多様な利用形態に対応した
小規模組織用ネットワークに関する研究

東京工業大学大学院 情報理工学研究科
上田 仁
(学籍番号 97M37064)

平成 10 年度 修士論文

指導教官: 大野浩之講師

1999 年 1 月 29 日

目 次

第 1 章　はじめに **6**

第 2 章　ネットワーク構築運営の現状と問題点 **7**
2.1　大規模組織によるネットワーク構築と運用 7
2.1.1　大規模組織ネットワークの現状 7
2.1.2　大規模組織ネットワークの特徴 11
2.2　小規模組織によるネットワーク構築と運用 12
2.2.1　小規模組織ネットワークの現状 12
2.2.2　小規模組織ネットワークの特徴 13
2.3　本研究の目的 14

第 3 章　小規模組織に適したネットワークの構築・運用手法 **16**
3.1　ネットワークの機動性の定義 16
3.2　機動性に配慮したネットワークの利点 16
3.3　ネットワークモデル 17
3.3.1　ネットワークの高い独立性 19
3.3.2　セキュリティの確保 19
3.3.3　環境への適応 21
3.3.4　安価なネットワーク 22
3.3.5　長期間の運用を想定した態勢の整備 22

第 4 章　研究室内ネットワークの設計 **23**
4.1　環境層 23
4.1.1　物理的な防御 23
4.1.2　不意の停電対策 23
4.2　ネットワーク構成層 25
4.2.1　端末の選定 25
4.2.2　ファイアウォールの構築 26
4.2.3　物品管理 31
4.2.4　IPv6 への対応 31
4.2.5　NAT 31
4.3　サービス層 32
4.3.1　導入するサービス 32

4.3.2 ドメイン名の取得 . . . 32
4.3.3 IP アドレスの割り当て . . . 33
4.4 構成員層 . . . 33
4.4.1 大野研 FYI . . . 33

第 5 章 研究室内ネットワークの運用 35
5.1 概要 . . . 35
5.2 旧ネットワーク期 . . . 36
5.2.1 物品管理システム . . . 36
5.2.2 第 1 回棚卸し . . . 37
5.3 ネットワーク構築期 . . . 39
5.3.1 ネットワークトポロジーの変更 . . . 39
5.3.2 全ての主要なサーバ計算機の PICKLES 端末化 . . . 39
5.3.3 ohnolab-cfp . . . 41
5.3.4 NIS . . . 42
5.3.5 スクリーニング . . . 42
5.3.6 ドメイン名の取得 . . . 43
5.3.7 研究室内メーリングリスト名の整備 . . . 43
5.3.8 第 2 回棚卸し . . . 44
5.3.9 管理者権限のガイドライン . . . 45
5.4 ネットワーク運用整備期 . . . 46
5.4.1 電力構成 . . . 51
5.4.2 ベンチマークガイドライン作成 . . . 51
5.4.3 ssh の導入 . . . 52
5.4.4 構成人数 . . . 53
5.4.5 ログの記録 . . . 55
5.4.6 Reborn System . . . 55

第 6 章 評価と考察 58
6.1 研究室内ネットワークの評価 . . . 58
6.1.1 ネットワークの高い独立性 . . . 58
6.1.2 セキュリティの確保 . . . 60
6.1.3 環境への適応 . . . 65
6.1.4 安価なネットワーク . . . 65
6.1.5 長期間の運用を想定した態勢の整備 . . . 65
6.1.6 管理者の負担軽減 . . . 66
6.2 プロトコルが異なるネットワークへの移動 . . . 67
6.2.1 IPv6 デーの概要 . . . 68
6.2.2 ネットワーク構成図 . . . 68
6.2.3 IPv6 デーの実施 . . . 68
6.2.4 IPv6 デーのまとめ . . . 70

第 7 章　今後の課題 **71**
7.1　全ての計算機での PICKLES 端末の採用 71
7.2　ネットワーク管理用メタデータの規定 71
7.3　不正侵入検知システムの導入 72
7.4　100Base Ethernet の利用者増加 72
7.5　ゲストアカウントの整備 73

第 8 章　結論 **74**

付 録 A　研究室内ネットワークの歴史 **80**

付 録 B　セキュリティ情報の情報源 **85**

図 目 次

2.1 OCN のネットワーク構成 8
2.2 ODINS2 のネットワーク構成 9
2.3 ATM Network Management Model 10
2.4 Customer Management of Private & Public Networks 10
2.5 WIDE プロジェクトによる仮設型ネットワークの構成図 11

3.1 ネットワークの移動 17
3.2 小規模組織のネットワークモデル図 18
3.3 CERT に報告された不正アクセス届出数の推移 20
3.4 JPCERT に報告された不正アクセス届出数の推移 20
3.5 日本国内におけるファイアウォールの設置状況 21

4.1 デュアルホームホストを利用したファイアウォール 27
4.2 要塞ホストを利用したファイアウォール 28
4.3 境界ネットワークを利用したファイアーウォール 29
4.4 内部チョークと外部チョークを統合したファイアーウォール 30
4.5 研究室内ネットワークのファイアーウォール 30

5.1 1996 年度ネットワーク構成 37
5.2 物品番号により管理された MO ドライブ 38
5.3 移行前の状態 40
5.4 移行中の状態 40
5.5 移行後の状態 41
5.6 ネットワーク構成 47
5.7 ルータ及び各種サーバ計算機の写真 48
5.8 スクリーニングのログ 54
5.9 安全ではない通信 55
5.10 障害を起こした計算機の機能を代行 56
5.11 運用例 57

6.1 メモリ消費率と CPU 消費率 59
6.2 スクリーニングによるルータの性能低下を計測する実験環境 60
6.3 実験で用いた各 PC の性能 60
6.4 月別総数 67

6.5 IPv6 網 68
6.6 IPv6 デー実施時のネットワーク構成図 69

第1章　はじめに

少人数の事務所や家庭などの小規模組織がコンピュータネットワークを構築する場合、管理者不足や管理運用技術の未熟さ、運用資金の不足などが問題となり、自組織だけでネットワークを構築運用するのが困難である。しかし、小規模組織でも自由度の高いネットワークを構築運用し、メールや WWW など各種サービスを自主運用したいという要求が高まりつつある。本研究では、小規模組織ネットワークのひとつである大野研究室内ネットワークの構築運用経験から、小規模組織に適したネットワークの構築運用手法を議論する。

筆者が中心となり構築運用している大野研究室内ネットワークでは、サーバ計算機を含めて主要な計算機は PICKLES 端末で統一している。PICKLES 端末は、単独で運用可能な自律型 PC 計算機であり、各端末間で共通な領域と端末固有の領域が、ソフトウェア的にもハードウェア的にも分離されている。

大野研究室内ネットワークで運用している Reborn System は、PICKL ES 端末の相互の交換性の高さを活用した障害管理システムであり、障害からの迅速かつ容易な回復を目的とする。Reborn System は、各端末の固有な情報のみを定期的に取得し、それを基に障害回復を行う。Reborn System は、管理者の負担軽減や管理技術の不足に対応できるため、小規模組織においても有効である。

次世代インターネットプロトコル (IPv6) への対応が世界的に始まりつつある。大野研究室内ネットワークでは、IPv4 と IPv6 の両方のプロトコルに対応できるデュアルスタック環境のネットワークを構築した。IPv6 を利用したネットワークでは広大な IP アドレス空間が利用可能になることやホストの自動設定が可能など、小規模組織においても IPv6 を導入する利点は多い。大野研究室内ネットワークのデュアルスタック環境の構築経験を基に、IPv4 を利用した小規模組織ネットワークが IPv6 に移行する手法を述べる。また、IPv6 への移行上の問題点の解明や利用者への利用促進を目的として、大野研究室で行った IPv6 Day と呼ぶ取り組みの結果を報告する。

これらの他にも、大野研究室内ネットワークのセキュリティ確保のために行ったファイアウォールの構築と運用方法及び結果について述べる。この方法は、管理者の負担軽減とセキュリティの確保を同時に実現しているため、一般の小規模組織でも有効である。また、小規模組織ネットワークの対外接続先の変更を想定した取り組みなど、大野研究室内ネットワークを構築運用する上で行ったさまざまな手法について述べ、その手法の小規模組織への適応を議論する。最後にそれらのまとめと考察を述べる。

第2章　ネットワーク構築運営の現状と問題点

本章では大規模組織と小規模組織の各々について、ネットワーク構築運用手法の現状と特徴を述べる。そして、小規模組織ネットワークにおけるネットワーク構築運用上の問題点を明らかにし、本研究の目的を述べる。

2.1　大規模組織によるネットワーク構築と運用

従来、企業や学術組織等の大規模組織がネットワークを構築し運営してきた。そのためネットワークの構築や管理、運用などの手法は、主に大規模で高速なネットワークを対象として開発されてきた。

2.1.1　大規模組織ネットワークの現状

本項では、大規模組織のネットワーク構築運営の例として、NTTが運用するオープンコンピュータネットワーク(OCN)[5]と大阪大学が運用するキャンパスネットワークODINS[43]、WIDEプロジェクト[24]が運用した仮設型ネットワーク[52]を取り上げる。

OCN

OCNはNTTが提供する大規模商用ネットワークであり、OCNサービスにより利用者にインターネットとの接続性を提供する。1998年6月の時点で、ダイアルアップ接続により約20万人、常時接続により約2万人の利用者がOCNサービスを利用している。OCNは商用ネットワークであるため、高信頼性や高品質、確実なサービス提供、故障処理などが要求される。

文献[5]によれば、OCNのネットワーク構成はバックボーンネットワークと数千の加入者系ネットワークから構成される(図2.1)。バックボーンネットワークは数十のバックボーンルータから構成され、加入者系ネットワークとインターネットの間を中継する。加入者系ネットワークは数千のエッジルータから構成され、利用者が接続する。

OCNの運用は、Network Management Forum(NMF)[13]が体系化したSMARTプロセスモデルを基にする。SMARTモデルは、通信サービスを提供する際のオペレー

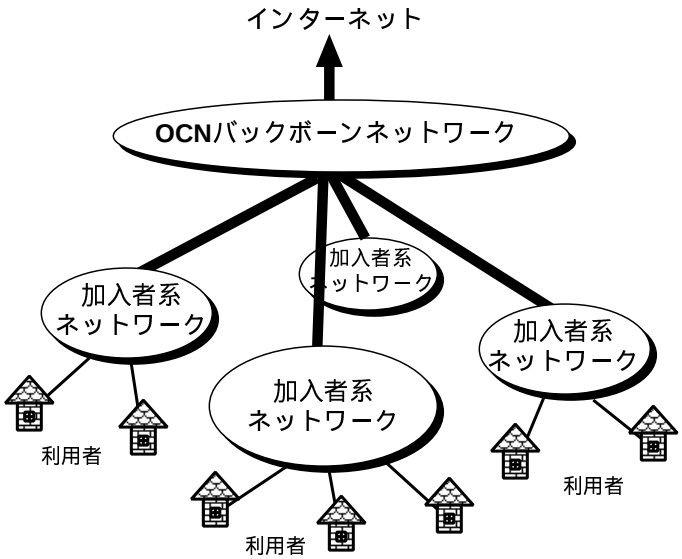

図 2.1: OCN のネットワーク構成

ションの業務プロセスを分類したものである。OCN ではネットワークの運用を、サービスフロント業務とネットワーク管理業務の大きく 2 つに分けている。

サービスフロント業務

- 申込み受付 利用者のサービス加入・変更・廃止の要求などを処理する。
- 料金請求業務 利用者の利用料金の請求・収集を行う。
- 故障対応 故障解析や故障復旧を行う。

ネットワーク管理業務

- ネットワーク監視業務 ネットワークを監視し問題点を発見する。
- サービス品質管理業務 サービスが適切に運用されるように管理する。
- 設備計画業務 ネットワーク設備の計画を立案する。

ここでは、ネットワーク管理の一部であるネットワーク監視分野を特に取り上げる。OCN では、バックボーンネットワークを構成するバックボーンルータや加入者ネットワーク内のエッジルータを、SNMP[22] による Network Management System(NMS)、syslog 管理ツール、UNIX コマンド、perl などのスクリプト言語で書かれた管理ツールなどを利用して管理する。管理者はバックボーンルータとエッジルータの管理者に分けられ、管理業務を分散している。これはそれぞれのルータで管理に必要となる知識や技術が異なるためである。バックボーンルータの管理者は、BGP や OSPF などのルーティングプロトコルを理解し、障害に対処できる必要がある。エッジルータの管理者は、電話網や ISDN 網などの利用者インターフェイスに関する知識や認証技術に関する知識が特に必要とされる。

ODINS

大阪大学では、ATM を利用したキャンパスネットワーク ODINS (Osaka Daigaku Information Network System) を 1993 年から構築・運用している。1995 年には、バックボーン ATM ネットワークの高帯域化や冗長構成の採用を行い、高い拡張性をもったネットワーク ODINS2 を構築した。文献 [5] によるネットワーク構成図を図 2.2 に示す。ODINS2 では、ATM 交換機の電源モジュールやコントローラ、スイッチファブリック、回線インターフェイスを冗長化し、耐故障性を高めている。

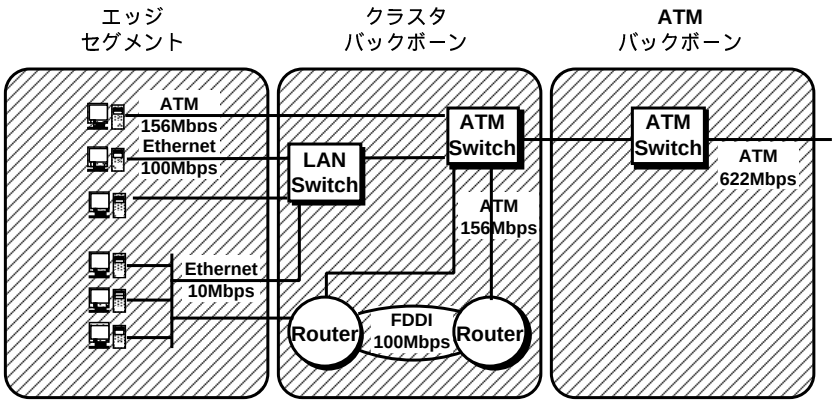

図 2.2: ODINS2 のネットワーク構成

ATM を導入したキャンパスネットワークは他にも、京都大学の KUINS-II や東京大学の UTnet などがある。一般に、これらのキャンパスネットワークでは、管理者の人員の制約などのため、計算機センターや情報処理センターなどに管理拠点を集中させる。また、管理者間の技術格差を補うため補助的な管理システムが導入される場合もある。

ATM と既存 LAN、インターネットを混在して管理するネットワーク管理システムとして、SNMP を用いたネットワーク管理システムがある。例えば、MRTG[1] のようなネットワーク管理モニタリングツールなどである。ATM 管理インターフェイスのモデル化 (図 2.3) は、ATM Forum によって行われている。ATM Forum はこのモデルを用いて、公衆ネットワークサービスにおける Customrer Network Management(CNM) モデル [10] を定義している (図 2.4)。

WIDE プロジェクトによる仮設型ネットワーク

WIDE プロジェクトは、WIDE プロジェクトに参加する研究者が一同に集まるワークショップを年 2 回数日に及んで開催する。ワークショップの開催中は会場に仮設型ネットワークが構築され、ワークショップ参加者に対するインターネットへのアクセスサービスの提供や、ワークショップ参加者に対するワークショップ内の情報提供、実際のネットワークと同様な状態でのネットワーク実験が行われる。このワークショッ

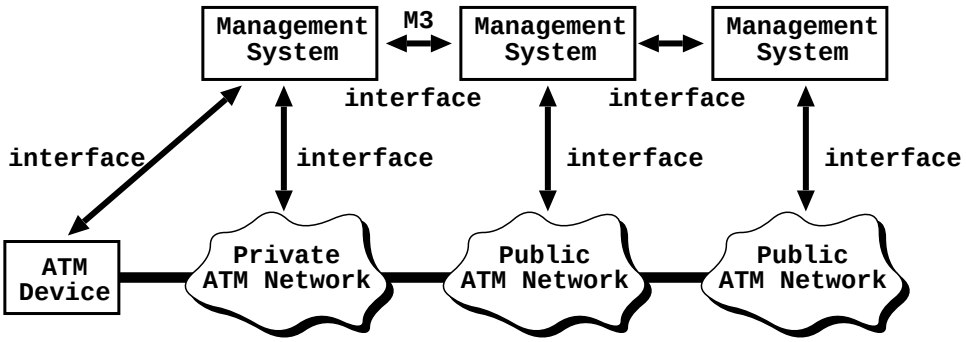

図 2.3: ATM Network Management Model

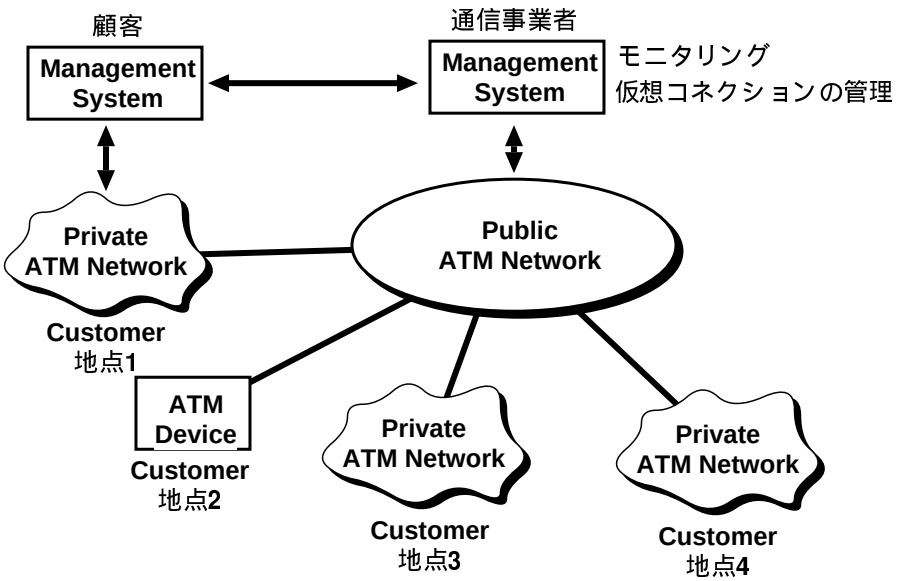

図 2.4: Customer Management of Private & Public Networks

プには 250 人程度のネットワーク研究者が参加し、各参加者によって数百台の計算機が持ち込まれる。

1997 年 9 月に 4 日間に及んで開催されたワークショップでのネットワーク構成図を図 2.5 に示す。このネットワークでは、高速性を重視してバックボーンには Cell Switch Router(CSR)[19] 技術が用いられた。約 20 人強の研究者がネットワーク担当となり、ネットワークの設計や構築を行った。

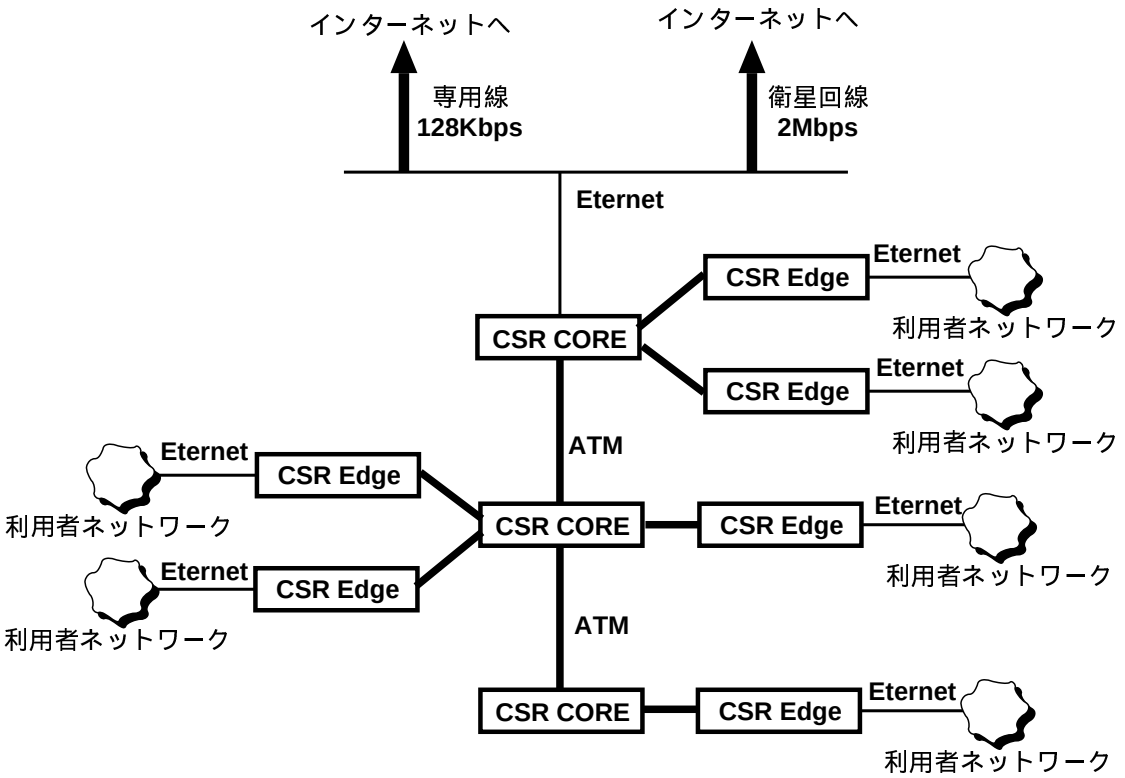

図 2.5: WIDE プロジェクトによる仮設型ネットワークの構成図

このような大規模な仮設型ネットワークでは、ネットワーク上の計算機を一意に定める global IP アドレスを用いるのが困難なため、任意に利用できる private IP アドレスが主に利用された。また、次世代インターネットプロトコルである IPv6 や、RSVP、WWW クラスタ、NAT ルータなどが評価実験用に運用された。

2.1.2 大規模組織ネットワークの特徴

本節では、大規模組織が構築するネットワークの特徴を考察する。前節の 3 つの実例から大規模組織が構築運用するネットワークの特徴として次の 3 つの点が挙げられる。

- 熟練したネットワーク管理者が存在する
  ネットワーク管理に熟練した管理者が構築や運用をしている。WIDE プロジェク

トによる仮設型ネットワークでは、ネットワーク研究者である WIDE プロジェクトの構成員が構築運用に携わっている。OCN では、ネットワーク管理者を管理内容に応じて 2 つに分け、それぞれの管理内容に精通した管理者を割り当てる。大規模組織では、熟練したネットワーク管理者が存在するため、ネットワーク管理知識を必要とする NMS の利用や、短時間でのネットワーク構築が可能である。

- 利用者と管理者が分離されている
  OCN サービスの利用者である一般の顧客は一定の利用料金を NTT に支払い、OCN の提供するサービスを受ける。OCN において管理者と利用者は明確に分けられている。ODINS やその他のキャンパスネットワークでは、情報計算機センターや情報処理センターで管理者が集中管理する。大規模組織では、ネットワークの管理者は管理作業にのみ集中して取り組める。

- 潤沢な資金を保持している
  大阪大学の ODINS は、構成機器を冗長化してネットワークの耐故障性をあげている。大規模組織は潤沢な資金があるため、大規模な高速バックボーンネットワークの構築や構成機器の冗長化などが比較的行いやすい。WIDE プロジェクトによる仮設型ネットワークでは、ワークショップに参加する組織が、ネットワークの設営に必要なネットワーク機材を持ち寄った。

