プロトコル検証に基づく
不正通信ホスト識別手法の研究

北川 直哉

概要

世界中でインターネットが普及し，我々の社会生活において欠かすことのできない存在となっている．一方で，spam メール送信や DoS 攻撃，機密情報の漏洩等のインシデントが日常的に発生しており，セキュリティ対策の重要性が叫ばれている．

インターネットサービスの中で，電子メールは長年にわたり世界中の人々の間で最も広く利用されているサービスの一つである．しかし，大量の spam メールに起因する膨大な量のトラフィックは電子メールサービスのみならず，インターネット全体に対する重大な脅威である．

長年にわたって spam メールによる被害を軽減するための研究が広く行われており，様々な技術が提案されている．メール送信側と受信側の双方で様々な対策手法が存在するが，受信サーバにおける spam メール対策手法は，メール本体を受信した後，メールのコンテンツを解析して判定する手法と，メール本体を受信する前の段階で，送信ホストの通信挙動によって判定する手法の 2 つに大別できる．前者のコンテンツフィルタリングは判定精度が高いものの，メールデータを全て受信した後で判定処理を実施するため，spam メール送信に起因するトラフィック量の軽減には一切貢献しない．本論文では，spam メールに起因するトラフィック量を減少させる手法の提案を目的とし，メール本体を受信する前の段階で，ホストの通信挙動の特異性を様々な観点から見出すことにより，spam メール送信ホストを識別する手法に注目する．

メール受信前の通信挙動の特徴によって spam メール送信ホストを識別する代表的な従来手法に，Tempfailing や 5-Way Handshake と呼ばれる手法が存在する．Tempfailing は SMTP セッション中に一時拒否エラーを示す 400 番台の応答を行い，SMTP 接続に失敗した送信ホストが一定時間経過後に再送を行った場合には正当な送信ホストであると判断して受信する手法である．しかし，spam 送信ホストはメール配送の信頼性よりも配送効率を優先するため，一時的エラーを受信しても再送処理を行わないことが多い．Tempfailing はこのような spam メール送信ホスト特有の動作に注目した手法であり，spam メール送信ホストによる接続を排除する効果は高いものの，受信までに長時間の遅延が発生する欠点がある．RFC5321 によれば，送信ホストは一時的エラーを

受信後，少なくとも 30 分以上経過後に再送を行うよう推奨されているため，30 分以上の配送遅延が予想される．

Tempfailing の遅延問題を解決するために，5-Way Handshake と呼ばれる TCP 接続時の通信挙動に注目した手法が提案されている．RFC5321 により，送信ホストは配送先ドメインの MX レコードを問い合わせた後，その優先度順に接続を試みることが定められている．5-Way Handshake は，MX レコードにプリファレンス値の異なる 2 つの受信ホストを用意し，送信ホストから最も優先度の高いプライマリ MX に対して送られる SYN パケットに対し，プライマリ MX は SYN+ACK パケットの代わりに RST パケットで応答する．これにより，MX フォールバックを促し，セカンダリ MX への再送を受信する手法である．

5-Way Handshake の代表的な実装法として，Nolisting と Unlisting がある．Nolisting は，固定的にプライマリ MX への TCP 接続を拒否し，セカンダリ MX では常に接続を許可するものである．しかし，多くの spam メール送信ホストは MX レコードの優先度を無視するため，1 度目の配送でプライマリ MX とセカンダリ MX を区別すること無く配送を試みる．その結果，多くの False Negative が発生することになる．

Unlisting は Nolisting を強化した手法であり，MX フォールバック後の配送のみをセカンダリ MX で受信するものである．送信ホストはプライマリ MX からの RST パケットを受信すると，即座にセカンダリ MX への再送を試みる．従って，送信ホストからの 1 回目の SYN パケットに対し，プライマリ MX が即座に RST パケットを返してしまうと，プライマリ MX から通知される送信ホストに関する情報の処理がセカンダリ MX で完了する前に再送が始まってしまい，セカンダリ MX では受信の可否を判断することができなくなる．さらに，高負荷時にパケットフィルタリングの処理が遅延した場合の対応が困難になるなど，実用性に問題がある．

本論文では，5-Way Handshake が spam メール送信ホストを識別するために有効な手段であることを確認するため，MX フォールバックまでの挙動や時間について調査し，正当な送信ホストの通信挙動の特徴から “正当な送信ホストと見なす条件” を独自に定めた．この条件と spam メール送信ホストによの通信挙動を比較したところ，大多数の spam メール送信ホストによる配送ではこの条件を満たさず，両者が判別可能であることを確認した．

この知見に基づき，主要なOSが複数回にわたってSYNパケットの再送を行う機構を有することに注目したMXフォールバック検出手法について述べる．この手法は，プライマリMXおよびセカンダリMXのどちらにおいても全ての送信ホストからの接続を拒否する状態で待機させる．プライマリMXに1度目のSYNパケットが到着するとこれを棄却し，同時に当該送信ホストを一時ホワイトリストに登録する．この登録は，プライマリMXへのSYNパケットの再送が繰り返される間に完了すれば良く，また，調査した全てのOSの中で最短のものでも再送は9秒間繰り返されることが観測された．このため，高負荷等の理由で一時ホワイトリストの処理が遅延した場合でも，9秒以内であればMXフォールバック検査を確実に実施できる．

送信ホストが一時ホワイトリストに登録されると，プライマリMXは当該送信ホストからのSYNパケットに対しRSTパケットで応答し，セカンダリMXは接続を許可するよう一時的に対応が変化する．その結果，当該送信ホストにおいてMXフォールバックが誘導され，セカンダリMXにSYNパケットが再送される．その後，セカンダリMXと送信ホストの間でTCPコネクションが確立し，SMTPセッションが開始される．この手法は，調査を行った全てのOSが最初のSYNパケットの送信から3秒以内に2度目のSYNパケットの送信を行うことから，Tempfailingで発生する配送の遅延の問題を解決した．この手法により，Nolistingの判別精度の低さやUnlistingの非柔軟性等，従来の手法の様々な弱点を克服できる．さらに，システム実装の要となる一時ホワイトリストの保持時間の変化によるspamメール送信ホスト判別精度の評価を行い，5秒から20秒程度の設定が判別精度と負荷耐性の確保のいずれの観点からも適切であるという知見を得た．

さらに，今後精巧なspamメール送信プログラムが増加することが懸念されるため，前述のMXフォールバック検査に加え，メール送信時の挙動を様々な視点から監視することにより，spamメール検出精度を向上させることが望まれている．前述の一時ホワイトリストを用いたMXフォールバック検査のspamメール送信ホスト識別精度をさらに向上させるため，応答するMXレコードのリストを定期的に変更する特殊なDNSコンテンツサーバを用いた検査を提案する．この検査は，MXフォールバック検査の前段として，送信ホストによって参照されるDNSキャッシュサーバがMXレコードのTTLを遵守し，かつ，送信ホストが正しいMXサーバを選択する機構を有するかを検

査する．

このシステムを実際に spam メール収集ドメインに導入し，spam メール送信ホスト識別精度の評価を行ったところ，spam メール送信に起因する SMTP セッション数が導入前後で約 96.7%削減された．本手法は，高速かつ低負荷に spam メール送信ホストの識別が行え，また他手法と容易に組み合わせて運用することができる柔軟性や拡張性が高い MX フォールバック検出手法の長所を維持しつつ，機能拡張により判定性能をさらに高められることを確認した．

目 次

図一覧

表一覧

第1章

序論

世界中でインターネットが普及し，我々の社会生活において欠くことのできない存在となっているが，spam メール送信や DoS（Denial of Service）攻撃への加担，機密情報の漏洩等のインシデントを発生させるホストが無数に存在し，インターネットの信頼性が脅かされている．このような不正通信ホストを検出し，被害を抑える必要がある．

インターネットサービスの中で，電子メールは長年にわたって世界中の人々の間で最も広く利用されているサービスの一つであり，昨今でも我々の社会生活において欠くことのできない重要な情報伝達ツールの一つである．しかしながら，大量の spam メールに起因する大量のトラフィックはメールサーバのみならず，インターネット全体に深刻な影響を与えている．

spam メールは，国内では “迷惑メール” とも呼ばれ，不特定多数の相手に対し，受信者の承諾なしに送信される広告メールや，ウィルス配布やフィッシング等の詐欺を目的として送信されるメールのことを指す．海外ではこのような望まない宣伝メールのことを “UCE(Unsolicited Commercial E-mail)” とも呼ばれ，商用目的以外の内容も含めて，大量に送りつけられるメールのことを “UBE(Unsolicited Bulc E-mail)” と呼ばれる．

このように，メールの内容に基づいて spam メールと認識されることが多いが，その基準が曖昧である．本論文では，電子メールの送信動作に関連する通信プロトコルである，DNS による宛先ドメイン名の名前解決，TCP コネクション，SMTP セッションの各段階において，通信規約で定められた正当な挙動を示さないホストから送信さ

れるメールについて，spam メールとして定義する．

多くの MTA は，送信ホストが軽微なプロトコル違反をしていても受信する場合が多い．プロトコル違反によって，ボット感染などによって送り込む送信プログラムを小さくすることができ，より効率的な spam メール送信が可能となる．従って，プロトコル検証は spam メールを判別する手法として精度が高いと言える．

“spam メール” という名称は，Hormel Foods 社が発売しているランチョンミート製品の “SPAM” に由来する．イギリスのテレビ局 BBC 放映のコメディ番組である “Monty Python’s Flying Circus” の “SPAM SKETCH” というスケッチ・コメディで，ある夫婦が食堂で食事を注文しようとするものの，SPAM 入りのメニューしか存在せず，隣のテーブルのヴァイキング達が「SPAM，SPAM」と連呼し，邪魔をするという場面がある．このことから，“何度も執拗に繰り返され，それによって肝心の会話が妨げられるような迷惑行為” を “spam” と呼ばれるようになったと言われている [1]．また，大文字表記の “SPAM” は Homel Foods 社の登録商標であるため，迷惑メールについては小文字で “spam” と表記して区別することを同社は要求している [2]．

spam メールによる被害は，電子メール利用者が削除が煩わしいと感じる点，あるいは誤って非 spam メールを削除するリスクがある点や，内容を閲覧して不快感を覚える点等があるが，このような被害は氷山の一角にすぎない．メール内容を読んだ電子メールユーザが思わずクリックしてしまうよう巧妙に作成された spam メールが多く送信されており，フィッシングやワンクリック詐欺等の犯罪行為の契機として，メール利用者に被害を及ぼす危険性がある [3]．また，spam メールによって労働者の生産性が低下し，巨額の経済損失の原因となっている [4][5]．

spam メールの最大の脅威は，膨大な量の不必要なメールの受信によりサーバリソースやネットワークリソースを浪費してしまう点である．シマンテック社のレポート [6] によれば，2013 年 10 月現在の世界全体のメールトラフィックに占める spam メールの割合は約 67.7%であり，2011 年後半から徐々に減少する傾向があるものの，世界中で通信される過半数を超えるメールが spam である状況は変わっていない．2008 年後半にも spam メールの割合が減少したが，2009 年，2010 年には再び spam メールの割合が急増したこともあり，今後さらに増加する恐れがある．

また，多くの spam メールが差出人メールアドレスを詐称して送信される．spam メー

ルの発信者アドレスを自ドメインに詐称された場合，大量の宛先不明を通知するエラーメール（バウンスメール）が発生し，DoS 攻撃となり，MTA が過負荷になる [7]．この攻撃は一般に，“バックスキャッタ” と呼ばれるほか，1990 年代に “Joe’s Cyberpost” というウェブサイトの運営者である Joe Doll 氏が最初に被害に遭ったことから，“Joe job” とも呼ばれる．

このように，長年にわたって spam メールの被害が後を絶たないが，法律による対策に加え，送信側，受信側の双方で様々な対策がとられている．我が国では，法的な spam メール対策として，“特定商取引に関する法律” [8] や，“特定電子メールの送信の適正化等に関する法律” [9] が定められている．しかし，殆どの広告 spam メールはこの法律の表示義務に違反しているにも関わらず，違反者の特定が困難であるため，効果は限定的である．

また，送信側の対策として，spam メールの多くがボット感染したエンドユーザの PC であることに注目し，OP25B（Outbound Port 25 Blocking）が多くの ISP で実施されている．OP25B は，自ネットワークから外部への SMTP（25/tcp）アクセスをブロックするものである．

さらに，受信側でも spam メール対策に関する様々な研究が広く行われている．spam メール対策において，理想的な手法は，管理ポリシによって観点が異なるが，以下の項目が挙げられる．

- False Negative（見逃し）が少ないこと
- False Positive（誤検出）が少ないこと
- 配送遅延が少ないこと
- スループットが高いこと
- 導入が容易であり，また管理コストが低いこと
- 負荷耐性があり，DoS 攻撃に強いこと

spam メール対策の手法は，大きく分けて次の 3 種類に分類することができる．

1. メール通信時（受信時）の対策

2. メール受信後の対策

3. 送信ドメイン認証

これらの手法についての詳細は 2.2 節で議論する．本論文では，spam メールに起因する不要なトラフィックを削減することが出来る 1. のメール通信時の対策に注目した手法について述べる．大部分の spam メールの送信元はボット感染した PC であり，正確なメール配送よりも配送効率を優先するため，正当な送信ホストとは異なる通信挙動を示す．これに基づき本論文では，spam メールそのものを識別するのではなく，通信挙動から spam メールの配送を実施するホストを識別する手法に注目する．

1. のメール通信時の spam 対策のうち，代表的な手法である Tempfailing は，送信ホストの SMTP セッション時における再送ポリシの特徴を利用した spam 対策手法であり，その効果は高いものの，メール配送に長時間の遅延が発生する欠点がある．この欠点を解決するため，Nolisting[21] や Unlisting[22] 等，5-Way Handshake と呼ばれる手法が提案されている．しかし，これらの手法も重大な問題を抱えており，例えば Nolisting では False Negative（見逃し）が非常に多く発生し，Unlisting は容易に実装可能だが，仕組みが単純すぎるため柔軟性に乏しく，実用性に問題を抱えている．本研究では，このように諸問題を抱えるメール通信時の spam 対策手法の開発に取り組んだ．

2. のメール受信後の spam 対策は，受信サーバでは送信ホストからのメール本体を受信した後で spam メール判定処理を実施するため，大きなサイズのデータをやり取りする必要がある．このため，トラフィック量の軽減には一切貢献しない点に加え，受信した全てのメールに対してコンテンツ検査を実施するため，多くのサーバリソースが消費され，短期間に大量の spam メールが寄せられた場合に正常な処理が実施できず，受信障害が発生しやすい点が深刻な問題点として挙げられる．メール受信後の spam 対策手法は，1. の通信時の対策を行った後で，検査対象となるメールを十分に削減させてから行うべきであると考える．

本論文では，2 章で既存の spam メール対策手法について述べる．3 章では，正当な送信ホストが使用するメール転送エージェント（MTA）の通信挙動の特徴から，“正当な送信ホストの条件” を独自に定めた．この条件と spammer が使用する送信プログラムの通信挙動を比較したところ，大多数の spam 送信ホストによる配送ではこの

条件を満たさず，両者が判別可能であることを確認した．また，この特徴を利用したspam 対策システムの実装方法を検討した．この知見に基づき，4 章では，従来の 5-Way Handshake の実装が抱える諸問題を解決する，送信ホストの再送動作をリアルタイムで検出し，spam 送信ホストを効率的に識別する手法の実装について述べる．さらに，実際に spam 対策システムとして動作させる上で考慮すべきシステムの拡張性の確保や，負荷耐性の評価等について述べる．

5 章では，4 章で述べたリアルタイム再送検出手法をさらに強化するため，DNS プロトコル違反を検出することにより判定性能を向上させるた手法について述べる．この手法は，送信ホストによって参照される DNS キャッシュサーバが MX レコードの TTL を遵守し，かつ，送信ホストが正しく MX サーバを選択するかを確認する検査を組み合わせるものである．また，このシステムを実際に spam メール収集ドメインに導入し，spam 送信ホストの判別精度と安定運用について評価を行った．

本手法の導入により，大量の spam メールによるトラフィックを大幅に軽減することができ，また 2 章で述べる従来の spam 対策システムが抱えていた諸問題を解決することができた．また，複数の手法を組み合わせて運用することが一般的である spam メール対策に対し，本手法は従来の手法の前段に設置することで容易に組み合わせて運用することができる高い柔軟性を示した．

第2章

プロトコル検証に基づく不正通信ホストの識別

2.1 電子メール通信におけるプロトコル検証

本章では，ホストの挙動がプロトコルに準拠しているかを検査することにより，不正な通信を行うホストを識別する手法について述べる．はじめに，電子メールの送受信の手順を図 2.1 に示す．なお，図中における括弧付き番号は次のような動作を示す．

- **DNS による名前解決**

(1) 電子メール利用者がメールを送信すると，送信ホストは宛先に指定されているドメインの MX レコードを，送信ホストが使用する DNS キャッシュサーバに問い合わせを行う．

(2) DNS キャッシュサーバが当該ドメインの MX レコードの情報を保持していない場合，ルートネームサーバから再帰検索を行い，最終的に宛先ドメインの権威ネームサーバ（図 2.1:DNS Contents Server）に問い合わせを行う．ただし，当該ドメインの MX レコードの情報を保持していた場合には，名前解決処理の必要が生じないためこの動作は発生せず，(1) で問い合わせを行った送信ホストにその情報を応答し，(4) に進む．

(3) 問い合わせを受けた DNS コンテンツサーバは，問い合わせ元である DNS キャッシュサーバに MX レコード情報を応答する．以上のやり取りにより，宛先ドメイン名の名前解決が完了する．

- **TCP コネクション（Three Way Handhshake）**

(4) 送信ホストは (3) で得た情報に基づき，宛先である受信ホストとの間で TCP コネクションを確立するために，SYN パケットを送信する．

(5) 送信ホストからの SYN パケットを受信した受信ホストは，SYN+ACK パケットで応答する．

(6) 受信ホストからの SYN+ACK パケットを受信した SMTP サーバは，ACK パケットで応答する．これにより，以上のやり取りにより，送信ホストと受信ホストとの間で TCP コネクションが確立する．

- **SMTP セッション**

(7) TCP コネクションが確立すると，SMTP セッションが開始される．はじめに，受信ホストはサービスの準備が完了したことを示すリプライコード “220” を送信ホストに送信する．

(8) 送信ホストは，メール転送を開始することを受信ホストに知らせる “HELO” コマンドあるいは拡張である “EHLO” コマンドを，自身のホスト名を引数に指定して送信する．

(9) “HELO/EHLO” コマンドを受信した受信ホストは，メール転送が可能である場合には，コマンドが正常に完了したことを示すリプライコード “250” を送信ホストに応答する．これにより，両ホストの間でメール転送を開始することが出来るようになる．

(10) 送信ホストは，“MAIL” コマンドを使用し，自身のメールアドレスを引数に指定して受信ホストに送信する．

(11) 受信ホストは送信ホストのメールアドレスを正常に受け取ると，コマンドが正常に完了したことを示すリプライコード “250” を送信ホストに応答する．

(12) 送信ホストは，“RCPT” コマンドを使用し，宛先メールアドレスを引数に指定して受信ホストに送信する．

(13) 受信ホストは宛先メールアドレスを正常に受け取ると，コマンドが正常に完了したことを示すリプライコード “250” を送信ホストに応答する．

(14) 送信ホストは “DATA” コマンドを送信し，メールデータの送信を開始する．

(15) 受信ホストはメールデータの受信準備が出来ていた場合，それを示すリプライコード “354” を送信ホストに応答する．

(16) 送信ホストはメールデータ（From:，To:，Subject:，本文）と，最後にデータの終わりを示す “<CRLF>.<CRLF>” を受信ホストに送信する．

(17) 受信ホストはメールデータを正常に受信すると，コマンドが正常に完了したことを示すリプライコード “250” を送信ホストに応答する．

(18) 送信ホストは一連のメール送信が終了したことを示す “QUIT” コマンドを受信ホストに送信する．

(19) 受信ホストは “QUIT” コマンドを正常に受信すると，コマンドが正常に完了したことを示すリプライコード “250” を送信ホストに応答する．これにより，メール転送は終了となる．

受信サーバにおける spam メール対策手法では，以上のメール配送手順のうち，図 2.1 の (A) から (G) で示した各段階で判定する．これらの手法については，次節で詳細に述べる．

2.2 様々な spam 対策手法

序論で述べたように，spam 対策システムには大きく分類して次の 3 種類が存在し，spam 判定を行うタイミングがそれぞれ異なる．

1. メール通信時（受信時）の対策
2. メール受信後の対策
3. 送信ドメイン認証

1. のメール通信時の対策は，図 2.1 の (A) から (F) の段階で，2. のメール受信後の対策は (G)，3. の送信ドメイン認証は (D) および (F) の段階で spam 判定を実施する．これらの詳細について，以降で段階別に示す．

