筑波大学技術報告
26: 60-66 , 2006

# 情報システムの管理と運用

川上彰、和田勉、山形朝義
筑波大学システム情報工学等支援室（情報システム管理班）
〒305-8573 茨城県つくば市天王台 1-1-1

## 概要

平成１６年度からシステム情報工学等支援室の技術職員は、「情報システム管理班」、「情報アプリケーション班」、「装置開発班」の３班からなる新体制となった。この中の「情報システム管理班」の担当者が行っている業務等について、その一部ではあるが紹介を兼ねて報告する。

今回は、主に以下の３点を中心に、成果及び経過について報告する。

- 無線 LAN システムの改善
- 社会工学類教育用計算機システムの運用
- LDAP によるユーザ認証

## １．はじめに

「無線 LAN システムの改善」については、主に無線 LAN のセキュリティを中心に、その構築までの過程とテストの結果について報告する。

また、「社会工学類教育用計算機システムの運用」については、システムの紹介と、その中の Windows 環境の管理方法を中心に報告する。

３つ目の「LDAP によるユーザ認証」では、昨年度の技術発表会で報告した、システム情報工学研究科経営政策科学専攻における LDAP(Lightweight Directory Access Protocol)を使った認証を、今年度は社会工学類へも対象を広げるとともに実際に運用する上での問題点等について検討した。

## ２．無線 LAN システムの改善

現在管理している２系統の無線 LAN は、系統毎にネットワーク管理組織及び建物が別ではあるが、実際一部のユーザは両方の無線 LAN を利用している。このため利用者から、認証を１つにしてもらいたいとの要望があり、システムの改善を行ったので簡単に報告する。無線 LAN システムの移行にあたって先ずテストシステムを構築し、成功を確認してから本システムの移行を行う予定である。

### 2.1　現在の無線 LAN 構成

図１－１で示すように、系統AはLinuxマシンをゲートウエイとして五つのAP(Access Point) が接続されており、利用時の認証はRADIUS(Remote Authentication DialIn User Service) を使ったMAC(Media Access Control address)アドレス認証と、APの機能を利用した１２８ビットのWEP(Wired Equivalent Privacy)キーを使っている。もうひとつの系統Bは FreeBSDマシンをゲートウエイとして、九つのAPが接続されており、利用時の認証はユーザ名とパスワードを入力するOpengate(ネットワーク利用認証ゲートウエイ)[1]システムと、APの機能を利用した１２８ビットのWEPキーを使っている。それぞれ利用申請によって、前者はMACアドレスの追加を、後者はユーザ登録の追加を行っている。

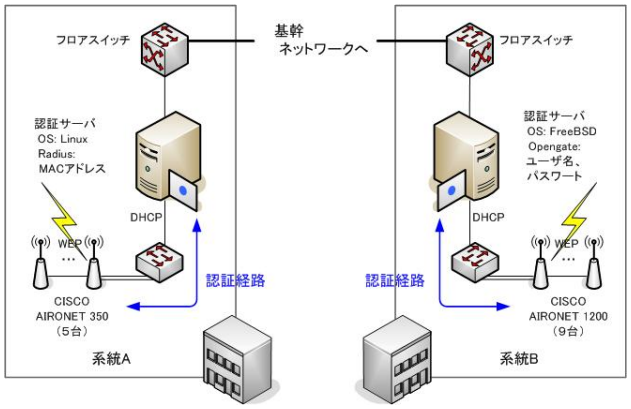


図１－１　改善前の構成

### 2.2　改善後の無線 LAN 構成

考慮した点として、認証を１つにまとめること、通信のセキュリティ強化を図ること、現在の機器を利用することが考えられ、いくつかの機能の中から、電子証明書を利用した RADIUS を使って１台のサーバで管理が可能であることに注目し、EAP-TLS(Extensible Authentication Protocol - Transport Layer Security)認証と RADIUS プロキシー機能を利用した。図１－２で示すように各 RADIUS プロキシーサーバは認証サーバに認証を委ねる。この機能によって２系統の無線 LAN 認証を１台の認証サーバで行うことが出来る。

