

postLDAPadmin

平成 27 年 10 月 22 日

目次

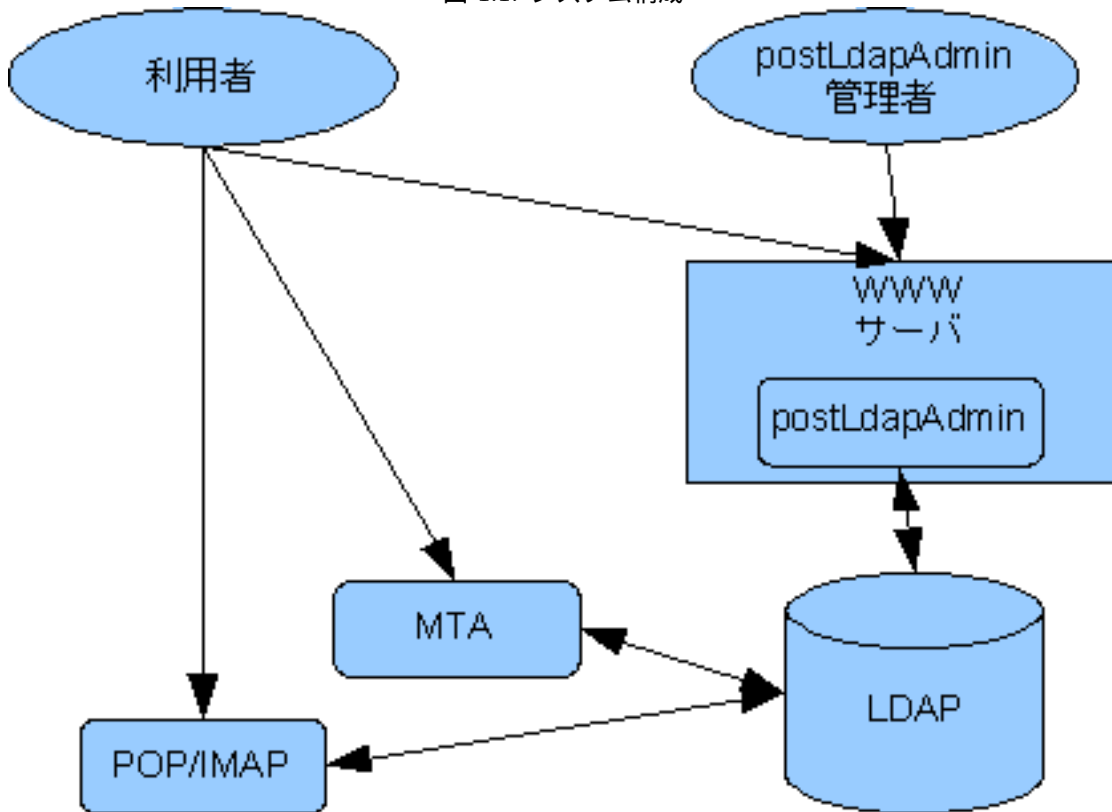
第 1 章	postLDAPAdmin とは	4
1.1	メールシステムと LDAP の連携	4
1.2	メールシステムの仮想ユーザ管理を LDAP で行うことのメリット	5
1.3	postLDAPAdmin を利用するメリット	5
1.4	postLDAPAdmin で管理する LDAP データ	5
第 2 章	計画	6
2.1	事前に用意しておくソフトウェア	6
2.2	決めておかななくてはならないこと	6
2.3	設定概要	6
第 3 章	インストール	10
3.1	postLDAPAdmin の入手と展開	10
3.2	デザインテンプレートについて	11
3.3	LDAP サーバの設定	24
3.3.1	postLDAPAdmin で管理する LDAP データ	24
3.3.2	スキーマファイルの読み込み	24
3.3.3	LDAP データベースの索引	25
3.4	postLDAPAdmin の設定	25
3.4.1	設定ファイルの設置	25
3.4.2	メール保管アカウント、ディレクトリの準備	29
3.4.3	スクリプトの設定	30
3.5	Web サーバの設定	30
3.5.1	ディレクトリアクセス制御設定	31
3.5.2	環境変数の設定	31
3.5.3	DirectoryIndex の設定	31
3.5.4	php の include_path の設定	32
3.5.5	エイリアス設定	32
3.5.6	複数の仮想ドメインを管理したいとき	32
第 4 章	使い方	35
4.1	基本的な機能	35
4.2	postLDAPAdmin の Web インタフェースの画面構成	35
4.2.1	postLDAPAdmin 管理者用インタフェース	37

	3
4.2.2 ユーザ用インタフェース	48
4.3 メール転送詳細設定の利用	50
4.3.1 メール転送詳細設定で実現出来る事	50
4.3.2 メール転送詳細設定への切り替え	50
4.3.3 必要な動作環境	50
4.3.4 メール転送詳細設定利用時の画面構成図	51
4.3.5 管理者側のメール転送詳細設定	52
4.3.6 ユーザ側のメール転送詳細設定	59
第 5 章 設定詳細 (web.conf)	62
付 録 A Appendix	65
A.1 LDAP サーバの設定例	65
A.1.1 LDAP サーバの基本設定	65
A.1.2 LDAP の基本構造の作成	66
A.2 メールサーバの設定例	67
A.2.1 LDAP による仮想ユーザ管理	67
A.3 POP/IMAP サーバの設定例	69
A.3.1 postLDAPAdmin の web.conf の設定	70
A.3.2 LDAP による仮想ユーザ管理	70
A.4 既に LDAP 環境がある場合	70
A.4.1 postLDAPAdmin オブジェクトクラス	70
A.4.2 uid 属性・mail 属性	70
A.4.3 メール保管ディレクトリのパスの設定	72
A.5 dovecot-sieve の設定例	72
A.5.1 dovecot を利用したローカル配送の設定例	72
A.6 参考文献	74

第1章 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 では、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 1
			メールエイリアス 1
			メール転送アドレス 1
		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 1
			メールエイリアス 1
		メール転送の編集	メール転送アドレス 1
		転送ルール 2	
		仮想ユーザの削除	
	仮想ユーザの検索		
	メーリングリスト機能	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 1		
	仮想ユーザのメールフィルタオーダー、メールフィルタアークティクル管理 2		

1 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 転送ルールは web.conf の ForwardConf が on(=1) に設定されているときのみ登録されます。その場合、メール転送アドレスは登録されません。

第2章 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
- PHP5.3 以上 (LDAP、mbstring、openssl 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。

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。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。

表 2.1: 決めておかな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.designet.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.designet.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	/var/log/postLDAPAdmin.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、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。	図 2.1: LDAP の基本構造の例
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

