TCP/IPセミナー

オンラインセミナー
ウェビナー

Allied Telesis

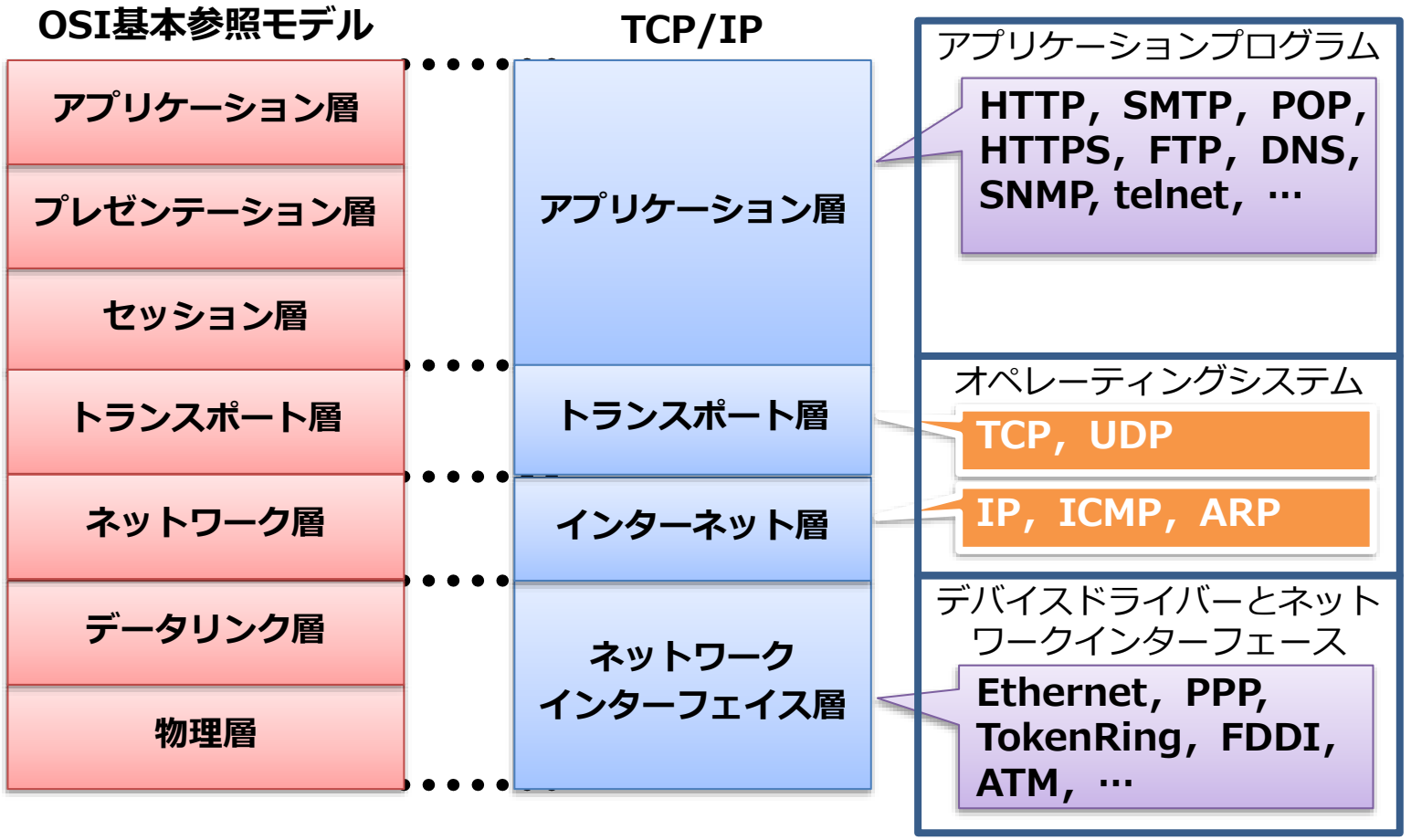
V1.1

目次

①TCP/IPの概要

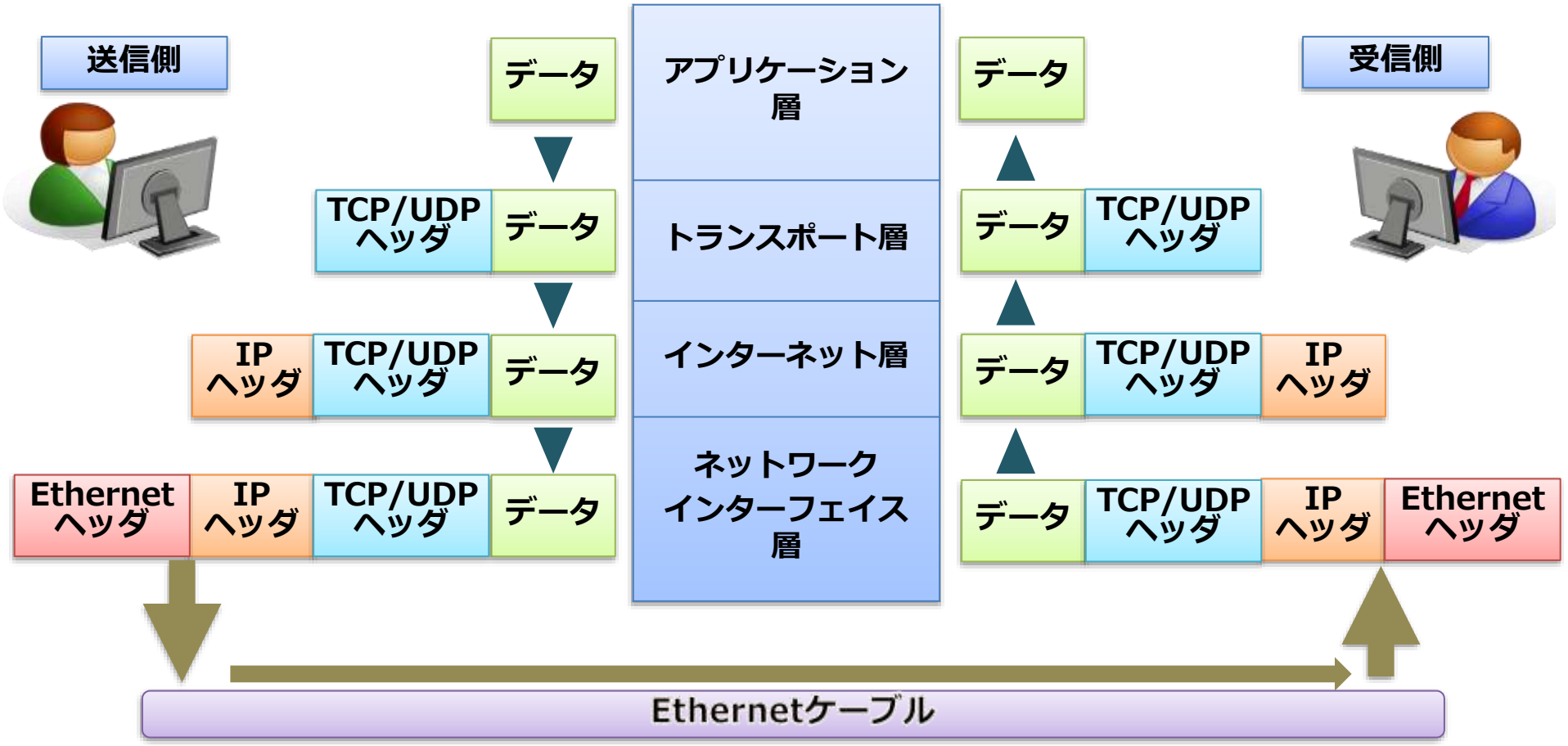
TCP/IPのプロトコル

- 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

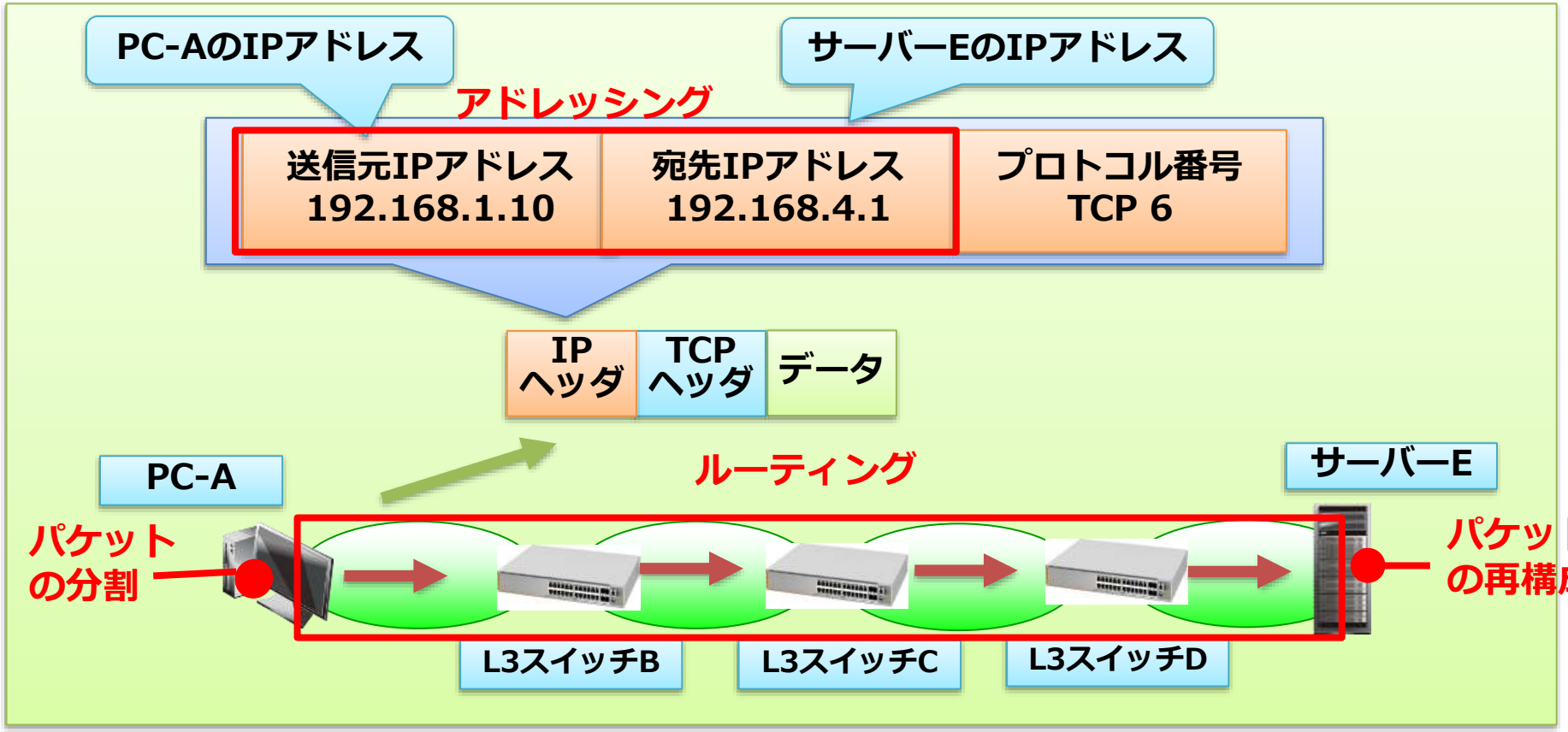
- アプリケーション層で作成されたデータの前には、各階層で動作するプロトコルによりヘッダが付けられます。
- IPヘッダが付いたデータをパケット、Ethernetヘッダが付いたデータをフレームと呼びます。最大パケット長(MTU: Maximum Transfer Unit)は 1,500Byte、最大フレーム長は 1,518Byteになります。



②IP(Internet Protocol)

