電子メールのウイルス・スパム対策について

学術情報部情報基盤課情報基盤グループ
須藤勝弘　stowe@cc.hirosaki-u.ac.jp

1 はじめに

電子メールが研究や業務に重要な役割を果たすようになって久しいですが，メールを利用する際の最大の問題は，ウイルスの感染と迷惑メールへの対応ではないでしょうか。本稿では，総合情報処理センターが，いままでとってきたウイルスチェックや迷惑メール対策と近々本格運用を開始する予定のウイルス・スパムゲートウェイの紹介を行います。

2 これまでのウイルスメールと迷惑メール対策

メールのウイルスチェックを行うサーバであるウイルスゲートウェイは，平成14年，ギガビットネットワークシステムの一部として導入されました。Linux上でトレンドマイクロのInterScan Messaging Security Suite[1]（導入当時はInterScan VirusWall）という製品が動作しています。ウイルスチェックの対象メールアドレスは，センターの****@cc.hirosaki-u.ac.jpと****@stu.hirosaki-u.ac.jpおよび，理工学研究科の****@eit.hirosaki-u.ac.jpです。@以降が異なるメールアドレス同士および，学外と学内でやりとりされるメールは，すべてウイルスゲートウェイによるウイルスチェックが行われています。センターでは，ギガビットネットワークシステムとともにウイルスゲートウェイを6年間運用してきました。ウイルスゲートウェイが導入されてはじめの頃は，表1に示すようなトラブルが発生していましたが，最近はほとんどトラブルがありません。

表1 ウイルスゲートウェイで発生した主なトラブル

トラブルの内容	原　因	対　策
外部からの迷惑メール中継に利用された	サーバの設定ミス	設定を変更した
身におぼえがないのにウイルスゲートウェイからウイルスを送信したと通知メールが来た	メールの送信元を偽装する迷惑メールがあり，偽装されたアドレスに通知メールが送信された	通知メールを送信しないようにした
添付ファイルがウイルスに感染していないのに外部にメールが届かない	多数のファイルが圧縮されており，ウイルスゲートウェイに設定されていた数を超えていた	処理可能なファイルを十分な数に増やした

迷惑メールについては，ここ数年にわたりまさに“迷惑”以外のなにものでもない，という状態ですが，ギガビットネットワークシステムを導入した6年前には，現在ほど大量の迷惑メールが送りつけられることはなく，対策製品もそれほど一般的ではありませんでした。しかしその後，迷惑メールは増加の一途をたどり，利用者からの苦情も寄せられるようになりました。それに手をこまねいているわけにもいきませんので，できるものから対応を行ってきました。

2-1 特定のメールアドレスからの受信を拒否[2]

迷惑メールが流行しはじめの頃は，同一のアドレスから送信される迷惑メールが多かったように記憶しています。ウイルスゲートウェイでは，現在よく使われているメールサーバソフトウェアのPostfixが稼動していましたので，Postfixが標準で搭載している送信元メールアドレスによる受信拒否機能を使いました。この設定では，利用者から苦情のあったメールアドレスやメールサーバのログを調査して，特に悪質と思われたメール送信者のアドレスを受信拒否リスト記述していました。しばらくの間はそれなりの効果を発揮していたのですが，迷惑メールの件数が増え，それに加えて送信元アドレスをどんどん変更しながら送信されるメールも増えてきたので，だんだん受信拒否リストの保守を行わなくなりました。しかし，現在でも同一のアドレスからの迷惑メールが目立つ場合はこの方法でメールの受信拒否を行っています。

2-2 特定のDNSサーバに登録されているアドレスからの受信を拒否[3]

メールアドレスの@より右の部分は，DNSサーバに登録されたドメイン名を用いるのですが，迷惑メールの送信元アドレスで用いられるドメインが大量に登録されている海外のDNSサーバが存在し問題になったことがありました[4]。弘前大学にもこのパターンの迷惑メールが大量に届いておりましたので，対策をとることにしました。Postfixには，DNSサーバを指定し，そのDNSサーバに登録されているドメインから送信される全てのメールを受信拒否する機能があります。これを用いて設定を行い，一時期はそれなりの効果は得られたのですが，yahoo.comなど迷惑メールもちゃんとしたメールもどちらも多いようなドメインには適用できない仕組みなので，結局，焼け石に水だったかもしれません。

