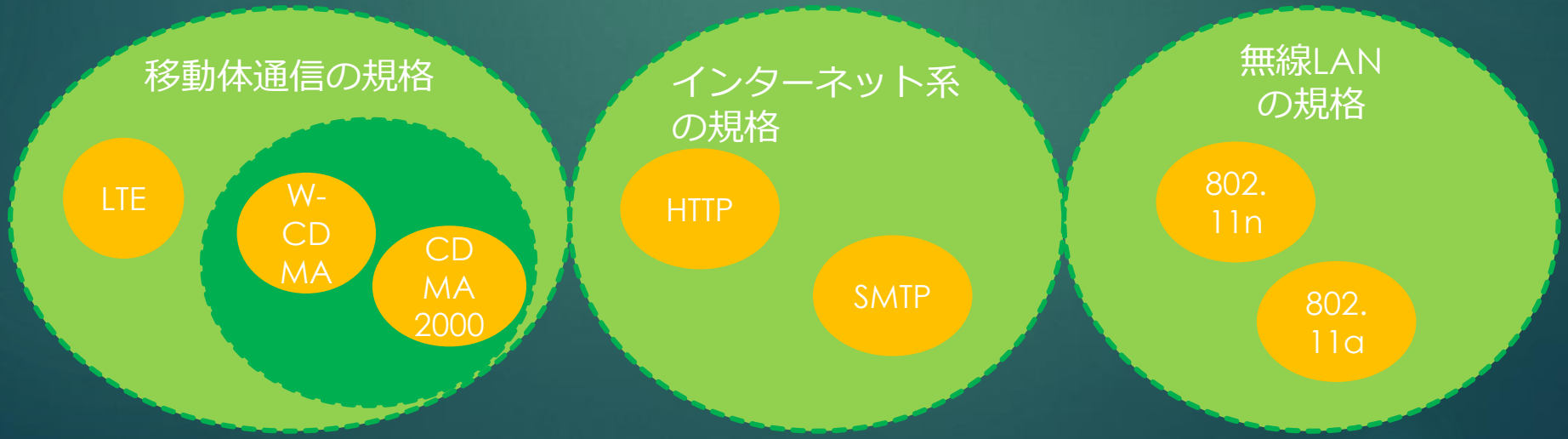
応用情報技術者試験

第7章　ネットワーク

1. プロトコルの全体像
通信規格とプロトコル

- 通信には“規格”が必要である。例えば移動体（携帯）通信の世界にはLTEと呼ばれる高速通信規格や3Gと総称される規格群があり、それらに対応する携帯電話やスマートフォンに限り通信を行うことができる。これらの規格には「通信を行う上でのさまざまな約束事」が含まれている。それら個々の約束事や約束事の集まりを“**プロトコル（通信規約）**”とよぶ。



プロトコルと階層

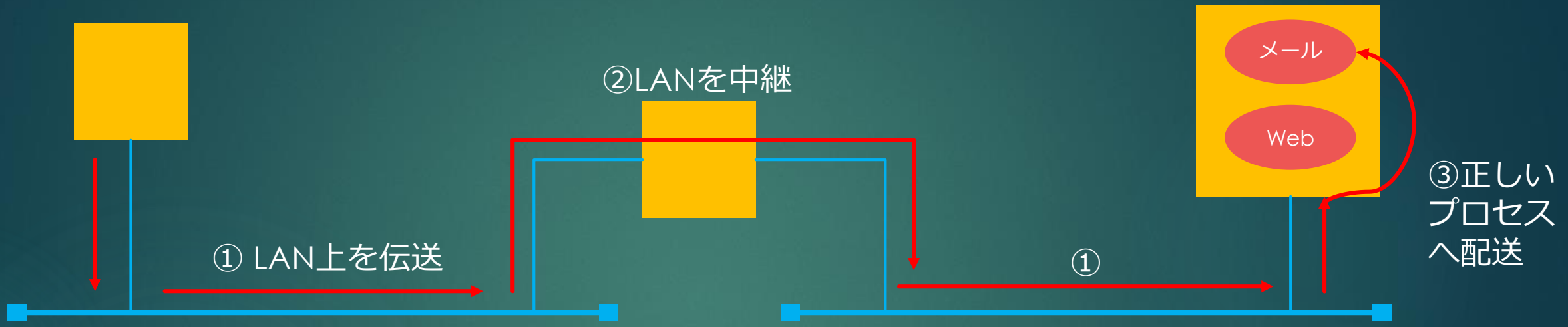
- プロトコルは、その役割に応じていくつかのレベルに分けられる。

（例）インターネット上の伝送

まず、LAN上でデータを転送するために、**LANレベルのプロトコル**が必要である。LANレベルのプロトコルは「同一LAN内の伝送」に限られるため、LANをまたぐ機能はない。LANをまたいであて先は届けるためには、**LANを中継するプロトコル**が必要になる。

あて先のマシンに届いたデータは、電子メールのデータであれば電子メールプロセスに、HTMLデータであればWebプロセスに届けられる。そのためには、アプリケーションプロセスを識別子、**正しいプロセスに配送するためのプロトコル**が必要になる。さらに、電子メールやWebプロセスのデータ形式や伝送手順といった、**個々のアプリケーションプロセスに関するプロトコル**も必要である。

プロトコルと階層



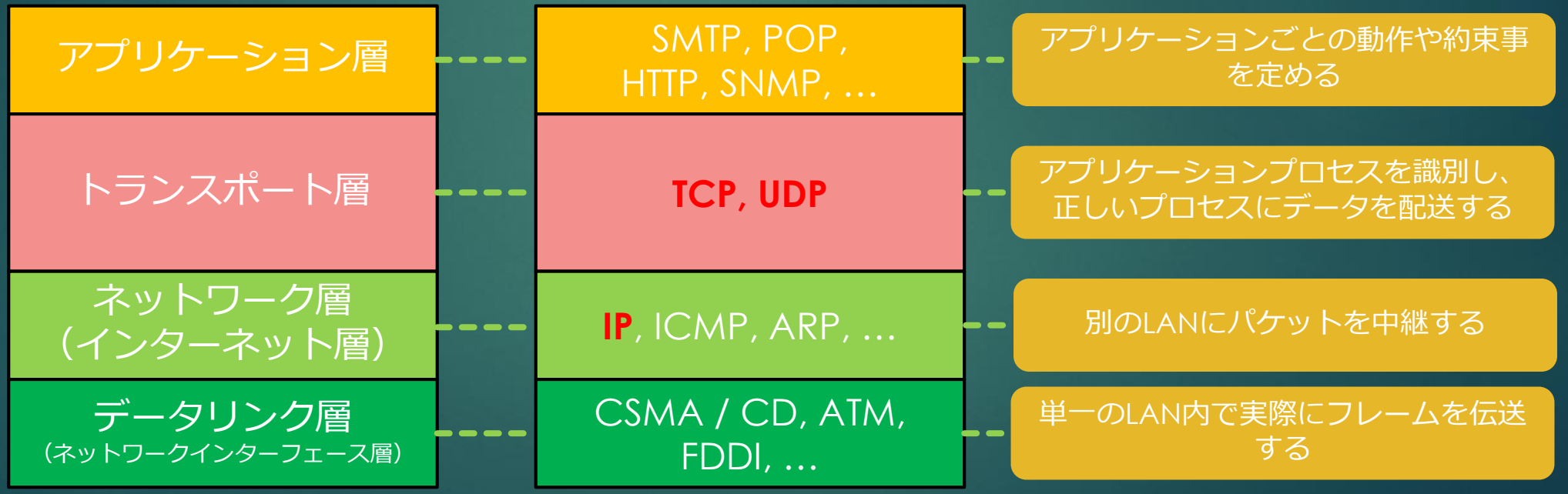
④各アプリケーションの動作を定めたプロトコル
③正しいプロセスに配送するプロトコル
②LANを中継するプロトコル
①LANレベルのプロトコル

プロトコル階層

- インターネットではプロトコル群は四つのレベルに分けられる。各レベルのことを**層（レイヤ）**、複数レイヤからなるプロトコル構造を**プロトコル階層（プロトコルスタック）**とよぶ。

TCP / IPの階層

- TCP / IPはインターネットで利用されているプロトコル群の総称で、世界で最も普及している。TCP / IPは前述の働きをもつ4階層から構成されている。



TCP / IPの階層とヘッダ

- 階層化されたプロトコルでは、データは各層の適切なプロトコルを用いて処理される。たとえば、有線LANで電子メールを送信するのであれば、

  アプリケーション層：SMTP

  トランスポート層：TCP

  ネットワーク層：IP

  データリンク層：CSMA / CD など

が選ばれる

TCP / IPの階層とヘッダ

- ある層で処理されたデータには、その層の機能を利用するためのヘッダが付与され、下位層に引き継がれる。ヘッダには様々な情報が設定されるが、中でも最も大切なものがアドレスなどの識別子である。たとえば、トランスポート層の**ヘッダ**には、アプリケーションの識別番号であるポート番号が設定されている。このように、アプリケーションが作成したデータは、最終的にはデータリンク層のフレームの形式で、LANに送出される。
- フレームを受信した側は、送信側とは逆に階層を上りながらヘッダを取り外し、元のデータを復元する。

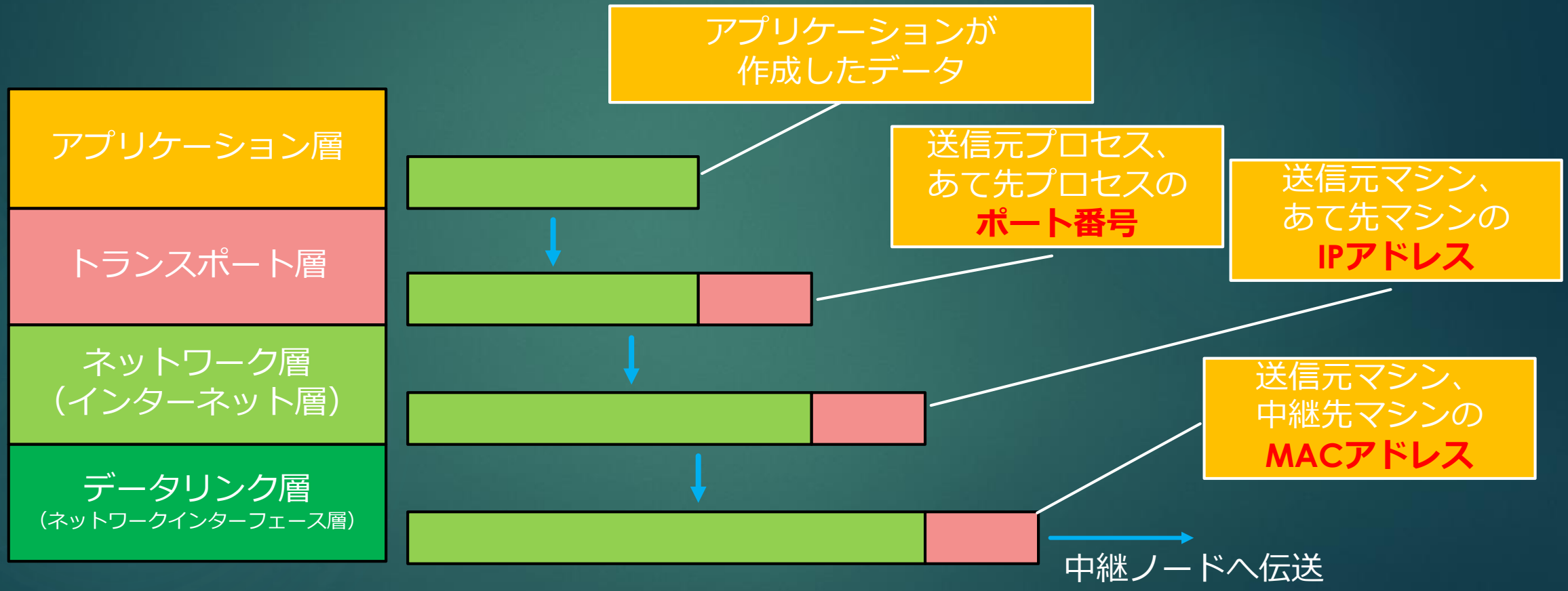
ヘッダ

伝送用の制御情報を格納する領域

フレーム、パケット

データの伝送単位の呼び方。特にデータリンク層の伝送単位をフレームとよぶ

TCP / IPの階層とヘッダ



TCP / IPの階層とヘッダ

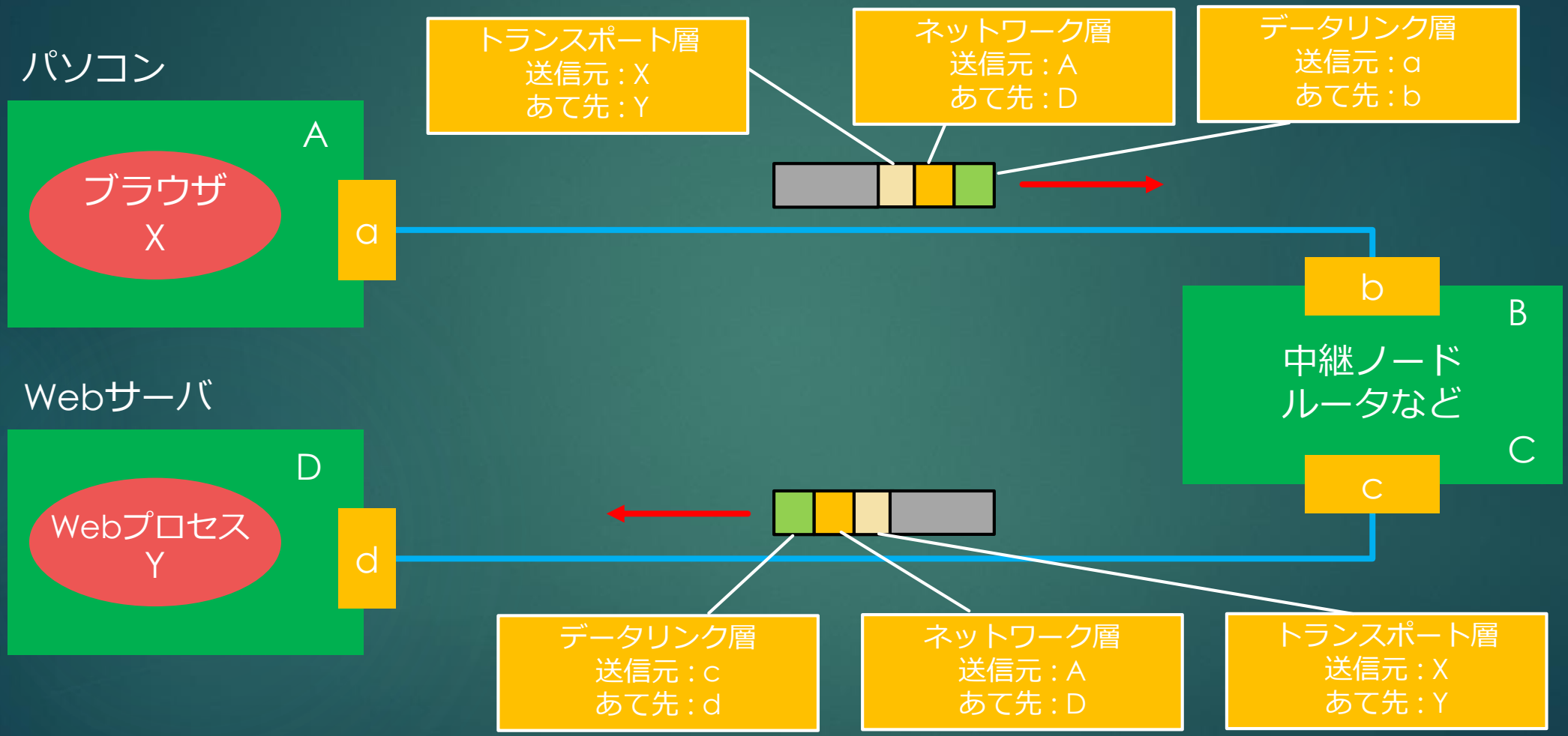
- TCP / IPで用いる識別子

ポート番号	ホスト上の**アプリケーションプロセスを識別**する番号
IPアドレス	インターネット上の**ホストを一意に識別**するアドレス
MACアドレス	LANに接続された**機器（LANボード）を物理的に識別する**アドレス。LAN内のフレーム伝送に用いる

