1章
インターネットのつながる仕組み

演習①
インターネット接続に必要な契約・機器

演習①インターネット接続に必要な契約・機器

有線PC1台、無線PC1台、タブレット1台を同時にインターネット接続するためには、どのような機器が必要か、
下部の記入欄に構成図を描いて下さい。また、インターネット開通に必要な契約も併せて記入してください。
なお、フレッツ光1回線による接続とする。

●機器の設定情報を確認する

■実機で確認しながら、各機器の設定情報を埋めてください。

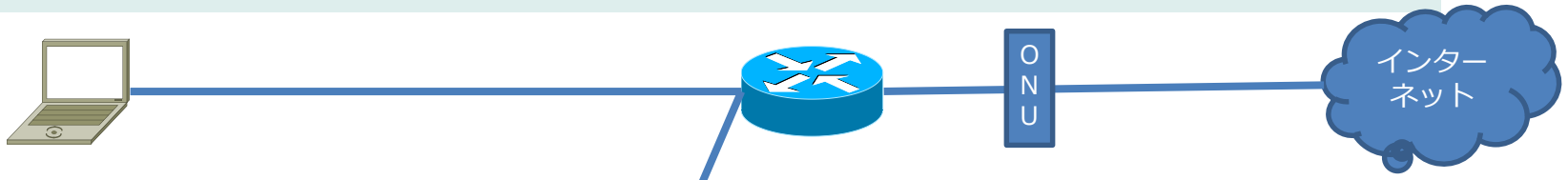
ルータ

LAN側

〔　　〕 IPアドレス
〔　　〕 サブネットマスク

WAN側

〔　　〕 IPアドレス
〔　　〕 サブネットマスク
〔　　〕 DNS

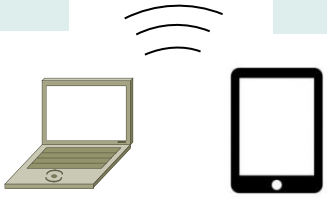


有線パソコン

〔　　〕 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

アクセスポイント

〔　　〕 IPアドレス
〔　　〕 サブネットマスク
〔　　〕 デフォルトゲートウェイ



無線パソコン

〔　　〕 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

タブレット

〔　　〕 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

IP基礎

●OSI参照モデル

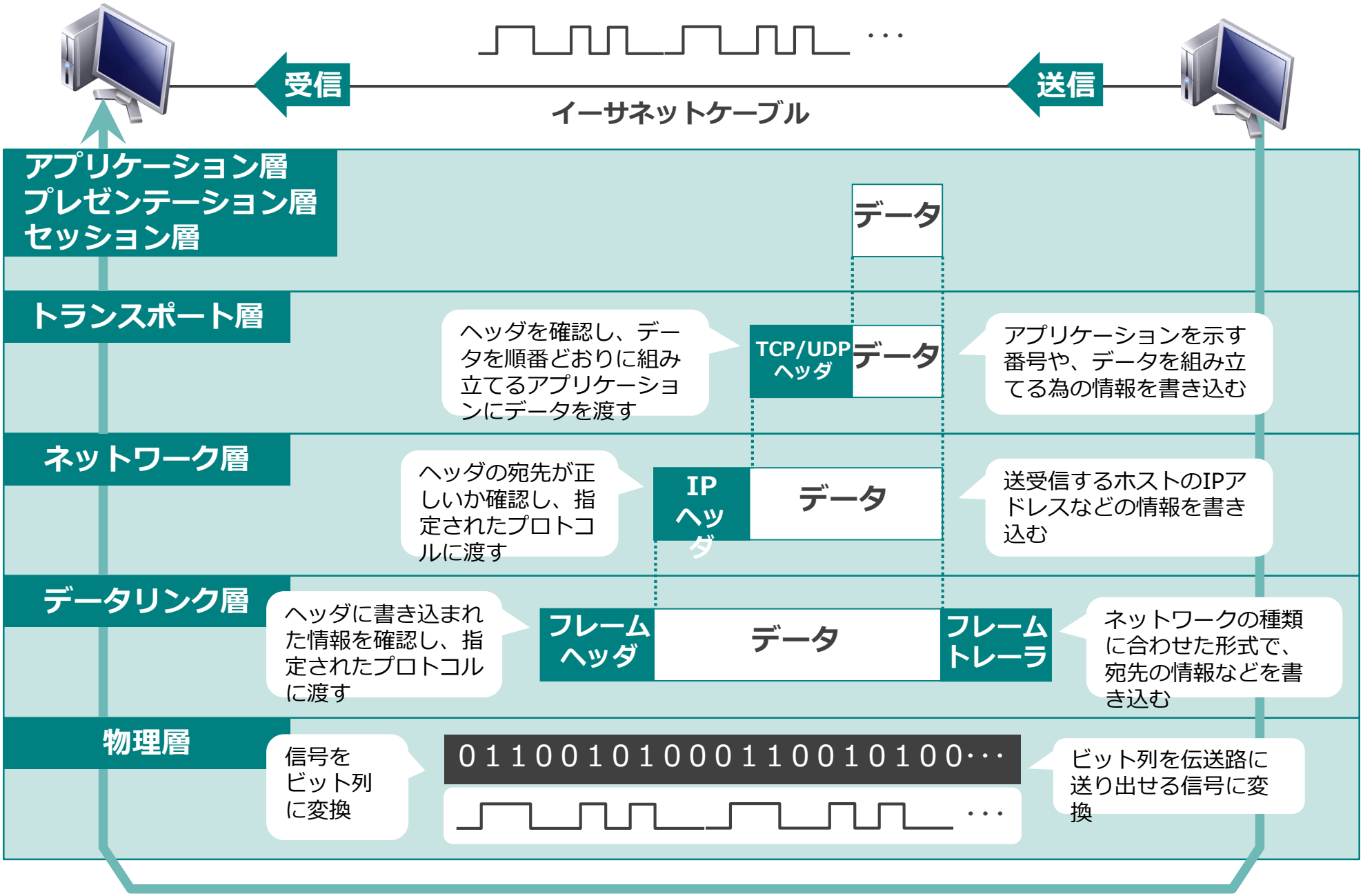
アプリケーション層	Layer7	アプリケーションソフトと直接連携する部分
プレゼンテーション層	Layer6	データの書式（フォーマット）を規定する部分
セッション層	Layer5	アドレス関係を調整し接続を管理する部分
トランスポート層	Layer4	通信の信頼性を管理する部分
ネットワーク層	Layer3	目的のアドレスまでの経路を管理する部分
データリンク層	Layer2	目的のホストを判別してデータを受け渡す部分
物理層	Layer1	通信に用いるケーブルやコネクタなどの規格を管理する部分

●OSI参照モデル

世界共通となる通信プロトコルとして、代表的なものとして、ISOのOSI（Open Systems Interconnection）やIBMのSNA（Systems Network Architecture）があります。これらは、通信プロトコルを７つの階層（大きな役割分担区分）に分けて構成しています。上位層ほどユーザ（人間）に近く、下位層ほどハードウェアに近いものになっています。

※ISO：International Organization for Standardization（国際標準化機構）
電気分野を除く工業分野の国際的な標準規格を策定するための民間の非営利団体。

●階層で見るデータの送受信

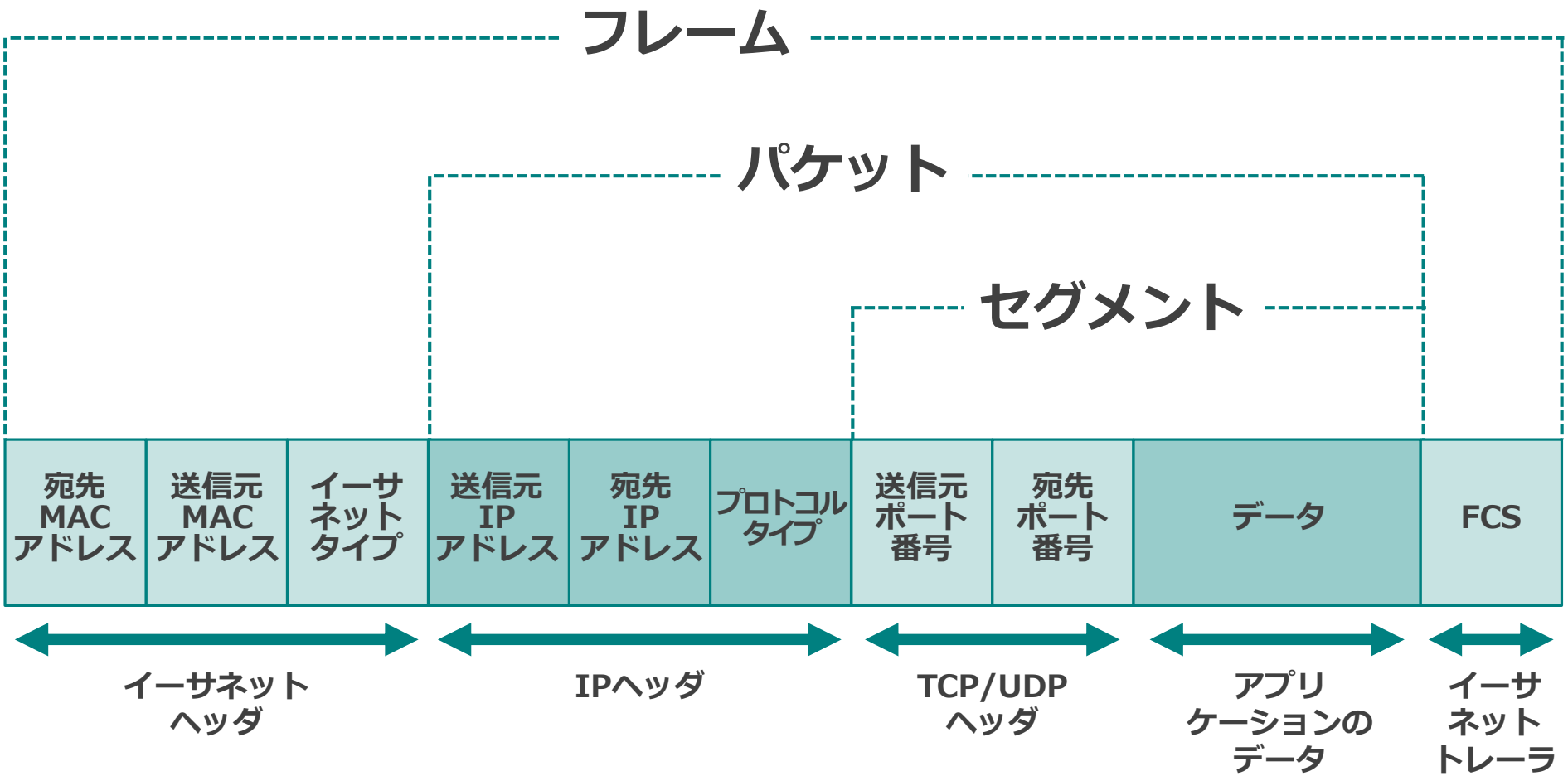


●階層で見るデータの送受信

【データが階層で処理されていく過程】
アプリケーションソフトで作成された文章は、データファイルとして途中の伝送路やルータを経由させるための処理をする必要があります。階層ごとに機能を分担し、ルールに則ってデータを処理する過程を「カプセル化」と言います。カプセル化したデータを伝送路や各デバイスを経由させて宛先ホストへ届けます。受信したパソコンは逆の行程を辿り、アプリケーションソフトへ渡します。

1. 作成されたデータを相手のホストに転送する場合、トランスポート層では、アプリケーションの識別に必要なポート番号等の入ったTCP/UDPヘッダを付加します。
2. TCP/UDPヘッダが付加されたデータをセグメントと呼びます。
3. ネットワーク層でIPヘッダを付加します。
4. IPヘッダの中には、送信先IPアドレス・送信元IPアドレスが付加されます。IPヘッダが付加されたデータをパケットと呼びます。
5. データリンク層でフレームヘッダを付加します。
6. フレームヘッダの中には送信先MACアドレス・送信元MACアドレス等を、データの末尾にはフレームトレーラを付与します。
7. フレームヘッダ・トレーラが付加されたデータをフレームと呼びます。
8. 次に、フレームをコネクタやケーブルなどの規定に合わせ、ビットを電気信号や光信号に変換し、イーサネットケーブルに流します。

●イーサネットのフレーム形式



●イーサネットのフレーム形式

フレームの先頭にイーサネットのヘッダ、次にIPヘッダが付きます。
その後ろにTCPまたはUDPヘッダが付き、アプリケーションのデータが続きます。
フレームの最後にはフレームトレーラが付いています。
それぞれのヘッダには、少なくとも2種類の情報が入っています。それは「宛先と送信元のアドレス」と「上位層のプロトコルが何かを示す情報」です。
データを送受信するホストやプログラムを識別するために必要な情報は、階層ごとに決まっています。イーサネットではMACアドレス、IPではIPアドレス、TCP／UDPではポート番号と呼ばれる識別子が利用されます。

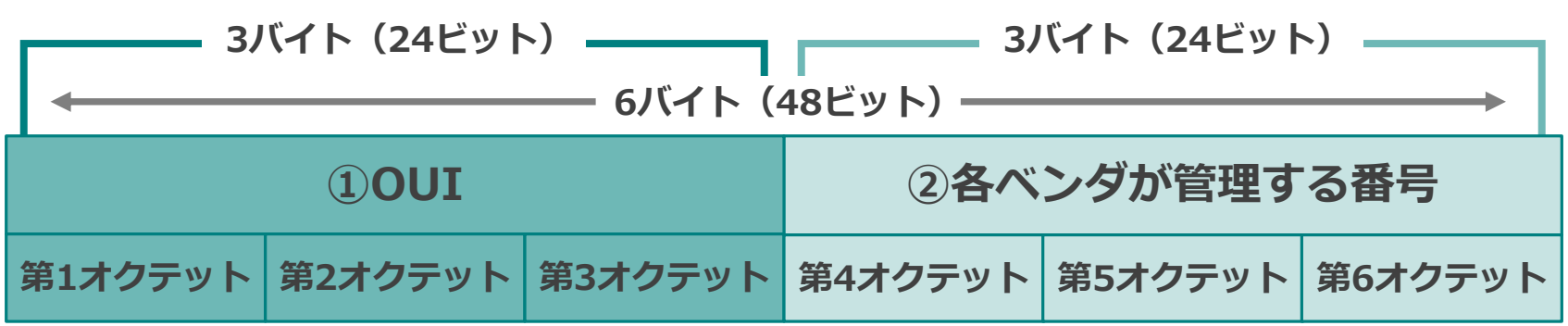
また、各階層のヘッダには、そのヘッダに続くデータが何かを示す識別子が付いています。この識別子は上位層のプロトコルの種類を表す情報です。
フレームヘッダの場合にはタイプ、IPの場合はプロトコルタイプ、TCP／UDPの場合では宛先ポート番号がこれにあたります。
このような形式で、アプリケーションのデータを目的のホストのアプリケーションソフトへと受け渡しています。

●MACアドレス

各ノードに装備されたNIC(Network Interface Card)
に付けられている物理的なアドレス

48桁のビット列を8ビットずつ「：(コロン)」または
「－(ハイフン)」で区切って16進数で表す。

67:89:AB:CD:EF:01



①OUI：製造ベンダ毎に特定の数字
②各ベンダ(メーカ)が管理する番号：ベンダが製造したカード毎に違う数字

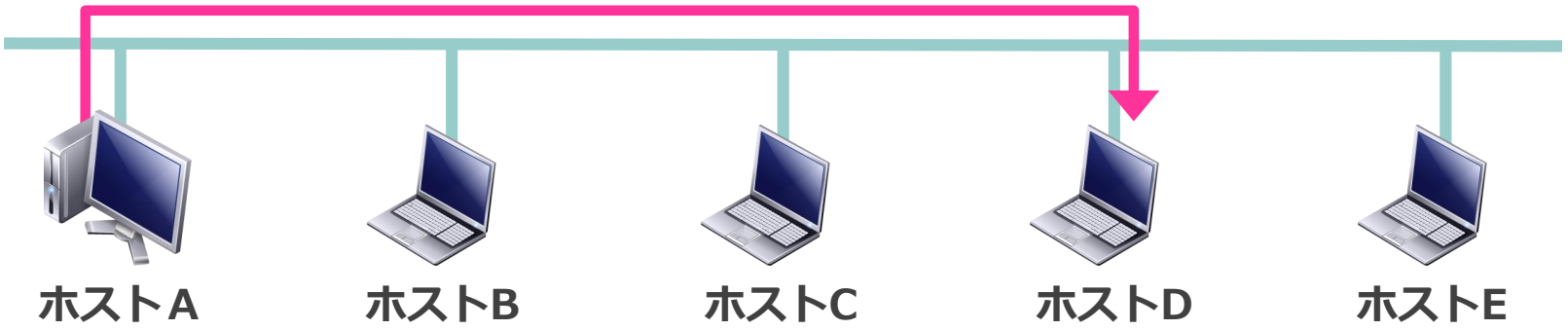
●MACアドレス

ネットワーク上に接続されているノードが通信するには、それぞれが固有のアドレスをもつ必要があります。
そのアドレスは、データリンク層で動作する機器すべてに割り振られており、そのアドレスをMAC（Media　Access　Control：媒体アクセス制御）アドレスと言います。
MACアドレスとは、イーサネットにおけるデータリンク層でのアドレスのことを意味します。

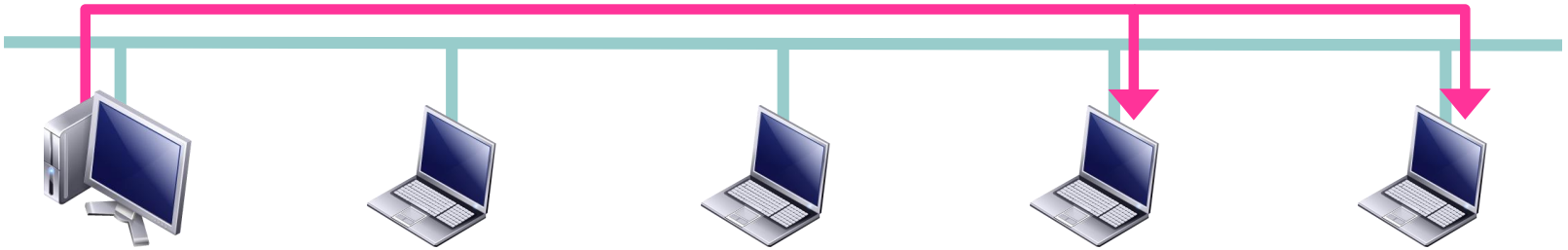
ネットワークに接続されているノードを特定するために使うのがMACアドレスで、「イーサネット・アドレス」や「物理アドレス」、「ハードウェア・アドレス」などとも呼ばれています。
MACアドレスは、インターフェース毎に割り当てられている番号で、１つのデバイスが複数のインターフェースを持つ場合は、それぞれに異なるMACアドレスが割り当てられています。
48bit長のMACアドレスは「12:34:56:78:9A:BC」または「12-34-56-78-9A-BC」という形で、各オクテット（8ビットで1つの塊となるデータの単位）を「:（コロン）」または「-（ハイフン）」で区切った16進数で表記するのが一般的です。

●イーサネット通信の種類

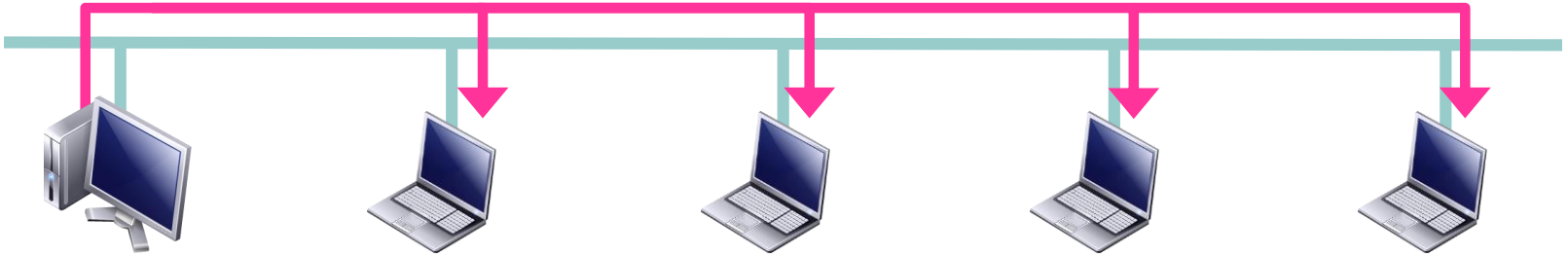
ユニキャスト通信（1対1の通信）



マルチキャスト通信（1対グループの通信）



ブロードキャスト通信（1対全員の通信）



●イーサネット通信の種類

【ユニキャスト】
特定の1つのノードだけに向けた通信です。このとき使われる送信先アドレスをユニキャストアドレスと言います。

【マルチキャスト】
ネットワークにおいて、あらかじめ決められた複数のノードに対して同時に送信を行うことです。たとえばビデオオンデマンドや、音声データの配信などの用途で、複数のノードに対して一斉に放送する、というような用途で使われます。このとき使われる送信先アドレスをマルチキャストアドレスと言います。

【ブロードキャスト】
ネットワークにおいて、そのネットワーク上に存在するすべてのノードを対象としてパケットを送信する形態のことです。一斉同報通信とも言います。マルチキャストと違って、ネットワーク上のすべてのノードが送信対象となります。このとき使われる宛先アドレスをブロードキャストアドレスと言います。

●IPアドレスの表現

IPアドレス＝ネットワーク上の各ホストの住所番地

	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	32
2進数表記	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	1	1	0	0	1	0	0
	第１オクテット								第２オクテット								第３オクテット								第４オクテット							
10進数表記	192								168								1								100							

IPアドレス：
192.168.1.100

●IPアドレスの表現

IPアドレスとは、ネットワーク上の各ホストの住所にあたるものです。

このような表記になっている背景ですが、コンピュータなどのデジタル機器の内部では、全て“0”と“1”の2進数で処理が行われています。IPv4のIPアドレスもコンピュータ内では32桁の2進数で処理されています。
しかし、この32桁の2進数のままでは、アドレスを使用する人間には判別しづらい表記となります。そこで32桁を8桁ずつ4つのパートに分け、それぞれのオクテット※１内の２進数を10進数に置き換えたものを“．”で区切って表記したものが、IPv4のIPアドレスとなります。32ビットのアドレス空間は約43億ものアドレスをサポートしますが、世界人口の約65億人に対して考えれば 7割弱でしかなく、アドレスの枯渇が目前となっています。

※8桁(ビット)の塊を「**オクテット**」と呼びます。8ビット（bit）を1バイト（Byte）とすることがありますが、必ずしも8ビット＝1バイトとは限りません。

ネットワーク部とホスト部の区切り

1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0	1	0	0
192								168								1								100						
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	
255								255								255								0						
ネットワーク部																								ホスト部						

192.168.1.100 255.255.255.0

192.168.1.100 /24

●サブネットマスクの表現

どこまでがネットワーク部であるかを表しているのがサブネットマスクです。

サブネットマスクの表記
10進数表記の例：　　192.168.1.100　255.255.255.0
プレフィックス表記の例：　192.168.1.100　/24

ネットワークアドレスとはネットワーク自体を表すアドレスです

例：IPアドレス：192.168.1.100 /24の場合

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	1	1	0	0	1	0	0
192								168								1								100							
ネットワーク部はそのまま																								ホスト部のビットを 全部“０”にする							
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
192								168								1								0							

ネットワークアドレス：192.168.1.0 /24

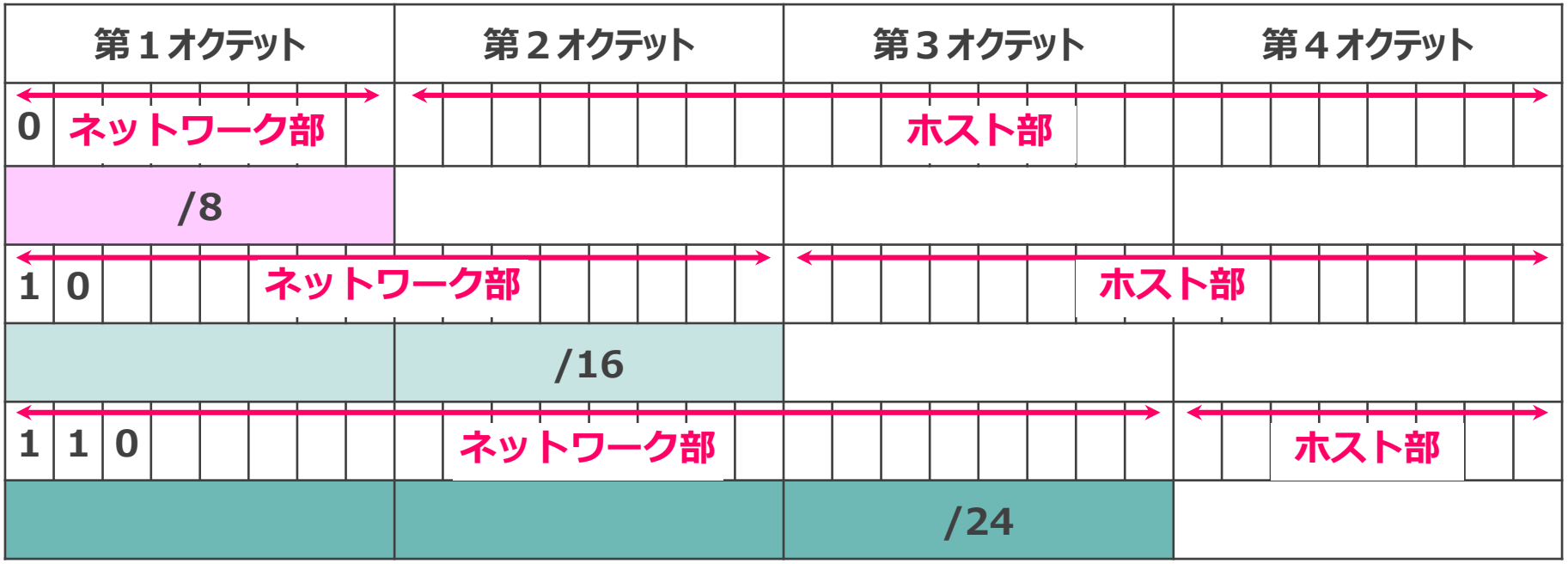
●ネットワークアドレス

ネットワークアドレスは、IPアドレスのホスト部のビットを全て“0”にして算出します。
上図のアドレス 192.168.1.0/24 のネットワーク部は 「/24」で示されているように 24ビットまでなので 「192.168.1」 の部分となり、ホスト部のビットを全部 0 にすると、ネットワークアドレスは「192.168.1.0」となります。

ネットワークアドレスはそのネットワーク自体を表すアドレスなので、パソコンやルータのインターフェースなどのホストアドレスとしては付与することはできません。

クラス毎のアドレス範囲

クラスA	1.0.0.0	～	126.255.255.255
クラスB	128.0.0.0	～	191.255.255.255
クラスC	192.0.0.0	～	223.255.255.255
クラスD	224.0.0.0	～	239.255.255.255
クラスE	240.0.0.0	～	255.255.255.255



●IPアドレスのクラス

IPアドレスはクラスによって分けられます。先頭から8ビット目までをネットワーク部とするものを「クラスA」、同様に16ビット目までとするものを「クラスB」、24ビット目までとするものを「クラスC」と呼びます。クラスＡは第1オクテットの先頭ビットが必ず“0”で始まるという規定になっています。
第1オクテットの数字は1～127が当てはまります※１が、“01111111”（127）はホスト自身を示す特殊なアドレス「ループバックアドレス」※２として予約してあるため、クラスAは1～126がネットワークに割り振れるアドレスとなります。クラスBは第1オクテットの先頭から2ビットが必ず“10”で始まるという規定になっています。
同様に、クラスＣは“110”で始まるように規定されています。クラスに準じたネットワーク構成では、クラスAが約1,677万台、クラスBが65,534台、クラスCが254台のホストを同一ネットワーク内に接続することができます。

しかし、同一のネットワークに何万台ものホストを繋ぐのは現実的ではありません。クラスを用いたIPアドレス割り当ての問題点として、ほとんどのネットワークではクラスAやBは1つのネットワークとして扱うには大きすぎ、使わないIPアドレスが出来てしまうことにありました。
そこで、現在ではネットワーク部とホスト部の境界を8ビット単位に固定せず、統合したり細分化したりなど、クラスレス（クラスの観念に囚われない）による割り当てが一般的です。

※1　第1オクテットが“0”のみで構成されるアドレスは使用できません。
※2　ループバックアドレス：127.0.0.1～127.255.255.254 の範囲のアドレスが予約されています。

●クラスフル・クラスレスネットワークアドレス

クラスフル

クラスで、ネットワーク部の範囲が決まっている

IPアドレス		ネットワークアドレス
61.193.200.62	⇒	61.0.0.0
129.42.18.103	⇒	129.42.0.0
198.133.219.23	⇒	198.133.219.0

クラスレス

サブネットマスクで、ネットワーク部の範囲が指定可能になる

IPアドレス		ネットワークアドレス
61.193.200.62 /24	⇒	61.193.200.0
129.42.18.103 /8	⇒	129.0.0.0
198.133.219.23 /16	⇒	198.133.0.0

●クラスフル・クラスレスネットワークアドレス

IPアドレスを効率よく使用する手段として、クラスを崩してネットワーク部の長さを別途指定し、ホスト部に余りが出ないように管理するクラスレス方式が考えられました。
クラスレスなアドレスは、ネットワーク部がどこまでかを表すサブネットマスクが必要となり、計算しなければネットワークアドレスが判断出来なくなります。

●ブロードキャストアドレス

ネットワーク内の全ホストに一斉通信を行う為に使用するアドレス

例：IPアドレス：192.168.1.100 /24の場合

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	1	1	0	0	1	0	0
192								168								1								100							
ネットワーク部はそのまま																								ホスト部のビットを全部“1”にする							
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
192								168								1								255							

ブロードキャストアドレス：192.168.1.255 /24

●ブロードキャストアドレス

ブロードキャストアドレスは、そのネットワークに存在する全ホストに一斉通信を行うときに利用するアドレスのため、ネットワークデバイスに割振ることが禁じられています。
ネットワークアドレス同様、ホストに付与することが出来ないアドレスとなります。
同一ネットワーク内では、ネットワークアドレスが最初のアドレスで、ブロードキャストアドレスが最後のアドレスとなります。

●IPアドレスの区別

プライベートIPアドレス

LANの内部で使用するIPアドレス（インターネット上では使用できません）

【範囲】

クラスA	10.0.0.0	～	10.255.255.255
クラスB	172.16.0.0	～	172.31.255.255
クラスC	192.168.0.0	～	192.168.255.255

グローバルIPアドレス

インターネット上で使用するIPアドレス

●IPアドレスの区別

IPアドレスは、グローバルIPアドレスとプライベートIPアドレスの２つの種類に分けられます。

【プライベートIPアドレス】
プライベートIPアドレスは、企業のLANの中で使用するIPアドレスです。３つのクラス範囲が決められており、ネットワークを分けるなど用途に応じてIPアドレスの設計を行います。

【グローバルIPアドレス】
グローバルIPアドレスとはインターネット上で使用できるアドレスです。IPアドレスの管理は各国のNIC(ネットワークインフォメーションセンター)が行なっており、ユーザへの払い出し管理はプロバイダ（ISP）が行っています。

●サブネット分割

/24

ネットワーク部																						ホスト部							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
255								255								255						0							

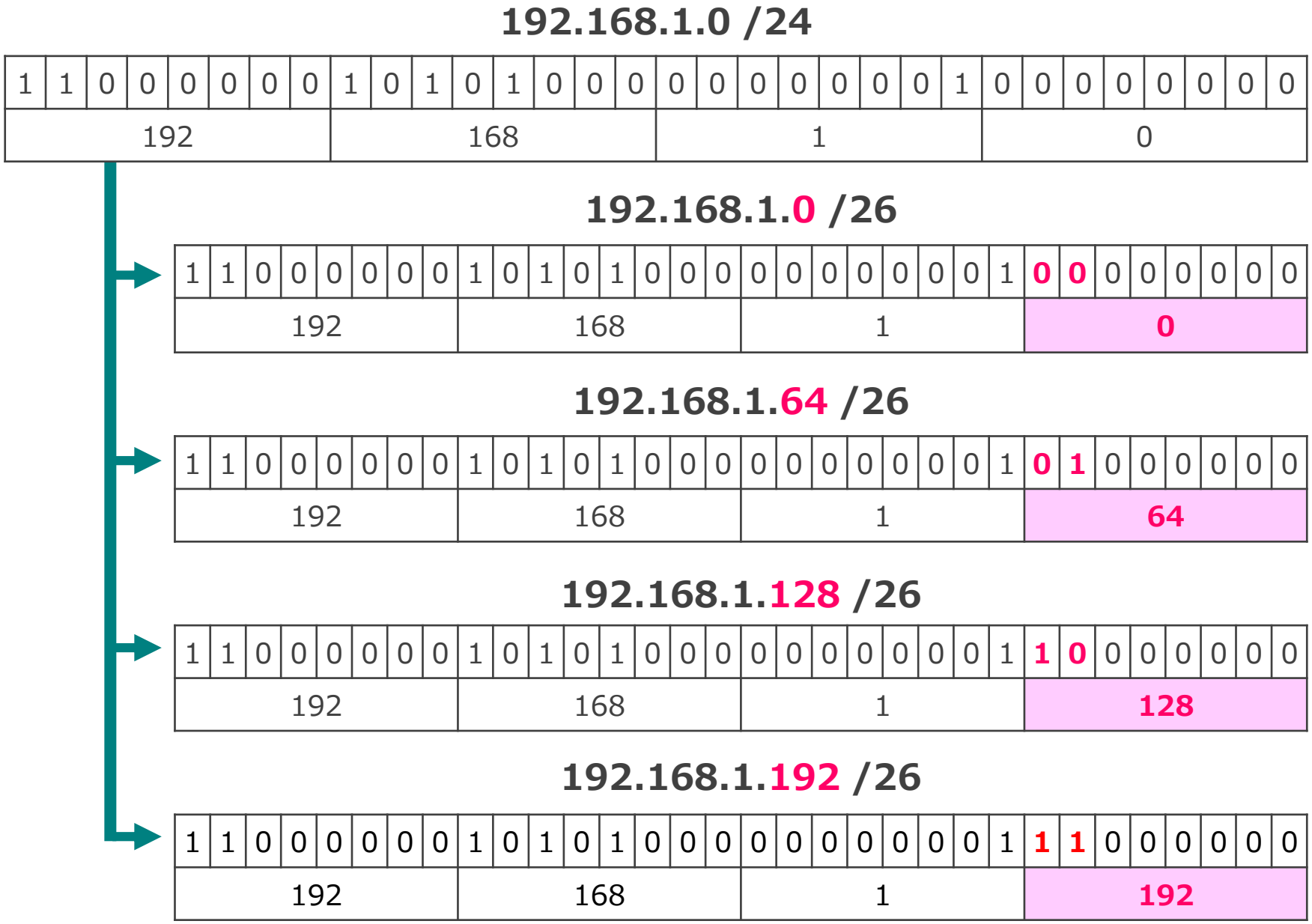
/26

ネットワーク部																								ホスト部						
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0
255								255								255								192					

●サブネット分割

サブネット分割する場合、ネットワーク部のビットを増やします、その分ホスト部のビットが減り使用できるホストアドレス数が減ります。

●ネットワークの分割


192.168.1.0 /24
1 1 0 0 0 0 0 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0
192
168
1
0
192.168.1.0 /26
1 1 0 0 0 0 0 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0
192
168
1
0
192.168.1.64 /26
1 1 0 0 0 0 0 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0 0 0 0 0 0
192
168
1
64
192.168.1.128 /26
1 1 0 0 0 0 0 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0
192
168
1
128
192.168.1.192 /26
1 1 0 0 0 0 0 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 1 1 1 0 0 0 0 0 0
192
168
1
192

●ネットワークの分割

192.168.1.0/24　のネットワークは

192.168.1.0　　/26
192.168.1.64　/26
192.168.1.128　/26
192.168.1.192　/26

4つそれぞれ異なるネットワークアドレスを持つ、サブネットに分割されます。

●CIDR (Classless Inter-Domain Routing)

CIDR	10進数表記/ 2進数表記	同一ネットワーク内 総アドレス数	サブネットワークの数/ サブネット内の最大ホスト数
/24	255.255.255.0 ・・・11 00000000	$2^8 = 256$	1個 / 254個
/25	255.255.255.128 ・・・11 10000000	$2^7 = 128$	2個 / 126個
/26	255.255.255.192 ・・・11 11000000	$2^6 = 64$	4個 / 62個
/27	255.255.255.224 ・・・11 11100000	$2^5 = 32$	8個 / 30個
/28	255.255.255.240 ・・・11 11110000	$2^4 = 16$	16個 / 14個
/29	255.255.255.248 ・・・11 11111000	$2^3 = 8$	32個 / 6個
/30	255.255.255.252 ・・・11 11111100	$2^2 = 4$	64個 / 2個

●CIDR（Classless Inter-Domain Routing ）

●ホストアドレスが属するネットワークアドレスの求め方①

ホストアドレスのホスト部のビットを0にすれば ネットワークアドレスがわかる

ホストアドレス：192.168.200.62 /27

ネットワーク部																								ホスト部				
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	1	1	0	0	1	0	0	0	0	0	1	1	1	1	1	0
192								168								200								62					

ネットワーク部																								ホスト部				
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	1	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0
192								168								200								32					

ネットワークアドレス：192.168.200.32 /27

●ホストアドレスが属するネットワークアドレスの求め方①

ホストアドレスが 192.168.200.62/27 と付与されている場合、このホストアドレスが属するネットワークアドレスについて考えてみましょう。

ネットワークアドレスの求め方

1. 2進数で表す
2. ネットワーク部（27ビットまで）はそのまま保持し、ホスト部は全て“0”にする
3. 8ビット区切りで10進数に戻す

第4オクテットが 00100000 = 32 となります。よって、ネットワークアドレスは 192.168.200.32/27 となります。

●ホストアドレスが属するネットワークアドレスの求め方②

■サブネットマスクからネットワークがいくつのアドレス範囲に分かれているかを割り出し、ホストアドレスがどのネットワーク範囲に属するかを判断し、その範囲の最小値がネットワークアドレスとなる

192.168.200.62 /27

↓

32個ずつのネットワーク範囲

↓

0~31, 32~63, 64~95, 96~127・・・

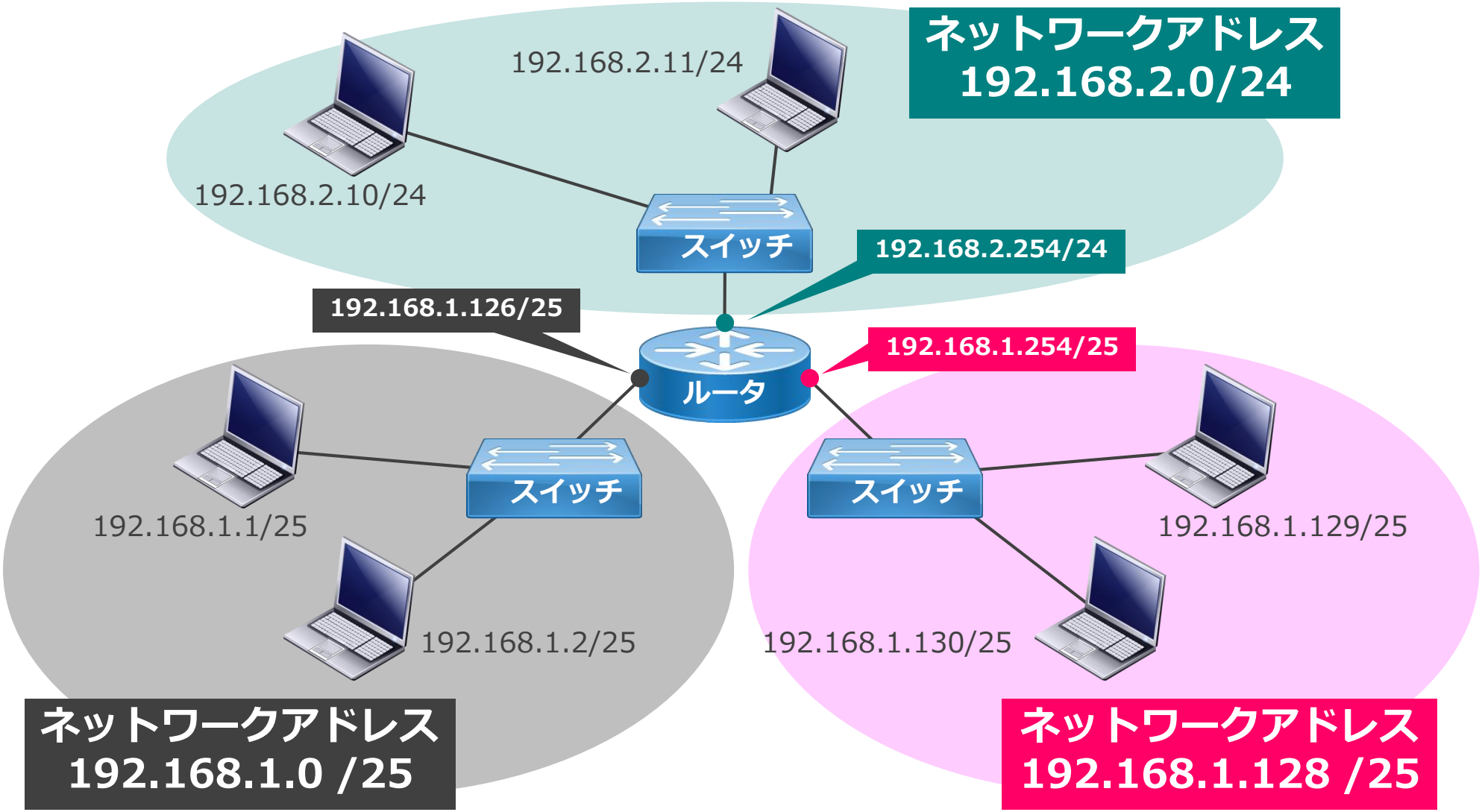
↓

62が存在する32~63の範囲の最小値がネットワークアドレス

ネットワークアドレス：192.168.200.32

●ホストアドレスが属するネットワークアドレスの求め方②

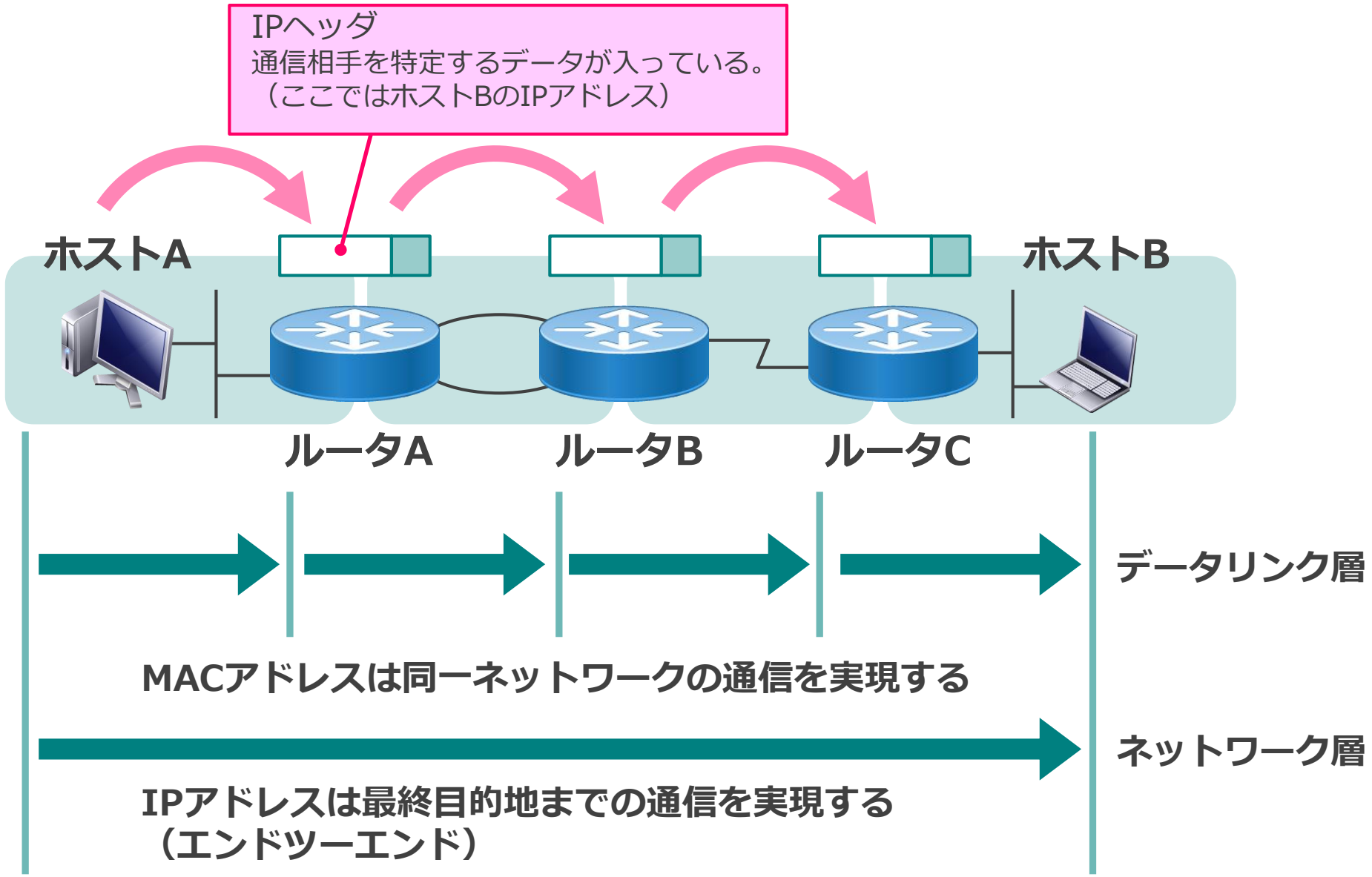
ネットワークアドレスやホストアドレスは重複しないようにIPアドレス設計を行います



