postLdapadmin

1.00版　2007年10月12日

目次

1. postLdapAdmin とは

postLdapadmin とは、メールサーバで利用する LDAP の管理を Web インタフェース上で行うための Web アプリケーションです。postLdapAdmin が前提とするシステム構成は図 1.1 のとおりです。

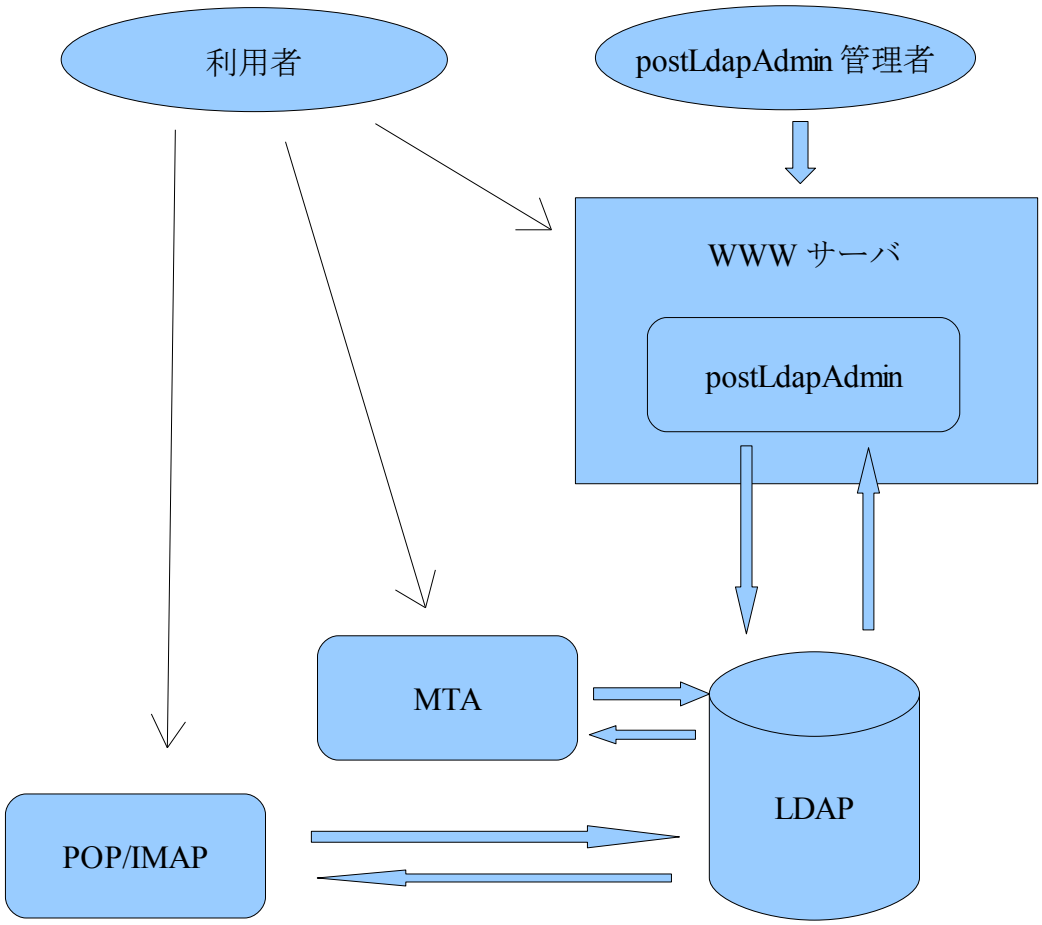


図 1.1 システム構成

1.1 メールシステムと LDAP の連携

ユーザ情報を LDAP に登録することで、従来はサーバ上で管理していた UNIX アカウントを、システムから完全に切り離してまとめて管理することができるようになります。これを仮想ユーザ管理といいます。

1.2 メールシステムの仮想ユーザ管理を LDAP で行うことのメリット

メールシステムの仮想ユーザ管理を LDAP で行うことには、次のようなメリットがあります。

- メール配送のためにシステムアカウントを作成する必要がありません。
- メールのユーザ管理をすべて LDAP だけで行うことができます。
- 別名配送や転送などもすべて LDAP 上で統合管理することができます。

1.3 postLdapAdmin を利用するメリット

postLdapAdmin を利用することには、次のようなメリットがあります。

- LDAP データの管理に関する知識がなくても比較的簡単に LDAP データの追加・編集・削除ができます。
- LDAP データの追加・編集・削除のために LDAP 管理コマンドを使用する手間がありません。

1.4 postLdapAdmin で管理する LDAP データ

postLdapAdmin には、表 1.1 のような LDAP のデータを管理することができます。

表 1.1: postLdapAdmin で管理できる LDAP データ

管理者用インタフェース	ユーザ管理機能	仮想ユーザの追加	仮想ユーザパスワード
			仮想ユーザごとのクォータ値※
			メールエイリアス※
			メール転送アドレス※
		仮想ユーザの編集	仮想ユーザパスワード
			仮想ユーザごとのクォータ値※
			メールエイリアス※
			メール転送アドレス※
		仮想ユーザの削除	
		仮想ユーザの検索	
	メーリングリスト管理機能	メーリングリストの追加	
		メーリングリストの削除	
		メーリングリストの検索	
		メーリングリストに所属するメールアドレスの追加	
		メーリングリストに所属するメールアドレスの削除	
	仮想ユーザ管理を行う管理者（postLdapAdmin 管理者）のパスワード管理		
ユーザ用インタフェース	仮想ユーザのユーザパスワード、メール転送アドレス管理※		

※クォータ制御、メールエイリアス、メール転送アドレスの機能を利用するためには、メールサーバの機能が対応している必要があります。

2. 計画

本章では、次のことを解説します。

- 事前に用意しておくソフトウェア
- 決めておかなくてはならないこと
- 設定概要

2.1 事前に用意しておくソフトウェア

postLdapAdmin は、以下のソフトウェアと連携して動作します。

- LDAP サーバ
- メールサーバ
- POP/IMAP サーバ
- Web サーバ
- PHP5.1 以上（LDAP、mbstring、mcrypt 機能をサポートしている必要があります）

本書では、LDAP サーバに OpenLDAP、メールサーバに Postfix、POP/IMAP サーバに courier-imap、Web サーバに Apache を利用することを前提に解説します。

2.2 決めておかなくてはならないこと

postLdapAdmin のインストールの前に、表 2.1 の項目を決定しておいてください。本書では、設定例の項目に挙げた値を設定することを前提として解説します。

表 2.1: 決めておかなくてはならないこと

項目	解説	設定例
postLdapAdmin インストールディレクトリ	postLdapAdmin ソフトウェアをインストールするディレクトリ	/usr/local
postLdapAdmin 管理者パスワード	postLdapAdmin の管理者パスワード	admin
仮想ドメイン	仮想メールボックスに配送するドメイン（仮想ドメイン）	test.desginet.jp
メール管理アカウント	メールのデータを管理するアカウント 仮想ユーザへのメール配信では、メールアドレス毎にアカウントを用意する必要がありません。全メールを一つのアカウントの権限で管理します。	vmail（ユーザ ID: 400）
メール保管ディレクトリ	メールを保管するディレクトリ ディレクトリの所有者・グループは、メール管理アカウントの権限である必要があります。	/home/mail/test.desinet.jp
postLdapAdmin ログファイル	postLdapAdmin の Web インタフェースのログファイル名 ログファイルを格納するディレクトリは、Web サーバの実行アカウントの権限にします。	/home/mail/test.desinet.jp/log/result.log
LDAP データの構造	仮想ドメインの管理を行う LDAP データの構造 管理する仮想ドメインの階層、メールユーザを管理する階層、	図 2.1: LDAP の基本構造の例

	メーリングリストを管理する階層を準備する必要があります。メールユーザを管理する階層、メーリングリストを管理する階層は、管理する仮想ドメインの階層の配下に作成してください。	
LDAP suffix	このデータベースのデータの DN	dc=designet,dc=jp
LDAP バインド DN	LDAP のバインド DN	cn=Manager,dc=designet,dc=jp
LDAP バインドパスワード	LDAP のバインドパスワード	secret
LDAP 検索 DN	LDAP サーバの検索を開始する DN	dc=test,dc=designet,dc=jp

