高速ネットワークと教育用 PC クラスタシステムの構築およびディレクトリサービスを用いたユーザアカウント管理

倉前 宏行　　島野 顕継
大阪工業大学 工学部 経営工学科
E-mail: kuramae@dim.oit.ac.jp, shimano@hitomi.dim.oit.ac.jp

概要： 大阪工業大学工学部経営工学科において，学科内ネットワークを増強すると共に，学科専用の教育用 PC クラスタシステムを構築した．クライアント PC には Windows NT Workstation と PC-UNIX の 2 つのオペレーティングシステムをインストールし，利用形態に応じてデュアルブートできる環境を構築した．学生ユーザアカウントは，学内の共通施設とシームレスに利用できるようにするため，Windows と UNIX を同じアカウントで利用できるようにすると共に，情報センターと連携して一元管理した．さらに，ユーザアカウント管理を省力化するため，ディレクトリサービスを導入し OS 混在環境における全学的な一元管理を実現した．

キーワード： PC クラスタシステム，ユーザアカウント管理，ディレクトリサービス

1. 緒言

近年，情報処理教育の増大により大学共通施設である情報センターの演習教室が飽和状態となっている．これを解決するとともに，学科独自の教育内容に柔軟に対応できる演習教室として，著者らはこれまで，Windows NT と PC-UNIX のデュアルブート環境を提供する学科専用の PC クラスタシステムを構築してきた [1–3]．

このシステムは，コンピュータリテラシ教育からプログラミング，数値実験などの演習，さらには研究利用や授業時間外のオープン利用まで，のべ 1000 名もの学生がさまざまな授業演習等で利用する．よって，ユーザはコンピュータに初めて触れる者から，研究のためのシステムソフトウェア開発を行う者まで，スキルやその利用形態はきわめて幅広く，これに対応した管理・運用が求められる．一方でこのシステムは，情報処理センターのようなシステム管理・運用のための専門組織を持たない．したがって，本システムでは，あらかじめセキュリティ対策を万全にしておくことや，システムの運用管理を出来る限り省力化することが特に必要となる．

そこで，本システムでは Windows 環境のファイル共有および NT ドメインへのユーザ認証を行うため，UNIX サーバに Samba [4] を導入し，ユーザのデータ領域とアカウントを一元管理した．また，本学情報センターで一括管理されている学生ユーザ情報と連携させることにより，本システムではユーザ管理を一切すること無く Windows と UNIX のパスワード情報の一元化を実現してきた．

さらに，本年度全学的に新規導入されたディレクトリサービス NDS (Novell Directory Services) を用いて，情報センターが全学生に発行している計算機利用アカウント 1 つで大学共通施設とシームレスに本システムが利用できるようにシステムの変更を行った．本稿では学生ユーザの振舞に基礎をおいたシステムの設計方針，および Windows と UNIX の 2 つの OS (Operating System) の混在環境におけるユーザアカウントの全学的な一元管理の方法について述べる．

2. 教育用システムの設計方針

2.1 性善説システムと性悪説システム

教育用システムを設計する際には，授業演習内容に基づいて導入するアプリケーションソフトウェアや OS がほぼ自動的に選択できる．一方で，システムの管理運用の立場からは，学生ユーザのモラルの高さ，すなわち学生ユーザの振舞を性善とするか性悪とするかによって，表 1 に示す 2 つの管理形態が考えられる．

表 1: 性善説システムと性悪説システム

	性善説システム	性悪説システム
前提	善意のユーザのみ	悪意のユーザが存在
学生の振舞	常識を持って利用 システムを改変しない 操作ミスをしない	非常識な利用 システムを改悪する 操作ミスをする
管理形態	特に管理の必要なし	ユーザ認証 利用制限 セルフメンテナンス