●IPアドレス設計

ネットワーク上の個々のホストは、IPアドレスによって識別されます。IPを使用して通信を行うすべてのホスト（PC）とルータのインターフェースには異なるIPアドレスが必要です。

●データリンク層とネットワーク層の関係



●データリンク層とネットワーク層の関係

データリンク層は、同一ネットワーク内のホスト同士の通信を提供します。それに対して、ネットワーク層はネットワーク間の転送を提供します。

■TCP（コネクション型通信：3ウェイハンドシェイク）

受信側がデータを受け取れる状態かどうかを確認してから通信開始。これを「コネクションを確立する」という。

（TCPの通信）

SYN　通信要求

SYN/ACK　応答、通信要求

ACK　応答

データが壊れていたら再送要求

送信側

受信側

■UDP（コネクションレス型通信）

受信側が受け取れるかどうかを調べず送信する。再送はしない。

受信しても確認応答を返さない。

データが破損していれば破棄する。

送信側

（UDP、IPの通信）

受信側

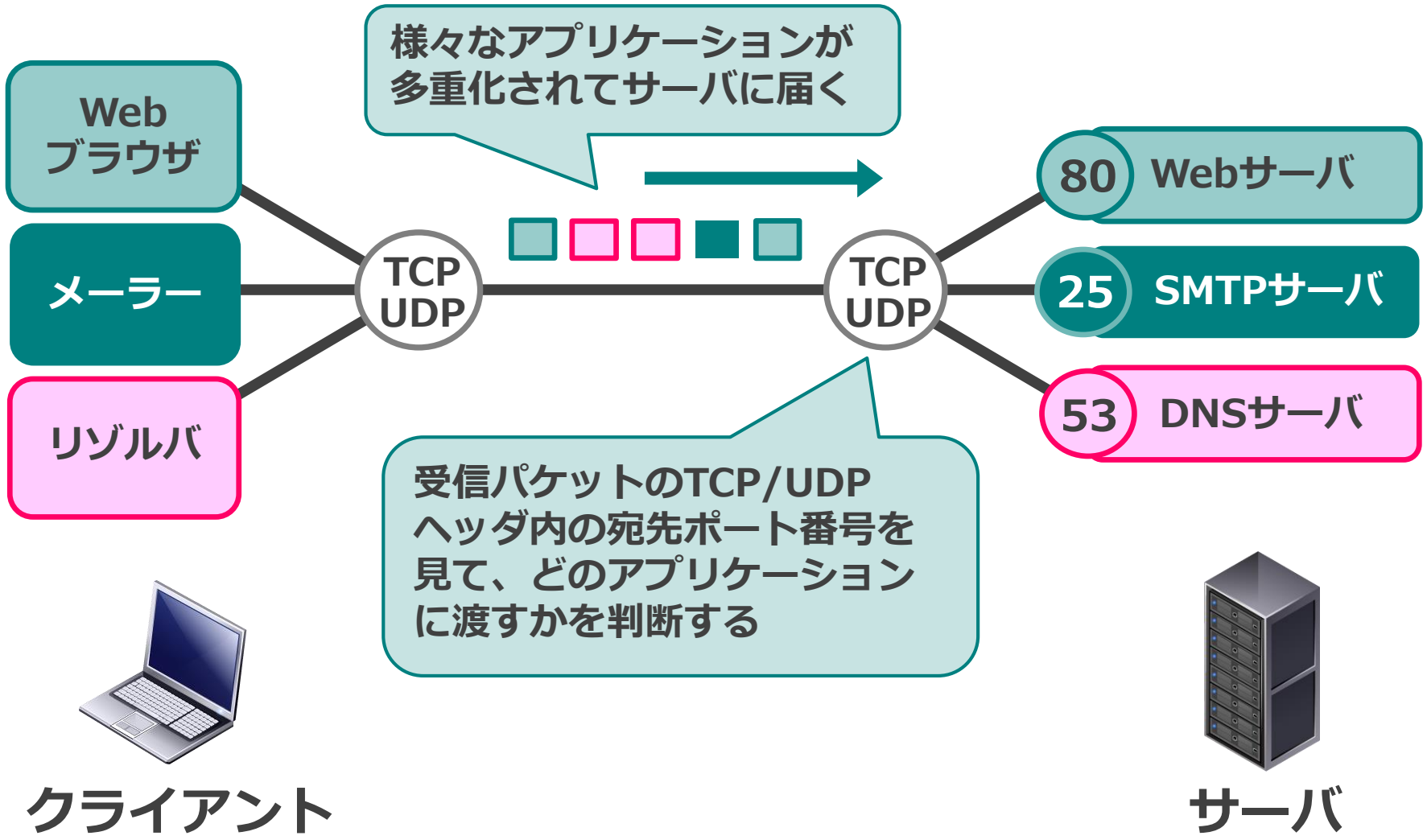
●TCPとUDP

【TCP】
TCPはコネクション型のプロトコルと呼ばれ、通信を行うホスト間でend-to-endのコネクションを確立してからデータ転送を開始します。相手が確実にデータを受け取ったかを確認したり、データの欠落や破損を検知して再送したり、届いたデータを送信順に並べなおしたりといった制御を行います。

【UDP】
UDPはコネクションレス型のプロトコルと呼ばれ、コネクションを確立しません。コネクションレス型の通信は、コネクション型の通信に比べると信頼性は低いものの、手順がシンプルなので高速に通信を行うことができます。

TCPでは、通信する2つのホストを決定してからコネクションを確立するので、ユニキャストの通信形態になります。ブロードキャストやマルチキャストの通信をしたい場合はUDPを使います。

●ポート番号によるアプリケーションの識別



●ポート番号によるアプリケーションの識別

TCP/UDPヘッダには宛先と送信元のポート番号が書かれています。宛先ポート番号を見て、受信データをどのアプリケーションに渡すかを判断します。

■代表的なウェルノウンポート

アプリケーション層のプロトコル	ポート番号	説明	トランスポート層のプロトコル
FTP	20	ファイル転送（FTPデータ送信用）	TCP
FTP	21	ファイル転送（FTP制御用）	TCP
SSH	22	遠隔ログイン(セキュリティ付)	TCP
TELNET	23	遠隔ログイン	TCP
SMTP	25	電子メール（送信）	TCP
DNS	53	名前解決	TCP(同期),UDP
DHCP	67	DHCP（サーバ用）	UDP
DHCP	68	DHCP（クライアント用）	UDP
HTTP	80	WWW	TCP
POP3	110	電子メール（受信）	TCP
HTTPS	443	http protocol over TLS/SSL	TCP

●ポート番号とプロトコル

ポート番号の情報は、TCPやUDPのヘッダに格納され、0～65,535番の範囲が使われます。そのうち、0～1,023番の範囲のポート番号はウェルノウンポート番号（Well-known Port Number）と呼ばれます。サーバマシンがアプリケーションプロトコルのサービスを提供するために使用するポート番号で、インターネットで広く利用されているサービスに割り当てられています。

ウェルノウンポート番号を別のサービスに割り当てて使用することは禁止されています。TCPとUDPのそれぞれに予約されており、上の表のようなものがあります。1,024番以上の番号は、空いていれば自由に使うことができます。

●IPv6

項目	IPv4	IPv6
アドレス表記方法	192.168.1.0	abcd:0000:0000:0000:0011:0220:0000:ffff
サブネット表記	あり　例：/24等	あり　例：/64等
アドレス長	32bits	128bits
アドレス個数	約43億個	約340澗個

●IPv6

IPv6 (IP version 6) は、IPv4アドレス不足の問題を根本的に解決するためにIETFによって開発された新しいインターネットプロトコルで、1999年にはIANAによってIPv6アドレスの割り振りが開始されました。
IPv4アドレスの在庫枯渇をきっかけとして、ISPをはじめとする多くの通信事業者でIPv6の導入が進められています。

ネットワーク
基礎

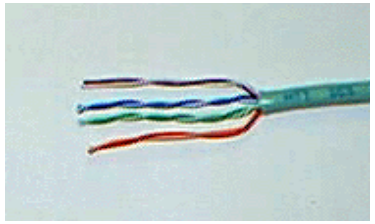
●インターネットで利用する回線の種類

回線	専用装置	接続ケーブル
光	ONU 	光ファイバー
ISDN	DSU 	メタル
ADSL	ADSLモデム 	メタル
モバイル	モバイルルータ 	無線
ケーブルテレビ	ケーブルモデム 	同軸ケーブル

●インターネットで利用する回線の種類

●有線LAN（ツイストペアケーブル）

カテゴリ	伝送速度	周波数	運用規格	最大伝送距離
5	100Mbps	100MHz	100BASE-TX	100m
5e	1Gbps	100MHz	100BASE-TX 1000BASE-T	100m
6	1Gbps	250MHz	100BASE-TX 1000BASE-T	55~100m
6e	10Gbps	500MHz	1000BASE-T 10GBASE-T	100m
7	10Gbps	600MHz	1000BASE-T 10GBASE-T	100m



銅線を絶縁体で被覆し、
2線を1対としてより合わせている

●有線LAN（ツイストペアケーブル）

【ケーブルの形状】
シールドツイストペア（STP)、アンシールドツイストペア（UTP)、耐候性ケーブル、フラットケーブル、難燃性ケーブルなど様々な形状があります。

●有線LAN（光ファイバケーブル）

光の伝搬モード	波長	運用規格	最大伝送距離
マルチモード	長波長	100BASE-FX 1000BASE-LX	2km 550m
マルチモード	短波長	1000BASE-SX	550m
シングルモード	長波長	100BASE-FX 1000BASE-LX	20km 5km

FCコネクタ	SCコネクタ	MUコネクタ	LCコネクタ
			
			

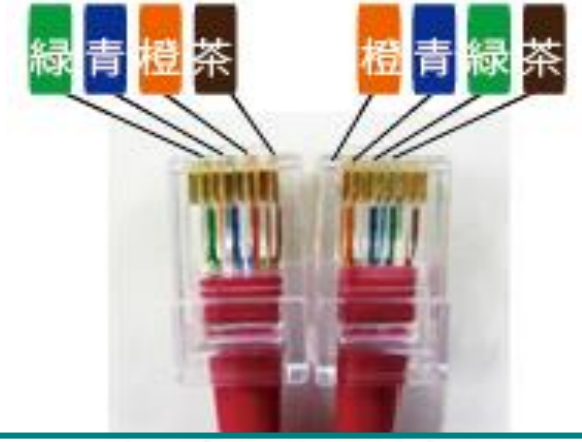
●有線LAN（光ファイバケーブル）

コネクタは優れた特性で脱着が容易なSCコネクタが一般的に普及しています。SCコネクタはLANにおいても世界標準とされているコネクタです。測定器等に使用するような固定やある程度の強度が必要な場合は、FCコネクタが適用されます。

●LANケーブルの識別

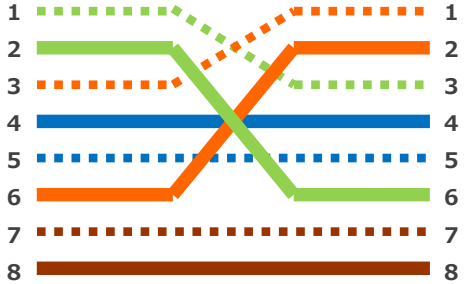
ストレートケーブル

クロスケーブル

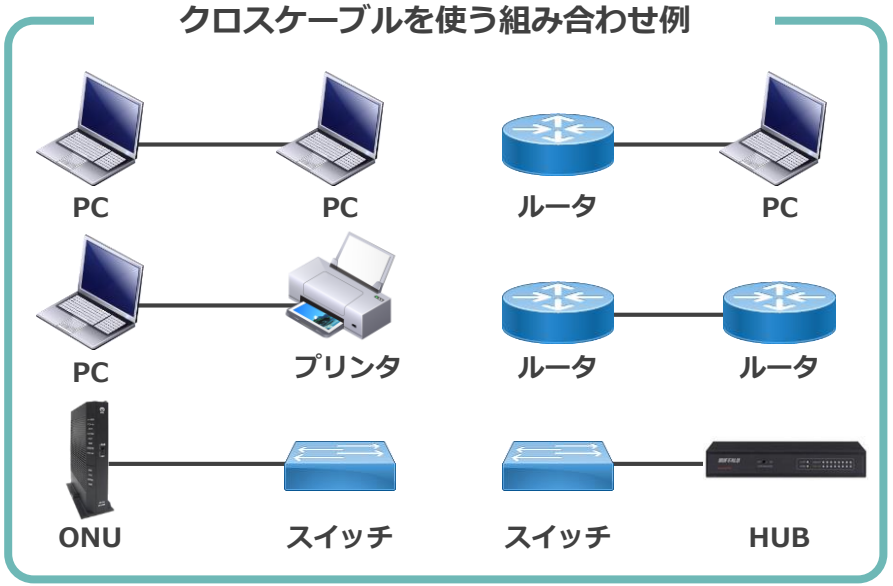


ストレートケーブル

クロスケーブル



クロスケーブルを使う組み合わせ例



●LANケーブルの種類

LANケーブルには、ケーブル内の信号線の配列によって「ストレートケーブル」と「クロスケーブル」があります。ただし最近は、ネットワークを構築する際にクロスケーブルを使うことは、ほぼありません。

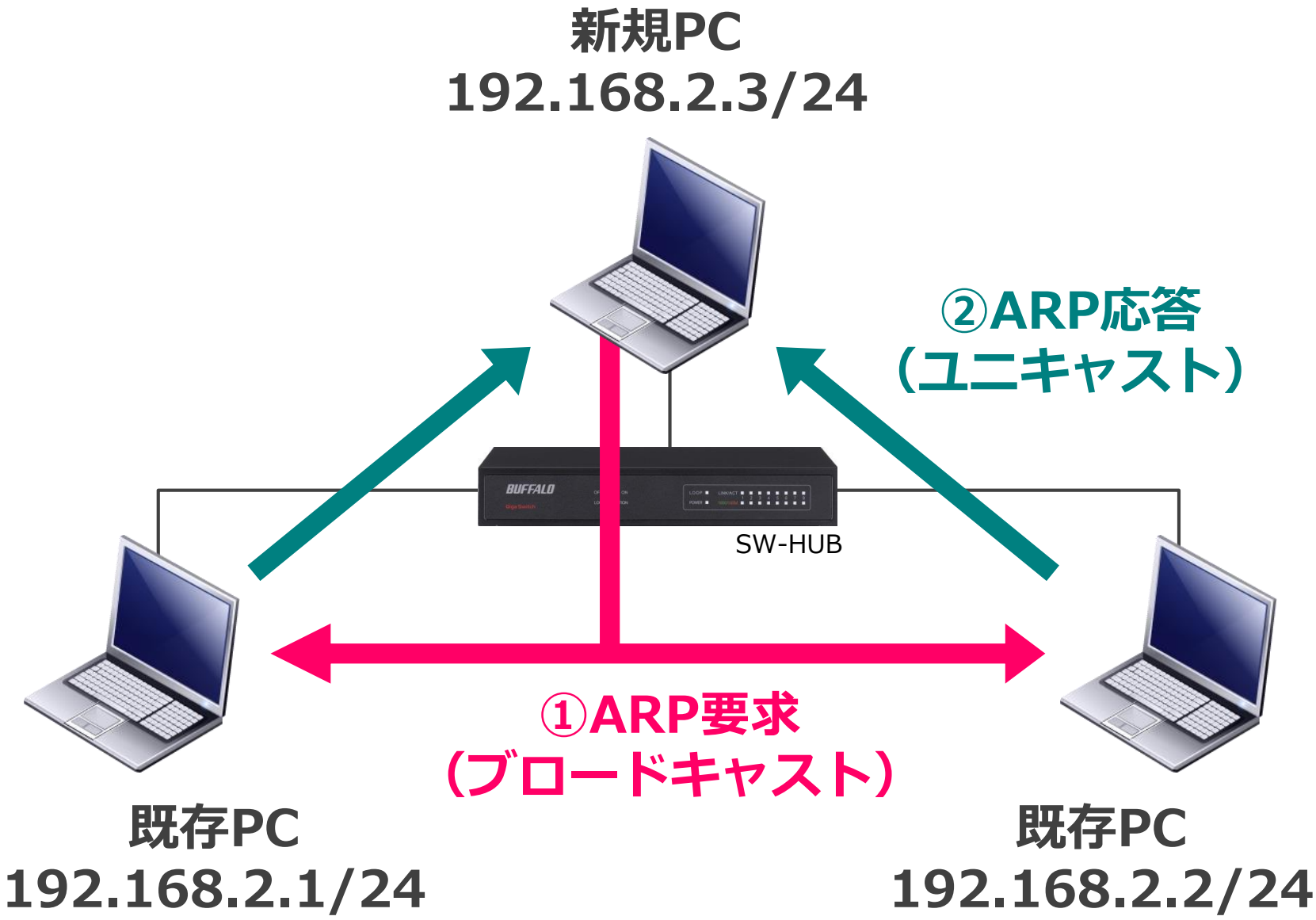
通信相手のポートやLANケーブルの配列を自動判別して通信を可能にする「オートMDI/MDI-X」と呼ぶ機能あります。今ではほとんどの機器にこの機能を搭載しており、LANケーブルはストレートでもクロスでも区別する必要がなくなりました。

●有線NICの規格

主な規格	通信速度	利用状況
10BASE-T	10Mbps	ほとんど利用なし
100BASE-T	100Mbps	旧型で一部利用
1000BASE-T	1Gbps	現在の主流
10G-BASE-T	10Gbps	一部のサーバや機器で利用

●有線NICの規格

●ARP（Address Resolution Protocol）

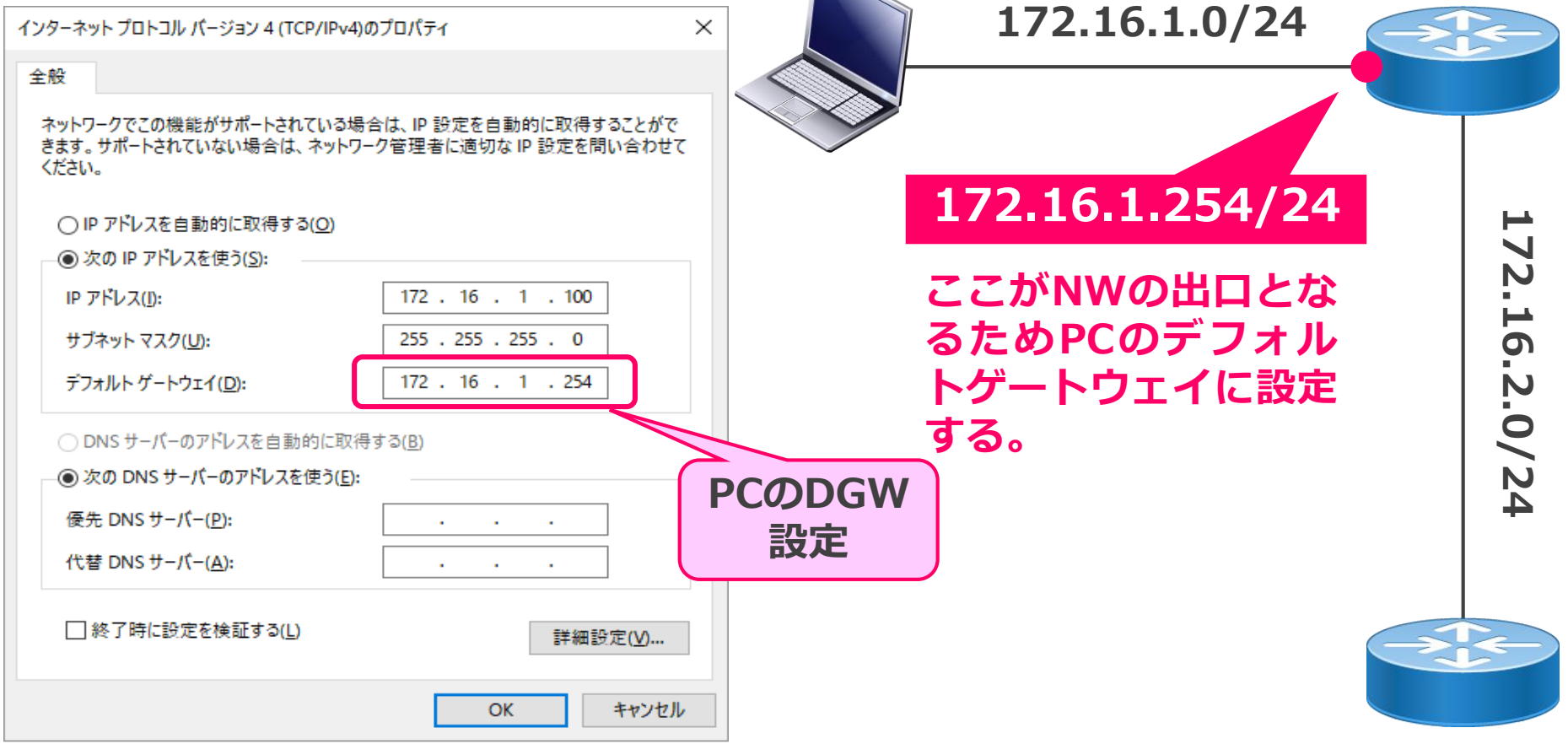


●ARP（Address Resolution Protocol）

ARPは与えられたIPアドレスからMACアドレスを求めるためのプロトコルです。新規PCと既存PCで通信をする場合、宛先のMACアドレスが不明なためブロードキャストでARP要求というものを送信します。
該当するIPアドレスを持つ既存PCがARP応答を返し、宛先のMACアドレスが新規PCのARPテーブルに登録されます。

●デフォルトゲートウェイ

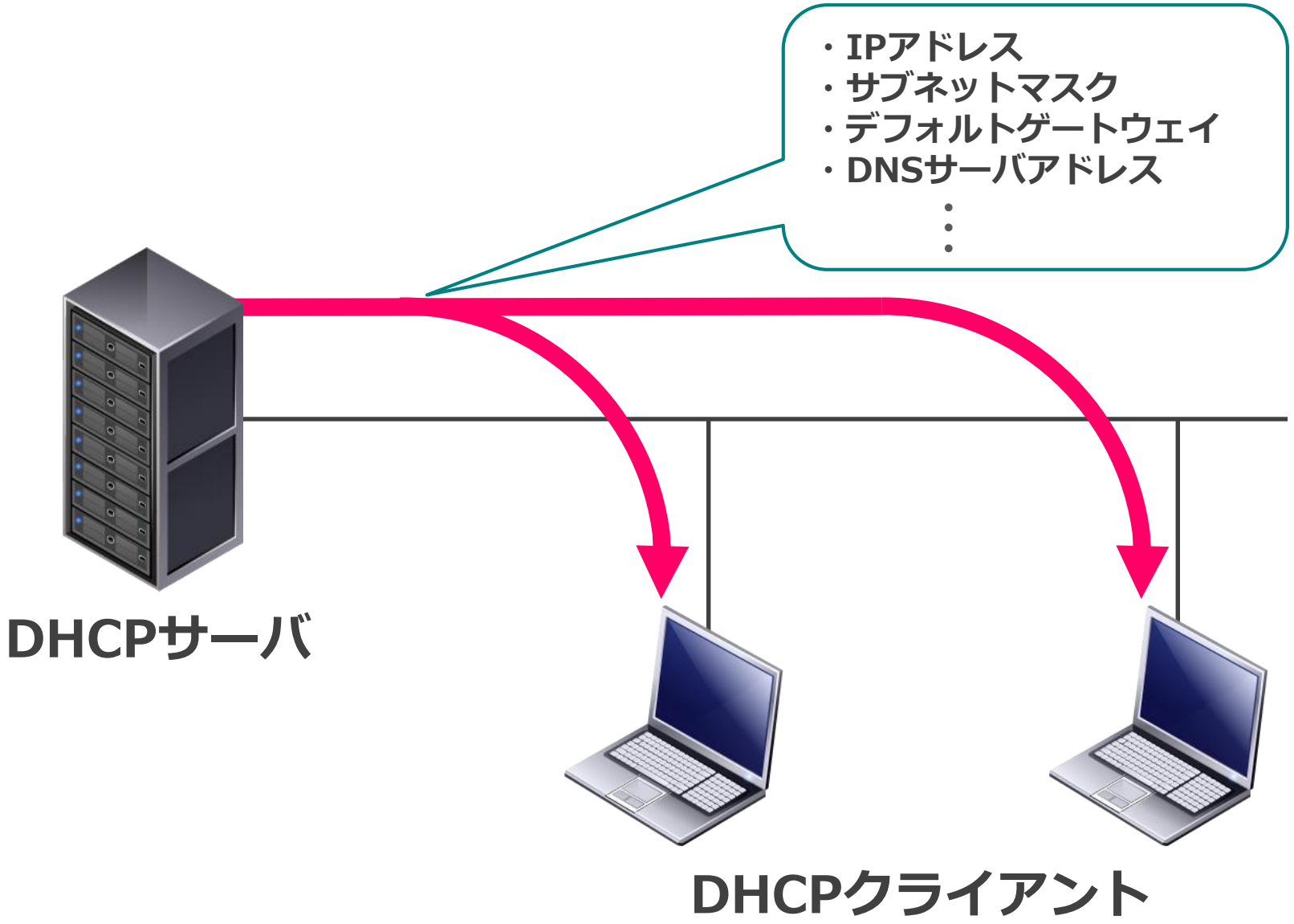
IP:172.16.1.100/24
デフォルトゲートウェイ：172.16.1.254



●デフォルトゲートウェイ

デフォルトゲートウェイとは、所属するネットワークの外へアクセスする際に出口となる機器のことです。
一般的には、ルータがデフォルトゲートウェイになります。

●DHCP（Dynamic Host Configuration Protocol）



●DHCP（Dynamic Host Configuration Protocol）

DHCPを使うと、IPアドレスに限らず、サブネットマスクや、DNSなどの設定パラメータも割り当てられます。
新規端末を追加したときに、手作業によるIPアドレスの割り当て作業から解放され、ネットワーク管理の手間が軽減されます。

●DNS（Domain Name System）

1 www.ntt.co.jpにアクセス

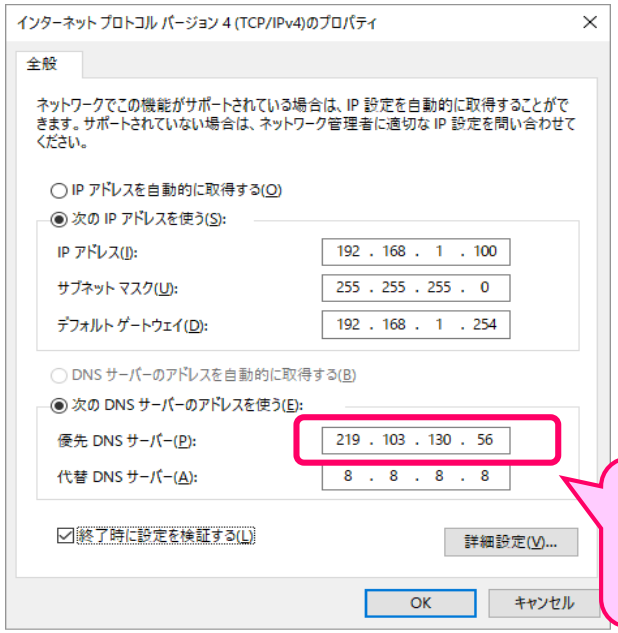
4 IPアドレス
103.28.248.95
でアクセス

Webサーバ
www.ntt.co.jp
103.28.248.95

2 www.ntt.co.jpの
IPアドレスは？

3 103.28.248.95 だよ

DNSサーバ
219.103.130.56



PCのDNS
設定

●DNS（Domain Name System）

DNSは、ホスト名（URL）を元に、ホスト（Webサーバ）のIPアドレスを教えてくれる仕組みです。
あらかじめクライアントに、DNSサーバのIPアドレスを設定、もしくはDHCPによる払い出しを受ける必要があります。

●OS（OperatingSystem）の種類

OS	バージョン(コードネーム)など
windows	Windows10、8.1、7、vista （HomeEdition、Profesional）
	Windows Server2016、2012… （StandardEdition、DatacenterEdition）
Linux	Redhat系、Debian系、Slackwave系
macOS	10.13 (HighSiera) 10.12 (Siera)、10.11など
android	8.1、8.0(oreo) 7.0、7.1-7.1.2(Nougat)など
IOS	11、10、9

●OS（OperatingSystem）の種類

OS（オペレ―ティングシステム）とは、コンピュータを動かすために必要な基本的な機能

例）
・キーボードから文字を入力する
・マウスやタッチパッドで操作する
・インターネットを見るためのブラウザソフトを起動する

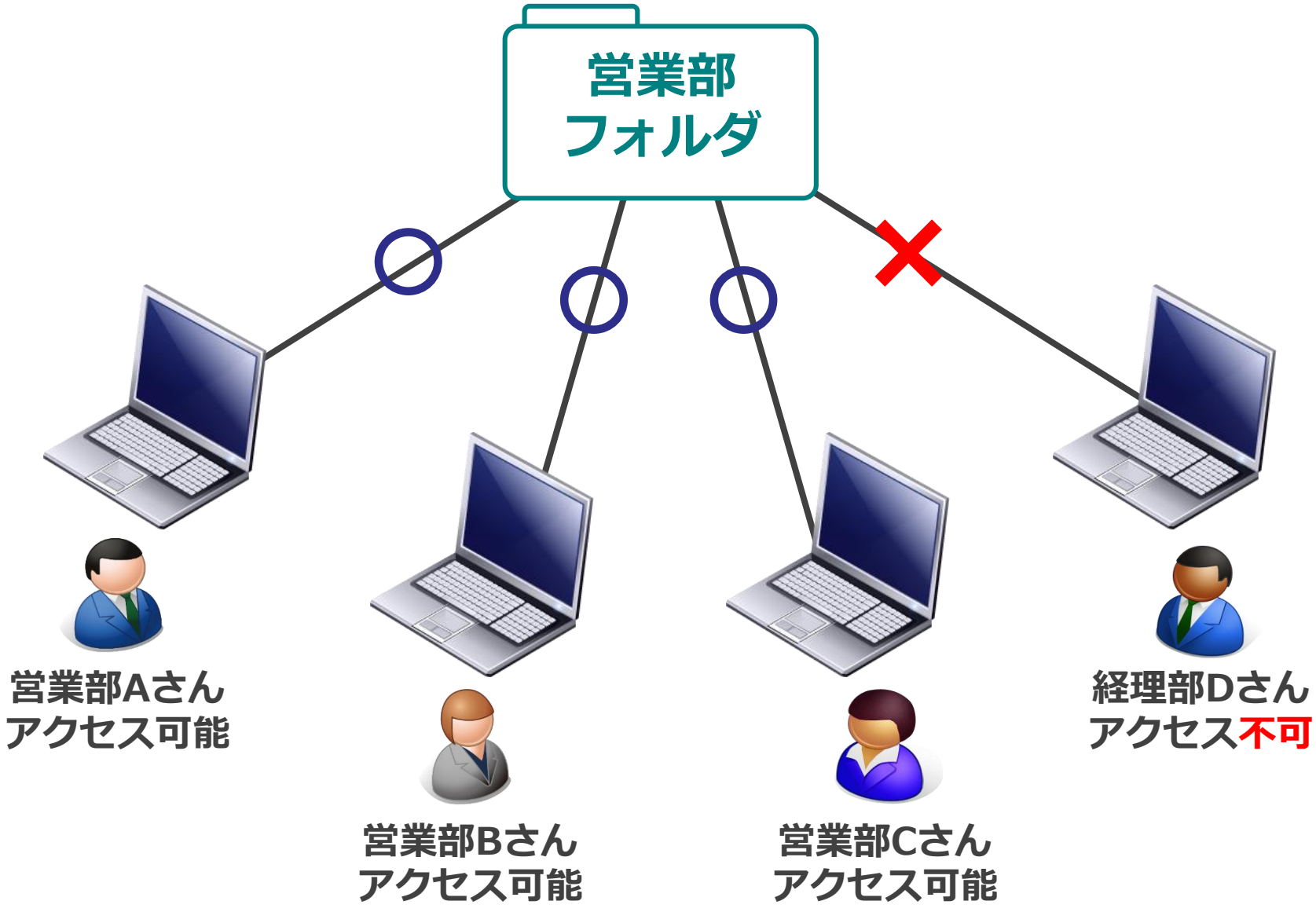
●ブラウザの種類

会社	ブラウザソフト	世界シェア(2018年)
Microsoft	IE	3.13%
	Edge	1.50%
Google	GoogleChrome	57.69%
Mozzila	FireFox	5.40%
Apple	Safari	14.79%

出典「StatCounter」
Feb2017-Feb2018
Browser　MarketShare　WorldWide

●ブラウザの種類

●ファイル共有


営業部
フォルダ
営業部Aさん
アクセス可能
営業部Bさん
アクセス可能
営業部Cさん
アクセス可能
経理部Dさん
アクセス不可

●ファイル共有

ネットワークを通じて１つのファイルを複数のコンピューターからも利用出来るようにする仕組みのことです。

ファイル共有を行うメリット
・１つのファイルを複数人で利用、管理出来る
・ファイルにアクセスする権限を設定できる

ファイル共有を行うデメリット
・初期設定に手間がかかる

●よく使われるWindowsコマンド

コマンド	内容	手順
cmd	コマンドプロンプトを起動する	スタートメニューのプログラムとファイルの検索に入力
ncpa.cpl	ネットワークアダプタ(NIC)の一覧画面を表示する	スタートメニューのプログラムとファイルの検索に入力
ipconfig	ネットワークアダプタ(NIC)のIP情報を表示・更新する。	コマンドプロンプトから入力

●よく使われるWindowsコマンド

【ipconfigのオプション】

/all	詳細なIP設定を表示する
/release	アダプタのIP設定を解放する（DHCPクライアントのときにのみ有効）
/renew	アダプタのIP設定を更新する（DHCPクライアントのときにのみ有効）
/flushdns	DNSキャッシュをクリアする
/displaydns	DNSキャッシュを表示する

●ICMP(Internet Control Message Protocol)

IPの「エラー通知」や「制御メッセージ」を転送するためのプロトコルです。

TCP/IPが実装されたコンピュータ間で、通信状態を確認するために使用されます。

ICMPはOSI参照モデルのネットワーク層で動作するプロトコルです。

●ICMP

pingやtraceroute(tracert)は、このICMPプロトコルを使用したプログラムです。

●ping

pingとは、おもにネットワークの疎通を確認するために使用されるコマンドです。

pingは、ICMPのechoコマンドを利用して、指定した相手先（IPアドレスまたはホスト名）に文字列を送り、その戻りの有無によりネットワークの接続が確認できます。

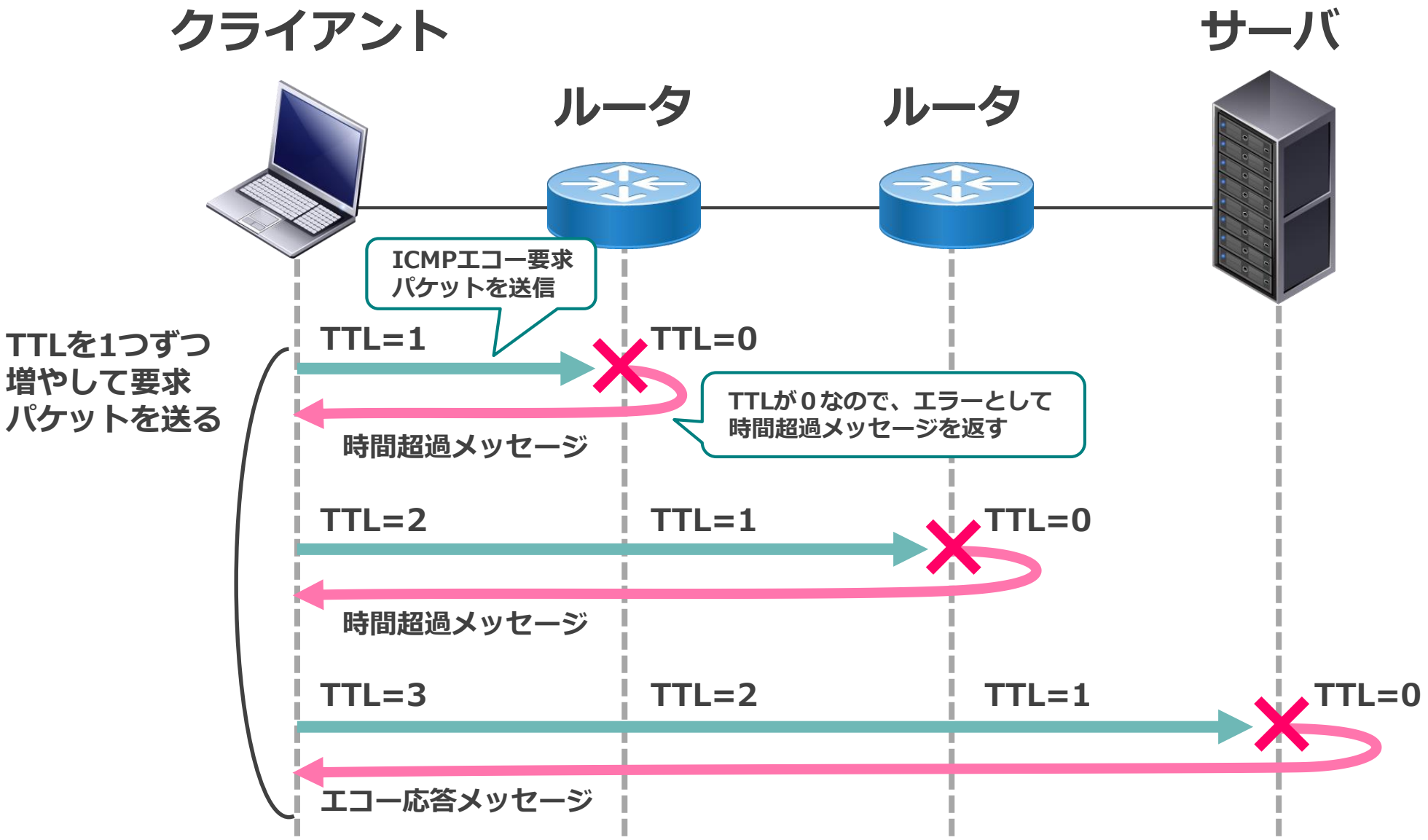
また、応答速度も表示されるため、ネットワークの速度を確認することもできます。

●ping

Windowsコマンドプロンプトにおける主なエラーメッセージ
・要求がタイムアウトしました【Request timed out 】
　宛先の機器と通信できない
・宛先ホストに到達できません【Destination net(host) unreachable】
　宛先ネットワーク(ホスト)にパケット転送(ルーティング)できない
・TTLが期限切れになりました 【TTL expired in transit 】
　TTL超過(128以上)によるエラー、一般的にルーティングループの可能性が高い

※pingのオプション
-t　中止するまでパケットを送信する
-n　パケットの送信回数を指定する（デフォルトは4回）
-l　送信するパケットのデータサイズを指定する（デフォルトは32Byte）

●traceroute / tracert



●traceroute / tracert

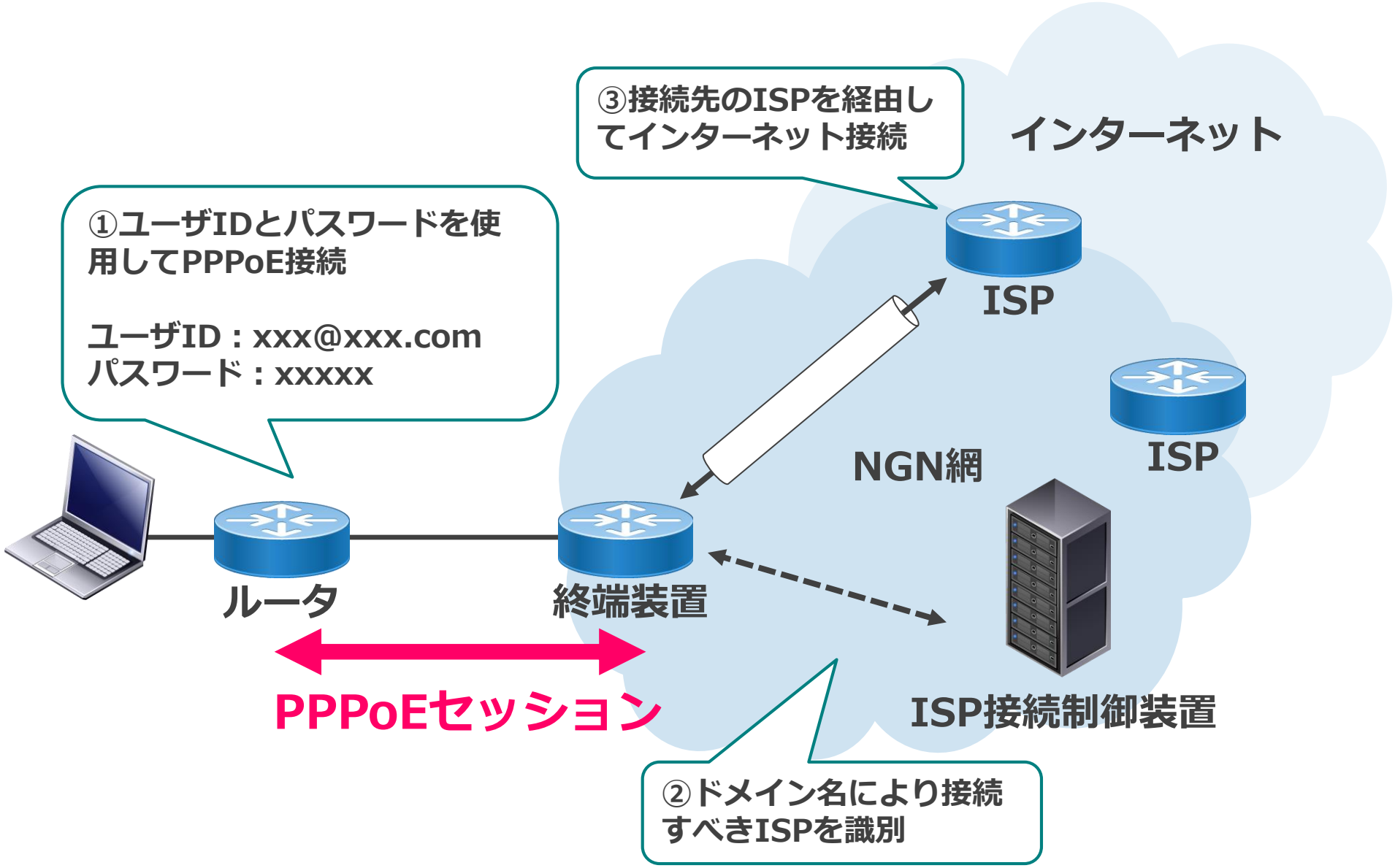
traceroute（Windowsでは「tracert」）コマンドは、あるホストから別のホストまでのネットワーク経路をリスト表示するコマンドです。経路とは、ホスト間を接続するルータという意味で、経路上にどのようなルータが位置しているかを表示することができ経路を確認することができます。

【TTL（Time to Live）】
ルータを通過できる最大回数を表しています。
（初期値：Windows 128 ,Linux 64 ,Solaris 255）（最大値：255)

※tracertのオプション
-d　　経路途中にあるルータの名前解決を行わない

インターネット接続技術

●PPP/PPPoE

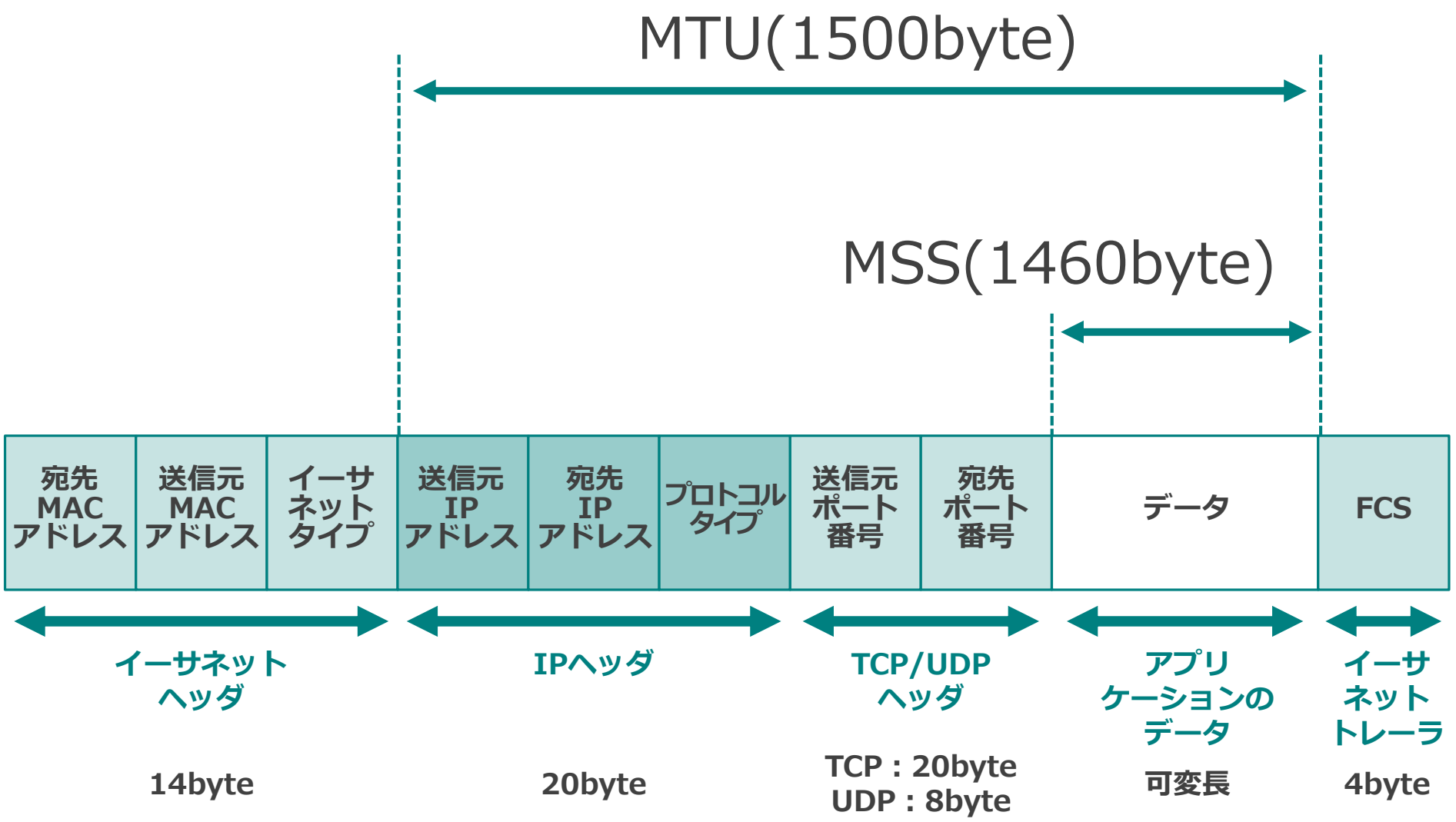

③接続先のISPを経由してインターネット接続
インターネット
①ユーザIDとパスワードを使用してPPPoE接続
ユーザID：xxx@xxx.com
パスワード：xxxxx
ISP
ISP
NGN網
ルータ
終端装置
PPPoEセッション
ISP接続制御装置
②ドメイン名により接続すべきISPを識別

