ITプロ／ITエンジニアのための

徹底攻略

試験番号
640-802J*
640-822J

Cisco CCNA／CCENT

［640-802J］［640-822J］対応

ICND1編

教科書

株式会社ソキウス・ジャパン 編著

*CCNA（640-802J）は、ICND1（640-822J）の出題範囲に相当する部分のみを記載しています

インプレスジャパン

本書は、CCNA（Cisco Certified Network Associate）およびICND1（Interconnecting Cisco Networking Devices Part 1）の受験用教材です。著者、株式会社インプレスジャパンは、本書の使用による「CCNA」および「ICND1」試験への合格を一切保証しません。

本書の内容については正確な記述に努めましたが、著者、株式会社インプレスジャパンは本書の内容に基づくいかなる試験の結果にも一切責任を負いません。

はじめに

Cisco CCNAおよびCCENTは、インターネット分野のリーディングカンパニーであるシスコシステムズの認定資格です。

これまでCCNAは、「シスコのルータやスイッチング機器を使用した比較的単純なネットワークの設定やトラブルシューティングが実践できる」ことを認定する、ネットワーク技術者のための登竜門的な資格でした。しかし技術の進展に伴い、アソシエイトレベルであるCCNAに要求される知識範囲は大幅に拡大しています。そこで2007年に、登場したのが、エントリーレベルの新資格であるCCENTです。CCENTは、CCNAの試験範囲のうち基本的な事項を対象にしている「ICND1」試験に合格することで取得できますので、シスコの資格がより身近なものになったということができるでしょう。

本書はCCNAおよびICND1受験のための学習書です。ネットワークの初心者の方でも無理なく学習に取り組んでいただけるように、ネットワークの基礎知識も丁寧に解説しました。日々シスコ製品に接していても、試験のために機器を自由に操作・検証しながら学習ができる方は多くはないでしょう。そこで本書では、ネットワークの構成図や出力を豊富に掲載しました。図を確認し、出力を追っていくことによって、だんだんに実際の設定の感覚が身に付くはずです。また、章末の演習問題は、その章で学習した内容が理解できているか確認していただけると同時に、試験の雰囲気をつかんでいただくためにも有効です。

本書をご活用いただき、より多くの方がシスコのネットワークに親しみ、目指す資格を取得されることを願ってやみません。

2008年8月

著者

シスコ技術者認定の概要

シスコ技術者認定（Cisco Career Certification）は、インターネットワーキングや同社ルータ製品に関する技術の証明および、エンジニアの育成を目的とした認定資格です。認定基準は米国シスコシステムズにより厳格に定められ、最新のIPネットワークに対応した技術者資格として世界的に認知されています。

シスコ技術者認定資格は、技術分野別に7つのカテゴリに分類されています。それぞれのカテゴリに、エントリ、アソシエイト、プロフェッショナル、エキスパートの4つの認定レベルがあります。

【シスコ技術者認定資格一覧】

認定分野	エントリー	アソシエイト	プロフェッショナル	エキスパート
ルーティング&スイッチング	CCENT	CCNA	CCNP	CCIE Routing & Switching
デザイン	CCENT	CCNA、CCDA	CCDP	CCDE
ネットワークセキュリティ	CCENT	CCNA Security	CCSP	CCIE Security
サービスプロバイダー	CCENT	CCNA	CCIP	CCIE Service Provider
ストレージネットワーキング	CCENT	CCNA	CCNP	CCIE Storage Networking
ボイス	CCENT	CCNA Voice	CCVP	CCIE Voice
ワイヤレス	CCENT	CCNA Wireless	CCVP	CCIE Wireless

CCENTおよびCCNAの取得方法

● CCENTの取得方法

CCENTはICND1（試験番号640-822J）に合格することで取得できます。

・ICND1（試験番号640-822J）
試験時間：90分、出題数：40～50問、受験料：13,388円（税込）

● CCNAの取得方法

CCNAは、次の2つの方法で取得することができます。

・1科目で取得
・CCNA（試験番号640-802J）
試験時間：90分、出題数：50～60問、受験料：26,775円（税込）

・以下の2科目に合格することで取得
・ICND1（試験番号640-822J）
試験時間：90分、出題数：40～50問、受験料：13,388円（税込）
・ICND2（試験番号640-816J）
試験時間：75～90分、出題数：40～50問、受験料：13,388円（税込）

※試験時間と問題数は、変更になる可能性があります。

受験申し込み方法

シスコ技術者認定試験を受験するには、ピアソンVUEもしくはピアソンVUEのテストセンターに受験を申し込みます。

● ID番号の取得

ピアソンVUEで初めて受験する場合は、ピアソンVUE IDを取得する必要があります。以下のURLの指示に従って、登録します。

http://www.vue.com/japan/Registration/index.html

①ピアソンVUEのWebサイトで申し込み

以下のURLにログイン後、試験名、会場、日時を指定します。

URL：http://www.vue.com/japan/index.html

②ピアソンVUEのコールセンターで申し込み

以下の受付番号に電話をし、申し込みます。

Tel：0120-355-173 または0120-355-583
Fax：0120-355-163
E-mail：pvjpreg@pearson.com
営業時間：土日祝日を除く平日、午前9時～午後6時

③テストセンター

以下のサイトで受験を希望するテストセンターを選択し、電話で申し込みます。テストセンターによっては、受験当日の申し込みを受け付けているところもあります。

http://www.vue.com/japan/TestcentersList/

Fax：0120-355-163
E-mail：pvjpreg@pearson.com
営業時間：土日祝日を除く平日、午前9時～午後6時

試験日程

ピアソンVUEの各試験会場で随時、受験することができます。

CCNAの問い合わせ先

試験の概要、受験後の認定証の取得に関する詳細および問い合わせについては、シスコのWebサイトを参照してください。

・シスコシステムズ
URL http://www.cisco.com/jp/index.shtml

本書の活用方法

本書は解説ページと演習問題の2部構成になっています。

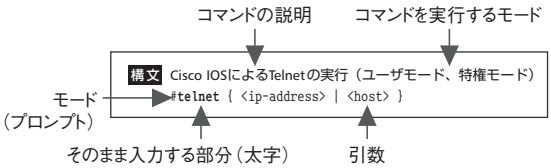
解説

● 用語

ネットワーク技術の習得に、用語の理解は不可欠です。すぐに参照したい用語には米印（※）を付け、脚注で解説しました。また、アスタリスク（*）を付けた用語は巻末の用語集で説明しています。

● 構文

ルータやスイッチの設定・管理操作に必要な構文を多数掲載しています。構文は次のルールで記述しています。



- **太字** ……表記されたとおり入力する。省略形で入力できるコマンドもある
- < > ……引数。該当する文字や値を入力する
  例）<username> →ユーザ名を入力する
- [ ] ……オプション。必要に応じて設定する要素
- { | } ……選択。{ }で括られたものから、いずれか1つを選択して入力する
  例）{ a | b } →「a」か「b」のいずれかを入力する

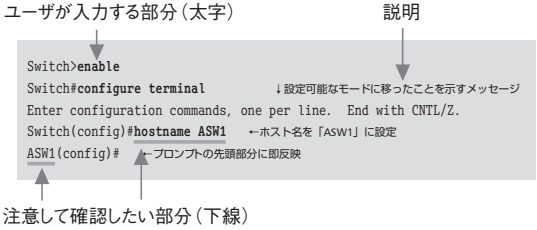
ユーザモード、特権モードのいずれも可能な場合のプロンプトは「#」で示しました。また、モードは以下のとおり省略しています。

- ユーザEXECモード → ユーザモード
- 特権EXECモード → 特権モード
- コンフィギュレーションモード → コンフィグモード

巻末に構文索引を掲載しましたので活用してください。

● 出力

実際の設定作業を理解しやすくするために、本書ではコマンドの出力結果を数多く掲載しています。出力の中、ユーザが入力する部分は太字で示しました。また、必要な事項を的確に参照できるように、重要なポイントには適宜下線や説明を付加してあります。



● 本書で使用したマーク

解説の中で重要な事項や補足情報は次のマークで示しています。

Point	重要な技術情報や試験対策のうえで必ず理解しておかなければならない重要事項
Memo	試験対策としては必須ではないが、解説の内容を理解したり、知識を深めたりするために役立つ情報

演習問題

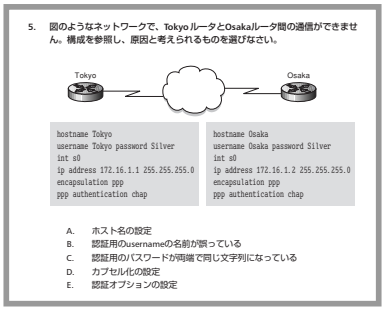
各章の最後には5問～10問の演習問題が用意されています。演習問題を解くことによって、理解度を確認できるだけでなく、試験の出題傾向を把握することができます。

●【問題】

シスコ技術者認定試験には、さまざまな出題形式があります。出題形式の詳細は付録で説明していますので、参照してください。各章の演習問題には選択形式の問題を、付録ではシミュレーション形式の問題を、それぞれ実際の試験と同じイメージで掲載しました。

多肢選択式

問題文を読んで、選択肢の中から正しいもの、あるいは誤りのあるものを選びます。必要に応じて、ネットワーク図や出力を参照します。


5. 図のようなネットワークで、TokyoルータとOsakaルータ間の通信ができません。構成を参照し、原因と考えられるものを選びなさい。

Tokyo　Osaka

```
hostname Tokyo
username Tokyo password Silver
int s0
ip address 172.16.1.1 255.255.255.0
encapsulation ppp
ppp authentication chap
```

```
hostname Osaka
username Osaka password Silver
int s0
ip address 172.16.1.2 255.255.255.0
encapsulation ppp
ppp authentication chap
```

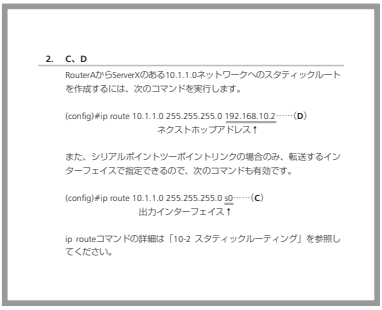
A. ホスト名の設定
B. 認証用のusernameの名前が誤っている
C. 認証用のパスワードが両端で同じ文字列になっている
D. カプセル化の設定
E. 認証オプションの設定

●【解答】

演習問題の解答と解説を読んで、理解できているかどうかを確認します。

解答と解説

解答のポイントを説明しています。必要に応じて、本文の参照箇所を示しています。また、正解の選択肢は太字で表記しています。


2. C、D

RouterAからServerXのある10.1.1.0ネットワークへのスタティックルートを作成するには、次のコマンドを実行します。

(config)#ip route 10.1.1.0 255.255.255.0 192.168.10.2……(D)
ネクストホップアドレス↑

また、シリアルポイントツーポイントリンクの場合のみ、転送するインターフェイスで指定できるので、次のコマンドも有効です。

(config)#ip route 10.1.1.0 255.255.255.0 s0……(C)
出力インターフェイス↑

ip routeコマンドの詳細は「10-2 スタティックルーティング」を参照してください。

※ 本書に掲載したURLは2008年8月現在のものです。URLとWebサイトの内容は変更になる可能性があります。

目次

はじめに …… 3
シスコ技術者認定の概要 …… 4
本書の活用方法 …… 6

第1章 ネットワークの基礎とOSI参照モデル

1-1 ネットワークとは …… 14
1-2 ネットワークでできること …… 16
1-3 ネットワークトポロジ …… 20
1-4 プロトコル …… 24
1-5 OSI参照モデル …… 25
1-6 カプセル化と非カプセル化 …… 31
1-7 ピアツーピア通信 …… 33
1-8 2進数／10進数／16進数の変換 …… 34
1-9 演習問題 …… 40
1-10 解答 …… 42

第2章 TCP/IPプロトコル

2-1 TCP/IPプロトコルスタック …… 44
2-2 IP …… 48
2-3 ARP …… 52
2-4 ICMP …… 57
2-5 TCP …… 66
2-6 UDP …… 79
2-7 DHCP …… 82
2-8 DNS …… 90
2-9 HTTP …… 96
2-10 FTPとTFTP …… 100
2-11 SMTPとPOP …… 105
2-12 Telnet …… 107
2-13 SNMP …… 109
2-14 演習問題 …… 113
2-15 解答 …… 115

第3章 イーサネットLAN

3-1 イーサネットの概要 …… 118
3-2 LANの規格とイーサネットの種類 …… 121
3-3 接続メディア …… 127
3-4 イーサネットフレーム …… 134
3-5 MACアドレス …… 136
3-6 CSMA/CD …… 138
3-7 ネットワークデバイス …… 143
3-8 レイヤ2スイッチング …… 152
3-9 スパニングツリープロトコル …… 162
3-10 演習問題 …… 175
3-11 解答 …… 177

第4章 ネットワークセキュリティの基礎

4-1 ネットワークセキュリティの必要性 …… 180
4-2 攻撃の主体や目的の把握 …… 182
4-3 攻撃の手法 …… 184
4-4 一般的な脅威の緩和 …… 186
4-5 セキュリティシステム …… 187
4-6 暗号技術 …… 190
4-7 演習問題 …… 194
4-8 解答 …… 196

第5章 Cisco IOSソフトウェアの操作

5-1 Ciscoデバイスへの接続 …… 198
5-2 Cisco IOSソフトウェアのEXECモード …… 202
5-3 CLIの使い方 …… 206
5-4 Cisco IOSの接続診断ツール …… 220
5-5 演習問題 …… 227
5-6 解答 …… 229

第6章 IPv4アドレスとサブネット化

6-1 IPアドレッシング …… 232
6-2 NATおよびPATの概要 …… 238
6-3 サブネットワーク …… 246
6-4 IPアドレスの計算 …… 253
6-5 演習問題 …… 263
6-6 解答 …… 265

第7章 Catalystスイッチの起動と基本設定

7-1 Catalystスイッチの種類 …… 270
7-2 企業内LANの設計 …… 273
7-3 Catalystスイッチの初期起動 …… 275
7-4 IOS CLIによるスイッチの基本設定 …… 284
7-5 スイッチの基本ステータスの表示 …… 290
7-6 コンフィギュレーションの保存 …… 298
7-7 MACアドレステーブルの管理 …… 301
7-8 二重方式と速度の設定 …… 305
7-9 スイッチのセキュリティ …… 308
7-10 演習問題 …… 331
7-11 解答 …… 333

第8章 Ciscoルータの起動と基本設定

8-1 サービス統合型ルータ …… 336
8-2 Ciscoルータの初期起動 …… 338
8-3 IOS CLIによるルータの基本設定 …… 344
8-4 ルータの基本ステータスの表示 …… 350
8-5 コンフィギュレーションの保存 …… 360
8-6 ルータのセキュリティ …… 362
8-7 演習問題 …… 371
8-8 解答 …… 373

第9章 Ciscoデバイスの管理

9-1 CDP …… 376
9-2 Cisco IOSによるTelnet操作 …… 385
9-3 Ciscoルータのメモリと起動の流れ …… 398
9-4 Cisco IOSソフトウェアの管理 …… 408
9-5 パスワードの復旧 …… 418
9-6 デバッグによるトラブルシューティング …… 423
9-7 演習問題 …… 431
9-8 解答 …… 433

第10章 ルーティングの基礎

10-1 ルーティング …… 436
10-2 スタティックルーティング …… 441
10-3 ダイナミックルーティング …… 448
10-4 アドミニストレーティブディスタンスとメトリック …… 458
10-5 演習問題 …… 463
10-6 解答 …… 465

第11章 ディスタンスベクタールーティング

11-1 ディスタンスベクター …… 468
11-2 ルーティングループの回避 …… 472
11-3 RIPの概要 …… 487
11-4 RIPの設定 …… 489
11-5 RIPの検証 …… 498
11-6 演習問題 …… 502
11-7 解答 …… 505

