情報科学2

2019年　神戸大学　担当　片山　修

目次

[ネットワーク 1](#_Toc26387517)

[通信プロトコル 1](#_Toc26387518)

[プロトコルとは 1](#_Toc26387519)

[ネットワークインターフェイス層 2](#_Toc26387520)

[インターネット層 2](#_Toc26387521)

[トランスポート層 2](#_Toc26387522)

[アプリケーション層 3](#_Toc26387523)

[Ethernetプロトコル 4](#_Toc26387524)

[イーサネットの規格 4](#_Toc26387525)

[MACアドレス 4](#_Toc26387526)

[自分のMACアドレス 5](#_Toc26387527)

[インターネットプロトコル（IP） 5](#_Toc26387528)

[IPv4ヘッダのフォーマット 5](#_Toc26387529)

[IPアドレスの管理 7](#_Toc26387530)

[IPアドレスの表現 7](#_Toc26387531)

[IPアドレスのクラスと種類 8](#_Toc26387532)

[サブネットマスク 9](#_Toc26387533)

[TCPとUDP 10](#_Toc26387534)

[TCPヘッダのフォーマット 11](#_Toc26387535)

[ポート番号 12](#_Toc26387536)

[TCPでの送受信 12](#_Toc26387537)

# ネットワーク

複数のコンピュータを線（ケーブル）で接続して相互に通信できるようにしたものをネットワークと呼びます。ネットワークを構成する機器には、スイッチ、ルータやハブなどがあります。

また、接続の形態によって、バス型、リング型、スター型といった型があります。

コンピュータ同士の通信では、送り手と受け手を識別するために、MACアドレスやIPアドレスといった固有の番号を利用して、情報のやり取りを行っています。

ハブ

バス型

リング型

スター型

# 通信プロトコル

## プロトコルとは

機器同士が通信を行うときに使用する取り決めのことです。コンピュータ同士の単なる通信であっても途中にさまざまな機器やケーブルを介して通信を行います。また、扱われるソフトウェアによってやり取りするデータも異なります。ですので、データのやり取りの手順は、いくつかの階層に分けられて、それぞれにプロトコル（手続き）が存在しています。これにより、プロトコルの変更が生じた場合に、全プロトコルを変更する必要は無く、該当のプロトコルのみを変更するという単純化が図られています。データのやり取りの手順の階層構造として「OSI参照モデル」と「TCP/IP」が挙げられます。表１のようにOSI参照モデルは7層に分けられていますが細かすぎるため、インターネットで標準的に使用される「TCP/IP」では4層に分けられています。

以下では、TCP/IPのそれぞれの層について説明します。

表１：OSI参照モデルとTCP/IPモデルの対応

|  |  |  |  |
| --- | --- | --- | --- |
|  | **OSI参照モデル** | **TCP/IPモデル** | **プロトコル** |
| 上位層 | 第７層　アプリケーション層 | アプリケーション層 | SMTP、POP3、HTTP、FTP、TELNET、SNMP、DNS、DHCP、NTP |
| 第６層　プレゼンテーション層 |
| 第５層　セッション層 |
| 下位層 | 第４層　トランスポート層 | トランスポート層 | TCP、UDP |
| 第３層　ネットワーク層 | インターネット層 | IP、ICMP |
| 第２層　データリンク層 | ネットワークインターフェイス層 | Ethernet、PPP、PPPoE、ARP、RARP、FDDI、ISDN |
| 第１層　物理層 |

### ネットワークインターフェイス層

ネットワークインターフェイス層は、OSI参照モデルのデータリンク層と物理層に相当します。ネットワークインターフェイス層に規定されているプロトコルのEthernetでは同一ネットワーク内の個々の機器を物理アドレスである**MAC**（Media Access Control）アドレスで識別して通信を行っています。通信に使われるデータは、フレームと呼ばれます。さらに、物理的なケーブルやコネクタの形状についても規格が定められています。

