1 電子メールの基礎知識

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

「1.1 世界の電子メールを spam 制御へ」(pp.741-746) でも紹介されているが，電子メール配送システム（MHS）は巨大なシステムであり，多くの構成要素が複雑に関係している．特に 2 部で紹介するような技術的側面での spam メール対策では，電子メール配送の仕組みを巧みに利用し，特に DNS との連携により実現しているものが多い．
そこで本稿では，spam メール対策技術を理解するために最低限必要な基礎知識を解説する．

電子メール配送プロトコル（SMTP）の概要

【配送手順】

SMTP[1), 2)] は，ユーザ（MUA）からメールサーバ（MTA）への，あるいは MTA から MTA への電子メール配送の際に標準的に用いられるプロトコルである．SMTP では，クライアント（MUA または MTA）からサーバ（MTA）への配送手順が以下のように定められている．

(1) TCP コネクションの確立

クライアントが電子メールを配送する場合，まず配送先のサーバを決定し（後述），そのサーバとの間で TCP コネクションを確立する．サーバは通常，クライアントに対して 220 番[☆1] で始まる応答（greeting メッセージ）を返す．

(2) 通信の準備

クライアントはサーバから greeting メッセージを受け取ると，通常クライアントは EHLO（Extended Hello）コマンドあるいは HELO（Hello）コマンドを送る．その際に引数としてクライアントの識別子（通常はドメインつきホスト名）を指定する．サーバは通常，クライアントに対して 250 番で始まる応答を返す．EHLO コマンドに対する応答では，利用可能な機能を示すキーワードの一覧が付加される．

ここまでの手順は，1 つのセッションにおいて 1 度だけ行われる．すなわち，1 つのセッションで複数の電子メール配送を行う場合には，(3) 以降の手順を繰り返して行うことになる．

(3) 発信者の指定

次に，クライアントは MAIL コマンドを用いてサーバ側に発信者アドレスを通知する．このアドレスは郵便において封筒に書かれる差出人に相当し，Reverse-Path，MAIL-FROM アドレス，エンベロープ From アドレスなどと呼ばれる．発信者アドレスに問題がないとサーバが判断した場合には，通常 250 番で始まる応答を返す．

(4) 宛先の指定

引き続いてクライアントは RCPT（Recipient）コマンドを用いてサーバに宛先アドレスを通知する．このアドレスは郵便において封筒に書かれる宛先に相当し，Forward-Path，RCPT-TO アドレス，エンベロープ To アドレスなどと呼ばれている．投函時に MUA で Cc（Carbon Copy）や Bcc（Blind Carbon Copy）などを用いて複数の宛先が指定された場合には，複数の RCPT コマンドが発行されることになる．宛先アドレスあるいは発信者アドレスと宛先アドレスの組合せに問題がないとサーバが判断した場合には，通常 250 番で始まる応答を返す．

(5) 本文の送付

ここでようやくクライアントは，本文を送ることができる．まずクライアントは DATA コマンドを送り，サーバから 354 番の応答を受信すると引き続いて本文を送る．本文の最後を表す「.」のみの行をサーバが受信すると，サーバは通常 250 番で始まる応答をクライアントに返し，受信したメールの処理（メールボックスへの格納や他の MTA への中継など）を行う．

本文はヘッダ（header）部分とメッセージ本体（body）部分から構成され，両者は空白行で区分される．ヘッダ中には From: で示される発信者アドレスが含まれるが，これは郵便において便箋に書かれる差出人に相当し，ヘッダ From アドレス，あるいは単に From アドレスと呼ばれる．

その後，クライアントは（3）以降の手順を繰り返してほかの電子メールを送ったり，QUIT コマンドを送ってセッションを終了したりする．

☆1 この番号（応答コード）については後述する．

以上のやりとりの例は「2.4 バウンスメール対策」の図 -1（p.763）に示されているので，ご参照いただきたい．

【応答コード】

サーバの応答は，クライアントの実装を簡単にするため，3 桁の数字から始まる文字列を用いることになっている．これにより，クライアントは 3 桁の数字の部分を識別するだけでコマンドが成功したのか失敗したのか判定することができる．

