

コンピュータネットワーク

Rev. 2017.10.13

講義ホームページ

cvwww.ee.ous.ac.jp/lect/cn/



講義概要

- ❖ コンピュータネットワークは、近年急速に発展・普及し、社会の基盤として欠かせないものになっている。今後、IoT時代を迎えるにあたって、その重要性はますます高まっていく。
- ❖ 本講義では、今日のコンピュータネットワークで使われているOSI参照モデルを軸において、通信機器やネットワーク構造、プロトコル、セキュリティなどについて習得する。

講義内容

❖ コンピュータネットワークの構成

LAN、WAN、インターネット、VLAN、・・・
ネットワーク機器、伝送路、・・・

❖ ネットワーク通信の方法

TCP/IP、ルーティング、ドメイン管理、・・・
Web、電子メールの通信プロトコル、・・・

❖ ネットワークセキュリティ

ファイアウォール、DMZ、暗号化通信、・・・

コンピュータネットワークの役割

- ❖ 世界中に膨大な情報が存在している。
- ❖ コンピュータネットワークを利用すると、あらゆる情報を、瞬間的に、低コストで入手できる。
- ❖ コンピュータネットワークがさらに進歩すると、ネットワークの存在を意識しないで情報の入手ができるようになる。

身近にあるコンピュータネットワーク

- ✦ ホームネットワーク、SOHO
- ✦ 銀行のATM
- ✦ 有料道路のETC
- ✦ コンビニエンスストアのPOS
- ✦ カーナビゲーション、VICS

インターネットサービス

Webページ、検索エンジン、電子メール、
ファイル転送、ネットワークストレージ、
SNS、コミュニケーションサービス、
電子掲示板、電子書籍、音楽配信、
動画共有、リモート接続、IP電話、
電子商取引、クレジットカード決済

ネットワークの形態

♣ LAN

♣ WAN

♣ イン트라ネット

♣ インターネット

♣ IP-VPN網、広域イーサネット網

インターネットの始まり

❖ ARPANET

1969年 アメリカ国防総省によって研究開発が始まる。

最初は、カリフォルニア大学、ユタ大学などの4箇所のコンピュータを結ぶ。

パケット交換技術を使用

1983年 TCP/IP 通信方式を導入

1990年 学術利用から商用利用へ移行

インターネットの基礎となる

通信方式の種類

ネットワークの構造や働きによる分類

- ❖ ネットワーク トポロジー
- ❖ 回線交換方式、パケット交換方式
- ❖ コネクション型、コネクションレス型
- ❖ ユニキャスト、マルチキャスト、
ブロードキャスト

回線交換・パケット交換

❖ 回線交換

回線交換機が通信回線を切り替えて、2台のコンピュータを接続する。

通信が切れるまで、回線を占有する。

❖ パケット交換

データを細分化することで、1つの回線で複数のコンピュータのデータを送る。

コネクション型、コネクションレス型

❖ コネクション型

通信相手との接続を確認してから、データを送信する。

❖ コネクションレス型

通信相手がいるか確認しないで、データを送信する。

通信プロトコル

重要

通信手順やデータ構成を決めたもの

プロトコルの標準化によって、異なる機器同士でも通信が可能になる。

Web	HTTP
メール	SMTP, POP, IMAP
ファイル転送	FTP
時刻合わせ	NTP
遠隔操作	Telnet, SSH

ネットワーク機器

✦ リピータ

✦ ブリッジ

✦ ハブ

✦ スイッチングハブ

✦ ルータ

✦ ゲートウェイ

IPアドレスの基礎

ネットワークに接続された機器を区別するための固有番号

ネットワークアドレス部

ホストアドレス部

1	0	0	1	0	1	1	0	0	0	1	1	0	1	1	1	0	0	0	1	1	1	1	1	0	0	0	0	0	1	0	1
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

150 . 55 . 31 . 5

非営利法人ICANNとその下部組織IANAがIPアドレスを管理している。日本では、一般社団法人JPNICがIPアドレスの割り当てを行っている。

OSI参照モデル

ネットワーク通信の基本構造

通信に関する様々な仕組みを階層の形で分類している。

各層が独立しているため、新たな技術を導入するとき、一つの層の変更だけに留めることができる。

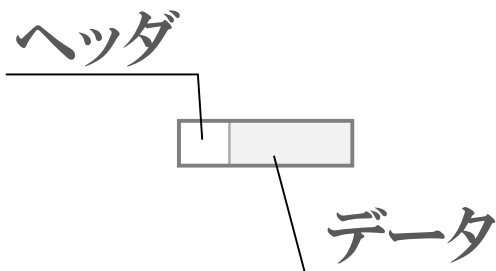
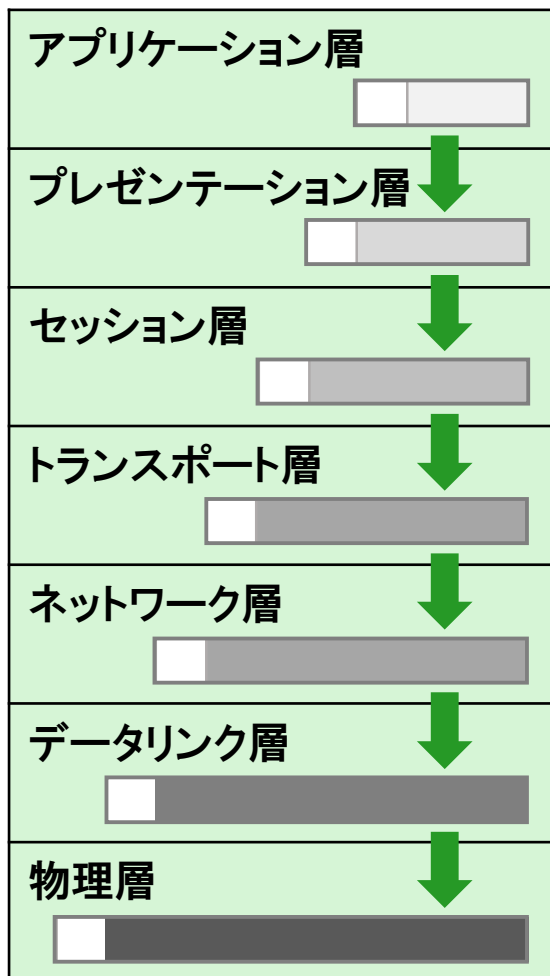
OSI参照モデル

重要

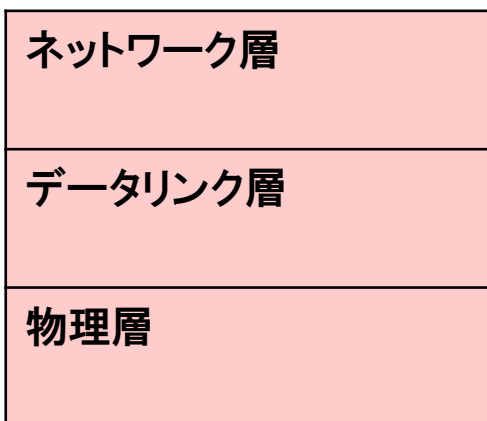
	名称	役割
第7層	アプリケーション層	アプリケーションごとのサービス提供 ※ Web, 電子メール など
第6層	プレゼンテーション層	データ形式の変換 ※ 文字コード、画像フォーマット、圧縮など
第5層	セッション層	コネクションの確立と切断
第4層	トランスポート層	通信の信頼性を提供 (宛先にデータを確実に送る)
第3層	ネットワーク層	アドレスの管理 通信経路の選択
第2層	データリンク層	直接接続された機器間でのデータ転送
第1層	物理層	コネクタやケーブルの形状の規定 電気的な信号変換

OSI参照モデルによる送受信

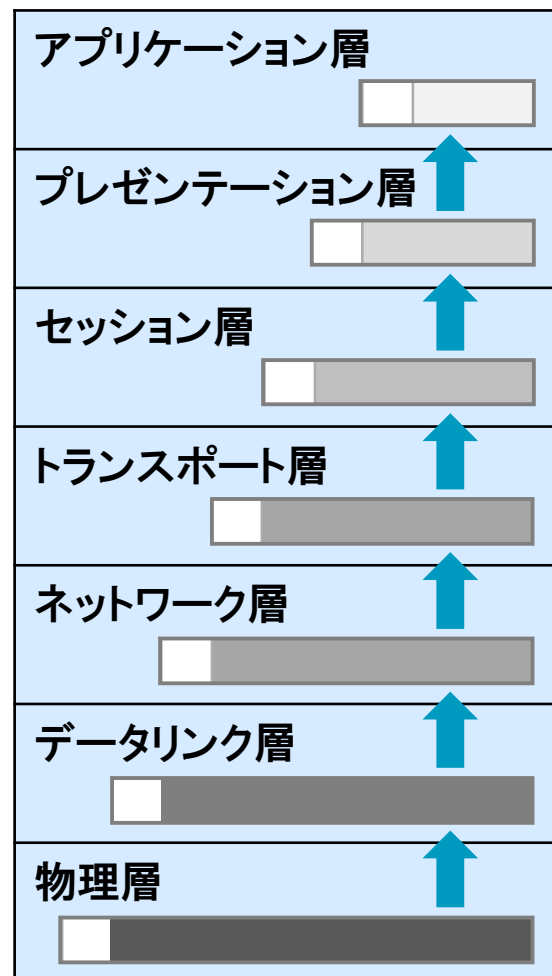
送信側A



ルータB

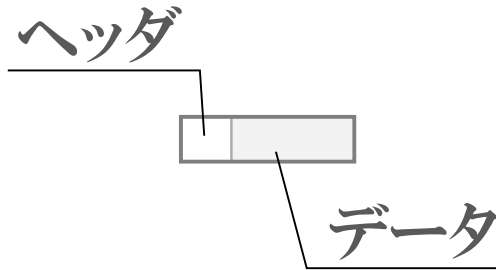
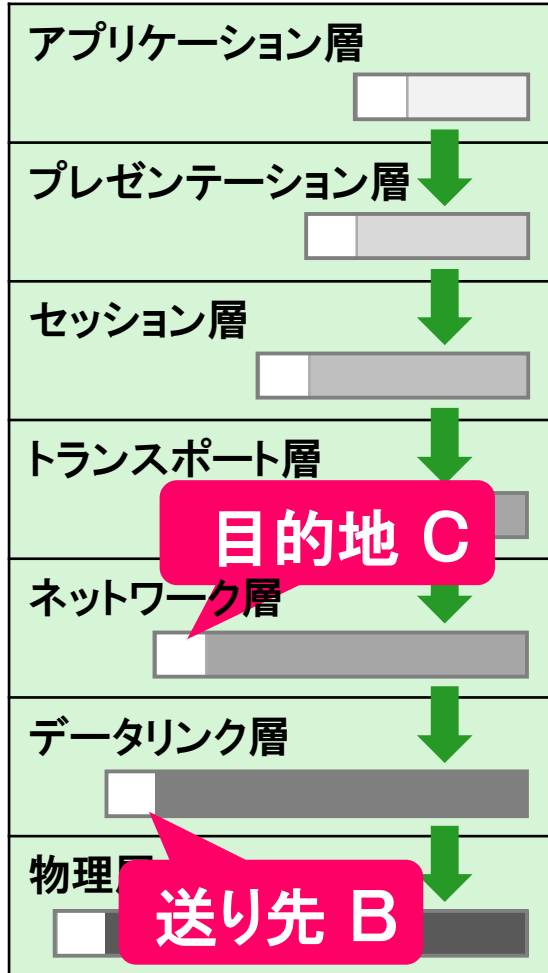


