日本LDAPユーザ会 設立記念セミナー

LDAP入門

設立発起人代表：小田切耕司

オープンソース・ソリューション・テクノロジ株式会社

【お問い合わせ先】
staff@ldap.jp
http://www.ldap.jp

Part 1.

ディレクトリ・サービスとLDAP

ディレクトリ・サービスとは？『Wikipedia』より

- ディレクトリ・サービスは、LANなどのコンピュータ・ネットワーク上にあるユーザ情報、グループ情報、接続されているコンピュータやプリンター、アプリケーション、さまざまなソフトの設定情報などの資源を記憶し、検索しやすいようにまとめたものである。（つまりいろいろなコンピュータの中にある情報を統合管理するもの。 一カ所で集中管理する訳ではない、分散管理が可能）
- ネットワークを一元管理するための情報を保存し、利用するために、企業等の比較的規模の大きいコンピュータ・ネットワークで利用されることが多い。
- ディレクトリ・サービスにアクセスするためのプロトコルをDAPと呼ぶが、近年では、LDAPというプロトコルが標準的に用いられるようになってきた。
- LDAPに対応していない製品も多く、その場合には専用のプロトコルを利用することとなる。
- LDAP以外のディレクトリ・サービス例
  - NIS、NIS+、DNS
- ディレクトリ・サービスを提供するベンダー独自製品例
  - （1990年代の）Novell Netware、Lotus Nots、MS Exchange

LDAPとは？『Wikipedia』より

- LDAP(えるだっぷ、Lightweight Directory Access Protocol)は、ディレクトリ・サービスに接続するために使用されるプロトコル(DAP)の一つ。
- ITU勧告X.500モデルをサポートするディレクトリに対するアクセスを提供するために設計され、一方で、X.500ディレクトリアクセスプロトコル(Directory Access Protocol : DAP)の資源要求は課されない。
- 本プロトコルは、ディレクトリに対する対話的な読み込み/書き込み(read/write)アクセスを提供する管理アプリケーションやブラウザアプリケーションを特に対象とする。
- X.500プロトコルをサポートするディレクトリと共に使用する際に、X.500のDAPを補完するものとなることが意図されて開発。
- 「X.500の90%の機能を10%のコストで実現する」が目標で設計

LDAPとは？『Wikipedia』より

- コンピュータ・ネットワークでは、ネットワークを構成する機器が多くなるにつれて扱うべきネットワーク・リソースが増大する。
- DAP が登場した背景には、個々に異なるディレクトリ・サービスを扱うよりも、統一されたプロトコルで拡張可能な情報にアクセスする方法が求められるようになった。
- X.500 シリーズは、分散可能な統合案内サービスとして優れた機能を有していたものの、DAP が複雑なため処理が重たく、TCP/IP によるインターネットでは使用されにくいという欠点があった。
- この点を改良した LDAPv2(RFC1777) が IETF によって標準化され、ミシガン大学において最初の処理系が誕生した。
- LDAPv2 では、LDAP サーバは X.500 のフロントエンドとして機能し、分散化は X.500 が担っている。
- LDAP サーバによる分散化を実現する LDAPv2+ は、多くの処理系で使用された。その後、分散化のための仕様を含み、セキュリティが強化された LDAPv3(RFC2251) が規定されている。

商用LDAP製品

- Sun Java Directory Server (Sun Microsystems)
- Active Directory (Microsoft)
  - でもUnixでADをLDAPとして使うのは大変（Sambaを使うと良い）
- Tivoli Directory Server (IBM)
- Lotus Notes/Domino (IBM)
- Enterprise Directory Server(NEC)
- Oracle Internet Directory(Oracle)
- Novell eDirectory(Novell)
- InfoDirectory（富士通）
- SDS : Sendmail Directory Server (sendmail社）
- Red Hat Directory Server (Red Hat社)

オープンソースソフトLDAP製品

- OpenLDAP
  - ほとんどのLinux ディストリビューションに同梱されるオープンソースのLDAP
  - Red Hat、SuSE、Debianなどに採用済み
  - 無償で使える（サポートは有償）
- Fedora Directory Server (Red Hat)
  - かつてのNetscape Directory ServerをRed Hat社が買い取りOSSにしたもの
  - 開発者向けで業務用ではない

Part 2.

LDAPの基本

LDAPの基本アクセス

- 基本は以下のアクセス
  - ldapadd：エントリ追加
  - ldapdelete：エントリ削除
  - ldapmodify：エントリ更新
  - ldapsearch：検索
- やり取りするデータは原則LDIF形式
  - LDAP Data Interchange Format
  - テキスト形式：文字コードはUTF-8
  - バイナリはbase64でエンコード
  - 「属性：データ」で一行
  - 最初は「dn: 識別名(Distinguished Name）」
  - 空白行でエントリの切れ目

