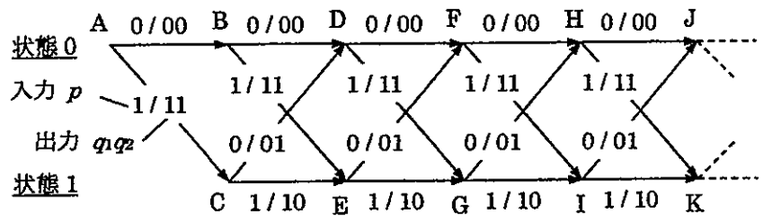


図 7-6　送信側における符号器の状態遷移を表すトレリス線図

直列変換器からなっている。入力 p とそのひとつ前のビットに相当するレジスタ内のビット（r）の排他的論理和（$p \oplus r$）を求め、その結果である q_2 と入力 p に相当する q_1 とを並列直列変換して出力 q_1 q_2 を送出する。従って出力の信号速度は入力の２倍になる。付加した排他的論理和の結果 q_2 が信号に冗長性を与えており、これが誤り制御の機能を生み出している。

このようにして得られたビット列を受信側ではもとのビット列に戻すことになる。その代表的な手法であるビタビ(Viterbi)復号アルゴリズムを以下に述べる。このアルゴリズムでは、トレリス(trellis)線図が用いられる。トレリス線図は符号器の状態遷移を時系列的に描いた図であり、その中に入力、出力のほかハミング距離を付記することによって信号の分析に利用できる。

図 7-5 の符号器において r がとる２つの値を符号器の２つの状態と定義し、初期状態を ０とする。このとき送信側のトレリス線図は図 7-6 のようになる。横方向は入力１ビットごとの時間経過をリンク（矢印）で表しており、各リンクには対応する入力（１ビット）と出力（２ビット）を斜線で分けて付記している。トレリス線図では、初期の時間帯を除けば同じパターンがビット列の終了まで繰り返される。

受信側では、受信したビット列とトレリス線図とを逐次比較しながら誤り制御を行う。具体的な例として、送信しようとするビット列が 00111 の場合を考える。このときの図 7-6 における状態遷移は A→B→D→G→I→K となる。そして送信側の符号器から出力されるビット列は 0000111010 となる。伝送中に３ビット目に誤りが生じ受信ビット列が 0010111010 となったときの受信側の動作について時間を追って見てみよう。受信側でも送信側と同じく、初期状態（時刻 t_0）は０であり、図 7-7 のトレリス線図でもこれを A で表している。一般的に最初の２ビットが誤りなく受信されると、次の時刻 t_1 における状態は、図 7-7(a)のように B あるいは C へ遷移するはずである。誤りのない場合の受信ビット列（A→B のとき 00、A→C のとき 11）と実際の受信ビット列 00 とのハミング距離はそれぞれ０および２である。図中にはこれらを示すとともに、各状態におけるハミング距離の累積値もカッコ内に付記している。この段階でもし判断するならば、ハミング距離の小さい A→B に対応した 00 が選ぶべきビット列ということになる。しかし、この段階では判断をしない。

これに続く２ビットがもし誤りなく受信されると、時刻 t_2 における状態は、一般的に図 7-7(b)に示すように D あるいは E になるはずである。ここで D への遷移には B→D および C→D の２通りがあり得る。実際の受信ビット列は 10 であるから、ビット列 00 に対応した B→D ではハミング距離が１であり、従って A→B→D のパスを経た D での累積ハミング距離は１となる。これに対してビット列 01 に対応した C→D ではハミング距離が２であり、この場合の A→C→D のパスを経た D での累積ハミング距離は４となる。これら２つの累積ハミング距離を比較すると前者の方が小さいので、D へ至るパスとしては A→B→D のみを残す。図ではこれを太い矢印で表している。そして D での累積ハミング距離を小さい方の値である１と定める。一方、E への遷移には B→E および C→E の２通りがあ