### インターネット層

インターネット層は、OSI参照モデルのネットワーク層に相当し、ネットワーク上でデータをやり取りする相手との通信に関するルールを規定しています。この層で使われるIP（Internet Protocol）は、TCP/IPプロトコル群の基盤となるプロトコルです。ネットワーク上のすべての機器に固有のIPアドレスを付けることで、通信のための相手先までの経路を決定するができます。上位層から渡されたセグメントに宛先、送信元のIPアドレス情報を付加してパケットを生成します。

### トランスポート層

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相当します。この層ではTCP（Transmission Control Protocol）とUDP（User Datagram Protocol）の２つのプロトコルが規定されています。これらのプロトコルは、ネットワーク通信におけるデータのやり取りの開始から終了まで制御を行っています。

データ通信は、複数のアプリケーションでやり取りされるデータが衝突しないように**ポート番号**を利用した通信の仮想的な通路を作成して行われます。ここで生成されるデータは、アプリケーション層からのデータにポート番号などが付加されてセグメントと呼ばれます。

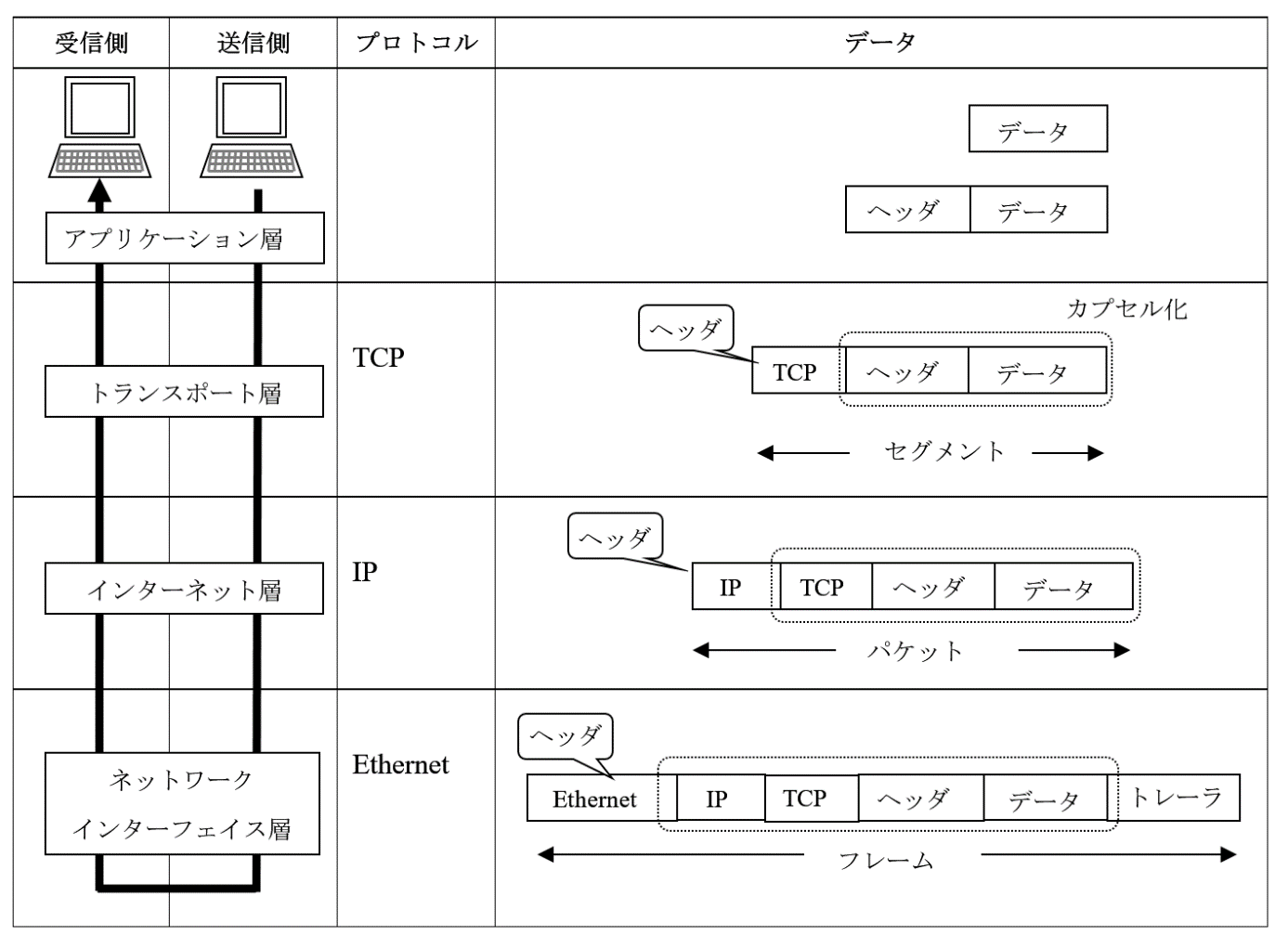
UDPは、データの送信が正しく行われたかのチェックを行いませんが、TCPは正しく送信されたことを確認しながら通信を行うという違いがあります。

