初級レベル研修

TCP/IPセミナー
-アプリケーション編-

NETREND 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

V2.1

内容

① TCP/UDP

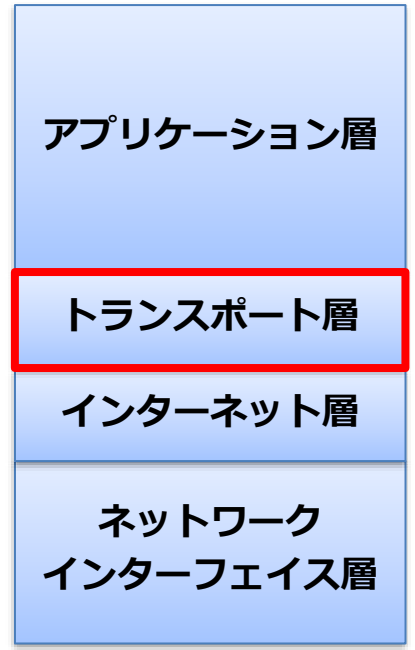
② アプリケーションプロトコル

③ インターネット通信を実現するアプリケーションプロトコル

④ 通信機器におけるIPアドレス・アプリケーション

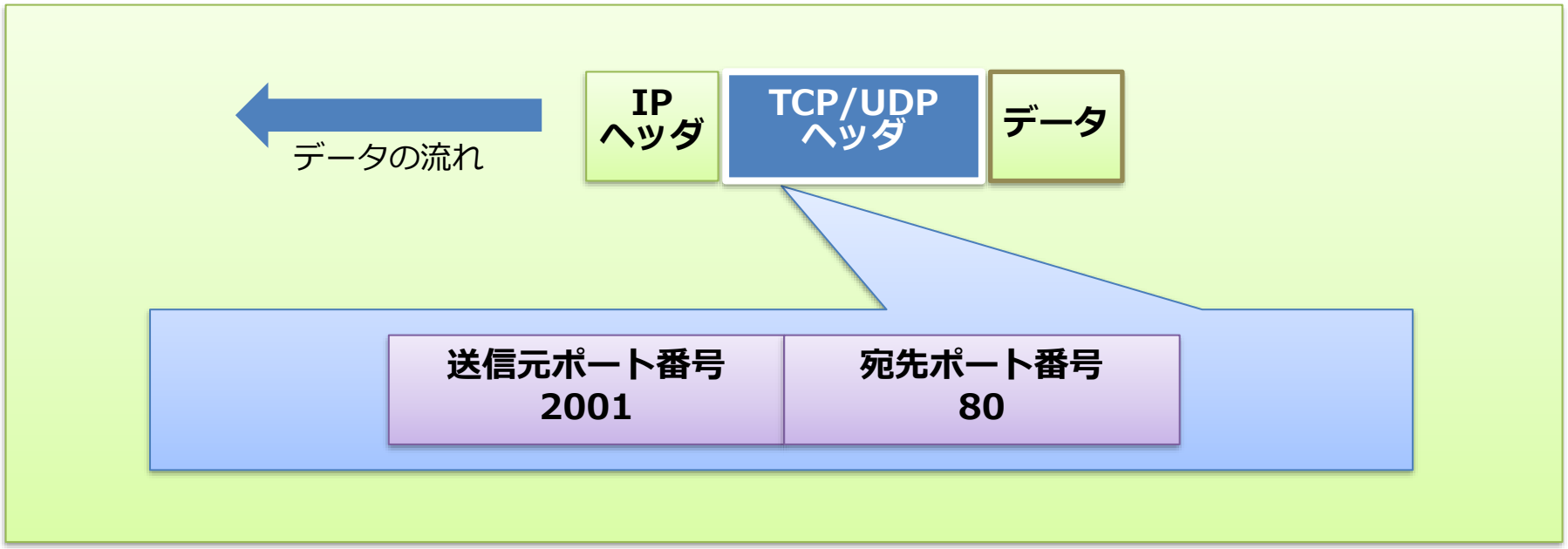
Appendix：各種販促情報のご案内など

①TCP/UDP



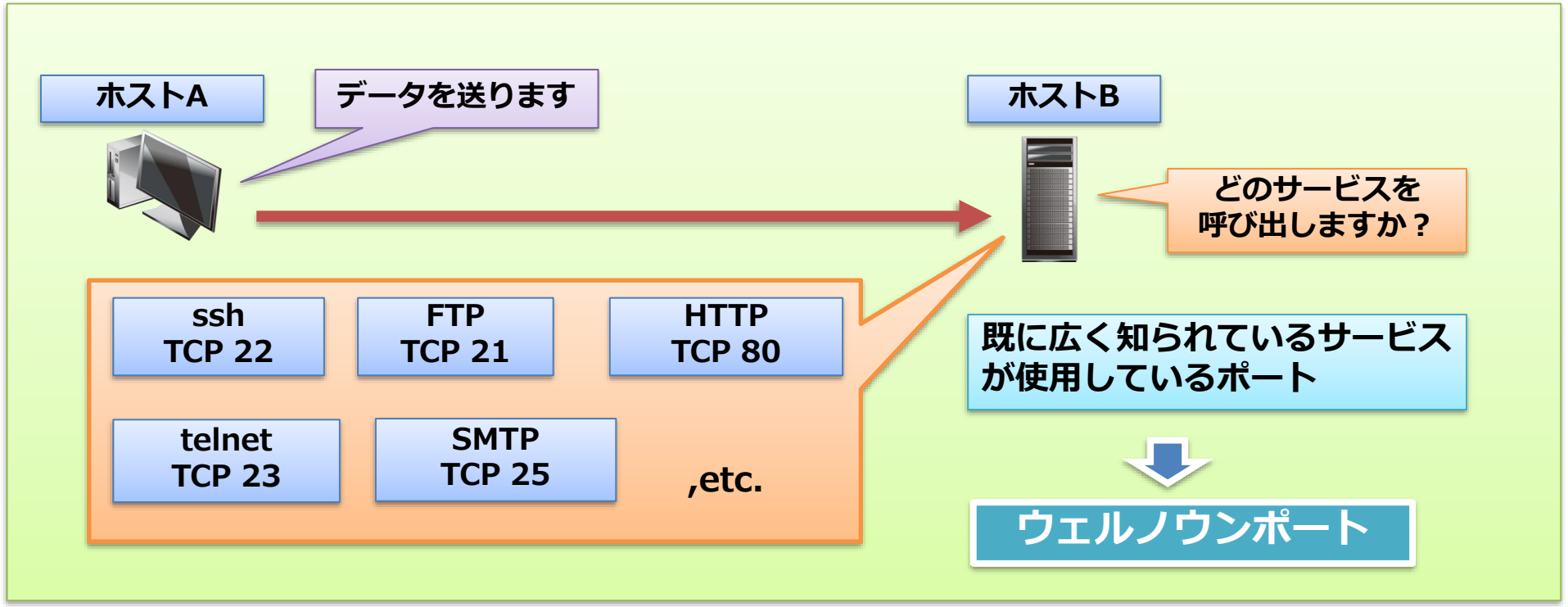
TCP/UDPの役割

- 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。



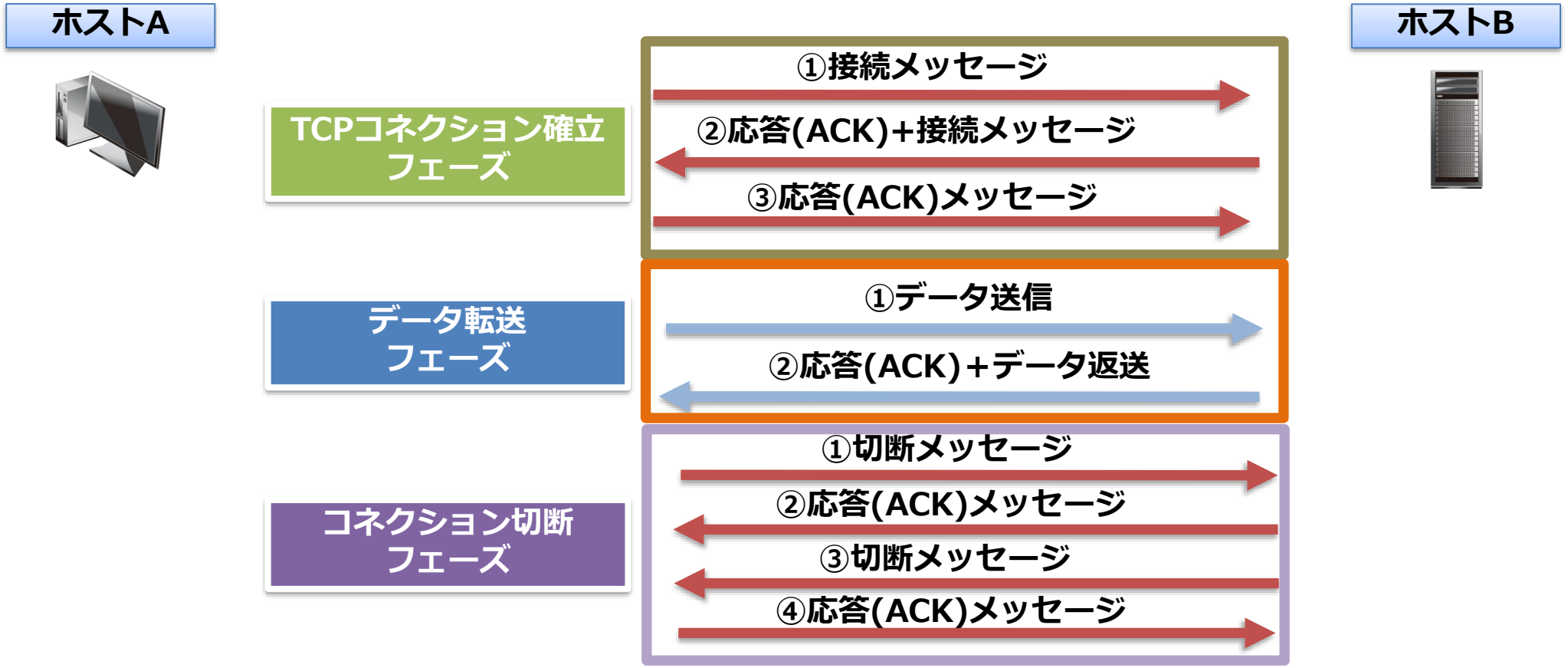
ポート番号の役割

- 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。



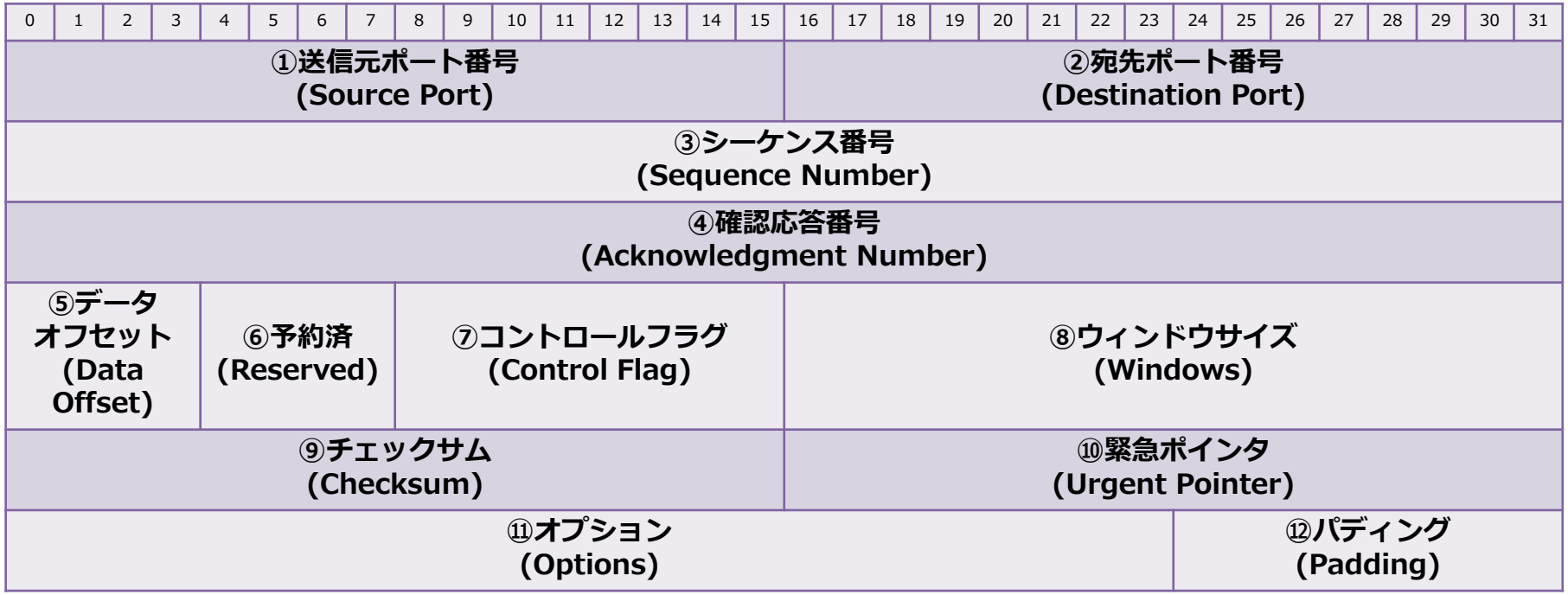
TCPの機能

- 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。
  - 確認応答を行い、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します。**
  - **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します。**
  - ⑤データオフセット：TCPのデータの開始位置を示します。
  - **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します。**
  - ⑨チェックサム：ヘッダとデータの信頼性を提供します。
  - 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します。
  - 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ります。

