インターネットの基礎知識

－各種プロトコルから Web 関連技術まで－

森下 泰宏（(社）日本ネットワークインフォメーションセンター）

1999 年 12 月 14 日

Internet Week 99　パシフィコ横浜

（社）日本ネットワークインフォメーションセンター編

目次

1 概要

この講演では、インターネットのしくみを知る上で大変重要な「プロトコル」について説明します。この講演は、主に次のような方を対象としています。

- インターネットは普段から使っているが、インターネット自身のしくみについて、もう少し詳しく知りたい方
- 社内のシステム管理部門に配属になり、インターネットや社内ネットワークの管理をしなければならなくなった方
- 社内のユーザ向けに、インターネットの基礎について講義することになった方

この講演では、次の順に説明を進めます。

- インターネットのしくみ（2 を参照）

  インターネットのプロトコルを理解するために役立つ「OSI 7 層モデル」について詳しく説明します。また、プロトコルの仕様を決定している RFC についても説明します。

- さまざまなプロトコル（3 と 4 を参照）

  インターネットを支える重要なプロトコルである IP に始まり、電子メールで使われる SMTP や Web で使われる HTTP 等、さまざまなプロトコルの概要を説明します。

- 商用化以降のインターネット技術動向（5 を参照）

  日本におけるインターネットの商用利用は 1992 年に開始されました。それに伴い新たな要求も増え、またプロトコルの標準化を取り巻く環境も変わってきました。それらについて簡単に説明します。

2 インターネットのしくみ

最近のインターネットでは、「何かクリックすれば電子メールを使える」、「何かクリックすれば Web を見られる」というのが当たり前になっています。インターネットのしくみを全く知らなくても、インターネットを使えるのです。電源コードをコンセントに差せば、いつのまにか冷蔵庫を使えるというのと同じです。

しくみを知らなくても使えると言えばそれまでですが、しくみを理解すれば、より効率良くインターネットを使えます。また、トラブルの際も、その原因を究明できます。つまり、しくみを知ることによって、より賢くインターネットを使えるようになります。

ここでは、まず、プロトコルという言葉を定義し、インターネットのプロトコルを理解するために役立つ「OSI 7 層モデル」について説明します。そして、プロトコルの仕様を決定している RFC についても説明します。

2.1 プロトコルとは

「プロトコル *」という言葉を辞書で引くと、「コンピュータシステムで、データ通信を行うために定められた規約。情報フォーマット、交信手順、誤り検出法等を定める（広辞苑 第 4 版）」とあります。簡単に言ってしまえば、「複数台のコンピュータが通信を行う際の、さまざまな約束、決め事」がプロトコルということになります。

たとえば、「どんな電気信号を送り合って通信するのか」、「どんな形式でデータを送るのか」というようなことを、あらかじめプロトコルで決めておけば、別のコンピュータと通信できるわけです。見方を変えれば、プロトコルは、「赤信号では止まる」等の日常生活のルールに相当するとも言えるでしょう。

2.2 OSI 7 層モデル

インターネットは、さまざまなプロトコルを使用することで成り立っています。このような通信のためのプロトコルを分類するために、ISO* という組織が提案した「OSI* 7 層モデル」という階層モデルがあります。OSI 7 層モデルはプロトコルそのものを規定したものではなく、「プロトコルがどの辺りの事柄を規定したものか」が分かる枠組です。

ここで、インターネットやプロトコルそのものからは離れてしまいますが、OSI 7 層モデルをより理解しやすくするために、「宅配便（クール便）を利用して荷物を送る」という交通網システムについて考えてみましょう。この交通網システムを階層モデルとして見ると、図 1 のようになります。

プロトコル	コンピュータシステム（複数台のコンピュータ）が通信を行う際の約束事。インターネットのプロトコルには、IP、TCP、UDP、SMTP、HTTP、FTP 等があります。
ISO	「International Standards Organization：国際標準化機構」の略。ISO は工業製品等の国際標準化を進め、各種規格を作成しています。
OSI	「Open System Interconnection」の略。ISO が異機種間の通信接続のために定めた、ネットワークプロトコルの標準です。

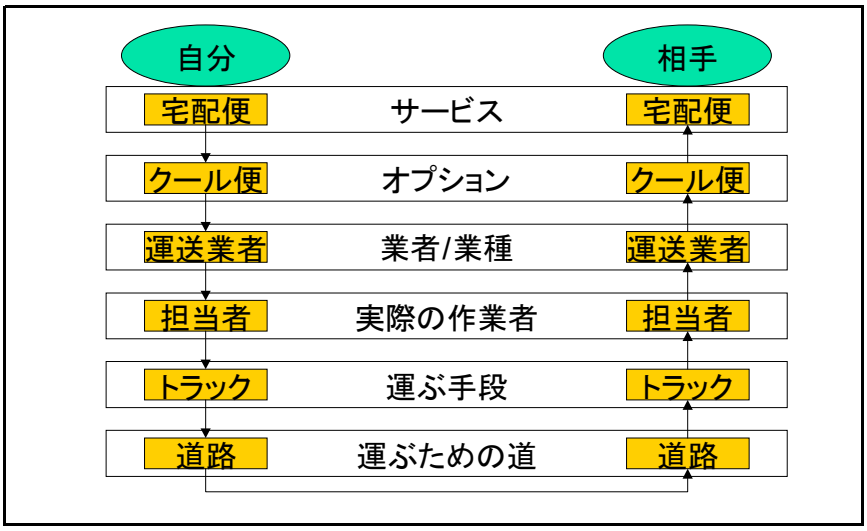


図 1：交通網システムの階層モデル

図 1 の階層モデルでは、上の層に、サービスである宅配便やクール便（オプション）といった論理的なものが位置付けられています。その逆に、道路、トラックといった物理的なものは下の層に位置付けられています。この「論理的なものを上の層に、物理的なものを下の層に」という考え方は、OSI 7 層モデルにもそのまま当てはまります。

OSI 7 層モデルを図 2 に示します。物理層（第 1 層）からアプリケーション（第 7 層）まで、7 つの階層で構成されます。数字の大きい方が、より論理的な層（ソフトウェアに近い層）になります。数字の小さい方が、より物理的な層（ハードウェアに近い層）になります。

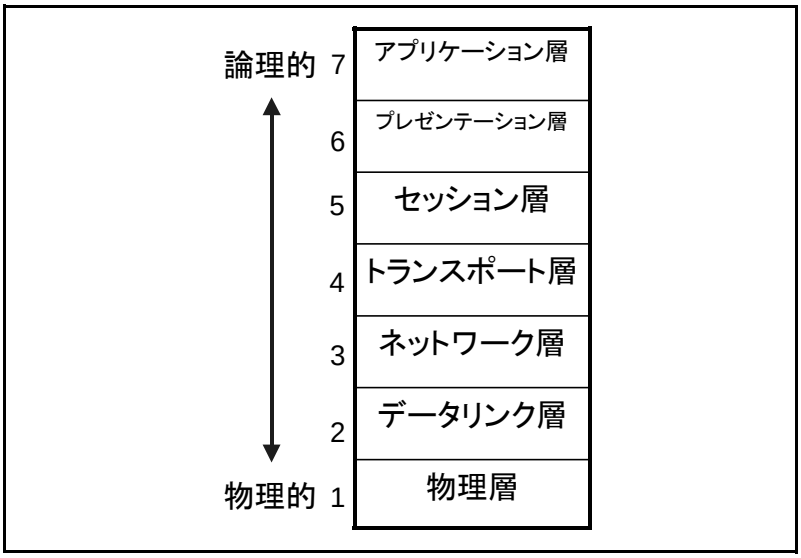


図 2：OSI 7 層モデル

引き続き、OSI 7 層モデルの各層について説明します。理解を助けるために、コンピュータの通信における約束事と、前述の交通網システムの例を対比させながら説明していきます。

2.2.1 物理層

OSI 7 層モデルの物理層（第 1 層）は、次のような事柄を定義する層です。「物理的な繋がりを定義する層」とも言えます。

- 電気的な接続条件
  - たとえば、何ボルトで通信するか、どのように電気を流すかを決めます。
- コネクタの形状、各信号ピンの配列
  - どんな信号を流すためにピンを使うかを決めます。
- データ信号の ON/OFF の定義
  - たとえば、「5V が ON で 0V が OFF」と決めます。

インターネットにおける物理層の役割と、交通網システムとの対比を表 1 に示します。

表 1：物理層

インターネット	交通網システム
• 使用するケーブルの規格 - RJ45 カテゴリ 5 のケーブルを使うこと、等 • 流れるデータの電気的な規格 - LAN ケーブル - 専用線 - 公衆回線	• 信号の青、黄、赤の定義 - 青、黄、赤の光の波長 - 点滅信号の秒数 • 道路の材質 - アスファルト - コンクリート - 砂利道

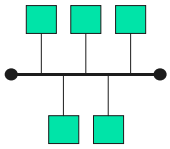
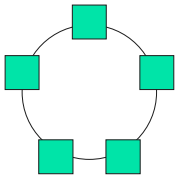
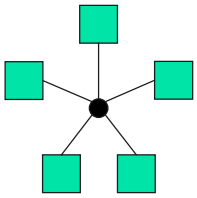
2.2.2 データリンク層

OSI 7 層モデルのデータリンク層（第 2 層）は、次のような事柄を定義する層です。データリンク層は、「物理層で繋がった直接の隣に、データを届けることを保証するための層」とも言えます。

- 隣接装置（通信用語では「ノード」）間における通信手順に関する取り決め
- 隣接装置との接続形態
- 送受信されるデータのフォーマットの定義
  - データをどんな形で送るのかを決めます。
- 装置間におけるデータの誤り検出、訂正方法等の定義
  - ノイズが乗って信号に誤りが発生したような場合に、どのようにそれを検出して訂正するかを決めます。

