〈報　告〉

LDAPを利用したさくらキャンパスネットワークの認証の統一化

西村　英俊*・奥野　　浩**

Unified authentication of Sakura Campus Network using LDAP

Hidetoshi NISHIMURA* and Hiroshi OKUNO**

1. はじめに

さくらキャンパスのネットワークは，いくつかのサブネットに分けられ，運用されている．その中に，実習等で学生が利用できる環境として，計算機実習室ネットワークがある．計算機実習室のネットワークは，十数年にわたる運用実績があり，拡大と改善が行われてきた．現在のシステムは2006年4月に構築されたもので，LDAP（Lightweight Directory Access Protocol）サーバーよる認証の一元化を目指したシステムである．LDAPとは読取り，閲覧，検索の用途に最適化された特殊なデータベースであるディレクトリサービスと通信するネットワークプロトコルのことで，LDAPサーバーと連携するファイルサーバー，メールサーバー，プロキシサーバーなどのサーバー群によって，学生にさまざまなサービスを提供している．これらのサーバーは，さくらキャンパス全体のネットワークにあるサーバー群と通信をして機能している．

一方，2008年4月の時点で，さくらキャンパスネットワークには次のような問題があった．一つは，多数のサーバーにおけるユーザーの管理の煩雑さであり，もう一つは，メールに関するものである．メールに関するものとしては，現在所属していないユーザーへのメールの処理よるシステムへの高負荷と学外からのメールの取扱への要望とがあった．

* スポーツ健康科学部　マネージメント学科
** 医学部

そこで，LDAPによるユーザー管理を学生だけでなく，教職員にまで広げ，ユーザー管理の一元化を実現し，さらに，その情報を使って，メールに関する問題の解決を図った．

2. 問題の詳細

2.1 ユーザー管理の問題

さくらキャンパスネットワークは，メールイクスチェンジャー（mx），メールサーバー（arukas0），ウェッブサーバー（www1），プロキシサーバー（squid）など12台，および計算機実習室ネットワークを管理する3台，計15台のサーバーによってサービスが提供されている．1つのサーバーは基本的に1つのサービスのみを提供するように構成している．これは，サーバーに障害が発生した場合でも，そのほかのサービスに影響が出にくい，サーバーの更新がしやすい，新たなサービスが立ちあげられやすいなどの長所がある．一方，管理が煩雑であるという短所がある．特に，ユーザー管理については，変更があるとすべてのサーバー上で変更の必要があり，また，各サーバー上のユーザー情報の同期も問題になる．

これを解消するために，ユーザー管理情報を1つのサーバーに収納し，それを他のサーバーで利用するように考えた．するとユーザー管理情報の変更は1つのサーバー上でそのユーザー情報のみを変更すればよくなる．このようなシステムを組むには，各サーバーのユーザー情報の差がないようにし，ま

た，運用中であるので，ユーザーには，システムの変更がわからないようにする必要があった．

2.2　メールの問題と要望

さくらキャンパスのネットワークのユーザーは毎年400人のユーザーの削除と追加がある．そのため，過去のユーザーへのメールが大量に送り付けられてくる．多くの場合，こちらのエラーメールによって，送付を止めるが，きちんと管理されていないメーリングリストなどでは，エラーメールをきちんと処理せず，メールサーバーに送り返し，送付をやめない．一方，さくらキャンパスメールシステムは，インターネットとの通信を行う mx，内部のメールを処理する arukas0，実習室ネットワーク内で学生用のメールを処理する compserv の 3 台によって構成されている．外部から来たメールは，mx が受けて，教職員宛のメールは arukas0 に学生宛てのメールは compserv に渡す．過去のユーザーのメールは，arukas0 または compserv で処理され，エラーメールは，この逆の流れで，送信される．これが大量に発生することにより，キャンパス内のメールシステムに大きな負荷がかかる．

この負荷を軽減するため，mx 上でメールのエンベロープ情報を読み，それと LDAP 上のさくらキャンパスネットワークのユーザー情報を参照し，宛先が現存しないユーザーであるときには，そのまま破棄する．これにより，mx 上での処理に必要な作業量は数分の 1 以下になり，また，arukas0 や compserv の負荷は 0 となる．また，この処理をシステムに組むことにより，SPAM メール配布の道具となる危険性を軽減できる．