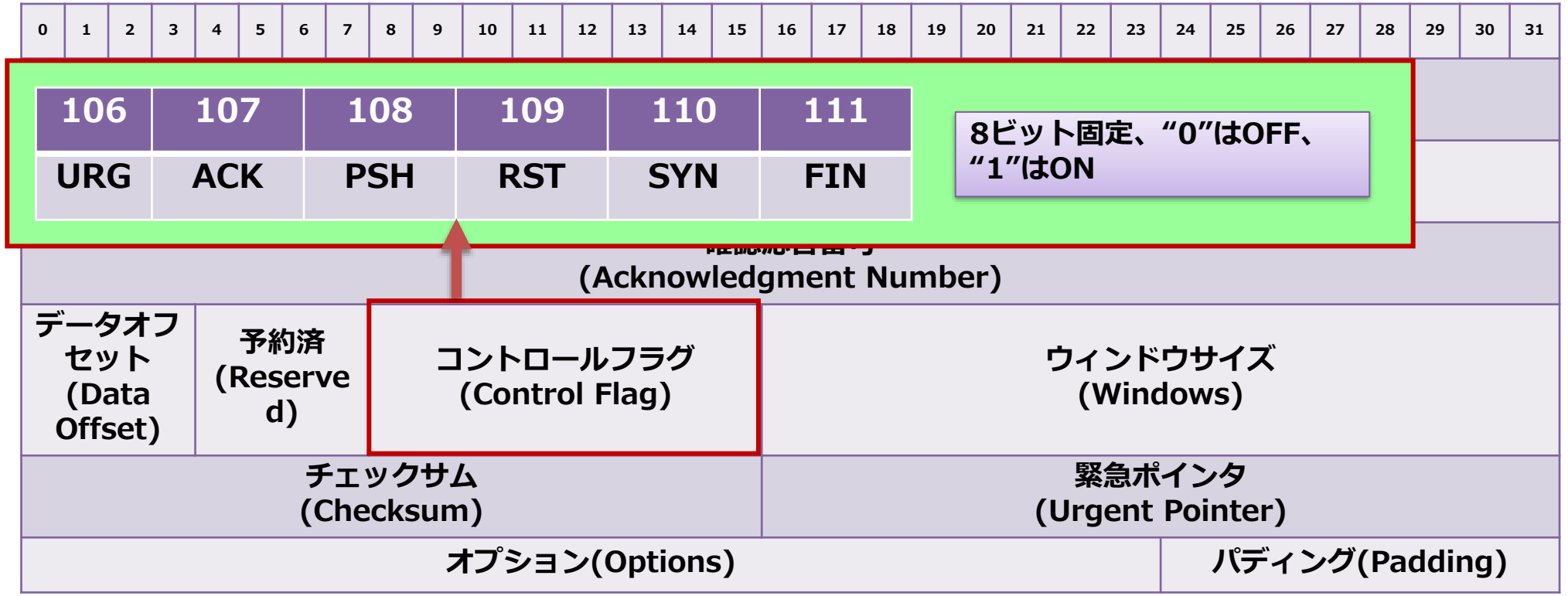


TCPのコネクションの確立と切断

- コネクションの確立は、 3ウェイハンドシェイクと呼ぶ方法で行います。
  - ① AからBへ制御ビットのSYNフラグを「1」にした「SYNパケット」を送信します。
  - ② BはACKフラグをオンにし、さらにSYNフラグを「1」にしたパケットを返信します。
  - ③ AもACKフラグをオンにして返信し、双方向でコネクションを確立します。
- コネクションの切断は以下の流れになります。
  - ④ Aから制御ビットのFINフラグを「1」にしたFINパケットを送信します。
  - ⑤ Bは切断を了解したという意味のACKパケットを送信します。
  - ⑥ Bは残った処理があれば処理を継続し、終了後、改めてFINパケットを送信します。
  - ⑦ Aがその返信のACKパケットを送信し、コネクションを切断します。

コントロールフラグ（制御ビット）

- セッションの制御は、TCPヘッダのコントロールフラグで行います。
  - URG（Urgent　Flag）：緊急に処理すべきデータが含まれていることを意味
  - ACK（Acknowledgement Flag）：確認応答番号のフィールドが有効であることを意味
  - PSH （Push Flag）：受信したデータをすぐ上位アプリケーションに渡す必要があることを意味
  - RST （Reset Flag）：コネクションの強制的な切断
  - SYN（Synchronize Flag）：コネクション確立の意思表示を意味
  - FIN（Fin Flag）：以後送信データが無いことを意味し、コネクション切断の意思表示を意味

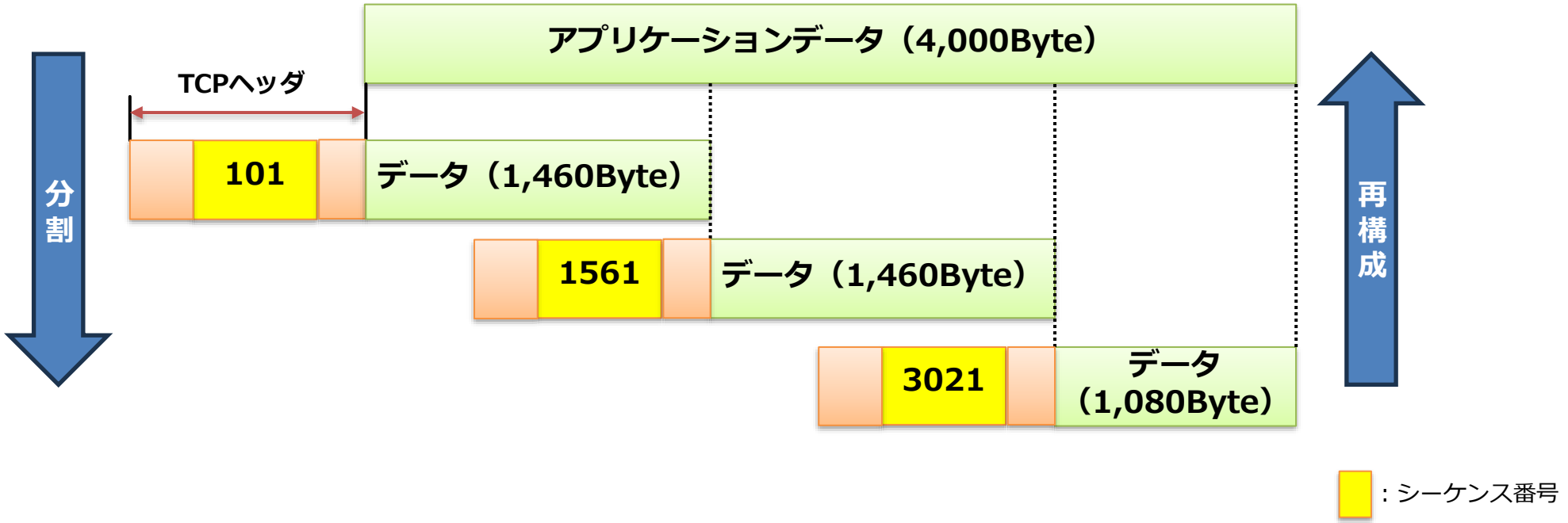


TCPの確認応答

- 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バイト送信します。
  - 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、データを送信します。
  - 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。

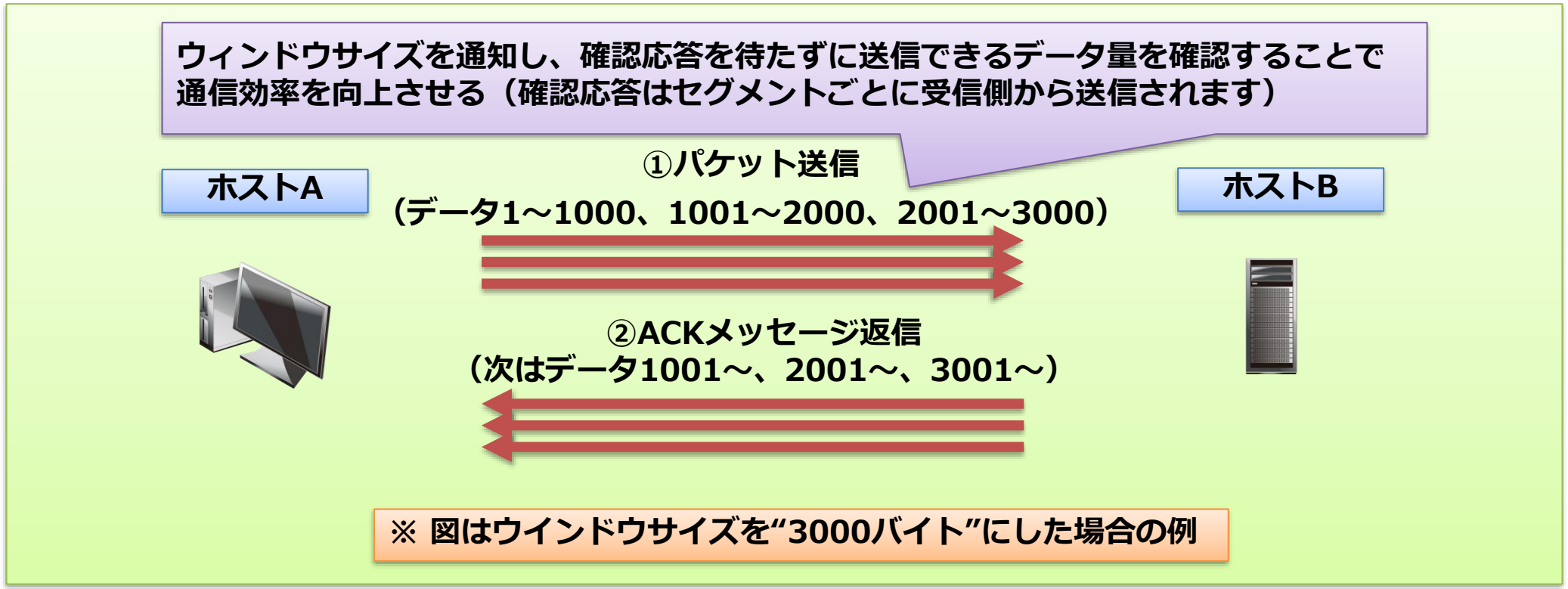
TCPの順序制御

- 送信ホストのTCPは、アプリケーションからIPヘッダとTCPヘッダを付加するとMTUサイズを超えるデータを受け取ると、MSS（Maximum Segment Size）に収まるようにデータを分割します。MSSはMTUからIPヘッダとTCPヘッダを引いた大きさで、MTUが1,500ByteでIPv4ヘッダを付加する場合は、1,460Byteになります。
- 分割されたデータは、受信ホストのTCPで元の順番通りに再構成されます。この機能を順序制御と呼び、TCPヘッダ内のシーケンス番号の値を元に行います。
- データの分割は送信ホストのIPでも行います。IPでは主にUDPデータを分割します。また、ネットワークの途中経路にMTUサイズの小さいネットワークが存在する場合は、TCPデータ・UDPデータに関係なく、ルーティング機器のIPがMTUサイズ内に収まるようパケットを分割します。



