コンピュータネットワーク

Rev. 2018.09.20

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参照モデルに軸をおいて、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学習する。

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、ネットワーク機器、
LANケーブル、無線LAN、サーバ・クライアント など

✤ ネットワーク通信の方法

OSI参照モデル、TCP/IP、ルーティング、ポート、
DNS、WWWや電子メールの通信プロトコル　など

✤ ネットワークセキュリティ

ファイアウォール、暗号化通信、電子署名　など

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

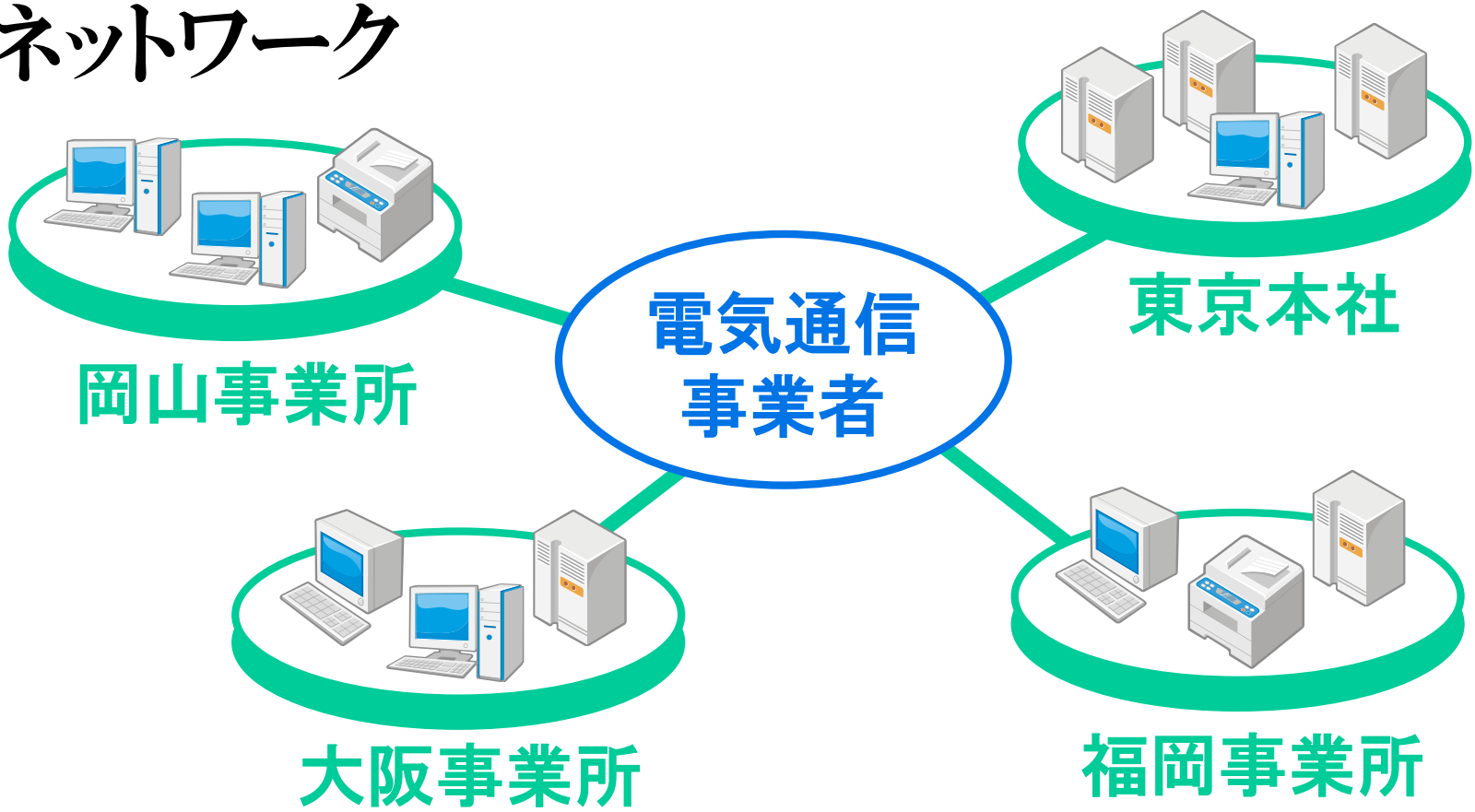
ネットワークの形態

重要

- LAN (Local Area Network)
- WAN (Wide Area Network)
- イントラネット
- インターネット

WAN

電気通信事業者が提供するネットワークを利用して、離れた地域のLAN同士を接続したネットワーク



インターネットとイントラネット

- **インターネット**

  複数のLANを接続して作られた世界規模のネットワーク。誰でも利用できる。

- **イントラネット**

  インターネットの技術を利用して作られた、組織内のネットワーク。利用者は限定される。

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

回線交換・パケット交換

✤ 回線交換

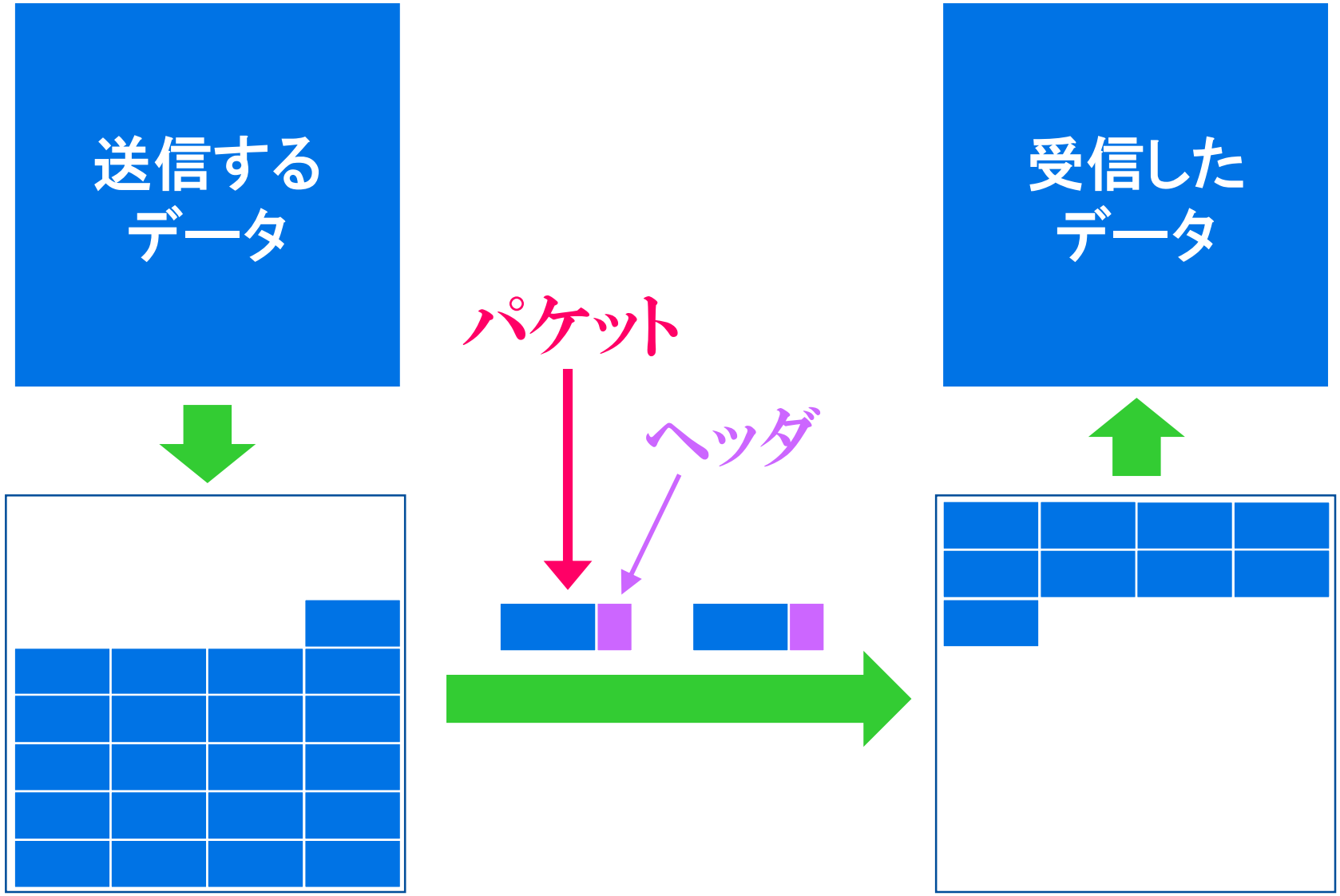
回線交換機が通信回線を切り替えて、2台のコンピュータを接続する。

通信が切れるまで回線を占有する。

✤ パケット交換

データを小さく分割して送る。一つの回線を複数のコンピュータが同時に利用できる。

パケット



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

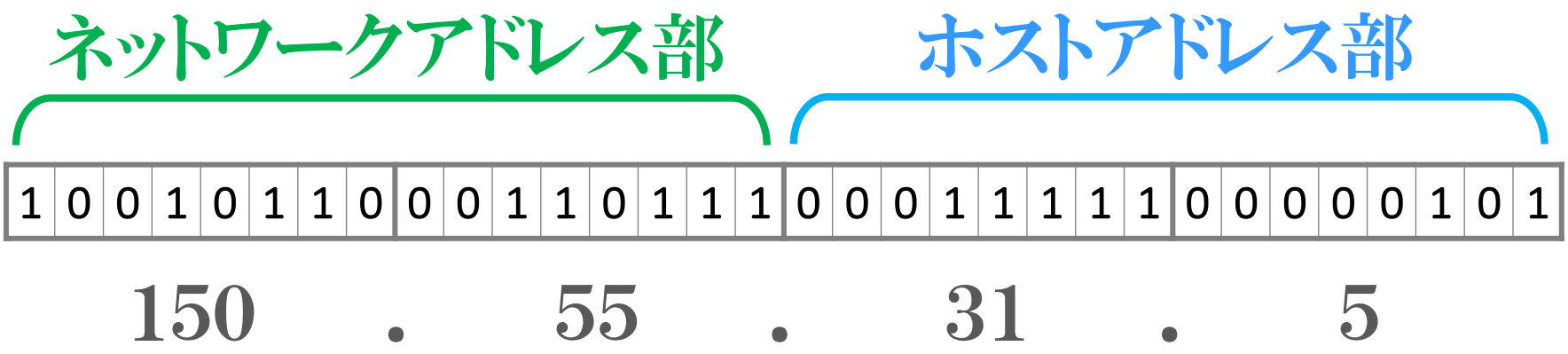
