ネットワーク1

http://cobayasi.com/koza/security/3_network1.pdf

1. ネットワークの基礎
2. TCP/IP
3. IPアドレス
4. ポート番号

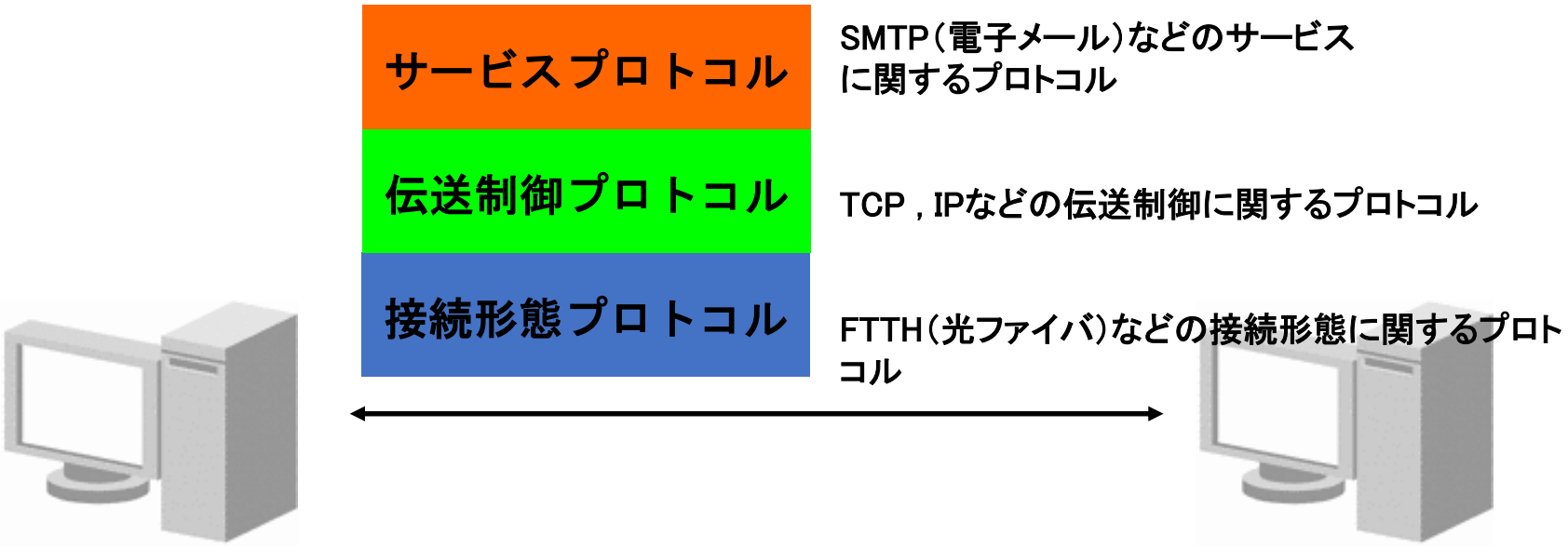
ネットワークの基礎

テキストP248-253

プロトコル(Protocol)

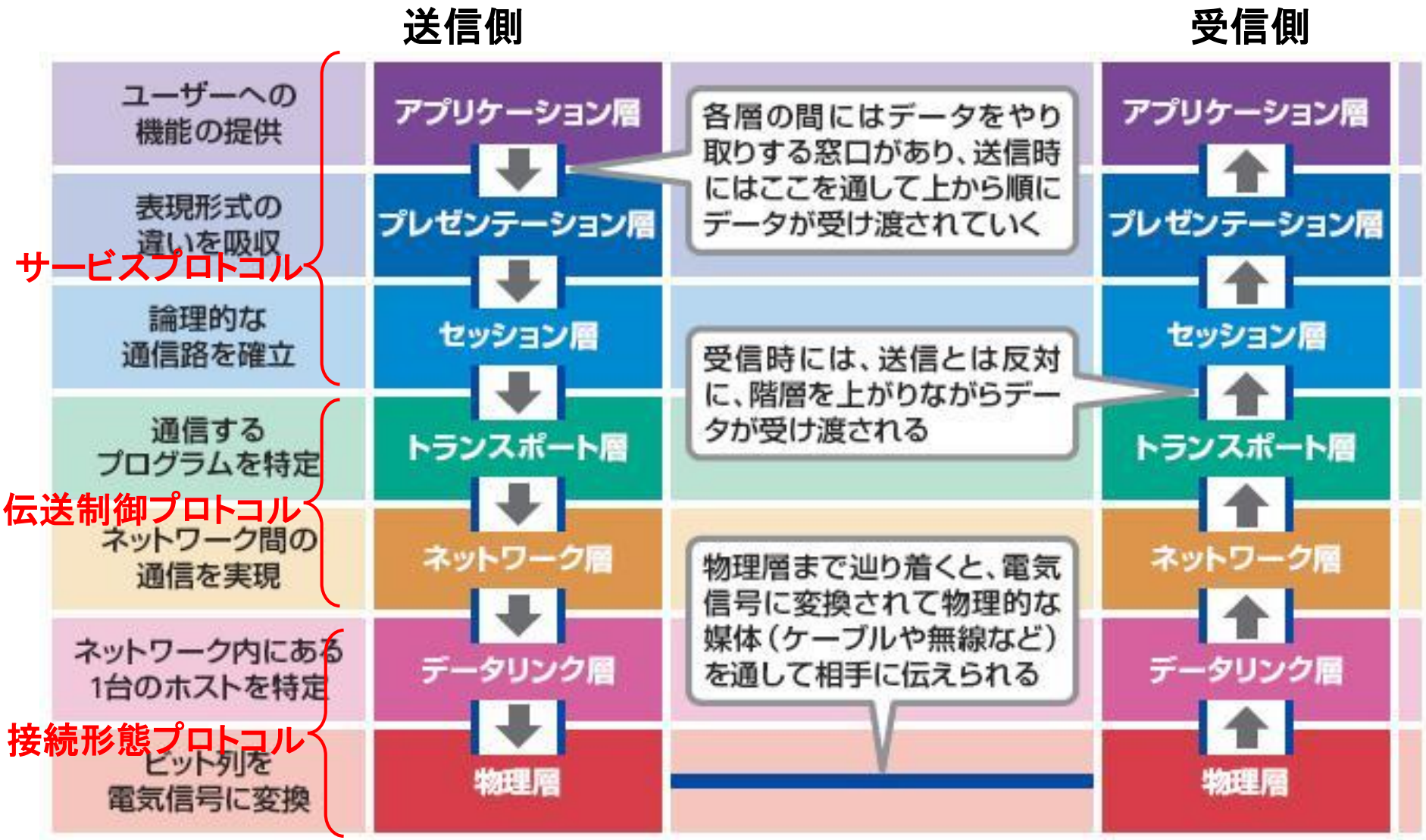
コンピュータ同士が、支障なくデータをやり取りするための共通の決まり事

階層構造



OSI(Open Systems Interconnection)参照モデル

〈通信プロトコルの役割を細分化したもの〉



階層化のメリット

- **シンプルである**

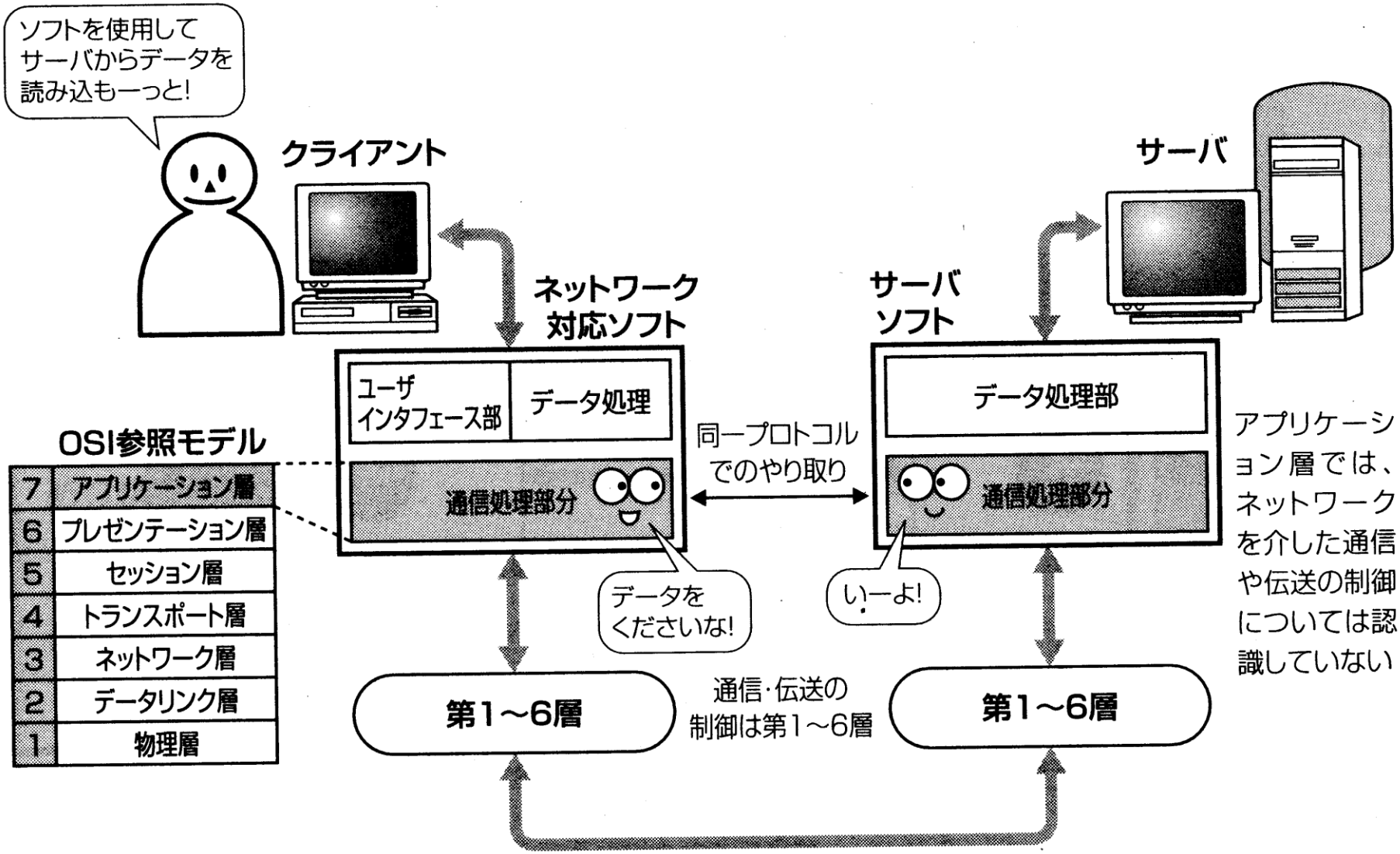
　通信プロトコルを階層化することで、たくさんの機能を、１つの階層に詰め込む必要がなく、各層では、安定した動作をすることができる