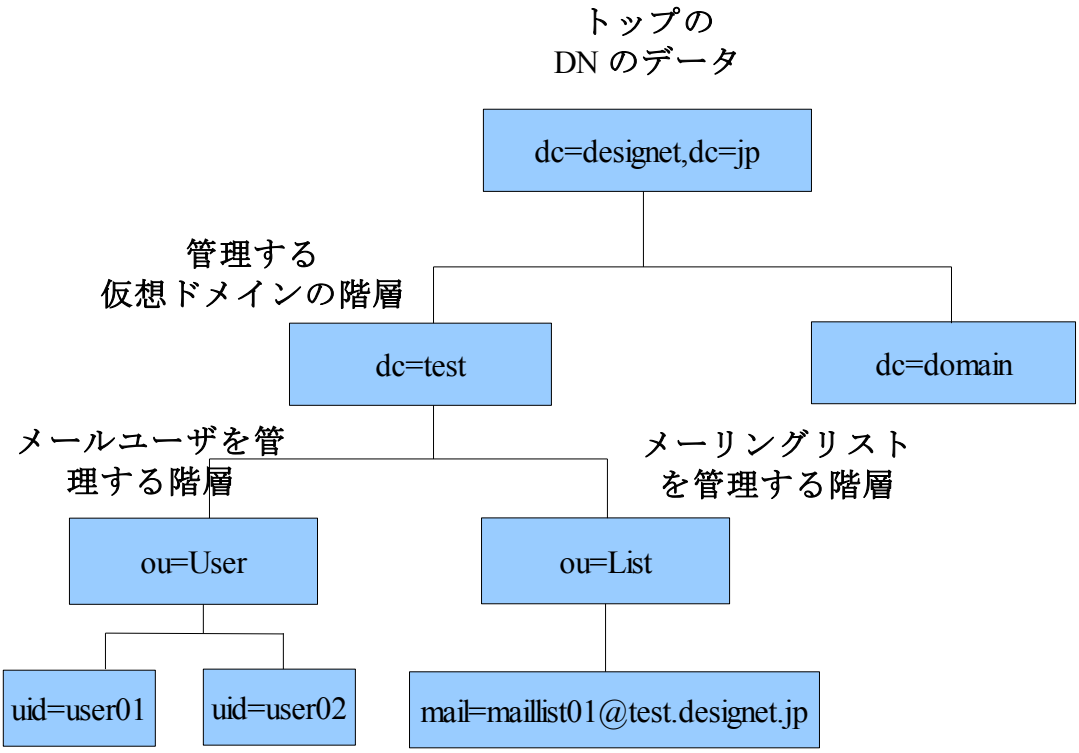


図 2.1: LDAP の基本構造の例

2.3 設定概要

各システムを構成し、postLdapAdmin を導入するには、図 2.2 の手順で設定を行ってください。

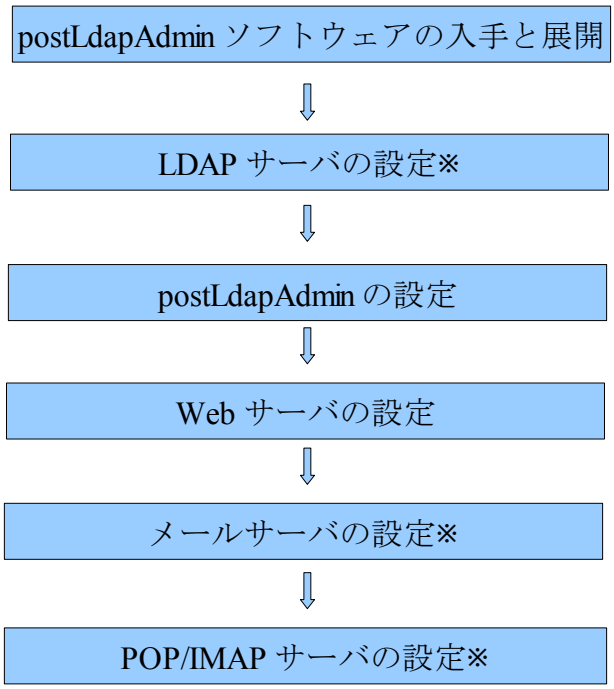


図 2.2: postLdapAdmin 導入手順

導入手順の中の※の項目については、設定の例を Appendix で解説します。

3. インストール

3.1 postLdapAdmin の入手と展開

postLdapAdmin ソフトウェアは、postLdapAdmin プロジェクトのダウンロードページから入手することができます。

http://sourceforge.jp/postldapadmin

postLdapAdmin ソフトウェアをダウンロードしたら、圧縮されたアーカイブファイルを展開します。展開するディレクトリは Web サーバから参照可能である必要があります。次は、/usr/local/配下に展開する例です。

```
# tar zxf postLdapAdmin-VERSION.tar.gz -C /usr/local
```

このように展開した場合、展開後のディレクトリ構成は、表 3.1 のようになります。

表 3.1: postLdapAdmin のディレクトリ構成例

ディレクトリ名	解説
/usr/local/postLdapAdmin/htdocs	Web インタフェースに関するファイルを格納するディレクトリ
/usr/local/postLdapAdmin/lib	ライブラリを格納するディレクトリ
/usr/local/postLdapAdmin/etc	仮想ドメインごとの設定ファイルを格納するディレクトリ
/usr/local/postLdapAdmin/postLdapAdmin.schema	LDAP 用スキーマファイル

3.2 LDAP サーバの設定

LDAP サーバとして OpenLDAP を例に解説を行います。LDAP サーバの設定は次の手順で設定を行います。

- スキーマファイルの読み込み
- LDAP データベースの索引

LDAP サーバの基本的な設定、LDAP データの基本構造の作成については、Appendix を参照してください。

3.2.1 スキーマファイルの読み込み

postLdapAdmin で扱うエントリには、postLdapAdmin オブジェクトクラスが含まれている必要があります。postLdapAdmin のアーカイブには、スキーマファイル postLdapAdmin.schema が同梱されています。OpenLDAP の場合は、この postLdapAdmin.schema を読み込むだけで postLdapAdmin オブジェクトクラスを利用できるようになります。postLdapAdmin.schema によって使用できる属性は表 3.2 のとおりです。

表 3.2: postLdapAdmin.schema

項目	内容	解説
オブジェクトクラス	postLdapAdmin	補助型のオブジェクトクラスです。構造型のオブジェクトクラスを同時に指定する必要があります。
必須属性	uid	ユーザ名を指定します。
	mail	メールアドレスを指定します。
オプション属性	userPassword	ユーザパスワードを指定します。
	quotaSize※	メール容量を指定します。
	mailAlias※	メールエイリアスのアドレスを指定します。
	mailDirectory※	メール保管ディレクトリを指定します。
	mailForwardingAddr※	メール転送先アドレスを指定します。

※postLdapAdmin.schema に収録されている属性。各属性名を任意で変更することはできません。

slapd.conf に postLdapAdmin.schema を読み込むように設定を行います。postLdapAdmin.schema は次の場所にあります。

[展開ディレクトリ]/postLdapAdmin/

次は、postLdapAdmin アーカイブを/usr/local/に展開したときの例です。

slapd.conf の設定例

```
include         /usr/local/postLdapAdmin/postLdapAdmin.schema
```

3.2.2 LDAP データベースの索引

postLdapAdmin では、LDAP の検索フィルタに属性「uid」「mail」を使用するため、次

の例のように索引（index）を設定してください。

slapd.conf の設定例

```
index uid,mail                  eq,sub
```

また、メールサーバ、POP/IMAP の設定で指定する LDAP の検索フィルタに使用する属性についても、index を作成してください。メールサーバ、POP/IMAP の設定については、Appendix を参照してください。

3.3 postLdapAdmin の設定

postLdapAdmin の設定は以下の手順で行います。

- 設定ファイルの設置
- メール保管アカウント、ディレクトリの準備

3.3.1 設定ファイルの設置

postLdapAdmin の設定ファイルは、次のディレクトリ配下に設置します。

[展開ディレクトリ]/postLdapAdmin/etc/[管理する仮想ドメイン名]/

postLdapAdmin アーカイブを/usr/local/に展開した場合は、次の例のように管理する仮想ドメイン名のディレクトリを作成します。

```
# cd /usr/local/postLdapAdmin/etc
# mkdir test.designet.jp
```

3.3.1.1 web.conf

管理する仮想ドメイン名のディレクトリを作成しましたら、postLdapAdmin の設定ファイル（web.conf）を用意します。次のディレクトリに web.conf のサンプルが用意されています。