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

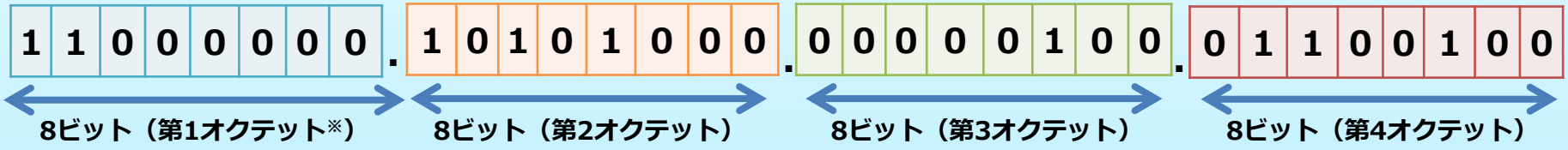


IPv4アドレス

- 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

32ビット

【2進数の表記】



【10進数への変換方法】

2進数8ビットの位は上から順に、128 64 32 16 8 4 2 1 となる
位取りの位置が1であれば（ビットが立っていれば）、位の数を合計することで10進数に変換できる

[例：第1オクテット]

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

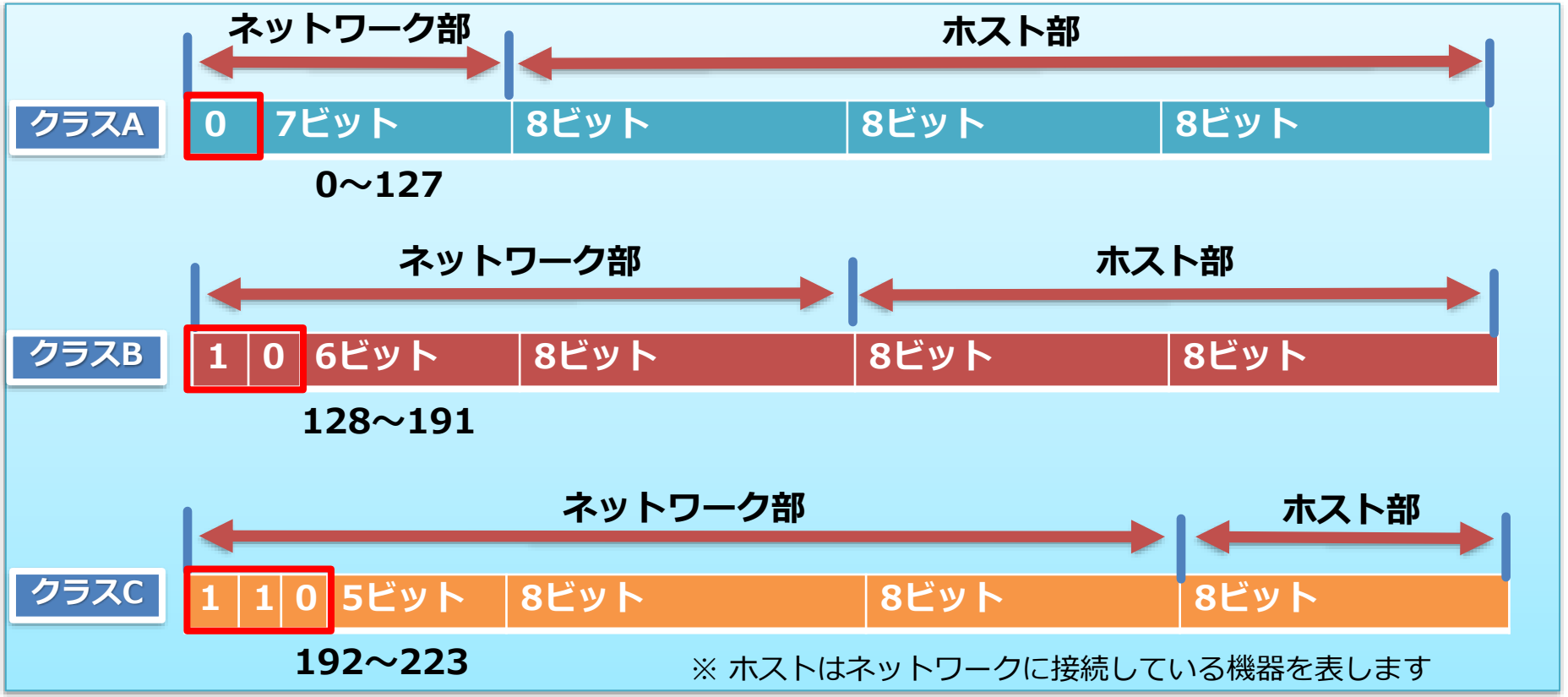
⇒ 128 + 64 = 192

同様の手順で、全てを10進数に変換すると、上記のIPv4アドレスは **192.168.4.100** となる

※ オクテット（octet）は 8ビットを表す情報量の単位です

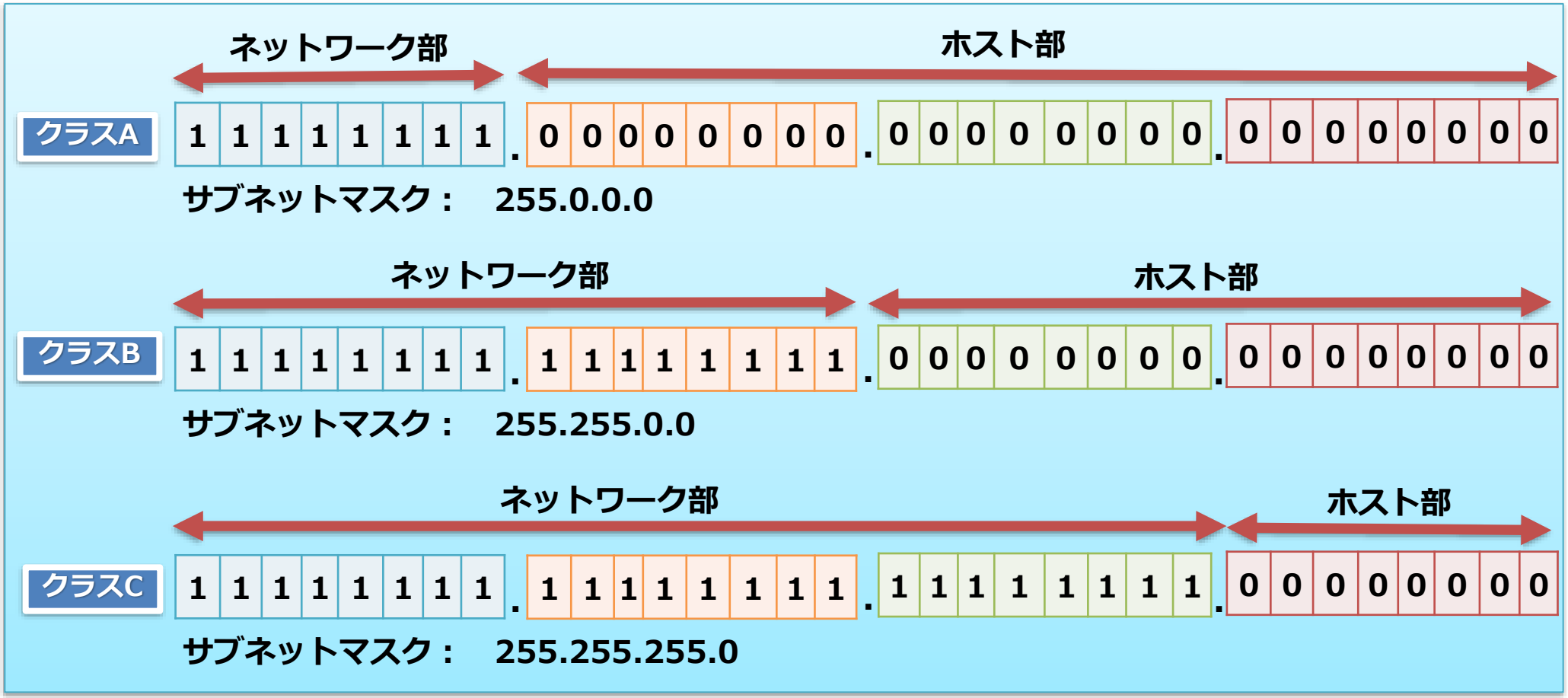
IPv4アドレスのクラス

- 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



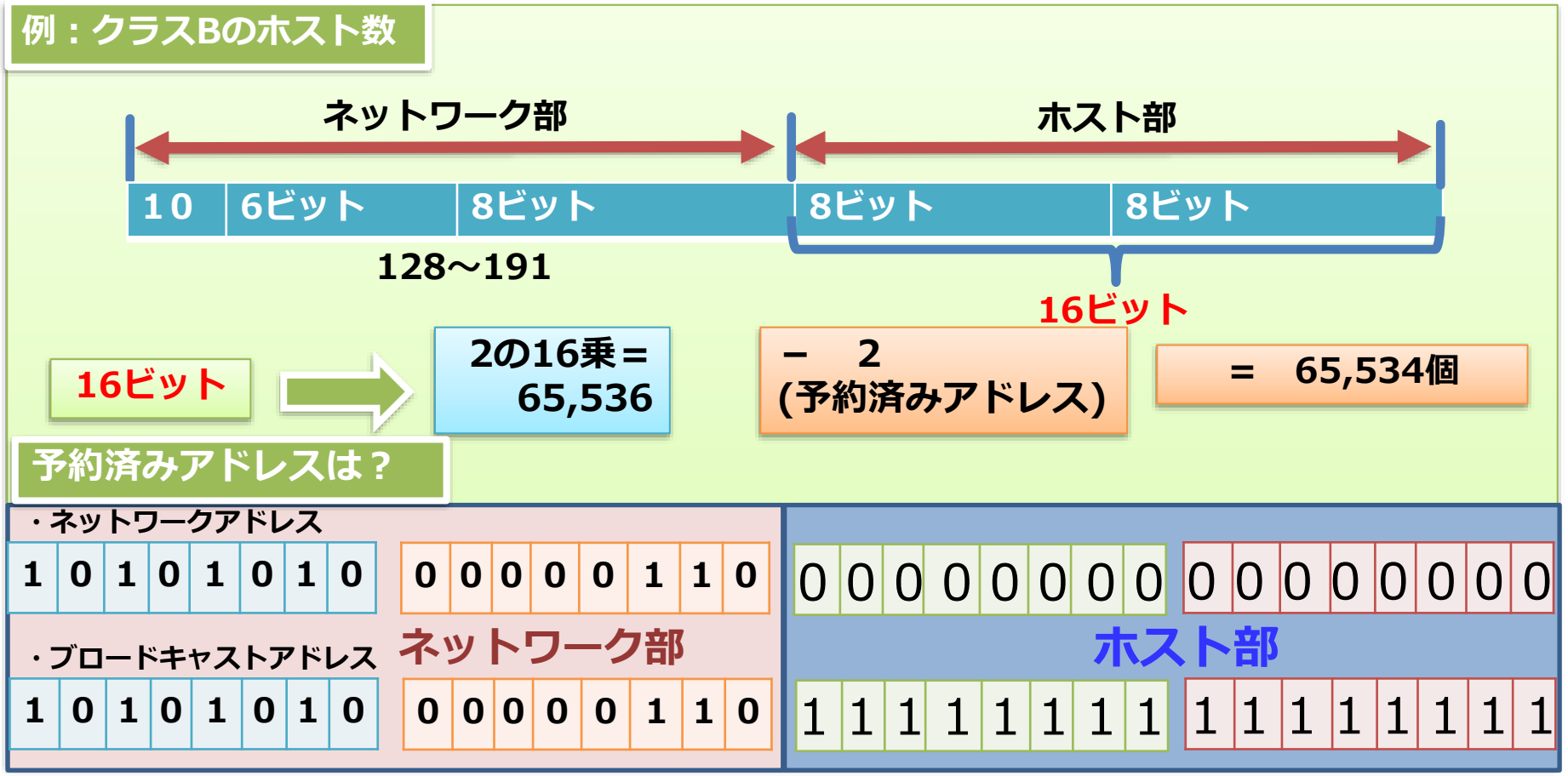
各クラスのサブネットマスク

- 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



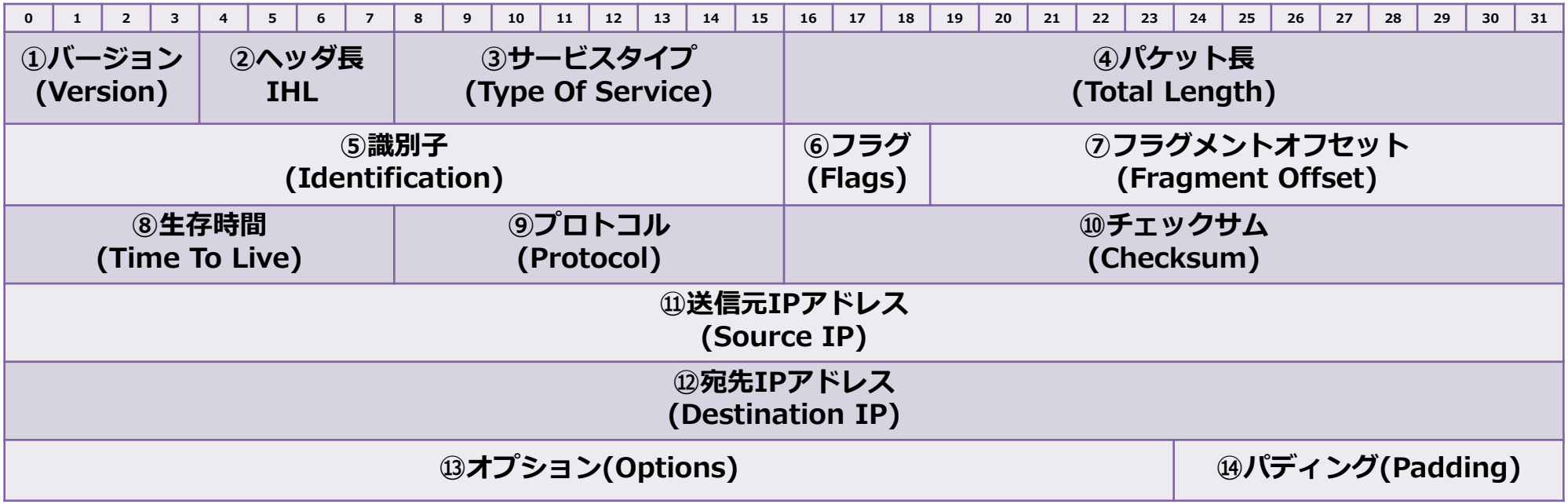
IPv4アドレスのホスト部

- 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



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**

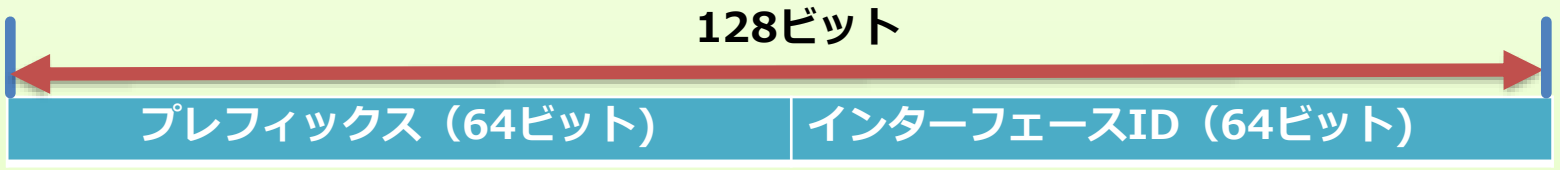


