OpenLDAP サーバの設定・管理技術の習得について

藤原冨未治、中務孝広、野崎公隆、佐々木康俊、鬼頭良彦、若松　進
工学研究科・工学部 技術部 情報通信技術系

はじめに

サーバ管理者にとって、ネットワークを経由した情報管理は必要な技術の１つである。名古屋大学においても「名古屋大学ＩＤ」管理に LDAP サーバが利用されており、既存の LDAP サーバを利用する場合でも、サーバの構築方法、管理データの構築とその管理方法、サーバの運用方法、LDAP サーバの応用例等の一連の知識を習得することには意義がある。

１．目的

現在、情報管理技術の１つとして「ネットワークを経由した情報管理」が重要視されており、この管理技術を習得することが必要となってきた。また、サーバ毎で異なっている「ユーザ認証情報」を一元管理することが求められている。そこで、分散管理されている様々な情報を統合する解決策の一つとして、LDAP を利用した手法の確立を検討することにした。

なお、本研修を実施するに当たり、

(1) LDAP によるデータ管理技術およびデータ通信技術を習得すること、

(2) LDAP サーバの管理および LDAP を利用したアプリケーションの作成ができるようにすること

ということを目標とした。

２．LDAP とは

LDAP(Lightweight Directory Access Protocol)は、TCP/IP 上の分散された環境上で、ディレクトリサービスを提供するインターネット標準のプロトコルである。LDAP で扱うことのできる情報には様々なものがあるが、これらの情報を一元管理して保存し、検索しやすくまとめたものをディレクトリサービスと呼んでいる。そして、OpenLDAP は OpenLDAP Foundation が運営する OpenLDAP Project によって開発されている代表的な LDAP サーバソフトウェアである。

OpenLDAP には、

(1) 認証情報、住所、メールアドレスなどを扱うデータベースと同様なサービスと、検索機能をもつ、

(2) 様々なアプリケーションに対応した機能がある、

(3) 格納するデータの形式を自由に定義・拡張できる、

(4) LDAP サーバにアクセスできるクライアントを制限したりデータごとにアクセス権を設定したりすることができる、

(5) 通信を暗号化することも可能である

という特徴がある。

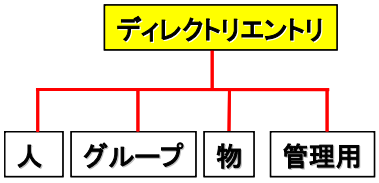

図１．DIT の概念図

次に、LDAP サーバでは取扱うデータとして DIT(Directory Information Tree)と呼ばれる階層構造で管理(図１．参照)されており、属性(データの値を保存するための規則)は「属性名」と「属性値」で構成される。そして、それぞれの属性には、どんな値を格納するのかを予め決めておくこと、

ディレクトリエントリには、属性を組み合わせたテンプレートである「オブジェクトクラス」が必要となる。

クライアントから Web サーバにアクセスした後、LDAP 認証を経由してから目的ページを表示するステップは以下の通りである（図２．参照)。

(1) クライアントから、目的の Web ページへのアクセス要求を出す。
(2) ディスプレイには ID とパスワードを入力するウィンドウが表示される。
(3) キーボードから、正しく ID とパスワードを入力して送信する。
(4) Web(WWW)サーバは、LDAP サーバに ID とパスワードを問い合わせる。
(5) LDAP サーバは、ID とパスワードを検索して、正しいことを Web(WWW)サーバに回答する。
(6) Web(WWW)サーバは、クライアントに要求されたコンテンツ(Web ページ)をクライアントに送る。
(7) その結果、クライアントのディスプレイ上に目的の Web ページが表示される。

