



初級レベル研修

TCP/IPセミナー -IPアドレス編-

NETTrend ウェビナー
(技術セミナー)

一般社団法人 情報通信設備協会

内容

① TCP/IPの概要

② IPv4アドレス

③ IPv6アドレス

④ ARPとICMP

Appendix : 各種販促情報のご案内など



①TCP/IPの概要

アプリケーション層

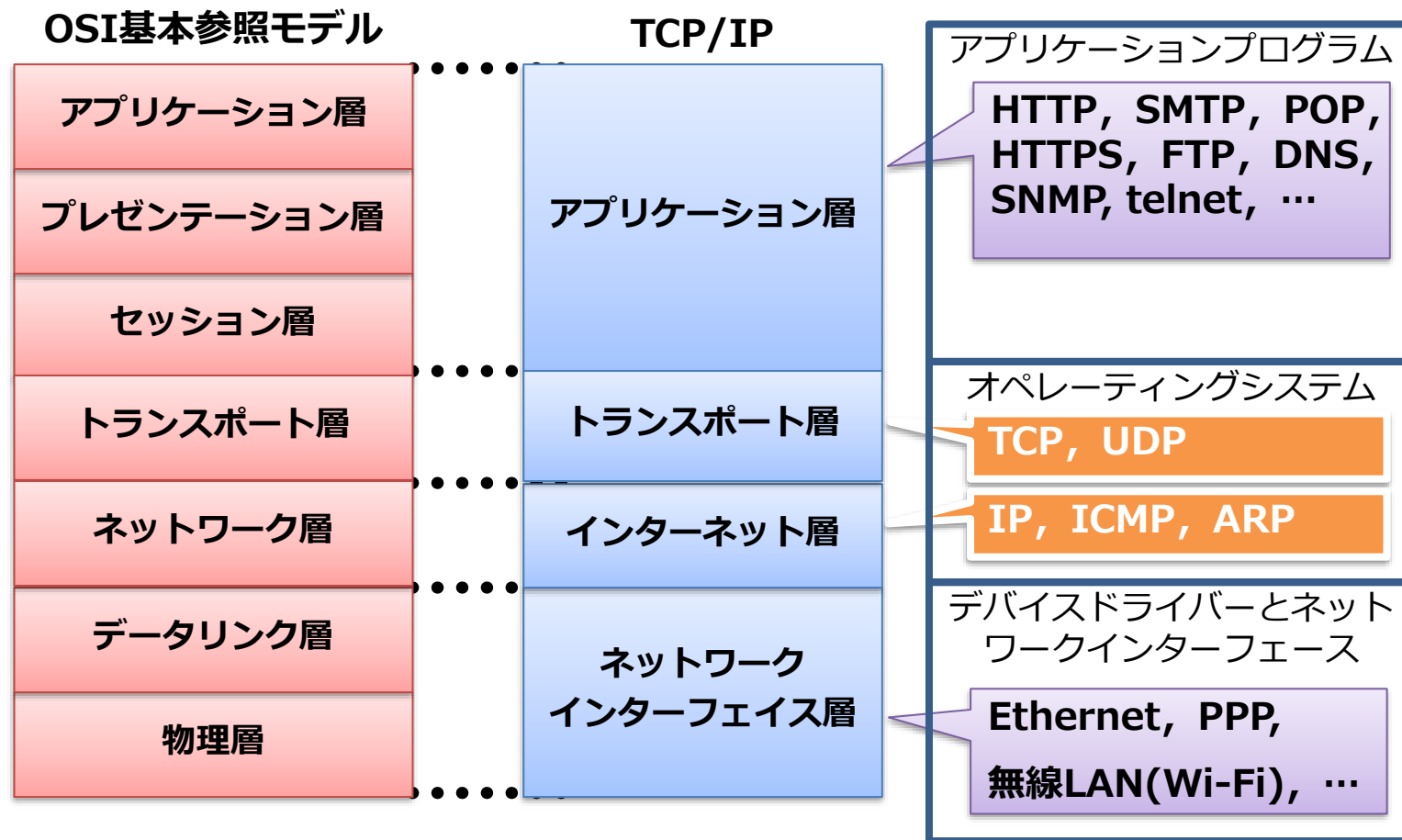
トランスポート層

インターネット層

ネットワーク
インターフェイス層

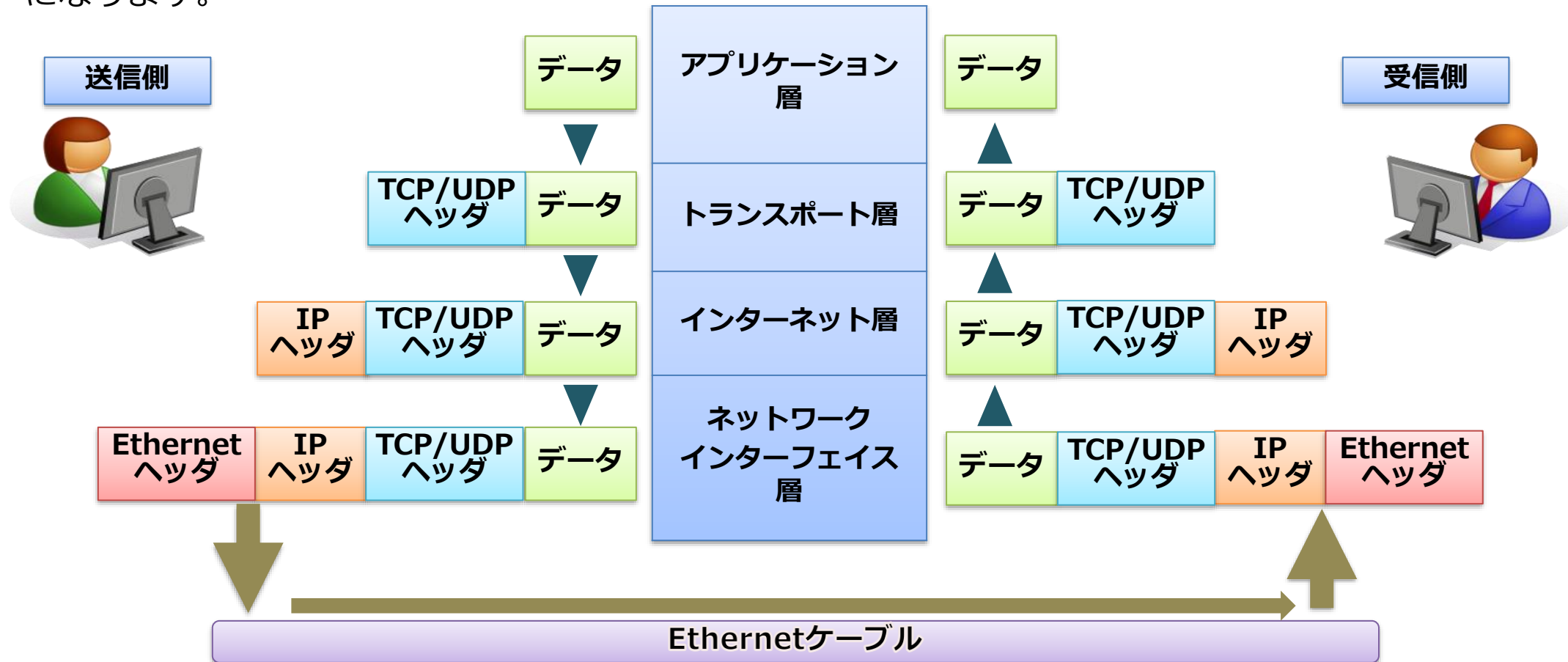
TCP/IPのプロトコル

- TCP/IPの各階層で動作するプロトコルの位置付けは以下になります。
- トランスポート層では、アプリケーションによりTCPを使用するかUDPを使用するかが異なります。また、インターネット層には、IP以外にARPやICMPというプロトコルが存在します。



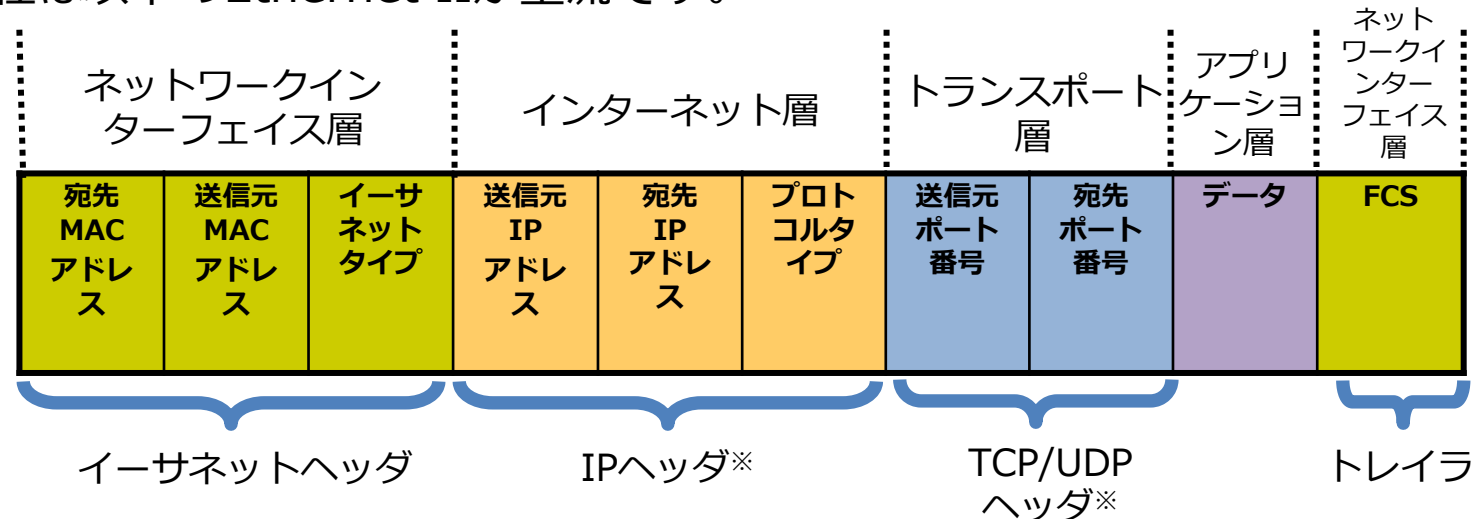
TCP/IP通信の流れ

- アプリケーション層で作成されたデータの時には、各階層で動作するプロトコルによりヘッダが付けられます。
- IPヘッダが付いたデータをパケット、Ethernetヘッダが付いたデータをフレームと呼びます。
最大パケット長(MTU: Maximum Transfer Unit)は 1,500Byte、最大フレーム長は 1,518Byte になります。



