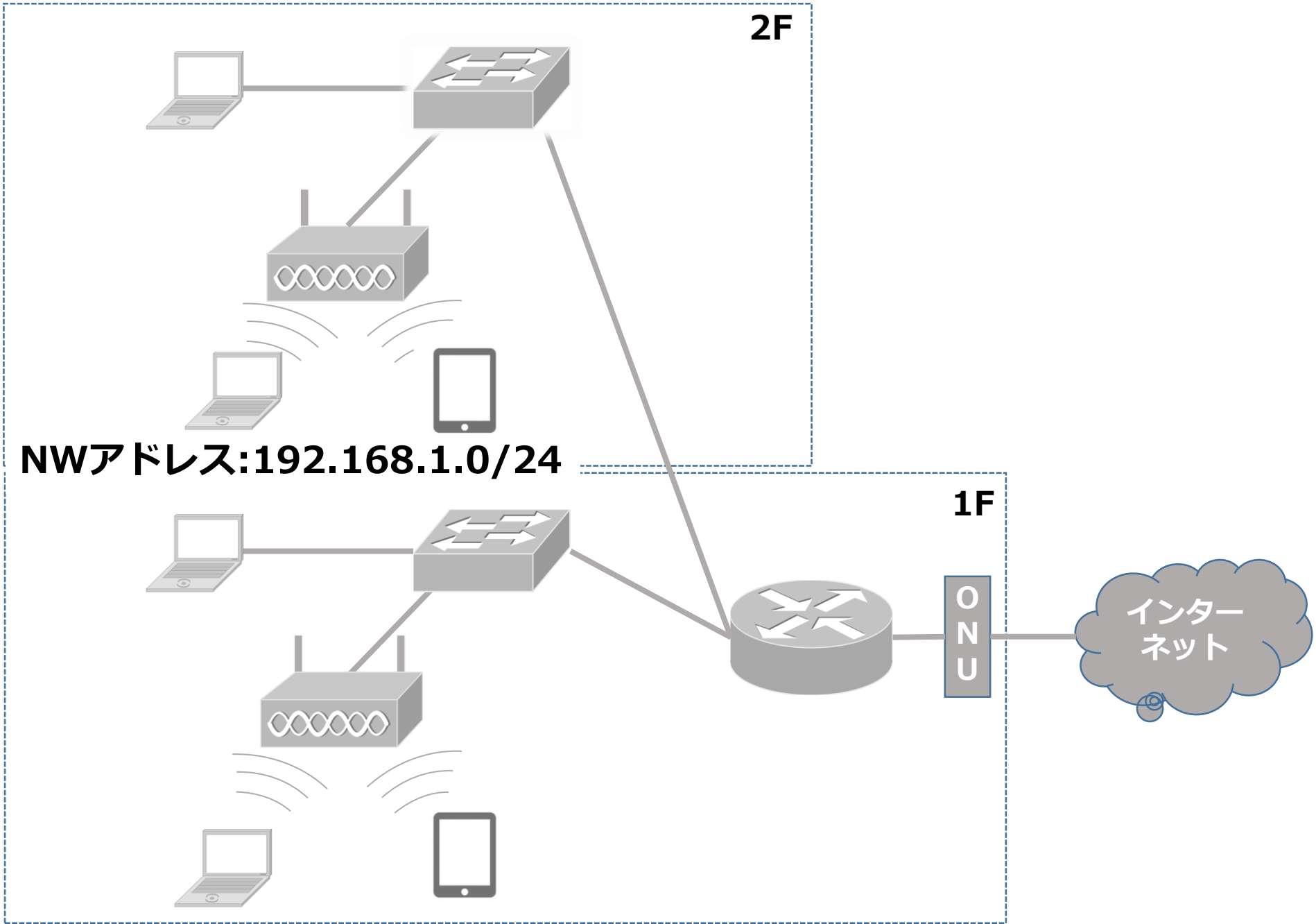
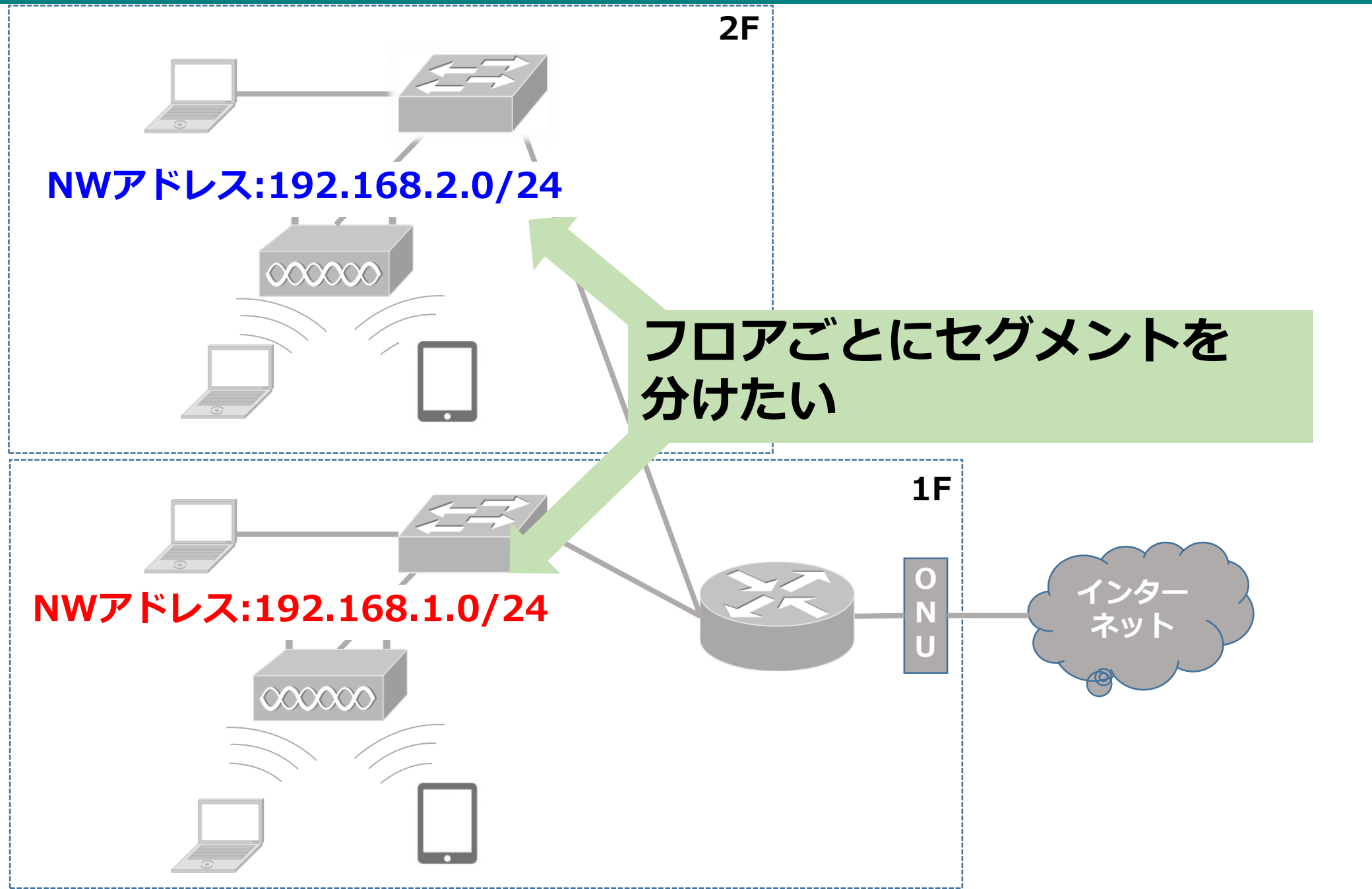
5章
セグメント分割

Vlan

分割前

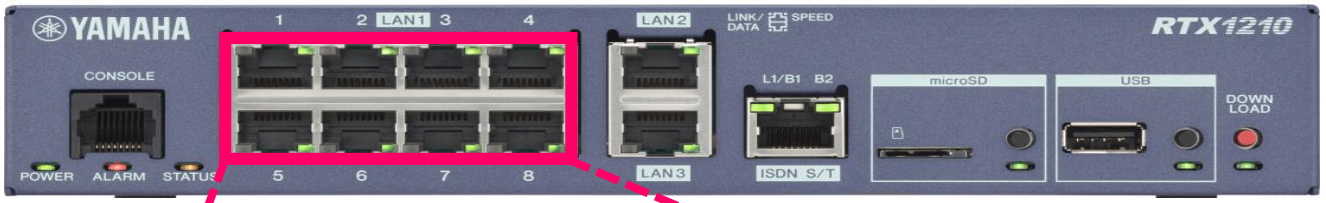


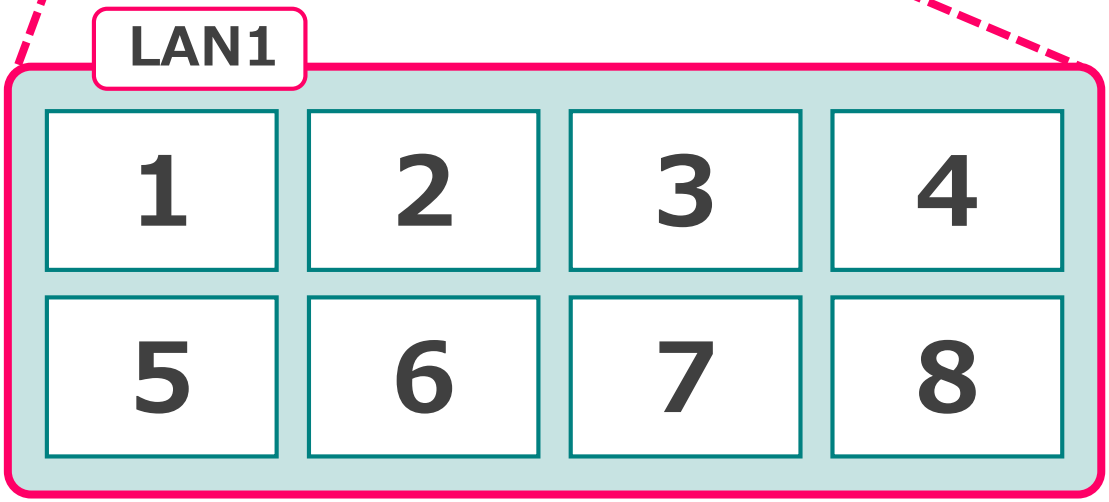
分割後


2F
NWアドレス:192.168.2.0/24
フロアごとにセグメントを
分けたい
1F
NWアドレス:192.168.1.0/24
ONU
インター
ネット

●セグメント分割（Vlan）

LAN1の全てのポートが同一セグメント

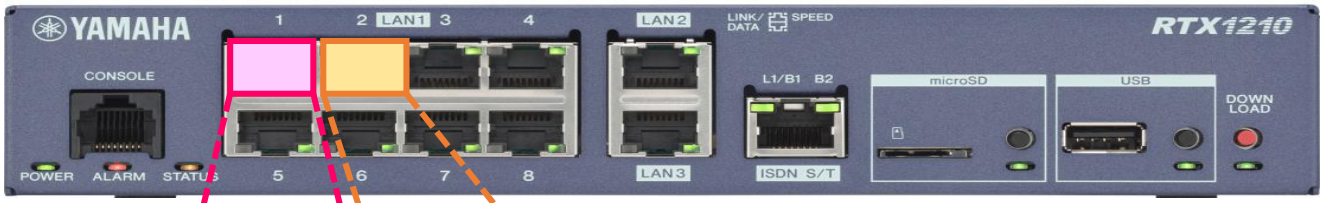


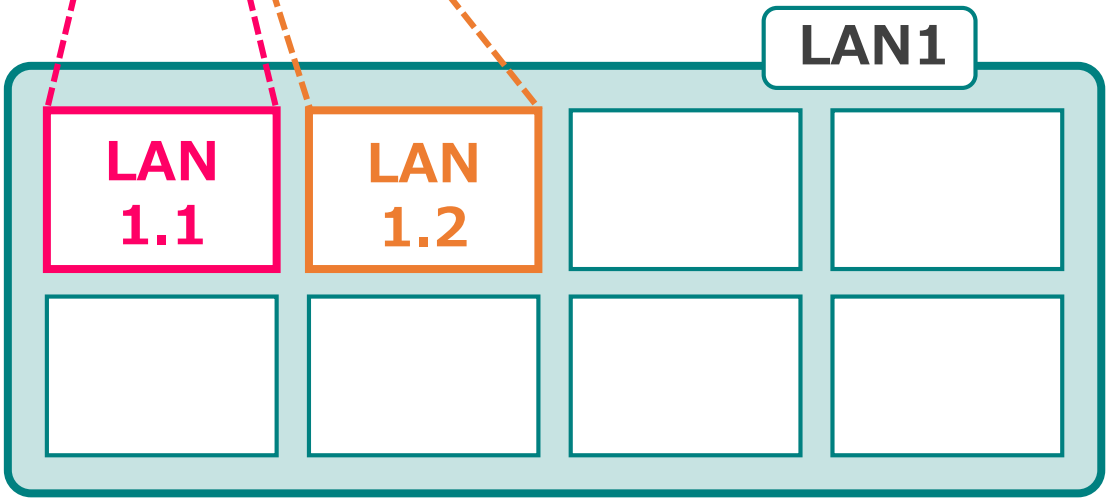


IPアドレス:192.168.1.254/24

●セグメント分割（Vlan）

ポート毎にVlanを設定しセグメントを分ける



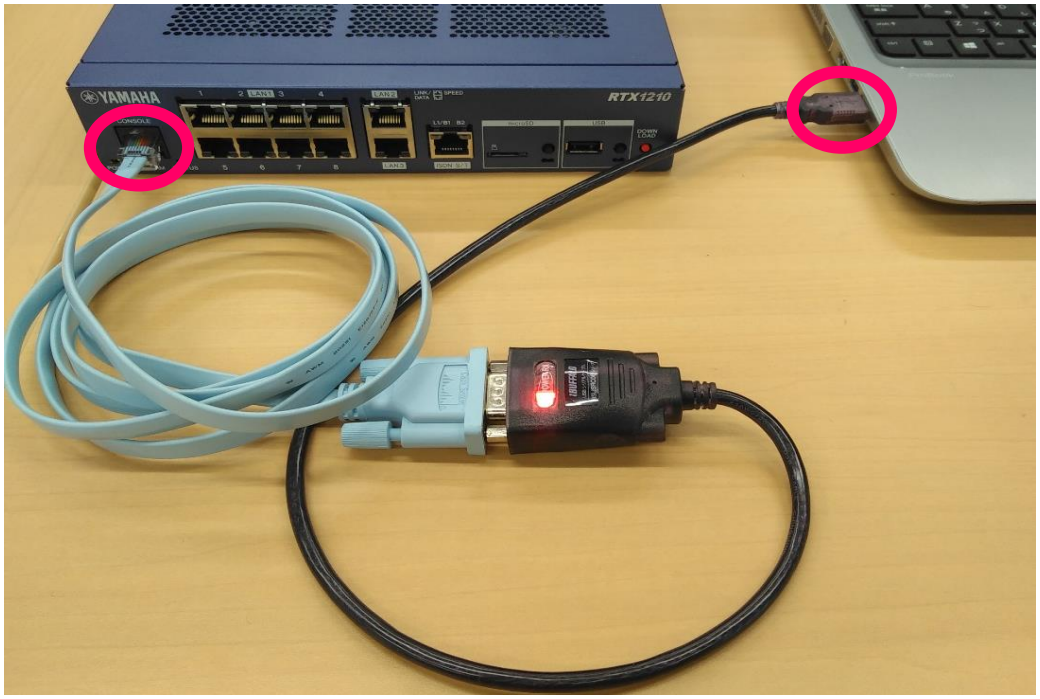


Vlan1 : 192.168.1.254/24

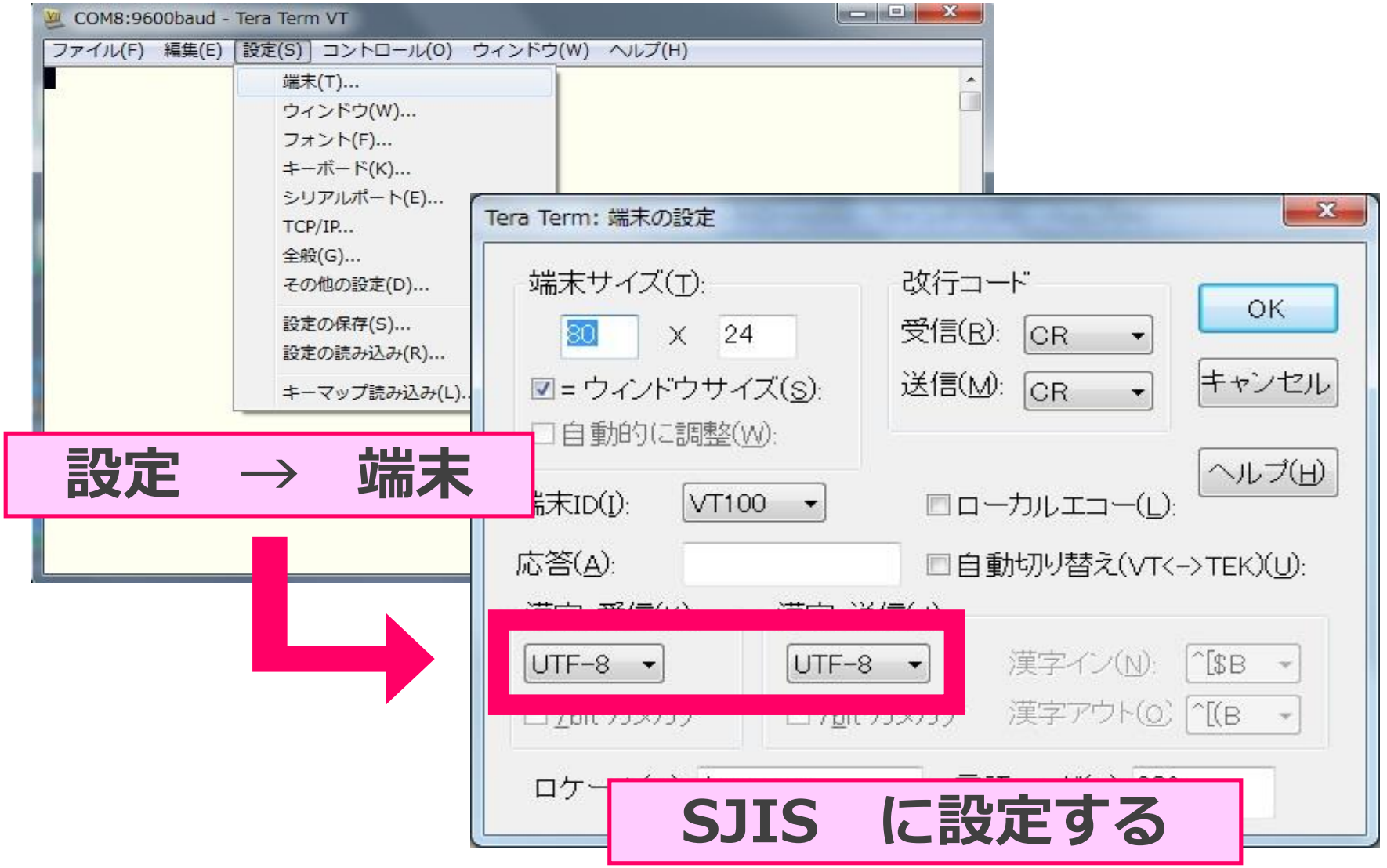
Vlan2 : 192.168.2.254/24

YAMAHA機器のCLI設定

CLI操作をおこなう場合は、Consoleケーブル(水色)をYAMAHA側に接続し、シリアル変換ケーブルはPCのUSBポートに接続します。



●ターミナルソフトの設定



●基本操作

■ログイン
Password: と表示されるので、Enterを押す。(デフォルトパスなし)。
プロンプトが「>」に変化します。

「administrator」と入力すると再度パスワードを聞かれますので、
Enterを押す。プロンプトが「#」に変化します。

■ログアウト
quit (exit)　コマンドを使用します

■保存
 # save　コマンドを使用します。

■工場出荷
 # cold start コマンドを使用します。
※コマンド入力後、自動的に再起動し工場出荷時の状態になります。

●showコマンド(show config)

```
# RTX1210 Rev.14.01.16 (Tue Nov 22 19:03:24 2016)
# MAC Address : ac:44:f2:3a:de:2f, ac:44:f2:3a:de:30, ac:44:f2:3a:de:31
# Memory 256Mbytes, 3LAN, 1BRI
# main:  RTX1210 ver=00 serial=S4H109178 MAC-Address=ac:44:f2:3a:de:2f
    MAC-Address=ac:44:f2:3a:de:30 MAC-Address=ac:44:f2:3a:de:31
# Reporting Date: Apr 9 18:08:44 2018
ip route default gateway pp 1 ] デフォルトルート
ip lan1 address 192.168.1.254/24 ] LAN1のIPアドレス
switch control use lan1 on
switch control use lan2 on
```

●showコマンド(show config)

```
pp select 1
description pp WAKWAK
pp keepalive interval 30 retry-interval=30 count=12
pp always-on on
pppoe use lan2
pppoe auto disconnect off
pp auth accept pap chap
pp auth myname ydm4w3e8e@st@wakwak.com e63e8euw6
ppp lcp mru on 1454
ppp ipcp ipaddress on
ppp ipcp msext on
ppp ccp type none
```

PPPoE設定

●showコマンド(show config)

```
ip pp secure filter in 200003 200020 200021 200022 200023 200024 200025
  200030 200032
 ip pp secure filter out 200013 200020 200021 200022 200023 200024 200025
 200026 200027 200099 dynamic 200080 200081 200082 200083 200084
 200085 200098 200099
 ip pp nat descriptor 1000
 pp enable 1
ip filter 200000 reject 10.0.0.0/8 * * * *
ip filter 200001 reject 172.16.0.0/12 * * * *
ip filter 200002 reject 192.168.0.0/16 * * * *
ip filter 200003 reject 192.168.1.0/24 * * * *
ip filter 200010 reject * 10.0.0.0/8 * * *
ip filter 200011 reject * 172.16.0.0/12 * * *
ip filter 200012 reject * 192.168.0.0/16 * * *
ip filter 200013 reject * 192.168.1.0/24 * * *
ip filter 200020 reject * * udp,tcp 135 *
ip filter 200021 reject * * udp,tcp * 135
```

フィルタ適用

NAT適用

IPフィルタ作成

●showコマンド(show config)

```
ip filter 200022 reject * * udp,tcp netbios_ns-netbios_ssn *
ip filter 200023 reject * * udp,tcp * netbios_ns-netbios_ssn
ip filter 200024 reject * * udp,tcp 445 *
ip filter 200025 reject * * udp,tcp * 445
ip filter 200026 restrict * * tcpfin * www,21,nntp
ip filter 200027 restrict * * tcprst * www,21,nntp
ip filter 200030 pass * 192.168.1.0/24 icmp * *
ip filter 200031 pass * 192.168.1.0/24 established * *
ip filter 200032 pass * 192.168.1.0/24 tcp * ident
ip filter 200033 pass * 192.168.1.0/24 tcp ftpdata *
ip filter 200034 pass * 192.168.1.0/24 tcp,udp * domain
ip filter 200035 pass * 192.168.1.0/24 udp domain *
ip filter 200036 pass * 192.168.1.0/24 udp * ntp
ip filter 200037 pass * 192.168.1.0/24 udp ntp *
ip filter 200099 pass * * * * *
```

IPフィルタ作成

●showコマンド(show config)

```
nat descriptor type 1000 masquerade
dhcp service server
dhcp server rfc2131 compliant except remain-silent
dhcp scope 1 192.168.1.1-192.168.1.20/24
dns host lan1
dns server 8.8.8.8
dns server select 500001 pp 1 any . restrict pp 1
dns private address spoof on
dashboard accumulate traffic on
```

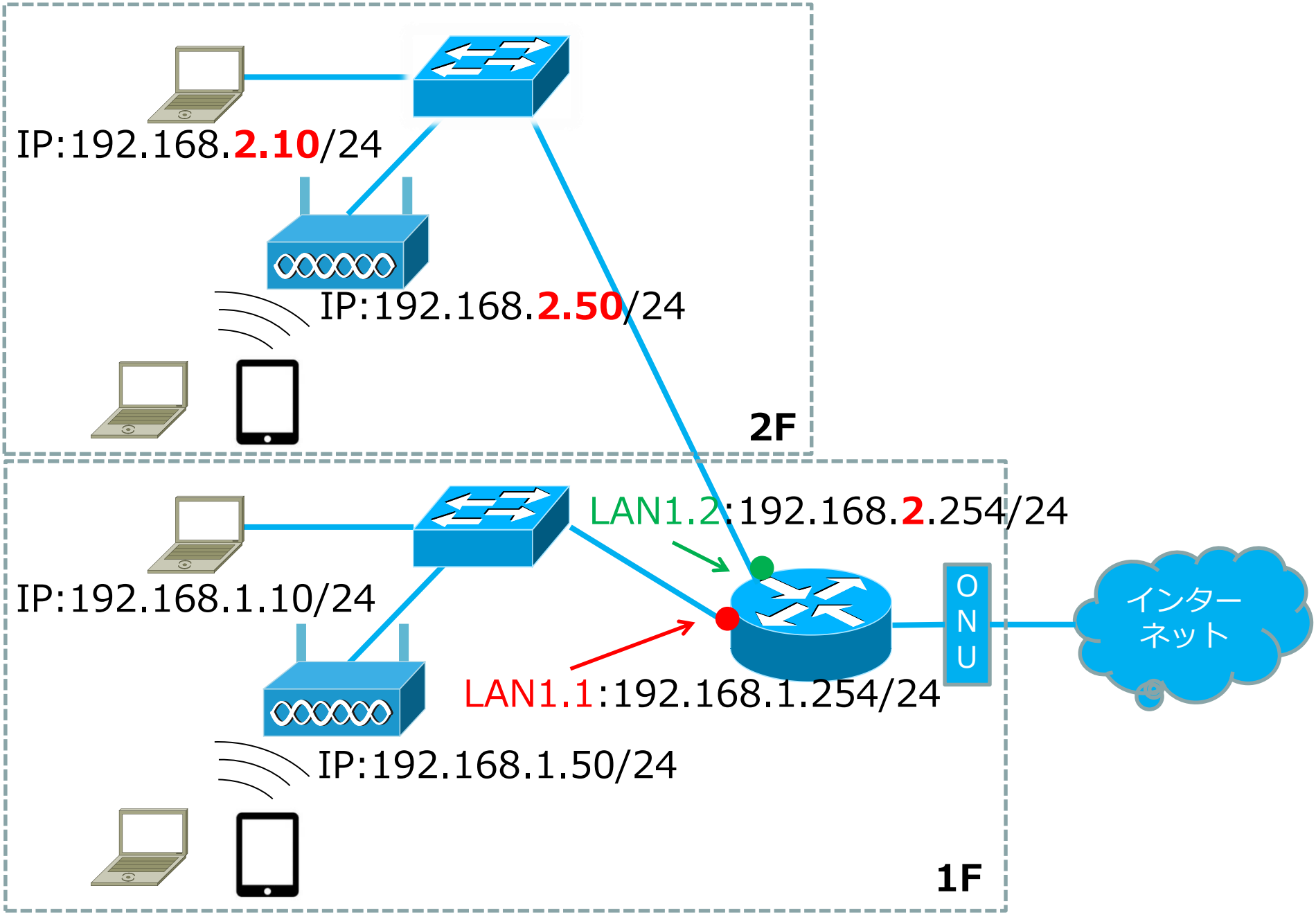
NAT作成（NAPT）

DHCP設定

DNS設定

演習①
LAN環境の構築（セグメント分割）

演習構成


IP:192.168.2.10/24
IP:192.168.2.50/24
2F
LAN1.2:192.168.2.254/24
IP:192.168.1.10/24
LAN1.1:192.168.1.254/24
ONU
インターネット
IP:192.168.1.50/24
1F

●演習内容

① ルータのLAN1ポートをポートごと（LAN1.1、LAN1.2）にセグメント分割し、IPアドレスを変更します。
② ルータのDHCP機能に2F向けの設定を追加します。
③ 2Fのアクセスポイント(AP)のIPアドレスを変更します
④ 2Fの有線PCのIPアドレスとデフォルトゲートウェイを変更します。
⑤ 2Fの無線PCとタブレットにて、DHCPによるIPアドレス再取得のため再起動します。
⑥ 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
⑦ 全てのPCとタブレットでインターネット通信ができることを確認します。

