

【完全理解】

IPアドレスと通信の仕組み

- 世界中から端末を特定する仕組み
- 宛先の経路を取得するルーティング技術
(サブネットマスクとデフォルトゲートウェイの役割)
- EthernetにおけるMACアドレスとの役割分担

全体目次

1. IPアドレス概要
2. IPアドレスの種類と割り当て
3. ルーティングの仕組み
4. EthernetとMACアドレス

1. IPアドレス概要

1-1. RFCとは？

1-2. TCP/IPとは？

1-3. プロトコルスタック

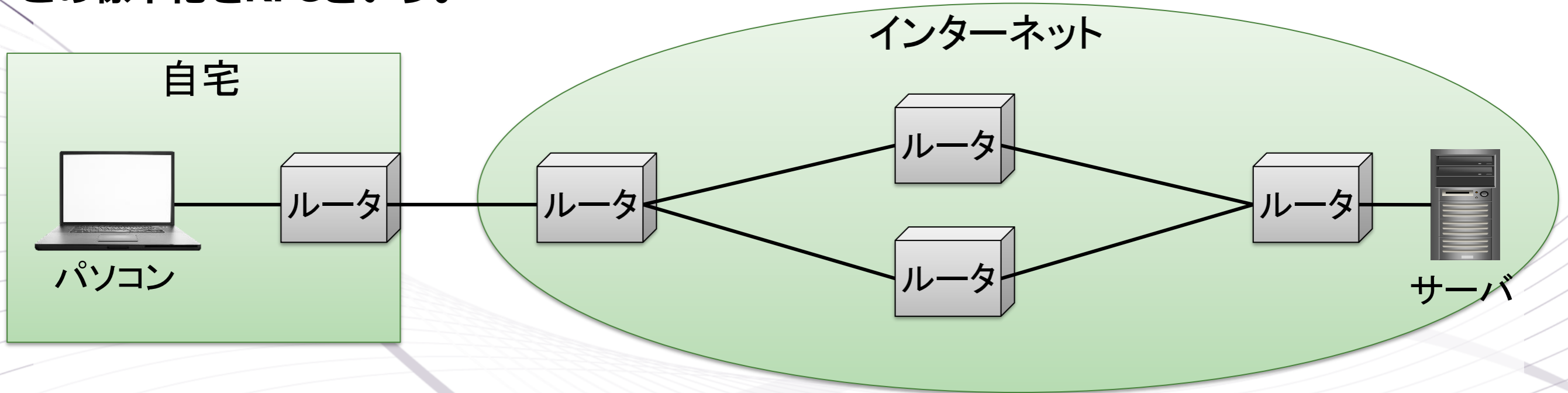
1-4. パケットデータ（キャプチャ）

1-5. 「IPv4」と「IPv6」

1-6. IPアドレスのデータフォーマット

1-1. RFCとは？

インターネット通信に関わる全ての機器は予め規定された技術でデータを扱うことが必要。
そのため、インターネット技術の標準化（取り決め）が行われている。
この標準化をRFCという。

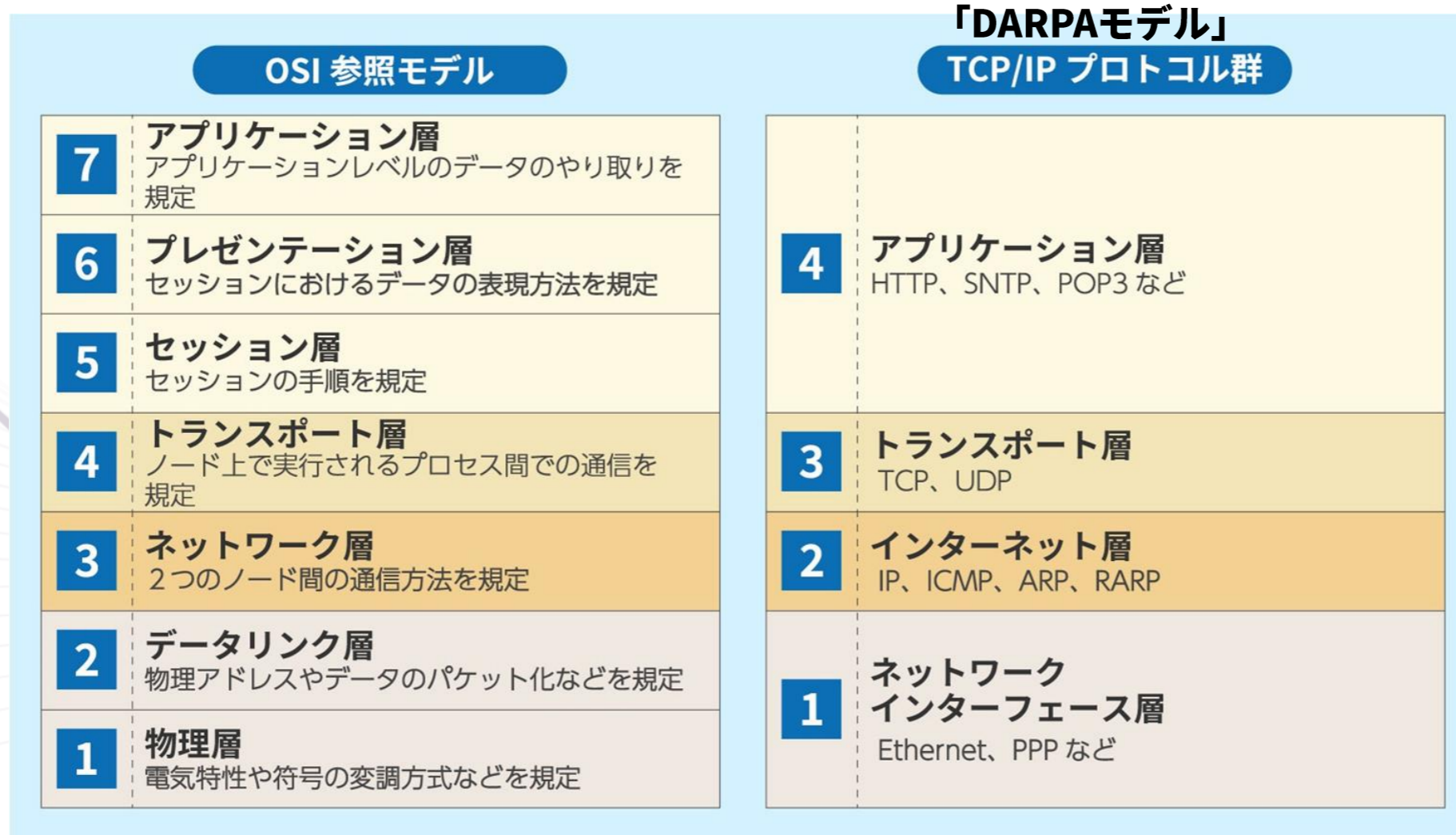


- ・ 標準化を行う団体：IETF (Internet Engineering Task Force)
- ・ 標準化された規定：RFC (Request for Comments)
 - 1) IP : RFC791(IPv4), RFC8200(IPv6) 2017年7月公開 (RFC2460廃止)
 - 2) TCP : RFC9293 2022年8月公開 (RFC793廃止)

