

# LDAPの使われ方

OpenLDAPを中心とした、  
大学におけるシステム管理・運用

2007年12月8日

県立長崎シーボルト大学  
情報センター 堀田 倫英

# 本日のレジュメ

- LDAPとは
- Name Service／PAM／authconfig
- LDAPとDBMSとの対比
- LDAPの見え方
- OpenLDAPの構成
- 本学の運用例
- 構築・運用環境
- まとめ

# LDAPとは？

Lightweight Directory Access Protocol

- ディレクトリ
  - 住所録、電話帳
  - 例)メーラのアドレス帳
- /etc/passwdの代わり
- /etc/groupの代わり
- ...
- /etc/hogehogeの代わり

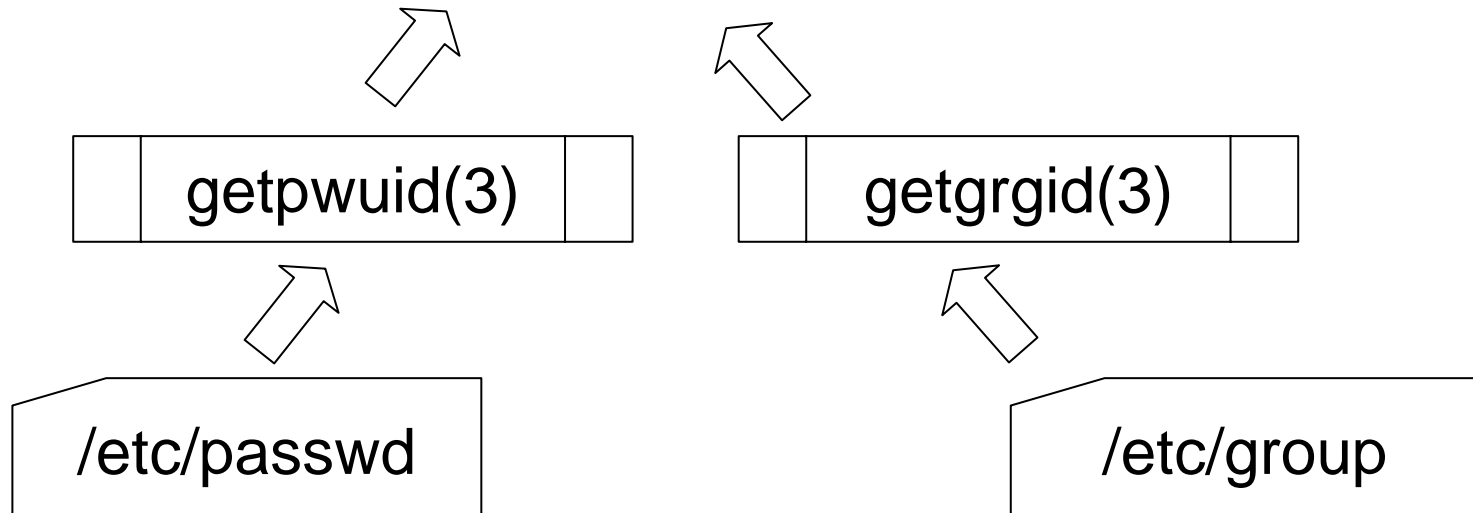
# Name Service

➤ `ls -l a.txt`

➤ `-rw-r--r-- 1 hotta hotta 0 10月20日 10:11 a.txt`

➤ `ls -ln a.txt`    ↑    ↑

➤ `-rw-r--r-- 1 500 500 0 10月20日 10:11 a.txt`



# Name Service

```
$ whoami
```

```
hotta
```

```
$ id hotta
```

```
uid=500(hotta) gid=500(hotta) 所属グループ  
=500(hotta)
```

```
$ strace id hotta 2>&1 | grep '^open("/etc' | uniq
```

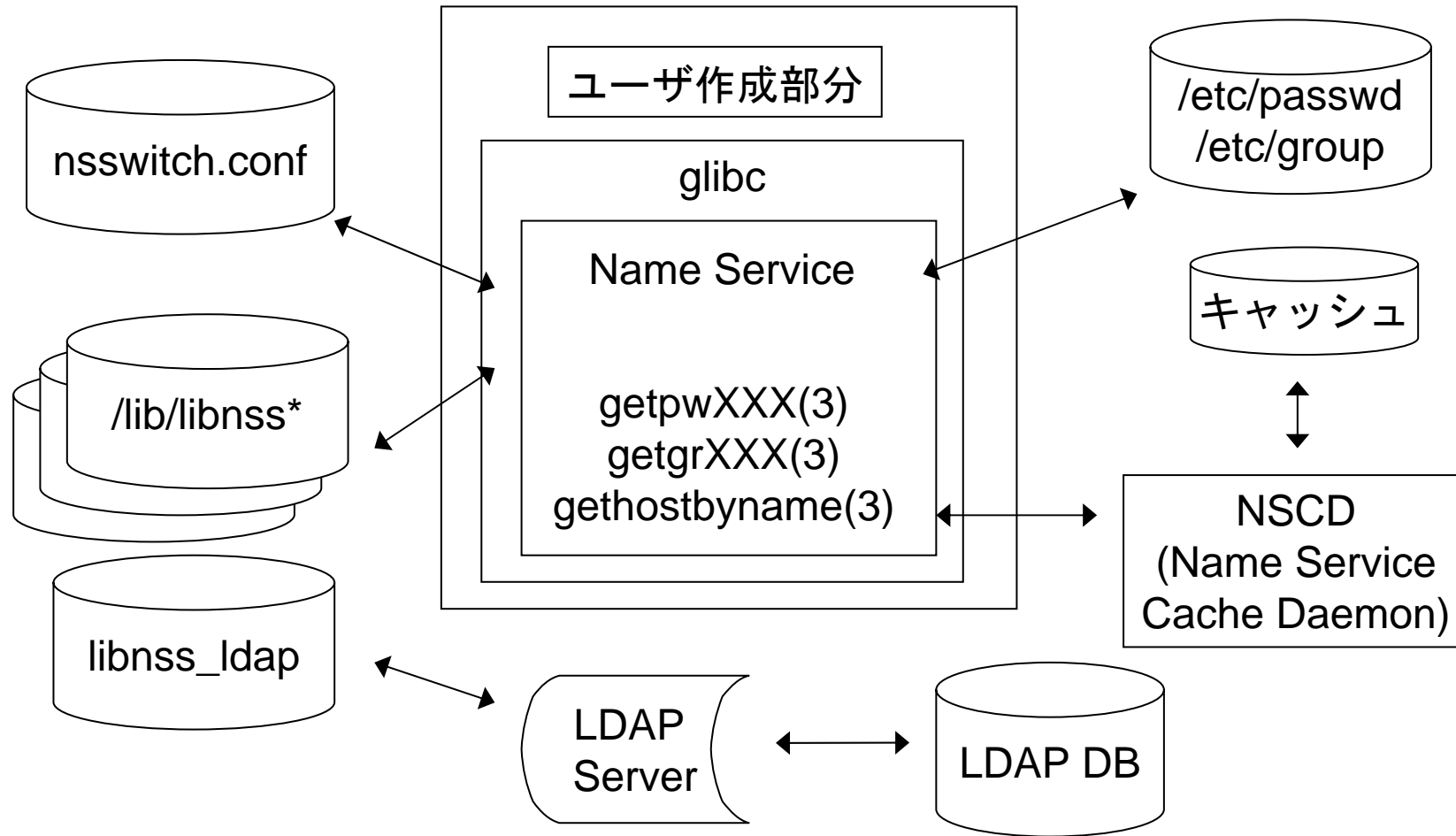
```
open("/etc/ld.so.cache", O_RDONLY) = 3
```

```
open("/etc/nsswitch.conf", O_RDONLY) = 3
```

```
open("/etc/passwd", O_RDONLY) = 3
```

```
open("/etc/group", O_RDONLY) = 3
```

# Name Service



# nsswitch.conf

NSS=Name Service Switch

```
$ grep ^[a-z] /etc/nsswitch.conf
```

```
passwd: files ldap
```

```
shadow: files ldap
```

```
group: files ldap
```