2.2 小規模組織によるネットワーク構築と運用

近年、事務所や家庭等の小規模な組織がコンピュータネットワークを構築・運営する例が増加している。本節では小規模組織ネットワークの現状を取り挙げその構築運営上の問題点を議論する。

2.2.1 小規模組織ネットワークの現状

本節では、小規模組織のネットワーク構築運営の例として、SOHO 環境でのネットワーク、一般家庭での家電製品を繋いだネットワーク、教育現場でのネットワーク、老人ホームでのネットワークを取り上げる。

SOHO 環境の普及

事務所や家庭等の SOHO(Small Office Home Office) とよばれる小規模な組織がネットワークを構築し、インターネットと接続する例が増加している。大規模な企業等の組織でも、サテライトオフィスとして従業員がネットワークを自宅に構築する場合がある。SOHO という語に厳密な定義が確立されているとは言えないが、本研究では個人または少数の構成員が所属する、家庭や事務所等の小規模な組織と定義する。SOHO 環境のネットワークでは、数台のサーバ計算機やクライアント計算機が接続され、外部ネットワークとの接続に専用線やダイアルアップ接続が用いられる場合が多い。NTT が提供する ISDN サービスなどによって比較的安価な通信環境が整いつ

つあり、今後も SOHO 環境のネットワークは増加していくと考えられる。SOHO 環境では、外部ネットワークとの情報交換や組織内の情報共有にネットワークが利用される。

教育現場への導入

文部省と通商産業省が協力して実施した 100 校プロジェクト [31] や新 100 校プロジェクト、こねっと・プラン [28]、メディアキッズなどに代表されるように、ネットワークを初等中等教育に利用する試みがさかんに行われている。100 校プロジェクトでは、全国 100 箇所程度の学校や施設に、サーバとなる計算機やクライアントの計算機を提供し、インターネットと接続することで、ネットワークを活用した情報交換や共同研究を可能にした。これらの学校や施設では、少数のサーバやクライアント計算機を、ダイアルアップによってネットワークと接続する方法が主流である。例えばこねっとプランでは、端末数が 5 台以下の学校が全体の 78%を占めている。これらの端末を管理するために他組織の支援は十分ではなく、各校のネットワーク接続が成功するか否かは、ネットワーク管理に熟練した構成員が校内にいるかどうかに依存する。

このように初等中等教育など教育現場でのネットワーク導入が急激に行われている。日本のドメイン名や IP アドレスを管理している JPNIC では、今後数年間のうちに、約 42,000 の学校がインターネット接続を行うと予想している [16]。JPNIC では、これらの学校を含む全ての学校施設がインターネットに接続されることを想定し、それらの施設のネットワークに付与するドメイン名を収容する第 2 レベルドメイン「ed」の新設を予定している。

家庭への普及

家庭内の計算機やデジタル AV 機器などを相互に接続することで、各機器の相互操作を可能にするホームネットワークがさかんに研究されている [35][45]。家庭内の家電がネットワークに接続され一つのネットワークが生成される可能性が生じてきた。

老人ホームへの導入

各種老人ホームでネットワーク接続をおこない福祉活動などに利用する試みがある [34]。このような老人ホームでは、端末をダイアルアップ接続で外部ネットワークに接続し、WWW や電子メールの利用を通して各老人ホーム間の交流や活動に役立てている。

2.2.2 小規模組織ネットワークの特徴

前節で挙げた小規模組織ネットワークの例から小規模組織ネットワークの特徴として次の点が挙げられる。

- 熟練した管理者の不足

  ネットワークを管理するのにネットワークに対する管理者の知識が十分ではないことが多い。また、十分な知識をもった管理者がいたとしても、構成員の入れ替わりが比

較的頻繁に行われる小規模組織では、将来もその構成員がいるとは限らない。そのため、ネットワークの構築運用に際し、熟練したネットワーク管理者の存在を仮定できない。

- 利用者と管理者が明確には分離されていない。

  小規模組織がネットワークを運用する場合、構成員の有志が本来の業務の副業でネットワーク管理を行うことが多い。そのため、管理者はネットワーク管理に全ての時間を費せない。また、障害が発生したときなど本来の業務を中断して復旧作業を行うため、管理者の負担が大きい。

- 潤沢な資金を保持していない。

  小規模組織では、ネットワークの構築運営に十分な費用をかけられるとは限らない。ネットワークの構成機器は安価である必要があり、ネットワーク管理に必要な金銭的コストも低い必要がある。

2.3 本研究の目的

ネットワークの構築運用上の問題点を解消し、小規模組織が独自にネットワークを運用できれば、小規模組織自身は独自の方針でネットワークを利用でき、ネットワークの柔軟な利用が期待できる。また、小規模組織が独自でネットワークを運用できれば、ネットワークを持つものと持たないものとの情報格差の解消に有効である。必ずしも全ての小規模組織が独自にネットワークを構築し運用しなければならないわけではない。小規模組織がその選択を可能な状態にすることが重要である。そのためには、小規模組織の特徴に配慮したネットワークの構築運用手法を確立する必要がある。

熟練したネットワーク管理者の有無や、利用者と管理者の分離状態、資金量の差など、大規模組織と小規模組織の特徴の差を考慮すると、従来の大規模組織で用いられて来た方法は、小規模組織が構築運用するネットワークでは必ずしも有効ではない。例えば、通信事業者と顧客間の通信設備に関する参照や制御を定める Customer Network Management と呼ばれる概念は、利用者と管理者が明確に区別されていない大部分の小規模組織には適応できない。国際電気通信連合 (ITU) の一部門である電気通信標準化部門 (ITU-T) が行う Telecommunications Management Network(TMN) に関する研究は、顧客への各種通信サービスを提供することを目的とした電気通信網管理の研究である。TMN は、小規模組織ネットワークの特徴であるネットワーク管理者が不足した状況下での管理を考慮していない。

本研究では小規模組織が構築し運用する、計算機の台数が数十台規模のネットワークを対象とし、小規模組織のネットワーク構築・運用の指針を示す。小規模組織という語に厳密な定義はないが、本研究では構成員数が一人からせいぜい数十人までの組織と定義する。特に多様な小規模組織にネットワークに対応させるため、以下の項目を満たすことを目標にする。

- 熟練した管理者の存在を仮定しない

- 利用者が管理者を兼任する状況を考慮する
- 金銭的コストに配慮する

第3章　小規模組織に適したネットワークの構築・運用手法

本研究では、小規模組織に適したネットワークとして、「機動性に配慮した小規模組織用ネットワーク」を提案する。本章ではまず、「ネットワークの機動性」を定義し、小規模組織における有効性を述べる。次に、機動性に配慮した小規模組織ネットワークのモデルを示し、構築運用上の問題点を考察する。

3.1　ネットワークの機動性の定義

一般に機動性 (モバイリティ) といえば、小型携帯端末を対象として考えることが多い。ノート型計算機や PDA などの小型携帯端末を持ち歩く利用者は、移動する先々でその場のネットワークに小型携帯端末を接続してネットワークを利用する。システムやその設定などを持ち歩くため、利用者は常に同じ環境からネットワークを利用できる。つまり、移動する先々のネットワークで端末を確保し、利用者自身の環境を再構築するなどの手間は不要である。

筆者らはモバイリティの対象をネットワーク全体に拡張して考え、これを “ネットワークのモバイリティ” と呼んでいる [33][41][44][46]。小型携帯端末を持ち歩く利用者が移動する先々でその場のネットワークに接続し設定の変更や利用者環境の再構築などをすることなしにネットワークを利用できるように、ネットワークを運用する組織が移動してそのネットワークの接続先が変更されたときも、ネットワークの再構築などをすることなしに容易にその変更ができることを、ネットワークのモバイリティと定義する。

3.2　機動性に配慮したネットワークの利点

研究室などの小規模な組織がモバイリティをもつネットワークを構築している場合、その組織は組織構成の変更があっても同じネットワークを維持できる (図 3.1)。さらに組織自体が物理的に移動し、対外接続のネットワークが変化したとしてもネットワークを構築し直す必要がない。従業員が自宅でサテライトオフィスを構築する場合、必要に応じて企業内ネットワークを分離し自宅に移動できれば、ネットワークを構築する負担が軽減される。

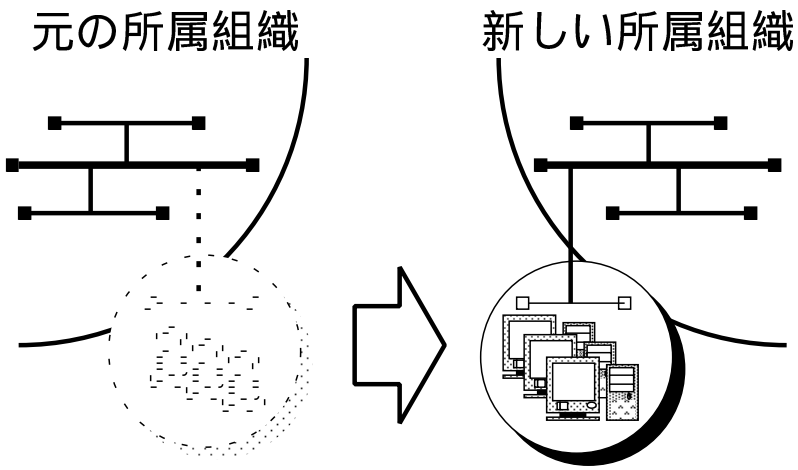

図 3.1: ネットワークの移動

3.3 ネットワークモデル

機動性に配慮した小規模組織ネットワークを構築運用する上で、必要な条件を次に示す。

- ネットワークの高い独立性
  ネットワークが移動すると、ネットワーク上で利用していたサービスの継続性が問題となる。例えば、他組織のメールサーバを利用していた場合、ネットワークの移動に伴いメールサービスは利用できなくなる。他のサービスについても同様の事態が生じるため、ネットワーク上で利用するサービスは極力自組織で運用し、ネットワークの独立性を高める必要がある。

- セキュリティの確保
  端末数の多少や規模の大小に関わらず、ネットワークや端末のセキュリティは厳重に確保する必要がある [8]。特に、ネットワークに機動性を持たせた場合、小規模組織のネットワークが移動した先のネットワークで、十分なネットワークセキュリティが確保されている保証はない。そのため、自組織で十分なセキュリティを確保する必要がある。

- 環境への適応
  ネットワークを構築する場合、ネットワークを構築するその場所の環境が問題となる。移動先の環境によってネットワークが運用できない状態になってはいけない。よって、ネットワークの移動に伴う環境の変化を考慮して、あらかじめそれらの変化に対応できるようにネットワークを構築する必要がある。

- 安価なネットワーク
  小規模組織がネットワークを構築する場合、小規模組織の資金力の少なさから安価にネットワークを構築できる必要がある。そのため、ネットワークの性能を考慮しつつ、可能な限り少ない資金力で構築できる必要がある。

- 長期間の運用を想定した態勢の整備

  ネットワークを構築する際、そのネットワークをどのくらいの期間運用するか想定しておくことは重要である。日単位の運用を想定した仮設型のネットワークでは、いかに目的に応じたネットワークを現地の環境に合わせて短期間で構築できるかが問題になる [52]。逆に、何十年単位の運用を想定した常設型のネットワークでは、構成機器やサービスの陳腐化、障害管理、構成員の流動性などが問題となる。

  機動性に配慮したネットワークを構築している場合、ネットワークの移動に伴いネットワークを再構築することはない。そのため、ネットワークを長期間に及んで運用することが想定される。ネットワークの構築時から、長期に及ぶ運用を想定した態勢を整える必要がある。

- 管理者の負担軽減

  小規模組織では、専任のネットワーク管理者の存在を仮定できない。一部の利用者が管理者を兼任する形でネットワーク管理に参加する場合が多いため、熟練した管理者でなくてもネットワークを管理し運用できる態勢を整える必要がある。

これらの条件を基に、機動性に配慮した小規模組織のネットワークモデル図を図 3.2 に提示した。これをもとに、各必要条件を詳しく議論する。

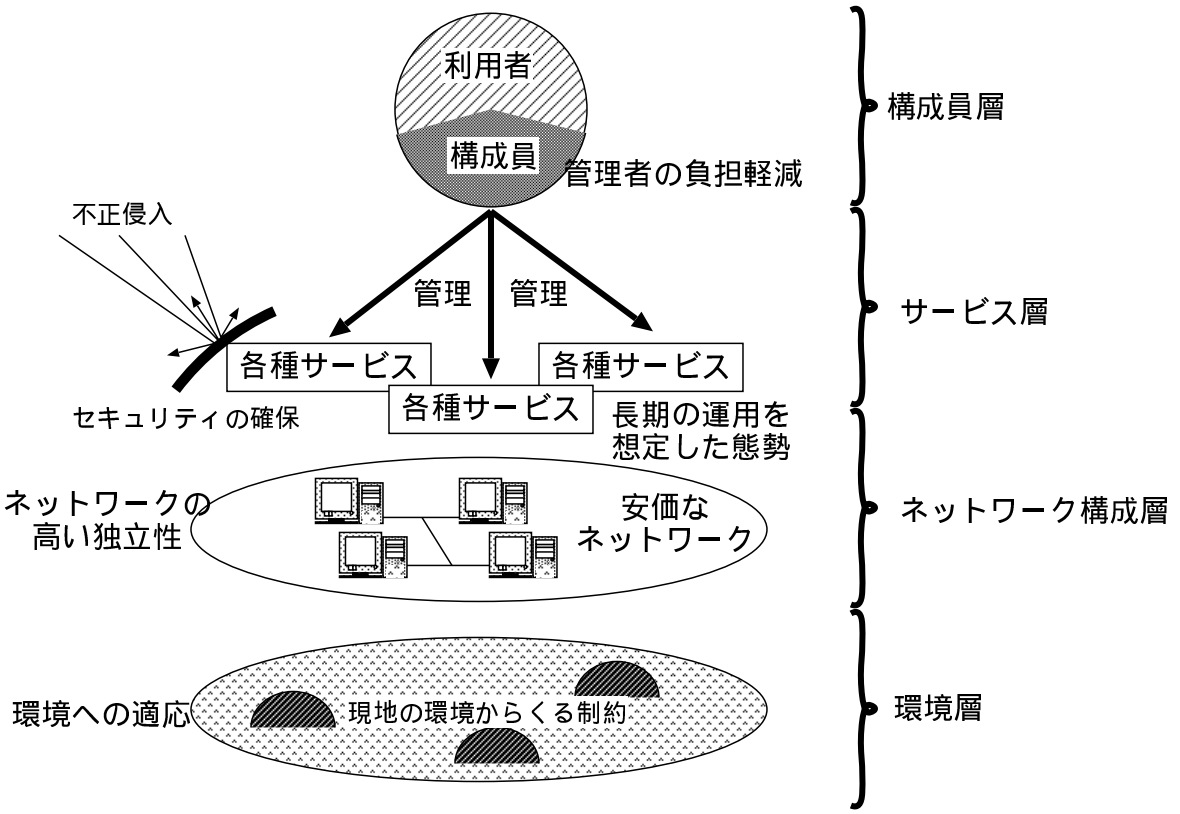

図 3.2: 小規模組織のネットワークモデル図

3.3.1 ネットワークの高い独立性

一般に複数のサービスを運用することは、管理者の負担となることが多い。とくに小規模な組織では、不要なサービスを運用することによる負担増は管理者の不足から無視できない。従って複数のサービスを運用する場合は、そのサービスは本当に必要か判断し、取捨選択する必要がある。例えば、WWW を利用しメールの交換がしたいだけならば、高トラフィックの原因となるニュースサーバを運用する必要はない。逆に多様なネットワークサービスを柔軟に運用したいというのであれば、DNS などの、様々なサービスの基本となるものから運用する必要がある。また例え必要なサービスであっても、導入のための環境が整備されていなかったり管理者の都合などから一度には導入できないかもしれない。このため、サービスを導入する順番を考え、判断基準を事前に定めておくことが重要である。

しかし、自組織でサーバを運用したからといっても、独立性が完全に保持できるわけではない。例えば、メールや WWW はメールアドレスや URL に、その組織のドメイン名を含む。このため、ネットワーク移動に伴いドメイン名が変更されるといままで利用していた電子メールや URL は利用できない。このような問題を名前空間の問題 [38][40] と定義する。

名前空間の問題を避けるため、例えば生涯に及んで利用できる生涯電子メールアドレスを利用し、そのメールアドレスから現在利用しているメールアドレスにメールを逐一転送する方法がある。しかし生涯電子メールアドレスはまだ完全に実現しているとはいえない。また、WWW ではページの移動先をリンクページという形で残す方法がある。しかし、この方法ではリンクページが途絶えるという問題が解決できない。さらに、サービスごとの個別の対応では、管理運用する管理者の負担が増加する問題がある。移動に伴うドメイン名の変更が問題の原因であるため、移動する組織自体が自組織でドメイン名を取得する方法 [39] が考えられる。ドメイン名を維持管理する負担も多くはなく、この方法ならばサービス毎に個別に対応する必要はない利点がある。

3.3.2 セキュリティの確保

不正なシステム侵入に対する緊急対応を中心にインターネットセキュリティの情報収集や分析、再発防止策の検討、セキュリティ技術の教育・啓発活動を行っている CERT や JPCERT による報告 (図 3.3, 図 3.4) では、不正アクセスの届出の報告が年々増加している。 CERT や JPCERT の活動が一般に認知され、届出の数が増加している事情はあるが、インターネットの普及による未熟な管理者の増加や不正アクセスツールの流布が原因で不正アクセスの件数が増えていると考えられる。セキュリティ対策が不十分だと、自組織が不正に侵入され被害を被る可能性がある。また、直接的な被害が無くても、自組織のネットワークが利用され、他の組織への不正侵入の手助けとなる可能性がある。

ネットワークのセキュリティを高める方法として、対外接続地点にファイアウォールを構築しアクセス制御を行う方法 [9] がある。警視庁の調査による日本の会社・大学のファイアウォール設置率は図 3.5 に示される。ファイアウォールの設置率が 50%弱と低いのは、ファイアウォールを設置する必要性の認識が低いためだと思われる。しかし、ファイアウォールは最近急増しているポートスキャンを用いた不正侵入を防ぐ手段として特に有効である。

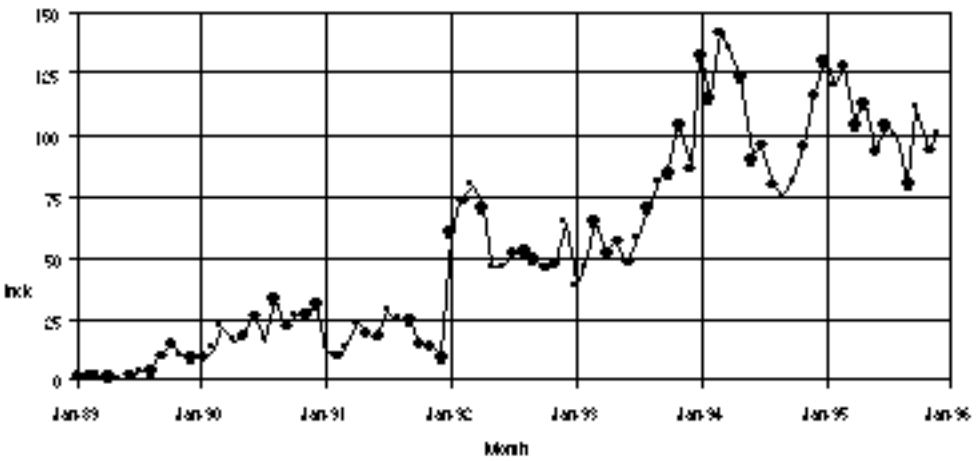

図 3.3: CERT に報告された不正アクセス届出数の推移

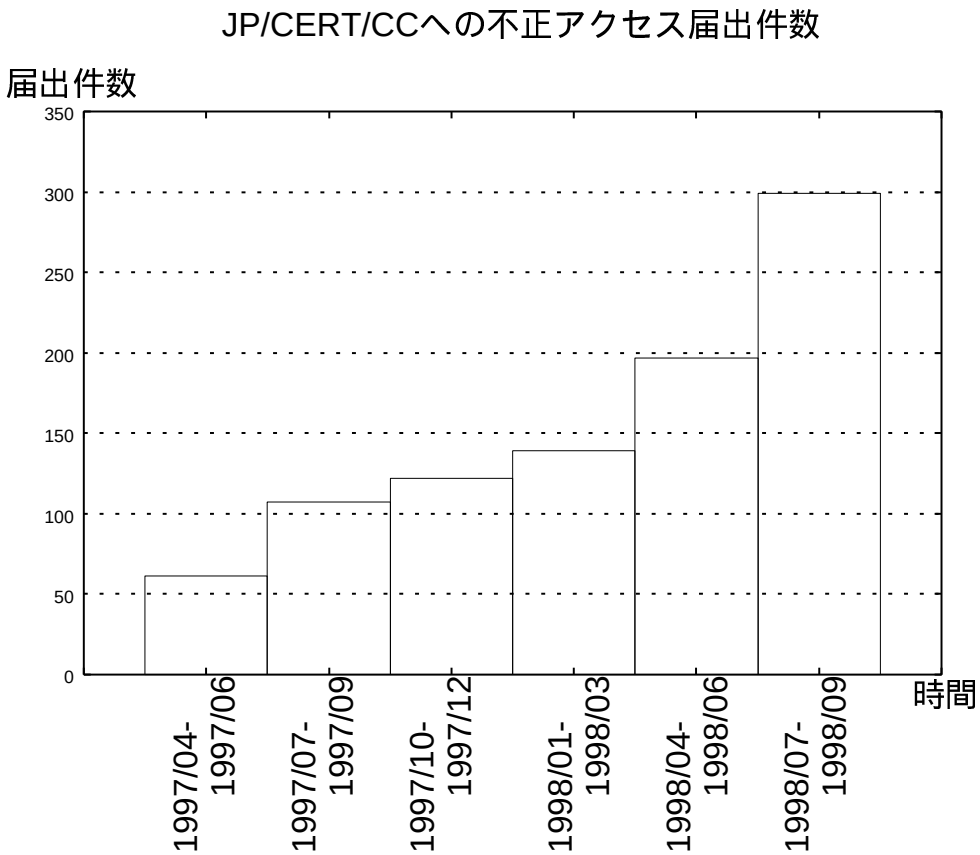

図 3.4: JPCERT に報告された不正アクセス届出数の推移

ファイアウォールを構築する上で重要なことは、どのような方針でアクセス制御を行うか

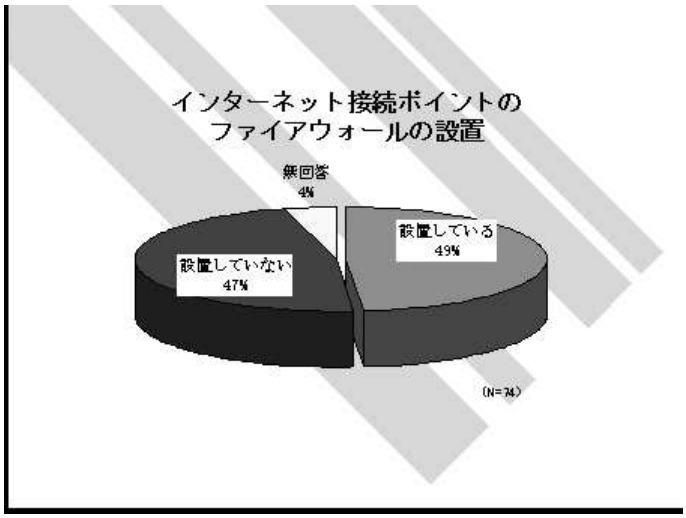

図 3.5: 日本国内におけるファイアウォールの設置状況

事前に決定しておくことである。また、決定した方針はネットワークの利用者に十分説明する必要がある。

このほかにも、ネットワーク自体の物理的な防御を考える必要がある [6]。侵入者による故意の通信路切断や計算機の破壊を防止するだけではなく、正規の利用者の不注意による通信線の切断なども防止する。そのためには、アクセス制限と物理的な環境が一致していることが望ましい。サーバなど管理者のみがアクセスする必要がある計算機は、利用者端末がある場所とは別の場所に設置するなどである。