受信側C

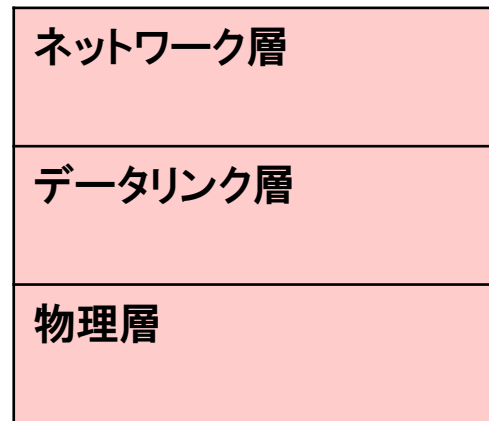


OSI参照モデルによる送受信

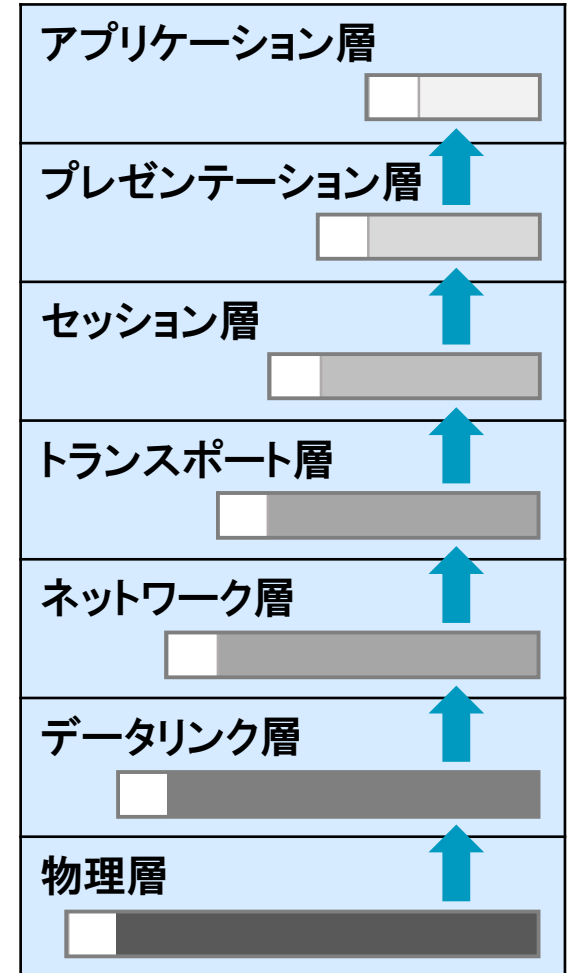
送信側A



ルータB

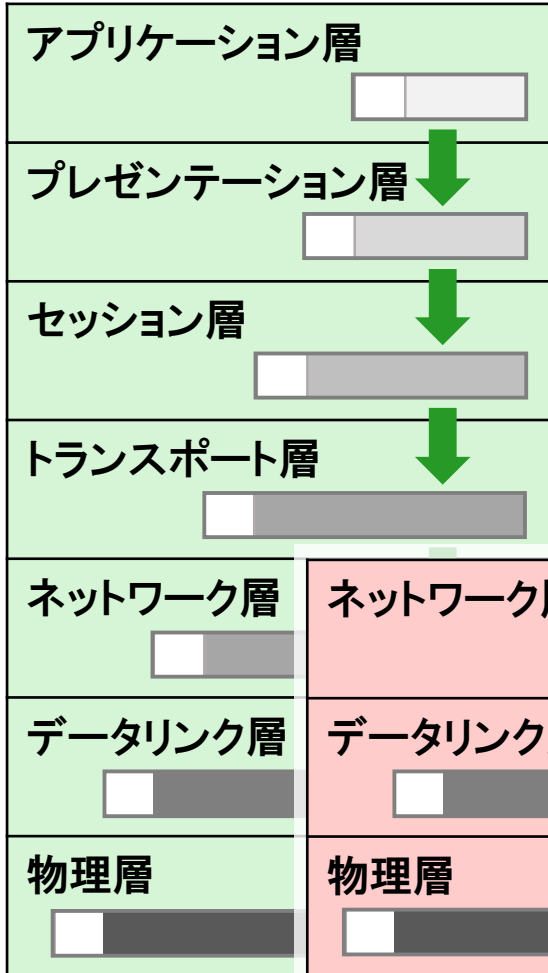


受信側C

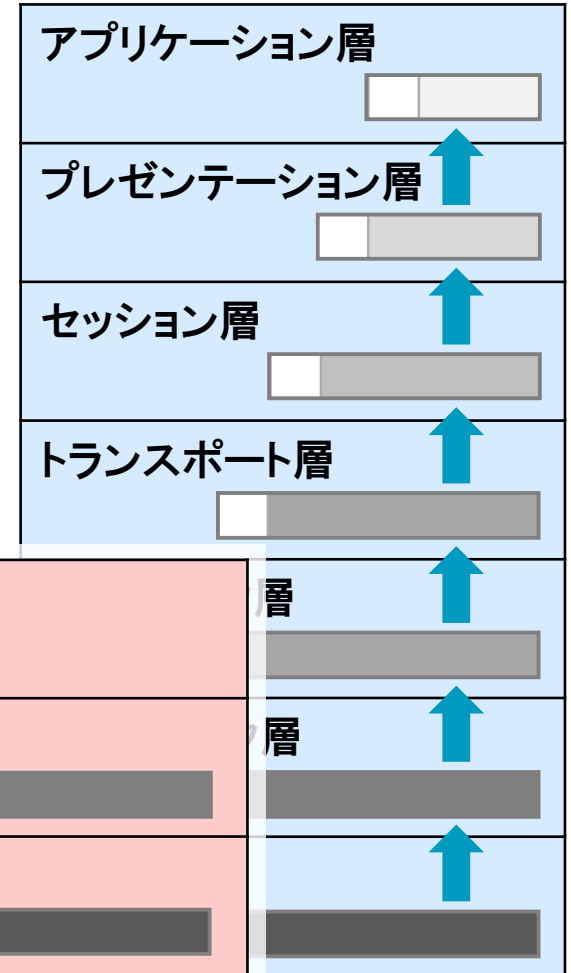


OSI参照モデルによる送受信

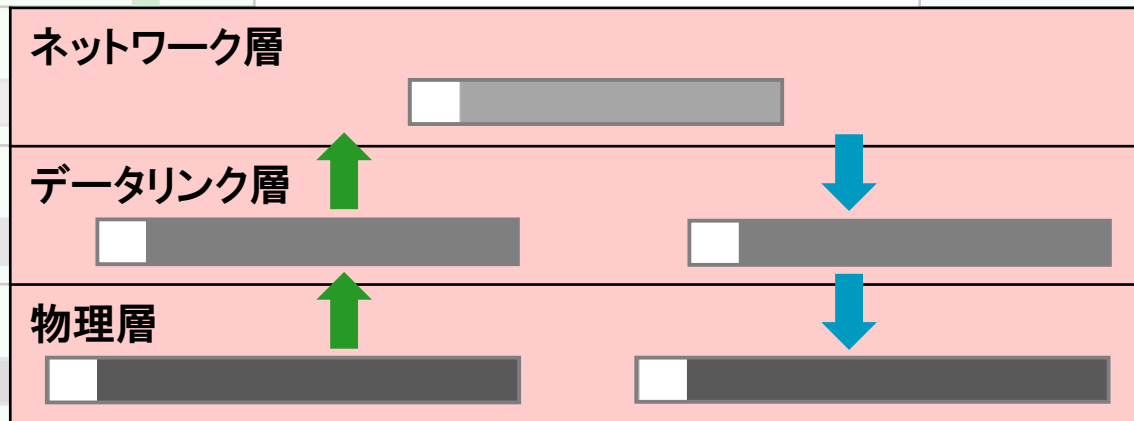
送信側A



受信側C



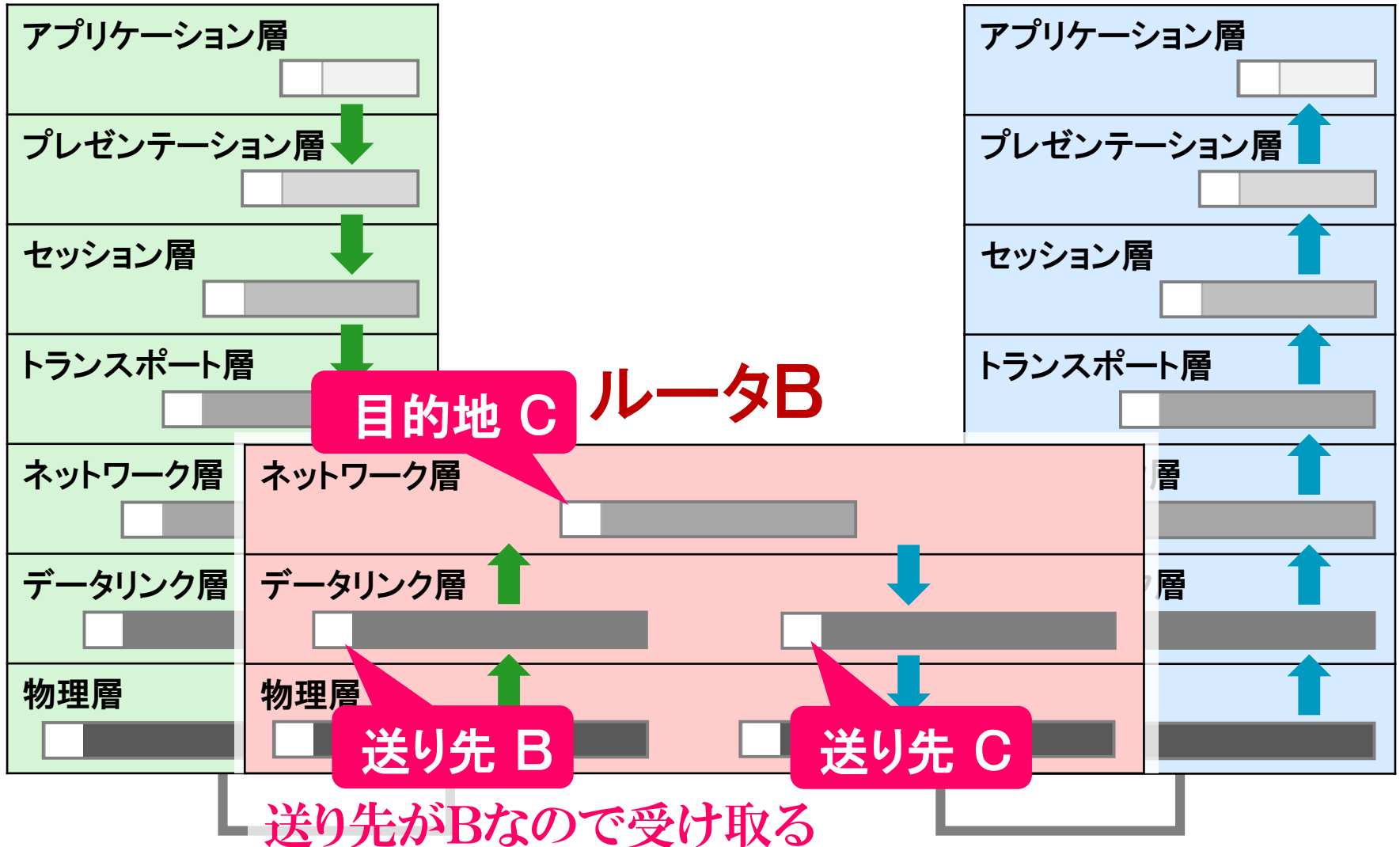
ルータB



OSI参照モデルによる送受信

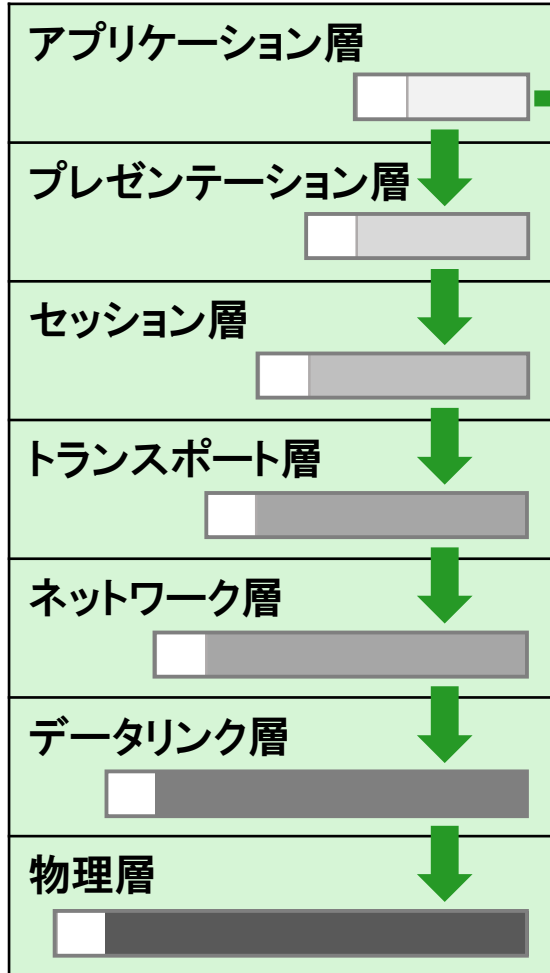
送信側A

受信側C

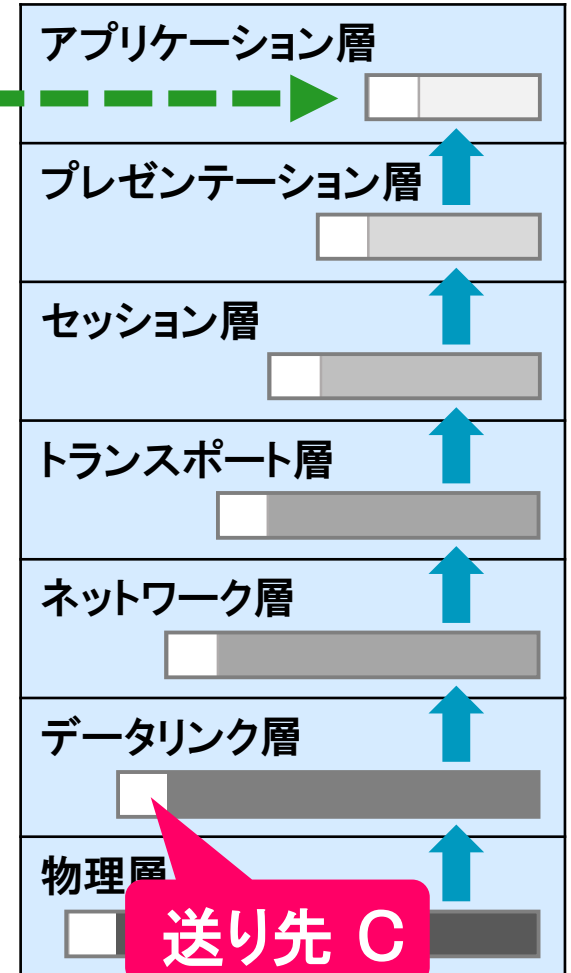


OSI参照モデルによる送受信

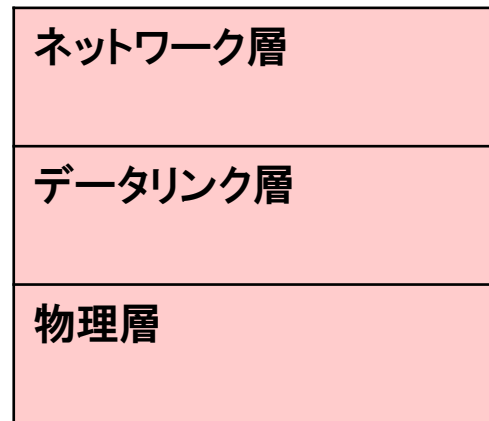