2.2.1 メール通信時の対策

- (A) DNS 応答による優先受信制御
  この手法は，受信ホストが高負荷状態にある際に正当なメールの配送をスムーズに行うためのものであり，DNS 問い合わせに対する応答で，1 度目の送信ホストに対しては性能の低い MX サーバを，過去の履歴から正当であると判断した送信ホストには性能の高い MX サーバを応答する [26][27]．この手法は効果的に動作するが，DNS サーバへの付加的なオーバーヘッドを要し，また SMTP セッションの経過を追う必要がある．さらに昨今では，Google 等，多くのパブリック DNS サーバが広く利用されており，DNS キャッシュサーバが正当な送信者のものか否かを分類するのは困難である．

- (A) DNS キャッシュ機構の正当性検査
  メール送信ホストがメールを送信する際，宛先ドメインの MX レコードの問い合わせを行う．メール送信ホストが利用する DNS キャッシュサーバが，問い合わせ結果である MX レコード情報を TTL に基づいて適切に管理し，また適切な MX サーバの選択を行う機構を有するかを検査し，spam 送信ホストを検出する．この検査手法についての詳細は 4 章で述べる．

- (B) 5-Way Handshake
  RFC5321[15] によれば，送信ホストは配送先ドメインの MX レコードの問い合わせを行った後，その優先度の順に接続を試みなければならないと定められている．5-Way Handshake は，まず MX レコードに優先度の異なる 2 つの受信ホストを用意する．SMTP セッション確立時に送信ホストからプライマリ MX に送られる SYN パケットに対し，プライマリ MX が RST パケットで応答する．これによりセカンダリ MX への再送（MX フォールバック）を促し，セカンダリ MX で受信する手法である [23]．セカンダリ MX への配送を受信する spam 対策手法

は，Nolisting と Unlisting と呼ばれる手法が広く利用されている．また，本論文で述べるリアルタイム MX フォールバック検出手法も 5-Way Handshake の一種と分類できる．

・Nolisting

この手法は，プライマリ MX への TCP 接続を固定的に拒否し，セカンダリ MX では常に接続を許可するものである．しかし，spam 送信ホストは MX レコードの優先度を守らない場合が多く，MX フォールバックの手順に従わずに 1 度目の配送でプライマリ MX とセカンダリ MX を区別すること無く配送を試みる．その結果，多くの False Negative が発生し，効果的な手法とは言い難い．

・Unlisting

この手法は，Nolisting を強化した手法であり，MX フォールバック後の配送のみをセカンダリ MX で受信するものである．Unlisting は，Tempfailing で生じる長時間の遅延の問題や，Nolisting で非常に多く発生する False Negative を改善する手法であるが，送信ホストがラウンドロビン等の理由で，再送時に異なる IP アドレスから送信した場合，これを再送であるという判断をすることができないため，False Positive が発生する．この手法はパケットフィルタリングによって容易に実装することができるが，送信ホストからの最初の SYN パケットに対し即座に RST パケットを応答するため，送信ホストは瞬時に再送を行う．従って，セカンダリ MX は受信の可否を判断する時間を確保することができなくなる．さらに，高負荷時にパケットフィルタリングの処理が遅延した場合，何らかの対応が必要となるが，そのための時間を確保することが出来ないなど，実用性に問題がある．

・MX フォールバック検査

送信ホストが，(A) の MX レコードの問い合わせによって得た情報に基づき，優先度の異なる複数の MX サーバリストについて，その優先度順に配送を試みる機構を有するかを検査する手法であり，優先度順に配送された場合にのみ spam 送信ホストを検出する．類似手法である前述した Nolisting や Unlisting の実装方法では様々な欠点が存在する．これらの欠点を解決する手法についての詳細は 4

章で述べる．

以上の手法は，SMTP セッションに入る前の TCP コネクション確立までの過程で spam 送信ホストを判別する手法である．

- (C) HELO/EHLO 検査
  RFC5321 によれば，送信ホストが最初に発行する SMTP コマンドは EHLO あるいは HELO であり，それに続いて完全修飾ドメイン名，または送信ホスト自身の IP アドレスを角括弧で囲んだものを指定することが定められている．送信ホストが HELO/EHLO を送信しない場合，および HELO/EHLO で指定された値が不正な要求であった場合に，spam 送信ホストであると判断し，SMTP エラーを応答する．

- (E) RCPT TO 検査
  多くの spammer が，ランダムな文字や数字の組み合わせや辞書等に基づいて生成したメールアドレスに対して spam メールを送信する．そのため，存在しないアカウント名に宛てた大量の spam メールが受信サーバに届くことになり，高い負荷がかかることになる．RCPT TO 検査は，実際に存在しないアカウント宛のメールを受信する前に拒否し，負荷を軽減する手法である．

- (B)∼(E) QoS コントロール
  Symantec Traffic Shaper powered by Brightmail[24] や Symantec Messaging Gateway powered by Brightmail[25] では，レピュテーションサービスと自己学習によって，送信ホストの IP アドレスを複数のグループに分類する．送信ホストの IP アドレスが完全な spammer グループに属すると判断された場合，当該システムは RST パケットを送信し，SMTP コネクションを即座に切断する．spam 送信の頻度等に応じて，400 番台の一時的エラー応答または QoS コントロールを選択する．QoS コントロールは，秒あたりのセッション数やコネクションあたりのメール数の制御を行うことにより，spam 送信ホストに対する QoS を低下させるものである．

  spammer グループの判定は，(1) 製造元から配布される情報，(2) 個々の機器が自己学習によって取得する情報が逐次データベースに格納されており，これを参照

することで行われている．一般に，MTA は複数のネットワークに分散配置され，かつ，その台数も多いため，(2) の情報を機器間で共有すると，通信のオーバーヘッド，およびデータベースへの負荷が増大する．このため，機器間の情報共有を行わない設定を推奨したり，そもそもそのような機能を持たないことが多い．

- (C)∼(E) ブロッキング
  ブロッキングは，送信ホストの IP アドレスや SMTP セッション中の “MAIL FROM:” で示されるエンベロープ From アドレス等の情報に基づいて spam メール判定を行い，メールデータを受信する前に spam メールを拒否する手法である．代表的なブロッキングの実装例として，次に挙げる手法が存在する．

  ・IP アドレス逆引き検査

  IP アドレス逆引き検査の実装は，S25R（Selective SMTP Rejection）が一般的である．IP アドレスの逆引きに失敗した場合には恒久拒否または一時拒否，応答遅延等，運用ポリシに応じてペナルティを課す．また，この手法は spam メールがエンドユーザの使用するボット感染した PC から送信されることが多いことに注目した手法であり，逆引きホスト名が例えば多くの数字からなる場合には，ISP 事業者がエンドユーザ向けに付与された可能性が高いことから，動的 IP アドレスからの送信であると判断する．この手法は容易に導入が可能である長所を持つが，PTR レコードを持たない正当な MTA も多く存在し，またネットワークや DNS サーバのトラブルによって False Positive が多く発生する．さらに，DNS 検索を行うため，ネットワークや DNS サーバに負荷となる点も短所として挙げられる．

  ・ブラックリストの利用

  ブラックリストの利用では，spam メール送信ホスト，不正アクセスホスト，spam メール本文に含まれる URL 等が登録された公開ブラックリストまたは自前ブラックリストの情報に基づいて spam 判定を行う．公開ブラックリストは DNSBL（DNS Blacklist）と呼ばれ，Spamhaus ZEN[34]，SpamCop SCBL[35]，SORBS[36] 等が代表的である．例えば，Spamhaus ZEN は次のように使用する．IP アドレスが “1.2.3.4” である送信ホストからの SMTP 接続を観測すると，“`4.3.2.1.zen.`

spamhaus.org" の A レコードを検索し，A レコード（127.0.0.x）が得られた場合に接続を拒否する．DNSBL に登録されているホストは，実際のボット感染ホスト数の約 6%程度に留まるとの報告 [37] もあり，また検出後直ちに登録されるホストは少ないことから，効果が限定的であると言える．

・Tempfailing

RFC5321 によれば，送信者 MTA が一時的エラーを示す 400 番台の応答を受信した場合，一定時間後に再送処理を行わなければならないと定められている．しかしながら，spam 送信ホストはメール配送の信頼性よりも配送効率を優先するため，一時的エラーを受信しても再送処理を行わないことが多い．Tempfailing はこのような spam 送信ホスト特有の動作に注目し，spam 判別を行う手法である．

Tempfailing の代表的な手法として，greylisting[16][17][18][19] やお馴染みさん方式 [20] が広く利用されている．greylisting は三つ組（mail from:，rcpt to:，送信者の IP アドレス）を SMTP セッション中に取得し，これらの組によって再送の判定を行う．1 度目の配送では，送信ホストに対して一時的エラーを応答し，三つ組を数時間保持する．この情報を保持している間に，同一の三つ組からの配送が行われた場合に再送であると見なし，受信処理を行う．また，これと類似した手法にお馴染みさん方式がある．この手法は三つ組ではなく送信者ホストの IP アドレスのみによって再送の判断を行う．

Tempfailing は spam メールの判別を行うのに効果的であるものの，配送に長時間の遅延を生じる欠点がある．RFC5321 によれば，送信ホストは一時的エラーを受信後，少なくとも 30 分以上経過後に再送を行うよう推奨されているため，30 分以上の配送遅延が予想される．また大規模な組織では，複数の MTA を使用し，1 度目の送信時とは異なる MTA から再送する運用を行っているものもある．この場合，再送の判断が正しく行えない問題が発生する．

- (C)∼(E) スロットリング
  スロットリングは，意図的に通信速度等を制限し，大量送信を妨害する手法である．代表的なスロットリングの実装例として，同時接続数やセッションの確立頻度，帯域の制限を行うものや，Tarpitting と呼ばれる手法がある．同時接続数や

セッションの確立頻度，帯域の制限を行うと，DoS 攻撃に対する防御として機能し，spam メールの大量配送を阻止することができる．一方で，spam メールではない正当なメール配送時にも影響を与える点が問題となる．Tarpitting は，意図的に応答を遅延させ，spam 送信ホストに接続をタイムアウトさせることを誘発させる手法である．Tarpitting の代表的な実装である Greet pause は，コネクション確立時の応答であるリプライコード “220” を遅延させる．RFC5321 では，送信ホストは 5 分間待機するよう定められているが，多くの spam 送信ホストはこれを守らず，15 秒程度で切断する．また，“MAIL” や “RCPT” コマンドの応答を遅延させる手法も存在する．

- (F) SMTP セッション強制切断
  前述の Tempfailing は，再送時に異なる MTA から配送が行われた場合に管理者が手作業で MTA を登録するなどの問題があるが，この手法ではヘッダや本文を受信後に強制切断することにより，メッセージの同一性を確認して再送判定を行うことができる [45][46].

2.2.2 メール受信後の対策

- (G) コンテンツフィルタリング
  メールのヘッダ情報や内容に基づいて spam 判定を行うコンテンツフィルタリングは，メール受信後に判定する．コンテンツフィルタリングの判定手法は多岐に渡るが，ルールベースフィルタ，ベイジアンフィルタ，分散協調型フィルタが一般的に利用されている．キーワードや公開データベース，学習フィルタ等の視点から点数化して spam 評価を行う SpamAssasin[10][11] や，ベイジアンフィルタ [38][39] の実装例として Bogofilter[12][13] や，日本語に対応した Bsfilter[14] が挙げられる．さらに，サポートベクタマシンによる spam 分類 [40] や機械学習による spam 分類手法 [41]，本文中に含まれる URL の解析によって spam 判定を行う手法 [42][43] 等も提案されている．

  これらの手法はいずれも，送信ホストと受信サーバの間において，メールの送受信に関する全ての通信が完了した後で判定するため，spam 送信に起因するト

ラフィック量の軽減には一切貢献しない．特に，SMTP セッション中の “DATA” コマンドの送信時に大容量のデータが送信され，短期間に集中的に大量の spam メールを受信した際，DoS 状態に陥り，正常なメール受信処理を行えなくなる危険性がある．

2.2.3 送信ドメイン認証

- (D) 送信ドメイン認証（SPF）
  序論で述べたように，spammer は自身のメールアドレスを詐称して spam メールを送信することが多い．SPF（Sender Policy Framework）[44] は MAIL FROM:（エンベロープ From）で示された送信元メールアドレスのドメインについて，DNS の SPF レコードで指定された送信元ドメインの正規の送信ホストの IP アドレスと，配送を行っているホストの IP アドレスとを照合し，なりすましを検出する手法である．

- (F) 送信ドメイン認証（Sender ID）
  (D) で述べた SPF と類似した手法に Sender ID[47][48] がある．Sender ID は，SPF のエンベロープ From の送信ドメインチェックに加えてヘッダ情報（PRA:Purported Responsible Address）による認証も併せて行う．PRA はヘッダの Resent-Sender:，Resent-From:，Sender:，From:の順序で判定する．

2.3 提案手法による改良点

本論文で述べる MX フォールバック検出手法や DNS キャッシュ機構の正当性検査は，メール通信時に spam 送信ホストを識別する．これらの手法は，2.2 節に記した各手法が抱える問題点に対し，以下の点を解決する．

- トラフィック量の軽減と低負荷化
  メール受信後に spam メール判定を行うコンテンツフィルタリングでは，2.2.2 節に示すように，トラフィック量の削減に貢献せず，また判定処理によっては多くの計算資源を消費する．本論文で述べるいずれの手法もメール受信前の通信挙動

によってspam送信ホストを判別するため，トラフィック量の削減とサーバ負荷の低減が実現できる．

- 配送遅延問題の解消

  SMTPセッション時に一時的エラーを応答し，送信ホストからの再送を受信する手法であるTempfailingは，メールの受信までに数十分から1時間以上の遅延が生じる．本論文で述べる手法は，SMTPセッションの前段階であるTCP接続時の再送機構を利用することにより，遅延を数秒程度に抑制することができる．

- 判別精度の向上

  固定的にプライマリMXではTCP接続を拒否し，セカンダリMXでは接続を拒否するNolistingは多くのFalse Negativeが発生する．本論文で述べる手法はUnlistingと同様に，MXフォールバック後の配送のみをセカンダリMXで受信するため，spamメール送信ホストの識別精度を向上させることができる．

  さらに，本論文で述べる定期的にMXレコードを変更して応答する特殊なDNSコンテンツサーバを利用したspam対策手法は，メール通信時の対策のみでなく，メール受信後にspam判定を行う各手法にも適用が可能であり，汎用性が高い．

- 実用性の確保

  Unlistingでは，送信ホストからの1度目のSYNパケットに対し，プライマリMXが即座にRSTパケットを応答するため，送信ホストは即座にMXフォールバックによりセカンダリMXに再送する．従って，プライマリMXから通知される送信ホストに関する情報の処理がセカンダリMXで完了する前に再送が開始され，セカンダリMXでは受信の可否を判断することができなくなる．また，高負荷時にパケットフィルタリングの処理が遅延した場合の対応が困難となり，判定・受信処理を行うために十分な時間を確保する必要がある．

  本論文で述べる一時ホワイトリストを利用した再送検出手法では，送信ホストからプライマリMXへのSYNパケットの再送が繰り返される間に当該ホストを一時ホワイトリストに登録出来れば良い．また，調査した全てのOSの中でタイムアウトが最短のものでも再送は9秒間繰り返されることが確認され，高負荷等の

理由で一時ホワイトリストの処理が遅延した場合でも，十分な時間が確保でき，検査を確実に実施できる．

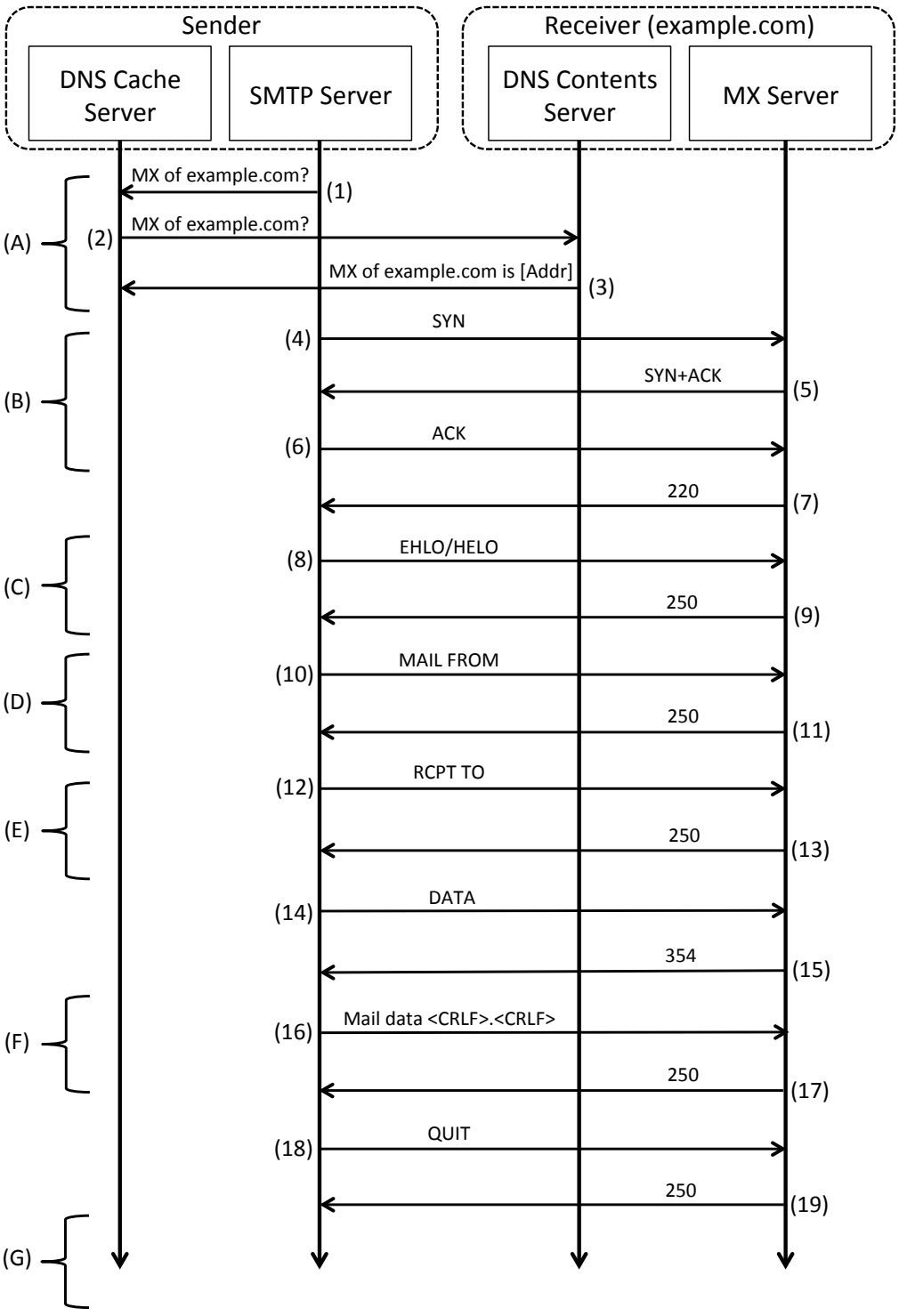

図 2.1: メール送受信の手順

第3章

送信ホストの通信挙動調査と spam送信ホスト識別法

2章で述べたように，従来のspamメール対策手法には様々な問題点が存在する．本論文では，spamメールのトラフィック量を減少させ，サーバ負荷の軽減を図ることにより，運用コストの削減や安定運用が行えるspamメール対策手法を提案する．

その中で本章では，これらの問題を解決するリアルタイム再送検出手法の提案に向けて，正当な送信ホストの通信挙動を詳細に解析し，その差分により両者を識別できることを確認した．さらに，この知見に基づいたspam送信ホスト識別システムの実装法について検討する．

3.1 まえがき

2章で述べたように，Tempfailingや5-Way Handshake等，SMTPセッション時の振舞いの特徴を利用したspam対策システムが存在する．Tempfailingは，送信ホストの再送ポリシの特徴を利用したspamメール対策手法である．この手法は効果的であるものの，メール配送に長時間の遅延を生じる欠点がある．この欠点を解決するため，Nolisting[21]やUnlisting[22]等，5-Way Handshakeと呼ばれる手法が提案されている．しかし，これらの手法も重大な問題を抱えており，例えばNolistingはFalse negative（見逃し）が非常に多く発生し，Unlistingは容易に実装可能だが，仕組みが単純すぎるため柔軟性に乏しく，実用性に問題を抱えている．

本章では，これらの諸問題を解決する新たな手法の提案を目的として，正当な送信

ホストが使用するメール転送エージェント（MTA）と spammer の使用する送信プログラムの再送戦略ポリシを詳細に調査し，そこから両者が判別可能であるか調査を示す．

