OSSTech 製

LDAP Account Manager

管理者ガイド

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 : 2010 年 1 月 20 日

リビジョン: 3.1

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 5、 CentOS5、Solairs10 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 rpm パッケージ一式を提供します。

各 OS ごとのインストール手順に従って、パッケージのインストールを実施してください。

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
```

続いて、弊社提供の rpm パッケージをインストールします。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
```

2.1.1 提供パッケージ一覧

x86-64 版の場合は、下記の i386 の部分を x86_64 と読み替えてください。 パッケージのバージョン番号等は、バージョンアップ等に伴い変更されることがあります。

- osstech-base-2.0.0-40.el5.noarch.rpm
- osstech-support-2.0.0-40.el5.noarch.rpm
- osstech-ldap-account-manager-2.4.0-1.2.el5.noarch.rpm
- osstech-libssh2-0.18-3.el5.i386.rpm
- osstech-php-ssh2-5.1.6-3.1.el5.i386.rpm
- osstech-perl-Quota-1.6.2-1.el5.i386.rpm

2.2 Solaris10

弊社提供の Solaris 版 LAM は、rpm 形式で提供します。

そのため、まず最初に Solaris10 用の rpm 環境を導入する必要があります。

弊社提供のパッケージを Solaris10 で展開し、次のコマンドで rpm 環境を構築します。

パッケージ一式を展開したディレクトリに移動し、root ユーザーで次のコマンドを実行します。

```
#  ./bootstrap/osstech-bootstrap.ksh  ./bootstrap
osstech-bootstrap.ksh: INFO: Extracting RPM packages by rpm2cpio and cpio ...
osstech-base-2.0.0-21.sol10.noarch.rpm
81 blocks
osstech-rpm-4.4.2.3-2.15.sol10.i386.rpm
7133 blocks
osstech-rpm-libs-4.4.2.3-2.15.sol10.i386.rpm
17550 blocks
osstech-bootstrap.ksh: INFO: Initializing RPM database ...
osstech-bootstrap.ksh: INFO: Installing RPM packages by rpm ...
Preparing packages for installation...
osstech-base-2.0.0-21.sol10
osstech-rpm-4.4.2.3-2.15.sol10
osstech-logrotate-3.7.7-1.3.sol10
osstech-rpm-build-4.4.2.3-2.15.sol10
osstech-rpm-devel-4.4.2.3-2.15.sol10
osstech-rpm-libs-4.4.2.3-2.15.sol10
osstech-rpm-python-4.4.2.3-2.15.sol10
osstech-support-2.0.0-21.sol10
osstech-bootstrap.ksh: INFO: Done.
```

以上で、Solaris 用 RPM 環境の導入は完了です。

/opt/osstech/bin/rpm コマンドで、rpm 環境の操作を行うことが可能です。

続いて、LAM 関連パッケージ一式をインストールします。

```
# /opt/osstech/bin/rpm  -ihv  lam/*.rpm
```

以上で、パッケージの導入は完了です。

2.2.1 提供パッケージ一覧

Sparc 版の場合は、下記の i386 の部分を sparc と読み替えてください。 パッケージのバージョン番号等は、バージョンアップ等に伴い変更されることがあります。

- osstech-ldap-account-manager-2.4.0-1.6.sol10.noarch.rpm
- osstech-libssh2-0.18-3.sol10.i386.rpm
- osstech-m4-1.4.11-1.2.sol10.i386.rpm

- osstech-pcre-7.8-0.1.sol10.i386.rpm
- osstech-pcre-devel-7.8-0.1.sol10.i386.rpm
- osstech-php-5.2.8-2.8.sol10.i386.rpm
- osstech-php-bcmath-5.2.8-2.8.sol10.i386.rpm
- osstech-php-cli-5.2.8-2.8.sol10.i386.rpm
- osstech-php-common-5.2.8-2.8.sol10.i386.rpm
- osstech-php-dba-5.2.8-2.8.sol10.i386.rpm
- osstech-php-devel-5.2.8-2.8.sol10.i386.rpm
- osstech-php-ldap-5.2.8-2.8.sol10.i386.rpm
- osstech-php-mbstring-5.2.8-2.8.sol10.i386.rpm
- osstech-php-mysql-5.2.8-2.8.sol10.i386.rpm
- osstech-php-pdo-5.2.8-2.8.sol10.i386.rpm
- osstech-php-pgsql-5.2.8-2.8.sol10.i386.rpm
- osstech-php-pspell-5.2.8-2.8.sol10.i386.rpm
- osstech-php-snmp-5.2.8-2.8.sol10.i386.rpm
- osstech-php-soap-5.2.8-2.8.sol10.i386.rpm
- osstech-php-ssh2-5.2.8-3.2.sol10.i386.rpm
- osstech-php-xml-5.2.8-2.8.sol10.i386.rpm
- osstech-php-xmlrpc-5.2.8-2.8.sol10.i386.rpm
- osstech-sudo-1.6.9p17-2.1.sol10.i386.rpm
- osstech-autoconf-2.61-0.2.sol10.noarch.rpm
- osstech-automake-1.10.1-0.3.sol10.noarch.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 = 128M
```

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、

/opt/osstech/lib/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:/opt/osstech/lib/lam/lib/lamdaemon.pl
```

また「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「/opt/osstech/lib/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。

3.4.1 RHEL5/CentOS5 の場合

service コマンドで 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
```

3.4.2 Solaris10 の場合

Web サーバーの設定が行われていない場合、サンプルの設定ファイルとして Solaris10 が提供している /etc/apache2/httpd.conf-example を参考に/etc/apache2/httpd.conf を作成します。

```
#  cp  /etc/apache2/httpd.conf-example  /etc/apache2/httpd.conf
```

PHP、および LAM の設定を有効にするために、/etc/apache2/httpd.conf の一番最後に、次の設定を追加します。

```
Include /opt/osstech/etc/apache2/conf.d/php.conf
Include  /opt/osstech/etc/apache2/conf.d/ldap-account-manager.conf
```

svcadm コマンドで Web サーバーを起動します。

```
#  svcadm  enable  apache2
```

Web サーバーを停止させたいときは、次のコマンドを実行します。

```
#  svcadm  disable apache2
```

Web サーバーが起動しないときなど、ステータスを確認したいときは、次のコマンドを実行します。