●PPP/PPPoE

PPP（Point-to-Point Protocol）とは、ダイヤルアップ接続で用いられる2拠点間での通信を確立・維持するためのプロトコルです。
通信の状態を監視するLCP（Link Control Protocol）、IPアドレスの割り当てを行うNCP（Network Control Protocol）、認証プロトコル（PAP、CHAPなど）が含まれます。

PPPoE とは、Point to Point Protocol over Ethernet（Ethernet 経由のポイントツーポイント・プロトコル）を省略したものです。
PPPではなくPPPoEを利用するのは、PPPには電話で呼び出すための手順が規定されており、電話をかけない常時接続では利用できないからです。

●MTUとMSS



※物理ヘッダのプリアンブルは省略

●MTUとMSS

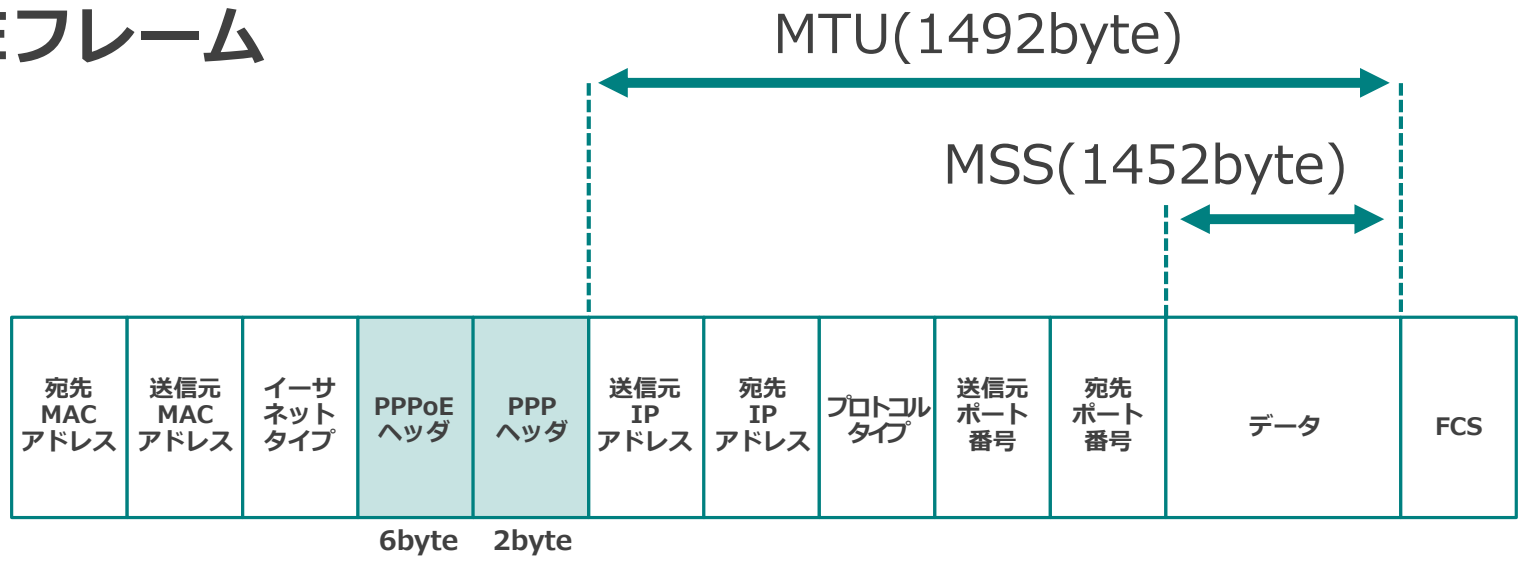
・MTU (Maximum Transmission Unit)MTUとは、一回のデータ転送にて送信可能なパケットの最大値のことです。Ethernetフレームが最大1518byteなので、Ethernetヘッダ(14byte)とFCS(4byte)を除く、1500byteがMTUサイズとなります。

・MSS（Maximum Segment Size)MSSとは、データの最大値のことです。Ethernetフレームが最大1518byteなので、Ethernetヘッダ（14byte)・FCS(4byte)・TCPヘッダ(20byte)・IPヘッダ(20byte)を除く、1460byteがMSSサイズとなります。

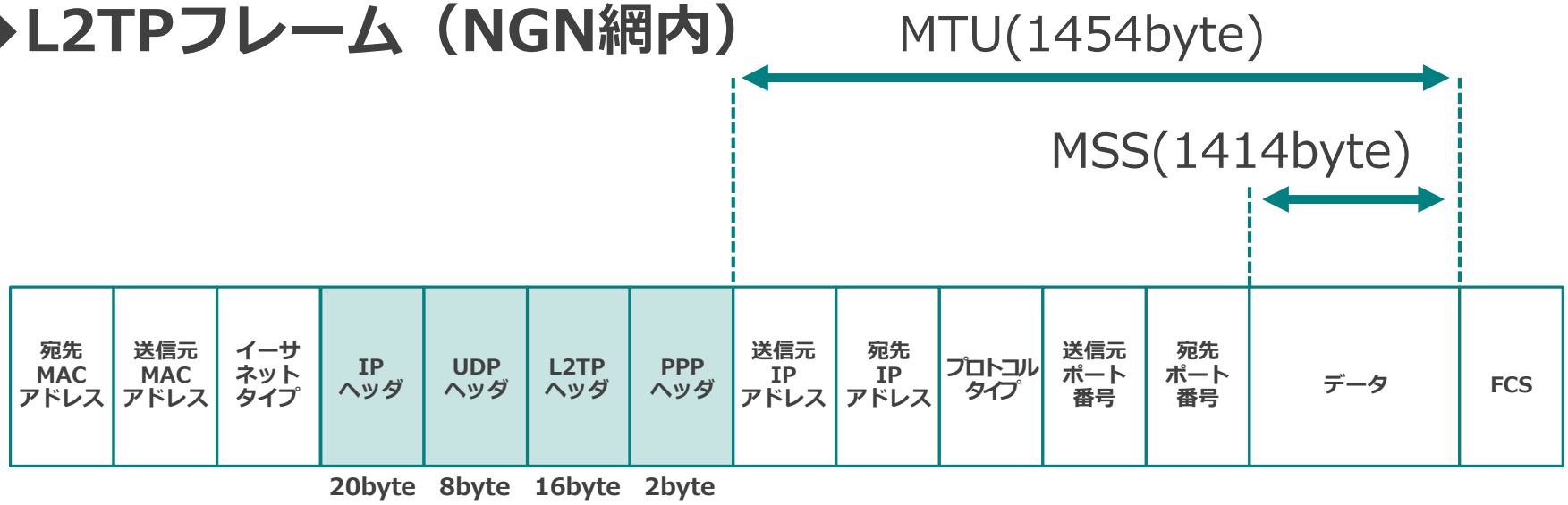
※パケットがルータを通過する際、送信先の伝送路のMTUサイズよりパケットのMTUサイズが大きい場合、フラグメント（パケット分割）が発生する場合があります。

●PPPoE/L2TP(NGN網内）フレーム

◆PPPoEフレーム



◆L2TPフレーム（NGN網内）



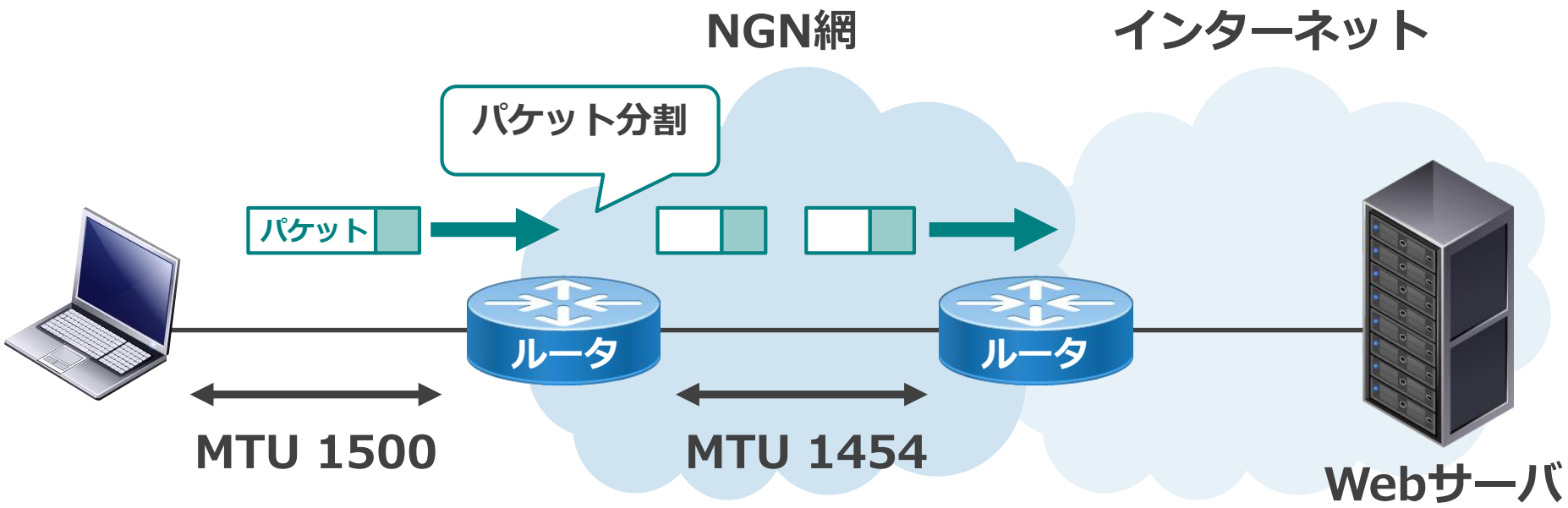
●PPPoE/L2TP(NGN網内）フレーム

【PPPoEフレーム】
PPPoE接続（MTU：1492byte）はNTT収容ビルにある集線装置までで、その先(NGN網内)はL2TP接続となる。

【L2TPフレーム（NGN網内）】
L2TP接続でのMTU値は1454byteとなる、よってNGN網使用時はMTU値が最も小さい値である1454byteをルータのインターフェースに設定します。

●フラグメント

パケットがルータを通過する際、送信先の伝送路のMTUサイズよりパケットのMTUサイズが大きい場合、**フラグメント（パケット分割）**が発生する場合があります。

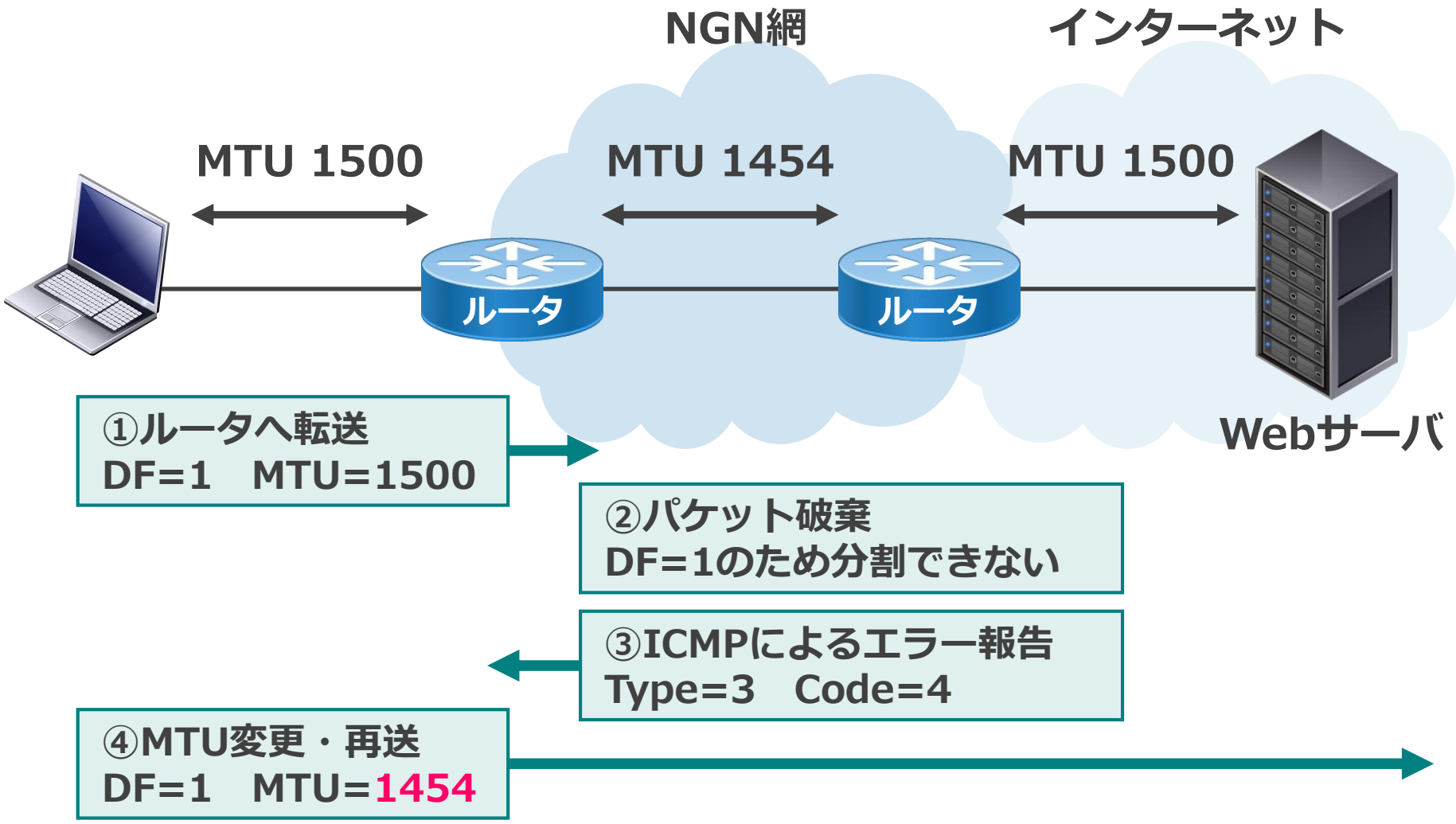


●フラグメント

フラグメントが多発すると、パケットの分割処理や再組立て処理を行うためのルータの処理が増大し、スループットの低下、または分割できない場合にはパケット損失につながります。
その場合、音声通信での音声の乱れや、Web閲覧でホームページが一部しか表示されない（例　画像部分が表示されない）等の事象が発生することがあります。

そのため、ネットワーク遅延等のトラブル防止のためにも、あらかじめMTUとMSSを中継装置（ルータなど）やクライアント、サーバで調整するのが一般的です。

●Path MTU Discovery



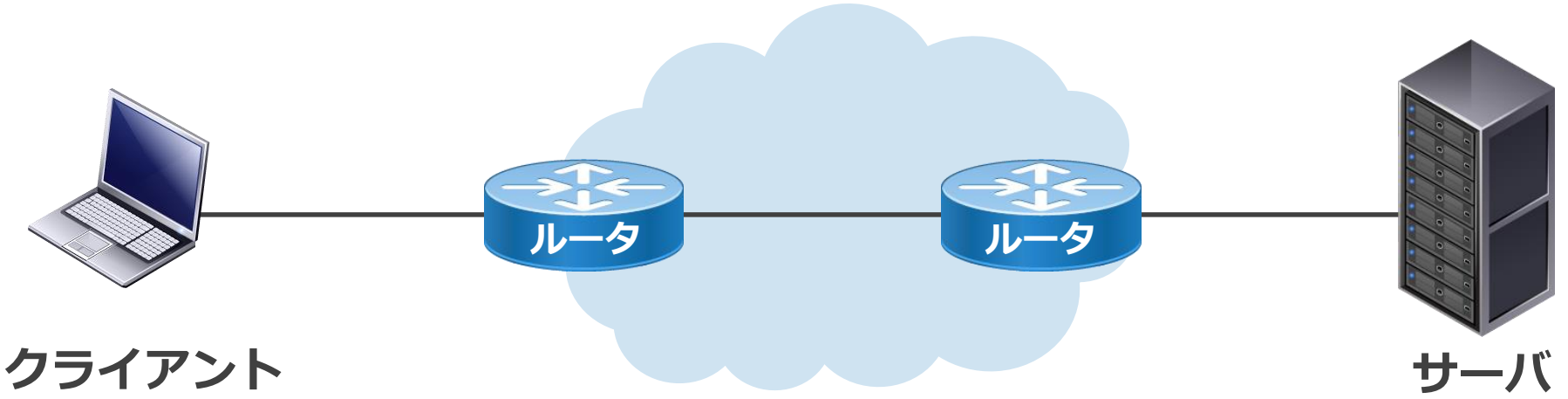
●Path MTU Discovery

Path MTU Discoveryとは、経路のMTUサイズを検出する機能です。TCP通信の経路上にあるリンクの最小MTU値を検出し、送信元へICMPを使い最小MTU値の情報を送信します。

経路上のルータは、パケットサイズが大きくDFビットが設定されている場合、パケットを破棄してICMPを送信元へ送信します。
ICMPを受信したホストはMTU値を調整して、再度パケットを転送し正常に通信するようになります。
DFビットが設定されていない場合はルータがフラグメントを行いパケットを送信することができますが、その場合は、フラグメント処理のためにスループットが落ちたり、処理不可になることがあります。

※Path MTU Discoveryのブラックホール問題
適正なMTU値を伝達するためのICMP（Ping）を送信元に送信しない設定、または途中の経路でファイアウォール等によりICMPがフィルタリングされている場合には、適切なMTU値が伝達できない状況が発生します。そのため適切なMTU値に変更されないまま（MTU=1500）送信されることで、ルータでのパケット破棄を繰り返し、通信できない状態に陥ります。

●TCPの3ウェイハンドシェイク



①SYN

あなたと通信してもいいですか？

②SYN／ACK

いいですよ！こちらからも通信していいですか？

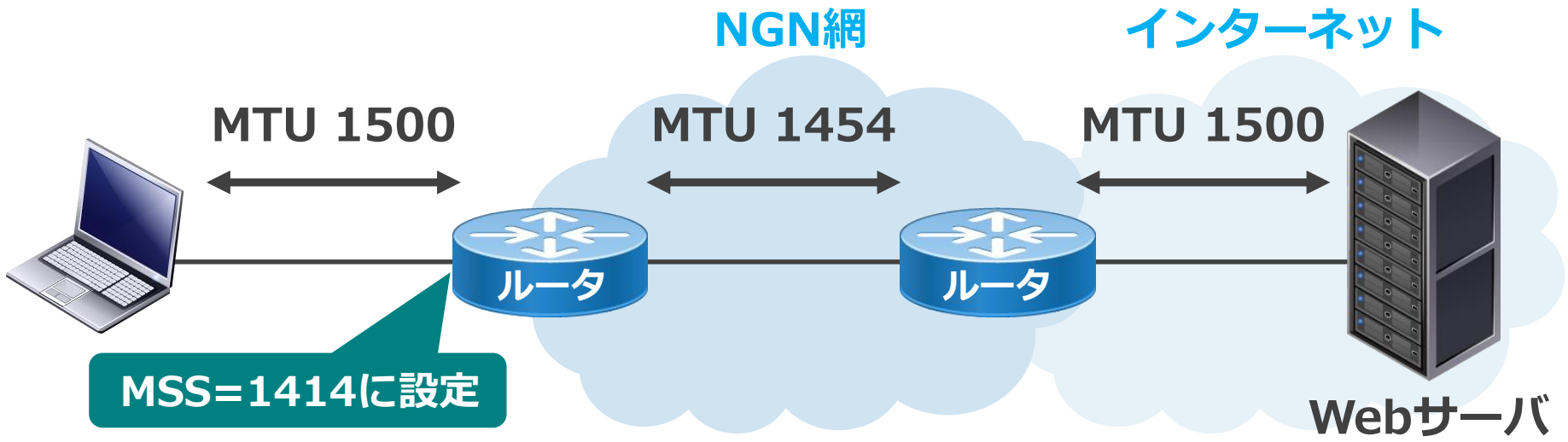
③ACK

OK！

●TCPの3ウェイハンドシェイク

TCPは通信を始める前に必ず3ウェイハンドシェイクを行います。
3ウェイハンドシェイクは3回のやりとりによってコネクションを確立します。

●3ウェイハンドシェイクによるMSS値の決定



①SYN
MSS=1460

①SYN
MSS=1414

ルータが設定されているMSS値に書き換える

②SYN／ACK
MSS=1460

MSS値は小さい値の1414でOKですよ

③ACK
MSS=1414

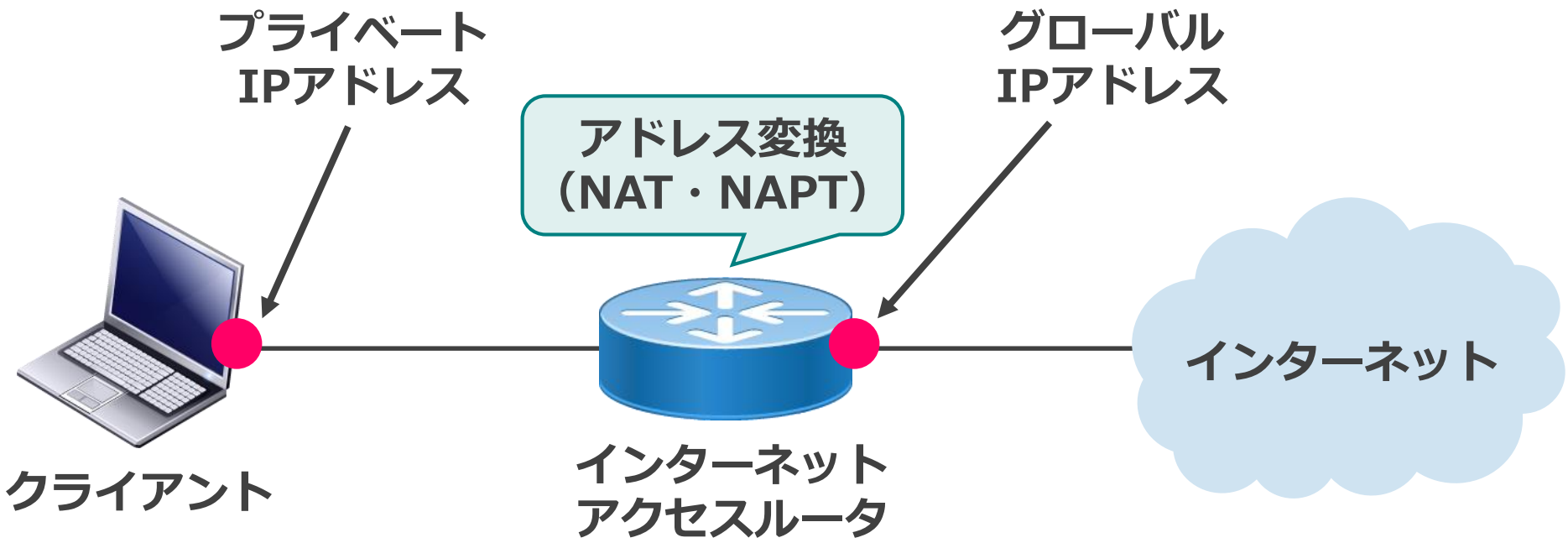
MSS値は1414にしますね

●3ウェイハンドシェイクによるMSS値の決定

TCPでは3ウェイハンドシェイク時にMSS値の決定も行います。

経路上のルータなどに、あらかじめ通信経路の最小MSS値の設定をしておくことで、
フラグメントの発生を防ぐことができます。

●アドレス変換（NAT・NAPT）

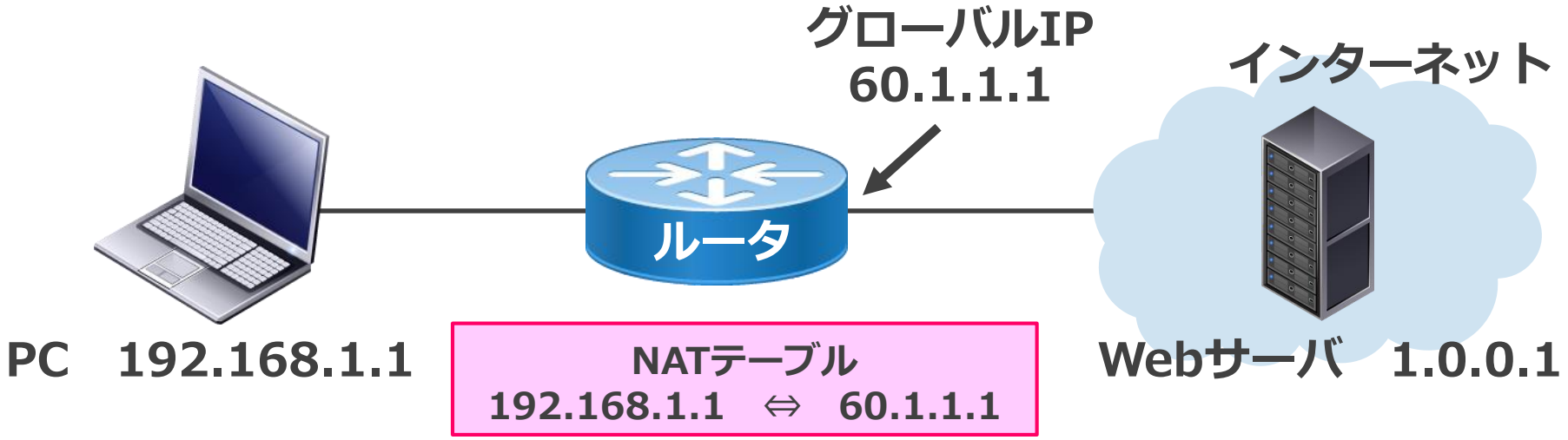


●アドレス変換(NAT・NAPT)

NATは、IPアドレスを変換する技術です。一般的にはプライベートIPアドレスをグローバルIPアドレスへ変換する技術です。

プライベートIPアドレスではインターネットへ接続できないため、グローバルIPアドレスに変換する必要があります。

●NAT（Network Address Translation）



ルータを通過する際に、1対1のNATテーブルを作成します。

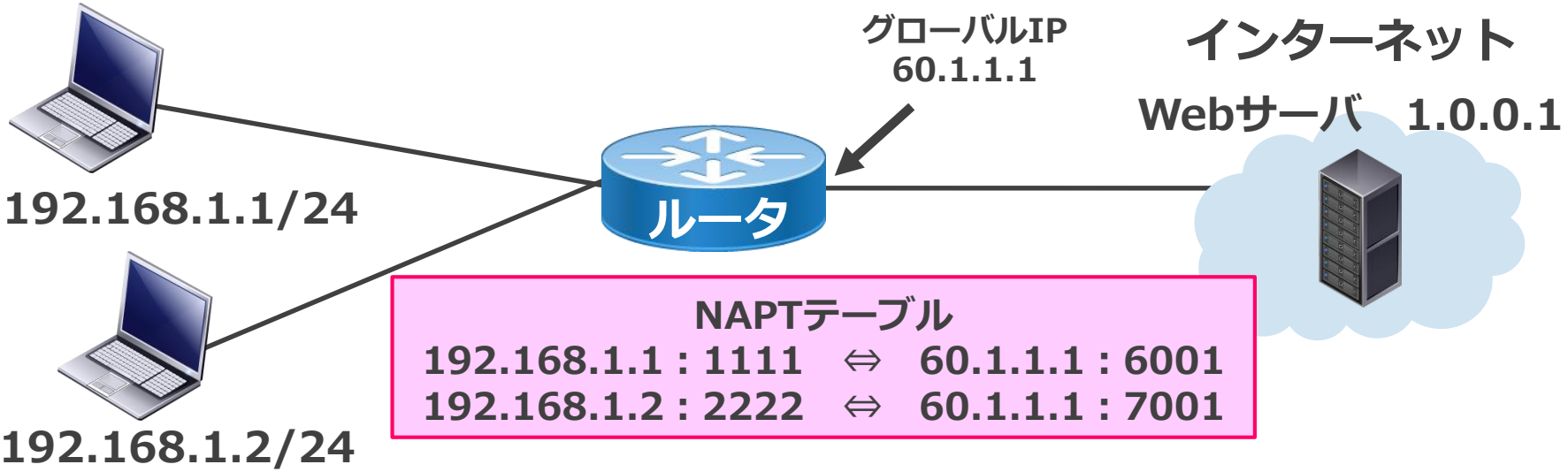
NATテーブルを参照し、IPヘッダを変換します。

●NAT(Network Address Translations)

【PC → サーバ】送るIPヘッダ
1. PCが、サーバへデータを送るため、ルータへパケットを送ります。
2. ルータが、プライベートIPをグローバルIPへ変換します。
3. ルータが、どのように変換したかNATテーブルに記録します。
4. ルータが、宛先へパケットを転送します。
5. サーバが、パケットを受け取ります。

【サーバ → PC】送られてきたIPヘッダ
6. サーバから返答が返ってきます。このとき、宛先IPは変換後のIP(60.1.1.1)です。
7. 受け取ったルータが、宛元IPアドレスをNATテーブルを元に変換します。
8. ルータが、役割が終ったNATテーブルの記録を削除します。
9. ルータが、変換後のIPアドレスに基づき、ホストへパケットを転送します。
10. PCが、パケットを受け取ります。

●NAPT（Network Address Port Translation）



NAPTテーブル

192.168.1.1 : 1111 ⇔ 60.1.1.1 : 6001
192.168.1.2 : 2222 ⇔ 60.1.1.1 : 7001

宛先IP	宛先Port	送信元IP	送信元Port
1.0.0.1	80	192.168.1.1	1111

IPアドレス変換にポート番号も含めて変換することで、複数の端末を同時接続させることができる

宛先IP	宛先Port	送信元IP	送信元Port
1.0.0.1	80	60.1.1.1	6001

宛先IP	宛先Port	送信元IP	送信元Port
60.1.1.1	6001	1.0.0.1	80

宛先IP	宛先Port	送信元IP	送信元Port
192.168.1.1	1111	1.0.0.1	80

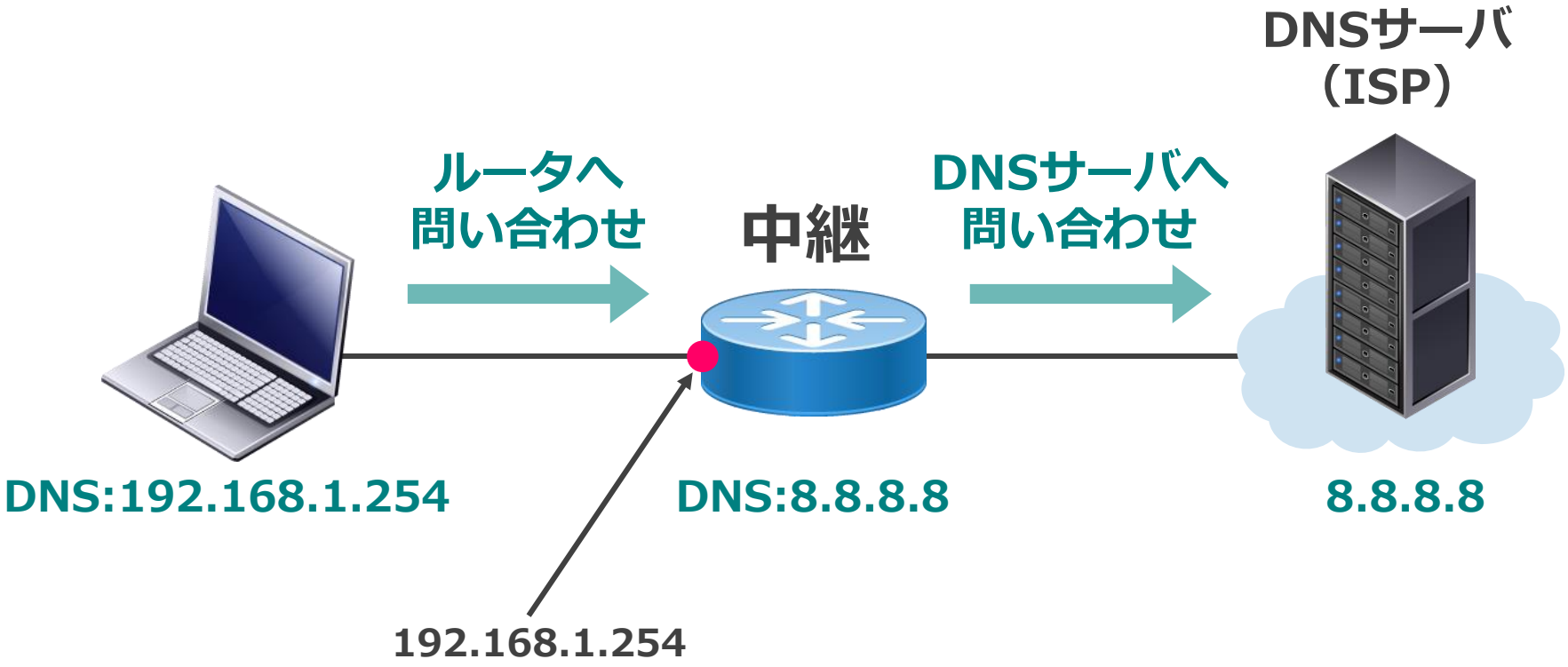
●NAPT(Network Address Port Translations)

IPアドレス変換にポート番号も含めて変換することで、複数の端末を同時接続させることができる。

【PC1 → サーバ】送るIPヘッダ
1. PC1が、サーバへデータを送るため、NAPT機能のあるルータへパケットを送ります。
2. ルータが、NAPT機能により、プライベートIPをグローバルIPに、さらにポート番号を変換します。
3. ルータが、どのように変換したかNAPTテーブルに記録します。アドレスとポート番号がセットで記録されます。
4. ルータが、宛先へパケットを転送します。
5. サーバが、パケットを受け取ります。

【サーバ → PC1】送られてきたIPヘッダ
6. サーバから返答が返ってきます。
7. このとき、宛先は、変換後の送信元アドレスと送信元ポートです。
8. 受け取ったルータが、NAPTテーブルを参照して、アドレスをポート番号を変換します。
9. ルータが、役割が終ったNAPTテーブルの記録を削除します。
10. ルータが、変換後のアドレスに従い、パケットをPC1へ転送します。
11. PC1がパケットを受け取ります。

●DNSリレー

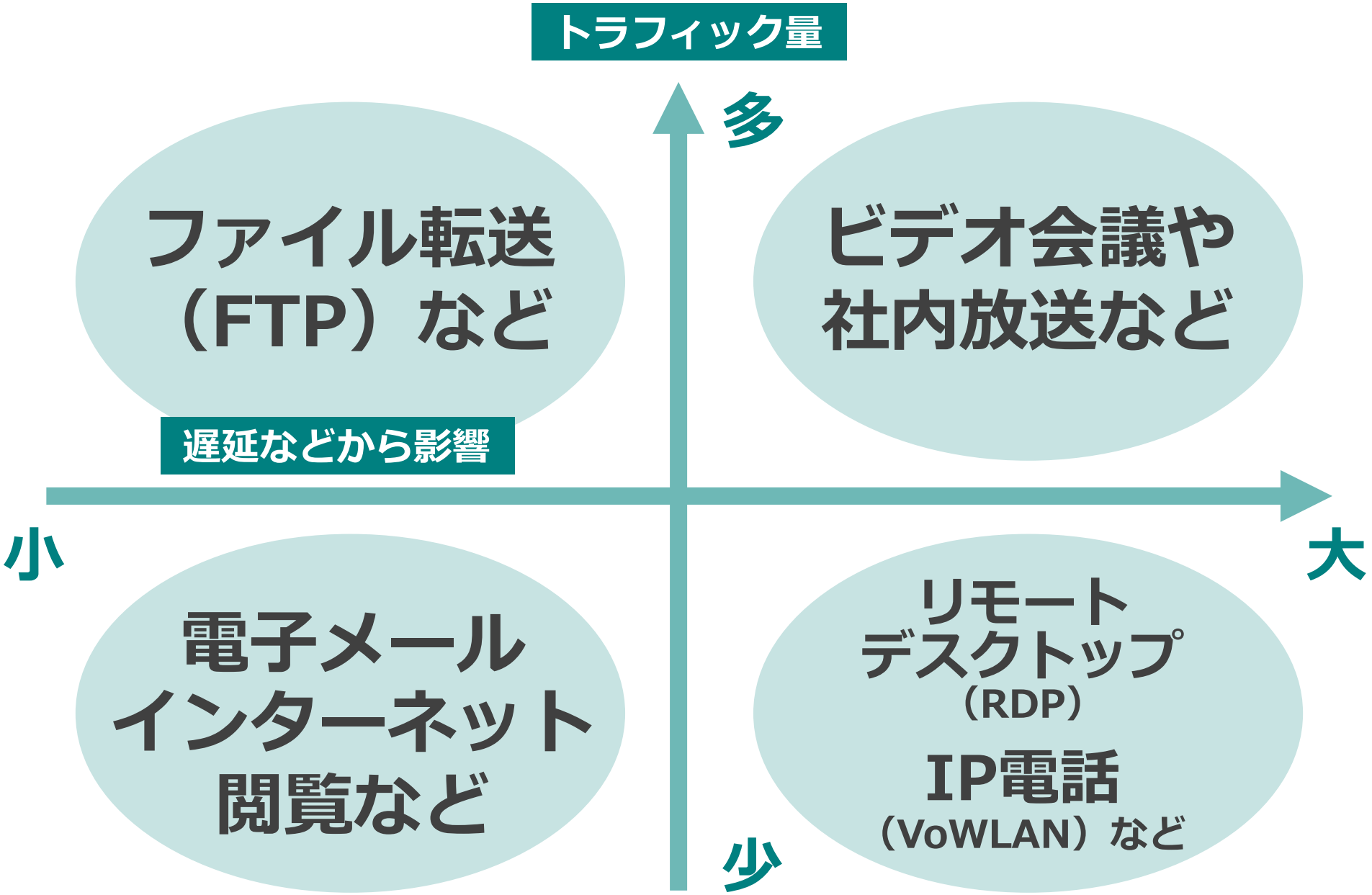

DNSサーバ
（ISP）
ルータへ
問い合わせ
中継
DNSサーバへ
問い合わせ
DNS:192.168.1.254
DNS:8.8.8.8
8.8.8.8
192.168.1.254

●DNSリレー

DNSクライアントからの問い合わせをDNSサーバに中継するルータの機能です。

無線LAN

●無線LANの利用環境


トラフィック量
多
少
小
大
遅延などから影響
ファイル転送
（FTP）など
ビデオ会議や
社内放送など
電子メール
インターネット
閲覧など
リモート
デスクトップ
（RDP）
IP電話
（VoWLAN）など

●無線LANの利用環境

企業内の業務で生じるトラフィックの特徴を把握することで、無線LAN環境での注意すべきポイントが見えてきます。

FTPによるファイルのアップロード・ダウンロードする場合、トラフィックの量は多くなりますが、パケットに多少遅延が発生したとしても影響は比較的小さいものです。

しかし、RDPによるリモート接続の場合、トラフィック自体は大きくありませんが遅延による影響が問題になります。

遅延が発生することで、マウスを移動させても画面にすぐに反映されなくなり、様々な操作の時間がかかり誤操作の原因にもつながります。

また、無線LANを使用するIP電話（VoWLAN）も同様に、遅延が発生すると相手の音声が遅れて聞こえたり、急に途切れたりして会話に支障が出ます。

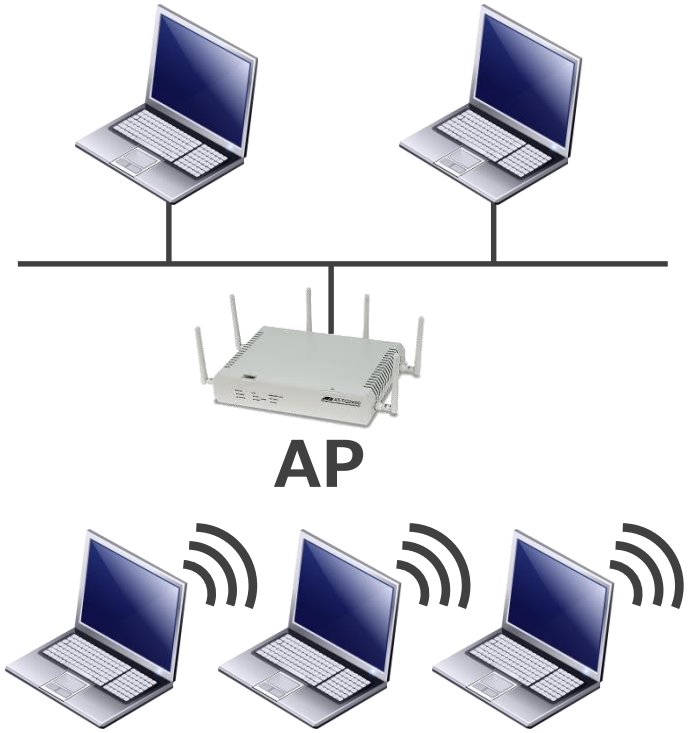
●無線LAN動作のポイント

- 1台のクライアントのみがデータ送信可能で、他のクライアントは待機する
- 無線LANの速度は、1台のアクセスポイントに所属する全てのクライアントで共有する
- 思ってもいない所に電波は到達する
- 他の電波の影響を受ける
- 受信電波の強弱によりクライアント側で自動的に速度調整が行われる
- 物理的なセキュリティが確保できないため、論理的なセキュリティが必要となる

