "入力担当者 : $name{'tantou'}<BR><BR>\n";

print "</BODY>\n";
print "</HTML>\n";
exit;
```


受け取りフォームの解説

ア \$macaddr・\$ipaddr

入力フォームから入力されたMACアドレスとIPアドレスを記録するための書式を定義している。ここで定義された書式を#backup data と#dhcpd.conf data で活用する。

```
$macaddr="$name{'mac1'}:$name{'mac2'}:$name{'mac3'}:$name{'mac4'}:$name{'mac5'}:$name{'mac6'}";  
$ipaddr="$name{'ip1'}.$name{'ip2'}.$name{'ip3'}.$name{'ip4'}";
```

イ #backup data

open 文で、/etc/dhcpd-data/という場所に格納されている bkdata.txt ファイルを開き、print 文の内容を書き込んでから閉じるという内容である。print 文で記述している内容は、dhcpd.confに利用者を登録するための書式となる。

```
#backup data  
open(OUT, ">>/etc/dhcpd-data/bkdata.txt");  
print OUT "host ";  
print OUT "$name{'name'}";  
print OUT " {\n";  
print OUT "   hardware ethernet $macaddr";  
print OUT ";\n";  
  
print OUT "   fixed-address $ipaddr";  
print OUT ";\n";  
print OUT "#tantou : $name{tantou}\n";  
print OUT "#jyoukyou : $name{jyoukyou}\n";  
print OUT "}\n";  
close(OUT);
```

ウ #dhcpd.conf data

上記の#backup data とほとんど同じであり、保存先と保存するファイル名が異なる程度である。open 文で、/etc/dhcpd-data/という場所に格納されている test.txt ファイルを開き、print 文の内容を書き込んでから閉じるという内容である。print 文で記述している内容は、dhcpd.confに利用者を登録するための書式となり、このファイルが dhcpd.conf ファイルに直接コピーされる。

```
#dhcpd.conf data  
open(OUT, ">>/etc/dhcpd-data/test.txt");  
print OUT "host ";  
print OUT "$name{'name'}";  
print OUT " {\n";  
print OUT "   hardware ethernet $macaddr";  
print OUT ";\n";  
  
print OUT "   fixed-address $ipaddr";  
print OUT ";\n";  
print OUT "#tantou : $name{tantou}\n";  
print OUT "#jyoukyou : $name{jyoukyou}\n";  
print OUT "}\n";  
close(OUT);
```

```
ddns-update-style interim;  
subnet 192.168.0.0 netmask 255.255.255.0 {  
    range 192.168.0.10 192.168.0.17;  
    option subnet-mask 255.255.255.0;  
    option routers 192.168.0.1;  
    option broadcast-address 192.168.0.255;  
    option domain-name-servers _____, _____, _____;  
}  
host work {  
    hardware ethernet 00:0d:60:93:1e:0c; # work  
    fixed-address 192.168.0.2;  
}  
host sasano {  
    hardware ethernet 00:0d:60:93:1e:0c;  
    fixed-address 192.168.0.3;  
    #tantou : sasano  
    #jyoukyou : new  
}
```

dhcpd.conf ファイル

エ 受け取りフォーム

以下のプログラムが受け取りフォームのソースとなる。

```
print "Content-type: text/html\n\n";
print "<META http-equiv=\"Content-Type\"text/html;
charset=EUC-JP\">\n";

print "<HTML>\n";
print "<HEAD><TITLE>IPアドレス受け取り</TITLE></HEAD>\n";
print "<BODY>\n";
print "<H2>IPアドレス受け取り状況</H2><HR>\n";

print '<H3>書き出しが完了しました。</H3><BR>';
print "ユーザ名 $name{'name'} <BR><BR>";
print "MACアドレス $name{'mac1'}:$name{'mac2'}:$name{'mac3'}:$name{'mac4'}:
$name{'mac5'}:$name{'mac6'} <BR><BR>";
print "割当IPアドレス $name{'ip1'}.$name{'ip2'}.$name{'ip3'}.$name{'ip4'}
<BR><BR>";
print "設定状況 : $name{'jyoukyou'}<BR><BR>\n";
print "入力担当者 : $name{'tantou'}<BR><BR>\n";

print "</BODY>\n";
print "</HTML>\n";
exit;
```

IPアドレス受け取り状況

書き出しが完了しました。

ユーザ名 sasano

MACアドレス 00:0d:60:93:1e:0c

割当IPアドレス 192.168.0.3

設定状況 : new

入力担当者 : sasano

print "ユーザ名 \$name{'name'}";

print "MAC アドレス \$name{'mac1'}: ~ \$name{'mac6'}";

print "割当 IP アドレス \$name{'ip1'}: ~ \$name{'ip4'}";

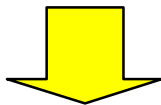
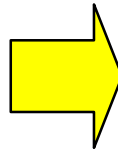
print "設定状況 \$name{'jyoukyou'}";

print "入力担当者 \$name{'tantou'}";

各動作の流れ

ブラウザで入力フォームを表示し、利用者の必要事項を入力する。「登録」ボタンをクリックすると受け取りフォームに入力データが入ったものが表示されると同時に、dhcpd.confの元になるデータ(この場合のファイル名: test.txt)とバックアップデータ(bkdata.txt)がテキストファイルとして保存される。この2つのファイルは、既存のファイルに追加されたデータを上書きして保存するようになる。受け取りフォームのソースプログラムの「#backup data」と「#dhcpd.conf data」の部分がそれぞれ

の操作の内容である。

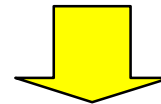



```
ddns-update-style interin;
subnet 192.168.0.0 netmask 255.255.255.0 {
  range 192.168.0.10 192.168.0.17;
  option subnet mask 255.255.255.0;
  option routers 192.168.0.1;
  option broadcast-address 192.168.0.255;
  option domain-name-servers [redacted];
}
host work {
  hardware ethernet 00:0d:80:93:1c:0e; # work
  fixed-address 192.168.0.2;
}
host sasano {
  hardware ethernet 00:0d:60:93:1c:0c;
  fixed address 192.168.0.3;
  #lan100 : sasano
  #jyoukyou : new
}
```

bkdata.txt (backup data)

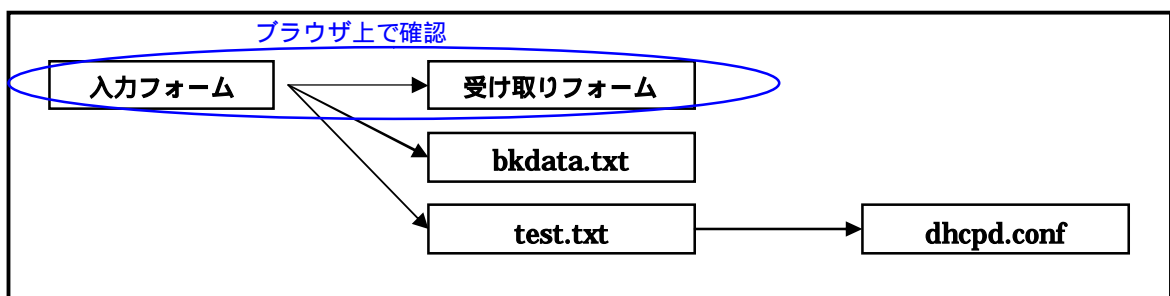
```
ddns-update-style interin;
subnet 192.168.0.0 netmask 255.255.255.0 {
  range 192.168.0.10 192.168.0.17;
  option subnet mask 255.255.255.0;
  option routers 192.168.0.1;
  option broadcast-address 192.168.0.255;
  option domain-name-servers [redacted];
}
host work {
  hardware ethernet 00:0d:80:93:1c:0e; # work
  fixed-address 192.168.0.2;
}
host sasano {
  hardware ethernet 00:0d:60:93:1c:0c;
  fixed address 192.168.0.3;
  #lan100 : sasano
  #jyoukyou : new
}
```

test.txt (dhcpd.conf data)



```
ddns-update-style interin;
subnet 192.168.0.0 netmask 255.255.255.0 {
  range 192.168.0.10 192.168.0.17;
  option subnet mask 255.255.255.0;
  option routers 192.168.0.1;
  option broadcast-address 192.168.0.255;
  option domain-name-servers [redacted];
}
host work {
  hardware ethernet 00:0d:80:93:1c:0e; # work
  fixed-address 192.168.0.2;
}
host sasano {
  hardware ethernet 00:0d:60:93:1c:0c;
  fixed address 192.168.0.3;
  #lan100 : sasano
  #jyoukyou : new
}
```

dhcpd.conf ファイル



入力フォームで入力されたデータが、受け取りフォーム・bkdata.txt・test.txt の3つファイルに渡され、受け取りフォームはブラウザに表示され、bkdata.txt と test.txt ファイルは /etc/dhcpd-data/ に保存される。また、test.txt は、dhcpd.conf (/etc/dhcpd.conf) に書き替えられる。

このような流れにより、新たに登録された利用者のデータが dhcpd.conf とバックアップファイルに追加される。

2 dhcpd.conf とバックアップファイルの作成

dhcpd.conf の reload

入力フォームから入力されたデータが bkdata.txt と test.txt に書き込まれることについては、上記で説明したが、test.txt として作成されたファイルを dhcpd.conf にどのようにして反映させているかというと、reload (再読み込み) させている。dhcpd.conf のファイルは、DHCP サーバの中核的なプログラムのため、フォームで操作を行った内容をそのまま書き込ませるとトラブルの原因になりかねない。また、Linux では dhcpd.conf ファイルの書き換えを行うと DHCP サーバを再起動させなければならない。そこで、一旦別のテキストファイルに書き込んだファイルを dhcpd.conf に再読み込みさせるといったイメージとなる。そのプログラム例としては、以下ようになる。

```
#!/bin/sh
cd /etc/dhcpd-data
if [ -f test.txt ]; then
    mv /etc/dhcpd.conf /etc/dhcpd.conf-bak
    cp test.txt /etc/dhcpd.conf
    kill -TERM `cat /var/run/dhcpd.pid`
    /usr/sbin/dhcpd eth1
fi
```

ここでは、/etc/dhcpd-data/という記憶場所に、dhcpd-conf-reload というファイル名で上記のファイルを保存する。こうすることにより、入力フォームで入力されたデータが、dhcpd.conf ファイルに反映され、上書き保存される。

バックアップファイルの作成

バックアップファイルの作成については、上記でも述べたように受け取りフォームのプログラムに記述されている (#backup data) のところの open 文で、/etc/dhcpd-data/という場所に格納されている bkdata.txt ファイルを開き、print 文の内容を書き込んでから閉じる。当然上書きされるということになる。このファイルがあれば dhcpd.conf ファイルが壊れたりしても、dhcpd.conf ファイルの内容と同じものをほぼ同時にバックアップファイルとして作成しているため、バックアップファイル (bkdata.txt) のファイル名を変更することにより dhcpd.conf ファイルを再生することができる。

バックアップのタイミング

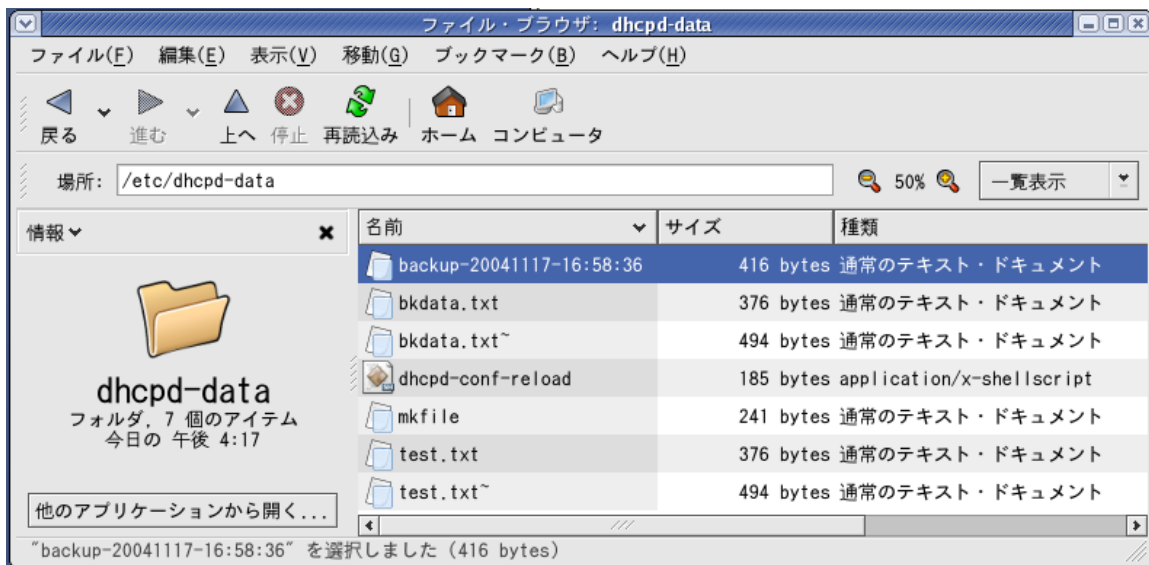
上記のように、利用者を登録する都度バックアップファイルを作成しているが、更に Linux の cron を使ったタイマー的なバックアップを行う。ここでは、毎日 5 分おきにバックアップの更新を行うようにしている。

```
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (/tmp/crontab.5866 installed on Wed Nov 17 16:45:49 2004)
# (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
0,5,10,15,20,25,30,35,40,46,50,55 * * * * /etc/dhcpd-data/dhcpd-conf-reload
```

プログラムといっても、上記プログラム例の 4 行目だけである。左から 5 分おきに時間指定がなされている。この見方については、0,5,10,15,~50,55 の部分が、分 (minutes) のみの指定で、その後の * が時 (hour)、その次の * が日 (day)、月 (month)、年 (year) となっている。このように細かく指定することができる。

このファイルについては、/var/spool/cron/という場所にある root に4行目だけを書き足し保存すればよい。また、バックアップファイルを生成する際に、日付と時間入りのファイル名で保存するプログラムの例を示す。このプログラムについても、/etc/dhcpd-data/という場所にmkfileというファイル名で保存している。

