

シェルとか設定ファイルとか
シェル変更

```
chsh
```

ファイルのパーミッション設定
.login ファイルとかに

```
umask 022
```

ls の日付表示

```
ls --time-style=long-iso --color=auto
```

にすると見やすいかも

ユーザー管理

ユーザ追加

```
useradd ユーザ名
```

ユーザ削除

```
userdel ユーザ名
```

ユーザのホームディレクトリも消す場合は、

```
userdel -r ユーザ名
```

パスワード変更

自分のパスワードなら

```
passwd
```

管理者が他のユーザのパスワードを変更する場合は、

```
passwd ユーザ名
```

グループ管理

グループを追加

```
groupadd グループ名
```

グループを削除

```
groupdel グループ名
```

管理者用ユーザーの設定

root になれるユーザを管理者のみにする

例として、管理者用の一般ユーザ名を fedora とする

```
usermod -G wheel fedora      管理者ユーザ (例 : fedora) を wheel グループに追加
```

```
vi /etc/pam.d/su             PAM の su モジュール設定ファイル編集
```

```
#auth      required      pam_wheel.so use_uid
```

```
auth      required      pam_wheel.so use_uid      コメント解除 (wheel グループ所属ユーザのみ root にな  
れるようにする)
```

```
echo "SU_WHEEL_ONLY yes" >> /etc/login.defs      最終行へ追加
```

管理者用一般ユーザからは root になれて、管理者以外の一般ユーザからは root になれないことを確認

httpd

/etc/httpd/conf/httpd.conf を修正

```
<IfModule mod_userdir.c>
#
# UserDir is disabled by default since it can confirm the presence
# of a username on the system (depending on home directory
# permissions).
#
#UserDir disable      コメントアウト

#
# To enable requests to / user/ to serve the user's public_html
# directory, remove the "UserDir disable" line above, and uncomment
# the following line instead:
#
UserDir public_html      コメントイン

</IfModule>

#
# Control access to UserDir directories. The following is an example
# for a site where these directories are restricted to read-only.
#
以下を全てコメントイン
<Directory /home/*/public_html>
    AllowOverride FileInfo AuthConfig Limit
    Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
    <Limit GET POST OPTIONS>
        Order allow,deny
        Allow from all
    </Limit>
    <LimitExcept GET POST OPTIONS>
        Order deny,allow
        Deny from all
    </LimitExcept>
</Directory>
```

SELinux 導入時の注意点

もし SELinux が有効になっている場合は【 Forbidden 】とエラーが出てしまいます。 You don't have permission to access 対象ファイル、のエラーです。

Apache のエラーログにも以下のような記録が残ります。

```
[Sun Jun 19 21:05:42 2005] [error] [client 192.168.11.102] (13)Permission denied: access to /~akane/test.html denied
```

原因は SELinux の【タイプ遷移】によるセキュリティーポリシーの制限を受けるからです。SELinux では新しくディレクトリを作成すると、その親ディレクトリのセキュリティコンテキストを継承します。

```
ls -lZ
```

こちらのコマンドを実行すると、ディレクトリ内のセキュリティコンテキストが表示されます。public_html には user_u:object_r:user_home_t というセキュリティコンテキストが割り当てられています。apache ではルール上、public_html を表示出来ません。

Fedora Core 4 では予め /home/ ユーザー名 /public_html に対するセキュリティコンテキストが設定されています。/sbin/restorecon コマンドを用いて、public_html へ適切なラベルを割り当てなくてはなりません。

```
/sbin/restorecon -R /home/ ユーザー名
```

smb のマウント

```
mount -t cifs //(Windows コンピュータ名)/(共有フォルダ名) (マウントディレクトリ) -o  
username=(Windows ユーザー名)[,password=(Windows パスワード)][,iocharset=(デフォルト文字コード)][,codepage=(コードページ)]
```

例)

```
mount -t cifs //MyComputer/Shared /mnt/folder -o  
username=winlogin,password=winpass,iocharset=euc-jp,codepage=932
```

yum の proxy 設定

```
setenv http_proxy http://xx.xx.xx.xx:port/  
yum -y update
```

もし、https を使う場合は

```
setenv https_proxy http://xx.xx.xx.xx:port/
```

MySQL インストール

```
yum -y install mysql-server
```

MySQL 設定

```
vi /etc/my.cnf MySQL 設定ファイル編集
```

```
[mysqld]
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
# Default to using old password format for compatibility with mysql 3.x
# clients (those using the mysqlclient10 compatibility package).
old_passwords=1
default-character-set = utf8      追加 (MySQL サーバーの文字コードを UTF-8 にする )
```

以下を追加 (MySQL クライアントの文字コードを UTF-8 にする)

```
[mysql]
default-character-set = utf8
```

MySQL 起動

```
/etc/rc.d/init.d/mysqld start      MySQL 起動
```

```
chkconfig mysqld on              MySQL 自動起動設定
```

```
chkconfig --list mysqld          MySQL 自動起動設定確認
mysqld 0:off 1:off 2:on 3:on 4:on 5:on 6:off   ランレベル 2 ~ 5 の on を確
認
```

MySQL 設定

root ユーザへのパスワード設定

```
mysql -u root                    MySQL サーバーへ root ユーザでログイン
```

```
mysql> select user,host,password from mysql.user;      登録済ユーザ、パスワード確認
```

```
mysql> set password for root@localhost=password('root パスワード ');   接続元ホストが localhost の
root ユーザにパスワード設定
```