3.3.3 環境への適応

ネットワークを運用するさい、構成機器が動作するのに十分な電源容量を確保する必要がある。小規模組織のネットワークは構成機器の数が比較的少ないとはいえ、その重要性は大規模組織のネットワークの場合と同様である。十分な電源容量を確保していない場合、何らかの事情で消費電力が電源容量を上回ったとき電源側で安全機能が働き停電が生じる可能性がある。停電による計算機の不意の停止は、ハードディスクなどの機器に被害を与え、障害の原因ともなる。ネットワーク全体の消費電力を算出する場合、個々の機器の消費電力を実際に計測するか、製造企業が情報を出す消費電力の値から算出する。計測時は、機器の起動時に生じる起電力に注意して最大消費電力を求める。

不意の停電に備えて 無停電装置などを利用することも重要である。無停電装置は高価であるため、小規模組織では金銭的コストの問題から全ての構成機器に給電できないかもしれない。どの構成機器を優先するか、どの構成機器には給電しないか、方針を明確にするべきである。

ネットワーク構成機器は、極端に高温や低温な環境、高湿度の環境では誤動作を生じる可能性がある。ネットワーク構成機器の設置してある場所の温度や湿度にも注意しなければならない。構成機器を密集して配置している場合、局所的に構成機器周辺が高温になる場合もあるため、通風性を高めて空気を循環させる等の対策を行う。ネットワークの構築には、その環境の対策まで含めた広い視野が必要である。

3.3.4 安価なネットワーク

小規模組織では、ネットワーク構成機器に金銭的なコストを十分にかけられない場合がある。そのため、できるだけ安価にネットワークを構築できる必要がある。また、保持しているネットワーク構成機器の種類や個数を把握することも重要である。不必要なネットワーク構成機器を購入しないとともに、一度購入したネットワーク構成機器の存在場所や利用状況を知ることは金銭的コストの削減に有効である。

3.3.5 長期間の運用を想定した態勢の整備

小規模組織では、構成員の流動性の問題からネットワークの運用から得られた知識が定着しない傾向にある。このため、構成員個人の熟練度に依存した運用態勢をつくるべきではなく、管理者個人がネットワークの運用を通じて取得した知識は構成員全員に共有されなければならない。そのため、構成員間の情報共有を密にするとともに、卒業や退職等でそのネットワークを利用しなくなった構成員が持つ知識を後から参照できる仕組みが必要である。

管理者は、利用者に対してログインアカウントやメールアカウントなど各種のアカウントを発行する。複数の利用者が同一アカウントを希望した場合など、アカウントの衝突がしばしば問題となる。ISP などで一般的に行われている方法では、アドレスの衝突の可能性を考慮してアカウントの申請時に複数個のアドレスを事前に申請させ、アドレスの衝突が起きないアカウントを割り当てている。しかし、現在では複数のアドレスを保持する人も増え、複数のアドレスを同一の名前で取得したいという要求から、任意のアカウント名を利用したという要望も増加しつつある。小規模組織では、その構成員の少なさからアドレスの衝突が発生する問題は生じにくい。

第4章　研究室内ネットワークの設計

前章のモデルのもと、筆者らの研究室では機動性に配慮した小規模組織ネットワークを実現するべく 1996 年度から研究室内ネットワークの再構築をすすめている。本章では、この研究室内ネットワークの設計を取り上げる。まず初めに、温度や電源問題への対策などを行う「環境層」について述べる。次にネットワークトポロジやネットワーク構成機器を決定する「ネットワーク層」に述べる。そしてネットワーク上で運営する各種サービスを決定する「サービス層」について述べ、最後に運営態勢や利用者管理態勢を決定する「構成員層」について述べる。

4.1　環境層

この節では、ネットワークの物理的な防御と電源容量の確保について議論する。

4.1.1　物理的な防御

研究室内ネットワークでは、サーバとなる計算機は利用者が普段利用しない鍵のかかる部屋に集める。これにより利用者の注意による電源切断などの事故を防げる。鍵はネットワークの構成員で共同管理している。構成員の不正行為や妨害行為に対処できないが、研究室内部ネットワークでは利用者の信用性を仮定しているため問題にはならない。

4.1.2　不意の停電対策

研究室ネットワークでは、瞬電や停電対策のためネットワーク構成機器を無停電装置で給電する方針にし、給電の優先順位を表 4.1 のように決定した。無停電装置が確保できしだい、優先度の高い機器から順次無停電装置の接続を行う。ルータ計算機やサーバ計算機が停電に伴う不意の電源切断で故障した場合、ルータ計算機やサーバ計算機は多くの利用者が利用するため利用者端末の故障に比べて影響が多い。プリンタや家電機器はネットワークに対する影響が低いため、給電対象から除く。

長時間の電力供給の停止

ネットワーク機器に長時間電力が供給されない状態が予想されるとき、管理者は全ての計算機やネットワーク機器を停止しネットワークの運用を停止する必要がある。しかしこ

高優先度の機器 ルータ計算機、サーバ計算機、ハブ など

低優先度の機器 利用者端末、 ディスプレイ など

給電しない機器 プリンタ、家電機器 など

表 4.1: 無停電装置の優先度

の作業は管理者にとって負担の大きい作業である。それは主に次の 2 つの原因に起因する。

不定期な停電

停電は日中だけではなく、夜中や祭日にも発生する可能性がある。小規模組織では、ネットワーク管理者が常時ネットワークを保守や管理しているわけではない。そのため、停電時にネットワーク管理者が不在である可能性がある。そのため、不意の停電に備えた事前の対策が重要である。

停電が生じる時間帯に管理者の不在が予想される場合は、事前にネットワークの運用を停止し、復電後は適当な時間にネットワーク管理者が計算機を起動して、ネットワークの運用を再開することが一般に行われる。しかし、ネットワークの不必要な停止は避けるべきである。なぜなら、メールサーバはメールを常時送受信し、WWW サーバは世界中の WWW 利用者に情報を常時提供しているためである。停電にネットワークを停止し、復電後は速やかにネットワークの運用を再開する必要がある。これを実現するためには、ネットワーク管理者は停電やその後の復電時にネットワークの保守管理を行っていなければならない。これはネットワーク管理者にとって負担の大きい作業である。

各々の計算機の依存関係

停電時には管理者は計算機を順次停止し、復電時には管理者は計算機を順次起動していく。しかし、各々の計算機の間には依存関係があり、計算機の停止や機動の順番には順序関係が存在する。正しい順番で計算機を起動または停止しなければ、サービスが起動されなかったり、起動に不必要な時間を必要とする。例えば、NIS サーバが起動していないとき、NIS クライアントを起動しても正しく起動しない。ファイルシステムを他の計算機に公開しているときは、その公開先の計算機から順次停止していく必要がある。さらにその計算機が他の計算機にファイルシステムを公開している可能性も考慮する必要がある。ネットワーク管理者に十分な管理経験と知識がなければ、この順序関係は把握できない。

計算機の起動や停止の順番を考慮する必要がなく、任意の時刻に停止や起動が可能ならば、管理者の負担軽減に有効である。まず、「 各々の計算機の依存関係 」の問題を解決するために、管理文書の作成が考えられる。ネットワークの起動・停止の方法を記した詳細な文書を事前に作成し、停電・復電時に、管理者はそれに従い作業する。一旦文書を作成した後は、運用に応じて適時変更を加えていく。

次に、「不定期な停電」の問題を解決するため、まず Personal Computer(PC) の起動や停止を考察する。PC の電源スイッチには、主に AT と ATX と呼ばれる 2 種類の規格がある。この規格の違いによって、PC の起動時や停止時に計算機の扱いに差異が生じる。

AT 規格

AT 規格の PC は、電源の供給がないと計算機が停止する。復電時に電源の供給が再開されると、計算機が起動する。能動的に計算機を停止させるには、管理者は電源スイッチを利用する。

ATX 規格

ATX 規格の PC は、電源の供給がないと計算機が停止する。復電時に電源の供給が再開されても、管理者が電源スイッチを明示的に入れない限り計算機は起動しない。能動的に計算機を停止させるには、管理者は電源スイッチを利用するか、管理者がソフトウェア上から制御する。

停電が発生したとき、AT 規格と ATX 規格の両方の規格の計算機とも、計算機が停止する。その状態から復電したとき、AT 規格の計算機は即起動される。しかし、復電直後に計算機を起動させるのは避けるべきである。なぜならば、電力の供給テストのためなどで復電直後は停電や復電が繰り返されるためである。そのため、ある一定の時間を待って十分安定して電力が給電されるのを確認してから計算機を起動しなければならない。これは AT 規格の計算機では実現できない。各計算機になんらかのハードウェアパッチを当てて、電源の制御を補佐する必要がある。

4.2 ネットワーク構成層

ネットワーク構成機器や端末の選定について議論する。

4.2.1 端末の選定

ネットワークの構成機器は、性能と金銭的コストを考慮して安価な PC を利用し、PC UNIX で運用を行う。「PC UNIX を用いる方法は経済的なインパクトは少ないが、障害発生などによる人的コストが却って高くつく」という説 [30] がある。本研究室ネットワークでは障害発生に十分対処できる態勢を整えることで、この問題を解決する。

異なるプラットホームの端末を管理するのは、一般に管理者にとって負担が大きい。利用者から見ると、利用する端末毎にインターフェイスや設定が異なると端末を利用しづらい。このため、利用者がどの端末を利用しても同じ操作・環境で利用できることが重要である。小規模組織では、サーバやクライアントとなる計算機は、せいぜい数十台の規模である。そのため、全ての計算機を同じプラットホームで統一することは不可能ではない。

研究室内ネットワークでは、統一した計算機プラットホームとして PICKLES 端末 [18][47] を利用する。PICKLES 端末は PICKLES プロジェクトの一環として大野研究室が開発し

ている端末であり、PC UNIX の一種である BSD/OS を利用している。PICKLES 端末を利用する者は、全ての PICKLES 端末で常に同じ環境で端末を利用できる。そのため、管理者にとっては端末毎に異なった管理方法を憶える必要が無い。利用者は常に同じ環境で端末を利用できる。

4.2.2 ファイアウォールの構築

ファイアウォールを設けるにはまず、市販のファイアウォール製品を購入するか、フリーソフトウェアによって構築するか決定しなければならない。現在では、多くの市販ファイアウォール製品が開発・販売され、フリーソフトウェアも多くの種類が開発されている。フリーソフトウェアを組み合わせてファイアウォールを構築した場合、市販ファイアウォール製品を購入した場合に比べて販売元によるサポートを受けられないなどの問題がある。しかし、フリーソフトウェアはソースコードが公開されているため、構築時や問題の発生時に、インターネット上のコミニュティとの情報交換による解決や、ソフトウェアのソースコードを基にした解決ができる。研究室内ネットワークでは、フリーソフトウェアの利点と金銭的コストの点から、フリーソフトウェアを組み合わせてファイアウォールを構築する。

次に、ファイアウォールの形態には大きく分類して下記の 3 つの形態があり [9]、どの形態を採用するか決定する。これは、ネットワークトポロジの問題とも密接な関わりがある。

デュアルホームホストによるファイアウォール (図 4.1)

自組織が構築する内部ネットワークとインターネットなどの外部ネットワークとを接続する計算機 (デュアルホームホスト) は、IP パケットを交換しない。このため、内部ネットワークから外部ネットワークの通信や、外部ネットワークから内部ネットワークへの直接の通信はできない。内部から外部ネットワークへの通信は、デュアルホームホスト上で運用するプロキシサーバを経由して行う。

この方法では、利用者が利用するサービス毎にプロキシサーバを運用し、管理しなければならない。プロキシが運用されていないサービスは利用できない。また、新しく開発されたサービスは、そのサービスに対応するプロキシサーバが開発されるまで時間がかかる。プロキシサーバにより、利用者の認証や利用者履歴の保存が可能である。内部ネットワークでは、プライベート IP アドレスが利用できる。

要塞ホストを利用したファイアウォール (図 4.2)

内部ネットワークと外部ネットワークを接続する計算機 (チョークホスト) で、パケットフィルタリングと呼ばれる通信パケットの制限を行う。

内部ネットワーク内には、要塞ホストと呼ばれる計算機を用意し、その計算機を介した通信のみを許可する。要塞ホストは、外部ネットワークから接続されることを想定し、その通信を適切に処理する目的のホストを指す。チョークホストを通過するパケットは、外部から要塞ホストへの通信か要塞ホストから外部への通信を行うパケットのみである。

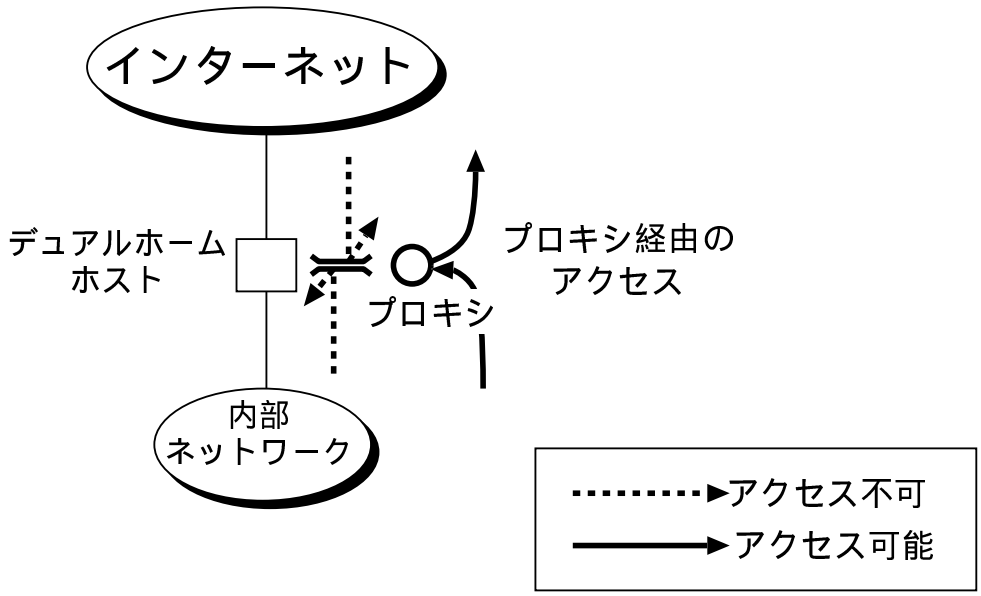

図 4.1: デュアルホームホストを利用したファイアウォール

外部ネットワークに接続する計算機でパケットフィルタリングをするだけであり、構成が簡単である。パケットフィルタリングの設定により、柔軟なパケットの制限ができる。パケットフィルタリングの設定が複雑になると、適切に管理できなくなる問題もある。チョークホストは、パケットの宛先や送り元などの簡単な記録しかできない。

境界ネットワークを利用したファイアウォール (図 **4.3**)

要塞ホストを利用した形態とほぼ同形態だが、外部ネットワークと内部ネットワークの間に境界ネットワークを配置する。境界ネットワーク上には、一つまたは複数の要塞ホストが運用される。また、境界ネットワークと内部ネットワークの間にもチョークホストを設ける。

境界ネットワークに利用者ネットワークのパケットが流れないため、万一要塞ホストが不正侵入されたときでも、ネットワーク上のパケットは盗聴されない。また、外部ネットワークの不正侵入者が内部ネットワークに侵入する際、2 つのチョークホストを通過しなければならず安全性は高い。境界ネットワークと内部ネットワークで管理領域が分けられるため、管理が容易である。境界ネットワークは、非武装地帯 (De-Militarized Zone) や防御ネットワークとも呼ばれる。この形態のファイアーウォールでは、外部チョークホストと内部チョークホストを一つに統合した形態もある (図 4.4)。

大野研究室では構成員はネットワークの研究に従事するため、WWW やメールなど予め決まったアプリケーションだけを利用するわけではなく、多様な通信やネットワークを利用した実験を行う。そのため、デュアルホームホストを利用したファイアウォールは外部

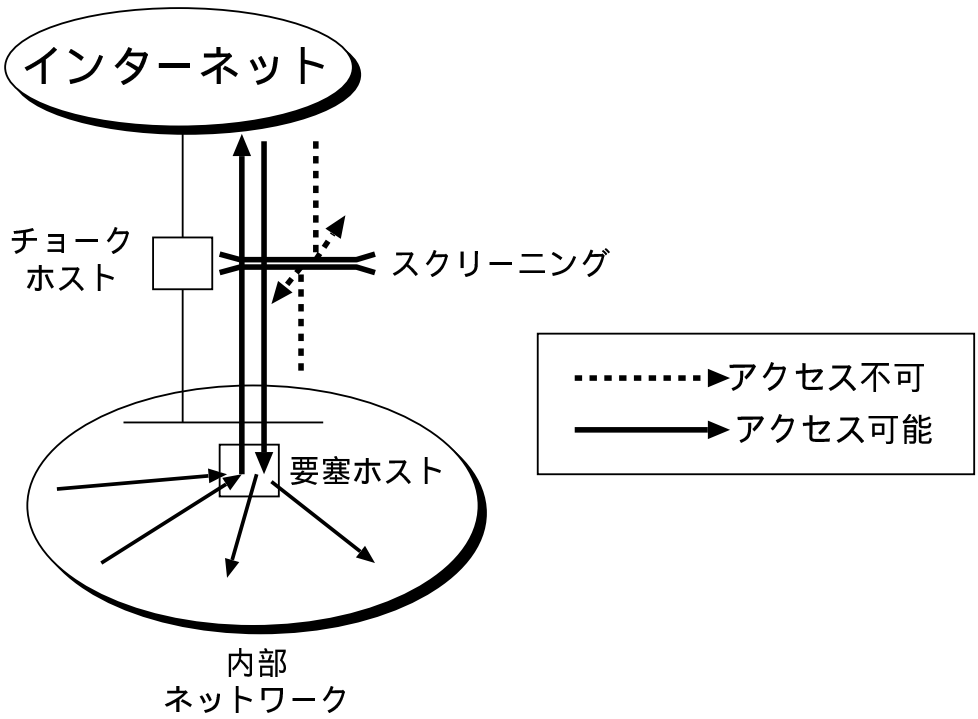

図 4.2: 要塞ホストを利用したファイアウォール

ネットワークとの通信にプロキシを中継しなければならず利用者の利便性を損なうため不適切である。

要塞ホストを利用したファイアウォールでは、利用者に要塞ホストとの通信以外を許可しないため、利用者の利便性を損なう。しかしこれは、スクリーニングの設定を工夫することで回避できる。要塞ホストと利用者端末が同一のネットワークに混在するため、安全上の問題が生じる。

境界ネットワークを用いたファイアウォールでは、境界ネットワークに要塞ホストを集めるため、要塞ホストを利用したファイアウォールに比べて安全性が高い。また、管理領域が、境界ネットワークと内部ネットワークに別れているため管理が容易である。通常では、利用者に要塞ホストとの通信しか許可しないため、利用者の利便性を損なう。しかしこれはパケットフィルタリングの設定により回避できる。

上記の点から、研究室内ネットワークでは境界ネットワークを利用したファイアウォールを構築する。しかし研究室内ネットワークでは、利用者の利便性を優先させるため、パケットフィルタリングの設定を工夫し、内部ネットワークから外部ネットワークの利用は基本的に制限しない方針とした。研究室内ネットワークでもちいたファイアウォールを図 4.5 に示す。

