〈報 告〉

オープンソースソフトウェアによるさくらキャンパス計算機実習室のシステムの構築

奥野 浩*・西村 英俊**

Construction of PC room system using open-source software

Hiroshi OKUNO* and Hidetoshi NISHIMURA**

2006年4月さくらキャンパス計算機実習室はサーバおよびクライアントの機器の更新ため，新たなシステムを導入した．このレポートでは，新しいシステムを紹介する．

1. さくらキャンパスのネットワークにおける計算機実習室

1988年にこのキャンパスの移転時に設けられた計算機実習室は，実習上での利用のみならず，早い時点からその空時間を学生に開放していた．スタンドアローン状態から始まり，実習室のみで閉じたLAN，さらに，インターネットへの接続とその形態は変わっていったが，長い間，学生が自由に利用できるこのキャンパスの唯一の施設であった．2002年より，マルティメディア教室，コンピュータ実習室と環境が整えられ，また，学生に研究室等でサービスを提供する教員も増えたが，学生に対するサービスの大部分は，実習室のサーバを介在して行われている．このため，学生に対するサービスやセキュリティ上の管理と実習室のシステムは直結しており，さくらキャンパスのネットワークにとって重要なものとなっている．以前から，サーバOSとしてFreeBSD，さらに，Sambaによる認証とファイルサービス，およびSquidによるhttpプロキシと定評のあるオープンソース製品を利用してシステムを組んでいたが，今回更に，認証にデータを供給するOpenLDAP，ユーザ認証セキュリティ用にFreeRADIUS等を採用し，パフォーマンスと管理効率の向上と，環境の変化に柔軟に対応できるシステムを目指した．

* 医学部数学研究室
Department of Mathematics, School of Medicine
** 情報科学研究室
Information Science

2. 以前のシステムからの主な変更点

以前のシステムでの一番の問題は，認証におけるパフォーマンスの不足で，実習開始時のように，多くのクライアントが同時にログオンすると処理に遅延がおきることがあった．これは，ドメインコントローラ上の認証データベースsambapasswdが低効率であることが原因と考えられる．このため，今回はバックエンドの認証データベースとして，LDAPを採用しこの問題に対応することとした．また，このLDAPの情報を利用して，以前はそれぞれのサーバが独自に認証していたのを一元化し管理の手間を省けるように考えた．また，今後のユーザの要求への対応の準備として，ウェッブメール，学内ネットワークでの学生ノートパソコンの接続等の利用環境を整備した．

3. システムの概要

実習室のシステムは，82台のクライアントと4台のサーバほかプリンタ，ビデオプロジェクタ等の周辺機器からなっている．

82台のクライアント（富士通　FMV−K5210 Pentium−M740 2 GB メモリ，40 GB ハードディスク，DVD−ROM & CD−R/RW ドライブ　17インチディスプレイ）は，液晶一体化の WindowsXP Professional SP2 を OS とする機械で，1台を教師用，1台をビデオプロジェクタ用，残りの60台を学生実習用，また，20台を補助室のパソコンルームに割り当てている．管理や設置面積の少ない一体型で，消費電力量の少ない CPU を搭載したものを採用した．学生はローカルマシンにアカウントを持たなく，ドメインユーザとしてのみログオンできる．また，指定された領域にあるプログラム以外を実行できないようにすることにより，誤操作による障害の発生や，ウィルスの感染等の危険性を小さくしている．一方，各学生は，クライアント上で様々な環境設定ができ，あるクライアント上で設定した環境が，他の端末でも有効になるように移動プロファイルを利用している．実習室と同時に更新したパソコンルームにおいても，ハードウェアソフトウェアを実習室と共通し，移動プロファイルにより，ほぼ同等に扱えるようになっている．

プリンタは，ネットワーク上に直結されているが，クライアントからはサーバ（FS）を通してのみアクセスでき，IP アドレスによるアクセス制限や個人の利用状況の掌握ができるようにしている．

システムのサーバ群は，4 台のサーバからなっている．すべて消費電力量の少ない CPU 搭載のものになっている．3 台はブレードサーバ（NEC Express5800/11Ba−e3　Pentium−MULV733　1 GB メモリ，40 GB ハードディスク）で，残りの 1 台はファイルサービスを行うためディスク容量のあるラックサーバ（NEC　Express5800/i110Ra−1h Pentium−M　1.73 GHz　1 GB メモリ，500 GB ハードディスク）になっている．

ラックサーバ（ホスト名　FS）は，Samba をイントールしてドメインコントローラとファイルサービスを提供している．ユーザプロファイル等の機能もこのサーバが提供している．

