LDAP Account Manager 利用者ガイド

オープンソース・ソリューション・テクノロジ株式会社

作成 : 2008 年 2 月 14 日

リビジョン: 1.3

目次

1. 概要

LDAP Account Manager(以降 LAM)は、LDAP に登録されたアカウント情報を Web インターフェース上で管理するためのツールです。
本ドキュメントは RedHat Enterprise Linux、CentOS、Asianux で OSS テクノロジ提供の LAM を利用する方法を説明します。

2. LAM のインストール

LAM を利用するために必要な RPM パッケージとして、OSS テクノロジより後述の rpm パッケージを提供します。パッケージ名は、x86 版について載せていますが、x86_64 版では i386 の部分を x86_64 に読み替えてください。なおパッケージのバージョン番号等はパッケージのアップデートに伴い変更されることがあります。

まず各 OS ごとのインストールにおける注意事項を確認したのち、パッケージのインストールを実施してください。

パッケージのインストールは rpm コマンドで行います。各パッケージが/tmp/lam ディレクトリに用意されている場合、root 権限にて、次のコマンドでパッケージをインストールします。

```
# cd  /tmp/lam
# rpm -Uhv *.rpm
```

2.1 RedHat Enterprise Linux 5 / CentOS 5

LAM 関連パッケージのインストール前に、perl-Convert-ASN1 パッケージをインストールする必要があります。perl-Convert-ASN1 パッケージがインストールされていない場合、下記のコマンドで perl-Convert-ASN1 パッケージをインストールしておいてください。

```
# yum install perl-Convert-ASN1
```

- ldap-account-manager-2.2.0-1.1_OSSTECH.noarch.rpm
- mhash-0.9.2-3.i386.rpm
- mhash-devel-0.9.2-3.i386.rpm
- libssh2-devel-0.18-1.1_OSSTECH.el4.i386.rpm
- php-mhash-5.1.6-2.el4.i386.rpm
- php-ssh2-5.1.6-1.el4.i386.rpm
- perl-Class-ErrorHandler-0.01-1.1_OSSTECH.noarch.rpm
- perl-Class-Loader-2.03-1.2.1_OSSTECH.noarch.rpm
- perl-Convert-ASCII-Armour-1.4-1.2.1_OSSTECH.noarch.rpm
- perl-Convert-PEM-0.07-1.2.1_OSSTECH.noarch.rpm
- perl-Crypt-CBC-2.17-1.1_OSSTECH.noarch.rpm
- perl-Crypt-DES-2.05-3.1_OSSTECH.i386.rpm
- perl-Crypt-DES_EDE3-0.01-1.2.1_OSSTECH.noarch.rpm

- perl-Crypt-DH-0.06-1.1_OSSTECH.noarch.rpm
- perl-Crypt-DSA-0.13-1.1_OSSTECH.noarch.rpm
- perl-Crypt-IDEA-1.08-1.1_OSSTECH.i386.rpm
- perl-Crypt-Primes-0.50-1.1_OSSTECH.i386.rpm
- perl-Crypt-RSA-1.57-1.1_OSSTECH.noarch.rpm
- perl-Crypt-Random-1.25-1.2.1_OSSTECH.noarch.rpm
- perl-Data-Buffer-0.04-1.2.1_OSSTECH.noarch.rpm
- perl-Digest-MD2-2.03-1.2.1_OSSTECH.i386.rpm
- perl-Math-GMP-2.04-1.1_OSSTECH.i386.rpm
- perl-Math-Pari-2.010706-1.1_OSSTECH.i386.rpm
- perl-Module-Build-0.2611-1.2.1_OSSTECH.noarch.rpm
- perl-Net-SSH-Perl-1.30-2.1_OSSTECH.noarch.rpm
- perl-Quota-1.5.1-1.2.1_OSSTECH.i386.rpm
- perl-Sort-Versions-1.5-1.2.1_OSSTECH.noarch.rpm
- perl-Tie-EncryptedHash-1.21-1.2.1_OSSTECH.noarch.rpm

2.2 RedHat Enterprise Linux 4 / CentOS 4

- ldap-account-manager-1.3.0-1.2_OSSTECH.noarch.rpm
- mhash-0.9.2-3.i386.rpm
- mhash-devel-0.9.2-3.i386.rpm
- libssh2-devel-0.18-1.1_OSSTECH.el4.i386.rpm
- php-mhash-4.3.9-2.el4.i386.rpm
- php-ssh2-4.3.9-1.el4.i386.rpm
- perl-Archive-Tar-1.26-1.1_OSSTECH.noarch.rpm
- perl-Class-ErrorHandler-0.01-1.1_OSSTECH.noarch.rpm
- perl-Class-Loader-2.03-1.2.1_OSSTECH.noarch.rpm
- perl-Compress-Zlib-1.41-1.1_OSSTECH.i386.rpm
- perl-Convert-ASCII-Armour-1.4-1.2.1_OSSTECH.noarch.rpm
- perl-Convert-PEM-0.07-1.2.1_OSSTECH.noarch.rpm
- perl-Crypt-CBC-2.17-1.1_OSSTECH.noarch.rpm
- perl-Crypt-DES-2.05-3.1_OSSTECH.i386.rpm
- perl-Crypt-DES_EDE3-0.01-1.2.1_OSSTECH.noarch.rpm
- perl-Crypt-DH-0.06-1.1_OSSTECH.noarch.rpm

- perl-Crypt-DSA-0.13-1.1_OSSTECH.noarch.rpm
- perl-Crypt-IDEA-1.08-1.1_OSSTECH.i386.rpm
- perl-Crypt-Primes-0.50-1.1_OSSTECH.i386.rpm
- perl-Crypt-RSA-1.57-1.1_OSSTECH.noarch.rpm
- perl-Crypt-Random-1.25-1.2.1_OSSTECH.noarch.rpm
- perl-Data-Buffer-0.04-1.2.1_OSSTECH.noarch.rpm
- perl-Digest-MD2-2.03-1.2.1_OSSTECH.i386.rpm
- perl-IO-Socket-SSL-0.999-1.1_OSSTECH.noarch.rpm
- perl-Jcode-2.03-1.1_OSSTECH.i386.rpm
- perl-Math-GMP-2.04-1.1_OSSTECH.i386.rpm
- perl-Math-Pari-2.010706-1.1_OSSTECH.i386.rpm
- perl-Module-Build-0.2611-1.2.1_OSSTECH.noarch.rpm
- perl-Net-SSH-Perl-1.30-2.1_OSSTECH.noarch.rpm
- perl-Net-SSLeay-1.25-3.1_OSSTECH.i386.rpm
- perl-Quota-1.5.1-1.2.1_OSSTECH.i386.rpm
- perl-Sort-Versions-1.5-1.2.1_OSSTECH.noarch.rpm
- perl-String-CRC32-1.4-1.1_OSSTECH.i386.rpm
- perl-Tie-EncryptedHash-1.21-1.2.1_OSSTECH.noarch.rpm
- perl-Unicode-Map-0.112-0.2.1_OSSTECH.i386.rpm
- perl-Unicode-Map8-0.12-0.2.1_OSSTECH.i386.rpm
- perl-Unicode-MapUTF8-1.11-1.1_OSSTECH.noarch.rpm
- perl-Unicode-String-2.09-1.1_OSSTECH.i386.rpm

