第2章 メールの仕組みと課題

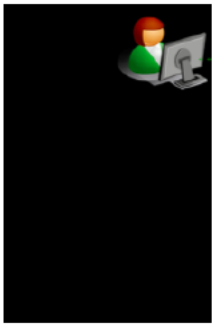
第2章　メールの仕組みと課題

本章では、送信したメールが受信者に届くまでの仕組みについて解説します。また、迷惑メールがなぜ受信者に届いてしまったり、受信側で迷惑メールを防ぐのが難しかったりする原因となっている、メール配送の課題についても解説します。

なお、ここでは、携帯電話で利用する SMS (Short Message Service) など宛先に電話番号を指定する方法ではない、PC で送受信するドメイン名を @（アットマーク）で区切るメールアドレスを宛先に指定するメールを対象とします。

2.1　メールシステムの概要

メールの送信者が作成したメールは、インターネット上の幾つかのサーバを経由して受信者に届けられます。図表２－１ に、example.com ドメインを利用している送信者が、example.jp ドメインを利用している受信者へメールが届けられるまでの流れを示します。



図表２－１　インターネットでのメール送信

図表２－１の説明

1　要素

Mail Transfer Agent　（MTA：メール転送エージェント）

メールを異なるメールシステム間で転送する役割を持ち、他の MTA や MSA と SMTP プロトコルなどを利用してメールの送受信を行う機能を提供します。

メールの宛先に応じて転送する先を振り分ける機能や、受信側のシステムで受信する準備ができていない場合などに一時的にメールを保存（キュー）する機能などを持ちます。

一般にサーバ・アプリケーション・プログラムとして実装されます（例： sendmail 、 Postfix 等）。

Mail User Agent　(MUA：メール・ユーザ・エージェント)

エンドユーザがメールを作成し、送信する（MSA にメールを投稿する）機能や、受信したメールをエンドユーザが読む（メール・スプールから読み出し、表示する）ための機能を提供します。

MUA から MSA へのメールの送信は、一般に SMTP プロトコルを利用して行われます。また、メール・スプールからの読み出しは、 Post Office Protocol 3 （POP 3） や Internet Message Access Protocol 4 （IMAP 4） プロトコルを利用して行われます。

一般的にエンドユーザの端末上で動作するアプリケーションとして実装され、メールクライアント、メールソフト等と呼ばれる場合が多いです（例：Microsoft 社の Outlook や Mozilla の Thunderbird 等）。

Mail Submission Agent　（MSA：メール・サブミッション（投稿）・エージェント）

エンドユーザにより作成されたメールを MUA などから受信し、メールの配送を開始する機能を提供します。

MTA の役割をもつサーバ･アプリケーション･プログラムが MSA を兼ねる場合もあります。MSA から MTA へ SMTP プロトコルを利用してメールを送信すると、 MTA は、次の配送先（他の MTA や MDA ）へメールを転送します。

Mail Delivery Agent　（MDA：メール・配送・エージェント）

メールの受信側（宛先）で、MTA からメールを受信し、メール・スプールへメールを保存する機能を提供します。

MTA の役割をもつサーバ・アプリケーション・プログラムが MDA を兼ねる場合もあります。

Mail Spool　（MSPOOL：メール・スプール）

メールの受信側（宛先）で、エンドユーザが MUA を利用してメールを読み取るためにメールを保存する機能を提供します。Mail Box と呼ぶ場合もあります。

2　処理

① ドメイン example.com のエンドユーザが、 MUA を利用してメールを作成
② エンドユーザは、 MUA を操作し、 MSA にアクセスしてメールを送信（投稿）
③ MSA は、受け取ったメールを MTA へ配送
④ MTA は、宛先ドメインの MTA を見つけ出して、その MTA へメールを配送
⑤ 受け取った宛先ドメインの MTA は、内部の MDA へメールを配送
⑥ MDA は、メール・スプールへメールを届け、メール・スプールでメールを格納
⑦ 宛先のエンドユーザは、MUA を利用してメール・スプールへアクセスし、自分宛のメールを読み出す

③④⑤のメールの配送では、複数の MTA を経由する可能性があります。最近では、アンチウィルスフィルタや迷惑メールフィルタなどを運用しているドメインも多く、そうしたフィルタを用いたフィルタリングは MTA で実施されている場合が多く、１つのドメインの内部であっても複数の MTA を経由してメールが配送されることが一般的になっています。

