実施報告

横浜キャンパスメールサーバの機能強化

萩原　拓郎

家庭や企業でのインターネット利用が進み，生活の様々な場面で当たり前に利用されるようになってきている．これに伴い電子メールの重要性が増すと共に，メールサーバ運用に対する要求も厳しくなってきた．拡大を続けている spam メール被害に対する対策およびメールサーバの可用性向上のための機能強化について報告する．合わせて現在対応が必要となってきている問題点についても指摘する．

キーワード：spam メール，メールサーバ，WebShield，可用性向上

1　spam メール対策実施

1．1　背景

国内でも年々spam メール（以下単に spam）の送信数が増加しており，横浜キャンパスでも受信数が増えてきた．spam とは受信者の意思と関係なく無差別に送られてくる迷惑メールである．受信者は spam により，不快な思いをしたり，通常の電子メールのやりとりを妨げられたり，詐欺などの危険にさらされる．

被害の規模を大雑把に推定するため，横浜キャンパスの 2500 のユーザが各自 spam を削除するために毎日１分費やしたとすると，キャンパス全体では１ヶ月で 1250 時間が spam 処理に費やされることになる．たとえば時給 1000 円で換算すると，2500×30×1000÷60=毎月 125 万円になる．こうした被害を削減するために，キャンパスのメールシステムにおいて spam 対策を実施した．

spam 対策として，利用者の PC にて利用できる対策がいくつか存在している．spam 対策ソフト，ウィルス対策ソフトの spam 対策機能，電子メールソフトの spam 対策機能であるが，こうしたものは利用者それぞれに費用負担やソフトウェア変更の負担がかかるためキャンパス全体として実施することは難しい．そこでキャンパスの全ユーザをカバーすることのできる，メールサーバ用 spam 対策システムを導入した．

1．2　対策の詳細

spam 対策を行うのはウィルス対策システムで，これは直接外部と電子メールのやりとりを行う中継サーバと，直接ユーザ PC と電子メールのやりとりを行う送受信サーバの中間にある．

本キャンパスで導入しているウィルス対策システムは，McAfee WebShield アプライアンス e3100 の２台構成となっており，ソフトウェアのバージョンアップにより spam 対策が利用可能となった．このアプライアンスでは，メーカの提供する spam の特徴と電子メールの学習によって電子メールの spam らしさ(spam レベル)を求め，一定以上の spam レベルの電子メールを spam と判断する．spam と判断された電子メールの件名の先頭には"[spam]"と挿入され，受信者へ届けられる．

受信者へ届けられた電子メールは，件名の先頭にある文字列"[spam]"をキーとして，利用者ごとに振り分け処理を行い自動的に処理される．メールサーバシステムにて spam を廃棄しないのは，spam ではないものを spam であると誤って処理する危険性があるとともに、サーバ管理者がユーザの通信の自由を侵害することの懸念に慎重に対処すべきとの本学部情報システム委員会の決定にもとづくものである．そもそもどの電子メールを spam と判断するかは利用者ごとに異なるため，一律に処理したのでは spam でないものを spam であると誤って処理する可能性がある．こうしたものを利用者側で処理できるようにする必要があるために件名に文字列"[spam]"を挿入して受信者へ配信している．

また，spam であるかどうかの判断において，判断基準を安全側へ振って spam を spam ではないと判断してしまう可能性を増やす代わりに，spam ではないものを spam と判断する危険性を減少させている．

1．3　対策の効果

spam 被害の効果について述べる．武蔵工業大学環境情報学部・環境情報学研究科（横浜キャンパス）の全ての電子メールは横浜キャンパス内ネットワーク（YC-NET）の spam 対策サーバを経由して配送されるため，ここを通過した電子メール数と，検出された spam の数について比較を行った．データの用意できた 2006/01/01 から 2006/02/14 までの，電子メール数，ウィルスメール数，spam およびその全体に占める割合を以下に示す．

HAGIWARA Takuro
武蔵工業大学横浜事務室情報メディアセンター事務課技術員

表１　spam 対策システムでの spam 検出状況

年月	総数	ウィルス	率[%]	spam	率[%]
2006/2	92177	683	0.74	43252	46.92
2006/1	233504	1645	0.70	76153	32.61

※2006/2 はデータの用意の都合から 2006/02/01 から@2006/02/14 まで
※1 月のウィルス数および spam 数は一部データの欠落があり，実際にはより多いはず

上記の結果から分かるとおり，YC-NET で流通する４割から５割近くの電子メールが spam で占められている．一方，危険性は spam より高いと考えられるもののウィルスメールの数は非常に少ない．サーバ全体としては多数の spam を処理することができていることが分かる．

では実際に利用者への効果はどのようになっているのだろうか．受信者が受け取り，spam であると判断した全電子メール数のどれだけが，spam であると処理されていたか見ることで効果の概要を得られると考えられる．ここでは筆者へ届いた電子メールから spam を分別し，spam のどれだけを spam 対策サーバが spam であると判定していたかを集計した結果が下記である．