IPv6アドレスの構造と種類

- 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の通信で使用

・**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つに区切る

② 連続する0は省略し、:: と表記できる

③ 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) 長い方を省略する

(b) 長さが同じ場合、先に現れる方を省略する

アドレス表記例

（1）fe80:0:0:0:0a00:46ff:fe60:ee2b ⇒ fe80::a00:46ff:fe60:ee2b と表記

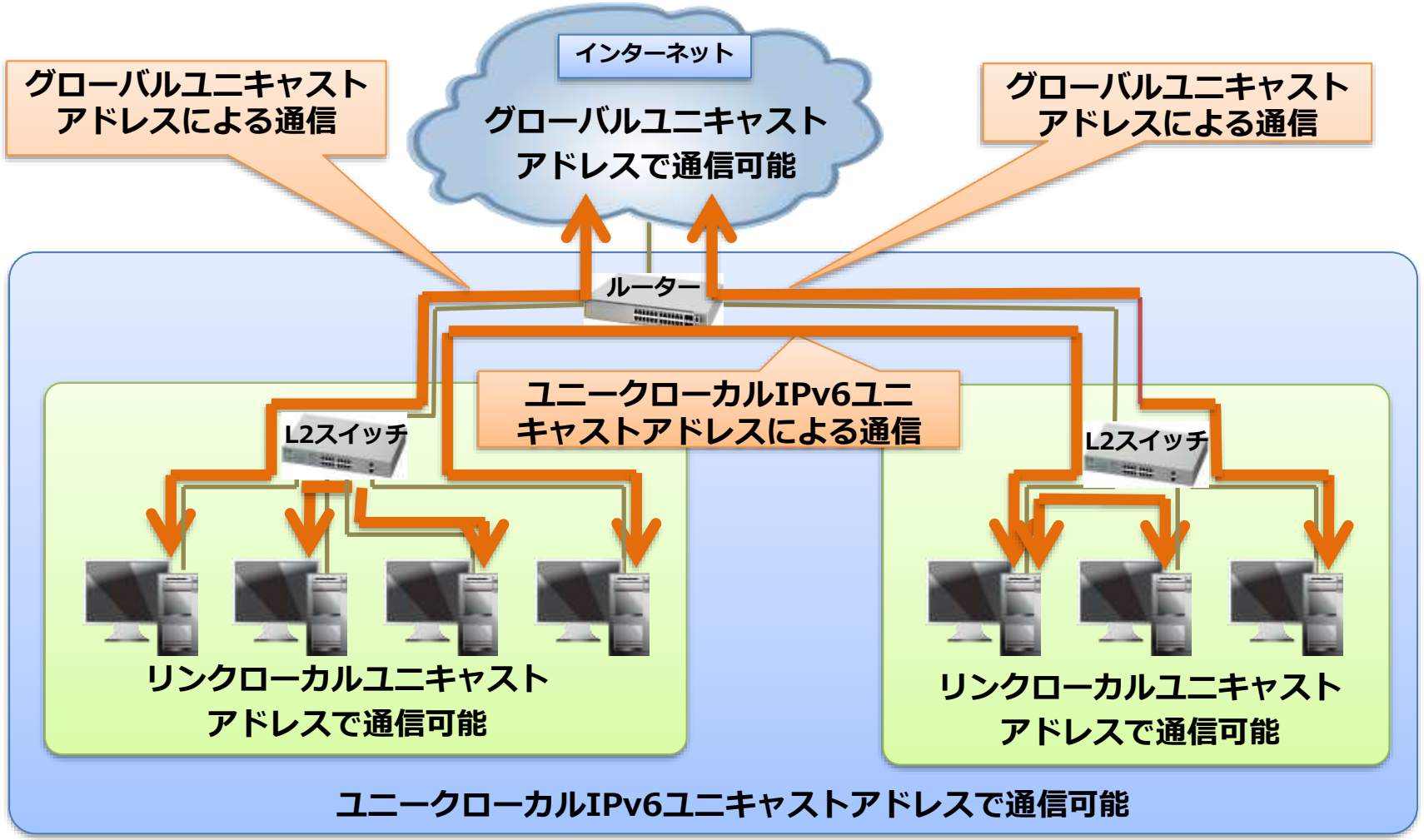
※ 表記規則の②を適用しています

（2）fe80:0:0:8a00:46ff:0:0:ee2b ⇒ fe80::8a00:46ff:0:0:ee2b と表記

※ 表記規則の③(b)を適用しています

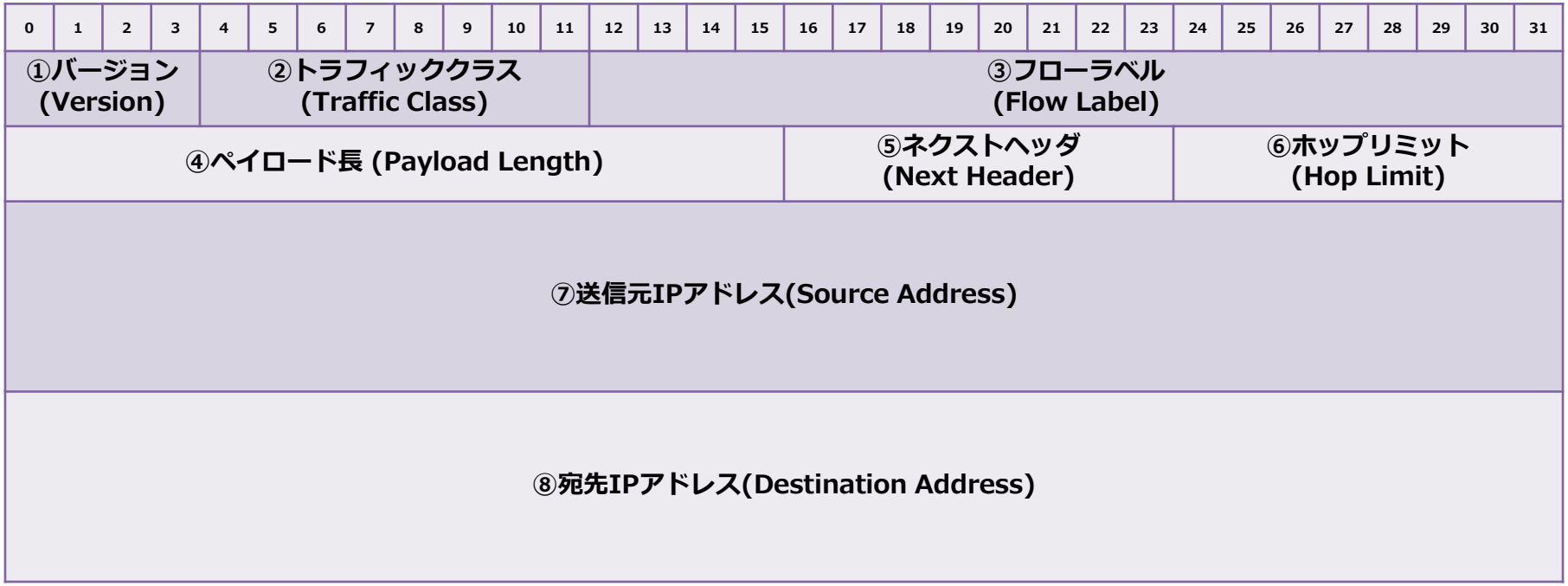
IPv6ユニキャストアドレスの通信

- ユニキャストアドレスがどの通信で使用される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**

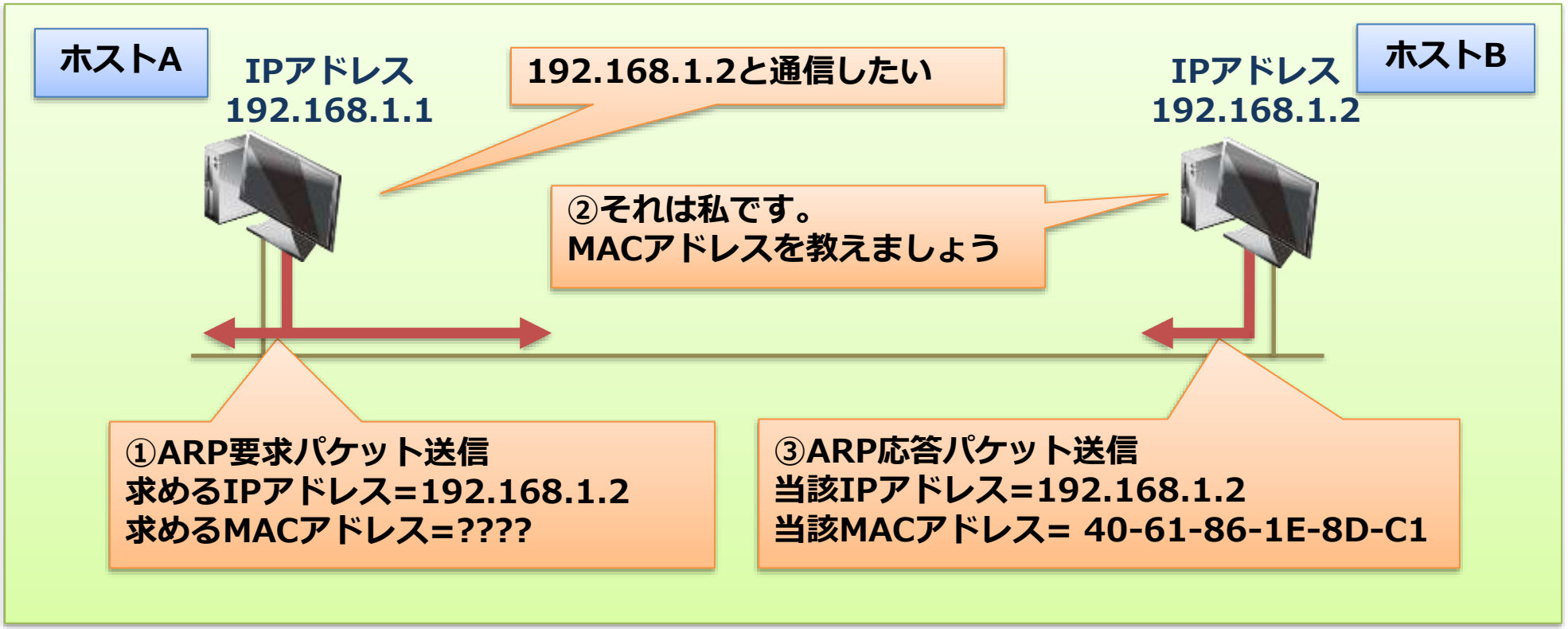


③その他のインターネット層プロトコル

ARP(Address Resolution Protocol)

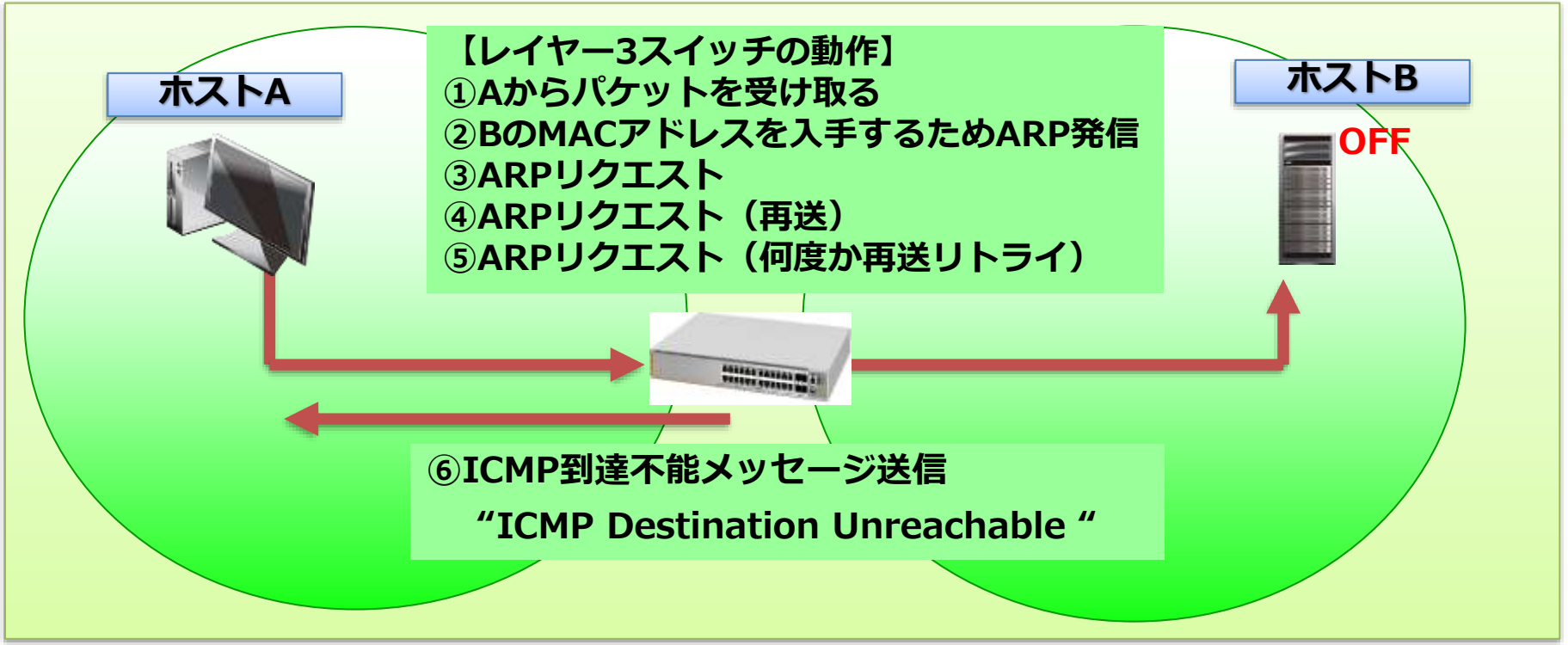
- ARPは、宛先IPアドレスから宛先MACアドレスを知るためのIPv4限定のプロトコルです
- ARPは以下の順序で動作します
  - ①MACアドレスを知りたい宛先IPアドレスをセットし、ARP要求をブロードキャストで送出します
  - ②該当する端末のみが、このブロードキャスト通信に反応します
  - ③該当する端末は、自分のMACアドレスを含めた応答を返します