1-2. TCP/IPとは？

- **TCP/IP** インターネットで通信を行うための規定
 - ① **IP** : インターネット上の住所を表す役割
 - ② **TCP** : 通信路の状態に応じて効率的かつ確実にデータを届ける役割
- **UDP/IP**
 - ③ **UDP** : 届けるだけで通信制御をおこなわない。

1-3. プロトコルスタック



- 送受信端末で各層の利用する規定を一致させる
- 各層間の依存関係がない。各々の層毎に利用する規定を決める

【出典：（ビジネス+IT）OSI参照モデルとTCP/IPの階層の違いとは？】

<https://www.sbbit.jp/article/cont1/12099>

1-4. パケットキャプチャ (Wireshark)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.7	157.7.107.210	TCP	66	53275 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.000364	192.168.1.7	157.7.107.210	TCP	66	59662 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3	0.015081	157.7.107.210	192.168.1.7	TCP	66	80 → 53275 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1414 SACK_PERM=1 WS=128
4	0.015193	192.168.1.7	157.7.107.210	TCP	54	53275 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
5	0.016168	192.168.1.7	157.7.107.210	HTTP	614	GET / HTTP/1.1
6	0.016390	157.7.107.210	192.168.1.7	TCP	66	80 → 59662 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1414 SACK_PERM=1 WS=128
7	0.016462	192.168.1.7	157.7.107.210	TCP	54	59662 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
8	0.031443	157.7.107.210	192.168.1.7	TCP	60	80 → 53275 [ACK] Seq=1 Ack=561 Win=30336 Len=0
9	0.542488	157.7.107.210	192.168.1.7	TCP	392	80 → 53275 [PSH, ACK] Seq=1 Ack=561 Win=30336 Len=338 [TCP segment of a reassembled PDU]
10	0.543525	157.7.107.210	192.168.1.7	TCP	2882	80 → 53275 [ACK] Seq=339 Ack=561 Win=30336 Len=2828 [TCP segment of a reassembled PDU]
11	0.543622	192.168.1.7	157.7.107.210	TCP	54	53275 → 80 [ACK] Seq=561 Ack=3167 Win=131328 Len=0
12	0.544684	157.7.107.210	192.168.1.7	TCP	8538	80 → 53275 [ACK] Seq=3167 Ack=561 Win=30336 Len=8484 [TCP segment of a reassembled PDU]

- > Frame 5: 614 bytes on wire (4912 bits), 614 bytes captured (4912 bits) on interface \Device\NPF_{EE298557-9F26-440F-870F-072F5825E194}, id 0
- > Ethernet II, Src: Tp-LinkT 09:d6:7d (28:ee:52:09:d6:7d), Dst: Mitsubis 86:d6:65 (10:4b:46:86:d6:65)
- > Internet Protocol Version 4, Src: 192.168.1.7, Dst: 157.7.107.210
- > Transmission Control Protocol, Src Port: 53275, Dst Port: 80, Seq: 1, Ack: 1, Len: 560
- > Hypertext Transfer Protocol

Ethernet: 14Byte

IP: 20Byte

TCP: 20Byte

0000	10 4b 46 86 d6 65 28 ee 52 09 d6 7d 08 00 45 00	·KF··e(· R··}··E·
0010	02 58 15 30 40 00 80 06 18 e7 c0 a8 01 07 9d 07	·X·0@··· ······
0020	6b d2 d0 1b 00 50 38 57 b9 9e 16 b5 52 a1 50 18	k··· P8W ····R·P·
0030	02 01 e5 e0 00 00 47 45 54 20 2f 20 48 54 50	······GE T / HTTP
0040	2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 6d 61 6e 61	/1.1·Ho st: mana
0050	6b 61 6e 2e 6e 65 74 0d 0a 43 6f 6e 6e 65 63 74	kan.net· ·Connect
0060	69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d	ion: kee p-alive·
0070	0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72	·Upgrade ·Insecur
0080	65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55	e·Reques ts: 1·U
0090	73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c	ser·Agen t: Mozil

1-5. 「IPv4」と「IPv6」

アドレスに用いるBit数の差

- IPv4 **32Bit**で識別する。 → 2の32乗なので「4,294,967,296（約4億3千万）」

10進表記

192 . 168 . 1 . 7

10進数表記で
8bitを0~255で表す

2進表記

128 32
64 16 8 4 2 1
1100 0000
8bit

1010 1000
8bit

0000 0001
8bit

0000 0111
8bit

8bit × 4
合計 **32Bit**

- IPv6 **128Bit**で識別する → 2の128乗なので「3.4×10の32乗（約340潤?）」

16進表記

2 0 0 1 : 0 D b 8 : (全てゼロは省略可)

16進数表記で
4bitを0~fで表す

2進表記

8 4 2 1
0010 0000 0000 0001 0000 1101 1011 1000 0000 0000 0000 0000 000 ・・・ (省略)
4bit 4bit 4bit 4bit 4bit 4bit 4bit 4bit 4bit 4bit 4bit 4bit

合計 **128Bit**

(340282366920938463463374607431768211456)

1-6. IPデータフォーマット (規定RFCより抜粋)

- IPv4 RFC791

0				1				2				3											
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1		
Version				IHL				Type of Service				Total Length											
								Identification				Flags				Fragment Offset							
				Time to Live								Protocol								Header Checksum			
								送信IPv4アドレス				Source Address				32bit							
								受信IPv4アドレス				Destination Address				32bit							
								Options								Padding							

基本サイズはこの**20バイト**
(1行は32Bitなので4バイト)