通信手順やデータ構成を決めたもの

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

IPアドレスの基礎

ネットワークに接続された機器を識別するための固有番号



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。

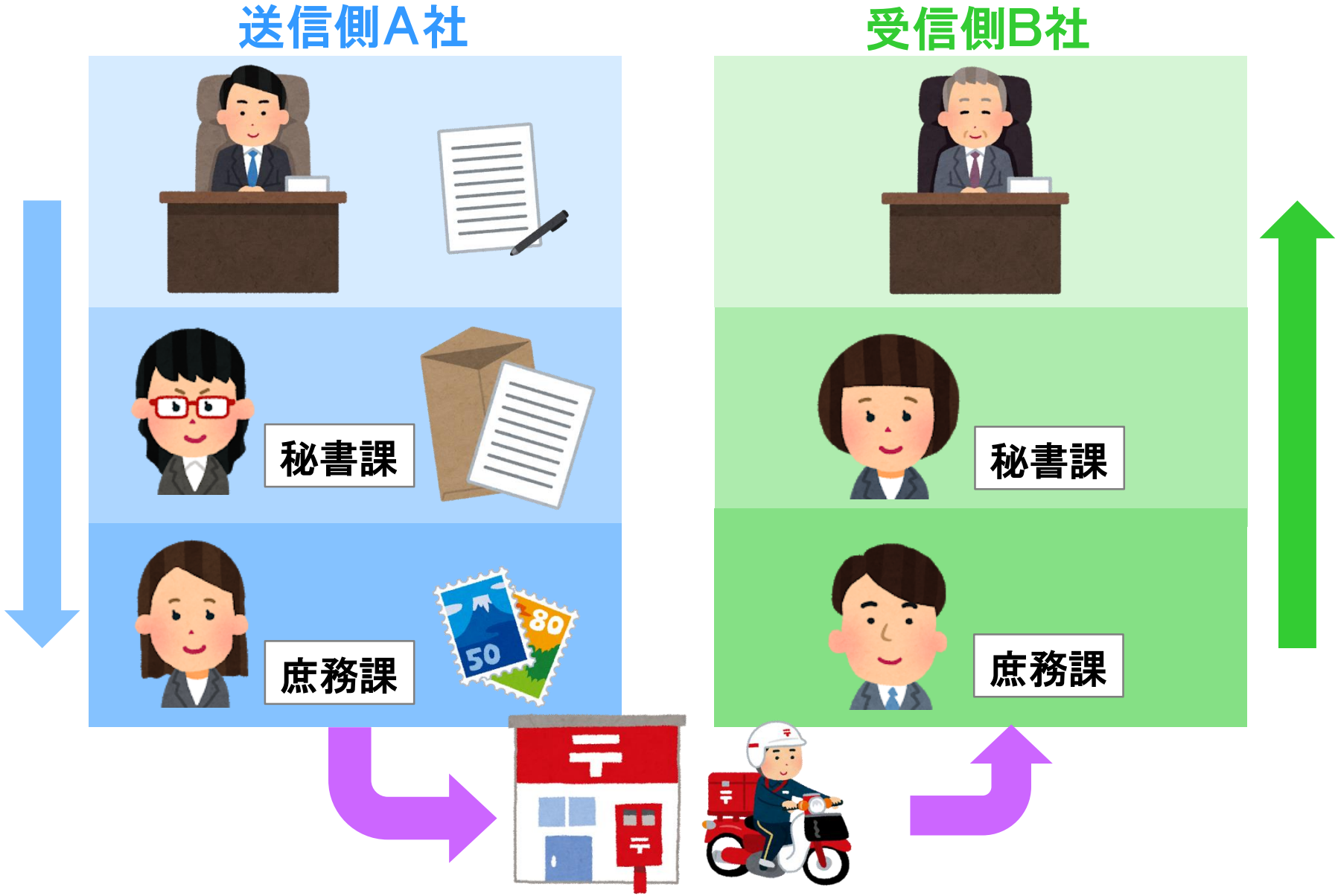
OSI参照モデル

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。

通信のイメージ

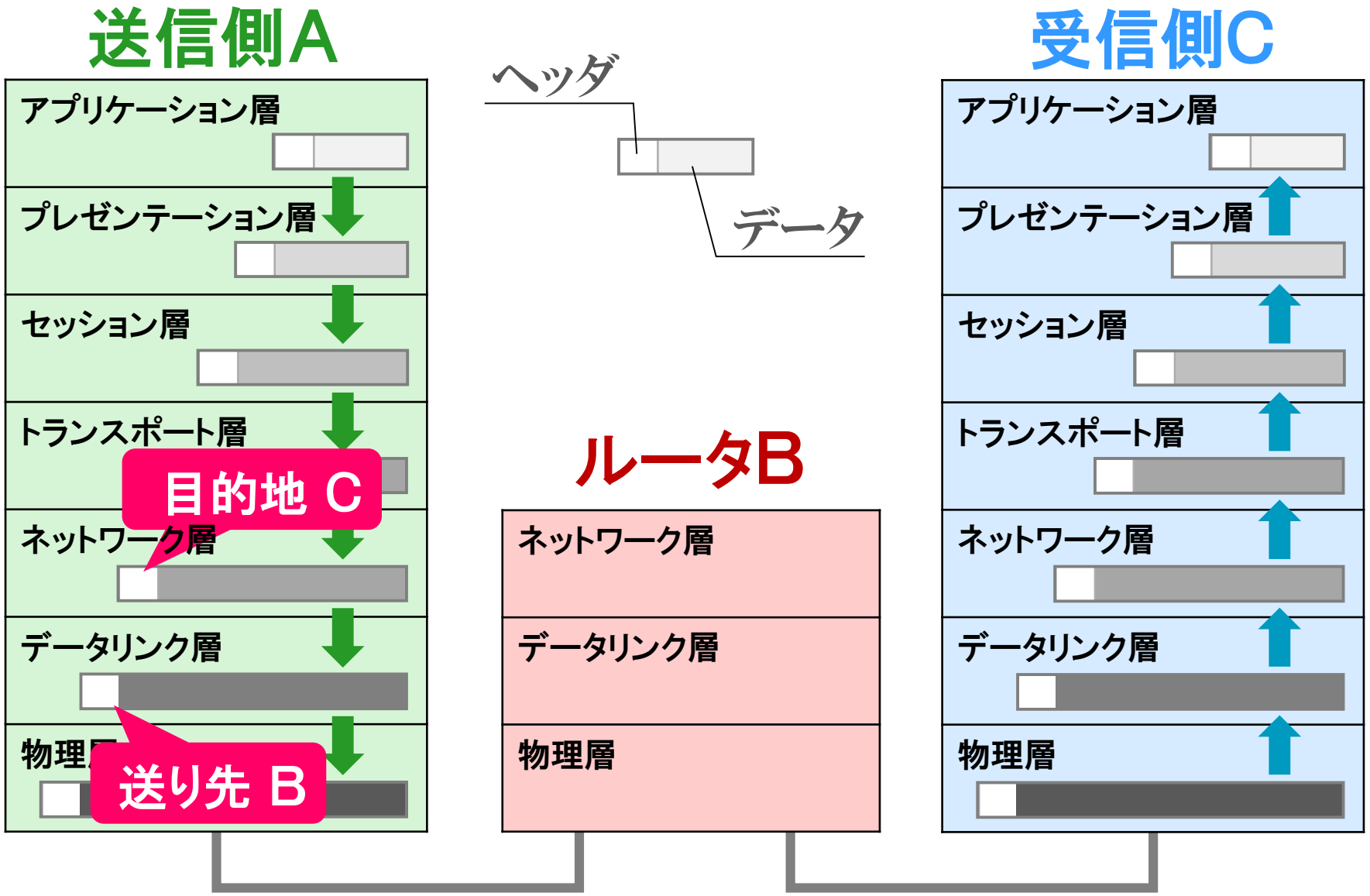


OSI参照モデル

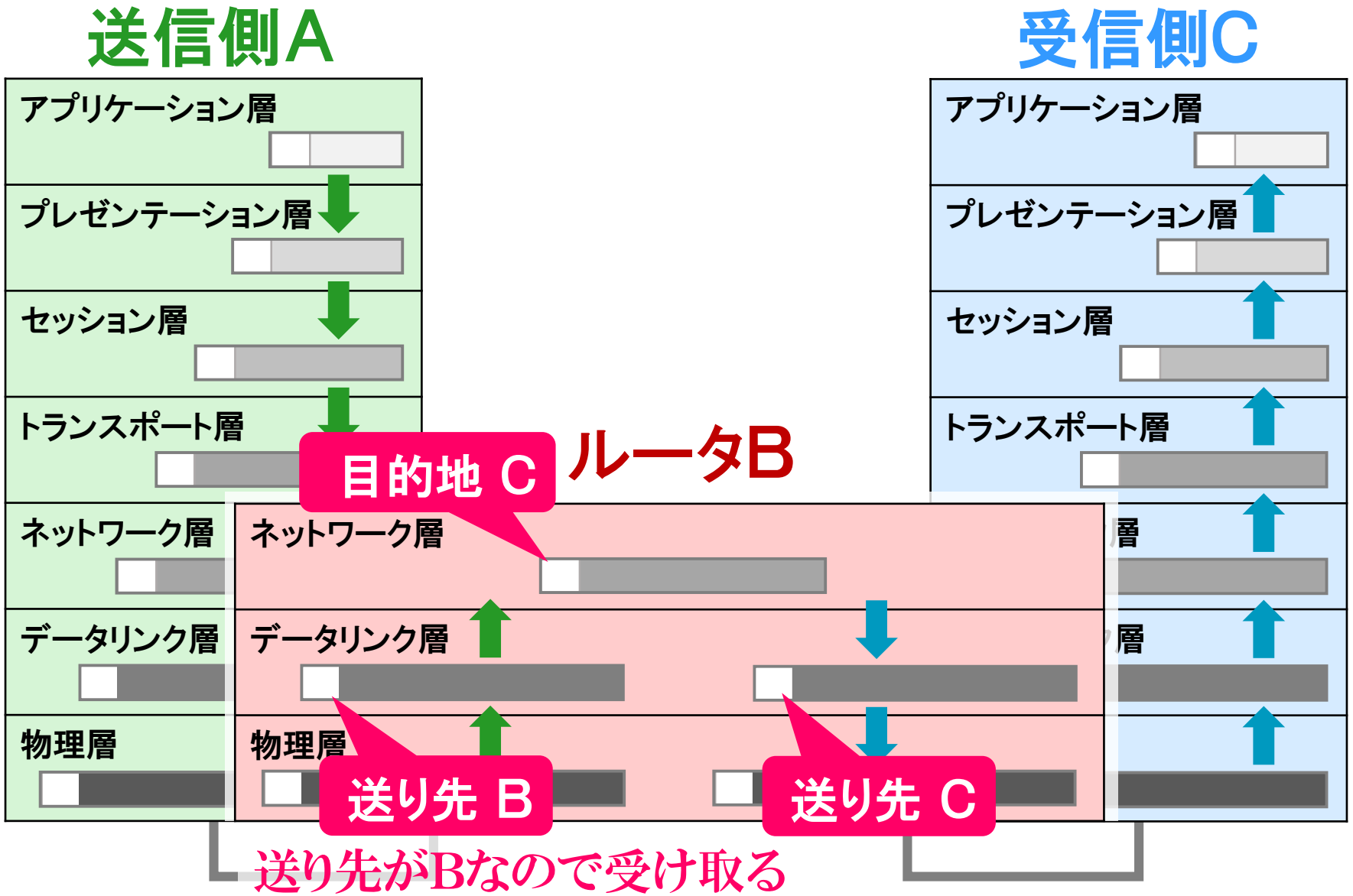
重要

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

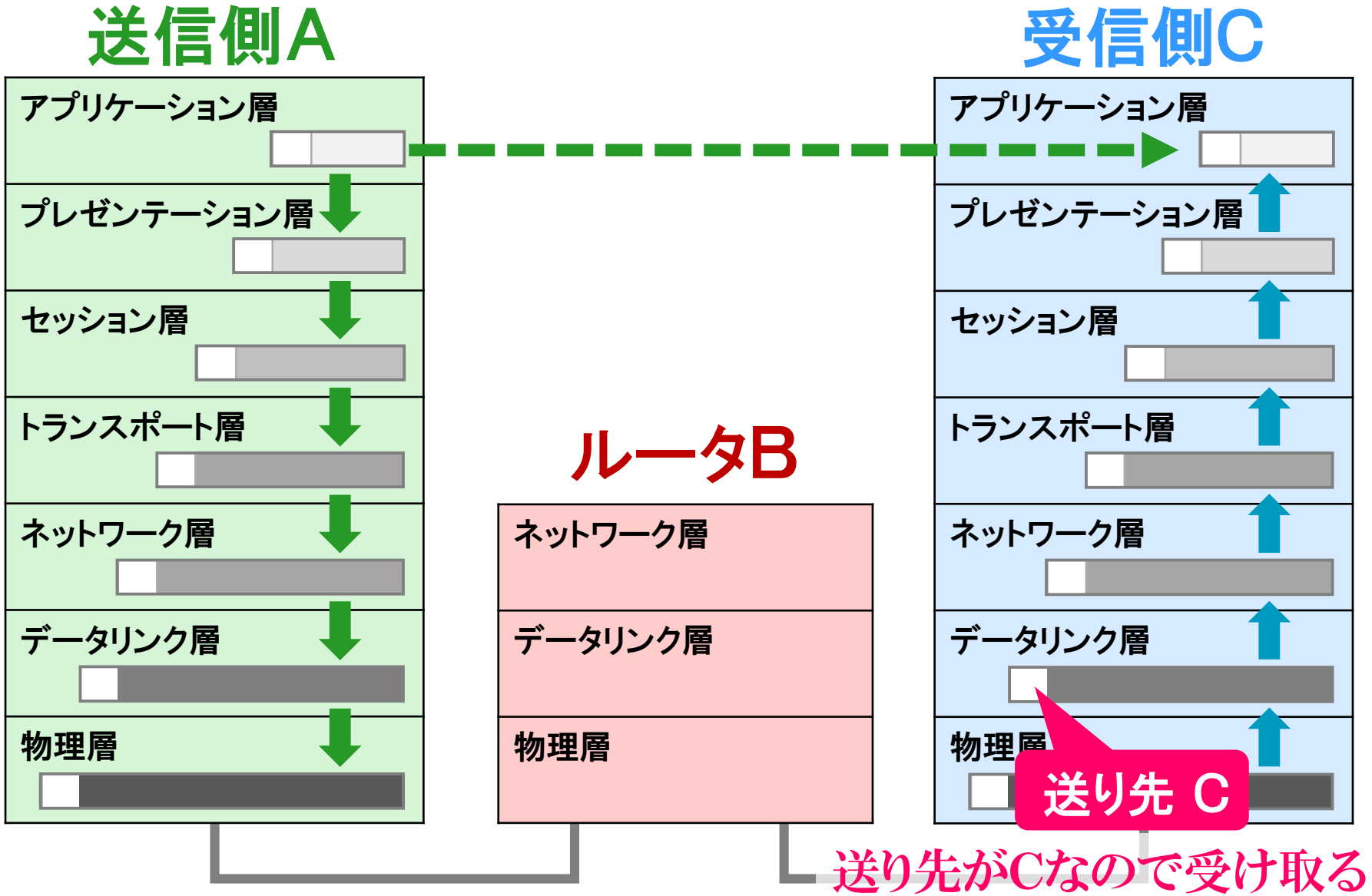
OSI参照モデルによる送受信



OSI参照モデルによる送受信



OSI参照モデルによる送受信



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

2種類のアドレス

✣ MACアドレス（物理アドレス）

データリンク層で利用されるアドレス。

NICに製造時に付けられる。変更はできない。

物理アドレスとも呼ぶ。

✣ IPアドレス（論理アドレス）

ネットワーク層で利用されるアドレス。

接続先のネットワーク内において、個々の機器を識別するために付けられる。

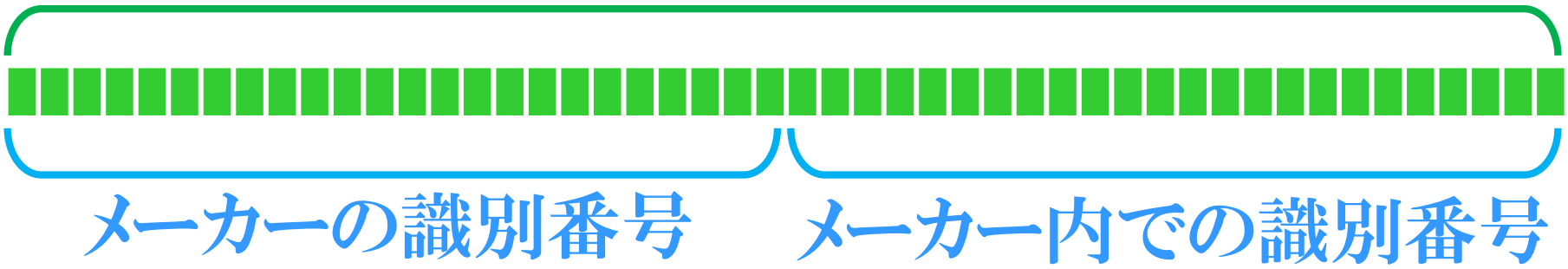
MACアドレス

重要

Media Access Control Address

データリンク層でのノードの識別に利用される。

製造メーカーによってNICに固有のアドレスが書き込まれる。



階層別ネットワーク機器

重要

OSI参照モデル	対応する機器	利用するアドレス
アプリケーション層	ゲートウェイ	IPアドレス
プレゼンテーション層		
セッション層		
トランスポート層		
ネットワーク層	ルータ	
データリンク層	ブリッジ スイッチングハブ	MACアドレス
物理層	リピータ	なし

