Vol.2020-CSEC-89 No.18
Vol.2020-IOT-49 No.18
2020/5/15

送信者側サーバの設定情報にもとづく迷惑メール対策

石島 悌[1,a),b)]

概要：2020 年になった現在でも，迷惑メールは利用者にとってもシステム管理者にとっても問題となったままである．これらの迷惑メールは，管理の行きとどいていないサーバなどを踏み台にして送られてくることがある．そこで本報告では，踏み台になっていそうなサーバをメールの送受信の中で簡単にわかる設定情報を用いて識別する．そして，そのようなサーバを経由して送られてくるメールを受信しない手法を紹介する．

キーワード：迷惑メール，サーバ設定，踏み台，配送遅延

Anti Spam Method Based on Settings of Sender Servers

Abstract: Even in the year 2020, spam mails are still problems for both users and system administrators. These spam emails may be sent from stepping-stone servers or servers that are not well managed. Therefore, in this report, we identify such servers using the setting information that can be easily found in sending and receiving mail. Then we will describe the method that refuse mails sent via such servers.

Keywords: Spam Mail, Server Settings, Stepping Stone, Delivery Delay

1. はじめに

2020 年となった現在でも，迷惑メールは個別のユーザにとっても，サーバ管理者にとってもやっかいな存在である．ここでの迷惑メールにはフィッシングメールや標的型攻撃メール，ビジネスメール詐欺などを含む [1].

これらのメールは，管理の甘いサーバが乗っ取られて送信されることがある．たとえば日本郵政の事例 [2] や，慶応大学宛の詐欺メール [3] をその例をして挙げることができる．

メールを送受信する際には，双方の送受信 MTA を DNS を用いて確認するなどの手順が存在する．本報告では，それらの情報に不備があった場合に「管理の甘い」あるいは「すでに踏み台として悪用されている」送信 MTA として判断し，それらから送信される迷惑メールをなるべく排除する方法を紹介する．

著者（と共同研究者）は，これまでに greylisting[4], [5] を用いた迷惑メール対策を発表してきた [6], [7]．今回紹介する手法にも greylisting の手法を応用した．残念ながら上述のような MTA から送信されるメールの中には迷惑メール以外のメールも存在する．そこで迷惑メールを完全に排除することはあきらめ，メールを積極的に配送遅延させる方法を選択した．

常時メールが配送遅延するようであれば，受信者はそれに気づくであろうし，送信側 MTA の管理者もログなりメールの配送待ちキューをチェックしていれば配送遅延に気がつくと考えられる．管理者が気づかないようであれば，個々のメールの受信者あるいは送信者からは管理者へクレームが入り，結果として，そのサーバの欠点が修正されることも期待できる．

本報告では，第 2 章において送受信 MTA を DNS などを用いて確認し，どのような問題が存在するかを紹介する．第 3 章では，問題があると考えられる組織や MTA からのメールを積極的に配送遅延させる方法を説明する．第 4 章では，問題があると考えられる組織ならびにそれらが運用する DNS，MTA 以外のサーバへのアクセスにおける注意

[1] 独立行政法人 製品評価技術基盤機構 製品安全センター（大阪）製品安全技術課 製品事故調査員
Investigator, Consumer Product Safety Technology Divition, Product Safety Technology Center,
National Institute of Technology and Evaluation
[a)] ishijima@jikocho.jp
[b)] ishijima-dai@nite.go.jp

© 2020 Information Processing Society of Japan

```
% nslookup -q=soa example1.jp.
Server:         dns102.provider.ne.jp.
Address:        10.61.216.35#53

example1.jp
        origin = ns.example1.jp
        mail addr = postmaster.example1.jp
        serial = 2020022893
        refresh = 10800
        retry = 3600
        expire = 2419200
        minimum = 3600

% host ns.example.jp.
ns.example1.jp has address 10.224.31.98
ns.example1.jp has IPv6 address 2001:db8:268:810::98
```

