入門LDAP認証（1）

― 準 備 ―

平 野　　靖

Ⅰ．本連載の目的

本連載では，LDAP（Lightweight Directory Access Protocol）に関する基礎知識を説明するとともに，各部局で情報サービスを提供している（あるいは，しようとしている）職員を主な対象とし，LDAPサーバを使うと何ができるのか，そしてどうやって使えばよいのかを説明する。おそらく個人向けの情報サービスを提供する上で，もっとも面倒な部分はユーザのID管理であろう。つまり，そのユーザが実在するのか，そしてIDとパスワードの生成と管理をどうすればよいのか，などである。そこで，情報連携基盤センターでは，全学，及び各部局で運用される情報サービスでのユーザの認証や所属などの情報を提供することを目的として，LDAPサーバ（LDAP Version 3に準拠）を運用している。ただし，このLDAPサーバに対して，ユーザ（個人または部局）が内容を追加したり，書き換えたりすることは原則として許可していない。そのため，本連載での説明は主にLDAPサーバに格納された情報の検索や抽出に関するものであり，LDAPサーバ自体のインストール方法や設定方法などについてはあまり詳しくは説明しない。

Ⅱ．LDAP

1．LDAPとは何であろうか？

LDAPとは，電子的な電話帳（ディレクトリサーバ，あるいはLDAPサーバ[1]と呼ばれる）と通信し，各種の情報を読み書きするためのプロトコルである。電話帳と言っても，名前，電話番号，住所のみを格納できるのではなく，運用目的にあわせて任意の情報を追加することができる。LDAP Version 3の仕様はRFC（Request for Comments）[2]によって定義されている（[1]－[13]）。また，それぞれのRFCがどのように関連しているかは文献［14］を参照して頂きたい。

LDAPサーバのフリーソフトとしてはOpenLDAPがとくに有名であり，ほとんど唯一のフリーのLDAPサーバであると言える。商用のものとしてはeDirectory（Novell），Internet Directory（Oracle），Domino（Lotus），Exchange Server（Microsoft），Active Directory（Microsoft）[3]，

1　厳密にはLDAP Version 3をサポートする任意のディレクトリサーバをLDAPサーバという。

2　http://www.ietf.org/rfc.html

3　Active DirectoryはLDAPを含む各種のプロトコルを理解するディレクトリサーバである。

及びiPlanet Directory Server（Sun/Netscape）[4]などが有名である。これらのLDAPサーバはクライアント側から見れば，ほとんど同じ振る舞いをする。しかし，レプリケーション（後述）や分散ディレクトリなど，LDAPサーバ間の通信においては，RFCで定義されていない部分も多く，互換性はないと考えた方がよい。そのため，複数のLDAPサーバを連携させながら運用する場合には，同じソフトを用いる方が安全である。

LDAPサーバでは，通常の電話帳と同じように，情報は頻繁には更新されないことを仮定しており，検索（コンピュータへのログイン時の認証など）は高速にできるように設計されている。しかしその反面，情報の更新や追加などの処理は遅い。そのため，頻繁に情報が更新される用途には不向きとされる。

詳しくは参考文献やWebページを参考にしてほしい。LDAPの一般的な参考書としては文献［15］［16］など，OpenLDAPやiPlanet Directory Serverに関するものは，それぞれ文献［17］［18］，文献［19］［20］などが挙げられる。その他，LDAPサーバを提供するベンダーや実際にLDAPサーバを運用している人のWebページも検索すれば多く見つかるし，メーリングリスト[5]も運営されている。

２．LDAPで何ができるのか？

LDAPサーバがどのようなものであるのかを理解してもらうために，LDAPでできることを簡単に書いておく。

認証と情報の読み込み

LDAPサーバのもっとも単純な利用方法は認証である。認証の中でももっともポピュラーな使い方としては，コンピュータの利用資格があるかどうかの問い合わせではあるが，入退館管理や入退室管理なども基本的には個々人の認証によって行える。さらに，LDAPサーバは認証以外の用途にも使える。先にも書いたがLDAPサーバには必要に応じて任意の情報を格納できる。例えば，サービスによっては，ユーザ名の漢字表記，読み仮名，あるいは所属部局名などの情報が有用であろう。LDAPサーバに格納された情報は，ldapsearchや対応する関数（C言語，Java，Perlなどから利用できる）を使うことで取り出すことができる。これに関しては次回説明する。

UNIXマシンへのログインのための認証というと，NISやNIS+が思い浮かぶ。少なくともNISは現在でも広く使われており，小規模なグループでのUNIXマシンへのログインという用途では十分であろう。しかし，ユーザを階層的に管理することができない，あるいはセキュリティ的に問題