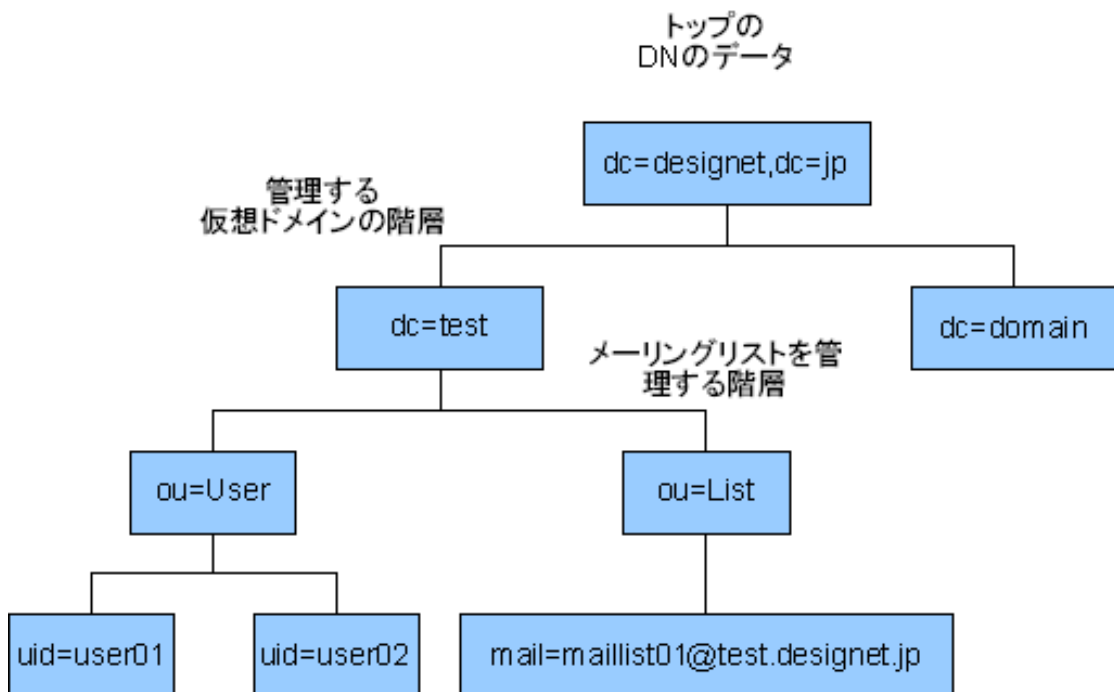
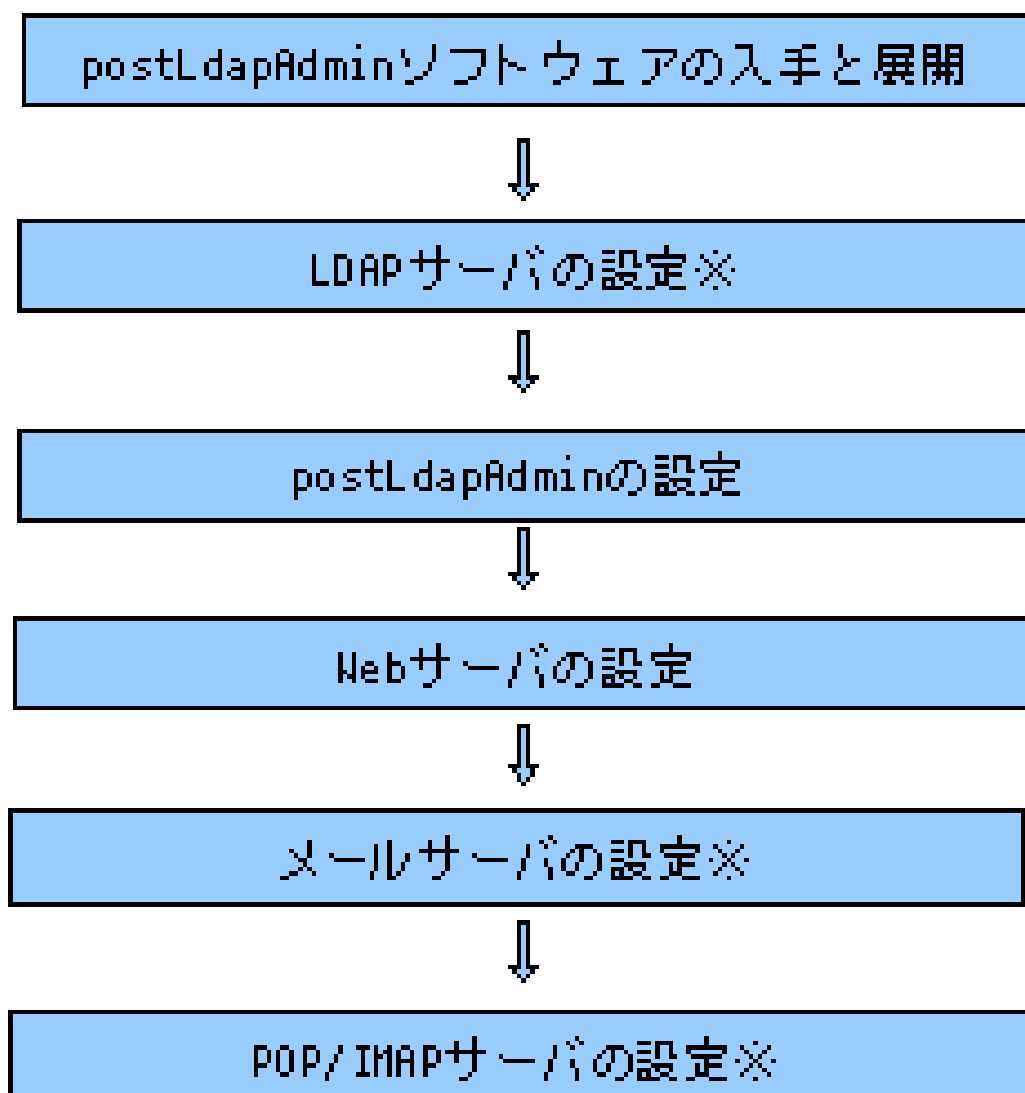


図 2.2: postLDAPAdmin 導入手順



第3章 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://osdn.jp/projects/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。

postLDAPAdmin のインストール

```
# tar xzf postLDAPAdmin_frame-VERSION.tar.gz -C /usr/local
# tar xzf postLDAPAdmin_admin-VERSION.tar.gz -C /usr/local/postldapadmin/htdocs/admin
# tar xzf postLDAPAdmin_user-VERSION.tar.gz -C /usr/local/postldapadmin/htdocs
# tar xzf postLDAPAdmin_lib-VERSION.tar.gz -C /usr/local/postldapadmin/lib
```

postLDAPAdmin.schema と postLDAPAdmin.ldif の配置

```
# cd /usr/local/postldapadmin/
# mv htdocs/admin/postldapadmin/postLDAPAdmin.schema ./
# mv htdocs/admin/postldapadmin/postLDAPAdmin.ldif ./
```

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
<code>/usr/local/postldapadmin/htdocs/admin/postldapadmin</code>	管理者用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
<code>/usr/local/postldapadmin/htdocs/user</code>	ユーザ用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
<code>/usr/local/postldapadmin/lib</code>	ライブラリを格納するディレクトリ
<code>/usr/local/postldapadmin/etc</code>	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
<code>/usr/local/postldapadmin/tmpl</code>	テンプレートファイルを格納するディレクトリ
<code>/usr/local/postldapadmin/postLDAPAdmin.schema</code>	LDAP 用スキーマファイル
<code>/usr/local/postldapadmin/postLDAPAdmin.ldif</code>	LDAP 用スキーマファイル (LDIF 形式)

3.2 デザインテンプレートについて

postLDAPadmin は、テンプレートを読み込んで特定の文字列（タグ）を置換して表示します。そのため、テンプレートファイル名やタグ情報を正しく設定すれば好みのデザインテンプレートを使用することができます。

各画面のファイル名とタグ情報は以下の通りです。

[展開ディレクトリ] /postldapadmin/tmpl/

表 3.2: テンプレートファイル名とタグ一覧 (管理者用インターフェース)

画面名	テンプレート名	タグ名	説明
ログイン画面	admin_login.tpl	<<TITLE>>	タイトル
		<<JAVASCRIPT>>	JavaScript
		<<MESSAGE>>	メッセージ
ユーザアカウント管理画面	admin_user_menu.tpl	<<TITLE>>	タイトル
		<<JAVASCRIPT>>	JavaScript
		<<MESSAGE>>	メッセージ
		<<SK>>	セッションキー
		<<TOPIC>>	トピック
		<<TAB>>	タブ
ユーザアカウント検索画面	admin_user_search.tpl	<<TITLE>>	タイトル
		<<JAVASCRIPT>>	JavaScript
		<<MESSAGE>>	メッセージ
		<<SK>>	セッションキー
		<<TOPIC>>	トピック
		<<TAB>>	タブ
		<<SEARCH_UID>>	検索条件: ユーザ名
		<<INCLUDE_ON>>	検索条件: を含む
		<<MATCH_ON>>	検索条件: と一致する
		<<NUM>>	全件数
		<<PRE>>	前ページリンク
		<<NEXT>>	次ページリンク
		<<UID>>	ユーザ名
		<<ALIAS>>	メールエイリアス
		<<TRANS>>	メール転送アドレス
		<<QUOTA>>	メールボックス容量
		<<MOD>>	編集リンク
		<<HIDDEN>>	データ受け渡し用 POST データ
		<<STARTLOOP>>	ループ処理開始
		<<ENDLOOP>>	ループ処理終了
<<FORWARD_START>>	コメントアウト開始		
<<FORWARD_END>>	コメントアウト終了		
<<FORWARD>>	転送設定リンク		
ユーザアカウント編集画面	admin_user_mod.tpl	<<TITLE>>	タイトル
		<<JAVASCRIPT>>	JavaScript
		<<MESSAGE>>	メッセージ

		<<SK>>	セッションキー
		<<TOPIC>>	トピック
		<<TAB>>	タブ
		<<UID>>	ユーザ名
		<<QUOTA>>	メールボックス容量
		<<QUOTASIZE>>	メールボックス容量桁数
		<<QUOTAUNIT>>	メールボックス容量単位
		<<ALIAS>>	メールエイリアス
		<<TRANS>>	メール転送アドレス
		<<SAVEON>>	サーバにメールを残す
		<<SAVEOFF>>	サーバにメールを残さない
		<<HIDDEN>>	データ受け渡し用 POST データ
		<<FORWARD_START>>	コメントアウト開始
		<<FORWARD_END>>	コメントアウト終了
ユーザメール転送設定画面	admin_user_mod.tpl	<<TITLE>>	タイトル
		<<JAVASCRIPT>>	JavaScript
		<<MESSAGE>>	メッセージ
		<<SK>>	セッションキー
		<<TOPIC>>	トピック
		<<TAB>>	タブ
		<<STARTLOOP>>	ループ処理開始
		<<ENDLOOP>>	ループ処理終了
		<<FILTER_ID>>	フィルタ ID
		<<ALL_FORWARD>>	全て転送
		<<DETAIL_FORWARD>>	詳細設定
		<<FORWARD_CHECK>>	送信者チェックボックス
		<<FORWARD_TEXT>>	送信者テキストボックス
		<<FORWARD_MATCH>>	送信者が一致する
		<<FORWARD_INCLUDE>>	送信者を含む
		<<FORWARD_NOT_INC>>	送信者を含まない
		<<FORWARD_EMPTY>>	送信者が空である
		<<SUBJECT_CHECK>>	件名チェックボックス
		<<SUBJECT_TEXT>>	件名テキストボックス
		<<SUBJECT_MATCH>>	件名が一致する
		<<SUBJECT_INCLUDE>>	件名を含む
		<<SUBJECT_NOT_INC>>	件名を含まない
		<<SUBJECT_EMPTY>>	件名が空である
		<<RECIPT_CHECK>>	宛先チェックボックス
		<<RECIPT_TEXT>>	宛先テキストボックス
		<<RECIPT_MATCH>>	宛先が一致する
		<<RECIPT_INCLUDE>>	宛先を含む
		<<RECIPT_NOT_INC>>	宛先を含まない
		<<RECIPT_EMPTY>>	宛先が空である
		<<TRANSFER_ADDR>>	転送先アドレス
		<<MAIL_LEAVE>>	メールを残す
		<<MAIL_DEL>>	メールを残さない
		<<HIDDEN>>	データ受け渡し用 POST データ
ユーザアカウント追加画面	admin_forward_mod.tpl	<<TITLE>>	タイトル