3.2 再送動作の調査

図 3.1 のように構成した Unlisting の受信環境を用意し，送信ホストの再送挙動を調査を行った．調査を明確にするために，全ての MX サーバを同一のネットワークセグメントに指定した．本調査は，図 2.1 の (4)(5)(6) で示す TCP コネクション時の動作に該当し，図 2.1 中の “MX Server” が 3 台存在する場合を示す．

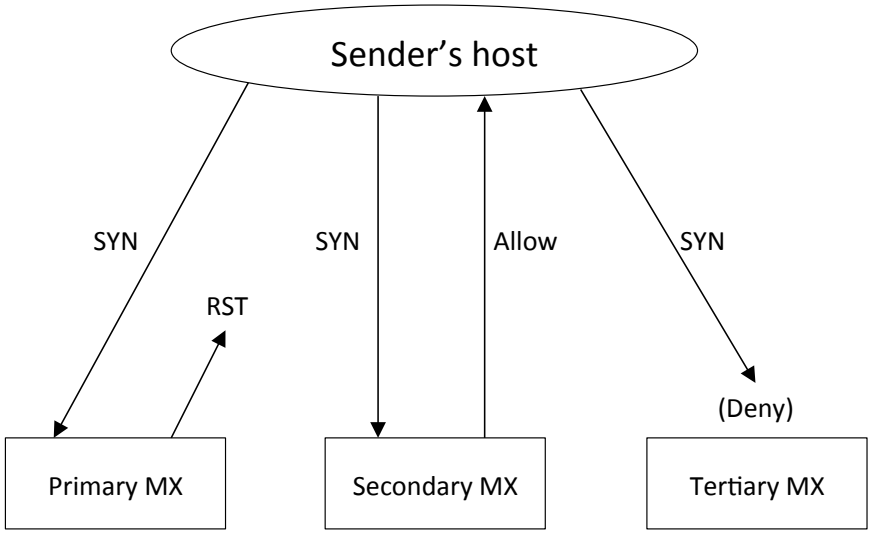

図 3.1: 調査に用いた受信サーバの構成

3-Way Handshake の SYN パケットに対してプライマリ MX が応答を行わずに沈黙した場合，多くの送信者 MTA はプライマリ MX に対して SYN パケットの再送を数回行う．また，プライマリ MX が SYN パケットへの標準的な応答である SYN+ACK パケットを応答した場合，殆どの送信ホストは ACK パケットを送信し，タイムアウト（数分間）までの間プライマリ MX との通信を試みる．従って，これらの応答は送信ホストが MX フォールバックを行うまでに非常に長い時間を要することになり，正当な送信ホストに対してこれだけの負担を強いることは得策ではない．このことから，プライマリ MX は SYN+ACK パケットの代わりに RST パケットで応答することにより，

MX フォールバックを誘発させている．

さらに，spam メール送信ホストの異常な振舞いの調査を行うために最も優先度を低く指定したターシャリ MX を設置した．ターシャリ MX は通常使用されるべき MX サーバではないため，全ての通信を拒否し，単に spam 送信ホストが優先度の参照を行うか否かを調査するために用いる．この章では，この環境に対する正当な送信ホストおよび spam 送信ホストの送信動作を詳細に調べ，それらを比較することで判別可能であるか検討を行う．

3.2.1 正当な送信ホスト

正当な送信ホストとして，大学，ISP，携帯電話，フリーメールサービス，web メール等のアカウントを使用して調査環境に対してメール送信を行った．本調査は，一つの OS に 3 個の IP アドレスを備えさせ，それぞれにプライマリ，セカンダリ，ターシャリ MX を割り当て，パケットフィルタリングによりログを取得して解析した．従って，本調査では一つの OS で情報を収集することで，各 MX 間の同期問題や時間精度の問題を解決した．

この結果，一部のドメインにおいて，一つのメールの配送でプライマリ MX およびセカンダリ MX への送信を異なるホストから行うものを確認した．本調査では，このようなドメインに対応するため，各ホストの DNS 逆引き検索を行い，それらの権威サーバが同一であればこれらのホストは同じドメインに所属すると判断した．なお，今回の調査でこのように判定が必要だったのは 4 ドメインであり，そのいずれの場合も，一度目の配送とそれ以降の配送で使用したホストの IP アドレスはクラス C(/24) に属していた．

本調査の結果を表 3.1 および 3.2 に示すが，上記のようなドメインを区別せず，同一ホストから再送を行ったと見なした．

表 3.1 は正当な送信ホストの再送挙動を示す．“*” 印の後の数字は再送回数を表し，例えば “Primary * 3 → Secondary” はプライマリ MX への接続を 3 回試行した後にセカンダリ MX に再送を行ったことを意味する．この調査により，実験に使用した正当な送信ホストによる配送では，全てのホストがプライマリ MX に対して 1 度目の送信を行い，その後 MX フォールバックしてセカンダリ MX に再送を行うことを確認した．

表 3.1: 再送動作

送信先 MX サーバの順	ホスト数	割合
Primary → Secondary	20	91.0%
Primary * 2 → Secondary	1	4.5%
Primary * 3 → Secondary	1	4.5%

表 3.2: 再送までの時間間隔

MX フォールバックまでの時間	ホスト数	割合
∼ 1 sec.	20	91.0%
1 ∼ 2 sec.	2	9.0%

また，表 3.2 に示すように MX フォールバックを調査に用いた全ての送信ホストが 2 秒以内に行っており，非常に高速に行われることを確認した．

同様の調査を，現在広く利用されている MTA として Postfix 及び Sendmail を実装したホストから調査環境に対してメール送信を行ったところ，どちらの MTA による配送も “Primary→Secondary”（表 3.1 最上段に該当）の配送順であり，またセカンダリ MX への再送までに要した時間は 1 秒未満（表 3.2 最上段に該当）であった．

これらの結果を踏まえ，“正当な送信ホストの条件” を次のように定義した．

1. 1 度目の送信はプライマリ MX に対して行う．
2. プライマリ MX への再送は 3 回以下．
3. MX フォールバックは 2 秒以内に行う．

3.2.2 spam 送信ホスト

3.2 節で述べた調査と同一の調査環境を使用して spam 送信ホストの配送動作の調査を行った．本調査では，筆者自身による通常のメールは送信せず，spam メールのみを受信させた．従って，このメールサーバに対して正当なメールが送信されることは考え難く，当該 spam 収集サーバに送られたメールを spam メールであるものとした．誤

送信などによる正当なメールの誤送信が含まれる可能性は排除できないが，その可能性は極めて低く，また含まれていた場合でもその数はごく僅かであるため，性能評価には影響しないと判断した．

はじめに，どの程度の spam 送信ホストが前節で定義した “正当な送信ホストの条件” を満たすかを調べ，次に spam 送信ホストを効果的に判別する手法を検討した結果，spam 送信ホストの配送動作に基づき以下の 5 種類に分類した．

(1) 正当なホストの条件を満たしたもの（正しく MX フォールバックを行うもの）

(2) 1 度目の送信をセカンダリ MX に対して行ったもの（優先度を無視）

(3) 1 度目の送信をターシャリ MX に対して行ったもの（優先度を無視）

(4) プライマリ MX への試行からセカンダリ MX への再送までに 2 秒以上の時間を要したもの（タイムオーバー）

(5) プライマリ MX への試行後にセカンダリ MX へ送信を行わないもの（プライマリ MX のみに送信）

上記 5 つの項目のうち，(1) のみが正当な送信ホストと同様の挙動を示した spam メールの配送であり，その他の項目は前節で定義した条件を満たさなかったものである．

ただし，正当なメール送信ホストと同様の挙動である (1) に分類された spam メールの配送であっても，RFC5321 で定められた再送戦略を適切に実装した spam 送信プログラムからの配送であるとは限らない．例えば，ポートスキャン等によって MTA を発見したり，近隣の IP アドレスに対して総当たり的に送信を試み，偶然に優先度順の配送となった場合が含まれる．従って，(1) に分類された spam 送信ホストからの配送は，別の配送時には (2) や (3) の挙動を示すものが含まれる可能性がある．同様に，MX レコードの優先度順序に従わない配送である，(2) や (3) の挙動を示した spam 送信ホストは，別の配送時には (1) の挙動を示すものが若干数含まれる可能性がある．

さらに，(5) はプライマリ MX に一度のみ接続を試みて試行を取りやめるものと，プライマリ MX への接続失敗後に次優先度であるセカンダリ MX ではなく，プライマリ MX のみに対して接続試行を継続するものの両方が含まれる．また，(5) は，プリファレンス値の参照に基づいた MX サーバの選択した場合だけではなく，偶然にプライマ

リ MX に対して配送を試みた場合も含まれるため，別の配送時には 1 度目の配送をセカンダリ MX やターシャリ MX に行う (2) や (3) の挙動を示すものが含まれる可能性がある．

表 3.3: spam 送信ホストの動作（月別の割合）

	2011/10		2011/11		2011/12	
(1)	22	2.42%	27	2.46%	20	1.02%
(2)	125	13.74%	163	14.86%	530	27.05%
(3)	90	9.89%	170	15.50%	514	26.24%
(4)	19	2.09%	34	3.10%	93	4.75%
(5)	654	71.87%	703	64.08%	802	40.94%
合計	910	100.00%	1,097	100.00%	1,959	100.00%
	2012/1		2012/2		2012/3	
(1)	52	2.59%	50	2.44%	26	1.73%
(2)	541	26.94%	443	21.60%	435	28.92%
(3)	493	24.55%	439	21.40%	414	27.53%
(4)	83	4.13%	149	7.26%	101	6.72%
(5)	839	41.78%	970	47.29%	528	35.11%
合計	2,008	100.00%	2,051	100.00%	1,504	100.00%

表 3.3 は，2011 年 10 月から 2012 年 3 月までの 6ヶ月間に調査環境に送信された spam メールの送信動作を上記の (1) から (5) に分類し，各項目に該当する spam メール送信ホストの合計数と全体に占める割合を示したものである．

これらの結果から，正当な送信ホストと同様に動作する spam 送信ホストの割合 (1) は 1.02%~2.59%と非常に低く，また表 3.3 の (2) および (3) が示すように，多くの spam メール送信ホストは MX レコードの優先度を無視して送信することが確認できる．従って，Nolisting では多くの False Negative が発生することが分かる．このような spam メール送信ホストの振舞いは，正確なメール配送よりも，できるだけ多くの spam メールをばら撒くことを優先しているためであると推測される．

この調査の結果，正当な送信ホストと spam 送信ホストの再送動作を解析することによって，これらを判別可能であることを確認した．

3.3 再送動作検出によるspam送信ホスト識別手法

本節では，3.2.2 節で述べた，正当な送信ホストと spam 送信ホストの配送挙動の差異を利用して，TCP コネクション時に spam 送信ホストを識別するシステムの実装法について述べる．

セカンダリ MX において，プライマリ MX への接続失敗後の再送のみに対して TCP コネクションを許可するシステムでは次のような処理の手順が考えられる．

(I) プライマリ MX およびセカンダリ MX はスタンバイモードであり，プライマリ MX は SYN パケットに対して RST パケットを応答し，セカンダリ MX は接続を拒否する．

(II) プライマリ MX への最初の SYN パケットを受信すると，その送信ホストからセカンダリ MX への接続を許可するように対応を変化させる．

(III) その送信ホストはセカンダリ MX に対して再送を行い，TCP コネクションを確立する．

Nolisting のように，セカンダリ MX が固定的に接続を許可して待機した場合には False Negative が多く発生するため，プライマリ MX は SYN パケットに対して RST パケットを応答し，セカンダリ MX は接続を拒否する設定で待機する (I)．プライマリ MX においてこのような応答を行うのは，3.2 節で述べたように，セカンダリ MX への再送を誘発させる必要があるためである．次に，この状態で送信ホストからプライマリ MX への 1 度目の SYN パケットを観測した瞬間に，セカンダリ MX で接続を許可するように対応を変化させ，再送時の接続許可に備え (II)，送信ホストからセカンダリ MX への再送時に接続を許可する (III)．

しかし，表 3.2 に示すように，送信ホストはプライマリ MX への接続失敗後のセカンダリ MX への再送は非常に高速に行われる．従って，上記の手順で処理した場合，(II) の処理がセカンダリ MX への再送までに間に合わない場合が生じ，多くの False Positive が発生してしまうため，得策ではない．

以上のことから，送信ホストからの 1 度目のプライマリ MX への接続試行観測からセカンダリ MX での接続許可までに十分な時間を確保し，システムの信頼性を確保するため，以下のような実装法を提案する．

本手法の実装には，一時ホワイトリストを用いる．一時ホワイトリストはFreeBSDのパケットフィルタ “ipfw” の検索表である “table” によって実装する．また，プライマリMX，セカンダリMX，ターシャリMXは全て同一OS上に実装することにより，全てのMXサーバからOS上で実装したipfw及びipfwのtableが参照可能である．

本手法では以下のような手順を踏むことにより，セカンダリMXはMXフォールバックを行った後の配送に対してのみ接続を許可することが可能である．

1. 初期状態では，プライマリMXおよびセカンダリMXはスタンバイモードであり，どちらのMXサーバにおいても送信ホストからの接続を拒否する．

2. プライマリMXへの最初のSYNパケットを受信すると，その送信ホストは一時ホワイトリストに登録され，プライマリMXはSYNパケットに対してRSTパケットを応答し，セカンダリMXは即座にその送信ホストからの接続を許可するように対応を変化させる．

3. その送信ホストはセカンダリMXに対して再送を行い，TCPコネクションを確立する．

表 3.4: ipfwのルール例

140 reset log tcp from table(1) to Primary MX dst-port 25 setup via bge0
160 deny log tcp from any to Primary MX dst-port 25 setup via bge0
240 allow log tcp from table(1) to Secondary MX dst-port 25 setup via bge0
260 deny log tcp from any to Secondary MX dst-port 25 setup via bge0
360 deny log tcp from any to Tertiary MX dst-port 25 setup via bge0

初期状態（1.）において，あるホストからプライマリMXへのSYNパケットを観測すると，表3.4のルール番号160によりログが出力される．本手法はログを監視し，当該ホストの送信元IPアドレスをtable(1)に “ipfw table 1 add” により追加する．次に，当該ホストからプライマリMXへ再送のSYNパケットが到達する（2.）と，ルール番号140により直ちにRSTパケットが送信される．MXフォールバックにより，当該ホストがセカンダリMXへSYNパケットを送れば，ルール番号240により3-Way

Handshake が行われる（3.）．このように，正しく MX フォールバックを行った送信ホストのみがセカンダリ MX への TCP コネクションを許可される．なお，ルール番号 260 および 360 でもログを出力しているが，これは，MX フォールバックを行わないホストを検出するために用いている．

図 3.2 は，本手法における TCP コネクション確立までの流れを示す．

最初の SYN パケットが到着すると（図 3.2：(1)），プライマリ MX はそれに応答を行わないが (Deny)，その送信ホストを一時ホワイトリストに登録する（図 3.2：(A)）．送信ホストはプライマリ MX から何も応答が得られない場合，OS で事前定義された時間後に別の SYN パケットを送信する．一時ホワイトリストに登録された送信ホストによる再送の SYN パケットに対してプライマリ MX は RST パケットを応答する（図 3.2：(3)）．RST パケットを受信すると，送信ホストは MX フォールバックを行い，セカンダリ MX への接続を試み（図 3.2：(4)），送信ホストとセカンダリ MX との間で 3-Way Handshake が完了する（図 3.2：(5)(6)）．これにより，TCP コネクションが確立し，SMTP セッションを開始することが可能となる．

また，これまでに述べた再送検出手法を実装するためには少なくとも 2 つの MX サーバを設置すればよいが，本実装ではターシャリ MX を設置している．ターシャリ MX は補助的な存在であるが，表 3.3(3) から読み取れるように，プリファレンスに従わずに無作為に選択した MX サーバに対してメールの送信を試みる spam 送信ホストが多く存在する．そのような spam 送信ホストへの対応のためにターシャリ MX を設置し，これに接続を試みる送信ホストを監視することによりプリファレンスに従わない spam 送信ホストを検出することができ，False Negative の抑制が期待できる．

3.4 まとめ

本章では，Unlisting 環境を用いて正当な送信ホストと spam 送信ホストの通信挙動を詳細に調査した．実際に利用されている正当な送信ホストからの配送で，調査範囲内の全てのホストが満たす “正当な送信ホストの条件” を独自に定め，その条件をどの程度の割合の spam 送信ホストが満たすかを確認したところ，ほぼ全ての spam 送信ホストが条件を満たさず，特有の挙動を示すことを確認した．このような spam 送信ホスト特有の通信挙動は，spammer が正確なメール配送よりも送信効率を重視してでき

るだけ大量の spam メールの配送を試みるためであると考えられる．

表 3.3 の結果から，正当な送信ホストと同様の配送挙動を示す spam メール送信ホストの割合（表 3.3：(1)）は各期間で 1.02%から 2.59%で推移しており，大多数の spam 送信では正当な送信ホストとは異なる挙動を示すことを確認した．

一方で，MX レコードの優先順序に従わない配送である（表 3.3：(2)）および（表 3.3：(3)）の配送や，MX フォールバック機構を持たないホスト（表 3.3：(5)）の割合が大多数を占めていた．また，(2)，(3)，(5) は月毎に割合の変動があるものの，正当な再送戦略を採る spam 送信プログラムはわずかであることが読み取れる．

また，正しい優先順序であるが，正当なホストと比較して再送までに長時間を要した spam 送信ホスト（表 3.3：(4)）の割合は低く推移しており，MX フォールバックを行うまでに要する時間を厳格に検査しても効果は限定的であるという知見を得た．

さらに，この知見を利用して spam メール送信ホストを識別するシステムを実装する際，送信ホストからの 1 度目の SYN パケット観測時にセカンダリ MX の対応を変化させると適切に処理出来ない可能性がある．この問題を解決するため，一時ホワイトリストを使用した実装法を検討した．この手法は MX フォールバック後のセカンダリ MX への配送のみを確実に受信し，かつ受信までに要する時間もわずかであるため，少ない遅延時間で spam 送信ホストからの配送を識別することができる．

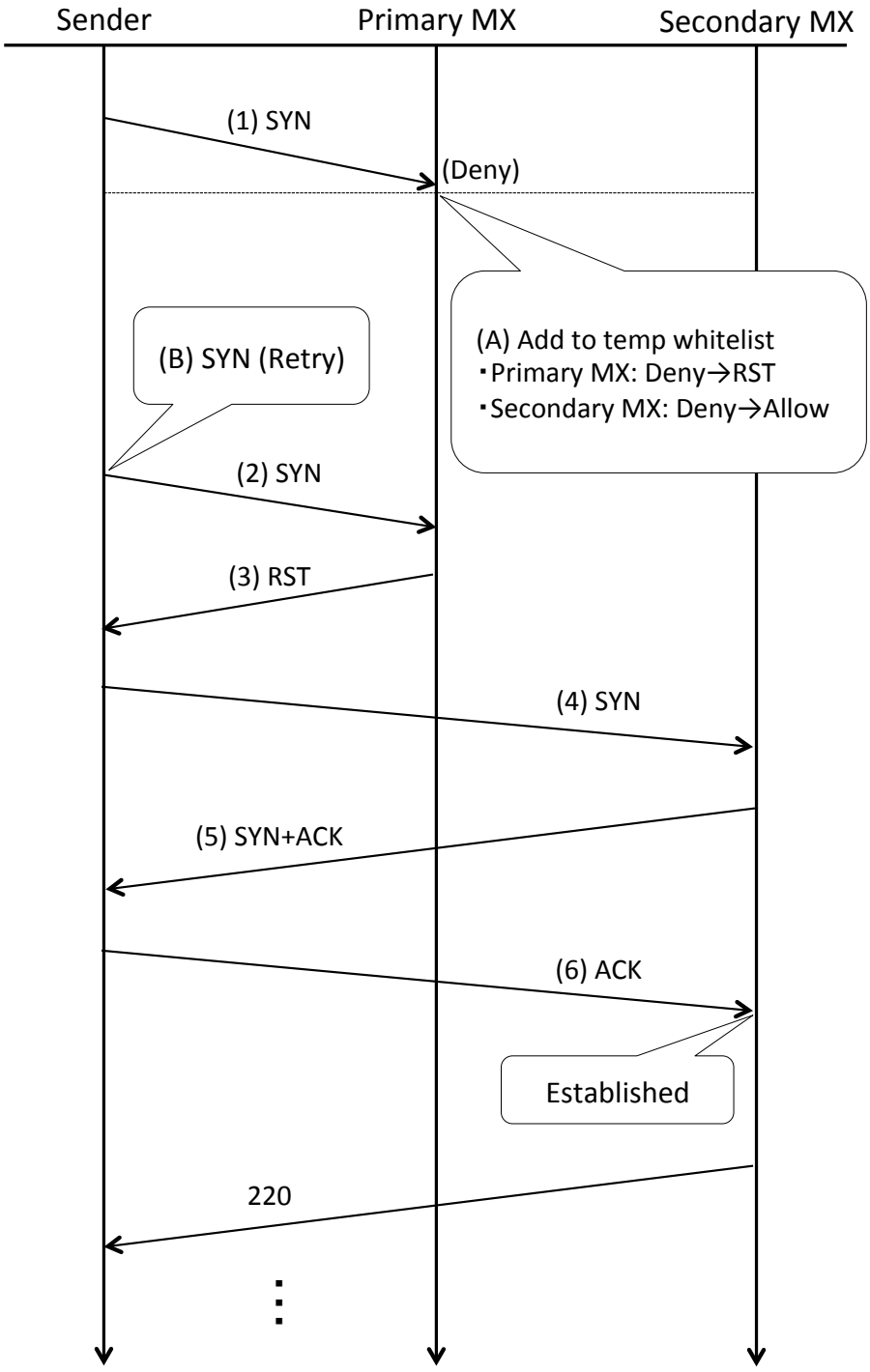

図 3.2: TCP コネクション確立の流れ

第4章

再送動作のリアルタイム検出によるspam判別手法

3章において，正当なメール送信ホストとspamメール送信ホストの識別が可能であることを確認し，その知見に基づいたspam送信ホスト判別システムの実装法を検討した．本章では，従来の5-Way Handshakeが抱える諸問題を解決し，さらに効果を高める手法であるリアルタイム再送検出手法の実装や実運用時における評価，および拡張機能の提案にについて述べる．