図 1 SOA レコードの検証

点について述べる．

なお，本報告では説明用のグローバル IPv4 アドレスとして 10.0.0.0/8 を使用し，プライベート IPv4 アドレスとしては 192.168.0.0/16 を用いる．同じく IPv6 アドレスとしては 2001:db8::/32 を用いる．本文中に出てくるドメイン名ならびに IP アドレス，JPNIC ハンドルなどは実在する組織や人物とは全く関係のない架空のものである．

2. 問題のある組織および送信 MTA

本章では，DNS その他の情報を用いて問題のある組織ならびに MTA を検出する手法を紹介する．手法としては非常に簡単なものであり，通常のメールを送受信する際にログなどから簡単に問題のある組織や MTA の情報を採取できる．

MTA や DNS は通常，冗長構成を用いることができる．このようにしておけば，プライマリサーバが利用できなければセカンダリサーバを用いることが可能となる．本章で紹介する問題のあるサーバ類はどちらかが恒常的に機能していないなどの縮退運転状態となっているものである．

2.1 受信 MTA が存在しないか機能していない

受信に使用する MTA は，DNS における MX レコードを用いて優先順位をつけて運用することができる．しかしながら DNS に登録していた情報がメンテナンスされずに，機能していない MTA の情報がそのまま公開されたままとなっていることがある．

まず，このような情報が公開されいる組織の SOA レコード情報などを**図 1** のとおり検査してみる．

SOA レコードはシリアル番号からすると最新情報に更新されているようである．その一方で MX レコードは**図 2** のようになっている．

優先度の高い MTA の IPv4/IPv6 アドレスは**図 3** のとおりである．

```
% nslookup -q=mx example1.jp.
Server:         dns102.provider.ne.jp.
Address:        10.61.216.35#53

Server:         dns102.provider.ne.jp.
Address:        10.61.216.35#53

example1.jp     mail exchanger = 100 ⇒
                                  kerochan.example1.jp.
example1.jp     mail exchanger = 10 ishtar.example1.jp.
```

図 2 example1.jp の MX レコード
長い行は「⇒」で折り返している

```
% host ishtar.example1.jp.
ishtar.example1.jp has address 10.224.31.110
ishtar.example1.jp has IPv6 address ⇒
                                    2001:db8:268:810::110
```

図 3 example1.jp の MTA の IPv4/v6 アドレス

```
% telnet ishtar.example1.jp smtp
Trying 2001:db8:268:810::110...
telnet: connect to address
                 2001:db8:268:810::110 No route to host
Trying 10.224.31.110...
telnet: connect to address ⇒
                         10.224.31.110: No route to host
telnet: Unable to connect to remote host

% ping -c 10 ishtar.example1.jp
PING ishtar.example1.jp (10.224.31.110): 56 data bytes
<中略>
--- ishtar.example1.jp ping statistics ---
10 packets transmitted, 0 packets received, ⇒
                                      100.0% packet loss
```

図 4 example1.jp の MTA に対する接続の試行

しかし，この MTA に SMTP パケットを送信しても，PING による疎通確認をしても**図 4** のとおり応答がない．この MTA は IPv4/v6 デュアルスタックで運用されているため，無駄な SMTP 接続が二度必要となっている．セカンダリ MX がすんなりと受信していればメールはすぐに受理されるが，greylisting が用いられていれば，メールが先方に送信されるまでに IPv6/IPv4 を合わせて計 6 回の SMTP の試行が無駄になる．

MTA が機能していない，あるいは存在していないということは，その組織においては適切にメールを受信する意志がないということを公表しているものと著者は考える．そこで，このような組織からのメールは積極的に遅配させることにする．

© 2020 Information Processing Society of Japan

```
% nslookup -q=soa example2.jp. w03.example2.jp.
Server:         w03.example2.jp.
Address:        10.203.181.152#53

example2.jp
        origin = dns.example2.jp
        mail addr = root.example2.jp
        serial = 2013042893
        refresh = 3600
        retry = 900
        expire = 604800
        minimum = 3600
```