送信側A



受信側C



ルータB



送り先がCなので受け取る

第1層 物理層

ノード間を物理的に接続するための、
電氣的・機械的な仕様を規定する。

✦ 通信媒体

同軸ケーブル、ツイストペアケーブル、
光ファイバーケーブル、無線（電磁波）

✦ 物理層に位置する機器

リピータ

リピータ

物理層で、ネットワークを延長する機器

伝送路に流れてきた信号を受信して、
増幅や波形を整形する。

伝送方向による通信の分類

❖ 単方向通信 (simplex)

一方向のみに信号を送る

❖ 半二重通信 (Half Duplex)

双方向に信号を送れるが、同時には送れない。

❖ 全二重通信 (Full Duplex)

同時に、双方向に信号を送れる。

ネットワーク トポロジー

複数のコンピュータを接続する形態

✦ スター型

✦ ツリー型

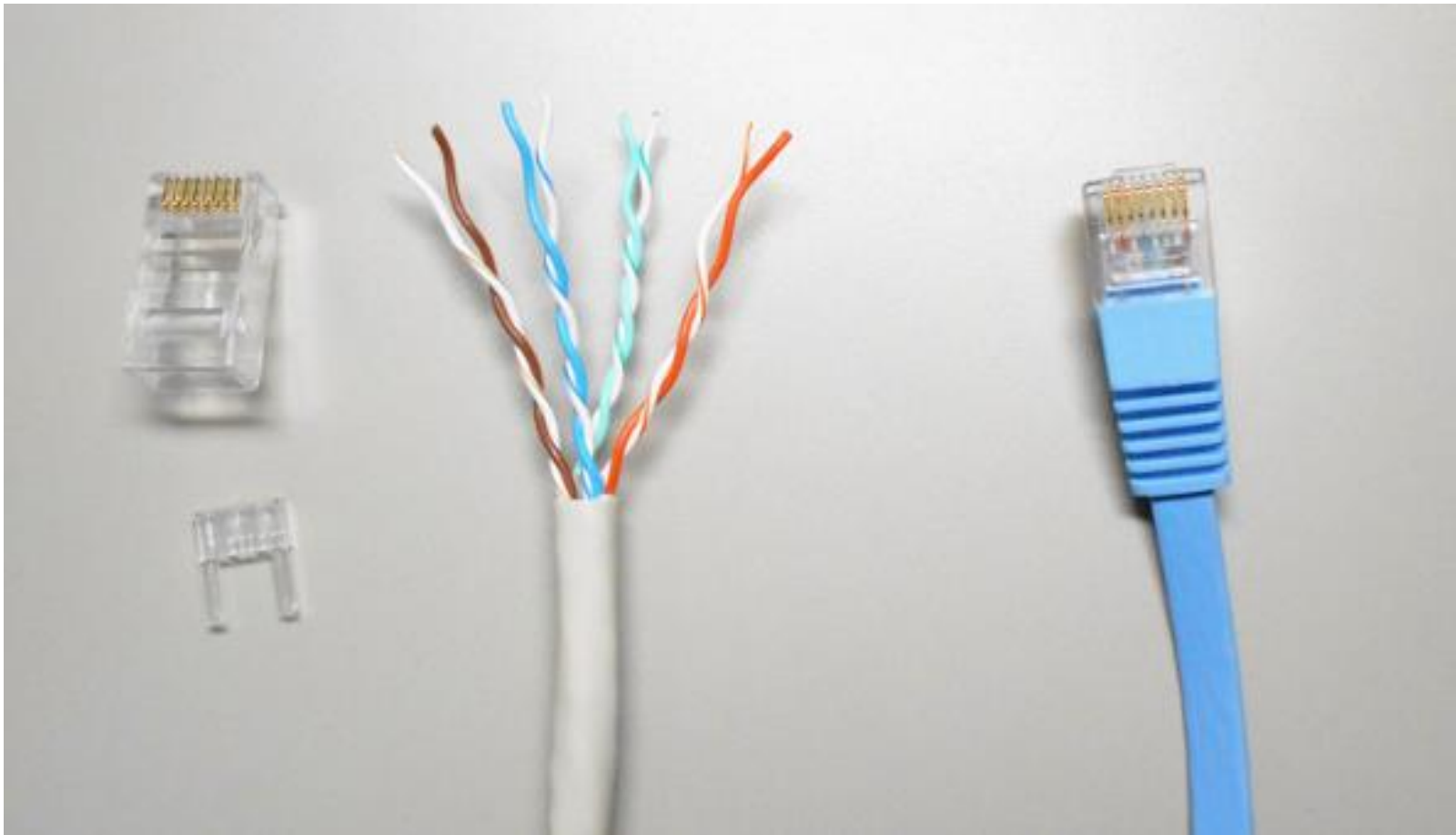
✦ リング型

✦ バス型

✦ メッシュ型

LANケーブル

ツイストペアケーブル(より対線)