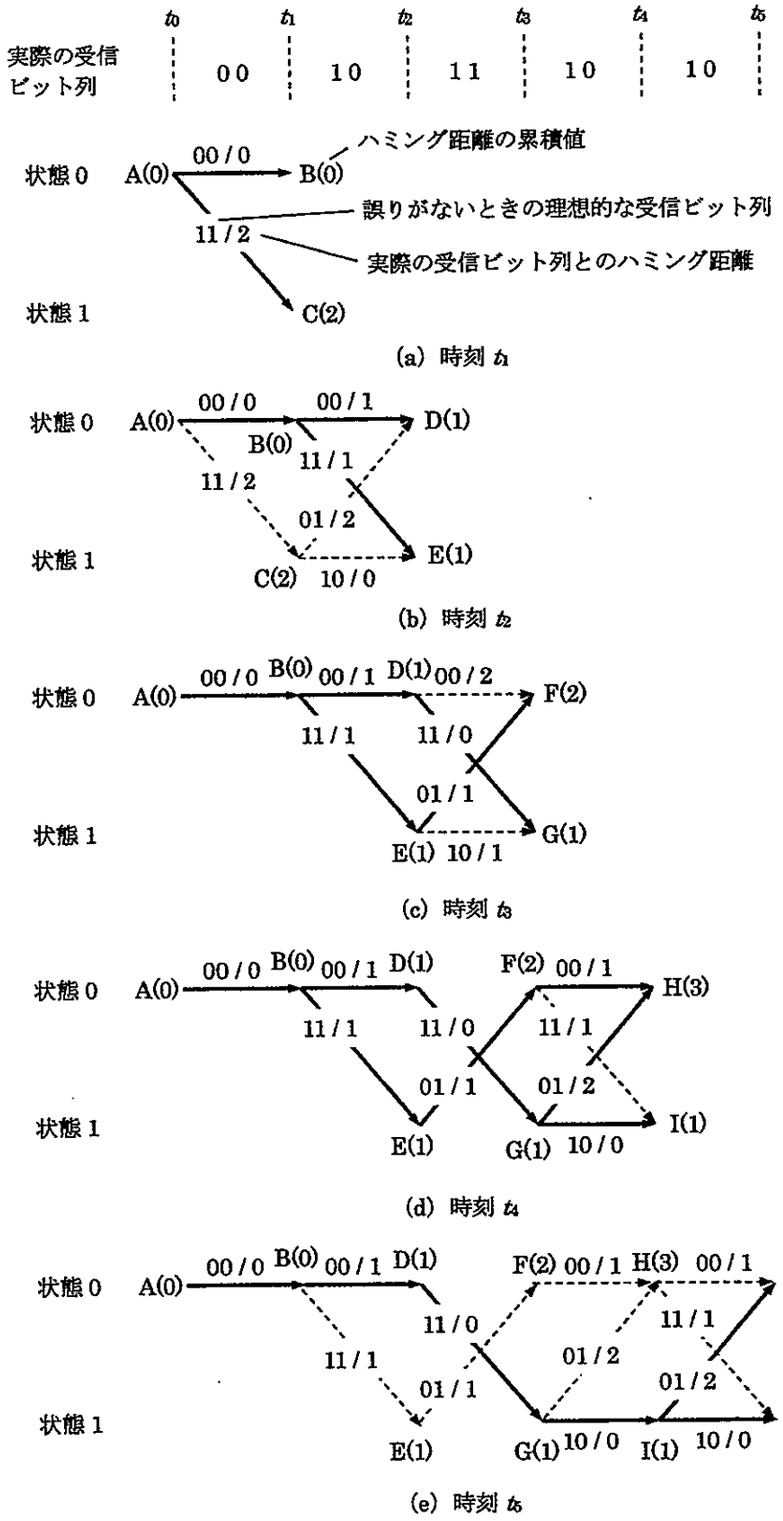


図 7-7 受信側における復号器の状態遷移を表すトレリス線図

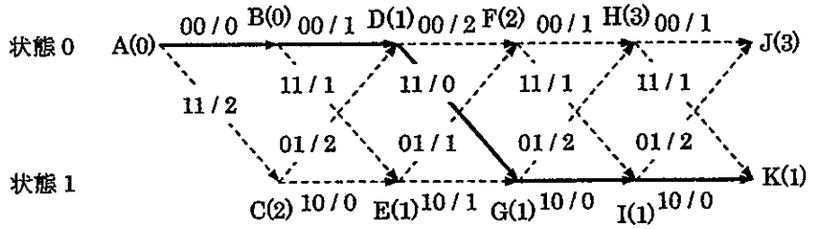


図 7-8 誤り制御をしたあとのトレリス線図

りうる。実際の受信ビット列は 10 であるから、ビット列 11 に対応した B→E ではハミング距離が 1 であり、従って A→B→E のパスを経た E での累積ハミング距離は 1 となる。これに対してビット列 10 に対応した C→E ではハミング距離が 0 であり、この場合の A→C→E のパスを経た E での累積ハミング距離は 2 となる。これら 2 つの累積ハミング距離を比較すると前者の方が小さいので、E へ至るパスとしては A→B→E のみを残す。図ではこれを太い矢印で表している。そして E での累積ハミング距離を小さい方の値である 1 と定める。

これ以降の時刻においても、上と同様に、各状態へ移る 2 つのリンクに対応した累積ハミング距離を順次比較し、それらのうちの小さいパスのみを残していく。これにより図 7-7(c)～(e)を得ることができる。最終時刻 t_6においては、2 つの状態 J および K での累積ハミング距離はそれぞれ 3 および 1 である。従って小さい方の累積ハミング距離に対応するパス A→B→D→G→I→K が最適な求めるパスであることが分かる。この結果をトレリス線図に示すと図 7-8 のようになる。従ってこれに対応するビット列 0000111010 が求めるべき誤り訂正されたビット列である。受信したビット列 0010111010 とこれとを比較すると、受信したビット列の中の 3 ビット目に誤りが発生していたことが分かる。

図 7-5 で示した符号器は最も簡単な構造の例であり、実際の符号器ではレジスタ（シフトレジスタ）のビット数（k ビット）はより大きくなっている。それらのビットをもとにした論理演算は複雑になっていて、出力のビット数も図 7-5 の例より大きくなっている。従って、トレリス線図の中の状態数（2^k個）は多く、トレリス線図はより複雑なものになる。

8．インターネット

電話を中心とした過去の通信サービスの時代では、公的な性格をもつ組織・企業体が公衆通信ネットワークと称して大規模なネットワーク設備を提供し、サービスに見あう料金を徴収するしくみをとっていた。1980 年代の半ば以降、通信事業の民営化・通信設備の開放とともに数多くの大規模ネットワークが現れると同時に、パーソナルコンピュータの普及に伴ってオフィス等に LAN が積極的に導入されるようになった。ネットワークに接続された端末がそのネットワークに接続された他の端末と通信をするのであれば特段の問題は生じない。しかし、通信サービスの本来の役割を実現し任意の端末間で信号のやりとりを可能とするには、これらの多種多様なネットワークを相互接続する必要がある。このために現れたのがインターネットである。インターネットではその構造からプロトコルが重

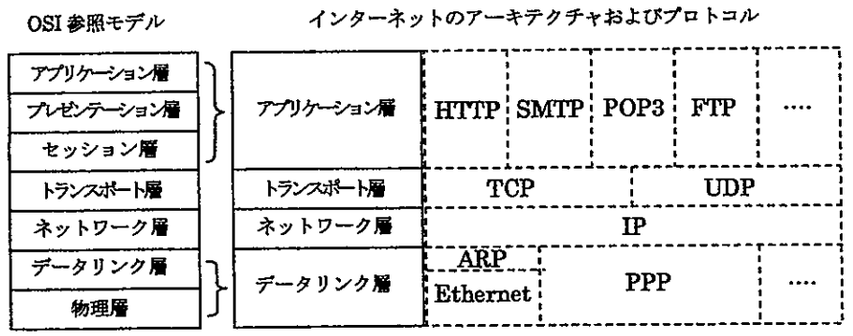


図 8-1 OSI 参照モデルとインターネットのアーキテクチャおよびプロトコルとの関係

要な役割を担っている。この章ではインターネットに関わる基本事項を解説する。

8．1 インターネットのアーキテクチャ

インターネットに関わる技術の国際標準を議論し策定しているのは IETF（Internet Engineering Task Force）と呼ばれる団体である。そこでは、OSI 参照モデルをもとにしつつも、より単純化したプロトコルの枠組みが用いられている。それは TCP/IP モデルと呼ばれており、4 つの階層が定められている。図 8.1 には、OSI 参照モデルと TCP/IP モデルの関係を示している。TCP/IP モデルの最下位層であるデータリンク層は、OSI 参照モデルの物理層とデータリンク層を統合したものであり、TCP/IP モデルの最上位層であるアプリケーション層は、OSI 参照モデルのセッション層とプレゼンテーション層、アプリケーション層を統合したものである。

