ウィルス、SPAM 検出機能を持つメール中継システムの構築と運用
Construction and Operation of the mail relay system with virus and SPAM detecting function

本田修啓
Naohiro Honda
福島大学総合情報処理センター
Fukushima University Information Network Center

概要

福島大学では、複数運用されている学系等組織毎のメールサーバとインターネット間に配置し、コンピュータ Virus,Worm および SPAM を検出除去機能を有するメール中継システムを平成 16 年 9 月に構築し、改良を加えながら運用を行なっている。このシステムはインターネットとの通信を受け持つ 2 台のサーバと Virus,Worm,SPAM の検出と除去を行い学内メールサーバにメールを中継するゲートウェイの 3 台から構成されており、VRRP 等による冗長性とフリーソフトを積極的に活用した経済性を特徴としている。本稿では上記構築と運用状況、運用を通して得られた Virus および SPAM 流入状況について報告する。

キーワード

電子メール、SPAM メール対策、コンピュータウィルス、メールゲートウェイ

1 はじめに

福島大学は、学生および教職員あわせ約 4500 名のメールユーザがおり、全体で 1 日あたり約 7000 通（平日）/3000 通(休日)のメールをインターネットから受信し、約 2000 通のメールを発信している。これらは学類等の組織毎のメールサーバがユーザ向け POP/IMAP サービスを提供している。これらのサーバとインターネット間に配置されるメールゲートウェイとして中継システムを構築した。

構築の目標は、Virus/SPAM 対策方式の共通化と効率化、メールシステム信頼性の向上、セキュリティの向上である。これらを低コストで実現することもあわせて目指した。

2 システム構築

2.1 ネットワーク基本構成

中継システムは 3 台のサーバから構成されている。(図-1)

ネットワーク冗長性を確保する目的で、直接インターネット上のメールサーバと SMTP にてメール送受信処理を行なう外部配送サーバを 2 台 Firewall の外側に設置している(outmsv1,outmsv2)。これらはそれぞれ学術インターネットである TOPIC および商用インターネットである Plala を上流としており、一方のネットワークが利用できない場合あるいは一方のサーバメインテナンス時でも、DNS MX RR の設定によりメール受

信の冗長化がおこなえる構成としている。

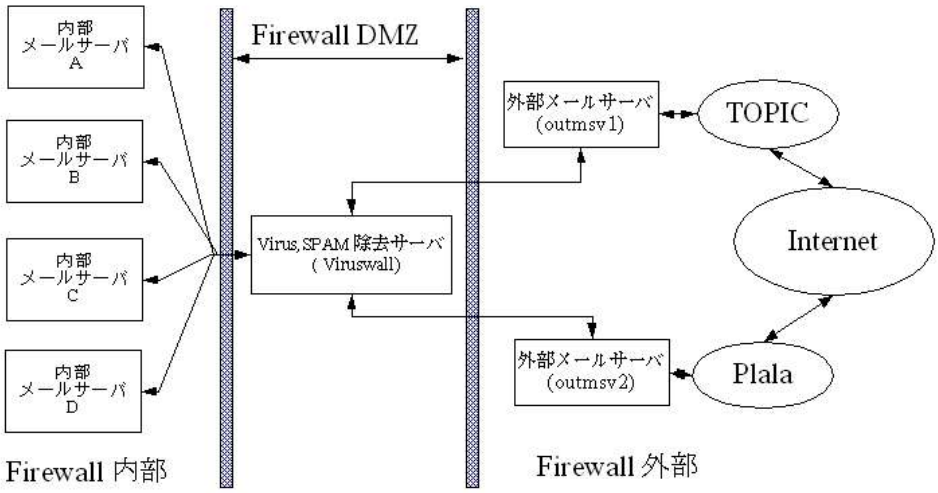

図-*1* メール中継システムの構成

外部配送サーバと既存の内部メールサーバの間に、Virus/SPAM 検出削除機能を有するゲートウェイサーバ(Viruswall)を設置している（Firewall DMZ)。外部配送サーバとゲートウェイサーバ間は、専用の Private network を構築し、この閉じたネットワークを使用して通信する構成としている。また 2 台の外部配送サーバの NIC で VRRP を構成することで、メール送信時の冗長性を高めている。

2.2 ハードウェア構成

3 台のサーバはハードウェアとしては全く同じ構成の NEC 製 19 インチラックマウント型 PC サーバ(Express5800/1100GR-1b)を使用した。主要スペックを表-1 に示す。