### アプリケーション層

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、アプリケーション層に相当します。ユーザが作成したデータを直接取り扱い、データ形式（文字コード、圧縮方式）を整え、通信目的に応じたデータの送受信の管理を行います。

TCP/IPモデルのアプリケーション層に規定されているプロトコルには、Webサービスでのハイパーテキストを転送するHTTP（Hyper Text Transfer Protocol）、メールサービスを提供するSMTP（Simple Mail Transfer Protocol）、POP3（Post Office Protocol）、IMAP4（Internet Message Access Protocol）などがあります。Webブラウザやメールソフトには様々な製品がありますが、これらのプロトコルを実装することによって同じサービスが提供されることになります。

通信プロトコルとデータ



## Ethernetプロトコル

ネットワークインターフェイス層で利用されるプロトコルのイーサネット(Ethernet)ついて説明します。これは、現在最も普及しているネットワークの国際標準規格で、通信に使用するケーブルとその上を流れる信号の両方を定義しています。

### イーサネットの規格

イーサネットは、IEEE（Institute of Electrical and Electronics Engineers）の802プロジェクトでCSMA/CD方式のネットワークの国際的な標準規格として規定されました。最初は転送速度が10Mbit/s(Mbps)で同軸ケーブル（黄色のケーブルが多かったため、イエロー・ケーブルなどと呼ばれていた）を用いた10BASE5と呼ばれる規格でしたが、現在は8本の銅線を2本ずつ撚り合わせたツイストペアケーブルが主に用いられています。

|  |  |  |
| --- | --- | --- |
| ツイストペアイーサネットケーブルの規格 | | |
| **カテゴリ** | **規格** | **伝送速度** |
| Catgory3 | 10BASE-T | 10Mbps |
| Catgory5 | 100BASE-TX | 100Mbps |
| Catgory5e | 1000BASE-T | 1000Mbps |
| Catgory6 | 1000BASE-TX | 1000Mbps |
| Catgory6a | 10GBASE-T | 10Gbps |
| Catgory7 | 10GBASE-T | 10Gbps |

### MACアドレス

Ethernetプロトコルが作成するフレームに付けられるヘッダには同じネットワーク内で直接に通信する相手を特定するためのMACアドレスという識別子情報が含まれています。MACアドレスは、LANカードなど個々のハードウェアに一意に値が割り当てられていて、製品にハード的に書き込まれています。

MACアドレスは、48ビット（EUI-48）で定義されています。8ビット(=1バイト)ずつにコロンまたはハイフンで分けられてそれぞれの8ビットは16進数で表現され、「12:34:56:78:90:AB」や「1F-E2-3D-C4-5B-A6」などと表記されます。前半の24ビットがOUI(Organizationally Unique Identifier)と呼ばれるIEEEが割り当てているハードウェアのメーカーの番号、残りの24ビットが製品固有の番号になります。ヘッダは、宛先のMACアドレスの6バイトと送信元のMACアドレスの6バイトと２バイトのタイプで構成されます。タイプは上位層でデータの処理に使用されるプロトコルの種類を表す16進数の番号が入ります。

タイプ

（2バイト）

送信元MACアドレス

（6バイト）

宛先MACアドレス

（6バイト）

イーサネット（Ethernet）ヘッダの構成

Ethernetでは、同一のネットワーク上の機器とデータのやり取りを行います。たとえば、サーバからネットワーク機器を通して他のネットワークのパソコンにデータを送る場合、