インターネットにおけるデータリンク層の役割と、交通網システムとの対比を表 2 に示します。

表 2：データリンク層

インターネット	交通網システム
• Ethernet、FDDI、専用回線等の実際のデータ形式 • ネットワークの形態 - バス型  - リング型  - スター型 	• 交通の最も基本的なルール - 左側通行 - 青は進め、赤は止まれ • トラックの積載量 - 幹線なら 4 t トラック 1 台で - 積載量制限のある木製の橋なら、軽トラック複数台に分けて • トラックが実際に走る速度 - 高速道路なら 80 km/h で - 道の狭い市街地なら 30 km/h で

2.2.3 ネットワーク層

OSI 7 層モデルのネットワーク層（第 3 層）は、次のような事柄を定義する層です。通信においては、データをやりとりする相手が、直接繋がっているとは限りません。間に別の装置が入り、それを経由してデータが運ばれることが多いものです。ネットワーク層は、「隣同士以外の相手との通信手順を取り決める層」とも言えます。

- ノード間の経路制御（ルーティング）に関する取り決め
  - どこをどのように通るかを決めます。
- データをやりとりする相手までの通信経路の決定に関する定義
- アドレスによる仮想的な接続の確立
  - あたかも隣同士で通信しているかのような、仮想的な繋がりを作ります。

インターネットにおけるネットワーク層の役割と、交通網システムとの対比を表 3 に示します。

表 3：ネットワーク層

インターネット	交通網システム
• あるコンピュータから、別のあるコンピュータまでの通信経路の決定 • IP アドレスによるコンピュータの特定 - 「202.12.30.131」	• ある地点からある地点まで車を走らせる場合の通り道の決定 • 住所による場所の特定 - 「東京都千代田区神田小川町 1-2」

2.2.4 トランスポート層

OSI 7 層モデルのトランスポート層（第 4 層）は、次のような事柄を定義する層です。3 層までででは「相手に届きうること」しか保証されないのに対し、トランスポート層は、「相手の手元までちゃんと届くことを保証する層」となります。

- 始点⇔終点間のデータの信頼性の確保
- エラー訂正
  - データ到着順を訂正します。
  - エラーになったデータの再送を要求します。
- フローコントロール
  - 処理しきれる範囲に、流量を制御します。

エラーが発生した場合の訂正処理はデータリンク層にもありましたが、それは「隣までエラーなしで届ける」ものでした。これに対して、トランスポート層のエラー訂正処理は、「通信相手までエラーなしで届ける」ものになります。トランスポート層のエラー訂正処理では、本来のデータとは異なる順序でデータが届いたときには、並べ直して元の順序に戻します。また、受け取ったデータがエラーとなっていた場合は、送信元に対して、再送を要求したりします。

インターネットにおけるトランスポート層の役割と、交通網システムとの対比を表 4 に示します。

表 4：トランスポート層

インターネット	交通網システム
• ポート * 番号の確定 - 「TCP ポートの 25 番」	• 最終到達先の決定 - 「風雲堂ビル 3F の受付」
• IP パケット * の順番の整列、エラーパケットの再送等の処理	• 荷物の個数（何個口）や、破損のないこと等の確認
• 回線の速度、データの処理速度に合わせたデータ送信速度の調整	• 大量に搬入がある場合に、荷物を片付けながら少しずつ運びこむ等

ポート　データをやりとりする窓口のことです。複数のプログラムを識別するために使われます。「電子メールのデータは TCP プロトコルのポート 25 番宛てに送る」といった約束事があります。

パケット　データをある程度まとまった固まりにして、または大きなデータを小さな固まりに分けて送るときの単位のことです。インターネットでは、「IP パケット」がやりとりされます。

2.2.5 セッション層

OSI 7 層モデルのセッション層（第 5 層）は、次のような事柄を定義する層です。セッション層は、「誰が送ったデータなのか、また、その相手とどのような方法で通信するかを確認する層」と言えます。

- 目的装置における通信手段の提供に関する取り決め
- 認証（Authentication）
  - 「あなたは○○さんですね？」と確認します。
- 権限（Authorization）
  - 「○○さんだったら、××のサービスを使ってもいいですよ」と確認します。
- 同期*（Synchronization）

インターネットにおけるセッション層の役割と、交通網システムとの対比を表 5 に示します。

表 5：セッション層

インターネット	交通網システム
• 接続相手の IP アドレスから、接続相手のホストを確定 • IP アドレスによるアクセス制限 - 「この IP アドレスからのアクセスは受け付けない」 • SPAM* メールの受け取り拒否 - 「この IP アドレスからの電子メールは SPAM だから受け取らない」 • 接続を拒否された場合のエラーの通知	• ○○さんからの荷物であるという確認 - 認証に相当 • ○○さんからの荷物は受け取っても問題ないという判断 - 権限に相当 • 留守の場合の不在票の処理

同期 データをやりとりする格好を決めるものです。電話のように、一方が話していても、もう一方からも話しかけられるような「全二重（Full Duplex）」や、無線通信のように、一方が話している間はもう一方は話せない「半二重（Half Duplex）」等があります。

SPAM 不特定多数の相手に、広告宣伝の電子メール（ダイレクトメールのようなもの）を送りつけることです。

2.2.6 プレゼンテーション層

OSI 7 層モデルのプレゼンテーション層（第 6 層）は、次のような事柄を定義する層です。プレゼンテーション層は、「データ表現の方法を定める層」と言えます。

- 目的装置とのデータのやりとり（表現方法）に関する取り決め
- データの暗号化方法、復号方法
- データの圧縮方法、展開方法
- 使用する文字コード、データフォーマット等の決定

プレゼンテーション層の役割は「何語でしゃべるか？」と言い換えることもできます。たとえば、日本語で説明しようと、英語で説明しようと、説明する事柄には変わりはありません。これと同様、プレゼンテーション層で暗号化してあろうとなかろうと、データそのものには変わりはありません。あくまでも、データ表現の違いだけなのです。

インターネットにおけるプレゼンテーション層の役割と、交通網システムとの対比を表 6 に示します。

表 6：プレゼンテーション層

インターネット	交通網システム
• 日本語メールの文字コードの指定 　- 「ISO-2022-JP」 • PGP* を用いたメールの暗号化 • MIME* を使った画像ファイルの転送	• いろいろなオプション（荷物そのものには変わりはないが、扱い方が違う） 　- 「クール便」 　- 「取り扱い注意」 　- 「天地無用」

PGP	「Pretty Good Privacy」の略。メールを暗号化するための規格の 1 つで、さまざまなメールアプリケーションで利用されています。RFC1991 で規定されています。
MIME	「Multipurpose Internet Mail Extensions」の略。本来、テキストデータだけを送るように作られた電子メールで、画像や音声等のバイナリデータを送れるようにするための規格です。RFC1521 で規定されています。

2.2.7 アプリケーション層

OSI 7 層モデルのアプリケーション層（第 7 層）は、次のような事柄を定義する層です。アプリケーション層は、「やりたいことについて定める層」、「実際のサービス内容を定める層」と言えます。

- 実際のサービスの内容に関する取り決め
- 実際にユーザに見える部分
- 利用可能なサービスそのもの

インターネットにおけるアプリケーション層の役割と、交通網システムとの対比を表 7 に示します。

表 7：アプリケーション層

インターネット	交通網システム
• 電子メール • WWW(World Wide Web) • ファイル転送 • 電子掲示板 • ファイルの共有	• 宅配便 • バイク便 • 観光バスツアー • タクシー • 運転代行サービス

2.2.8 階層モデルのメリット

ここで、OSI 7 層モデルのような階層モデルをとることに、どんなメリットがあるかについて考えてみましょう。まず、次の 2 つが挙げられます。ともに、役割分担がはっきりしているので、処理が複雑にならないということです。

- 上の層は、下の層にデータを渡して命令するだけでよい

  上の層は、下の層がどのように処理をするかについて気にする必要はありません。

- 下の層は、上の層との約束（インタフェース）どおりに処理をするだけでよい

  下の層は、渡したデータを上の層がどう使うかについて気にする必要はありません。

また、階層モデルには、「さまざまな形に応用しやすい」というメリットもあります。理解しやすいように、交通網システムの例を図3に示します。

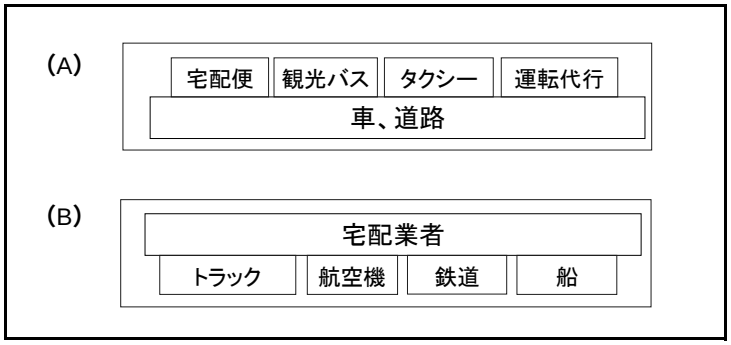


図3：階層モデルのメリット

- 1つの層の上に、さまざまなサービスを展開できる

  図3（A）では、車、道路といった下の層の上に、複数のサービスを乗せています。目的に応じたサービスを容易に作成でき、可能性を広げることができます。インターネットの例では、電子メールとWebだけを使っていたネットワークで、配線等のネットワーク自体には何も手を加えずに、新たにファイル転送のサービスを追加できるといったメリットです。

- サービスに応じて、下の層の手段をいろいろ選べる

  図3（B）では、宅配というサービスが、時間、コストに応じて、運送手段を選んでいます。どの手段を選ぼうと、宅配というサービスそのものには変わりがありません。インターネットの例では、あるサービスを利用するために Ethernet を利用していたが、あるときにそれを FDDI に切り替えたとしても、サービス自体には影響がないといったメリットです。

