4 バウンスメール対策

岡山大学総合情報基盤センター
山井 成良　yamai@cc.okayama-u.ac.jp

バウンスメールによる被害

本来の SMTP の仕様[1)] では，たとえば宛先不明など再送信しても回復できない理由により中継先 MTA から受信を拒否された場合には，受信できない理由とともにメッセージを発信者に送り返すことになっている．バウンスメール（bounce mail）とは，このような理由により送り返されたメッセージを指す．また最近では，spam メール対策の一環として，spam と疑われるメッセージに対して受取りを拒否したり，発信者に再送を促すメッセージを送り返したり（「2.3 フィルタリング」の「自動確認付きホワイトリスト」（p.760）参照）する方法もよく用いられている．このようなものもバウンスメールの一種といえる．

ところで，spam メールの宛先アドレスには，「1.2 spam メールの現状」（pp.747-751）で述べられているように使われそうなアドレスを手当たり次第作成したものや，アドレス収集業者が Web のサーチエンジンと同様の仕組みを用いて自動収集したものがよく用いられている．これらのアドレスには，以前は有効であったが現在は無効になっているものや，電子メールやネットニュースのメッセージ ID のように形式だけは電子メールアドレスに準拠しているが実際には無効であるものなどが大量に含まれており，実際に多くの spam メールが宛先不明で発信者に送り返されている．これに spam メール対策により送り返されるものを含めると，バウンスメールの数はさらに多くなる．

ところが，現時点における電子メールシステムの大多数は発信者アドレスおよび他の MTA/MUA の認証を行っていないため，発信者アドレスの詐称が容易であり，事実上ほとんどの spam メールは発信者アドレスの詐称が行われた状態で発信されている．このためバウンスメールは実際の spam メール発信者とは無関係のアドレスに送り返されることになる．特に，同一ドメインの発信者アドレスを付した spam メールが大量に発信された場合，バウンスメールはその詐称発信者ドメインの MTA（以下，被害 MTA）に集中して送られることになる．これにより，被害 MTA が過負荷になったり詐称発信者アドレス（以下，被害アドレス）が実在する場合にはディスクが溢れたりするなど，大きな被害が生じる．

たとえば，平成 14 年 11 月に国内のプロバイダで発生した事例では，30 万通以上のバウンスメールが被害 MTA に送られ，負荷の集中により最大 15 時間の配送遅延が生じ，また復旧までに約 2 日半を要したという被害が発生している．また，国外でも平成 15 年 10 月に少なくとも米国の 2 つのドメインがそれぞれ 10 万通以上のエラーメール集中による被害を受けている．このように，バウンスメールの集中は事実上 MTA に対するサービス不能（DoS）攻撃といってもよく，普段から膨大な数のメッセージを扱っている大規模なドメイン以外では大きな問題となる．特に，特定の個人やドメインを標的にした，バウンスメールによる故意のサービス不能攻撃は "Joe job" と呼ばれている．

バウンスメールの配送経路

バウンスメールによる被害への対策手法を紹介する前に，まずバウンスメールの配送経路について考える．spam メールおよびこれに起因するバウンスメールの典型的な配送経路を図 -1 に示す．

最近では，たとえばコンピュータウイルスの検出・駆除など管理上の理由によりメールゲートウェイを導入しているドメインが多数見受けられる．この場合，spam メールは spam 発信者の支配下にある MTA（spam 配送 MTA）からまずメールゲートウェイに送られる．この