ファイアウォールを構築した後、運用方針として最初に基本的な方針を決める必要がある。ファイアウォールを運用する基本的な方針には、次の 2 つの方針がある。

- デフォルトオフ

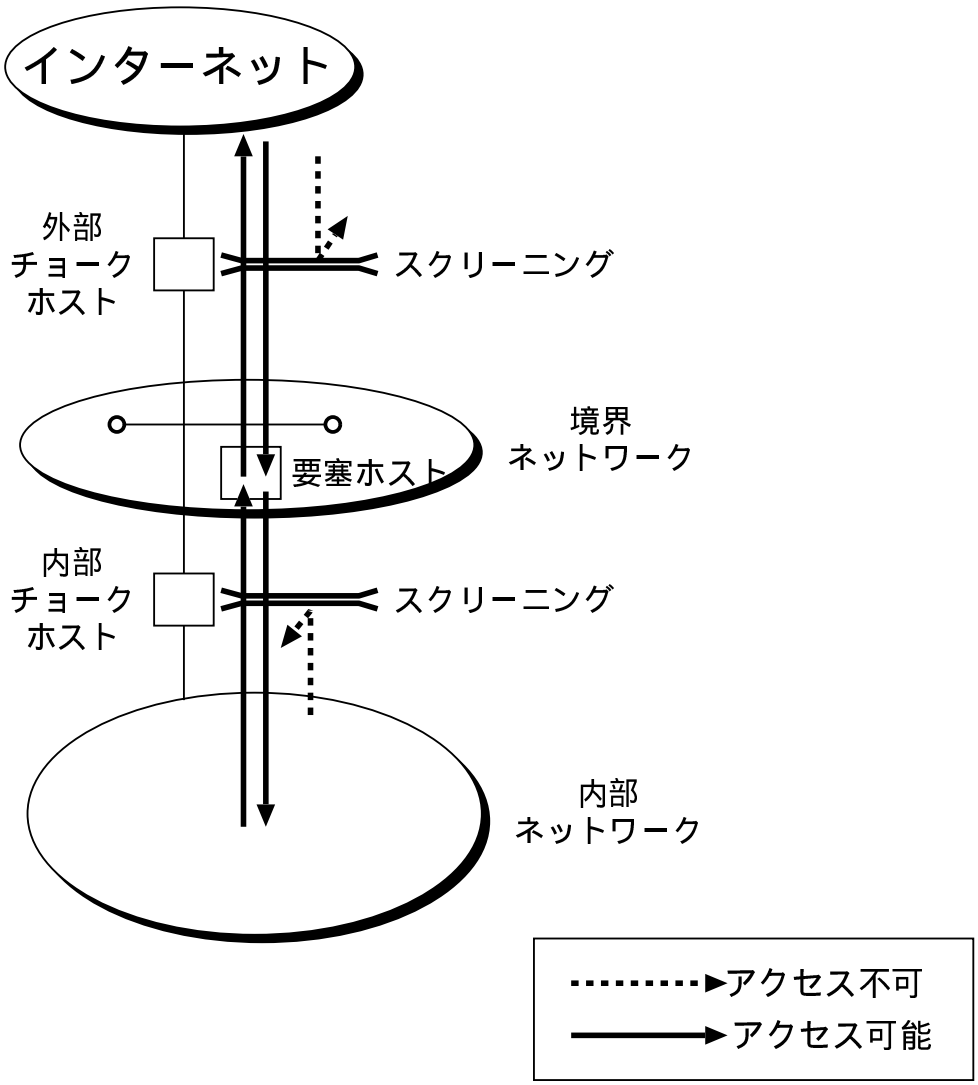

図 4.3: 境界ネットワークを利用したファイアーウォール

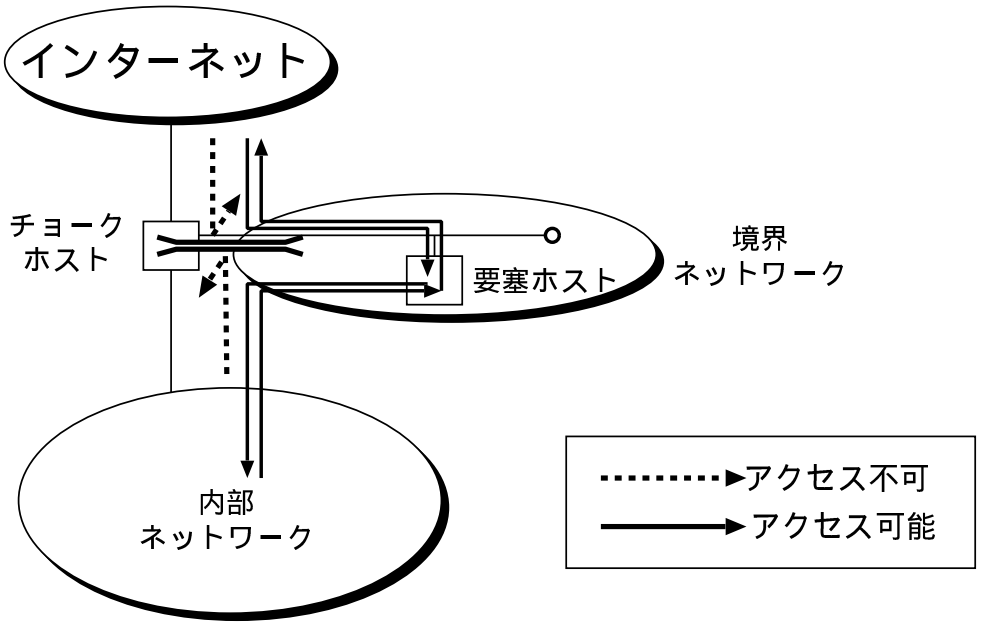

図 4.4: 内部チョークと外部チョークを統合したファイアーウォール

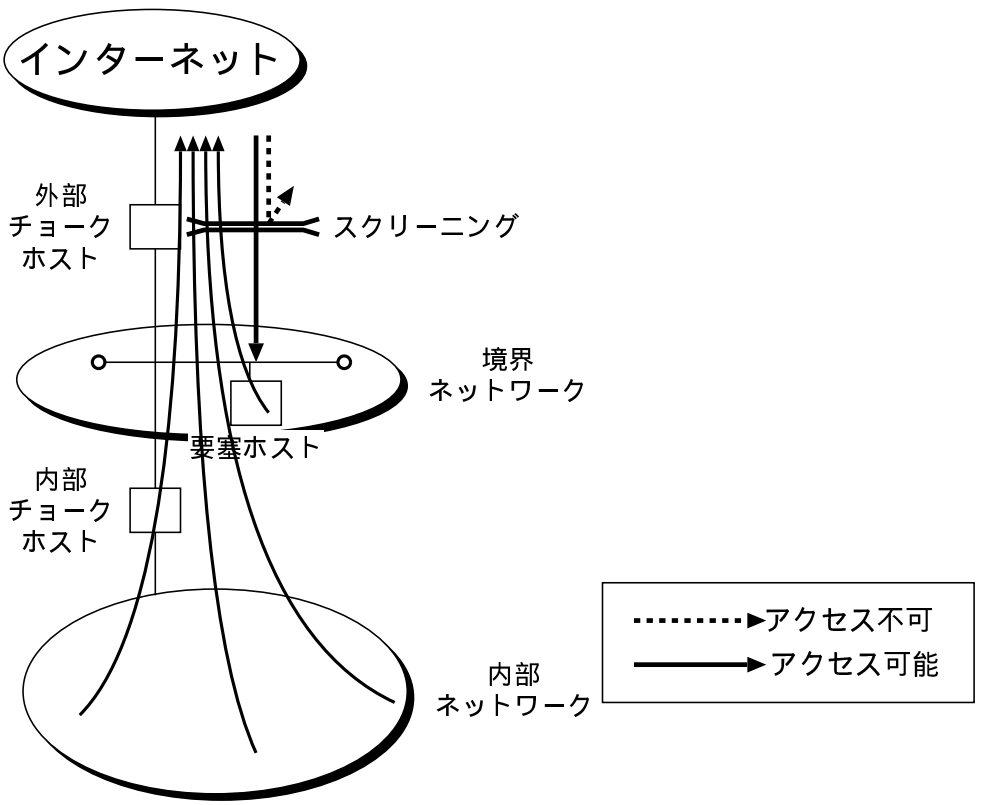

図 4.5: 研究室内ネットワークのファイアーウォール

全ての動作やサービスを原則禁止にし、安全に提供できる正当な動作やサービスのみを許可する。

- デフォルトオン
  問題がある動作やサービスのみを禁止し、その他の動作やサービスを原則許可する。

インターネット上の危険性や脅威を、管理者が全て事前に予想するのは困難である。多くの場合、危険性や脅威が判明するのは事件や事故が生じた後である。そのためデフォルトオンの方針でフィアウォールを構築した場合、何らかの事件や事故が発生した後でなければその問題が明らかにならない。その時にはネットワークに重大な被害が生じている可能性がある。デフォルトオフの方針でフィアウォールを構築した場合、フィアウォールの設定が不適切だと内部ネットワークの利用者の利便性を不必要に妨げる。

研究室内ネットワークでは、デフォルトオフの考え方を基本とした。小規模組織ではその構成員の少なさから、構成員相互の意志疎通が十分行いやすい。そのため、デフォルトオフを基本方針とし、研究室に所属する全構成員間の立ち会いのもとでスクリーニングの試験を行い、ファイアウォールの設定を確認する。

4.2.3 物品管理

物品管理はネットワーク管理の中の重要な要素である。物品管理の目標は、ネットワーク構成機器などネットワーク運営や管理に必要な物品を適切に管理し、購入年度や個数を把握し盗難などを未然に防ぐことである。小規模組織では、構成機器を余分に確保する金銭的な余裕がないため、現在の構成機器の個数を把握し、必要な個数を調達することは重要である。そのためには、全ての物品に対して固有の番号を一意に割当て、データベースで管理する。

4.2.4 IPv6 への対応

IP アドレスの枯渇や経路制御表の増大などの問題に対応するため、現在広く利用されているインターネットプロトコル IPv4 に変わるべく、次世代のインターネットプロトコルである IPv6[27] の研究が進んでいる。研究室内ネットワークでは、IPv6 に対応するため IPv4 と IPv6 の両方に対応させるデュアルスタック戦略をとる。

4.2.5 NAT

各計算機に一意に付与される global IP アドレスの枯渇が世界的に問題となっている。そのため、新規に IP アドレスを取得することが困難に成りつつある。多くの小規模組織のネットワークでは、外部ネットワークと直接通信しない内部ネットワークの計算機には global IP アドレスを付与せず、ネットワークを構築する組織が任意に設定できる private IP アドレスを付与する。また、内部ネットワークの計算機が外部ネットワークと通信する

場合でも、glocal IP アドレスを付与し、外部ネットワークへの接続地点で NAT[17] 技術を用いて、global IP アドレスと private IP アドレスの変換を行う。

ポート変換の技術を用いて、一つ global IP アドレスに複数の IP アドレスを割り付ける NAPT という技術を、小規模組織では用いることも多い。しかし NAPT はポート番号の変更をともなうため、通信後に動的に割り当てたポート番号を使って通信を行う ftp のようなサービスは、スクリーニングとの関係で問題が生じる場合があるため、事前に別途対応する必要がある。大野研究室の構成員はネットワークの研究をしているため、このようなサービスを利用する可能性がある。ftp など良く知られたサービスを除けば、利用できないサービスが生じるのは避けたい。このため、NAT や NAPT は用いずに、全ての計算機に glocal IP アドレスを割り当てる方針とした。

現在の IP は IPversion4 と呼ばれる。IP アドレスの枯渇などの理由から次世代インターネットプロトコルである IPversion6(IPv6) の開発がすすんでおり、IPv6 を利用したネットワークも増加しつつある。IP アドレスの枯渇に対する解決方法として、IPv6 を利用したネットワーク構築の方法もある。

4.3 サービス層

4.3.1 導入するサービス

大野研究室の構成員はネットワークに関する研究を行う。そのため、ネットワーク運営の基本となる DNS やメールサービスの設定を変更することが頻繁にある。また、通常とはことなるサービス利用を実験として行うことがある。これらを迅速に柔軟に行うため、ネットワーク運営の基本となるサービスを独自の方針で運用する必要がある。研究室内ネットワークでは、インターネットで一般に利用されるサービスは独自に運用する方針にした。DNS[21] やメールサーバ、WWW サーバなど全員が利用する必須な項目を最優先で運用し、ニュースサーバや IRC サーバなど必ずしも全員が利用しないサービスは順次運用していく方針である。

4.3.2 ドメイン名の取得

ドメイン名を取得する場合、どのトップレベルドメインの下に属するサブドメインを取得するか決めなければならない。トップレベルドメイン名の種類は、多く分けて次の 3 種類がある。

- gTLD(generic Top Level Domain)
- ccTLD(contry code Top Level Domain)
- iTLD(international Top Level Domain)

gTLD は、「.com」や「.org」、「.net」など地理的な位置によらず一般に利用できるドメイン名である。ccTLD は、ISO-3166 に基づく 2 文字コードで構成され、国別に割り当て

られるドメイン名である。日本に割り当てられている「.jp」などが該当する。iTLD は、ITU など国際組織が利用するドメイン名で、「.int」が該当する。

本研究室のような非営利組織がドメイン名を取得する場合、日本の ccTLD である jp ドメイン名の下にドメイン名を取得する方法と、非企業の組織を収容する gTLD である org ドメイン名の下にドメイン名を取得する方法があった。本研究室ネットワークの海外への移動の可能性も考慮すると、日本という地域に縛られる jp ドメインよりも、地域を限定しない gTLD である org ドメインの方が適切である。そのため、本研究室では org ドメインの下に、「ohnolab.org」ドメイン名を習得する方針とした。

4.3.3 IP アドレスの割り当て

ネットワークを運用していると、計算機に付与した IP アドレスと計算機の計算機名の対応が変更される場合がある。変更が繰り返されると利用されない IP アドレスが増加し、IP アドレスの利用率が低下する。これとは逆に、本来計算機に付与していない IP アドレスに計算機が不正に接続されているのを管理者が看過する可能性もある。

他の計算機に付与されている IP アドレスを重複して付与すると、そのネットワーク上で IP アドレスの重複が発生する。この重複がルータとなる計算機の IP アドレスで生じた場合、そのネットワークに繋がる全ての計算機はルータを通して外部に接続することができない。また、接続前に ping などのコマンドを利用して該当 IP アドレスの利用状況を調べられるが、一時的に当該計算機がネットワークから外れているだけかもしれないため、その IP アドレスが利用可能であるか必ずしも判断できない。これらの理由から、IP アドレス割当の方針を事前に決め、それに沿った運用を行う必要がある。

4.4 構成員層

利用者のアカウント

研究室内ネットワークでは、アカウントは先に取得した方が優先されるという先願主義をとる。また、インターネットサービスプロバイダなどの一般の組織では使われなくなったアドレスを再利用している。そのため、正しいメールアドレスにメールを送ったにもかかわらず、新たにそのメールアドレスに割り当てられた別の人へメールが到達する事故が生じる可能性がある。このため、研究室内ネットワークでは各種アドレスの再利用を行わない。

4.4.1 大野研 FYI

小規模組織ネットワークの管理は複数管理者による協調管理となるため、管理者各自の知識を互いに共有化する必要がある。組織内の構成員が比較的頻繁に入れ替わる流動性に対処するため、構成員がネットワークの運用や利用から得た経験や知識を、その組織自体の知識として定着される仕組みが必要である。

大野研究室では、これらの必要性から大野研 FYI(For Your Information) 制度を制定した。この制度では、各計算機毎のアプリケーションのインストール記録などの管理者間で共有するべき知識を、電子文書化して残す制度である。この制度により、ある計算機の設定は卒業生が行ったため、その人に問い合わせなければ詳細が判明しないなどの事態を防げる。

第5章　研究室内ネットワークの運用

前章の設計方針に基づいて設計した研究室内ネットワークの構築と運用について、本章では述べる。

5.1　概要

大野研究室では、1996 年度から研究室内ネットワークの再構築を進めている。本節では大野研究室内ネットワークの歴史の概要を示す。日時を含めた詳細な歴史は付録にまとめた。

ここでは大野研ネットワークの歴史を 3 つの時期に分類した。まずはじめは、1997 年 3 月以前の、ネットワーク機動性に配慮したネットワークを構築する前の、「旧ネットワーク期」である。この期間では、「利用者一人に一台の計算機を配置する」という目標を実現した。この期間の利用者端末には、X 端末やワークステーション、PC UNIX の一種である BSD/OS を用いた PC など、多種多様な計算機が用いられた。

1997 年 4 月から 1998 年 3 月までは、「ネットワーク構築期」である。この時期に、現在とほぼ同じトポロジのネットワークが構成された。主要なサーバ計算機には、PCIKLES 端末が用いられた。ohnolab.org ドメイン名を取得したのもこの時期である。

1998 年 4 月から 1999 年 3 月までは、「ネットワーク運用整備期」である。この時期はネットワークの運用体制を確立していく時期であり、ネットワーク管理に必要な各種のガイドラインが決定された。構成機器にも余裕が生じてきており、「4 年生にも Pentium 計算機を」という目標のもと、高速な Pentium CPU を持った計算機をほぼ全ての利用者に割り当てられた。

旧ネットワーク期 (~ **1997** 年 **3** 月)

- 物品管理システム運用開始
- PC 用音源カードとメモリの整備
- 第 1 回棚卸し

ネットワーク構築期 (**1997** 年 **4** 月 ~ **1998** 年 **3** 月)

- ネットワークトポロジ変更

- サーバ計算機の全 PICKLES 化
- IPv6 網構築
- ohnolab-cfp 開始
- 大野研 FYI 制度運用開始
- 管理者権限取得ガイドライン決定
- 独自ドメイン名取得
- 電源周り整備
- 利用者領域の制限 (quota) の開始
- スクリーニング開始
- サーバ計算機の無停電電源設置

ネットワーク運用整備期 (1998 年 4 月 ~)

- ベンチマークガイドライン作成
- ssh 導入
- Reborn System 運用開始
- 利用者端末の無停電電源設置

5.2 旧ネットワーク期

1997 年 3 月までの期間で、計算機などのネットワーク構成機器の整備に重点が置かれた。この時点でのネットワーク構成図を図 5.3 に示す。このネットワークは、NFS と NIS の利用を前提として構築されていた。

利用者が利用する各種のコマンドなどは、NFS で共有していた。利用者端末として、PC や X 端末、ワークステーションが数多く利用された。この時期はネットワークの運用体制が明確になっておらず、ネットワーク管理技術に長けた構成員が管理者として管理を行った。

5.2.1 物品管理システム

大野研究室の野田らが 1996 年 5 月から開発し運用している物品管理システム [50] は、各々の物品に一意に付与する「物品番号」とその全ての物品番号を管理する「物品データベース」から構成され、大野研究室内の物品を一元管理する。

物品番号
: 大野研究室で購入した、電気を通して利用する物品全てに対して、各々を一意に区

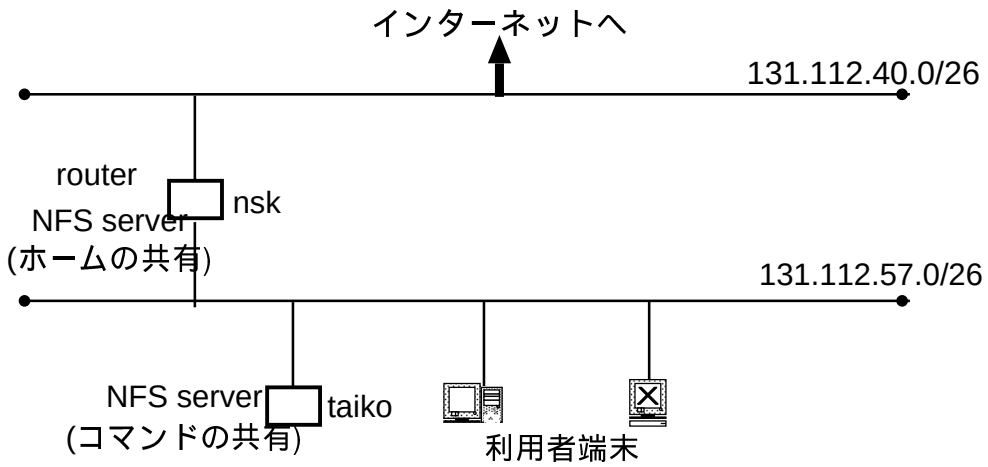

図 5.1: 1996 年度ネットワーク構成

別する固有な番号を発行する。これを物品番号と呼ぶ。現在の物品番号体系は下記の通りである。

物品番号 (6 桁) = 購入年度 (2 桁) + 通し番号 (4 桁)

購入年度は、西暦の下 2 桁を利用する。通し番号は対象となる物品が研究室に到着した時点で互いに重複しないように付加される。

各物品に割り当てられた物品番号はシールに印刷され、各物品に張り付けられる。シールは物品を購入した予算により特有な色が、割り当てられている。赤色のシールは、その物品が校費で購入されたことを示す。橙色は共同研究費または受託研究費、黄色は委任経理金、または奨学寄付金で購入されたことを示す。これらの色の他にも、黒や緑、青、白のシールが存在する。

一例をあげると、図 5.2 は物品番号が「970248」で、シールの色は黄色である。そのためこのシールを見れば、この物品が 97 年度に購入された物品で、委任経理金または奨学寄付金で購入されたことがわかる。より詳しい購入年月日や購入店を知りたいときは、この物品番号をキーに後述の物品番号データベースを検索する。

物品番号データベース

大野研究室で管理する各物品ごとに、物品番号や購入年月日、発注年月日、購入金額、設置場所、出資元、発注番号、発注先の情報が記載されている。物品ごとに登録されている情報は表 5.1 の通りである。

5.2.2 第 1 回棚卸し

96 年度末に 第 1 回目の棚卸し作業を行った。構成員全員が棚卸し作業に参加し、実際にひとつひとつの物品から物品番号シールと物品データベースとの整合性を調べた。その目

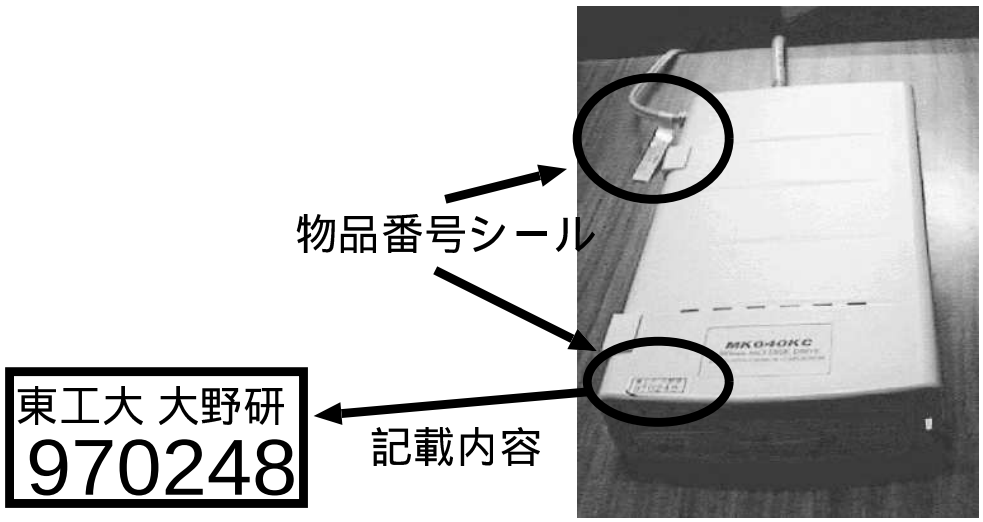

図 5.2: 物品番号により管理された MO ドライブ

物品番号 物品毎に固有な番号

購入日 物品の購入日

発注日 物品の発注日

購入額 物品の購入金額

場所 物品が現在存在する場所

出資元 予算区分

発注番号 発注作業中に割り当てる番号

発注先 発注先の店名

表 5.1: データベース登録情報

的は紛失した物品を明らかにするとともに、物品の現状を台帳に反映させることである。第 1 回棚卸しの結果を下記に記す。

- 調査物品総数 ... 2200 個
- 行方不明物品数 ... 54 個

研究室内で管理している物品総数は 2200 個で、紛失物品は 54 個であった。物品紛失割合は、全物品数の 2.5%程度である。紛失物品は物品データベースからその製品名や購入予算などがわかるため、必要に応じて新たに購入するなどの対策がとれる。

5.3 ネットワーク構築期

1997 年 4 月から 1998 年 3 月の間である。この期間で、現在稼働しているネットワークとほぼ同じトポロジーのネットワークが構築された。

5.3.1 ネットワークトポロジーの変更

ネットワークトポロジの変更を行った。稼働中のネットワークから新しいトポロジのネットワークへ円滑に移行するため、中間状態を経て移行させた。

図 5.3 移行前の状態

図 5.4 移行中の状態。移行前のネットワークと移行後のネットワークとが一時的に両方運用されている。

図 5.5 移行後の状態

最終的な目標では、ファイルサーバの障害対策としてファイルサーバをミラーするミラーサーバを設置する予定だったが、ミラーを行う予定の計算機の設定が終了せず実現しなかった。これは 1999 年 1 月現在でも実現していない。

5.3.2 全ての主要なサーバ計算機の PICKLES 端末化

1997 年 7 月の下旬に WWW サーバを PICKLES 端末で稼働させたのを始めとして、非 PICKLES 端末で運用していたルータ計算機やメールサーバを順次 PICKLES 端末で置き換えた。1997 年 10 月には、ルータ計算機とメールサーバ、WWW サーバが PICKLES 端末 (PICKLES 1.61 β) で運用されるようになった。これにより、管理者は異なるプラットホーム毎の計算機の管理方法を習得する必要が無くなり、PICKLES 端末の管理方法を習得するだけで良くなった。これにより統一した方針の元で管理可能になり、管理者の負担が減少した。

PICKLES 端末は、通常 2 台のハードディスクから構成される端末である。しかしこれらの計算機では一台のハードディスクから構成される mixPICKLES と呼ばれる仕様の PICKLES