現在，ほとんどの教育用システムは性悪説に基づくシステムが構築・運用されているのが一般的であり，悪意を持ったユーザや操作ミスによって

システムが改変されないようにするため，ユーザ認証を行ったり，ユーザ区分による利用制限が必要となる．

2.2 性悪説に対応するためのシステム設計

教育用システムの要求仕様を実現する手段は，管理者のスキル，予算額などによって異なる．性悪説に基づくシステムの設計として，たとえばサーバとクライアントを全て UNIX 系 OS で統一すると，マルチユーザ環境に対応した OS であるため，NIS (Network Information System) によるユーザ認証と NFS (Network File System) によるユーザファイルの一元管理によって，システム管理者と学生ユーザを区別することにより，ファイルのアクセス権などから利用制限を設定することができる．また，シェルやデスクトップの設定といった個人環境は，カスタマイズ情報がユーザ領域に保存されることから，ユーザごとに独立に行うことができ使用するクライアントを移動してもそれらが完全に反映される．

サーバおよびクライアントを全て Windows 系の OS で統一した場合にも，OS 標準の機能によってユーザ認証とユーザファイルの一元管理が可能である．しかし，元々個人利用を前提に開発された OS であるため，デスクトップ環境設定などの情報は，クライアントを移動してもそれが反映される移動プロファイル機能が実用的ではない．このため，プロファイル情報はクライアントのシステム領域に保存することになり，ユーザごとの設定を独立に行うことができない．また，OS 自体が不安定であるため，講義の開始前などにサーバを再起動させるなどといった必要もある．

しかし，OS が混在するシステムにおいては，ファイルシステムやユーザ認証を相互参照できるようにするためのシステムソフトウェアが必須となるほか，ユーザアカウントを一元管理するのは容易ではない．

2.3 システムの利用形態

学科専用の PC 演習室における授業演習の利用内容 (要望) として，次の 7 項目が上がった．

1. コンピュータリテラシ教育
   ワープロ・表計算・電子メールといった基本的な PC の使い方の修得
2. プログラミング言語教育
   C 言語・Fortran 言語のほか，基本的なアルゴリズムの修得
3. 経営工学諸問題の解法
   表計算･統計計算ソフトウェアを利用した計算
4. 数値実験
   システムシミュレーションなどの数値仮想実験の実施
5. ネットワークコンピューティング
   MPI (Message Passing Interface) や PVM (Parallel Virtual Machine) を用いた PC クラスタによる並列分散処理
6. 研究利用
   卒業研究生，大学院生，教員向けの研究利用環境
7. オープン利用
   レポート作成やインターネット端末などの，空き時間のオープン利用

この要望を満足させるとともに性悪説に基づいた管理運用が可能なシステムを構築した．

3. ハードウェア構成

3.1 学科内 LAN

1999 年 9 月，これまで敷設されていた 10BASE-5 ネットワークに加え，学科内の教員室，研究室および PC 演習室に 100Mbps の通信容量を持つ 100BASE-TX ネットワークを敷設して相互接続した．セキュリティ対策のため，演習室と研究室を別サブネットとし，IP VLAN (Internet Protocol Virtual Local Area Network) を設定するため，図 1 に示すように，合計 7 台のレイヤ 4 スイッチングハブ (ケーブルトロン SSR2000) を導入した [2]．VLAN の仕様は IEEE 820.1Q によって標準化されているものの，異機種間で VLAN を設定した際の相性を考慮して，7 台とも全て同じ機器とした．本ネットワークの幹線にあたるスイッチングハブ間は，それぞれ 2 本の UTP ケーブルで接続されており，トランキング機能により 400Mbps の通信容量を持っている．