- **交換が容易である**

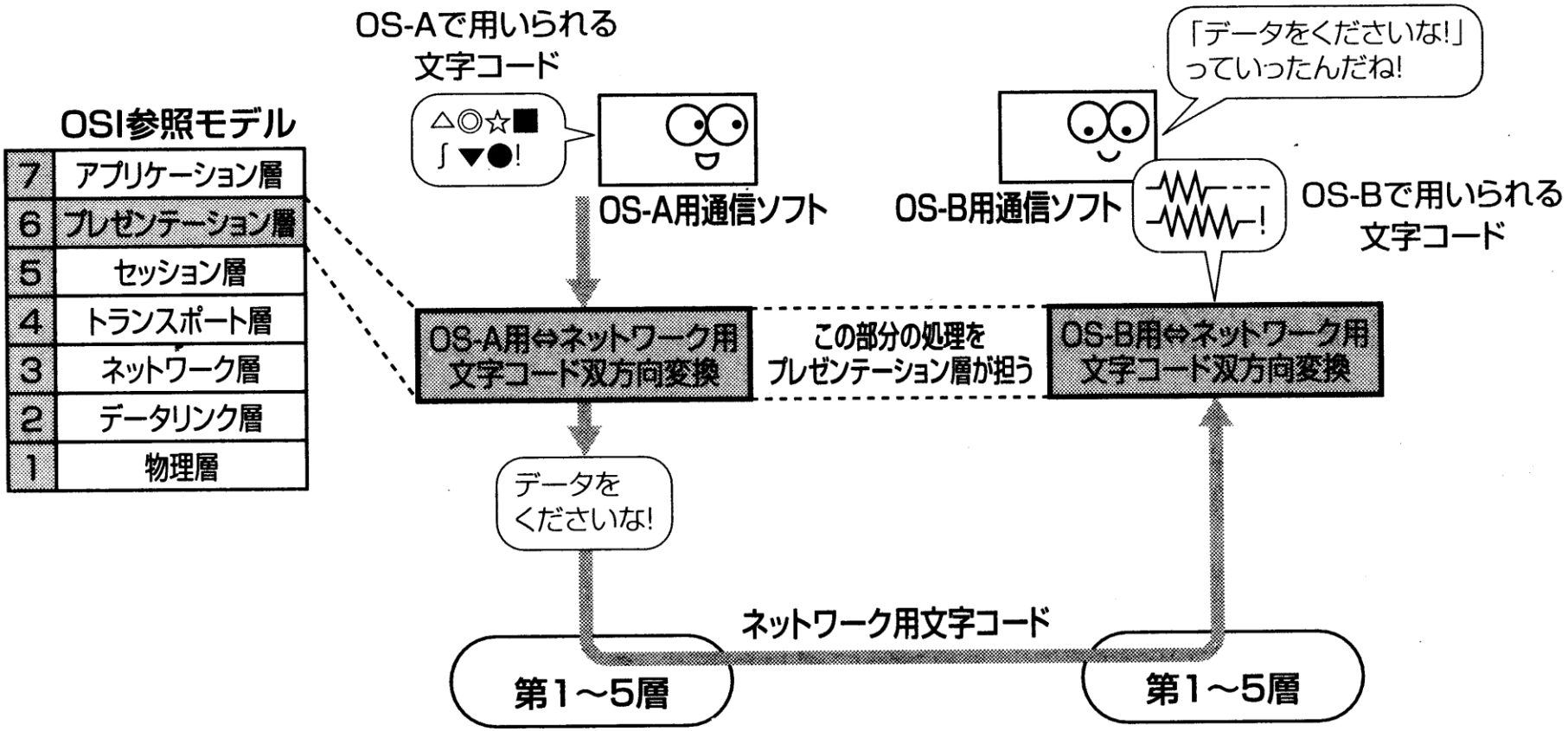
　１つの階層に必要最低限度の機能を持たせることで、何らかの理由で、通信機能の変更が生じた場合には、他の階層と容易に交換・更新することができる

OSI参照モデルの詳細

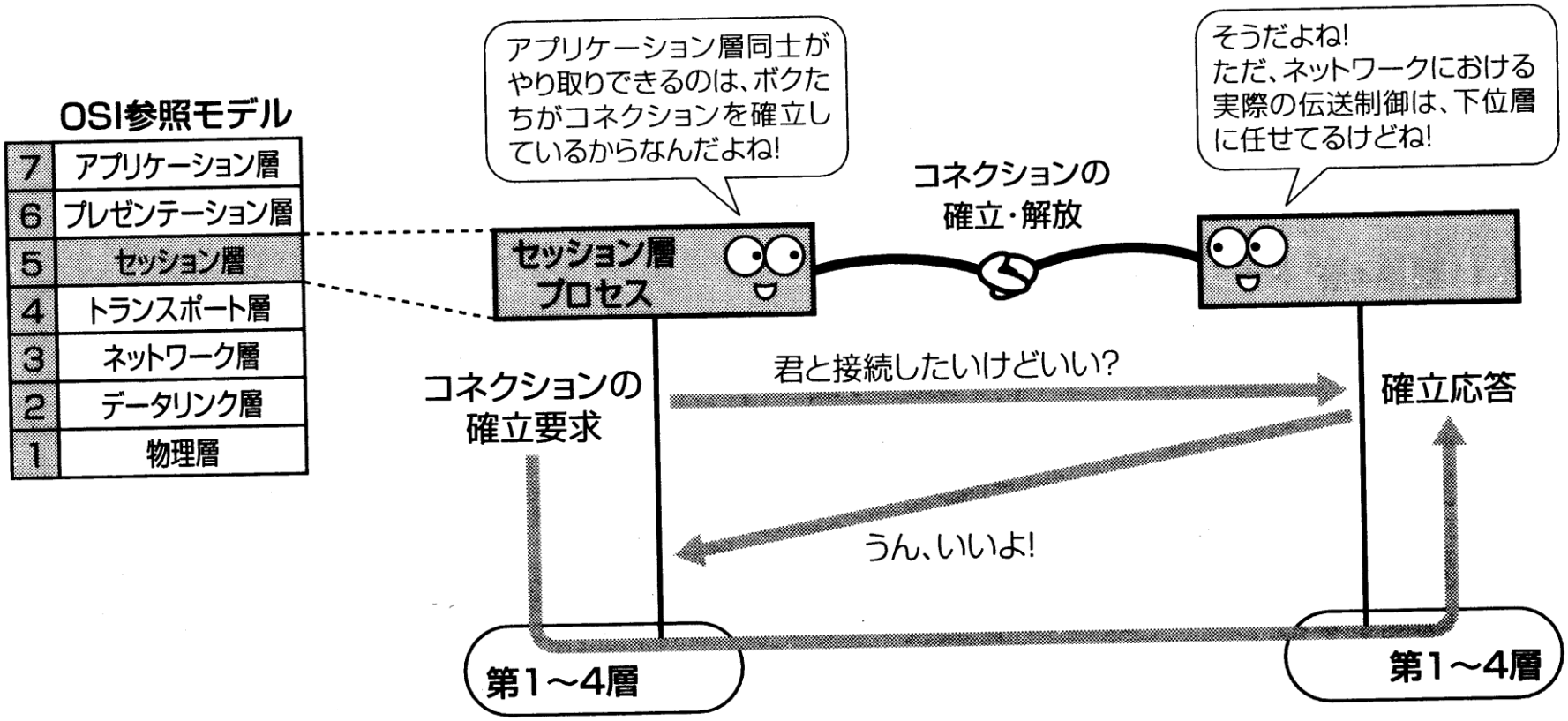
アプリケーション層（第7層）



プレゼンテーション層（第6層）



セッション層（第5層）

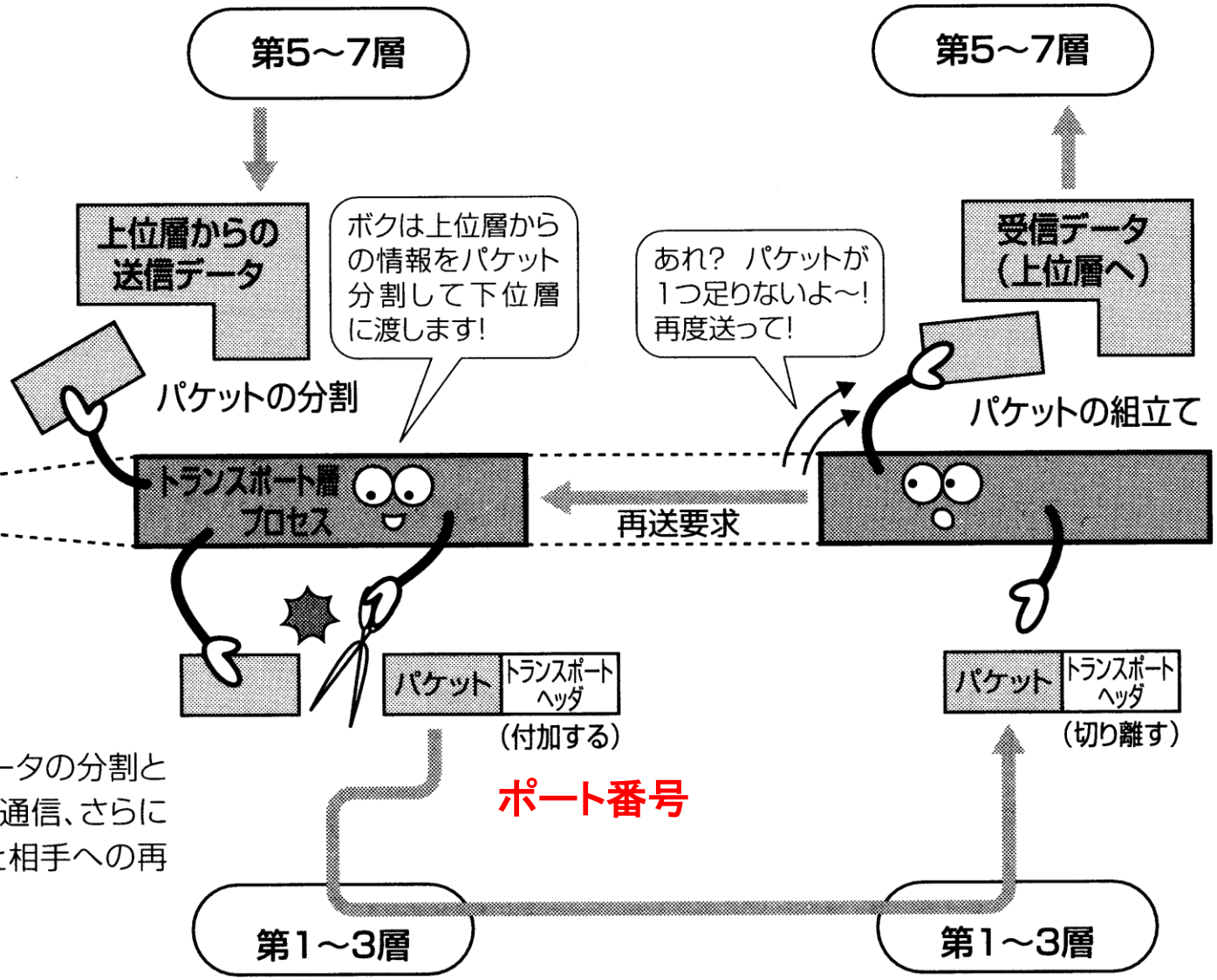

OSI参照モデル
7 アプリケーション層
6 プレゼンテーション層
5 セッション層
4 トランスポート層
3 ネットワーク層
2 データリンク層
1 物理層
アプリケーション層同士がやり取りできるのは、ボクたちがコネクションを確立しているからなんだよね!
そうだよね!
ただ、ネットワークにおける実際の伝送制御は、下位層に任せてるけどね!
セッション層プロセス
コネクションの確立・解放
コネクションの確立要求
君と接続したいけどいい?
確立応答
うん、いいよ!
第1～4層
第1～4層