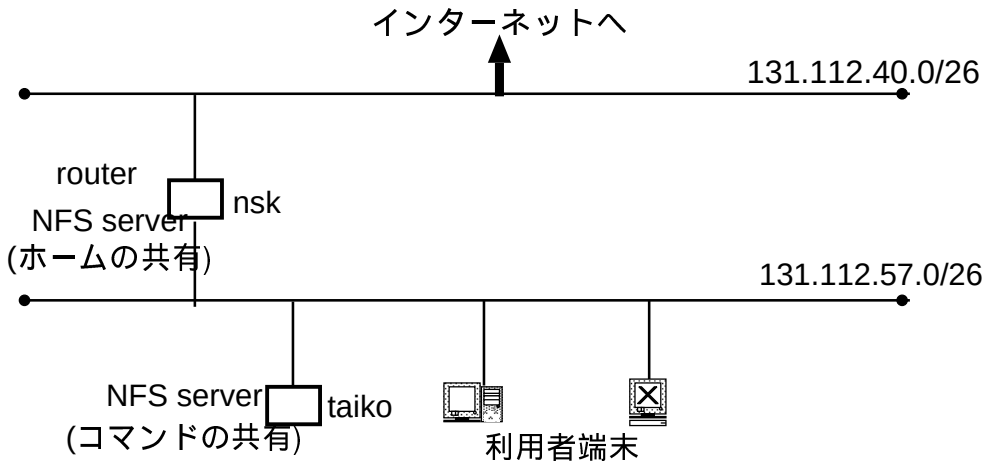

図 5.3: 移行前の状態

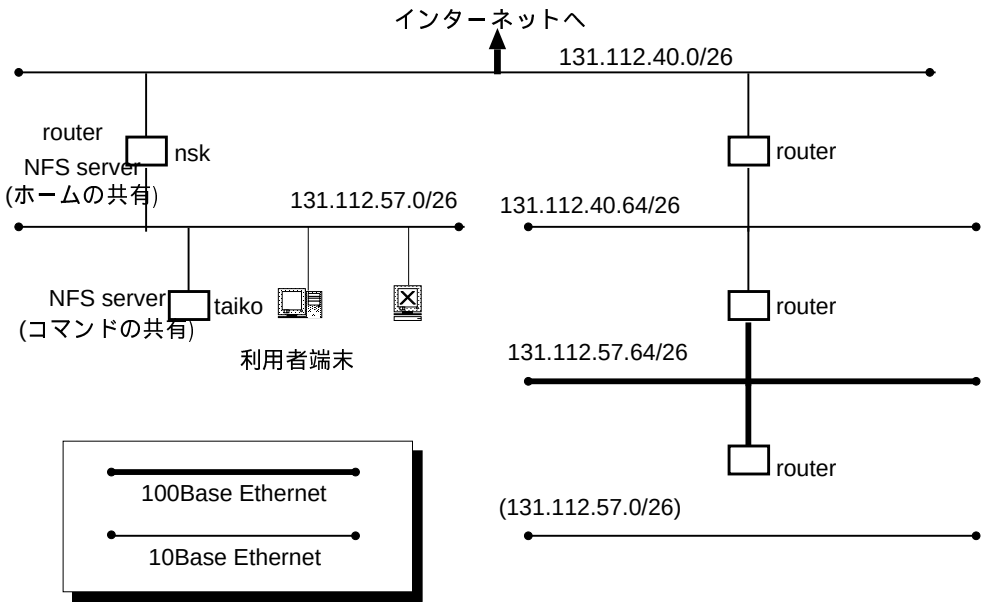

図 5.4: 移行中の状態

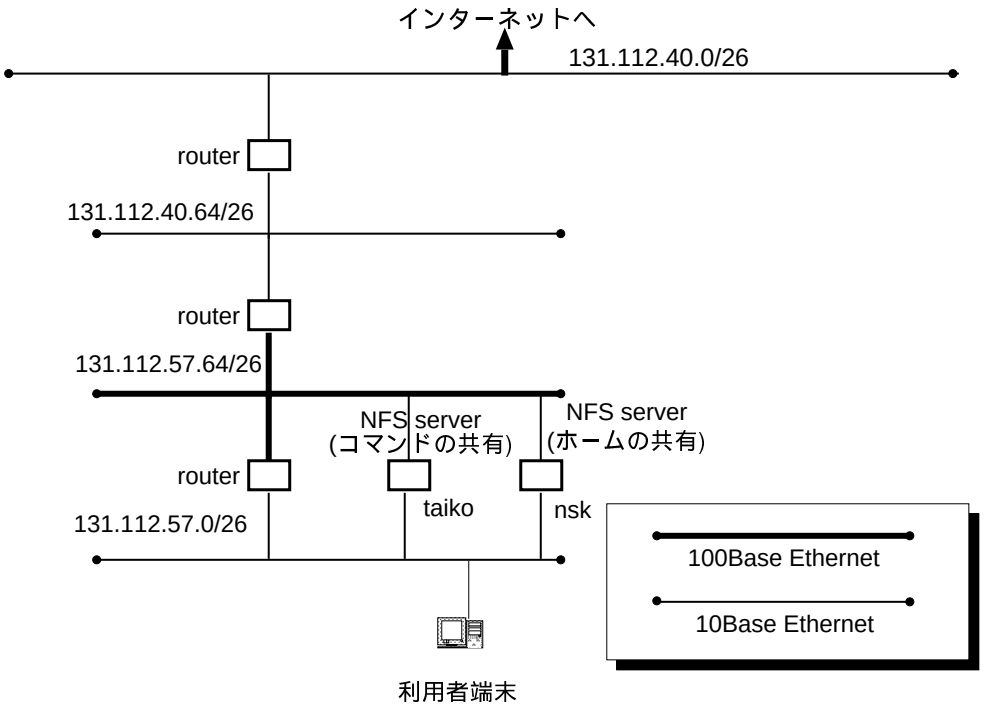

図 5.5: 移行後の状態

端末を採用している。これは当時ハードディスクの台数に十分な余裕がなかったことに起因する。

ハードディスクは、規格の違いから主に 2 種類に分類される。一つは、IDE ハードディスクと呼ばれる低速だが価格は安いハードディスクである。もう一つは、SCSI ハードディスクと呼ばれる高速だが高価なハードディスクである。

主要なサーバ計算機を PICKLES 端末化するにあたり、性能と価格 [2] からどちらのハードディスクを使用するか検討した。

その結果、価格を重視して IDE ハードディスクを採用するが、ディスクへの頻繁な入出力が予想されるメールの保存領域や WWW のコンテンツを記録する領域だけ、高速な SCSI ハードディスクを追加してその領域を割り当てた。

5.3.3 ohnolab-cfp

ohnolab-cfp とは、計算機による支援で論文募集情報や講演参加者募集の情報を集約する機構 [48] である。1997 年 4 月から研究室内で運用され、構成員の情報共有手段として利用されている。計算機による支援により、ohnolab-cfp 担当者は少ない負担でこの機構を運用できる。

5.3.4 NIS

各計算機のパスワードなどの設定を共有する手段として NIS がある。NIS では、全ての設定の基となる情報を管理する NIS サーバを運用し、各計算機は NIS サーバから情報を取得する。研究室内ネットワークでは、非 PICKLES 端末のパスワードファイルの管理にだけ NIS を利用する。PICKLES 端末では NIS を利用しない。PICKLES 端末のパスワード管理は、パスワード配布スクリプトによって行う。パスワード配布スクリプトは、ある一箇所の計算機から各 PICKLES 端末にパスワードを配布するプログラムである。

5.3.5 スクリーニング

1997 年 7 月から screend を用いてスクリーニングを開始した。screend はパケットフィルタリングを行うプログラムであり、IP パケットの送信元や送信先、パケットの種類、パケットの送信先や送信元のポート番号によりパケットの転送を制限できる。また、転送を制限したパケットや通過したパケットの記録をとれる。

スクリーニングの設定は、適切に設定した後でも、ネットワーク構成の変化や外的な状況変化に対応して、適時変更する必要がある。またスクリーニングの設定は、一つの誤設定が、セキュリティホールの出現など重大な問題を引き起こす可能性がある。そのため、スクリーニング変更のガイドラインを定め、スクリーニングの設定変更が適切に行われるようにした。このガイドラインは、「通常時」と「緊急時」におけるスクリーニングの設定変更の手順を規定している。緊急時とは、現在自組織ネットワークが不正に侵入されており緊急に管理者が対処しなければならない状態を示す。通常時とは、緊急時に該当しない状態のときである。

通常時のスクリーニング設定変更の手順

1. 管理者メーリングリストなどを利用して、二人以上の管理者から合意をとる
2. 合意後、一時間の猶予期間を設ける
3. 新しい設定をテスト後、ログを管理者メーリングリスト通知する

緊急時のスクリーニング設定変更の手順

1. ページャなどを利用して、大野研管理者に通知する
2. 新しい設定を行う。
3. 不都合が指摘されたらそれを解決する

実際の運用では、スクリーニングの設定変更を行う管理者は変更する旨を管理者メーリングリストに流し、異義がなければスクリーニングの設定変更を行い結果を管理者メーリングリストに報告する方法が多く用いられた。

管理者がスクリーニングの設定や変更作業に習熟してきたため、猶予期間が負担となり、猶予期間である一時間が省かれると考えられる。このガイドラインは、スクリーニング開

始時に取り決めたものであり、運用の経験から猶予期間などの変更を議論する時期にきている。

5.3.6 ドメイン名の取得

大野研究室では、ドメイン名 (ohnolab.org) を 1997 年 12 月に InterNIC[14] から取得した。取得作業は、WWW と電子メールを利用して行った。手順は下記の通りである。

1. 所定の書式に従い、WWW 利用してドメイン名の登録申請をする
2. 確認のため InterNIC から来るメールへ返答する
3. 所定の金額を振込む

ohnolab.org のドメイン名を取得し利用できるまでには、1ヵ月程度の時間がかかった。1ヶ月もの時間を必要とした理由は、当初 primary ネームサーバの IP アドレスを誤申請したため、ドメイン名を一旦登録後、再度 primary ネームサーバの変更を行ったためである。このような誤申請がない限り、通常 1 週間から 2 週間程度で登録は完了すると推測される。InterNIC が管理するドメイン名を取得し維持するのに必要なコストは下記の通りである。

- 金銭的コスト
  - 1998 年 3 月以前の登録分
  - 初期登録費用 $100/2 年
  - 維持費用 $50/年
  - 1998 年 4 月以降の登録分
  - 初期登録費用 $70/2 年
  - 維持費用 $35/年
- 人的コスト
  primary nameserver 及び secondary nameserver の維持管理

ohnolab.org ドメイン名は 1997 年 12 月に登録したため、その 2 年後の 1999 年 12 月の一ヶ月前に$50 の維持費用が InterNIC から請求される。

5.3.7 研究室内メーリングリスト名の整備

メールアドレスには、利用者個人が利用する個人用メールアドレスと、複数の個人用メールアドレスにメールを配送するメーリングリスト用メールアドレスがある。研究室内ネットワークではメールサーバを運用しているため、任意のメールアドレスを設定できる。個人用メールアドレスは、利用者個人に一人一つ割り当てる。メーリングリストアドレスは、必要に応じて管理者が適時設定する。

メーリングリスト名が無計画に増加すると、将来新しい利用者が加入したときその利用者に与えるメールアドレスと衝突する可能性がある。このようなメールアドレスの名前空間の衝突を回避するめ、メールアドレスを次の 2 つのドメイン名に分類し、メーリングリスト開設のガイドラインを作成した。

ohnolab.org

- ueda@ohnolab.org など、構成員一人一人に割り当てるメールアドレス。
- wide-kids@ohnolab.org など、研究室内で「プロジェクト」として認定された研究のメールアドレス。

trad.ohnolab.org

- プロジェクトに認定されていない研究や個人が開設するために、一時的に付与するメールアドレス。「trad」は、英単語「traditional」を語源とする。

ohnolab.org ドメインを付与されたメールアドレスは、メールアドレスの再利用をしない。例えば、研究室内ネットワークが存在する限り ueda@ohnolab.org 宛てのメールは、このメールアドレスの所有者である上田に配送される。しかし、trad.ohnolab.org ドメインを付与されたメールアドレスは、メールアドレスの再利用をする。このドメインを付与されたメールアドレスは、将来別の所有者が管理する可能性がある。

5.3.8 第 2 回棚卸し

第 1 回目の棚卸し作業と同様に、原則構成員全員参加で第 2 回目の棚卸し作業を行った。行った時期は、97 年度末である。

- 調査物品総数 ... 2662 個
- 行方不明物品数 ...979 個

研究室内で管理している物品総数は 2662 個で、行方不明物品数は 979 であった。物品紛失割合は、全物品数の 36.8%程度である。第一回棚卸し作業の紛失物品割合 2.5%に比べて、第二回棚卸し作業の紛失物品割合が 36.8%と極めて大きいのは幾つかの理由が考えられる。

行方不明物品の捜索不足
: 第二回棚卸しでは、第一回棚卸しに比べて行方不明物品の捜索が不十分であった。そのため、実際は存在しているにも関わらず調査が行われずに行方不明物品として扱われた物品も多数あったと思われる。

未作業領域の存在
: 棚卸し作業が全く行われなかった領域や十分行われなかった領域が存在したため、未調査領域に多量の物品が存在していると思われる。

総物品数の増大による作業量の増大

棚卸し作業を行った人数は第 1 回棚卸し作業と第 2 回棚卸し作業とも、15 人前後である。作業人数はほぼ変化がないが総物品数は、462 個増加している。作業員一人辺りが調査しなければならない物品数は増加しており、作業員の負担が高まっている。このため、誤調査や物品の調査し忘れなどがあったと思われる。作業人数はほぼ変化がないが総物品数は、462 個増加している。各作業員にかかる負担は増加しており、誤調査や物品の調査し忘れなどがあったと思われる。

行方不明物品が把握できるなど、2 年間の運用から物品管理システムの有効性が明らかになりつつある。しかし、同時に増え続ける物品に対する作業員の負担増や、物品の現在位置と物品データベースに登録された物品の位置の不一致など、幾つかの問題点も明かになりつつある。これらの問題を解決する新しい物品管理システムとして、大野研究室の野田らは IPv6 の特徴を活用した研究資材管理システム [49] を提案している。

5.3.9 管理者権限のガイドライン

1997 年度 4 月 30 日に、研究室内ネットワークの管理者になるためのガイドラインを制定した。このガイドラインでは、ある一定の条件 (表 5.3.9) を満たした利用者は、表の手順 (表 5.3) を踏めば管理者権限を取得し管理者になれる。

- 管理者になれる知識がある、M1 以上または大野研が認めた 4 年生
- ルート権限が欲しいと申し出ること
- 以下のことを守ると誓うこと
  - 大野研ネットワークの管理に積極的に参加する
  - 障害が発生したら、すぐに復旧活動を行う
  - 故意に悪いことをしない
  - 他人の個人情報を覗かない
  - ユーザからの苦情に快く対応する
  - 自分のしたことに責任をもつ
  - 期せずして知ってしまった個人情報は決して口外しない
  - 無断でサービスを停止しない

表 5.2: 管理者権限取得の条件

1998 年度 5 月には、4 名の利用者がこのガイドラインに沿った手続きを行い、管理者権限を取得した。管理者権限の取得条件・手順が明文化されたため、管理者権限の無放図な

1. 大野研ルート権限を持っている人から、推薦者になってくれる人を探す
2. 大野研ミーティングで、推薦者が申請者にルート権限を与える承認を求める
3. 大野研ミーティングで承認
4. 推薦者の推薦書、申請者の誓約書を、電子署名して暗号化したメールで大野先生に送る
5. 大野先生の承認

表 5.3: 管理者権限取得の手順

拡散の防止に有効だった。ネットワークの運用を通して、管理者権限の取得とは別に管理者権限の剥奪の問題が明らかになった。管理者権限を持つ構成員が例えば卒業などでその組織の構成員からはずれた場合、管理者権限を停止する。しかし以前としてその組織の構成員である場合でも、管理者権限を剥奪するときがある。例えば、管理者権限を取得する際誓約した条件に違反した場合、管理者権限の剥奪を考慮するべきである。事実、誓約条件に違反したとして、管理者間の協議の上、1998 年の春に 1 名の管理者の管理者権限を停止した。統一した方針の元に管理者権限の剥奪をおこなうため、今後管理者権限剥奪のガイドラインを作成する必要がある。

5.4 ネットワーク運用整備期

1998 年 4 月から 1999 年 3 月までの期間は、「ネットワーク運用整備期」である。ネットワークの運用から明らかになった問題に対処するとともに、ネットワークを運営する上で有効な各種の取り決めがガイドラインとして作成された期間である。1999 年 1 月は、この期間中である。1999 年 1 月の時点でのネットワークの全体構成図を図 5.6 に示す。

外部ネットワークと通信する計算機を配置したバリアセグメントと 2 本の利用者サブネットから構成される。これらのネットワークはそれぞれ名前が付けられており、バリアセグメントは「動物ネットワーク」、100Base Ethernet の利用者ネットワークは「スターネットワーク」、10Base Ethernet の利用者ネットワークは「楽器ネットワーク」と命名されている。それぞれのネットワークに接続される計算機は、基本的にそれぞれのネットワーク名に因んだ名前が設定されている。これらの計算機名は、インターネット上の計算機名の名前付けの指針を示した RFC1178[12] を満たす。各ネットワークは、RIP[20] で動的に経路情報を交換する。サーバ計算機およびルータ計算機は、鍵のかかる部屋に設置した棚に収容されている (図 5.7)。

構成機器

主要なルータ計算機やサーバ計算機の役割と性能を記す。

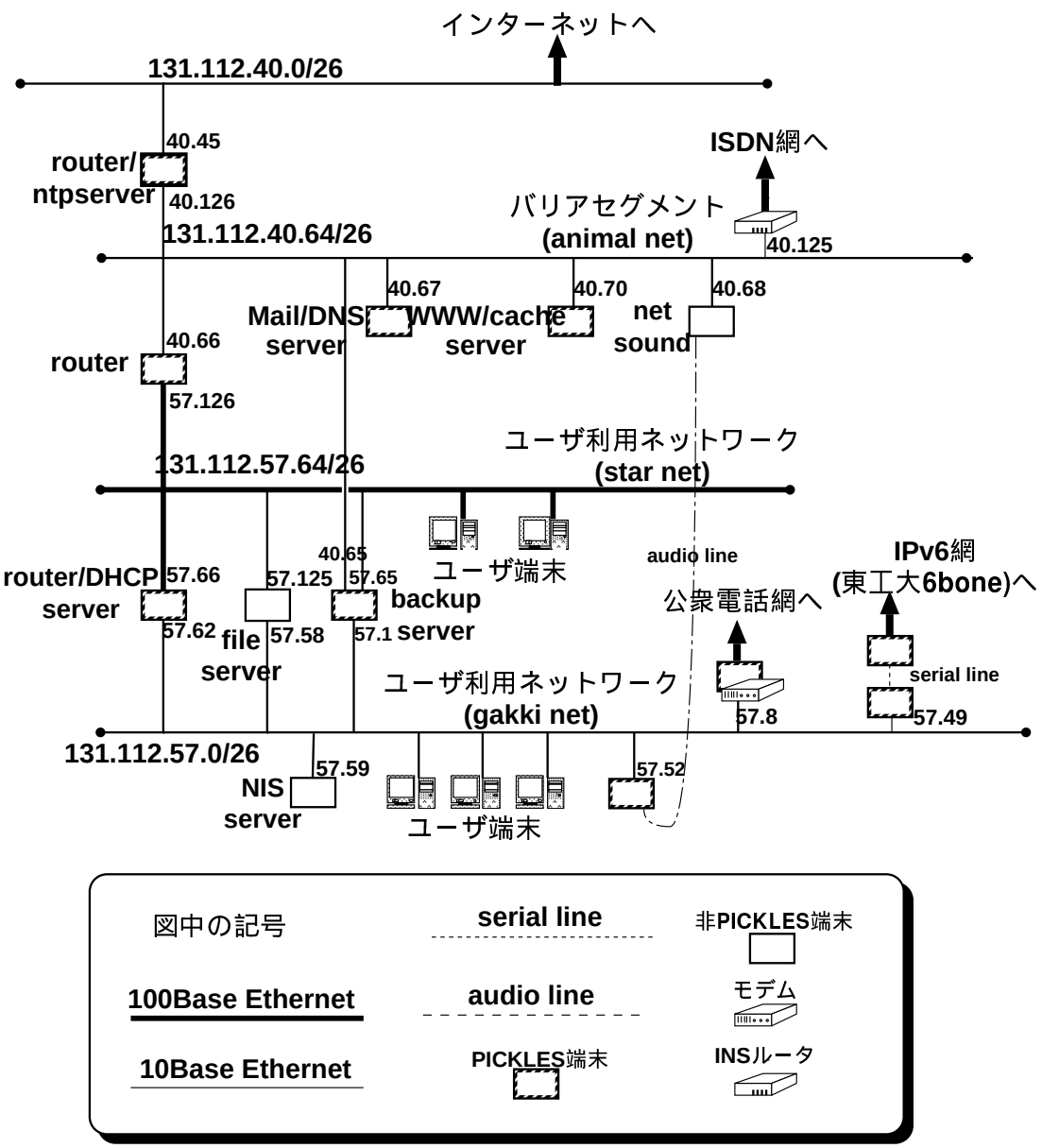

図 5.6: ネットワーク構成

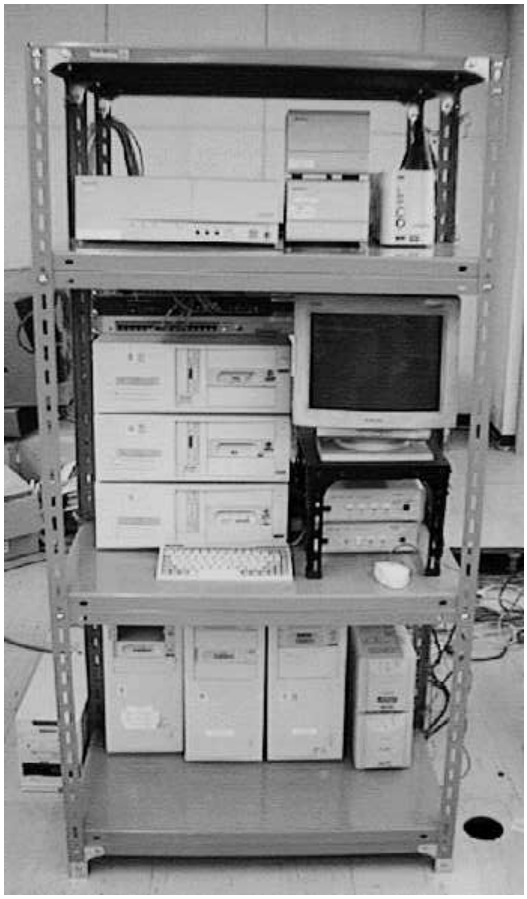

図 5.7: ルータ及び各種サーバ計算機の写真

ホスト名	役割	CPU	メモリ	HDD
wide	router	Pentium 133MHz	32Mbyte	IDE 1.2GByte
falcon	router	Pentium 133MHz	32Mbyte	IDE 1.2GByte
orion	router DHCP server	Pentium 133MHz	16Mbyte	IDE 1.2GByte
goat	Mail server DNS server	Pentium 200MHz	64Mbyte	IDE 1.6GByte SCSI 1.0GByte
tanuki	WWW server chache server	Pentium 100MHz	64Mbyte	IDE 1.0GByte SCSI 1.0GByte

構成機器の価格

主要なサーバやルータ計算機の構築に費した費用を記す。同一の物品でも値段が異なるのは、購入年度による価格の相違や、消費税率の違いによる。物品管理を行う以前に購入した物品なため記録が残っていない物品や、他の PC から部品を流用しているため正確な金額がわからない物品に関する金額は不明として扱った。

ホスト名	構成部品	物品番号	購入年月	購入金額
wide	PC 一式	960679	97 年 2 月	139,800 円
	NIC	960591	97 年 2 月	12,600 円
	NIC	960472	96 年 12 月	12,978 円
合計				165,378 円