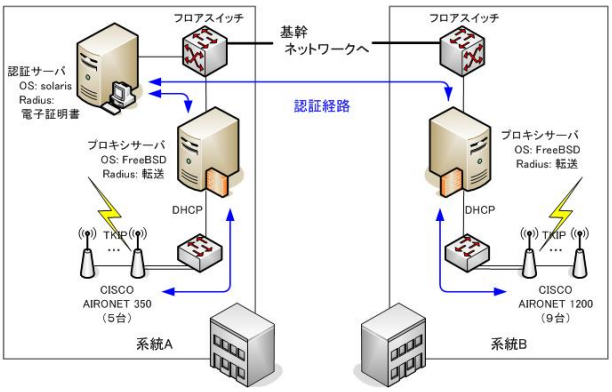


図１－２　改善後の構成

[1] http://www.cc.saga-u.ac.jp/opengate/

## 2.3　システムの設定

以下に各システムの設定において重要と思われる設定項目を記述する。

### 2.3.1 プロキシーサーバ

プロキシーサーバに必要な、DHCP(Dynamic Host Configuration Protocol)と FreeRADIUS のインストールは FreeBSD の PORTS 機能を利用した。ゲートウエイ機能については予め動作していることを前提にしているので省略する。

```
DHCP 関連ファイル（系統 B）
dhcpd.conf:
   default-lease-time 600;
   max-lease-time 7200;
   ddns-update-style none;
   #ddns-updates off;
   log-facility local7;
   option domain-name "sie.tsukuba.ac.jp";
   option domain-name-servers sv.sie.tsukuba.ac.jp;
   subnet 192.168.1.0 netmask 255.255.255.0 {
        range 192.168.1.1 192.168.1.63;
        option broadcast-address 192.168.1.255;
        option subnet-mask       255.255.255.0;
        option routers           192.168.1.254;
        }
   subnet 130.158.xx.0 netmask 255.255.255.0 {
        }

RADIUS 関連ファイル
clients.conf:（AP の情報）
    client 192.168.1.220 {
        secret = AP の設定と同じ
        shortname = an1200-1
        nastype = other
}
proxy.conf
   realm NULL {
        type        = radius
        authhost =  認証サーバ IP アドレス:1812
        accthost =  認証サーバ IP アドレス:1813
        secret     =  認証サーバの設定と同じ
        }
```

### 2.3.2 認証サーバ

FreeRADIUS のインストール：

既に稼動している UNIX マシンの Solaris9 に freeradius-1.0.5　を make install した。Makefile を作るための configure 文は以下の様に書いた。

```
configure --prefix=/usr/local/freeradius ¥
  --disable-shared ¥
  --with-openssl-includes=/usr/local/ssl/include ¥
  --with-openssl-libraries=/usr/local/ssl/lib
```

これで出来上がった Make ファイルを make すればよい。

```
RADIUS 関連ファイル
users:
   "an1200-1"          Auth-Type := EAP
clients.conf:（プロキシーサーバの情報）
   client 130.158.aa.bb {
        secret =  プロキシーサーバの設定と同じ
        shortname = yama-bsd
        }
   client 130.158.cc.dd {
        .
        .
        }
eap.conf:
   default_eap_type = tls
   tls {
        private_key_password =  サーバ証明書の秘密
                                鍵のパスフレーズ
        private_key_file=/usr/local/etc/1x/cert-srv.pem
        certificate_file=/usr/local/etc/1x/cert-srv.pem
        CA_file = /usr/local/etc/1x/root.pem
        dh_file = /usr/local/etc/1x/DH
        random_file = /usr/local/etc/1x/random
        check_crl = no
        }
proxy.conf:
      realm NULL {
        type                = radius
        authhost            = LOCAL
        accthost            = LOCAL
        }
/etc/services:
        radius      1812/udp
        radacct     1813/udp
```