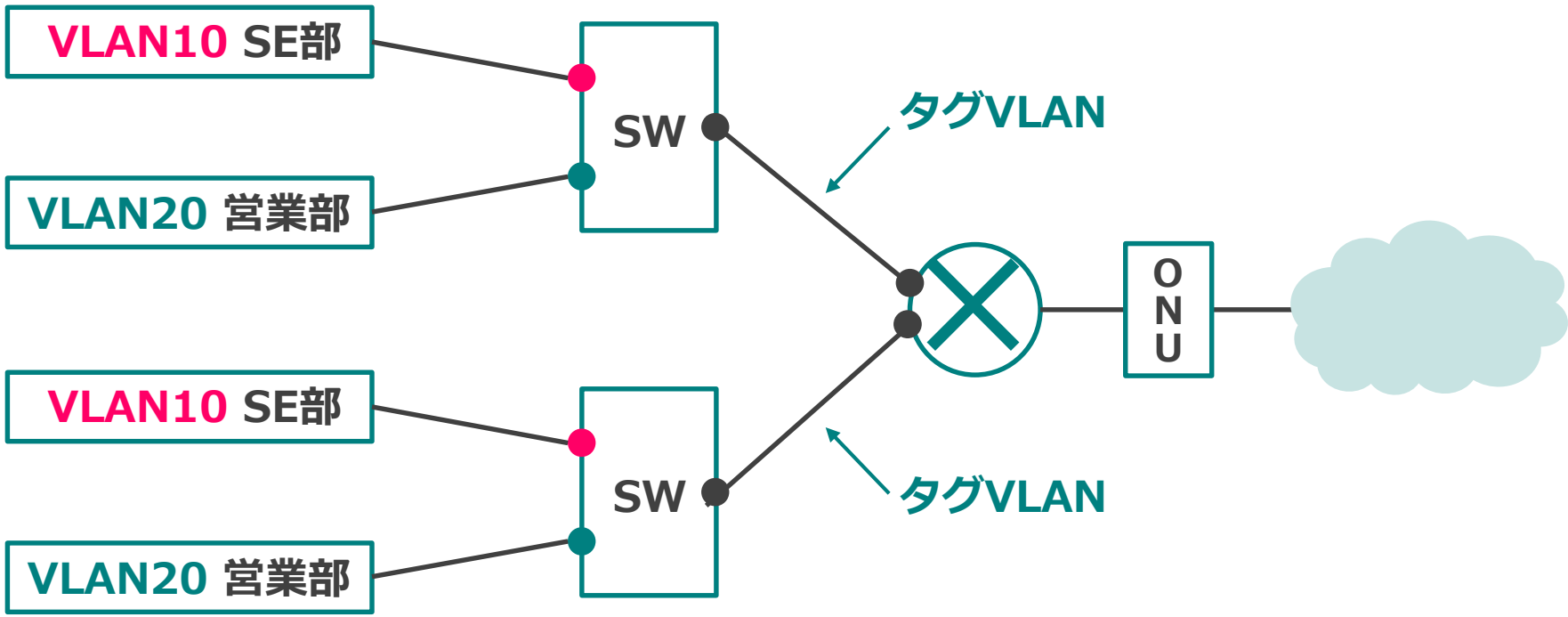
1.ルータの設定

①ルータに下記configをコマンドライン(CLI)にて設定します。

```
lan type lan1 port-based-option=divide-network
・LAN分割の機能を有効にする
ip vlan1 address 192.168.1.254/24
・vlan1にIPアドレスを設定する
ip vlan2 address 192.168.2.254/24
・vlan2にIPアドレスを設定する
vlan port mapping lan1.1 vlan1
・vlan1をlan1.1ポートにマッピングする
vlan port mapping lan1.2 vlan2
・vlan2をlan1.2ポートにマッピングする
dhcp scope 2 192.168.2.1-192.168.2.9/24
・DHCPの払い出しIPアドレス範囲を追加する
dns host vlan1 vlan2
・DNSサーバーへアクセスできるホストの設定をする
ip filter 200030 pass * 192.168.0.0/16 * *
・LANからのping通信を許可する
save
・設定の保存
```

よくあるLANの構成

●よくあるLANの構成（VLANとタグVLANの構成）



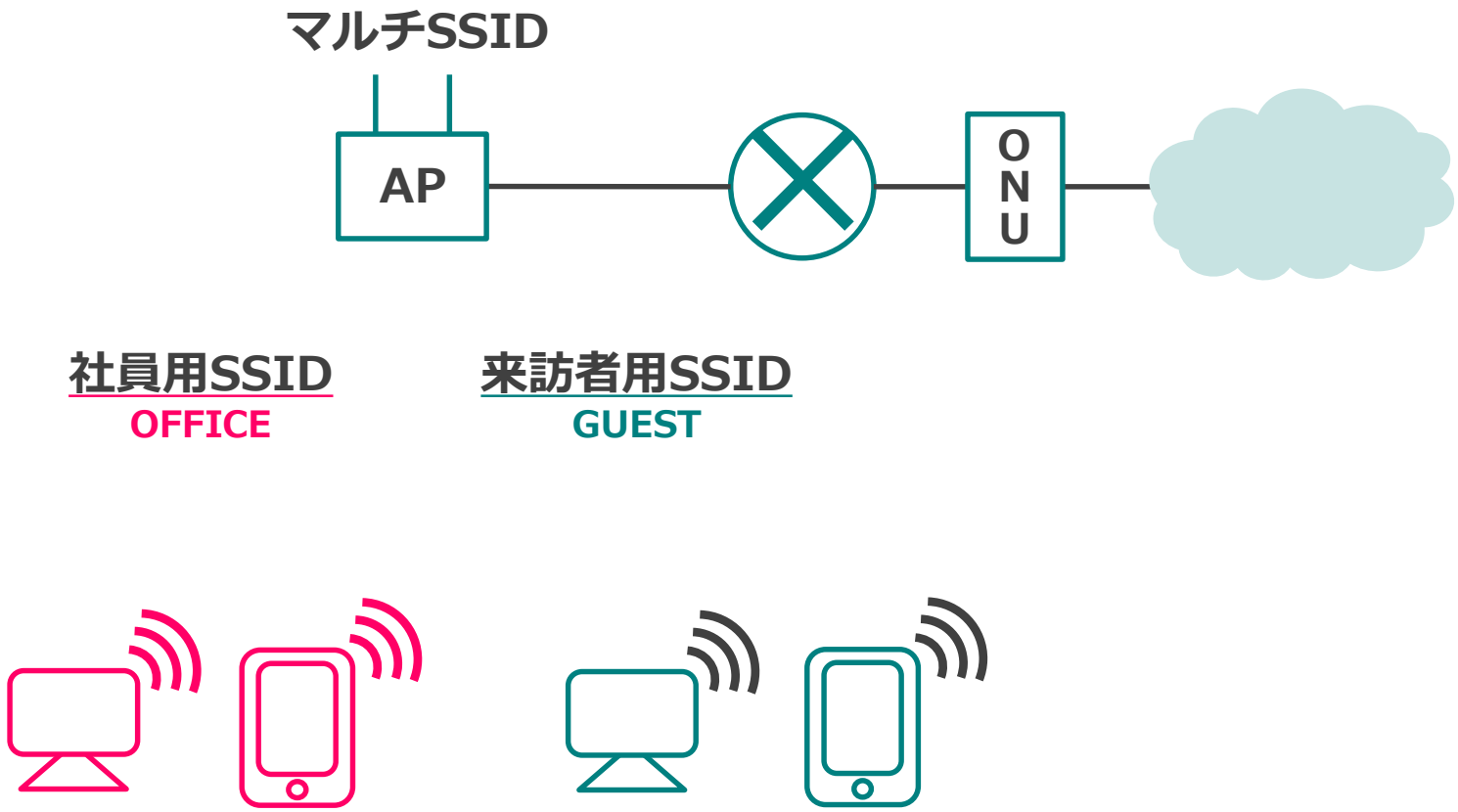
●よくあるLANの構成（VLANとタグVLANの構成）

【VLAN】
物理的に1つのスイッチを、あたかも複数のスイッチがあるかのように見せる技術です。

【タグVLAN】
スイッチ間をまたぐ複数のvlanを1本のケーブルで接続して通信を行うための機能です。

【タグvlanの動作】
スイッチはタグvlanポートを通過するフレームにvlan情報を付加して送信します
フレームを受信したスイッチは、vlanタグを調べて、どのvlanに流すべきフレームであるかを判断します。

●よくあるLANの構成　（複数のSSIDを展開する構成）



●よくあるLANの構成（複数のSSIDを展開する構成）

企業向けAPの特徴（廉価版との比較）

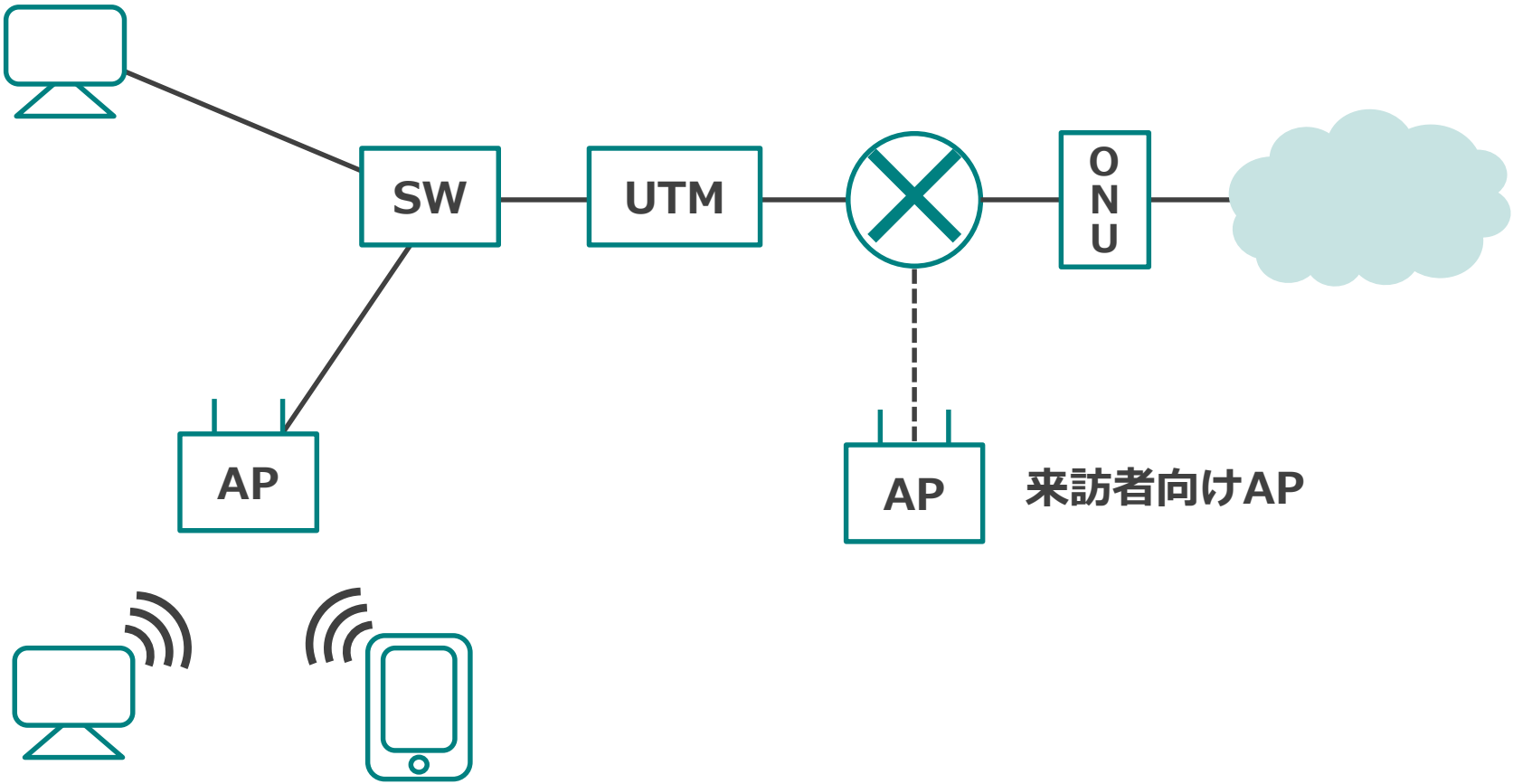
【マルチSSID機能】
1つのAPで複数のSSIDを設定できる機能です。

【同時接続台数】
沢山の無線端末を同時に接続できます。

【一括管理（ワイヤレスLANコントローラー導入）】
設定の一元管理や電波調整の自動化、管理負荷低減と安定稼働が実現できます。

【セキュリティ機能】
接続できるユーザを制限するためWPA2エンタープライズ認証が可能です。

●よくあるLANの構成（UTMを導入する構成）



●UTM (Unified Threat Management) を導入する構成

UTMとは、複数の異なるセキュリティ機能を一つに統合できる統合脅威管理をおこなう機器です。

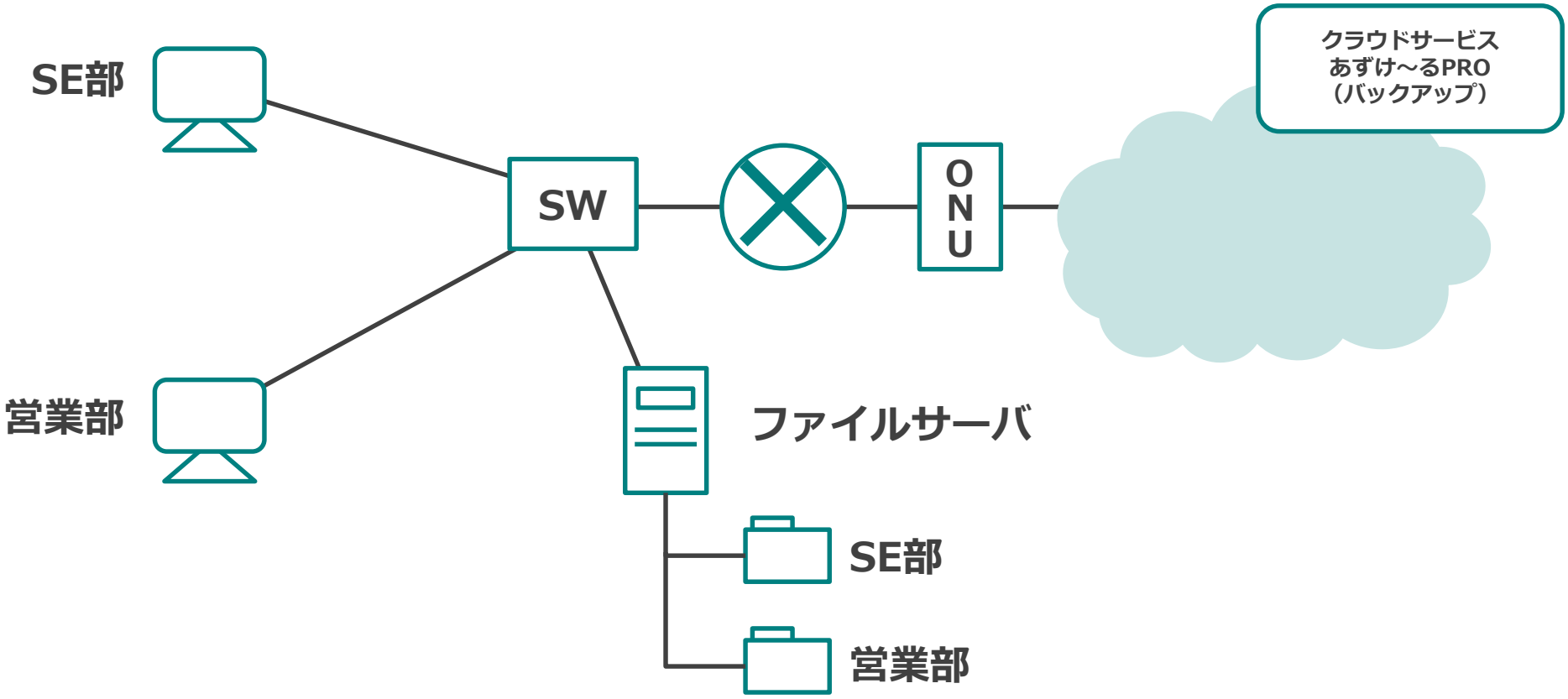
【アンチスパム】
無差別に送られてくるスパムメール（迷惑メール）から守るためのシステムのことです。

【アンチウイルス】
コンピュータウィルスからPCやサーバを守るためのシステムのことです。
例：トロイの木馬、キーロガー、スパイウェアなど

【IDS（Intrusion Detection System）】
ネットワークに対する不正侵入を検出し検知できるシステムです。

【IPS（Intrusion Detection System）】
ネットワークに対する不正侵入を検出し検出後に防御措置おこなうシステムです。

●よくあるLANの構成（ファイルサーバのある構成）



●よくあるLANの構成（ファイルサーバのある構成）

【ファイルサーバ】
ネットワーク上でOSのファイル共有機能を用いて、他のコンピュータから読み書き可能なストレージ(外部記憶装置)を提供するサーバです。

【クラウドサービス】
ネットワーク経由で、必要なサービスに応じて利用する形態を総称してクラウドサービスといいます。

【あずけ～るPRO】
クラウド上にデータを保管できるNTT東日本が提供するオンラインストレージサービスです。

6章
ルーティング基礎

●ルーティング方式

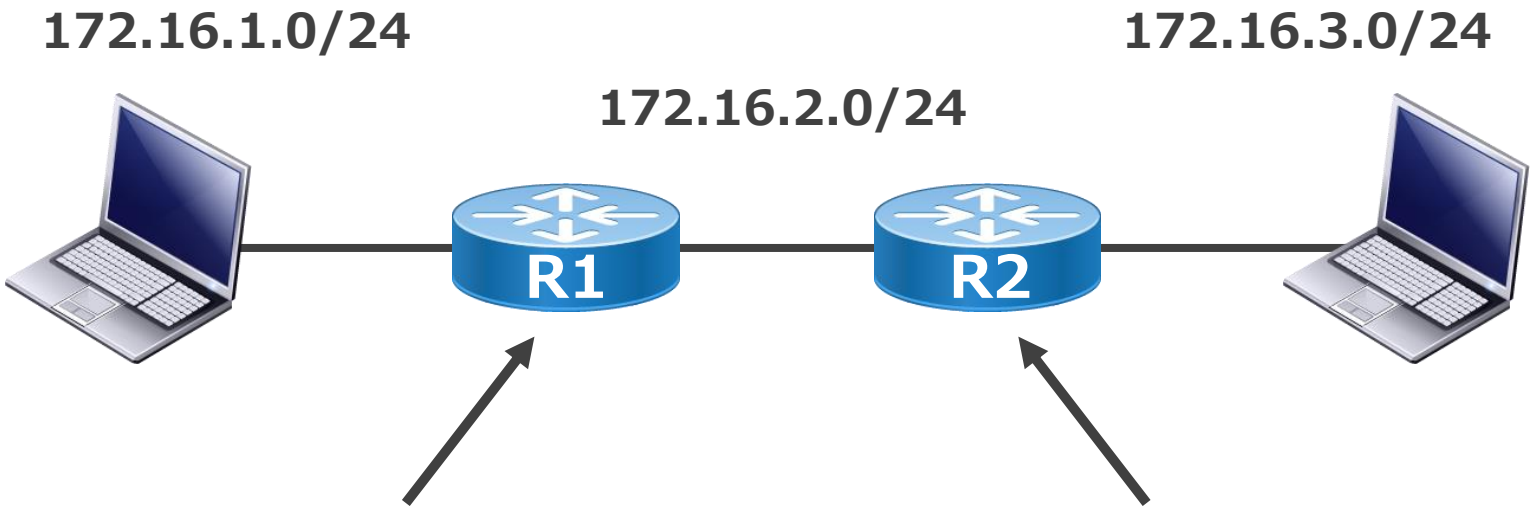
	スタティック ルーティング	ダイナミック ルーティング
ルータの処理	「小」	「大」 情報をやりとりし、計算するので ルータに負荷がかかる
管理者の作業量	「多」 手入力のため、初期設定や変更時 に作業量が多い	「少」 初期設定さえすれば、自動で設定 されるため作業量は少ない
ルーティング テーブルの維持	「手動」 NWに変更があるたびに、ルー ティング設定を手動で入力する必 要がある	「自動」 NWに変更があっても、自動的に 変更される
帯域の使用	「無」なし	「有」 ルータが情報をやりとりするため、 帯域を使用する

●ルーティング方式

IPネットワークにおいて経路情報を管理する方式として、「スタティック・ルーティング」と「ダイナミック・ルーティング」が存在します。

スタティック・ルーティングの長所は、管理される経路情報が基本的にルーティングテーブルより削除されることがないため、安定したネットワーク到達性の提供が可能なことです。また、経路情報を手動で設定するので情報交換のためのCPU処理やトラフィックも発生せず、ルータの処理が少なくて済みます。しかし、あて先ネットワークが実在しなくなった場合にもこの情報に基づくトラフィックの転送が行われてしまったり、経路情報の数に比例して、その管理に要する手間も膨大になるという短所があります。

●ルーティングテーブル



R1:ルーティングテーブル

宛先ネットワーク	ネクストホップ	ルーティング
172.16.1.0/24	—	直接接続
172.16.2.0/24	—	直接接続
172.16.3.0/24	R2	スタティック/ダイナミック

R2:ルーティングテーブル

宛先ネットワーク	ネクストホップ	ルーティング
172.16.1.0/24	R1	スタティック/ダイナミック
172.16.2.0/24	—	直接接続
172.16.3.0/24	—	直接接続

●ルーティングテーブル

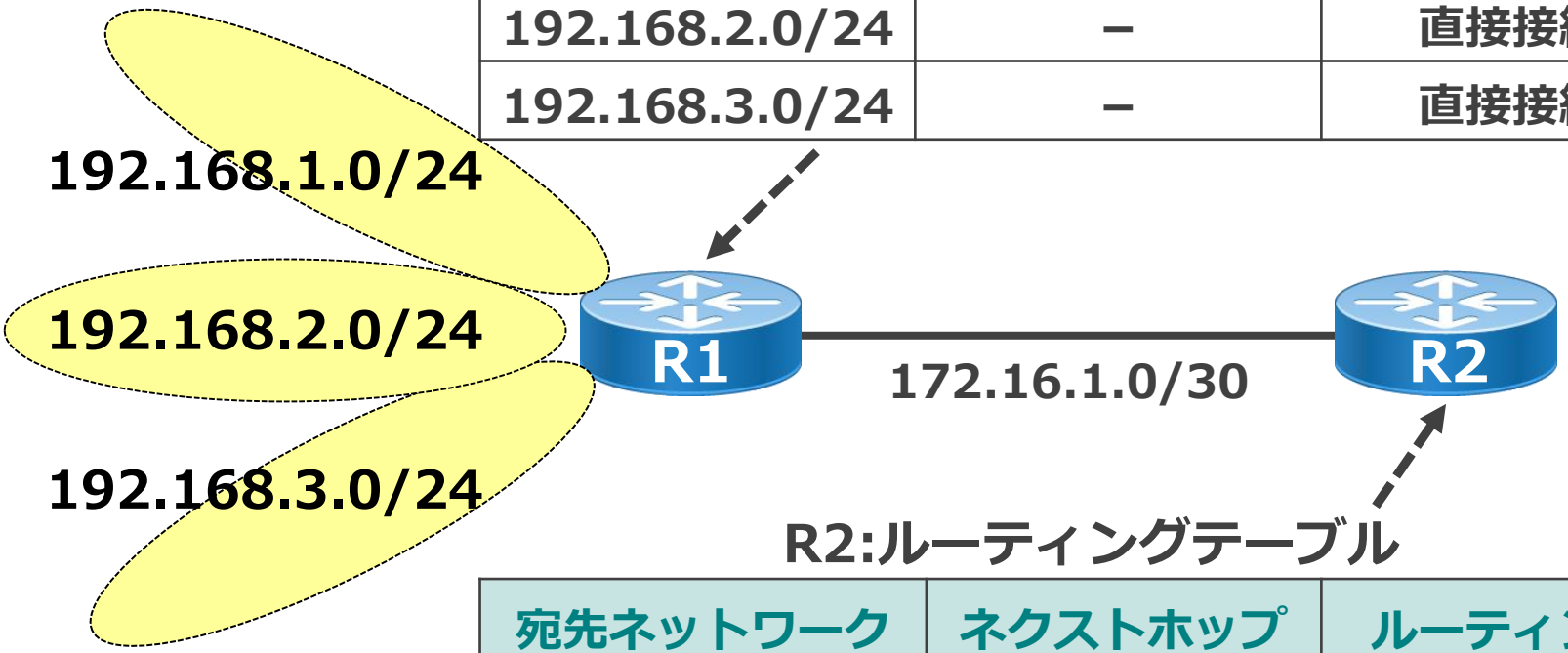
スタティックルーティングは、ネットワーク管理者が手動で各ルータのルーティングテーブルを作成し経路を決定させる方法です。
ダイナミックルーティングは、ルータが動的にルーティングテーブルを更新する方法です。

ネクストホップは、宛先ネットワークに到達するために、次にどの隣接ルータにIPパケットを転送すればよいのかについての情報です。

●経路集約

R1:ルーティングテーブル

宛先ネットワーク	ネクストホップ	ルーティング
172.16.1.0/30	–	直接接続
192.168.1.0/24	–	直接接続
192.168.2.0/24	–	直接接続
192.168.3.0/24	–	直接接続



R2:ルーティングテーブル

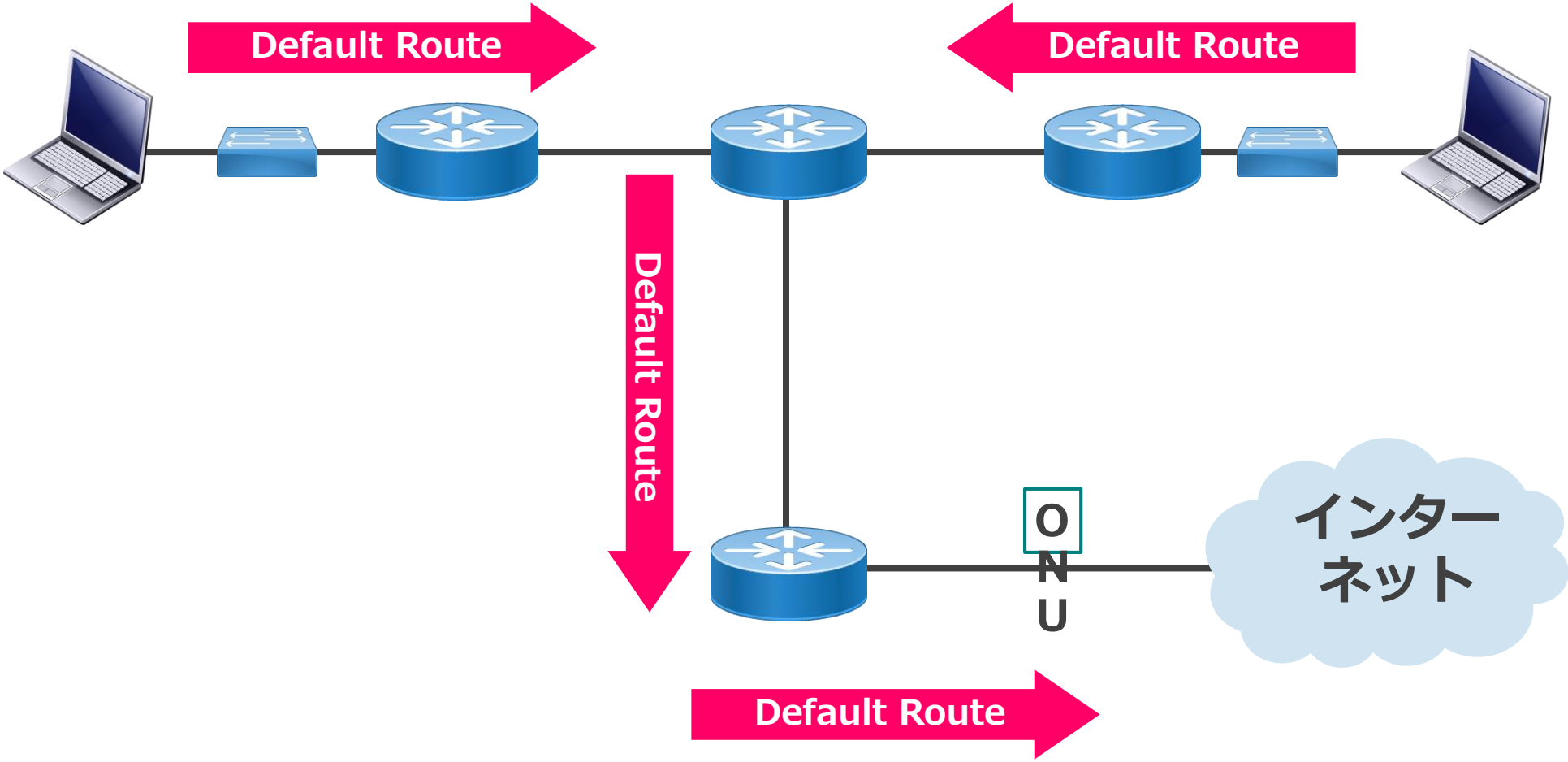
宛先ネットワーク	ネクストホップ	ルーティング
172.16.1.0/30	–	直接接続
192.168.0.0/16	R1	スタティック