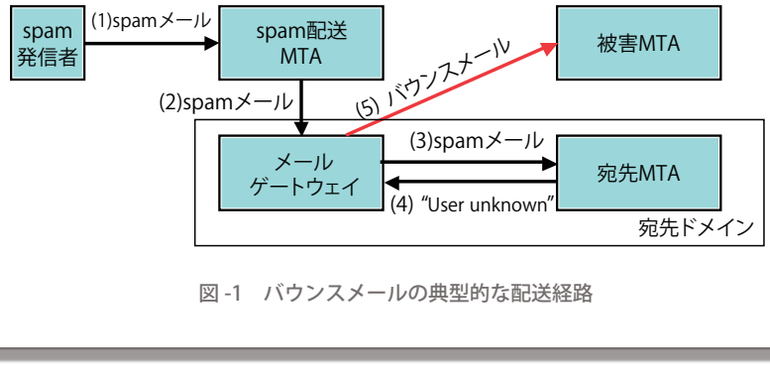

図 -1　バウンスメールの典型的な配送経路

時点では，メールゲートウェイは宛先アドレスが実在するかどうかなどの検証は行わず，@ 以降のドメイン名が自組織のものであれば送られてきた spam メールを受理する．次に，メールゲートウェイは受け取った spam メールを宛先アドレスに対応する MTA（宛先 MTA）に中継しようとするが，宛先 MTA はこのメールを受信すべきかどうかを検証し，たとえば宛先アドレスが実在しない場合には User unknown エラーを返すなど，受信を拒否する場合にはその旨を応答する．その結果，メールゲートウェイは配送不能であることを通知するバウンスメールを作成し，詐称された発信者アドレス宛てに発信する．

このほかの配送経路としては，spam 配送 MTA から被害 MTA への直接配送があるが，最近では spam 配送 MTA としてゾンビ PC 上に仕掛けられている専用プログラムが用いられる場合が多く，その場合にはエラー処理が行われないのが通常であるため，バウンスメールの配送経路としてはあまり問題とはならない．

■ バウンスメール集中への対策

前章で述べたように，多くのバウンスメールは spam メールの発信にはまったく無関係なドメインのメールゲートウェイから送られることが多い．これらのゲートウェイからは同時に通常のメールも送られる可能性があるため，バウンスメール集中の対策では通常メールの配送に影響を及ぼさないように配慮する必要もある．したがって，ブロッキングなどの単純な手法ではうまくいかないことが多い．

バウンスメール集中の根本的な原因は，発信者認証が現在のところそれほど普及していない点にあるが，それ以外にもいくつかの対策手法が知られている．以下では，そのうち代表的なものを紹介する．なお，発信者認証については本特集の別稿で述べられているため，本稿では触れない．

【宛先不明メールのメールゲートウェイでの受信拒否】

まず，メールゲートウェイ側でバウンスメールを抑制する対策から紹介する．

従来の場合，図 -2（a）に示すようにメールゲートウェイでは送信 MTA との間の SMTP セッションを完全に終了させてから宛先 MTA への中継を行っている．したがって，発信者へのエラー発生の報告義務はメッセージ本文を受け付けた時点で送信 MTA からメールゲートウェイに移管される．したがって，その後の宛先 MTA とのセッションで受取りが拒否されると，メールゲートウェイはバウンスメールを発信せざるを得ない．

そこで，アプライアンス製品などでは，図 -2（b）に示すように，まず宛先 MTA に対して宛先アドレスが存在するかを確認し，存在しない場合にはメールゲートウェイが受信を拒否する方法がよく用いられている．この機能は本来は宛先不明メールに対するウイルス検出・駆除などの無駄な処理を抑制するためのものであるが，これによりエラー報告義務は送信 MTA 側にとどまることになるため，バウンスメールの発生まで抑制することができる．受信を拒否された送信 MTA が spam 配送 MTA の場合にはこのエラーは無視されるが，そうでない場合には送信 MTA がバウンスメールを発信者に配送するため，通常の宛先不明メールに対して配送不能通知が発信者に届けられる機能は損なわれない．

同様の方法として，大分大学では学内の利用者情報を一元管理し，メールゲートウェイにおいてこの利用者情報を参照して宛先不明であるかどうかを判定する方法を採用している [2]．