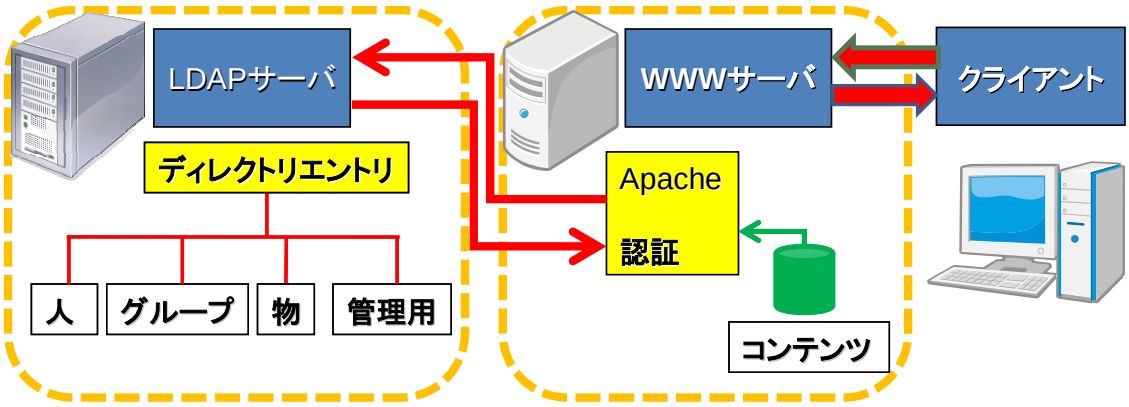

図２．テストモデルにおける LDAP 認証例

３．各種サーバの設定

３－１．サーバ設定

本研修を行うにあたり、情報通信技術系保有のマシンを利用し、研修予算で購入した HDD 上に各種サーバを構築した。また、サーバのスペック、およびインストールしたソフトウェアについては、表１．に示す。

３－２．LDAP サーバの設定

OpenLDAP サーバ自体は、apt-get コマンドを用いて VineLinux 用のパッケージをインストールした。その後、LDAP サーバ運用のための設定を行った。

次に、本研修で使用したディレクトリ階層構造は、ディレクトリエントリとしてサーバのホスト名である joho09.etec.engg を使用し、その下にグループを、このグループの下にユーザ名を置くという構造として設定した(図３．参

表１．構築サーバの概要

(1) スペック
　CPU：Pentium4 3GHz、メモリ：1Gbyte
(2) OS：VineLinux-4.2
(3) LDAP：OpenLDAP(2.3.27-2.5v14)
　　OpenLDAP-Server(2.3.27-2.5v14)
(4) DB：BerkeleyDB(4.2.52-6v1)
(5) 管理ソフト：phpLDAPadmin(1.1.0.5)

照)。

また、LDAP サーバ起動時に利用される設定ファイルと、設定の概略は以下の通りである。

(1) /etc/ldap.conf

LDAP サーバのホスト IP、ポート番号、検索方法等を指定する。

(2) /etc/openldap/slapd.conf

ドメインの識別名、使用するスキーマのインクルード、接続パスワード、構築ディレクトリ場所などを設定する。また、LDAP サーバへのアクセス制限にも用いる。

(3) /etc/syslog.conf

トラブル等の情報収集用のログファイルとして利用する。

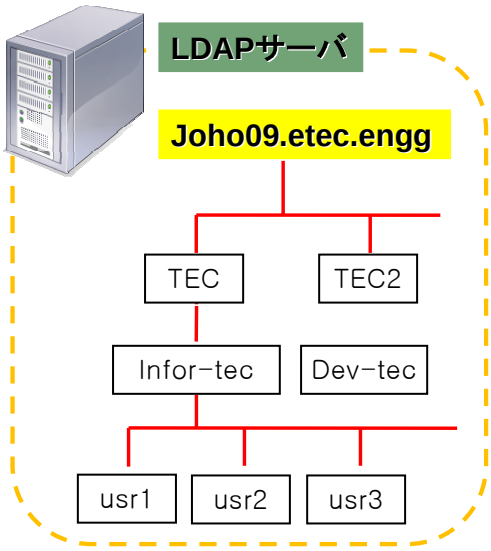

図３．研修で設定した DIT

４．各種動作テスト

４－１．LDAP データの管理

LDAP サーバで取り扱かうデータは、LDIF(LDAP Data Interchange Format)という形式で表記され(図４．参照)、これらのデータ管理には様々なコマンドを利用する。LDAP サーバで利用できるコマンドは多く用意されているが、主に利用するコマンドとして次の４つが挙げられる。コマンド名とその役割は、

dn:ドメインのディレクトリサーバ識別名
cn: 属性名
objectClass: オブジェクトクラスの定義
userPassword: 属性値の設定
loginShell: /bin/bash
homeDirectory: /home/test

