本校のメール運用状況及び迷惑メール対策の有用性と課題

髙木 美咲穂[*1]　林 嘉雄[*1]　鳥居 恵子[*1]　新田 貴之[*2]

Operation status of email and usefulness and challenges of countermeasures against spam

Misaho TAKAKI[*1], Yoshio HAYASHI[*1],
Keiko TORII[*1] and Takayuki NITTA[*2]

Abstract

National Institute of Technology, Tokuyama College has been using email since 1986, and it has become an essential means of communication. In 2007, we successfully implemented Symantec's spam filter to reduce unwelcome email and protect against viruses. In recent years, we also started using Microsoft Exchange Online, an email system using the cloud of Microsoft Office365, and procured by the National Institute of Technology headquarters. This paper describes how to set up the countermeasures against email spam in our original email system and the Microsoft Exchange Online. It also explains the current operation of these email systems.

Key Words : email, spam, Symantec Messaging Gateway, Microsoft Exchange Online

1. はじめに

本校では，昭和 62 年から電子メールを利用し始めており，日常業務で頻繁にメールでの連絡が行われている．メールは，離れている人へ連絡する以外にも，資料を送付する手段や非同期で仕事を進める手段としても便利なツールである．

しかし，便利な反面で，迷惑メールやウイルス付きメール(以下,spam メール)が送られてくることより，必要なメールの見落としや，セキュリティインシデント発生の恐れが高まる．そのため，これらの不必要なメールに対する対策が必要である．

本校では，spam メール対策として，平成 19 年度から有償ソフトウェアのシマンテック社製[1)]スパムフィルター(以下，SMG[Symantec Messaging Gateway])を学内からの要望によって導入し，運用を開始した．これにより，spam メールが利用者に届かなくなり，必要なメールが spam メールで埋もれてしまうことが少なくなったことについて報告した[2)]．

一方，近年では高専機構本部(以下，機構本部)が全国の国立高専で利用するために調達した Microsoft Office365[3)](以下，Office365)で用いているクラウド型のメールシステムである Microsoft Exchange Online(以下,Exchange Online)の利用も開始している．

本論文では，学内で運用している SMG を利用したメールシステム(以下，本校の SMG メールシステム)による spam メール対策を 2 章で述べ，機構本部が調達した Exchange Online での spam メール対策について 3 章で述べる．4 章では，これらのメールシステムの運用上の課題について整理して述べる．

2. SMG の概要と運用状況

本節では，本校の SMG メールシステムを活用した spam メール対策について，SMG の概要，ならびに，本校での設定状況と運用状況について述べる．

2.1 SMG の概要

SMG では，外部から受信したメールだけでなく，内部から送信したメールに対しても spam メールとして判定

[*1] 教育研究支援センター　第三技術室

[*2] 情報電子工学科

することが可能である．spam メールと判定するために利用する定義ファイルは，システムを無停止で自動更新され，常に最新の定義ファイルによって運用可能である．

spam メールと判定された際には，事前に設定している spam メールに対する処理方針(以下，spam ポリシー)の内容に沿って処理が行われる．spam ポリシーは，デフォルトで登録されている spam ポリシー以外にも，状況に応じてシステムに設定することができる．

また，Web からアクセスできる管理用ダッシュボードから，SMG を経由したメールのうち，spam メールの判定処理結果をリアルタイムで確認できるレポート機能が備わっている．さらに，この機能では，スケジュールを組むことによって，レポートを自動生成し，あらかじめ設定した宛先にメールで通知することもできる．

2.2 本校の SMG メールシステムの設定

本校では，Firewall とメールサーバの間に SMG を設置しており，「@tokuyama.ac.jp」に関するメールについて処理を行っている．この設置形態では，以下に述べる 1)～3)の配送パターンが存在する．

1) SMG におけるインバウンド・メッセージ
学外から本校(@tokuyama.ac.jp)宛に送られるメール

2) SMG におけるアウトバウンド・メッセージ
本校(@tokuyama.ac.jp)から学外宛に送られるメール

3) SMG を通過しないメッセージ
学内から学内宛に送受信されるメール(SMG を通過しないためアンチスパム処理は行わない)