オプション部分になり、
必要なオプション情報により
サイズは可変

- IPv6 RFC8200

Version				Traffic Class				Flow Label															
								Payload Length								Next Header				Hop Limit			
								Source Address				送信IPv6アドレス				32bit * 4line = 128 bit							
								Destination Address				受信IPv6アドレス				32bit * 4line = 128 bit							

基本サイズはこの**40バイト**
(1行は32Bitなので4バイト)

2. IPアドレスの種類と割り当て

2-1. クラスとCIDR

2-2. IPアドレスの管理組織と割り当て

2-3. グローバルとプライベート

2-4. プライベートIPアドレスでのネット通信

2-1. クラスとCIDR



- クラス：以下の表に示すとおり、予め決められた大きさの単位でネットワークを構築する → **無駄が多くなる**

クラス	アドレス範囲	ネットワーク部	端末数
クラスA	0.0.0.0 ~ 127.255.255.255	8 Bit	約1600万個
クラスB	128.0.0.0 ~ 191.255.255.255	16 Bit	約65000個
クラスC	192.0.0.0 ~ 233.255.255.255	24 Bit	254個
クラスD/E	224.0.0.0 ~ 255.255.255.255	(マルチキャスト及び予約用)	-

- CIDR (Classless Inter-Domain Routing) : クラスに関係なく、自由な範囲で利用する **普通に、こちらが利用されている**

サブネットマスクを設定し、ネットワーク部とホスト部の区切りを明確にして利用する

例) 1.0.16.0 / 20
 192.168.10.0 / 23

2-2. IPアドレスの管理組織と割り当て

- ・IPアドレスは世界中で重複しないよう厳しく管理
- ・日本では次の順番で払い出されて管理されており、場所を特定できるようになっている。
IANA → APNIC → JPNIC → ISP → エンドユーザ

IPアドレス管理組織

地域	管理組織	記事
世界	IANA (Internet Assigned Numbers Authority)	世界レベルで管理
アジア	APNIC (Asia-Pacific Network Information Centre)	世界を5地域に分けて管理
日本	JPNIC (Japan Network Information Center)	国レベルで管理

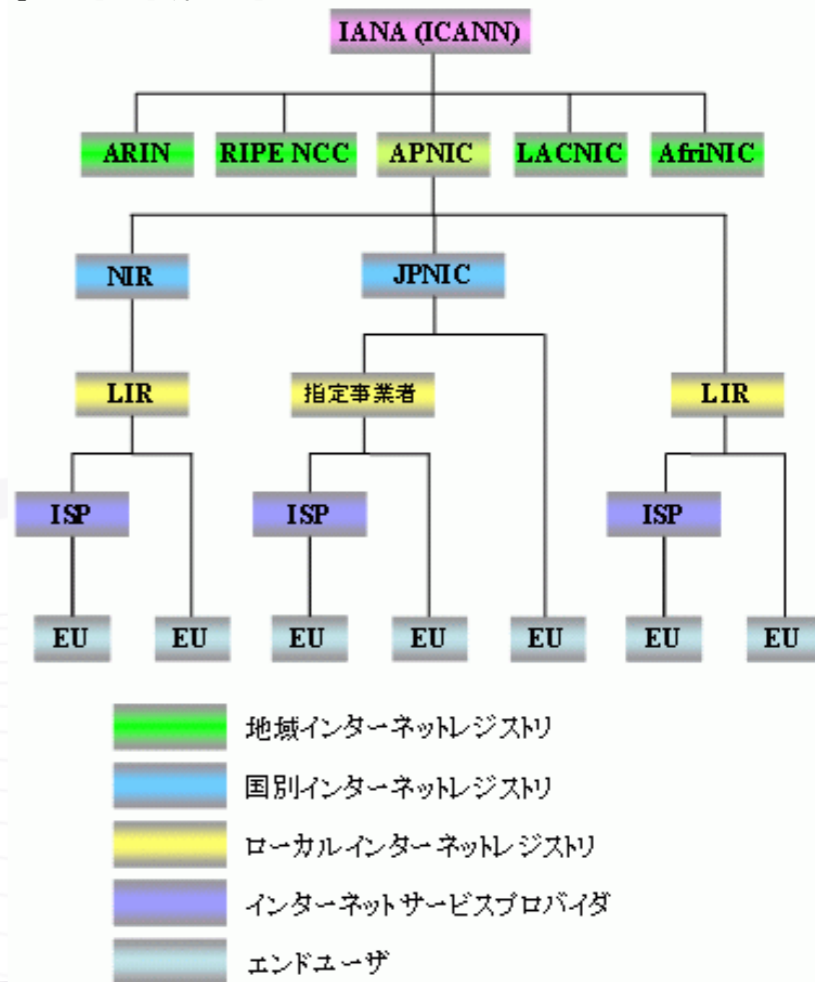
日本への割り当て

<https://ipv4.fetus.jp/jp> より抜粋

CIDR	IPアドレス	割り振り日	レジストリ
1.0.16.0/20	1.0.16.0 - 1.0.31.255	2011/04/12	APNIC
1.0.64.0/18	1.0.64.0 - 1.0.127.255	2011/04/12	APNIC
1.1.64.0/18	1.1.64.0 - 1.1.127.255	2011/04/12	APNIC
1.5.0.0/16	1.5.0.0 - 1.5.255.255	2011/04/01	APNIC
1.21.0.0/18	1.21.0.0 - 1.21.63.255	2010/06/16	APNIC
1.21.64.0/19	1.21.64.0 - 1.21.95.255	2010/06/16	APNIC
1.21.96.0/20	1.21.96.0 - 1.21.111.255	2010/06/16	APNIC
1.21.112.0/20	1.21.112.0 - 1.21.127.255	2010/06/16	APNIC
1.21.128.0/20	1.21.128.0 - 1.21.143.255	2010/06/16	APNIC

