

メーリングリスト宛メールへの 個人別スパム処理ポリシーを適用可能とする配送システムの構築

Construction of a mailing system with individual user's SPAM policy for mailing lists

増井 健司*
Kenji MASUI

北陸先端科学技術大学院大学†
Japan Advanced Institute of Science and Technology‡

本学に導入されたメールシステムが有するスパムチェッカは、スパムメールへマーキング、スパム専用スプールへ配送、何もしないという処理ポリシーを個人毎に選択可能である。しかし、メーリングリスト（ML）宛のメールはスプールに届くまで一通として配送されるので、個人別ポリシーが有効にならない。そこで、ML 情報と個人別のポリシーを LDAP で参照し、メールを振り分ける配送サーバを構築し、ML 宛のメールにも個人ポリシーが適用されるシステムを構築する。

キーワード：電子メール、SPAM、メーリングリスト

The SPAM checker we have just introduced into our institute can check and mark SPAM mails on the header. The system can also quarantine them when the SPAM policy of the recipient of them is set to "quarantine". However, the system does not comply individual SPAM policy when the SPAM mail is addressed to not a person but a mailing list. In order to solve the problem, we construct a mailing system with individual user's SPAM policy for mailing lists, by building a new server which expands a mailing list address into a list of the members of the mailing list.

Keywords: E-mail, SPAM, Mailing list

1 はじめに

インターネット上にスパムメールが蔓延するようになって久しい。今日では各サイトのメールシステムの管理者は何らかのスパムメール対策を行わざるを得ない状況である。北陸先端科学技術大学院大学（JAIST）では、2005 年 3 月にメールシステムの更新を行い、スパムメール対策を導入した。

この新システムでは、学外から受信した全てのメールに対してスパム判定とウイルス判定をし、スパム判定についてはヘッダへのマーキングおよびスパム専用スプールへの隔離が可能である。これらの動作はユーザ単位で選択可能であり、ユーザの選択は LDAP[1] 上の各ユーザのスパム処理ポリシー属性として保持する。

ところが、メーリングリスト宛のメールについてはユーザ単位でのスパム処理ポリシーに従うことができない。現在運用中のスパム隔離サーバは、宛先のアドレス単位でしか処理ポリシーを選べないため、メーリングリスト単位でのポリシー設定となり、個人別ポリシーの適用ができない。仮に、あるメーリングリスト

*masui@jaist.ac.jp

†〒 923-1292 石川県能美市旭台 1-1

‡1-1, Asahidai, Nomi, Ishikawa 923-1292 Japan.

宛メールを隔離してしまうと、そのメンバとして含まれているユーザが隔離を望んでいない場合であっても、そのユーザのメールボックスに届かないため、そのユーザのポリシーに反した動作となってしまう。これを解決するためにあらかじめメーリングリストのアドレスを全メンバのアドレスに展開することが考えられるが、後で述べる通りシステム構成やリソースの都合上、現在運用中の配送システムの各コンポーネントで直接行うことは難しい。

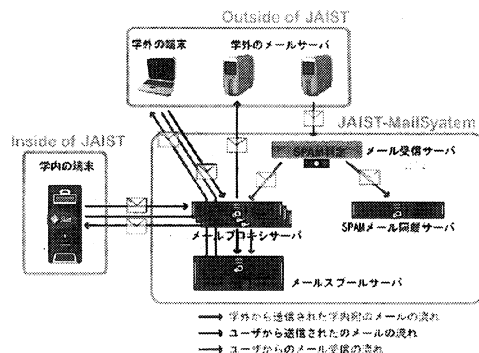
これを解決するために、メーリングリストの展開と個人別ポリシー適用を行う新たなサーバを構築する。この展開サーバはエンベロップTOに指定されたメーリングリストのアドレスをメンバのアドレスに展開し、個人別のポリシー毎に仕訳してスパム隔離サーバと各個人のメールボックスへ配送する機能を持つ。個人別のポリシー設定を有効にできると同時に、エンベロップの展開のみに留めるためメールの配送量の増大を押さえられることが特長である。

