初級レベル研修

ルーター基礎セミナー

オンラインセミナー
ウェビナー

一般社団法人　情報通信設備協会

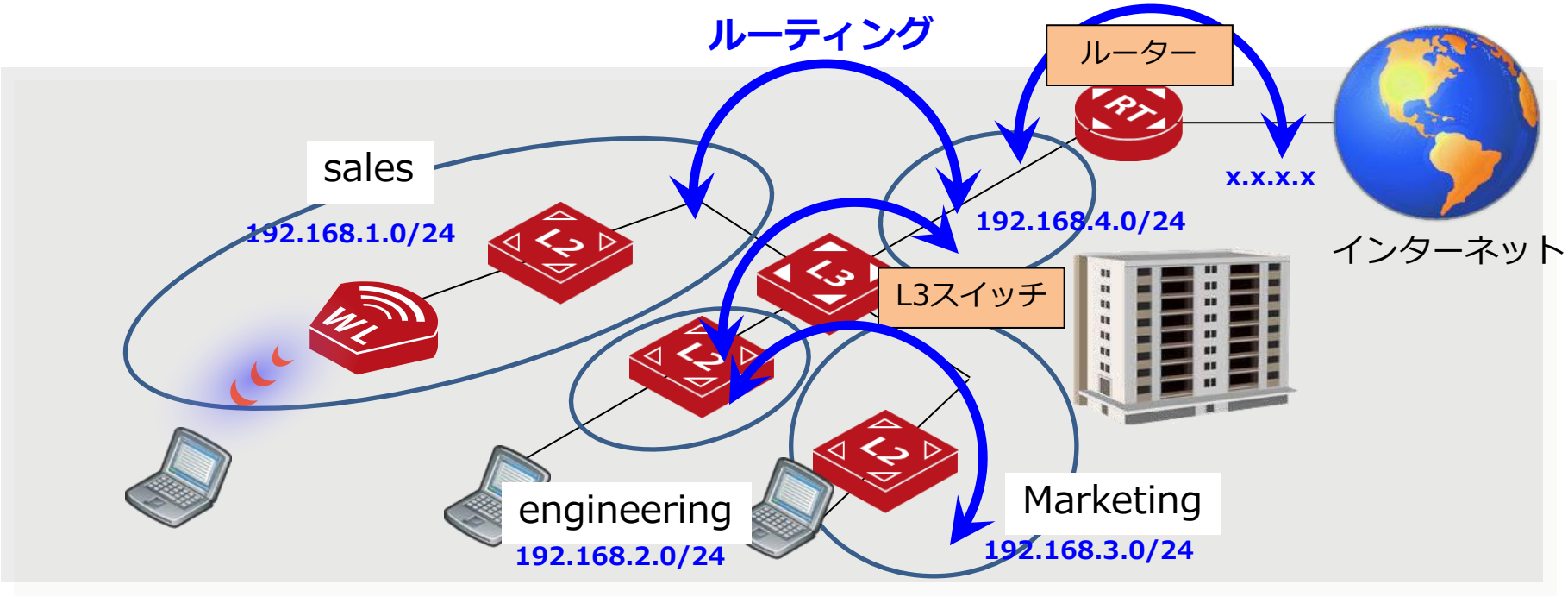
V3.0

目次

①ルーティングの役割・種類

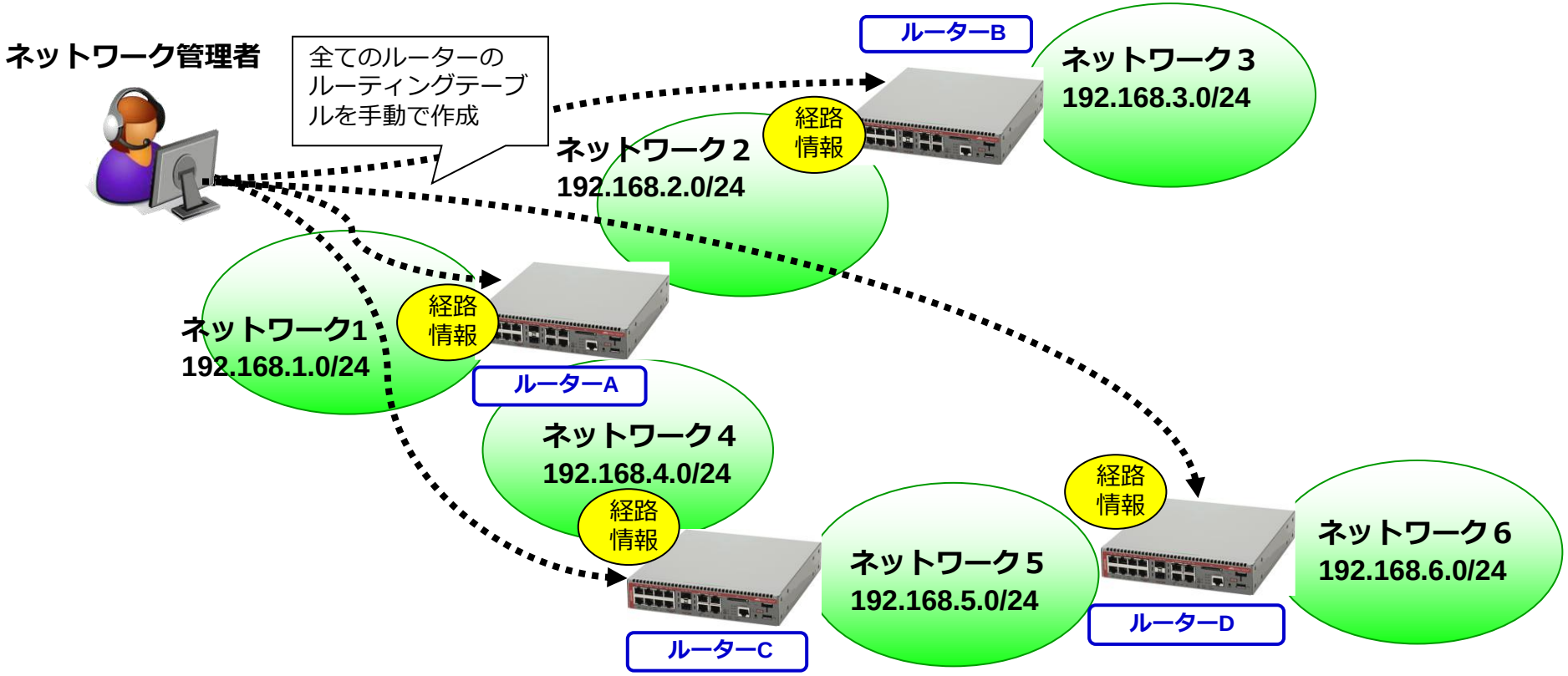
ルーティングとは

- ルーターやレイヤー3スイッチがパケットをネットワークを越えて目的地に正しく届けるための経路を選定・転送する機能です。
- スイッチがMACアドレスの情報に基づきブロードキャストドメイン内（サブネット）での通信を実現にするのに対し、ルーターやレイヤー3スイッチはIPアドレスを理解することにより異なるネットワーク間の通信を実現します。



スタティックルーティング

- ルーティングテーブルの内容をネットワーク管理者が構築する方法です。ネットワーク上の全ルーター（L3スイッチ）に経路情報を1つずつ登録します。
- 「経路情報の管理がしやすい」、「ルーティング機器への負担が少なくダイナミックルーティングに比べネットワークトラフィックが低くなる」、というメリットはありますが、全ルーターに経路情報を手動で設定する必要があるため、「手間がかかる」、「障害発生時には経路の再設定が必要」、などのデメリットもあります。