第12章 WAN接続

12-1 WANテクノロジーの概要 …… 508
12-2 WANデバイス …… 510
12-3 WAN回線の種類 …… 516
12-4 HDLC …… 527
12-5 PPP …… 529
12-6 インターネットへの接続 …… 536
12-7 演習問題 …… 543
12-8 解答 …… 545

第13章 Cisco SDM

13-1 Cisco SDMの概要 …… 548
13-2 Cisco SDMの基本設定 …… 553
13-3 Cisco SDMを使用したDHCP設定 …… 561
13-4 Cisco SDMを使用したPATの設定 …… 567
13-5 演習問題 …… 572
13-6 解答 …… 574

第14章 無線LANの基礎

14-1 無線LANとは …… 576
14-2 電波の種類 …… 577
14-3 無線LANの規格 …… 581
14-4 無線LANの基本構成 …… 586
14-5 無線LANのアクセス制御 …… 590
14-6 無線LANクライアントのアソシエーション …… 593
14-7 無線LANのセキュリティ …… 596
14-8 無線LAN実装時の考慮事項 …… 613
14-9 演習問題 …… 616
14-10 解答 …… 618

用語集

用語集 …… 619

付　録　試験の出題形式とシミュレーション問題

付録-1 試験の出題形式 …… 646
付録-2 シミュレーション問題 …… 654

索引 …… 670
Cisco IOSコマンド構文索引 …… 684

第1章

ネットワークの基礎とOSI参照モデル

1-1 ネットワークとは
1-2 ネットワークでできること
1-3 ネットワークトポロジ
1-4 プロトコル
1-5 OSI参照モデル
1-6 カプセル化と非カプセル化
1-7 ピアツーピア通信
1-8 2進数／10進数／16進数の変換
1-9 演習問題
1-10 解答

1-1 ネットワークとは

ネットワークとは、複数台のコンピュータをケーブルや赤外線、電波など何らかの手段でつなぎ、相互に情報をやり取りできるようにした仕組みをいいます。正式にはコンピュータネットワークと呼ばれ、企業や学校、家庭などで幅広く利用されています。

■ コンピュータネットワークの分類

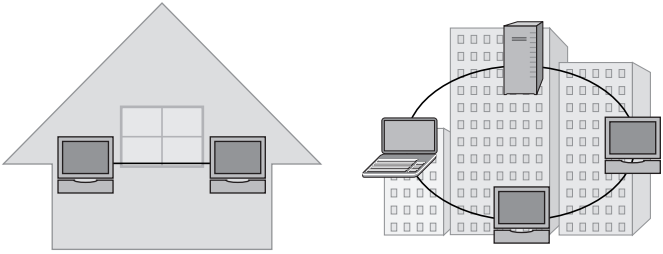
コンピュータネットワークには、2台のコンピュータを1本のケーブルで接続した小規模なネットワークから、インターネットのように地球規模でコンピュータを接続したものまでさまざまです。本書では、規模や用途に応じて、ネットワークを次のように分類しています。

・LAN
・WAN
・インターネット

■ LAN

LAN（Local Area Network）は、家庭内や学校、企業内など限られた範囲にある機器を接続したネットワークを指します。LANは利用するユーザが自由にネットワークを構築し、使用することができます。

【さまざまなLAN】

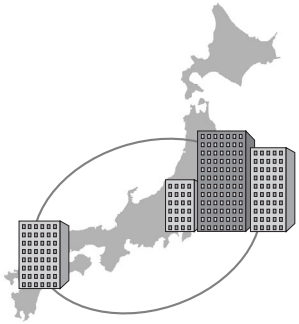


家庭内LAN　　企業内LAN

■ WAN

WAN（Wide Area Network）は、地理的に離れた場所にあるLANとLANを結ぶ比較的大きな範囲のネットワークを指します。そのためWANは、NTTやKDDIなどの電気通信事業者が提供する通信サービスを利用して通信を行います。企業の拠点間や、大学のキャンパスのLAN同士を接続するといった目的に使用されます。

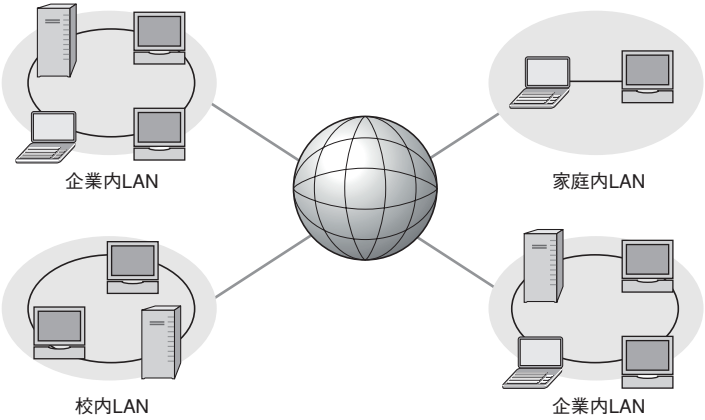
【WAN】



■ インターネット

インターネット（Internet）は、世界中のさまざまなネットワークを相互に接続することによって形成された巨大なコンピュータネットワークです。インターネットは誰でも自由に使用することができ、パソコンだけでなく携帯電話やPDA（個人用の携帯情報端末）、ゲーム機などからも手軽に接続して情報をやり取りできます。

【インターネット】



また、インターネットの技術を使って構築された企業内ネットワークを**イントラネット**といいます。イントラ（intra）は「内部の」という意味を持ち、利用者は特定の企業内や地域内のユーザのみに限定されます。イントラネットを利用すると、ユーザはWebブラウザや電子メールなどの使い慣れたアプリケーションソフトをそのまま利用し、外出先からインターネット経由で社内情報システムや電子掲示板を利用することができます。

1-2 ネットワークでできること

コンピュータをネットワークに接続することで、データやハードウェアなどのリソースを共有し、効率的に活用することができます。

■ リソースの共有

コンピュータネットワークを利用すると、ユーザは情報とハードウェアリソース（資源）を**共有**することができます。たとえば、あるサーバ内のファイルをコピーして使用したり、ほかのコンピュータに接続されたプリンタを使って印刷したりすることが可能になります。

ネットワークで共有されるリソースには、次のようなものがあります。

● データおよびアプリケーション

ネットワークでは、サーバやほかのコンピュータに保存されたデータやアプリケーションを使用することができます。

たとえば、サーバに共有するデータを保存すると、データの一元管理が可能になり、また既存のデータをすべてのユーザで活用できるので、作業の効率化を図ることができます。アプリケーションを共有すると、インストールや管理の手間を省けるだけでなく、個々のコンピュータのディスクスペースの節約にもなります。

● ハードウェアリソース

周辺機器をネットワークに接続すると、ネットワーク上の複数のユーザで共有でき、機器を効率的に活用できるようになります。共有するハードウェアとしては、カメラやスキャナなどの入力装置、プリンタなどの出力装置が一般的です。記憶装置については、次の「ネットワークストレージ」の項を参照してください。

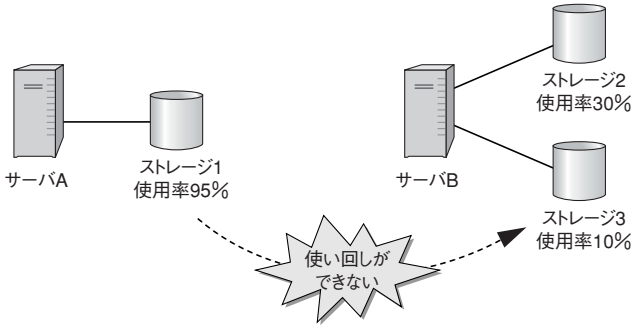
● ネットワークストレージ

ネットワークストレージとは、ネットワークを介して接続するストレージ（記憶装置）やその利用形態を指します。接続形態により、次の3種類に分類されます。

・DAS（Direct Attached Storage）

サーバとなるコンピュータ本体にストレージを直接接続する形態、あるいは装置そのものを指します。DASは、複数のサーバでストレージを共有することができないため、サーバ台数の増加や、特定のストレージ容量が不足した場合でも、ほかのサーバに接続されたストレージを利用することができないなど非効率的です。

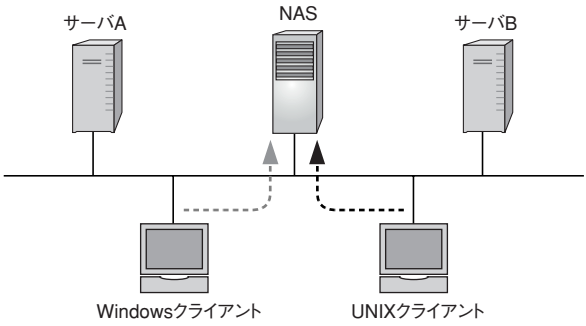
【DAS】



・NAS（Network Attached Storage）

サーバとなるコンピュータなしでストレージをネットワークに直接接続する形態、あるいは装置そのものを指します。NASにはファイルシステムやネットワーク通信機能が最初から内蔵されているので、導入や追加が容易です。また、OSが異なる複数のクライアントからでも簡単にデータを共有することができます。

【NAS】

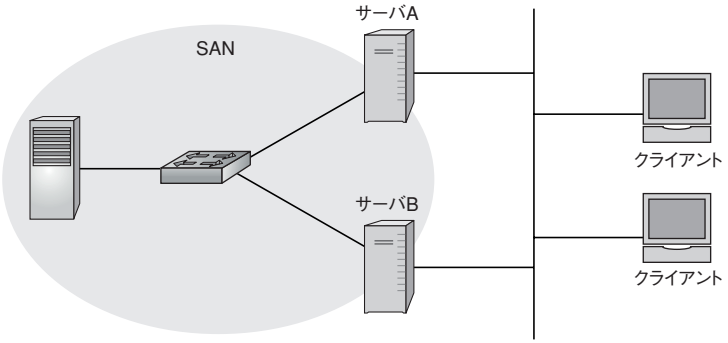


・SAN（Storage Area Network）

サーバとストレージ間をファイバチャネル※1で接続したストレージ専用のネットワークです。分散配置されたストレージを仮想的に1つに集約することで、ストレージの一元管理を可能にしています。

※1 **【ファイバチャネル】**Fibre Channel：コンピュータと外部記憶装置を結び高速なデータ転送を可能にする方式、または高速に相互通信するためのチャネル（通信路）技術のこと。伝送媒体には光ファイバのほか、銅線を使用することも可能

【SAN】



● バックアップデバイス

テープドライブのようなバックアップデバイスを接続し、複数のコンピュータからのファイルを集約して一元管理することができます。ネットワークストレージを使用し、複数のファイルを1つにまとめるアーカイブなどを行うこともできます。

■ ネットワークユーザアプリケーション

ネットワーク上にはネットワークに接続するユーザ向けのさまざまなアプリケーションがあります。一般的なネットワークユーザアプリケーションには、次のものがあります。

● 電子メールアプリケーション

電子メールは、ユーザ同士がメッセージやファイルを気軽にやり取りできるアプリケーションです。ユーザはMicrosoft OutlookやEudora、Thunderbirdなどさまざまな電子メールアプリケーションを使用し、メールサーバを介して情報をやり取りします。

● Webブラウザ

Webブラウザは、Webページ*を閲覧するためのアプリケーションです。Webブラウザを使用すると、インターネット上に公開されている豊富な情報を閲覧できるほか、メーカーや顧客との連絡、注文や調達処理、情報検索などの作業を共通のインターフェイスで実行できるため、全体的な生産性を向上させることができます。代表的なWebブラウザには、Microsoft Internet ExplorerやFirefox、Opera、Netscape Navigatorなどがあります。

● インスタントメッセージング

インスタントメッセージングとは、インターネットに接続中のユーザを確認し、その中の任意のユーザとリアルタイムにチャット（会話）することができるアプリケーションです。代表的なインスタントメッセージングソフトには、Windows Live MessengerやYahoo!メッセンジャー、ICQなどがあります。

● コラボレーション

コラボレーションとは、業務に関連する複数の担当者が互いに協調しながら進めていく共同作業を指します。コンピュータネットワークを利用して、情報共有やコミュニケーションの円滑化を図り、グループでの協調作業を支援することが容易にできます。コラボレーションソフトウェアは、グループ内の連携作業から大規模なプロジェクトまで幅広い範囲で利用することができます。最も一般的に使用されているソフトの1つにLotus Notesがあります。なお、コラボレーションソフトウェアは**グループウェア**とも呼ばれます。

● データベース（ファイルサーバ）

データベースとは、大量のデータを一定の規則に従って蓄積し、一元管理できるようにしたものを指します。データベースの操作や保守、管理をするためのソフトウェアを**DBMS**（DataBase Management System）といいます。ユーザはアプリケーションからDBMSへアクセスしてデータを操作することで情報を一括管理し、効率的に活用することができます。代表的なデータベースソフトウェアには、Oracle DatabaseやMicrosoft Accessがあります。

1-3 ネットワークトポロジ

ネットワークトポロジとは、コンピュータやプリンタ、ネットワークデバイス※2の「つなぎかた」のこと、つまり、接続形態を指します。ネットワークトポロジによって、ノード※3の物理的なレイアウトやデータの通信路（パス）が決定されます。

■ トポロジの種類

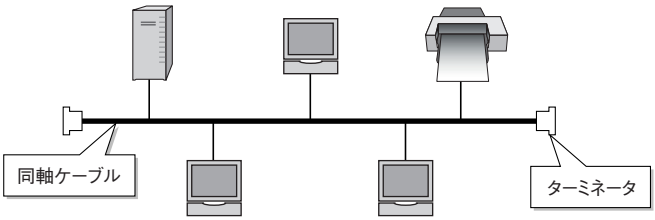
ネットワークには、物理トポロジと論理トポロジがあります。**物理トポロジ**とは、ノードとケーブル接続の物理的なレイアウトを指します。**論理トポロジ**とは、データの流れ方を表す論理的な構造を指します。代表的なトポロジには、バス型、スター型、リング型、フルメッシュ型の4つがあります。

■ バス型

バス型トポロジでは、軸となる1本のケーブルに一定の間隔でノードを接続します。

物理バストポロジでは、バスの端に**ターミネータ**（終端抵抗）が取り付けられます。ターミネータによってケーブルの端に到達した電気信号が反射して跳ね返り、ネットワーク内でエラーが発生するのを防ぎます。

【バス型トポロジ】



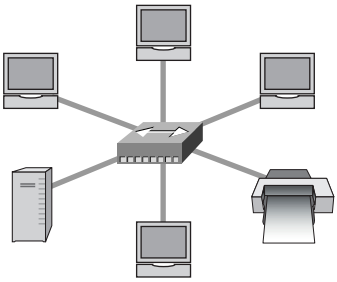
バス型では、すべてのノードが1本のケーブルを共有するため、ケーブルに1カ所でも障害が発生すると、すべてのノードがネットワークを利用することができなくなってしまいます。

※2　**【ネットワークデバイス】**ネットワークに直接接続して通信できるようにするための機器
※3　**【ノード】**node：ネットワークに接続されている端末やネットワークデバイスのこと。コンピュータもノードの1つ

■ スター型

スター型トポロジでは、1つのネットワークデバイスを中心にほかのノードを接続します。形状が自転車の車輪などに使われている「スポーク」に似ているため、**ハブアンドスポーク**とも呼ばれています。