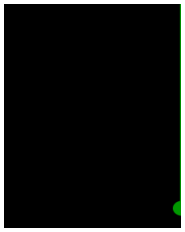
また、④で宛先ドメインの MTA を探すときに、送信元の MTA は、宛先ドメインの DNS 上の MX レコードを参照します。 MX レコードとして登録されているホストは、そのドメインにおいて外部ドメインからのメールを受信する役割をもつホストと解釈されます。

2.2　メール配送の手順

メールを宛先に届けるための配送手順として、SMTP (Simple Mail Transfer Protocol, RFC5321) が使われます。

メール配送では、メールを送りたい側（送信側)が、メールを届けたい先（受信側）にネットワーク的に接続を要求し、受信側が要求を受理することにより、一連の配送手続が開始されます。そして、実行したいコマンド名とその引数を相手方に送信し、相手方がそれに対する応答を返信するやりとりを繰り返すことにより手続が進みます。なお、メール送信は、送信側から受信側へ処理を伝えるので、ほとんどの場合、送信側が受信側に実行したいコマンドを送信することになります。

このときの接続の方法やメールの受け渡し、受信側からの応答の仕方などを決めたものが SMTP です。SMTP での手続の一般的な流れを図表２－２に示します。



図表２－２　SMTP によるメール通信手順

送信側では、処理の内容を示すコマンド（MAIL, RCPT, DATA など）を、引数とともに受信側に伝えます。例えば、MAIL FROM で送信者の情報（メールアドレス）を、RCPT TO で宛先の情報（メールアドレス）を、DATA でメール本体の情報を伝えます。

受信側では、それぞれのコマンドを解釈して応答をします。コマンドに対する応答の種別は、数字（220 や 250 などの３桁の数字）で示されます。例えばメールを受け取れない場合には、否定的な応答番号（500 番台の数字）を返すことになります。受信側は、このようなコマンドに対する応答という形で、受信側の判断や意図を送信側に伝えることができます。

SMTP の規格（RFC5321)では、送信側が指定する各コマンドの形式や順番、それぞれのコマンドに対して受信側が返すことができる応答番号の種類などが定められています。

こうしたメールの配送時に指定される、送信者や宛先のメールアドレスなどは、郵便の手紙になぞらえてエンベロープ(封筒)情報とも呼ばれます。

なお、SMTP は、メールサーバ間の配送時だけでなく、利用者がメールを作成する MUA（メール

ソフト）からメール投稿サーバ（MSA）への送信時にも使われます。

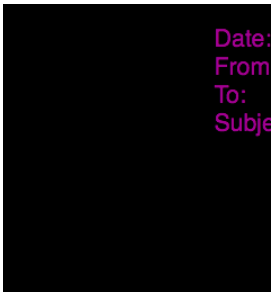
2.3　メール本体の構造

メール本体は、送信側が DATA コマンドを送信し、受信側がその応答として "354" を返した場合に、送信側から送信されます。メール本体の最後に、ドット (".") 文字だけの行（ドット行）が送信されます。なお、この場合のドット行は、メール本体には含まれません。

メール本体は、ヘッダ領域とメール本文によって構成されます。いずれの領域もテキスト文字列で表現され、専用の区切り記号は決められていませんが、文字列の構成方法によって区別ができるように決められています。

ヘッダ領域は、メール本体の先頭からヘッダ行が連続する領域で、ヘッダ行ではない空行 (改行だけの行) がメール本文との区切りとなります。

メール本文は、ヘッダ領域の区切り(空行)から、メール本体の末尾までとなります。メール本体の例を図表２－３ に示します。



図表２－３　メール本体

ヘッダ行は、ヘッダ名と続くコロン（":"）、ヘッダ本文で構成されます。ヘッダ行はそれぞれ形式や構文が決まっており、ヘッダを追加する場合には、正しく構文に従って記述しなければなりません。

なお、メール本体の構造及びヘッダ行の構文については、SMTP の規格（RFC5321）とは別に、Internet Message Format（RFC5322, インターネットメッセージの形式）で決められています。

2.4　メールの送信者情報

2.4.1　概要

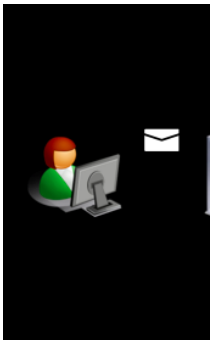
メールの作成者や送信者を示す情報には、メールの配送時に指定される送信者情報（エンベロープ情報に含まれる送信者情報）と、メール本体のヘッダ領域に記述される送信者情報の 2 種類があります。これらの送信者情報は、メールで利用される情報なので、いずれも、メールアドレスで示されます。