```
#  svcs  -xv  apache2
```

4. LAM の基本設定

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。

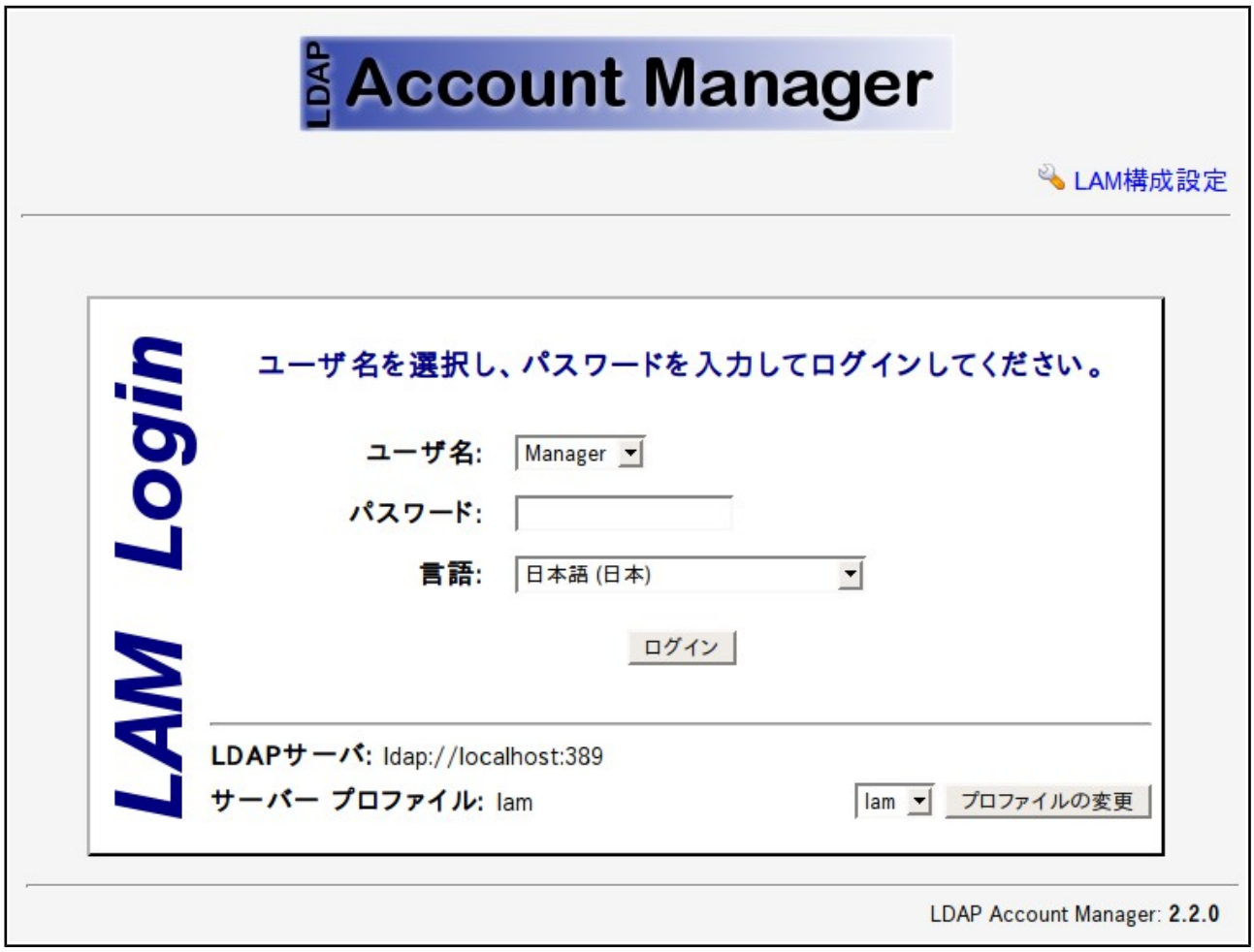

図 4.1.: LAM のログイン画面

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 構成設定」をクリックし、図 4.2 に移ります。

図 4.2.: LAM 構成設定の選択画面

図 4.2 では、**「サーバープロファイルの編集」**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。

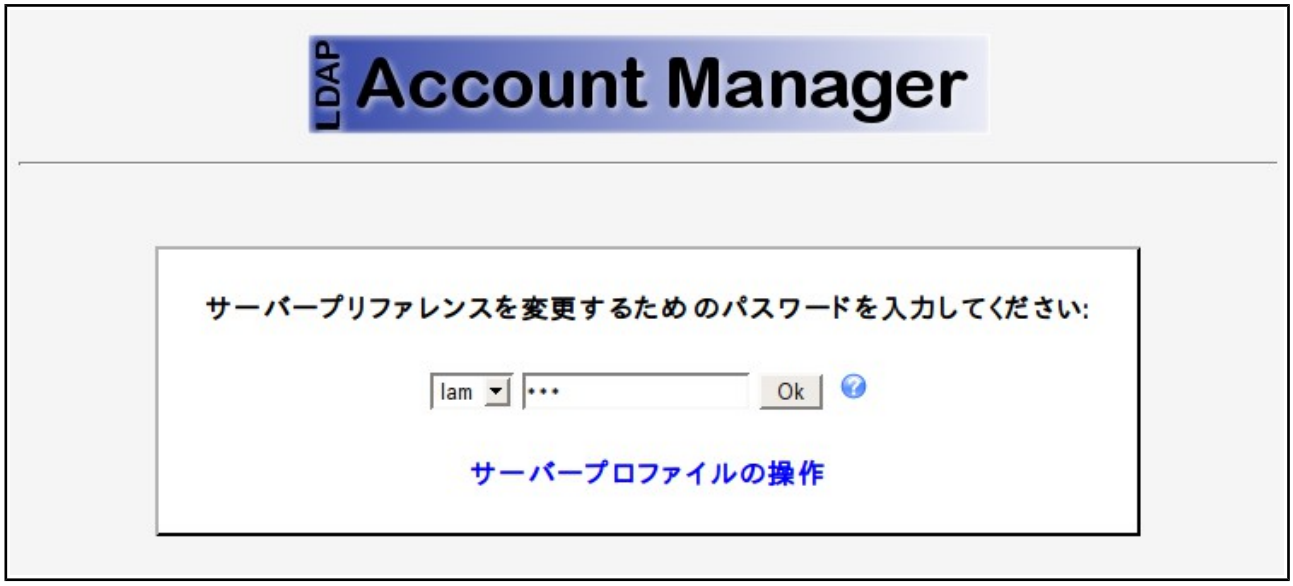

図 4.3.: LAM の管理者パスワードの入力

パスワードの認証が正常に行われると、管理する LDAP 関連の基本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 が起動されているものとします。

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「**アカウント種別とモジュール**」の「**モジュールの編集**」をクリックし、図 4.5 を表示させます。

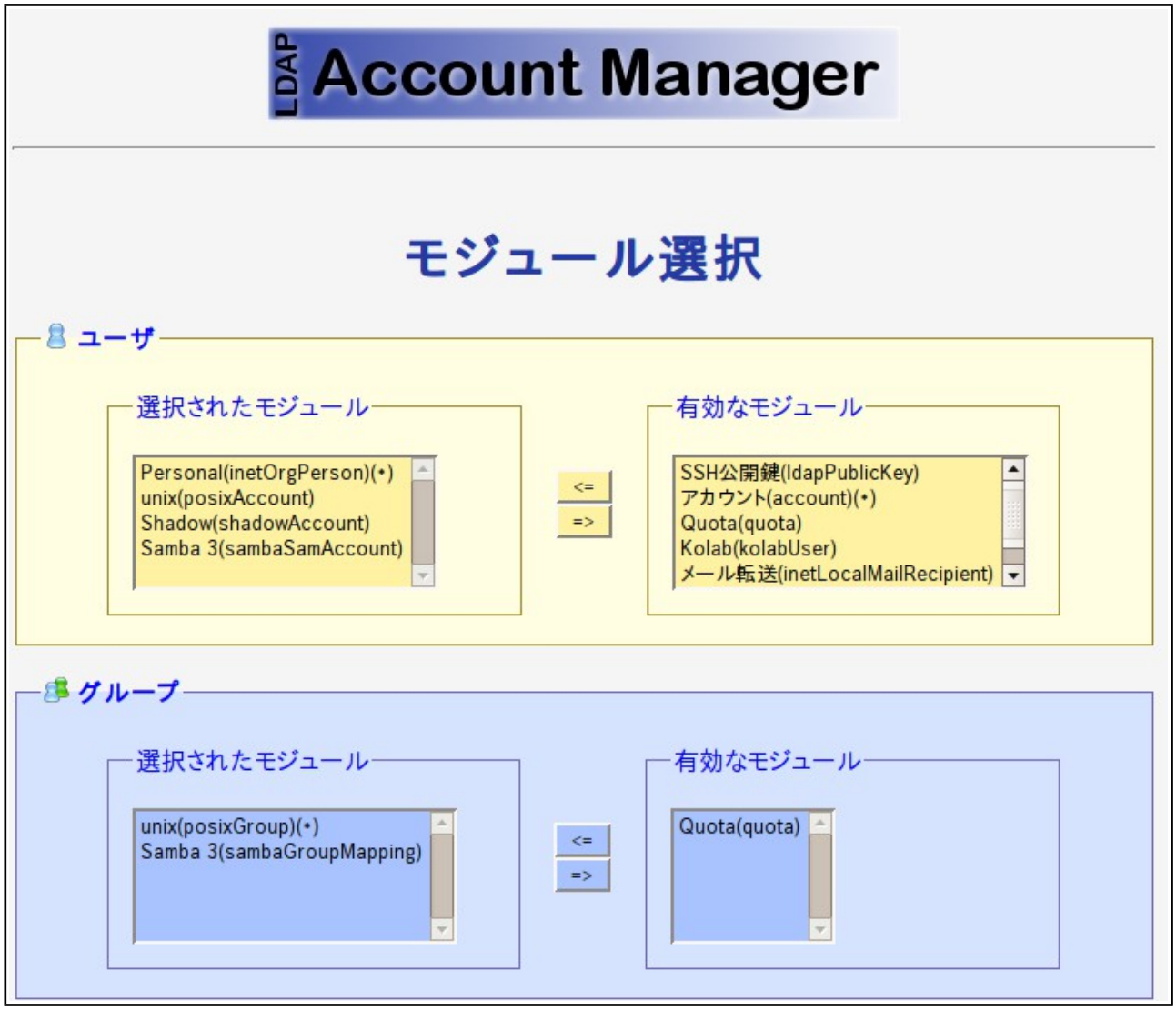

図 4.5.: モジュール選択

図 4.5 では、LDAP Account Manager で管理するユーザ、グループなどに設定する 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 との連携用の設定となっています。

運用環境で Samba 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。

- ユーザー
  - Samba 3(sambaSamAccount)の削除
- グループ
  - Samba 3(sambaGroupMapping)の削除
- ホスト

- Samba 3(sambaSamAccount)の削除

LAM から Quota の設定を行いたい場合は、図 4.6 に示すように、モジュール種別のユーザ、グループのそれぞれの Quota モジュールを有効にし、「選択されたモジュール」に含まれるようにします。

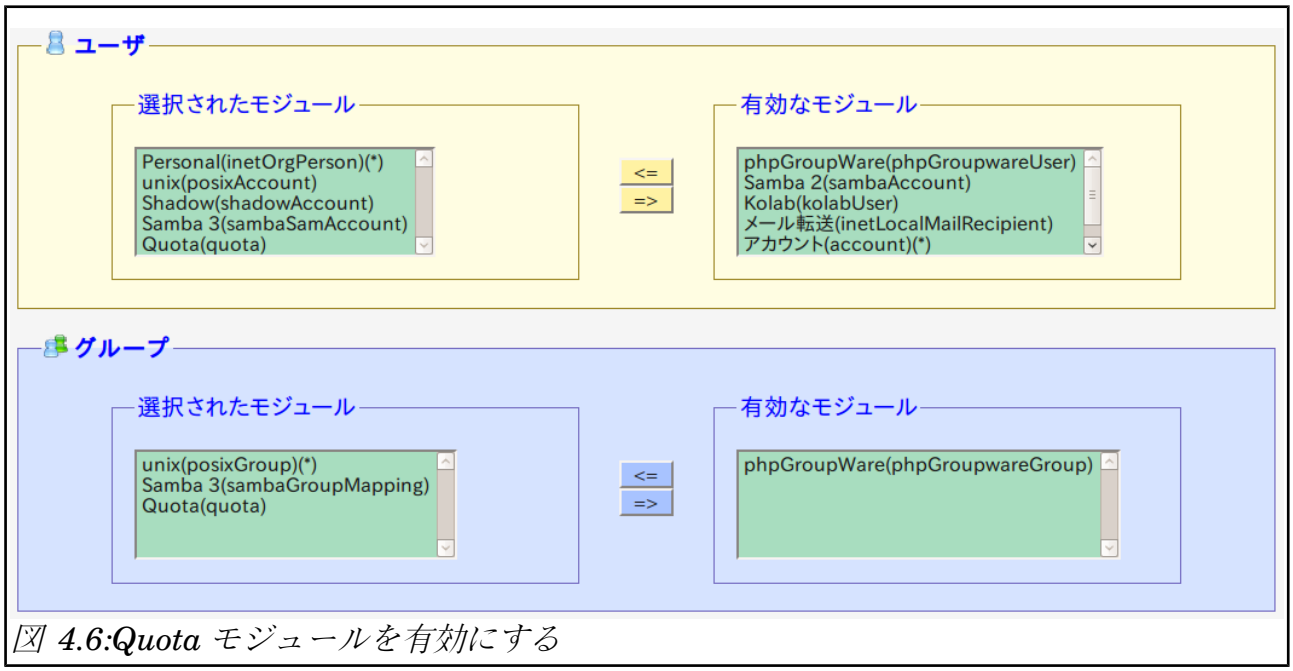

図 4.6:Quota モジュールを有効にする

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「**アカウント種別とモジュール**」の「**アカウント種別の編集**」をクリックし、図 4.7 を表示させます。

図 4.7.: アカウント種別の設定

ユーザー、グループ、ホスト、Samba ドメインの各項目の 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。

- ユーザー: ou=Users,dc=example,dc=jp
- グループ: ou=Groups,dc=example,dc=jp
- ホスト: ou=Computers,dc=example,dc=jp
- Samba ドメイン : ou=domains,dc=example,dc=jp

属性の一覧に設定されている属性は、LAM で一覧表示した際に表示される項目です。

ユーザーの「属性の一覧」に含まれる#givenName、#sn の属性ですが、日本語表記にあわせるため「#sn,#givenName」の順番に設定してあることを確認してください。

以上の設定を終えたら、図 4.7 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。

- サーバー設定