ここでネットワーク層に対応した IP（Internet Protocol）は、複数の個別ネットワークを相互接続し、それらの間にパケット（IP パケット）を伝達するためのプロトコルであり、インターネットにおいて重要な役割を担っている。トランスポート層に対応したプロトコルには TCP（Transmission Control Protocol）と UDP (User Datagram Protocol)とがある。前者は、パケットをアプリケーション層に届けるにあたって信頼性を重視し、欠落や順不同のないパケットを届けるためのプロトコルである。それに対して後者は、遅延が小さくなることを優先し、機能を単純化したプロトコルである。

データリンク層にある ARP (Address Resolution Protocol) は、IP パケットに付けられるアドレス（IP アドレス）からそれに対応した MAC アドレスを求めるためのプロトコルである。また、アプリケーション層の HTTP (Hyper Text Transfer Protocol)はホームページの閲覧、SMTP (Simple Mail Transfer Protocol)および POP3 (Post Office Protocol version 3)は E メールのやりとり、FTP (File Transfer Protocol)はファイルの転送に使われる。

8．2 IP パケット

インターネットにおいてネットワーク間を伝搬する IP パケットの内部構成を図 8-2 に示す。これは現在広く用いられている IP である IPv4 (Internet Protocol version 4)において定められているものである。「サービスタイプ」は、通信目的に応じて決まるサービス品質（QoS: Quality of Service）を確保するため、パケットに優先順位とともに、高スループット、低コストなどの条件を付すための

ネットワークアドレスとを比較する。両者が一致した場合には、それに対応したポートから IP パケットを送出する。ルーティングテーブルの中にある「0.0.0.0」は、宛先ネットワークアドレスがルーティングテーブルの中で見つからなかった場合を意味しており、その場合はそこに対応づけられているポートから IP パケットが送出される。

（サブ）ネットワーク内の通信には Ethernet が適用される場合が多いが、必ずしもそれに限定されたものではなく、FDDI や ATM が使われる場合もある。従って１つの信号が（サブ）ネットワーク間を転送されるとき、データリンク層での PDU（MAC フレーム）は（サブ）ネットワークごとに異なる場合もある。しかしこのような場合でも、その中に積み込まれている IP パケットは、（サブ）ネットワークが異なっても共通である。すなわち、IP パケットはデータリンク層におけるシステムの違いを吸収あるいは隠蔽するはたらきをもっている。これをネットワーク透過性と呼ぶ。

ルーティングテーブルの内容を設定時のまま固定してルーティングする方法を静的ルーティングと呼ぶ。これに対して、ルータ間でルーティングテーブルを交換し、時間の経過とともに新しい内容に更新していく方法を動的ルーティングと呼ぶ。インターネットでは後者が用いられている。

ルーティングを行う機器として、近年、ルータ以外にスイッチも使われるようになっている。 ルータは汎用プロセッサを用いて IP パケットをソフトウェアで処理するのに対して、スイッチではロジックが組み込まれた専用 IC（ASIC: Application Specific Integrated Circuit）を用いてハードウェアで処理する。スイッチはデータリンク層で使われるものであることから、このようにネットワーク層で使われるものは特にレイヤ３スイッチと呼ばれる。ルータはサービス仕様が多岐にわたる場合に適しており、スイッチは高速処理が必要な場合に適している。

８．５　ホストの識別

インターネットでは、ホストを識別する記号として上で述べた IP アドレスのほかに、MAC アドレスおよびドメイン名が使われる。MAC アドレスは、ホストがもつネットワーク接続デバイスに対応づけて、ネットワークを意識しないで付けられている識別記号である。従って、ネットワーク側で使われている IP アドレスをそのまま MAC アドレスとして使うことはできず、両者は相互に独立な関係にある。一方、ドメイン名は、インターネットを使う人間にとってホストの識別記号を使いやすくする目的で、ホストの属性を表す身近な用語や文字をもとに作られたものである。ネットワークの接続関係よりもむしろインターネット使用者が帰属する組織などをもとに作られている。

ホスト識別のためのこれらの記号は独立に決められているので、そのままではインターネットで利用することができない。これらに対して相互変換をする必要があり、そのためにいくつかの技術が準備されている。図 8-7 にそれらを示す。

（1）アドレス解決とアドレス発見

ホストは、自分の IP アドレスとサブネットワークマスクからネットワークアドレスを知ることができる。従って、送ろうとする IP パケットの宛先が同じネットワークに属しているかそうでないかを IP アドレスから判断することができる。属している場合には IP パケットを入れ込んだ MAC フレームを宛先ホストへ直接送り、属していない場合にはネットワークに接続されているルータへ MAC フレームを送り、そこから他ネットワークへの転送はルータに委ねる。いずれの場合にしろ、送信元のホストは属しているネットワーク内に MAC フレームを送出するので MAC アドレスを必要とする。