```
#!/perl
($sec,$min,$hour,$mday,$mon,$year,$wday,$yday,$isdst) = localtime(time);
$mon = $mon + 1;
$year = $year + 1900;
$sti = "$year$mon$mday-$hour:$min:$sec";
open(FILE, "> backup-$sti");
print FILE "current date-time is $sti\n";
close(FILE);
```



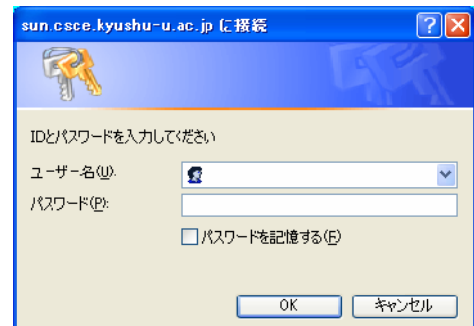
3 ユーザ認証用フォームの作成

パスワードファイルの作成

今回は BASIC 認証を利用したため、その作成について簡単に述べておく。

BASIC 認証でアクセス制限を行うには、「.htaccess ファイル」と「パスワードファイル」の2つが必要である。まず、「パスワードファイル」を作成する。ファイル名は特に決まりはしないが、一般的に「.htpasswd」というファイル名が用いられる。

このファイルには、許可するユーザ名とパスワードを保存する。このとき、パスワードを暗号化の必要があり、パスワードを暗号化する方法について2つの方法を紹介しておきたい。



パスワードの暗号化

パスワードを暗号化する場合、サーバのコンソールにコマンドを入力して作成する方法と、ウェブ上にある暗号化ツールを使うという方法がある。

ア サーバ上での暗号化

サーバのコンソールに telnet や SSH で接続し、htpasswd というコマンドを利用してパスワードファイルを作成することができる。次の例では、現在のフォルダに.htpasswd というファイルを新しく作成し、sasano というユーザを登録する。パスワードを聞かれるため、同じパスワードを2回入力する(画面には表示されない)。

```
%> htpasswd -c .htpasswd sasano
New password: test
Re-type password: test
Adding password for user sasano
```

「-c」はオプションで、パスワードファイルを新しく作成するという意味である。すでにあるファイルにユーザを追加したい場合は不要。作成された.htpasswd は、root 権限で作成すると/root/に保存され、ユーザモードで作成すると、/home/sasano/に保存される。

イ 暗号化ツールを使う

ウェブ上には、多くの暗号化を行うページが存在し、誰でも自由に利用できるものとして提供されているページがある。そのページにアクセスし、ID とパスワードを入力するとパスワードが暗号化される。 < BASIC 認証用パスワード暗号化ツール <http://orange-factory.com/tool/crypt.cgi> >

そこで暗号化されたパスワードを以下のようにテキストエディタ(メモ帳等)に貼り付け、パスワードファイルとして保存すればよい。(ファイル名: .htpasswd) 保存する場所は特に指定されていないため、ここでは/var/www/html/rensyuu/model/に保存した。

```
sasano:E13BRLEjwKRLU
```

「.htaccess ファイル」の作成

アクセス制限したいフォルダに「.htaccess」という名前のファイルを作る。これも、内容は普通のテキストファイルである。パスワードファイルと違い、必ずこの名前にする必要がある。

認証用のフォームについては、校内の IP アドレス設定のためのフォームを利用者が閲覧できないようにするための工夫として作成する。これは、制限付きでウェブページを公開する際に用いられる。

作成方法としては、テキストエディタ(メモ帳等)で以下のプログラムコードを入力し、「.htaccess」(拡張子が htaccess ということで、ドットが必要である。)といったファイル名で保存する。保存する場所は、入力フォームを保存しているディレクトリに置いて制限をかけるということになる。

```
AuthType Basic
AuthUserFile /var/www/html/rensyuu/model/.htpasswd
AuthGroupFile /dev/null
AuthName "IDとパスワードを入力してください。"
<limit GET POST>
require valid-user
</limit>
```

・ 1 行目「AuthType Basic」:

認証方式を設定する。 Basic 認証を利用する時には「Basic」を指定する。これは、ID とパスワードによるアクセス制御 (Basic 認証) を表す。

- 2行目「**AuthUserFile**」:
準備したパスワードファイルを、フルパスで指定する。Webページのルートからのパスではなく、サーバ上パスとなるため、注意が必要である。
- 3行目「**AuthGroupFile**」:
グループファイル名を指定する。グループを使わないときには「/dev/null」を指定する。グループファイルを使うと、あるフォルダは全員閲覧できて、別のフォルダは特定のグループの人だけ閲覧可能、というようなことを実現できる。
- 4行目「**AuthName**」:
ユーザ名・パスワードを入力するダイアログボックスに表示されるメッセージ。全角文字も指定できるが、文字化けの可能性がある。スペースを含むメッセージを設定するときには、メッセージ全体をダブルクォートで括る。
- 5行目「**require valid-user**」:
認証させるユーザを指定する。「**valid-user**」と指定すると、「**AuthUserFile**」で指定したファイル内の全ユーザが認証される。「**user ユーザ名**」と指定すると、そのユーザだけが認証される。「**group グループ名**」と指定すると、「**AuthGroupFile**」内に書かれた該当グループのユーザだけが認証される。

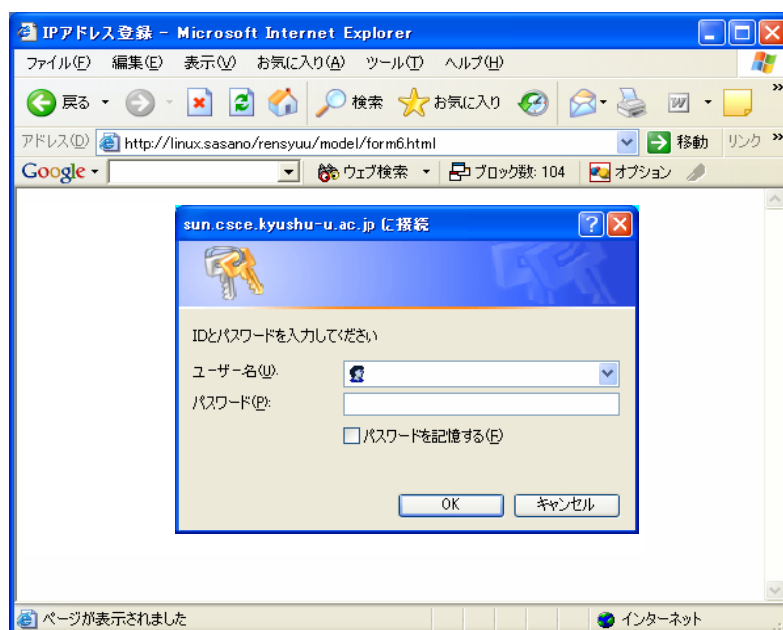
4 その他

システム開発の構築手順として、以上のように記述したが、これは実行ファイル（exe）とは異なるため、様々な記録媒体に保存して配布することができない。そのため、以上のような操作をコマンドラインで記述していかなければならない。

システムの使用方法

- 1 ネットワーク管理者（入力担当者）が行う操作
メニューを開く

Linuxサーバ上にあるフォームをブラウザで開く。そうすると、ユーザ認証用のフォームが現れ、あらかじめ登録している入力担当以外は入力操作等できない。入力担当者は、ユーザIDとパスワードを入力し、「OK」をクリックする。



入力フォームで必要事項入力

必要事項(ユーザ名・MAC アドレス・割当 IP アドレス・設定状況・入力担当者)を入力し、「登録」をクリックする。

ア ユーザ名

利用者のユーザ ID を入力する。

イ MAC アドレス

利用者に自分のパソコンから調べてもらったMACアドレスを入力する。

ウ 割当 IP アドレス

事前に割当 IP 一覧表を作成しておき、空きアドレスを利用者に割り当てる。

エ 設定状況

初めてネットワークに接続する利用者の場合が「新規」、そうでない利用者については「修正」を選択する。

オ 入力担当者

あらかじめ入力フォーム作成時に入力している担当者をプルダウンメニューから選択する。

校内IPアドレス設定フォーム

ユーザ名: *半角英数字で入力して下さい

MAC アドレス: : : : : : *例 00:01:80:31:EC:E7

割当IPアドレス: . . . *例 192.168.0.1

設定状況: 新規 修正

入力担当者: 笹野

登録 クリア



校内IPアドレス設定フォーム

ユーザ名: sasano *半角英数字で入力して下さい

MAC アドレス: 01 : e0 : aw : 6e : t2 : e7 *例 00:01:80:31:EC:E7

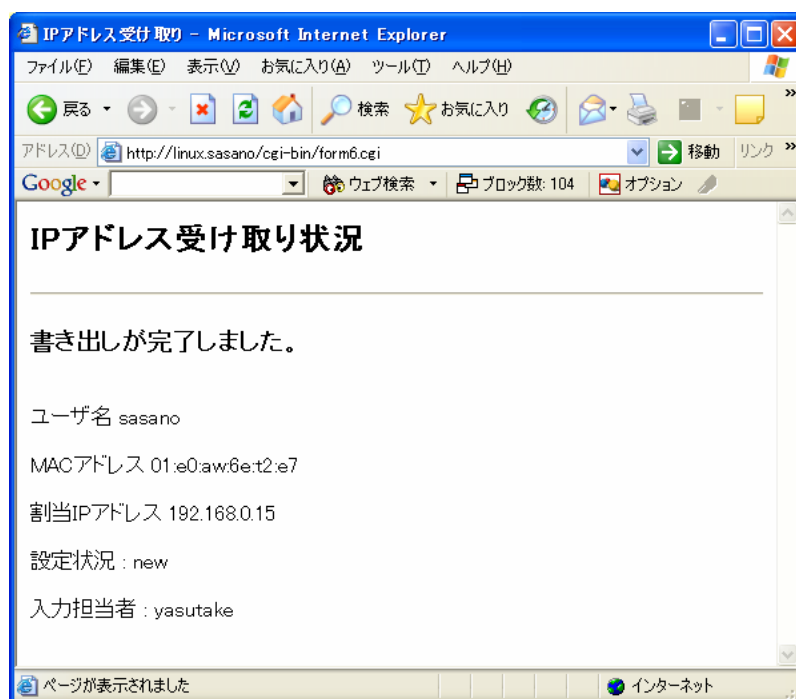
割当IPアドレス: 192 . 168 . 0 . 15 *例 192.168.0.1

設定状況: 新規 修正

入力担当者: 安武

登録 クリア

入力後、「登録」をクリックすると、入力されたデータの受け取り状況が表示される。



2 利用者が行う操作

MAC アドレスを調べる

校内ネットワークに接続したいパソコンの MAC アドレスを調べる。その方法については、以下のようになる。

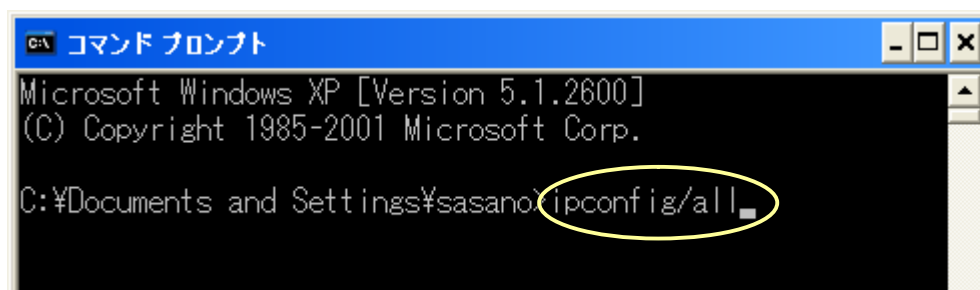
ア コマンドプロンプトの起動

ホストのコマンドプロンプトを使い、NIC (ネットワークインタフェースカード) の MAC アドレスを表示させ、そのアドレスをメモ帳などに書き留めておく。

Windows XP では、「スタート」メニューの「すべてのプログラム」「アクセサリ」「コマンドプロンプト」を選択すると、コマンドプロンプトが起動する。その他の OS では、操作方法は同じであるが、コマンドプロンプトという名称が DOS プロンプトとなっている。

イ コマンドの入力

以下の画面に「ipconfig/all」と入力し、Enter を押す。



構築手順書 「登録端末への DHCP による自動アドレス割当機構」

フォームの作成

1 入力フォーム

入力フォームでは、管理者が利用者のユーザデータを入力しやすく、かつ入力誤りが少なくなるように配慮して作成する。「校内 IP アドレス設定フォーム」では、利用者の最低限必要データとしてユーザ名、MAC アドレスが必要となる。その他に、割り当てる IP アドレスを入力する必要がある。それ以外の情報として、登録するユーザが新規または修正なのか、誰が登録作業を行ったかといった情報を残すために、設定状況と入力担当者の欄を設けている。

ユーザ名

ユーザ名については、利用者を判別する際に利用されるため、ここでは半角英数字で入力するようコメントを表示する。

MAC アドレス

MAC アドレスは、16 進数 12 桁で 2 桁ずつの区切りがあるため、その記述が統一した形で入力できるように半角英数字のみ入力させるようにする。

割当 IP アドレス

ここに入力する IP アドレスは、校内で決めたプライベートアドレスを利用する。別に校内割当 IP 一覧などを作成し、空きアドレスを割り当てるといったことを行う。MAC アドレス同様、半角数字のみの入力となる。

設定状況

これは必ずしも必要ではないが、用途に応じて導入するか検討する。ここでは 2 つを選択するようにしているため、ラジオボタンを採用している。

入力担当者

入力した係りが責任を持つように、また誰が利用者の登録を行ったかわかるように、あらかじめ入力担当の係りの名前をこのページ作成時に入力しておく。ここではプルダウンメニューを使い、入力担当者を選択するようにしている。

登録ボタン

入力が完了すると、「登録」のボタンをクリックすることにより登録作業が終了する。

クリアボタン

入力の中止の際に利用する。

The screenshot shows a web browser window titled "IPアドレス登録 - Microsoft Internet Explorer". The address bar shows "http://linux.sasano/rensyuu/model/form6.html". The page content is titled "校内IPアドレス設定フォーム". It contains the following form elements:

- ユーザ名: [] *半角英数字で入力して下さい
- MAC アドレス: []:[]:[]:[]:[]:[] *例 00:01:80:31:EC:E7
- 割当IPアドレス: [].[].[].[] *例 192.168.0.1
- 設定状況: 新規 修正
- 入力担当者: 笹野 (dropdown menu)
- Buttons: 登録, クリア

2 入力フォームのソースプログラム

ここでは、CGI・Perlのプログラムを使い、入力フォームに必要事項を入力し、「登録」ボタンをクリックすると form6.cgi の画面が戻ってくるようにしている。完成したフォームの保存場所については、Linux サーバ上の / var / www / html / に保存する。ファイル名については任意でよいが、ここでは form.html としている。(/ var / www / html / form.html)

