第３章　ＬＡＮのソフトウェア

第３章　LANのソフトウェア

第１節　プロトコルとTCP/IP

１－１　プロトコル

プロトコルとは、コンピュータによるデータ通信を行うために必要な取り決めの意味である。その代表的な取り決めには次のようなものがある。

●使用アプリケーションの認識
●効率的な情報交換
●通信の開始と終了の認識
●通信異常が発生した際の対応策
●データのパケット加工法（分割・組立のための）
●使用伝送路
●伝送路上における電気信号や光信号を認識

LANなどのネットワークを介した通信においては、ISOが定めたOSI基本参照モデルに表されるような階層構造をとっており、それぞれの階層で通信するための規約を提供している。

第3層及び第4層においては、米ノベルのNetWareで採用されているIPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange)やUNIXやインターネットで利用されるTCP/IP(Transport Protocol/Internet Protocol)が、また第5層以上ではファイル転送のFTP（File Transfer Protocol）、仮想端末のTelnet、WWWのHTTP（Hypertext Transfer Protocol）などがある。

一方、パソコン通信など公衆回線や専用線を介した通信には、ITU-T勧告のVシリーズと米マイクロコムが提唱しているMNP（Microcom Networking Protocol）シリーズなどがある。Vシリーズはモデムのインターフェースや通信速度、誤り訂正方式、データ圧縮方式などを定めた規格であり、MNPシリーズは1～10に分けられたクラスごとに誤り訂正方式、データ圧縮方式などが規定されている。

この背景には、異なるメーカやコンピュータの機種でもネットワーク環境下で接続できなければ汎用性に欠け、問題が生じるためである。この問題を解消するために、ITU(国際電気通信連合: international Telecommunication Union)や ISO（国際標準化機構: Intemational Organization for Standardization)といった機関が中心となり、ネットワーク構築に必要な全体構成やプロトコルなどの標準化が進められた。この標準化によってできたものが、 OSI 参照モデル(Open Systems lnterconnection)である。

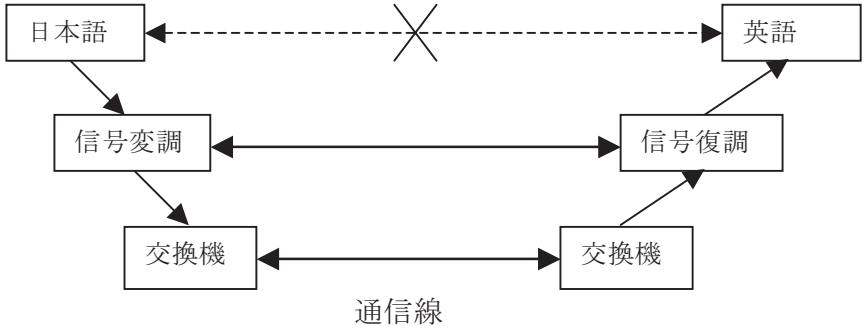
１－２　OSI 参照モデル各階層の機能

OSI 参照モデルは,必要となる多くのプロトコルを、それぞれ機能別に層（カテゴリー）で区分する。層は、より人の操作に近い部分を上位層として、通信における電気的な部分に近いものを下位層と構成されている。各層の機能は独立していて、各層のプロトコルは、自分の機能のみを管理するだけで良くなっている。このように各プロトコルの役割分担がはっきりしていることで、簡単に管理できるようになっている。

この層という概念は、電話による人と人の会話を例に挙げると理解しやすい。

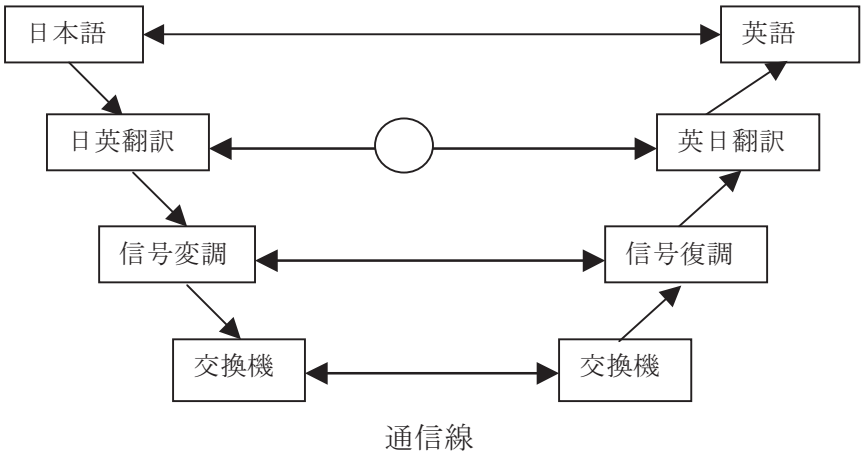
●話者が互いの言語を理解できなければ、意思を伝達できない。

⇒これは、プロトコルが異なることを表す。



●話者が互いの言語を理解できるか、翻訳機があれば、意思を伝達できる。

⇒これは、プロトコルが一致していることを表す。



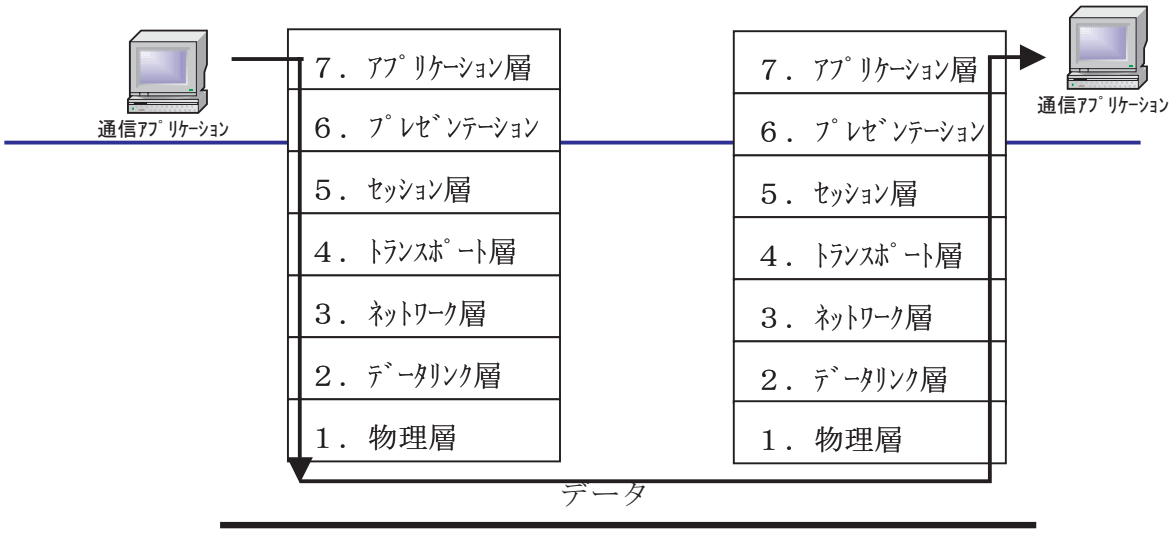
下表に、OSI 参照モデルの分類を表す。

	ＯＳＩ参照モデルの分類		概　　要
	層	層名称	
上位層	第７層	アプリケーション層 (Application Layer)	ﾌｧｲﾙ転送やﾒｯｾｰｼﾞ通信(E-Mail)などﾕｰｻﾞが実行する多くのｻｰﾋﾞｽ間ﾌﾟﾛﾄｺﾙを制御する。
	第６層	プレゼンテーション層 (Presentation Layer)	文字ｺｰﾄﾞや画像ﾃﾞｰﾀの表現形式を制御し、ﾌﾟﾛｾｽ間におけるﾃﾞｰﾀ形式などを確認する。
	第５層	セッション層 (Session Layer)	ｱﾌﾟﾘｹｰｼｮﾝ・ﾌﾟﾛｾｽ間の情報の流れなど、通信ﾓｰﾄﾞの管理や情報伝達に関する通信を制御する。
下位層	第４層	トランスポート層 (Transport Layer)	通信情報の質を高めるための通信制御などを行う。ﾃﾞｰﾀに抜けがあった場合、相手に通知する
	第３層	ネットワーク層 (Network Layer)	複数のﾈｯﾄﾜｰｸにまたがったｺﾝﾋﾟｭｰﾀ間のﾃﾞｰﾀ転送やﾃﾞｰﾀの中継機能など
	第２層	データリンク層 (Data Link Layer)	ﾉｰﾄﾞ間で信頼性の高いﾃﾞｰﾀ伝送を保証、中継局間のﾃﾞｰﾀ伝送を確実に行う。
	第１層	物理層 (Physical Layer)	ﾃﾞｰﾀを電気信号に変換し、実際の伝送を行う。