第1層　物理層

ノード間を物理的に接続するための、
電気的・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。

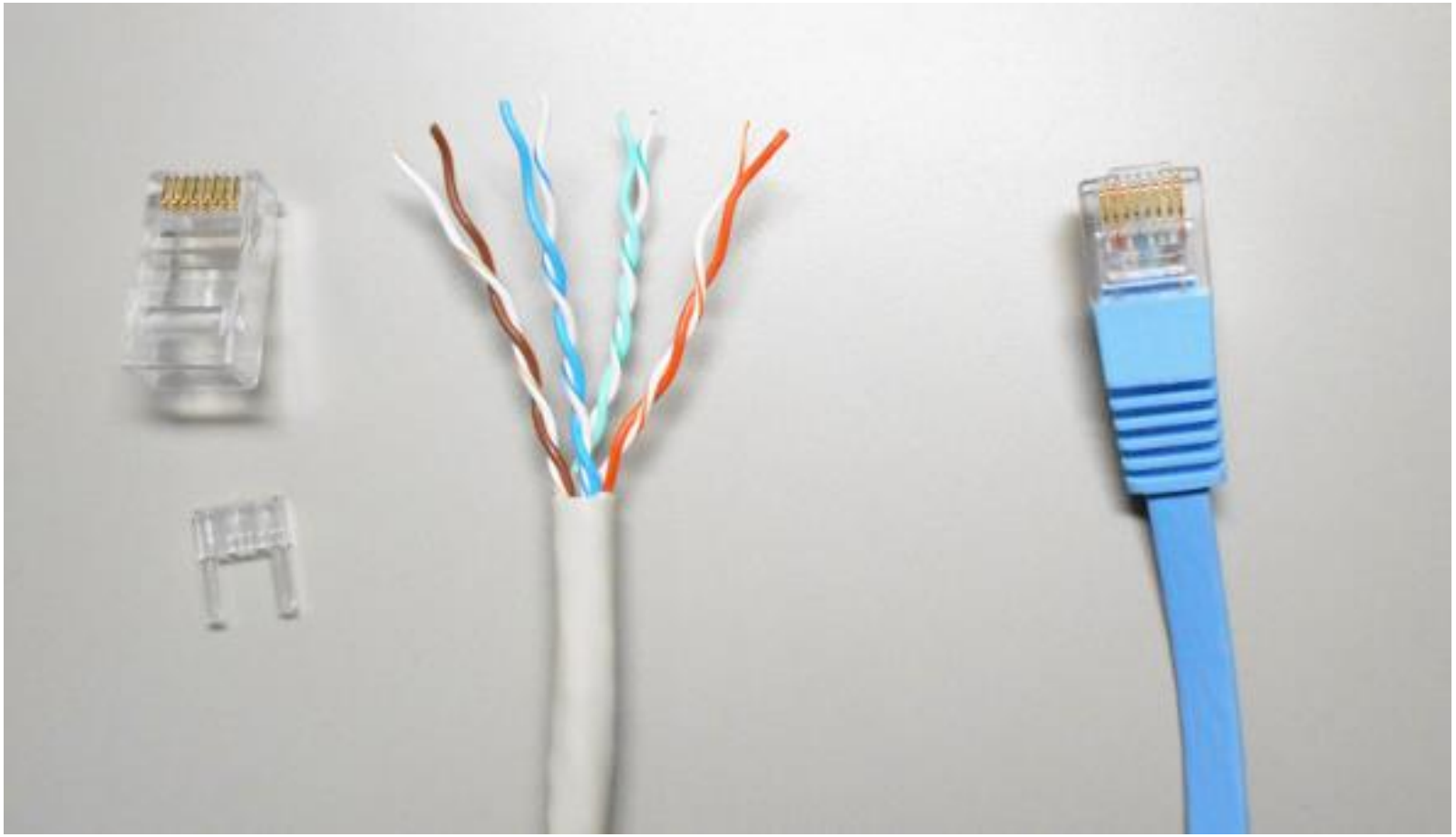
ネットワーク トポロジー

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

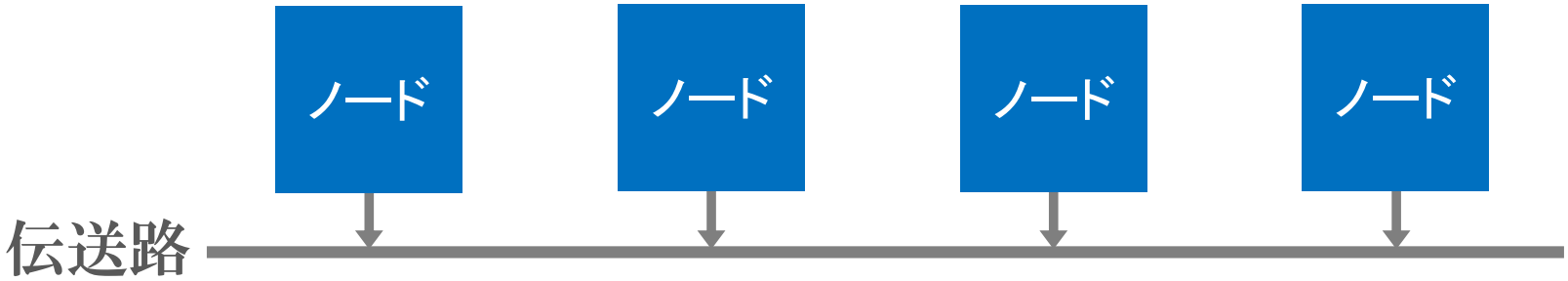
CSMA/CD

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。

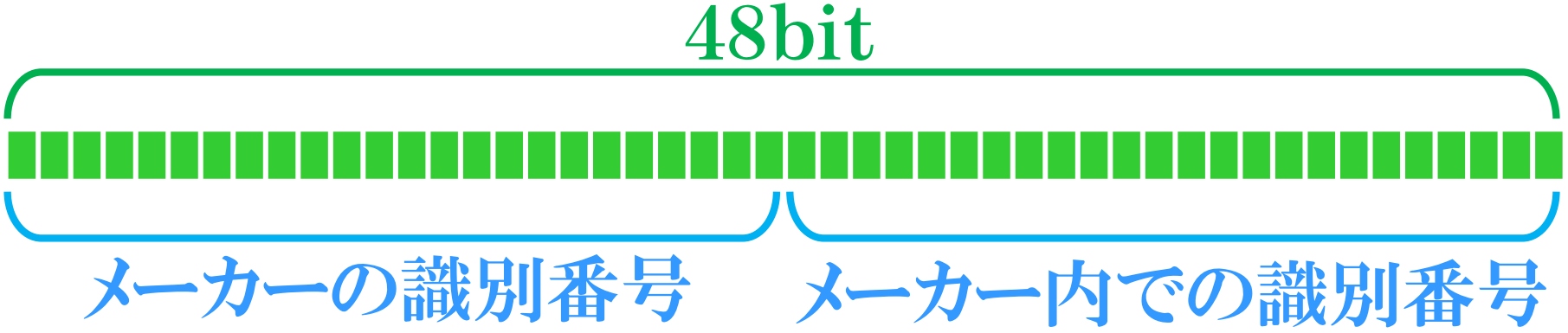
MACアドレス

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。



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）

重要

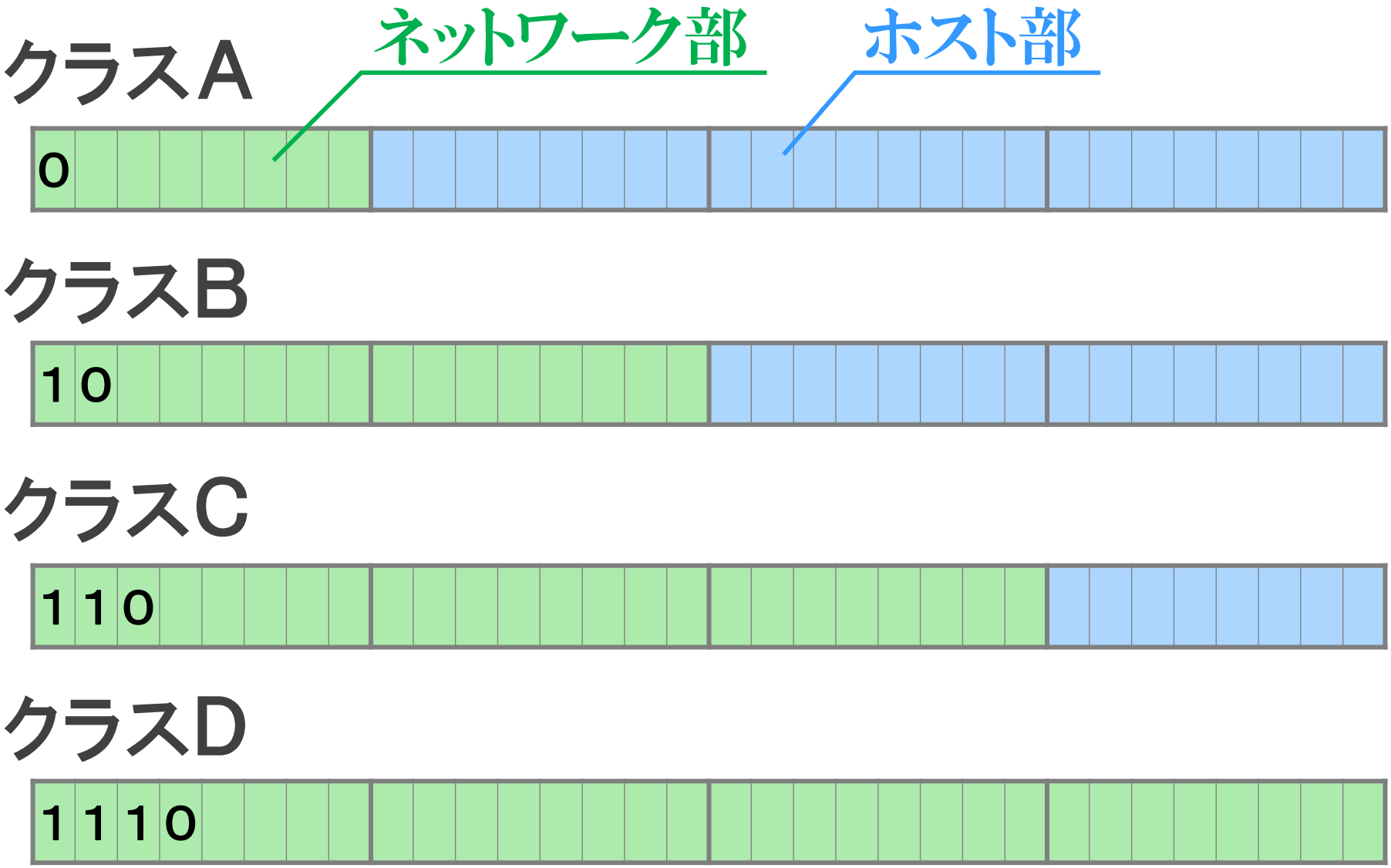
終端ノード間（end-to-end）
の通信を実現する。

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

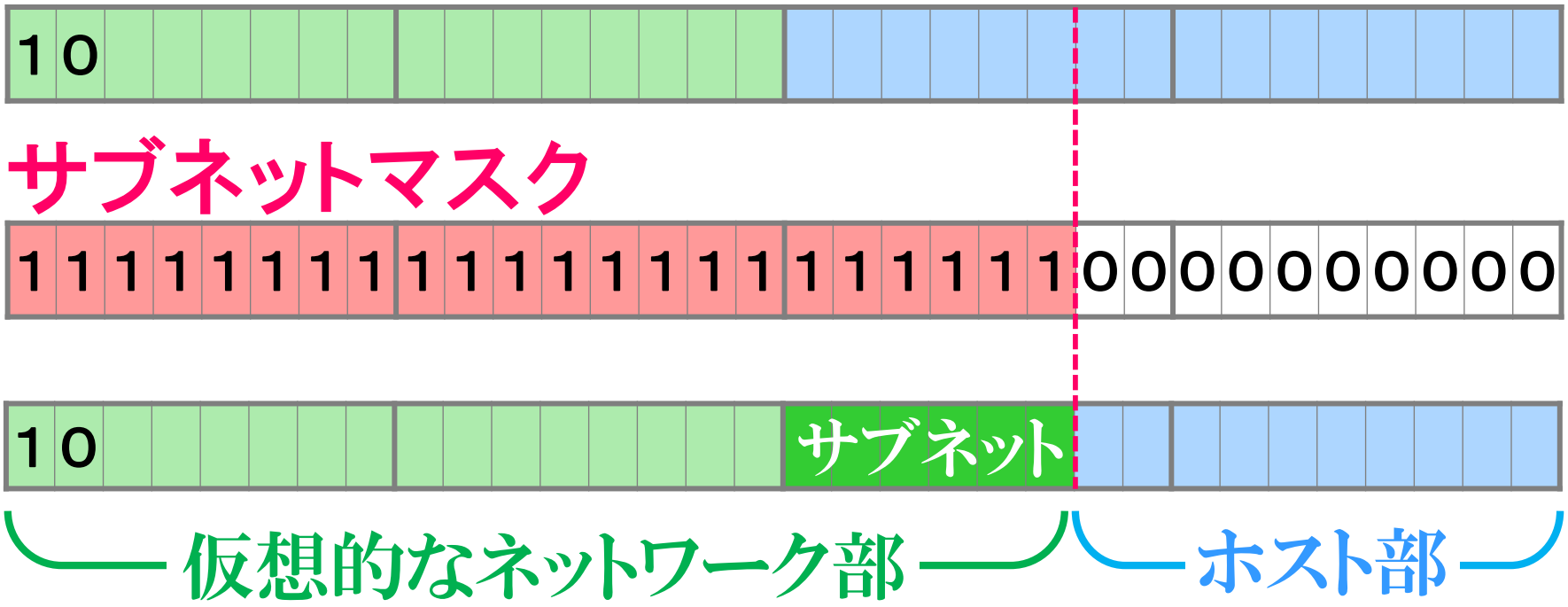


サブネットワーク

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



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　$2^{128} \fallingdotseq 340 \times 10^{36}$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

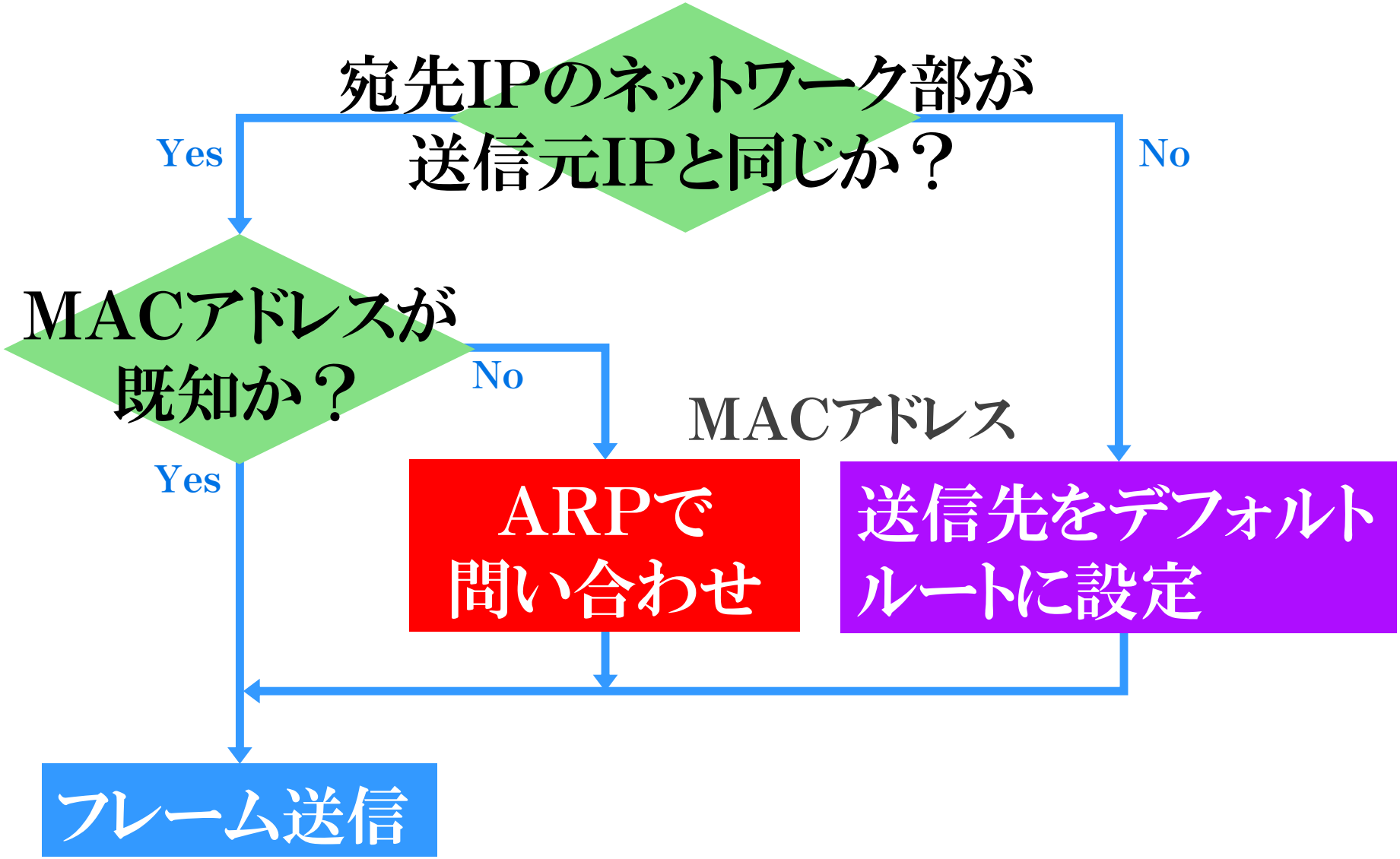
IPアドレスからMACアドレスを知るために、ネットワーク内の全ノードに問い合わせるプロトコル。

ネットワーク層のプロトコル。

ARPパケット

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)

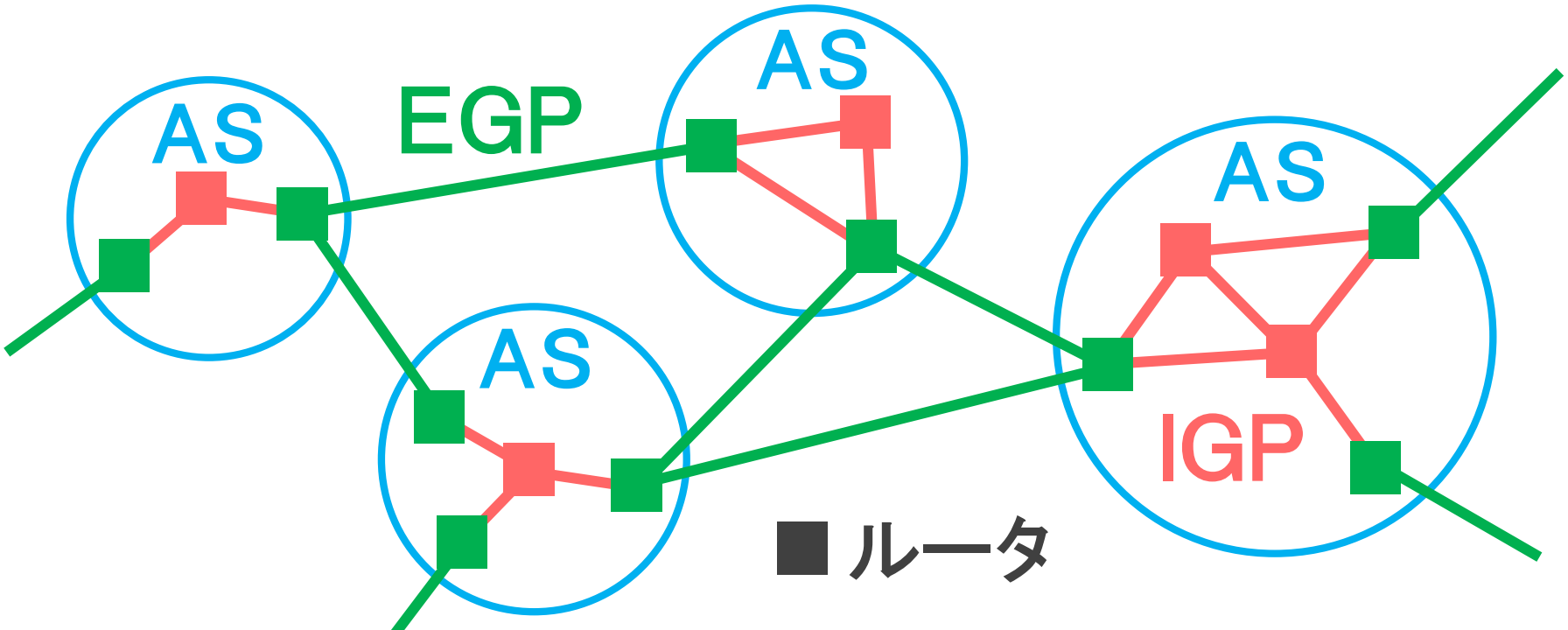
受信したパケットの宛先アドレスと**経路制御表(ルーティングテーブル)**を比較して、次の送り先のルータを決定する。