スタティックルーティングによる構築

- 下記ネットワーク構成における各ルーターのルーティングテーブル登録情報を示します。登録するネットワーク情報は、直接接続されていない（=他ルーターへの転送が必要な）ネットワーク情報（青字の部分）で、通常1つのコマンドで1つのネットワーク情報を登録します。
- NextHopとは、ルーターが目的ネットワークにパケットを送るために次に渡すルーターのインターフェースアドレスです。なお、インターフェースアドレスでなく、パケットを転送するルーターのインターフェース名を指定する場合もあります。

ルーターAのルーティングテーブル

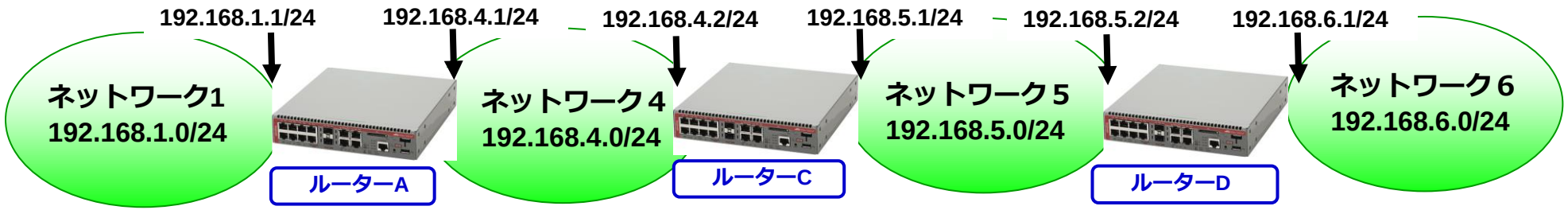
Network	NextHop
192.168.1.0/24	無
192.168.4.0/24	無
192.168.5.0/24	192.168.4.2
192.168.6.0/24	192.168.4.2

ルーターCのルーティングテーブル

Network	NextHop
192.168.1.0/24	192.168.4.1
192.168.4.0/24	無
192.168.5.0/24	無
192.168.6.0/24	192.168.5.2