（１）第7層：アプリケーション層(Application Layer)

OSI基本参照モデルの第7層（最上位層）の名称。エンド・ツー・エンドで授受するデータの用途に応じた各種のプロトコルがある。ネットワーク管理もアプリケーション層の重要な機能である。データ転送のほかに、通信相手の確認、データのインテグリティの制御、アプリケーション間の同期などを行う。

●ファイル転送用の FTAM（File Transfer, Access and Management）
●遠隔データベース・アクセス用の RDA（Remote Database Access）
●ジョブ転送及び操作用の JTM
●電子メール用の MHS
●仮想端末用のVT（Virtual Terminal）

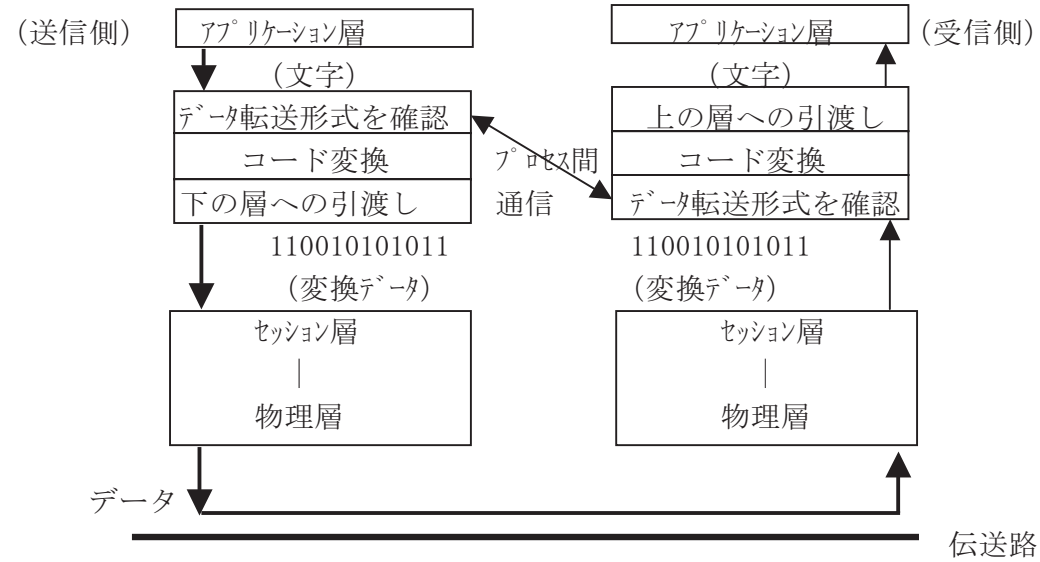


（２）第6層：プレゼンテーション層(Presentation Layer)

OSI基本参照モデルの第6層の名称。アプリケーション層が授受するデータの表現方法を規定する。

●アプリケーション層で扱う任意の構文に対応でき、必要ならば構文を変換する。

●符号や文字セットの変換、データの形式の変更



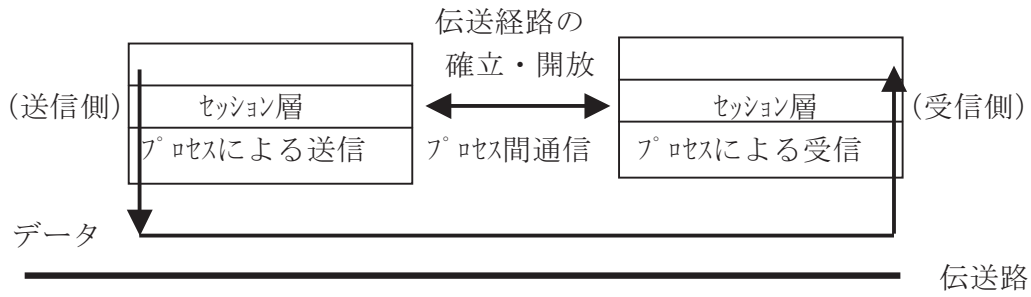
ＯＳＩ参照モデル

（３）第5層：セッション層(Session Layer)

OSI基本参照モデルの第5層の名称。アプリケーションが授受するデータの構造に着目した制御機能を実行する。

●データの区切りや誤りがあったときの再送の開始点を同期点として規定する。

●コネクションの設定と解放の動作



ＯＳＩ参照モデル

（４）第4層：トランスポート層(Transport Layer)

OSI基本参照モデルの第4層の名称。データを授受する端末間で信頼性が高いトランスペアレントなデータ転送を行う。

●通信回線の伝送品質と伝送効率を考慮して５種類がある。

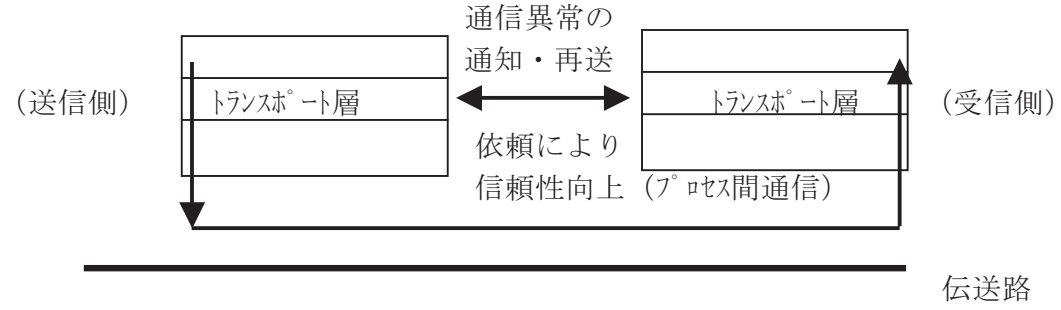
・クラス０は単純クラスでビット誤りが少なく、伝送品質が良い場合に適している

・クラス１は基本誤り回復クラス

・クラス２は多重化クラス

・クラス３は誤り回復クラス

・クラス4は誤り検出回復クラス

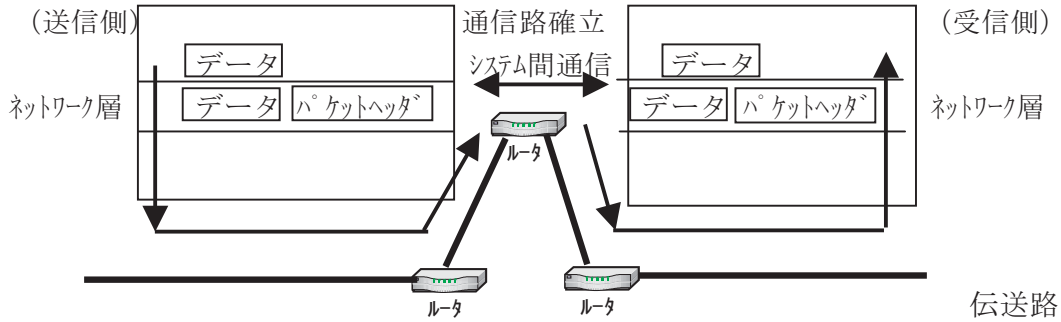


ＯＳＩ参照モデル

（５）第３層：ネットワーク層(Network Layer)

OSI基本参照モデルの第3層の名称。ネットワーク層プロトコルによって、端末間のエンド・ツー・エンドのデータ授受のルールを規定する。

●ITU-T 勧告 X.25 のレイヤ 3 プロトコル
●インターネット・プロトコル（IP）

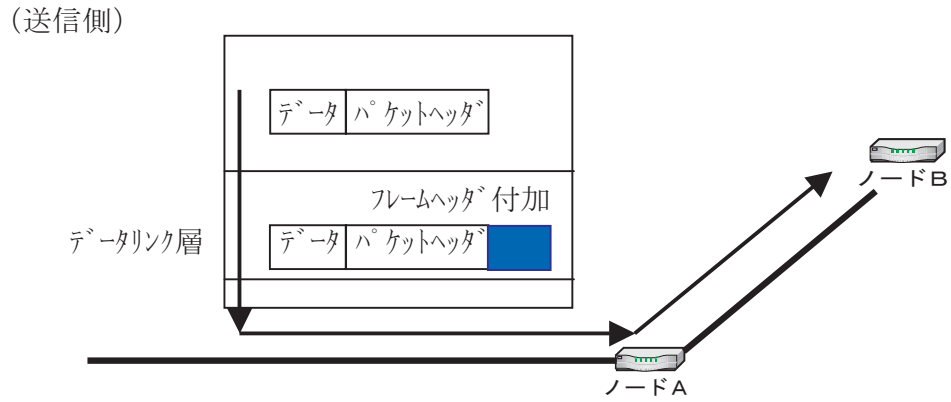


ＯＳＩ参照モデル

（６）第2層：データリンク層(Datalink Layer)

