本校における迷惑メール対策の運用とその状況

林 嘉雄[*1]　鳥居 恵子[*1]　義永 常宏[*2]　新田 貴之[*2]　力 規晃[*2]
国重 徹[*3]　室長 大應[*4]　池田 光優[*5]　桑嶋 啓治[*6]　柳澤 秀明[*2]

PA Countermeasure against Unwanted E-mails at Tokuyama College of Technology

Yoshio HAYASHI[*1], Keiko TORII[*1],
Tsunehiro YOSHINAGA[*2], Takayuki NITTA[*2], Noriaki CHIKARA[*2],
Toru KUNISHIGE[*3], Daio MURONAGA[*4], Mitsumasa IKEDA[*5],
Keiji KUWAJIMA[*6] and Hideaki YANAGISAWA[*2]

Abstract

E-mail is an indispensable tool for communication in our current day-to-day work. At Tokuyama College of Technology, we have taken measures against virus-infected e-mails. However, no effective measures had been taken to block unwanted e-mails. With a massive increase in spam volume, we had been bothered by the unwanted e-mails. Identifying spam messages and deleting them by ourselves are time-consuming. Occasionally we misclassify an important e-mail as spam and delete it by accident. The problem became so serious that we decided to introduce a paid-for spam filter system produced by Symantec Corporation. This paper aims to describe how we configured the settings for the filter system, how we have been operating it, and how much it has improved the situation.

Key Words : e-mail, spam, virus, Symantec, SMS

1．まえがき

現在，電子メールは，日常業務の欠かせない連絡ツールである．これまで，本校では，セキュリティ強化のために，メールサーバや，クライアントPCに対するウイルス対策に関しては行ってきたが，迷惑メール（以下spamメール）については，必要なメールをspamメールと誤識別する可能性があるため，無償ツールでは，有効な対策を講じることが困難であり，ユーザ各自で処理を行う形態であった．

しかしながら，近年，spamメールの増加に伴い，spamメールを削除する作業に時間をとられ，さらに，必要なメールが埋もれてしまい見落とすなど，日常業務に支障を及ぼすようになった．これらのspamメールに関する苦情や，対策方法など，情報処理センターへの問い合わせも増加し，コストをかけてでも全学の問題として迷惑メール対策を行う必要となった．

そこで，本校では，有償ソフトウェアのシマンテッ

[*1] 教育研究支援センター　第三技術室　[*2] 情報電子工学科
[*3] 一般科目（英語）　[*4] 一般科目（物理）
[*5] 機械電気工学科　[*6] 土木建築工学科

ク社製スパムフィルタを平成18年度末に試用し，改善される見通しが立ったため，導入を決定し，平成19年度当初から運用を開始することになった．

本論文では，本校の実情にあわせた設定，並びに運用形態について述べ，それによる改善状況について述べる．

2．spamメール対策の検討

spamメール対策としては，大きく分けると，各ユーザのクライアント側で個別に対策する方法とサーバ側で一括して対策する方法がある．この2つの方法において，人的負担が少ない方法を選択するために，クライアント側においては，メーラの操作や設定変更が少ない方法であり，かつ，サーバ側においては，既存のメール配送システムの設定を大幅に変更せずに導入できることを前提として検討を行った．これらに基づくと，アプライアンス型の機器を設置することが適切であるため，シマンテック社製スパムフィルタSymantec Mail Security 8360[1]（以下SMS）という製品を選択した．このSMSは，評価機の貸し出しがあり，本校も借用し試行運用を行った．その結果，評価期間中でのトラブルも無く，検討事項として挙げた2点を十分満たしていたので，平成19年4月から導入し，運用を開始した．

3．システムの概要

3－1　システムの主な特徴

本SMSは，アンチウイルス処理と，アンチスパム処理をはじめ，数々のセキュリティ機能を実装した総合型のメールセキュリティアプライアンスであり，spamメールの評価と識別を高い精度で行うことが可能である．フィルタリングの結果に応じて，件名にタグを追加，X-headerの追加など，様々な処理を自動的に実行できる．また，インバウンドおよびアウトバウンドにおいて，別々のMTAを有しているので，送受信のどちらにおいても，能力を発揮する．

システムの初期セットアップは，出荷時にOS，MTA，各セキュリティソフトウェアを実装したアプライアンス製品のため，既存のメール配送システムの経路へ挿入する形で組み込むことになる．そのため，容易に設置することができ，ほぼ無停止で稼動を開始することが可能である．運用管理については，スパムフィルタの定義ファイルやウイルス定義ファイルが最新版に自動アップデートされるため，管理者の負担が少ない．また，Webブラウザを使用して，各機能の集中管理，フィルタリングパフォーマンスのリアルタイム監視などが行える．