※ 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



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
  - 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
- 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

ICMPメッセージの役割と主なメッセージ

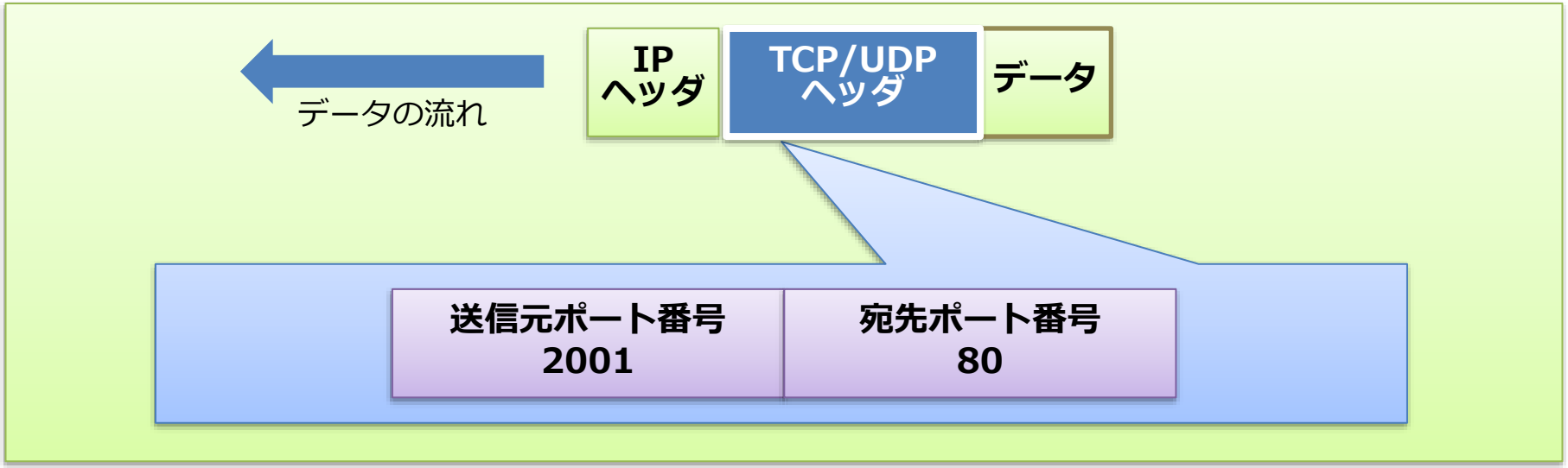
- ICMPメッセージには以下の役割があります
  - 「①**宛先IPアドレスへの通信の可否**を確認」「②Pingパケットによる**宛先ホストの稼働の有無**と応答速度を確認」「③TTLパラメータによる**時間超過**を確認」「④機器間の通信速度の違いを調整する**フロー制御**」「⑤アドレスマスク要求・応答により**サブネットマスク情報を取得**」「⑥URLなどへのリクエストを転送する**Redirect機能**、送信ホストへの送信経路の変更も指示」
- 主なICMPメッセージは以下になります

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

④TCP/UDP

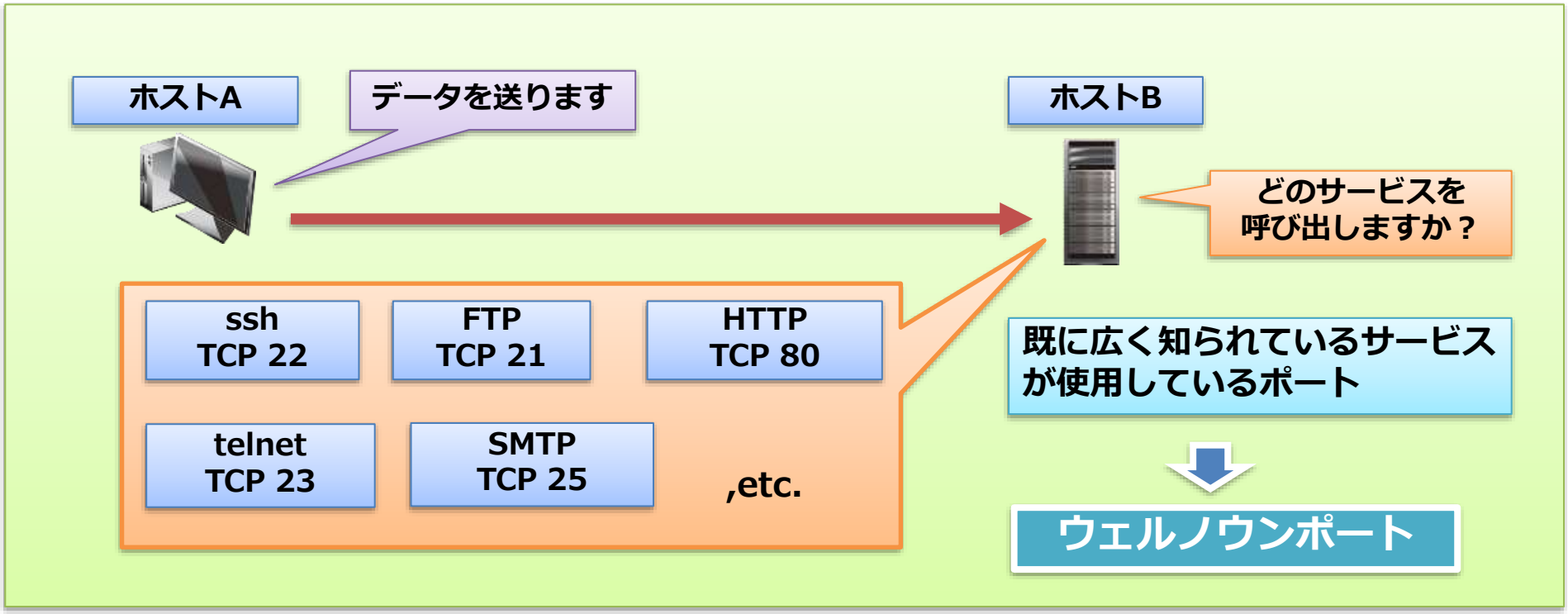
TCP/UDPの役割

- TCP/IPのトランスポート層には、コネクション型のTCP(Transmission Control Protocol)と、コネクションレス型のUDP(User Datagram Protocol)があります。各プロトコルは「ポート番号」と呼ばれる識別番号を利用して上位層のプロトコルを識別します
- TCPは、データの受信後に確認応答を行っており、送信側で一定時間内に確認応答を受信できない場合には、送信元がデータの再送処理を行うことでデータの整合性を保証します
- UDPは再送制御などを行わず「送りっぱなし」にすることで、確実性より転送効率や即時性を重視する用途に用いられます



