Postfix を使った簡易 spam メール対策

岡田哲治*、桝田秀夫†　　京都工芸繊維大学

「概要」

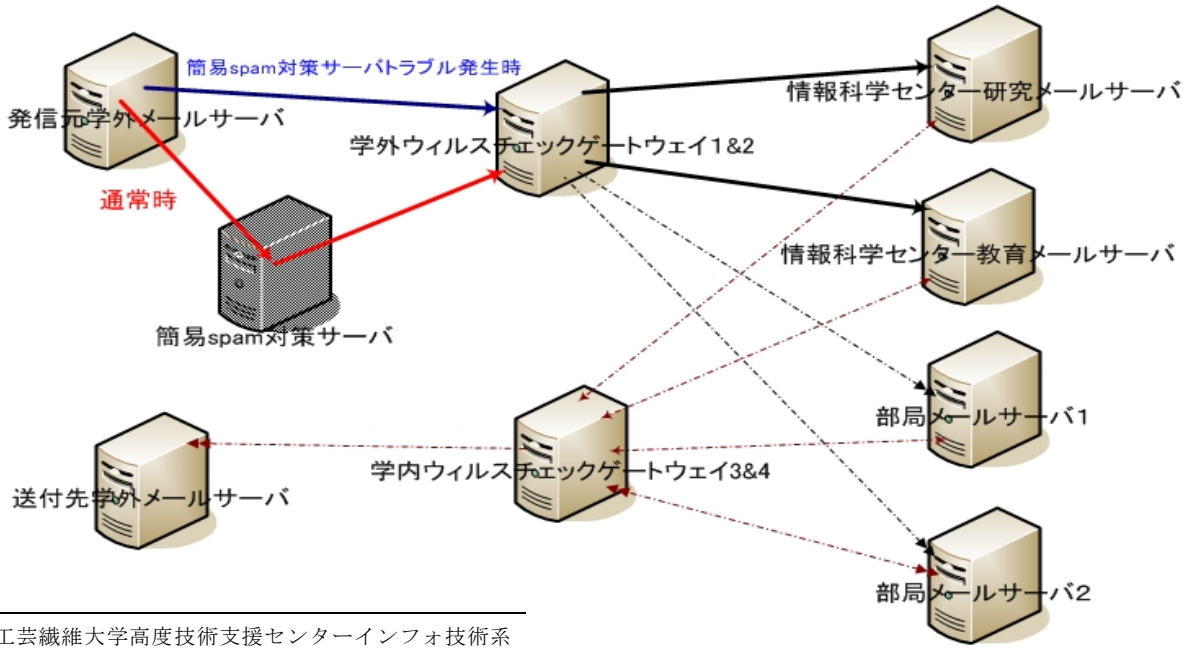
spam メールは増加の一途をたどっており、利用者にとっては必要なメールを見逃してしまったり、その処理に時間を取られたり、厄介な存在である。またメールサーバを管理する立場からは、大量の spam メールは、サーバの負荷を上げ、ログの量や管理メールが増えてしまうなど、まさに厄介者である。どこの大学でも同じ悩みと思うが、その対策に対してなかなか完璧なものが無いのが実情と思われる。現在 spam メールに対応するアプライアンスが多く存在するが高価で、チューニングの為に人手が必要といわれている。そこで「お金も人手もできるだけかけない」ということで、メールサーバの MTA として良く使われている Postfix の機能を使った簡易な spam メール対策をテスト的に一部のドメインに導入し、運用した結果を報告する。

１．本学のメールシステム

本学は学生約 4,300 人、教職員約 500 人の工科系大学で、メールサーバの構成は以下の通りである。

学外向けウィルスチェックゲートウェイ(mailgw1,2)	学外からのメールのウィルスチェック
学内向けウィルスチェックゲートウェイ(mailgw3,4)	学内からのメールのウィルスチェック
研究ドメインメールサーバ(rmail)	教職員用メールサーバ
教育ドメインメールサーバ(email)	学生用メールサーバ
事務ドメインメールサーバ(jmail)	事務職員用メールサーバ
各部局ドメインメールサーバサーバ(xxx-mail)	各部局用メールサーバ

各ドメインのメールは、最初に学外向けウィルスチェックゲートウェイを通り、ウィルスチェックを受けてから、各ドメインのメールサーバに配送される。また各ドメインメールサーバから送信されたメールは学内向けウィルスチェックゲートウェイで検査を受けてから配送される。