３つのネットワークを
経路集約

●経路集約

ルーティングテーブルの複数の宛先ネットワークを、１つの宛先ネットワークにまとめることを経路集約と言います。

●デフォルトルート

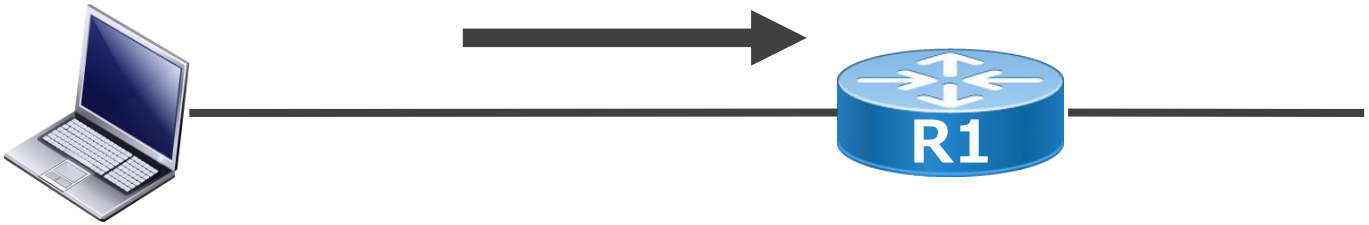

Default Route
Default Route
Default Route
Default Route
ONU
インター
ネット

●デフォルトルート

デフォルトルートとは、「**0.0.0.0/0**」で表し、全ての経路を指し示す特殊経路のことです。
主にインターネット宛の通信のルーティングとして使用されます。設定方法としては、主にスタティックルーティングで設定しますが、ダイナミックルーティングによる設定も可能です。
ルータはパケットのIPアドレスとルーティングテーブルを照合して、一致するエントリがないとパケットを転送することができずにパケットを破棄します。しかし、デフォルトルートの設定がされていると、ルーティングテーブル上に一致するエントリがない場合は、デフォルトルートの転送先(ネクストホップ)にパケットをルーティングします。

●ロンゲストマッチ

宛先：192.168.2.1



R1:ルーティングテーブル

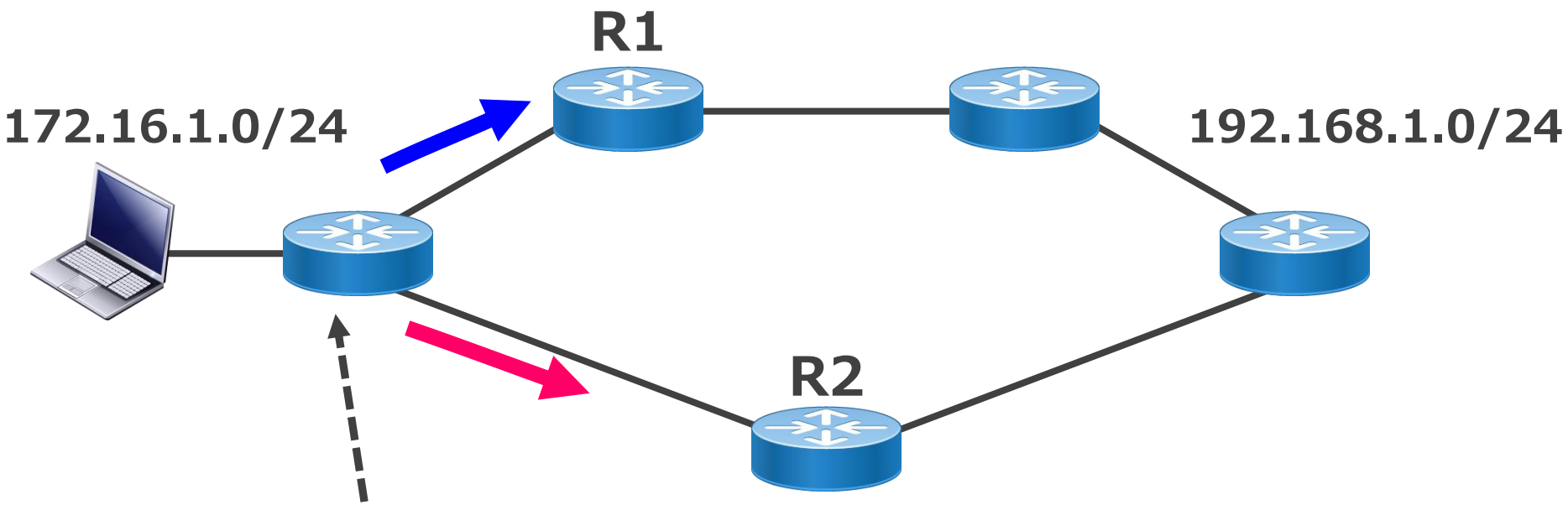
宛先ネットワーク	ネクストホップ	
192.168.0.0/16	R2	一致：16ビット
192.168.1.0/24	R3	一致しない
192.168.2.0/24	R4	一致：24ビット
0.0.0.0/0	R5	一致：0ビット

宛先IPアドレスに対して最も一致する
ビット数が長いルート情報を採用

●ロンゲストマッチ

ルーティングテーブルから宛先を選択する際、条件に合う宛先が複数ある場合にプレフィックス長が長い方のネットワークアドレスを選択する規則のことを指します。
別名で最長一致とも呼ばれます。

●AD値(アドミニストレーティブディスタンス)



ルーティングテーブル

宛先ネットワーク	ネクストホップ	ルーティング	AD値※
192.168.1.0/24	R2	OSPF	110
192.168.1.0/24	R1	スタティック	1

●AD値(アドミニストレーティブディスタンス)

ルーティングテーブルに複数の経路が存在する場合、経路選択の判断基準となる値のことです。

※ルーティングプロトコルのAD値（Cisco）

経路の学習方法	AD値（低い値が優先）
直接接続	0
スタティック	1
EIGRP	90
OSPF	110
RIP	120

7章
Cisco機器の基本操作

●ルータ（Cisco891F）

①ルーテッドポート
　インターネット接続、VPN接続など

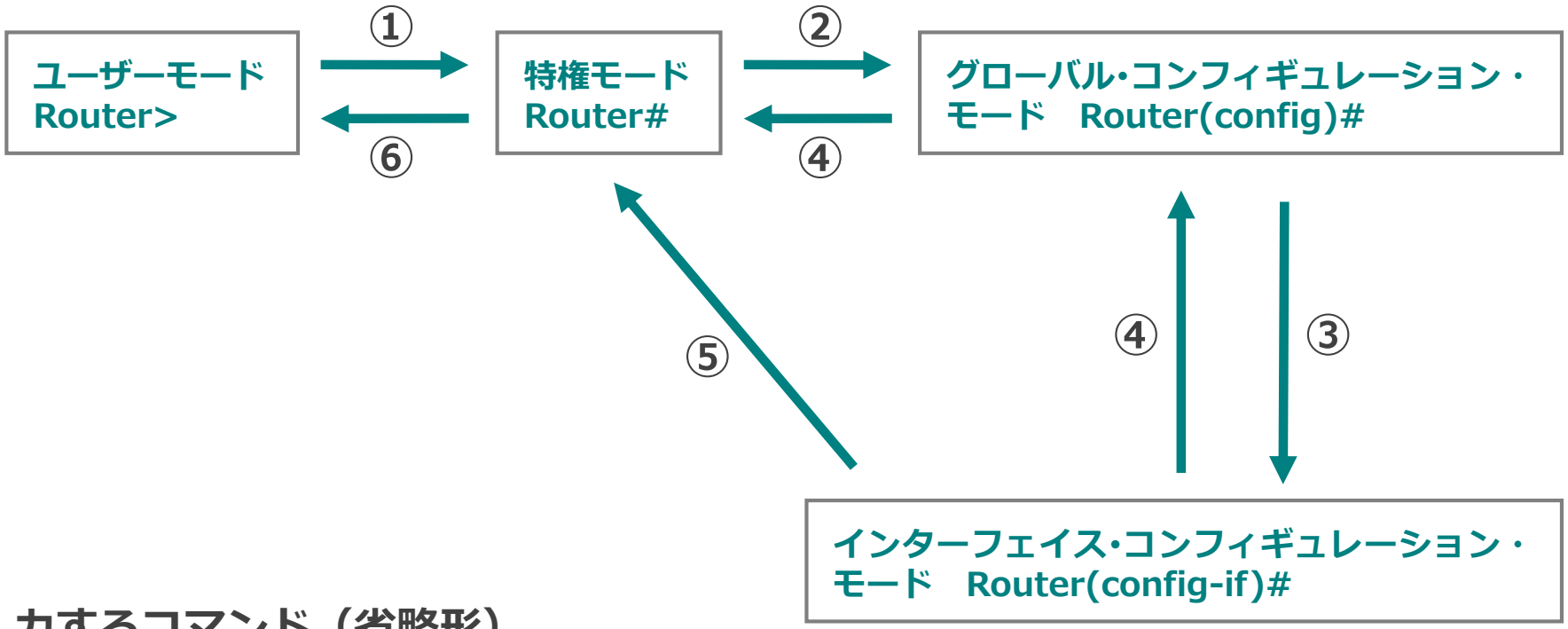
②コンソールポート
　Config設定のためにConsoleケーブルでPCと接続するポート

③スイッチングハブポート
　クライアントPCの接続など

● ルータ（Cisco891F）

ルータは、異なるネットワーク間のパケットを転送できるルーティング機能を持ち、
様々なプロトコルに対応しています。
※Config設定にはPCにターミナルソフト（TeraTerm）が必要になります。

●主な設定モード



入力するコマンド（省略形）

① enable　（en）
② configure terminal（conf t）
③ interface xx　(int fa 0)　　xxはfastethernet 0など
④ exit （exi）
⑤ end
⑥ disable（disa）

● **主な設定モード**

・ユーザモード
「参照のみ」のモードで、ルータのステータスを調べることは出来ますが、設定の変更は出来ません。

・特権モード
ユーザモード（非特権モード）よりも多くのコマンドを利用する事ができ、運用レベルの設定を行うことが出来ます。

・グローバル･コンフィギュレーション･モード
ルータのシステム全体に関わる設定を行う時に使用するモードです。

・インターフェース・コンフィギュレーション・モード
個々の機能を設定する際に使用するモードです。インターフェースなどの設定をする場合に使用します。

※コマンド補完機能
長いコマンドを入力する場合にすべてのコマンド打つのは大変です。コマンドを途中まで打った後、その語句に続く文字列候補が無い場合は「Tabキー」を押す事でコマンドが綺麗に入力されます。例えば、”conf”と入力してTabキーを入力すると自動的に”configure”と表示されます。

●確認コマンド(show running-config)

```
Router#sh run
Building configuration...

Current configuration : 1556 bytes
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model

!
 --More--
```

● 確認コマンド(show running-config)

・show running-config（sh run）
現在設定内容を表示します。

・More表示
“--More--”と表示される場合は、一定以上の長さの内容があるためです。EnterやSpaceで次の行（ページ）を表示できます。

●確認コマンド(show ip interface brief)

```
Router#sh ip int brie
Interface    IP-Address    OK? Method  Status                Protocol
Async3                     unassigned  YES unset   down                  down
BRI0                       unassigned  YES unset   administratively down down
BRI0:1                     unassigned  YES unset   administratively down down
BRI0:2                     unassigned  YES unset   administratively down down
FastEthernet0              unassigned  YES unset   administratively down down
GigabitEthernet0   unassigned  YES unset   down                  down
GigabitEthernet1   unassigned  YES unset   down                  down
GigabitEthernet2   unassigned  YES unset   down                  down
GigabitEthernet3   unassigned  YES unset   down                  down
GigabitEthernet4   unassigned  YES unset   down                  down
GigabitEthernet5   unassigned  YES unset   down                  down
GigabitEthernet6   unassigned  YES unset   down                  down
GigabitEthernet7   unassigned  YES unset   down                  down
GigabitEthernet8   unassigned  YES unset   administratively down down
Vlan1              unassigned  YES unset   down                  down
```

● 確認コマンド(show ip interface brief)

・show ip interface brief（sh ip int brie）
ルータの全てのインターフェースのステータスを簡易表示するコマンドです。

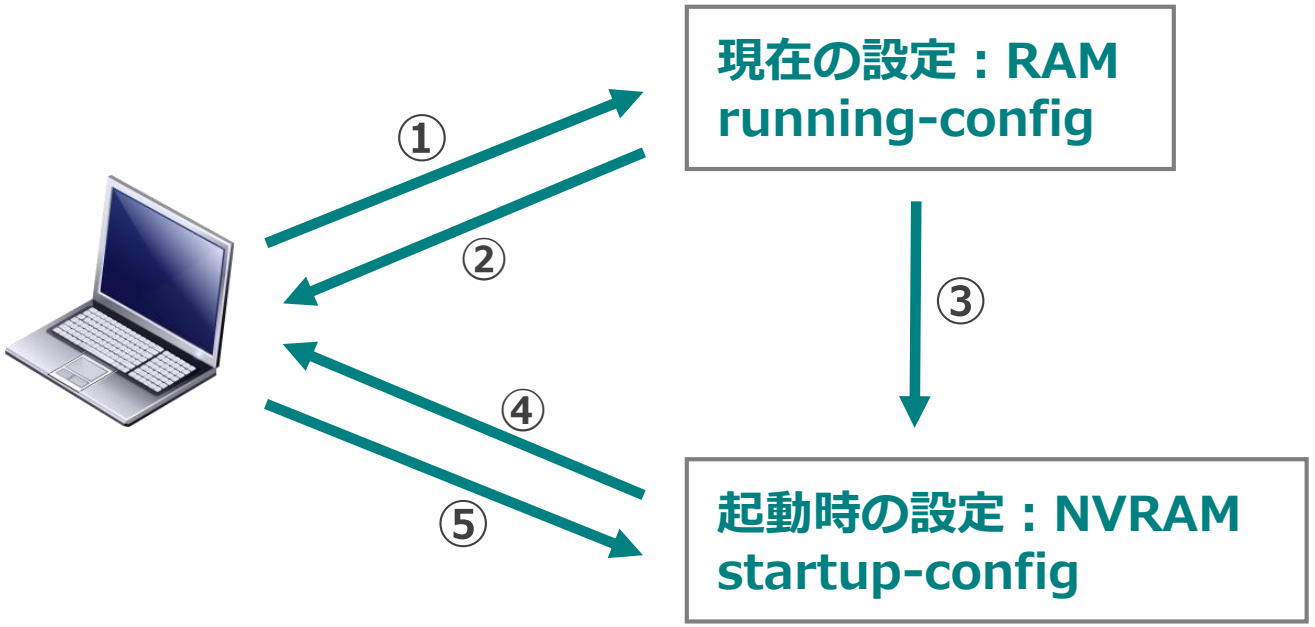
●確認コマンド(show ip route)

```
Router#sh ip ro
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.10.100.0/24 is directly connected, GigabitEthernet8
L        10.10.100.1/32 is directly connected, GigabitEthernet8
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.0.0/16 is directly connected, Vlan1
L        172.16.100.1/32 is directly connected, Vlan1
      192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.100.0/24 is directly connected, FastEthernet0
L        192.168.100.1/32 is directly connected, FastEthernet0
S     192.168.200.0/24 [1/0] via 192.168.100.254
```

● 確認コマンド(show ip route)

・show ip route（sh ip ro）
ルーティングテーブルを確認するためのコマンドです。

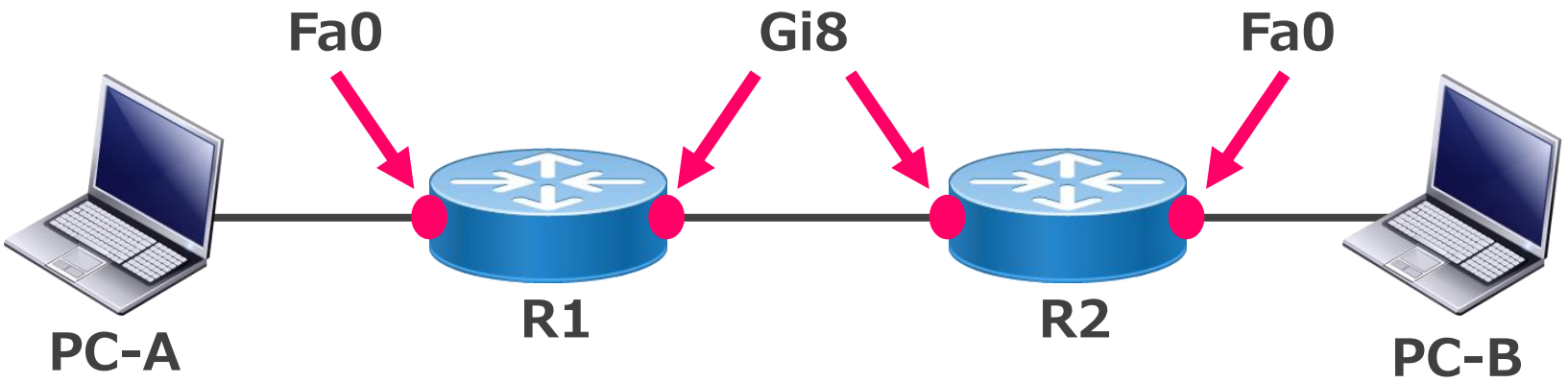
●保存と初期化



入力するコマンド（省略形）

① configure terminal　（conf t）
② show running-config（sh run）
③ copy running-config startup-config（copy run star）
④ show startup-config（sh star）
⑤ erase startup-config（era star）

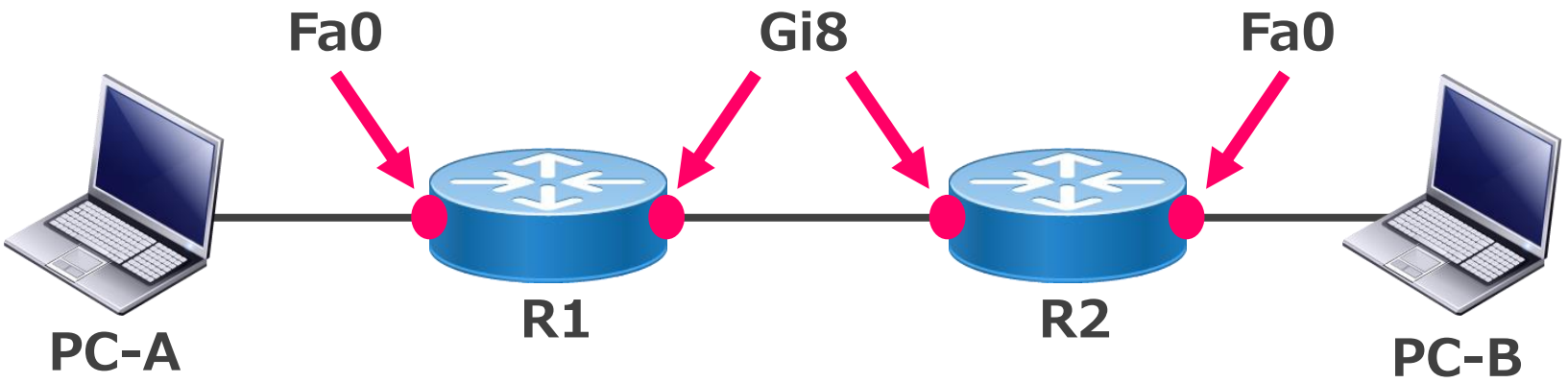
●スタティックルーティング演習



R1
Gi8:172.16.1.1/30
Fa0:192.168.1.62/27

R2
Gi8:172.16.1.2/30
Fa0:192.168.1.94/27

●スタティックルーティング演習



R1
Gi8:172.16.1.1/30
Fa0:192.168.1.62/27

R2
Gi8:172.16.1.2/30
Fa0:192.168.1.94/27

● スタティックルーティング演習

実施項目
・各ルータのインターフェースにIPアドレスを設定して下さい。
・各ルータにスタティックルーティングを設定して下さい。
・PCのIPアドレスは、PCが属するネットワーク範囲で使用できるホストアドレスの最小値を設定して下さい。

確認項目
・各PCからコマンドプロンプトを使用し、ping通信が可能なことを確認して下さい。
・showコマンドを使用し、ルータのルーティングテーブル情報を確認して下さい。

●演習のルータ設定

```
Router>en
Router#conf t
Router(config)# int fa 0
Router(config-if)# ip address IPアドレス  サブネットマスク
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# int gi 8
Router(config-if)# ip address IPアドレス サブネットマスク
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# ip route ネットワークアドレス サブネットマスク ネクストホップアドレス
Router(config)# end
Router# copy run start
```

● 演習のルータ設定

IPアドレス設定
(config-if)# ip address　IPアドレス　サブネットマスク
例：ip address 192.168.1.1 255.255.255.0

スタティックルーティングの設定
(config)# ip route ネットワークアドレス　サブネットマスク　ネクストホップアドレス
例：ip route 10.10.10.0 255.255.255.0 192.168.100.254

インタフェースの有効化
(config-if)# no　shutdown
※ルータのインターフェースは初期状態で管理的に無効になっているため、有効化が必要です。

間違った設定の一部削除
設定した内容を取り消して無効にするには、設定コマンドの先頭に【no】を付けて削除します。
例：no ip address 192.168.1.1 255.255.255.0

8章
WANの構成

WANサービス

●WANサービスの大別

1.広域イーサネット

2.IP-VPN

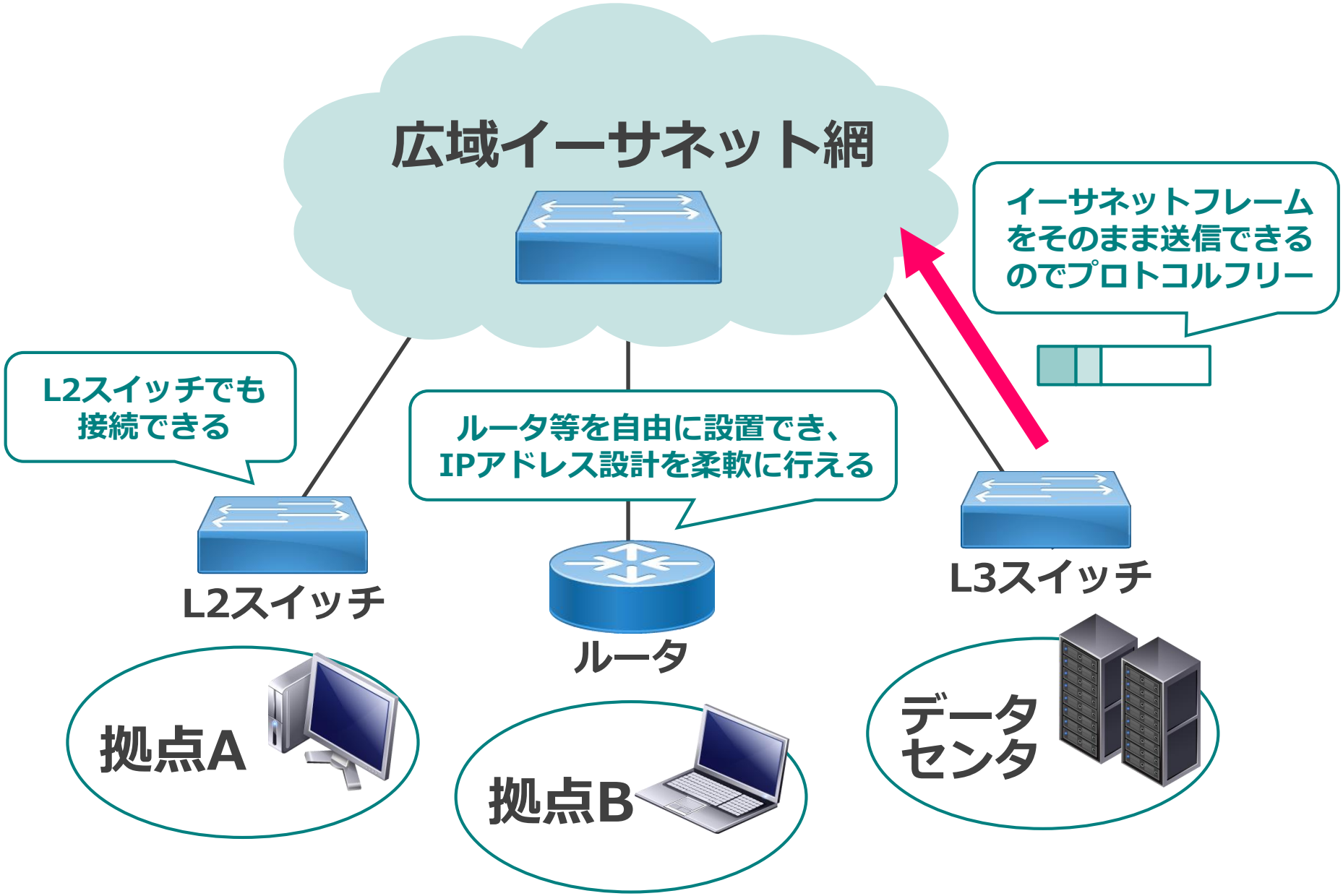
3.エントリー型IP-VPN

4.インターネットVPN

●WANサービスの大別

一般的には1～3は通信事業者が提供、管理する閉域網を使用した拠点間接続サービスになります。４のインターネットVPNは、通信網にインターネットを使用し、ユーザが独自で構築できる拠点間接続の方法ですが、通信事業者がサービスとして提供しているものもあります。

●広域イーサネット


広域イーサネット網
イーサネットフレーム
をそのまま送信できる
のでプロトコルフリー
L2スイッチでも
接続できる
ルータ等を自由に設置でき、
IPアドレス設計を柔軟に行える
L2スイッチ
ルータ
L3スイッチ
拠点A
拠点B
データ
センタ

●広域イーサネット

広域イーサネットサービスを利用して離れた複数の拠点を、まるで1つのネットワーク（セグメント）であるかのように構築する事が出来ます。

広域イーサネットサービスのメリット
・フルメッシュで接続出来る
・IPに依存しない
・ルーティングプロトコルに制限がない
・SLAや監視サービス等が充実している

広域イーサネットサービスのデメリット
・アクセス回線の費用が比較的高価
・サービス提供地域が限定される事がある

●主な広域イーサネットサービス

1.ビジネスイーサワイド

2.ビジネスイーサプレミア

3.Arcstar Universal One VPNサービス　（ギャランティorプレミアムプランのL2接続）

4.XePhion広域イーサネットサービス

5.KDDI Powered Ethernet

6.ULTINA Wide Ethernet

●主な広域イーサネットサービス

広域イーサネットサービスを利用して離れた複数の拠点を、まるで1つのネットワーク（セグメント）であるかのように構築する事が出来ます。

1.ビジネスイーサワイド(NTT東日本)
既存のビジネスイーサにはない新機能を実装するとともに、更なる信頼性と利便性の向上を実現し、県間･東西間・ゾーン間の接続も可能な広域イーサネットサービス。

2.ビジネスイーサプレミア(NTT東日本)
中継区間の無瞬断切り替えによる回線借用の回避でお客様システム影響の軽減。低遅延によるスループットの向上の実現。シンプルな料金体系（距離によらず県内・県間それぞれ一律）

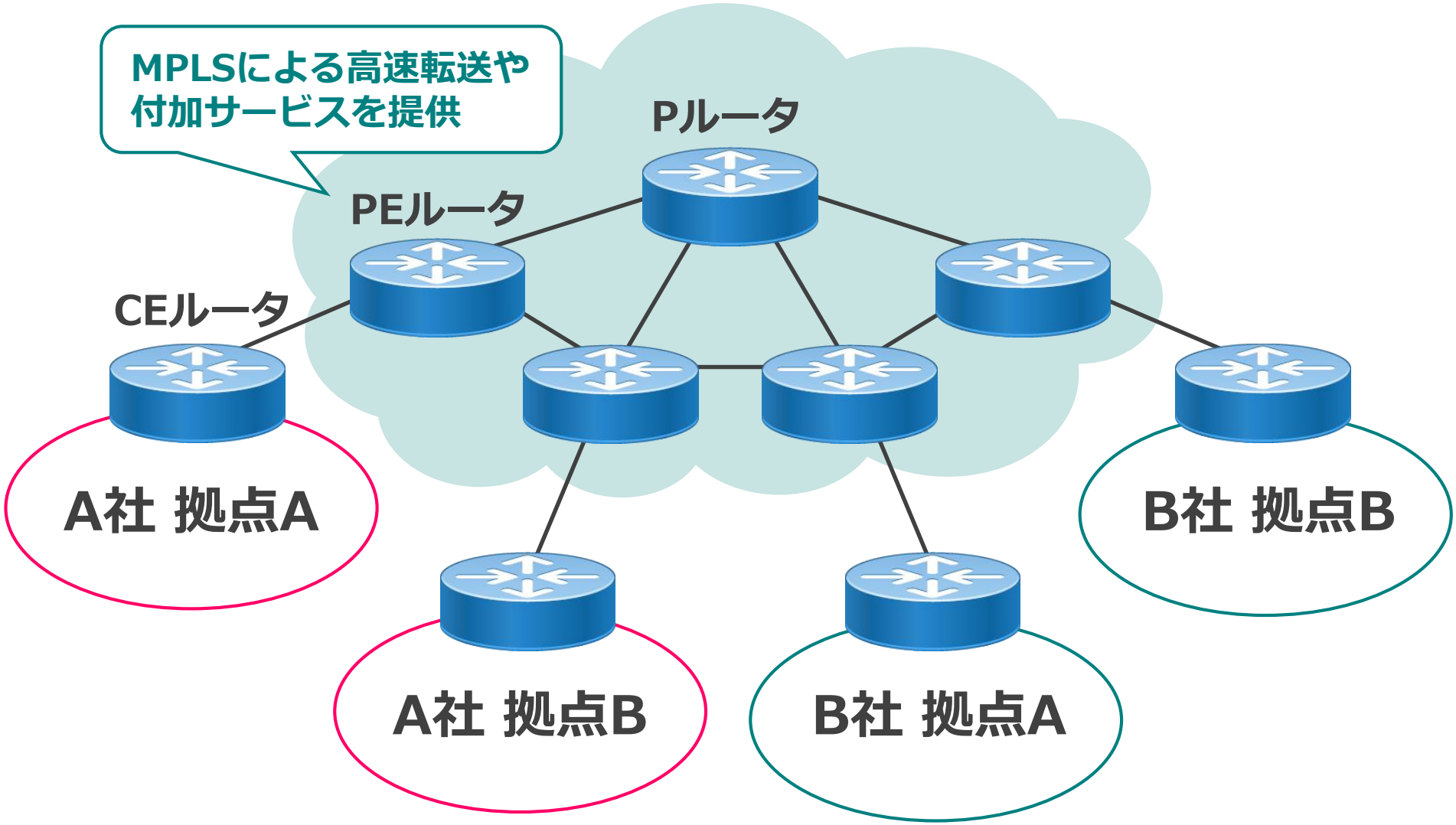
3.ArcstarUniversalOne VPNサービス(NTT-COM)
クラウド利用に求められる高品質・高信頼ネットワークサービスを国内外シームレスに利用できるクラウド対応データネットワークサービス。アクセス回線のメイン回線のみにギャランティ型を適用するギャランティプランと、バックアップ回線にも適用するプレミアムプランを選択でき、レイヤー2接続サービスを実現。