		<<JAVASCRIPT>>	JavaScript
		<<MESSAGE>>	メッセージ
		<<SK>>	セッションキー
		<<TOPIC>>	トピック
		<<TAB>>	タブ
		<<UID>>	ユーザ名
		<<QUOTA>>	メールボックス容量
		<<QUOTASIZE>>	メールボックス容量桁数
		<<QUOTAUNIT>>	メールボックス容量単位
		<<ALIAS>>	メールエイリアス
		<<TRANS>>	メール転送アドレス
		<<SAVEON>>	サーバにメールを残す
		<<SAVEOFF>>	サーバにメールを残さない
		<<FORWARD_START>>	コメントアウト開始
		<<FORWARD_END>>	コメントアウト終了
CSV 一括登録画面	admin_user.csv.tpl	<<TITLE>>	タイトル
		<<JAVASCRIPT>>	JavaScript
		<<MESSAGE>>	メッセージ
		<<SK>>	セッションキー
		<<TOPIC>>	トピック
		<<TAB>>	タブ
メールリスト管理画面	admin_ml.menu.tpl	<<TITLE>>	タイトル
		<<JAVASCRIPT>>	JavaScript
		<<MESSAGE>>	メッセージ
		<<SK>>	セッションキー
		<<TOPIC>>	トピック
		<<TAB>>	タブ
		<<MENU>>	メニュー
メールリスト編集画面	admin_ml.mod.tpl	<<TITLE>>	タイトル
		<<JAVASCRIPT>>	JavaScript
		<<MESSAGE>>	メッセージ
		<<SK>>	セッションキー
		<<TOPIC>>	トピック
		<<TAB>>	タブ
		<<MLADDRS>>	メールリスト一覧
		<<NEWML>>	新規登録メールアドレス
		<<MLDOMAIN>>	ドメイン
メールアドレス管理画面	admin_ml.mod_mod.tpl	<<TITLE>>	タイトル
		<<JAVASCRIPT>>	JavaScript
		<<MESSAGE>>	メッセージ
		<<SK>>	セッションキー
		<<TOPIC>>	トピック
		<<TAB>>	タブ
		<<MLADDR>>	メールリストアドレス
		<<MAILADDRS>>	メールアドレス一覧
		<<NEWADDR>>	新規登録メールアドレス
		<<HIDDEN>>	データ受け渡し用 POST データ

管理者アカウント管理画面	admin_adminpass_mod.tpl	<<TITLE>>	タイトル
		<<JAVASCRIPT>>	JavaScript
		<<MESSAGE>>	メッセージ
		<<SK>>	セッションキー
		<<TOPIC>>	トピック
		<<TAB>>	タブ

表 3.3: テンプレートファイル名とタグ一覧 (ユーザインターフェース)

画面名	テンプレート名	タグ名	説明
ログイン画面	user_login.tpl	<<TITLE>>	タイトル
		<<JAVASCRIPT>>	JavaScript
		<<MESSAGE>>	メッセージ
ユーザ編集画面	user_user_mod.tpl	<<TITLE>>	タイトル
		<<JAVASCRIPT>>	JavaScript
		<<MESSAGE>>	メッセージ
		<<SK>>	セッションキー
		<<TOPIC>>	トピック
		<<TAB>>	タブ
		<<UID>>	ユーザ名
		<<TRANSFERADDR>>	メール転送アドレス
		<<SAVEMAILENABLED>>	サーバにメールを残す
		<<SAVEMAILDISABLED>>	サーバにメールを残さない
		<<FORWARD_START>>	コメントアウト開始
		<<FORWARD_END>>	コメントアウト終了
ユーザメール転送設定画面	user_forward_mod.tpl	<<TITLE>>	タイトル
		<<JAVASCRIPT>>	JavaScript
		<<MESSAGE>>	メッセージ
		<<SK>>	セッションキー
		<<TOPIC>>	トピック
		<<TAB>>	タブ
		<<STARTLOOP>>	ループ処理開始
		<<ENDLOOP>>	ループ処理終了
		<<FILTER_ID>>	フィルタ ID
		<<ALL_FORWARD>>	全て転送
		<<DETAIL_FORWARD>>	詳細設定
		<<FORWARD_CHECK>>	送信者チェックボックス
		<<FORWARD_TEXT>>	送信者テキストボックス
		<<FORWARD_MATCH>>	送信者が一致する
		<<FORWARD_INCLUDE>>	送信者を含む
		<<FORWARD_NOT_INC>>	送信者を含まない
		<<FORWARD_EMPTY>>	送信者が空である
		<<SUBJECT_CHECK>>	件名チェックボックス
		<<SUBJECT_TEXT>>	件名テキストボックス
		<<SUBJECT_MATCH>>	件名が一致する
		<<SUBJECT_INCLUDE>>	件名を含む
		<<SUBJECT_NOT_INC>>	件名を含まない
		<<SUBJECT_EMPTY>>	件名が空である
		<<RECIPT_CHECK>>	宛先チェックボックス
		<<RECIPT_TEXT>>	宛先テキストボックス
		<<RECIPT_MATCH>>	宛先が一致する
		<<RECIPT_INCLUDE>>	宛先を含む
		<<RECIPT_NOT_INC>>	宛先を含まない
		<<RECIPT_EMPTY>>	宛先が空である
		<<TRANSFER_ADDR>>	転送先アドレス
		<<MAIL_LEAVE>>	メールを残す
		<<MAIL_DEL>>	メールを残さない

	<<HIDDEN>>	データ受け渡し用 POST データ
--	------------	----------------------

セレクトボックス・チェックボックスの属性として使われるタグは、選択された場合「selected」もしくは「checked」に置換されます。選択されない場合は、空の文字列に置換されます。

以下は、ユーザアカウント検索画面のタグ置換の例です。

テンプレートファイル例

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<meta http-equiv="Cache-Control" content="no-cache, must-revalidate">
<meta http-equiv="Pragma" content="no-cache">
<meta http-equiv="Content-Type" content="text/html; charset=EUC-JP">
<title><<TITLE>></title>
<<JAVASCRIPT>>
<link rel="stylesheet" type="text/css" href="../../postldapadmin.css">
</head>
<body topmargin="0" leftmargin="0">
<div class="title">
  <form method="post" action="../../logout.php">
    <<SK>>
    <input type="submit" value="" name="logout" class="logout_btn">
  </form>
</div>
<div class="topic"><<TOPIC>></div>
<div class="message"><<MESSAGE>></div>
<<TAB>>
<div class="frame">
  <form method="post" name="form_main" action="index.php">
    <b>ユーザの検索</b><br><br>
    <table class="normal">
      <tr>
        <td class="normal" style="text-align:right;">
          ユーザ名
        </td>
        <td class="normal">
          <input type="text" size="30" name="form_name" value="<<SEARCH_UID>>"
            maxlength="256">

          <select name="name_match">
            <option value="0" <<INCLUDE_ON>>>を含む</option>
            <option value="1" <<MATCH_ON>>>と一致する</option>
          </select>
        </td>
      </tr>
    </table> <br>
    <<SK>>
    <input type="submit" name="search" value="" class="search_btn">
    <input type="submit" name="csvdownload" value="" class="csv_btn">
    <<HIDDEN>>
  <br><br>

```