以上で FreeRADIUS が EAP-TLS を利用できる状態になった。

OpenSSL による、証明書の作成：

OpenSSL についても予め動作していることを前提にしているので省略する。ディレクトリ内で（このシステムでは/usr/local/ssl/radius/misc とした）ルート証明書(root)、サーバ証明書(cert-srv)、クライアント証明書(cert-clt)を作成する。事前に EAP/TLS に必要な OID(Object IDentifier)を置く必要があったので、以下の xpextensions ファイルを作成する。

```
xpextensions:
   [ xpclient_ext ]
   extendedKeyUsage = 1.3.6.1.5.5.7.3.2
   [ xpserver_ext ]
   extendedKeyUsage = 1.3.6.1.5.5.7.3.1
```

次に、eap.conf で指定した証明書を置くためのディレクトリを作成する。

```
   #mkdir /usr/local/etc/1x
   #chmod o-r /usr/local/etc/1x
```

それにランダムファイルを作成する。

#date > /usr/local/etc/1x/DH
#date > /usr/local/etc/1x/random

前述 OID の場所で、３つの証明書を作るスクリプトを別途作成し（ここでは省略）実行した。出来上がった証明書を、/usr/local/etc/1x/以下に配置した。

例）当初の無線クライアント１台の場合
# ls -l /usr/local/etc/1x
-rw-r--r--1 root other DH
-r--------1 root other cert-clt.pem
-r--------1 root other cert-srv.pem
-rw-r--r--1 root other random
-r--------1 root other root.pem

以上の作業完了後 FreeRADIUS を起動する。

### 2.3.3 アクセスポイント

ここでは CISCO AIRONET 1200 について報告する。
設定するにはアクセスポイント（AP）に有線で接続したパソコンの Web 設定画面を使って、AP の管理者権限で設定する。重要と思われる箇所を以下に記述する。

Security: Server Manager:
Current Server List: RADIUS
Server: プロキシーサーバの IP アドレス
Shared Secret: プロキシーサーバの設定と同じ
Authentication Port: 1812
Accounting Port: 1813
EAP Authentication Priority 1: プロキシーサーバの IP アドレス

Security: Encryption Manager:
WEP Encryption: Mandatory
Cipher: TKIP
Broadcast Key Rotation interval: Enable Rotation with interval 3600

Security SSID Manager:
SSID: siewave2（任意の名前）
Open Authentication: with EAP
Network EAP: NO ADDITION (要らないかも）
EAP Authentication Servers Customize Priority1: プロキシーサーバの IP アドレス
Key Management: Mandatory , WPA

Accounting Settings:
Enable Accounting
Accounting Server Priorities: Customize Priority 1: プロキシーサーバの IP アドレス
Set Guest Mode SSID: siewave2（任意の名前）

以上の設定で動作した。

### 2.3.4 無線 LAN クライアント PC

無線ネットワークの設定と、証明書のインストールを以下の要領で行う。

Windows XP のセットアップ：
ワイヤレスネットワーク接続プロパティにて、ネットワーク認証を「WPA」、データの暗号化を「TKIP」と選択する。次に認証タブにて「このネットワークで IEEE802.1X 認証を有効にする」を有効に、EAP の種類を「スマートカードまたはその他の証明書」を選択、「コンピュータの情報が利用できるときは…」を有効にする。

証明書のインストール：
認証サーバの証明書を作るスクリプトを実行後、２つの証明書（root.der 、cert-clt.p12）をクライアント PC にインストールする。

１）ルート証明書（root.der）
USB メモリー等にコピーした root.der をダブルクリックし、「証明書のインストール」から「証明書をすべて次のストアに配置する」を選択、参照ボタンをクリックし「信頼されたルート証明機関」を選択後、OK ボタンを押す。後は完了まで進む。

２）クライアント証明書（cert-clt.p12）
同じく cert-clt.p12 をダブルクリックし、証明書のインポートウイザードから「秘密キーのパスワードを入力…」に対してサーバ証明書の秘密鍵のパスフレーズを入力する。最後に「証明書の種類に基づいて、自動的に証明書ストアを…」を選択してから完了まで進む。

