OpenLDAP サーバの動的設定

OpenLDAP バージョン 2.4 より、設定が slapd.conf ファイルから LDAP データベースに変更されました。従来どおり slapd.conf ファイルを使った設定も可能ですが、ここでは新しいやり方を紹介します。

OpenLDAP サーバの設定が格納される設定データベースは、/etc/openldap/slapd.d ディレクトリ以下に配置されています。トップエントリは「cn=config」です。

```
# ls -R /etc/openldap/slapd.d/
/etc/openldap/slapd.d/:
cn=config  cn=config.ldif

/etc/openldap/slapd.d/cn=config:
cn=schema      olcDatabase={-1}frontend.ldif
olcDatabase={1}bdb.ldif     olcDatabase={2}hdb.ldif
cn=schema.ldif  olcDatabase={0}config.ldif
olcDatabase={1}monitor.ldif

/etc/openldap/slapd.d/cn=config/cn=schema:
cn={0}corba.ldif       cn={1}core.ldif
cn={5}inetorgperson.ldif  cn={9}openldap.ldif
cn={0}core.ldif        cn={2}cosine.ldif    cn={6}java.ldif
cn={10}ppolicy.ldif     cn={3}duaconf.ldif   cn={7}misc.ldif
cn={11}collective.ldif  cn={4}dyngroup.ldif  cn={8}nis.ldif
```

設定データベースの構成ファイルを直接編集しないようにしてください。ldapsearch コマンドを使って設定を参照したり、ldapadd コマンドや ldapmodify コマンドを使って設定データベースを動的に書き換えたりして設定を行います。例として、LDAP サーバの設定の一部（olcDatabase={2}hdb,cn=config）を表示します。

注：「-Y EXTERNAL」は SASL 認証の方式です。「-H ldapi://」はローカルなサーバに接続することを意味します。

```
# ldapsearch -LLL -Y EXTERNAL -H ldapi:// -b
'olcDatabase={2}hdb,cn=config'
SASL/EXTERNAL authentication started
SASL username:
gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
```

```
dn: olcDatabase={2}hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {2}hdb
olcDbDirectory: /var/lib/ldap
olcSuffix: dc=example,dc=com
olcRootDN: cn=Manager,dc=example,dc=com
olcDbIndex: objectClass eq,pres
olcDbIndex: ou,cn,mail,surname,givenname eq,pres,sub
```

今度は、LDAP の管理者(root エントリ)パスワードを変更してみます。まず、slappasswd コマンドでパスワードを生成します。

```
# slappasswd
New password:           ← パスワードを入力
Re-enter new password:  ← パスワードを再入力
{SSHA}7FjK6ObzTNs6FtLPWO6C/wsDO7XZwLrY
```

以下のような LDIF ファイルを作成し、出力されたパスワードを記述します。

password.ldif

```
dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcRootPW
olcRootPW:{SSHA}7FjK6ObzTNs6FtLPWO6C/wsDO7XZwLrY        ←出力された
                                                        パスワード
```

以下のコマンドでパスワードを変更します。

```
# ldapadd -Y EXTERNAL -H ldapi:// -f password.ldif
SASL/EXTERNAL authentication started
SASL username:
gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={0}config,cn=config"
```

変更を確認します。

```
# ldapsearch -LLL -Y EXTERNAL -H ldapi:// -b
'olcDatabase={0}config,cn=config' olcRootPw
```

```
SASL/EXTERNAL authentication started
SASL username:
gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
dn: olcDatabase={0}config,cn=config
olcRootPW: {SSHA}7FjK6ObzTNs6FtLPWO6C/wsDO7XZwLrY     ← パスワードが
                                                      設定されている
```

このように、ldapadd コマンドを使ってエントリを登録したり、ldapmodify コマンドを使ってエントリを編集したりすることで動的に LDAP サーバの設定を変更できます。