今までのまとめとして、OSI 7層モデル、インターネット、交通網システムの対応を表8 に示します。なお、インターネットプロトコルについては、トランスポート層とネットワーク層を明確に切り分けられないことが多いので、表8では1つにまとめてあります。

表 8：OSI 7 層モデル（まとめ）

OSI 7 層モデル	インターネット	交通網システム
アプリケーション	電子メール	宅配便
プレゼンテーション	文字コード	クール便
セッション	SMTP プロトコル	運送業者
トランスポート／ ネットワーク	TCP プロトコル、 IP プロトコル	担当者
データリンク	モデム	トラック
物理	電話回線	道路
運ばれるもの	IP パケット	荷物
利用の取り決め	各種プロトコル	各種ルール
取り決めの根拠	RFC（後述）	法律等

2.3 RFC

今まで説明してきた OSI 7 層モデルは、プロトコルの枠組みを決めたものでした。ここでは、枠組みではなく、インターネットのプロトコル（取り決め）の仕様そのものを決定している RFC* について説明します。

取り決めと言っても、RFC は国会議員が決めた法律のようなものではありません。RFC は、インターネットのユーザ（使っている人、技術者）の話し合いによって作られています。この話し合いには誰でも参加できます。話し合いは主に電子メールで行われますが、年 3 回、IETF（Internet Engineering Task Force）という定例会合も持たれています。

最初の RFC は 1969 年に発行され、1999 年 10 月 26 日現在、RFC2719 まで発行されています。この中で、Jon Postel 博士 * が編纂した基本的な 100 以上の RFC が、現在もなお使われ続けていることは特筆すべきでしょう。

RFC　「Request For Comments」の略。インターネットの各種プロトコルを規定した文書です。

Jon Postel **博士**　インターネットの発展に寄与したさまざまな業績から「インターネットの神様」と呼ばれています。1998 年逝去。

RFC は「Request For Comments」、つまり「コメント求む」という意味です。「取り決め」には一見そぐわないようですが、RFC は、不備があればそれを修正、更新し、また、新しい要求が出ればそれに応じて改良するという柔軟な姿勢で運用されているので、「Request For Comments」は「更新、改良のためのコメント歓迎」であると理解してください。

改良の例で言えば、Web で使われる HTTP には次の 3 つの RFC があります。インターネットプロトコルの仕様をチェックする際は、プロトコル名だけではなく、どの RFC に準拠したものかも確認する必要があります。

- RFC1945（HTTP/1.0）
- RFC2068（HTTP/1.1）
- RFC2616（HTTP/1.1）

RFC の情報は、次の方法で入手できます。

- RFC のホームページ

  http://www.ietf.org/rfc.html

- RFC の書き方の説明

  http://www.rfc-editor.org/

- RFC の今までの変遷

  rfc-index.txt

3　インターネットのさまざまなプロトコル（1）

プロトコルという言葉や、OSI 7 層モデル、RFC について理解したところで、いよいよ具体的なプロトコルの説明に入ります。最初に説明するのは、図 4 に示す基本部分のプロトコルです。

インターネットの基本部分を構成し、インターネットを支えているプロトコルは、通常はユーザには見えない部分で機能しています。図 4 に示す、OSI 7 層モデルのネットワーク層とトランスポート層にあたるプロトコルです。ただし、DNS だけは、セッション層のプロトコルになります。

なお、基本部分のプロトコル以外の、ユーザに見える部分のプロトコルである SMTP、HTTP、FTP については、4 で説明します。

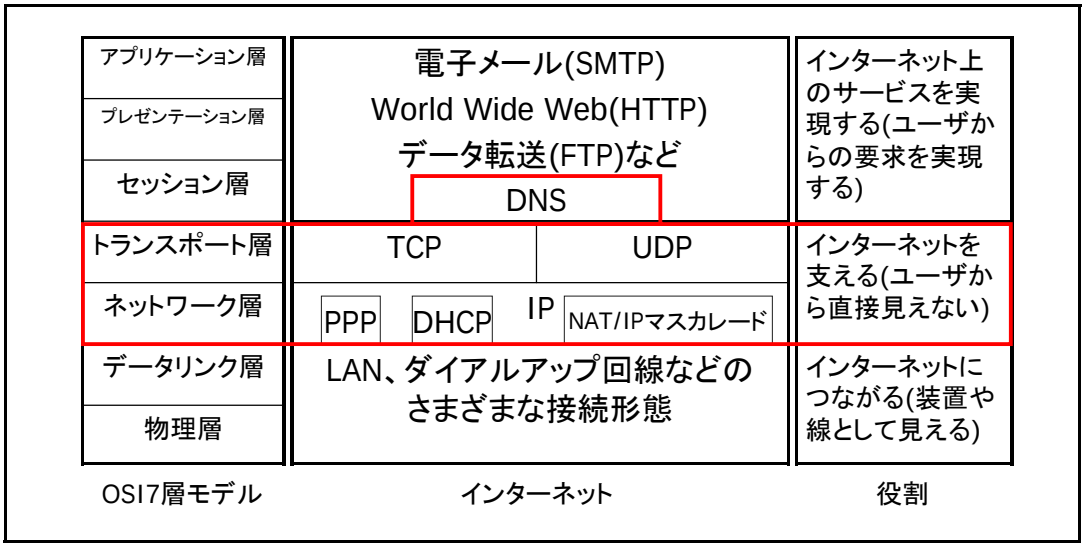


図 4：インターネットを支えるプロトコル（1）

3.1 IP

IP*（Internet Protocol）は、ネットワーク層のプロトコルです。IP は RFC791 で規定されており、後述の TCP とともに「TCP/IP」と呼ばれ、インターネットにおける基本プロトコルとして機能しています。

IP で取り決められている事柄のうち、大変重要なのが「IP アドレス*」です。ここでは、IP アドレスの概要、およびその割り当て方法や関連プロトコル等について説明します。

3.1.1 IP アドレスの概要

IP アドレスは、TCP/IP において通信相手を指定、識別するために使われるアドレスです。電話をかけるときに電話番号が必要なように、インターネット上で TCP/IP による通信を行うときには IP が必要です。IP アドレスについては、次の特徴があります。

- 通信元、通信先の双方の機器に IP アドレスが割り当てられていることが必要。
- インターネット上には、同じ IP アドレスを持つ機器が複数台存在してはならない。

IP アドレスは 32 ビットの符号なし整数で表現されますが、そのまま整数で書くと分かりづらいので、「202.12.30.131」のように、8 ビットずつ分割した上で、ピリオドで区切る形式で表記するのが一般的です（図 5）。

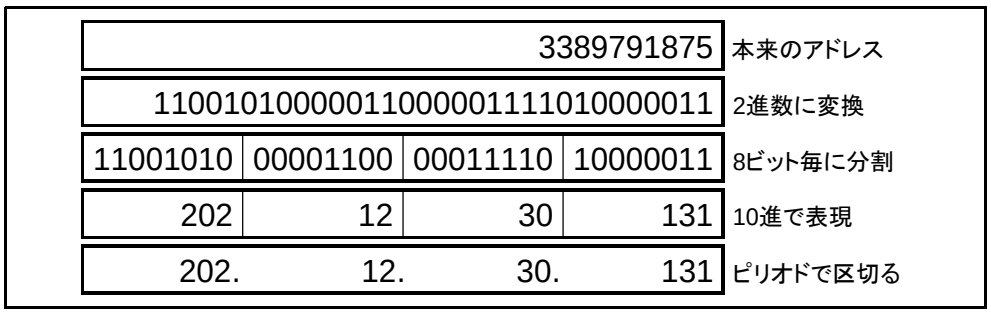


図 5：IP アドレスの表記方法

IP	「Internet Protocol」の略。IP アドレス等、インターネットの基本となる事柄を取り決めたプロトコルです（RFC791）。TCP とともに、「TCP/IP」と呼ばれます。
IP **アドレス**	TCP/IP において通信相手を指定、識別するためのアドレスです。現在は、32 ビットのアドレスが使われています。

3.1.2 IP アドレスの割り当て（CIDR）

前述のように、インターネット上には、同じ IP アドレスを持つ機器が複数台存在してはなりません。同じ IP アドレスを持つ機器が複数台あったら、どの機器と通信したらよいのか判断できないからです。このため、「IP アドレスを重複しないように管理するしくみ」が必要になります。

インターネットが利用され始めてから最近まで、ネットワークの規模によってクラス A、クラス B、クラス C というクラス分けをする方式で IP アドレスが管理されていました。現在は、クラスを使わない CIDR* という方式で、より効率的に IP アドレス管理が行われています。将来、また別の方式が使われるようになるかもしれませんが、現在は CIDR です。

CIDR（Classless Inter-Domain Routing）は、「202.12.30.128/26」のような表記を使う IP アドレス管理方式です。CIDR は RFC1519 で規定されています。CIDR には、次のような特徴があります。

- 「ネットワーク番号 / プレフィックス長」という表記を使う

  「202.12.30.128/26」の例では、「202.12.30.128」がネットワーク番号で、「26」がプレフィックス長です。

- プレフィックス長は、1 つのネットワークに割り当てる IP アドレスの数を表す

  プレフィックス長は、「上位何ビット分がネットワーク番号か」を示す値です。「202.12.30.128/26」の例では、上位 26 ビットがネットワーク番号となります。上位 26 ビット分（IP アドレスブロック）がネットワークを識別するために用いられ、32 － 26 ＝ 6 ビット分が、ネットワーク内のコンピュータを識別するために用いられます（図 6）。

  プレフィックス長の値が大きいほど、ネットワーク内のコンピュータを識別するためのビット数が減るので、ネットワークの規模としては小さくなります。逆に、プレフィックス長の値が小さいほど、ネットワークの規模としては大きくなります。