4.XePhion広域イーサネットサービス(NTT-ME)
XePhion 広域イーサネットサービスは、「全国一律」の料金体系で、全国のご利用拠点で1つのLANを構築できるネットワークサービス。豊富なアクセス回線ラインナップ、オプションサービスによりお客様に合ったネットワークを構築できます 。

5.KDDI Powered Ethernet（KDDI）
広帯域なメッシュ型ネットワークを、バックボーンからアクセス回線までワンストップで提供する広域イーサネットサービスです。クローズドネットワークとVLAN技術を活用し、専用線クラスの高いセキュリティを実現。

6.ULTINA Wide Ethernet（ソフトバンクテレコム）
フラット全国プラン：
全国統一の距離に依存しないアクセス回線毎の料金を規定した全国一律型の価格設定のプランを提供。
フラット地域プラン：
全国を７つの地域網に分け、地域網に閉じたネットワークに対してアクセス回線毎に料金を規定した料金プランを提供。

通信事業者が提供するIP-VPN網



●IP-VPN

通信事業者のVPNサービスを契約後、通信事業者の提供する網を利用した複数拠点でのIP通信を行うことができます。

IP-VPNのメリット
・フルメッシュで接続できる
・閉域網のためセキュリティが保たれる
・網内でQoS（優先制御）等の付加サービスを受けることができる

IP-VPNのデメリット
・プロトコルがIPに限定される
・サービスを提供している通信事業者にIPアドレス設計等で制約を受ける場合がある

※MPLS（Multi-Protocol Label Switching）
フレームやパケットの前方にラベルと呼ばれる識別子を付加して転送を行うことにより、高速化や機能の付加を図る技術。

※P（Provider）ルータ
プロバイダネットワーク内に存在し、顧客のルータとの接続を持たないルータ。PルータはMPLSをサポートしていなければいけない。

※PE（Proveider Edge）ルータ
顧客のルータであるCEルータと接続するルータ。プロバイダネットワークの境界に位置し、ラベルの付加/除去を行います。IP-VPNでは最も重要なルータ。

※CE（Customer Edge）ルータ
顧客のネットワークを構成するルータ。特殊な機能は必要なくIPパケットをルーティングできれば良い。

●主なIP-VPNサービス

1.Arcstar Universal One　VPNサービス
　（ギャランティorプレミアムプランのL3接続）

2.XePhion IP-VPNサービス

3.ULTINA IP-VPN

4.KDDI IP-VPN

●主なIP-VPNサービス

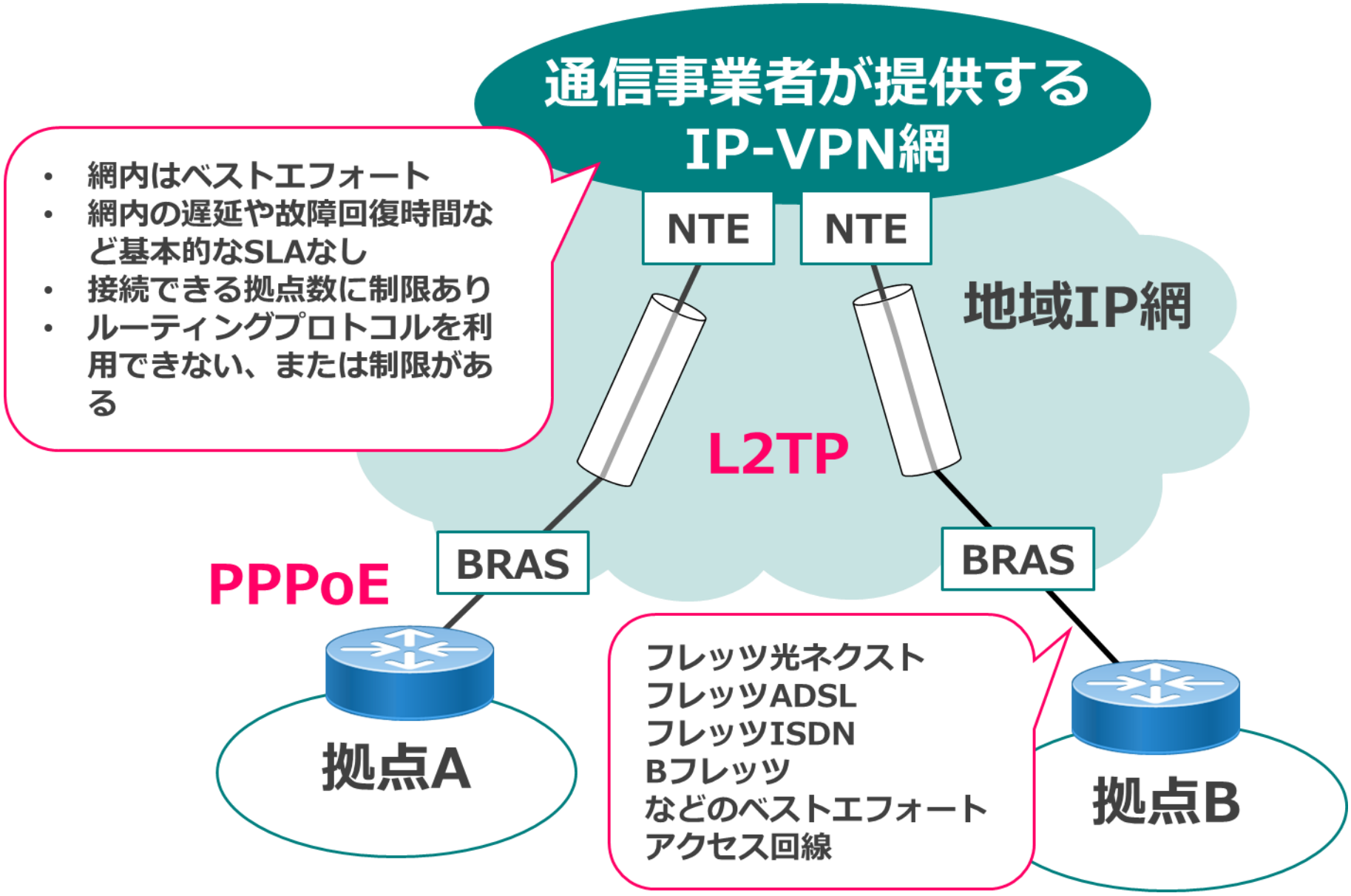
1.Arcstar Universal One VPNサービス(NTT-COM)
クラウド利用に求められる高品質・高信頼ネットワークサービスを国内外シームレスに利用できるクラウド対応データネットワークサービス。アクセス回線のメイン回線のみにギャランティ型を適用するギャランティプランと、バックアップ回線にも適用するプレミアムプランを選択でき、レイヤー3接続サービスを実現。

2.XePhion IP-VPNサービス(NTT-ME)
中継区間は距離に関係のない帯域ごとの定額料金のため、全国にまたがるネットワークを事業所間の距離を気にせず、県間接続を経済的に構築することができます。

3.ULTINA IP-VPN(ソフトバンクテレコム)
ソフトバンクの独自光網である「Etherコネクト」など豊富なアクセスラインナップから、お客様の通信状況に合わせた回線速度を選択することができるIP-VPNサービスです。

4.KDDI IP-VPN(KDDI)
世界主要都市にIP-VPN専用接続ノードを設置し、海外拠点から国内IP-VPN網へアクセスできるようにしています。KDDI Powered Ethernetと相互接続することも可能です。

●エントリー型IP-VPN



●エントリー型IP-VPN

エントリー型IP-VPNは明確な定義はありませんが、通信事業者が提供する閉域IP網を利用したセキュアでありながら安価なVPNサービスです。

エントリー型IP-VPNのメリット
・インターネットVPNと同等かそれ以下の低コスト
・閉域IP網を使用しているため高セキュリティ

エントリー型IP-VPNのデメリット
・東西間でネットワークが分かれてしまうことがある
・接続拠点数に上限がある
・網内でインターネット接続ができない
・拠点ごとのネットワークが1セグメントまでしか利用できない

※L2TP（Layer2 Tunneling Protocol）
第二層のデータリンク層で動作するプロトコルで、PPPを使用する際にポイントツーポイントで仮想的に通信路を確立する必要がある場合に使用されるプロトコルです。なお、暗号化機能は備わっておりません。

※NTE（Network Termination Equipment）
ネットワーク終端装置でISPと対応するルータのこと。1つのISP毎に最低1台設置が必要です。

※BRAS（Broadband Remort Access Server）
光アクセスユーザ、ADSLアクセスユーザを収容するためのルータでPPPoEを終端する。

※PPPoE（Point to Point Protocol over Ethernet）
PPPではなくPPPoEを利用するのは、PPPには電話で呼び出す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。

●主なエントリー型IP-VPNサービス

1.フレッツVPNワイド
　（フレッツVPNプライオ含む）

2.Arcstar Universal One　VPNサービス
　（ベストエフォートプランのL3接続）

3.Xephion ブロードバンド接続サービス
　フレッツタイプR

4.ULTINA Managed Ether

5.KDDI IP-VPN ブロードバンドValue パック

●主なエントリー型IP-VPNサービス

1.フレッツVPNワイド（フレッツVPNプライオ含む）
NTT東日本エリアのフレッツ 光ネクストやBフレッツ、フレッツ・ADSL、フレッツ・ISDNを利用して、複数の拠点を接続することが可能なVPNサービスです。

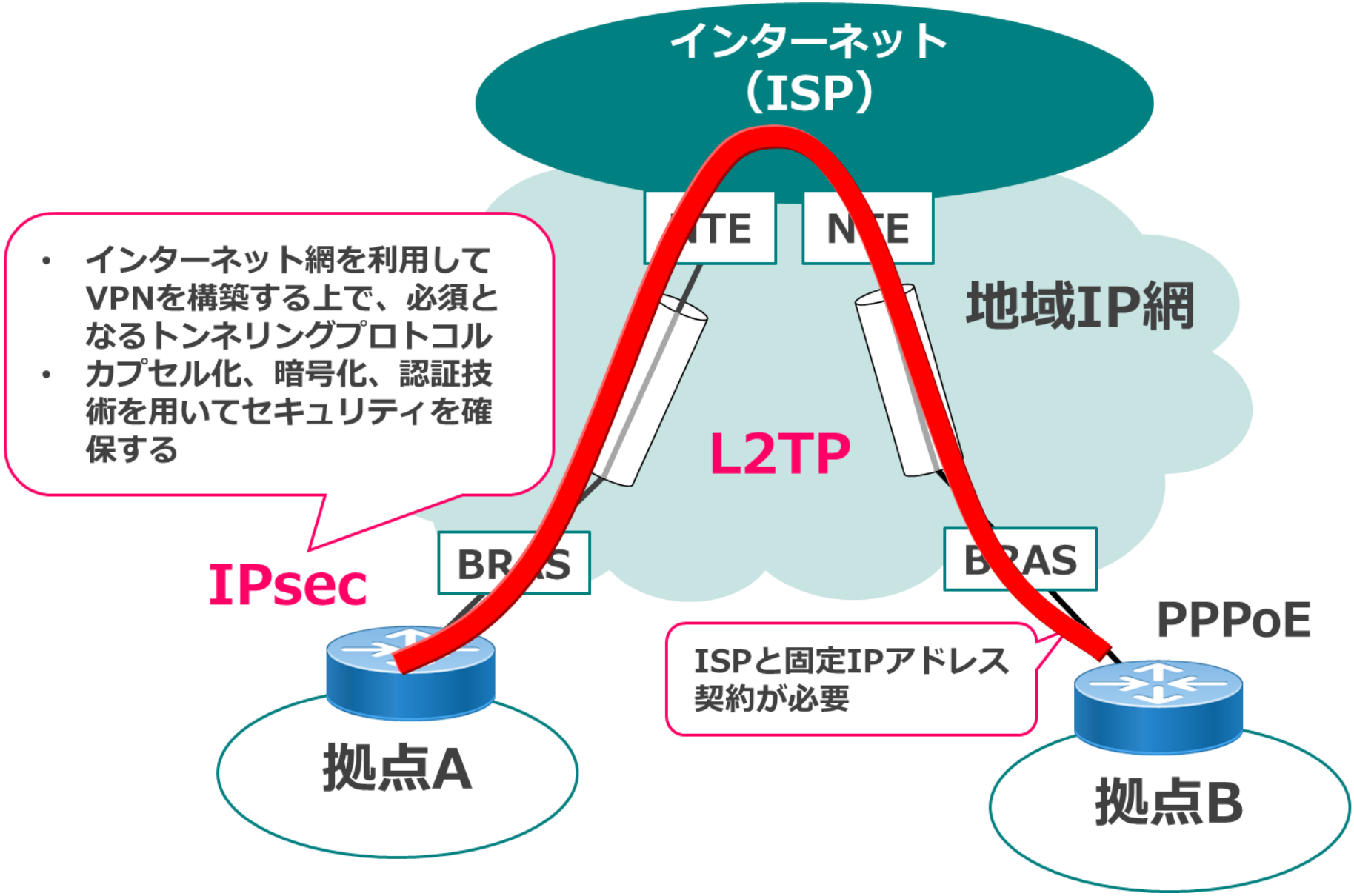
2.Arcstar Universal One VPNサービス(NTT-COM)
クラウド利用に求められる高品質・高信頼ネットワークサービスを国内外シームレスに利用できるクラウド対応データネットワークサービス。アクセス回線はNTT東日本・西日本のフレッツやNTTドコモLTEのワイヤレスアクセス（LTE）をメインアクセスとしたレイヤー3接続サービスを実現。

3.Xephion ブロードバンド接続サービス　フレッツタイプR(NTT-ME)
NTT-MEよりルータ機能内蔵の宅内装置を提供するため、ユーザ側でルータの準備・設定が不要。運用負担を軽減できる。

4.ULTINA Managed Ether(ソフトバンクテレコム)
低価格な閉域エントリーVPNサービスです。Managed Ether網内では、ユーザ単位で論理的にネットワークを分割することで異なるユーザ間の通信を完全に遮断できる。

5.KDDI IP-VPN ブロードバンドValue パック(KDDI)
企業向けデータ通信サービス「KDDI IP-VPN」のアクセス回線にNTT東西のフレッツ回線を利用したサービスです。KDDI専用IP網の利用料金やレンタルルータを低コストで提供できる。

●インターネットVPN



- インターネット網を利用してVPNを構築する上で、必須となるトンネリングプロトコル
- カプセル化、暗号化、認証技術を用いてセキュリティを確保する

●インターネットVPN

インターネットを経由して構築される仮想的なプライベートネットワークのこと。IPsecを利用したIPパケットの暗号化や、SSLを利用したアプリケーションレベルで暗号化等のセキュリティ対策が必須となる。インターネットVPNサービスとして、レンタルルータ（CPEルータ）や運用管理を申し込むことも可能ですが、ネットワーク知識があれば自前でVPN構築ができます。

インターネットVPNのメリット
・低コストで実現可能
・導入までの期間が短い

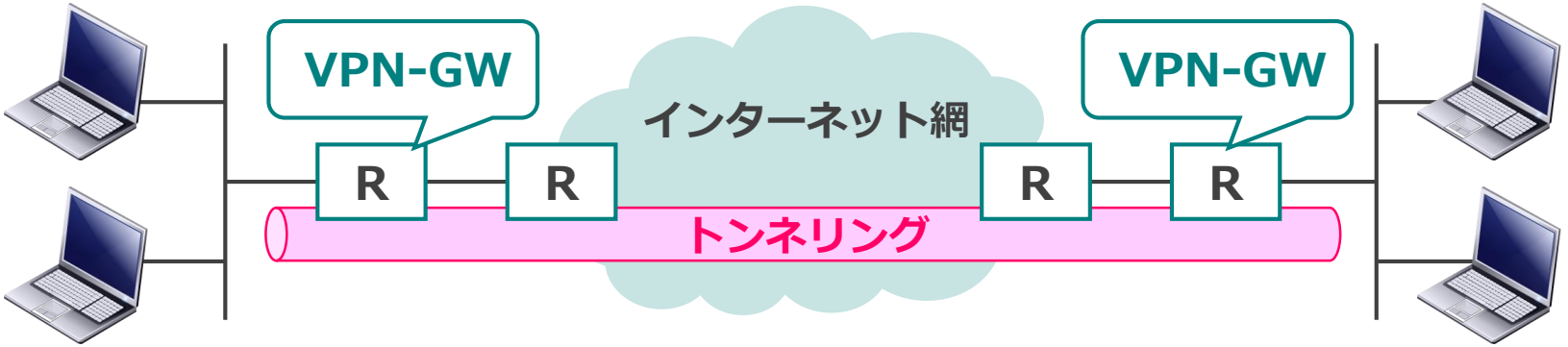
インターネットVPNのデメリット
・帯域制御が困難
・運用管理を自前で行う場合が多い
・暗号化処理によるルータ等への負荷が高い

フレッツVPNワイド

●VPNの種類

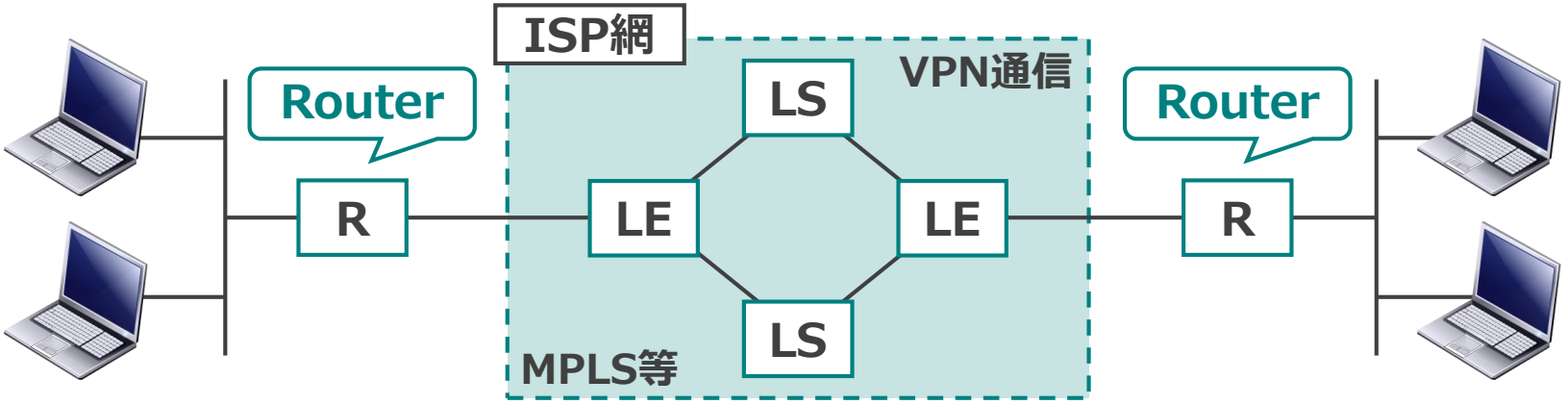
インターネットVPN

ユーザ（システム管理者）が、ネットワーク（OCNなどのISPサービス）やネットワーク機器（VPN-GW）を独自で調達して構築します。



IP-VPN

通信キャリアやISPが独自のVPN技術で構築したISPネットワークをユーザが借りる形で実現します。



●VPNの種類

VPNを実現するネットワークには、二つの形態があります。使用するネットワークのトラフィック量、ネットワークの使用目的、性能要件などを考慮し選択する必要があります。

【インターネットVPNの特徴】
ユーザのVPNゲートウェイ間でIPトンネルを形成します。インターネット上で利用します。暗号化によるセキュリティ確保が必須です。

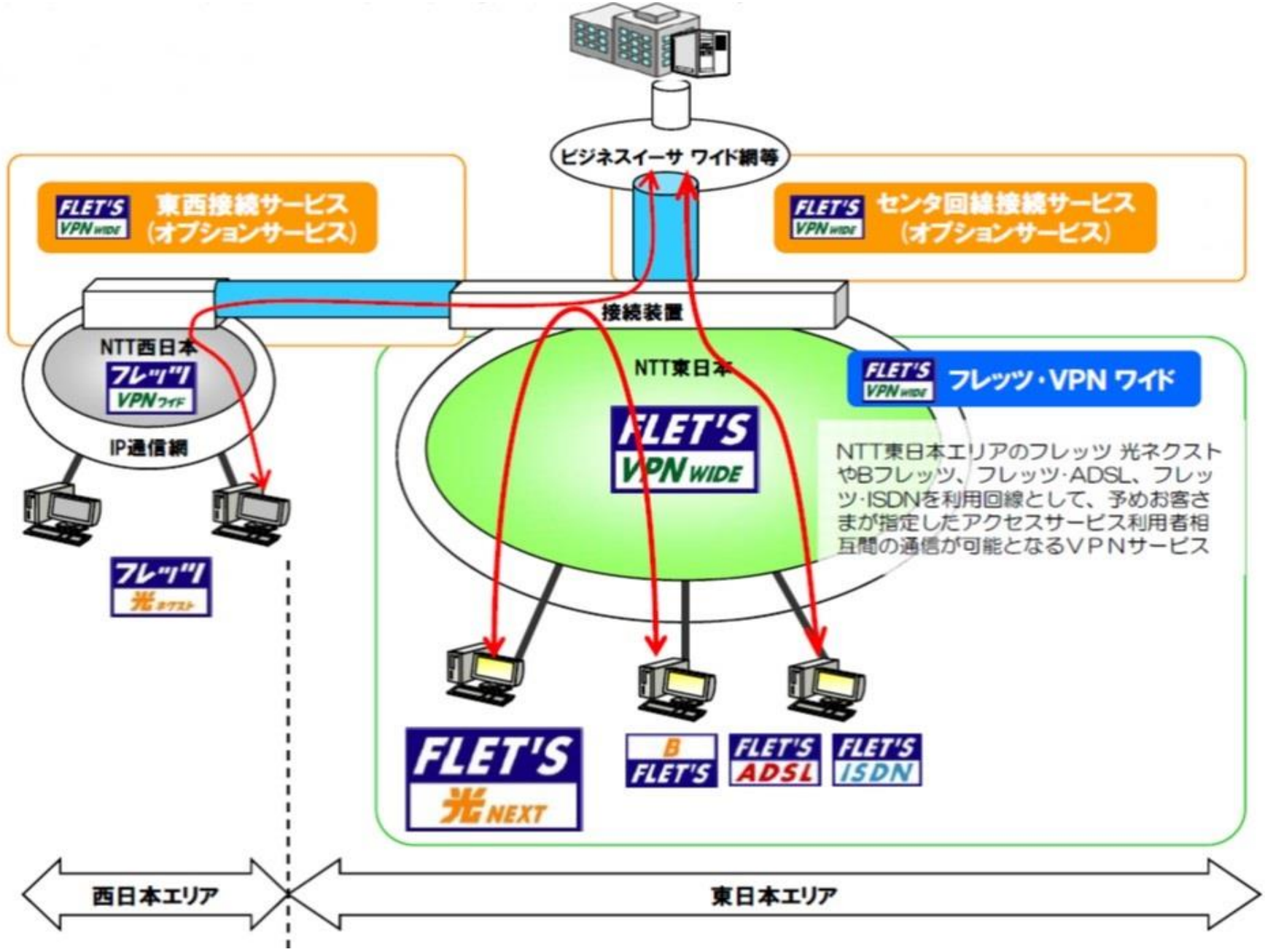
【IP-VPNの特徴】
ユーザは、通信キャリア／ISPのVPNサービス内容による制限がある場合があります。通信キャリア／ISPによって通話品質が保証されます（フレッツVPNワイド等のエントリー型IP-VPNは例外）。閉域網のため暗号化が必須ではありません。基本的にはユーザ側にVPN-GWが必要となりません。

●VPN特徴比較

		IP－VPN		インターネットVPN	
セキュリティ		◎	・インターネットと隔絶された閉域網を利用するためセキュリティが高い。 ・接続拠点を回線で限定することが可能なためセキュリティが高い。	△	・インターネットを利用するため、インターネットを介した情報漏洩等の危険は完全には避けられない。 ・接続拠点を端末のVPN設定で限定しているため、VPN設定情報が漏洩した場合に危険。
コスト	イニシャル	◎	・VPN機能が端末に必要ない。	○	・VPN機能が端末に必要。
	ランニング	◎	・VPN機能付端末やVPNソフトウェアのレンタル/保守費用が必要ない。 ・ISP月額利用料が必要ない。	○	・VPN機能付端末やソフトウェアのレンタル/保守費用が必要。 ・ISP月額利用料が必要。
導入の容易さ		◎	・端末にIPSec等のVPN設定が必要なく設定が簡単。 ・短期間で開通可能。	△	・端末にIPSec等のVPN設定が必要であり設定が煩雑。
通信の安定性		◎	・インターネットのトラヒックの影響を受けにくい。	△	・インターネットのトラヒックの影響を受ける。 ・インターネットからの攻撃（DoS攻撃等）を受けた場合、通信の遅延や切断の可能性がある。

●VPN特徴比較

●サービス概要


ビジネスイーサ ワイド網等
FLET'S VPN WIDE 東西接続サービス（オプションサービス）
FLET'S VPN WIDE センタ回線接続サービス（オプションサービス）
接続装置
NTT西日本
フレッツ VPNワイド
IP通信網
フレッツ 光ネクスト
NTT東日本
FLET'S VPN WIDE
FLET'S VPN WIDE フレッツ・VPN ワイド
NTT東日本エリアのフレッツ 光ネクストやBフレッツ、フレッツ・ADSL、フレッツ・ISDNを利用回線として、予めお客さまが指定したアクセスサービス利用者相互間の通信が可能となるVPNサービス
FLET'S 光NEXT
B FLET'S
FLET'S ADSL
FLET'S ISDN
西日本エリア
東日本エリア

●サービス概要

フレッツ･VPNワイドは、フレッツ光ネクスト、Bフレッツ、フレッツ･ADSL、フレッツ･ISDN等のアクセスサービスを利用のお客さま間にて、簡易なプライベートネットワークの構築を実現する、ベストエフォート型のサービスです。本サービスを利用することにより、同一プライベートネットワーク内のお客さま間でお互いの共有ファイルへのアクセス等をセキュアに行うことができます。

オプションサービスとして、お客さまのネットワークやサーバ等を接続可能である「センタ回線接続サービス」や、NTT西日本のフレッツ･VPNワイドと接続可能である「東西接続サービス」を利用することで、より柔軟に様々な形態でのプライベートネットワークを構築することができます。

●フレッツVPNワイドの4つのメリット

◆多彩なオプションサービス

オプションサービスを利用して、ギャランティ型ネットワークとの組み合わせや、
NTT西日本エリアの拠点との接続が可能となります

◆高セキュリティで安心

閉域のIPネットワーク内で特定の拠点のみと接続
加えて、ユーザ認証によりさらに強固なセキュリティを実現
VPNへの接続には、ユーザID、パスワード、フレッツナンバー通知
または発信者番号通知を用いた認証を実施します

◆低コストで導入・運用

毎月リーズナブルな定額料金
また、一般的な機器で接続するため、導入コストを削減

◆簡単に拠点を接続

フレッツ 光ネクスト、Bフレッツ等のフレッツ・アクセスサービスを
利用するため、手軽に、しかも広範囲の拠点を接続できます

●フレッツVPNワイドの４つのメリット

●カスタマーコントロール

NTT東日本

FLET'S

フレッツ・VPN ワイド ご利用状況詳細

お客さま名：東日本電信電話　株式会社 様
お客さまID：CAF112[redacted]

フレッツ・VPN ワイドの「新規」「変更」「廃止」の各種申し込み、「ご利用状況の確認」を行うことができます。

新規お申し込み

フレッツ・VPN ワイドの新規申し込みを行います。
必ず本サービスのお申し込み前に、「サービス概要」「ご利用上の注意」をご確認願います。
「サービス概要」「ご利用上の注意」の閲覧にはインターネット(IPv4)接続が必要です。

サービス概要　ご利用上の注意

サービス名	申し込み内容	説明	申し込みボタン
フレッツ・VPN ワイド	新規VPN開設	・新たにVPN開設を行います。 ・VPN管理者になります。	新規VPN開設
	既存VPN参加 ※	・既に開設されてるVPNに参加します。 ・VPN参加者になります。	既存VPN参加