なお、スパムという単語はいわゆる俗語であり、UBE または UCE[§] という呼び方が推奨されているが、これらは一般ユーザに対して浸透している単語ではなく、JAIST でもユーザ向け案内は「スパム」と記述している。本稿でもこれに従い UBE/UCE のことを「スパム」と記述する。

2 JAIST メールシステムの構成

JAIST のメールシステムは、2005 年 3 月に旧来のシステムを更新し新しい構成となった。システムは、メール受信サーバ、メールプロキシサーバ、メールスプールサーバ、その他のホストから構成されている。

システムを構成する各サーバは LDAP により統合されており、ユーザ情報、メーリングリスト定義、個人のスパム処理ポリシーなどはすべて LDAP により参照される。この LDAP のマスターサーバはメールスプールサーバが行っており、各メールプロキシサーバはそのレプリカである。また、ユーザ情報などのメールシステムに固有ではない情報は、メールシステム外に



ある一般向けの LDAP マスタサーバと同期しており、これを用いて学内のワークステーションのユーザ管理などが行われている。この同期には Sun Java System Directory Server[2] の持つマルチマスタ同期機能が用いられている。さらに、2006 年 3 月のシステム更新により、Sun Java System Identity Synchronization for Windows が導入され、一般向け LDAP マスタサーバと Windows 用 ActiveDirectory の双方向同期が実現した。これにより、一箇所ですべてデータ更新を行うだけで UNIX ワークステーション、Windows、メールシステムの全てに反映される構成となっており、管理のコストを低減している。

2.1 メール受信サーバ

DNS の MX レコードに登録され、学外からのメールを最初に受けとる役割を果たすメール受信サーバには、IronPort[3] 社の IronPort C30 (図 2) を採用した。IronPort C30 はメール配送に特化したラックマウント型アプライアンスサーバであり、高いメール処理性能、SPAM 判定機能、GUI による設定などが特徴である。

JAIST ではこれを 2 台導入し、電源、ネットワーク、物理的ロケーションがすべて異なる場所にそれぞれを配置して運用している。

[§]Unsolicited Bulk/Commercial E-mail

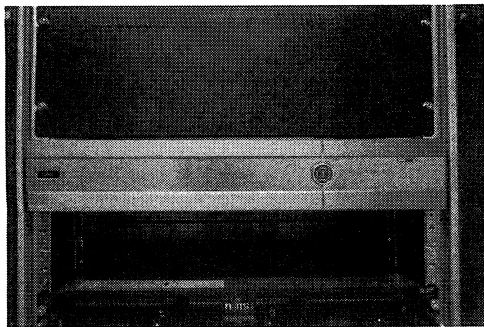


図 2: IronPort C30

2.2 メールプロキシサーバ

メールプロキシサーバおよび次節で説明するメールスプールサーバには、Sun Microsystems 社の Sun Java Messaging Server 5.2 (SJMS)[4] を採用した。メールプロキシサーバはメールスプールサーバにアクセスする際に用いるプロキシの役割を果たす。ユーザから見たときの POP[5] や web-mail などの接続先はこのサーバとなる。

JAIST ではメールプロキシサーバを 3 台体制で運用し、F5 社 BIG-IP 2400 をロードバランサとして用いることにより高いメール処理性能と高可用性を確保している。メールプロキシサーバのハードウェアには Fujitsu PRIMEPOWER250 を採用した。

2.3 メールスプールサーバ

メールスプールサーバは、ユーザのメールボックスを格納するサーバである。高い信頼性が求められるため、2 台で Active-Standby のクラスタ構成としている。メールスプールサーバのハードウェアには Fujitsu PRIMEPOWER450 を採用した。