  なお、コンピュータを識別する部分が全部 0 のアドレスはそのネットワーク自身を表し、コンピュータを識別する部分が全部 1 のアドレスはそのネットワークに繋がったコンピュータ全体を表します。このため、「202.12.30.128/26」のネットワークに実際に接続できる台数は、6 ビットで表せる 2^6 ＝ 64 台ではなく、64 － 2 ＝ 62 台となります。

CIDR　「Classless Inter-Domain Routing」の略。現在使用されている IP アドレス管理の方式で、ネットワーク番号とプレフィックス長を用いて表記します（RFC1519）。

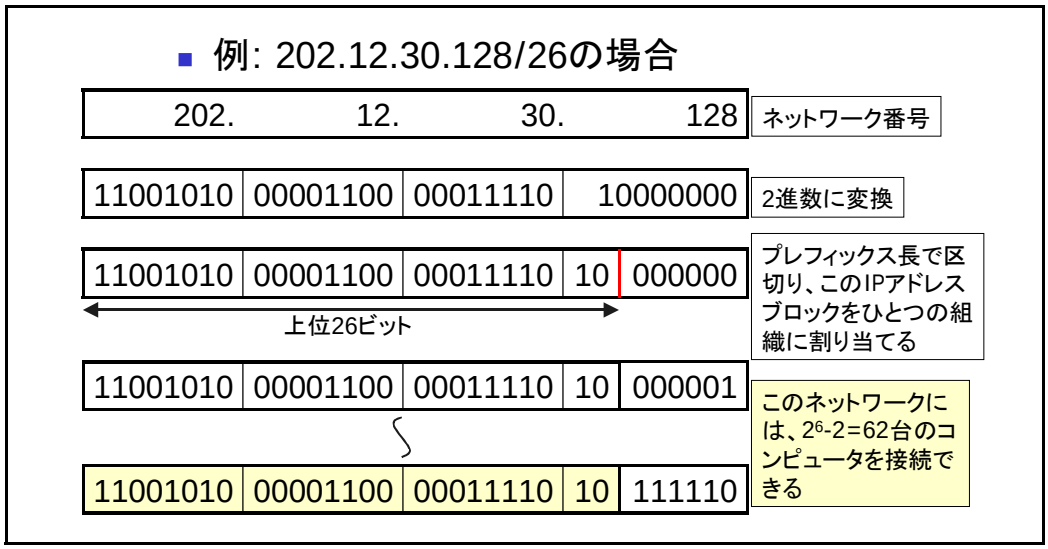


図 6：CIDR による IP アドレス管理

CIDR による IP アドレス管理は、階層的な管理体系をとることができるのも大きな特徴です。現在、IP アドレスは、図 7 に示すように、IANA*（ICANN*）、APNIC*、JPNIC* といった組織が IP アドレスブロックを階層的に管理し、それをプロバイダに割り当て、さらにプロバイダが組織に割り当てるという管理体系をとっています。これによって、世界中で IP アドレスがぶつからないように管理することが可能になっています。

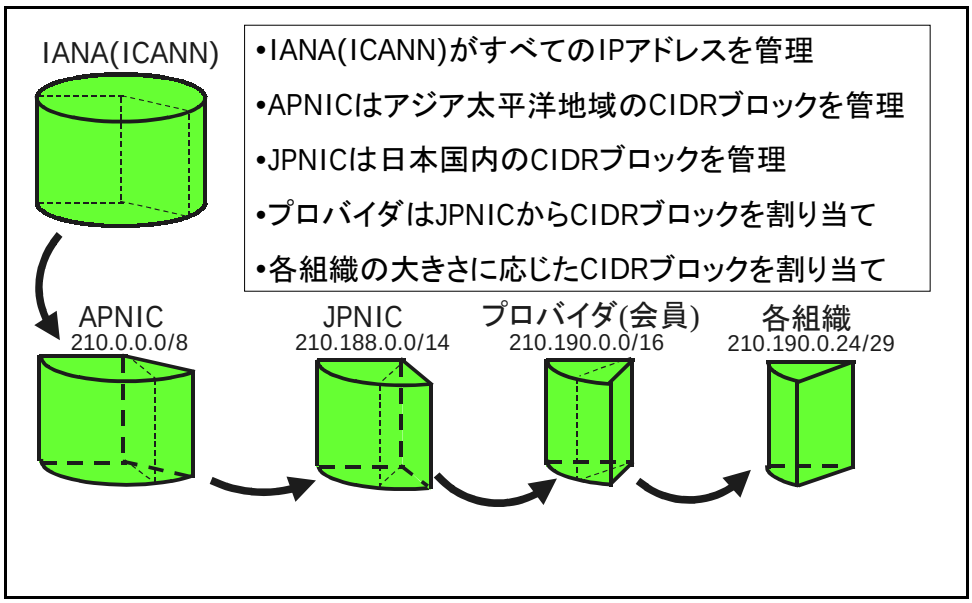


図 7：IP アドレスの階層的な管理体系

さて、以前の方式に比べ、より効率的に IP アドレスを管理できる CIDR ですが、現在使用している 32 ビットの IP アドレス、2^{32} ＝ 4,294,967,296（43 億弱）個は、インターネットの爆発的な普及に伴って 21 世紀前半には枯渇するだろうと言われています。次世代の IP（IPv6）の運用も一部で始まっていますが、現在の IP アドレスという限りある資源を、より有効に利用する工夫が必要です。

IP アドレスの有効利用のために、いくつかの方法が編み出されています。

- 動的な IP アドレス割り当て

  インターネットネットワークに接続するときにだけIPアドレスを割り当て、接続しないときは IP アドレスを返す方法です。動的に IP アドレスを割り当てるためのプロトコルには、DHCP（3.1.3 を参照）、PPP（3.1.4 を参照）があります。

- プライベートアドレスの利用

  インターネットに直接接続されないネットワークには、インターネット上で使用されていないIPアドレス（プライベートアドレス。RFC1918 で規定）を割り当てる方法です。たとえば、人事部のネットワークに接続したコンピュータからはインターネットのサービスを利用しない、人事情報が万一にでも外から覗かれたら困るというような場合は、プライベートアドレスだけを割り当てればよいのです。

  ただし、通常はインターネットに直接接続しないのでプライベートアドレスを使うが、インターネット上のサービスを利用することもある場合は、インターネットに接続するときだけ、プライベートアドレスをインターネット上で使用される IP アドレス（グローバルアドレス）に変換する必要があります。このグローバルアドレスへの変換のためには、NAT や IP マスカレード（3.1.5 を参照）という方法があります。

IANA	「Internet Assigned Numbers Authority」の略。IANA は、IP アドレス等インターネット上で重要なパラメータを登録、管理している組織です
ICANN	「Internet Corporation for Assigned Names and Numbers」の略。IANA を前身として 1998 年に設立されました。
APNIC	「Asia Pacific Network Information Center」の略。アジア太平洋地域に関する IP アドレスの割り当て等を行っています。
JPNIC	「社団法人 日本ネットワークインフォメーションセンター（Japan Network Information Center）」の略。日本で、JP ドメイン名の登録管理や IP アドレス割り当て管理等の業務を行っている公益法人です。

3.1.3 DHCP

DHCP*（Dynamic Host Configuration Protocol）は、ネットワーク層のプロトコルです。DHCP は RFC2131 で規定されています。

DHCP は、IP アドレスを集中管理する DHCP サーバをネットワーク上に用意し、コンピュータをネットワークに接続したときに、空いている IP アドレスを DHCP サーバからコンピュータに割り当てるものです。コンピュータの電源を切ったりして、ネットワークから切断されると、その IP アドレスは DHCP サーバに返されます。コンピュータをネットワークに接続しただけで使えるので、DHCP によって、「Plug & Play」環境を実現できます。DHCP は従来は社内ネットワークで使われてきましたが、最近は CATV（ケーブル TV）配線を利用したインターネット接続サービスでも、DHCP によって IP アドレスを動的に割り当てるようになってきています。

3.1.4 PPP

PPP*（Point-to-Point Protocol）は、ネットワーク層のプロトコルです。PPP は RFC1661 で規定されています。

PPP には、専用回線、電話回線等で利用される動的な IP アドレス割り当ての方法が含まれており、ダイヤルアップ IP のためのプロトコルとして広く普及しています。PPP では、DHCP の場合の DHCP サーバのように、アクセスサーバ（プロバイダ側の接続機器）が IP アドレスを集中管理します。

3.1.5 NAT/IP マスカレード（プライベートアドレス）

プライベートアドレスは、「組織内で自由に使ってよい」、「インターネット上では使われていないことが保証されている」IP アドレスです。プライベートアドレスについては、RFC1918 で規定されています。プライベートアドレスは具体的には、次の範囲の IP アドレスです。

- 10.0.0.0 ～ 10.255.255.255（10.0.0.0/8）
- 172.16.0.0 ～ 172.31.255.255（172.16.0.0/12）
- 192.168.0.0 ～ 192.168.255.255（192.168.0.0/16）

DHCP	「Dynamic Host Configuration Protocol」の略。動的な IP アドレス割り当てについて取り決めたプロトコルです（RFC2131）。
PPP	「Point-to-Point Protocol」の略。動的な IP アドレス割り当てについて取り決めたプロトコルです（RFC1661）。ダイヤルアップ接続で使われています。

プライベートアドレスが割り当てられているコンピュータは、そのままではインターネットを利用できません。プライベートアドレスは、インターネット上では使用できないアドレスだからです。この場合、図 8 のように途中で IP アドレスを変換することにより、インターネットの利用が可能になります。