＊京都工芸繊維大学高度技術支援センターインフォ技術系

†京都工芸繊維大学情報科学センター次長・准教授

２．導入した簡易 spam メール対策システム

今回テストシステムは、「お金も、人手もほとんどかけずに実施する」ということを前提に、前システム時代にウィルス対策用に購入し、現在遊休中のサーバに、フリーの Linux「CentOS」をインストールし構築した[1]。

サーバ　：Express5800/120Rb-2
HDD　　：36GB×3（RAID1 36GB ミラーリング , 36GB 1 台予備）
メモリー：512MB

この Linux サーバに Postfix を稼働させ MTA とし、学外から到着するメールをまずはこの対策システムを経由させてから、学外向けウィルスチェックゲートウェイを通り、メールサーバに配送するようにした。現在テスト中のメールドメインは、情報科学センター管理者ドメイン（2007 年 6 月 4 日から)と教育ドメイン（2007 年 12 月 26 日から)である。

Postfix の環境設定は、デフォルトでは/etc/postfix/main.cf である。この main.cf に以下の設定を施している。

２．１　SMTP 接続時に関する設定　（ smtpd_client_restrictons ）

①Check_client_access regexp:/etc/postfix/client_access

「/etc/postfix/client_access」を検索して、接続の可否を決定する。

いわゆる **Greet Pause の設定**である。学外からの SMTP クライアントに対して、SMTP セッション確立後の「220 ホスト名」のグリーティングバナーを送るまでに遅延をかける。次々と連続で配信してくるクライアントに対して、遅延をかけることによりメール送信をあきらめることをねらっている。現在は 100 秒の遅延をかけている。

/etc/postfix/client_access の内容

```
/^localhost/     sleep 0
/kit¥.ac¥.jp$/   sleep 0
/^133¥.16¥./     sleep 0
/^.*/            sleep 100
```

②reject_unauth_pipelining（デフォルト応答コード:503)

Postfix が実際に SMTP コマンドパイプライニングをサポートしていることを知る前に、クライアントが SMTP コマンドを送ってきた場合に要求を拒否する。これは配送を高速化するために不正に SMTP コマンドパイプライニングを使うバルクメールソフトウェアからのメールを止めることをねらっている。

２．２　HELO 受信時に関する設定　（ smtpd_helo_restrictons ）

①reject_invalid_hostname　（デフォルト応答コード:501)

HELO とともに送付されてきたホスト名の書式が有効でない場合に拒否する。

②reject_unknown_hostname　（デフォルト応答コード:450)

HELO,EHLO のホスト名が DNS A または MX レコードを持たない場合に拒否する。

③reject_non_fqdn_hostname　（デフォルト応答コード:504)

HELO,EHLO ホスト名の文法が、完全修飾ドメイン形式(RFC)で無い場合に拒否する。

２．３　HELO コマンドの要求（ smtpd_helo_required=yes ）

SMTP クライアントに対して SMTP セッションの最初が HELO,EHLO で無かった場合に拒否する。

２．４　宛先情報(RCPT To)受信時に関する設定（ smtpd_recipient_restrictions ）

①reject_unauth_destination　（デフォルト応答コード:554）
第三者中継(オープンリレー)を防止する。

②reject_unknown_recipient_domain　（デフォルト応答コード:450）
宛先アドレスが DNS A もしくは MX レコードを持たない場合に拒否する。

③reject_unverified_recipient　（デフォルト応答コード:450）
宛先アドレスがバウンスするとわかっている場合や、受信者アドレスの配送先に到達できない場合に要求を拒否する。

３．これらの設定による拒否状況

2007 年 12 月 26 日より 2008 年 8 月 11 日までの maillog より、今回の設定による拒否状況を以下にまとめる。

総コネクションレコード数	４６４，０２９
ウィルスチェックゲートウェイに送付できたメール数	９７，２４９

各設定によるリジェクト数とコネクションレコード数全体からの割合				
２．１	①	Greet Pause	１５８，４８３	３４．２％
	②	不正 SMTP コマンドパイプライニング防止	３８２	０．１％
２．２	①	HELO(EHLO) ホスト名書式チェック	１，１１７	０．２％
	②	HELO(EHLO) ホスト名 DNS チェック	１２１，７０６	２６．２％
	③	HELO(EHLO) ホスト名文法チェック	０	０　％
２．３		SMTP セッションの先頭が HELO(EHLO)?	０	０　％
２．４	①	第三者中継(オープンリレー)を防止	４８３	０．１％
	②,③	宛先アドレスチェック	１８０，１６１	３８．８％