また，ユーザーから学外からのメールの扱いについて，多くの要望があり，上記の問題を解決するにあたって，システム全体を見直した．

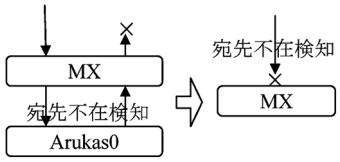

図 1　メールの流れ

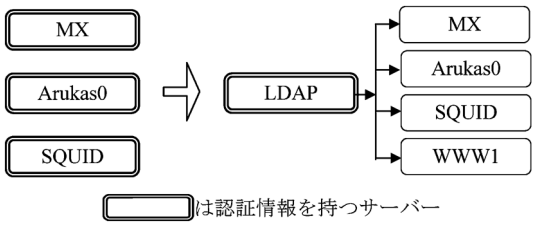

図 2　認証情報を持つサーバー

3.　システムの構成

実習室ネットワークの中に，OpenLDAP[2)]をインストールした ldap というサーバーが既に稼働している．ldap がもつ情報を利用して，実習室ネットワークのメールサーバー compserv および samba をよるファイルサーバーと PDC である fs がある．ここでは，更に次のようなユーザーにサービスを提供するサーバーの設定を変更し，認証の統一を行った．なお，これ以外にも DNS サーバーなどシステムを構成するサーバーが存在するが，一般ユーザーが直接利用することはないので，認証の統合からは除外している．

サーバー名	機能	アプリケーション
mx	メール	postfix, gnu-mailutils
arukas0	メール	postfix, gnu-mailutils
squid	WWW キャッシュ	squid
www	http サーバー	apache

各サーバーの OS は，FreeBSD になっている．

3.1　準備

さくらキャンパスネットワーク上で稼働しているサーバーは，それぞれ稼働開始時期の違い，サービス内容によるユーザーの範囲や情報に不統一があった．これを各サーバー上で統一した．

3.2　LDAP サーバーの構成

3.2.1　OpenLDAP のインストールと設定

NEC Express5800/110Ba-e3（Pentium-M1.1GHz, 1GB メモリ，40GBHDD）に，OS として

FreeBSD5.4 がインストールされている状態で，package よ　り OpenLDAP-sasl-server2.2.21, OpenLDAP-sasl-client2.2.21 をインストールした．

3.2.2　slapd.conf[1]の変更

slapd.conf.default をコピーし，次の変更を行う．

3.2.2.1　スキーマファイルの追加

samba, postfix, squid の各サーバープログラムで LDAP を利用して認証を行うため次のスキーマファイルのインクルードの追加する．

corba.schma, cosine.schma, intorgperson.schma, openldap.schma, samba.schma, nis.schma, samba.schma, misc.schma

3.2.2.2　アクセスポリシーの設定

ユーザーパスワードのエントリに関しては，認証に使えるようにして，認証後は情報を読み，また，自分自身のパスワードの変更ができるようにした．そのほかのエントリについては，自分自身のデータは読むことと変更が可能で，アプリケーションソフトウェアからはデータが読めるように設定した．次を追加する．

```
access to attrs=userPassword
        by self write
        by users read
        by anonymous auth

access to *
        by self write
        by users read
        by anonymous read
```

3.2.2.3　BDB database defition

利用実態に合わせ，次のように変更した．

```
suffix      ‘‘dc=sakura,dc=juntendo’’
rootdn      ‘‘cn=Manager,dc=sakura,dc=juntendo
```

また，rootpw を設定した．これは，暗号化されて保存される．

さらに，検索の高速化を考え次の行を追加した．

```
index       uid,uidNumber
```

3.2.3　起動とエラーチェック

次を実行し，起動スクリプトと設定をチェックする．

```
# /usr/local/etx/rc.d/slapd.sh start
# ldapsearch -h localhost -x -s base ‘(objectclass=*)’ namingContext
```

3.2.4　LDIF ファイルによるデータの作成

3.2.4.1　初期データと管理者の定義（init.ldif）

次の内容のファイルを作成する．

```
dn: dc=sakura.dc=juntendo
objectclass: dcObject
objectclass: organization
o: Juntendo Univ
dc: sakura

dn: cn=Manager,dc=sakura.dc=juntendo
objectclass: organizationRole
cn: Manager
```

次のコマンドで LDAP のデータとして組み込む．

```
# ldapadd -x -D ‘‘cn=Manager,dc=sakura.dc=juntendo’’ -w〈パスワード〉-f init.ldif
```

3.2.4.2　基本クラスの作成（base.ldif）

データの基本構造を表す次のファイル（base.ldif）を作成する．

```
dn: ou=Peoples,dc=sakura,dc=juntendo
objectClass: organizationalUnit
ou: Peoples
```

```
dn: ou=Groups,dc=sakura,dc=juntendo
objectClass: organizationalUnit
ou: Groups

dn: ou=Aliases,dc=sakura,dc=juntendo
objectClass: organizationalUnit
ou: Aliases
```

次のコマンドで LDAP のデータとして組み込む.

```
# ldapadd -x -D ''cn=Manager,dc=sakura.dc=juntendo'' -w〈パスワード〉-f base.ldif
```

実際のデータを作成し，LDAP のデータとして組み込む.