LDIFの例

```
dn: dc=osstech,dc=co,dc=jp
objectClass: dcObject,organization
o: osstech
dc: osstech

dn: ou=Users,dc=osstech,dc=co,dc=jp
objectClass: top,organizationalUnit
ou: Users

dn: uid=Administrator,ou=Users,dc=osstech,dc=co,dc=jp
cn: Administrator
sn: Administrator
objectClass: top,person,organizationalPerson
objectClass: inetOrgPerson,posixAccount,shadowAccount
gidNumber: 0
uid: Administrator
uidNumber: 0
userPassword:: e1NTSEF9YTlCdFpmYVVVeTVLWUtSaWFWaFo=
homeDirectory: /home
```

LDAPとRDBMSの違い

- LDAP(ネットワークプロトコル)とSQL(言語)
- ディレクトリサービスにはACID特性がないことに注意！
  - 今書いたデータが今すぐ読めるとは限らない！

	LDAP	RDBMS
用途	検索性能重視、頻繁な更新には向かない	検索だけでなく頻繁な更新も重視
構造	木構造(行や列といった概念はない)	表構造(行や列が存在)
スキーマ	既存の登録済みスキーマ(ObjectClass)を利用するのが一般的	ユーザが業務に合わせて個別に設計し、利用する
更新	トランザクションの概念はない (トランザクション機能を持った製品もある) 大量更新には向かないので1時間に数件といった更新頻度のものに利用する	トランザクションの概念あり 1秒間に何十、何百もの更新に耐えられる設計となっている
分散	ツリーの枝単位で分散配置が可能	キーの範囲で分散配置が可能
操作	LDAP(ネットワークプロトコル)で操作 プロトコルは単純	SQL(プログラム言語)で操作 複雑な操作が可能
検索手法	木の枝葉をたどるイメージ	表の行を走査するイメージ

LDAPで何ができるか？

- Linuxユーザの統合管理
  (Mail,FTP,Telnet,Proxy,sshなど)
- Samba/Windowsユーザの統合管理
- Webサーバ(Apache)のアクセス制御
- 電話帳、メールアドレス帳
- PKI(公開キー)の保管場所として

OpenLDAPが標準で提供するスキーマ(1)

- 標準提供のスキーマを見ればLDAP何ができるかわかる
- core.schema
  - OpenLDAPの核となるスキーマで以下のRFCで定義されたスキーマが定義されている。
    - ・RFC 2252/2256 (LDAPv3)
    - ・RFC 1274 (uid/dc)
    - ・RFC 2079 (URI)
    - ・RFC 2247 (dc/dcObject)
    - ・RFC 2587 (PKI)
    - ・RFC 2589 (Dynamic Directory Services)
    - ・RFC 2377 (uidObject)
  - これだけでは何もできないが、CNやOUなど他のスキーマを使うための基本部分が定義されている。
- cosine.schema
  - X.500やX.400で規定されたアトリビュートなど以下のようなものが定義されている。
    - ・RFC1274で定義されるhost,manager, documentIdentifierなど
    - ・DNSレコードであるAレコード、MXレコード、NXレコード、SOAレコード、CNAMEレコード
  - これらからDNSレコードの格納先としてLDAPサービスが利用できることがわかる。

OpenLDAPが標準で提供するスキーマ(2)

- inetorgperson.schema
  - インターネット特にメールアドレス帳のためのスキーマで以下のようなものが定義される。
    - メールアドレス、社員番号、オフィスと自宅住所、会社と自宅の電話番号、写真、
- misc.schema
  - mailLocalAddressやnisMailAliasなどメールサーバが使うスキーマが定義される。
- nis.schema
  - posixAccountやposixGroupなどLinux/UNIXのユーザ認証統合に必須なスキーマが定義される。
  - NISをLDAPに置き換えるのに必要なスキーマも定義されている。
- samba.schema
  - このスキーマはOpenLDAPではなく、Sambaパッケージによって提供されるが、Sambaを使ってWindows/Linux/UNIXのユーザ認証統合に必須なスキーマが定義される。
  - WindowsドメインをSambaに置き換えるのに必要なスキーマも定義されている。
- java.schema
  - javaClassName, javaCodebaseなどJava Object (RFC 2713)を扱うためのスキーマが定義される。
- corba.schema
  - corbaIor、corbaRepositoryIdなどCorba Object (RFC 2714) を扱うためのスキーマが定義される。

アドレス帳の構築例


```
dn: uid=ユーザ名,ou=Users,dc=ドメイン名,dc=co,dc=j
objectClass: posixAccount
objectClass: inetOrgPerson
cn: ユーザ名
sn: 名字
givenname: 名前
mail: メールアドレス
o: 会社名
ou: 所属
title: 役職
employeeNumber: 社員番号
telephoneNumber: 電話番号
facsimileTelephoneNumber: FAX番号
mobile: 携帯電話
st: 都道府県
l: 市区
street: 番地
postalAddress: 番地
postOfficeBox: ビル名
postalCode: 郵便番号
homePostalAddress: 自宅住所
homePhone: 自宅電話
```

```
dn: uid=odagiri, ou=Users, dc=osstech,dc=co,dc=jp
objectClass: posixAccount
objectClass: inetOrgPerson
cn: odagiri
sn: 小田切
givenname: 耕司
mail: odagiri@osstech.co.jp
o: オープンソース・ソリューション・テクノロジ株式会社
ou: 技術部
title: チーフアーキテクト
employeeNumber: 1
telephoneNumber: 03-1234-5678
facsimileTelephoneNumber: 03-8765-4321
mobile: 090-5432-1234
st: 東京都
l: 品川区西五反田
street: 2-6-3
postalAddress: 2-6-3
postOfficeBox: 東洋ビル
postalCode: 107-0052
homePostalAddress: 神奈川県藤沢市藤沢123-45
homePhone: 0466-23-4567
```