1)や 2)の配送によって，SMG が「spam または spam の疑いのメール」を受信した場合には，図 1 のように設定した spam ポリシーに基づいて，spam の検疫場所にメールを隔離し，利用者にはメールを配送しないことを基本の設定としている．

但し，1)のような外部から到達するメールのうち，「spam の疑い」の場合については，誤検出の可能性があるために，図 2 のように設定し，検疫場所に隔離することを行わずに，各利用者に配送する．具体的には，「[SPAM の疑いがあります]」を件名の先頭に追加し，値「Suspected Spam」のヘッダー「X-SMS-Scanned」を追加して，利用者にメールを配送し，利用者側にて，spam メールかどうかの判断をお願いしている．

2.3 SMG の運用状況

SMG の運用状況は，図 3 のように Web 上のダッシュボードからインバウンドとアウトバウンドの処理状況を確認することができる．ダッシュボードでは，過去 1 時間，過去 24 時間，過去 7 日間，過去 30 日間の情報を選択して表示することができる．

図 1　受信メールの spam 検出設定

図 2　受信メールの spam の疑い検出設定

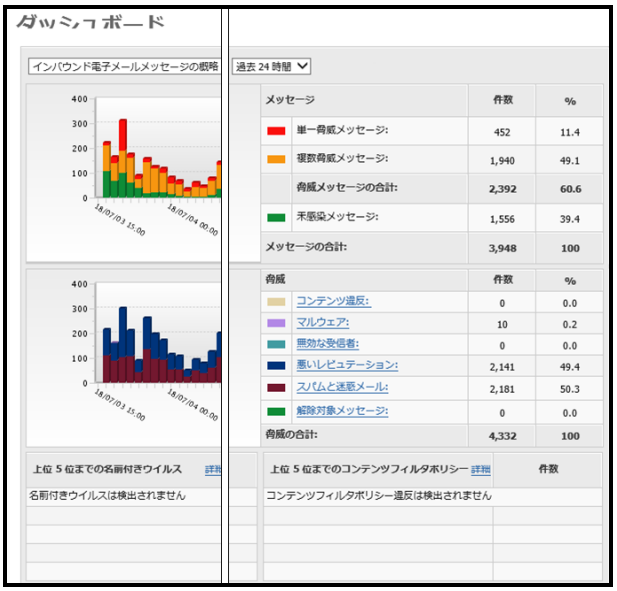

図 3　ダッシュボード

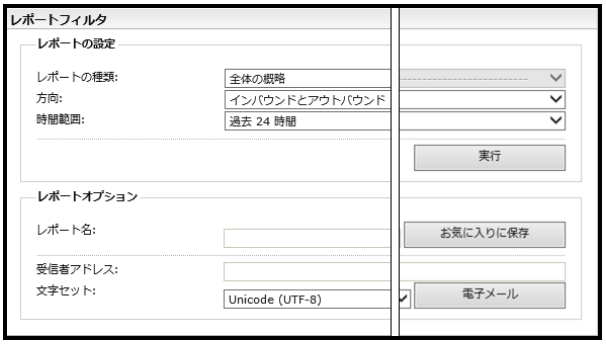

図 4　レポート作成

運用状況をより詳細に確認するには，図 4 のレポート作成画面からレポートを作成する．レポートの設定部分を変更することで，取得したい情報のレポートが作成できる．

レポートをエクスポートする場合には，HTML，PDF の各形式でのファイルまたは CSV 形式でのファイルでエクスポートすることができる．

SMG が 2017/9/1～2018/3/31 の期間で処理したメールの内訳を表 1 に示す．同様に，表 1 の脅威を含む数のうち，脅威の種類の内訳を表 2 に示す．

表 2 の脅威の種類のうち，現在の設定では，悪いレピュテーションのメールの全てが，シマンテックグローバルの悪い送信者からのメールであることをレピュテーションの概略レポートから確認している．