- **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

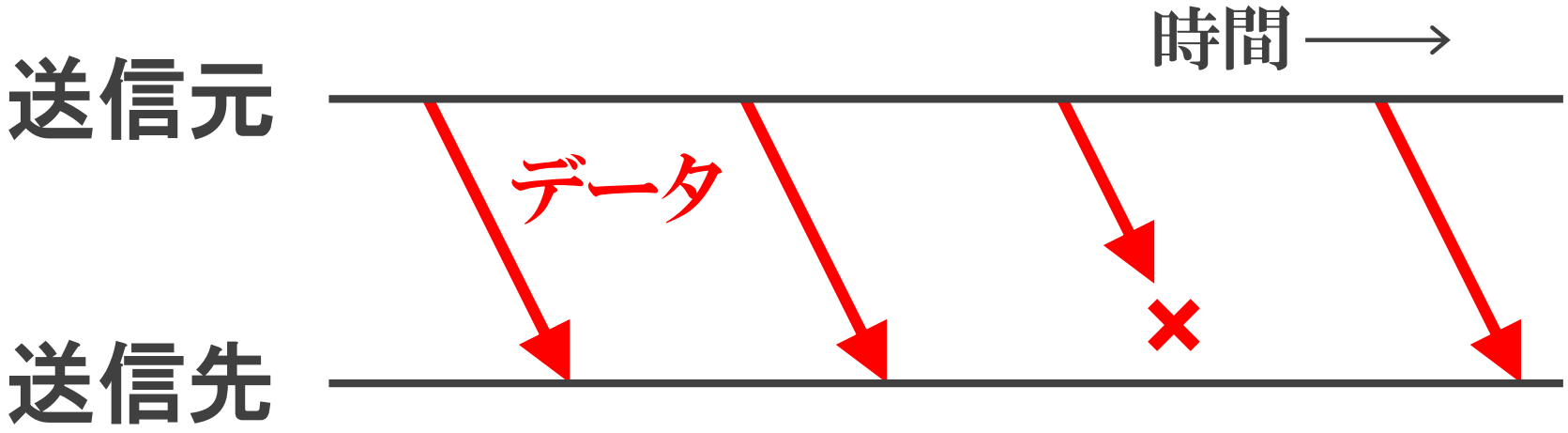
重要

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。

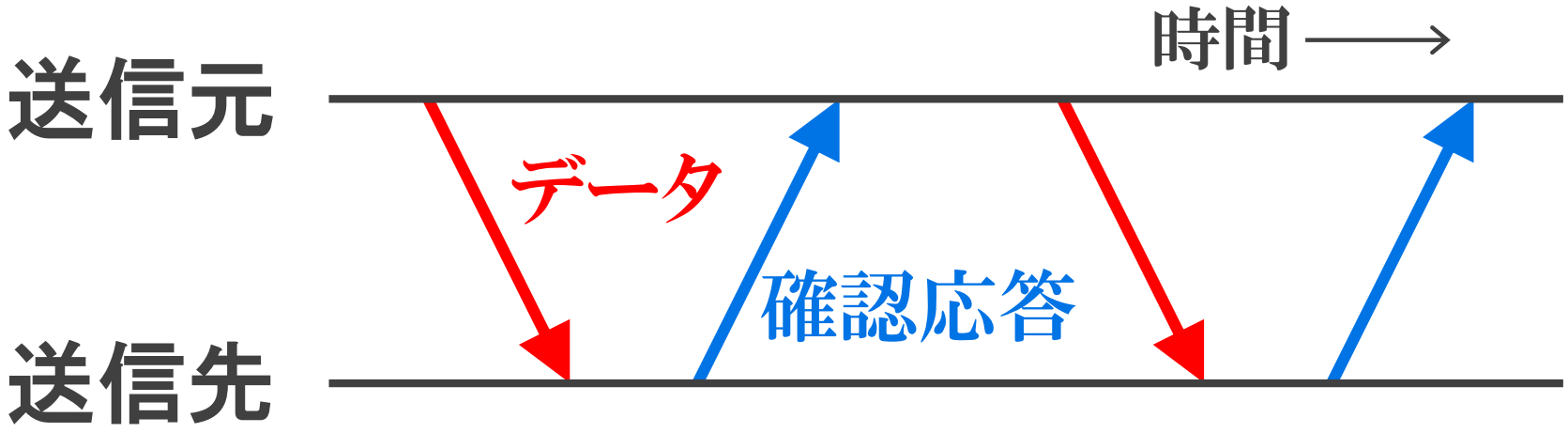
UDP

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

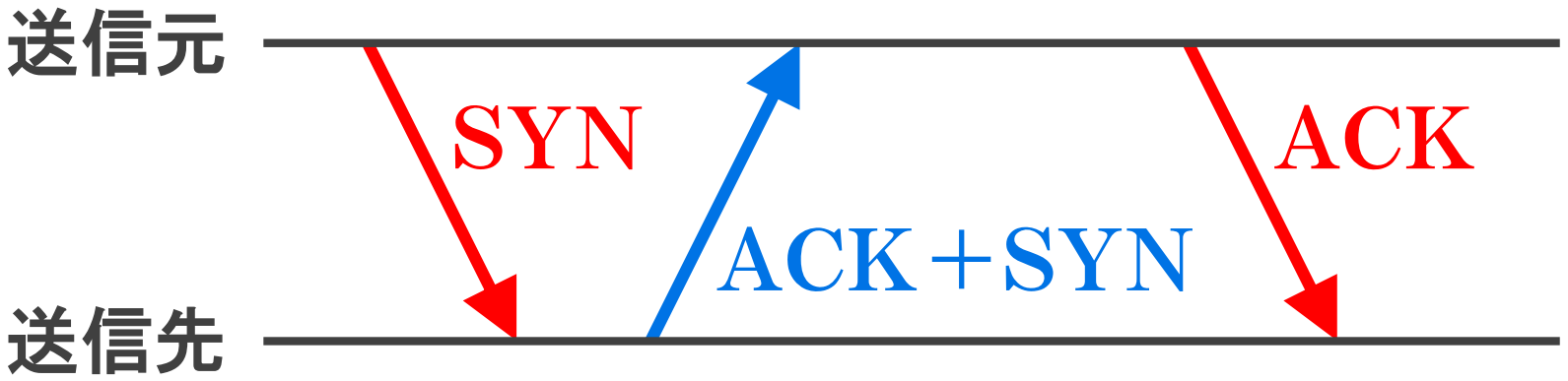
<table>
<tr><td colspan="3">送信側ポート番号(16bit)</td><td colspan="3">受信側ポート番号(16bit)</td></tr>
<tr><td colspan="6">シーケンス番号(32bit)</td></tr>
<tr><td colspan="6">確認応答番号(32bit)</td></tr>
<tr><td rowspan="2">データオフセット(4bit)</td><td rowspan="2">予約(6bit)</td><td colspan="4">コントロールフラグ(6bit)</td><td rowspan="2">ウインドウサイズ(16bit)</td></tr>
<tr><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td></tr>
<tr><td colspan="3">チェックサム(16bit)</td><td colspan="3">緊急ポインタ(16bit)</td></tr>
<tr><td colspan="5">オプション</td><td>パディング</td></tr>
<tr><td colspan="6">データ</td></tr>
</table>

TCP コントロールフラグ

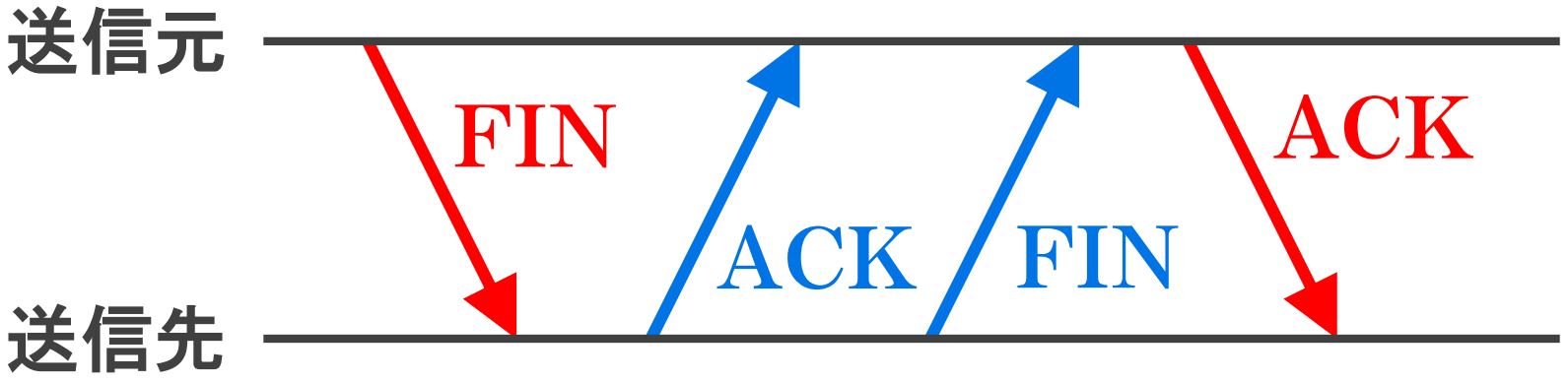
コントロールフラグ		役割・意味
URG	Urgent	緊急に処理すべきデータが含まれている
ACK	Acknowledgment	確認応答
PSH	Push	アプリケーション層へすぐにデータを渡す
RST	Reset	通信の強制切断
SYN	Synchronize	通信開始の要求
FIN	Fin	通信終了の要求