日本 : 190,438,656個
・全アドレス空間の4.43%
・予約除くと5.14%

管理組織の構造



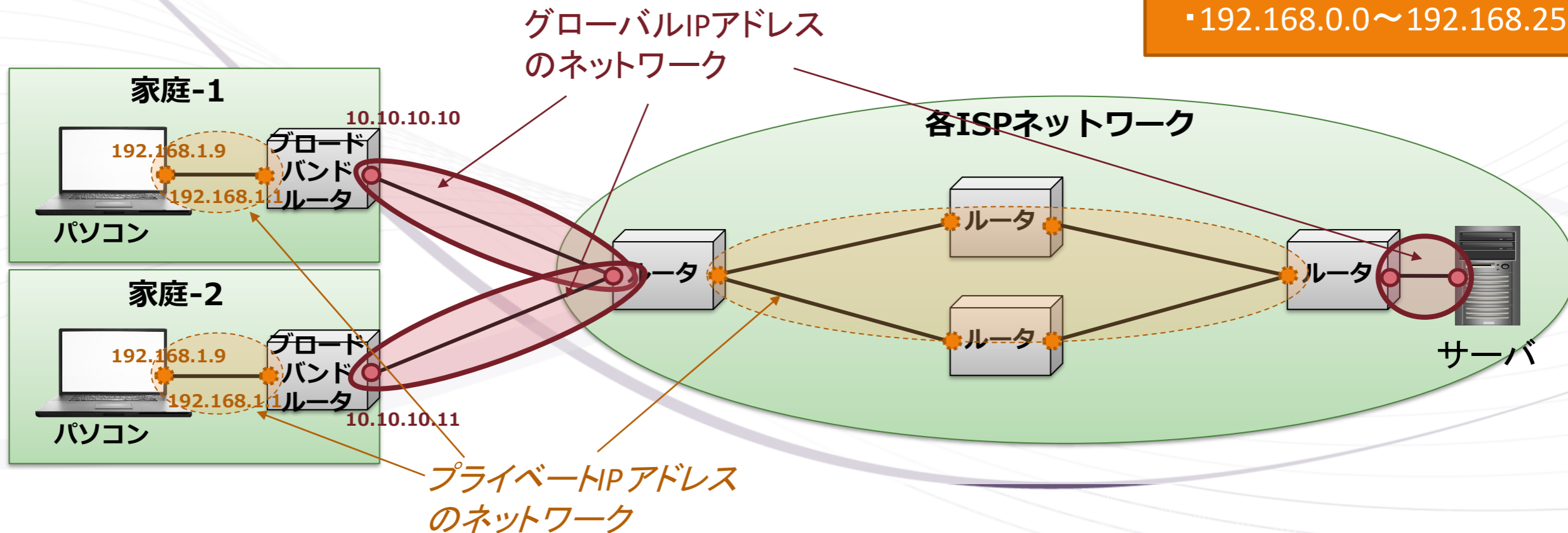
<https://www.nic.ad.jp/ja/ip/admin.html>

2-3. グローバルとプライベートIPアドレス

- **グローバルIPアドレス**
世界で唯一のアドレス（世界中から特定できるので、ネット通信するために利用）
- **プライベートIPアドレス**
各家庭や企業内などのネットワークで繰り返し利用されるアドレス。
（世界中から特定できないが、該当のネットワーク内では重複しないでユニーク）

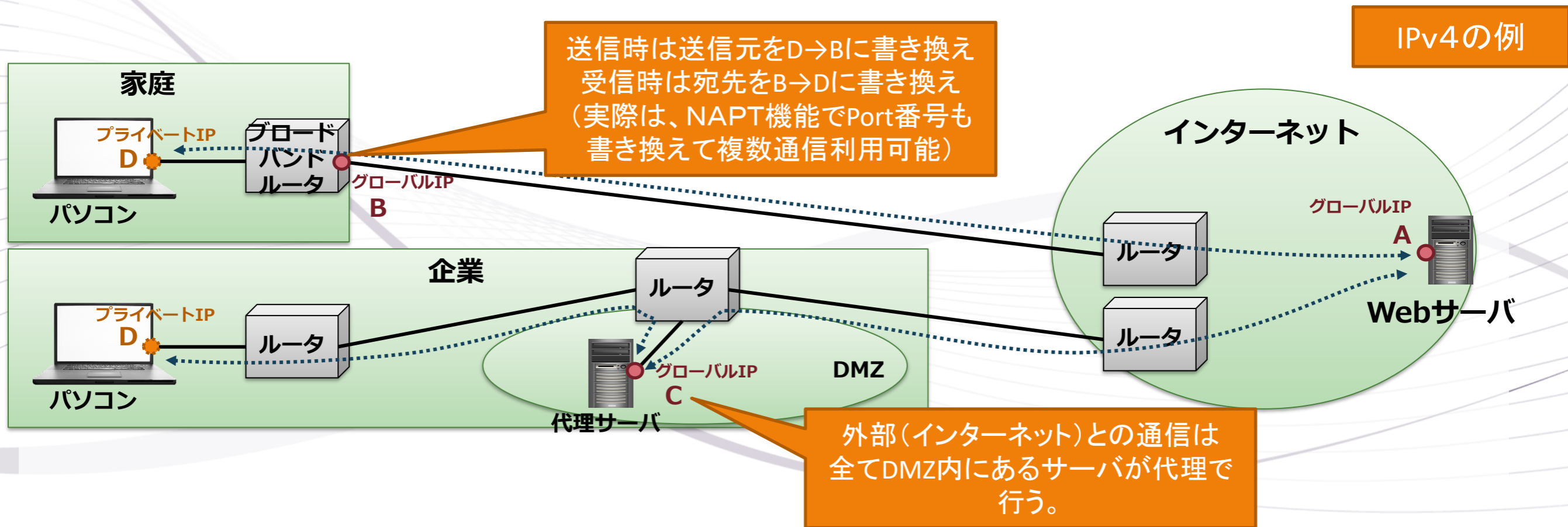
【プライベートIPアドレス範囲】

- ・10.0.0.0～10.255.255.255
- ・172.16.0.0～172.31.255.255
- ・192.168.0.0～192.168.255.255



2-4. プライベートIPアドレスでのネット利用

- 各家庭でのプライベートIP利用
ブロードバンドルータにて、グローバルIPアドレスとプライベートIPアドレスを置き換えて通信
- 各企業でのプライベートIP利用
DMZ内のProxyサーバが外部との通信を中継し通信を行う。