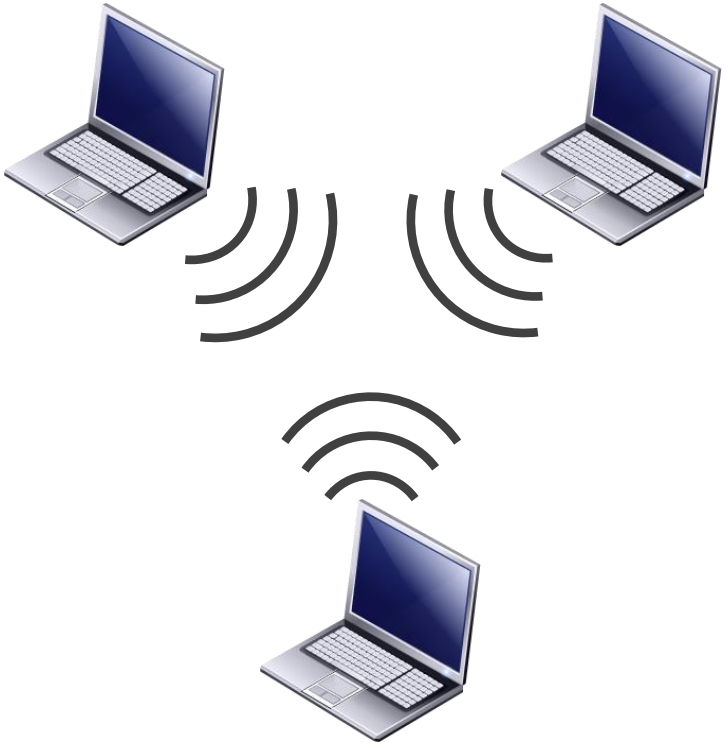
●無線LAN動作のポイント

●無線LANの利用形態

インフラストラクチャモード



アドホックモード



●無線LANの利用形態

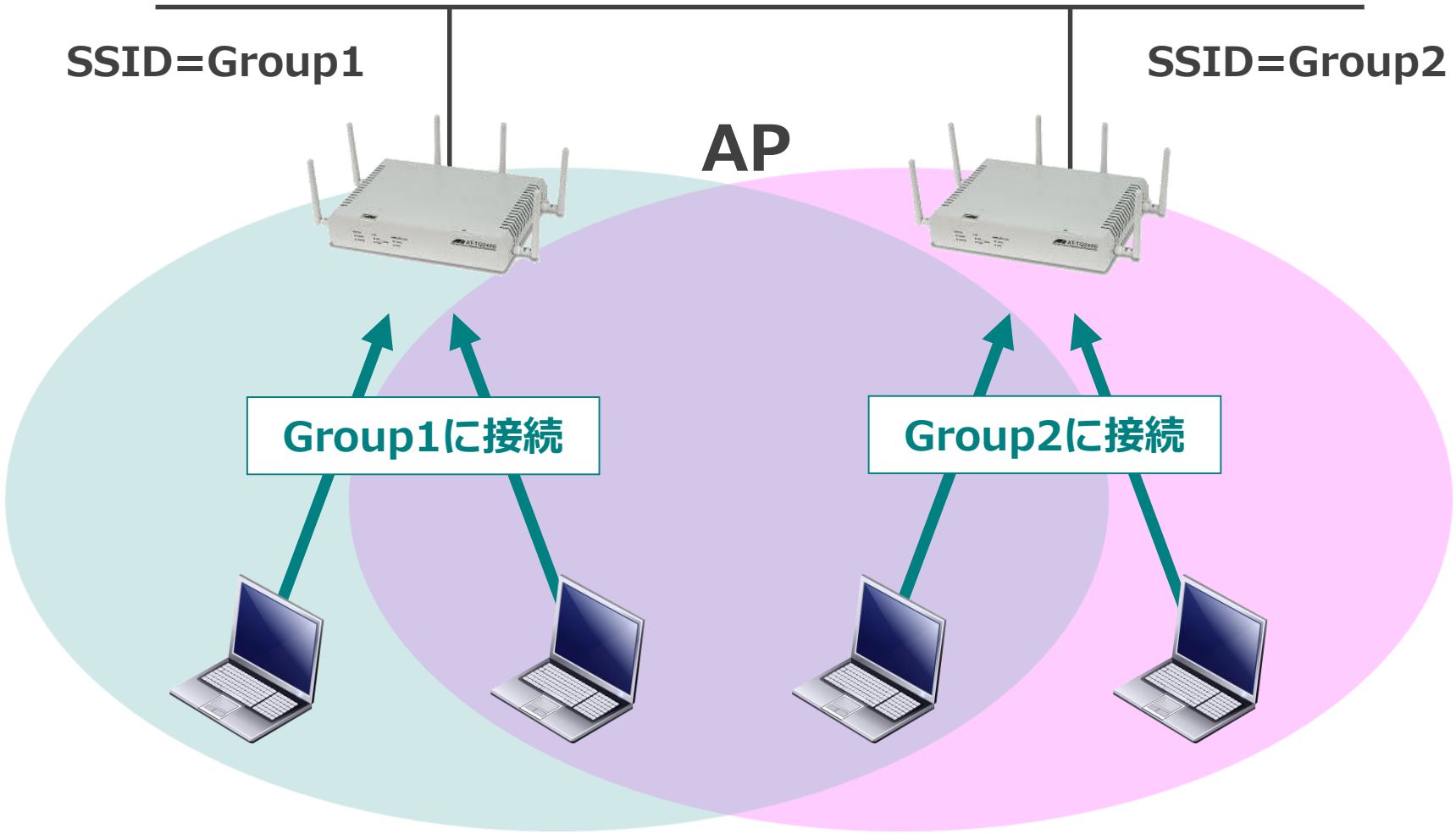
【インフラストラクチャモード】

ネットワークに接続した無線LAN用のアクセスポイントを経由して、各クライアントが有線LANやインターネットに接続する方式です。一般に無線LANといえば、この形態で使用されるケースが多いです。

【アドホックモード】

無線LANクライアント同士が直接通信する方式です。インフラストラクチャモードと比較すると、アクセスポイントが不要というメリットがあり単純な通信として利用されます。

●SSID(Service Set ID)



●SSID(Service Set ID)

SSIDとは、無線LANを利用する利用者が接続する無線LANサービスを指定し、接続するためのIDです。

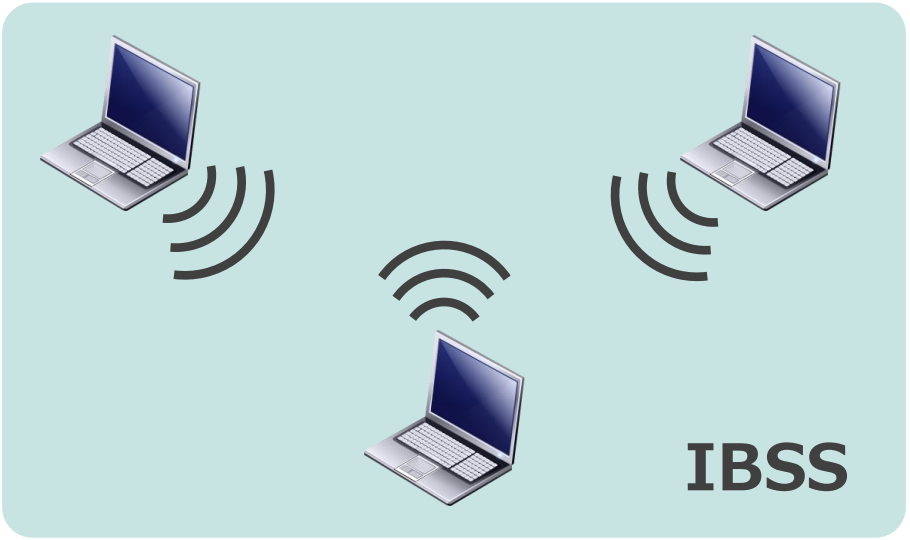
無線LANの場合、利用者が接続したいアクセスポイントを選択「アソシエーション」を確立していくことが必要となります。

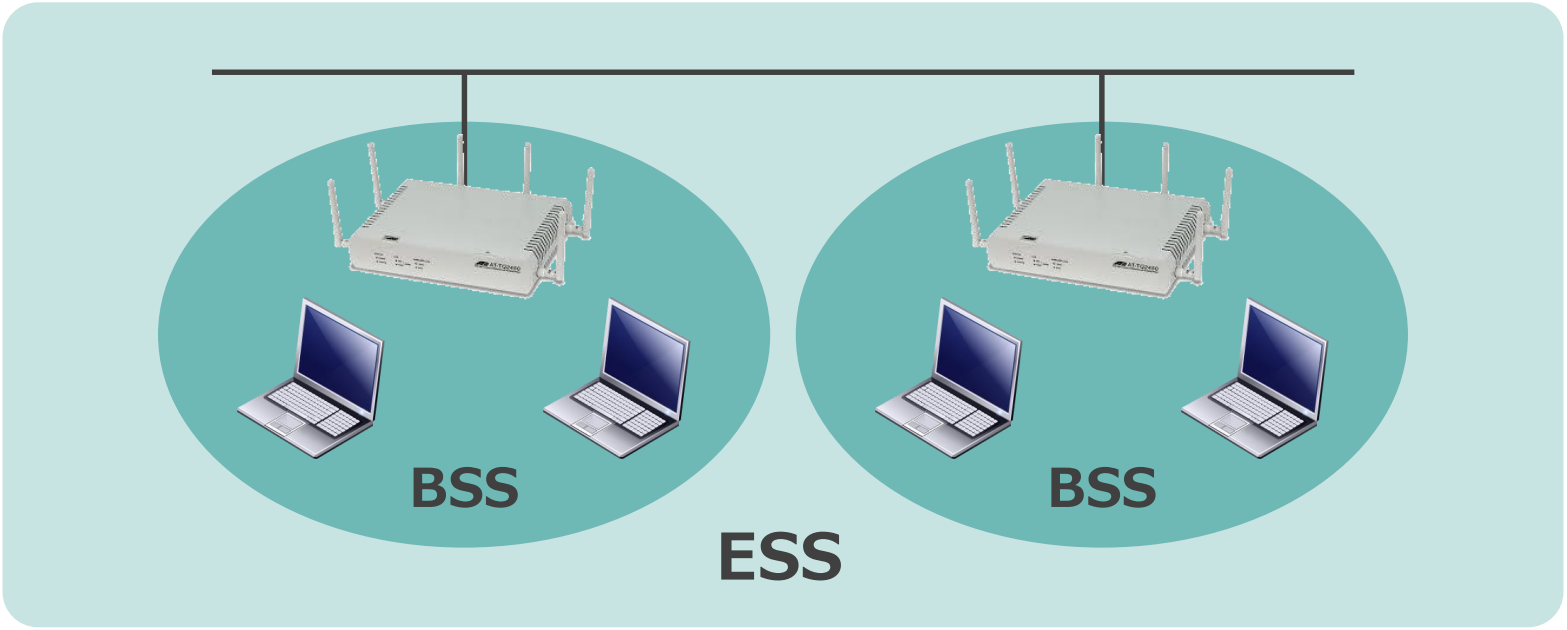
このため論理的に接続するアクセスポイントを識別できるようにSSIDをアクセスポイントに事前に設定します。

このSSIDはアクセスポイントから定期的（デフォルトでは1/10秒毎）に通知され、クライアントから接続可能なアクセスポイントの存在を常にリアルタイムで把握できるようになっています。

クライアントはこのSSIDを識別子としてアクセスポイント、およびその先にある有線ネットワークへの接続を行います。

●サービスセットの種類





●サービスセットの種類

【IBSS（Independent Basic Service Set）】
アドホックモードでの集合単位

【BSS（Basic Service Set）】
1アクセスポイントと配下のクライアントの集合

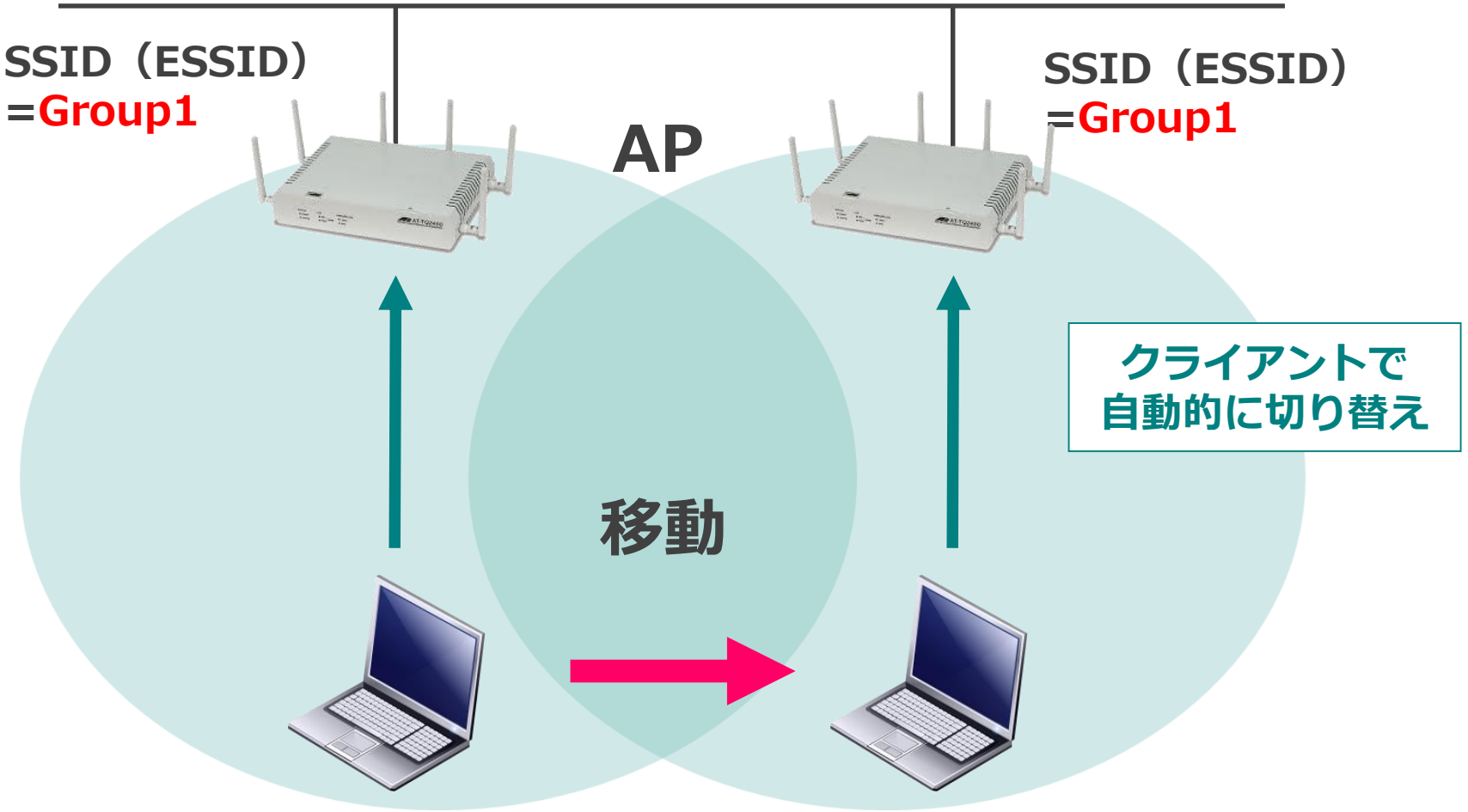
【ESS（Extended Service Set）】
複数のアクセスポイントで、一つのグループを形成する場合の集合

【BSSID（Basic Service Set Identifier）】
アクセスポイントの識別子（MACアドレス）通常はあまり意識しないID

【ESSID（Extended Service Set Identifier）】
SSIDと略される場合が多い

●ローミング（ハンドオーバー）

同一のSSID名が複数のAPで提供されている場合、クライアントは
電波の状態によって自動的にAPを切り替える



●ローミング（ハンドオーバー）

複数のアクセスポイントが同じSSID名を通知することが許されています。

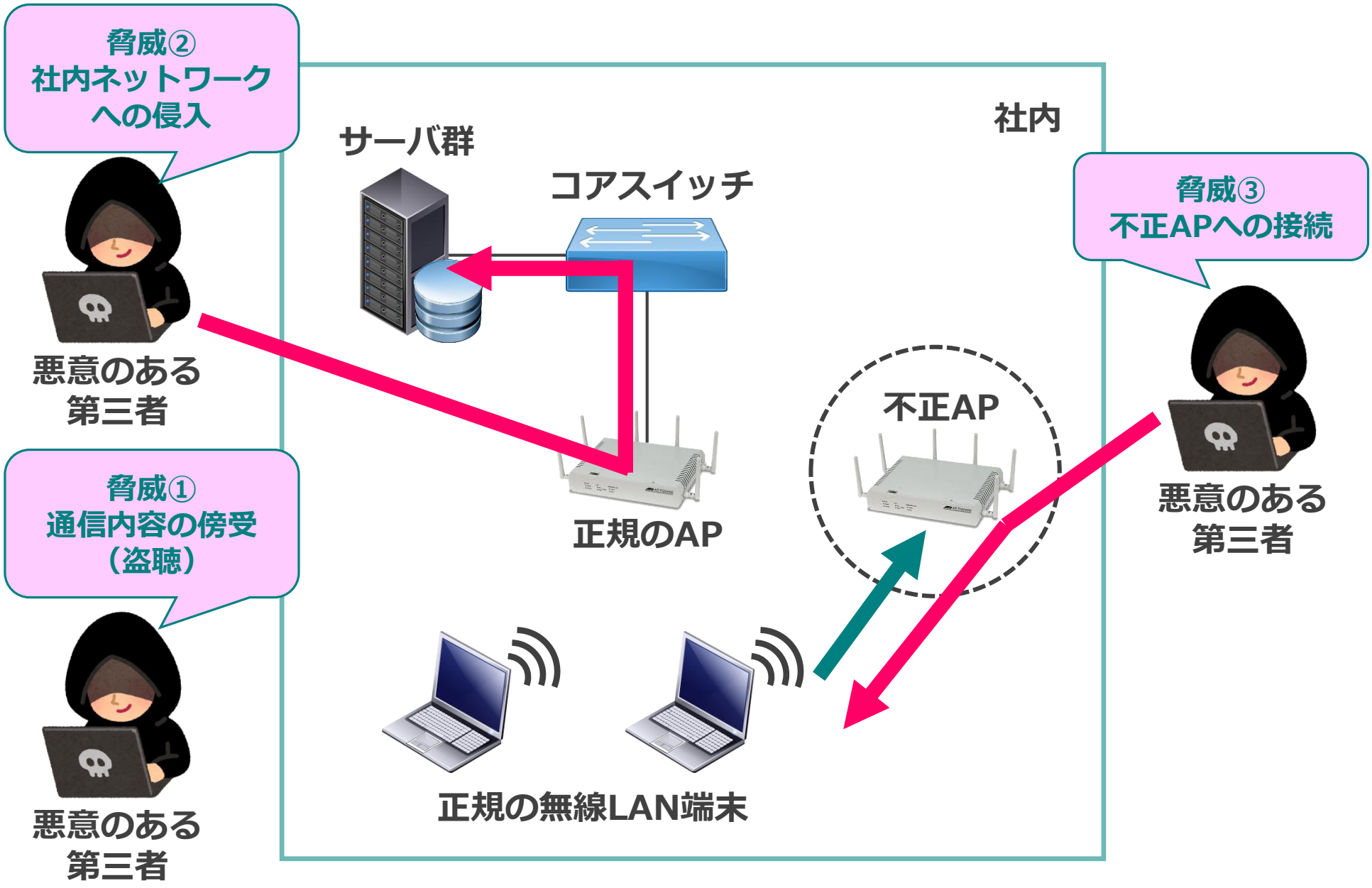
この機能を利用することで、物理位置に関係なく同一のサービス（暗号化、認証、所属サブネットなど）を複数のアクセスポイントで共有して提供することができます。

クライアントは電波状況がもっとも良好なアクセスポイント（BSSID）に最初に接続します。

また、このクライアントが物理的に移動し、より良い電波状況で同じSSIDを提供するアクセスポイントを検出した場合、サービスはそのままに、自動的に新しいアクセスポイントに移動することができます。

この機能をローミング、またはハンドオーバーと呼びます。

●無線LANにおける脅威



●無線LANにおける脅威

【脅威①通信内容の傍受（盗聴）】

悪意のある第三者が電波をキャッチして、ネットワークでやり取りされているデータを解読することです。無線LANの脅威の中でも最も発生しやすいと考えられます。

【脅威②社内ネットワークへの侵入】

建物外に漏れ出た電波を利用して行われます。悪意のある第三者が何らかの方法で社員のIDとパスワードを入手して社内ネットワークに侵入すると、データの改ざんや破壊を行う可能性があります。

【脅威③不正なアクセスポイントへの接続】

社内ネットワークに対して、システム管理者が知らないうちに接続されたアクセスポイントを使った攻撃のことです。社員が勝手にアクセスポイントを設置した場合などのケースが該当します。社員が勝手に設置したアクセスポイントは、きちんとした暗号化や認証の設定がされておらず、セキュリティレベルが低いことが多いです。こうしたアクセスポイントを悪意のある第三者に利用されると、社内から様々なデータを抜き出されたり、端末の破壊攻撃を実施されたりする恐れがあります。

●脅威に対するセキュリティ対策

◆不正アクセス防止
- ・SSID（ESSID）のステルス化
- ・MACアドレスフィルタリング
- ・不正APの検知

◆認証強化で不正な接続を遮断
- ・PSK（共通鍵方式）
- ・IEEE802.1X認証

◆電波盗聴から守る
- ・データの暗号化

●脅威に対するセキュリティ対策

【 SSID（ESSID）のステルス化】

アクセスポイントから送信されるビーコン信号で、SSID名を通知しないようにします。※無線接続時ビーコン信号以外にSSIDを含むフレームが存在するため、ステルスモードでも読み取られる可能性があります。

【 MACアドレスフィルタリング】

無線LAN端末のMACアドレスを登録しておき、登録済みのクライアントからのみ接続を許可します。※無線送受信パケットのMACアドレスが盗聴された場合、「なりすまし」による不正アクセス被害を受ける可能性があります。

【不正APの検知】

主に集中管理型（WLC）の機器が備える機能です。予め登録してあるフロア図面上に、不正APを表示したり、APがつながっているスイッチのポートを自動的に遮断することができます。

【 PSK（Pre-Shared-Key）】

無線LAN端末とアクセスポイントとの認証のために使用する共通鍵（認証キー）です。

【 IEEE802.1X認証】

RADIUSサーバによるEAPを使用したクライアント認証機能。

【データの暗号化】

WEP、WPA（TKIP）、WPA2（AES）などの暗号化アルゴリズム。※WEPとTKIPは2014年以降、暗号解読成功例が報告されておりWi-Fi Allianceでは使用を中止する予定となっております。

●無線LANのセキュリティ規格

規格	暗号化方式	アルゴリズム	暗号鍵	サポート認証技術
WPA2	AES	AES	128ビット	PSK、802.1X
	TKIP	RC4	128ビット	PSK、802.1X
WPA	AES	AES	128ビット	PSK、802.1X
	TKIP	RC4	128ビット	PSK、802.1X
WEP	WEP	RC4	64/128ビット	802.1X

●無線LANのセキュリティ規格

無線LANのセキュリティ規格にはWEP、WPA、WPA2の3種類があります。現在一般的に使われているのものは、WPAやWPA2です。それぞれ暗号化方式としてTKIPとAESがあり、AESの方が暗号強度が高いとされています。WPA2のAESを採用することで、強固なセキュリティを実現できます。

【WEP】

無線LANの規格が策定された時に、有線LANと同程度のセキュリティを目指して作られた暗号化方式。パケットを多数キャプチャして解析すると暗号鍵が分かり、通信内容を解読できてしまうという脆弱性が見つかっています。現在では、セキュリティレベルが低いとされているため使用を避けるべきです。

【WPA（WPA2）】

無線LAN機器の認定プログラムを定める業界団体「Wi-Fiアライアンス」が、IEEE802.11iが出来上がる前に策定したセキュリティ規格。WPA2はIEEE802.11iに完全に準拠した形で策定されたセキュリティ規格。

【TKIP】

暗号鍵を一定時間ごとに自動的に更新する暗号化方式。

【AES】

暗号鍵の生成や改ざん検知にCCMP方式を使用した暗号化方式。

●PSK（Pre-Shared-Key）

アクセスポイントと
同じ認証鍵を持って
いれば認証成功

無線LAN端末

①接続要求

②共通鍵の確認

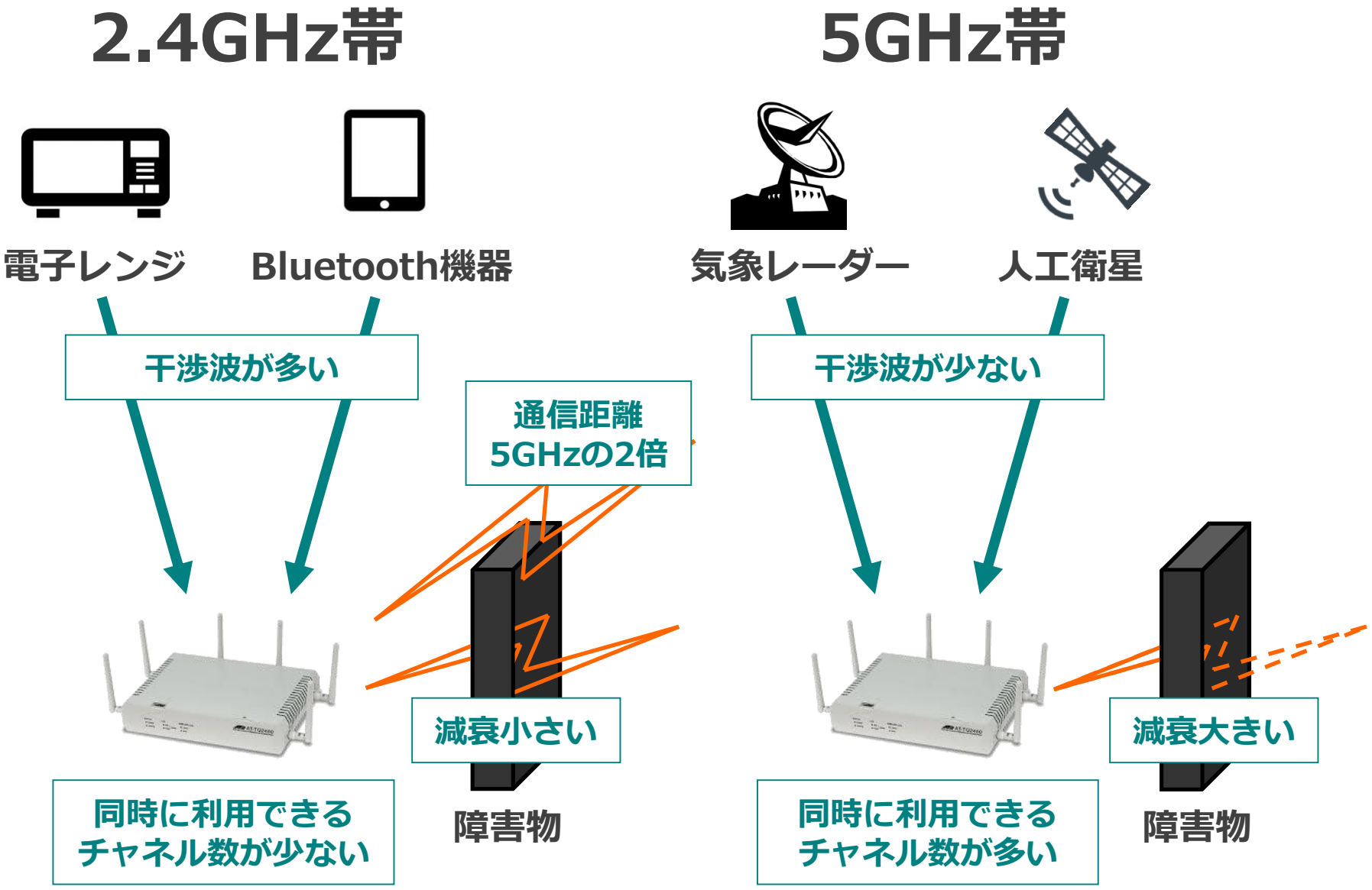
AP

③接続OK

社内
LAN

●PSK（Pre-Shared-Key）

●無線LANの周波数帯域



●無線LANの周波数帯域

2.4GHz帯は、無線LAN機器以外にも下記のような様々な機器で使用されています。

・電子レンジ

・アマチュア無線

・医療機器

・Bluetooth

・VICS（カーナビ）

そのため、周辺にこれらの機器がある場合には、無線LAN通信中に他の機器からの干渉の影響を受ける可能性があることに注意する必要があります。

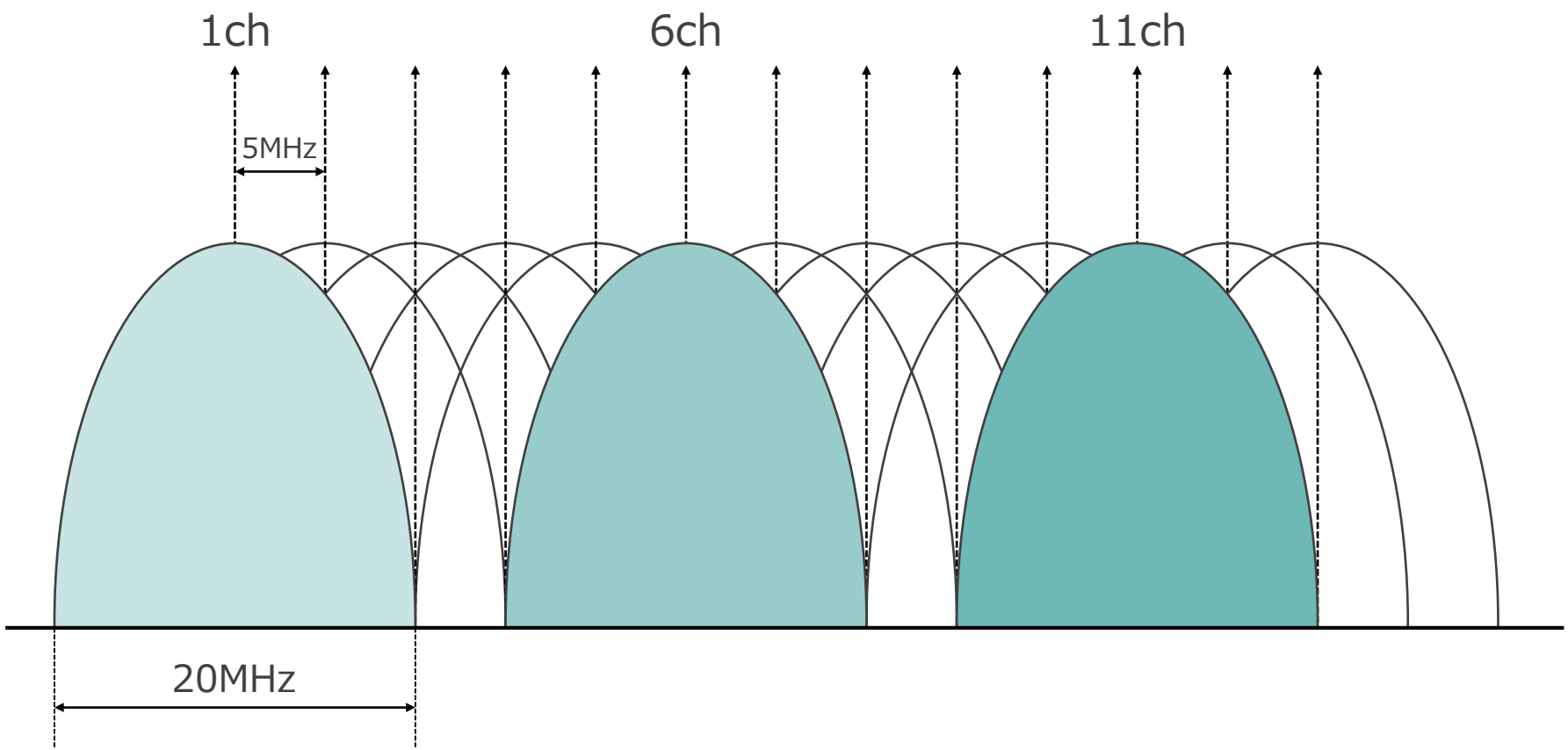
●無線LANの規格

規格名	IEEE802.11a	IEEE802.11b	IEEE802.11g	IEEE802.11n	IEEE802.11ac
策定年	1999年	1999年	2003年	2009年	2014年
周波数帯	5GHz帯	2.4GHz帯	2.4GHz帯	2.4GHz/5GHz帯	5GHz帯
伝送速度	最大54Mbps	最大11Mbps	最大54Mbps	最大600Mbps	最大6900Mbps
通信距離	狭い	広い	広い	広い	狭い
障害物の影響	受けやすい	受けにくい	受けにくい	受けにくい	受けやすい
電波干渉	強い	弱い	弱い	強い	強い

●無線LANの規格

802.11gは11bとの互換性があり、802.11a、802.11acは電子レンジなどの影響などは受けないが、壁を通りにくい等の特性があります。

●無線のチャネル（2.4GHz帯）



2.4GHz帯チャンネル分布

電波干渉を避けるために、一部のチャンネルだけ使用
（1、6、11chを使用するのが一般的）

●無線のチャネル（2.4GHz帯）

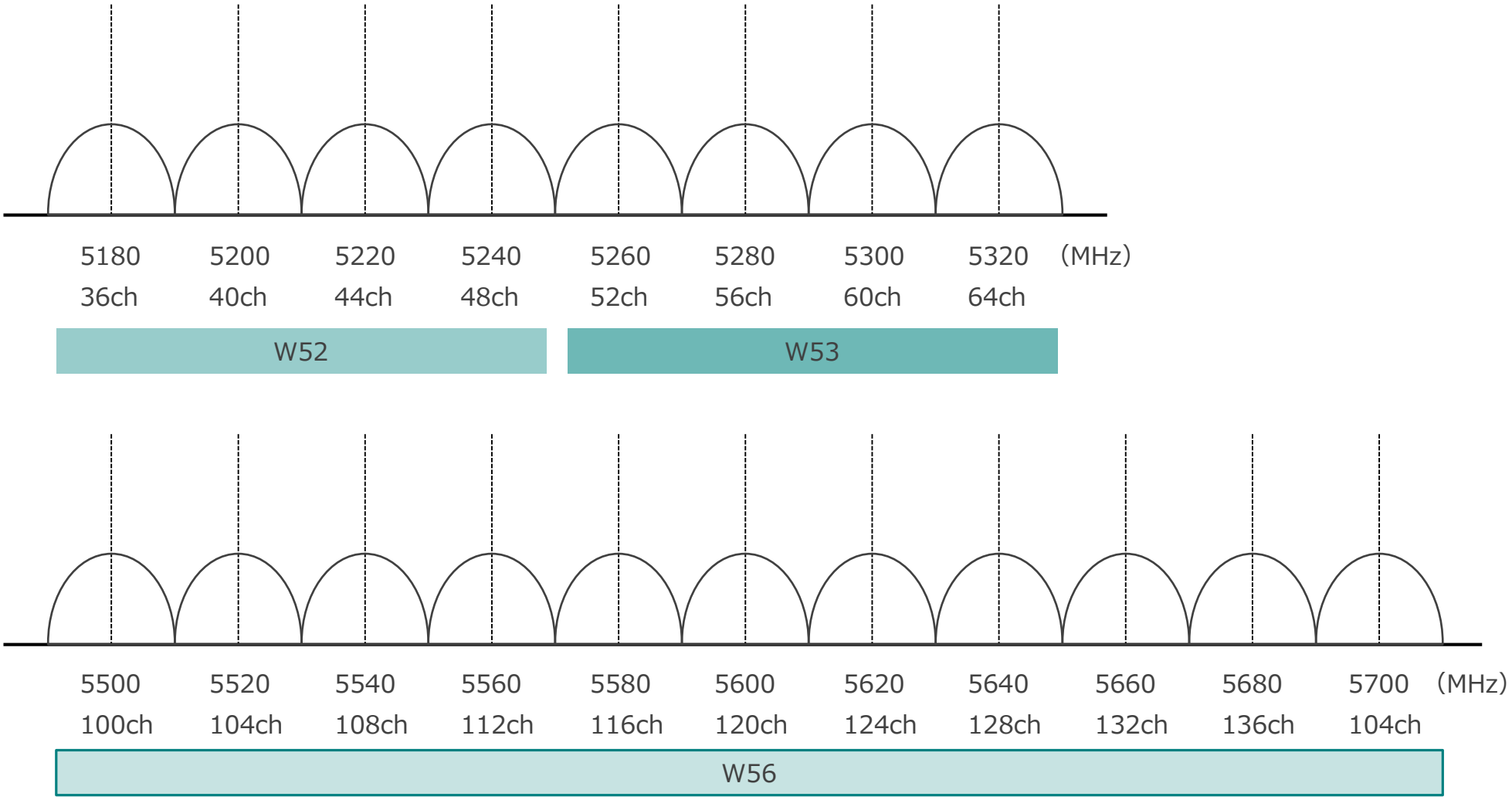
各アクセスポイントがまったく同じ電波を発信するとすれば、各アクセスポイント同士が相互に電波干渉して、正常に通信できなくなります。

そのため、無線LANにはチャネルが存在します。IEEE802.11b/gでは、2.4GHz帯を5MHz間隔で13個に分割し、1～13chとして使用されます。

無線LANのチャネルは、基本的に1APでひとつ使用します（11nは例外）。どのチャネルを使用するかは、アクセスポイント管理者が決定することとなり、アクセスポイント同士が干渉しないように無線LANを構築する必要があります。

なお、クライアントはアクセスポイントから通知される電波を自動検知し、そのチャネルに自動適応しますので設定不要です。

●無線のチャネル（5GHz帯）



5GHz帯　チャネル分布

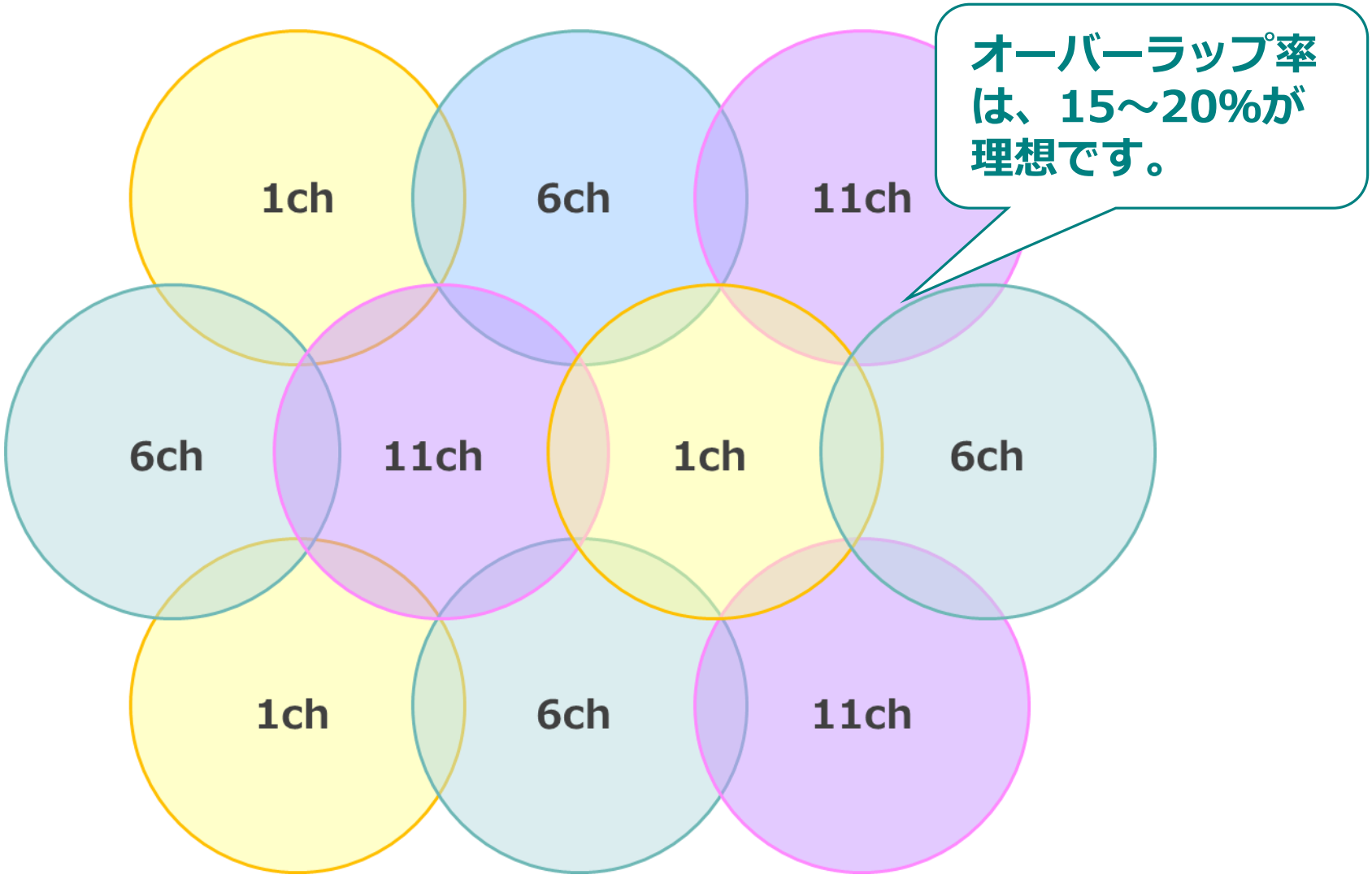
●無線のチャネル（5GHz帯）

5GHz帯は2.4Ghz帯のように各チャネルが使用する周波数が重複しておらず、またチャネル数も全体で19chと多く規定されています。この5GHz帯を活用することで、電波干渉の発生を回避しつつ、面単位で高速な無線LANを構築することが可能となります。なお、屋外で使用できるのはW56のみとなります。

5GHz帯（W53,W56）では衛星や気象レーダーなどの同一周波数帯の使用を検知した場合、自動的にチャネルを変更（DFS）する必要があります。この場合は約１分間、電波が使用できなくなるため無線LAN通信が切断される可能性があります。

※DFS（動的周波数選択）は、電波法の施行規則で決められており、W53・W56に対応するAPは必ず実装しなければいけない

●電波干渉の回避



チャネルが十分違えば相互に影響しない

●電波干渉の回避

APから電波が届く範囲をセルと言います。セルは隣同士で少し重なるように配置することでシームレスにローミングができるようになります。隣接するセルで使用するチャネルは、周波数が重ならないものを選択します。

電波干渉による影響を回避するためには、無線LANを導入する際に設置場所の環境を事前に調査し、電波干渉が発生しないように設置場所や使用するchを慎重に設定する必要があります。このような事前調査は「無線LANサイトサーベイ」と呼ばれます。

◆ パッシブサーベイ
周囲の信号の受信のみを行い、検出される複数のAPの情報を記録すること。

◆ アクティブサーベイ
APにテストフレームを送信し、それに対するACKフレームを測定すること。

●サイトサーベイ（実地調査）

【パッシブサーベイ】

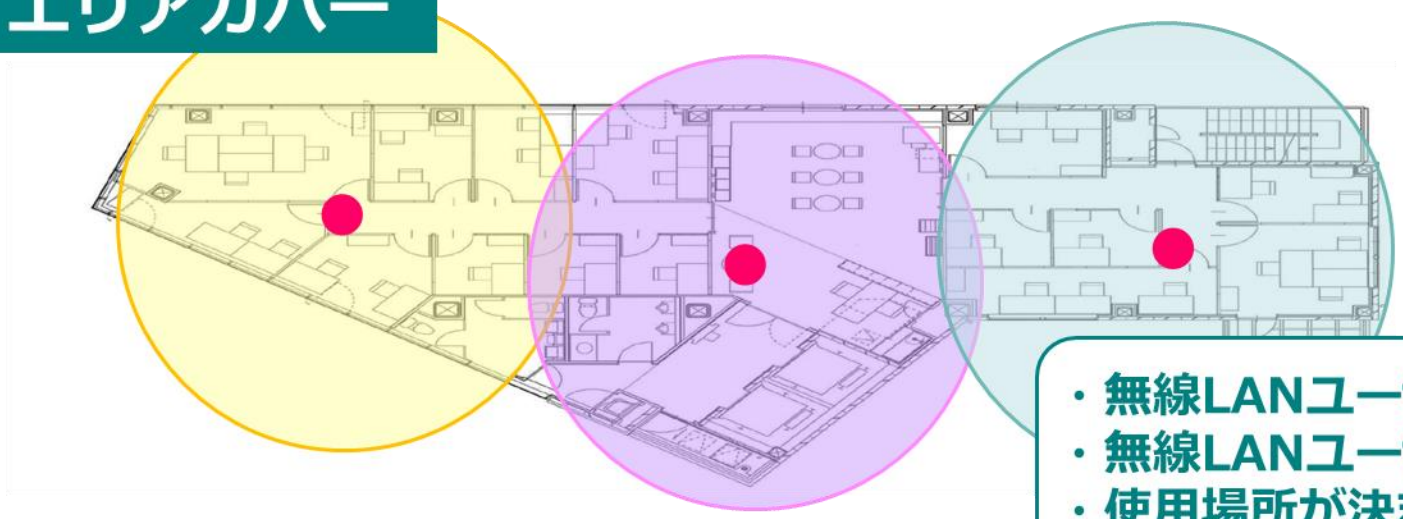
パッシブサーベイでは自社内のAPはもちろん、近隣のビルなどから漏れ届いた管理外のAPも発見できます。自社のAPを設置する前に近隣で使用されているチャネルを把握することで、無線LANの干渉を事前に避けることもできます。

【アクティブサーベイ】

アクティブサーベイでは信号強度や雑音レベルの情報だけでなく、パッシブサーベイでは収集できないフレームの再試行やロス率、フレームスピードなど、無線LAN通信を実運用した場合の情報を収集できます。APとクライアントの適切な配置位置を探し出すのに有効です。

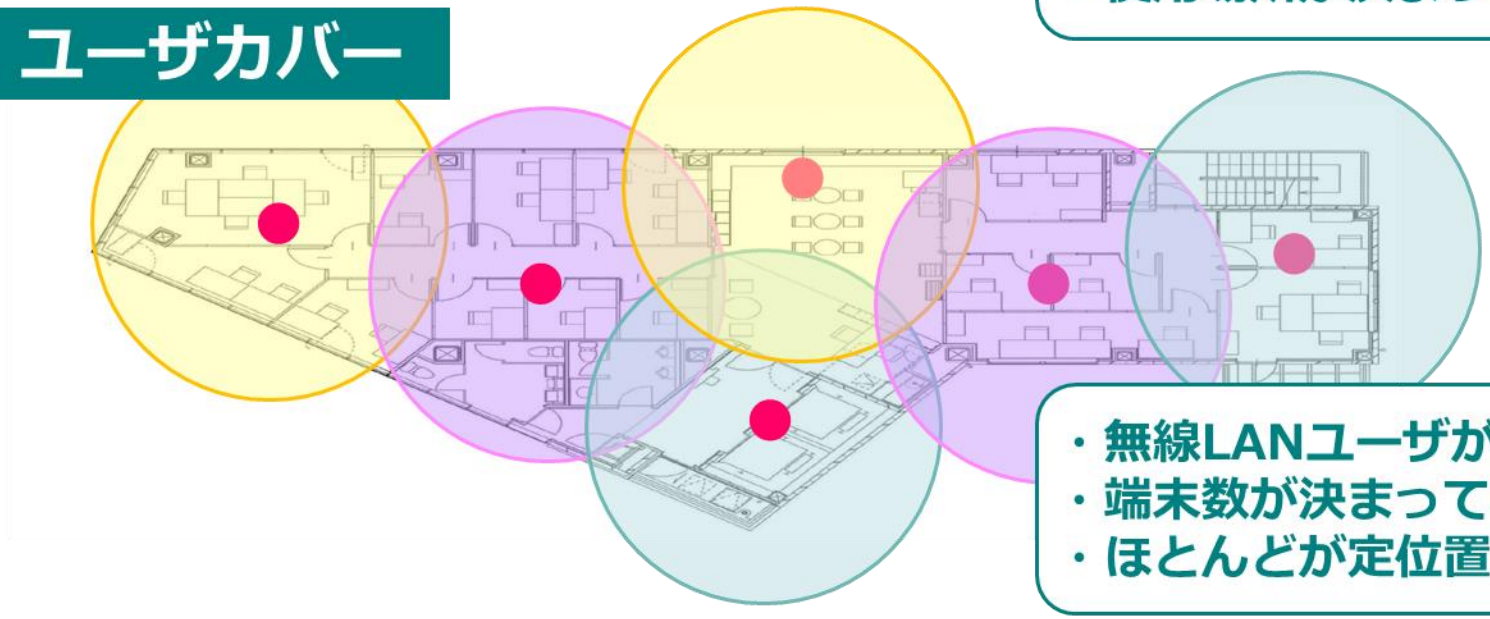
●エリア構築の考え方

エリアカバー



・無線LANユーザが少ない
・無線LANユーザの数がわからない
・使用場所が決まっていない

ユーザカバー



・無線LANユーザが多い
・端末数が決まっている
・ほとんどが定位置にて利用

●エリア構築の考え方

【エリアカバー】

対象エリア内のどの位置でも無線LANで通信できるようにする考え方です。端末の台数や分布状況を考慮せず、単に「つながる」環境を構築することを重視しています。主に、オフィスの会議室や倉庫、工場、病院など、ユーザ収容数をさほど必要としないケースに向いています。

