

鈴鹿国際大学メールサーバの構築

SPAM メールへの対応と Web メールシステムの導入

Construction of the Mail Server of Suzuka International University Spam Filtering and Introduction of Webmail System

原 仁 志*
Hitoshi Hara

Abstract

In this paper the process of building a university mail server using Linux operating system, spam filtering and a Webmail system is introduced. The hardware and specifications of the operating system are described.

Keywords : mail server, spam filtering, Webmail system

1. はじめに

近年 spam¹⁾メールの届く量が増大し、本学教職員からも spam 対策についての要望が出ていた。現在稼働しているメールサーバ（以降、旧メールサーバと呼ぶ）は本学にネットワークが敷設された当初から稼働しているシステムであり、機器、OS（Operating System）ともに旧式となっている。OS を新しくしようにも既に対応機種から外れている。よって今回、機器と OS を一新したメールサーバ（以降、新メールサーバと呼ぶ）を構築して spam メール対策を行うことにした。

旧メールサーバでは電子メールの送信、受信、フォワード（転送）機能を有している。この旧メールサーバの機能をすべて含み、更に spam メール対策その他の機能を追加することとする。つまり本学教職員及び全学生のメールアドレスを用意し、電子メールの送受信ができることに加えて、届くメールに対する spam メール対策を施す。また、今回は

*本学准教授、情報教育(Associate Professor, Information Education)

学外からの電子メール送受信を可能とするため Webmail システムの導入も行う。更に Web サーバも旧メールサーバと同型のマシンであり最近不安定であったため、これも新しいサーバで運用することとした。

表-1 に旧メールサーバと新メールサーバの機能を比較したものを示す。

表-1 旧メールサーバと新メールサーバの機能比較

| 機能 | 旧メールサーバ | 新メールサーバ |
|--------------|---------|---------|
| 電子メール受信 | ○ | ○ |
| 電子メール送信 | ○ | ○ |
| フォワード（転送） | ○ | ○ |
| spam メール対策 | × | ○ |
| Webmail システム | × | ○ |

2. 機器構成

新メールサーバには日本 HP 社の ProLiant サーバ ML115 を採用した。ML115 の主要スペックは表-2 のようになる。OS は付属していないが非常に安価なモデルであり、様々なカスタマイズも可能である。今回使用したのは必要最低限のハードウェアを搭載したモデルだが、スペックとしては十分である。今回はこの ML115 を合計 4 台導入してシステムを構築する。

表-2 ML115 の主要スペック

| | |
|---------|--------------------------|
| CPU | AMD Athlon 3500+(2.2GHz) |
| メモリ | PC2-5300 512MB |
| グラフィック | 内蔵 2MB ビデオコントローラ |
| 光学ドライブ | CD-ROM ドライブ |
| ハードディスク | SATA 80GB 1 台 |

それぞれの機器は以下のように構成する。

(1) 教職員用メールサーバ

旧メールサーバでは学生も教職員も同じサーバで電子メールの送受信を行っていたが、これを分割することとした。そのうちの教職員用アカウントを管理するサーバ

である。spam 対策や Webmail システムを導入する。

(2) Web サーバ兼学生用メールサーバ

学生用電子メールアカウントを管理するサーバと、これまで運用していた旧 Web サーバの機能を 1 台に集約することとした。学生用アカウントは登録アカウント数が多いこともあり、教職員用アカウントよりも使用できる容量を少なくし、また負荷軽減のため spam 対策を行わない。また、Webmail システムも導入しない。

(3) NetCommons2 用サーバ

グループウェアとして NetCommons2 を運用予定のサーバ。試験運用中である。

(4) 予備機器

メールサーバが不具合をおこした際に入れ替えるための予備機器。

また、運用中の各サーバには停電や瞬電等に対応できるように UPS²⁾を導入した。

3. OS

OS は Linux を採用するが、様々なディストリビューションが存在する。今回は以前にも内部サーバ用に利用したことのある Vine Linux 4.2 を採用した。日本で開発されているディストリビューションであり、日本語を利用した環境に有利である。インストールに先立ち、まずパーティション構成を考える。ここでは表-3 のようにした。