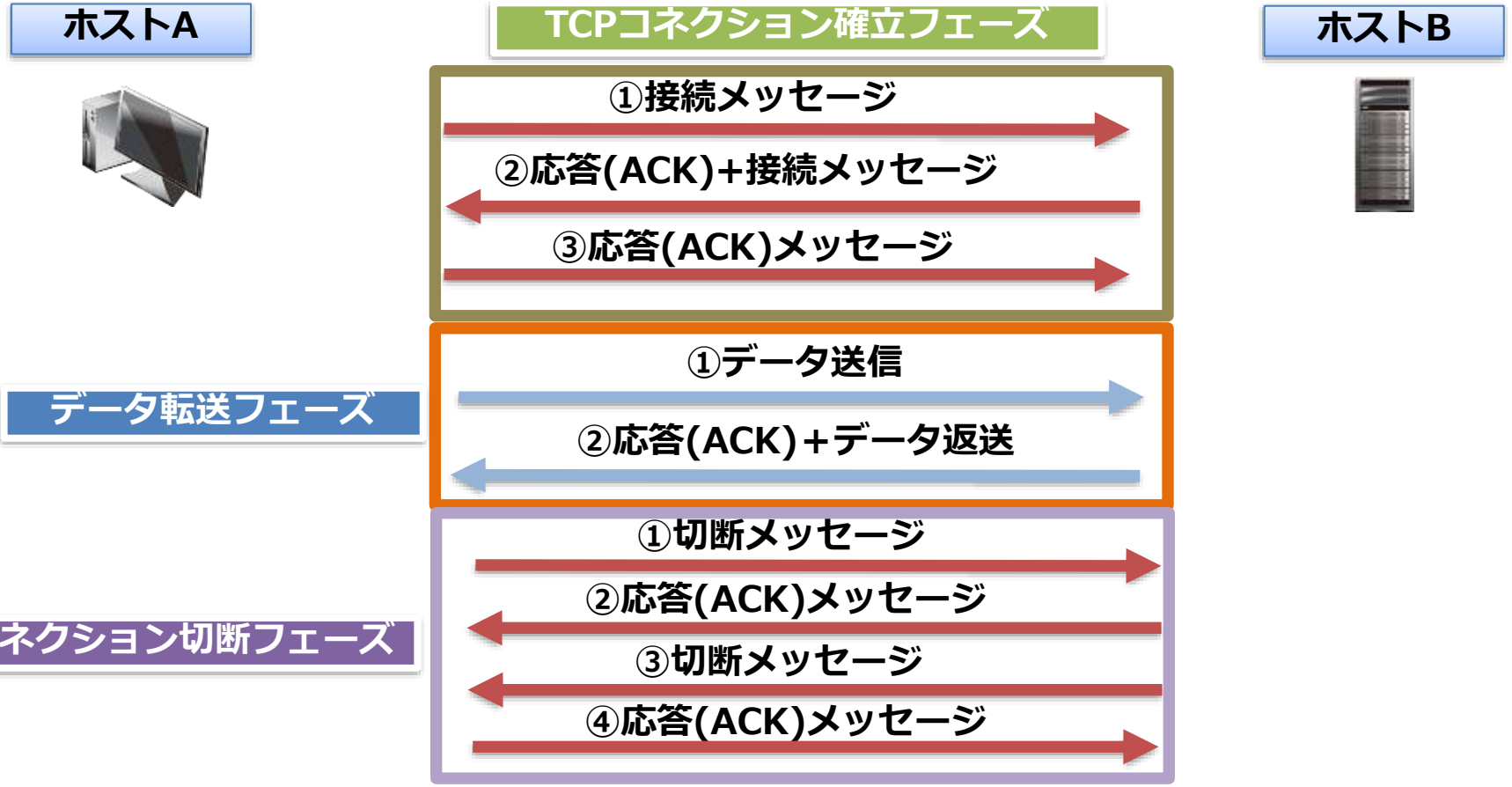
ポート番号の役割

- ポート番号は、通信サービス（アプリケーションプロトコル）を識別する情報です。TCP/IP通信においては、データ受信後にどのプログラムに通信パケットを渡すのかを決定するために、ポート番号を利用します
- アプリケーションプロトコルには決められた番号が割り当てられています。これを、ウェルノウンポートといいます。ウェルノウンポートはポート番号0～65535の内、0～1023番までに割り当てられています



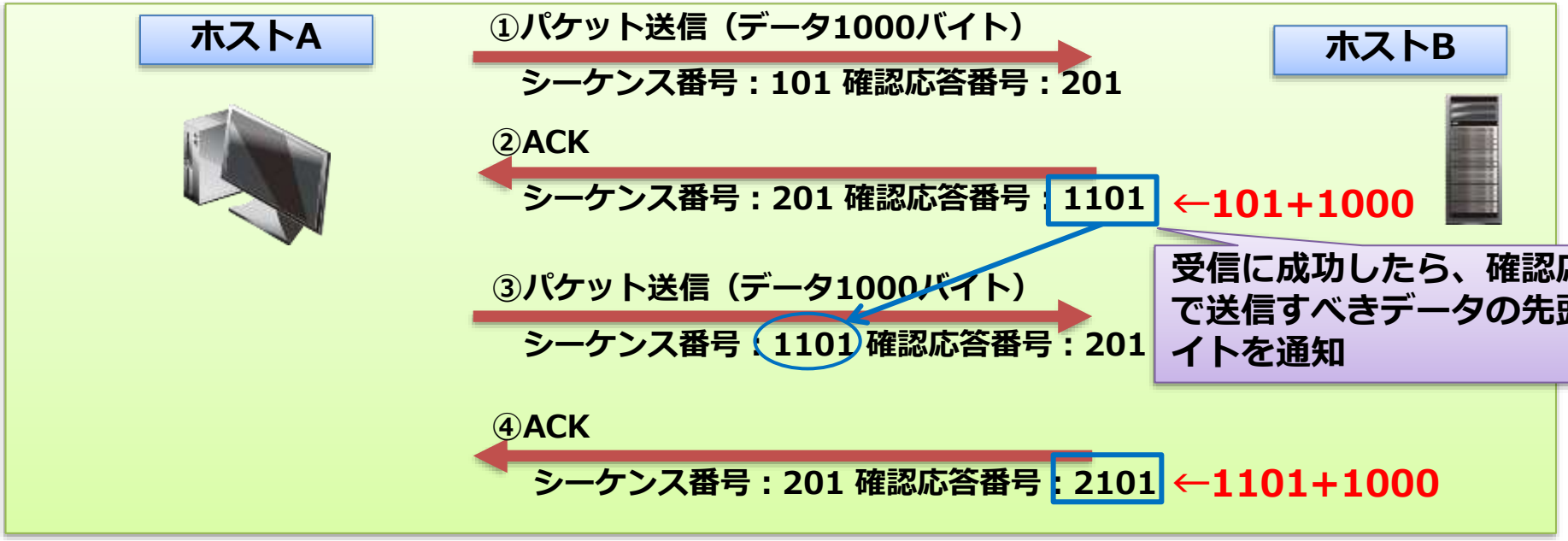
TCPの機能

- TCPは、信頼性の高い通信を実現するために、主に次のような機能で制御を行います
  - 3ウェイハンドシェイクでセッションを確立します
  - 応答確認を行い、ACKが届かない場合はパケットが消失したとみなし再送します
  - 順序制御で、順不同で届いたパケットを正しい順番にします
  - フロー制御で受信側がバッファであるウィンドウのサイズを通知し、適正サイズのデータを送ります



TCPの確認応答

- データ受信側は、送信側へACK（肯定確認応答）でデータが届いたことを知らせます。送信側はデータ送信後に一定時間以内に確認応答が無ければ、もう一度同じデータを送信します。パケットを再送することで、信頼性の高い通信を実現します
- 肯定確認応答は次のように機能します。
  - ① Aはコネクション確立時のシーケンス番号、確認応答番号を使い、Bにデータを1000バイト送信
  - ② Bは受信したシーケンス番号に受信データサイズを加え、確認応答番号として返信します。この例では、「次は1101番目のデータから送信してください」という応答を返します
  - ③ Aは受信した確認応答番号をシーケンス番号にセットし、データを送信
  - ④ Bは受信したシーケンス番号に受信データサイズを加え、確認応答番号として返信します。この例では、「次は2101番目のデータから送信してください」という応答を返します



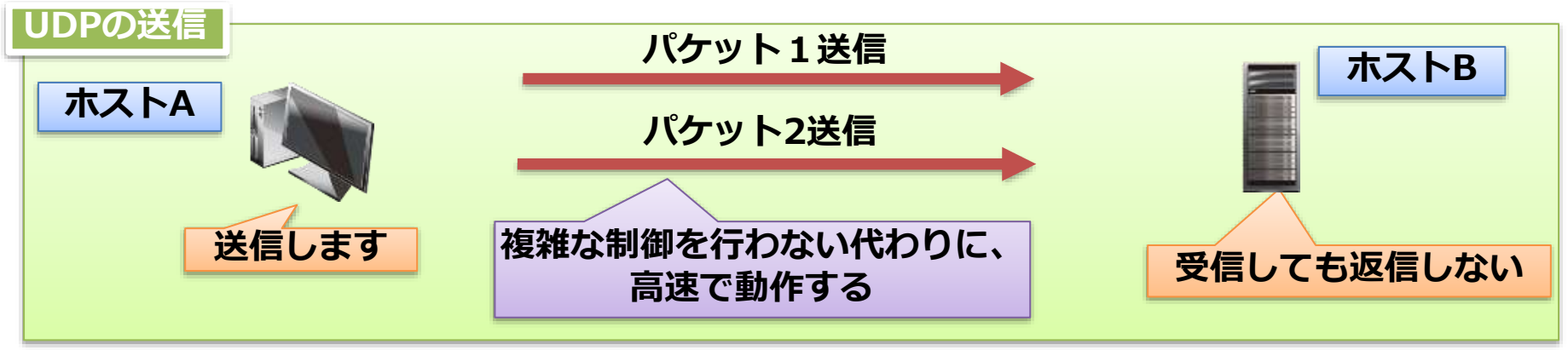
TCPヘッダ

- TCPヘッダのフォーマットは以下になります
  - **①送信元ポート番号、②宛先ポート番号：送信元/宛先のアプリケーションを識別する**
  - **③シーケンス番号は④確認応答番号と連携し、データの整合性を確保する**
  - ⑤データオフセット：TCPのデータの開始位置を示す
  - **⑧ウインドウサイズ：受信可能なデータサイズを通知するために使用する**
  - ⑨チェックサム：ヘッダとデータの信頼性を提供する
  - ⑩緊急ポインタ：URGフラグが1の場合のみ有効で、緊急を要するデータの格納場所を示す
  - ⑫パディング：オプションによりヘッダが32ビット単位でなくなるとダミーのデータが入る