4.1 まえがき

3章で述べたように，正当な送信ホストが使用するメール転送エージェント（MTA）とspam送信者の送信プログラムを，両者の通信挙動の違いから識別することが出来る．また，その特徴を利用したシステムを実装する際，送信ホストからプライマリMXへの1度目のSYNパケット観測時にセカンダリMXの対応を変化させる方法では，対応処理が再送の観測までに完了しない恐れがある．この問題を解決するため，一時ホワイトリストを使用することにより，セカンダリMXへの再送までに対応変更処理を確実に実施できる．

本章では，この手法を実装して動作させ，実際に運用する上で考慮すべき点についての考察や，拡張機能の提案を行い，リアルタイムで再送動作を検出し，spam送信を行うホストを検出する手法の開発について述べる．本手法は，セカンダリMXとの間のTCPコネクションを確立できるのは，正しくMXフォールバックした送信ホスト

のみに限定することで，高速かつ低負荷を維持したまま，正確に spam 送信ホストを判別できる．

4.2 再送動作のリアルタイム検出システム

4.2.1 一時ホワイトリストによる実装

3.3 節で議論したように，再送戦略の違いに基づいて spam 送信ホストからの配送を判別するシステムの実装法が検討されている．この実装法は，プライマリ MX への 1 度目の SYN パケットの観測からセカンダリ MX への再送の SYN パケットを観測するまでに，受信対応のための処理を行うために十分な時間を確保することが出来る．

送信ホストの視点では，プライマリ MX への 1 度目の SYN パケットに対する応答が得られないため，再度プライマリ MX に対して SYN パケットを送信することが考えられる．次に，このプライマリ MX への再送の SYN パケットに対しては RST パケットの応答が得られるため，瞬時にセカンダリ MX に対し接続試行を行う．

本手法の実装では，特に次に挙げる点が重要となる．

- 正当な送信ホストからプライマリ MX への SYN パケットの再送はもれなく行われるか．
- 送信ホストを一時ホワイトリストに保持する期間の違いによって判別精度は変化するか．
- 特に高負荷時においても，受信対応のための処理は遅延なく実施可能であるか．

プライマリ MX への SYN パケットの再送が実施されない場合，その配送は False Positive となり受信不可となるため，十分な検証の必要がある．これについて 4.2.2 節で詳細に議論する．

また，一時ホワイトリストに登録されている期間は，その送信ホストはセカンダリ MX と接続することができる．従って，一時ホワイトリストの保持時間を長く設定すると，spam 送信ホストからの配送で，ポートスキャンやランダムな送信等で複数の MX サーバに当て推量で送信した場合，偶然に正しい優先度順配送となり，セカンダ

リ MX で spam メールを受信してしまう可能性が高まることが予想される．これについて，4.2.4 節で述べる．

さらに，本システムは再送ホストからプライマリ MX への SYN パケットの再送が継続している間に一時ホワイトリストへの登録処理が完了しなければならない．この処理が遅延した場合，受信処理が行えないことになるため，検討を行う必要がある．これについて，4.3 節で評価する．

4.2.2 本手法の実行可能性

3.3.1 節の一時ホワイトリストを実装するために，プライマリ MX への 1 度目の SYN パケットを監視し，セカンダリ MX への接続を許可するようファイアウォール (ipfw) の設定を変更する方法を採用した．ただし，表 3.2 から読み取れるように，殆どの正当な送信ホストは非常に高速に MX フォールバックを行うため，ファイアウォールの設定変更が 3.3 節の手順（3.）の開始までに完了できない可能性がある．この問題の影響を受けないためには，上記手順を完了するために十分な時間を確保する必要がある．

本手法の実装では，この時間を十分に確保するために，プライマリ MX への 1 度目の SYN パケットを棄却し，2 度目の SYN パケットの再送を MX フォールバックを促すために利用しているが，各 OS がこのメカニズムと互換性を有するかを調査しなければならない．

図 4.1 は，受信ホストが送信ホストからの SYN パケットに対して何も応答しなかった場合の，主要な OS による SYN パケットの再送時間間隔を示す．送信ホストと同一のネットワークセグメントに配置した受信ホストで tcpdump コマンドを用いて送信ホストから送られるパケットを観測した．本調査は各 OS についてそれぞれ数回ずつ送信を行い，観測した再送時間間隔にズレが無く，結果の信頼性を確認した上で SYN パケットの再送時間をプロットした．

本調査は同一のネットワークセグメントに配置したホスト間で行ったが，実際のインターネット越しで同様の調査を行った場合，ネットワーク遅延等の影響により，実験結果と比べ SYN パケットの到着間隔にズレが生じることが予想される．しかし，本調査の目的は各 OS が SYN パケットの再送機能を有していることを確認するためであり，到着間隔のズレが以後の考察に影響を及ぼすことはない．また，実験結果よりも

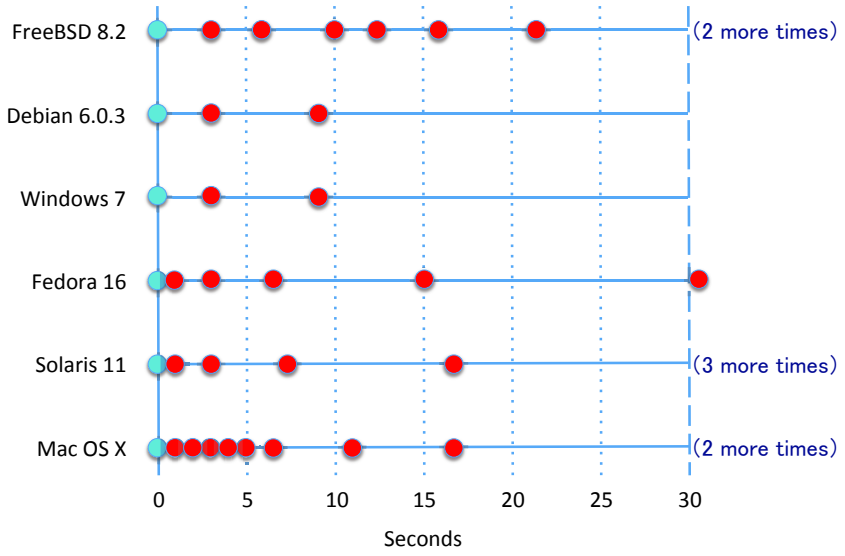

図 4.1: SYN 再送の時間間隔

到着間隔が短くならないことは，提案手法の動作に時間的な猶予を与えることを意味する．図 4.1 の最も左側の点はそれぞれの OS について 1 度目の SYN パケットの配送を表し，それに続く点はその再送を表す．

この結果，全ての OS は数回 SYN パケットの再送を行うことが確認された．これらの OS の中で，1 度目の送信と最後の送信の時間間隔が最も短いものは 9 秒であった．従って，9 秒でタイムアウトとなるホストが存在することから，本手法では一時ホワイトリストへの登録を 9 秒以内に行わなければならない．この制限時間は，受信ホストの負荷が極端に高くならない限り十分な余裕があると考えられる．

図 4.1 が示すように，1 度目の SYN パケットの後の 2 度目の SYN パケットの再送は直ちに（例えば 1 秒）行われる．本システムの実装において，一時ホワイトリストは ipfw を用いて実装しているため，SYN パケットの再送までに登録が間に合わない可能性がある．このため，プライマリ MX が一時ホワイトリスト登録後に 1 度目の SYN パケットに RST パケットを応答すると，2 度目の SYN パケットの到着後となってしまう恐れがある．その場合，送信ホストはこの RST パケットに対してさらに RST パケッ

トを送信するため[1]，送信ホストに RST パケットを一度多く送信させる可能性があり効率的でない．また図 4.1 から，いずれの OS も SYN パケットの再送を何度か繰り返しており，わずか 1 秒から数秒程度の遅延を解消する目的で送信者ホストにコストを強いるべきではない．

さらに，Unlisting のように最初の SYN パケットに対して即座に RST パケットを応答すると，当該送信ホストの一時ホワイトリストへの登録がセカンダリ MX への再送までに間に合わず，セカンダリ MX への接続に失敗するため，送信ホストは接続をスムーズに行えず再度リトライを強いられたり，あるいはターシャリ MX に MX フォールバックするような意図しない動作をする恐れがある．

以上のことから，本手法は実運用環境に適した運用を行うことが可能であると言える．

4.2.3 一時ブラックリスト

3.2.1 節の結果から，調査を行った全ての正当な送信者ホストは 1 度目の試行はプライマリ MX に行うのに対し，spam 送信ホストによる多く配送で，表 3.3 のように 1 度目の試行でセカンダリ MX(2) やターシャリ MX(3) に対して送信している．このことから，1 度目の試行でプライマリ MX 以外の MX サーバに対して送信するホストを一時ブラックリストに登録し，前述の手順を踏まず直ちに TCP コネクション確立を拒否すべきである．

3.2.2 節で述べたように，多くの spam 送信ホストは MX レコードの優先度を無視し，プライマリ，セカンダリ，ターシャリ MX に対してランダムに接続を試みる．この結果，spam 送信ホストの配送で偶然に正当な送信ホストの条件を満たす可能性がある．例えば，“セカンダリ MX→ プライマリ MX→ セカンダリ MX” や “プライマリ MX→ ターシャリ MX→ セカンダリ MX” のような順序で送信を試みた場合，4.2.1 節で述べた手法では受信を許可してしまうため，False Negative 率が上昇する．このような spam 配送への対策として，一時ブラックリストを活用して該当する送信ホストの一時ホワイトリストへの登録を行わないことにより，False Negative を抑制することが可能である．また，ブラックリストは参照を高速に行うために，恒久的ではなく一時的に保持するべきである．現在は 60 秒間の保持で運用を行っているが，最も適切なブラックリ

[1]仕様依存である．RST パケットを応答せずに棄却する仕様も存在する．

ストの保持時間は今後の検討課題である．

また，プライマリ MX への再送回数が 3 回より多い場合，表 3.1 で示す正当な送信ホストによる動作とは異なるが，これは一時ブラックリストに登録すべきではない．例えば，ある正当な送信ホストが数通のメールをほぼ同時に送信を行う場合が想定され，プライマリ MX への送信回数の監視を行うと多くの False Positive（誤検出）が発生するためである．

4.2.4 一時ホワイトリストの保持時間

図 4.1 の結果から，全ての OS が最初の SYN パケットの送信から 3 秒以内に 2 度目の SYN パケットの送信を行うことを確認した．従って，一時ホワイトリストは少なくとも 3 秒間は保持しなければほとんどの配送を受信することができない．一方，一時ホワイトリストの保持時間を極端に長く指定した場合，False Negative 率が悪化することが予想される．これは，4.2.3 節で示した例と同様に，spam 送信ホストが配送先の MX サーバをランダムに選択したのにも関わらず，偶然正しい MX フォールバックと類似した挙動となる可能性が高まるためである．

図 4.2 は，2012 年 1 月から 3 月までの月毎の一時ホワイトリスト保持時間と False Negative 率の関係を示す．前述の通り，一時ホワイトリストは最低 3 秒間以上保持しなければならないが，この調査ではこれに 2 秒のマージンを与え，5 秒間の保持から開始している．一時ホワイトリストの保持時間が 20 秒程度までは，False Negative 率にそれほど変化は見られないが，30 秒程度から以降は前述の理由により急激に悪化していることが分かる．この結果から，一時ホワイトリストの保持時間は 5 秒から 20 秒程度で運用するのが適切であると考えられる．

保持時間を短くすると，正当な送信ホストがホワイトリストに登録される時間が短くなるが，短い保持時間が原因となって発生する False Positive の評価を行うため，3.2.1 節で使用した正当なホストによる送信を解析した．この結果，保持時間を 5 秒とした場合でも False Positive は観測されず，5~20 秒という保持時間が適切であることを確認した．

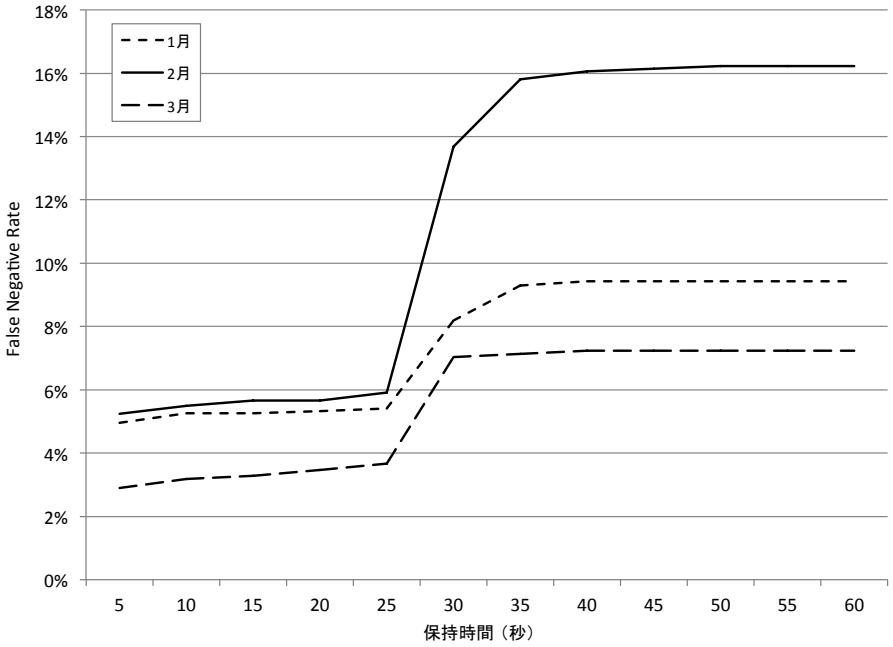

図 4.2: 一時ホワイトリストの保持時間と False Negative 率の関係

4.2.5 恒久ホワイトリスト

これまでの節で述べた手法は初めて接続する送信ホストに対しては効果的であるが，何度か正しく受信した実績のある送信ホストに対して適用する必要はない．そのため，恒久ホワイトリストを利用し，これに登録された送信ホストからの配送は全ての MX サーバで即座に接続を許可する．

恒久ホワイトリストは以下のようにして運用する．

1. 各正当な送信ホストに対して，一時ホワイトリストの保持時間内にセカンダリ MX への TCP 接続の数をカウントする．
2. 接続回数が閾値を超えた場合，その送信ホストは恒久ホワイトリストに登録される．

現在の我々の実装では，閾値を 3 回に設定しているが，配送実績回数の閾値の適切な回数は，今後の運用を通して判断する必要がある．

また，MTA の機能で，配送先 MX サーバの状態をキャッシュする機能を持っているものがある．例えば，Sendmail[30] の “confTO_HOSTSTATUS” の設定では，デフォルトでは無効となっているが，MX サーバの状態を一定時間キャッシュする．この機能を有効にした送信ホストから本手法を用いたシステムに対して送信実験を行ったところ，無効にした場合と同一の送信動作であることを確認した．この機能は，Sendmail のドキュメントで述べられているとおり，本手法で生じる数秒程度の遅延ではなく，数十分程度の遅延が生じる場合に発動するものであるため，本手法に対する影響は生じない．

このように，本手法は状況に応じて多様に対応を変化させる．図 4.3 に本手法のフローチャートを示す．

4.2.6 例外的な送信ホストへの対応

3.2.1 節で述べたように，プライマリ MX への 1 度目の送信時とは異なるホストから MX フォールバック後の再送を行う一部のサイトを観測した．この場合，再送時に使用されたホストの IP アドレスは一時ホワイトリストに登録されていないため，本手法は正しく配送を受信することができない．そのようなサイトに対応させるため，個別の IP アドレスの代わりに最初の SYN パケットを送信したホストの IP アドレスを含むクラス C(/24) の IP アドレスブロック[2]を一時ホワイトリストに登録することにより，暫定的な対応を行った．この対応の実装を行ってからこれまでの間，問題の発生は確認されていない．

また，正当な送信ホストからの同時送信を正しく受信できるかどうかを考慮に入れる必要がある．例えば ISP 等の大規模な組織からの配送では，プライマリ MX に対してほぼ同時に複数のメールが送信されることがあるが，この場合，本手法では 3.2.2 節の (5) のような，spam 送信ホストによる送信動作であると誤って判定する可能性が考えられるため，4.2.2 節と同様に，本手法がこのような送信ホストからの配送を正しく

[2]送信ホストが IPv6 アドレスの場合の一時ホワイトリストへの登録は，未実装であるが/64 を想定している．

処理できるかを確認する必要がある．この場合の動作は次のように実行される．

1. 送信ホストは 1 度目の SYN パケットをプライマリ MX に送信すると，その送信ホストの IP アドレスブロック (/24) は一時ホワイトリストに登録される．

2. 一時ホワイトリストの保持時間内に送信ホストが別の配送の SYN パケットを送信した場合，プライマリ MX は RST を応答し，セカンダリ MX は接続を許可する．(配送成功)

3. 一時ホワイトリストの保持終了後に送信ホストが別の配送の SYN パケットを送信した場合，この送信ホストは再度一時ホワイトリストに登録される．(MX フォールバック後に配送成功)

これまでに述べたように，本手法ではプライマリ MX への再送回数によって一時ブラックリストの変更を行わないため，上記のような大規模な組織からの配送と，MX フォールバックを行わない spam 送信ホストからの配送を正しく判別することができる．

さらに，MX フォールバックを行わない特定の送信ホストからのメール配送を受信したい場合を考慮する必要がある．このような動作は RFC5321 の規定に違反するものであるが，MX フォールバックを行わない MTA が確認されている [28]．当該 MTA のように規定を守らない MTA を使用する送信ホストからのメール配送は図 4.3 に示したシステムでは受信することができず，False Positive が発生する．このような送信ホストに対して，本手法では暫定的であるが，恒久ホワイトリストに該当するホストを登録することによって対処することができる．しかし，これらの MTA は提案手法以外でも配送失敗等のトラブルを起こすことが予想されており，製品側で対応されることを期待する．

4.3 高負荷時における耐久性の評価

本手法を実装したシステムに対して大量のメールが送信されるような状況でも，一時ホワイトリストへの登録を漏れや遅延なく行えるか評価する必要がある．本検査は，CPU が Pentium Dual-Core2180(2GHz)，メモリ合計 2GB という構成のシステムを使用した．

はじめに，負荷のかかっていない通常時にメール送信を行われた場合に，その送信ホストを一時ホワイトリストに登録するのに要した時間を “/usr/bin/time” を用いて調べたところ 0.01 秒未満であり，瞬時に登録できることを確認した．次に，大量のメールが寄せられている状況での評価を行うため，本システムに対して毎秒約 50 回の送信を行い続け，その状態で別の送信 MTA から本システムに対してメール送信を行った場合の一時ホワイトリスト登録に要する時間を同様に調べたところ，0.01 秒未満であり，負荷の影響を受けなかった．

本手法は，従来の spam 対策システムとは異なり，正しく MX フォールバックを行った場合の配送以外は，送信ホストからの SYN パケットに対して単に RST パケットを応答するだけであり，非常に高い負荷耐性を持つ．従来の spam 対策システムは，HELO や MAIL FROM，RCPT TO のチェックや，メールのコンテンツの検査を行うような手順を踏むため，SMTP セッションを確立することが前提条件となる．このため，この検査のように毎秒 50 送信のような高頻度の接続を受けると，その SMTP セッションを維持するためのプロセスが増殖し，DoS 状態に陥る．