2.3 MIRACLE LINUX V4.0

- ldap-account-manager-1.3.0-1.2_OSSTECH.noarch.rpm
- mhash-0.9.2-3.i386.rpm
- mhash-devel-0.9.2-3.i386.rpm
- libssh2-devel-0.18-1.1_OSSTECH.el4.i386.rpm
- php-mhash-5.0.5-2.el4.i386.rpm
- php-ssh2-5.0.5-1.el4.i386.rpm
- perl-Archive-Tar-1.26-1.1_OSSTECH.noarch.rpm
- perl-Class-ErrorHandler-0.01-1.1_OSSTECH.noarch.rpm
- perl-Class-Loader-2.03-1.2.1_OSSTECH.noarch.rpm

- perl-Compress-Zlib-1.41-1.1_OSSTECH.i386.rpm
- perl-Convert-ASCII-Armour-1.4-1.2.1_OSSTECH.noarch.rpm
- perl-Convert-PEM-0.07-1.2.1_OSSTECH.noarch.rpm
- perl-Crypt-CBC-2.17-1.1_OSSTECH.noarch.rpm
- perl-Crypt-DES-2.05-3.1_OSSTECH.i386.rpm
- perl-Crypt-DES_EDE3-0.01-1.2.1_OSSTECH.noarch.rpm
- perl-Crypt-DH-0.06-1.1_OSSTECH.noarch.rpm
- perl-Crypt-DSA-0.13-1.1_OSSTECH.noarch.rpm
- perl-Crypt-IDEA-1.08-1.1_OSSTECH.i386.rpm
- perl-Crypt-Primes-0.50-1.1_OSSTECH.i386.rpm
- perl-Crypt-RSA-1.57-1.1_OSSTECH.noarch.rpm
- perl-Crypt-Random-1.25-1.2.1_OSSTECH.noarch.rpm
- perl-Data-Buffer-0.04-1.2.1_OSSTECH.noarch.rpm
- perl-Digest-MD2-2.03-1.2.1_OSSTECH.i386.rpm
- perl-Jcode-2.03-1.1_OSSTECH.i386.rpm
- perl-Math-GMP-2.04-1.1_OSSTECH.i386.rpm
- perl-Math-Pari-2.010706-1.1_OSSTECH.i386.rpm
- perl-Module-Build-0.2611-1.2.1_OSSTECH.noarch.rpm
- perl-Net-SSH-Perl-1.30-2.1_OSSTECH.noarch.rpm
- perl-Quota-1.5.1-1.2.1_OSSTECH.i386.rpm
- perl-Sort-Versions-1.5-1.2.1_OSSTECH.noarch.rpm
- perl-String-CRC32-1.4-1.1_OSSTECH.i386.rpm
- perl-Tie-EncryptedHash-1.21-1.2.1_OSSTECH.noarch.rpm
- perl-Unicode-Map-0.112-0.2.1_OSSTECH.i386.rpm
- perl-Unicode-Map8-0.12-0.2.1_OSSTECH.i386.rpm
- perl-Unicode-MapUTF8-1.11-1.1_OSSTECH.noarch.rpm
- perl-Unicode-String-2.09-1.1_OSSTECH.i386.rpm

3. LAM の初期設定

LAM の初期設定は次の手順で行ってください。

3.1 PHP の設定

LAM を利用する前に、/etc/php.ini の memory_limit の値を 32M 以上に設定します。

ユーザー数が数千エントリある場合には、128M～256M のメモリを利用可能に設定しておく必要があります。

```
memory_limit = 64M
```

3.2 LAM の設定ファイルの準備

続いて LAM の初期設定ファイルを作成します。/var/www/html/lam/config に設定ファイルのサンプルとして、config.cfg_sample がインストールされていますので、このファイルを config.cfg としてコピーし、パスワードとプロファイル名を設定します。

```
# cd /var/www/html/lam/config
# cp config.cfg_sample config.cfg
# vi config.cfg
```

/var/www/html/lam/config/config.cfg には LAM 管理用のパスワードとデフォルトプロファイルを設定します。

```
# password to add/delete/rename configuration  profiles
password: secret

# default profile, without  ".conf"
default: lam
```

上記設定では、パスワードを"secret"、デフォルトプロファイルの設定ファイルを lam.conf として設定しています。

暗号化パスワードを設定したいときは、slappasswd コマンドで暗号化したパスワード文字列を取得し、config.cfg ファイルに設定します。

例えば、パスワード「lam」を、SSHA 形式で暗号化したい場合、次のコマンドを実行し、表示された文字列を config.cfg の「password」パラメーターに設定します。

```
# /usr/sbin/slappasswd -h \{SSHA\} -s lam
{SSHA}2Js044HgUMWeR9aRPPHcEZ3GXMHpn5RT
```

以下は暗号化パスワードの config.cfg への設定例です。

```
# password to add/delete/rename configuration  profiles
password: {SSHA}2Js044HgUMWeR9aRPPHcEZ3GXMHpn5RT

# default profile, without  ".conf"
default: lam
```

次に lam.conf の初期設定ファイルを作成します。config.cfg ファイルと同じディレクトリ(/var/www/html/lam/config)に、サンプルとして lam.conf_sample ファイルがありますので、このファイルをコピーして lam.conf を作成します。

```
# cd /var/www/html/lam/config
# cp lam.conf_sample lam.conf
```

最後に config.cfg と lam.conf のパーミッションを apache ユーザーに変更します。

```
# chown apache:apache config.cfg
# chown apache:apache lam.conf
```

3.3 ユーザーのホームディレクトリ作成機能の設定

LAM には、ユーザーの作成時にホームディレクトリを作成し、ユーザーの削除時にホームディレクトリを削除する機能があります。この機能を利用するためには、次の設定を行う必要があります。

3.3.1 LDAP 管理者の設定

ユーザーのホームディレクトリを作成する際に、LAM 経由で ssh を実行し、ホームディレクトリの作成を行います。この際に、ssh でログインするユーザーとして LAM にログインしている LDAP 管理者のユーザー名と、LAM にログインした際のパスワードを使って ssh の認証を行います。

そのため、LDAP 管理者のエントリが、posixAccount として登録されており、かつ、OS にログインできる状態でなければなりません。そのために、LDAP 管理者のエントリが次の条件を満たす必要があります。

- LDAP 管理者が posixAccount のユーザーエントリとして LDAP に登録されていること
  - [例] uid=Manager,ou=Users,dc=example,dc=jp
- LDAP 管理者のパスワードが LDAP に格納されていること
  - LDAP 管理者のパスワードを slapd.conf ではなく、LDAP に登録する必要があります。LAM の初期設定後に、LAM からパスワードを設定することができます。

3.3.2 sudo の設定

ユーザーのホームディレクトリを作成する際には、LDAP 管理者の権限で ssh 経由で、/var/www/html/lam/lib/lamdaemon.pl コマンドを実行します。この際に、root 権限でコマンドを実行する必要があるため、sudo の設定を行います。sudo の設定は visudo コマンドで行います。

```
# visudo
```