<table>
<tr><td colspan="32">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</td></tr>
<tr><td colspan="16">**①送信元ポート番号
(Source Port)**</td><td colspan="16">**②宛先ポート番号
(Destination Port)**</td></tr>
<tr><td colspan="32">**③シーケンス番号
(Sequence Number)**</td></tr>
<tr><td colspan="32">**④確認応答番号
(Acknowledgment Number)**</td></tr>
<tr><td colspan="4">**⑤データオフセット
(Data Offset)**</td><td colspan="4">**⑥予約済
(Reserved)**</td><td colspan="8">**⑦コントロールフラグ
(Control Flag)**</td><td colspan="16">**⑧ウィンドウサイズ
(Windows)**</td></tr>
<tr><td colspan="16">**⑨チェックサム
(Checksum)**</td><td colspan="16">**⑩緊急ポインタ
(Urgent Pointer)**</td></tr>
<tr><td colspan="24">**⑪オプション
(Options)**</td><td colspan="8">**⑫パディング
(Padding)**</td></tr>
</table>

UDPの機能

- UDPは、コネクションレス型の通信サービスを提供します。そのため、通信の信頼性は低くなりますが、処理は簡単なことから高速に動作します
- UDPはこの特性により、以下のような用途に向いています
  - 総パケット数が少ない通信
  - 動画や音声などのマルチメディア通信
  - （LANなど）特定のネットワークに限定したアプリケーションの通信
  - 同報性が必要となる通信（ブロードキャスト、マルチキャスト）
- UDPのヘッダは 8バイト長の固定で、非常にシンプルな構成となっています



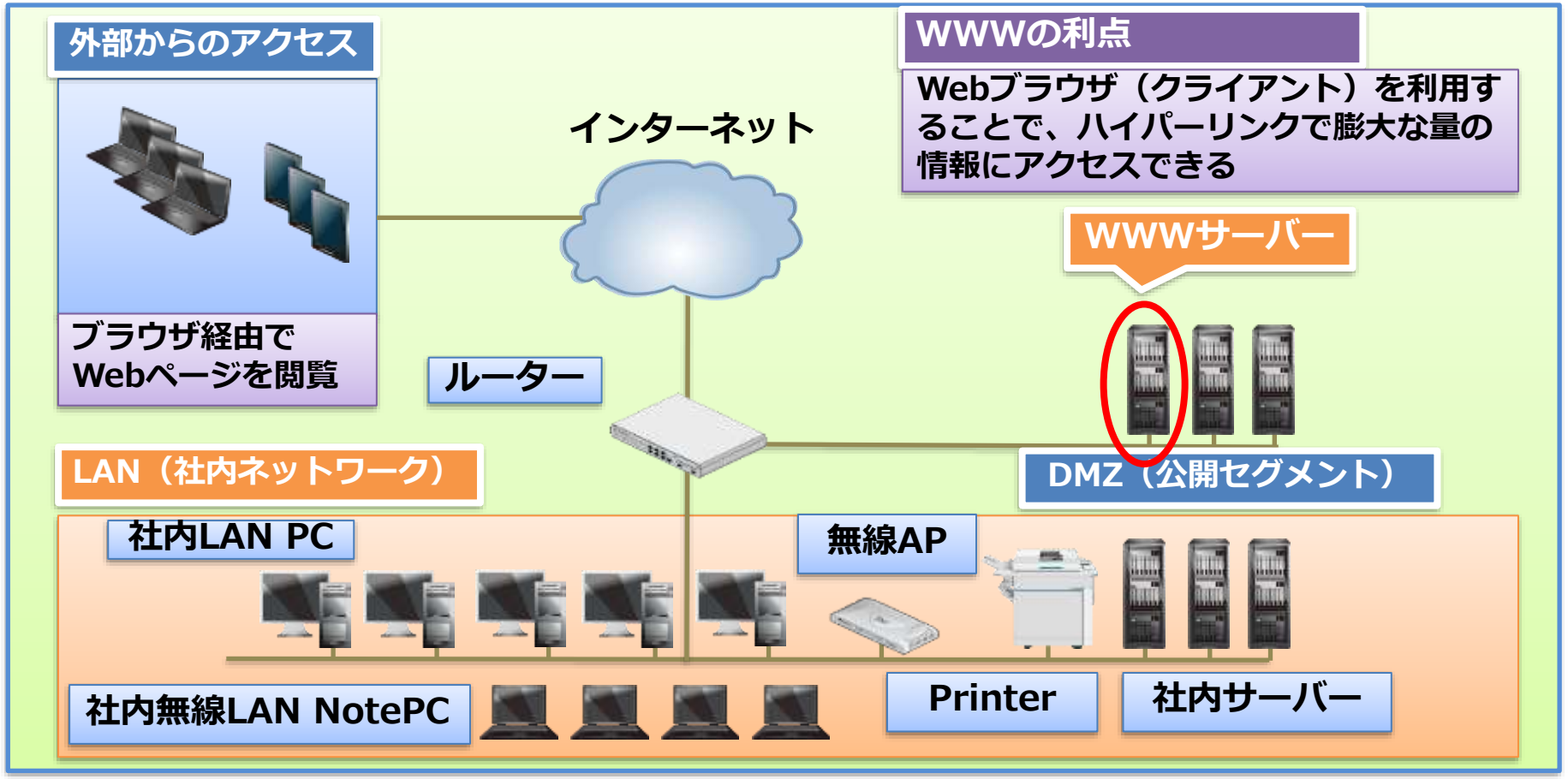
UDPヘッダ

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
送信元ポート番号(Source Port)																宛先ポート番号(Destination Port)															
パケット長(length)																チェックサム(Checksum)															

⑤アプリケーションプロトコル

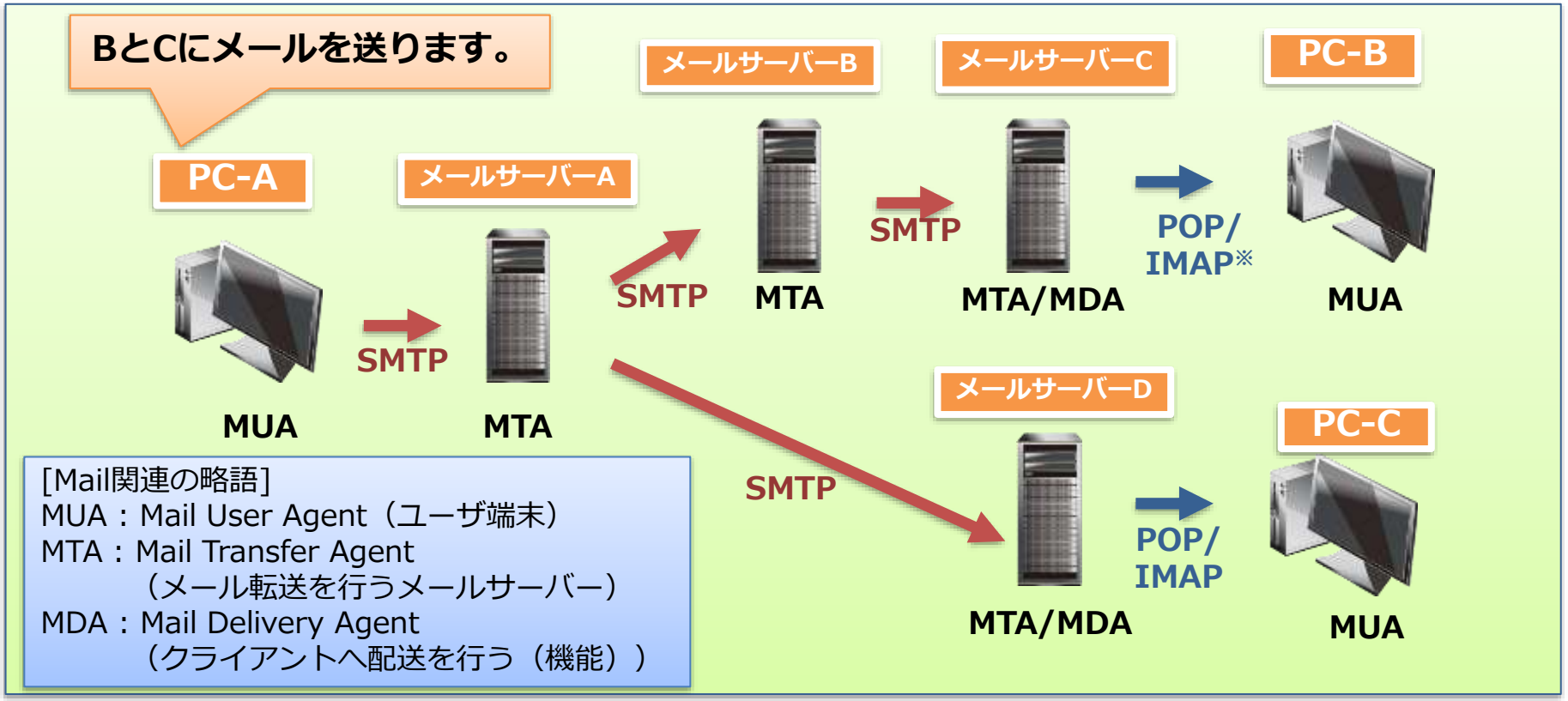
HTTP(Hyper Text Transfer Protocol)

- HTTPは、主にWebブラウザでサーバーとクライアント間での情報をやり取りするプロトコルです
- インターネット上でハイパーテキストの通信を行うしくみのことをWWW(World Wide Web)といいます。WWWのドキュメント（ウェブページ）の記述には主にHTMLやXMLといったハイパーテキスト記述言語を使用します。ハイパーテキストとは、ドキュメントに参照リンク（ハイパーリンク）を埋め込むことでインターネット上に散在するドキュメント同士を相互に参照可能にする技術です



SMTP(Simple Mail Transfer Protocol)

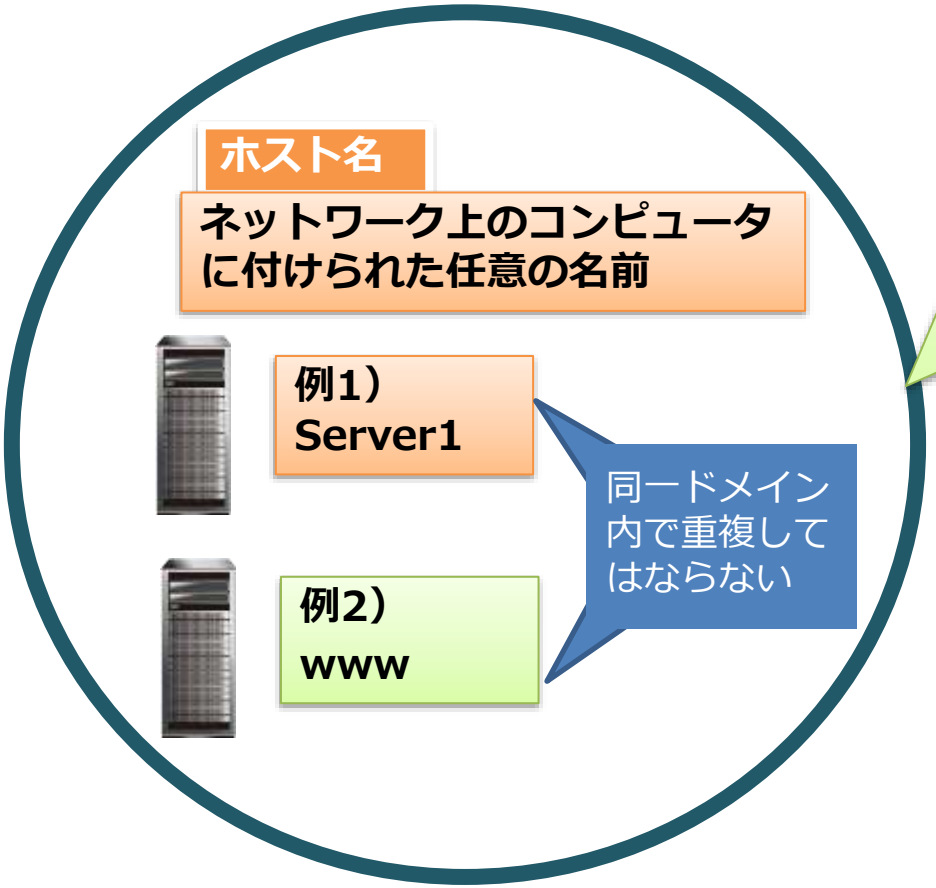
- SMTPは、電子メールを送信するためのプロトコルで、メールをクライアントからメールサーバーへ送信する時、およびメールサーバーからメールサーバーに転送する時に用いられます
- クライアントはMUAとも呼ばれ、MUAはSMTPでメールサーバーにメールを送信します。メールを受け取ったメールサーバーはMTAと呼ばれ、SMTPを用いてメールを転送します。クライアントが自分のメールボックスからメールを読み出す時使用するメール配送の機能をMDAと呼ぶこともあります