## 2.4 作業を終えて

当初、Solaris９に freeradius-1.0.4 をインストールしたが、EAP-TLS モジュールがうまく組み込まれていないため、モジュールの Makefile を手で修正した。現在のバージョンでは問題は出なかった。それと xpextensions にある数字の間になぜか余計なブランクが入ってしまい認証動作に失敗した。これに気づくまでにかなり（無駄な）時間をかけてしまった。

## ３．社会工学類計算機システムの運用について

現在、社会工学類計算機システムでは社会工学類、システム情報工学研究科社会システム専攻、経営政策科学研究科等に所属する学生及び教職員に対して各種サービスの提供を行っており、このシステム環境の利用者として登録管理されているユーザアカウント数は、平成 17 年 10 月現在では 1 千ユーザを超える状況となっている。

われわれ技術職員はこの計算機システムの登録ユーザに対し、使用するシステム環境や周辺機器についての障害が起きないように、あるいは障害が起きてもその障害の波及範囲を最小限に止めかつ迅速にその障害を取り除くように、システムの利用状況を管理し適正な運用を行うことが業務となる。また、この計算機システムの利用目的は、主に学類等教育用として講義や演習・実習などを行う際に、利用度の高い教育用資源として活用されることが大きな役割の一つとして挙げられることから、一般的な計算機システムの管理運用といった面からだけではなく、これらを含む資源が有効に機能できるように計算機システム以外での教育環境の整備や、人員削減等による実作業時の増大における作業の効率化といった面においても、われわれ技術職員が日ごろから色々な形で改善に取り組んでいる中の 1 部を紹介する。

### 3.1　社会工学類計算機システム構成

社会工学類計算機システムは、レンタル制度により４年または５年に 1 度リプレースをされている。現在のシステムは、平成 12 年度に導入されたもので以下のような機器構成となっている。

①Unix メール・ファイルサーバ×１
②Unix 計算サーバ×１
③Windows ネットワークサーバ×１
④Windows ファイルサーバ×１
⑤Windows クライアント×９０
⑥Macintosh クライアント×４５
⑦ユーザデータのバックアップ装置（UNIX 用×１、Windows 用×１）
⑧プリンター装置（高速×３、中速×３）
⑨プロッター装置×１
⑩大型スキャナー読込装置×１

### 3.2　システム環境の管理･メンテナンス

#### 3.2.1 Windows マシンのシステム更新作業

現在クライアント用 Windows マシン（Windows 2000 Professional）が 90 台設置されており、これらマシン群の OS や各種アプリケーションソフトウェア等についての更新作業を行う際には、図２－１にあるようにシステム配布用サーバを用いて作業が行われている。この配布用サーバで行われる作業には、PC 管理システム用ソフト「Symantec Ghost v7.5」を用いて行われており、あらかじめシステム更新の雛形マシン上に構築しておいたシステム環境の内容をネットワーク経由により、配布用サーバ上にクライアントマシンに配布するためのシステムイメージファイルとして作成保存する。また、実際にクライアントマシンへの配布作業を行う場合、講義等での利用時間帯を避けて一般ユーザにも事前にこの作業予定を掲示して実施される。

