秋田高専の迷惑メール対策について

技術職員　神　　智　也

1.　はじめに

ここ数年，本校でも「迷惑（スパム）メール」の受信件数が大幅に増加している。このような多くの迷惑メールを受信することにより，必要なメールと迷惑メールを自分で判断して分類し，必要なメールを探し出すのに膨大な時間がかかり，重要なメールを見落とす危険も大きく，業務効率を著しく低下させていた。また，教職員から対策の要望が多く寄せられ，システム的な対応が強く求められていた。このような状況の中，試験運用を経て平成18年５月から対策システムの本運用を開始することになった。これにより，迷惑メールをシステム側で自動検知および自動隔離が可能となり，自分でメーラのフィルタ設定や迷惑メール対応ソフトのインストールが不要となり，メール分類の負担が軽減された。本稿では今回導入した迷惑メール対策システムの概要，運用方針，導入効果について述べる。

2.　対策システムの概要

2.1　メールの配送経路

図１にメールの配送経路の概略図を示す。本校のメールシステムは４台のサーバから構成されている。まず，外部から送られてきたメールは，対外用中継サーバに集められ，送信元の逆引きやアクセスファイルにてあきらかな不要メールを拒否している。次にメールは，ウィルス対策システムでチェックがかけられ，そしてこの迷惑メール対策システムに送られ判定にかけられる。このように複数のチェックを施すことで不要なメールを除去し，正常なメールだけが受信メールサーバに送信されユーザに届けられる。一方，内部からメールを送信する場合は，ウィルス対策システムを内部 SMTP サーバとして兼用しているので，必ずウィルスチェックがかけられてから送信される。内部同士のメールは，迷惑メール対策システムを通過するが，内部ユーザをホワイトリスト化しているので判定を行わずユーザに届ける。

2.2　システムの主な特徴

導入した対策システムは，バラクーダ社の「Spam Firewall」というアプライアンス製品である。主な特徴として，ライセンスはフリーで，既存のメールシステムへの組み込みが容易である。フィルタ機能については，ブラックリスト，インテンション解析，レートコントロール，ベイジアンフィルタ，キーワードブロックなどの機能があり，多言語対応なので日本語スパムも検知できる。また，ユーザ（メールアカウント）毎の設定や隔離が可能であり，検知後の処理については，タグ付け配信，隔離，拒否（ブロック）のような対応アクションが実施できる。システムの初期設定や運用管理については，日本語化されたウェブインタフェースを用いて行い，詳細なログやレポート機能もあり，操作が容易である。メール不達等のトラブルが発生した場合に対応するための必要なログも取れている。

