E-23

電子メールの大量送信を選択的に制限する中継システム

A Mail Transfer System Selectively Restricting Huge Amount of E-mails

津崎 善晴†1　松本 亮介†1　小谷 大祐†1†2　宮崎 修一†3　岡部 寿男†3
Yoshiharu Tsuzaki　Ryosuke Matsumoto　Daisuke Kotani　Shuichi Miyazaki　Yasuo Okabe

1. はじめに

電子メール（以下，メールとする）は複数のメール配送システムを経由して送信者から受信者へと配送される．従来のメール配送システムの目的は途中でメールを失うことなく，受信者へ確実に配送することであり，配送に要する時間に関しての保証はなかった．しかし，メールの普及が進むにつれて，個人で利用するだけでなくビジネスでも広く利用されるようになり，メールを遅滞することなく配送することが重要となってきた．

メール配送の仕組みは，SMTP[1]（Simple Mail Transfer Protocol）で規定されており，単純なプロトコルで実装されている．容易に大量のメールを送信可能なため，ネットワーク帯域の圧迫や，メールサーバの処理能力超過によるメール配送の遅延といった問題を引き起こす．従来，大量のメール配送は spam と呼ばれる社会問題として取り上げられる．spam とは意図的に不特定多数の受信者に一括して送信されるメールのことを指し，UCE（Unsolicited Commercial E-mail），UBE（Unsolicited Bulk E-mail）とも呼ばれる．spam メール配送は一般的にメール送信時のセッションタイムアウトが短く，配送の確実性よりもスループットを重要視する傾向がある．これらの傾向を利用して spam 対策として流量制限を行う手法が研究されている．spam メールを受信側で排除する手段として，ブロッキング，スロットリング，フィルタリングの 3 種類に大別される．ブロッキング，スロットリングはメールの受信前の対策であり，フィルタリングは受信後の対策である．

上記の spam 以外に，メールの大量送信が想定される．メール送信サーバの誤送信に起因する場合や，メール配送システムの設定不備に起因する場合である．例として，メール送信サーバの不具合から制御不能となり，メール送信プログラムの誤動作で大量送信されることや，メーリングリストの設定不備によるメールループが発生することが挙げられる．上記のような送信者の意図しない特定の送信アドレスから特定の宛先アドレスに対してのメールの大量送信のことを大量の誤送信と呼ぶ．spam とは異なり，大量の誤送信は通常のメール配送であるため，spam 対策を利用することができない．また，大量の誤送信はメールサーバの処理能力超過によるメール配送遅延の原因となる．予め，メール配送システムへのメール流量帯域を制限することが考えられるが，大量送信による帯域占有で，同メール配送システムを利用している他ユーザにも配送制限の影響を与える．さらに，一旦，メールサーバがメール受信するとその後の配送処理を継続して行わなければならないため，大量受信による負荷も発生する．そこで，本稿では通常の利用者に正常なメール配送を提供するために，メール配送システムに過負荷を与える大量の誤送信を選択的に制限することを提案する．また，大量の誤送信を行った送信元のメールサーバに一時的なエラーとして返信することでメールサーバの負荷を低減する．本システムを導入する場合，設置場所として考えられるのは，送信元システム，受信システム，中継（リレー）システムの 3 通り考えられるが，既存のシステムへの変更を最小限にでき，メール配送システムの負荷を低減可能な中継システムに導入することとする．メール配送システムに入る最前段に設置することで，大量の誤送信に対する流量制限を実現する．

本稿で提案するシステムは，まず SMTP セッションからエンベロープ FROM とエンベロープ TO を抽出し，メールの受信時間とともにデータベースに登録する．次に，新たに SMTP セッションが開始されてからエンベロープ FROM とエンベロープ TO の組が，過去のある期間中に何通送信されたかをデータベースから計算する．もし，規定値を超過した場合は，大量の誤送信とみなし，一時的なエラーとして送信元メールサーバに返送し，それ以外は正常なメールとして処理を行う．その結果，大量の誤送信のみを制限し，通常のメールは問題なく配送するシステムが完成する．

2 節で spam 対策で用いられる流量制限手法を従来手法として説明し，3 節で大量の誤送信に対する提案手法の概要を示す．4 節で実装方針と検討事項の説明し，5 節でまとめとする．