''ou = Peoples,dc = sakura,dc = juntendo'' 以下には，ユーザー情報として，ユーザー名，パスワード，シェル，ホームディレクトリの情報を格納した.

''ou=Groups,dc=sakura,dc=juntendo'' 以下には，UNIX 系のユーザーグループの情報を格納した.

''ou=Aliases,dc=sakura,dc=juntendo'' 以下には，メール転送用の情報を格納した.

3.3 squid の設定

OpenLDAP-sasl-client を package から，pam を ports よりインストールした．squid は，ソースをダウンロードし，コンパイルしたものをインストールした．実習室ネットワークなどすでに認証を受けたもの以外からの squid へのアクセスに対して，pam を利用して認証を行うようにした．これによって，アクセスコントロールを行っている.

3.3.1 ldap.conf の設定

LDAP サーバーの指定，baseDN の指定，pam の利用するフィルターの設定，nsswitch の利用するパスワードとグループの指定を行う.

```
host 172.16.0.6
base dc=sakura,dc=juntendo
pam_filter &（objectClass=postfixAccount)(o=*s*)

nss_base_passwd
  ou=Peoples,dc=sakura,dc=juntendo?one?o=*s*
nss_base_group
  ou=Groups,dc=sakura,dc=juntendo?one
```

3.3.2 /etc/pam.d/squid の作成

pam を squid から利用できるようにするため，次の内容のファイルを作成した.

```
auth        sufficient    pam_ldap.so
                                no_warm try_first_pass
auth        required      pam_ldap.so
                                no_warm try_first_pass
account     sufficient    pam_ldap.so
                                no_warm try_first_pass
account     required      pam_ldap.so
                                no_warm try_first_pass
```

3.3.3 squid.conf

認証のため，次を付け加えた.

```
auth_param basic program /usr/local/squid/libexec/pam_auth -m ''squid''
auth_param basic program children 100
auth_param basic program realm Sakura Campus
auth_param basic program credentialsttl 1 hours
authenticate_ttl 15 minutes
```

これを利用したアクセスアクセスコントロールを設定した.

3.4 arukas0 の設定

OpenLDAP-sasl-client と postfix を package から，pam と nsswitch を ports よりインストールする．また，ソースから，gnu-mailutils をインストールした.

UNIX ユーザーとして認証が必要なので，ここでは，pam と nssswitch を通して，LDAP のデータを利用して認証を行う.

3.4.1　ldap.conf の設定

ldap のクライアントソフトの設定を行う．pam および nsswitch のための設定を加えた．

OpenLDAP サーバーの IP アドレス，base　dn, pam_filter，nss_base_passwd，nss_base_group を次のように設定した．

```
host 192.168.3.1
base dc=sakura,dc=juntendo

pam_filter &(objectClass=postfixAccount)(o=*a*)

nss_base_passwd
    ou=Peoples,dc=sakura,dc=juntendo?one?o=*a*
nss_base_group
    ou=Groups,dc=sakura,dc=juntendo?one
```

3.4.2　/etc/pam.d/system

UNIX ユーザーとして LDAP データを利用して認証を受けられるようにするため，次のように設定した．

```
auth        sufficient    pam_opie.so
                          no_warm no_fake_prompts
auth        requisite     pam_opieaccess.so
                          no_warm allow_local
auth        sufficient    pam_ldap.so
                          no_warm try_first_pass
auth        required      pam_unix.so
                          no_warm try_first_pass nullok

account     required      pam_login_access.so
account     required      pam_unix.so

session     required      pam_lastlog.so
                          no_fail

password    required      pam_unix.so
                          no_warn try_first_pass
```

pop3, ftpd 等については，この system ファイルをインクルードするように設定した．

3.4.3　/etc/nsswitch.conf

パスワードとユーザーグループ情報が LDAP により定義されていることを宣言する．

```
group: compat
group_compat: ldap
passwd: compat
passwd_compat: ldap
```

3.4.4　main.cf

LDAP に関する設定はない．ただし，クライアントから受けたメールは，自分のサーバーのユーザー以外のものは，mx に転送する．

3.5　www1

apache を ports よりインストールする．ただし，--enable-ldap と -enable-authnz-ldap オプションを有効にしてコンパイルする．

学内ホームページを閲覧するときに，認証し，それによりアクセスコントロールを行えるようにした．

3.5.1　/usr/local/etc/apatch2.2/httpd.conf の設定

次を追加する．

(a)　LDAP を利用するためのモジュールをロードする．

```
LoadModule authnz_ldap_module modules/mod_authenz_ldap.so
LoadModule ldap_module modules/mod_ldap
```

(b)　次の設定を追加する．

```
<DirectoryMatch ''^/www/data/(.+/)*authldap''>
    AuthBasicProvider ldap
    AuthzLDAPAuthoritative off
    AuthLDAPURL  ldap://ldap/ou=Peoples,dc=sakura,dc=juntendo?uid
    AuthName ''Website of Juntendo Univ. Sakura''
    AuthType Basic
```

```
    require valid-user
</DirectoryMatch>
```