TCPのフロー制御（1）

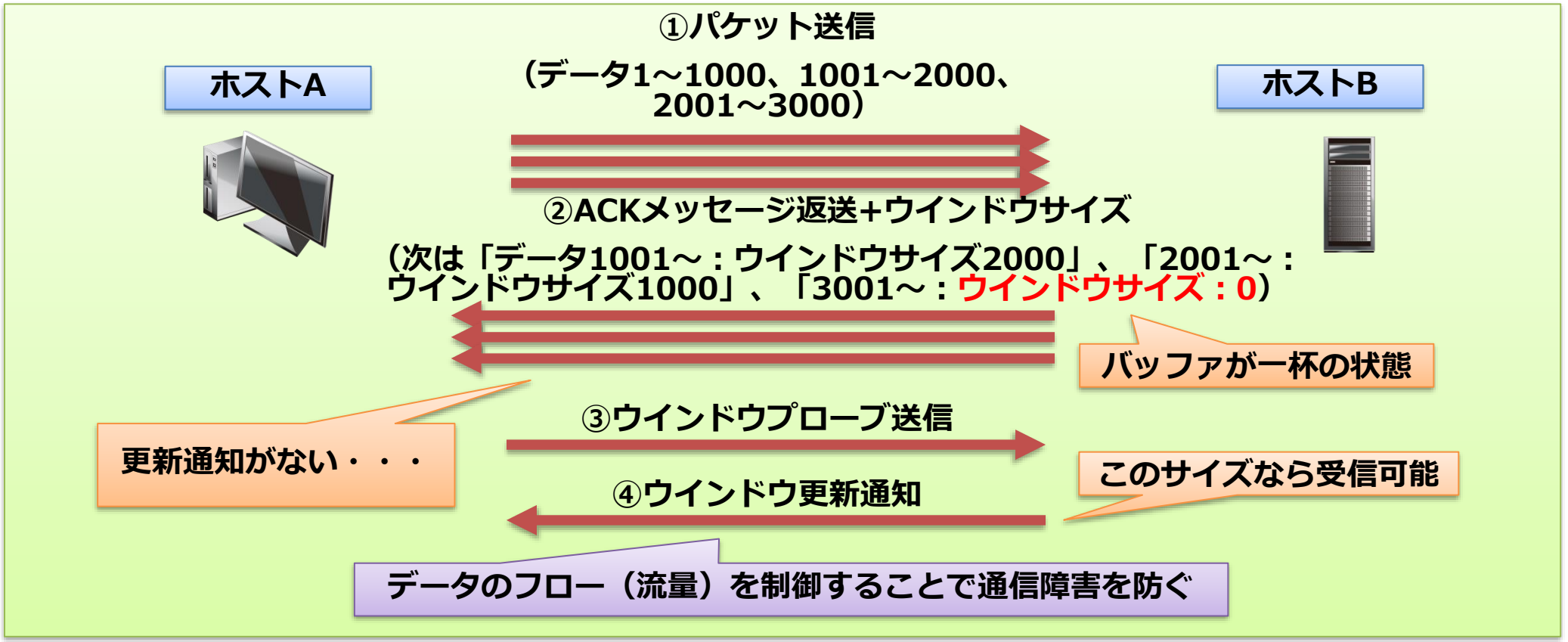
- 前頁では、1セグメント※1ごとに確認応答を行っている例を確認しましたが、1セグメント送信ごとに確認応答を返すとパフォーマンスが悪くなるという問題があります。
- 受信側はTCPヘッダ内のウィンドウサイズで、ACKを待たずに一度に送信できるデータ量を送信側に通知します。送信側はウィンドウサイズ分のデータを複数のセグメントに分けて送信することで、通信効率が向上します（これをウィンドウ制御と呼びます）。



※1 セグメントとはトランスポート層プロトコル（TCP、UDP）のデータ転送単位で、TCPヘッダもしくはUDPヘッダが付加されたデータのことです。

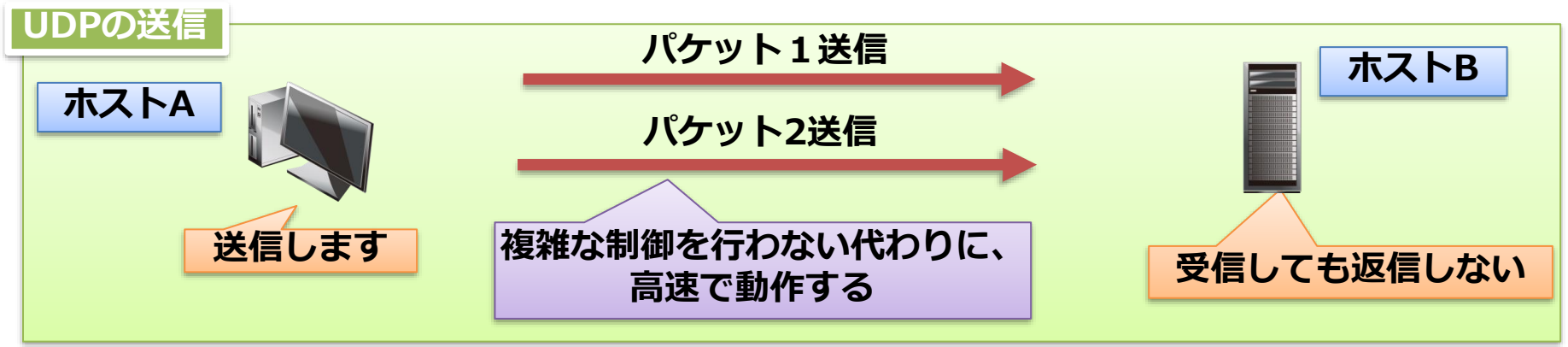
TCPのフロー制御（2）

- 受信側からはACKを返信する際、ウィンドウサイズを都度通知します。これにより、データが受信しきれず、データの再送処理が発生することを防止します。
- 受信側のウィンドウサイズが0(ゼロ)となり、再送タイムアウトの時間が経過しても受信側からウインドウサイズの更新通知がない場合、送信側は「ウインドウプローブ」と呼ばれる1オクテットのデータのみを含むセグメントを送信して、ウインドウサイズの最新情報を取得します。



UDPの機能

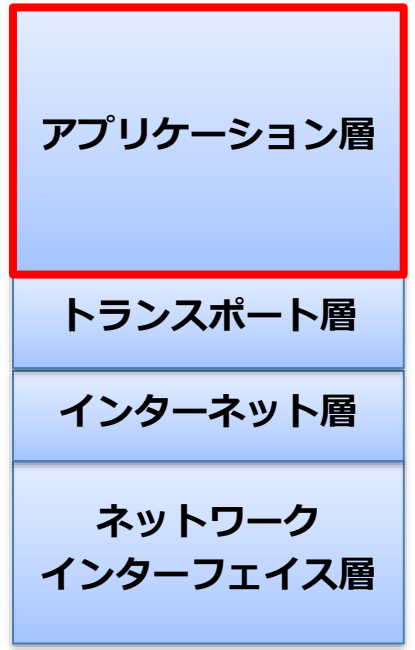
- UDPは、コネクションレス型の通信サービスを提供します。そのため、通信の信頼性は低くなりますが、処理は簡単なことから高速に動作します。
- UDPはこの特性により、以下のような用途に向いています。
  - 総パケット数が少ない通信
  - 動画や音声などのマルチメディア通信
  - （LANなど）特定のネットワークに限定したアプリケーションの通信
  - 同報性が必要となる通信（ブロードキャスト、マルチキャスト）
- UDPのヘッダは 8バイト長の固定で、非常にシンプルな構成となっています。



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)															

②アプリケーションプロトコル



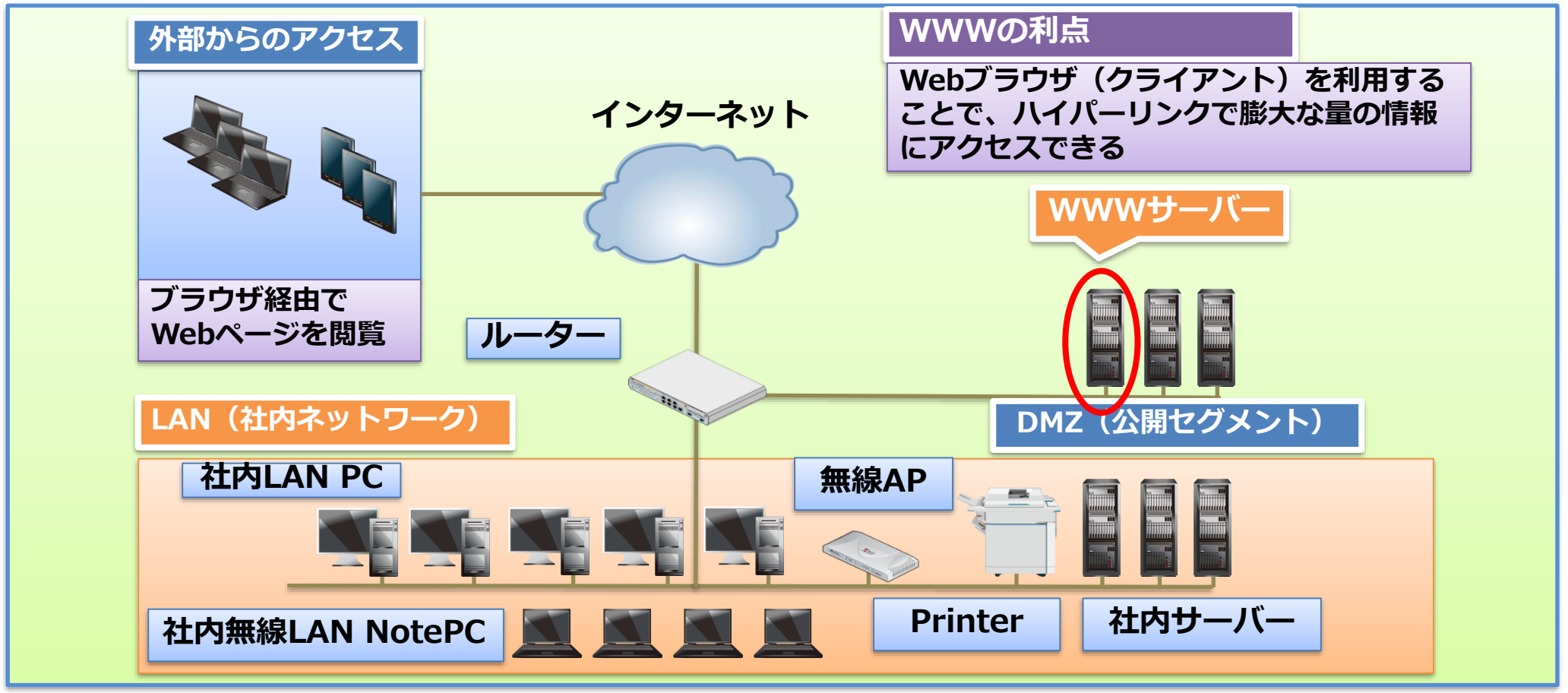
代表的なアプリケーション

- 下表は代表的なアプリケーションのウェルノウンポート番号です。ポート番号はIPアドレスと同様に、ICANN（The Internet Corporation for Assigned Names and Numbers）が管理しています。
- 表の「トランスポート層プロトコル」は、TCPとUDPのどちらを使用するプロトコルかを意味しますが、アプリケーションには、送信元ホスト/宛先ホストなどの違いでTCPとUDPを使い分けるプロトコルもあります。

ポート番号	アプリケーション	トランスポート層プロトコル
20	FTP（File Transfer Protocol）-Data	TCP
21	FTP （File Transfer Protocol）-Control	TCP
22	SSH（Secure Shell）	TCP
23	telnet	TCP
25	SMTP（Simple Mail Transfer Protocol）	TCP
53	DNS（Domain Name System）	TCP/UDP
67	DHCP（Dynamic Host Control Protocol） Server（bootps）	UDP
68	DHCP（Dynamic Host Control Protocol） Client（bootpc）	UDP
80	HTTP（Hyper Text Transfer Protocol ）	TCP
110	POP3（Post Office Protocol 3）	TCP
143	IMAP4（Internet Message Access Protocol 4）	TCP
161	SNMP（Simple Network Management Protocol）	UDP
162	SNMP（Simple Network Management Protocol）-trap	UDP
443	SSL/TLS（Secure Socket Layer/Transport Layer Security）	TCP