LDAPへのデータ投入

実行例）Windows上でuser-sjis.txtを作成し、Linux上に転送した場合

```
# iconv -f SJIS -t UTF8 user-sjis.txt -o user-utf8.ldif
```

- -f SJISは入力ファイルがSJISで記述されていることを示す。
- -t UTF8は出力ファイルをUTF-8に変換することを意味する。
- user-sjis.txtは入力ファイル名、-o user-utf8.ldifは出力ファイル名を意味する。

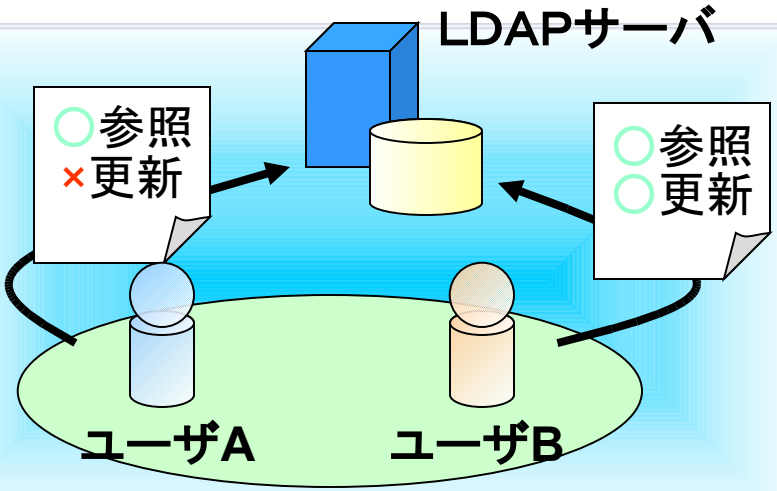
```
# ldapmodify -x -w secret -D
  cn=Manager,dc=osstech,dc=co,dc=com -f user-utf8.ldif
```

- -DはLDAP管理者のDN、-Wは管理者パワード

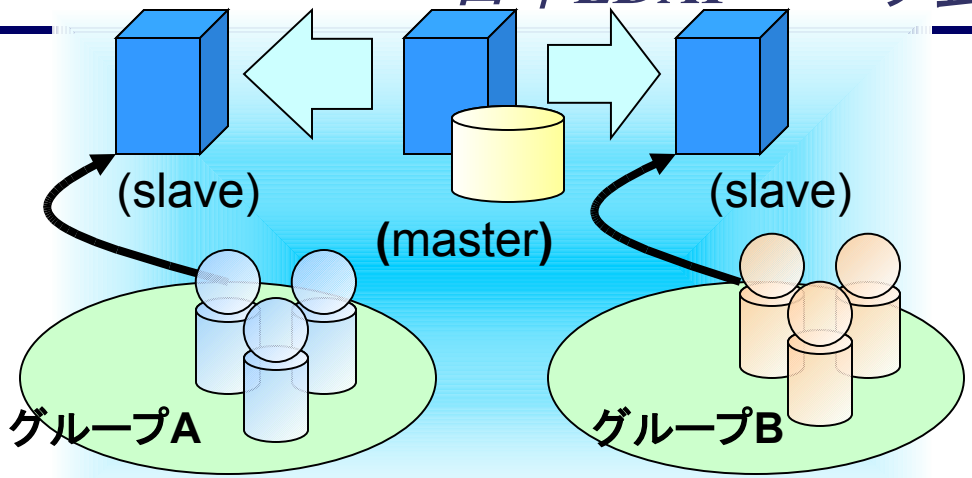
LDAPを使うことの利点

- **機能拡張性が高い**
  ユーザー管理だけでなく，組織情報の管理，コンピュータの管理，アプリケーションの管理，メール・アドレス帳，電話帳などいろいろな用途で自由に拡張して使用できる
- **UNIX/Linux だけでなくSamba やWindows でも利用できる**
- **性能に関しても拡張性が高い**
  商用のLDAP 製品は数十億のデータ・エントリでも実運用に耐える処理性能を備えている。
  Linux ディストリビューションに添付されるオープンソースのOpenLDAPも数千～数万エントリでの実績が多数ある
- **細かなアクセス制御機能を有しており，SSL などでの暗号化も可能でセキュリティが強固である**
- **ディレクトリを木構造で管理でき，サーバーの分散管理が可能である**
- **複製機能を備えており，障害にも対応できる**