ホスト名	構成部品	物品番号	購入年月	購入金額
falcon	PC 一式	960661	97 年 2 月	139,800 円
	NIC	960591	97 年 2 月	12,600 円
	NIC	960472	96 年 12 月	12,978 円
合計				165,378 円

ホスト名	構成部品	物品番号	購入年月	購入金額
orion	M/B	960503	97 年 1 月	不明
	メモリ	550218	不明	不明
	メモリ	550219	不明	不明
	CPU(P133MHz)	960508	97 年 1 月	不明
	CPU ファン	960203	96 年 9 月	6180 円
	電源分岐ケーブル	960204	96 年 9 月	CPU ファンに含む
	FDD	550217	不明	不明
	FDD フラットケーブル	55D049	不明	不明
	VGA カード	970124-8	97 年 2 月	不明
	IDE-HDD	970175	97 年 10 月	20,450 円
	IDE フラットケーブル	95B009	不明	不明
	シリアルケーブル	960504	97 年 1 月	不明
	パラレルケーブル	960505	97 年 1 月	不明
	IDE removable case(内)	960193	96 年 9 月	4,223 円
	IDE removable case(外)	550091	96 年 9 月	(4,223 円)
	NIC	960555	97 年 1 月	14,214 円
	NIC	960707	97 年 2 月	15,398 円
合計				不明

ホスト名	構成部品	物品番号	購入年月	購入金額
tanuki	M/B	550282	不明	不明
	本体ケース	550281	不明	不明
	CPU ファン	550283	不明	不明
	VGA カード	550284	不明	不明
	SCSI フラットケーブル	550285	不明	不明
	シリアル (9pin) ケーブル	550286	不明	不明
	シリアル (25pin) ケーブル	550287	不明	不明
	パラレルケーブル	550288	不明	不明
	IDE フラットケーブル	550301	不明	不明
	メモリ (32MByte)	970128	97 年 8 月	13,440 円
	メモリ (32MByte)	970125	97 年 8 月	13,440 円
合計				不明

ホスト名	構成部品	物品番号	購入年月	購入金額
goat.ohnolab.org	IDE-HDD	960086	96 年 7 月	46,144
	SCSI-HDD	不明	不明	不明
	VGA カード	960302	96 年 11 月	不明
	CPU	960381	96 年 12 月	不明
	CPU ファン	960382	96 年 12 月	不明
	M/B	960383	96 年 12 月	不明
	SCSI I/F	960548	97 年 1 月	30,694
	NIC	960189	96 年 9 月	4,738
合計				不明

ハブ種類	利用ネットワーク	物品番号	購入年月	購入金額
10Base Hub	131.112.40.64/26	550215	不明	(22,866 円)
100Base Switching Hub	131.112.57.64/26	970326	98 年 2 月	187,000 円
10Base Hub	131.112.57. 0/26	95H060	96 年 2 月	22,866 円
合計				232,732 円

物品名	物品番号	購入年月	購入金額
CPU 切り替え機	970086	97 年 5 月	48,300 円
CPU 切り替え機	960360	96 年 11 月	40,685 円
UPS	980156	98 年 12 月	(67,557 円)
UPS	970088	97 年 5 月	67,557 円
ディスプレイ	90K001	不明	不明
合計			不明

5.4.1 電力構成

計算機などのネットワーク構成機器と、電子レンジや蛍光灯などの家庭用機器は、別の電源系統から電力をとるように配置した。これにより、電子レンジやストーブの使用によって電力の遮断した場合でも、ネットワーク構成機器に影響が及ばない。ルータ計算機やサーバ計算機には、無停電装置を設置し停電対策を行った。

5.4.2 ベンチマークガイドライン作成

計算機の性能を評価・比較するための手段としてベンチマークテストがある。ベンチマークテストは、結果を他の計算機のベンチマークテストの結果と比較できればより有効である。そのため、ベンチマークソフトやベンチマークの結果が系統立てて保存されている必要がある。ベンチマークテストに関するガイドラインをもうけ、各計算機のベンチマークの結果の登録を推奨している。1999 年 1 月 11 日現在 2 個の登録しかないが、今後増えることが期待される。

5.4.3 ssh の導入

研究室内ネットワークでは、1997 年 7 月から screend を用いてスクリーニングを行っている。スクリーニングによって通信制限されたパケットの記録をみると、実際にスクリーニングが機能している様子がわかる。例えば、1998 年 12 月 31 日の screend のログ (図 5.8) を見ると、ファイアーウォールの内側に位置する複数のホストに対して、同一ホスト (195.122.172.139) から、短時間の内に TCP の port 番号 23 に対して執拗な通信がある。これは、telnet プログラム (port 番号 23) に対して通信をし、ログイン可能な計算機を探していたと考えられる。

研究室内ネットワークでは、1998 年 7 月まで外部ネットワークから内部ネットワークに通信する手段として S/KEY を利用していた。また、研究室内メールサーバと通信しメールを取得する手段として、APOP を提供している。しかし、運用を通して幾つかの問題点が明かになった。

ISP からのログイン

利用者が ISP から研究室ネットワークへ接続するとき、多くの場合は ISP が割り当てられた IP アドレスをもつ計算機から行う。計算機に割り当てられる IP アドレスは事前に正確に予想はできない。そのため、予想される範囲の IP アドレス全てに対して、スクリーニングを解除する必要がある。これは、研究室内ネットワークの利用者が加入する ISP に対しては、スクリーニングが緩くなる原因になった。

通信制限の一時的な緩和

学会やワークショップなどの現地でネットワーク接続性が提供されることも多くなった。S/KEY では、その度ごとに現地の IP アドレスのスクリーニングを解除しなければならない。この作業は管理者の負担になるとともに、期間終了後のスクリーニング解除設定の削除し忘れなどから、スクリーニングの設定が現状とあわない原因となった。これはセキュリティ上問題があった。

ログインポートの扱い

S/KEY を導入し利用者認証を行っているとはいえ、世界中の全ての計算機に対してログインポート (tcp 23 番) を開けるのはセキュリティ上問題があった。

これらの問題点を解決するため、1998 年 9 月から内部ネットワークに接続する手段として S/KEY の変わりに ssh[3] を提供した。これにより、学会やワークショップが開催される度にスクリーニングの設定を変更する必要がなくなった。管理者の負担が減少するとともに、誤設定の可能性が減った。

ssh の導入により、安全性はより高まったが、利用者の利用の仕方によっては、ssh が必ずしも期待された効果を発揮しない場合がある。実際に研究室内ネットワークを運用する上で生じた例だが、利用者が自宅から電話網経由で内部ネットワークにログインしたが、その途中一部のネットワークにログインのための生パスワードを流してしまった例があった (図 5.9)。ネットワーク上を生パスワードが流れると、不正侵入者がネットワークを監視していた場合、パスワードを不正に取得される恐れがある。

道具がいくら安全でもそれを利用する人の使い方次第では、危険が生じる例である。そのため、ssh の仕組みを説明するなど利用者への教育が重要である。

5.4.4 構成人数

構成員と管理者の人数推移を年度別に表 5.4 に記す。

```
Dec 31 15:49:21 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.87](17514->23)02
Dec 31 15:49:27 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.107](2118->23)02
Dec 31 15:49:32 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.79](13350->23)02
Dec 31 15:49:35 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.82](19686->23)02
Dec 31 15:49:51 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.101](21611->23)02
Dec 31 15:49:54 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.105](28789->23)02
Dec 31 15:50:02 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.66](15843->23)02
Dec 31 15:50:27 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.90](13479->23)02
Dec 31 15:50:40 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.74](12354->23)02
Dec 31 15:50:45 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.113](22023->23)02
Dec 31 15:51:17 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.75](25574->23)02
Dec 31 15:52:04 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.80](25226->23)02
Dec 31 15:52:08 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.117](3691->23)02
Dec 31 15:52:44 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.71](10598->23)02
Dec 31 15:53:21 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.89](22061->23)02
Dec 31 15:53:50 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.67](23011->23)02
Dec 31 15:54:03 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.118](22628->23)02
Dec 31 15:54:13 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.102](12370->23)02
Dec 31 15:54:18 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.86](23341->23)02
Dec 31 15:54:54 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.70](6497->23)02
Dec 31 15:55:08 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.77](2188->23)02
Dec 31 15:55:36 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.73](31349->23)02
Dec 31 15:56:07 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.110](9929->23)02
Dec 31 15:56:33 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.116](6312->23)02
Dec 31 15:56:49 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.95](6541->23)02
Dec 31 15:58:11 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.115](1914->23)02
Dec 31 15:58:34 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.72](20538->23)02
Dec 31 15:59:45 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.122](21557->23)02
Dec 31 15:59:53 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.98](10806->23)02
Dec 31 16:00:01 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.109](29771->23)02
Dec 31 16:00:06 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.96](10767->23)02
Dec 31 16:00:21 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.108](15480->23)02
Dec 31 16:00:42 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.94](29410->23)02
Dec 31 16:00:54 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.120](25924->23)02
Dec 31 16:01:06 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.99](19288->23)02
Dec 31 16:01:22 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.106](20572->23)02
Dec 31 16:02:09 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.91](4651->23)02
Dec 31 16:02:33 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.104](29854->23)02
Dec 31 16:03:06 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.100](11626->23)02
Dec 31 16:03:26 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.83](22255->23)02
Dec 31 16:03:34 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.68](8976->23)02
Dec 31 16:03:44 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.93](31920->23)02
Dec 31 16:04:17 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.76](9808->23)02
Dec 31 16:04:54 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.123](4221->23)02
Dec 31 16:05:22 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.78](32494->23)02
Dec 31 16:05:39 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.124](4647->23)02
Dec 31 16:06:14 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.69](16515->23)02
Dec 31 16:06:33 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.85](22098->23)02
Dec 31 16:06:48 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.97](20598->23)02
Dec 31 16:07:27 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.112](9507->23)02
Dec 31 16:07:46 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.65](16817->23)02
Dec 31 16:08:08 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.111](27636->23)02
Dec 31 16:08:38 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.103](24775->23)02
Dec 31 16:10:25 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.92](17545->23)02
Dec 31 16:10:38 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.121](13368->23)02
Dec 31 16:10:43 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.88](22599->23)02
Dec 31 16:11:11 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.114](21810->23)02
Dec 31 16:11:25 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.84](20686->23)02
Dec 31 16:12:04 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.119](14042->23)02
Dec 31 16:12:17 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.57.45](80->1159)04
Dec 31 16:12:17 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.57.45](80->1160)04
Dec 31 16:12:17 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.57.45](80->1162)04
Dec 31 16:12:17 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.57.45](80->1161)04
Dec 31 16:12:48 wide screend[1022]: REJECT: TCP [195.122.172.139]->[131.112.40.125](16922->23)02
```

図 5.8: スクリーニングのログ

年度	構成員人数 (人)	管理者数 (人)
1996 年度	16	8
1997 年度	17	7
1998 年度	17	10

表 5.4: 構成員人数の推移

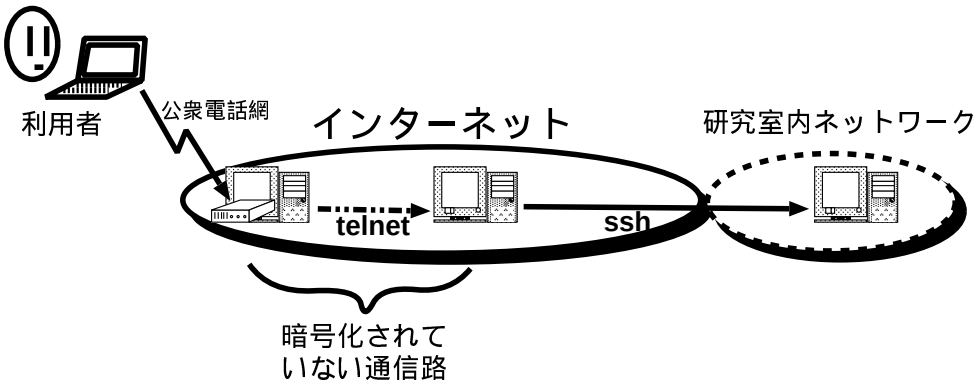

図 5.9: 安全ではない通信

5.4.5 ログの記録

障害に備えて通信記録や利用者のアクセス記録やシステムの動作記録を残すことは、2つの点で重要である。

- 障害からの迅速な復旧
- 障害原因の特定

5.4.6 Reborn System

ネットワーク構成機器の故障等にそなえる障害管理はネットワーク管理の中でも重要である。研究室内ネットワークにおいても、主にハードディスクの故障に伴う障害が発生している。下記にその障害の事例を示す。

1998/09/04 netsound の故障

1998/02/04 ルータ (wide.ohnolab.org) の故障

1998/08/12 WWW サーバ (tanuki.ohnolab.org) の故障

これらの障害に対応するため、PICKLES 上で動作する障害管理システムとして Reborn System を開発 [42] し、1998 年 7 月から大野研究室ネットワーク上で運用している。Reborn System は、PICKLES 端末同士の相互互換性を生かして、運用中の PICKLES 端末同士で互いの計算機の冗長性を確保するシステムである。WWW サーバの故障時に実際に利用し、その有効性を確認した。

Reborn System の設計

Reborn System では、障害が発生したとき、障害が発生したと推測される計算機 A を、正常に動作している別の計算機 B と置き換える。計算機 A が正常に動作していたときの機

能を計算機 B が行うあいだ、管理者は計算機 A を調べ故障の原因を調査する。計算機 A が障害から回復したとき、計算機 A と計算機 B をそれぞれ本来の機能へ戻す。計算機 A の障害が致命的であり回復できないとき、新たな計算機 C を用意し計算機 B の機能を担当させることもできる。この方法の利点は、経験と技術を必要とする障害の特定・回復作業が最小限で済むことである。そのため管理者の負担は減る。経験の少ない管理者でも、障害が発生した計算機の機能を維持できる。

管理者があるコマンドを実行すると、Reborn System を備えた計算機は障害を起こした計算機の機能を代行する (図 5.10)。このコマンドを reborn command と名づける。他の計算機の機能を代行するためには、代行する機能をあらかじめ全て保持していなければならない。他の計算機の機能を代行するとき、Reborn System を備えた計算機が代行する機能を、管理者が選択する。障害回復にかかる時間は、管理者が reborn command を実行する時間と計算機が再起動する時間だけである。そのため、障害時には障害を起こした計算機の代用が迅速にできる。

複数の計算機で障害が発生した場合、優先度や重要度に従って管理者が複数の計算機で reborn command を実行する。たとえば、筆者らの研究室ネットワークで外部と接続するルータと Mail サーバが故障した場合、バックアップサーバと WWW サーバがそれぞれ故障した計算機の機能を代行する。この場合、WWW サービスとバックアップ作業は一時停止するが、インターネットへの接続性とメールの送受信のサービスは確保できる。

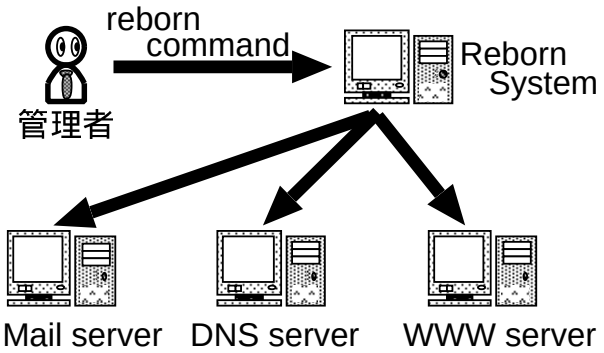

図 5.10: 障害を起こした計算機の機能を代行

Reborn System の実装と運用

Reborn System を研究室内ネットワーク上で実装した。PICKLES 端末を元に幾つかの変更を行った計算機を相互交換可能な端末として用いた。今回実装した相互交換可能な端末は、IDE ハードディスクインターフェイスをそなえており、IDE ハードディスク一台で起動する。

Reborn System を備えた計算機は 6 つの機能を代行できる。列挙すると、WWW、DNS、firewall、router、Mail、bench の各機能である。これらの機能は同時に複数選べる。

- WWW
  WWW サーバとキャッシュサーバを起動する。
- DNS
  DNS サーバを起動する。
- firewall
  スクリーニングを行う。
- router
  経路制御を行う。セキュリティ上の理由から、DNS を利用しない。
- Mail
  Mail の送受信を行う。
- bench
  バックアップ作業を行う。筆者らはバックアップ間隔 h を 24 時間に設定した。

Reborn System の考察

1998 年 7 月から Reborn System を研究室内ネットワークで運用している。Reborn System を運用中 WWW サーバに障害が発生したときの障害回復事例を報告し、考察を述べる。

1998 年 8 月 10 日、WWW で外部に公開する情報にアクセスできない障害が発生した。その場に居あわせた管理者は、WWW サーバに接続されているディスプレイを見てハードディスクの故障が原因だと判断した。そのため、バックアップ作業用の計算機のハードディスクを故障したハードディスクと入れ換え、reborn command を実行した (図 5.11)。reborn command を実行した計算機は WWW の機能を代行した。必要とした時間は約 1 時半間程度であった。このように Reborn System を用いると、経験の少ない管理者でも十分にネットワーク管理ができる。

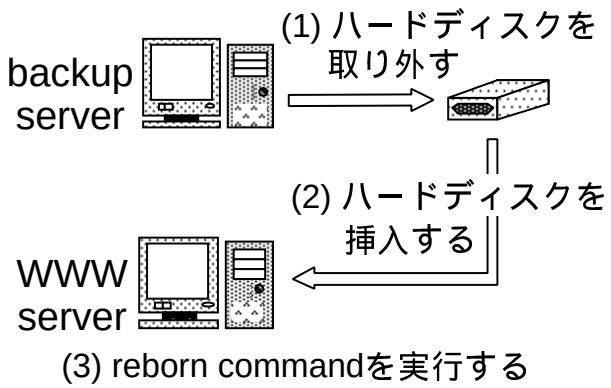

図 5.11: 運用例

第6章　評価と考察

本章では、まず研究室内ネットワークの評価を行う。次に、IPv4 から IPv6 への移行上の問題点を明らかにするとともに、利用者への IPv6 の普及を図った「IPv6 デー」と呼ぶイベントについて記述する。

6.1　研究室内ネットワークの評価

機動性を配慮した規模組織ネットワークを構築運用する上で必要な条件として、3 章では「ネットワークの高い独立性」「セキュリティの確保」「環境への適応」「安価なネットワーク」「長期間の運用を想定した態勢の整備」「管理者の負担軽減」の 6 項目を挙げた。研究室ネットワークで、この各項目が満たされているかどうかを評価する。

6.1.1　ネットワークの高い独立性

ネームサーバやメールサーバ、WWW サーバなど各種サーバを研究室内ネットワークで独自に運用することで、ネットワークの独立性をある程度高められた。しかし、ネームサーバに関しては完全には独立性を保てない部分があった。

DNS

ネームサーバは、IP アドレスから計算機名の変換を行う「正引き」サービスと、計算機名から IP アドレスの変換を行う「逆引き」サービスを行う。

ns.ohnolab.org 上で運用するネームサーバ は、ohnolab.org ゾーンを管理するプライマリネームサーバである。このネームサーバは、org ドメインを管理する InterNIC に登録された権威あるネームサーバである。このため、DNS により名前解決を行う計算機は、ohnolab.org ドメインに属する計算機名の IP アドレスを引く正引きをおこなうと、最終的に、ns.ohnolab.org 上で運用するネームサーバに問い合わせを行う。ohnolab.org ドメインに関する正引きは ns.ohnolab.org 上のネームサーバにより解決できる。

ohnolab.org ドメインに属する計算機名の IP アドレスから計算機名を引く正引きをおこなうと、in-addr.arpa ドメイン内の探索を行い、最終的に研究室内ネットワークが属する上位のネットワークのネームサーバに問い合わせを行う。このため、逆引きは、ns.ohnolab.org のネームサーバにより解決できない。研究室内ネットワークが利用するネットワークアドレスの逆引きを他のネームサーバから委任してもらう方法として、研究室内ネットワーク

が利用する計算機の全ての逆引きを委任してもらう方法 [15] が一般に用いられる。しかし、この方法では委任を行うネームサーバに、委任を行う計算機に比例する量の設定を行う必要であり、委任を行うネームサーバの運用方針によっては必ずしもこの委任を行えないかもしれない。現在のところ、ohnolab.org ドメインに関する逆引きは ns.ohnolab.org 上のネームサーバ以外で運用しているため、独立性を保っているとはいえない。

最後に、ohnolab.org ゾーンを管理するネームサーバの統計情報を記載する。

図 6.1 一時間ごとメモリ消費率と CPU 消費率

1998 年 12 月 20 から 1999 年 1 月 19 日までの 2616139 秒 (約 30 日強) の間に、このネームサーバには 3974852 回の問い合わせを処理している。これは、約 1.52 回/秒の割合である。InterNIC が管理するネームサーバ (ns.internic.net) は、約 71 回/秒の割合で問い合わせを処理しているため、このネームサーバと比較すると単位時間辺りの処理数は非常に少ない。ohnolab.org ドメインを取得してから 1 年余りしか経過していないため知名度が低く、名前解決の問い合わせ数自体が少ないためと思われる。文献 [7] によれば、ネームサーバは子プロセスを起動してゾーン転送を行うのに通常のメモリの 2 から 3 倍程度が必要である。図 6.1 を見る限り現在の運用態勢でも十分である。また、CPU 消費率はほぼ 0.01%であり、この計算機は十分な CPU 能力を持っている。

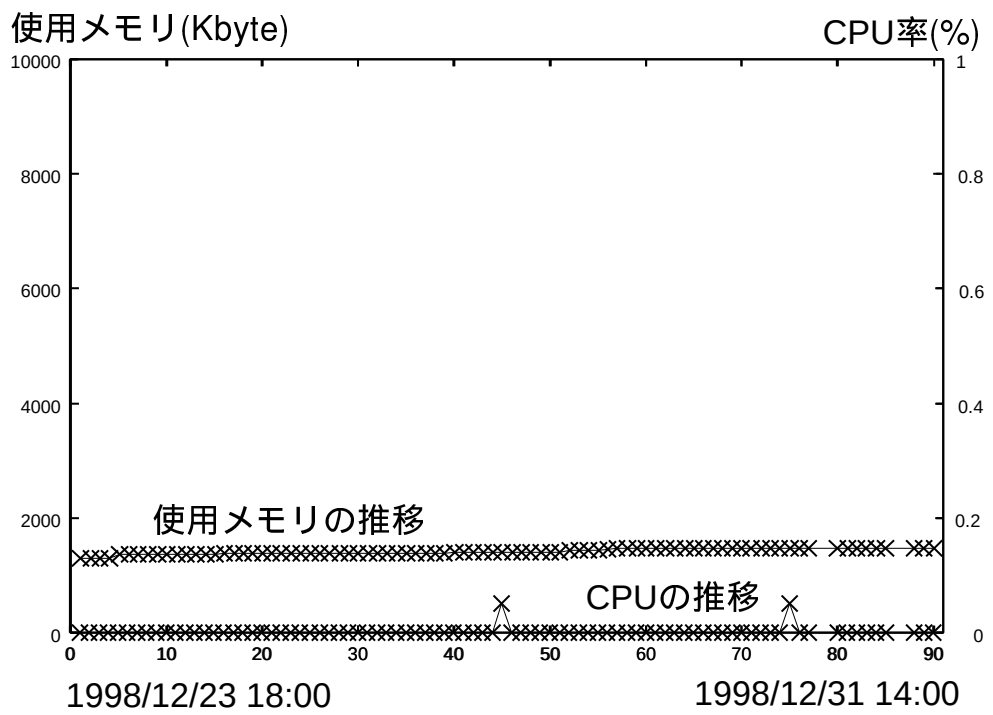

図 6.1: メモリ消費率と CPU 消費率

6.1.2 セキュリティの確保

ネットワークの防御手段として運用したファイアウォールと、計算機の防御について評価する。

日本でコンピュータネットワークに対する不正侵入を予防し対策するため、警視庁や郵政省により不正アクセス防止法案 [32][51] が制定される予定である。ロギングの義務化などが行われる可能性があるため、ネットワーク管理者として注目していく必要がある。