①サーバのイーサネットで作られるヘッダには、宛先として直接やり取りをする同一ネットワーク上の機器のMACアドレスが指定されてフレームが作成される。

②データを受け取った機器は、次にデータを送る機器のMACアドレスを宛先としてフレームを作成する。

このようにデータが経由した機器ごとに宛先のMACアドレスを指定されていきます。また、データはネットワーク全体に流れていきますが、最終的には宛先のMACアドレスを持ったパソコンだけがデータを受け取ることになります。

### 自分のMACアドレス

自分が使っているパソコンのマックアドレスを調べてみよう。

Windowsの場合  
「コマンドプロンプト」を起動し、コマンド「ipconfig /all」を実行する。物理アドレスの項を見る。あるいは、「getmac/v」を実行する。

Macの場合

「ターミナル」を起動し、コマンド「ifconfig」を実行する。etherの項を見る。

## インターネットプロトコル（IP）

IP（Internet Protocol）はインターネット層で利用されるプロトコルで、コンピュータや機器を特定するためにIPアドレスという識別子を使用します。

上位のトランスポート層で作成されたセグメントにネットワーク上での送信元のIPアドレスと最終的な宛先となる機器のIPアドレスをヘッダとして付けてパケットが作成されます。インターネット層では、この宛先のIPアドレスを元にパケットの送信を行いますが、伝送エラー発生時には再送信を行いません。

現在は、IPはバージョン4（IPv4）が主に利用されています。IPv4でのIPアドレスは32ビットで構成され約43億個が利用可能です。しかし、インターネットの普及によってIPアドレスの枯渇が問題となってきており、現在、IPアドレスを128ビットで構成するIPv6の利用が始まりつつあります。

### IPv4ヘッダのフォーマット

IPパケットを受け取ったコンピュータは、IPヘッダを見て、自分のIPアドレス宛かどうかを判断し、自分宛でなければ他の機器に再送します。自分宛であれば、IPパケットからデータを取り出して、上位のTCPなどのプロトコルに渡されます。



データ部分には、セグメントが入っています。

|  |  |
| --- | --- |
| フィールド | 説明 |
| **バージョン(4 bit)** | IPヘッダのバージョン。IPv4では「4」となる |
| **ヘッダ長(4 bit)** | IPヘッダの長さで4byteが単位となります。オプションとパディングがない場合は、20byteなので、5(=0101)となります。  これで、どこからデータが始まるのかが分かります。 |
| **サービスタイプ(8 bit)** | IPパケットの優先順位の情報。ほとんど使用されない。 |
| **全長(16 bit)** | IPヘッダを含むパケットの全長。 |
| **識別番号(16 bit)** | パケットを識別するための番号。IPパケットをいくつかに分割して送信する場合に、受け取った側で同じ識別を判断して元のIPパケットに再構成する。 |
| **フラグ(3 bit)** | 3bitの内使われるのは、MF(More Fragment)bitとDF(Don’t Fragment)です。  MF:1つのIPパケットを複数に分割した場合、最後のパケットでは「1」にし、それ以外のパケットでは「0」にします。  DF:「1」になっているとIPパケットを分割してはいけないことになり、「0」では分割してよいことになります。 |
| **フラグメントオフセット(13 bit)** | 分割していないパケットや分割した先頭のパケットでは「0」となります。分割した後続では、元のデータに戻すときの位置を示します。分割は8byte単位で行われるので、100がセットされている場合は、再構成では800byte目からこのデータが入るということが分かります。 |
| **生存時間:TTL(8 bit)** | パケットが転送されるたびに１ずつ減らされます。TTL=0になるとパケットは破棄されます。これによりルーティングループが発生してもネットワーク上にパケットが残らない様になっています。 |
| **プロトコル(8 bit)** | 上位のトランスポート層のプロトコルが何であるかを示す。 |
| **ヘッダチェックサム**  **(16 bit)** | IPヘッダに破損がないかを確認する項目。（通信機器の高性能化で行わなくてもよくなっている。）  計算方法：（送信側も受信側も同じ計算をし一致するとOK）   1. ヘッダチェックサム16bitをすべて0とする。 2. IPヘッダを16bitに分けてすべて加算 3. 総計の下位16bitの1の補数を取る |
| **送信元IPアドレス**  **(32 bit)** | 送信元のIPアドレス |
| **宛先IPアドレス(32 bit)** | 宛先のIPアドレス |
| **オプション(可変長)** | 通常は使用されない。 |
| **パディング(可変長)** | オプションと合わせて32bitになるように調整する。 |