4　このLDAPサーバはNetscapeとSunが共同で開発してきたが，現在はSunからリリースされている。呼称に関しては，Sun内部でも多少の混乱があるようで，同じバージョンでも複数の呼称が存在する。例えば，Netscape Directory Server 4.16及びiPlanet Directory Server 4.x，iPlanet Directory Server 5.0及びSun ONE Directory Server 5.0，Sun ONE Directory Server 5.1及びiPlanet Directory Server 5.1，Sun ONE Directory Server 5.2及びSun Java System Directory Server 5.2などである。ここでは，これらの総称としてiPlanet Directory Serverを用いる

5　http://www.ricoh.co.jp/src/people/nishida/ldap-jp/

があるなど，大規模なグループに対してサービスを行おうと思うと，不十分である。

アクセス制御

ACI（Access Control Information，アクセス制御情報）[6]でアクセス制御が可能である。例えば，ユーザごとにアクセスできる情報，許可するアクセスの種類やアクセスできる範囲を設定するなど，きめ細かいアクセス制御を設定できる。また，OpenLDAPではTCP Wrappersと組み合わせることによって，特定のホストからのアクセスのみを許可することができるが，特定のホストから特定のユーザのみがアクセス可能，という設定はできない。一方，iPlanet Directory Serverでは，そのような設定も可能である。

レプリカ

１台のLDAPサーバだけでは，ユーザからのアクセスを処理しきれなくなり，認証や情報の読み出しに遅延が生じる可能性がある。そこで，同じ内容を保持するLDAPサーバを複数台設置することにより，負荷を分散させることができる。これらのLDAPサーバは，通常はツリー状に接続される。そのうち１台がマスターレプリカサーバと呼ばれ，その他がコンシューマレプリカサーバと呼ばれる[7]。情報の修正や追加はすべてマスターレプリカサーバに対して行われ，変更結果はコンシューマレプリカサーバに伝播していき，LDAPサーバ群で常に同一の情報を保持する。認証や読み出しはマスターレプリカサーバでも，コンシューマレプリカサーバでも処理することができる。

セキュリティ

LDAPサーバはIDとパスワードのみではなく，いろいろな情報を格納することができる。

そのため，情報の漏洩には特別の配慮が必要である。情報漏洩の防止には，LDAPサーバ内部と，クライアントとの情報のやり取りの過程の２つを考える必要がある。

まず，LDAPサーバ内部のセキュリティ対策としては，パスワードをそのままの形では保存しない，ということが挙げられる。平文で保存することもできるが，一方向ハッシュ（SHAやSSHAなど）をかけた状態で保存すれば，たとえパスワードが漏洩しても元のパスワードを復元することは非常に困難であり，不正なアクセスを防止することに有効である。

つぎに，クライアントとの情報のやり取りに関してであるが，これにはネットワークに流れる

6　Sunの説明によれば，ACIの集合をACL（Access Control List，アクセス制御リスト）と呼ぶ。一方，文献［18］などによれば，ACIとは運用中に動的に変更でき，レプリケーション（後述）を行った際にコンシューマレプリカに自動的に伝播するもの，ACLは静的な設定しかできないもの，と説明されている。本特集では，ACIやACLを単にアクセス制御を行うための設定，という意味で用いる。なお，アクセス制御に関してはIETFのLDAP Extension Working Groupで検討されているようであるが，現時点ではLDAP Version ３に対するアクセス制限の標準仕様は決定されていないようである。

7　運用形態によっては異なる形態で接続されることもある。本文で示した例は最も簡単な形態である。

情報を暗号化する必要がある。この方法には２種類あり，パスワードのみを暗号化して送る方法と，情報のすべてを暗号化して送る方法である。前者はSASL（[21] [22]）であり，後者はSSL/StartTLSと呼ばれる。SASLはLDAPサーバが対応していれば比較的簡単に使用できるが，暗号化されるのはパスワードのみなので，注意が必要である。SSL/StartTLSは通信のすべてが暗号化されるので，安全性が高い。しかし，独自にCA（Certificate Authority，認証局）を構築するか，サーバ証明書（SSL証明書）[8]を購入してLDAPサーバにインストールする必要がある。この他に，LDAPサーバソフトの機能は使わずにSSH Port Forwordingを使ってすべての通信を暗号化する方法もある。この場合にはLDAPサーバが稼動しているマシンにログインできるようにアカウントを用意する。SASL，及びSSL/StartTLSに関しては第３回で紹介する予定である。