OSI基本参照モデルの第2層の名称。データリンク層プロトコルはいわゆる伝送制御手順である。

●隣接したノード間あるいは端末と隣接ノードの間のリンク単位でデータを授受する機能
●MAC（メディア・アクセス制御）プロトコル



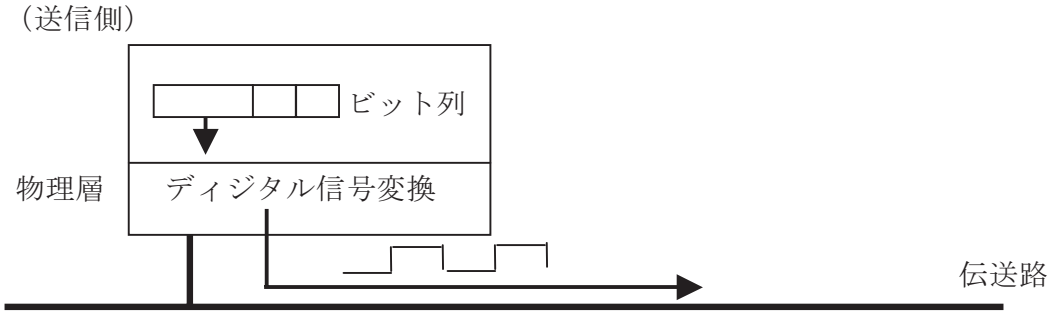
ＯＳＩ参照モデル

ルータはネットワーク層においてパケットヘッダを参照する。つぎにフレームヘッダの宛先ノードをノードＢにしてフレームを送信する。

（７）第１層：物理層(Physical Layer)

OSI基本参照モデルの第1層（最下位層）の名称。

DTE（Data Terminal Equipment）/DCE（Data Circuit-terminating Equipment）インターフェースの物理的、電気的及び論理的インターフェース条件を規定。



ＯＳＩ参照モデル

１－３　TCP/IP

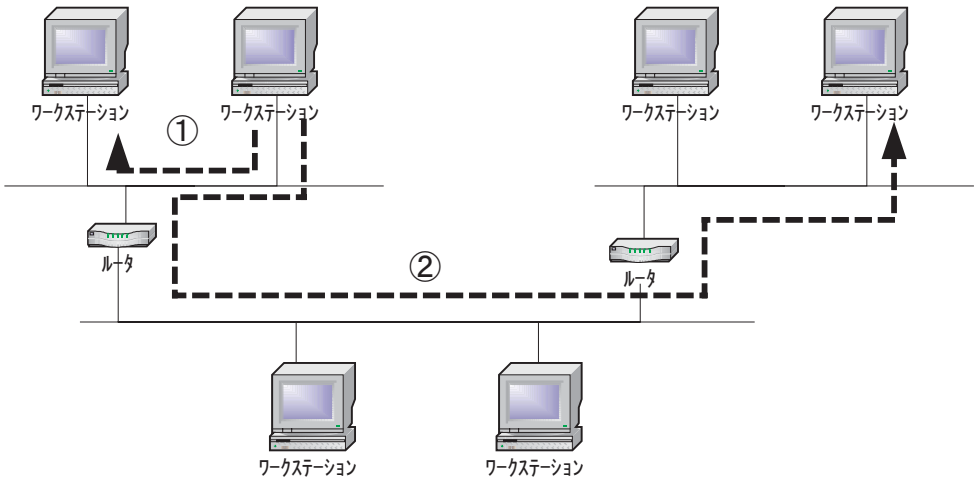
（１）EthernetとTCP/IPの関係

EthernetやIEEE802.3などのLANプロトコルは、主にOSI参照モデルのデータリンク層と物理層において取り決めを行い、データ通信をするものである。

Ethernet や IEEE802.3 は LAN プロトコル
⇒同一 LAN 上に接続されている PC やコンピュータ間でデータのやり取りを実現

インターネットのグローバルなデータ通信の実現が必要

OSI 参照モデルのネットワーク層やトランスポート層のプロトコル－TCP/IP－により同一の LAN におけるデータのやり取りという枠を超えた、グローバルのデータ通信が可能



a　同一セグメントやネットワーク内のノード間通信であれば、データリンク層を中心とするEthernetやIEEE802.3等のLANプロトコルのみで実現できる。

b　中継器やネットワークを介して通信の場合は、セグメントやネットワークの相手と情報のやり取りを行う必要がある。この規模になるとLANプロトコルのみでは対処できない。

（２）世界標準のTCP/IPプロトコル

TCP/IPは、インターネットにおける通信プロトコルの総称で、「TCP」(Transmission Control Protocol)と「IP」(internet Protocol)という二つの代表的なプロトコルをあわせたものです。一般にTCP/IPとは、TCP/IP通信に関わる多くのプロトコルから構成される一群の総称として用いられている。

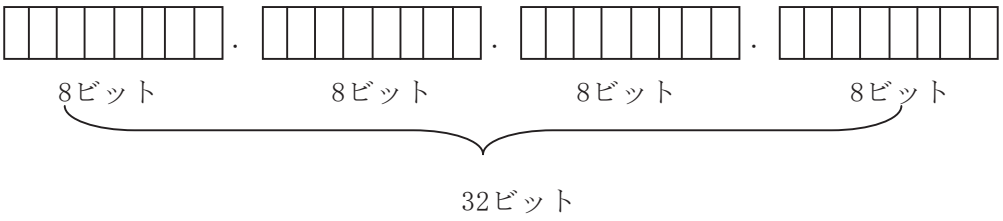
インターネットへのアクセスが可能なコンピュータやPCは、すべてTCP/IPを用いている。

OSI	TCP/IP	プロトコル名称	概　　要
第7層	アプリケーション層	BOOTP(Bootstrap Protocol)	マシン起動に必要な情報交換プロトコル
		DHCP(Dynamic Host Configuration Protocol)	マシン起動時、IPアドレスを自動付与するためのプロトコル
		DNS(Domain Name Sysytem)	ドメイン名とIPアドレスを管理するための方式
		FTP(File Transfer Protocol)	ファイル転送プロトコル
		HTTP(Hyper Text Transfer Protocol)	HTML転送プロトコル
		MIBⅡ(Management Information Base Ⅱ)	標準MIBの１つ。エージェントとマネージャ間通信プロトコル
		MIME(Multipurpose Internet Mail Extentions)	ﾃｷｽﾄﾃﾞｰﾀ以外の拡張ｺｰﾄﾞや画像、音声をｲﾝﾀｰﾈｯﾄﾒｰﾙで転送
		NNTP(Network News Transfer Protocol)	ネットワークニュース転送プロトコル
		NTPV2(Network Time Protocol Version 2)	ネットワーク上のシステム時刻の調整プロトコル
		POP3(post Office Protocol Version 3)	メールサーバからメールをゲットするためのプロトコル
		SMB(Server Message Block Protocol)	サーバ資源アクセスなどのメッセージ形式
第6層		SMTP(Simple Mail Transfer Protocol)	簡易メール転送プロトコル
		SNMP(Simple Network Management Protocol)	簡易ネットワーク管理プログラム
		TELNET	仮想端末プロトコル
		TFTP(Trivial File Transfer Protocol)	簡易ファイル転送プロトコル
		XDR(External Data Representation)	CPUの差異によって生ずるﾊﾞｲﾄｵｰﾀﾞｰなどの調整
第5層		NETBIOS(Network basic Input Output System)	ネットワーク基本入出力システム
		RPC(Remote Procedure Call)	リモート・プロシージャ呼び出し
		SOCKET	BSD版UNIXにおけるネットワークI/OのAPI
第4層	トランスポート層	TCP(Transmission Control Protocol)	TCP/IPのﾄﾗﾝｽﾎﾟｰﾄ層ﾌﾟﾛﾄｺﾙ。ｺﾈｸｼｮﾝ型ﾄﾗﾝｽﾎﾟｰﾄｻｰﾋﾞｽ。
		UDP(User Datagram Protocol)	TCP/IPのﾄﾗﾝｽﾎﾟｰﾄ層ﾌﾟﾛﾄｺﾙ。ｺﾈｸｼｮﾝﾚｽ型ﾄﾗﾝｽﾎﾟｰﾄｻｰﾋﾞｽ。
第3層	インターネット層	ICMP(Internet Control Message Protocol)	IP通信時などのエラー応答プロトコル
		IP(Internet Protocol)	通信間の通信路の確立プロトコル
		RIP(Routing information Protocol)	通信経路選択情報プロトコル
		SIPP(Simple Internet Protocol Plus)	次世代IP(IPng Next Generation)
		OSPF(Open Shortest Path First)	RIPの連続サブネット制限を解消したｲﾝﾃﾘｱﾙｰﾃｨﾝｸﾞﾌﾟﾛﾄｺﾙ
		ARP(Address Resolution Protocol)	IPアドレスからﾊｰﾄﾞｳｪｱｱﾄﾞﾚｽなどを得るプロトコル
		RARP(Reverse ARP)	EthernetなどﾊｰﾄﾞｳｪｱｱﾄﾞﾚｽをIPｱﾄﾞﾚｽに変換するﾌﾟﾛﾄｺﾙ
第2層	ネットワークインターフェース	PPP(Point to Point Protocol)	電話回線等でTCP/IP接続を行うためのﾌﾟﾛﾄｺﾙ
		SLIP(Serial Line Internet Protocol)	ｼﾘｱﾙ回線によるIP接続可能なﾌﾟﾛﾄｺﾙ
第1層		Ethernet,FDDI,X.25	
		ISDN,ATM	