3. ルーティングの仕組み

3-1. ルーティングとは

3-2. サブネットマスクとは

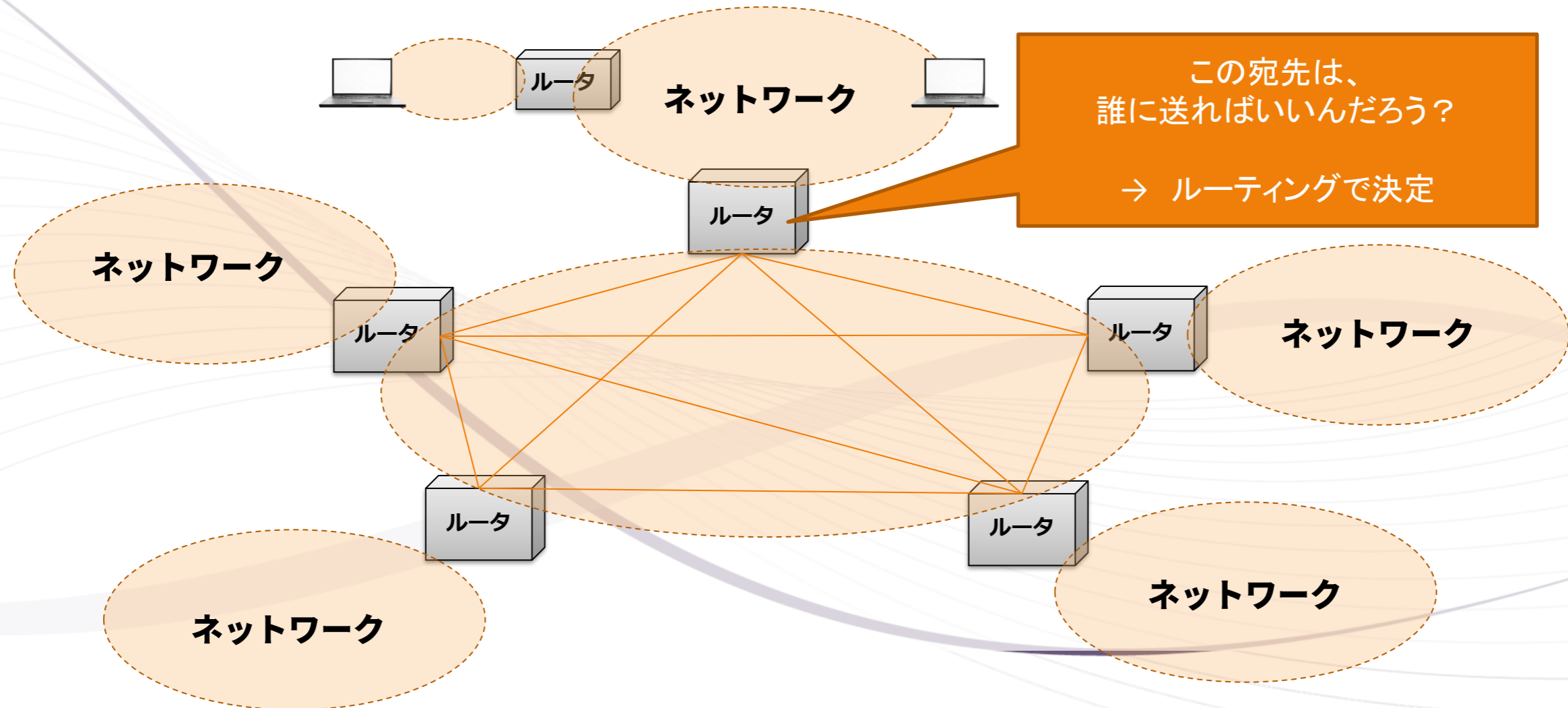
3-3. ルーティングテーブルによる決定

3-4. ルーティング決定の優先度

3-5. インターネットのルーティング

3-1. ルーティングとは？

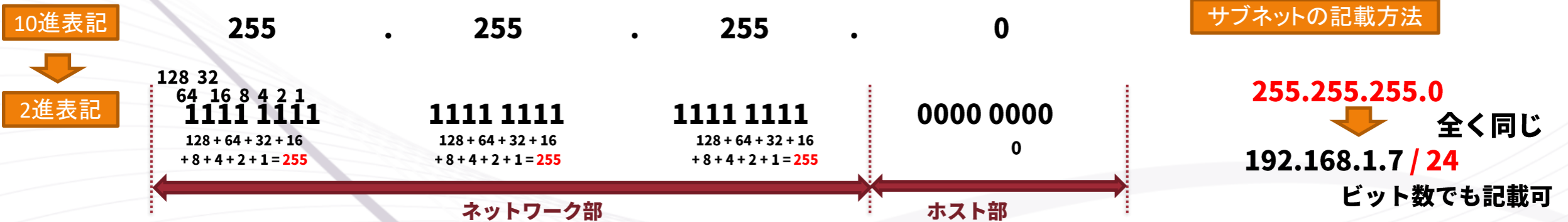
宛先アドレスから、接続されているネットワーク内の誰に送信するか決定する。



3-2. サブネットマスクとデフォルトゲートウェイ

- サブネットマスクはネットワーク部の長さを表す(ネットワークの大きさを表す)
⇒ ネットワーク部が同じビット列か否かで、同じネットワークか判定
- デフォルトゲートウェイはネットワーク部がゼロで設定されるので「全アドレスが該当」

サブネットマスクが「255.255.255.0」の場合は24Bitとなります。



宛先のIPアドレスが「192.168.1.7」の場合

● ネットワークが「192.168.1.0/24」

宛先: 1100 0000 1010 1000 0000 0001 0000 0111

NW: 1100 0000 1010 1000 0000 0001 0000 0000

ネットワーク部が同じビット列なので「同じネットワーク」

● ネットワークが「10.10.10.0/24」

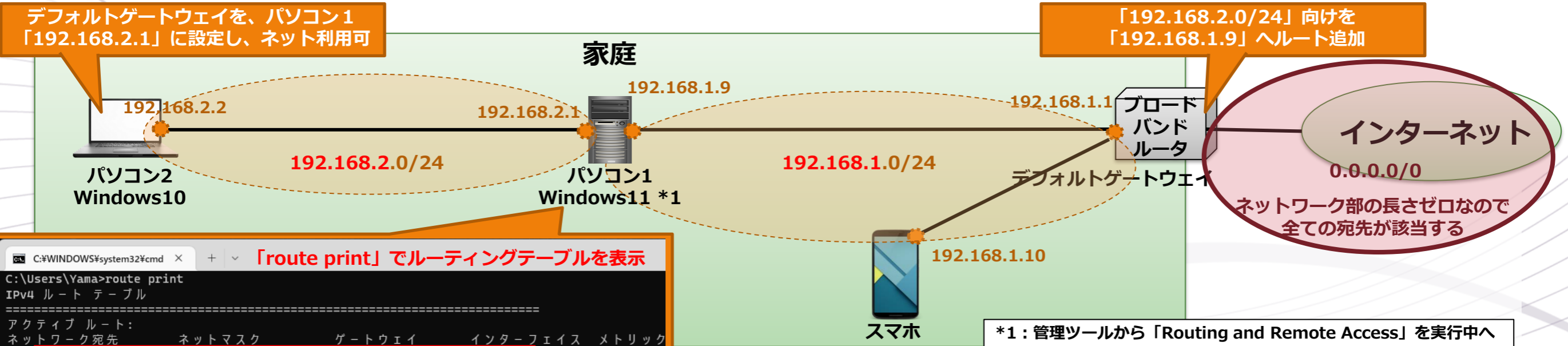
宛先: 1100 0000 1010 1000 0000 0001 0000 0111