図 5 問題のある SOA レコード

```
% nslookup -q=soa example2.jp. dns.example2.jp.
;; connection timed out; no servers could be reached

% ping -c 3 dns.example2.jp.
PING dns.example2.jp (10.203.181.101): 56 data bytes

--- dns.example2.jp ping statistics ---
3 packets transmitted, 0 packets received, ⇒
                                    100.0% packet loss
```

図 6 MNAME で示されるネームサーバが存在しない

```
% nslookup -q=ns example2.jp. w03.example2.jp.
Server:         w03.example2.jp.
Address:        10.203.181.152#53

example2.jp     nameserver = sigw.sinet.ad.jp.
example2.jp     nameserver = w03.example2.jp.
```

図 7 example2.or.jp の NS レコード

2.2 DNS の設定における問題を放置している組織

次に DNS 設定における問題について検証する．**図 5** に，そのような組織の SOA レコードを示す．

「origin =」の右辺で示されるサーバは RFC1035[8] における「MNAME」であり，このドメインの一次情報を保持するものである．しかしながら，**図 6** 以下に示すようにネームサーバとしては動作していない模様である．

図 7 では，ネームサーバは二つ存在するように見えるが，残念ながら「sigw.sinet.ad.jp」はすでに引退しており，事実上，この組織の DNS は十分に機能しているとはいえない．法定点検による停電などが原因でキャッシュから情報が消えた場合は，ドメインそのものが存在しないように見え，そのようなときは，もちろんメールの送受信が不可能となる．

余談ではあるが，whois 情報においては，**図 8** のとおりネームサーバは一つである．また，担当者もすでに退職しているものと思われ，トラブル発生時に（ウェブサイトも閲覧不能であれば）連絡をとることも困難であろう．

```
% whois -h whois.jprs.jp example2.jp
中略
m. [登録担当者]                 RT0040JP
n. [技術連絡担当者]             RT0040JP
p. [ネームサーバ]               w03.example2.jp
s. [署名鍵]
[状態]                          Connected (2020/11/30)
[登録年月日]                    2009/11/18
[接続年月日]                    2009/11/18
[最終更新]                      2019/12/01 01:11:07 (JST)
```

図 8 example2.or.jp の whois 情報

```
% whois -h whois.nic.ad.jp 10.224.31.96
a. [IP ネットワークアドレス]    10.224.31.96/28
m. [管理者連絡窓口]             RT030JP
n. [技術連絡担当者]             RT030JP
[割当年月日]                    1998/08/24
[最終更新]                      2017/06/29 17:02:05(JST)
```

図 9 example1.jp の whois 情報

```
% whois -h whois.nic.ad.jp JP00000000
[部署]                          伏字
[電話番号]                      0ABC-DE-2617
[最終更新]                      2017/01/17 12:11:06(JST)
```

図 10 example1.jp が利用している IP アドレスの連絡先情報

2.3 WHOIS 情報が古い

前節で whois 情報に触れたが，前々節の組織も whois 情報が古い．この組織の IP アドレスで whois 情報を検索してみると**図 9** のとおり，窓口ならびに担当者は退職者のままである．

同組織が前節の組織との VPN 接続に用いている IP アドレスについても，**図 10** 電話番号などが退職者のもとなっている．

2.4 一貫性のない DNS 情報

ある組織が新しいドメインを取得して，新たにウェブサイトを開設することがある．ここで大切なことは，その新しいドメインに関して一貫した情報を管理することである．

新しいドメイン example3.jp を example1.jp が取得した場合を考える．すでにネームサーバは example1.jp で稼働しているので，そこで example3.jp のゾーン情報を管理するのは簡単である（**図 11**）．