ドメイン内のサーバにユーザアカウント情報を与えるデータベースとしては，今回 LDAP を使った．このため，ブレードサーバの一台（ホスト名　LDAP）に OpenLDAP をインストールし，ほかのサーバはこのアカウント情報利用ように設定した．

さらに，実習室，パソコンルームのみならず，学生が http でアクセスするとき，認証し，また，Web の効率のよい閲覧ができるように，Squid を一台（ホスト名　Squid.student）にインストールした．このサーバはさくらキャンパス全体のキャッシュサーバを通して外部ネットワークと接続している．

最後の一台は，メールサーバ（ホスト名 Compserv）で，学生全員のメールの管理を行っている．このサーバもキャンパス全体のメールサーバを経由して外部ネットワークに接続している．また，将来外部ネットワークからのアクセスの便を考えて，Web メールサーバソフト squirrelmail や ML 管理ソフト fml をインストールしている．

4.　サーバの設定

サーバはすべて OS として，FreeBSD5.4−RELEASE を使った．インストール時に内蔵のネットワークインターフェイスが認識されなかったので，メーカー[3)5)]のサイトを参考にしてドライバにパッチをあてて稼働するようにした．また，それぞれのマシンでは，時刻設定プログラム ntpd をクライアントとして動かし，さくらキャンパスネットワーク上の NTP サーバに定期的にアクセスして時刻の同期をとるようにしている．OS のネットワーク等の基本的な設定については説明を省略する．その他のアプリケーション等の個別の設定は次のようになっている．

4.1　FS

旧システムからの移行のため，スポーツ健康科学部の 2 年生以上に関しては，このサーバにユーザとして登録したが，新入生については，Samba を通してのみアクセスできる．これによってセキュリティを向上させた．

4.1.1　SAMBA（samba−3.0.20b）の設定[7)]

ドメインのログオン時の認証はLDAPを通して行うため，ソースをダウンロードし，コンパイルオプションで，LDAPサポートを有効にしてコンパイルする必要があった．また，quotas（ユーザの使用容量の制限機能）とacl-support（ファイルのアクセス管理機能）オプションも同時に有効にし，将来に備えた．さらに設定ファイル/usr/local/samba/lib/smb.confで以下の設定をおこなう（デフォルトと異なる部分のみを記述した．）

Ⓐ　PDCとしての設定

Sambaによるドメイン環境を構築するための設定．

domain logons＝Yes

Workgroup＝STUDENT

ホスト名も設定した．

Ⓑ　LDAPの使用のための設定[8)]

認証用のデータベースとしてLDAPサーバ上のデータを使うため以下のパラメータを設定した．

passwdb backend＝ldapsam

ldap admin dn

ldap suffix

ldap user suffix

ldap group suffix

ldap machine suffix

ldap ssl

Ⓒ　共有homesの設定

個々の学生用にネットワークドライブを設定した．これにより，各学生はどのクライアントからでも常にこの共有にアクセスできるようになる．また，このディレクトリと，UNIX上のリンクを使い，ファイルの配布回収を行える．

Ⓓ　共有netlogonの設定

startup.bat，logon.bat，logoff.bat，shutdown.batというファイルを用意して，接続情報の管理のためのログをとっている．

Ⓔ　移動プロファイルのための設定

個人設定の記録し，各ユーザがそれぞれの設定を各クライアントで常に同じ環境で利用できるようにした．

logon path ¥¥%L¥JunProfiles

学生の不用意なアクセスよるファイルの破壊をさけるため，移動プロファイル専用のディレクトリを準備した．

Ⓕ　printer共有の設定

実習における使用を考え，実習室のクライアントだけからアクセスできるようにした．

Ⓖ　共有ディレクトリpublicおよびcommonの設定

学生に対するファイルの提供用や管理用作業用に共有ディレクトリを準備した．

4.1.2　NFSの設定

学生のディレクトリの一部をhttpで公開できるように，webサーバ（compserv）からマウントできるように設定した．

4.2　LDAP

サーバ内部のユーザはほぼ管理者のみに限定し，セキュリティ対策としている．ネットワーク上での位置を工夫して，サーバのみからアクセスできるようにした．LDIF形式のファイルを作成し，アカウント情報をLDAPに登録した．