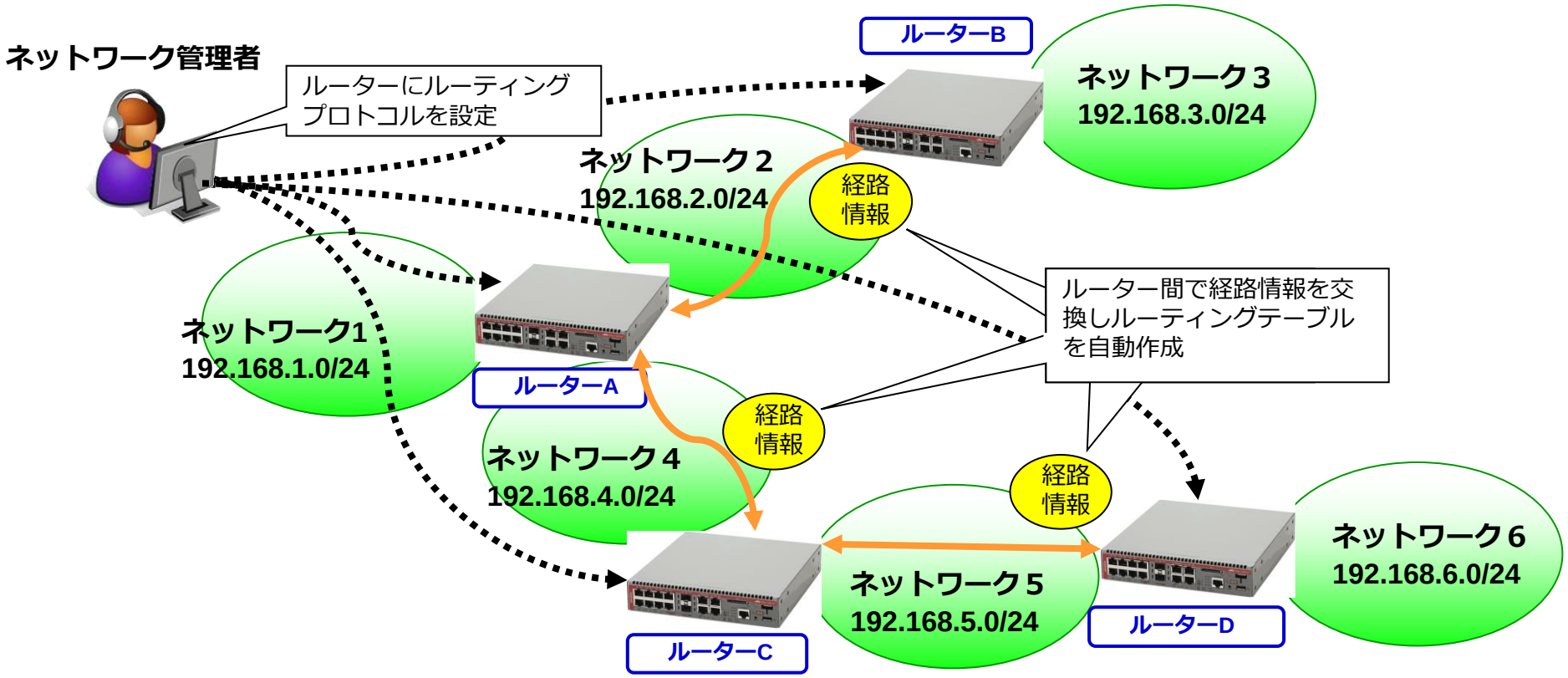
ルーターDのルーティングテーブル

Network	NextHop
192.168.1.0/24	192.168.5.1
192.168.4.0/24	192.168.5.1
192.168.5.0/24	無
192.168.6.0/24	無