ファイアウォールの性能

スクリーニングを行うと、スクリーニングを行わないときに比べ、ルータとしての転送性能が低下すると予想される。そのため、複数の条件下で実験を行い、転送性能の低下に関する考察を行った。その結果、スクリーニングによるルータの転送性能の低下は無視できる程であった。

実験環境は、 図 6.2 のように 3 台の PC を 10Base Ethernet のクロスケーブルで直列に接続して構築した。中央のルータ計算機でルーティングを行い、スクリーニングを実行た。各 PC の性能は、図 6.3 の通りである。

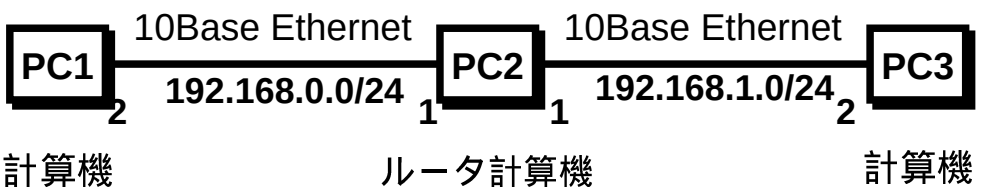

図 6.2: スクリーニングによるルータの性能低下を計測する実験環境

計算機名	CPU	メモリ	NIC
PC1	Pentium 200MHz	64Mbyte	3C905
PC2	Pentium 200MHz	32Mbyte	NE2000 互換 3C509
PC3	PentiumII 266MHz	64Mbyte	3C905

図 6.3: 実験で用いた各 PC の性能

この実験環境下で下記の実験を行った。エントリとはスクリーニングの規則の設定であり、IP アドレスやポート番号別に IP パケットを転送するか否かを記述する。エントリ数はエントリの総数である。

1. PC2 でスクリーニングを行わないときのルータ性能の測定

2. PC2 でエントリ数が 1 のスクリーニングを行うときのルータ性能の測定
3. PC2 でエントリ数が 10 のスクリーニングを行うときのルータ性能の測定
4. PC2 でエントリ数が 100 のスクリーニングを行うときのルータ性能の測定
5. PC2 でエントリ数が 1000 のスクリーニングを行うときのルータ性能の測定
6. PC2 でエントリ数が 10000 のスクリーニングを行うときのルータ性能の測定
7. PC2 でエントリ数が 100000 のスクリーニングを行うときのルータ性能の測定

PC1 から PC3 へ向けてと、PC1 から PC3 へ向けての方向で、転送性能を計測する ttcp というプログラムでルータ性能を測定した。実験の結果を表 6.1 に示す。

	PC1 → PC3		PC1 ← PC3	
スクリーニング無	5190	5175	4618	4645
	11513	10373	16298	16510
1 エントリ	5044	5020	4653	4677
	23158	22648	10837	10886
10 エントリ	5220	5201	4566	4592
	1594	1495	1098	1064
100 エントリ	5203	5183	4603	4627
	9025	9102	9351	9404
1000 エントリ	5199	5180	4609	4629
	16159	15507	5831	5937
10000 エントリ	4758	4751	4647	4663
	24410	23300	180	203
100000 エントリ	4647	3987	3934	3741
	10024	92234	11957	8189

表 6.1: 転送性能の実測値

各項目の上段の値は ttcp で計測した値の 10 回平均であり、下段の値はその分散である。表中単位は Kbits/sec である。

10000 エントリを越えるあたりからルータの転送性能にスクリーニングの影響が見られる。しかし、1999 年 1 月 31 日の時点では、研究室内ネットワークにおけるスクリーニングのエントリ数は 45 であるため、ルータの転送性能に影響はないと考えられる。主にこのエントリ数は、バリアセグメントに属する計算機に関する記述と、内部ネットワークのサブネットワーク単位での記述から構成されるため、研究室内ネットワークの計算機やネットワーク数が増えたとしても、エントリ数が急激に増大することはない。このため、ルータの転送性能の低下は無視できる。

計算機の防御

不正侵入の手口として、ポートスキャンを実行して不用意に運用されているサービスのセキュリティホールを探索する方法がある。ポートスキャンは、対象となる計算機の特定の範囲のポート番号を網羅的に調査する。DNS に登録された計算機を再帰的に自動で調査する方法が多く用いられるため、DNS に登録された計算機は全てこの攻撃を受ける可能性がある。

ポートスキャンによる不正侵入を防ぐため、計算機上で不用なサービスを運用しないことが重要である。しかし、ネットワークに熟練した管理者といえども、計算機上で運用されている全てのサービスを把握するのは困難である。そのため、研究室内ネットワークのバリアセグメントに属する計算機の 1 番から 1024 番までのポート番号を対象にポートスキャンを実際に行い、運用されているサービスを検査した。調査日は、1998 年 12 月 10 日であり、対象となった計算機は BSD/OS3.1 を基にした PICKLES 端末である。その結果を表 6.2、表 6.3、表 6.4 に示す。

計算機名 wide	ポート番号	サービス名
	1	tcpmux
	7	echo
	9	discard
	13	daytime
	19	chargen
	21	ftp
	22	ssh
	23	telnet
	37	time
	79	finger
	111	sunrpc
	113	auth
	444	snpp
	513	login
	514	shell
	515	printer

表 6.2: 運用中のサービス (wide.ohnolab.org)

この結果を受けて、スクリーニングを行っている計算機では、不要なサービスの運用を停止した。その結果を表 6.5 に記す。これによりセキュリティの頑強度が向上した。

その他の計算機は、まだ不要なサービスを運用していが、これらの計算機の設定も順次対応していく予定である。研究室内ネットワークでは、外部ネットワークと内部ネットワー

計算機名 goat	ポート番号	サービス名
	1	tcpmux
	7	echo
	9	discard
	13	daytime
	19	chargen
	21	ftp
	22	ssh
	23	telnet
	25	smtp
	37	time
	53	domain
	79	finger
	110	pop3
	111	sunrpc
	113	auth
	512	exec
	513	login
	514	shell

表 6.3: 運用中のサービス (goat.ohnolab.org)

計算機名 tanuki	ポート番号	サービス名
	1	tcpmux
	7	echo
	9	discard
	13	daytime
	19	chargen
	21	ftp
	22	ssh
	23	telnet
	25	smtp
	37	time
	79	finger
	80	http
	111	sunrpc
	113	auth
	513	login
	514	shell

表 6.4: 運用中のサービス (tanuki.ohnolab.org)

クの境界でスクリーニングをしているため、内部ネットワーク内のこれらの計算機で不要なサービスを運用していたとしても、それが直にセキュリティ上の問題にはならない。

計算機名 wide	ポート番号	サービス名
	13	daytime
	19	chargen
	21	ftp
	22	ssh
	23	telnet
	79	finger
	111	sunrpc
	113	auth
	513	login
	514	shell

表 6.5: 不要なサービスを停止した後 (wide.ohnolab.org)

6.1.3 環境への適応

無停電電源による給電で対応できない長時間の電源切断時には、ネットワークの運用を停止する。現在では、管理者が二人一組でこの作業を担当している。管理者はこの作業の度に一人ずつ入れ換わるため、作業経験者と作業未経験が常に一組みで作業にあたる。この作業は深夜や早朝に行われることが多かったため、管理者に負担となっている。

6.1.4 安価なネットワーク

安価な PC を利用したネットワーク構成であり、安価に製作しているといえる。

6.1.5 長期間の運用を想定した態勢の整備

研究室内ネットワークでは、一度構成員に付与したアカウントは再利用しない。毎年数人ずつの新規アカウントを発行しているため、アカウントの名前空間は年々狭くなっている。新規構成員が各自が希望するアカウントを取得できるか評価を文献 [36] を基に行う。

文献 [36] によれば、利用者がアドレスを希望するとき利用者自身の名前を希望することが最も多い。利用者が自分自身の名前のアドレスを希望する割合は、ネットニュースによる分析と JPNIC の WHOIS データベースエントリの分析、個人に対する地域ドメインの登録状況の分析から、約 32%と推測している。日本ソフト販売株式会社が発行する「たずね

人 CD-ROM for personal」を用いた分析では、日本人の姓で最も多いのは sato (佐藤, 佐東, 左藤左東, 佐当, 砂藤, 里) であり、全体の 1.6%を占める。このため、アドレスの重複が最も生じる可能性があるのは、sato 姓の利用者が、sato というアカウントを希望したときである。毎年 5 人の新規利用者がいるとして、研究室内ネットワークを 50 年運用したとき sato 姓の利用者のアカウントが重複するか評価する。

アカウントの期待値 = 50 年間 x 5 人 x 1.6% x 32% = 1.28

よって、研究室内ネットワークを 50 年間運用しても、sato 姓のアカウントは 1.28 個しか発行されず、重複する可能性はないと期待される。この結果から、研究室内ネットワークを 50 年間運用してもアカウントの重複は生じないと考えられる。

しかし、この調査のもとになったデータは一般の人を対象にしており、研究室内ネットワークの新規利用者の偏りを考慮していない。研究室ネットワークの新規加入者はほぼ全員がコンピュータリテラシの教育を受けたものである。また、男女比の割合も一般の人とは異なる。今後これらの事情を考慮して、文献の妥当性を今後評価する必要がある。

名前空間の問題自体、com レベルドメイン名の増大によるルートネームサーバの負荷など多様な議論 [29] があり、今後の動向に注目する必要がある。また、トップレベルドメイン名である新しい gTLD[11] の取得も考えるべきである。

6.1.6 管理者の負担軽減

スクリーニング

screend を運用し、IP とポート番号の組合せでスクリーニングを行っている。コストの面からこの妥当性を検討する。

金銭的なコスト

screend はフリーソフトウェアとして公開されている。そのため金銭的なコストはない。

管理者の負担増

構築・運用に要する管理者の負担を定量的に計るのは難しい。スクリーニングに関する管理者の負担を計るため、ここでは研究室内で運用されている管理用メーリングリストに流れたメールの中で、スクリーニングに関する議論を行ったメールの総数を月別に集計した (図 6.4)。

外部ネットワークから研究室内ネットワークの計算機資源を利用する手段を、1998 年 9 月から S/KEY から ssh に変更したため、スクリーニングに関する議論のメールが減少している。この原因は主に、学会やカンファレンスなどで一時的に運用される外部ネットワークから、内部ネットワークのメールを受信するために、スクリーニングの設定をその都度変更したことによる。ssh に変更後、このような変更作業必要がなくなったため、スクリー

ニングに関する議論は、ほとんど行う必要がなかった。現在では、スクリーニングを運用するために必要な管理者の負担は極めて少ないものであると判断できる。

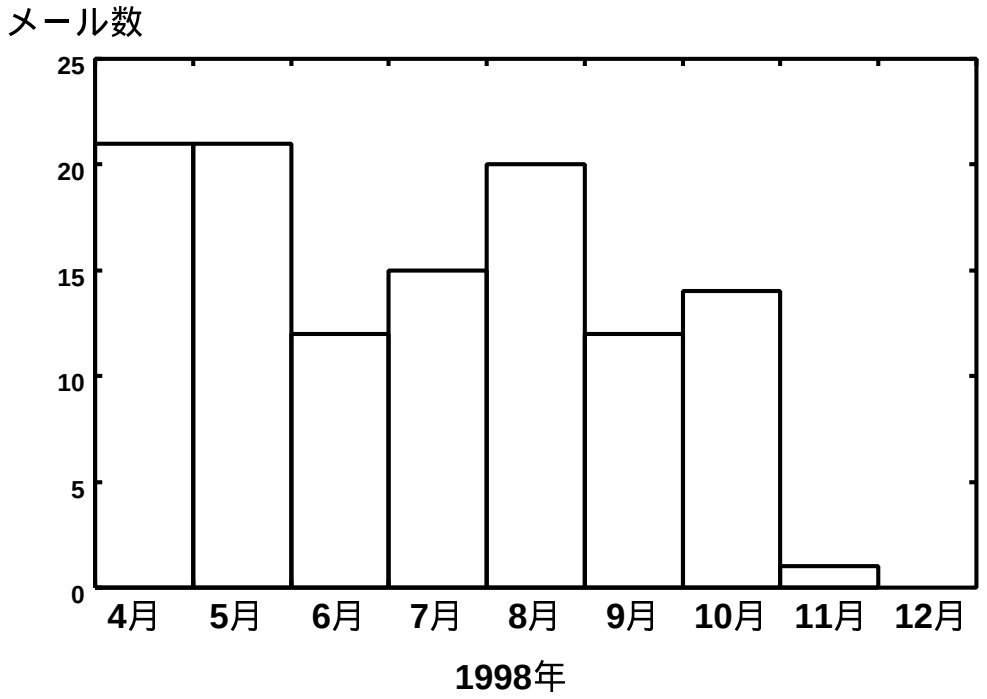

図 6.4: 月別総数

6.2 プロトコルが異なるネットワークへの移動

ネットワークの移動を考えた場合、ネットワークプロトコルが異なるネットワークへの移動を考慮する必要がある。そのため、次世代インターネットプロトコル (IPv6) を使用した IPv6 網への接続運用実験を事例とし、プロトコルが異なるネットワークへの移動上の問題点を明らかにする。

研究室内ネットワークは、東京工業大学情報理工学研究科のネットワークを通してインターネット (IPv4 網) と接続されている。これとは別に、研究室内ネットワークは、東京工業大学 6bone を通して IPv6 を利用したインターネット (IPv6 網) と接続している (図 6.5)。しかし、IPv6 網は利用者にほとんど利用されておらず、IPv6 網との接続性や運用上の問題点が明らかになっていなかった。そのため、IPv6 網への移行を視野に、IPv4 から IPv6 への移行上の問題点を明らかにするとともに、利用者への IPv6 の普及を目標とした「IPv6 デー」を、研究室で行った。

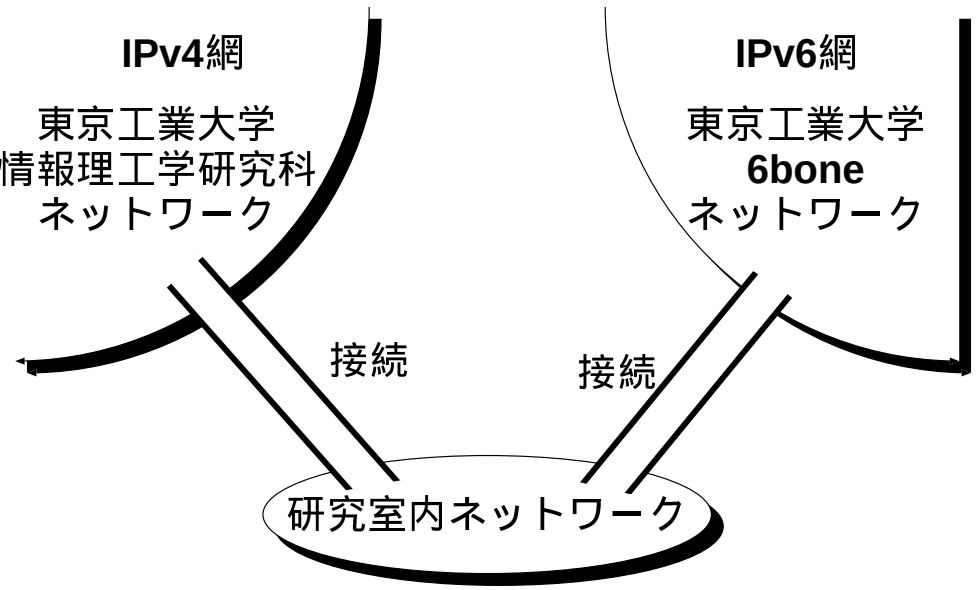

図 6.5: IPv6 網

6.2.1 IPv6デーの概要

IPv6 デーの目標を実現するため、東京工業大学 6bone 経由で IPv6 網への接続性を約一日確保し、研究室内ネットワークから IPv6 網の利用を可能にした。また、研究室内ネットワーク内の利用者セグメントでの IPv4 の利用を原則禁止にし、利用者の IPv6 利用を促した。

6.2.2 ネットワーク構成図

利用者セグメントでの IPv4 の利用を原則禁止にするため、利用者セグメントとバリアセグメントとの間で、IPv4 のパケットの中継を禁止した。これにより、利用者は IPv4 を利用したメールの送受信や、WWW の利用が不可能となる。そして、研究室内ネットワークと東京工業大学 6bone との接続性を確保し、バリアセグメントと利用者セグメントで IPv6 の利用を可能にした。IPv4 で構築された東京工業大学情報理工学研究科ネットワークに IPv6 パケットが流失しないように、IPv4 のパケットの中継を東京工業大学情報理工学研究科ネットワークとバリアセグメントの間で禁止した。IPv6 デー実施日のネットワーク構成を図 6.6 に示す。

6.2.3 IPv6デーの実施

1999 年 2 月 1 日 10:00 から同 22:00 まで、IPv6 デーを実施した。その結果を記す。

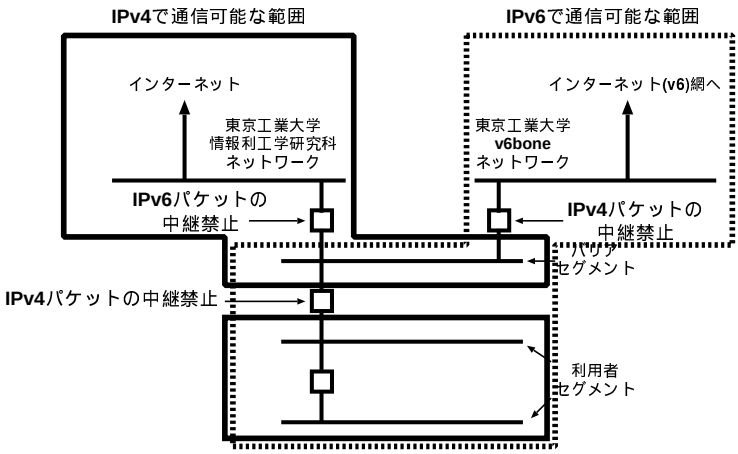

図 6.6: IPv6 デー実施時のネットワーク構成図

IPv6 網への接続性

13 時に利用者セグメントのルータ計算機を再起動したところ、利用者セグメントから外部 IPv6 網への接続性が途絶えた。これは、IPv6 のルーティングに異常が発生したと推測されるが、具体的な原因は調査中である。最終的に 21:15 にルータ計算機を再度起動しなおしたところ、外部 IPv6 網への接続性が回復した。

IPv6 デーの運用期間中、利用者セグメントから外部 IPv6 ネットワークへの接続を試みていたが、東京工業大学 6bone の上流ネットワークである松下電送システム株式会社が運用する v6 ネットワークを越えて上流へ到達できなかった。これは東京工業大学 6bone の経路情報が、外部 v6 ネットワークへ正しく流れていないためと推測されているが、詳細は調査中である。

これらの運用結果から、ネットワークの運用及び移動に関して幾つかの改善すべき点が判明した。

接続試験不足

今回の IPv6 デーは準備期間が実質数日と短かったため、事前に十分な接続試験ができなかった。このため、外部 v6 ネットワークとの接続性を確保できないまま IPv6 デー当日を迎た。IPv6 デー当日も接続性を確保しようとしたが、期間中一度も接続性を確保できなかった。ネットワークの接続先の新設や変更を行うさい、経路制御の取扱など注意を要することが多い。そのため、可能な限り事前の接続試験を行う必要がある。

管理運用態勢の不備

利用者セグメントでネットワーク障害が発生した後、IPv6 の取扱に習熟した管理者が一時期不在となった。そのため、障害の回復に時間を要した。管理者間の知識の共有をより進めるとともに、非常時における管理態勢を整備しなければならない。

提供したサービス

今回の IPv6 デーでは、利用者に DNS とメール、WWW のサービスを提供した。各サービスごとの実施状況と問題点を議論する。

DNS

IPv6 に対応したネームサーバの準備が間に合わなかったため、IPv4 にのみ対応したネームサーバを、利用者セグメントとバリアセグメントとの間で運用した。このため、IPv6 デーの期間中、利用者は IPv4 による名前解決を行った。

メール

メールの送信には IPv4 にのみ対応したメールサーバをバリアセグメント上に用意した。ネットワークからの接続要求とサービスを繋ぐ inetd と呼ばれるプログラムを IPv4 と IPv6 用に用意したため、IPv4 にのみ対応したメールサーバでも IPv6 によるメールの送信要求を処理できた。メールの受信には、利用者端末とメールサーバとの間に、IPv6 によるトンネルを張り、従来の IPv4 の技術で処理した。

WWW

IPv6 に対応した lynx と呼ばれる WWW クライアントを用意した。lynx を用いた利用者は、WWW サーバを IPv6 により参照できた。

各サービスの運用結果から、IPv6 対応への問題点が明らかになった。まず、現時点では IPv6 へ対応していないサービスが存在するため、従来の IPv4 によるサービスの提供が必要である。inted や ssh などのプログラムにより、IPv4 と IPv6 の技術を混在させて利用できた。異なるプロトコルへ移行する場合、元のプロトコル技術と新しいプロトコル技術が混在する状態が発生するため、それへの対応が必要である。

6.2.4 IPv6 デーのまとめ

IPv6 網への接続運用実験を通して、ネットワーク接続や運用態勢の問題点が明らかになった。また、利用者への IPv6 の普及を促進した。これにより、ネットワークの接続先の変更時における問題点を明らかにするとともに、利用者への対応が判明した。

第7章　今後の課題

本章では、機動性に配慮した小規模組織ネットワークとして構築・運用している研究室内ネットワークの今後の課題について述べる。

7.1　全ての計算機でのPICKLES端末の採用

研究室内ネットワークで運営しているNISサーバやファイルサーバ、内部情報共有用WWWサーバなどは、PICKLES仕様の計算機ではない。

これが原因で、研究室内ネットワークではSunOSをプラットホームとする内部情報共有用WWWサーバの運用中に問題が発生した。PICKLES端末のプラットホームであるBSD/OSとSunOSには、「hostname」と呼ばれる計算機名の設定や表示を行うコマンドがある。BSD/OSでは、管理者が「hostname -s」と入力すると、ドメイン名情報を取り除いた計算機名が表示される。同様のコマンドをSunOS上で管理者が実行すると、計算機名を「-s」に設定する。PICKLES端末の管理に習熟していた管理者は、SunOS上で「hostname -s」を実行し、計算機名を「-s」に誤設定した。そのため、該当計算機では、メールの運用などに障害が発生した。

また、ファイルサーバのプラットホームはNEWS-OSである。NEWS-OSの構造は他のPCの計算機とは異なる部分が多い。そのため、計算機内部の冷却ファンの掃除など計算機内部の整備を行う際、管理者の負担が大きい。他の計算機の大部分を占めるPCとは部品の交換性が低いため、部品の十分な冗長性を確保するのが困難である。