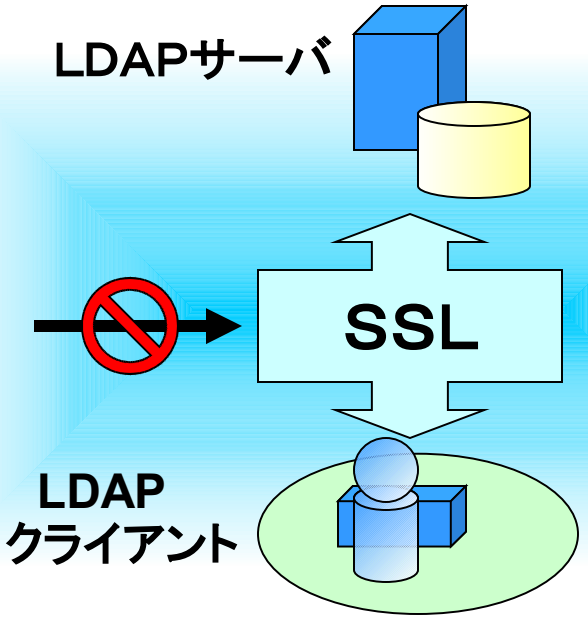
アクセス制御



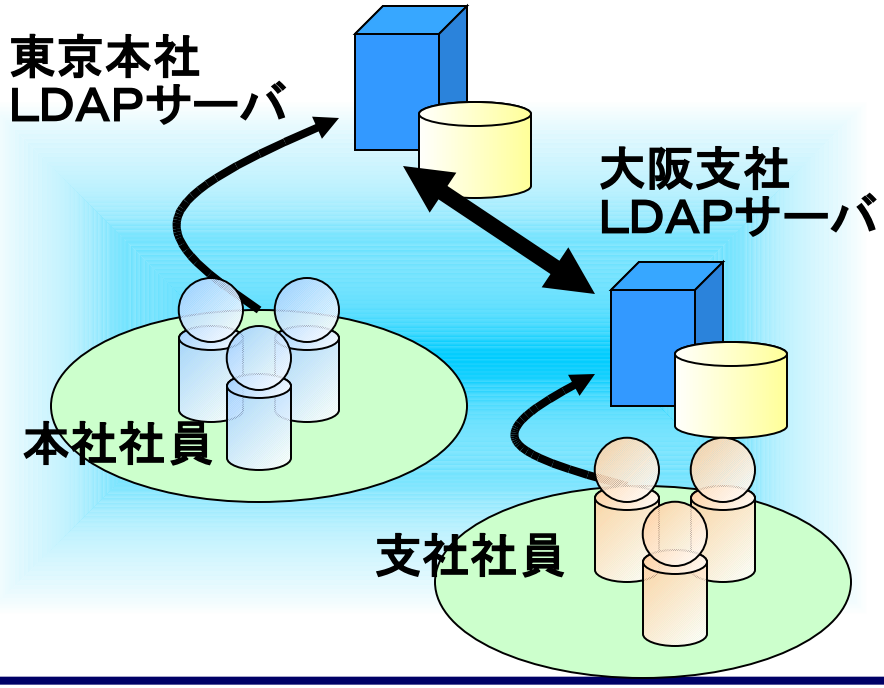
レプリケーション



通信経路暗号化



分散管理(referral)



Part 3

OpenLDAPサーバ簡単設定

OpenLDAPサーバの設定

- **設定ファイル**
  サーバ：/etc/openldap/slapd.conf
  クライアント：
  - NSS,PAM**用：**/etc/ldap.conf
  - ldapadd**などの管理コマンド用**:
    /etc/openldap/ldap.conf

/etc/slapd.confﾊﾟﾗﾒｰﾀ(必須1)

- suffix **ベース・サフィックスを指定する**
  通常はﾄﾞﾒｲﾝ名をﾍﾞｰｽに指定
  例）suffix dc=osstech,dc=co,dc=jp
  suffix "ou=sales,ou=yokohama,dc=local"

CN=commonName
L=localityName
ST=stateOrProvinceName
O=organizationName
OU=organizationalUnitName
C=countryName
STREET=streetAddress
DC=domainComponent
UID=userid

/etc/slapd.confﾊﾟﾗﾒｰﾀ(必須2)

- rootdn
  LDAPサーバの管理者のDN(Distinguished Name：識別名)を指定する。
  なお管理者DNを含むユーザDNには、英大文字、英子文字の区別はない。
  管理者DNの例）
  - rootdn "cn=Manager,dc=osstech,dc=co,dc=jp"
- rootpw
  LDAPサーバの管理者パスワードを設定する。
  - そのままのパスワードを指定するか暗号化したものを設定する
  - 例）miracleというパスワードをMD5ハッシュする
    # slappasswd -s secret -h {sha}
  - rootdnをLDAPに登録されているユーザを指定し、LDAPの中にパスワードが格納されていれば、rootpwを指定する必要はない。

/etc/slapd.confパラメータ(3)