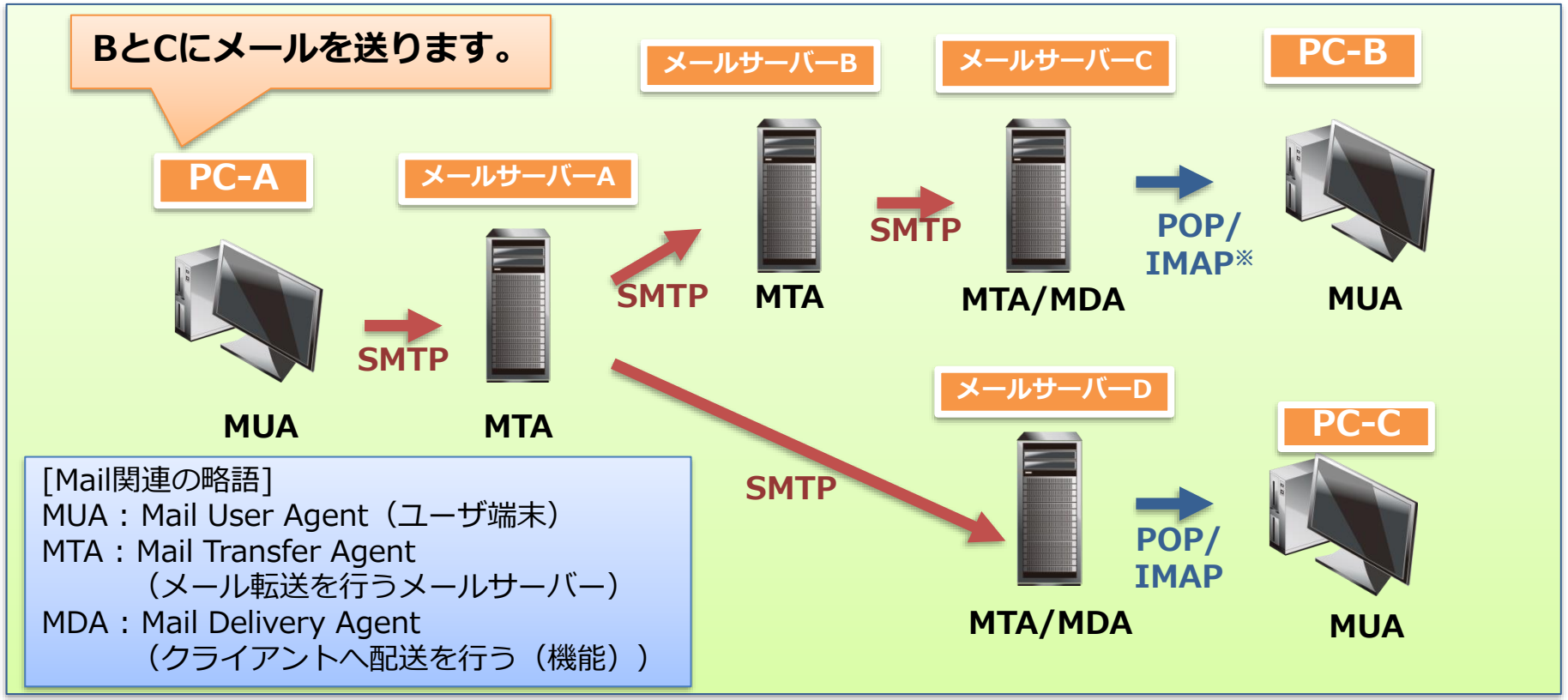
HTTP(Hyper Text Transfer Protocol)

- 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、一般的にはPOP3やIMAP4が使われます。

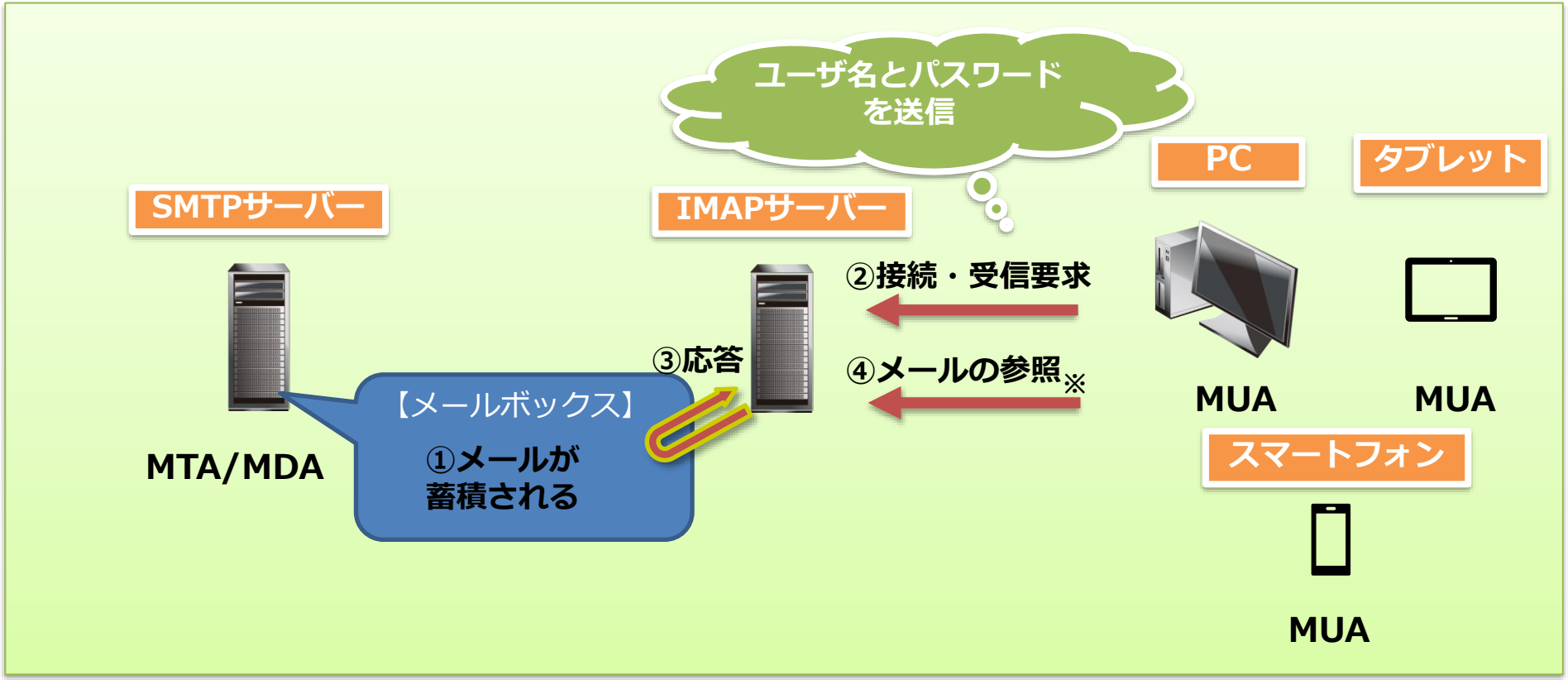
POP(Post Office Protocol)

- POPは電子メールを受信するためのプロトコルで、メールサーバーに蓄積された電子メールをMUAへダウンロードするときに用いられます。現在はバージョン3で一般にPOP3と呼ばれ、使用するポートはTCPの110番です。
- POPはメールをクライアント上で管理するため、ダウンロードしたメールはインターネットに接続していなくても参照することは可能ですが、複数デバイスでメールを参照することはできません。現在メールサーバー上で管理するIMAP（Internet Mail Access Protocol）が主流になりつつあります。

※ 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。

IMAP(Internet Message Access Protocol)

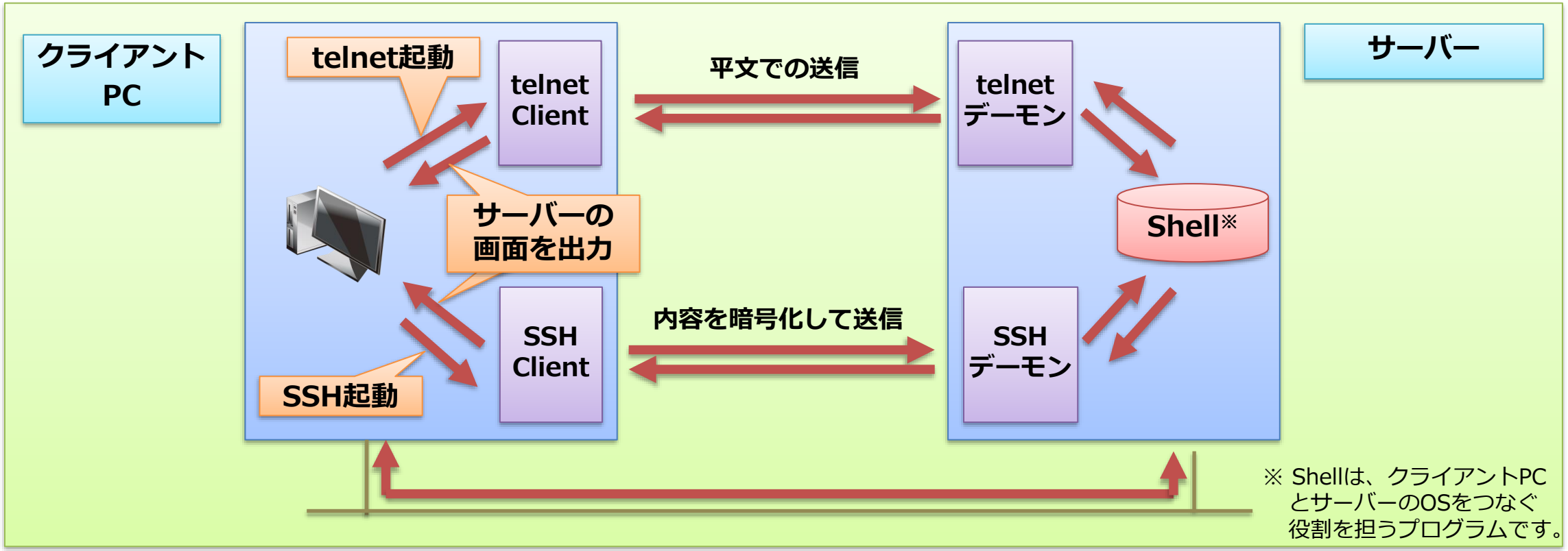
- IMAPは電子メールをメールサーバー上で管理するためのプロトコルです。利用者は受信メールをメールサーバーで管理し、クライアントのメールソフトに表示させます。メールサーバー上にフォルダを作成したり、メールの一覧だけを取得する、といったことができ、Webメールでも使用されています。現在は、バージョンは4で、使用するポートはTCPの143番です。
- IMAPは受信メールをメールサーバーのメールボックスに保存したまま管理できるため、複数のデバイス(パソコン、タブレット、スマートフォンなど)でメールを閲覧することができます。



※ IMAPはクライアントにメールをダウンロードせず、基本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。

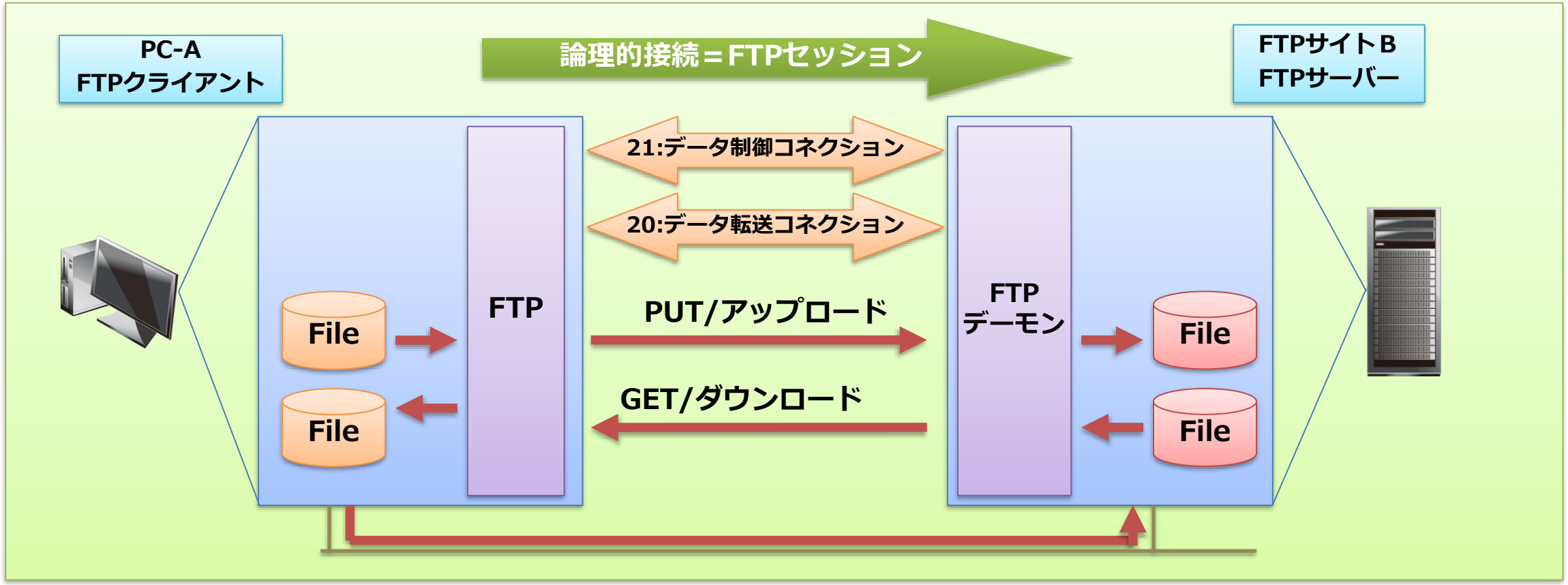
Telnet / SSH

- Telnet（Telecommunication Network）とは、ネットワーク上のサーバーなどにリモートアクセスするプロトコルです。パスワードを含む全文が平文でやり取りされるため、悪意のある第三者から簡単に読み取られてしまうという欠点があります。
- SSH（Secure Shell）もTelnetと同様に、リモートコンピュータと通信するためのプロトコルです。SSHは、認証部分を含めネットワーク上の通信が全て暗号化されるため、安全に通信することができます。
- TelnetとSSHは、主にネットワーク管理者がネットワーク経由でサーバーやネットワーク機器にログインし、機器の稼働状況の確認や必要な設定を行う際に利用します。



