第２回　ｅメールが届く仕組み

インターネットを利用したサービスにおいてよく使われているのが「ｅメール」です。今やｅメールはビジネスにおいても日常生活においても電話と並ぶ身近なコミュニケーション手段の一つとなっています。

ｅメールの仕組みは、アプリケーションソフト（メールソフト、メーラー、メールクライアントソフトなどと呼ばれる）によって作成された文書データが「TCP/IP」によりパケット化され、各種のサーバを介して送信先に送り届けられるというものです。

【今回登場するキーワード】

「（メール）サーバ」
「SMTP（Simple Mail Transfer Protocol　エスエムティーピー）」
「POP3（Post Office Protocol　ポップスリー）」
「DNS（Domain Name System）ドメインネームシステム」
「バウンスメール」
「メールヘッダー」
「添付文書と BASE64（ベースロクヨン）」
「迷惑メール」
「Web メール（ウェブメール）」

■メールシステムを支える各種のサーバ

インターネット上でメール文書が間違いなく相手先に送り届けられるのは、各種のサーバがそれぞれ連携して働いているからです。メールシステムは次のようなサーバの働きによって機能しています(図１)。

１）メールの送信・受信に関わる「SMTP（Simple Mail Transfer Protocol）サーバ」
２）受信したメールを蓄積し、要求に応じて目的のメールをユーザー端末に渡す「POP（Post Office Protocol）サーバ」
３）送信先メールアドレスに対応する送信先 IP アドレスを探し出す「DNS（Domain Name System）サーバ」

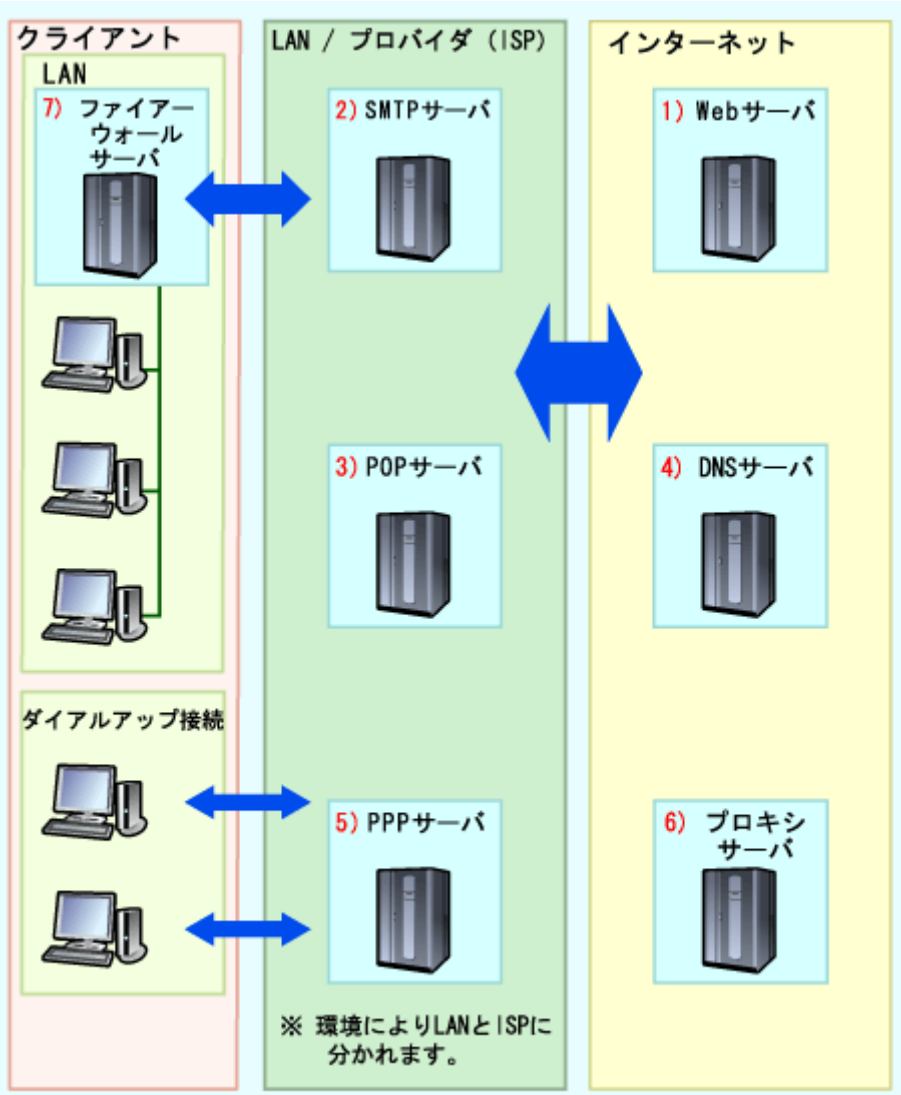
あらためて「サーバ」について説明しておきましょう。「サーバ」とはサーバコンピュータのことで、その基本的仕組みは PC と同じです。ただサーバコンピュータはネットワークに接続して 24 時間稼働するので連続運用にも耐えられる信頼性や、稼働したままメンテナンスができるなどの機能を備えています。