筐体	19 インチラックマウント 1U
CPU	Pentium 4 (3GHz)
メモリ	256M byte
NIC	1000BASE-TX 2 個 (on board)
HDD	80Gbyte

表-*1* ハードウェア主要スペック

この PC サーバは標準で 2 個の NIC を内臓しているが、うち 1 個を 3 台間の Private Network 構築用に、他の 1 個を一般の通信用に使用している。

2.3 ソフトウェア構成

OS を含め利用した主要ソフトウェアを表-2 にまとめる。主に無料で利用可能なオープンソフトを採用したが、ウイルス検出・除去については市販の製品を選択した。また管理用スクリプトは自作である。

機能	ソフトウェア名	備考
OS	Linux	Fedora Core 2
MTA	Qmail-1.03	Netqmail-1.05
AutiVirus	Vexira antivirus for Mail server	Viruswall
AntiSPAM	Spamassassin-3.0	外部配送サーバ
NTP	ntpd-4.2.0a	
VRRP	Vrrpd-1.0	外部配送サーバ

表-*2* 主要ソフトウェア一覧

2.2.1 Message transfer Agent

3 台のサーバにおいて MTA として qmail を使用した。利用パッケージは netqmail-1.05 である。

内部メール配送については、直接 IP アドレスによる静的配送とし、DNS 不調の影響を受けないよう配慮

した。ゲートウェイサーバ(Viruswall)については、SMTP 接続可能な IP アドレスを関係する学内メールサーバのみに制限し、セキュリティを高めた。送信処理の流れを図-2、受信処理の流れを図-3 に示す。

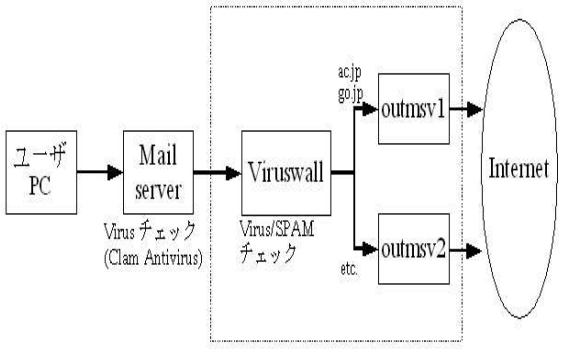

図-*2* 送信処理の流れ

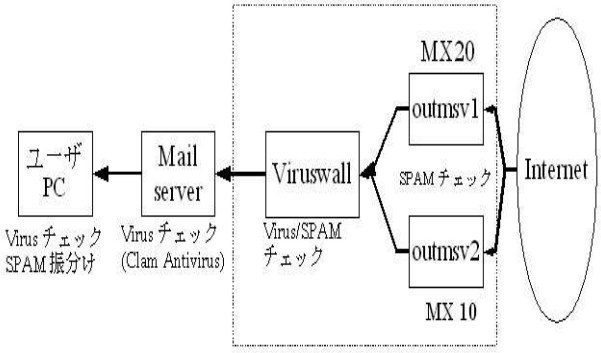

図-*3* 受信処理の流れ

2.2.2　Virus 検出・除去ソフトウェア

本学では、内部メールサーバおよびクライアント PC にも、Virus 対策ソフトの導入を推奨している。これは、複数の手段を併用することで、より安全性がより高める狙いである。例えば総合情報処理センターではメールサーバにも Clam Antivirus を導入している。データベースを同一にする Virus チェックを複数通過させるより、異なるデータベースのチェックを行なうことでより安全性が高まると考え、中継システムの Virus 対策ソフトウェアは、Virus データベースとして、クライアントやメールサーバ用として学内で利用されていなかった米 Central Command 社製 Vexira Antivirus for Mail server を採用した。

データベース更新は附属プログラムを利用し 1 時間ごとに更新するよう設定した。

2.2.3　SPAM 検出・除去ソフトウェア

オープンソフトである spamassassin を利用することにし、外部配送サーバ 2 台にそれぞれ導入を行なった。Vexira Antivirus for Mail server のバージョンアップにより、SPAM 検出除去機能が付加されたため、現在はこちらをメインに運用している。Spamassasin については 6.8 以上のポイントで[SPAM]文字列を Subject:に追加し、ユーザ MUA のフィルタ機能で必要に応じて対応するようにしている。また Vexira では、SPAM データベースを信頼し該当メールを「削除」する設定としている。