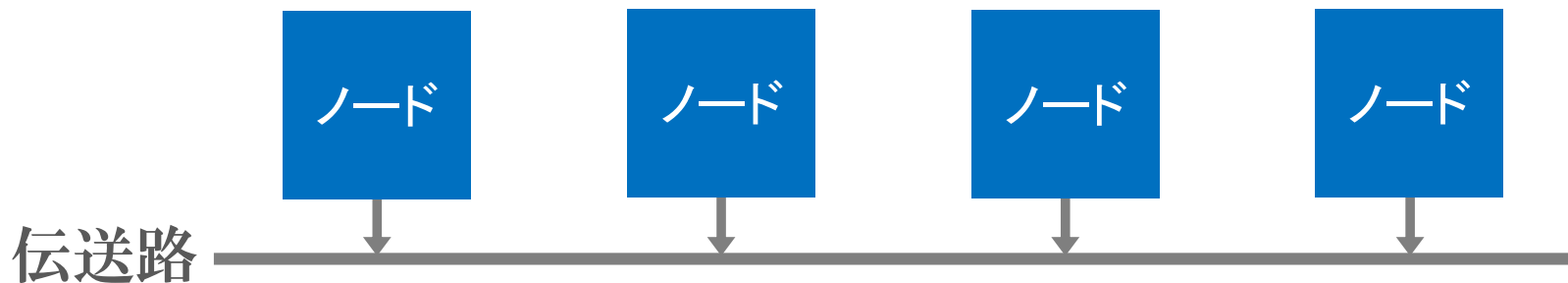
LANケーブルのカテゴリ

カテゴリ	通信速度	伝送帯域
CAT5	100Mbps	100MHz
CAT5e	1Gbps	100MHz
CAT6	1Gbps	250MHz
CAT6a	10Gbps	500MHz
CAT7	10Gbps	600MHz

CSMA/CD

重要

- ① 送信前に伝送路にデータが流れていないか調べる。(CS)
- ② 伝送路にデータが流れていなければ、どのノードも送信する権利がある。(MA)
- ③ データの衝突を検出した場合、送信を停止する。(CD)



第2層 データリンク層

通信媒体で直接接続されたノード間で通信するための仕様を規定する。

❖ データリンク層に位置する機器

ブリッジ、スイッチングハブ、L2スイッチ

ブリッジ, スイッチ

データリンク層で、ネットワーク同士を接続する装置。

コリジョンドメインを分割できる。

受信したフレームを一時的に記憶する。

フレームが壊れていないかチェックする。

宛先アドレスを見て、フレームを送り出すネットワークを選択する。

MACアドレス

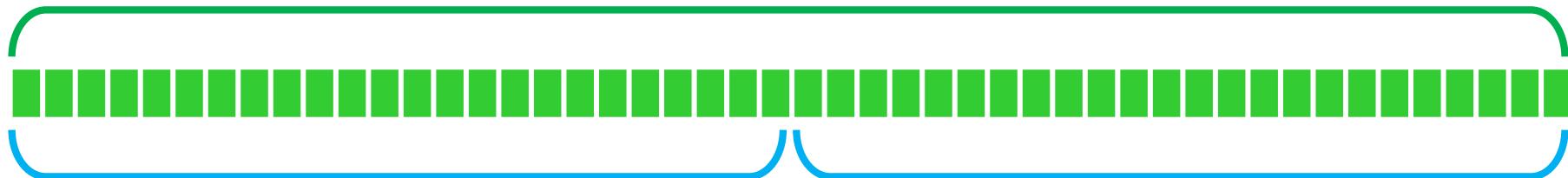
重要

Media Access Control Address

データリンクに接続しているノードの識別に利用される。

LANカードやネットワーク機器の製造時に固有のアドレスが書き込まれる。

48bit



メーカーの識別番号

メーカー内での識別番号

イーサネット(Ethernet)

重要

有線LANで最も使われている規格。

物理層とデータリンク層を規定する。

❖ LANケーブルの規格

❖ CSMA/CD 方式

❖ MACアドレス

❖ イーサネットフレーム

イーサネットフレーム

同期信号 (56bit)	開始信号 (8bit)
宛先MACアドレス (48bit)	
送信元MACアドレス (48bit)	
タイプ/フレーム長 (16bit)	
データ (46~1500byte)	
FCS (Frame Check Sequence) (32bit)	

第3層 ネットワーク層

送信元から送信先まで、終端ノード間の通信の仕様を規定する。

❖ ネットワーク層に位置する機器

ルータ、L3スイッチ

❖ ネットワーク層のプロトコル

IP、ARP、ICMP

ルータ, L3スイッチ

ネットワーク層で、ネットワーク同士を接続する装置。

パケットの宛先アドレスを見て、伝送経路を決定する。

ルータ同士が通信して、経路制御情報を自動的に更新する。

IP(インターネット プロトコル)

終端ノード間(end-to-end)
の通信を実現する。

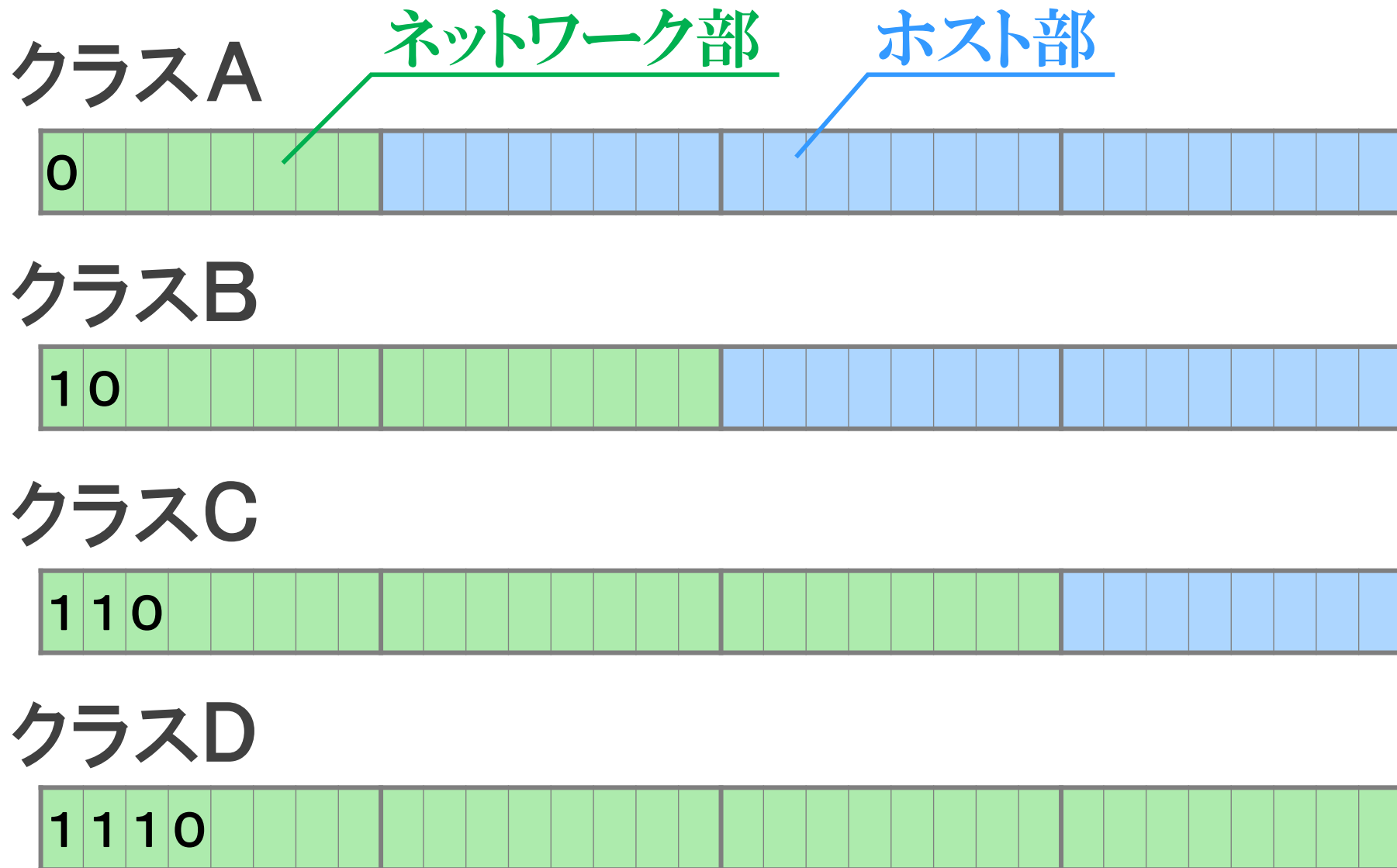
重要

役割

- ✦ IPアドレスの規定
- ✦ 経路制御(ルーティング)

IPアドレス (IPv4)

重要

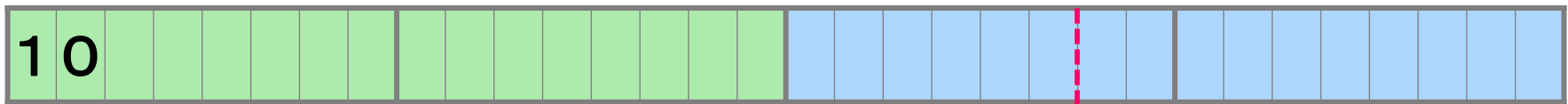


サブネットワーク

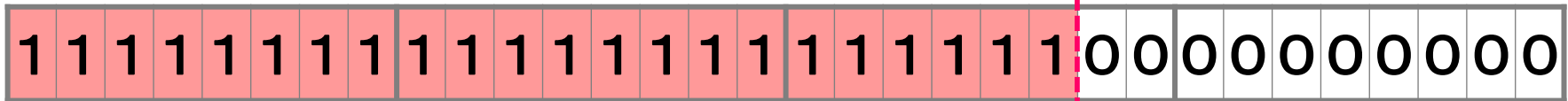
重要

1つのネットワークを小さなネットワークに
仮想的に細分化する。

例: クラスB



サブネットマスク



— 仮想的なネットワーク部 — — ホスト部 —

プライベートアドレス

重要

インターネットから独立したネットワーク内
のみで使用できるIPアドレス

クラスA 10. 0. 0. 0 ~ 10. 255. 255. 255

クラスB 172. 16. 0. 0 ~ 172. 31. 255. 255

クラスC 192. 168. 0. 0 ~ 192. 168. 255. 255

グローバルアドレス

インターネットへの接続に使用するIPアドレス

NAT

Network Address Translation

プライベートアドレスをグローバルアドレスに変換する技術。

プライベートアドレスのコンピュータをインターネットに接続できるようになる。

ルータの機能の一つ。

IPv6

IPv4のアドレスの枯渇に備えて、アドレス数を大幅に増やした新しい規格のIPアドレス。

- ✦ 128bit $2^{128} \doteq 340 \times 10^{36}$ 個
- ✦ 16bitごとに「:」で区切り、16進数で書く。
- ✦ 「0000」は「0」と表記する。
- ✦ :0:が連続する場合、0 を省略できる。