３．LDAPに格納できる情報とその構造

属性型と属性値

LDAPサーバに格納される情報は属性型と属性値の組で表現される。属性型は情報の種類をあらわし，属性値は情報そのものをあらわす。広く使われる属性型はLDAPサーバで用意されているが，必要に応じてLDAPサーバの管理者が追加することも可能である[9]。また，属性型によっては，複数の属性値を持つこともできる。代表的な属性型を表１に示す。

表１　代表的な属性型

属性型	説明
dn（distinguished name）	LDAPサーバ中で一意な名前
o（organizationName）	組織の名前
ou（organizationUnitName）	部署などの名前
cn（commonName）	一般名。氏名，社員番号などをあらわす
sn（surname）	姓
givenName	名
mail（rfc822Mailbox）	メールアドレス
userPassword	パスワード

エントリ

人物や組織は属性型と属性値の組の集合で表現され，この集合はエントリと呼ばれる。エントリはdn（識別名，Distinguished Name）と呼ばれる名前で区別される。

8　サーバ証明書の発行においては，VeriSign，Entrust，及びBaltimoreなどが大手であり，これらがルートCAとなっているが，他の企業からも同等のものを購入することができる。

9　iPlanet Directory ServerやNovell eDirectoryなどではテキストファイルに追加すべき属性型の定義を記述してコマンドあるいはGUIで読み込ませる。OpenLDAPでは属性型の定義をファイルに記述し，起動時にそのファイルを読み込むようにLDAPサーバの設定ファイル（環境によって異なる可能性があるが，例えば，/usr/local/etc/openldap/slapd.conf）に記述しておく必要がある。なお，製品によって属性型の定義の方法が異なるので注意が必要である。

DIT（Directory Information Tree）

LDAPサーバではDITと呼ばれるツリーで情報を保存する。DITの各ノード（ブランチ・ノード，及びリーフ・ノード）がエントリに対応する。ブランチ・ノードにあるエントリは組織やグループなどをあらわすことが多いが，人物をあらわすエントリがブランチ・ノードにあってもよい。DITの例を図１に示す。図１のように，実際の組織の構成と同じようにDITを構成することにより，直感的に分かりやすいものになる。

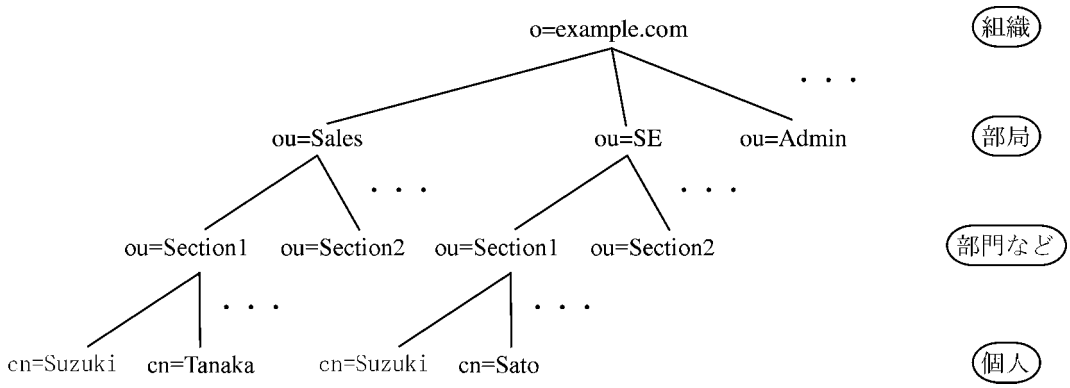


図１　DITの例

ldif（LDAP Data Interchange Format）ファイル

ldifファイルとは，LDAPサーバに新しいエントリや属性型を登録したり，ACIを設定したりするために用いるテキストファイルであり，UTF-８という文字コードで記述する必要がある[10]。これにより，アルファベットのみでなく，漢字，ひらがなやカタカナなども扱うことが可能になる。表２に人物に対応したエントリのldifファイルの例を示す。表２から分かるように，エントリは“：”の左側の属性型と右側の属性値の集合で記述される。１行目のdnはエントリの名前をあらわしている。dnはDIT内で一意の名前であり，dnを右端から読んでいくと，LDAP-TESTという組織の下のEdoという部局に所属しているe00001というcn（14行目）を持っているエントリであることが分かる。２行目から８行目はこのエントリに割り当てられたオブジェクトクラスを示しており，オブジェクトクラスはエントリが格納できる属性型をあらわしている。例えば，posixAccountというオブジェクトクラスは

```
objectclass ( 1.3.6.1.1.1.2.0 NAME 'posixAccount'
  SUP top AUXILIARY DESC 'Abstraction of an account with POSIX attributes'
  MUST ( cn $ uid $ uidNumber $ gidNumber $ homeDirectory )
  MAY ( userPassword $ loginShell $ gecos $ description ) )
```

