フィルタリング環境下における迷惑メールの分析

松田 勝敬*

Analyzing Spam Mail Under the Filtering Environment

Masahiro MATSUDA *

abstract

This paper analyzes spam mail filtered out at and passed through the anti-spam filter deployed in the campus network, in order to understand the characteristics of recent spam mails. The analysis was done on spam mails received by three email accounts that have different usage characteristics. This analysis results show that the trend in the change of the number of received spam mail does not heavily depend on the usage characteristics of email accounts. Then, the author focused on the specific email address which was involved in past security incident occurred within the campus network. The author found that interpret as an indication of the occurrence of some security incidents. The analysis technique described in this paper uses only generic information available for all users. Therefore, the technique can be utilized as a useful security measure for user in future cloud environments when they can handle the only limited information.

1. はじめに

電子メールの歴史はインターネットより古く，インターネットが普及する過程の中で最初期から広く使われており，今日でも世界中で使われている重要なツールである。現在では，インターネットを利用する情報伝達手段として一般的に普及しており，様々な業務を行う上で必要不可欠なものとなっている。電子メールの基本的な仕組みは，コンピュータやコンピュータネットワークにおいてセキュリティ対策の実装がほとんど必要なかった時に作られたものである[1]。そのため現在では様々な脅威にさらされており，全て後付の対策をシステムに付加することにより運用されている。多くの対策が実装されているにもかかわらず，根本的な対策が難しいことから，電子メールには様々な脅威が存在している。

特に「迷惑メール（spam）」と呼ばれる，受信を望んでいないが一方的に送られてくる電子メールが大きな問題となっている。総務省の調査[2]では，世帯において迷惑メールを 1 日に 10 通以上の頻度で受信する割合が，自宅のパソコン，携帯電話，スマートフォンの全てで 20%を超えており，国内でも迷惑メールが多く流通していることがわかる。また，全世界で流通する電子メールの内 8 割以上が迷惑メールであるとする調査[3]もあり，電子メールというシステムのリソースの多くが有効に使われていない状態と考えることもできる。

このような現状でも，電子メールは重要なインフラのひとつとして使われ続けており，今後も同じ状況が続くと考えられる。よって，電子メールに関する様々なセキュリティ対策を施すことにより，脅威の影響を少なくし，対処しながら利用することが現実的である。そこで本論文では，電子メールシステムのセキュリティ対策を実装している環境における，迷惑メールの受信状況を解析することにより，ユーザーに対する有効な対策を検討する。

セキュリティ対策を実装している電子メール環境として，東北工業大学（以下本学）の環境で調査を行った。

2. 東北工業大学の電子メール受信環境

2.1 概要

本学は SINET[4]に加入しており，WAN 回線は SINET5 に接続しており，SINET 経由でインター

2016 年 10 月 25 日受理
* 情報通信工学科 准教授

ネットに接続している。基幹情報システムは 2015 年度に更改され，電子メールシステムもその時に更改されている。その際に，それまでは学内に設置したサーバ（オンプレミスサーバ）で一括して処理を行っていた電子メールを，一部クラウドメール[5]に移行している。 クラウドメールの環境は，運用している業者が様々なセキュリティ対策を施しているが，実際にどのような対策を実装しているか，またその実装の詳細については公開されていないことが多く，公開されている情報も限定されている。そこで学内のオンプレミスサーバで受信できるメールアカウントについて扱うこととした。

本学のクラウドメールの環境は，新たにクラウドメール用のメールアドレスとして，第 4 レベルドメインを付与したドメイン名で運用している。オンプレミスサーバによるメールシステムは，2015 年度のシステム更改以前からのメールアドレスを継続して利用することができる。

2.2 メール受信環境の構成

本学のオンプレミスサーバによるメールの受信時の流れの概要を図 1 に示す。WAN から本学のメールアドレス宛に届いたメールは，IPS(Intrusion Protection System)と Firewall で不正な通信ではないか監視を受ける。IPS と Firewall を通過すると，外部向けの MTA(Mail Transfer Agent, メール転送サーバ)が受信し，Anti spam フィルタに転送する。