```
<table class="table">
  <tr>
    <td class="search_sum">[全 <<NUM>> 件]</td>
    <td colspan="5" class="search_tmp" style="border:1px solid #000000;">
      <table class="guide" align="right">
        <tr>
          <td class="search_prev"><<PRE>></td>
          <td class="search_next"><<NEXT>></td>
        </tr>
      </table>
    </td>
  </tr>
  <tr>
    <td class="search_name">ユーザ名</td>
    <td class="search_name">メールエイリアス</td>
    <td class="search_trans">メール転送アドレス</td>
    <td class="search_quota">メール容量</td>
    <td class="search_ref"></td>
  <<FORWARD_START>>
    <td class="search_quota">転送設定</td>
  <<FORWARD_END>>
  </tr>
  <<STARTLOOP>>
    <tr>
      <td class="value"><<UID>></td>
      <td class="value_alias"><<ALIAS>></td>
      <td class="value_trans"><<TRANS>></td>
      <td class="value_right"><<QUOTA>></td>
      <td class="value_center"><<MOD>></td>
    <<FORWARD_START>>
      <td class="value_forward"><<FORWARD>></td>
    <<FORWARD_END>>
  </tr>
  <<ENDLOOP>>
  </table>
</form>
</div>
<form method="post" name="common">
  <<SK>>
</form>
<div class="footer"></div>
</body>
</html>
```

図 3.1: ユーザ検索画面 (メール転送設定 OFF 時)

ユーザーアカウント管理 > ユーザーアカウント検索

ユーザーを更新しました。(testuser2)

ユーザーアカウント | メールリングリスト | 管理者アカウント

ユーザーの検索

ユーザー名 を含む

ユーザー名	メールエイリアス	メール転送アドレス	メール容量	操作
testuser2	testuser-2		100Kbytes	<input type="button" value="編集"/>
user01		user02@example.com	100Kbytes	<input type="button" value="編集"/>

図 3.2: ユーザ検索画面 (メール転送設定 ON 時)

postLDAPadmin ログアウト

ユーザアカウント管理 > ユーザアカウント検索

ユーザを更新しました。(testuser2)

ユーザアカウント メンバーリスト 管理者アカウント

ユーザの検索

ユーザ名 e を含む

検索 CSVダウンロード

[全 2 件]

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	転送設定
testuser2	testuser-2		100Kbytes	転送設定 16
user01		user02@example.com	100Kbytes	転送設定

postLDAPadmin

番号	タグ名	説明
1	<<TITLE>>	タイトル
2	<<TOPIC>>	トピック
3	<<MESSAGE>>	表示メッセージ
4	<<TAB>>	タブ
5	<<SEARCH_UID>>	検索条件：ユーザ名
6	<<INCLUDE_ON>>	検索条件：を含む
7	<<MATCH_ON>>	検索条件：と一致する
8	<<NUM>>	全件数
9	<<PRE>>	前ページリンク
10	<<NEXT>>	次ページリンク
11	<<UID>>	ユーザ名
12	<<ALIAS>>	メールエイリアス
13	<<TRANS>>	メール転送アドレス
14	<<QUOTA>>	メールボックス容量
15	<<MOD>>	編集リンク
16	<<FORWARD>>	転送設定リンク

上記のほかにも、以下のタグが存在します。これらは、画面上に出力されることはありませんが、置換されていることが HTML で確認できます。

タグ名	説明
<<JAVASCRIPT>>	JavaScript
<<SK>>	セッションキー
<<STARTLOOP>>	ループ処理開始
<<ENDLOOP>>	ループ処理終了
<<HIDDEN>>	データ受け渡し用 POST データ


```

        onClick="dgpSubmit('../.../postldapadmin/ml/')">
        </a></td>
    <td class="tab"><a href="#"
        onClick="dgpSubmit('../.../postldapadmin/adminpass/')">
        </a></td>
</tr>
</table>

<div class="frame">
    <form method="post" name="form_main" action="index.php">
    <b>ユーザの検索</b><br><br>
    <table class="normal">
    <tr>
    <td class="normal" style="text-align:right;">
    ユーザ名
    </td>
    <td class="normal">
    <input type="text" size="30" name="form_name" value="" maxlength="256">
    <select name="name_match">
    <option value="0" selected>を含む</option>
    <option value="1" >と一致する</option>
    </select>
    </td>
    </tr>
</table> <br>
    <input type="hidden"
        name="sk"
        value="ptiseLZlYPnZDYrrKlWZP+GuA+Nkpc/+kxr0r5PdejQ=">
    <input type="submit" name="search" value="" class="search_btn">
    <input type="submit" name="csvdownload" value="" class="csv_btn">
    <input type="hidden"
        name="filter"
        value="Ca0i4yoj4p0E/Im+InkJprmZDPKWpuJBvRcSs/
            Py7PcDPnIIb5L4WPRr1cKoHoeXuRBE+8GNDFZc7a7zkitkNCEDUROPaU7e">
    <input type="hidden" name="dn">
    <input type="hidden" name="page" value="0">

    <br><br>
    <table class="table">
    <tr>
    <td class="search_sum">[全 2 件]</td>
    <td colspan="5" class="search_tmp" style="border:1px solid #000000;">
    <table class="guide" align="right">
    <tr>
    <td class="search_prev"></td>
    <td class="search_next"></td>
    </tr>
    </table>
    </td>
    </tr>
</table>

```

```

        <td class="search_name">ユーザ名</td>
        <td class="search_name">メールエイリアス</td>
        <td class="search_trans">メール転送アドレス</td>
        <td class="search_quota">メール容量</td>
        <td class="search_ref"></td>
<!--
        <td class="search_quota">転送設定</td>
-->
</tr>

<tr>
    <td class="value">testuser2</td>
    <td class="value_alias">testuser-2</td>
    <td class="value_trans"></td>
    <td class="value_right">100Kbytes</td>
    <td class="value_center">
        <input type="button"
            class="list_mod_btn"
            onClick="allSubmit('mod.php',
                '0',
                'oJScoQ10MKA0qKAypwWNqTImqP5xMKAcM25yqP5dp
                PkiqG1Ip2IlyTEwCKEyp3DfMTZ9MTImnJqhMKDfMTZ9naN=',
                '')"
            title="ユーザ編集">
        </td>
    <td class="value_forward"><<FORWARD>></td>
</tr>

<tr>
    <td class="value">user01</td>
    <td class="value_alias"></td>
    <td class="value_trans">user02@example.com</td>
    <td class="value_right">100Kbytes</td>
    <td class="value_center">
        <input type="button"
            class="list_mod_btn"
            onClick="allSubmit('mod.php',
                '0',
                'oJScoQ11p2I1ZQSNqTImqP5xMKAcM25yqP5dpPkiq
                G1Ip2IlyTEwCKEyp3DfMTZ9MTImnJqhMKDfMTZ9naN=',
                '')"
            title="ユーザ編集">
        </td>
    <td class="value_forward"><<FORWARD>></td>
</tr>
</table>
</form>
</div>
<form method="post" name="common">
    <input type="hidden" name="sk" value="ptiseLZlYPnZDYrrKlWZP+GuA+Nkpc/+kxror5PdejQ=">
</form>
<div class="footer"></div>

```

```
</body>
</html>
```

3.3 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。

3.3.1 postLDAPAdmin で管理する LDAP データ

postLDAPAdmin で扱うエントリーには、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、postLDAPAdmin スキーマファイル (postLDAPAdmin.schema, postLDAPAdmin.ldif) が同梱されています。OpenLDAP の場合は、この postLDAPAdmin スキーマファイルを読み込むだけで postLDAPAdmin オブジェクトクラスを利用できるようになります。postLDAPAdmin スキーマファイルによって使用できる属性は表 3.4 のとおりです。

表 3.4: postLDAPAdmin スキーマ

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。
	mailFilterOrder	メールフィルタの順序、on/off を指定します。
	mailFilterArticle	メールフィルタの条件を指定します。

postLDAPAdmin スキーマファイルに収録されている属性、各属性名を任意に変更することはできません。

3.3.2 スキーマファイルの読み込み

OpenLDAP サーバの設定に、LDIF 形式のスキーマファイル postLDAPAdmin.ldif を読み込みます。postLDAPAdmin.ldif 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。

```
# ldapadd -Y EXTERNAL -H ldapi:/// -f /usr/local/postldapadmin/postLDAPAdmin.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=postldapadmin,cn=schema,cn=config"
```

3.3.3 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。すでに設定がある場合は不要です。

```
# ldapmodify -Y EXTERNAL -H ldapi:///<CR>
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
dn: olcDatabase={2}bdb,cn=config<CR>
changetype: modify<CR>
add: olcDbIndex<CR>
olcDbIndex: uid,mail eq,sub<CR>
-<CR>
<CR>
modifying entry "olcDatabase={2}bdb,cn=config"
<CTRL+D>
```

<CR>は Enter キーの入力、<CTRL+D>は CTRL キー + D キーの入力を示しています。

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。

3.4 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

3.4.1 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
# chown apache:apache test.designet.jp
```

web.conf

管理する仮想ドメイン名のディレクトリを作成したら、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 は、Web サーバの実行アカウントの権限である必要があります。次のコマンドで web.conf のパーミッションを確認してください。

```
# ls -l test.designet.jp
-rw-r--r-- 1 apache apache 655 10月 27 10:21 test.designet.jp/web.conf
```

Web サーバの実行アカウントの権限がない場合は、次のように設定してください。

```
# chown apache:apache test.designet.jp/web.conf
```

本書では、Web サーバの実行アカウントを「apache」として権限を付与しています。

web.conf の設定例

```
[global]
TitleName=postLDAPadmin
ReferrerUrl=http://test.designet.jp/
AdminName=admin
AdminPasswd=21232f297a57a5a743894a0e4a801fc3
LogFile=syslog
SyslogFacility=local1
SessionTimeout=900
MaxPasswordLength=8
MinPasswordLength=3
PasswordEncrypt=CRYPT

[postldapadmin]
LdapServer=127.0.0.1
LdapPort=389
LdapBindDn=cn=Manager,dc=designet,dc=jp
LdapBindPw=secret
LdapBaseDn=dc=test,dc=designet,dc=jp
DiskQuotaDefault=100
BaseMailDir=/home/mail/test.designet.jp
LinePerPage=5
MailDelcommand=sudo -u vmail deluser
LdapUserSuffix=ou=User
LdapListSuffix=ou=List
LdapScope=sub
LdapFilter=(uid=%u)
LdapMlFilter=(mail=*)
LdapObjectClass=account
DisplayUser=uid
DisplayMl=mail
QuotaUnit=KB
QuotaSize=3
LocalPartRFCCheck=0
ForwardConf=0
ForwardNum=3
ForwardFirstMatch=0
```

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行う、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。