10　Windows上でUTF-8を扱うことができるエディタにはxyzzy，サクラエディタ，TepaEditorなどがある。また，MeadowでもMule-UCSを併用することによりUTF-8を使用できるようになる。

と定義されている。posixAccountオブジェクトクラスが設定されたエントリではcnやuidNumberなどの属性型を持たなくてはならないし（MUST），userPasswordやloginShellなどの属性型を持ってもよい（MAY）。

iPlanet Directory ServerなどではGUIでエントリを追加・削除・変更ができるが，ldifファイルを作って操作する方が一般的であるし，操作記録が残ってよい。また，大量のエントリを簡便に操作するためには，自動的にldifファイルを生成するプログラムを作成し，生成されたldifファイルをGUIから読み込むという方法をとることができる。

なお，既存のLDAPサーバから情報をldifファイルに書き出すことも可能で，バックアップを取ったり，コンシューマレプリカサーバの初期化に使ったりする。

iPlanet Directory ServerやeDirectoryと，OpenLDAPでは，受け入れられるldifファイルが多少異なる。もちろん，RFCで決められたフォーマットに厳密にしたがったldifファイルであれば，どのLDAPサーバでも受け入れられるはずである。どちらかというと，iPlanet Directory ServerやeDirectoryはOpenLDAPよりも柔軟にldifファイルを解釈するようである。

表２　ldifファイルの例（抜粋）

１行目	dn: cn=e00001,ou=Edo,o=LDAP-TEST
２行目	objectClass: inetOrgPerson
３行目	objectClass: organizationalPerson
４行目	objectClass: person
５行目	objectClass: pubLdapProperties
６行目	objectClass: top
７行目	objectClass: posixAccount
８行目	objectClass: mailRecipient
９行目	groupMembership: tycoon
10行目	loginShell: /bin/tcsh
11行目	uidNumber: 04001
12行目	gidNumber: 0004
13行目	userPassword: pe00001
14行目	cn: e00001
15行目	sn: 徳川 家康
16行目	fullName: 徳川 家康
17行目	fullNameKana: トクガワ イエヤス
18行目	fullNameRoman: Tokugawa Ieyasu
19行目	idNo: e00001
20行目	mailhost: example.com
21行目	mail: e00001@example.com
22行目	working: 将軍（太政大臣）
23行目	workingCode: 01
24行目	department: 江戸幕府
25行目	departmentCode: 04

アクセスの種類

各エントリに対して，どのようなアクセスを許可するかを設定できる。ただし，前述のように，アクセス制御に関する標準仕様はないため，ベンダーによっては種類や意味が異なる可能性がある。iPlanet Directory Severで設定できるアクセスの種類は下記のとおりである。

write（書き込み） 属性値の追加，変更

read（読み取り） 属性値の読み取り

search（検索） 属性値の検索

compare（比較） 属性値の比較

selfwrite（自己書き込み） 自分自身のエントリに対する属性値の追加，変更

delete（削除） エントリの削除

add（追加） 新規エントリの追加

proxy（プロキシ） 他のエントリの権限でのアクセス

一方，OpenLDAPでは下記のアクセスが規定されている。

none アクセス不可

auth 認証

compare auth + 属性値の比較

search compare + 属性値の検索

read search + 属性値の読み取り

write read + 属性値の追加，変更

selfwrite 自分自身のエントリに対する属性値の追加，変更

Ⅲ．情報連携基盤センターのLDAPサーバ

情報連携基盤センターで運用しているLDAPサーバには，事務局総務企画部人事労務課，財務部情報企画課，及び学務部との協力体制のもと，名古屋大学の全職員（教職員，事務職員，及び技術職員），全非常勤職員（非常勤講師や研究員も含む），及び全学生のID（以下，全学IDと呼ぶ）とパスワードなどが格納されている。全学IDとパスワードのペアがあれば，例えばコンピュータの使用権限があるかどうかの問い合わせに答えることができる。実際に情報メディア教育センターの教育用クライアントシステムやWebCTのユーザ認証に使われている。LDAPサーバはさらなる可能性を持っている。つまり，単にIDとパスワードの組のみではなく，名前，所属部局や職名などのユーザに付随する情報もIDと対応付けて格納することができる。これによって，例えば，認証を受けたユーザの所属部局名をLDAPサーバから受け取って，自動的に他のアプリケーションに渡すこともできる。