※ POP(Post Office Protocol) / IMAP(Internet Message Access Protocol)：電子メールを受信するためのプロトコルで、POPはクライアントにメールがダウンロードされメールサーバーに残りませんが、IMAPはクライアントにメールをダウンロードせず、メールサーバー上のメールをクライアントで閲覧します。一般的にはPOP3やIMAP4が使われます

DNS(Domain Name System)

- DNSは、IPアドレスとホスト名を紐付けて相互に名前解決するための仕組みです。IPアドレスとホスト名を変換することを「名前解決」といいます
- ドメイン名とは、インターネット上のネットワークを特定するための文字列です。ドメイン名は、「他のドメイン名と重複してはいけない」というルールがあるため、ICANN(Internet Corporation for Assigned Names and Numbers)を頂点とした組織で一元管理しています。また、ホスト名とは、ネットワーク上のコンピュータにつける識別用の文字列で、同一ドメイン内での重複はできません



ドメイン名

インターネット上のネットワークを特定するための文字列
ドメイン名は、一元管理されており一意（ユニーク）なもの

例）allied-telesis.co.jp

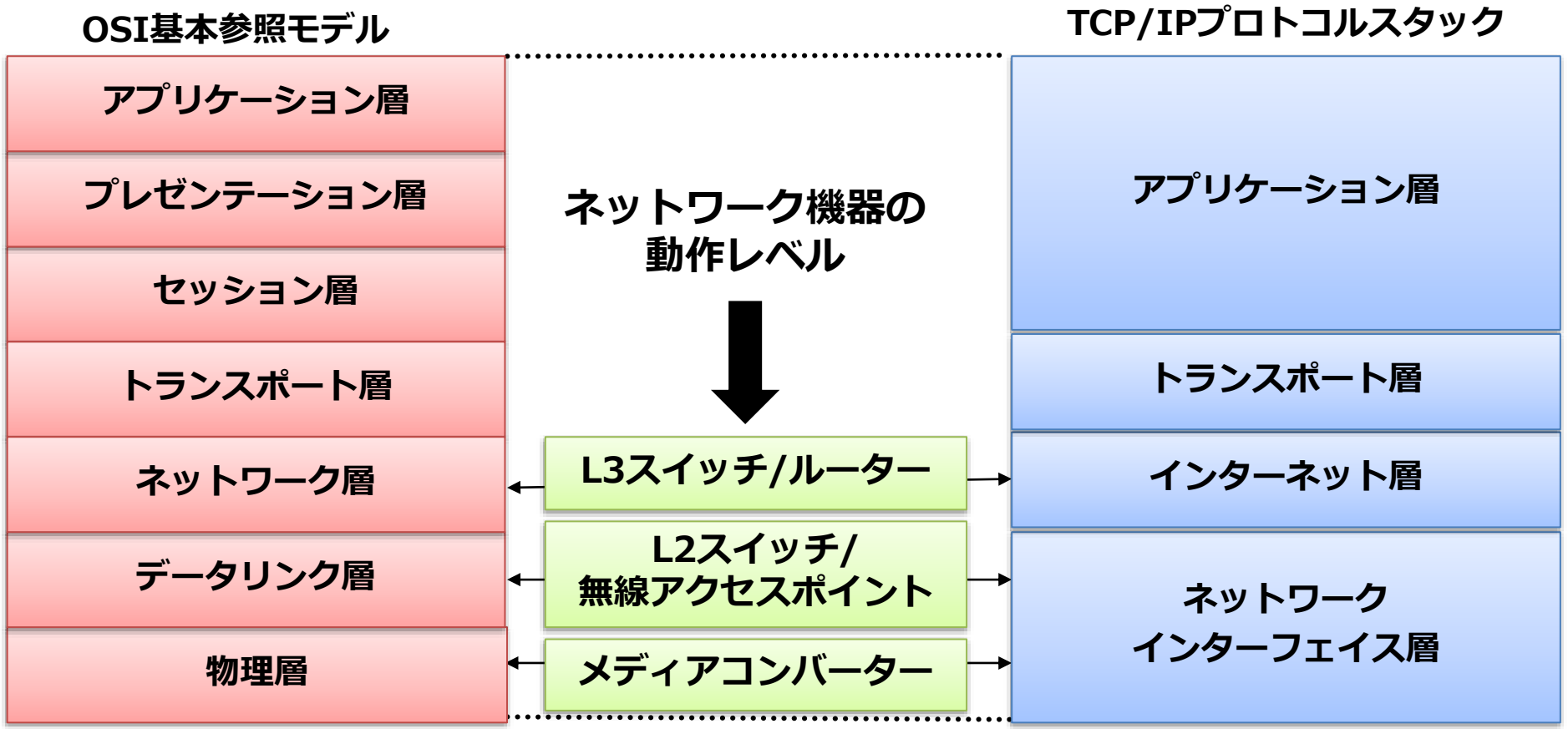
FQDN（Fully Qualified Domain Name : 完全修飾ドメイン名）

ホスト名とドメイン名を連結した文字列のこと。例えば、「www.allied-telesis.co.jp」は、「allied-telesis.co.jp のドメイン内にある wwwという名前のコンピュータ」ということになる。

⑥ネットワーク機器とIPアドレス

ネットワーク機器とTCP/IP階層

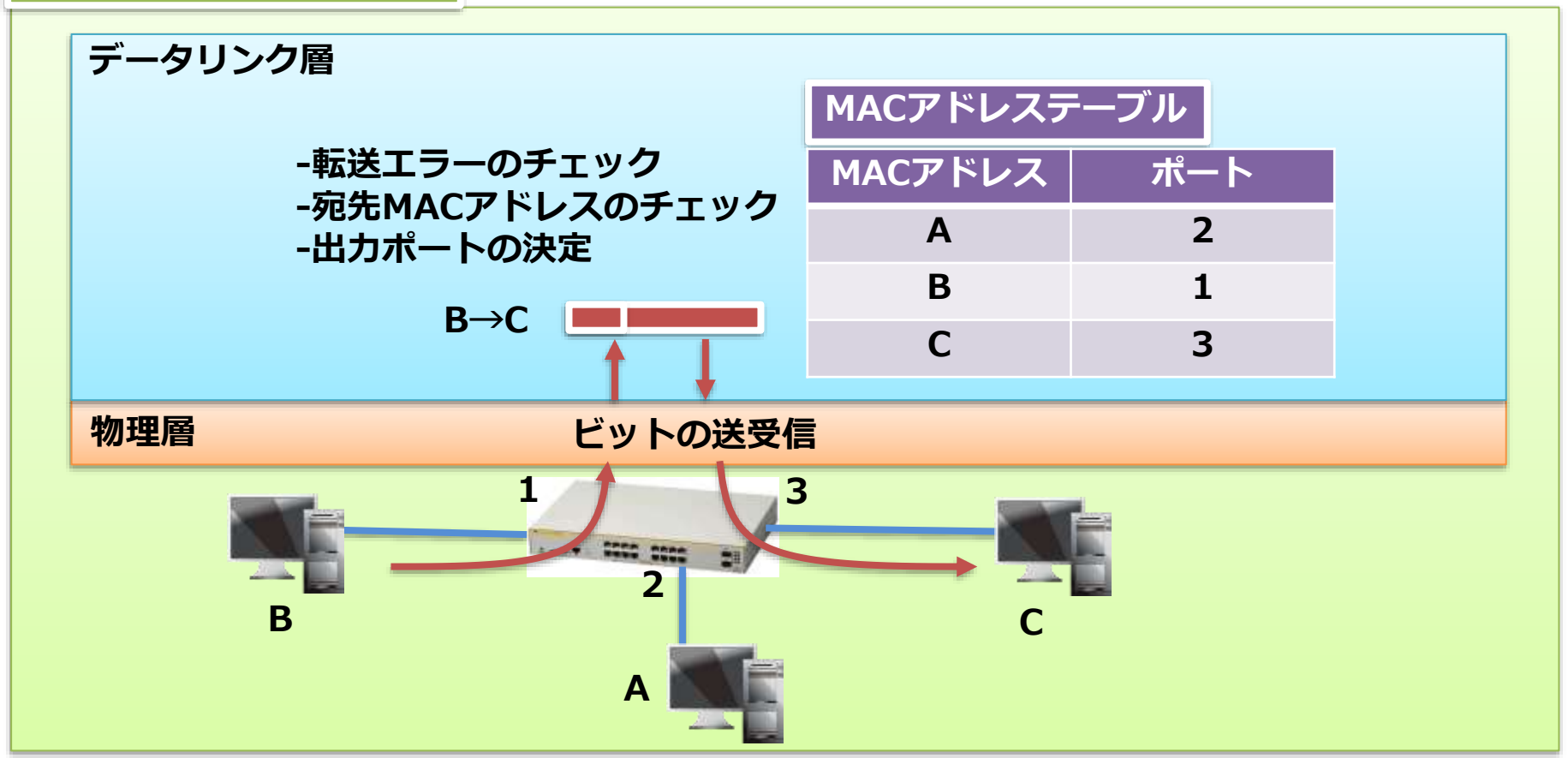
- ネットワーク機器は主に第3層のネットワーク層以下の機能を持つため、インターネット層以下の情報を使用します。ただし、L3スイッチおよびルーターは、アプリケーション制御の機能などでトランスポート層レベルの情報を使用することもあります