このような信頼性の高いサーバコンピュータに各種のソフトウェア、例えばSMTPのプログラムをインストールすれば1)の「SMTPサーバ」に、またDNSのプログラムやデータをインストールすれば3)の「DNSサーバ」として機能し始めるのです。1台のサーバに複数のプログラムをインストールしていくつもの働きをさせることも可能ですが、やり取りするデータが膨大になることを考慮し、単機能で動作させるのが一般的です。

●インターネットの多様な機能を支える多様なサーバ

LANやインターネットの世界でデータをやり取りする上で重要な働きをしているのがサーバです。LAN環境で働くサーバとしては複数の端末でデータを共有する「ファイルサーバ」や、ネットワークを介して1台のプリンタを共有するための「プリンタサーバ」などがあります。一方、インターネットやイントラネットなどTCP/IPネットワークの世界で働くサーバには、次のように数多くの種類があります。

1) Webサーバ
Webページのファイルを記憶し、ブラウザソフトからのリクエストに応えてファイルデータを配布する。
2) SMTPサーバ
メール送信を担当するサーバ。PCから送られたメールを受け取って、相手のメールボックスにメールを送り届ける。
3) POPサーバ
SMTPサーバから送られメールボックスに蓄積したメールを、PCからの要求に応じて取り出す。
4) DNSサーバ
IPアドレスとドメインネームを変換するサーバ。
5) PPP（Point-to-Point Protocol）サーバ
ダイヤルアップでインターネットに接続する場合の橋渡し役をするサーバ。
6) プロキシサーバ
LANとインターネットの間に位置し、LAN内のPCの代理としてWebサーバにアクセスする役割を持つ。
7) ファイアーウォールサーバ
LANとインターネットの間に位置し、インターネットからLANへのアクセスやデータの漏洩を防ぐ。