図４．LDIF ファイルの概要

(1) ldapadd：LDAP サーバにデータを登録するためのコマンド、

(2) ldapdelete：LDAP サーバからデータを削除するためのコマンド、

(3) ldapmodify：LDAP サーバに登録したデータを編集するためのコマンド、

(4) ldapsearch：LDAP サーバに登録されたデータを検索するためのコマンド

である。

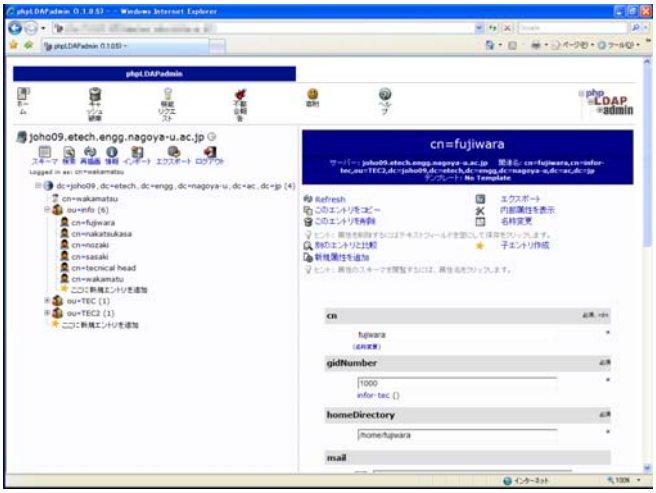

図５．phpLDAPadmin のデータ設定画面

次に、コマンド使用例として、test.ldif ファイルに登録されている管理データを LDAP に追加するには、LDAP サーバ上で次のコマンドを実行する。

ldapadd -x -D "ou=info, dc=joho, dc=engg, dc=nagoya-u, dc=ac, dc=jp" -W –f test.ldif

これで、LDAP サーバ上にデータが登録される。

また、今回利用した OpenLDAP サーバ用に、Web ブラウザ上からデータ管理ができるフリーのアプリケーションとして「phpLDAPadmin」が利用でき、ldif ファイルを用意することなく表示された属

性名に対して属性値を設定することでデータが登録できる(図５．参照)。

４－２．LDAP データの動作テスト

ldif ファイルの設定についての動作確認をするためのテストを以下の様に実施した。

(1) スキーマの設定

LDAP を利用したユーザ管理を行うために､LDAP サーバが読み込むスキーマの設定を slapd.conf ファイルで行い、nis.schema を有効にした。

(2) データ登録作業

データ登録作業は、ldapadd コマンドを利用し ldif ファイルをインポートするという方法で行った。登録の確認作業は、ladpsearch コマンドと、管理ツール(phpLDAPadmin)を利用して行った。

なお、表２．に本研修で使用した ldif ファイルを示す。

表２．研修で使用した ldif ファイル

```
dn: uid=test,dc=joho,dc=engg,dc=nagoya-u,dc=ac,dc=jp
uid: test
cn: test
objectClass: account
objectClass: posixAccount
objectClass: top
userPassword: {crypt}x
loginShell: /bin/bash
uidNumber: 500
gidNumber: 500
homeDirectory: /home/test
gecos: test
```

(3) クライアントの設定

図６．に LDAP を利用したユーザ認証の仕組みを示す。nss_ldap を LDAP サーバに連携することでユーザ情報とパスワード情報を取得することができ、PAM 認証設定によりこれらの情報がクライアント上で使用できるようになる。