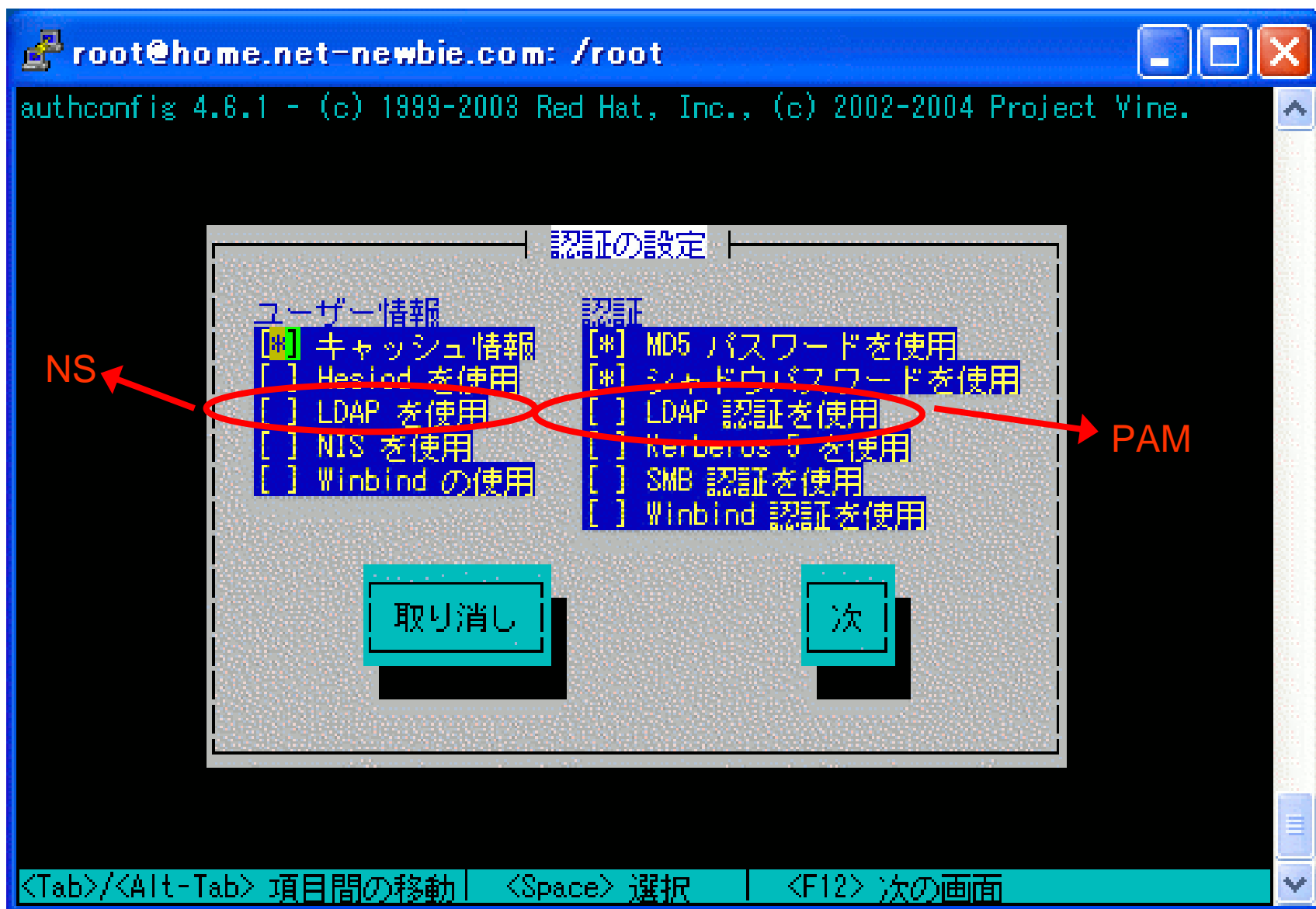
```
hosts: files dns
```

```
services: files
```

```
aliases: files ldap
```

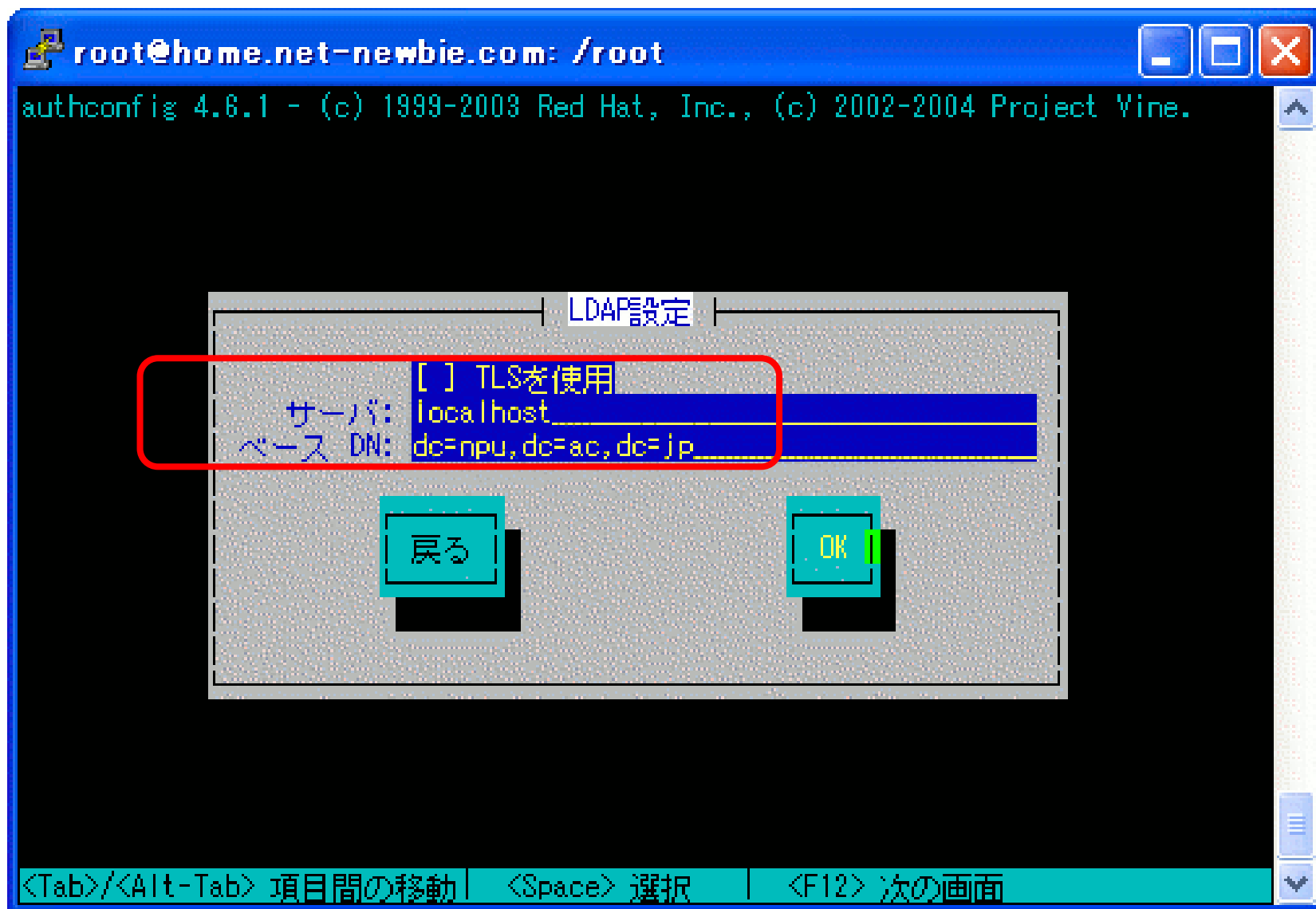
(その他いろいろ)

# authconfig





# authconfig



# authconfig

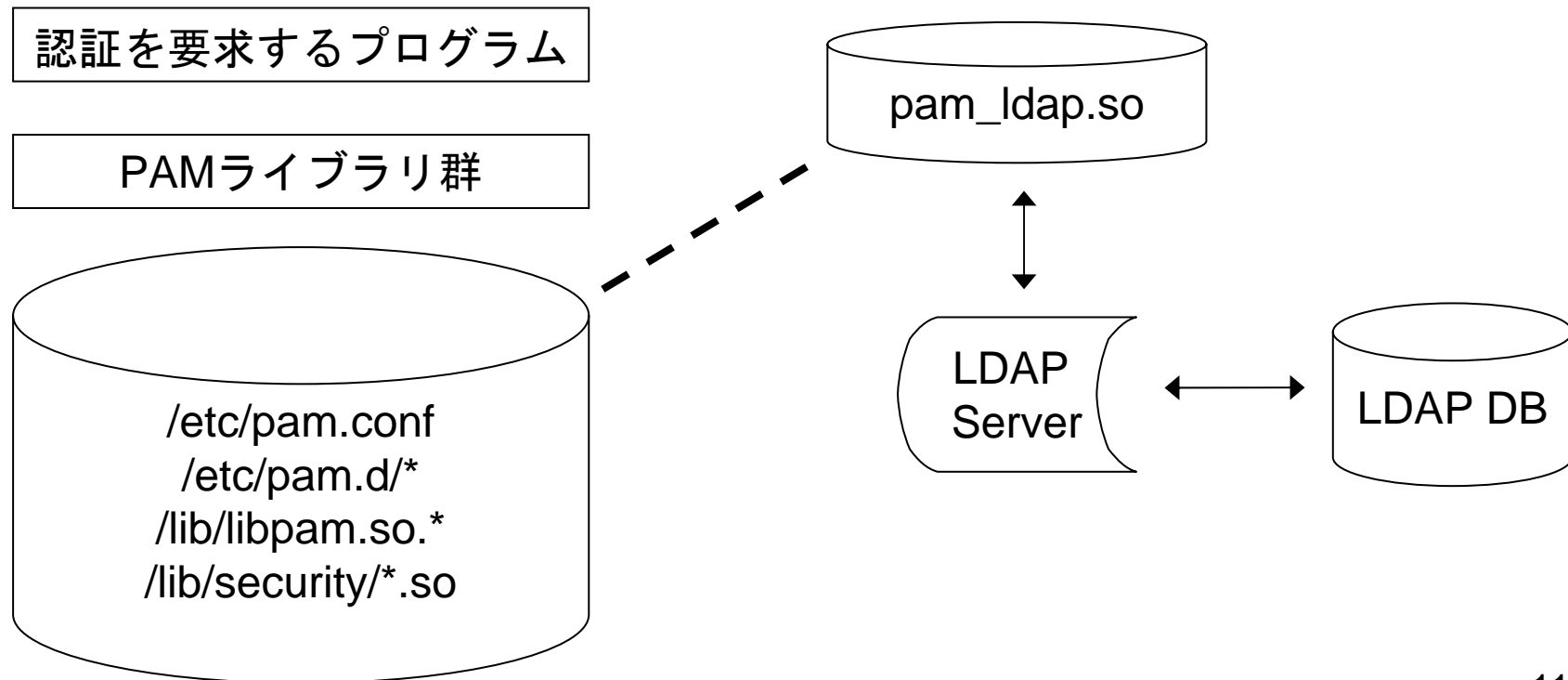
- /etc/sysconfig/authconfig
- /etc/yp.conf
- /etc/sysconfig/network
- /etc/ldap.conf
- /etc/krb5.conf
- /etc/krb.conf
- /etc/hesiod.conf
- /etc/pam\_smb.conf
- /etc/samba/smb.conf
- /etc/nsswitch.conf
- /etc/pam.d/system-auth