3.2 学科内 PC 演習教室

学科内にネットワーク接続された PC 演習教室を 2 部屋設置した．100BASE-TX ネットワークの敷設と同時期に，経営情報システム実験室に 28 台

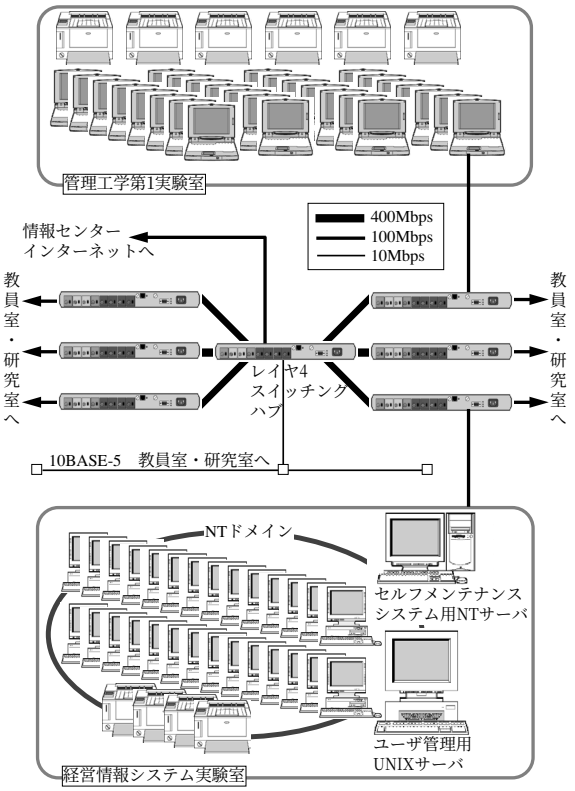

図 1: 学科内 LAN と PC 演習室

のデスクトップ PC (富士通 FMV-6450DX3) を導入した．幅広い利用形態に対応するため，OS として Windows NT Workstation と FreeBSD 2.2.8R をそれぞれインストールし，デュアルブート環境を構築した [1].

管理用サーバとして，UNIX サーバ (富士通 GP400S5) および Windows NT サーバ (富士通 FMV-6550TX3) をそれぞれ 1 台ずつ設置している．NT サーバは，セルフメンテナンス [5] のサーバとして動作し，深夜に Windows NT 環境のファイルシステムを自動的にメンテナンスする．

また，管理工学第 1 実験室にはノート PC (富士通 FMV-3233NA/X) を 29 台設置し，OS として Windows 98 を利用している．それぞれの演習室は少人数制の演習教育に利用している [6].

4. ユーザアカウントの一元化

4.1 UNIX と Windows 混在環境

UNIX と Windows の混在環境において，ユーザのデータ領域 (ホームディレクトリ) は，UNIX サーバに Samba といった UNIX リソースを Windows 環境に提供できるようにするためのシステムソフトウェアを導入することによって，一元化することができる．しかしながら，ユーザの認証は UNIX と Windows においてパスワードの暗号化など認証方式が異なるため，図 2 に示すように，NIS と SMB (Server Message Block) パスワードファイルにより，それぞれユーザアカウントのデータベースを作成保持しなければならない．

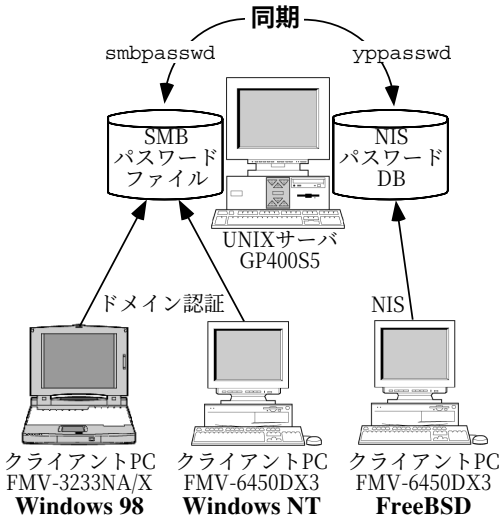

図 2: パスワードファイル

この 2 つのアカウントデータベースを一元化し，さまざまな OS の利用を同じユーザ名とパスワードで利用できるようにする方が，管理運用上さらにはユーザにとっても便利である．しかし，パスワードの暗号化をはじめとするユーザ認証方法は，セキュリティ上，OS にとっては最も機密を保持しなければならない機構であることから，異なる OS のユーザ認証方法を容易に一元化することは不可能である．