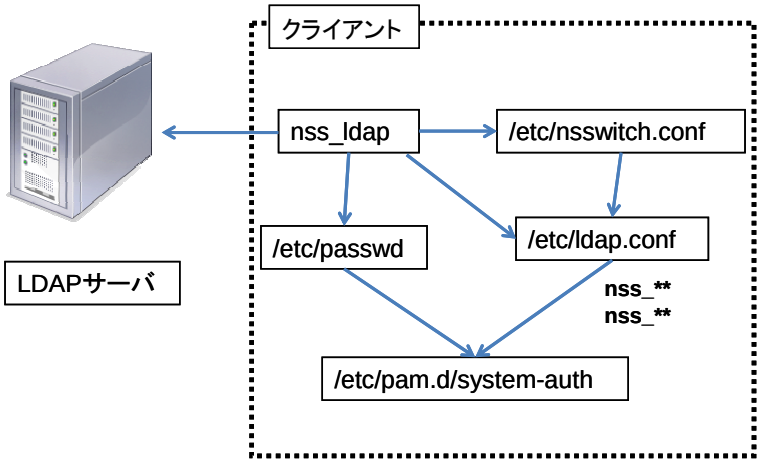

図６．クライアントから LDAP への連携

LDAP サーバ上の情報をクライアント上から利用するためには､クライアント側に以下の設定を行う必要がある。

① クライアント上に、nss_ldap(251-0v11) をインストールする。

② 次に、設定ファイル /etc/ldap.conf ファイルに LDAP サーバの IP アドレス、ポート番号、検索スコープ、パスワードのハッシュアルゴリズム等を設定する。

③ /etc/nsswitch.conf ファイルを変更する。記述順序は、ファイルを参照し、次に LDAP を参照する設定にしておく。もし LDAP を先に設定してしまうと、LDAP サーバに接続できない時クライアントが起動できなくなるので注意する（表３．参照)。

表 3. /etc/nsswitch.conf 設定例

```
passwd:     file     ldap
shadow:     file     ldap
group :     file     ldap
```

④ ユーザ管理を行うため、クライアント上のユーザ認証設定である PAM 認証部分の system-auth ファイルの設定を変更する（表４．参照)。

以上の設定変更をすることで、

「クライアントから LDAP サーバへのアクセス」→「ログイン後、必要な識別子上にバインド」→「指定の検索条件にマッチしたエントリの取得」→「結果が得られるか？」という流れで、クライアントサーバから LDAP サーバへの通信が確立される。

表 4．/etc/pam.d/system-auth 設定例

```
auth       sufficient    /lib/security/$ISA/pam_ldap.so use_first_pass
account    [default=bad success=ok user_unknown=ignore service_err=ignore system_err=ignore
           authinfo_unavail=ignore]   /lib/security/$ISA/pam_ldap.so
password   sufficient    /lib/security/$ISA/pam_ldap.so use_authtok
session    optional      /lib/security/$ISA/pam_ldap.so
```

(4) ユーザ認証動作テスト

ユーザ認証確認テストとして、次の動作テストを実施した。

① クライアントサーバ上から LDAP サーバの情報を取得する getent コマンドを利用して、ユーザ情報の取得を試みたところ、クライアントのローカルユーザ名に続いて LDAP サーバ上のユーザ名が表示され、クライアントから LDAP サーバにアクセスして情報を取得できることを確認した。

② LDAP サーバのユーザ管理情報を利用するために、su コマンドを用いてクライアントで LDAP サーバの登録ユーザへの変更を試み、無事ログインできることを確認した。

③ ネットワーク接続からクライアント上に LDAP サーバの登録ユーザでログインできるかどうか確認するため、ssh コマンドを用いて LDAP サーバの登録ユーザでログインを試みたところ、ログインできることを確認した。

④ クライアント上において、最初 LDAP サーバの登録ユーザ作業環境であるホームディレクトリは存在しないが、ログイン後 LDAP サーバの登録ユーザのホームディレクトリが自動的に作成され、クライアント上での作業環境が整うことが確認できた。

これらのことから、クライアント上からネットワークを経由して、LDAP サーバのユーザ管理情報を利用できることが確認できた。

(5) Web 動作テスト

次に、LDAP データ取得の応用例として、Web アプリケーションから LDAP サーバにアクセスして情報を取得するという動作テストを行った。ユーザ認証部分には Apache 上の Basic 認証を使用し、PHP 言語で作成した検索プログラムを用いて Web サーバ(今回は Apache2 を使用)上で動作テストを試みた。その流れは以下の通りである(図７．参照)。