一方，ネームサーバとして「example3.jp」を指定して名前解決すると，**図 12** のとおり全く違った結果が得られる．example4.com ならびに example4.jp は example3.jp のサービスを提供しているレンタルサーバ事業者である．dns3.example4.com は同事業者のネームサーバであるので，同事業者内で名前解決するとメール配送に支障が生じる恐れがある．

© 2020 Information Processing Society of Japan

```
% nslookup -q=soa example3.jp. dns102.provider.ne.jp.
Server:         dns102.provider.ne.jp.
Address:        10.61.216.35#53

example3.jp
        origin = ns.example1.jp
        mail addr = postmaster.example1.jp
        serial = 2020022893
        refresh = 10800
        retry = 3600
        expire = 1209600
        minimum = 3600

% host example3.jp.
example3.jp has address 10.158.129.144
example3.jp has IPv6 address ⇒
               2001:db8:250:21a0:1000:222:4dff:fe69:390
example3.jp mail is handled by 10 ns.example3.jp.
```

図 11 example3.jp の SOA 情報と IPv4/v6 アドレス

図 11 と図 12 の情報が一致しない原因は，後者はレンタルサーバ事業者が提供しているウェブベースのサーバ管理システムを用いていることに起因しているようである．可能であれば，図 11 か図 12 のいずれかを一次情報として，それを片方に反映させるべきである．

やはり，このようにメール受信に関して一貫性のない情報が得られるサーバや組織，レンタルサーバ事業者などからのメールは可能であれば排除するのが無難である．

また，新しいウェブサイトを開設するにあたって，レンタルサーバ事業者の選定が終わる前に仮のウェブサイトを運用する場面もあるだろう．このような場合は，既存の「example1.jp」の IPv4/IPv6 アドレスを用いて，ウェブサーバのバーチャルホストなどの機能を用いて，新しいウェブページの設計などをすることができる．

しかし，ウェブページの設計や開発に携わる担当者が IPv6 環境を利用できない，あるいは IPv6 に詳しくない場合には，IPv4 環境と IPv6 環境で違ったコンテンツが表示される恐れがある．

また，「example3.jp」に IPv6 アドレスを割り当てておいたものの，レンタルサーバ事業者のサーバ室に IPv6 reachability が確保されていないと IPv6 → IPv4 フォールバックのために，閲覧者が余計な時間を費してしまう．また，IPv4 でしか動作確認をせずに運用してしまうなどのオペレーティングミスなども，これまでに述べた組織や管理者においては十分に予想される．

IPv4 アドレスの枯渇により，特にスマートフォンでは利用者も気づかないうちに IPv6 が優先的に利用される場合がある．キャリアが提供する無線 LAN でも IPv6 が優先的に用いられることがある．IPv4/IPv6 デュアルスタックでの運用においては，入念なテストが欠かせない．

蛇足ではあるが，組織内のみにアクセスを限定したウェブサーバが外部から判別できることもよいとはいえない．そのようなリンクを公開ウェブサーバに掲載する場合は，適切なスクリプトを用いて，リンクを外部に公開しない方策をとるべきである．さらには名前解決を行った場合に**図 13** のようにプライベート IP アドレスが判別できる状態も望ましいものとはいえない．

```
% nslookup -q=soa example3.jp. example3.jp.
Server:         example3.jp.
Address:        10.158.129.144#53

example3.jp
        origin = dns3.example4.com
        mail addr = info.example4.co.jp
        serial = 1523237442
        refresh = 12000
        retry = 1800
        expire = 604800
        minimum = 86400

% nslookup -q=mx example3.jp. example3.jp.
Server:         example3.jp.
Address:        10.158.129.144#53

example3.jp     mail exchanger = 10 mail.example3.jp.

% nslookup -q=aaaa mail.example3.jp. example3.jp.
Server:         example3.jp.
Address:        10.158.129.144#53

*** Can't find mail.example3.jp.: No answer
```

図 12 一貫性のない example3.jp の情報

```
% host tokkyo.example3.jp.
tokkyo.example3 has address 192.168.110.109
```