2.4 スпам隔離サーバ

メール受信サーバによりスパムと判定されたメールは、LDAP 上の個人別ポリシーに従って処理される。

受け取り人がスパムを隔離するポリシーを持っていた場合、スパムメールはスパム隔離サーバへ配送され、メールスプールサーバへは配送されない。各ユーザへはスパムメールのリストが定期的に送信される。ユーザは web ブラウザを用いてスパム隔離サーバへアクセスすることにより、格納されているメールを参照することが可能である。

スパム隔離サーバのソフトウェアには、IronPort のオプション製品である Brightmail Quarantine を採用した。IronPort とスパム隔離サーバの間の配送には SMTP[6, 7] が用いられるため、他のメール配送ソフトウェアで構築することも可能である。ハードウェアとしては、Fujitsu PRIMEPOWER250 を採用した。

2.5 その他のホスト

メールプロキシサーバでは、SJMS の制限により POP before SMTP[8] と SMTP 認証 [9] を同時にサービスすることができない。そのため、POP before SMTP 専用のメールプロキシサーバを別に 1 台用意した。また、JAIST のユーザが学外から JAIST メールシステムを経由してメールの送受信を行うために、学外専用メールプロキシサーバも別に 1 台用意した。

メール受信サーバは LDAP 上の各ユーザのスパム処理ポリシーを参照する機能があるが、そのポリシーを編集する機能は持っていない。そのため、LDAP 上のポリシーを個人の権限で編集するための web システムを構築し運用している。

3 メーリングリスト宛スパムの問題点

前節で述べた JAIST メールシステムの構成のメリットは、メール受信サーバに LDAP を用いたユーザの存在チェックおよびスパム判定機能を持たせていることである。これにより、user unknown となるメールや、スパムメールを後段の配送系へ流すことなく処理できるため、メール管理者へ届くバウンスメー

ルの数を大幅に減らしたり、メール配送系の負荷を下げる事が可能となった。

ただし、この構成ではメーリングリスト宛に届いたスパムメールを効率的に処理することができない。一般に、メーリングリスト（エイリアス）の展開はメールスプールサーバで行うことが常である。本システムでも同様の設定となっているため、メール受信サーバの段階ではそのメーリングリスト宛のメールを受けとる個人が確定しておらず、個人のスパム処理ポリシーを参照することができない。

メール受信サーバでエイリアスを展開する方法も考えられるが、本システムで採用している IronPort C30 はエイリアス展開をする機能は持っていないため実現できない。また、全てのメールのエイリアスを展開する負荷やその後の配送系の負荷も問題となる。メール受信サーバには信頼性と迅速なレスポンスが求められるため、負荷の高い処理を追加するのには不向きである。

4 メーリングリスト展開サーバ

前節で述べた問題を解決するために、メーリングリスト宛スパムメールを展開するサーバを構築する。

4.1 展開サーバの設計

設計のポイントは以下の通りである。

1. スパムと判定されたメーリングリスト宛メールのみが入力される。
2. メーリングリストの展開を行い、ポリシーの一致するユーザ宛にまとめて一通として配送する。

スパムと判定されたメーリングリスト宛メールのみを展開サーバに入力するようメール受信サーバである IronPort を設定する。IronPort はスパム判定結果および LDAP 上の属性を参照し配送先を決定できるため、あるアドレスがメーリングリストか否かを示す属性を LDAP 上に用意すれば実現可能な設定で