トランスポート層（第4層）

TCP/UDP

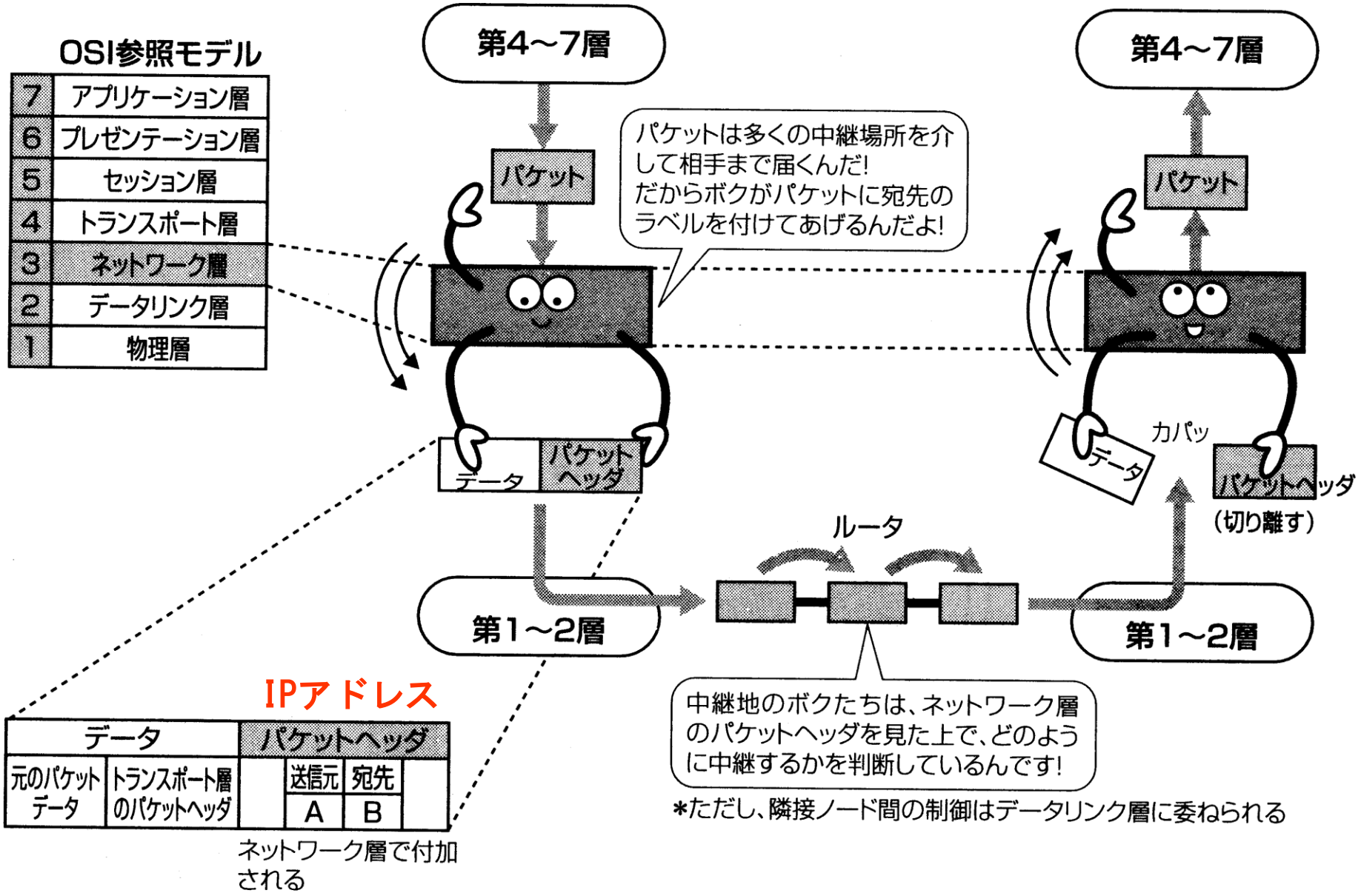
OSI参照モデル

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

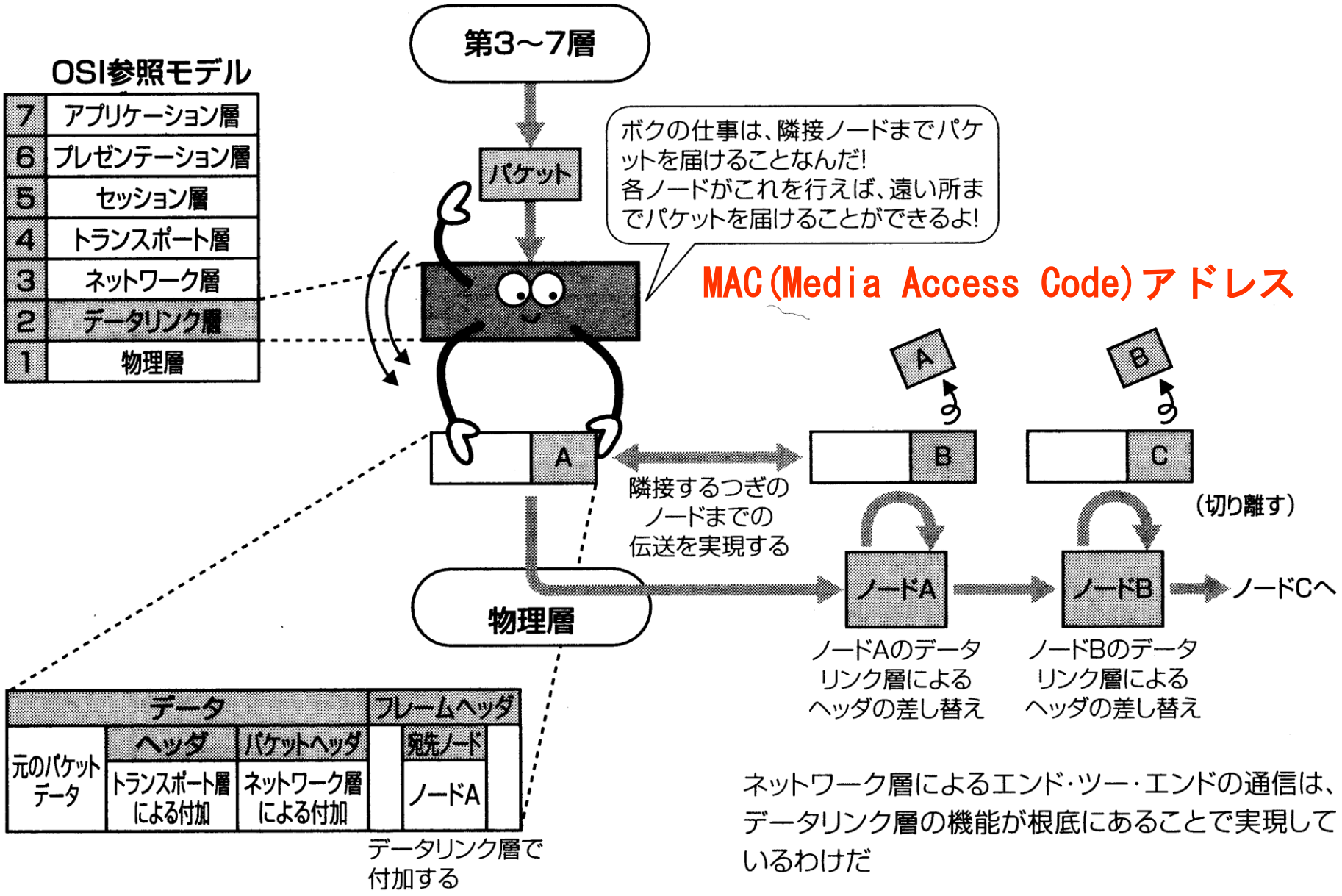


トランスポート層では、データの分割と組立て、パケット単位での通信、さらにはパケットの欠如の監視と相手への再送要求などを行う

ネットワーク層（第3層）

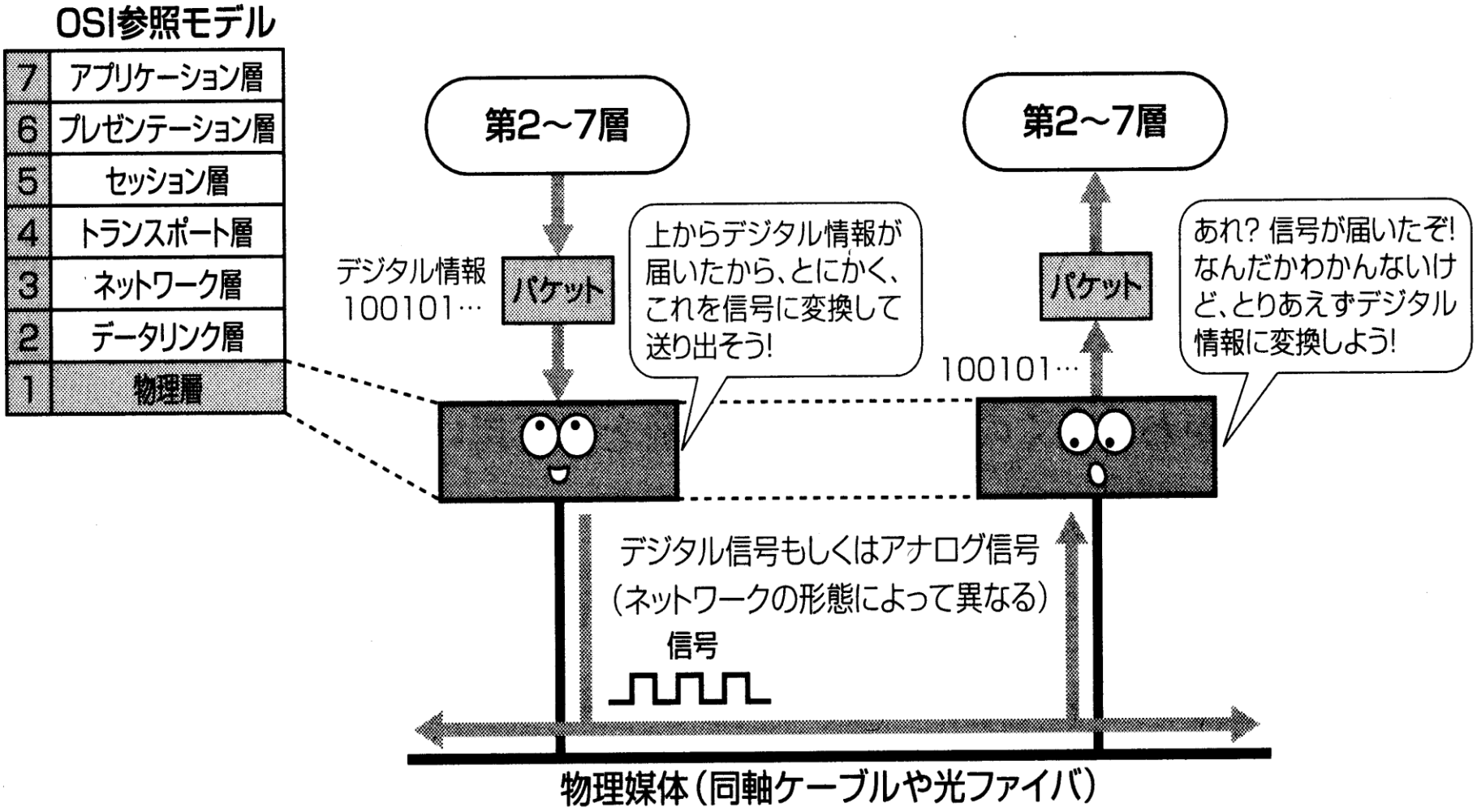

OSI参照モデル
7 アプリケーション層
6 プレゼンテーション層
5 セッション層
4 トランスポート層
3 ネットワーク層
2 データリンク層
1 物理層
第4～7層
パケット
パケットは多くの中継場所を介して相手まで届くんだ!
だからボクがパケットに宛先のラベルを付けてあげるんだよ!
データ
パケットヘッダ
第1～2層
ルータ
第4～7層
パケット
カパッ
データ
パケットヘッダ
（切り離す）
第1～2層
中継地のボクたちは、ネットワーク層のパケットヘッダを見た上で、どのように中継するかを判断しているんです!
*ただし、隣接ノード間の制御はデータリンク層に委ねられる
IPアドレス
データ
パケットヘッダ
元のパケットデータ
トランスポート層のパケットヘッダ
送信元
A
宛先
B
ネットワーク層で付加される

データリンク層(第2層)