```
<HTML>
<HEAD>
<meta http-equiv="Content-Type" content="text/html; charset=euc-jp">
<TITLE>IPアドレス登録</TITLE>
</HEAD>
<BODY>

<H2>校内IPアドレス設定フォーム</H2>

<FORM METHOD="POST" ACTION="/cgi-bin/form6.cgi">
ユーザ名：
<INPUT TYPE="text" name="name">
*半角英数字で入力して下さい
<P>

MAC アドレス：
<INPUT size="1.5" TYPE="text" name="mac1"> :
<INPUT size="1.5" TYPE="text" name="mac2"> :
<INPUT size="1.5" TYPE="text" name="mac3"> :
<INPUT size="1.5" TYPE="text" name="mac4"> :
<INPUT size="1.5" TYPE="text" name="mac5"> :
<INPUT size="1.5" TYPE="text" name="mac6">
*例 00:01:80:31:EC:E7
<P>

割当IPアドレス：
<INPUT size="2" TYPE="text" name="ip1"> .
<INPUT size="2" TYPE="text" name="ip2"> .
<INPUT size="2" TYPE="text" name="ip3"> .
<INPUT size="2" TYPE="text" name="ip4">
*例 192.168.0.1
<P>

設定状況：
<INPUT TYPE="radio" name="jyoukyou" VALUE="new" CHECKED>新規
<INPUT TYPE="radio" name="jyoukyou" VALUE="correction">修正
<P>

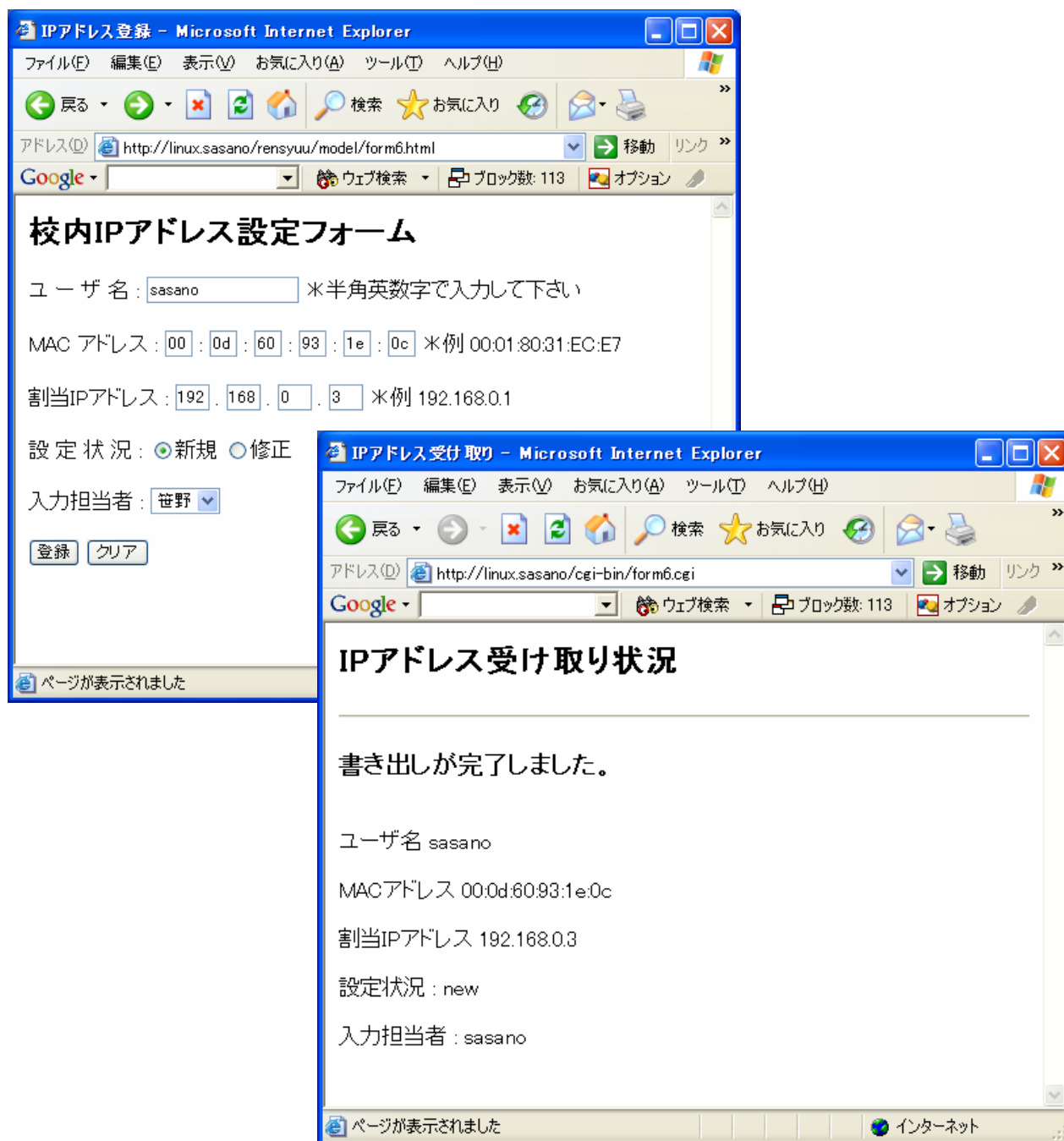
入力担当者：
<SELECT NAME="tantou">
<OPTION SELECTED VALUE="sasano">笹野
<OPTION VALUE="yasutake">安武
<OPTION VALUE="yamauchi">山内
</SELECT>
<P>

<INPUT TYPE="submit" VALUE="登録">
<INPUT TYPE="reset" VALUE="クリア">
</FORM>

</BODY>
</HTML>
```

3 受け取りフォーム

入力フォームに必要事項を入力し、「登録」ボタンをクリックすると「IP アドレス受け取り状況」が表示されるようにする。ここでは、ユーザ名を sasano、MAC アドレスを 00:0d:60:1e:0c、割当 IP アドレスを 192.168.0.3、設定状況を「新規」、入力担当者を「笹野」とし、登録ボタンをクリックした状態である。入力フォーム（校内 IP アドレス設定フォーム）で入力されたデータが、受け取りフォーム（IP アドレス受け取り状況）に表示される。



4 受け取りフォームのソースプログラム

入力フォームで「登録」のボタンをクリックすることにより、受け取りフォームにデータを返し表示させるというアクションだけではなく、ここではそれと同時に dhcpd.conf とバックアップファイルにも書き出すようにしている。dhcpd.conf とバックアップファイル作成については後で述べる。

完成した受け取りフォームの保存場所については、Linux サーバ上の /var/www/cgi-bin/ に保存する。ファイル名については任意でよいが、ここでは form6.cgi としている。(/var/www/cgi-bin/form6.cgi)

```
#!/usr/bin/perl

read(STDIN,$formin,$ENV{'CONTENT_LENGTH'});

@indata = split(/&/,$formin);
foreach $tmp(@indata)
{
    ($name,$value)=split(/=/,$tmp);
    $name{$name}=$value;
}

$macaddr="$name{'mac1'}:$name{'mac2'}:$name{'mac3'}:$name{'mac4'}:$name{'mac5'}:$name{'mac6'}";
$ipaddr="$name{'ip1'}.${name{'ip2'}.${name{'ip3'}.${name{'ip4'}}}";

#backup data
open(OUT,">>/etc/dhcpd-data/bkdata.txt");
print OUT "host ";
print OUT "$name{'name'}";
print OUT " {\n";
print OUT "    hardware ethernet $macaddr";
print OUT ";\n";

print OUT "    fixed-address $ipaddr";
print OUT ";\n";
print OUT "#tantou : $name{'tantou'}\n";
print OUT "#jyoukyou : $name{'jyoukyou'}\n";
print OUT "}\n";
close(OUT);

#dhcpd.conf data
open(OUT,">>/etc/dhcpd-data/test.txt");
print OUT "host ";
print OUT "$name{'name'}";
print OUT " {\n";
print OUT "    hardware ethernet $macaddr";
print OUT ";\n";

print OUT "    fixed-address $ipaddr";
print OUT ";\n";
print OUT "#tantou : $name{'tantou'}\n";
print OUT "#jyoukyou : $name{'jyoukyou'}\n";
print OUT "}\n";
close(OUT);

print "Content-type: text/html\n\n";
print "<META http-equiv=\"Content-Type\" text/html; charset=EUC-JP\">\n";

print "<HTML>\n";
print "<HEAD><TITLE>IPアドレス受け取り</TITLE></HEAD>\n";
print "<BODY>\n";
print "<H2>IPアドレス受け取り状況</H2><HR>\n";

print '<H3>書き出しが完了しました。</H3><BR>';
print "ユーザ名 $name{'name'} <BR><BR>";
print "MACアドレス $name{'mac1'}:$name{'mac2'}:$name{'mac3'}:$name{'mac4'}:$name{'mac5'}:$name{'mac6'} <BR><BR>";
print "割当IPアドレス $name{'ip1'}.${name{'ip2'}.${name{'ip3'}.${name{'ip4'}}} <BR><BR>";
print "設定状況 : $name{'jyoukyou'}<BR><BR>\n";
print "入力担当者 : $name{'tantou'}<BR><BR>\n";

print "</BODY>\n";
print "</HTML>\n";
exit;
```


5 受け取りフォームの解説

\$macaddr ・ \$ipaddr

入力フォームから入力された MAC アドレスと IP アドレスを記録するための書式を定義している。ここで定義された書式を#backup data と#dhcpd.conf data で活用する。

```
$macaddr="$name{'mac1'}:$name{'mac2'}:$name{'mac3'}:$name{'mac4'}:$name{'mac5'}:$name{'mac6'}";  
$ipaddr="$name{'ip1'}.${name{'ip2'}.${name{'ip3'}.${name{'ip4'}}}";
```

#backup data

open 文で、/etc/dhcpd-data/という場所に格納されている bkdata.txt ファイルを開き、print 文の内容を書き込んでから閉じるという内容である。print 文で記述している内容は、dhcpd.conf に利用者を登録するための書式となる。

```
#backup data  
open(OUT, ">>/etc/dhcpd-data/bkdata.txt");  
print OUT "host ";  
print OUT "$name{'name'}";  
print OUT " {\n";  
print OUT "   hardware ethernet $macaddr";  
print OUT ";\n";  
  
print OUT "   fixed-address $ipaddr";  
print OUT ";\n";  
print OUT "#tantou : $name{tantou}\n";  
print OUT "#jyoukyou : $name{jyoukyou}\n";  
print OUT "};\n";  
close(OUT);
```

#dhcpd.conf data

上記の#backup data とほとんど同じであり、保存先と保存するファイル名が異なる程度である。open 文で、/etc/dhcpd-data/という場所に格納されている test.txt ファイルを開き、print 文の内容を書き込んでから閉じるという内容である。print 文で記述している内容は、dhcpd.conf に利用者を登録するための書式となり、このファイルが dhcpd.conf ファイルに直接コピーされる。

```
#dhcpd.conf data  
open(OUT, ">>/etc/dhcpd-data/test.txt");  
print OUT "host ";  
print OUT "$name{'name'}";  
print OUT " {\n";  
print OUT "   hardware ethernet $macaddr";  
print OUT ";\n";  
  
print OUT "   fixed-address $ipaddr";  
print OUT ";\n";  
print OUT "#tantou : $name{tantou}\n";  
print OUT "#jyoukyou : $name{jyoukyou}\n";  
print OUT "};\n";  
close(OUT);
```

```
ddns-update-style interim;  
subnet 192.168.0.0 netmask 255.255.255.0 {  
    range 192.168.0.10 192.168.0.17;  
    option subnet-mask 255.255.255.0;  
    option routers 192.168.0.1;  
    option broadcast-address 192.168.0.255;  
    option domain-name-servers _____, _____, _____;  
}  
host work {  
    hardware ethernet 00:0d:60:93:1e:0c; # work  
    fixed-address 192.168.0.2;  
}  
host sasano {  
    hardware ethernet 00:0d:60:93:1e:0c;  
    fixed-address 192.168.0.3;  
    #tantou : sasano  
    #jyoukyou : new  
}
```

dhcpd.conf ファイル

受け取りフォーム

以下のプログラムが受け取りフォームのソースとなる。