[展開ディレクトリ]/postLdapAdmin/etc/web.conf.sample

コピーして環境に合わせて編集してください。

```
# cp web.conf.sample test.designet.jp/web.conf
```

web.conf の設定例

```
LdapServer=127.0.0.1
LdapPort=389
LdapBindDn=cn=Manager,dc=designet,dc=jp
LdapBindPw=secret
LdapBaseDn=dc=test,dc=designet,dc=jp
ReferrerUrl=http://test.designet.jp/
DiskQuotaDefault=100
BaseMailDir=/home/mail/test.designet.jp
LinePerPage=5
AdminName=admin
AdminPasswd=21232f297a57a5a743894a0e4a801fc3
```

```
LogFile=/home/mail/test.designet.jp/log/result.log
MailDelcommand=sudo -u vmail deluser
LdapUserSuffix=ou=User
LdapListSuffix=ou=List
LdapScope=sub
LdapFilter=(uid=%u)
LdapMlFilter=(mail=*)
LdapObjectClass=account
DisplayUser=uid
DisplayMl=mail
```

AdminPasswd の項目には、MD5 エンコードしたパスワード文字列を設定します。パスワードを『admin』と設定する場合は次のようにコマンドを実行します。

```
$ echo -n admin | openssl dgst -md5
```

MailDelcommand の項目には、仮想ユーザを削除する際に実行する、該当の仮想ユーザのメール保管ディレクトリを削除するコマンドを指定します。ここで指定したコマンドには、引数として削除対象仮想ユーザのメールディレクトリのパスが渡されます。上記の web.conf の例では、sudo コマンドを利用して deluser スクリプトを実行し、削除対象仮想ユーザのメールディレクトリを削除するように設定しています。deluser スクリプトとしては、指定されたディレクトリがメールディレクトリかどうか確認してから削除するようなスクリプトを作成することをお勧めします。sudo の設定では、deluser スクリプトを実行できる権限を Web 稼動ユーザに与えておいてください。また本書の例では、vmail ユーザで deluser スクリプトを実行するように指定しているので、vmail ユーザが deluser スクリプトを実行できる権限を与えておいてください。

deluser スクリプトの例

```
#!/bin/bash

DELDIR=$1
BASEMAILDIR=/home/mail/test.designet.jp

# 引数のメールディレクトリがメール保管ディレクトリ名を
# 含んでいればメールディレクトリと判断
echo ${DELDIR} | grep ${BASEMAILDIR} > /dev/null
if [ $? -ne 0 ]
then
        exit 1
fi

# 引数のメールディレクトリがディレクトリかどうか判定
if [ ! -d ${DELDIR} ]
then
        exit 1
fi

# メールディレクトリ削除
rm -rf ${DELDIR}
if [ $? -ne 0 ]
```

```
then
        exit 1
fi

exit 0
```

MailDelcommand には、削除対象仮想ユーザのメールディレクトリをバックアップディレクトリへ移動するようなスクリプトを指定することも可能です。また、コマンドをリモートから実行することもできます。

web.conf の設定項目については、第 5 章を参照してください。

3.3.1.2 admin.key

web.conf を用意したら、暗号化キーファイル（admin.key）を設定します。postLdapAdmin では、admin.key で指定した文字列をもとに暗号化したキーを利用してセッション管理を行っています。任意の文字列を設定してください。次のディレクトリに admin.key のサンプルが用意されています。

[展開ディレクトリ]/postLdapAdmin/etc/admin.key.sample

サンプルを利用する場合は、そのままコピーしてください。

```
# cp admin.key.sample test.designet.jp/admin.key
```

admin.key の設定例

```
DxcMSHCM
```

3.3.2 メール保管アカウント、ディレクトリの準備

設定ファイルの準備ができたら、以下の設定を行います。

- メール保管アカウントの作成
- メール保管ディレクトリ
- postLdapAdmin ログディレクトリ

次の例にしたがって設定を行ってください。

メール保管アカウントの作成

```
# useradd -u 400 -s /sbin/nologin -M vmail
```

メール保管ディレクトリの作成

```
# mkdir -p /home/mail/test.designet.jp
# chown -R vmail:vmail /home/mail/test.designet.jp
```

postLdapAdmin ログディレクトリの作成

```
# mkdir /home/mail/test.designet.jp/log
# chown apache:apache /home/mail/test.designet.jp/log
```

本書では、Web サーバの実行アカウントを「apache」として、ログディレクトリに apache アカウントの権限を付与しています。

3.4 Web サーバの設定

Apache の設定のために httpd.conf ファイルを編集します。以下の 3 点の設定を行ってください。

- ディレクトリアクセス制御設定
- 環境変数の設定
- DirectoryIndex の設定

3.4.1 ディレクトリアクセス制御設定

postLdapAdmin の管理者用インターフェースとユーザ用インタフェースに対してアクセス許可設定を行います。次のディレクトリに対してアクセス許可の設定を行ってください。

[展開ディレクトリ]/postLdapAdmin/htdocs/

次は、postLdapAdmin アーカイブを/usr/local/に展開した場合の例です。

httpd.conf の設定例

```
<Directory "/usr/local/postLdapAdmin/htdocs">
order deny,allow
deny from all
allow from all
</Directory>
```

3.4.2 環境変数の設定

postLdapAdmin の Web インタフェースで使用する環境変数を設定します。

httpd.conf の設定例

```
SetEnv LOG_NAME test.designet.jp
SetEnv DOMAIN test.designet.jp
```

LOG_NAME

postLdapAdmin のログに出力するサーバ名を設定してください。

DOMAIN

postLdapAdmin の Web インタフェースから仮想ユーザを登録する際のメールアドレスのドメインパートとして使用する値を設定します。仮想メールボックスに配送するドメイン名（仮想ドメイン）を設定してください。

3.4.3 DirectoryIndex の設定

DirectoryIndex に「index.php」の指定がない場合は、DirectoryIndex の記述に「index.php」を追加してください。

httpd.conf の設定例

```
DirectoryIndex  index.html index.php
```

3.4.4 エイリアス設定

postLdapAdmin アーカイブをドキュメントディレクトリ以外の場所で展開した場合は、

エイリアスの設定を行ってください。postLdapAdmin の管理者用インタフェース、ユーザ用インタフェースの URL を、次のディレクトリへマッピングします。

[展開ディレクトリ]/postLdapAdmin/htdocs/

次は、postLdapAdmin アーカイブを/usr/local/に展開した場合の例です。

httpd.conf の設定例

```
Alias /postLdapAdmin/ "/usr/local/postLdapAdmin/htdocs/"
```

以上の設定を行い、Web サービスを起動したら、postLdapAdmin の Web インタフェースにアクセスすることができます。

管理者用インタフェース

http://test.designet.jp/postLdapAdmin/admin/

ユーザ用インタフェース

http://test.designet.jp/postLdapAdmin/user/

管理者用インタフェース、ユーザ用インタフェースにアクセスすると、図 3.1 のようなログイン画面が表示されます。

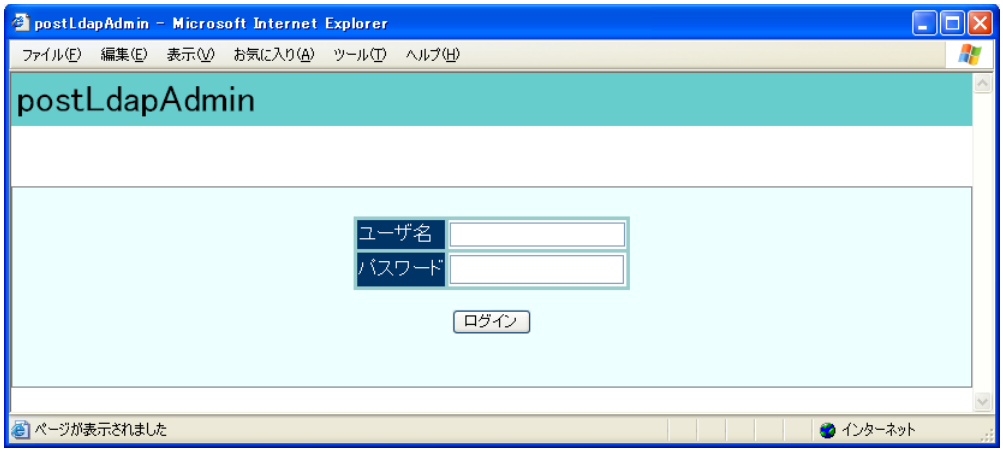


図 3.1: ログイン画面

3.4.5 複数の仮想ドメインを管理したいとき

複数の仮想ドメインを管理する場合は、仮想ドメイン毎に環境変数 LOG_NAME、DOMAIN の値を設定する必要があります。次の例にならい、VirtualHost を作成し、VirtualHost ごとに環境変数 LOG_NAME、DOMAIN を設定してください。

httpd.conf の設定例

```
<VirtualHost 192.168.1.98>
    ServerName test.designet.jp                ← 管理する仮想ドメイン①

    SetEnv LOG_NAME test.designet.jp
    SetEnv DOMAIN test.designet.jp
```

```
    Alias /postLdapAdmin/ "/usr/local/postLdapAdmin/htdocs/"
</VirtualHost>

<VirtualHost 192.168.1.98>
    ServerName domain.designet.jp              ← 管理する仮想ドメイン②

    SetEnv LOG_NAME domain.designet.jp
    SetEnv DOMAIN domain.designet.jp

    Alias /postLdapAdmin/ "/usr/local/postLdapAdmin/htdocs/"
</VirtualHost>
```