- ホスト

サーバやクライアント・ルータなどデータの送受・中継を行う機器

データ伝送とアドレス変化



X, Y：ポート番号　A ~ D：IPアドレス　a ~ d：MACアドレス

データ転送とアドレス変化

- トランスポート層のヘッダには、プロセスを識別する**ポート番号**が設定される。送信元はX（ブラウザ）で、あて先はY（サーバのWebプロセス）である。
- ネットワーク層は、あて先ホストを識別してパケットを中継しなければならない。そこで、ホストを一意に識別する**IPアドレス**が設定される。送信元はA（パソコン）で、あて先はD（Webサーバ）である。
- データリンク層は、LAN内の伝送を行う。そこで、LANの規格に沿った物理的な（変更できない）アドレスである**MACアドレス**が設定される。LAN内の伝送は「パソコンと中継ノード間」と「中継ノードとWebサーバ間」の2回に分けて行われる。そのため、最初の伝送と2回目の伝送では、指定されるアドレスが異なっている。伝達の都度、LAN内のMACアドレスが指定しなおされているためである。
- **IPアドレスはエンドノードを指定し、MACアドレスは中継ノードを指定する**。

ノード

ネットワークに接続される機器全般を指す呼び方

エンドノード

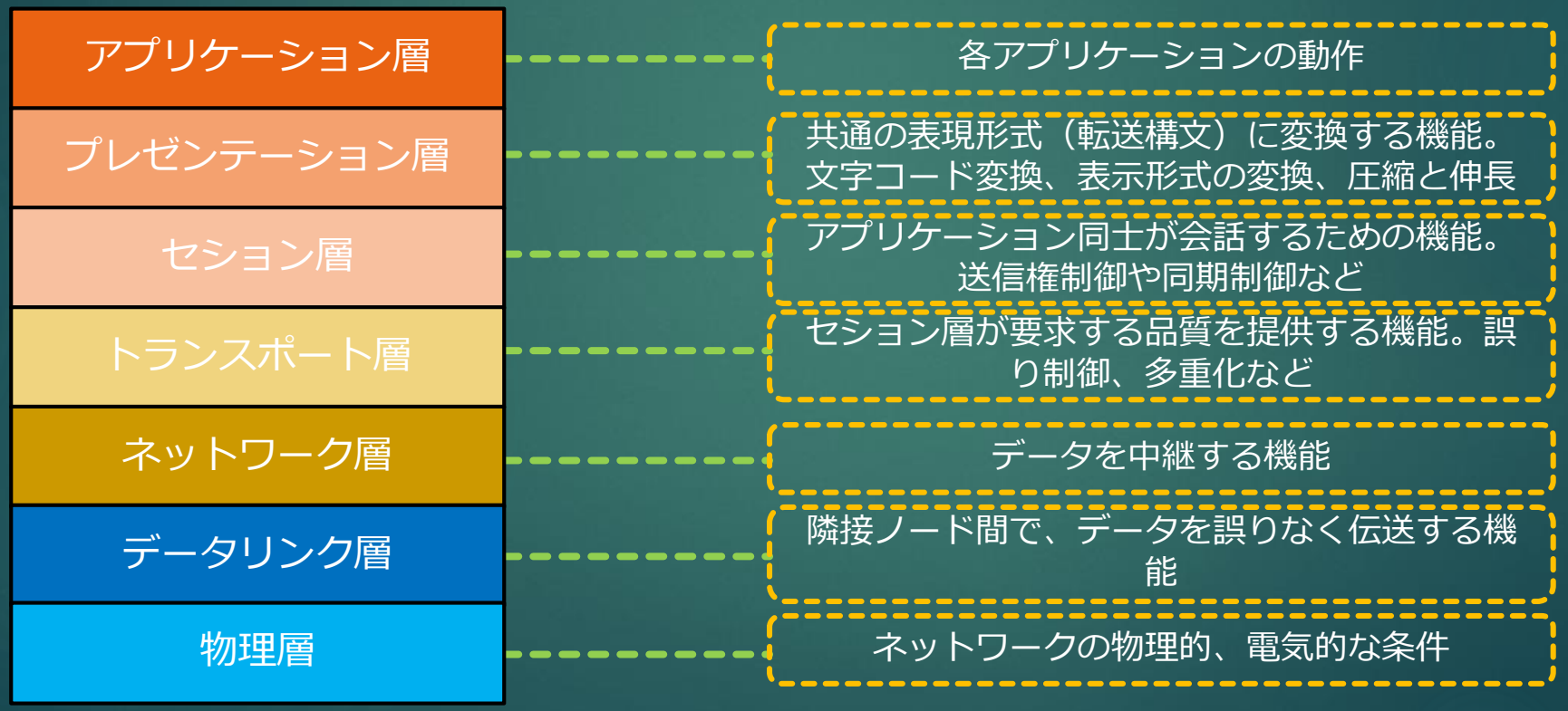
通信の末端に位置するノード。実際の送信元およびあて先

中継ノード

データを中継するノード

TCP / IPとOSI基本参照モデル

- TCP / IPが事実上の標準となる前に、ISOがOSI基本参照モデルとよばれる7階層モデルを提案した。



2. データリンク層
LANのプロトコル

- TCP / IPの代表的なデータリンク層のプロトコルが「LANのプロトコル」である。

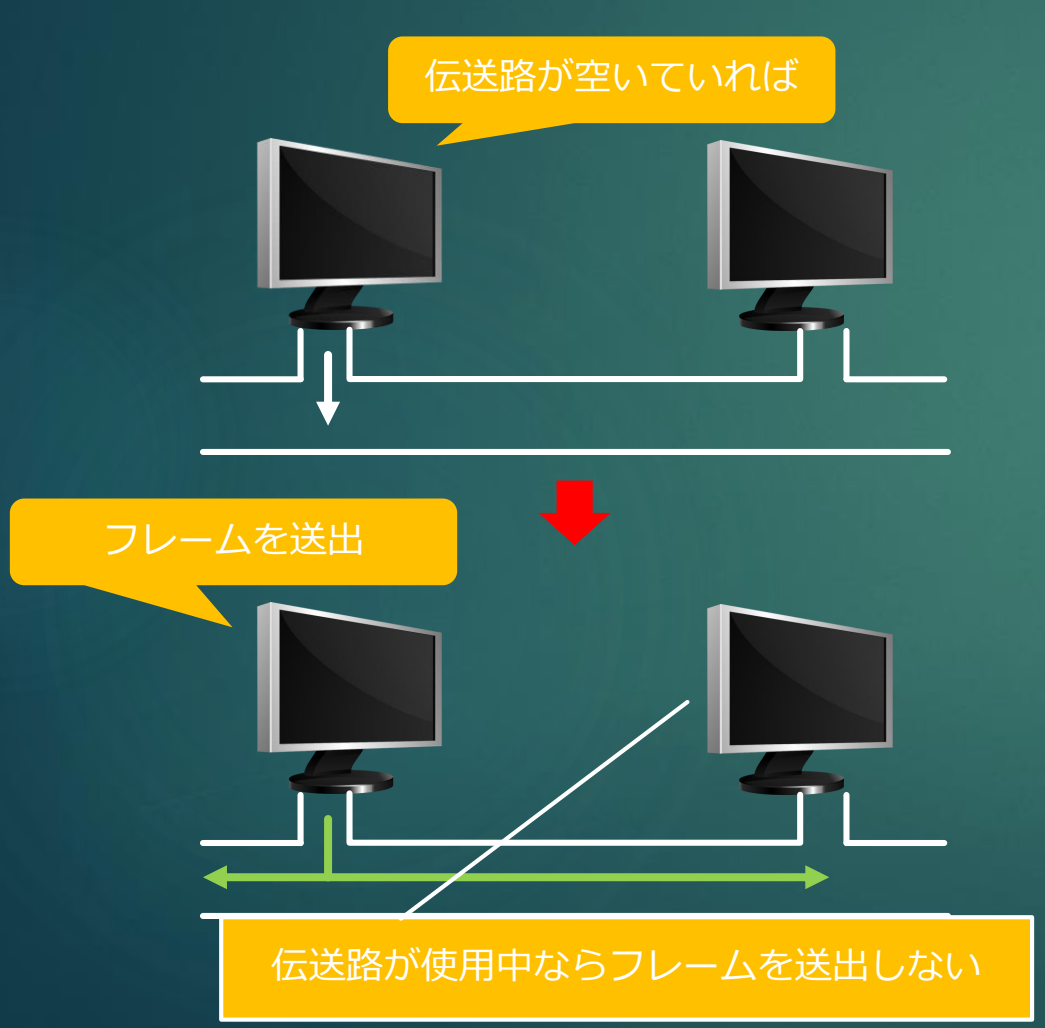
- LANのプロトコルは、**媒体アクセス制御方式(Media Access Control : MAC)**の規格と伝送に必要な電気的な規格を含んでいる。媒体アクセス制御方式には、一般的な有線LANで用いられてきたCSMA/CD、リング型のLANで用いられたトークンパッシング、無線LANで用いられるCSMA/CAなどがある。

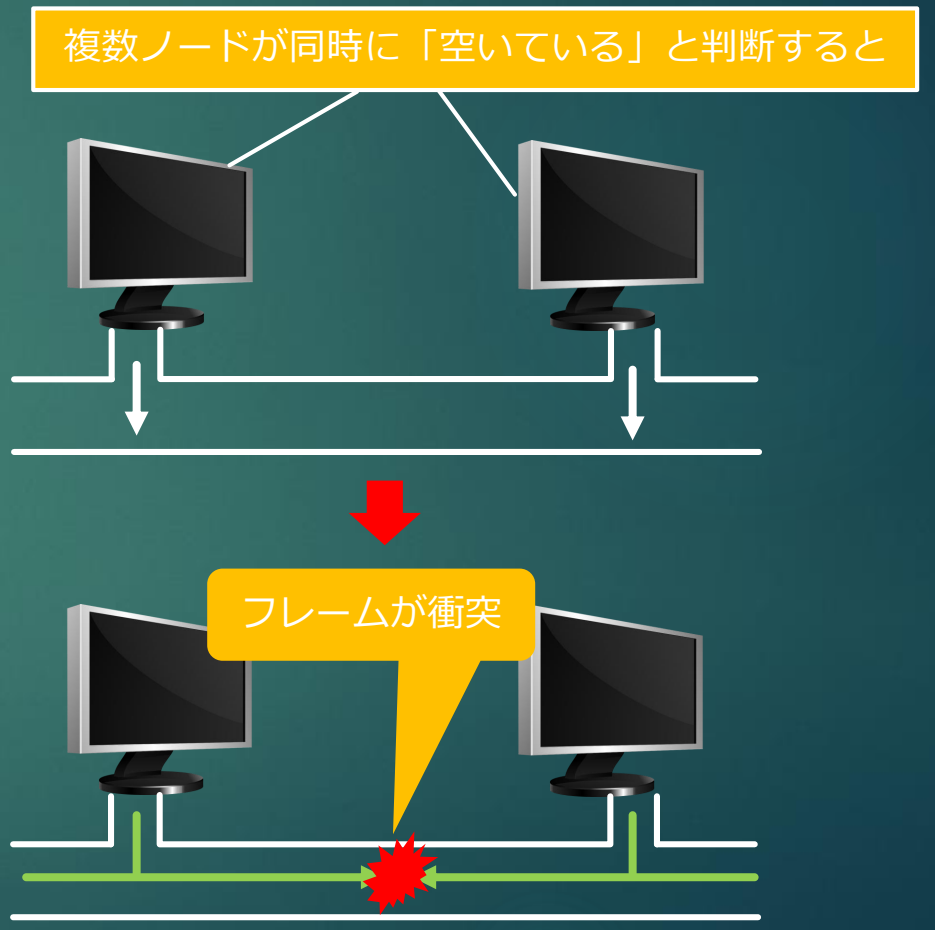
CSMA/CD(Carrier Sense Multiple Access with Collision Detection)方式

- CSMD/CDは、各ノードがフレームの送出に先立って、**伝送路にフレームが流れていないことを確認し、フレームの送出を開始する**方式である。

- 複数ノードがほぼ同時にフレームを送出すると、フレームの**衝突(collision)**が発生する。これを検出したノードはフレームの送出を停止し、他のノードに衝突を知らせる信号（**ジャム信号**）を送出する。フレームは、任意の時間待機した後に再送される。

CSMA/CD(Carrier Sense Multiple Access with Collision Detection)方式





CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)方式

- **CSMA/CA**は無線LANで用いられる方式である。無線LANでは、フレームの衝突を検知できないので、**一定時間回線が空いていることを確認してからフレームを送出する**など、フレームの衝突をできるだけ**回避(avoidance)**するような制御を行う。

- 受信側のノードは、フレームを正しく受信できた場合に**確認応答(ACK)**を返す。ACKが返ってこないとき、送信側のノードはフレームを再送出する。

トークンパッシング方式

- **トークンパッシング方式**は、**トークン（フリートークン）**とよばれる送信権を表す制御フレームを伝送路上に巡回させ、トークンを取得したノードのみがフレームを送出する方式である。**リング型LAN**のほかにも**バス型LAN**の媒体アクセス制御に用いられる。なお、イーサネットや無線LANの普及に伴い、トークンパッシング方式は、ほとんど用いられることがなくなった。

イーサネット(IEEE802.3)

- **イーサネット(Ethernet)**は媒体アクセス制御にCSMA/CD方式を採用するLANで、これをもとに**IEEE802委員会**が**IEEE802.3**を規格化した。

- 主なイーサネット規格

規格	トポロジ	伝送媒体	最大伝送距離	最大伝送速度
10BASE2	バス型	細芯同軸ケーブル	185m	10Mビット/秒
10BASE5	バス型	標準同軸ケーブル	500m	10Mビット/秒
10BASE-T	スター型	UTPケーブル	100m	10Mビット/秒
100BASE-TX	スター型	UTPケーブル	100m	100Mビット/秒
100BASE-SX	スター型	光ファイバ	550m	1Gビット/秒
1000BASE-T	スター型	UTPケーブル	100m	1Gビット/秒

無線LAN(IEEE802.11)