```
print "Content-type: text/html\n\n";
print "<META http-equiv=\"Content-Type\"text/html;
charset=EUC-JP\">\n";

print "<HTML>\n";
print "<HEAD><TITLE>IPアドレス受け取り</TITLE></HEAD>\n";
print "<BODY>\n";
print "<H2>IPアドレス受け取り状況</H2><HR>\n";

print '<H3>書き出しが完了しました。</H3><BR>';
print "ユーザ名 $name{'name'} <BR><BR>";
print "MACアドレス $name{'mac1'}:$name{'mac2'}:$name{'mac3'}:$name{'mac4'}:
$name{'mac5'}:$name{'mac6'} <BR><BR>";
print "割当IPアドレス $name{'ip1'}.$name{'ip2'}.$name{'ip3'}.$name{'ip4'}
<BR><BR>";
print "設定状況 : $name{'jyoukyou'}<BR><BR>\n";
print "入力担当者 : $name{'tantou'}<BR><BR>\n";

print "</BODY>\n";
print "</HTML>\n";
exit;
```

IPアドレス受け取り状況

書き出しが完了しました。

ユーザ名 sasano

MACアドレス 00:0d:60:93:1e:0c

割当IPアドレス 192.168.0.3

設定状況 : new

入力担当者 : sasano

print "ユーザ名 \$name{'name'}";

print "MAC アドレス \$name{'mac1'}: ~ \$name{'mac6'}";

print "割当 IP アドレス \$name{'ip1'}: ~ \$name{'ip4'}";

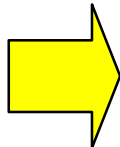
print "設定状況 \$name{'jyoukyou'}";

print "入力担当者 \$name{'tantou'}";

6 各動作の流れ

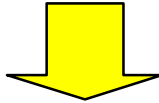
ブラウザで入力フォームを表示し、利用者の必要事項を入力する。「登録」ボタンをクリックすると受け取りフォームに入力データが入ったものが表示されると同時に、dhcpd.conf の元になるデータ（この場合のファイル名：test.txt）とバックアップデータ（bkdata.txt）がテキストファイルとして保存される。この2つのファイルは、既存のファイルに追加されたデータを上書きして保存するようになる。受け取りフォームのソースプログラムの「#backup data」と「#dhcpd.conf data」の部分がそれぞれの操作

の内容である。



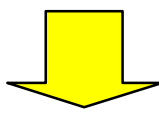
```
ddns-update-style interin;
subnet 192.168.0.0 netmask 255.255.255.0 {
  range 192.168.0.10 192.168.0.17;
  option subnet mask 255.255.255.0;
  option routers 192.168.0.1;
  option broadcast-address 192.168.0.255;
  option domain-name-servers [redacted];
}
host work {
  hardware ethernet 00:0d:80:93:1c:0e; # work
  fixed-address 192.168.0.2;
}
host sasano {
  hardware ethernet 00:0d:60:93:1c:0c;
  fixed address 192.168.0.3;
  #lan100 : sasano
  #jyoukyou : new
}
```

bkdata.txt (backup data)



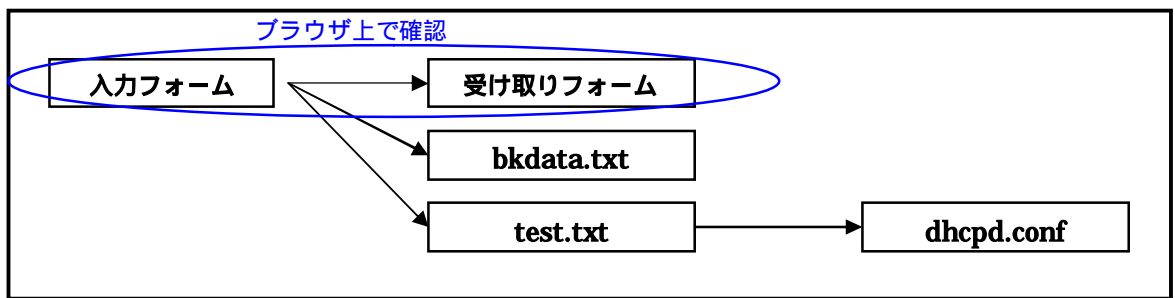
```
ddns-update-style interin;
subnet 192.168.0.0 netmask 255.255.255.0 {
  range 192.168.0.10 192.168.0.17;
  option subnet mask 255.255.255.0;
  option routers 192.168.0.1;
  option broadcast-address 192.168.0.255;
  option domain-name-servers [redacted];
}
host work {
  hardware ethernet 00:0d:80:93:1c:0e; # work
  fixed-address 192.168.0.2;
}
host sasano {
  hardware ethernet 00:0d:60:93:1c:0c;
  fixed address 192.168.0.3;
  #lan100 : sasano
  #jyoukyou : new
}
```

test.txt (dhcpd.conf data)



```
ddns-update-style interin;
subnet 192.168.0.0 netmask 255.255.255.0 {
  range 192.168.0.10 192.168.0.17;
  option subnet mask 255.255.255.0;
  option routers 192.168.0.1;
  option broadcast-address 192.168.0.255;
  option domain-name-servers [redacted];
}
host work {
  hardware ethernet 00:0d:80:93:1c:0e; # work
  fixed-address 192.168.0.2;
}
host sasano {
  hardware ethernet 00:0d:60:93:1c:0c;
  fixed address 192.168.0.3;
  #lan100 : sasano
  #jyoukyou : new
}
```

dhcpd.conf ファイル



入力フォームで入力されたデータが、受け取りフォーム・bkdata.txt・test.txt の3つファイルに渡され、受け取りフォームはブラウザに表示され、bkdata.txt と test.txt ファイルは /etc/dhcpd-data/ に保存される。また、test.txt は、dhcpd.conf (/etc/dhcpd.conf) に書き替えられる。

このような流れにより、新たに登録された利用者のデータが dhcpd.conf とバックアップファイルに追加される。

dhcpd.conf とバックアップファイルの作成

1 dhcpd.conf の reload

入力フォームから入力されたデータが bkdata.txt と test.txt に書き込まれることについては、上記で説明したが、test.txt として作成されたファイルを dhcpd.conf にどのようにして反映させているかという点、reload (再読み込み) させている。dhcpd.conf のファイルは、DHCP サーバの中核的なプログラムのため、フォームで操作を行った内容をそのまま書き込ませるとトラブルの原因になりかねない。また、Linux では dhcpd.conf ファイルの書き換えを行うと DHCP サーバを再起動させなければならない。そこで、一旦別のテキストファイルに書き込んだファイルを dhcpd.conf に再読み込みさせるといったイメージとなる。そのプログラム例としては、以下のようになる。

```
#!/bin/sh
cd /etc/dhcpd-data
if [ -f test.txt ]; then
    mv /etc/dhcpd.conf /etc/dhcpd.conf-bak
    cp test.txt /etc/dhcpd.conf
    kill -TERM `cat /var/run/dhcpd.pid`
    /usr/sbin/dhcpd eth1
fi
```

ここでは、/etc/dhcpd-data/という記憶場所に、dhcpd-conf-reload というファイル名で上記のファイルを保存する。こうすることにより、入力フォームで入力されたデータが、dhcpd.conf ファイルに反映され、上書き保存される。

2 バックアップファイルの作成

バックアップファイルの作成については、上記でも述べたように受け取りフォームのプログラムに記述されている (#backup data) のところの open 文で、/etc/dhcpd-data/という場所に格納されている bkdata.txt ファイルを開き、print 文の内容を書き込んでから閉じる。当然上書きされるということになる。このファイルがあれば dhcpd.conf ファイルが壊れたりしても、dhcpd.conf ファイルの内容と同じものをほぼ同時にバックアップファイルとして作成しているため、バックアップファイル (bkdata.txt) のファイル名を変更することにより dhcpd.conf ファイルを再生することができる。

3 バックアップのタイミング

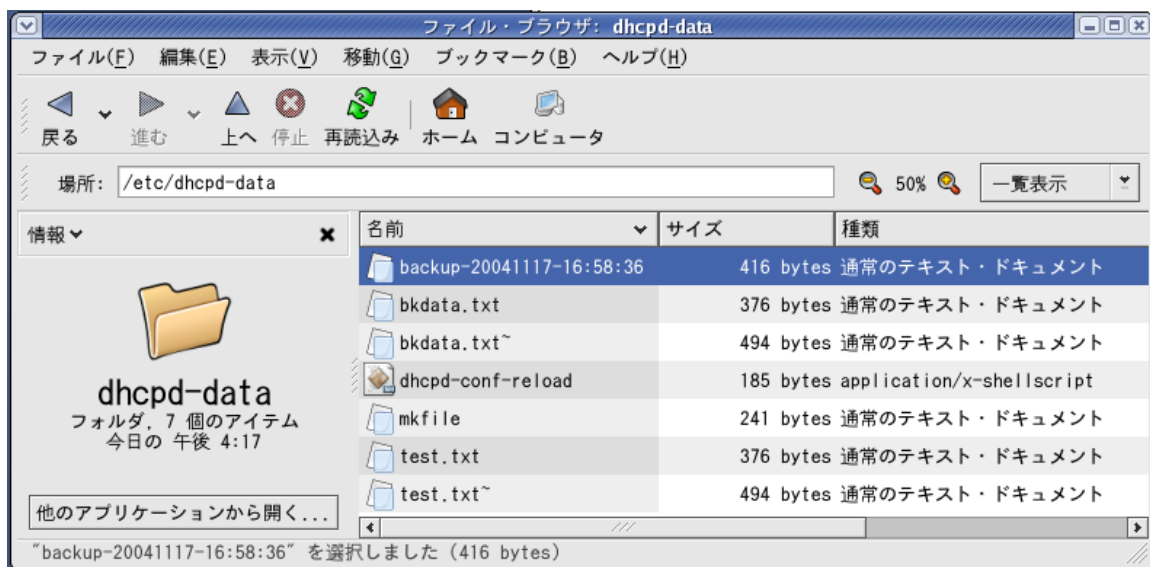
上記のように、利用者を登録する都度バックアップファイルを作成しているが、更に Linux の cron を使ったタイマー的なバックアップを行う。ここでは、毎日 5 分おきにバックアップの更新を行うようにしている。

```
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (/tmp/crontab.5866 installed on Wed Nov 17 16:45:49 2004)
# (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
0,5,10,15,20,25,30,35,40,46,50,55 * * * * /etc/dhcpd-data/dhcpd-conf-reload
```

プログラムといっても、上記プログラム例の 4 行目だけである。左から 5 分おきに時間指定がなされている。この見方については、0,5,10,15,~50,55 の部分が、分 (minutes) のみの指定で、その後の * が時 (hour)、その次の * が日 (day)、月 (month)、年 (year) となっている。このように細かく指定することができる。

このファイルについては、/var/spool/cron/という場所にある root に 4 行目だけを書き足し保存すればよい。また、バックアップファイルを作成する際に、日付と時間入りのファイル名で保存するプログラムの例を示す。このプログラムについても、/etc/dhcpd-data/という場所に mkfile というファイル名で保存している。

```
#!/perl
($sec,$min,$hour,$mday,$mon,$year,$wday,$yday,$isdst) = localtime(time);
$mon = $mon + 1;
$year = $year + 1900;
$sti = "$year$mon$mday-$hour:$min:$sec";
open(FILE, "> backup-$sti");
print FILE "current date-time is $sti\n";
close(FILE);
```



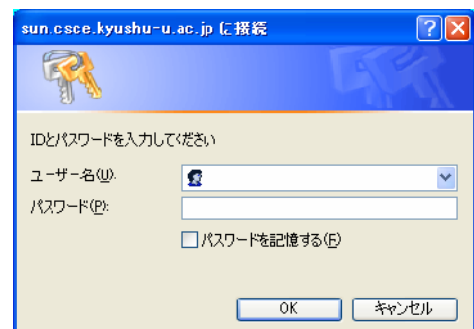
ユーザ認証用フォームの作成

1 パスワードファイルの作成

今回は BASIC 認証を利用したため、その作成について簡単に述べておく。

BASIC 認証でアクセス制限を行うには、「.htaccess ファイル」と「パスワードファイル」の 2 つが必要である。まず、「パスワードファイル」を作成する。ファイル名は特に決まりはないが、一般的に「.htpasswd」というファイル名が用いられる。

このファイルには、許可するユーザ名とパスワードを保存する。このとき、パスワードを暗号化の必要があり、パスワードを暗号化する方法について 2 つの方法を紹介しておきたい。



2 パスワードの暗号化

パスワードを暗号化する場合、サーバのコンソールにコマンドを入力して作成する方法と、ウェブ上にある暗号化ツールを使うという方法がある。

サーバ上での暗号化

サーバのコンソールに telnet や SSH で接続し、htpasswd というコマンドを利用してパスワードフ

ファイルを作成することができる。次の例では、現在のフォルダに.htpasswd というファイルを新しく作成し、sasano というユーザを登録する。パスワードを聞かれるため、同じパスワードを2回入力する(画面には表示されない)。

「-c」はオプションで、パスワードファイルを新しく作成するという意味である。すでにあるファイルにユーザを追加したい場合は不要。作成された.htpasswd は、root 権限で作成すると/root/に保存され、ユーザモードで作成すると、/home/sasano/に保存される。

```
%> htpasswd -c .htpasswd sasano
New password: test
Re-type password: test
Adding password for user sasano
```

暗号化ツールを使う

ウェブ上には、多くの暗号化を行うページが存在し、誰でも自由に利用できるものとして提供されているページがある。そのページにアクセスし、ID とパスワードを入力するとパスワードが暗号化される。 <BASIC 認証用パスワード暗号化ツール <http://orange-factory.com/tool/crypt.cgi> >

そこで暗号化されたパスワードを以下のようにテキストエディタ(メモ帳等)に貼り付け、パスワードファイルとして保存すればよい。(ファイル名: .htpasswd) 保存する場所は特に指定されていないため、ここでは/var/www/html/rensyuu/model/に保存した。

```
sasano:E13BRLEjwKRLU
```

3 「.htaccess ファイル」の作成

アクセス制限したいフォルダに「.htaccess」という名前のファイルを作る。これも、内容は普通のテキストファイルである。パスワードファイルと違い、必ずこの名前にする必要がある。

認証用のフォームについては、校内の IP アドレス設定のためのフォームを利用者が閲覧できないようにするための工夫として作成する。これは、制限付きでウェブページを公開する際に用いられる。

作成方法としては、テキストエディタ(メモ帳等)で以下のプログラムコードを入力し、「.htaccess」(拡張子が htaccess ということで、ドットが必要である。)といったファイル名で保存する。保存する場所は、入力フォームを保存しているディレクトリに置いて制限をかけるということになる。