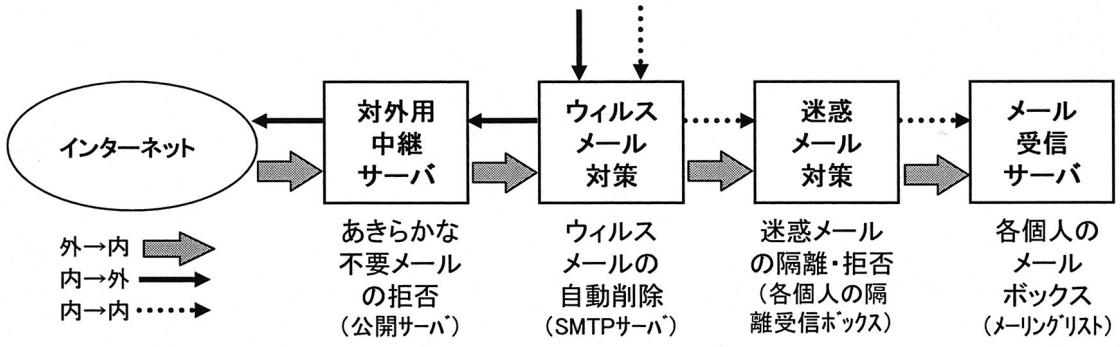

図１　メールの配送経路図

2.3　ユーザの利用環境

このシステムを利用した場合，迷惑メールと判定されたメールは，受信メールサーバと分離・独立している個人毎に用意されているシステム（サーバ）側の「隔離受信ボックス」へ送られ，30日間保管される。そして，毎日１度午前７時に「隔離受信ボックス」にどのようなメールが隔離されたかの情報をメールで各個人に通知する。次に，この受け取ったメールをもとにウェブインタフェースを用いて，「隔離受信ボックス」にアクセスし，誤検知された正常なメールがないか確認する。このウィンドウ上では，日付，送信元，件名が一覧表として表示されており，メールの内容も閲覧できる。もし，確認中に必要なメールを発見した場合，ウィンドウ上にあるそのメールの「ホワイトリスト」という項目をクリックすると，アドレスがホワイトリストに自動登録され，自分のメールボックスへ再配送される。次回から，このアドレスからのメールに関しては，検知が行われず正常なメールとして送られてくる。このようなシステム環境で全てのユーザは管理操作を行っているが，このボックスを利用せず，迷惑メールと判定されたメールのタイトル（サブジェクト）にタグを付けて配信し，個人のメーラで自動振り分けを行うことも可能であるが，混乱する可能性もあり，また，各自で振り分けの設定も行わなければならないことから，推奨はしていない。

3.　運用方針

今現在，次のような方針で迷惑メール対策システムを運用している。まず，この対策システムを利用するかどうかはユーザ個人の判断に任せ，当分の間は教職員だけに提供するサービスとする。利用する場合は，迷惑メールと判定されたメールのうち，ブラックリストで迷惑メールと判定されたメールは「あきらかに100%迷惑メールである」と定義付けし受信を拒否（ブロック），インテンション解析とスコア方式で迷惑メールと判定されたメールは「隔離受信ボックス」へ自動隔離する。また，迷惑メールの判定に関しては必ず誤検知がついて回るので，利用ユーザには「隔離受信ボックス」を必ず最終確認してもらうようお願いして各個人で責任を持って管理してもらう。内部同士でメールの送受信を行う場合と内部から外部へメールを送信する場合については，迷惑メールの判定（検知）は行わない。また，事務部のメーリングリストにも利用可能で「隔離受信ボックス」の管理担当者を係等で決めて利用してもらう。

4.　運用状況

迷惑メール対策システムの運用を開始して５ヶ月が経過し，次のような統計情報が得られた。利用者数は全教職員の73%で，迷惑メールの総受信数は１日平均約1200通，教職員宛に届くメールの64%である。迷惑メールの判定内訳として，ブラックリストが60%，インテンション解析が30%，スコア方式が10%となった。参考までに，筆者に送られてくるメールについて，迷惑メールの検知率は93%で，すり抜けてきたメールも４%と数少なく，検知率には満足している。なお，誤検知されたメール３%の全ては，メルマガやユーザ登録サイトのダイレクトメールで，これらはスコア方式による判定で迷惑メールと検知されたもので，ホワイトリスト化することで対応できる。また，これ以外正常なメールが誤検知されたことはなく，学校全体としても，迷惑メールの判定や不達等などのトラブルはなく，順調に稼働している。

5.　これからの課題

受信者が存在しないアドレス宛のメール（１日平均約1100通）が増加している。これらのほとんどは迷惑メールと考えられるが，これを受信してしまうと，送信者アドレスは一般に偽装しているものが多いので，エラーメッセージを返すことができない。また，エラーメッセージを送信できたとしても，実際の送信者ではなく，関係ない第三者に送られることになる。これらにより，大量のメールが対外用中継サーバにとどまってしまいディスク容量を圧迫し，送信されないメールの再送処理が繰り返され，さらなる負荷がサーバにかかってしまう。これに対応するために，対外用中継サーバのメールソフトを変更し見直しを図り，本校ネットワークの入口で止めるような対策が急務であると考えている。

6.　まとめ

今回，構築した迷惑メール対策において，コストは多少かかったものの，できる限り人手を介さない自動的に処理される対策システムにより，ユーザと管理者双方に利便性をもたらすことができた。今後は，この迷惑メール対策に限らず，メールシステム全体の見直しを図り，ユーザのメール環境の更なる向上につなげていきたいと考えている。