第２節　ＩＰアドレス設計

２－１　IPアドレス(Internet Protocol Address)

インターネットに接続されたコンピュータの住所にあたる数列。ピリオドで四つに区切られた0～255までの10進数（「オクテット」と呼ばれる8ビット単位の固まり）で表される。世界中のコンピュータはこの合計32ビットの数値で他と区別されている。



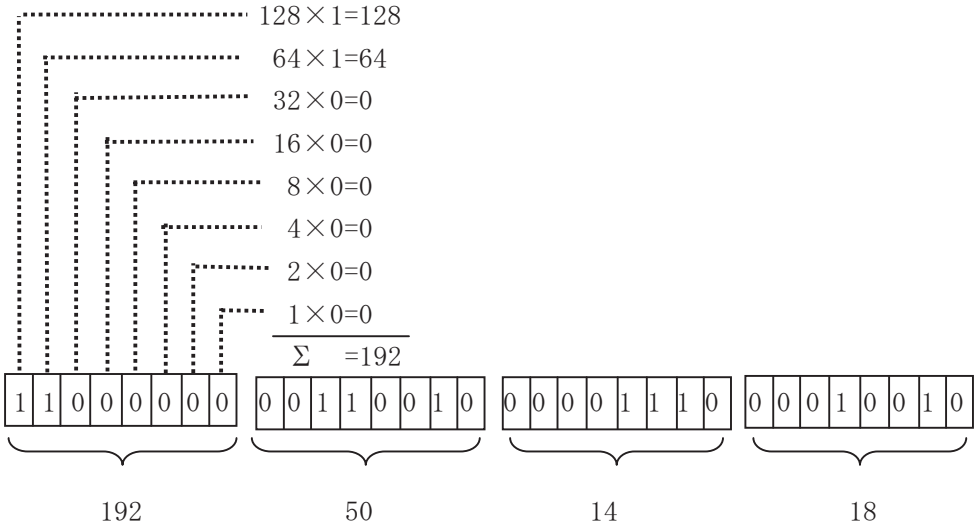
（１）　IPアドレスのクラス分け

ネットワークを構築してこれを外部ネットワーク（インターネット）と接続する際には､日本ではJPNICに申請をしてIPアドレスを取得する。

一つのネットワークに接続されるホスト数､つまりコンピュータの数は､構築するネットワークによって変わる。

IPアドレスの表現方法としてA～Eの5クラスがああり、各クラスの特徴を下表に表す。

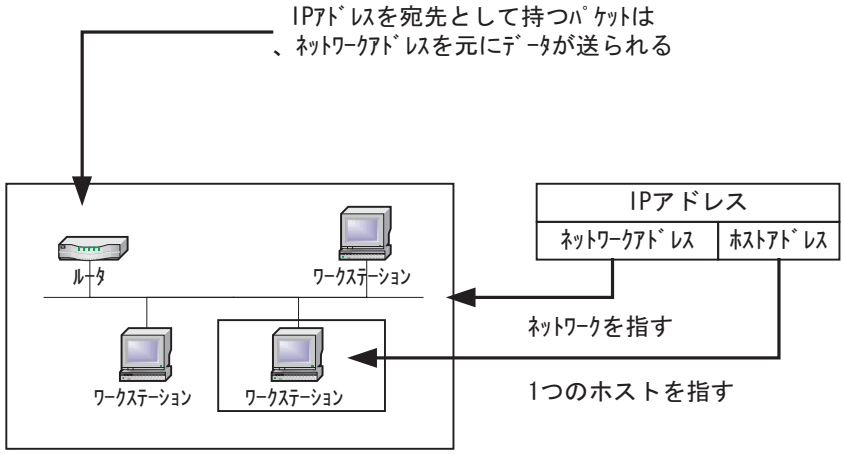
クラス	最大ホスト数	特　　徴
A	16,777,214	先頭ビット”0”で識別
B	65,534	先頭ビット”10”で識別
C	254	先頭ビット”110”で識別
D	－	ネットワーク番号だけの32ビットの特殊ケース
E	－	試験用



（２）ネットワークアドレスとホストアドレス

IPアドレスは、IPネットワークアドレスとIPホストアドレスからなる。

インターネットでは､多数のネットワークが集まって構成されており、ネットワークにはそれぞれ複数のコンピュータが接続されている｡これらを識別するには、IPアドレスにおいて､どのネットワークかを表現するためのネットワークアドレスが必要となり、さらには､このネットワーク内のどのコンピュータかを示すためのホストアドレスが必要となる。



●クラスＡ

クラス識別子：0

0	ﾈｯﾄﾜｰｸｱﾄﾞﾚｽ部	ホストアドレス部
1	7ビット	24ビット

ｱﾄﾞﾚｽ範囲:1.*.*.*～126.*.*.*
ﾈｯﾄﾜｰｸ数 :126
ホスト数 : 16,777,214
ｻﾌﾞﾈｯﾄﾏｽｸ:255.0.0.0

●クラスＢ

クラス識別子：10

10	ﾈｯﾄﾜｰｸｱﾄﾞﾚｽ部	ホストアドレス部
2	14ビット	16ビット

ｱﾄﾞﾚｽ範囲:128.1.*.*～191.254.*.*
ﾈｯﾄﾜｰｸ数 :16,382
ホスト数 : 65,534
ｻﾌﾞﾈｯﾄﾏｽｸ:255.255.0.0

●クラスＣ

クラス識別子：110

110	ﾈｯﾄﾜｰｸｱﾄﾞﾚｽ部	ホストアドレス部
3	21ビット	8ビット

ｱﾄﾞﾚｽ範囲:192.0.1.*～223.255.254.*
ﾈｯﾄﾜｰｸ数 :2,097,150
ホスト数 : 254
ｻﾌﾞﾈｯﾄﾏｽｸ:255.255.255.0

（３）サブネットマスク

サブネットマスクとは、IPホストアドレスを合理的に利用しようとするものである。ホストアドレス部の一部をサブネットアドレス部として定義することで、ネットワークに接続することのできるコンピュータの台数は少なくなるものの、より多くの企業などにネットワークを割り振ることを実現することができる。

また、割り当てられたIPアドレスを用いて、一つの企業が複数のLANなどを構築する場合にも有効であり、本来は一つのネットワークを意味するIPアドレスでも、サブネットマスクによって複数のネットワークを表現することが可能となるためである。

200.1.1.0というIPアドレスを例にとって、サブネットマスクを説明する。

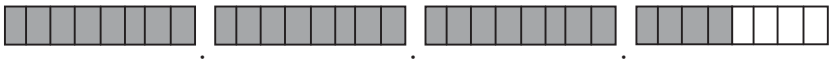
●クラス C(サブネットマスク値は 255.255.255.0)に対して２５４台のホストの接続が可能

２５４＝２５６（2^8）－２

●ホストアドレス”00000000”と”1111111”の２台分は使用できない
次節で説明。

●IP アドレス　２００．１．１．０／２８　の意味
IP アドレス 32 ビット中、２８ビットをプリフィックスとしてネットワークアドレスとして使用、残り４ビットをホストアドレスを利用することを表す。

●サブネットマスク（２５５．２５５．２５５．２４０）に相当



●200.1.1 というネットワークアドレスに対して 1 から 14 までの 14 のサブネット(0 と 15 を除く)を設定可能

●一つのネットワークには 14 台のノードを接続可能

このように、割り当てられた空間の区分けを変えるための仕組み、これがサブネットマスクです。なお、サブネットはRFC950によって定義されている。

クラスＣ	110	ネットワークアドレス																				ホストアドレス							
IPｱﾄﾞﾚｽ	200								1								1								0					
	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0