4. 使い方

postLdapAdmin の利用方法を次の順に解説します。

- 基本的な機能
- postLdapAdmin の Web インタフェースの画面構成

4.1 基本的な機能

postLdapAdmin には次のような機能があります。

- 管理者用インタフェース
  - ユーザ管理機能
    - 仮想ユーザの追加
    - 仮想ユーザの検索
    - 仮想ユーザの編集
    - 仮想ユーザの削除
  - メーリングリスト管理機能
    - メーリングリストの追加
    - メーリングリストの削除
    - メーリングリストに所属するメールアドレスの追加
    - メーリングリストに所属するメールアドレスの削除
  - postLdapAdmin 管理者のパスワード管理
- ユーザ用インタフェース
  - 仮想ユーザのユーザパスワード、メール転送アドレス管理

4.2 postLdapAdmin の Web インタフェースの画面構成

postLdapAdmin の Web インタフェースの画面構成は図 4.1 のようになっています。

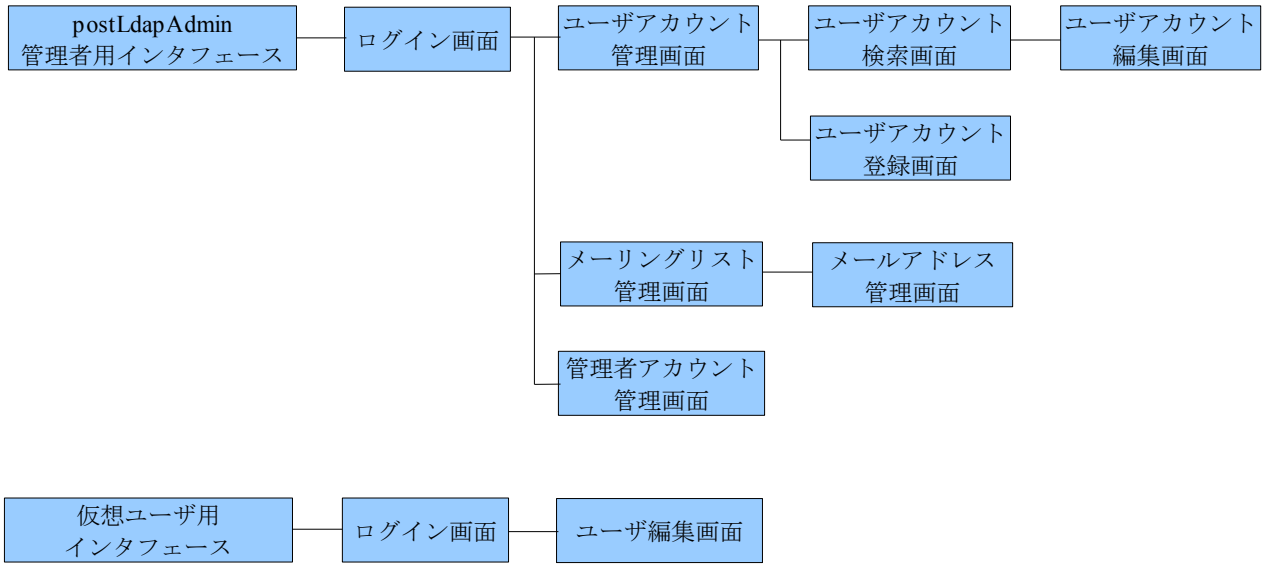
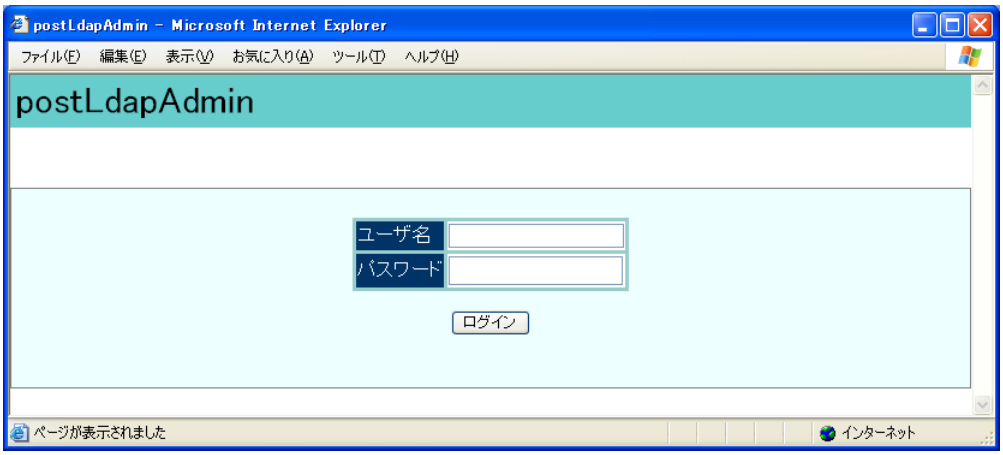


図 4.1: postLdapAdmin の画面構成

4.2.1 postLdapAdmin 管理者用インタフェース

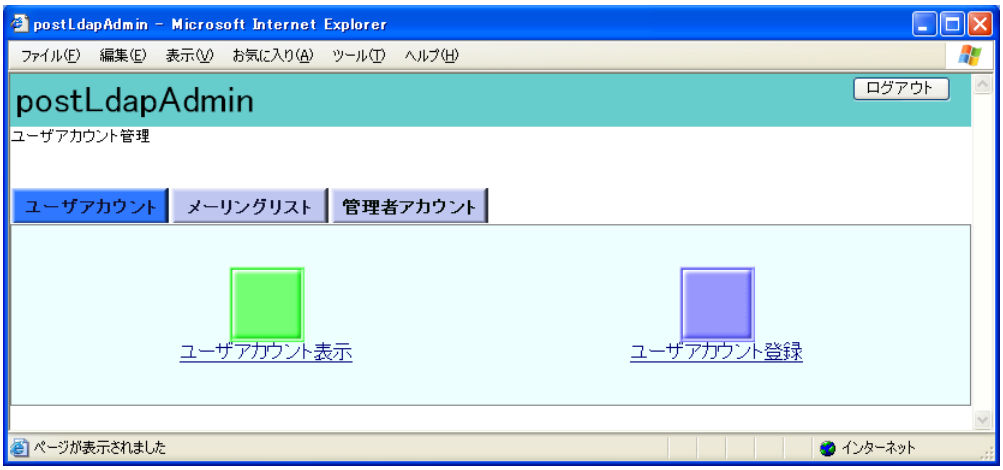
4.2.1.1 管理者ログイン画面



[ログイン]

