WindowsでLDAP運用のこつ

JPUG PostgreSQL技術セミナー2007年春

2007 - 02 – 24

NPO法人　日本PostgreSQLユーザ会
（株）オープンソース総合研究所

桑村　潤

OpenLDAP

- LDAP
  - ディレクトリサービス
  - ディレクトリ情報
    - 伝統的命名法の階層ツリーの例
    - ドメイン名の階層ツリーの例
- OpenLDAP
  - OpenLDAPのプログラム
  - slapd.confの構成
    - database bdb
    - database sql

LDAP

- Lightweight Directory Access Protocol
- TCP/IPによるディレクトリサービスのフロントエンド
- ITU勧告X.500(DAP)をアクセス面で補完
- DAPv2(RFC1777) が IETF によって標準化
- LDAPv3(RFC2251) は分散化とセキュリティ強化

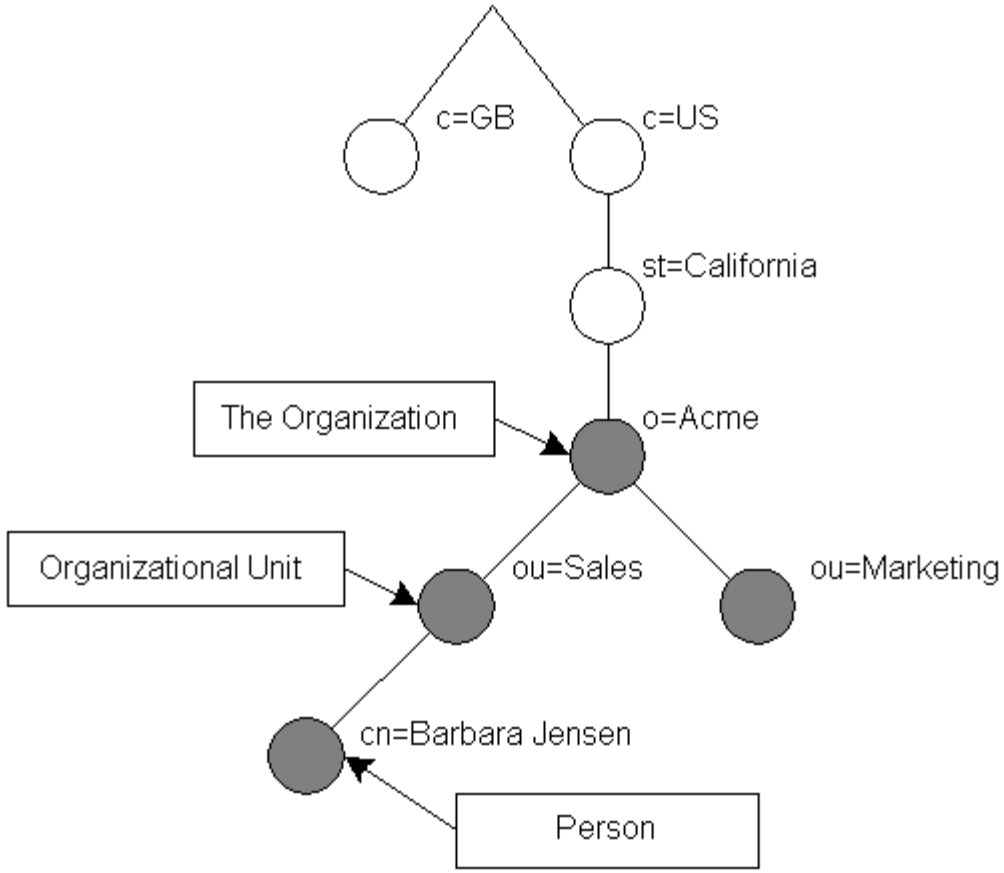
ディレクトリサービス

- ネットワークを一元管理するための情報提供
- 比較的大規模コンピュータ・ネットワークで利用
- 大量の照会あるいは検索操作
- ユーザ情報、プリンタ情報、その他サービス情報
  - eDirectory（ノベル）
  - SunONE（サン・マイクロシステムズ）
  - Open Directory（アップルコンピュータ）
  - Active Directory（マイクロソフト）