### IPアドレスの管理

IPアドレスは、MACアドレスと同様に、重複することなく割り当てられなければなりません。そのため、IPアドレスはIANA（Internet Assigned Numbers Authority）により管理されていて、世界の地域ごとに設置されたIR（Internet Registry）と呼ばれる組織によって、階層的に管理・分配が行われています。日本では、APNICの管轄下にあるJPNICがIPアドレスを管理しています。IPアドレスには、直接インターネットに接続する機器のために申請して割り当てられるグローバルIPアドレスと届け出無しで組織内において自由に使用することができるプライベートIPアドレスの2種類が有ります。

### IPアドレスの表現

IPv4では、IPアドレスは32ビットの2進数で構成されます。これを人に分かりやすいように8ビットのオクテットに分割します。各オクテットを10進数に変換し「．」（ピリオド）で接続して表記するのが一般的です。たとえば「192.168.240.10」は次のように変換されています。

11000000101010001111000000001010

IPアドレス（32ビット）

IPアドレス（32ビット）をオクテット（8ビット）に分ける

11000000 10101000 11110000 00001010

各オクテット（8ビット）を10進数に変換する

192 . 168 . 240 . 10

第1オクテット

第2オクテット

第3オクテット

第4オクテット

### IPアドレスのクラスと種類

IPアドレスの32ビットを２つに分けて「ネットワーク部」と「ホスト部」と呼びます。何ビットで分けるかによってネットワーク部を大きくしたり、ホスト部を大きくしたりすることができます。ネットワーク部分の大きさでA、B、C、D、Eの５つのクラスに分けられています。なお、近年ではクラスよりもCIDR(Classless Inter-Domain Routing)によるネットワーク部の指定が一般的になっています。

IPアドレスのクラスと範囲

|  |  |  |
| --- | --- | --- |
| **クラス** | **説明** | **IPアドレスの範囲** |
| クラスA | 第1オクテットがネットワーク部に割り当てられ、IPアドレスの上位１ビットが「0」で始まる．第1オクテットは「0～127」（000000～01111111）をとり、ホスト部は第2オクテットから第4オクテットとなる．1つのネットワークに約1677万（≒256×256×256）のIPアドレスを割り当てることができる． | 0.0.0.0から127.255.255.255  プライベートアドレス  10.0.0.0から10.255.255.255 |
| クラスB | 第1オクテットから第2オクテットまでがネットワーク部に割り当てられる．IPアドレスの上位2ビットは「10」で始まる．第1オクテットは「128～191」、第2オクテットは「0～255」をとり、ホスト部は第3オクテットから第4オクテットとなる．1つのネットワークに約65000（≒256×256）のIPアドレスを割り当てることができる． | 128.0.0.0から191.255.255.255  プライベートアドレス  172.16.0.0から172.31.255.255 |
| クラスC | 第1オクテットから3オクテットまでがネットワーク部に割り当てられる．IPアドレスの上位3ビットは「110」で始まる．第1オクテットは「192～223」、第2、3オクテットは「0～255」をとり、ホスト部は第4オクテットのみとなる．1つのネットワークに254(第4オクテットに0と255となるIPアドレスを利用しないため-2)のIPアドレスを割り当てることができる． | 192.0.0.0から223.255.255.255  プライベートアドレス  192.168.0.0から192.168.255.255 |
| クラスD | IPアドレスの上位4ビットが「1110」で始まる．ネットワーク内の複数の機器に一斉にデータ通信を行うマルチキャスト通信のために使われ、一般には割り当てられない． | 224.0.0.0から239.255.255.255 |
| クラスE | IPアドレスの上位4ビットが「1111」で始まる．  研究・実験用として使われ、一般には割り当てられない． | 240.0.0.0から255.255.255.255 |