NW: 0000 1010 0000 1010 0000 1010 0000 0000

ネットワーク部のビット列が異なるので「同じではない」

3-3. ルーティング

- ・ パソコンやルータなどの端末は送信先を解決するためのルーティングテーブルを持っている。
- ・ 宛先アドレスに対して、ルーティングテーブルから同じネットワークアドレスの宛先を見つける。
- ・ 該当するネットワークアドレスの送信先 (Next-Hop) にパケットを送信する。



```
C:\Users\Yama>route print
IPv4 ルート テーブル
=====
アクティブ ルート:
ネットワーク宛先    ネットマスク    ゲートウェイ    インターフェイス    メトリック
-----
0.0.0.0            0.0.0.0        192.168.1.1    192.168.1.9        331
127.0.0.0        255.0.0.0      リンク上      リンク上            331
127.0.0.1        255.255.255.255 リンク上      リンク上            331
127.255.255.255  255.255.255.255 リンク上      リンク上            331
192.168.1.0      255.255.255.0 リンク上      リンク上            291
192.168.1.9      255.255.255.255 リンク上      リンク上            291
192.168.1.255    255.255.255.255 リンク上      リンク上            291
192.168.2.0      255.255.255.0 リンク上      リンク上            291
192.168.2.1      255.255.255.255 リンク上      リンク上            291
192.168.2.255    255.255.255.255 リンク上      リンク上            291
224.0.0.0        240.0.0.0      リンク上      リンク上            331
224.0.0.0        240.0.0.0      リンク上      リンク上            291
224.0.0.0        240.0.0.0      リンク上      リンク上            291
255.255.255.255  255.255.255.255 リンク上      リンク上            331
255.255.255.255  255.255.255.255 リンク上      リンク上            291
255.255.255.255  255.255.255.255 リンク上      リンク上            291
```

- ・ 宛先が、サブネットマスクで示されるネットワーク部の長さのbit列に対して合致する宛先に送信される。
- ・ デフォルトゲートウェイはネットワーク部が長さが0なので、全ての宛先が該当先となるので、インターネット向けの全アドレスが選択される。
- ・ 接続されているリンクはネットワーク部の長さが24なので、デフォルトゲートウェイより優先して選択される

デフォルトゲートウェイ

接続ネットワーク

接続ネットワーク

赤枠は主に選択されるルート

3-3. ルーティング決定の優先度

- ・ルーティングは複数の要因で決定されるが優先度がある。
- ・優先度は、以下のようにになっている

優先度1：Longest Match

ネットワーク部の長さ（サブネットマスクの長さ）が最も優先される。

例) ルーティングテーブルに①, ②の2つが存在する場合において
宛先「192.168.1.1」は以下の両方に該当するが、長さ24の①が選択される

	ネットワークアドレス	Next-Hop
①	192.168.1.0/24	192.168.1.1
②	192.168.0.0/16	192.168.1.11

← ネットワーク超の長いこのルートが選択される

優先度2：アドミニストレーティブディスタンス どの経路種別を優先させるかが決まっている。

- ・スタティックルート
運用者が手動で設定したルート
- ・ダイナミックルーティング
ルーティングプロトコルにより自動で経路情報を更新すること
自分の経路を相手に通知することにより動的に経路情報を更新

《標準的な設定値》（一部抜粋）

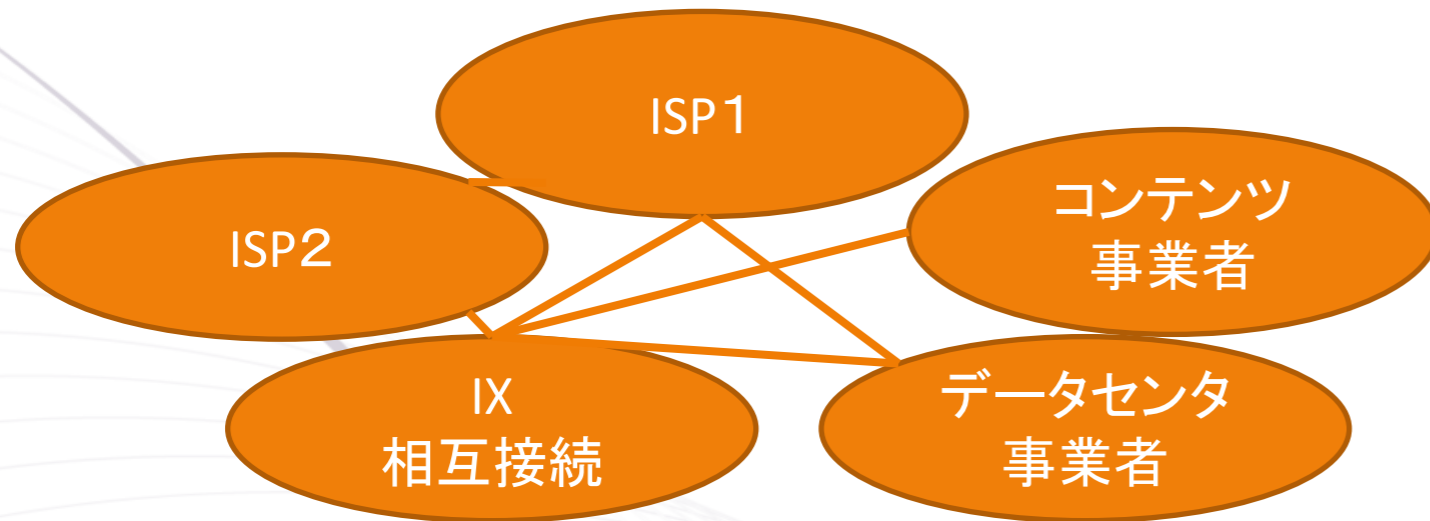
経路の情報元		アドミニストレーティブ ディスタンス値
直接接続（同じネットワーク）		0
スタティックルート		1
ダイナミック ルーティング	BGP（外部）	20
	OSPF	110
	RIP	120
	BGP（内部）	200