ディレクトリ情報

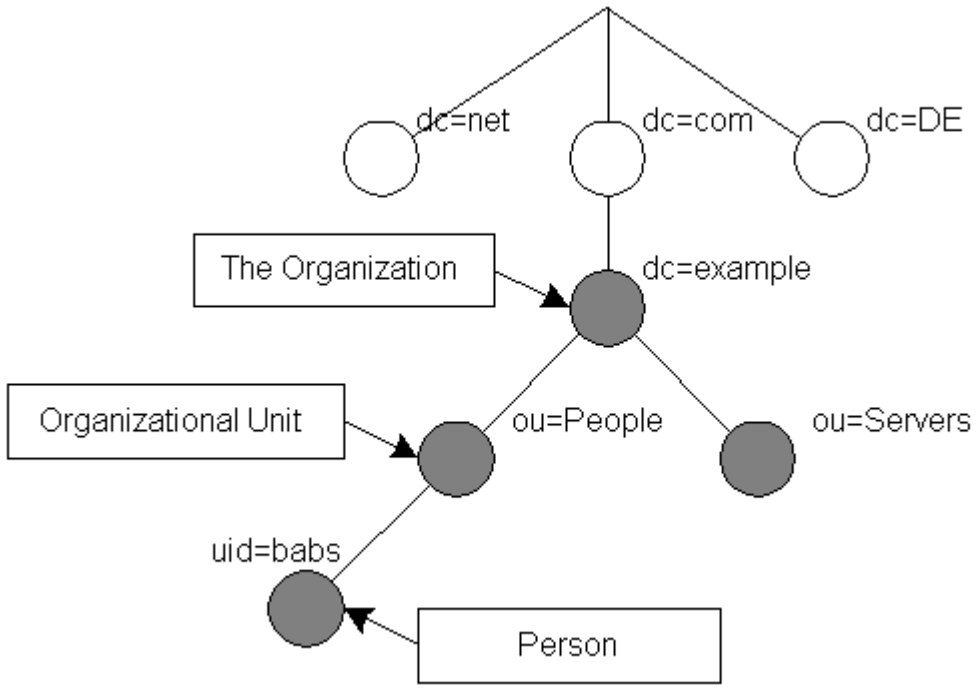
- ツリー構造
- グローバルに一意な名前のエントリを基
  - 識別名 (Distinguished Name: DN)という
  - 地域、組織、インターネットドメインなど
- エントリの属性には型と一つ以上の値
- 型には憶えやすい名前
  - 一般名(common name)は ″cn″
  - 電子メールアドレス (email address)は ″mail″

伝統的命名法の階層ツリーの例



（OpenLDAP ソフトウェア 2.3 管理者ガイドより）

ドメイン名の階層ツリーの例



（OpenLDAP ソフトウェア 2.3 管理者ガイドより）

OpenLDAP

- 初期版はミシガン大学が開発(LDAPv2)
- OpenLDAPプロジェクトで開発中(LDAPv3)
- OpenLDAP財団がコーディネート
- オープンソースライセンス
  - OpenLDAP Public License
    - (http://www.OpenLDAP.org/license.html)

OpenLDAPのプログラム

- サーバ
  - slapd
    - ディレクトリサービスのサーバ
  - slurpd
    - マスター／スレーブ複製機構のための伝播サーバ
- クライアント
  - ldapadd, ldapmodify, ldapdelete, ldapmodrdn
    - エントリ管理ツール用コマンド
  - ldapsearch, ldapcompare
    - 検索等ユーティリティ用コマンド
- 構成ファイル
  - slapd.conf

slapd.confの設定

- スキーマファイルの取り込み
  - include
    - サービス毎に定義されたスキーマが存在する
- セキュリティ
  - sasl-*, TLS*,
    - 認証、暗号化など
- データベース
  - **database**
    - **bdb**, ldbm, **sql**
- ACL(アクセス制御リスト)
  - access to ... by ... {read|write|search|compare|...}

database bdb

- 標準構成
- slapd.confの関連記述

```
database bdb
suffix   "dc=example,dc=com"
rootdn   "cn=root,dc=example,dc=com"
rootpw   secret
directory ./data
```