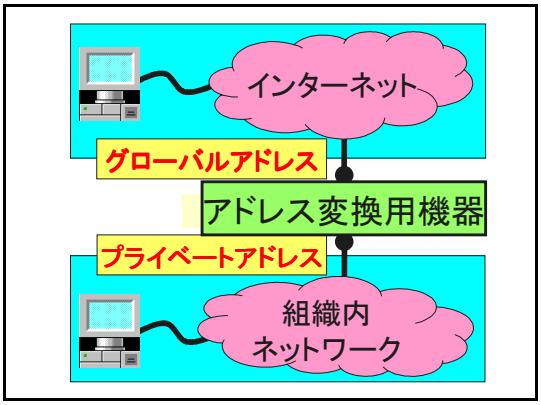


図 8：IP アドレス変換

IP アドレスの変換には、次の 2 つの方法があります。IP アドレス変換機能は、最近のルータには標準で装備されています。

- NAT（Network Address Translation）

  プライベートアドレスとグローバルアドレスを 1 対 1 で対応づける方法です。ただし、現在では IP マスカレードと同じ意味で使われる場合もあります。

- IP マスカレード（IP masquerade）

  ポート番号を識別することによって、複数のプライベートアドレスを 1 つのグローバルアドレスに対応づける方法です。

3.1.6 経路制御

インターネットはさまざまなネットワークが繋ぎ合って形成されたネットワークです。このため、インターネットで通信する場合には「どの経路でデータを送るか」、つまり経路制御（ルーティング）が大変重要になります。経路制御が正しく行われないと、インターネットは利用できません。経路制御は、IP の基本機能として規定されています。

経路制御では、IP アドレスから適切な経路を判断します。膨大な IP アドレスのうちの 1 つを目指すのですから、やみくもに探すのは効率的ではありません。このため、まず、最初は大まかな経路を決め、徐々に細かい経路を決め、最終目的の IP アドレスを目指すようになっています。

これは、「大阪市伊丹市○○町△番地」に向かうとき、まず、大阪府、次に伊丹市、○○町、最後に○○町の△番地を探すのと同じです。

経路制御には、次の 2 種類があります。個々のプロトコルについては、別の講演で取り上げられていますので、ここでは説明しません。

- EGP*（Exterior Gateway Protocol）

  組織間の経路制御、つまり「大まかな経路制御」を行うためのプロトコルです。プロバイダ等の大規模ネットワーク間での経路制御に使用されています。代表的なものには BGP4（RFC1771）があります。

- IGP*（Interior Gateway Protocol）

  組織内の経路制御、つまり「細かい経路制御」を行うためのプロトコルです。代表的なものには RIP（RFC1058）、OSPF（RFC2328）があります。

EGP と IGP の関係を図 9 に示します。

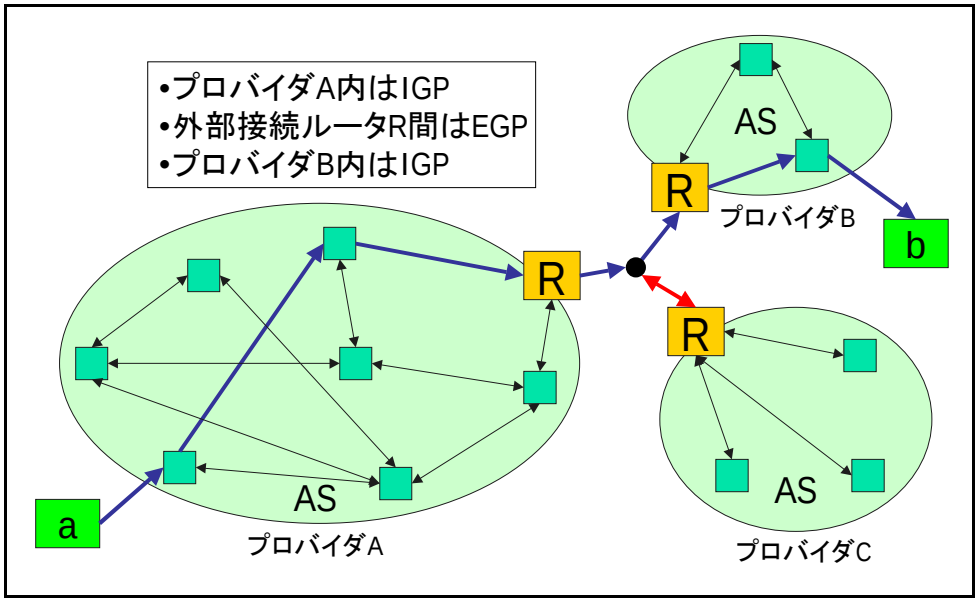


図 9：EGP と IGP による経路制御

EGP	「Exterior Gateway Protocol」の略。大規模なネットワーク間で経路情報を交換するためのプロトコルです。代表的なものに BGP4 があります。
IGP	「Interior Gateway Protocol」の略。組織内ネットワークの経路情報を制御するプロトコルです。代表的なもの RIP、OSPF があります。

3.2 TCP

TCP*（Transmission Control Protocol）は、トランスポート層のプロトコルです。TCP は RFC793 で規定されています。

TCP の特徴は、データの信頼性を保証して通信することです。データが失われたり、内容が変わったりすることなく、送信した順番でデータが通信相手に正しく届きます。TCP は、データが正しく届いたかどうかを送信元で確認できるしくみを持っています。これらのことから、電子メールやファイル転送等、多くのインターネットプロトコルは TCP を使用しています。「TCP/IP」がインターネットプロトコルの基本中の基本と言われるのは、このためです。

3.3 UDP

UDP*（User Datagram Protocol）は、トランスポート層のプロトコルです。UDP は RFC768 で規定されています。

UDP は、データ通信に関する取り決めであるところは TCP と同じですが、データの信頼性を保証しない点が異なります。エラーが発生してもデータの再送は行いませんし、フローコントロールも行いません。行わなければいけない処理が減りますので、UDP は TCP よりもプロトコル自身のオーバーヘッドが少なくなります。

この特徴から UDP は、処理速度が重要なデータや、到着確認が必ずしも必要ないデータ等のために利用されています。たとえば、画像データを受け取りながら表示するような場合は、オーバーヘッドが少ない方が速く処理できますし、画像表示では数ビット分のデータがおかしくなったとしても大勢に影響しないので、TCP ではなく、UDP でデータ通信を行います。

TCP	「Transmission Control Protocol」の略。全二重、フローコントロール付きで、信頼性のあるデータ通信を提供するプロトコルです（RFC793）。
UDP	「User Datagram Protocol」の略。TCP 同様、データ通信について規定していますが、信頼性は保証しません。TCP よりもオーバーヘッドが少ないのが特徴です（RFC768）。

3.4 DNS

DNS*（Domain Name System）は、セッション層のプロトコルです。DNS は RFC1034、RFC1035 で規定されています。DNS は IP アドレスとドメイン名 * を結び付けるしくみです。

ドメイン名については別の講演で詳しく説明していますので、ここでは概要のみ説明しましょう。インターネット上の通信では IP アドレスで通信相手を特定すると説明しましたが、IP アドレスは数字の羅列なので覚えにくく不便です。そこで、「www.nic.ad.jp」のような覚えやすい名前（ドメイン名）を付ける方法が考え出されました。ドメイン名と IP アドレスを結び付けるしくみ（DNS）を使うことによって、ドメイン名を指定すれば、インターネットで通信を行えるようになっているのです。

DNS は、ドメイン名を階層的に管理する分散型のデータベースです。DNS における木構造を図 10 に示します。DNS では、「ゾーン（名前空間）」と呼ばれる管理範囲を定め、それぞれのゾーンについて、IP アドレスとドメインの対応を管理するネームサーバを運用します。最上位のルート（.）ゾーンを管理するルートサーバに始まり、階層的にネームサーバが配置されるわけです。

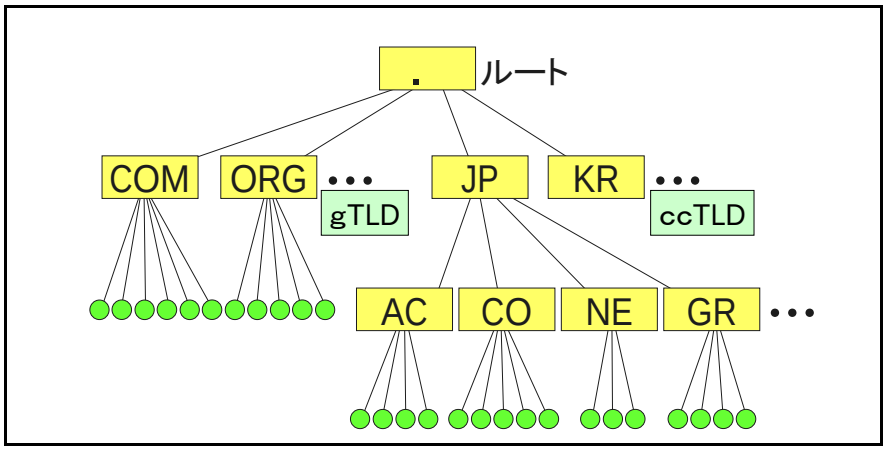


図 10：DNS の木構造

DNS　「Domain Name System」の略。IP アドレスとドメイン名を結び付けるしくみです（RFC1034、RFC1035）。

ドメイン名　コンピュータや複数のコンピュータが接続されるネットワークをグループとして管理する場合に、グループに付けられる名前です。インターネットで単にドメイン名と言う場合は、通常、DNS による階層化された構造のドメイン名を指します。