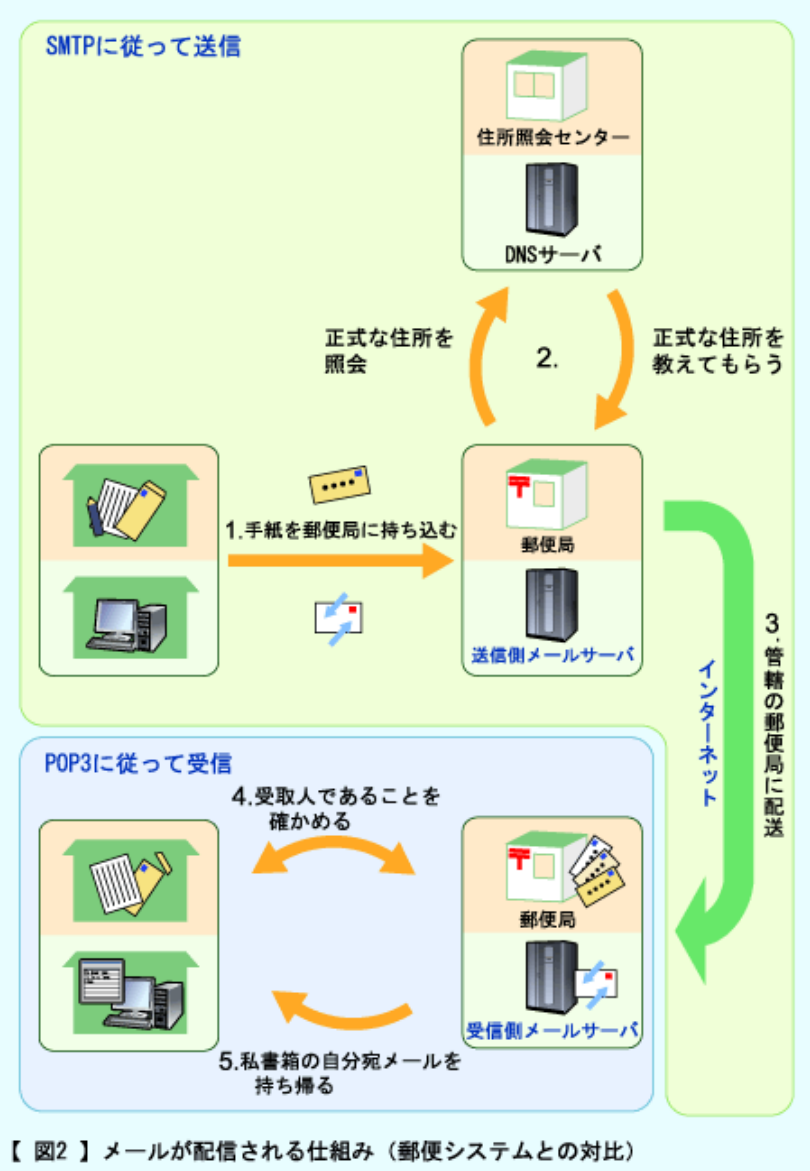
【 図1 】各種サーバの働き

■メール送信の仕組み

ｅメール送受信は次の５つのステップを経て行われています。

メールソフトで作成したデータをメールサーバ（SMTP サーバ）に送信
↓
メールサーバが DNS サーバに対して送信先 IP アドレスを照会する
↓
送信先 IP アドレスを持つメールサーバに向けてメールデータを送信
↓
送信先ユーザーが認証のうえで送信先メールサーバをチェック
↓
受信メールを取り出す

この５つのステップを郵便システムに置き換えてみると次のようになります。



【 図2 】メールが配信される仕組み（郵便システムとの対比）

ｅメールシステムの場合、ユーザーはメールソフト上でメール文書を作成し、送信ボタンを押すだけで受信側のメールサーバに送り届けられますが、裏側では図２のようにメールサーバ、DNS サーバが連携して働いています。

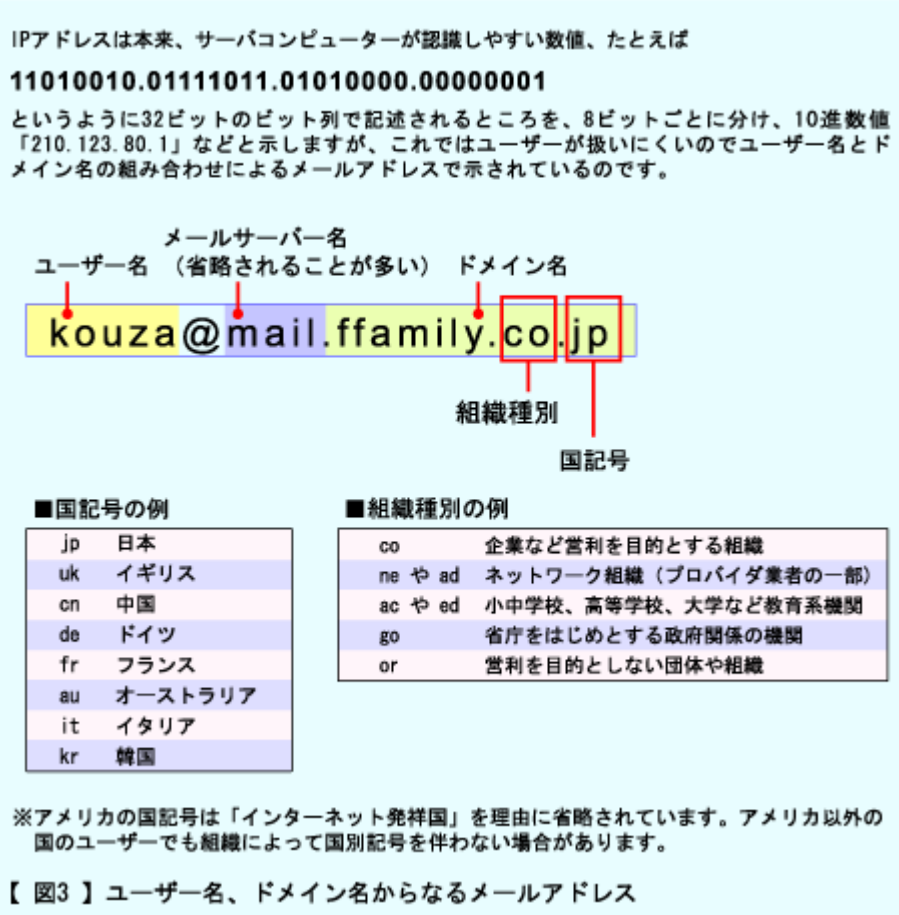
１）メールソフトで作成されたデータは、まず送信側のメールサーバ（SMTP サーバ）に送られる

この時のやり取りは SMTP と呼ばれるプロトコルにしたがって行われます。少し詳しくみると SMTP は TCP/IP プロトコルの上位で働いています。つまり、まずメールソフトがメールサーバに対して TCP で接続状態を作りだし、その上で SMTP にしたがってデータをメールサーバに送信しているのです。個人で ISP を利用している場合、メールサーバは ISP 内にあり、企業では社内 LAN に設置されていることが多いようです。