ARP

Address Resolution Protocol

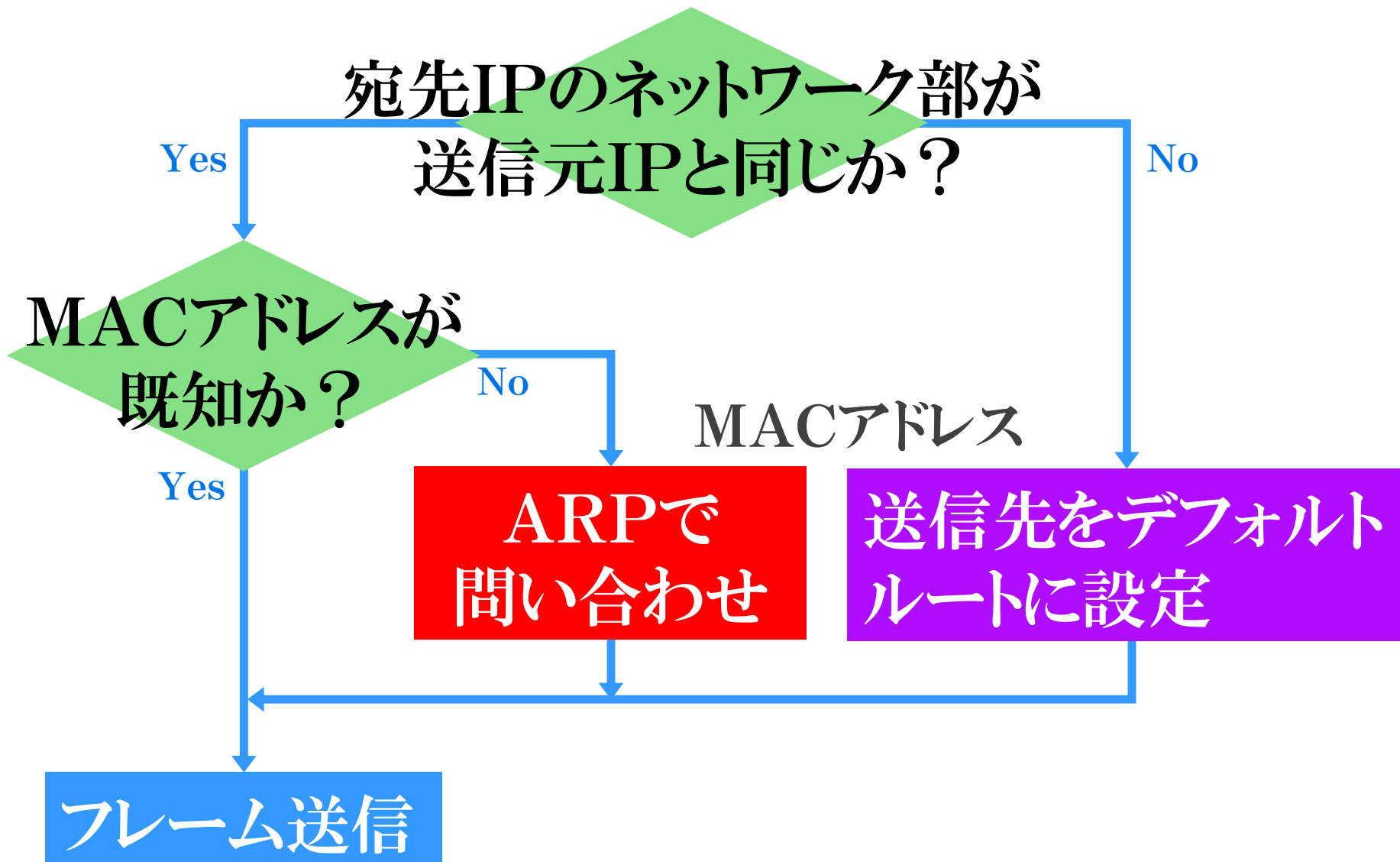
IPアドレスからMACアドレスを知るために、ネットワーク内の全ノードに問い合わせるプロトコル。

ネットワーク層のプロトコル。

ARPパッケージ

ハードウェアタイプ (16bit)	プロトコルタイプ (16bit)	
HLEN (8bit)	PLEN (8bit)	オペレーション (16bit)
送信元MACアドレス (48bit)		
送信元IPアドレス (32bit)		
探索するMACアドレス (48bit) 要求時にはすべて0		
探索するIPアドレス (32bit)		

ネットワーク内部と外部への通信



経路制御(ルーティング)

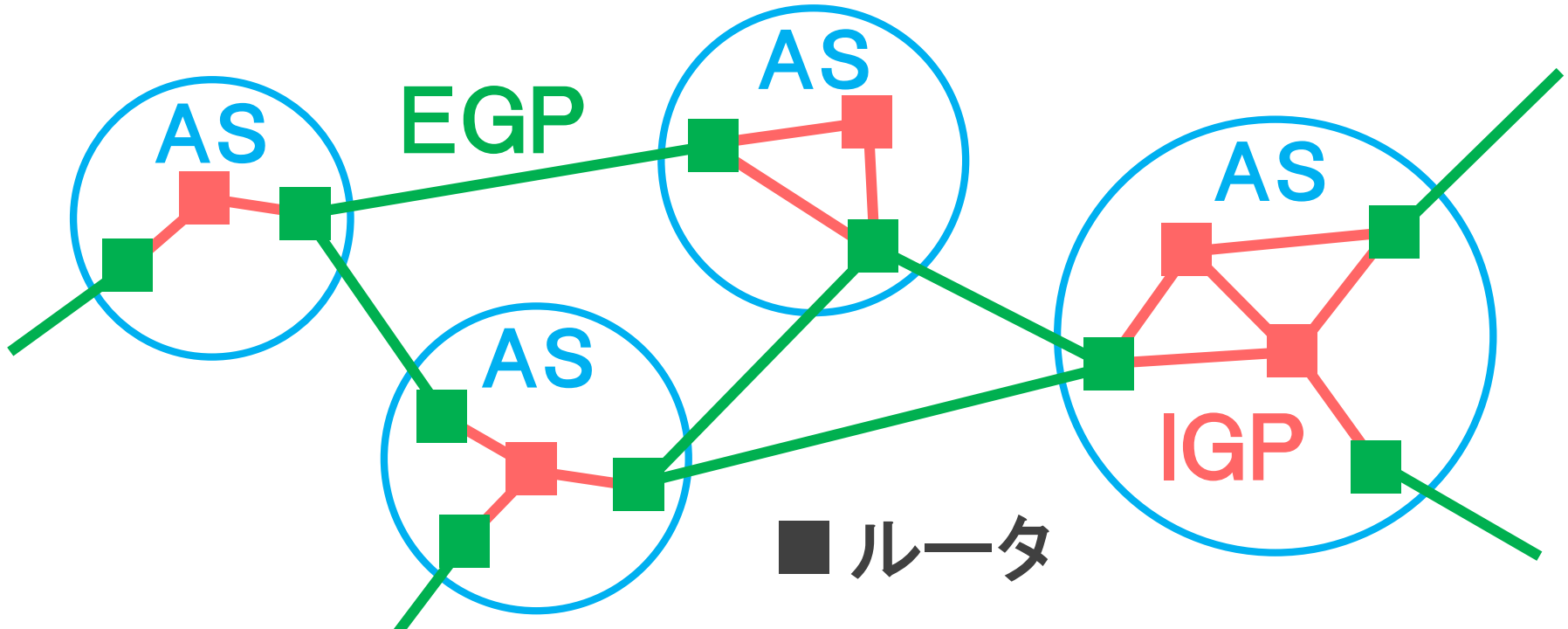
受信したパケットの宛先アドレスと**経路制御表(ルーティングテーブル)**を比較して、次の送り先のルータを決定する。

- ❖ **静的経路制御(スタティックルーティング)**
経路制御表を手作業で設定する。
- ❖ **動的経路制御(ダイナミックルーティング)**
ルータ同士が通信して、経路制御表を自動更新する。

自律システムと経路制御

自律システム (Autonomous System)

経路制御を行う単位。インターネット接続業者(プロバイダ)や、組織、機関など。



ルーティングプロトコル

重要

❖ IGP (Interior Gateway Protocol)

AS内で使用するルーティングプロトコル

❖ RIP (Routing Information Protocol)

❖ OSPF (Open Shortest Path First)

❖ EGP (Exterior Gateway Protocol)

AS間で使用するルーティングプロトコル

❖ BGP (Border Gateway Protocol)