### サブネットマスク

IPアドレスのネットワーク部とホスト部を区別するのがサブネットマスク（ネットマスク）です。サブネットマスクは、ネットワーク部分を2進数「１」で、ホスト部を2進数「0」で表します。クラスBでは第3と第4オクテットが「0」、およびクラスCでは第4オクテットが「0」なので、

クラスB:「11111111111111110000000000000000」

クラスC:「11111111111111111111111100000000」

と表されます。これをオクテットごとの10進数で表現すると「255.255.0.0」（クラスB）、「255.255.255.0」（クラスC）となります。

### CIDRについて

たとえば、192.168.0.0から始まるIPアドレスを利用するネットワークにおいて、サブネットマスクの違いによって利用できるIPアドレスの範囲は、次のようになります。

|  |  |  |  |
| --- | --- | --- | --- |
| サブネットマスク | CIDR表記 | IPアドレスの範囲 | IPアドレス数 |
| 255.255.255.255 | 192.168.0.0/32 | 192.168.0.0 | 1 |
| 255.255.255.128 | 192.168.0.0/25 | 192.168.0.0～192.168.0.127 | 128 |
| 255.255.255.0 | 192.168.0.0/24 | 192.168.0.0～192.168.0.255 | 256(Cクラス) |
| 255.255.254.0 | 192.168.0.0/23 | 192.168.0.0～192.168.1.255 | 512 |
| 255.255.252.0  第3オクテット111111002=252 | 192.168.0.0/22 | 192.168.0.0～192.168.3.255 | 1024 |
| 255.255.0.0 | 192.168.0.0/16 | 192.168.0.0～192.168.255.255 | 65536(Bクラス) |
| 255.0.0.0 | 192.0.0.0/8 | 192.0.0.0～192.255.255.255 | 16777216(Aクラス) |

IPアドレスが300個必要な組織の場合、CクラスのIPアドレスを2つ用意する必要はなく192.168.0.0/23のネットワークを１つ用意するだけで済みます。また、クラス分類でしかIPアドレスを設定できない場合に、512個だけのIPアドレスが必要であってもBクラスのネットワークを構築しなければならず、65000個余りのIPアドレスが無駄になってしまいます。

## TCPとUDP

TCPは、相手側にデータを確実に届けるために、エラーチェックをし、エラー発生時にはデータの再送を行う役割を負います。また、扱われているデータがどのアプリケーションソフトのためのデータかを判断し、正確に届けるという役割も持っています。TCPはコネクション型のプロトコルと呼ばれています。通信路はソケットという仕組みを使用し、アプリケーションソフトごとに作られます。通信路をコネクションと呼び、通信路を区別するためにポート番号という識別子が使用されます。TCPで扱われるデータは、セグメントと呼ばれます。セグメントはデータにTCPヘッダを付けて作成されます。TCPヘッダは、送信元ポート番号と宛先ポート番号やシーケンス番号やコードビット、応答確認番号などで構成されているいて、このセグメントのことをパケット（TCPパケット）と呼びます。

UDPは、TCPと違って通信路の確保や受信確認をしないコネクションレス型のプロトコルです。受信確認を行わないため信頼性は低くなるが、高速なデータ送信が可能となっています。UDPで作られるパケットのUDPヘッダの構成は、「送信元ポート番号（2byte）+宛先ポート番号（2byte）+UDPデータサイズ（2byte）+チェックサム（2byte）」です。チェックサムは、UDPパケットの情報に誤りが含まれていないかを確認するために使われます。TCPヘッダと比べるとヘッダ部分が小さくなっていてデータを多く送れるようになっています。

UDPが使用される場面は、

1. コネクションを貼る必要がないので複数の相手にメッセージを送る（同報通信）  
   利用：DHCPなど
2. 高速に効率よくデータを送る  
   利用：動画や音声などのマルチメディアデータの送信
3. 扱われるデータ量が小さく信頼性が不要である．  
   利用：ドメイン名からIPアドレスを調べるDNS(Domain Name System)や時刻同期であるNTP(Network Time Protocol)