これだけの  
ファイルを  
一挙に設定

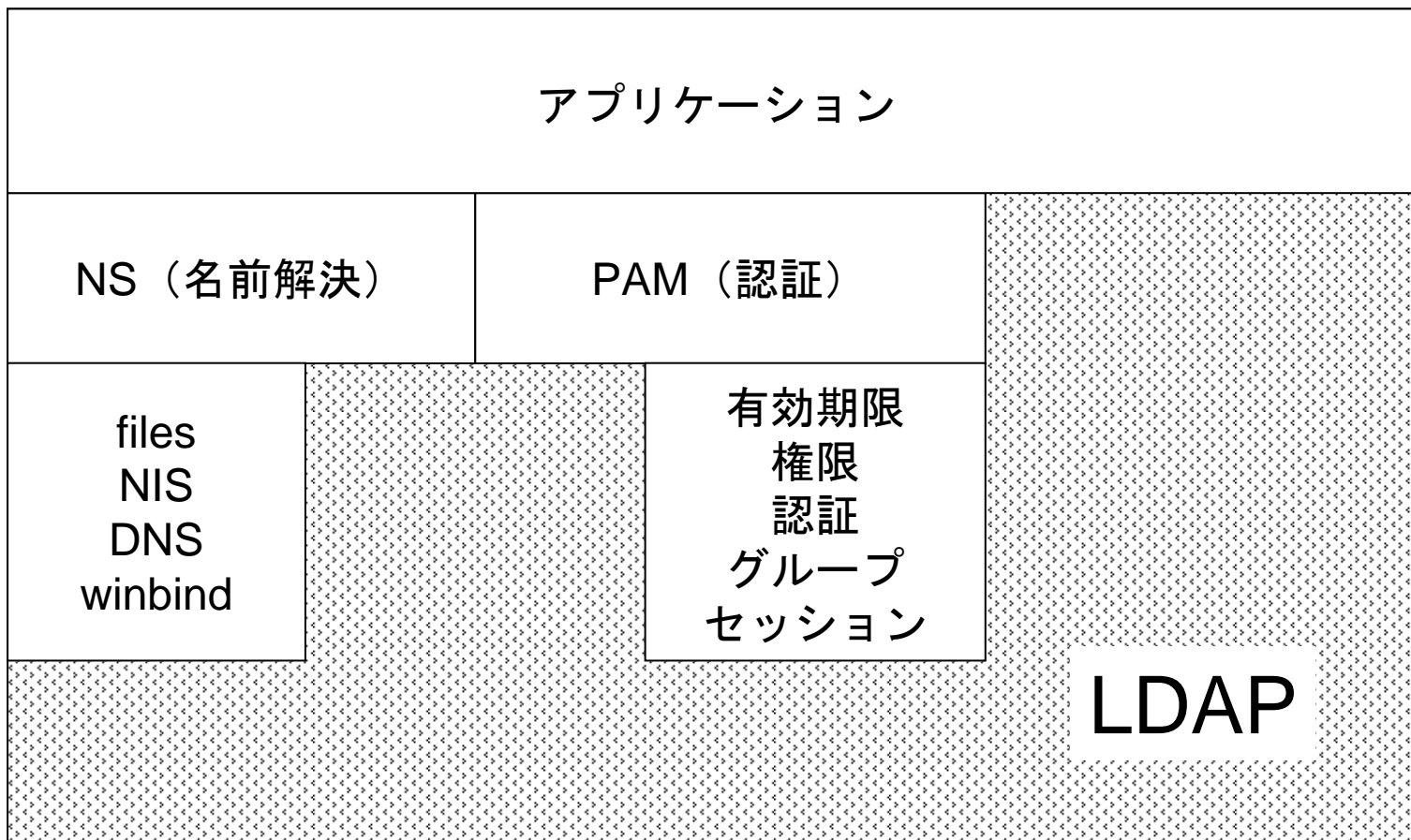
# PAM

## PAM(Pluggable Authentication Module)

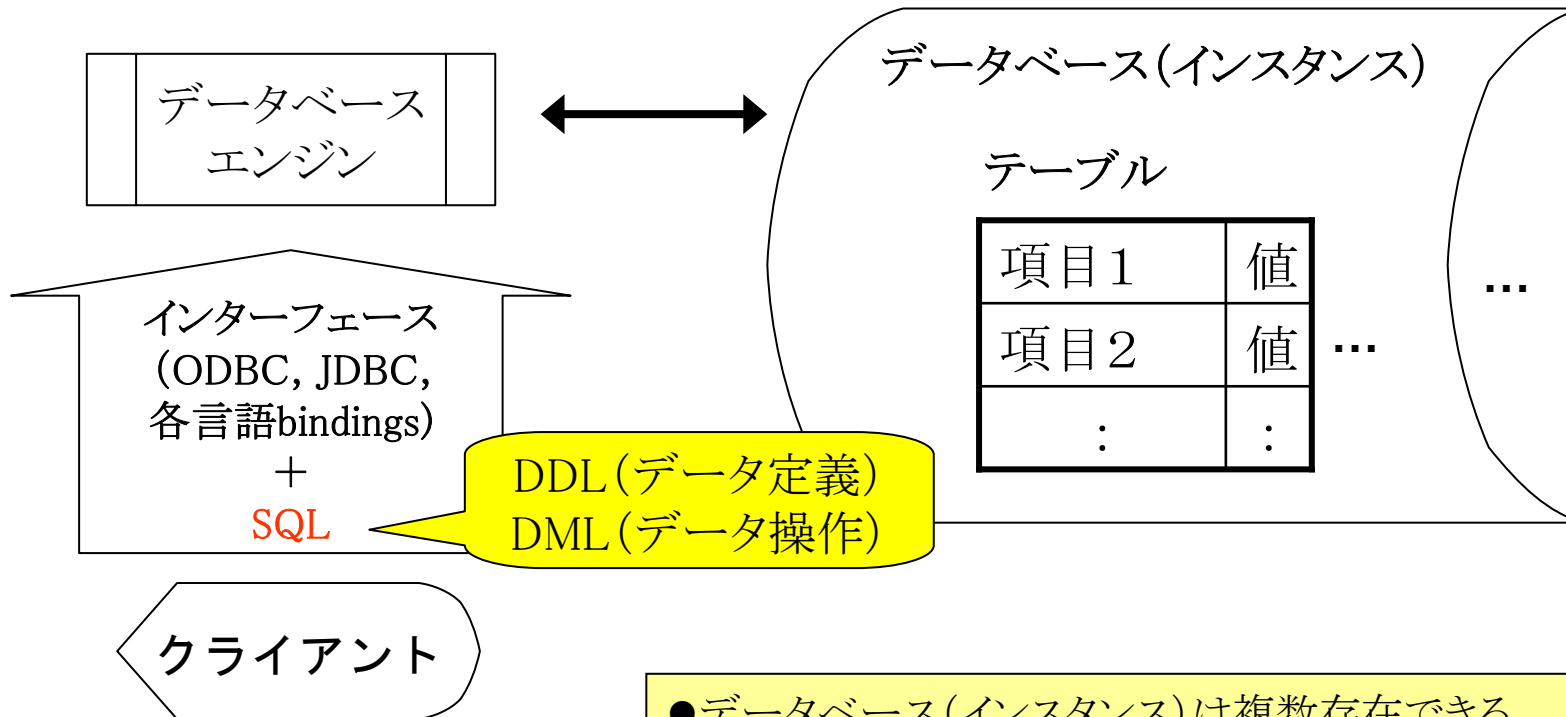
認証部分を自由に入れ替え可能に



# LDAPの位置づけ

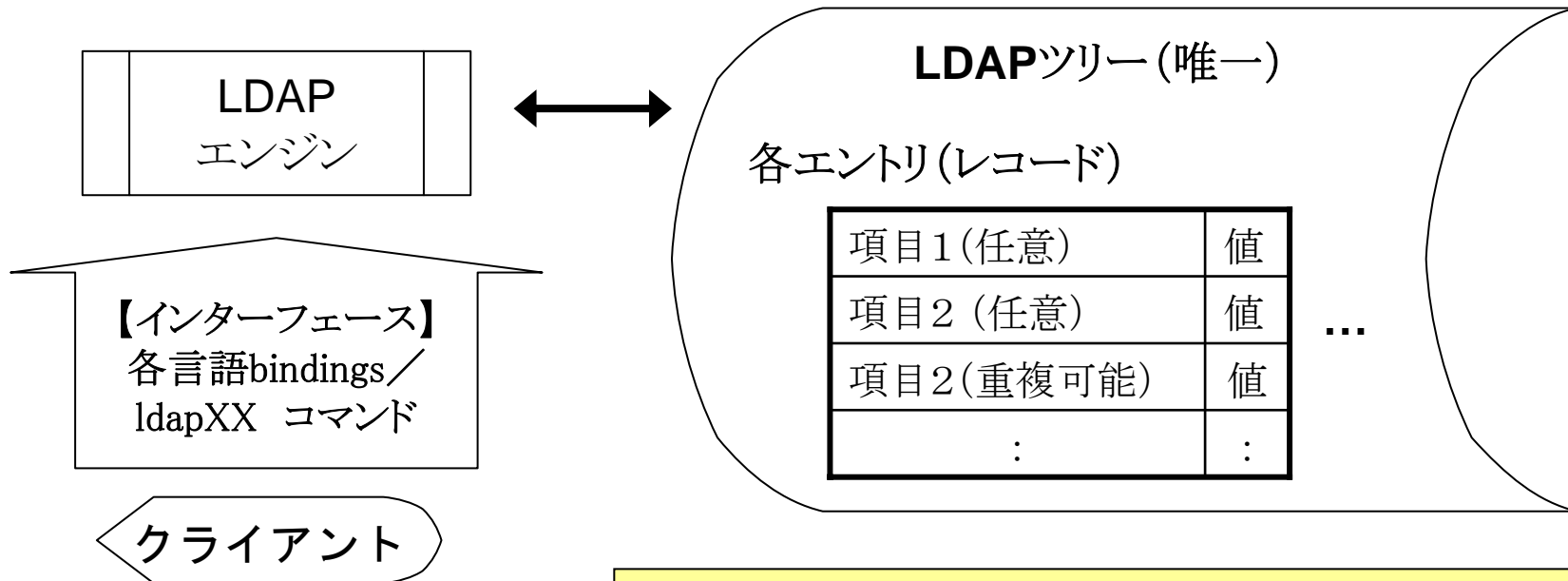


# DBMSの構成



- データベース(インスタンス)は複数存在できる
- 1データベース内に、複数のテーブルが定義できる
- 動的にデータベースやテーブルの追加、削除が可能
- 1テーブル内の構造は、全レコード同じ(表形式)