設定内容は次のとおりです。ユーザー名の部分には、前述の LDAP 管理者のユーザー名を指定します。下記設定例では管理者ユーザーとして「Manager」を設定しています。

```
Manager ALL=NOPASSWD:/var/www/html/lam/lib/lamdaemon.pl
```

また RHEL5/CentOS5 では、「Defaults requiretty」の設定行の先頭に「#」を追加して無効にしてください。

```
# Defaults requiretty
```

3.3.3 スクリプトファイルの設定

lamdaemon.pl を LAM が実行できるように、スクリプトの設定を行います。

LAM のログイン画面で、右上の「LAM Configuration(LAM 構成設定)」をクリックします。

設定画面の「Server List」に「127.0.0.1」を設定し、「スクリプト設定」に「/var/www/html/lam/lib/lamdaemon.pl」を設定します。

3.3.4 sshd_config の設定

ホームディレクトリ作成時に、ssh 経由の認証を行いますが、この際にユーザー名とパスワードを使って認証を行うため、sshd の設定でパスワード認証を設定しておく必要があります。OS インストール後のデフォルト設定ではパスワード認証が有効になっていますが、パスワード認証が無効になっている場合は、/etc/ssh/sshd_config の PasswordAuthentication パラメーターを yes に変更します。

```
PasswordAuthentication yes
```

sshd_config の設定を変更したら、sshd を再起動します。

```
# /sbin/service sshd restart
```

以上でホームディレクトリの自動作成機能の設定は完了です。

3.4 Web サーバーの起動

LAM の初期設定が完了したら、Web サーバーを起動します。

```
# /sbin/service httpd start
```

既に Web サーバーが起動している場合は、Web サーバーを再起動します。

```
# /sbin/service httpd restart
```

4. LAM の全体設定

4.1 LAM のログイン画面

LAM にログインするため、Web ブラウザから下記の URL にアクセスします。

http://localhost/lam/index.html

【注意】

リモートからログインする際には、ファイアーウォールによるアクセス制限が行われている場合がありますので、そのような場合には HTTP 経由のアクセスが可能となるようにアクセス制限を変更してください。

正常に設定が完了していれば、図 4.1 が表示されます。

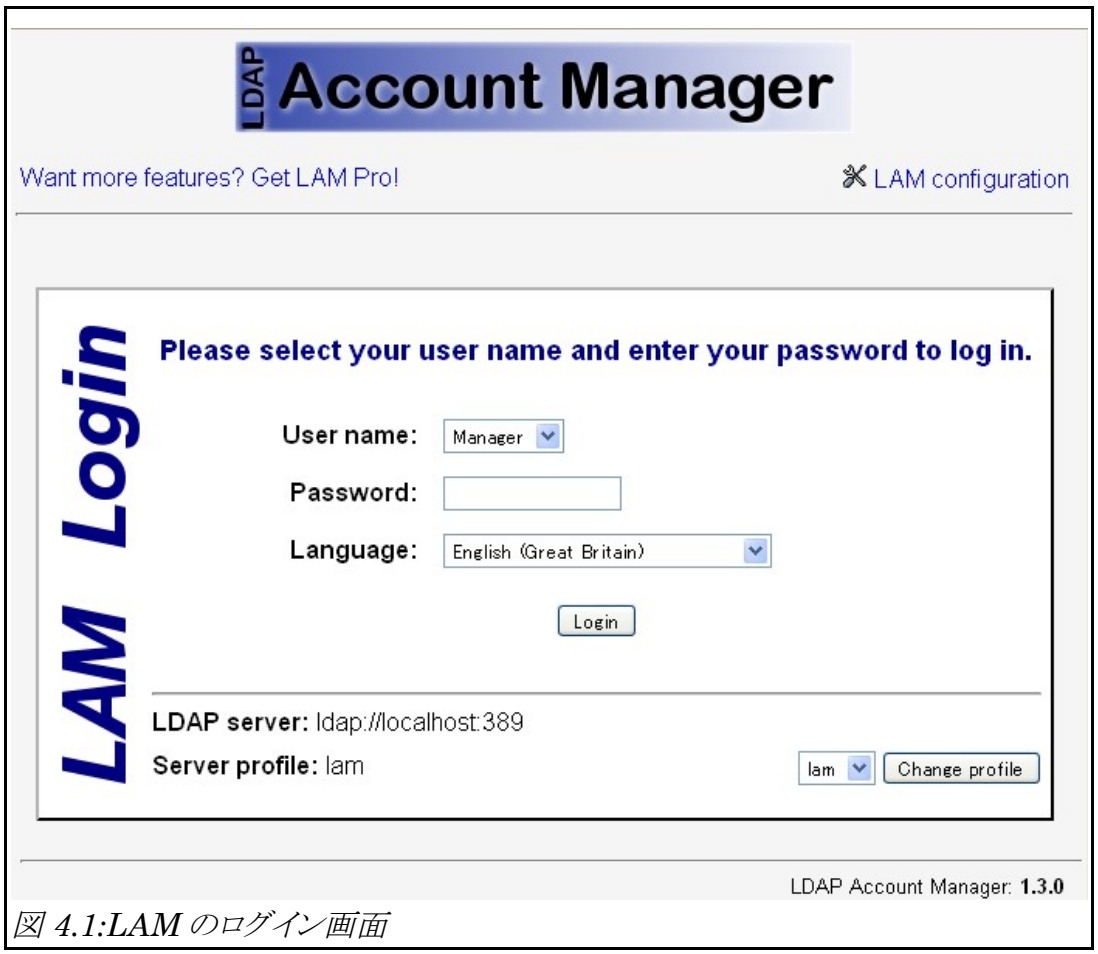

図 4.1:LAM のログイン画面

4.2 LDAP 関連の基本設定

LAM の初期設定ファイル(lam.conf)では、各パラメータにサンプルの値が指定されていますので、実際の運用

環境に適した値に、設定を変更する必要があります。そのために、LAM のログイン画面の右上にある「LAM Configuration」をクリックし、画面 4.2 に移ります。

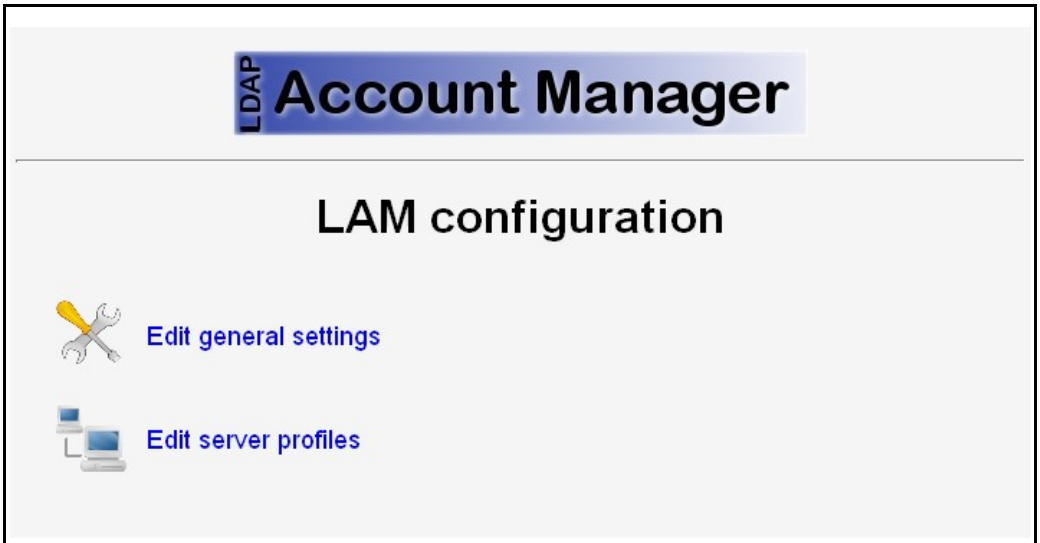

図 4.2:LAM Configuration の選択画面

図 4.2 では、「**Edit server profiles**」を選択します。

続けて、パスワードの入力画面(図 4.3)が表示されます。ここで入力するパスワードは、lam.conf の passwd の項目に設定されているパスワードを入力します。サンプルファイルの lam.conf_sample ではパスワードとして"lam"が設定されていますので、このサンプルファイルを利用して lam.conf を作成した場合は、パスワードの入力欄に「**lam**」を入力し、「OK」をクリックします。