※「光ステーション」をご利用中のお客さまは、本サイトの「既存VPN参加」から申し込み出来ません(本サイトからお申し込みをいただいても「フレッツ・VPN ワイド」へ接続できません)。
弊社営業担当者、またはフレッツ・VPN ワイド サービスに関するお問い合わせフォーム(フレッツ公式ホームページ https://flets.com/inquiry/vpnwide/form.html)よりお申し込みいただきますようお願いいたします。

ご利用状況の確認、変更・廃止のお申し込み

こちらでは現在のお客さまのご利用状況が表示されています。

プラン変更の申し込み

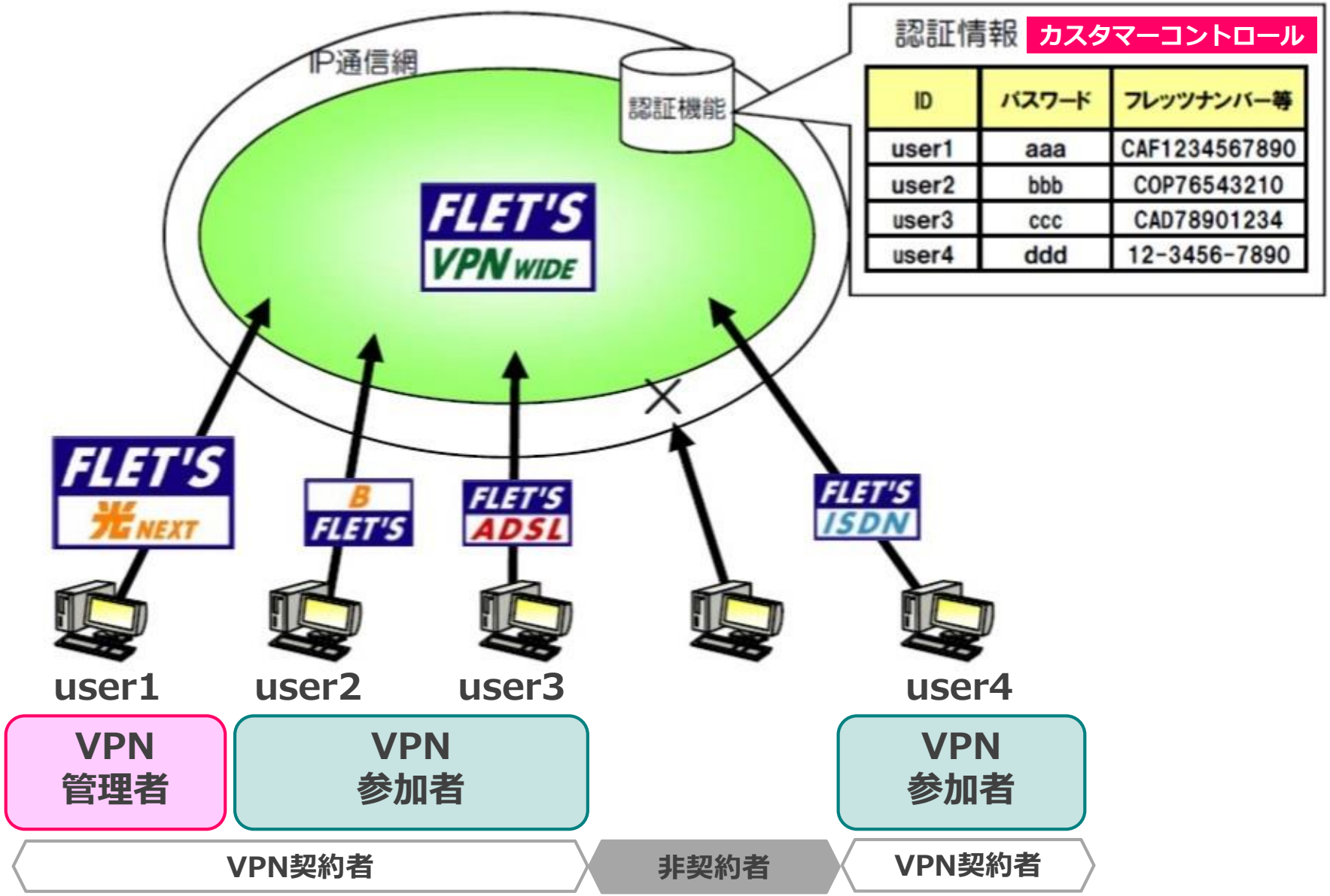
ご利用のプランを変更される場合は、対象の「プラン変更」ボタンを押し、次画面以降でプラン変更手続きを行ってください。

●カスタマーコントロール

カスタマコントロールとは、契約者自身が契約の範囲内で、直接利用環境を設定できる機能のことです。カスタマコントロールへの接続は、ONUとPCを直接接続する方法や、ルータを介して接続する方法があります。
また、接続の際には、回線開通時にお客様へ届く「開通のご案内」を事前に用意し、記載されているお客様IDとアクセスキーを準備する必要があります。

フレッツVPNワイドのカスタマコントロールでは、管理者となる拠点をあらかじめ決めておき、VPNグループで使用されるユーザIDやパスワード、IPアドレスなどを設定することができます。
設定した情報は、管理者がVPN参加拠点へ周知する必要があります。

●ユーザタイプ(管理者と参加者)



●ユーザタイプ(管理者と参加者)

【VPN契約者】
同一VPNを利用する本サービスの契約者で、管理者と参加者の2種類があります。

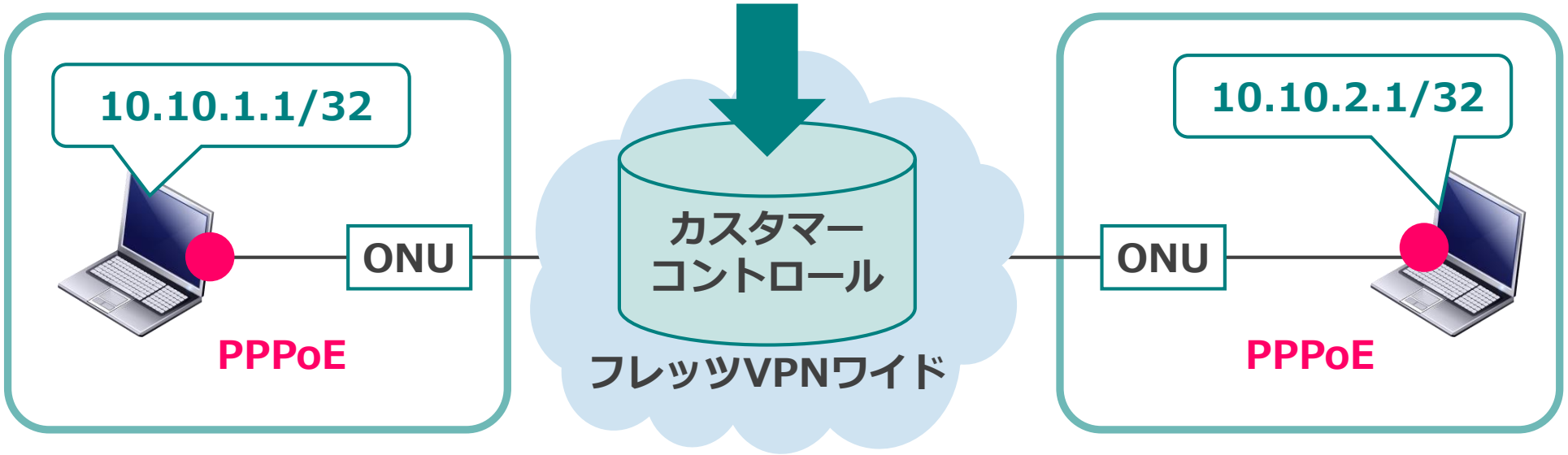
【VPN管理者】
VPNの管理を行う契約者です。カスタマコントロールを利用して、VPNの様々な設定を行うとともに、VPN参加希望者に対して、必要な情報の通知等を行います。VPN管理者は、VPN内に1契約者のみであり、VPNを開設した契約者が初期のVPN管理者となります。VPN管理者は、アクセスサービスとしてフレッツ光ネクスト、Bフレッツ、フレッツ･ADSL、フレッツ･ISDNを利用することができます。また、センタ回線接続サービス、東西接続サービス、サポートオプションは、VPN管理者のみが申込可能です。

【VPN参加者】
VPN管理者以外のVPN契約者であり、VPN管理者の承諾のもとVPNに参加するVPN契約者です。VPN管理者より通知された情報によりVPNを利用することができます。アクセスサービスとしてフレッツ光ネクスト、Bフレッツ、フレッツ･ADSL、フレッツ･ISDNを利用することができます。

●PCによるVPN接続のIPアドレス

カスタマーコントロールに登録したIPアドレス(端末型払い出し)

IPアドレス	サブネットマスク
10.10.1.1	255.255.255.255
10.10.2.1	255.255.255.255



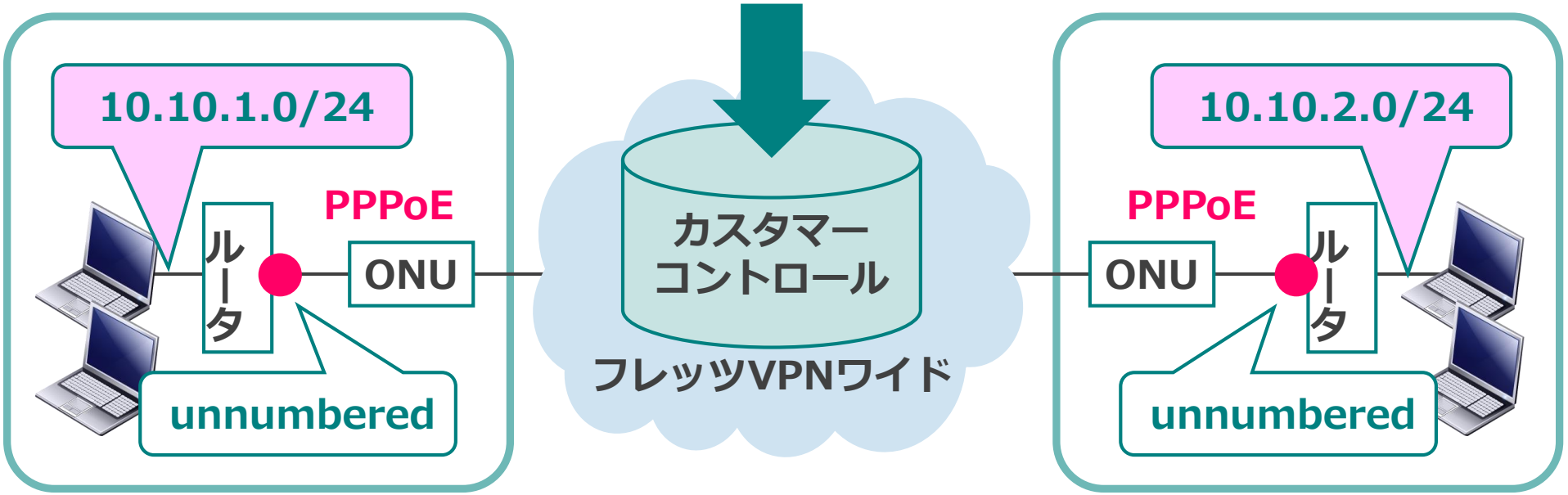
●PCによるVPN接続のIPアドレス

フレッツVPNワイドを用いて拠点間通信をおこなう際は、事前にカスタマーコントロールに通信を行う拠点のIPアドレスを登録する必要があります。

●ルータによるVPN接続のIPアドレス

カスタマーコントロールに登録したIPアドレス(LAN型払い出し)

IPアドレス	サブネットマスク
10.10.1.1	255.255.255.0
10.10.2.1	255.255.255.0



●ルータによるVPN接続のIPアドレス

フレッツVPNワイドを用いて拠点間通信をおこなう際は、事前にカスタマーコントロールに通信を行う拠点のIPアドレスを登録する必要があります。

VPN技術

◆トンネリング

元のパケットに**新しいIPヘッダを付加**することを**カプセル化**と呼び、VPN技術ではカプセル化のことをトンネリングと呼びます。

◆暗号化

盗聴されても、元のデータが**容易に推定できないように変換**することを暗号化といいます。公共のネットワークであるインターネットを利用したVPNでは、暗号の技術が非常に重要である為、IPデータを暗号化し通信を行います。

◆認証

データ通信の場合の認証とは、通信する相手が本当に正しい相手であるのか、といったことや、受け取った通信内容が途中で「**改ざん**」されていない本当に正しい内容であるのかといったことを確認することを認証と呼んでいます。相手方のVPN装置自体を認証し、「**なりすまし**」を防ぐ為に行われます。

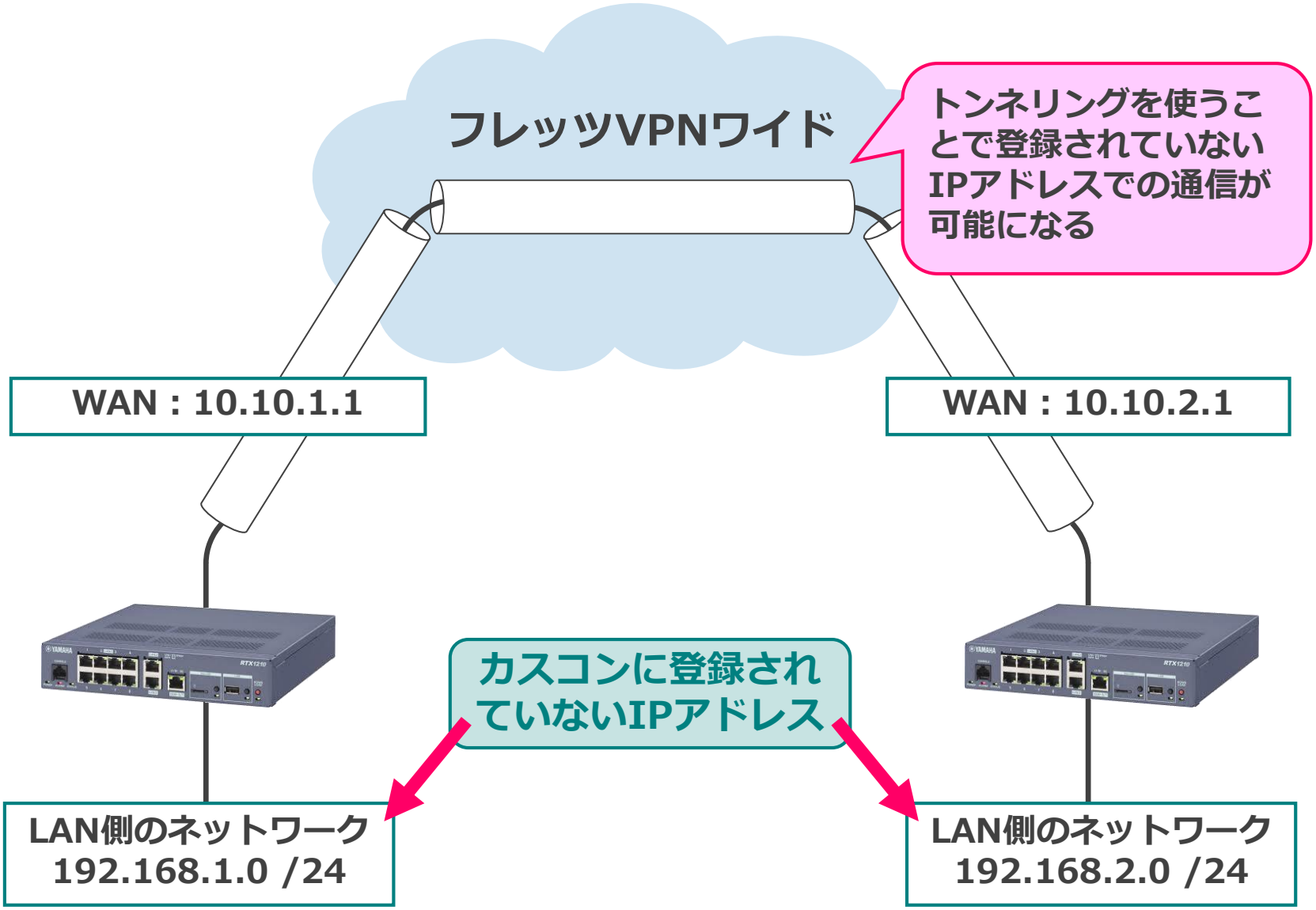
●VPNの基礎となる技術

トンネリング
・トンネリングプロトコル

暗号化
・共通鍵暗号方式
・公開鍵暗号方式

認証
・Pre-Shared key
・ハッシュ関数
・デジタル署名
・PKI

●トンネリングが必要な構成

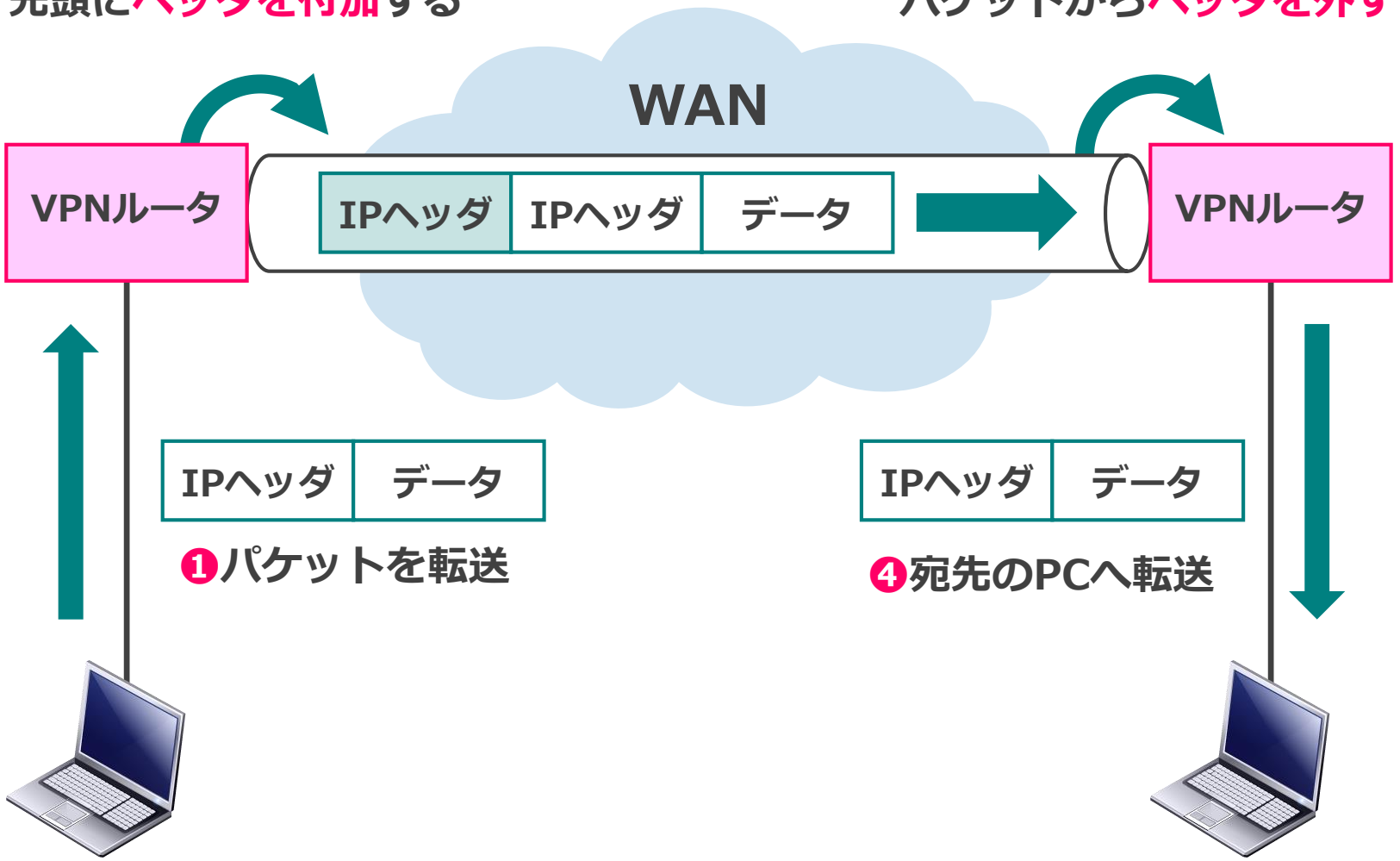


●トンネリングが必要な構成

フレッツVPNワイドでは、カスタマーコントロール上に登録されたIPアドレス以外はルーティングができないため、上記のような構成で拠点間通信を実現するためにはトンネリング技術を使用することで解決できます。

インターネットVPNでも、理屈は同じでインターネット上ではグローバルIPアドレス以外はルーティングできないため、プライベートIPアドレスでの拠点間通信を実現するためにトンネリング技術を使用します。

●トンネリング（カプセル化）



●トンネリング（カプセル化）

トンネリングとは、元のパケットに新しいIPヘッダを付加して、通信を行うことです。IPヘッダを付加することをカプセル化と呼びます。

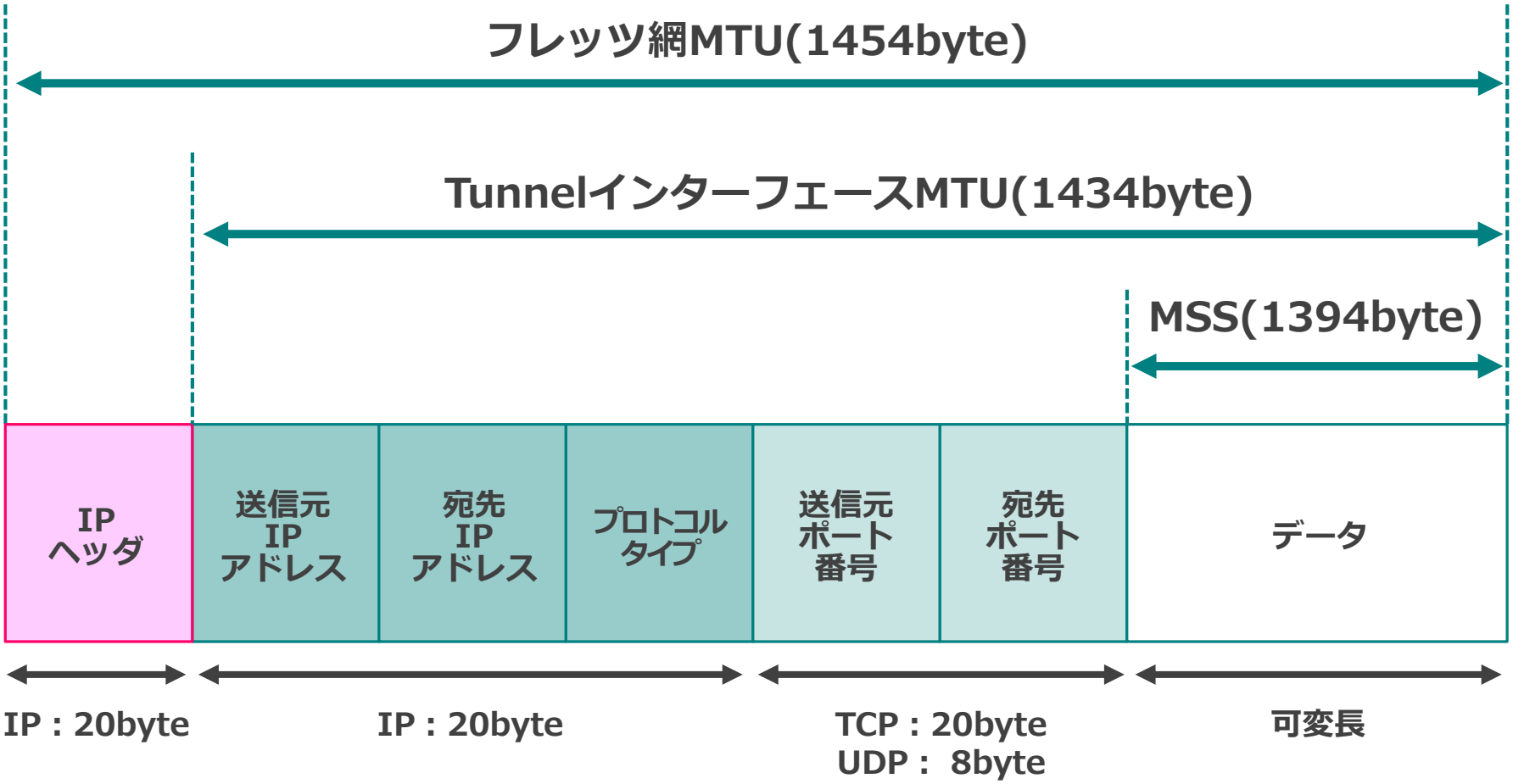
●IPIP（トンネリングプロトコル）

■IPIPは暗号・認証を行わない方法で通信トンネルを構成するシンプルなトンネリングプロトコルです

●IPIP（トンネリングプロトコル）

ONUに接続するルータでIPIPトンネルの設定をおこない、トンネリングします。

●IPIP（パケットサイズ）



●IPIPトンネルパケット

MTU(1454byte) = IPIP overhead (20byte) + IP Header (20byte) + TCP Header (20byte) + MSS (可変長)

適切なMTUサイズとMSSのサイズを設定することにより、パケットのフラグメント（分割）を防ぐことができます。

●IPsec（トンネリングプロトコル）

IPsecルータ

IKE ポート番号 UDP：500

IPsecルータ

ISAKAMP　SA

フェーズ2で使う鍵を作成

暗号鍵　認証鍵

フェーズ1

IPsec　SA

暗号鍵　暗号鍵

認証鍵　認証鍵

IPsecの暗号通信で使う鍵を作成

暗号鍵　認証鍵

ESP

プロトコル番号:50

暗号鍵　暗号鍵

通信確立

認証鍵　認証鍵

以降は作成した鍵を使って
パケットをやり取りする

フェーズ2

●IPsec

IPsecの最大の特徴としては通信の暗号化ができることです、主にインターネットVPNで使用されます。暗号化をおこなうためのIPsecシーケンスは大きく分けて2段階に分かれています。
フェーズ1では、対向の拠点が正しい相手なのか認証した上で、フェーズ2で行う鍵交換のためのコネクションを確立します。フェーズ2では、フェーズ1で確立されたコネクションを使用し、実際の通信を行うための鍵の交換を行います。
フェーズ1,2で確立されるコネクションのことをSAといい、SAを生成するために使われる鍵交換プロトコルをIKEといいます。
通信確立後はフェーズ2で交換した鍵を使用して、データの暗号化・復号化・改ざんのチェックを行います。

このようにセキュリティを高めることによって、インターネットなどの公共インフラでも暗号化することにより、安全に通信することが可能になります。
なお、IPsecの仕様によりマルチキャストを通過させることができないため、ダイナミックルーティングプロトコルの通信には別の技術が必要となります。

●VPNプロトコルのまとめ

VPN プロトコル	対応 プロトコル	マルチ キャスト 伝送	暗号化 完全性保障	ポピュラーな ソリューション
IPsec	L3 (IP)	×	○	IPユニキャストの トンネリング
IPIP	L３ (IP)	○	× 代替案：IPIP/IPsec	ルーティング プロトコルの トンネリング
L2TP	L2 (PPP) L3 (IP、IPX、など)	○	× 代替案：L2TP/IPsec	L2通信 リモートアクセス