このため，たとえば，FreeBSD 環境から `yppasswd` コマンドを用いて自分のパスワードを変更すると，NIS のパスワード情報のみが変更され，SMB パスワードファイルにはそれが反映されない．同様に Windows からのパスワード変更は SMB ファイルに対してのみ行われることから，2 つの OS 環境においてユーザは同じログイン名を用いていても，パスワードは別々に使い分けなければならず，学生ユーザにとって混乱の原因となる．

4.2 パスワードファイルの疑似一元化方法

本学においては，入学時に全学生に対して情報センターがユーザアカウントを交付している．そ

こで，本システムにおいてもこのアカウントをそのまま利用できるようにするため，図 3 に示すように，情報センターで作成されているユーザアカウントデータベースを参照し，2 つの OS のパスワードを一元化するための仕組みを構築した．

情報センター側に Samba の SMB パスワードサーバを設置し，同図のように本システムと連携させた．さらに本システムの UNIX サーバを NIS レプリカサーバに設定し，UNIX のアカウントも連携させた．

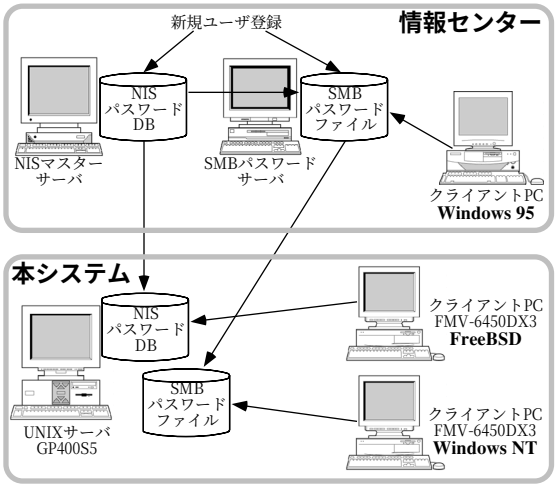

図 3: ユーザ認証方法

FreeBSD には NIS，Windows NT には Samba と，パスワード情報が二重化されているため，これらの同期を取る必要がある．そこで，パスワード変更の仕組みを，図 4 のように作成した．

Windows NT においては，OS 付属のパスワード変更機能を使用できないようにし，この代わりにメーラ (Win/YAT 32) に付属している `poppasswd` コマンドを用いることにする．UNIX サーバが TCP (Transmission Control Protocol) の 106 番ポートで要求を受け取ると，`poppassd` デーモンは `smbpasswd` コマンドを発行し情報センターの SMB パスワードファイルを更新する．さらに `poppassd` デーモン本来の動作である `yppasswd` コマンドも発行し，NIS データベースを更新する．

FreeBSD においても，付属の `yppasswd` コマンドを UNIX サーバに対する `poppasswd` として動作するシェルスクリプトに置き換えた．以上により，Windows NT，FreeBSD のいずれからのパスワード変更操作も，UNIX サーバの `poppassd`

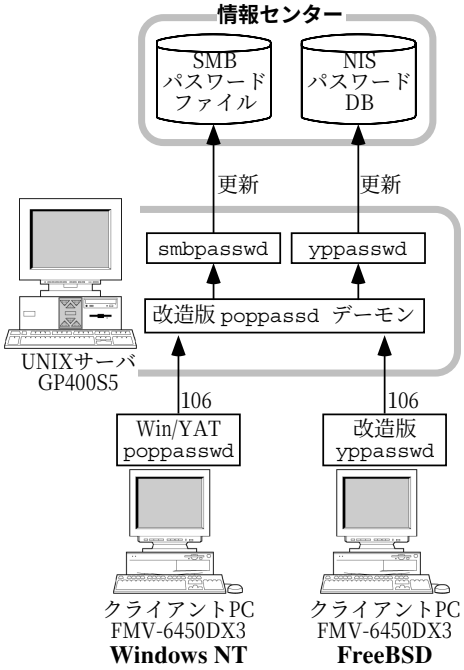

図 4: パスワードファイルの疑似一元化

デーモンを通じて同時に双方のパスワードファイルに反映され，2 つの OS のパスワードが疑似的に一元化されることになる．このシステムは，構築後約 1 年間ほぼ問題なく運用してきた．

