PAMによる認証

概要

UNIXログイン時の認証（システム認証）をLDAPに関連付けて行うようにする。これにより、ログインユーザ名とパスワードについて、LDAPに登録された一元的なものを使うようにできる。以下、ログインしたいホストを「ログイン先ホスト」と呼ぶこととする。ログイン先ホストで、PAMを使用し、LDAPにアクセスするように設定する。なお、PAMからLDAPにアクセスして認証する際は、ホストごとに発行されるLDAPアクセス用のアカウント（アクセスDN）とパスワードをLDAP管理者から発行してもらう必要がある。アクセスDN等は、ログイン先ホストの設定ファイルに記述して使用する。

ユーザ情報の扱い

LDAPで認証する際、ユーザ情報をログイン先ホストとLDAPサーバの間でどのように分担して持つか、いくつかのパターンが考えられる。

パターン１：すべてLDAPサーバに持たせる
ユーザ名、ユーザID、パスワード、ホームディレクトリ、ログインシェル、グループ情報等、アカウント管理に必要な情報をすべてLDAPに持たせる。
→ログイン先ホストでは、LDAPサーバに関する設定のみでＯＫ。ただし、ユーザ名とパスワード以外の情報を持つので、複数ホストで同じLDAPサーバのデータを使うときに矛盾が発生する。ユーザIDなども決まってしまうので、ログイン先ホストによってはそのまま使えない場合もある。また、ユーザIDの数でLDAP登録上限数が制限される、IDが重複しないような管理が必要、等の諸問題がある。

パターン２：ユーザ名とパスワードのみLDAPサーバに持たせる
ユーザ名とパスワードのみLDAPにアクセスして認証し、他の情報はログイン先ホストごとに/etc/passwdや/etc/groupに記述する。
→ログイン先ホストでは、通常とほぼ同じようなユーザ定義が必要。パスワードに関する部分（通常は/etc/shadow）のみLDAPを使って認証するように設定する。こうすればログイン先ホストごとに必要なユーザのみ登録でき、柔軟な運用が可能となる。

現在、LDAPではパターン１のようなアカウント管理に必要なすべての情報を格納しているわけではないので、パターン２で各ログイン先ホストを構築することとする。

以下、RedHatやFedora系のホストで、PAMを使ったLDAP認証を行う方法を記述する。

設定ファイル

関連する設定ファイルと役割は以下のとおり。

/etc/nsswitch.conf
　認証の切り替えを設定する

/etc/pam.d/system-auth
　PAMに対し、システム認証の手順を指定する

/etc/ldap.conf
　PAMのLDAPへのアクセス方法を設定する

/etc/passwd
　ユーザ名やユーザIDなど、ユーザアカウントの基本情報を設定する

/etc/group
　グループ名やグループIDなどを設定する

PAM認証のLDAP利用設定

PAM認証でLDAPを使用するように設定する。/etc/nsswitch.confおよび/etc/pam.d/system-authファイルを記述する。Fedoreの場合、/usr/bin/authconfig-gtkコマンドを使えば、大まかな設定が簡単に行える。このツールにより、/etc/nsswitch.confおよび/etc/pam.dディレクトリ配下のファイルすべてが変更されるので、あらかじめバックアップ等をしておく。

authconfig-gtk利用時の設定内容は次のとおり。

- Fedora core2の場合
  [ユーザ情報の設定]で「LDAPを使用」にチェック。「TLSを使用」はチェックをはずし、サーバ：「10.249.98.180」（ldap0.kogaku.kyoto-u.ac.jpのアドレス）、ベースDN：「ou=people,o=kogaku,dc=kyoto-u,dc=ac,dc=jp」で「次」ボタンを押す。
  [認証の設定]で「シャドウパスワードを使用」「MD5パスワードを使用」「LDAP認証を使用」にチェックし、「LDAP認証を使用」の右側の欄を、前述の[ユーザ情報の設定]と同じ内容に設定する。最後に「OK」で完了する。
- Fedora core3の場合
  [ユーザ情報]で「LDAPを使用」にチェック。「認証」で「MD5パスワードを使用」「シャドウパスワードを使用」「LDAP認証を使用」にチェック。次へ。「TLSを使用」はチェックをはずし、サーバ：「ldap.kogaku.kyoto-u.ac.jp」、ベースDN：「ou=people,o=kogaku,dc=kyoto-u,dc=ac,dc=jp」で「OK」ボタンを押す。

以降、/etc/nsswitch.confファイルを直接編集して、関連する部分を以下のように設定する。

/etc/nsswitch.conf（関連部分のみ抜粋）

```
passwd:     files ← passwd=アカウント情報はfiles=/etc/passwdファイルを参照する
shadow:     files ldap  ← shadow=パスワードはfiles=/etc/shadowとldapサーバを参照する
group:      files ← group=グループ情報はfiles=/etc/groupファイルを参照する
```

このように設定することで、ログイン先ホストのユーザは/etc/passwdで管理し、該当ユーザのパスワードのみをldapサーバに問い合わせるようになる。詳しく書くと、ログイン認証時に入力されたユーザ名を/etc/passwdから探し、無ければ認証ＮＧ。あれば、入力されたパスワードを/etc/shadowと照合する。そこで一致すれば認証OKだが、一致しないときはldapサーバに問い合わせる。その結果OKであれば認証される。