第4層 トランスポート層

重要

アプリケーション間の通信方式を規定する。通信の信頼性を提供する。

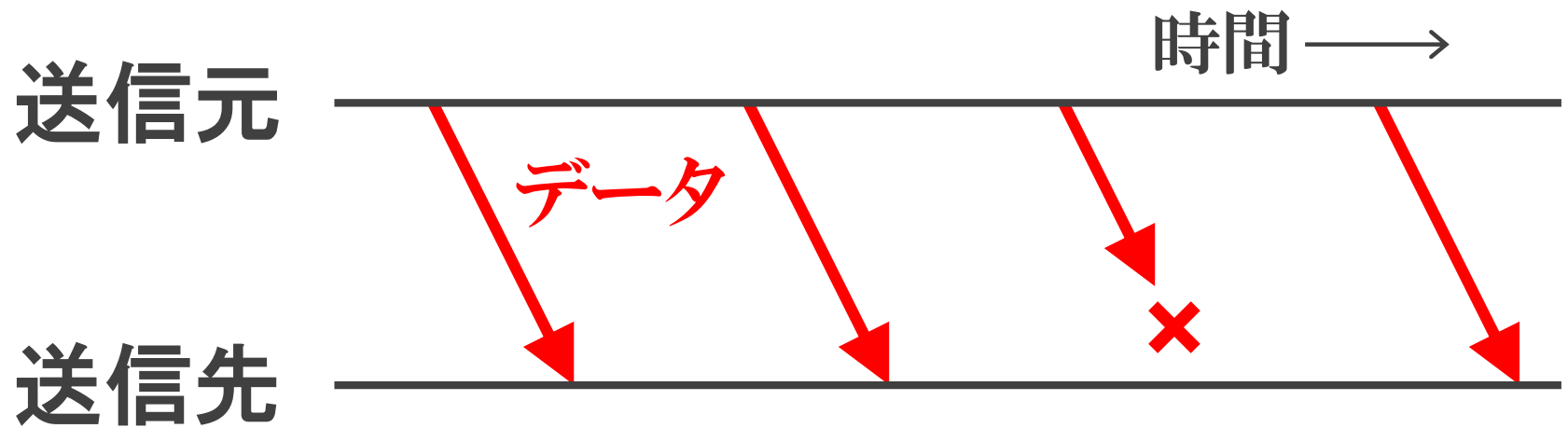
✦ トランスポート層のプロトコル

✦ **TCP** (Transmission Control Protocol)
コネクション型。信頼性を保証する。

✦ **UDP** (User Datagram Protocol)
コネクションレス型。信頼性を保証しない。

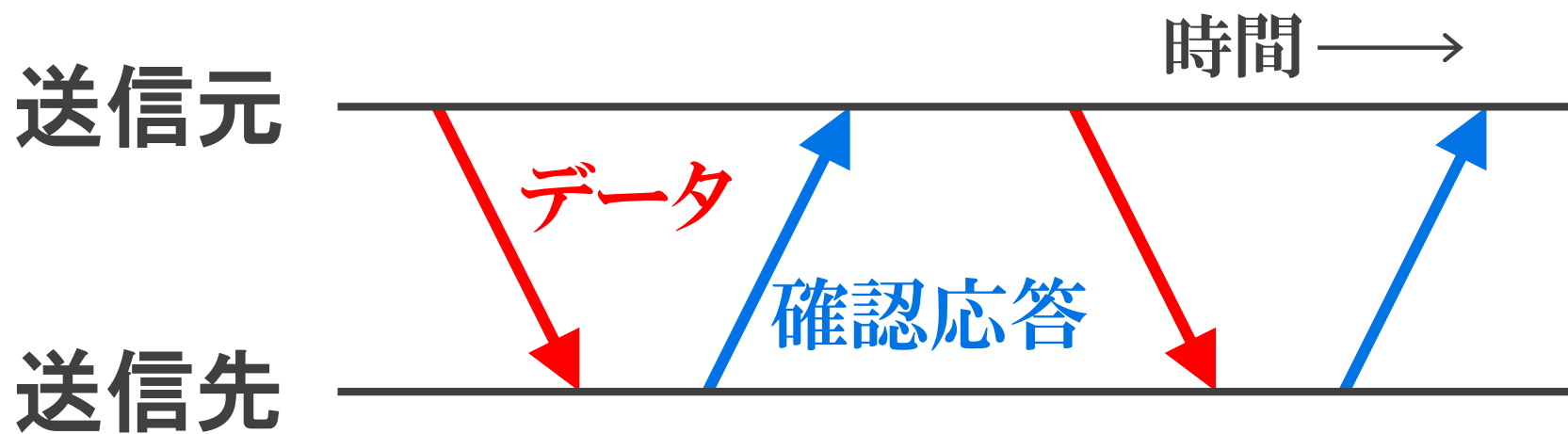
UDP

IPを用いてコネクションレス型の通信を行う。通信の信頼性は低い^が、高速に実行できる。



TCP

IPを用いてコネクション型の通信を行う。
通信の信頼性が高いが、UDPに比べて、
通信制御が複雑で時間がかかる。



UDPヘッダ

送信側ポート番号 (16bit)	受信側ポート番号 (16bit)
データ長 (16bit)	チェックサム (16bit)
データ	

TCPヘッダ

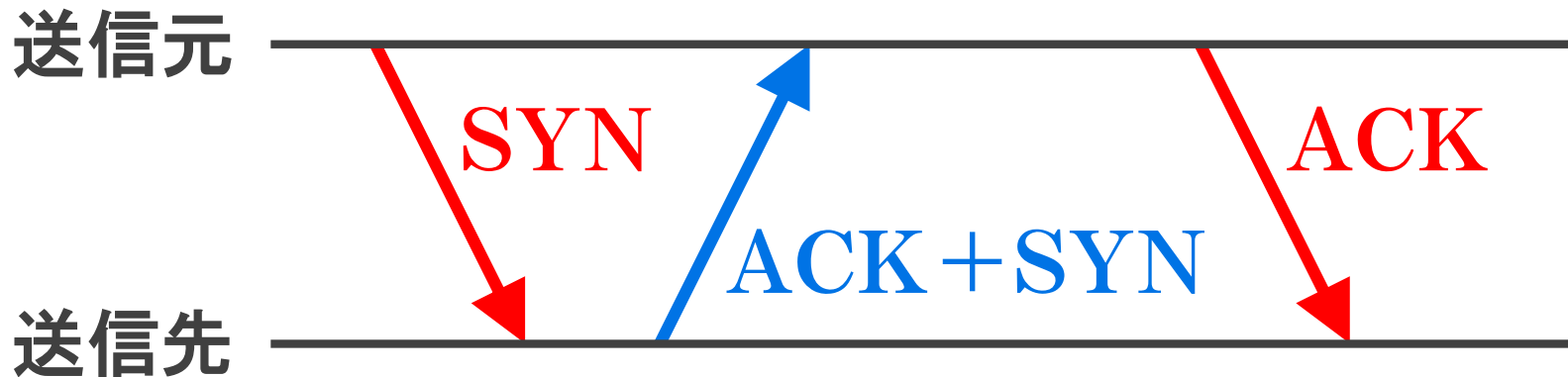
送信側ポート番号 (16bit)		受信側ポート番号 (16bit)				
シーケンス番号 (32bit)						
確認応答番号 (32bit)						
データ オフ セット (4bit)	予約 (6bit)	コントロール フラグ (6bit)				ウィンドウサイズ (16bit)
		U R G	A C K	P S H	R S T	
チェックサム (16bit)			緊急ポインタ (16bit)			
オプション					パディング	
データ						

TCP コントロールフラグ

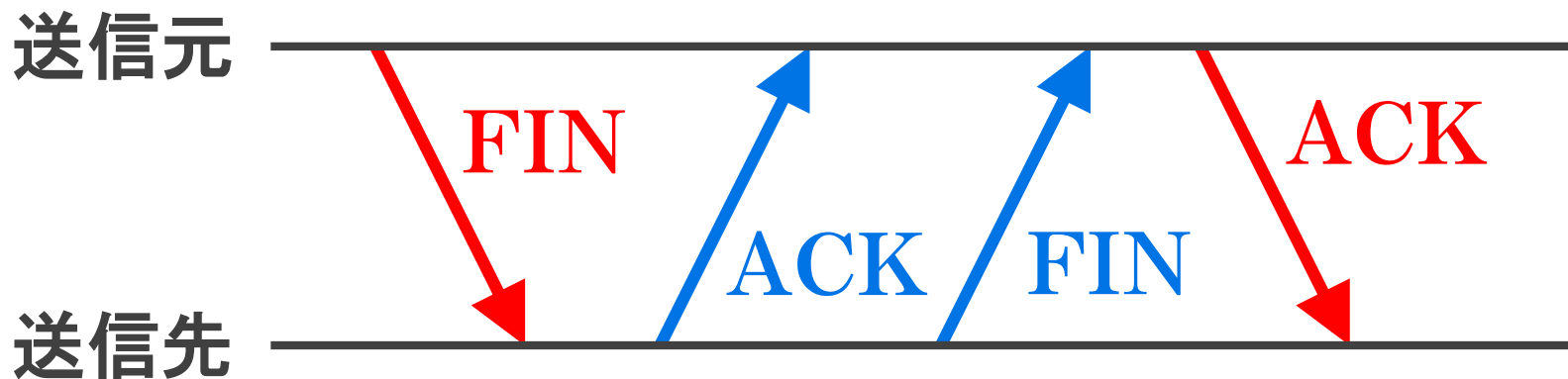
コントロールフラグ	役割・意味
URG Urgent	緊急に処理すべきデータが含まれている
ACK Acknowledgment	確認応答
PSH Push	アプリケーション層へすぐにデータを渡す
RST Reset	通信の強制切断
SYN Synchronize	通信開始の要求
FIN Fin	通信終了の要求

