Vol.2018-IOT-42 No.5
2018/6/28

送信元メールアドレス検査による spam 検知とその効果

吉田和幸[†1]，池部実[†2]，吉崎弘一[†1]

概要：インターネットの普及に伴い，電子メールは通信手段の基盤となっている．一方，電子メールは不正侵入のきっかけとなりやすいため，spam 対策は不可欠である．従来から用いられてきた spam 対策は，送信メールサーバの FQDN が，メールサーバらしいか，利用者端末らしいかを判断する S25R，一時エラー後のメールサーバの動作を確認するグレイリスティング，spam を送信したメールサーバの一覧表（ブラックリスト）など，メールサーバを検査するものが多かった．しかしながら，ID/パスワードの流出により，プロバイダのメールサーバ等の正規のサーバから送られる spam も増えてきている．そのため，2017 年 5 月より送信元メールアドレスの検査を強化した．本稿では，spam 検出方法とその運用結果について述べる．

キーワード：メール，spam，spam 対策

Anti-spam measures by sender mail address check and its effect

KAZUYUKI YOSHIDA[†1]　MINORU IKEBE[†2]
KOICHI YOSHIZAKI[†1]

Abstract: With the spread of the Internet, e-mail is the basis of communication means. Meanwhile, countermeasures against spam are indispensable because e-mail tends to trigger illegal invasions. Spam countermeasures conventionally used check sender MTAs, such as S25R for judging whether the FQDN of the sender MTA is like a mail server or user terminal, gray listing for checking the operation of the sender MTA after a temporary error, or sender MTA is on blacklist. However, due to the leakage of ID / password, spam sent from an authorized server such as a provider's MTA is increasing. Therefore, from May 2017 the inspection of the sender's mail address was strengthened. In this paper, we describe spam detection method by checking sender mail address and its operation result.

Keywords: e-mail, spam, anti-spam measures

1. はじめに

インターネットの普及に伴い，電子メールは通信手段の基盤となっている．一方，電子メールは不正侵入のきっかけとなりやすいため，spam 対策は不可欠である．従来から用いられてきた spam 対策は，送信メールサーバの FQDN が，メールサーバらしいか，利用者端末らしいかを判断する S25R, 一時エラー後のメールサーバの動作を確認するグレイリスティング, spam を送信したメールサーバの一覧表（ブラックリスト）など，メールサーバを検査するものが多かった．しかしながら，ID/パスワードの流出により，プロバイダのメールサーバ等の正規のサーバから送られる spam も増えてきている．大分大学情報基盤センターが運用するメールサーバでの，2016 年，2017 年の spam 検知数の推移を図 1，図 2 に示す．2016 年 9 月以降正常と判定されたメール(ham)の数が増減を繰り返すようになったため，2017 年 5 月より送信元メールアドレスの検査を強化した．

本稿では，2 章で，従来行ってきた spam 検知手法について述べる．3 章では，送信元メールアドレスによる検知法について述べ，4 章でメールログから集計した検知数により，効果について示す．5 章では，まとめと今後の課題について述べる．

†1 大分大学学術情報拠点情報基盤センター
Information Technology Center, Oita University
†2 大分大学理工学部共創理工学科知能情報システムコース
Computer Science and Intelligent Systems, Oita University

2. メールシステムの構成と従来実施してきた spam 対策

2.1 メールシステムの構成

大分大学のメールシステムは，インターネットからメールを受信して spam 対策を行う MTA(mail transfer agent, サーバ名 ajimu)とそれを通過したメールを受け取って受信者のメールボックスに配送する MDA(mail delivery agent)からなる[1]. ajimu での spam 対策の構成を図 3 に示す．図 3 では，各対策で spam と判定された場合には左に，ham（通常メール）と判定された場合には下に進む.