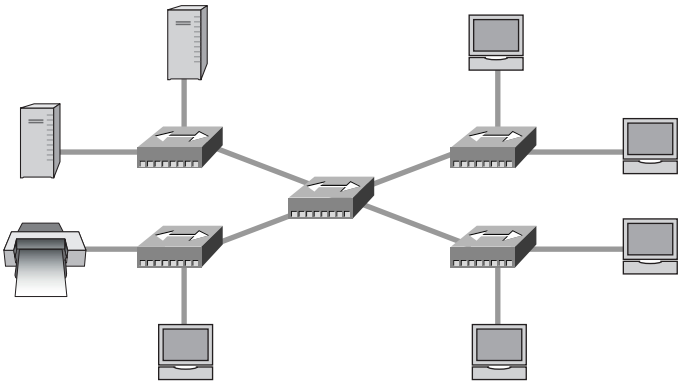
【スター型トポロジ】



スター型では、どこか1本のケーブルが切れてしまっても、影響を受けるのはそのケーブルを使用しているノードだけで、ほかのノードは影響を受けることなく通信し続けることができます。

なお、スター型を拡張して、中心のネットワークデバイスにさらに別のネットワークデバイスを接続したタイプを**拡張スター型**と呼びます。

【拡張スター型トポロジ】



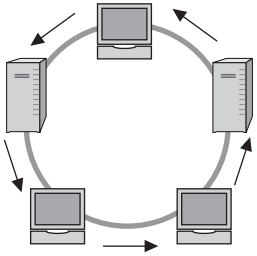
■ リング型

リング型トポロジでは、隣り合うノード同士をリング状に接続します。リング型には始まりも終わりもないため、バス型のようにターミネータが必要になることはありません。

リングには1つの**トークン**※4が一方向でリングをたどるように巡回しています。データはトークンに付加して転送され、各ノードを順番に巡回していきます。自分宛のデータを受け取ったノードは、トークンからデータを取り出します。したがって、リング型ではデータの衝突は発生しません。

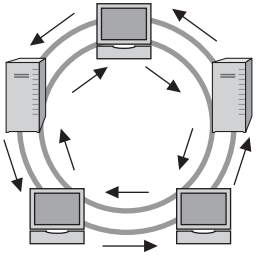
しかし、シングルリング型では、どこか1カ所のケーブルが切れたり、ケーブルに接続されたノードのうちの1つでも故障したりすると、そこで情報の流れが途絶えてしまいます。

【シングルリング型トポロジ】



この問題を回避するための構成がデュアルリング型トポロジです。デュアルリング型では、2つのリング上をデータが逆方向に送信されるため、一方のリングに障害が発生しても、もう一方のリングを使用して通信し続けることができます。

【デュアルリング型トポロジ】

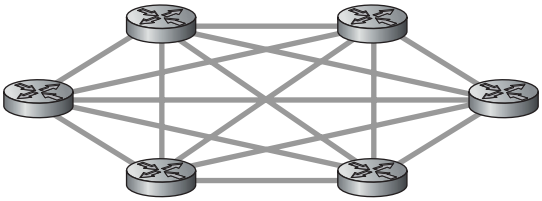


※4　**【トークン】**token：トークンパッシングと呼ばれるリング型LANのアクセス制御方式で使用される送信権のこと

■ フルメッシュ型

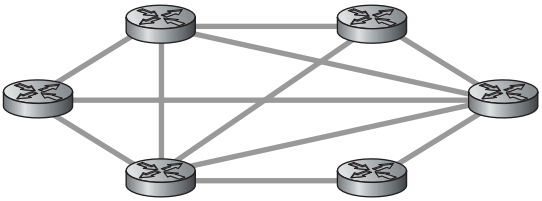
フルメッシュ型トポロジでは、すべてのノードを相互に接続し合います。そのため、特定のケーブルやノードに障害が発生しても、その部分を避けて通信し続けることが可能です。

【フルメッシュ型トポロジ】



フルメッシュ型は高い**冗長性**※5を持つため、最も**フォールトトレランス**※6が高いトポロジといえます。ただし、この方法はコストがかかるので一般的には実装が困難です。そこで、完全なメッシュではないけれども、どのノードもほかのノードとの間に複数の接続を持つ部分メッシュ型（パーシャルメッシュ型）が利用されることもあります。この方法では、重要なノード間を相互接続しながら代替ルートを持つため、冗長性も実現しています。

【パーシャルメッシュ型トポロジ】



※5　**【冗長性】**redundancy：設備的に余裕を持った構成のことで、故障が発生してもほかの設備でカバーできるようになっていること

※6　**【フォールトトレランス】**fault tolerance：システムに障害が発生したときに、正常な動作を保ち続ける能力。「耐障害性」とも訳される

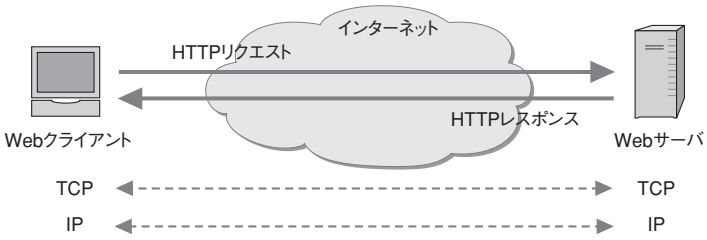
1-4 プロトコル

ノード間をケーブルなどで接続するだけでは、通信をすることはできません。人と人が会話をするために、日本語や英語といった特定のルールに則った同一の言語を使う必要があるように、コンピュータ同士が通信をする場合にも、あらかじめ決められたルールに従って処理がなされなければなりません。このルールである通信規約のことをプロトコルといいます。

■ プロトコルスタック

コンピュータの種類や通信の目的などによって、使用されるプロトコルはさまざまです。また通信は、非常に複雑な処理を必要とするため、複数のプロトコルが連携することによって実現されています。たとえば、インターネットに接続して、あるWebページをダウンロードするとき、WebブラウザとWebサーバの間では**HTTP**※7というプロトコルが使用されますが、HTTPは単独で機能しているのではなく、その下の階層では**TCP**※8と**IP**※9というプロトコルも使用されています（HTTPの動作については「2-9 HTTP」で説明しています）。このように、ある機能のために必要なプロトコルを階層上に積み重ねたプロトコル群を**プロトコルスタック**、あるいは**通信アーキテクチャ**と呼びます。

【プロトコルスタック】



※7　**【HTTP】**(エイチティーティーピー) HyperText Transfer Protocol：Webサーバとクライアント（Webブラウザ）がデータを送受信するのに使われるプロトコル

※8　**【TCP】**(ティーシーピー) Transmission Control Protocol：トランスポート層の信頼性のある通信を実現するプロトコル

※9　**【IP】**(アイピー) Internet Protocol：OSI参照モデルのネットワーク層の中心となるプロトコル。IPによってネットワーク層で使用されるアドレスや、データの形式を定義したりしている

1-5 OSI参照モデル

OSI（Open System Interconnection、開放型システム間相互接続）参照モデルは、国際標準化機構（ISO：International Organization for Standardization）によって定義された、通信機能を階層構造に分割したモデルです。このモデルに準拠することにより、異機種間の相互運用性が向上するなどのメリットがあります。

■ 階層化モデル

OSI参照モデルが考案される前のネットワークは、単一のベンダ※10が作った機器だけで構成され、独自の通信アーキテクチャを提供していました。そのため、異なるベンダのコンピュータ同士の通信が困難であるという問題点がありました。ネットワークが普及するにつれてマルチベンダネットワーク接続の要望が高まってきたため、ISOは「異なるベンダ間の相互通信」の検討を1970年後半から開始し、1984年にOSI参照モデルを発表しました。

OSI参照モデルでは、通信にかかわる一連の作業を7つの階層に分割しており、それぞれの層は**レイヤ**（Layer）と呼ばれます。

【OSI参照モデル】

第7層（レイヤ7）	アプリケーション層
第6層（レイヤ6）	プレゼンテーション層
第5層（レイヤ5）	セッション層
第4層（レイヤ4）	トランスポート層
第3層（レイヤ3）	ネットワーク層
第2層（レイヤ2）	データリンク層
第1層（レイヤ1）	物理層

OSI参照モデルのように通信機能を階層化することには、次のような利点があります。

・ベンダに依存することなく、相互運用性が実現される
・通信の複雑な処理を単純化できる
・標準インターフェイスを定義できる
・さまざまな種類のハードウェアとソフトウェアを組み合わせて相互に通信できる
・ある階層の機能を処理するソフトウェアを変更しても、ほかの階層に影響を与えずに済むため、更新や改善を効率的に行える

※10 **【ベンダ】**vendor：製品を販売する会社のこと。メーカーと呼ぶ場合もある。複数のベンダの製品を組み合わせて構築することを「マルチベンダ」という

・通信の機能をモジュール（部品）化することで、説明あるいは習得が簡略化できる

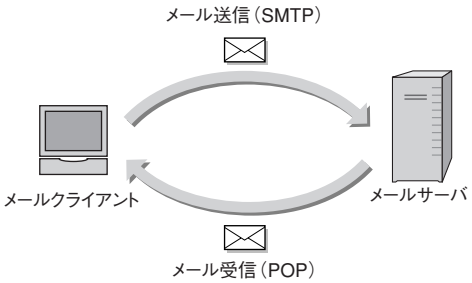
次に、OSI参照モデルの各階層の機能を説明します。

■ 第7層（レイヤ7）：アプリケーション層

アプリケーション層は、アプリケーション固有の通信サービスを実現するための機能を定義しています。そのため、電子メールやWebページの閲覧、ファイル転送などサービスの数だけアプリケーションプロトコルが存在します。

たとえば電子メールの場合、メールソフトでメッセージを作成して送信を開始すると、アプリケーションプロトコルがメールソフトからデータを受け取って、メールの送信手続きを行います。また、メールを受信するときは、自身のメールサーバからメッセージをダウンロードするプロセスを定義しているアプリケーションプロトコルを使用します。

【アプリケーション固有のサービスの実行】



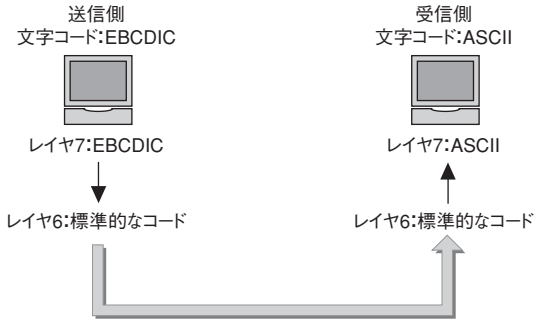
■ 第6層（レイヤ6）：プレゼンテーション層

プレゼンテーション層は、文字コードや圧縮方式などデータの表現形式を定義しています。

コンピュータやソフトウェアの種類によって、送信側と受信側で使用するデータの表現方法が異なることがあります。このような場合「文字化け」などが起こり、受信した情報を使えなくなることがあります。この問題を解決するために、プレゼンテーション層では共通の表現形式を定義し、通信するアプリケーション同士が理解できる形式にデータを変換します。

たとえば、異なる文字コード※11を持つアプリケーション同士で文字データをやり取りする場合の例として、送信者のアプリケーションがEBCDIC※12、受信者のアプリケーションがASCII※13を使用しているとしましょう。送信側でEBCDICのデータを送信する際には、上位層（アプリケーション層）から受け取ったデータをプレゼンテーション層で通信に適したコードにデータ形式を変換します。その後、下位層（セッション層～物理層）によって受信者へデータが運ばれます。受信側のプレゼンテーション層では、上位層へデータを渡す前にアプリケーションが要求するASCIIコードにデータ形式を変換します。

【データの表現形式の変換】



このように、データの表現形式をいったん標準的な形式（コード）に変換してから送り、受信側で必要な形式に変換することで、異なる形式を扱うアプリケーション間でも問題なく通信することが可能になります。

データ形式の変換対象となるのは文字だけではありません。以下に代表的なプレゼンテーション層の規格をまとめます。

・文字……ASCII、EBCDIC、Unicode、JIS
・画像……GIF、JPEG、TIFF
・動画……MPEG、AVI、MOV
・音声……MIDI、WAVE、PCM

なお、プレゼンテーション層ではデータの暗号化やデータの圧縮も定義しています。

■ 第5層（レイヤ5）：セッション層

セッション層は、アプリケーションプロセスを識別し、アプリケーション対アプリケーションのセッションを確立・維持・終了するための機能を定義しています。

多くの場合、1台のコンピュータでは複数のアプリケーションが同時に稼働しています。セッション層では、どのようにデータを送れば効率が良いか、送信方法はどうするかなどを互いに決めて、送信したデータが受信側コンピュータの正しいアプリケーションプロセスに届くようにデータの交通整理をします。

たとえば、あるユーザがWebブラウザとメールソフトを同時に使用した場合、Web

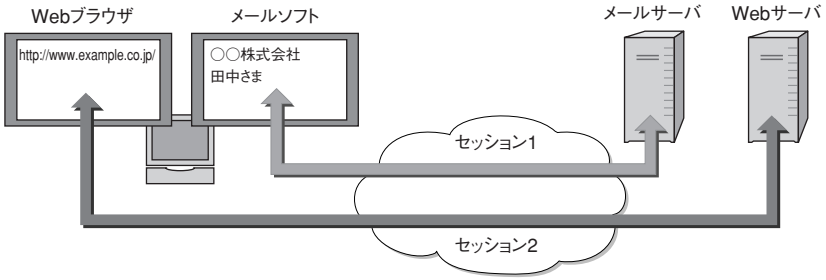
※11 **【文字コード】**character code：コンピュータで処理できるように、文字や記号に割り当てられた固有の数字のこと

※12 **【EBCDIC】**（エビシディック）Extended Binary Coded Decimal Interchange Code：IBMが策定した8ビットの文字コード規格。汎用コンピュータなどで利用されることが多い

※13 **【ASCII】**（アスキー）American Standard Code for Information Interchange：アメリカ規格協会（ANSI）が定めた情報交換用の文字コード規格。7ビットで表現され、128種類のローマ字、数字、記号、制御コードで構成される

サーバから送られてきたデータをメールソフトが受信したり、メールのメッセージをWebブラウザが受信したりすることがないように、コンピュータ内部で各アプリケーションの論理的な経路を用意します。この論理的な経路を**セッション**といいます。

【アプリケーション間のセッションを確立】



■ 第4層（レイヤ4）：トランスポート層

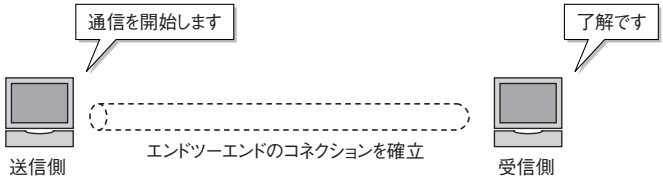
トランスポート層は、送受信を行うノード対ノードでの通信の信頼性を保証するための機能や、アプリケーション間でセッションを開始するために必要となるポート番号の割り当てを定義しています。

信頼性のある通信を実現するための機能には、コネクション（仮想回線）の確立・維持・終了や、通信障害の検出と回復、フロー制御、順序制御などがあります。ただし、このような制御を行うことによって転送効率が低下するため、すべてのアプリケーションで必須というわけではありません。トランスポート層では、アプリケーションに見合った品質の通信機能を提供します。

【信頼性を保証するための機能】

・コネクションの確立……相手が正常に通信できる状態であるか確認してから転送を開始する
・エラー制御……伝送エラーが検出された場合、データを再送する
・フロー制御　……ネットワークの混雑状態によって送信するデータ量を調整する
・順序制御　……データがバラバラに到着した場合、受信側で元の順番に再構成する