QuotaUnit の項目には、クォータの単位を設定します。設定されたクォータ単位に応じて値の計算はしないため（入力された値がそのまま登録）、メールサーバソフトウェアのクォータ単位に合わせて設定する必要があります。

web.conf の設定項目については、第5章を参照してください。

tab.conf

次のディレクトリに tab.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/tab.conf.sample

以下のようにコピーしてください。

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

user_tab.conf

次のディレクトリに tab.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/user_tab.conf.sample

以下のようにコピーしてください。

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

web.conf の ForwardConf を on(=1) に設定する場合は user_tab.conf に以下を追記してください。

```
postldapadmin/forward:メール転送設定
```

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

コピーして以下のように設定してください。

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

admin.key の設定例

```
DxcMSHCM
```

3.4.2 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なら、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の作成
- postLDAPAdmin ログの設定

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 ログの設定

ログ出力には syslog を使用します。/etc/syslog.conf に以下を追記してください

```
local1.*          /var/log/postLDAPAdmin.log
```

syslog を再起動し、設定を反映させてください

```
# /etc/rc.d/init.d/syslog restart
```

以下のようにログファイルに権限を付加します。

```
# chown apache:apache /var/log/postLDAPAdmin.log
```

本書では、Web サーバの実行アカウントを「apache」として、ログファイルに apache アカウントの権限を付与しています。

3.4.3 スクリプトの設定

web.conf の ForwardConf を on(=1) に設定して利用する場合には、dovecot.sieve ファイルを作成するスクリプトの設定を行う必要があります。次の例にしたがって設定を行ってください。
実行スクリプトは以下のパスです。

```
[展開ディレクトリ]/postldapadmin/bin/make_sieve
```

sudo に実行登録を行いません。

以下は httpd が apache ユーザで実行されている場合の設定例です。

```
# visudo  
apache ALL=(ALL) NOPASSWD: [展開ディレクトリ]/postldapadmin/bin/make_sieve
```

3.5 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4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
- include_path の設定

3.5.1 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>
```

3.5.2 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 LOGNAME test.designet.jp
SetEnv DOMAIN test.designet.jp
```

LOGNAME

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。

3.5.3 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
```

3.5.4 php の include_path の設定

postLDAPadmin のインストール先の情報を得るために、php.ini の include_path の設定を行います。次は、postLDAPadmin を /usr/local/ に展開した例です。既に設定されている場合には、/usr/local/postldapadmin/ を追記してください。

```
include_path=".:usr/local/lib:usr/local/postldapadmin/"
```

3.5.5 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 3.3 のようなログイン画面が表示されます。

3.5.6 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 LOGNAME、DOMAIN の値を設定する必要があります。次の例にない、VirtualHost を作成し、VirtualHost ごとに環境変数 LOGNAME、DOMAIN を設定してください。

図 3.3: ログイン画面



httpd.conf の設定例

```
<VirtualHost *:80>
    ServerName test.designet.jp                管理する仮想ドメイン (1)

    SetEnv LOGNAME test.designet.jp
    SetEnv DOMAIN test.designet.jp

    Alias /postldapadmin/ "/usr/local/postldapadmin/htdocs/"
</VirtualHost>

<VirtualHost *:80>
    ServerName domain.designet.jp            管理する仮想ドメイン (2)

    SetEnv LOGNAME domain.designet.jp
    SetEnv DOMAIN domain.designet.jp

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

複数の仮想ドメインを管理している場合、VirtualHost 単位で include_path の設定も可能です。次は、httpd.conf の VirtualHost に設定した例です。

httpd.conf の設定例

```
<VirtualHost *:80>
  ServerName test.designet.jp

  SetEnv LOGNAME test.designet.jp
  SetEnv DOMAIN test.designet.jp

  Alias /postldapadmin/ "/usr/local/postldapadmin/htdocs/"

  php_value include_path ".:usr/local/lib:/usr/local/postldapadmin/"    include_path
の指定
</VirtualHost>
```

第4章 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
- メールユーザ管理をすべて LDAP だけで行うことができます。
- 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
 - * 仮想ユーザの一括登録
 - * 仮想ユーザの一括編集
 - * 仮想ユーザの一括削除
 - 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。

4.2.1 postLDAPAdmin 管理者用インタフェース

管理者ログイン画面

- ログイン
次の項目を指定し、[ログイン] ボタンをクリックしてください。
 - ユーザ名
 - パスワード

ユーザ名とパスワードには、web.conf で設定した「AdminName」と「AdminPasswd」の項目で設定した値を指定します。

ユーザアカウント管理画面

図 4.3: 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。

仮想ユーザの一括登録・編集・削除するには、[CSV一括処理] ボタン/リンクをクリックし、CSV一括処理画面に移動します。

ユーザアカウント検索画面

図 4.4: 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。

- 仮想ユーザの検索結果ダウンロード

次の項目を指定し、[CSV ダウンロード] 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 CSV ダウンロードを行うと、登録されている仮想ユーザの情報をすべてダウンロードファイルに表示します。

検索結果として、以下の項目が CSV 形式のファイルでダウンロードされます。ダウンロードされるファイルの名前は「userdata_ (Web サーバで設定した環境変数 DOMAIN の値) .csv」です。

```
username,quotasize,mailalias,mailforwardaddr,save
```

表 4.1: 各項目の説明

項目	説明
username	ユーザ名
quotasize	メールボックス容量
mailalias	メールエイリアス
mailforwardaddr	メール転送アドレス
save	サーバにメールを残す (0)/残さない (1)

値が設定されていない項目は空欄となります。

図 4.5: ユーザアカウント編集画面

ユーザアカウント管理 > ユーザアカウント検索

ユーザアカウント | メーリングリスト | 管理者アカウント

ユーザ名	testuser
パスワード	<input type="password"/>
パスワード(確認)	<input type="password"/>
メールボックス容量	100 Kbytes
メールエイリアス	<input type="text"/>
メール転送アドレス	サーバにメールを <input type="radio"/> 残す <input type="radio"/> 残さない

更新 | 削除 | キャンセル

postLDAPadmin

- 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。

ユーザアカウント追加画面

図 4.6: ユーザアカウント追加画面

ユーザアカウント管理 > ユーザアカウント追加

ユーザアカウント | メーリングリスト | 管理者アカウント

ユーザ名	<input type="text"/>
パスワード	<input type="password"/>
パスワード(確認)	<input type="password"/>
メールボックス容量	100 Kbytes
メールエイリアス	<input type="text"/>
メール転送アドレス	サーバにメールを <input type="radio"/> 残す <input type="radio"/> 残さない

登録 | キャンセル

postLDAPadmin

● 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。

CSV 一括登録画面

図 4.7: CSV 一括登録画面

- 仮想ユーザの一括登録・編集
動作タイプに登録を指定します。以下の形式の CSV ファイルを作成し、アップロードファイルに指定します。

```
username,password,quotasize,mailalias,mailforwardaddr,save
```

オプションを選択すると以下の動作を行います。

- 『既存のデータを上書き』を選択
指定された仮想ユーザが既に登録されている場合、仮想ユーザ情報の編集を行います。
- 『エラーの場合も処理を継続』を選択
エラーが発生した場合、処理を終了せず次の行の処理を行います。

LDAP への追加・変更を行わずファイルの形式チェックのみを行う場合は [ファイルチェック開始] ボタンをクリックします。

LDAP への追加・編集処理を行う場合は [更新] ボタンをクリックします。

[ファイルチェック開始] ボタン、[更新] ボタンを押すと、別ウィンドウに処理結果が表示されます。

- 仮想ユーザの一括削除
動作タイプに削除を指定し、一括削除するユーザ名を記載したファイルをアップロードファイルに指定します。

表 4.2: 各項目の説明

項目	説明	必須
username	ユーザ名	
passwd	パスワード	
quotasize	メールボックス容量	
mailalias	メールエイリアス	
mailforwardaddr	メール転送アドレス	
save	サーバにメールを残す (0)/残さない (1)	

メール転送アドレスが指定されている場合必須項目です。

CSV 一括登録ファイルの例

```
add01,passwd,100,alias01,fw01@test.designet.jp,0
add02,passwd,,,,
:
```

CSV 一括削除ファイルの例

```
del01
del02
:
```

オプションを選択すると以下の動作を行います。

- 『既存のデータを上書き』を選択
削除の場合、このオプションは無視されます。
- 『エラーの場合も処理を継続』を選択
エラーが発生した場合、処理を終了せず次の行の処理を行います。

LDAP への削除を行わずファイルの形式チェックのみを行う場合は [ファイルチェック開始] ボタンをクリックします。

LDAP への削除処理を行う場合は [更新] ボタンをクリックします。

[ファイルチェック開始] ボタン、[更新] ボタンを押すと、別ウィンドウに処理結果が表示されます。

● 注意事項

- アップロードファイルに指定されるファイルのサイズが php.ini の upload_max_filesize の設定値を超えるとファイルをアップロードすることができません。
この場合、upload_max_filesize の設定値を変更してください。
- CSV ファイルの処理時間が php.ini の max_execution_time の設定値を超えると、PHP の処理がタイムアウトします。この場合、max_execution_time の設定値を変更してください

メーリングリスト管理画面

図 4.8: メーリングリスト管理画面



メーリングリストを編集するために、[メーリングリスト編集] ボタン/リンクをクリックし、メーリングリスト編集画面に移動します。

メーリングリスト編集画面

図 4.9: メーリングリスト編集画面



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、メーリングリスト修正画面に移動します。
- 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、[新規追加] ボタンをクリックします。

図 4.10: メールアドレス管理画面

The screenshot shows the 'postLDAPadmin' web interface. At the top, there is a navigation bar with the site logo and a 'ログアウト' (Logout) button. Below the navigation bar, the breadcrumb path 'メーリングリスト管理 > メーリングリスト編集' is displayed. A secondary navigation bar contains three tabs: 'ユーザアカウント', 'メーリングリスト' (which is active), and '管理者アカウント'. The main content area is titled 'メーリングリストアドレス' and shows the current address 'ml@test.designet.jp'. Below this is a list of addresses, with 'user@test.designet.jp' selected. A '選択したメールアドレスを削除' (Delete selected email address) button is positioned to the right of the list. Below the list, there are three input fields: the first is empty, the second contains a file path, and the third is empty. To the right of the first input field is a '登録' (Register) button. To the right of the second input field are '参照...' (Reference...) and '一括追加' (Batch Add) buttons. A 'キャンセル' (Cancel) button is located at the bottom left of the main content area. The footer of the page features the 'postLDAPadmin' logo.

