分散管理とアクセス制御

サーバの分散管理

LDAPサーバは、サブツリー配下を別サーバで管理させるように構成できます。サブツリーのLDAPサーバは、元のツリーのLDAPサーバとは独立にアクセス制御を定義できるので、サーバの管理責任単位でLDAPサーバを分散させることが出来ます。

現時点ではサブツリーによりサーバを分散させる方法はとりません。将来的に全学のツリーができれば、kogaku配下をそのサブツリーとして運用する可能性はあります。

アクセス制御

openLDAPでは設定ファイルにアクセス制御リスト(ACL:Access Control List)を記述することで、静的にアクセス制御を行います。LDAPへのアクセス権は、バインドするDNによって決まります。DNを明示してアクセス権を定義したり、あるグループDNを明示して、そこに属するメンバDNに対するアクセス権を定義したりできます。運用では主にou=groups配下にエントリをいくつか作成し、これらのグループに属するメンバに対してのアクセス権を定義していきます。

アクセス制御の主な要素は次の通りです。
構成：access to <what> by <who> <access>
<what>：アクセスを制御する対象となるエントリや属性の１セット
<who>：アクセスを要求するもの
<aceess>：アクセス権

ACLの例：

```
access to dn.regex="cn=(.+),ou=groups,o=kogaku,dc=kyoto-u,dc=ac,dc=jp"
 by dn="cn=Administrator,o=kogaku,dc=kyoto-u,dc=ac,dc=jp" write
 by group/groupOfUniqueNames/owner.expand="cn=$1,ou=groups,\
  o=kogaku,dc=kyoto-u,dc=ac,dc=jp" write
 by group/groupOfUniqueNames/uniqueMember="cn=admin,ou=groups,\
  o=kogaku,dc=kyoto-u,dc=ac,dc=jp" write
 by group/groupOfUniqueNames/uniqueMember.expand="cn=$1,ou=groups,\
  o=kogaku,dc=kyoto-u,dc=ac,dc=jp" read
 by * none
```

上の場合、ou=groups内の「cn=XXXX（１文字以上の名称）」エントリに対する読み取り、書き込みの権限を設定しています。「(.+)」というのは正規表現で、後の行で「$1」「$2」などとして、括弧内を引用できるようになっています。正規表現を使う場合は、1行目の「access to dn.regex」のようにregexスタイル（正規表現）であることを明示し、参照側ではexpandスタイルを明示します。上記を表で表すと以下のようになります。

<what>：ou=groups直下のcn=XXXX各エントリ

<who>	<access>
LDAPのルートユーザ（cn=Administrator）	読み込み／書き込み可能→グループのメンバの追

	加・削除が可能。
該当グループのオーナー（owner属性に登録されているDN)	読み込み／書き込み可能→グループのメンバの追加・削除が可能。
adminグループのメンバー（cn=admin,ou=groups...のメンバー)	読み込み／書き込み可能→グループのメンバの追加・削除が可能。
該当グループのメンバー（uniqueMember属性に登録されているDN)	読み込み可能→グループの中身を読み取れる。
その他（他のユーザまたは匿名バインド）	権限なし

このようなACLが<what>ごとに複数羅列されます。

LDAPシステム構築時に定義する基本的なACLと、あらかじめ定義しておく管理用エントリがあります。代表的なものに「LDAPの管理者」エントリと「LDAP管理者グループ」そして、それらに関するACLがあります。
&ref(): File not found: "ldap_admin.png" at page "Service/LDAP0.5/60000";
図：あらかじめ定義しておく管理用エントリの代表例

ou=usersの配下にユーザcn=admin（LDAP管理者）を、ou=groupsの配下にグループcn=admin（LDAP管理者グループ）を作成します。グループにはuniqueMember属性とowner属性があり、それぞれ図の通りに設定します。

これらに関係するACLの一部を表形式で記述すると次のとおり。下記のようにLDAP管理グループに対しては特別に大きな権限が与えられています。

1. <what>：cn=admin,ou=groups...

<who>	<access>
adminグループのオーナー cn=admin,ou=users,...	読み込み／書き込み可能→グループのメンバーの追加・削除が可能。
adminグループのメンバー cn=admin,ou=groups,...のメンバー	読み込み可能→グループの中身を読み取れる。
一般ユーザまたは匿名ユーザ	権限なし

2. <what>：ou=groups配下の各エントリ

<who>	<access>
adminグループのメンバー	読み込み／書き込み可能→グループのメンバの追加・削除が可能。
該当グループのメンバー	読み込み可能→グループの中身を読み取れる。
一般ユーザまたは匿名ユーザ	権限なし

3. <what>：各エントリのユーザパスワード(userPassword)

<who>	<access>
adminグループのメンバー	読み込み／書き込み可能→パスワードの変更が可能。
匿名ユーザ	認証のためのアクセスのみ。読み込むことはできないがパスワードが正しいかど

	うかを確認することのみ可能。
その他	権限なし

4. <what>：その他

<who>	<access>
adminグループのメンバー	読み込み／書き込み可能→エントリ内容の変更が可能。
一般ユーザ	読み込み可能→エントリの内容を読み取れる。
匿名ユーザ	権限なし

システム構築時に定義するグループは他にもあります。詳細は、詳細編 アクセス制御を参照してください。

バインドDNの発行

各webアプリに対してバインド用のエントリを作成して発行します。通常の人（ou=people）がアクセスするのと同様に、webアプリも１つのクライアントとみなしてエントリを作成します。このようなアプリ用のエントリはou=usersの下に作成します。

例：webアプリ「people edit（個人エントリの編集）」を作成する場合。

cn=people_edit,ou=users,...

を作成します。また、必要であれば、既存のグループ(ou=groups）にこのエントリをメンバとして登録します。グループはアクセス制御に使用します。あらかじめグループと、そのグループに対するLDAPへのアクセス権を定義しておき、後から作成したユーザをののグループに加えることで、そのユーザに対してアクセス権が適用されるようにします。このように、ユーザに対する直接的なアクセス制御は定義せず、グループを介して制御することとします。

バインドDNを発行されたwebアプリは、それを利用してLDAPにアクセスします。ただし、必ずしも発行されたバインドDNを使用する必要はありません。

- バインドDNを使用
  バインドDNに設定されている権限内でのアクセスが可能。webページにアクセスした人は、みな同じアクセス権限をもつことになります。あらかじめ割り当てられたDN以外を用いてwebページを使用することはできません。
- バインドDNを使用しない
  web利用時に認証(LDAP)を行い、その時のDNでLDAPにアクセスします。ユーザは自分のDNの権限に応じてWebページを利用します。

なお、ou=groups以下のグループエントリは、その所有者が自分のDN権限でメンバーを追加したり削除したりできるようにします。これにより、グループメンバの管理を所有者に委譲することができます。

View Edit