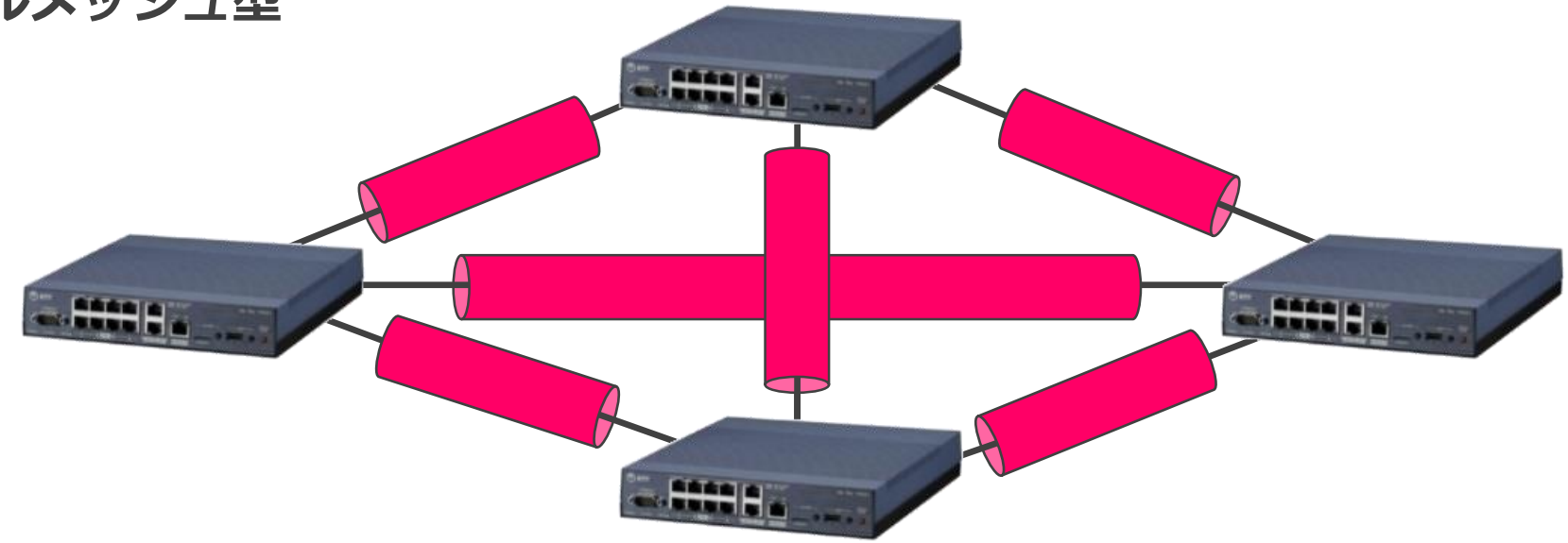
●VPNプロトコルのまとめ

トンネルプロトコルには他にも、PPTP、GRE等があります。

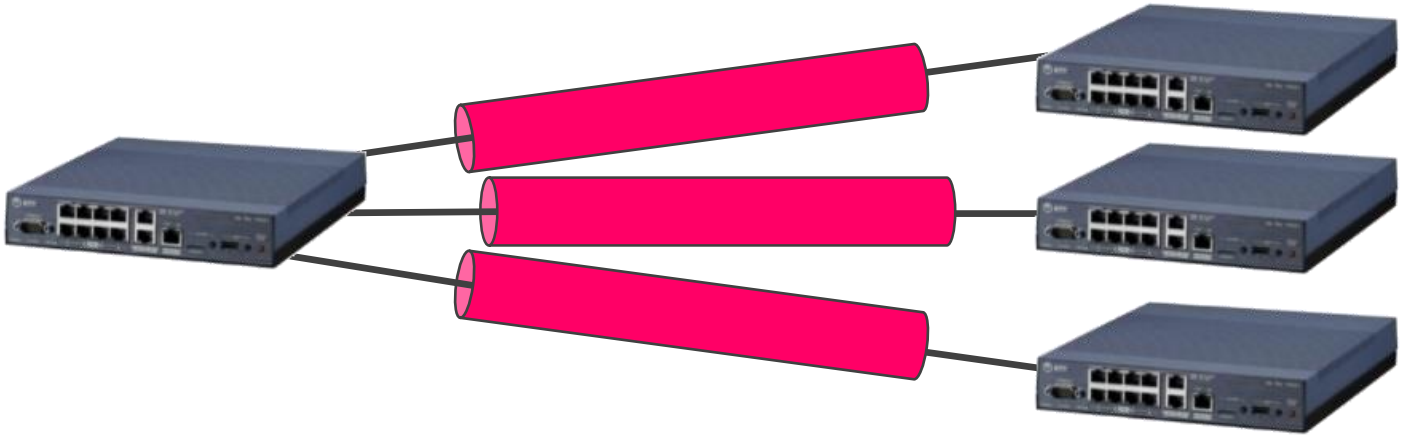
IPIPは暗号化機能を備えていない事から、データに対するセキュリティが保たれていません。そのため、データの安全性を保ちたい場合は、IPIP over IPSec等を使用します。
一般的に、IPIPはルーティングプロトコル等のマルチキャストパケットのトンネリングなどに使用されます。

●WANのトポロジ構成

フルメッシュ型



センタ・エンド型（ハブアンドスポーク）



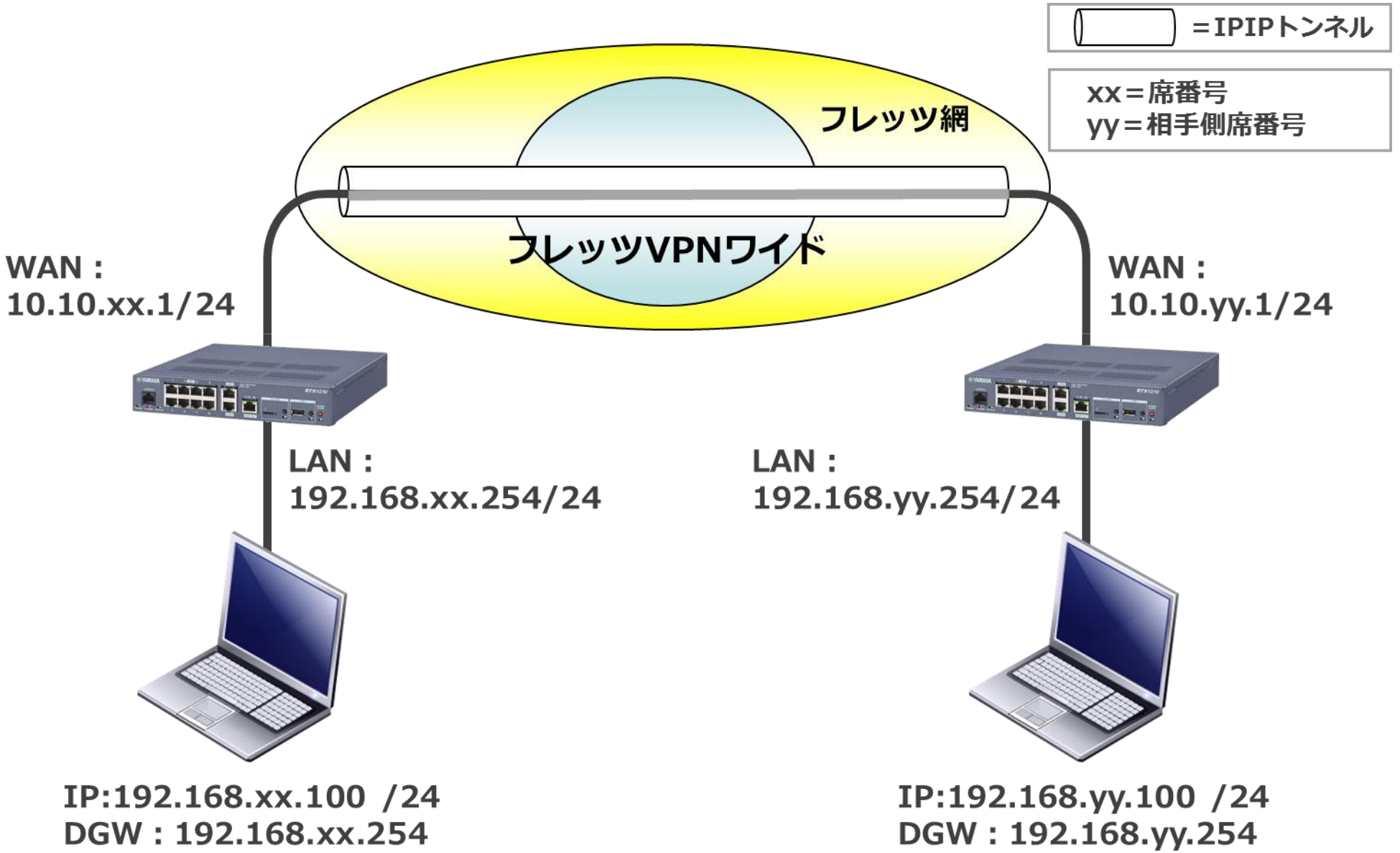
●WANのトポロジ構成

【フルメッシュ型】
拠点数が増える度に各拠点のルータにトンネル設定をおこなっていく必要があるため、設定が複雑になりがちです。ただし、どの拠点でも他拠点と直接接続できるため、ルーティング情報の設定がしやすくなります。

【センタ・エンド型（ハブアンドスポーク型）】
センタ・エンド型はトンネルの数を抑えられますが、センタ側ルータにトラフィックの負荷が掛かります。そのため、センタ側ルータには高い処理能力を備えたルータが必要になります。一般的に多拠点接続をおこなう際は、センタ・エンド型のトポロジを採用することが多いです。

演習①
トンネル技術を用いた
フレッツVPNワイドによる
拠点間接続

演習構成


＝IPIPトンネル
xx＝席番号
yy＝相手側席番号
フレッツ網
フレッツVPNワイド
WAN :
10.10.xx.1/24
WAN :
10.10.yy.1/24
LAN :
192.168.xx.254/24
LAN :
192.168.yy.254/24
IP:192.168.xx.100 /24
DGW : 192.168.xx.254
IP:192.168.yy.100 /24
DGW : 192.168.yy.254

1.端末とルータの設定確認

①PCのネットワーク設定をDHCP自動取得に変更します。

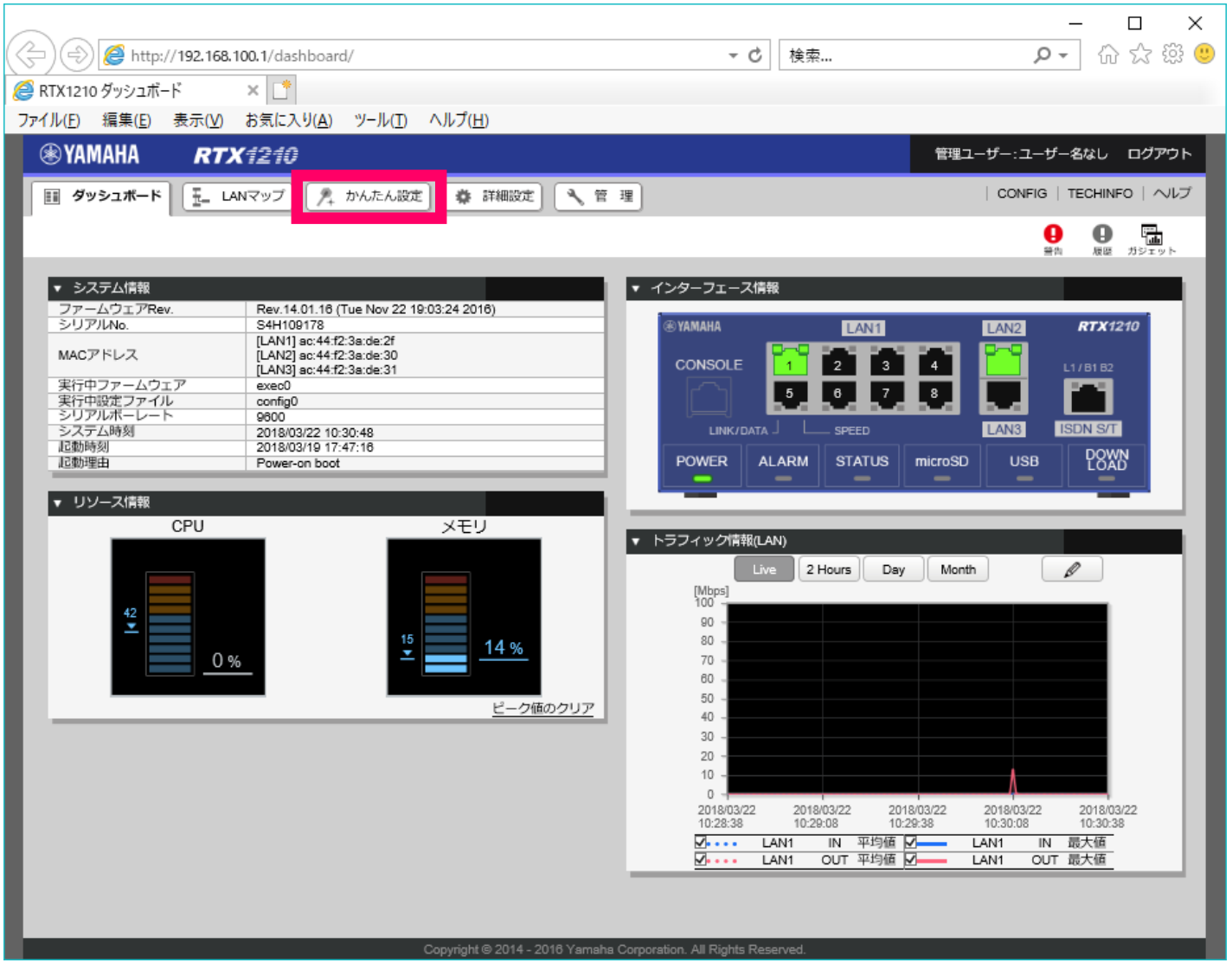
②PCとRTX1210、ONUとRTX1210をそれぞれLANケーブルで接続します。

③コマンドプロンプトからIPアドレスが自動取得できていることを確認します。

④ブラウザを起動し、RTX1210へ管理者としてログインします。

2.LAN1アドレスの変更

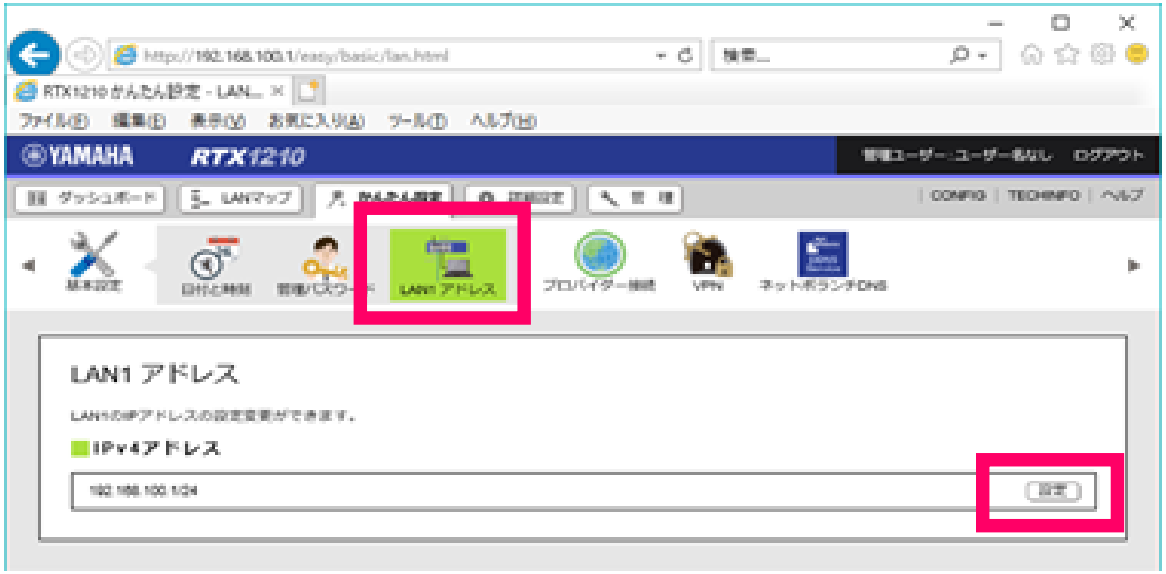
①【かんたん設定】をクリックします。



2.LAN1アドレスの変更

②【基本設定】をクリックし、【LAN1アドレス】をクリックします。

③IPv4アドレスの【設定】をクリックします

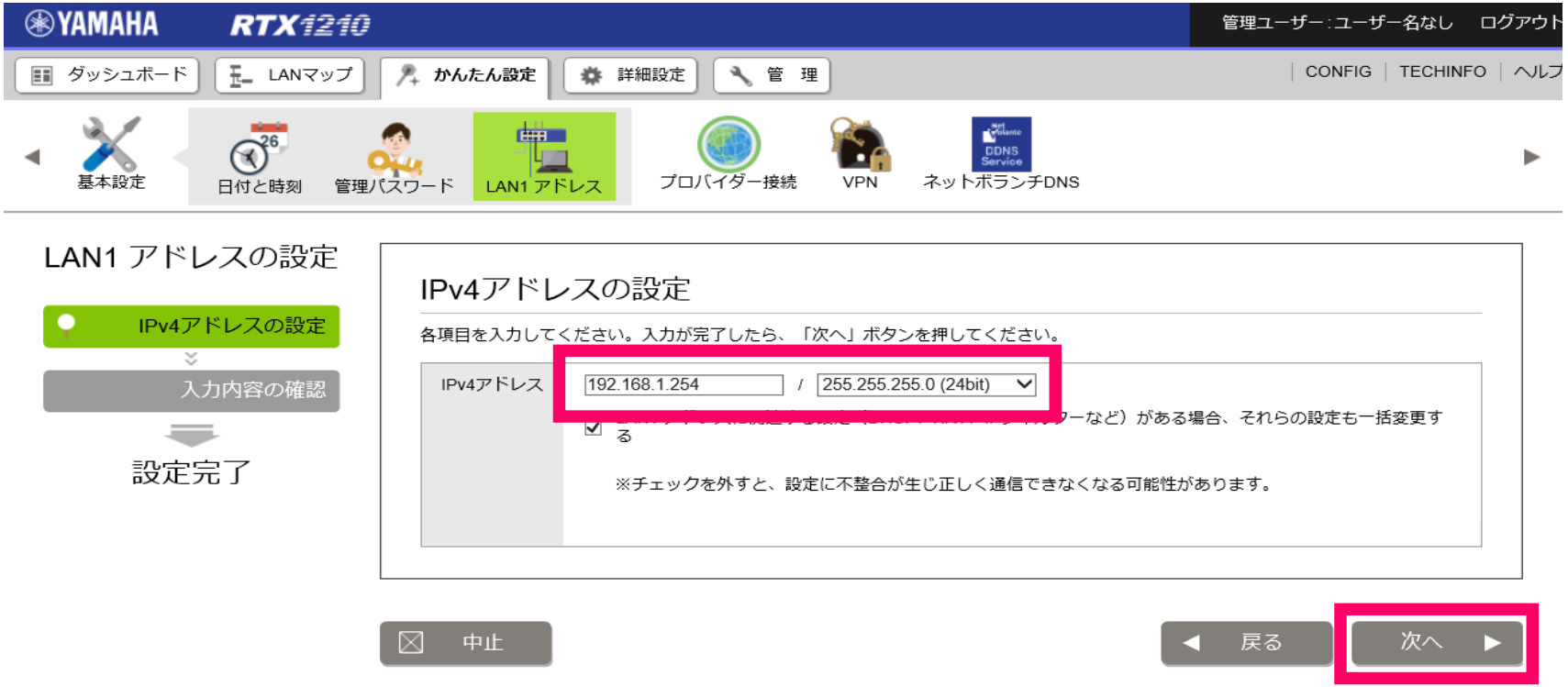


2.LAN1アドレスの変更

④IPv4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.ｘｘ.254】　サブネットマスク【255.255.255.0】

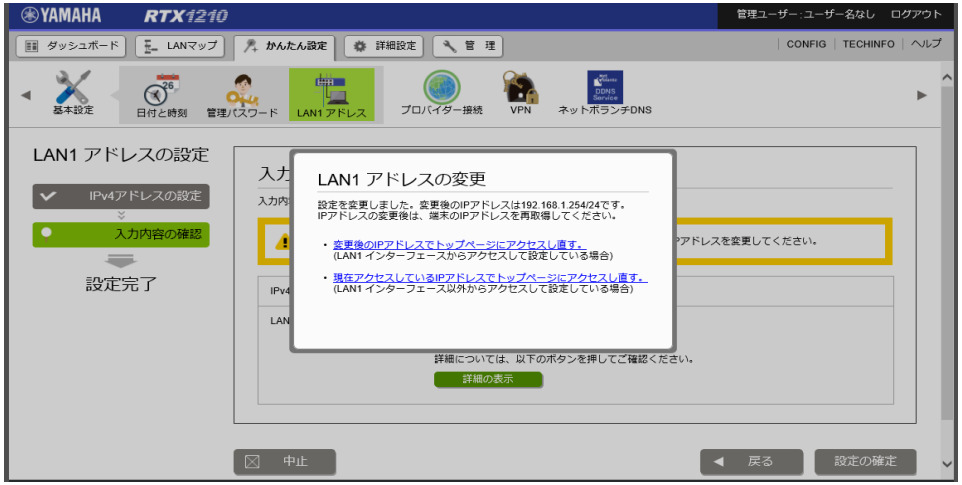
（ｘｘは席番号）



2.LAN1アドレスの変更

⑤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。

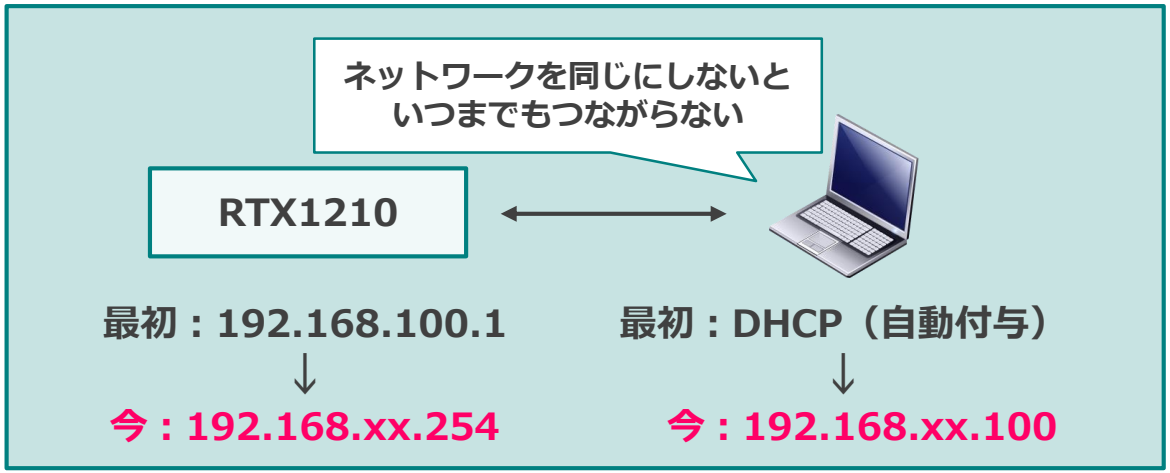
⑥設定の確定をクリックすると、ポップアップが表示されますが、そのままブラウザを閉じてください。



3.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。

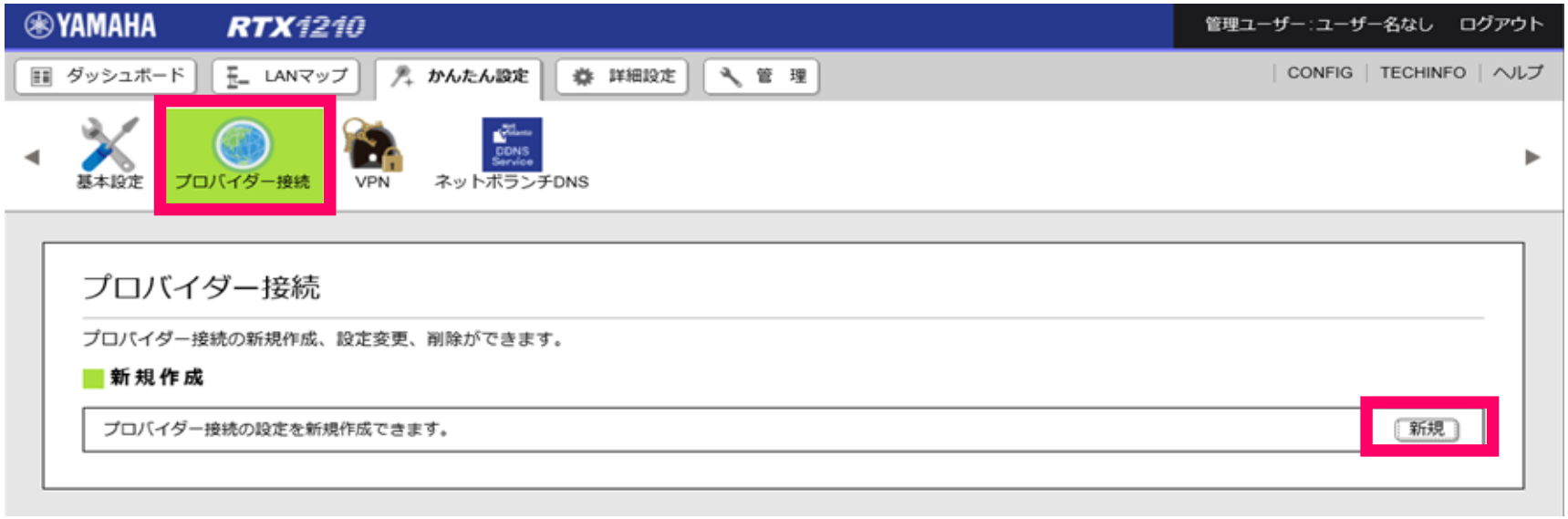
IPアドレス：192.168.ｘｘ.100　（ｘｘは席番号）
サブネットマスク：255.255.255.0
デフォルトゲートウェイ：192.168.ｘｘ.254
DNS：192.168.xx.254



