

LDAPサーバにStartTLSで接続する方法（LDAPサーバがCentOS 6の場合）

CentOS 6 標準のopenldap-serversパッケージでLDAPサーバを構築した環境において、IdPからLDAPサーバにStartTLSで接続する設定について記載します。

LDAPサーバはホスト名 `ldaptest1.gakunin.nii.ac.jp` として説明します。 [LDAPプロキシサーバ：複数台LDAPサーバ向けのLDAPプロキシサーバ設定方法](#) の「LDAPサーバ設定(ldaptest1)」を参考に OpenLDAP の設定を行ってください。この説明で利用する証明書の情報は「LDAPサーバ設定(ldaptest1)」の設定に準じます。



上記資料はCentOS 5系で記載されたものであるため、利用するバージョンに合わせて適宜読み替える必要があります。

IdPでは `ldap.properties`, `attribute-resolver.xml` に下記の設定を行います。例としてLDAPサーバのCA証明書は `/etc/pki/tls/certs/gakuninca.pem` として配置しています。

/opt/shibboleth-idp/conf/ldap.properties の設定

```
(省略)
## Connection properties ##
idp.authn.LDAP.ldapURL           = ldap://ldaptest1.gakunin.nii.ac.jp
idp.authn.LDAP.useStartTLS        = true
#idp.authn.LDAP.useSSL            = false
#idp.authn.LDAP.connectTimeout    = 3000

## SSL configuration, either jvmTrust, certificateTrust, or keyStoreTrust
idp.authn.LDAP.sslConfig          = certificateTrust ← アンコメント
## If using certificateTrust above, set to the trusted certificate's path
idp.authn.LDAP.trustCertificates   = /etc/pki/tls/certs/gakuninca.pem
## If using keyStoreTrust above, set to the truststore path
idp.authn.LDAP.trustStore          = ${idp.home}/credentials/ldap-server.truststore

(省略)
```

/opt/shibboleth-idp/conf/attribute-resolver.xml の設定

```
<DataConnector id="myLDAP" xsi:type="LDAPDirectory">
  ldapURL="${idp.attribute.resolver.LDAP.ldapURL}"
  baseDN="${idp.attribute.resolver.LDAP.baseDN}"
  principal="${idp.attribute.resolver.LDAP.bindDN}"
  principalCredential="${idp.attribute.resolver.LDAP.bindDNCredential}"
  useStartTLS="${idp.attribute.resolver.LDAP.useStartTLS:true}"
  connectTimeout="${idp.attribute.resolver.LDAP.connectTimeout}"
  responseTimeout="${idp.attribute.resolver.LDAP.responseTimeout}"
  noResultIsError="${idp.attribute.resolver.LDAP.noResultIsError:true}"
  trustFile="${idp.attribute.resolver.LDAP.trustCertificates}">
```

↑上記のように > の直前に挿入してください

/opt/shibboleth-idp/conf/attribute-resolver.xml の設定 (Shibboleth IdP 3.2.xおよびそれ以前の場合)

```
<resolver:DataConnector id="myLDAP" xsi:type="dc:LDAPDirectory">
(省略)
  ↓以下の3行を</resolver:DataConnector>の直前に挿入してください
  <dc:StartTLSTrustCredential id="LDAPtoIdPCredential" xsi:type="sec:X509ResourceBacked">
    <sec:Certificate>${idp.attribute.resolver.LDAP.trustCertificates}</sec:Certificate>
  </dc:StartTLSTrustCredential>
</resolver:DataConnector>
```



IdPバージョン2向けのattribute-resolver.xmlはldap.propertiesを参照しないため齟齬が発生する恐れがあります。 [最新のattribute-resolver テンプレート](#)を使用するようにしてください。



LDAP Data Connectorでは、`idp.authn.LDAP.sslConfig`は`certificateTrust`のみ使用可能です。