database sql

- ODBCマネージャ経由DBMS接続

```
database    sql
suffix  "dc=example,dc=com"
rootdn  "cn=root,dc=example,dc=com"
rootpw  secret
dbname  PostgreSQL
dbuser  ldap
dbpasswd    pass
insentry_query    "insert into ldap_entries
  (id,dn,oc_map_id,parent,keyval) values ((select max(id)+1
  from ldap_entries),?,?,?,?)"
upper_func        "upper"
strcast_func      "text"
concat_pattern    "?||?"
has_ldapinfo_dn_ru    no
```

slapd-sql

- slapd-sqlの設定概要
  - slapd-sql(unixODBC導入)
  - slapd-sql(OpenLDAP導入)
  - slapd-sql(PostgreSQL設定)
  - slapd-sql(unixODBC設定)
  - slapd-sql(OpenLDAP設定)
- slapd-sql(テスト)

slapd-sqlの設定概要

- PostgreSQL
  - createuser, createdb, pg_hba.conf, password
  - slapd-sqlバックエンドテーブルスキーマ登録
- UnixODBC
  - odbcinst.ini, odbc.ini, isql
- OpenLDAP
  - slapd.conf, ldapadd, ldapsearch

slapd-sql(unixODBC導入)

- unixODBCのインストール例

```
