```
# kadmin -p root/admin
Authenticating as principal root/admin with password.
Password for root/admin@MY-COMPANY.COM: ←―― pas4admin Enter を入力
kadmin:  addprinc -randkey ldap/ldap01.my-company.com
WARNING: no policy specified for ldap/ldap01.my-company.com@MY-COMPANY.COM; defaulting to no
policy
Principal "ldap/ldap01.my-company.com@MY-COMPANY.COM" created.
kadmin:  ktadd -k /etc/openldap/ldap.keytab ldap/ldap01.my-company.com
Entry for principal ldap/ldap01.my-company.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/openldap/ldap.keytab.
Entry for principal ldap/ldap01.my-company.com with kvno 3, encryption type ArcFour with HMAC/
md5 added to keytab WRFILE:/etc/openldap/ldap.keytab.
Entry for principal ldap/ldap01.my-company.com with kvno 3, encryption type DES with HMAC/sha1
added to keytab WRFILE:/etc/openldap/ldap.keytab.
Entry for principal ldap/ldap01.my-company.com with kvno 3, encryption type DES cbc mode with
RSA-MD5 added to keytab WRFILE:/etc/openldap/ldap.keytab.
kadmin:  exit
```

図 4.24　LDAP 接続用サービス・プリンシパルの作成

次のコマンドを実行して ldap グループに対する keytab ファイルのアクセス権を設定します。

```
# chgrp ldap /etc/openldap/ldap.keytab
# chmod g+r /etc/openldap/ldap.keytab
```

/etc/sysconfig/ldap に**図 4.25** の設定を追加します。これは，LDAP サーバが Kerberos 認証に使用する keytab ファイルの指定です。そして，「3.3 OpenLDAP による Linux ユーザの統合管理」の**図 3.18** で作成した **slapd.conf** における「ルート・サフィックス」の最後に，**図 4.26** の設定を追加します。この設定の意味は，「3.5 Digest-MD5 による SASL 認証」で説明したものとほぼ同じです。

/etc/sysconfig/ldap（追加部分）

```
KRB5_KTNAME=/etc/openldap/ldap.keytab
```

図 4.25　LDAP サーバが使用する keytab ファイルの指定

/etc/openldap/slapd.conf（追加部分）

```
sasl-realm my-company.com
authz-regexp
        "uid=root/admin,cn=my-company.com,cn=gssapi,cn=auth"
        "cn=Manager,dc=my-company,dc=com"
authz-regexp
        "uid=([^/,]+).*,cn=my-company.com,cn=gssapi,cn=auth"
        "uid=$1,ou=People,o=Linux Users,dc=my-company,dc=com"
```

図 4.26　GSS-API/KerberosV による SASL 認証設定