表-3 パーティション構成

| マウント位置 | 役割 | 容量 |
|--------|----------------|-------|
| / | ルート (主要ディレクトリ) | 14GB |
| /swap | スワップ (仮想メモリ) | 256MB |
| /boot | ブート (起動ファイル) | 100MB |
| /home | ホームディレクトリ | 60GB |

ルートディレクトリ (主要ディレクトリ) はプログラム等システムのメインとなる部分である。ユーザアカウントの電子メール等が記憶されるホームディレクトリは別のパーティションとすることで、クラッシュ時のリスクを分散する。

OS のインストール自体は非常に容易である。まず他の PC から Vine Linux の公式サイトへアクセスし、CD のイメージファイルをダウンロードする。そのイメージファイルを書き込みソフトで CD-R へ書き込む。その後、インストールするマシンで CD-R から起動すれば自動的にインストーラが起動する。

インストーラではインストールオプションやパーティション構成、ネットワーク接続 (IP アドレスやネットマスク等の設定) を設定すればあとは自動でインストールが行われる。サーバとして運用するので、インストールオプションは「サーバ」を選ぶ。パーティション構成は先に示した表-3 のように構成した。後は自動的にフォーマット、ファイルのコピー、インストールが行われる。再起動した後はログイン画面が表示される。

4. メールサーバの仕様

メールサーバを構築するにあたり、メール管理に関して以下のことを仕様とする。

(1) MTA³⁾として Postfix を採用する

MTA としては sendmail が採用されることが多いが、設定が難解で運用が難しい。ここでは運用管理が比較的容易な Postfix を採用する。

(2) MDA⁴⁾として Dovecot を採用する

ユーザがメールクライアント⁵⁾で電子メールを読む際に必要となる配送 (POP3⁶⁾) を司るソフトウェアとして Dovecot を採用した。IMAP プロトコルもサポートしており、後述する Webmail システムの際にも利用する。

(3) ユーザ管理は Linux のアカウントと同期する

MySQL などのデータベースと同期して電子メールを管理することも可能だが、ここでは一般的な Linux のアカウントと同期することを仕様とする。

(4) 各ユーザは Linux のアカウントとしてログインできない

サーバのセキュリティを確保する意味で、ログインが不要なユーザは Linux のアカウントとしてログインできなくする。仮に新メールサーバマシンへ直接触れる機会があったとしてもログインできない。

(5) 各ユーザは Quota により容量制限を設ける

Quota を導入し、各ユーザに容量制限を設ける。ハードディスクの容量は限られているので、1 ユーザあたりが利用できる容量を制限する。

(6) メールは 1 メール 1 ファイルとする

メールは 1 ファイルに複数メールを格納する方式 (Mailbox 方式) と 1 ファイル 1 メールとする方式 (Maildir 方式) があるが、ここでは後者を採用する。Maildir 方式だと管理するファイル数は増えるが、ファイルが破損した場合の被害は Mailbox 方式よりも大幅に少ない。

5. Postfix の設定

ユーザは学外からメールを送信できない設定とする。学外からの SMTP⁷⁾によるメール送信を許す場合、通常の SMTP プロトコルのみでは暗号化が全くかかっておらず危険なので何らかの対策が必要となる。また、そのままだと誰でも認証なしでメールが送信できてしまう。よって SMTP-AUTH による認証が必要となるが、それでも認証する際のパスワードが平文でインターネット上を流れることになる。よって学外からのメール送信を許す場合には TLS⁸⁾による暗号化が必要となるが、これを行うとユーザ側のメールクライアントに追加の設定が必要となる。