ここで迷惑メールと判断されたメールは，フィルタによって保留される。メールの送信先には，メールが届いたが，迷惑メールと判断されたという内容のメールが配信される。このメールには，下記情報が含まれている。

① 差出人のメールアドレス
② 宛先に記載されたメールアドレス
③ Cc に記載されたメールアドレス
④ 件名
⑤ 迷惑メールを保留した旨のメッセージ
⑥ 保留されたメールを確認する Web UI のログインアドレス

このメールを受信したユーザーは，⑥の Web UI を用いると, spam と判定され保留されたメールを確認することができる。これにより，誤ってフィルタで保留されたメールもユーザーが確認できるようになっている。

Anti spam フィルタを通過したメールは，次に Malware Filter に転送される。添付ファイルに悪意のあるファイルが含まれていると判断された場合は，添付ファイルが削除されメールの送信先

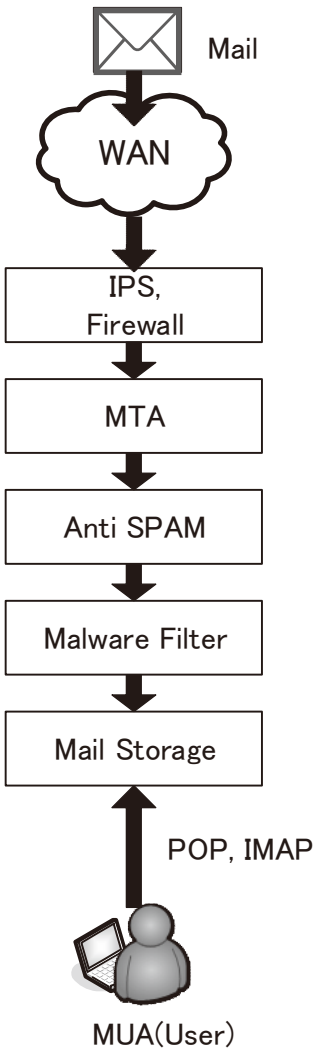

図 1　メールの受信時の流れ

に Malware と判断されたファイルがあった旨のメールが送信される。Malware が検出されなかったメールは, Mail Storage に転送され, 保存される。

Mail Storage に対して，ユーザーは学内ネットワークからのみ POP や IMAP でアクセスすることができ，受信したメールを確認，PC などにダウンロードすることができる。ユーザーは各自で MUA(Message User Agent, メールソフト)を用いることが可能で，PC やスマートフォンで学内ネットワークを経由してメールを管理している。MUA によっては，独自の迷惑メールをフィルタリングしたり隔離する機能を実装している場合もある。基幹部のセキュリティ対策をくぐり抜け Mail Storage に届いた迷惑メールを, MUA で対応できる場合もある。

本学では，Web UI による MUA[6](Web Mail)がオンプレミスサーバによるメールシステムのユーザーに対し提供されている。

3. 迷惑メールの受信状況

3.1 調査概要

電子メールシステムのセキュリティ対策を実装している環境における，迷惑メールの受信状況を調査した。本学のオンプレミスメールサーバによるメールシステムのアカウント3つを対象とした。それぞれ，日常的に利用している個人アカウントA, 日常的に利用している共有アカウントB, 利用頻度が低い共有アカウントCについて，調査を行った。ここで「共有アカウント」とは，学科や課などに割り当てられた，その組織に所属する複数の教職員で利用しているメールアカウントのことである。迷惑メールではないメールも含めたメールの送受信数は，Aが一番多く，次にBとなり，Cが最も少ない。