2.4.2　メール配送時に指定される送信者情報

メールの配送時に指定される送信者情報は、図表２－２ で示した MAIL コマンドの引数として指定されるメールアドレスです。このメールアドレスは、配送上で何か問題が発生した場合に送信者に通知を送る際に利用されます。そのため、リバースパス（reverse-path）という

名称が付いています。リバースパスは、SMTP によるメールの配送時に渡される情報なので、一般にはメールの受信者には渡されない情報になります。

なお、受信側の MTA は、この MAIL コマンドに対する応答として、メールを受け取らないことを示すエラーコードを返すことができます。例えば、指定されたメールアドレスが明らかに実在しないものであった場合や、過去に迷惑メールを送信してきた送信者であった場合などには、受け取らないことを応答コードで示すことができます。また、受信側の MTA が、一旦メールを受け取った後で、MDA (Mail Delivery Agent) 上でメールスプールに保存ができなかった場合や宛先が実際には存在しなかった場合など何らかの問題があった場合には、このリバースパス宛にエラーメールを送信することになります。



図表２－４　エラーメールの送信例

2.4.3　ヘッダ領域に記述される送信者情報

ヘッダは、メール本体の一部として受信者に届けられるため、受信者が見ることのできる情報です。しかし、ヘッダにはたくさんの種類があるために、受信者が利用する MUA (Mail User Agent, メールソフトウェア) の多くは、全てのヘッダを表示しません。送信者情報を示すヘッダの仕様としては図表２－５に掲げるものがありますが、MUA が送信者情報として表示する情報は、通常は From ヘッダになっています。

ヘッダ名	用途
Sender	メール送信を実際に行った送信者を示す情報
From	メールの作成者を示す情報
Reply-to	返事を送信する場合の宛先を示す情報

図表２－５　ヘッダ上の送信元アドレス

Sender ヘッダが最も良く使われるケースとしては、メーリングリストがあります。メーリングリストでは、リストへの投稿者が From ヘッダに示されます。しかし、リストメンバへの送信は、実際にはメーリングリスト機能を実現するプログラムなどが配送しています。そのため、Sender ヘッダにはメーリングリストの管理者などのメールアドレスが示されることになります。また、今ではあまり行われないかもしれませんが、例えば実際のメール内容の作成者に

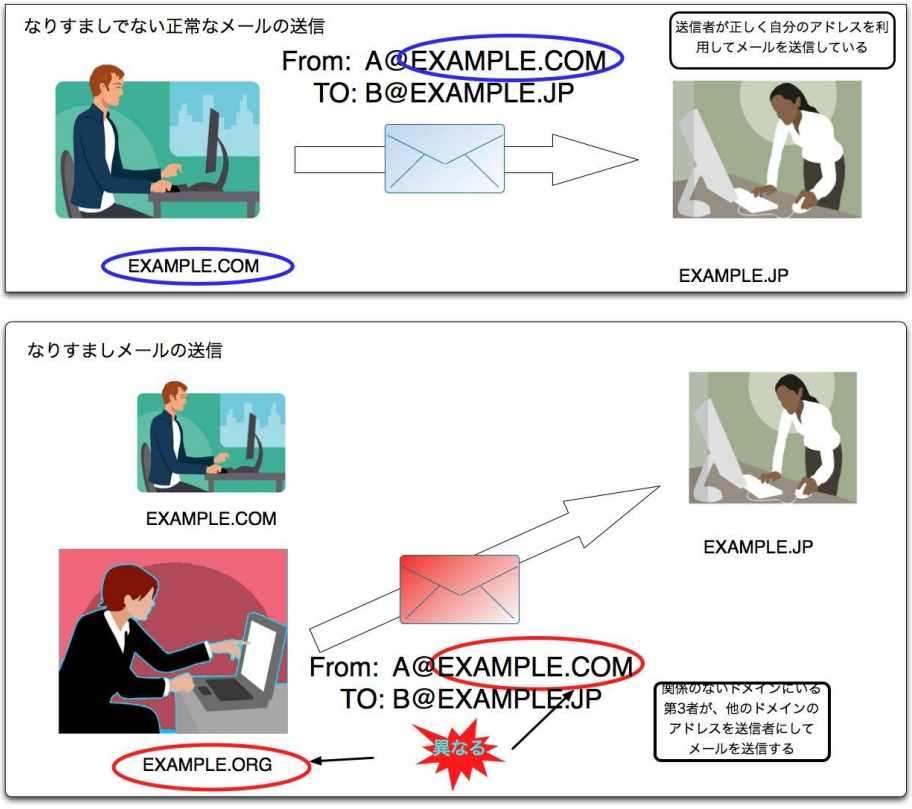
代わって秘書がメール送信するような場合に、送信者のメールアドレスを Sender ヘッダに示されることがあります。