# wget http://www.unixodbc.org/unixODBC-2.2.x.tar.gz
# tar xvfz unixODBC-2.2.x.tar.gz
# cd unixODBC-2.2.x
# ./configure --prefix=/usr
    （設定ファイルの場所を指定する場合は、--sysconfdir=/etc 追加）
# make
# make install
```

slapd-sql(OpenLDAP導入)

- OpenLDAPのインストール例

```
# wget ftp://ftp.openldap.org/pub/OpenLDAP/openldap-
  release/openldap-2.3.x.tgz
# tar zxf openldap-2.3.x.tgz
# cd openldap-2.3.x
# ./configure --enable-spasswd ¥
    --enable-wrappers --enable-sql ¥
    --with-cyrus-sasl --with-tls
# make depend
# make
# make check
# make install
```

slapd-sql(PostgreSQL設定)

- SQLバックエンドのDB作成

  $ createuser --no-createdb --no-adduser --password ldap

  $ createdb --owner ldap pg_ldap

- テスト用スキーマ
  - openldap-2.3.x/servers/slapd/back-sql/rdbms_depend/pgsql/

  $ psql　pg_ldap < backsql_create.sql　（SQLバックエンド）

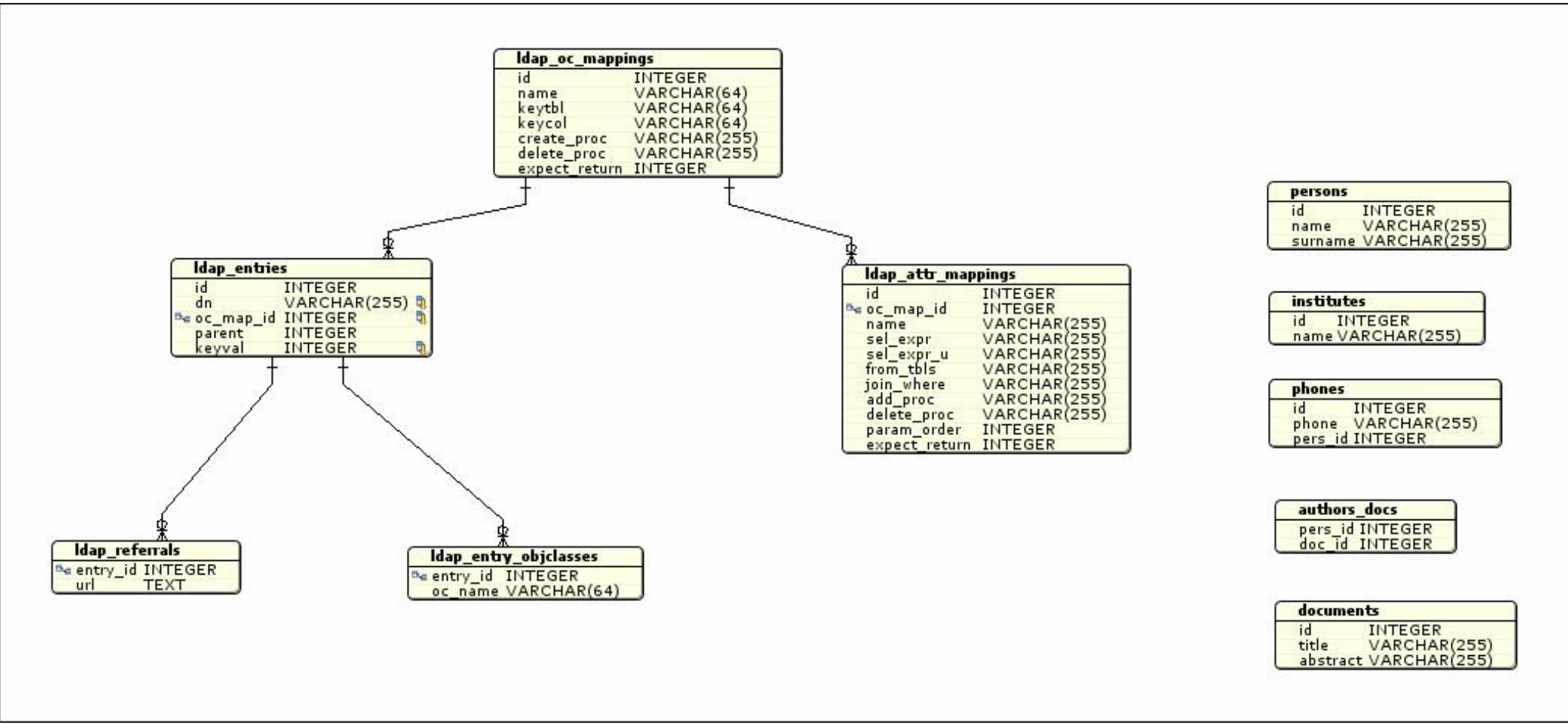
  $ psql　pg_ldap < testdb_create.sql　（DBスキーマ）