また，アカウントAに届いた迷惑メールから，Phishing Mailの手口について調査を行った。

3.2 調査対象メールアカウントのアドレス

調査対象の3つのアカウントのメールアドレス公表状況は次のとおりである。

アカウントAは本学や所属する組織のWebサイトでは, 名簿や問い合わせ先としてhtmlファイルへのテキストによる記載や，画像ファイルなどでのメールアドレス表記もされていない。大学ホームページから閲覧可能なpdfファイルや，学会などでの論文に関連したページなどでメールアドレスがテキストで公表されている。また，個人のメールアドレスのため，名刺への記載や，日常業務でのメールの送受信で用いており，学内外を問わず多くの個人や組織が管理しているアドレス帳への登録や，メール情報として保存されている。学内外のどちらにも頻繁にメールが送受信されている，アカウントである。

アカウントBは，組織の代表メールアドレスとして，Webページで mailto タグでの記載もされ，公表されている。また，各種イベントなどの案内において，電子媒体でも紙媒体などでも広く公表されているアドレスである。利用目的としては，学外とのやり取りに用いられることが多い。

アカウントCは組織の代表メールアドレスであるが, 本学や組織のWebページでの公表はされていない。イベント開催時などの受付メールアドレスとして，pdf ファイルや紙媒体の配付物などに記載されているが，調査期間内および調査機関の過去1年間の間には，これらの公表もされていない。利用目的としては，学外とのやり取りに用いるためのアカウントである。