図 4.3:LAM の管理者パスワードの入力

パスワードの認証が正常に行われると、管理する LDAP 関連の項目を設定する画面(図 4.4)が表示されます。

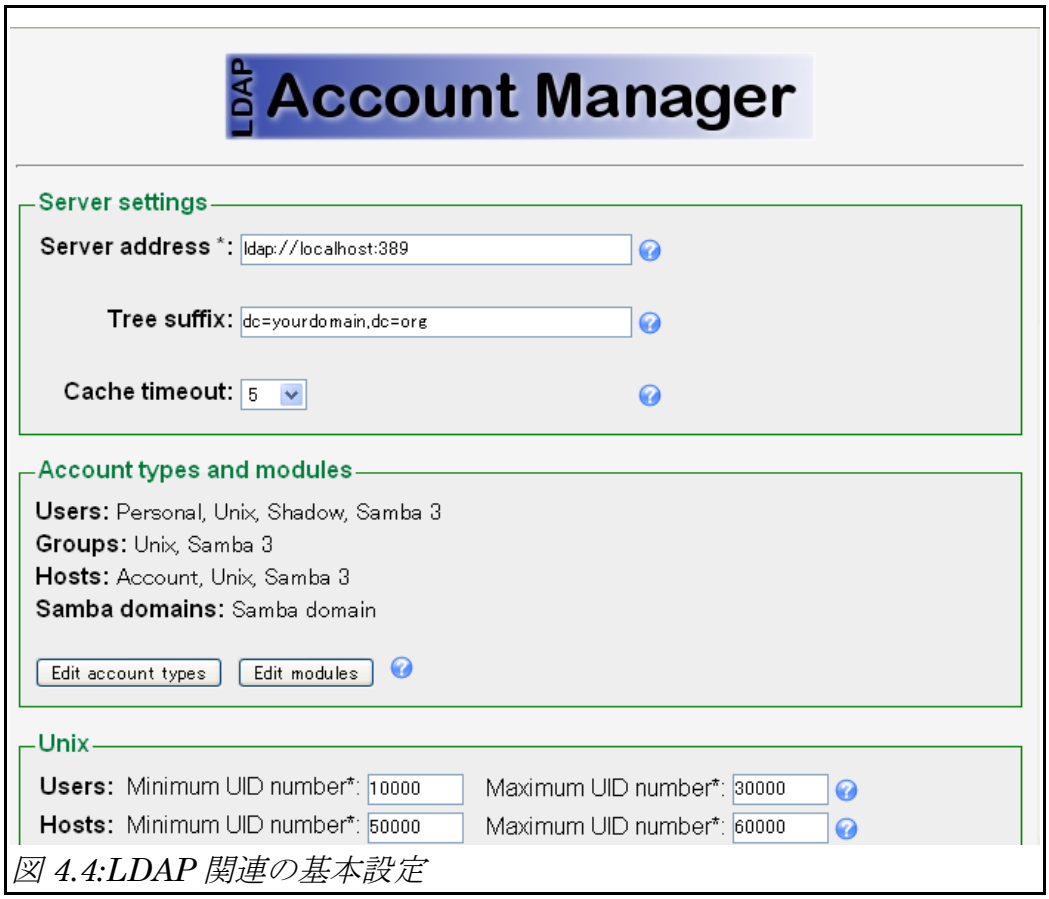

図 4.4:LDAP 関連の基本設定

本ドキュメントでは、LAM がインストールされているサーバーと同じマシンに、OpenLDAP による LDAP サーバが構築されているものとして、説明を行います。本ドキュメントの設定例として、/etc/openldap/slapd.conf には、次の値が設定されているものとします。

```
suffix   “dc=example,dc=jp”
rootdn  “uid=Manager,ou=People,dc=example,dc=jp”
rootpw   secret
```