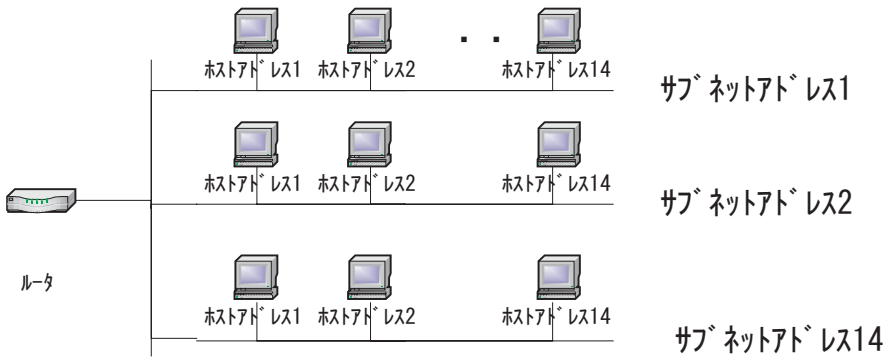
クラスＣでは、ホストを１～２５４の合計２５４台接続できる。しかし、個人、小規模の会社では、これほど必要ない。

ｻﾌﾞﾈｯﾄ	255								255								255								255							
ﾏｽｸ	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

そこで、255.255.255.240でサブネットマスクを行い、ホストアドレスの４ビットをサブネットアドレスとする。

ｻﾌﾞﾈｯﾄ	110	ネットワークアドレス																				ｻﾌﾞﾈｯﾄｱﾄﾞﾚｽ				ﾎｽﾄｱﾄﾞﾚｽ			
ﾜｰｸｱﾄﾞﾚｽ	200								1								1								0					
	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0

サブネット１～１４の１４ネットワーク、各サブネットに１～１４ホストの接続が可能になる。



サブネットワーク

①200.1.1.　17～200.1.1.　30	⑧200.1.1.129～200.1.1.142
②200.1.1.　33～200.1.1.　46	⑨200.1.1.145～200.1.1.158
③200.1.1.　49～200.1.1.　62	⑩200.1.1.161～200.1.1.174
④200.1.1.　65～200.1.1.　78	⑪200.1.1.177～200.1.1.190
⑤200.1.1.　81～200.1.1.　94	⑫200.1.1.193～200.1.1.206
⑥200.1.1.　97～200.1.1.110	⑬200.1.1.209～200.1.1.222
⑦200.1.1.113～200.1.1.126	⑭200.1.1.225～200.1.1.238

●サブネットマスクのマスク

bitパターンの中のある部分に覆いをかけ、必要な部分だけを取り出すことをマスキングという。0の並びを覆いとするもので、bit配列の中から必要なbit情報だけを取り出す際に使われる。

①8bitの情報の下位4bitにマスクをかけ上位4bitだけを取り出す

このとき、ビット毎のAND(論理積)処理した場合、すなわち元データのビットとマスキングデータのビットが共に“１”である場合のみ“１”となる演算を用いる。

真理値表

AND	0	1
0	0	0
1	0	1

元データ	１１０１０１０１
ﾏｽｷﾝｸﾞﾃﾞｰﾀによるAND	１１１１００００
マスキング結果	１１０１００００

（４）グローバルアドレスとプライベートアドレス

IPアドレスがネットワークとコンピュータそれぞれを表し、このアドレスをもとに通信が行われる。すなわち、IPアドレスは同じものが二つ以上存在してはならないことになる。

世界のIPアドレスはNIC(Network Information Center)で一元管理され、日本国内のIPアドレスの割り当てはJPNIC(Japan Network Information Center)が行っている。これらの機関はIPアドレスが重複しないように管理している。この世界レベルで割り振られたIPアドレスを**グローバルアドレス**という。

LANにおいてTCP/IPを用いる場合、RFC1918で定義されているインターネット上では利用を許可されないIPアドレスを用いることがあるが、このIPアドレスをプライベートアドレスと呼ぶ。この宛先を持つパケットが仮にインターネット上に送信されたとしてもルーティングしてはならないことになっているため、このパケットは破棄されます。これを**プライベートアドレス**という。

クラス別プライベートアドレス

クラス	ﾈｯﾄﾜｰｸ数	アドレス範囲
A	1	10.0.0.0～10.255.255.255
B	16	172.16.0.0～172.31.255.255
C	256	192.168.0.0～192.168.255.255

（５）ブロードキャストアドレス

IPホストアドレスの説明で、すべてのビットが０かもしくは１であるホストアドレスは、あらかじめ特別な意味を持つアドレスとして定義されて、使用できないことになっている。

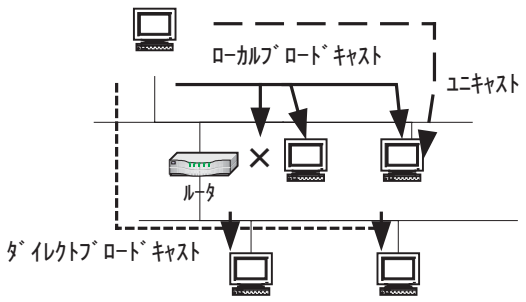
●ビットがすべて０（すべてが０である８ビットの数値は１０進数でも０となります）のアドレスは、ホストアドレスが不明なノードとしての意味を持つ。
●ビットがすべて１（すべてが１である８ビットの数値は１０進数で２５５となります）のIPホストアドレスは、ブロードキャストアドレスとしてリサーブされている。
●ブロードキャストとは同報通信という意味であり、ネットワーク全体へ同時にデータを送信するための宛先 IP アドレスとして扱われます。パケットを一つ送信するだけでネットワーク全体にデータが送信される。

●ローカルブロードキャストアドレスとダイレクトブロードキャストアドレス

●ローカルブロードキャストアドレスとは、自己の属したネットワーク内にブロードキャストをするためのもの
●ダイレクトブロードキャストアドレスとは、異なる IP ネットワークに対してブロードキャスト

●ユニキャスト

宛先を限定するため、パケットが届く相手が決まっている。



- ローカルブロードキャスト

ブロードキャストアドレス130.1.255.255とすると130.1.0.0のネットワークすべてに同時にパケットを送信する。

ルータは通過できない。

●ダイレクトブロードキャスト

ダイレクトブロードキャストは130.2.255.255である。

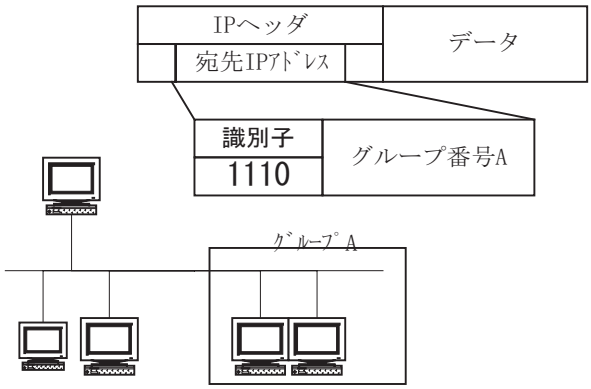
他のネットワークへ発信可能。

（６）IPマルチキャスト

マルチキャストとはブロードキャストと同様に、一度に複数のノードに対してデータを送信することのできる機能である。マルチキャストとブロードキャストの違いは、ブロードキャストがネットワーク全体にデータを送信し、その中でそれを受け取るべき該当ノードがこれを取得する一方で、それ以外のノードはこのデータを破棄するというものである。これ対して、マルチキャストは必要とするグループ内のノードに限定しデータを送信するというものである。

ブロードキャストでは、不要なノードに対してもデータを送信するためネットワーク全体に負荷をかけやすいという欠点があるが、マルチキャストでは必要なノードに限定して一度にデータを送信できるので、ネットワークの負担を最小限にとどめることが可能である。

IPマルチキャストはクラスDのIPアドレスを使用し、先頭４ビットの識別子を除く２８ビットをグループアドレスとして活用する。



※IPマルチキャストを行うには、宛先IPアドレスにクラスDのIPアドレスを使う。

●ループバックアドレス

●クラスAのネットワークアドレス１２７．０．０．０は、ループバック(loopback)のために予約されているため、IPアドレスとして使用することができない。
●ループバックアドレスは、ネットワーク上などでローカルなテストなどを行う際に利用されるものであり、これもまた一般のIPアドレスではない。