では、ドメイン名から IP アドレスを知る具体的な手順を見てみましょう。この手順を「名前解決」と呼びます。名前解決の様子を図 11 に示します。

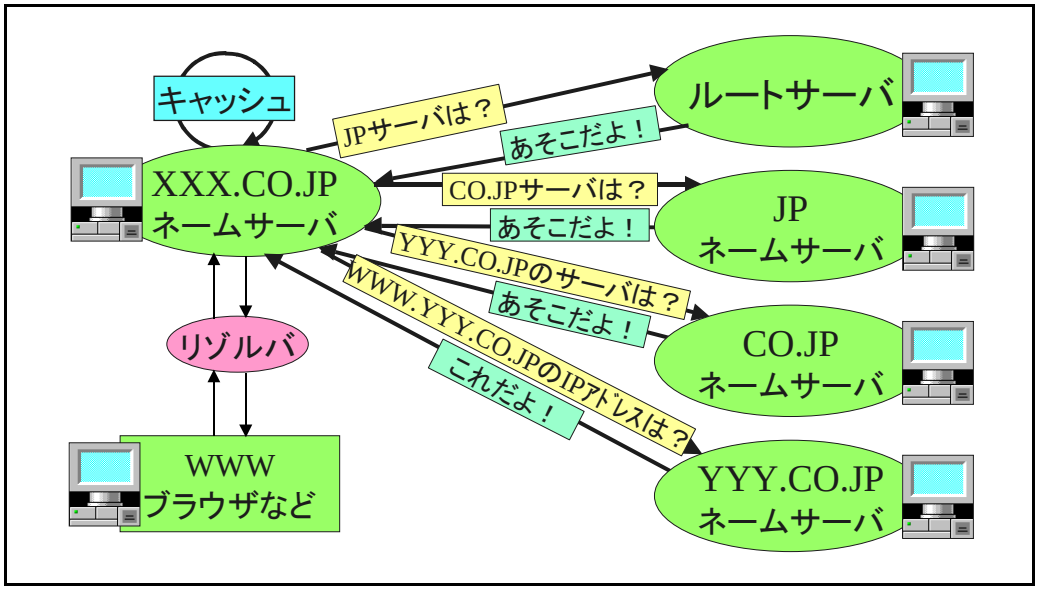


図 11：名前解決の流れ

たとえば、「www.yyy.co.jp」の Web ページを見たいとします。まず、リゾルバが www.yyy.co.jp の IP アドレスを知っているかどうかを、自分の組織のネームサーバ（xxx.co.jp のネームサーバ）に問い合わせます。最近問い合わせがあったものについては、キャッシュに情報を一定期間保存しているので、すぐに IP アドレスを知ることができます。

そこで IP アドレスが分からないとなると、xxx.co.jp のネームサーバは、ルートサーバに対して、「JP ネームサーバはどこ？（JP ネームサーバの IP アドレスは何？）」と問い合わせます。ルートサーバに JP ネームサーバの IP アドレスを教えてもらったら、次に、JP ネームサーバに対して、CO.JP ネームサーバの IP アドレスを問い合わせます。このように、下位のネームサーバに対して順繰りに問い合わせていけば、最後には「www.yyy.co.jp」の IP アドレスを得ることができます。

「まず、ルートサーバに問い合わせる」ということから、ルートサーバの重要性が分かります。少なくとも 1 台のルートサーバに到達できないと、インターネットで通信を行うことはできないのです。1999 年 10 月の時点でインターネット上には 13 台のルートサーバがあり、インターネットを支えています。日本には、1997 年に m.root-servers.net というルートサーバが設置され、WIDE プロジェクトが管理しています。国内にルートサーバがあるので、万一海外とのリンクが切れた場合でも、国内のインターネットを利用できる体制になっています。

前述の DNS でドメイン名から IP アドレスを得る方法を「正引き」と呼びます。反対に IP アドレスからドメイン名を得る方法もあり、こちらは「逆引き」と呼びます。逆引きは、たとえば、インターネットのサービス提供者が、どのドメインからのアクセスなのかを調べるために、統計情報やログ等を管理する際等に使われます。

逆引きの様子を図 12 に示します。逆引きでは「IN-ADDR.ARPA」という特殊なドメイン名を使用します。たとえば、「202.12.30.131」という IP アドレスを逆引きしたいなら、IP アドレスの数字の並びを逆にして IN-ADDR.ARPA を付けた「131.30.12.202.IN-ADDR.ARPA」についてルートサーバに問い合わせるのです。逆引きの場合も同様に、自分の組織のネームサーバのキャッシュにデータがない場合、ルートサーバに対して最初に問い合わせが行われます。

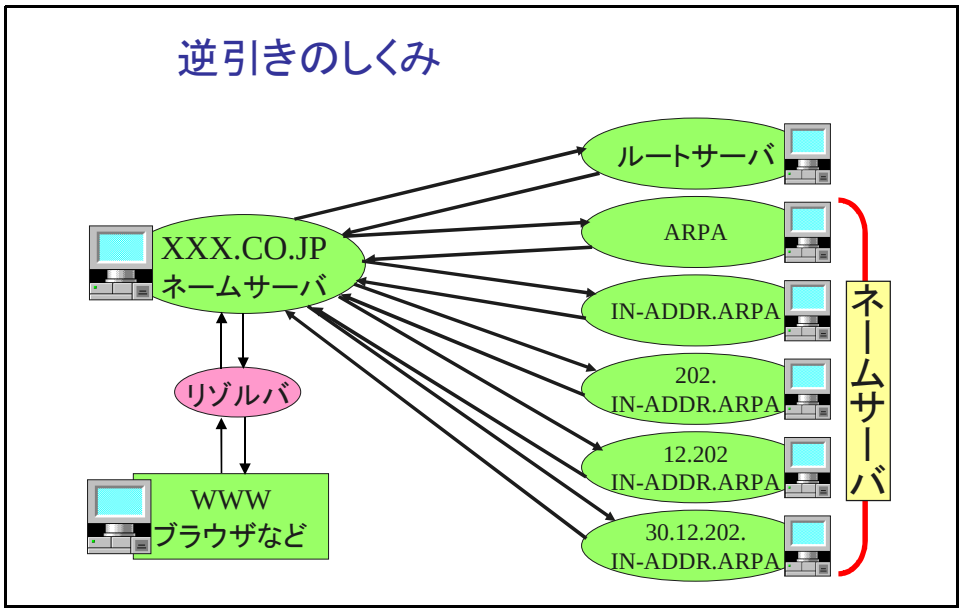


図 12：DNS の逆引き

4　インターネットのさまざまなプロトコル（2）

基本部分のプロトコルの説明に続き、「インターネットでできること」を実現するためのプロトコルの説明に入ります。ここで説明するプロトコルを図 13 に示します。これらは、実際にユーザが使う部分であるアプリケーション層のほか、プレゼンテーション層、セッション層にも係わる機能を果たすプロトコルです。

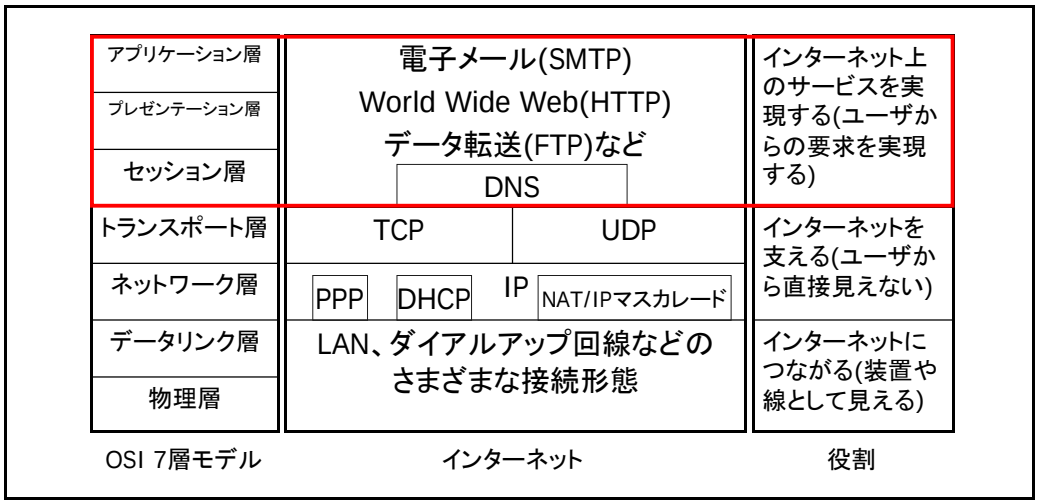


図 13：インターネットを支えるプロトコル（2）

トランスポート層の説明で「ポート」について触れましたが、ここで少し補足します。インターネット上のサービスのうち代表的なものについて、プロトコルが使用するポート番号が「Well-known Port」として IANA によって定義されています。Well-known Port の例を表 9 に示します。これらのプロトコルについては特に指定を変更しない限り、これらのポートが使用されます。

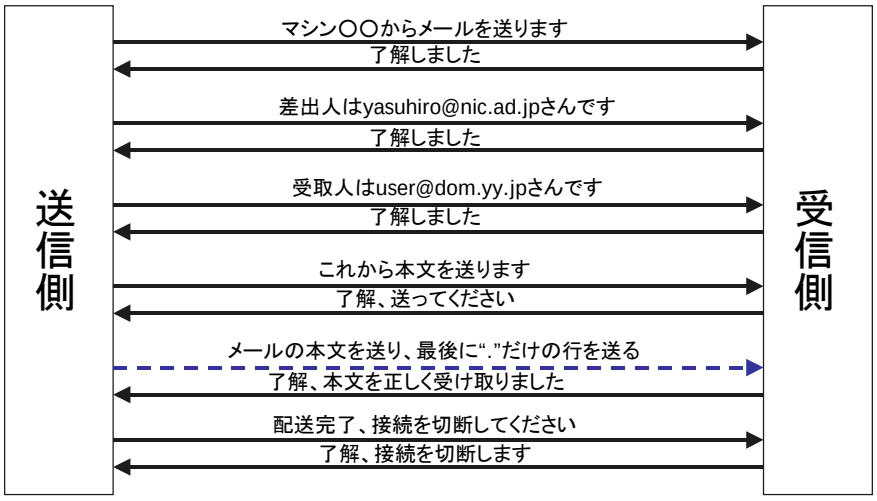
表 9：Well-konwn Port の例

プロトコル	ポート番号
SMTP	TCP/25
HTTP	TCP/80
DNS	TCP/53、UDP/53
FTP	TCP/20（ftp data） TCP/21（ftp command）

