ディレクトリサービスを用いた教育用PCクラスタシステムの学生ユーザアカウント管理

倉前宏行，　島野顕継，　木村彰徳，
松本政秀，　亀島鉱二†

大阪工業大学工学部経営工学科において，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とPC-UNIXの２つのOS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，ユーザアカウントを情報センターと連携し，WindowsとUNIXを同じアカウントで利用できるようにした．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．

Management of User Account of PC Cluster System for Education using Directory Service

HIROYUKI KURAMAE, AKITSUGU SHIMANO, AKINORI KIMURA,
MASAHIDE MATSUMOTO and KOHJI KAMEJIMA†

The PC cluster system for education has been constructed in the Department of Industrial Management, Osaka Institute of Technology. Windows NT and PC-UNIX are installed in the client PC, and the environment where dual boot is possible in proportion to the utility form is constructed. In order to be able to seamlessly utilize with common facilites in the institute and to reduce labor on user management, the user account database is cooperated with information center. In addition, directory service is introduced and central management of the user accounts in the multiple OS is realized.

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するための演習教室として，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，学科専用のものであるため，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でき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，２つのOS (Operating System) 環境において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アカウントの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た．

さらに，2000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本システムとがシームレスに利用できるようシステムの変更を行った．本稿では，WindowsとUNIXの２つのOS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. ハードウェア構成

1999年９月より，本学科内には，図１に示すように，ネットワーク接続されたPC演習教室を２部屋設置している．経営情報システム実験室には，28台のデスクトップPC (富士通 FMV-6450DX3) を導入した．幅広

† 大阪工業大学
Osaka Institute of Technology
kuramae@dim.oit.ac.jp

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, 日本語 Solaris 7 Entire Distribution) および NT サーバ (富士通 FMV-6550TX3, Windows NT Server 4.0) 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 クライアントのファイルシステムを自動的にメンテナンスする．

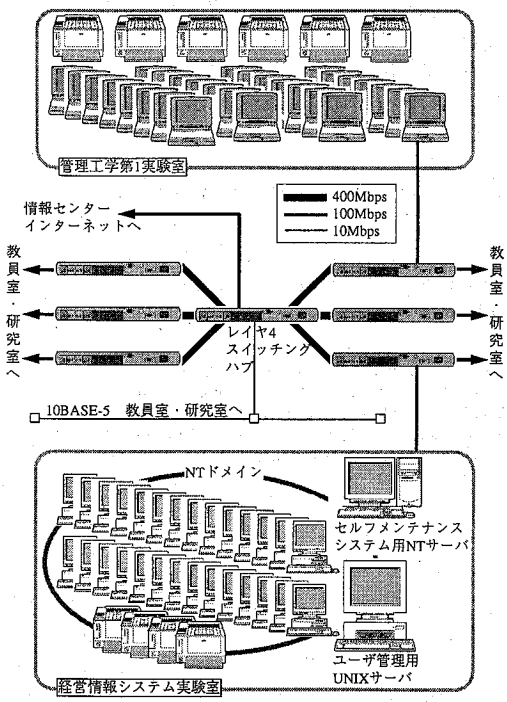

図 1　学科内 LAN と PC 演習室

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，本学科における少人数制の演習教育に利用している[6]．

3. ユーザアカウントの一元化

3.1 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 (Network Information Service) 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．

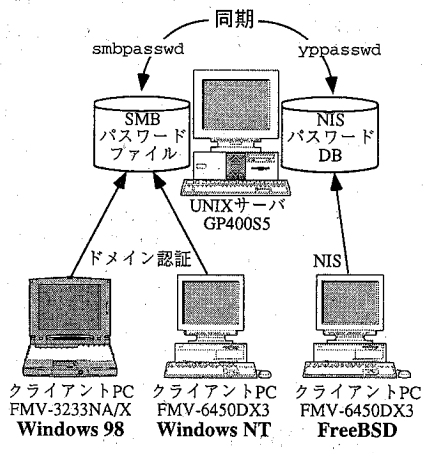

図 2　OS 混在環境におけるパスワードファイル

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一元化することは容易ではない．

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．

3.2 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利用のための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，情報センターで運用管理されているユーザアカウントデータベースを参照できるように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 スレーブサーバに設定し，UNIX のアカウントも連携させた．

FreeBSD には NIS，Windows NT には SMB と，パスワード情報が二重化されているため，ユーザがパスワード変更を行う際には，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