（７）IPv4

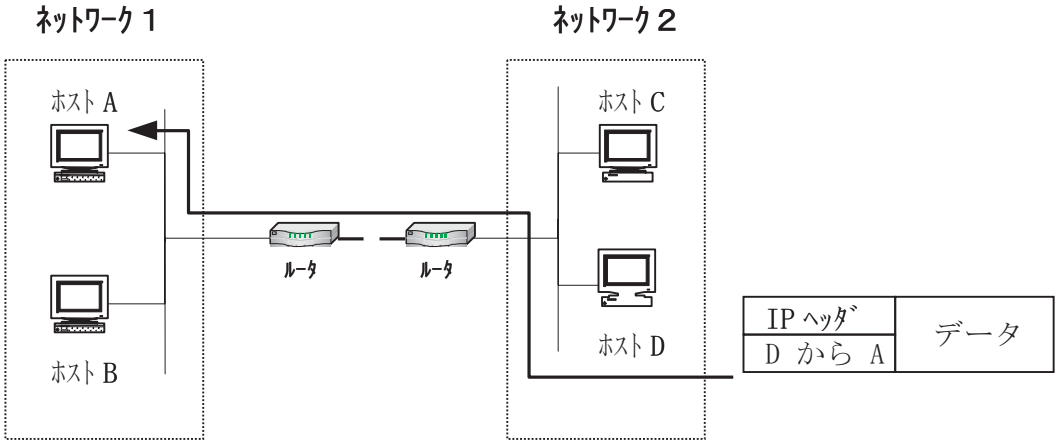
●IPv4機能

IPは現在、インターネットの大部分においてバージョン4(IPv4)が使用されているが、IPアドレスの不足などの要因から、バックボーン・ネットワークレベルのIPアドレスからバージョン6(IPv6)へと移行が今後、進むとしている。

IPは、 OSI参照モデルの第3層であるネットワーク層(TCP/IPではインターネット層ともいいます)のプロトコルである。

トランスポート層プロトコルは､互いのポート間の情報交換を管理していたが､これだけでは離れたどのコンピュータに対してデータを送信するのかがわからず、データを相手のコンピュータに送り届けることができない｡そこで､トランスポート層のTCPヘッダにネットワーク層のヘッダを付加し、トランスポート層では実現しなかった、互いのコンピュータアドレスに関するやり取りを実現しようというものである。

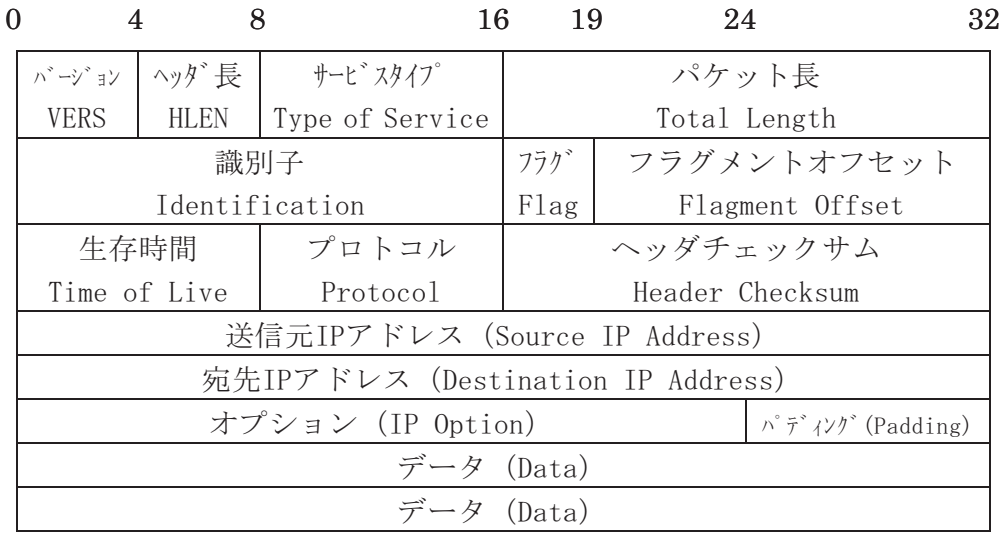
IPはコネクションレス型となっている｡すなわち、IPがデータの送信に確認応答などを行わないプロトコルということになる｡この機能は、トランスポート層におけるTCPに委ねられており､TCPで互いのデータのやり取りを保証しているため、IPではアドレスに関わる機能を完全にしていることで役割を分担している。



●IPv4の構造

IPによって情報を転送する場合、ネットワーク層により、データにIPヘッダを付加して下位層に引き渡すことになる。IPヘッダは､トランスポート層によって付加されたTCPヘッダの上部に付加されることになり､これは､一つのデータをトランスポート層でTCPのラベルが付いた容器に入れてネットワーク層に渡し､ネットワーク層では渡された容器をさらにIPのラベルが付いた容器に入れるという物理的な動だと考えることができる。

下図にIPv4の構造を示す。



・**バージョン(VERS)**はIPがつねに進化できるようにその進化過程の通番を管理するものです。現在のバージョンの多くは4が使われているが、受信したIPヘッダのバージョン番号を確認することで、それ以降のデータの並びが上図のようになっていることを暗黙のうちに知ることができる。

・**フラグ(Flags)**は、パケットの分割に関する情報を表している。データは複数のパケットに分割され、複数回の送信で引き渡されることになる。そのフラグメントが途中のものなのか、最後のものなのかはデータの中味を見なければ認識ができないため、ネットワーク層で確認する術が無い。そこで、このフィールドのビット２を参照することで認識できるようにしている。ビット２が１であれば途中のパケットであり、０であれば最後のパケットであることを表している。

・**生存時間(Time To Live)**は、パケットの寿命に関する情報である。パケットは複数の中継点を介して相手のコンピュータに引き渡される際、通信経路情報の誤りなどによって宛先に到達することができなく、同じ経路を回り続けるような事態が発生する。パケットがネットワークに複数存在するとネットワーク全体に負荷をかけることになるため、これを防止するためパケットに寿命を設定している。ルータなどでルーティングされるたびにその寿命が減らされて、それが０となった時点でこのパケットをルーティングせずに破棄することになる。

・**プロトコル(Protocol)**は上位層のプロトコルが何であるのかを示している。これは、 IPのラベルがパケットの中には何が入っているか、という情報を表記するものである。

（８）IPv6(Internet Protocol Version 6)

現在の標準的なインターネット・プロトコルである「IPv4」に代わる次世代プロトコルである。現在のインターネットのアドレス空間がもつ問題（クラスBの枯渇、経路制御情報の飽和、32ビット・アドレスの枯渇など）を解決するために策定されたものである。

IPv4からの主な変更点は、

①32ビットから128ビットへのアドレス空間の飛躍的な拡大

②ヘッダー・フォーマットの簡素化

③経路処理などの高速化

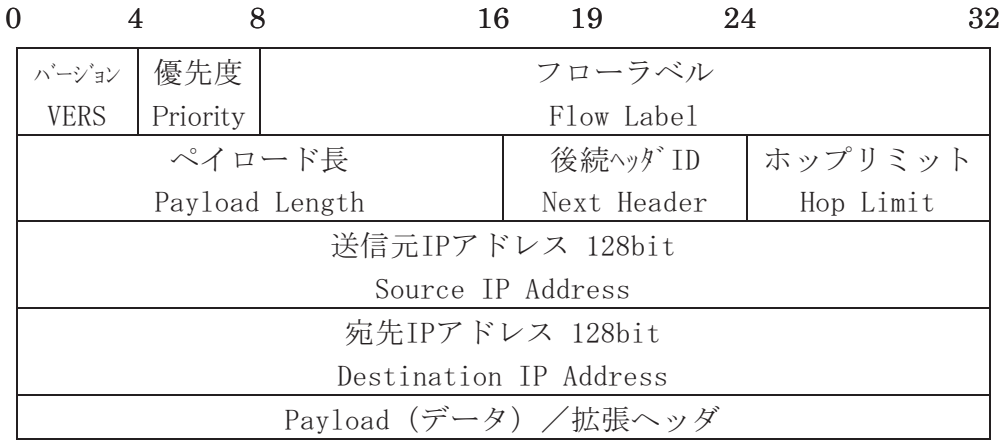
④機能の拡張性と柔軟性

⑤フロー・ラベル機能やセキュリティ機能の導入

などである。

●IPv6の構造

下図にIPv6の構造を示す。



・バージョン(VERS)はIPv6なので、６という数字が設定されている。

・優先度(Priority)はIPv4にはないもので、通信効率を上げるため新たに作られたフィールドである。パケットを処理する上での優先順位を表現できる。4ビットで構成される。

・フローラベル(Flow Label)では、優先度で表現されたパケットをあるまとまりの単位で区別する。２４ビットで構成される。

・ペイロード長(Payload Length)は、IPv4における全パケット長に相当するものであり、IPv6ヘッダの後に続くデータの長さを示すものである。IPv6ヘッダには、通常TCPヘッダが続くが、このTCPヘッダとその後ろのデータの長さを足した長さが、このフィールドにセットされる。

・拡張ヘッダには中継点オプションヘッダ、経路制御ヘッダ、断片ヘッダ、認証ヘッダ、暗号ペイロードヘッダ、終点オプションヘッダの6種類のヘッダがある。IPv6では、こ