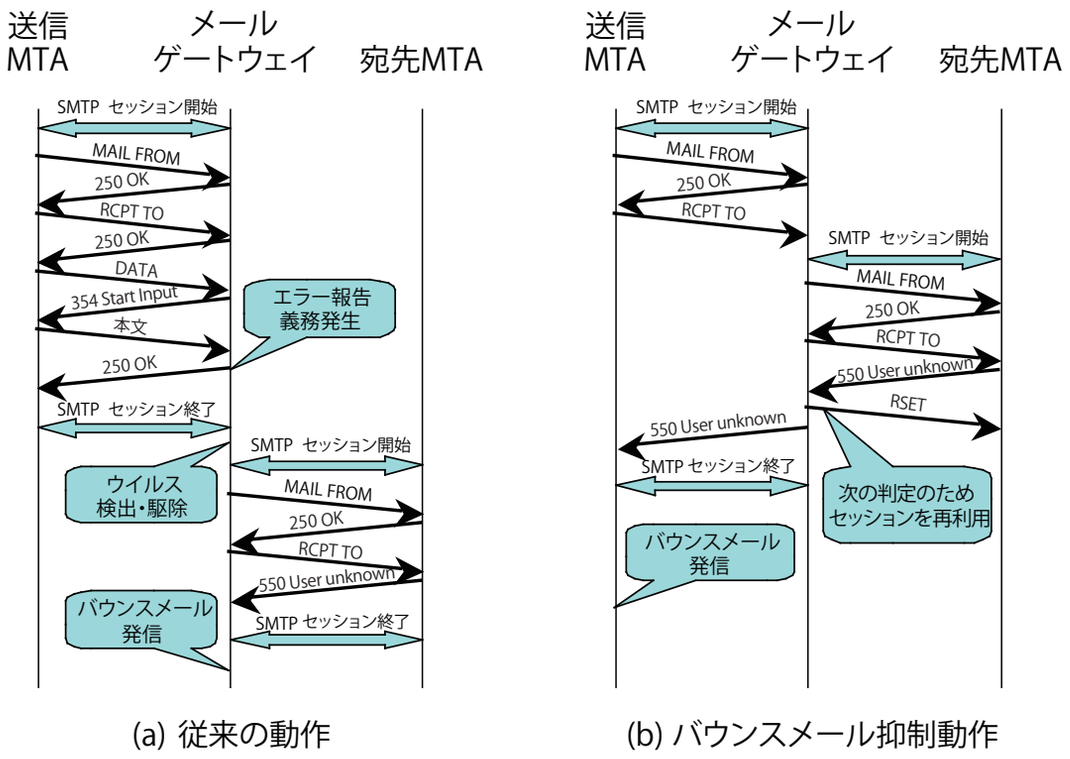

図-2　メールゲートウェイにおける動作

【バウンスメールの検証】

次に，バウンスメールを受信する被害 MTA での対策について紹介する．

被害アドレスとして実在のものが用いられた場合，被害 MTA では多数のバウンスメールが到着するだけでなく，通常はこれらを被害アドレスのメールボックスに保存する．その結果，メールボックスに不要なバウンスメールが大量に保存され，ディスクが満杯になったり，メールボックスの容量に制限を設けているサーバでは他のメッセージを受け取れなかったりするなどの問題が生じる．

この問題を解決する方法として，バウンスメールが正規の利用者が発信したメッセージに対するものかどうかを検証する方法がある．その代表的な枠組みが BATV（Bounce Address Tag Validation）[3] である．BATV では SMTP セッション中で MAIL FROM コマンドの引数として用いられるアドレス（エンベロープ From）を利用して検証を行う．この方法では本文中のヘッダに含まれる発信者アドレスは書き換えないため，受信者による返信には影響を与えない点に注意する．

たとえば，BATV の枠組みを用いた共有鍵認証方式である PRVS（Simple Private Signature）[3] では，図-3 に示すようにドメイン example.jp の発信用 MTA はエンベロープ From アドレスのローカルパート（@ より左側の部分）に検証用の情報 KDDDSSSSSS を付加して外部 MTA に発信する．もし，宛先アドレスに誤りがあり，外部 MTA からバウンスメールが送られてきた場合には，受信用 MTA（送信用 MTA と同一のものでもよい）は宛先アドレスに KDDDSSSSSS の部分が存在するかどうか，存在する場合にはそれが正しいかどうかを検証する．その結果，検証に失敗すればそのバウンスメールを破棄するか受信を拒否する．なお，バウンスメール以外のメッセージ（エンベロープ From アドレスが空でないメッセージ）に対しては，特別な処理は行われない．

この枠組みの特徴としては，発信者認証とは異なり，自ドメインの MTA に導入するだけで十分な効果を発揮する点が挙げられる．ただし，正しいエンベロープ From が spam 発信者に知られた場合，このアドレスを発信者アドレスに流用して spam メールを発信されると