イーサネットフレーム

- イーサネット(Ethernet)フレームとは、LANの通信規格であるEthernetで使用するデータの書式になります。一般的には「MACフレーム」や「フレーム」と呼ばれます。
- フレームはパケットに以下の情報を付加し、ネットワークインターフェイス層で作成されます。
 - 宛先MACアドレス(6Byte)：フレームの宛先となる機器のMACアドレス
 - 送信元MACアドレス(6Byte)：フレームを送信する機器のMACアドレス
 - イーサネットタイプ(2Byte)：上位層のプロトコルを示します。0x0800(0xは16進数表記を意味)はIPv4、0x0806はARP、0x86ddはIPv6になります。
 - FCS(Frame Check Sequence、4Byte)：ノイズなどでフレーム全体のデータが破損されていないかどうかを検出します。
- イーサネットフレームには、Ethernet II、IEEE 802.2 LLC およびIEEE 802.2 SNAPなどの種類がありますが、現在は以下のEthernet IIが主流です。



※ IPヘッダおよびTCP/UDPヘッダには、他にも様々な値がセットされます。詳細は後述します。



②IPv4アドレス

アプリケーション層

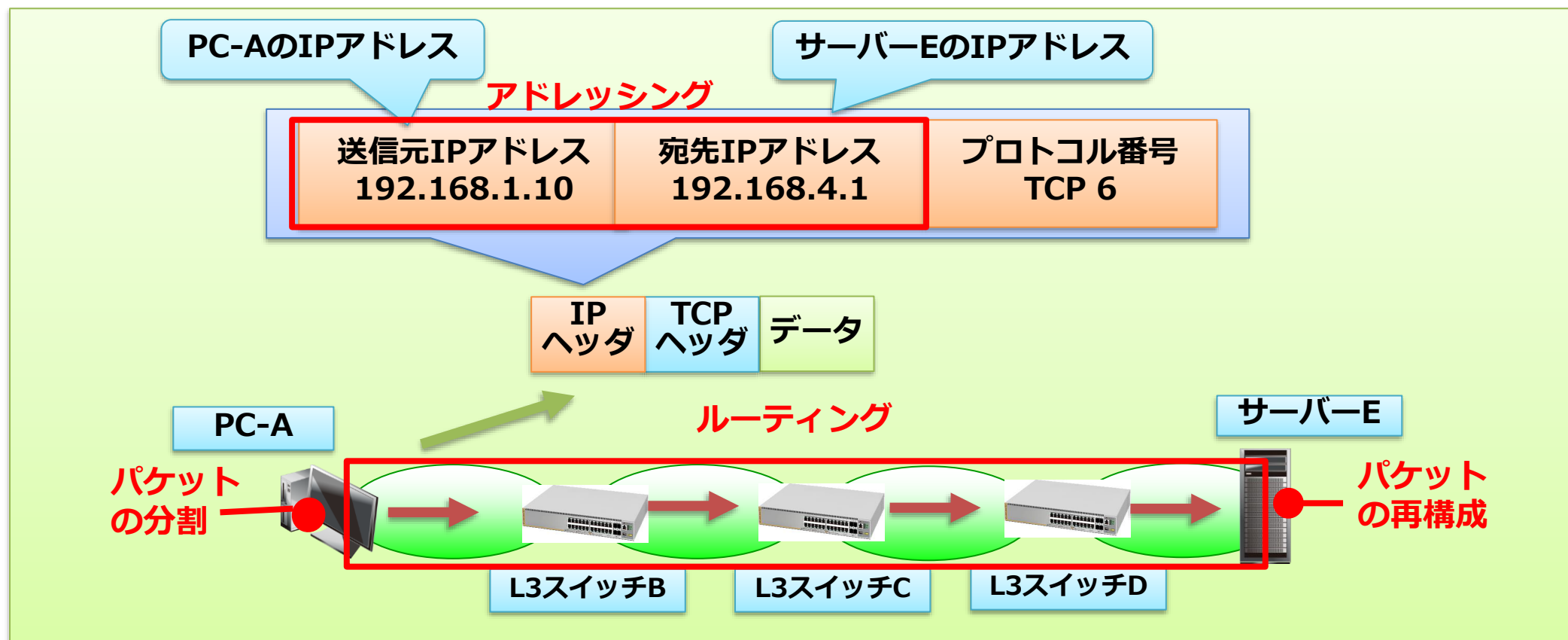
トランスポート層

インターネット層

ネットワーク
インターフェイス層

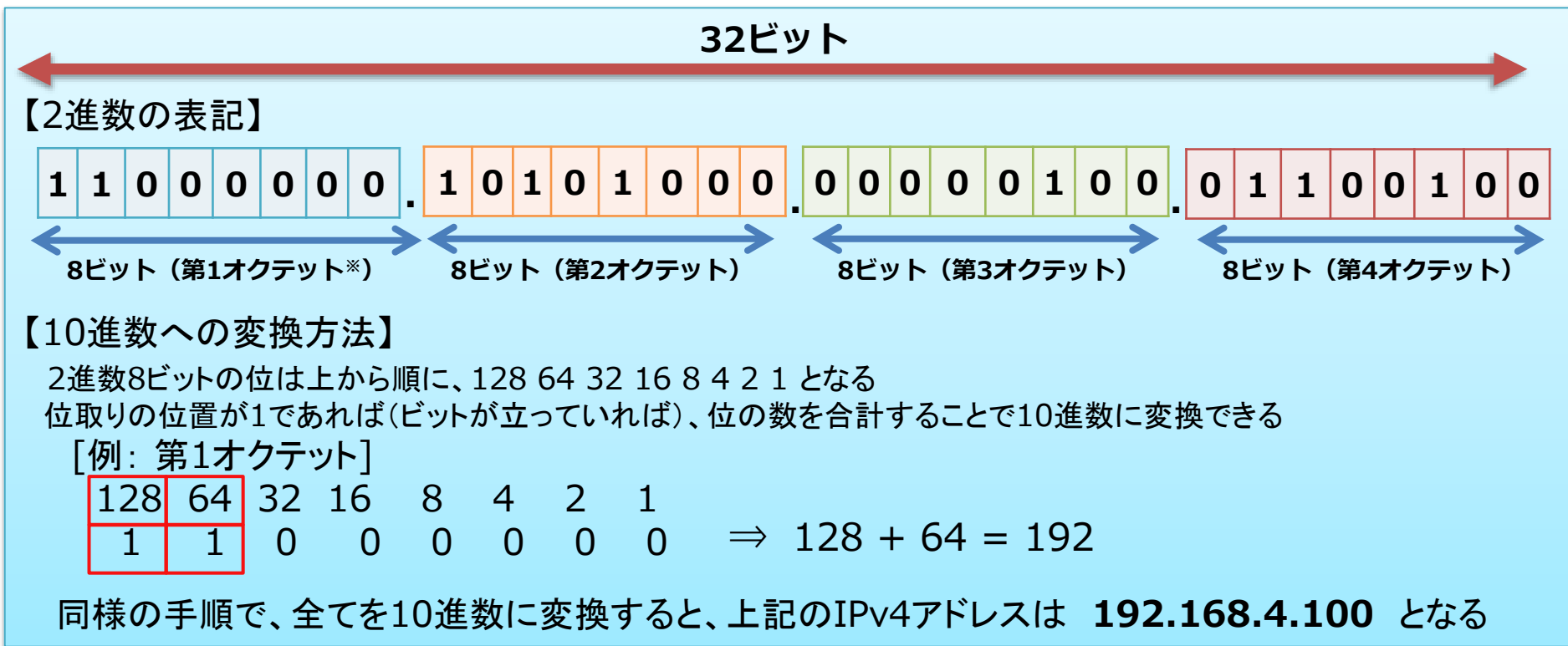
IPの役割

- IPはパケットをエンドツーエンドで相手に送信する役割を担います。
- IPには大きく分けて主に3つの機能があります。
 - 1. IPアドレスを利用した端末への個別番号の割り当て機能（アドレッシング）
 - 2. エンドツーエンドのパケット配送機能（ルーティング）
 - 3. 送信元でのIPパケットの分割や宛先でのIPパケットの再構成を行う機能



IPv4アドレス

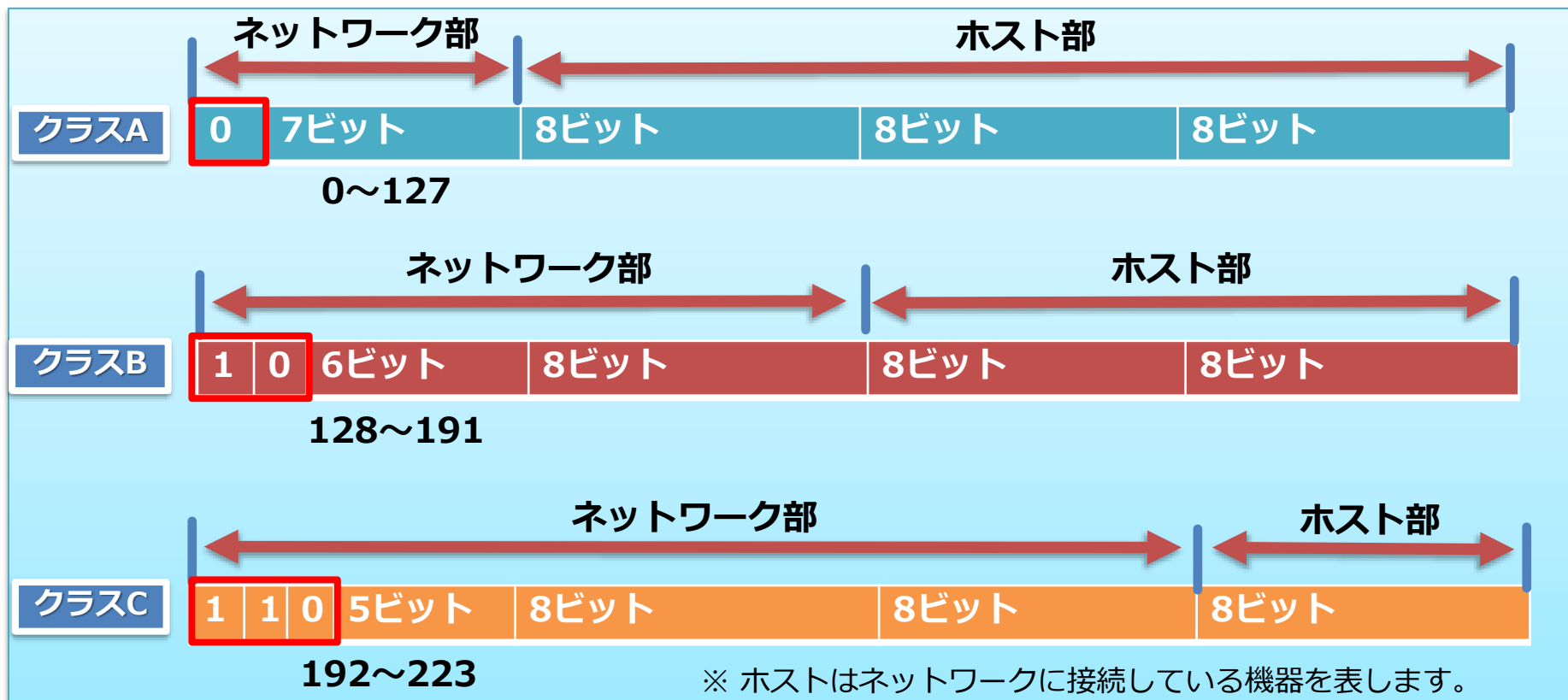
- IPv4アドレスは32ビットのアドレスです。2進数の表記では32個の0もしくは1の数値列となり人間には把握しづらいため、8ビット単位で区切り10進数で表記します。
- 現状IPv4アドレスは、アドレスの在庫が無いため、通常の申請による割り振りは終了しています。
- この問題を解消するために、 JPNIC(JAPAN Network Information Center)に返却済みIPv4アドレスからの割り振り、NATによるプライベートIPアドレスとグローバルIPアドレスの変換、IPv6アドレスへの移行などが行われています。