もし，全学IDが広く使われるようになれば，サービスを提供する主体が異なっても，認証部分は共通化できる（図２）[11]。したがって，誰が提供するサービスであっても，共通のIDとパスワー

11 この図でいうデータベースは，所属部局や職名などを格納するものであり，部局独自の情報を格納するデータベースを別途用意する必要があるかもしれない。

ドを用いることでサービスを受けることができる。これによって，全学レベルでは認証システムの一元化によるTCO（Total Cost of Ownership）の低減，ユーザレベルではどのシステムでも同じIDとパスワードの組でログインができる，という利点がある。

このLDAPサーバは，情報連携基盤センターに申請することにより，学部やセンターなどの学内部局が情報サービス提供者として利用することができる。もちろん，名前や所属部局などの個人情報が漏洩することは大きな問題であるため，暗号化されていないパスワードが情報連携基盤センター外のネットワークに流れないような措置，通信路の暗号化，及びアクセス制御などを行うとともに，LDAPサーバを利用する部局においては，責任の所在を明確化して頂いている。表３に情報連携基盤センターが提供する属性型の一覧を示す。また，このLDAPサーバを使って認証を行っているサービスの一覧と，全学IDの詳細を知るには，下記のURLにアクセスしてほしい。

http://www2.itc.nagoya-u.ac.jp/center/id.htm

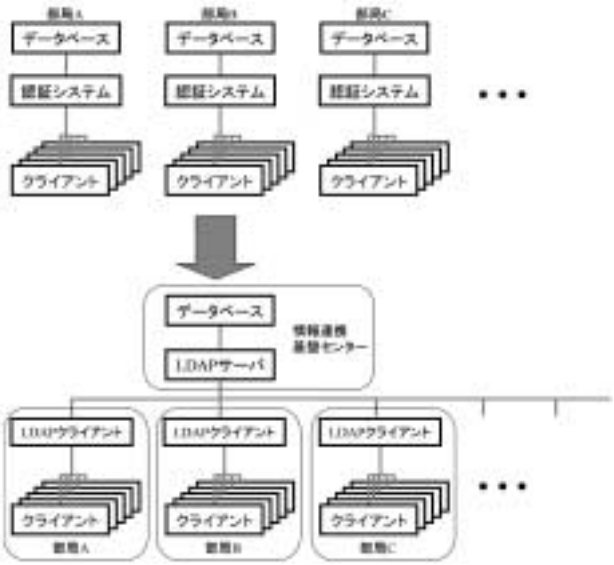


図２　認証システムの一元化

表３　情報連携基盤センターで運用するLDAPサーバで提供している情報（抜粋）

提供される情報	備考
識別名	全学ID
暗号化されたパスワード	compareのみ可能
姓名（漢字）	
姓名（カタカナ）	
姓名（ローマ字）	
職員番号，あるいは学籍番号	
学部・研究科名（漢字）	学生のみ格納
学年	学生のみ格納
学部生・大学院生（前期課程）・大学院生（後期課程）の別	学生のみ格納
所属部局名（漢字）	教員・事務職員・技術職員のみ格納
掛・講座名（漢字）	教員・事務職員・技術職員のみ格納
職種（漢字）	教員・事務職員・技術職員のみ格納

Ⅳ．お試しLDAPサーバ

LDAPサーバがどのようなものであるのかを知るためには，実際に使ってみるのが一番の近道である。OpenLDAPのもとになったLDAPサーバを開発していたミシガン大学や，Netscape社，OpenLDAPの開発者たちなどが誰でもアクセスすることができるLDAPサーバを運用していたが，現在のところ，下記のような状態である。なお，いずれもポート番号は389である。

ldap.itd.umich.edu・・・・・・・・・・・・・ 接続できるが，“ no such objects ”といわれる

ldap.netscape.com・・・・・・・・・・・・・ 接続できない

www.openldap.com ・・・・・・・・・・・ 接続できるが，あまり中身がない

そこで，情報連携基盤センターではダミーデータを格納したお試しLDAPサーバを構築した。いずれも，IPアドレスやホスト名でのアクセス制御は行っていないので，自由に使ってほしい。お試しサーバのホスト名はpub-ldap.itc.nagoya-u.ac.jpであり，ポート番号は1024である。