- include
  - 与えたファイルから追加の設定情報を読み込む。
  - 通常はスキーマ定義ファイルを読み込むために使用する
    例) include /etc/openldap/schema/samba.schema
- database
  - LDAPのデータを格納するのに使用するバックエンド・データベースを指定。現在bdb, hdb, ldap, sql などを指定できる。
    通常 bdb を使用
- directory
  - BDBファイルを格納するディレクトリを指定
  - 例)directory /var/lib/ldap
- index
  - 作成する索引の属性とタイプを指定する。
    - 例1) uid,gidに関してequal(等値)検索用の索引を作成
      index uidNumber,gidNumber eq
    - 例2) mail(メールアドレス)、surname(名字)に関して、equal検索用とsubinitial(前方一致)の索引を作成
      index mail,surname eq,subinitial

/etc/slapd.confﾊﾟﾗﾒｰﾀ(4)

- Slapd.confの例：サフィックスと管理者DN、管理者パスワードを設定（この3つだけで動かすことは可能、ただし正式運用にはもっと設定が必要）

```
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
include /etc/openldap/schema/nis.schema
include /etc/openldap/schema/samba.schema
database bdb
directory /var/lib/ldap
suffix "dc=osstech,dc=co,dc=jp“
rootdn "cn=Manager,dc=osstech,dc=co,dc=jp“
rootpw secret
index  objectClass,uidNumber,gidNumber,memberUid  eq
index  cn,mail,surname,givenname                 eq,subinitial
index  uid                                       pres,eq
index  rid                                       eq
```

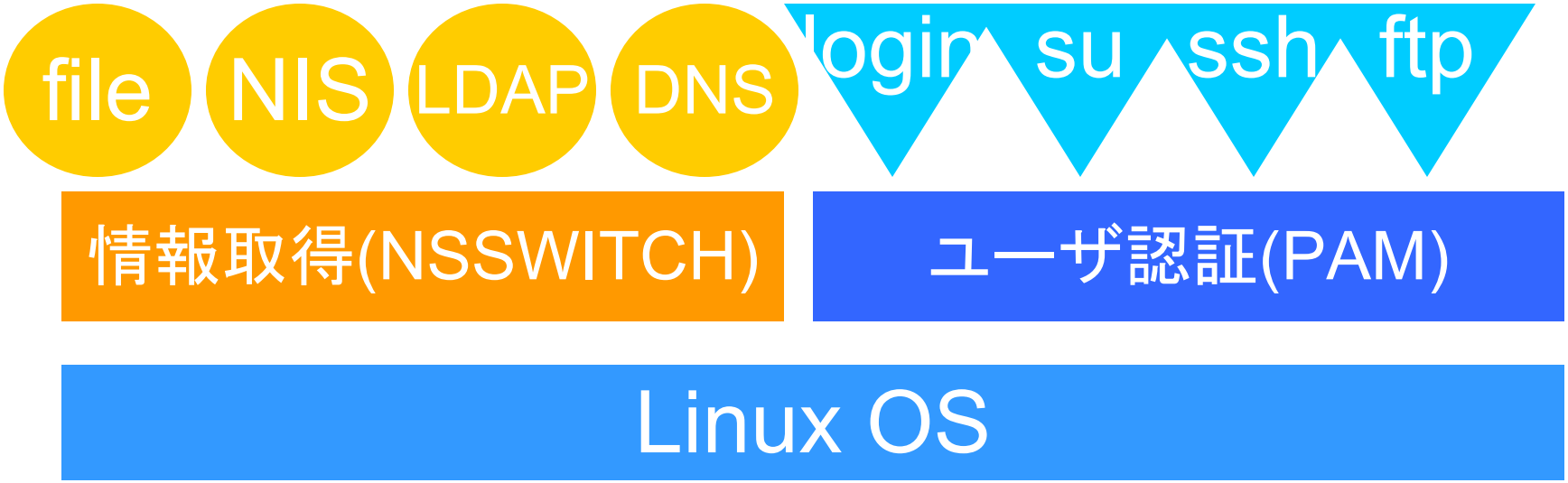
- 設定が終了したら、OpenLDAPデーモンを起動させる。
  # service ldap restart
- システム起動時に自動的に動くように以下を設定
  # chkconfig ldap on

Part 4.

LDAPによる認証統合

Linux/UNIXのユーザ管理機構

- NSSWITCH機能
  - /etc/nsswitch.confで、各種情報の取得先を指定可能
- PAM認証機構
  - /etc/pam.d/の中でアプリケーションごとの認証ルールを指定可能
- LDAP認証を使うには、NSS,PAMのサポートが必須
  - NSS,PAMに対応しないSUN4,HP-UX10に対しては、NIS-LDAPゲートウェイ(ypldapd: http://www.padl.com/)で対応可能



ネームサービススイッチ機能

- LDAPを認証で使用するには/etc/nsswitch.confを以下のように変更

```
passwd:   files   ldap
group:    files   ldap
shadow:   files   ldap
hosts:    files   dns   wins
```

- /lib/libnss_ldap.so.2が呼ばれる。
- /lib/libnss_wins.so.2 を使うとWINS(Windows Internet Name Service)を使って名前解決可能