※ オクテット (octet) は 8ビットを表す情報量の単位です。

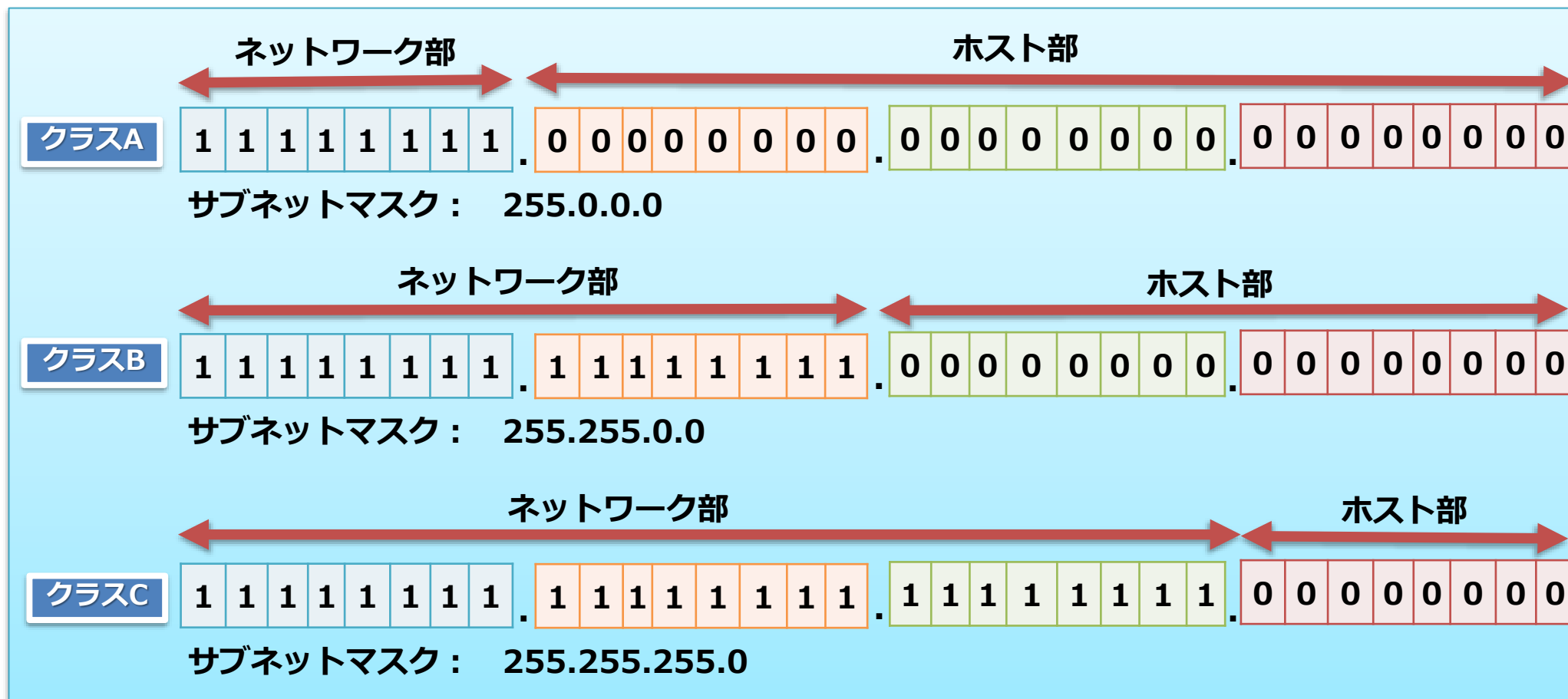
IPv4アドレスのクラス

- IPv4アドレスは、効率的なパケット配送のためにネットワーク部(ネットワークアドレス)とホスト*部(ホストアドレス)に分けられており、クラスフルアドレッシングでは先頭のクラス識別子（以下図の赤枠のビット）によりネットワーク部の長さを判別します。
- IPv4アドレスは、クラス識別子によって「クラスA」から「クラスE」までの5つに分類されています。ただし、「クラスD」はマルチキャスト通信用、「クラスE」は実験用として確保されているため、残るクラスA/B/Cが、通常のネットワーク構築に用いられ、収容できるホスト（=ネットワークに接続されている機器）数によって使い分けられています。



各クラスのサブネットマスク

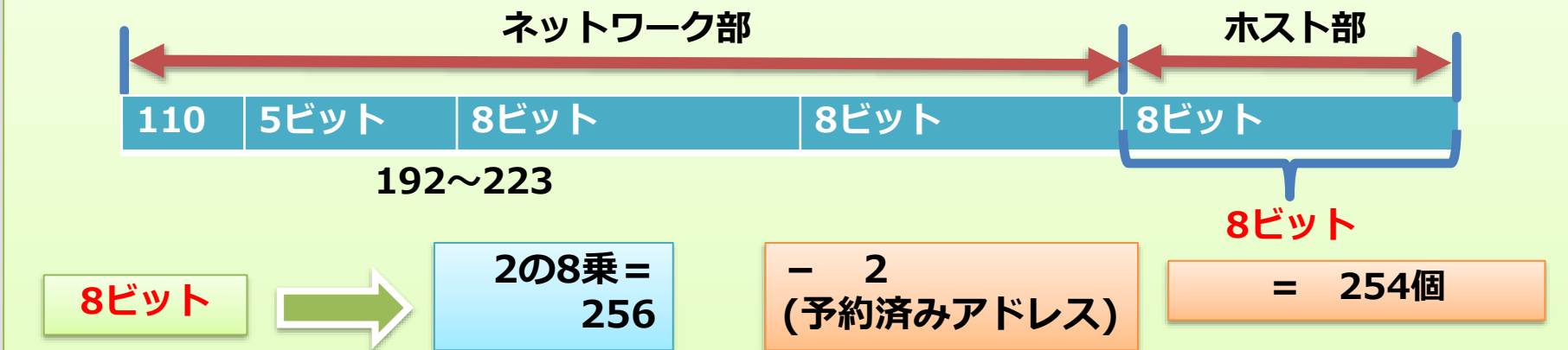
- IPアドレスでは、ネットワーク部の長さを明確にするため、サブネットマスクをIPアドレスと一緒にホストへ設定します。
- 各クラスのサブネットマスクは以下になります。IPアドレスのネットワーク部に対応するビットを全て 1、ホスト部に対応するビットを全て 0 にし、10進数へ変換したものがサブネットマスクです。



IPv4アドレスのホスト部

- 一つのネットワークアドレスで何台の端末（=ホスト）を管理できるかは、各クラスのホスト部のビット数をnとすると、2のn乗から、2を引いた値となります。
- ホスト部のビットを全て「0」にしたアドレスは「ネットワークアドレス」として宛先ネットワークを表すのに使用し、ホスト部のビットを全て「1」にしたアドレスは「ブロードキャストアドレス」として使用されます。

例：クラスCのホスト数



予約済みアドレスは？

・ネットワークアドレス

1 1 0 0 0 0 0 0

1 0 1 0 1 0 0 0

0 0 0 0 0 0 0 1

0 0 0 0 0 0 0 0

・ブロードキャストアドレス

1 1 0 0 0 0 0 0

1 0 1 0 1 0 0 0

0 0 0 0 0 0 0 1

1 1 1 1 1 1 1 1

ネットワーク部

ホスト部

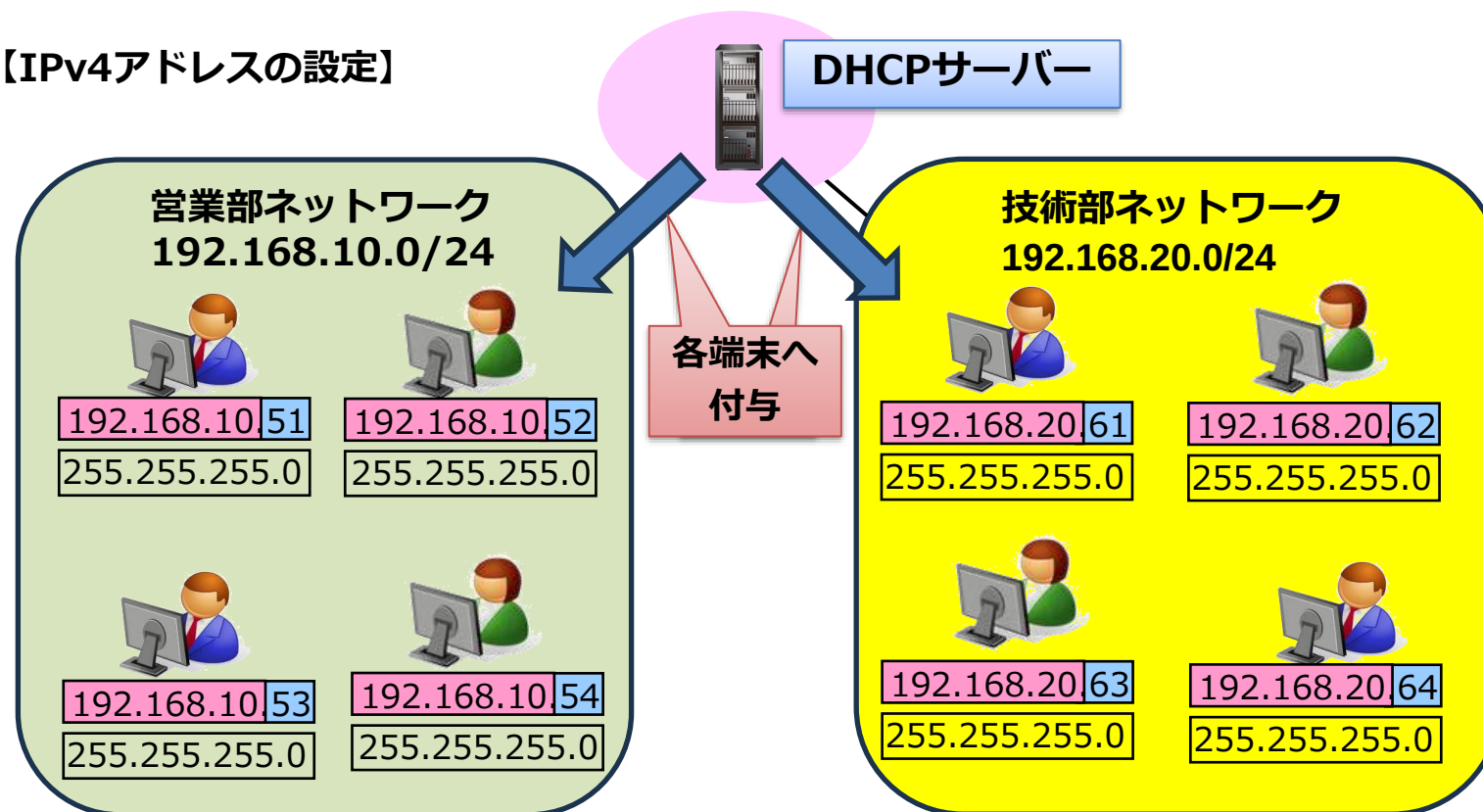
IPv4アドレスの設定

- IPv4アドレスをネットワーク上の機器に設定する場合、使用するネットワークアドレスの決定とともに、ホストアドレスの設計を行うことでネットワークが管理しやすくなります。例えば、クラスCのアドレスを使用する場合は、下表のようにどの機器にどのアドレスを割り当てるかを決定します。
- IPv4アドレスの割り当て方法には、ネットワーク管理者や端末利用者が各端末に個別に設定する方法と、DHCPサーバーから自動的にIPv4アドレスとサブネットマスクを付与する方法があります。