管理者ユーザ名、パスワードを入力し、[ログイン]ボタンをクリックします。

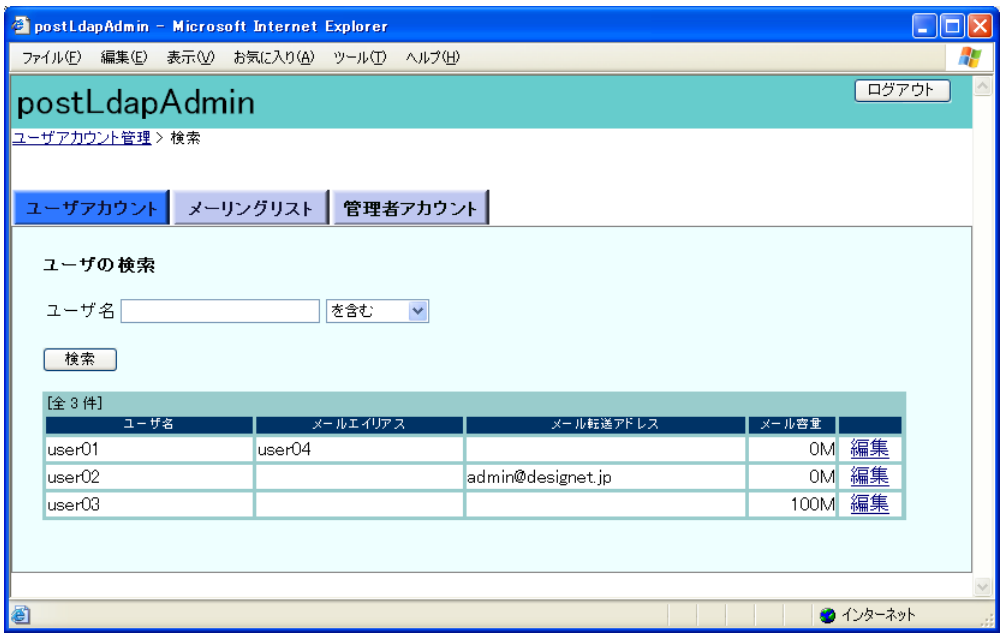
4.2.1.2 ユーザアカウント管理画面



仮想ユーザを検索・編集・削除するには、[ユーザアカウント表示]ボタン/リンクをクリックし、ユーザアカウント検索画面に移動します。

仮想ユーザを追加するには、[ユーザアカウント登録]ボタン/リンクをクリックし、ユーザアカウント登録画面に移動します。

4.2.1.2.1 ユーザアカウント検索画面



[仮想ユーザの検索]

次の項目を指定し、[検索]ボタンをクリックします。

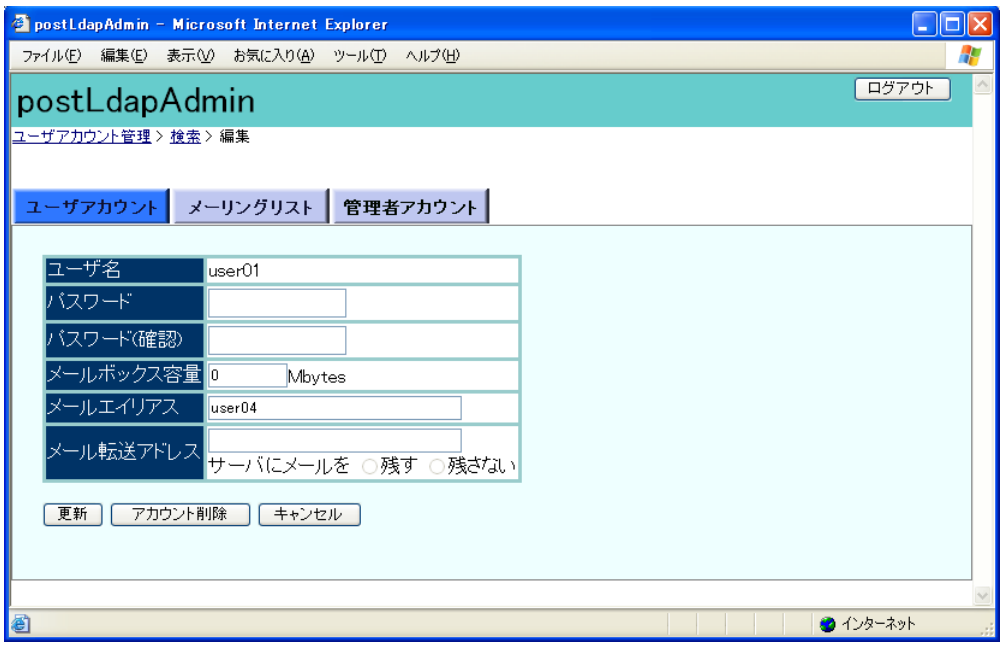
- 検索する文字列（ユーザ名）
- 検索条件（を含む/と一致する）

ユーザ名に何も入力しないで検索を行うと、登録されている仮想ユーザすべてを表示します。

検索結果として、次の項目が表示されます。

- ユーザ名
- メールエイリアス
- メール転送アドレス
- メール容量
- [編集]リンク
  - ○ 仮想ユーザの編集を行う画面に移動します。

4.2.1.2.2 ユーザアカウント編集画面



[仮想ユーザの編集]

次の編集する項目を入力し、[更新]ボタンをクリックします。

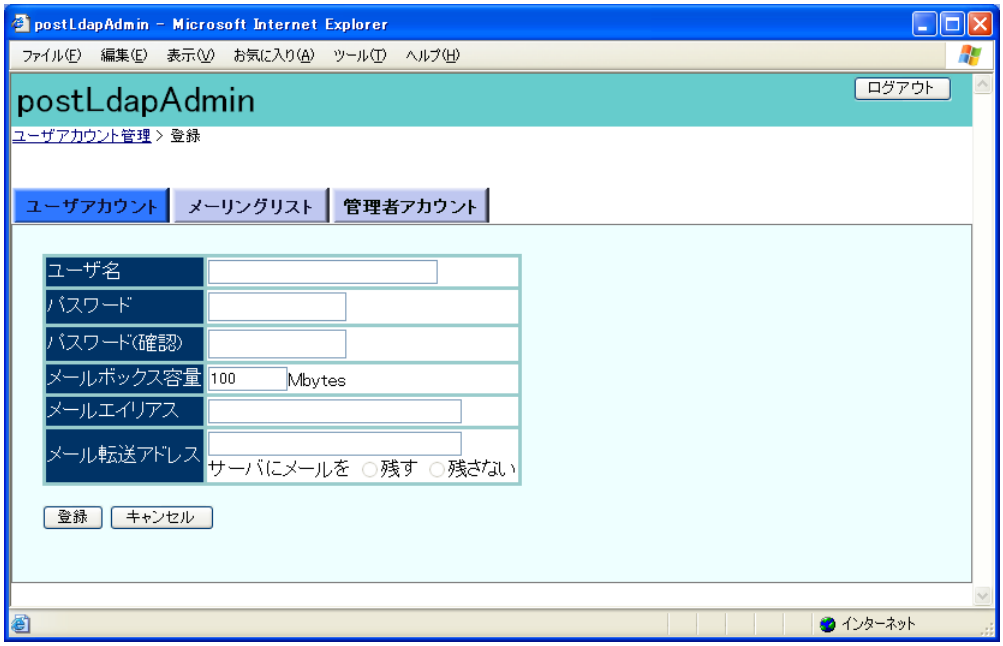
- ユーザ名
- パスワード/パスワード（確認）
- メールボックス容量
- メールエイリアス
- メール転送アドレス

メール転送アドレスを指定した場合は、サーバにメールを残すか残さないかを選択してください。

[仮想ユーザの削除]