２）メールサーバは受け取ったメールの宛先アドレスを DNS サーバに照会する

ｅメールで使われているメールアドレスは郵便システムの宛先住所・氏名に当たるもので、ｅメールが間違いなく相手先に届く手がかりとなるものです。メールアドレスは図３のようにユーザーに分かりやすいよう表記されているのですが、メールサーバは受信側の IP アドレスを識別して送信するので、メールアドレスを IP アドレスに置き換える必要があります。これを行うのが DNS（Domain Name System）です。メールサーバは最寄りの DNS サーバに照会してメールアドレスに対応する IP アドレスを教えてもらい、同アドレスのメールサーバにメールデータを送信します。郵便システムでは宛名から判断して郵便物を配送するのは人間なので、宛名は一貫して文字でよいのですが、ｅ メールシステムでは文字を頼りに送信・受信の手続きをする人間の他、「１」「０」の数値を読み取るコンピュータが介在します。そのためにメールアドレスと IP アドレスを照合する DNS が必要となります。

DNS サーバはインターネットメールの要となる装置であることからプライマリーとセカンダリーの複数の DNS を設置する場合があります。企業などはとくにメールシステムの信頼性を高めるためにセカンダリーDNS を外部に設置するなどしています。



【 図3 】ユーザー名、ドメイン名からなるメールアドレス

３）送信側メールサーバはメール転送プロトコル SMTP にしたがって、メールデータを送信先メールサーバ（SMTP サーバ）に転送

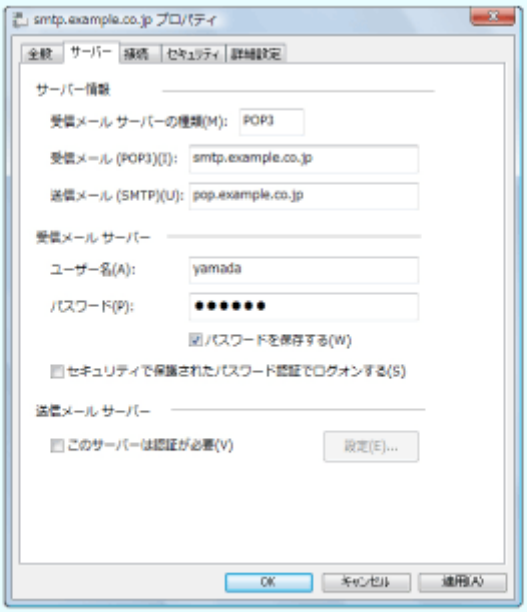
この時も、まず TCP プロトコルによって受信側メールサーバとの間に接続状態を作り出し、その上で SMTP に従いデータを送信しています。

４）受信側ユーザーはメールソフトを使い、POP３プロトコルにしたがって確かに受信側ユーザーであることを認証してもらう

メール送信時は SMTP に従いましたが受信時は POP3 によって行われます。受信時のプロトコル POP3 の特徴は認証の手続きを行う点にあります。認証はもちろん、本来の受信者以外のユーザーが誤ってメールを受け取ることがないようにするものです。メールソフトの設定で「受信メールのユーザー名とパスワード」を設定するのはこのためです（図４）。

５）認証後、POP３に従ってメールサーバ内の着信メールを確認し取り出す

現在、POP は最新バージョンの「POP３」が使われています。また「POP3」のほか、「IMAP4（Internet Message Access Protocol４　アイマップフォー）」と呼ばれるプロトコルも使われています。「IMAP4」はモバイル機器用メールソフトとしてよく使われ、タイトルや発信者を確認してから受信するかどうかを決めることができるなどの特徴を持っています。



【 図4 】メールシステムを利用するには、メールソフトの設定画面でPOP3サーバ、SMTPサーバを指定しておく必要がある。

■メール送信時のエラーメッセージの意味

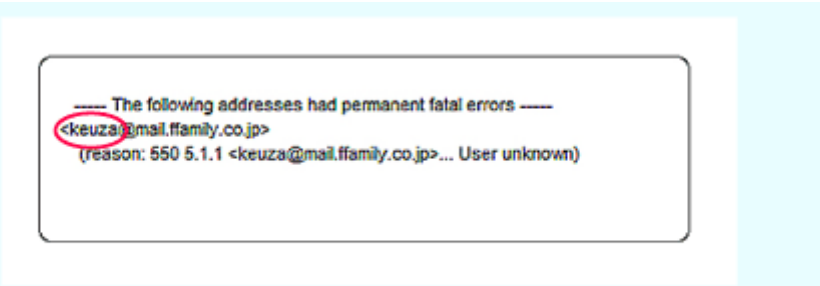
何らかの理由で相手先の SMTP サーバがメールを受信できない場合、エラーが発生したことを知らせる「バウンスメール」が返信されてきます。バウンスメールに記載されるメッセージには次のような種類があり、その内容からおおよそのエラー原因を知ることができます。