これらの設定値は、運用環境に合わせて、読み替えてください。

また、これらの値が設定された slapd が下記コマンドで起動されているものとします。

```
# /sbin/service ldap start
```

図 4.4 で表示されている LDAP 関連の基本設定を、運用環境に合わせて設定を行います。

まず最初に「**Account types and modules**」の「**Edit modules**」をクリックし、図 4.5 を表示させます。

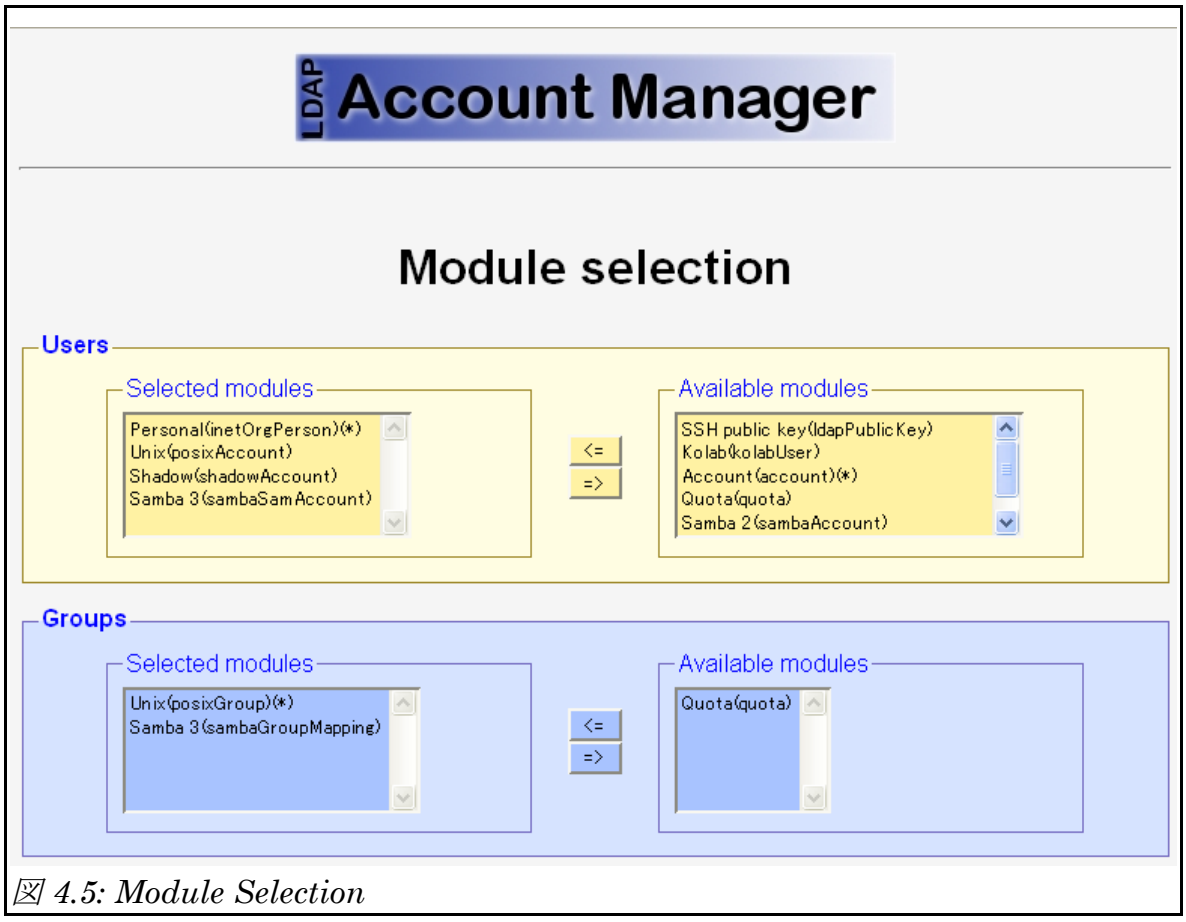

図 4.5: Module Selection

図 4.5 では、ユーザ、グループなどの LDAP エントリの属性を定義しています。デフォルト設定では Samba 3.0 との連携用の設定となっています。運用環境で Samba 3.0 との連携を行わない場合には、各エントリから、「Samba3」のモジュールを削除します。モジュールの削除は、「Samba3」を選択し、「=>」ボタンをクリックすることで設定できます。

- Users: Samba 3(sambaSamAccount)の削除
- Groups:Samba 3(sambaGroupMapping)の削除
- Hosts: Samba 3(sambaSamAccount)の削除

各モジュールの設定が完了したら、画面下部の「OK」ボタンをクリックし、図 4.4 に戻ります。

次に「**Account types and modules**」の「**Edit account types**」をクリックし、図 4.6 を表示させます。

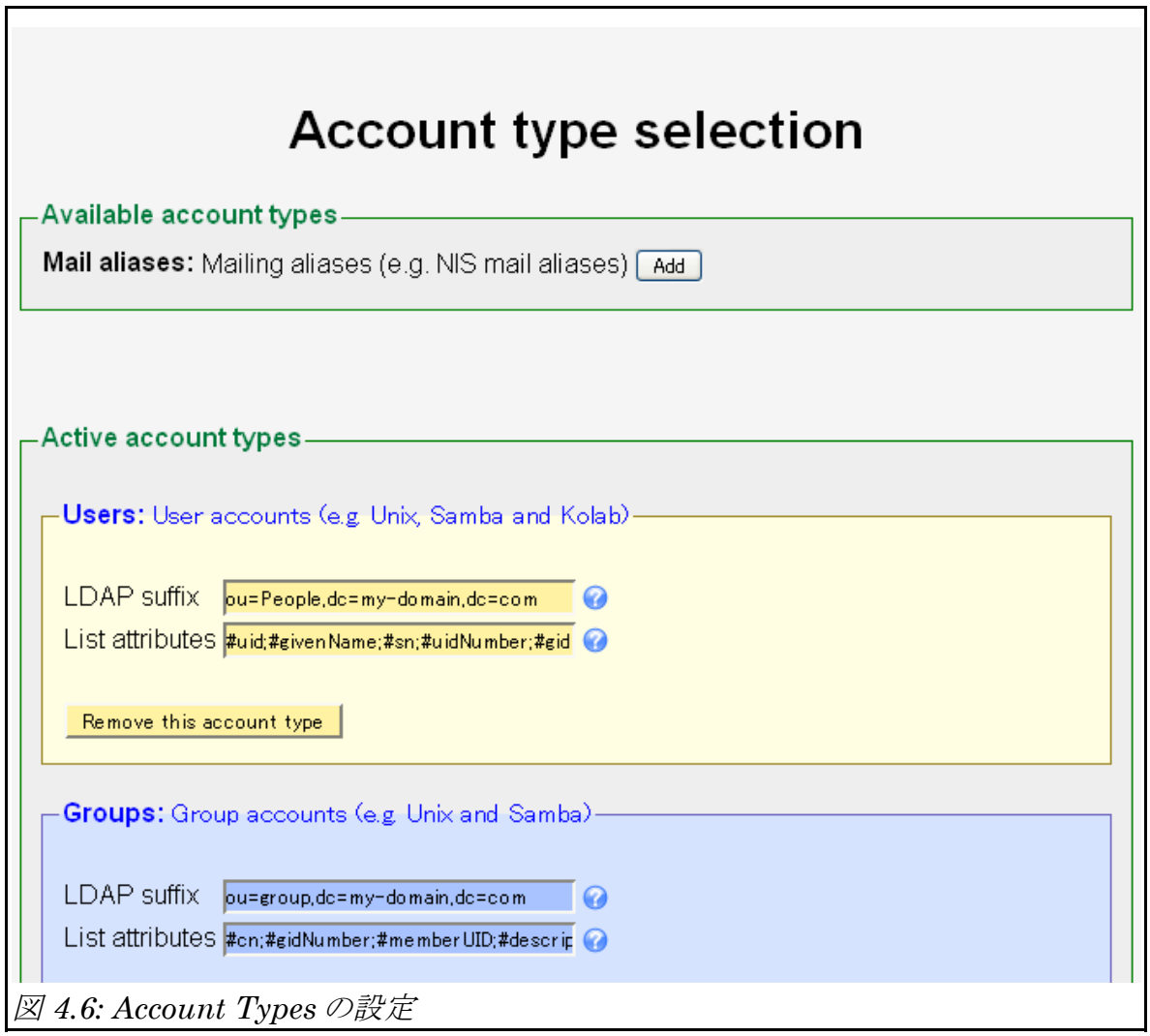

図 4.6: Account Types の設定

Users、Groups、Hosts、Samba domains の各項目の LDAP suffix を、運用環境の LDAP suffix に合わせます。本ドキュメントの環境では、以下の設定を行うことになります。

- Users: ou=People,dc=example,dc=jp
- Groups: ou=group,dc=example,dc=jp
- Hosts: ou=machines,dc=example,dc=jp
- Samba domains: ou=domains,dc=example,dc=jp

Users の「List attributes」に含まれる#givenName、#sn ですが、英語表記の順番のため「First Name(名)、Last Name(姓)」で並んでいます。そのため、ユーザーの一覧表示の際などに「名、姓」で表示されてしまうため、「#sn,#givenName」の順番に変更しておきます。