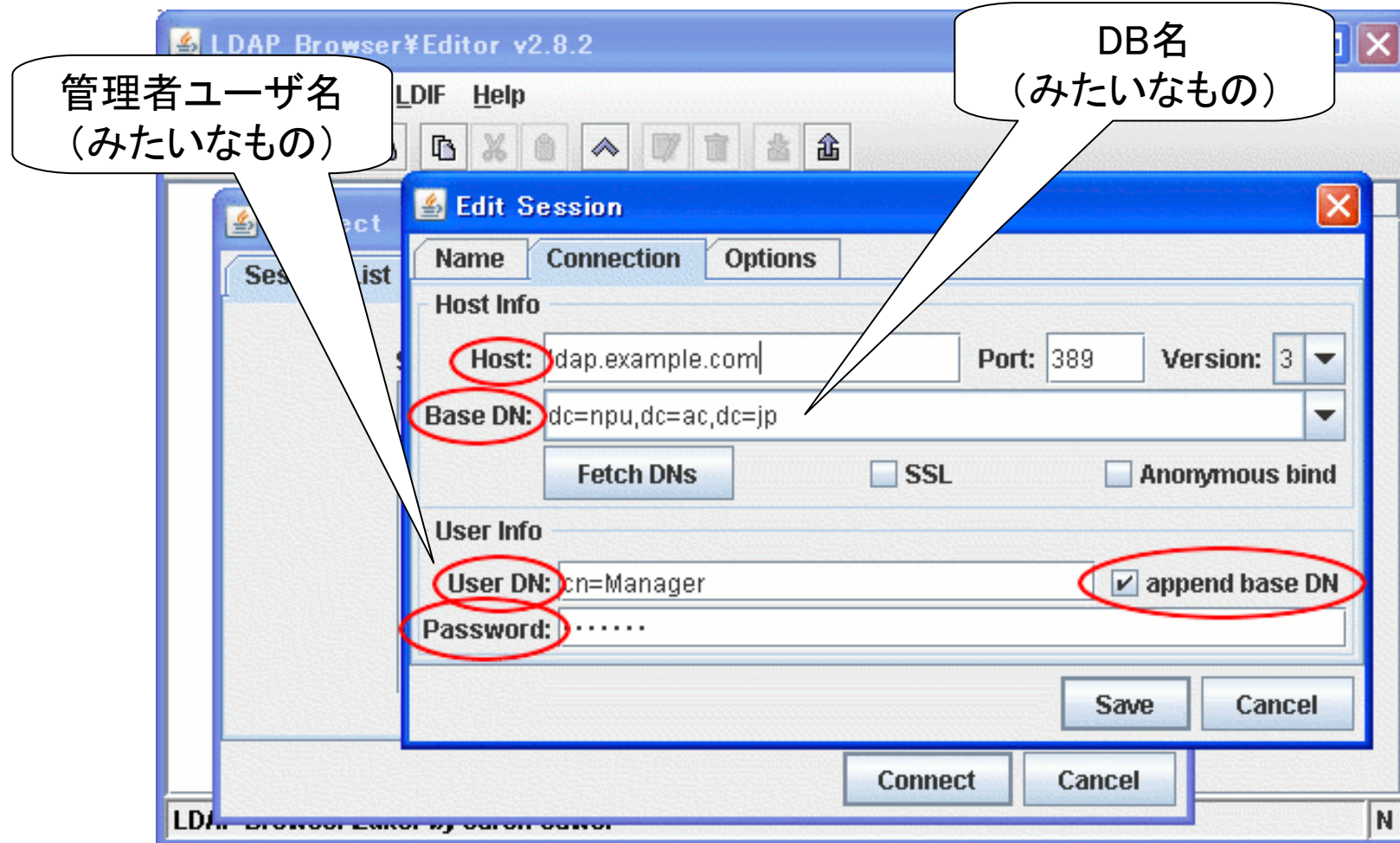
# LDAPの構成



【object class】  
create table SQL文  
のようなもの

- 単独のLDAPツリーを全ノードが参照
- テーブルという概念はない
- 各エントリの構造は、異なってもよい
- 項目はobject classまたは属性のいずれか
- そのエントリに「属性a」が存在するためには、そのエントリ内に「属性a」を含むobject classが必要

# LDAP Browser



# ツリーの最上位

LDAP Browser#Editor v2.8.2 - [ldap://hiace.ngs.nagasakiu.ac.jp/dc=npu,dc=ac,dc=jp]

File Edit View LDIF Help

dc=npu,dc=ac,dc=jp

- ou=Users
- ou=Groups
- ou=Idmap
- sambaDomainName=NPU
- ou=Computers
- ou=NFS
- sambaDomainName=CALINA
- sambaDomainName=MIGRATE
- ou=DHCP
- sambaDomainName=SPRINTER

Attribute	Value
gidNumber	1000
sambaSID	S-1-5-21-1116196674-3591202597-2404333293
uidNumber	106341
objectClass	sambaDomain
objectClass	sambaUnixIdPool
sambaDomainName	NPU

Ready. U



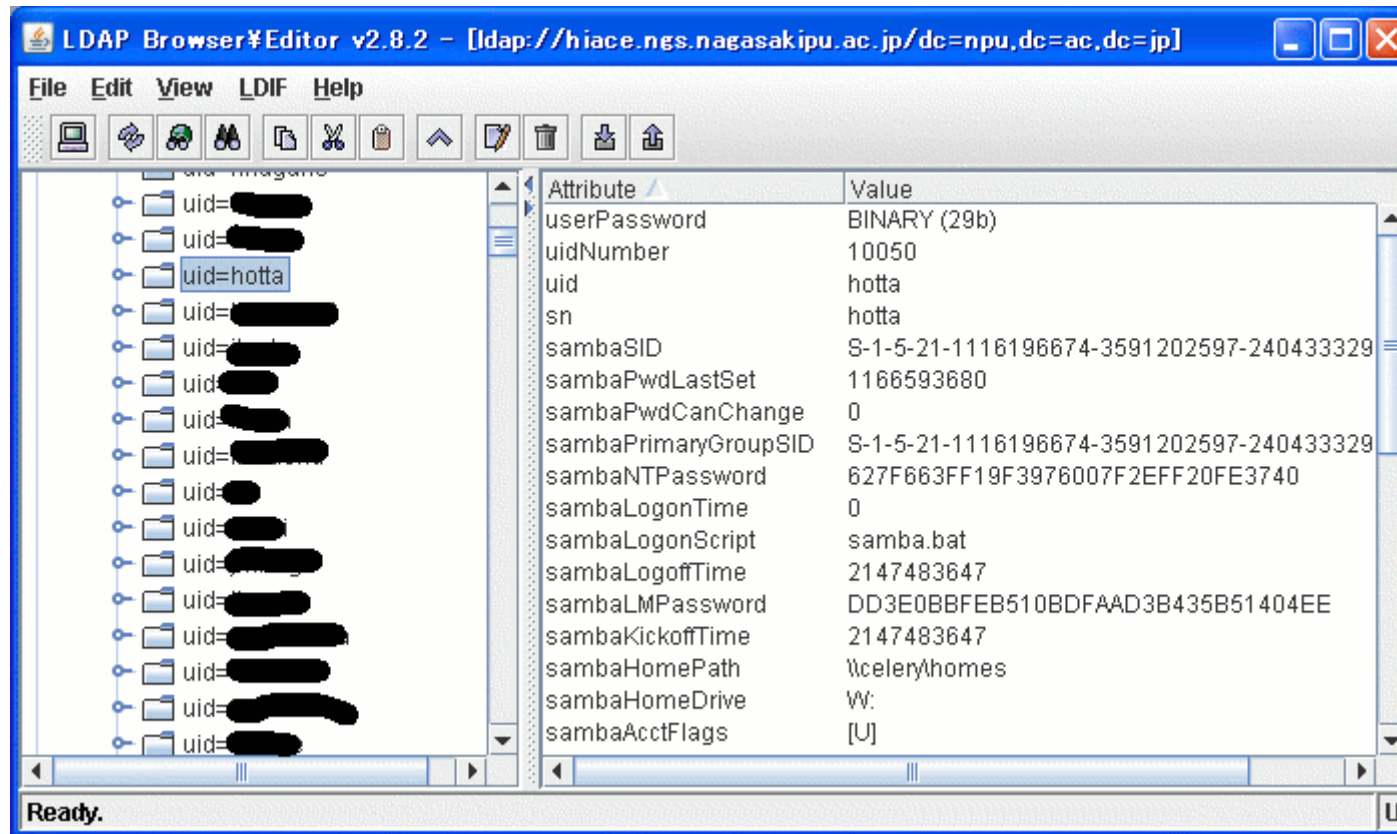
# グループエントリの例

The screenshot shows the LDAP Browser Editor v2.8.2 interface. The title bar indicates the connection path: [ldap://hiace.ngs.nagasakiu.ac.jp/dc=npu,dc=ac,dc=jp]. The menu bar includes File, Edit, View, LDIF, and Help. The toolbar contains icons for navigation and editing. The left pane shows a tree view of the LDAP directory structure, with 'cn=Domain Computers' selected under 'ou=Groups'. The right pane displays the attributes and values for this entry.