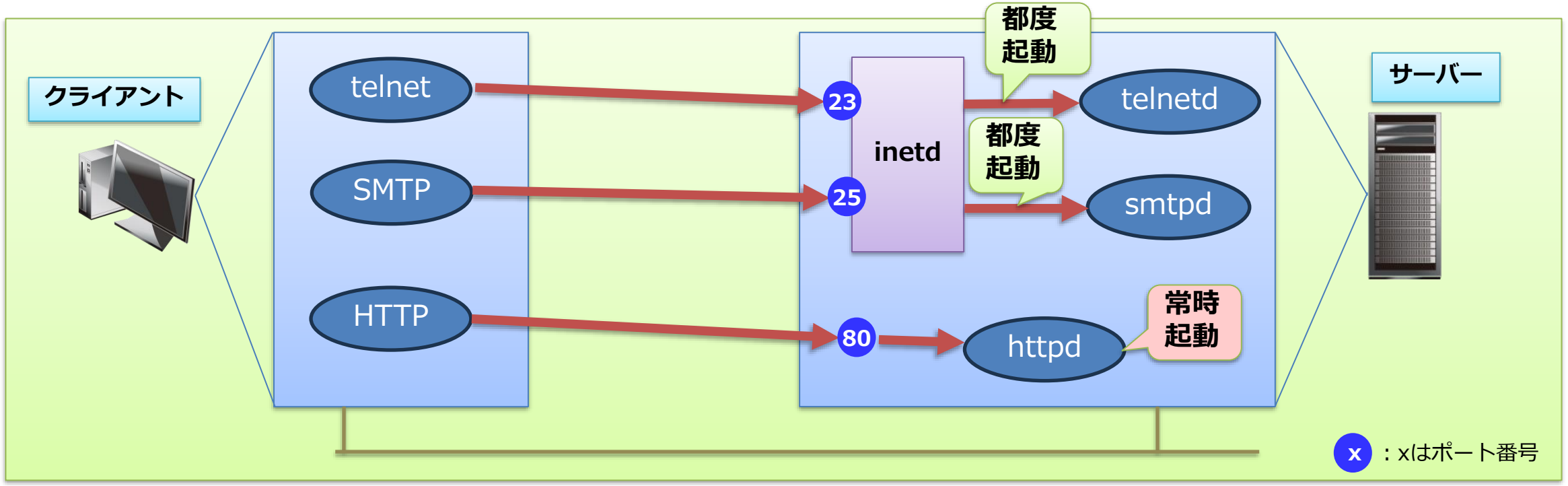
FTP(File Transfer Protocol)

- FTPはファイル転送を行うためのプロトコルで、クライアントからサーバーに対して、ファイルのダウンロード・アップロード、一覧表示やディレクトリ作成等の操作が可能です。
- FTPでは制御用コネクション（21番ポート）の確立後、ログインのためのユーザ名やパスワードの確認、転送するファイルや方法の指示を行います。その後データの転送用コネクション（20番ポート）を確立しデータ転送を行い、データの転送が終了するとコネクションは切断されます。コネクションを分離することで、緊急時のデータ転送の中止などの制御をリアルタイムに行うことが可能です。

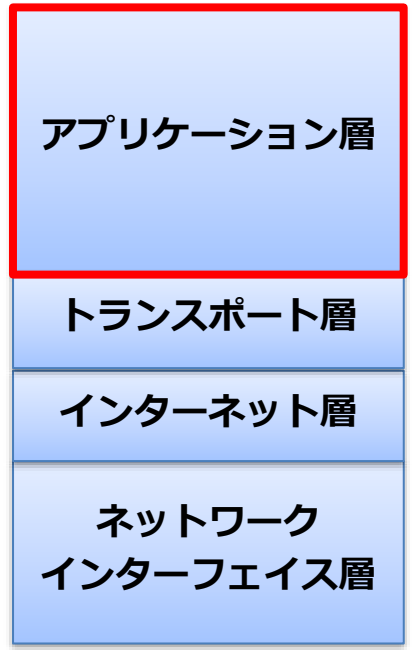


デーモンとは

- TCP/IPのアプリケーションには、バックグラウンドで実行され、ウェルノウンポート宛てのパケットを監視しコネクションを制御するプロセス (サーバープログラムとも呼ばれる) が存在します。FTPにはftpd（dはデーモン）、HTTPにはhttpd、SMTPにはsmtpdなどがあります。
- TCP/IP通信では、各アプリケーションのサーバープログラムが起動していないと通信を行うことができません。ただし、各アプリケーションのサーバープログラムが常時起動しているとメモリを消費するため、inetd（アイネットディー：Internet Daemon）から必要なサーバープログラムを起動します。
- inetdはウェルノウンポートを監視し、監視しているポートでTCPパケットもしくはUDPパケットを受信すると対応するアプリケーションのサーバープログラムを起動します（httpdなどレスポンスを重視するプログラムは、一般的にinetd経由でなく常時起動しています）。

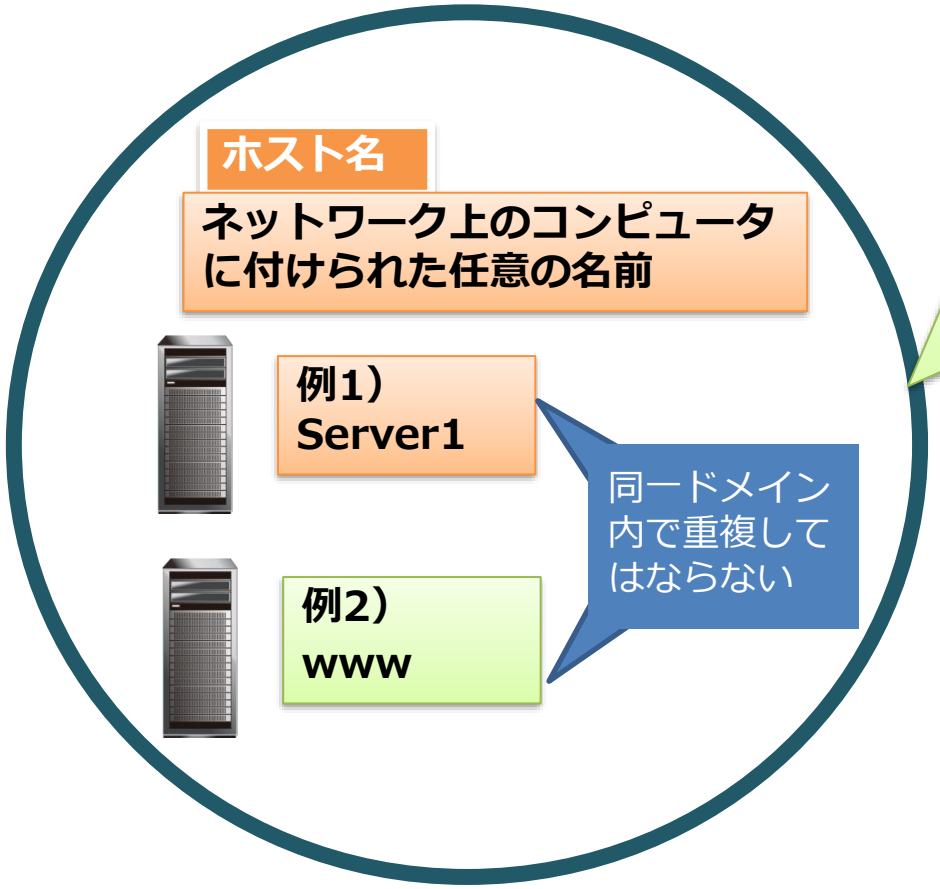


③インターネット通信を実現する
アプリケーションプロトコル



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

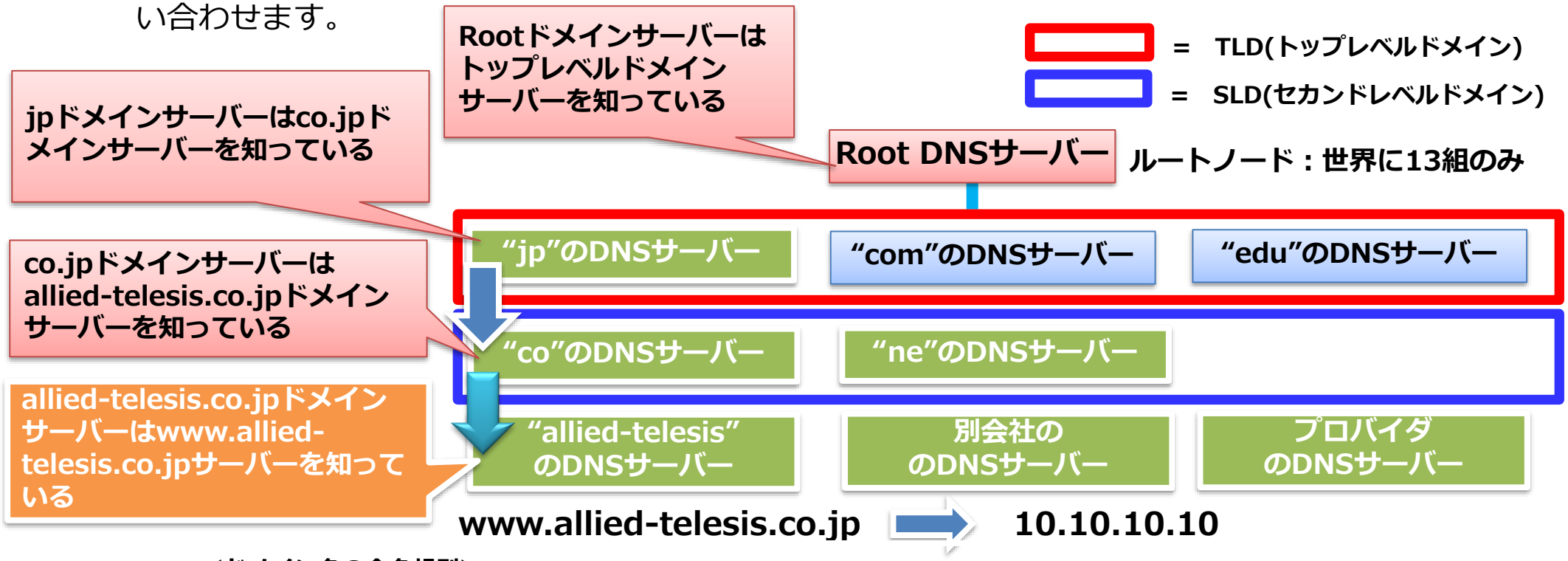
例）allied-telesis.co.jp

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。

DNSの動作

- DNSは、インターネットに存在する全ホストの名前解決をする必要があり、ツリー構造のデータベースで管理します。ドメイン名は、「.（ピリオド）」でいくつかの階層に区切られており、各階層ごとに担当するDNSサーバーが決まっています。
- 各階層に位置するDNSサーバーは、自身の管理するドメイン内情報とサブドメインのDNSサーバー名のみしか知らないため、自身の下位ドメイン（サブドメイン）のDNSサーバーに対して、当該ホストのIPアドレスを問い合わせます。



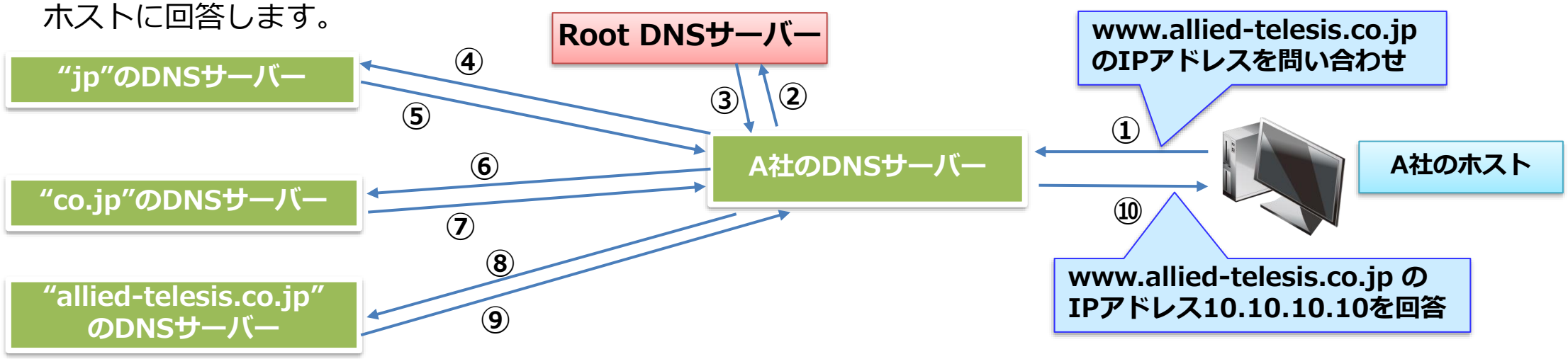
＜ドメイン名の命名規則＞

1. 組織種別（トップレベルドメイン（TLD）、米国）：edu：学術組織、com：企業、gov：政府機関、org：社団法人・財団法人など、net：ネットワークサービス提供組織
2. 組織種別（セカンドレベルドメイン（SLD）、日本）：ac：学術組織、co：企業、go：政府機関、or：社団法人・財団法人など、ne：ネットワークサービス提供組織、gr：任意団体・個人、ad：ネットワーク管理組織