ネットワーク層によるエンド・ツー・エンドの通信は、データリンク層の機能が根底にあることで実現しているわけだ

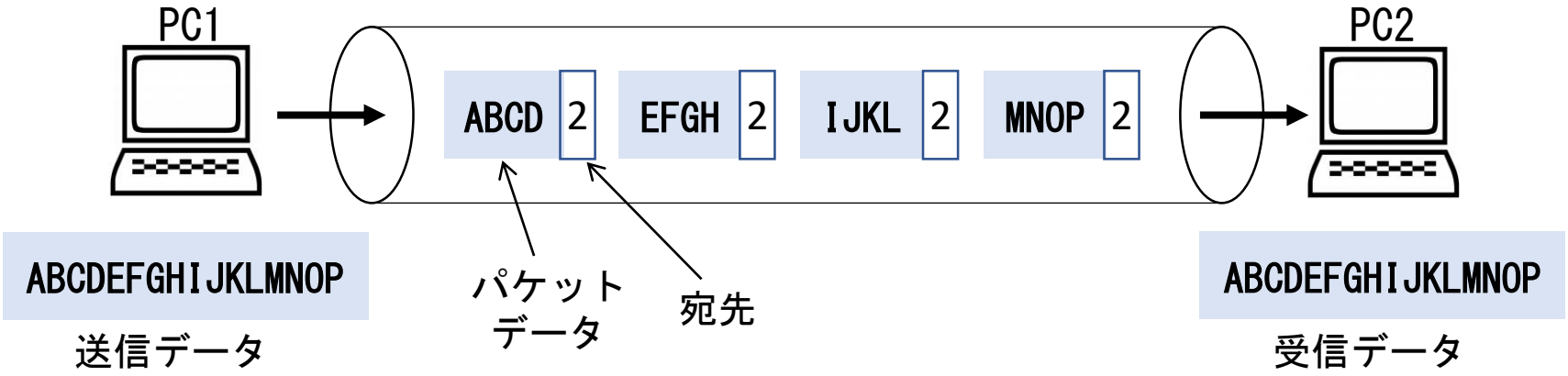
物理層（第１層）


OSI参照モデル
7 アプリケーション層
6 プレゼンテーション層
5 セッション層
4 トランスポート層
3 ネットワーク層
2 データリンク層
1 物理層
第2～7層
第2～7層
デジタル情報
100101…
パケット
パケット
上からデジタル情報が届いたから、とにかく、これを信号に変換して送り出そう!
100101…
あれ? 信号が届いたぞ! なんだかわかんないけど、とりあえずデジタル情報に変換しよう!
デジタル信号もしくはアナログ信号
（ネットワークの形態によって異なる）
信号
物理媒体（同軸ケーブルや光ファイバ）

パケット交換方式

ノード(通信機器のこと、例えば、コンピュータ）同士を接続してデータ通信するには、データをパケットと呼ぶ単位に区切り、このパケットに宛先を添付して送信する。こうした通信のやり方を、パケット交換(または通信)方式と呼ぶ

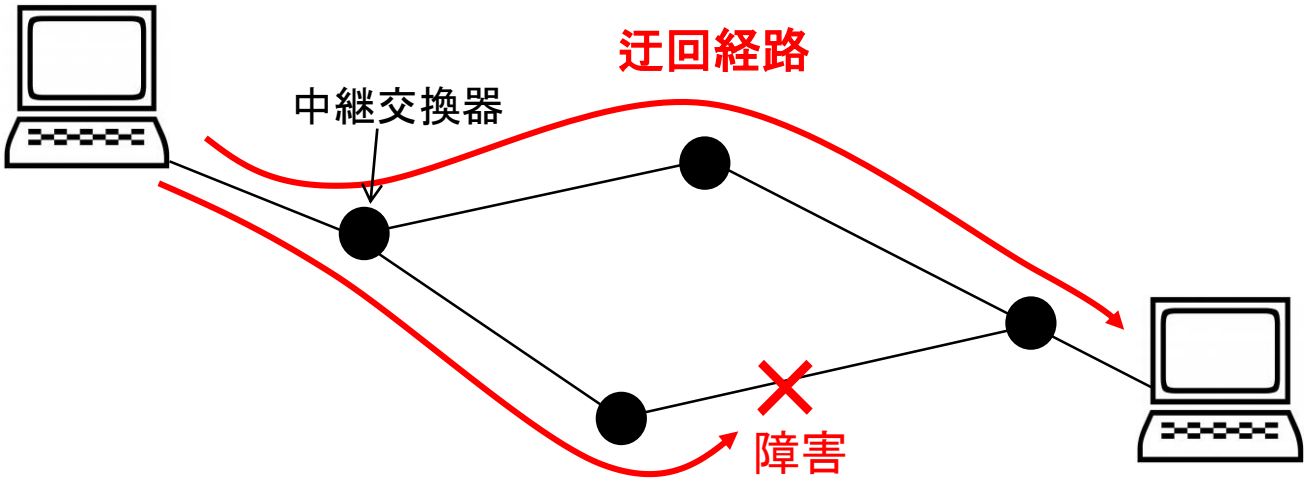
実装規定：ITU-T勧告x.25



パケット交換方式の特徴

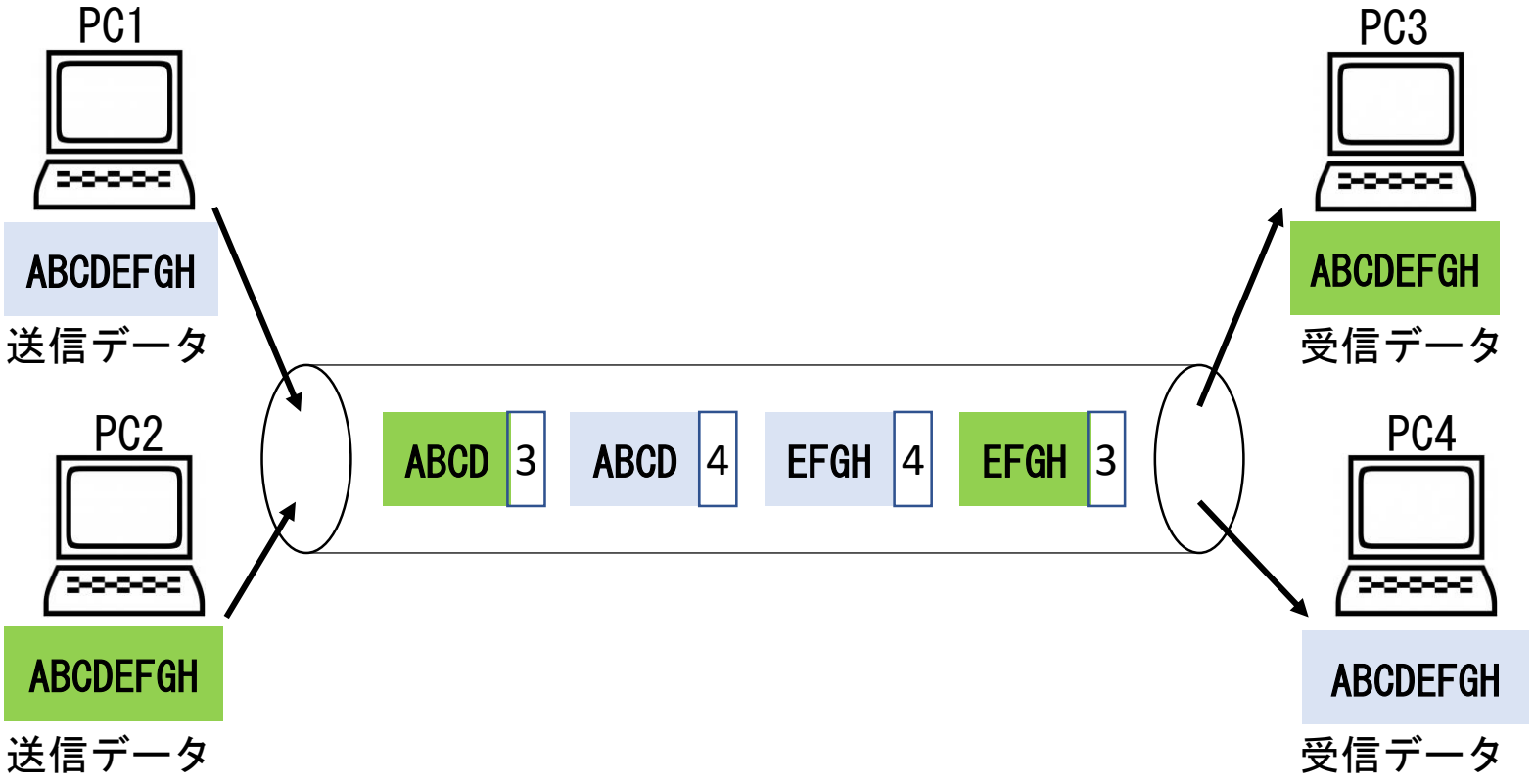
- **耐障害性**

　パケット通信では、通信相手までのパケットを送る経路(通信経路)が固定でないので、通信路に障害が起こっても、迂回経路をとることができる



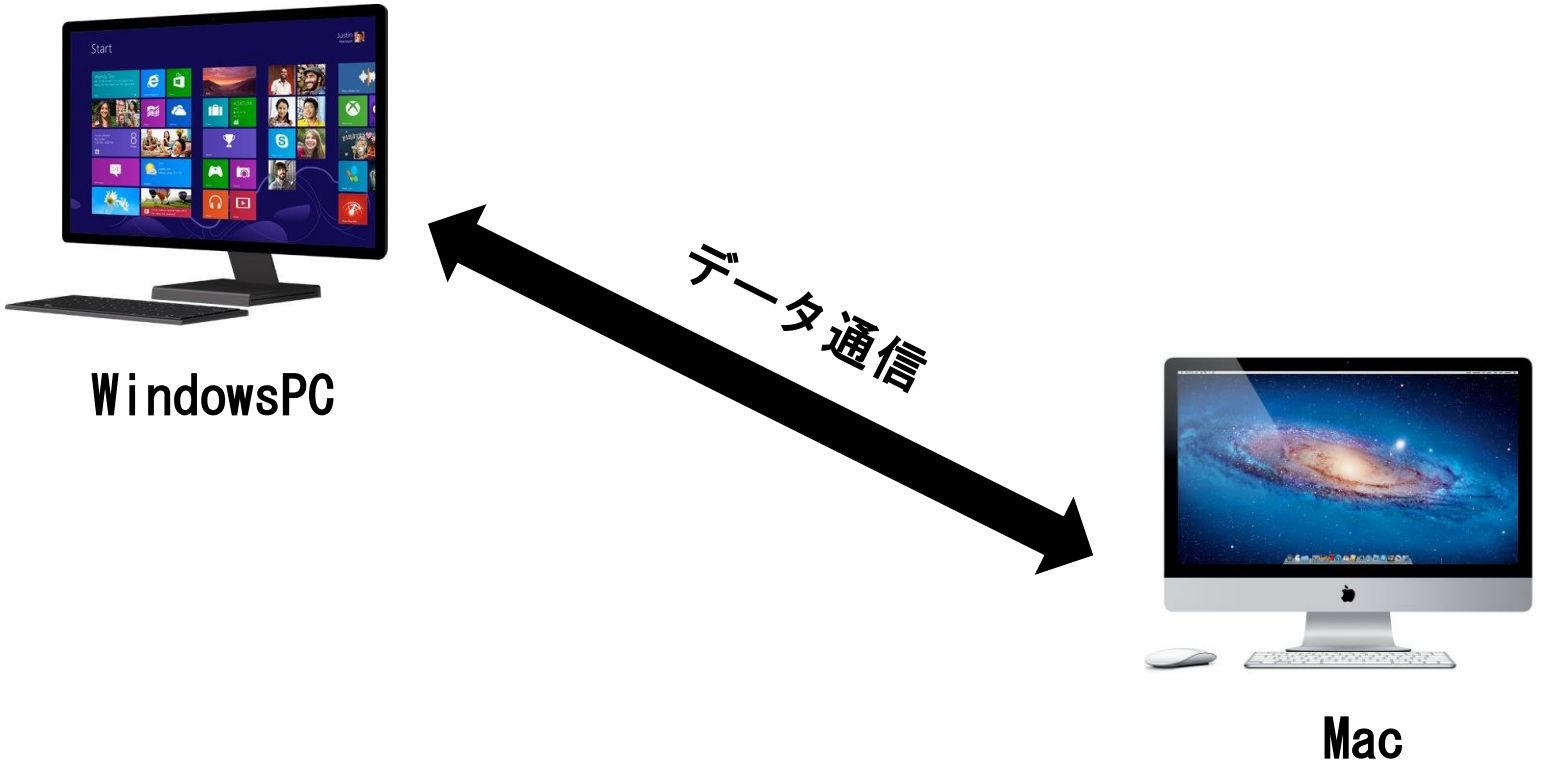
- **パケットの多重化**

1本の回線(通信ケーブルが1本)で複数のパケットを送ることができるので、回線の使用効率が高い。



- **異機種間の接続性**

　ノード同士が、異なるOSやハードウェア(例えば、WindowsとMac)でも、支障なく通信することができる



コネクション型通信とコネクションレス型通信

ノード間の接続方式は、2種類ある

コネクション型通信

実際にデータを送る前に、送信ノードと受信ノードの間で通信路が固定される接続方式を、コネクション型通信と呼ぶ。

データ通信を行う際には、ネットワーク上での相手の所在や通信経路を探し出し、通信を行っても良いか問い合わせる等の準備が必要となるが、データを送出するたびにこのような手順を踏むのは煩雑で無駄が多いため、相手が通信可能になった段階で仮想的な独占通信路を確保して、簡易な手順でデータの送受信ができるようする。安定した信頼性の高い通信が可能。