Attribute	Value
cn	Domain Computers
description	Netbios Domain Computers accounts
displayName	Domain Computers
gidNumber	515
objectClass	posixGroup
objectClass	sambaGroupMapping
sambaGroupType	2
sambaSID	S-1-5-21-1116196674-3591202597-2404333293-515

Ready. U

# ユーザエントリの例



# ユーザエントリの例（続き）

The screenshot shows the LDAP Browser Editor v2.8.2 interface. The title bar indicates the connection path: [ldap://hiace.ngs.nagasakiu.ac.jp/dc=npu,dc=ac,dc=jp]. The left pane displays a tree view of LDAP entries, with 'uid=hotta' selected. The right pane shows the details for this entry in a table format.

Attribute	Value
objectClass	shadowAccount
objectClass	sambaSamAccount
objectClass	inetOrgPerson
objectClass	posixAccount
objectClass	npuUser
npuKubun	23
npuJname	堀田 倫英
npuDept	15
npuCapaWebP	40
npuCapaWebG	40
npuCapaMail	500
npuCapaFile	5000
npuCampus	1
mail	hotta@net-newbie.com
loginShell	/bin/bash
homeDirectory	/home/hotta
gidNumber	513
gecos	hotta2
displayName	hotta
description	07/02/15
cn	hotta

Ready. U

# Idapsearch

```
$ Idapsearch -h localhost -x -LLL ¥  
  -b ou=Users,dc=npu,dc=ac,dc=jp '(uid=hotta)' uid npujname  
dn: uid=hotta,ou=Nagasaki,ou=Users,dc=npu,dc=ac,dc=jp  
uid: hotta  
npuJname:: 5aCA55Sw44CA5YCr6lux  
$ psql -h localhost  
# select uid, npujname  
# from 'ou=Users,dc=npu,dc=ac,dc=jp' where uid= 'hotta';  
uid | hotta  
npuJname | 5aCA55Sw44CA5YCr6lux  
$ php -r 'print base64_decode("5aCA55Sw44CA5YCr6lux");'  
堀田 倫英
```

DN: ユニークキー  
(必ず存在する)

:: エンコードされ  
ていることを表す

# スキーマ(データ定義)

ファイル名	object class(o)/attribute type(a) の例
ビルトイン(schema_init.c)	uid(a), userPassword(a)
core.schema	ou(a), organization(o)
cosine.schema	(主にinetorgperson用としてincludeされる)
inetorgperson.schema	inetOrgPerson(o), displayName(a)
misc.schema	mailHost(a)
nis.schema	posixAccount(o), memberUid(a)
samba.schema	sambaLMPassword(a), sambaBadPasswordTime(a)
dhcp.schema	dhcpHWAddress(a)

(openldap-2.3.27より抜粋)

# object classとattribute type

```
$ grep m-hotta /etc/passwd
```

```
m-hotta:x:601:601::/home/m-hotta:/bin/bash
```

```
$ sed -n '/posixAccount/,/^$/p' /etc/openldap/schema/nis.schema
```

```
objectclass ( 1.3.6.1.1.1.2.0 NAME 'posixAccount'
```

```
DESC 'Abstraction of an account with POSIX attributes'
```

```
SUP top AUXILIARY
```

```
MUST ( cn $ uid $ uidNumber $ gidNumber $ homeDirectory )
```

```
MAY ( userPassword $ loginShell $ gecos $ description ) )
```

```
$ sed -n "/loginShell/,/^$/p" /etc/openldap/schema/nis.schema
```

```
attributetype ( 1.3.6.1.1.1.1.4 NAME 'loginShell'
```

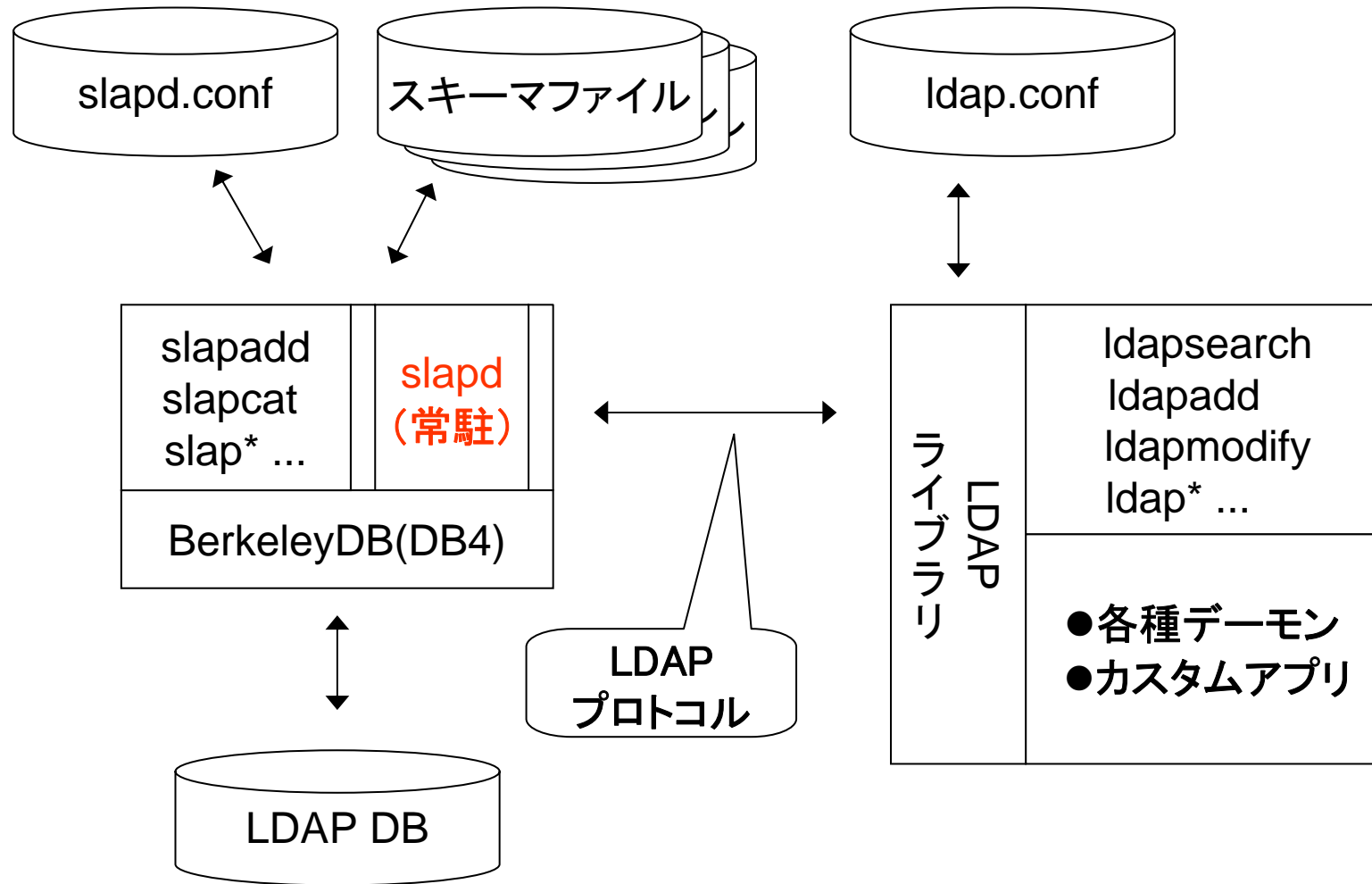
```
DESC 'The path to the login shell'
```

```
EQUALITY caseExactIA5Match
```

```
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
```

ASCII文字列の英大小文字  
区別あり、スペース無視

# OpenLDAPの構成



# OpenLDAPの実際

各デーモンやアプリケーションで、  
OpenLDAPがどう連携して使われているのかを見てみましょう。



# vsftpd (ログイン認証)

- vsftpd = FTP Server
  - /etc/vsftpd/vsftpd.confの設定変更箇所
    - 一切変更なし
  - authconfigで「LDAP認証を使用する」にするだけ

```
$ rpm -q vsftpd  
vsftpd-2.0.1-5.EL4.5
```

# dovecot (ログイン認証)

- dovecot = IMAP Server
  - /etc/dovecot.confの設定変更箇所
    - 一切変更なし
  - authconfigで「LDAP認証を使用する」にするだけ
- TIPS
  - pam\_mkhome.soを使うと、ホームディレクトリがない時に自動で作ってくれる(らしい)

```
$ rpm -q dovecot
dovecot-1.0-0.1.rc7.npuc
```

# postfix (user/group mapping)

- authconfigで「LDAP認証を使用する」にする

- /etc/postfix/main.cf

ldapalias\_server\_host = 127.0.0.1

ldapalias\_server\_port = 389

ldapalias\_search\_base = ou=Users,dc=npu,dc=ac,dc=jp

ldapalias\_scope = sub

ldapalias\_timeout = 15

ldapalias\_query\_filter = (|(uid=%u)(gecos=%u))

ldapalias\_result\_attribute = mail

alias\_maps = hash:/etc/postfix/aliases

hash:/etc/postfix/mailman\_aliases ldap:ldapalias

```
$ rpm -q postfix mailman
postfix-2.3.3-2.npuc
mailman-2.1.8-0.FC5.1.npuc
```

# apache (BASIC認証)

AuthType	basic
AuthName	"LDAP Working Group"
AuthzLDAPMethod	ldap
AuthzLDAPServer	localhost
AuthzLDAPUserBase	ou=Users,dc=npu,dc=ac,dc=jp
AuthzLDAPGroupBase	ou=Groups,dc=npu,dc=ac,dc=jp
AuthzLDAPUserScope	subtree
AuthzLDAPGroupScope	subtree
AuthzLDAPUserKey	uid
AuthzLDAPGroupKey	cn
AuthzLDAPMemberKey	memberUid
AuthzLDAPMapUserToAttr	uid
AuthzLDAPSetGroupAuth	map
Require group グループ名	

```
$ rpm -q httpd  
httpd-2.2.3-5.npuc
```