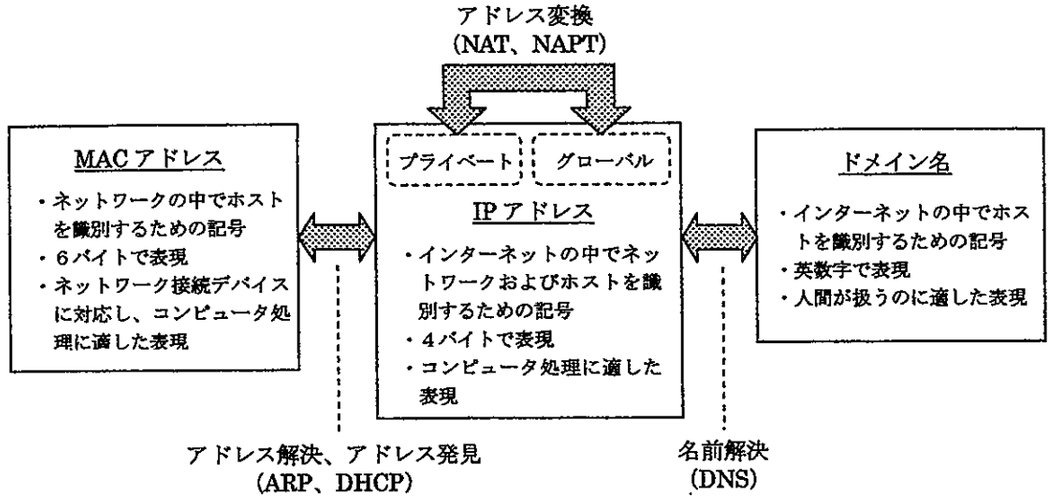


図 8-7　インターネットにおける識別記号の変換

もし MAC アドレスを知らない場合にはそれを調べなければならない。この調べる操作をアドレス解決と呼び、そのためのしくみが ARP（Address Resolution Protocol）である。

ARP では、送信元のホストは宛先 IP アドレスを付けた MAC フレームをネットワーク内の全ての機器に送出（このことをブロードキャストと呼ぶ）する。この IP アドレスに対応した機器のみが MAC フレームを返し自身の MAC アドレスを問い合わせたホストに伝える。これによりその送信元ホストは求める MAC アドレスを手に入れることができる。

インターネットでは ARP とは逆の機能も必要である。多数のホストに IP アドレスを割り当てる場合には、労力を軽減するために作業の自動化が求められる。またホストが他のネットワークへ移動したり、ネットワークのアドレスを変更したりする場合にも自動化が望ましい。このように IP アドレスを得る操作をアドレス発見と呼び、そのための自動化のしくみとして DHCP（Dynamic Host Configuration Protocol）がある。

DHCP では、IP アドレスを求めるホストは、IP アドレスを割り当てる役割をもつ DHCP サーバとの間で IP パケットを用いて通信することにより IP アドレスを得る。ただし、要求および応答において宛先機器の IP アドレスは不明であったり未定であるため、使うことができない。そこで、これらの操作でもブロードキャストを利用する。DHCP サーバは要求に対して IP アドレスを割り当てる際、その有効期限も併せて通知する。

（2）アドレス変換

IP アドレスには、プライベートアドレスとグローバルアドレスがあることは既に述べた。組織内では、割り当てに自由度が大きいプライベートアドレスが多く用いられている。その場合、ホストはグローバルアドレスを使うインターネットには接続することができない。このことはセキュリティの点では好ましいが、通信という観点からは大きな制約を受けていることになる。

そこで、組織内のネットワークと外部のネットワークとの接続点に設けるルータ（これをアクセスルータと呼ぶ）に、プライベートアドレスとグローバルアドレスとを相互に変換する機能を備える。これをアドレス変換と呼び、具体的なしくみには NAT(Network Address Translation)や

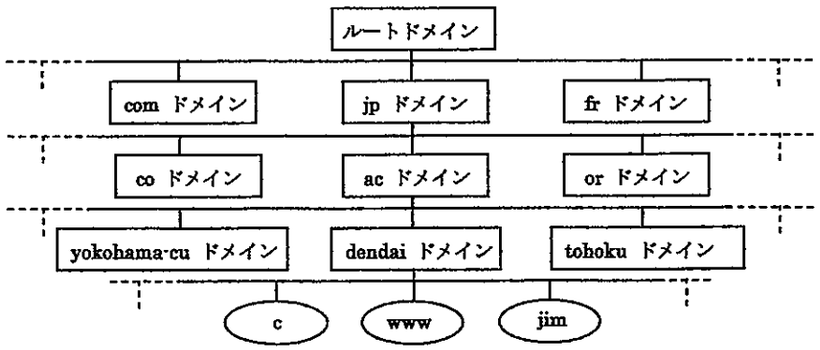


図 8-8　インターネットにおけるドメインの階層構造

NAPT(Network Address Port Translation)がある。NAPT は「IP マスカレード」とも呼ばれる。前者は２つのアドレスを一対一で変換し、後者はポート番号を使って一対多の変換を行う。

（3）ドメイン名と名前解決

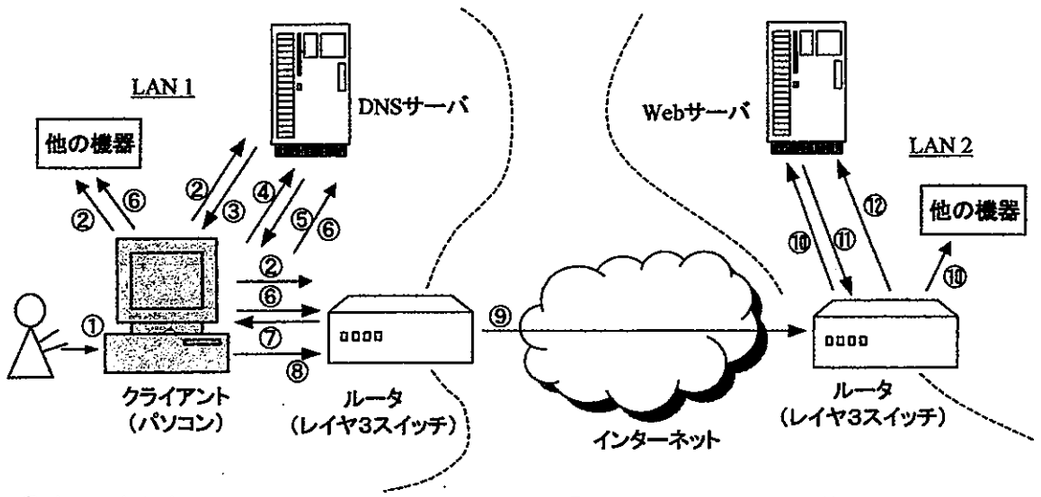
E メールアドレスでは「kingkong@c.dendai.ac.jp」、Web サイトの URL では「http://www.dendai.ac.jp」という表記が使われるが、これらの中でそれぞれ「c.dendai.ac.jp」、「www.dendai.ac.jp」がドメイン名と呼ばれる部分である。これらのドメイン名の例は具体的なアプリケーションに対応したホストを指しているが、より広い範囲を指しホストを特に指定しない「dendai.ac.jp」もドメイン名と呼ばれる。