  - サーバーアドレス : ldap://localhost:389 (デフォルト値のまま)
  - ツリーサフィックス : dc=example,dc=jp (運用環境の slapd.conf の suffix に合わせます)
  - キャッシュ有効時間 : 5 分 (LAM が保持する LDAP のキャッシュを更新する間隔です。)
- アカウント種別とモジュール:
  - 詳細については既に説明しました。
- Unix
  - ユーザー : 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。
  - ホスト : 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。ユーザーに割り当てている範囲と重ならないように設定します。
  - パスワードハッシュ形式 : 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
  - タイムゾーン : 「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
  - グループ :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。
- 言語の設定
  - 規定の言語 : 日本語(日本)を選択します。
- スクリプト設定
  - サーバー一覧
    - 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。
  - 外部スクリプトのパス
    - 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、「/opt/osstech/var/lib/lam/lib/lamdaemon.pl」を指定してください。
  - ホームディレクトリに対する権限
    - 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。

- セキュリティ設定
  - 有効なユーザーのリスト
    - 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=Users,dc=example,dc=jp”のエントリを設定します。
  - 新しいパスワード
    - 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 4.8 が表示されます。

図 4.8.: lam.conf の設定変更を完了

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

図 4.8 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 (Solaris の場合は webservd)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 5.2)を表示します。

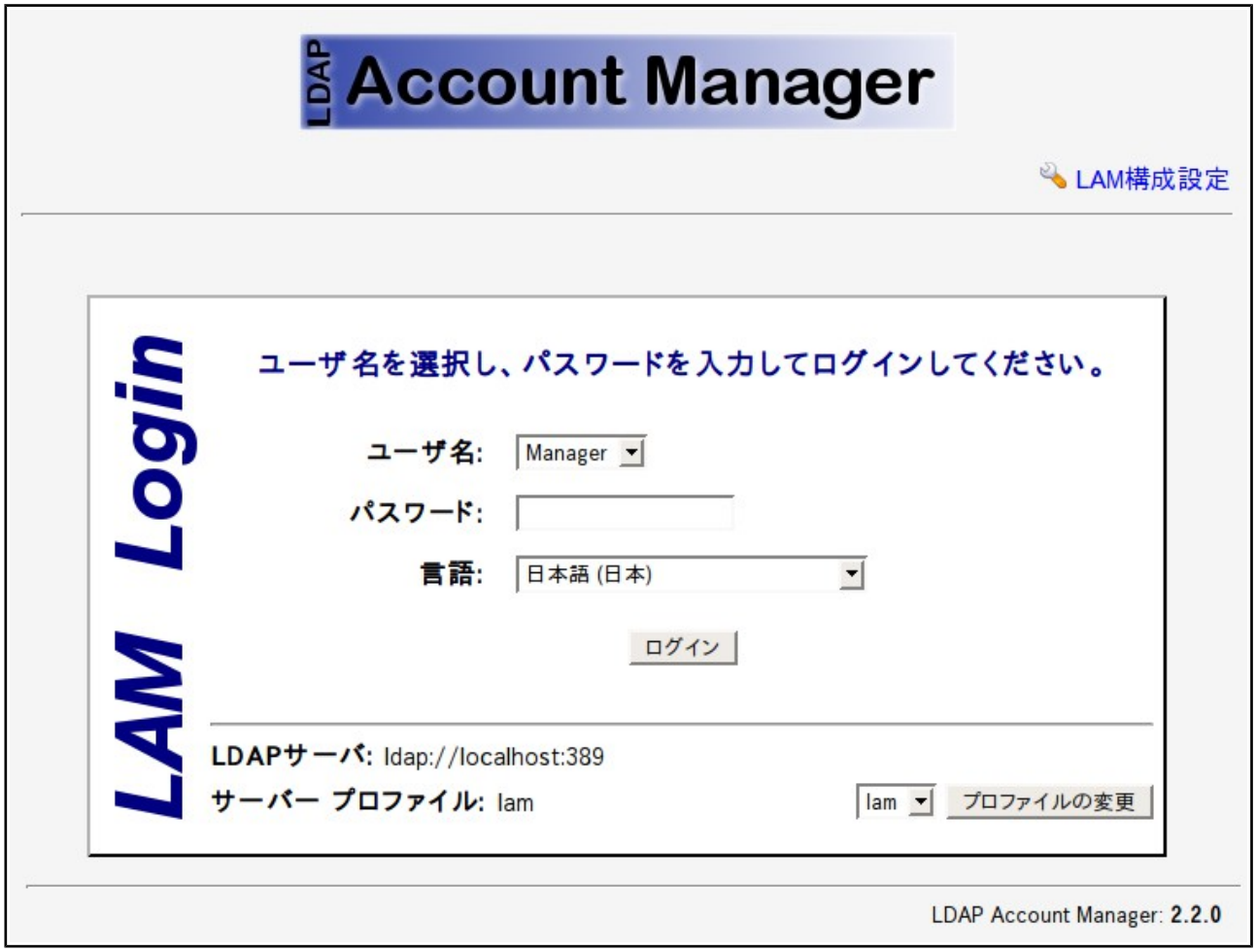

図 5.1.: LAM のログイン画面

LAM の基本設定で設定したユーザ(uid=Manager,ou=Users,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.: ツリービューの表示

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.: グループの作成

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。

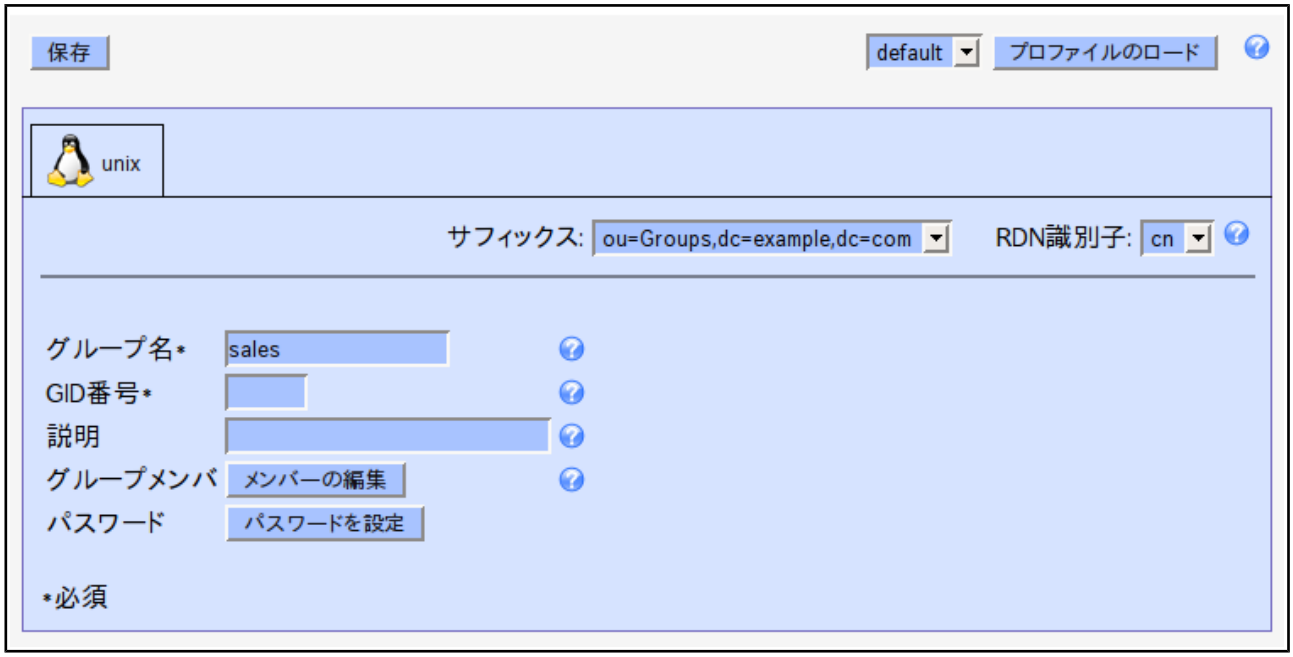

図 6.2.: グループの UNIX 属性の設定

図 6.2 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。