ここまで設定してまでユーザがメールクライアントで外部からの接続を許す必要があるかどうかだが、わざわざ TLS を導入して外部から接続できるようにするよりも、内部ネットワークのみで解決できるほうが安全性は高い。

当初、spam メール対策の一環として、厳密なチェックを行った上で通過した電子メールのみを受け取るように設定したが、ユーザからメールが受け取れないことがあるとの報告があったため徐々に制限を緩めた。現在では制限らしい制限はあまりかけていないが、ブラックリストデータベースによるチェックやユーザ認証は有効にしてある。また、不正中継によるいわゆる「spam メールの踏み台」として利用されないように、不正中継チェックサイトによるチェックを行った。これにより現在の設定で不正中継が行われなかったことを確認している。

6. Webmail システム

これまでのシステムでは学外からの電子メール送受信はできなかった。旧メールサーバのフォワード機能を利用した電子メールの転送で、個人契約のプロバイダへ転送することによって対応するのみであった。これでは、学外から大学のメールアカウントに受信したメールを読むことはできるが、学外から大学のメールアカウントを利用してメールを送信することはできない。そこで今回、Webmail システムを構築し、この問題を解決することにした。

学外から新メールサーバへメールクライアントから接続できるようにして、学外と学内で同等の利用環境にするという方法もあるが、セキュリティの面で不安があったため中止した。Webmail システムならば Internet Explorer や Firefox などのブラウザがあればどんな PC 環境でもインターネットを経由して利用可能であり、SSL⁹⁾による通信暗号化でセキュリティも保たれる。また、アクセスできる URL を知らなければ Webmail のページへたどり着くこともできない。更に、Webmail システムは新メールサーバと同じシステム

上に配置してあるので安全に運用することができる。

今回は Webmail システムに SquirrelMail を採用した。これは PHP ベースのシステムで、IMAP プロトコルによりメールサーバと通信して電子メールを送受信する。よって MTA が POP3 以外に IMAP をサポートしている必要がある。

インストールは Apache2^{1 0)} の SSL サポートがインストールされた環境であれば比較的容易である。SquirrelMail のソフトウェアアーカイブを展開し、ブラウザからアクセスできるディレクトリへ展開したソースファイルを移動、その後設定プログラムにより設定を行えばよい。

利用方法はブラウザから指定した URL へアクセスし、ログイン名（アカウント名）とパスワードを入力してログインするだけである。一般的なプロバイダが提供している Webmail システムよりは若干機能が劣るが、電子メールの送受信、アドレス帳機能等一通りの操作ができる。またプラグインを導入することにより、メッセージアーカイブ機能（電子メールを圧縮してダウンロードできる機能）、現在の使用容量表示（画面左上）ができるようにしてある（図-1）。

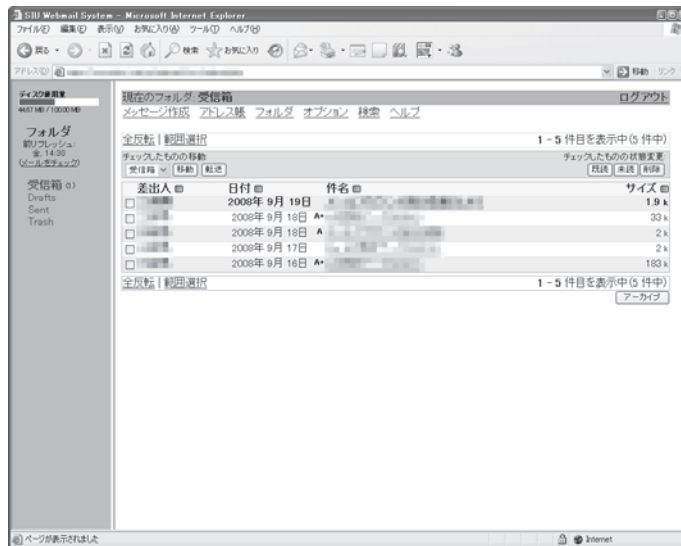


図-1 Webmail システムの画面

7. spam メール対策

spam メールは年々増加している。プロバイダや各種ソフトウェア側も様々な対策を行っているが決定的なものは未だにない。ここで言う spam メール対策も万全ではないが、