4.2.1　OpenLDAP（ver.2.2.23）の設定[8)]

FreeBSDのパッケージよりインストールして，slapd.confで次を設定する．

samba用スキーマファイル（samba.schema）の読み込み

ディレクトリサービスのベースDNの指定

rootpwの設定

現在は，学生用の認証情報を扱っている．将来的には，接続する端末や教員の情報も格納し，さくらキャンパスのネットワーク全体の認証情報の一元化を考えている．

4.2.2　FreeRADIUS（ver.1.0.2）の設定

FreeBSDのportsを利用してインストールした．キャンパス内に持ち込まれた機器をネットワークに接続するときのユーザ認証の準備として用意している．

4.3　compserv

学生用メールサーバ．PAMを使いOS上のユーザは管理者のみになっている．

4.3.1　sendmail（ver.8.13.3）の設定

smtpサーバとして設定する．

4.3.2　DNS サーバとしての設定（bind9.3.1）

学生用サブドメイン student.sakura.juntendo.ac.jp の管理用に設定する．これにより，このサブネット内のコンピュータに DNS のサービスを提供する．

4.3.3　apache（ver2.1）

FreeBSD のパッケージよりインストールした．また，関連プログラムの PHP5 等は，FreeBSD の ports よりインストールした．学生の web ページ作成の実習に利用している．

4.3.4　fml（ver.4.0.3）[1)]

ソースファイル[2)]をダウンロードし，コンパイルして，インストールした．メーリングリスト管理プログラム．現在，2 つのメーリングリストを試用中．

4.3.5　GNU mail-utils（ver.1.0）

ソースファイル[6)]をダウンロードしてインストールした．pop および imap に使用する．/etc/inted.conf でこれらのプログラムを使用するように設定する．/usr/local/etc/mailutil.rc に PAM を使う設定とログの設定を行う．

4.3.6　PAM

ディレクトリ / etc / pam.d に PAM を通して LDAP の認証情報使うプロトコルについて設定する．今回は，login, passward, pop, imap について設定した．

4.3.7　squirrelmail（ver.1.9.5）

FreeBSD のパッケージよりインストールした．将来，外部ネットワークからのメールサーバへのアクセスを考え，Web メールへの対応のため準備した．

4.4　stud-squid

squid（ver.2.5−stable12）を FreeBSD のパッケージが古かったので，ソースファイル6）をダウンロードしてインストールした．Web プロキシとして，標準的な設定をした．

5.　クライアントの設定

5.1　BIOS の設定

起動ドライブを制限した．また，BIOS 設定メニューへのアクセスに対してパスワードを設定した．

5.2　ローカルユーザの設定

クライアントの管理用ユーザを作成する．

5.3　レジストリの設定

ドメインユーザは，ローカルなハードディスクをデータのキャッシュとしてしか書込めないようにした．また，ある領域にあるプログラム以外は起動できないように設定した．

設定したクライアントから，グループポリシーファイルをコピーし，ネット上におき，それぞれのクライアントにローカルユーザとしてログオンし，ネットからグループポリシーファイルをコピーすることにより設定した．

5.3　プリンタの設定

ドメインユーザの場合，プリンタの設定はここのユーザで必要になる．各ユーザごとに，プリンタのインストールを行った．

6.　現在のシステムの評価と今後の課題

LDAP によるバックエンドデータベースの利用により，前のシステムに見られた遅延はまったく見られなくなった．また，実習室おいてアカウントの一元管理に成功した．以前よりサーバの数が減った上にラック一個にまとまり，それぞれのサーバ上でユーザ管理をほとんど必要なくなって管理省力化が進んだ．クライアントの設定に関しても不完全ではあるが，グループポリシーの利用により，設定が楽になった．さらに，ユーザの個人設定に関する重要なファイルを隠蔽できたので，安全性が高まった．

今後の課題としては以下のようなことが挙げられる．

○LDAP サーバの二重化

LDAP サーバに障害が起きると，システム全体が機能しなくなる．耐障害性を高めるため，二重化が必要である．

○教職員を含めたさくらキャンパス全体のアカウントの一元管理

キャンパス全体を効率良く管理できるようにするため，一元管理が必要である．

○RADIUS によるネットワーク接続時のユーザ認証の管理

学内のさまざまな要望に応じるため，ユーザ認証の管理が必要である．

文　献

1） 深町賢一（2001）*fml* バイブル　東京　オライリー・ジャパン
2） FML.ORG　http://www.fml.org
3） Intel　http://downloadfinder.intel.com/scripts-df-external/File_Filter.aspx?FileName＝em-
4） ミラクルリナックス　http://www.miraclelinux.com/technet/document/samba/pdf/samba0010.pdf
5） NEC　http://www.express.nec.co.jp/products/i/i110Ra-1h_FBSD54.html
6） Ring Server Project　ftp://ftp.ring.gr.jp
7） 高橋基信（2005）*Samba* のすべて　東京　翔泳社
8） 武田保真（2004）*徹底解説 Samba LDAP* サーバ構築　東京　技術評論社

（平成18年10月10日　受付
平成18年12月12日　受理）