Samba のアカウントも管理する場合は、Samba3 属性も入力します。

各モジュール種別の「＊必須」の項目は全て設定する必要があります。

ホームディレクトリの作成機能を設定済みで、Quota モジュールを有効にしている場合は、Quota タブより Quota の設定が可能です。

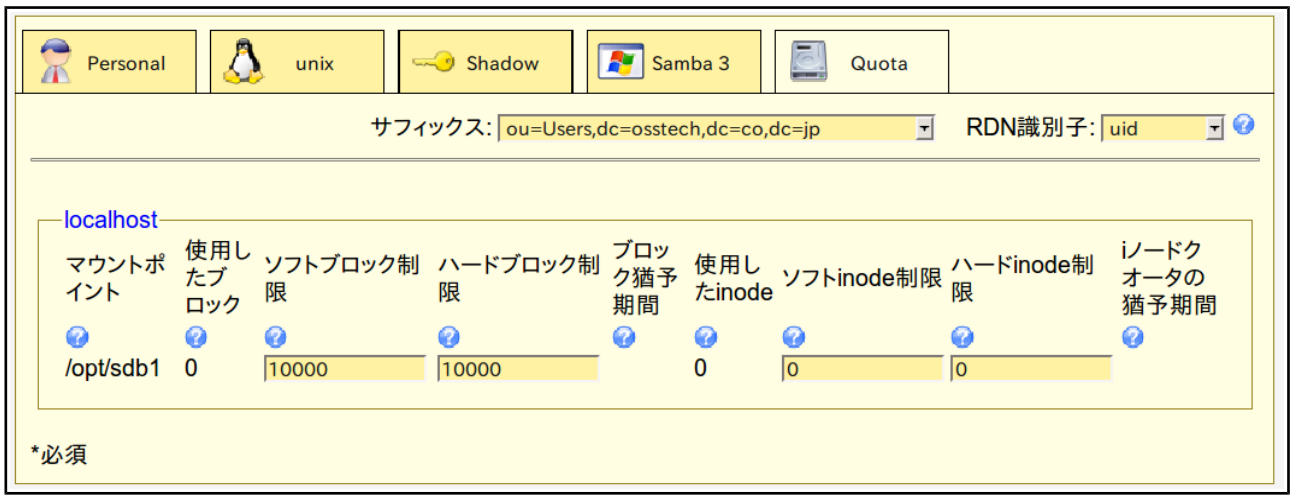

図 6.3:Quota の設定

全てのモジュールで必要な項目の設定を終えたら、「保存」ボタンをクリックします。

図 6.4.: アカウントの登録成功

アカウントの作成に成功すると、図 6.4 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。

グループアカウントの一覧画面に戻ると、図 6.5 のように作成したグループの情報が表示されます。

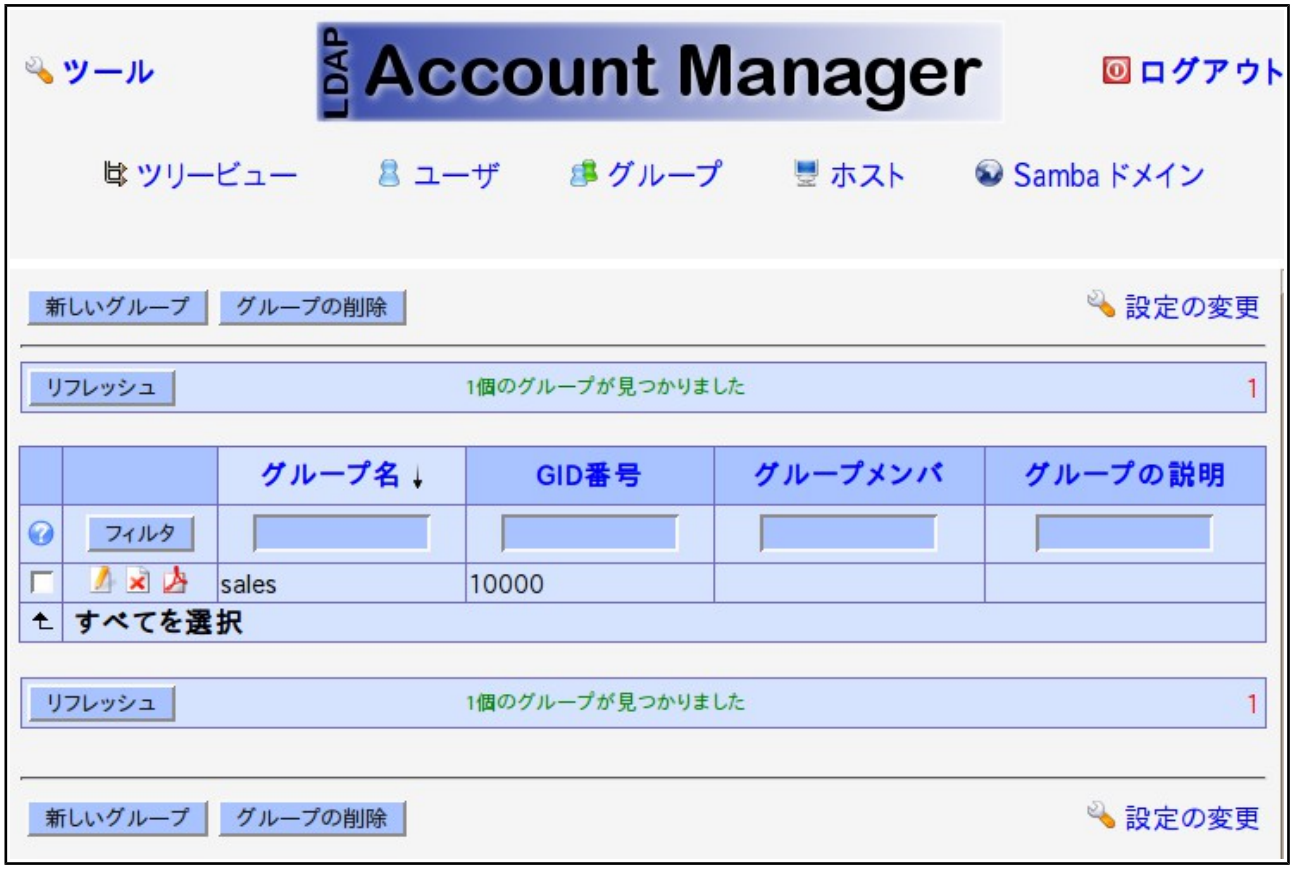

図 6.5.: グループアカウント一覧

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。

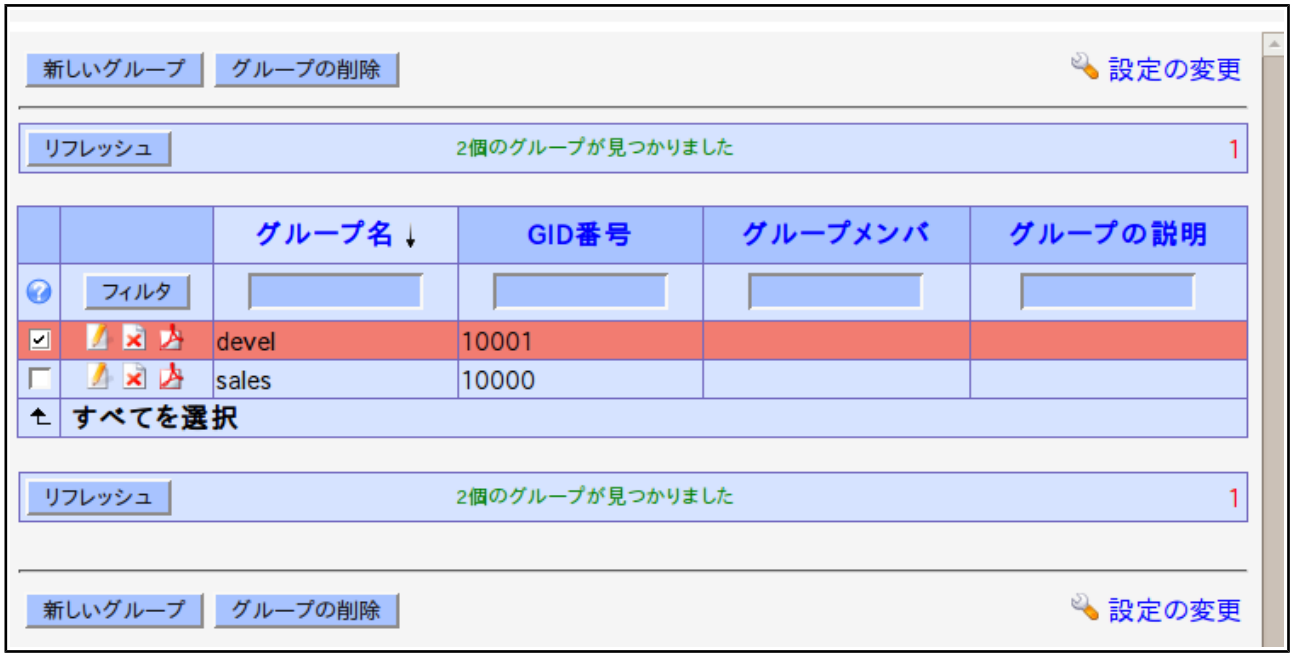

図 6.6.: 削除するグループの選択

図 6.6 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。

「グループを削除する」ボタンをクリックすると、図 6.7 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。

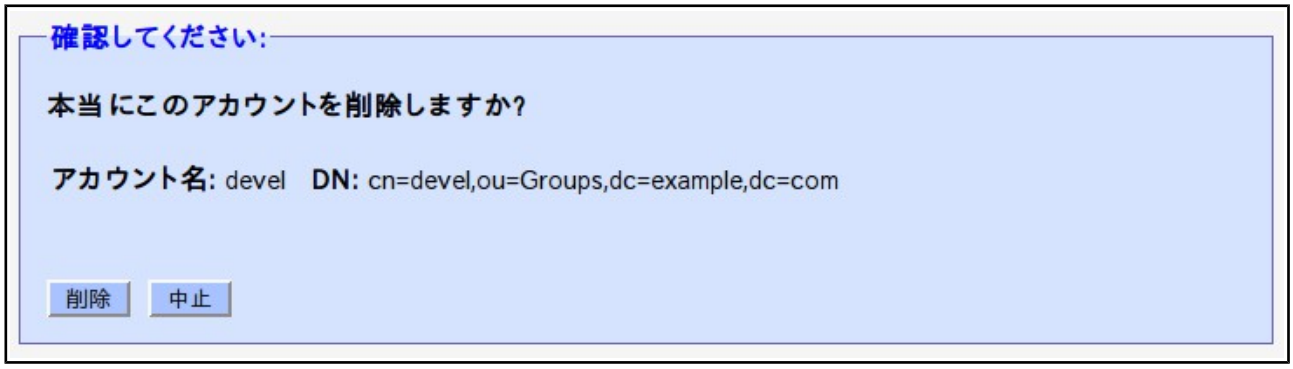

図 6.7.: グループ削除の確認

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 6.8 が表示されます。

図 6.8.: グループ削除の完了

図 6.8 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 6.9 が表示されます。

図 6.9.: ユーザー一覧の表示

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 6.10 が表示されます。

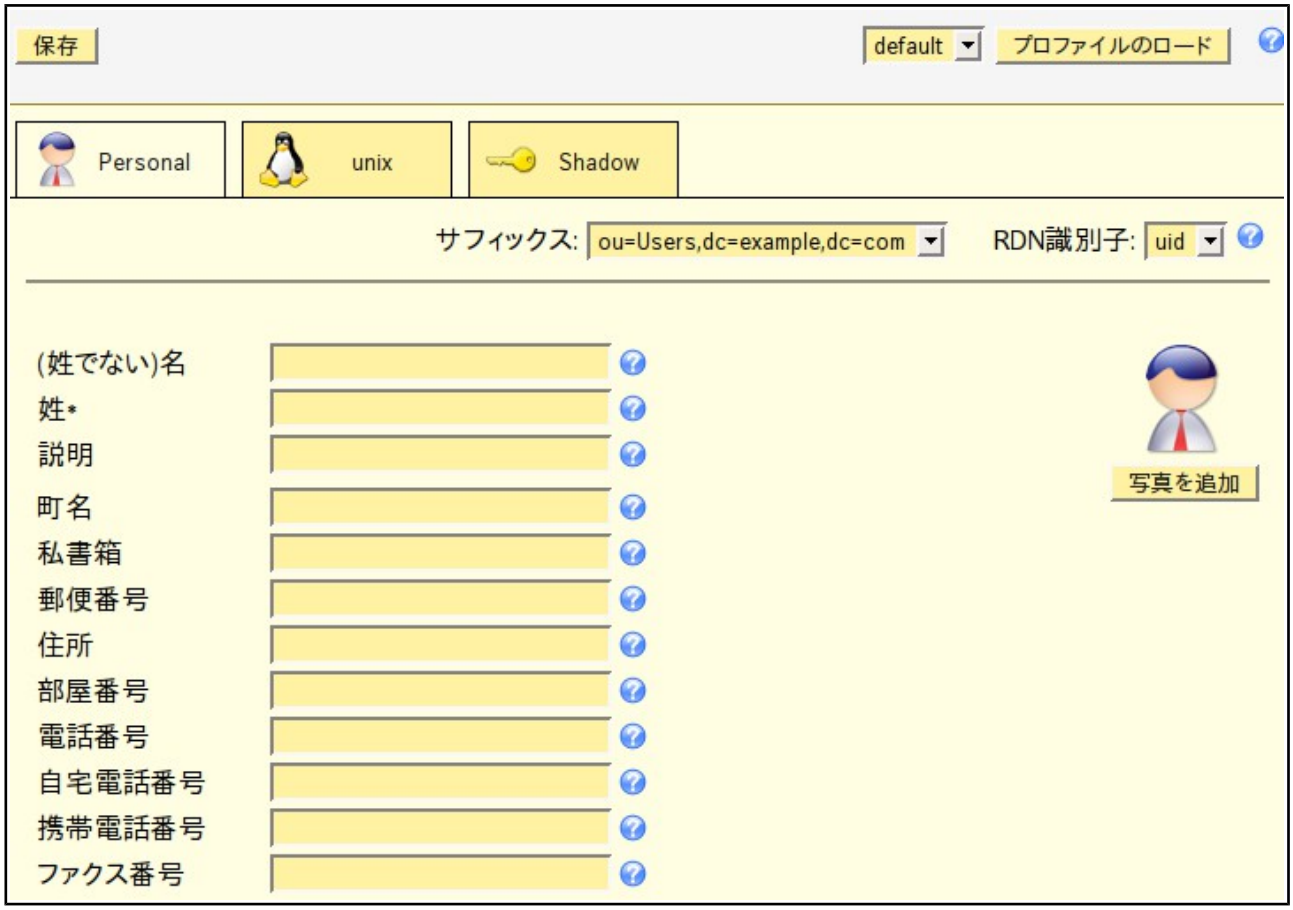

図 6.10.: Personal 属性の設定

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、ページ上部の「unix」ボタンをクリックしてください。

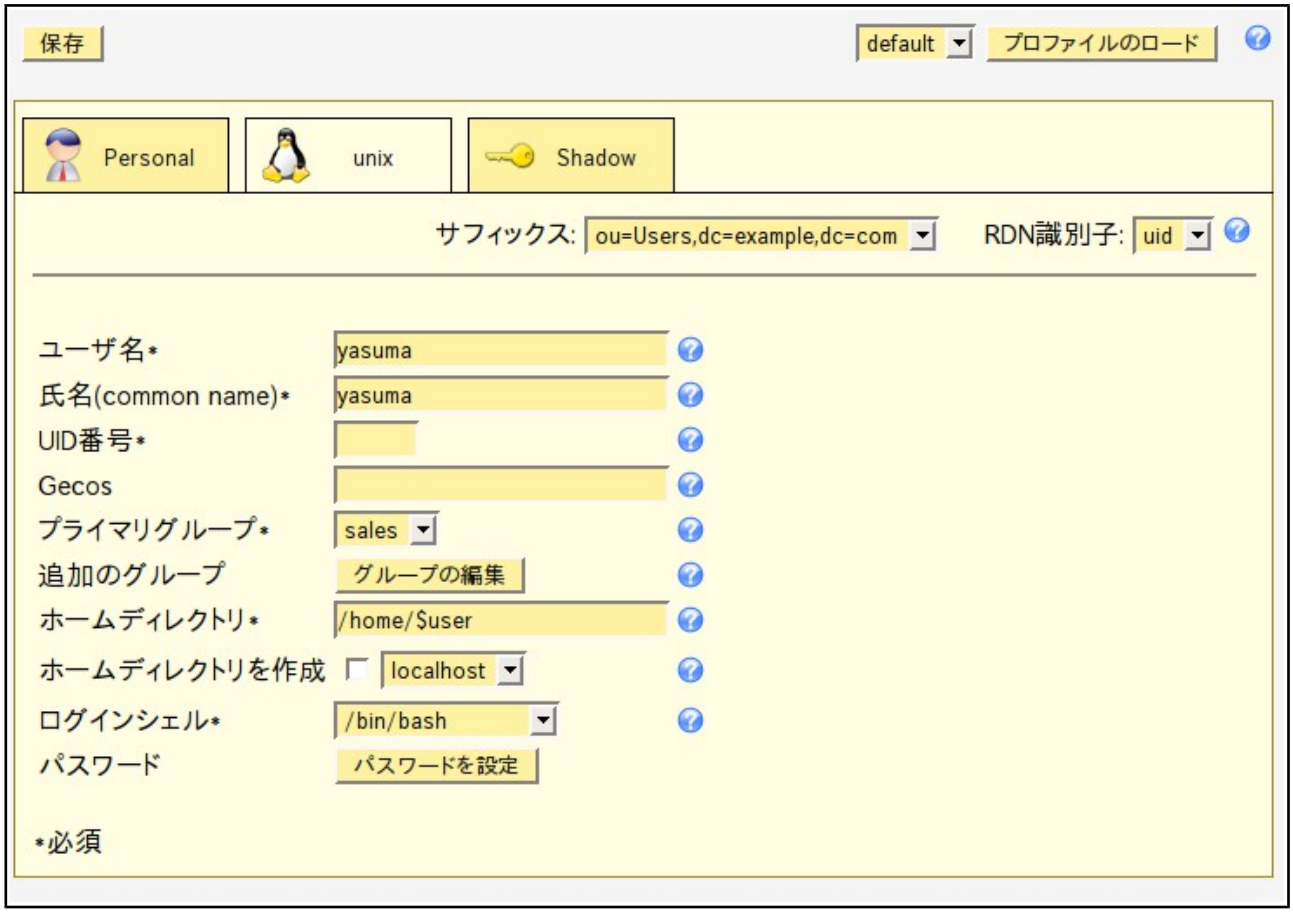

図 6.11.: unix 属性の設定

図 6.11 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、「Shadow」をクリックします。「Shadow」では図 6.12 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。

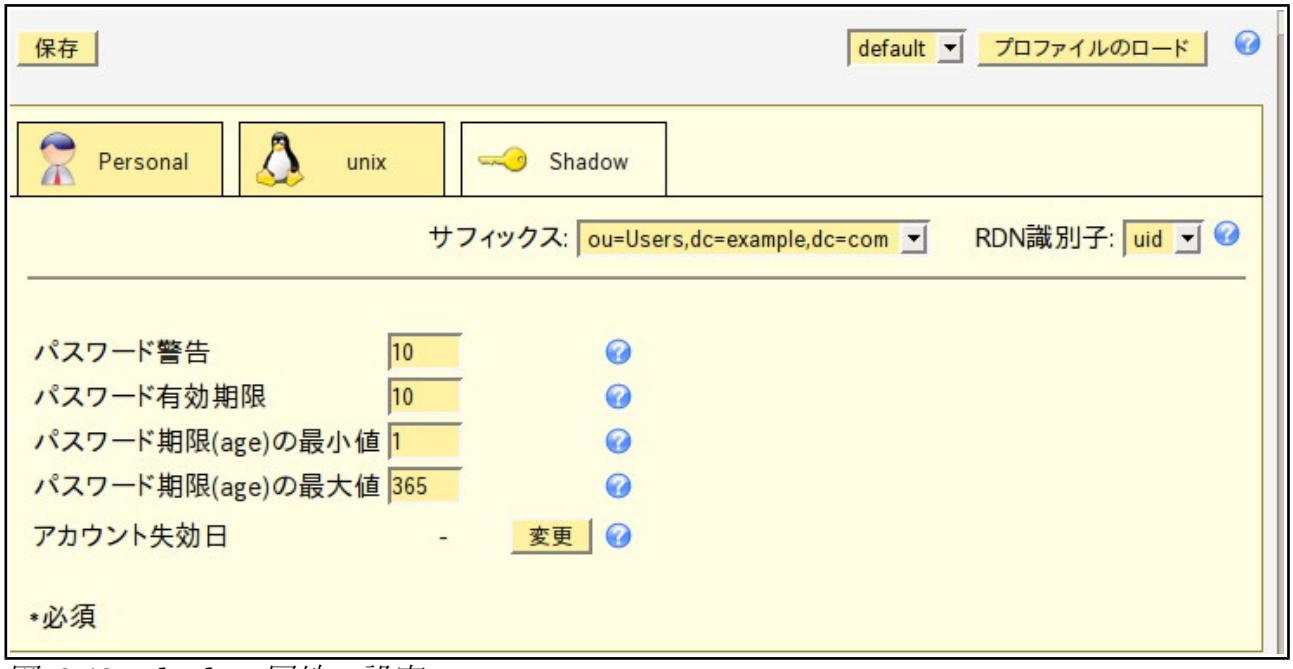

図 6.12.: shadow 属性の設定

ユーザ作成に関する全ての必須属性の入力が完了したら、ページ上部の「保存」ボタンをクリックしてください。

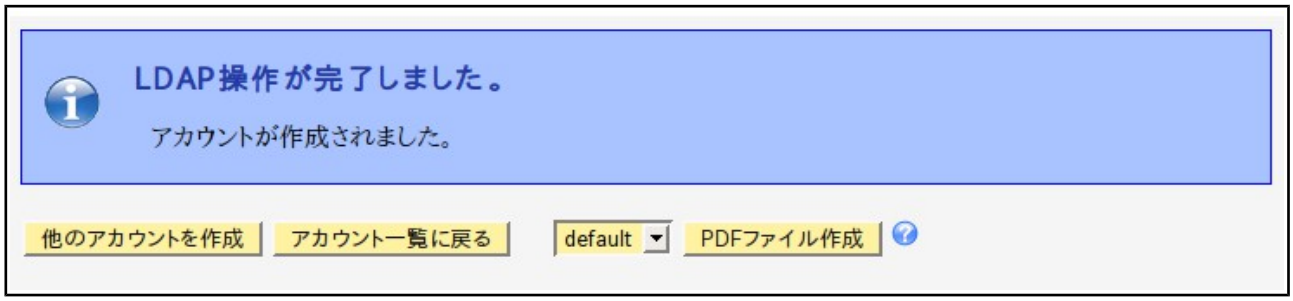

図 6.13.: ユーザーアカウントの作成完了

LDAP に正常にユーザーアカウントを作成できた場合、図 6.13 が表示されます。

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。

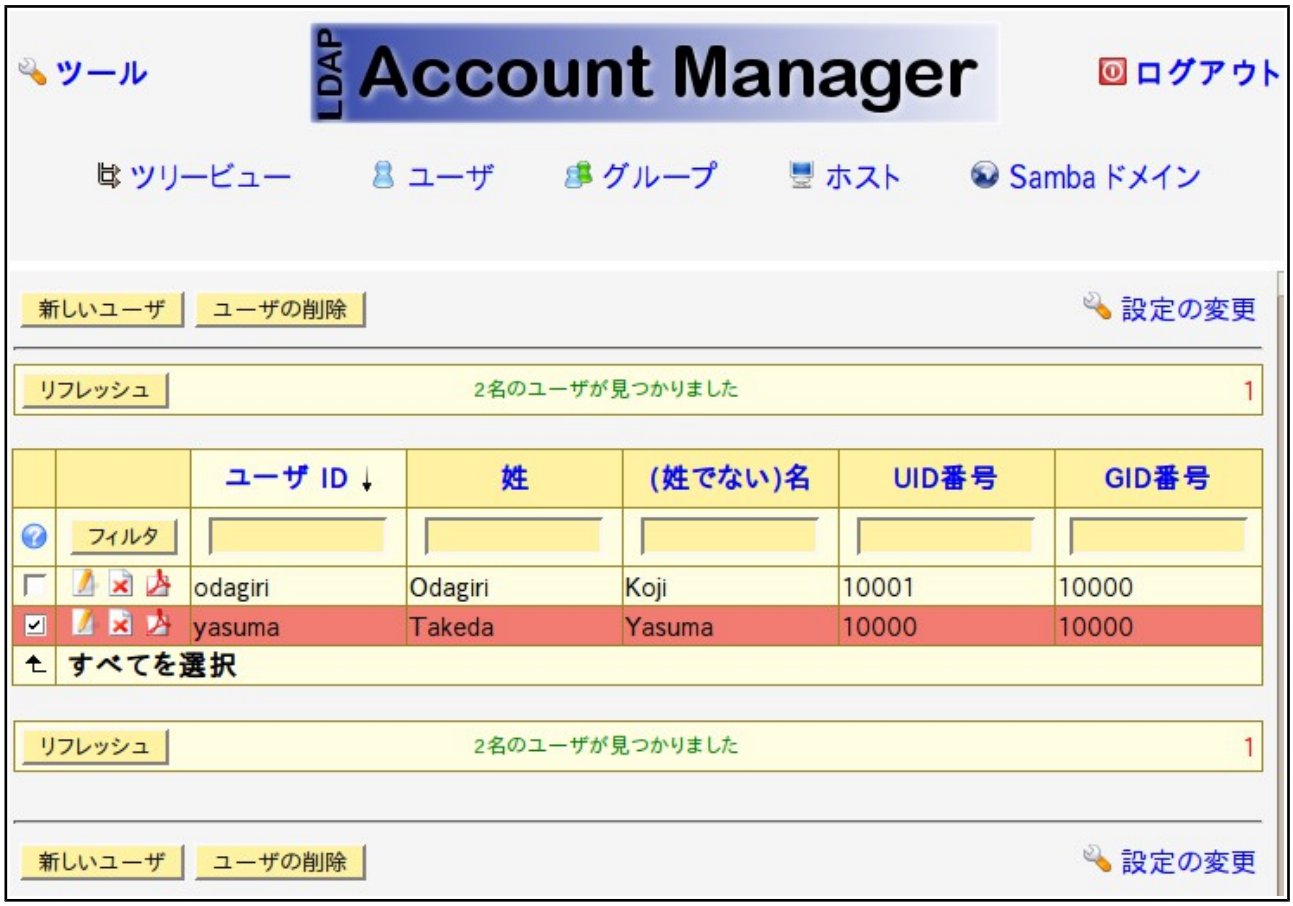

図 6.14.: ユーザーの削除