2.2.4 セキュリティ関係

セキュリティについては外部配送サーバが Firewall 外に配置されることを配慮し、不要サービスの停止、IPchains による TCP/IP アクセス制限、SMTP については tcpserver も併用して要塞化を図っている。

2.2.5　ログ関係

検出 Virus, SPAM 件数等について、統計処理を行なう Perl script を作成した。毎日夜中に自動実行し、管理者あてメールとして報告するようにしている。

3 運用実験

平成16年10月からVirusチェックを中心に試験運用を開始した。学内メールサーバの設定変更(DNS,静的配送化)を各管理者の協力を得ながら実施した。またSMTP配送を中心とするネットワーク系の調整をあわせて行なった。平成17年2月より、SPAM削除機能を有効にし本格運用を開始した。また必要に応じてスクリプトを作成し、運用状態および統計情報を取得できるようシステム改善を実施しながら、現在も運用実験を行なっている。平成18年8月中旬まで、ほとんど停止することなく順調に作動している。(表-3)

	2月	3月	4月	5月	6月	7月
Virus/WORM	5153	3717	3861	5285	3871	7616
SPAM	18883	18257	17046	28142	31691	42427

表-*3 Virus / SPAM* 検出状況

3.2　Virus検出と除去状況

検出virusの種類別統計を表-4にまとめた。ゲートウェイサーバ(Viruswall)を通過したにもかかわらず、メールサーバのvirusチェック(Clam Antivirus)で検出される状況もまれにPhishing系を中心に見受けられるが、主要Virusに対する大きなチェック漏れは発生していない。

	2月	3月	4月	5月	6月	7月
Exploit.IFrame.B	1555	916	1043	1211	814	844
HTML.Bankfraud	34	150	35	16	3	33
Bagle	76	19	19	0	0	9
Bugbear.B	1	1	3	1	0	3902
Klez.H	13	10	10	20	19	3
Lovegate	25	2	8	362	4	14
Mabutu	0	0	0	14	8	10
MyDoom	12	3	0	0	6	34
MyTob	0	0	87	753	715	393
NetSky	3433	2616	2654	2899	2280	2366
Etc.	4	0	2	9	22	6
合計	5153	3717	3861	5285	3871	7614

表-*4* 検出した *Virus* 一覧

3.3　SPAM検出と除去状況

月別SPAM検出状況を表-5にまとめた。インターネットから受信するメールの20～30%はSPAMとして除去されているが、抜けてくるメールも少なくない。いくつかの日本語メールマガジンがspamassassinでSPAM判定されること、およびVexiraが空白Subjectメールを削除すること等が運用を通して判明した。

	5月	6月	7月
メール送信件数	39001	41708	44993
メール受信件数	131125	140370	142335
SPAM除去件数	28142	31698	42427
SPAM比	21.5%	22.6%	29.8%

表-*5* 月別 *SPAM* 検出状況

3.4　過負荷試験

平成17年7月にVirusに感染したと思われる米国のPCから集中豪雨的なメール送信があったがシステム異常は発生しなかった。実運用開始後のシステムでは、評価のための過負荷試験は行いにくいが、システムの実用性を評価する上でよい「試験」となった。このときの状況を表-5にまとめる。

受信開始	2005/7/16 00:04:29
受信終了	2005/7/16 00:29:35
受信メール数	3898
分平均	457.37
感染ウィルス	I-Worm.Bugbear.C
送信元	1台　(U.S.A)

表-*3* 7月 *16* 日に発生した大量 *Virus* メール

1 まとめと今後の課題

PCサーバをハードウェアとしオープンソフトおよび比較的安価な市販製品を使用した Virus、SPAM対策システム構築の1例を報告した。インターネットから学内に配送されるメールについて、統一的に Virus/SPAMのチェックが行なえること、Firewallの外側に配送専用サーバを設置したことで、内部メールサーバ

の安全性が高まったこと、インターネットメールの大学全体の量的な把握が可能となったことが、Virus およびSPAM除去という本来の効果と並んで大きなメリットであったと感じている。ただし日本語SPAM除去に関しては、漏れてくるメールが少なくなく、この面での機能を向上させることが今後の課題である。

2 参考文献およびURL

[1] Dave Sill: The qmail Handbook ISBN 1-893115-40-2
[2] http://www.redhat.com/fedora/
[3] http://www.qmail.org/
[4] http://www.qmail.jp/
[5] http://www.centralcommand.com/index.html
[6] http://spamassassin.apache.org/
[7] https://sourceforge.net/projects/vrrpd/