このシマンテックグローバルの悪い送信者とは，SMG が spam メールやウイルス付メールなどの好まれないメールを大量に配信しているサーバのリストを作成しており，そのリストの中に存在するサーバから送信されたメールのことである．

この仕組みにより，管理者が spam メールを大量に配信しているサーバのリストを作成・更新することなく，管理者の運用負荷をかけないで，spam メールを判定することができている．特に，本校では，表 2 で示したとおり，悪いレピュテーションと spam メールがほぼ同数であるために，シマンテック社が作成している悪い送信者のリストが有用に働いている．

なお，マルウェアと判定されたメールの中には，メールの添付ファイルを暗号化していた場合も数に含まれている．そのため，アウトバウンドのメールでマルウェアと判定されたメールのほとんどが添付ファイルを暗号化して送信したメールであった．

3.Microsoft Exchange Online の運用状況

本節では，機構本部が調達した Exchange Online の概要，ならびに，機構全体での設定と本校における運用状況について述べる．

3.1 Microsoft Exchange Online の概要

機構本部が調達した Office365 は，機構に在籍する全教職員及び全学生が利用可能であり，教職員は教職員用のライセンス形態が，学生には学生用のライセンス形態が付与され，アカウントが登録されている．

このアカウントは，「@tokuyama.kosen-ac.jp」というドメイン名で本校には割り当てられており，Office365 の Exchange Online のメールアドレスとしても利用できる．

表 1　SMG が処理したメール(2017/9/1～2018/3/31)

メール	インバウンド	アウトバウンド
処理した数	869,044	47,531
脅威を含む数	600,802(69.1%)	101(0.2%)

表 2　脅威メールの種類(2017/9/1～2018/3/31)

脅威の種類	インバウンド	アウトバウンド
マルウェア	32,915(2.8%)	49(48.5%)
悪いレピュテーション	565,937(48.3%)	0(0.0%)
spam メール	572,567(48.9%)	52(51.5%)

1 つのメールに複数の脅威が含まれている場合もあるため，表 1 の脅威を含む数と，表 2 のそれぞれの脅威メールを合計した数は一致しない．

この Exchange Online のメール機能を利用するには，Web アプリケーションとして，Office365 へサインインし，Outlook のアプリケーションを使用することで，Exchange Online 宛のメールを各自の利用端末にて送受信することができる．

また，パソコンやモバイル端末に Outlook をインストールしてアカウントの設定をする，もしくは，SMTP や IMAP などの汎用のプロトコルを用いて，利用者の好みとするメーラで接続すれば，Exchange Online にあるメールを送受信することができる．

3.2 Microsoft Exchange Online の spam 設定

現在，Exchange Online の spam に関する設定は，Office365 の管理ツールにある Exchange 管理センターから行うことができる．現行の設定は，次の通りになっている．

機構全体として管理している「kosen-ac.jp」のドメインからの送信メールの場合，spam メールであるかを判定するための spam フィルターの処理内容は，『spam フィルターは常に有効』から変更できないようになっている．

送信メールが spam メールと判定された場合，spam メールと判定されたメールをコピーして，機構本部が指定したメールアドレスへ送信する設定ができるが，現在は，機構全体の管理としては，この設定を無効にしている．この設定による動作は，少量の spam メールの送信に対して適用される設定内容であり，大量に spam メールが送信された場合には，その該当ユーザからの送信を Exchange Online の仕様としてブロックする動作となっている．

そして，大量に spam メールを送信し，メールの送信がブロックされたユーザがいる場合，管理者が指定したメールアドレスへ通知する設定ができるが，先ほどの設定と同様で，こちらも通知しない設定としている．

一方，受信メールが spam メールと判定された場合，受信者の迷惑メールフォルダにメールを振り分けるように設定されている．そして，広告メールや宣伝メールのように不特定多数に大量に配信されるメールについても受信者の迷惑メールフォルダに振り分けるように設定されている．そのため，必要なメールが spam メールと判定されたとしても，各利用者の迷惑メールフォルダに入っているため，各利用者の判断において，メールを確認することができる．迷惑メールフォルダに誤判定で分類されてしまった場合は，図 5 のように各利用者で迷惑メールフォルダに分類されないように，信頼できる差出人として設定することができる．