本検査に使用したシステムは，比較的性能の低いマシンで実装しており，ハイエンドマシンではさらに実用的なシステムの構築が可能であることが期待できる．

4.4 spammer の送信戦略の影響

本手法の効果が期待できなくなる状況として，spam 送信ホストが RFC に従った正しい挙動をするようになることが考えられる．もし spam 送信ホストが本手法に適応した場合，言い換えれば，正当な送信ホストと同様に正しく MX フォールバックを行うようになった場合，その配送を spam であると判断することはできないため，本手法による効果が減少することが懸念される．しかし，多くの spammer はマルウェア感染した PC で構成されたボットネットから送信を行うが，マルウェアプログラムが MX フォールバックをサポートすることは，マルウェア制作者に負担を増大させ，また spam メールの配送効率を低下させると考えられる．

また，短時間に大量かつ不自然な DNS の問合せを行う挙動に注目し，bot 感染マシンを検知する手法も提案され [31][32][33]，実際に，IDS のシグネチャ等で提供されている．さらに，一つの bot 感染マシンから同じドメイン宛に spam メールを大量に送

信すれば，anti-spam 製品の自己学習により受信拒否を受ける可能性が高くなる．このため，spammer は，受信可能な MTA 全てに spam メールを送信する戦略や，ドメインあたりの宛先数を抑える代わりに多数のドメインに送信する戦略や，bot 感染マシンで MX レコードを検索させず，C&C サーバが送信先 MTA の IP アドレスを直接指示する戦略等をとることがある．

従って，RFC に意図的に従わない現在の送信手順を使う spammer は当面の間残り続けると想定している．このような spam 送信ホストの振舞いは，spam 送信ホストが正確なメール配送よりも，できるだけ多くの spam メールをばら撒くことを優先しているためであると推測される．

4.5 まとめ

本章では，送信ホスト再送動作を効率的に検出する spam 送信ホスト検出手法を提案した．本手法は，tempfailing で発生する配送の遅延や，Nolisting の判別精度の低さ，また Unlisting の非柔軟性等，従来の手法の様々な弱点を克服することができた．また，一時および恒久ホワイトリストと一時ブラックリストを上手く使用することで，本手法の実現可能性を示した．

さらに，提案手法の作業負荷は商用製品よりも軽量であることから，本システムはエンタプライズ環境で使用することが可能である．本手法は TCP のメカニズム（レイヤ 3）をベースにしているため，例えば 400 番台エラーの応答等，高レイヤで動作する他の spam 対策手法の前段に設置して使用することができる．

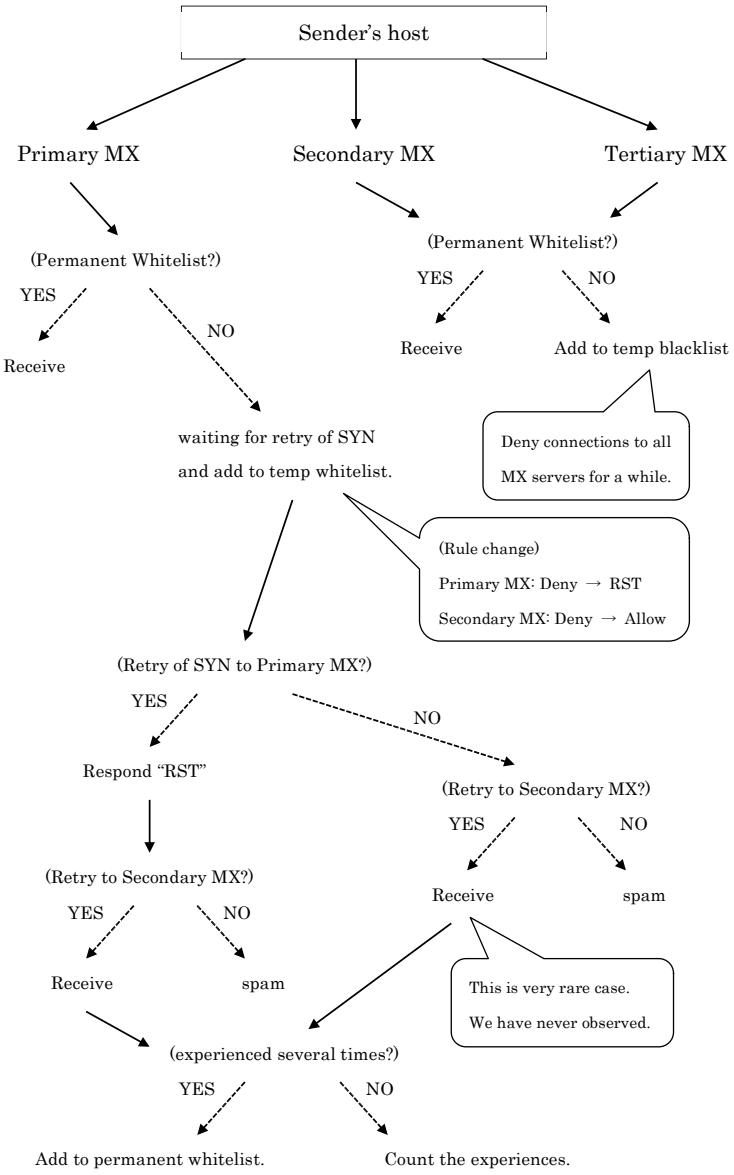

図 4.3: 本手法のフローチャート

第5章

通信挙動の特異性を利用したspam送信ホスト検出手法

4章では，3章で得た知見に基づき，2章で述べた従来手法の諸問題を解決するMXフォールバックのリアルタイム検出手法について述べた．本章では，その改良として，DNSプロトコル違反を検出することにより判定性能を向上させる手法について述べる．

5.1 まえがき

2章で述べたように，電子メール受信時に，送信ホストの挙動によってspamメールの配送を判別する手法がいくつか存在する．その代表的な手法であるTempfailingは，送信ホストのSMTPセッション時における再送ポリシの特徴を利用したspam対策手法であり，その効果は高いものの，メール配送に長時間の遅延が発生する欠点がある．この欠点を解決する手法として，Nolisting[21]やその改良であるUnlisting[22]等，5-Way Handshakeと呼ばれるTCPセッション時の再送を検出する手法があり，4章ではこれらの手法の判別精度や実用性を高めたMXフォールバック検出手法を提案した．この手法はUnlistingと比較して高負荷時の対応や受信の可否の判断等の柔軟な対応を行うことができるが，送信ホストがMXレコードの優先度順に送信を行うかのみを検査する点は同一であるため，spam送信ホスト検出精度の大幅な向上は期待できない．さらに今後精巧なspam送信プログラムが増加することが懸念されることから，これまでに提案したMXフォールバック検査に加え，通信時の挙動を様々な視点から監視することにより，更なるspam送信ホスト検出精度の向上が期待されている．

本研究では，MX フォールバック検出の精度を向上させる手法として，以下の機能拡張を行った．

- 特殊な DNS コンテンツサーバによる，MX レコードのリストを定期的に変化させた応答
- 送信ホストによって参照される DNS キャッシュサーバが MX レコードの TTL を遵守し，かつ，送信ホストが正しく MX サーバを選択するかを確認する検査

また，本システムを spam 収集ドメインで実際に動作させ，spam 送信ホストの検出性能の評価を行った．その結果，本手法は，高速かつ低負荷に spam 判定を行える MX フォールバック検出手法の大きなメリットを維持しつつ，機能拡張により判定性能をさらに高められることを確認した．

4 章までに述べた MX フォールバック手法は，Unlisting と比較して高負荷時の対応や受信の可否の判断等の柔軟な対応を行うことができるが，送信ホストが MX レコードの優先度順に送信を行うかどうかのみを検査する点は同一であるため，spam 送信ホスト検出精度の大幅な向上は期待できない．

一般的な spam 対策システムの運用は，単一手法によって実施するのではなく，複数の手法を組み合わせて判別精度や信頼性の向上を図る．これまでに挙げた手法は，メール本体を受信する前に，送信ホストの通信挙動の特徴に基づき spam の配送か否かを判断するものであり，本体受信後に spam 判定を行うコンテンツフィルタリング技法 [38][10] の前段に設置することが想定される．

5.2 MX フォールバック検査拡張時の課題

今後増加が懸念される精巧な spam 送信プログラムへの対策として，送信ホストの挙動を様々な視点から監視し，spam 送信ホスト検出精度を向上させる必要がある．本章では，MX フォールバック検出手法を強化するため，MX レコードの優先度に加え，送信ホストが MX レコード情報を適切に処理するかという別の視点に基づいて spam 送信ホストを検出する検査を併せて行う手法を提案する．

3 章の研究で行った調査で示したとおり，spam 送信プログラムの挙動は正当な送信ホストとは異なり，DNS 問い合わせや名前情報の処理を正しく行わない特徴的な挙動

を示すことが多い．さらに，MX レコードの優先度を参照しないホストが大多数であることを鑑みると，DNS コンテンツサーバが優先度の低い多数の MX レコードを囮として応答すれば，各 MX サーバに当て推量で再送を行う spam 送信ホストが正しい優先度順で偶然に送信を試みる確率を下げられ，MX フォールバック検出手法の検出精度の向上が期待できる．

しかし，1 回の DNS 応答で多数の MX レコードを応答した場合，パケットサイズが増大し，DNS メッセージの最大長である 512 バイトを超過することも考えられる．TCP フォールバックや Extension Mechanisms for DNS (EDNS0)[49] のように，大きなサイズの DNS 通信に対応するための手段は存在するが，次に挙げる問題があるため，安易に DNS 応答サイズを巨大化することは避けるべきである．

TCP フォールバックは DNS 応答に TCP を使用する方法だが，RFC1123[50] で定められている通り，必ず UDP による通信の後で TCP 通信に切り替えるため，名前解決に時間を要する点や，TCP 通信ではコネクションの確立が必須となるため，UDP と比較してサーバ側，クライアント側ともにそのためのリソースが増大する点が問題点として挙げられ，多くの問い合わせや応答を処理する DNS に使用するプロトコルに適合しているとは言い難い．

また，EDNS0 は DNS の拡張プロトコルであり，512 バイトよりも大きなサイズの DNS 応答パケットが UDP によって送信される．しかし，一部のルータやファイアウォール等のネットワーク機器はこれに対応しておらず，誤動作や名前解決エラー等が発生する恐れがある．

これらの問題点に加え，その DNS 応答パケットサイズが問い合わせ時のパケットサイズと比較して十分な増幅が得られると攻撃者に判断された場合，DNS コンテンツサーバであっても DNS amp 攻撃の踏み台として使用される可能性がある．

以上の点を踏まえ，本手法は検出精度向上を目的として多数の MX レコードを応答するのではなく，応答する MX レコードを定期的に切り替える手法を採る．この方法は，送信ホストが MX レコードの TTL 値に従って適切にキャッシュ情報を破棄し，正しい宛先 MX サーバを選択するかを検査するものである．RFC1123 によれば，DNS リゾルバには問い合わせ結果の情報をローカルキャッシュする機能を実装することと，TTL 値で指定された時間経過後にその情報を破棄することが定められている．

また，spammer が複数のドメイン宛に spam を送信する際に MX レコードの大量問い合わせを行うと，その挙動に基づく bot 発見手法 [51] によって IDS 等で検知されてしまうことになる．この検知を回避するために，bot 感染機器では，DNS 問い合わせをさせなかったり，TTL に従った適切なキャッシュ情報の管理を行わないことが観測されている．

本章ではこれらの点に注目し，メール送信ホストが MX レコード情報の問い合わせに使用する DNS キャッシュサーバが，TTL 値に従って MX レコード情報を適切に破棄する機構を有するかを識別し，それに続いて MX フォールバック検査を実施する手法を提案する．

5.3 通信挙動検査による spam 送信ホスト判別手法

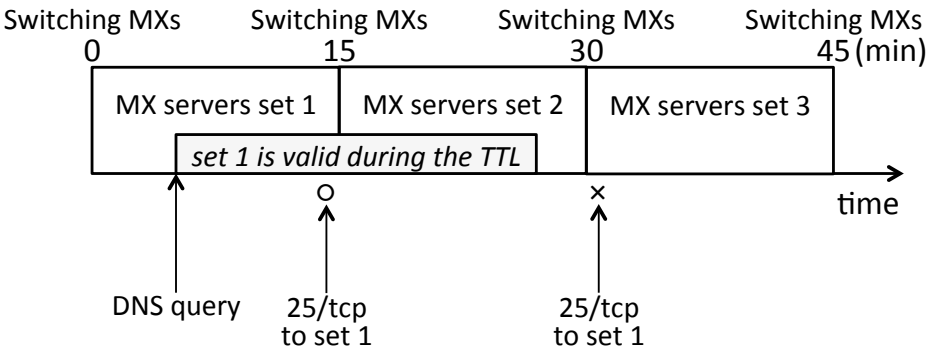

図 5.1: TTL に基づいた受信可否判定の概要

図 5.1 に MX レコードを 15 分間隔で切り替える例を示す．送信ホストが使用する DNS リゾルバからの DNS 問い合わせに対し，DNS コンテンツサーバが MX レコード情報として MX サーバセット 1 を応答する．当該 MX レコードは，この応答を行った時点から TTL の期間だけ有効となる．つまり，図 5.1 において MX サーバセット 1 が選択されている期間であっても，DNS 問い合わせが行われるまでは有効とはならない．また，次の切り替えでは，MX サーバセット 2 を選択する．なお，図 5.1 に示すように，切り替え間隔と TTL を同じ値にする必要はない．切り替え間隔と TTL の関連については，5.4.1 節で後述する．

図 5.2 に本手法の概観を示す．この例では，DNS コンテンツサーバ（第 4 オクテッ

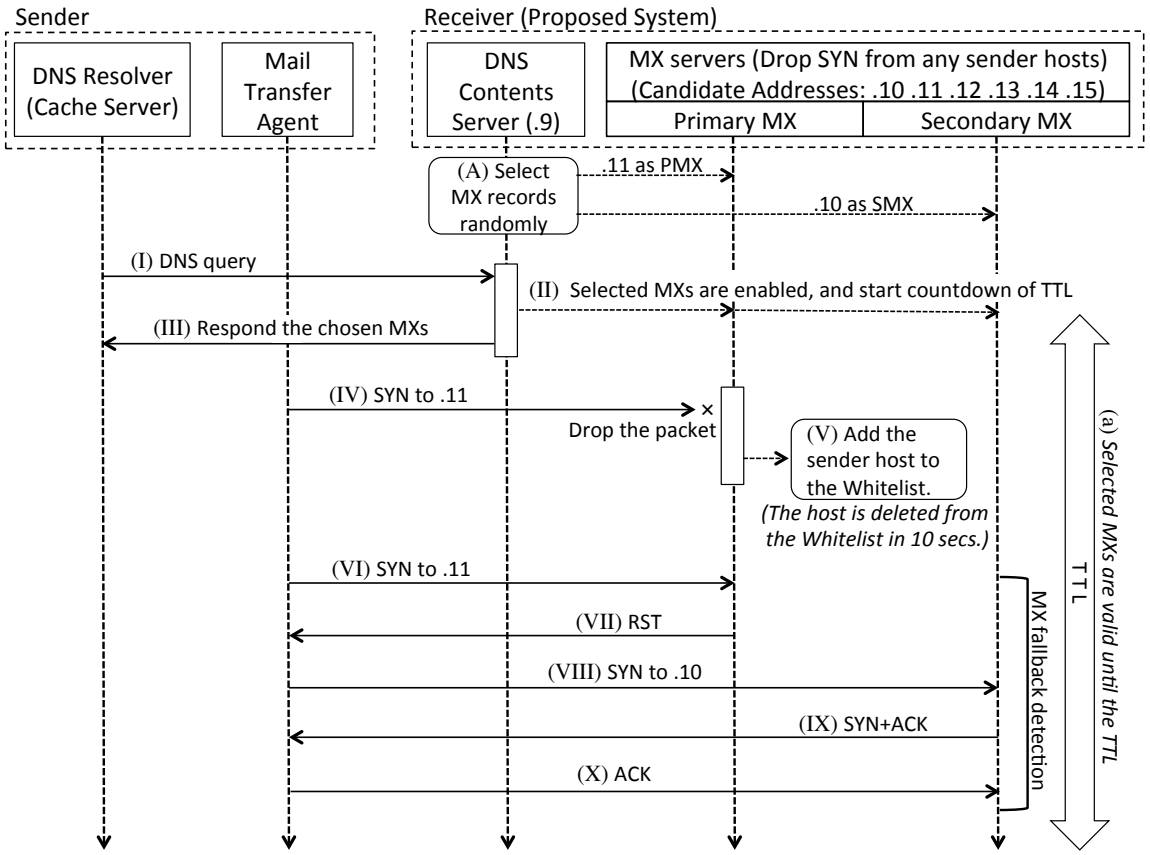

図 5.2: 提案システムの概観

トが.9）が MX レコードの候補となる 6 つの IP アドレス（第 4 オクテットが.10 ～ .15）からプリファレンス値の異なる 2 つの MX レコードとして，プライマリ MX に “.11” を，セカンダリ MX に “.10” を選択した場合を示す (A)．はじめに，送信側の DNS リゾルバはメール送信ホストからの MX レコード情報の問合せを受けると，当該情報がキャッシュされていなければ，名前解決のためにメール送信前に DNS 問い合わせを行う (I)．これを観測すると，この状態において選択されている MX サーバが有効化され (II)，その MX レコード情報を応答する (III)．DNS 問い合わせ観測時に有効となった MX サーバは，(III) で応答した時刻から MX レコード情報の TTL で指定した時刻までが有効であり，これを経過すると無効となる (a)．

DNS 問い合わせ観測後，(III) で応答した MX サーバが有効である間に，送信ホストからの配送が MX レコードの優先度順に行われた場合，以下の手順で送信ホストを処

理する．

(IV) プライマリ MX(.11) では，送信ホストからの最初の SYN パケットを観測する．以降は我々が提案した従来手法（2 節）と同じ手順を実施する．

(V) 当該送信ホストを一時ホワイトリストに登録する．

(VI) 主要 OS が複数回にわたって SYN パケットを再送する機構に基づき，送信ホストはプライマリ MX に SYN パケットを再送する．

(VII) 一時ホワイトリストに登録された送信ホストからの再送 SYN パケットに対し，プライマリ MX は RST を応答する．

(VIII) プライマリ MX からの RST を受信した送信ホストは，MX フォールバックにより，セカンダリ MX(.10) に SYN パケットを送信する．

(IX) セカンダリ MX は SYN+ACK を応答する．

(X) 送信ホストは ACK を応答し，TCP 接続が確立する．以降，送信ホストとセカンダリ MX の間で SMTP 接続が行われる．

実際には，DNS 問い合わせを行うホストとメール送信を行うホストの各 IP アドレスの間に相関は期待できないため，どの DNS 問い合わせがどのメール配送と対応しているかを判断することは不可能である．従って，MX レコード情報は，送信ホスト毎に有効期限を定めるのではなく，選択された期間内において，最初の DNS 問合せの観測時刻から，最後に観測された DNS 問合せ時刻に TTL を加えた間まで有効と判断する．

本手法では，上記の手順により，以下の挙動を示す送信ホストによるメール配送のみを受け付ける．

- MX レコード情報が有効な期間内に（図 5.2(a)），
- MX レコード情報のプリファレンス値に従ってプライマリ MX への接続を試み (IV)，
- MX フォールバックによりセカンダリ MX への接続を行う (VI ∼ X)．

一方，これ以外の挙動を示す送信ホストに対しては，spam 送信ホストと判断し接続を許可しない．本システムにおいて，spam 送信ホストと判別される例を図 5.3 に示す．