図 13 プライベート IP アドレスが公開されている事例

2.5 問題のある組織や MTA の検出

これまでに列挙した問題のある組織や MTA については，メールサーバのログや DNS のログをチェックすることにより，簡単に発見することが可能である．特にこちらから送信しようとしたメールが拒絶されたかどうかは，ログを「deferred」などのキーワードで検索すればよい．

ただし，問題が恒常的に発生しているのか，あるいは一時的なものかを区別する必要がある．提案方式では問題が恒常的に発生している場合のみ，その組織あるいは MTA を問題ありとしている．

3. メール配送の遅延手順

前章で問題のある組織ならびに MTA について列挙した．本章では，それらの組織やそこで運用されている MTA から送信されるメールを遅配させる方法を説明する．

© 2020 Information Processing Society of Japan

```
中略
MAIL From: postmaster@example.jp
250 2.1.0 Ok
RCPT To: ishijima@jikocho.jp
450 4.7.1 <example1.jp>: Helo command rejected: ⇒
                We don't talk to broken sites/servers.
```

図 14 メールの着信拒否と応答コード

著者と共同研究者は，greylisting を用いた迷惑メールについて発表し，また，その副作用である配送遅延を改善する方式を提案した．今回はそれとは逆のアプローチで積極的に配送を遅延することを試みている．

まず，優先順位の高い MTA においては，問題のある組織や MTA からのメールを**図 14** のように「450」で応答して受信を拒否する．

次に優先順位の低い MTA においては greylisting を用いて配送を遅延させる．仮に送信側 MTA がスループットを重視しており，再送を試みない spam 送信者であれば，最初に「450」の応答を受け取ったか，greylisting により再送を促された場合に，そのままメールの配送をあきらめることが期待できる．

送信側 MTA が再送を試みた場合，優先順位の高い MTA では再度受信を拒否する．次に優先順位の高い MTA に再送を試みた場合はやむなくメールを受信するが，この時点で greylisting の当該 MTA に関するエントリを削除する．これにより，次回の送信は greylisting により配送が遅延することとなる．

サーバ管理者がログを確認する習慣を持ち合わせていれば，何かがおかしいことには簡単に気づく．送信キューも同様で滞留したままのメールが常時存在し，これについても確認の習慣づけができていれば容易に検知することができる．

ログやキューの確認は難しいことではなく，平易なシェルスクリプトなどで記述することができる．また，さまざまな可視化ツールによりわかりやすく表示することも簡単である．

しかし残念なことに，2 章で示したような初歩的なミスを犯すような組織やサーバ管理者であればあるほど，ログの確認や可視化を疎かにしがちである．

4. メール以外の留意点

本報告では，メールに着目して管理の行き届いていない組織やサーバを見つける方法と積極的にメールの配送を遅延させる方法を説明した．しかし，管理の行き届いていないサーバやそれを保有している組織は潜在的にセキュリティに関するリスクを抱えているといえる．このような組織が管理するメール以外のサーバにも，セキュリティに関するリスクが存在する可能性は高い．

その中で最も問題となるのはウェブサーバであろう．ウェブサーバに脆弱性が残存しており，それを悪用されると，悪意のあるコンテンツが管理者の知らない間に配置され，いわゆる「水飲み場攻撃」に利用される恐れがある．2 章で示したように，簡単に問題点が見つかるような組織のウェブサイトに安易にアクセスすることは避けるべきである．

ウェブサイトの安全性については，https を用いていれば安全であり，そうではなく，プレインな http であれば「安全な接続ではありません」と表示することがブラウザにおいては一般的となっている．しかし，今回示したような管理の行き届いていない組織やそれらが運用しているサーバは，通信プロトコル以前の段階で潜在的な危険性をはらんでいる．

今後はこのような管理の行き届いていない組織やそれらが運用しているサーバについて「危険ですが本当に閲覧しますか」と表示するブラウザ向けプラグインの作成を検討している．