レイヤー2スイッチとIPアドレス

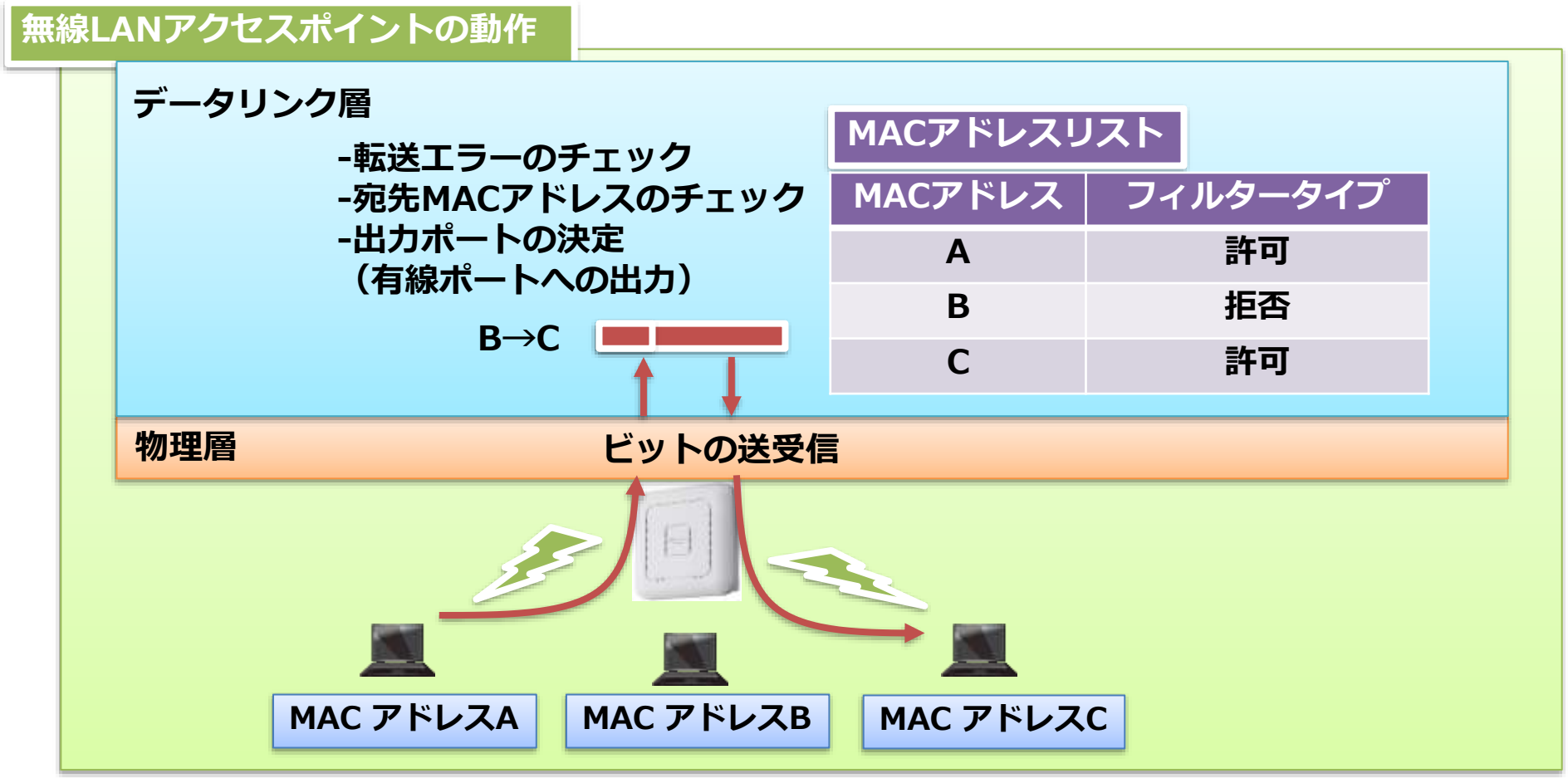
- レイヤー2スイッチへのIPアドレス設定は、ノンインテリジェントスイッチには行えませんが、インテリジェントスイッチには通常管理目的で設定します
- レイヤー2スイッチは転送処理にMACアドレス情報を利用し、IPアドレス情報は利用しません

レイヤー2スイッチの動作



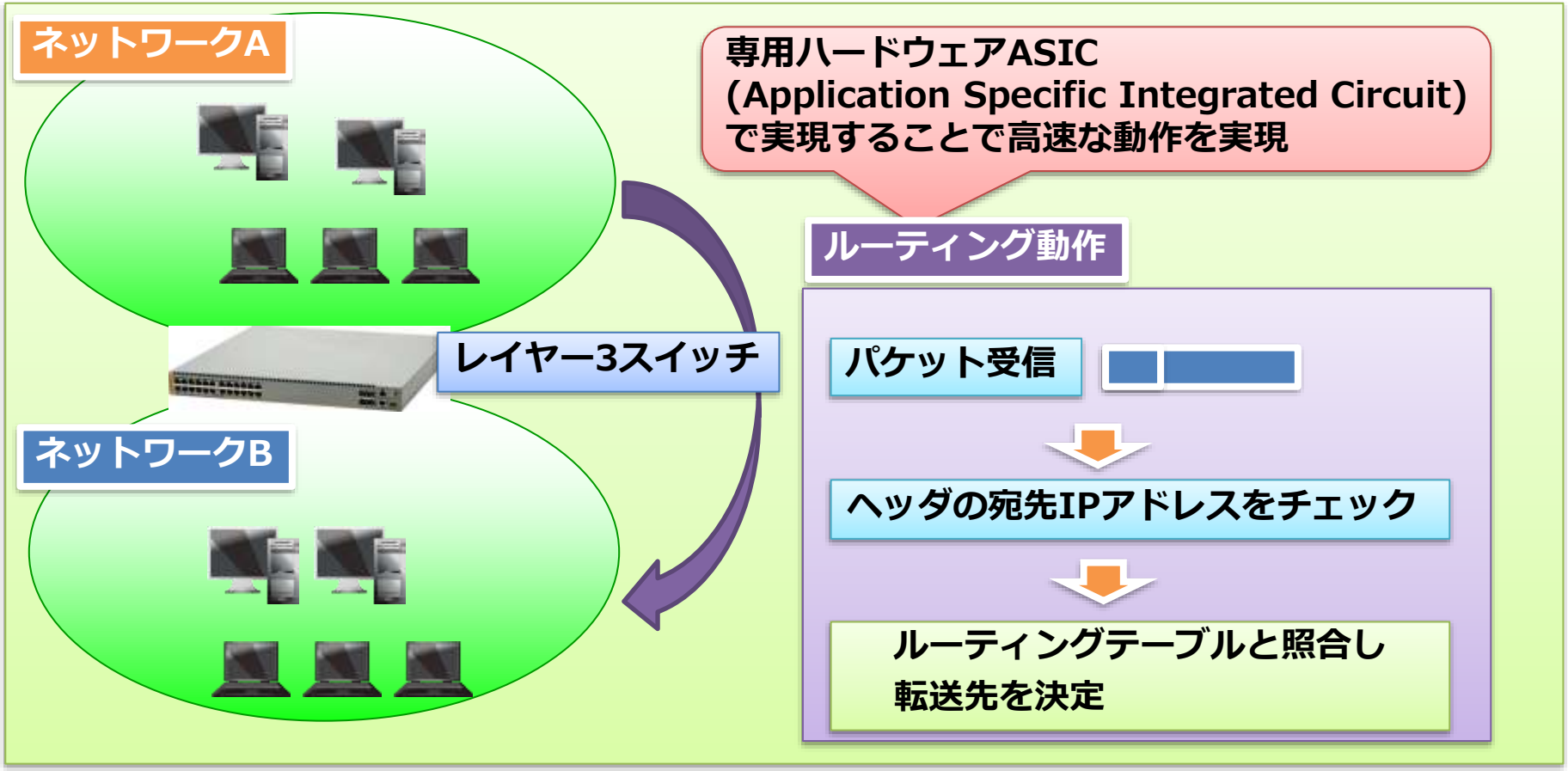
無線LANアクセスポイントとIPアドレス

- 無線LANアクセスポイントへのIPアドレス設定は、通常管理目的で設定します
- 無線LANアクセスポイントは、転送処理にはMACアドレス情報を利用し、IPアドレス情報は利用しません（同一SSIDの無線端末同士が通信する）
- 無線LANアクセスポイントには接続可能な無線端末のMACアドレスを設定可能です



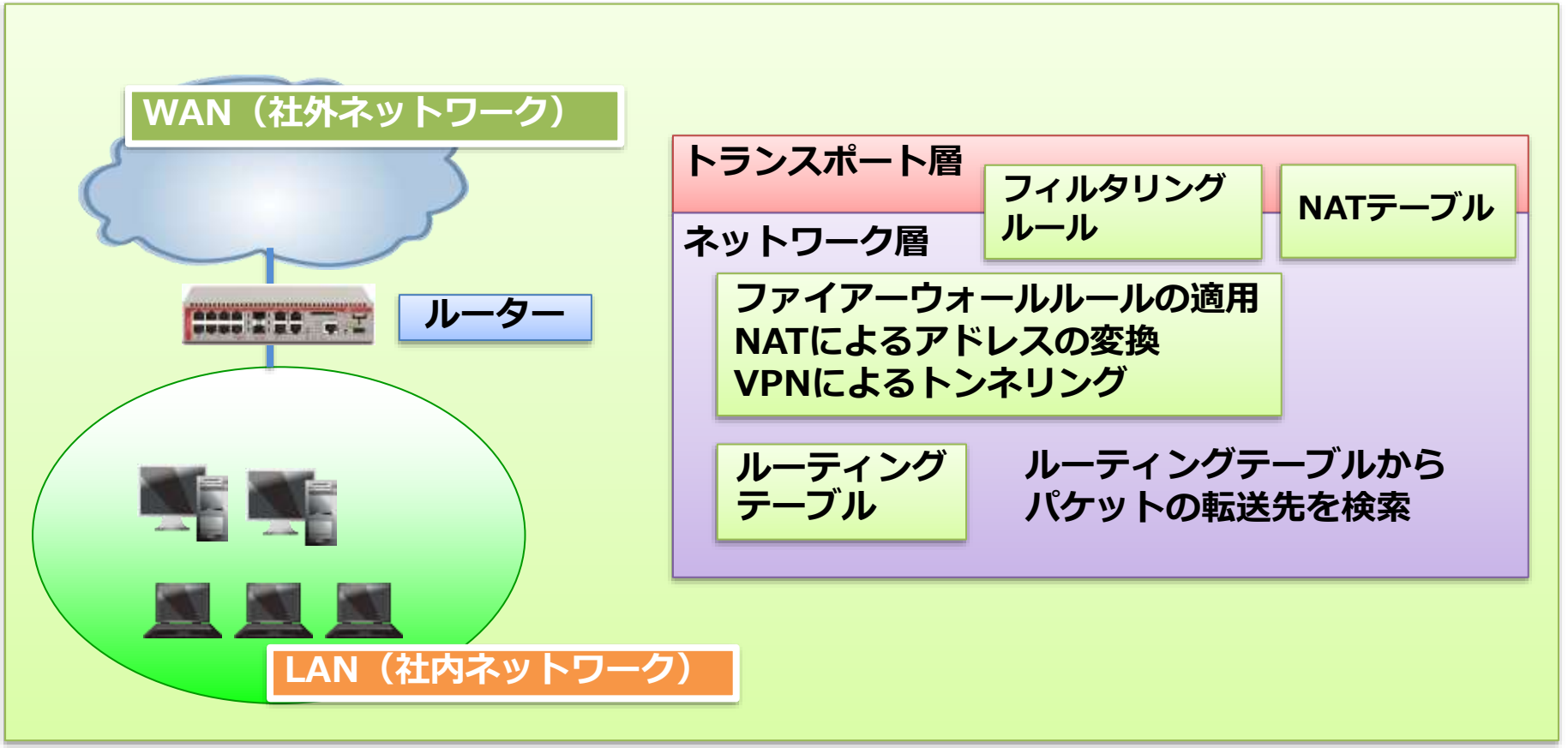
レイヤー3スイッチとIPアドレス

- レイヤー３スイッチには、インターフェース単位でIPアドレスを設定します
- レイヤー3スイッチは、転送処理にIPアドレス情報とMACアドレス情報を利用します。そのため、IP(ネットワーク)アドレス情報をルーティングテーブルに事前に登録します
- IPアドレス情報は、レイヤー3スイッチが持つパケットフィルタリング、QoSなどの様々な転送機能（別セミナーで説明）で利用されます



ルーターとIPアドレス

- ルーターには、インターフェース単位でIPアドレスを設定します
- ルーターは、転送処理にIPアドレス情報とMACアドレス情報を利用します。そのため、IP(ネットワーク)アドレス情報をルーティングテーブルに事前に登録します
- IPアドレス情報は、ルーターが持つファイアウォール、NAT、パケットフィルタリング、QoSなどの様々な転送機能（別セミナーで説明）で利用されます



ご清聴ありがとうございました。

Allied Telesis

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。