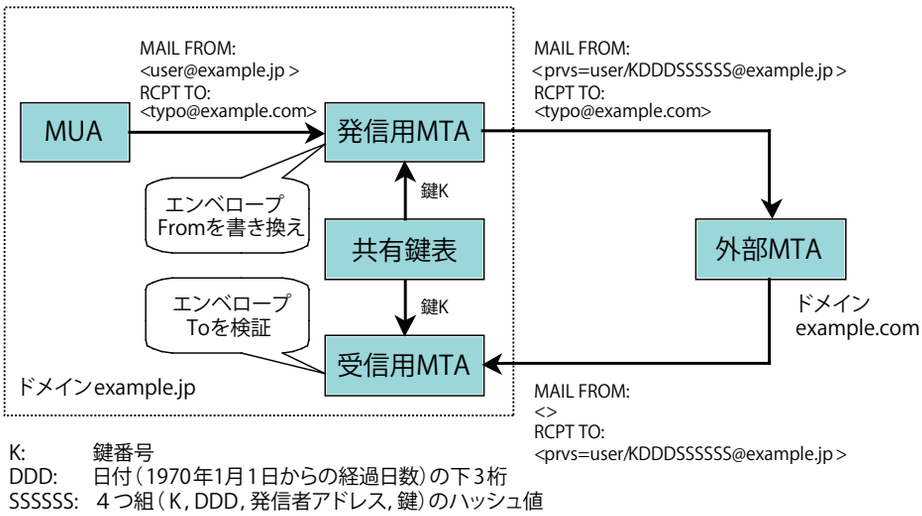

図 -3　PRVS における MTA の動作

Joe job 攻撃を受ける可能性は残されている．

【ネームサーバを利用した被害 MTA の負荷分散】

バウンスメールが特定の被害 MTA に集中して送られると，その宛先が実在するかどうかにかかわらず，被害 MTA が過負荷になったり通常のメールに配送遅延が生じたりする危険性がある．しかし，前節で述べたバウンスメールの検証は，メールボックスの保護が目的であり，被害 MTA の過負荷には無力である．そこで，被害 MTA を過負荷から保護するためには，負荷分散が必要となる．

MTA の負荷分散手法としては，MTA の多重化が一般的によく用いられている．普段から膨大な数のメールをやり取りしている大規模なプロバイダでは，数十台以上の MTA を設置して負荷分散を行いながらサービスを提供している．しかし，中小規模の組織ではこのような大規模な多重化を行っていないため，短時間に数十万通ものバウンスメールが到着する状況では通常メールの配送遅延が生じるのは避けられない．実際，冒頭で紹介した国内プロバイダの例では，4 台の MTA を導入していたにもかかわらず，通常メールの配送に大きな遅延が生じている．

この問題に対する対策としては，DNS を利用した負荷分散手法 [4] が提案されている．この方法では，中小規模の組織ではバウンスメールの大部分が普段は電子メールをやり取りしていない組織のメールゲートウェイから送られる点に着目し，バウンスメールと通常メールを異なる MTA で分離して処理を行う．

具体的には，図 -4 に示すように被害ドメインでは 2 種類の MTA（MTA1 と MTA2）を用意し，あらかじめ MTA1 の優先度が高くなるように DNS において MX レコードを設定しておく．また，MX レコードに対するキャッシュの有効期限（TTL）を長め（たとえば 7 日）に設定しておく．この状態では，普段から電子メールをやり取りしている組織では，組織内の DNS サーバに MX レコードがキャッシュされることになる．ここで被害ドメインにおいてバウンスメール集中の兆候を検出すると，被害ドメインの MX レコードのうち，優先度の高い方を削除する．その結果，普段は電子メールのやり取りがない組織からは，配送先の問合せが被害ドメインの DNS サーバまで達するため，新たな電子メールが MTA2 に送られる．一方，普段から電子メールのやり取りがある組織からは，当該組織の DNS サーバにキャッシュされている MX レコードに従い，新たな電子メールは MTA1 に送られる．これらの動作の結果，普段から電子メールのやり取りがあるかどうかの違いにより配送先の MTA を分離でき，通常メールの配送遅延を小さくすることが可能になる．

この方法の特徴としては，前節の BATV と同様に，自ドメインの MTA に導入するだけで十分な効果を発揮する点が挙げられる．また，たとえば MTA2 を被害ドメ