コネクションレス型通信

実際にデータを送る前に、通信ノードの確認や通信路の確保などを行わず、一方的にデータを送信する接続方式。

信頼性が低くデータが確実に届くかどうかは通信経路や通信相手の状況に依存するが、確認のやり取りなどが無いぶん、制御が簡単で通信速度を向上させやすく、通信経路の状況が悪くても、とりあえず送信してみるという使い方ができる。

TCP/IP

(Transmission Control Protocol/Internet Protocol)

テキストP254-258

IPとTCP/IPプロトコルスイート

IPのプロトコルを使用することを前提としたプロトコル(群)を、TCP/IPプロトコルスイートと呼ぶ

OSI基本参照モデル	TCP/IP	実装例
アプリケーション層	アプリケーション層	HTTP, SMTP, FTP, DHCP DNS, SNMP, POP, Telnet
プレゼンテーション層		
セッション層		
トランスポート層	トランスポート層	TCP, UDP
ネットワーク層	インターネット層	IP, ICMP, ARP, RARP
データリンク層	ネットワーク インタフェース層	イーサネット
物理層		

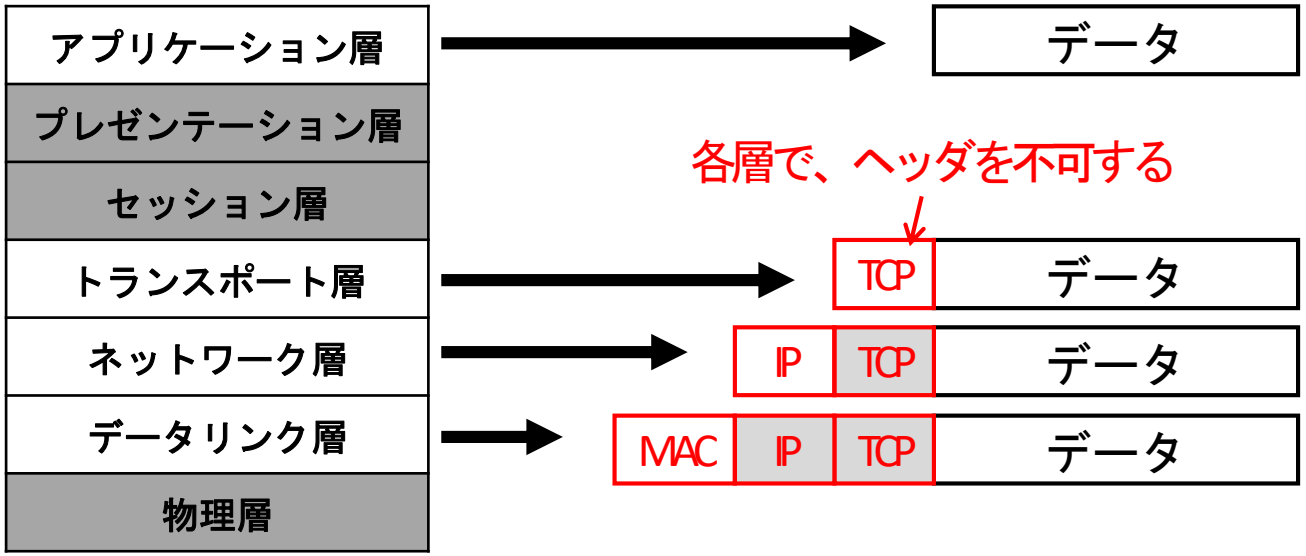
IP(通信)の特徴

① パケット通信技術
② ベストエフォート(最大限努力)型のコネクションレス型通信である
③ 経路制御を行う

IPを使って信頼性のある通信を行うには、IPで行うのではなく、別の技術(アプリケーション層のプロトコルなど)を使って行う

IPヘッダ

パケットの中には、実際に送りたい内容（データ）の他に、パケットの宛先（受信先）や送信元、大きさなどのパケット自身の情報を付加する。この不可情報を、ヘッダと呼ぶ。



ネットワーク層で付加するIPヘッダには、送信元IPアドレスと受信元IPアドレスを挿入する

IPバージョン6(IPv6)

現行のIPv4の枯渇問題に対応するために、アドレス空間の拡張などを目的として、IPv6が利用され始めている

アドレス空間の拡張

	ビット数	アドレス空間
IPv4	32bit	2^{32} =約43億個
IPv6	128bit	2^{128} =約43億個の4乗

表記方法(16進表示)

FFFF:FFFF:0000:0000:0000:0000:0000:FFFF

⬇ ゼロ(0)は短縮できる

FFFF:FFFF:0:0:0:0:0:FFFF

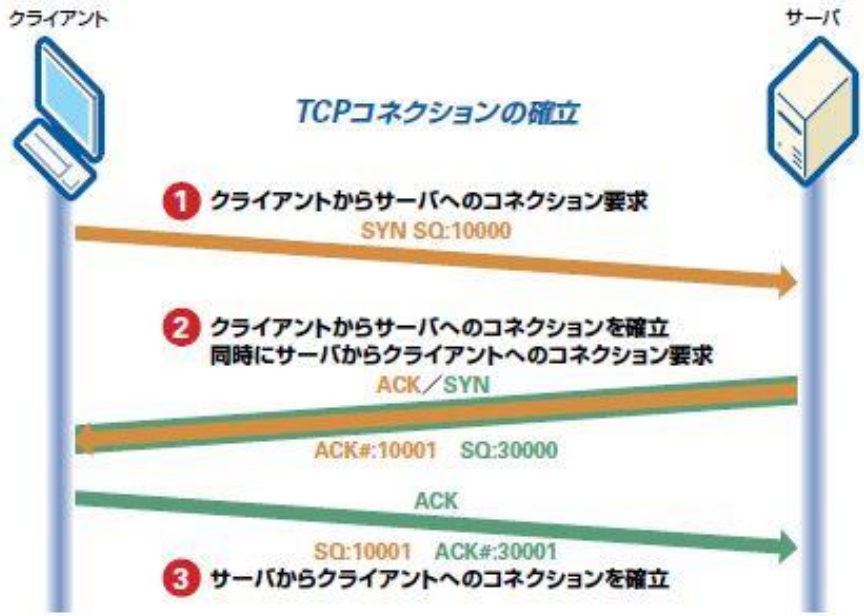
⬇ ゼロ(0)が連続する場合は::で表記できる

FFFF:FFFF::FFFF

TCP

IPを使った通信の不完全性を補う送達管理(相手にパケットが届いたか)や伝送管理(パケットを送る途中で、パケットがなくならないか)の機能を追加したプロトコル

コネクションの確立



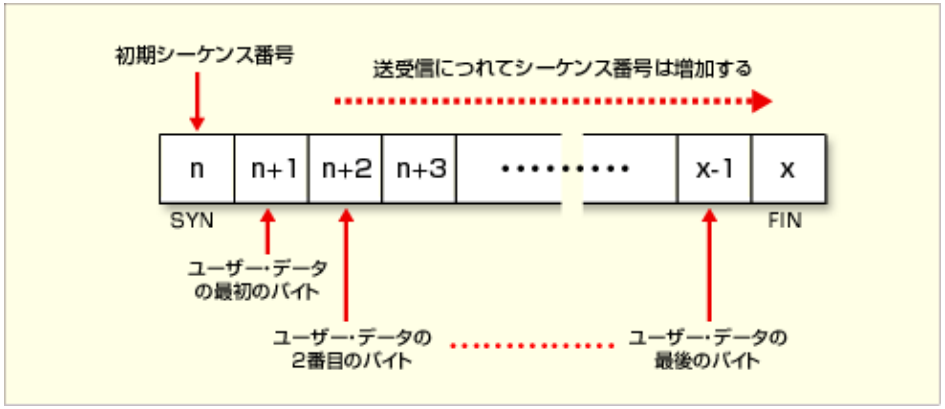
クライアント側から接続要求を意味するSYNパケットを送り、サーバ側は接続許可を意味するACKパケットと接続要求のSYNパケットを組み合わせたパケットを送る。最後に、クライアント側からもACKパケットを送り、コネクションが確立する。これを、3ウェイハンドシェイクと呼ぶ。

TCPヘッダフォーマット

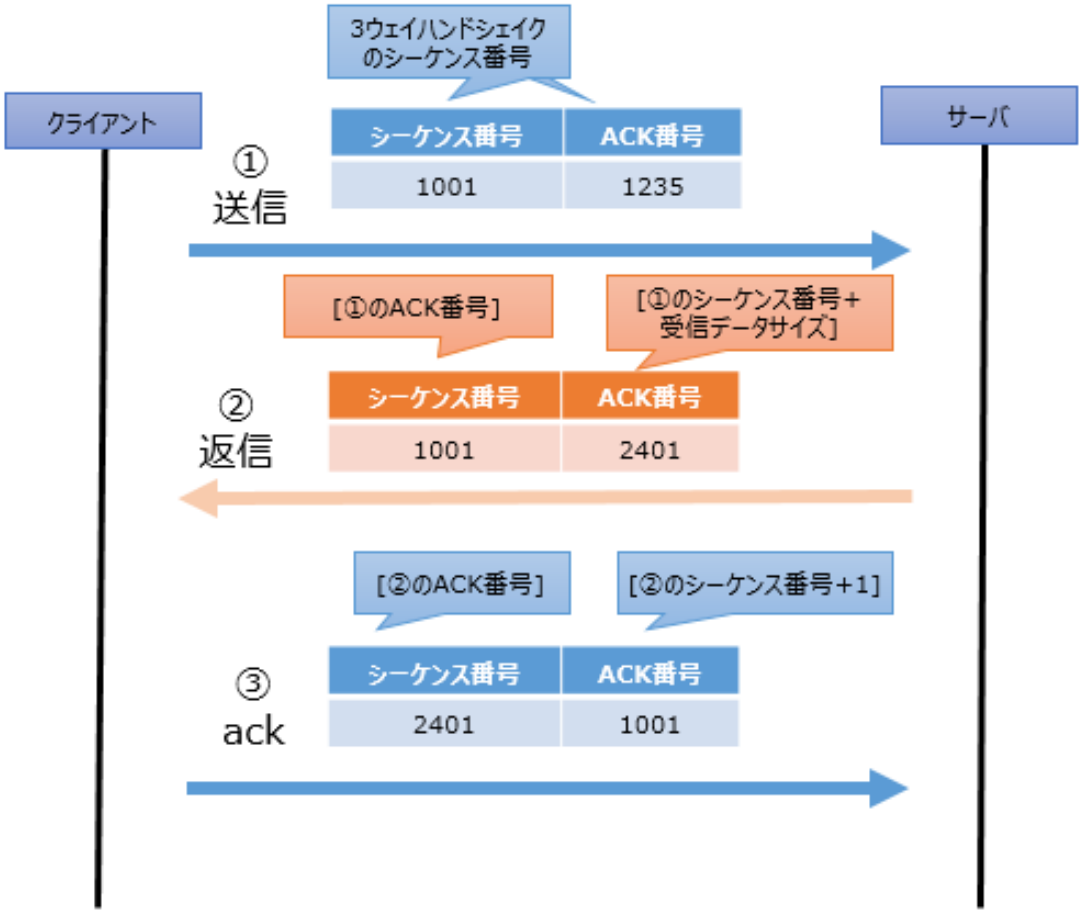
TCPはフロー制御(受信側の処理が追いつかずにデータを取りこぼしたりするのを防ぐため、通信状況に応じて送信停止や速度制限などの調整を行う)などを行うための情報を、TCPヘッダに保存している