5. ディレクトリサービスの導入

5.1 NDS (Novell Directory Services)

2000 年 9 月，情報センターのシステム更新に合わせて，全学の学生ユーザアカウントを一元管理するため，図 5 に示すように，本学の 2 つのキャンパスに NDS Corporate Edition を導入した．NDS はもともと NetWare 4.x 用に開発されたディレクトリサービスであるが，今回導入した Corporate Edition では IP (Internet Protocol) に対応し，図 6 に示すように，Windows NT における SAM (Security Account Manager) 認証，および，Solaris，Linux などにおける PAM (Pluggable Authentication Modules) 認証と NSS (Name Service Switch) フレームを提供することができる．NDS では，図 7 に示すように，アカウント名，パスワード，ログインスクリプトなど，50 以上の情報を一元管理することができる．なお，NDS におけるパスワードは RSA 暗号方式を採用している．

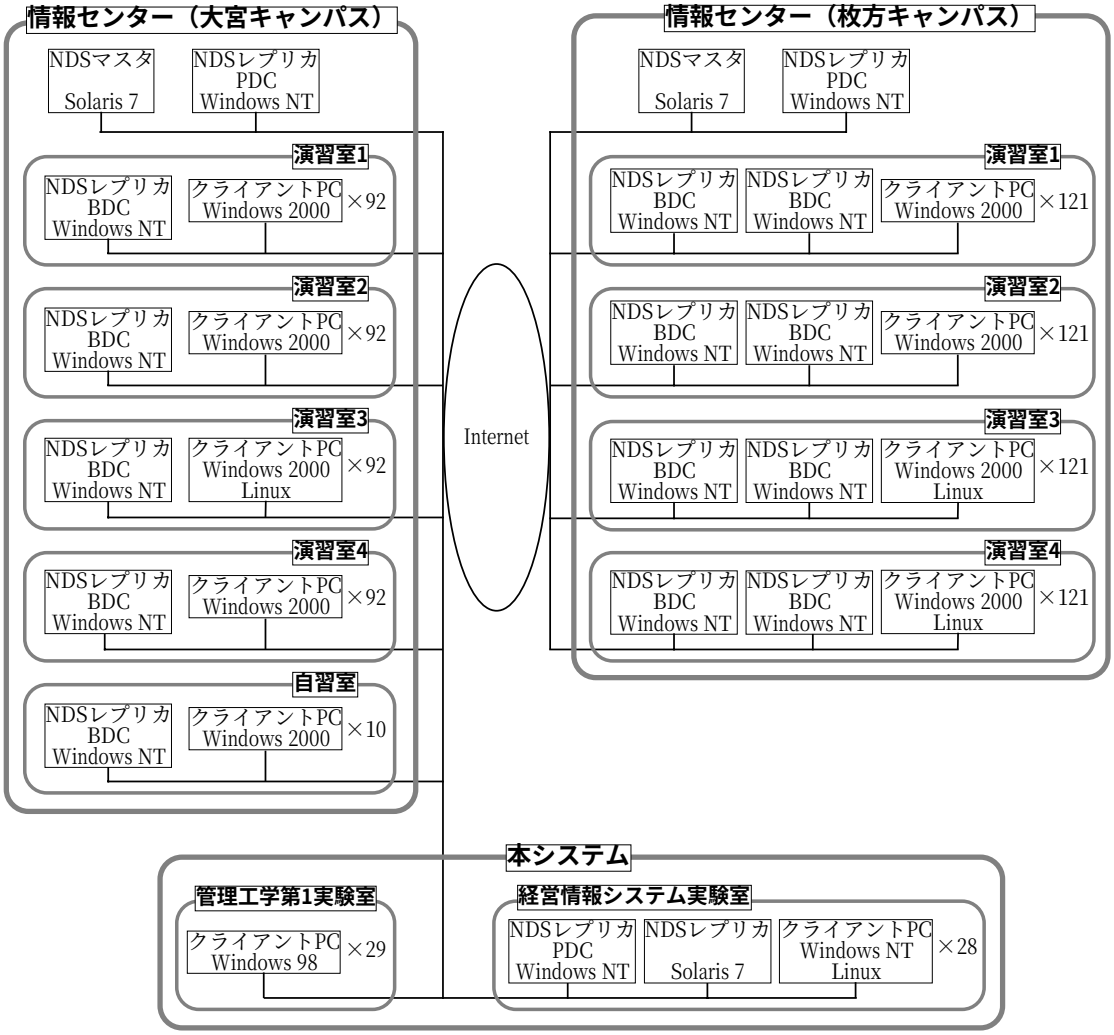

図 5: NDS の全学的導入