【エンドツーエンドの接続を確立】

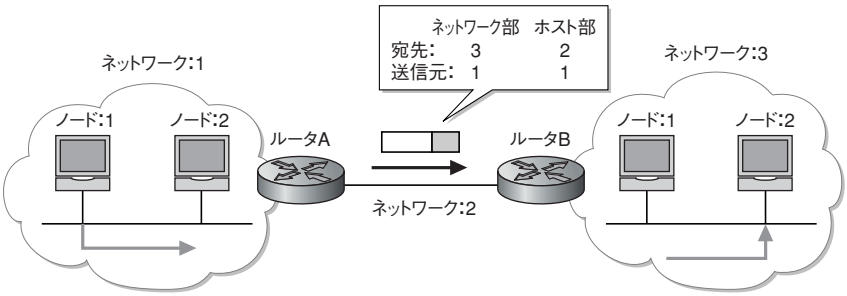


■ 第3層（レイヤ3）：ネットワーク層

ネットワーク層は、異なるネットワーク上にあるノード間の通信を実現するための機能を定義しています。通常、ネットワークを分割することができるのは**ルータ**※14であるため、ルータによって分断されたネットワーク間の通信を実現します。

ネットワーク層によって配信されるデータは、中継地点となるルータで最適パスを選択して転送されます。これを**ルーティング**といいます。ルーティングは、各ノードに割り当てられたソフトウェアアドレスに基づいて行われます。ソフトウェアアドレスはネットワーク管理者などが割り当てる論理アドレスで、ネットワークを識別する「ネットワーク部」と、ネットワーク上のノードを識別する「ホスト部（ノード部）」で構成されています。

【ネットワーク間の通信】



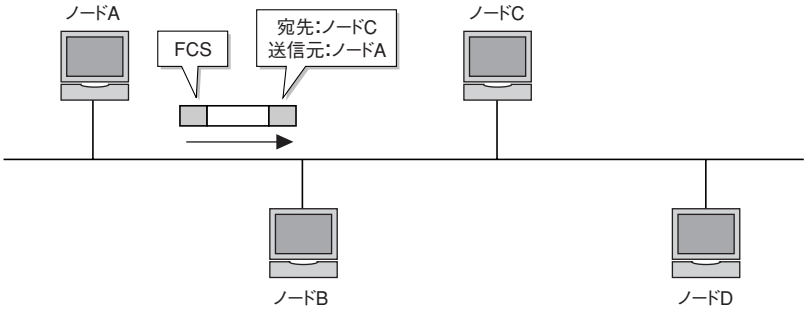
※14 **【ルータ】** Router：複数のネットワークを相互に接続するネットワークデバイス。ネットワーク層のデバイスで、離れたネットワークにデータを転送するためルーティング処理を行うほか、メディア変換やパケットフィルタリングなどの機能を持つ

■ 第2層（レイヤ2）：データリンク層

データリンク層は、1つの回線に接続されたノード間の通信を定義しています。ノードの識別には、物理アドレスとも呼ばれるハードウェアアドレスが使用されます。

データリンク層ではまた、データの後ろに**FCS**[※15]を付加して、受信した電気信号のエラー検出や訂正も行います。

【ノード間の通信】

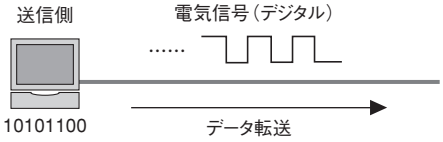


■ 第1層（レイヤ1）：物理層

物理層は、電気的および機械的な通信媒体について定義しています。その中には、ケーブルの種類やケーブルのコネクタの形状、電気信号の電圧などの仕様が含まれます。

また、コンピュータ内部で扱っている「0」と「1」のビット列を電気信号に変換してネットワーク上へ転送したり、受信した電気信号を「0」と「1」のビット列に変換してコンピュータ内に渡したりするのも物理層の役割です。

【電気信号をネットワークに送出】



※15 **【FCS】**(エフシーエス) Frame Check Sequence：データリンク層でカプセル化する際に、データの後ろに付加するエラー検出のための制御情報。FCS内にはCRCと呼ばれる整合性を確認するための値が入る

1-6 カプセル化と非カプセル化

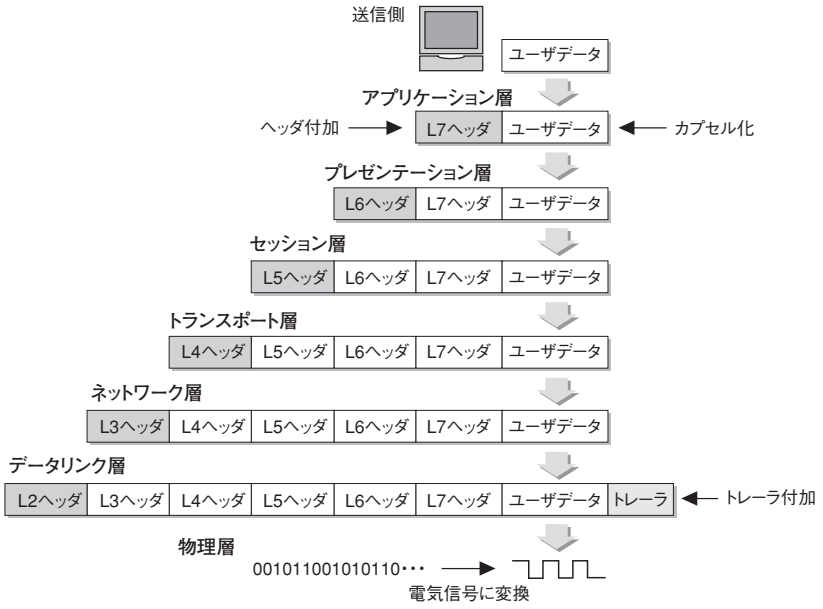
通信にはデータを送る送信者と、データを受け取る受信者がいます。送信側ではデータを送信するときにカプセル化という処理を行ってデータをパッケージ化する必要があります。一方、受信側では受け取ったデータを非カプセル化することで通信を実現しています。

■ カプセル化

送信側ノードでは、まずアプリケーション層で定義されている機能を処理し、その処理情報をデータの前に付加します。データの前に付加される情報を**ヘッダ**と呼び、この処理のことを**カプセル化**と呼びます。カプセル化が終わると、下位のプレゼンテーション層にデータを渡します。このときのデータにはヘッダと元のデータが含まれます。

プレゼンテーション層では、上位層から受け取ったデータからプレゼンテーション層の処理を行い、その情報をヘッダとしてデータの前に付加してカプセル化し、下位のセッション層にデータを渡します。このようにして、セッション層以下でも同じように定義されている機能の処理を行ってカプセル化し、下位の階層に渡していきます。ただし、データリンク層ではヘッダのほかに、受信したデータ全体をエラーチェックするための情報をデータの後ろに付加します。この情報を**トレーラ**と呼びます。最下位の物理層では、データリンク層から受け取ったデータ（ビット列）を電気信号に変換し、ネットワーク上に転送します。

【送信時のデータの処理】

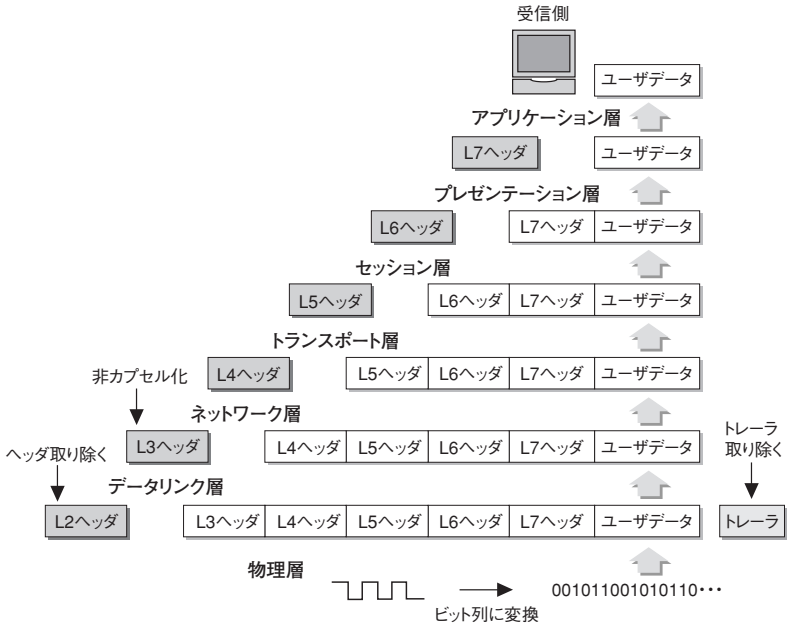


■ 非カプセル化

受信側ノードでは、送信とは逆の手順で処理します。まず物理層では、受信した電気信号をビット列に変換し上位層のデータリンク層へ渡します。データリンク層はトレーラをチェックして受信したデータにエラーがあるかどうかを確認します。エラーがある場合、データはその時点で破棄され、そのデータを再送信するよう要求します。データにエラーがない場合、データリンク層のヘッダ内の情報を確認します。データリンク層はヘッダとトレーラを取り外し、ヘッダ内で指定された情報に基づいてデータをネットワーク層に渡します。この処理を**非カプセル化**と呼びます。

以降の階層でも同様に非カプセル化の処理を行い、最後には指定されたアプリケーションに渡します。

【受信時のデータの処理】



1-7 ピアツーピア通信

送信側から受信側へ送られるデータは、OSI参照モデルの各層でカプセル化され、受信側では非カプセル化されます。これによって、同一の層では同一のヘッダ情報を使用して通信します。

■ピアツーピア通信

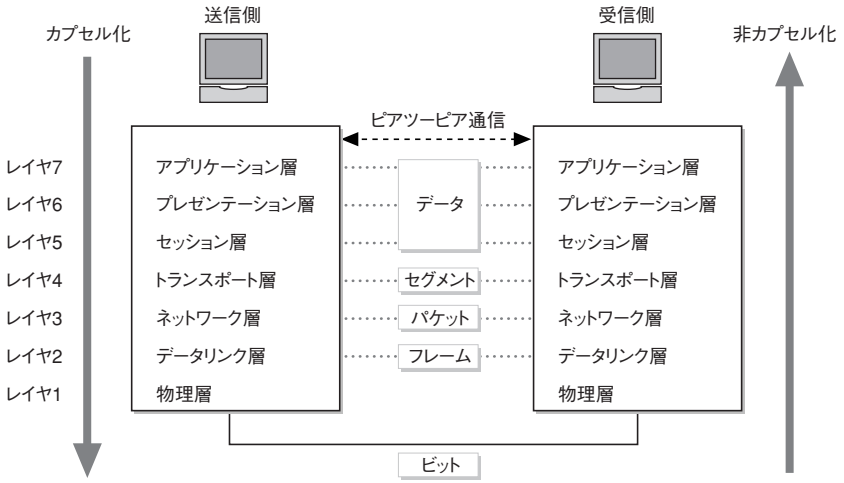
OSI参照モデルでは、送信側と受信側の同じ階層のプロトコル同士が情報交換しながらデータ通信を実現しています。階層ごとに同じ（同等の）プロトコルと通信するこの通信形態を**ピアツーピア通信**（peerは英語で「同等」の意）と呼びます。

■ プロトコルデータユニット

ピアツーピア通信では、ネットワークを介して送信されるヘッダ部分とデータによってカプセル化されたデータの単位を**プロトコルデータユニット**（PDU）と呼びます。また、トランスポート層で扱うPDUを**セグメント**、ネットワーク層で扱うPDUを**パケット**、データリンク層で扱うPDUを**フレーム**といいます。しかし、実際にはこれらの呼び方が厳密に区別されているとは限りません。たとえば、レイヤ2（データリンク層）のPDUがフレームと呼ばれることは多いものの、それ以上の階層のPDUを総じてパケットと呼ぶこともあります。

なお、パケットやフレームのデータ部分のことを**ペイロード**と呼ぶこともあります。

【ピアツーピア通信およびPDU】



1-8　2進数／10進数／16進数の変換

日常、私たちが使っている数値は10進数ですが、コンピュータで扱う数値には2進数が使用されています。しかし、大きな数値を2進数で表現すると桁数が多くなり、わかりにくくなります。そこで、コンピュータネットワークでは、2進数を10進数や16進数に変換して表現することが少なくありません。CCENTおよびCCNAの受験では、これらの変換方法を理解しておくことが非常に重要です。

【10進数、2進数、16進数の対応表】

10進数	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2進数	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111	10000
16進数	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10

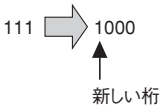
<以下省略>

■ 2進数

コンピュータでは、オンかオフの2つの状態が基本となるため**2進数**が使用されます。2進数では「0」と「1」の2つの数値が使用され、2進数における1つの桁はビット※16（bit）と呼ばれます。2進数を表現する場合、8桁（8ビット）単位で表現したり、計算したりすることが多くあります。

10進数では9の次の数値で位が上がりますが、2進数では1の次で位が上がります。

例）　2進数「111」の次の数値は、桁が1つ上がる
↓
新しい桁に1をたて、以下の桁をすべて0にリセット



● 2進数から10進数への変換

2進数の数値を10進数へ変換するには、次の8つの基準の数値を使用します。

【基準の数値】

128	64	32	16	8	4	2	1

これらの数値は、2進数で桁上がりするときの数値を10進数で表記し、上の桁から順に並べたものです。

※16【ビット】bit：コンピュータが扱う情報の最小単位。2進数の0と1で表現され、nビットで2のn乗の情報量を持つ

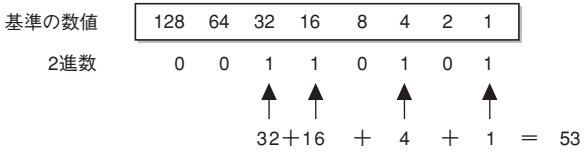
【10進数、2進数対応表】

10進数	0	1	2	3	4	5	6	7	8	9	…
2進数	0	1	10	11	100	101	110	111	1000	1001	…

10進数	15	16	…	31	32	…	64	…	128	…	255
2進数	1111	10000	…	11111	100000	…	1000000	…	10000000	…	11111111

※ 太字は位が上がる数、「…」は省略を表す

2進数の「1」になっているビットに対応する「基準の数値」を合計することで、2進数を10進数に変換することができます。たとえば、2進数「110101」の場合、次の図のように、32、16、4、1に対応するビットが1になるため、「32＋16＋4＋1」を求めます。



例）2進数　10100010の場合 ⇒ 128 ＋ 32 ＋ 2 ＝ 162
01011100の場合 ⇒ 64 ＋ 16 ＋ 8 ＋ 4 ＝ 92
11111111の場合 ⇒ 128 ＋ 64 ＋ 32 ＋ 16 ＋ 8 ＋ 4 ＋ 2 ＋ 1 ＝255

● 10進数から2進数への変換

10進数から2進数に変換するとき、10進数の数値が比較的小さい場合は、0になるまで繰り返し「基準の数値」をマイナス（減算）することで求めることができます。10進数の「44」を例にとって考えてみましょう。

まず、44以下の「基準の数値」の中で最大の値である32を44からマイナスします。

44－32＝12

次に、12以下の「基準の数値」の中で最大の値である8を12からマイナスします。

12－8＝4

さらに、4以下の「基準の数値」の中で最大の値である4を4からマイナスします。

4－4＝0

「基準の数値」のうち減算に用いた、32、8、4の桁を1、それ以外の桁を0にすると、2進数になります。

基準の数値	128	64	32	16	8	4	2	1
	0	0	1	0	1	1	0	0

つまり、「44」を2進数で表記すると「101100」になります。

通信における情報の単位には、**オクテット**※17が使われます。オクテットは8ビットなので2進数に変換した結果が8桁よりも小さい場合は、上位の桁に0を補って表記します。たとえば、「101100」の場合は6桁しかないので、上位2桁に0を補って「00101100」と記述します。

例）10進数　49の場合　⇒　49－32＝17、17－16＝1、1－1＝0 ……「00110001」

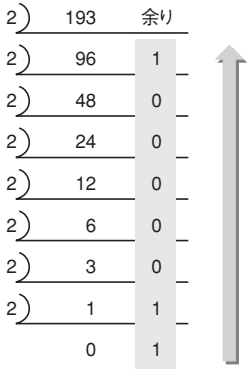
また、2進数に変換したい数が「基準の数値」の特定の数よりも1つ小さい数値の場合、その桁より下をすべて1にします。たとえば10進数「31」の場合、32よりも1つ小さい値なので、2進数表記にすると「00011111」になります。