```
AuthType Basic
AuthUserFile /var/www/html/rensyuu/model/.htpasswd
AuthGroupFile /dev/null
AuthName "IDとパスワードを入力してください。"
<limit GET POST>
require valid-user
</limit>
```

- 1行目「AuthType Basic」:

認証方式を設定する。Basic 認証を利用する時には「Basic」を指定する。これは、ID とパスワードによるアクセス制御(Basic 認証)を表す。

- 2行目「AuthUserFile」:

準備したパスワードファイルを、フルパスで指定する。Web ページのルートからのパスではなく、

サーバ上パスとなるため、注意が必要である。

・ 3 行目「**AuthGroupFile**」:

グループファイル名を指定する。グループを使わないときには「**/dev/null**」を指定する。グループファイルを使うと、あるフォルダは全員閲覧できて、別のフォルダは特定のグループの人だけ閲覧可能、というようなことを実現できる。

・ 4 行目「**AuthName**」:

ユーザ名・パスワードを入力するダイアログボックスに表示されるメッセージ。全角文字も指定できるが、文字化けの可能性はある。スペースを含むメッセージを設定するときには、メッセージ全体をダブルクォートで括る。

・ 5 行目「**require valid-user**」:

認証させるユーザを指定する。「**valid-user**」と指定すると、「**AuthUserFile**」で指定したファイル内の全ユーザが認証される。「**user ユーザ名**」と指定すると、そのユーザだけが認証される。「**group グループ名**」と指定すると、「**AuthGroupFile**」内に書かれた該当グループのユーザだけが認証される。

その他

以上のファイルを作成し、Linux サーバ上に保存しておけば、DHCP 機能を用いた利用者の固定 IP アドレス割り当てを実現させることができる。

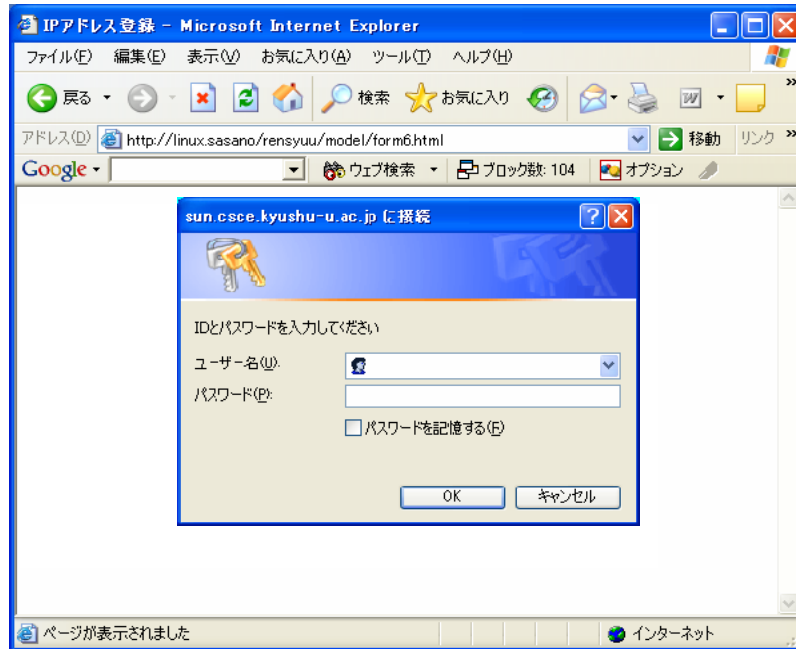
システム開発の構築手順として、以上のように記述したが、これは実行ファイル(exe)とは異なるため、様々な記録媒体に保存して配布することができない。そのため、以上のような操作をコマンドラインで記述していかなければならない。ぜひ、各学校の状況に応じて改良し、活用していただきたいと思う。

使用説明書 「登録端末への DHCP による自動アドレス割当機構」

ネットワーク管理者（入力担当者）が行う操作

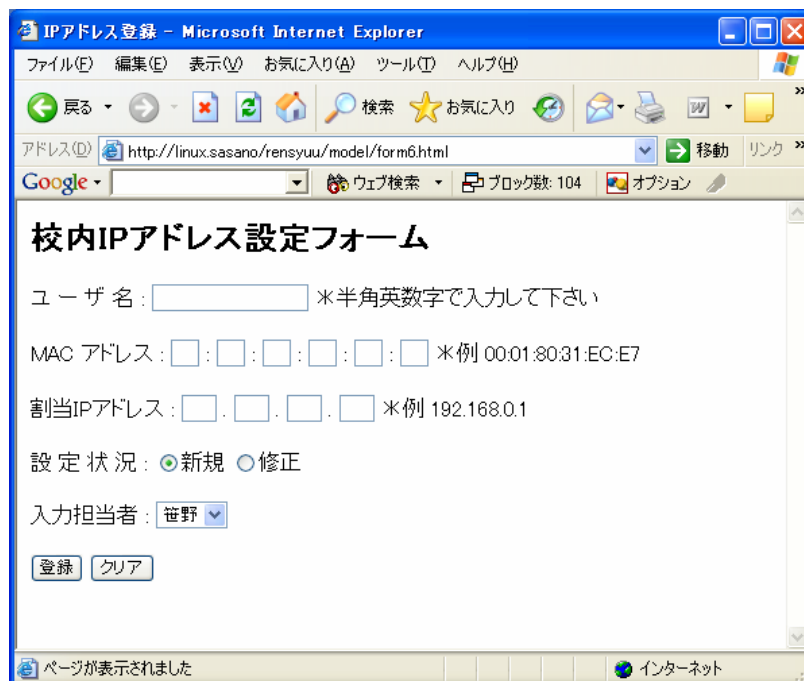
1 メニューを開く

Linux サーバ上にあるフォームをブラウザで開く。そうすると、ユーザ認証用のフォームが現れ、あらかじめ登録している入力担当以外は入力操作等できない。入力担当者は、ユーザ ID とパスワードを入力し、「OK」をクリックする。



2 入力フォームで必要事項入力

必要事項（ユーザ名・MAC アドレス・割当 IP アドレス・設定状況・入力担当者）を入力し、「登録」をクリックする。



ユーザ名

利用者の ID を入力する。

MAC アドレス

利用者に自分のパソコンから調べてもらった MAC アドレスを入力する。

割当 IP アドレス

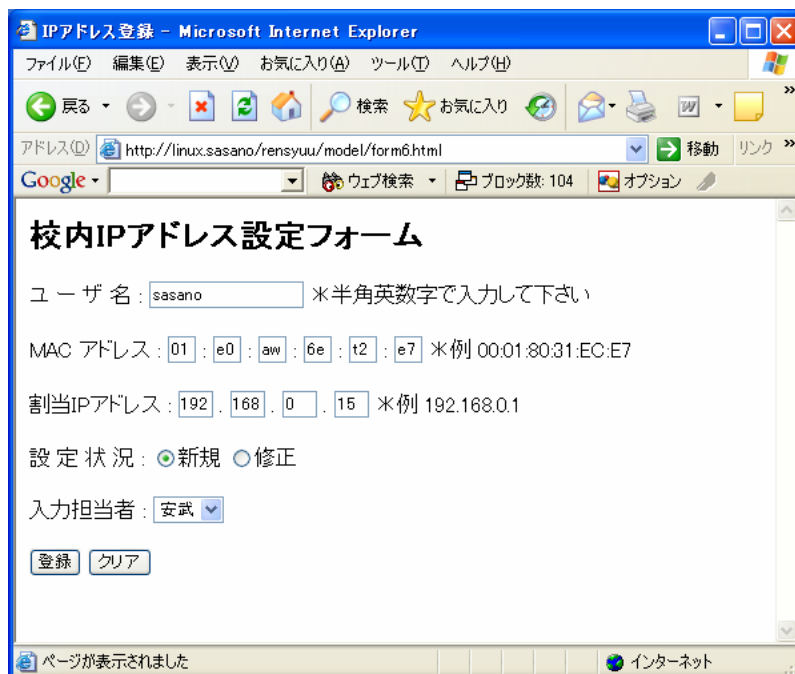
事前に割当 IP 一覧表を作成しておき、空きアドレスを利用者に割り当てる。

設定状況

初めてネットワークに接続する利用者の場合が「新規」、そうでない利用者については「修正」を選択する。

入力担当者

あらかじめ入力フォーム作成時に入力している担当者をプルダウンメニューから選択する。



校内IPアドレス設定フォーム

ユーザ名 : sasano *半角英数字で入力して下さい

MAC アドレス : 01 : e0 : aw : 6e : t2 : e7 *例 00:01:80:31:EC:E7

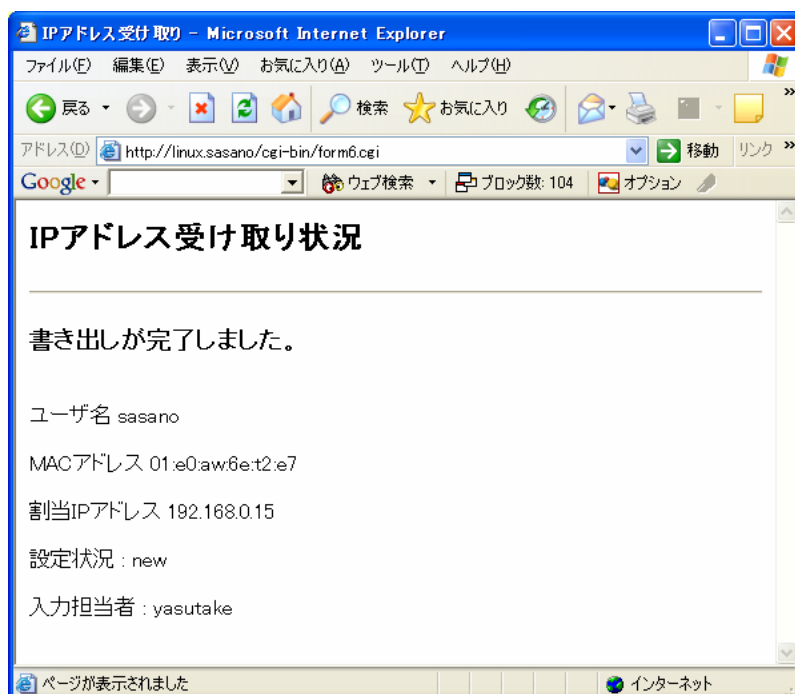
割当IPアドレス : 192 . 168 . 0 . 15 *例 192.168.0.1

設定状況 : 新規 修正

入力担当者 : 安武

登録 クリア

入力後、「登録」をクリックすると、入力されたデータの受け取り状況が表示される。



IPアドレス受け取り状況

書き出しが完了しました。

ユーザ名 sasano

MACアドレス 01:e0:aw:6e:t2:e7

割当IPアドレス 192.168.0.15

設定状況 : new

入力担当者 : yasutake

利用者が行う操作

1 MAC アドレスを調べる

校内ネットワークに接続したいパソコンの MAC アドレスを調べる。その方法については、以下のようになる。

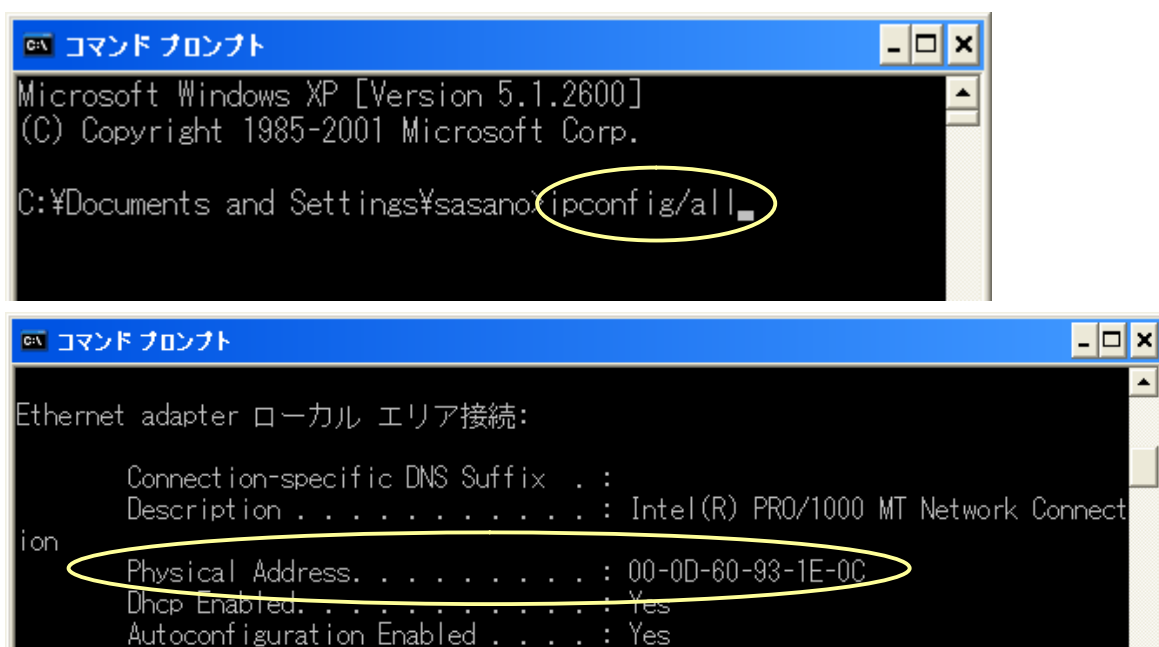
コマンドプロンプトの起動

ホストのコマンドプロンプトを使い、NIC (ネットワークインタフェースカード) の MAC アドレスを表示させ、そのアドレスをメモ帳などに書き留めておく。

Windows XP では、「スタート」メニューの「すべてのプログラム」「アクセサリ」「コマンドプロンプト」を選択すると、コマンドプロンプトが起動する。その他の OS では、操作方法は同じであるが、コマンドプロンプトという名称が DOS プロンプトとなっている。

コマンドの入力

以下の画面に「ipconfig/all」と入力し、Enter を押す。



そうすると、パソコンにおける現在の情報が表示され、その中の「Physical Address」の部分 MAC アドレスとなる。ここでは、「00-0D-60-93-1E-0C」が MAC アドレスである。

2 MAC アドレスの連絡

16 進数 12 桁で表示されたアドレスを所定の用紙 (例 : 校内ネットワーク接続申請用紙) に記入し、ネットワーク管理者または入力担当者に提出する。

3 校内ネットワークへの接続

ネットワーク管理者から接続設定終了の連絡を受けた後、ネットワークに接続するための LAN ケーブルを、校内に設置されている HUB (またはスイッチ) と自分のパソコンとをつなぐ。

校内ネットワーク接続設定システムの開発 ～DHCPサーバの固定IPアドレスの割り当て～

独立行政法人教員研修センター 研修員 笹野 明裕

研修場所：九州大学大学院システム情報科学研究院
所 属：福岡県立宇美商業高等学校

1

1 開発の動機

(1) 現在の状況

本校では、教員が個人のパソコンを学校に持ち込みネットワークに接続する事例がしばしばみられる。その際、ネットワークに関する知識がない教員に対しては、不正な設定(誤ったデータの入力や重複したIPアドレス等の入力)を避けるため、専門知識を有する教員が個別に対応している状況にある。