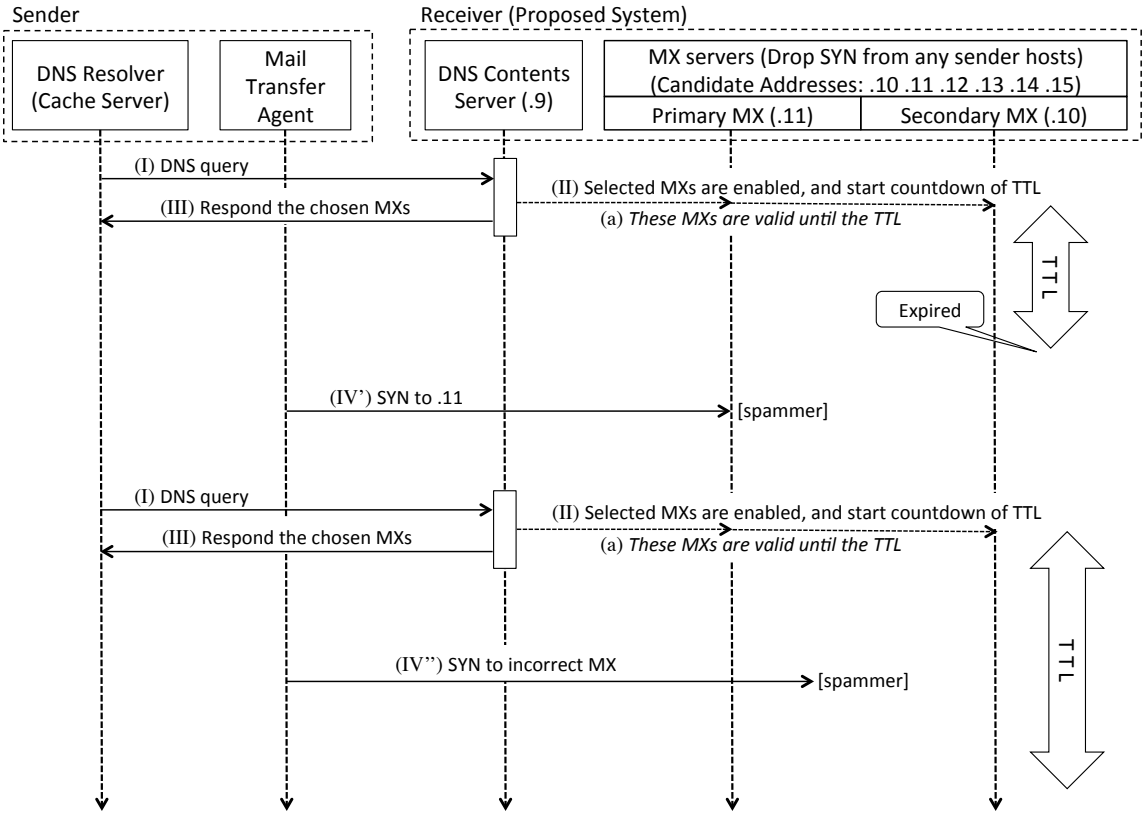

図 5.3: spam 送信ホストの検出例

図 5.3 の (IV') は，MX レコードの問い合わせから TTL が経過し，送信ホストが無効となった MX サーバに対して配送を試み，本システムで spam 送信ホストと判断した例を示す．また，MX レコードの問い合わせが観測されなかった場合もこの例と同様に，全ての MX サーバが無効であるため，spam 送信ホストと判断する．図 5.3 の (IV'') は，MX レコード情報の問い合わせ観測によって有効となっている MX サーバが存在する状態において，送信ホストがプリファレンス値に従った配送を行わない場合や，無効となっている MX サーバに対して接続を試みて spam 送信ホストと判断された例を示す．これらに加えて，従来の MX フォールバック検査と同様に，MX フォールバックによりセカンダリ MX への再送 (図 5.2(VIII)) を行わない場合には spam 送信ホストと判断する．

なお，本手法においては，MX レコード情報の連続する切り替えにおいて，同一の IP アドレスを含めてしまった場合，どちらの MX サーバセットに基づく配送なのかを判断することができない．また，TTL の設定を切り替えの間隔よりも長く設定すると，レコード情報の有効期間が跨がる MX サーバセットの増加を招いてしまい，同様の問題を生じることになる．この問題の対応については，具体的な実装例を示しながら 5.4.1 節で議論する．

5.4 実装法

本システムの実装は一定の周期で応答する MX レコードを入れ替える定期動作系と，DNS 問い合わせおよび TCP セッション時のパケットを監視し，それに応じた処理を行うパケット監視系によって構成する．本章で述べるシステムの実装例では，1 台の FreeBSD 上に DNS コンテンツサーバと MTA を動作させ，パケットフィルタリング（ipfw）により接続制御とログ取得を行い，そのログを監視して様々な制御を行う．また，我々がこれまでに提案した MX フォールバック検出手法と同様に一時ブラックリストの実装等の拡張性を維持するため，設置が必須ではない 3 番優先度のターシャリ MX も設置する実装例を述べる．

5.4.1 定期動作系

5.3 節で示した，MX レコード情報の切り替えにおいて同一の IP アドレスが連続して含まれる場合に生じる問題を回避するため，MX レコードの候補となる IP アドレスのグループ分けを行う．MX レコードの候補となる n 個の IP アドレスをグループ A，グループ B にそれぞれ $n/2$ アドレスずつ割り当てる．各グループから MX フォールバック検査に用いるプライマリ MX，セカンダリ MX，ターシャリ MX の 3 個の IP アドレスを選択するため，その組み合わせは ${}_{n/2}P_3 \times 2$ 通りとなる．これら 3 個の IP アドレスを MX レコードとし，それらに異なるプリファレンスを割り当ててプライマリ MX，セカンダリ MX，ターシャリ MX とする．

DNS 応答情報を更新する時間間隔を T とし，k を時区間番号 (任意の自然数) としたときの時区間 $[(k-1)\cdot T, k\cdot T)$ において，k が奇数のときグループ A から，k が偶数

のときグループBから構成されるゾーンをランダムに選択して応答する．

以降は，実装の具体例として，MXレコードの候補となるIPアドレス数$n = 6$，DNS応答情報の更新間隔$T = 900$秒，応答するMXレコードのTTL値を900秒とした場合について述べる．MXレコードの候補となる6つのIPアドレスの第4オクテットを“.10”～“.15”としたとき，本例では“.10”，“.11”，“.12”をグループA，“.13”，“.14”，“.15”をグループBとしてグループ分けを行う．この例では各グループはそれぞれ3アドレスずつであることから，プライマリ，セカンダリ，ターシャリMXの組み合わせは${}_3P_3 \times 2 = 12$通りとなり，表5.1のような組合せになる．なお，表5.1中ではプライマリMXを“PMX”，セカンダリMXを“SMX”，ターシャリMXを“TMX”と表記した．

表5.1: 各ゾーンファイルのMXレコード一覧

MXレコード候補となるIPアドレス .10, .11, .12, .13, .14, .15							
グループA				グループB			
zone	PMX	SMX	TMX	zone	PMX	SMX	TMX
a1	.10	.11	.12	b1	.13	.14	.15
a2	.10	.12	.11	b2	.13	.15	.14
a3	.11	.10	.12	b3	.14	.13	.15
a4	.11	.12	.10	b4	.14	.15	.13
a5	.12	.10	.11	b5	.15	.13	.14
a6	.12	.11	.10	b6	.15	.14	.13

図5.4に，例として9時台に応答するMXレコード情報の切り替え周期とMXレコードのTTL値の関係を示す．毎時0分，30分にグループAに属するIPアドレスからなるa[1-6]の6個のゾーン候補から一つを選択し，毎時15分，45分にグループBに属するIPアドレスからなるb[1-6]の6個のゾーン候補から一つ選択する．これにより，毎時0分から15分および30分から45分の間のDNS問い合わせにはグループAから，毎時15分から30分および45分から60分の間のDNS問い合わせにはグループBから構成されるMXレコードを応答する．

図5.4中の(A)は，4節で述べた，TTLをMXレコード情報切り替え間隔より長く

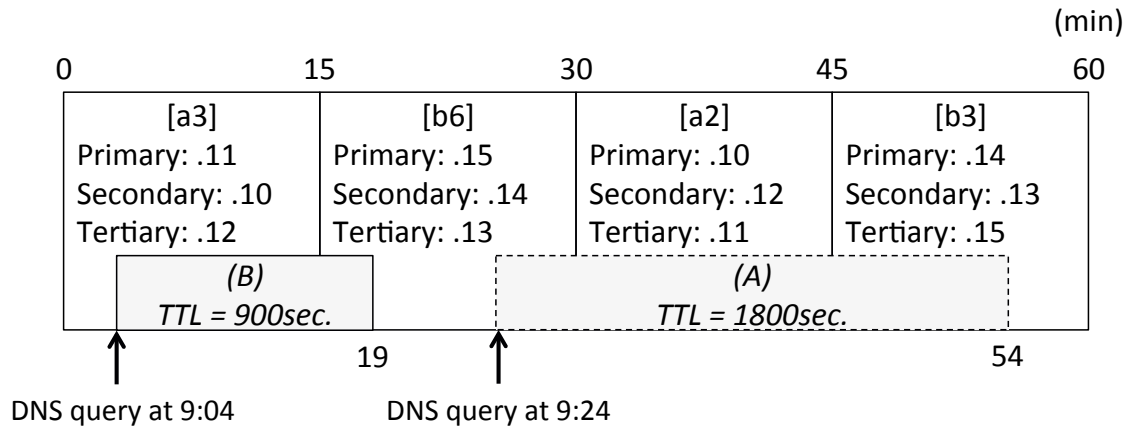

図 5.4: DNS 応答の更新間隔と TTL 値の関係

設定した場合に問題が生じる一例として，TTL を MX レコードの切り替え周期である 900 秒よりも長い 1,800 秒とした場合を示す．DNS リゾルバからの DNS 問い合わせを 9 時 24 分に観測した場合，“b6” の MX レコードは 1,800 秒後の同 54 分まで有効となる．この間，同 30 分と 45 分の 2 度にわたって応答する MX レコード情報が更新されているため，グループ B から選択された “b6” と “b3” の MX レコードが同時に有効となる期間が発生する．その結果，“b6” に基づけばプライマリ MX である “.15” は，同時に “b3” ではターシャリ MX として有効になるため，送信ホストが “.15” に接続試行を行ったとしても，どちらの情報に基づくものなのか，即ち，プリファレンス値に従ったものなのか，無視したものなのかを判別することは不可能となる．従って，TTL 値で示す MX レコードの有効期間の長さは，応答する MX レコードの更新間隔（T）以下に設定し，当該グループが次に選ばれる前までに無効となる必要がある．

図 5.4 中の (B) は，TTL 値を応答する MX レコードの切り替え周期と同じ 900 秒とした場合の例を示す．DNS リゾルバからの DNS 問い合わせを 9 時 4 分に観測した場合，“a3” の MX レコードは 900 秒後の同 19 分まで有効となる．同 15 分に DNS 応答情報が更新されているため，同 15 分から 19 分までの間に DNS 問い合わせを観測した場合，“a3” と “b6” の MX レコードが共に有効となるが，グループ A とグループ B を交互に選択することにより，4 節で述べた MX レコード情報の連続した切り替えにおいて同一の IP アドレスを含めた場合に生じる問題を回避でき，正常に検査を実施することができる．

また，本システムではMXフォールバック検査のために一時ホワイトリストを用いるが，以下に述べる状況を想定しなければならない．前述の “a3” と “b6” の例のように，複数のMXサーバリストが共に有効となる期間が存在する．この期間中にspam送信者が例えば近隣IPアドレスに総当たり的に配送を試みたり，複数回のDNS問い合わせをすれば，グループA，グループB両方のMXレコード情報を所持することが起こり得る．

その場合，spam送信者がその中から無作為に選択して送信を試みれば，“.11→.14” あるいは “.15→.10” という順序，即ち各グループを跨ぐものの，“プライマリMX→セカンダリMX” という順序となってしまう．もし，一時ホワイトリストを各グループで共有した場合，この跨ぎを識別できず，False Negativeが生じる．従って，一時ホワイトリストはそれぞれのグループに個別に割り当てる必要がある．

5.4.2 パケット監視系

DNS問い合わせパケットおよびその後のTCP接続時のSYNパケットを監視し，状況に応じた処理を行う．本章では，一時ホワイトリストを，大量アドレスの登録や削除が容易なipfwの検索表tableを用いる．ipfwのtableは，最大128個の異なる検索表を持つことができる．本システムでは5.1節で述べたように各グループ毎に別々の一時ホワイトリストが必要であるため，これらをtable(1)とtable(2)の2つの検索表を用いて実装する．

表5.2に，待機中のipfwのルール例を示す．なお，ipfwではルール番号の昇順にマッチングを行うため，一時ホワイトリストで用いるルール番号の順番に配慮する必要がある．

表 5.2: 待機中のipfwのルール例

100 allow log udp from any to .9 dst-port 53
900 deny tcp from any to any dst-port 25 setup

前節と同様に，図5.4を例として考える．待機状態では，表5.2に示すとおり，DNS問い合わせに対する応答は行うが，各MXレコード候補IPアドレスへのSYNパケッ

トを棄却する．

表 5.2 のルール番号 100 で出力される DNS コンテンツサーバへの DNS 問い合わせ時のログを観測した際，その問い合わせが MX レコード情報切り替え後の初回の問い合わせか，あるいは 2 回目以降の問い合わせかにより，異なる処理を行う．

図 5.4 のサーバセット “a3” の例では，9 時 0 分から同 15 分の間に，プライマリ MX，セカンダリ MX，ターシャリ MX としてそれぞれ “.11”，“.10”，“.12” が選択されている．この選択の後，同 4 分に 1 回目の DNS 問い合わせを観測（図 5.2(I)）したとすると，DNS コンテンツサーバは上記の MX レコード情報の応答（図 5.2(III)）を行い，それと同時にルール番号 100 によってログが出力される．これを観測すると，表 5.3 に示すように MX サーバセットに含まれる 3 台の MX サーバに関するルール（表 5.3 の太字部分）を追加し，これらの MX サーバを有効化する（図 5.2(II)）．

表 5.3: グループ A 選択時に追加される ipfw のルール例

100 allow log udp from any to .9 dst-port 53
300 reset tcp from table(1) to PMX dst-port 25 setup
350 deny log tcp from any to PMX dst-port 25 setup
400 allow tcp from table(1) to SMX dst-port 25 setup
500 deny log tcp from any to TMX dst-port 25 setup
900 deny tcp from any to any dst-port 25 setup

有効化された MX サーバでは，送信ホストからの配送を次のように処理する．このときプライマリ MX である “.11” に対して 1 度目の SYN パケットが送信されると，ルール番号 350 によりそれを棄却し，ログを出力する（図 5.2(IV)）．これを観測すると，当該送信ホストをグループ A から構成される MX サーバ用の一時ホワイトリスト（table(1)）に登録する（図 5.2(V)）．これに続いて table(1) に登録された送信ホストから，プライマリ MX である “.11” に SYN パケットが再送されると（図 5.2(VI)），ルール番号 300 により RST パケットで応答する（図 5.2(VII)）．MX フォールバックによりセカンダリ MX である “.10” に再送が行われると（図 5.2(VIII)），ルール番号 400 により TCP Handshake が確立され，SMTP セッションを開始する．また，表 5.3 のルールは，DNS 問い合わせから TTL 値で指定した 900 秒後の 9 時 19 分まで有効であ

り，これ以降は削除され，無効となる（図 5.2(a)，図 5.4(B)）．

一方，9 時 12 分に DNS 問い合わせを観測した場合，MX レコード情報切り替え後 2 回目の問い合わせとなるため，初回の問い合わせとは異なる処理を行う．既に当該 MX サーバに対応した表 5.3 のルールは追加されているため，このルールを削除するまでの時間をリセットし，この DNS 問い合わせから 900 秒後の 9 時 27 分にルールを削除するように変更する．また，DNS 問い合わせに続くメール配送に対しては，前述の例と同様に処理する．

その後，9 時 15 分の更新により MX サーバセット “b6” が選択され，同 16 分に更新後初の DNS 問い合わせを観測したとする．前述の通り，更新前に使用していたグループ A に対応するルール（表 5.3）には関与せず，グループ B のために新たなルール（表 5.4 の太字部分）を追加する．

表 5.4: グループ B 選択時に追加される ipfw のルール例

100 allow log udp from any to .9 dst-port 53
600 reset tcp from table(2) to PMX dst-port 25 setup
650 deny log tcp from any to PMX dst-port 25 setup
700 allow tcp from table(2) to SMX dst-port 25 setup
800 deny log tcp from any to TMX dst-port 25 setup
900 deny tcp from any to any dst-port 25 setup

表 5.4 の table(2) はグループ B から構成される MX サーバ用の一時ホワイトリストを示しており，table(1) の例と同様に，プライマリ MX として選択されている “.15” への接続試行観測時に一時ホワイトリスト（table(2)）に当該送信ホストを登録し，MX フォールバック検査を実施する．

なお，一時ホワイトリストの保持時間は 3 章で述べた MX フォールバック検出実験で 5~20 秒の間の任意の時間であれば妥当との結果を得ていることから，10 秒間とした．

表 5.4 のルールは新たな DNS 問い合わせが無ければ，31 分に削除される．なお，表 5.3 のルールは同 27 分まで有効であるため，表 5.3，5.4 のルールは 16 分から 27 分まで同時に存在することになる．

ルール番号 500（表 5.3）およびルール番号 800（表 5.4）は，前述した本手法の拡張

のために，ターシャリ MX への接続試行を観測するものである．送信ホストが MX レコードの優先度順にメールを配送するのであれば，この接続試行は行われない．これを観測した際に当該送信ホストを一時ブラックリストに登録し，全ての MX サーバにおいて接続を拒否することで，spammer による総当たり送信が偶然 “ターシャリ MX→プライマリ MX→ セカンダリ MX” のような順序となった場合でも，False Negative を回避できることになり，精度向上が期待できる．

一時ブラックリストを実装する場合には，新たに検索表 “table(3)” を設け，前述したルール番号 500 または 800 を観測した際に当該送信ホストを一定期間登録する．一時ブラックリストを構成する検索表は，一時ホワイトリストの場合とは異なり，spam 送信ホストを登録する目的であることから，各グループで 1 つの table を共有する必要がある．また，一時ブラックリスト “table(3)” を参照し，各 MX サーバへの接続を拒否するルールは，表 5.2，5.3，5.4 の何れのルールよりも先に評価されるようにする必要があるため，本稿の例ではルール番号を 100 未満とする必要がある．

5.5 評価

本節では，これまでに述べたシステムに対して，正当な送信ホストが問題なく配送できることを確認した上で，spam 送信ホストの検出効果について検証する．なお，本節で述べる評価では提案手法の効果を確認するために，前節で述べた一時ブラックリストの運用は対象外とした．

5.5.1 正当な送信ホストからの配送

正当な送信ホストからのメール配送で，本システムで False Positive となるのは，送信ホストが使用する DNS キャッシュサーバが指定された TTL 期間を超えて MX レコード情報のキャッシュを保持する場合と，MX フォールバックを行わない場合である．本節では，正当な送信ホストの使用する DNS キャッシュサーバが TTL に従って適切に MX レコード情報のキャッシュを破棄するかを確認するため，3 章で述べた MX フォールバックの実験に使用したものと同じ 22 ドメインを用いて配送実験を行った．

送信ホストの使用する DNS キャッシュサーバが指定された TTL に基づいた適切な

キャッシュ管理機構を有するか検査するため，次の 3 ステップの配送実験を実施した．

(1) 各送信ドメインから 1 回目のメールを送信する．このとき，送信ホストの使用する DNS キャッシュサーバには本システムのどの MX レコード情報もキャッシュされていない状態である．

(2) (1) で本システムの DNS コンテンツサーバが応答した MX レコード情報が無効となった後（TTL が経過した後）に，各送信ドメインからメールを送信する．

(3) (2) で本システムの DNS コンテンツサーバが応答した MX レコード情報が有効である間（TTL が有効である間）に，各送信ドメインからメールを送信する．

この結果，(1) はどの送信ドメインからの配送も MX レコード情報の問い合わせ後，応答した MX レコードの優先度順に配送を行い，正常に受信した．なお，MX レコード情報の問い合わせからプライマリ MX への最初の SYN パケットの送信までに要する時間が最も長い送信ドメインで 2 秒だった．

(2) は，MX レコードが無効となった後の配送であるため，(1) と同様に MX レコード情報の問い合わせが必須となるが，全ての送信ドメインから MX レコードの問い合わせを観測し，MX フォールバック検査を経て正常に受信した．

(3) は，MX レコードが有効である期間であるため，MX レコード情報の問い合わせは必要ないはずであるが，22 ドメイン中 11 ドメインは (2) の挙動と同様に，TTL が有効な期間であっても MX レコードの問い合わせを行った．

本システムで False Positive となるのは TTL の有効期間を超えてキャッシュを保持し続ける場合，すなわち (2) で MX レコードの問い合わせを行わない送信ドメインが存在する場合であるため，実験を行ったいずれのドメインにおいても配送に問題は生じないことを確認した．また，ISP の提供する DNS キャッシュサーバの調査 [29] においても，TTL が有効な期間を超えてキャッシュを保持し続けるサーバは確認されていない．

5.5.2 spam 送信ホストからの配送

spam 収集を目的として 2006 年 10 月より筆者らが運営しているドメインで提案システムを動作させ，spam 送信ホスト検出性能の評価を行った．本システムは 2013 年 5

月 30 日に導入し，同年 4 月 1 日から 5 月 29 日までの期間を導入前，5 月 31 日から 7 月 8 日までの期間を導入後とする．なお，5.5.3 節で述べるポートスキャンに伴うオープンリレーの試行による影響を抑えるため，本システムで使用する DNS コンテンツサーバおよび MTA は，導入前に使用していた旧 MTA とは異なる /24 アドレスブロックに設置した．導入後，旧 MTA は MX レコード情報には含まれないが，MX レコードの問い合わせを伴わずに送信する spam 配送の観測を目的とし，当該ドメイン宛のメールを受信し続けるようにした．