2. 従来手法

本節では spam 対策で用いられる大量送信メールの流量制限手法を従来手法として説明する．

2.1 ブロッキングとスロットリング

受信側ではメール配送システムを spam から守るために，最前段のメールサーバにおいて spam を受信しない対策が必要とされる．ブロッキングにおいての大量送信メールの流用制限として，SORBS[2]（Spam and Open-Relay Blocking System）やレピュテーションがある．SORBS は不正を働く第三者からの中継が可能であるメールサーバをブラックリストとして管理している．利用者は SMTP セッション中にブラックリストと照合し，ブラックリストに含まれる場合はセッションを中断する等して spam 対策を行う．Spam と判断された場合，メール配送は行われないため結果として

†1 京都大学大学院情報学研究科
Graduate School of Informatics, Kyoto University
†2 日本学術振興会特別研究員
JSPS Research Fellow
†3 京都大学学術情報メディアセンター
Academic Center for Computing and Media Studies, Kyoto University

流量制限を実現できる．次に，レピュテーションは送信者評価とも呼ばれ，メールサーバを評価するサービスである．送信元メールサーバに関する情報を収集してスコア化し，受信側で任意のスコア以下のメールは受信拒否をすることでメール流量を制限する．

また，スロットリング[3]はspamメールの配送でのSMTPセッションのタイムアウト値が短いとの仮説に基づく対策手法であり，SMTP コネクションが確立された後の応答を遅延させることで送信元からのセッションをタイムアウトさせる狙いがある．結果として，spamであればセッションタイムアウトによりエラーとして返信されるため，流量を制限できる．

2.2 OP25B

OP25B[4]は ISP（Internet Service Provider）のネットワークを経由して ISP 外へ接続する SMTP セッション（25 番ポートでの通信）を全てブロックする手法である．spamの送信者は ISP が設置したメールサーバを使用せずに，直移設外部のメールサーバに送信する場合が多く，許可した特定のメールサーバ以外からの25番ポートでの送信を制限することにより，ISP 内部のユーザアカウントが spam の踏み台となり spam を大量送信しても 25 番ポートでの通信ができないため，メールの流量が制限される．

2 節で従来手法として．spam 対策等で大量送信されたメールの流量を制限する手法を紹介した．

大量の誤送信は spam とは異なる特徴を持っているため，従来手法を用いて解決できない．次節で大量の誤送信を制限する手法を説明する．

3. 提案手法

本節では大量の誤送信を制限する手法の概要を説明する．

3.1 大量の誤送信を判定するタイミング

まず，SMTP セッションにおける手続きを図 1 に示す．SMTP セッションはクライアント側からサーバへの接続を開き，サーバ側からグリーティングメッセージで応答することにより開始される．クライアント側からサーバに EHLO（HELO）コマンドを送信し，自身の身元を示す．その後，メールトランザクションに移行し，MAIL コマンド，RCPT コマンド（複数の宛先を指定する場合は複数回発行），DATA コマンドを送信する．クライアント側から QUIT コマンドを送り，SMTP セッションを終了する．メールトランザクション部は，MAIL コマンドから DATA コマンドまでを一連の流れで続けて送ることで複数のメールを送信することができる．

まず，大量の誤送信があった場合に上述の SMTP セッション中でエラーとして送信元メールサーバへ返信する判定を行う箇所を説明する．判定候補は図 1 中の①～⑤の箇所である．

①セッションの開始後に情報として送信元メールサーバの IP アドレスが得られる．

②①で得られた情報と送信元メールサーバのホスト名（FQDN）が得られる．

③①，②の情報と MAIL コマンドで送信されてきたエンベロープ FROM が得られる．

④①～③の情報と RCPT コマンドで送信されてきたエンベロープ TO が得られる．

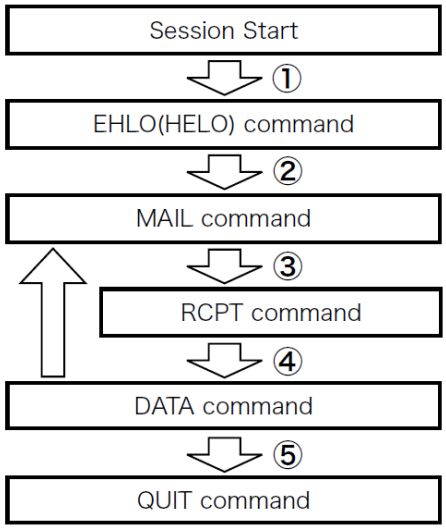

図 1. SMTP セッションの手続き

⑤①～④の情報と DATA コマンドから送られてきたヘッダ情報とメッセージが得られる．

大量の誤送信を他のメールと区別できる情報として，エンベロープ FROM とエンベロープ TO が得られており，かつメールサーバへの負荷を下げるために処理にかかる時間を最短で満たすのは，④の箇所となる．⑤は④と同様に必要な情報が得られているが，DATA コマンドで送られてくる情報量は①～④と比べて非常に多く，今回の大量の誤送信の判定には不要であるため，④で返信する方が処理を短くできる．上述より，大量のメール配送と判定する箇所は SMTP セッション中の RCPT コマンドを受信した時点とすることが最も効果的であると考えられる．