  $ psql　pg_ldap < testdb_metadata.sql（メタデータ）

  $ psql　pg_ldap < testdb_data.sql　（テストデータ）

  （参照 http://www.samse.fr/GPL/ldap_pg/HOWTO/x67.html）

slapd-sql(サンプルスキーマER図)



slapd-sql(unixODBC設定)

- odbcinst.ini
  - ODBCドライバの設定
- [.]odbc.ini
  - ODBCエントリの設定
    - Driver = ＜ODBCドライバ名＞
- isql
  - アクセステスト
    - isql ＜ODBCエントリ名＞

slapd-sql(OpenLDAP設定)

- slapd.conf

  suffix ＜基となるディレクトリ名（“dc=example,dc=com”）＞

  rootdn ＜管理者名（“cn=root,dc=example,dc=com”）＞

  rootpw ＜rootdnのパスワード＞

  dbname ＜ODBCエントリ名＞

  dbuser ＜データベースにアクセスするためのユーザ名＞

  dbpasswd ＜dbuserのパスワード＞

- デバグモードでの実行

  # slapd -d 5

slapd-sql(テスト)

- 検索テスト

  $ ldapsearch -x -b "dc=example,dc=com" "(objectClass=*)"

- エントリの作成

  $ ldapadd -x -D "cn=root,dc=example,dc=com" -w secret ¥
  -f newentry.ldif

- エントリ属性設定

  $ ldapmodify -x -D "cn=root,dc=example,dc=com" -w secret ¥
  -f setattrib.ldif

- エントリの削除

  $ ldapadd -x -D "cn=root,dc=example,dc=com" -w secret ¥
  -f delentry.ldif

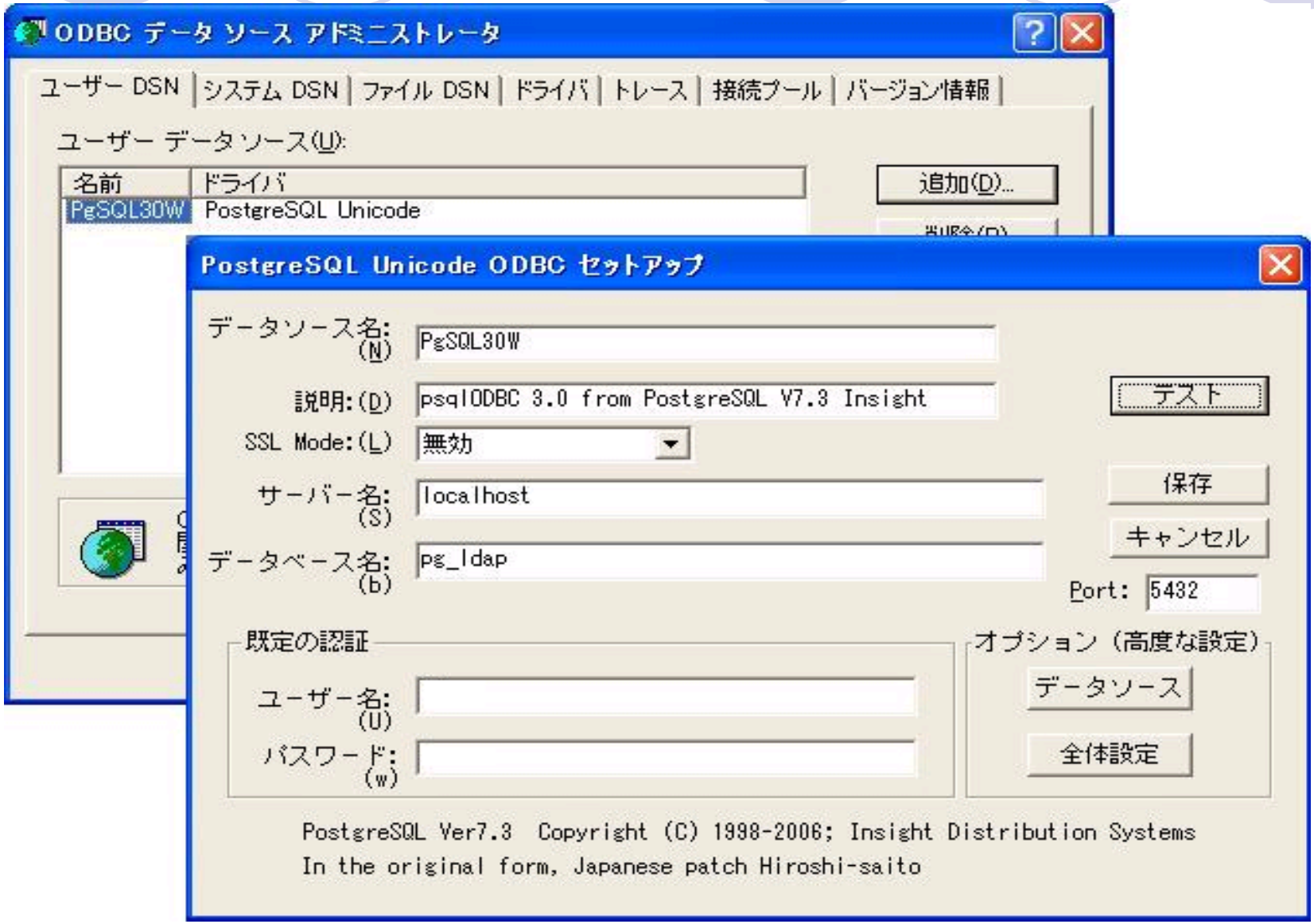
  (参照 http://www.samse.fr/GPL/ldap_pg/HOWTO/x67.html)