- IEEE802.11シリーズは、媒体アクセス制御に**CSMA/CA方式を用いた無線LANの規格群**である。

- 主な無線LANの規格

規格名称	周波数帯域	最大伝送速度
IEEE802.11	2.4GHz帯域	2Mビット/秒
IEEE802.11a	5GHz帯域	54Mビット/秒
IEEE802.11b	2.4GHz帯域	11Mビット/秒
IEEE802.11g	2.4GHz帯域	54Mビット/秒
IEEE802.11n	2.4/5GHz帯域	600Mビット/秒

- なお、無線LANは物理的な回線接続が不要である分、不正アクセスへの備えが必要となる。そこで、正規のMACアドレスをアクセスポイントに事前登録し、それ以外の端末からアクセスを制限する。そのような仕組みを**MACアドレスフィルタリング**とよぶ。

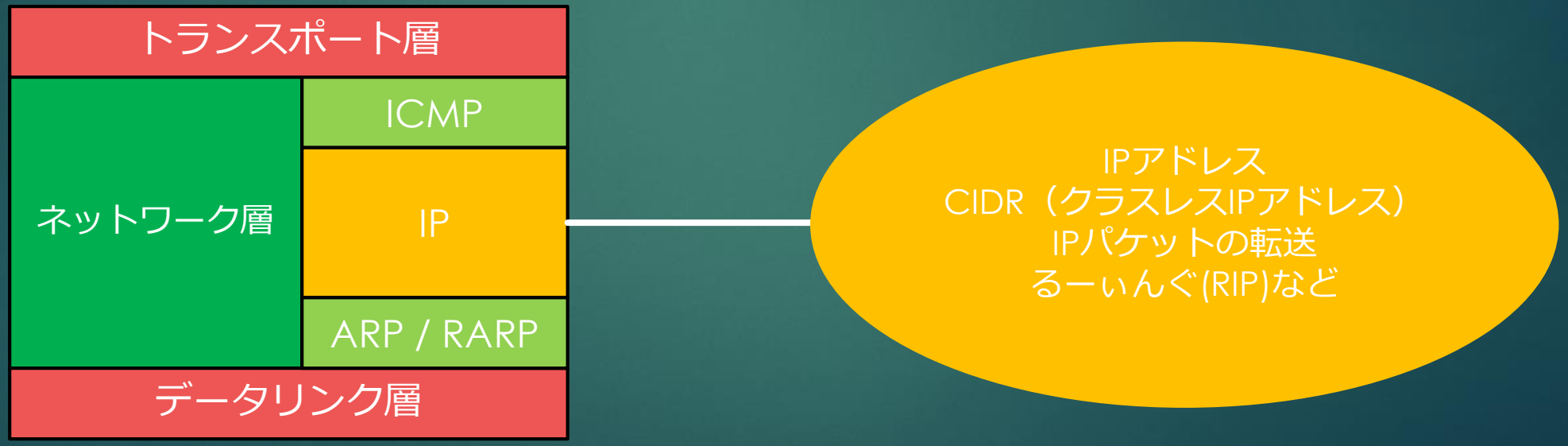
PLC(Power Line Communication)

- **PLC**は、**電力線を通信回線として利用する**技術である。屋内の電力線を用いて手軽にLANを構築することができる。

- 屋外の電力線を利用したWANや、電柱からの引き込みにのみ屋外の電力線を利用することも考えられているが、漏洩電磁波レベルが大きいことなどから実用に至っていない。

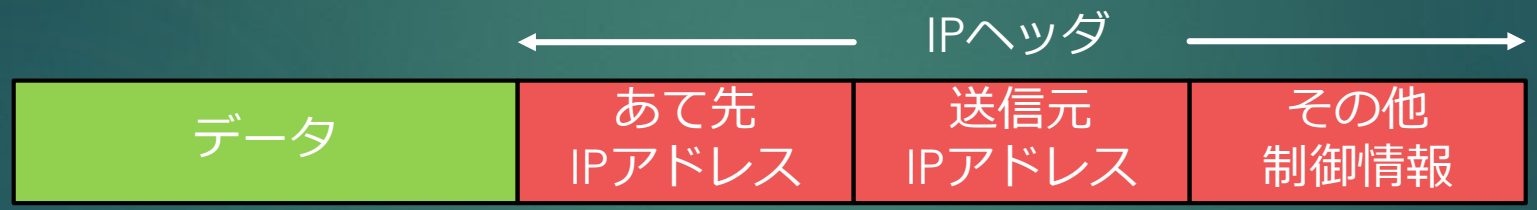
3. ネットワーク層
ネットワーク層のプロトコル

- TCP / IPのネットワーク層には、ICMP, IP, ARP / RARPなどのプロトコルが含まれる。その中心がIPである。



IP(Internet Protocol)の役割

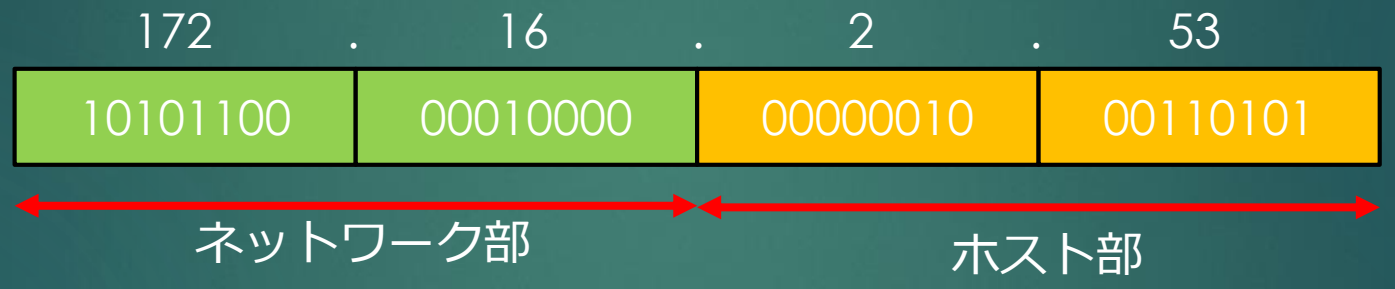
- IPの役割は、パケットを中継してエンドノードに送り届けることにある。これを行うため、IPパケットのヘッダには、送信元とあて先をエンドツーエンドで指定するIPアドレスが指定される。



- IPアドレスは、各ノードとネットワークの接点（**接続ポート**）ごとに付与される。ルータなどの複数のネットワークを接続する機器には、**接続ポートごとに異なるIPアドレスが付与される**ことになる。

IPアドレス

- IPアドレスは32ビットのアドレスであり、8ビットごとにピリオド(.)で区切り、10進数で表記される。



A社

B社

IPアドレス

- IPアドレスは、大きく**ネットワーク部**と**ホスト部**に分かれている。ネットワーク部は**組織の識別**に用いられ、ホスト部は同一組織（同一ネットワーク）に接続する**ホストの識別**に用いられる。同じ組織に属するホストには、ネットワーク部が等しくホスト部が異なるアドレスが割り当てられる。

IPアドレスとクラス

- IPアドレスは、ネットワーク部の長さにより**クラスA~C**に分けられる。クラスはネットワークの規模を表す概念で、クラスAのIPアドレスを割り当てられた組織は、1,000万を超えるIPアドレスを利用することが可能である。
- 組織がどのクラスに属するかは、IPアドレスの上位数ビットによって判断することができる。

クラス	IPアドレス(2進/10進)	組織数	組織内アドレス数
A	0NNNNNNN LLLLLLLL LLLLLLLL LLLLLLL 0.0.0.0 ~ 127.255.255.255	128	16,777,216
B	10NNNNNN NNNNNNNN LLLLLLLL LLLLLLLL 128.0.0.0 ~ 191.255.255.255	16,384	65,536
C	110NNNNN NNNNNNNN NNNNNNNN LLLLLLLL 192.0.0.0 ~ 223.255.255.255	2,097,152	256

N:ネットワーク部
L:ホスト部

- なお、現在ではIPアドレスの有効活用のため、クラスの枠組みは取り払われている。

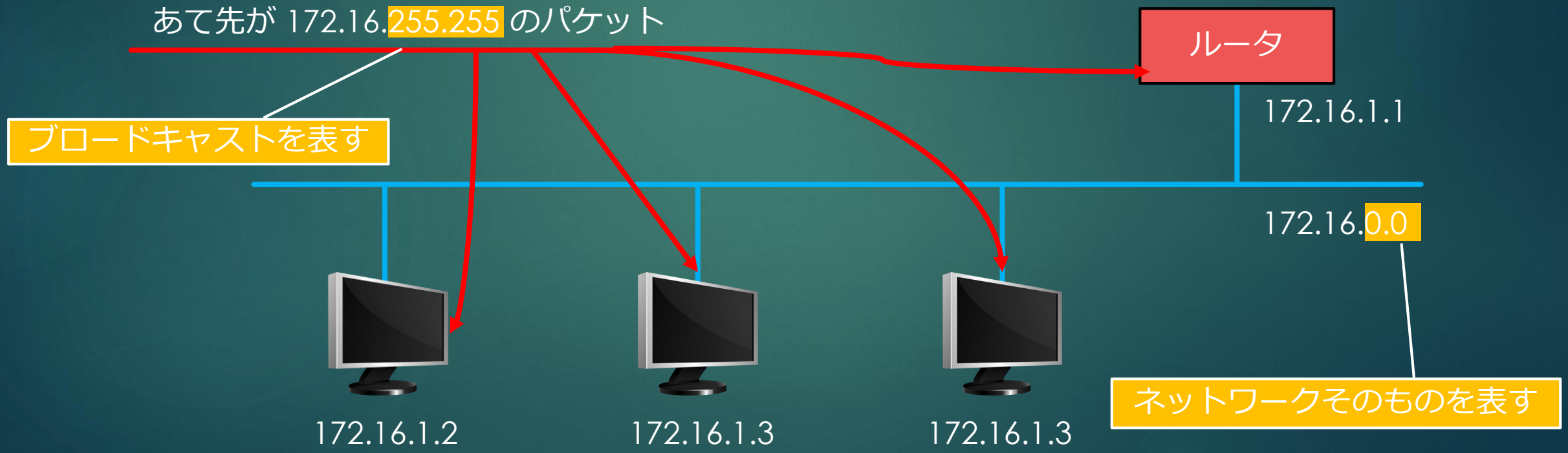
特殊なIPアドレス

- IPアドレスのうち、ホスト部の値が「すべて0」または「すべて1」のアドレスは、特別な用途に用いるため、ホストに割り当てることはできない。

- ホスト部の値がすべて0のアドレスは**ネットワークアドレス**とよばれ、特定のホストではなく「**ネットワークそのもの**」に付与される。ホスト部がすべて1のアドレスは、ネットワークに属する「**すべてのホスト**」を表すアドレスで、全ホストを対象とする通信（**ブロードキャスト**）のあて先として用いられる。

特殊なIPアドレス


172
16
XXX
XXX


あて先が 172.16.255.255 のパケット
ルータ
172.16.1.1
ブロードキャストを表す
172.16.0.0
ネットワークそのものを表す
172.16.1.2
172.16.1.3
172.16.1.3

特殊なIPアドレス

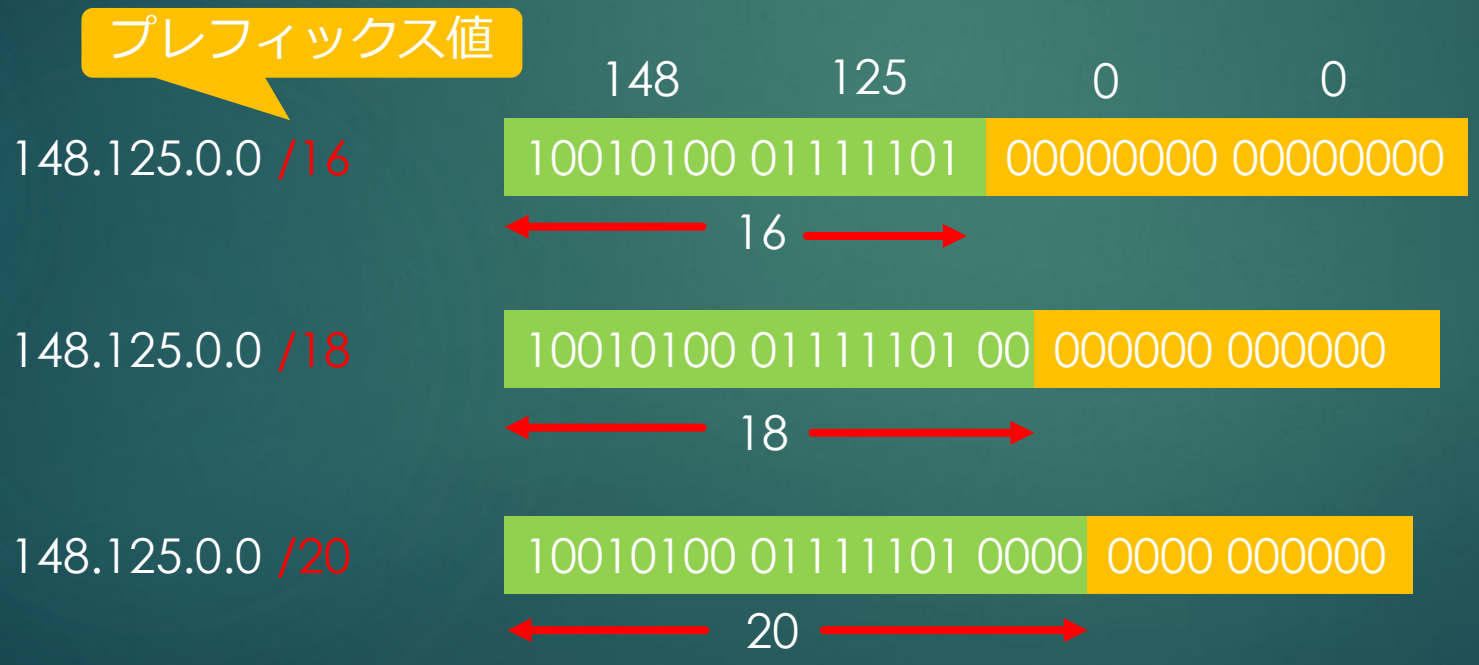
- ホストに割り当てることができるIPアドレスの数は、ホスト部がnビットである場合、2^nから「すべて0」と「すべて1」を除いた

$$2^n - 2[\text{種類}]$$

で求められることになる。例えばクラスCのIPアドレスであれば、ホスト部のビット数が8なので、最大$2^8 - 2 = 254$個のアドレスをホストに割り当てることが可能である。

CIDR (Classless Inter Domain Routing)

- CIDRは、IPアドレスからクラスの枠組みを取り払い、最適な規模のIPアドレスを割り当てる仕組みである。
- CIDRでは、**ネットワーク部（およびサブネット識別子）の長さを自由に設定する**ことができる。これらの長さをプレフィックス値とよび、IPアドレスの後にスラッシュとプレフィックス値を用いて表記する。