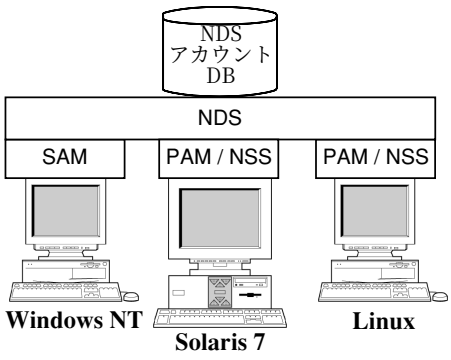

図 6: NDS Corporate Edition

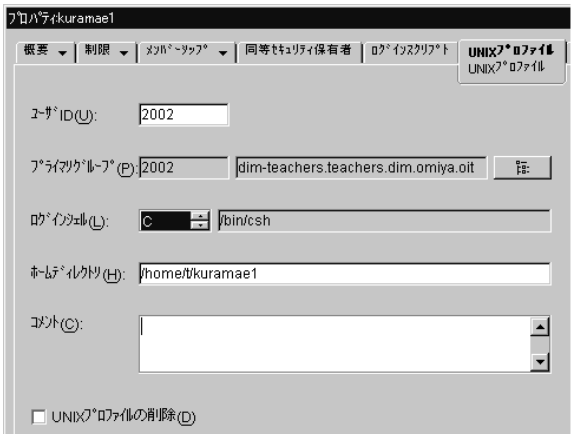

図 7: NDS のユーザ情報設定画面 (一部)

5.2 NDS によるアカウントの一元管理

NDS の導入にあたり，情報センター側に本ユーザのアカウントを管理するための NDS マスターサーバが置かれるため，本学科内のシステムにおいては，図8 に示すように，NT サーバ，UNIX サーバをそれぞれNDS レプリカサーバに設定した．NT

ドメインの PDC (Primary Domain Controller) は，NT サーバ上で立てることとし，NDS による SAM 認証を行う．Samba を用いた UNIX サーバのホームディレクトリの NetBIOS (Network Basic Input Output System) マウントの際にも，NDS による PDC へのドメイン認証が必要となる．また，クライアント機でこれまで利用してきた FreeBSD は NDS に対応していないため，RedHat 6.2J (Linux 2.2.16) に置き換え，NDS による PAM 認証を行うことで，2 つの OS 混在環境において全学合わせて 8000 名分のユーザアカウントの完全一元化を実現した．