例）10進数　127の場合　⇒　128よりも1つ小さい値であるため「01111111」

しかし、10進数の数値が大きい場合には、引き算を繰り返すのは煩雑になります。この場合、変換対象の10進数の数値を0になるまで順に2で割っていき、そのときの余りを並べて2進数を求めます。

たとえば、「193」を2進数に変換してみましょう。次の図のように、順次2で割り、余りを下から順番に並べていくと、2進数「11000001」になります。

※17 **【オクテット】**octet：情報量の単位。1オクテット＝8ビット（固定）。1バイト＝8ビットと確実に言えないことがあるため、「バイト」よりもビットの数が8つであることを強調したいときに使用する



■ 16進数

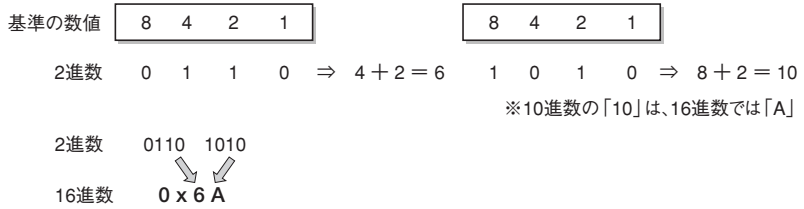
16進数は基数が16ですから、それを表現するには16個の数値が必要です。そこで、0～9までについては10進数と同じ数値を使用し、10進数の10～15にあたる数値にはA～Fのアルファベットを使います。したがって、Fの次の数値で桁上がりし「10」になります。また、10進数と区別するために、16進数の数値の先頭には「0x（ゼロエックス）」を付けて記述します。

例）10進数の「10」を16進数で表すと「0xA」

● 2進数から16進数への変換

2進数を16進数へ変換する場合、2進数を4桁の数値に区切って処理します。これは、16進数の1桁を2進数では4桁で表現するためです。

たとえば、2進数「01101010」を16進数へ変換する場合、「0110」と「1010」に分割して変換します。この場合、「基準の数値」として「8　4　2　1」を使用します。



例）2進数　00111100の場合、0011⇒3、1100⇒12（10進数）→ 0xC ……「0x3C」
2進数　10011110の場合、1001⇒9、1110⇒14（10進数）→ 0xE ……「0x9E」

● 16進数から2進数への変換

16進数から2進数に変換する場合、2進数から16進数への変換方法の逆になります。変換には、34ページの【10進数、2進数、16進数の対応表】を参照してください。

たとえば、0x7Bは「7」と「B」の2つに分けて変換します。

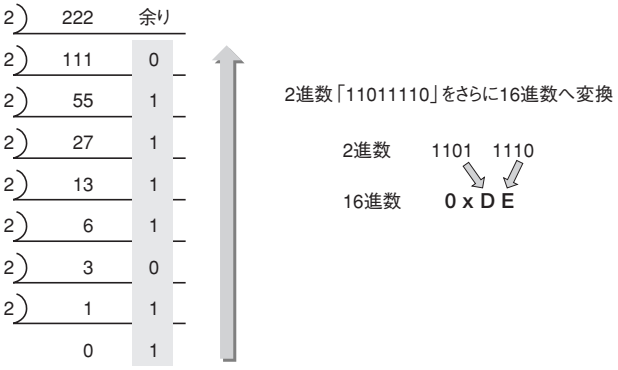
例）0x42の場合、4⇒0100、2⇒0010 ……「01000010」
　　0xF8の場合、F⇒1111、8⇒1000 ……「11111000」

● 10進数から16進数への変換

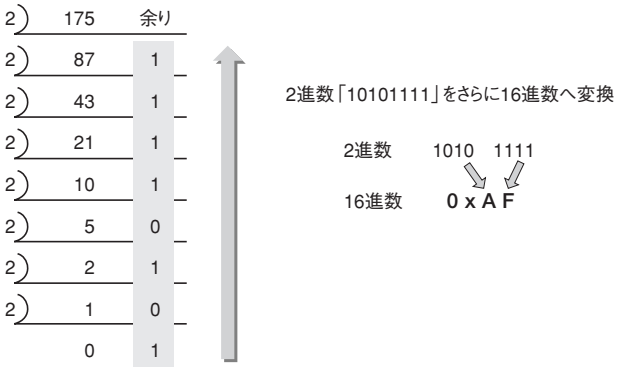
10進数から16進数へ変換する場合も、基本的な考え方はこれまでと同じです。ただし、10進数の数値が比較的大きい場合には「間に2進数を入れる」、つまり、いったん2進数へ変換してから16進数へ変換することで変換が容易になります。

たとえば、10進数222を16進数に変換するとしましょう。

まず、10進数222を2進数に変換します。下の図のように順次2で割っていくと、「11011110」であることがわかります。次に「11011110」を「1101」と「1110」に分割し、それぞれを16進数に変換します。最後に2つの16進数を合わせると、変換結果である「0xDE」が求められます。



例） 10進数「175」の場合

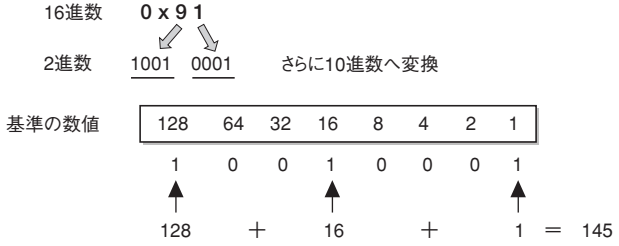


● 16進数から10進数への変換

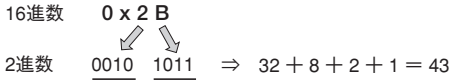
16進数から10進数へ変換する場合も、「間に2進数を入れる」方式で同じように変換します。

たとえば、16進数0x91を10進数に変換するとしましょう。

まず、「9」と「1」をそれぞれ2進数に変換します。その変換結果である「1001」「0001」を1つの2進数にし、「10010001」を10進数に変換します。



例） 16進数「0x2B」の場合



1-9 演習問題

1. OSI参照モデルの説明として誤っているものを選びなさい。

A. ネットワークの動作を単純な要素に分割することができる
B. 信頼性のある通信が実現する
C. インターネットワークの動作の理解に役立つ
D. 異なるベンダ間での相互運用を可能にする
E. アプリケーション開発者は、専門分野での設計・開発をすることができる

2. カプセル化されるときのプロトコルデータユニットの順番が正しいものを選びなさい。

A. データ → パケット → フレーム → セグメント → ビット
B. ビット → フレーム → パケット → セグメント → データ
C. データ → セグメント → パケット → フレーム → ビット
D. データ → セグメント → フレーム → パケット → セグメント
E. セグメント →フレーム → パケット → データ → ビット

3. 次の①～⑥の役割を担うOSI参照モデルの層を、選択肢から選びなさい。

① アプリケーション固有の通信サービスを実現する
② データの表現形式を定義
③ 電気的および機械的な通信媒体について定義
④ 送受信を行うノード間での信頼性を保証する
⑤ 異なるネットワーク上にあるノード間の通信を実現する
⑥ 1つの回線上に接続されたノード間の通信を定義

A. プレゼンテーション層
B. データリンク層
C. セッション層
D. コネクション層
E. メディアコントロール層
F. ネットワーク層
G. データフロー層
H. トランスポート層
I. アプリケーション層
J. 物理層

4. 2進数「11000110」を10進数と16進数に変換しなさい。

5. 次の10進数の数値をすべて2進数に変換しなさい。

① 48 ② 179 ③ 153 ④ 240 ⑤ 255

1-10 解答

1.　B

信頼性のある通信の実現（**B**）は、OSI参照モデルのトランスポート層が持つ機能であり、OSI参照モデルそのものの説明ではありません。
OSI参照モデルは複雑なデータ通信を7つの階層に分け、異なるベンダ同士が相互に通信できるようにする目的で設計されたものです。ネットワーク上でどのように通信が行われているかを説明したり、通信アーキテクチャの比較を行ったりするときに「ものさし」の役割をする重要な概念です。

2.　C

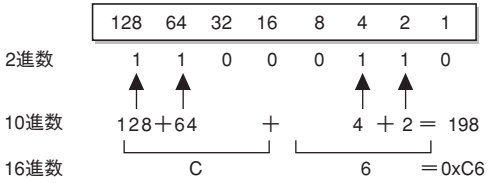
カプセル化の正しい順番は、「データ→セグメント→パケット→フレーム→ビット」です。詳細は「1-6 カプセル化と非カプセル化」、「1-7 ピアツーピア通信」を参照してください。

3.　① I、② A、③ J、④ H、⑤ F、⑥ B

OSI参照モデルの各層の特徴は「1-5 OSI参照モデル」を参照してください。

4.　10進数：198、16進数：0xC6

2進数から10進数への変換は、次の「基準の数値」を使用します。また、16進数への変換は32ページの対応表を使用します。



5.　① 00110000、② 10110011、③ 10011001、④ 11110000、⑤ 11111111

10進数から2進数への変換は、値が比較的小さい場合は「基準の数値」をマイナス（減算）することで求めます。①はこの方法で変換するといいでしょう。値が大きい場合は「0になるまで順に2で割り、そのときの余りを並べる」ことで求めます。②～④はこの方法が適しています。計算方法は35ページの「10進数から2進数への変換」を参照してください。
なお、⑤の「255」は基準の値をすべて加算した「11111111」になります。この値は計算しなくてもわかるように、覚えておきましょう。

第2章

TCP/IPプロトコル

2-1 TCP/IPプロトコルスタック
2-2 IP
2-3 ARP
2-4 ICMP
2-5 TCP
2-6 UDP
2-7 DHCP
2-8 DNS
2-9 HTTP
2-10 FTPとTFTP
2-11 SMTPとPOP
2-12 Telnet
2-13 SNMP
2-14 演習問題
2-15 解答

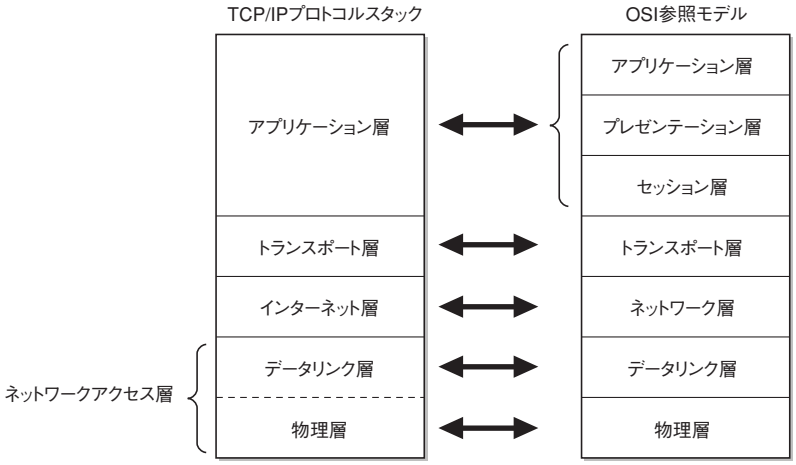
2-1 TCP/IPプロトコルスタック

TCP/IPはインターネットの標準プロトコルであり、全世界共通の通信プロトコルとして利用されています。TCP/IPプロトコルスタックとは、TCP（Transmission Control Protocol）とIP（Internet Protocol）の2つのプロトコルを中心とするプロトコルの集まりを指します。

■ TCP/IPプロトコルスタック

OSI参照モデルのようにTCP/IPも通信機能を階層構造に分割して構成していますが、TCP/IPの場合は4階層です。TCP/IPプロトコルスタックの各階層をOSI参照モデルのそれと対比すると、次のようになります。

【TCP/IPプロトコルスタックとOSI参照モデル】



■ TCP/IPアプリケーション層

TCP/IPのアプリケーション層は、OSI参照モデルのセッション層、プレゼンテーション層、およびアプリケーション層に対応しています。アプリケーション層のプロトコルは、ユーザが使用する特定のアプリケーションの機能を実現するためのサービスを提供します。たとえば、アプリケーションであるWebブラウザを使用してWebページを要求すると、アプリケーション層プロトコルであるHTTPが通信を実行します。

TCP/IPのアプリケーション層プロトコルには、次のようなものがあります。

・ファイル転送……FTP、TFTP
・電子メール……SMTP、POP
・リモートログイン……Telnet、SSH
・名前管理……DNS

・Web閲覧 ……HTTP
・ネットワーク管理……SNMP

■ TCP/IPトランスポート層

TCP/IPのトランスポート層は、OSI参照モデルのトランスポート層に対応しています。トランスポート層は、データを送受信する2つのノード間で稼働するアプリケーションプロセスに、直接通信サービスを提供しています。

TCP/IPのトランスポート層プロトコルには、TCPとUDPがあります。TCPについては「2-5 TCP」を、UDPについては「2-6 UDP」を参照してください。

■ インターネット層

インターネット層は、パケットの概要とアドレッシング方法などの定義によって、異なるネットワーク上にあるノード間の通信を実現しています。つまり、OSI参照モデルのネットワーク層に相当する層といえます。

インターネット層にはさまざまなプロトコルが存在しますが、最も中心的なプロトコルがIP（Internet Protocol）です。IPはネットワーク上のノードに論理アドレスを割り当てたり、パケットを複数のネットワーク間で相互通信するための最適経路を決定（ルーティング）したりするための機能を定義しています。現在、**IPv4**※1が主流ですが、アドレス空間の枯渇などが問題になっています。そこで、アドレス空間の増大、セキュリティ機能の追加などさまざまな改良を施した次世代のインターネットプロトコルである**IPv6**※2が開発され、一部ではすでに使用されています。

IPのほか、インターネット層の重要なプロトコルにARP（Address Resolution Protocol）とICMP（Internet Control Message Protocol）があります。

ARPは、IPアドレスからイーサネット※3の物理アドレス（**MACアドレス**※4）を要求するために使われるプロトコルです。

ICMPは、IPのエラー通知や通信状態の診断を行ったりするためのメッセージなどを転送するプロトコルです。

※1 **【IPv4】**(アイピーブイフォー、アイピーブイヨン) IP version4：1981年に公開され、現在インターネットで最もよく使用されているインターネットプロトコル。32ビットのIPアドレスを使用し、アドレスの枯渇が問題視されている

※2 **【IPv6】**(アイピーブイシックス、アイピーブイロク) IP version6：IPv4をベースにさまざまな改良を施した次世代インターネットプロトコル。128ビットのIPアドレスを使用するため、事実上、無制限のアドレス範囲を確保する

※3 **【イーサネット】** Ethernet：現在最もよく使用されているLANの規格。米国の企業、ゼロックスとDECが考案し、後にIEEE 802.3委員会によって標準化された。トポロジにはバス型とスター型の2種類があるが、現在はスター型が多く使用されている

※4 **【MACアドレス】**(マックアドレス) Media Access Control address：ネットワーク機器を識別するために、全世界で重複しないように割り当てられた48ビットのアドレス。16進数で「xx-xx-xx-xx-xx-xx」のように12桁で表記される。NICやルータなどのネットワーク機器にはMACアドレスが割り当てられている