匿名ユーザ削除

MySQL には匿名ユーザ (ユーザ名が空白でパスワードが設定されていないユーザ) がデフォルトで登録されており、ユーザ名とパスワードなしで MySQL サーバーへログインできてしまうため、安全のためにこのユーザを削除する。

```
mysql> delete from mysql.user where user='';          匿名ユーザ削除
```

```
mysql> select user,host from mysql.user;              登録ユーザ確認
```

ユーザー作成

```
mysql -u root -proot パスワード      root で MySQL サーバーへログイン
```

```
grant all privileges on *.* to fedora@localhost identified by 'fedorapass';
```

全てのデータベースへの全てのアクセス権限を持った、新規ユーザ fedora を登録

Fedora 5 で PHP Sqlite を使う

sqlite-open 関数が、未定義で使用出来ない場合。

<http://pecl.php.net/package/SQLite> から SQLite-1.0.3.tgz をダウンロード。

```
$ tar zxvf SQLite-1.0.3.tgz
$ cd SQLite-1.0.3
$ phpize
$ ./configure
$ make
```

edit sqlite.c, comment out the following line:

```
/* static unsigned char arg3_force_ref[] = {3, BYREF_NONE, BYREF_NONE, BYREF_FORCE }; */
```

And then change these lines

```
function_entry sqlite_functions[] = {
    PHP_FE(sqlite_open, arg3_force_ref)
    PHP_FE(sqlite_popen, arg3_force_ref)
```

以下へ変更

```
function_entry sqlite_functions[] = {
    PHP_FE(sqlite_open, third_arg_force_ref)
    PHP_FE(sqlite_popen, third_arg_force_ref)
```

```
$ make
```

それでもまだ sqlite-open 関数が、未定義で使用できませんと出る場合は

```
if (!extension_loaded("sqlite")) {
    dl("sqlite.so");
}
```

でモジュールをロード。

SELinux

無効

```
setenforce 0
```

有効

```
setenforce 1
```

ホスト名

```
hostname ホスト名
```

または

```
/etc/sysconfig/network
```

```
HOSTNAME= ホスト名
```

再起動

Active Directory 参加

hosts に Active Directory のマシンを登録

```
192.168.0.1      AD.PC
```

Kerberos の設定

レルム名は基本的に全て大文字。

/etc/krb5.conf

```
[libdefaults]
default_realm = TEST.DOMAIN (大文字)
default_tkt_enctypes = des-cbc-md5
default_tgs_enctypes = des-cbc-md5

dns_lookup_realm = false
dns_lookup_kdc = false
ticket_lifetime = 24h
forwardable = yes

[realms]
TEST.DOMAIN (大文字) = {
    kdc = AD.PC:88
    admin_server = AD.PC:749
    #default_domain = example.com
}

[domain_realm]
.test.domain = TEST.DOMAIN (大文字)
test.domain = TEST.DOMAIN (大文字)
```

Kerberos 認証の確認

```
kinit administrator@TEST.DOMAIN
```

認証されると何も表示されずにプロンプトに戻ります。

Winbind の設定

/etc/samba/smb.conf

```
workgroup = TEST
realm = TEST.DOMAIN
security = ads
password server = AD.PC
encrypt passwords = yes
winbind separator = +

winbind uid = 10000-12000
winbind gid = 10000-12000
template shell = /bin/bash
template homedir = /home/%D/%U
```

アカウント取得方法の変更

/etc/nsswitch.conf

```
passwd:      files winbind
shadow:      files winbind
group:       files winbind
```

Active Directory への参加

```
net ads join -U AD 管理者 I D
```

エラーになる場合は

```
setenforce 0
```

で SELinux を一時的にオフにする

Winbind の起動と確認

```
/etc/init.d/winbind start  
/etc/init.d/winbind status
```

正常に動作していたら自動起動の設定

```
chkconfig winbind on
```

Active Directory に登録されているユーザーを取得できるかどうか確認

```
# wbinfo -u  
Administrator  
Guest
```

....

Winbind により、ユーザー認証が行えるかどうかを確認

```
wbinfo -a 'ユーザー名 % パスワード '
```

PAM の設定

```
/etc/pam.d/system-auth-ac
```

```
auth      required      pam_env.so  
auth      sufficient   pam_unix.so nullok try_first_pass  
auth      sufficient   pam_winbind.so ( 追記 )  
auth      requisite    pam_succeed_if.so uid >= 500 quiet  
auth      required     pam_deny.so  
  
account   required     pam_unix.so  
account   sufficient   pam_succeed_if.so uid < 500 quiet  
account   required     pam_permit.so  
account   sufficient   pam_winbind.so ( 追記 )  
  
password  requisite    pam_cracklib.so try_first_pass retry=3  
password  sufficient   pam_unix.so md5 shadow nullok try_first_pass use_authn  
ok  
password  required     pam_deny.so  
  
session   required     pam_limits.so  
session   required     pam_unix.so  
session   required     /lib/security/pam_mkhomedir.so skel=/etc/skel umask=0022 ( 追記 )
```

状況に応じてローカルに AD のユーザーと同じユーザーを作る

```
/sbin/service winbind stop #winbindをとめる  
/usr/sbin/useradd -M -d /home/ ドメイン名 /$1 $1 # ホームを指定  
/usr/bin/passwd -l $1 # ローカルユーザーのロック (winbind のみで認証するのでローカルとしてはロックする)  
/sbin/service winbind start #winbind再開
```