5. おわりに

本報告では，メールの送受信の過程で簡単に取得できる情報に基づき，送信 MTA やそれを管理している組織がサーバを適切に運用できているかどうかを判断する方法を説明した．そして，それにより，不適切なサーバやそれを有する組織からのメールを積極的に配送遅延させる方法を提案した．

SNS に代表される，さまざまなコミュニケーションツールが登場した現在においても，メールは欠かせない存在である．そのメールの利用を不便にする迷惑メール送信者を簡便に判別し，そのような組織やサーバの利用者の気づきをうながすことが本報告の目的一つである．

IPv4/IPv6 デュアルスタック運用について，本報告で留意点を記述したが，現段階ではすべての組織が無理に IPv6 に対応する必要はないと著者は考える．官公庁などでは対応を求められることがあるかもしれない．しかし，そうでないのなら背伸びはせずに「AAAA レコード」を消せばよい．

逆に地方公共団体やそれらが所管する独立行政法人であれば，サーバなどを運用する前に地方自治情報センター（LASDEC）[9] のシステムセキュリティチェックを実施し，得られた結果のとおり改善すればよい．そうすれば本報告で述べたような初歩的な問題のあるサーバ運用を簡単に避けることができる．

インターネットは参加するそれぞれの組織が分散協調することによって成り立っている．そのような背景に気づけず，ローカルルールを優先したり管理者の思い込みによって，知らず知らずに他の組織や一般利用者に不便を強いている組織が少数ではあるが存在している．このことは残念

© 2020 Information Processing Society of Japan

としか表現のしようがない．

ある組織（あるいは個人）がドメインを取得し，メールやウェブサーバを運用するということは，それなりの責任を負うということである．先に述べたような組織には，このことを理解している人が在籍していないのであろう．

本報告が，迷惑メールの送信に利用される踏み台となっているサーバや，それらを有する組織の管理者の気づきになることを期待している．また，そのような組織に悩まされている人々の一助になれば幸いである．

参考文献

[1] 独立行政法人 情報処理推進機構：情報セキュリティ 10 大脅威 2020（online），入手先〈https://www.ipa.go.jp/security/vuln/10threats2020.html〉(参照 2020-04-01).
[2] 株式会社イード ScanNetSecurity：保有ドメインへ不正アクセス、迷惑メール送信の踏み台に（日本郵便）（online)，入手先〈https://scan.netsecurity.ne.jp/article/2020/02/18/43703.html〉(参照 2020-03-31).
[3] 産経新聞社：文科省装い慶大にウイルス送信 過去の実在メール悪用か（online），入手先 〈https://www.sankei.com/affairs/news/160526/afr1605260025-n1.html〉(参照 2018-03-15).
[4] Harris, E.: The Next Step in the Spam Control War: Greylisting (online). available from 〈http://projects.puremagic.com/greylisting/whitepaper.html〉(accessed 2020-03-21).
[5] 吉田和幸：greylisting による spam メールの抑制について，情報処理学会分散システム/インターネット運用技術研究会研究報告，No. 2004-DSM-35, pp. 19–24 (2004).
[6] 石島 悌，平松 初珠，林 治尚：適用時間限定型 greylisting を用いた迷惑メール対策における配送遅延の改善，情報処理学会論文誌 Vol. 51, No. 3, pp. 989—997 (2010).
[7] 石島 悌, 平松 初珠, 中井 亮：適用時間を限定した greylisting の透過型プロキシを用いた実装と評価，インターネットと運用技術シンポジウム 2009（IOTS2009）論文集, pp. 61—68, (2009/12).
[8] DOMAIN NAMES – IMPLEMENTATION AND SPECIFICATION, available from〈https://www.ietf.org/rfc/rfc1035.txt〉(accessed 2020-03-21).
[9] 地方公共団体情報システム機構，(online)，入手先〈https://www.j-lis.go.jp/〉(参照 2020-04-05).

© 2020 Information Processing Society of Japan