ある。この設定には、構築した展開サーバに何らかのトラブルが生じた場合でも、スパムメール以外のメールの配送に影響が及ばないという利点がある。

2 番目のポイントについては、配送量を膨大にしないための工夫である。エンベロープのみ展開し、本文は一通のまま配送すればメールの配送量を押さえることができる。

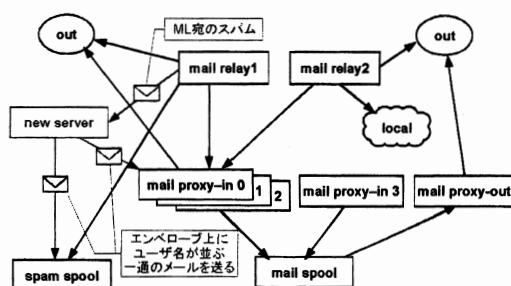


図 3: 展開サーバ導入後の構成

4.2 展開サーバの動作

メールが入力されると、展開サーバはそれをキューイングし、以下の流れで処理を行う。

1. メーリングリストが有効かどうか調べる。メーリングリスト名で LDAP を検索し、属性 inet-MailGroupStatus の値が active であることを確認する。active でなければメール配送はそこでエラーとなる。
2. メーリングリストのメンバー一覧を LDAP から得る。
3. SJMS のメーリングリストのメンバー定義には外部メンバと内部メンバという区分があり、内部メンバは RFC822[10, 11] のメールアドレス形式ではない。これを変換するため、内部メンバの

れないが、メーリングリストとして定義しておけば、メールプロキシサーバ向けに発信するメール（マーキングのみ希望するメンバ宛）のメールは、エンベロープに展開結果を並べなくても、元のメーリングリストから生成した、マーキングを希望するユーザだけを含むリスト宛に送信すれば、メールスプールサーバ上で展開されて配送されるため、エンベロープが長くならないというメリットがある。

ただし、スパムスプール側の仕様により、スパムスプールへ送るメールはエンベロープに展開されたアドレスを並べておく必要がある。もちろん、スパムスプールはSMTPでメールを受けとるため、メーリングリストの展開を行うプロキシを作成してスパムスプール上で動作させれば、ネットワーク上を流れるエンベロープの長さを抑えられるが、最初のバージョンではとりあえずスパムスプール向けのメールは展開して送ることとする。この場合でも、たとえばマーキング・隔離を希望するユーザ数が半々だった場合、 $L * N/2 + L = 1020$ バイトと、展開後のエンベロープの長さをほぼ半減できる。

6 実装状況

現在、メーリングリスト展開サーバの実装を行っている途中である。実装にはC言語を用いている。開発用システムはSun Blade 1500、Solaris9の環境となっている。システムが完成した後は、テスト運用の後、PRIMEPOWER250クラスのハードウェアを用いて実運用を行う予定である。

7 まとめ

本稿では、メーリングリスト宛のスパムメールにも個人別スパム処理ポリシーの適用が可能となるように、エンベロープの展開を行うサーバを設計した。

今後は、展開サーバの実装を完了させ、テスト運用を行うことによって実際のメール処理性能や、LDAPサーバに与える負荷の度合いを測定する予定である。

参考文献

- [1] M. Wahl, T. Howes, and S. Kille. *Lightweight Directory Access Protocol (v3)*, (1997). RFC2251.
- [2] Sun Microsystems, Inc. *Sun Java System Directory Server*.
<http://jp.sun.com/products/software/javasystem/directoryserver/>.
- [3] IronPort Systems, Inc. *IronPort*.
<http://www.ironport.com/jp/>.
- [4] Sun Microsystems, Inc. *Sun Java System Messaging Server*.
<http://jp.sun.com/products/software/javasystem/messagingserver/>.
- [5] J. Myers and M. Rose. *Post Office Protocol – Version 3*, (1996). RFC1939.
- [6] J. Postel. *Simple Mail Transfer Protocol*, (1982). RFC821.
- [7] J. Postel and J. Klensin(Editor). *Simple Mail Transfer Protocol*, (2001). RFC2821.
- [8] R. Gellens and J. Klensin. *Message Submission*, (1998). RFC2476.
- [9] J. Myers. *SMTP Service Extension for Authentication*, (1999). RFC2554.
- [10] David H. Crocker. *STANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGES*, (1982). RFC822.
- [11] P. Resnick(Editor). *Internet Message Format*, (2001). RFC2822.