# apache (グループ定義の例)

View - [cn=cron, ou=Private, ou=Domestic, ou=...

objectClass: sambaGroupMapping  
posixGroup

sambaSID: S-1-5-21-1116196674-3591202597-2404333293-1026

gidNumber: 1026

memberUid: hotta  
akase  
m-ogawa  
mskimr  
minemaz  
ko1  
tsaito  
mogawa  
tyoshida

sambaGroupType: 2

sambaSIDList: S-1-5-21-1116196674-3591202597-2404333293-513

description: cron メール転送先

cn: cron

グループ番号

グループに所属するメンバー

グループ名

OK

# Samba (PDC/BDC, ファイルサーバ)

- smbldap\_tools相当の機能をPHPで内製して運用中
  - perlスクリプトに手を入れるスキルと気力がなかった
- /etc/samba/smb.confのあちこちで設定
- 参考文献
  - 徹底解説 Samba LDAPサーバ構築(武田 保真 (著))
  - Sambaのすべて(高橋 基信 (著))
  - <http://www.samba.gr.jp/>
- 詳細内容の掲載は割愛
  - 現時点ではSambaのバージョンごとに微妙な差異
  - 将来的にはSambaにLDAPサーバ機能が統合される？
  - 今後のSambaとOpenLDAPとの関係はどうなるの？

```
$ rpm -q samba  
samba-3.0.21b-2.npuc
```

# DHCP（全データをLDAPで）

```
$ rpm -q dhcp
```

```
dhcp-3.0.1-58.EL4.npuc
```

```
$ cat rpm/SPECS dhcp.spec
```

（中略）

```
Patch155: dhcp-3.0pl2-npuc.lldap.patch
```

```
Patch156: dhcp-3.0.1-  
  ldap_dynamicoption.patch
```

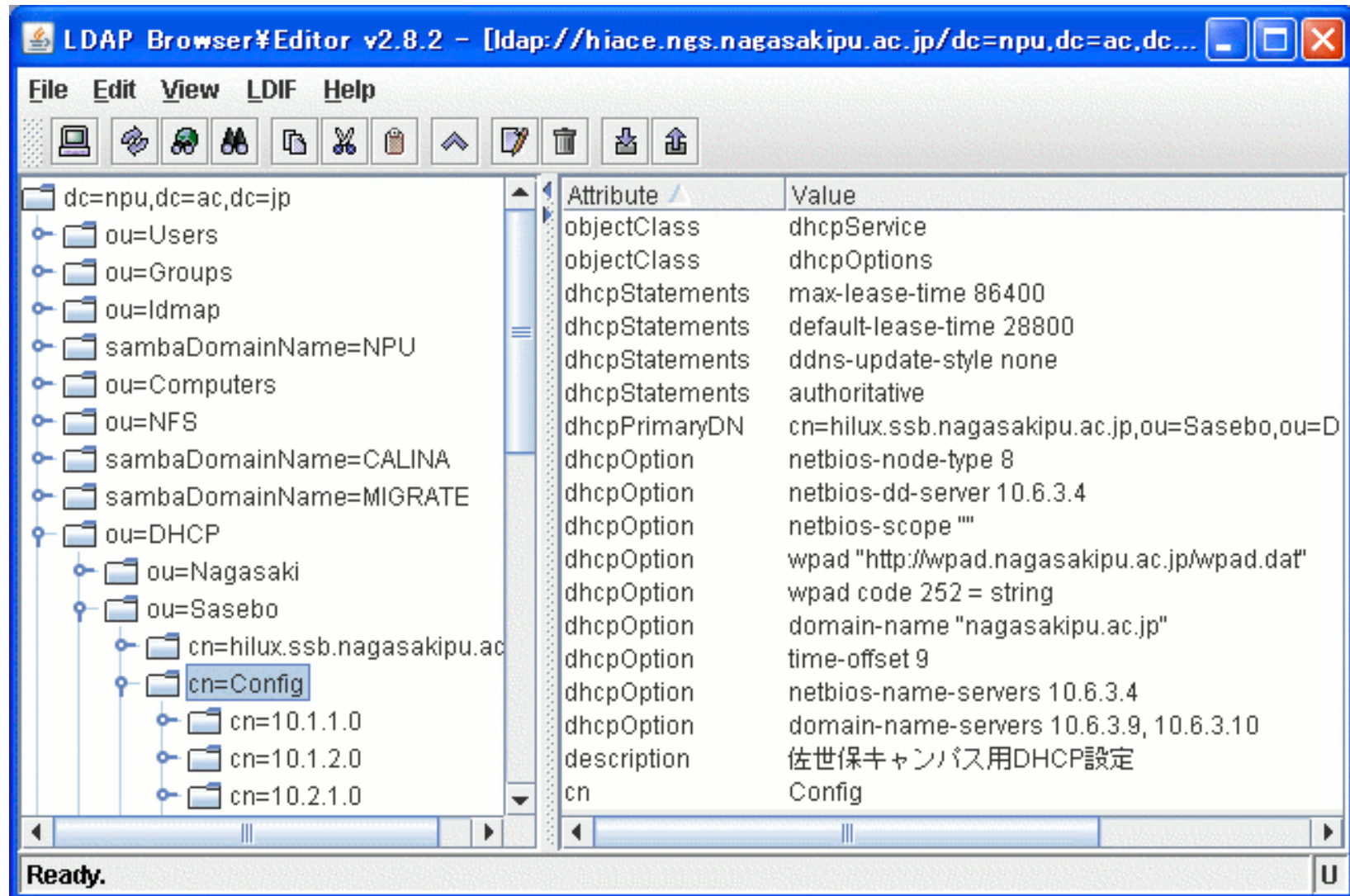
```
Patch157: dhcp-3.0.1-npuc-verbose.patch
```

# DHCP設定ファイル

```
$ cat /etc/dhcpd.conf
ldap-server "127.0.0.1";
ldap-port 389;
ldap-username
    "cn=Manager,dc=npu,dc=ac,dc=jp";
ldap-password "ないしょ";
ldap-base-dn
    "ou=Sasebo,ou=DHCP,dc=npu,dc=ac,dc=jp";
ldap-method dynamic;
(これだけ)
```



# DHCP (グローバル設定)



The screenshot shows the LDAP Browser Editor v2.8.2 interface. The left pane displays a tree view of the LDAP directory structure. The right pane shows the details of the selected entry, which is a DHCP service configuration.

LDAP Browser Editor v2.8.2 - [ldap://hiace.ngs.nagasakiu.ac.jp/dc=npu,dc=ac,dc=...

File Edit View LDIF Help

dc=npu,dc=ac,dc=jp

- ou=Users
- ou=Groups
- ou=ldmap
- sambaDomainName=NPU
- ou=Computers
- ou=NFS
- sambaDomainName=CALINA
- sambaDomainName=MIGRATE
- ou=DHCP
  - ou=Nagasaki
    - ou=Sasebo
      - cn=hilux.ssb.nagasakiu.ac.jp
        - cn=Config
        - cn=10.1.1.0
        - cn=10.1.2.0
        - cn=10.2.1.0

Attribute	Value
objectClass	dhcpService
objectClass	dhcpOptions
dhcpStatements	max-lease-time 86400
dhcpStatements	default-lease-time 28800
dhcpStatements	ddns-update-style none
dhcpStatements	authoritative
dhcpPrimaryDN	cn=hilux.ssb.nagasakiu.ac.jp,ou=Sasebo,ou=D
dhcpOption	netbios-node-type 8
dhcpOption	netbios-dd-server 10.6.3.4
dhcpOption	netbios-scope ""
dhcpOption	wpad "http://wpad.nagasakiu.ac.jp/wpad.dat"
dhcpOption	wpad code 252 = string
dhcpOption	domain-name "nagasakiu.ac.jp"
dhcpOption	time-offset 9
dhcpOption	netbios-name-servers 10.6.3.4
dhcpOption	domain-name-servers 10.6.3.9, 10.6.3.10
description	佐世保キャンパス用DHCP設定
cn	Config

Ready. U

# DHCP (セグメント設定)

The screenshot shows the LDAP Browser Editor v2.8.2 interface. The window title is "LDAP Browser Editor v2.8.2 - [ldap://hiace.nsg.nagasakiu.ac.jp/dc=...". The menu bar includes "File", "Edit", "View", "LDIF", and "Help". The toolbar contains icons for home, refresh, search, zoom, print, cut, paste, undo, redo, delete, and save. The left pane shows a tree view of LDAP entries under "ou=DHCP":

- ou=DHCP
  - ou=Nagasaki
  - ou=Sasebo
    - cn=hilux.ssb.nagasakiu.ac
    - cn=Config
      - cn=10.1.1.0 (selected)
      - cn=pool
      - cn=shige\_01
      - cn=kikaku\_001
      - cn=kouenkai\_001

The right pane displays the attributes and values for the selected entry:

Attribute	Value
objectClass	dhcpOptions
objectClass	dhcpSubnet
dhcpOption	routers 10.1.1.254
dhcpOption	subnet-mask 255.255.255.0
dhcpOption	broadcast-address 10.1.1.255
dhcpNetMask	24
description	本館：総務課、学生支援課、企...
cn	10.1.1.0

The status bar at the bottom left shows "Ready." and the bottom right shows "U".

# DHCP（個別エントリ）

The screenshot shows the LDAP Browser Editor v2.8.2 interface. The window title is "LDAP Browser Editor v2.8.2 - [ldap://hiace.ngs.nagasakiu.ac.jp/dc=npu,dc=ac,dc=...". The menu bar includes File, Edit, View, LDIF, and Help. The toolbar contains icons for home, refresh, connect, disconnect, search, print, cut, copy, paste, up, edit, delete, download, and upload. The left pane shows a tree view of LDAP entries under "sambaDomainName=MIGRATE" and "ou=DHCP". The selected entry is "cn=kikaku\_001" under "cn=10.1.1.0". The right pane displays the attributes and values for this entry:

Attribute	Value
objectClass	dhcpHost
dhcpStatements	fixed-address 10.1.1.11
dhcpHWAddress	ethernet 00:19:db:10:95:f5
description	2007/04/21 18:13:44 sa-kikakuC1 企画広報課
cn	kikaku_001

The status bar at the bottom left shows "Ready." and the bottom right shows "U".