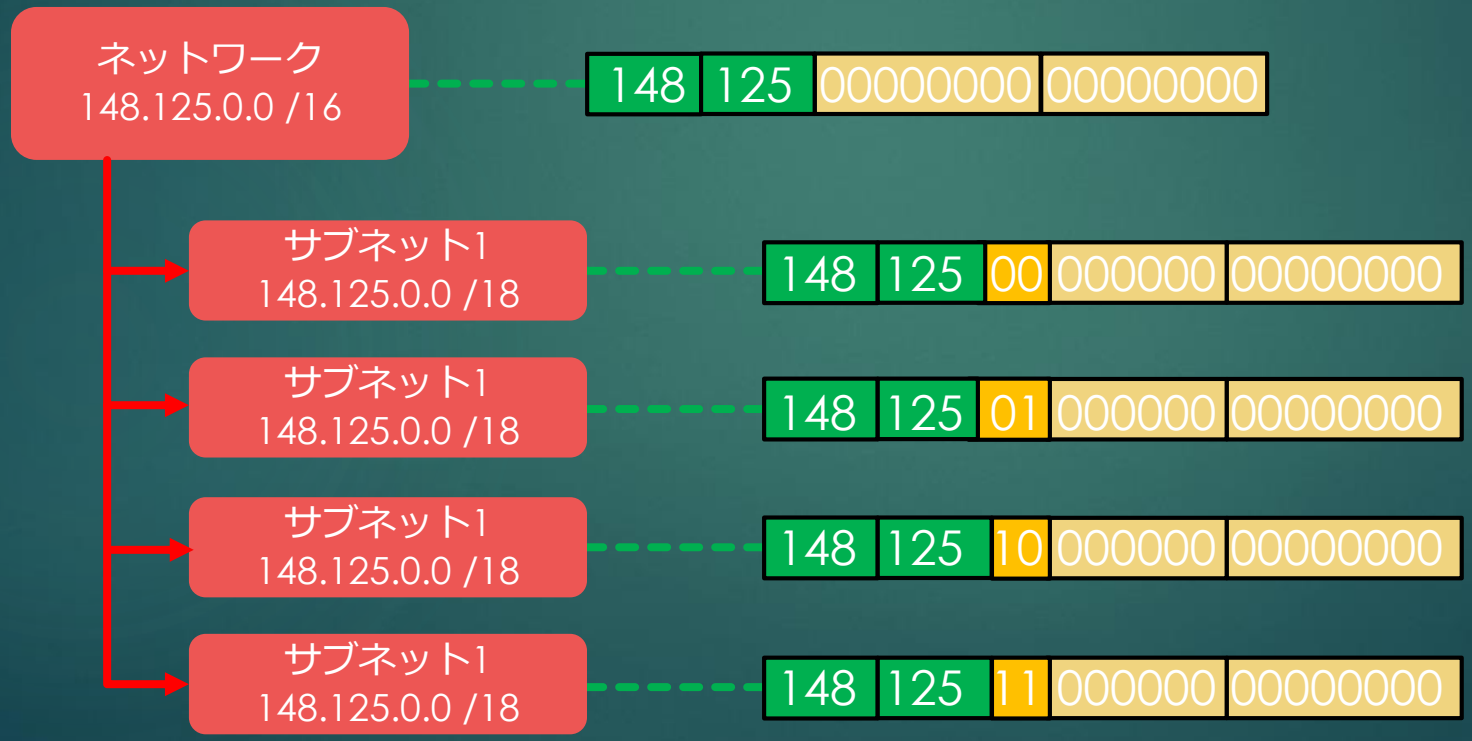


CIDR (Classless Inter Domain Routing)

- プレフィックス値が大きければ、相対的にホスト部のビット数は少なくなり、利用できるIPアドレス数も少なくなる。ネットワークの規模に見合ったプレフィックス値を用いることで、限られた資源であるIPアドレスを、有効に利用することができる。

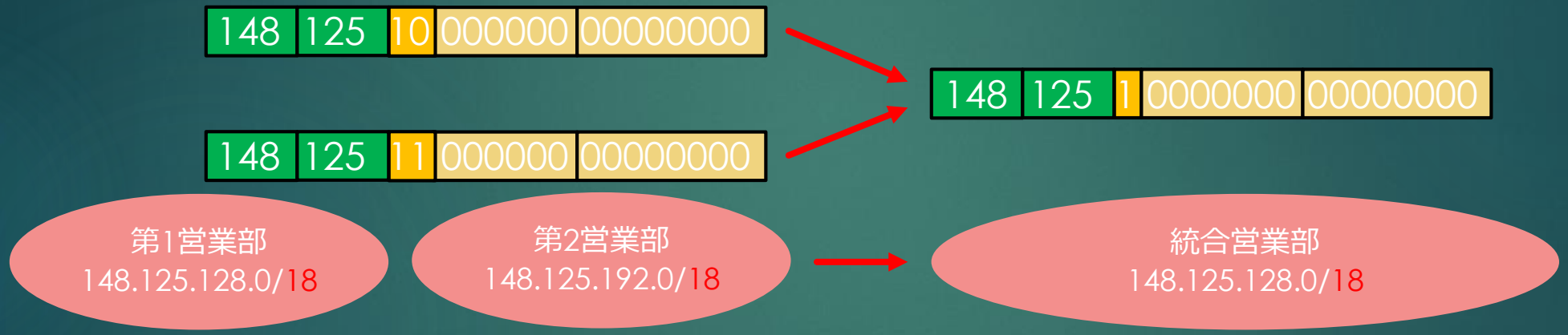
ネットワークの分割

- IPアドレス空間の有効利用や運用負荷の分散を図るため、ネットワークを複数の**サブネットワーク（サブネット）**に分割することがある。分割を実現するため、ホスト部の一部を「**サブネットの識別子**」として扱う。たとえばホスト部の2ビットをサブネット識別子に用いる、四つのサブネットに分割することができる。



ネットワークの集約

- また、分割の逆を行うことで、複数の小さなアドレスブロックをまとめてより大きなアドレスブロックを作成することもできる。このような自在で柔軟な運用もCIDRの効果の一つである。

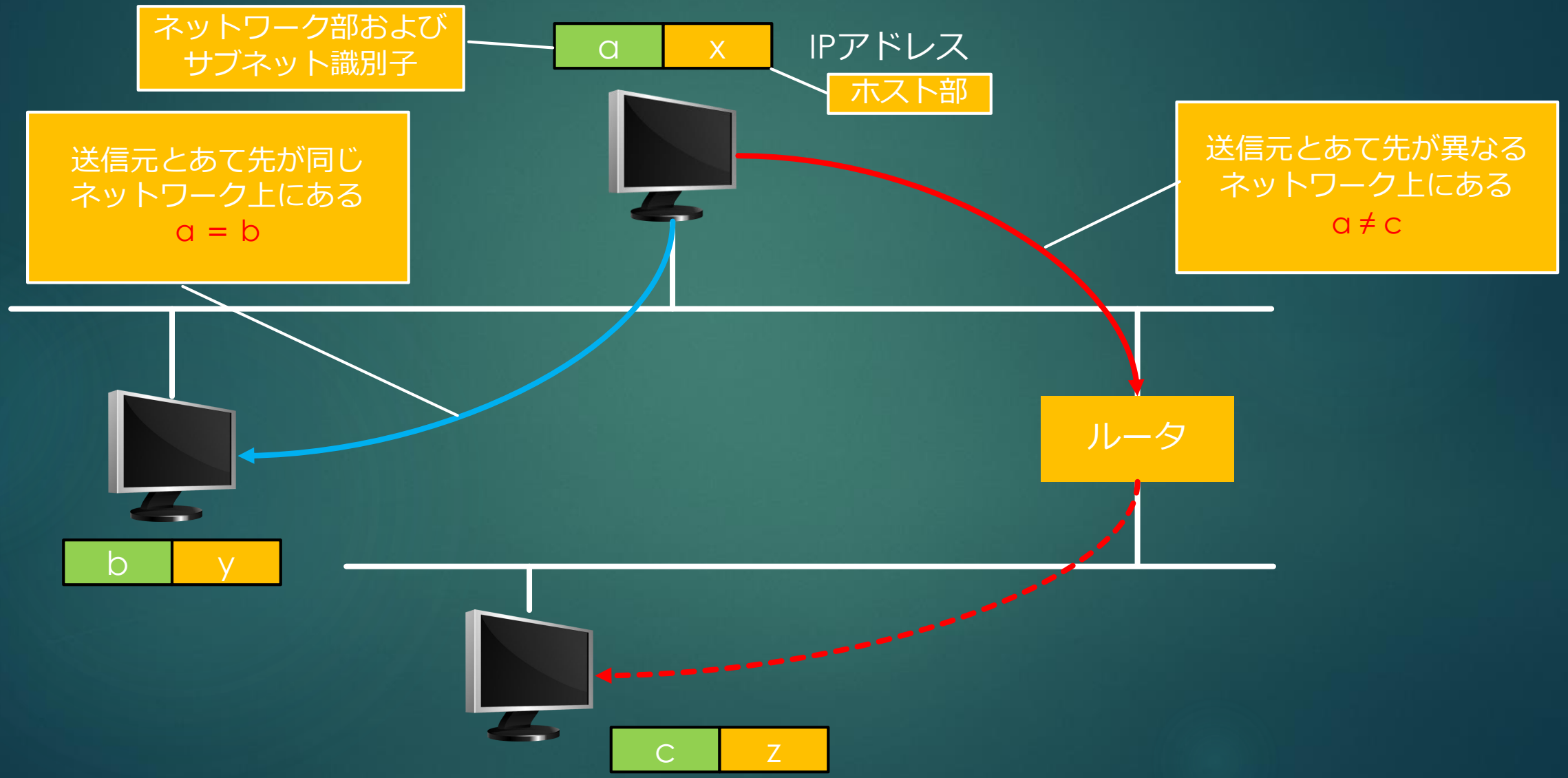


- なお、ネットワークの分割を進めればプレフィックス値は大きくなり、逆に集約を進めれば小さくなる。

データ送信とサブネットマスク

- ホストはデータ送信にさいして「あて先が自身と同じネットワークに存在するかどうか」を確かめる。もし同じネットワーク上にあればあて先に直接フレームを送信し、そうでなければルータなどの中継機器にフレームを送出する。
- 「送信元とあて先が同じネットワークにある」ことは、両者につけられた**IPアドレスのネットワーク部およびサブネット識別子の値が等しいかどうか**で確かめることができる。

データ送信とサブネットマスク



データ送信とサブネットマスク

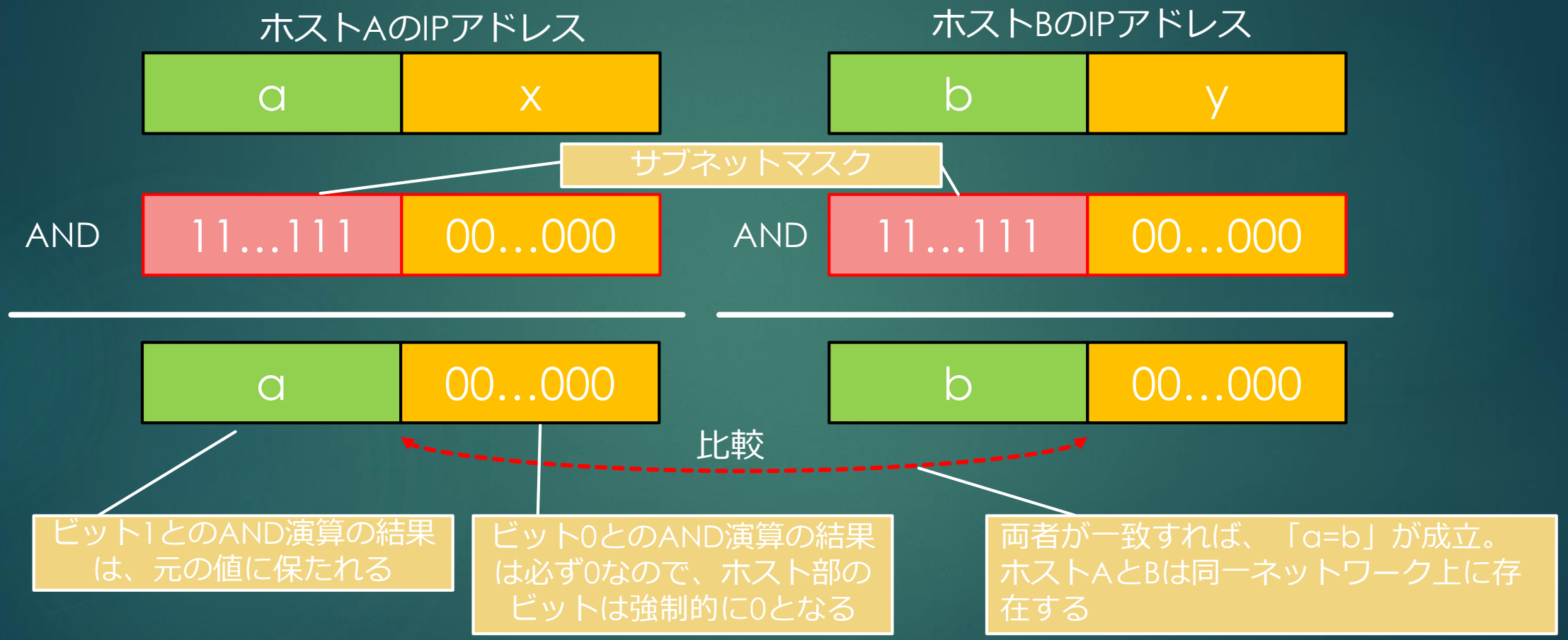
- ネットワーク部およびサブネット識別子の比較は、実際にはIPアドレスから「ホスト部のビットを0にしたアドレス」を生成して行う。ホスト部のビットのみを0にするためには、

・ネットワーク部およびサブネット識別子のビットがすべて1

・ホスト部のビットがすべて0

というマスクパターンを用意して、これとIPアドレスとの論理積をとる。このとき用いるマスクパターンを**サブネットマスク**とよぶ。

データ送信とサブネットマスク



データ送信とサブネットマスク

- サブネットマスクのビット1の部分は、IPアドレスのネットワーク部およびサブネット識別子部分に対応する。この部分が大きくなればなるほど、分割の進んだ小さなネットワークを表す。

IPv6

- 現在、主流となっている**IPv4**で用いられるIPアドレスは32ビットであり、世界的なインターネット普及に伴ってIPアドレスの数が枯渇している。そこで**IPv6**とよばれる後継規格が策定された。IPv6は、