/etc/pam.d/system-authファイルは以下のとおりとなる。

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      /lib/security/$ISA/pam_env.so
auth        sufficient    /lib/security/$ISA/pam_unix.so likeauth nullok
auth        sufficient    /lib/security/$ISA/pam_ldap.so use_first_pass
↑ldap認証用のモジュールが追加されている。（以下同様）
auth        required      /lib/security/$ISA/pam_deny.so
account required /lib/security/$ISA/pam_unix.so
account [default=bad success=ok user_unknown=ignore service_err=ignore system_err=ignore] /lib/security/$ISA/pam_ldap.so
password required /lib/security/$ISA/pam_cracklib.so retry=3 type=
password sufficient /lib/security/$ISA/pam_unix.so nullok use_authtok md5 shadow
password sufficient /lib/security/$ISA/pam_ldap.so use_authtok
password required /lib/security/$ISA/pam_deny.sosession required /lib/security/$ISA/pam_limits.so
session required /lib/security/$ISA/pam_unix.so
session optional /lib/security/$ISA/pam_ldap.so
```

次に、/etc/ldap.confを以下のように設定する。（関連部分のみ抜粋）

```
host 10.249.98.180 ← LDAPのホストを設定する。
base ou=people,o=kogaku,dc=kyoto-u,dc=ac,dc=jp ← ユーザ名を検索するベースDNを指定する。
binddn cn=polaris,ou=users,o=kogaku,dc=kyoto-u,dc=ac,dc=jp
↑LDAP管理者から割り当てられたアクセスDNを設定する。
bindpw secret
↑アクセスDNのパスワードを平文で設定する。
port 636 ← LDAPサーバへはldapsで接続する
ssl yes
pam_password md5
```

ldap.confはbindpwを平文で格納するため、ファイルパーミッションに注意する。以下のように、othersにはreadできないようにしておく。

- rw-r----- 1 root root 6830 1月 11 16:55 ldap.conf

Fedora core3などでは、ldapクライアントのセキュリティが厳しくなっており、ldaps使用時には相手サーバの公開鍵をもっていないとうまく通信できないようになっている。この制限を回避するため、/etc/openldap/ldap.confに以下の指定を追加する。

```
TLS_REQCERT    never
```

アカウントの登録

システムにアカウントを登録する際は、通常とほぼ同じように行う。適切にユーザ名やユーザID等を決めて/etc/passwdや/etc/groupファイルに登録する。ホームディレクトリなども作成する。ldapで認証する場合は、/etc/shadowファイルに該当ユーザを登録しないようにする。

ユーザ名は、LDAPのNetIDとなる（uid属性値）。NetIDをユーザ名として登録するようにする。（ただし、それ以外の任意のユーザ名を使用することも可能。後述）

例：lwq9999というNetIDをもつユーザを登録する。
/etc/passwd

```
lwq9999:x:509:509::/home/lwq9999:/bin/bash
```

/etc/group

```
lwq9999:x:509:
```

ホームディレクトリ

```
drwx------ 3 lwq9999 lwq9999 4096 11月 2 16:04 /home/lwq9999/
```

ここまでの設定で、LDAPを使ったユーザ認証ができるようになる。/etc/passwdに登録され、かつLDAPに登録されたパスワードを入力したユー

ザのみが認証OKとなる。

任意のユーザ名利用

下記設定は重大なセキュリティホールとなるため再検討が必要
~~ユーザ名がNetIDの文字列に固定されていては、普段使っているアカウント名が使えない場合がある等、不便が生じる。そこで、各ユーザがLDAPの「ユーザID（ニックネーム）：eduPersonNicknname属性」に設定した文字列を、アカウント名として使えるように設定する。このようにすれば、ユーザが自由にアカウント名を設定できる。ただし、ログイン先ホストの/etc/passwdファイル等にもアカウント名を記述するので、アカウント名をあとからユーザが自由に変更できるわけではない。~~

~~また、ニックネームはNetIDと異なり、一意性が保証されないので、以下のような制限がある。~~

- ~~同じログイン先ホストでは、ニックネームが重複しないようにする必要がある。同じログイン先ホストで、同じニックネームを持つユーザが複数登録されていた場合、認証時にはLDAP検索でいちばん先にマッチしたNetIDを持つユーザが有効となり、それ以外のユーザは正しいパスワードを入力しても認証NGとなる。つまり、最初の１人のみ有効となる。~~

~~アカウント名が重複した場合、アカウントが重複しないように変更してもらう必要がある。そのとき、すでに別のログイン先ホストにアカウントが登録されていたりすると、そちらも変更しなければならず、変更の連鎖が発生してしまう。よって、最初からできるだけ重複しにくい文字列を設定しておくことをユーザに勧めるべきである。~~

~~設定は次のとおり行う。上記までの設定に加えて、/etc/ldap.confの以下の箇所を編集する。~~
~~pam_filter |(uid=lwq9999)(uid=mvt8888)(uid=mqr7777)~~
~~↑認証時のLDAP検索フィルタ。ここにアカウントを作成するユーザのNetIDをorフィルタとして~~
~~列挙する。これにより、認証時の検索がこれらのNetIDをもつエントリに限定されるので、~~
~~関係ないエントリとのアカウント名重複を避けられる。~~
~~pam_login_attribute eduPersonNicknname~~
~~↑ユーザ名として使用するLDAP属性名を設定する。~~
~~デフォルトはuidなので、これを変更してニックネームとする。~~

~~これにより、ユーザ名としてNetIDではなく、ニックネームを使えるようになる。~~