2-3 メールの送信相手によって接続を遅延させるStarpit[5]の適用

メールサーバは，設定ミスがない限り，mail.cc.hirosaki-u.ac.jpのようなDNSに登録された名前を持っているのが普通です。その一方で，メールサーバに限らずサーバではない機器は，DNS登録名を持っていなかったり，IPアドレスの一部または全部を示す数字が含まれたDNS登録名を持っていたりします。迷惑メールの送信は，法律で禁止されているなどの理由でまっとうなメールサーバを経由して送信しにくくなっており，サーバではない機器から送られてくることが多いようです。そのような傾向を利用し，この“サーバではない”機器からのメール送信要求に一定時間待ったをかけるのが，Starpitという方式です。この方式では，Postfixが標準で持つアクセス制限機能を応用して設定を行います。Starpitの提唱者の方のウェブページでその原理と接続遅延時間の設定によ

る効果を読んで，センターで導入を行うことにしました。

Starpitの設定を行うにあたり，ウイルスゲートウェイで動作しているPostfixのバージョンが低いこと，また，標準状態のPostfixでは，ログに残すことができない情報があることがわかりましたので，ログを残すことができるようにした（パッチをあてた）最新バージョンのPostfixに更新を行いました[6]。前述の2-1と2-2については，テスト運用を行った結果，利用者への正式なアナウンスは必要ないと判断し，行いませんでした。Starpitでも，正規のメールが届かない可能性かなり低いのではないかと思い，またそれがこの方式を選択した理由でもあるのですが，検討の結果，センターの利用者全員へのメールとウェブページでアナウンスを行い，2006年11月27日から運用を行ってきました。Starpit設定後は，かなりの迷惑メールを遮断することができるようになり，センター関係の委員の先生などからも喜びの言葉をいただきました。

3 新ウイルス・スパムゲートウェイの導入

平成19年2月からセンターの新計算機システムが稼動していますが，新システムには，これまで使用してきたウイルスゲートウェイの代わりとなるウイルス・スパムゲートウェイが含まれています。新しいウイルス・スパムゲートウェイは，Linux OS上でトランスウェア社のActive!hunter[7] [8]という製品が動いています。ウイルス・スパムゲートウェイの更新を行った理由としては，利用者が自らの意思で迷惑メール対策機能のON/OFFをコントロールできる仕組みがほしかったこと，システムである計算機システムに含めることでメーカーおよび対応業者による手厚いサポートが期待できることがあげられます。

4 Active!hunterの概要と使用方法

Active!hunterは，外部のメールサーバと直接通信を行うようにネットワークに接続されています。Active!hunterを経由するメールは，十数段階に構成されているフィルタでウイルスおよび迷惑メールのチェックが行われますが，このフィルタは，管理者が設定を行う部分と，利用者がウェブ経由で個別に設定可能なパーソナルコントローラーに分かれています。フィルタによってウイルスメールや迷惑メールと判断されたメールは，管理者の設定により，件名やメールヘッダにマークして送信先に送信するか，Acitve!hunter自体に一時的に保存し，利用者がパーソナルコントローラーで配送するか削除するようにするかどちらかの処理がされます。図1がパーソナルコントローラーのログイン画面です。