インターネットに接続されている極めて多数のホストをドメインという枠組みで管理しているのが DNS(Domain Name System)であり、各ドメインに付けられた識別記号がドメイン名である。ドメインは階層構造で管理されている。ドメイン名に含まれている「.（ピリオド）」は階層の区分に対応している。ドメイン名の末尾に付けられる「jp」や「com」などに対応したドメインをトップレベルドメイン、ひとつ前の「ac」や「co」などに対応したものをセカンドレベルドメインと呼ぶ。トップレベルドメインの更に上位にあるのはルートドメインである。図 8-8 にドメインの階層構造を示す。

各ドメインには DNS サーバが配置されており、そこにはそのドメインに属している下位ドメインに関する情報（下位ドメインの名前と下位ドメインに配置された DNS サーバの IP アドレスとの対応関係など）が蓄積されている。また最下位のドメインにある DNS サーバには、そのドメインに属するホスト名と IP アドレスとの関係が蓄積されている。従って、インターネットの中では DNS サーバはツリー状に配置されていることになる。

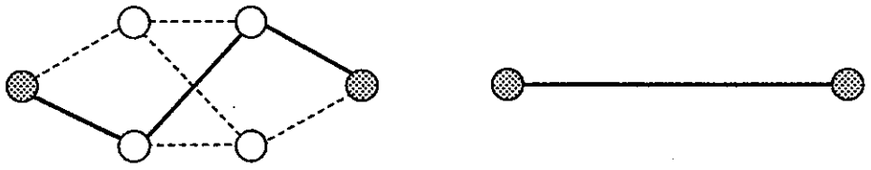
宛先のドメイン名を保持しているがそれに対応する IP アドレスを知らないホストは、DNS サーバに問い合わせをして IP アドレスを手に入れる。これを名前解決と呼ぶ。最下位ドメインの DNS サーバ（ローカル DNS サーバ）では、名前解決を繰り返す過程で他の DNS サーバから入手した情報を保存している。従って、ホストはまずこのローカル DNS サーバへ問い合わせを行う。そこで回答が得られない場合には、より高位のドメインに配置された DNS サーバへ問い合わせ、そこから下位へ順次問い合わせるようにする。

図 8-9 には、ホームページを閲覧する場合のように遠隔地のネットワークにある Web サーバへアク



①ドメイン名入力
②DNSサーバのMACアドレス問い合わせ(ARP)
③DNSサーバのMACアドレス回答
④ドメイン名送信(IPアドレスの問い合わせ)
⑤IPアドレス回答(DNS名前解決)
⑥ルータのMACアドレス問い合わせ(ARP)
⑦ルータのMACアドレス回答
⑧IPパケット送信
⑨IPパケット送信(　　PPP)
⑩WebサーバのMACアドレス問い合わせ(ARP)
⑪WebサーバのMACアドレス回答
⑫IPパケット送信

図 8-9　遠隔地のネットワークにある Web サーバへのアクセス手順



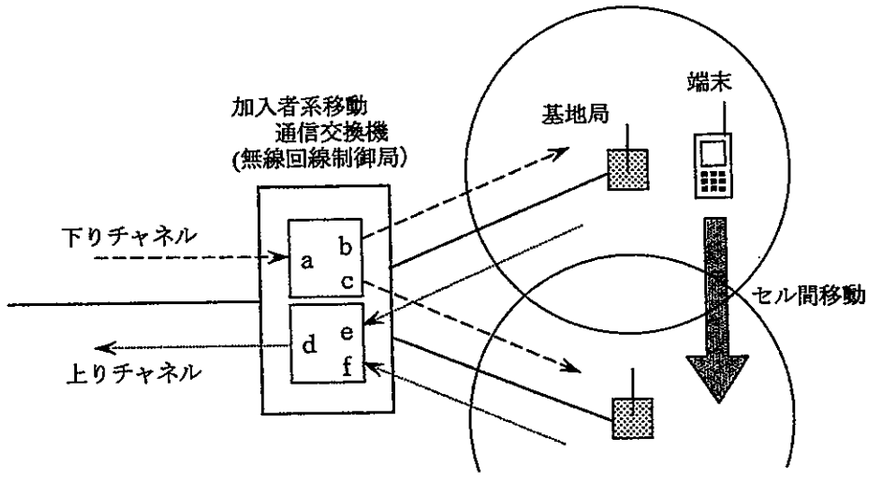
(a) IP で見たネットワーク　　(b) TCP で見たネットワーク

図 8-10 プロトコルによって異なるネットワークの形

セスする手順の例を示している。ここでは、ローカル DNS サーバ内の保存情報を使ってアドレス解決や名前解決をしながら、信号を Web サーバまで転送する様子を表している。

8．6　TCP と UDP

トランスポート層は、ネットワークの存在を意識することなく送信側端末と受信側端末が正確に通信でき、同時にアプリケーション層に存在する各アプリケーションとの間で信号のやりとりをするための階層である（図 8-10）。インターネットではトランスポート層のためのプロトコルとして TCP（Transport Control Protocol）と UDP（User Datagram Protocol）が準備されている。一言で表すとパケット交換に基づく IP がもっている欠点（信号欠落、順不同）を補うのが TCP であり、補わず処理の簡略化を優先しているのが UDP である。前者はコネクション型の通信、後者はコネクション