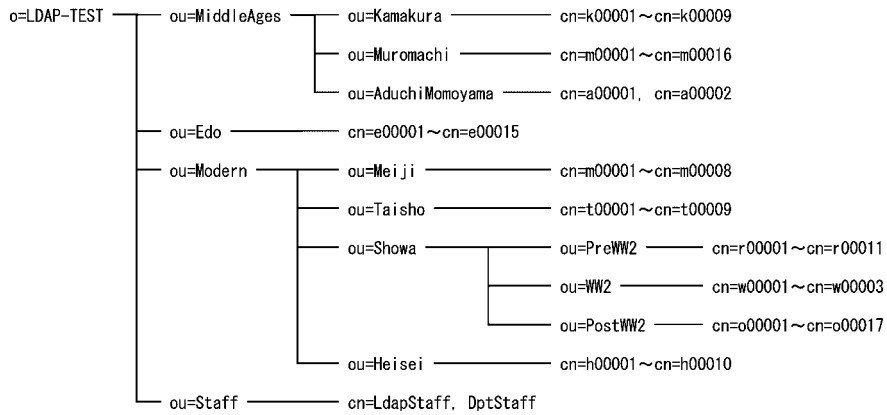


図３　お試しサーバのDIT

このお試しサーバには，鎌倉時代以降の歴代の将軍や首相経験者が各時代ごとに格納されている。なお，複数回にわたって首相を経験した人もいるが，そのような場合でも１つのエントリしか作成していない。また，首相の所属は最初の就任時のものである。安土桃山時代に関しては全国的なリーダーが不明確であるので，織田信長と豊臣秀吉のみを格納した[12]。

図３にお試しサーバに格納されている情報のDITを示す。この図は紙面の都合により，図１とは異なる書き方をした。お試しサーバのDITはo=LDAP-TESTをルート（根）とし，その直下に４つのouがある。そのうち１つは管理者用のouであり，その他の３つは一般ユーザ用のouである。表２のようなldifファイルによって100人分のユーザのエントリと２つの管理者用エントリが格納されている。図３から分かるように，個々人を示すエントリ[13]は，DITのルートから数えて同じレ

12　筆者は日本史の専門家ではないし，多少の間違いがあっても，本文の目的には影響しないのでご容赦頂きたい。

13　図３ではcnで始まり，DITの“ 葉 ”に相当するエントリ。

ベルにある必要はない。また，m00001というcnを持つ人物がou=Muromachi,ou=MiddleAges,o=LDAP-TESTとou=Meiji,ou=Modern,o=LDAPTESTの下にいるが，問題はない。これらはcnのみを見れば同一であるが，dnは

dn: cn=m00001,ou=Muromachi,ou=MiddleAges,o=LDAP-TESTと，

dn: cn=m00001,ou=Meiji,ou=Modern,o=LDAP-TEST

のように異なるため，区別することができる。

このサーバで提供される属性型の一部を表４に示す。なお，一般ユーザ用エントリのuserPasswordは，cnの先頭にpをつけたものにしてある。例えば，dn: cn=m00001,ou=Meiji,ou=Modern,o=LDAP-TESTのuserPasswordはpm00001に設定してある。また，管理者用エントリのdn: cn=LdapStaff,ou=Staff,o=LDAP-TESTとdn: cn=DptStaff,ou=Staff,o=LDAP-TESTのuserPasswordは，それぞれps00001とps00002である。

表４　お試しサーバで提供している属性型

属性型名	説明
dn	識別名
userPassword	SSHAで暗号化されたパスワード
cn	一般名
fullName	姓名（漢字）
fullNameKana	姓名（カタカナ）
fullNameRoman	姓名（ローマ字）
idNo	シリアル番号
mailHost	メールサーバ
mail	電子メールアドレス
working	職種（漢字）
workingCode	職種コード
department	所属部局名（漢字）
departmentCode	所属部局コード

前述のように，LDAPサーバではきめ細かいアクセス制御を行うことができる。匿名アクセス（anonymous access）ではuserPasswordに対してはcompareのみ，その他の属性型に対してはreadとsearchが可能であるように設定してある。また，管理者用エントリであるdn:cn=LdapStaff,ou=Staff,o=LDAP-TESTからのアクセスではo=LDAP-TEST全体に対してすべての属性値のread, search, compareが可能であり，もう１つの管理者用エントリであるdn: cn=DptStaff,ou=Staff,o=LDAP-TESTからのアクセスではou=Edo,o=LDAP-TESTだけは暗号化されたuserPasswordも含めてすべての属性型のread, search, compareが可能，その他のou以下のエントリに対しては匿名アクセスと同等の権限を持つ。

