LDAP と GoogleApps の連携

田中美里
Misato TANAKA

1　はじめに

近年，IT 技術の導入が進み，企業や団体に所属するユーザの利便性はますます向上している．一方で，同一ユーザが複数のサーバにアカウントを持つ等，情報資源が重複して管理されるといった事態は数多い．

このような重複を省き，統合的な管理を行うための技術として注目されているのが LDAP（Lightweight Directory Access Protocol）である．LDAP によって，Web サーバのアクセス制御，メールサーバのアカウント管理，エイリアス管理などを効率的に行うことができる．

本発表では，LDAP の概要について述べる．さらに，Google の提供する独自ドメイン向けサービスである Google Apps のユーザ管理機能と LDAP の連携を行うアプリケーションを開発し，その機能について検討する．

2　LDAP

2.1　ディレクトリサービス

インターネット上には多くの情報資源が存在している．ここで言う情報資源とは，ニュースや地図情報ではなく，ユーザ情報，サーバやサーバ上で提供されているサービス，またはプリンタ等の機器情報等を含んでいる．これらの資源や属性情報を記憶し，更新，検索する機能を提供するシステムがディレクトリサービスである．

ディレクトリサービスにおけるディレクトリとは，階層構造を持ったファイルシステムのことであり，具体的にはユーザ情報を格納するデータベースのようなものである．コンピュータがネットワークに接続し，ファイルやプリンタを共有するとき，他者のファイルへのアクセス権が問題となる．そこで，ユーザの識別とアクセス権限を管理するために，情報資源の管理が容易なディレクトリサービスが利用されるようになった．

このディレクトリ情報は少数のサーバによって管理され，メールサーバやアプリケーションサーバといった多数のサーバによって参照される．こうして一貫したユーザ管理が可能となり，管理工数の削減や，ミスの排除といったメリットを得ることができる．

ディレクトリサービスを提供するシステムには，NIS（Netowork Information System）や LDAP が挙げられる．前者に対してはアクセス制御機能が弱く，また，Windows やファイル共有システムの Samba との連携が難しいなど，以前から多くの問題が指摘されてきた．そのため現在では，よりセキュリティが高く，機能拡張性に優れた LDAP の普及が進んでいる．

2.2　LDAP

LDAP とは，ITU 勧告 X.500 モデルのディレクトリへとアクセスすることを目的としたネットワークプロトコルである．このプロトコルを実装したディレクトリサービスそのものを LDAP と呼ぶこともある．

LDAP のディレクトリは，木構造（Directory Information Tree：DIT）によって階層的に管理されている．Fig. 1 にディレクトリ構造の概念図を示す．

Fig. 1 における一つ一つのノードはエントリ（entry）と呼ばれ，RDBMS（Relational DataBase Management System）におけるレコードのようなものである．頂点のエントリは特にベース（Base）と呼ばれている．各エントリは，識別名（Distinguished Name：DN）によって一意に識別される．また，”ou=students”，”ou=teachers”などは相対識別名（Relative Distinguished Name：RDN）と呼ばれ，親ノードに対して一意なものでなければならない．

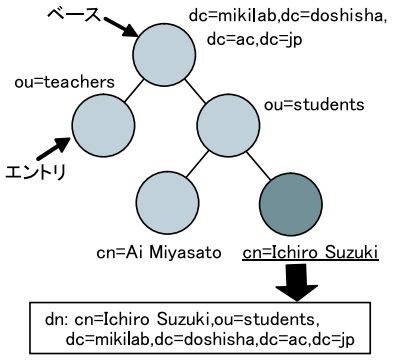

Fig.1　LDAP の木構造（参照：参考文献 [2]）

LDAP は高速な読み取り機能と柔軟な検索能力を持つ．また，標準化されたネットワークプロトコルであるため，OS やマシンアーキテクチャに関係なく接続することができる．SQL 言語によって接続する RDBMS（Relational DataBase Management System）と比較して，LDAP はアクセスが容易である．

しかし，RDBMS が頻繁な更新に耐え得る性能を持つのに対し，LDAP は更新は滅多に発生しないという思想を基に最適化されている．そのために大量更新には向かないといった特性を持つ．

3　Google Apps

3.1　独自ドメイン向けサービス

Google Apps（Google Apps for Your Domain）は Google Inc. による企業，団体向けのホスティングサービスである．独自のドメイン，またはサブドメインを有す

る組織がこのサービスに自身のドメイン名を登録すると，その組織や構成員は，様々な Web アプリケーションサービスを Google から受けることが出来る．

例えば，”example.co.jp” という独自のドメイン名を持つ企業が，このサービスに登録したケースを考える．この時，Google Apps 上で”tanaka” というユーザアカウントが発行されると”tanaka@example.co.jp” というメールアドレスが自動的に生成される．このアドレスは，Google 提供のメールサービスである Gmail 上で利用できる．