といったところです。

### TCPヘッダのフォーマット

TCP(Transmission Control Protocol)は、インターネットにおいて標準的に使用されているプロトコルで、受け渡しするデータに次の表に示される情報をヘッダとして付加します。



|  |  |  |
| --- | --- | --- |
| フィールド | | 説明 |
| **送信元ポート(16 bit)** | | 送信元のアプリケーションソフトが使用しているポート |
| **宛先ポート(16 bit)** | | 宛先のアプリケーションソフトが使用しているポート |
| **シーケンス番号(32 bit)** | | データを分割したときに付けられる順番を表す番号 |
| **確認応答番号(32 bit)** | | 受信したデータのサイズとシーケンス番号から作られ，  受信側から送信元へ応答が帰るときに付けられる |
| **ヘッダ長(4bit)** | | TCPヘッダの長さであり，セグメントのデータが始まる位置を表す |
| **予約済み(6 bit)** | | 将来の利用向けて用意されている |
| **コードビット (各1 bit) 初期値は「0」 説明はすべて「1」のとき** | **URG** | 緊急に処理されるべきデータが含まれている |
| **ACK** | 確認応答番号が有効，すなわち受信側がパケットからデータを取り出せたことを意味する |
| **PSH** | 受信したデータをすぐにアプリケーションソフトへ送る |
| **RST** | コネクションを強制的に切断する |
| **SYN** | コネクションの接続を要求している |
| **FIN** | コネクションの切断を要求している |
| **ウィンドウサイズ**  **(16 bit)** | | 受信側が受信可能なデータサイズを送信側に伝える |
| **チェックサム(16bit)** | | 通信中のパケットの整合性をチェックするための検査データが入る |
| **緊急ポインタ(16bit)** | | URGが「1」のときのみ有効で，緊急データの場所を表す |
| **オプション(32 bit)** | | 送信側が受信側に送る特別な設定を指定する情報  MSS ( Maximum Segment Size )で受信可能な最大セグメント・サイズを相手に通知するオプションなどがある |

### ポート番号

ポート番号は、利用するアプリケーションソフトが通信時に利用する番号のことです。コンピュータ間の通信は、基本IPアドレスで行われますが、受け取ったデータがどのアプリケーションソフトで利用されるかを判断するためにポート番号が必要となります。

次の図では、IPアドレスが192.168.0.1のPCのブラウザがポート番号54321でWebサーバにデータを要求しています。Webサーバは、データに自身のIPアドレスとWeb用のポート番号80と宛先IPが192.168.0.1、宛先ポート番号54321がついたIPパケットを送り返しています。

IP:192.168.0.1

WebサーバIP:192.168.0.2

ポート:80

アプリケーションA

ブラウザ

ポート:54321

ポート:10

IPパケット

宛先IP:192.168.0.1

宛先ポート:50

送信元IP:192.168.0.2

送信元ポート:80

データの要求

ポート番号は、16bitなので0～65535の範囲で割り当てられます。

|  |  |  |
| --- | --- | --- |
| ポート番号タイプ | 番号範囲 |  |
| ウェルノウン | 0～1023 | IANA＊で管理。サーバアプリケーションで利用される。 |
| 登録済み | 1024～49151 | IANA＊で管理。独自に作成したアプリケーションに割り当てられる。 |
| ダイナミック | 49152～65535 | クライアント側のアプリで自動的に割りあてられる。 |

＊Internet Assigned Numbers Authority（インターネット割当番号公社）

### TCPでの送受信

通信相手との専用のコネクションを確立するためのパケットの流れを図に示します。

①ホストAは切断（CLOSE）された状態から「データのやり取りをしたい」という要求である“SYN”ビットが「1」、シーケンス番号が「10」であるパケットをホストBに送り、SYN\_SENTの状態になります。シーケンス番号は、最初はデータがないためランダムな値が設定されていますが、ここでは「10」としています。また、確認応答番号は通信の最初においては設定されません。