なお，お試しサーバは読み出し専用に設定してあるので，例え一般ユーザのエントリでアクセスしても当該ユーザ自身の属性値を変更することはできない。

次回以降，実際にどうすれば利用できるのかを，お試しLDAPサーバを例にとってコードを示しながら説明する。

表５　主なGUI版LDAPクライアント

名称	URL	備考
LDAP Browser/Editor version 2.8.1	http://www.iit.edu/~gawojar/ldap/	Java
LDAP Administrator 3.0.1	http://www.ldapadministrator.com	Win（商用）
LDAP Browser 2.6 for Windows NT/2000/XP	http://www.ldapadministrator.com	Win（フリー）
JXplorer	http://pegacat.com/jxplorer/	Win
LDAP Browser Editor	http://www.openchannelfoundation.org/projects/LDAP Browser Editor/	Win
GQ 0.6.0	http://biot.com/gq	GTK

Ⅴ．GUIのLDAPクライアント

Windows，Macintosh，あるいはX Window System上で使えるLDAPクライアントがいくつか公開されている。Internet ExplorerやNetscapeのアドレス帳などもLDAPクライアントであるが，ここで紹介するものはエントリに格納されている情報をそのまま見ることができるものであり，なかには編集できるものもある。表５に主なGUI版のLDAPクライアントを紹介する。表中の備考の意味は下記のとおりである。

Java　Javaで書かれているのでJavaが動作する環境であればOSを問わない

Win　Windowsでのみ動作する

GTK　GTKベースでありX Window Systemで動作する
（もしかしたら，GTK+ for Windows（http://www.gimp.org/~tml/gimp/win32/downloads.html）やcygwin（http://www.cygwin.com/）を駆使すれば，Windowsでも動作するかもしれない）

以下，Javaベースのソフトである LDAP Browser/Editor version 2.8.1を例にとって，お試しサーバにアクセスするための設定方法を見ていく。このソフトを動作させるには，Java Runtime Environment[14]が必要である。まず，http://www.iit.edu/~gawojar/ldap/download.htmlからBrowser281.zipあるいはBrowser281.tar.gzをダウンロードし，適当な場所に展開する。作成されたディレクトリ（フォルダ）の中にbrowser.jarというファイルがあるので，これを実行する。「Connect」という名前のウィンドウが出てきたら“New”ボタンを押す。もし出てこなかったら，FileタブからConnectを選び（図４（a)），出てきたウィンドウで“New”ボタンを押す。さらに，あらわれるウィンドウのHost，Port及びBase DNには，それぞれ“pub-ldap.itc.nagoyau.ac.jp”，“1024”及び“o=LDAP-TEST”を入力し，Versionは“３”を選ぶ。もし，管理者権限でアクセスする場合にはUser InfoのUser DNに“cn=LdapStaff, ou=Staff, o=LDAP-TEST”あるいは“cn=DptStaff, ou=Staff, o=LDAP-TEST”を，Passwordに“ps00001”あるいは“ps00002”を入力する（図４（b))。匿名アクセスの場合には，User DNやPasswordを入力する代わりに

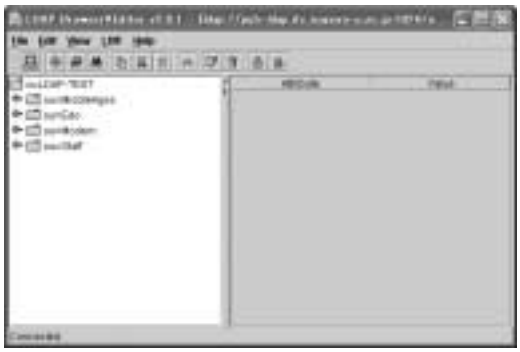
14　http://java.com/ja/download/manual.jsp

Anonymous bindにチェックを入れる。設定が終了したら“ Save ”ボタンを押すとnewという項目（Session）ができるので，必要であれば“ Rename ”ボタンを押して名前を変更する。最後に右下の“ Connect ”ボタンを押すと（図４（c)），設定が間違っていなければpub-ldap.itc.nagoya-u.ac.jpに接続できるはずである（図４（d)）。この図でo=LDAP-TESTの直下のouが年代順に並んでいるが，状況によってはアルファベット順に表示される場合もある。