これにより，ディレクトリ中に authldap という名称のディレクトリを作成すると，そこを閲覧する時に，認証を求めらるようになる．

3.6　mx

OpenLDAP-sasl-client を package から，postfix を ports からインストールする．また，ソースから，gnu-mailutils をインストールした．

postfix は，sasl を使って，LDAP と通信し情報を得るようにした．これによって，次の 2 つのことを実現した．1 つは，外部から来たメールの宛先が内部のものに関して，実際にそのユーザーが存在しない場合には，受け取りを拒否することである．もう 1 つは，さくらキャンパスネットワークのユーザーが，学外から，mx にアクセスして，学外へメールを配送できるようすることである．

3.6.1　/usr/local/etc/saslauthd.conf

LDAP サーバーの位置と baseDB とフィルターを定義する．

```
ldap_servers: ldap://172.16.0.6/
ldap_search_base: dc=sakura,dc=juntendo
ldap_filter: (&(uid=%u)(o=*a*))
```

3.6.2　main.cf

Postfix が sasl を通して，認証が可能になるように次を追加する．

```
smtpd_sasl_auth_enable = yes
smtpd_client_restrictions = permit_mynetworks,
        permit_sasl_authenticated,
    check_client_access  regexp:/usr/local/etc/postfix
    /whitelist,
        reject_unknown_client
        permit

smtpd_helo_restrictions = permit_mynetworks,
        permit_sasl_authenticated,
    check_helo_access   hash:/usr/local/etc/postfix/
    helo_access,
        reject_non_fqdn_hostname,
        reject_invalid_hostname,
        permit

smtpd_recipient_restrictions  =  permit_sasl_authenti-
cated,
        permit_mynetworks,
        permit_auth_destination,
        reject
```

学内のユーザー宛のメールであるかをチェックするために次を追加する．

```
relay_recipient_maps = ldap:ldaprecipient
ldaprecipient_server_host = 172.16.0.6
ldaprecipient_search_base = dc=sakura,dc=juntendo
ldaprecipient_query_filter = (uid=%u)
ldaprecipient_result_attribute = uid
```

別名への対応のため次を追加する．

```
alias_maps = hash:/etc/aliases
```

3.6.3　master.cf

サブミッションポートを有効にするために次を追加する．

```
submission inet n - n - -smtpd -o smtp_enforce_tls=yes
```

4.　メールシステムについて

mx の設定により次のことを今回実現した．

4.1　さくらキャンパスネットワークの存在しないユーザー宛のメールの処理

3.6.2 の設定により，さくらキャンパスネットワークに存在しないユーザー宛のメールは，smtp 接続の最初の段階である hello を相手から送りつけ

られたところで接続を拒否するようにした．これにより，システム全体におけるエラーメールの処理が減少した．また，from アドレスを詐称することによる return メールを悪用した SPAM メールの配送に利用されることも防ぐことができるようになった．

4.2　さくらキャンパスネットワークユーザーの外部ネットからの mx を利用したメールの配送

mx におけるユーザー認証を利用して，外部のネットワークから，メールを mx を経由して配送できるようにした．これは，一種のメールの転送になる．一般に，メールの転送はセキュリティ上問題があるとされているが，それをさくらキャンパスネットワークのユーザーに限定することにより，安全に実現した．今後，メール利用に関するセキュリティの強化の一環として，メールがどのサーバーから送られてきたかの確認をするようになりつつある．この設定によって，外部からでも相手から受け入れられるメールを配信できるようになった．

5. 考　　察

5.1　ユーザー管理について

これまではユーザの登録及び削除処理をユーザ認証が必要なメールサーバー（arukas0），ウェブプロキシサーバー（squid），及びウェッブサーバ www1，それぞれでおこなってきた．このため誤操作もあったが，LDAP サーバー上で登録・削除処理行うようになり，管理者の負担が軽減し，また，システム全体の見通しが良くなったので，誤操作の可能性も減った．

5.2　メールシステムについて

以前のシステムで大量に発生していたエラーメールがまったく発生しなくなった．以前はそのエラーメールの処理を毎日行わないとシステムが不安定になっていたが，今はその操作自体が不必要となった．

5.3　今後について

RADIUS と LDAP を連携し，無線 LAN のユーザー認証に LDAP を利用できるようにして，ユーザーの便宜を図りたい．

文　　献

1）　河津正人，山形昌也，恒田正哉，桑田雅彦，島村英（2001）LDAP ハンドブック　ソフト・リサーチ・センター

2）　OpenLDAP Foundation
http://www.opneldap.org/

（平成20年10月 7 日　受付
平成21年 2 月 6 日　受理）