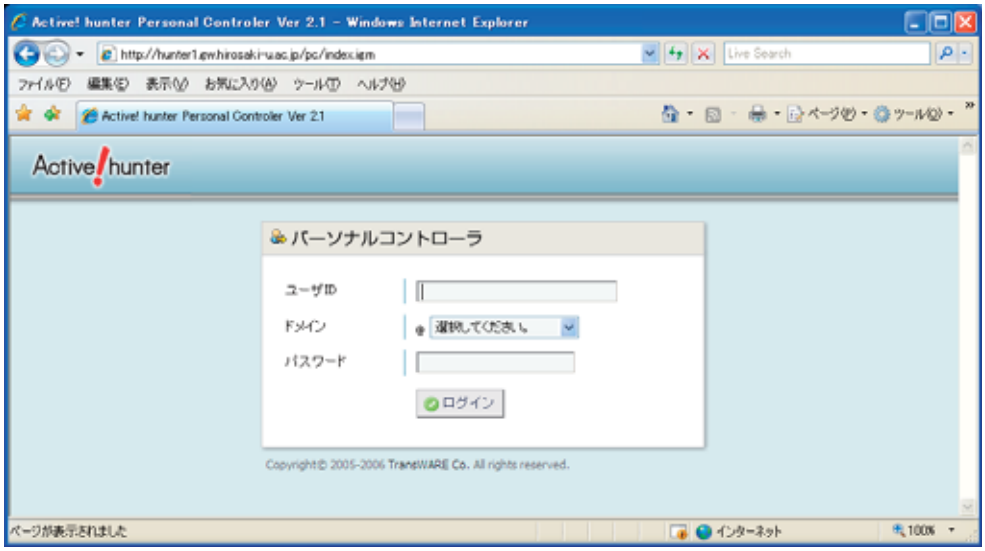

図1　ログイン画面

ログイン画面では，センターシステムに登録されているユーザ名，パスワードを入力し，一覧からメールアドレスのドメイン部分を選択します。ログインに成功すると図2の画面が表示されます。

図2　メニュー画面

図2では，“フィルタの使用”と“ウイルスチェックの使用”の両方を使用することになっています。はじめて接続を行ったときは，“フィルタの使用”が無効となっており，迷惑メールの処理は行われないようになっていますので，各自でフィルタを有効にする必要があります。ウイルスチェックについては，特に必要がない場合を除いて設定を解除しないようにしてください。ちなみに，Active!Hunerでは，ウイルスチェック機能としてF-Secure社[9]のものを搭載しています。

迷惑メールの判定状況を確認するためには，画面左側のMENUから“受信メール一覧”を選択します。図3がメールの一覧画面です。受信したメールの件名，本文の一行目，送信者，受信日時が表示され，さらに正常なメールと判断された場合は“受信”が，迷惑メールと判断された場合は，その処理内容とどのフィルタが適用されたかが表示されています。図3の例では，一番上のメールがユーザ設定フィルタによって迷惑メールとして判定され，件名またはメールヘッダにマークを付加されて配送されています。

図3　受信メール一覧

ユーザ設定フィルタを適用する場合は，MENUから“受信フィルタ設定”を選択してください。メール送信者，件名，本文について文字列を指定し，条件に一致したメールを正常なメールまたは迷惑メールとして処理するようフィルタを設定することが可能です。図4では，件名に指定した文字列が含まれる場合に迷惑メールとするよう設定を行っています。

図4　ユーザフィルタ設定画面

5 管理者フィルタについて

Active!hunterでは，十数段階にフィルタが構成されていると述べました。前項で説明を行ったユーザ設定フィルタもそのなかに含まれますが，ほかのフィルタは，管理者が設定を行い，パーソナルコントローラーでフィルタを使用するように選択を行った利用者の全てのメールに適用されます。管理者フィルタには，メールアドレスや接続元のIPアドレスで判定を行うもののほかに，RBL[10]と呼ばれているスパム送信者のIPアドレスのリストを管理している外部のサイトに問い合わせを行うフィルタ，SVM[11]理論を用いて受信されたメールを学習することで判定を行うフィルタなどがあります。

6 おわりに

本稿に掲載したパーソナルコントローラーの画面に掲載されているURLやメールアドレスは，テスト中のものです。利用者のみなさんには，接続先などの情報を別途お知らせしますのでよろしくお願いいたします。

参考資料

[1] http://jp.trendmicro.com/jp/products/enterprise/imss/, 2008
[2] /etc/postfix/main.cf(設定ファイル)のsmtpd_sender_restrictions を設定
[3] /etc/postfix/main.cf の smtpd_sender_restrictions = check_sender_ns_access を設定
[4] “qsv 系スパム”などと呼ばれていました。
[5] http://d.hatena.ne.jp/stealthinu/20060706/p5/, 2006
[6] PostfixをRedhat ES3付属のものからバージョン2.3.4に変更しました。
[7] http://www.transware.co.jp/product/ah/, 2008
[8]佐藤友暁 「新システムにおけるメールシステムとスパム対策」HIROIN No.20, pp35-41, 2007
[9] http://www.f-secure.co.jp/,2008
[10] Realtime Blackhole の略。Active!hunter の場合は, DNSBL(DNS-based Blackhole List)と呼ぶのが正確かもしません。(http://d.hatena.ne.jp/keyword/DNSBL ,2008 より)
[11] Support Vector Machine の略。V.Vapnik, “The Nature of Statistical Learning Theory”, Springer, 1995