その他の項目の「List attributes」は、通常変更する必要はありません。

以上の設定を終えたら、図 4.6 の下部にある「OK」ボタンをクリックします。

続いて図 4.4 に戻りますので、各項目について、以下の通り設定します。

- Server settings
  - Server address: ldap://localhost:389　(デフォルト値のまま)
  - Tree suffix: dc=example,dc=jp　(運用環境の slapd.conf の suffix に合わせます)
  - Cache timeout : 5 分　(LAM が保持する LDAP のキャッシュを更新する間隔です。)
- Account types and modules:
  - 「Edit account types」をクリックします。詳細については既に説明しました。
- Unix
  - Users: LAM でユーザ作成時に割り当てる UID の最小値と最大値を指定します。
  - Hosts: LAM で Samba 用マシンアカウント作成時に割り当てる UID の最小値と最大値を設定します。Samba を使用しない場合には利用されません。Users に割り当てている範囲と重ならないように設定します。
  - Password hash type: ユーザのパスワードの暗号化方式を指定します。通常はデフォルトの「SSHA」で問題ありません。
- Samba3
  - Time zone:「GMT+09」を選択します。(Samba3 用の設定を削除している場合は表示されません。)
- Unix
  - Groups:グループ作成時に割り当てる GID の最小値と最大値を設定します。
- List settings
  - LDAP のエントリを表示する際に、一度に表示するエントリ数です。最大 100 エントリの表示まで選択することが可能です。
- Language settings
  - Default language : 日本語(日本)を選択します。
- Script settings
  - Server list
    - ホームディレクトリの自動作成を行う場合に、対象となるサーバを指定します。LAM が動作するホストにホームディレクトリを作成する場合は、「127.0.0.1」を指定します。
  - Path to external script
    - ホームディレクトリの自動作成を行う場合に、ホームディレクトリの自動作成を行うスクリプトを指定します。弊社提供パッケージでは、「/var/www/html/lam/lib/lamdaemon.pl」を指定してください。
  - Rights for the home directory

- ホームディレクトリの自動作成時に、ホームディレクトリに設定するパーミッションを設定します。

- Security settings
  - List of valid users
    - LAM にログインすることを許可するユーザの DN を設定します。本ドキュメントでは設定例として、slapd.conf に設定した”uid=Manager,ou=People,dc=example,dc=jp”のエントリを設定します。
  - New passwor
    - 現在ログインしている LDAP の基本設定画面にログインするためのパスワードを変更する場合に、新しいパスワードを入力します。本ドキュメントでは、デフォルトで設定されている”lam”を“secret”に変更します。

以上の設定を終えたら、画面下部の「OK」ボタンをクリックします。正常に変更が完了すれば、図 4.7 が表示されます。

図 4.7: lam.conf の設定変更に成功

画面下部の「Back to Login」をクリックし、LAM のログイン画面に戻ります。

図 4.7 が表示されずエラーが表示される場合には、lam.conf ファイルの所有者が apache ユーザになっているか確認してください。

5. LAM の利用

基本設定が完了したら、LAM を利用することができます。

http://localhost/lam/index.html

にアクセスして、LAM のログイン画面(図 5.1)を表示します。

図 5.1: LAM のログイン画面

LAM の基本設定で設定したユーザ(uid=Manager,ou=People, dc=example, dc=jp)名が「ユーザ名」の選択肢に表示されていますので、基本設定で設定したパスワードを入力し、「ログイン」ボタンをクリックします。

初回ログイン時には、LDAP にエントリが作成されていないため、図 5.2 が表示されますので、「作成」ボタンをクリックします。

図 5.2: LDAP の初期エントリの作成

LDAP エントリの作成に成功すると、図 5.3 が表示されます。

図 5.3: LDAP エントリの作成に成功

作成された LDAP エントリを確認するために、「ツリービュー」をクリックします。

図 5.4:ツリービューによる表示

6. ユーザー・グループ管理操作

6.1 グループ作成

LAM でグループエントリを作成したい場合、画面上部の「グループ」をクリックします。

図 6.1: グループ管理

最初はグループエントリが存在しないため、「グループが見つかりません!」のメッセージが表示されます。そこで、「新しいグループ」ボタンをクリックし、グループの作成を行います。

図 6.2: グループの新規作成

図 6.2 のように、「ページ unix の必須属性を全て設定してください」と表示されますので、画面左部分の「unix」のボタンをクリックします。

図 6.3: グループの UNIX 属性の設定

図 6.3 が表示されますので、「グループ名」を入力します。GID 番号は自動的に割り振られますので、通常は変更する必要はありません。グループ名を入力し終えたら、画面左部の「メイン」をクリックします。

メインページに戻ると、図 6.4 のように「アカウント作成」のボタンが有効になっていますので、「アカウント作成」をクリックします。

図 6.4: グループアカウントの作成

アカウントの作成に成功すると、図 6.5 が表示されます。さらにグループを作成する場合は、「他のアカウントを作成」ボタンをクリックします。グループ一覧を表示したい場合は、「アカウント一覧に戻る」をクリックします。