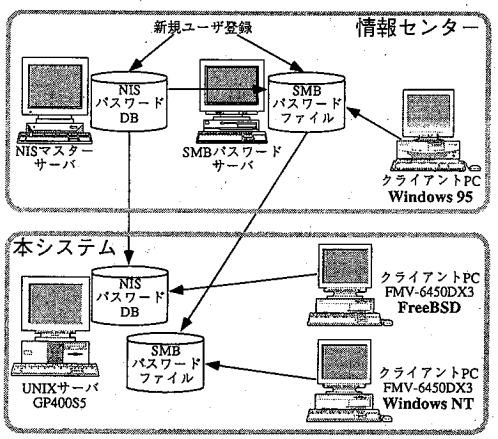

図3　情報センターと連携したユーザ認証方法

した．

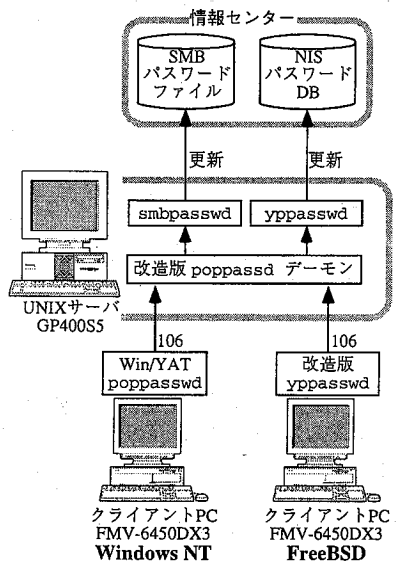

図4　2つのパスワードファイルの疑似一元化

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 poppassd コマンドを用いることにする．UNIX サーバが TCP (Transmission Control Protocol) の 106 番ポートでパスワード変更の要求を受け取ると，poppassd デーモンは smbpasswd コマンドを実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 コマンドも実行し，NIS データベースも同時に更新する．

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 デーモンを通じて同時に双方のパスワードファイルが更新されることから，2 つの OS のパスワードが疑似的に一元化できる．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．

4. ディレクトリサービスの導入

4.1 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，アカウント名，パスワード，ログインスクリプトなどをはじめとする 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．

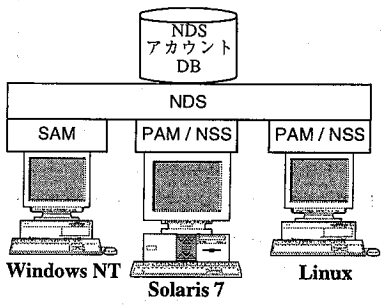

図6　NDS Corporate Edition の機能

4.2 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 7 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，NDS はクライアント機においてこれまで利用してきた FreeBSD に対応していないため，RedHat 6.2J (Linux 2.2.16) に