図 6.14 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 6.15 の確認画面が表示されます。

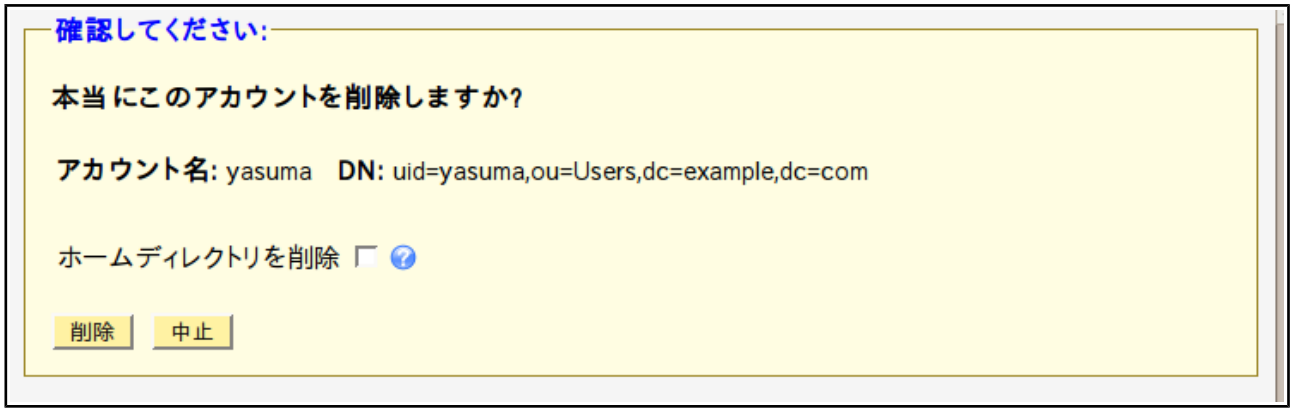

図 6.15.: ユーザー削除の確認

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 6.16.: ユーザーの削除に成功

正常にユーザエントリが削除されると、図 6.16 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

登録されている情報を変更したい場合、「ユーザー」、「グループ」などの一覧から該当するユーザを選択し、登録内容を変更します。

さらに詳細な LDAP のデーターを変更したい場合は、ツリービューから該当エントリを選択します。

図 6.17 は、「uid=yasuma」ユーザを選択しています。

図 6.17.: ユーザー情報の詳細表示

図 6.18 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 6.18.: 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 6.18 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。

7.1 ユーザー登録用 CSV のフォーマット

ユーザー登録用 CSV ファイルは、次の項目で構成されます。

- CSV ファイルの 1 行目には、その列に記載される項目のパラメーター名を記載します。2 行目以降が各ユーザーごとのパラメーターとなります。
- 表中の必須項目は、CSV ファイルに必ず含まれている必要があります。

パラメーター名	意味	サンプル値	必須項目	日本語
dn_suffix	LDAP の DN サフィックス	ou=Users,dc=example,dc=com		×
dn_rdn	ユーザーのエントリを格納する RDN	uid	○	×
inetOrgPerson_firstName	名	Yasuma		
inetOrgPerson_lastName	姓	Takeda	○	
inetOrgPerson_description	ユーザーの説明	2007 年入社		
inetOrgPerson_title	役職	エンジニア		
inetOrgPerson_type	雇用形態	正社員		
inetOrgPerson_manager	管理者	uid=odagiri,ou=Users,dc=example,dc=com		×
inetOrgPerson_businessCategory	業種	技術		
inetOrgPerson_street	町名	西五反田 2-6-3		
inetOrgPerson_postalCode	郵便番号	141-0031		
inetOrgPerson_address	住所	東京都品川区		
inetOrgPerson_postOfficeBox	私書箱	1234		
inetOrgPerson_telephone	電話番号	123-456-7890		

inetOrgPerson_homePhone	自宅電話番号	098-765-4321		
inetOrgPerson_mobile	携帯電話番号	0123-456-789		
inetOrgPerson_fax	FAX 番号	234-567-8901		
inetOrgPerson_email	電子メールアドレス	yasuma@example.com		×
inetOrgPerson_roomNumber	部屋番号	0789		
posixAccount_username	Unix ユーザー名	yasuma	○	×
posixAccount_cn	氏名	Yasuma Takeda		
posixAccount_uid	UID 番号	10001		×