【ホストアドレス設計】
～クラスCの場合～

ホストアドレス	付与する機器
0	ネットワークアドレス
1～30	ネットワーク機器
31～50	サーバー/プリンタなどの共用機器
51～200	端末
201～254	予備
255	ブロードキャストアドレス

【IPv4アドレスの設定】



■ : ネットワークアドレス部 ■ : ホストアドレス部

クラスレスアドレッシング

- ネットワーク部とホスト部を決められたビット数で利用するアドレッシング（クラスフルアドレッシング）では、ネットワーク上のホスト数がIPアドレス数よりも少ない場合、多くのIPアドレスが活用されない問題が発生します。
- クラスレスアドレッシングは、ネットワーク部を1ビット単位で指定できるため、活用されないIPアドレスが減少しIPv4のアドレス空間を有効利用できるようになります。CIDR（Classless Inter-Domain Routing）とも呼びます。

（例）50台の端末が存在するネットワークへクラスCのIPv4アドレスを使用する場合

【クラスフルアドレッシング】

クラスCに収容できるホスト数は $2^8 - 2 = 256 - 2 = 254$ 台であり、このうち50のアドレスを使うと $254 - 50 = 204$ より、200強のアドレスが利用されないことになります。

【クラスレスアドレッシング】

一方、クラスレスアドレッシングでは50台のホストを識別するために必要なホスト部は、

$$2^5 - 2 = 30 < 50$$

$$2^6 - 2 = 62 > 50 \text{ より、6ビット必要と分かります。}$$

この場合、利用されないことになるIPアドレスは、 $62 - 50 = 12$ 個で済むことになります。

なお、ネットワーク部の長さは、IPアドレス32ビットからホスト部 6ビットを引いた26ビットになります。この26ビットが「サブネットマスク長」となります。

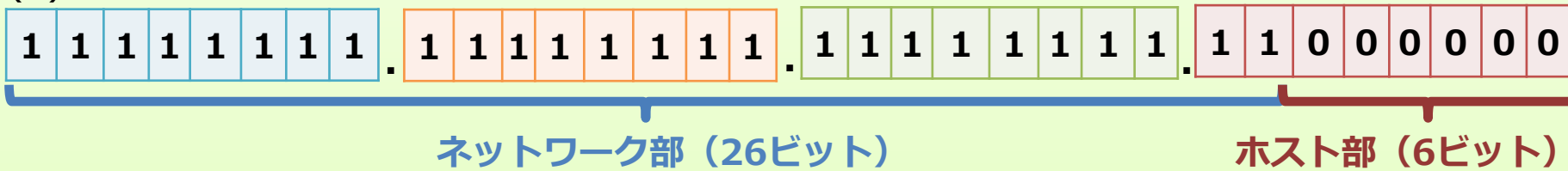
クラスレスアドレッシング

- 前頁で説明した26ビットのネットワーク部を使用した場合、以下の通りサブネットマスクは255.255.255.192 となります。
- ネットワーク部の長さを示す際には、サブネットマスク以外にプレフィックス表記（/26）が用いられます。

（例）192.168.10.0 のネットワークで、26ビットのネットワーク部を使用する場合

【サブネットマスク表記】

(1) ネットワーク部に1、ホスト部に0を並べた32ビットの2進数列を用意します。



(2) オクテットを10進数に変換すると、255.255.255.192 となります。

以上より

ネットワークアドレス ⇒ 192.168.10.0

サブネットマスク ⇒ 255.255.255.192

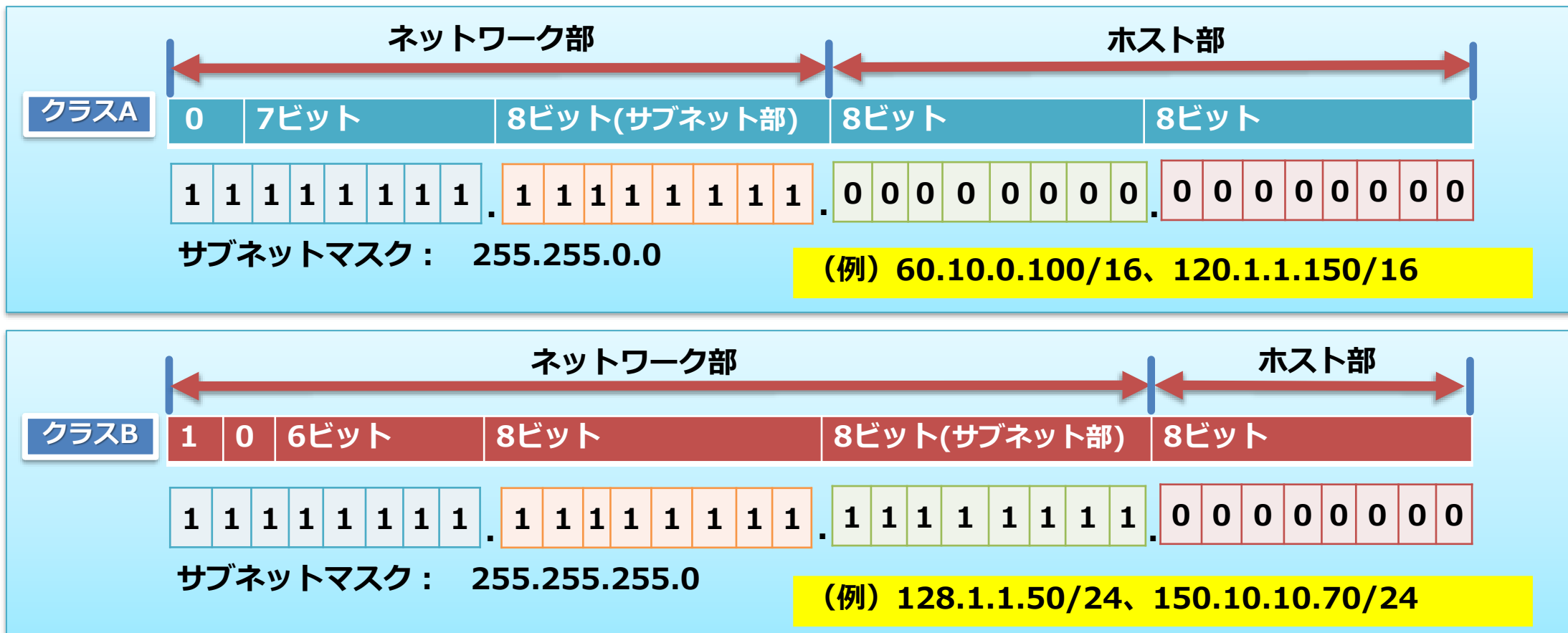
【プレフィックス表記】

ネットワークアドレスの後ろに、/(スラッシュ)を入れてネットワーク部の長さを記述します。

192.168.10.0 / 26

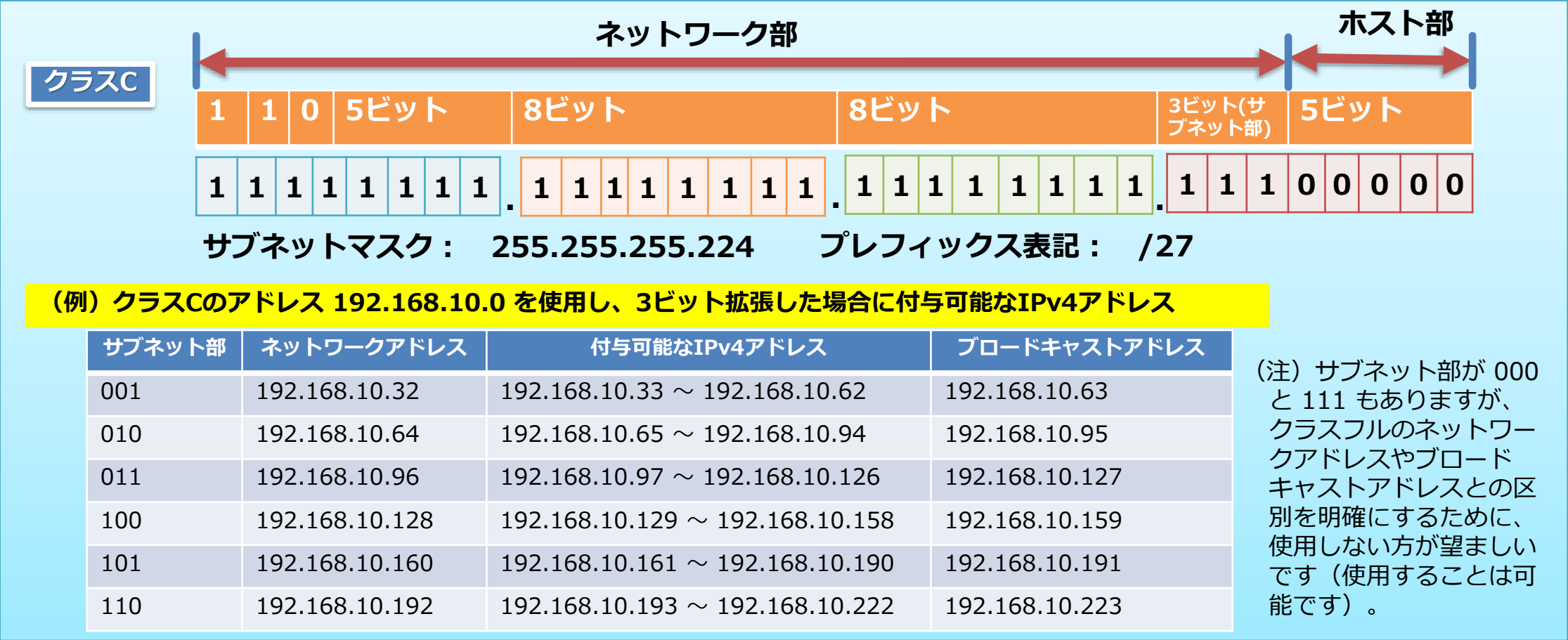
クラスAとBのクラスレスアドレスリング

- クラスAとBのIPv4アドレスを使用した場合、バイト単位でネットワーク部を拡張できます（ビット単位での拡張も可能です）。クラスAのネットワーク部を16ビット、クラスBは24ビットにすることで、一つのアドレスを使用して複数のネットワークにアドレスを設定することが可能となります。
- ネットワーク部を拡張することをサブネット化と言い、拡張したネットワーク部はサブネットワーク部やサブネット部と言います。