「User unknown」＝ユーザーが不明。（図１の受信側ユーザーが存在しない）

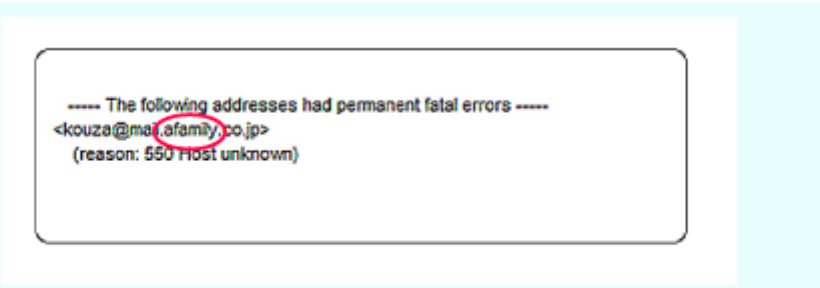
「Host unknown」＝ドメイン名が不明。（図１の受信側メールサーバが存在しない）

「Message size exceed fixed maximum size」＝メールのサイズが大きすぎて受信できない。

「Mail box full」＝受信側のメールボックスが満杯で受信できない。



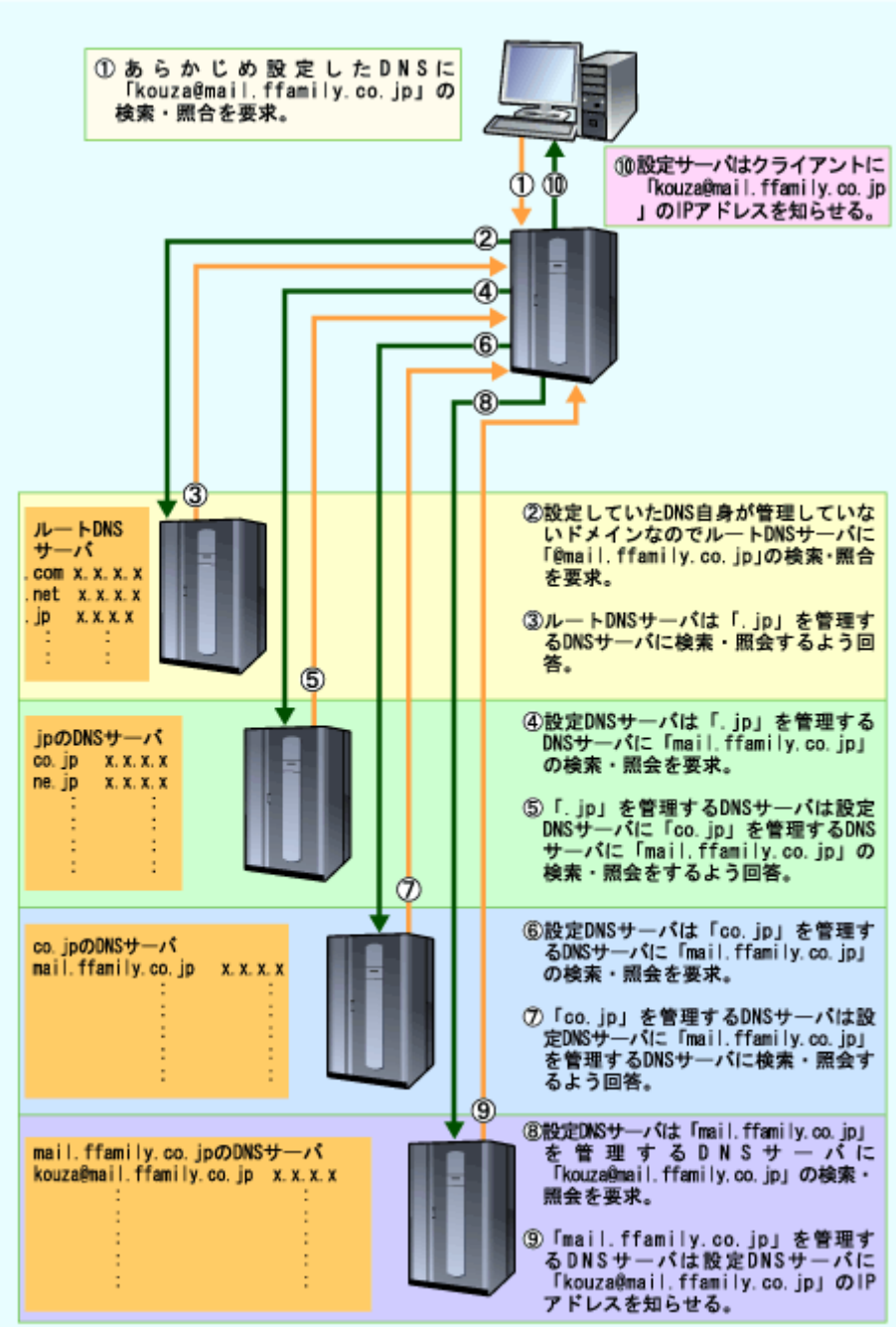
【 図5 】「kouza」となるべきところを「keuza」となっているために「User unknown」のメッセージが表示された。