① クライアント上からブラウザでテストページにアクセスする。Basic 認証によりユーザ名とパスワードの入力が求められる。

② ユーザ名とパスワードを入力すると、Web サーバから LDAP サーバに対してログイン処理と LDAP サーバ上のユーザ情報とパスワード情報の確認作業が行われる。

③ ユーザ認証が完了した後、テストページである検索入力ページが表示され、それと同時に検索プログラムの内部処理により、Web サーバから LDAP サーバに対してログイン処理が行われる。

④ テストページ上で検索条件を指定し実行することにより、Web サーバを介して LDAP サーバ上のデータ検索処理を行う。

⑤ LDAP サーバは検索条件に合致した情報をデータから探し出しその情報を Web サーバに返す。この情報を元に検索プログラムの内部処理より検索結果をテストページ上で表示する。

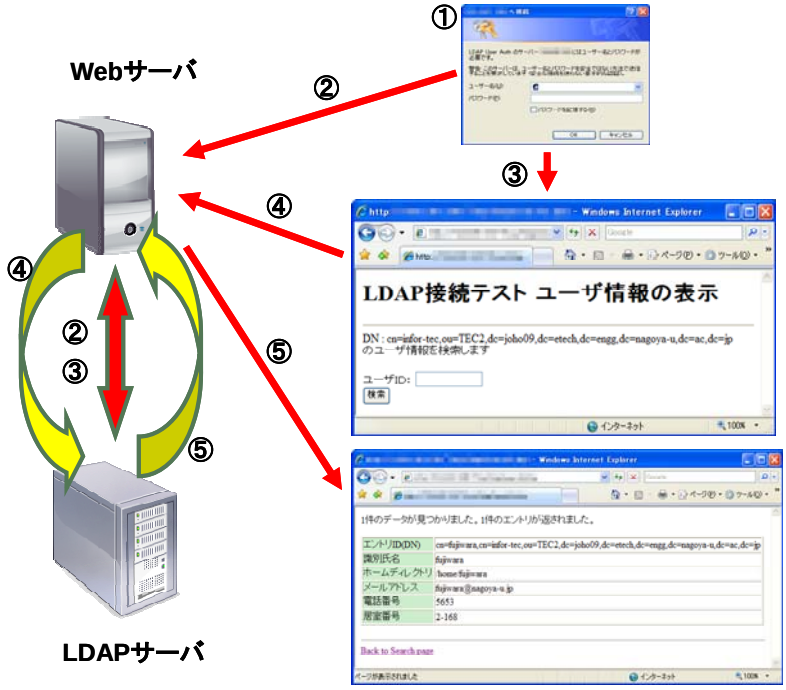

図 7. Web アプリケーションに応用したときの処理の流れ

この様に、Web アプリケーションにおいても LDAP サーバを使ったユーザ認証の利用と LDAP データの検索が行えることが確認できた。

5．まとめと今後の課題

今回の技術系研修を通して、

(1) OpenLDAP についての知識の習得が出来たこと、

(2) LDAP サーバの構築、その設定方法のノウハウの習得ができたこと、

(3) クライアントから LDAP サーバのユーザ認証が利用可能であること、

(4) Apache の Basic 認証で LDAP サーバのユーザ認証が利用可能であること、

(5) Web 上から LDAP サーバへのデータ検索を確認できたこと

等を確認することができ、本研修で当初予定していた目的を達成することが出来た。

今後は、今回の研修でテストモデルとして構築した OpenLDAP サーバを用いたユーザ管理と、Web アプリケーション等への応用を検討する予定である。

参考文献

1．デージーネット、「入門 LDAP/OpenLDAP ディレクトリサービス導入・運用ガイド」、秀和システム

2．Gerald Carter 著 でびあんぐる監訳、「LDAP －設定・管理・プログラミング－」、オーム社