表２　spam 判定の精度

	数	割合[%]
非 spam 判定	329	14.80
spam 判定	1894	85.20
総数	2223	100.00

この結果から spam 対策サーバにおいて，spam を 85%除去できている事が分かる．

１．４　問題点

表２の例からわかるように検出精度は必ずしも十分ではない．過去の運用経験からは運用時期によっては 85%より低かったこともあり，検出精度 85%であっても利用上妨げになると思われる．

「対策の詳細」でも述べたが，そもそも spam 対策をメールサーバで行うのでは精度向上に限界があり，個人ごとに spam 判定を行える仕組みが求められる．個人ごとの spam 判定を行える仕組みでは，個人の spam 判断を取り込み反映した spam 判定が行えなければならない．

こうした仕組みとしては学習型 spam 対策システムが最適であると思われ，一部の Web メールや，電子メールソフトやそのプラグインソフトなどで実装され始めてきている．まだこうしたものはインストールや設定，操作が難しかったり，利用環境を変更しなければ利用できないものばかりである．こうしたものがより一般的になってきた際には，それまでの利用環境に大きな変更を加えずに利用者が spam に悩まされない環境を実現できるだろう．

また大量の spam がメールサーバに大きな負荷を強いることも問題である．

メールサーバに存在しないユーザ宛の電子メールが届くと，指定されている送信元メールアドレスへ「宛先メールアドレスが存在しない」旨のエラーメールをキャンパスメールサーバが送信しなければならない．

ウィルスメールや spam はデタラメな送信元メールアドレスと，デタラメな宛先ユーザ名を指定して送られてくる．このため送信しなければならないエラーメールはほとんどは正しく送信できない．こうしたエラーメールは正規の電子メールと機械的に判別できないため，正規の電子メールと同様に１週間程度の間廃棄せずに再送を試みなければならない．

こうした条件の中で，spam がキャンパスメールサーバへ大量に届けられた場合には，大量の spam によって大量の送信できないエラーメールがメールサーバに蓄積される．大量のエラーメールはメールサーバのハードディスク，メールサーバソフト資源を浪費してしまう．ついには大量のエラーメール送信の後に正規の電子メールを処理するようになってしまい，正規の電子メールが遅延したり，正しく届けられないなどの問題が発生する．

こうした問題の解決策としては，

(A)存在しないユーザへの電子メールの受信拒否
(B)存在しないユーザへの電子メールの廃棄
(C)メールサーバの強化

などが一般的に行われている．しかしそれぞれに問題がある．

(A)は，電子メールが拒否されたかどうかによって，spam 送信者に存在するメールアドレスの情報を提供してしまう．これは結局のところ効率的な spam 送信を可能にすることで，被害を悪化させる危険がある．

(B)は，正規の電子メールにてメールアドレスの入力間違いがあった場合にも，送信者にエラーメールが送信されなくなってしまうという副作用がある．多数の利用者を抱える横浜キャンパスメールサーバでは適用しにくい．

(C)は，費用がかかる上，それが spam のためであるとなればなかなか導入に踏み切りにくい．

現状では，メールサーバソフトの変更とそのチューニング，動作状況監視強化，予備的なサーバの増強によって対策しているが，今後 spam 被害の拡大が進んだ場合に

は別の対策が必要になる可能性がある．今後のメールサーバの機能強化によって改善を模索していく必要がある．

２　メールサーバの構成強化

利用者にとって電子メールの重要性は高まっており，キャンパスメールサーバを停止することは極力避けなければならなくなってきている．これまでのキャンパスメールサーバシステムは，spam 対策サーバは１台だけ，受信メールサーバと送信メールサーバは同一の１台だけで運用していた．こうした構成ではどれか１台が停止しただけでメールシステム全体が停止してしまう．

可用性を高めメールシステム停止の危険性を低減するため，メールサーバの構成を強化した．改善点は次の通りである．

・spam 対策サーバを２台に増やし，Active-Active で運用する．
・メール送信サーバとメール受信サーバを別々に分ける．
・メール送信サーバを２台とし，Active-Active で運用する．
・メール送信サーバでは，ユーザ認証(SMTP AUTH)により学外からでもメール送信を受け付ける．
・メール受信サーバを２台とし，Active-Stanby で運用する．

上記構成強化は，可用性向上(サーバの冗長化)，セキュリティ向上(送信時ユーザ認証)とまとめることができる．こうした構成強化によって，システム停止の危険性を低減し，学外からでもメール送信を行えるようサービスを向上した．

３　まとめ

横浜キャンパス内のメールサーバは機能強化により，spam 対策，可用性向上，セキュリティ向上を実現した．spam 対策の精度が十分には高くない事，エラーメールによるサーバ負荷の問題，についても述べた．spam 検出精度向上のためには学習型 spam 対策システムの導入，エラーメールによるサーバ負荷への対応については今後模索していく必要があることを述べた．