（a）“ File ”から“ Connect ”を選択

（b）ホスト名やポート番号を入力

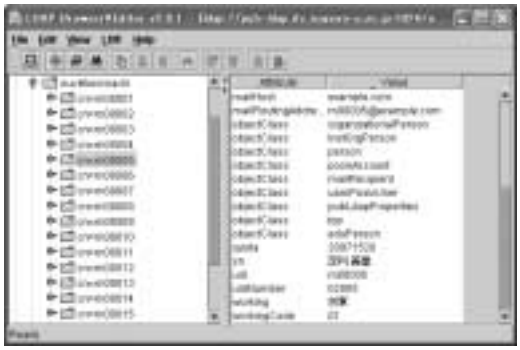
（c）Session名を変更してConnect



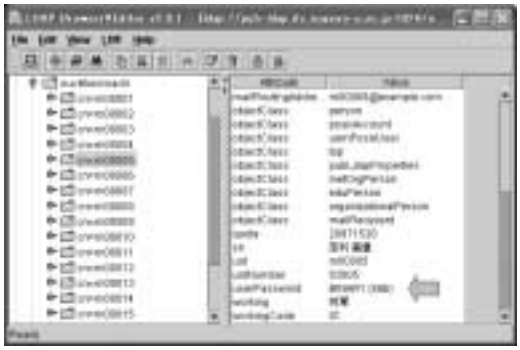
（d）接続成功

図４　LDAP Browser/Editor version 2.8.1の設定方法

ブランチ・ノードに存在するエントリを順にリーフ・ノードまでたどっていくと，そこが人物をあらわすエントリである（図５（a）（b)）。図５（a）は匿名アクセス，同図（b）はcn=LdapStaffによるアクセスの結果である。前節で述べたように，匿名アクセスではuserPassword属性を読み取ることはできないが，cn=LdapStaffによるアクセスでは読み取れることが分かる（図５（b）の矢印の行)。cn=LdapStaffによるアクセスではuserPassword属性をダブルクリックすることにより，さらに詳しい情報（userPassword属性の場合には，暗号化されたパスワード）を表示させることができる（図５（c)）。もし，Writeの権限も持っていれば，属性値を変更することもできる。



（a）匿名アクセス



（b）cn=LdapStaffによるアクセス

（c）userPassword属性の詳細

図５　権限の有無による得られる情報の違い

Ⅵ．むすび

今回はLDAPの概要を説明した。LDAPというプロトコルは便利な反面，かなり複雑であり理解するのが難しい。なるべく分かりやすいように説明したつもりであるが，説明が足りない部分もあるかもしれない。疑問点があれば，ぜひ質問して頂きたい。

次回は実際にJavaやC言語，Perlなどによるプログラムを示し，実際の部局における情報サービスではどのようにしてLDAPサーバにアクセスすればよいのかを説明する。

参考文献

［１］Wahl, M., Howes, T., and S. Kille : “ Lightweight Directory Access Protocol (v3) ”, RFC 2251, December 1997

［２］http://www.ipa.go.jp/security/rfc/RFC2251EN.html

［３］http://www.ipa.go.jp/security/rfc/RFC2251JA.htm（文献［２］の和訳）

［４］Wahl, M., Coulbeck, A., Howes, T. and S. Kille : “ Lightweight Directory Access Protocol (v3) : Attribute Syntax Definitions ”, RFC 2252, December 1997

［５］http://www.ipa.go.jp/security/rfc/RFC2252EN.html

［６］http://www.ipa.go.jp/security/rfc/RFC2252JA.html（文献［５］の和訳）

［７］Wahl, M., Kille, S., and T. Howes : “ Lightweight Directory Access Protocol (v3) : UTF-8 String Representation of Distinguished Names ”, RFC 2253, December 1997

［８］http://www.ipa.go.jp/security/rfc/RFC2253EN.html

［９］http://www.ipa.go.jp/security/rfc/RFC2253JA.html（文献［８］の和訳）

［10］http://www.ipa.go.jp/security/rfc/RFC2254EN.html
［11］http://www.ipa.go.jp/security/rfc/RFC2254JA.html（文献［10］の和訳）
［12］http://www.ipa.go.jp/security/rfc/RFC2255EN.html
［13］http://www.ipa.go.jp/security/rfc/RFC2255JA.html（文献［12］の和訳）
［14］http://www.ipa.go.jp/security/rfc/RFC3377EN.html
［15］Gerald Carter：“LDAP System Administration”, O’Reilly & Associates.
［16］Gerald Carter：“LDAP －設定・管理・プログラミング－”，でびあんぐる監訳，オーム社，東京，2003（文献［15］の和訳）
［17］http://www.openldap.org/
［18］稲地稔:“OpenLDAP入門－オープンソースではじめるディレクトリサービス－”，技術評論社，東京，2003
［19］http://docs.sun.com/db/prod/s1dirsrv?l=ja#hic
［20］トム・バイアラスキー，マイケル・ヘインズ:“SolarisによるLDAP実践ガイド”，増月孝信，丹治宏彰，大森明央，矢吹大輔訳，ピアソン・エデュケーション，東京，2002
［21］http://www.ipa.go.jp/security/rfc/RFC2222EN.html
［22］http://www.ipa.go.jp/security/rfc/RFC2222JA.html（文献［21］の和訳）

（ひらの　やすし：名古屋大学情報連携基盤センター大規模計算支援環境研究部門）