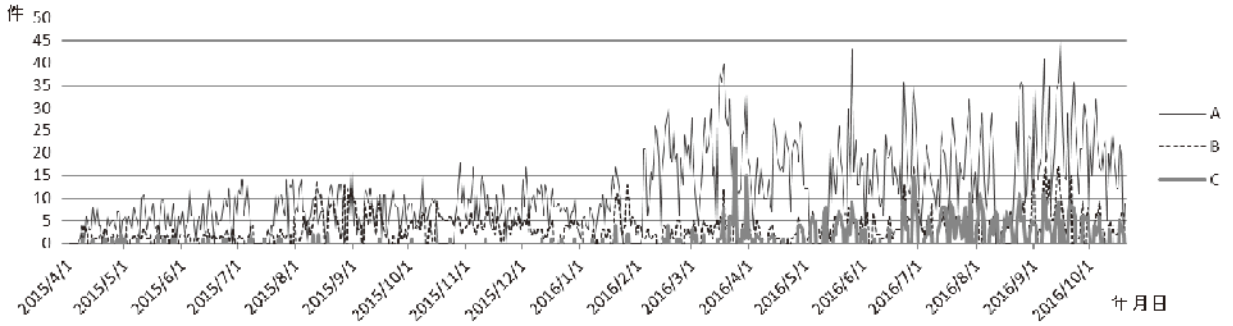

図2　迷惑メール受信件数（Anti spam フィルタ）

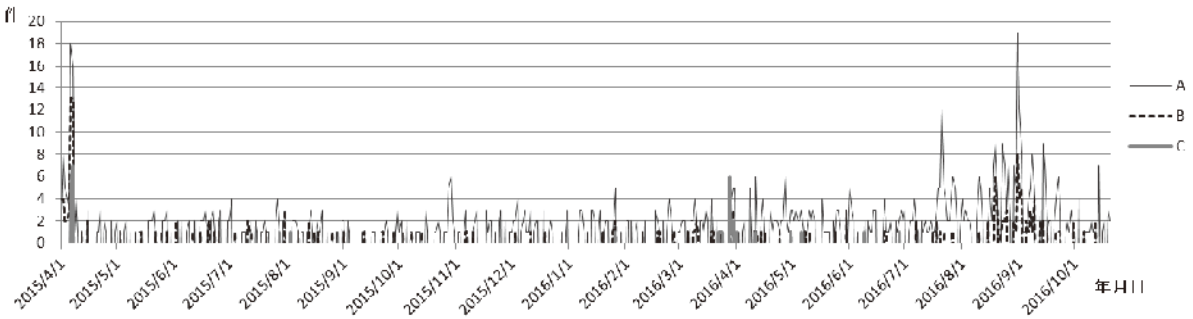

図3　迷惑メール受信件数（Mail Storage）

3.3 迷惑メール受信数

メールアカウント A, B, C について，迷惑メールの受信数を調査した。迷惑メールは，Anti spam フィルタで検出されたものは保留され，Mail Storage に配送されない。そのため，迷惑メールの数は Anti spam フィルタで検出されたもの，および Mail Storage に配送されたものの両方を数えた。Anti spam フィルタでは，自動的に迷惑メールと判断され保留した件数を数えた。Mail Storage に配送されたものについては，MUA の迷惑メール振り分け機能による自動振り分けによるものと，内容を確認して手動で迷惑メールと判断し振り分けたものをあわせた件数とした。MUA の迷惑メール振り分け機能では，送信先のメールアドレスが存在しない場合のエラー通知メールも自動で迷惑メールとして振り分けられていた。これらのエラー通知メールは迷惑メールではないため，手動で除外をした。

Anti spam フィルタで検出された迷惑メール数を図 2，Mail Storage に配送された迷惑メール数を図 3 に示す。縦軸は迷惑メールの件数，横軸は年月日を示す。現在のシステムが導入された 2015 年 4 月 1 日から，2016 年 10 月 20 日までの期間について示した。

4. 迷惑メールの受信に関する考察

4.1 時期による受信状況

A, B, C の全てのメールアカウントで，概ね半数以上の迷惑メールが Anti spam フィルタで保留されていた。そのため，Mail Storage での迷惑メール件数は，Anti spam フィルタでの検出件数より少なくなっているが，全てのアカウントで運用開始直後の 2015 年 4 月初旬は，Mail Storage での件数が多くなっている。これは，システム稼働直後は本学の環境にあわせたフィルタの調整が不十分であったり，フィルタに迷惑メールとして登録されていた情報が少なかったことにより，機能が有効に働かなかったことが考えられる。稼働環境や状況にシステムが適応し，2015 年 4 月中旬以降は安定稼働していると思われるアカウント A については 2016 年 2 月頃から，Anti spam フィルタの検出件数が増えている傾向にある。また，調査した全てのアカウントで，2016 年 3 月下旬や，2016 年 9 月で受信件数が増えている期間などがある。これらの原因は，対象となるメールアドレスがイベントなどで周知されたり Web などで公開され，迷惑メール送信者の送信リストに新たに登録されたりしたことが原因と考えられるが，特定するには更に多くのアカウントについて，迷惑メール状況を調査する必要がある。

4.2 アカウントによる受信状況

メールアカウントの利用頻度の違いと同じように，アカウント毎に迷惑メールの受信数も異なっている。通常のメールも含めてメールの送受信数が最も多いアカウント A は，Anti spam フィルタ，Mail Storage のどちらも他の B, C のアカウントより迷惑メール受信件数も多い。最も利用頻度が低いアカウント C が，迷惑メールの受信件数が少ない。

メールアカウントの利用頻度が多いと，イベントなどで出版物や Web サイトなどでメールアドレスが公表される機会も多く，迷惑メールなどを送信する目的でメールアドレスを収集したリストなどに，メールアドレスが登録される機会も増えることが考えられる。また，メールをやり取りしている他のアカウントが，Malware などにより汚染された場合に，アドレス帳や保存されていたメールの情報が漏洩し，迷惑メール送信先アドレスとして使われる機会も多くなる。

これらのことから，総合的なメールアカウントの利用頻度に応じて迷惑メールの受信件数も増減すると考えられる。

また，アカウント毎の迷惑メール受信件数について，相関係数を求めた。Anti spam フィルタでの迷惑メール受信件数の相関係数を表 1 に，Mail Storage での迷惑メール受信件数の相関係数を表 2 に示す。件数が少ないこともあるが，それぞれのアカウント間である程度の相関があることがわかる。このことより，これらのアカウントについては，同じ時期に迷惑メール数が増えるといえる。この要因としては，3 つのアカウントの共通ドメインに関してセキュリティインシデントが発生した，共通ドメインのメールアドレスに対する迷