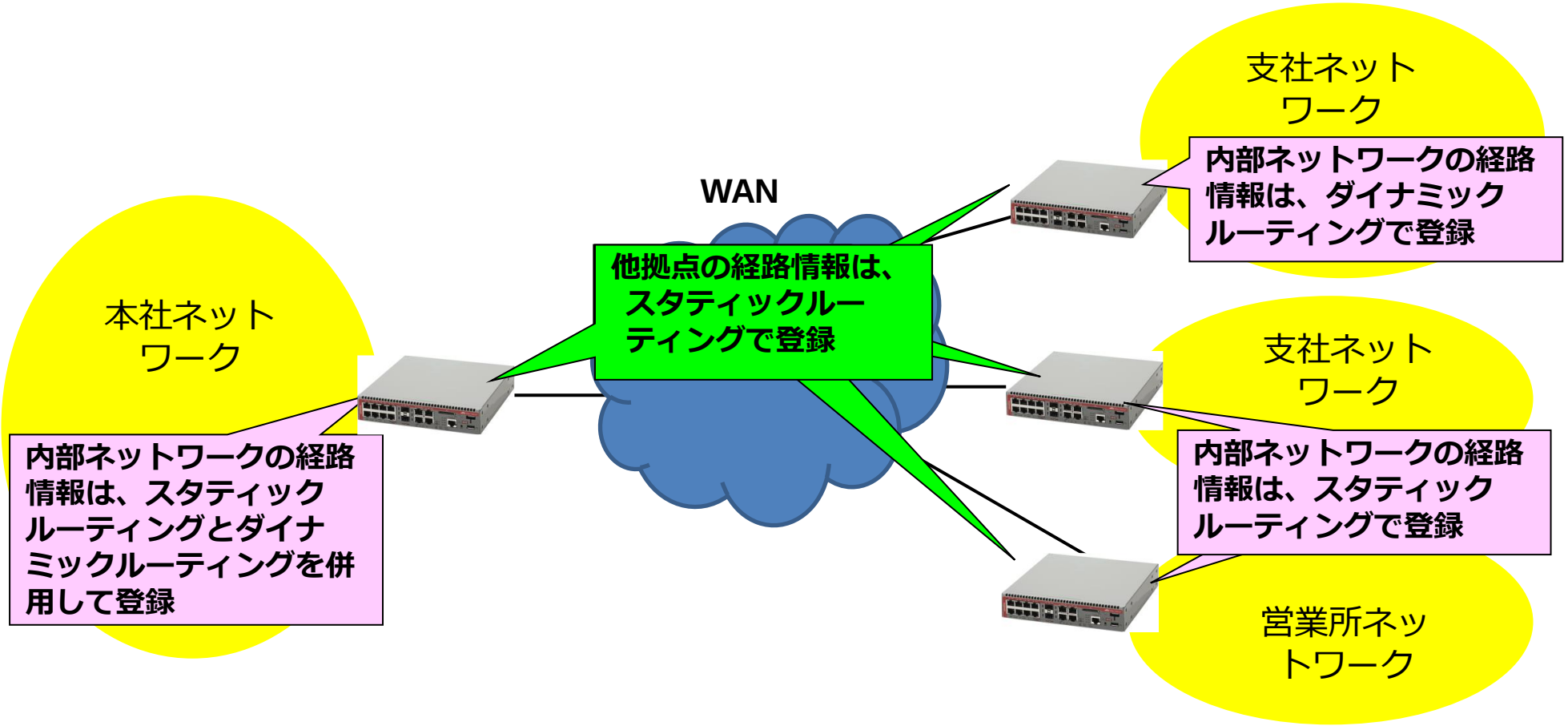
ダイナミックルーティング

- 連結されるネットワークの数が多い大規模ネットワークでは、手動でネットワーク情報を設定するのは工数がかかります。
- そこで、ルーター（L3スイッチ）でルーティングプロトコルを動作させて自動的にルーティングテーブルを作成します。この方法をダイナミックルーティングと呼びます。



ルーターにおける経路情報の登録方法

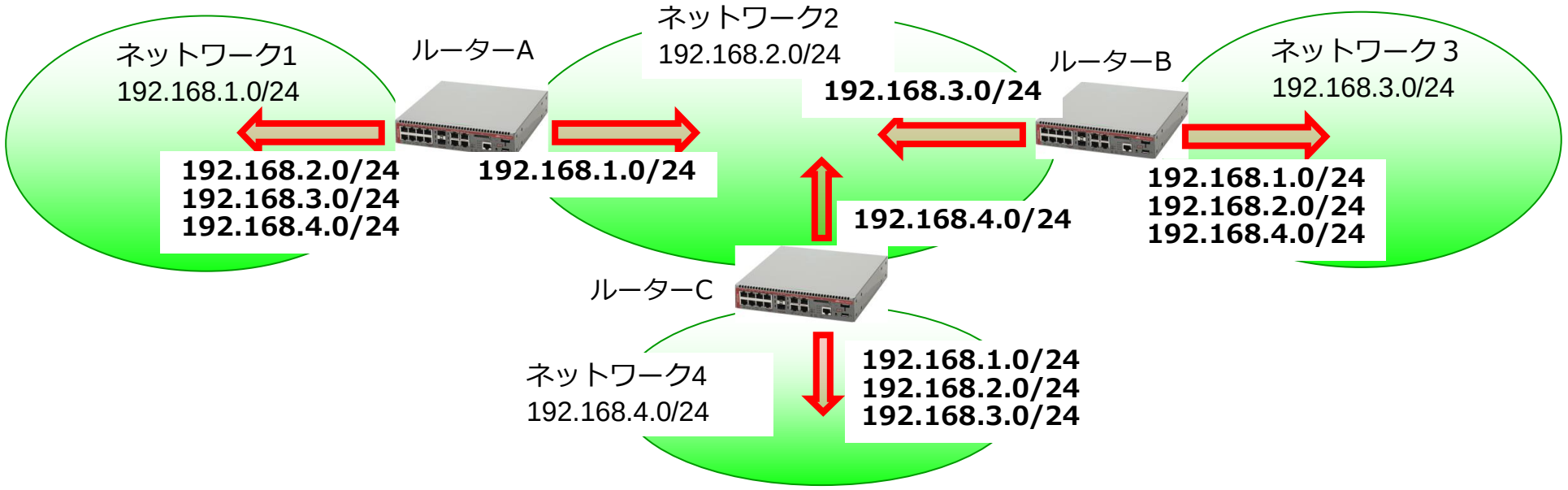
– ネットワーク構築において、主に外部ネットワークと内部ネットワークを接続する位置に設置されるルーターでは、外部ネットワーク及び他拠点の経路情報はスタティックルーティングで登録し、内部ネットワークの経路情報はスタティックルーティングもしくはダイナミックルーティングで登録します。



②RIP

RIP(Routing Information Protocol)

- ルーティングテーブルの情報を定期的（30秒に1回）に隣接ルーターに通知します。RIPv1ではブロードキャストアドレスを使用し、RIPv2ではマルチキャストアドレス（224.0.0.9）を使用します（現在の主流はRIPv2のため、以降RIPv2の内容をベースに記載します）。
- Metric（経路選択の指標）はホップ数（経由するルーティング機器の数）を使用。ホップ数の上限は15のため、小・中規模のネットワーク向けルーティングプロトコル
- 経路計算アルゴリズムが簡素なためルーターにかかる負荷が少なく、処理能力の低いルーターにも実装可能です。また、設定も容易です。