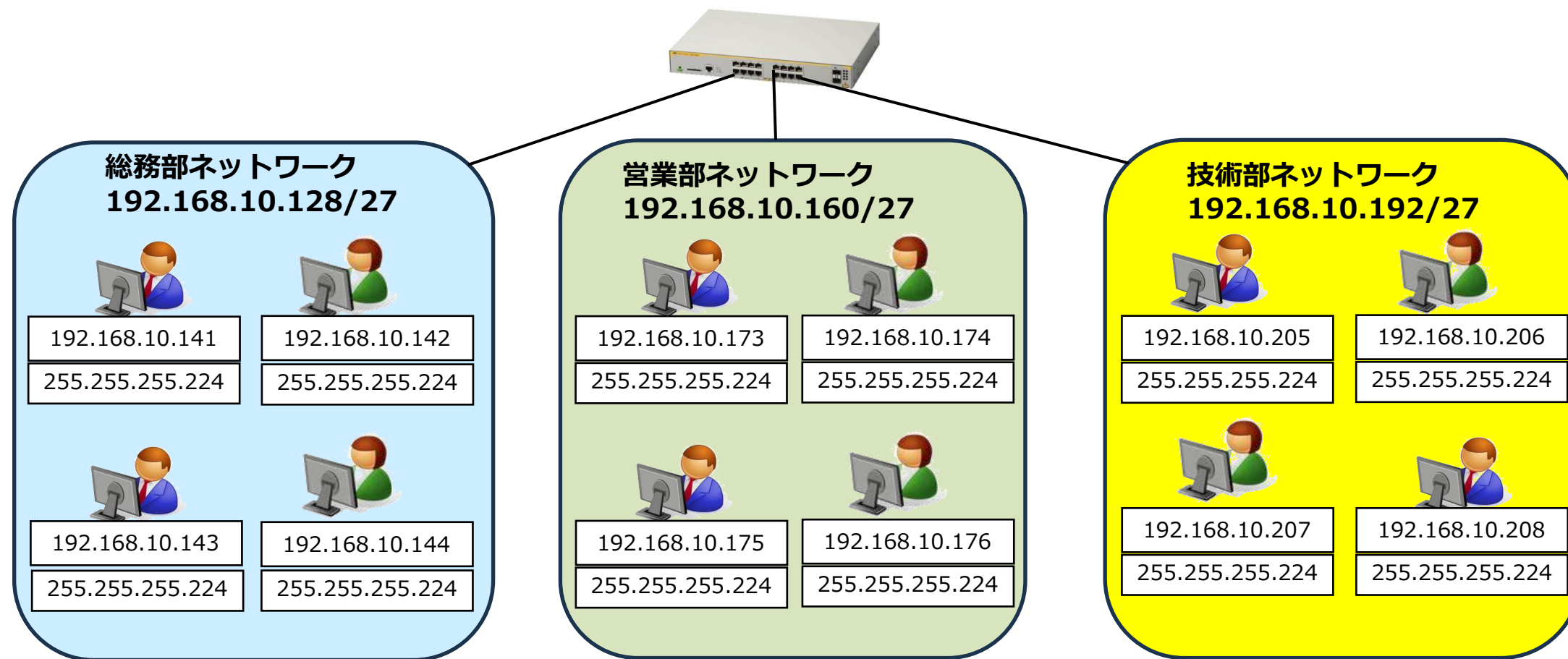
クラスCのクラスレスアドレスリング

- クラスCのIPv4アドレスを使用した場合は、ビット単位でのネットワーク部の拡張になります。一つのクラスCアドレスで管理したいネットワーク数と、一つのネットワークに存在するホスト数を考慮して拡張するビット数を決定します。
- ネットワーク部を拡張した場合でも、ホスト部のビットが全て0はネットワークアドレス、ビットが全て1はブロードキャストアドレスとして使用しますので、ホストに付与することはできません。



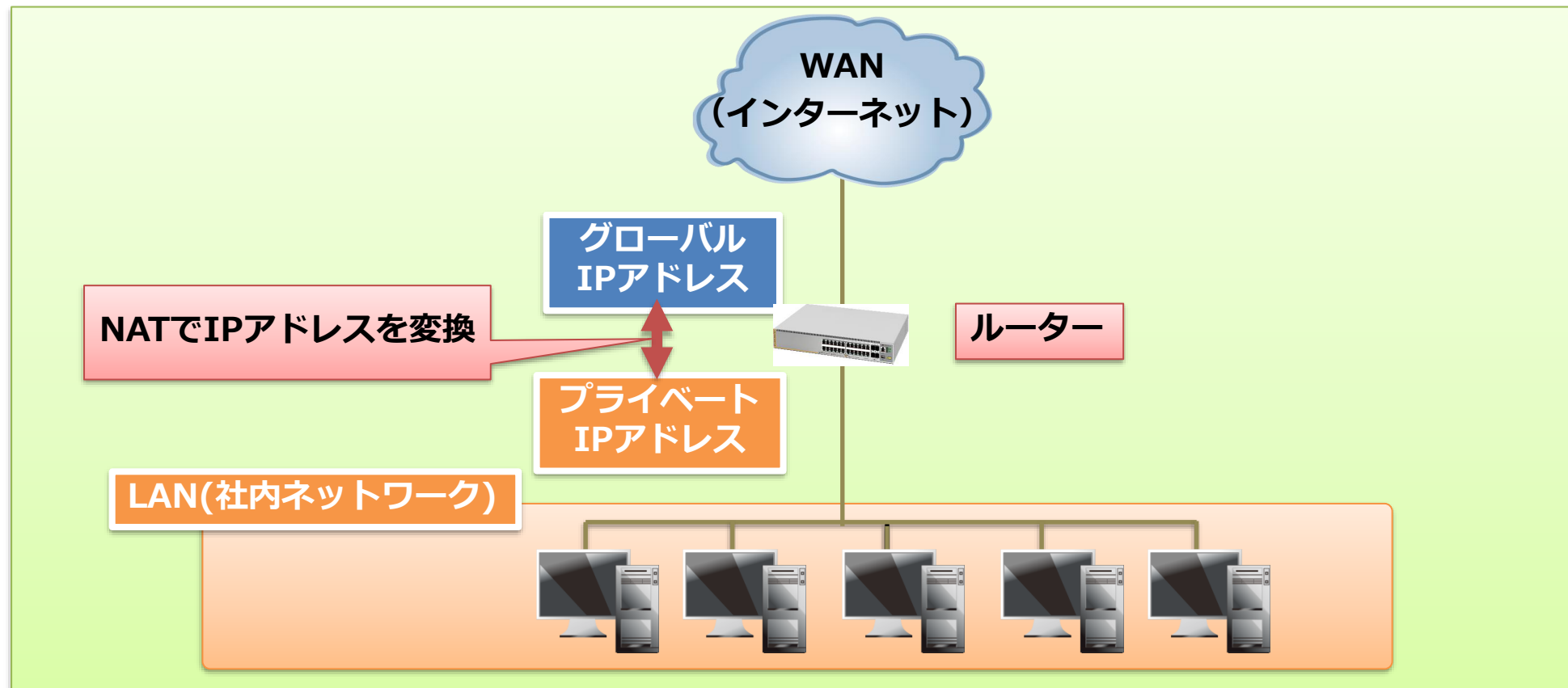
IPv4アドレスの設定（クラスレスアドレッシング）

- 下図は、クラスレスアドレッシングを使用したIPv4アドレスの設定例です。
- クラスレスアドレッシングにおいても、ネットワーク機器やサーバーなどの共用機器に付与するアドレスを考慮してPCに付与するアドレスを決定する必要があります。



プライベートIPアドレスとグローバルIPアドレス

- プライベートIPアドレスは、LAN内部だけで管理・使用されるアドレスです。WANとの通信では、グローバルIPアドレスと呼ばれるキャリアから付与されるアドレスを使用する必要があります。
- プライベートIPとグローバルIPの変換は、ルーターなどの機器が持つNAT（Network Address Translation）機能で行います。



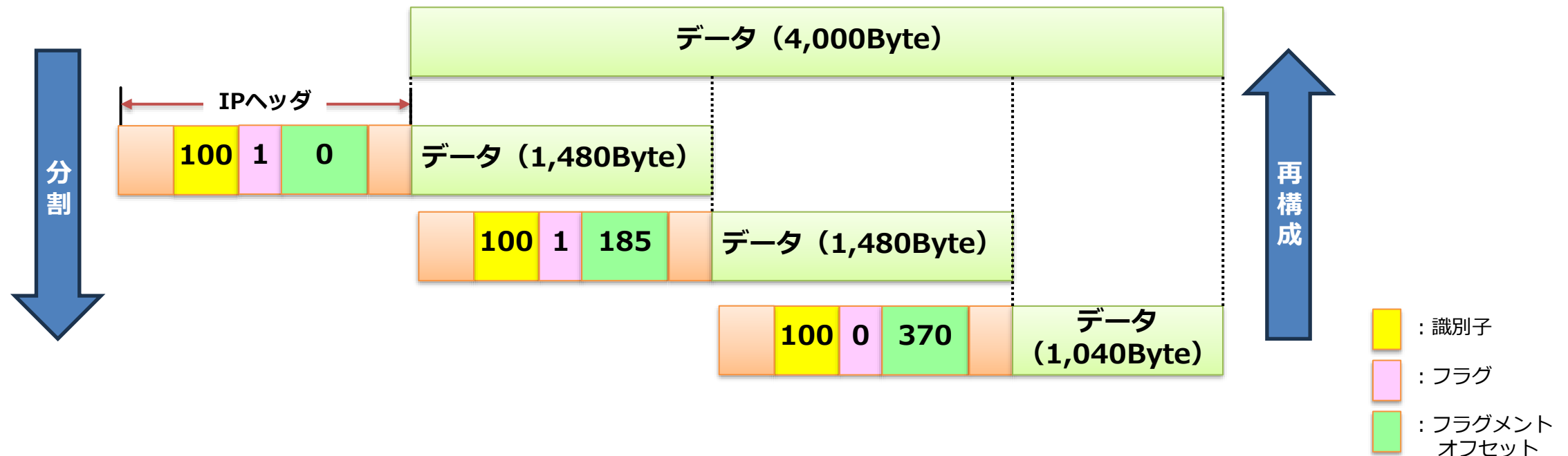
IPv4ヘッダ

- IPv4ヘッダの標準ヘッダ長は20バイトです。主なパラメーターを以下で説明します。
 - ①バージョン：IPのバージョン ②ヘッダ長：IPヘッダの長さで4バイトを1で表し標準では5
 - ③サービスタイプ：IPのサービス品質 ④パケット長：IPヘッダを含むパケット全体のバイト長
 - ⑤識別子、⑥フラグ、⑦フラグメントオフセット：経路上の機器でパケットが分割された時に使用
 - ⑧生存時間：経由できるルーティング機器の数を表します。
 ルーティング機器を経由するごとにこの値から1が引かれ、0になった時点でそのパケットは破棄されます。
 - ⑨プロトコル：上位層プロトコルを示すプロトコル番号、例えば、TCPは6、UDPは17
 - ⑩チェックサム：ヘッダの誤り検出に使用。データ部の誤り検出は上位層のプロトコルで行う。
 - ⑪送信元IPアドレス、⑫宛先IPアドレスはそれぞれ送信元、宛先ホストのIPアドレスが格納されます。