■ ネットワークアクセス層（ネットワークインターフェイス層）

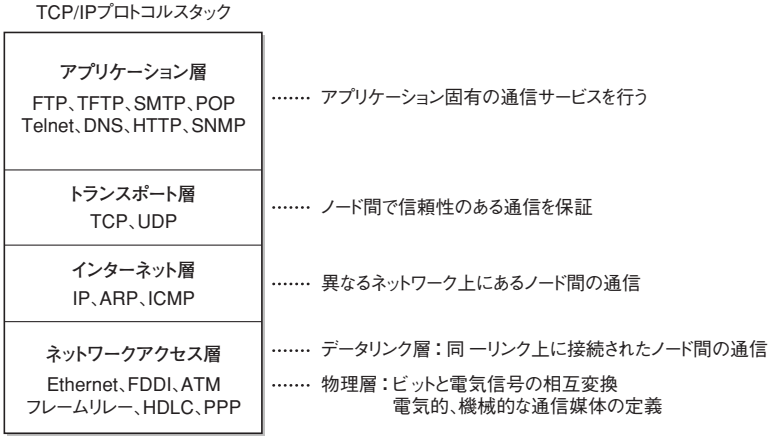
ネットワークアクセス層では、パケットがネットワーク上のメディア（媒体）にアクセスするために必要となるすべての機能を定義しています。この層に含まれるプロトコルは接続する物理ネットワークのタイプによって、次のようにさまざまなものがあります（イーサネット、トークンリング、FDDIについては第3章、HDLC、PPP、フレームリレー、ATMについては第12章でそれぞれ詳しく説明しています）。

・イーサネット
・トークンリング
・FDDI
・HDLC
・PPP
・フレームリレー
・ATM

ネットワークアクセス層で定義されている機能は、OSI参照モデルの物理層およびデータリンク層とほぼ同じであるため、TCP/IPプロトコルを5階層モデルで表現する場合もありますが、IETF※5ではTCP/IP発展のため意図的にOSI物理層とデータリンク層の2つに分割することを避けています。これによって、新しい物理ネットワークのサポートを容易にしています。

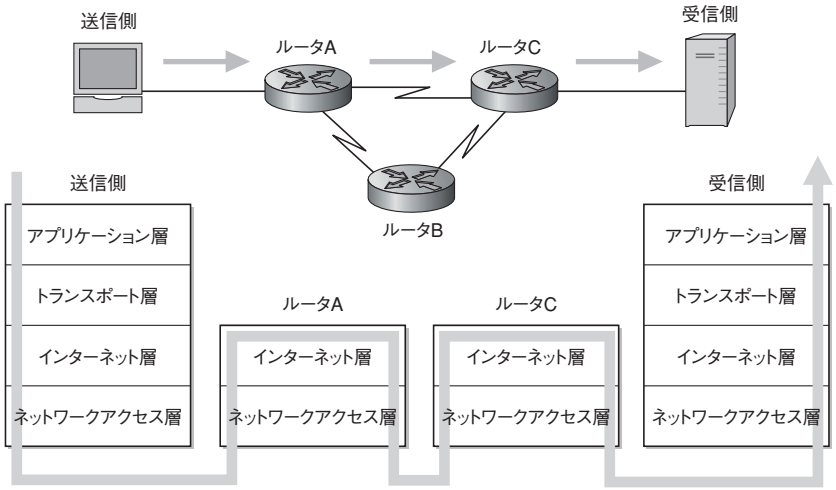
TCP/IPプロトコルスタックの各階層の役割と代表的なプロトコルは、次のとおりです。

【TCP/IPプロトコルスタックの各階層の役割とプロトコル】



TCP/IPプロトコルスタックにおいても、データは送信側でカプセル化され、受信側で非カプセル化されて宛先へと送信されます。データを受け取ったルータでは、最適経路を決定してデータを転送するために、インターネット層まで非カプセル化してヘッダ情報を確認し「次の行き先（ネクストホップ）」を決定すると、再びカプセル化処理を行ってデータを宛先まで転送します。

【パケットのカプセル化と非カプセル化の流れ】



※5 【IETF】(アイイーティーエフ) Internet Engineering Task Force：インターネット上で使われている各種プロトコルなどを標準化したRFCを発行する組織

2-2 IP

ここから3節にわたって、TCP/IPインターネット層のプロトコルについて、詳しく見ていくことにしましょう。最初に紹介するのは、インターネット層で最も中心的な役割を果たすIPです。なお、以下の説明では、特に明記しない限りIPはIPv4のことを指し、IPv6の場合はその都度記述することにします。

■ IPの特徴

IP（Internet Protocol）は、インターネット層で最も中心的な役割を果たすプロトコルです。IPには次のような特徴があります。

● コネクションレス型プロトコル

IPは通信の際に、送信者と受信者の間でコネクションを確立しないためコネクションレス型プロトコルといわれます。

● ベストエフォート型の配信

「パケット配送の保証はしないが最善の努力はする」という、ベストエフォートの通信タイプです。ただし、トランスポート層のTCPなど上位層で信頼性を高めることができます。

● データ回復機能なし

IPプロトコル自体には破棄されたパケットの再送信を要求するエラー回復機能はありません。この場合も、必要であれば上位層で回復します。

● 階層型アドレッシング

IPを含め、論理アドレスは2つの階層を持ちます。ネットワークを識別する「ネットワーク部」と、そのネットワークに接続されたノードを識別する「ホスト部」で構成されます（詳細は「6-1 IPアドレッシング」を参照）。

■ IPヘッダのフォーマット

インターネット層でカプセル化される際に、データの前に付加されるIPヘッダのフォーマットは次の図のとおりです。

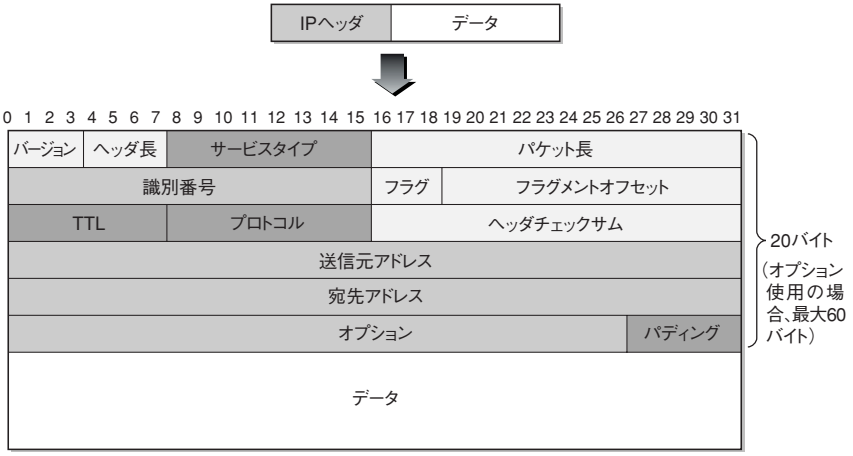
● バージョン（4ビット）

IPプロトコルのバージョン番号。現在は「4」です。

● ヘッダ長（4ビット）

IPヘッダの長さ。32ビット単位なので、32ビット×nの「n」が入ります。通常は「5」です。

【IPヘッダのフォーマット】



● **サービスタイプ（Type of Service：優先順位）（8ビット）**

パケットの優先順位を決め、サービス品質を高くすることができます。たとえば、データが集中したときに音声などの遅延の影響を受けやすいパケットを優先的に伝送するようにします（この処理をQoS※6と呼びます）。

● **パケット長（16ビット）**

ヘッダを含むIPパケット全体の長さ。オクテット（8ビット）単位なので、8ビット×nの「n」が入ります。

● **識別番号（16ビット）、フラグ（3ビット）、フラグメントオフセット（13ビット）**

識別番号は、個々のパケットを識別する情報。パケットを転送するルータがデータを分割したとき、識別番号には同じ値を付けます。これによって、宛先でバラバラになった複数のパケットを受信した場合でも、識別番号が同じであれば1つのデータであったと判断することができます。

フラグは、分割されたデータの分割状況を知らせるための情報。3ビットの情報で、先頭ビットは未使用です。真ん中のビットは、送信元でフラグメントを禁止する場合にビットに「1」を立てて指示します。最後のビットはフラグメント化された場合にのみ使用し、後続に分割されたデータがある場合には「1」を立てて通知し、最後のパケットには「0」を立てて、受信側に分割された最後のデータ部分であることを通知します。

※6 【QoS】(キューオーエス) Quality of Service：ネットワークにおける「サービス（通信）の品質」を制御する技術を指す。音声や動画などのリアルタイム性が要求される通信において、優先的に帯域を割り当てるなどの制御によって通信の品質を維持する

【フラグフィールドの意味】

ビット	意味	値
0	未使用	0
1	分割許可の有無	0（分割を許可する）
		1（分割を禁止する）
2	最後のフラグメント	0（最後のフラグメントである）
		1（途中のフラグメントである）

フラグメントオフセットは分割されたデータが、全体の何番目だったかを判断するために使用します。この値によって元のデータに再構成することができます。

以上3つの情報から、**フラグメント**を行うことができます。パケットが宛先へ転送されるとき、伝送路に一度に転送できるデータの最大値が決められています。この最大値を**MTU**（Maximum Transmission Unit）と呼びます。たとえば、イーサネットの場合、MTUは1,500バイト※7です。MTUサイズを超えるような大きなパケットを受け取った場合、データ部分を分割してパケットを作り直します。この処理がフラグメントです。

● **TTL（Time To Live）（8ビット）**

パケットの生存時間。ただし、時間で指定するのは難しいため、実際には秒数ではなく「パケットが経由することができるルータの数」でカウントされています。ルータは受け取ったパケットのTTL値を1ずつ減らし、パケットを送出するときTTL値が0になっていた場合、そのパケットを破棄します。これによってルータの持つルーティングテーブル※8に不具合があってもパケットが無限にネットワーク内をループしてしまうことを防ぐことができます。TTLは8ビットなので、0～255の値をセットして送信することができます。

● **プロトコル（8ビット）**

受信側で上位のプロトコルを識別するための番号。この番号はIANA*（現在はICANN*）によって管理されています。送信側はIPヘッダのプロトコルフィールド内に上位のプロトコル番号を書き込んで送出し、受信側のIPはこの番号を確認して上位プロトコルにデータを渡します。代表的なプロトコル番号は次のとおりです。

※7　【バイト】byte：情報の単位の1つ。1バイト＝8ビット。ただし、一部の汎用機では1バイト＝9ビットとして扱うなどの例外もある

※8　【ルーティングテーブル】Routing Table：主にルータが持つ経路情報のこと。ルータがパケットをルーティングする際に、この情報を参照する

【代表的なプロトコル番号】

番号	プロトコル名	番号	プロトコル名
1	ICMP	41	IPv6
6	TCP	88	EIGRP
17	UDP	89	OSPF

※その他の番号については、http://www.iana.org/assignments/protocol-numbersを参照

● ヘッダチェックサム（16ビット）

IPヘッダ部分にエラーがないかをチェックします（データ部分のチェックはTCPやUDP、アプリケーションに任せます）。

IPヘッダのチェックは、宛先の途中で経由するルータでも行います。ルータはTTL値を1つ減らすため、新しくなったヘッダを基にチェックサムを再計算した値を格納してパケットを転送します。

● 送信元アドレス（32ビット）

パケットを送信したノードに割り当てられているIPアドレス（詳細は、「6-1 IPアドレッシング」を参照）。

● 宛先アドレス（32ビット）

パケットの宛先を示すIPアドレス。宛先アドレスには、特定ノードだけを指定する**ユニキャストアドレス**※9、すべてのノードを対象にする**ブロードキャストアドレス**※10、あるいはグループのメンバーを対象にする**マルチキャストアドレス**※11のいずれかが入ります。

● オプション（可変長）

オプションとして次のような機能を付加することができます。通常はあまり使用されません。

・セキュリティ
・ルーズソースルーティング／ストリクトソースルーティング
・レコードルート
・インターネットタイムスタンプ

● パディング（可変長）

IPヘッダが32ビットの整数倍にならない場合、「0」を足して調整します。

※9 **【ユニキャストアドレス】**unicast address：特定のノードを表すアドレス
※10 **【ブロードキャストアドレス】**broadcast address：ネットワーク上のすべてのノードを対象にデータを送信する（ブロードキャスト）のに予約されている特別なアドレス
※11 **【マルチキャストアドレス】**multicast address：特定のグループを対象にして、データを送るときに使用するアドレス

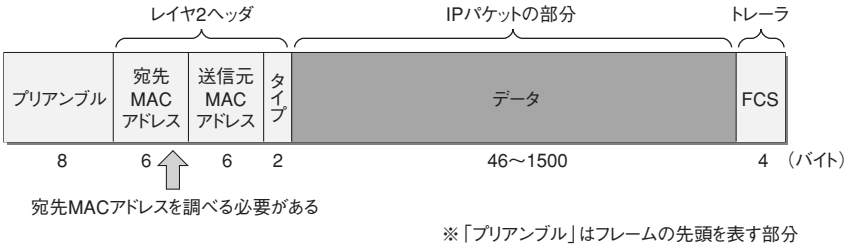
2-3 ARP

現在ほとんどのLANではイーサネットと呼ばれる規格が使用されています。イーサネットなどのLANに接続されたノード同士が通信する場合、IPパケットはイーサネットフレーム※12にカプセル化されて運ばれるため、お互いのMACアドレスが必要になります。この際にアドレス解決をしてくれるのがARPです。

■ ARPの概要

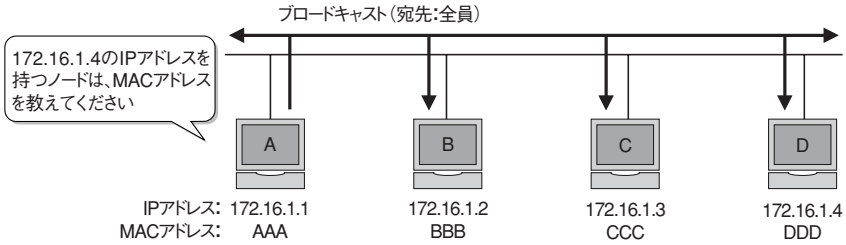
ARP（Address Resolution Protocol）は、IPアドレスを基にしてMACアドレスを取得するためのプロトコルです。ARPでは、ブロードキャストを利用して、同じネットワークに接続されているすべてのノードにMACアドレスを問い合わせます。

【一般的なイーサネットフレームのフォーマット】



次の図でホストAからホストDへ通信する場合を例に、ARPの動作を説明します。

【ARPの動作（ARPリクエスト）】



※12 **【イーサネットフレーム】**Ethernet frame：イーサネットにおいて、「パケット」の代わりに用いる語

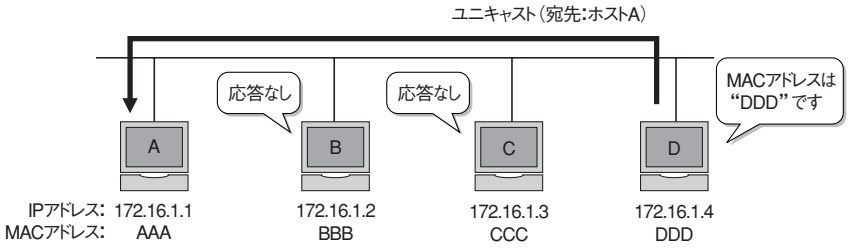
① ホストAは宛先のIPアドレスが自分の所属するネットワークと同じかどうかを調べます（異なるネットワークの場合、デフォルトゲートウェイ※13を指定していれば、そこにパケットを届けて中継してもらいます）。ここでは、宛先Dは同一ネットワークにあるものとして説明します。

② ホストAは自身のARPテーブルを検索します。**ARPテーブル**はARPキャッシュテーブルとも呼ばれ、アドレス解決をしてから一定の期間、キャッシュメモリ※14に保存されるMACアドレスとIPアドレスの対照表です。このテーブルを利用することによって、頻繁に同じ相手と通信する場合、その都度ARPでアドレス解決する（ブロードキャストされる）ことを防ぎます。ここでは、ARPテーブルにホストDのMACアドレスが存在しなかったとします。