優先度3：メトリック

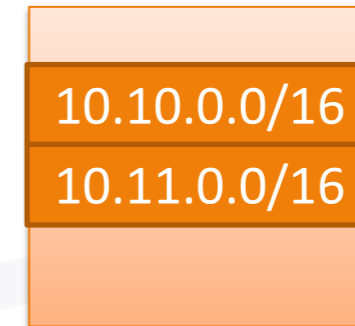
手動で優先度を設定したり、ホップ数やコストにより経路の優先度を操作する場合に利用します。

3-4. インターネットのルーティング

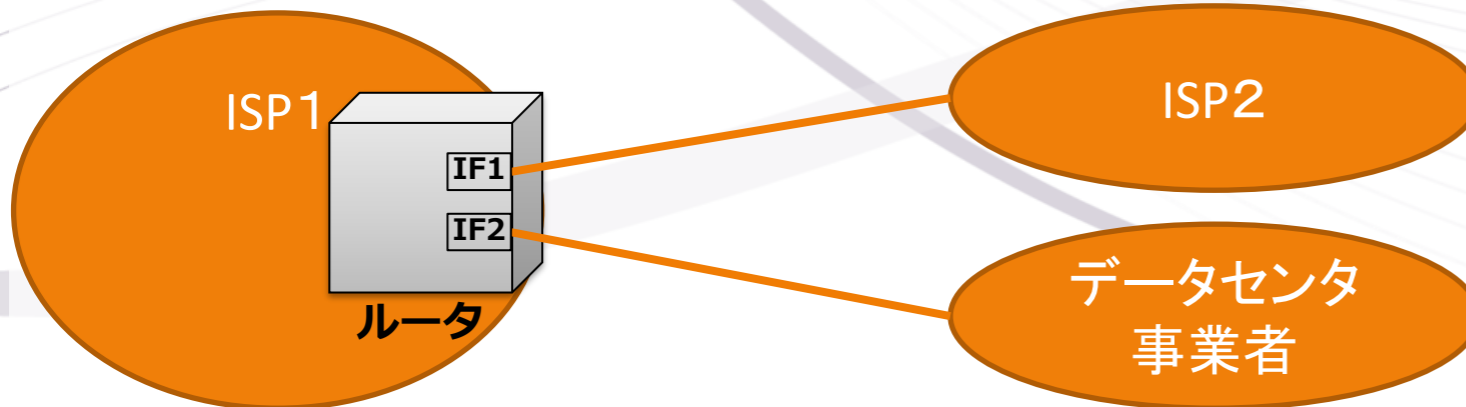
・利用しているネットワークアドレスを事業者間で交換することでルーティングを構築



各事業者は自分の利用しているネットワークアドレスを接続先に相互に通知している。
(BGPというプロトコルで自動で相互に通知している)



通知するネットワークアドレスは出来るだけまとめて送信します。



基本的に、相手から通知されたネットワークアドレスは、その事業者が利用しているということなので、送信先になります。

4. EthernetとMACアドレス

4-1. Ethernetとは？

4-2. Nex-Hopへの送信とMacアドレス

4-2. MACアドレス解決の仕組み「ARP」

4-3. Ethernet端末における送信処理まとめ

4-1. Ethernetとは？

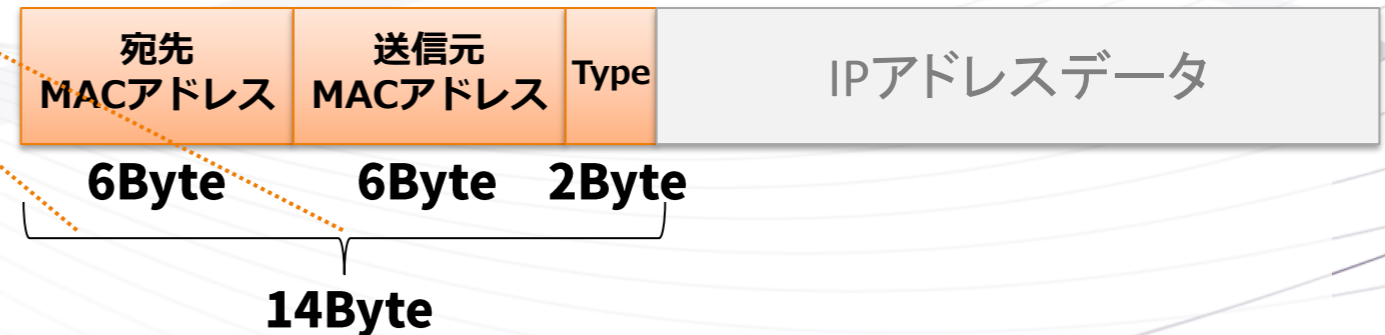
- EthernetはIEEEの通信技術で、レイヤ2のデータリンク層の技術
- Ethernetでは端末識別にMACアドレスを用いる。



- Ethernet規格
 - 有線：LANケーブル、同軸、光ケーブル
標準化 IEEE802.3
 - 無線：Wi-Fi
標準化 IEEE802.11 ac/a/n/g/b

- プロトコルスタックの位置づけ
 - OSI参照モデルの物理～データリンク層に相当（IPアドレスの下層）

- Ethernet データフォーマット



- MACアドレスとは？
 - インターフェースに付与された6 Byteのアドレス。製造メーカーが付与。

Wireshark packet capture details for Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol (ICMP Echo request).

Ethernet II
Destination: Mitsubis_86:d6:65 (10:4b:46:86:d6:65) **宛先 Macアドレス**
Source: Tp-LinkT_09:d6:7d (28:ee:52:09:d6:7d) **送信元 Macアドレス**
Type: IPv4 (0x0800)

Ethernet ヘッダ

IP ヘッダ
Source Address: 192.168.1.9 **送信元 IPアドレス**
Destination Address: 23.59.13.91 **宛先 IPアドレス**