2.2 従来から実施してきた spam 対策

(1) **throttling**

throttling とは「spam 発信 MTA は timeout が短い」,「spam 発信 MTA は SMTP(Simple Mail Transfer Protocol)の確認応答手順を無視してメールを送る」との仮説に基づき，コネクション確立後の応答をわざと遅延させ，送信 MTA がこちらの応答を待たずにメールを送信してきた場合, spam と判断して受信を拒否する対策手法である[2]. throttling は遅延時間のみをパラメータとして設定する.

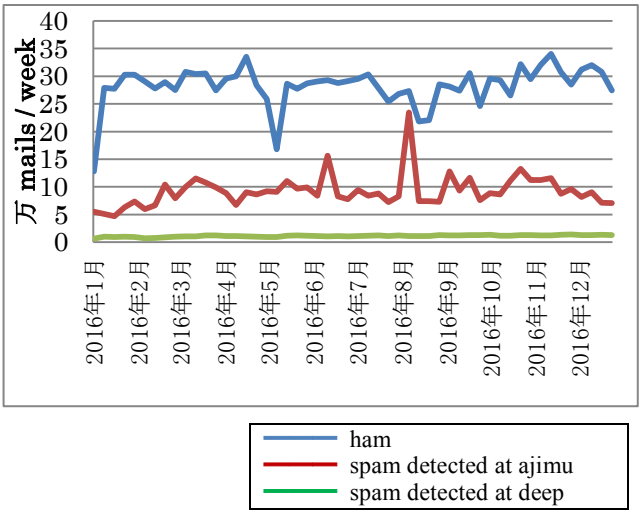

図 1　2016 年のメール受信数の内訳

Figure 1　Number of e-mails on 2016.

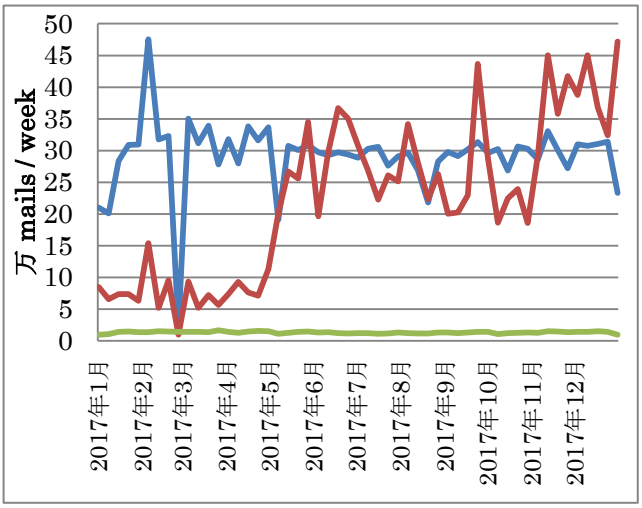

図 2　2017 年のメール受信数の内訳

Figure 2　Number of e-mails on 2017

(2)　送信元／宛先の検査

送信元メールアドレス，宛先メールアドレスの検査についてはドメイン部，ローカル部に分けて行う．

ドメイン部：(ア)．TLD(Top Level Domain)が，local または localdomain は，エラーとする．(イ)　DNS に登録がなければ一時エラーとする．(ウ)　A レコードが 127.0.0.1 と登録されていれば，エラーとする．(エ) 学外から来たメールの送信元アドレスのドメイン部が oita-u.ac.jp のときエラーとする．

ローカル部：(ア) ドメイン部が oita-u.ac.jp のときに，ldap にアカウントの有無を問い合わせる．アカウントが存在しなければエラーとする[3].