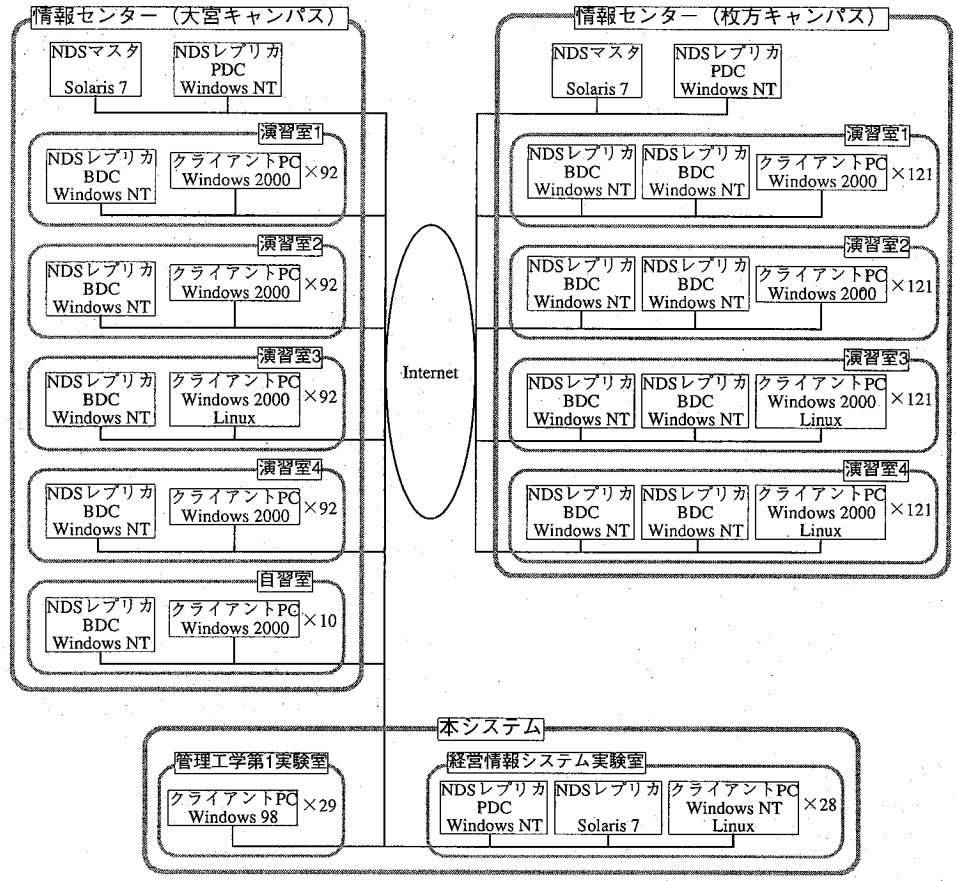

図5　NDS の全学的導入

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．

4.3 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，表 1 に示すように，大幅にレスポンスが低下した．同表は，1 台の Linux クライアント (他のクライアントは電源 OFF 状態) からパスワードを入力し GNOME (GNU Network Object Model Environment) デスクトップが起動するまでに要した時間，`ls -l` コマンドは所有者が全て異なるディレクトリ名を表示させるのに要した時間である．

表 1　NDS を導入した Linux 環境のレスポンス性能

	チューニング前	チューニング後
ログイン時間	3 分 15 秒	23 秒
`ls -l` (250 個)	3 分 45 秒	8.49 秒
`ls -l` (935 個)	2 時間 27 分 28 秒	1 分 19 秒
`ls -l` (8000 個)	N/A*	2 時間 33 分 30 秒

*一晩かかっても終了せず

NDS の性能を向上させるため，メーカ/ベンダの協力のもとユーザオブジェクトツリー上の検索経路に関するチューニングを行ったものの，同表に示すように `ls -l` コマンド実行時の NSS 参照性能を実用的なレベルへ改善することはできなかった．このレスポンス低下は，`ls -l`

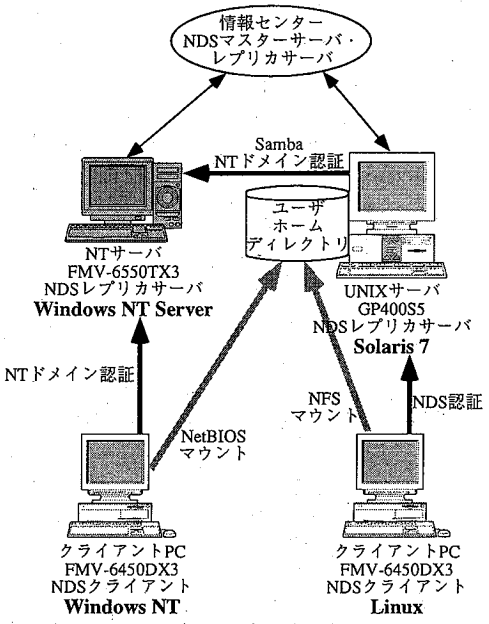

図7　NDS を用いたシステム構成

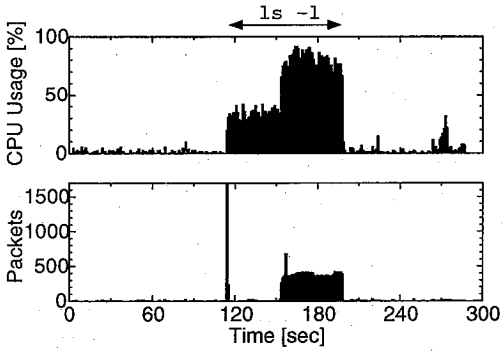

図8　Linux クライアント動作中のレプリカサーバとネットワークの負荷

や ps コマンドなどを実行した際，ファイル (ディレクトリ) やプロセスの所有者名・グループ名を NSS を経由して NDS へ参照する際に時間を要しているのが原因である．

NDS を導入した Linux 環境は，チューニングを施してもユーザ認証時や NSS 参照時にレプリカサーバに対して多大な負荷を及ぼしている．図 8 は，1 台の Linux クライアントにおいて 935 個のディレクトリ名表示の ls -l コマンドを実行した時のレプリカサーバの CPU 利用率と本演習室セグメント内のネットワークトラフィックを示している．同図より，たった 1 台のクライアントからの NSS 参照要求によってもレプリカサーバの CPU 利用率を大きく押し上げ，ネットワーク上には大量のパケットが連続的に流れることがわかる．図 9 は，この時のレ