その一助となるものである。

今回の spam メール対策には SpamAssassin を利用した。あらかじめ spam (あるいは ham¹⁾) のルールを設定しておく、SpamAssassin がスコアをつける。そのスコアを元に spam かどうかの判断をするのである。スコアのしきい値を何点に設定するかによって spam の判定を厳しくも甘くもできる。

また、これはベイジアンフィルタを利用して学習させることもできる。ユーザが spam、もしくは ham と判定したメールを SpamAssassin で学習させることにより、判定の精度を高めることができるのである。SpamAssassin の仕組みは図-2 のようになっており、その手順は次のようになっている。

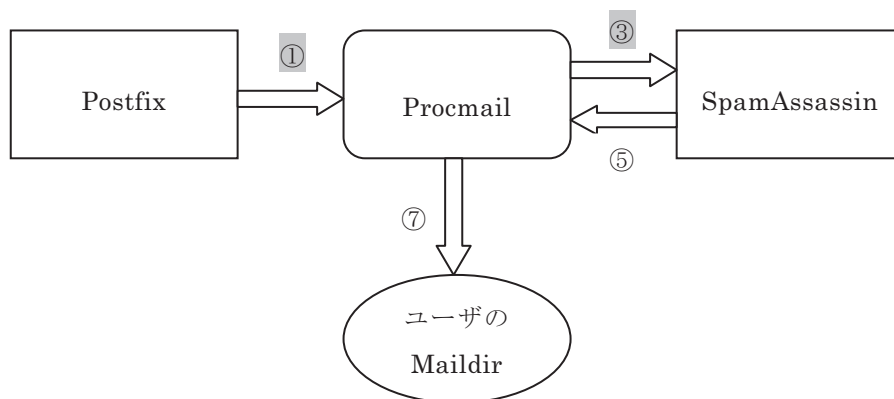


図-2 Procmail と SpamAssassin の仕組み

- (1) MTA である Postfix が配送先であるユーザの Maildir ディレクトリへ電子メールをコピーする間にメールフィルタ Procmail を割り込ませる。Procmail は本来、受信した電子メールを特定のルールに従って振り分けるソフトウェアであるが、これを利用して SpamAssassin へ電子メールを転送する。
- (2) 電子メールを受け取った SpamAssassin は設定されたルールによってスコアをつけて電子メールのヘッダ情報 (X-Spam-*) にスコアやその他の情報を付加する。spam であった場合は、表題 (Subject) の先頭へ「[SPAM]」の文字を付加する。
- (3) 情報を付加したメールを Procmail へ戻し、そこからユーザの Maildir ディレクトリへ配送する。

Procmail へ電子メールが戻された時点で判定を行い、spam 自体を削除してユーザへ配

送されないようにすることも可能であるが、今回は削除せずにそのまま配送することにした。これは SpamAssassin のつけるスコアが適切でなく、誤判定を行ってしまうという可能性を排除するためである。100%の確率で spam かどうかを機械的に判断する方法がない限りはこのようにしたほうが安全である。このため削除するか否かの最終判断はユーザへ委ねることになる。ユーザはメールクライアントにより表題の「[SPAM]」をキーワードとして spam 専用フォルダへ振り分け等行う。後はそのまま削除することも、表題や内容をチェックしてから削除することも自由に選択できる。メールクライアントでフォルダ振り分けをしておけば、表題や内容をチェックしてから削除する場合でも spam かどうかの判断は比較的短時間で済ませることができると考えられる。