当該ドメインに実ユーザは存在せず，大量の spam 収集用のメールアドレスを Web 等に公開することにより，spam 発信業者に収集させている．導入前には，1 日平均およそ 33,000 セッションにおよぶ SMTP セッションを観測するようになっている．従って，このドメインへの誤送信等によって正当なメールが含まれる可能性は排除できないが，その可能性は極めて低く，また含まれていた場合でもその数はごくわずかであるため，性能評価には影響しないと判断し，本ドメインに送られたメールを spam メールであるものとした．

表 5.5: 各セッションで送信されたメールの特徴

	導入前	導入後
日本語で記述されたメールを送信	1,696,935 (87.3%)	33,602 (92.2%)
日本語以外で記述されたメールを送信	198,061 (10.2%)	2,486 (6.8%)
接続のみで送信なし	48,557 (2.5%)	366 (1.0%)

表 5.5 は，導入前の旧 MTA，および，導入後の提案システムで観測したセッションについて，日本語で記述されたメールの送信，日本語以外で記述されたメールの送信，メール送信を伴わずに接続のみを行うものの割合を示している．本 spam 収集ドメインは AC.JP ドメインであるが，表 5.5 に示すように，受信するメールは日本語で記述されているものが導入前で 87.3%，導入後で 92.2%を占めており，日本の法人や個人をターゲットにした spam が大多数であった．なお，Subject:の文字コードが Shift_JIS

またはISO-2022-JPで記述されていたものを日本語で記述されたメールであると判断した．また，表5.5の最下段に示すものは，オープンリレーの要求を拒絶され，メール本文の送信に至らなかったものと，SMTP Authへのbrute force攻撃を行ったもののいずれかであり，導入前で2.5%，導入後で1.0%を占めていた．

5.5.3 spam送信ホスト検出効果

本観測環境における観測期間全体（4月1日から7月8日）のSMTPセッション数の推移を図5.5に示し，本システム導入後（5月31日から7月8日）の部分を抽出したのものを図5.6に示す．

本システム導入前に旧MTAで観測したSMTPセッションは一日あたり平均32,941セッションだった．一方で，導入後では一日あたり平均1,087セッションとなり，これらを直接比較することはできないが，導入前後で約96.7%のspam配送セッションの削減を確認した．以上の結果より，多くのspam送信ホストがMXフォールバックを行わないこと，TTL値に従って適切にMXレコード情報を破棄する運用を行わないことが確認された．

本システム導入後に旧MTAはMXレコードの応答に含まれていないにも関わらず，接続を試みるホストが僅かに観測された．これらの配送は，前述したSMTP認証の試行観測の結果から，旧MTAを示す古いMXレコード情報を記憶していたのではなく，ポートスキャン等によってMTAの存在を発見し，オープンリレー等を試みたものであると考えられる．

また，本システム導入後の旧MTAへの配送は，6月7日の一日のみ5,123セッションを観測したが，これ以外の日では少数で推移している．この5,123セッションのうち5,113セッションは，1ホストからのSMTP認証（AUTH-LOGIN）の試行観測のみであり，実際のメール送信は行われなかった．この挙動は，表5.5の最下段の項目に相当する．導入前の旧MTAで2.5%，導入後の本システムで1.0%となっていることから分かるように，このようなspam送信ホストの挙動を観測する割合は極めて低く，6月7日の事象は特異なものであったと言える．

表5.6は，本システム導入前に受信したspamと，導入後にFalse Negativeとなり受信したspamの統計情報を示す．導入前後のいずれの観測でも，1セッションで複数

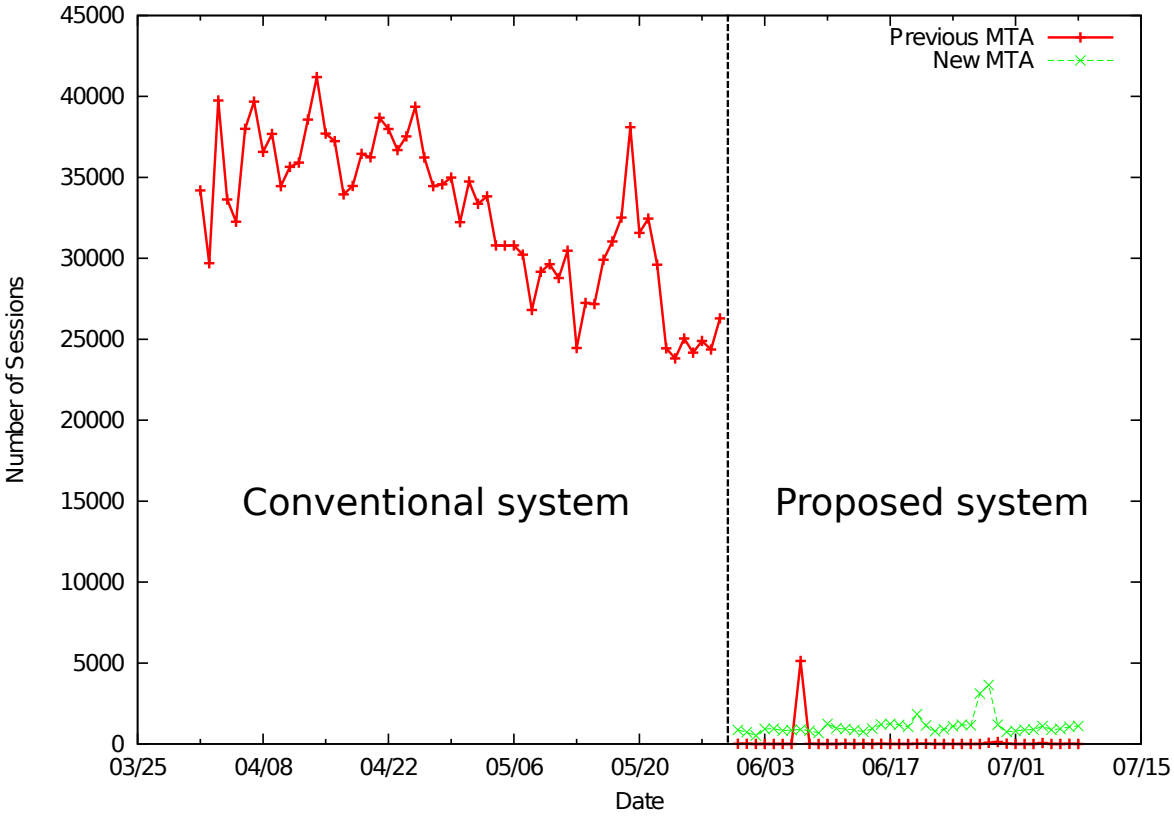

図 5.5: 実験期間に観測した SMTP セッション数の推移

件のメールを送信する挙動が多く観測された[1]．表 5.6(3) で示す 1 セッションあたりのメール件数の平均値は導入前後でそれほど大きな差は見られないが，(4) に示す分散に大きな違いが見られ，1 セッションで大量件数のメールを送信するホストの割合が増大した．この特徴については 5.5.5 節で考察する．

5.5.4 MX レコード情報の定期変更による効果

4 章で述べた MX フォールバック検出検査からの本手法の主な強化点は，過去に問い合わせた MX レコード情報を，TTL 値を無視して記憶し続けるホストの検出が可能な点である．また，5.5.3 節で述べたような DNS 問い合わせを行わず，ポートスキャン等によって MTA を発見し，その後 spam メールを送信するホストの存在を確認している．しかし，このようなホストがポートスキャンでアクセスする IP アドレスの順番

[1] 1 セッションあたりのメール件数は，SMTP セッション中に RCPT TO:で示されたメールアドレス数によって集計した．

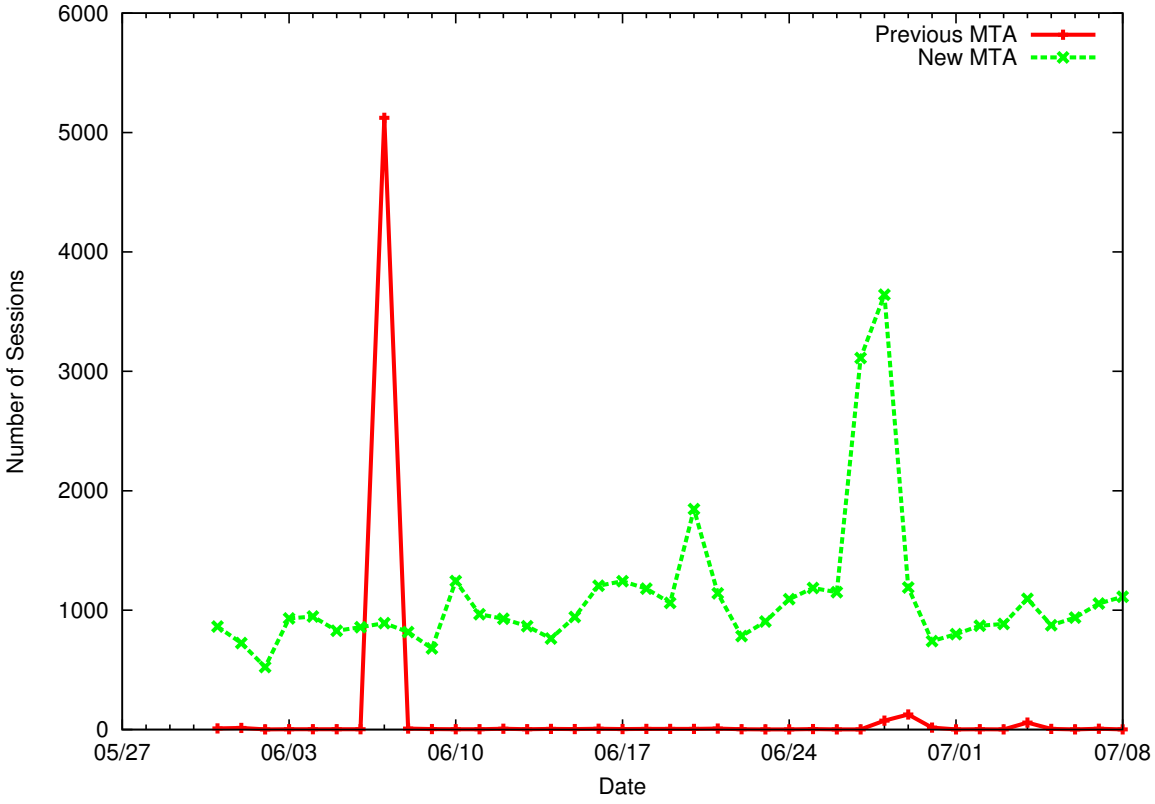

図 5.6: 導入後に観測した SMTP セッション数の推移

と，MX サーバセットのプリファレンスの順番が一致する可能性は，ランダムスキャンの場合でも 3 分の 1 と低いため，次に挙げるような効果が期待できる．

- 順番が一致しない場合，セカンダリ MX は spam 送信ホストからの SYN パケットに応答しないため，MTA の存在を察知されることはない．
- 偶然，順番が一致した場合は，セカンダリ MX の MTA の存在を察知される．しかし，TTL 経過後は別の MX サーバセットに切り替わっているため，察知された MTA ではメールを受信することはない．

上記の効果を確認するため，導入後の観測結果から，0 分から 59 分までの 1 時間分のトラフィックデータ 3 期間を無作為に抽出し，解析した結果を表 5.7 に示す．

解析の手順を，図 5.4 の (B) を例として説明する．各時刻の 0 分から 15 分の間に選ばれていた MX サーバセットの MX レコード情報が無効（19 分）となってから，30 分

表 5.6: MTA で観測した spam の統計

	導入前	導入後
(1)1 日あたりの平均セッション数	32,941	1,087
(2)1 日あたりの平均メール件数	81,151	4,696
(3)1 セッションあたりの平均メール件数	2.46	4.25
(4)(3) の分散	43.7	690.3

表 5.7: TTL 終了後の観測結果

	期間 1	期間 2	期間 3	合計
全接続試行	6,884	6,077	6,296	19,257
有効配送	24 (0.35%)	98 (1.61%)	163 (2.59%)	285 (1.48%)
期限切れ配送	65 (0.94%)	60 (0.99%)	48 (0.76%)	173 (0.90%)

後（49 分）までのトラフィックデータを調査する．なお，有効期限の調査の対象となるサーバセットが，2 回後の更新時に再度選択された場合，有効期限調査が行えないため本調査には含まれていない．以下に，表 5.7 で用いる用語を定義する．

- 全接続試行
  MX レコード情報が無効となってから 30 分後までの間に，6 台全ての MX サーバで観測した TCP 接続試行の総数

- 有効配送
  15 分から 30 分，30 分から 45 分，または，45 分から 60 分の間のそれぞれについて，その期間に選ばれていた MX サーバセットのプリファレンスに基づいて正しい優先度順に配送を行った TCP 接続の総数

- 期限切れ配送
  0 分から 15 分の間に選択されていた MX サーバセットについて，無効となってから 30 分後までの期間で，当該 MX レコード情報のプリファレンスに基づいた

正しい優先度順に配送を行った TCP 接続の総数

なお，表 5.7 の括弧書きは，それぞれ全接続試行に対する割合を示す．

4 章で述べた MX フォールバック検査は，本手法において，一つのサーバセットのみを恒久使用する場合に相当する．このため，“期限切れ配送” を判別することができず，“有効配送” として扱うことになる．すなわち，本手法では “有効配送” のみが False Negative になる一方で，従来手法では “有効配送” と “期限切れ配送” の両方が False Negative となる．このことより，実験環境が異なるため直接の比較とはならないが，表 5.7 の 3 期間の合計で考えると，本手法と従来手法において False Negative となるのは，それぞれ 285 件と 458 件となる．従って，従来手法によっても spam 送信ホストによる接続試行の約 97.6%を排除できるが，本手法による改良の結果，従来手法を擦り抜ける接続試行の約 38%を排除できることを意味している．

5.5.5 False Negative となる spam 送信ホストの特徴

表 5.6(4) において，導入前後の分散の変化から分かるように，本システムで False Negative となり，spam 送信元ではないと判断されたホストでは，1 セッションで大量件数のメールを送信するものの割合が増加した．これらのセッションの大多数の配送では，RCPT TO:は異なるユーザアカウントを指定し，MAIL FROM:は同一のメールアドレスを名乗っていた．以上より，当該ホストは MX サーバを正しく選択する正当な MTA を使用して，同一ドメインへの送信を一括して行う MTA が実装されており，僅かではあるが，一定の割合の spam 送信ホストはそのような MTA を利用しているものと推定される．

表 5.8 は導入前の旧 MTA において，表 5.9 は導入後の提案システムにおいて，SMTP 接続を確立させたセッション数とホスト数を所属国別に集計し，それぞれ上位 5 カ国を示したものである．また，合計は上位 5 カ国を含めた総数を，括弧書きは総数に対する割合を示している．

まず，日本に属するホストからの spam 配送による SMTP 接続確立について述べる．導入前は，ホスト数ベースで 16 位，セッション数ベースで 10 位であったため表 5.8 には記載されていないが，それぞれ 462 ホスト（約 1.5%），49,841 セッション（約 2.6%）

表 5.8: SMTP 接続の確立数（導入前，上位 5 カ国）

セッション数		ホスト数	
国名	#(%)	国名	#(%)
中国	590,289 (30.3%)	中国	6,386 (21.0%)
ブラジル	181,951 (9.3%)	ベトナム	2,145 (7.1%)
ロシア	122,391 (6.3%)	インド	1,957 (6.4%)
アメリカ	122,337 (6.3%)	ペルー	1,703 (5.6%)
フランス	83,424 (4.3%)	台湾	1,570 (5.2%)
合計	1,948,977	合計	30,379

しか観測されなかった．一方，導入後は 205 ホスト（約 10.8%），20,594 セッション（約 57.6%）を占めるようになり，その比率が著しく増加した．

次に，日本以外の国に属するホストからの spam 配送による SMTP 接続確立について述べる．導入前に観測した spam 送信ホスト数は 29,917 ホストで，SMTP セッション数は 1,899,136 セッションであった．一方，導入後に SMTP 接続を確立させたホスト数は 1,690 ホストで，SMTP セッション数は 14,841 セッションとなった．導入前後で観測期間が異なるため，正確な比較ではないが，ホスト数，セッション数ともに大幅に減少した．

日本以外の国に属するホストからの spam 配送では，MX レコードのプリファレンス値や TTL を無視するものが大多数を占めていた．一方，日本に属するホストでは，正しく実装された MTA と DNS キャッシュサーバを使用したものの比率が高く，導入前後で日本に属するホストの占める割合に大きな変化が見られた．

表 5.9: SMTP 接続の確立数（導入後，上位 5 カ国）

セッション数		ホスト数	
国名	#(%)	国名	#(%)
日本	20,594 (57.6%)	シンガポール	348 (18.4%)
中国	3,703 (10.4%)	中国	301 (15.9%)
アメリカ	2,415 (6.8%)	日本	205 (10.8%)
ロシア	1,332 (3.7%)	韓国	143 (7.6%)
ブラジル	1,311 (3.7%)	アメリカ	121 (6.4%)
合計	35,735	合計	1,895

5.6 考察

5.6.1 適切な TTL 値の検討

5.4.1 節で述べた通り，本手法は TTL 値を MX サーバセットの切り替え間隔以下とする必要がある．現在，実運用中の DNS コンテンツサーバでは，60 秒以下のような極端に短い TTL 値を設定しているものも若干見受けられるが，数時間程度のものが大部分を占めている．

一方，本章の実験では TTL 値を 900 秒として運用した．このような短い TTL 値では，DNS 問い合わせの頻度が高まるため，DNS コンテンツサーバの負荷が高まる点や，DNS キャッシュポイズニングの危険性が高まる点が懸念される．そこで，TTL 値の違いによる判別精度の変化や，問い合わせ頻度の増減によるサーバ負荷の変化について調査を行い，運用上の最適値を検討する必要がある．

図 5.7 は，MX レコードの有効期限が失効した直後から 30 分間（1,800 秒間）に観測した，表 5.7 の “期限切れ配送” に相当する配送の時系列推移について，表 5.7 で示した 0 分から 59 分までの 1 時間分のトラフィックデータ 3 期間に，同じ条件でさらに無作為に抽出した 2 期間分を追加した 5 サンプルを示す．5.4.1 節で述べたように，本

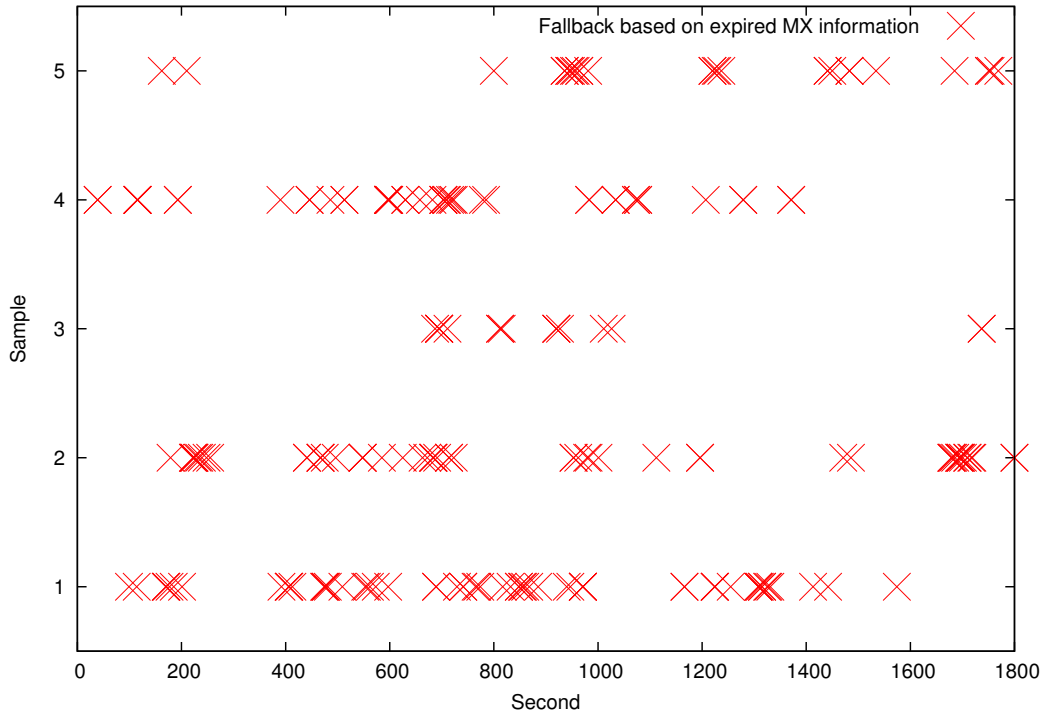

図 5.7: 期限切れ MX レコードへの優先度順配送の頻度

システムは応答する候補となるゾーンをグループ A および B から交互に選択する．図 5.7 では，サンプル毎にばらつきがあるが，全体として MX レコード情報が無効となった後の配送には，集中や周期性は見られない．また，時間経過による配送の増減も見られない．このような傾向は 30 分以上経過しても同様に観測され，TTL 値を無視した spam 配送は TTL 値の長さとは無関係であると予想される．