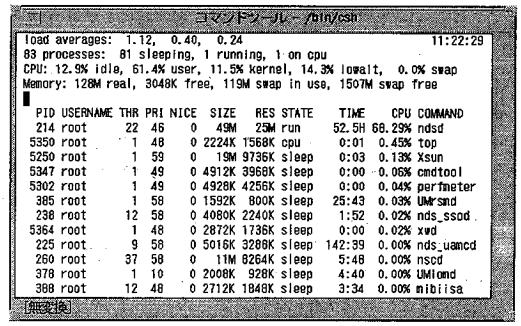

図9　NDS レプリカサーバの負荷状態

プリカサーバ内のプロセスの状態を表しており，これより NDS デーモン (ndsd) が 49MB ものメモリ空間および CPU 資源を占有していることがわかる．

図 8 に示した ls -l コマンド実行中において，レプリカサーバが送受信したネットワークパケットを採取し，通信相手先別に整理したところ表 2 のようになった．これより，Linux クライアントとレプリカサーバとの間で 4MB ものデータ転送が発生していること，さらに情報センターの演習室などのレプリカサーバとの間でも通信が行われていることがわかる．

以上のように，現時点での NDS は，20 数台の Linux クライアントで同時に使用するには，実用に耐えがたいものである．

4.4　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 10 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 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 11 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．

NDS と NIS とのユーザ情報の整合性を保ため，定期的 (1 日に 1 回) に NDS アカウントデータベースから NIS データベース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 のパスワードフィールドは変換することができず空となるが，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．むしろ，NIS データベースにパスワード情報が含まれない方がセキュリティの上で安全である．

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，表 3 に示すように十分に実用に耐えうるシステムとなり，レプリカサーバの負荷も下げることができた．

5. 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

表2　NSS参照時にレプリカサーバが送受信したネットワークパケット

相手先	レプリカサーバ→相手先			相手先→レプリカサーバ			パケット数小計	バイト数小計[Byte]
	パケット数	バイト数[Byte]	平均パケットサイズ[Byte]	パケット数	バイト数[Byte]	平均パケットサイズ[Byte]		
Linuxクライアント(NDS)	8,474	2,501,373	295	8,437	2,061,254	244	16,911	4,562,627
情報センター計算サーバ	57	20,672	363	45	8,972	199	102	29,644
情報センターレプリカ1	85	12,514	147	104	15,026	144	189	27,540
Linuxクライアント(NFS)	73	12,734	174	72	11,656	162	145	24,390
情報センターレプリカ2	19	6,940	365	20	3,622	181	39	10,562
演習室内NTレプリカサーバ	3	390	130	3	454	151	6	844
NTPサーバ	1	94	94	1	94	94	2	188
枚方情報センターレプリカ	1	64	64	1	64	64	2	128
合計	8,713	2,554,781		8,683	2,101,142		17,396	4,655,923

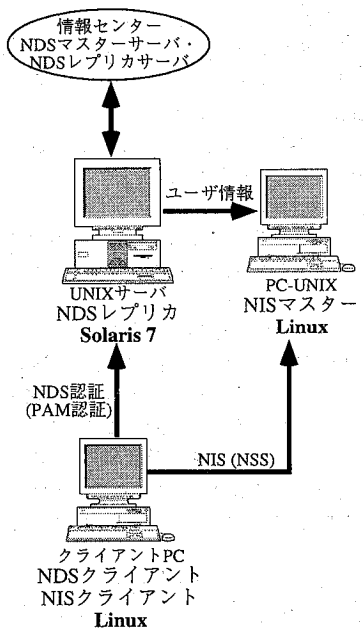

図10　NDSとNISの併用システム

表3　NISを併用したシステムのレスポンス性能

	NDSのみ	NISの併用
ログイン時間	23秒	18秒
250個のls -l	8.49秒	0.27秒
953個のls -l	1分19秒	1.19秒
8000個のls -l	2時間33分30秒	20.86秒

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結果，実用的なシステムが完成した．

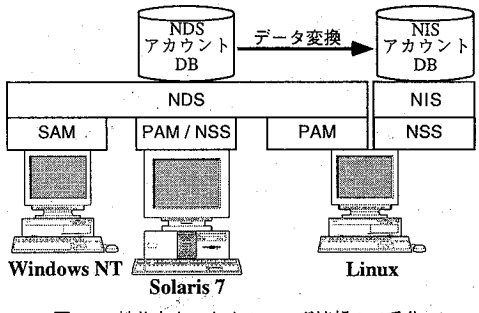

図11　性能向上のためのユーザ情報の二重化

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).