データ

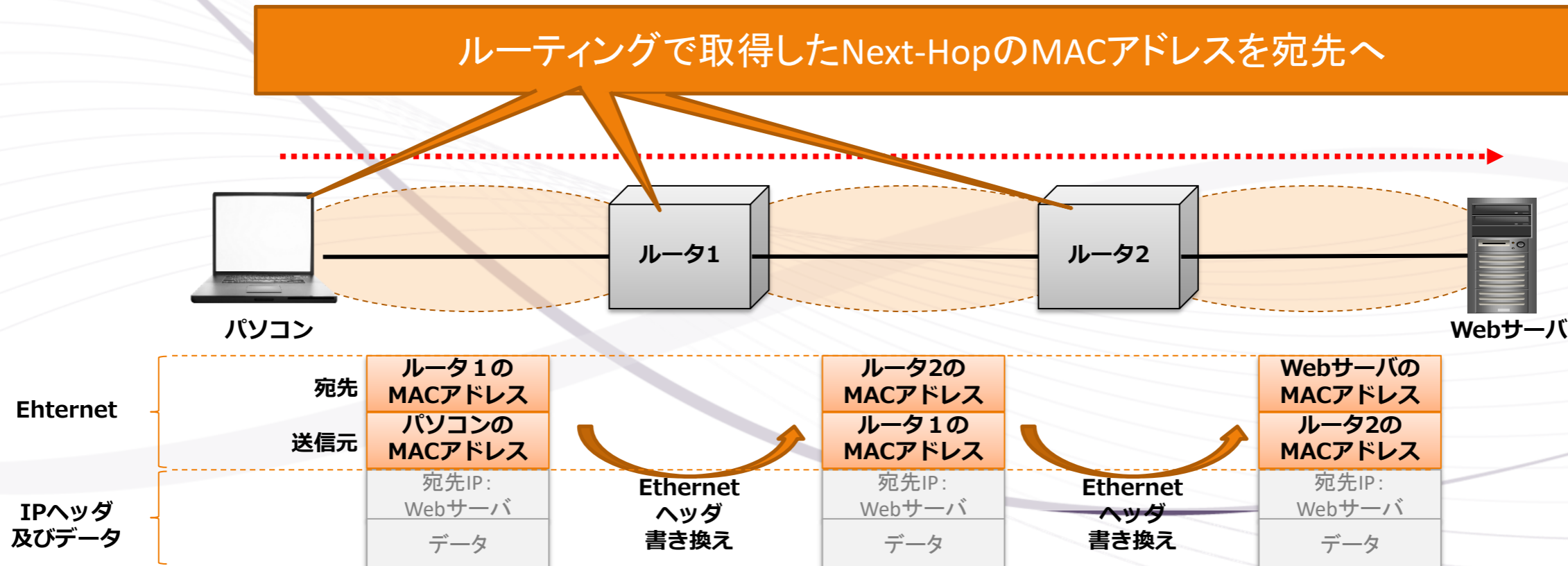
Ethernet 14Byte (includes header and data)
IP アドレス 20Byte (includes header and data)

4-1. Nex-Hopへの送信とMacアドレス

・ルーティングで取得したNext-Hopの宛先端末のMACアドレス宛に送信を行う。

● パソコンからWebサーバへの通信

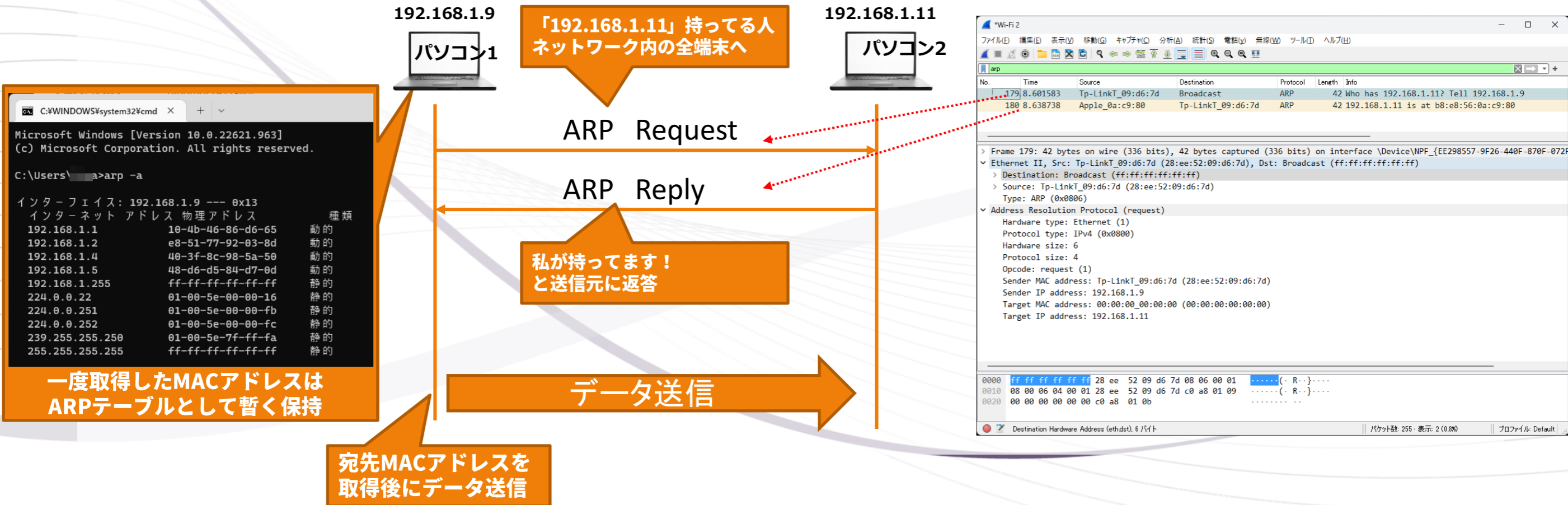
端末やルータはルーティングで取得したNext-HopのMACアドレスにEthernetヘッダを作成し送信する。そのため、ルータを経由する度にEthernetヘッダが書き換えて通信する。



4-2. MACアドレス解決の仕組み「ARP」

- ・ルーティングでは取得するのはIPアドレスのため、MACアドレスを取得する仕組みが必要。
- ・宛先MACアドレスはルーティングで取得したIPアドレスからARPを用いて取得する。

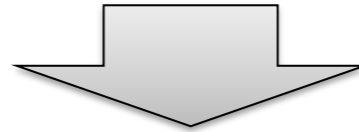
● パソコン1がパソコン2へ通信する場合



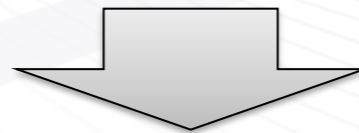
4-3. Ethernet端末における送信処理まとめ

宛先の決定からデータ送信までの処理

ルーティングテーブルから送信先 (Next-Hop) を決定する



ARPで送信先 (Next-Hop) のMACアドレスを取得する。



Ehternetヘッダを付加し、データを構築して送信する