TCP コネクション管理

✤ コネクションの確立

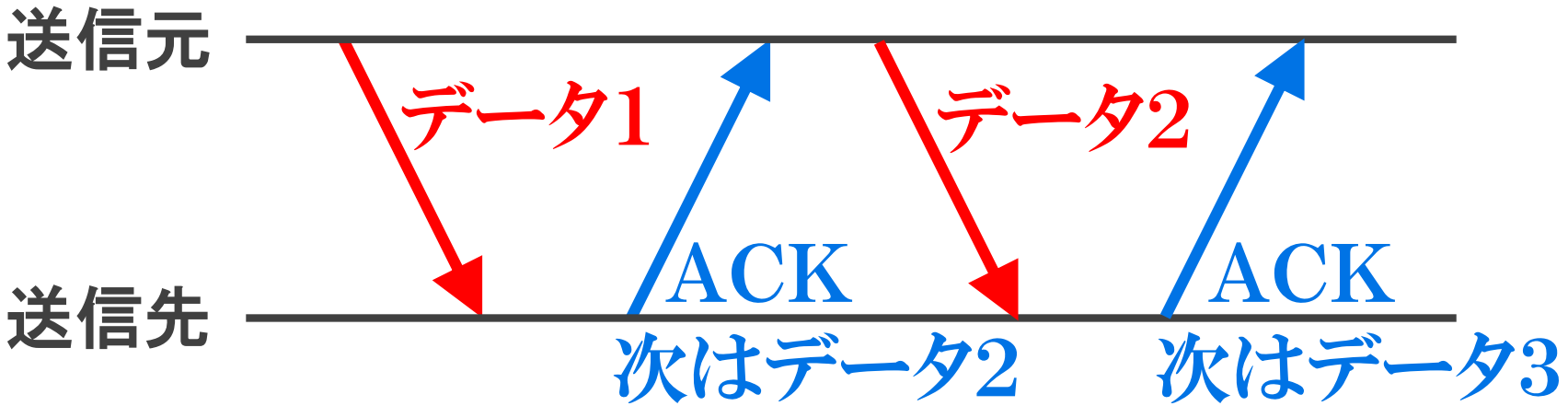


✤ コネクションの切断

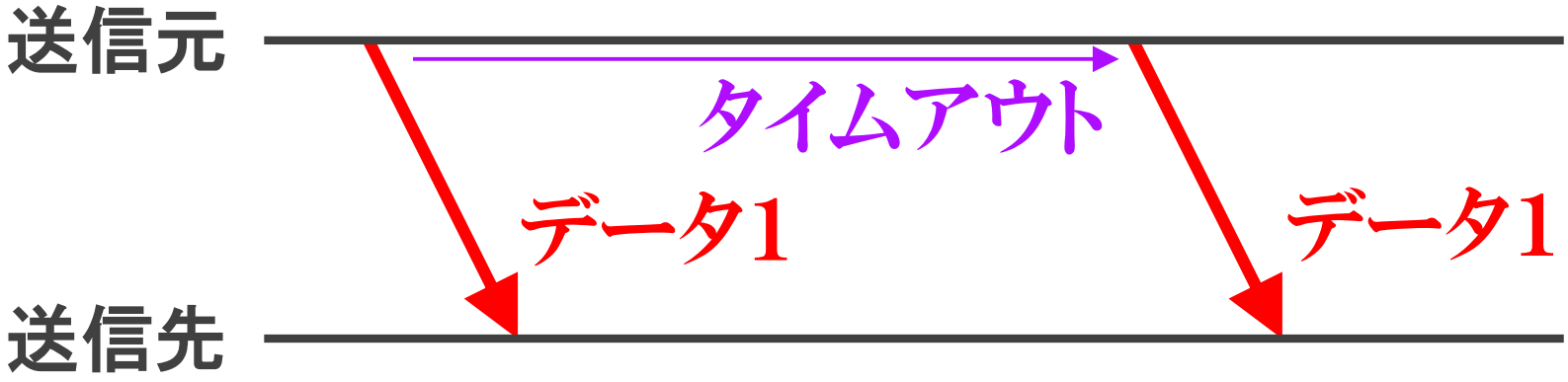


TCP　セグメントの送信

✣ 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

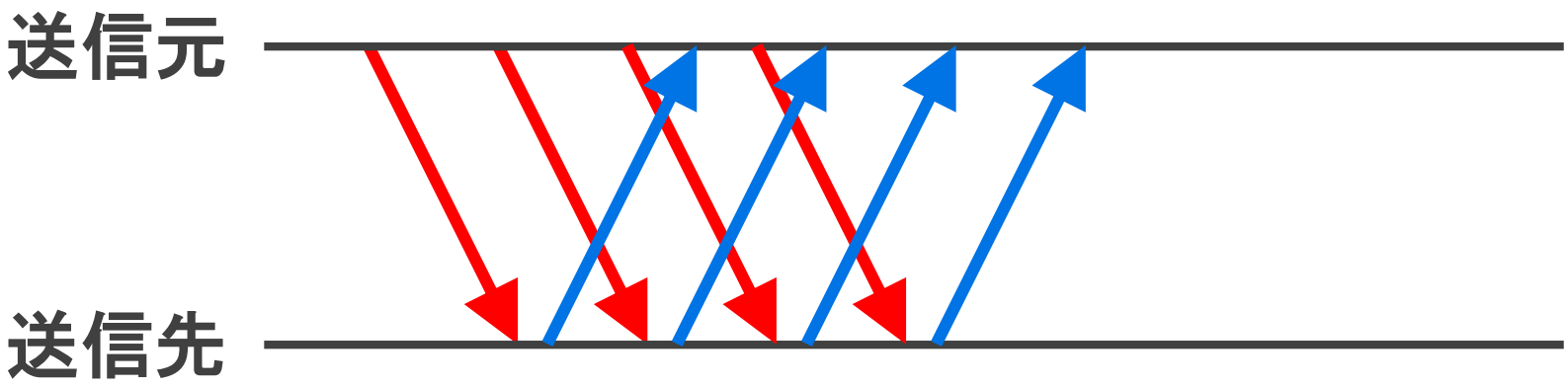
次に送信してもらうデータの先頭が、
全データの何byte目になるかを表す。

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。

ウインドウサイズ

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



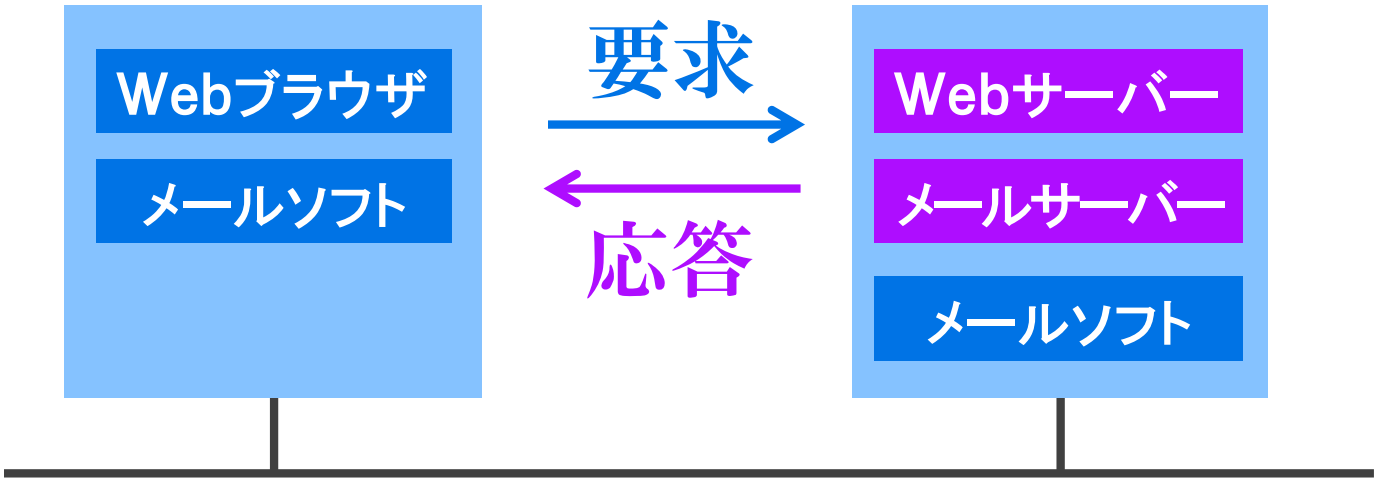
クライアント・サーバー モデル

- **サーバー**

  サービスを提供するプログラム

- **クライアント**

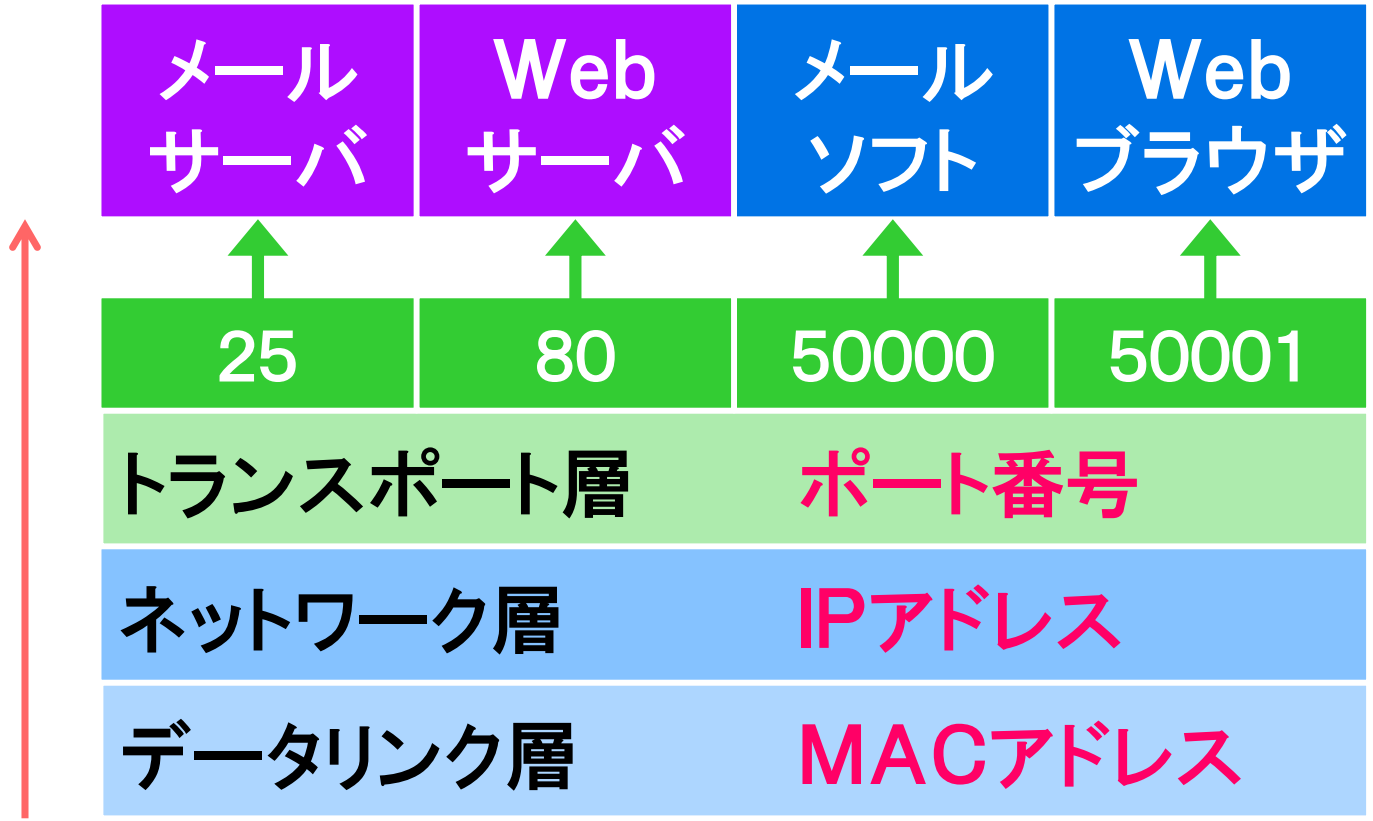
  サービスを受けるプログラム



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／NAPT
- ICMP
- ARP

DNS

重要

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。

UDPを使用する。ポート番号は53。

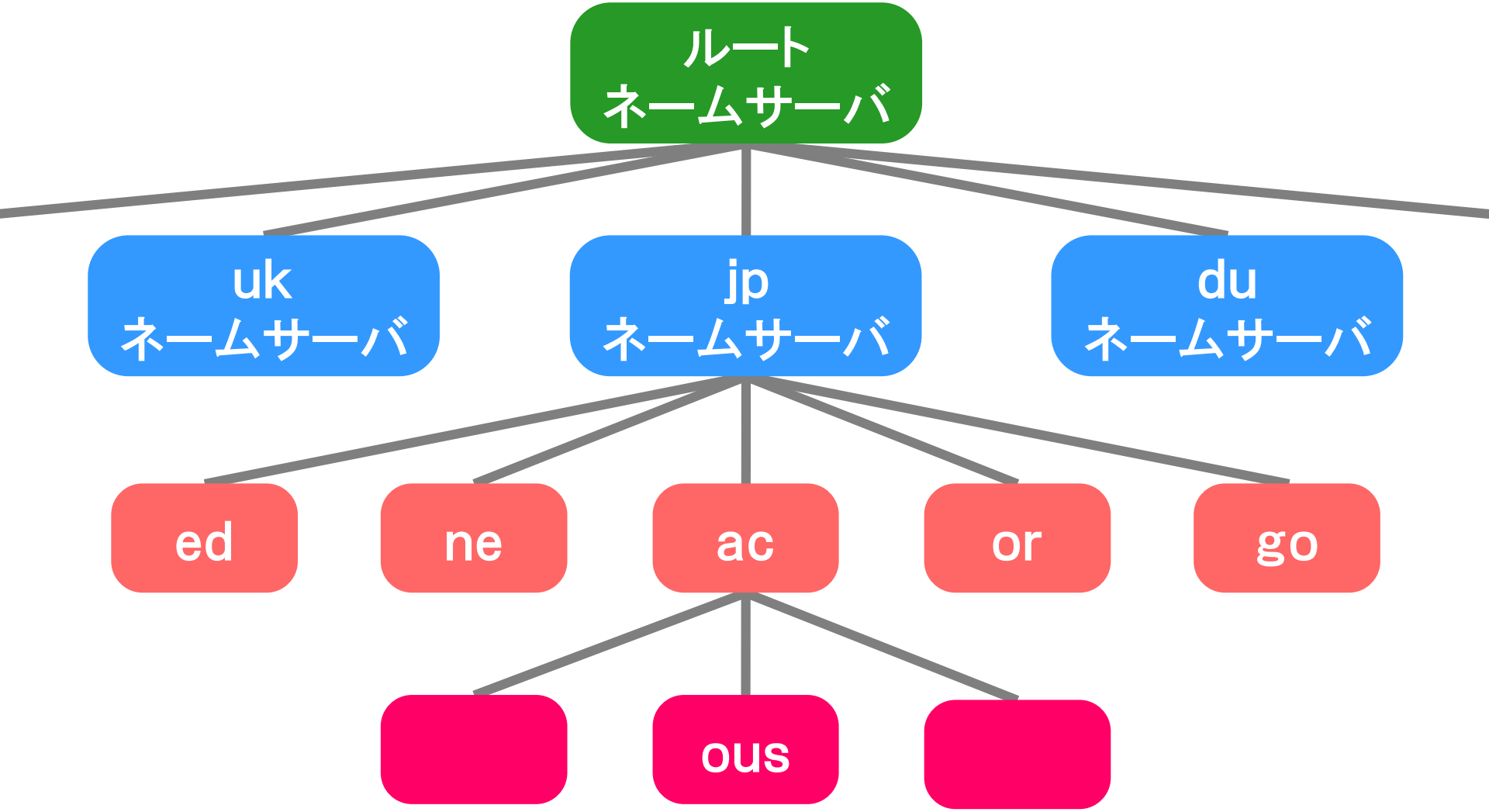
ドメイン名

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。

UDPを使用する。ポート番号は67，68。

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サーバーが確認応答パケットを送り返して、通信が完了する。

ICMP

Internet Contorl 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。

TCP/IP参照モデル

重要

OSI参照モデル	TCP/IP参照モデル
7　アプリケーション層	4　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　トランスポート層
3　ネットワーク層	2　インターネット層
2　データリンク層	1　ネットワークインタフェース層
1　物理層	

第5層～第7層

第5層 セッション層

通信の開始と終了の手順を定める。

第6層 プレゼンテーション層

データの符号化や変換の方式を定める。

第7層 アプリケーション層

アプリケーションごとの通信方式を定める。ユーザと接する部分。

アプリケーションプロトコル

アプリケーションに特化した通信方式を定めたプロトコル。

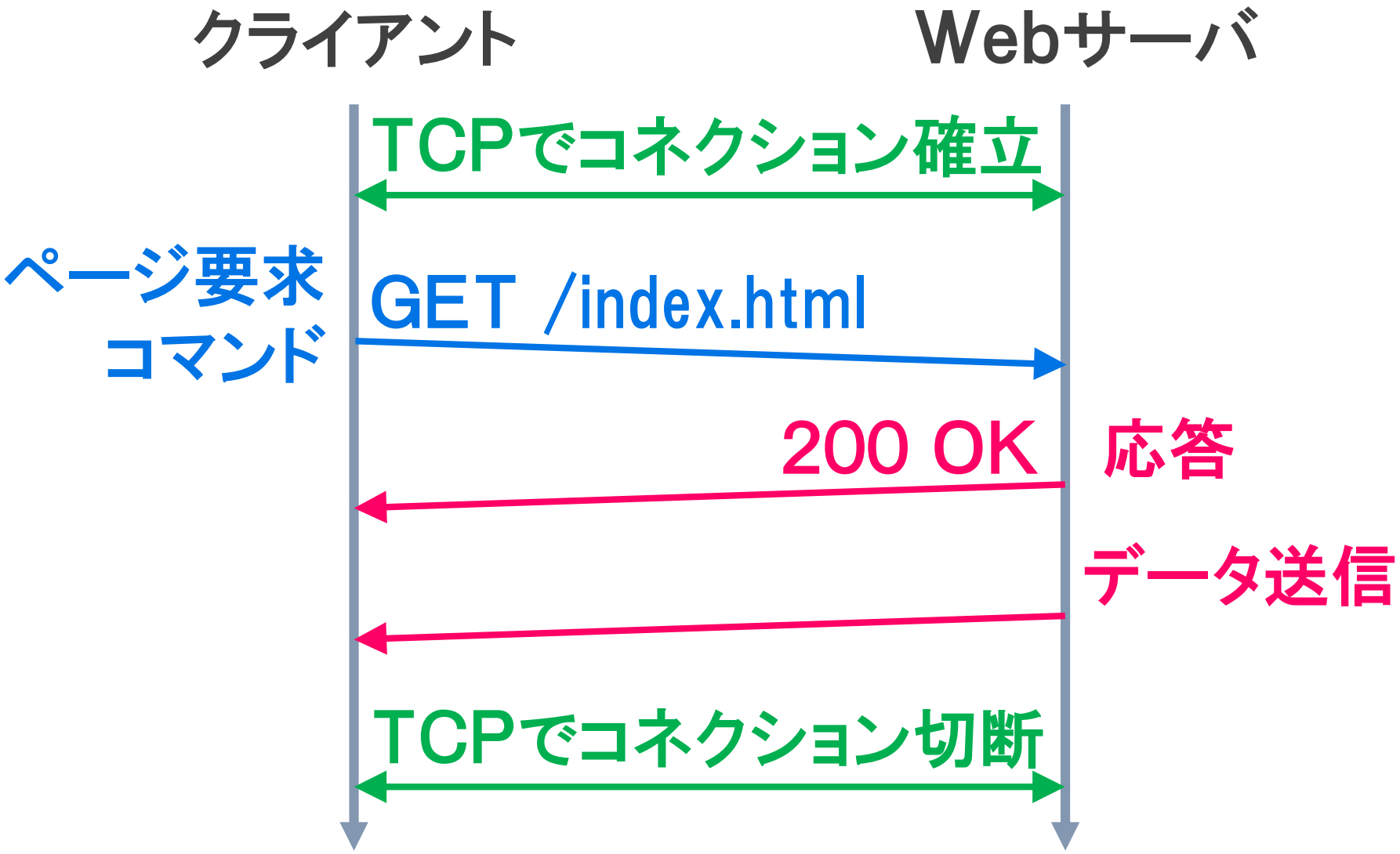
通信サービスごとにプロトコルが異なる。

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の機能がアプリケーションプログラムに組み込まれる。

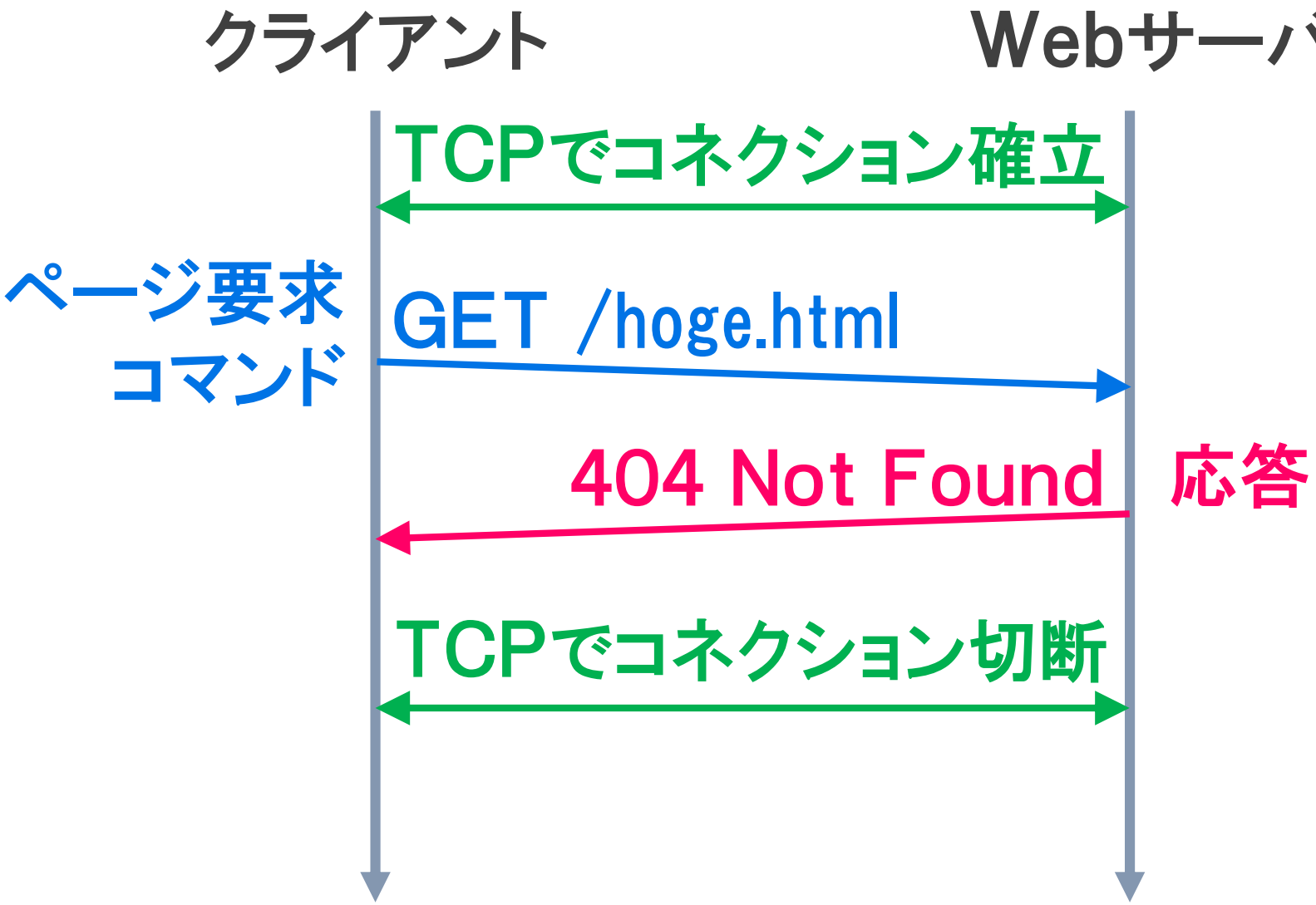
アプリケーションプロトコル例

プロトコル名	サービス内容
TELNET	遠隔ログイン
SSH	遠隔ログイン（暗号化通信）
FTP	ファイル転送
SMTP	電子メールの配信
POP	電子メールの受信（クライアントで管理）
IMAP	電子メールの受信（サーバで管理）
HTTP	Webページの転送
HTTPS	Webページの転送（暗号化通信）
DNS	ドメイン名管理