	下りチャネル		上りチャネル	
	a－b	a－c	d－e	d－f
ハンドオーバ前	ON	OFF	ON	OFF
ハンドオーバ時	ON	ON	ON	ON
ハンドオーバ後	OFF	ON	OFF	ON

図9-3　ハンドオーバ時におけるマルチ接続

のではなく、セル内にある全ての移動端末に送信される。端末が移動するので位置に関しては常に不確定性があること、および媒体として電波を用いていることから、この方法が用いられる。

（5）ハンドオーバ

通信中に移動端末が隣接するセル境界を横切った場合に、回線を基地局間で切替えて通信を継続させることをハンドオーバと呼ぶ。ハンドオーバ時に通信品質の低下（瞬断など）が生じないようにすることが重要である（図9-3）。

１０．無線 LAN

LANに接続する端末の移動性を確保したり、接続用ケーブルの輻輳をなくし、接続替えの煩雑さを軽減しようとすると、有線よりも無線の技術の方が適している。端末の入出力リンクに無線を利用したLANを無線LANと呼ぶ。近年では無線機器の低価格化とともに無線LANのオフィスや家庭への導入が進んでいる。ただ、無線 LAN は、利用可能な帯域に限界がありセキュリティ上の危険性（盗聴）を抱えていることを念頭において利用しなければならない。

ここでは無線LANの規格として広く用いられているIEEE802.11について概要を述べる。

１０－１　無線 LAN の構成

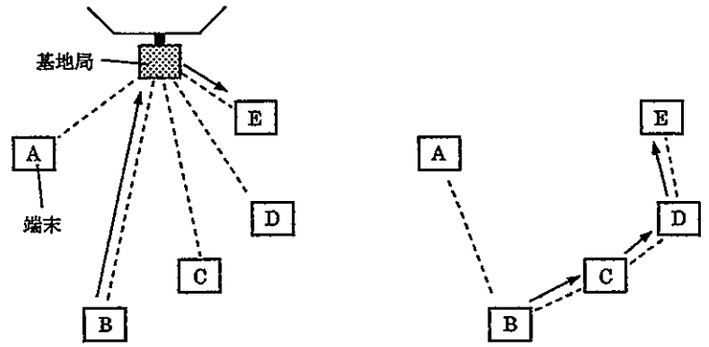


図 10-1　無線 LAN の形態（端末ＢからＥへの通信を太い矢印で示している）

利用する電波には 2.4 GHz 帯と 5 GHz 帯とがある。前者は ISM (Industrial, Scientific, and Medical) 帯と呼ばれ、免許を持つことなく幅広い用途で利用できる周波数帯である。後者は無線 LAN に限定して無免許で利用することができる。現在広く用いられている最大伝送速度 54 Mbit/s のシステムでは、これら２つの周波数帯が使われており（5 GHz 帯を使うものを 802.11a 標準、2.4 GHz 帯を使うものを 802.11g 標準と呼ぶ）、変調形式としては OFDM (Orthogonal Frequency Division Multiplexing) が用いられている。OFDM は、もとの信号を複数の低速信号に分離し、それぞれの低速信号を周波数と位相の異なる直交信号に当てはめて並列伝送をする方式である。伝送条件に適応させながら低速信号を割り振ることができるので、無線システムのように伝送条件が不安定なシステムに適した変調形式である。

ネットワークには図 10-1 に示すように２通りの形態がある。そのうちの１つはインフラモードと呼ばれ、固定した基地局と移動可能な端末とからなる。端末と外部ネットワーク間の通信のほか、端末間の通信もすべて基地局を介して行われる。これは通常の無線 LAN で用いられている形態である。他の１つはアドホックモードと呼ばれ、基地局を設けず、端末だけからなるネットワークである。従って通信は端末間で直接行われる。固定した基地局をもたないことから、移動性に優れている。遠く離れた端末間の通信は、隣接した端末間の通信を複数回繰り返して達成される（これをマルチホップと呼ぶ）。従って端末は中継ノード（ルータ）の機能も備える必要があり、端末で行う信号処理が複雑なものとなる。

１０－２　媒体へのアクセス方式

媒体へのアクセス方式としては CSMA/CA（Carrier Sense Multiple Access with Collision Avoidance）が用いられている。これは Ethernet で用いられている CSMA/CD（Carrier Sense Multiple Access with Collision Detection）に類似した方式である。送りたいパケットをもつ基地局または端末は、送信前にまず無線チャネルをモニタする。無線チャネルが使われていなければ直ちにパケットを送出する。使われていればチャネルが空いたのを確認後、ある時間 t_d だけ待って無線チャネルのモニタを再度開始し、送信できるまで上記と同じ手順を繰り返す。時間 t_d は、固定した長さを

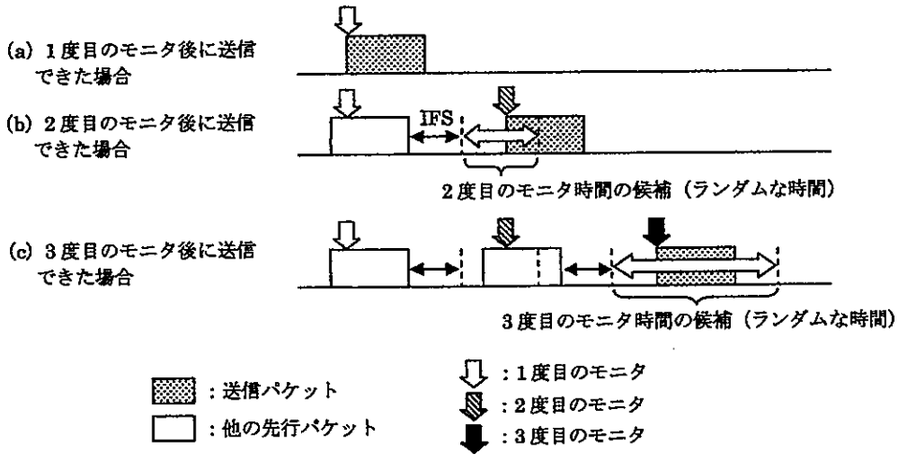
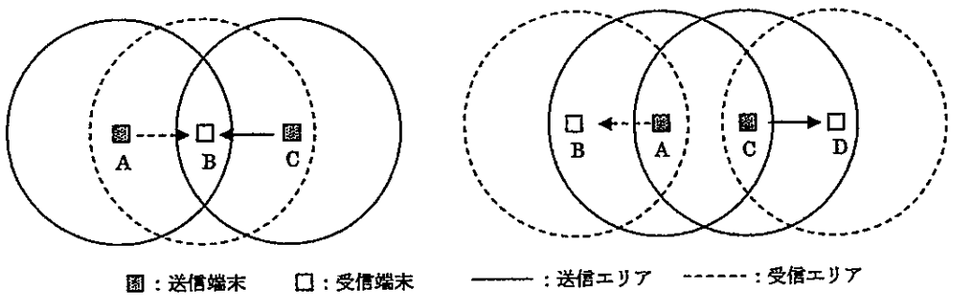