利用者がパソコンを持ち込んだら

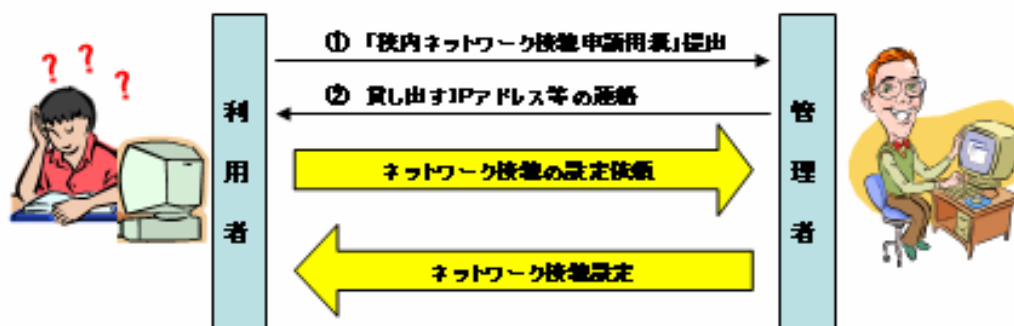


- ① 利用者が校内ネットワークに接続する場合、「校内ネットワーク接続申請用紙」に必要事項を記入し、ネットワーク管理担当者へ提出する。
- ② ネットワーク管理担当者は、受け取った申請用紙から新しいユーザを作成し、ユーザIDとパスワード、グループ等を管理用のサーバに登録し、空きIPアドレスを利用者に連絡する。
- ③ 利用者は、ネットワーク管理担当者から連絡を受け、「ネットワーク接続マニュアル」を見ながらIPアドレスとゲートウェイ等を各自で設定する。
各自で設定できない利用者は、ネットワーク管理担当者にネットワーク接続のための設定を依頼する。

2

1 開発の動機

(1)現在の状況



利用者が自分で設定できない場合は、ネットワーク管理担当者にネットワーク接続の設定を依頼し、ネットワーク担当者がその作業を行わなければならない。

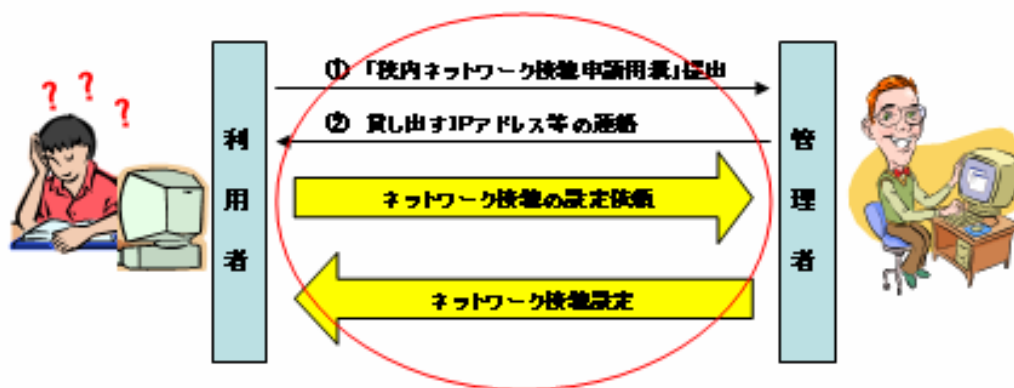
問題点として、

- ① 利用者が行う作業としては高負である。
- ② 依頼を受けた担当者は、自分の仕事の時間を奪われる。
- ③ 利用者が誤ったデータを入力する可能性がある。

3

1 開発の動機

(2)何を改善すべきか

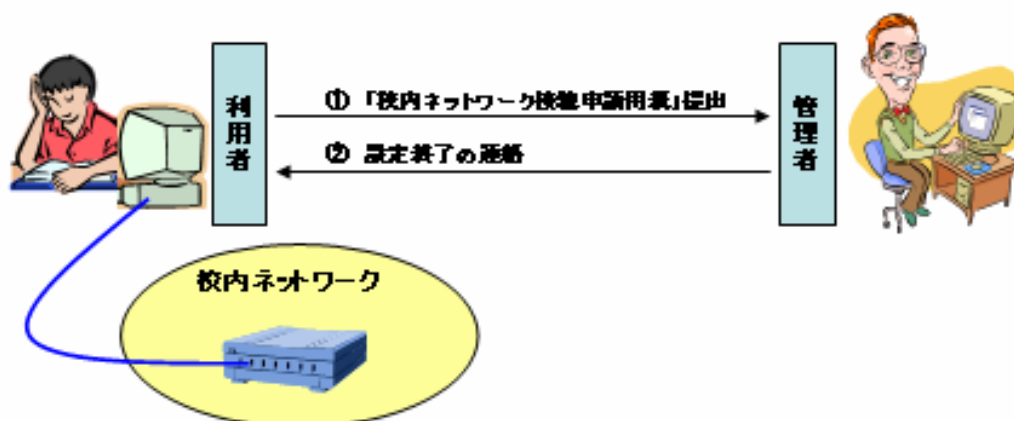


上記部分の簡略化と、現在の問題点を解決する方法として、利用者が行うべきネットワーク接続のための設定を、自動で行うようにするシステムの開発に着手した。

4

1 開発の動機

(3) 利用者が校内ネットワークへ接続する方法



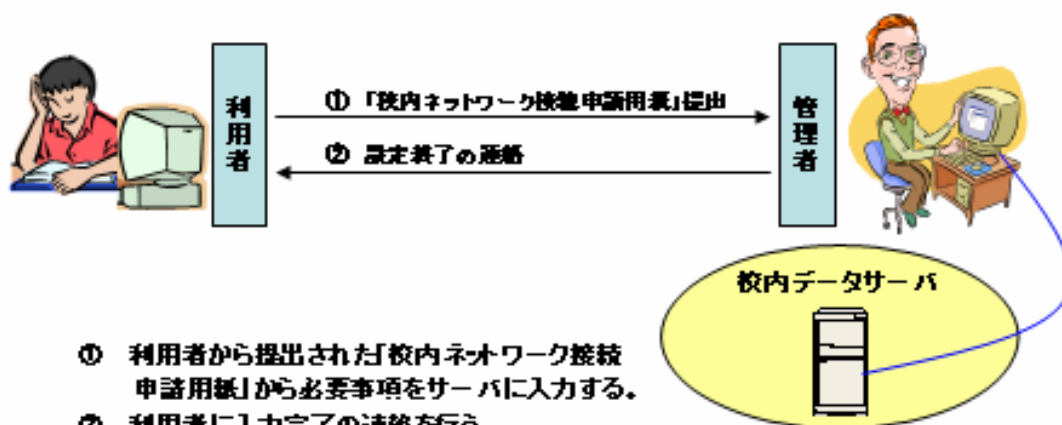
- ① 「校内ネットワーク接続申請用紙」をネットワーク管理担当者へ提出する。
- ② 持ち込まれた利用者のパソコンをLANケーブルで校内ネットワークに接続する。接続完了！ インターネットもファイルサーバも使える。

※ 校内ネットワーク接続に必要な機器等
個人のパソコン・LANケーブル

5

1 開発の動機

(4) ネットワーク管理者が行う作業



- ① 利用者から提出された「校内ネットワーク接続申請用紙」から必要事項をサーバに入力する。
- ② 利用者に入力完了の連絡を行う。

6

2 開発の概要

(1)どのようなシステムを開発するか

- ・利用者が行うべきネットワーク接続のための設定を自動化する。
- ・管理者の入力・設定等の負担軽減を可能にする。
(入力画面はGUIで入力すべき項目を最小限に)
- ・利用者のパソコン設定に時間を奪われない。
- ・定期的なバックアップを自動で行う。
- ・利用者に割り当てたアドレスを管理できる。

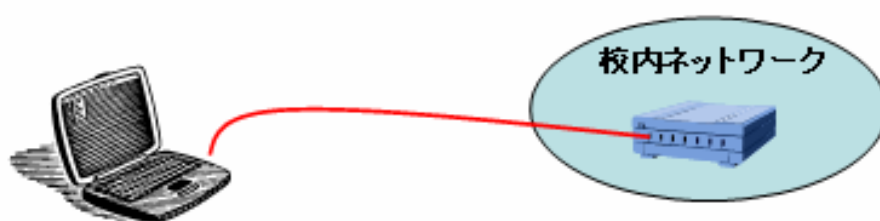


このようなシステムを開発する！

7

2 開発の概要

(2)利用者



- ① 「校内ネットワーク接続申請紙」に「ユーザ名」とMACアドレスを記入して、ネットワーク管理担当者へ提出する。
- ② 持ち込まれた個人用のパソコンをLANケーブルで校内ネットワークに接続する。

簡単にネットワークへの接続が完了する。

8

2 開発の概要

(3) 管理者



- ① 利用者から受け取ったユーザ名とMACアドレス、IPアドレス割当一覧から割当可能アドレスを入力する。
- ② 利用者へ設定完了の連絡を行う。
※ 誰がどのアドレスを使用しているか把握できる。

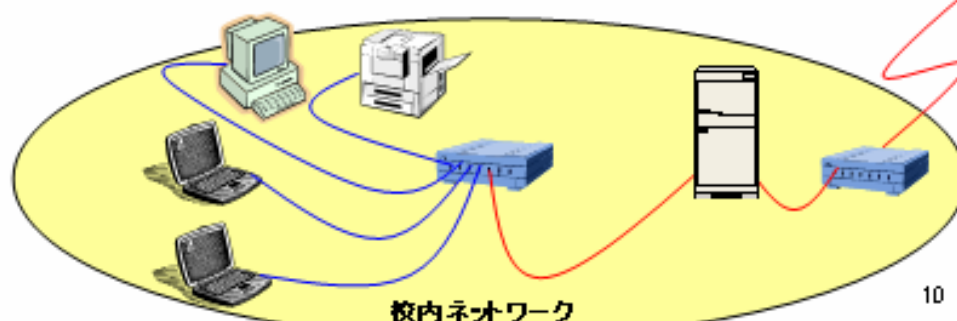
9

2 開発の概要

(4) 運用にあたって

運用については、

- ① 校内ネットワークが構築されており、職員室内にスイッチやHUBが設置されておかなければならない。
- ② 開発したシステムは、Linuxサーバ用であり、Windows系のサーバでは使用できない。そのため、Linuxサーバがネットワーク内に接続されていなければならない。
- ③ 個人用のパソコンをネットワークに接続するためには、LANケーブルか無線LANが必要となる。
- ④ ユーザ管理を行うためには、別に利用者へIPアドレスを割り当てた一覧を作成しておかなければならない。



10

3 成果物の公開などについて

- Linux サーバの導入に関するマニュアル作成したものを、研修成果として文書として残す。
- 登録端末へのDHCPによる自動アドレス割振り機構仕様書、設計書、使用説明書および成果物(プログラムコード)を研修成果として文書として残す。必要に応じて、各学校に使っていただくことを念頭に置き作成する。

11

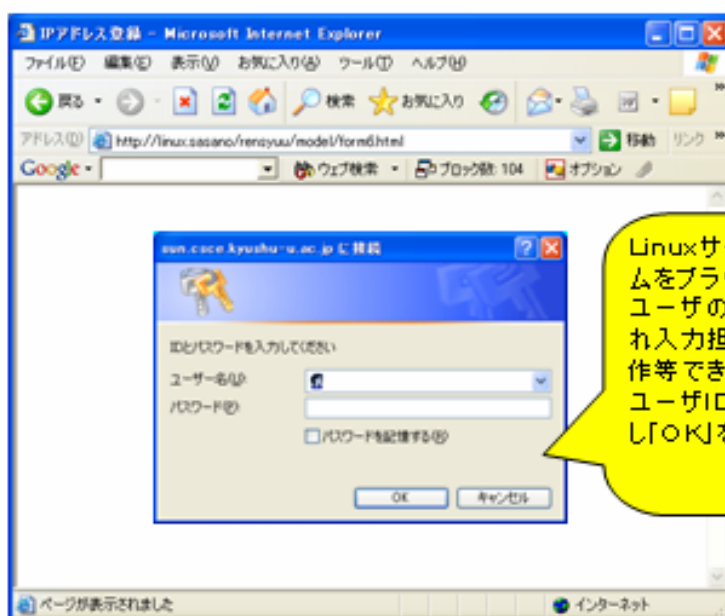
4 成果物の利用計画

- 宇美商業高校においては、H16年2月に調達した Linux サーバの活用を計画しているため、その活用計画の一部に本成果物を導入し活用する。
- 今回のソフトウェア開発環境の研修成果を生かし、ネットワーク管理を行う教員の労力を軽減するシステムを企画したい。
- 導入希望の学校へは、仕様書、設計書、使用説明書および成果物(プログラムコード)を配布する。

12

5 システムの紹介

(1) 入力フォームを開く

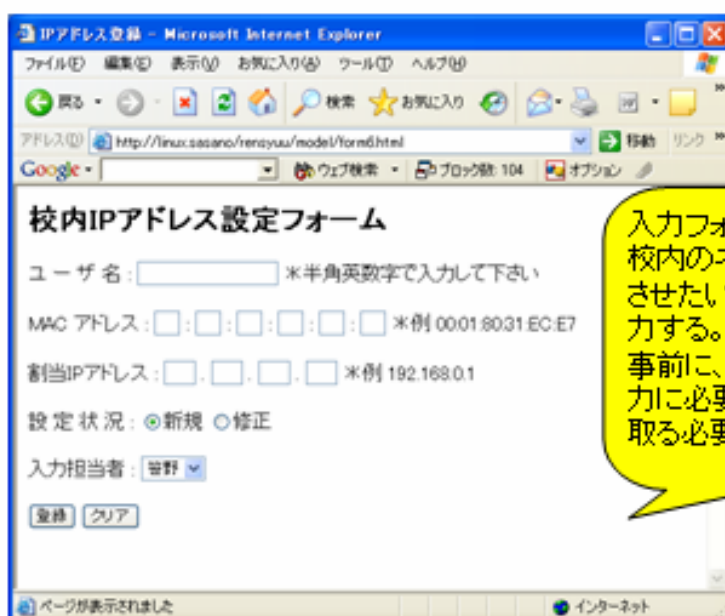


Linuxサーバ上にあるフォームをブラウザで呼び出すが、ユーザの認証フォームが現われ入力担当者以外は入力操作等できないようにする。ユーザIDとパスワードを入力し「OK」をクリックする。

13

5 システムの紹介

(1) 入力フォームを開く



入力フォームが表示され、校内のネットワークに参加させたい教員のデータを入力する。事前に、その教員から入力に必要なデータを受け取る必要がある。

14

5 システムの紹介

(1) 入力フォームを開く

本校では、校内ネットワーク接続申請用紙を作成し、それに記入後提出していただいている。

校内ネットワーク接続申請用紙(例)

- 1 ネットワークに参加するためのユーザ名を決めて、記入してください。
ユーザ名() ※ 英数字で記入
- 2 ネットワークに接続するPCから、MACアドレスを調べ、そのアドレス(英数字12文字)を書き写してください。(別紙説明資料参照)
例 ab : 02 : cd : 01 : ef : ab (: : : :)

※ その他の項目については、ここでは省略する。

15

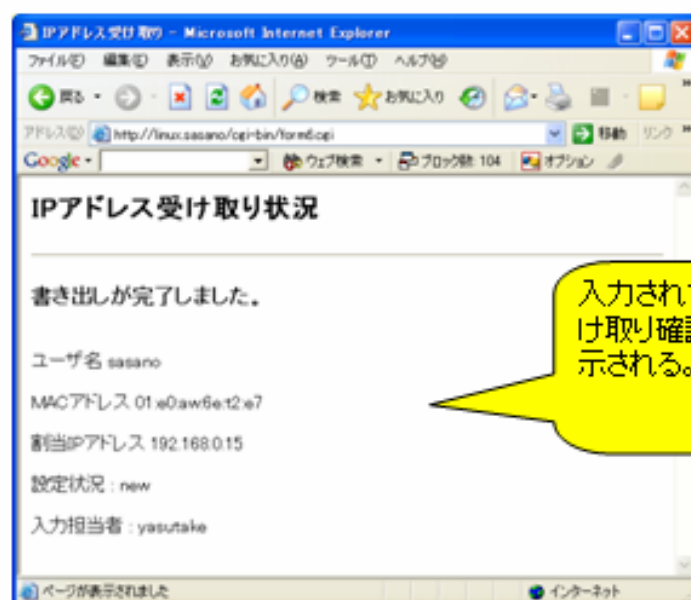
5 システムの紹介

(1) 入力フォームを開く

16

5 システムの紹介

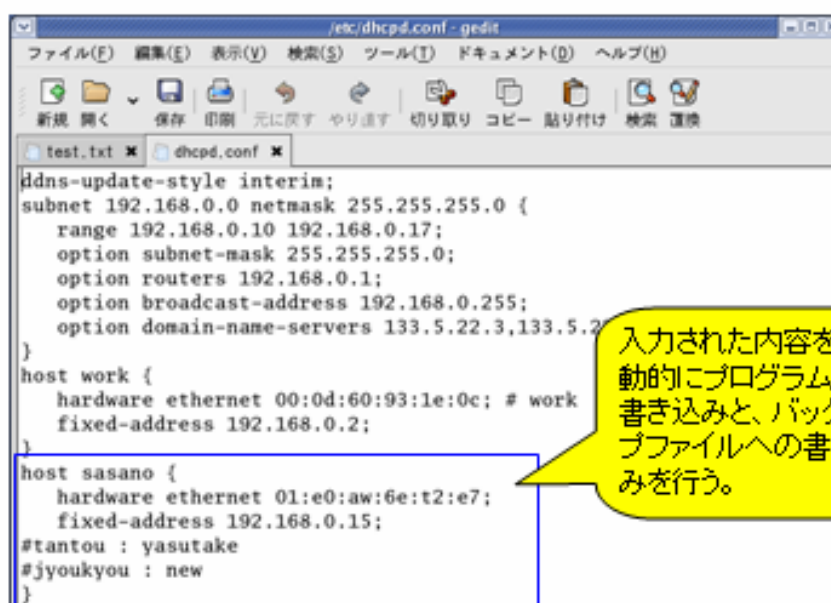
(2) 受け取り確認フォーム



17

5 システムの紹介

(3) DHCPサーバ(dhcpd.conf)での登録状況



18

5 システムの紹介

(3) DHCPサーバ(バックアップファイル)での登録状況