表 1　迷惑メール受信件数の相関係数
(Anti spam フィルタ)

	A	B	C
A	1.00		
B	0.44	1.00	
C	0.64	0.59	1.00

表 2　迷惑メール受信件数の相関係数
(Mail Storage)

	A	B	C
A	1.00		
B	0.62	1.00	
C	0.36	0.56	1.00

惑メールの送信がおこなわれた，などが考えられる。

例えば 3 つのアカウントは同じ学内の同じドメインに所属しているため，学内で Malware などによるセキュリティインシデントが発生し，同時期にメールアドレスが漏洩し迷惑メールの送信先に登録されたり，インシデントによって直接迷惑メールが送信されると，3 つのアカウントは同じ時期に迷惑メールを受信することは有り得る。

4.3 迷惑メール送信先

迷惑メールを受信する場合には，受信したメールアドレスが迷惑メールのヘッダの To, Cc, Bcc のフィールドの値として記載されている。そこでメールの宛先を示す To フィールドの値について，調べた。それぞれのアカウント A, B, C が受信した迷惑メールの To フィールドの値上位 3 つまでを，Anti spam フィルタでの受信件数(表 3)，Mail Storage での受信件数（表 4）をまとめた。「bcc のみ」は，To フィールドの値は無く，bcc フィールドにのみ送信先メールアドレスが記載されていた場合を示す。「学内の実在アドレス」は，同じドメイン内（大学内）で実際に存在するメールアドレスの値を示す。Mail Storage で受信した C で 2 番目に多かった「他ドメインのアドレス」は，実在する国際会議に関連するメールアドレスであった。

アカウント A が Anti spam フィルタで受信した迷惑メール以外は，そのアカウント自体のメールアドレスが最も多かった。アカウント A についても，2 番目に A のメールアドレスが多くなっている。迷惑メールの送信は，何かしらの方法で入手したメールアドレスを To フィールドに記載して送信することが多い事がわかった。これは，メールの受信者は，一般的に自分に届いたメールのなかで，自分のメールアドレスが Cc などでなく，To フィールドに記載されているメールの方が自分宛てに届いたと理解するため，メールを開封する確率が高くなるからと思われる。

「Bcc のみ」の場合は，Bcc フィールドの値にその中に受信したアカウントのメールアドレスがあった場合である。Anti spam フィルタで受信した迷惑メールの中では，アカウント A は最も多く，アカウント B, C では 2 番目に多かった。Mail Storage で受信した件数でも，アカウント A, B で 2 番目に多い結果であった。この方法でメールを送信すると，一つのメールが複数の送信先に配信されるようにメールを送信しても，他にどのメールアドレス宛に送信されたかがわからなくなる。一般的に，To や Cc フィールドに多数の宛先メールアドレスを記述することは，セキュリティ上も好ましくないとされている。そのようなメールは余り見られず，受信者な通常のメールではないと気づき易いことなどから，「Bcc のみ」の迷惑メールが多いことなどが想像できる。

表 3　To フィールドの値(Anti spam フィルタ)

順位	A	B	C
1	Bcc のみ	Bのアドレス	Cのアドレス
2	Aのアドレス	Bcc のみ	Bcc のみ
3	学内の実在アドレス	学内の実在アドレス	学内の実在アドレス

表 4　To フィールドの値(Mail Storage)

順位	A	B	C
1	Aのアドレス	Bのアドレス	Cのアドレス
2	Bcc のみ	Bcc のみ	他ドメインのアドレス
3	学内の実在アドレス	学内の実在アドレス	学内の実在アドレス