応答に使われる 3 桁の数字は，特に最初（最上位）の桁によって以下のように分類できる．

200 番台　肯定完了応答（Positive Completion reply）
300 番台　肯定中間応答（Positive Intermediate reply）
400 番台　一時的否定完了応答（Transient Negative Completion reply）
500 番台　恒久的否定完了応答（Permanent Negative Completion reply）

ここで重要なのは，400 番台と 500 番台の違いである．すなわち，400 番台はメールボックスの容量制限などのために一時的に発生したエラーを表し，一定時間後の再送を促しているのに対して，500 番台は宛先不明などの理由により再送しても受理されないエラーであることを意味する．

DNS との連携

電子メールの配送には DNS（Domain Name Service）[3] が深く関連している．DNS はドメイン名に対して IP アドレスなどの情報（リソースレコード，RR）を検索する仕組みを提供する，巨大な分散システムとみなすことができる．すなわち，DNS では各ドメインに対応する DNS サーバがインターネット上に多数配置され，それらが相互に協調しながら動作するように工夫されている．

IN クラス（TCP/IP に対応する）で用いられる代表的なリソースレコードと意味を以下に示す．

A（Address）　ホスト名に対する IP アドレス（IP version 4 用）
MX（Mail eXchange）　ドメイン名に対する MTA☆2
CNAME（Canonical NAME）　別名に対する正式名
NS（Name Server）　ドメイン名に対するネームサーバ
PTR（PoinTeR）　主に IP アドレスに対応するホスト名
TXT（TeXT）　ドメイン名に関連するテキストデータ

このうち，電子メールの配送に最も関連しているのが MX である．MTA は電子メールを受け取ると宛先アドレスの @ 以降の部分をキーとして MX レコードを検索し，最も優先度の高い（数値の小さい）レコードの MTA から順に（同じ順位のものが複数あればそれらの間ではランダムに）配送を試みる．

また，PTR はサーバがクライアントの IP アドレスをもとにそのホスト名を求める場合に使う．たとえば，クライアントの IP アドレスが AAA.BBB.CCC.DDD の場合，DDD.CCC.BBB.AAA.in-addr.arpa に対する PTR を検索すれば，そのホスト名を得ることができる．

DNS はスケーラビリティについても十分配慮されている．DNS ではドメイン名が階層構造になっているため，何の工夫もなければ上位ドメインに対応する DNS サーバに問合せが集中しがちである．実際の DNS ではこの問題を解決するため，DNS クライアントにキャッシュを設け，同じリソースレコードの問合せが頻繁には発生しないように工夫されている．ただし，キャッシュの有効期限を長くするとリソースレコードの一貫性に支障が生じるため，有効期限（Time To Live, TTL）をレコードごとに管理者が設定できるようになっている．

spam 対策技術の性能評価基準

2 部で紹介するように，現在までに多くの spam 対策技術が提案されている．これらの技術を比較する場合，問題となるのが評価基準である．実際には spam メールを通常メールと判定してしまう誤りを false negative と呼び，その割合（false negative rate）が性能評価基準として使われる．この値は「spam 見逃し率」とも呼ばれ，1 からこの値を引いた「spam 検出率」とともに最もよく使われる性能評価基準である．一方，実際には通常メールであるものを spam メールと判断する誤りを false positive と呼び，その割合を false positive rate と呼ぶ．この用語の代わりに日本語の「spam 誤検出率」が使われることも多い．

false negative rate と false positive rate は一般にはトレードオフの関係にあるが，実際には false positive rate のほうが重要であり，これが十分小さくないと実用にはならない．これは，false negative が発生した場合には，検出漏れの spam メールを利用者が判断して削除する必要があるという比較的小さな影響が生じるだけであるが，逆に false positive が発生した場合には，重要な通常メールが誤って配送されないかもしれず，そうなると大きな損害を利用者に与えることになるためである．

このほかにも，管理者の手間，MTA の負荷，適用範囲の広さなど，さまざまな性能評価基準が存在するが，誌面の都合上割愛する．

☆2　優先順位 (preference) つきで複数指定可能．

参考文献
1）Postel, J. B.: Simple Mail Transfer Protocol, RFC821, IETF（1982）.
2）Klensin, J.（ed.）: Simple Mail Transfer Protocol, RFC2821, IETF（2001）.
3）Mockapetris, P. : Domain Names - Concepts and Facilities, RFC1034, IETF（1987）.

（平成 17 年 6 月 14 日受付）