Windows版OpenLDAP

- Win32版のインストール

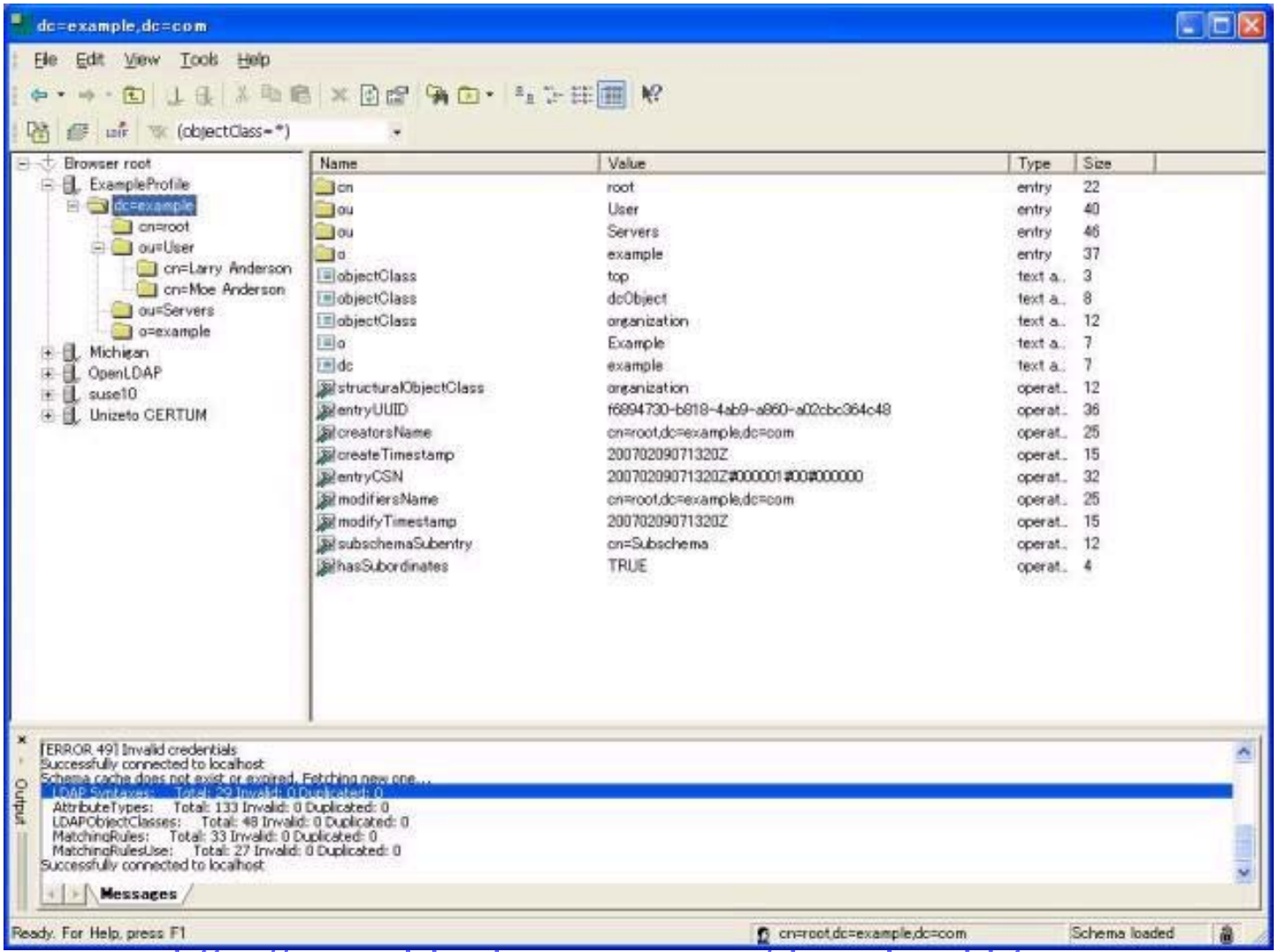
  http://download.bergmans.us/openldap/openldap-2.2.29/¥
  openldap-2.2.29-db-4.3.29-openssl-0.9.8a-win32_Setup.exe