[アカウント削除]ボタンをクリックします。

4.2.1.2.3 ユーザアカウント登録画面



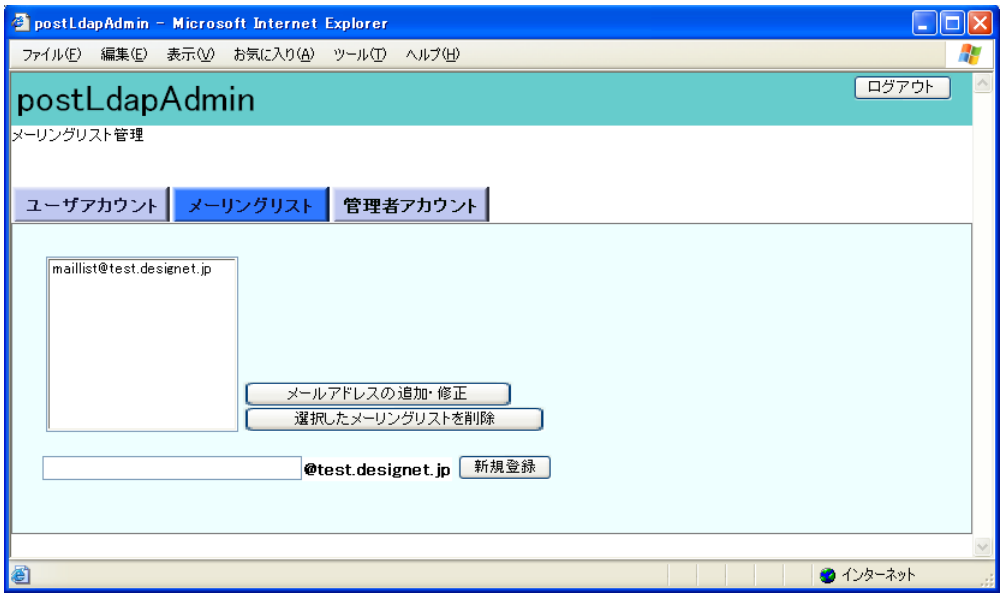
[仮想ユーザの追加]
　次の項目を入力し、[登録]ボタンをクリックします。

- ユーザ名
- パスワード/パスワード（確認）
- メールボックス容量※
- メールエイリアス※
- メール転送アドレス※

※必須項目ではありません。

　メール転送アドレスを指定した場合は、サーバにメールを残すか残さないかを選択します。

4.2.1.3 メーリングリスト管理画面



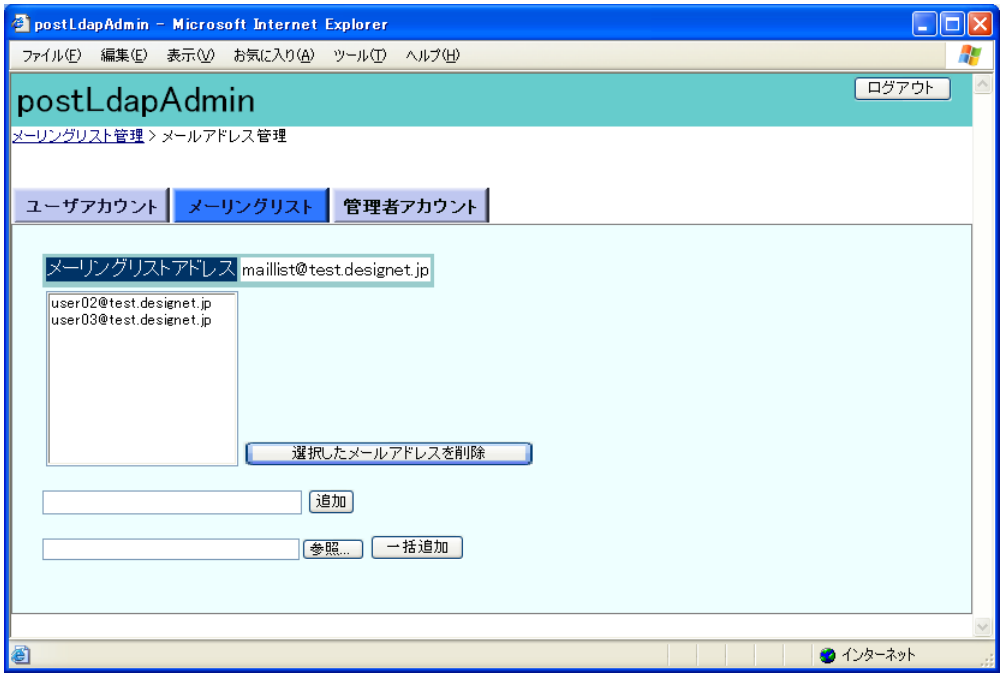
　画面左側のテキストエリアに、登録されているメーリングリストアドレスの一覧が表示されます。

[メーリングリストに所属するメールアドレスの追加・削除]
　メーリングリストアドレス一覧から削除するメーリングリストアドレスを選択します。[メールアドレスの追加・修正]ボタンをクリックし、メールアドレス管理画面に移動します。

[メーリングリストの削除]
　メーリングリストアドレス一覧から削除するメーリングリストアドレスを選択し、[選択したメーリングリストを削除]ボタンをクリックします。

[メーリングリストの追加]
　画面下部のメーリングリストアドレス入力欄に追加するメーリングリストアドレスを入力し、[新規登録]ボタンをクリックします。

4.2.1.4 メールアドレス管理画面



画面左側のテキストエリアに、メーリングリストに所属するメールアドレスの一覧が表示されます。

[メールアドレスの削除]

メールアドレス一覧から削除するメールアドレスを選択し、[選択したメールアドレスを削除]ボタンをクリックします。

[メールアドレスの追加]

画面中央のメールアドレス入力欄に追加するメールアドレスを入力し、[追加]ボタンをクリックします。

[メールアドレスの一括追加]

メールアドレスの一括追加は、次のように行います。

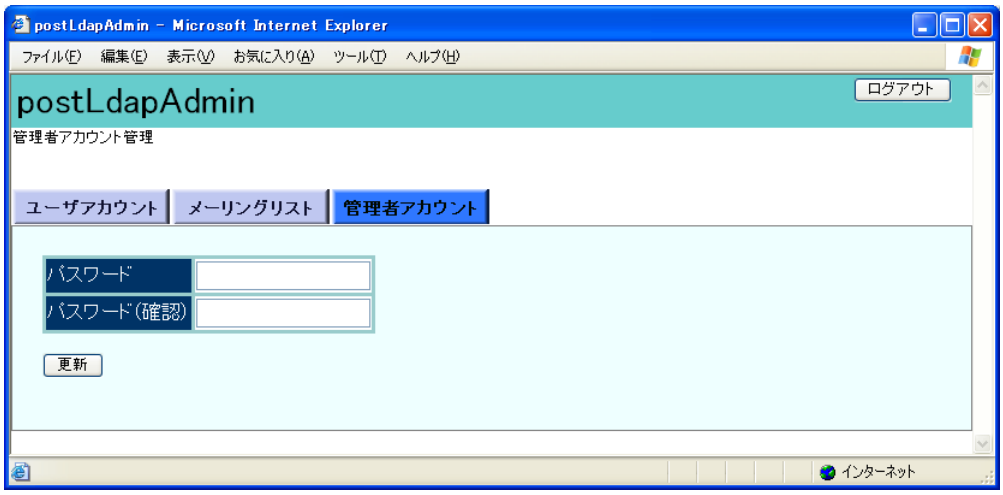
- [参照]ボタンをクリックし、一括追加するメールアドレスを記述したファイルをアップロードします。
- [一括追加]ボタンをクリックします。

一括追加で指定するファイルには、次の例のように一行に 1 つのメールアドレスを記述してください。

一括追加ファイルの例

```
add01@test.designet.jp
add02@test.designet.jp
   :
```

4.2.1.5 管理者アカウント管理画面

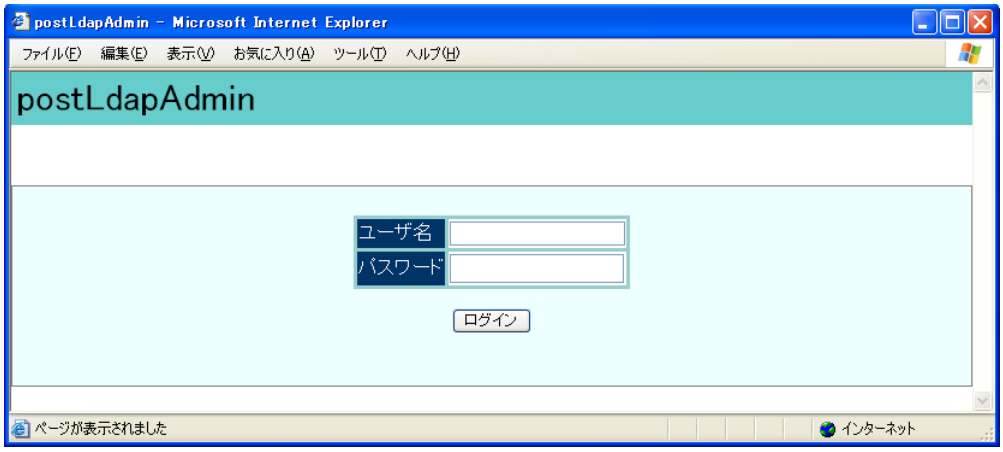


[管理者パスワードの変更]

　新しい管理者パスワードを入力し、[更新]ボタンをクリックします。

4.2.2 ユーザ用インタフェース

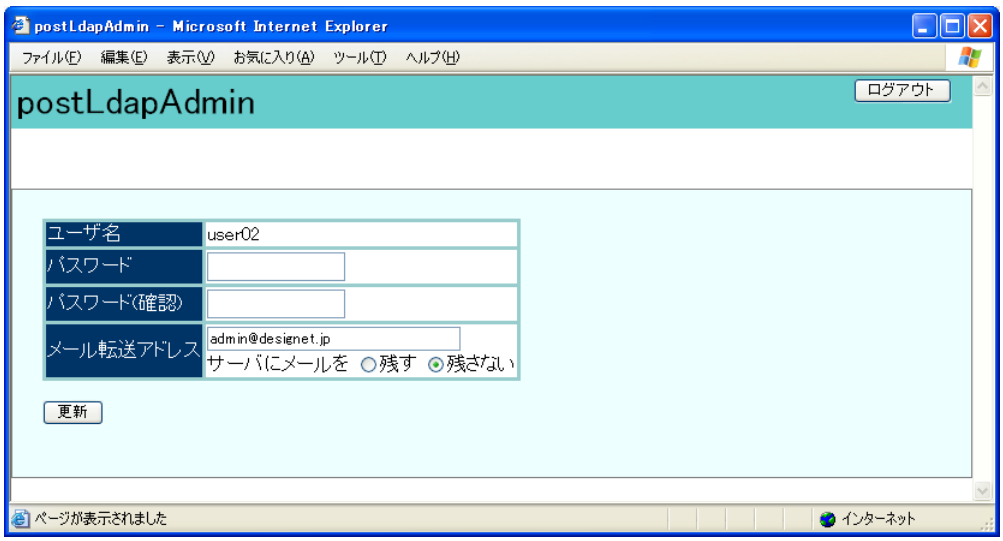
4.2.2.1 ユーザログイン画面



[ログイン]