3.2 大量の誤送信を判定する仕組み

SMTP セッションで得られたエンベロープ FROM とエンベロープ TO を利用して，大量のメール配送と判定する仕組みの概要を説明する．予め，決まった送信元から大量のメール配送が行われるかわかっている場合の流量制限は簡単である．しかし，一般的なメール配送システムには送信元アドレス，宛先アドレスの組は無数であり，どの組で大量にメールが配送されるか予期できない．そこで，SMTP セッション中に得られた送信元アドレスと宛先アドレスを一つの組として保存する．大量の誤送信の判定は，過去に得られたエンベロープ FROM とエンベロープ TO の同じ組を単位時間当たりに何通送信されたかを導出する．単位時間当たりの通数が，閾値を超えた場合に一時的なエラーとして送信元メールサーバに返信する．閾値を超えない場合は正常にメール配送を行う．大量の誤送信に対する流量制限の動作は以下の通りとなる．

a. SMTP セッション中の MAIL コマンドからエンベロープ FROM を得る．
b. SMTP セッション中の RCPT コマンドからエンベロープ TO を得る．
c. エンベロープ FROM とエンベロープ TO の組でのある期間中の通数を計算する．
d. 計算結果が閾値以上であれば送信元アドレスにエラーメールとして返信する．閾値未満であれば SMTP セッションを続ける．

さらに，本システムを他のメールサーバと連携する方法を説明する．本システムは選択的に大量の誤送信の流量を制限するため，流量制限を行いたいメールサーバの前段に置くことでメール配送システム内に大量の誤送信が制限された状態で配送されるため，内部のメールサーバへの負荷を低減することができ，正常メールはそのまま送信できる．

4. 実装方針と検討事項

本節で 3 節の提案手法を実現するための実装方針と検討事項について説明する．

4.1 実装方針

提案手法を実現するための実装方針の概要を説明する．本システムにおいて sendmail[5]や postfix[6]のメールフィルタプラグインの仕組みを提供している milter[7][8]を用いる．milter を通じて SMTP セッションから取得する情報は MAIL コマンドから得られるエンベロープ FROM，RCPT コマンドから得られるエンベロープ TO，メールの受信時間の 3 つの値である．

次に，上記で得られたエンベロープ FROM，エンベロープ TO，メールの受信時間の組を管理する仕組みについて説明する．無数に存在するペアを管理するためにデータベースを用いる．3 つの値をそれぞれテーブルとして準備し，3 つの値が取得できた時点で，一つのエントリーとしてデータベースに保存する．新たに SMTP セッションが開始されると上記の SMTP セッション中に得られたエンベロープ FROM とエンベロープ TO の組み合わせが過去のある期間に何回存在したかを受信時間からデータベースを通じて計算する．エンベロープ TO が得られた時点で，制限したい値以上にメール送信があった場合は，4xx の一時的なエラーとして返す．それ以外の場合は，データベースに 3 つの値をエントリーとして保存する．また，データベースの容量を小さく保つために，ある一定期間を過ぎたエントリーは定期的に削除する仕組みも導入する．

以下に，本システムで上述の大量の誤送信に対する処理の流れを示す．図 2 は正常メールの処理の流れ，図 3 は大量の誤送信と判定されたメールの処理の流れを表している．

①クライアント側から SMTP セッションの開始要求を受け取り，クライアント側にグリーティングメッセージを送り，SMTP セッションを開始する．

②クライアント側から EHLO（HELO）コマンドを受け取り，milter 側で処理は行わず，クライアント側にステータス 250 を返す．

③クライアント側から MAIL コマンドを受け取り milter でエンベロープ FROM を取得する．取得後，クライアント側にステータス 250 を返す．

④クライアント側から RCPT コマンドが送信されたら milter でエンベロープ TO を取得する．得られたエンベロープ FROM とエンベロープ TO の組がある期間で何回配送されたかデータベースから計算する．得られた通数が閾値を超えている場合はステータス 4xx を送信元のメールサーバに返す（大量の誤送信と判断された場合はここで本メールに対する配送処理が終了する）．閾値以下はクライアント側にステータス 250 を返す．