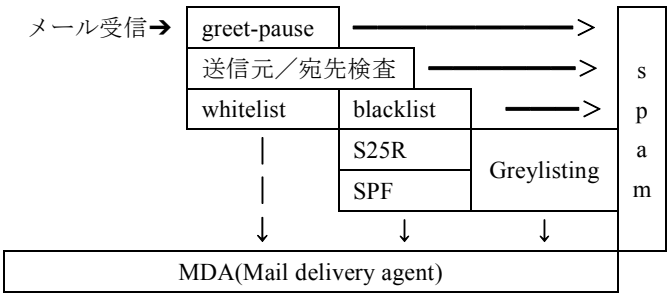

図 3．メールサーバでの spam 対策の構成

Figure 3. Antispam measures on MTA(ajimu)

(3)　whitelist

whitelist は，信頼できる MTA の IP アドレスを記述したリストである．通常 MTA からのメールであっても，spam 対策において spam と誤検知するケースが存在する．そのため，whitelist に spam 対策で誤検知されるが，信頼できる MTA の IP アドレスをリストすることで，誤検知される通常メールを受信できる．大分大学においては，dnswl.org[4]および独自に作成した whitelist を使用している．whitelist に記載された MTA から送信されるメールは spam 対策を省くことで，通常メールを遅延なく受信できる．

(4)　blacklist

blacklist は，spam 送信 MTA の IP アドレスを登録したリストである．メールの送信者と受信者の間に TCP コネクションが確立した時に，blacklist に掲載されている IP アドレスからのアクセスを拒否する対策である．blacklist として Sorbs.net[5]や Spamhaus Project[6]を用いている．

(5)　S25R

S25R は接続してきた MTA の FQDN を S25R のルールと照合し，エンドユーザコンピュータであるかどうかを推定する．エンドユーザコンピュータの多くは FQDN を設定していない．あるいは，エンドユーザコンピュータに対して FQDN を設定していても，IP アドレスの下位 16 ビットなど多くの数字を含むことが多い．図 4 に S25R で検知可能な FQDN の例を示す．S25R では，エンドユーザコンピュータからの spam をほとんど検出できる．しかし，通常の MTA の中には，S25R の規則に該当する FQDN を設定していることがある．そのため，このような MTA からの通常メールをエンドユーザコンピュータからの spam と誤検知する可能性がある．そのため，S25R で spam とされた場合は，すぐに spam とするのではなく greylisting により再度検査を行う．

ml-192-168-0-1.exampl.jp
adsl-192-168-0-1.example.com
1.0.168.192.example.net

図 4. S25R で検知可能な FQDN の例

Figure 4. Example FQDNs detected by S25R

(6) **SPF**

SPF(Sender Policy Framework)[7]は SMTP によるメールの送受信において，送信者の正当性を検証し送信者のドメインの偽称を防ぐ送信ドメイン認証方式である．SPF はメール受信時に，メールが送信者であるメールアドレス（エンベロープ送信者）のドメインから送信されたものかどうかを検証することで，メール送信者の正当性を確認する．送信側はあらかじめ自ドメインの権威 DNS サーバに，自ドメインでメール送信を許可する MTA を特定する SPF レコードを登録する．同時にその他の MTA からメールの送信があった場合の判定を SPF レコードの末尾に「記号(+, -, ~)all」の形式で記述する．「+」は当該ドメインの送信 MTA として認証(pass)，「-」は拒否(fail)，「~」は当該ドメインの送信 MTA ではないが，通常 MTA の可能性があることを示す(softfail)．SPF レコードの記述例を図 4 に示す．例えば，図 4 の example.jp の SPF レコードの場合，192.0.2.0/24 のネットワークから送信されたメールは，自ドメインからのメールであるため認証成功とし，それ以外のネットワークからのメールは認証拒否とする．

example.jp. IN TXT “v=spf1 +ip4:192.0.2.0/24 –all”
example.com. IN TXT “v=spf1 +ip4:192.0.2.0/24 +all”
example.info. IN TXT “v=spf1 +ip4:192.0.2.0/24 ~all”