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
①バージョン (Version)				②ヘッダ長 IHL				③サービスタイプ (Type Of Service)								④パケット長 (Total Length)															
⑤識別子 (Identification)															⑥フラグ (Flags)				⑦フラグメントオフセット (Fragment Offset)												
⑧生存時間 (Time To Live)								⑨プロトコル (Protocol)								⑩チェックサム (Checksum)															
⑪送信元IPアドレス (Source IP)																															
⑫宛先IPアドレス (Destination IP)																															
⑬オプション(Options)																								⑭パディング(Padding)							

IPパケットの分割と再構成

- パケット送信元のIPがMTUサイズを超えるデータを上位プロトコルから受け取った場合、MTUサイズ内に収まるようにパケットを分割します。
- パケットを分割した場合、宛先のIPがデータの再構成を行えるようIPv4ヘッダの以下のフィールドに再構成に必要な情報をセットします。
 - **識別子**：パケットの識別に使用。通常はパケット毎に異なる番号になるが、分割時は同じ番号をセットします。
 - **フラグ**：この中のMF（More Fragment）ビットが0ならば最後のデータが入ったパケットを意味し、1ならば途中のデータであることを意味します。
 - **フラグメントオフセット**：パケットが、分割前のパケットのどの位置にあったかを表します。8Byteのデータがオフセット値1になる（2,000Byteであれば250）ため、データは8Byte単位で分割されます。





③IPv6アドレス

アプリケーション層

トランスポート層

インターネット層

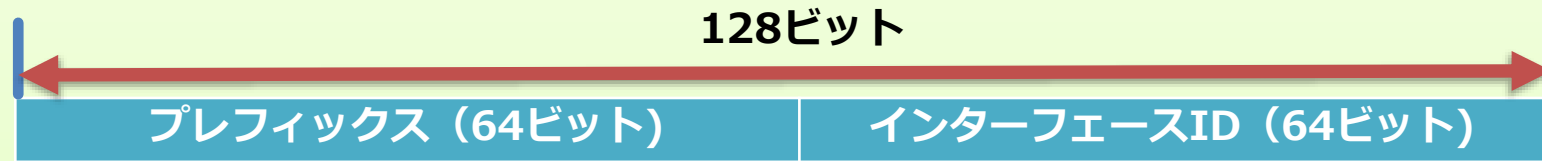
ネットワーク
インターフェイス層

IPv6アドレスの構造と種類

- IPv6はIPv4の後継プロトコルで、128ビットに拡大されたアドレス空間を持ちます。
- IPv6アドレスは機器のネットワークインターフェースに付与します。複数のIPv6アドレスを1つのインターフェースへ、1つのIPv6アドレスを複数のインターフェースへ付与することもあります。

IPv6のアドレス構造

マルチキャストアドレスや特殊なアドレスを除き、IPv6アドレスは一般的に前半64bitの「プレフィックス」と後半64bitの「インターフェースID」に分かれます。



IPv6アドレスの種類

- **ユニキャストアドレス** : 1つのインターフェースの識別番号、1対1の通信で使します。
- **マルチキャストアドレス** : 1対多通信で使用するアドレス、マルチキャストアドレス宛のパケットはそのアドレスを持つ全てのインターフェース（機器）に送られます。
- **エニーキャストアドレス** : マルチキャストと同様に複数のインターフェースに割り当てられますが、エニーキャストアドレス宛のパケットは最も近いインターフェース（機器）にのみ送られます。

なお、IPv4アドレスとは異なりIPv6アドレスにはブロードキャストアドレスは存在しません。この役割はマルチキャストアドレスが行います。

IPv6アドレスの表記規則

- IPv6は128ビットという長いアドレスを使用するため、その表記は短くなるよう工夫されています。具体的には16進数での表記や、連続する0の省略になります。

IPv6アドレスの表記規則

- ① 16進数で表し、16ビットごとにコロン (:) で 8つに区切ります。
※16ビットのひと区切りをフィールドと言います。
- ② 16進数の a ~ f は小文字を使用します。
- ③ 連続する0は省略し、:: と表記する。ただし、全ての0のフィールドが一つだけの場合、:: を使用して省略はできません。
- ④ 0の連続する箇所が2箇所以上ある場合は以下になります。
 - (a) 長い方を省略します。
 - (b) 長さが同じ場合、先に現れる方を省略します。
- ⑤ 各フィールドの先頭の0は省略します。

アドレス表記例

- (1) fe80:0:0:0:0a00:46ff:fe60:ee2b ⇒ fe80::a00:46ff:fe60:ee2b と表記
※ 表記規則の②、③、⑤を適用しています。
- (2) fe80:0:0:8a00:46ff:0:0:ee2b ⇒ fe80::8a00:46ff:0:0:ee2b と表記
※ 表記規則の②、④(b)を適用しています。

IPv6ユニキャストアドレスの種類

- 通信で使用するIPv6ユニキャストアドレスには以下の種類があります。

グローバルユニキャストアドレス (プレフィックス 2000::/3)

インターネット内で一意なアドレスで通常の通信に使用。IPv4のグローバルIPアドレスに相当します。

グローバルルーティング プレフィックス		サブネットID (61-n)	インターフェースID (64)
001	(n)		

()内はビット数

リンクローカルユニキャストアドレス (プレフィックス fe80::/10)

各ネットワークインターフェース毎に自動設定される同一セグメント内でのみ有効なアドレスです。
ルーターと通信してアドレス設定や近隣探索 (IPv4のARPに相当) に使用します。

1111 1110 10 fe80(10)	0000...0000 (54)	インターフェースID (64)
--------------------------	---------------------	--------------------

()内はビット数

ユニークローカルIPv6ユニキャストアドレス (プレフィックス fc00::/7、通常はfd00::/8)

ローカルで使用するアドレスで、IPv4のプライベートアドレスに相当。アドレスの一部を乱数で生成するため完全な一意性は保証しないが、異なるセグメント間でアドレス重複の可能性を低減します。

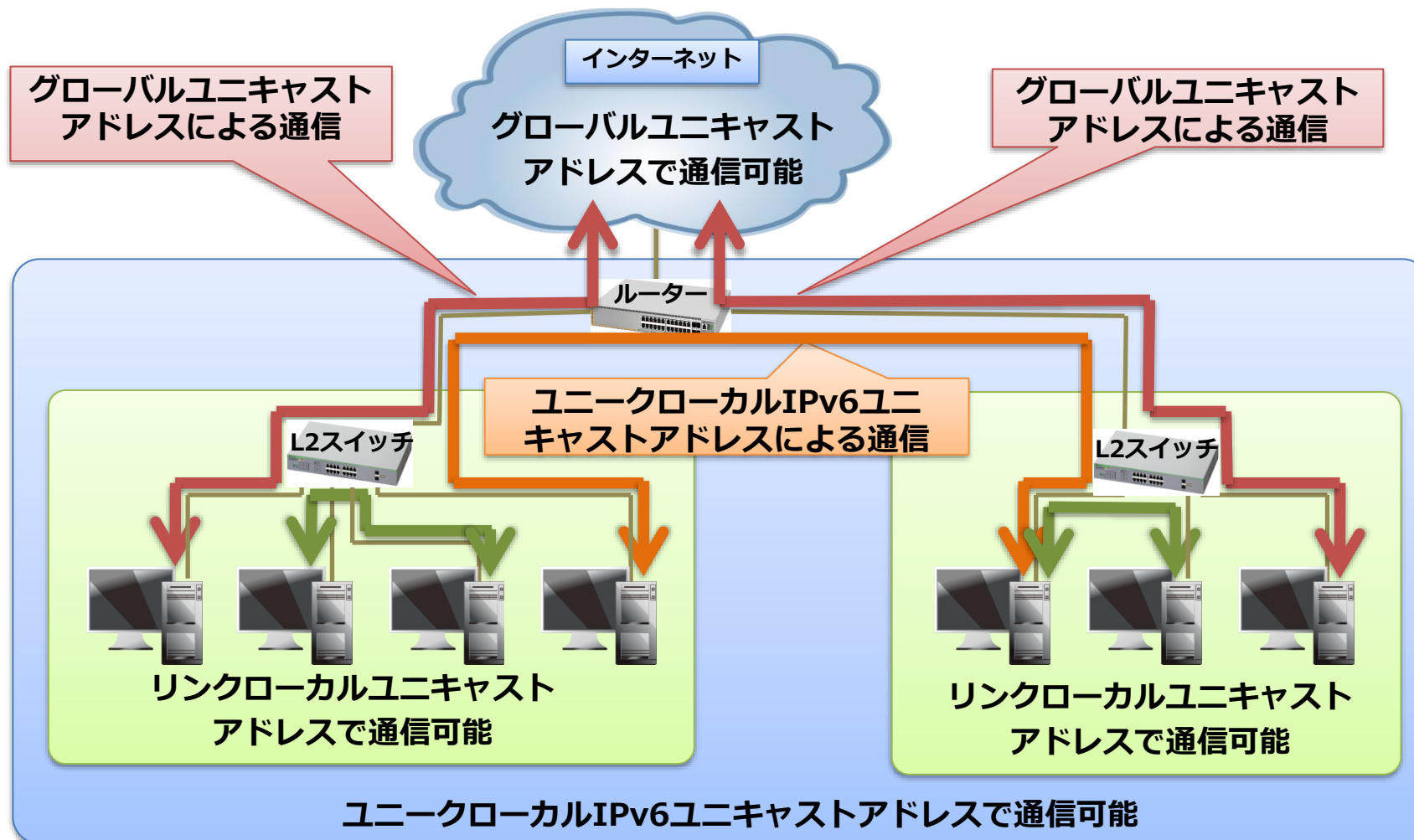
1111 110 fc00(7)	L (1)	グローバルID (40)	サブネットID (16)	インターフェースID (64)
---------------------	----------	-----------------	-----------------	--------------------