図 5　迷惑メールフォルダ設定

3.3 Microsoft Exchange Online の運用状況

Exchange Online の運用状況は，セキュリティ/コンプライアンスセンターのレポートメニューの中にあるダッシュボードからメールの送受信の数量や迷惑メール，マルウェアの送受信の数量をグラフで確認することができる．

ダッシュボード上では，各グラフが 1 つの画面上に表示されているため，spam メールの量をより詳細に確認したい場合は，迷惑メールの検出というグラフを選択する．迷惑メールの検出を表示させた場合は，次のようになっている．

- 既定の設定では，前日から過去 7 日間について表示されている．そのため，当日の現況について，リアルタイムで spam メールの現状を把握することができない．
- グラフに表示することができる期間は，前日から過去 90 日前までである．
- 横軸が日付となっているため，各日付の spam メールの数量は把握できる．しかし，表示している期間の合計での spam メール量となると，各日付の spam メールの量を足していかないと把握することができない．

また，Office365 は機構本部で調達されたシステムであるため，Exchange Online の運用状況も機構全体としての状況は把握しやすいが，本校だけの運用状況を確認することが難しい．

4. 運用上の課題と現時点の解決策

本節では，二つのメールシステムの運用上の課題と現状における解決策を記載する．

4.1 Exchange Online 用メーリングリストの運用

本校では，各クラスへの連絡で利用できるように，各クラスのメーリングリスト(以下，ML)を作成し，年度初めにメンバー更新を行い，活用している．この ML に登録されているメールアドレスは，本校の SMG メールシステムのメールアドレス「@tokuyama.ac.jp」についてである．

学生は，学内の教育電算室に設置されているパソコン，または Web メーラである xGate4 を利用し，本校のメールを確認することができる．この xGate4 は，学外からも利用可能であるが，あらかじめログイン URL を知っておく必要がある．これらの環境で学生は，自ら定期的にメールの確認を行う必要があり，そのための教育も必要である．

一方，Exchange Online で使用するメールアドレス「@tokuyama.kosen-ac.jp」を活用すれば，第 3.1 節でも述べたようにアカウントの設定を各利用者が行えば，いつでもプッシュ型メールで受信ができる利点がある．

今年度，1 年生担任から Exchange Online の利点を活用し，クラス連絡を行いたいという依頼があった．そこで，情報処理センターでは，Exchange Online のメールアドレスを登録し，ML を作成することになった．

ML の作成においては，次の 1)～3)の方法がある．

1)　既存の ML システム[4]を使用

本校では，独自開発した Web 上から本校のメールシステムを用いて ML が作成できるようになっている．

この機能は，本校のメールアドレス以外のメールアドレスも登録できるようになっているため，既存システム上で ML を作成可能である．

2)　Office365 セキュリティ・グループを使用

「@tokuyama.kosen-ac.jp」のドメインをグ

ループのアドレスとして利用できる．各ユーザでグループを作成することができず，管理者が作成しなくてはならない．また，グループメンバーの更新を手作業で行う必要がある．

このグループは，Office365 アプリケーションでも活用できる．外部の送信者を受け付ける設定にしない限り，「kosen-ac.jp」以外からの送信はできない．

3)　Office365 グループを使用

各ユーザで自由に作成することができる．「@tokuyama.kosen-ac.jp」のドメインをグループのアドレスとして利用できない．グループメンバーの更新を手作業で行う必要がある．

先に示した 2)，3)の通り，Office365 上でグループを作成し，ML として利用することはできる．しかし，ML の利用方法について，高専機構全体としてはほぼ定まってきた段階であるため，本校における利用方法を定めるまでには進んでいない．現時点では，更新するためのリストをグループ作成希望者が準備し，作成から登録までを管理者(情報処理センター)が手作業で行うような試行をしている段階である．