図 5　SPF レコードの記述例

Figure 5. Example of SPF record

(7) **Greylisting**

greylisting[8]は tempfailing 手法のひとつで，「spam 発信 MTA は再送をしない」との仮説に基づいた対策手法である．一時エラーにより受信を拒否し，一定時間経過後に再送されたメールのみを受信する．再送した MTA は一定期間 greylisting の autowhitelist に登録される．autowhitelist に登録されていれば再送要求はせず，すぐにメールを受信する．ただし，短時間で再送された場合には，再度一時エラーで応答する．多くの spam 発信 MTA は配送効率を重視しているため，仮説通りに動作し，spam 排除の効果が高い．しかし，MTA に再送を要求するため配送遅延が大きくなりやすく，1 時間以上の遅延が発生する場合も多い．そのため，我々は，S25R, SPF で spam 判定されたメールのみ greylisting で検査する．

3. 送信元メールアドレスの検査

3.1 エンベロープ From とヘッダ From

送信元メールアドレスが現れるエンベロープ From, ヘッダ From の 2 か所について検査を行う．エンベロープ From は，メールを送る smtp プロトコル[9]の中で現れるものである．2 章(2)で行っている検査は，このエンベロープ From について検査をしている．smtp プロトコルの例を図 6 に示す．一方，ヘッダ From は，メールの中の From:ヘッダ[10]

送信元 MTA		宛先 MTA
	←	220
EHLO mail.example.jp	→	
	←	250
MAIL FROM:<foo@example.jp>	→	
	←	250
RCPT TO:<baa@example.com>	→	
	←	250
DATA	→	
	←	345
（メールデータの送信）	→	
.	→	
	←	250

図 6 smtp プロトコルの概要

Figure 6. Outline of smtp

に現れるメールアドレスである．通常，これら２つの送信元メールアドレスは同じものであるが，メーリングリスト等で，エンベロープ From は書き換えられることがある．

3.2 ドメイン名ブラックリスト／ホワイトリスト

独自のドメイン名ブラックリスト／ホワイトリストを作成するとともに，Spamhaus Project[6]のドメイン名ブラックリストを参照する．ホワイトリストには，属性型 JP ドメインをはじめ，受信するメール数が多いドメインを列挙している．ブラックリストには，筆者に届いた spam の送信元アドレスから再度送られてきそうなドメインを列挙している．ブラックリストの一部を図 7 に示す．たとえば，jp.com は，apple.co.jp.com, netflix.co.jp.com というドメイン名の送信元アドレスとし使われたことがある．

jp.com
ssl.com
service.com

図 7. 独自ドメイン名ブラックリスト(部分)

Figure 7. Example of domain blacklist

3.3 メールアドレスブラックリスト

筆者に届いた spam のうち，ドメイン名ブラックリストに登録できないものは，メールアドレスそのものをブラックリストに列挙する．メールアドレスブラックリストの一部を図 8 に示す.

3.4 表示名の検査

メールの From ヘッダの形式を図 9 に示す．From ヘッダは，＜と＞で囲まれたメールアドレスとその前に書かれる表示名からなる．Amazon からのメールでは，表示名に Amazon.co.jp と書かれている．それをまねて，表示名に Amazon.co.jp と書かれた spam も多数ある．そのため表示名がこのようになっていて，メールアドレスのドメイン部が

*amazon.co.jp，あるいは，*amazon.com でないものは，spam とする．現在，このような検査を netflix についても行っている．

3.5 適用順

ドメイン名の検査は, ホワイトリスト, ブラックリスト, spamhaus の dbl の順であり，MTA の IP アドレスの検査より優先する．Id，パスワードの流出等により，プロバイダのメールサーバから spam が送られる可能性があるからである．通常のメールも同じブラックリストに載せたメールアドレスを使っている可能性があるため，IP アドレスホワイトリストに載っていない MTA から来たメールのみにメールアドレスブラックリストを適用する. 表示名の検査は，ヘッダ From のみで，独立しているので，最初に行っている．

jp@icloud.com
noreply@icloud.com
noreply2@icloud.com
noreply3@icloud.com
noreply4@icloud.com
appleid@id.apple.com
appleid@appleid.apple.com
support@appleid.apple.com
info@mail.rakuten-card.co.jp
support@mail.rakuten-card.co.jp
webshop_noreply@emagazine.rakuten.co.jp
partner@shop.rakuten.co.jp
order@rakuten.co.jp