スパムとコンテンツのフィルタリング，ウイルススキャンの統計などについては，詳細なレポートを生成すること可能であり，スケジューリングによって，レポートをメール送信したり，エクスポートしたりすること可能である．

3－2．メールの配送

SMSを設置したメール配送図を図1に示す．本校では，学内ネットワークのFirewallとMailサーバの間にSMSを設置した．spamメールは，不特定多数への一方的な広告メールであり，送信者のメールアドレスを偽装して送信することがある．そのため，宛先不明のエラーメールを本校からspamの送信者に送信しても，正しく届く可能性は限りなく低い．それらのエラーメールの送信は，本校のメール配送システムに負荷がかかるだけに留まらず，偽装された関係のない第三者にエラーメールを送信してしまい，新たな被害を発生させる恐れがある．

そこで，アウトバウンドで，spamメールと判定されたメールは，SMSのスパム検疫に格納する設定を行った．この設定によって，本校に存在しないメールアドレス宛のメールで，かつspamメールの場合は，SMSのスパム検疫に格納することになる．

3－3．システムの運用

本SMSを教職員，学生の全員に適用する場合において，spamメールの検出率が限りなく100%である場合においても，誤検知の可能性が完全に否定できない限り，真にspamメールだとしても，基幹システム側でブロックせずに，ユーザに配送することを導入時の基本方針とし，次の設定を行った．

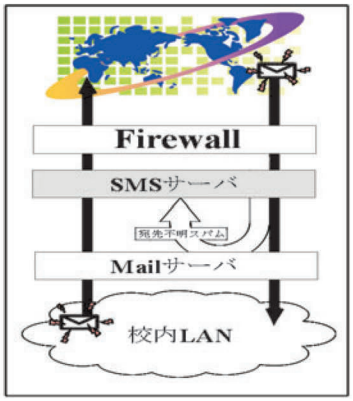

図1　メール配送図

SMS において，インバウンド側のメールでは，メッセージを spam メールと判定した場合は，図 2 のように，件名タグの先頭に「[SPAM と判断しました]」を追加し，値を「Spam」とした「X-SMS-Scanned」ヘッダーを追加するように設定した．同様に，spam メールの疑いがある場合は，件名タグの先頭に「[SPAM の疑いがあります]」を追加し，値を「Suspected Spam」とした「X-SMS-Scanned」ヘッダーを追加する設定にし，配送することにした．

これらの検出結果を基に，ユーザ側のメーラ設定で自動振り分け機能を用いて，spam メールを分類する処理が可能である．Microsoft におけるメーラの Outlook Express では，図 3 のメッセージ ルール機能を使用して，件名に指定した文字「[SPAM と判断しました]」が含まれるかによって判断させることが可能である．Outlook では，図 4 の自動仕訳ウィザード機能を使用し，メッセージヘッダーに「X-SMS-Scanned: Spam」が含まれているかによって，判断させることが可能である．

4．システムの管理・機能

SMS に対する全ての管理操作は，Web ブラウザから行う．SMS の状態を表示するページを図 5 に示す．このページのグラフは，過去 24 時間と過去 30 日間のスパムとウイルスの割合がグラフで表示され，表については，ウイルス定義ファイルのバージョンや，スパムフィルタの更新など，システムに関する状態を示す．さらに，インバウンドとアウトバウンド別に分類して，過去 60 分と設定した日から現在までの，ウイルス数と spam メール数が表示される．管理者は，このページを確認するだけで，メールの識別状態とシステムの稼働状態をリアルタイムに把握することが可能である．

レポート機能は，図 6 に示すレポート生成ページから，詳細なレポートを生成することが可能である．細分化された項目を選択し，実行するだけで，必要とする情報をグラフや表に詳しく出力することが可能である．さらに，それらを CSV ファイルで保存したり，メールで送信したりすることも可能である．また，スケジュール機能を使用することで，図 7 に示す管理者宛メール送信レポート／週のように，設定した内容のレポートを決まった日時に送信することが可能である．

以上の機能を用いて，本システムが正常に稼動しているかを確認することができ，また，本校における spam メールやウイルス付メールの現状を把握することができる．本校におけるメールの現状については，次章で述べる．

