LDAPを用いたパスワード認証

Shibboleth IdP 3からは、LDAPモジュールを用いたJAASによるパスワード認証に加えて、直接LDAPを参照するパスワード認証が追加されました。

デフォルトは直接LDAPを参照するパスワード認証です。

直接LDAPを参照するパスワード認証

- conf/ldap.properties
  参照するLDAPにあわせて、Connection properties, SSL configuration, Search DN resolutionのプロパティを設定します。

conf/ldap.properties

```
## Connection properties ##
idp.authn.LDAP.ldapURL                  = ldap://localhost:389
idp.authn.LDAP.useStartTLS              = false
#idp.authn.LDAP.useSSL                  = false
#idp.authn.LDAP.connectTimeout          = 3000



# Search DN resolution, used by anonSearchAuthenticator, bindSearchAuthenticator
# for AD: CN=Users,DC=example,DC=org
idp.authn.LDAP.baseDN                   = ou=people,dc=example,dc=ac,dc=jp
idp.authn.LDAP.subtreeSearch            = true
idp.authn.LDAP.userFilter               = (uid={user})
# bind search configuration
# for AD: idp.authn.LDAP.bindDN=adminuser@domain.com
idp.authn.LDAP.bindDN                   =
idp.authn.LDAP.bindDNCredential         =
```

差分

```
 ## Connection properties ##
-idp.authn.LDAP.ldapURL                  = ldap://localhost:10389
-#idp.authn.LDAP.useStartTLS             = true
+idp.authn.LDAP.ldapURL                  = ldap://localhost:389
+idp.authn.LDAP.useStartTLS              = false
 #idp.authn.LDAP.useSSL                  = false
 #idp.authn.LDAP.connectTimeout          = 3000



 # Search DN resolution, used by anonSearchAuthenticator, bindSearchAuthenticator
 # for AD: CN=Users,DC=example,DC=org
-idp.authn.LDAP.baseDN                   = ou=people,dc=example,dc=org
-#idp.authn.LDAP.subtreeSearch           = false
+idp.authn.LDAP.baseDN                   = ou=people,dc=example,dc=ac,dc=jp
+idp.authn.LDAP.subtreeSearch            = true
 idp.authn.LDAP.userFilter               = (uid={user})
 # bind search configuration
 # for AD: idp.authn.LDAP.bindDN=adminuser@domain.com
-idp.authn.LDAP.bindDN                   = uid=myservice,ou=system
-idp.authn.LDAP.bindDNCredential         = myServicePassword
+idp.authn.LDAP.bindDN                   =
+idp.authn.LDAP.bindDNCredential         =
```

JAASによるパスワード認証

- conf/authn/password-authn-config.xml

  <import resource="jaas-authn-config.xml" />の行をアンコメントして、<import resource="ldap-authn-config.xml" />の行をコメントアウトします。

conf/authn/password-authn-config.xml

```
<!-- Choose an import based on the back-end you want to use. -->
<import resource="jaas-authn-config.xml" />
<!-- <import resource="krb5-authn-config.xml" /> -->
<!-- <import resource="ldap-authn-config.xml" /> -->
```

- conf/authn/jaas.config

  参照するLDAPにあわせて、org.ldaptive.jaas.LdapLoginModule required以降の行を設定します。

conf/authn/jaas.config

```
ShibUserPassAuth {
    /*
        com.sun.security.auth.module.Krb5LoginModule required;
        */
    org.ldaptive.jaas.LdapLoginModule required
      ldapUrl="ldap://localhost"
      baseDn="ou=people,dc=example,dc=ac,dc=jp"
      ssl="false"
      userFilter="uid={user}"
      subtreeSearch="true"
      ;
};
```