```
ddns-update-style interim;
subnet 192.168.0.0 netmask 255.255.255.0 {
  range 192.168.0.10 192.168.0.17;
  option subnet-mask 255.255.255.0;
  option routers 192.168.0.1;
  option broadcast-address 192.168.0.255;
  option domain-name-servers 133.5.22.3,133.5.2
}
host work {
  hardware ethernet 00:0d:60:93:1e:0c; # work
  fixed-address 192.168.0.2;
}
host sasano {
  hardware ethernet 01:e0:aw:6e:t2:e7;
  fixed-address 192.168.0.15;
  #tantou : yasutake
  #jyoukyou : new
}
```

バックアップファイルへ追加書き込みが行われた内容。プログラムに追加された内容とももちろん同じである。

19

6 まとめ

開発したシステムを導入することにより、

- ① 利用者による不正な設定を避ける。
- ② 利用者にとっては簡単に校内のネットワークへ接続できる。
- ③ 管理者の手を煩わすことがない。
- ④ 管理者による利用者の登録がGUI環境で容易にできる。
- ⑤ 自動で定期的にバックアップファイルが更新される。
- ⑥ 登録者の認証を行い、入力担当者以外は操作できない。
- ⑦ 不慮のトラブル等で登録データが消えても、復旧作業が容易に行える。

以上のように、校内ネットワークに接続するための作業の簡略化と、本校における現在の問題点の解決策として、利用者が行うべきネットワーク接続の設定を、サーバのDHCP機能を使って自動で行うように考えた。

20

開発したシステムの有用性について

学校訪問での聞き取り調査を実施した際、対応していただいた情報担当およびネットワーク管理者の先生方に対して、私が作成したシステムを紹介し、各学校での有用性または必要性について調査を行った。

このシステムは、Linux サーバ上で動作するプログラムであり、個人所有の持ち込みパソコンによる校内ネットワークへの接続設定における職員の不正な設定（誤ったデータの入力や重複した IP アドレス等の入力）を避け、利用者側の負担軽減と、ネットワーク管理者側の作業軽減を目指したシステムである。そのシステムは、あらかじめ登録された端末への DHCP 機能による IP アドレスの自動割当機構を実現するものであり、端末登録を GUI で簡単に操作を行うことができるようにしている。また、DHCP サーバの設定ファイルは難解で、編集にあたっては専門的知識が必要となり、文法ミスがあると正常に稼動しないため、このようなシステムを企画し、入出力画面の作成および入力されたデータの定期的なバックアップまでを行うことが可能である。このシステムを用いることで、現在の問題点の一つについては解決することが十分期待できる。

1 各学校からの回答

(1) 必要と答えた学校

このシステムを必要と回答していただいた学校は、15校中4校（県立3校、私立1校）であった。その4校では、個人所有のパソコンを校内ネットワークへ接続させるための設定を手動で行っているか、あるいは DHCP 機能を用いて自動で IP アドレス等を配布しているため、配布先のパソコンが把握できないという問題点を抱えていた。そこで、私が作成したシステムを紹介させていただいたところ、非常に興味を持っていただき、Linux サーバの導入についても検討したいというご意見をいただくことができた。この4校のネットワーク接続設定の状況および、その問題点については、所属校と非常によく似た状況であった。

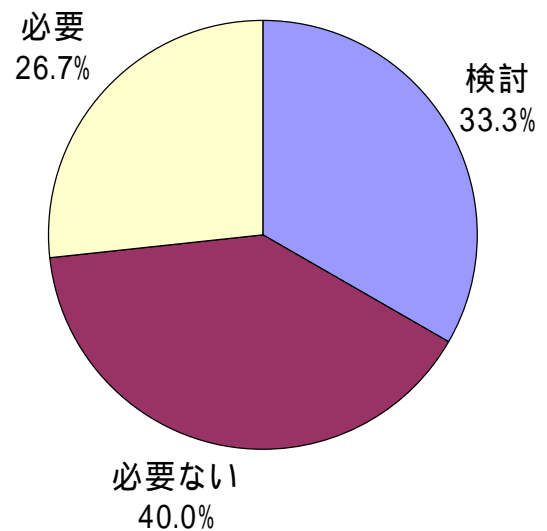
(2) 必要ないと答えた学校

このシステムを必要としない回答いただいた学校は、15校中6校（県立4校、私立2校）であった。その6校においては、ネットワークへの接続設定が様々な状況であった。そのうちの5校は、他校と比べ校内ネットワークの構築状況が比較的進んでいると思われ、現在のままで不自由していない、または私の設計したシステムと同じようなことが可能なシステムを導入しているということであった。残りの1校については、現在個人所有のパソコンを校内のネットワークに接続させていないため必要ないとのことであった。

(3) 検討と答えた学校

検討とは、今後の検討課題ということであり、そう回答した学校が5校（県立4校、私立1校）であった。5校のうちの4校については、他校と比べ比較的校内ネットワークの構築状況が遅れているといった学校であった。そのため、システム自体には興味を持っていただくことができたが、Linux サーバの導

開発したシステムの必要性



入については考えていないといった回答であった。また、校内のネットワークの構築がまだ十分でなく、登録端末への自動アドレス割り当てについては今後の話といった意見を聞くことができた。その他の1校は、現在固定 IP アドレスを割り当てているため、そういったシステムを導入するかについて今後検討したいといった回答であった。

2 システムについて

このシステム（登録端末への DHCP による自動アドレス割り当て機構）については、本研修において開発したものであり、この研究のまとめ（資料）にプログラムコードと構築手順書、使用説明書を収録している。また、これは実行ファイル（.exe）とは異なるため、様々な記録媒体を使い配布することができない。そのため、上記資料を参照していただき、必要とされる学校については使っていただければ幸いである。

その他の研修

九州大学工学部電気情報工学科目から、前期では4科目、後期では2科目の講義を聴講させていただいた。それぞれの情報システムに関する講義で、現代のコンピュータの動作原理とそれを実現する構成要素の動作と構造や、ハードウェアとソフトウェアのインタフェースとしてのコンピュータアーキテクチャの概念を理解することができた。また、演習補助を行うことで、高校生と大学生における指導内容および多様な到達度を有する大学生に対する指導について、実践を通してその指導法を習得することができた。また、高校生に問題解決能力を身につけさせる必要性についての課題を見出すことができた。

その他に、専門的な研修以外に「共同作業における実践的な手法」と「文書作成のための方法論」について学ぶことができた。「共同作業における実践的な手法」とは、直接顔を合わせる機会が少なくても、当事者同士で共通認識することができ、共同作業における相互の意志疎通を図り確認するための実践的な手法である。「文書作成のための方法論」とは、技術報告書の類に関する文書の作成のための方法論についてである。そういった技術的手法を習得することができた。

情報システムに関する研修について

九州大学工学部電気情報工学科目から、前期では4科目、後期では2科目を聴講させていただいた。「コンピュータアーキテクチャ」・「コンピュータアーキテクチャ」・「コンピュータシステム」では、現代のコンピュータの動作原理とそれを実現する構成要素の動作と構造や、ハードウェアとソフトウェアのインタフェースとしてのコンピュータアーキテクチャの概念を理解することができた。「情報ネットワーク」と「通信ネットワーク」では、今後の校内ネットワーク構築と深く関わっており、コンピュータネットワークの最新技術や課題、今後の技術開発と展開状況等について理解することができた。

「コンピュータシステム」の講義内容は、今後情報分野の指導を行っていく中で、基礎基本となるコンピュータシステムを構成する計算機のハードウェアやソフトウェアについて学ぶことができた。また、「コンピュータアーキテクチャ」・「コンピュータアーキテクチャ」・「通信ネットワーク」の講義内容は高等学校の課程を超える専門的な内容であったため、高校での授業で直接その内容を指導する機会はないと思われるが、情報システム構築のための要素技術について理解を深めることは、今後情報処理関連科目の授業を実施する上で大変有益であったと思われる。その他にも、「計算機システム構成論」では、隔週におけるレポート提出をはじめ、講義の中でセキュア OS、社会システムとしての計算機、ヒューマンインタフェース、ユビキタスコンピューティングなどのトピックスを紹介していただき、それについて調べ学習を深めていく大切さを学ぶことができた。

情報処理演習における指導法に関する研修

情報処理演習では、櫻井教授担当の「情報処理基礎演習」において、演習補助として2名のTA（ティーチングアシスタント：大学院生）とともに受講者の理解を促すための支援を行った。この授業を通し、多様な到達度を有する受講生に対しての指導法を習得することができた。また、大学生と高校生を比較することにより、高校生に問題解決能力を身につけさせる必要性を強く感じた。

この授業は、情報処理に関する内容を初めて学習する受講生が対象であり、ワープロソフトの操作から Pascal 言語によるプログラミング、HTML 言語を用いたウェブページ作成といった内容であった。本授業は、12回でその内容をすべて行うといった少ない時間での実施であったため、当初受講生の到達度が懸念されたが、全員が本授業のスキルを身に付けることができたと思われる。

授業内容では、情報処理に関する基本的なものであったため、指導にあたっては商業高校において実施している情報処理に関する授業と大差なかったが、受講生の違いで授業の進度および指導の方法に大きな違いが見られた。

1 ワープロソフトの操作

本授業におけるワープロソフトの操作については、課題提出に必要なワープロ操作を身につけさせることを目的とし、十分な時間を割いての指導ではなかった。受講生の状況としては、初めてワープロソフトを利用したという者は見られず、ある程度の操作能力を身につけているようで、受講生間で多様な到達度を有していた。そのため、どこを基準にして指導するか、また基本操作をどの程度まで指導するのか、受講生の状況を確認しながら授業を進める必要があった。高等学校での授業では、生徒の到達度を度外視して全員に同じ内容を始めから指導するといった状況である。ここでの大きな違いは、受講生に対して始めからすべてを指導するというのではなく、到達度が異なる受講生に対して各自のスキルに応じて取り組めるよう配慮するといったことであった。ここでは、各自のスキルに応じて取り組めるための課題を準備することで、より効果的な授業を実施できるということを学ぶことができた。

2 プログラミング

本授業では、Pascal 言語を使ったプログラミングを実施した。講義では、重要なポイントについて復習を行い、様々な実習課題を準備することにより受講生が各自のスキルに応じて取り組むといった方法で実施した。また、準備した課題をすべて行うことにより、各受講生における授業の到達度を統一させるといった手法を実施した。しかし、これは九州大学の学生が受講生だから実施できる方法であって、本校で行っている COBOL 言語によるプログラミングの授業でこれと同じ方法を用いて生徒に指導した場合、個人のスキルの差がますます広がっていくように思われた。

ここでの大学生と高校生の大きな違いは、わからない問題を自ら調べ解決するといった能力の差にあるように思われる。そのため、受講生の理解度を確認せずに授業を先に進めても本授業の受講生では、様々な手段を用いて問題を解決し理解するといった能力を有している。しかし、本校の生徒においては、わからないところをそのままにしているといった傾向が見受けられる。そのため、このような問題解決能力を高校生にどう養うかが、これからの課題と思われる。

本授業では、Pascal プログラミングを8回（90分×8回）実施したが、本校ではその約10倍の120時間（4単位を1年間）をかける内容であった。このように同じ到達度を目指した指導であっても、授業に配当する時間が大きく異なる。今後高校におけるプログラミング教育の指導のあり方と指導内容の工夫

改善が求められるよう思われた。

3 ウェブページの作成

ウェブページの作成実習における受講生の視点および実施状況については、高校生も大学生も大差がないように思われた。本授業において受講生が作成したウェブページでは、閲覧者に何を見せたいのかということよりも、技術的なものに主眼が置かれ、ウェブページの本質的なものが欠けていたように思われた。本校でも同様にウェブページ作成の授業を行ったが、それと同様で技術的なことに囚われ、本質的なものが欠けていた。その原因は、作成実習ということで、自ら研究した内容を閲覧させるという目的がなかったためだと思われた。

以上、演習補助として本授業に参加して、高校生と大学生における指導内容および多様な到達度を有する大学生に対する指導について、実践を通してその指導法を習得することができた。また、高校生に問題解決能力を身につけさせる必要性についての課題を見出すことができた。

この貴重な経験を活かし、今後高校生にプログラミングの指導をどのように行っていくか十分検討し、本授業で習得した指導法について、さらに検討し発展させていきたいと思う。

専門的研修以外で学んだこと