TCP コネクション管理

✦ コネクションの確立

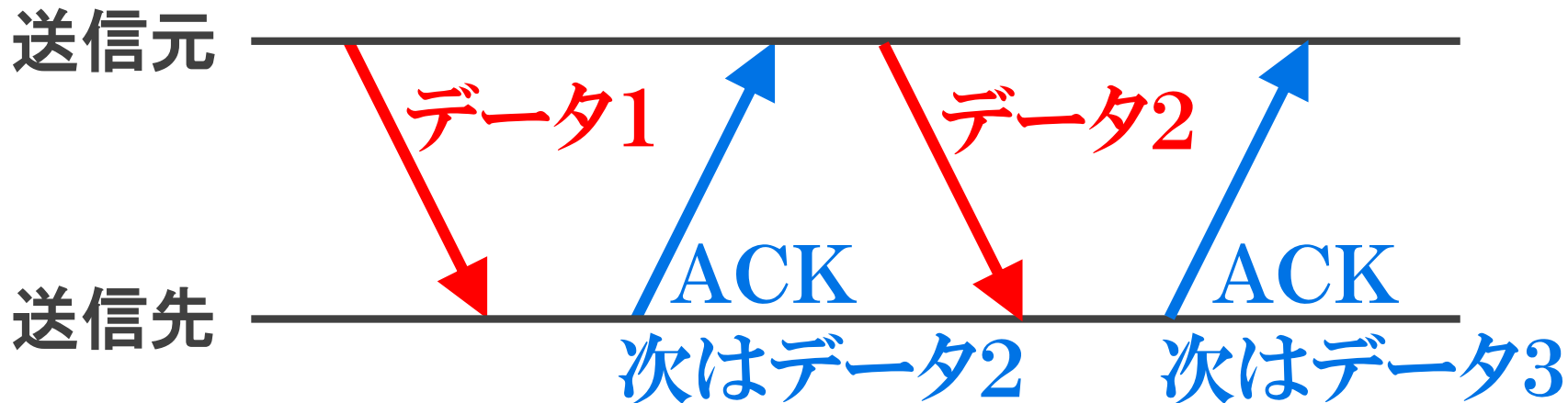


✦ コネクションの切断

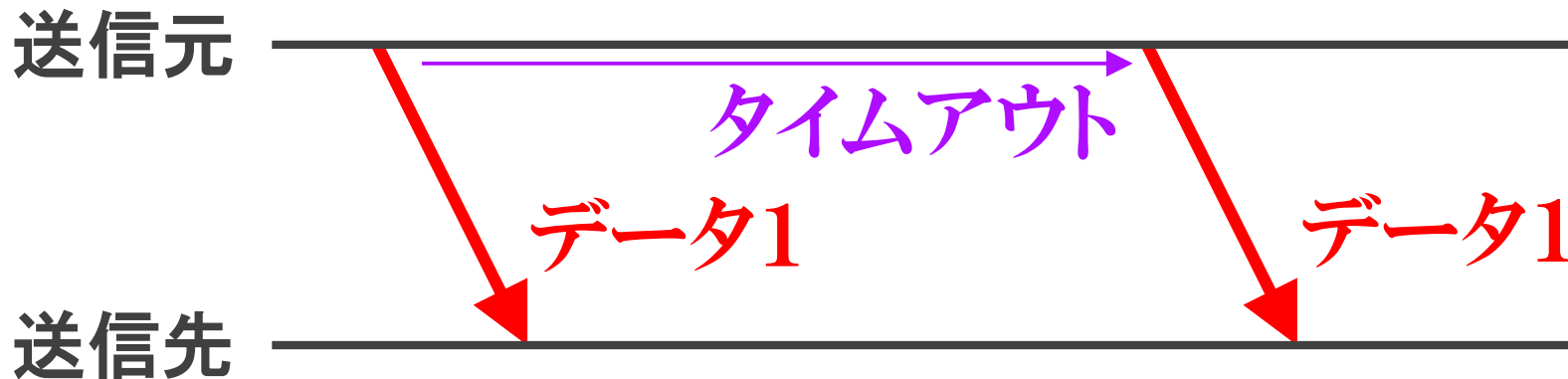


TCP セグメントの送信

❖ セグメントの送信



❖ セグメントの再送



TCP シーケンス番号と確認応答番号

❖ シーケンス番号

送信するデータの先頭が、全データの何byte目であるかを表す。

❖ 確認応答番号

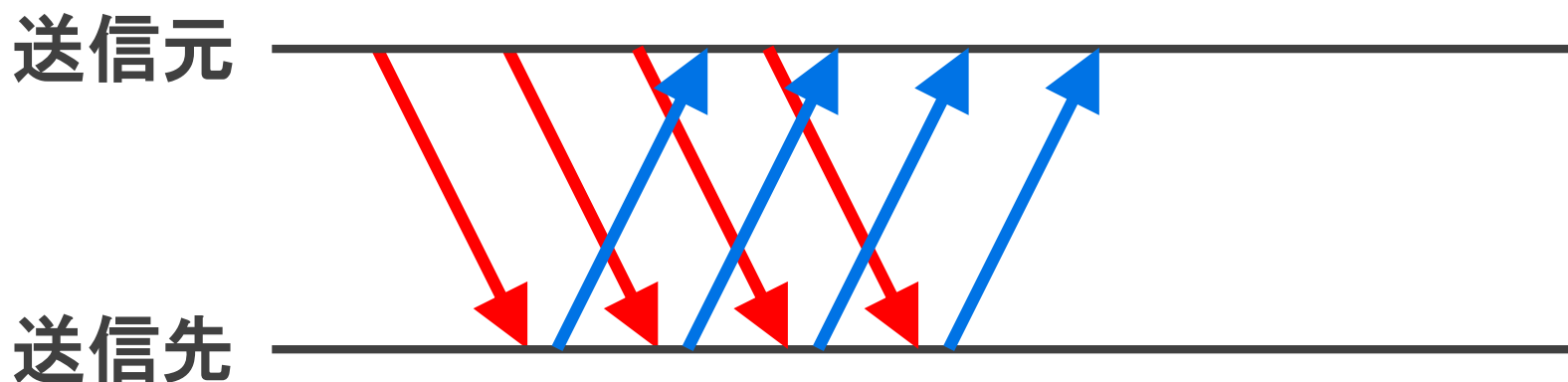
次に送信してもらおうデータの先頭が、全データの何byte目になるかを表す。

TCP フロー制御

確認応答を待たないで、複数のセグメントを連続して送る方式。

ウィンドウサイズ

受信側が一度に受け取れるデータ量。
通信途中にウィンドウサイズを変更できる。



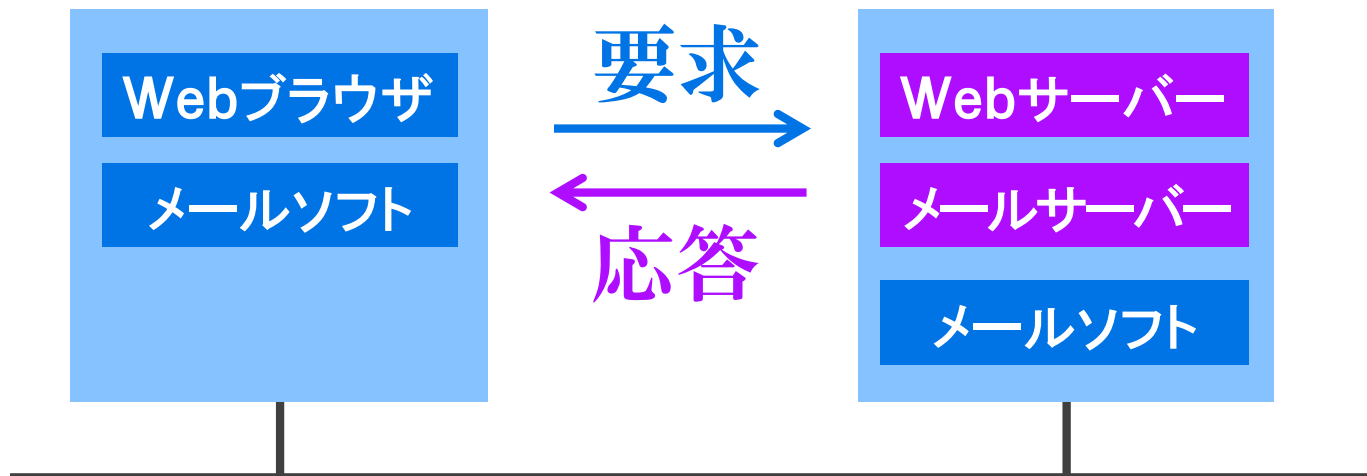
クライアント・サーバー モデル

❖ サーバー

サービスを提供するプログラム

❖ クライアント

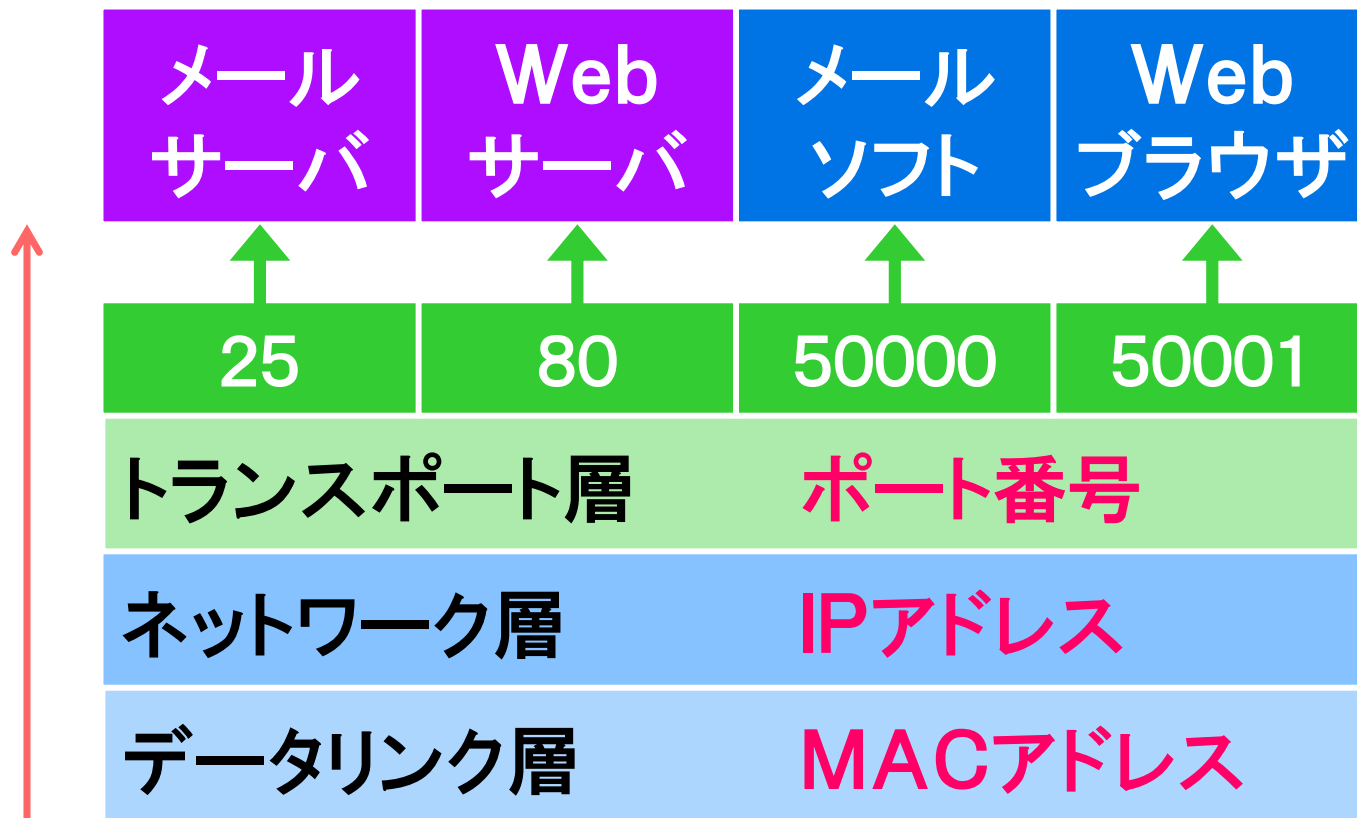
サービスを受けるプログラム



ポート番号

重要

コンピュータ内で通信を行っているプログラムの識別に用いる。



ポート番号の分類

- ❖ ウェルノウン・ポート (well-known port)
広く利用されるサービスに、あらかじめ定められているポート番号。(0~1023番)
- ❖ 登録済みポート (registered port)
あらかじめ定められているポート番号。
(1024~49151番)
- ❖ 動的ポート (dynamic port)
自由に利用できるポート番号。
(49152~65535番)