そのため，学生へのサービスとなると，不具合が生じたときに対処の行いやすい運用実績のある前述の 1)の方法で，本年度は実現した．

実際に，1)の方法により作成した ML を運用したところ，図 6(a)のように Exchange Online のメールアドレスから，登録した ML にメールを送信すると Outlook で確認した際に，迷惑メールフォルダに振り分けられるという問題が発生した．

一方で，図 6(b)のように，学内のメールアドレスから今回作成した ML に送信した場合は，迷惑メールフォルダには振り分けられなかった．

原因として，学内から送信したメールは，SMG，Firewall を通過して，Exchange Online に届き，各ユーザに配送される．しかし，Exchange Online から ML 宛にメールを送信すると，図 6(a)のように Exchange Online から一度学内のメールサーバに届き，そこから，もう一度 Exchange Online へ配送される．そのため，Exchange Online 内で完結するような配送であるにも関わらず，外部のメールサーバを経由して届くために，なりすましやその他の spam メールと判断され，迷惑メールフォルダに振り分けられるのではないかと考えた．

迷惑メールフォルダへの振り分けを停止するには，第 3.2 節の図 5 で示した方法により，各ユーザで，tokuyama.ac.jp を信頼するように設定をする方法がある．しかし，上記の方法で ML を利用する全てのユーザ

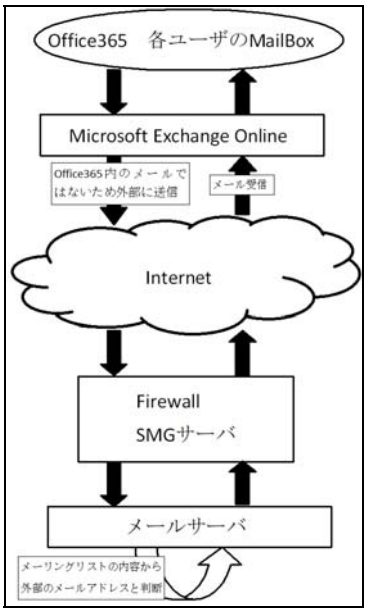

図 6(a)　ML へのメール送信

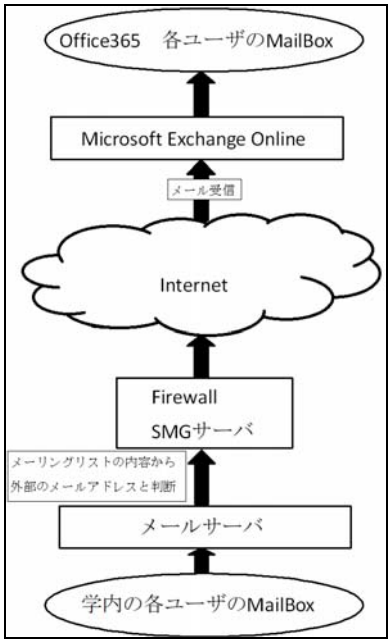

図 6(b)　学内からの ML へのメール送信

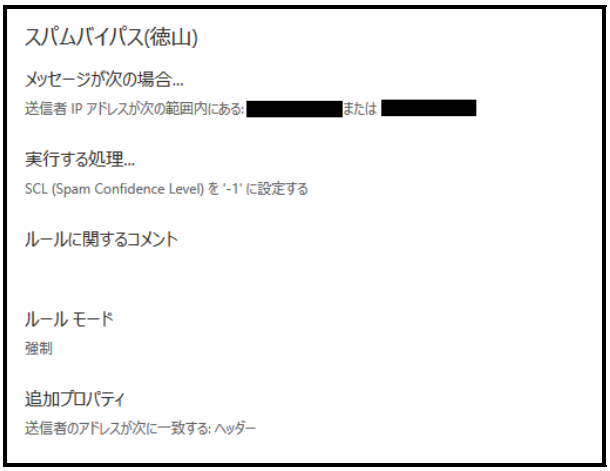

図 7　迷惑メールフォルダの振り分け設定

を手作業で登録するのにはユーザの手間がかかる.