ルーティングテーブル作成の流れ（1）

- 自身のインターフェースアドレスのネットワークアドレスをルーティングテーブルに登録し、その情報を配信します。

ルーターAのルーティングテーブル

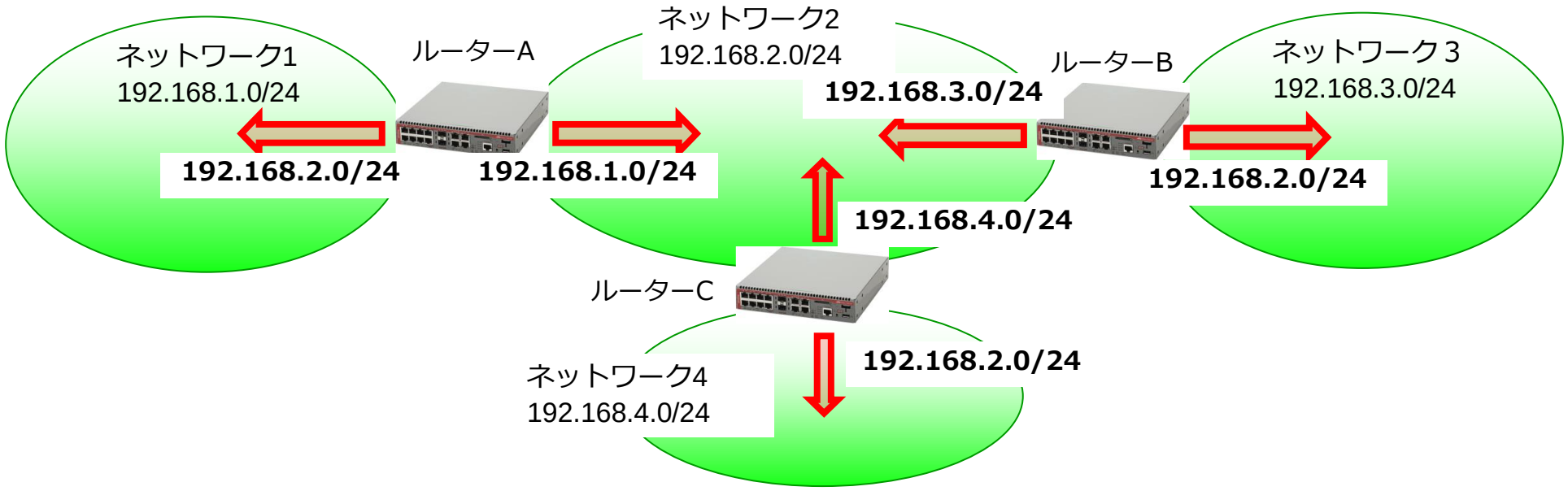
Network	Metric	NextHop
192.168.1.0/24	直接	無
192.168.2.0/24	直接	無

ルーターCのルーティングテーブル

Network	Metric	NextHop
192.168.2.0/24	直接	無
192.168.4.0/24	直接	無

ルーターBのルーティングテーブル

Network	Metric	NextHop
192.168.2.0/24	直接	無
192.168.3.0/24	直接	無



ルーティングテーブル作成の流れ（2）

- ルーティングテーブル未登録の経路情報を他ルーターから受信した場合、ホップ数を1プラスしその経路情報をルーティングテーブルに登録します。
- ルーターが直接接続のネットワーク情報をホップ数0（ゼロ）で配信するか、ホップ数1で配信するかはベンダー機器により異なります。ここでは、ホップ数1で配信した場合の流れを記載します。※1

ルーターAのルーティングテーブル

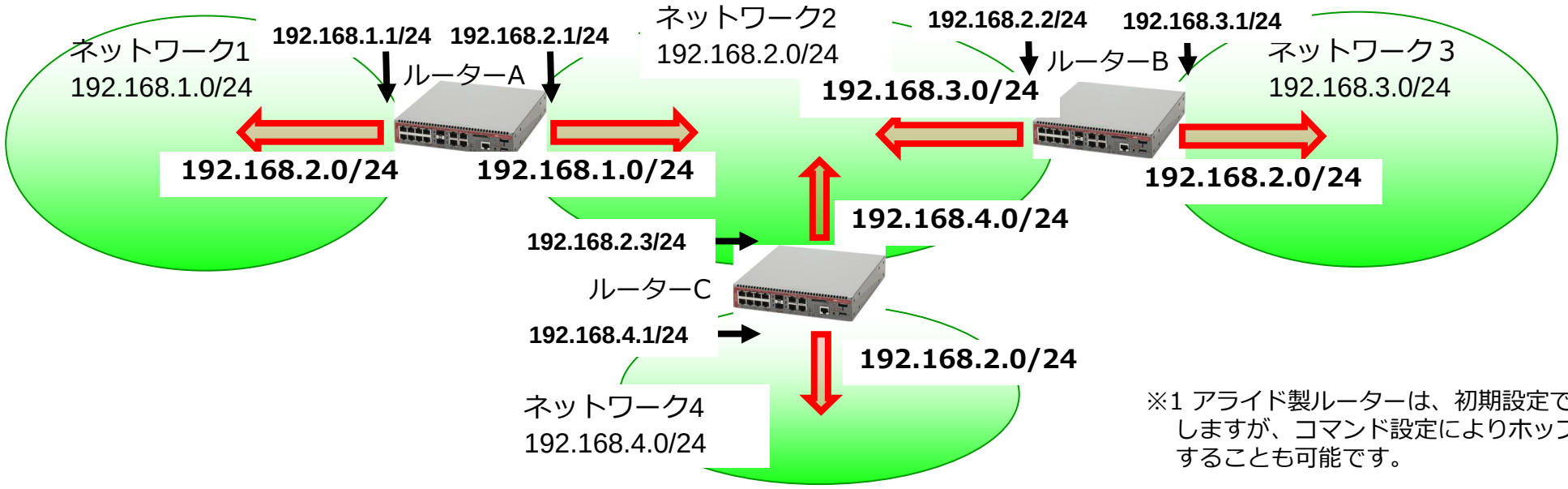
Network	Metric	NextHop
192.168.1.0/24	直接	無
192.168.2.0/24	直接	無
192.168.3.0/24	2	192.168.2.2
192.168.4.0/24	2	192.168.2.3