【 図6 】「ffamily」となるべきところを「afamily」となっているために「Host unknown」のメッセージが表示された。

●世界中の IP アドレスとメールアドレスを照合する DNS の仕組み

インターネット上には何万台もの DNS サーバがあります。あるドメイン名に対応する IP アドレスを検索してもらう場合、何万台もの DNS を総当たりで調べるわけにはいきません。そこで DNS では DNS サーバを階層化し(図７)、下位のドメインを管理する DNS サーバをすぐ上位の DNS サーバに登録するというように順に登録する方法を採っています。このように階層ごとの DNS がドメイン名と IP アドレスのデータを分担して保持すれば、国別のドメイン記号を管理する DNS サーバから、下位の組織種別のドメイン記号を管理する DNS サーバへとたどる方法で容易に、効率的に目的のドメイン名と IP アドレスを分担にたどり着くことができるわけです。



【 図7 】階層化されたDNSサーバとIPアドレス照会の仕組み

■電子メール１通ごとに付けられる「メールヘッダー」

受信したｅメールのそれぞれには図８のような「メールヘッダー」と呼ばれるデータがついています。メールヘッダーにはメールの送信者、受信者、経由したサーバや題名などが書き込まれており、受信側のメールソフトはこのメールヘッダー情報をもとにして受信メール一覧の表示、返信時のアドレスを書き込んでいるのです。

ほとんどのメールソフトでは、普段メールヘッダーは表示されない設定になっていますが、「メールヘッダーを表示する」などのメニューを選択することで簡単に表示することができます。メ

ールヘッダーの最初の部分には、メールが経由してきたメールサーバが下から順に記述されています。送信メールが何らかの理由で戻ってきた場合、メールヘッダーを表示し「Received」の欄をたどっていくと、どこまで届いていたか確かめることができます。

赤字：メールヘッダを構成する要素
黒字：内容（メールごとに内容は異なる）

経由するサーバごとに書き込まれる	Received: from mailserver.ffamily.co.jp([172.23.1.116]) by mail01.aabb.jp with SMTP Mon, 25 Jun 2007 17:47:52 +0900 (JST)
経由するサーバごとに書き込まれる	Received: mailserver.ashita.co.jp([210.188.220.149]) by mail01.xyz.jp(xyz-Fsecure); with SMTP 25 Jun 2007 17 17:47:47 +0900
送信側メールソフトによって書き込まれる（メールソフトによって記述が異なる）	Message-ID: <004c01c7b705$8e2afd50$1f01a8c0@TOSHIBA986A84B> From: taro@ benkyou.co.jp To: 会員・花子様 <hanako@.ffamily.co.jp> Subject: インターネット講座の案内 Date: Mon, 25 Jun 2007 17:47:59 +0900 MIME-Version: 1.0 Content-Type: text/plain X-Priority:3 X-MSMail-Priority: Normal X-Mailer: Microsoft Outlook Express 6.00.2800.1807
	（1行分の空きスペース）
メール本文が続く	こんにちは。インターネット講座の案内です。 ・ ・ ・

メールヘッダ要素と内容の意味

メールヘッダ要素	内容の意味
Received	経由してきたサーバのIPアドレス、経由の日時・時刻など
From	送信者メールアドレス
To	メールの宛先
Subject	メールタイトル
MIME-Version	MIMEのバージョン
Content-Type	テキストやHTMLの形式
X-MSMail-Priority	メールの優先順位（マイクロソフトのOutlookの場合。他のメールソフトでは書かれない。）
X-Mailer	送信者側のメールソフト名

【 図8 】メールヘッダーの例

■MIME で送信される日本語やデータ

インターネットのｅメールシステムで使われるプロトコル SMTP は、もともと英語圏のテキストである ASCII（American Standard Code for Information Interchange アスキー）コードをやり取りする前提で設計され、これと異なる日本語文字や 1 行が 1000 文字を超える長文データ、また画像や音声、アプリケーションデータなど（バイナリーデータ）は送信できませんでした。この制約を SMTP に手を加えずに取り払い、ASCII 文字以外の文字、たとえば日本語や画像、動画や音声データ、表計算データなどを送信できるようにする規格が MIME（Multipurpose