()内はビット数

↑ Lは0か1になるが、0は使用不可のため通常は1が入ります。

IPv6ユニキャストアドレスの通信

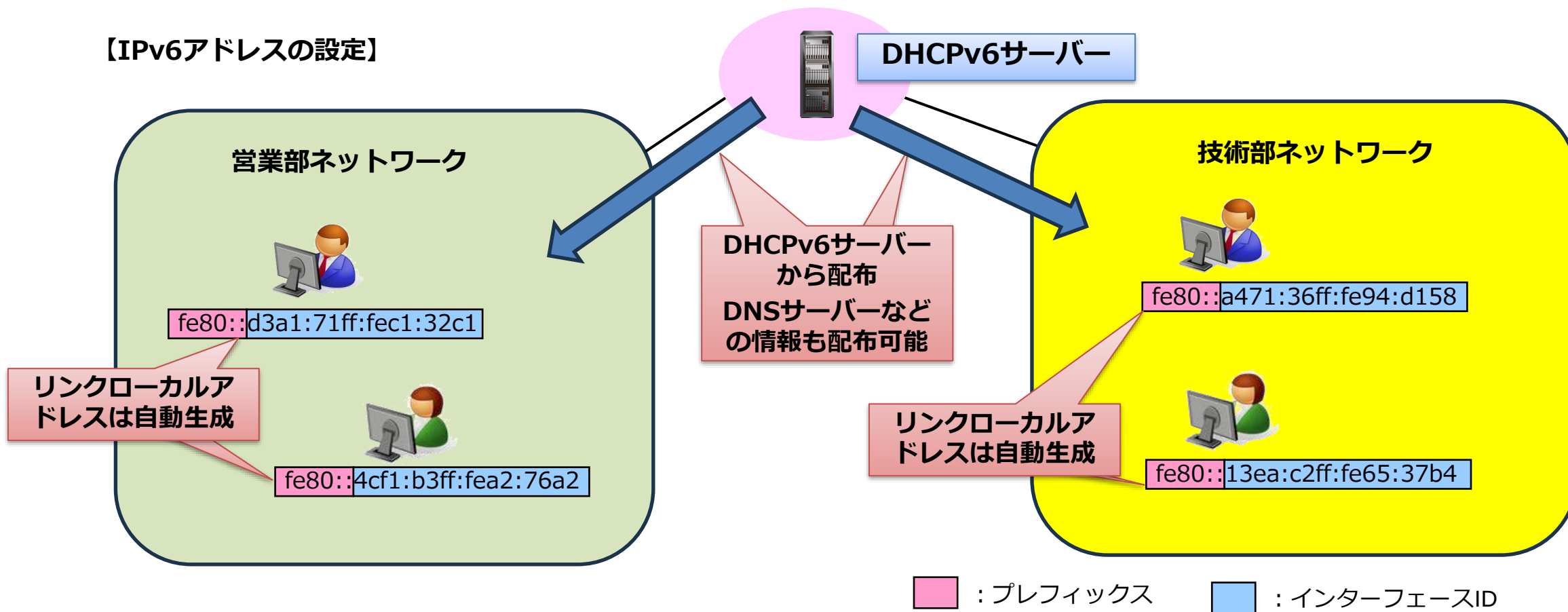
- ユニキャストアドレスがどの通信で 사용되는かは以下になります。
- 現在インターネットサービスプロバイダがIPv6に対応した通信サービスを提供し、PC側も標準でIPv6をサポートしています。



IPv6アドレスの設定

- IPv6アドレスの設定には、DHCPv6サーバーから取得、ルーティング機器から取得、インターフェースのMACアドレスから自動的に生成、手動で設定などの方法があります。
- IPv6のホストは、リンクローカルアドレスを自動的に生成します。インターフェースIDはインターフェースのMACアドレスに16ビットの値を付加して自動的に生成します。これをステートレスアドレス自動設定と言います。

【IPv6アドレスの設定】



IPv6ヘッダ

- IPv6では基本ヘッダと拡張ヘッダに分けており、基本ヘッダは40バイトの固定長になります。主なパラメーターは以下に記載します。
 - ①バージョン：IPのバージョン6で6 ②トラフィッククラス：IPv4のTOSに当たり優先制御の情報
 - ③フローラベル：品質制御（QoS）のフィールド
 - ④ペイロード長：ペイロードと呼ばれるパケットのデータ部の長さ。ペイロード長は拡張ヘッダとデータの合計で、基本ヘッダの40バイトは含まない
 - ⑤ネクストヘッダ：基本ヘッダに続く拡張ヘッダや上位プロトコルのタイプ
 - ⑥ホップリミット：IPv4のTTLにあたるフィールドで、経由できるルーティング機器の最大数
 - ⑦送信元IPアドレス、⑧宛先IPアドレス：各128ビットの長さ

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
①バージョン (Version)				②トラフィッククラス (Traffic Class)								③フローラベル (Flow Label)																			
④ペイロード長 (Payload Length)																⑤ネクストヘッダ (Next Header)								⑥ホップリミット (Hop Limit)							
⑦送信元IPアドレス(Source Address)																															
⑧宛先IPアドレス(Destination Address)																															



④ ARPとICMP

アプリケーション層

トランスポート層

インターネット層

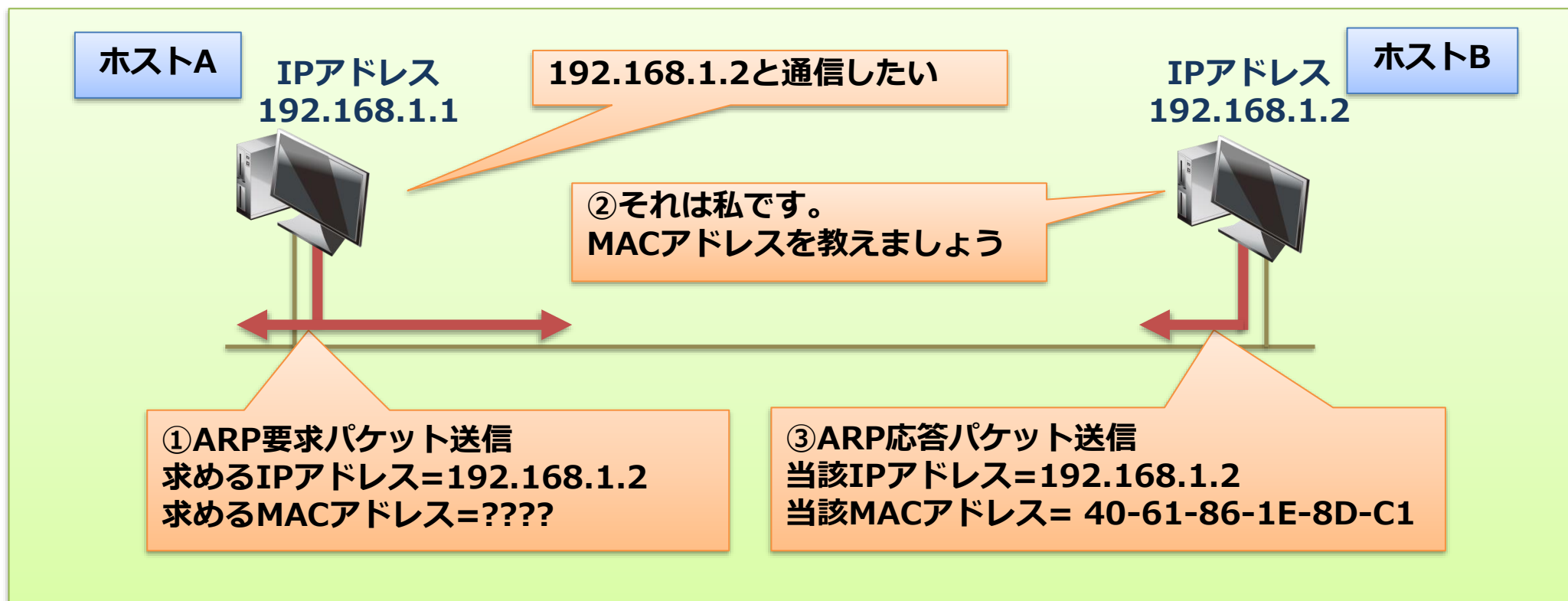
ネットワーク
インターフェイス層

ARP(Address Resolution Protocol)

- ARPは、宛先IPアドレスから宛先MACアドレスを知るためのIPv4限定のプロトコルです。
- ARPは以下の順序で動作します。

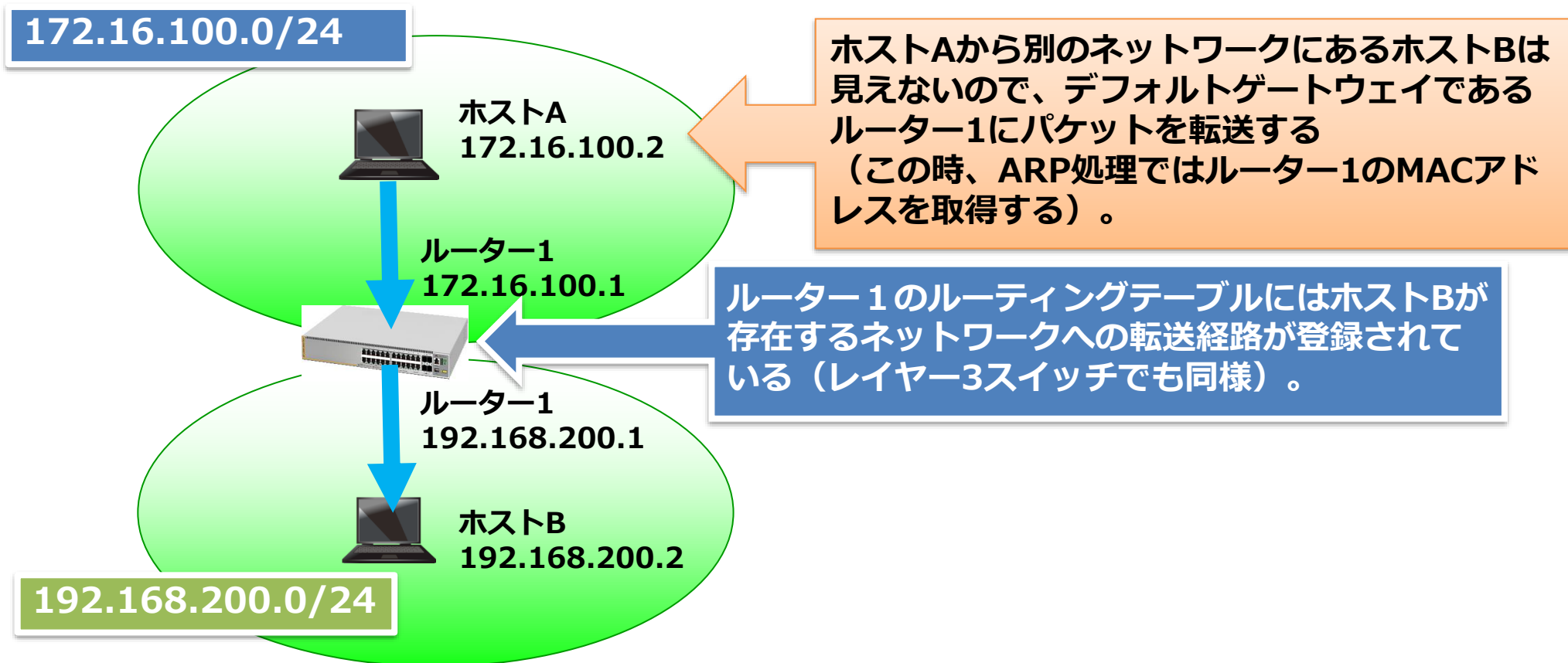
- ①MACアドレスを知りたい宛先IPアドレスをセットし、ARP要求をブロードキャストで送出します。
- ②該当する端末のみが、このブロードキャスト通信に反応します。
- ③該当する端末は、自分のMACアドレスを含めた応答を返します。