・**IPアドレスの128ビット化**

・ルータから通知される情報と自身が生成する情報からアドレスを自動生成する、**プラグアンドプレイの実現**

・IPsecを標準機能とすることによる**セキュリティ機能充実**

といったIPv4の弱点を補う特徴をもつ。

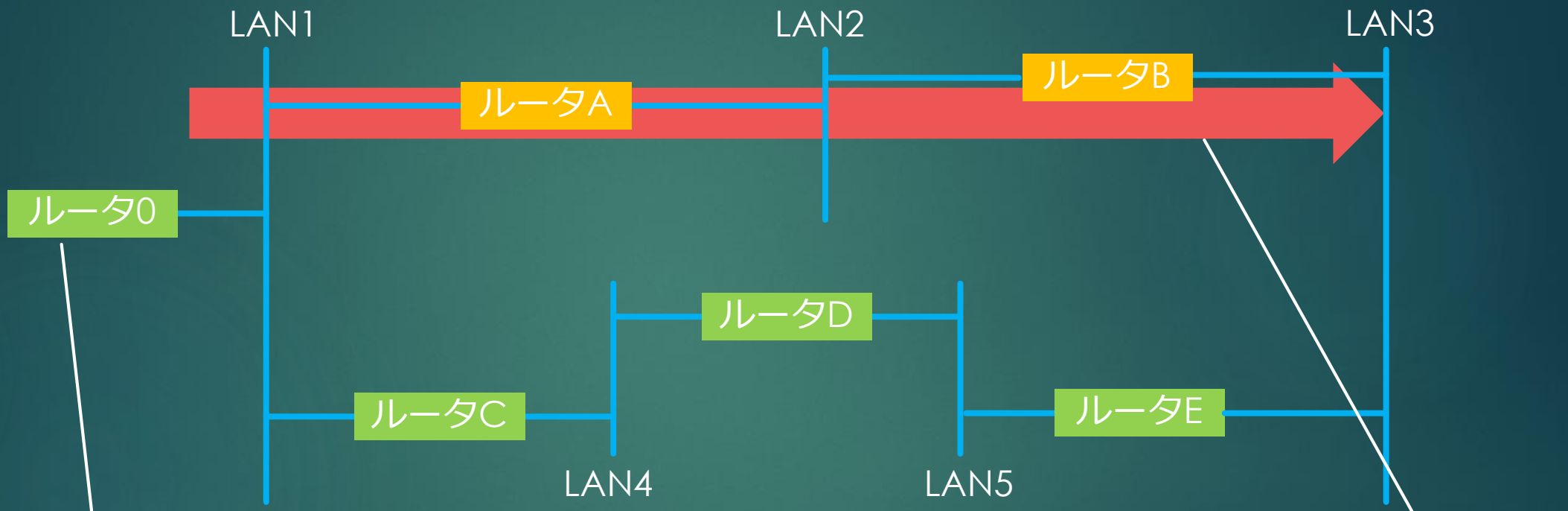
ルーティング

- **ルーティング**は、パケットを送る最適な経路を選択することである。
- ルーティングは、ルーティングテーブルに記録された経路情報に従って行われる。経路情報の設定・維持に用いるプロトコルを特にルーティングプロトコルという。
- ルーティングプロトコルの種類

RIP	**ホップ数（経由するルータ数）が最小となる経路を選択する** 距離ベクタ型のルーティングプロトコル。 単純だが中継するリンクの状態を経路に反映できない
OSPF	中継する**リンクの状態を加味して経路を選択**する リンクステート型のルーティングプロトコル

- RIPは古くから用いられてきたルーティングプロトコルで、あて先LANごとに「ホップ数の最も小さな経路」をルーティングテーブルに記録する。

ルーティング



LAN1は直接
LAN2はルータA経由で1ホップ
LAN3はルータA経由で2ホップ
LAN4はルータC経由で1ホップ
LAN5はルータC経由で2ホップ

ルータ0のルーティングテーブル

LAN3へは、ルータAを経由するホップ数2の経路が最短

ICMP(Internet Control Message Protocol)

- ICMPとは、IPを利用した通信においてエラーメッセージや制御メッセージなどを転送するためのプロトコルである。
- ICMPのメッセージ

TYPE	内容	意味
0	エコー応答	エコー要求に対する応答
3	あて先到達不能	送信元ホストにパケットが到達しない原因を通知する
5	リダイレクト	最適ルートが使用されていない場合に最適ルータを通知する
8	エコー要求	あて先ホストまでの到達確認
11	時間超過	TTL(Time To Live)値が0になったことを通知する

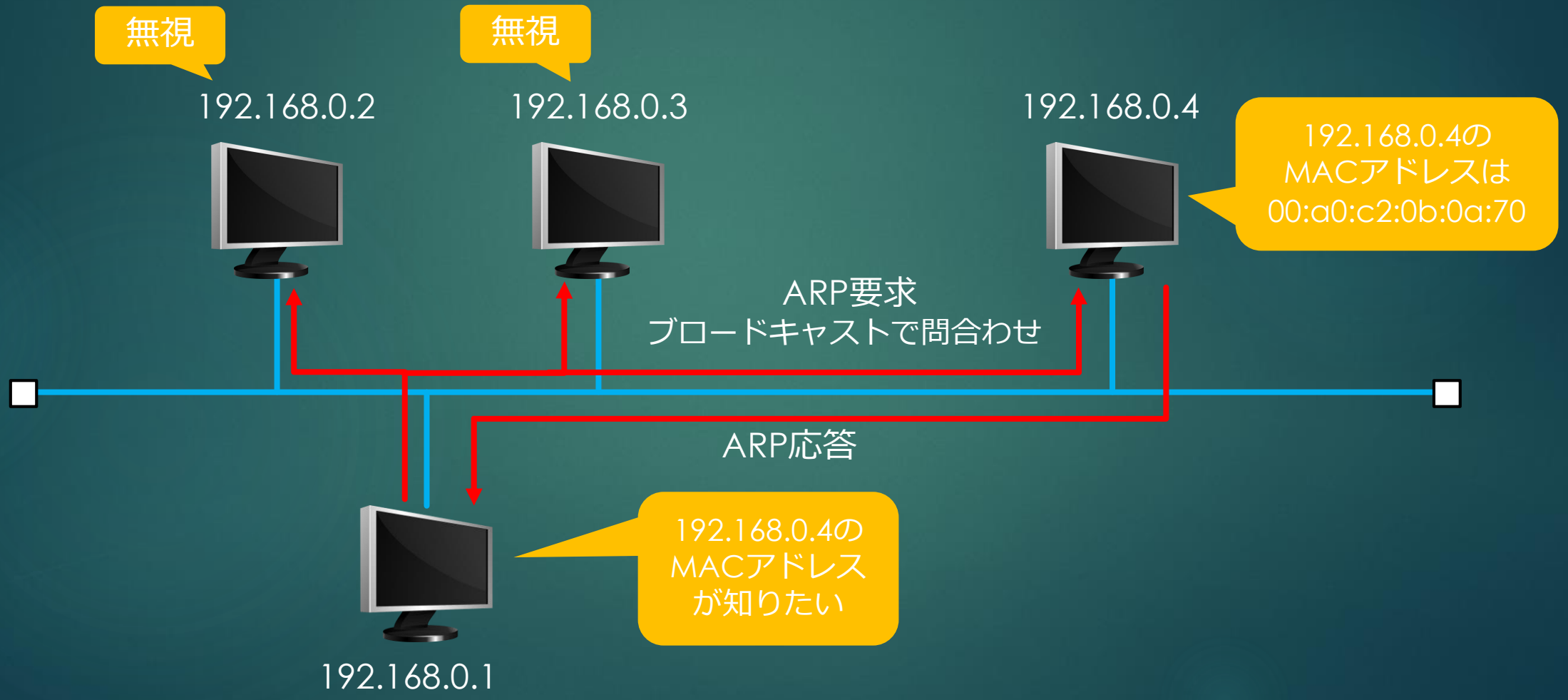
- ICMPを利用したプログラムに**ping**がある。pingは、ICMPの**エコー要求**と**エコー応答**を利用してネットワークの到達確認を行う

ARP/RARP(Address Resolution Protocol Reverse ARP)

- ホストがフレームを中継先に送出するためには、中継先のMACアドレスが必要となる。ところが、TCP/IPにはMACアドレスを一元管理する仕組みがなく、MACアドレスの記録や管理は個々のホストに任されている。そのため、ホストの起動直後などにおいて「中継先のIPアドレスは判明しているがMACアドレスがわからない」という状況がおこる。このような場合に、IPアドレスからMACアドレスを問い合わせる**ARP**が用いられる。

- ARPは、MACアドレスを問い合わせる**ARP要求**と、それに応える**ARP応答**からなる。**ARP要求はネットワーク中の全ノードに対するブロードキャストで、ARP応答は要求したノードへのユニキャスト**である。

ARP/RARP(Address Resolution Protocol Reverse ARP)



ARP/RARP(Address Resolution Protocol Reverse ARP)

- ARPとは逆に、MACアドレスをもとにIPアドレスを問い合わせるプロトコルが**RARP**である。RARPはディスクレスマシンなど、IPアドレスを記録できない機器が、自身のIPアドレスを問い合わせる場合に利用される。

4. トランスポート層
コネクション / コネクションレス

- TCP/IPのトランスポート層には、信頼性の高い**コネクション型**の通信方式と、簡素で高速な**コネクションレス型**の通信方式が用意されている。
- コネクション型通信は、信頼性を高めるため、

・パケットの**順序制御**

・誤りを検出した際の**再送制御**

・受信能力の範囲内でパケットを送信する**フロー制御**

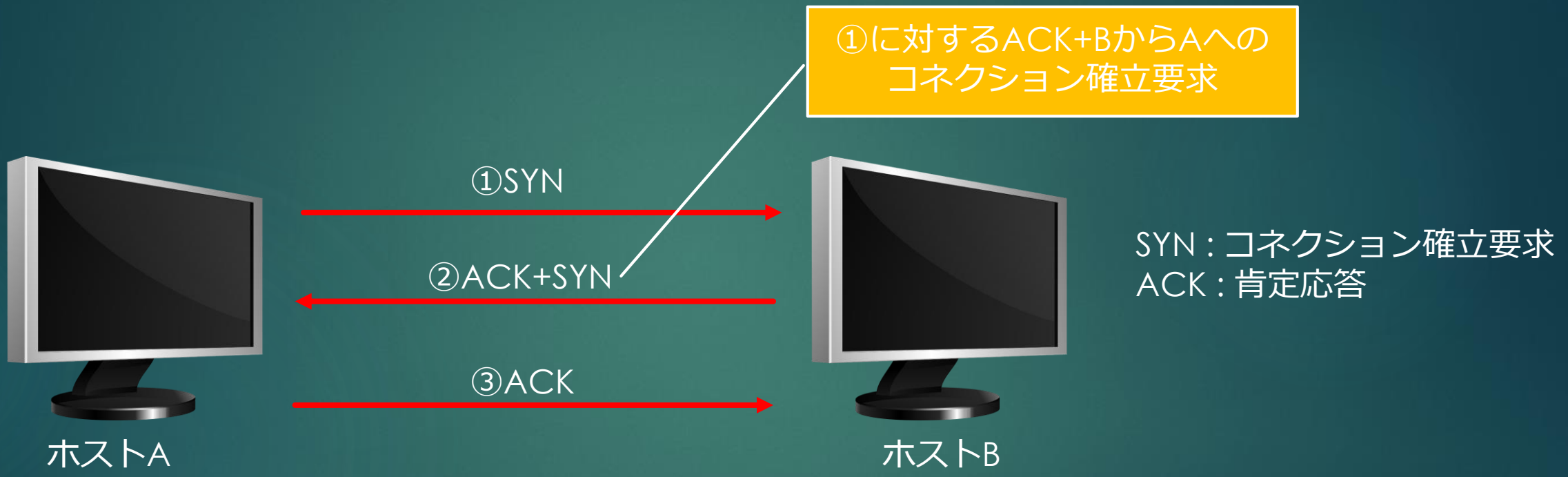
などの各種制御を行う。

- これに対し、コネクションレス型は「パケットを送ること」のみを目的とする方式で、各種制御を省いた高速な通信を実現する。

TCP

- **TCP**は、TCP/IPのトランスポート層のプロトコルの一つで、**信頼性の高いコネクション型の通信機能**を提供する。電子メールやファイル転送、HTTPなど信頼性の高い通信機能が必要なアプリケーションは、トランスポート層のプロトコルにTCPを選ぶ。
- TCPは、通信に先立って**TCPコネクション**とよばれる論理的な通信路を確立し、通信終了時にそれを解放する。コネクション確立のため、**スリーウェイハンドシェイク**とよばれる手順を行う。

スリーウェイハンドシェイク



SYN：コネクション確立要求
ACK：肯定応答

UDP / フロー制御

- **UDP**は、TCP/IPのトランスポート層のプロトコルの一つで、**コネクションレス型の簡素な通信機能**を提供する。IP電話や動画の配信、SNMP（ネットワーク管理）など、（音声や画像上の）少々の乱れよりも高いリアルタイム性を重視するアプリケーションは、トランスポート層のプロトコルにUDPを用いる。

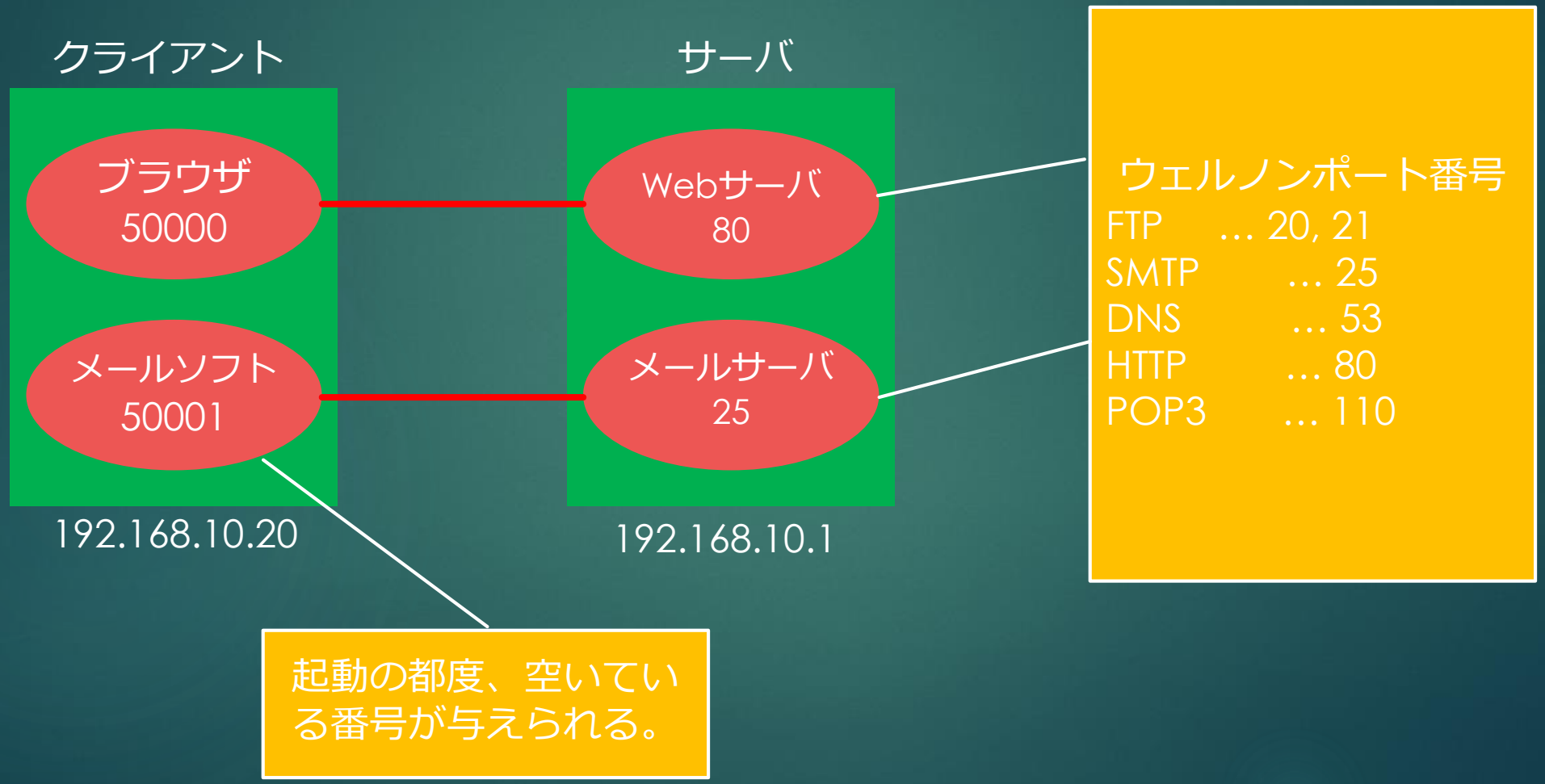
- **フロー制御**は通信相手の受信能力を超えないよう、**送信データの量を調整する制御**である。TCPでは**ウィンドウサイズ**（連続受信できるデータ量）を送信相手から適宜通知してもらい、ウィンドウサイズの範囲内でデータを連続送信する。