DNSの動作

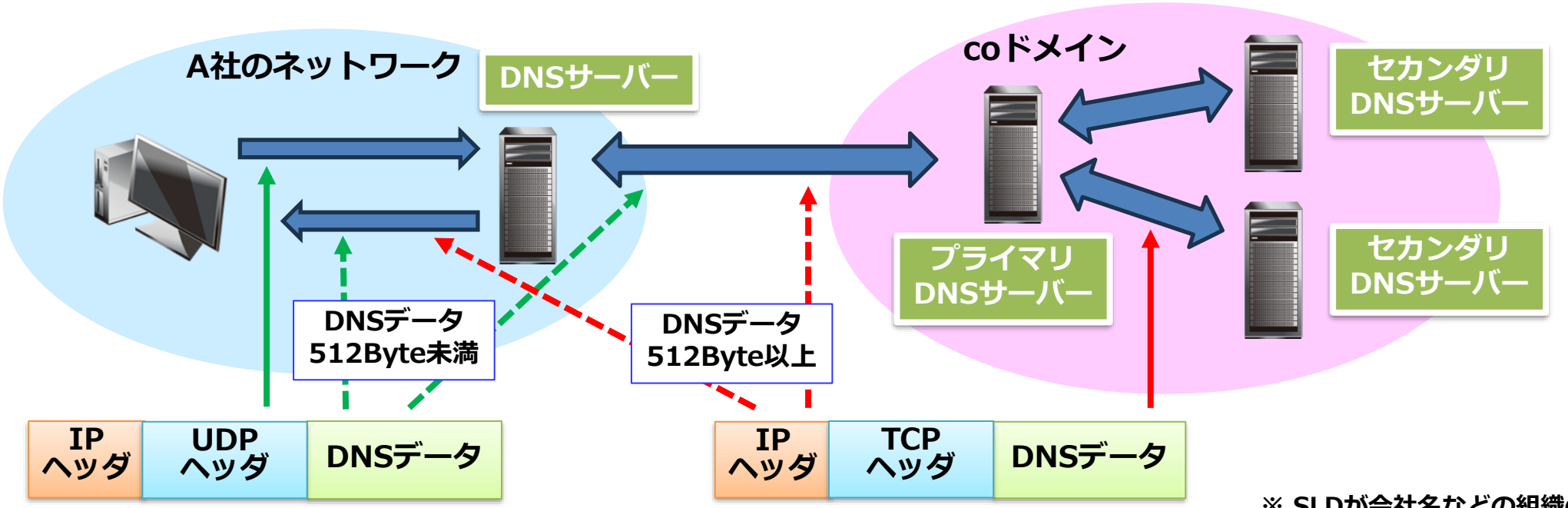
- DNSの問い合わせに対する処理の流れは以下になります。以下は、A社のホストが www.allied-telesis.co.jp のIPアドレスを取得する流れになります。
  ①A社のホストは、自社のDNSサーバーへ www.allied-telesis.co.jp のIPアドレスを問い合わせ
  ②A社のDNSサーバーは、①の情報を持っていないため、Root DNSサーバーへ問い合わせ
  ③Root DNSサーバーは、”jp”のDNSサーバーのIPアドレスを回答
  ④A社のDNSサーバーは、”jp”のDNSサーバーへwww.allied-telesis.co.jp のIPアドレスを問い合わせ
  ⑤”jp”のDNSサーバーは、“co.jp”のDNSサーバーのIPアドレスを回答
  ⑥A社のDNSサーバーは、”co.jp”のDNSサーバーへwww.allied-telesis.co.jp のIPアドレスを問い合わせ
  ⑦”co.jp”のDNSサーバーは、“allied-telesis.co.jp”のDNSサーバーのIPアドレスを回答
  ⑧A社のDNSサーバーは、”allied-telesis.co.jp”のDNSサーバーへwww.allied-telesis.co.jp のIPアドレスを問い合わせ
  ⑨”allied-telesis.co.jp”のDNSサーバーは、www.allied-telesis.co.jp のIPアドレス 10.10.10.10 を回答
  ⑩A社のDNSサーバーは、A社のホストへIPアドレス 10.10.10.10 を回答

➢ A社のDNSサーバーには、同一の問い合わせを繰り返し行うことを防止するため、問い合わせ結果を一定時間記憶する（キャッシュする）仕組みがあります。キャッシュ内に情報が保存されている場合は、その情報を問い合わせホストに回答します。



DNSパケット

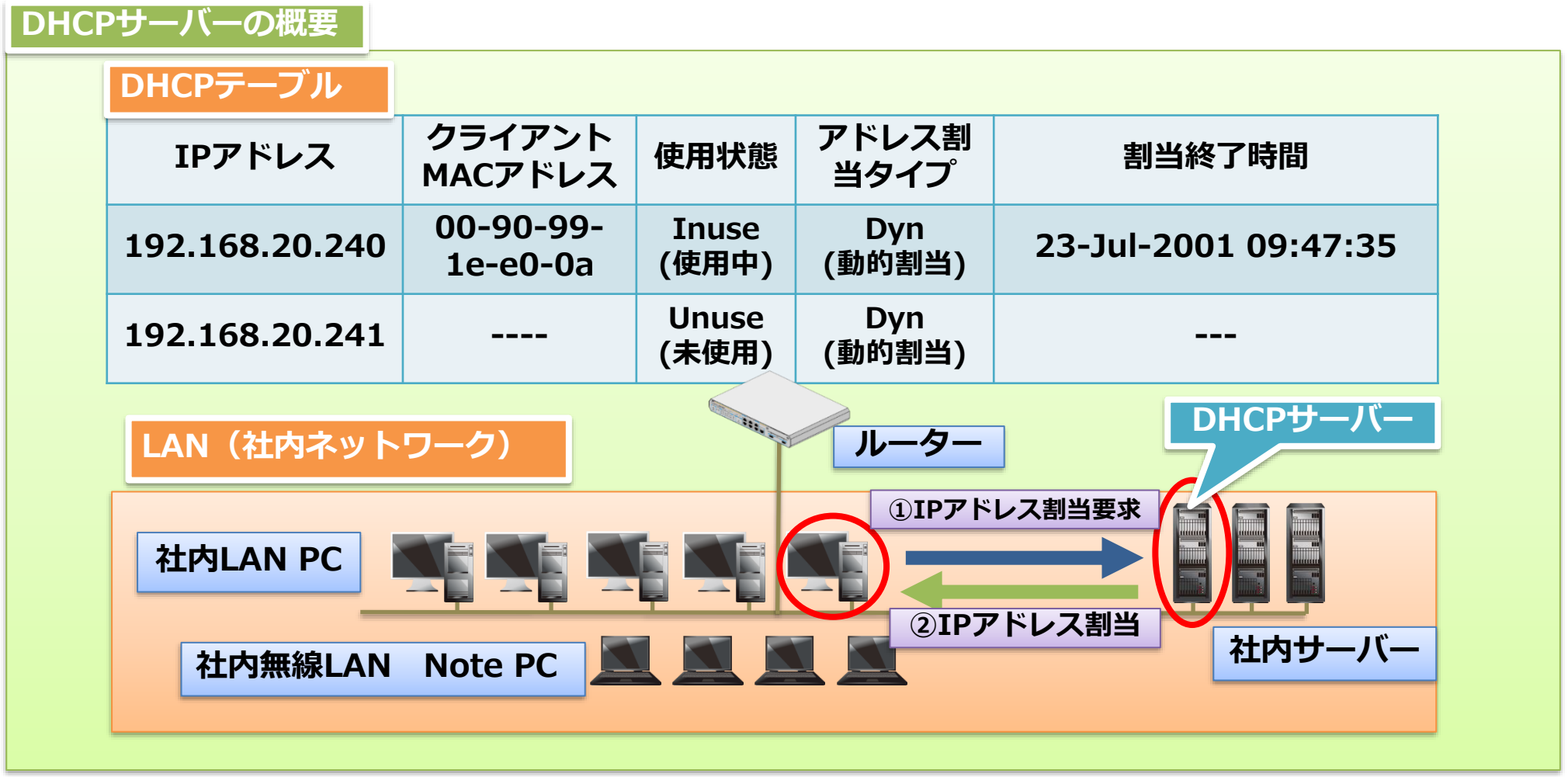
- 各ドメインのDNSサーバーには、プライマリDNSサーバーとセカンダリDNSサーバーが存在します。
  - プライマリDNSサーバー：ゾーン情報（ドメイン名とIPアドレスなどの対応付け情報）のマスターデータを管理
  - セカンダリDNSサーバー：バックアップとなるDNSサーバーでTLDやSLD※の各ドメインに1台以上存在し、ゾーン情報をプライマリDNSサーバーから受信
- 端末がDNSサーバーに行う問い合わせはUDP、DNSサーバー間（プライマリDNSサーバーとセカンダリDNSサーバー間）でゾーン情報を転送する場合や、512Byte以上のDNSデータをやりとりする通信はTCPを使用します（ポート番号はTCP・UDPとも53です）。
- DNSデータは最大512Byteの大きさで、DNSレコード（ゾーン情報の中の一行単位の詳細情報）が格納されます。DNSレコードは、ドメイン名、TTL、タイプおよびデータ（IPアドレスなど）などで構成されます。



※ SLDが会社名などの組織の場合は、各組織の方針に依存します。

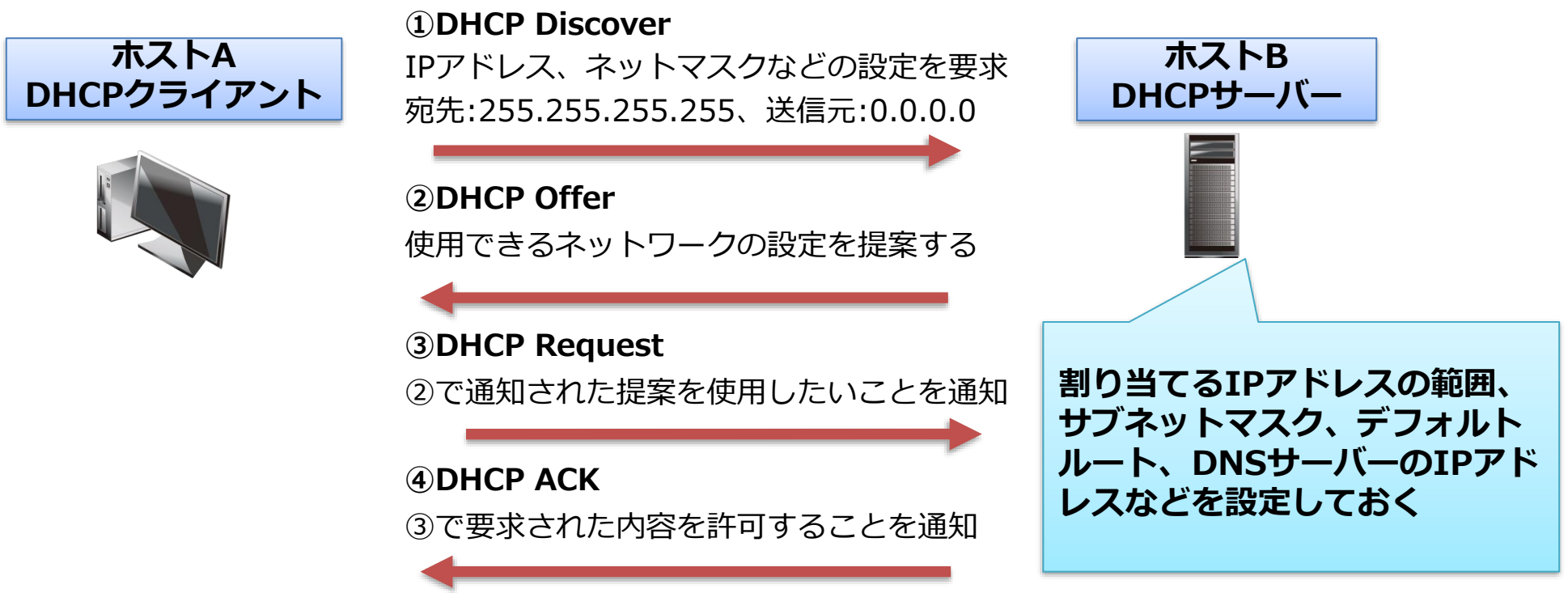
DHCP(Dynamic Host Configuration Protocol)