posixAccount_group	Unix のプライマリグループ	Domain Users	○	×
posixAccount_additionalGroups	Unix の補足グループ	development		×
posixAccount_homedir	Unix のホームディレクトリ	/home/yasuma		×
posixAccount_createHomeDir	ホームディレクトリの作成場所	localhost		×
posixAccount_shell	ログインシェル	/bin/bash		×
posixAccount_password	Unix アカウントのパスワード	secret		×
posixAccount_passwordDisabled	パスワードのロック	true もしくは false		×
posixAccount_gecos	Unix の GECOS エントリ	Yasuma Takeda,0789		×
shadowAccount_warning	パスワード期限切れ警告日数	14		×
shadowAccount_expiration	パスワード期限切れからログインを許可される日数	7		×
shadowAccount_minAge	パスワード変更までの最小日数	7		×
shadowAccount_maxAge	パスワードの有効期限	30		×
shadowAccount_expireDate	パスワードの有効期日	25-03-2008		×

sambaSamAccount_domain	ユーザーの所属するドメイン	EXAMPLE	○	
sambaSamAccount_displayName	Windows で利用されるユーザーの表示名	武田 保真		
sambaSamAccount_password	Windows のパスワード	secret		×
sambaSamAccount_pwdUnix	Unix のパスワードと同じパスワードを Windows でも利用	true もしくは false		×
sambaSamAccount_noPassword	パスワードなしを許可する	true もしくは false		×
sambaSamAccount_noExpire	無期限のパスワードを許可する	true もしくは false		×
sambaSamAccount_deactivated	このアカウントを無効とする	true もしくは false		×
sambaSamAccount_pwdCanChange	ユーザーがパスワードを変更可能に許可する	true もしくは false		×
sambaSamAccount_pwdMustChange	Windows のパスワードの有効期日	31-12-2008		×
sambaSamAccount_expireDate	Windows のアカウントの有効期日	31-12-2010		×
sambaSamAccount_homeDrive	Windows で割り当てるホームドライブのドライブレター	Z:		×
sambaSamAccount_homePath	Windows 用のホームディレクトリの UNC	\\fileserver\username		
sambaSamAccount_profilePath	Windows 用のプロファイルの格納されている UNC	\\fileserver\profile\username		
sambaSamAccount_logonScript	ログオンスクリプトのファイル名	logon.bat		
sambaSamAccount_workstations	ユーザーがログオンできるコンピューター名	HOST1,HOST2		
sambaSamAccount_group	Windows のプライマリグループ	Domain Users		×
sambaSamAccount_rid	Windows の RID	25002		×
sambaSamAccount_logonHours	Windows のログオン許可時間	FFFFFFFFFFFFFFFFFFFFFF		×