ルーターCのルーティングテーブル

Network	Metric	NextHop
192.168.2.0/24	直接	無
192.168.4.0/24	直接	無
192.168.1.0/24	2	192.168.2.1
192.168.3.0/24	2	192.168.2.2

ルーターBのルーティングテーブル

Network	Metric	NextHop
192.168.2.0/24	直接	無
192.168.3.0/24	直接	無
192.168.1.0/24	2	192.168.2.1
192.168.4.0/24	2	192.168.2.3



※1 アライド製ルーターは、初期設定ではホップ数1で配信しますが、コマンド設定によりホップ数0（ゼロ）で配信することも可能です。

ルーティングテーブル作成の流れ（3）

- 各ルーターは、新しく登録した経路情報を追加して経路情報を配信します。RIPの各ルーターは隣接ルーターからの経路情報のみでルーティングテーブルを作成します。そのため、スプリットホライズンなどのルーティングループ防止機能があります。
  - スプリットホライズンとは、隣接ルーターから受信した経路情報は受信したインターフェースに送信しない機能です。

ルーターAのルーティングテーブル

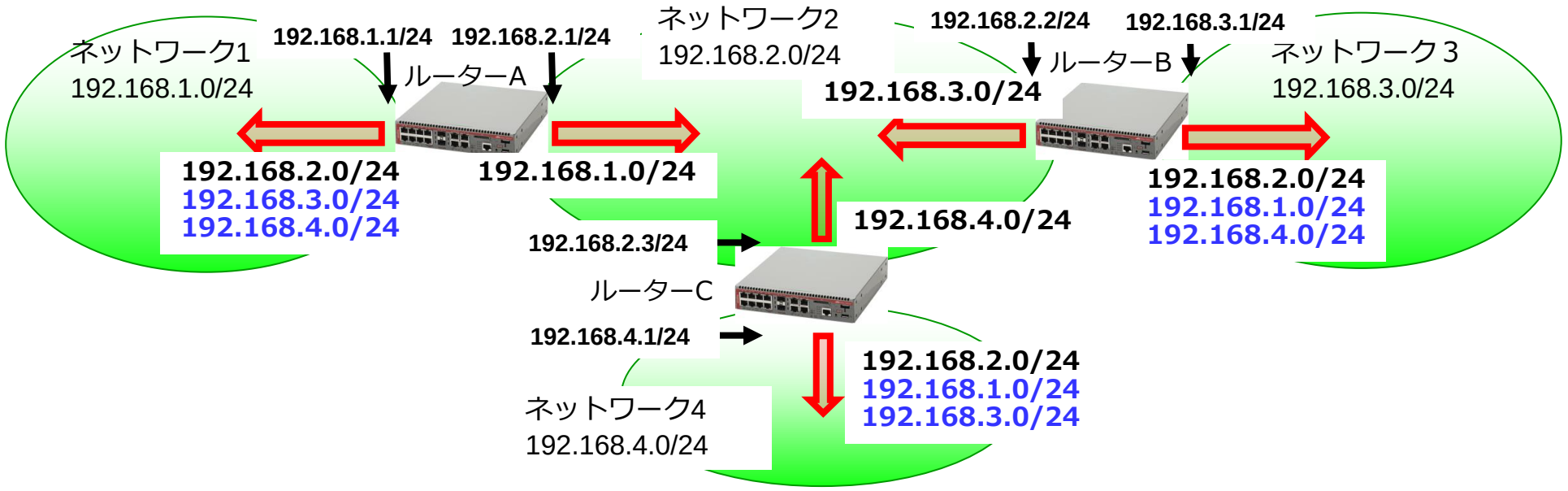
Network	Metric	NextHop
192.168.1.0/24	直接	無
192.168.2.0/24	直接	無
192.168.3.0/24	2	192.168.2.2
192.168.4.0/24	2	192.168.2.3

ルーターCのルーティングテーブル

Network	Metric	NextHop
192.168.2.0/24	直接	無
192.168.4.0/24	直接	無
192.168.1.0/24	2	192.168.2.1
192.168.3.0/24	2	192.168.2.2

ルーターBのルーティングテーブル

Network	Metric	NextHop
192.168.2.0/24	直接	無
192.168.3.0/24	直接	無
192.168.1.0/24	2	192.168.2.1
192.168.4.0/24	2	192.168.2.3



