ツリーの構造

LDAPはディレクトリ型のデータベースなので、階層的にデータが表現されます。工学部・工学研究科のLDAPツリー概念図は以下の通りです。

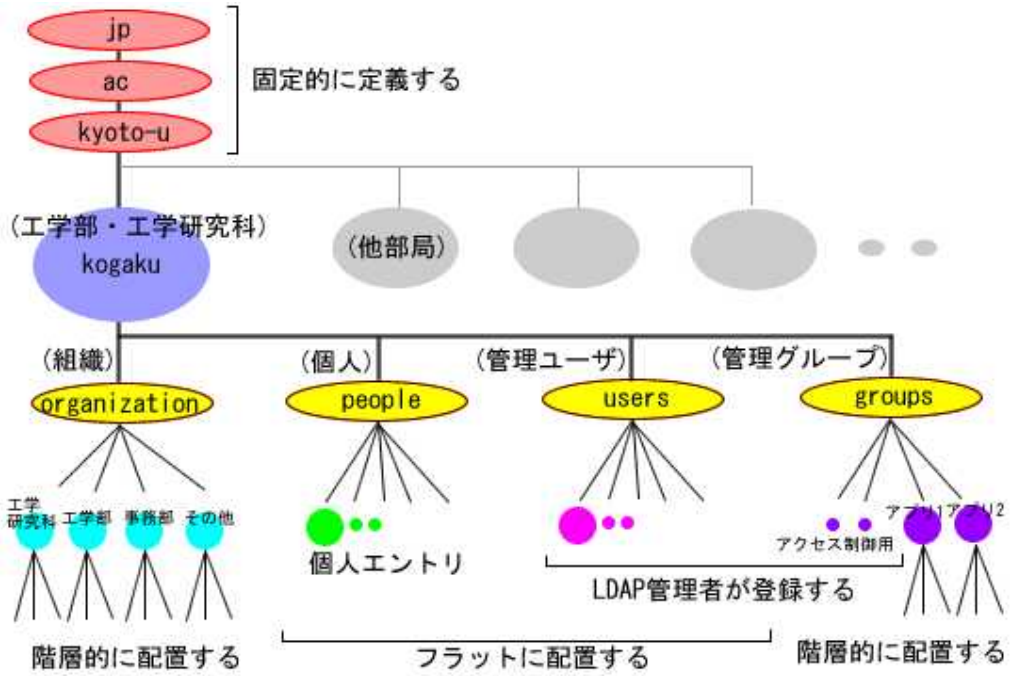

図　工学部・工学研究科LDAPツリー概念図

階層の最上部はjp,ac,kyoto-uとします。これらの階層は固定的に定義するだけで、実際のデータは格納しません。これはLDAPの慣習で、グローバルに使用することを前提に、ホストのFQDN（完全修飾ドメイン名）に準じた階層を設けます。

kyoto-uの配下に各部局のエントリを定義します。工学部・工学研究科の場合はFQDNに倣って「kogaku」というエントリ名とします。

kogakuの配下に前述の4つの情報「組織、個人、管理ユーザ、管理グループ」を格納するエントリを配置します。それぞれの名前を「organization,people,users,groups」とします。

organization
組織のエントリを階層的に配置します。直下には「事務部」、「専攻」、「委員会」、および「その他」のように、大きな区切りでエントリを作成します。それらのエントリの配下にそれぞれの組織に対応したエントリを階層的に配置します。

people
各個人のエントリを格納します。工学部・工学研究科に主に所属する人に対し、１対１で対応します。peopleの直下に個人の数だけエントリをフラットに作成します。

users
管理用ユーザやアプリが使用するための特別なエントリを格納します。LDAP管理者がエントリを作成し、webアプリ作成者がそれらのエントリを利用してLDAPにバインドする

などして使用します。基本的にエントリ情報は一般ユーザや外部には公開しません。

groups
グループのエントリを格納します。役割が2通りあり、1つは管理用としてLDAPサーバそのもののアクセス制御のために使用します。この場合、LDAP管理者がグループへのメンバ登録を行い、各ユーザやアプリに対して権限を付与します。もう1つの役割は、一般ユーザへ公開し、そこにメンバーを追加することで、特定アプリでのアクセス権を制御するために使用します。この場合、一般ユーザがグループ編集用のインタフェースを介してグループを編集します。なお、現時点ではgroups以下の階層構造は2階層まで、ということを前提としています。

View Edit