Quota モジュールを有効にしている場合は、Quota も設定することが可能です。

パラメーター名	意味	サンプル値	必須項目	日本語
quota_localhost:<マウントポイント>	localhost に対して設定する Quota のブロックのソフトリミット、ハードリミット、inode のソフトリミット、ハードリミット	10000,10000,5000,5000		×

7.2 CSV ファイルの文字コードの変換

CSV による一括登録を行う場合、CSV ファイルの文字コードは UTF-8 でなければなりません。

日本語を全く含まない場合は問題ありませんが、日本語を含むデーターの場合は、UTF-8 で保存してください。

Excel を利用して作成したデーターは Shift-JIS でファイルを保存するため、次の手順で文字コードを変換してください。

1. Excel でユーザー登録用の CSV ファイルを完成させ、保存します。
2. Excel を終了します。
3. CSV ファイルを Windows XP 以降の「ノートパッド」で開きます。
4. 「ファイル」メニューから、「名前をつけて保存」を選択し、「文字コード」として「UTF-8」を選択して、「OK」します。

以上の手順で作成された CSV ファイルは、UTF-8 エンコーディングで保存されています。

OpenOffice を利用している場合は、ファイルを保存する際に「フィルタ設定を編集する」にチェックを付けることで、ファイルに保存するデーターの文字コードを設定することができますので、「UTF-8」を選択してください。

Linux などで文字コードを 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。

7.3 一括登録の実行

CSV ファイルが作成できたら、LAM を使ってアカウントの一括登録を行います。一括登録作業は、LAM にログインした後に、ブラウザの左上の「ツール」メニューから行います。

図 7.1.: 「ツール」機能

メニュー中の「ファイルのアップロード」を選択します。

図 7.2.: CSV ファイルのデーターの種類を選択

登録するデーターのアカウントタイプとして、「ユーザー」を選択し、「OK」をクリックします。

図 7.3.: CSV ファイルの参照

アップロードする CSV ファイルを「参照」し、「ファイルをアップロードして、アカウントを作成します。」をクリックします。

CSV ファイルの形式に問題がないか簡単にチェックが行われ、問題が無ければアカウントの作成ができます。

問題がある場合には、次のようにエラー内容が表示されます。

図 7.4.: CSV ファイルに問題があった場合のエラー

上記の画面でのエラーでは、アカウント番号 1 番、つまり 2 人目のデーターの「sambaSamAccount_noExpire」のセルに指定されている値が、「true」、「false」以外であるということを示しています。

このようにエラーが発生した場合は、問題があったデーターを修正し、再度 CSV ファイルのアップロードを試みてください。

全てのエラーが解決すると、次の画面になります。

図 7.5.: アカウントの作成準備が完了

実際にアカウントを作成してよければ、「アカウントを LDAP にアップロード」をクリックしてください。

アカウントの作成が始まります。

図 7.6.: アカウントの登録中

しばらくすると、アカウントの作成が終了し、次の画面になります。

図 7.7.: アカウント作成が完了

以上でアカウントの作成が完了です。

8. RHEL 5, CentOS 5 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 5、および CentOS5 では、authconfig-tui 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-tui
```