図 2　spam フィルタポリシーの詳細

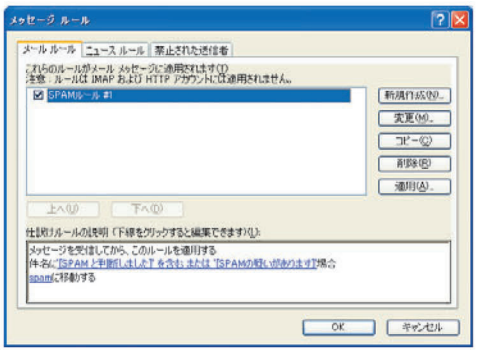

図 3　メッセージ ルール

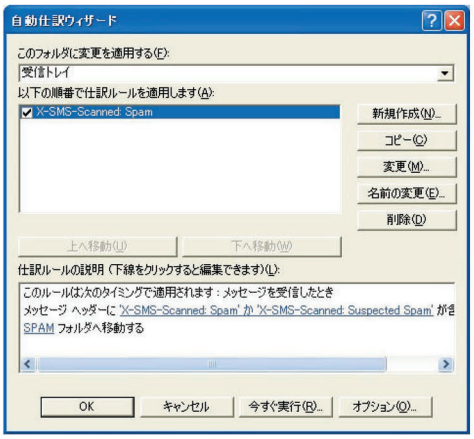

図 4　自動仕訳ウィザード

図 5　SMS の状態ページ

図6　レポート生成ページ

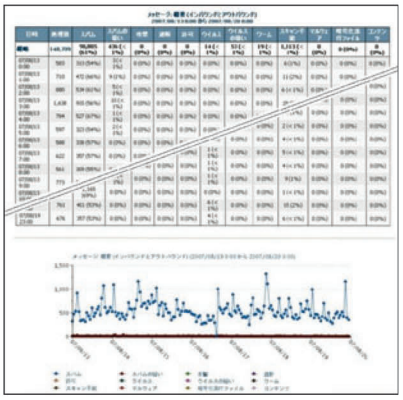

図7 管理者宛メール送信レポート／週

5．運用状況

SMS の運用当初，学会からの案内（国際会議や論文募集）が spam メールの疑いがあると判断していると，数件の報告を受けた．これらの案内メールは，論文集などのメールアドレスなどを拾い上げて，全世界的に発信しているメールであることや，国際会議のバーナー画像や，案内 URL を含むことが多い．その行為は有害なスパムと同様の振る舞いであり，内容の形態も spam メールと酷似しているため，スパムと疑われても仕方ないこと思われる．そのため，本校の業務形態では，利用者各位で，削除の判断をして頂くという当初の判断に誤りがなかったと言える．その他の正常なメールが誤識別されたという連絡は受けていない．

運用を開始して 5 ヶ月が経過し，SMS が処理したメールの内訳を表 1 に示す．本校に届くメールの約 91%が spam メールで，約 0.1%がウイルスを含むメールだということがわかった．また，本校に存在しない宛先不明の spam メールは，全体の約 40%だということがわかった．宛先不明の spam メールを，SMS で検疫することで，メール配送システムの負荷が軽減されている．

表 1　SMS メッセージ処理結果

メッセージ	インバウンド	アウトバウンド
処理した数	1,893,492	780,756
spam メール	1,717,505(91％)	680,241(87％)
ウイルス	1,304(0.1％)	0(0％)

ウイルス対策においては，既存のメールサーバにインストールしてあるウイルス対策ソフトと異なったウイルス対策ソフトを導入したことで，2 重のメールセキュリティ対策が行えるようになった．

6．まとめ

今回，SMS の導入と本校の実情に合わせた設定により，spam メールは，SMS のフィルタリングで自動識別され，ユーザ各自のメーラで，自動振り分けによる対応が可能になった．ユーザからの評価も高く，spam メールを削除する作業にも時間をとられず，さらに，必要なメールだけを読めるようになり，全利用者において spam メールによる負担が軽減されたものと認識している．

管理側においても，既存のメール配送システムへの組み込みが容易であったため，導入当初から安定したサービスを開始することが可能であった．また，スパムフィルタの定義ファイルやウイルス定義ファイルは，最新版へ自動更新されるので，メールの諸問題に関して，高セキュリティを確保することが可能となった．さらに，管理者は SMS の管理 Web ページを確認するだけで，システムの稼働状態やメールの識別状態を適切に監視することが可能となり，レポーティング機能を活用することで，必要とする統計情報を容易に収集が行え，本報告のような現状解析を行うことが可能となった．また，スケジューリング機能によって，定期的に生成したレポートを管理に携わるメンバーにメールを送信することで，現状のフィルタリングのパフォーマンスやメールの流量を把握することが可能となった．

今後は，基幹システム側において，spam メールの削除を行うかについて，学内全教職員の合意が得られるかなどに関して，議論や検討を深める必要がある．

謝辞

本システムの導入にあたり，有益な御助言，御指導いただきました本校の教職員並びに，日商エレクトロニクス株式会社中国支店に，感謝の意を表します．

文献

1) Symantec　http://www.symantec.com/ja/jp/

(2007.09.05 受理)