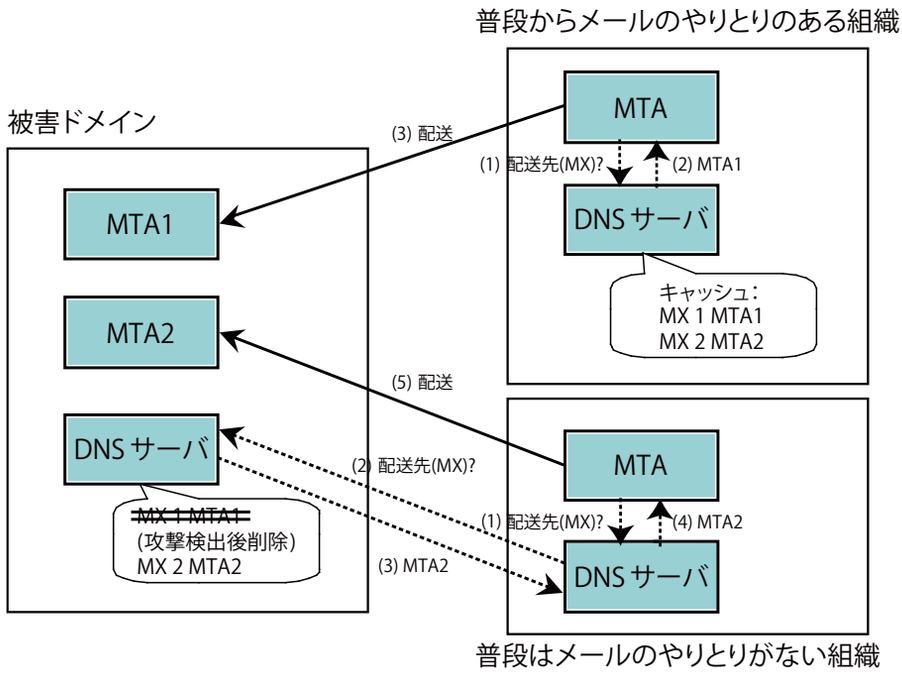

図 -4　DNS を用いた MTA の負荷分散

インの外部に設置することにより，バウンスメールによる輻輳を軽減することも可能である．一方，この方法の欠点として，普段から電子メールのやり取りがある組織でもキャッシュの有効期限切れや定期的なキャッシュ無効化により新たな電子メールを MTA2 に送ってしまう危険性がある点が挙げられる．この問題に対しては，問合せ元の DNS サーバに応じて異なる MX レコードを返す方法[5]が提案されているが，今後の検証が待たれるところである．

■ 今後の動向

バウンスメールによる被害は，発信者アドレスを特定のドメインのものに固定して発信する spam メールが最近ではあまり見受けられないためか，それほど重要視されていない．また，バウンスメール集中への対策手法の開発も，実際に被害に遭わなければ検証が困難であることもあり，他の問題点への対策と比べると進んでいない．

しかし，たとえばサイバーテロに用いられる潜在的な危険性は無視できず，実際に平成 17 年 1 月には靖国神社のメールサーバが以前から継続的に Joe job 攻撃を受けているとの報道があった．このような現状から，今後もバウンスメール対策の継続した開発および展開が望まれる．

参考文献
1）Klensin, J. (ed.): Simple Mail Transfer Protocol, RFC2821, IETF (2001).
2）吉田和幸，矢田哲二，原山博文，伊藤哲郎：spam メール対策と統合メール管理システムについて，情報処理学会論文誌，Vol.46, No.4, pp.1035-1040 (Apr. 2005).
3）Levine, J., Crocker, D., Silberman, S. and Finch, T.: Bounce Address Tag Validation (BATV), http://mipassoc.org/batv/draft-levine-mass-batv-00.txt, 2004.
4）山井成良，繁田展史，岡山聖彦，宮下卓也，丸山　伸，中村素典：発信者詐称 spam メールに起因するエラーメール集中への対策手法，第 3 回情報科学技術フォーラム情報技術レターズ，pp.313-316 (2004).
5）丸山　伸，中村素典，岡部寿男，山井成良：動的に応答が変化するネームサーバ技術のメール配送エージェントへの応用，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，2004-DSM-32-14，pp.79-84 (2004).

（平成 17 年 6 月 15 日受付）