図 6.5: グループアカウントの作成に成功

グループアカウントの一覧画面に戻ると、図 6.6 のように作成したグループの情報が表示されます。

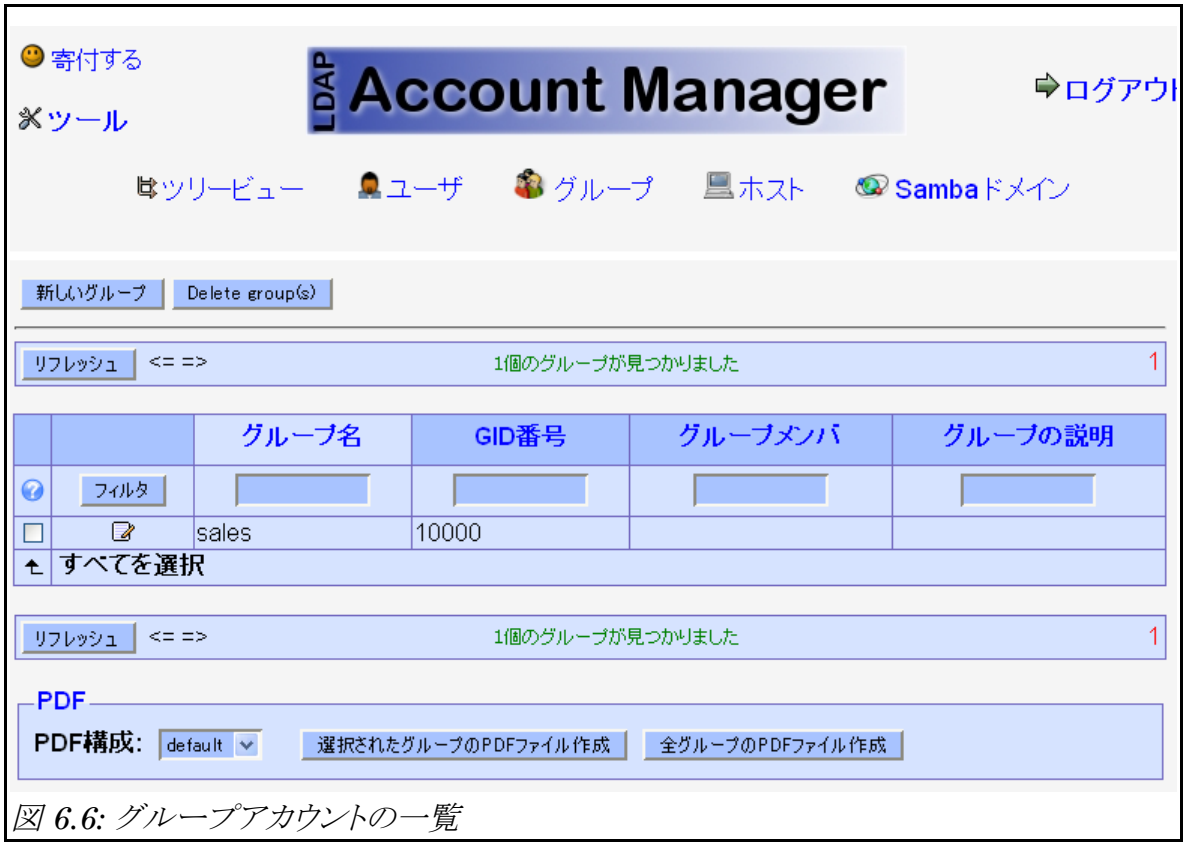

図 6.6: グループアカウントの一覧

6.2 グループ削除

LDAP に登録されているグループを削除したい場合、グループアカウント一覧の画面で、削除したいグループのチェックボックスにチェックを付けて、「グループを削除する」ボタンをクリックします。

図 6.7 では、「devel」グループの削除を行うために、チェックボックスにチェックをつけています。

図 6.7: 削除するグループの選択

「グループを削除する」ボタンをクリックすると、図 6.8 の確認画面が表示されますので、「削除」か「中止」のどちらかを選択します。

図 6.8: グループ削除の確認

削除を選択すると、LDAP から該当するグループエントリが削除され、図 6.9 が表示されます。

図 6.9: LDAP からグループを削除

図 6.9 が表示されると、グループの削除が完了するため、「一覧に戻る」をクリックして、グループの削除処理を終了します。

6.3 ユーザー作成

LDAP にユーザエントリを作成したい場合には、画面上部の「ユーザ」をクリックします。LDAP エントリにまだユーザエントリが作成されていない場合、図 6.10 が表示されます。

図 6.10: ユーザーエントリの一覧

ユーザアカウントを作成したい場合、「新しいユーザ」ボタンをクリックすると、図 6.11 が表示されます。

図 6.11: ユーザー情報の入力

Personal、unix の必須属性を設定するために、最初に「ページを選択」内の「Personal」ボタンをクリックします。

図 6.12: Personal 属性の入力

Personal 属性の入力項目のうち、必須項目は、「姓」のみですので、それ以外の項目の入力については任意で選択し入力してください。Personal 属性の入力が完了したら、「ページを選択」の「unix」ボタンをクリックしてください。

図 6.13: UNIX 属性の設定

図 6.13 が表示されますので、ユーザアカウントに設定する内容を、それぞれの項目に入力してください。なお、UID 番号が入力されなかった場合は、自動的に割り当てられます。

それぞれの項目の入力が終了したら、「ページを選択」のうち、「Shadow」か「メイン」をクリックします。
「Shadow」では図 6.14 で表示されているように、パスワードの有効期限などの属性を設定することができます。なお、Shadow 属性の設定は必須ではありません。

図 6.14: shadow 属性の設定

ユーザ作成に関する全ての必須属性の入力が完了すると、「メイン」ページの「アカウント作成」ボタンが有効になります(図 6.15)。入力した内容でユーザアカウントを LDAP エントリに作成する場合、「アカウント作成」ボタンをクリックします。

図 6.15: ユーザーアカウントの作成

LDAP に正常にユーザーアカウントを作成できた場合、図 6.16 が表示されます。

図 6.16: ユーザー登録の完了

さらにユーザアカウントの作成を続ける場合には、「他のアカウントを作成」を選択します。ユーザアカウントの作成を終了する場合には、「アカウント一覧に戻る」を選択します。

6.4 ユーザの削除

LDAP に登録されているユーザアカウントのエントリを作成したい場合、ユーザ一覧表示の画面から、削除したいユーザのチェックボックスにチェックを付け、「ユーザーを削除する」ボタンをクリックします。

図 6.17: ユーザー一覧から削除するユーザーを選択

図 6.17 では、ユーザ ID「yasuma」のユーザを選択しています。

「ユーザーを削除する」をクリックすると、図 6.18 の確認画面が表示されます。

図 6.18: ユーザーエントリ削除の確認

LDAP からユーザエントリを削除する場合には、「削除」ボタンをクリックしてください。 同時にユーザのホームディレクトリの削除を行う場合、「ホームディレクトリを削除」のチェックボックスにチェックを入れてください。

図 6.19:ユーザーアカウントの削除に成功

正常にユーザエントリが削除されると、図 6.19 が表示されますので、「一覧に戻る」をクリックして、ユーザ一覧の画面に戻ってください。

6.5 ユーザ情報の変更

ユーザ情報を変更したい場合、「ツリービュー」から該当するユーザを選択します。図 6.20 は、「uid=yasuma」ユーザを選択しています。

図 6.20: ユーザー情報の詳細表示

図 6.20 の右側部分に選択したユーザアカウントに設定されている各エントリの内容が表示されていますので、変更したい項目を修正し、画面下部にある「保存」ボタンをクリックして、変更内容を保存します。

図 6.21: 変更内容の確認

「保存」ボタンをクリックすると、変更箇所が図 6.21 のように表示されますので、問題なければ、「更新」ボタンをクリックします。

7. CSVによる一括登録

LAMではCSVファイルを使って一度に多数のユーザを登録することが可能です。

左上の「ツール」メニューから「ファイルのアップロード」を選択します。

図 7.1: CSV ファイルのアップデート用メニュー

ユーザを一括登録する場合は、アカウントタイプで「ユーザ」を選択します。

図 7.2: ユーザー登録用 CSV のアップロード画面

画面の中に説明がありますが、まず一番下にある「サンプル CSV ファイルをダウンロード」をクリックし、ファイルをダウンロードします。このファイルを編集してアップロードすれば良いですが、CSV の中の文字コードは UTF-8 で記述する必要があります。日本語を全く使わなければマイクロソフト社 EXCEL を利用できますが、UTF-8 に対応していないため、日本語を利用するには以下のソフトウェアを利用する必要があります。

- OpenOffice Calc : http://ja.openoffice.org/
  - UTF-8 の CSV ファイルを表形式のまま編集可能
  - 無償のオープンソース・ソフト
- 秀丸 : http://hide.maruo.co.jp/software/hidemaru.html
  - テキストファイルの編集が可能。
  - Excel で編集したファイルを UTF-8 に変換することが可能
  - シェアウェア【4,200 円(消費税込み)】
- MKEditor for Windows: http://www.mk-square.com/home/software/mkeditor/
  - テキストファイルの編集が可能。
  - Excel で編集したファイルを UTF-8 に変換することが可能
  - フリー・ソフトウェア

上記のソフトウェアを使って編集し、保存ください。特に OpenOffice Calc は保存する時に文字コードを

UTF-8 にすることを忘れないでください。また Excel でファイル編集した場合は秀丸や MKEditor for Windows などで文字コードを UTF-8 に変更してください。

Linux の上で文字コードを UTF-8 に変換する場合は以下のコマンドで行えます。

```
# iconv -f cp932 -t utf-8 < 入力ファイル > 出力ファイル
```