プラグマブル認証機能

- /etc/pam.d/system-authに以下を設定

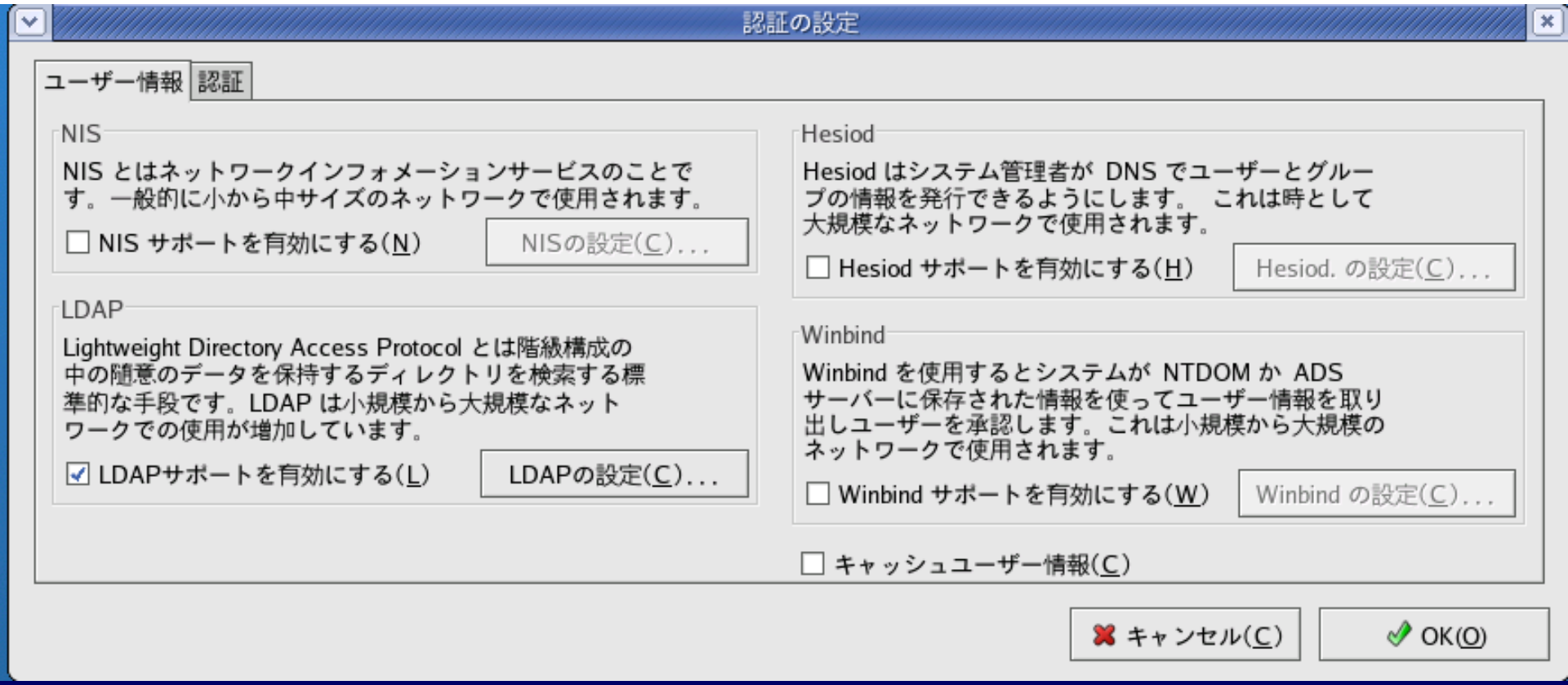
```
[root@fs02 /etc]# cat /etc/pam.d/system-auth
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      /lib/security/pam_env.so
auth        sufficient    /lib/security/pam_unix.so likeauth nullok
auth        sufficient    /lib/security/pam_ldap.so use_first_pass
auth        required      /lib/security/pam_deny.so

account     required      /lib/security/pam_unix.so
account     [default=ok user_unknown=ignore service_err=ignore system_err=ignore] /lib/security/pam_ldap.so

password    required      /lib/security/pam_cracklib.so retry=3
password    sufficient    /lib/security/pam_unix.so nullok use_authtok md5 shadow
password    sufficient    /lib/security/pam_ldap.so use_authtok
password    required      /lib/security/pam_deny.so

session     required      /lib/security/pam_limits.so
session     required      /lib/security/pam_unix.so
session     optional      /lib/security/pam_ldap.so
session     required      /lib/security/pam_mkhomedir.so skel=/etc/skel umask=0022
```

- /etc/pam.d/sshdなどに以下を設定

```
#%PAM-1.0
auth        required    /lib/security/pam_stack.so    service=system-auth
account     required    /lib/security/pam_stack.so    service=system-auth
password    required    /lib/security/pam_stack.so    service=system-auth
session     required    /lib/security/pam_stack.so    service=system-auth
```

LDAPクライアントをauthconfigで設定

- authconigにより/etc/nsswitc.confと/etc/openldap/ldap.conf、/etc/pam.d/system-authが変更される。
- authconfig実行例（ユーザ情報の設定）NSSWITCHの設定が行われる。