②ホストBは、要求に応え、さらにホストAとのデータのやり取りを要求します。“ACK”ビットと“SYN”ビットが「1」で、シーケンス番号が「20」（ここでも最初はランダムですが20としておく）、確認応答番号が「11」のパケットを送信します。確認応答番号は、「受信したシーケンス番号＋１」で計算されます。ホストAは、受け取ったパケットの確認応答番号が、自分の送ったパケットのシーケンス番号＋1になっていることを確認して接続（ESTABLISH）状態になります。

③ホストAは要求に応えるために “ACK”が「1」、シーケンス番号が「11」、確認応答番号が「21（20+1）」のパケットを送ります（“SYN”ビットは「0」）。シーケンス番号は受信したパケットの確認応答番号となっています。ホストBは相手からの確認応答番号が、自分が送ったシーケンス番号＋1となっていることを確認して接続（ESTABLISH）状態になります。両方とも接続（ESTABLISH）状態になり、コネクションが確立します。このように、3回のパケットのやり取りによってコネクションを確立することを3ウェイハンドシェイクと呼びます。

SYN受信

（SYS\_RCVD）

切断

（Close）

接続

（ESTABLISHED）

**3ウェイハンドシェイク**

ホストA

ホストB

SYN送信

（SYS\_SENT）

SYN=1 シーケンス番号：10

SYN=1 ACK=1

シーケンス番号：20

確認応答番号：11

SYN=0 ACK=1

シーケンス番号：11

確認応答番号：21

①接続開始要求

②応答/接続開始要求

③応答

接続

（ESTABLISHED）

待ち受け

（LISTENING）

TCPにおける送受信通路の確立

次にデータのやり取りについて図に示します。シーケンス番号には、3ウェイハンドシェイクの最後に使われたシーケンス番号を初期値としてデータの大きさの1byteごとに１ずつ増えていく32bitの数値が割り当てられます。これは、32bitの最大値に達するとまた0から割り当てられていきます。TCPヘッダのオプションであるMSS(最大セグメント・サイズ）によってセグメントの最大サイズが決まっているため、データは必要に応じて分割されて送信されます。分割した位置を表すのにシーケンス番号が使用される仕組みになっています。

１ホストAからシーケンス番号が「11」、確認応答番号が「21」でデータサイズが200byteのパケットが送信されています。

２ホストBは、データを受け取ったことを伝えるために“ACK”ビットが「1」、シーケンス番号が「21」（受け取った確認応答番号）、確認応答番号が「211（受信したシーケンス番号＋データサイズ=11+200）」であるヘッダを作成し、さらにサイズが10byteのデータを付けたパケットを送信しています。

３ホストAは10byteのデータを受け取ったので確認応答番号を「31」（=21+10）、シーケンス番号を「211」として200byteのデータをホストBへ送信しています。データがなくなるまでこの手順が繰り返されます。また、お互いにパケットを送信した後に、“ACK”ビットが「1」のパケットを受け取らなかった場合は、パケットの再送信を行います。１つ１つのパケットを送って、受信の確認をすると、やり取りに時間が掛かってしまうため、効率化のために、いくつかのパケットをまとめて送信し、まとまりごとに受信確認を1回行う「ウィンドウ制御」といった方法があります。受信側がまとめて受け取れるデータサイズはTCPヘッダのウィンドウサイズとして3ウェイハンドシェイクの際にお互いに通知されています。

通信の切断は、“FIN”ビットが「1」となっているパケットを切断要求としてどちらかから送られます。受信した側は要求を受け入れて“ACK”ビットを「1」とし、さらに切断要求として“FIN”ビットが「1」となっているパケットを送信します。これの返信として“ACK”ビットが「1」のパケットを受け取って双方とも切断終了となります。

TCPにおけるデータのやり取り

ホストA

接続

（ESTABLISHED）

）

**データ送信**

ホストB

PSH=1 シーケンス番号：11

確認応答番号：21 データ：200byte

接続

（ESTABLISHED）

）

PSH=1 ACK=1 シーケンス番号：21

確認応答番号：211 データ：10byte

PSH=1 ACK=1 シーケンス番号：211

確認応答番号：31 データ：200byte

１

２

３