- DHCPは、ネットワークで使用するIPアドレスの貸与（リース）や、貸与したIPアドレスの一括管理を行うために利用されます。これにより、コンピュータを接続しただけでTCP/IPによる通信が可能になります。リースが確定すると、DHCPサーバーはDHCPテーブルにこの情報を格納します。



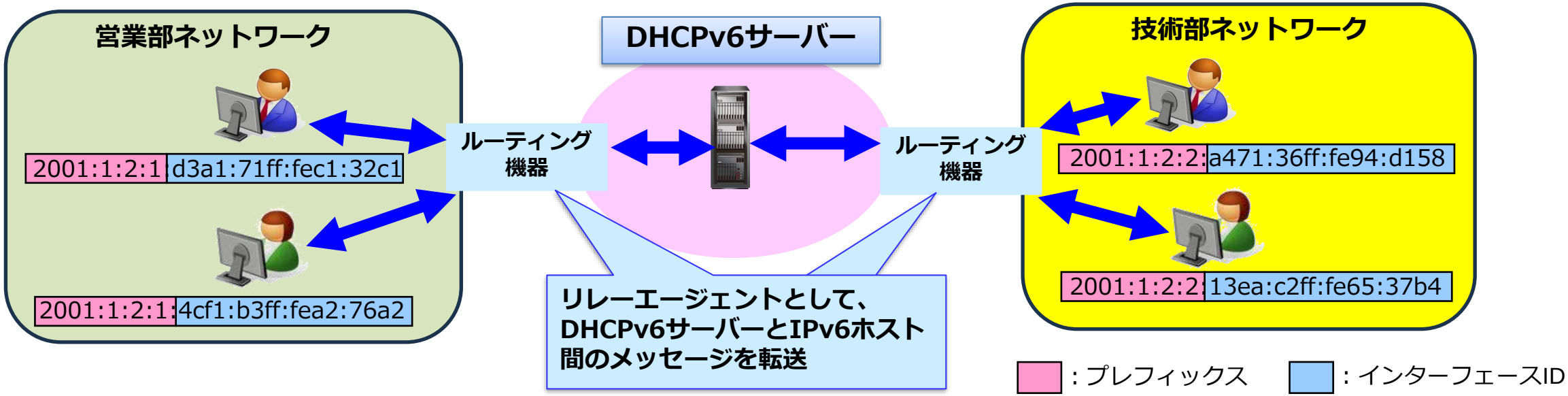
DHCPの動作

- DHCPサーバーには、配布するIPアドレス、サブネットマスク、デフォルトゲートウェイ、DNSサーバーのアドレスなどを必要に応じて設定します。DHCPクライアントとサーバーが別ネットワークの場合は、ルーティング機器のDHCPリレー機能でブロードキャストパケットを転送します。
- DHCPは以下のように動作します。
  - ①DHCP Discover：クライアントはブロードキャスト「255.255.255.255」でIPアドレスの割り当てを要求します。
  - ②DHCP Offer：DHCPサーバーは、送信元に候補IPアドレスを提案（Offer）します。
  - ③DHCP Request：クライアントは、候補IPアドレスの使用申請（Request）をブロードキャストします。
  - ④DHCP ACK：DHCPサーバーは、クライアントに承認（DHCP ACK）メッセージを送信します。

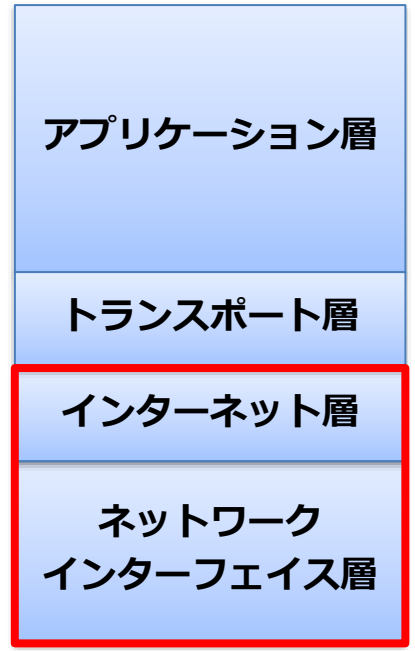


DHCPv6

- DHCPには、IPv4アドレスを付与するDHCPv4とIPv6アドレスを付与するDHCPv6が存在します。DHCPv6とDHCPv4の互換性はありません。DHCPという用語は一般的にDHCPv4を表します。
- DHCPv6サーバーから配布する情報には、IPv6アドレス、プレフィックス、デフォルトゲートウェイ、DNSサーバーのIPアドレスなどがあります。DHCPv6には、IPアドレス割り当て過程での認証機能などのセキュリティメカニズムがあり、ネットワークの不正利用を防止します。
- DHCPv6サーバーとアドレスを付与されるIPv6ホストは、同一ネットワーク上に存在する必要があります。ただ、ネットワーク毎にDHCPサーバーを設置するのは管理の負荷が高くなるため、実際のネットワークではルーティング機器にリレーエージェント機能の設定を行い、ホストとDHCPサーバーの間のメッセージを転送させます（これはDHCPv4サーバーとIPv4ホスト間も同様です。）