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  
:
```

管理者アカウント管理画面

図 4.11: 管理者アカウント管理画面


The screenshot shows the 'postLDAPadmin' web interface. At the top, there is a header with the 'postLDAPadmin' logo and a 'ログアウト' (Logout) button. Below the header, the text '管理者アカウント管理' (Administrator Account Management) is displayed. A navigation bar contains three tabs: 'ユーザアカウント' (User Accounts), 'メーリングリスト' (Mailing Lists), and '管理者アカウント' (Administrator Accounts), with the latter being the active tab. The main content area features a form for updating the administrator password, with fields for 'パスワード' (Password) and 'パスワード(確認)' (Password (Confirmation)), and an '更新' (Update) button. The 'postLDAPadmin' logo is also visible at the bottom right of the page.

- 管理者アカウント管理
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

ユーザログイン画面

図 4.12: ユーザログイン画面



The screenshot shows the user login interface for postLDAPadmin. At the top, there is a teal header with the postLDAPadmin logo and name. Below this, a light blue box contains the login form. The form has two input fields: 'ユーザ名' (Username) and 'パスワード' (Password). Below the password field is a 'ログイン' (Login) button. At the bottom of the page, there is another teal header with the postLDAPadmin name.

- 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。

ユーザ編集画面

図 4.13: ユーザ編集画面

ユーザアカウント編集

ユーザ名	user02
パスワード	
パスワード(確認)	
メール転送アドレス	サーバにメールを <input type="radio"/> 残す <input type="radio"/> 残さない

更新

postLDAPadmin

● 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。

4.3 メール転送詳細設定の利用

4.3.1 メール転送詳細設定で実現出来る事

メール転送詳細設定では、送信者や件名、宛先に含まれるキーワードと条件によって、それぞれ設定した転送先にメールを振り分ける事が可能になります。

4.3.2 メール転送詳細設定への切り替え

web.conf の ForwardConf を 1 に設定すると、メール転送詳細設定機能が ON に切り替わります。設定例は設定詳細 (web.conf) (62) を参照してください。

user_tab.conf を以下のように設定すると、ユーザ編集画面にメール転送詳細設定機能へのリンクタブが表示されます。

```
postldapadmin/user:ユーザアカウント編集  
postldapadmin/forward:メール転送設定
```

4.3.3 必要な動作環境

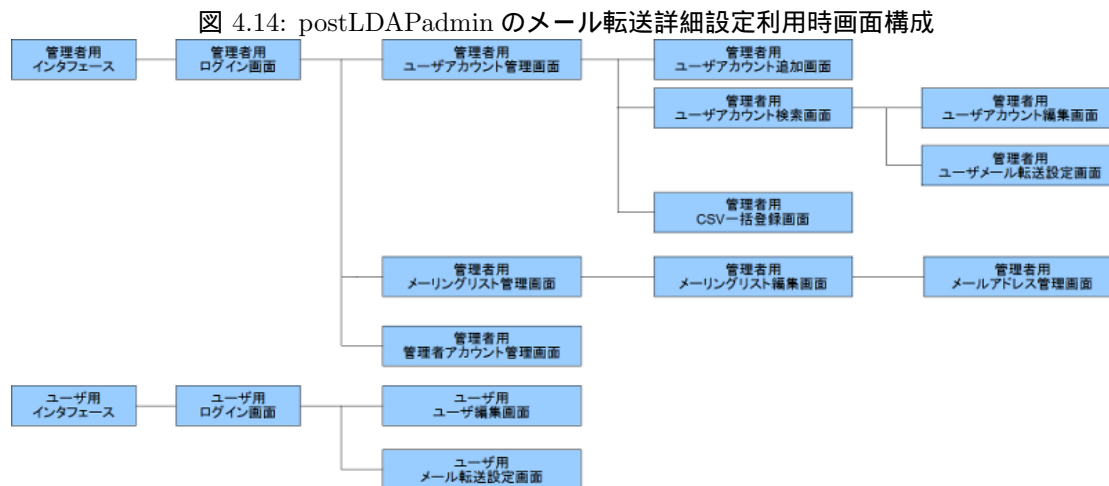
dovecot-sieve が動作する環境が必要です。設定例は Appendix(72) を参照してください。

httpd プロセスが apache ユーザで動作している場合、以下のように sudo の設定を追加する必要があります。

```
Defaults:apache !requiretty  
apache ALL=(ALL) NOPASSWD: /usr/local/postldapadmin/bin/make_sieve
```

4.3.4 メール転送詳細設定利用時の画面構成図

postLDAPAdmin のメール転送詳細設定利用時の画面構成は図 4.14 のようになっています。



4.3.5 管理者側のメール転送詳細設定

図 4.15: ユーザアカウント検索画面 (転送設定 ON 時)

ユーザアカウント管理 > ユーザアカウント検索

ユーザアカウント | メールリングリスト | 管理者アカウント

ユーザの検索

ユーザ名 を含む

検索 CSVダウンロード

[全 4 件]

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	転送設定
testuser			100Kbytes	転送設定
testuser2	testuser-2		100Kbytes	転送設定
user01		user02@example.com	100Kbytes	転送設定
user02			100Kbytes	転送設定

postLDAPAdmin

- 仮想ユーザの検索
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。

- [転送設定] リンク
 - * 仮想ユーザのメール転送設定を行う画面に移動します。

- 仮想ユーザの検索結果ダウンロード
次の項目を指定し、[CSV ダウンロード] 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 CSV ダウンロードを行うと、登録されている仮想ユーザの情報をすべてダウンロードファイルに表示します。

検索結果として、以下の項目が CSV 形式のファイルでダウンロードされます。ダウンロードされるファイルの名前は「userdata_ (Web サーバで設定した環境変数 DOMAIN の値) .csv」です。