③ ホストAはARPリクエスト（要求）パケットを送信します。ARPリクエストはブロードキャストで送信されるため、このときの宛先MACアドレスは「FF-FF-FF-FF-FF-FF」です。これによって、ネットワーク上の全員を対象に「IPアドレス172.16.1.4を持つノードは、MACアドレスを教えてください」とリクエストします（このとき通信相手に送るデータはバッファに保留されています）。

④ ホストDは要求されたIPアドレスが自身のIPアドレスと一致するため、ARPリプライ（応答）パケットを送信します。ARPリプライはユニキャストで送信されます。

【ARPの動作（ARPリプライ）】



⑤ ARPリクエストはブロードキャストであるため、ホストB、ホストCも受信しています。しかし、要求されたIPアドレスではないのでARPリプライは送信しません。

※13 **【デフォルトゲートウェイ】**default gateway：外部ネットワークに対して通信を行う際に、パケットの中継を依頼する代表（デフォルト）の「出入り口」となるノード。一般的にデフォルトゲートウェイにはルータを指定し、ルータによってパケットが中継される

※14 **【キャッシュメモリ】**cache memory：CPUの処理速度を低下させないように、メインメモリ（主記憶装置）にある情報を移動させて超高速な処理を可能にする高速小容量メモリのこと

⑥ ARPリプライによって、宛先のMACアドレスを入手したホストAは、データをイーサネットフレームに含めてLAN上に送信します。

■ ARPテーブルの表示

ARPによって取得したMACアドレスは、しばらくの間ARPテーブルに保存されます。ARPテーブルの情報を確認するには、Windowsコンピュータの場合、次の手順で行います。

①［スタート］メニュー→［すべてのプログラム］→［アクセサリ］→［コマンドプロンプト※15］を順にクリックしてコマンドプロンプトを起動します。

②「arp -a」と入力し Enter キーを押して実行すると、ARPキャッシュの内容が表示されます。

【コマンドプロンプトによるARPテーブルの表示例】

```
C:¥>arp -a

Interface: 192.168.11.4 --- 0x2    ← 使用しているノードの情報
  Internet Address ①    Physical Address ②    Type ③
  192.168.11.1          00.16.01.90.3d.62     dynamic   ← 保存されたARPエントリ
```

① Internet Address：IPアドレス
② Physical Address：MACアドレス
③ Type：アドレスの保存種別
・dynamic ……自動的に登録されたエントリ。一定時間使用されないと自動的に削除される
・static ……静的に登録されたエントリ。永続的に保存される
※現在、保存されている情報はホストDのMACアドレスとは関係ない

ARPテーブルにdynamicに登録されたエントリは、一定期間再利用されないとテーブルから削除されます。arp -aコマンド※16を実行して、「No ARP Entries Found」と表示された場合は、ARPテーブルにエントリが存在しないことを意味します。格納時間はOS*によって異なります。Windowsの場合は2分程度ですが、システムの実装によってこの時間には多少の差が生じます。

※15【コマンドプロンプト】command prompt：Windowsに付属しているコマンド（命令）を実行するための環境（シェル）
※16【コマンド】command：ユーザがキーボードなどで特定の文字列を入力してコンピュータに与える「命令」のこと

学習されているエントリをすぐに削除したい場合は、arp -dコマンドを実行します。

なお、CiscoルータおよびCatalystスイッチ※17でも同様にARPテーブルを表示することができます。その場合、show arp（あるいはshow ip arp）コマンドを実行します。

【Cisco IOS※18でのARPテーブル表示】

```
Router#show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.16.10.2           195   001f.c96b.71c0  ARPA   FastEthernet0/0
Internet  172.16.10.3             -   001f.6cef.d24c  ARPA   FastEthernet0/0
```

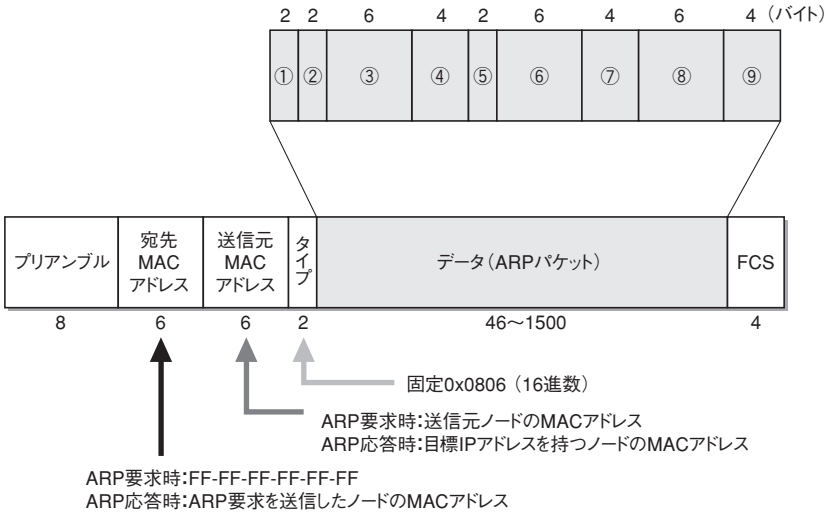
※17 【Catalystスイッチ】(カタリストスイッチ) Catalyst Switch：シスコ製スイッチ製品のシリーズ名。Catalystとは「触媒（ほかの物質の反応速度に影響するもの）」という意味

※18 【Cisco IOS】(シスコアイオーエス) Cisco Internet Operating System：シスコが提供するほとんどのルータおよびスイッチ製品で使用される基本ソフトウェアのこと

Memo　ARPパケットのフォーマット

ユーザがデータの送信を開始する際に宛先MACアドレスが不明であれば、ARPはアドレス解決のために自動的に動作します。ARPパケットのフォーマットは次のとおりです。

【ARPパケットのフォーマット】



① Hardware Type：ハードウェア種別。イーサネットの場合「0x0001（16進数）」
② Protocol Type：プロトコル種別。IPの場合「0x0800（16進数）」
③ Hardware Length：ハードウェアアドレス長で「6」
④ Protocol Length：プロトコルのアドレス長で「4」
⑤ Opcode：requestの場合「0x0001（16進数）」、replyの場合「0x0002（16進数）」
⑥ Sender MAC address：送信元MACアドレス
⑦ Sender IP address：送信元IPアドレス
⑧ Target MAC address：目標のMACアドレス。ARP要求時は「00-00-00-00-00-00」
⑨ Target IP address：目標のIPアドレス。このアドレスが自身と一致するとARPに応答する

2-4 ICMP

ICMPは、ネットワークに障害が発生したときのエラー通知や、ネットワーク状況の調査など、IP通信をサポートするためのさまざまな制御情報をやり取りする、IPにとってなくてはならない重要なプロトコルです。

■ ICMPの概要

ICMP（Internet Control Message Protocol）は、IP通信をサポートするインターネット層（ネットワーク層）のプロトコルです。

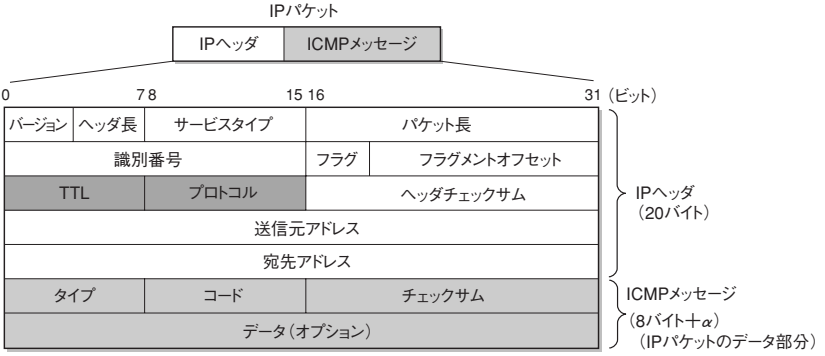
IPはコネクションレス型プロトコルであり、通信の途中で障害が発生したり、宛先となるノードが正しく受信できなくなったりしても、それを送信元に伝えることができません。そこで利用されるのが、ICMPの通知と問い合わせの機能です。

ICMPについてはRFC※19792で規定されており、文書中には「ICMPはIPの不可欠な要素であり、すべてのIPモジュールが実装していなければならない」と説明されています。このIPモジュールにはIPを実装するすべてのネットワーク機器が含まれるため、ICMPは当然ながらルータにも実装されています。

■ ICMPのフォーマット

ICMPの仕組みを理解することによって、IP通信時のトラブルの原因を突き止めることができるようになります。まず、ICMPでやり取りされるパケットのフォーマットを見てみることにします。

【ICMPのフォーマット】



※19 【RFC】（アールエフシー）Request for Comments：インターネットに関連する技術の標準を定める団体であるIETFが正式に発行する文書。RFCにより、インターネットで利用されるプロトコルやさまざまな技術の仕様および要件を公開している。各文書には識別するための通し番号が付けられている

ICMPの通知メッセージは、IPパケットのデータ部分に書き込まれています。このときのIPヘッダのプロトコルフィールドには「1」がセットされ、TTLはtracerouteコマンド（後述）で利用されます。

ICMPメッセージは、「タイプ（8ビット）」、「コード（8ビット）」、「チェックサム（16ビット）」および「データ（可変長）」の4つで構成されています。タイプでメッセージの概要を示し、コードによって詳細に分類しています。さらに、通知する必要がある情報はデータ部分に格納します。

RFCでは15種類以上のタイプが定義されています。よく使用されるタイプとコードの組み合わせは、次ページの表のとおりです。

ICMPメッセージには、大きく分けてエラー通知（Error）と問い合わせ（Query）の2種類があります。

エラー通知は、伝送経路に障害が発生したり、パケットが何らかの理由で転送途中に破棄されてしまったりした場合、エラーレポートを送信元に通知するメッセージです。エラー通知の例としては、タイプ3の「Destination Unreachable：宛先到達不能」がありますが、そのエラーの理由はさまざまです。たとえば、コード0は「宛先ネットワークに到達できない」、コード4は「パケットを分割する必要があるのに分割を禁止しているために、転送できなかった」ことをそれぞれ示しています。このように、タイプ3だけでも0～15のコードが用意されています。

一方、**問い合わせ**では、特定のノードに対して問い合わせを実行し、相手からの応答を受け取ることで「あるテーマに対するネットワークの診断」を行います。このICMPの問い合わせの仕組みを利用した代表的なコマンドがpingとtracerouteです。

■ ping

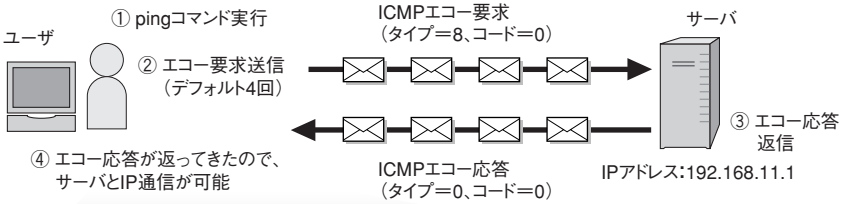
pingは、特定のノードとIP通信できるかどうかを確認するためのコマンドです。指定したノードにICMPメッセージのエコー要求を送り、エコー応答が返ってくるかどうかをチェックします。応答が返ってこなかったり、応答が届くまでに時間がかかり過ぎたりする場合、ネットワーク上に何らかの問題があると推測できます。

次に、Windowsのコマンドプロンプトを使って、pingコマンドの動作を説明します。

【代表的なICMPタイプとコードの組み合わせ一覧】

タイプ	コード	名前	意味	種類
0:Echo Reply（エコー応答）	0	Echo Reply Message	エコー応答	Query
3:Destination Unreachable（宛先到達不能）	0	Net Unreachable	宛先ネットワークに到達できない	Error
	1	Host Unreachable	宛先ホストに到達できない	
	2	Protocol Unreachable	プロトコルに到達できない（存在しない）	
	3	Port Unreachable	宛先ポートに到達できない	
	4	Fragmentation Needed and Don't Fragment was Set	パケットの分割が必要だが、分割禁止のフラグが立っているため破棄	
	5	Source Route Failed	ソースルーティングが失敗した	
	6	Destination Network Unknown	宛先ネットワークが不明である	
	7	Destination Host Unknown	宛先ホストが不明である	
	8	Source Host Isolated	送信元がインターネットにアクセスできない	
	9	Communication with Destination Network Administratively Prohibited	宛先ネットワークとの通信が管理的に禁止されている	
	10	Communication with Destination Host Administratively Prohibited	宛先ホストとの通信が管理的に禁止されている	
	11	Destination Network Unreachable for Type of Service	指定された優先制御の値では、宛先ネットワークに到達できない	
	12	Destination Host Unreachable for Type of Service	指定された優先制御の値では、宛先ホストに到達できない	
	13	Communication Administratively Prohibited	通信が管理的に禁止されている	
	14	Host Precedence Violation	ホストの優先度違反	
	15	Precedence Cutoff in Effect	優先制御が事実上切断された	
5:Redirect（経路変更）	0	Redirect Datagrams for the Network	指定されたネットワークへの最適経路変更を通知	Error
	1	Redirect Datagrams for the Host	指定されたホストへの最適経路を通知（ICMPリダイレクト）	
	2	Redirect Datagrams for the Type of Service and Network	優先制御時に指定されたネットワークへの最適経路を通知	
	3	Redirect Datagrams for the Type of Service and Host	優先制御時に指定されたホストへの最適経路を通知	
8:Echo Request（エコー要求）	0	Echo Request Message	エコー要求	Query
11:Time Exceeded（時間超過）	0	Time to Live exceeded in Transit	転送中にTTLの値が0になった（TTL超過）	Error
	1	Fragment Reassembly Time Exceeded	分割されたパケットの組み立て中に時間切れになった	

【コマンドプロンプトによるpingコマンドの実行例】




```
C:¥>ping 192.168.11.1 Enter  ←pingコマンド実行

Pinging 192.168.11.1 with 32 bytes of data:

Reply from 192.168.11.1: bytes=32 time<4ms TTL=64
Reply from 192.168.11.1: bytes=32 time<3ms TTL=64
Reply from 192.168.11.1: bytes=32 time<2ms TTL=64
Reply from 192.168.11.1: bytes=32 time<2ms TTL=64

Ping statistics for 192.168.11.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 4ms, Average = 2ms

C:¥>
```

pingの実行結果。エコー要求の結果、4回すべて応答が返ってきた状態

pingの実行結果をまとめた統計情報

① ユーザはネットワーク上のサーバと通信できるかどうかを確認するため、Windowsのコマンドプロンプトから、pingコマンドを入力し実行します。この場合、IPアドレスには「192.168.11.1」を指定しています。

構文 指定したIPアドレスとの接続を確認

ping ＜相手のIPアドレス＞

・ pingコマンドの宛先の指定には、IPアドレスのほかWindowsのコンピュータ名やドメイン名※20も利用できる

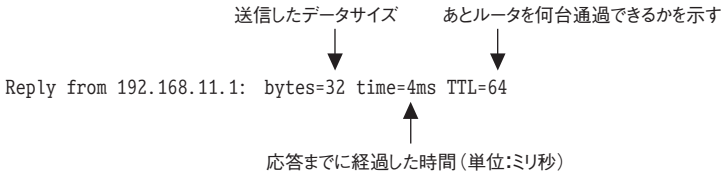
※20 **【ドメイン名】** domain name：インターネット上でIPアドレスの代わりに使用する、コンピュータを識別するための名前。Webサイトのアドレスや、電子メールのアドレスによく使用される。たとえば、「http://www.example.co.jp」の場合、「example.co.jp」部分がドメイン名である

② ユーザからサーバに向けて、ICMPのエコー要求メッセージが送信されます。Windowsの場合、デフォルト（標準状態）で4回のメッセージが送信されます（このときのICMPパケットは、タイプ8、コード0を使用）。