ポート番号

- **ポート番号**は、16ビットからなる**プロセスの識別番号**である。ポート番号とホストを識別するIPアドレスを組み合わせれば「どのホストのどのプロセスか」を識別することができる。

- サーバなどの常駐プロセスには、あらかじめ定まったポート番号（**ウェルノンポート番号**）が与えられている。クライアントのプロセスには、起動ごとに空き番号が与えられる。

ポート番号


クライアント
サーバ
ブラウザ
50000
メールソフト
50001
Webサーバ
80
メールサーバ
25
192.168.10.20
192.168.10.1
ウェルノンポート番号
FTP … 20, 21
SMTP … 25
DNS … 53
HTTP … 80
POP3 … 110
起動の都度、空いている番号が与えられる。

5. アプリケーション層 WWW(World Wide Web)

- **WWW**は、インターネットにおいて最も多く利用されるサービスの一つで、ブラウザとWWWサーバとの間でHTML文書のやり取りをする。このやり取りに用いるプロトコルがHTTPである。

- **URL(Uniform Resource Locator)**

URLは、HTML文書を含め、**インターネット上のリソースを指定する書式**である。URLでは、リソースにアクセスするための**スキーム**（プロトコル）、サーバ名（IPアドレスも可）、ディレクトリ名、ファイル名、ポート番号などが指定される。

http://www.waseda-university.co.jp : 80/rikou/joho/index.html

スキーム（プロトコル）　サーバ名　ポート番号　パス

WWW(World Wide Web)

- **HTTP(Hyper Text Transfer Protocol)**

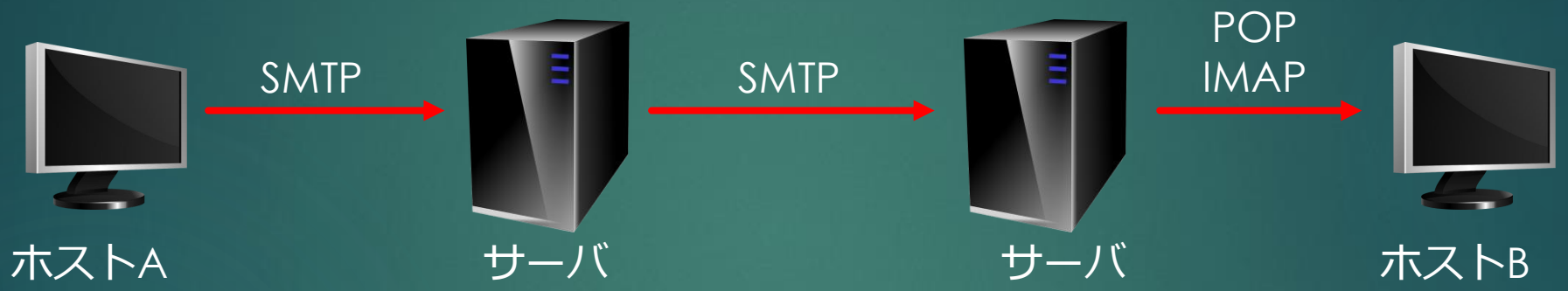
HTTPは、クライアントの要求に対して、WWWサーバが要求に基づいたリソースを送信するプロトコルである。リソースは、HTML文書のほか、画像ファイルや実行ファイル、音楽ファイルなどであっても構わない。**HTTPS**は、SSLによる暗号化通信を実装した「HTTPのセキュリティ強化版」である。

- **CGI(Common Gateway Interface)**

CGIは、WWWサーバがブラウザの要求に応じて**プログラムを起動するための仕組み**である。ブラウザがURLにCGIを指定してWWWサーバにアクセスすると、サーバ側ではアプリケーションプログラムが起動され、その処理結果がブラウザに返ってくる。

電子メール

- 電子メールは、WWWと並ぶインターネットの代表的なサービスである。
  電子メールサービスを実現するため、次のプロトコルが用いられる。

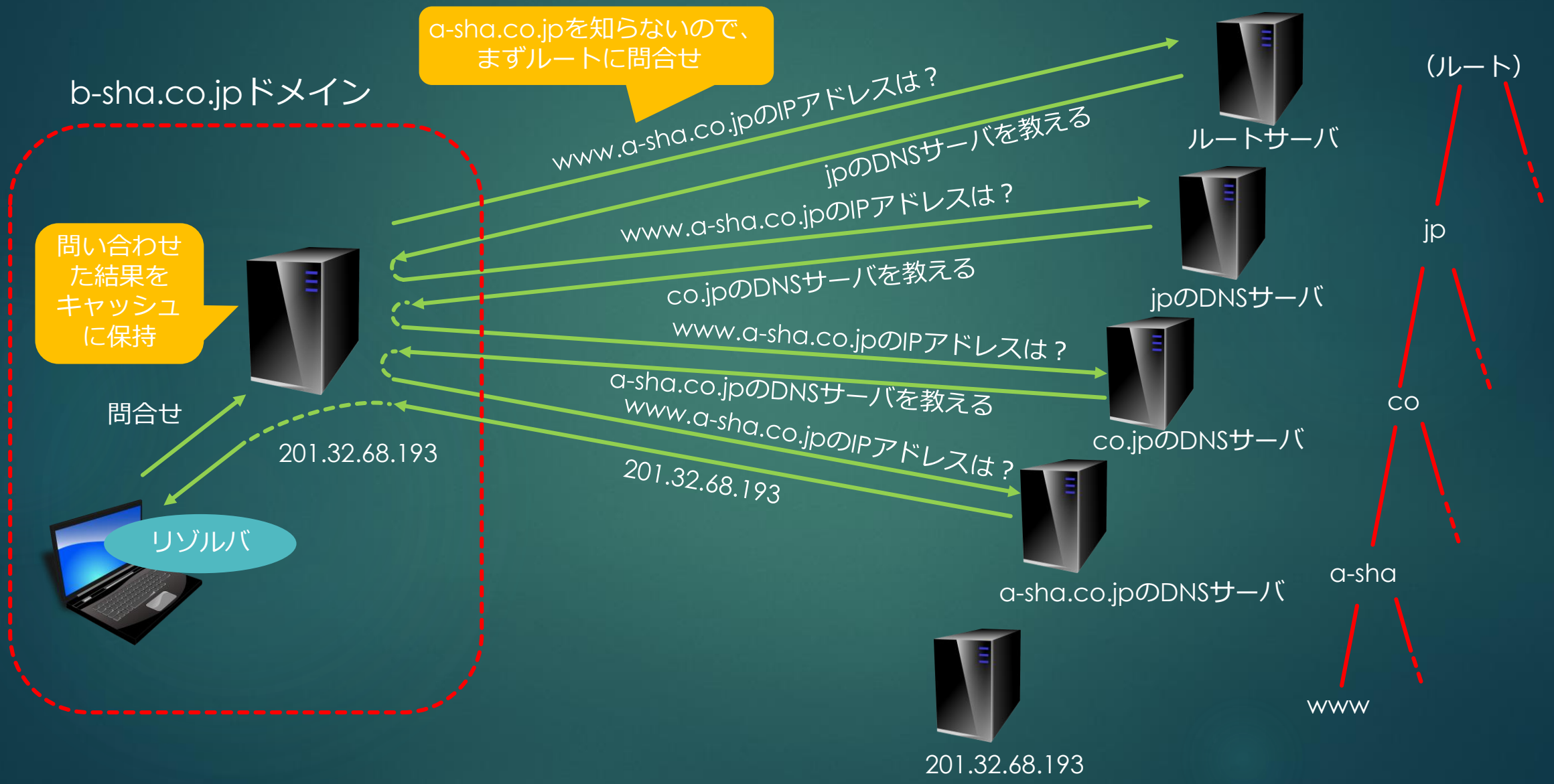


SMTP	電子メールの転送プロトコルで、メールサーバへの送信、サーバ間のメール転送に用いる。
POP	電子メールの受信（メールサーバからの取り出し）に用いるプロトコル。受信メールはクライアントにダウンロードされ、**クライアント上で管理**する。現行のバージョンはPOP3。
IMAP	電子メールの受信に用いるプロトコル。POPとは異なり、**メールはサーバ上で管理**される。現行バージョンはIMAP4。

DNS(Domain Name System)

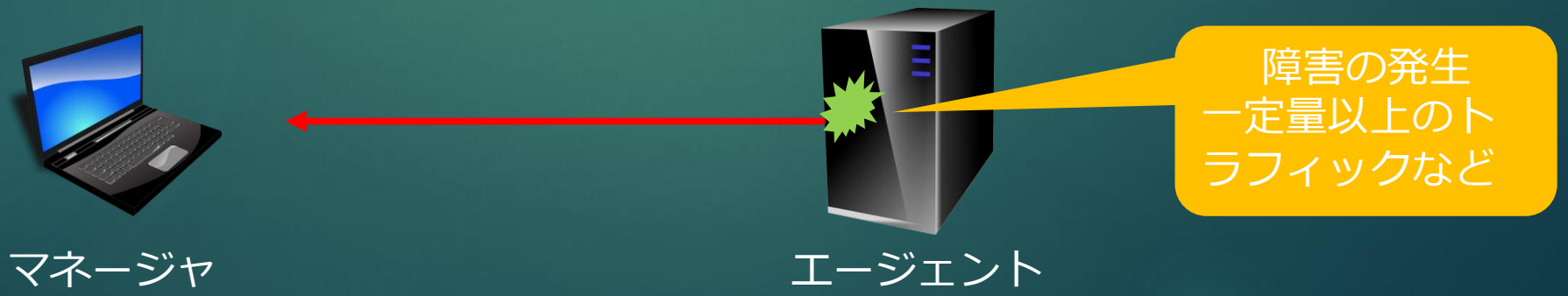
- URLにせよメールアドレスにせよ、ホストの指定にはホスト名（ドメイン名）を使う。これを、ホストを表すIPアドレスに変換する（名前を解決する）ことがDNSの役割である。インターネットでは、ホストの指定にIPアドレスを用いることはまずありえない。したがって、DNSはインターネットを支える基盤といえる。
- 名前解決を行う場合、クライアントはまず「自ドメインのDNサーバ」に対して問い合わせを行う。このとき、問い合わせの対象となるドメイン名が自ドメインのものであれば、自ドメインのDNSサーバが直接返答することになる。
- 一方、目的のドメイン名が他ドメインに属する場合、自ドメインのDNSサーバはルートドメインから下位のドメインに向かって順に検索を繰り返し、目的のIPアドレスを取得してクライアントに回答する。

DNSの問合わせ


a-sha.co.jpを知らないので、
まずルートに問合せ
b-sha.co.jpドメイン
問い合わせた結果をキャッシュに保持
問合せ
201.32.68.193
リゾルバ
www.a-sha.co.jpのIPアドレスは？
jpのDNSサーバを教える
www.a-sha.co.jpのIPアドレスは？
co.jpのDNSサーバを教える
www.a-sha.co.jpのIPアドレスは？
a-sha.co.jpのDNSサーバを教える
www.a-sha.co.jpのIPアドレスは？
201.32.68.193
ルートサーバ
jpのDNSサーバ
co.jpのDNSサーバ
a-sha.co.jpのDNSサーバ
201.32.68.193
(ルート)
jp
co
a-sha
www

SNMP(Simple Network Management Protocol)

- **SNMP**はTCP/IPにおける**通信機器（ルータやコンピュータなど）を管理する**ためのプロトコルである。SNMPでは、管理する側を「**マネージャ**」、管理される側を「**エージェント**」という。
- エージェントでは**MIB**(Management Information Base)とよばれる、管理される項目の集合（一種のデータベース）をもち、マネージャの指示によって設定変更や情報の通知を行う。
- SNMPに特有の**トラップ**(trap)という機能もある。これは、エージェントに特定のイベントが発生した場合に、**自律的にマネージャに通知する**機能である。



DHCP(Dynamic Host Configuration Protocol)

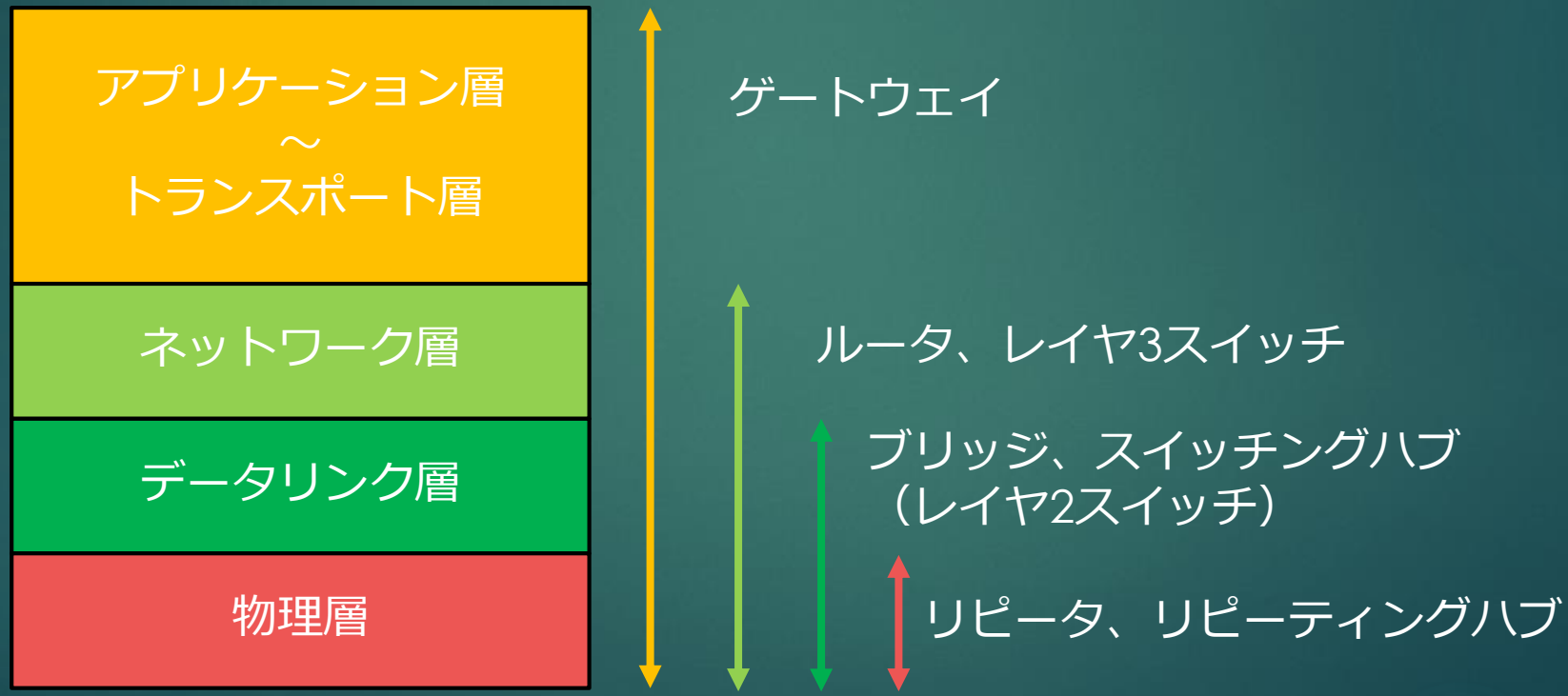
- **DHCP**とは、IPアドレス、アブネットマスク、デフォルトゲートウェイ、DNSサーバといった**ネットワーク接続に必要な設定を自動化する**プロトコルである。DHCPを利用することにより、管理者の負荷の軽減や設定情報の一元管理などが可能となる。