Win32版ODBC設定



Windows版LDAP Browser

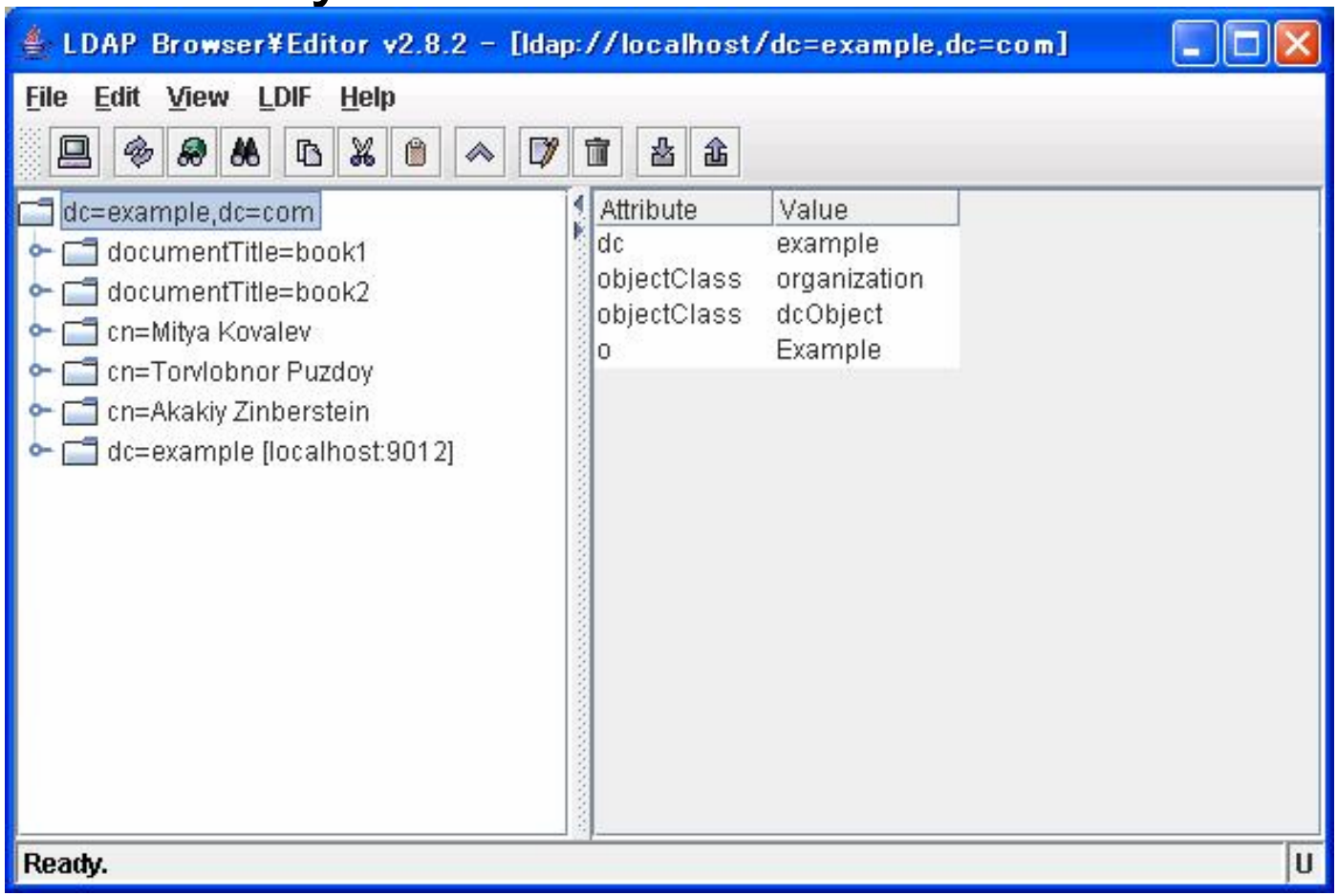
- Softera LDAP Browser



- http://www.ldapbrowser.com/download.htm

Java版LDAP Browser/Editor

- version 2.8.2 by Jarec Gawor



http://www.iit.edu/~gawojar/ldap

C# .NETプログラム

- monoでも稼動(SuSE Linux)
  - http://www.novell.com/coolsolutions/appnote/1673.html
- DirectoryEntry, DirectorySearcher

```
DirectoryEntry de = new DirectoryEntry(
      "LDAP://127.0.0.1:389/dc=example,dc=com"
      ,"cn=root,dc=example,dc=com", "secret"
      , System.DirectoryServices.AuthenticationTypes.ServerBind);
DirectorySearcher src = new DirectorySearcher("(objectclass=inetOrgPerson)");
src.SearchRoot = de;
src.SearchScope = SearchScope.Subtree;
foreach(SearchResult res in src.FindAll()){
  Response.Write(res.Properties["cn"][0] + "<BR>");
}
```