【ユーザカバー】

対象エリア内のどの位置でも接続できることに加え、端末の台数や分布状況も考慮した考え方です。たとえば、「特定のエリアで必ず端末を30台接続できるようにする」「1ユーザ当り2Mbpsのスループットが必要」などの要件があるケースに適用します。主に、オフィスの事務エリアや学校の教室、講堂などに向いています。

●APの配置パターン

設置パターン	メリット	デメリット
天井	・電波は円を描くように広がるため、電波を有効利用できる ・セル設計が容易になる	・天井配線が必須 ・拠点によってはビル管理者への届出が必要になる
壁・パーティション	・配線設計が比較的容易	・設置位置が限定される ・壁側へも電波が送出されるため、電波を有効に利用できない
じゅう器上	・設置が容易	・簡単に動かせてしまうため、AP移動によってカバーエリアが変動する
天井裏	・アンテナが隠蔽できるため、見た目が美しい	・電波劣化が発生する ・メンテナンスが不便

●APの配置パターン

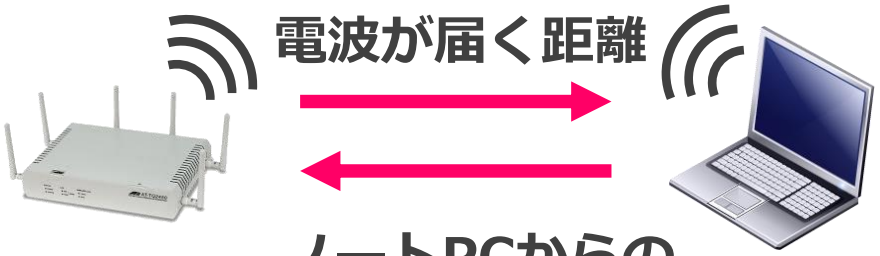
アクセスポイントの設置場所を決めるときには、周囲の障害物の有無を確かめます。電波は飛距離によって徐々に弱くなっていくだけでなく、間にある障害物を通すことによっても弱くなります。

壁の材質も電波の減衰に大きく影響します。オフィスでよく使われているスチール製のパーティションと、学校の教室を隔てるコンクリートの壁では、電波の通り方は異なります。

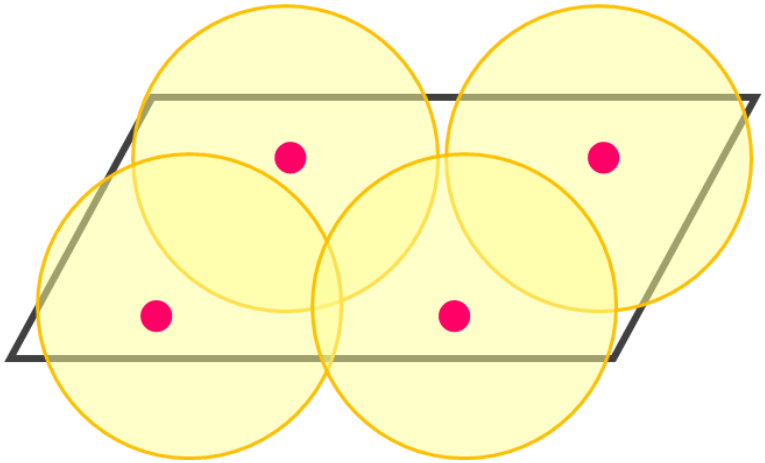
場合によっては、部屋ごとにアクセスポイントを設置する必要もでてきます。

●スマートデバイスのセル設計

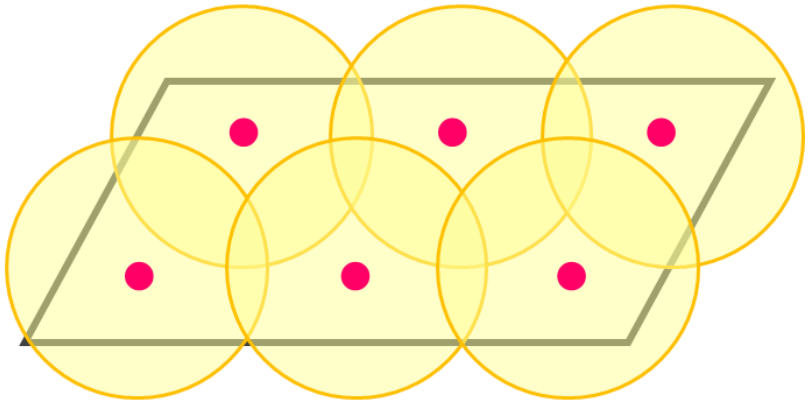
ノートPCの場合



スマートデバイスの場合



ある程度、広めのセルを描くことができます



端末からの電波の飛距離にセルを合わせるため、
やや狭いセルとなります

●スマートデバイスのセル設計

セル設計では、スマートデバイスを接続する場合、ノートPCを接続するケースに比べてセルを小さくする必要があります。スマートデバイスはノートPCに比べると、無線LANチップやアンテナの性能が劣ります。

このため、端末によっては「ノートPCよりも電波が届かない」「アクセスポイントからの電波を検知できない」といったことが生じます。

ノートPCに加えてスマートデバイスも接続する環境では、アクセスポイントの台数を増やすなどの対策が必要となります。

●主なサイトサーベイツール

【フリーウェア】
・inSSIDer（version4から有料）
・NetStumbler
・iPerf

【シェアウェア】
・AirMagnet
・Ekahau Site Survey

●主なサイトサーベイツール

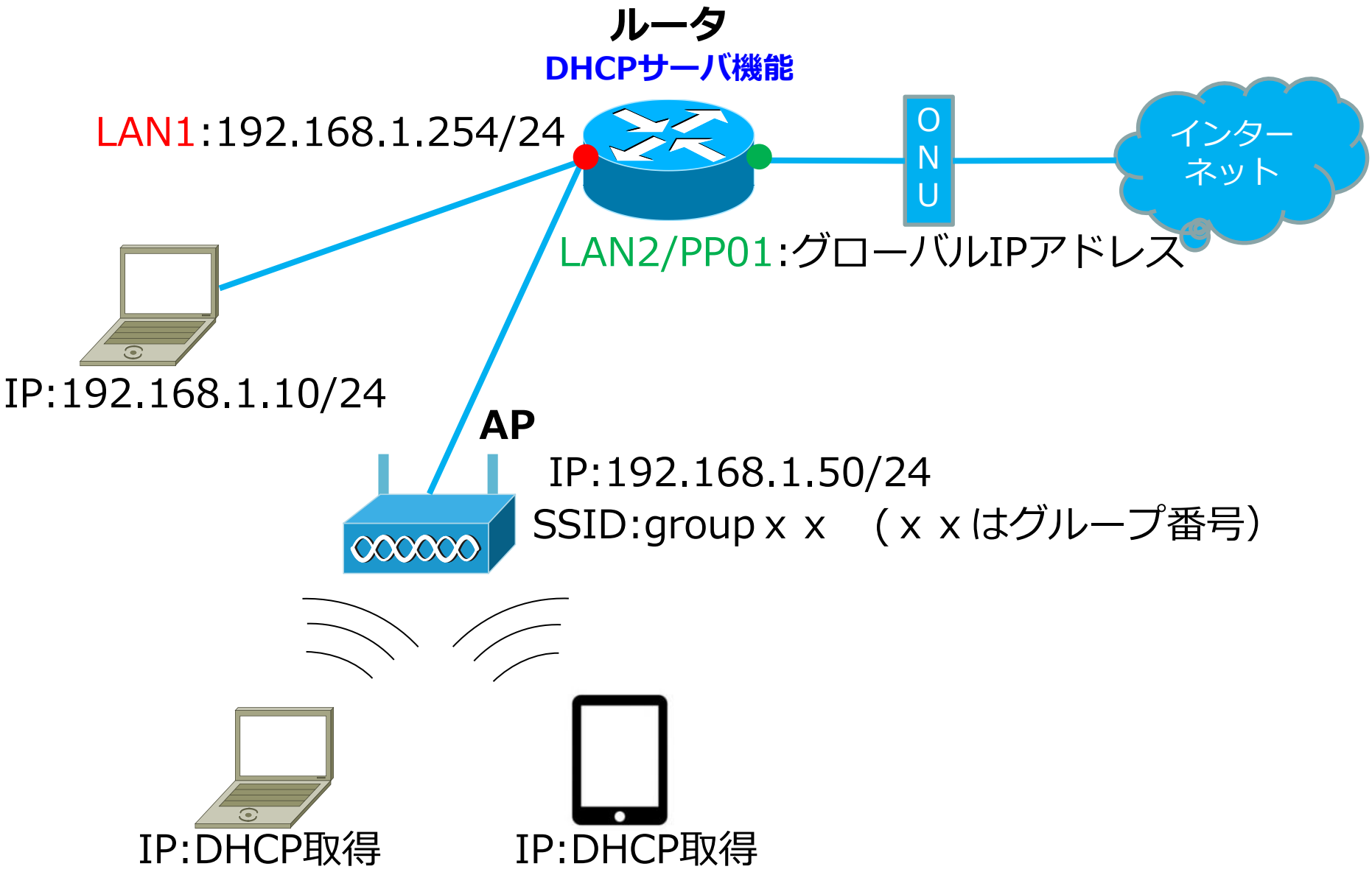
「inSSIDer」や「NetStumbler」などのフリーウェアでは、電波状況の確認やSSIDの一覧、周囲の使用チャネル、電波強度などを確認でき、パッシブサーベイに利用されます。

それに加えて「AirMagnet」や「Ekahau Site Survey」などのシェアウェアでは、電波の受信レベルやAPのオーバーラップを視覚的に表示するなど、サイトサーベイに特化した機能を使用することができます。

また、「iPerf」はネットワークスループットを測定するためのソフトウェアで、アクティブサーベイに利用されます。

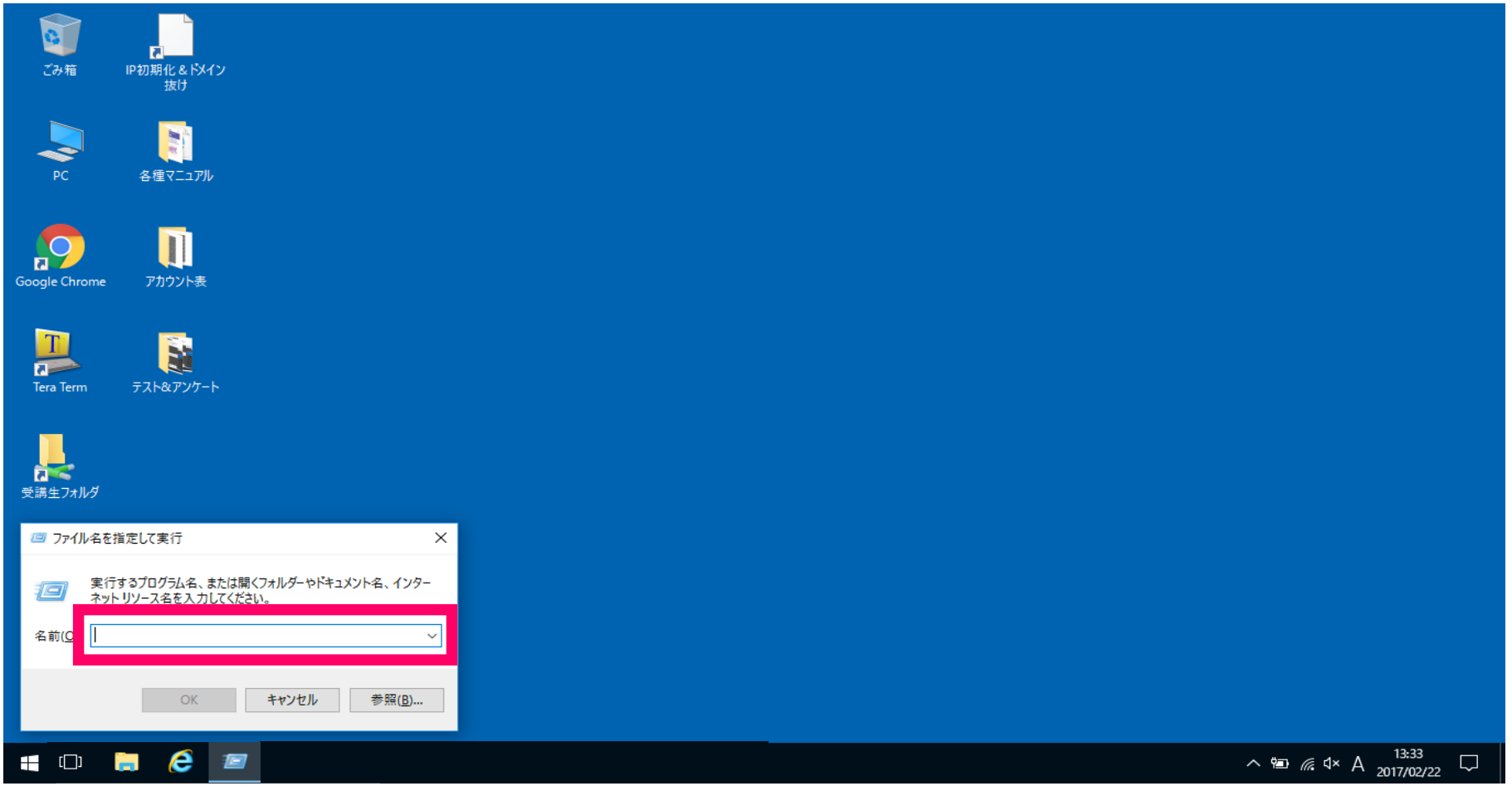
演習②
インターネット環境の構築

●演習構成

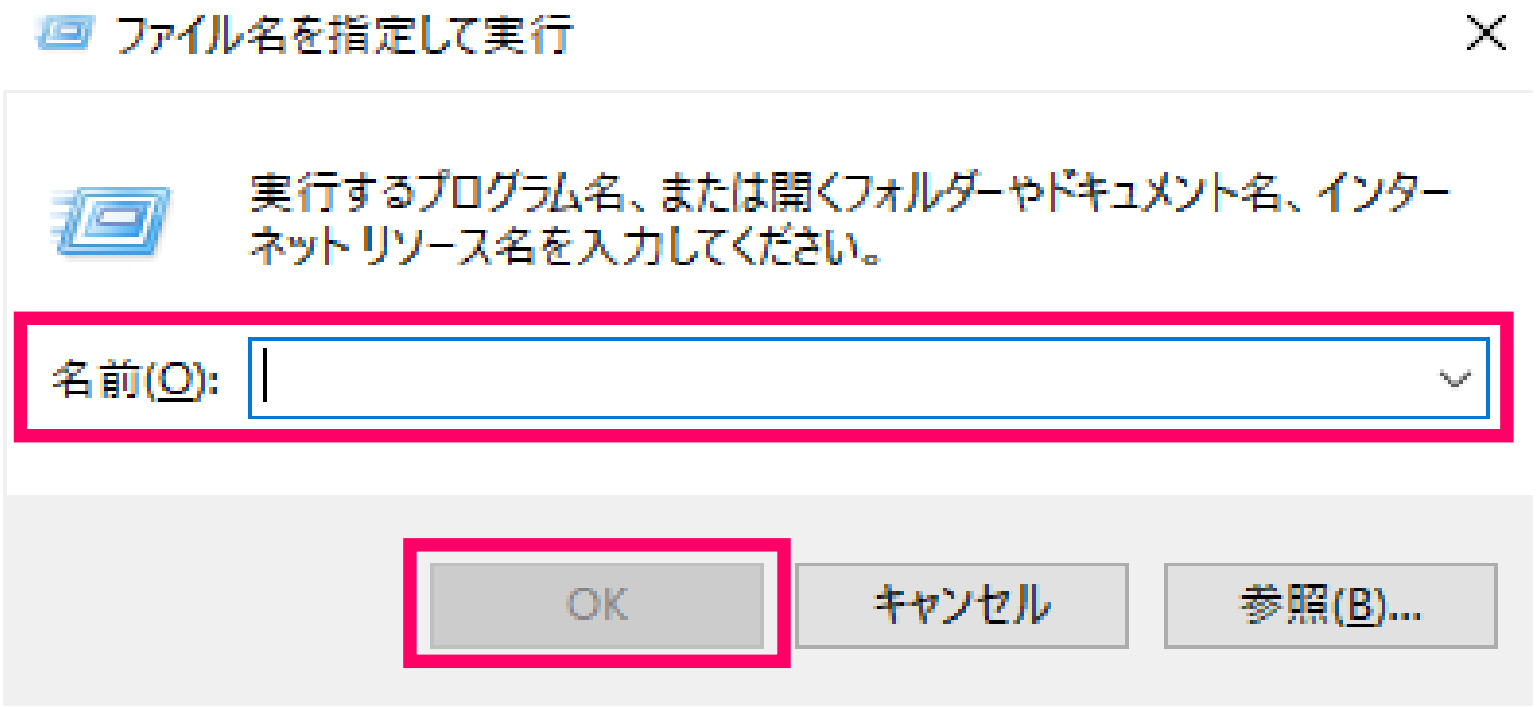

ルータ
DHCPサーバ機能
LAN1:192.168.1.254/24
ONU
インター
ネット
LAN2/PP01:グローバルIPアドレス
IP:192.168.1.10/24
AP
IP:192.168.1.50/24
SSID:group x x　（x x はグループ番号）
IP:DHCP取得
IP:DHCP取得

1.PCのネットワーク設定確認

①【キーボードのwindowsキー  ＋ Ｒ 】を押下し、ファイル名を指定して実行を開きます。

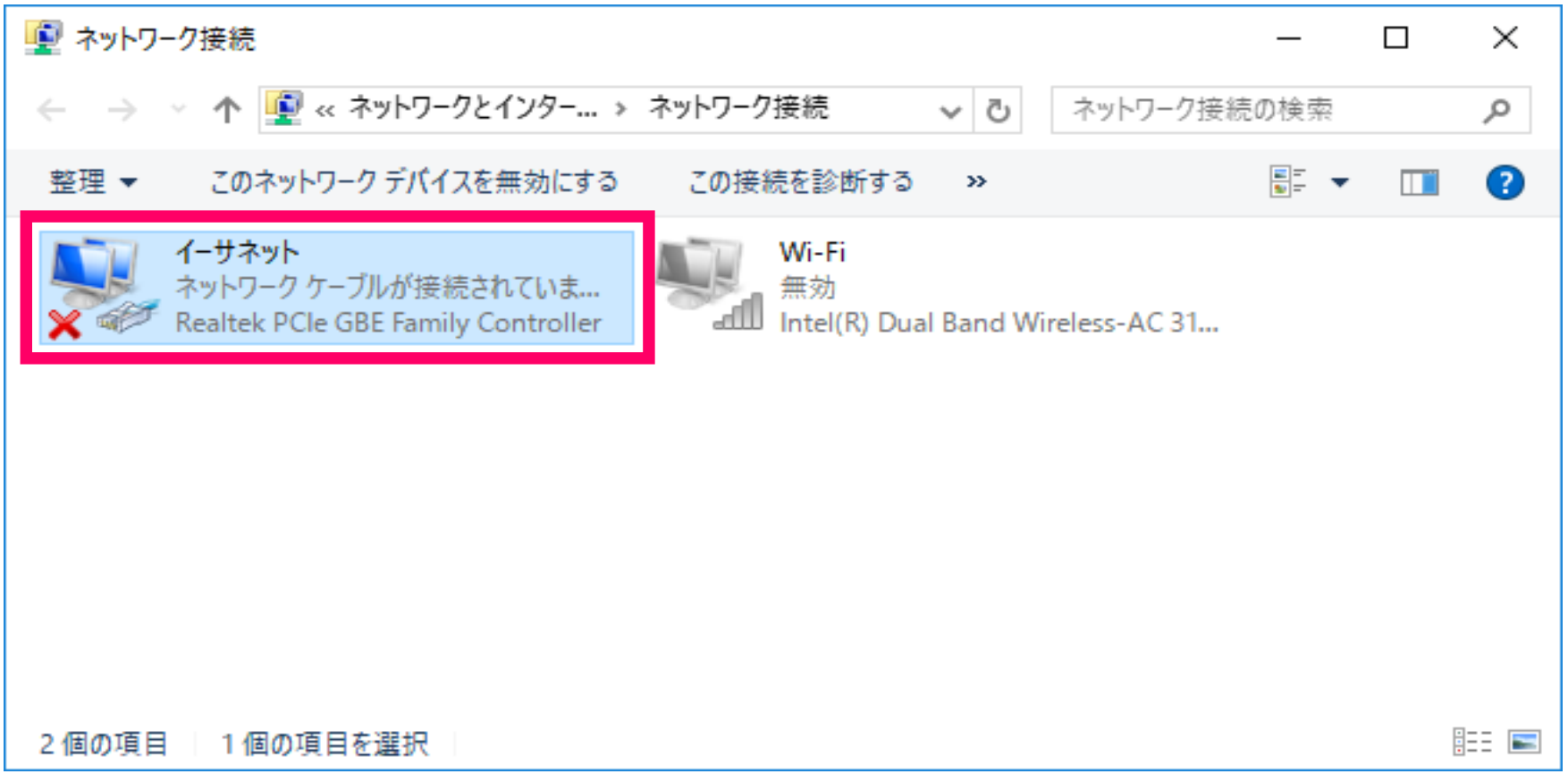


②【 ncpa.cpl 】を入力し、【OK】をクリックします。



1.PCのネットワーク設定確認

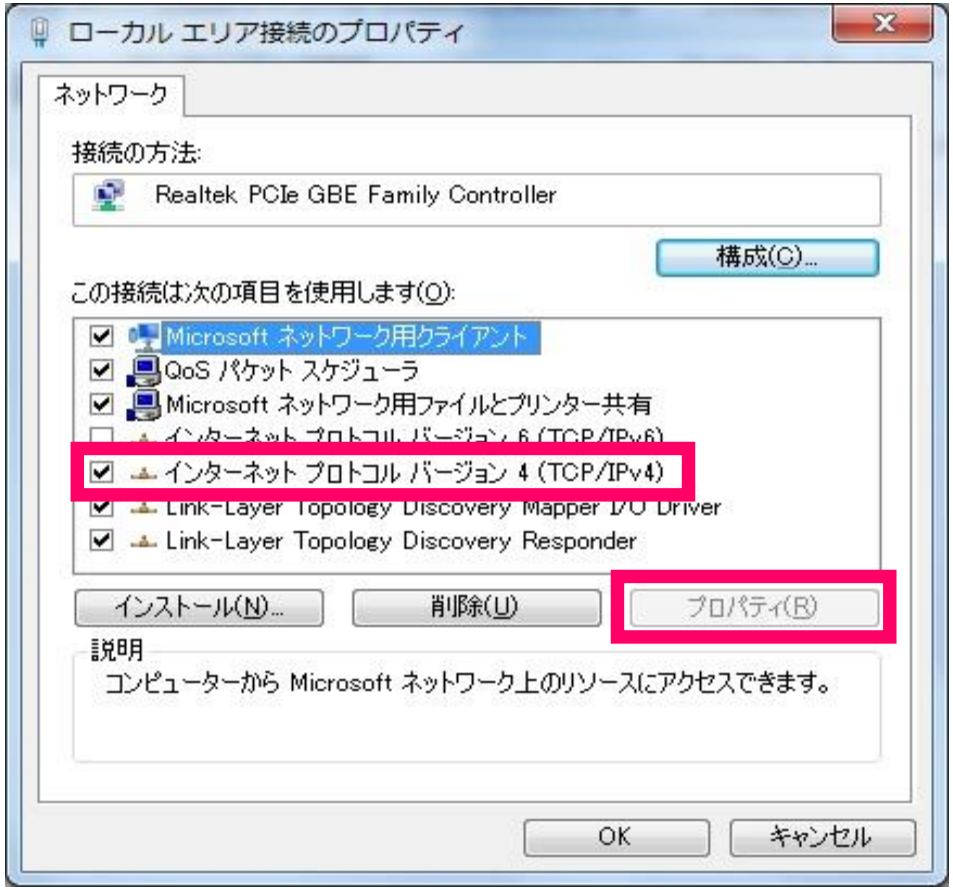
③【イーサネット】を【右クリック】し、プロパティを開きます



1.PCのネットワーク設定確認

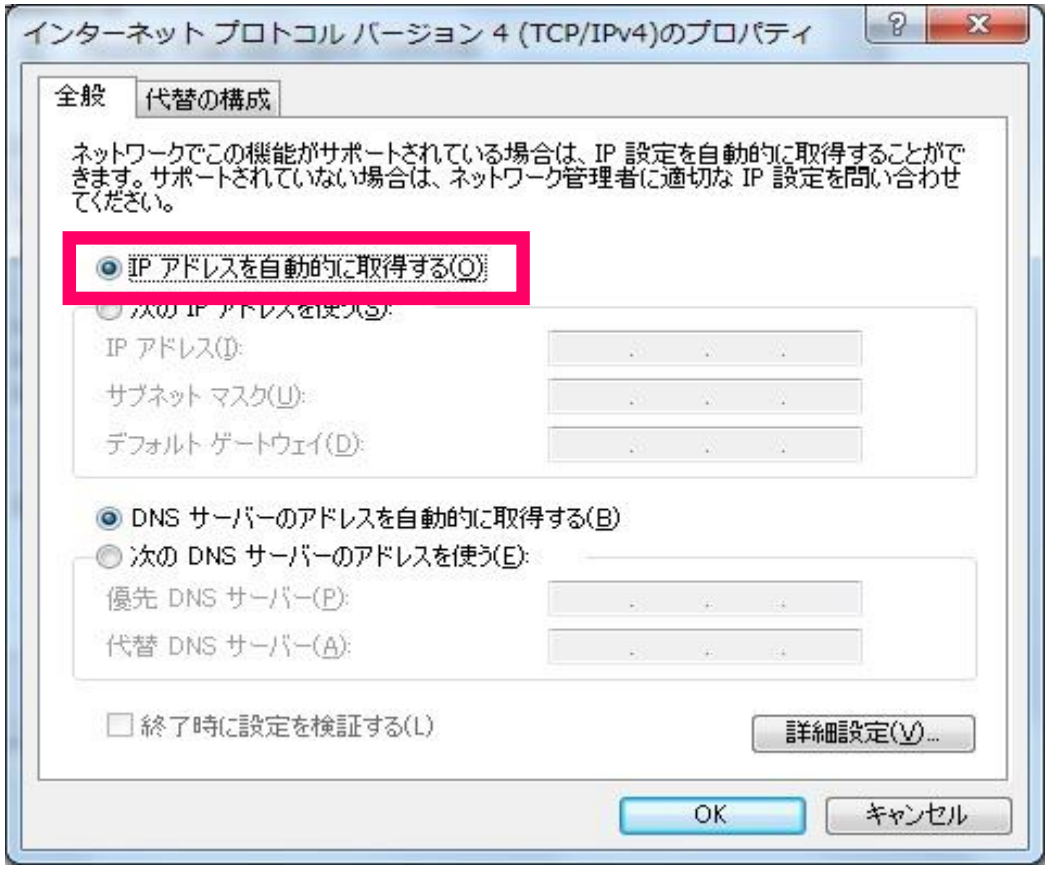
④【 インターネット プロトコル バージョン4 (TCP/IPv4) 】をクリックします。

⑤【プロパティ】をクリックします。



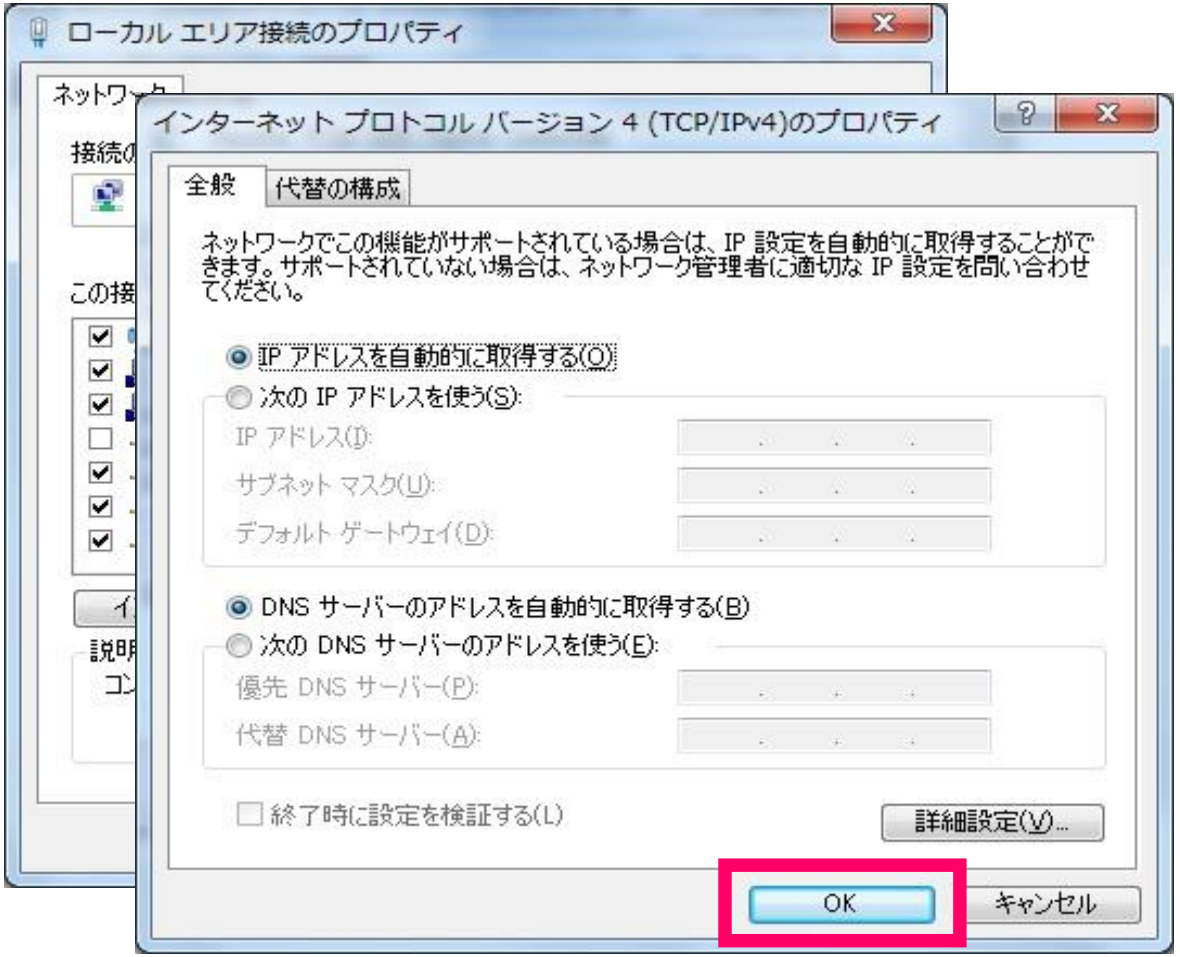
⑥【 IPアドレスを自動的に取得する 】であることを確認します。

※IPアドレスが既に設定されている場合は、自動取得に戻して下さい



⑦【 OK 】をクリックして2つのプロパティを閉じます。

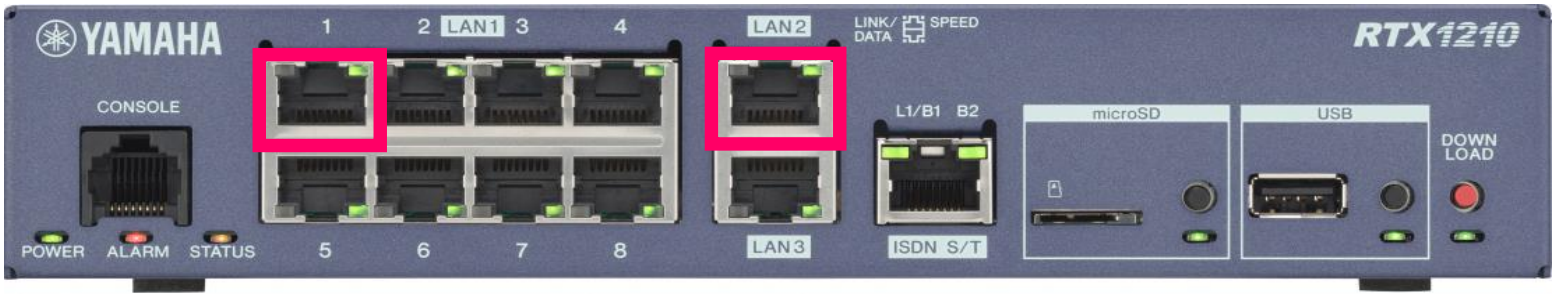
※注意　プロパティを閉じないと設定が反映されません

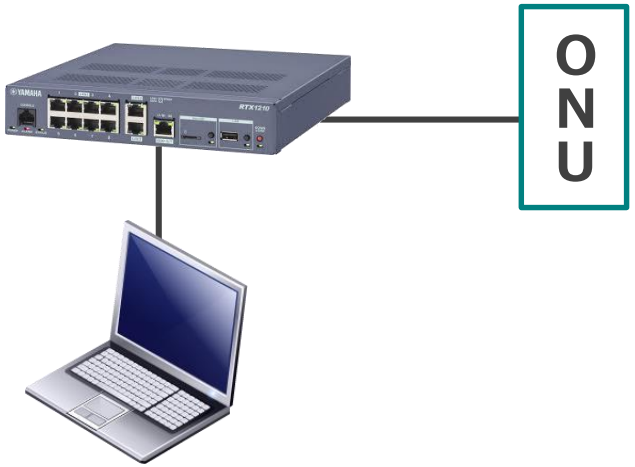


2.LANケーブル接続

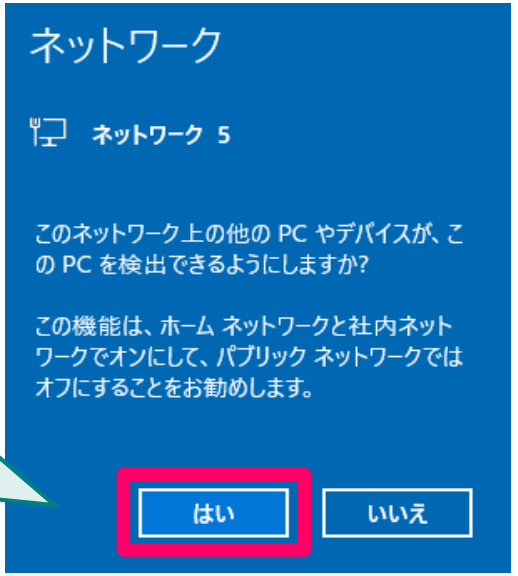
①【 LAN1.1 】とPC、【LAN2】とONUをそれぞれLANケーブルで接続します。

PCと接続　　**ONUと接続**





LANケーブルで接続すると画面右にポップアップがでるので「はい」を選択します

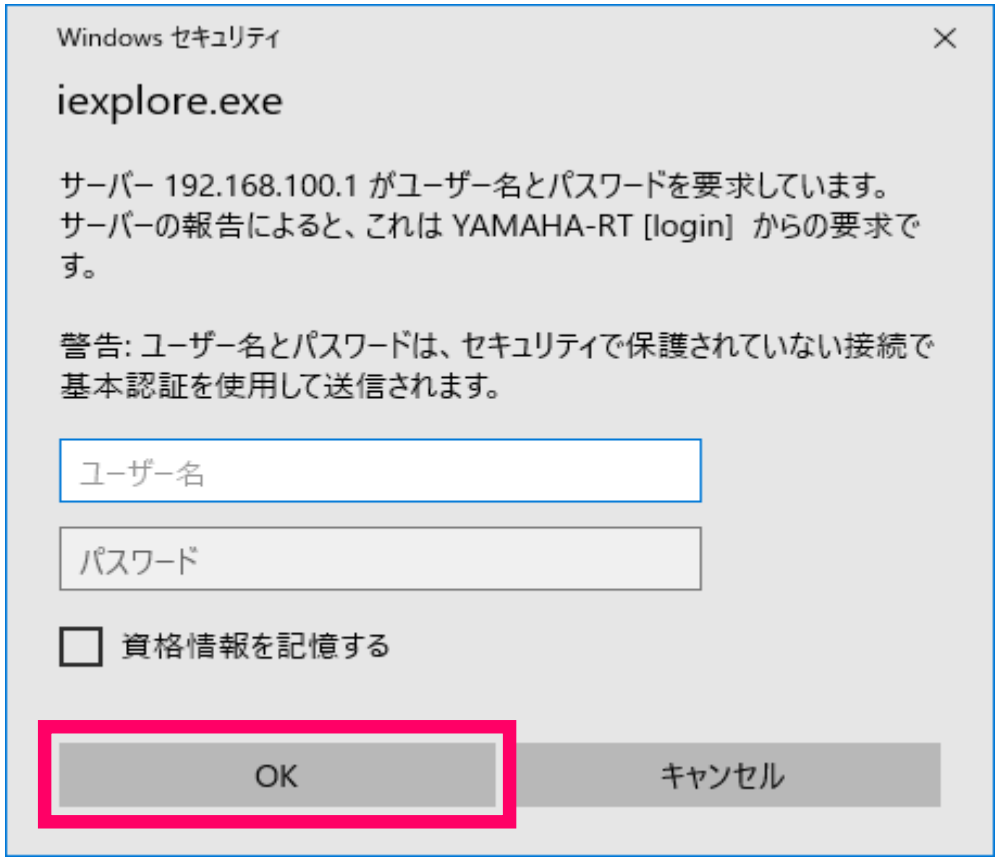


3.RTX1210ルータへログイン

①インターネットエクスプローラのブラウザ画面を開きます。
②ブラウザのアドレス記入欄に【192.168.100.1】を入力します。

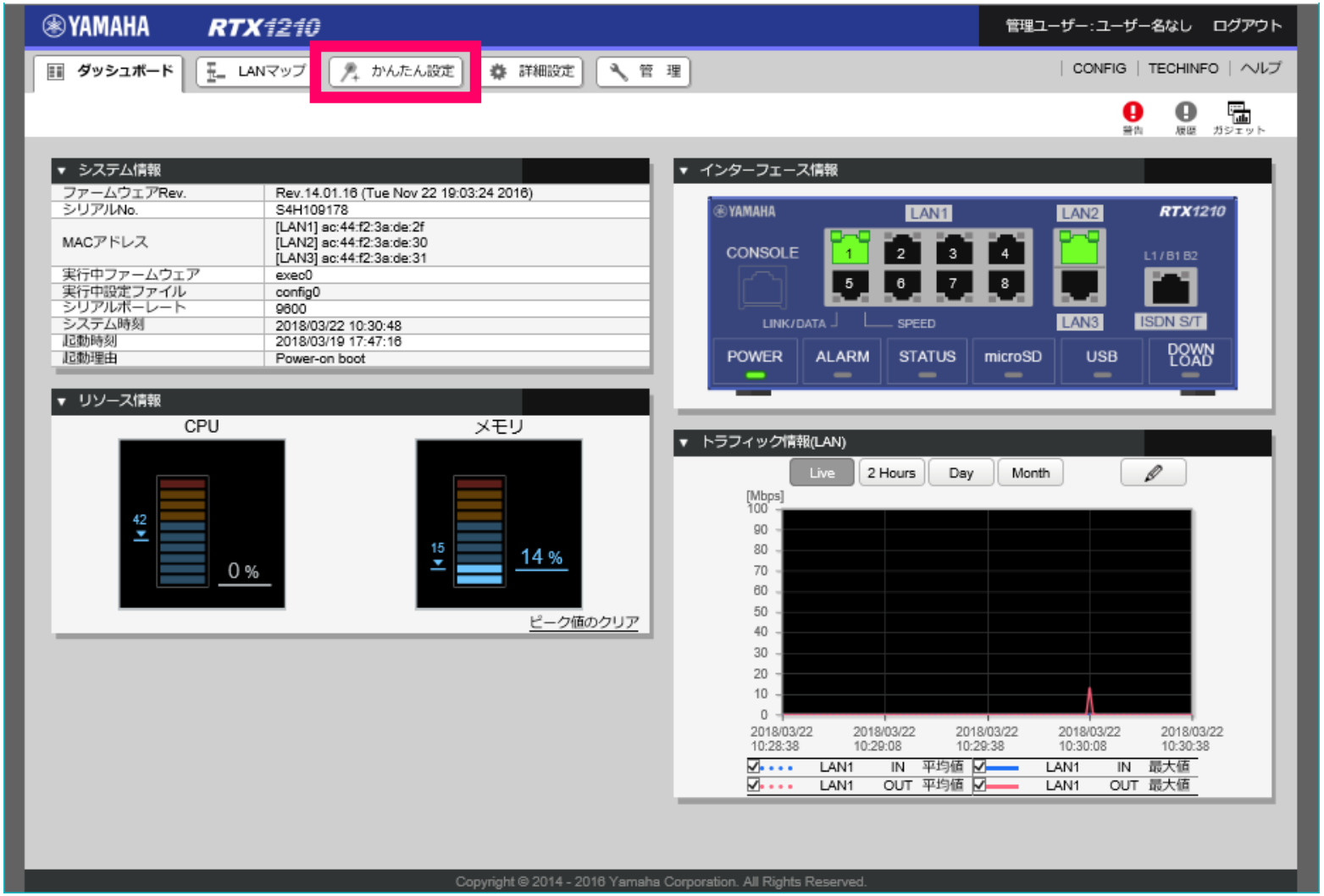
RTX1210ルータは初期設定でGUI設定アクセス用に
LAN1（スイッチポート）にIPアドレスが設定されています
初期IPアドレス： 192.168.100.1 /24

③【OK】をクリックし、ログインします。RTX1210ルータは初期設定でユーザ名/パスワードとも設定されていません



3.LAN1アドレスの変更

④【かんたん設定】をクリックします。



3.LAN1アドレスの変更

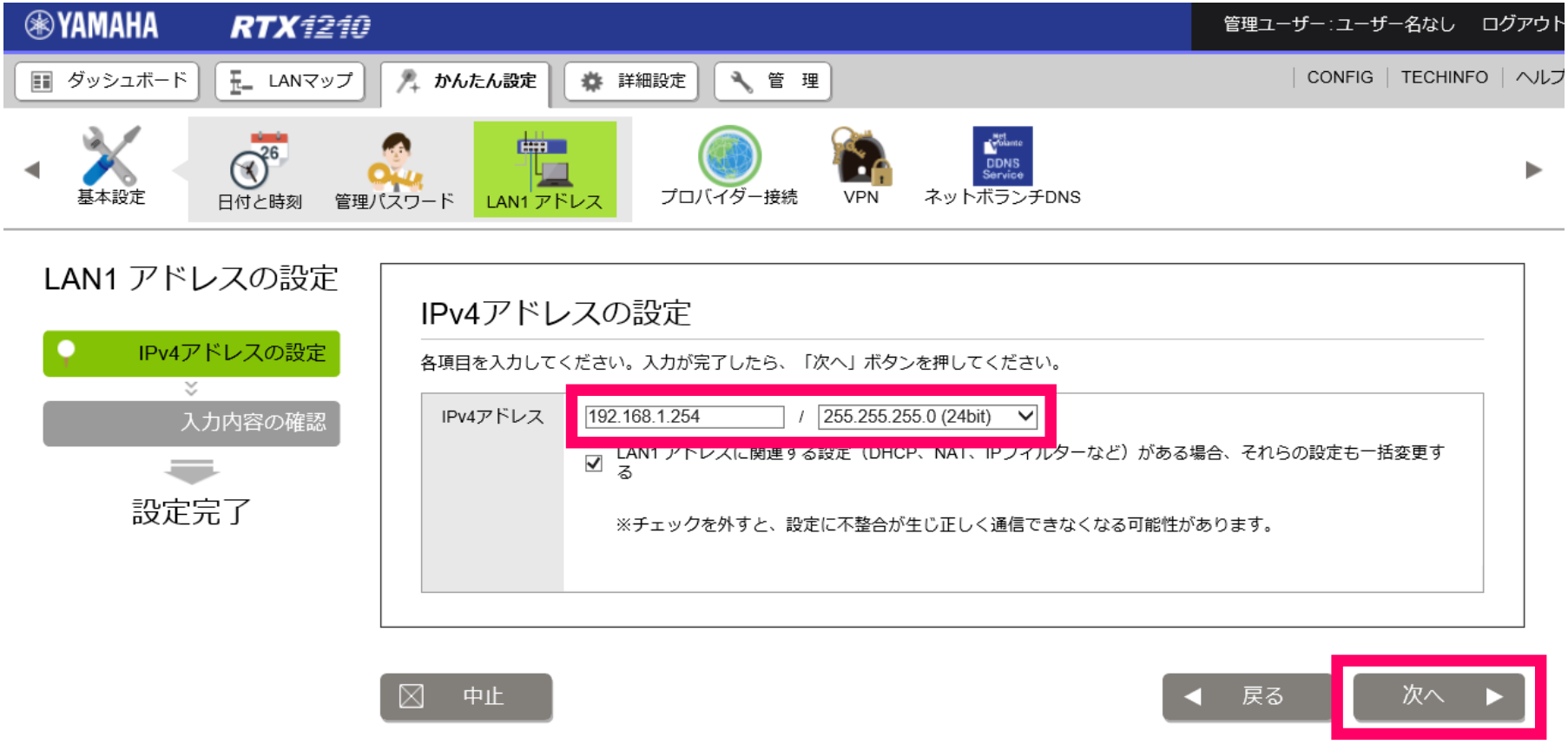
⑤【基本設定】をクリックし、【LAN1アドレス】をクリックします。

⑥IPv4アドレスの【設定】をクリックします

3.LAN1アドレスの変更

⑦IPv4アドレス設定の画面で、初期値のIPアドレスを下記のIPアドレスに変更します。

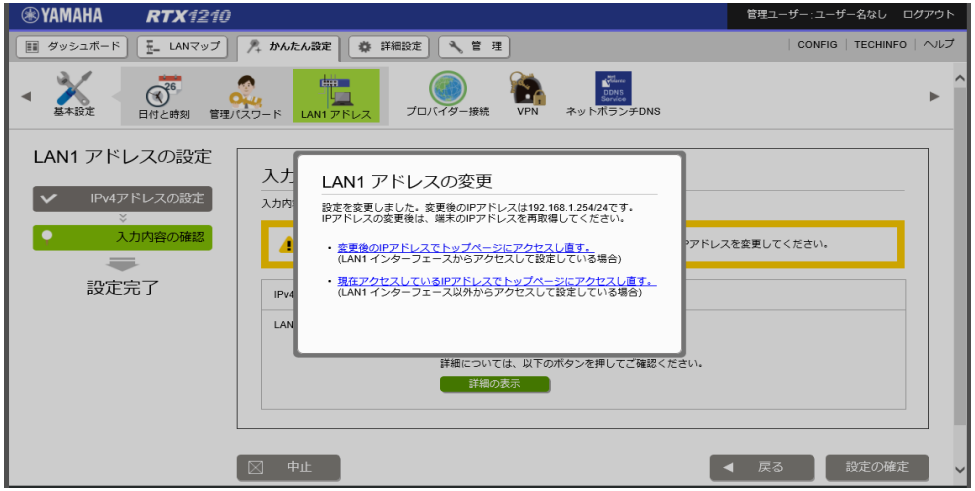
IPアドレス【192.168.1.254】　サブネットマスク【255.255.255.0】