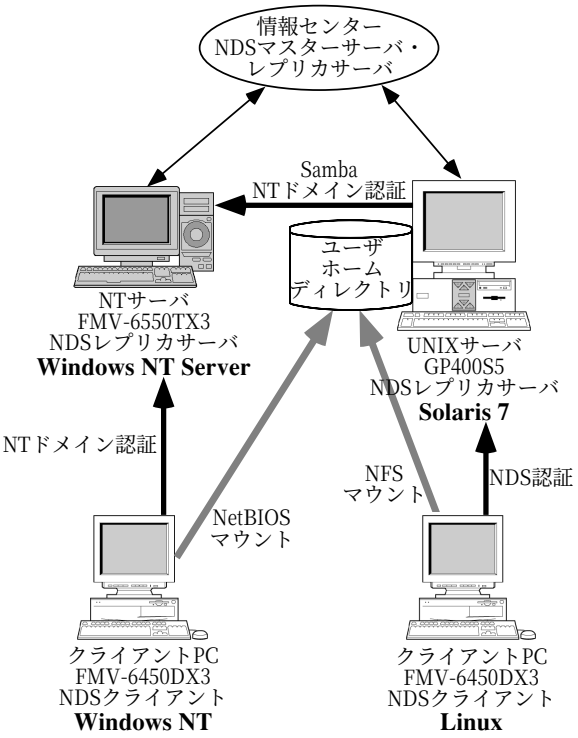

図 8: NDS を用いたシステム構成

5.3 NDS のレスポンス性能

Windows 環境にログインすると，NT ドメインの認証が成功した後，Samba によるホームディレクトリのマウントのため，UNIX サーバから NT サーバ (PDC) に対して再び NT ドメイン認証が実行される．このため，NDS 導入以前の SMB パスワードファイルを用いて 1 回のユーザ認証で済ませていた場合に比べ，多数のクライアントから一斉にログイン操作を行うと，サーバへの処理が集中し，全てのクライアントにおいてホームディレクトリがマウントされるまでに数分から十数分の時間を要するようになった．このサーバ間の認証処理はバックグラウンドで実行されるため，ホームディレクトリのマウント処理中であっても，クライアント側ではアプリケーションソフトウェア等を通常通り利用できるものの不便である．

一方，Linux 環境においても，NIS を用いて運用していた場合に比べて大幅にレスポンスが低下した．たとえば，`/home/t` という 119 名分のユーザホームディレクトリが格納されているディレクトリにおいて，`ls -l` コマンドを実行すると，NIS を用いた通常の Linux 環境ではミリ秒単位の処理時間で実行されるのに対し，NDS を用いたシステムでは，3 分以上の時間を要した．これは，`ls -l` や `ps` コマンドなどにおいて，ファイル (ディレクトリ) やプロセスの所有者名やグループ名を UID や GID から NSS を経由して NDS へ参照するのに時間を要していると考えられる．

こうした Linux 環境における NDS のレスポンス低下原因を調査するため，UNIX サーバ上で `snoop` コマンドや `tcpdump` コマンドを用いて，演習室内ネットワークおよび情報センター向けの経路を流れるネットワークパケットをモニタリングした．その結果，ユーザ認証時や `ls -l` コマンド実行中には，クライアントと UNIX サーバ (NDS レプリカサーバ) との間，さらに UNIX サーバと情報センターの NDS マスターサーバとの間で連続的にネットワークパケットが送受信されていることが分かった．また，連続して `ls -l` コマンドを実行しても，マスターとレプリカサーバ間で同様な通信が発生しており，このことからクライアントおよびレプリカサーバにおいて，NDS データのキャッシングがほとんど機能していないことが分かった．

NDS の性能を向上させるため，ユーザオブジェクトツリーの構成を変更するなどいくつかのチューニングを試みたものの，改善することはできなかった．このように，現時点では，NDS を用いた Linux 環境は実用に耐えがたいものである．

5.4 NDS と NIS を併用した運用

Linux 環境の動作レスポンスを抜本的に改善するため，図 9 に示すように，演習室内に NIS サーバを設置し，パスワード以外のユーザ情報を NIS マップによってクライアントへ提供するようにした．すなわち，図 10 に示すように，PAM 認証の

