HINES メールシステムについて

髙橋 亮太

北海道大学情報環境推進本部情報環境推進課

IT 推進グループ情報ネットワークチーム

ryo-takahashi@iic.hokudai.ac.jp

1 はじめに

北海道大学では現在、全学的なメールシステム（通称：HINES メール）を独自で構築・運用している。本稿では、HINES メールシステムについて、「システムの構成内容」、「ウィルス・スパムメール対策」、「システムの問題点と今後の構成」に焦点を当てて説明する。

2 システムの構成内容

2.1 メールシステム概要

本学には、我々が管理している HINES メールサーバの他に、各部局・研究室等で独自運用しているメールサーバが多数存在する。そのため、メール通信（Port 25 /tcp）について、学内独自のメールサーバ同士で配送されるメールを除き、一律にウィルス・スパムチェックを実施するために、メールゲートウェイ（以後メール GW と表記する）サーバを設置している。

2.2 メールシステム構成

本学のメールシステム構成を図 1 に示す。

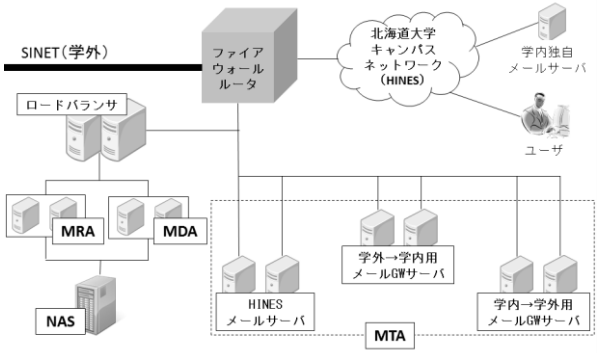

図 1.メールシステム構成

- ロードバランサ…ファイアウォールルータを経由してきた宛先 25/tcp（SMTP）の通信について、送信元 IP アドレスと宛先 IP アドレスによって、各メール GW サーバに振り分けを行う。
- MRA（Mail Retrieval Agent）…HINES メールユーザが POP3/IMAP を利用して、NAS の個人メールディレクトリからメールの受信を行うサーバ。
- MDA（Mail Delivery Agent）…HINES メールユーザ宛に届いたメールを、NAS の個人メールディレクトリに配送を行うサーバ。
- NAS…HINES メールユーザの個人メールディレクトリが保存されている共有ストレージ。
- HINES メールサーバ…MTA（Mail Transfer Agent）として、HINES メール宛のメール配送を行うサーバ。このサーバを通過するメールについて、ウィルスチェックを行う。
- 学外→学内用メール GW サーバ…学外から学内向けへの宛先 25/tcp（SMTP）の全ての通信を一度自分宛として処理し、ウィルス・スパムチェックを行うサーバ。ウィルス・スパムチェック後は、学内の各メールサーバ（HINES メールサーバを含む）にメール配送を行う。
- 学内→学外用メール GW サーバ…HINES メール以外の学内から学外向けへの宛先 25/tcp の通信を一度自分宛として処理し、ウィルス・配送量チェックを行うサーバ。ウィルス・配送量チェック後は、学外の各メールサーバにメール配送を行う。

3 ウィルス・スパムメール対策

3.1 ウィルスメール対策

MTA 機能を持つ 3 系統のメールサーバに、メール用ウィルス対策ソフトを導入し、ウィルスチェックを実施している。ウィルス判定されたメールは破棄し、パスワード付きのファイルが添付されている場合は、ウィルスチェックできなかった旨の警告文を本文に挿入し注意を促している。

3.2 スパムメール対策

学外からのスパムメール対策として、グレイリスト方式による自作フィルタを使用している。グレイリストとは、スパムメールと疑わしきメールに対し、その「送信元メールアドレス・宛先メールアドレス・送信元メールサーバ（IP アドレス)」の組をデータベースに記録して一時拒否し、その後、送信元が通常のメールサーバであれば、メールが自動で再送されてくるので、そのタイミングで配送許可を行うフィルタである。このフィルタにより、ウィルス等に感染した外部の不正なサーバからのメール配送を防止している。

教育機関等からのメールについてはホワイトリストを設定し、グレイリストのフィルタは適用していない。以下に主なホワイトリスト対象の送信元を記す。

- 大学等の教育機関（ac.*ドメイン）
- 日本の教育機関（ed.jp ドメイン）
- 政府機関（go.*ドメイン）
- 日本企業（co.jp ドメイン）
- 携帯メール（docomo.ne.jp/ezweb.ne.jp/ softbank.ne.jp 等）