その他のプロトコル

- その他アプリケーション層のプロトコル

FTP	**File Transfer Protocol**	ファイルを転送に用いるプロトコル
NTP	**Network Time Protocol**	時刻を同期するプロトコル
SIP	**Session Initiation Protocol**	セッションの確立に用いるプロトコル。 IP電話に用いられることが多い。

6. LAN間接続
LAN間接続機器とプロトコル階層



LAN間接続機器とプロトコル階層

- **リピータ、リピーティングハブ**

リピータは、LAN同士を**物理層で接続する**装置で、複数ポートをもつリピータを特に**リピーティングハブ**とよぶ。リピータは電気信号の整形・増幅を行う機能をもち、LANを延長（伝送距離の延長）する際に用いられる。

- **ブリッジ、レイヤ2スイッチ**

ブリッジは、LAN同士を**データリンク層で接続する**装置で、複数ポートをもつ機器を特に**スイッチングハブ（レイヤ2スイッチ）**とよぶ。ブリッジは、データリンク層のアドレスであるMACアドレスに従って、フレームを中継する。ブリッジを用いると、必要なポートにのみフレームを流すため、不要なトラフィックを発生させない。

LAN間接続機器とプロトコル階層

- **ルータ、レイヤ3スイッチ**

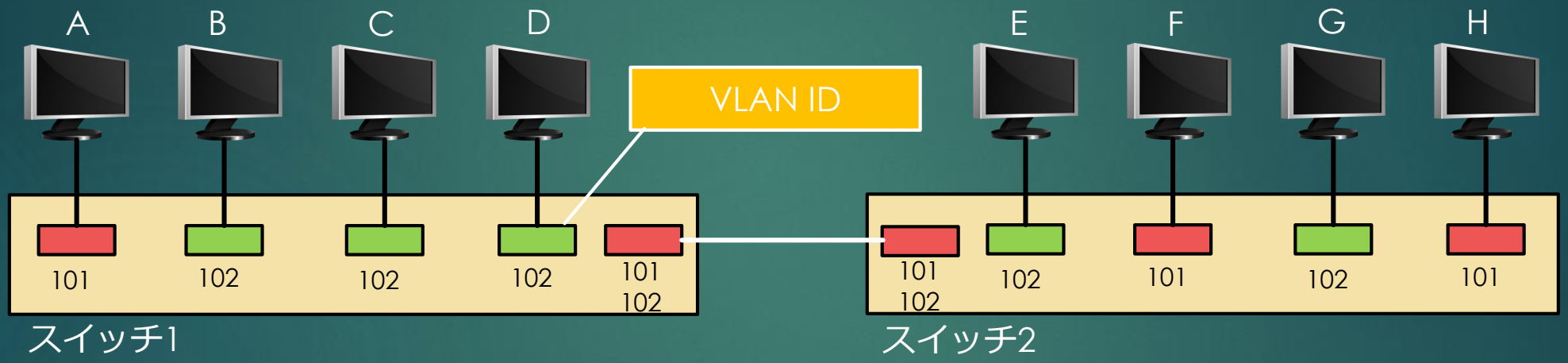
ルータは、LAN同士を**ネットワーク層で接続する**装置で、複数ポートをもつ機器を特に**レイヤ3スイッチ**とよぶ。ネットワーク層のアドレスであるIPアドレスに従い、最適な経路でパケットを中継することができる。ルータは、根とワーク層までのプロトコル変換機能をもつため、伝送媒体やアクセス制御方式の異なるLAN同士を接続することができる。

- **ゲートウェイ**

ゲートウェイは、LAN同士を**アプリケーション層で接続する**装置である。ゲートウェイは、アプリケーション層を含む全階層のプロトコルを解析・変換できるため、プロトコルが完全に異なるLANであっても接続することができる。

VLAN(Virtual LAN)

- **VLAN**とは、スイッチングハブのポートや接続される端末などをグループ化することで、**物理的な接続形態に依存しない論理的なネットワーク（仮想的なLAN）を構築する**技術である。



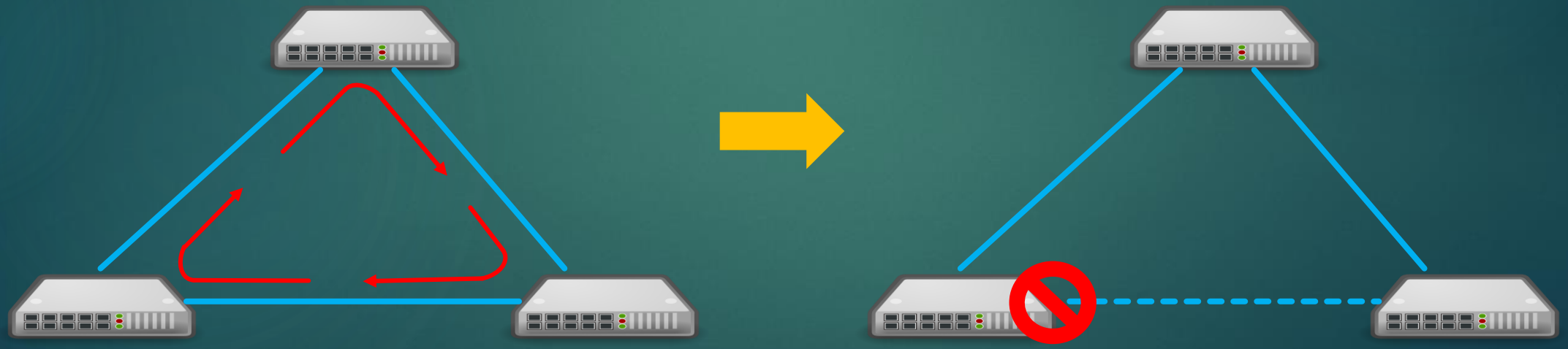
- LAN1：A, B, C, D　LAN2：E, F, G, HとLANが分かれるところだが、これをスイッチ1, 2のポートにID=101と102と割り振ることで、

LAN1：B, C, D, E, G　LAN2：A, F, Hという二つのLANに「配置や接続するスイッチに関わりなく」分けている。

- VLANを用いるとブロードキャストドメインも分割されるため**通信量の削減**を図ることができる。

スパニングツリー

- ブリッジやスイッチングハブは、受信したブロードキャストフレームをすべてのポートに送出する。そのため、通信経路上にループがあると、ループ中をブロードキャストフレームが循環し続けることになる。これを、**ブロードキャストストーム**とよぶ。これを防ぐためには、ポートの一部をブロックしてループを切断する必要がある。これを行うプロトコルを**スパニングツリープロトコル(STP)**とよぶ。



物理的なループを

論理的には木（ツリー）で扱う

VRRP(Virtual Router Redundancy Protocol)

- **VRRP**は**ルータを冗長化してネットワークの信頼性を高める**プロトコルである。複数のルータをグループにまとめ、その中の一つをマスタルータとして、他をバックアップルータとする。マスタルータの障害時には、自動的にバックアップルータに切り替わる。

7. インターネット技術
プロキシサーバ

- **プロキシ（proxy：代理）サーバ**とは、「クライアントからの要求を受け、クライアントの代理として他のサーバにアクセスする」サーバであり、WWWにおいて多く用いられる。これには、以下のような利点がある。

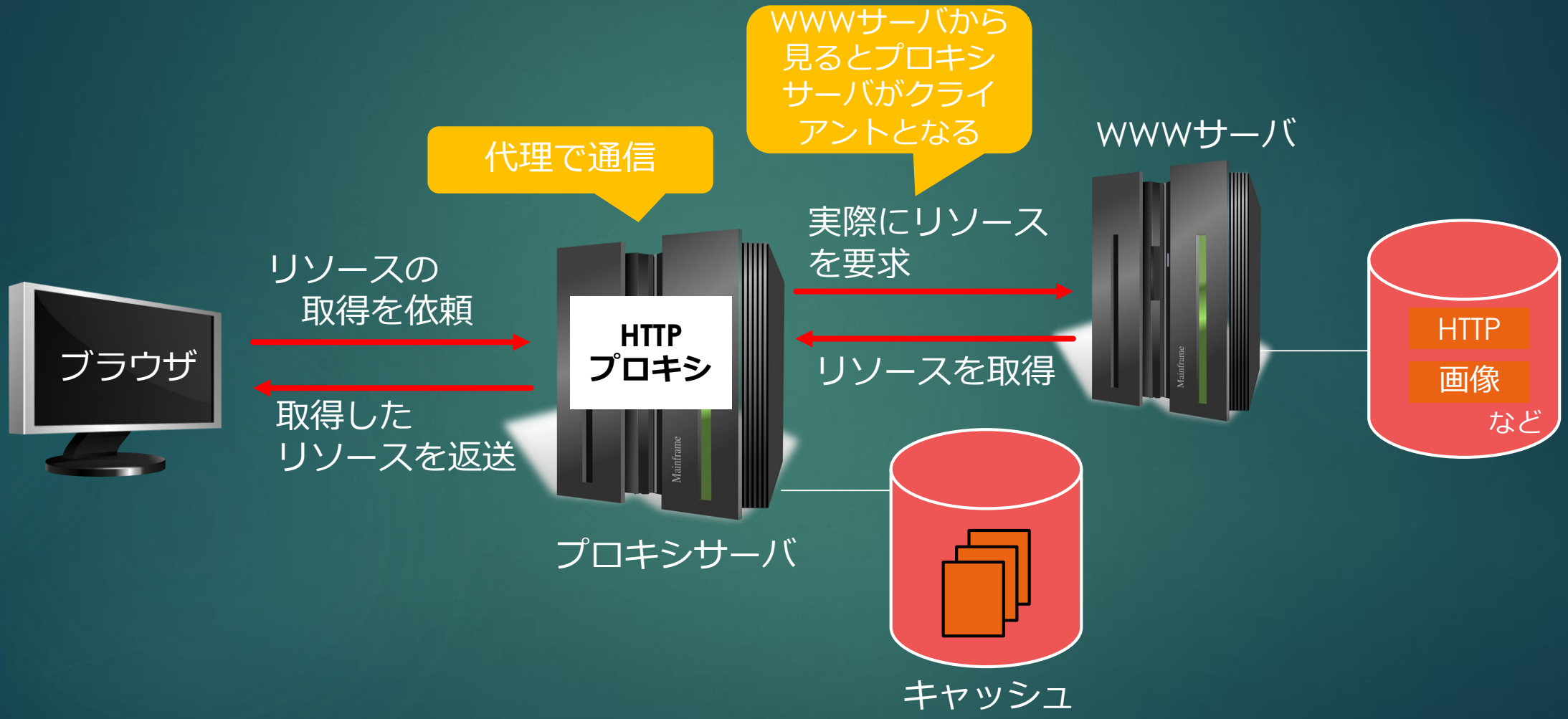
・キャッシュサーバとしての利用

クライアントから要求されたリソースがプロキシサーバ内にキャッシュされていれば、インターネットにはアクセスせずキャッシュされたリソースを返す。これにより、**応答性能を向上**させたり**トラフィック（通信量）を削減する**ことができる。

・セキュリティの向上

インターネットからは「プロキシサーバのみがアクセスしている」ように見えるため、**ネットワーク内部の構成を隠す**ことができる。

プロキシサーバ


WWWサーバから
見るとプロキシ
サーバがクライ
アントとなる
代理で通信
WWWサーバ
実際にリソース
を要求
リソースの
取得を依頼
ブラウザ
HTTP
プロキシ
リソースを取得
HTTP
画像
など
取得した
リソースを返送
プロキシサーバ
キャッシュ

NAPT

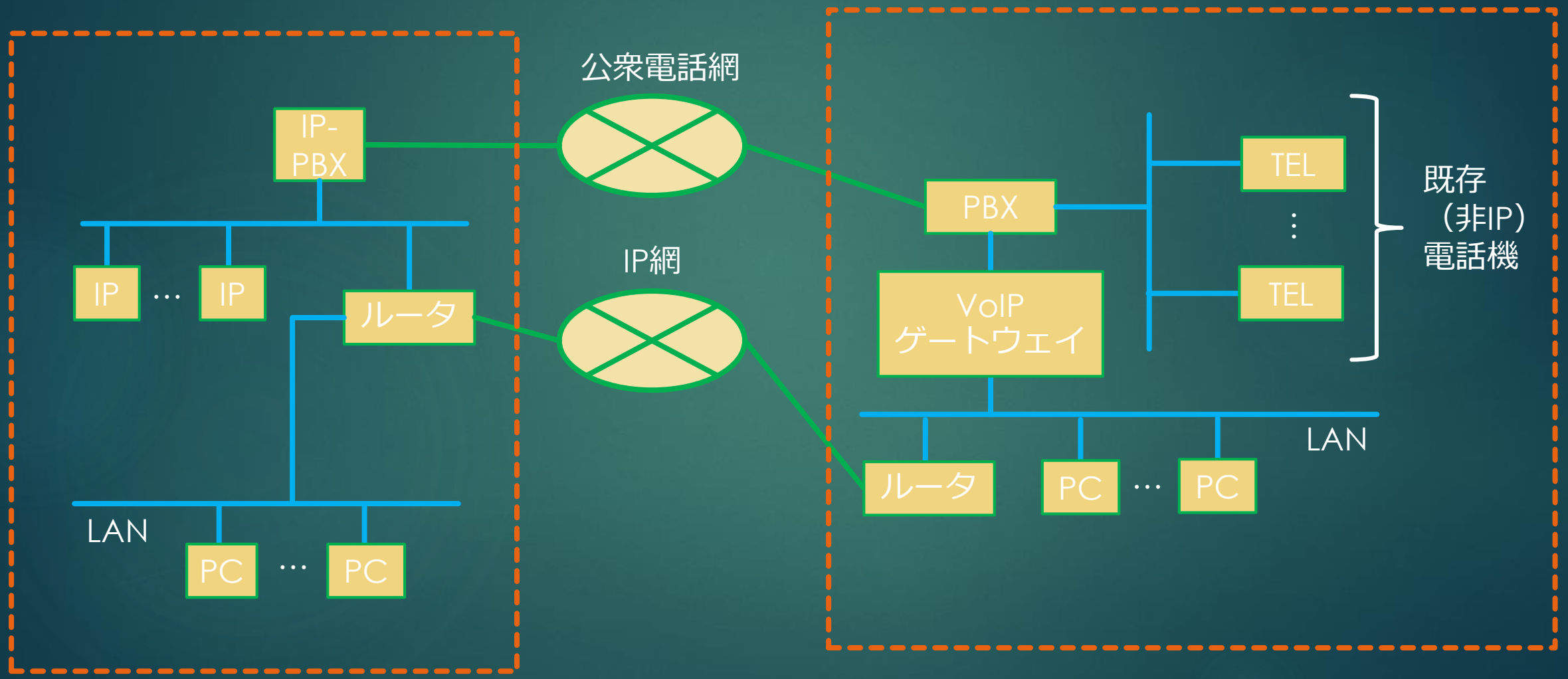
- IPv4形式のIPアドレスは既に枯渇している。そのため、組織内のホストには利用の制限のないプライベートIPアドレスを割当て、インターネットにアクセスするときのみグローバルIPアドレスに変換する、というアドレス変換技術が使われる。グルーバルIPアドレスはインターネットとの接点に割り当てればよいので、グローバルIPアドレスを節約することができる。