3.LAN1アドレスの変更

⑧入力内容の確認画面で、入力したIPアドレスの確認後、設定の確定をクリックします。

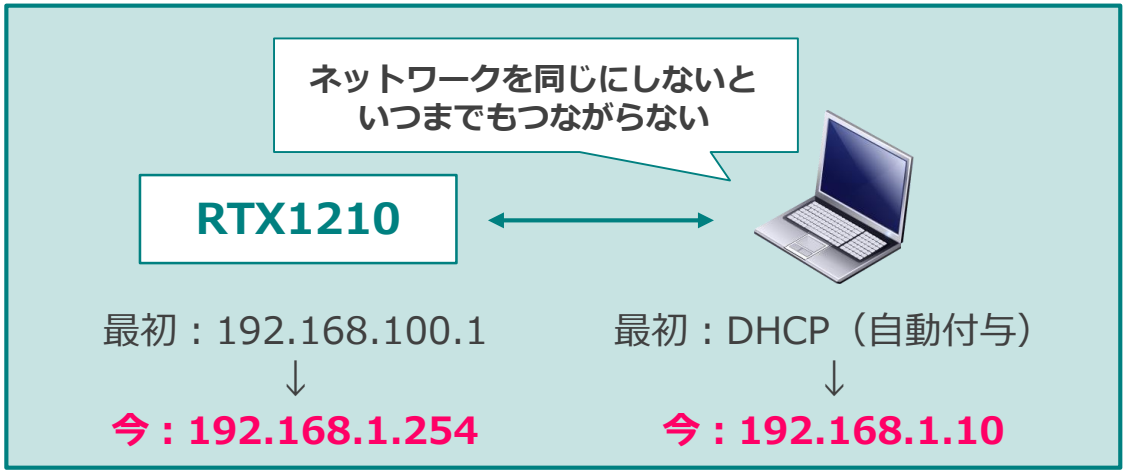
⑨設定の確定をクリックすると、ポップアップが表示されますが、そのままブラウザを閉じてください。



4.再ログイン

①再度ルータへログインするため、PCのIPアドレスを下記に変更します。

IPアドレス：192.168.1.10
サブネットマスク：255.255.255.0
デフォルトゲートウェイ：192.168.1.254
DNS：192.168.1.254



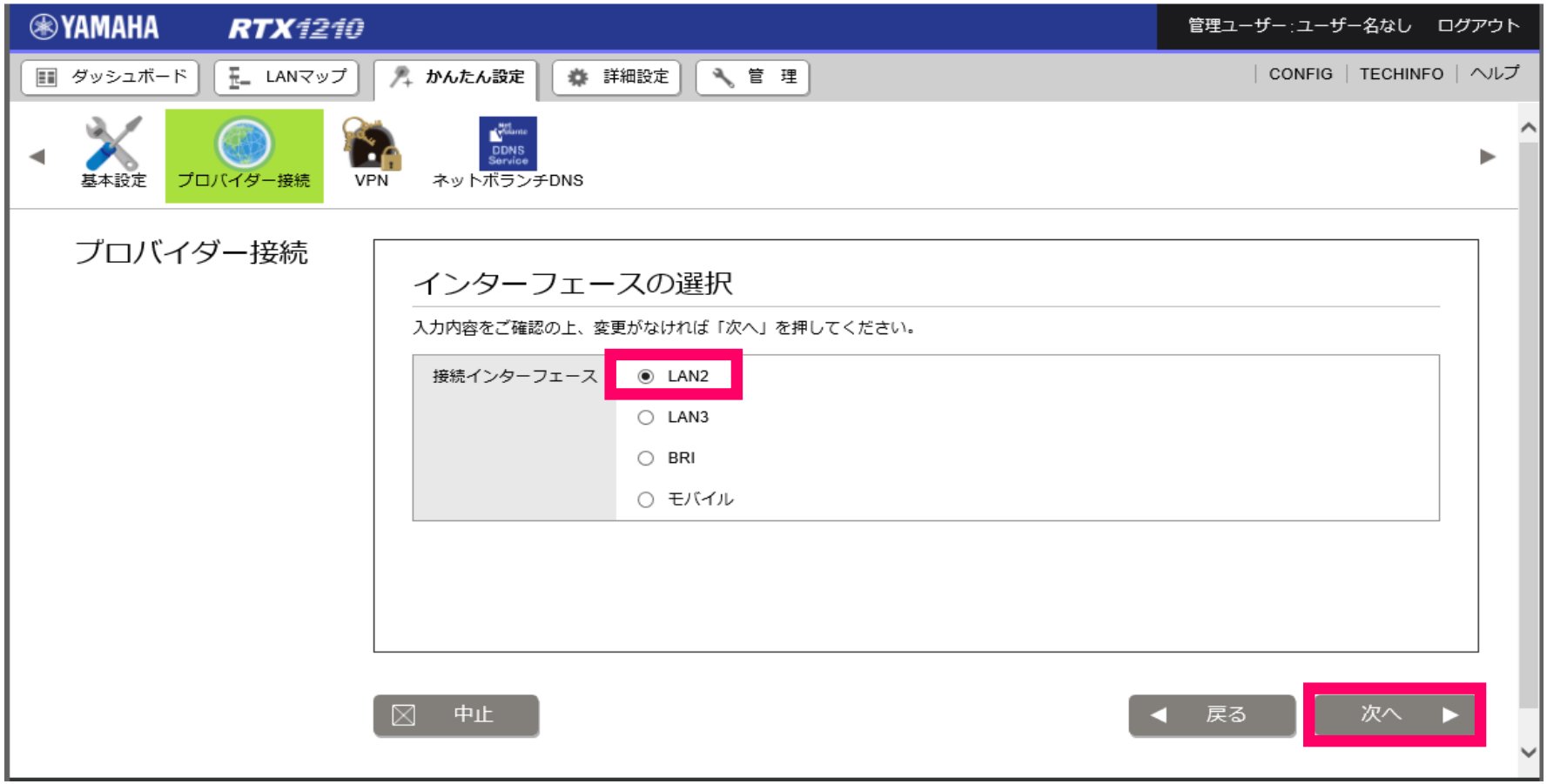
②PCの設定変更後、ブラウザのアドレス記入欄に【192.168.1.254】を入力し、ルータへ再ログインします。

5.PPPoEの設定(ISPとの認証)

①【かんたん設定】をクリックし、【プロバイダー接続】をクリックします。

5.PPPoEの設定(ISPとの認証)

②ウィザードに従い、インターフェースの選択画面で【LAN2】を選択し、次へをクリックします。



5.PPPoEの設定(ISPとの認証)

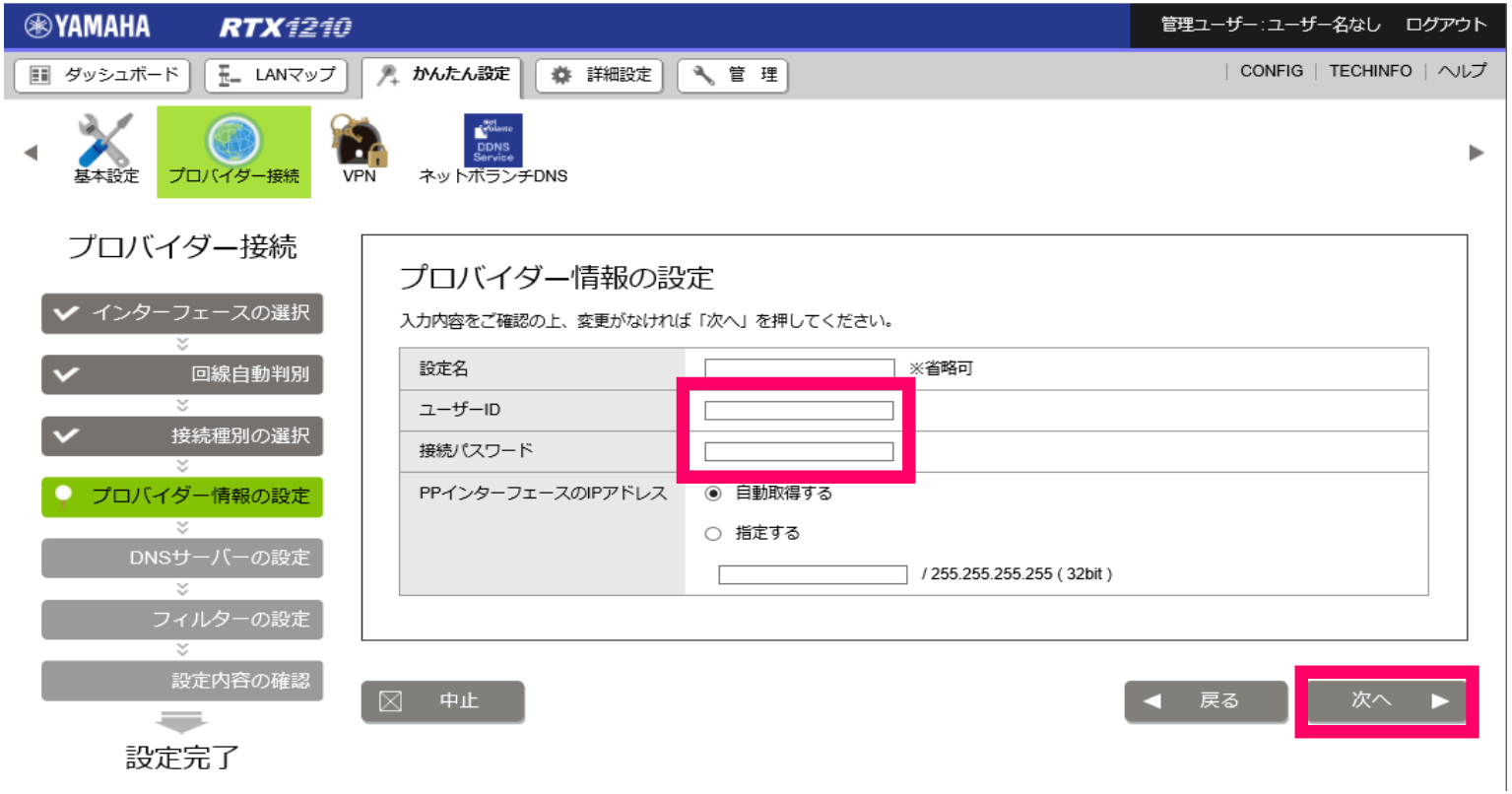
③回線自動判別の画面で、次へをクリックします。

④接続種別の選択の画面で、次へをクリックします。

5.PPPoEの設定(ISPとの認証)

⑤プロバイダー情報の設定の画面で、【ユーザーID】と【接続パスワード】を入力します。
※ISP情報はデスクトップのISPアカウント表を参照

⑥入力後、次へをクリックします。



5.PPPoEの設定(ISPとの認証)

⑦DNSサーバーの設定の画面で、【プロバイダーとの契約書にDNSサーバーアドレスの指定がある】を選択します。

⑧プライマリーDNSサーバーアドレス欄に下記を入力し、次へをクリックします。

プライマリーDNSサーバーアドレス：**8.8.8.8**

5.PPPoEの設定(ISPとの認証)

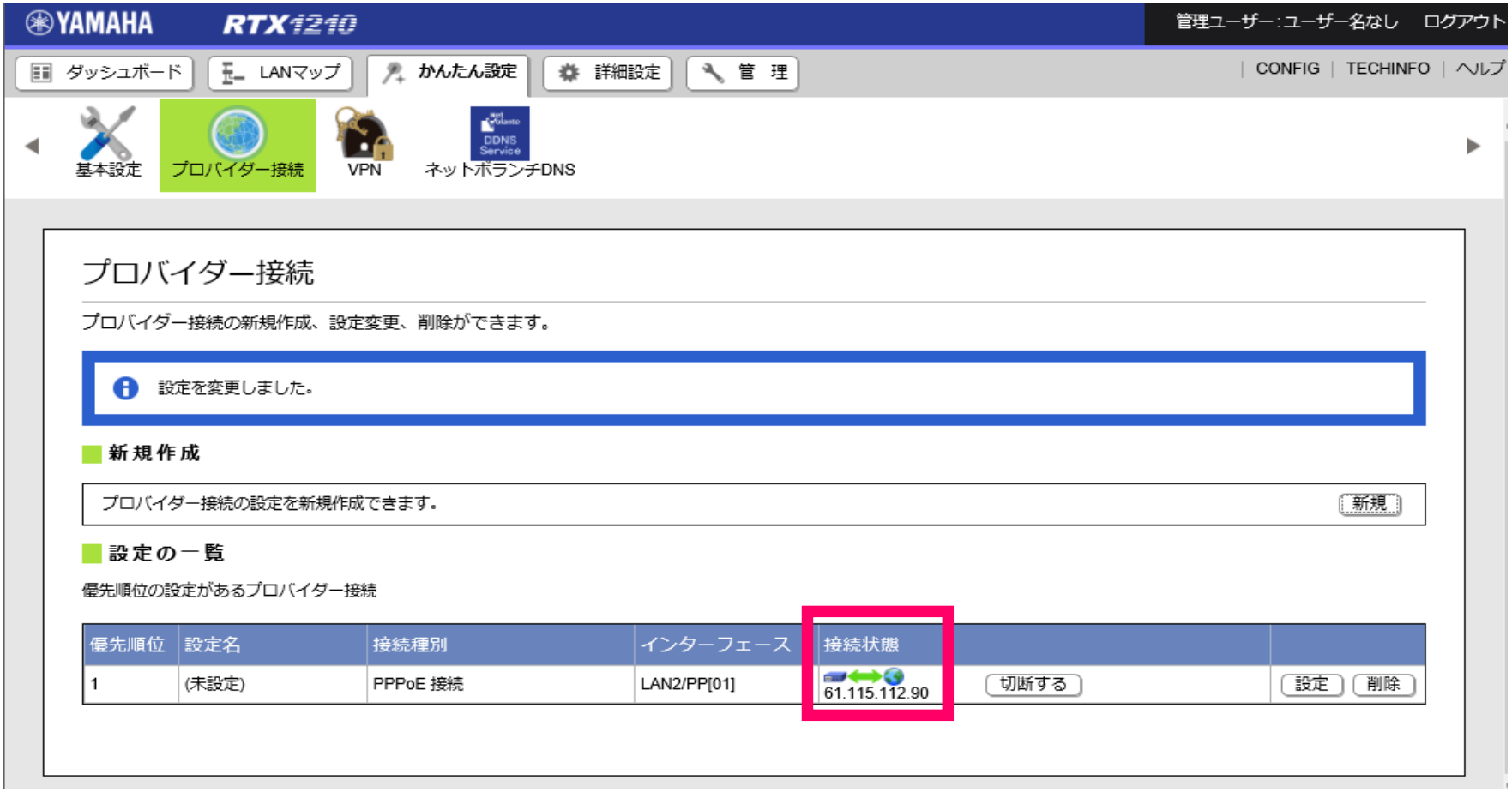
⑨フィルターの設定の画面で、次へをクリックします。

5.PPPoEの設定(ISPとの認証)

⑩設定内容の確認の画面で、設定した内容に間違いがないことを確認し、
【設定の確定】をクリックします。

5.PPPoEの設定(ISPとの認証)

⑪プロバイダー接続の画面で、接続状態の欄にグローバルIPアドレスが表示されていることを確認します。



6.アクセスポイント（AT-TQ2450）へログイン

①【 LANポート 】とPCをLANケーブルで接続します。

LANケーブルで接続

6.アクセスポイント（AT-TQ2450）へログイン

②インターネットエクスプローラのブラウザ画面を開きます。

③ブラウザのアドレス記入欄に【192.168.1.230】を入力します。

※今回はPCのIPアドレスが【192.168.1.10】のため、PCのIPアドレスは変更せずに使用できます。

AT-TQ2450は初期設定でGUIアクセス設定用に
LAN1ポートにIPアドレスが設定されています
初期IPアドレス： 192.168.1.230 /24

6.アクセスポイント（AT-TQ2450）へログイン

④【User Name】と【Password】に以下を入力後【Logon】をクリックします。

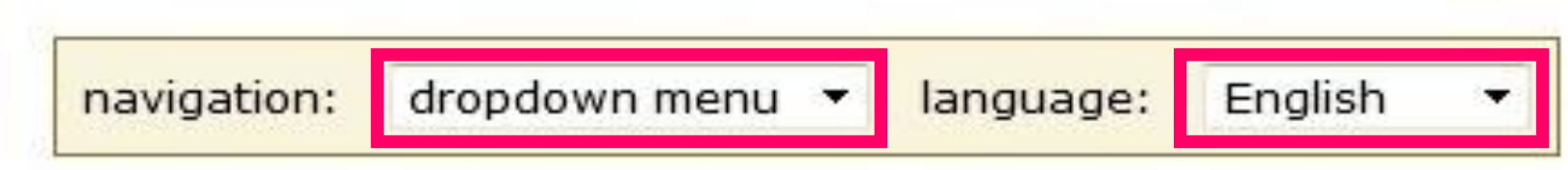
User Name : manager
Password : friend

※AT-TQ2450は初期設定でmanager/friendが設定されています。

7.GUI表示変更

①【language】を【日本語】に変更します。

②【navigation】を【垂直タブ】に変更します。



① 【VAP】をクリックします。

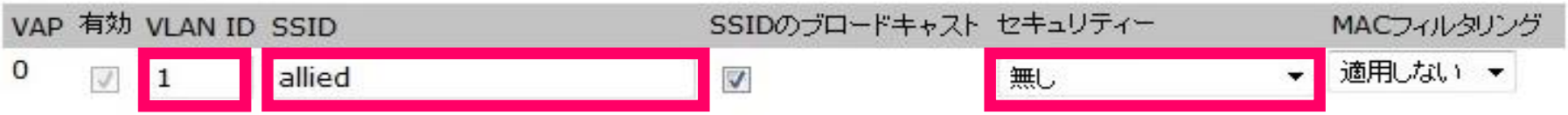
②【SSID】に下記を入力します。

SSID：groupｘｘ　（ｘｘ＝グループ番号01～30）

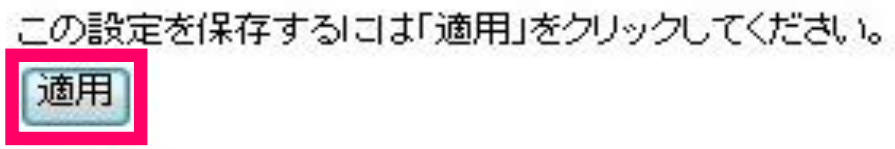
③【セキュリティー】で【WPAパーソナル】を選択し、下記を入力します。

キー：secretｘｘ　（ｘｘ＝グループ番号01～30）

④【適用】をクリックします。



下の方にスクロールすると適用があります



8.無線LAN設定

⑤【無線LAN設定】をクリックします。

⑥【オン】を選択します。

⑦【適用】をクリックします。

9.イーサネット設定

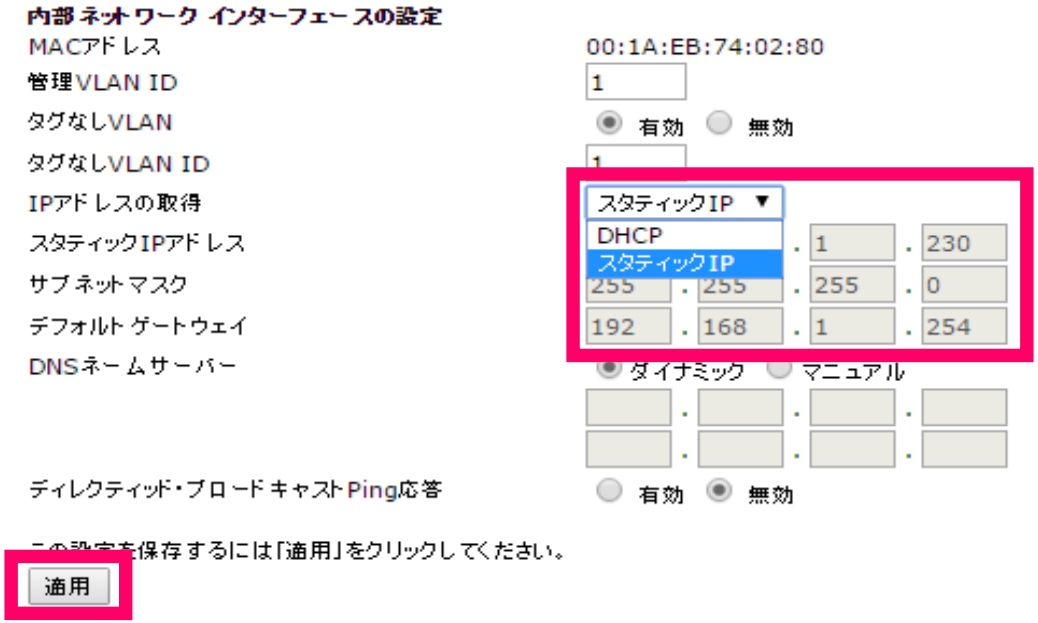
①【イーサネット設定】をクリックします。

9.イーサネット設定

②【IPアドレスの取得】の【スタティックIP】を選択し、下記を入力します。

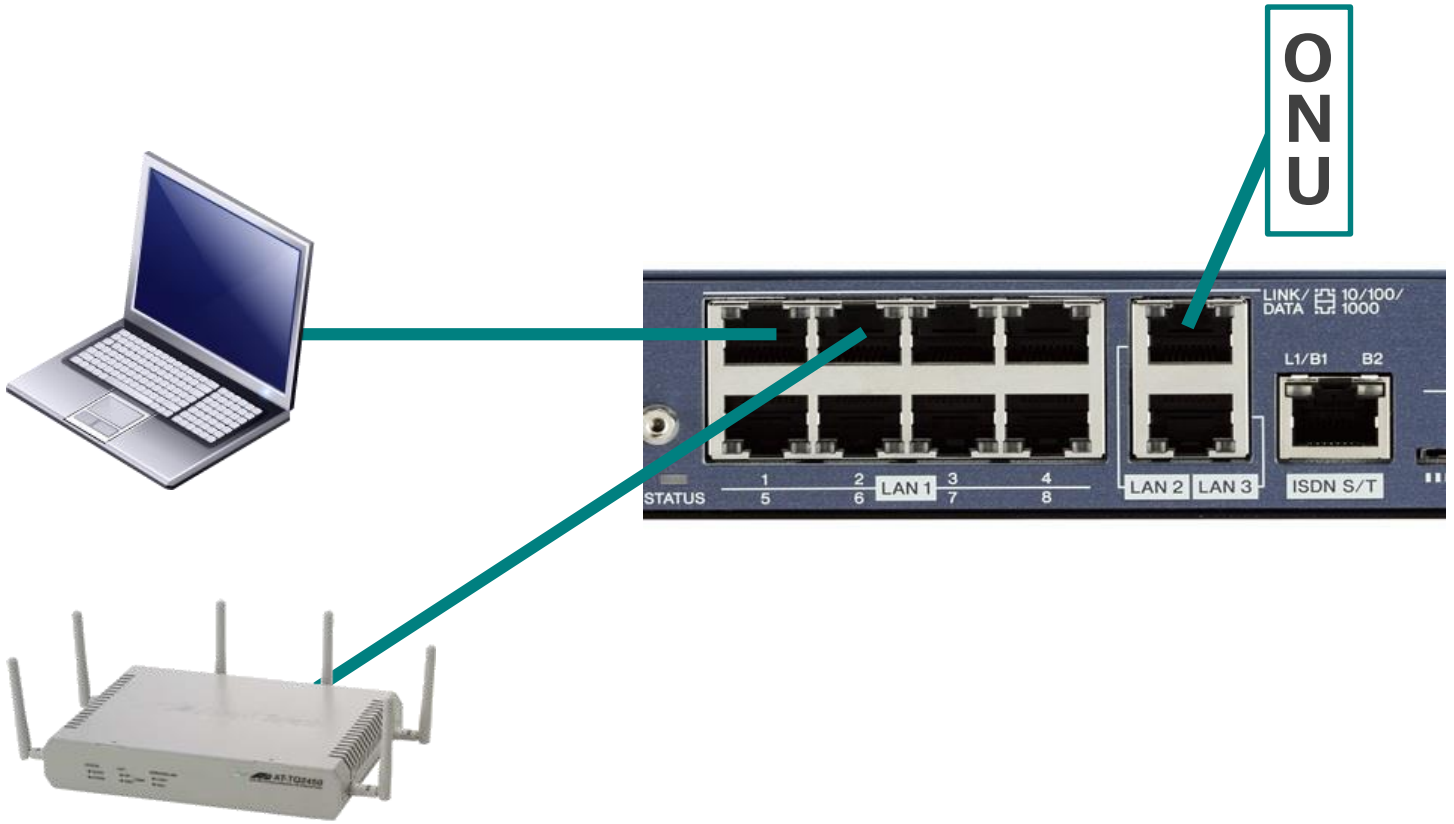
スタティックIPアドレス：192.168.1.50
サブネットマスク：255.255.255.0
デフォルトゲートウェイ：192.168.1.254

③【適用】をクリックします。



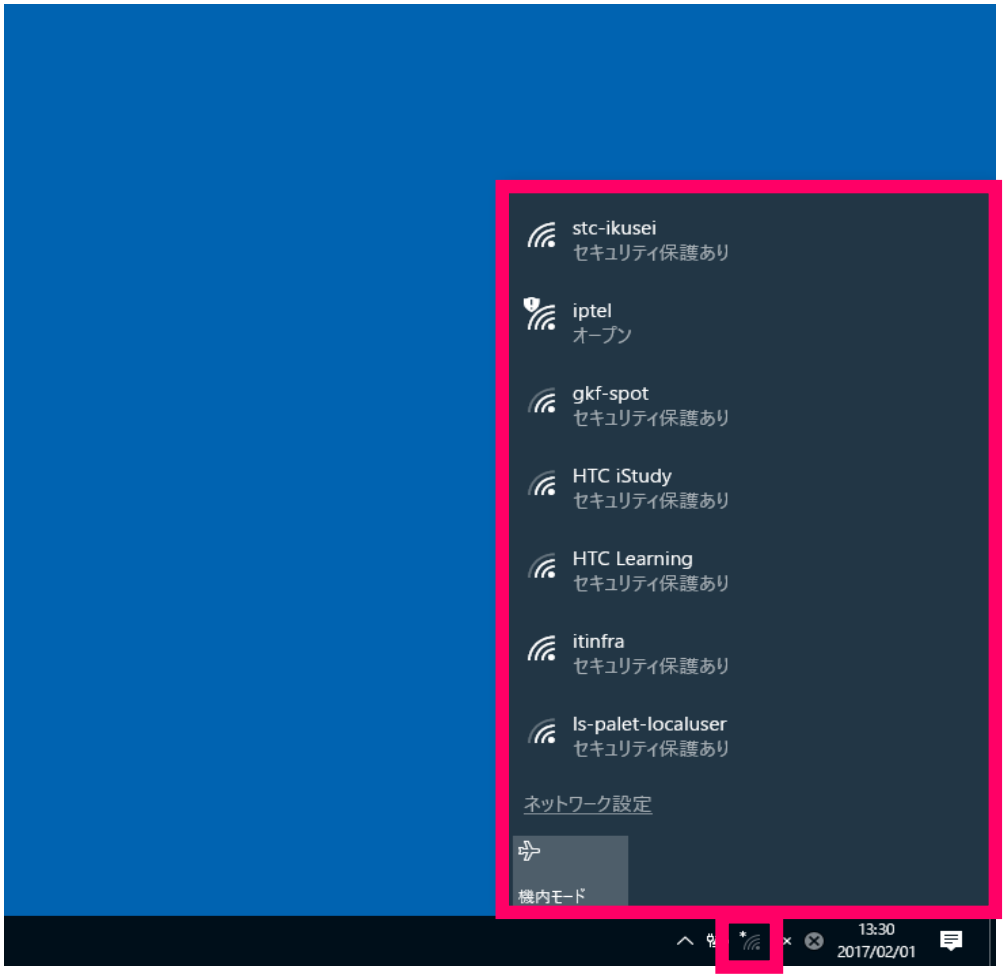
10.LANケーブル接続

①下記のようにLANケーブルを結線します。



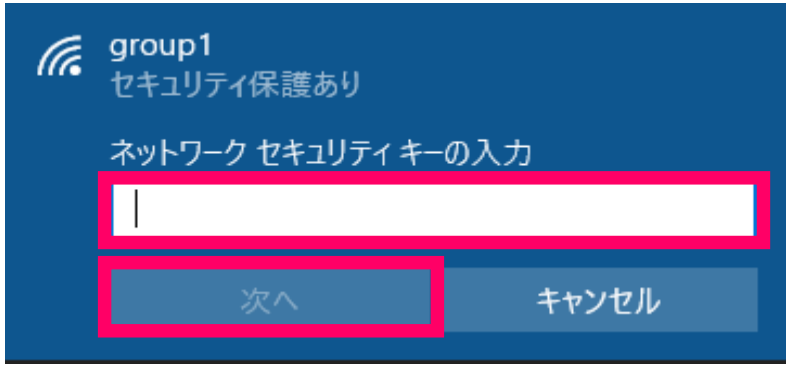
11.PCの無線設定

①  をクリックし、現在の接続先を表示します

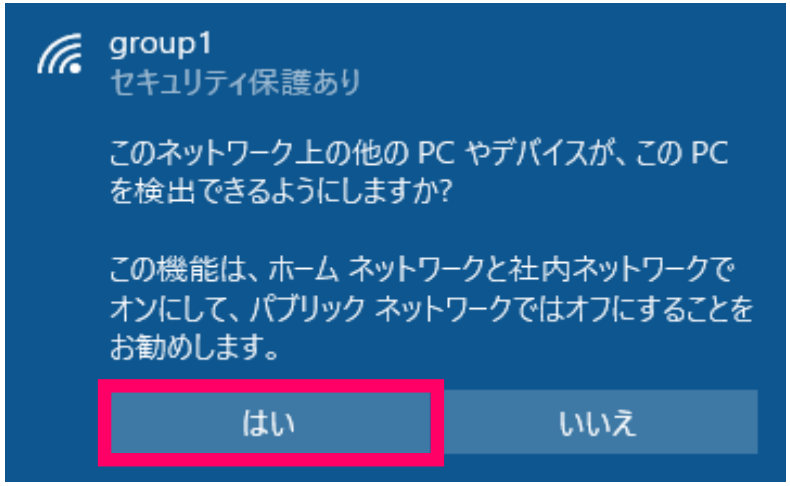


②【groupｘｘ】を選択し、【接続】をクリックします。
（ｘｘ=グループ番号01~30 ）

③【セキュリティキー】に下記を入力後、【次へ】をクリックします。
セキュリティキー：secret x x（x x =グループ番号01～30）



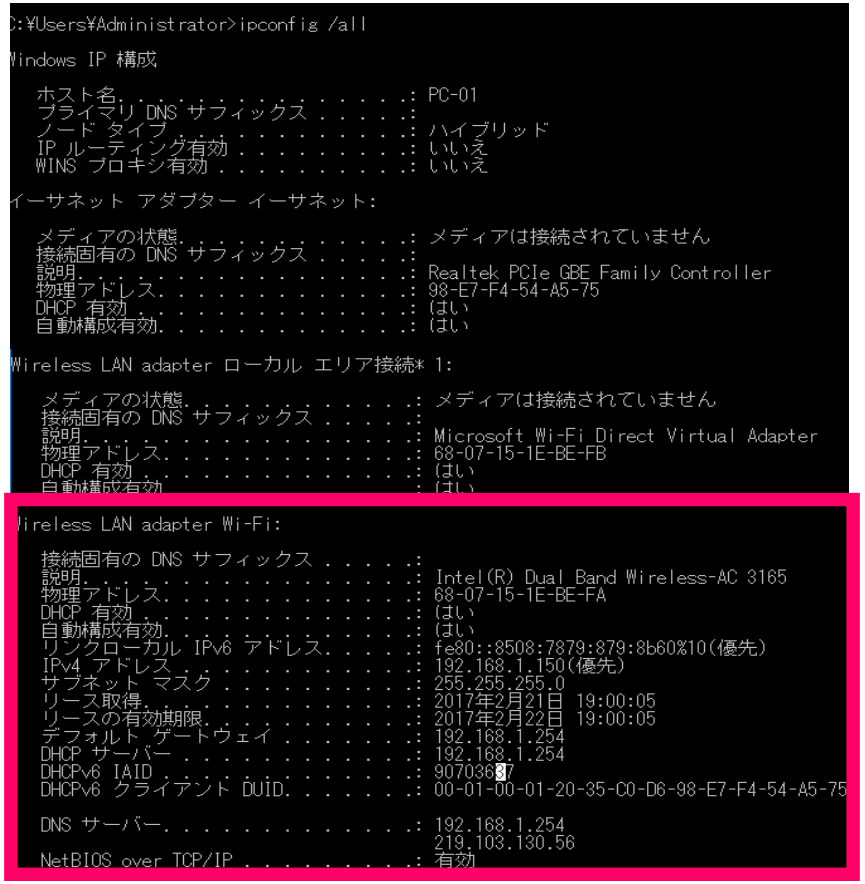
④下記の表示がでたら、【はい】をクリックします。



11.PCの無線設定

⑤【コマンドプロンプト】を起動します。

⑥【ipconfig /all】を入力し、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がDHCP自動取得内容を確認します。

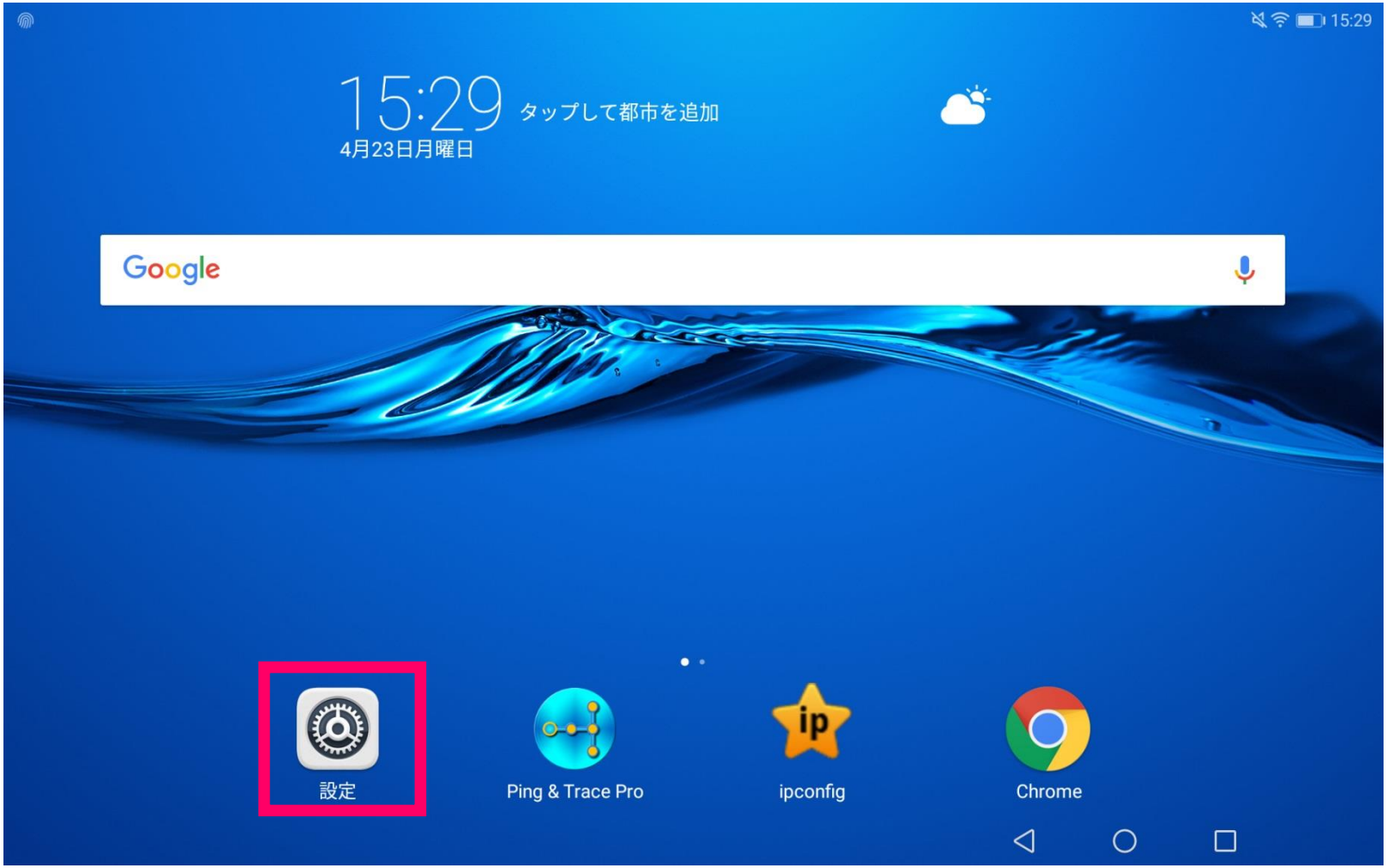


12.Androidの無線設定

①本体の電源ボタンを長押しし、タブレットを起動します。

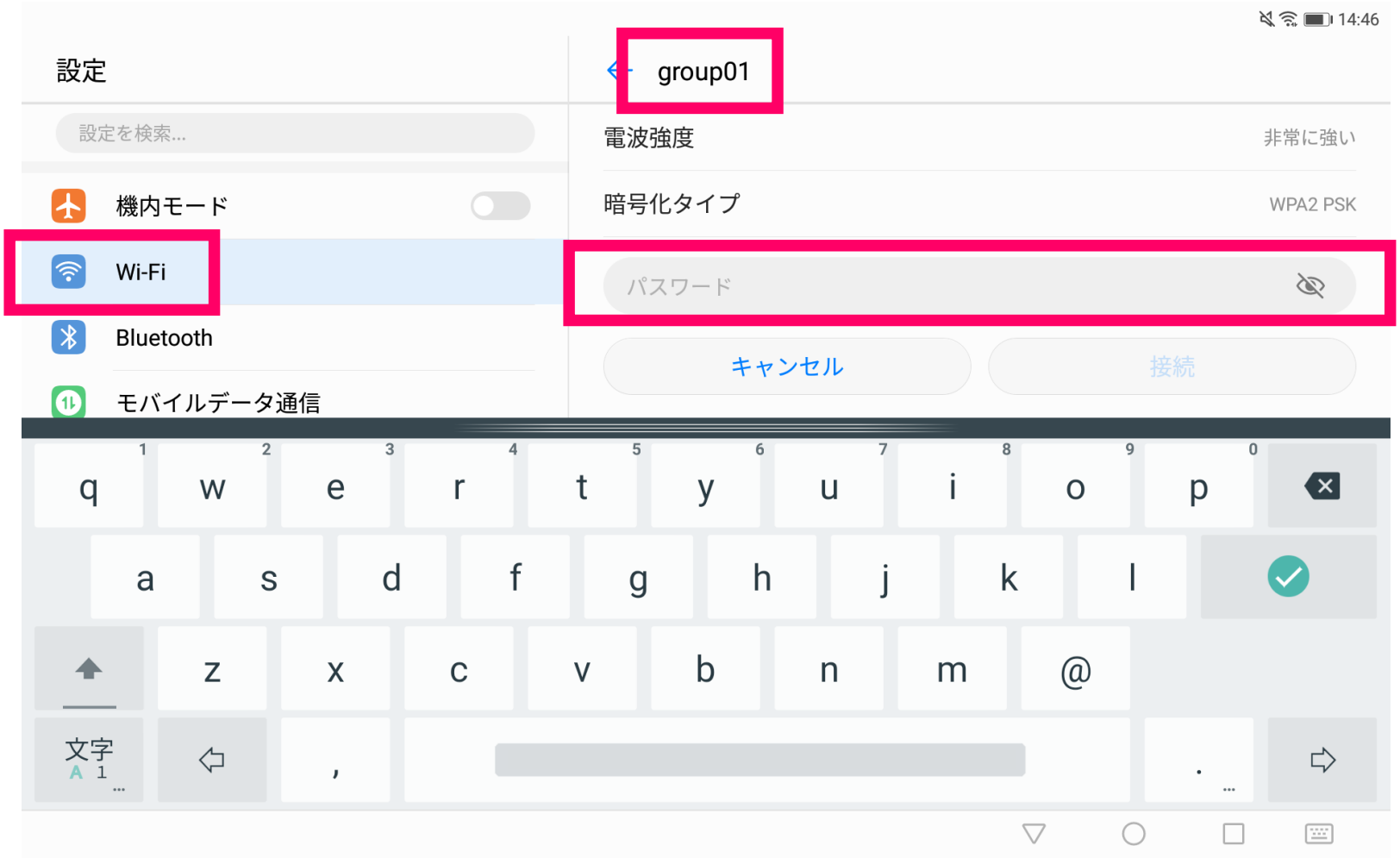
本体右側面の下側のボタンが
電源ボタンです

②ホーム画面の【設定】をタップします。

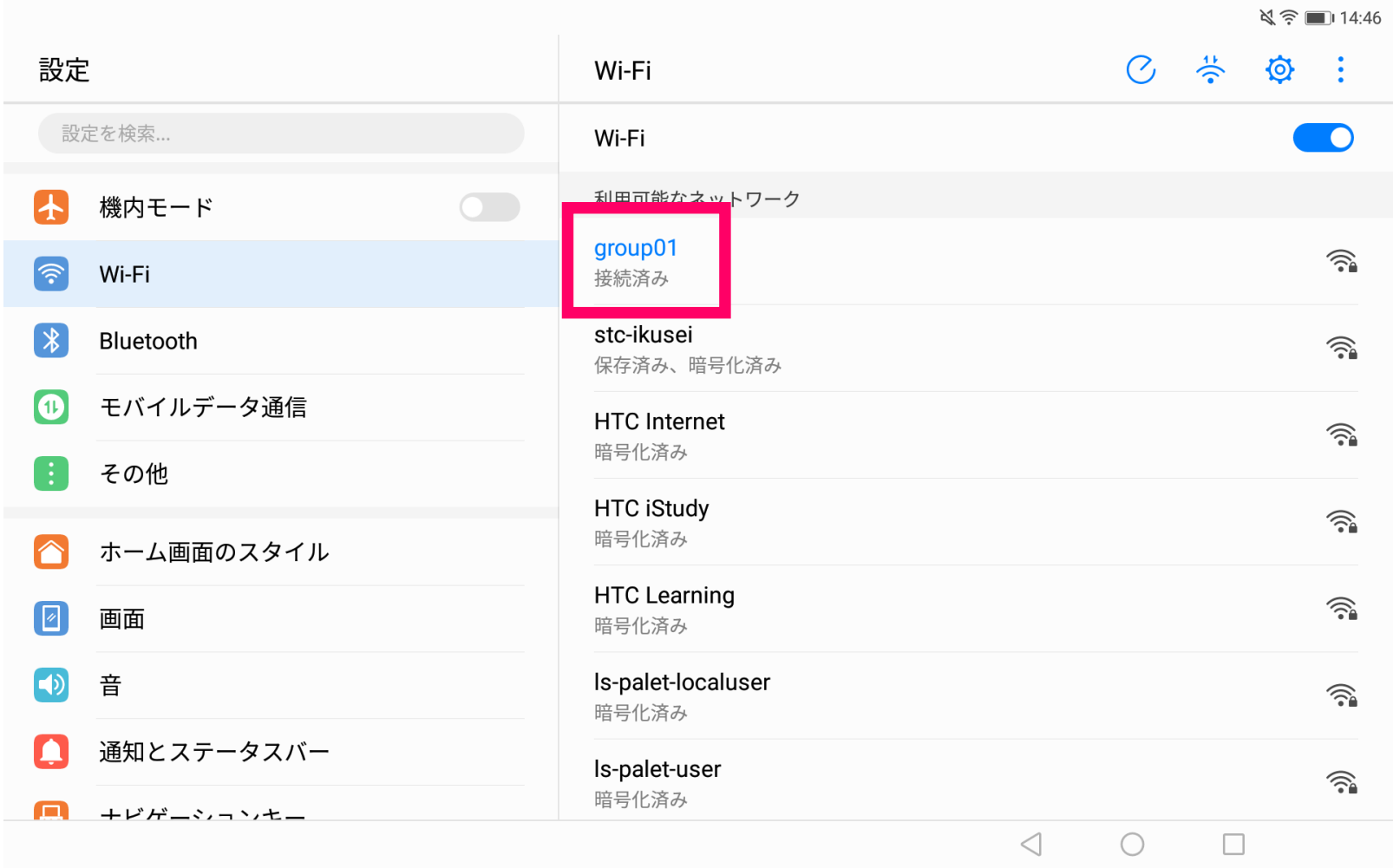


12.Androidの無線設定

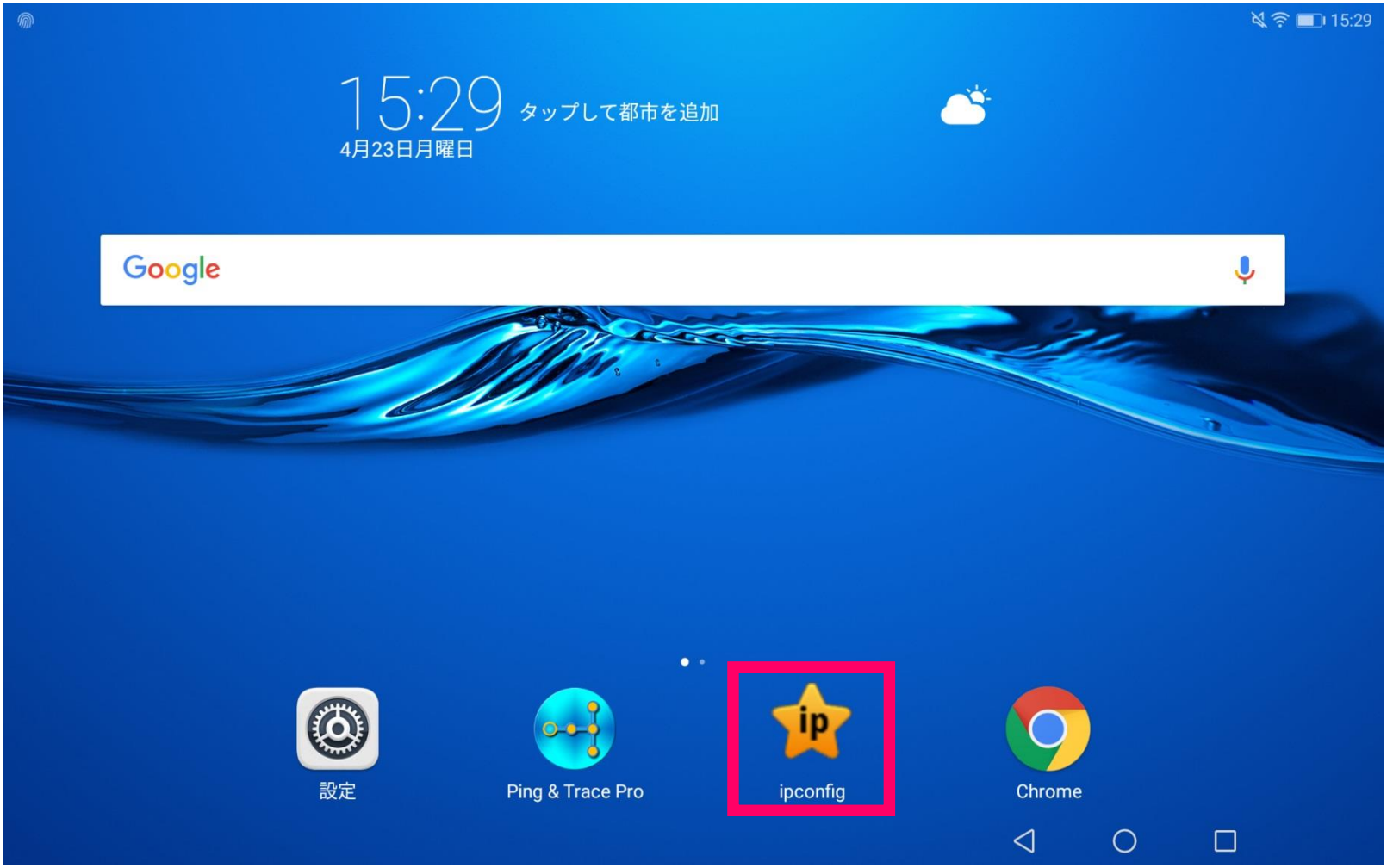
③左メニューの【Wi-Fi】から、下記SSIDを選んでパスワードを入力します。
SSID　　：groupｘｘ（ｘｘ＝グループ番号01～30）
パスワード　：secretｘｘ（ｘｘ＝グループ番号01～30）