- シーケンス番号

TCPで送信されるパケットに付けられる通し番号。受信側では、シーケンス番号を参照することによりパケットの正しい順番や通信途上でのパケットの欠落を知ることができる。

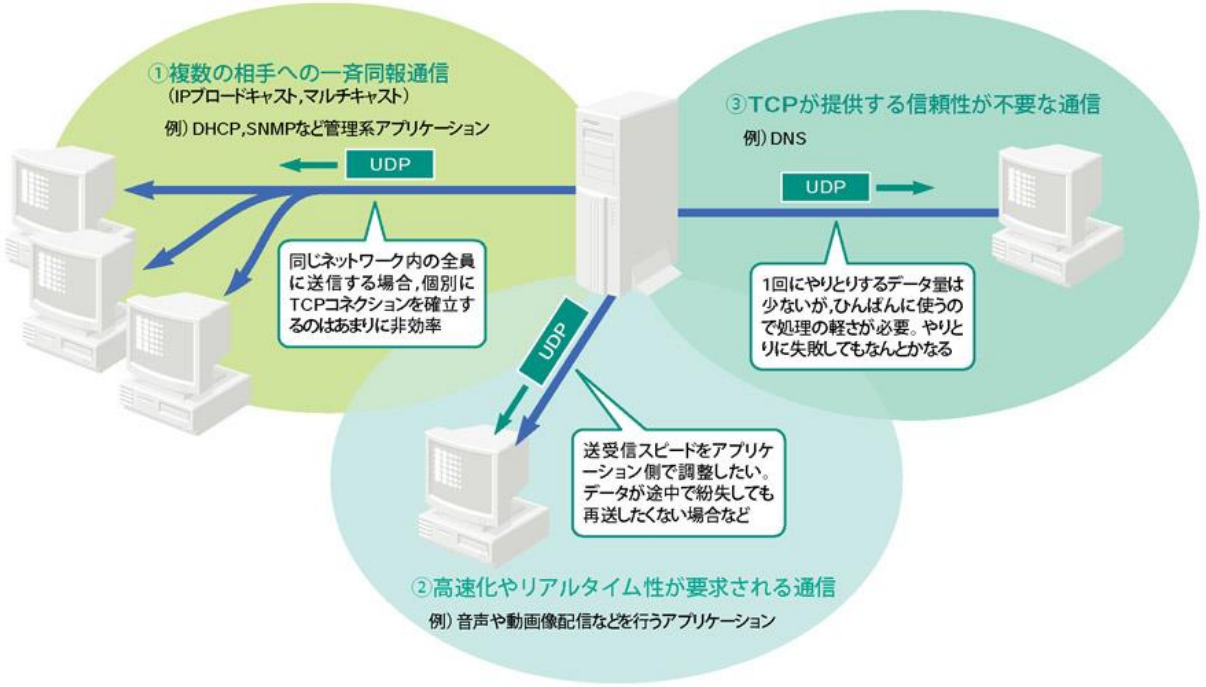


- ACK番号
　データを受信した際のACK(応答)時に利用する番号で、次に受信すべきシーケンス番号が入る



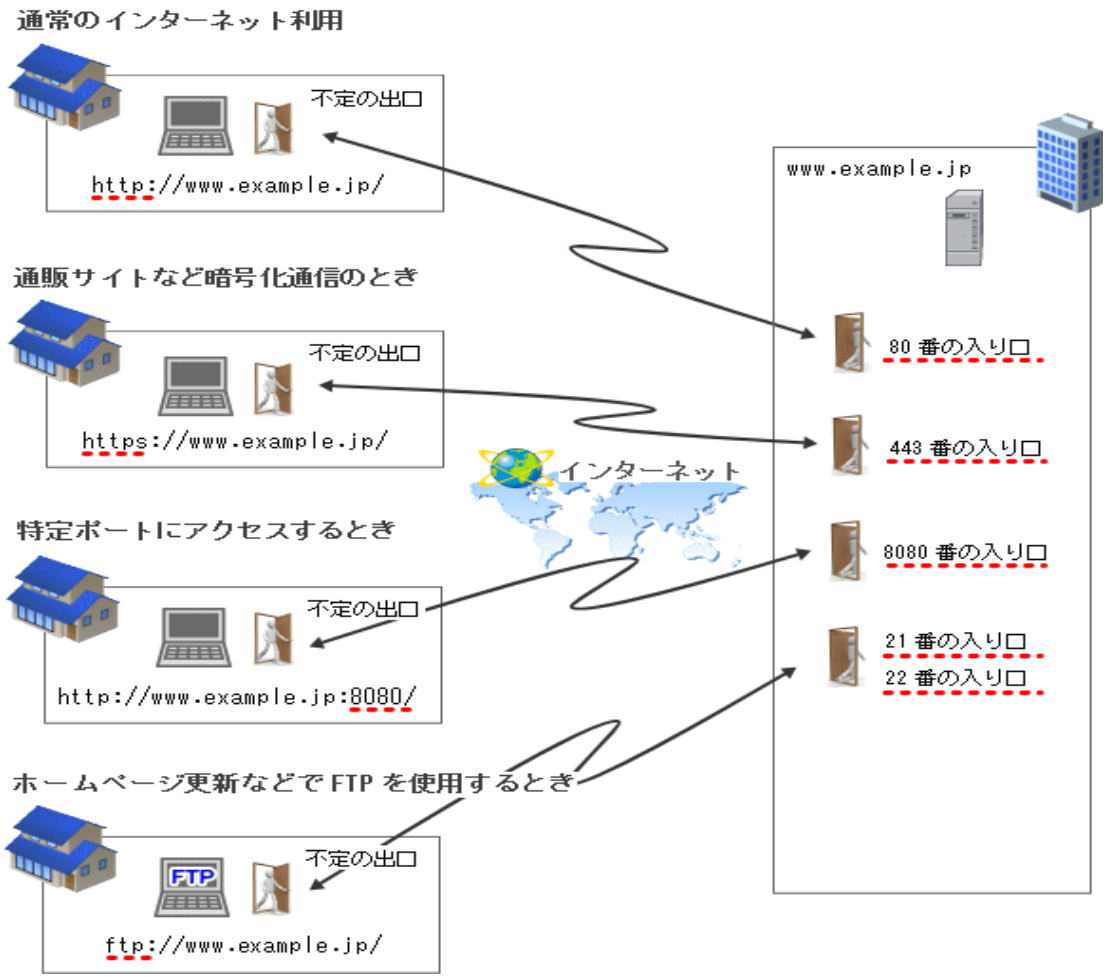
UDP(User Datagram Protocol)

コネクションレス型のプロトコルで、通信相手が確実にデータを受け取ったかどうか確認したり、データの欠落を検知して再送したり、送信順と着信順を一致させるといった制御を行わず、データを「送りっぱなし」にする。信頼性は低いが転送効率が高く、遅延が発生しにくいため、多少のデータの欠落があっても高速性や即時性(リアルタイム性)を重視する用途(通話、放送など)で、よく利用される



トランスポート層のプロトコルとポート番号

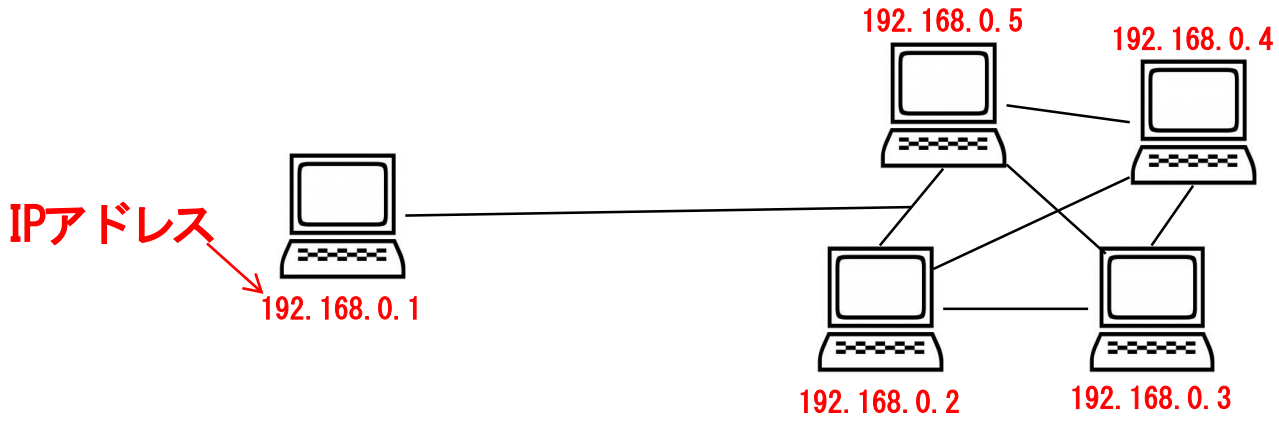
TCPとUDPでは、ヘッダに通信相手が提供しているサービス(メールサービスやWebサービスなど)を特定(認識)する番号(ポート番号)が入っている



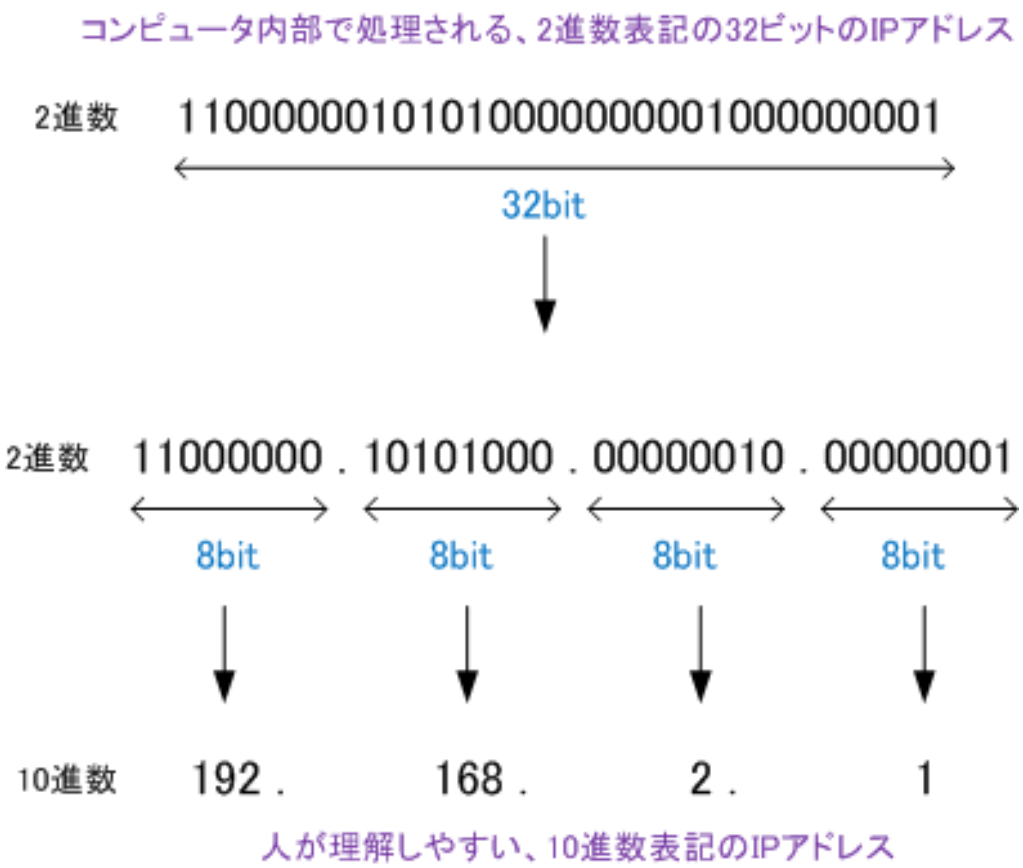
IPアドレス
(Internet Protocol address)
テキストP259-262