また、教職員等から依頼があり、明らかにスパムメールの送信元と確認できたものについてはブラックリストを設定し、メール GW サーバにて拒否を行っている。

3.3 メール配送量制限

学内→学外用メール GW サーバでは、送信者 IP アドレス単位で見たときに、1 分間に 500 通を超えるメール送信が行われた場合、該当 IP アドレスの 25/tcp 通信を停止するメールの配送量制限を行っている。ただし、メールサーバとして登録されている IP アドレスについては、メールの配送量制限の対象外としている。この制限により、ウィルス等に感染した学内端末からの学外への大量な不正メール送信を抑止している。

3.4 メール配送数

例として、2013 年 9 月分のメールの配送数を図 2・図 3 に示す。

※学外→学内向けのメール拒否数には、グレイリストによる初回拒否メールの数を含む

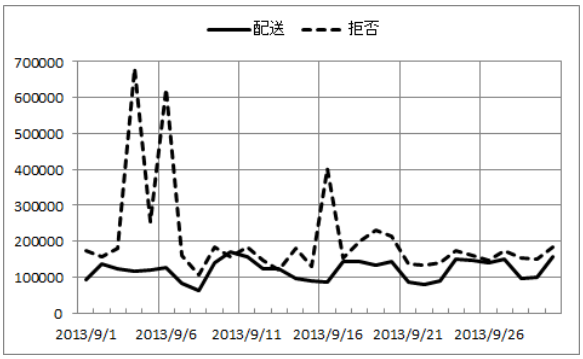

図 2.学外→学内向けメール配送数

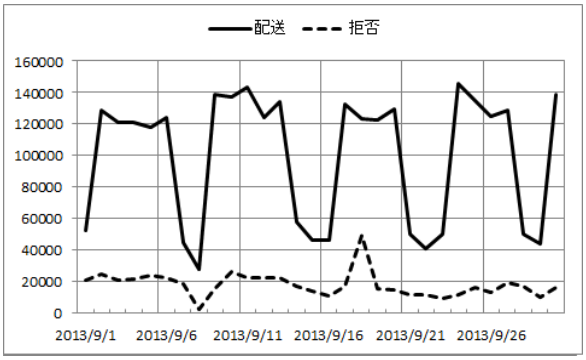

図 3.学内→学外向けメール配送数

4 システムの問題点と今後の構成

4.1 システムの問題点

本学のメール GW サーバを利用したメールシステムには、以下のような問題がある。

① 学内から学外向けへのメールは一度メール GW サーバで処理を行い、改めてメール GW サーバから学外に向けてメール配送を行うため、宛先側から見た送信元の IP アドレスは、全てメール GW サーバのものとなる。そのため、ウィルス感染端末等の不正メール送信により、北大のメール GW サーバの IP アドレスがブラックリスト登録されてしまった場合、学内から当該宛先へのメールは全て拒否されてしまう。

② 多数（12 台）のサーバが物理的に別なサーバとして稼働しているため、管理が煩雑である。

4.2 今後の構成

4.1 節で挙げた問題点に対する解決策として、現在検討している今後の構成を以下に記す。

① 完全透過（ブリッジ）型メール GW アプライアンスの導入

- 現行通りウィルス・スパムチェックを行いつつ、メール送信元の IP アドレスは実際にメールの送信を行う端末・メールサーバのものとすることが可能となる。これにより、仮にメール送信元の IP アドレスがブラックリスト登録されてしまった場合でも、学内にある他のメールサーバ等から送信されるメールに対して影響は発生しない。
- ウィルス・スパムチェックをアプライアンスで実施できるため、メール GW サーバが必要無くなり、管理するサーバの削減ができる。

② 各メール系サーバの KVM 仮想化基盤サーバへの移行

- システム系各種サーバの移行を目的に導入した仮想化基盤サーバ上に、各メール系サーバを KVM によって仮想化して配置することで、サーバの集中管理が可能となる。また、全 4 台の仮想化基盤サーバに、2 台または 4 台ずつ冗長化して配置することで、障害等にも対応できるようにする。

最終的には、計 10 台のサーバ類によるメールシステムの構成を検討している。現行のシステムと比べて 2 台のみの削減ではあるが、KVM による仮想サーバの管理が主軸となるため、より管理しやすくなるものと考えられる。

- メール GW アプライアンス　2 台
- ロードバランサ　2 台
  （KVM による仮想サーバ）
- HINES メールサーバ　2 台
  （KVM による仮想サーバ）
- MDA+MRA を統合したサーバ 4 台
  （KVM による仮想サーバ）

5 まとめ

本稿では、HINES メールシステムについて、3 つの項目に焦点を当てて説明を述べた。近年多様化するウィルス・スパムメール等にも柔軟な対応を行い、今後もメールシステムの安定的な運用を続けられるよう心掛けていきたい。