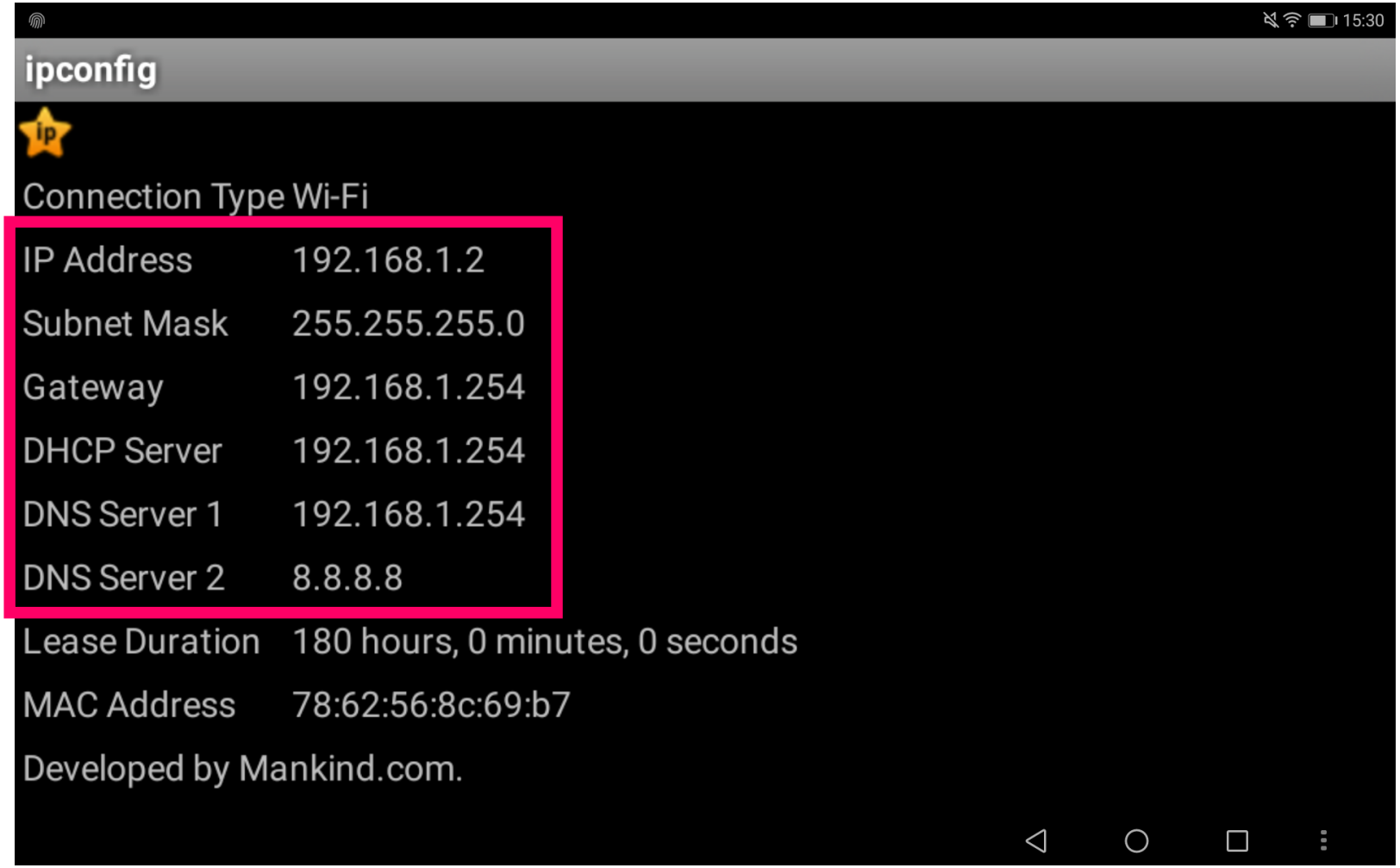
④SSIDの接続済み表示を確認します。



⑤ホーム画面の【ipconfig】をタップします。



⑥IPアドレス、サブネットマスク、デフォルトゲートウェイ、DNSなどのDHCP自動取得内容を確認します。



13.インターネット開通試験

①両方のPCで【コマンドプロンプト】を起動します。

②【ping 8.8.8.8】を入力し、応答があることを確認します。

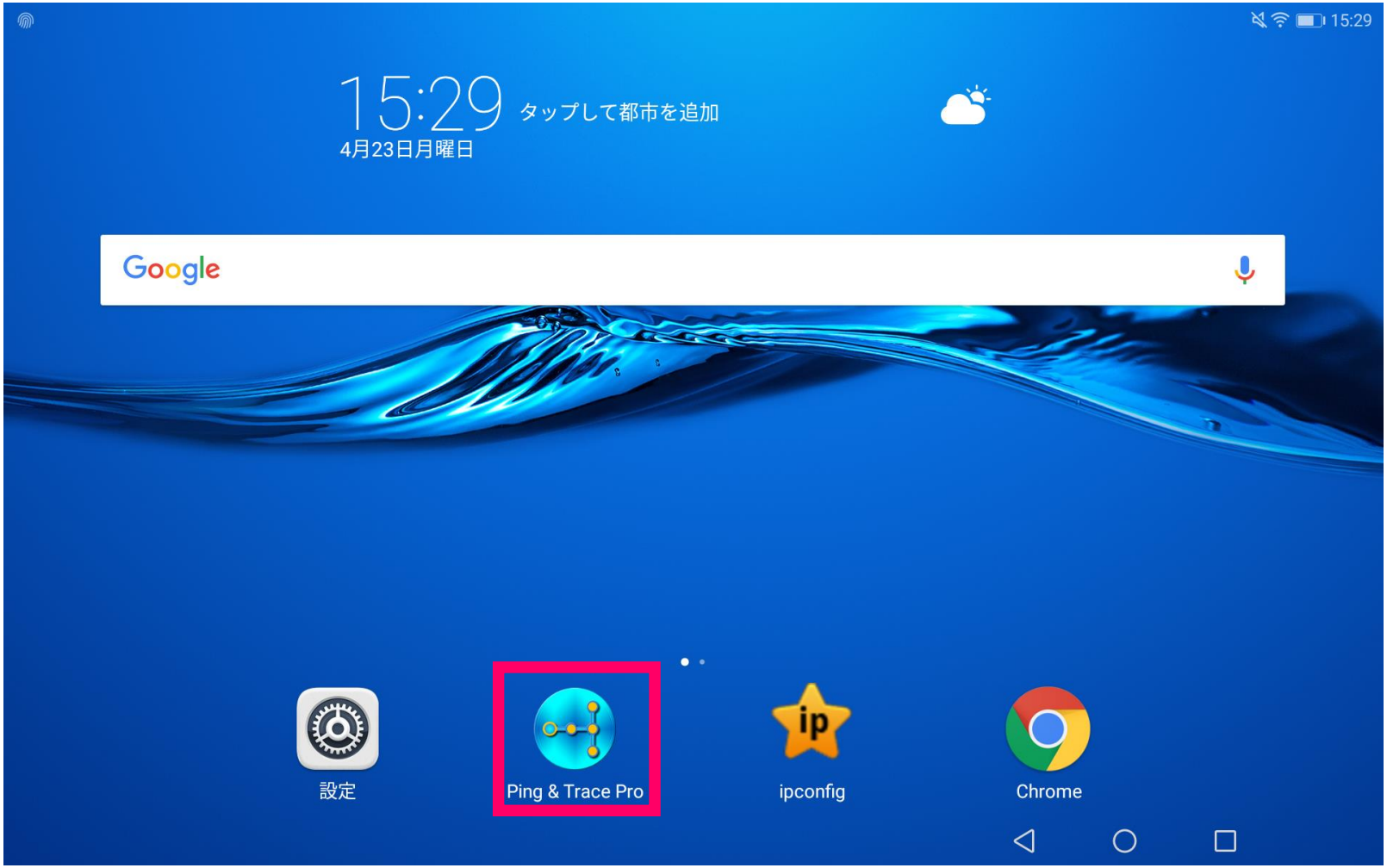
```
C:¥Users¥Administrator>ping 8.8.8.8

8.8.8.8 に ping を送信しています 32 バイトのデータ:
8.8.8.8 からの応答: バイト数 =32 時間 =44ms TTL=55
8.8.8.8 からの応答: バイト数 =32 時間 =40ms TTL=55
8.8.8.8 からの応答: バイト数 =32 時間 =44ms TTL=55
8.8.8.8 からの応答: バイト数 =32 時間 =42ms TTL=55

8.8.8.8 の ping 統計:
    パケット数: 送信 = 4、受信 = 4、損失 = 0 (0% の損失)、
ラウンド トリップの概算時間 (ミリ秒):
    最小 = 40ms、最大 = 44ms、平均 = 42ms
```

③【tracert　-d 8.8.8.8】を入力しGooglePublicDNSまでの経路を確認します。

```
C:¥Users¥Administrator>tracert -d 8.8.8.8

8.8.8.8 へのルートをトレースしています。経由するホップ数は最大 30 です

  1     1 ms    <1 ms     1 ms  192.168.1.254
  2     1 ms     1 ms     3 ms  172.20.1.2
  3     2 ms     1 ms     1 ms  172.20.1.1
  4    43 ms    40 ms    40 ms  61.115.19.50
  5    41 ms    43 ms    41 ms  61.115.21.53
  6    37 ms    35 ms    32 ms  61.115.20.177
  7    45 ms    62 ms    38 ms  211.9.229.134
  8    48 ms    44 ms    46 ms  211.9.229.97
  9    35 ms    37 ms    32 ms  210.173.176.243
 10    45 ms    46 ms    43 ms  108.170.242.97
 11    42 ms    45 ms    36 ms  209.85.247.161
 12    42 ms    39 ms    35 ms  8.8.8.8

トレースを完了しました。
```

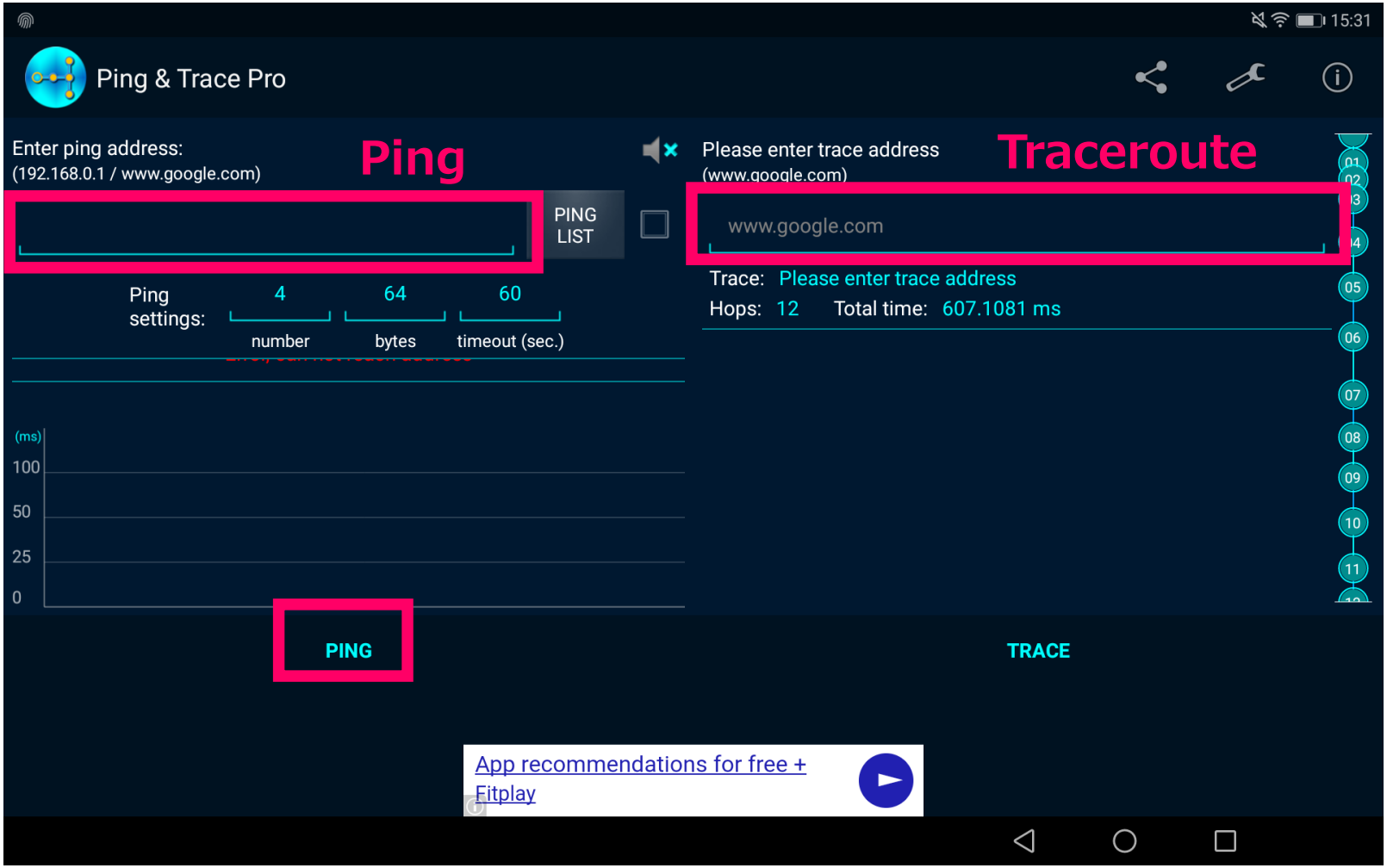
④ブラウザを起動しインターネット閲覧ができることを確認します。

⑤ホーム画面の【Ping & Trace Pro】をタップします。



13.インターネット開通試験

⑥Ping欄に【8.8.8.8】を入力し、【PING】をタップします。
⑦Traceroute欄に【8.8.8.8】を入力し、【TRACE】をタップします。



13.インターネット開通試験

⑧ GooglePublicDNSからPingによる応答と経路を確認します。

⑨ブラウザを起動しインターネット閲覧ができることを確認します。

演習③
実機を使用して
機器の設定情報を確認

演習③機器の設定情報を確認する

■実機で確認しながら、各機器の設定情報を埋めてください。

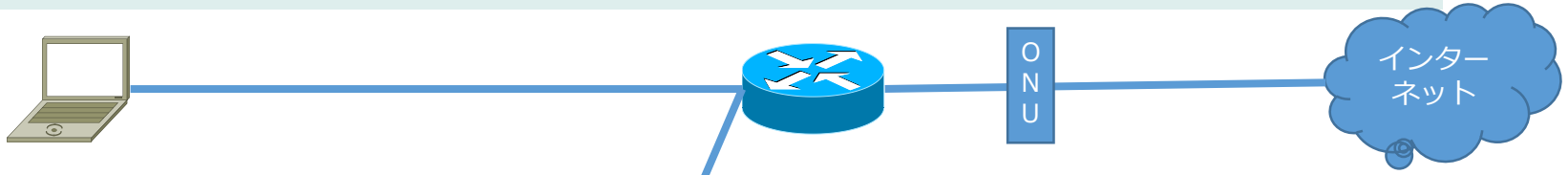
ルータ

LAN側

〔　　〕 IPアドレス
〔　　〕 サブネットマスク

WAN側

〔　　〕 IPアドレス
〔　　〕 サブネットマスク
〔　　〕 DNS

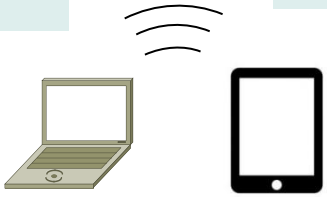


有線パソコン

〔　　〕 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

アクセスポイント

〔　　〕 IPアドレス
〔　　〕 サブネットマスク
〔　　〕 デフォルトゲートウェイ



無線パソコン

〔　　〕 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

タブレット

〔　　〕 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

2章
LANの構成

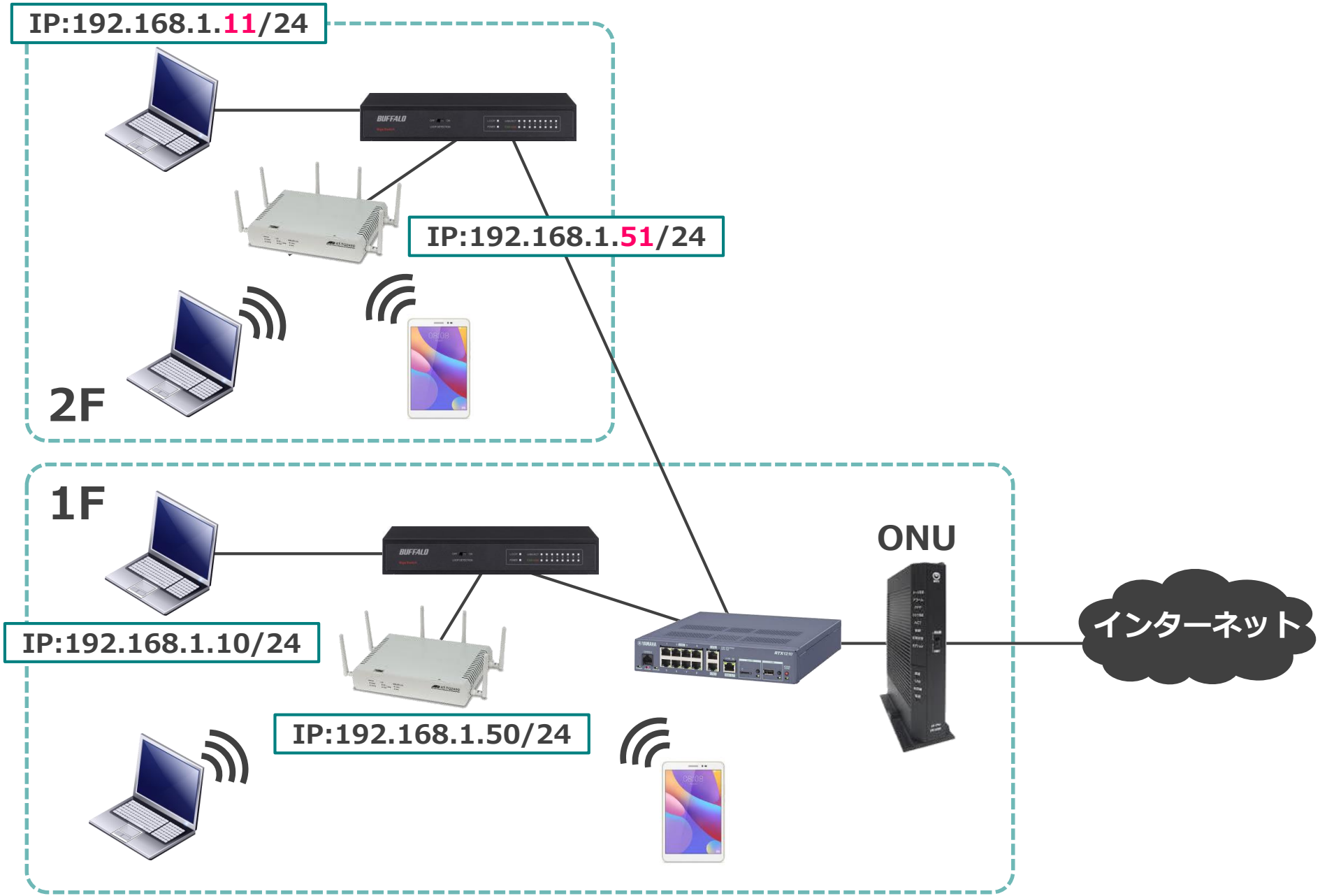
演習①
LANの構成に必要な機器

演習①LANの構成に必要な機器

1F、2Fとフロアを分けてLANを構成するためにはどのような構成になるか想像し、下部の記入欄に構成図を描いて下さい。
なお、1Fにフレッツ光が1回線あるものとし、各フロアには有線PC3台、無線PC2台、タブレット1台がインターネット通信をできるものとする。

演習②
LAN環境の構築（フロアを分ける）

演習構成

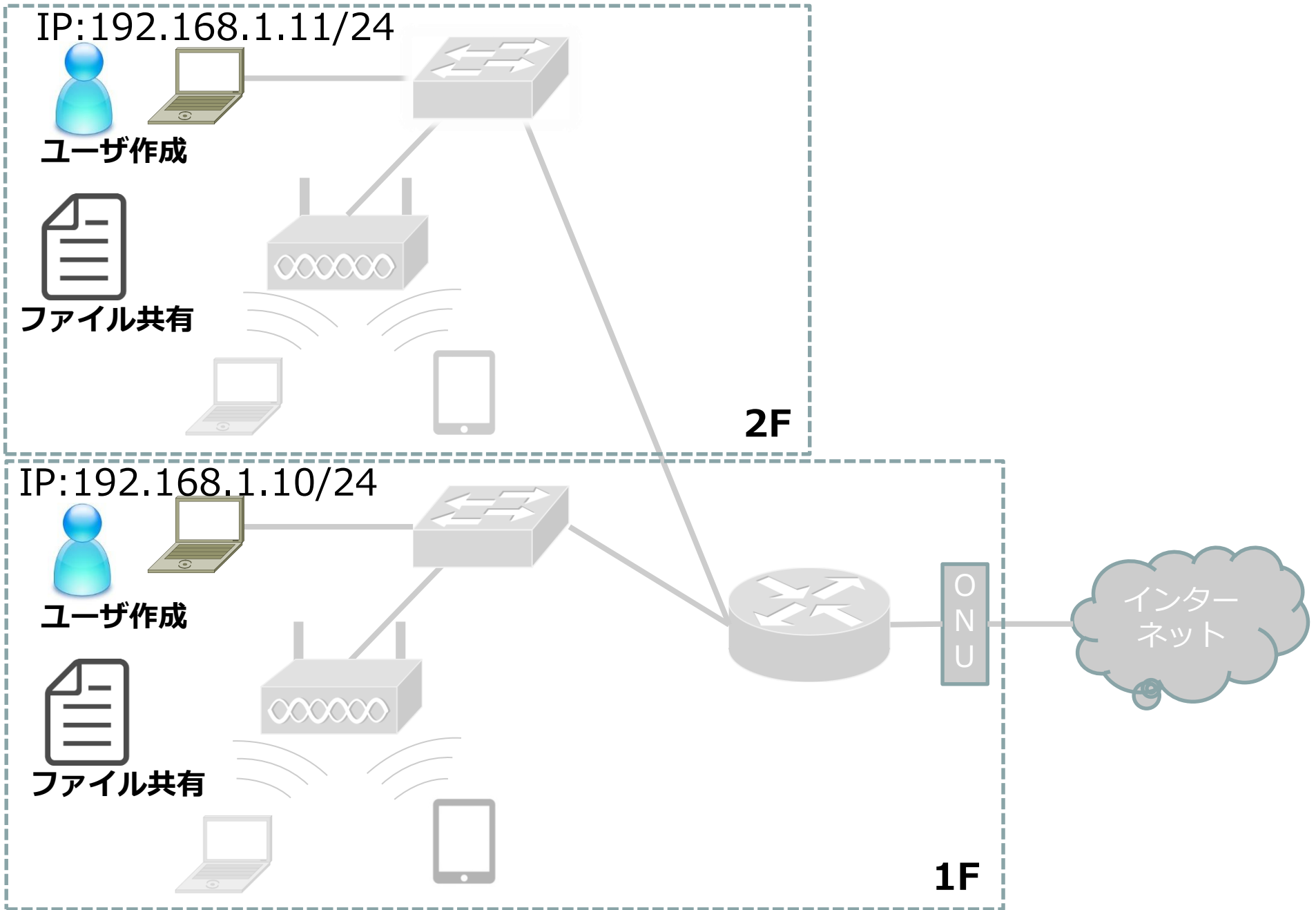

IP:192.168.1.11/24
IP:192.168.1.51/24
2F
1F
IP:192.168.1.10/24
IP:192.168.1.50/24
ONU
インターネット

●演習内容

① 有線PC、APのIPアドレス重複をなくします。
② 各フロアごとにSW-HUBを接続します。
③ DHCPによるIP取得端末は再起動する。
④ SSIDはフロアごとの無線を識別するため、そのままにします。
⑤ 各端末からインターネット閲覧ができることを確認します。

演習③
LAN環境の構築（ファイル共有）

演習構成

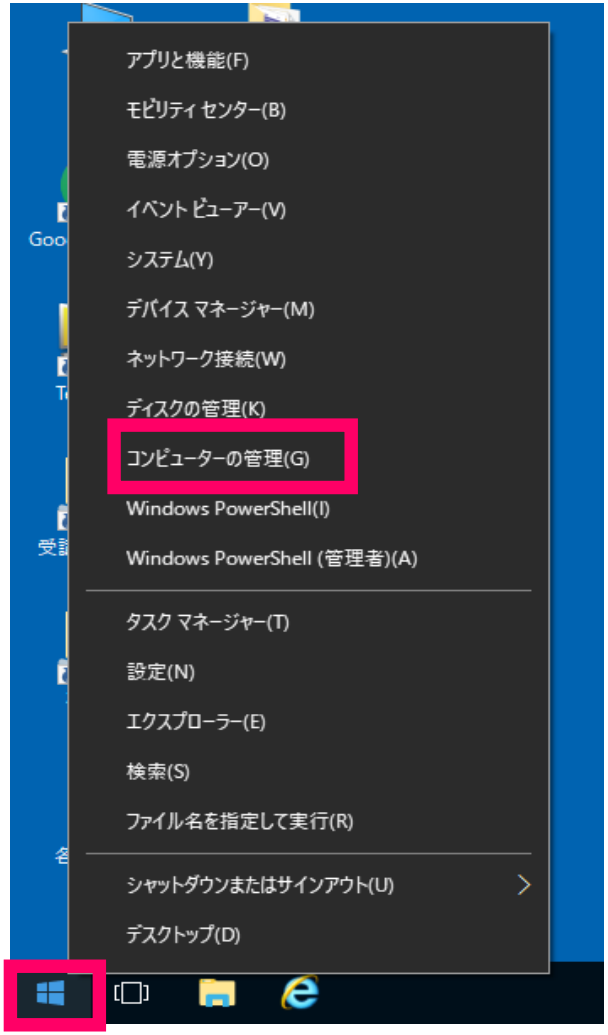

IP:192.168.1.11/24
ユーザ作成
ファイル共有
2F
IP:192.168.1.10/24
ユーザ作成
ファイル共有
1F
ONU
インター
ネット

●演習内容

- 有線PCにユーザを作成します（ユーザ名はアルファベットで受講生名）
- デスクトップに新規フォルダを作成し、フォルダ内にテキストファイルを作成します。
- 1Fと2Fの有線PCでお互いにファイル共有(閲覧）ができることを確認します。

1.ユーザアカウントの作成

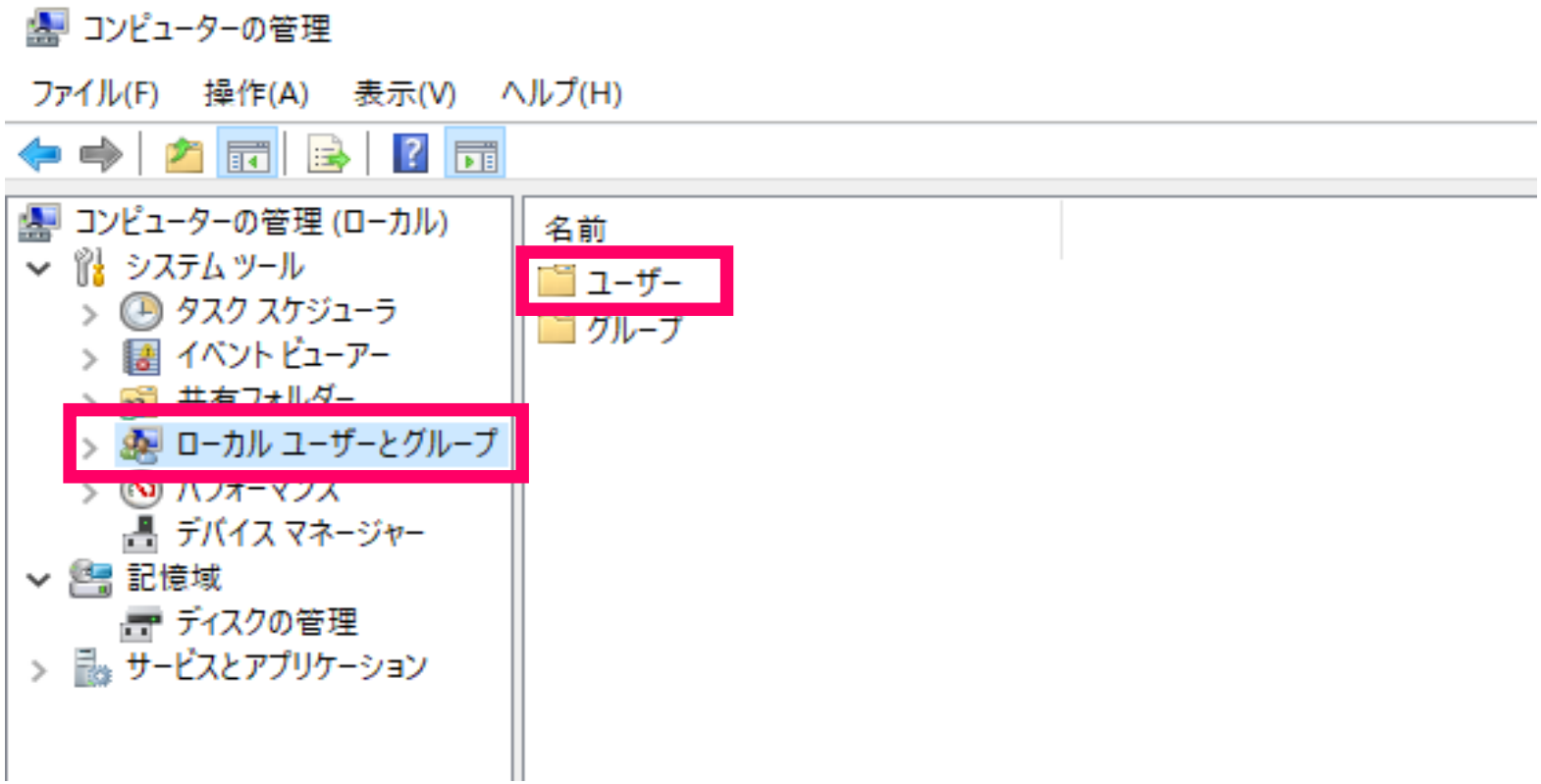
①スタートメニューを【右クリック】し、【コンピュータの管理】をクリックします。



1.ユーザアカウントの作成

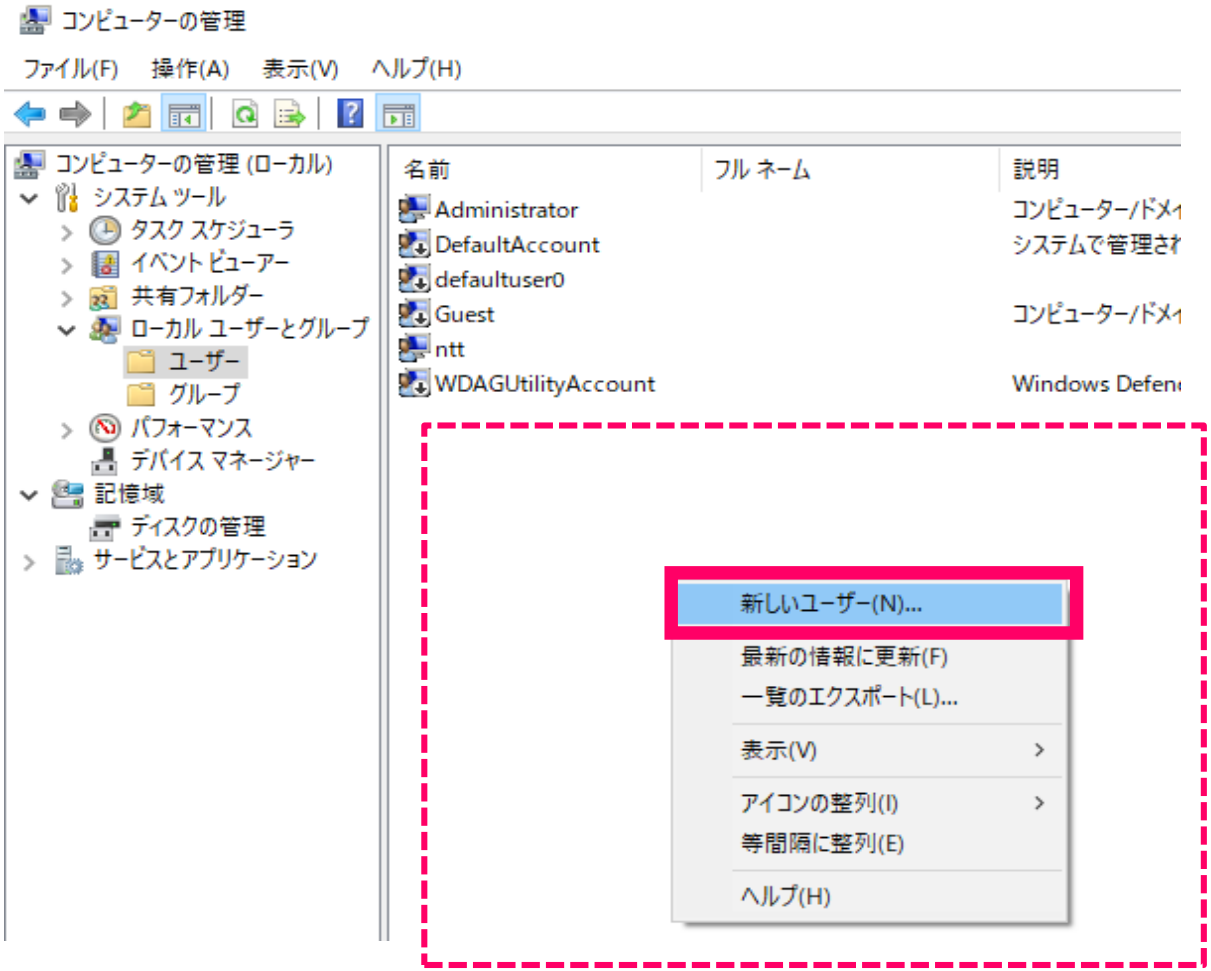
②コンピュータの管理画面から【ローカルユーザとグループ】をクリックします。

③【ユーザー】をクリックし開きます。



1.ユーザアカウントの作成

④余白部分（点線内側の任意の場所）で右クリックし、「新しいユーザ」をクリックします。

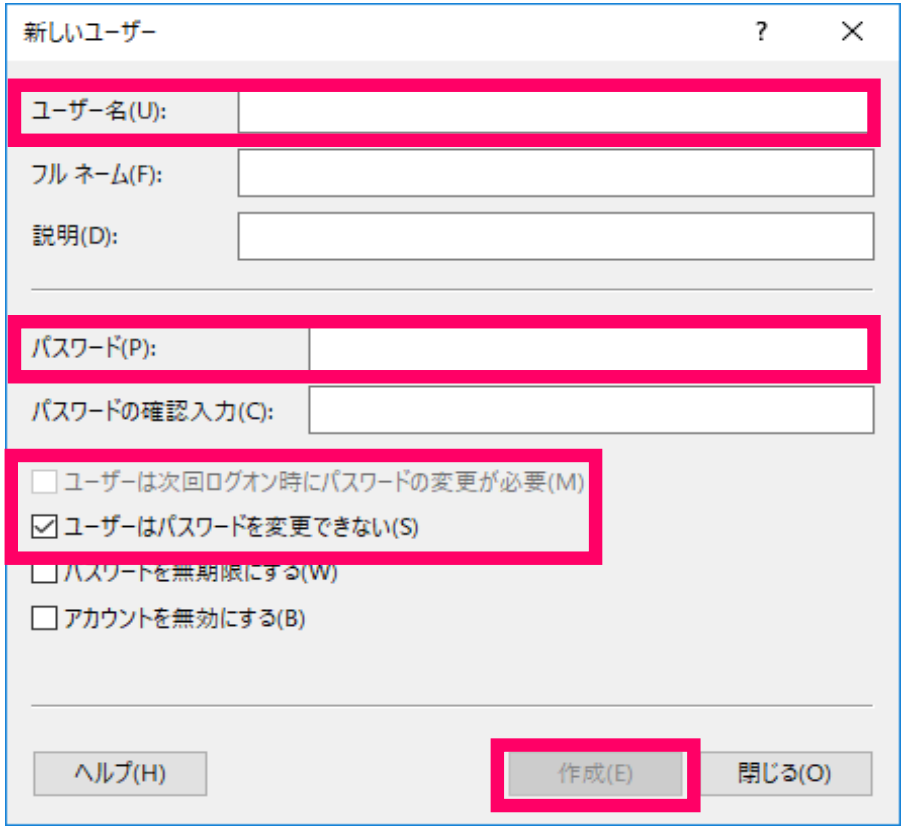


1.ユーザアカウントの作成

⑤以下の項目を設定し、【作成】ボタンを押下します。

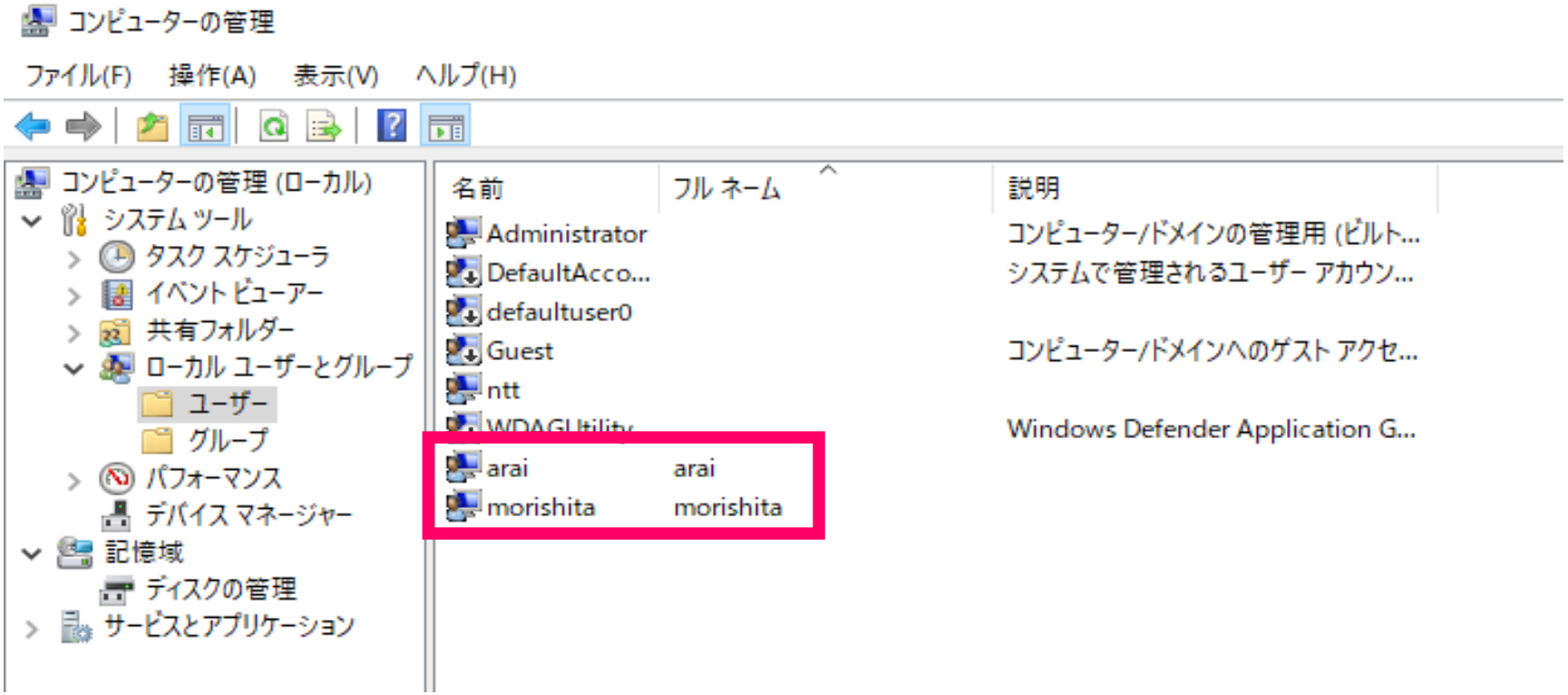
ユーザー名：アルファベット小文字で苗字（自分）
パスワード：アルファベット小文字で苗字（自分）
□ユーザは次回ログオン時にパスワードの変更が必要：**チェックを外す**
☑ユーザはパスワードを変更できない：**チェックを入れる**