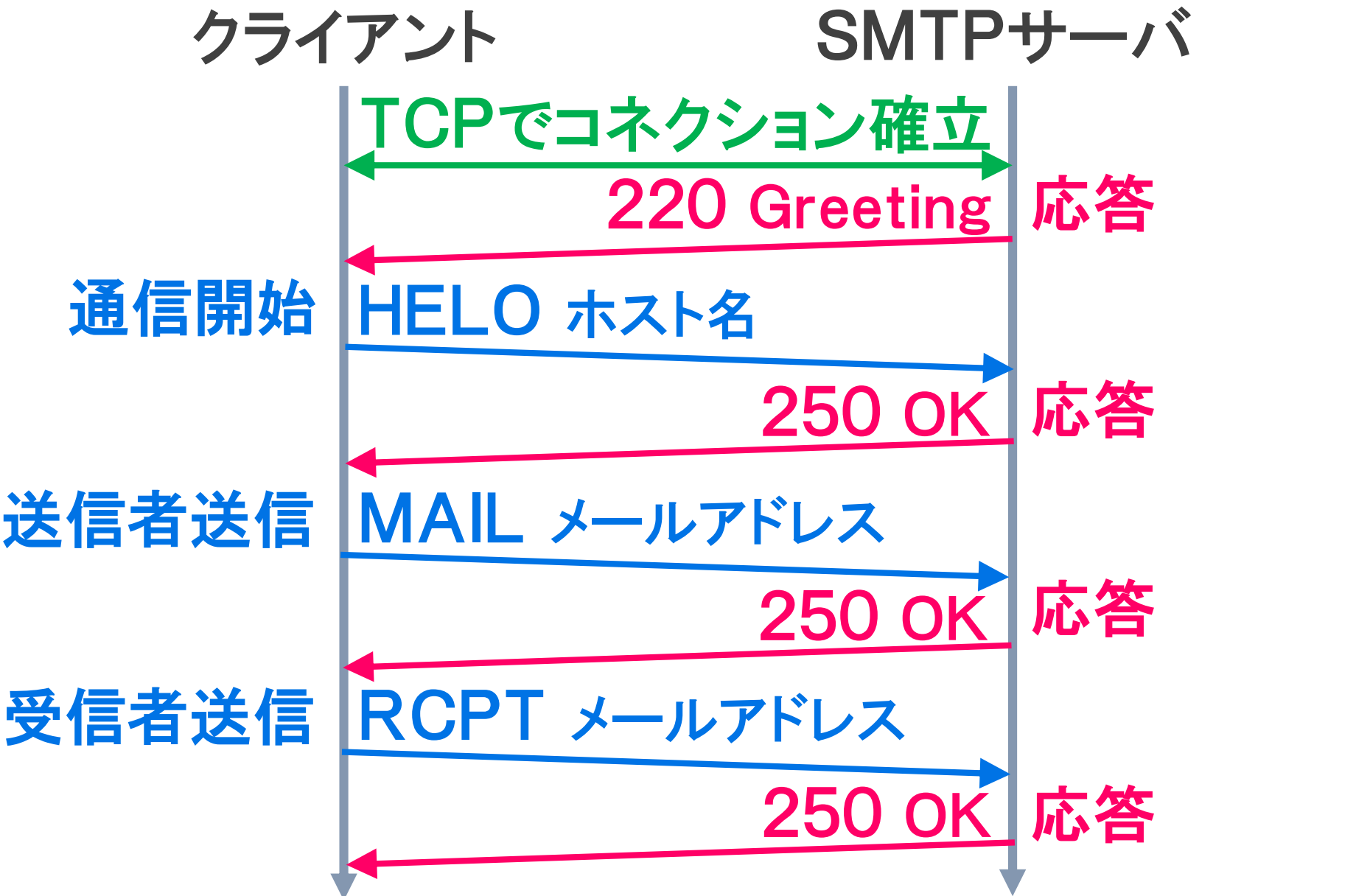
HTTP


クライアント
Webサーバ
TCPでコネクション確立
ページ要求
コマンド
GET /index.html
200 OK
応答
データ送信
TCPでコネクション切断

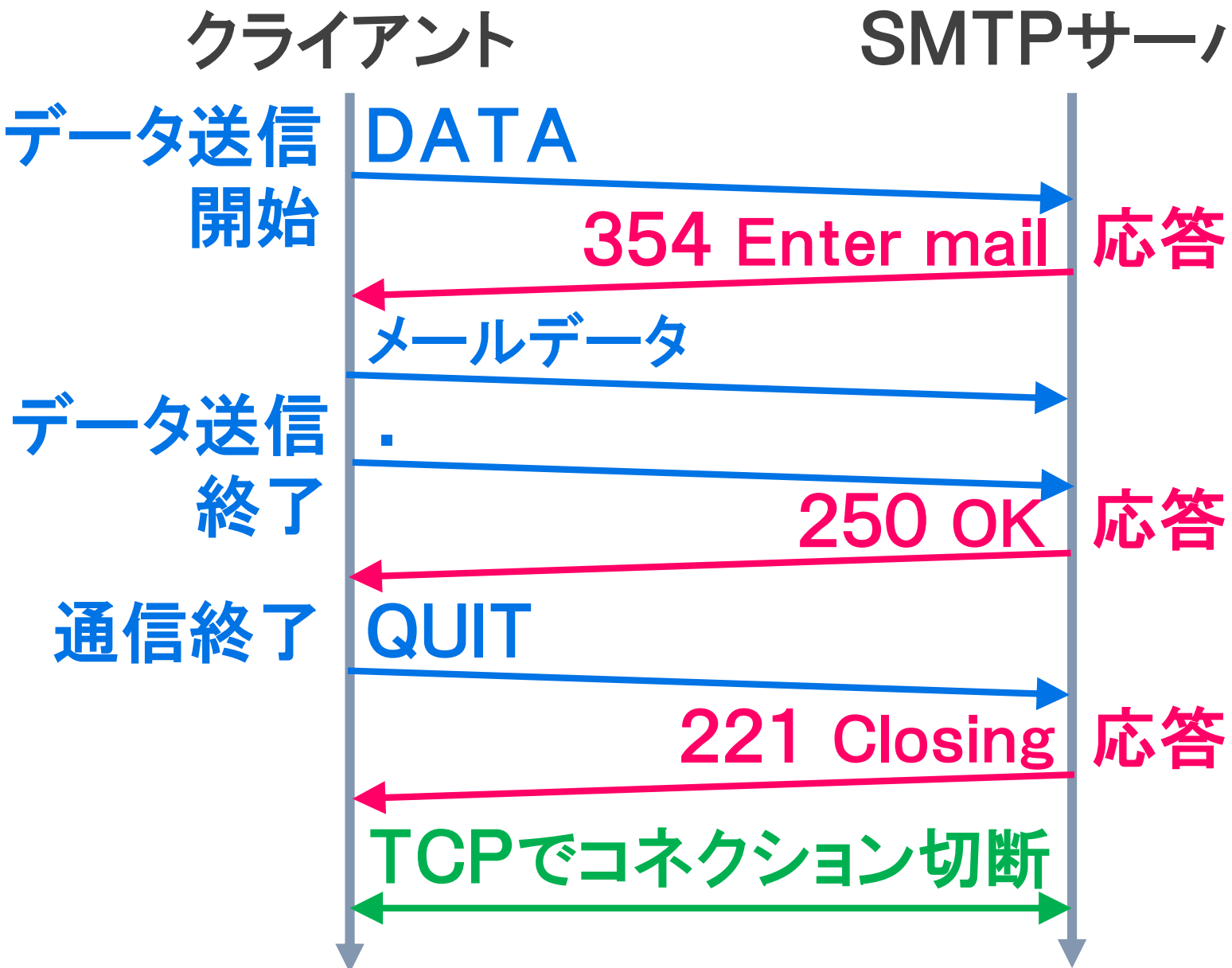
HTTP(ページが存在しない場合)



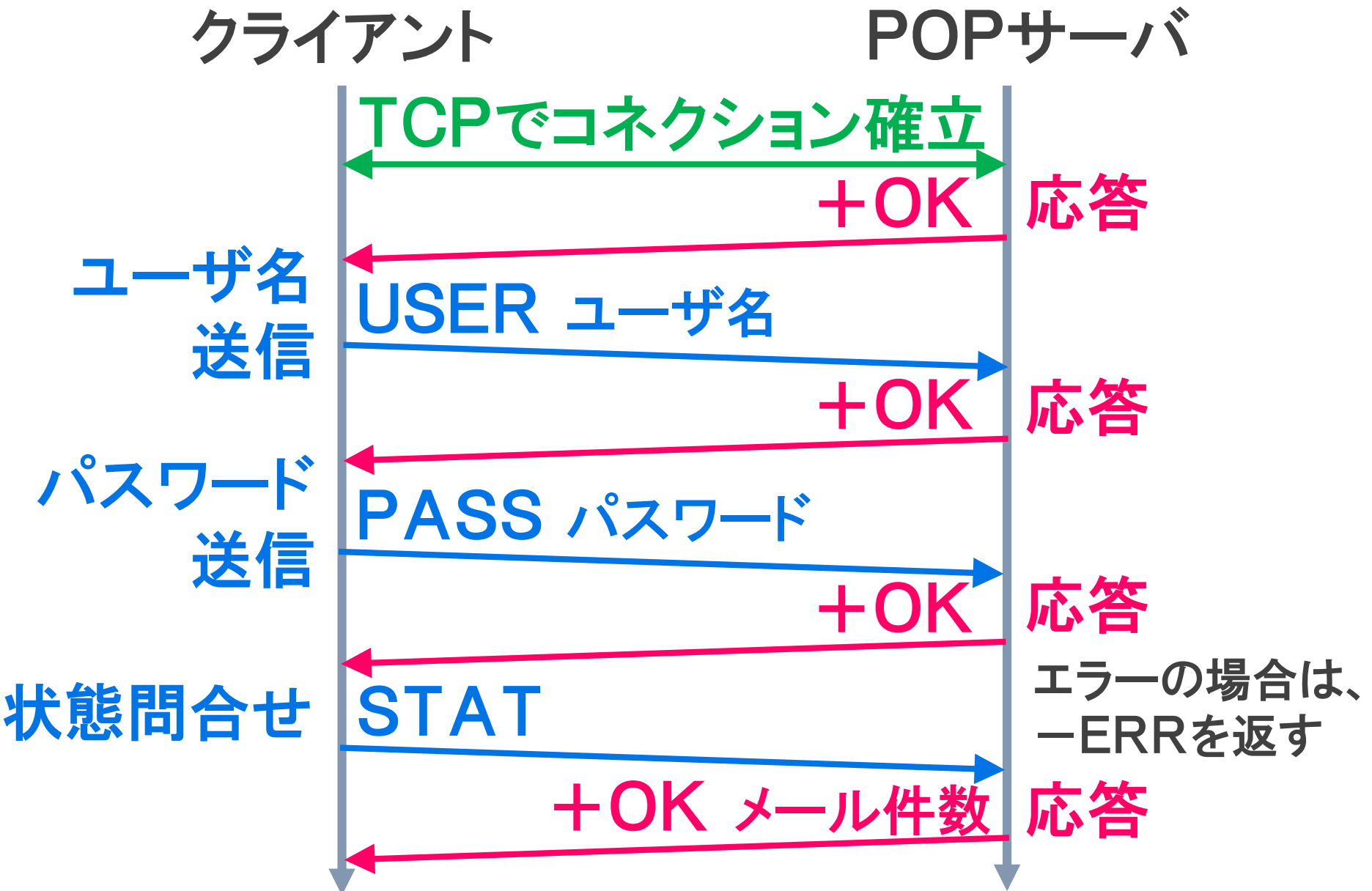
SMTP①


クライアント
SMTPサーバ
TCPでコネクション確立
220 Greeting
応答
通信開始
HELO ホスト名
250 OK
応答
送信者送信
MAIL メールアドレス
250 OK
応答
受信者送信
RCPT メールアドレス
250 OK
応答

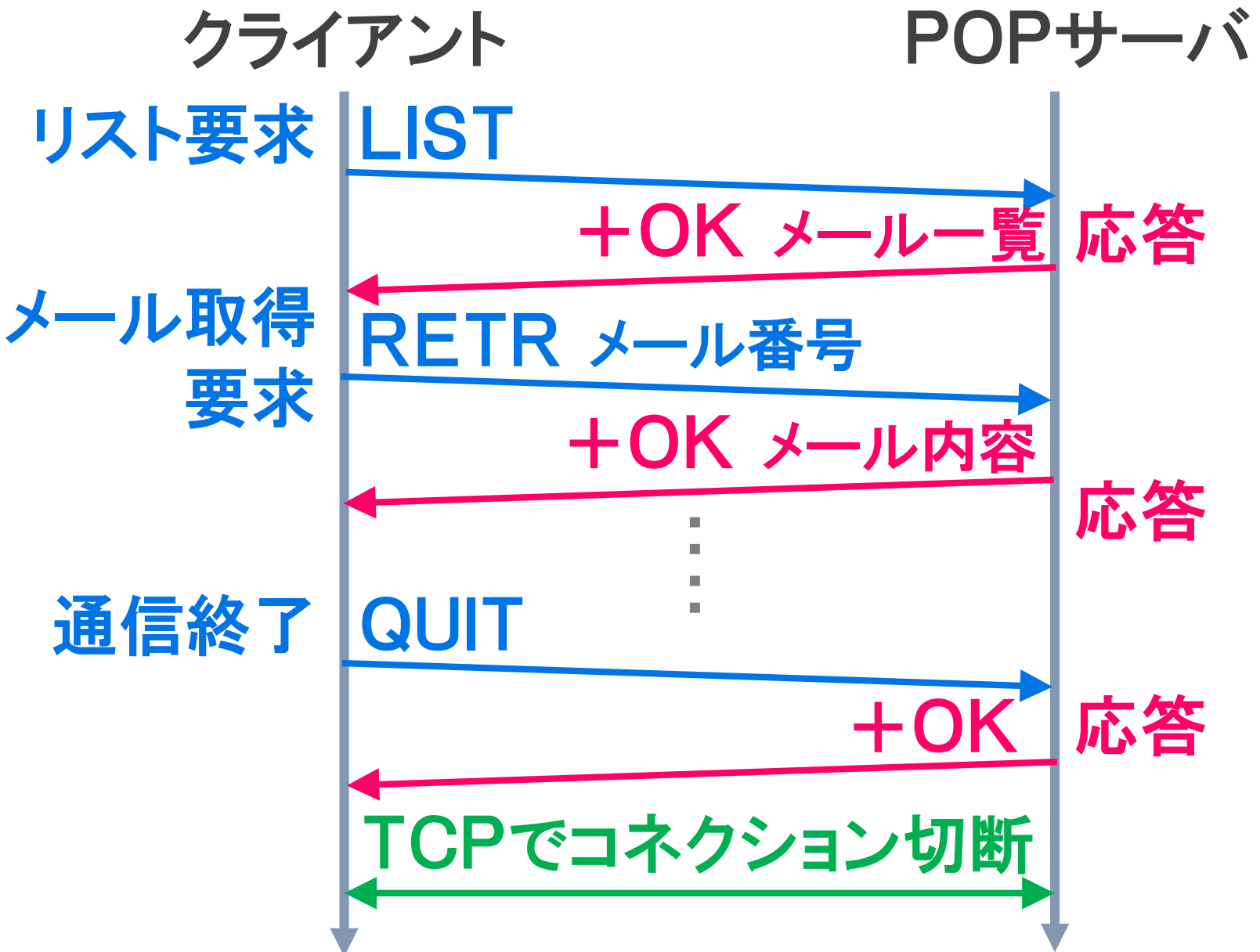
SMTP②


クライアント
SMTPサーバ
データ送信開始
DATA
354 Enter mail
応答
メールデータ
データ送信終了
.
250 OK
応答
通信終了
QUIT
221 Closing
応答
TCPでコネクション切断

POP①


クライアント
POPサーバ
TCPでコネクション確立
＋OK
応答
ユーザ名
送信
USER ユーザ名
＋OK
応答
パスワード
送信
PASS パスワード
＋OK
応答
状態問合せ
STAT
エラーの場合は、
－ERRを返す
＋OK メール件数
応答

POP②


クライアント
POPサーバ
リスト要求
LIST
＋OK メール一覧
応答
メール取得要求
RETR メール番号
＋OK メール内容
応答
通信終了
QUIT
＋OK
応答
TCPでコネクション切断