Google Apps の運用は教育現場でも既に進められており，日本大学では今年の 4 月から Gmail のソリューション「NU-MailG」[3] を稼動させている．大学側は 2007 年度新入生約 3 万人にアカウントを発行し，将来的には全学部 10 万人の利用を予定している．尚，このシステムのアカウント管理には，前述した LDAP が利用されている．

3.2 提供ツール

現在，Google Apps 日本語版によって提供されているツールを以下に示す．

- Gmail
  独自ドメインにおけるメールサービスを提供
- Google カレンダー
  個人のスケジュール管理，及びグループでのスケジュール調整が可能
- Google トーク
  インスタントメッセンジャー

これらに加えて，独自ドメインのホームページが簡単に作成できる Google Page Creator が，管理者向けに提供されている．また，英語版ではワープロ・表計算用ソフトである GoogleDocs&Spreadsheets，個人のスタートページをカスタマイズする iGoogle の機能もサポートされている．

4 LDAP と Google Apps の連携

4.1 システム構成

Fig. 2 に，今回作成するシステムの構成を示す．

本システムは，Web アプリケーションとして動作する．LDAP サーバの管理者がこのアプリケーションを用いて，LDAP サーバに情報の追加，削除，変更を要求した場合，同様の要求が Google Apps に対しても送信され，ユーザのアカウント情報が更新できる．

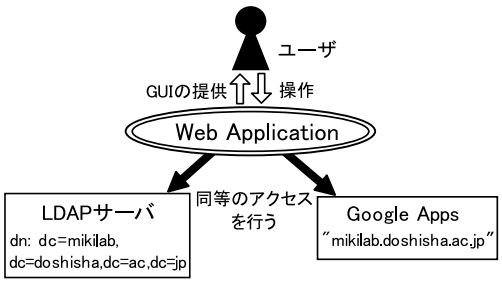

Fig.2 アプリケーションの構成（出典：自作）

また，本システムの作成のため，OpenLDAP Project によって開発されている OpenLDAP を用いて LDAP サーバを構築した．

4.2 作成したシステム

作成したシステムの GUI を，Fig. 3 に示す．ディレクトリの木構造は，画面左フレームにおいてツリー状に表現される．ツリーの頂点にはベースの名が，各エントリ名には RDN が表示されている．ここではベースの下に 3 つのグループが存在し，各ユーザはそれぞれのグループに属している．

ユーザの追加は，各グループの RDN の右にある「ユーザの追加ボタン」によって行う．クリックすると，右の作業フレーム上にユーザの追加を行うためのフォームが呼び出されるので，そこに必要な情報を入力する．ユーザ情報の変更，削除については，各ユーザの RDN の右にある「ユーザ情報の編集ボタン」，「ユーザの削除ボタン」を押す．追加と同様に，右の作業フレーム上に専用のフォームが現れる．

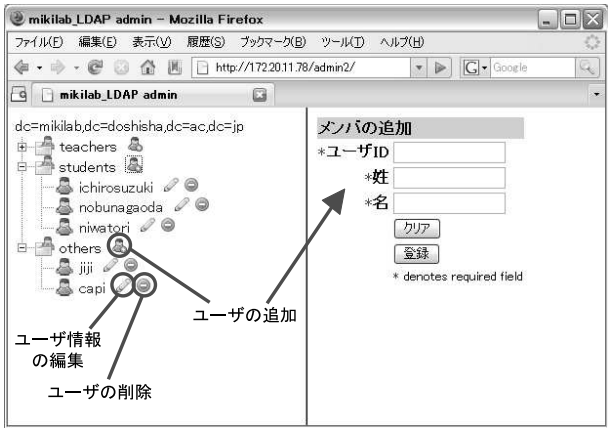

Fig.3 ユーザの追加画面（出典：自作）

5 今後の展望

現在のアプリケーションにおいて表示されいているエントリは，ベースからの階層の数を限定したものとなっている．ここに再帰処理を用いることで，より柔軟に，ディレクトリ構造の表示と操作を行うことができるようになる．

また，LDAP のエントリの追加には，入力フォームの動的な変化が有効である．ユーザのグループ間の移動などもマウスドラッグで実現できれば，ユーザの操作性が大いに向上すると思われることから，AJAX による実装が望ましい．

参考文献

1) LDAP Super Expert
株式会社技術評論者，2006 年

2) [ThinkIT] 実践！ OpenLDAP 活用術 第 1 回
http://www.thinkit.co.jp/cert/tech/18/1/2.htm

3) 日本大学学生用メールシステム～NU-MailG～について
http://www.nihon-u.ac.jp/news/2007/2007000001.html