設置済みノード一覧 - Mozilla Firefox

ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)

http://[redacted]/node-list/index.php?vlan

はじめよう 最新ニュース home 大学 地元・SNS 検索・地図 購買 OSS 旅行 読み物 ゲーム top

Google 検索

Yahoo! JA... [mixi] Google カ... Twitter codeなごがし Campusイ... 設置...

## 設置済みノード一覧 (2007/11/09 現在)

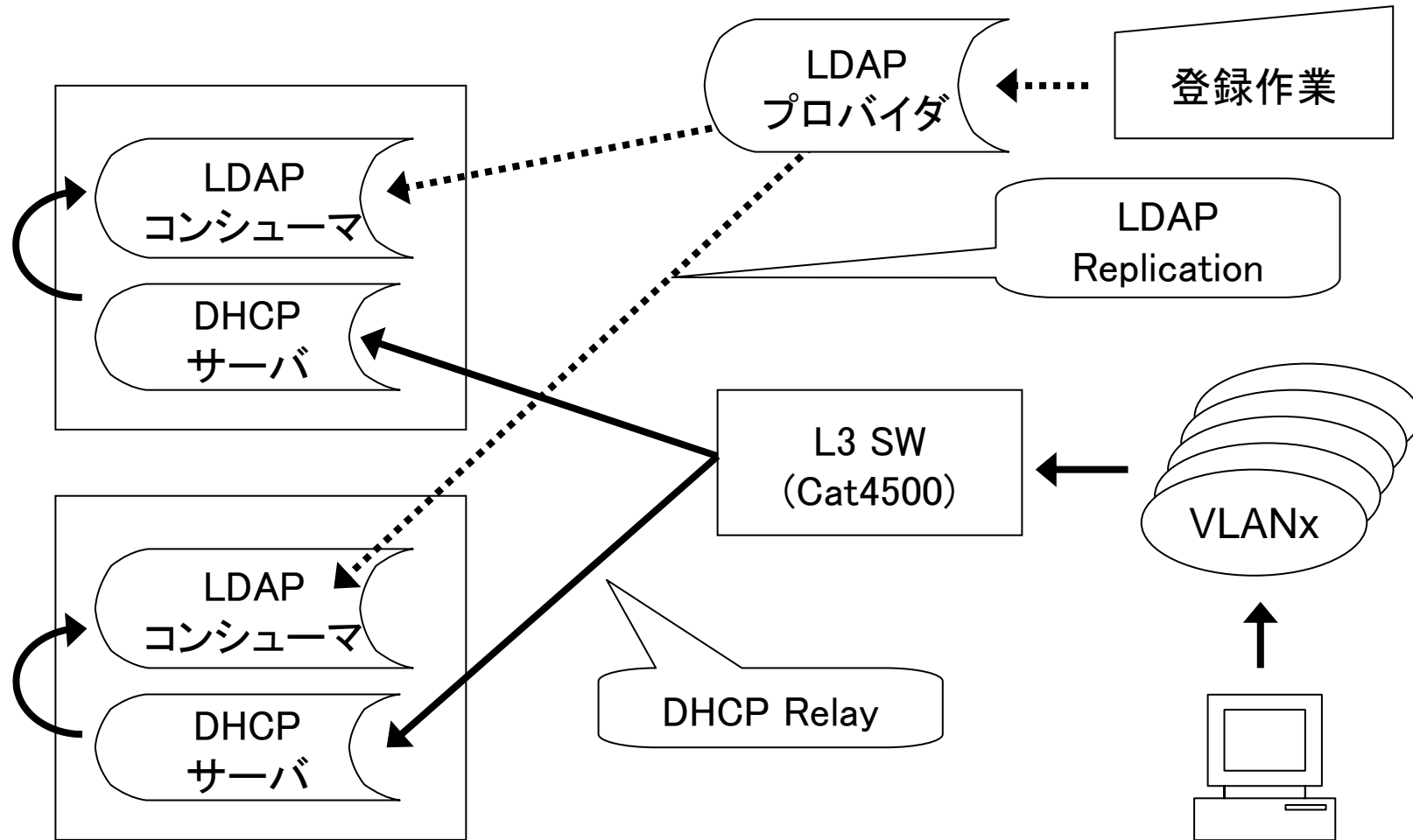
VLAN選択: [\[101\]](#) [\[102\]](#) [\[201\]](#) [\[301\]](#) [\[302\]](#) [\[303\]](#) [\[304\]](#) [\[401\]](#) [\[402\]](#) [\[601\]](#) [\[602\]](#) [\[607\]](#) [\[701\]](#) [\[702\]](#) [\[703\]](#) [\[704\]](#) [\[705\]](#) [\[706\]](#) [\[707\]](#) [\[709\]](#) [\[710\]](#) [\[711\]](#) 1301

VLAN1301 情報システム室

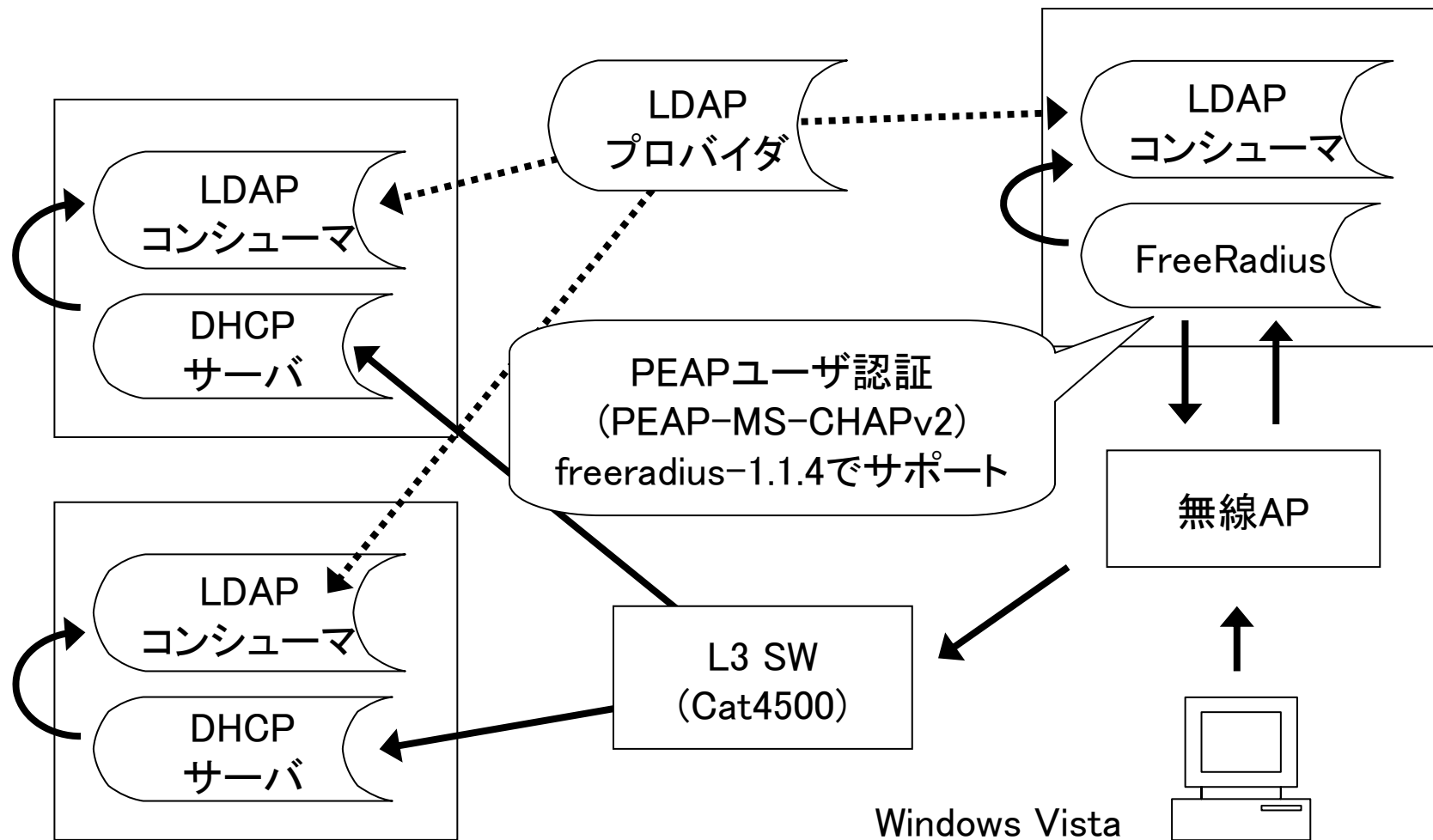
IP	MAC	cn	description
10.13.1.1	00:80:45:22:2a:59	ko1_001( [redacted] 浩一)	2007/04/28 14:29:19 [redacted]
10.13.1.2	08:00:46:99:5b:bc	kanri_002( DHCP登録管理者用)	2007/05/20 11:42:25 情報センター接続確認用PC VAI01 PCG-V505R/PB
10.13.1.3	00:0d:5e:fe:62:b7	shige_005( [redacted] 俊博)	2007/05/21 17:26:34 情報処理システム室管理図書情報センター貸出用ノートPC sl-LinfoC6 2007/11/08 11:30:16 vlan303追加登録
10.13.1.4	00:0d:5e:fe:5c:0f	shige_006( [redacted] 俊博)	2007/05/21 17:27:16 情報処理システム室管理図書情報センター貸出用ノートPC sl-LinfoC4 2007/11/08 14:37:34 vlan303追加登録
			2007/05/21 17:27:51 情報処理システム室管