れらのヘッダを数珠つなぎに組み合わせることができ、通信効率が向上する。16bitで構成される。また、一部の拡張ヘッダではインターネット上で必要となる認証や暗号化などセキュリティ機能を持つものもありますが、 IPV6では、セキュリティ機能も標準でサポートしている。

・後続ヘッダID(Next Header)は、後に続くヘッダがどのようなものなのかを示し、８ビットで構成される。

（９）TCP/IP 以外の LAN 対応プロトコル

多くのベンダからリリースされる NOS（Network　OS）によって、それぞれサポートされるプロトコルが異なるが TCP/IP もサポートしているのが一般的である。

これらの LAN で使用されるプロトコルは、 Ethernet など物理層やデータリンク層のプロトコルの上位層であるネットワーク層とトランスポート層において機能するものである。以下の表に 3 つの代表的な LAN 対応プロトコルを表す。

通信ﾌﾟﾛﾄｺﾙ	OS名	概　　要
IPX/SPX	NetWare	米・ノベル社の NetWare で使用されているプロトコル。Ethernet、トークンリング、FDDI などと組み合わせることも可能。
AppleTalk	MacOS	米・アップルコンピュータ社の提供するプロトコル。LocalTalk、EtherTalk、TokenTalk 等によって構成される。
NetBEUI	Windows OS	NetBIOSの拡張プロトコル。小規模LANの構築に適しているが、ルーティングに対応しないため、複数のネットワークにまたがるLAN間接続には向いていない。

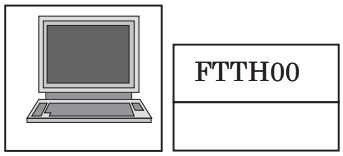
２－２　サブネットワーク化演習

現在、ネットワーク番号 10.19.133.0/24 が割当てられている。フロア内を６つのサブネットとし、サブネットは最大２５台のホストをサポートするために、サブネットおよびホストのＩＰアドレスを定義しなさい。

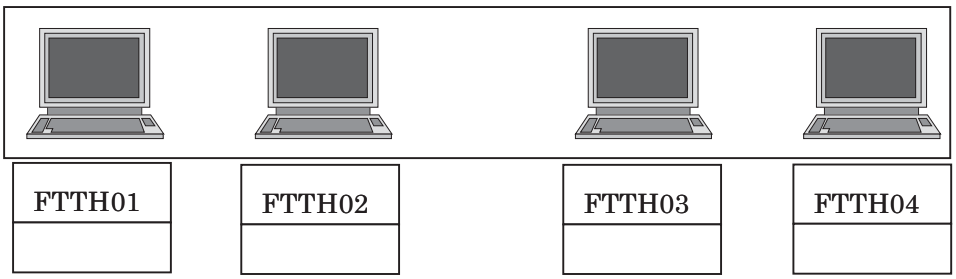
ここでは、教室内を４つのサブネットで使用することとし、ホストのＩＰアドレスの再定義、ネットマスクの再定義をしなさい。

確認は、ping 等を用いてグループ内、グループ外に対して問合せを行い実施しなさい。

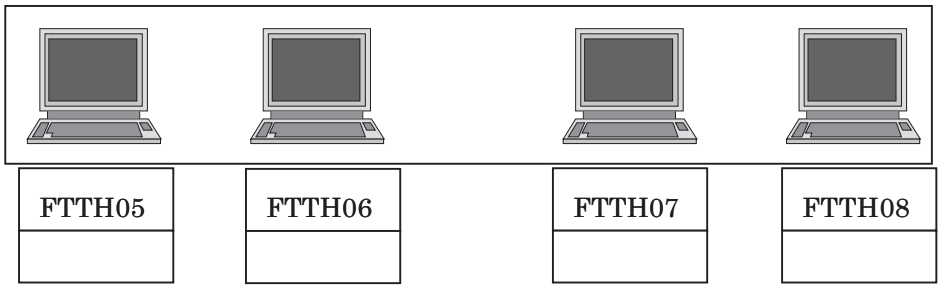
グループ０



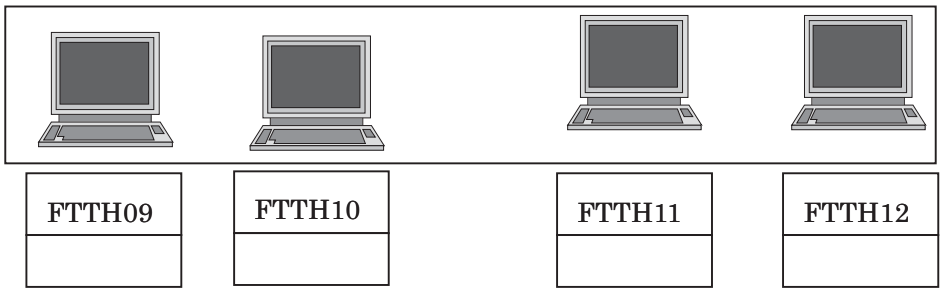
グループ１



グループ２



グループ３



第３節　ＬＡＮ構築実習

３－１　LAN 構築手順

LANを構築する場合、検討すべき課題や作業が数多くある。以下に、各フェーズごとにまとめると、下図のようになる。

（１）フェーズⅠ
（要求分析）

- 現状分析と新規システムのニーズ分析
- 将来構想

（２）フェーズⅡ
（設計）

- ネットワーク構成の設計
- システム構成機器の選定
- 回線構成／方式の決定
- 導入効果試算

（３）フェーズⅢ
（構築）

- 構築スケジュール決定
- 機器の数量決定と発注
- 導入機器の設置環境の整備
- ソフトウェアの開発
- 運用／利用の事前教育
- 回線／機器の動作確認とテスト

（４）フェーズⅣ
（運用・評価）

- 効率的なネットワーク管理
- 性能／機能の把握
- ユーザの満足度チェック
- ネットワーク利用促進

３－２　ネットワークシステムの要求定義

（１）現状分析とニーズ分析

a　現状分析

現在ネットワークシステムがある場合は、その実態調査を行って、実際の業務形態および問題点を把握する。とくに、現状システム利用者の不便、問題を洗い出して、把握する。具体的な方法として以下がある。

・ヒアリング

・トラフィック測定

b　ニーズ分析

・部門間でのワークフローの明確化

・情報機器の設置場所と台数、金額および納期の調査

・情報の管理責任者と情報に対するアクセス権の基準を明確化

・入出力条件の明確化

・トラフィック条件の調査

・システムの運用条件と障害対策基準の明確化

・機能要件

1)ホストと端末間(PC、WS)の接続機能

2)リソースシェアリング(資源の共有)

3)ファイル転送

4)オンラインデータ処理の有無

5)電子メール使用の有無

・性能要件

1)トラフィック量

2)応答時間

3)通信回線および機器の利用率

4)信頼性要件(MTBF と MTTR)

5)異常トラフィックと過負荷対策

6)通信回線・機器の安全性要件

7)情報セキュリティ

・運用要件

1)サービス時間

2)データバックアップ

3)システム立ち上げ手順

4)ネットワーク管理

5)課　金

・保守業務

1)消耗品の管理と補給

2)異常時の対応、データやプログラムの保存

・拡張性要件

（２）ネットワークシステムの設計

作成した要求定義書を基にネットワークシステムの設計を行う。設計は「論理的なシステム設計」と「物理的なシステム設計」の二つの段階で行う。論理設計ではネットワークの利用形態を規定し、物理設計では論理設計の結果を基に具体的な機器や情報ネットワークを決定する。

ａ　ネットワークシステムの論理設計

論理設計では、ネットワークの利用形態を規定する。

・ネットワークモデルの作成

1)照会応答型

2)データ収集型

3)データ分配型

4)メッセージ交換型

・ネットワークトポロジーの設計（バス型、リング型、スター型）

1)単一トポロジーの１階層ネットワーク

2)同じトポロジーのネットワーク階層構造

3)異なるトポロジーのネットワーク階層構造

・通信方式

1)コネクション型／コネクションレス型

2)連続転送/バースト転送

3)伝送速度

4)エンド・ツー・エンドの伝送遅延時間

5)エンド･ツー･エンドの通信品質(減衰歪み、瞬断、群遅延歪み、周波数変動、ノイズ)

・識別コード体系(番号計画、アドレス体系)

・ネットワーク･アーキテクチャ

・課金方法

ｂ　ネットワークシステムの物理設計

物理設計では、ネットワーク接続機器を選定し、機器の電源容量、スペース、空調などの容量を確定する。

・リンク設備の選択と設備容量の算出

・ノード設備の選択と設備容量の算出

1)多重化装置

2)交換機

3)LAN の相互接続装置

4)フレームリレーやセルリレーのインタフェース装置

・ネットワークの構成図

・機器の設置場所と数および回線数

1)床荷重

2)ケーブル配置場所(床下配線の可能性など)