Internet Mail Extensions　マイム）です。

実際にｅメールで画像データなどを送る場合「添付ファイル」をクリックする操作を行いますが、この時メールソフトは画像データを ASCII コードに変換（エンコード）しているのです。また受信側が、受け取った添付ファイルを開封する場合、メールソフトはエンコードされたデータを画像データに戻して（デコード）いるのです。MIME ではエンコード方式として Base64 と呼ばれる方式を採用しています。

●Base64 の考え方

そもそも、インターネットのメールシステムに用いられるテキスト（ASCII コード）がなぜ 7 ビットなのか？　それは ASCII コードが制定された 1963 年当時、コンピュータが扱うデータの最小単位は 8 ビット（8 桁の０と１）で、8 ビット目を通信における誤り検出（パリティチェック）用ビット（パリティビット）として使用していたこと、そして 7 ビット＝128 通り以内でアルファベットの大文字、小文字、数字や@、%、？（）などの記号類、空白文字などを表すことができたからです。

しかしインターネットが世界中に普及し、ASCII コードによる文字つまり英語圏以外の文字や、画像や音声など 8 ビットで表されるデータをメールシステムでやり取りする必要性が高まり 1992 年に MIME が登場します。MIME の登場によってインターネットメールは「7 ビットの呪縛」から解き放たれ、広く世界の文字文化とｅメールとを結び付けたことになります。

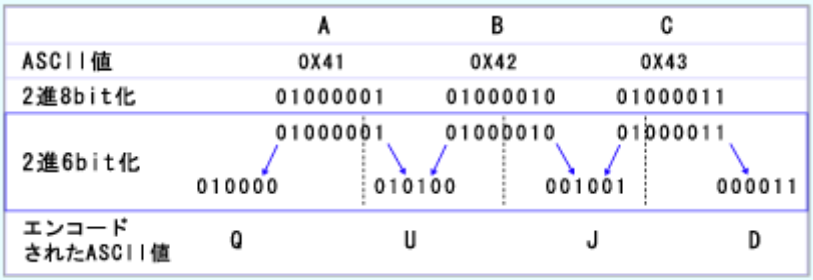
この MIME で採用されている Base64 とは、英数字 ASCII 文字だけを用いて英数字以外の文字やバイナリーデータを表すデータ変換（エンコード）方式で、名前の「64」はエンコードに用いられる ASCII 文字の A～Z、ａ～Ｚ、0~9 と記号類（＋と／、＝）の合計 64 に由来しています。

Base64 の手順は(英数字の場合)、

１）エンコードしたい元データの文字列を前から順に３バイト（3×8 ビット=24 ビット）ずつ取り出し、これを６ビットずつに分割し直す（６ビットに満たない部分には 0　を追加して６ビットに揃える)。

２）６ビットに分割した 2 進数に対応する ASCII コードの文字、数字、記号に置き換え（エンコード)。

例えば文字列「ABC」（3 バイト）を Base64 でエンコードしてみましょう。



【 図9 】Base64によるエンコードの方法

日本語を置き換える場合は、各文字の文字コードの２進８ビットで表し、同様に ASCII 文字（A-Z, a-z, +, /）にエンコードします。インターネットのメッセージで使う文字コードは ISO-2022-JP と定められています。これ以外の文字コードを使ってはいけないというわけではありませんが、他の文字コードの場合、文字化けを起こす可能性があります。

■増え続ける「迷惑メール」とその対策

ｅ メールは郵便システムに比べ、はるかにスピーディーで送信コストも安く大変便利なものですが、これを悪用した「迷惑メール」が増加の一途をたどり大きな問題となっています。迷惑メール対策を推進する業界団体でメール認証技術の標準策定作業を推進する MAAWG（Messaging Anti-Abu しく悪 se Working Group）による、2006 年第 4 四半期におけるインターネット上の全メールのなんと 75 パーセントが迷惑メールによって占められているといいます。

「迷惑メール」は「スパムメール」とも呼ばれ、その内容は一方的な商業広告の送りつけから、「～のために、このメールを○○人に転送するように」と書かれたチェーンメールなど様々です。郵便ダイレクトメールのように切手代がかかるといったこともなく、ヘッダの発信元を書き換えて送りつけることができるなどの理由で増え続けているのです。メール受信時にはユーザーの認証が必要ですが、SMTP によって送信する場合、認証を必要としないことが多いことを思い出してください（図２の①。最近では SMTP で送信時に認証を求める機能も利用されている）。迷惑メールはこうしたｅメールシステムのスキを突く手口から、手の込んだものまでさまざまで、最近では発信元をくらますためにロボットのように遠隔操作で動作する迷惑メール送信プログラムを数多くの PC にばらまいて感染させ、あちこちのメールサーバに一斉に迷惑メールを送信させる「ボット」型も登場しています。