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」、および「ローカル認証は十分です」にチェックを付け、「次」を選択します。

「ローカル認証は十分です」にチェックがついていないと、LDAP サーバーが起動していないときに root でログインができなくなりますので、注意してください。

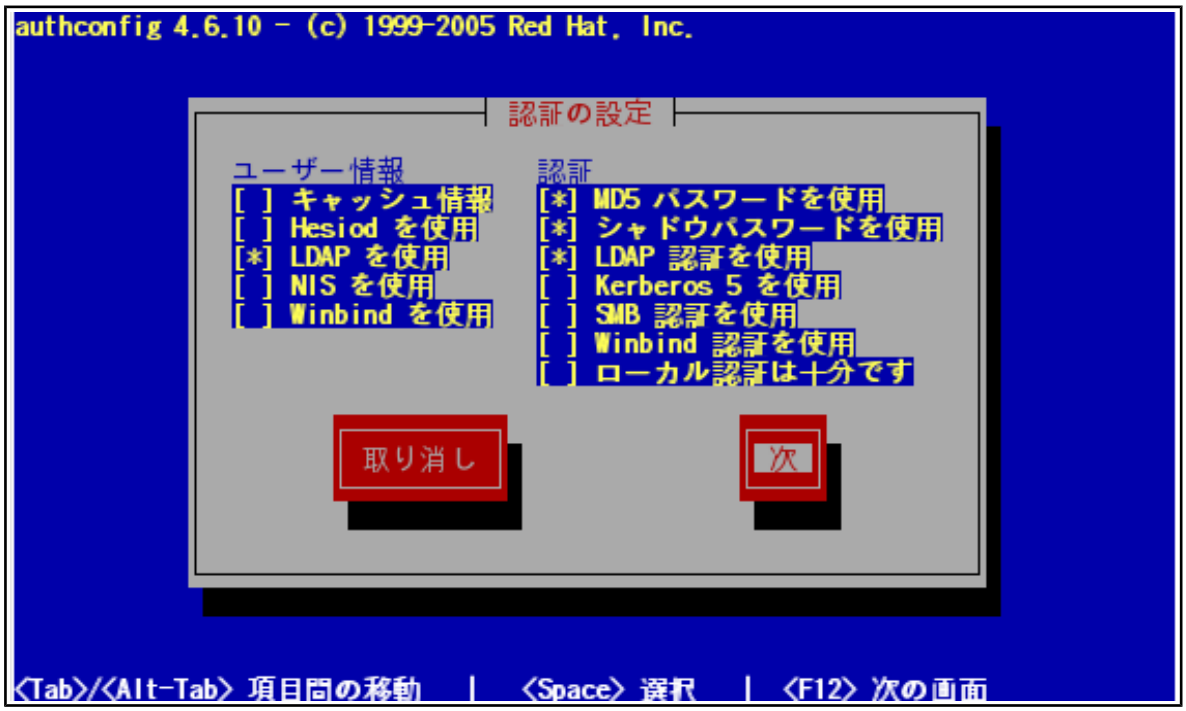

図 8.1: LDAP 利用のための設定

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。

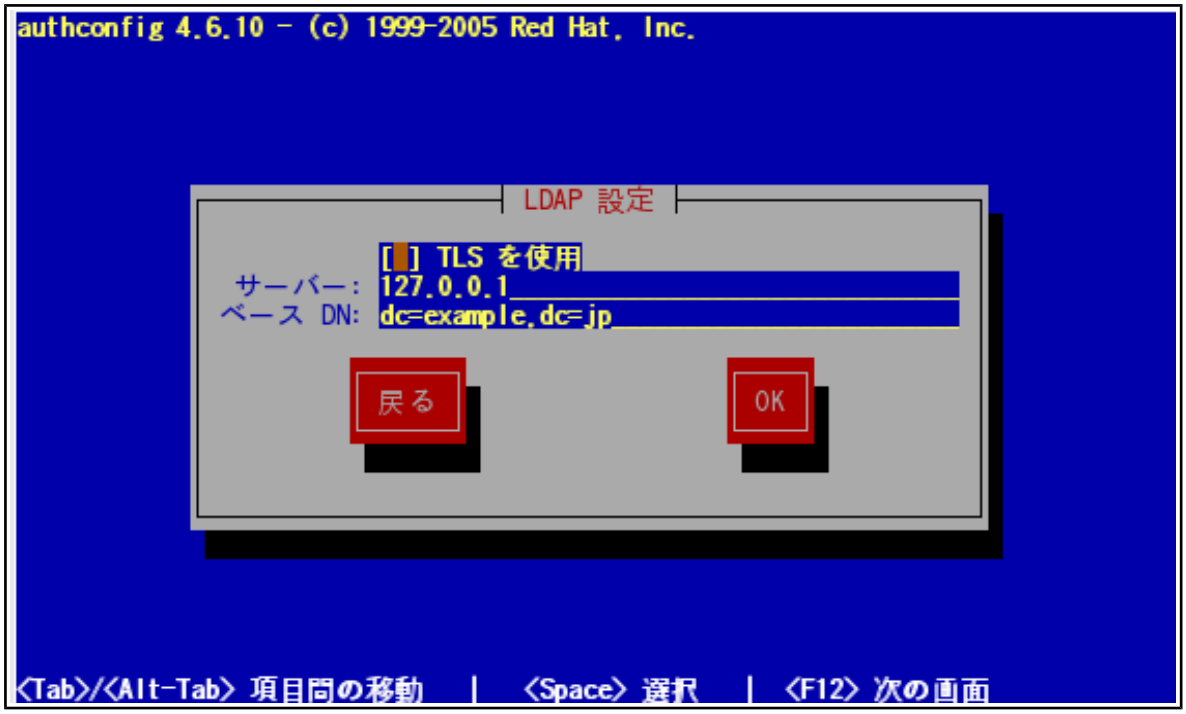

図 8.2: LDAP サーバーへの接続設定