図 10-2　CSMA/CA の動作例



(a) 隠れ端末問題　　(b) さらされ端末問題

図 10-3　無線 LAN の端末相互間に生じる問題

もつ成分 IFS（Inter Frame Space）とランダムな時間長をもつ成分とからなる。IFS はパケットの優先順位によって 3 段階に分けられており、優先順位が高いパケットのときほど短くなるように決められている。ランダムな時間長をもつ成分は、パケットの衝突を避けるためのものであり、方式の名称に含まれている「CA（Collision Avoidance）」はこの手法を指している。ランダムに設定するとはいえ衝突の発生する可能性はある。衝突が起こるとパケットを再送することになるが、再送を繰り返すごとにランダムな時間幅を拡大して衝突を起こりにくくする方法がとられている。CSMA/CA における信号の時間変化を図 10-2 に示す。

１０－３　隠れ端末問題、さらされ端末問題

CSMA/CA が機能するためには、相互に影響を及ぼす可能性のある端末の間で他端末の影響を把握できる必要がある。しかし実際のネットワークでは必ずしもそうではない。例としてアドホックモードの場合について見てみよう。図 10-3（a）のように端末 A が端末 B に向けてパケットを送ろうとしたとき、すでに端末 C は端末 B にパケットを送りつつあったとする。端末 A は、端末 C の信号を受

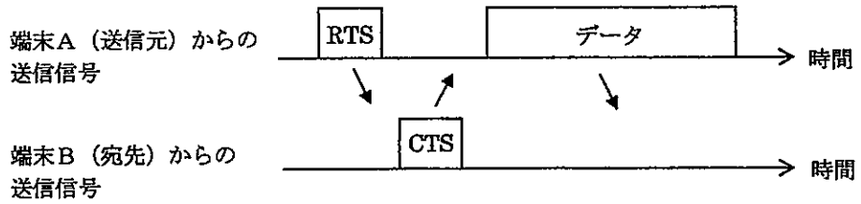


図 10-4　RTS/CTS 方式での信号のやりとり

信できない領域にいるので、チャネルが空いていると判断してパケットを送ることになる。そうすると、端末 B において 2 つのパケットが同時に受信され衝突を起こす。これを隠れ端末問題と呼ぶ。一方、図 10-3（b）のように端末 A が端末 B にパケットを送ろうとしたとき、すでに端末 C は端末 D に向けてパケットを送りつつあったとする。端末 A は端末 C からの信号を受信できる領域にいるので、チャネルが空いていないと判断してパケットの送出を控える。しかし、端末 B は端末 C からの信号を受信できない領域にいるので、たとえ端末 C が送信中であってもその影響は受けていない。従って、端末 A は本来は送信を開始すべきなのである。これをさらされ端末問題と呼ぶ。これら 2 つの問題はいずれも、送信側端末が受信側端末の状態を知ることができないことから生じている。図 10-3 ではアドホックモードのネットワークを例にあげているが、インフラストラクチャモードのネットワークにおいても同様の問題が存在する。図 10-3 の端末 B および D を基地局と見なせばインフラストラクチャモードの場合となる。

隠れ端末問題およびさらされ端末問題を解消するには、送受信を制御するための制御パケットが用いられる。これには RTS（request to send）パケットと CTS（clear to send）パケットがある（図 10-4）。前者は、送信端末 A がデータパケットを送信する前に、宛先となる端末 B の状況を調べるために送信するパケットである。内部には端末 A および B のアドレスが付加されている。後者は、宛先端末 B が RTS パケットを受信してデータを受信可能な状態にあるとき、そのことを送信端末 A に折り返し知らせるためのパケットである。内部にはやはり端末 A および B のアドレスが付加されている。送信端末 A は、RTS パケットを送信した後、宛先端末 B からの CTS パケットを受信できたときのみデータパケットを送信する。こうすることにより、隠れ端末問題およびさらされ端末問題を同時に解消することができる。RTS パケットや CTS パケットはデータパケットに比べて極めて短いので、もしこれらが他のパケットと衝突することがあっても、その影響は小さくて済む。

１０－４　ルーティング

アドホックモードのネットワークでは、端末に中継機能を付与する必要があるので、パケットの転送経路を決め、それに従ってパケットを送出する機能（ルーティング機能）も端末に持たせなければならない。通信ケーブルを用いた一般のネットワークでは、ノードやリンクは基本的には固定しているので、転送経路を決める主な要因はネットワーク内のトラヒックの分布やノード、リンクの容量である。トラヒックが特定のノードやリンクに集中したときは、それらを避けるように転送経路が決められる。ノードやリンクの容量はほぼ固定なのでトラヒックが安定していれば転送経路の変更が発生することは少ない。これに対してアドホックモードのネットワークでは、端末間の距離およびそこで

の伝搬条件が一定ではないので、トラヒックのほかにリンクの特性も変化する。さらに、バッテリー残量はノードとしての能力を左右する。バッテリー残量の少ない端末は、できるだけ中継に使わない方がよい。従って転送経路の決定は、通信ケーブルを用いた一般のネットワークに比べて複雑なものとなる。