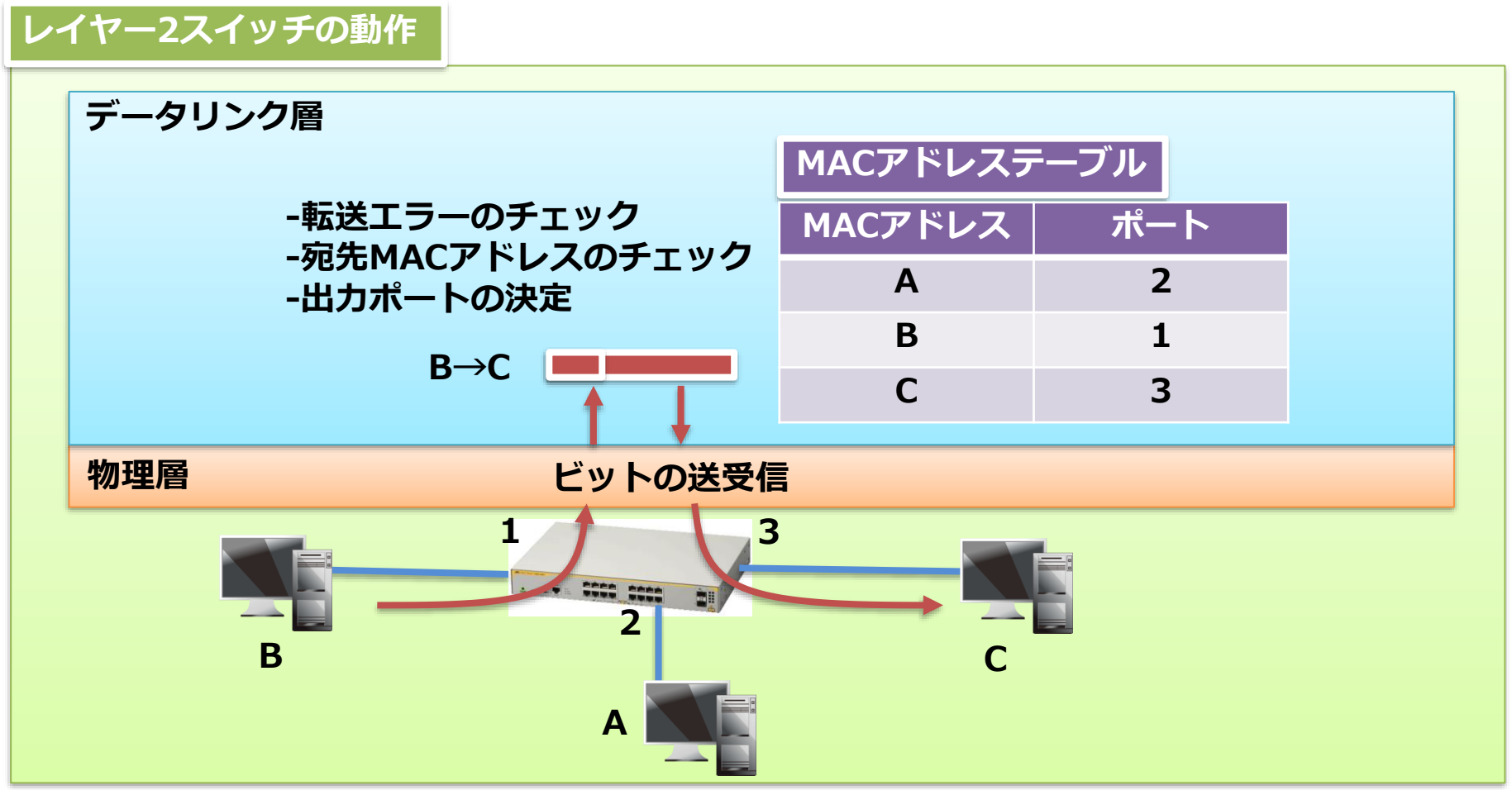


④通信機器におけるIPアドレス・アプリケーション



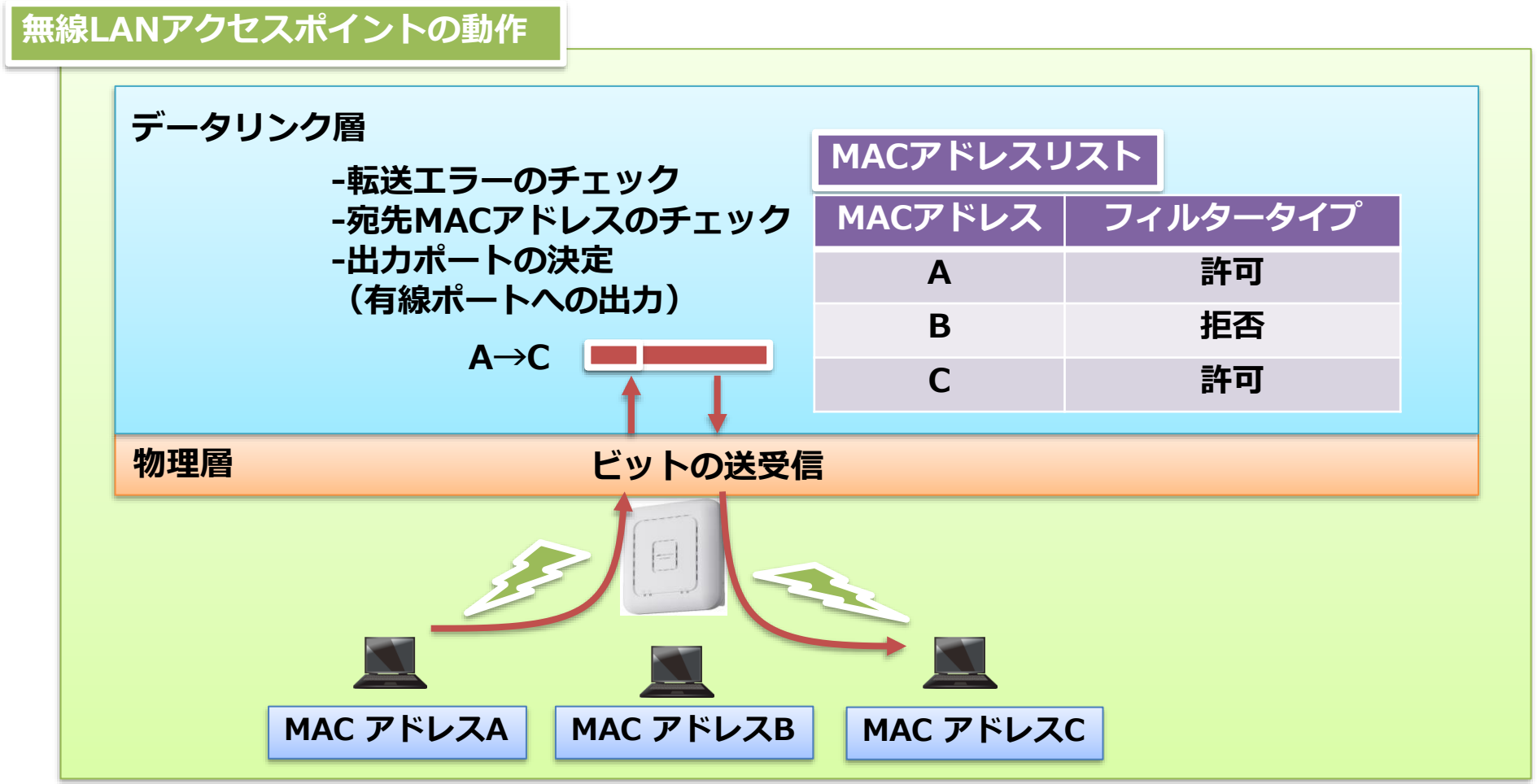
レイヤー2スイッチとIPアドレス

- 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。



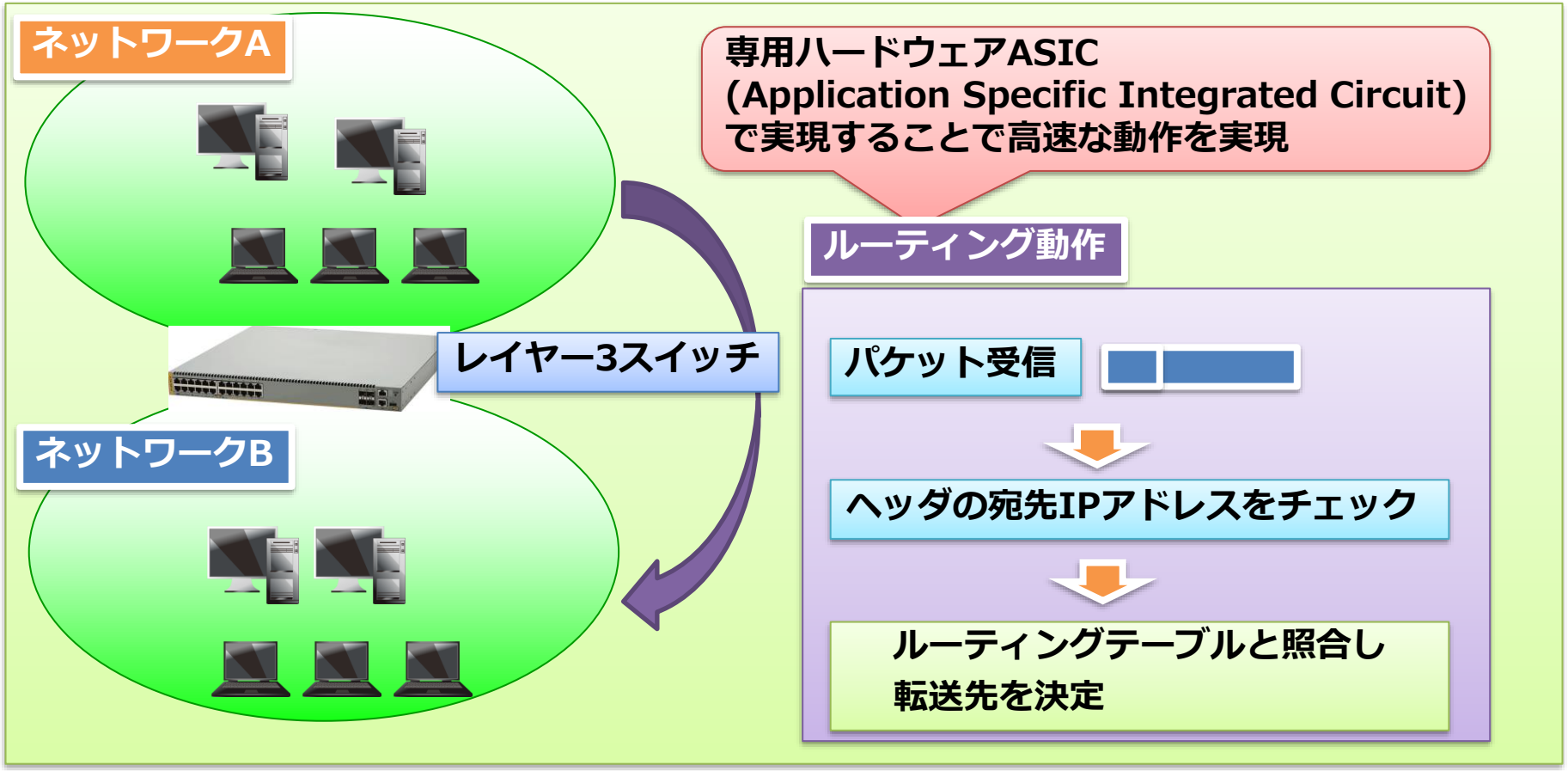
無線LANアクセスポイントとIPアドレス

- 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。



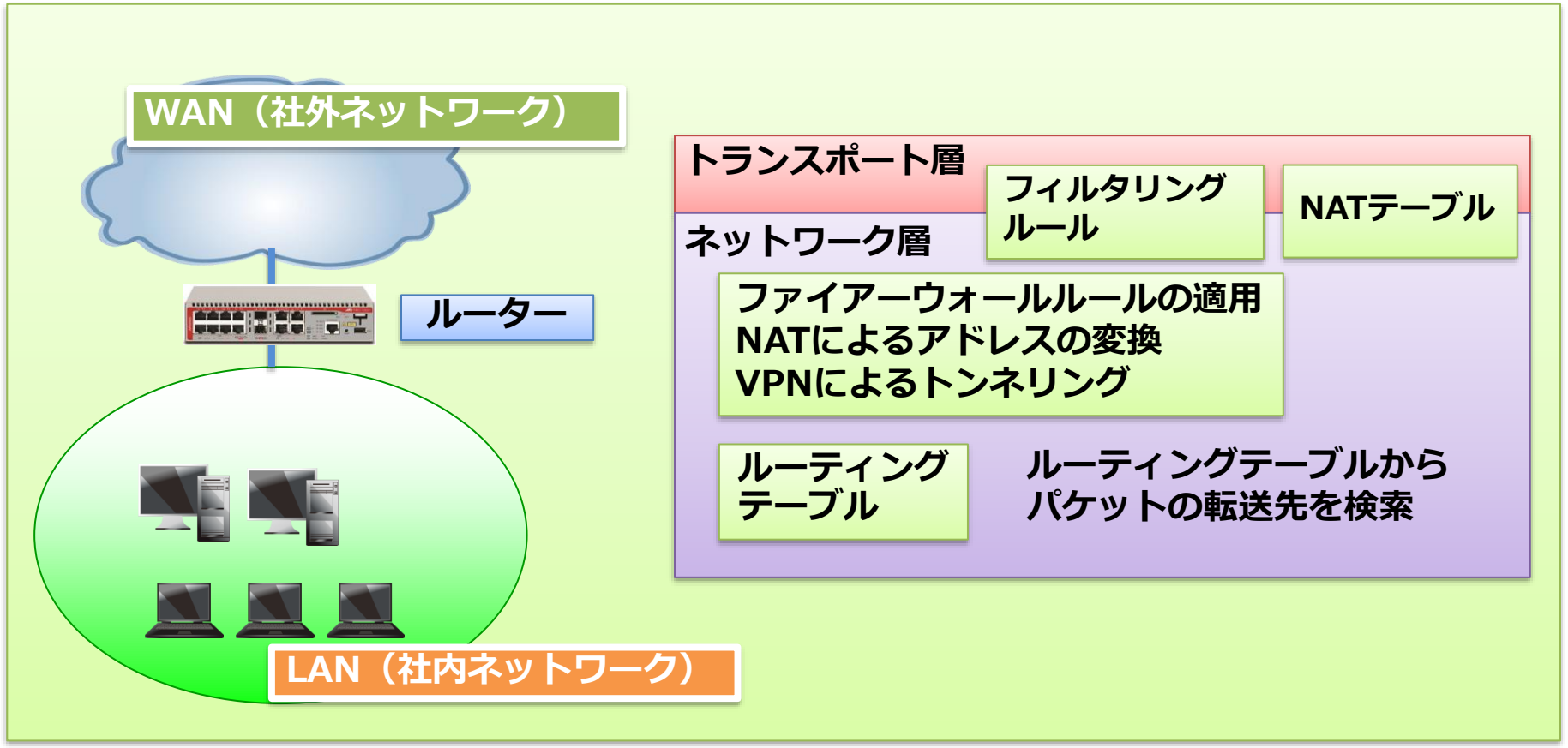
レイヤー3スイッチとIPアドレス

- 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。



通信機器とアプリケーションプロトコル

- 通信機器は主にインターネット層以下の機能を提供しますが、ネットワーク管理を効率良く行うため、いくつかのアプリケーションプロトコルを実装しています。
- 以下は、通信機器に実装されている主なアプリケーションプロトコルになります。

アプリケーションプロトコル	目的・機能
Telnet【サーバー機能 / クライアント機能】	ネットワーク経由でログインし、設定・管理を行う
SSH【サーバー機能 / クライアント機能】	
RADIUS(Remote Authentication Dial In User Service)【サーバー機能】	ネットワーク上のユーザーや機器を認証する
SNMP(Simple Network Management Protocol)	通信機器を監視装置で管理する
Syslog(System Logging Protocol)	ログメッセージをネットワーク上で転送する
DHCP【サーバー機能 / クライアント機能】	ネットワーク上の機器にIPアドレスを付与する
NTP(Network Time Protocol)【サーバー機能 / クライアント機能】	ネットワーク上の機器間で時刻同期を行う

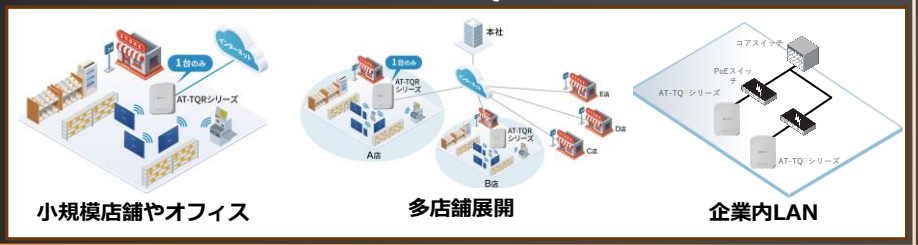
Appendix：各種販促情報のご案内など

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)

AT-TQ6702 GEN2-R

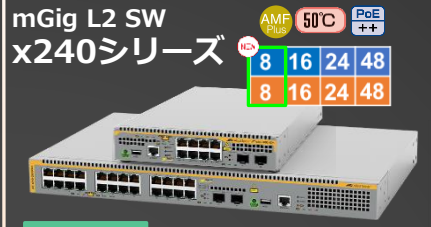
- **Wi-Fi6とVPNルーターの機能を1台で提供**
- **エンタープライズ向け機能を搭載**
  - FirewallやダイナミックENAT、IPsec、VAP、Captive Portal、WPA3など各種エンタープライズ向け機能を搭載
- **AMF Plusによる一元管理に対応**
- **様々なネットワークに適用可能**
  - **無線LANルータとして**、小規模店舗/ブランチオフィスや多店舗展開ネットワーク、**通常の無線LAN APとして**、企業内LANなど様々なネットワークをAT-TQ6702 GEN2-Rで構成可能



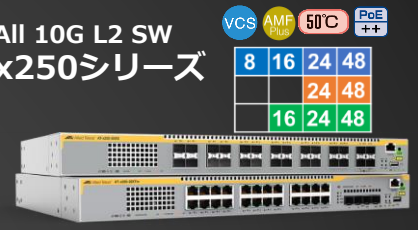
新製品のご紹介（エッジスイッチシリーズ）

Copper Model Lineup
PoE Model Lineup
Fiber Model Lineup

mGig L2 SW
x240シリーズ



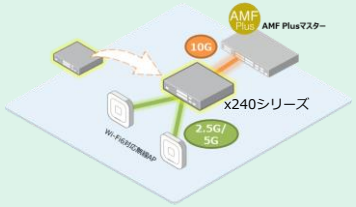
All 10G L2 SW
x250シリーズ



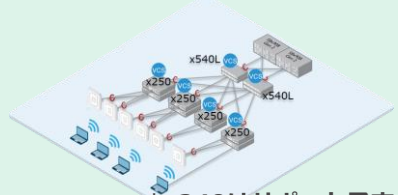
All 10G L3 SW
x540Lシリーズ

特長

Cat5e対応 mGig サポート
～配線の入れ替えなしで高速通信～

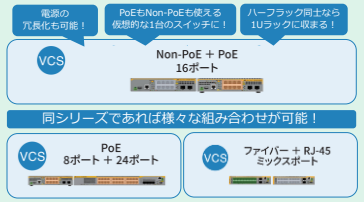


スタックサポート
～ ネットワークのエッジにまで冗長性を～



*x240はサポート予定

環境に応じた拡張性
～組み合わせ自由なスタック構成～

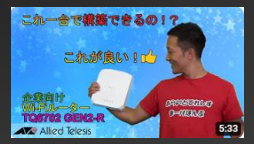


Allied Labのご紹介

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！

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。

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。