RIPルーティングテーブル（例）

- RIPのルーティングテーブルは以下になります。各項目の意味は以下の通りです。

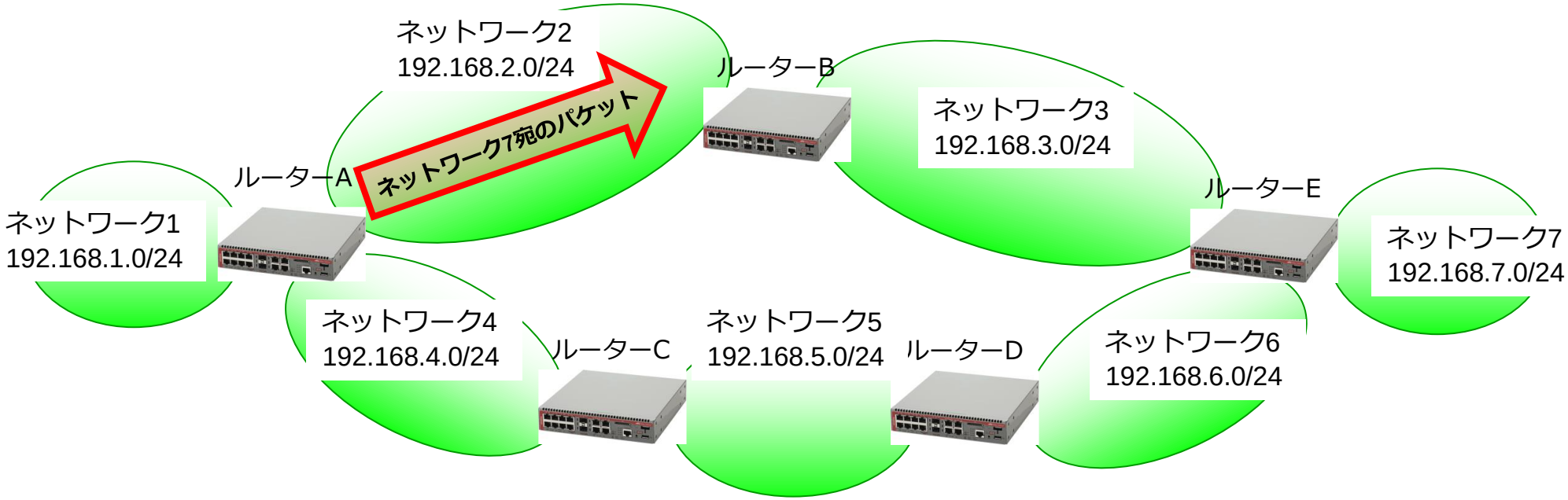
R 10.10.10.0/24 172.17.10.2 3 172.17.10.2 vlan20 02:56
① ② ③ ④ ⑤ ⑥ ⑦

①経路情報の取得方法： RIPはRです。RcはRIPが動作している直接接続のネットワークアドレス
②ネットワークアドレス及びサブネットマスク長 ③NextHop： 次に転送するルーターのアドレス
④Metric： RIPはホップ数 ⑤経路情報を送ってきたネットワーク機器のIPアドレス
⑥出力インターフェース： パケットを出力するインターフェース ⑦経路情報が登録されてからの経過時間

```
awplus> show ip rip ↓

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP

   Network            Next Hop         Metric From            If      Time
R  10.10.10.0/24      172.17.10.2           3 172.17.10.2     vlan20  02:56
R  10.10.20.0/24      192.168.10.2          4 192.168.10.2    vlan10  02:47
                      172.17.10.2           4 172.17.10.2     vlan20  02:56
R  172.16.10.0/24     192.168.10.3          2 192.168.10.3    vlan10  02:50
R  172.16.20.0/24     192.168.10.3          3 192.168.10.3    vlan10  02:50
Rc 172.17.10.0/24                           1                 vlan20
R  172.17.20.0/24     192.168.10.2          2 192.168.10.2    vlan10  02:47
R  172.17.30.0/24     172.17.10.2           2 172.17.10.2     vlan20  02:56
R  172.17.40.0/24     192.168.10.2          3 192.168.10.2    vlan10  02:47
                      172.17.10.2           3 172.17.10.2     vlan20  02:56
R  172.17.50.0/24     172.17.10.2           2 172.17.10.2     vlan20  02:56
Rc 192.168.10.0/24                          1                 vlan10
```