5. セキュリティインシデントの影響

5.1 迷惑メールの宛先への実在アドレスの記載

4.3 において，「To フィールドに受信者のメールアドレス」と，「Bcc のみ」の迷惑メールが多いことは，迷惑メールの受信者は自分のメールアドレス以外に送信先の情報が無いメールを受信することになる。この様な迷惑メールが多いことから，迷惑メールの送信者はなるべくメールの送信に関する情報は記載しないようにしている意図があると考えられる。しかし，今回の調査対象のなかで，各アカウントが受信した迷惑メールの宛先として，3 番目に多かったものは，表 3, 4 より全て「学内の実在アドレス」であった。「学内の実在アドレス」が記載されているということは，受信者以外のメールアドレスの情報が記載されていることになる。そこで，実際に記載されていた「学内の実在アドレス」について，検討を行った。

5.2 セキュリティインシデントによるメールアドレスの漏洩

Malware の実行による情報漏洩は，それに伴いアドレス帳やメールの情報から，直接セキュリティインシデントに関連しないアカウントのメールアドレスなどの情報も漏洩する。漏洩したメールアドレスが迷惑メール送信リストに登録され，その結果迷惑メールの受信件数が増えることも考えられる。また，インシデントの内容によっては，そのインシデントにより直接迷惑メールが送信されることもある。このように，Web サイトなどでメールを公表していたり，アカウントの利用者が情報漏洩を発生させない場合でも，迷惑メールの送信先とされることがある。

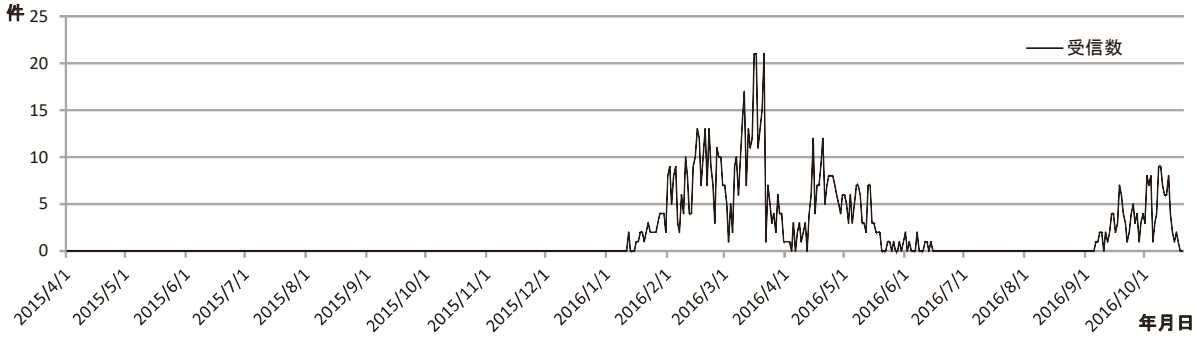

図 4　セキュリティインシデントに関連したメールアドレスを含む迷惑メール受信件数

5.3 セキュリティインシデントに関係するメールアドレス宛の迷惑メール

表 3 における，アカウント A が Anti spam フィルタで受信したなかで，3 番目に多い「学内の実在アドレス」は，セキュリティインシデントが発生したアカウントのメールアドレスであった。このインシデントに関連したメールアドレスを D とする。アカウント A に届いた，メールアドレス D が宛先として To フィールド含まれるメールについて，受信数を調べた。その結果を図 4 に示す。横軸は年月日を示し，2015 年 4 月 1 日から 2016 年 10 月 20 日までである。縦軸は，アカウント A が Anti spam フィルタで受信したメールアドレス D が宛先として To フィールド含まれるメール迷惑メール受信件数である。

2016 年 1 月 12 日に初めて，メールアドレス D が宛先として To フィールド含まれるメール迷惑メールを受信し，2016 年 6 月 14 日までの間に，775 件受信している。その後，メールアドレス D が宛先として To フィールド含まれるメール迷惑メールは届かなくなった。2016 年 9 月 6 日から再びメールアドレス D が宛先として To フィールド含まれるメール迷惑メールが届くようになり，2016 年 10 月 18 日までに 160 件受信している。調査期間が 2016 年 10 月 20 日までであるので，10 月 18 日から 2 日間は受信件数は 0 であるが，その後また続いていることも考えられる。