従って，一つの MX サーバセットに注視すれば，TTL 値を長くする程，時間経過に伴って False Negative となるメールの累積数は一次関数的に増加することになる．TTL 値を短くすればする程，単体のサーバセットの False Negative の累積数は減少するが，複数のサーバセットで考えると，その累積数と TTL の間の相関性は低いと言える．また，False Negative と同様，時間経過に伴う True Positive となるメールの累積数も増加するため，それらの比率は大きく変化することはない．

本システムで応答する TTL 値の最適値は，導入する環境に依存することが考えられるため，今後様々な環境での調査を行い，チューニング手法を検討する必要がある．

5.6.2 分散環境における運用

本章では，1 台の DNS コンテンツサーバによる実装例を示したが，汎用性を考慮すると以下の点への配慮が必要となる．

- DNS コンテンツサーバと MX サーバを異なるネットワークセグメントに設置
- 複数台の DNS コンテンツサーバを設置（プライマリ，セカンダリ）

前者については，現在のインターネット環境においても，DNS コンテンツサーバから MX サーバへの MX レコード情報選択の伝達に遅延を生じることになる．初回問い合わせ時の情報伝達の遅延では，MX サーバでの対応（図 5.2(II)，(V)）が間に合わないことになる．ただし，本システムでは，OS による SYN 再送が継続している間に対応が完了すれば良く，数秒程度であればこの問題の影響は受けない．それ以外の問い合わせ時の遅延では，MX レコード情報の切り替え時刻後の有効時間（TTL）に十分な余裕があれば問題は生じず，かつ，余裕が無い場合でも，初回問い合わせ時と同様，SYN 再送の継続期間内に対応が完了すれば良い．

後者については，コンテンツサーバ間の同期ズレに対応する必要がある．最も単純な対策として，各 DNS コンテンツサーバにおいて，応答した MX レコード情報に応答時刻を付加して MX サーバに伝達し，同期ズレを検知した MX サーバはその分だけ有効期間を延長することが考えられる．ただし，この手法では，切り替え時刻を跨ぐ同期ズレを生じた場合，旧情報の有効期間が次回の切り替え時刻を超えることが起こり得る．すなわち，次回の切り替え時に，同一グループに属する 2 つの MX レコード情報が共存し，False Negative の増大の原因となる．このため，著しい同期ズレにより長時間の共存が懸念される場合は，MX レコードの候補となる IP アドレスのグループ分けを 3 グループ化するという対応が必要になると考える．

何れの問題も，伝搬遅延や同期ズレが運用上の許容範囲内であれば解決できる．しかし，許容できない場合は，DNS コンテンツサーバへの改造により，MX レコード情報を事前に通知し，ntp 同期でほぼ同時期に MX レコード情報を切り替える仕組みを設ける等の対応が必要になると考えられる．

5.6.3　例外的な送信ホストへの対応

正当な送信ホストからのメール配送で，本システムでFalse Positiveとなるのは，送信ホストが使用するDNSキャッシュサーバがTTLの有効な期間を超えてMXレコード情報のキャッシュを保持し続ける場合と，MXフォールバックを行わない場合である．これらのうち，正当な送信ホストのMXフォールバックへの対応は，3章の実験で示したとおり，調査を行った範囲内ではFalse Positiveは発生しなかったが，RFC5321に違反してMXフォールバックを行わないMTAが一部確認されている[28]．

当該MTAのように規定を守らないMTAを使用する送信ホストからのメール配送は本システムではspamメールであると見なされて受信することができず，False Positiveが発生する．このような送信ホストに対して，暫定的であるが，全優先度のMXサーバで接続を即座に許可する恒久ホワイトリストに該当するホストを登録することによって対処する．

5.7　まとめ

本章では，正当なメールの送信ホストとspam送信ホストの通信挙動の違いに注目し，これまでに提案したMXフォールバック検出システムをさらに強化させ，MXレコードのTTL値に従って適切にキャッシュを破棄するホストからの配送時のみ，MXフォールバック検査を行う手法を提案した．本手法は，高速かつ低負荷にspam判定が行え，また他手法と容易に組み合わせることができる柔軟性や拡張性が高いMXフォールバック検出手法の長所を維持しつつ，機能拡張により判定性能をさらに高められることを確認した．

本章で提案した手法は全てのspamを完全に排除するものではなく，従来手法の前段に設置することを目的としている．本手法でFalse Negativeとなる配送では，1セッションで大量のメール送信を試みる特徴的な挙動を示すホストが多く見られたことから，本手法の後段として，スロットリング技法により1セッションあたりで送信可能なメール送信件数を制限することにより，更なる精度向上が期待できる．また本手法の導入により，メール受信前にspam送信によるセッションが削減されることで，大きなデータ量の通信が発生し，コンテンツ処理のための多くのリソースが必要なコン

テンツフィルタリング技法の弱点を補うことができる.

第6章

結論

本論文では，送信ホストの送信動作がプロトコルに準拠して正当に行われるかを検査することにより，spam メール送信ホストを検出する研究について述べた．本研究により，日々世界中で通信される膨大な量の spam メールトラフィックを軽減させることができ，従来の spam 対策手法が抱える諸問題解決の一助となる．

第 1 章では，電子メールサービスのみならず，インターネット全体の信頼性を脅かす spam メール送信ホストについて述べた．spam メール対策は長年にわたって取り組まれているにも関わらず，それらの対策を擦り抜ける spam メールは依然として多い．大量の spam メールの中から正当なメールを識別する処理を出来るだけ軽量に行い，正当なメールの処理のためにネットワークやサーバ資源を活用することが望ましい．本論文で提案するリアルタイム再送検出手法や DNS キャッシュ処理検査手法が，従来の spam 対策技術よりも低負荷で運用可能であり，また他手法と容易に組み合わせて運用することができる柔軟性を有する点について議論した．

第 2 章では，メール送信に関連する通信である，DNS による名前解決，TCP コネクション，SMTP セッションの各段階において，spam メール対策システムがどの段階で，どのように判定するかについて議論した．その中で，本稿で述べる手法は，DNS による名前解決，および TCP 接続のプロトコル検証によって判定するため，実際のメール通信が開始される前に spam メール送信ホストを識別する．これにより，少ない通信量で spam 送信ホストの識別が行えるだけでなく，コンテンツフィルタリング等の高負荷に脆弱な手法の前段として設置することで，他手法の弱点を補うことが可能であることを示した．

第 3 章では，正当なメール送信ホストと spam メール送信ホストの通信挙動を詳細に調査した．正当なメール送信ホストの通信挙動に基づいた “正当な送信ホストと見なす条件” を独自に定義し，その条件と spam メール送信ホストとの通信挙動を比較したところ，条件を満たした spam 送信ホストによる配送は 1.02%∼2.59%と僅かであり，大多数の spam 送信ホストによる通信挙動では条件を満たさないことを確認した．また，両者の通信挙動の違いの中で実際に spam 送信ホスト検出システムに使用可能な特徴について議論した．これらの結果から，通信挙動の違いによって spam 送信ホストの識別が可能であることを示した．さらに，正当な送信ホストと spam 送信ホストの通信挙動の違いに基づき，実際の spam 送信ホスト検出システムでどのように実装可能であるか検討した．

第 4 章では，送信ホストが SYN パケットを複数回にわたって再送し続ける特徴に注目した，再送動作のリアルタイム検出による spam 送信ホスト判別手法を提案し，さらにその評価や拡張性の確保等について述べた．この手法は，調査を行った全ての OS が最初の SYN パケットの送信から 3 秒以内に 2 度目の SYN パケットの送信を行うことから，Tempfailing で発生する配送の遅延の問題を解決し，負荷耐性を確保した．さらに，Nolisting の判別精度の低さ，また Unlisting の非柔軟性等，従来の手法の様々な弱点を克服することができた．システム実装の要となる一時ホワイトリストの保持時間の変化による spam 送信ホスト判別精度の評価を行い，5 秒から 20 秒程度の設定が判別精度と負荷耐性の確保のいずれの視点からも適切であるという知見を得た．

第 5 章では，定期的に応答する MX レコード情報を変更する特殊な DNS コンテンツサーバを使用して DNS プロトコル違反を検出し，再送動作のリアルタイム検出による spam 送信ホスト判別手法を強化させる手法について述べた．この手法では，MX フォールバック検査の前段として，MX レコードの TTL 値に従って適切にキャッシュを破棄するホストからの配送時のみ，MX フォールバック検査を行う．このシステムを実際に導入し，spam 送信ホスト識別精度の評価を行ったところ，spam メール送信に起因する SMTP セッションが約 96.7%削減された．この手法は，高速かつ低負荷に spam 送信ホストの識別が行え，また他手法と容易に組み合わせることができる柔軟性や拡張性が高い MX フォールバック検出手法の長所を維持しつつ，機能拡張により判定性能をさらに高められることを確認した．

本論文で述べた手法は，2 章で述べた既存手法や商用製品と比較して少ない作業負荷で運用することが可能である．また，本手法は実際のメール送信動作の前に行われる DNS による名前解決，および TCP コネクションのメカニズムをベースにしているため，従来のいずれの spam メール判別手法の判別よりも早い段階で処理を行う．従って，例えば Tempfailing やコンテンツフィルタリング等，高レイヤで動作する他の spam メール対策手法の前段に設置し，柔軟に組み合わせて使用することができる．

今後の課題として，電子メール以外の通信における不正な通信にも対応する必要がある．例えば，第 5 章で述べた DNS コンテンツサーバが定期的に応答内容を切り替える手法は，名前解決を行うホストと実際に攻撃を行うホストが異なることの多いウェブサーバへの DDoS 攻撃への対策にも応用が期待出来る．さらに，各種の通信プロトコルで不正通信を行うホストの特徴的挙動を見つけ出して識別する手法を考案し，インターネットの信頼性を高めていく必要がある．

謝辞

博士課程での研究を行うにあたり，多くのご指導を賜りました名古屋大学情報基盤センターの高倉弘喜教授に感謝いたします.

学部生の頃から修士課程まで研究室に所属させて頂き，様々なご指導を賜りました中京大学大学院情報科学研究科の鈴木常彦教授に感謝いたします.

本研究の評価実験にあたり，実験環境を提供頂いた，京都大学学術情報メディアセンターの岡部寿男教授，宮崎修一准教授に感謝いたします.

研究活動や論文執筆において多くのご意見を頂きました，名古屋大学情報基盤センターの嶋田創准教授，山口由紀子助教，東京電機大学情報環境学部の八槇博史准教授（前名古屋大学大学院情報科学研究科准教授）に感謝いたします.

ご多忙中にもかかわらず，本博士論文の副査を務めていただきました，名古屋大学情報基盤センターの石井克哉教授，名古屋大学大学院情報科学研究科の結縁祥治教授に感謝いたします.

研究活動で様々な支援をしていただき，また日常生活においてもご親切にしていただいた技術補佐員の森山さくらさん，共にワインを愉しみながら語り合った修士課程2年の佐藤正明君，さらに研究室生活において多くの支援を頂きました高倉研究室の皆様に感謝いたします.

最後に，長い学生生活を支えて頂いた家族の皆様に感謝いたします.

発表論文リスト

- 論文誌
  - 北川直哉, 高倉弘喜, 鈴木常彦,
    “通信挙動の特異性を利用した spam 送信ホスト検出システムの開発,”
    電子情報通信学会論文誌 Vol.J-xxx-D, 2014.
  - 北川直哉, 高倉弘喜, 鈴木常彦,
    “再送動作のリアルタイム検出による spam 判別手法の実装と評価,”
    電子情報通信学会論文誌 Vol.J-96-D No.3, pp.552-561, 2013.
- 国際会議
  - Naoya Kitagawa, Hiroki Takakura, Tsunehiko Suzuki,
    “An Anti-spam Method via Real-time Retransmission Detection,”
    The 18th IEEE International Conference on Networks (ICON2012),
    10.1109/ICON.2012.6506588, pp.382-388,2012.
- 査読付国内発表
  - Naoya Kitagawa, Hiroki Takakura, Tsunehiko Suzuki,
    “A lightweight method to discriminate spamming hosts by periodically changing DNS response,”
    Workshop on Internet Architecture2012, IEICE Technical Report Vol.112, no.250, IA2012-39, pp.31-35, 2012.（Abstract review）
  - 北川直哉, 鈴木常彦,
    “フォールバック検出による spam 対策システムの実装,”

第 12 回インターネットテクノロジーワークショップ（WIT2011），
一般講演 4-1, 2011.

- 国内発表
  - 北川直哉, 鈴木常彦,
    “再送戦略ポリシーの違いを利用した spam 判別,”
    情報科学技術フォーラム講演論文集 9(4), pp.231-234, 2010.
  - 北川直哉, 鈴木常彦,
    “MX fallback 分析,”
    電気関係学会東海支部連合大会講演論文集 2009, O-254, 2009.

参考文献

[1] クレイグ・ハント，“TCP/IP ネットワーク管理 第 3 版,”O’Reilly，2003.

[2] “SPAM and the Internet,” http://www.spam.com/legal/spam/

[3] 柴田賢介，神谷造，佐野和利，荒金陽助，塩野入理，金井敦，“迷惑メールにおける誘導手法に関する一考察,” 情報処理学会研究報告 CSEC,[コンピュータセキュリティ]2007(71),pp.325-330,2007.

[4] T.Takemura, H.Ebara,“Spam mail reduces economic effects,” IEEE Second International Conference on Digital Society, pp.20-24, 2008.

[5] Y.Ukai, T.Takemura,“Spam mails impede economic growth,” The Review of Socionetwork Strategies,1(1),pp.14-22,2007.

[6] “Symantec Intelligence Report,” http://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_10-2013.en-us.pdf,2013.

[7] S.Frei, I.Silvestri, G.Ollmann, “Mail Non-Delivery Notice Attacks,” http://www.techzoom.net/mailbomb

[8] “特定商取引に関する法律,” http://law.e-gov.go.jp/htmldata/S51/S51HO057.html

[9] “特定電子メールの送信の適正化等に関する法律,” http://law.e-gov.go.jp/htmldata/H14/H14HO026.html

[10] "The Apache SpamAssassin Project,"
http://spamassassin.apache.org/

[11] J.Mason,"Filtering spam with spamassassin,"
In HEANet Annual Conference, 2002.

[12] "BOGOFILTER,"
http://bogofilter.sourceforge.net/

[13] J.Blosser, D.Josephsen, "Scalable Centralized Bayesian Spam Mitigation with Bogofilter"
LISA '04 Proceedings of the 18th USENIX conference on System administration,pp.1-20,2004.

[14] http://sourceforge.jp/projects/bsfilter/

[15] J. Klensin,"Simple Mail Transfer Protocol,"
http://tools.ietf.org/html/rfc5321,Oct.2008.

[16] Evan Harris, "Greylisting,"
http://projects.puremagic.com/greylisting/

[17] John R. Lavigne,"Experiences with Greylisting," Proceedings of the Second Conference on Email and Anti-spam(CEAS 2005),
http://www.taugh.com/greylist.pdf,2005.

[18] T.Sochor,"Greylisting - long term analysis of anti-SPAM effect," Fourth International Conference on Risks and Security of Internet Systems (CRiSIS),pp.98-104,2009.

[19] Pin-Ren Chiou, Po-Ching Lin, Chun-Ta Li, "Blocking Spam Sessions with Greylisting and Block Listing based on Client Behavior" 15th International Conference on Advanced Communication Technology (ICACT),pp.184-189,2013.

[20] 前野年紀，“お馴染みさん方式”，
https://moin.qmail.jp/お馴染みさん方式

[21] “Nolisting,” http://nolisting.org/index.html

[22] “Unlisting,” http://nolisting.org/unlisting.html

[23] 山口榮作，鈴木常彦，“TCP Handshake 制御を利用した spam 対策システム,” 大学情報システム環境研究,No.8,pp.60-68,2005.

[24] “Symantec Traffic Shaper powered by Brightmail,”
http://www.symantec.com/traffic-shaper/

[25] “Symantec Messaging Gateway powered by Brightmail,”
http://www.symantec.com/messaging-gateway/

[26] 丸山伸，中村素典，岡部寿男，山井成良，岡山聖彦，宮下卓也，“動的に応答を変える DNS を利用した電子メール受信の優先制御,” 情報処理学会論文誌,No.47(4),pp.1021-1030,2006.

[27] S.Maruyama, M.Nakamura, Y.Okabe, N.Yamai, K.Okayama, T.Miyashita, “Priority control in receiving e-mails by giving a separate response to each DNS query,” International Symposium on Applications and the Internet SAINT 2006, p. 4 pp.-93,2006.

[28] http://www.reflection.co.jp/spam/rfc_ignorant.html

[29] http://www.e-ontap.com/dns/propagation/ttl.html

[30] “Sendmail,”
http://www.sendmail.com/sm/open_source/

[31] D.A.L.Romana, S.Kubota, K.Sugitani, Y.Musashi, “DNS Based Spam Bots Detection in a University,” Proceedings of the 2008 First International Conference on Intelligent Networks and Intelligent Systems,pp.205-208,2008.

[32] H.Choi, H.Lee, H.Lee, H.Kim,"Botnet Detection by Monitoring Group Activities in DNS Traffic" Proceedings of the 7th IEEE International Conference on Computer and Information Technology,pp.715-720,2007.

[33] R.V.Salomon, J.C.Brustoloni,"Bayesian Bot Detection Based on DNS Traffic Similarity" Proceedings of the 2009 ACM symposium on Applied Computing,pp.2035-2041,2009.

[34] "Spamhaus ZEN,"
http://www.spamhaus.org/zen/

[35] "SpamCop SCBL,"
http://www.spamcop.net/bl.shtml

[36] "SORBS,"
http://www.us.sorbs.net/

[37] A.Ramachandran, D.Dagon, N.Feamster,"Can DNS-based blacklists keep up with bots?," CEAS2006,http://ceas.cc/2006/14.pdf,2006.

[38] I.Androutsopoulos, J.Koutsias, K.V.Chandrinos, G.Paliouras, C.D.Spyropoulos, "An evaluation of Naive Bayesian anti-spam filtering," Proceedings of the workshop on Machine Learning in the New Information, pp.9-17,2000.

[39] I.Androutsopoulos, J.Koutsias, K.V.Chandrinos, C.D.Spyropoulos, "An experimental comparison of naive Bayesian and keyword-based anti-spam filtering with personal e-mail messages," Proceedings of the 23rd annual international ACM SIGIR conference on Reserch and development in information retrieval, pp.160-167,2000.

[40] H.Ducker, D.Wy, V.N. Vapnik, "Support vector machines for spam categorization," IEEE Transactions on 10(5), pp.1048-1054,1999.

[41] T.S.Guzella, W.M.Caminhas, "A review of machine learning approaches to spam filtering," Expert systems with Applications 36(7), pp.10206-10222,2009.

[42] S.Suwa, N.Yamai, K.Okayama, M.Nakamura, “DNS Resource Record Analysis of URLs in E-mail Messages for Improving Spam Filtering,” International Symposium on Applications and the Internet SAINT 2011, pp.439-444,2011.

[43] S.Suwa, N.Yamai, K.Okayama, M.Nakamura, K.Kawano, “Spam Mail Discrimination System Based on Behavior of DNS Servers Associated with URLs,” International Symposium on Applications and the Internet SAINT 2012, pp.381-386,2012.

[44] M.Wong, W.Schlitt,“Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1 ,” http://www.ietf.org/rfc/rfc4408.txt,2006.

[45] 山井成良，岡山聖彦，中村素典，清家巧，漣一平，河野圭太，宮下卓也，“SMTP セッションの強制切断による spam メール対策,” 情報処理学会論文誌 50(3), pp.940-949,2009.

[46] N.Yamai, K.Okayama, T.Seike, K.Kawano, M.Nakamura, S.Maruyama, “An Anti-Spam Method with SMTP Session Abort,” MIT Spam Conference,2008.

[47] J.Lyon, M. Wong,“Sender ID: Authenticating E-Mail,” http://www.ietf.org/rfc/rfc4406.txt,2006.

[48] J.Lyon,“Purported Responsible Address in E-Mail Messages,” http://www.ietf.org/rfc/rfc4407.txt,2006.

[49] P. Vixie,“Extension Mechanisms for DNS (EDNS0),” http://www.ietf.org/rfc/rfc2671.txt,1999.

[50] R. Braden,“Requirements for Internet Hosts – Application and Support,” http://www.ietf.org/rfc/rfc1123.txt,Oct.1989.

[51] 東角芳樹，鳥居悟，“DNS 通信の挙動からみたボット感染検知方式の検討” マルウェア対策研究人材育成ワークショップ 2008, http://www.iwsec.org/mws/2008/manuscript/1008.pdf,2008.