LDAPクライアントをauthconfigで設定

- authconigにより/etc/nsswitc.confと/etc/openldap/ldap.conf、/etc/pam.d/system-authが変更される。
- authconfig実行例（ユーザ情報の設定）
  PAMの設定が行われる。

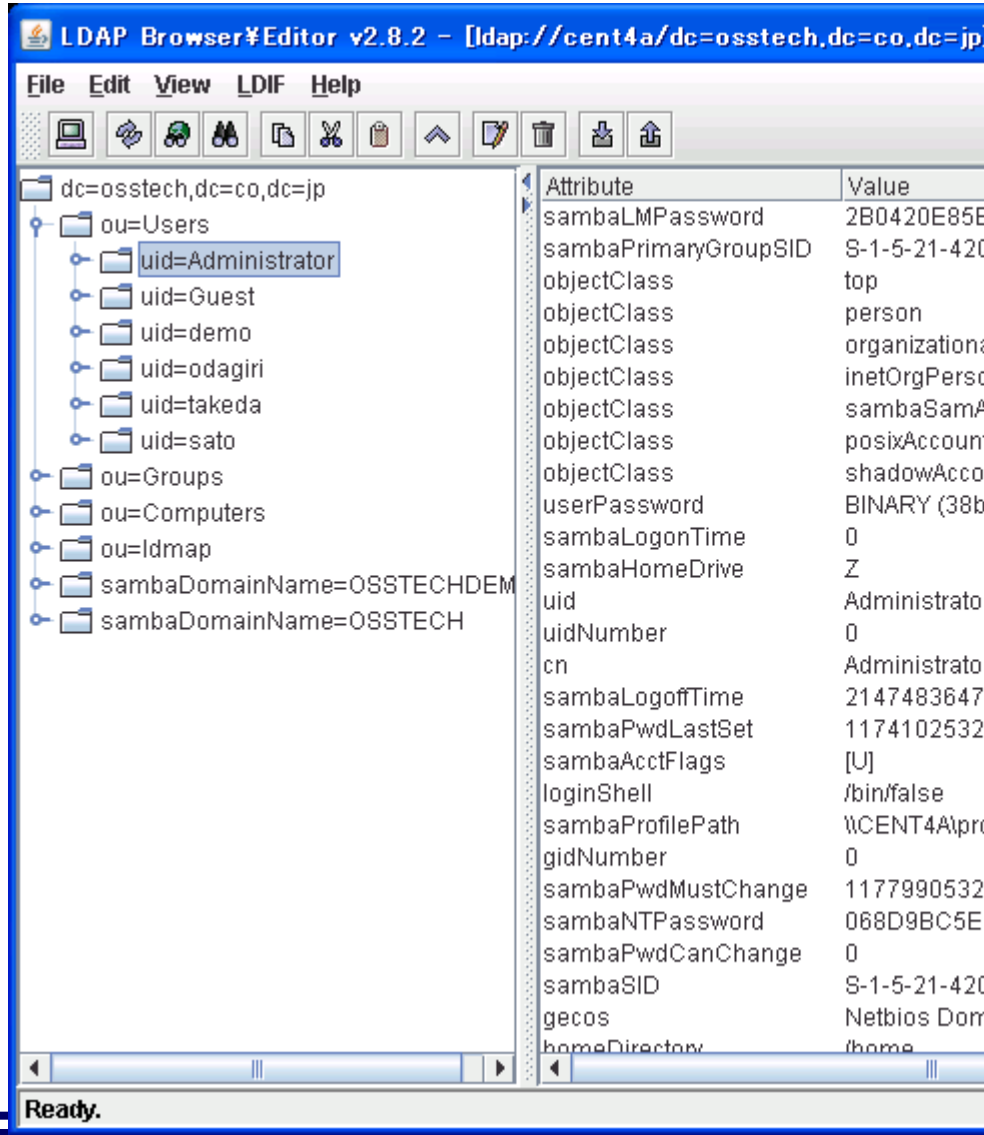
Part 5.

LDAP管理クライアント紹介

- smbldap-toolsによる管理
  - smbldap-populate.pl
    LDAPサーバの初期化を行う（rootツリーとデフォルトユーザの登録）
  - smbldap-useradd.pl
    UNIX/Linux およびSamba/Windowsユーザ アカウントを追加する
  - smbldap-userdel.pl
    UNIX/Linux およびSamba/Windowsユーザ アカウントを削除する
  - smbldap-usermod.pl
    UNIX/Linux およびSamba/Windowsユーザ アカウントを変更する
  - smbldap-usershow.pl
    UNIX/Linux およびSamba/Windowsユーザ アカウント情報を表示する
  - smbldap-passwd.pl
    UNIX/Linux およびSamba/Windowsユーザのパスワードを設定／変更する
  - smbldap-groupadd.pl
    UNIX/Linux およびSamba/Windowsのグループを追加する
  - smbldap-groupdel.pl
    UNIX/Linux およびSamba/Windowsのグループを削除する
  - smbldap-groupmod.pl
    UNIX/Linux およびSamba/Windowsのグループを変更る
  - smbldap-groupshow.pl
    UNIX/Linux およびSamba/Windowsのグループを表示する