みに NDS を利用し，パスワード照合以外の UID や GID といった NSS 経由のユーザ情報は NIS を参照するようにした．

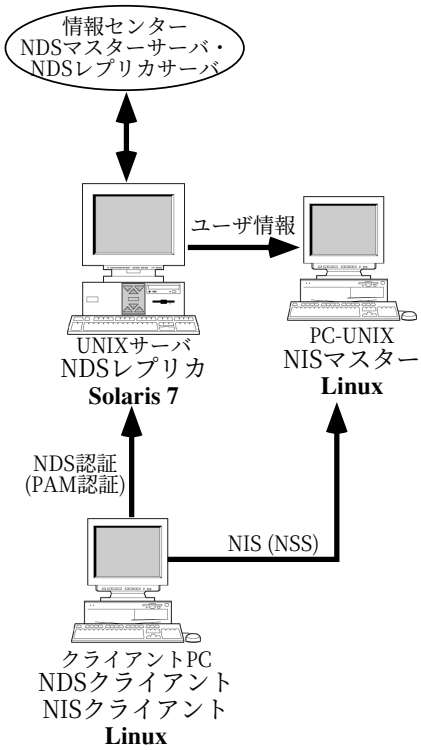

図 9: NDS と NIS の併用システム

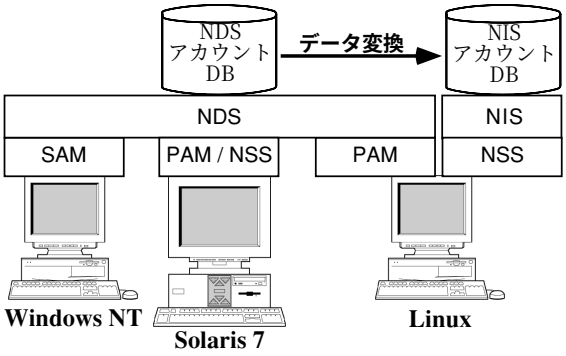

図 10: 性能向上のためのユーザ情報の二重化

ユーザ情報の更新に対応するため，定期的 (1 日に 1 回) に NDS のアカウントデータベースから NIS マップにデータを自動変換するようにした．このとき，NDS のパスワード情報は RSA 暗号となっているため，NIS の `passwd` マップのパスワードフィールドへは変換できないが，パスワードの参照は PAM 経由で NDS へ行われるため問題ない．

この仕組みより，パスワード照合以外の動作レスポンスは，NDS 導入以前の NIS を利用している場合と同程度となり，実用に耐えうるシステムとなった．

6. 結言

学科専用の PC 演習室を構築するとともに，Windows NT と UNIX の混在環境において，ユーザアカウントを全学的に一元化するために，ディレクトリサービス NDS を導入した．これにより情報センターおよび学科独自のシステムを 1 つのユーザアカウントでシームレスに利用できるようになり，学生の利便性が向上するとともに，学科システムの管理が省力化された．しかしながら，現時点での NDS の Linux モジュールおよびレプリカサーバのキャッシング機能に大きな問題があることがわかり，これを回避するために NIS を併用したシステムを構築した．

参考文献

[1] 倉前，島野，松本，亀島，ネットワーク型ソフト実験のための PC クラスタシステムの設計と構築，平成 11 年度情報処理教育研究集会講演論文集，文部省・東北大学，pp. 139–142, (1999).

[2] 島野，倉前，松本，亀島，ネットワーク型ソフト実験のためのネットワークシステムの設計と構築，平成 11 年度情報処理教育研究集会講演論文集，文部省・東北大学，pp. 143–146, (1999).

[3] A. Shimano and H. Kuramae, Design and Construction of Educational Computer System Using Self-mentenance System for Files and User Identification Agent, Proc. of 9th IEEE International Workshop on Robot and Human Interactive Communication, pp. 23–28, (2000).

[4] 例えば，http://www.samba.gr.jp/

[5] http://www1.infoeddy.ne.jp/ftk/selfmnt/

[6] 倉前，情報教育用 PC クラスタシステムの構築と経営工学科における計算力学教育，第 23 回 NCP 研究会・機械の強度と形態研究懇話会シンポジウム論文集，日本機械学会関西支部，pp. 21–23, (1999).