4.1 SMTP

SMTP*（Simple Mail Transfer Protocol）は、電子メールの配送について取り決めたプロトコルです。SMTP は RFC821 で規定されています。SMTP はインターネットメールのメッセージ形式を定義した RFC822 とともに、電子メールで重要な役割を果たしています。

SMTP のしくみと実際にやりとりされるコマンドを図 14 に示します。「メール送信」をクリックしたときに舞台裏で行われている事柄です。




```
% telnet ns1.dom.yy.jp 25
220 ns1.dom.yy.jp ESMTP Sendmail 8.9.3+3.2W/3.7W; Fri 12 Nov 1999 13:25:40 +0900
(JST)
HELO mx1.nic.ad.jp
250 ns1.dom.yy.jp Hello mx1.nic.ad.jp [202.12.30.137], pleased to meet you
MAIL From:<yasuhiro@nic.ad.jp>
250 <yasuhiro@nic.ad.jp>… Sender ok
RCPT To:<user@dom.yy.jp>
250 <user@dom.yy.jp>… Recipient ok
DATA
354 Enter mail, end with “.” on a line by itself
This is test.
.
250 NAA20561 Message accepted for delivery
QUIT
221 ns1.dom.yy.jp closing connection
```

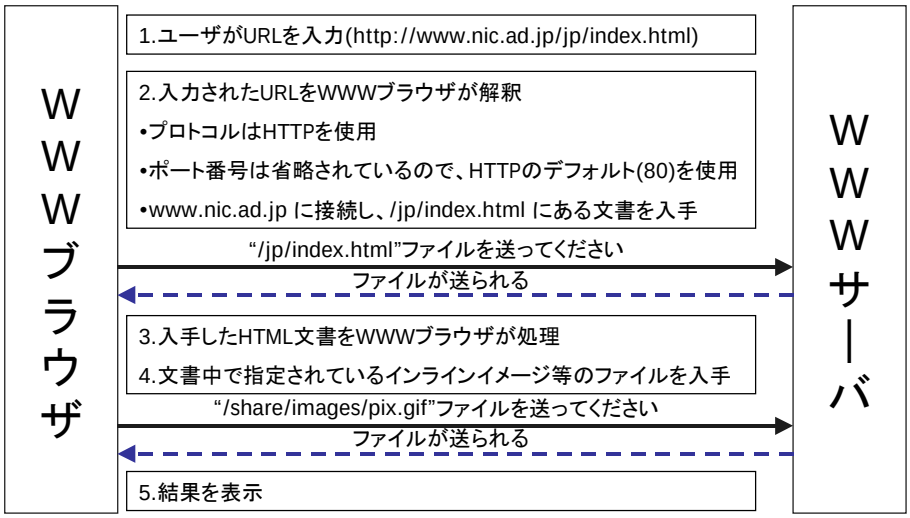
図 14：SMTP のしくみ

SMTP　「Simple Mail Transfer Protocol」の略。電子メール配送に関して取り決めているプロトコルです（RFC821）。

4.2 HTTP

HTTP*（Hypertext Transfer Protocol）は、Webでお馴染みのHTML（HyperText Markup Language）文書や画像、音声データ等の転送について取り決めたプロトコルです。HTTP は RFC2616 で規定されています。

HTTP のしくみと実際にやりとりされるコマンドを図 15 に示します。ブラウザで URL を入力したときに舞台裏で行われている事柄です。




```
% telnet www.nic.ad.jp 80
GET /jp/index.html

<HTML>
<HEAD>
        <META HTTP-EQUIV="Content-Type" CONTENT="text/html;CHARSET=iso-2022-jp">
        <META NAME="Resource-type" CONTENT="Document">

        <TITLE>Japan Network Information Center</TITLE>
（中略）
</TR>
</TABLE>
<!-- footer table end -->

<!-- bottom margin --><BR><BR><BR>
</BODY>
</HTML>
```

図 15：HTTP のしくみ

HTTP	「Hypertext Transfer Protocol」の略。HTML 転送等に利用されているプロトコルです（RFC2616）。

4.3 FTP

FTP*（File Transfer Protocol）は、ファイル転送のためのプロトコルで、現在でもソフトウェアの配布（ダウンロード）等のために広く利用されています。FTP は RFC959 で規定されています。

FTP は図 16 に示すように、相手側の FTP サーバとのやりとりを行う PI（プロトコルインタプリタ。セッション層とプレゼンテーション層の機能を実現）と、DTP（データ転送プロセス）の 2 つの構造を持っています。そして、次の順序でファイル転送を実現します。

1. PI 同士がやりとりして、認証、転送手順等を決定します。
2. DTP によって、実際のデータを転送します。

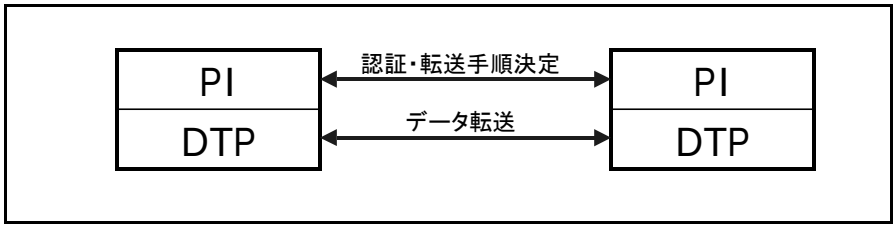
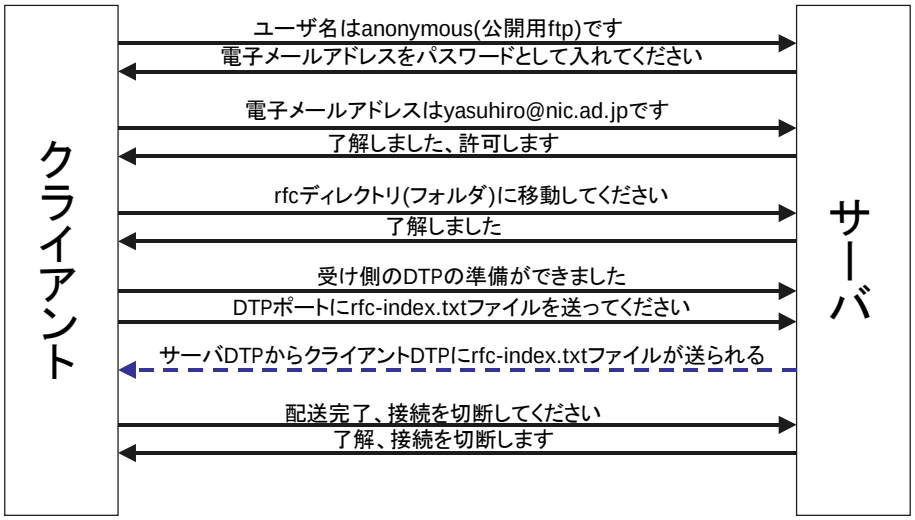


図 16：FTP の構造

FTP のしくみと実際にやりとりされるコマンドを図 17 に示します。たとえば、「ダウンロード開始」をクリックしたときに舞台裏で行われている事柄です。図 17 中で、クライアントからサーバに対して、「DTP ポートに rfc-index.txt ファイルを送ってください」というコマンドを送っているところまでが PI で、その後が DTP の処理です。

FTP　「File Transfer Protocol」の略。ファイル転送で使用されるプロトコルです（RFC959）。




```
% ftp -d ftp.nic.ad.jp
Connected to www1.nic.ad.jp.
220 www1.nic.ad.jp FTP server (Version wu-2.6.0(1) Thu Sep 2 15:31:24 JST 1999)
ready.
Name (ftp.nic.ad.jp:yasuhiro): anonymous
---> USER anonymous
331 Guest login ok, send your complete e-mail address as password.
Password:
---> PASS yasuhiro@nic.ad.jp
230 Guest login ok, access restrictions apply.
ftp> cd rfc
---> CWD rfc
250 CWD command successful.

ftp> get rfc-index.txt
---> PORT 202,12,30,131,163,72
200 PORT command successful.
---> RETR rfc-index.txt
150 Opening ASCII mode data connection for rfc-index.txt (411086 bytes).
226 Transfer complete.
local: rfc-index.txt remote: rfc-index.txt
420717 bytes received in 10 seconds (40.12 Kbytes/s)
ftp> quit
---> QUIT
221 Goodbye.
```

図 17：FTP のしくみ

5 商用化以降のインターネット技術動向

最後に、インターネットの商用サービス提供が始まってからの技術動向について説明します。日本では、1992 年に Spin（AT&T）、IIJ による接続サービスがスタートしたのが商用サービスの始まりでした。商用化が進むにつれて、利用者が研究者だけだった商用化以前とは異なり、さまざまなユーザからさまざまな要求がインターネットに対して寄せられるようになりました。

その変化に応じて、技術面でも新しい動きがあります。たとえば、次のような事柄が技術動向として挙げられるでしょう。

- 信頼性向上の必要性（5.1 を参照）
- より強固なセキュリティの必要性（5.2 を参照）
- Web 関連技術の充実（5.3 を参照）
- 標準化に対する実装（商品化）の先行（5.4 を参照）

5.1 信頼性向上の必要性

商用サービスにおいては、信頼性が重要です。サーバや経路（回線）にトラブルが発生しても、影響をできるだけ抑えなくてはなりません。そのために、さまざまな構成が使われるようになっています。