IPアドレス

IPネットワーク(インターネットやイントラネット)に接続されたコンピュータや通信機器1台1台に割り振られた識別番号。インターネット上では、この数値に重複があってはならないため、IPアドレスの割り当てなどの管理は各国のNIC(Network Information Center)が行っている。



IPアドレス(IPv4)は、32ビットで表現するが、人間が分かりやすいように、8ビット毎(1オクテット)に10進数で表記する

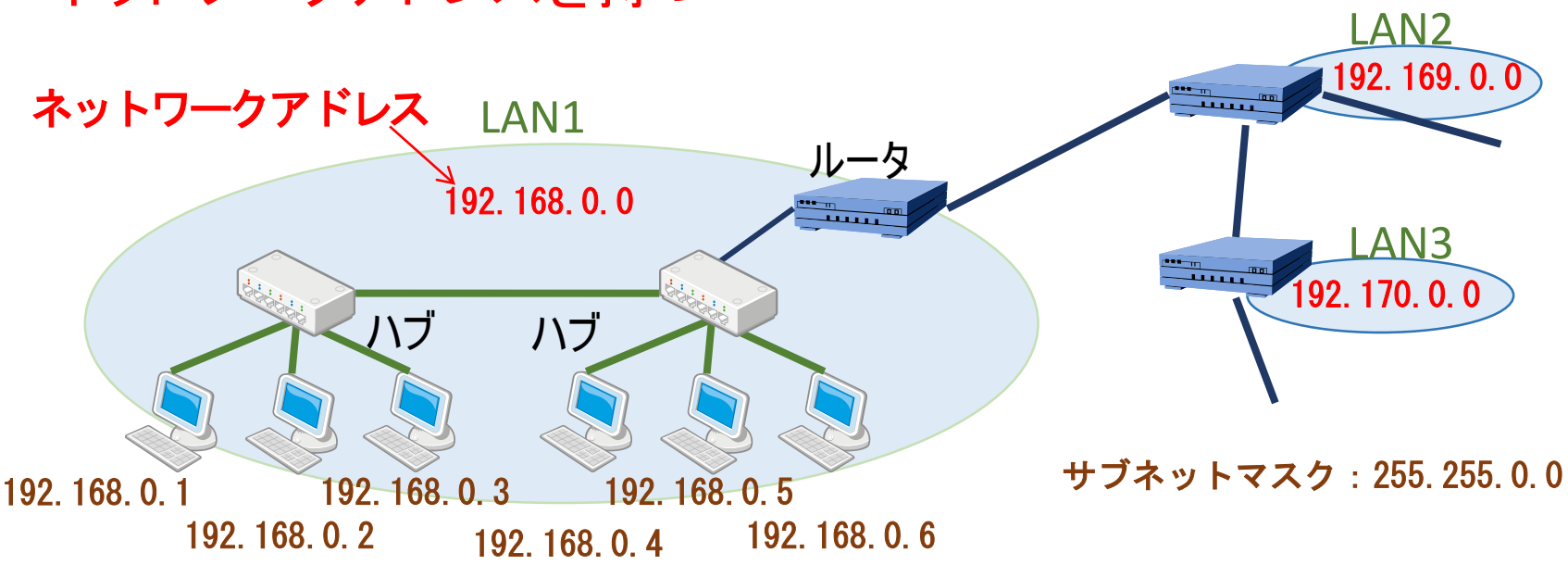


ネットワークアドレスとホストアドレス

IPアドレスは、ネットワークアドレスとホストアドレスに分かれる。この境目を決定するには、サブネットマスクが用いられる。

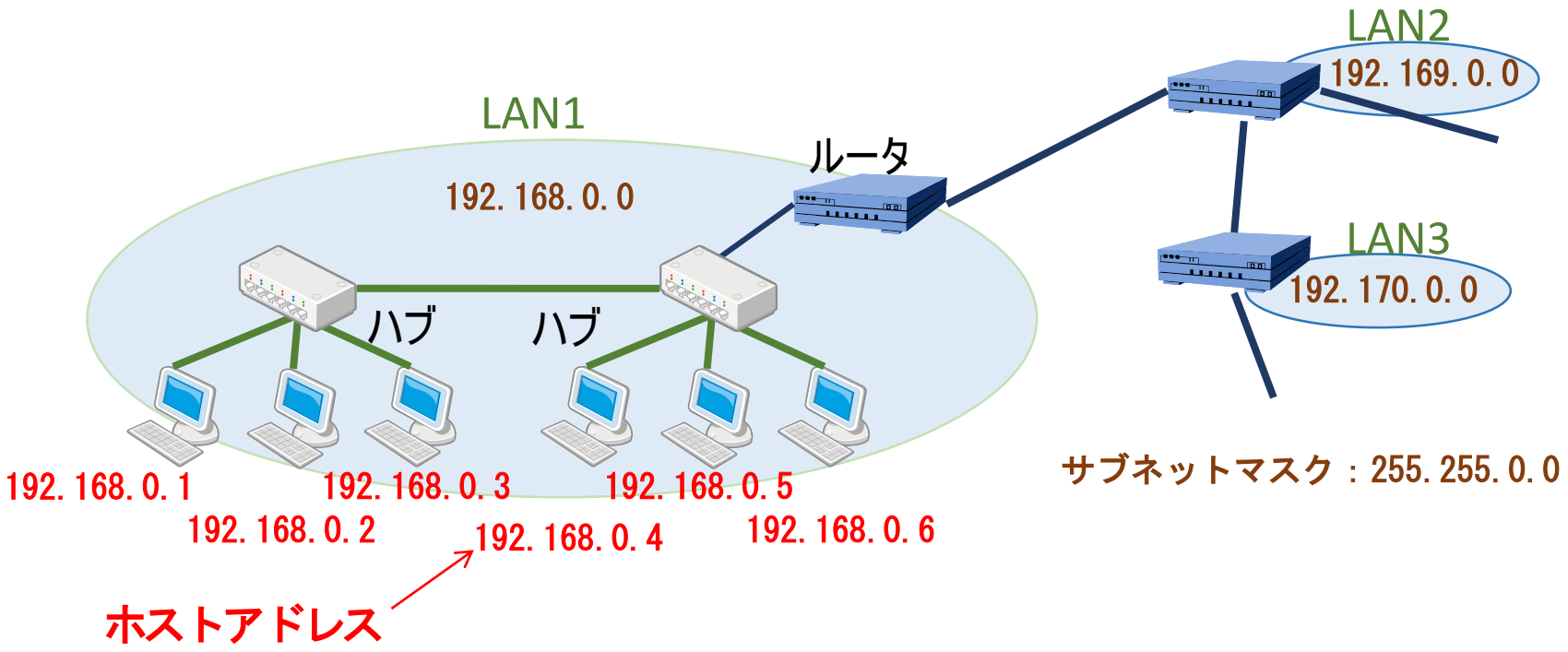
- ネットワークアドレス

  IPアドレスの割当機関によって、ネットワークごとに割り当てられるアドレスで、同じネットワークに属する端末は、全て同じネットワークアドレスを持つ



- ホストアドレス

ネットワーク管理者が、ネットワーク内で重複しないように割り当て、ネットワーク内でコンピュータごとに割り当てられる



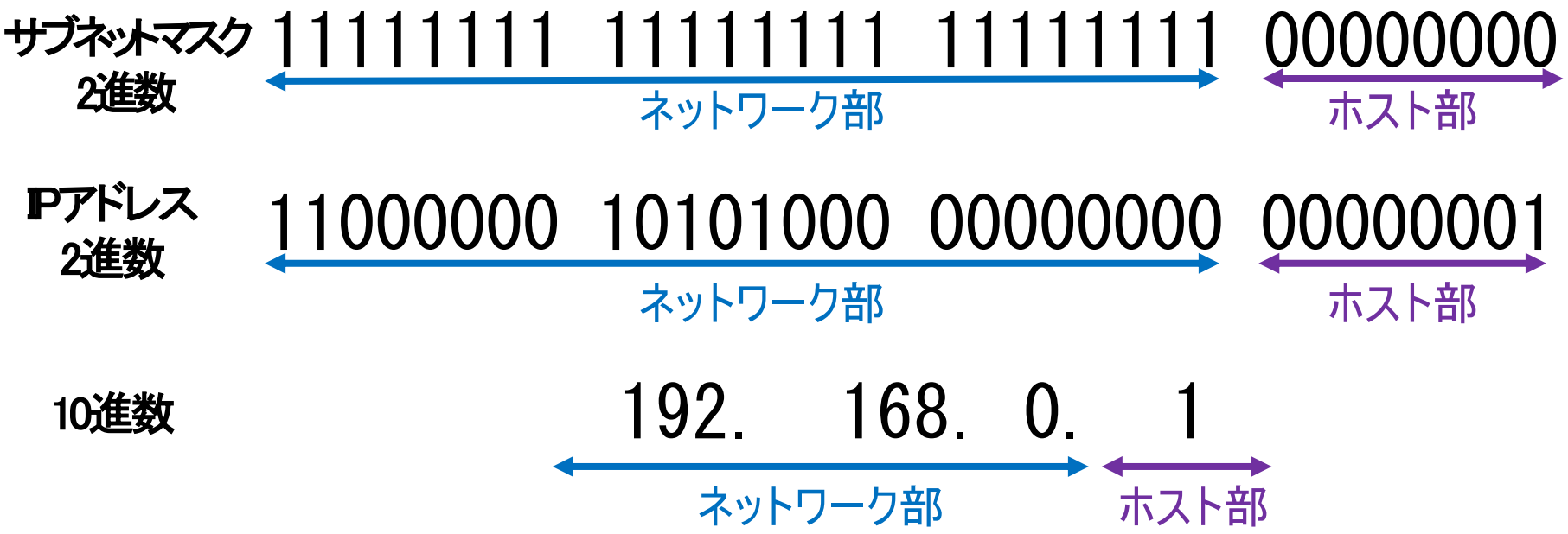
例）ネットワーク部が24bit、ホスト部が8bitの場合

2進数

10進数

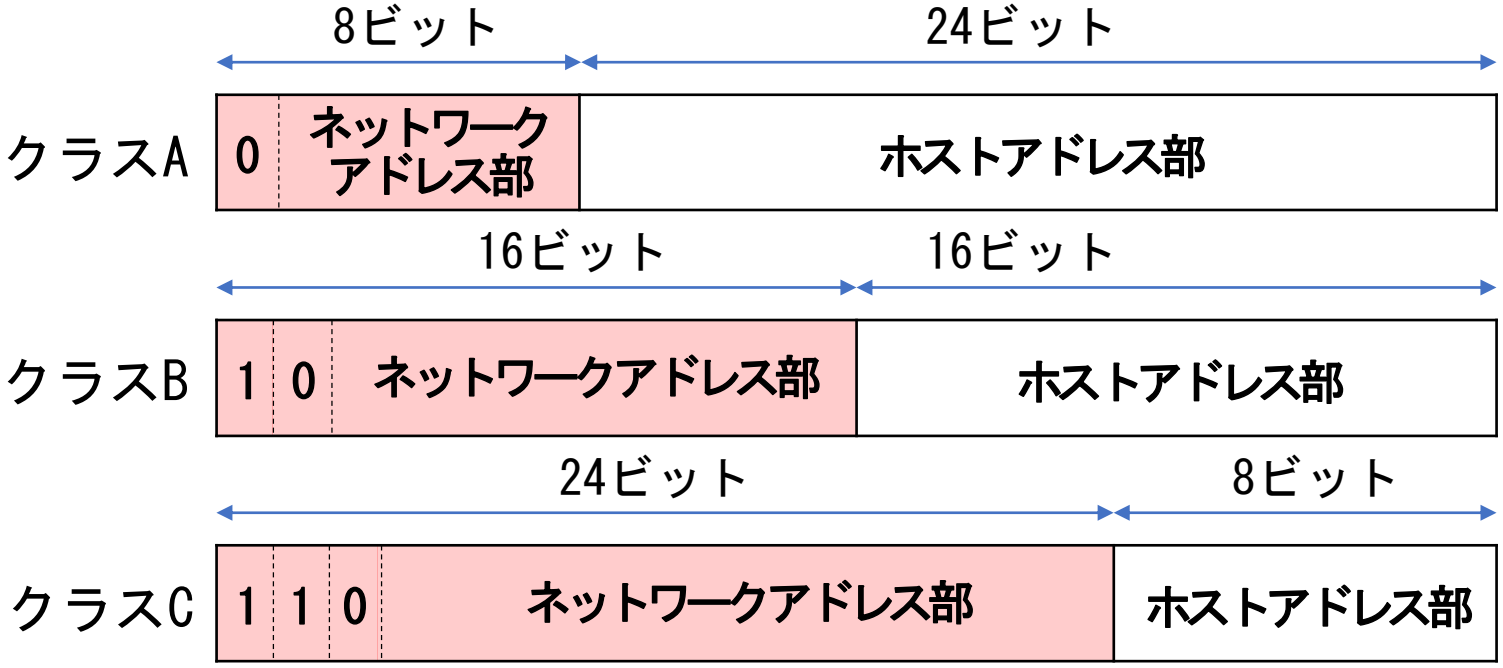
- サブネットマスク
  サブネットマスクを使って、ネットワーク部とホスト部に割り当てるビット数を変えることができる（区切り位置を示すための32ビットのビット列）