アドレス変換

プライベートアドレスとグローバルアドレスの変換を行う。

- NAT
- NAPT
- ポートフォワーディング

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。

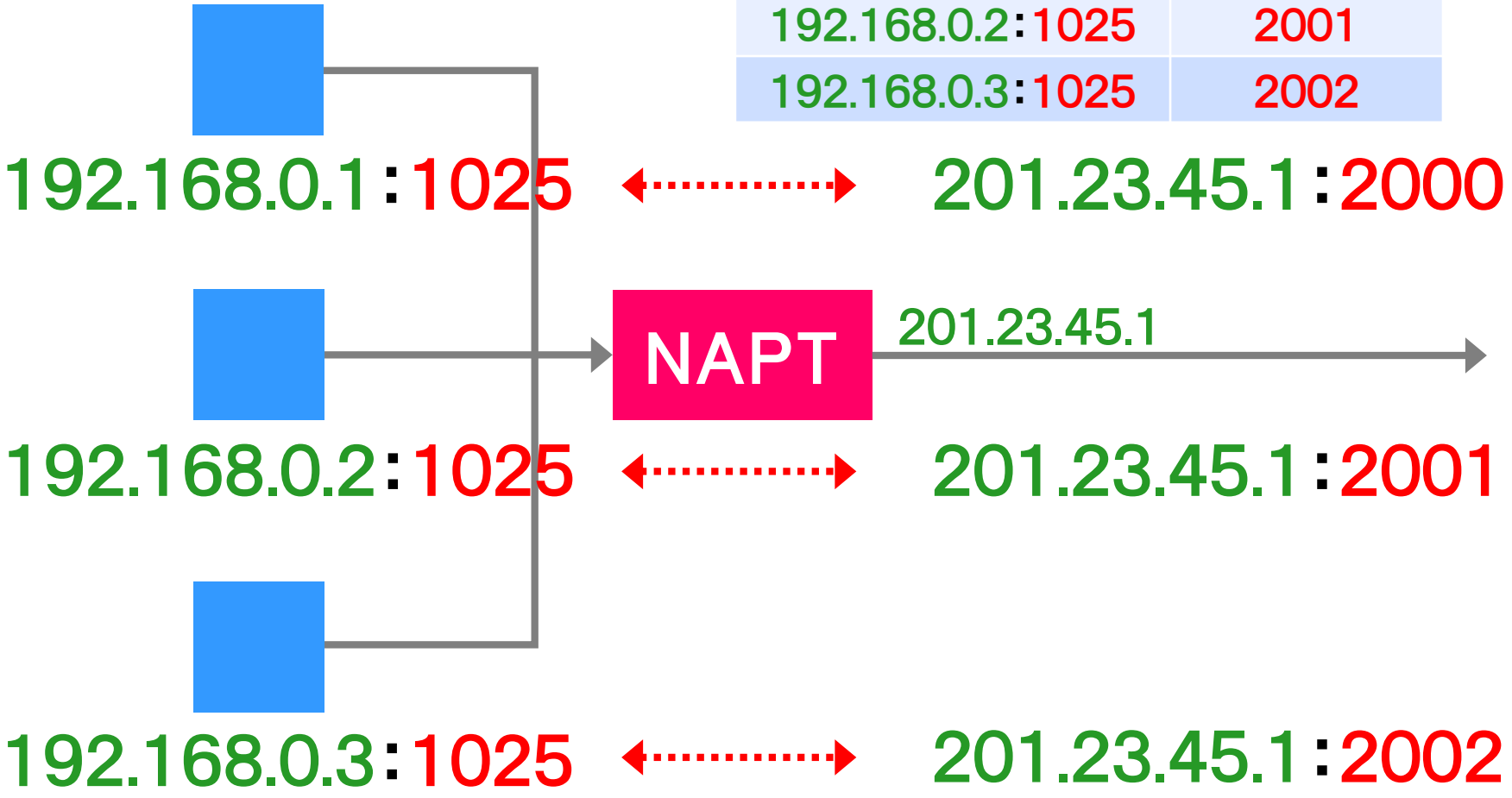
NATのIPアドレス変換の機能に加えて、ポート番号の変換も行う。

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

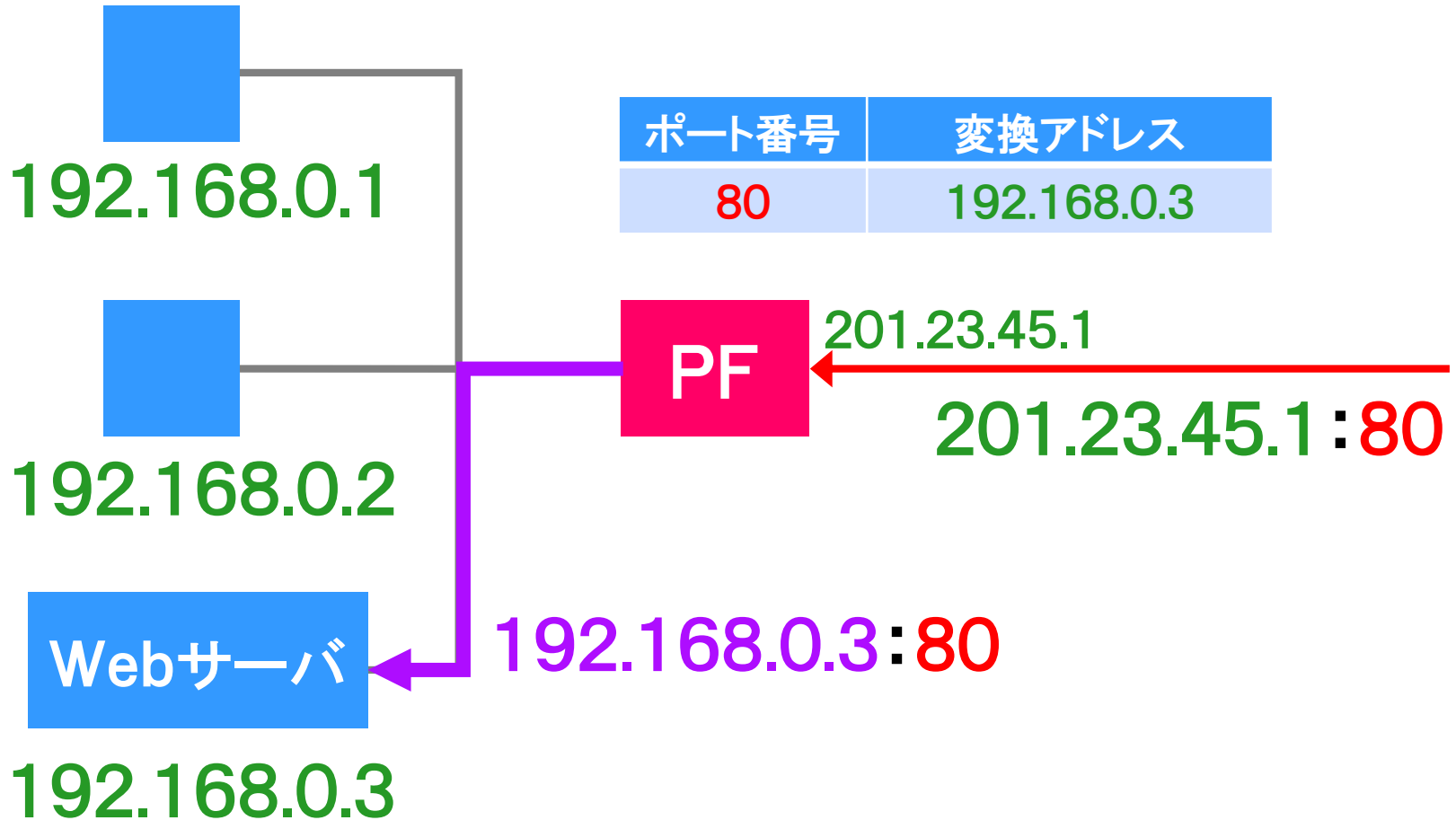


ポートフォワーディング

Port forwarding

特定のポート番号宛にインターネット側から届いたパケットを、プライベートネットワーク内のあらかじめ定めたノードへ転送する機能。

ポートフォワーディングのしくみ



プライベートネットワーク内のサーバを
インターネットからアクセスできる。

ファイアウォール

外部のネットワークの攻撃からコンピュータを守る仕組み。

外部から送られてきたパケットを調べ、条件に合うパケットだけを通過させる。

トランスポート層	許可されてないポート宛のパケットを破棄する。通信が確立していない相手からのパケットを破棄する。
ネットワーク層	許可されていないIPアドレスのパケットを破棄する。

DMZ（非武装地帯）

Demilitarized Zone

外部ネットワークからも内部ネットワークからも隔離したネットワーク。

外部へ公開するサーバを置く。万が一、サーバが攻撃を受けても、内部ネットワークには被害が及ばないようにする。

無線通信

分類	通信距離	技術名称
無線PAN (Personal Area Network)	10m前後	Bluetooth など
無線LAN (Local Area Network)	100m前後	WiFi
無線MAN (Metropolitan Area Network)	数km ～100km	WiMAX
無線WAN (Wide Area Network)	–	3G、4G LTE

無線LAN

アクセスポイント

無線LANと有線LANの接続、無線LANクライアント同士の接続を行う機器。

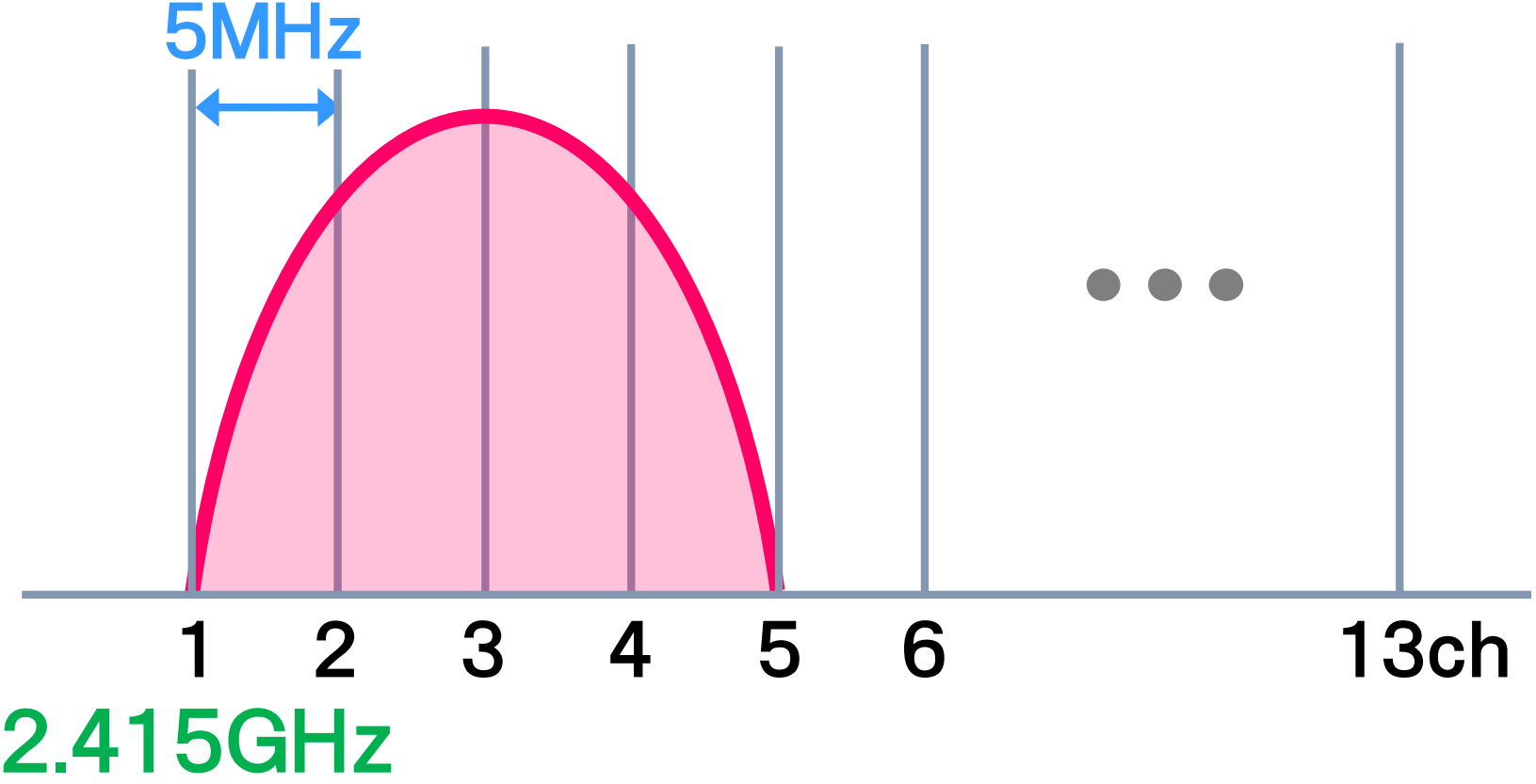
機種によってブリッジやルータの機能を持つ。

無線LANの規格

規格	最大速度	周波数
IEEE802.11	2Mbps	2.4GHz
IEEE802.11b	11Mbps	2.4GHz
IEEE802.11a	54Mbps	5GHz
IEEE802.11g	54Mbps	2.4GHz
IEEE802.11n	600Mbps	2.4GHz／5GHz
IEEE802.11ac	6.9Gbps	5GHz
IEEE802.11ad	6.8Gbps	60GHz

チャンネル

複数のノードが同時に通信できるように、
周波数帯域を分割したもの。



CSMA/CA

重要

① 送信前に同じチャンネルを使用しているノードがないか調べる。（CS）

② 他のノードが通信していなければ、どのノードも送信する権利がある。（MA）

③ 他のノードが通信していないことを検出したら、ランダムな待ち時間をとってから、通信を開始する。（CA）

無線のセキュリティ

- SSID
  - 無線LANのネットワークグループの名前
- 認証方式
  - WEP　脆弱性があり、推奨されない
  - WPA／WPA2
- 暗号化アルゴリズム
  - AES　共通鍵暗号方式の一つ

[基本設定]

無線機能	☑ 使用する
無線チャンネル	13 チャンネル ▼ (現在のチャンネル: 手動選択)
倍速モード	帯域: 216.7 Mbps (20 MHz) ▼ (Current: 20 MHz) 拡張チャンネル: 1 ▼
ANY接続	☑ 許可する

SSID1

SSID1	☑ 使用する
隔離機能	☐ 使用する
SSID	○ エアステーションのMACアドレスを設定 (Buffalo-G-40CE) ◉ 値を入力: C5-3F-oota@ee
無線の認証	WPA2-PSK ▼
無線の暗号化	AES ▼
WPA-PSK (事前共有キー)	xxxxxxxxxxxxxxxxxxxx
Key更新間隔	0 分