図 8.　メールアドレスブラックリスト（部分）
Figure 8. Example of mail address blacklist

From: 表示名 <メールアドレス>

図 9. From ヘッダの形式
Figure 9. Format of From header

4. 運用結果

2017 年 12 月 31 日から 2018 年 5 月 26 日までの 5 か月 (21 週間）メール数の集計結果を表 1 に，Greylisting の詳細を表 2 に示す．表 1，2 で，「Accept」は，再送により受信したメール数，「Autowhite」は，greylisting の autowhite list に載っているため，一時エラーなしで受信したメール数，「1st」は，最初に一時エラーとしたメール数，「2nd or more」は，短期間で再送されたため一時エラーとした回数である．greylisting により受信したメール数は，「Accept」＋「Autowhite」であり，検知した spam 数(greylist deny)は，

Spam 数　＝「1st」－「accept」

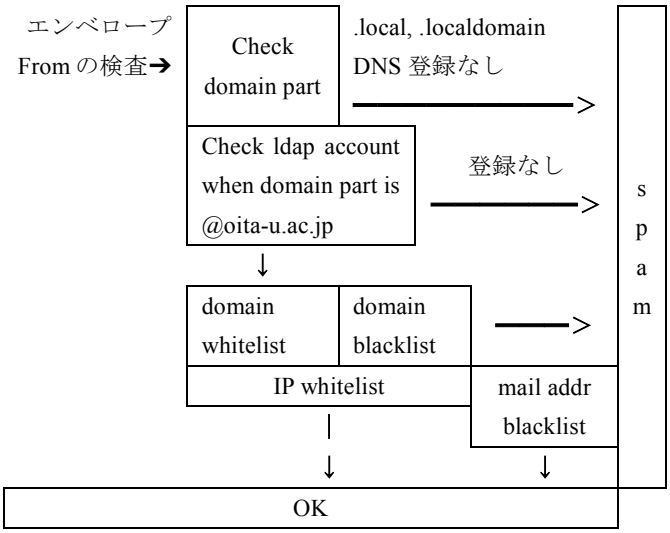

図 10. エンベロープ From の検査
Figure 10. Check for envelope From

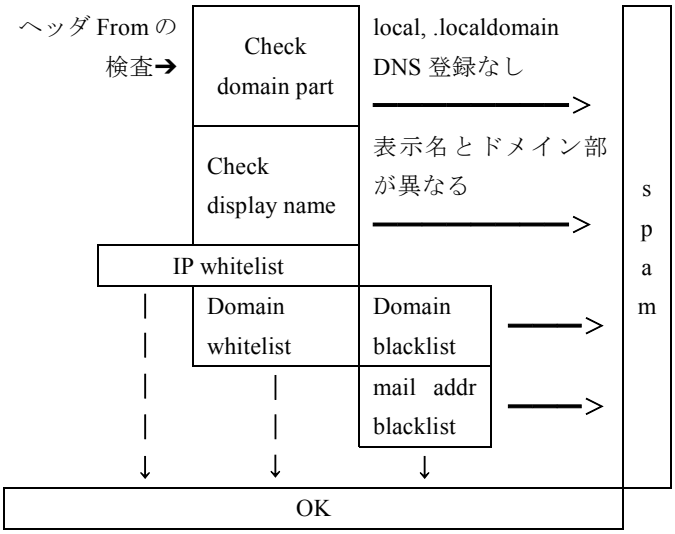

図 11　ヘッダ From の検査
Figure 11. Check for Header From

である．Ham（通常メール）および Greylist 関連の集計はメール数である．しかし，Greylist 以外の spam 数は，受信拒否の回数である．同じメールが何回も再送されている可能性もあり，多めに現れている．Ham(通常メール)数が，753 万通に対して，spam 数が，1320 万通と 2 倍近く多いのは，このためである．Firewall で Malware が検知された場合，当該 smtp コネクションはリセットされる．そのログには IP アドレスが表示されないため, Malware 欄の IPv4,IPv6 の内訳は不明である．