③ エコー要求を受け取ったサーバは、エコー応答メッセージを送信元に返信します（このときのICMPパケットは、タイプ0、コード0を使用）。

④ ユーザがエコー応答を受け取ると、コマンドプロンプトには「Reply from ～」で始まるメッセージが表示されます（この状態をping成功ということがあります）。これによって、ユーザは指定したサーバとIP通信ができることを確認します。なお、エコー要求メッセージには、「識別番号」と「シーケンス番号」という2つの情報が含まれます。受信したエコー応答の2つの値が同じかどうかチェックすることで、自身が送信したエコー要求に対する正しい応答であることを確認しています。

【pingコマンドが成功した場合の表示】



pingコマンドの実行結果の最後には、送受信したパケット数、往復にかかった最短時間や最長時間、平均時間などの統計情報が表示されます。

ただし、pingコマンドを実行しても、エコー応答が正常に返ってくるとは限りません。たとえば、時間内に応答が返ってこない場合は「Request timed out.」と表示されます。

タイムアウトには、次のような原因が考えられます。

・指定した相手が稼働していない
・指定したIPアドレスに誤りがある
・途中の経路に問題があるためエコー要求が相手に届いていない
・セキュリティの関係で、相手側でエコー要求の着信を許可していない

【エコー応答が返ってこないときの結果】

```
C:¥>ping 192.0.2.174    ←192.0.2.174へpingを実行

Pining 192.0.2.174 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.0.2.174:
    Packets: Sent = 4, Received = 0, Lost = 4(100% loss),
```

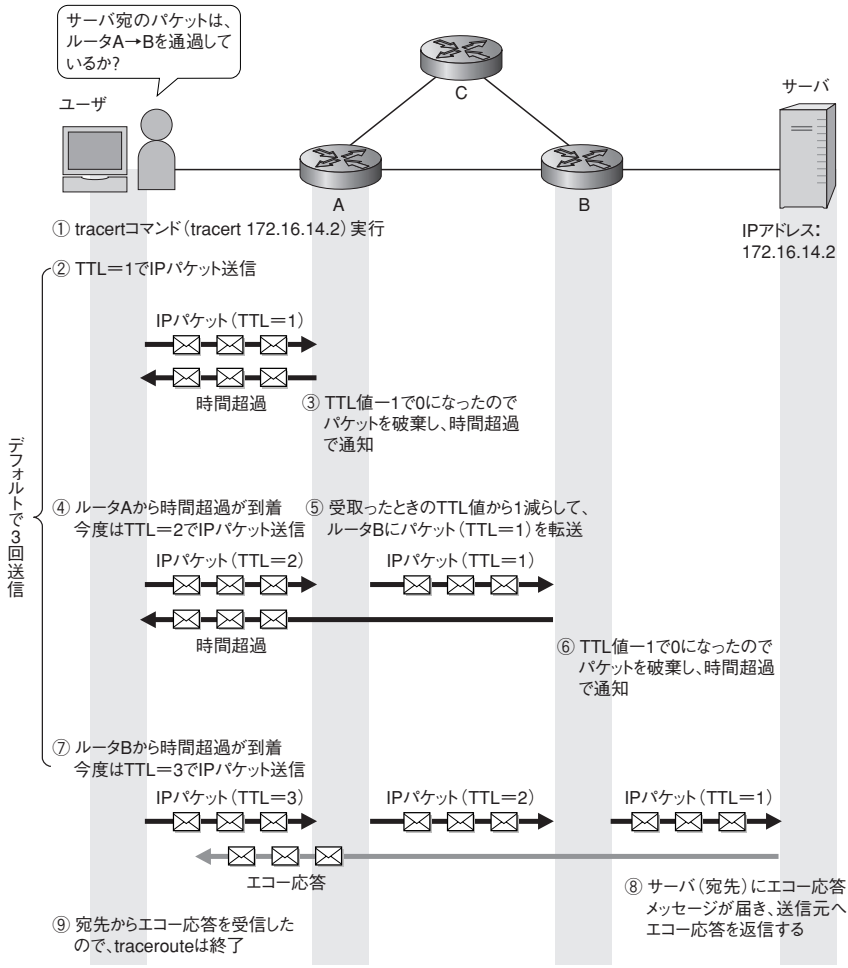
このほかにも、ICMPエコー応答が返ってこない理由はたくさんあり、pingが失敗したときの表示は「Request timed out.」以外にもいくつかあります。たとえば、「Reply from x.x.x.x: Destination net unreachable」と表示された場合、パケットが相手側の所属するネットワークに到達できなかったことを意味します。x.x.x.xの部分には、実際にエラーを返したルータのIPアドレスが入ります。この場合は、宛先までの途中にあるルータまではパケットが届き、そのルータがパケットを転送できなかったことがわかります。

■ traceroute

tracerouteは、宛先までの経路（通過するルータ）を調べるためのコマンドです。tracerouteでは、IPヘッダ内のTTL値を1にセットして指定したノードにICMPエコー要求メッセージを送ります。パケットを受け取った途中のルータによってTTL値が1ずつ減らされていき、値が0になったルータのところでパケットが破棄され、ICMP時間超過メッセージを使って送信元に通知します。tracerouteはこの仕組みを利用してTTL値を徐々に増やしていくことで、送信側から指定した宛先までの間に通過するルータがわかり、実際にデータが転送されるときの経路を確認することができます。

ここでは、Windowsのコマンドプロンプトを使って、tracerouteの動作を説明します。

【traceroute（tracertコマンド）の実行手順】



① ユーザはサーバと通信するときに使用する経路を調べるため、Windowsのコマンドプロンプトから、tracertコマンドを実行します。この場合は、IPアドレスに「172.16.14.2」を指定しています。

構文 宛先までの経路の確認

tracert ＜相手のIPアドレス＞

・Windowsでは、tracerouteを実行するコマンドはtracert
・tracerouteを強制終了するには、Ctrl＋C キーを押す

② ユーザからサーバに向けて、TTL値を1にセットしたIPパケットが送信されます。このとき、IPパケットのデータ部分にはICMPエコー要求メッセージが含まれます。

③ パケット（TTL＝1）を受け取った1台目のルータAは、TTL値を1減らして0になったためパケットを破棄し、ICMP時間超過メッセージ（タイプ11、コード0）で送信元に通知します。

④ 時間超過メッセージを受信したユーザのコマンドプロンプト上には、ルータAのIPアドレスと応答にかかった時間が表示されます。これにより、ユーザはパケットがルータAまで届いたことを知ります。次に、ユーザのコンピュータはTTL値を2にセットしたIPパケットを送信します。

⑤ パケット（TTL＝2）を受け取った1台目のルータAは、TTL値を1減らして次のルータ（ルータB）へパケット（TTL＝1）を転送します。

⑥ パケット（TTL＝1）を受け取った2台目のルータBは、TTL値を1減らして0になったためパケットを破棄し、ICMP時間超過メッセージ（タイプ11、コード0）で送信元に通知します。

⑦ 時間超過メッセージを受信したユーザのコマンドプロンプトの続きには、ルータBのIPアドレスと応答にかかった時間が表示されます。これにより、ユーザはパケットがルータBまで届いたことを知ります。さらにユーザのコンピュータは、TTL値を3にセットしたIPパケットを送信します。

⑧ 同じようにしてルータAとBを通過しサーバにパケット（ICMPエコー要求）が到着すると、サーバは送信者へエコー応答メッセージを返信します。

⑨ サーバからエコー応答メッセージが返ってきたので、tracerouteによるIPパケットの送信は終了します。ユーザのコマンドプロンプトの続きには、サーバのIPアドレスが表示されます。

ユーザが実行したtracertコマンドの結果は、次のようになります。

【コマンドプロンプトによるtracertコマンドの実行例】

```
C:¥>tracert 172.16.14.2    ←172.16.14.2へtracerouteを実行

Tracing route to 172.16.14.2 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1ms  172.16.1.254
  2    <1 ms    <1 ms    <1ms  172.16.2.101
  3    <1 ms    <1 ms    <1ms  172.16.14.2
  ①              ②               ③
Trace complete.
```

① 行番号：パケットが到着するまでに経由したルータの順番（ホップ数）。ただし、最終行は宛先の情報
② パケットが戻ってくるまでにかかった往復時間（単位：ミリ秒）。 Windowsでは3回計測する
③ 経由したルータのドメイン名またはIPアドレス

宛先までの途中の経路上にトラブルが発生している場合、途中から時間超過メッセージが送られてこなくなります。たとえば、「2 * * * Request timed out.」と表示された場合は、1台目と2台目のルータ間のリンクに障害があるか、2台目のルータに問題が発生していると考えられます。

このようにtracerouteを使用すると、パケットが適切な経路を通っているかを確認することができるため、ルータが適切に設定されているかどうかを調べることができます。また、トラブルが発生して通信ができない場合には、トラブルの原因がどのルータにあるかを突き止めたり、パケットの往復時間によってネットワークの混雑具合を調べたりするのにも役立ちます。

tracerouteを実行したときに送信されるパケットは、使用するOSやソフトウェアによって実装が若干異なる場合があります。たとえば、WindowsではICMPエコー要求を送信し、最終の宛先はエコー応答メッセージを返信しますが、Cisco IOSではUDP※21パケットを送信し、最終の宛先はICMP 宛先到達不能（Port Unreachable）の**メッセージ**※22を送信します（UDPの場合でも、IPヘッダ内のTTLを使用しているため、基本的な仕組みはWindowsの場合と同じです）。Ciscoルータにおけるpingとtracerouteコマンドの使用方法については、「5-4 Cisco IOSの接続診断ツール」を参照してください。

※21 **【UDP】**(ユーディーピー) User Datagram Protocol：TCP/IPプロトコルスタックのトランスポート層プロトコル。信頼性を保証するための制御を行わないので処理が軽く、高速転送が可能
※22 **【ICMP宛先到達不能メッセージ】**：ICMP宛先到達不能エラーを通知をするメッセージ。UDPヘッダ内の宛先ポート番号に、通常サーバ側で使用していない巨大なポート番号をセットすることによって送信される

2-5 TCP

ここからの2節では、TCP/IPトランスポート層のプロトコルであるTCPとUDPについて説明していきます。

まず、TCPとUDPのヘッダで指定されるポート番号について解説し、信頼性のある通信を実現するTCPから見てみることにしましょう。

■ ポート番号

ポート番号とは、1台のコンピュータの中で動作しているアプリケーションを識別するための番号です。

IPネットワーク上に接続されたホストは、IPアドレスによってお互いを認識して通信しますが、それだけでは正しいアプリケーションプロセスを識別することができません。つまり、宛先のコンピュータにデータを届けるまでがIPの役割で、その先のアプリケーションにデータを届けるのがポート番号の役割です。

ポート番号を利用することで、ユーザは1台のコンピュータで同時に複数のアプリケーションを使って通信をすることができます。たとえば「ブラウザを使ってWebページの閲覧をしながら、電子メールでメールの送受信をする」といった、マルチタスクを実現します。

ポート番号は16ビットで表現し、0～65,535の範囲になります。具体的にはトランスポート層プロトコルであるTCPおよびUDPのヘッダに含まれます。

ポート番号は、次の3つに分類されます。

【ポート番号の分類】

ポート番号の範囲	タイプ	説明
0～1,023	ウェルノウン	インターネットに不可欠なアプリケーションに割り当てられる番号で、IANAが管理
1,024～49,151	登録済み	IANAに登録された独自アプリケーションの番号。 例）Lotus Mailなど
49,152～65,535	ダイナミック	アプリケーションプロセスの要求に応じて自動的に割り当てられる番号

※ IANAでは、ユーザ側で使用するポート番号には49,152以上を推奨しているが、実際にはほとんどのケースで1,024以上をダイナミックポート番号として使用している

ポート番号の0～1,023は、ネットワーク上で一般的に使用されるサーバアプリケーションに割り当てられています。この範囲の番号を**ウェルノウンポート**（well-known port）といい、IANAによって管理されています。well-knownとは「既知の」「よく知られた」という意味です。

たとえば、Webサーバにアクセスして Webページを要求する場合、ユーザ側では80番（HTTP）を宛先ポートとしてアクセスします。Webサーバ側では80番のポートを開いて

接続を待ちます。同様に、メールサーバは25番のポートを開いて待ちます。このように、アプリケーションごとにあらかじめポート番号が決められているため、クライアントはこの番号を宛先に指定することで、特定のアプリケーションに簡単にアクセスすることができます。

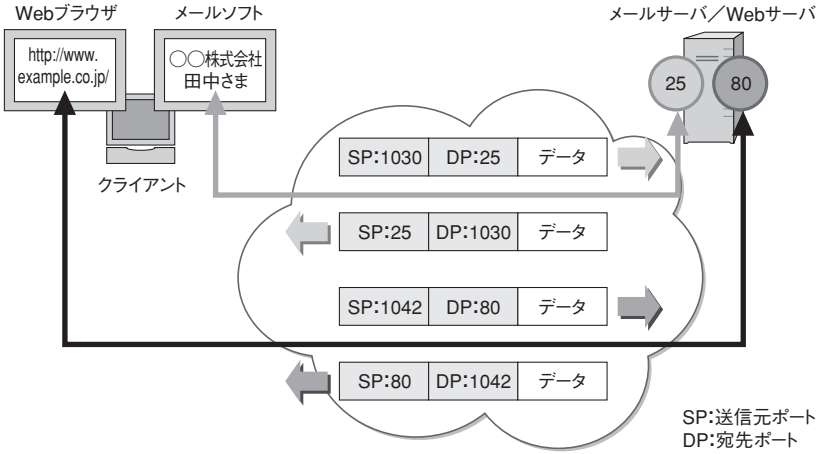
一方、サーバからのデータを適切なアプリケーションプロセスで受け取るためには、ユーザ側にもポート番号が必要になります。ユーザ側で使用するポート番号は、通常アプリケーションが重複しないようにランダムに割り当てられます。また、1つのアプリケーションを複数起動した場合にはそれぞれを識別するために異なるポート番号が割り当てられます。この仕組みにより、ユーザが複数のブラウザを使用していても、それぞれに目的のWebページが表示されるというわけです。

Memo 代表的なウェルノウンポート

代表的なウェルノウンポートには、次の表のようなものがあります。
IANAでは、ほとんどのプロトコルにTCPとUDPで共通のポートを予約していますが、一般にアプリケーションで使用されているのは、以下のとおりです。TCPとUDPの種別を確認しておきましょう。

ポート	プロトコル	TCP/UDP
20	FTP-DATA	TCP
21	FTP	TCP
22	SSH	TCP
23	TELNET	TCP
25	SMTP	TCP
53	DNS	UDP、TCP
67	DHCP（Bootstrap Protocol Server）	UDP
68	DHCP（Bootstrap Protocol Client）	UDP
69	TFTP	UDP
80	HTTP	TCP
110	POP3	TCP
123	NTP	UDP
161	SNMP	UDP
162	SNMP（TRAPS）	UDP
443	HTTPS	TCP
520	RIP	UDP

【ウェルノウンポートによるアプリケーションの指定】



■ TCPセグメントのフォーマット

TCP（Transmission Control Protocol）は、信頼性のある通信を実現するための、TCP/IPトランスポート層のコネクション型プロトコルです。「信頼性のある」とは、データの抜け、重複、誤りなどがなく、送信元から送られたデータが正しく宛先に届く通信を指しています。そのためTCPにはいくつかの制御機能が定義されています。

TCPの制御機能の説明の前に、ここではTCPセグメント※23のヘッダの内容について触れておきます。

● 送信元ポート番号（16ビット）

送信元のポート番号です。

● 宛先ポート番号（16ビット）

宛先のポート番号です。

● シーケンス番号（32ビット）

データの順序を示す番号です。受信側で到着したデータの順序制御に使用します。

● 確認応答番号（32ビット）

データを受信したことを通知し、次に受信したいデータのシーケンス番号を通知します。

※23 【TCPセグメント】(ティーシーピー・セグメント) TCP segment：トランスポート層のTCPで扱う分割されたTCPパケットのこと