3)電源提供と電源容量

4)空調条件

３－３　ＬＡＮ構築実習

最も基本的な構内ＬＡＮの構築を行う。

【構築例－１】１セグメント・ネットワーク構築演習

（ネットワークシステムの要件）

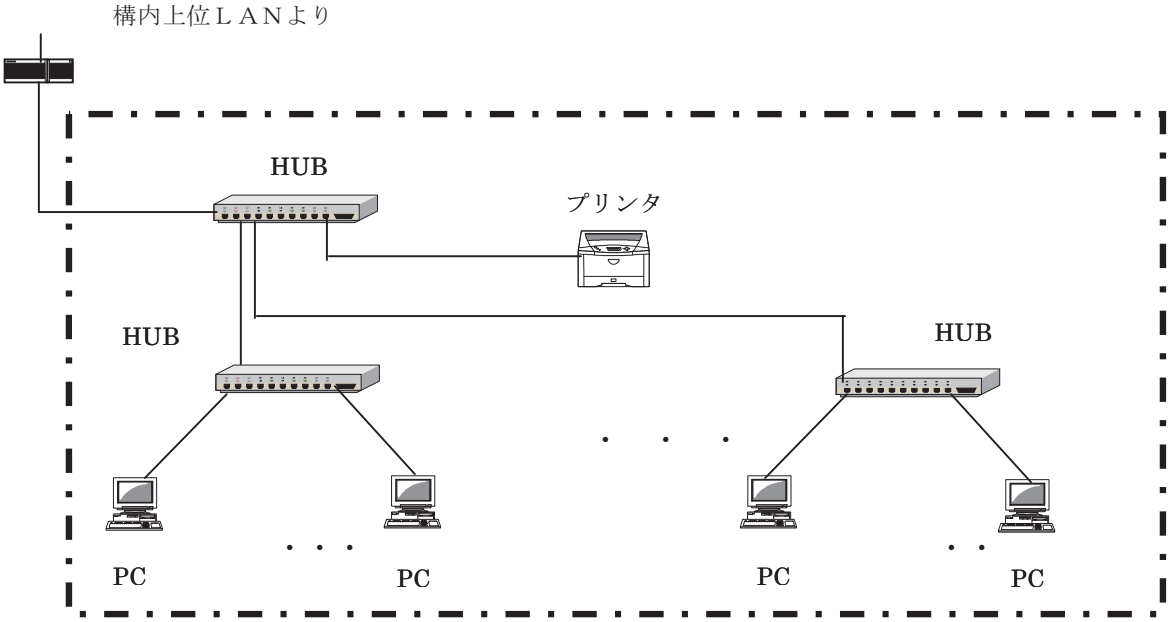
・管理者より与えられた、クラスＣのネットワーク・アドレス（10.19.133.0）を使用する。

・事務所内を１つのセグメントとして、PC(パソコン)２５台、ネットワーク・プリンタ１台を接続する。

・HUB は必要台数用意する。

（IP アドレスの設計）

No.	ｺﾝﾋﾟｭｰﾀ名	IP アドレス	No.	ｺﾝﾋﾟｭｰﾀ名	IP アドレス
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					



【構築例－２】サブネットワーク化演習

（ネットワークシステムの要件）

・管理者より与えられたクラスＣの内、ネットワーク番号（10.19.133.0/27）を使用する。

・６つのサブネットワークとし、サブネットワークは最大２５台のホストをサポートするために、サブネットおよびホストのＩＰアドレスを定義する。各サブネットワークにネットワーク・プリンタ１台を接続する。

・HUB は、必要台数用意する。

（IP アドレスの設計）

サブネットワークは以下となる。【参考】

① 00001010.00010011.10000101.000**00000** = 10.19.133.0/27

② 00001010.00010011.10000101.001**00000** = 10.19.133.32/27

③ 00001010.00010011.10000101.010**00000** = 10.19.133.64/27

④ 00001010.00010011.10000101.011**00000** = 10.19.133.96/27

⑤ 00001010.00010011.10000101.100**00000** = 10.19.133.128/27

⑥ 00001010.00010011.10000101.101**00000** = 10.19.133.160/27

⑦ 00001010.00010011.10000101.110**00000** = 10.19.133.192/27

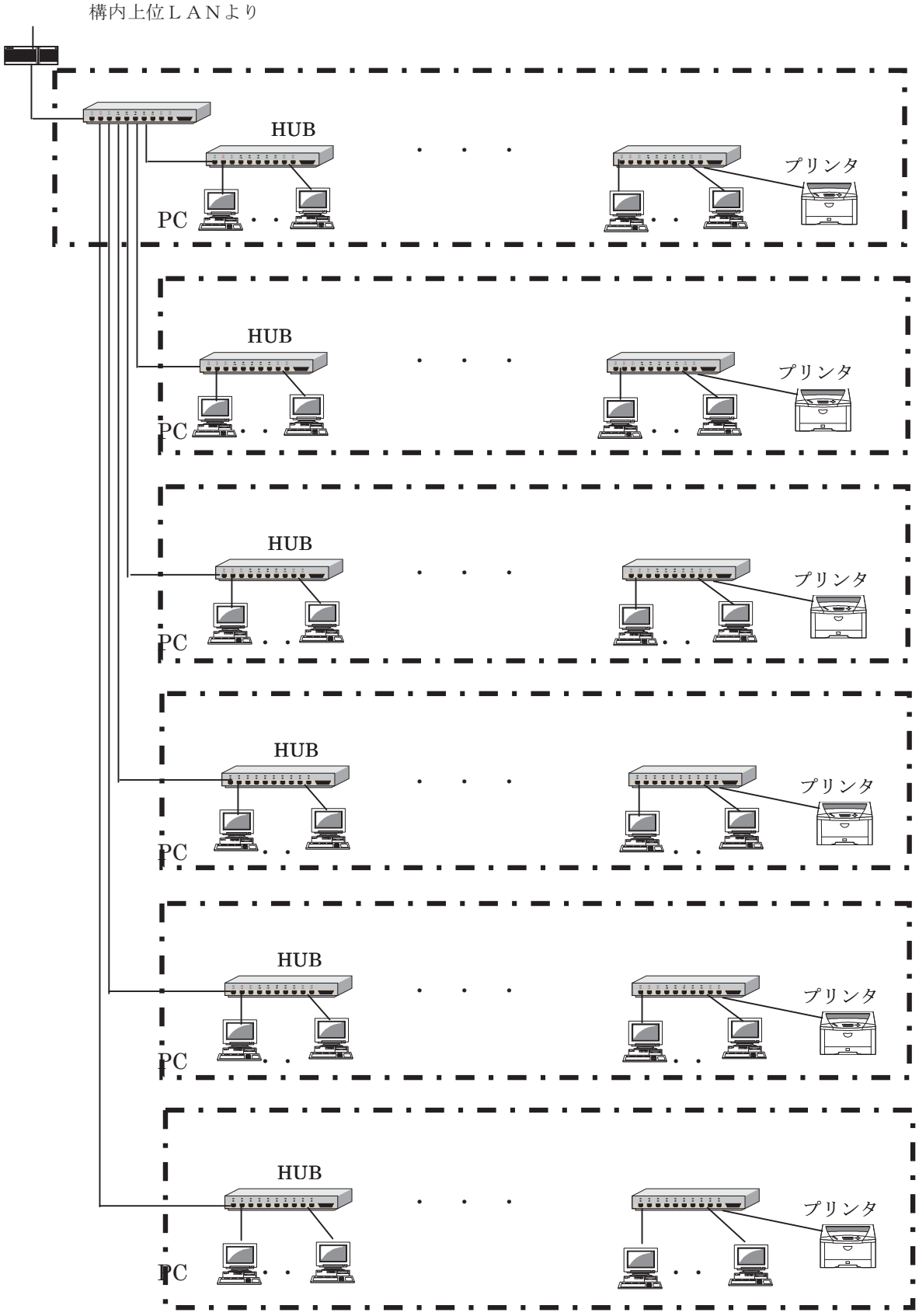
⑧ 00001010.00010011.10000101.111**00000** = 10.19.133.224/27

（接続確認）

確認は、ping 等を用いてグループ内、グループ外に対して問合せを行う。

（IP アドレスの設計）

No.	ｺﾝﾋﾟｭｰﾀ名	IP アドレス	No.	ｺﾝﾋﾟｭｰﾀ名	IP アドレス
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					


構内上位ＬＡＮより
HUB
PC
プリンタ
HUB
PC
プリンタ
HUB
PC
プリンタ
HUB
PC
プリンタ
HUB
PC
プリンタ
HUB
PC
プリンタ

【参考文献】

１．Open Design　LAN 技術総合入門　No.12　CQ 出版社　1997

２．TCP/IP　西田著　ソフトリサーチセンター　1991