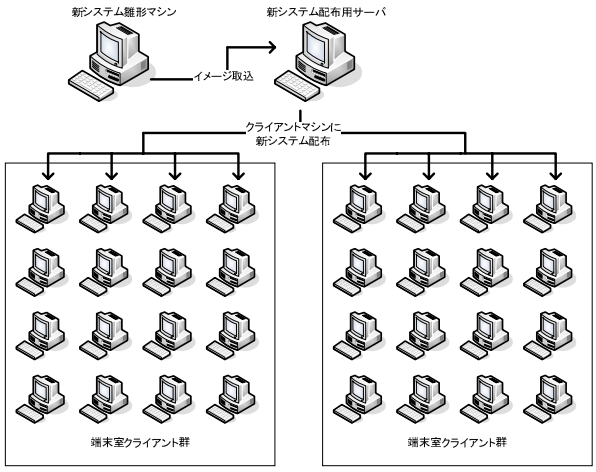


図２－１　システム更新作業の流れ

実際の配布用サーバからクライアントマシンへのシステム配布作業では、図２－２にある Ghost コンソール画面の操作によって処理を行う。

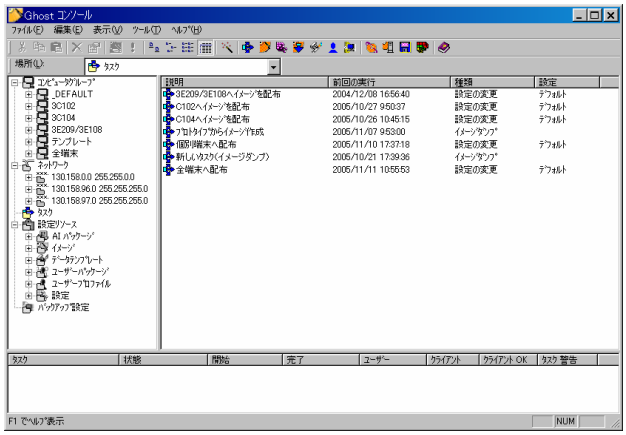


図２－２　Ghost コンソール画面

現在システム配布作業の処理形態については、全端末（90 台）、端末室１（45 台）、端末室２（45 台）、個別端末（1 台）の４形態を設定し、それぞれの処理内容について実行できるように登録されている。

システム配布用サーバから更新用システムの配布処理が実行されると、クライアントマシンのハードディスクに保存されている Ghost ブート機能によりクライアントマシン本体が再起動され、Ghost のリストア機能が実行され図２－３の画面を表示し、システムの更新処理の進捗状況が分かる。

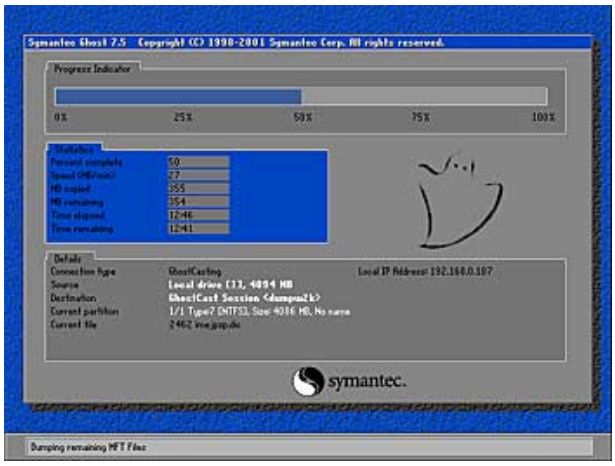


図２－３　Ghost コンソール クライアント画面

### 3.2.2 ジョブのプリントアウト

社会工学類計算機システムでは、３部屋の端末室にそれぞれプリンタ装置がネットワーク接続で常設されており、ユーザはどのプリンタに対しても出力できる環境となっている。各プリンタの稼動状況については、図２－４のように WEB 画面からリアルタイムで状況把握ができ、消耗品補給や故障状況の確認ができる。

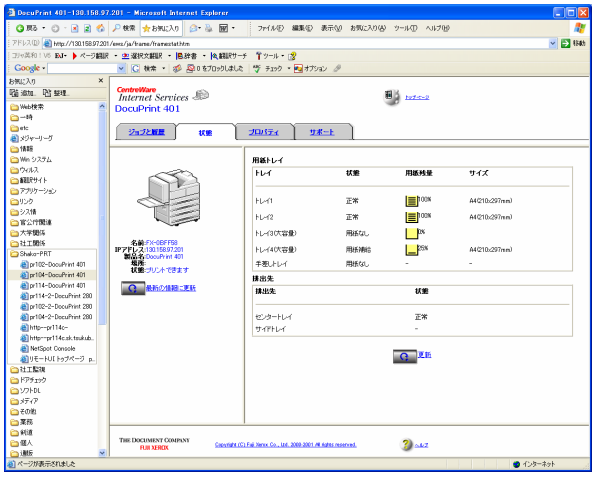


図２－４　プリンタ装置ＷＥＢモニタ画面

## 3.3 業務内容の見直しと作業改善

システム管理班では、平成 17 年３月に技術職員１名の削減が行われため、4 月からの社会工学類計算機システムの業務内容の見直しをしながら以下の改善策を講じて作業の効率化を行っている。