ウェルノウン・ポート番号(一部)

ポート番号	プロトコル	内容
20	FTP-data	ファイル転送(データ)
21	FTP	ファイル転送(制御)
22	SSH	遠隔ログイン(セキュリティあり)
23	Telnet	遠隔ログイン
25	SMTP	電子メール(送信)
53	DNS	ドメイン名管理
80	HTTP	WWW
110	POP3	電子メール(受信) POP ver.3
123	NTP	時刻同期
143	IMAP	電子メール(受信) IMAP ver.4
443	HTTPS	WWW(セキュリティあり)

IPに関連する技術

✿ DNS

✿ DHCP

✿ NAT / NAT

✿ ICMP

✿ ARP

DNS

Domain Name System

ドメイン名とIPアドレスの対応を管理し、その情報を提供する。

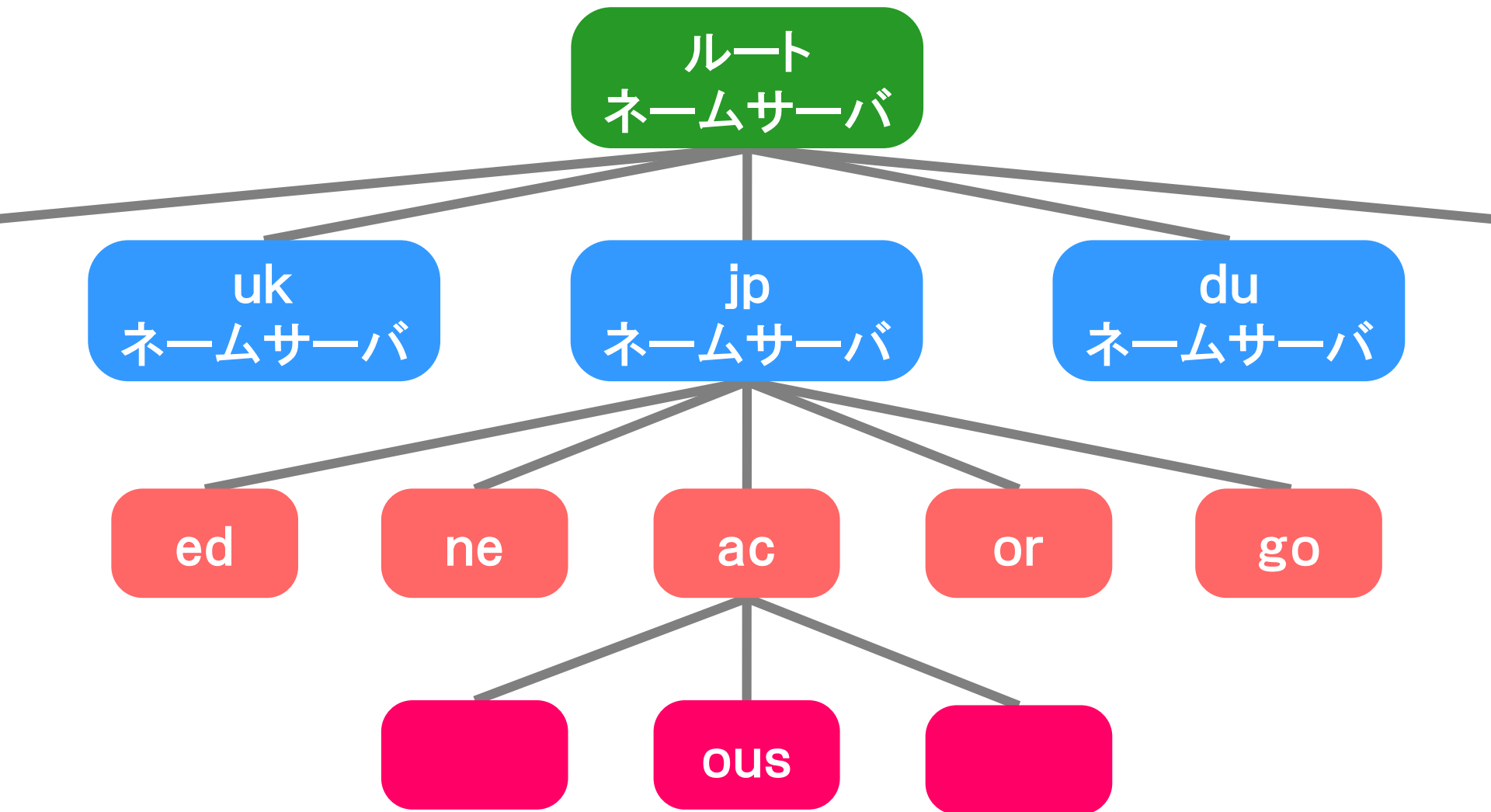
ドメイン名

IPアドレスに代えて、人間が理解しやすい表記にしたコンピュータの名前。

jp(日本)ドメイン下のドメイン

ドメイン名	組織
ac	大学
co	企業
ed	幼稚園、小・中・高等学校など
go	政府機関
ne	ネットワークサービス提供組織
gr	任意団体
ad	JPNICの会員
lg	地方公共団体
tokyo, osaka など	地域ドメイン

DNSの階層構造



DHCP

Dynamic Host Configuration Protocol

ネットワークに接続されたノードに、IPアドレスを自動的に割り振るプロトコル。

LANケーブルを接続、または、無線のアクセスポイントを選ぶだけで、ネットワークを利用できるようになる。

DHCPのしくみ

① DHCP発見

クライアントが**DHCP発見パケット**を送る。DHCPサーバが利用可能なIPアドレスを通知する(**提供パケット**)。

② DHCP要求

通知を受けて、クライアントが**要求パケット**を送る。DHCPサーバが**確認応答パケット**を送り返して、通信が完了する。

NAPT

Network Address Port Translation

プライベートネットワーク内の多数のノードをインターネットに接続する技術。

NATのIPアドレス変換の機能に加えて、ポート番号の変換も行う。

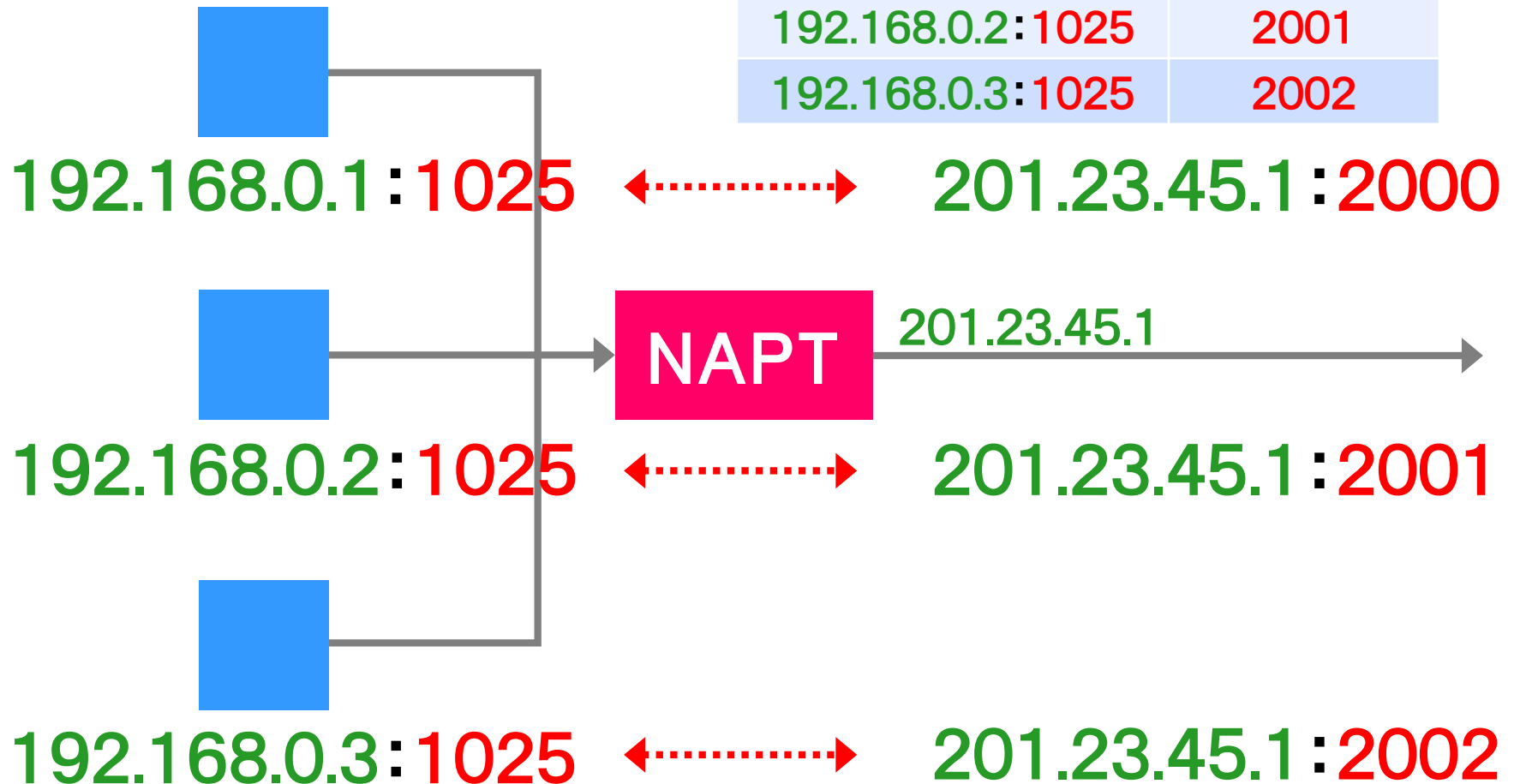
ポート番号で、プライベートネットワークのノードを区別する。

NAPTのしくみ

送信元

IPアドレス:ポート番号

プライベート側の IPアドレス:ポート番号	グローバル側 のポート番号
192.168.0.1:1025	2000
192.168.0.2:1025	2001
192.168.0.3:1025	2002



ICMP

Internet Control Message Protocol

インターネット層で、通信状態の確認に用いるプロトコル。

タイプ	内容	意味
8	エコー要求	IPパケットが宛先に届くか確認する。
0	エコー応答	エコー要求に対する応答
3	到達不能	IPパケットが宛先に届かない。
11	時間超過	規定数以上のルータを経由したため、パケットが破棄された。
10	ルータ請願	自分のネットワークのルータを探索する。