LDAPサーバ概要

概要

ディレクトリサービスを実現するための、サーバ構成や環境構築の方法、およびwebからのアクセス（アクセス制御）の実例などについて記述する。

サーバ構成

工学部・工学研究科のLDAPサーバ構成は以下の通り。

No.	ホスト名	IPアドレス	備考	OS
1	[ldap1] ldap1.kogaku.kyoto-u.ac.jp	133.3.140.11	工学部・工学研究科のldapサーバ	Fedora core3
2	[ldap2] ldap2.kogaku.kyoto-u.ac.jp	133.3.140.12	工学部・工学研究科のldapサーバ	Fedora core3
3	[www2] www2.kogaku.kyoto-u.ac.jp	130.54.44.148	各種サーバのバックアップ用サーバ	Fedora core3

LDAPはldaps（tcp:636)のみサポートし、ldap（tcp:389)は受け付けない。（localhostのみ有効）
各LDAPサーバ間およびLDAP-WEBサーバ間の通信はldapsを使用して行う。

LDAPサーバ

LDAPサーバは openldap-2.1以降を使用。なお、openldap-2.0の場合はDITの分割管理ができない。
[ldap1] openldap-2.2.13-2
[ldap2] openldap-2.2.13-2
[www2] openldap-2.2.13-2

データベース

LDAP用のデフォルトであるLDBMを使用する。他のバックエンドDBは性能面で劣るため使用しない。

セキュリティ

LDAPのホスト間通信はすべてldapsで行い、通信路を保護する。よってSASLなどの保護認証は使用せず、簡易認証を行う。なお、ldapsと同時にldapのポートで待ち受けをしても良いが、他ホストから接続できないよう、ポートに対する通信遮断をする。（iptables）

複製

slurpdによるLDAPデータの複製を行う。[ldap1][ldap2]は常にマスタとし、DNSで切り替えて使用する。[www2]は常に複製サーバとし、[ldap1]または[ldap2]をマスタとする。

設定ファイル

openldapの関連設定ファイルは以下の通り。（ただしパスワード記述部分は一部変更）

- ldap1
  - /etc/openldap/slapd.conf
  - /etc/openldap/ldap.conf
- ldap2
  - /etc/openldap/slapd.conf
  - /etc/openldap/ldap.conf
- www2
  - /etc/openldap/slapd.conf
  - /etc/openldap/ldap.conf