### 3.3.1 Windows システム作業

①作業手順のマニュアル化

作業内容についてできるだけ判り易いものとなるように、具体的な文章や写真などで工夫してマニュアルを作成した。

②作業内容のドキュメント化

実施したシステム作業の内容について、各種作業で行われた内容を記録データとして残し、過去に実施された作業内容については、詳細に確認できるようにした。

③システム環境のドキュメント化

計算機システムとして設置されている機器についての、それぞれの個別データ（製造番号、IP アドレス、Mac アドレス、Windows サーバ登録情報、端末室配置図、修理履歴状況）の履歴簿を作成した。

### 3.3.2 プリントログの管理

Windows サーバでは、設置プリンタから出力されるアウトプットジョブについて、毎日プリンタ別に全出力ジョブのログが保存されるので、そのログファイルから図２－５にあるように簡単な集計処理を行い、大量出力を行ったユーザを確認してメールによりその出力内容と使用目的を報告させ、資源の有効利用と無駄使い防止の指導を行う。表１は、４月から管理を行った９ヶ月間の前年度との比較を表している。

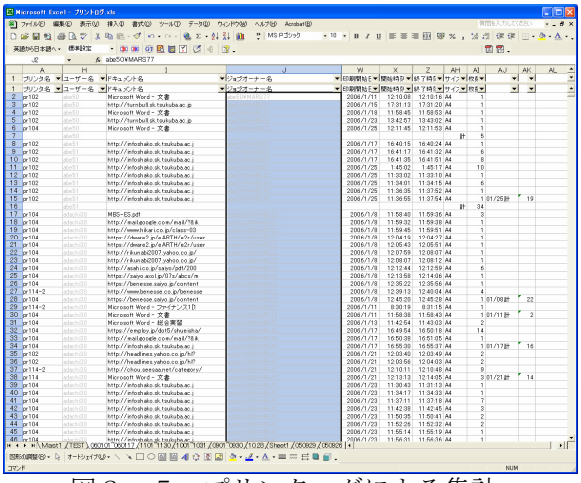


図２－５　プリンタログによる集計

表１　月別プリントアウト集計（2006-01-17 現在）

| | ４月 | ５月 | ６月 | ７月 | ８月 | ９月 | 10 月 | 11 月 | 12 月 | １月 | ２月 | ３月 | 合計 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2004 年度 | 44,837 | 66,960 | 82,965 | 39,929 | 17,996 | 41,936 | 111,774 | 60,391 | 55,393 | 70,673 | 51,216 | 27,172 | 671,242 |
| 2005 年度 | 44,316 | 53,742 | 63,954 | 26,100 | 16,419 | 36,853 | 42,711 | 27,562 | 41,899 | 18,633 | - | - | 388,065 |
| 前年比(%) | 98.8% | 80.3% | 77.1% | 65.4% | 91.2% | 87.9% | 38.2% | 45.6% | 75.6% | | | | |

## ４．LDAP によるユーザ認証

昨年度に構築した LDAP 認証環境を一部変更し、更に規模を拡張して図３－１に示すような環境を構築した。今回は、新たな機能追加に加えて、規模の拡張に伴って発生する問題点等について報告する。

規模を拡張するにあたっては、社会工学類の教育用システムにも LDAP 環境が適用できないか検討した。

### 4.1 ActiveDirectory と OpenLDAP の統合

社会工学類の教育用のシステムでは、ActiveDirectory 機能を使って Windows のドメイン管理を行っている。これと OpenLDAP の認証環境を一元化するためには幾つかの方法が考えられるが、以下のような２つ方法について検討した。

(1) ActiveDirectory による管理をやめて、新たに Samba サーバをドメインコントローラとし NT ドメイン環境を構築する。
(2) 市販されているソフトウェアを使って統合する。

(1) の方法は、既に経営政策科学専攻で使用しており、大きな問題は発生していない。しかし、大規模な Windows 環境の場合、Samba によるドメイン管理には限界があるように思われる。本来 Windows 管理で使える環境やツールが使用できない等の制約が発生することに加え、今後新たな機能の追加や変更等があった場合、問題が発生することも懸念される。