②PCの設定変更後、ブラウザのアドレス記入欄に【192.168.ｘｘ.254】を入力し、ルータへ再ログインします。（ｘｘは席番号）

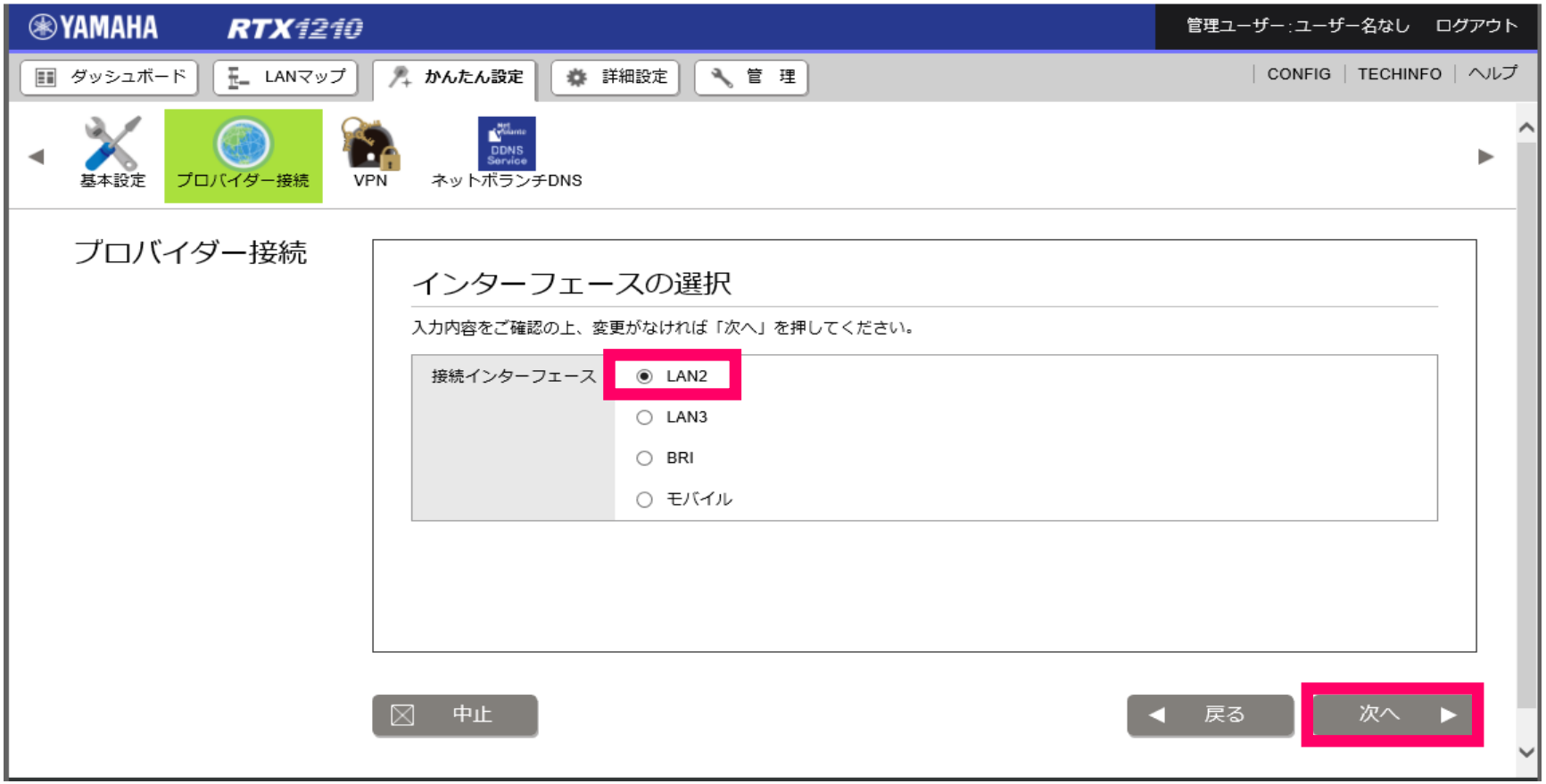
4.PPPoEの設定

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。



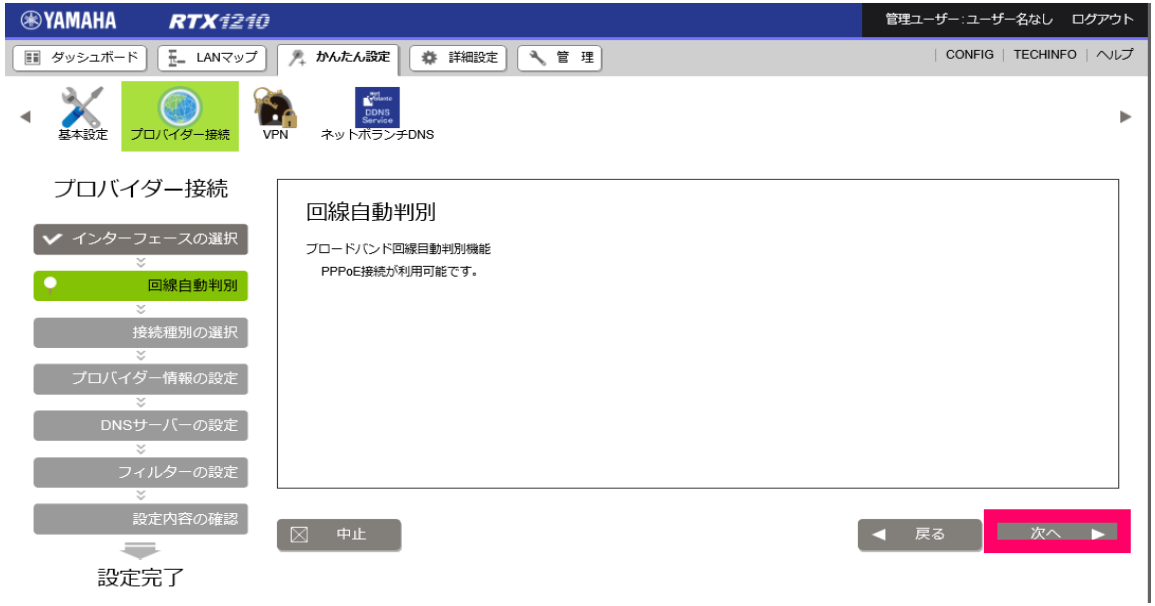
4.PPPoEの設定

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。



4.PPPoEの設定

③回線自動判別の画面で、次へをクリックします。



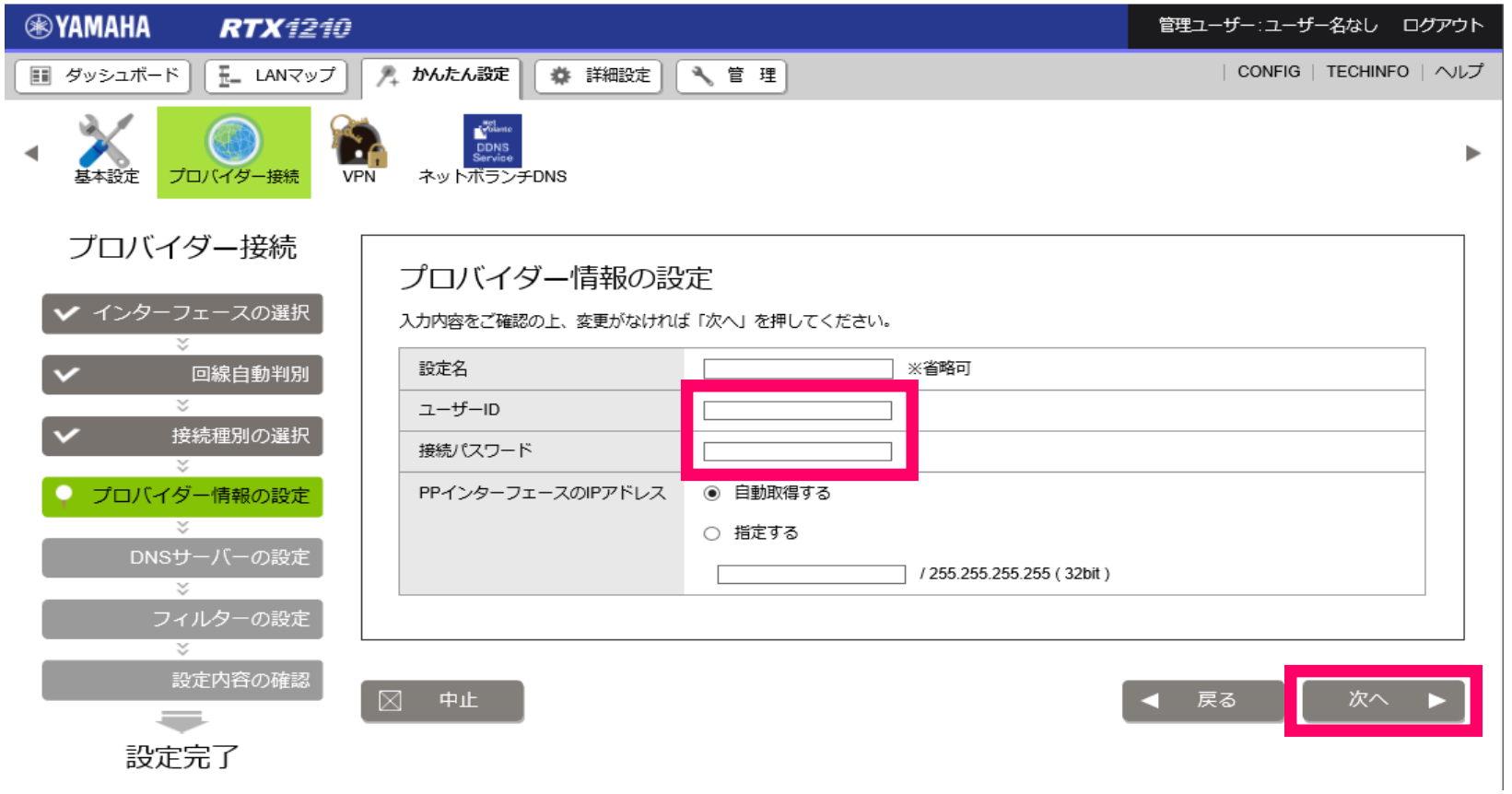
④接続種別の選択の画面で、次へをクリックします。

4.PPPoEの設定

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。

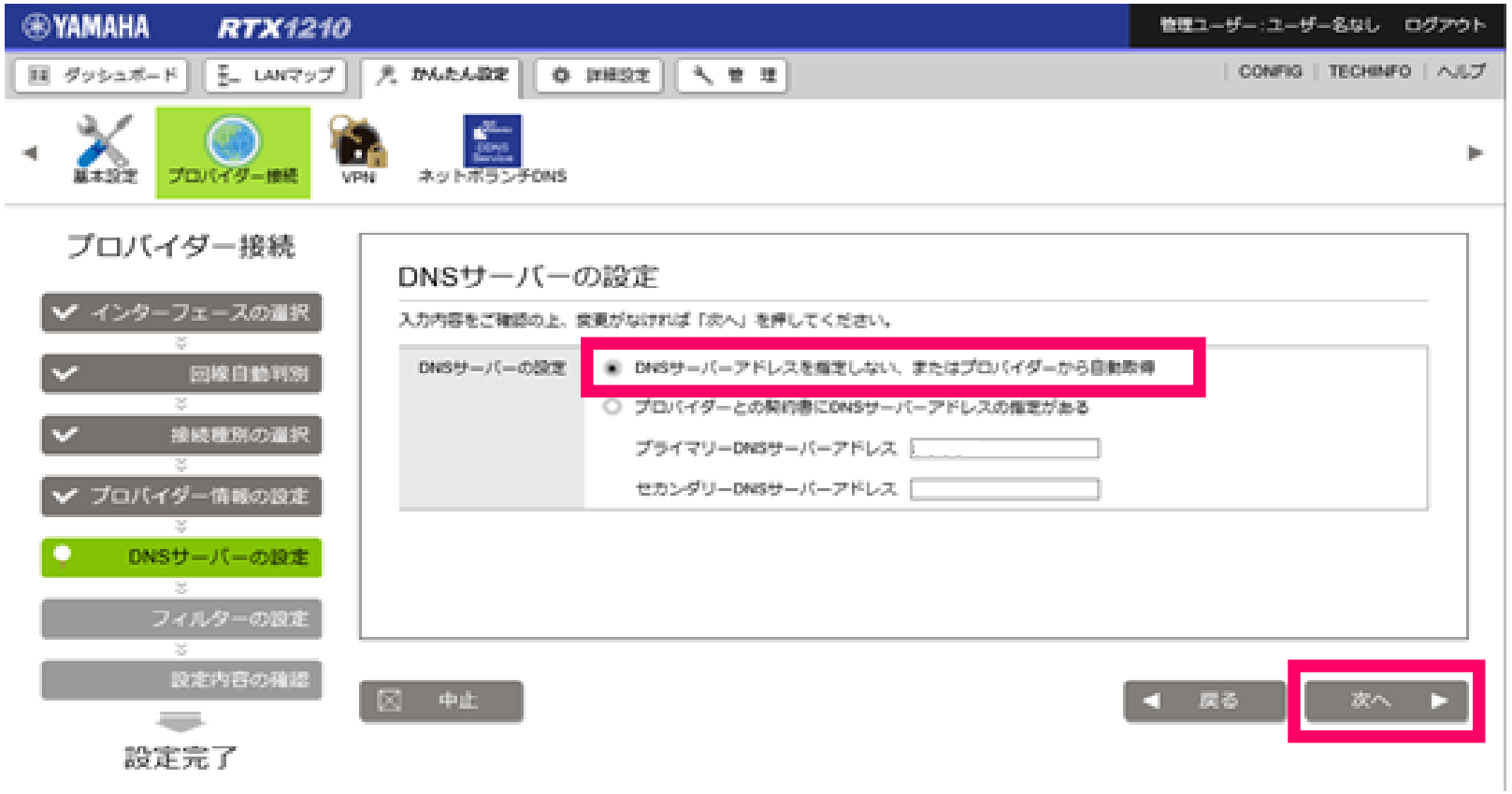
※ユーザ情報はデスクトップのフレッツVPNワイドアカウント表を参照

⑥入力後、次へをクリックします。



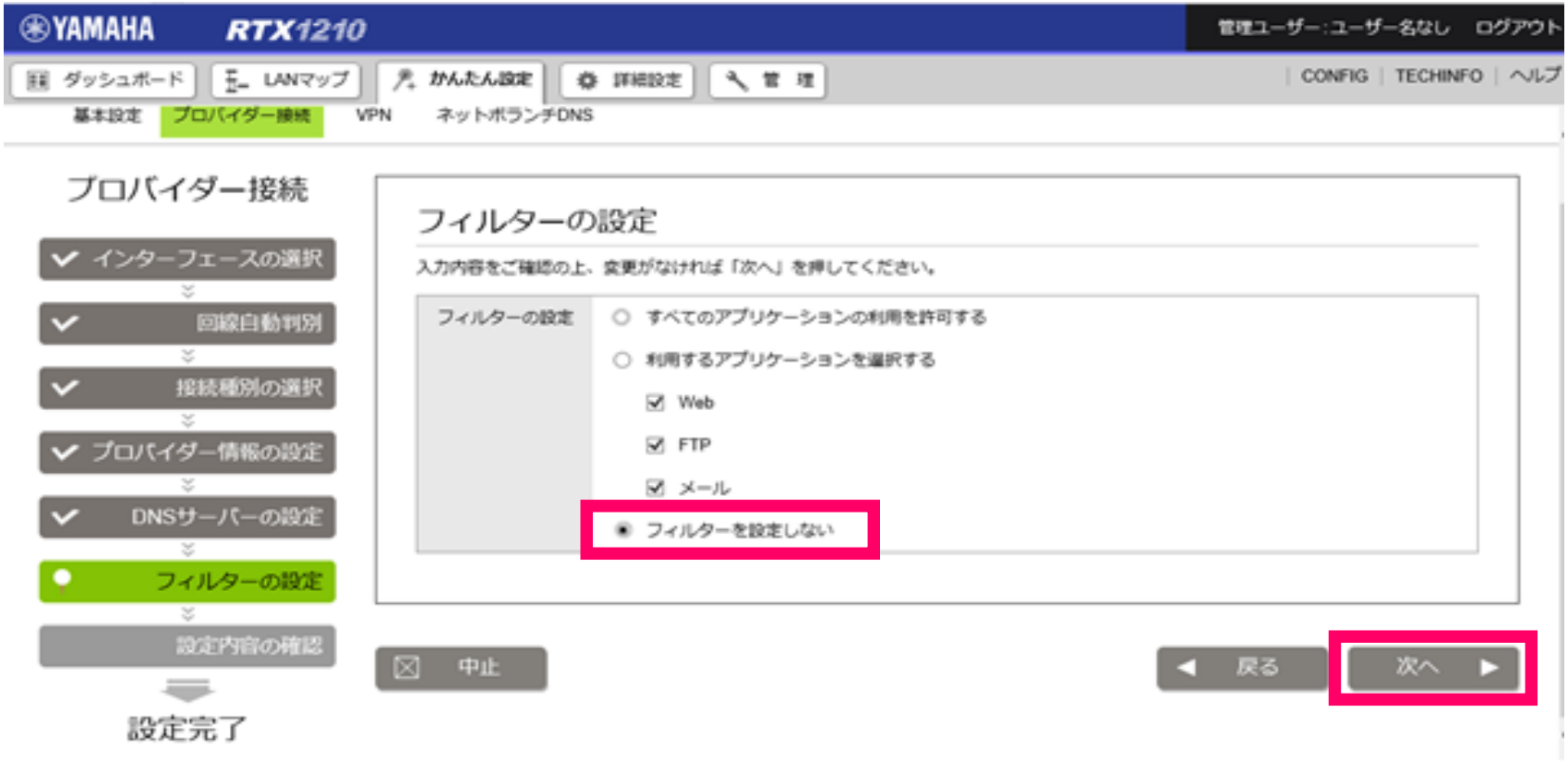
4.PPPoEの設定

⑦DNSサーバーの設定の画面で、【DNSサーバーアドレスを指定しない、またはプロバイダーから自動取得】を選択し、次へをクリックします。



4.PPPoEの設定

⑧フィルターの設定の画面で、【フィルターを設定しない】を選択し、次へをクリックします。



4.PPPoEの設定

⑨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。

4.PPPoEの設定

⑩プロバイダー接続の画面で、接続状態の欄にカスタマーコントロールから払いだされたIPアドレスが表示されていることを確認します。

例）10.10.ｘｘ.1（ｘｘは席番号）

5.VPN設定

①【VPN】をクリックし、【拠点間接続】をクリックします。

②拠点間接続VPNの新規作成で【新規】をクリックします

5.VPN設定

③接続種別の選択で【IPIP】を選択し、次へをクリックします。

5.VPN設定

④接続先のIPアドレスに、トンネルの接続先となる相手側のIPアドレスを入力します。

IPアドレス：10.10.yy.1　（yyは相手側席番号）

5.VPN設定

⑤IPIPトンネルを使用するインターフェースの設定で【指定する】を選択し、LAN2インターフェースのチェックボックスにチェックを入れ、次へをクリックします。

5.VPN設定

⑥経路に関する設定で、相手LAN側ネットワークに向けたルーティングを設定し、次へをクリックします。

接続先のLAN側アドレス：

192.168.yy.0 / 255.255.255.0（24bit）（yyは相手側席番号）

5.VPN設定

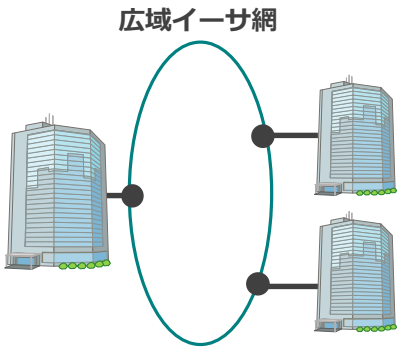
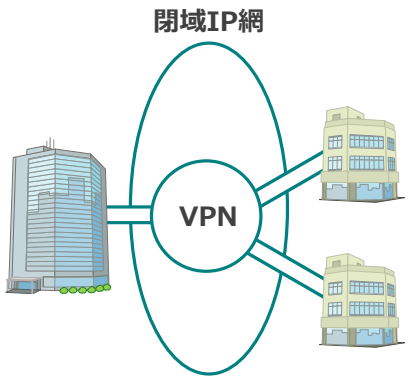
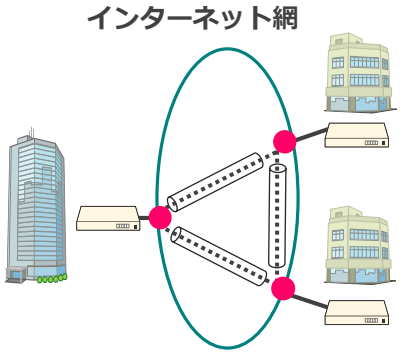
⑦入力内容の確認の画面で、設定した内容に間違いがないことを確認し、【設定の確定】をクリックします。

5.VPN設定

⑧拠点間接続VPNの画面で、接続状態の欄に⟷が表示され、正常に接続されていることを確認します。

ビジネスイーサワイド

●拠点間通信の種類

	専用線	広域イーサネット	エントリー型IP－VPN	インターネットVPN
拠点間通信の種類				
特徴	・ポイントツーポイント接続 ・物理層での専用網であるためセキュリティ、品質は高い ・帯域、距離等により異なるが、高価である	・通信速度が速く、遅延も小さい ・網構成の自由度が高く、拠点追加、プロトコル変更に柔軟に対応できる ・IP以外の通信プロトコル以外も通信	・インターネットと隔絶された閉域IP網内でVPNを実現 ・広範囲な拠点間通信を実現する	・インターネットの中に暗号化された専用経路を作り、VPNを実現する ・暗号化のための機器が必要。インターネットを介するため漏洩の危険は完全に回避できない
NTT東日本のサービス	HSD、DA、ATM メガリンクサービス	ビジネスイーサワイド	フレッツVPNワイド フレッツVPNプライオ	－
	ギャランティ型サービス： 契約した回線の帯域や故障回復時間、稼働率などを保証し、サービスの品質を『保証』。シビアな用途に使用する場合はギャランティ型サービスが適している		**ベストエフォート型サービス**： 『最善の努力』の意味からもわかるように、帯域が網の混雑状況等により左右される特性を持つ反面、安価な料金でのサービス提供を可能としている	

●拠点間通信の種類

現在、拠点間通信には様々な方法があります。専用線や広域イーサネットはギャランティ型サービスと呼ばれ、高セキュリティ・高品質というメリットがありますが、同時に高コストというデメリットがあります。
低コストであるエントリー型IP-VPNやインターネットVPN を用いた拠点間通信はベストエフォート型サービスと呼ばれています。

●広域イーサネットとIP-VPNの比較

	広域イーサネット（レイヤ2）	IP-VPN（レイヤ3）
ご利用に適したお客様業種／利用形態	**拠点数が少ない** 金融機関、メディア、通信事業者など拠点数は多くないがネットワークの重要度が高く、高度な設定が必要なお客様	**拠点数が多い** 製造業、流通業、サービス業等他店舗や、関連会社とのエクストラネット等、高度な設定は不要なお客様
他拠点ネットワークにおける設定のしやすさ	**煩雑** 接続拠点全てのルーティング情報を全拠点のルータに設定する必要がある	**簡単** 拠点のルータには通信事業者のルーターをネクストホップとして指定するだけ
カスタマイズのしやすさ	**自由度は高い** 多様なルーティングプロトコルを設定可能 （RIP、OSPF,IGRP、IS-ISなど）	**自由度は低い** 送信プロトコルはIPに限定 ルーティングプロトコルを使用する際はトンネリングプロトコルが必要

●広域イーサネットとIP-VPNの比較

ネットワークの多くがIP（インターネットプロトコル）というレイヤ3のプロトコルで設計されていること、そしてレイヤ3でのルーティング設定をお客さまが行うことは非常に煩雑であることから、一般的には、ネットワークに複雑な設計を必要としない標準的なお客さまは「IP-VPN（レイヤ3VPN）」を、高度なカスタマイズを求めるお客さまは「広域イーサネット（レイヤ2VPN）」を、選択する傾向にあります。

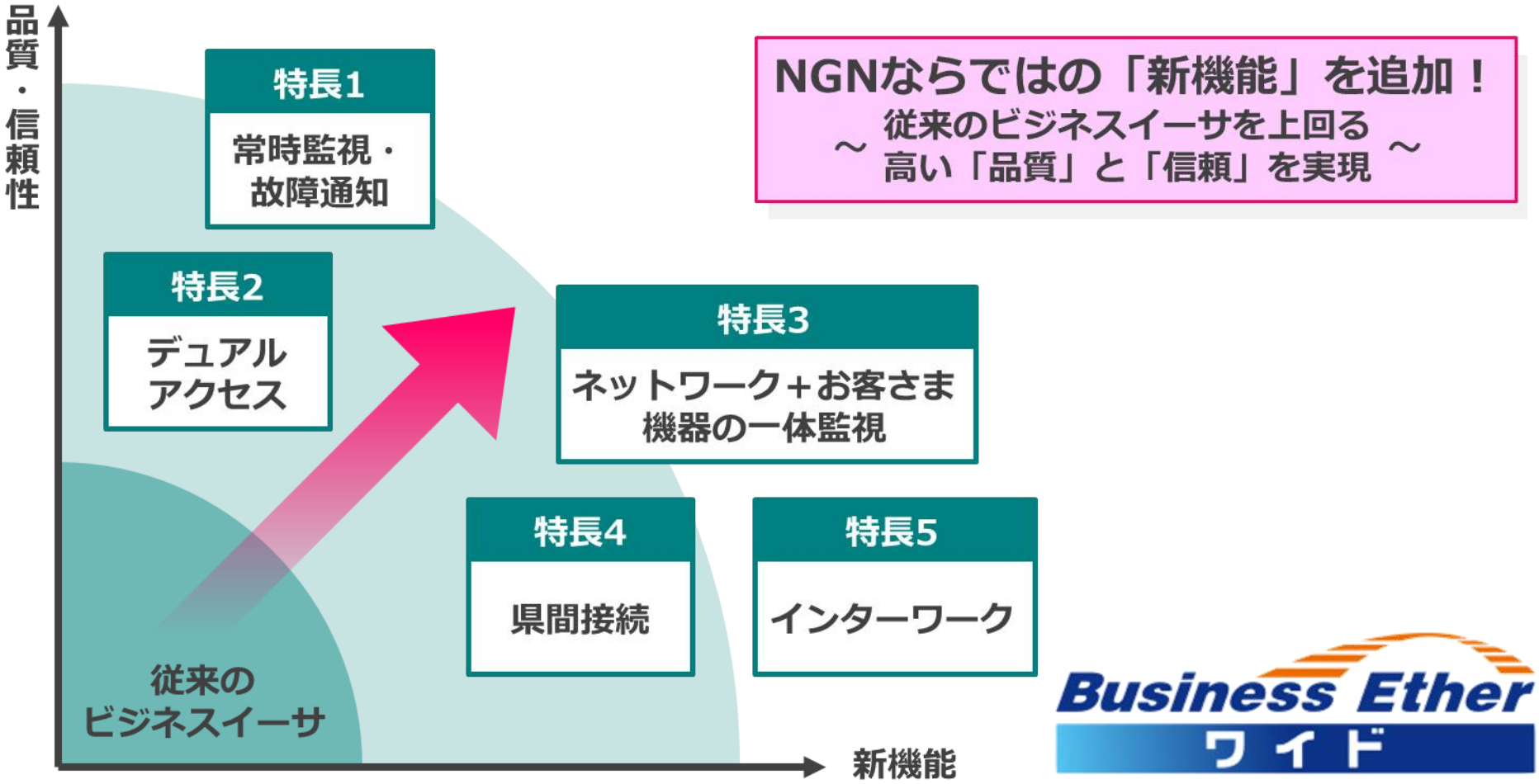
※NTTにおける主な広域イーサネットサービス

NTT東日本	ビジネスイーサワイド
NTT-ME	Xephion
NTT-COM	Arcstar Universal One、e-vlan

●ビジネスイーサワイド概要

既存のビジネスイーサ が持つ機能を網羅するとともに更なる利便性と信頼性の向上を実現した次世代（NGN）イーサーネットサービス

［従来のビジネスイーサとの比較 ］



NGNならではの「新機能」を追加！
～ 従来のビジネスイーサを上回る
高い「品質」と「信頼」を実現 ～

Business Ether ワイド

●ビジネスイーサワイド概要

【特長1：常時監視・故障通知】
イーサOAM技術（監視用フレームによる疎通確認）を採用することで、回線ごとに常時監視を行っていますので、従来のイーサネットサービス以上の高信頼性を実現しています。

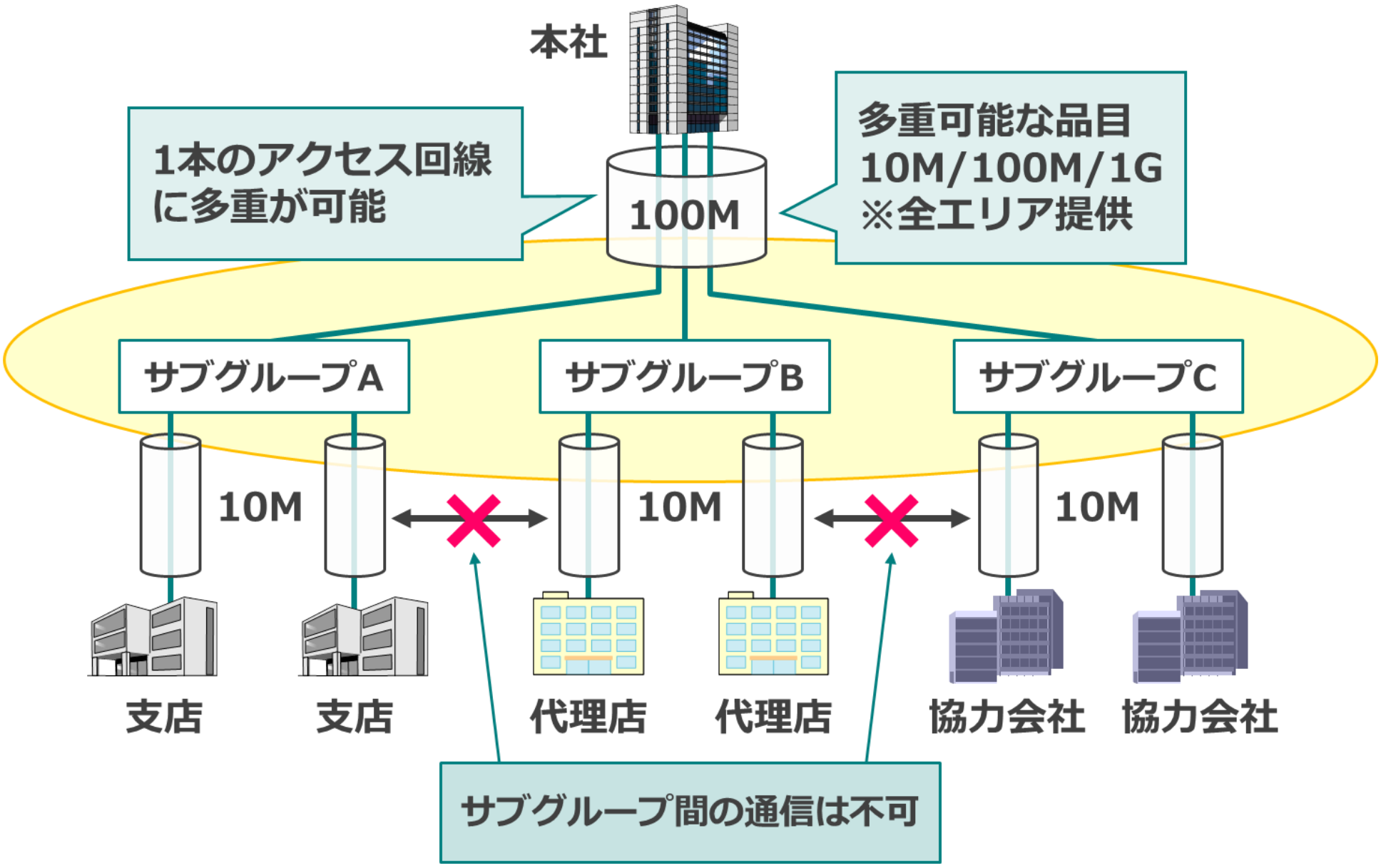
【特長2：デュアルアクセス】
網内（中継装置や中継回線等）が冗長構成となっており、万が一の障害発生時にも自動で迂回路へ切り替る構成となっています。

【特長3：ネットワーク＋NW機器の一体監視】
ビジネスイーサ網側からアクセス回線を通じて回線とNW機器の一体的な監視を行うことができ回線・端末機器の故障検知時には、管理者へ通知することができます。

【特長4：県間・東西間接続】
従来の県域内に閉じた通信に加えて県間通信も可能となりますので、複数の県に跨ったシームレスな広域ネットワークを実現します。

【特長5：インターワーク】
フレッツ・VPN ワイド等とのインターワーク接続により、拠点の規模や利用用途に応じて信頼性とコストのバランスが取れたネットワークが構築できます

●サブグループ


本社
1本のアクセス回線
に多重が可能
100M
多重可能な品目
10M/100M/1G
※全エリア提供
サブグループA
サブグループB
サブグループC
10M
10M
10M
支店
支店
代理店
代理店
協力会社
協力会社
サブグループ間の通信は不可