SpamAssassin のデフォルトルールは簡素で、更に日本語対応ができていないので、こちらで新たに作成する必要がある。これを 0 から作成するのは非常に時間がかかる上に困難なので、今回は TLEC (Tokyo Linux Entertainment Community) が配布するユーザ定義ファイルを利用させていただいた。これは日本語の spam にも対応した定義ファイルである。

メールサーバへ届いた spam メールから学習することも可能であるが、現在のところ学習は手作業で行っている。

また、spam と判定するスコアのしきい値は 5.0 と設定した。デフォルトでは 15.0 であったが、これではほとんどの spam が spam と判定されなかった。この設定で半年間運用したが、現在のところ ham と判定された spam はあっても、spam と判定された ham はなかった。だが依然として spam と判定されない spam が存在するので、もう少し統計をとってからしきい値を調整する必要があるかもしれない。

8. グループウェア

グループウェアの導入により業務の効率化をはかる。システムとしては国立情報学研究所が開発した NetCommons2 を採用する。その利点としては以下のようなものがあげられる。

- ① 学内文書の共有 (ダウンロード)
- ② 行事予定表 (カレンダー)
- ③ 施設予約
- ④ 掲示板
- ⑤ Q&A (FAQ)

以下は、基本的にログインしたユーザに対するサービスと考えている。

学内文書の共有は、提出書類のフォーマットや、各種マニュアル等のダウンロードができるようにすることである。これによってダウンロードしたフォーマットに Word 等で記入した後に印刷すれば、そのまま提出できる書類ができあがる。行事予定表については、NetCommons2 のカレンダー機能により常に統一された最新版を参照することができるようになる。もちろん、担当者は常に新しい予定を書き込んでおく必要がある。会議室や教室等の施設予約も行えるようになれば、NetCommons2 上ですぐに空いている時間帯がわかるので便利である。掲示板は電子メール会議に代わるものとして利用して欲しいと考えている。電子メールではログ（記録）が残りにくい、掲示板であればそのままログが残るので簡単に後から参照できる。Q&A ではよくある質問等の答えをまとめてデータベースとして残しておくことを考えている。また、会議の資料や議事録等を共有文書として置くことによりペーパーレスへの貢献もできると考えられる。

9. バックアップ

電源のバックアップと、システムやデータのバックアップについて対策を行うことにより、システム故障を回避し、復元を容易にする。

(1) 電源のバックアップ

停電や瞬電等、電源が確保されない場合の対策として UPS を導入している。停電等により電源が正しく確保されていない状態が長く続いたと判断された場合、UPS からサーバへシャットダウンの信号が送られる。その後、電源が正しく確保されれば再び UPS が復帰し、サーバも起動する。

(2) システムとデータのバックアップ

USB 接続の外付けハードディスク (I・O データ製 HDH-U500SR2、容量 500GB) を増設し、そちらへシステムとデータのバックアップをとることにする。外付けで別の記憶媒体へバックアップすることにより、安全性を確保する。

バックアップにはパーティション単位でバックアップでき、差分バックアップも可能な dump コマンドを使用した。具体的には以下のようなスケジュールでバックアップをとる。

① フルバックアップを日曜日午前 3 時 5 分に行う。

② 月曜日～土曜日の午前 3 時 5 分に、①でとったフルバックアップからの差分バ

ックアップを行う。

③ ①と②のスクリプト（一週間分、合計7ファイル）を cron^{1 2)}により実行する。

各バックアップは1週前のコピーを残す形とするので、最長で2週間前、最短でも1週間前の状態まで戻すことができる。各週の日曜日まで戻す場合は、フルバックアップのみをリストアすれば良い。月曜日～土曜日までの状態に戻す場合は、その週の日曜日のフルバックアップからリストアし、該当する曜日の差分バックアップを追加でリストアすれば良い。

10. 今後の課題

SpamAssassin のルールは定期的に新しいものへ手動で更新しているが、ham と判定される spam は依然として存在する。ある程度自動的に学習する仕組みを作ってルールを更新させる方法を探っている。