(2) の方法は、統合のためのソフトウェアとして幾つかの物が市販されているようであるが、何れも導入のためには高額な費用が必要となる。また、ユーザ認証で使用するパスワード変更には、通常の方法とは異なり、特定の WEB ページにアクセスして変更する必要がある等、ソフトウェアによって通常の環境とは異なった使用方法を強いられる場合があるようである。

以上のことから、社会工学類教育用計算機の認証に LDAP を使用することは今回は見送り、試験的に (1) の Samba による Windows ドメイン環境を構築し動作を確認することとした。

当初、社会工学類と経営政策科学専攻で別々の Windows ドメインを構築し、両者で同じ LDAP データベースを使ってユーザ認証の一元化を行うことを目標とした。Samba 環境の構築のためには smbldap-tools を使用した。この環境では各ユーザの情報は LDAP データベース内で多くの属性と値を持っている。その中に SID（Security IDentifier）という Windows ドメイン固有の ID 情報が含まれる。そのため複数の Windows ドメインで、個人の情報を共有して利用しようとすると各々のドメインの SID が異なるため利用できない。また、ユーザのプロファイルや Windows のホームディレクトリの場所も固定されてしまうため、不都合な場合もある

SID はユーザのレジストリ内にも含まれるようで、この面でも問題になる可能性がある。ActiveDirectory ドメインについては未確認であるが、今回使用した Samba による NT ドメイン環境を構築した場合は、異なるドメイン間でユーザ認証の一元化を LDAP データベースで行うことはできなかった。異なる Windows ドメイン間で、LDAP を使ってユーザ認証の一元化を行うためには、別な方法を検討する必要がある。

### 4.2 LDAP に対応したソフトウェアの導入

昨年度は、WEB アクセス、ログイン、ftp 接続、無線 LAN 等の利用に LDAP の認証が利用できることを確認した。今回は更にメール環境等について調査した。メールサーバとしては exim4 を、pop，imap 環境として Courier-pop および Courier-imap を使用した。WEB メールとしては、Squirrelmail を、メーリングリスト用には fml を使用した。また、SMTP 認証を使っ