Visual Web Developper 2005 Express

- マイクロソフト無償版

  http://www.microsoft.com/japan/msdn/vstudio/express/

- ASP.NET 2.0対応

  - .NET 1.1のプロジェクトは変換が可能

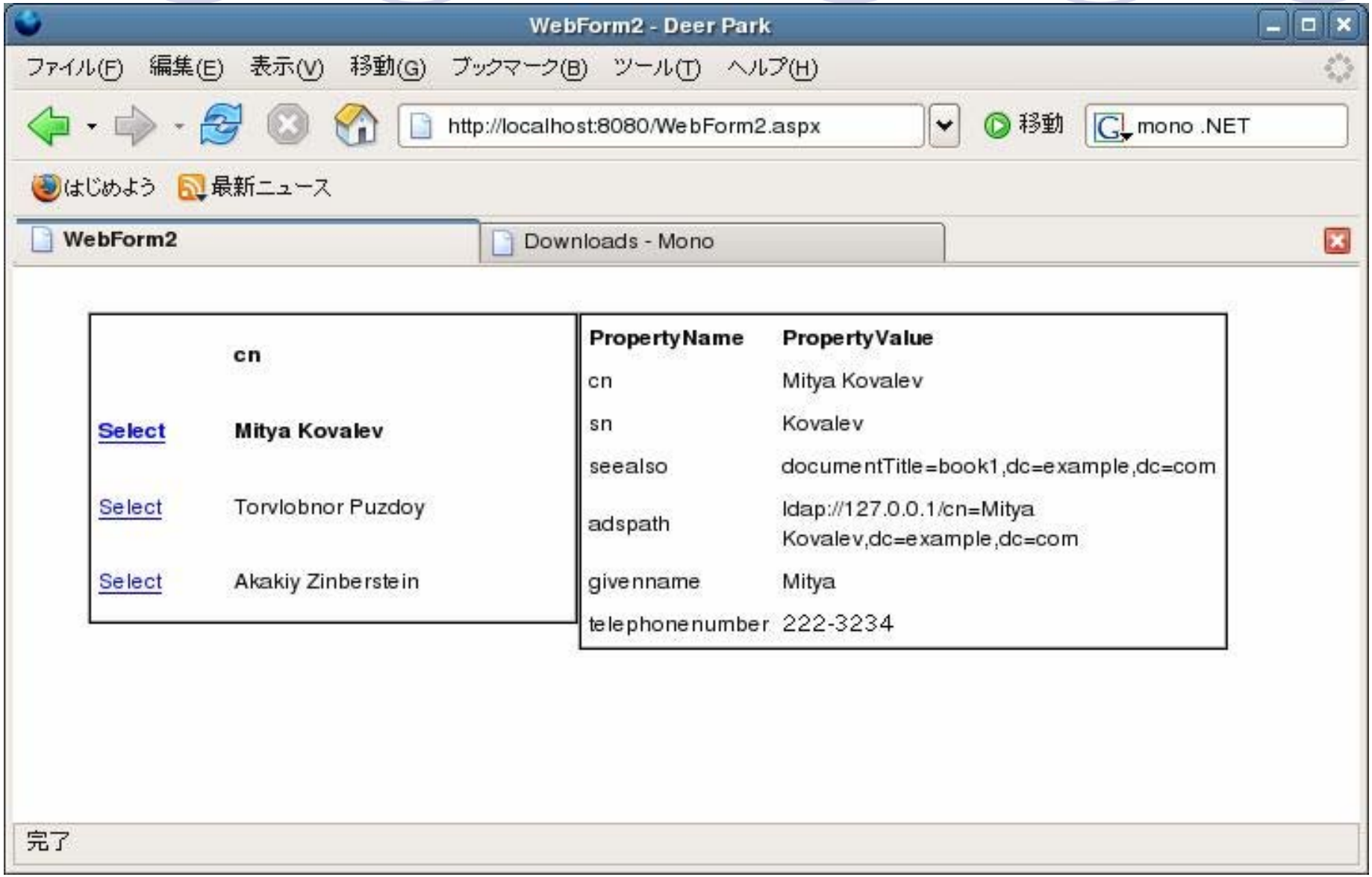
mono 1.2.3 ASP.NETサーバ

- mono-1.2.3.1(Feb/16/2007 release)
  - ASP.NET 2.0対応強化
  - Linuxバイナリインストーラパック
    - http://www.mono-project.com/Downloads

      たとえば、mono-1.2.3.1_0-installer.bin
      1. ダウンロード
      2. インストーラを実行
      3. $HOME/mono-1.2.3.1/binをPATHに追加
      4. VWD2005Expressでデバグしたプロジェクトをコピー
         （たとえば$HOME/mono/WebApp1）
      5. mono ASP.NET Webサーバを起動

```
$ xsp2 --root $HOME/mono/WebApp1
```

ASP.NET サーバ オン Linux



ありがとうございました

- アンケートのご記入をお願いします。

予告

- *PostgreSQLカンファレンス2007Japan（仮）*
  - *来たる6月5日秋葉原UDX、乞うご期待！*