この結果から，一度インシデントが発生して暫くの間迷惑メールの送信が続き，5 ヶ月程度でその送信が停止したが，また再び迷惑メールの送信が開始されたことを示している。このようなことが起こり得る場合は，例えば次の様な状況が考えられる。

(1) 同じアカウントに関してセキュリティインシデントが 2 回発生した。
(2) 一度漏洩したメールアドレスが，再度迷惑メール送信先として使われた。
(3) Malware などにより迷惑メールを送信しているコンピュータが，一定期間停止していた後再び稼働した。

いずれにしても，あるメールアドレスが含まれる迷惑メールの受信件数が増加した場合には，セキュリティインシデントの発生と関連していることがあることがわかった。これにより，特に同じドメイン内のメールアドレスを含む迷惑メールが増加した場合は，インシデントの発生を強く示唆していると考えられる。

迷惑メールに含まれるメールアドレスについてアドレス毎に件数を監視すれば，その件数の変化からセキュリティインシデントの検知などに応用することも可能である。

6. まとめ

オンプレミスサーバで構成される電子メールの受信システムにおいて，基幹部でセキュリティ対策を施している場合に，ユーザーが確認できる迷惑メール情報について考察を行った。

それぞれ詳細について調べれば，その原因が明らかになることもあると思われるが，今後の対策として対応しやすい手段を検討するために，自動化などがしやすい手段を中心に検討した。

メールの利用頻度が異なるアカウントについて迷惑メールの受信件数，受信した迷惑メールの宛先フィールドに含まれる値について調査をおこなった。その結果，メールの利用頻度に依らず，迷惑メールの受信件数の日時変化の傾向は大きな違いがないことがわかった。また，迷惑メールの送信先に含まれるメールアドレスは，受信したメールアドレス宛に届くものと，To フィールドの値がなく Bcc にのみ記載されて届くものが多いことがわかった。これらの傾向もメールの利用頻度によって大きく異ならないこともわかった。また，同じドメイン内で発生した，セキュリティインシ

デントに関係するメールアドレスを含む迷惑メールの受信状況から，セキュリティインシデント発生の検出要素の一つと成り得ることがわかった。

本論文では，基幹部に設置するサーバやセキュリティ装置ではなく，一般ユーザーとして入手できる情報を元に考察を行った。これらの考察は，クラウド環境などで，システムの構成が明らかにされていない場合にユーザーとしてのセキュリティ対策に応用することが可能である。例えば，MUA などのユーザーが使うツールに実装するセキュリティ対策などで，有効な手段となる。

今後は，情報システムのクラウド化が一層進むと考えられるが，システムのユーザーとし入手できる情報からのセキュリティ対策を検討することにより，PC やスマートフォンなどの端末にインストールするアプリケーションのセキュリティ対策機能の実装に役に立つであろう。

参 考 文 献

[1] D. H. Crocker, J. J. Vittal, K. T. Pogran, D. A. Henderson, Jr. : STANDARD FOR THE FORMAT OF ARPA NETWORK TEXT MESSAGES(1), RFC 733, (November 1977).

[2] 総務省 : 情報通信白書, 平成 28 年版, (2016).

[3] Cisco Systems : Sender Base , 入手先 http://www.senderbase.org/static/spam/ （参照 2016-10-20）

[4] 国立情報学研究所 : 学術情報ネットワーク SINET5, 入手先<http://www.sinet.ad.jp/>（参照 2016-10-20）.

[5] Microsoft : 教育機関向け Office365, 入手先 <https://www.microsoft.com/ja-jp/office/365/education/> （参照 2016 10-20）.

[6] 株式会社クオリティア : Active! mail, 入手先 http://www.qualitia.co.jp/product/am/ （参照 2016-10-20）.