  ✓ ネットワーク部に対応する部分を「0」で表す
  ✓ ホスト部に対応する部分を「1」で表す

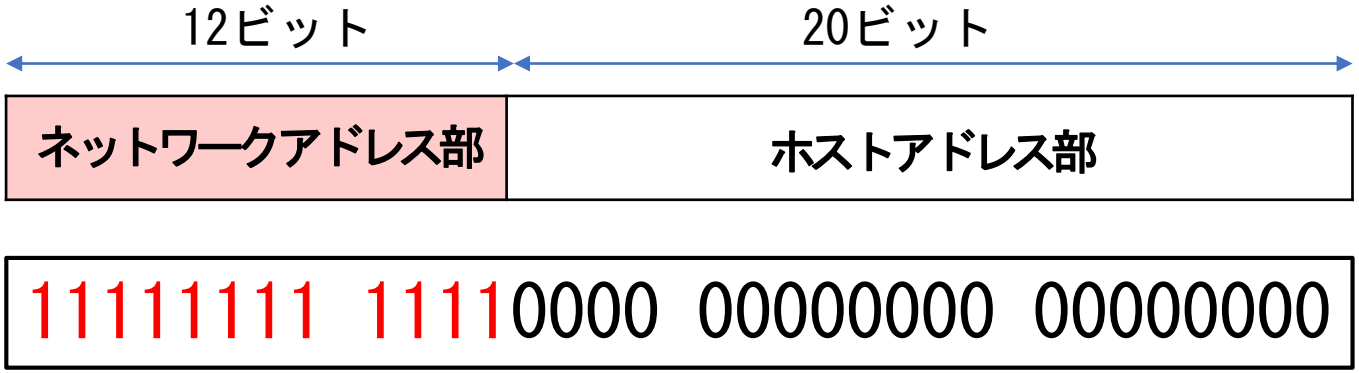


IPアドレスクラス

- クラスフル
  IPアドレスの初期割り当て方法で、先頭の1～3ビットのビットパターンでクラスA～Cに分ける



- クラスレス
　現在行っているIPアドレス割り当て方法で、8ビット毎のオクテットの途中であっても、ネットワーク部とホスト部の境目を指定する



プライベートIPアドレスとグローバルIPアドレス

- グローバルIPアドレス

  インターネットで（直接）使用するアドレス
  （JPNICによって一元管理）

  ⇓ グローバルIPアドレスは有限

- プライベートIPアドレス

  インターネットで（直接）使用しないアドレス

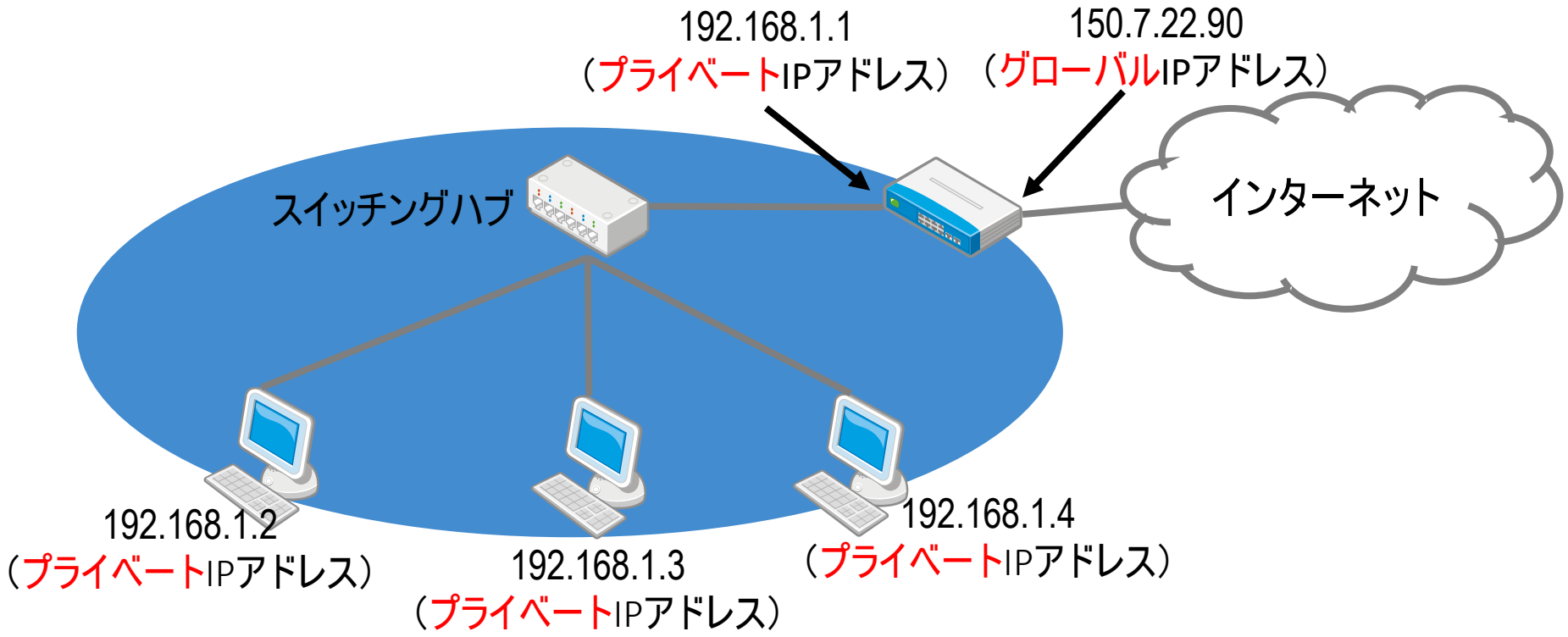
  このままではインターネットに接続できない

＜プライベートIPアドレスの例＞

10	.	0.	0.	0	～	10	.	255.	255.	255
172.	16.	0.	0	～	172.	31.	255.	255		
192.	168.	0.	0	～	192.	168.	255.	255		

- グローバルIPアドレスとプライベートIPアドレスの割り当て

グローバルIPアドレスの節約のため、ルータにはグローバルIPアドレスを、ホストにはプライベートIPアドレスを割り当てることが多い



MAC(Media Access Control)アドレス

物理アドレス

01:41:a6:08:80:80

メーカー番号　固有番号

- MACアドレスは6バイト(48bit)の長さであり、16進数で1バイトごとに :(コロン)で区切って表現する
- ユニークに(ダブらないように)しなければならない
- MACアドレスは(基本的には)変更できない
- ネットワーク機器(PCやネットワークインタフェースカードなど)の識別子として使用する

ポート番号

テキストP263-264

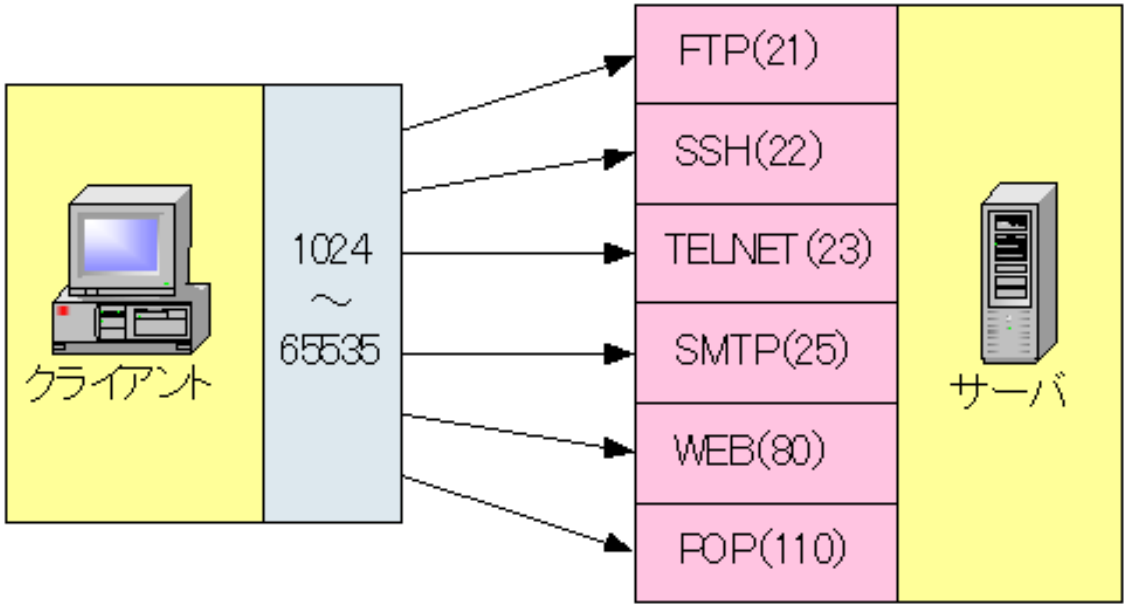
トランスポート層の役割

データ送信の品質や信頼性を向上するため、IPにない通信の品質管理を補完する。また、アプリケーション間の通信を実現(アプリケーション・サービスを識別)する。

ポート番号

ポート番号は、トランスポート層でアプリケーション・サービスの識別を行うための番号で、16ビットで表現されることから、0～65535の範囲になる。

TCPやUDPのヘッダ内に、送信元ポート番号と宛先ポート番号を挿入して、ノード間で通信相手のアプリケーション・サービスを識別する。



Well-Knownポート(番号):ウェルノウンポート

不特定多数の人が共有して利用するアプリケーション・サービスに対して、世界的に標準のポート番号を決めて利便性を上げる

サービス	ポート番号	説明
ftp-data	20	ftpでデータを転送する時に使う
ftp	21	ftpで接続する時等に使う
ssh	22	sshで使う
telnet	23	telnetで使う
smtp	25	メールを送る時に使う
domain	53	DNSでセカンダリにデータを送る時等に使う
http	80	Webサイトを参照する時に使う
pop3	110	パソコンがメールサーバーからメールを受信する時に使う
netbios-ns	137	Windowsが周辺のパソコンのIPアドレスを調べるために使う
netbios-ssn	139	Windowsが周辺のパソコンやプリンタと接続するために使う
imap	143	pop3の拡張版
submission	587	認証してメールを送信する時に使う
https	443	httpを暗号化して通信する
imaps	993	imapを暗号化して通信する
pop3s	995	pop3を暗号化して通信する