From ヘッダの使われ方にも注意すべき点があります。From ヘッダには、メールアドレス以外にも、補助情報としてディスプレイネーム（display-name）を追加することができます。ディスプレイネームには、任意の文字列を使用できますので、From ヘッダ上に示されたメールアドレスと全く関係の無い名前や文字列が使えます。MUA や Web ブラウザでメールの送受信を行ういわゆるウェブメールシステムの多くは、送信者情報として、このディスプレイネームを優先して表示しますので、送信者情報として表示される文字列は、実際の送信者情報とは全く関係が無いかもしれないものとなっているのです。

2.5　送信者情報詐称の問題

2.5.1　送信者情報詐称を判断する仕組み

メールシステムにおける送信者情報には、2.4 でみたように、用途に応じた複数の種類があります。しかし、これまで、いずれの送信者情報についても、それが正しく名乗られているかを判断する仕組みがありませんでした。もともとの電子メールシステムは、インターネットが現在のような形で普及する以前から存在してきたシステムであり、メールの利用者が限られていた時代から少しずつ拡張されて使われて続けているために、現在のように送信者情報が詐称されることを予め想定していなかったためです。



図表２－６　なりすましメール送信例

そのため、これまで受信側では、経験的な運用方法として、例えば、送信者情報として、存在しないドメイン名が指定された場合や、日本の有名ドメインを名乗っているものの海外など明らかに異なった送信元からのメールだった場合に受信を拒否するなどの工夫をしてきました。

しかし、それらの場合であっても、ドメイン名を管理する DNS(Domain Name System) が単に不調であったり、海外からメール転送をしていたりする場合など、ごくまれに送信者情報を故意に偽装したものではない、正しい送信である場合があります。

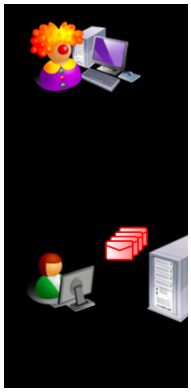
2.5.2　送信者情報詐称の問題点

メールの送信者情報が詐称されることによって、様々な問題が出てきています。

まず、受信側で、迷惑メールを受信しないために、送信者情報をもとに受信を拒絶しようとしても、詐称されていることにより、的確に受信の拒絶ができないことがあります。

また、実在する送信者を詐称し、実物とは異なる偽のウェブサイトに誘導し、個人情報を搾取するなどの犯罪行為（フィッシング）や、信頼性のある送信者を騙り、メールに添付された不正プログラムを実行させ、外部からコントロールされるボットにされたり、PC 内部にある個人情報や操作過程で得られる個人情報を搾取するなどの行為が行われています。

さらに、迷惑メールは宛先が存在するかどうかにかかわらず大量に送信される傾向にあるため、リバースパスを詐称し、実在するメールアドレスを指定している場合に、宛先が不明であることによるエラーメールが、詐称されたメールアドレスに宛てて大量に送信される、バックスキャッタ（backscatter）が大きな問題となってきています。その場合には、そのエラーメールが迷惑メールと判断され、迷惑メール判定機能を提供しているベンダやブラックリストを運営している組織に報告され、正しい処理としてエラーメールを送信している側（最初のメールの受信側）が、迷惑メール送信者として登録され、同じ出口から送信される通常メールまでもが、迷惑メール扱いされて届かなくなる、という 2 次的な問題も発生しています。



図表２－７　バックスキャッタ問題

2.5.3　送信ドメイン認証技術

このように、送信者情報が簡単に詐称できてしまい、それを受信側で簡単に判断することができない現在のメールの仕組みにより、大きな問題が生じています。これに対応するために、送信ドメイン認証技術が開発されており、その普及により、送信者情報詐称の問題点を防ぐことが可能になります。