⑥同様に**ファイル共有をさせたい相手**のユーザアカウントも作成します。



1.ユーザアカウントの作成

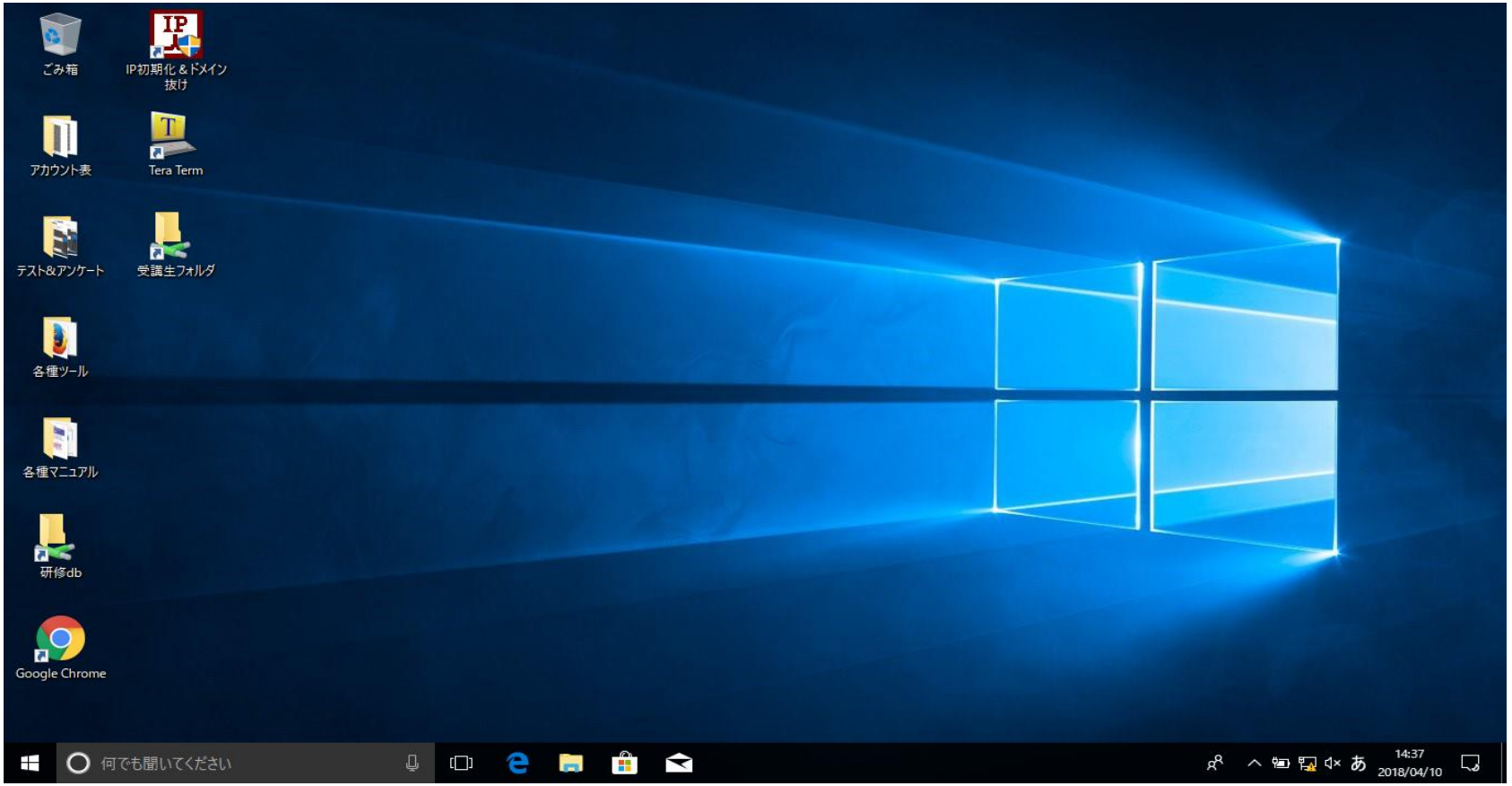
⑦ユーザー一覧に作成したユーザアカウント(自分と相手)が追加されていることを確認します。



2.作成したユーザでログイン

①PCを再起動し、作成したユーザ(自分)でログインします。

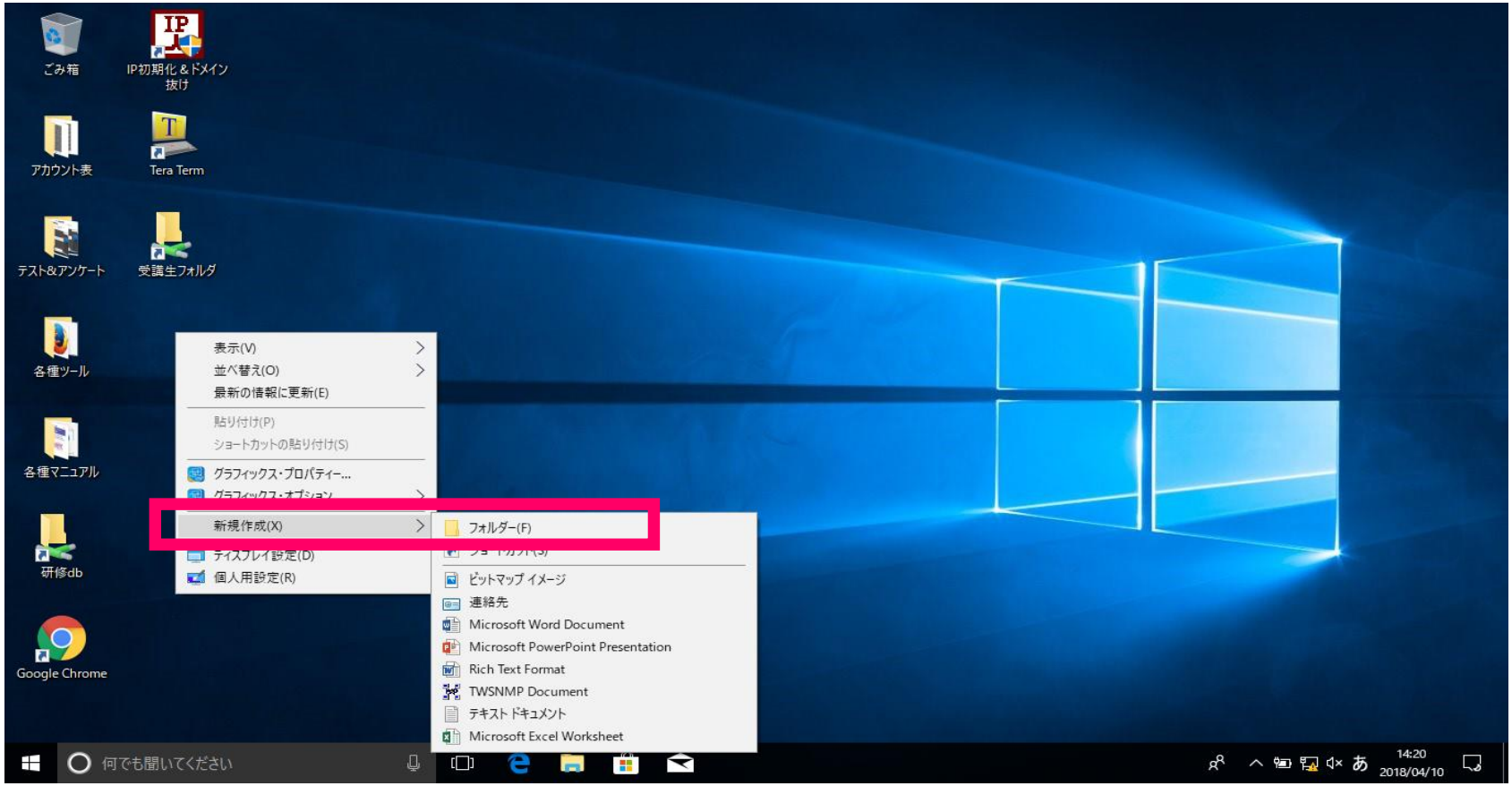
（初めてのログインのため、ユーザプロファイルを作成する時間が少しかかります）



3.共有フォルダ、共有ファイルの作成

①デスクトップの画面上で【右クリック】をし、【新規作成】⇒
【フォルダー】をクリックします。

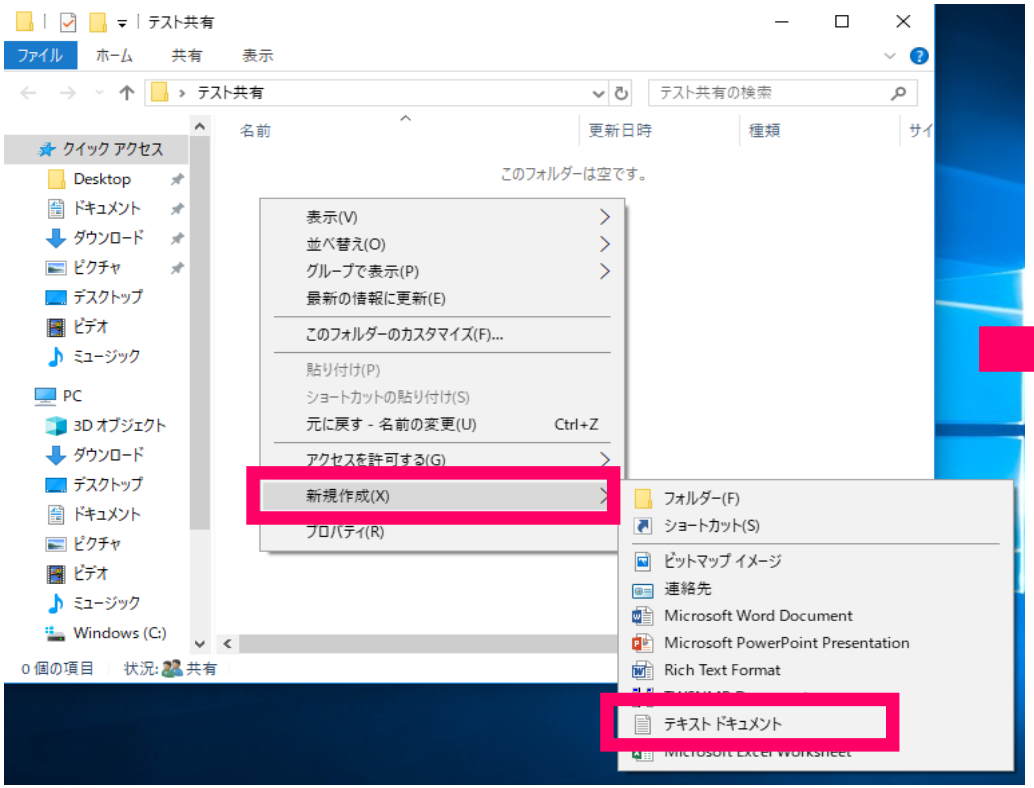
②フォルダのファイル名を「テスト共有」とします。

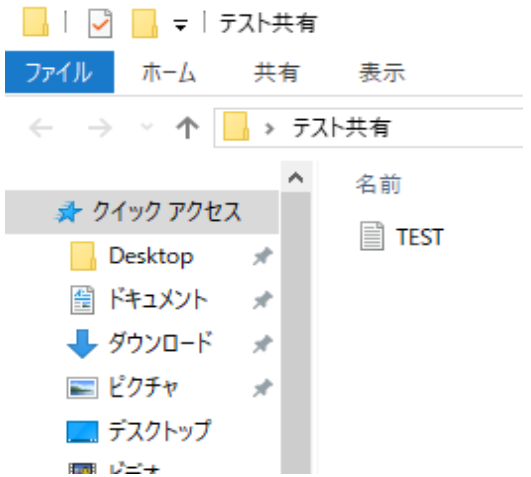


3.共有フォルダ、共有ファイルの作成

③テスト共有フォルダ内で【右クリック】し、【新規作成】⇒【テキストドキュメント】をクリックします。

④共有ファイル名を「TEST」とします。

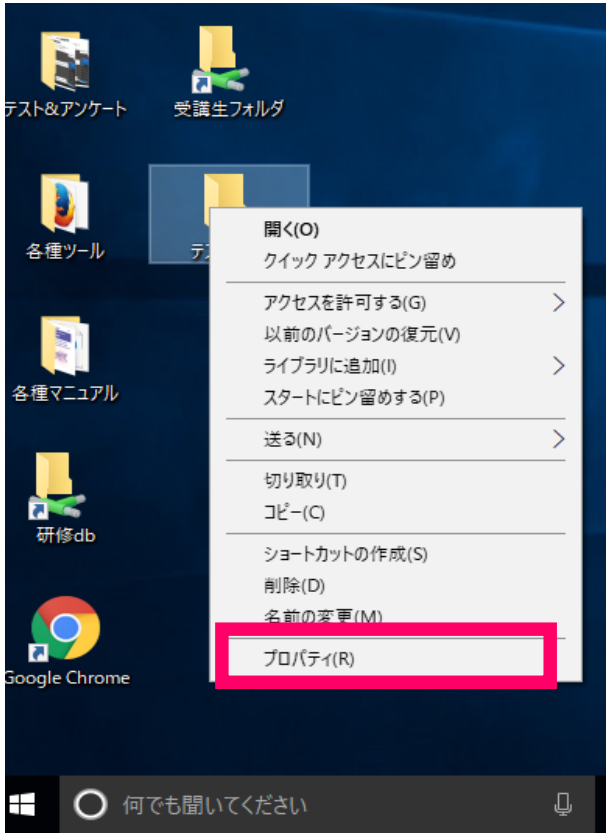


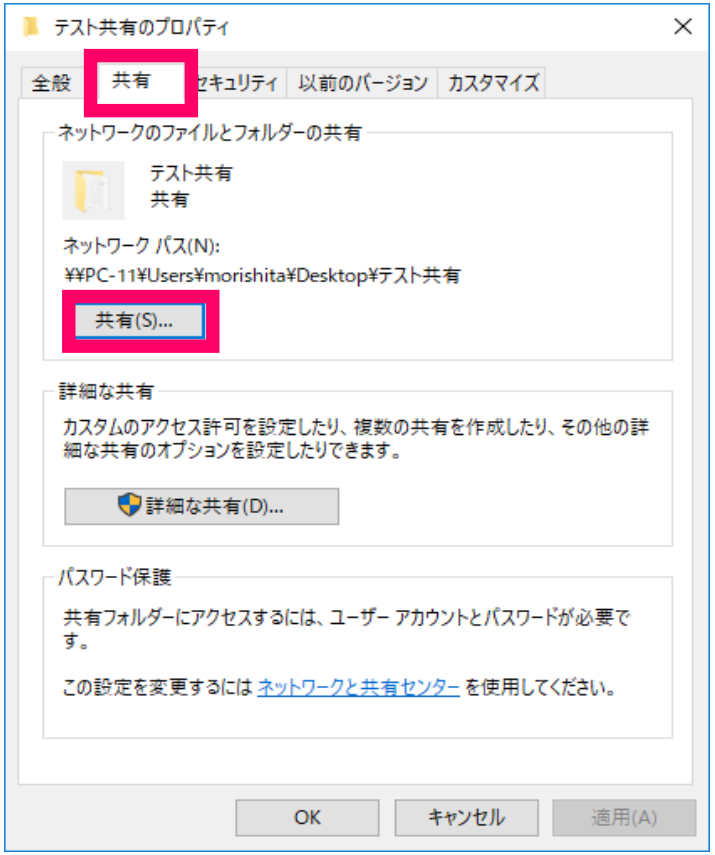


4.ファイル共有の設定

①テスト共有フォルダを【右クリック】し、【プロパティ】をクリックします。

②【共有タブ】をクリックし、【共有】ボタンを押下します



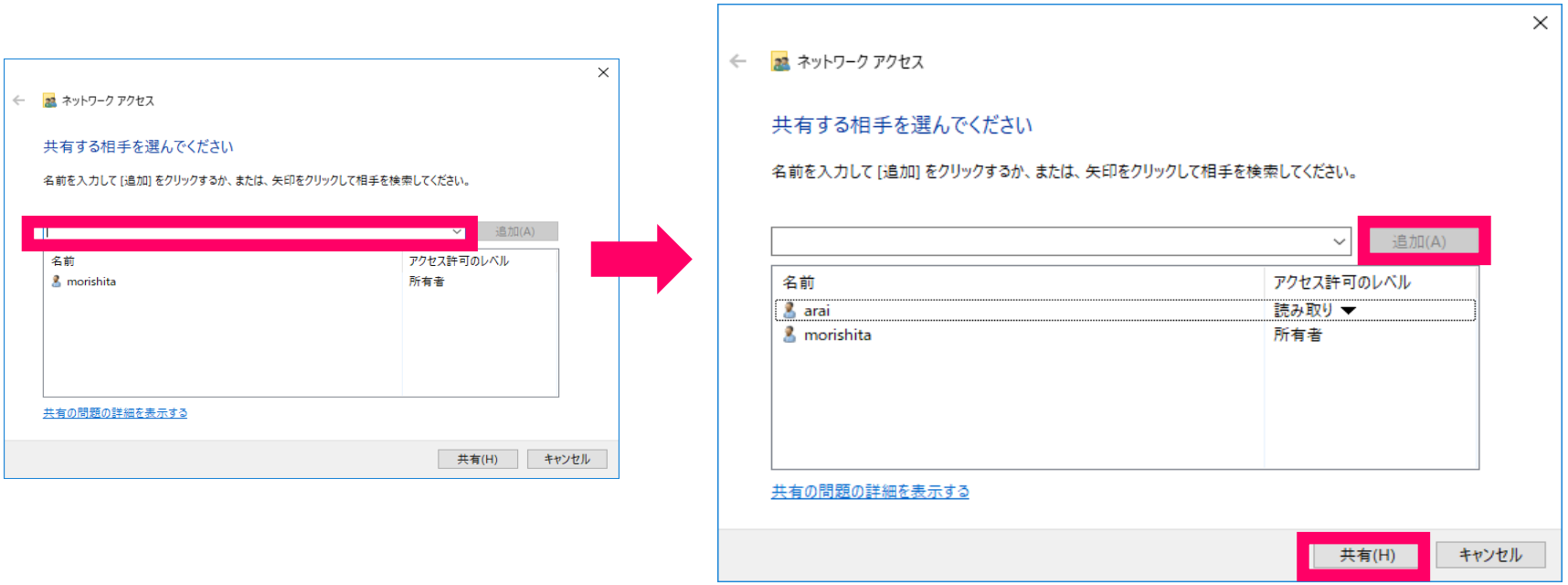


4.ファイル共有の設定

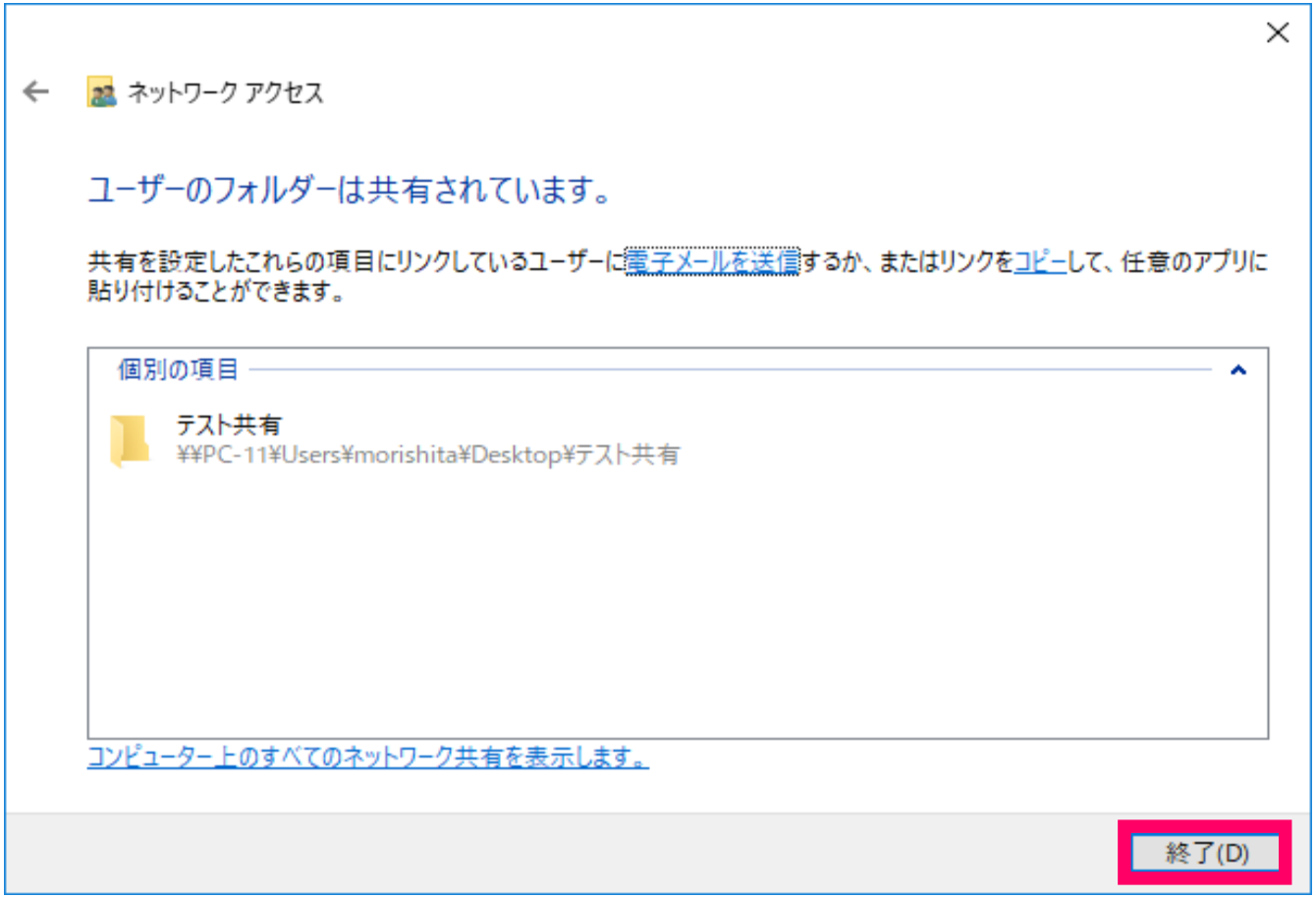
③ネットワークアクセスの画面で、プルダウンから共有させたい相手ユーザを選択します。

④選択後、【追加】ボタンをクリックし、共有させたい相手ユーザを登録します。

⑤追加後、【共有】ボタンをクリックします。



⑥最後に【終了】ボタンをクリックします。

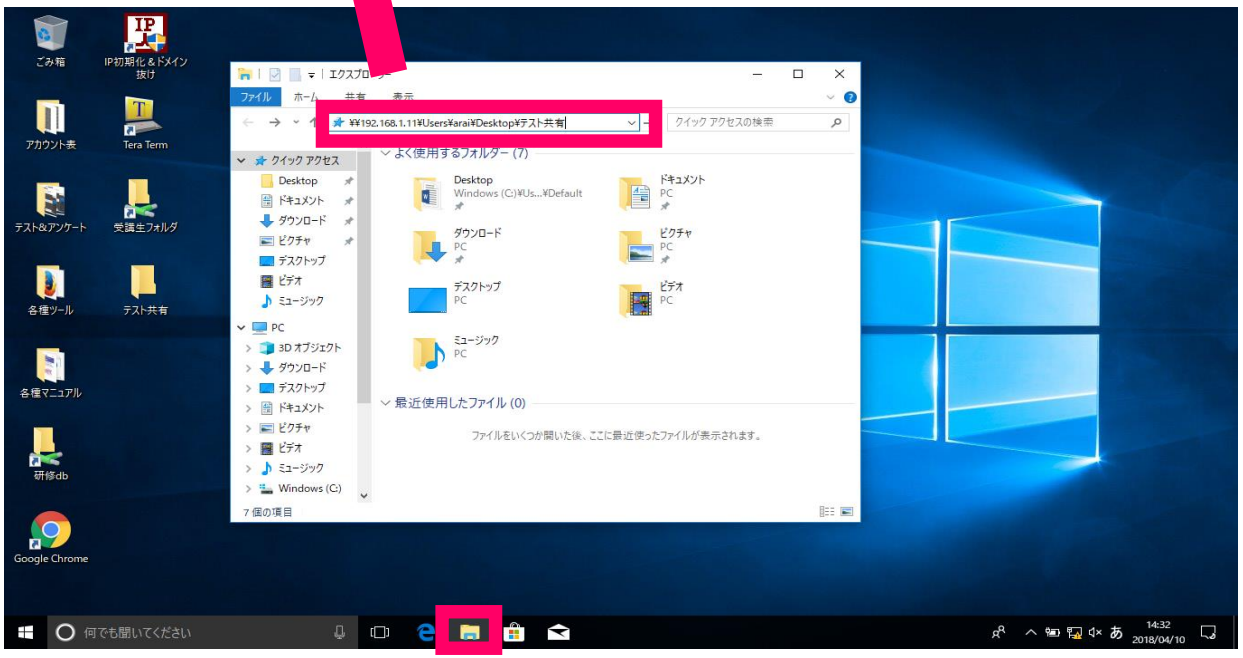


5.ファイル共有の確認

①タスクバーにある【エクスプローラー】アイコンをクリックし開きます。

②アドレスバーに共有ファイルが置かれている場所へのUNCパスを入力します。

UNCパス例



3章
トラブルから学ぶネットワーク基礎

トラブルから学ぶネットワーク基礎

①IPアドレスの重複

どんな現象が起きると思いますか？

メモ

現象の確認

メモ

②デフォルトゲートウェイの未設定

どんな現象が起きると思いますか？

メモ

現象の確認

メモ

③DNSサーバの未設定

どんな現象が起きると思いますか？

メモ

現象の確認

メモ

④DHCPサーバの機能停止

どんな現象が起きると思いますか？

メモ

現象の確認

メモ

4章
LAN基礎問題

●IPアドレス計算問題①

ネットワーク部が27ビットのIPネットワークがある。このネットワークに最大何個のホストを接続して同時に利用できるか。正しいものを1つ選びなさい。

●選択肢

a：　5個
b：14個
c：27個
d：30個
e：32個
f　：62個

●IPアドレス計算問題②

172.16.16.5/30のブロードキャストアドレスはどれか。正しいものを１つ選びなさい。

●選択肢

a：172.16.16.4
b：172.16.16.7
c：172.16.16.9
d：172.16.255.255
e：172.16.16.0
f ：172.16.16.255

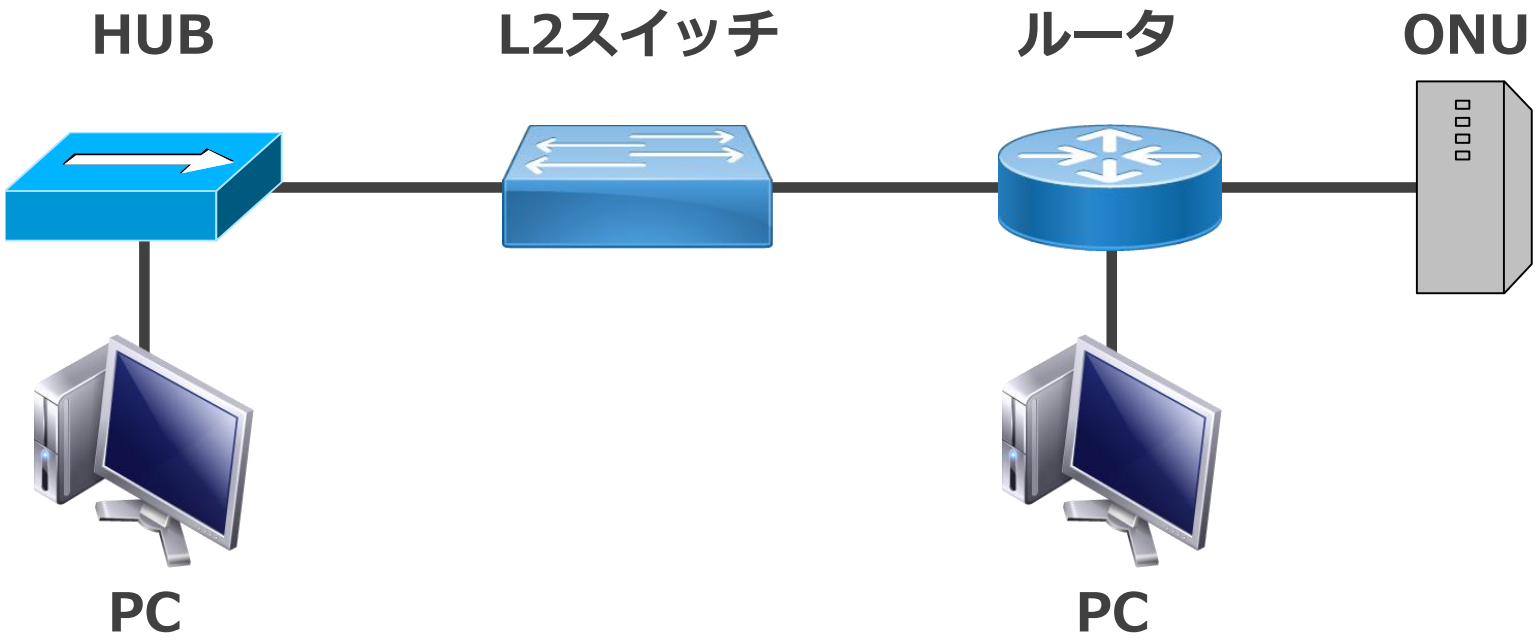
ルータのLAN側インターフェースのIPアドレス設定が以下の時、LAN内で接続可能なホストのIPアドレスを選択肢から正しいものを2つ選びなさい。

ネットワークアドレス	:192.168.1.0
サブネットマスク	:255.255.255.240
ルータLAN側インターフェース	:192.168.1.14

●選択肢

a：192.168.1.0
b：192.168.1.5
c：192.168.1.13
d：192.168.1.240
e：192.168.1.255
f ：192.168.0.1

各機器を接続するツイストペアケーブルの種類（クロスorストレート）は？

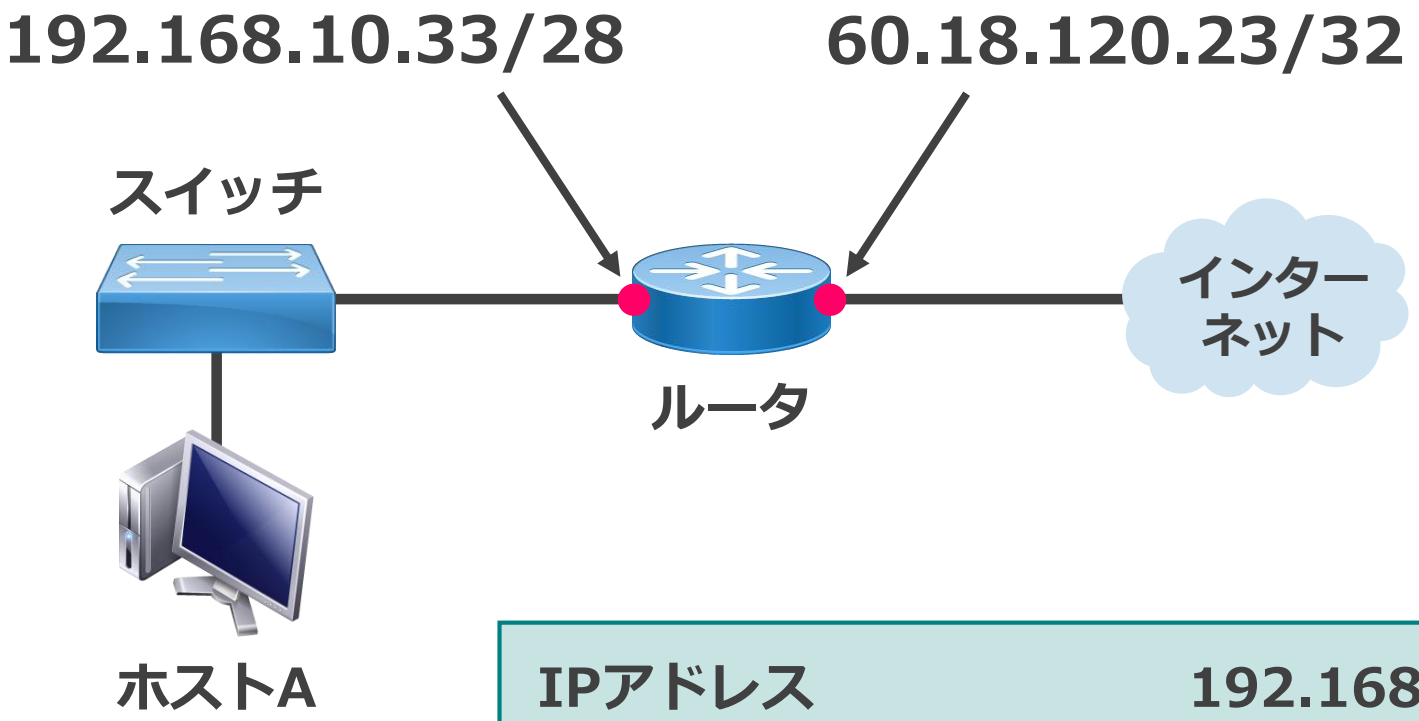


IPv4におけるループバックアドレスはどれか？

●選択肢

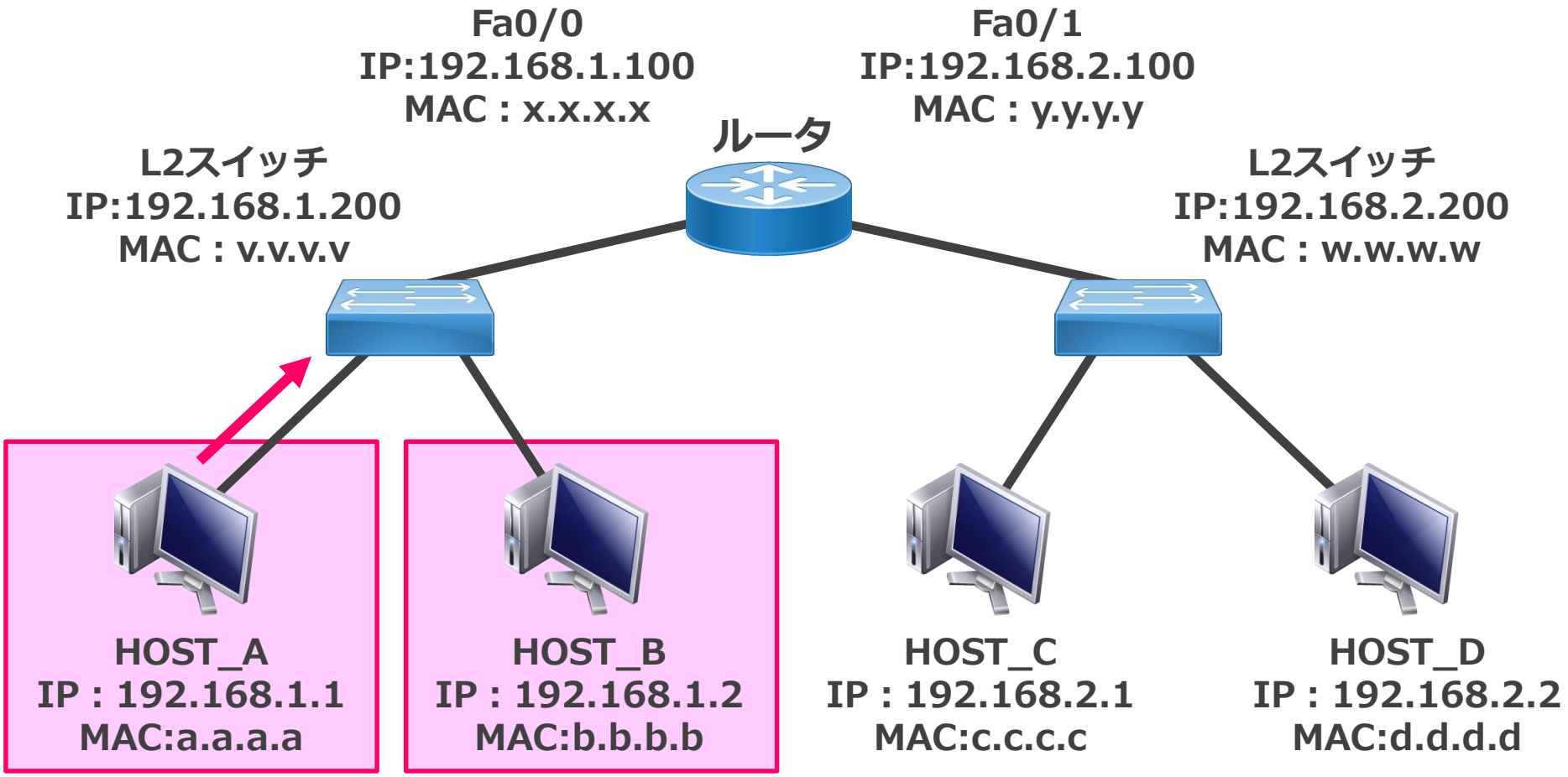
a：0.0.0.0
b：255.255.255.255
c：224.0.0.5
d：169.254.0.1
e：192.168.0.0
f ：127.0.0.1

ホストAがインターネットに接続できない。
接続するにはどのような設定変更が必要か?

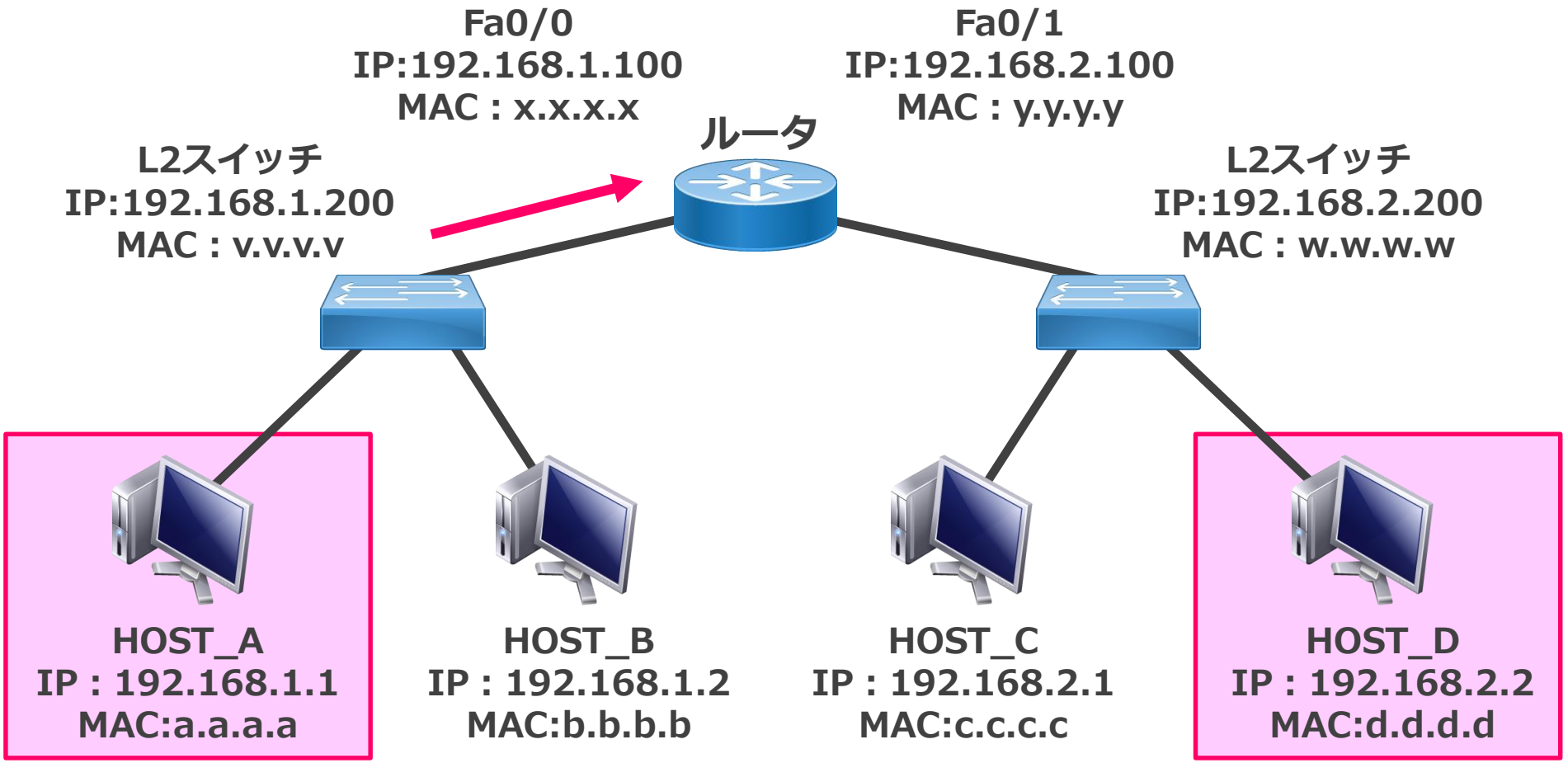


IPアドレス	192.168.10.44
サブネットマスク	255.255.255.240
デフォルトゲートウェイ	60.18.120.23

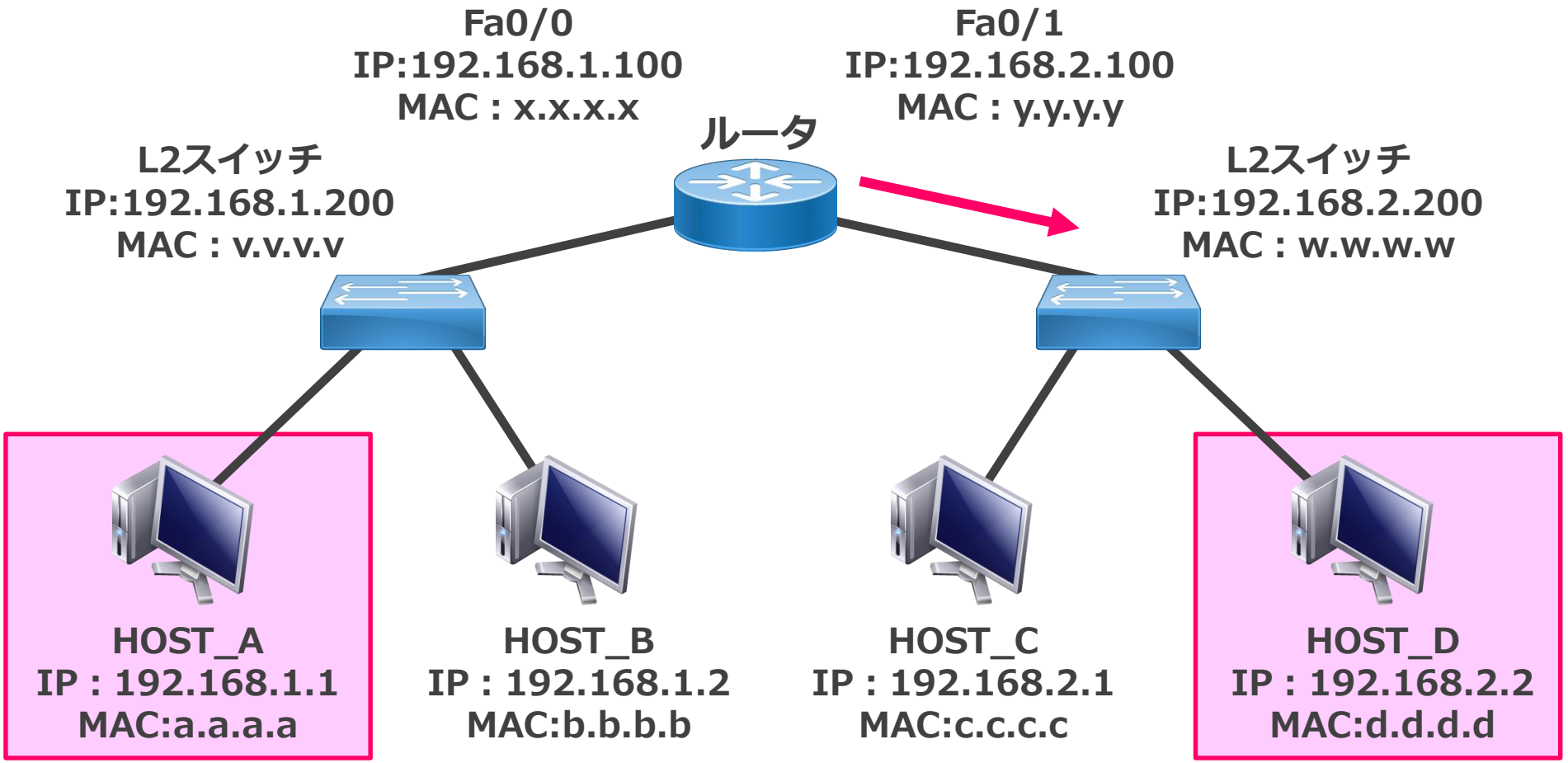
各NW機器でMACアドレス学習後、HOST_AからHOST_Bへの通信時HOST_Aから送出時の送信元IPアドレス・MACアドレスと宛先IPアドレス・MACアドレスは？



各NW機器でMACアドレス学習後、HOST_AからHOST_Dへの通信時ルータFa0/0で受ける際の送信元IPアドレス・MACアドレスと宛先IPアドレス・MACアドレスは?



各NW機器でMACアドレス学習後、HOST_AからHOST_Dへの通信時ルータFa0/1で送る際の送信元IPアドレス・MACアドレスと宛先IPアドレス・MACアドレスは?



TCPの特徴について正しいものはどれか？
（2つ選択）

●選択肢

a：IPの下位層にあたるプロトコルである
b：信頼性のある通信を確立できる
c：コネクションレス型のプロトコルである
d：データが届いたかどうかを常に確認する
e：UDPより高速に通信できる
f ：セッションを確立せず、一方向にデータを送信する

http、DNSに使用するポート番号はどれか?（それぞれ選択）

●選択肢

a：23
b：110
c：25
d：80
e：443
f ：53