　ユーザ名、パスワードを入力し、[ログイン]ボタンをクリックします。

4.2.2.2 ユーザ編集画面



[仮想ユーザの編集]

次の編集する項目を入力し、[更新]ボタンをクリックします。

- パスワード/パスワード（確認）
- メール転送アドレス

メール転送アドレスを編集した場合は、サーバにメールを残すか残さないかを選択します。

5. 設定詳細（web.conf）

web.conf には、表 5.1 の項目を設定します。

表 5.1: web.conf

項目	解説
LdapServer	LDAP サーバを指定します。
LdapPort	LDAP サーバのポート番号を指定します。指定しない場合は 389 となります。
LdapBindDn	LDAP にバインドする DN を指定します。
LdapBindPw	LDAP にバインドする DN のパスワードを指定します。
LdapBaseDn	LDAP サーバの検索を開始するベース DN を指定します。検索は、ここで指定した DN の配下に対して行われます。
ReferrerUrl	リファラ URL を指定します。アクセスする URL とリファラ URL を前方一致で比較し、一致しない場合はセッションエラーとなります。
DiskQuotaDefault	デフォルトのメール最大容量を指定します。
BaseMailDir	メール保管ディレクトリのベースディレクトリを指定します。ここで指定したディレクトリ配下にメールアカウント名のディレクトリが作成され、各ユーザへのメールが配送されます。
LinePerPage	ユーザ検索画面で 1 ページに表示させる検索結果件数を指定します。指定しない場合は 10 件となります。
AdminName	管理者名を指定します。
AdminPasswd	MD5 エンコードした管理者パスワードを指定します。
LogFile	postLdapAdmin のログの出力先ファイルを指定します。
MailDelcommand	アカウント削除時に実行するメールディレクトリ削除コマンドを指定します。ここで指定したコマンドには、引数として削除するアカウントのメールディレクトリのパスが渡されます。
LdapUserSuffix	LDAP のメールアカウントを管理する階層を指定します。
LdapListSuffix	LDAP のメーリングリストを管理する階層を指定します。
LdapScope	LDAP の検索スコープを指定します。sub（ベース DN で指定した LDAP ディレクトリ配下全体を検索）、base（ベース DN で指定した LDAP エントリだけを検索）、one（ベース DN で指定した LDAP エントリの直下のエントリのみを検索）のいずれかを指定します。
LdapFilter	LDAP の検索フィルタを指定します。ここで「%u」を指定した場合には uid、「%d」を指定した場合には WWW サーバの設定で指定した環境変数 DOMAIN の値、「%s」を指定した場合にはメールアドレスが補完されます。ここで設定された値と検索画面などで入力された値から検索フィルタが作成されます。
LdapMlFilter	メーリングリスト用の LDAP の検索フィルタを指定します。LdapFilter と同様に、「%u」には uid が、「%d」には WWW サーバの設定で指定した環境変数 DOMAIN の値、「%s」にはメールアドレスが補完されます。ここで設定された値と検索画面などで入力された値から検索フィルタが作成されます。
LdapObjectClass	ユーザ追加時に postLdapAdmin のオブジェクトクラスと一緒に使用する構造型のオブジェクトクラスを指定します。
DisplayUser	ユーザアカウント一覧画面で「ユーザ名」として表示する値の属性を指定します。
DisplayMl	メーリングリスト一覧画面でメーリングリストアドレスとして表示する値の属性を指定し

	ます。

Appendix

Appendix A. LDAP サーバの設定例

LDAP サーバは、次の例にしたがって設定を行ってください。

- LDAP サーバの基本設定
- LDAP の基本構造の作成

LDAP サーバの設定については、次のサイトを参考にしてください。

OpenLDAP ホームページ
http://www.openldap.org/

A.1 LDAP サーバの基本設定

LDAP サーバの設定は、slapd.conf ファイルで行います。環境に合わせて設定を行ってください。少なくとも、suffix、rootdn、rootpw の項目は設定します。

slapd.conf の設定例（コメント行を除く）

```
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/nis.schema
allow bind_v2
pidfile         /var/run/openldap/slapd.pid
argsfile        /var/run/openldap/slapd.args
database        bdb
suffix          "dc=designet,dc=jp"                                    ← 変更
rootdn          "cn=Manager,dc=designet,dc=jp"                         ← 変更
rootpw          {SSHA}IWKEmmIX7GqNGiQiVhjLMy0+7hVcYAHg ← 追加
directory       /var/lib/ldap
index objectClass                       eq,pres
index ou,cn,mail,surname,givenname      eq,pres,sub
index uidNumber,gidNumber,loginShell    eq,pres
index uid,memberUid                     eq,pres,sub
index nisMapName,nisMapEntry            eq,pres,sub
```

A.2 LDAP の基本構造の作成

LDAP の基本構造を準備します。LDAP の基本構造は、2.2 で紹介した LDAP の基本構造の例のように作成することをお勧めします。OpenLDAP の場合は、LDAP の基本構造を作成するために次のようなファイル（init.ldif）を用意します。

LDAP の初期設定例（init.ldif）

```
# designet.jp                                          ← トップの DN のデータ
dn: dc=designet,dc=jp
objectClass: organization
objectClass: dcObject
o: DesigNET, INC.
dc: designet

# test.designet.jp                                     ← 管理する仮想ドメインの階層
dn: dc=test,dc=designet,dc=jp
dc: test
objectClass: domain
```

```
objectClass: top

# User, test.designet.jp                    ← メールアカウントを管理する階層
dn: ou=User,dc=test,dc=designet,dc=jp
objectClass: organizationalUnit
objectClass: top
ou: User

# List, test.designet.jp                    ← メーリングリストを管理する階層
dn: ou=List,dc=test,dc=designet,dc=jp
objectClass: organizationalUnit
objectClass: top
ou: List
```

LDIF ファイルが用意できましたら、次のように ldapadd コマンドで登録します。

```
$ ldapadd -x -D "cn=Manager,dc=designet,dc=jp" -f init.ldif -W
```

Appendix B. メールサーバの設定例

本章では、MTA のひとつとして Postfix の設定方法を紹介します。postLdapAdmin では、仮想ユーザごとのクォータ値を管理することができます。仮想ユーザごとのクォータ機能は、VDA パッチを適用した Postfix をインストールすることで利用することができます。VDA パッチを適用した Postfix のインストール、設定方法は、以下のサイトを参考にして行ってください。

Postfix ホームページ
http://www.postfix.org/

Postfix VDA
http://vda.sourceforge.net/

本書の執筆時点での最新バージョンは、2.4 版のパッチレベル 5 です。

LDAP による仮想ユーザ管理

Postfix で LDAP を利用した仮想ユーザ管理を行うには、Postfix 検索テーブルで LDAP を参照するように設定する必要があります。

次の設定例にしたがって、以下の項目の設定を行ってください。

- Postfix 設定ファイルの準備
  - 仮想メールボックスに配送するドメインの設定
  - 仮想別名テーブルの設定
  - 仮想メールボックスの配送先の設定
  - 仮想メールボックス容量の設定
  - メール保管アカウントの設定

B.1 Postfix 設定ファイルの準備

main.cf に次の項目を設定します。

main.cf の設定例（追加行）

```
# 仮想メールボックスに配送するドメインの設定
virtual_mailbox_domains = test.designet.jp

# 仮想メールボックスの配送先の設定
virtual_mailbox_base = /
virtual_mailbox_maps = ldap:/etc/postfix/ldap-account.cf

# 仮想別名テーブルの設定
virtual_alias_maps = ldap:/etc/postfix/ldap-forward.cf

# 仮想メールボックス容量の設定（クォータ制御機能を利用するとき）
virtual_mailbox_limit = 0
virtual_mailbox_limit_maps = ldap:/etc/postfix/ldap-quota.cf
virtual_mailbox_limit_override = yes

# メール保管アカウントの設定
virtual_uid_maps = static:400
```

```
virtual_gid_maps = static:400
```