※ 入手したMACアドレスは、各ホストのARPテーブルに一定時間保存され、同一ホストとの通信ではARPテーブルの情報を使用します。



デフォルトゲートウェイ

- 自ネットワーク内（これをセグメントといいます）の送信であればルーターなどのルーティング機器は必要ありませんが、異なるネットワークアドレスを持つネットワークへのパケットは必ずルーティング機器を経由して転送されます。
- そのため、各ホストにはルーティング機器のアドレスをデフォルトゲートウェイとして設定します。各ホストはARPでデフォルトゲートウェイのMACアドレスを取得します。



ICMP(Internet Control Message Protocol)

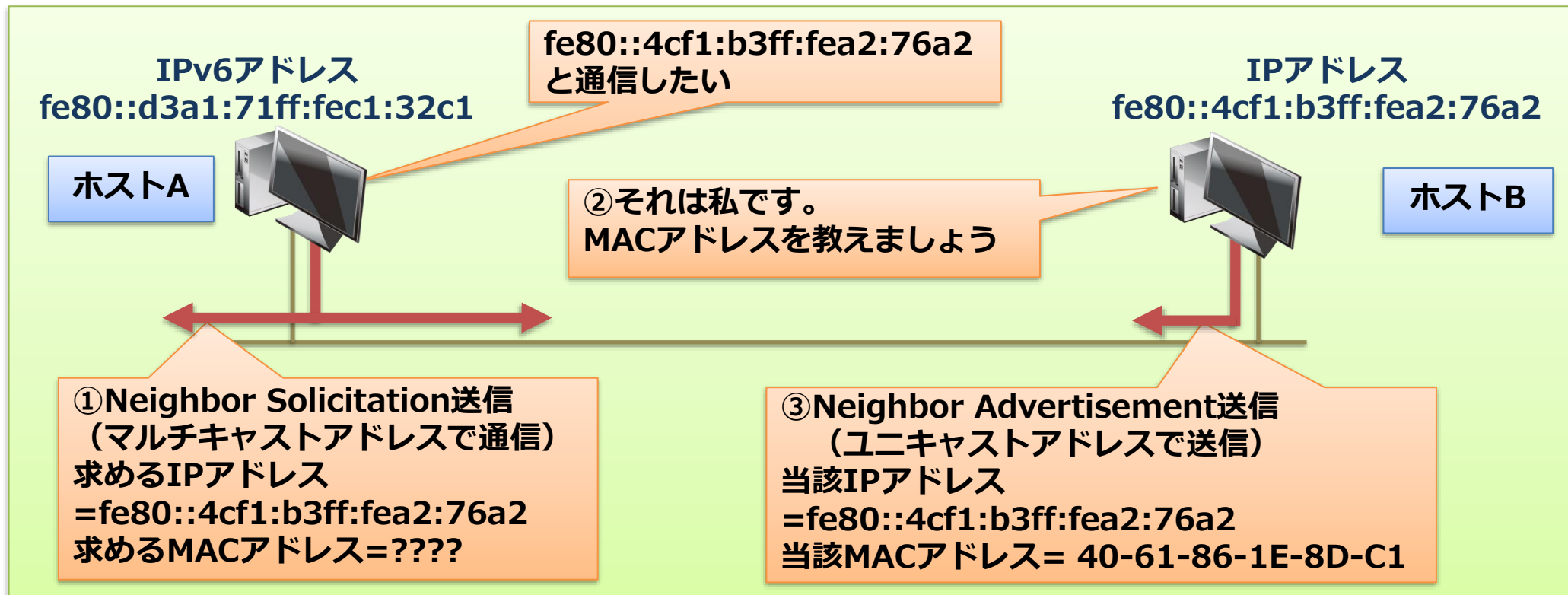
- ICMPは、IPプロトコルのエラー通知や制御メッセージを転送するプロトコルです。
- ICMPメッセージには大きく2種類あります。
 - ① 問い合わせ(Query)： pingやtracerouteというコマンドで、特定のノード※に対する通信状態を確認します。
 - ② エラー通知(Error)： 通信経路の途中でパケットが廃棄された場合に、その原因を送信元ノードに通知します。
- ICMPにはICMPv4とICMPv6があり、ICMPv6にはARPと同様の宛先MACアドレスを取得するメッセージがあります。



※ ノード：ネットワーク上の機器のことで、ホストと同じ意味です。

ICMPv6による宛先MACアドレスの取得

- IPv6アドレスのネットワークでは、宛先MACアドレスの取得にICMPv6のNeighborメッセージを使用します。Neighborメッセージには以下の2つがあります。
 - Neighbor Solicitation（近隣要請）<タイプ135>：宛先MACアドレス情報の要求
 - Neighbor Advertisement（近隣広告）<タイプ136>：Neighbor Solicitationメッセージへの応答
- Neighborメッセージは、IPv6ホストがステータスアドレス自動設定でIPv6アドレスを自動生成した場合、他のIPv6ホストとアドレスが重複していないかを検出する場合にも使用します。



ICMPメッセージの役割と主なICMPv4メッセージ

- ICMPメッセージには以下の役割があります。
 - 「①宛先IPアドレスへの通信の可否を確認」「②Pingパケットによる宛先ホストの稼働の有無と応答速度を確認」「③TTLパラメータによる時間超過を確認」「④機器間の通信速度の違いを調整するフロー制御」「⑤アドレスマスク要求・応答によりサブネットマスク情報を取得」「⑥URLなどへのリクエストを転送するRedirect機能、送信ホストへの送信経路の変更も指示」
- 主なICMPv4メッセージは以下になります。

タイプ	メッセージ	通知内容
0	Echo Reply Message	エコー(Ping)応答通知
3	Destination Unreachable Message	宛先到達不可能通知
4	Source Quench Message	送出抑制要求通知
5	Redirect Message	経路変更要求通知
8	Echo Message	エコー(Ping)要求通知
9	Router Advertisement Message	ルーター広告通知
11	Time Exceeded Message	時間切れ通知
12	Parameter Problem Message	不正引数通知
17	Address Mask Request Message	アドレスマスク要求通知
18	Address Mask Reply Message	アドレスマスク応答通知

ICMPv6メッセージ

- ICMPv4とICMPv6はプロトコル番号が異なる別のプロトコルで、ICMPv4のプロトコル番号は 1でICMPv6のプロトコル番号は58です。
- ICMPv6メッセージには、IPv6アドレス解決機能やマルチキャスト機能などの特有のメッセージがあり、同じ通知内容のメッセージでもICMPv4とICMPv6ではタイプ番号が異なります。
- 主なICMPv6メッセージは以下になります。

タイプ	メッセージ	通知内容
1	Destination Unreachable Message	宛先到達不可能通知
3	Time Exceeded Message	時間切れ通知
4	Parameter Problem Message	不正引数通知
128	Echo Message	エコー(Ping)要求通知
129	Echo Reply Message	エコー(Ping)応答通知
130	Multicast Listener Query	マルチキャストグループの確認
133	Router Solicitation Message	ルーター要請通知
135	Neighbor Solicitation Message	近隣要請通知
136	Neighbor Advertisement Message	近隣広告通知
137	Redirect Message	経路変更要求通知



Appendix : 各種販促情報のご案内など



各種販促情報のご案内

新製品のご紹介(Wi-Fi6対応無線LANルーター)

- Wi-Fi6とVPNルーターの機能を1台で提供
- エンタープライズ向け機能を搭載
 - FirewallやダイナミックENAT、IPsec、VAP、Captive Portal、WPA3など各種エンタープライズ向け機能を搭載
- AMF Plusによる一元管理に対応
- 様々なネットワークに適用可能
 - 無線LANルータとして、小規模店舗/ブランチオフィスや多店舗展開ネットワーク、通常の無線LAN APとして、企業内LANなど様々なネットワークをAT-TQ6702 GEN2-Rで構成可能



AT-TQ6702 GEN2-R



Allied Labのご紹介



Allied Lab

で検索！

アライドテレシスの技術を製品担当が分かりやすく紹介。



...第十四回目：次世代高速通信を実現！
「マルチギガビットイーサネットの実力とは！」

...第十三回目：これ一台で構築できる！
「高セキュリティのWi-Fi・VPN環境をまるっと低コストで実現！」

...第十二回目：ネットワーク統合管理
「ネットワーク管理の手間をごそっと削減！」

...他、多数！

新製品のご紹介（エッジスイッチシリーズ）

mGig L2 SW

x240シリーズ

AMF Plus	50°C	PoE ++
8	16	24 48
8	16	24 48



All 10G L2 SW

x250シリーズ

VCS	AMF Plus	50°C	PoE ++
8	16	24	48
		24	48
	16	24	48



Copper Model Lineup

PoE Model Lineup

Fiber Model Lineup

All 10G L3 SW

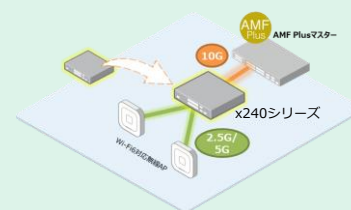
x540Lシリーズ

VCS	AMF Plus	50°C	PoE ++
24	48		
24	48		
24			

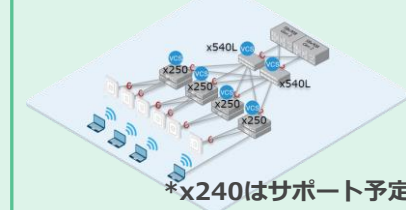


特長

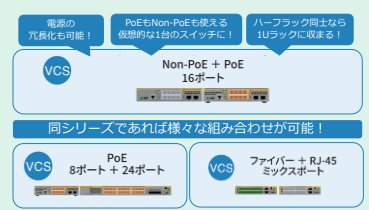
Cat5e対応 mGig サポート
～配線の入替えなしで高速通信～



スタックサポート
～ネットワークのエッジにまで冗長性を～



環境に応じた拡張性
～組み合わせ自由なスタック構成～



ビデオデータシートのご紹介



各種製品名

で検索！

製品の特長やユースケースなどを動画でご紹介します。



...PoE++対応マルチギガビットスイッチ
x530L GHXm シリーズ紹介

...マルチギガビット・インテリジェント・スイッチ
x240シリーズ 紹介

...マルチギガビット対応PoE++インジェクター
AT-7101GHTm紹介

...他、多数！



ご清聴ありがとうございました。



今回ご紹介しましたネットワーク製品に関して、
別途個別に相談がございましたら、お気軽に弊社
営業までお問い合わせください。