NAT	グローバルIPアドレスとプライベートIPアドレスを**1対1で対応づける**。 同時にインターネットと通信できるホストの数は、接点にプールしたグローバルIPアドレス数が上限となる
NAPT	対応づけの情報にポート番号を加えることで、**一つのグローバルIPアドレスに複数のプライベートIPアドレスを対応づける**ことができる。 接点に一つのグローバルIPアドレスを用意しておけば、同時に複数のホストがインターネット通信できる。

IP電話

- 符号化した音声データをIPネットワークで伝送する技術を**VoIP(Voice over IP)**という。VoIPを用いて音声を送受信するシステムが**IP電話**である。
- IP電話では、IP電話機や通話用ソフト（ソフトフォン）を搭載したパソコンを音声端末として利用する。IP網上のIP電話機がPSTN（公衆電話網）上の電話機と相互に通話する（外線発着信を行う）ためには、シグナリング機能やPSTNとIP網のプロトコル変換機能を持つ装置が必要である。そのような機器を**VoIPゲートウェイ**という。
- ある程度の規模になると、電話番号とIPアドレスの情報を保持して呼制御を行うサーバ（**SIPサーバ**や**ゲートキーパ**）が必要になる。特に、企業内線網にIP電話を利用する場合、内線通話や保留転送といった従来のPBX（構内交換機）の機能をもつ**IP-PBX**が用いられることが多くなる。IP-PBXは、呼制御サーバとVoIPゲートウェイの機能をもつ。

IP電話の構成例


公衆電話網
IP-
PBX
IP
…
IP
ルータ
LAN
PC
…
PC
IP網
PBX
VoIP
ゲートウェイ
TEL
TEL
既存
（非IP）
電話機
LAN
ルータ
PC
…
PC

WSN (Wireless Sensor Networks)

- **WSN**は、広範囲に張り巡らされた無線機能をもつセンサを利用して、リアルタイムなデータ通信を可能にするネットワークである。（**無線）センサネットワーク**ともよばれる。
- 元は軍事技術から出発したものであるが、現在では屋内のモニタリングから渋滞情報の収集や気象観測に至る様々な場面で利用されている。ユビキタスコンピューティングに欠かせない技術としてきたいされている。
- WSNはTCP/IPとは異なるプロトコルで動作するため、インターネットとの接続はゲートウェイを介して行われる。

8. WAN
セルリレー(ATM) / 広域イーサネット

- **セルリレー(ATM)**

ATM(Asynchronous Transfer Mode：**非同期転送モード**）は、**データを48バイトごとに区切り、5バイトのヘッダを付加**した「セル」とよばれる単位で伝送を行う方式である。ATMを用いた通信サービスは「**セルリレー**」とよぶ。ATMはセル長が短く、固定長であるため、多重化を実現しながらも遅延の少ない伝送が可能となった。

- **広域イーサネット**

広域イーサネットは、LAN間をイーサネットを用いて接続する技術である。**イーサネットフレームを直接ネットワーク上に送出できる**ため、ネットワーク層のプロトコルやルーティングプロトコルに制限がなく、ネットワークの自由度が高いことが特徴である。その反面、ネットワークの設計や運用など、利用者で管理すべき事項が多くなる。

FTTH(Fiber To The Home)

- **FTTH**とは、基地局から利用者宅内までの回線を光ファイバ化し、電話やデータ伝送などの通信サービスを統合的に提供するサービスである。広義には、光ファイバで構築されたブロードバンド網を指すこともある。

- FTTHでは、**メディアコンバータ**とよばれる機器が電気信号を光信号に変換し、伝送する。

無線系のWAN

- WANには有線系のサービスだけでなく、携帯電話網など無線を伝送媒体とするサービスもある。

W-CDMA	第3世代携帯電話で用いられる通信方式。最大伝送速度は384Kbps
	拡張規格にHSPA, HSPA+があり、最大数十Mbpsの伝送速度を得る。
WiMAX	IEEEと業界団体であるWiMAX Forumによって標準化が進められている無線通信規格 最大伝送距離は10~50km程度、最大伝送速度は数十Mbps程度である 後継規格であるWiMAX2の最大伝送速度は300Mbps程度
LTE	第4世代携帯電話に分類される通信方式。最大伝送速度は300Mbps程度

9. ネットワークの評価
伝送速度と時間

伝送時間＝伝送データ量 ／ 伝送速度

伝送速度はbps（ビット/ 秒）という単位で示される。これに次のような補助単位が加わる。

64k ビット/秒 = 64,000ビット/秒

100Mbps = 100,000,000ビット/秒

（例）100kバイトのデータを、64kbpsの回線で伝送するための時間は何秒か。

伝送速度：64kビット/秒

データ量：100×8kビット

単位をkビットに合わせる

伝送時間 ＝ 100×8÷64 = 12.5（秒）

実効的な伝送効率を考える

- ネットワークはカタログ上の性能を100%はっきできるわけではない。制御情報の伝送によるオーバヘッドや複数人での回線利用など、さまざま理由により実効的な伝送効率は低下する。計算にあたっては、カタログ上の効率ではなく実効的な効率を使う。

- 実効的な効率

回線速度の低下	回線を100%利用できない→**実効的な速度の低下** （例）100Mbpsの回線で利用率が80% 実効的な回線速度＝100×0.8 = 80Mbps
伝送情報の増加	制御情報の伝送が必要→**実効的な伝送データ量の増加** （例）送信にあたり、ファイルの大きさの30%の制御情報が付加される 実効的な伝送量＝ファイルサイズ×1.3

実効的な伝送効率を考える

（例1）512kバイトのデータを、64kbpsの回線で伝送するための時間は何秒か。なお、回線利用率（伝送効率）は80%であるものとする。

実行伝送速度：64×0.8kビット/秒

データ量：512×8kビット

伝送時間＝512×8÷(64×0.8)=80（秒）

（例2）100kバイトのデータを、64kbpsの回線で伝送するための時間は何秒か。なお、伝送にあたりデータの30%の制御情報が付加される。

伝送速度：64kビット/秒

実効的なデータ量：100×8×1.3kビット

伝送時間＝100×8×1.3÷64＝16.25（秒）

ボトルネックを考える

- いくつかの回線を経由してデータを伝送するとき、伝送速度は最も遅い回線のものになる。たとえルータやプロバイダ間を100Mbpsの光ファイバで結んでいても、ルータと端末との間が10Mbpsであれば、これがボトルネックとなり回線速度は10Mbpsとなる。

ボトルネックを考える

（例）次の構成で端末がサーバから540Mバイトのファイルをダウンロードするために必要な時間は何秒か。なお、端末 ー ルータ間の伝送効率は80%である。

端末 ー ルータ間 : 100Mbps
ルータ ー サーバ間 : 90Mbps

実行伝送速度（端末 ー ルータ） : 100×0.8Mビット/秒

伝送速度（ルータサーバ） : 900Mビット/秒

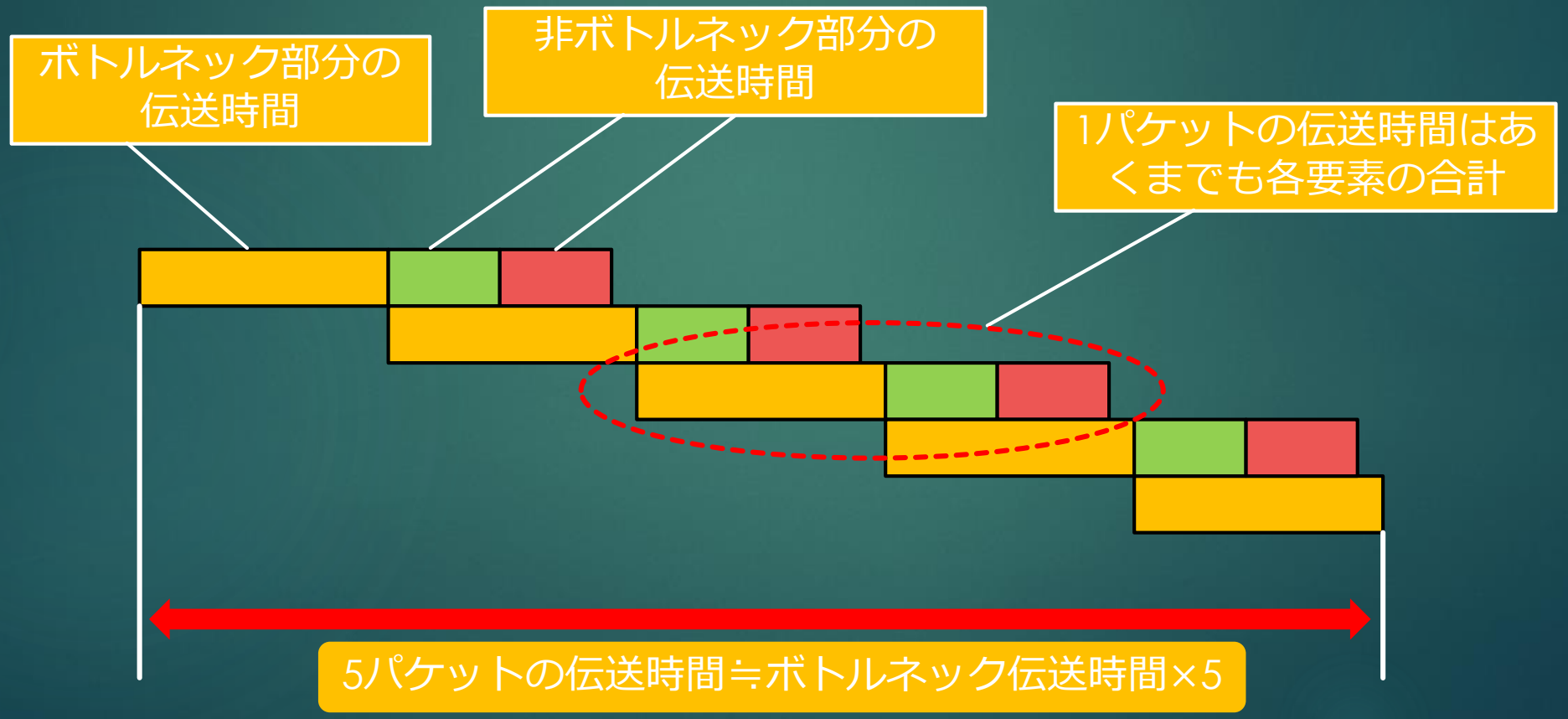
→伝送速度は80Mビット/秒で計算

データ量 : 540×8×Mビット

伝送時間＝540×8÷80＝54（秒）

各時間要素の合計を計算する

- パケットを連続して伝送する場合、全体の伝送時間はボトルネックの回線速度で計算すればよいことになる。ただし「1パケットだけの伝送時間」を精密に求めるのであれば、**各要素の伝送時間を合計**しなければならない。



各時間要素の合計を計算する

（例）次の構成で端末がフレームを送信するとき、フレームの送信を開始してからルータBがフレームの中継を終えるまでに要する時間は何ミリ秒か。

端末 ー ルータA間：10Mbps
中継回線（ルータ間）：1Mbps
ルータの中継処理：1ミリ秒/フレーム
フレーム長：1,500バイト

端末 ー ルータA間：1,500×8÷10,000,000（秒）＝1.2（ミリ秒）

ルータAの中継時間：1（ミリ秒）

中継回線：1,500×8÷1,000,000＝12（ミリ秒）

ルータBの中継時間：1（ミリ秒）

合計：1.2+1+12+1=15.2（ミリ秒）

回線利用率の計算

- ここでいう回線利用率は「回線を使用している割合」のことで「オーバヘッドを考慮した回線の利用効率」とは異なる。回線利用率は次式で求められる。

回線利用率＝伝送データ量÷回線速度

回線速度は「回線を100%使用した場合の伝送データ量」あり、これに対して「実際の伝送データ量」の割合が回線利用率である。なお、伝送データ量は回線速度と単位を合わせるため「1秒あたりのビット量」で計算する必要がある。

回線利用率の計算

（例）10MbpsのLAN上で、5kバイトのファイルを毎秒50回伝送する。このときの回線利用率は何%か。

伝送データ量：5×8×50 = 2,000kビット/秒
= 2Mビット/秒

回線速度：10Mビット/秒

回線利用率：2/10 = 0.2 = 20%

回線利用率計算上の注意

- 伝送データ量の算出においては、「他セグメントの伝送データ」が影響することもある。

From \ To	LAN1	LAN2
LAN1	5	10
LAN2	15	20

- LAN間接続装置がルータあるいはブリッジ（スイッチングハブ）であれば、LAN2固有のデータはLAN1へは流入しない。

回線利用率計算上の注意

- LAN間接続装置がルータあるいはブリッジ（スイッチングハブ）の場合

LAN1の固有のデータ量：5Mビット/秒

LAN1で発生しLAN2へ流れるデータ量：10Mビット/秒

LAN2で発生しLAN1へ流れるデータ量：15Mビット/秒

回線利用率：(5+10+15) / 100 = 0.3 = 30%

となる。

- LAN間接続装置がリピータ（リピータハブ）の場合

LAN2固有のデータであってもLAN1に中継されてしまう。個のときの回線利用率は

(5+10+15+20) / 100 = 0.5 = 50%

に悪化することになる。

回線のビット誤り率を計算する

- 回線のビット誤り率＝単位時間当たりの誤ビット数÷単位時間当たりの伝送ビット数

- （例）伝送速度64kビット/秒の回線を使ってデータを連続送信したとき、平均して100秒に1回の1ビット誤り率が発生する。この回線のビット誤り率はいくらになるか。

単位時間を100秒とすると

誤りビット数：1ビット

伝送ビット数：$64{,}000 \times 100 = 64 \times 10^5$

ビット誤り率＝$1 \div (64 \times 10^5) = 0.015625 \times 10^{-5}$

$\fallingdotseq 1.56 \times 10^{-7}$