B.2 Postfix 検索テーブルの LDAP 設定ファイルの準備

次に、「virtual_mailbox_maps」「virtual_alias_maps」「virtual_mailbox_limit_maps」で指定した Postfix 検索テーブルの LDAP 設定ファイルに LDAP の検索条件を設定します。

ldap-account.cf の設定例

```
server_host = 127.0.0.1
server_port = 389
bind = yes
bind_dn = cn=Manager,dc=designet,dc=jp
bind_pw = secret
scope = sub
search_base = dc=designet,dc=jp
query_filter = (|(mail=%s)(mailAlias=%s))
result_attribute = mailDirectory
result_format = %s/Maildir/
```

ldap-forward.cf の設定例

```
server_host = 127.0.0.1
server_port = 389
bind = yes
bind_dn = cn=Manager,dc=designet,dc=jp
bind_pw = secret
scope = sub
search_base = dc=designet,dc=jp
query_filter = (|(mail=%s)(mailAlias=%s))
result_attribute = mailForwardingAddr
```

ldap-quota.cf の設定例（クォータ機能利用時）

```
server_host = 127.0.0.1
server_port = 389
bind = yes
bind_dn = cn=Manager,dc=designet,dc=jp
bind_pw = secret
scope = sub
search_base = dc= designet,dc=jp
query_filter = (|(mail=%s)(mailAlias=%s))
result_attribute = quotaSize
```

Postfix 検索テーブルの LDAP 設定ファイルの設定項目は、表 B.1 のとおりです。

表 B.1: Postfix 検索テーブルの LDAP 設定ファイル

項目	解説
server_host	LDAP サーバのホスト名または IP アドレスを設定します。
server_port	LDAP サーバのポート番号を設定します。
timeout	LDAP 検索がタイムアウトする秒数を設定します。
search_base	LDAP 検索のときに使用するベース DN を指定します。
query_filter	LDAP 検索で使用する検索フィルタを設定します。

result_attribute	LDAP 検索の結果として取得すべき属性を指定します。複数の属性が必要な場合には、「,（コンマ）」で区切って並べることができます。
result_format	Postfix 検索テーブルの結果として返す結果を、指定した LDAP 検索の結果から作成する文字列を指定します。
scope	LDAP 検索を行う場合の検索範囲を指定します。 sub ベース DN で指定した LDAP ディレクトリ配下全体を検索します。 base ベース DN で指定した LDAP エントリだけを検索します。 one ベース DN で指定した LDAP エントリのサブエントリ（直下のエントリ）のみを検索します。
bind	LDAP サーバへの接続で、バインド処理を行うかどうかを指定します。no を指定すると、anonymous（匿名）モードで接続を行います。
bind_dn	LDAP サーバにバインドする DN を指定します。
bind_pw	bind_dn に対応する DN に対応するパスワードを指定します。

Appendix.C POP/IMAP サーバの設定例

メールソフトウェアからメールを読むために、POP/IMAP サーバの設定を行ってください。本書では、POP/IMAP サーバとして courier-imap を利用する場合を例として解説をします。courier-imap の設定は次のサイトを参考にしてください。

Courier-IMAP
http://www.courier-mta.org/imap/

Courier-Authlib
http://www.courier-mta.org/authlib/

LDAP による仮想ユーザ管理

courier-imap で LDAP 仮想ユーザ管理を行うには、authdaemond の LDAP 用の設定ファイル authldaprc を準備してください。

authldaprc の設定例

```
LDAP_URI                 ldap://127.0.0.1
LDAP_PROTOCOL_VERSION    3
LDAP_BASEDN              dc=designet,dc=jp
LDAP_BINDDN              cn=Manager,dc=designet,dc=jp
LDAP_BINDPW              secret
LDAP_TIMEOUT             5
LDAP_AUTHBIND            1
LDAP_MAIL                uid
LDAP_FILTER              (objectClass=postLdapAdmin)
LDAP_GLOB_UID            vmail
LDAP_GLOB_GID            vmail
LDAP_HOMEDIR             mailDirectory
LDAP_CRYPTPW             userPassword
LDAP_TLS                 0
```

authldaprc の設定項目は表 C.1 のとおりです。

表 C.1: authldaprc

項目	解説
LDAP_URI	LDAP サーバのアドレスを URI の形式で指定します。
LDAP_PROTOCOL_VERSION	LDAP サーバへ接続する LDAP のバージョンを指定します。OpenLdap の場合には 3 を指定します。
LDAP_BASEDN	LDAP 検索を行うときに使用するベース DN を指定します。
LDAP_BINDDN	LDAP サーバへの接続に使う DN を指定します。
LDAP_BINDPW	LDAP_BINDDN で設定した DN に対応するパスワードを指定します。
LDAP_TIMEOUT	LDAP 処理のタイムアウト時間を設定します。
LDAP_AUTHBIND	ユーザ認証の方法を指定します。0（BIND しない）を指定すると、LDAP サーバからパスワードを取得して authdaemond 側でパスワードを検証します。 1（BIND する）を指定すると、該当ユーザの DN で LDAP へ接続し、LDAP サーバ側の認証を利用します。

LDAP_MAIL	LDAP 検索を行ったときに、POP3 ログインで指定したユーザと比較する属性を設定します。POP3 のログインで、メールアドレスを入力する場合には mail 属性を指定し、ユーザ名を入力する場合には uid を指定します。
LDAP_FILTER	LDAP 検索を行うときに、検索対象とするエントリを示す検索フィルタを設定します。authdaemond は、ここで指定した検索フィルタと、LDAP_MAIL で設定した属性から作成したフィルタを組み合わせて検索を行います。
LDAP_GLOB_UID	ユーザの UID をサーバ全体で使用する場合に指定します。Postfix の設定ファイルで指定した virtual_uid_maps の値にしたがって設定しておく必要があります。
LDAP_GLOB_GID	ユーザの GID をサーバ全体で使用する場合に指定します。Postfix の設定ファイルで指定した virtual_gid_maps の値にしたがって設定しておく必要があります。
LDAP_HOMEDIR	メール保存ディレクトリ（ホームディレクトリ）の構成要素として取得すべき属性名を設定します。本書では、mailDirectory 属性値でディレクトリを設定していましたので、「mailDirectory」を設定します。
LDAP_CRYPTPW	LDAP のパスワードが設定されている属性名を指定します。
LDAP_CREARPW	LDAP 中に平文でパスワードが保管されている場合に属性名を指定します。必ず LDAP_CRYPTPW か LDAP_CREARPW のどちらかを設定しなければいけません。
LDAP_TLS	LDAP サーバへ接続するときに、STARTTLS を利用した TLS による暗号化を行うかどうかを設定します。

Appendix.D 既に LDAP 環境がある場合

すでに LDAP の環境が構築されている場合は、LDAP のユーザのエントリに、次の点に注意して設定を行ってください。

- オブジェクトクラス postLdapAdmin が必要であること
- uid、mail 属性が必要であること
- メール保管ディレクトリのパスを設定すること

postLdapAdmin オブジェクトクラス

postLdapAdmin の Web インタフェースでは、オブジェクトクラス postLdapAdmin が設定されたエントリだけを編集することができます。postLdapAdmin の Web インタフェースを利用する前に、ユーザのエントリに postLdapAdmin オブジェクトクラスを付加してください。

uid 属性・mail 属性

postLdapAdmin では、ユーザ名に uid 属性値、メールアドレスに mail 属性値を使用しています。postLdapAdmin の Web インタフェースを利用する前に、ユーザのエントリに uid 属性・mail 属性が設定されていることを確認してください。

メール保管ディレクトリのパスの設定

postLdapAdmin では、LDAP のユーザアカウントのデータからメール保管ディレクトリのパスを取得します。postLdapAdmin の Web インタフェースを利用する前に、ユーザのエントリにメール保管ディレクトリのパスを属性値として持つ属性を付加してください。

【参考文献】

- 『Linux で作る完全メールシステム構築ガイド』
  （2007 年 2 月 5 日第 1 版第 1 刷　デージーネット著）
- OpenLDAP ホームページ
  http://www.openldap.org/
- Postfix ホームページ
  http://www.postfix.org/
- Postfix VDA
  http://vda.sourceforge.net/
- Apache Software Foundation
  http://www.apache.org/