表 1 から，Ham(通常メール)753 万通のうち，受信時に再送遅延を強いているのは，「Greylist-accept」の 13 万 8 千通であり，受け取ったメールの 2%ほどである．

表 1 の spam 1320 万通のうち，envelope From での検知数は 1018 万通で 77%であり，Header From での検知数は 88

表 1　受信したメール数の内訳
Table 1 Breakdown list of received mails

種別	内訳	IPv4	IPv6	合計
ham	Whitelist	6,174,805	12,857	6,187,662
	SPF	278,458	0	278,458
	Greylist Accept	136,505	1,875	138,380
	Greylist Autowhite	925,671	4,481	930,152
	Subtotal	7,515,439	19,213	7,534,652
Spam	Greet-pause	7,331	63	7,394
	Envelope From	9,994,512	190,802	10,185,314
	Envelope To	1,499,262	6	1,499,268
	User unknown	254,788	0	254,788
	Header From	880,135	8,179	888,314
	Greylist deny	342,424	54	342,478
	Blacklist	15,536	41	15,577
	Malware	-	-	2,973
	Subtotal	13,003,988	199,145	13,206,106
Total		20,519,427	218,358	20,740,758

表 2. Greylisting 関連の詳細
Table 2. Detail of mail counts Greylisting

	IPv4	IPv6	total
accept	136,505	1,875	138,380
autowhite	925,671	4,481	930,152
1st	478,929	1,929	480,858
2nd or more	2,104,963	228	2,105,191

表 3. エンベロープ From での検知の詳細
Table 3. Detail of number of mails detected at Envelope From

	IPv4	IPv6	Total
DNS に登録なし	313,064	6,121	319,185
local / localdomain	33,388	428	33,816
学外から oita-u.ac.jp	139,416	0	139,416
Mail addr blacklist	905,804	105,539	1,011,343
Domain blacklist	367,499	18,192	385,691
Spamhaus dbl	8,229,232	60,519	8,289,751
その他	6,109	3	6,112
Total	9,994,512	190,802	10,185,314

万通であり 7%である．

表 3. にエンベロープ From での検知の詳細を，表 4 にヘッダ From での検知の詳細を示す．表 3，4 とも，spamhaus dbl の検知が，80%ほどを占めている．Spamhaus dbl で検知されるメールを送ってきた MTA は，5 か月間で，14966 であった．その MTA のドメイン名について第 2 レベルまでについての集計の一部を表 5 に示す．属性型 jp ドメイン名を持った MTA も 174 位，400 位，545 位，878 位，2472 位に現れている．

5 か月間で検知したメールアドレスは，108 種で，約 102

表 4. ヘッダ From での検知の詳細
Table 4. Detail of number of mails detected at Header From

	IPv4	IPv6	Total
DNS に登録なし	93,292	414	93,706
local / localdomain	2,890	0	2,890
Mail addr blacklist	13,920	2,571	16,491
Domain blacklist	12,972	509	13,481
Spamhaus dbl	733,372	80	733,452
@がない	22,668	4,605	27,273
表示名	1,014	0	1,014
その他	7	0	7
Total	880,135	8,179	888,314

表 5. Spamhaus dbl で検知されたメールの送信元 MTA のドメイン名（部分）
Table 5. Sender MTAs detected by spamhaus dbl (part)

順位	検知数	ドメイン名（第 2 レベルまで）
1	1971558	lstn.net
2	886538	co.in
3	589367	sendinmail.net
4	504962	omicspublishinggroup.com
5	167494	websoftmedia.online
6	156061	ijoear.online
7	147954	24x7mailers.com
8	146499	fifa14.top
9	136599	amazonaws.com
10	131028	ijoer.online
54	25284	myvps.jp
67	17949	outlook.com
174	4211	ac.jp
204	3130	google.com
400	581	ne.jp
545	286	or.jp
878	88	ad.jp
2472	15	co.jp