管理者の負担を軽減するため、ネットワーク内の計算機は可能な限り同一のプラットホームで運用することが望ましい。利用者端末以外で、PICKLES端末を採用していない計算機でのPICKLES端末の採用を検討する。

7.2　ネットワーク管理用メタデータの規定

ネットワークで運用しているサービスが記録するログは、サービス毎に多様な形式をしている。時間の表記に着目すると、syslogで記録に用いられる時間表記は、月と日、時、分、秒から構成され、「Jan 30 12:41:09 goat」の様な形式で表現されるプロキシサーバであるsquidで記録に用いられる時間表記は、年と月、日、時、分、秒、標準時間からの時差から構成されており、「08/Sep/1998:06:46:13 +0900」の様な形式で表現される。

ネットワーク管理においてログの解析は極めて重要だが、ログ解析をを行う管理者は、それぞれのログが出力する形式に対応した解析プログラムを使用しなければならない。ロ

グの出力形式の多様性が、管理者によるログ解析を困難にしている。また、管理者が管理に利用する各種コマンドの出力結果も多様である。このため、各種コマンドの出力結果を記録し後に解析する管理作業が困難になっている。

各種サービスやコマンドの出力形式を統一し、統一した手段による解析を可能にすれば管理者の負担の軽減に有効である。どのようなデータがネットワーク管理に必要か議論し、そのデータ形式を規定を検討する。大野研究室では松岡らにより、コンピュータが扱うメッセージ形式の統一化 [37] が行われている。

7.3 不正侵入検知システムの導入

研究室内ネットワークではファイアウォールを構築し、不要な IP パケットの転送を制限している。ファイアウォールの運用結果からその有効性は明らかであり、ネットワークセキュリティの頑強度は高い。しかし、ファイアウォールだけではネットワークの完全な安全性を確保できない。

第一に、既に自組織の内部に侵入してしまった不正侵入者に対してはファイアウォールは有効ではない。文献 [4] によれば不正侵入を受けた組織の 79%が内部から侵入されおり、ファイアウォールだけでは完全には安全性を確保できない。第二に、ファイアウォールは外部ネットワークに公開する必要のある計算機やサービスを保護できない。例えば外部ネットワークに公開しなければならない WWW サーバに対するサービス妨害攻撃などはファイアウォールでは対応できない。第三に、ファイアウォールは侵入者を感知できない。ファイアウォールは通過した IP パケットや転送制限した IP パケットの記録を取れるが、その記録からネットワークの不正侵入の試みを推測するのは、ネットワーク管理に対するある程度の知識と経験が管理者に要求される。

これらの問題を解決するため、不正侵入検知システム (Intrusion Detection System, IDS) の研究が盛んに行われている [23][25][26]。不正侵入検知システムは、単一または複数の計算機からネットワークを監視し、既知の侵入手口を用いた痕跡や計算機の弱点を利用しようとした形跡を調査し、不正侵入の検出を行うシステムである。このような不正侵入検知システムの中でソースコードを公開しているシステムとして、Network Fright Recorder 社が開発している NFR[25] がある。NFR は、ネットワークを監視しパケットの収集や解析を行い侵入者を検知する。

侵入者検知システムを開発するか、既存の侵入者検知システムを利用するかは別として、研究室内ネットワークでも侵入者検知のため何らかの対策を考慮する必要がある。

7.4 100Base Ethernet の利用者増加

研究室内ネットワークでは、利用者ネットワークとして、10Base Ethernet のネットワークと、100Base Ethernet のネットワークの 2 つがある。1998 年度初頭の時点で、100Base Ehternet に接続された利用者端末はなかったが、100Base に対応した NIC やハブの価格低下もあり、研究室内ネットワークでも 100Base に対応した NIC を保持する計算機も増加して

来た。1998 年 1 月 11 日現在では 10 台の計算機が 100Base 接続されている。今後も 100Base Ethernet に接続される計算機の増加が予想されるため、研究室内の 100Base Ethernet の構成や配線などを再考する。

7.5 ゲストアカウントの整備

研究室内の計算機は主に、研究室に所属する利用者が利用することを想定している。このため、研究室の来訪者などにネットワークの接続性を提供するとき、問題が生じた。研究室内ネットワークは、利用者の信用性を仮定している。しかし、一時的なネットワークの利用者に、通常の利用者と同じ権限を与えることは、セキュリティ上問題が生じる。来訪者への迅速な接続性や利便性の提供と、内部ネットワークの保護との両立を実現する必要がある。

第8章　結論

本研究では、小規模組織ネットワークのひとつである大野研究室内ネットワークの構築運用手法を議論し、小規模組織ネットワークにおける有効性を示した。

筆者が中心となり構築運用している大野研究室内ネットワークでは、サーバ計算機を含めて主要な計算機は PICKLES 端末で統一した。大野研究室内ネットワークで運用しているReborn Systemは、PICKL ES 端末の相互の交換性の高さを活用した障害管理システムであり、障害からの迅速かつ容易な回復を目的とする。Reborn Systemは、管理者の負担軽減や管理技術の不足に対応できるため、小規模組織においても有効である。

IPv6 への対応として、大野研究室内ネットワークでは、IPv4 とIPv6 の両方のプロトコルに対応できるデュアルスタック環境のネットワークを構築した。大野研究室内ネットワークのデュアルスタック環境の構築経験を基に、IPv4 を利用した小規模組織ネットワークがIPv6 に移行する手法を述べた。また、IPv6 への移行上の問題点の解明や利用者への利用促進を目的として、大野研究室で行った IPv6 Day と呼ぶ取り組みの結果を報告した。

これらの他にも、大野研究室内ネットワークのセキュリティ確保のために行ったファイアウォールの構築と運用方法及び結果について述べた。その運用結果を示し、ファイアウォールが有効に機能していることを示した。また、ファイアウォールの運用に要する管理者の負担が少ないことを示した。

その他にも、小規模組織ネットワークの対外接続先の変更を想定した取り組みなど、大野研究室内ネットワークを構築運用する上で行ったさまざまな手法について述べ、その手法の小規模組織への適応の有効性を述べた。

謝辞

本研究は大野研究室に所属する全員の協力がなければ決して成立しませんでした。大野研究室の構成員全員に感謝します。

指導教官である大野浩之講師には本研究を指導していただき、特に感謝します。そしてPICKLES プロジェクトに感謝します。WIDE プロジェクトでの活動を通して、一線の研究にふれることができました。WIDE プロジェクトのメンバに感謝するとともに、WIDE プロジェクト LifeLong Working Group の皆さんに特に感謝します。

参考文献

[1] Mrtg(multi router traffic grapher). http://ee-staff.ethz.ch/ oetiker/webtools/mrtg/mrtg.html",.

[2] Sakharov's akihabara report. http://www2s.biglobe.ne.jp/ sakharov/.

[3] Ssh communications security. http://www.ssh.fi.

[4] Csi/fbi computer crime survey. In *Computer Security Journal*, 1998.

[5] 特集 大規模・高速ネットワークの構築・管理運用. 情報処理学会, 10 月 1998 年.

[6] A.Bressen. Rita – the reliable internetwork troubleshooting agent. RFC2321, April 1998.

[7] Paul Albitz and Cricket Liu. *DNS and BIND 2nd Edition*. O'REILLY, 1997.

[8] B.Fraser. Site security handbook. RFC2196, September 1997.

[9] D.Brent Chapman and Elizabeth D.Zwicky. *Building Internet Firewalls*. O'REILY, 1995.

[10] The ATM Forum Technical Committee. Cumstomer network management(cnm) for atm public network service(m3 specification). http://www.atmforum.com/atmforum/specs/approved.html, October 1994.

[11] The Internet Community. Establishment of a memorandum of understanding of the generic top level domain name space of the internet domain name system(gtld-mou). http://www.gtld-mou.org/gTLD-MoU.html, February 1997.

[12] D.libes. Choosing a name for your computer. RFC1178, August 1990.

[13] Network Management Forum. http://www.nmf.org/.

[14] InterNIC. Internic registration services. http://www.internic.net/.

[15] JPNIC. /24 より小さい割り当てに対する、ネームサーバの逆引きの設定方法. ftp://ftp.nic.ad.jp/jpnic/ipaddress/ip-addr-delegation-dns.txt.

[16] JPNIC. Edドメイン名のページ. http://www.nic.ad.jp/jp/regist/dom/ed/index.html.

[17] K.Egevang and P.Francis. The ip network address translator.(nat). RFC1631, May 1994.

[18] Masahiko KIMOTO and Hiroyuki OHNO. A way to the ubiquitous computing: Design and implementation of the PICKLES information kiosk. In *International Workshop on Asia-Paciffic area advanced research information sharing technology, Internet Workshop '98*, March 1998.

[19] K.Nagami, Y.Katsube, Y.Shobatake, A.Mogi, S.Matsuzawa, T.Jinmei, and H.Esaki. Toshiba's flow attribute notification protocol(fanp) specification. RFC2129, April 1997.

[20] G. Mlkin. Rip version 2. RFC2453, November 1998.

[21] P. Mockapetris. Domain names - concepts and facilities. RFC1034, November 1987.

[22] M.Schoffstall, M.Fedor, J.Davin, and J.Case. A simple network management protocol(snmp). RFC1157, May 1990.

[23] Vern Paxson. Bro: A system for detecting network intruders in real-time. In *7th USENIX Security Symposium*, January 1998.

[24] WIDE Project. http://www.wide.ad.jp/.

[25] Marcus J. Ranum, Kent Landfield, Mike Stolarchuk, Mark Sienkiewicz, Andrew Lambeth, and Eric Wal. Implementing a generalized tool for network monitoring. In *Proceedings of the 11th Systems Administration Conference, USENIX LISA'97*, October 1997.

[26] Steven R. Snapp, Stephen E. Smaha, and Daniel M. Teal. The dids (distributed intrusion detection system) prototype. In *USENIX Conferece*, Summer 1992.

[27] T.Narten, E.Nordmark, and W.Simpson. Internet protocol, version 6(ipv6) secification. In *RFC2460*, December 1998.

[28] こねっと・プラン推進協議会. こねっと・プラン. http://www.wnn.or.jp/wnn-s/.

[29] インターネットドメインネームに関する研究会. ドメインネームのすべて. 株式会社クリエイト・クルーズ, 9月 1998年. 財団法人 日本データ通信協会・偏.

[30] 加藤朗. Root dnsについて. In *IP Meeting '97*, December 1997.

[31] 教育ソフト開発・利用促進センター. 100校プロジェクト. http://www.edu.ipa.go.jp/100school/.

[32] 警察庁. 不正アクセス対策法制に関する調査研究報告書. http://www.npa.go.jp/soumu7/nsreport.html.

[33] 大野浩之. 機動性に配慮した小規模ネットワークの構築経験 -(1) 総論-. 情報処理学会第 55 回全国大会, 9 月 1997 年.

[34] 松井彩. 高齢者・障碍者によるインターネットの利用. WIDE プロジェクト研究報告書, 3 月 1998 年.

[35] 斎藤健, 高畠由彰, 橋本幹生, 岡本利夫. デジタル情報家電の接続を考慮した家庭内ネットワークアーキテクチャ. In *TECHNICAL REPORT OF IEICE*, 11 月 1997 年.

[36] 山根健, 石橋啓一朗, 村井純. 生涯利用可能なネットワーク環境における名前空間と個人用ドメイン. In *Information Survivality Workshop*, 1998 年.

[37] 松岡保静. Pickles 情報キオスクでのメッセージ形式の統一とその評価. 東京工業大学大学院 情報理工学研究科 卒業論文, 2 月 1999 年.

[38] 上田仁. 1996 年度 wide プロジェクト研究報告書 (第 3 部,5 章,1 節, 生涯に渡って利用できる名前空間). WIDE プロジェクト, 7 月 1997 年.

[39] 上田仁. 1997 年度 wide プロジェクト研究報告書 (第 2 部,2 章,1 節, 大野研ネットワークの構築). WIDE プロジェクト, 7 月 1998 年.

[40] 上田仁, 大野浩之. 永年利用可能な url を利用したインターネット上の情報提供. 情報処理学会 第 84 回マルチメディアと分散処理研究会, 9 月 1997 年.

[41] 上田仁, 大野浩之. 機動性に配慮した小規模ネットワークの構築経験 -(2) 名前空間-. 情報処理学会 第 55 回全国大会, 9 月 1997 年.

[42] 上田仁, 木本雅彦, 大野浩之. 小規模組織に適した標準ネットワークとその管理支援系の構築. 情報処理学会 分散システム運用技術研究会, 9 月 1998 年.

[43] 東田学, 門林雄基, 下條真司, 宮原秀夫. Atm lan emulation による大阪大学キャンパス・ネットワークの構築. 分散システム運用技術シンポジウム, 2 月 1998 年.

[44] 本庄利守, 大野浩之. 機動性に配慮した小規模ネットワークの構築経験 -(3) 設計と実装-. 情報処理学会 第 55 回全国大会, 9 月 1997 年.

[45] 本田新九郎, 富岡展也, 木村尚亮, 大澤隆治, 岡田謙一, 松下温. 作業者の集中度に応じた在宅勤務環境の提供. 情報処理学会論文誌, 5 月 1998 年.

[46] 木本雅彦, 大野浩之. 機動性に配慮した小規模ネットワークの構築経験 -(4) 運用および管理-. 情報処理学会 第 55 回全国大会, 9 月 1997 年.

[47] 木本雅彦, 大野浩之. 自律型ネットワーク端末 (PICKLES) を用いたシステム運用技法. 分散システム運用技術 シンポジウム'98 論文集, February 1998.

[48] 門間信行. ネットワーク利用者が持つ情報の集約化支援機構とその評価. 東京工業大学大学院 情報理工学研究科 修士論文, 1 月 1998 年.

[49] 野田明生, 大野浩之. Ipv6 の特徴を活用した研究資材管理システムの提案. 分散システム運用技術 研究報告 No.11, 9 月 1998 年.

[50] 野田明生, 門間信行, 大野浩之. 小規模な組織の運営を支える情報共有機構-(1) 備品購入管理システムの設計-. 情報処理学会 第 55 回全国大会, 9 月 1997 年.

[51] 郵政省. 「電気通信システムに対する不正アクセス対策法制の在り方について」への意見 (パブリック・コメント) の募集. http://www.mpt.go.jp/pressrelease/japanese/new/981125j601.html.

[52] 宇夫陽次郎, 石山政浩, 新善文, 村井純. 大規模な仮設型ネットワークテストベッドの設計・構築とその運用. インターネットカンファレンス'97, 12 月 1997 年.

付 録A　研究室内ネットワークの歴史

大野研究室では基本的に 1 週間に 1 度、構成員全員が集まりミーティングを行う。そのミーティングの様子を記録した議事録をもとに、大野研ネットワークの歴史を記した。これは、1996 年 4 月から 1999 年 1 月までの記録である。日時は極力正確を期したつもりだが、議事録を基にしているため 7 日前後の相違がある可能性がある。

1996/04/24 ファイルサーバで利用者領域の制限 (quota) 開始

1996/05/01

- 大野研究室 WWW ページの整理
  - 表: 文献情報, 個人の WWW ページ, 配布ソフトウエァ, スケジュール情報
  - 裏: 研究室の内部情報, セキュリティ情報, その他プライベートな情報
- 物品管理システム開始
- 係分担において、物品係と買物係の新設

1996/05/01 物品購入システム確立

1996/06/12 私物 PC のネットワーク接続問題の議論開始

1996/07/23 計算機用メモリ購入計画

1996/08/14 計算機用音源カード 購入計画

1996/09/25 私物 PC のネットアーク接続問題の議論

1996/10/13,14 工大際で大野研テクノロジの紹介

1996/10/23 ファイルサーバのバックアップ体制の議論

1996/11/06 MAC 購入議論

1996/11/27 電話環境整備

1996/12/25 管理者権限取得条件の議論

1997/01/08 来年度ネットワーク構成の議論開始

1997/01/15 本庄案採用を用いてネットワークの設計

1997/01/22 新ネットワーク構成のため、ファイルサーバをマルチホーム化

1997/01/05 ネットワークの性能測定

1997/03/** ohnolab-cfp 開始

1997/03/05 物品管理システムに伴う第 1 回棚卸し

1997/03/11

- 個人 PC を含む PICKLES 化
- 大野研内 NIS サーバの運用開始

1997/03/26

- 電源周り議論 (3 系統)
- IP リナンバリング

1997/04/09 松下電送株式会社の IPv6 網と大野研究室の IPv6 網の接続

1997/04/16

- 管理者権限取得のガイドライン問題議論
- 無停電電源の設置問題議論

1997/04/23

- 研究室購入の論文誌・雑誌の管理開始
- 管理者権限取得のガイドライン問題議論 (再)

1997/04/30

- 研究室ネットワークの運用方針決定
- 管理者権限取得のガイドライン決定
- PPP 回線運用開始
- 大野研究室 IPv6 実験ネットワークのレビュー

1997/05/07

- 大野研 FYI 開始
- 電話線整備

1997/05/15

- satan や crack によるセキュリティのチェック
- PC 棚卸し

1997/05/21

- ファイルサーバの利用者領域制限 (quota)
- 対外接続点によるスクリーニングの議論開始
- I 内線整備

1997/06/18

- 100base Ethernet 線を 305 号室から 303 号室へ敷設
- 100base Ethernet 線を 303 号室から 305 号室へも敷設

1997/07/02 PICKLES 端末で WWW サーバの運用開始

1997/07/09

- 研究室内ネットワークのスクリーニング開始
- 10BASE-5 ハブの有効活用について議論
- エアコン稼働開始

1997/07/16

- 研究室内で運用するメーリングリスト名の整理
- セキュリティ議論

1997/07/30

- 停電に伴うネットワークの停止・起動手順作成
- 研究室内 WWW サーバ (www.ohnolab.org) 稼働開始
- 利用者アカウントの登録手順議論

1997/09/04

- netsound サーバ故障
- 重要な計算機のバックアップ体制の議論

1997/09/10 ルータ計算機の PICKLES 端末化議論

1997/09/17 AEF97, sensorium チーム金賞受賞

1997/09/23 研究室内ネットワークに流れる無意味な経路情報の削除を議論

1997/10/01 利用者アカウント作成のガイドライン作成

1997/10/08 WWW サーバを 101 号室へ移動

1997/10/17 全ルータ計算機で PICKLES 端末を利用

1997/10/29

- InterNIC へ、ドメイン名 ohnolab.org の申請
- メールサーバで DNS の運用開始

1997/11/12 プリンタ購入

1997/11/19

- ohnolab.org ゾーンに全計算機の登録
- メールサーバで PICKLES 端末の利用

1997/11/26 大野研究室内メーリングリストの整備

1997/01/14 4 年生による管理者権限取得

1997/01/24 ~ 1997/01/25 停電に伴うネットワークの運用停止

1998/02/04

- スクリーニングルータ (wide.ohnolab.org) の故障
- RebornSystem 作成開始

1998/02/11

- 紛失物品ガイドライン作成
- Reborn System 用計算機の運用開始

1998/02/28 停電に伴うネットワークの運用停止

1998/03/11 次年度利用者計算機構成案作成, 目標:4 年生にも Pentium を!

1998/03/17 計算機冷却のため、308 号室に旋風機を導入

1998/03/** 物品管理システムによる第 2 回棚卸し

1998/04/08

- IP アドレスのリナンバリング実施
- 携帯端末 (gon.ohnolab.org) の紛失

1998/04/15

- 大野研 IPv6 網の整備
- 公共利用 Windows 計算機整備

1998/05/06 論文執筆〆切ガイドライン作成

1998/05/27 ベンチマークガイドライン作成へ

1998/06/03 計算機冷却のため、308 号室にクーラ取り付け

1998/06/10 ファイルサーバの利用者領域の増設 (2.0Gbyte から 4.0Gbyte へ)

1998/07/01 バックアップ担当者の変更とバックアップ体制の再考

1998/07/07 qpopper のセキュリティホール報告に伴い、qpopper の最新版 (2.53) をメールサーバへインストール

1998/07/08 AV 環境整備

1998/08/01 ~ 1998/08/02 停電に伴うネットワークの運用停止

1998/08/10 WWW サーバ (tanuki.ohnolab.org) の故障

1998/08/19 計算機の物理的な防御 (鍵) 問題議論

1998/09/** PICKLES 開発マシン (jupiter.ohnolab.org) の運用

1998/09/** 対外接続ルータを除く、ルータ計算機の PICKLES 端末を更新 (DR03 化)

1998/09/** s/key を廃止し、ssh を導入

1998/09/02 論文〆切超過ガイドライン作成

1998/10/21

- 研究室内ネットワークの接続先変更議論
- SPAM メールの転送拒否設定

1998/11/04 ssh のセキュリティホールに関する議論

1998/11/18 2 名のゲストアカウント作成

1999/01/06 大野研 2000 年問題対策開始

付 録B　セキュリティ情報の情報源

- Computer Emergency Response Team(CERT, http://www.cert.org/)
  一般に CERT と呼ばれる。不正なシステム侵入に対する緊急対応を中心にインターネットセキュリティの情報収集や分析、再発防止策の検討、セキュリティ技術の教育・啓発活動を行っている。

- コンピュータ緊急対応センター (JPCERT/CC, http://www.jpcert.or.jp/)
  CERT の日本語版。セキュリティ関連の資料や情報を取得するのに有効。定期的に目を通すことが重要である。

- JPCERT/CC メーリングリスト (announce@jpcert.or.jp)
  セキュリティホール情報などの報告がある。このセキュリティホール情報が報告された直後の週末は、その内容を基にしたクラックの試みが多いといわれている。

- 電脳火消し隊 (http://www.firewall.gr.jp/)
  非営利の任意団体。この団体の announce メーリングリストには、多様なメーリングリストに流れるセキュリティホール情報 (英語) が転送される。会員同士の親睦も計っている。

- 「ファイアーウォール構築」「UNIX&インターネットセキュリティ」
  セキュリティに興味があるならまずこれらの書籍を読むこと。ファイアウォールの構築の仕方などを含めて、セキュリティ全般に関し詳細に解説している。

- RFC2196(Site Security Handbook)
  コンピュータのセキュリティポリシを設ける際のガイドラインが記載されている。セキュリティに関して全般的によくまとめられており、一通り目を通す価値はある。

- Internet Week のセキュリティ・ゼミナール
  Internet Week は、年 1 回行われるカンファレンスである。セキュリティ・ゼミナールは、その期間中に講座の一つとして開設される。セキュリティに関する最新の情報を網羅的に得られる。参加費が数万円するため個人では出席しづらいかもしれないが、出席した方がよい。1998 年度は、JPCERT の運営委員の人が講師をしていた。

- コンピュータ悪のマニュアル (1)(2)
  書籍として販売され、不正侵入の手口やそれに用いるソースコードを記載している。記載されている不正侵入の手口は良く知られた古い手段が多い。これらの書籍に記載されている手段には最低でも対処しておくこと。

- 不正アクセス防止法案 (http://www.npa.go.jp, http://www.mpt.go.jp)
  　警察庁や郵政省によって、不正アクセス防止法案の制定が進められている。一定期間のログ保存の義務化などの可能性もあり、管理者ならば注目していく必要がある。

- SPAM サイトリスト (VIX/MAPS RBL http://maps.vix.com, DORKSLAYERS/ORBS)

  　SPAM メールへの対策のため、各種のリストを提供している。例えばメールの不正中継を許しているサイトはこれらのリストに載る可能性がある。DORKSLAYERS は、一時サービスを停止している。