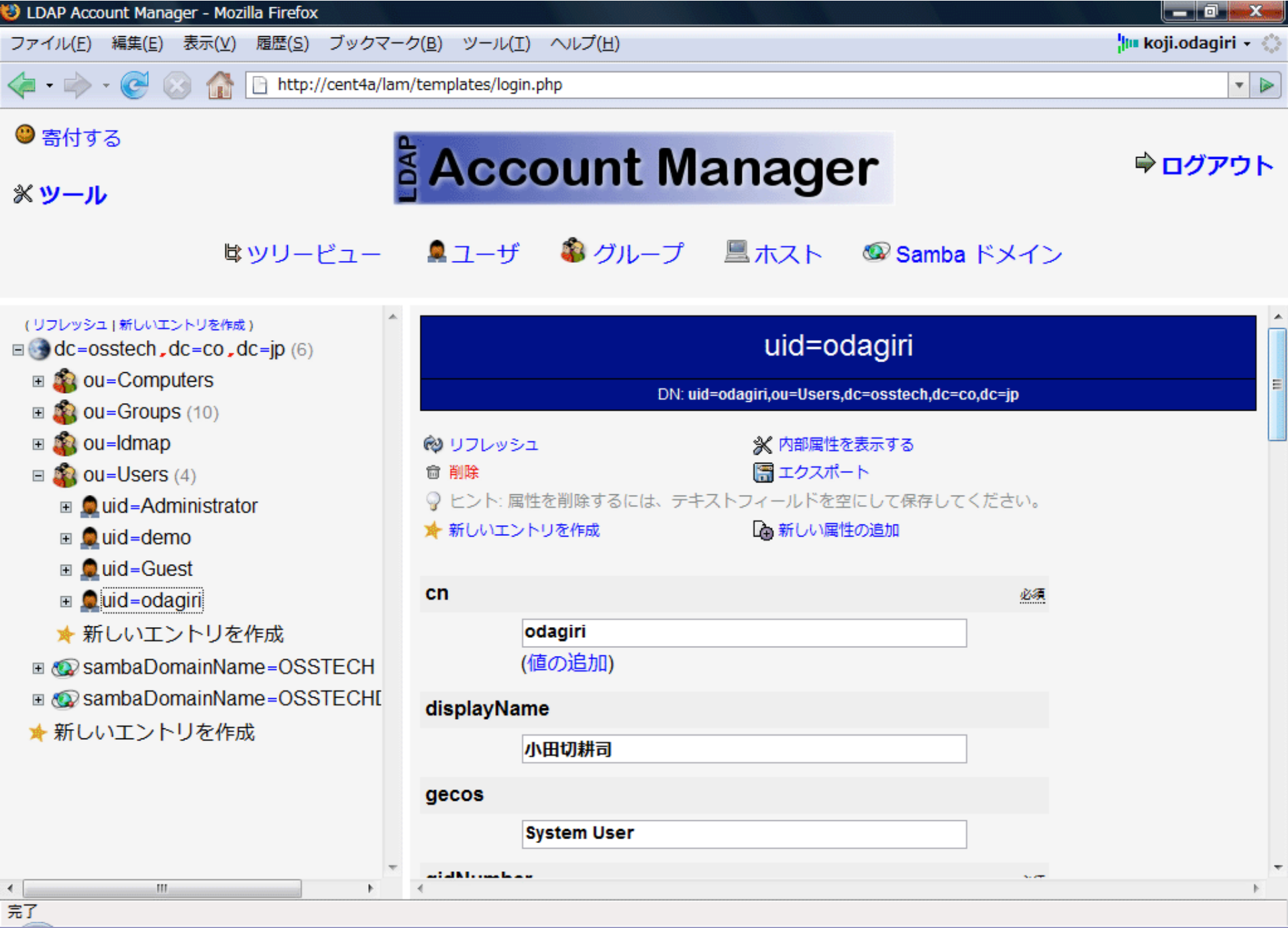
LDAPのGUIクライアントの紹介

- Linuxでのみ使用可能なツール
  - GQ(日本語利用不可):
    http://biot.com/gq/
- Windowsでのみ使用可能なツール
  - Softerra LDAP Browser(無償、図は実行例)、LDAP Administrator(有償):
    http://www.ldapadministrator.com/
- LinuxでもWindowsでも使用できるツール
  - LDAP Browser/Editor(JDK 1.2.2移行が必要)
    http://www.iit.edu/~gawojar/ldap/



LAM：LDAP Account Manager

- Solaris 10 / Red Hat EL 4 / CentOS 4**対応**
- Https**経由の**Web**クライアントから**LDAP**を管理可能**
- **プロファイルを変えることで分散管理を可能にする**



Samba 3.0.24 for Solaris/Linux （WinodwsのUSRMGR.EXEでユーザ管理）