教職員用メールサーバと学生用メールサーバの更新

杉谷賢一　島本勝　林恵里　辻一隆
総合情報基盤センター

[概要]
長年運用してサーバのハードウェアや OS も古くなっていた教職員用メールサーバと学生用メールサーバを更新しました。それに併せて、SPAM 対策ソフトやウィルス対策のソフトの導入や認証システムの変更を行いましので、これらについての概要を報告いたします。

1 本学の教職員用メールサーバと学生用メールサーバの運用

本学では、学内ネットワーク創設時に、ほとんどの部局 (学部) でそれぞれメールサーバを立ち上げ、サブドメインごとにメールサーバを運用しています。同時に、メールサーバを運用されない部局の教職員や、部局のメールサーバ以外に別のメールアドレスも持ちたい方のために、当センターでも全学共用のメールサーバを運用しています。ただし、こちらは利用される各ユーザに、サポート費用として毎年少々の校費を移算していただいています。この全学共用のメールサーバが、7 年以上同じマシンでの運用を続けたために、ユーザの増加にパフォーマンスがついていかなくなっていました。

また、これらとは別に、本学に在籍中の学生用のメールサーバも、平成 10 年より運用を開始しました。こちらは、入学と同時に全ての学生がメールを利用できるように環境を構築しております。こちらのサーバは、1 度サーバを更新したのですが、1 万を越える ID を一台のマシンでサポートしているため、学生さんの利用が活発になるに従って、パフォーマンスの低下が著しくなってきていました。

このような状況の上に、ディスク障害が発生するなどしてユーザの皆様にご迷惑をお掛けする事態が発生したため、それまで準備しておりました新しいサーバに急遽更新することにいたしました。

2 新サーバの構成

全学共用教職員用メールサーバと学生用メールサーバのハードウェア構成は、以下のようになっています。

- CPU: Xeon 2.8GHz * 2
- RAM: 6GB (ECC 付き)
- HDD: 143GB * 2 (15,000rpm, Urltra320 SCSI, RAID10)
- DVD-ROM
- OS: Cent OS
- MTA: Postfix
- POP3: Dovecot

本システムから、これまで mbox 形式だったメールボックスを、Maildir 形式に変更するとともに、quoata による容量制限も行うようにしています。

3 利用環境のセイキュア化

前システムまでは、SMTP ならびに POP3 は、暗号化機能を持たせていませんでした。これは、サーバの性能とクライアントソフトの対応状況からそのようにしていました。今回は、どちらの条件もクリアできていると判断し、暗号化機能に対応させました。

特に学生用のメールサーバでは、学外からの受信時には、暗号化機能有りの状態でないと受信できないような設定にしています。

更に、送信時の認証機能 (SMTP-Auth) も付加しましたので、送信時の暗号化も必要なりこれにも対応させました。ただし、送信時認証機能は、今のところ必須ではなく、学外からの送信でも、受信し動作後一定の時間だけは送信を行うことができる POP-Befor-SMTP 機能もこれまでどおり提供しています。

4 ウィルス、ワーム、spam 対策

ご存じのように、最近では、ウィルスやワームおよび spam 対策を行わないと、重要なメールを見落とすくらいの迷惑メールの受信量がひどい状況になっています。

そのため、新サーバでは以下のようなフリーソフトによって、これらの迷惑メールに対する対策を行っています。

4.1 ウィルスおよびワーム対策

ウィルスおよびワーム対策としては、以下のソフトを用いています。

- Clam AntiVirus (ClamAV)
  http://www.clamav.net/

ClamAV は、ウィルスおよびワームの検出を行うフリーソフトウェアです。ウィルスパターンも頻繁に更新されていますので、最新のウィルスやワームにも対応できます。

まず、メールサーバに届いたメールは、全てウィルスおよびワームの検出を行うように、設定しておきます。そして、届いたメール中にウィルスやワームが含まれていたと判断すると、届いたメールはは削除され、ウィルスを削除したことを知らせるメールを、送信者及び受信者に送ります。

もちろん、検出できなかった場合は、そのまま受信者のメールボックスに届けます。

4.2 spam 対策

spam 対策ソフトととしては、以下の 2 つを利用しています。

- Postgrey
  http://www.kozupon.com/postgrey/index.html
- SpamAssassin
  http://spamassassin.jp/

Postgrey とは、正確には Postfix Greylisting Policy Servergreylisting と呼ばれ、SPAM を防御するための一種の方法である Greylising を実装する Postfix ポリシーサーバです。

Greylisting は、spam の挙動をうまく利用して、spam を撃退するモジュールです。spam を送信するメールサーバの多くは、一度宛先に配送すると送信に失敗しても再送しないと言う特性があります。(通常のメールサーバであれば、何度か送信を試みます。) その特性を利用し、受信したメールを初回時は全て受信拒否します。これにより、spam メールの多くが自動的に届かなくなります。

ただし、これは完全ではありません。踏み台にされた正規のメールサーバから配信される spam は一回目拒否されても再送するからです。

そのため、届いたメールの内容や経由したメールサーバなどの情報を調べて、spam であるかないかを判断するフィルタソフトが必要となります。そこで利用したのが、SpamAssassin です。

SpamAssassin の判断するポイントは、過去に spam を送られたことがある IP アドレスを経由しているかどうか、本文中に spam で宣伝していたことがある URL があるかどうかなどを調べて、それぞれの項目毎に点数を付け、その合計点がある一定の値を超えると spam と判定されメールの本文もしくは表題 (Subject) にそのことを付加したメールを配送するシステムです。