「迷惑メール」は開封した人を不快にしたり、必要なメールの読み出しの邪魔になったりするだけでなく、インターネットを混雑させメールサーバや DNS サーバに負荷を掛けることになります。そこで採られているのが次のような迷惑メール対策です。

１）送信側ユーザーでの対策

「ウイルスチェックソフト」

ユーザーがセキュリティ対策ソフトでボットなどに感染していないかチェックする。

２）送信側メールサーバでの対策

件名や本文、添付ファイル内容の語句をチェックし、迷惑メールと判定されたメールは転送しない。一度に大量に送信するなど、迷惑メールの危険性が高い送信を拒否する。

３）受信側のメールソフトで機能する次のような迷惑メール検出法

「ルールフィルタ」

あらかじめ迷惑メールとみなす語句ルール集を作成し、件名や本文に該当する語句を検知した場合、迷惑メールと判定し処理する。（例：「格安」「出会い」など）

「シグネチャ・マッチング」

過去に検出された迷惑メールのパターンを記録したデータ（シグネチャ）をデータベース化しておき、本文や件名、ヘッダ中の語句と照合し、一定の計算ルールに従って迷惑メール度を算出し判定する。誤検知が少ない。

「ブラックリスト参照」

ユーザーが定義したブラックリストを参照して迷惑メールの判定をする。第三者組織によるスパム発信 IP アドレスのリスト（リアルタイムブラックリスト）に問い合わせて判定する。

４）受信側メールサーバで機能する迷惑メール対策

「グレイリスティング」

受信側メールサーバに対して初めて SMTP 接続してきた IP アドレスに対し、いったん受信を拒否し、同時に IP アドレスをデータベースに記録。ボットも含めて迷惑メールは、いったん受信を拒否されると再送信してこないことが多いことを利用し受信を拒否する。再送信してきた IP アドレスについてはデータベースと照合後、メール受信のやり取りに進む。

「S25(Selective SMTP Rejection)」

SMTP 接続時に送信元 IP アドレスを DNS サーバに照会し、得られた IP アドレスにスパム発信元に特有の文字列が含まれていたりドメイン名を確認できなかったりした場合に接続を拒否する。

「25 番ポートブロック（Outbound Port25 Blocking)」

TCP/IP による通信では、各サーバにメール送信用、メール受信用など数多くのポート（窓口）があり、それぞれのポートにデータを送ることで送信あるいは受信の処理がなされるようになっている。従来、メール送信では「25 番ポート」と呼ばれる、送信者の認証を必要とせずに直接インターネット上のメールサーバに送信できる窓口が利用されていた。しかし迷惑メールの発信者がこの「25 番ポート」を利用することから、各 ISP では同ポートを閉鎖し、認証機能付きの別のポート（587 番ポート）を使用し、迷惑メールの発信に対抗している。（悪意のないユーザーが、利用プロバイダーの外にあるメールサーバを使ってメール送信をしようとする場合もブロックされるため、ポート変更の設定が必要になる）

■「Web メール」

Web メールとは Web ブラウザで利用できるｅメールシステムです。Web ブラウザを利用できる環境であればどこからでもメールソフトなしにメールの送受信ができ、無料で利用できるサービスも提供され、そのユーザーは急速に増えています。

Web メールの仕組みは、受信メールサーバへアクセスして認証し受信メールを取得するプログラム（図２の④⑤）を Web サーバ上で実行、その結果を Web ブラウザ上に表示するというものです。

■おさらい

インターネットの主要機能ともいえるｅメールシステムでは、各種のサーバが重要な役割を果たしていることが分かりました。覚えておきたいポイントは、

1）メールソフトによって作成されたデータは、SMTP と呼ばれるプロトコルに従って送信側 SMTP サーバ、インターネット回線、受信側 SMTP サーバへ送られていく。
2）宛先メールアドレスは、送信側 SMTP サーバに送られてから DNS サーバの検索・照会により対応する受信側 SMTP サーバの IP アドレスに付け替えられる。
3）本来、e メールシステムは英数字、数字、そして記号（ASCII コード文字）以外は送信できない設計になっている。その機能を拡張し、多国の文字、画像や動画、音声データなどバイナリーデータを送信可能にしているのが MIME と呼ばれる規格である。
4）e メールシステムは便利でスピーディー、安価ゆえに迷惑メールの急増という課題を抱えている。
5）SMTP、POP3 とメールサーバの連携によるｅメールシステムをベースに、Web ブラウザを組み合わせることで Web メールなどが登場。メールシステムは進化している。

次回はｅメールと同様、インターネットでもっともよく使われ、インターネットの急速な普及の要因ともなった Web 機能について紹介します。