上記で -f cp932 は入力ファイルが Windows ファイルコード（SJIS 系）を利用しており、-t utf-8 は UTF-8 へ変換することを意味しています。

なお CSV ファイルの中で以下の項目は日本語ではなく、半角英数字を使うようにしてください。

- dn_suffix
- dn_rdn
- inetOrgoersin_manager
- inetOrgPerson_email
- posixAccount_username
- posixAccount_group
- posixAccount_addtitionalGroups
- posixAccount_homedir
- posixAccount_shell
- posixAccount_password
- posixAccount_passwordDisabled
- SambaSamAccount_Group

CSV ファイルが作成できたら図の画面からファイルをアップロードすることができます。

図 7.3.: CSV ファイルのアップロード

8. RedHat EL 4, CentOS 4 での LDAP 基本設定

LAM で作成した LDAP エントリを利用するためには、OS で LDAP のエントリを参照する設定が必要になります。RedHat Enterprise Linux 4、および CentOS4 では、authconfig コマンドで LDAP 参照の設定を行うことができます。

端末上で、root 権限で authconfig コマンドを実行します。

```
# authconfig
```

図 8.1 の設定画面で、「ユーザ情報」として「LDAP を使用」、「認証」として、「LDAP 認証を使用」にチェックを付け、「次」を選択します。

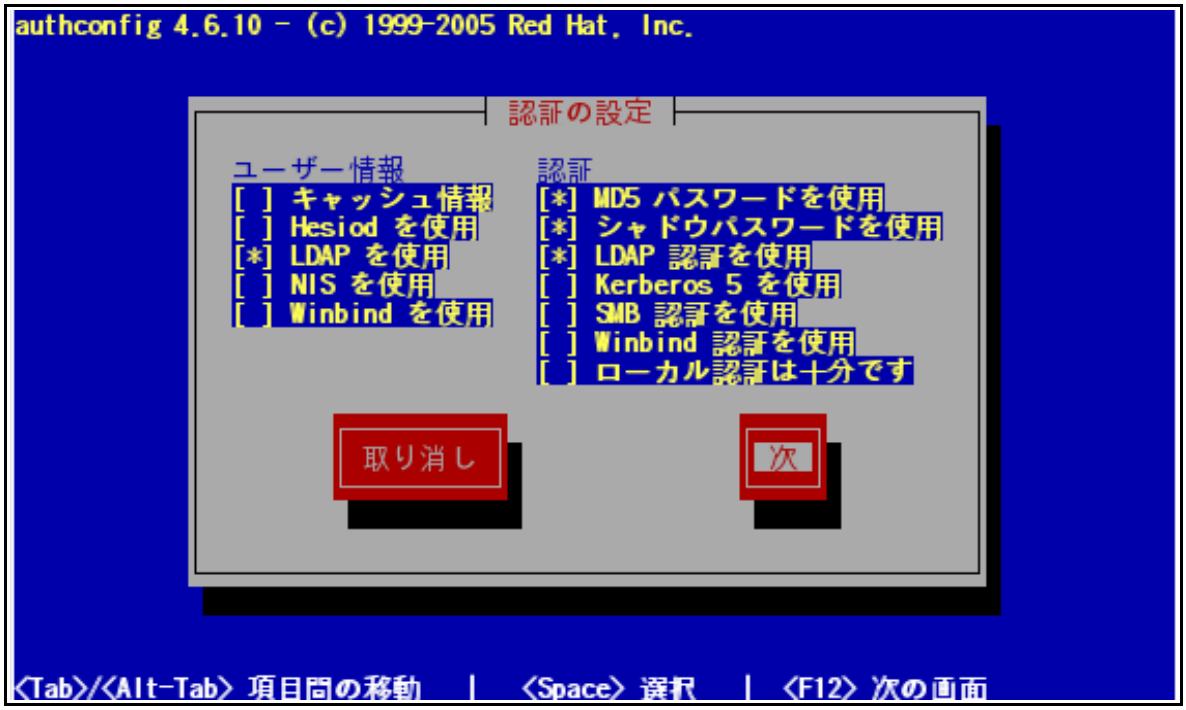

図 8.1: LDAP 利用のための設定

図 8.2 では、TLS 使用の有無、LDAP サーバの IP アドレス、および、LDAP のベース DN を指定します。本ドキュメントの環境では、ベース DN として、”dc=example,dc=jp”を設定することになります。

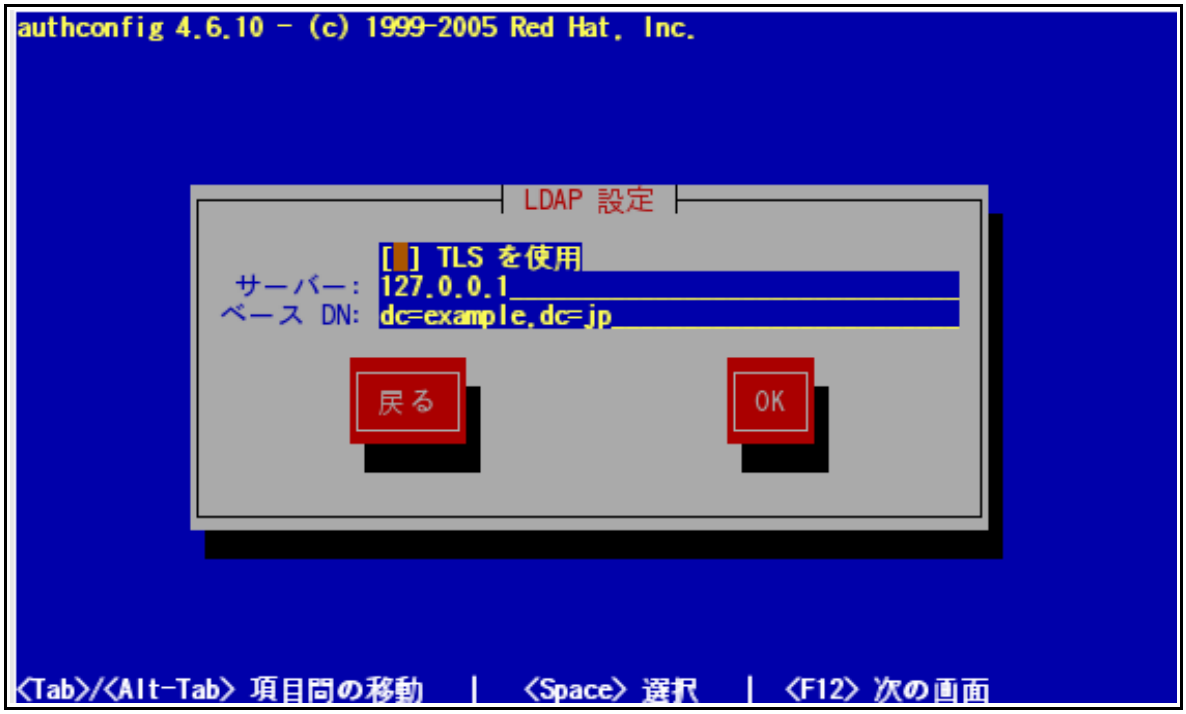

図 8.2: LDAP サーバーへの接続設定