- サーバの二重化
  - 単純な二重化

    図 18（A）のような構成をとるものです。IP アドレスを 2 個公開し、DNS のラウンドロビン機能を使った手法で二重化します。1 台目がダウンすると、2 台目に切り替わるしくみですが、切り替えの際に遅延が生じます。
  - レイヤ 4 スイッチの導入

    図 18（B）のような構成をとるものです。代表 IP アドレスを公開し、1 台のサーバに見せかけます。ただし、レイヤ 4 スイッチにトラブルが発生すると、どちらのサーバにもアクセスできなくなるので、レイヤ 4 スイッチ自身の信頼性の向上も考慮する必要があります。
- 複数経路の確保
  - マルチホーム接続

    図 18（C）のような構成をとるものです。1 つの経路がダウンしても、別の経路で通信できるので信頼性が向上します。ただし、複数の接続先を確保しなくてはなりませんので、コストがかかります。

- ハウジングサービスの利用

  図 18（D）のような構成をとるものです。複数の接続先を持っている接続業者のネットワーク上のサーバを借りる（ハウジングする）ことによって、複数経路を確保します。

• ミラーサーバの利用

  図 18（E）のように、インターネット上に複数のサーバを置くものです。大手新聞社の Web サーバ等で利用されています。各サーバ間でデータが矛盾しないように注意しなければなりません。

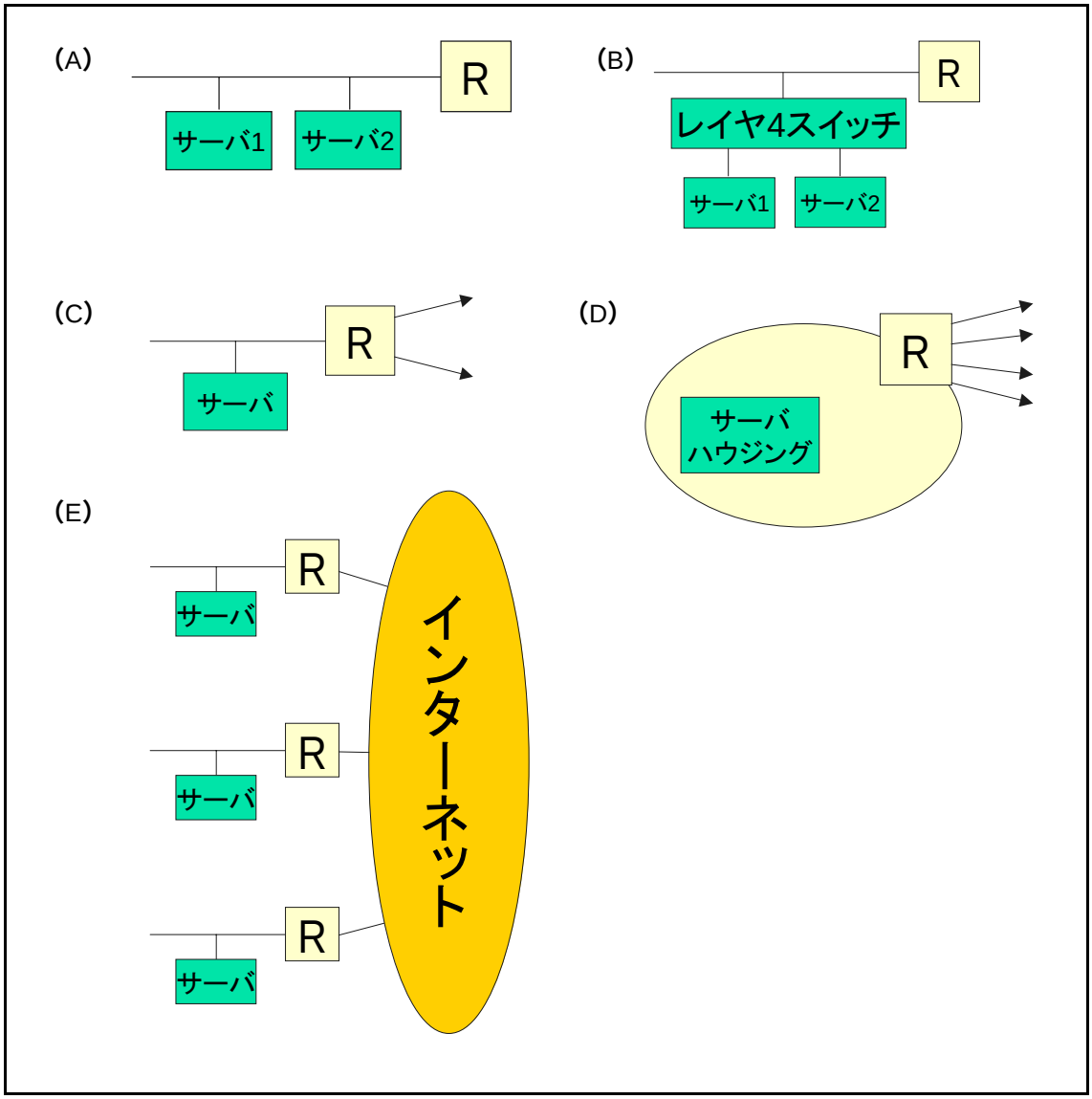


図 18：信頼性向上の手法

5.2 より強固なセキュリティの必要性

商用化以降、「いい人」だけがインターネットを利用する時代は終わり、インターネットを利用する際、セキュリティに留意する必要性が大変高くなりました。ただし、インターネットでは、不正侵入を完全に防ぐことは技術的にできません。まず、「入られにくいようにする」こと、「入られたことをすぐに見つけて対処する」こと、そして、万一侵入されたとしても「被害が最小限で済むようにする」ことが大切です。

- SPAM（前述）メールの防止

  MTA（Mail Transfer Agent：メール配送プログラム）に SPAM 防止機能を実装します。最新の sendmail、qmail 等にはこの機能が標準装備されていますが、設定を誤ったり、古い設定ファイル（sendmail.cf）を使用したりすると、SPAM 防止機能が生かされず、設定に不備のあるホストとして SPAM の踏み台にされてしまいます。

- ファイアウォールの利用

  不正侵入の防止、早期発見のために、ファイアウォールを導入するのも有用です。ファイアウォールには、フィルタ型、アプリケーションゲートウェイ型等の種類があります。ファイアウォールの設定に関しては、侵入を防止するのはもちろんですが、侵入を早く発見し、他のホストや内部ホストへの踏み台にされないように注意が必要です。なお、ファイアウォールについては、別の講演で詳しく解説されています。

- 通信路の安全の確保
- データの盗み見の防止
- データの改ざん、なりすましの防止

  Web ブラウザ等により利用され、安全なデータ転送を行うための SSL（Secure Socket Layer）、およびリモートホスト上で作業したり、ファイル転送を行ったりするための SSH（Secure Shell）等の技術があります。

今後、EC（Electronic Commerce）が普及していく上で、セキュリティはさらに重要になっていくでしょう。

5.3 Web 関連技術の充実

Web は、インターネットを爆発的に普及させた立役者と言ってもよいでしょう。インターネットの商用化以降、「Web でこんなことをやりたい」という要求がどんどん増え、そのための技術が充実してきています。

- CGI（Common Gateway Interface）による対話的な利用

  Web のフォーム入力や掲示板等で使われている技術で、Web サーバ側でプログラムを実行して、結果をブラウザ側に返す形式で処理するものです。処理が Web サーバ側で行われるため、Web サーバの設計の際に負荷を考慮する必要があります。

- クライアント側でのプログラム実行

  Web サーバに負荷のかかる CGI ではなく、サーバ側からプログラムをブラウザ側に送付し、ブラウザ側でプログラムを実行する形での利用も増えてきています。Java、JavaScript、VBScript が代表的なものです。アクセスが増えても Web サーバの負荷はあまり増加しませんが、送付されたプログラムがローカルのブラウザ側で実行されるので、セキュリティに配慮する必要があります。

- プラグイン機能

  ここ 4 ～ 5 年で使われるようになってきた技術で、Web ブラウザに機能を動的に追加するものです。

- プッシュ型アプリケーション

  サーバ側からクライアント側に、情報が更新されたタイミングで受動的に情報を配布する技術です。「ポイントキャスト」等が代表的です。天気予報や株価情報の配信等で利用されています。

- ストリーム型アプリケーション

  ダウンロードを行いながら、データを処理する技術です。従来のアプリケーションでは、ダウンロードが完了しないと処理を始められなかったので、大量のデータ処理やリアルタイム処理には無理がありました。

  ストリーム型アプリケーションでは、たとえば、画像や音声のデータをダウンロードしながら、リアルタイム処理を行えます。インターネットテレビやインターネットラジオでの応用が期待されています。

5.4 標準化に対する実装（商品化）の先行

インターネットが商用化されて以降、市場競争の原理が働き、「たくさん売れたものが事実上の標準」になってきました。新製品に盛り込んだ機能が、その製品でならうまく動くが、既存製品で問題が発生するとしても、その製品が売れてしまえば機能は普及するというわけです。この状況が進んできたため、インターネットプロトコルを IETF ＋ RFC で標準化するしくみに限界が出ているとも言われています。

5.5 まとめ

インターネットは、優れた拡張性、利便性、そして「自分たちで決める」自律性によって、今まで発展してきました。インターネットは、ほんのわずかの研究者、技術者のためのものではなく、誰でもが使う電化製品のようなものに変わってきたのです。

今、インターネットの技術的なしくみや標準化のしくみ、そして社会におけるインターネットの立場はターニングポイントに差しかかっています。将来のインターネット像を予測するのは難しいところですが、自律性を尊重しつつ発展していくことが望ましいと、発表者は考えています。