```
username,quotasize,mailalias,mailforwardaddr,save,mailfilterorder ,mailfilterarticle
```

表 4.3: 各項目の説明

項目	説明
username	ユーザ名
quotasize	メールボックス容量
mailalias	メールエイリアス
mailforwardaddr	メール転送アドレス
save	サーバにメールを残す/残さない
mailfilterorder	メールフィルタ順序、on/off
mailfilterarticle	メールフィルタ設定内容

web.conf で ForwardConf が on(=1) が設定されている場合に利用できる項目となります。
値が設定されていない項目は空欄となります。

図 4.16: ユーザアカウント編集画面 (転送設定 ON 時)

ユーザアカウント管理 > ユーザアカウント検索

ユーザアカウント | メーリングリスト | 管理者アカウント

ユーザ名	testuser
パスワード	<input type="password"/>
パスワード(確認)	<input type="password"/>
メールボックス容量	100 Kbytes
メールエイリアス	<input type="text"/>

更新 | 削除 | キャンセル

postLDAPadmin

- 仮想ユーザの編集
メール転送アドレス入力欄が非表示になります。

図 4.17: ユーザメール転送設定画面

postLDAPadmin ログアウト

ユーザアカウント管理 > ユーザアカウント検索

ユーザアカウント **メーリングリスト** 管理者アカウント

条件		削除
<input type="radio"/> 全て転送 <input checked="" type="radio"/> 詳細設定 <input checked="" type="checkbox"/> 送信者 <input type="text" value="company@example.c"/> <input type="button" value="と一致する"/> <input type="checkbox"/> 件名 <input type="text"/> <input type="button" value="と一致する"/> <input type="checkbox"/> 宛先(Cc, To) <input type="text"/> <input type="button" value="と一致する"/> 転送先 <input type="text" value="private@example.co"/> サーバにメールを <input type="button" value="残す"/>		
<input type="radio"/> 全て転送 <input checked="" type="radio"/> 詳細設定 <input type="checkbox"/> 送信者 <input type="text"/> <input type="button" value="と一致する"/> <input checked="" type="checkbox"/> 件名 <input type="text" value="緊急連絡"/> <input type="button" value="と一致する"/> <input type="checkbox"/> 宛先(Cc, To) <input type="text"/> <input type="button" value="と一致する"/> 転送先 <input type="text" value="house@example.com"/> サーバにメールを <input type="button" value="残す"/>		
<input checked="" type="radio"/> 全て転送 <input checked="" type="radio"/> 詳細設定 <input type="checkbox"/> 送信者 <input type="text"/> <input type="button" value="と一致する"/> <input type="checkbox"/> 件名 <input type="text"/> <input type="button" value="と一致する"/> <input type="checkbox"/> 宛先(Cc, To) <input type="text"/> <input type="button" value="と一致する"/> 転送先 <input type="text"/> サーバにメールを <input type="button" value="残す"/>		

postLDAPadmin

- ユーザメール転送設定の編集
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。
 - － 全て転送
 - － 詳細設定
 - － 送信者チェックボックス
 - － 送信者入力欄
 - － 送信者一致処理/ ~と一致する, ~を含む, ~を含まない, ~が空である
 - － 件名チェックボックス
 - － 件名入力欄
 - － 件名一致処理/ ~と一致する, ~を含む, ~を含まない, ~が空である
 - － 宛先チェックボックス
 - － 宛先入力欄
 - － 宛先一致処理/ ~と一致する, ~を含む, ~を含まない, ~が空である
 - － メール転送先アドレス入力欄
 - － サーバにメールを/残す, 残さない
- ユーザメール転送設定の削除
[削除] ボタンをクリックすると入力値が削除されます。削除の反映は更新ボタンのクリックで実行されます。

ユーザアカウント追加画面

図 4.18: ユーザアカウント追加画面 (転送設定 ON 時)

ユーザアカウント管理 > ユーザアカウント追加

ユーザアカウント メーリングリスト 管理者アカウント

ユーザ名	<input type="text"/>
パスワード	<input type="password"/>
パスワード(確認)	<input type="password"/>
メールボックス容量	100 Kbytes
メールエイリアス	<input type="text"/>

登録 キャンセル

postLDAPadmin

- 仮想ユーザの追加
メール転送アドレス入力欄が非表示になります。

CSV 一括登録画面

図 4.19: CSV 一括登録画面

ユーザアカウント管理 > csv一括登録

ユーザアカウント メーリングリスト 管理者アカウント

動作タイプ 登録 削除

オプション

既存のデータを上書き(削除の場合は無視されます)

エラーの場合も処理を継続

アップロードファイル 参照...

ファイルチェック ファイルチェック開始

更新

postLDAPadmin

- 仮想ユーザの一括登録・編集
動作タイプに登録を指定します。以下の形式の CSV ファイルを作成し、アップロードファイルに指定します。

```
username,quotasize,mailalias,mailforwardaddr,save,mailfilterorder 2,mailfilterarticle 2
```

表 4.4: 各項目の説明

項目	説明	必須
username	ユーザ名	
passwd	パスワード	
quotasize	メールボックス容量	
mailalias	メールエイリアス	
mailforwardaddr	メール転送アドレス	1
save	サーバにメールを残す (0)/残さない (1)	1
mailfilterorder	フィルタ順序、on/off	2
mailfilterarticle	フィルタ設定値	2

- 1 転送設定が ON の時は入力されていても登録されない項目です。
- 2 転送設定が ON の時に利用できる項目です。

CSV 一括登録ファイルの例

```
add01,passwd,100,alias01,fw01@test.designet.jp,0,,
add02,passwd,,,,,
add03,passwd,100,alias03,,+1:+2:-3,MTpGMTY6aG9nZUB1eGFtcGx1LmNvbWYxczBOMEZzMTpv
bm91ZV9mb3J3YXJkMDFAdGVzdC5leGFtcGx1LmpwZDA=:MjpmMFM00mhvZ2VzMXQwQTE30mhvdXN1QGV
4YW1wbGUuY29tZDA=:MzpmMHMwdDBBMDpkMA==
:
```

オプションを選択すると以下の動作を行います。

- 『既存のデータを上書き』を選択
指定された仮想ユーザが既に登録されている場合、仮想ユーザ情報の編集を行います。
- 『エラーの場合も処理を継続』を選択
エラーが発生した場合、処理を終了せず次の行の処理を行います。

LDAP への追加・変更を行わずファイルの形式チェックのみを行う場合は [ファイルチェック開始] ボタンをクリックします。

LDAP への追加・編集処理を行う場合は [更新] ボタンをクリックします。

[ファイルチェック開始] ボタン、[更新] ボタンを押すと、別ウィンドウに処理結果が表示されます。

- 仮想ユーザの一括削除
動作タイプに削除を指定し、一括削除するユーザ名を記載したファイルをアップロードファイルに指定します。

CSV 一括削除ファイルの例

```
del01
del02
:
```

オプションを選択すると以下の動作を行います。

- 『既存のデータを上書き』を選択
削除の場合、このオプションは無視されます。

- 『エラーの場合も処理を継続』を選択
エラーが発生した場合、処理を終了せず次の行の処理を行います。

LDAP への削除を行わずファイルの形式チェックのみを行う場合は [ファイルチェック開始] ボタンをクリックします。

LDAP への削除処理を行う場合は [更新] ボタンをクリックします。

[ファイルチェック開始] ボタン、[更新] ボタンを押すと、別ウィンドウに処理結果が表示されます。

- 注意事項

- アップロードファイルに指定されるファイルのサイズが php.ini の upload_max_filesize の設定値を超えるとファイルをアップロードすることができません。この場合、upload_max_filesize の設定値を変更してください。
- CSV ファイルの処理時間が php.ini の max_execution_time の設定値を超えると、PHP の処理がタイムアウトします。この場合、max_execution_time の設定値を変更してください

4.3.6 ユーザ側のメール転送詳細設定

ユーザ編集画面

図 4.20: ユーザ編集画面 (転送設定 ON 時)

The screenshot shows the 'postLDAPadmin' web interface. At the top, there is a logo and a 'ログアウト' (Logout) button. Below the header, the page title is 'ユーザアカウント編集' (User Account Edit). There are two tabs: 'ユーザアカウント' (User Account) and 'メール転送' (Mail Transfer). The 'メール転送' tab is active. The form contains three input fields: 'ユーザ名' (Username) with the value 'user02', 'パスワード' (Password), and 'パスワード(確認)' (Password (confirm)). A '更新' (Update) button is located below the form. At the bottom of the page, the 'postLDAPadmin' logo is displayed again.

- 仮想ユーザの編集
メール転送アドレス入力欄が非表示になります。

ユーザメール転送設定画面

図 4.21: ユーザメール転送設定画面

postLDAPadmin ログアウト

メール転送設定

ユーザアカウント メール転送

条件		削除
<input type="radio"/> 全て転送 <input checked="" type="radio"/> 詳細設定 <input checked="" type="checkbox"/> 送信者 company@example.co と一致する <input type="checkbox"/> 件名 と一致する <input type="checkbox"/> 宛先(Cc,To) と一致する 転送先 private@example.co サーバにメールを 残す		
<input type="radio"/> 全て転送 <input checked="" type="radio"/> 詳細設定 <input type="checkbox"/> 送信者 と一致する <input checked="" type="checkbox"/> 件名 緊急連絡 と一致する <input type="checkbox"/> 宛先(Cc,To) と一致する 転送先 house@example.com サーバにメールを 残す		
<input checked="" type="radio"/> 全て転送 <input type="radio"/> 詳細設定 <input type="checkbox"/> 送信者 と一致する <input type="checkbox"/> 件名 と一致する <input type="checkbox"/> 宛先(Cc,To) と一致する 転送先 サーバにメールを 残す		

更新

postLDAPadmin

- ユーザメール転送設定の編集
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。
 - － 全て転送
 - － 詳細設定
 - － 送信者チェックボックス
 - － 送信者入力欄
 - － 送信者一致処理/ ~と一致する, ~を含む, ~を含まない, ~が空である
 - － 件名チェックボックス
 - － 件名入力欄
 - － 件名一致処理/ ~と一致する, ~を含む, ~を含まない, ~が空である
 - － 宛先チェックボックス
 - － 宛先入力欄
 - － 宛先一致処理/ ~と一致する, ~を含む, ~を含まない, ~が空である
 - － メール転送先アドレス入力欄
 - － サーバにメールを/残す, 残さない
- ユーザメール転送設定の削除
[削除] ボタンをクリックすると入力値が削除されます。削除の反映は更新ボタンのクリックで実行されます。

第5章 設定詳細 (web.conf)

web.conf には、postLDAPAdmin のフレームワークの項目 5 と、postLDAPAdmin の項目 5.1 を設定します。

- postLDAPAdmin のフレームワークの項目 [global] の下に設定してください。

項目	解説
TitleName	ページのタイトルの設定をします。ページの上部に表示されるソフトウェア名称と、ブラウザのタイトルに使用されます。
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。
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。syslog を使用する場合は、「syslog」を指定します。
SyslogFacility	ログを出力するファシリティを指定します。
SessionTimeout	セッションのタイムアウト秒数を指定します。
MaxPasswordLength	パスワードに使用できる最大の文字数を指定します。PasswordEncrypt 設定で CRYPT を設定した場合は 8 に、MD5 を設定した場合にはそれ以上の数値を指定してください。デフォルトは 8 です。
MinPasswordLength	パスワード設定時に最低指定しなければならない文字数を指定します。
PasswordEncrypt	LDAP の userPassword 属性に格納するパスワードの暗号化方式を指定します。CRYPT と MD5 が指定できます。CRYPT は最大 8 文字までしかパスワードに指定することができません。デフォルトは CRYPT です。

- postLDAPAdmin の項目 [postldapadmin] の下に設定してください。

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。
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。
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。
QuotaUnit	ユーザアカウント追加画面、ユーザアカウント検索画面、ユーザアカウント変更画面でのメールボックス容量の単位を指定します。「b」を指定した場合には byte、「kb」を指定した場合には Kbyte、「mb」を指定した場合には Mbyte、「gb」を指定した場合には Gbyte となります。使用するメールサーバソフトウェアのクォータの単位に合わせて指定してください。
QuotaSize	ユーザアカウント追加画面、ユーザアカウント変更画面でのメールボックス容量の入力可能桁数 (maxlength) を指定します。

LocalPartRFCCheck	<p>メールアドレスのローカルパートの形式チェックの有効/無効を切り替える設定値となります。</p> <p>0 を指定した場合はチェックが行われず、1 を指定した場合にはチェックが行われます。</p> <p>本設定値が存在しない場合にはチェックは行われません。</p> <p>本設定を有効とした場合には以下の 3 つのチェックを行い該当する場合には形式エラーとします。</p> <ul style="list-style-type: none"> ・メールアドレスのローカルパートの先頭が「.」で始まっているか ・メールアドレスのローカルパートの末尾が「.」で始まっているか ・メールアドレスのローカルパートに「.」が連続しているか <p>チェックの対象となる項目は下記の通りです。</p> <p>【管理者用インタフェース】</p> <p>[ユーザアカウント追加画面]</p> <ul style="list-style-type: none"> ・ユーザ名 ・メールエイリアス ・メール転送アドレス <p>[ユーザアカウント編集画面]</p> <ul style="list-style-type: none"> ・メールエイリアス ・メール転送アドレス <p>[CSV 一括登録画面]</p> <ul style="list-style-type: none"> ・仮想ユーザー一括登録/編集で使用する CSV ファイルの以下の項目 <ul style="list-style-type: none"> - ユーザ名 - メールエイリアス - メール転送アドレス <p>[メールリングリスト編集画面]</p> <ul style="list-style-type: none"> ・メールリングリストアドレス <p>[メールアドレス管理画面]</p> <ul style="list-style-type: none"> ・メールアドレス ・一括登録に使用するファイルに記述されたメールアドレス <p>【ユーザ用インタフェース】</p> <p>[ユーザ編集画面]</p> <ul style="list-style-type: none"> ・メール転送アドレス
ForwardConf	<p>メール転送設定機能の有効/無効を切り替える設定値となります。</p> <p>0 を設定した場合は、転送条件は指定できず LDAP に登録された mailForwardingAddr にメールが転送されます。</p> <p>1 を設定した場合はメール転送条件を詳細に登録することができます。</p> <p>また、メールの転送を davecot.sieve によって行ないます。</p>
ForwardNum	<p>メール転送設定機能が ON の時、メール転送設定画面のフィルタ登録カラム数を変更出来ます。</p>
ForwardFirstMatch	<p>メール転送設定機能が ON の時、複数マッチしたメールの動作を切り替える事が出来ます。</p> <p>0 を設定した場合は、複数条件にマッチした時、全ての転送設定先にメールを転送します。</p> <p>1 を設定した場合は、複数条件にマッチした時、一番最初にマッチした転送先のみメールを転送します。</p>

付録 A Appendix

A.1 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.1.1 LDAP サーバの基本設定

LDAP サーバの設定は、`ldapadd`、`ldapmodify`、`ldapsearch` コマンドを使用して設定、確認を行うことができます。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 の設定例