万回検知した．表 6.に mail address blacklist で検知したメールアドレスの一部を示す．Mail address blacklist には，250 のメールアドレスを登録している．spam の送信元メールアドレスは，一過性のものもあり，その送信元メールアドレスから大量の spam を数時間送り続け，その後，その送信元メールアドレスからは，まったくメールが来なくなることもある．大量に検知される spam の送信元メールアドレスは，通常メールとしても使われるメールアドレスの場合と，そうでない場合がある．メールアドレスで遮断したことを察知したためか，大量のメールを同じ送信元メール

表 6. Mail address blacklist の検知数(部分)
Table 6. Number of spams by mail address blacklist(part)

順位	検知数	送信元メールアドレス
1	210234	noreply@email.apple.com
2	157512	info@mail.rakuten-card.co.jp
3	129684	order@rakuten.co.jp
4	74696	<do_not_reply@jp.oakley.com>
5	39112	<shipment-tracking@amazon.co.jp>
6	34165	myinfo@rakuten.co.jp
7	29603	<point@shop.rakuten.co.jp>
8	28660	<info@lows-jp.com>
9	28648	<info@mailthx.com>
10	28223	<info@thing-jp.com>
11	25015	<info@youtube-info.jp>
12	20575	<store-news@amazon.co.jp>
13	18618	<e-issues@shop.rakuten.co.jp>
14	18384	<yahoo@google-index.jp>
15	15919	<partne@uniqlo.com>
16	12896	<shipment_tracking@amazon.co.jp>
17	11964	support@mail.rakuten-card.co.jp
18	10314	<do_not_reply@line.me>
19	10112	<info@uk-mailer.com>
20	10006	<mail@googlehappy.net>

アドレスで送ると spam 判定されやすくなるためか，spam 送信者が送信元メールアドレスを微妙に変更することもある（表 6．5 位と 16 位など）．

5. おわりに

送信元メールアドレスそのものや，そのドメイン部を検査することによって spam 検知することの効果について大分大のメールサーバのログに基づいて報告した．ドメインブラックリスト，メールアドレスブラックリストへの登録は，手作業であり，登録するかどうかは筆者の経験によるところが大きい．登録基準を明らかにしていくことが今後の課題である．

謝辞 日頃，メールシステムの運用に．ご協力いただいています安徳先生をはじめとする医学情報センターの方々，情報基盤センターのスタッフの方々に感謝いたします．

参考文献

[1] 松井，金高，加来，池部，吉田. “milter の組み合わせによる低配送遅延を目指した spam 対策メールサーバの設計と導入の効果について”，情報処理学会論文誌, Vol.55, No.12, 2014, pp.2498-2510.
[2] 吉田. “Throttling による spam メール抑制の効果について”，情報処理学会研究報告，2005, Vol.2005-DSM-37, pp.69-74.
[3] 松竹，吉田. “メールの安定運用のためのメールゲートウェイにおけるサーバ連携について”，情報処理学会研究報告，2011, Vol.2011-IOT-14, No.9, pp.1-6.
[4] “DNSWL.ORG“. https://www.dnswl.org/, (参照 2018-05-23).
[5] “SORBS.NET”. http://www.sorbs.net, (参照 2018-05-23).
[6] “The Spamhaus Project”. https://www.spamhaus.org/, (参照 2018-05-23).
[7] Schlitt, W. “Sender Policy Framework(SPF) for Authorizing Use of Domains in E-Mail“. RFC4408, 2006.
[8] “Greylisting.org – a great weapon against spammer”. http://www.greylisting.org/, (参照 2018-05-23).
[9] J. Klensin. “Simple Mail Transfer Protocol”, RFC5321, 2008.
[10] B. Leiba. “Update to Internet Message Format to Allow Group Syntax in the "From:" and "Sender:" Header Fields”, RFC6854, 2013