管理者が一括で設定する方法を調べるとExchange管理センターで設定できることが判明した. Exchange管理センターのメールフローのルール設定を図7に示す. 本校のメールシステムから受信したメールはspamメールと判定されないよう, 常に Spam Confidence Level を‘-1’にするように設定した.

上記の設定により, Exchange Online のメールアドレスを利用して, 学内の ML に送信しても迷惑メールフォルダに振り分けられないようになった.

4.2 メール配送状況についての問い合わせ対応

本校のメールシステムを利用している利用者から「メールが正しく宛先に送信されたか確認してほしい」や「ある送信元からメールが届いているかどうか確認してほしい」などメールの配送状況について問い合わせがある.

本校のメールシステムの場合は, 管理者が本校の情報処理センターのため, 問い合わせがあった内容によって利用者の同意のもと, メールの配送状況を確認することで問い合わせに応じている.

しかし, Exchange Online で同様な問い合わせがあった場合, Office365 については, 全ての管理者権限を持つのは機構本部であり, 本校は Office365 の一部の管理者権限しかない. 状況に応じて, 機構本部にしかできない操作については, 機構本部へ問い合わせなければならない.

そのため, 本校では, ユーザからのメールの送信ができているかの問い合わせや, ある宛先からメールが届いているかのような問い合わせ内容に答えることができないことが予想される.

Office365 は, 共通のクラウド型システムのため, メールを送信する際に, 機密性を要する場合には, 推測されない件名の付け方や添付ファイルの暗号化が必要である. そのために, 学内でセキュリティ教育を実施し, ユーザのセキュリティに対する意識を高めていかなければならない.

4.3 課題の整理

現時点では, 本校のシステム(tokuyama.ac.jp)ならびに, 機構本部のシステム(tokuyama.kosen-ac.jp)の2つのシステムを並行稼働させている.

機構本部のメールシステムへ変更することは, 各利用者にメールアドレスを変更するようにお願いすることであるため, この先数年は, この 2 つのシステムのそれぞれの利点を生かしながら, 運用を継続することになる. 最終的には, 機構本部のメールシステムに移行することから, 現時点での課題は以下の通りとなる.

- 4.1 節に述べた「グループ」の仕組みについて, 機構本部の動向や他校の動向を見つつ, 技術的な方法を調査した上で, 運用方法を確立していく必要がある.
- 4.2 節に述べた通り, 各利用者からの問い合わせに対して, メールの疎通が適切に行えるという技術的な面での支援に加えて, 本校で調査可能なこと, 本校で技術的に対応可能なこと, 本部に依頼すべきことを事前に整理しておく必要がある.

5. まとめ

本論文では, SMG を利用した本校の SMG システムと機構本部が調達した Exchange Online の spam メール対策及び運用状況について述べた.

SMG のレポート機能を用いて, 現在も7割程度の spam メールが検出されており, spam メール対策が有用であることを確認した.

Exchange Online では, spam フィルターで迷惑メールフォルダに分類される設定になっていることを確認し, 報告した. 実運用として, spam メールに誤分類が発生した際の回避方法について調査し, その調査事項に基づいて運用していることを報告した.

本校のメールシステムや Exchange Online を利用する際の運用時の課題について整理した. これらを今後どうしていくのか学内で検討し, 解決する必要がある.

文献

1) シマンテック電子メールゲートウェイセキュリティソフト公式Webサイト
https://www.symantec.com/ja/jp/products/messaging-gateway (2018/09/05 Online)
2) 林, 鳥居, 義永, 新田, 力, 国重, 室長, 池田, 桑嶋, 栁澤 : 本校における迷惑メール対策の運用とその状況, 徳山工業高等専門学校紀要, 第 31 号, pp.69-72(2007)
3) Microsoft Office365 公式Webサイト
https://products.office.com/ja-jp/business/office (2018/09/05 Online)
4) 鳥居, 林, 新田, 力, 桑嶋, 栁澤, 池田, 国重, 室長, 義永 : Web ベースの簡単メーリングリスト管理システム, 徳山工業高等専門学校紀要, 第31号, pp.65-68(2007)

(2018.09.05 受理)