導入した Webmail システムは携帯電話からのアクセスに対応していないが、将来的には携帯電話からでも問題なくアクセスできる仕組みを導入したい。そうすれば出先から手軽に電子メールの確認ができるようになる。

グループウェアとして試験運用中の NetCommons2 を正式運用し、学内情報の共有を図りたいと考えている。グループウェアを学外から利用できると便利ではないかという意見も頂いた。これについては情報漏洩の危険性もあるので慎重に検討したい。

また、DNS (Domain Name Service) も今回と同様に Linux で構築し、新しいシステムとして運用したいと考えている。現在は外部向け DNS と内部向け DNS が動作しているが、これらを新しいシステムに置き換えてしまえば古いサーバは全て入れ替えることができる。そうすれば老朽化による故障の問題やマシンパワーの問題が解消されると思われる。

11. おわりに

今回新たにメールサーバを構築したが、設定の調整が難しいことが改めてわかった。Postfix の設定等、より良いシステムを構築できるようにこれからもメンテナンスを続けていかななくてはならない。

またネットワーク全体が老朽化しているので、順次新しい機器へのリプレースを考える必要がある。構築できるサーバに関しては自前で設定を行った方が全体構成が把握でき、運用管理も容易であると感じた。

注

- 1) 広告や勧誘などの迷惑メールのこと。
- 2) **Uninterruptible Power Supply**：無停電電源装置。
- 3) **Mail Transfer Agent**：メール転送エージェント。
- 4) **Mail Delivery Agent**：メール配送エージェント。
- 5) 電子メールを読み書きするためのソフトウェア。メーラ、MUA (Mail User Agent) ともいう。
- 6) **Post Office Protocol Version 3**：インターネットで電子メールを受信するためのプロトコル。
- 7) **Simple Mail Transfer Protocol**：インターネットで電子メールを転送するためのプロトコル。
- 8) **Transport Layer Security**：インターネット上で情報を暗号化して送受信するプロトコルの一種。
- 9) **Secure Socket Layer**：インターネット上で情報を暗号化して送受信するプロトコルの一種。
- 10) **Apache HTTP Server**。Web サーバソフトウェア。
- 11) **spam** ではなく、受け取りたいメールのこと。
- 12) ジョブ (スクリプト) を定期的に自動実行するためのコマンド。

参考文献

トップマネジメント『Vine Linux 2.5 と Webmin で作るコマンド不要の自宅サーバー』株式会社ローカス, 2002 年

野村直『Vine Linux 2.5 スタートブック』株式会社アスキー, 2002 年

国立情報学研究所『国立情報学研究所』<http://www.nii.ac.jp/>

日本 SpamAssassin ユーザ会『日本 SpamAssassin ユーザ会』<http://spamassassin.jp/>

Frederick P. Brooks, Jr.『The Postfix Home Page』<http://www.postfix.org/>

Hewlett-Packard Development Company, L.P『日本 HP へようこそ』

<http://welcome.hp.com/country/jp/ja/welcome.html>

ike@kobitosan.net『Postfix のページ』<http://www.postfix-jp.info/>

Project Vine『Vine Linux Home Page』<http://vinelinux.org/>

The Apache SpamAssassin Project『SpamAssassin: Welcome to SpamAssassin』

<http://spamassassin.apache.org/>

The NetCommons Project『NetCommons2 公式サイト』<http://www.netcommons.org/>

The SquirrelMail Project Team『SquirrelMail - Webmail for Nuts』<http://www.squirrelmail.org/>

The SquirrelMail Project, Japan『SquirrelMail Japan - Webmail for Nuts!』

<http://www.squirrelmail.jp/>

TLEC『Welcome to TLEC -Tokyo Linux Entertainment Community』<http://tlec.linux.or.jp/>