本研修において、専門的な研修以外に校務において自分自身に不足していた基本的な技術を学ぶことができた。その技術については、以下のようなものがある。

1 共同作業における実践的な手法

直接顔を合わせる機会が少なくても、当事者同士で共通認識することができ、共同作業における相互の意志疎通を図り確認するための実践的な手法を習得した。この手法は、打ち合わせなどの際は必ずメモを取り、その打ち合わせにおいて「明らかになったこと」「決めたこと」を文書として残し、その当事者が「明らかになったこと」「決めたこと」を誤解していないか確認する作業を行うというものである。

この手法については、今後学校現場に取り入れ、共同作業においてお互いが共通認識できるよう取り組んでいきたいと思う。

2 文書作成のための方法論

技術報告書の類に関する文書の作成のための方法論を習得した。その方法として、第一に優先されるのは、伝えるべき情報をできるだけ読み手の負担にならないように早く伝えることである。ようするに、簡潔に言いたいことをできるだけ最初に、事実とそれに関する評価や推論を区別する。そのためには節、見出し等を用いて視覚的に表現するといったテクニックである。

学校現場でもこの技法を用いて、相手に伝えるべき情報を読み手の負担にならないよう、文書を作成していきたいと思う。

ウェブページ

UNIX・Linux 関係

Linux の基礎学

<http://linux-topics.com/linuxBeginner/beginner.htm#1>

UNIX と Linux を振り返る

<http://www.atmarkit.co.jp/flinux/rensai/theory01/theory01.html>

UNIX / Linux コマンド Topics

<http://linux-topics.com/>

@IT (アットマーク・アイティ)

<http://www.atmarkit.co.jp/flinux/index/indexfiles/index-linux.html#theory>

DHCPD の設定

<http://www.mm-labo.com/computer/linux/dhcp.html>

crontab の設定

<http://www.coolbrain.net/cron.html>

cron で大切なデータをバックアップしよう

<http://www.geocities.jp/tetrahymana21/linuxtips/cron.html>

vi エディタの使用法

<http://www.affrc.go.jp/Cinfo/seminar/text/EDITOR/HTML/editor.htm>

dhcpd.conf 運用・管理

http://www.ep.sci.hokudai.ac.jp/~epdns/dvlop_old/2002-06-05/dvlop/dhcp/log.html

校内ネットワーク関係

NEC ビジネスソリューション NEC 教育プラザ

<http://www.sw.nec.co.jp/educate/>

ワークグループとドメイン管理 TechNet オンラインセミナー

<http://www.microsoft.com/japan/technet/treeview/default.asp?url=/japan/technet/tcevents/olseminars/winxpdep/default.asp>

ドメインとワークグループの見分け方

<http://www.atmarkit.co.jp/fwin2k/win2ktips/256nettype/nettype.html>

ドメイン一覧にコンピュータが表示されないようにする

<http://www.atmarkit.co.jp/fwin2k/win2ktips/261svhide/svhide.html>

ドメインにログオンしていないクライアントから共有資源にアクセスする

<http://www.atmarkit.co.jp/fwin2k/win2ktips/265stdcliaccess/stdcliaccess.html>

WIDE University, School of Internet

<http://www.soi.wide.ad.jp/contents.html>

アライドテレシス社 ソリューション (ガイド) 学校のネットワーク (文教市場)

<http://www.allied-telesis.co.jp/solution/school/index.html>

(株)大塚商会 ソリューション(ガイド) 学校向けシステム

<http://it.e-otsuka.com/contents/kankou/kankoutop.htm>

コンピュータ教室

http://it.e-otsuka.com/contents/kankou/comp_cam.htm

@IT (アットマーク・アイティ)

<http://www.atmarkit.co.jp/fnetwork/rensai/pki01/pki01.html>

http://www.atmarkit.co.jp/ad/ms/linuxvswin/top_index.html

CGI/Perl 関係

CGI/Perl 入門

http://www.ccad.sccs.chukyo-u.ac.jp/manualc/network/CGI_PERL/

CNS GUIDE2002 CGI とフォーム機能

<http://cns-guide.sfc.keio.ac.jp/2002.stu/9/6/3.html>

beginners CGI

<http://www.aimix.jp/cgi/syohoidx.html>

CGI・Perl 入門

http://home.interlink.or.jp/~kamitani/perl_lng/cgiperl.html

作ってみよう CGI

http://www1.kcn.ne.jp/~satan/myst/myst_031.htm

Introduction to CGI

<http://www.ipc.hokusei.ac.jp/~z00104/cgi/form.html>

セキュリティ関係

学校情報セキュリティガイド(神奈川県立総合教育センター)

<http://www.edu-ctr.pref.kanagawa.jp/security/index.html>

JPRING MRTG で行うサーバ監視

<http://www.jpring.net/jitaku/snmp-mrtg.html>

アクセス制御

<http://www.futomi.com/lecture/htaccess/htpasswd.html>

.htaccess によるアクセス制御

<http://yang.amp.i.kyoto-u.ac.jp/~yyama/FreeBSD/www/htaccess-j.html>

.htaccess 実践活用術

<http://www.shtml.jp/htaccess/>

学校情報セキュリティガイド

<http://www.edu-ctr.pref.kanagawa.jp/security/index.html>

用語集

IT 用語辞典 e-Words

<http://e-words.jp/> (株式会社インセプト)

アスキーデジタル用語辞典

<http://yougo.ascii24.com/> (株式会社アスキー)

ネットワークセキュリティ関連用語集

<http://www.ipa.go.jp/security/glossary/glossary.html> (情報処理振興事業協会)

@nifty 辞書

<http://www.nifty.com/dictionary/>

その他

情報教育テキスト (長岡市教育センター)

<http://www.kome100.ne.jp/nkcenter/lib/index2.htm>

文部科学省 報道発表「学校における情報教育の実態等に関する調査結果」

http://www.mext.go.jp/b_menu/houdou/16/07/04072101.htm

福岡県教育センター 「学校の情報化推進のために」

<http://www.educ.pref.fukuoka.jp/kiyou/148/primary/primary.htm>

毎日新聞 掲載記事「無防備な学校現場 残された時間少なく」

<http://www.mainichi-msn.co.jp/it/coverstory/news/20041117org00m300089000c.html>

書籍

情報ネットワークの通信技術 齊藤 忠夫 監修 石坂 充弘 著 オーム社

情報通信ネットワーク 遠藤 靖典 著 コロナ社

ネットワークの相互接続 堀良彰 池永全志 門林雄基 後藤滋樹 著 岩波書店

「The Entrance to a Perl User」 日本語 TEXT 加工入門ハンドブック 改定新版 中島 靖 著
株式会社情報管理 発行

Perl テクニック 日本語 TEXT 加工実践ガイドブック 中島 靖 著 株式会社情報管理 発行

Perl 書法 増井 俊之 著 ASCII

Perl5 パワフルテクニック大全集 インプレス社

いまさら人には聞けない Linux の超基本 K's Production 著 すばる舎

Fedora Core2 で作る 自宅サーバ for Linux 鈴木 哲哉 著 株式会社ラトルズ

超入門ネットワーク ASCII 社

完全図解式ネットワーク再入門 ASCII 社

実用 UNIX システム マーク・ソベル 著 工学社

UNIX システムプログラミング K・ハヴィランド B・サラマ 著 サイエンス社

ファイル&Web サーバー構築ガイド スタークスター 著 エーアイ出版

図解でわかる サーバのすべて 小泉 修 著 日本実業出版社

インサイド TCP/IP 片山 裕 インプレス社

イーサネットと TCP/IP CQ 出版社

ぼくたちはこうして学校をつないできた 奥村 晴彦 監修 共著 エーアイ出版

おわりに

福岡県は、福岡県教育センターを情報拠点とする「福岡県教育情報ネットワーク」を平成13年度より段階的に整備し、平成15年度までにすべての県立学校への接続を完了するとともに、各学校にネットワーク活用委員会を置いた。しかし、校内ネットワークは、各学校のネットワーク管理者を中心として学校独自で構築・運営している状況であった。そのような各学校の状況から問題を調査・分析し、校内ネットワークの管理体制の下、誰もが利用しやすいネットワーク環境を実現するため、校内ネットワークのあり方・運営・管理についてのモデルケースを作成することができた。そのモデルケースを作成するにあたり、情報システムの構成と運用に関する専門的な内容を深めるとともに、学校訪問を行い、高校における校内ネットワークシステムの管理・運用の現状を調査し、これからの校内ネットワークのあり方と運営、その管理組織について検討を行った。また、社会において注目を集めている個人情報保護に関する学校現場における問題提起を行うとともに、その対策についてまとめることができた。

来年度学校現場に戻り、Linuxサーバの構築をはじめ、校内ネットワークの再構築とセキュリティポリシーの策定、ネットワーク管理組織の検討を行いたいと考えている。これは校内の情報化が進みインターネットの教育への活用や、日常の業務の中での電子データの取り扱いなどの比重が日増しに大きくなってきている。そのように便利になってきた反面、生徒の個人情報漏洩に関する問題も懸念されており、校内ネットワークの整備に併せて、校内ネットワークの運用においては、セキュリティ対策や不正アクセス等のトラブル発生時の対応方針を明確にし、具体的な対応手順を整備していきたいと考えている。また、各学校のネットワーク管理者や情報教育担当者間で相談できる横のつながりを作るとともに、休業日等を活用して定期的に有志が集い、今年度研修したネットワーク技術や校内ネットワークの管理運営について勉強会を実施し、各学校の状況や問題点等が話せるような場を作りたいと考えている。

この1年研修では、じっくりと腰を据えてのネットワーク技術に関する学習や講義の聴講、Linuxのインストールと各サーバの構築、システム開発等の実習と、多くの研修を積み重ねたことは、今まで机上でしか学ぶことができなかった内容を実際に体験でき、それによって大きな自信となった。しかし、情報技術の分野においての進展は目覚ましいものがあり、今後新しいものへと日進月歩に変化していくと思われる。それに適宜対応していくためにも、これからも継続して研修に励み、自己研鑽に努めていくとともに、本研修で学んだことを一つでも多く学校現場と生徒に還元できるよう、工夫改善を行っていきたいと思う。

最後に、この研修を進めるにあたり、指導教員である櫻井教授並びに堀助教授には、研修内容の立案及びその場に合った的確なご指導、実習をするための環境等をご提供いただき、心より感謝申し上げます。また、指導助言等でご尽力頂いた福岡県教育委員会高校教育課の高野主任指導主事並びに泉指導主事に深く感謝するとともに、1年間という長期にわたる研修に専念できるようにご配慮頂いた文部科学省並びに福岡県教育委員会の関係各位、所属校校長である長濱英俊校長をはじめ、本校職員に対し感謝の意を表する次第である。

平成17年3月10日