予想通り宛先アドレスが不明で User Unknown なるもの(2.4②,③)が一番多く、いかに適当なアドレスをつけて送付されてくるメールが多いということがことよくわかる。また Greet Pause によりコネクションを張れなかったレコード(2.1①)も多く、RFC に従わずに大量メール配信をしている事例も多いことが伺える。さらに HELO(EHLO)のホスト名チェックで引っかかることも多く、spam メールを送付してくる SMTP クライアントがいいかげんな管理というか、隠蔽するために DNS にすら登録されていないホストが多いことが伺える。この３点チェックだけでも相当数の spam メールを拒否できたと見られるが、通過したメールの中にどれだけ spam メールが含まれているかというところまでの調査が難しく今後の課題である。「総コネクションレコード数」が「ウィルスチェックゲートウェイに送付できたメール数」と「各設定によるリジェクト数」の合計より少ないが、これは、１コネクションで送付メール数が１通とは限らないためと考えられる。

４．導入した Postfix 簡易 spam メール対策システムの特徴

第１には、spam メールの配送と推測される通常のメールの挙動と違ったもの、またおかしい情報を持ったメールを大量にくい止めている。その成果は確実にある。現実にセンター管理ドメイン宛の spam

メールは、確かに少なくなった。特に postmaster 宛の User Unknown のメールが極めて減少した。

第２には、このサーバにトラブルが発生しても、このサーバをスルーし、簡易 spam メール対策が実施されないだけで、メールの配送には何の問題も生じない。実際には DNS の MX のプリファレンス値で簡易 spam メール対策システムを上位の配送先として指定している。

○spam メール対策サーバを経由しないドメイン(□□□)のメールサーバの MX レコード

□□□.kit.ac.jp　　mail exchanger = 10　mailgw2.kit.ac.jp.

□□□.kit.ac.jp　　mail exchanger = 10　mailgw1.kit.ac.jp.

○spam メール対策サーバを経由するドメイン(△△△)のメールサーバの MX レコード

△△△.kit.ac.jp　mail　　exchanger = 100 mailgw2.kit.ac.jp.

△△△.kit.ac.jp　mail　　exchanger = 100 mailgw1.kit.ac.jp.

△△△.kit.ac.jp　mail　　exchanger = 10　spamgw.kit.ac.jp.

第３には、管理負担が少ないことである。Postfix を使った対策でもホワイトリスト等の作成などより個別に対応した設定を行うことは可能であるが、このサーバはそれらの管理コストがかからないことをコンセプトにしている。

第４には、導入コストも極めて少なくてすむ。今回は遊休サーバを活用したが、サーバがあれば、OS はフリーの Linux、CentOS をダウンロードし、Postfix もダウンロードしたので、ソフトもコストがほとんどかからない。

第５には、このサーバで明らかに怪しい SMTP の通信を一定数くい止めることができるため、後段のメールサーバの負荷を下げる効果がある。

５．今後の課題

運用上で生じた問題として、Greet Pause にひっかかり、メールが到着しないというものがあった。このケースでは、２．１①の/etc/postfix/client_access で、該当サーバの待ち時間を 0 にして回避した。このようにエラーとなっている状況が、spam メール送信に起因するのか、相手サーバの設定の問題なのか手間をかけずにチェックする仕組みが求められる。

６．おわりに

spam メールが全体の５割を超え、週末等には 7-8 割にも達することもあり、本学でも本格的アプライエンス導入の声は大きくなっている。しかし、いくら高価なものを導入しても誤検知もあり、かつ日々の管理コストがかかってくることから、現在本学では、利用者のメールクライアントソフトの spam メールフィルター機能の活用を呼びかけている。今の技術では完璧なものがなく、大学のゲートウェイで導入する場合、誤検知時の扱いの合意も必要になってくると考えられる。しかし今回安価で管理コストがほとんどかからないもので対応できるものならとテスト稼働させた。次期システムの導入は、2010 年 3 月であり、その時期には本格的何らかの対応を検討する必要がありますが、それまでの一定の下地になることを期待している。

[謝辞]

今回のテストシステム導入にあたり、本学情報科学センター次長の桝田准教授にご指導をいただき、大変お世話になりました。感謝申し上げます。

[参考文献]

[1] 桝田 秀夫, 落合 優:「メールゲートウェイにおけるバウンスメール発生の抑制法とその評価」,FIT2007 , LL-003, pp.369-372 (2007).