通信の暗号化

重要

- **共通鍵暗号方式**

  暗号化と復号に1つの**共通鍵**を使用する。

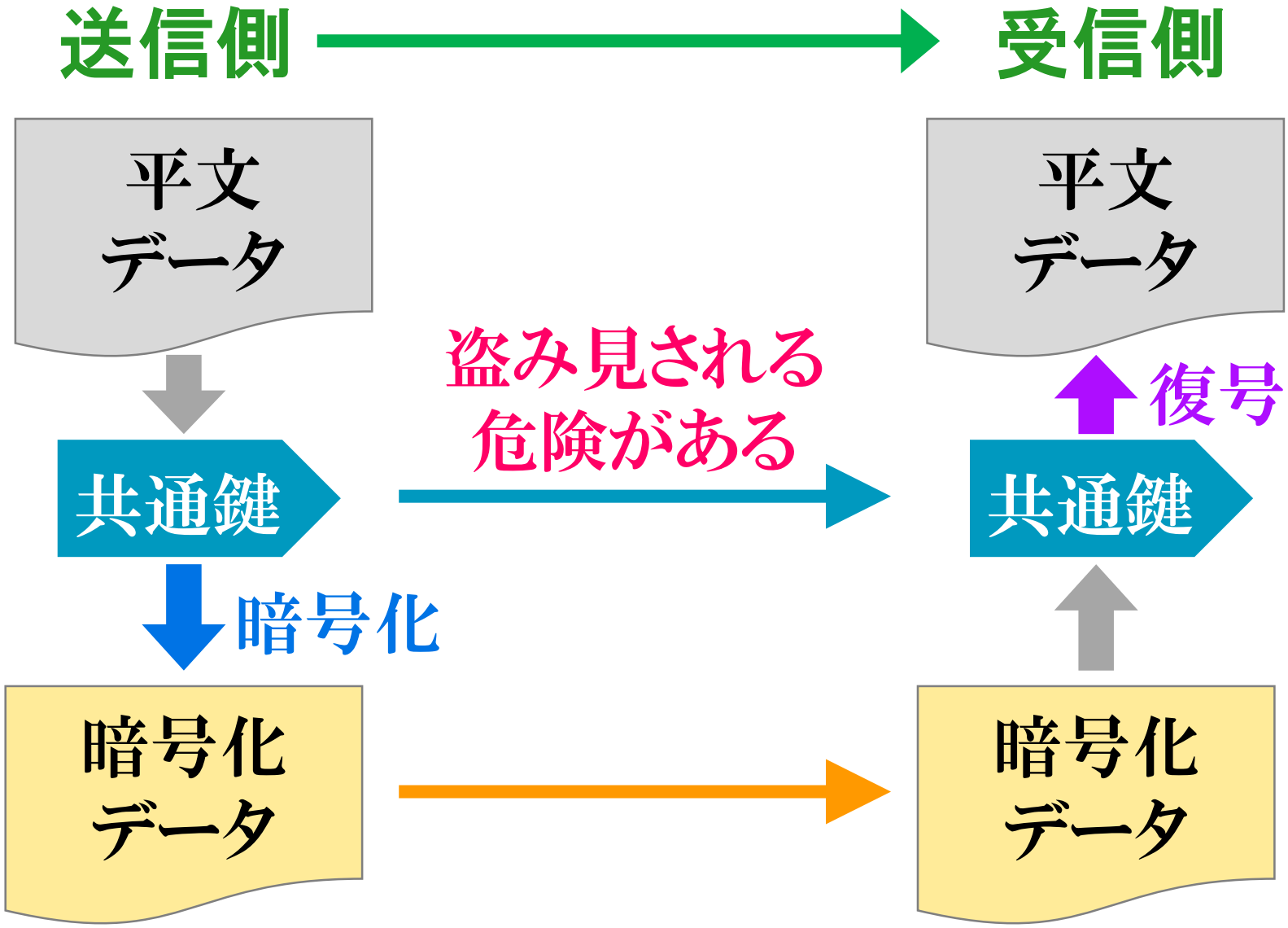
- **公開鍵暗号方式**

  暗号化に**公開鍵**、復号に**秘密鍵**を使用する。

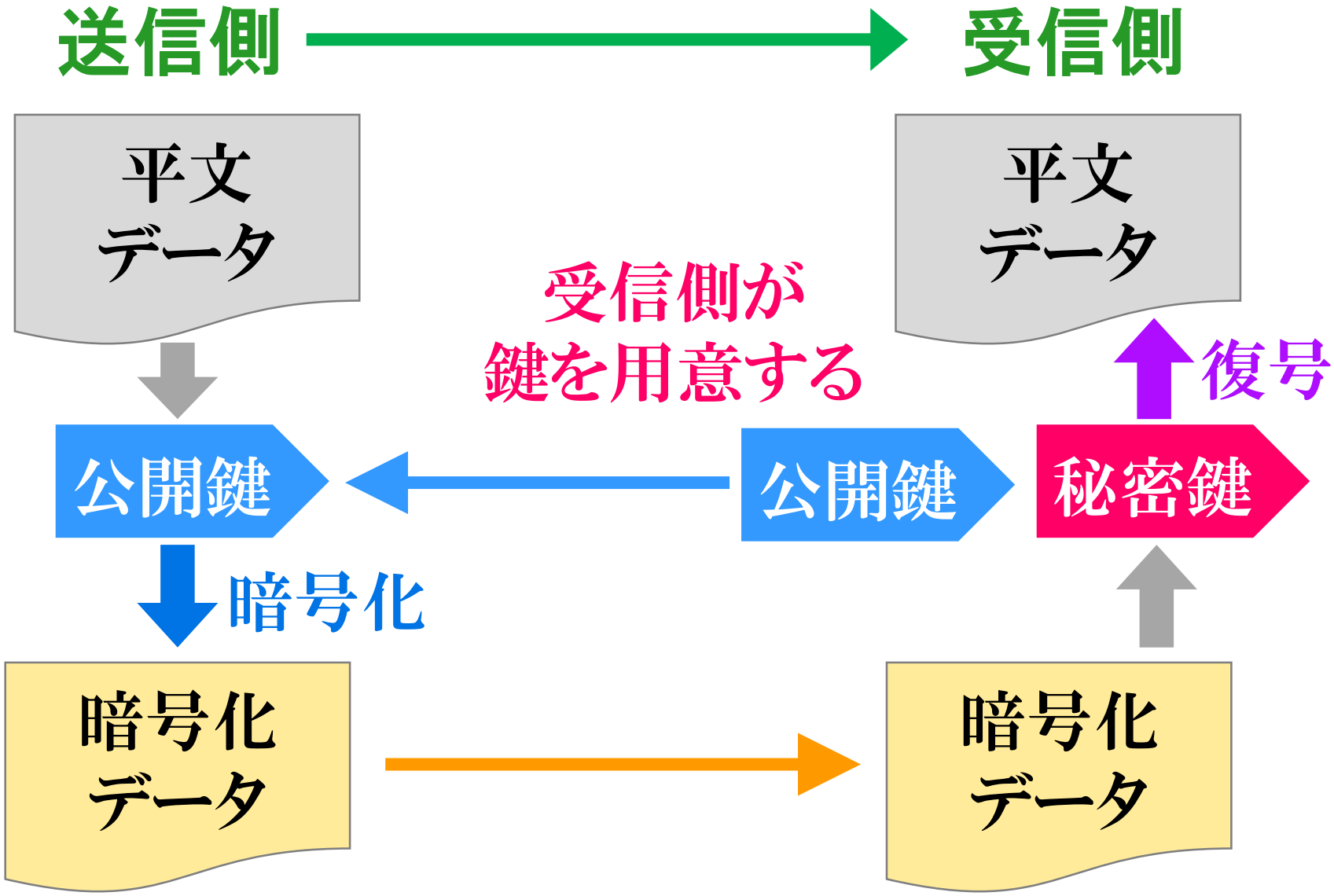
- **ハイブリッド暗号方式**

  暗号化と復号は共通鍵暗号で行い、共通鍵の伝達は公開鍵暗号で行う。

共通鍵暗号方式


送信側
受信側
平文
データ
平文
データ
盗み見される
危険がある
復号
共通鍵
共通鍵
暗号化
暗号化
データ
暗号化
データ

公開鍵暗号方式


送信側
受信側
平文
データ
平文
データ
受信側が
鍵を用意する
復号
公開鍵
公開鍵
秘密鍵
暗号化
暗号化
データ
暗号化
データ

ハイブリッド暗号方式

✣ 共通鍵暗号方式

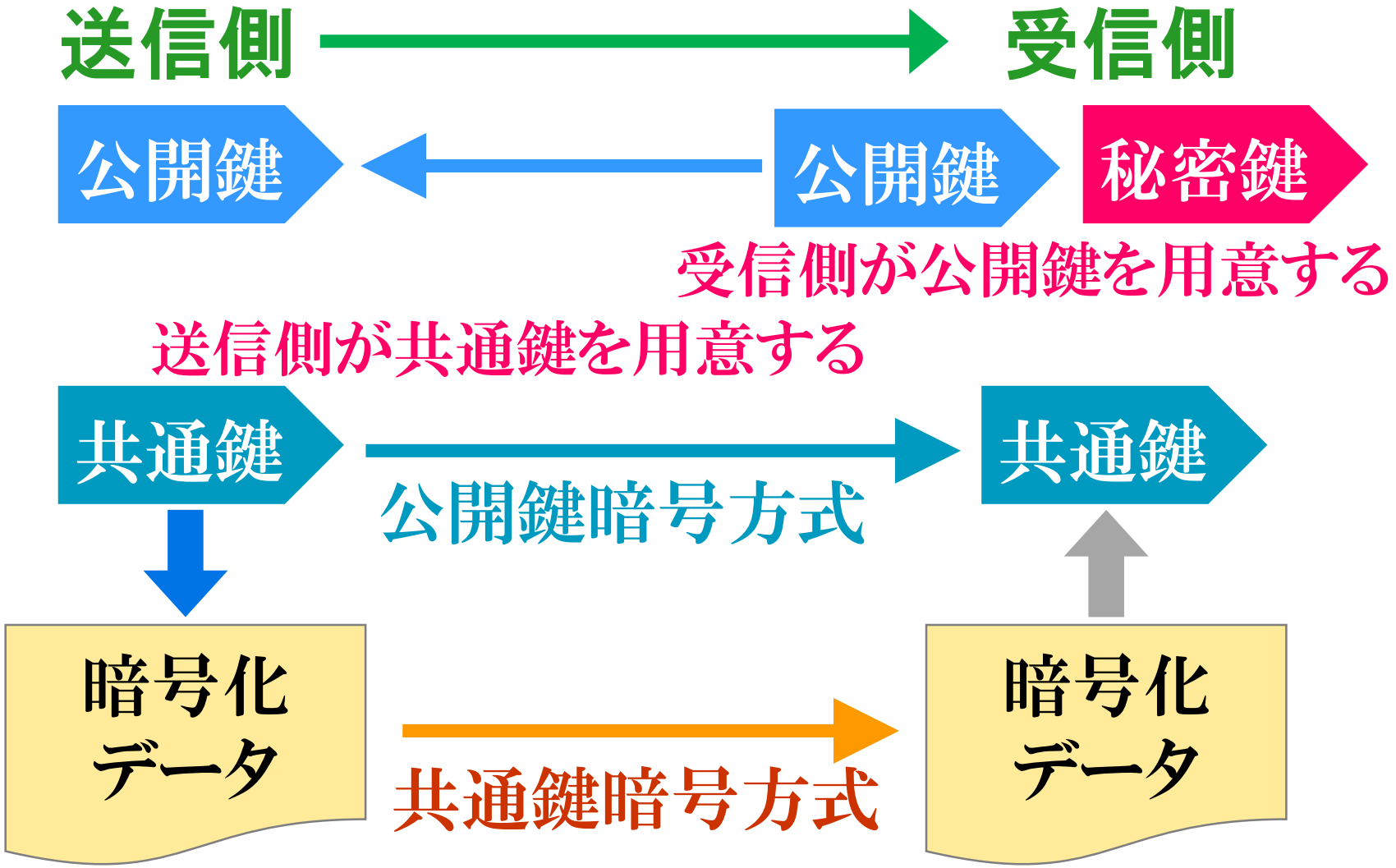
共通鍵を盗み見される危険がある。
暗号化と復号の計算処理は速い。

✣ 公開鍵暗号方式

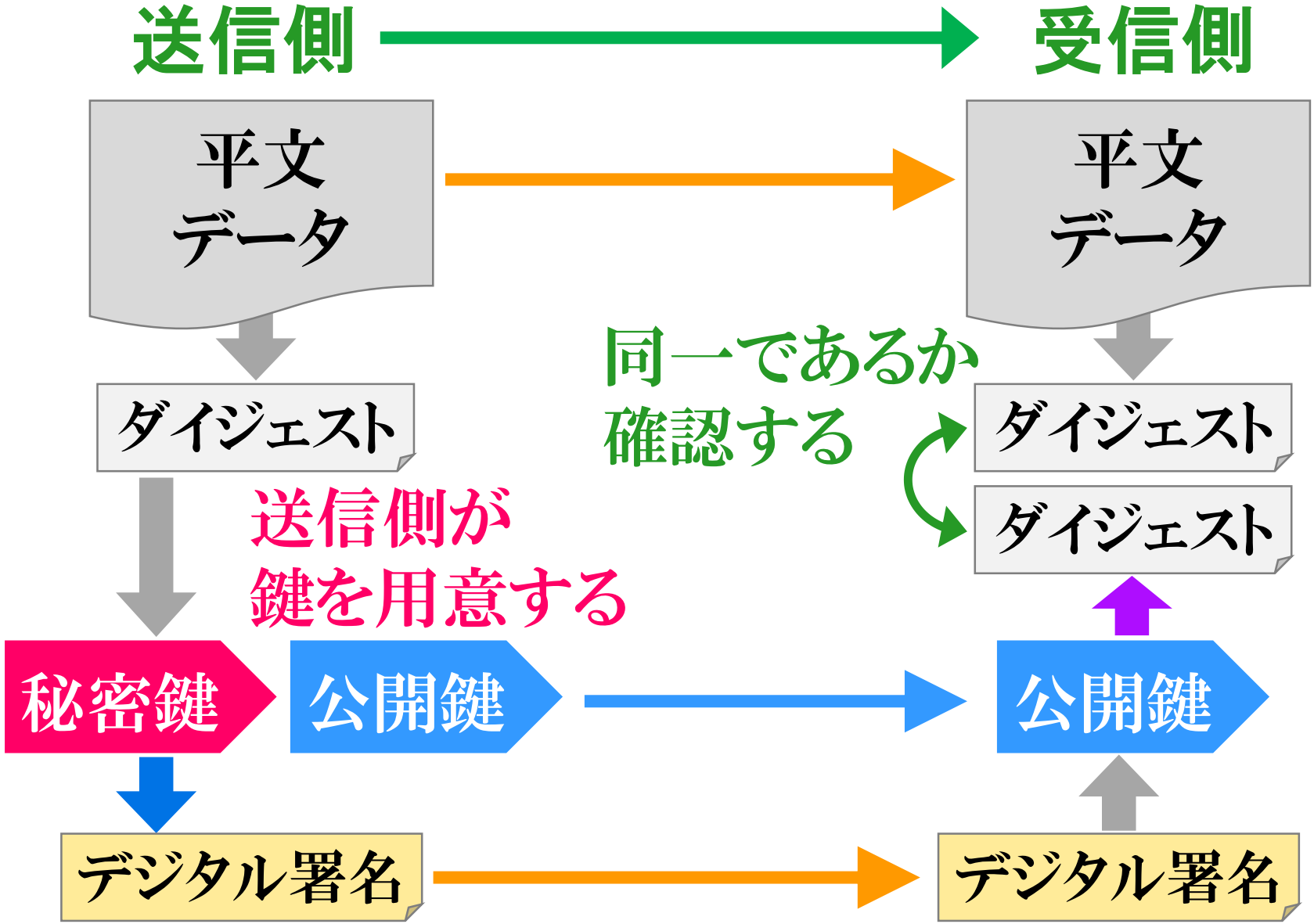
暗号化と復号の計算処理は遅い。

データ（通信量が大きい）を共通鍵方式で送り、その共通鍵（通信量が小さい）は公開鍵暗号方式で安全に送る。

ハイブリッド暗号方式


送信側
受信側
公開鍵
公開鍵
秘密鍵
受信側が公開鍵を用意する
送信側が共通鍵を用意する
共通鍵
公開鍵暗号方式
共通鍵
暗号化
データ
共通鍵暗号方式
暗号化
データ

ディジタル署名


送信側
受信側
平文
データ
平文
データ
同一であるか
確認する
ダイジェスト
ダイジェスト
ダイジェスト
送信側が
鍵を用意する
秘密鍵
公開鍵
公開鍵
デジタル署名
デジタル署名

認証局

第三者の立場で、通信相手の身元を保証する。身元を保証する電子証明書の発行と管理を行う。

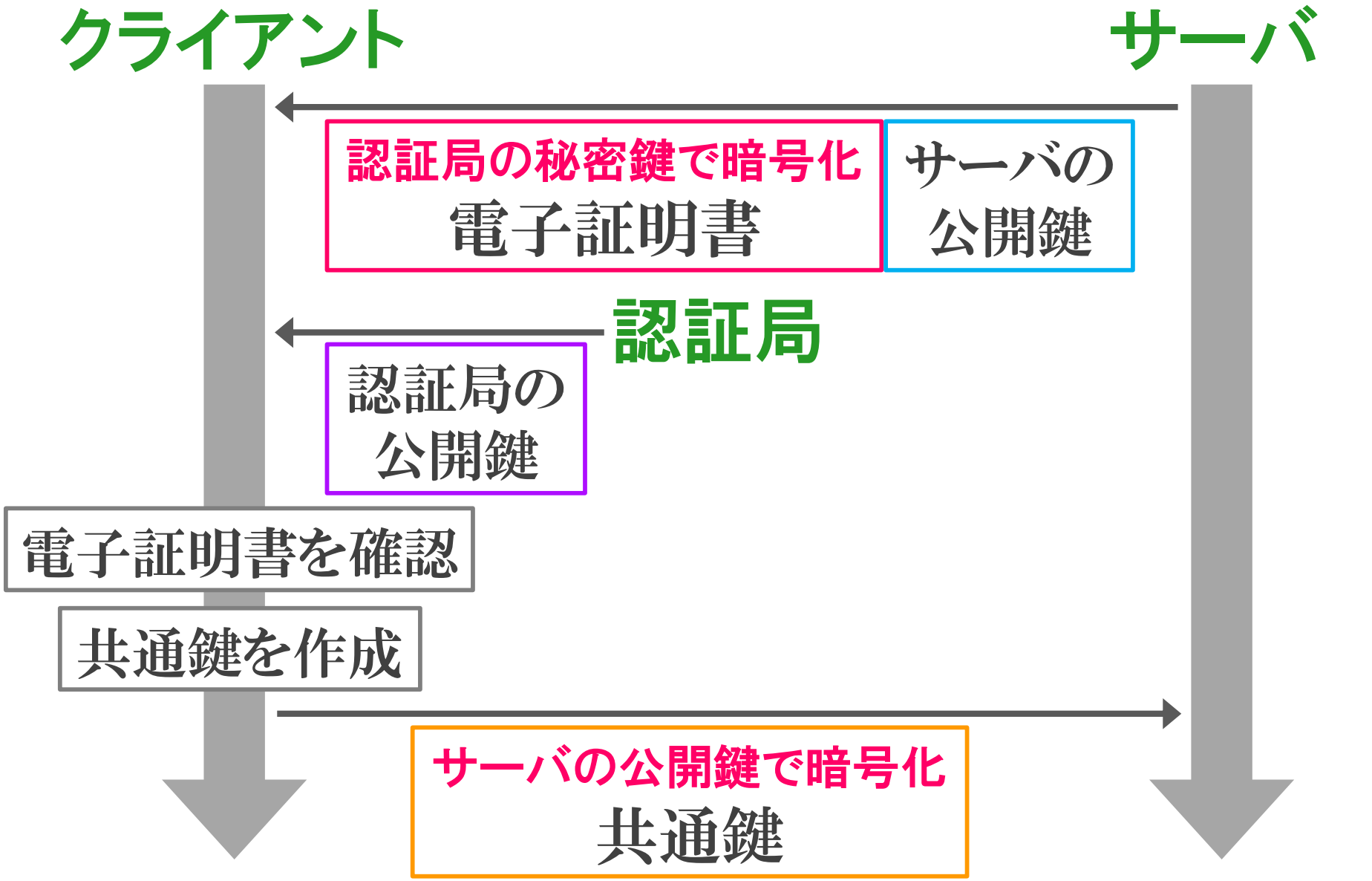
送信者

認証局に、証明書の発行を申請する。

受信者

認証局に、証明書の有効性を確認する。

HTTPS


クライアント
サーバ
認証局の秘密鍵で暗号化
電子証明書
サーバの
公開鍵
認証局
認証局の
公開鍵
電子証明書を確認
共通鍵を作成
サーバの公開鍵で暗号化
共通鍵

ネットワークを介した攻撃

- 不正アクセス
- 踏み台攻撃
- DoS攻撃 (Denial of Service)
- なりすまし
- フィッシング

クラウドコンピューティング

サーバに置かれているソフトウェアやデータを、ネットワークを介して使用する形態。

- **IaaS** (Infrastructure as a Service)
  ハードウェアとOSを提供する。
- **PaaS** (Platform as a Service)
  IaaSに加えて、サーバプログラムを提供する。
- **SaaS** (Software as a Service)
  PaaSに加えて、アプリケーションを提供する。