ルーティングには大きく分けると２つの方式がある。そのうちのひとつは、必要なデータ（ルーティングテーブル）を常時から全ての端末間で定期的にやりとりしておき、パケットを転送することが必要になったときにはそれを利用して端末間で順次パケットを転送していく方式である。これはプロアクティブ型（またはテーブル駆動型）と呼ばれる。もうひとつは、特定の２つの端末間でパケットを転送することが必要になったとき、その都度、それら端末間での最適な転送経路を求める方式である。これはリアクティブ型（またはオンデマンド型）と呼ばれる。アドホックモードのネットワークでは、ネットワークの状況が刻々と変化するので、これら２つの方式のうちリアクティブ型が適している。

図 10-4 にはリアクティブ型の手順を示す。まず送信元端末は、宛先端末の識別子を付加した経路探索用メッセージ（RREQ: route-request）を隣接する全ての端末へ送出（ブロードキャスト）する。ネットワーク内の各端末は、RREQ を受け取ると、それに端末の識別子を追加して隣接する端末へ送出する。複数の RREQ が届いたときは最初のものだけを受け取り、他は破棄する。RREQ にある宛先識別子が自分自身のものに一致したときには、その中にある一連の端末識別子を読み取り、それを経路通知メッセージ（RREP: route-report）に付けて、RREQ を受け取った相手の端末へ送出する。同様にして他の端末は RREP を受け取ると、その中にある一連の端末識別子に従って次の端末へ送出する。

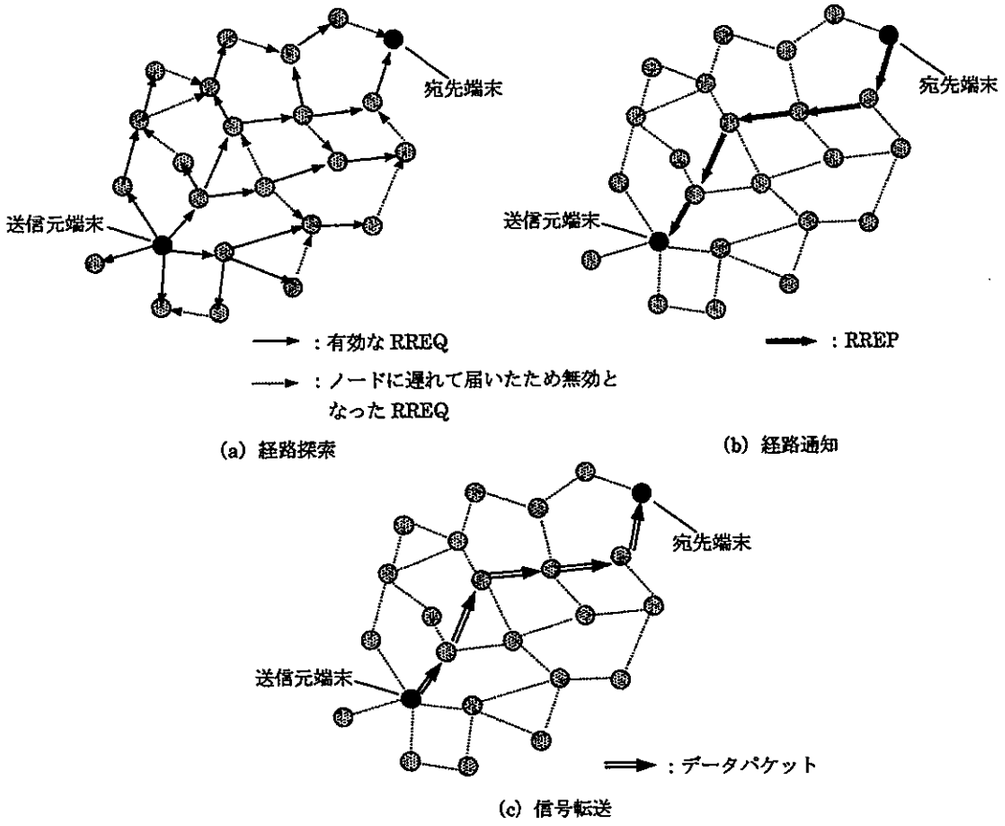


図 10-4　ルーティングの手順

これらの動作により、RREQ は最終的に宛先端末へ到着し、逆に RREP は送信元端末へ到着する（図 10-4 (a) および (b)）。送信元端末は、RREP の中にある一連の端末識別子を読み取り、最適な経路を知ることになる。その経路をデータパケットに付加しておけば、データパケットは RREP が通った経路を逆に進んで宛先端末へ届くことになる（図 10-4 (c)。

１１．むすび

このテキストでは、通信ネットワークに関わる要素技術を述べてきた。極めて多くの技術を集めて通信ネットワークが出来上がっていることが理解できると思う。ネットワークは、半導体集積回路や光ファイバーといったハードウェア技術の発展を基礎にして、有線・無線の伝送技術、プロトコル技術、アプリケーション技術の進展とともに変化してきている。特に、インターネットの登場はネットワークの歴史において大きな変革であった。それまで通信事業者主導で進められていた通信ネットワークの導入・管理をユーザ主導に変えてしまった。そして、ネットワークの利用形態もそれまでとは大きく変わり、インターネットは単に技術の枠に留まらず人間の生活までも変えてしまったと言える。

従来の電話を主体としたネットワークも、新たに登場したインターネットもそれぞれ長所と短所をもっている。今後は、これらの短所を補った新しい通信ネットワークを構築していく必要がある。数年前から通信事業者によって提供が始まっている NGN (Next Generation Network、次世代ネットワーク)はそれを狙ったネットワークであり、そこでは①全ての通信を IP (Internet Protocol)化するとともに、②QoS (Quality of Service)の制御設定を可能にして通信品質を保証できるようにし、③多彩なマルチメディアサービスを提供して、④ネットワークのセキュリティ機能を高めている。

通信ネットワークは、多くの個別技術が使われているだけではなく、それらが相互に結合して出来上がった巨大な組織体である。今後も、それぞれの技術の進歩とともに通信ネットワークは変革を遂げていくものと思われる。

以上