完了 Pathtraq 01/08

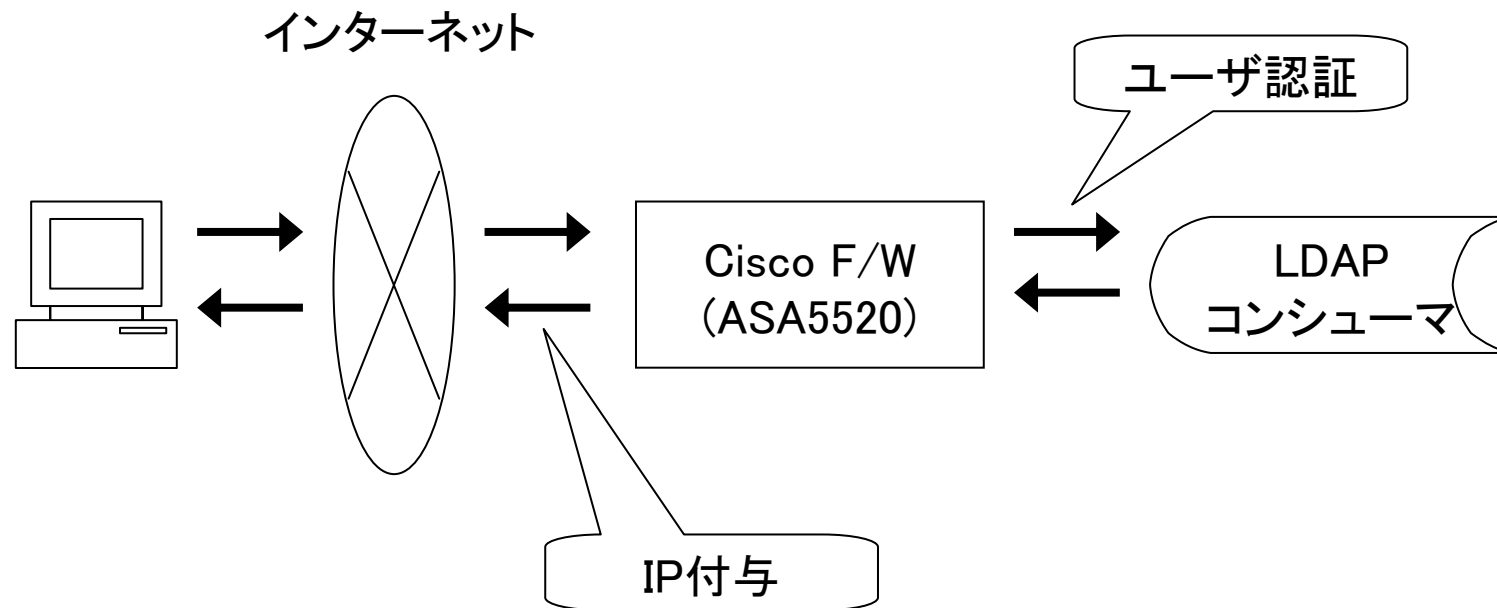
# DHCP



# Radius認証



# アプライアンスによるVPN認証



# VPN認証（設定部分）

The screenshot displays the Cisco ASDM 5.2 for ASA configuration interface. The main window is titled "Edit AAA Server" and shows the configuration for an LDAP server. The left sidebar shows the configuration tree with "AAA Server Groups" selected. The main configuration area includes the following fields:

- Server Group: ldap
- Interface Name: DMZ
- Server Name or IP Address: hiace
- Timeout: 5 seconds
- LDAP Parameters:
  - Enable LDAP over SSL
  - Server Port: 389
  - Server Type: -- Detect Automatically --
  - Base DN: ou=Users,dc=npu,dc=ac,dc=jp
  - Scope: All levels beneath the Base DN
  - Naming Attribute(s): uid
  - Login DN: cn=Manager,dc=npu,dc=ac,dc=jp
  - Login Password: [masked]
  - LDAP Attribute Map: -- None --



# 内製部分

```
$ rpm -qa|grep php|sort
```

```
php-5.2.5-1.npuc
```

```
php-cli-5.2.5-1.npuc
```

```
php-common-5.2.5-1.npuc
```

```
php-ldap-5.2.5-1.npuc
```

```
php-mbstring-5.2.5-1.npuc
```

```
php-oci8-5.2.5-1.npuc
```

```
php-pdo-5.2.5-1.npuc
```

```
php-pear-1.4.9-4
```

```
php-pear-Auth-SASL-1.0.2-4.el5.centos
```

```
php-pgsql-5.2.5-1.npuc
```

## 動作環境

PHP-5.2.x

PEAR(クラスライブラリ)

Smarty(テンプレートエンジン)

Creole(DB抽象レイヤー)

PostgreSQL-8.2.x

Oracle10g

mysql-5.0.22

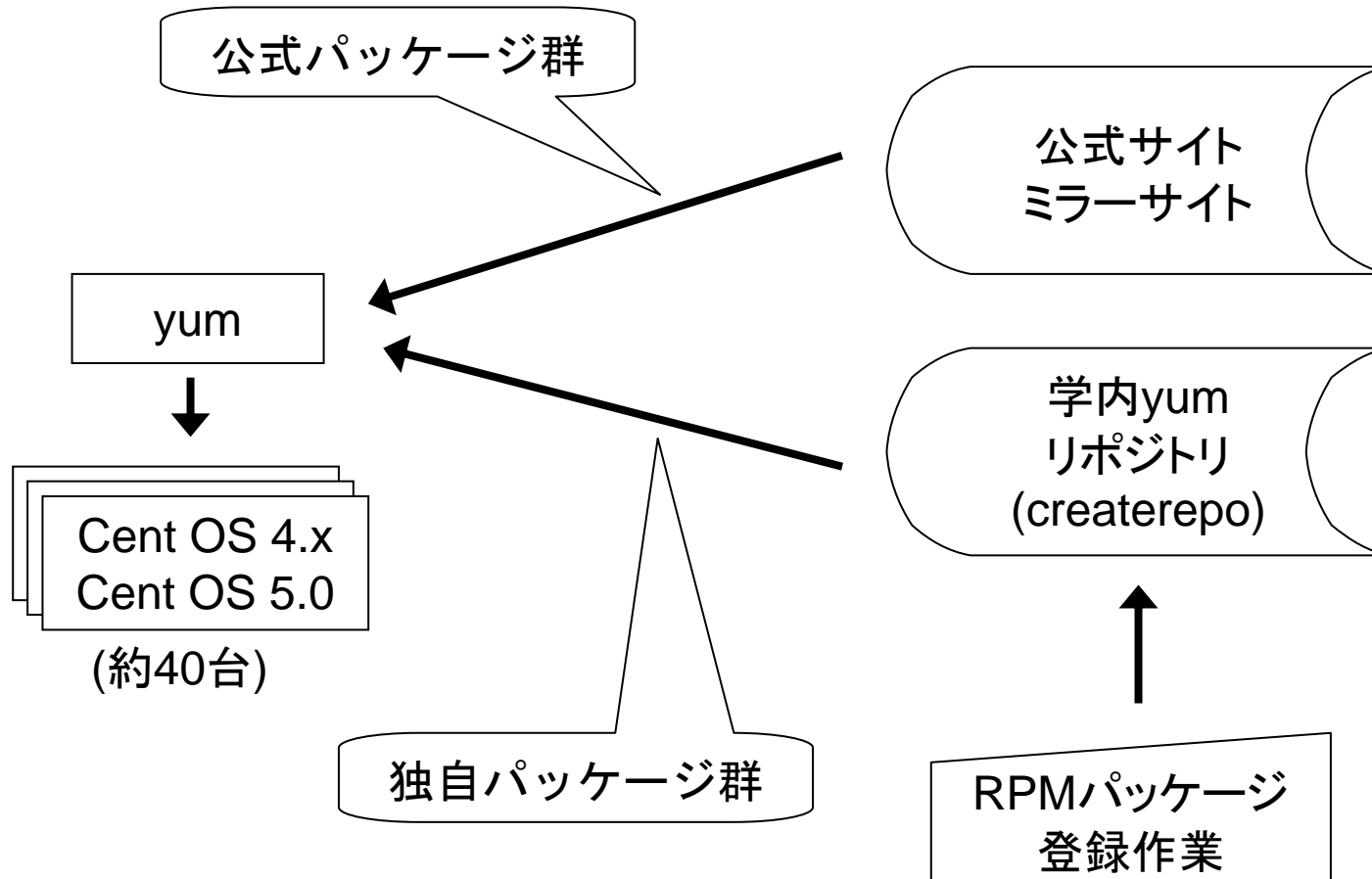
# 構築・運用環境

1. OSインストール
2. 環境構築スクリプト(引数:ホスト名のみ)
  1. ネットワーク設定(IPアドレス等)
  2. yumリポジトリを内部にも向ける
  3. yumにより最新環境へ追従
  4. 自動起動サービス設定
  5. 管理者アカウント設定 / ssh公開鍵設置
  6. 管理者グループ / sudoers設定
  7. LDAP コンシューマ設定スクリプト起動

# LDAP コンシューマ設定スクリプト

1. LDAPパッケージ群の取得・インストール
2. 設定ファイルの設置
3. LDAP-DB用データディレクトリの準備
4. ルートノードの作成
5. コンシューマ特有の設定(slapd.confの無効化)
6. sysylog設定
7. logrotate設定
8. olcReferral 設定の投入
9. syncrepl 設定の投入

# RPMパッケージ構築・運用環境



# まとめ

- LDAPは、とっつきにくい
- RDBMSとの住み分けが難しい

それでも

- /etc/passwordを配るよりはまし
- パスワードを付箋に書いて貼られるよりはまし
- アラユル一元管理が可能(かも?)

あなたもおひとついかがですか？

ご静聴ありがとうございました