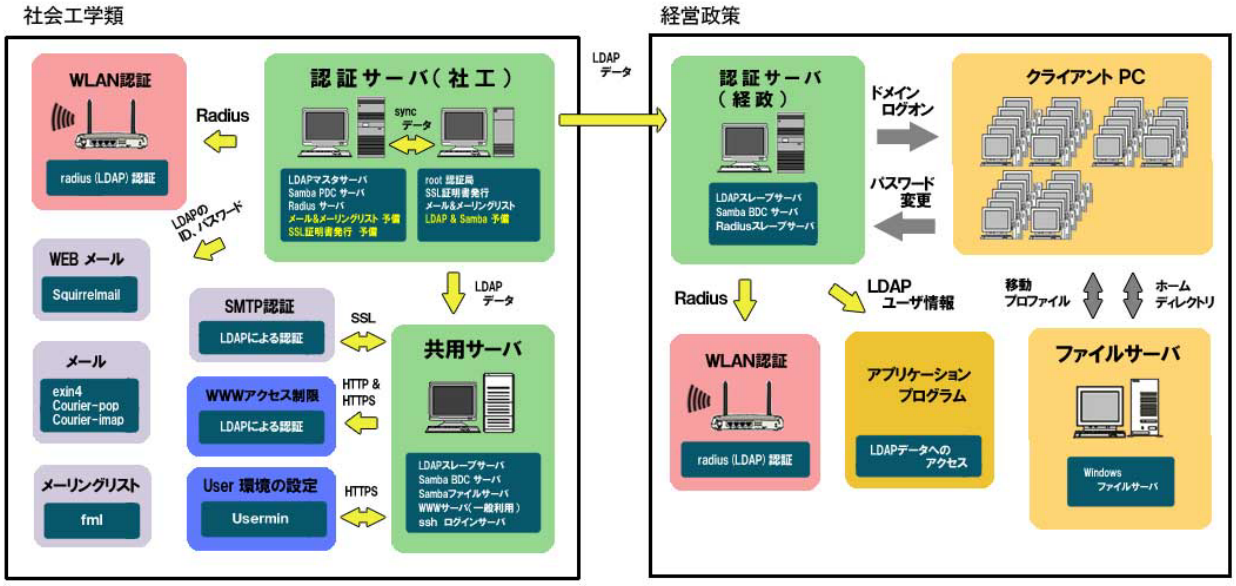


図３－１　システム構成

て、メールの中継を行うこともできるようにした。これらの機能の何れもが LDAP による同じ ID とパスワードで利用できる。

今回は、特にメーリングリストの管理を容易に行うための仕組みを作成した。メーリングリスト用のソフトウェアとしては fml を使用しているが、この管理を WEB インターフェースで行う環境は既に存在し公開されている。ただ、これは使い難いように思われたので独自に開発することにした。図３－２、図３－３に示すように、管理は WEB インターフェースを使って行い、リストメンバーの管理は予め設定されたユーザが行う。このユーザの認証、WEB ページへのアクセス制限等に LDAP サーバの情報を利用している。

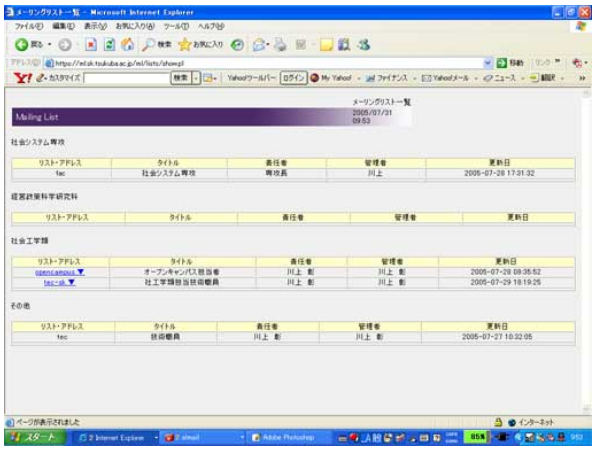

図３－２　メーリングリスト表示

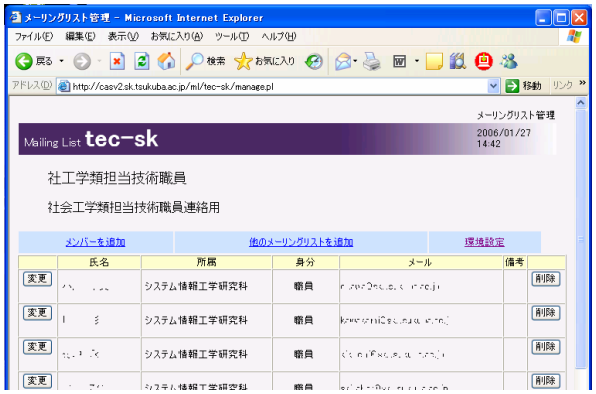


図３－３　メーリングリスト管理

## 4.3 今後の課題

報告した機能の一部は、実際に利用されているが、多くはまだ試験的な段階である。今後は、これらの機能を公開するとともに、最適な運用方法について検討し、調整していく必要がある。

## ５．まとめ

ここで紹介した内容については、今後共同して作業を行うことによって、更に便利で効率的な環境を作ることができる。そのためには、各人の協力体制、情報の共有化を図り、技術の向上を目指す必要性がある。今後、更なる協力体制を強化し、業務の改善、効率化等に向けて努力したい。

## 参考資料

[1] 第１特集　無線 LAN の構造と認証強化、UNIX USER、ソフトバンクパブリッシング（株）、2004.7
[2] 802.11 セキュリティ
http://www.famm.jp/wireless/modules/newbb/
[3] CISCO AIRONET 1200 マニュアル
http://www.cisco.com/japanese/warp/public/3/jp/service/manual-j/
[4] 梅垣まさひろ,寺村綾子．fml メーリングリスト管理, オーム社(2000)