⑤クライアント側から DATA コマンドが送信され，メールの受信が完了した時刻を取得する．得られたエンベロープ FROM，エンベロープ TO，メールの受信時間をデータベースに新しいエントリーとして保存する．

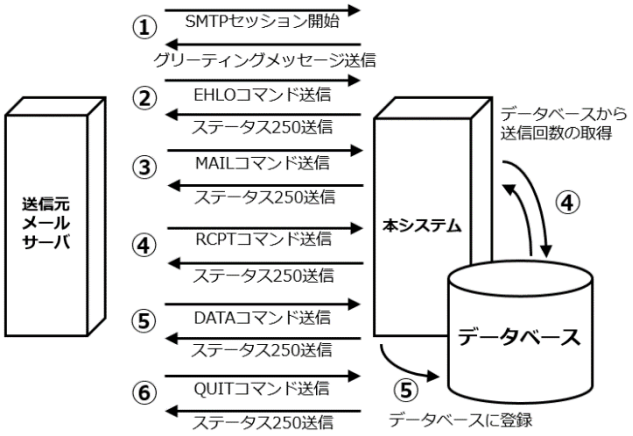

図 2．正常メールの処理の流れ

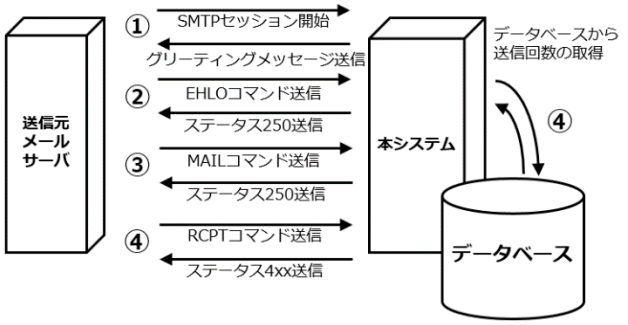

図 3．大量の誤送信と判定されたメールの処理の流れ

クライアント側にステータス 250 を返す．

⑥クライアント側からさらにメール送信がある場合は③からの処理に戻る．QUIT コマンドを受け取ると SMTP セッションを終了する．

上述の SMTP セッションから得られる情報とそれらを基に作成したデータベースを用いることにより，突発的に大量の誤送信に対して，動的に選択的に流量制限を実施でき，通常のメールはそのままメール配送機能を利用できる．

4.2 検討事項

現在，詳細な実装設計を行っているところであり，以下について検討を行っている．まず，無数に存在する送信元と宛先のアドレスの組をデータベースのエントリーとして扱う場合，データベースへのアクセス速度が問題になると考えられるため，効率の良いデータベースを選定する必要がある．また，本システムを複数のメールサーバで運用する場合に，データベースをどのようにして複数のサーバ間で保持するのかといった議論が残っている．さらに，大量のメール配送を判定するための条件を規定する必要がある．

5. まとめ

本稿では大量の誤送信に対して，選択的にメール流量を制限する手法を提案した．SMTP セッション中のエンベロープ FROM とエンベロープ TO の組を保持し，ある期間中に規定数以上のメール送信があった場合に，エンベロープ TO が得られた段階で，送信元にエラーメールを送り返すことで，メールの流量を制限することが可能となる．また，メール配送システムへの負荷が小さくなる仕組みも導入している．

しかし，実装段階で未だ検討中の内容も含まれており，結果を示すに至っていないため，有効性の部分での検討ができていないのが現状である．本稿の発表時に，本手法の有効性を示す予定である．

参考文献

[1] Klensin, J.: Simple Mail Transfer Protocol, RFC5321, IETF (2008)

[2] SORBS Publishing: SORBS (Spam and Open-Relay Blocking System) (online). available from http://www.sorbs.net/

[3] 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, Vol.2005 No.39, pp.69-74, 2005-05

[4] Klensin, J.: Message Submission for Mail, RFC6407, IETF (2011)

[5] Sendmail, Inc.: Sendmail (online). available from http://www.sendmail.com/sm/open_source/

[6] Wietse, Venema: POSTFIX (online). available from http://www.postfix.org/

[7] Sendmail, Inc.: milter.org An interactive catalog of sendmail mail filters (online). available from https://www.milter.org/

[8] SnertSoft: SnertSoft (online). available from http://www.milter.info/