```
# ldapmodify -Y EXTERNAL -H ldapi:///<CR>
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
dn: olcDatabase={2}hdb,cn=config<CR>
changetype: modify<CR>
replace: olcSuffix<CR>
olcSuffix: dc=designet,dc=jp<CR>
-<CR>
replace: olcRootDN<CR>
olcRootDN: cn=Manager,dc=designet,dc=jp<CR>
-<CR>
replace: olcRootPW<CR>
olcRootPW: {SSHA}H55wd4urFefNKQWc1Qc+jWKapTKMuBqg<CR>
-<CR>
<CR>
modifying entry "olcDatabase={2}hdb,cn=config"
<CTRL+D>
```

上記の例では、サフィックス、RootDN、RootDN のパスワードを変更しています。
<CR>は Enter キーの入力、<CTRL+D>は CTRL キー + D キーの入力を示しています。

slapd の設定確認例

```
# ldapsearch -LLL -Y EXTERNAL -H ldapi:/// -b olcDatabase={2}hdb,cn=config<CR>
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
dn: olcDatabase={2}hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {2}hdb
olcDbDirectory: /var/lib/ldap
olcSuffix: dc=designet,dc=jp
olcRootDN: cn=Manager,dc=designet,dc=jp
olcRootPW: {SSHA}BviUnbZ6FRbHBUwK34Be02BJpy82Uko9
olcDbIndex: objectClass eq,pres
olcDbIndex: ou,cn,mail,surname,givenname eq,pres,sub
olcDbIndex: uid eq,sub
```

A.1.2 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
```

A.2 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。

A.2.1 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

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

```

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 A.1 のとおりです。

表 A.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。

A.3 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/>

A.3.1 postLDAPadmin の web.conf の設定

postfix、courier-imap は byte 単位でクォータを参照するため、web.conf の QuotaUnit の項目は b を設定してください。

A.3.2 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、authdaemon 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（コメント行を除く）

```
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 A.2 のとおりです。

A.4 既に LDAP 環境がある場合

既に LDAP の環境が構築されている場合は、次の点に注意して LDAP のユーザのエントリの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

A.4.1 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。

A.4.2 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。

表 A.2: 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で検索を行います。
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。

A.4.3 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。

A.5 dovecot-sieve の設定例

以下の動作設定は CentOS 6.5 上に dovecot および dovecot-pigeonhole を用いて設定を行っています。以降の設定は、dovecot および dovecot-pigeonhole をインストール後に行なって下さい。

A.5.1 dovecot を利用したローカル配送の設定例

postfix の設定例

postfix の設定は、main.cf, master.cf 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。

/etc/postfix/main.cf の設定例 (コメント行を除く)

```
virtual_transport = dovecot          バーチャルドメインの配送で dovecot を利用するという設定
dovecot_destination_recipient_limit = 1 Dovecot の宛先の受信者の制限
```

/etc/postfix/master.cf の設定例 (コメント行を除く)

```
dovecot  unix -      n      n      -      -      pipe
         flags=DRhu user=vmail:vmail argv=/usr/libexec/dovecot/deliver -f ${sender} -d ${recipient}
dovecot の deliver を利用するのに必要な設定
```

以上の設定後、postfix を restart します。

dovecot の配送設定例

次に、dovecot によるバーチャルドメインの配送設定を行います。環境に合わせて設定してください。

/etc/dovecot/conf.d/10-mail.conf の設定例 (コメント行を除く)

```
mail_plugins          = $mail_plugins quota
mail_location         = maildir:~/Maildir
mail_uid              = vmail
mail_gid              = vmail
```


/etc/dovecot/conf.d/10-master.conf の設定例 (コメント行を除く)

```
service auth {
  unix_listener auth-userdb {
    mode      = 0600
    user      = vmail
    group     = vmail
  }
}
```

/etc/dovecot/conf.d/15-lda.conf の設定例 (コメント行を除く)

```
postmaster_address = root@localhost
protocol lda {
  userdb {
    driver = ldap
    args = /etc/dovecot/ldap/userdb-lda.conf.ext
  }
  mail_plugins = $mail_plugins sieve
}
```

/etc/dovecot/conf.d/90-quota.conf の設定例 (コメント行を除く)

```
plugin {
  quota = maildir:User quota
}
```

/etc/dovecot/ldap/userdb-lda.conf.ext の設定例 (コメント行を除く)

```
hosts = 127.0.0.1:389
dn = cn=Manager,dc=designet,dc=jp
dnpass = secret
base = dc=designet,dc=jp
scope = subtree
user_filter = (!mail=%u)(mailAlias=%u)
user_attrs = mailDirectory=home,quotaSize=quota_rule=*:bytes=%$K
```

dovecot の LDAP 設定ファイルの設定項目は、表 A.3 のとおりです。
以上の設定後、dovecot を start します。

sieve の設定例

次に、sieve を有効化する設定を行います。環境に合わせて設定してください。

/etc/dovecot/conf.d/90-sieve.conf の設定例 (コメント行を除く)

```
sieve = ~/Maildir/dovecot.sieve
```

以上の設定後、dovecot を restart します。

表 A.3: Postfix 検索テーブルの LDAP 設定ファイル

項目	解説
hosts	LDAP サーバのホスト名または IP アドレスを設定します。
dn	LDAP 検索の時に使用するベース DN を設定します。
dnpass	ベース DN に対応するパスワードを設定します。
auth_bind	パスワードの有効性を確認するために認証バインドを使用するかどうかを設定します。
base	LDAP 検索のときに使用するベース DN 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。
user_attr	user の属性を設定します。 本設定例では以下の設定を行っています。 home: メールディレクトリの PATH を指定しています。 quota_rule: 容量制限のルールをキロバイト単位で指定しています。
user_filter	user のフィルターを設定します。

A.6 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/>
- Dovecot ホームページ
<http://www.dovecot.org/>