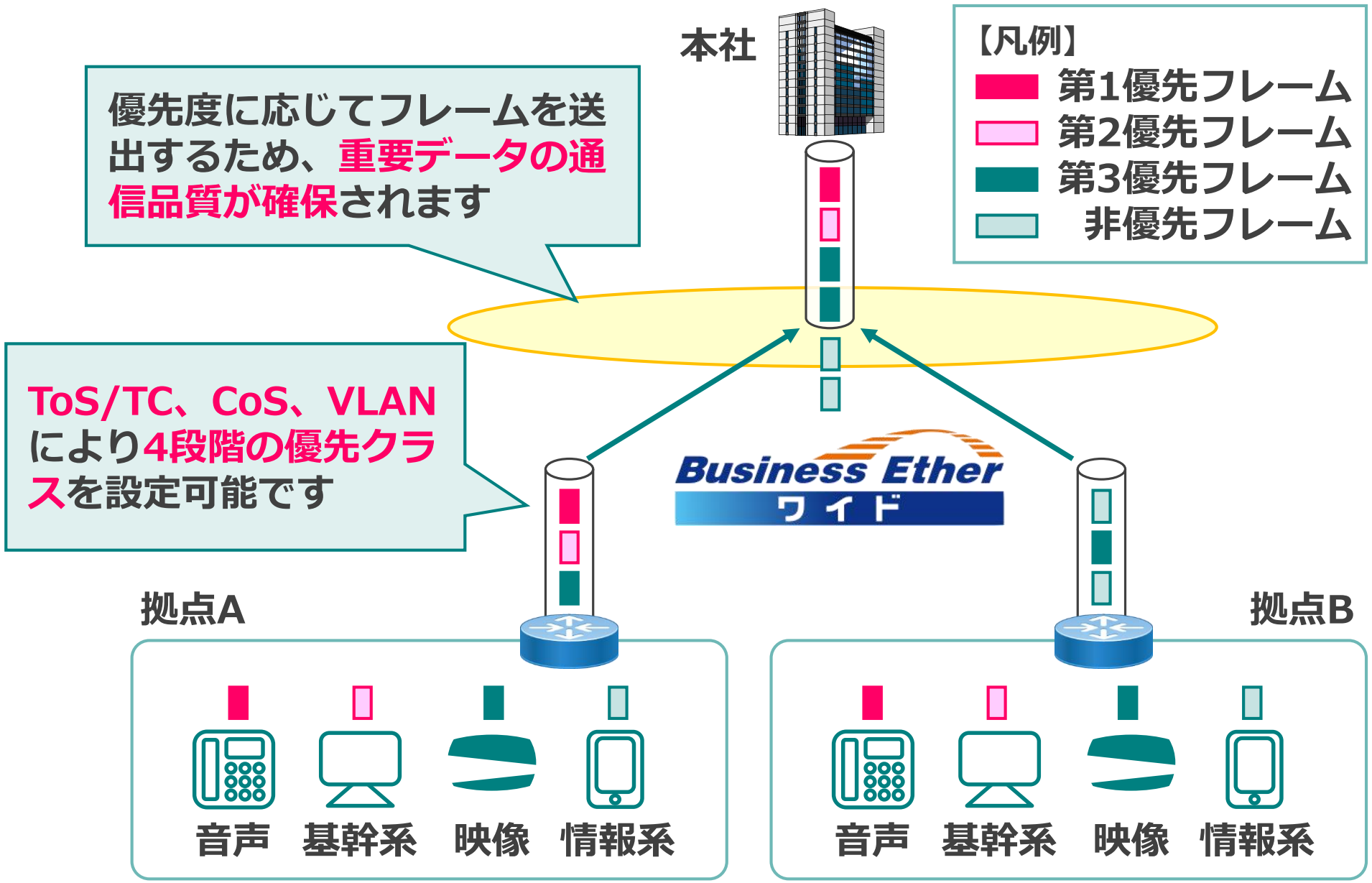
●サブグループ

同一通信グループ内において複数のグループを設定し、グループごとのセキュリティを確保することができるサービスです。

サブグループの特長
・利用目的ごとに複数のサブグループを設定可能
・サブグループ間の通信は非許容
・1本のアクセス回線に複数のサブグループを多重することが可能
（対応品目は10Mbit/s、100Mbit/s、1Gbit/s）
・1Mbit/s～1Gbit/sの全品目で利用可能
※同一通信グループ内のアクセス回線は全て最低1つのサブグループに属している必要があります。

各サブグループの識別は、IEEE802.1Q準拠のVLANタグのVLAN-IDを識別子として行います。VLAN-IDはNTT東日本から付与し、多重アクセス回線では指定されたVLAN-ID以外は通信できません。多重アクセス回線では、受信全てのフレームにVLANタグが付与されているため、VLANタグの識別可能なLAN機器を用意する必要があります。

●QoS制御機能

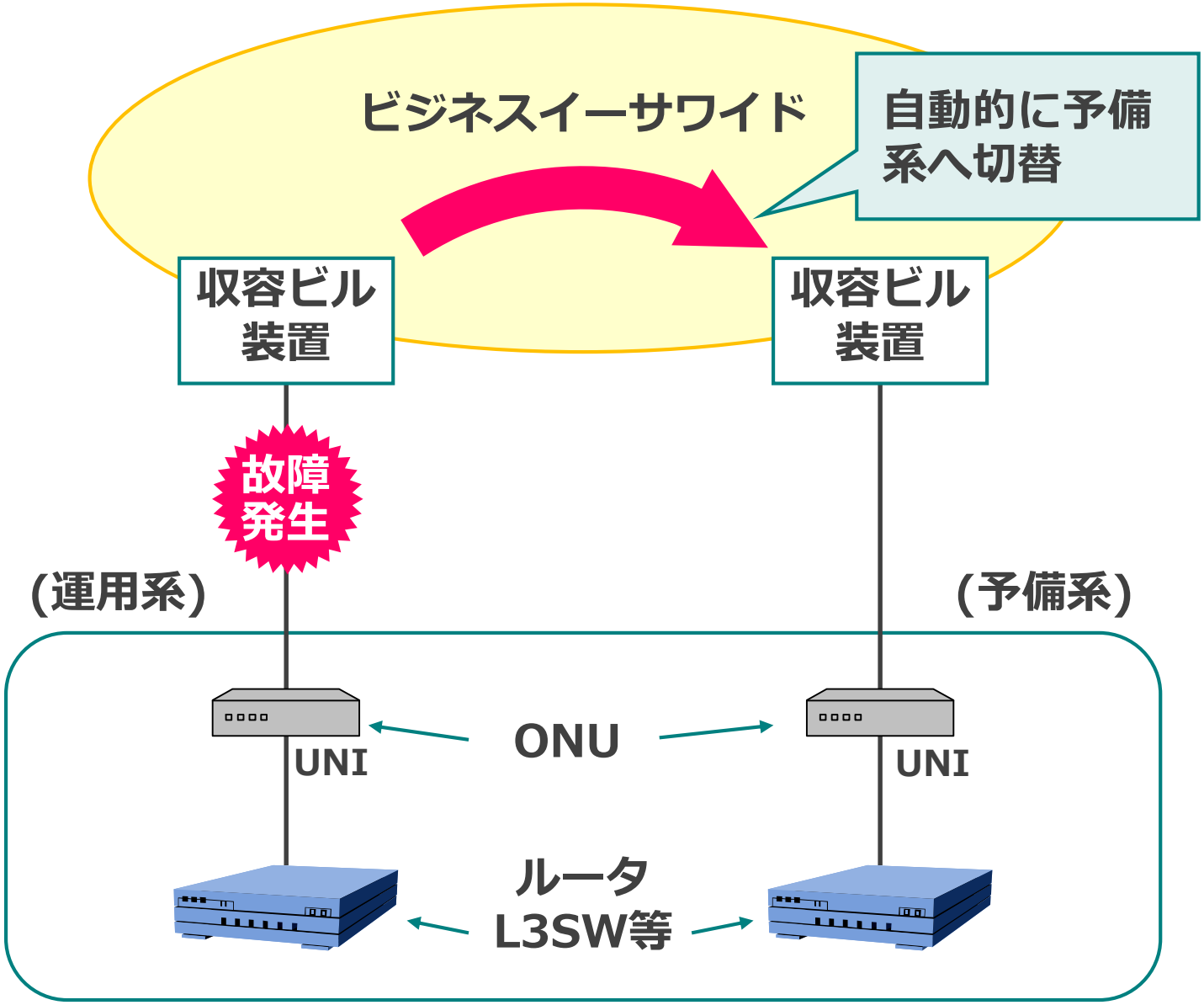

本社
【凡例】
第1優先フレーム
第2優先フレーム
第3優先フレーム
非優先フレーム
優先度に応じてフレームを送出するため、重要データの通信品質が確保されます
ToS/TC、CoS、VLANにより4段階の優先クラスを設定可能です
Business Ether
ワイド
拠点A
拠点B
音声
基幹系
映像
情報系
音声
基幹系
映像
情報系

●QoS制御機能

契約帯域を超えたトラフィックが流れた場合、お客様が指定した優先順位に従って、優先度の高いフレームを転送する機能です。
基幹系と情報系ネットワークの統合や、音声、映像データ等、複数のアプリケーションを同一ネットワークで利用したいお客様に最適です。

契約帯域を超えた場合、優先度の高いデータを送信するため、優先度の低い非優先のデータは破棄されます。

●デュアルアクセス概要


ビジネスイーサワイド
自動的に予備系へ切替
収容ビル装置
収容ビル装置
故障発生
(運用系)
(予備系)
UNI
ONU
UNI
ルータ
L3SW等

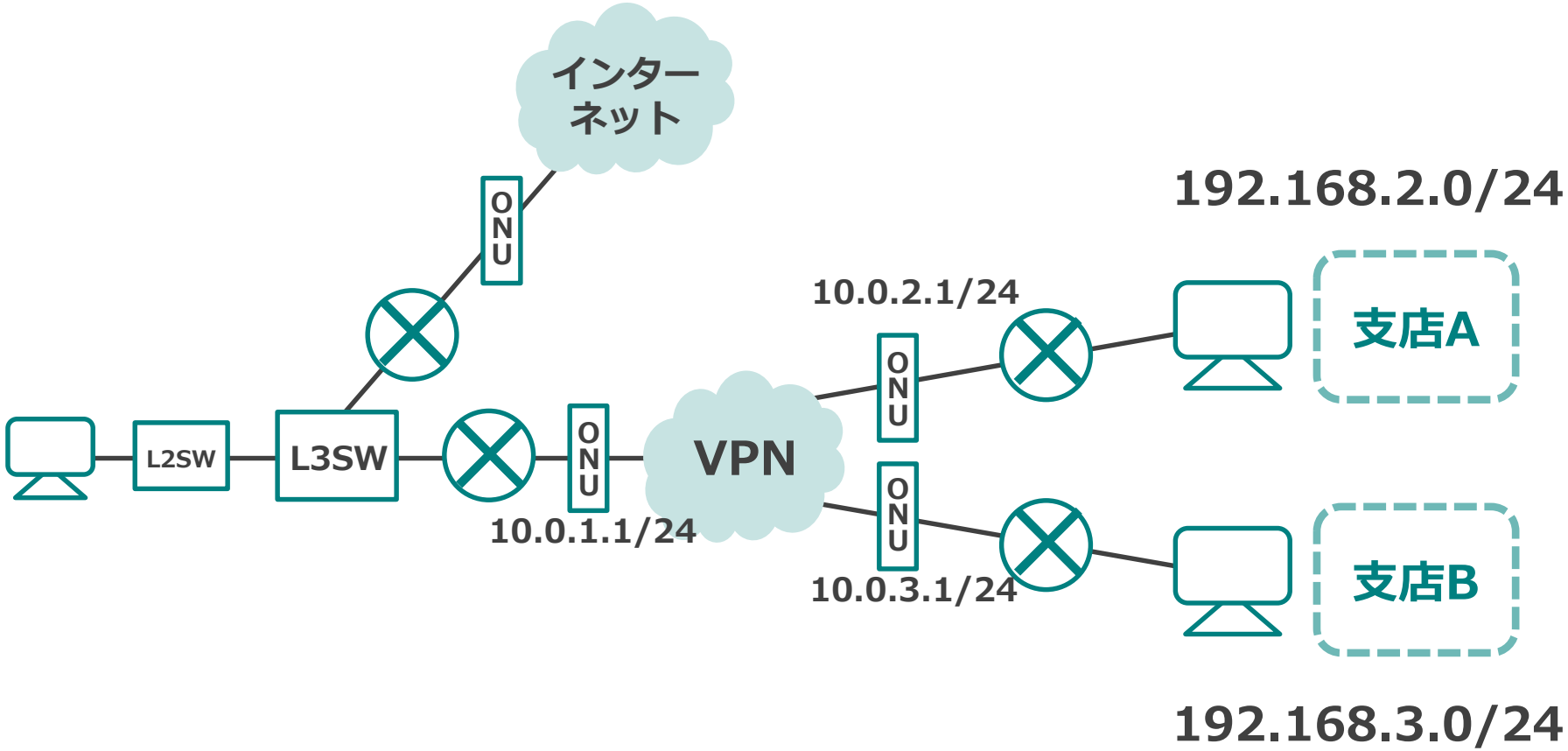
●デュアルアクセス概要

回線終端装置までの冗長化により、故障に強く高い信頼性を実現できます。デュアルアクセスは、中継区間（中継装置や中継回線等）だけでなく、アクセス回線の冗長化が可能なサービスです。基幹系・情報系ネットワークに信頼性と安定性を求めるお客様だけでなく、故障対策として信頼性の高いイーサネットサービスを利用したいというお客様に適したメニューです。

・万が一故障が発生した際には局内側で自動的に予備系回線へ切替ます
・予備系回線は局内側でブロックしており、同時に２回線は使用できません（ただし予備系ONUのONUランプはUPになります）
・10分未満という高基準の故障回復時間SLAを適用（シングル30分、デュアル10分）

よくあるWANの構成

●よくあるWANの構成（本社経由のインターネット接続の構成）

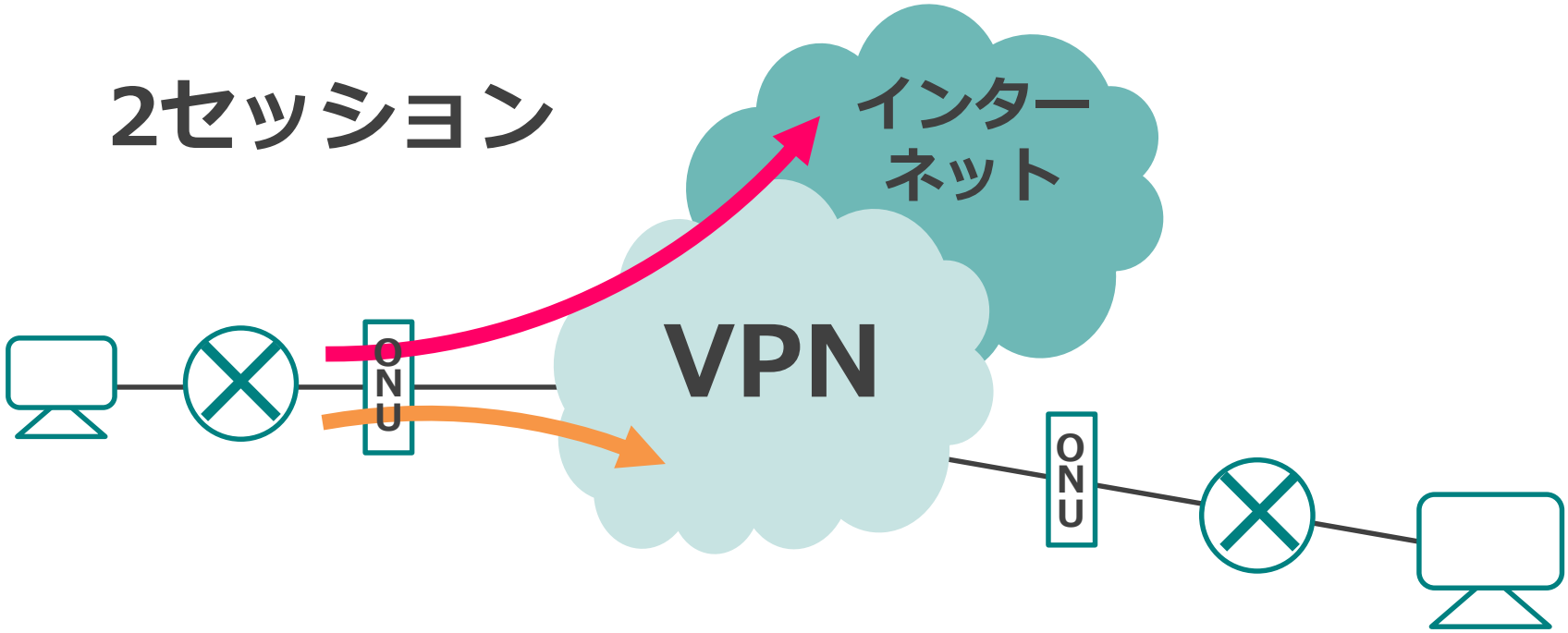


●よくあるWANの構成（本社経由のインターネット接続の構成）

・L3スイッチ
別々のセグメントを接続してセグメント間の通信を制御できる機器です。

・コアスイッチ
インターネット用ルータ、VPN用ルータ、異なる部署間のセグメントなどを収容し
企業ネットワークのバックボーンとして機能する機器です。

●よくあるWANの構成（2セッション構成）

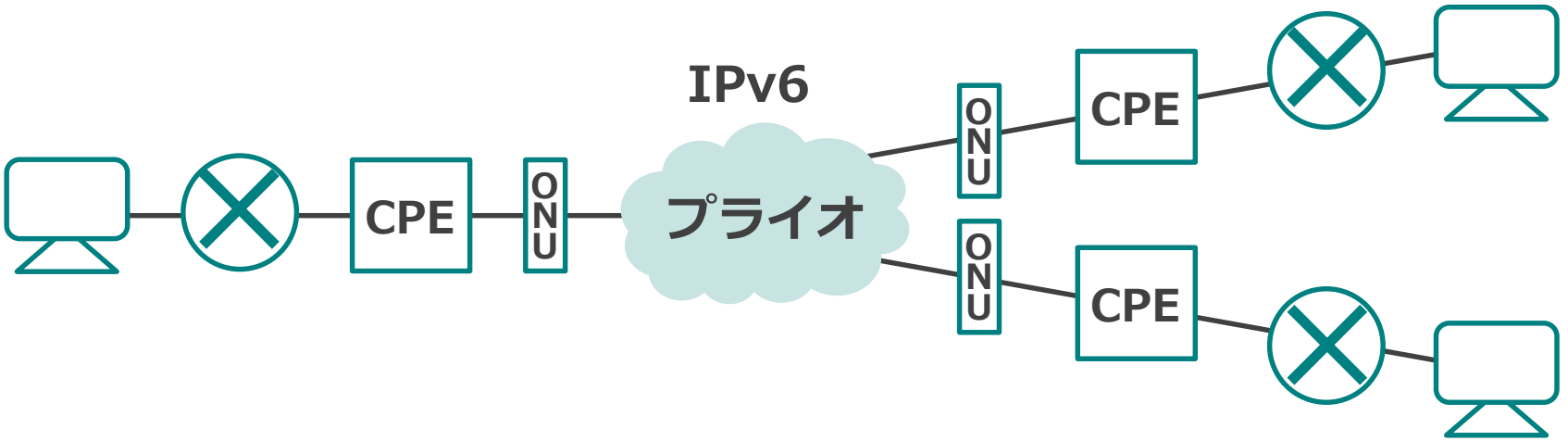


●よくあるWANの構成（2セッション構成）

・光アクセス回線のセッション数
NTT東日本のアクセス回線にはインターネットやVPN網と接続するための上限が設けられています。例：インターネット接続＋FVW＝2セッション

・セッションプラス（NTT東日本が提供する月額サービス）
セッション上限値を超えて利用したい場合は「セッションプラス」を契約することで上限を上げることができます。例：インターネット接続＋FVW＋カスコン＝ 3セッション

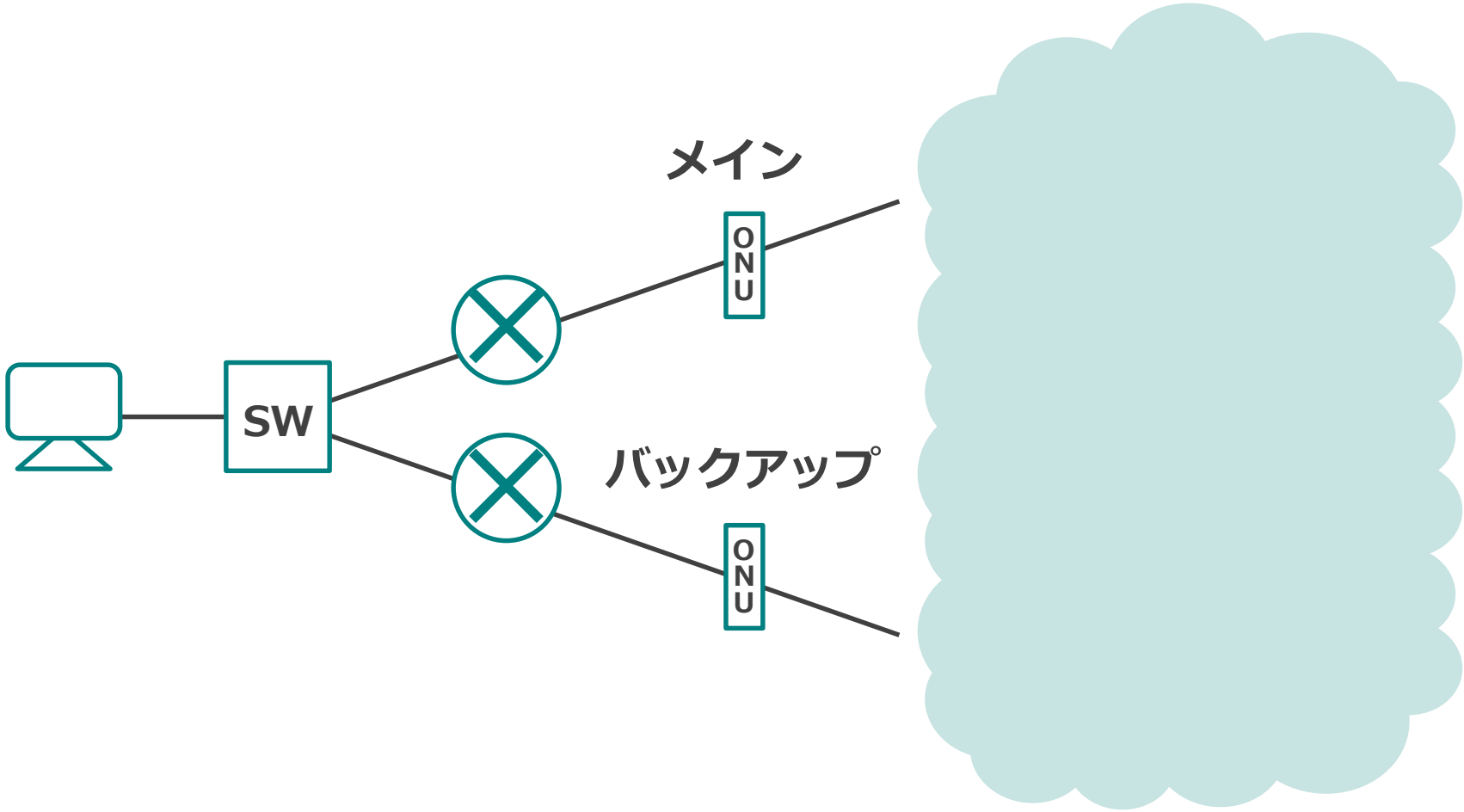
●よくあるWANの構成（フレッツVPNプライオの構成）



●よくあるWANの構成（フレッツVPNプライオの構成）

・CPE（Customer Premises Equipment　「顧客構内設備」　）
フレッツVPNプライオを利用する場合はONU配下にNTTのレンタルCPEを設置しなければ利用できません。
レンタルCPEでは、IPv4⇔IPv6変換やIPv6ルーティング等をおこなっています。

●よくあるWANの構成（バックアップのある構成）



●よくあるWANの構成（バックアップのある構成）

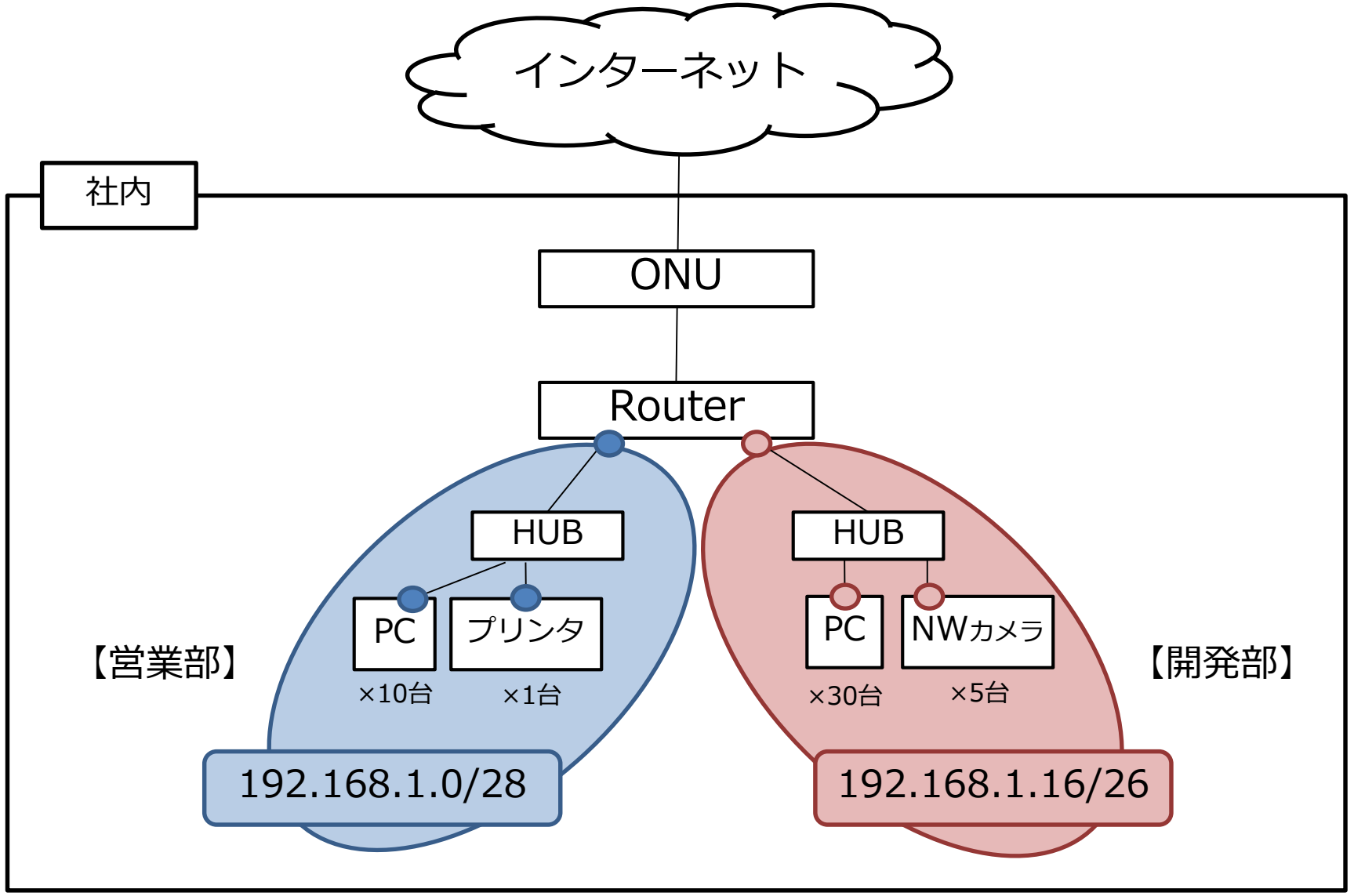
・切替方法
メインからバックアップに切り替える際は、切替動作を自動でおこなうプロトコルを検討することやユーザ影響度を把握しておく必要があります。

9章
総合実習

総合実習

構成図例

機器間接続の状態や端末台数、NWアドレスを記述します。



総合実習①

課題：各部署ごとのネットワークの範囲を求めて、構成図を作成してください。

【お客様基本情報】

- 事業内容：通販会社
- 拠点数　：1拠点
- 従業員数：210名
- 組織構成：営業部100名、サポート部60名、システム部25名、総務部25名

【条件】

- インターネットが利用できる構成とする
- システム部は無線接続でタブレット端末を利用できる構成とする
- システム部以外の全従業員に1人1台のPCを貸与します
- 部署毎にセグメントを分割する構成とする
- 使用するネットワークは192.168.1.0/24の範囲のみとする
- 必要なネットワーク機器等は想定して記入する

構成図

総合実習②

課題：各拠点、各部署のネットワークの範囲を求め、構成図を作成してください。

【お客様基本情報】

・事業内容：システムインテグレータ
・拠点数　：2拠点（本社1拠点、支社1拠点）
・従業員数：55名
・組織構成：本社(営業部20名、SE部20名、総務部5名)、支社(営業部5名、SE部5名)

【条件】

・各拠点はインターネットが利用できる構成とする
・総務部にはFS(ファイルサーバ)を1台設置し、全ての従業員がアクセスできる環境とする
・本社/支社の部署は部署毎にセグメント分割をおこないます
・本社で使用するネットワークは192.168.1.0/24の範囲のみとする
・支社で使用するネットワークは192.168.2.0/24の範囲のみとする
・全従業員に1人1台のPCを貸与します
・必要なネットワーク機器等は想定して記入する

構成図

総合実習②

課題：各拠点、各部署のネットワークの範囲を求め、構成図を作成してください。

【お客様基本情報】

・事業内容：システムインテグレータ
・拠点数　：2拠点（本社1拠点、支社1拠点）
・従業員数：55名
・組織構成：本社(営業部20名、SE部20名、総務部5名)、支社(営業部5名、SE部5名)

【条件】

・各拠点はインターネットが利用できる構成とする
・総務部にはFS(ファイルサーバ)を1台設置し、全ての従業員がアクセスできる環境とする
・本社/支社の部署は部署毎にセグメント分割をおこないます
・本社で使用するネットワークは192.168.1.0/24の範囲のみとする
・支社で使用するネットワークは192.168.2.0/24の範囲のみとする
・全従業員に1人1台のPCを貸与します
・必要なネットワーク機器等は想定して記入する

構成図