複数経路時の選択

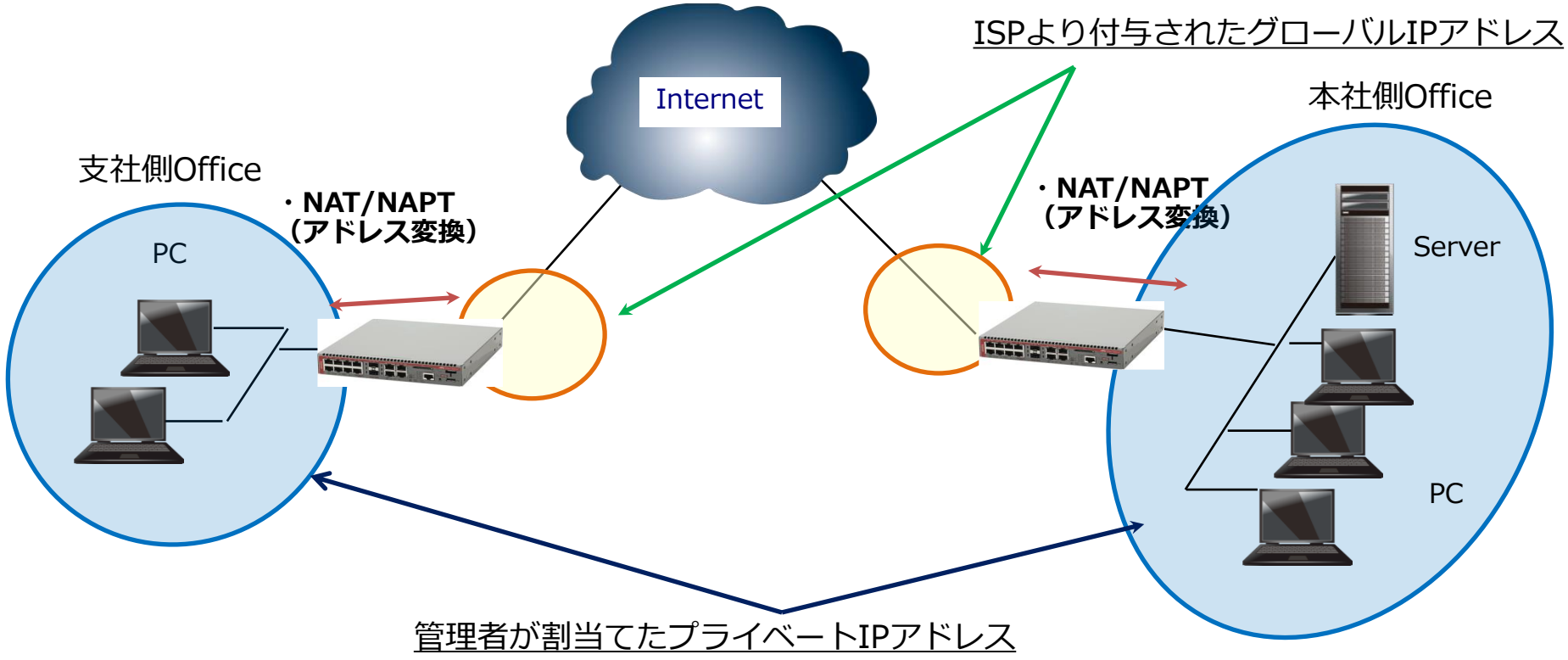
- 目的ネットワークへの経路が複数存在する場合の判断基準は以下になります。
  - Metric（ホップ数）が異なる経路が複数存在する場合、Metricの小さい経路を選択（回線速度は考慮されない）
  - Metricが同じ経路が複数存在する場合はベンダー機器によって動作が異なります。RFC1058に準拠している機器では先に受信した経路情報を使用しますが、複数経路に交互にパケットを転送するベンダー機器もあります。
- 以下の図はルーターAから見て、ネットワーク7宛の経路が2つ存在します。この場合、ルーターAはネットワーク7宛のパケットをMetric(経由するルーターの数)が少ないネットワーク2の経路に転送します。



③NAT

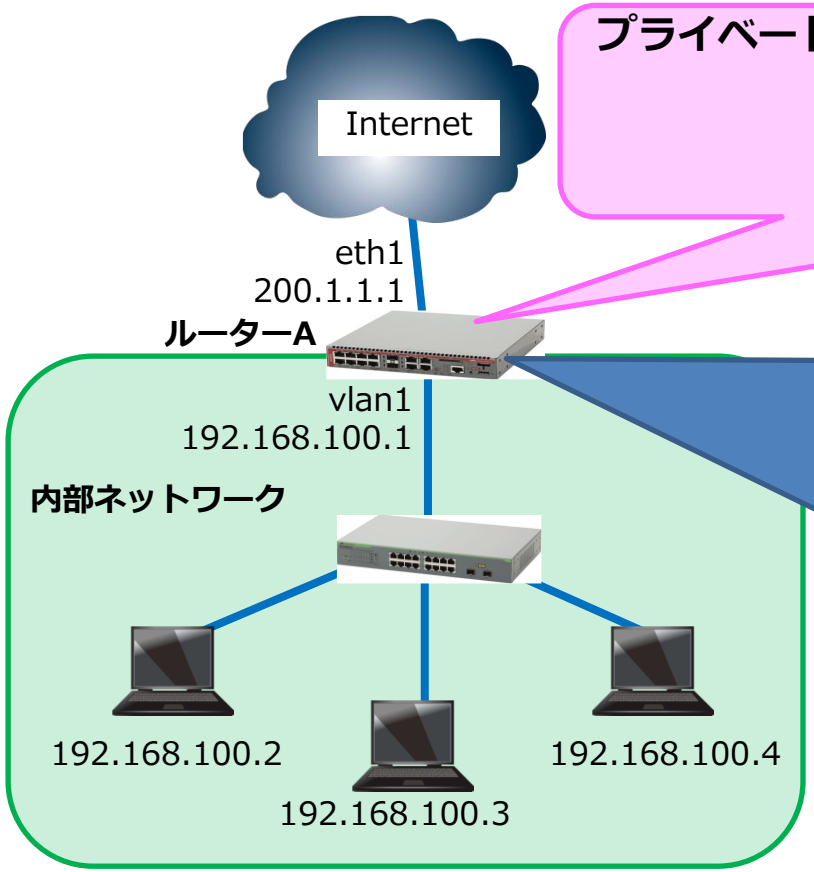
NAT(Network Address Translation)とは

- 外部アドレス(グローバルIPアドレス)と内部アドレス(プライベートIPアドレス)のアドレス変換技術です。
- Internet宛パケットでは、送信元IPアドレスがプライベートIPアドレスからグローバルIPアドレスへ変換され、内部ネットワーク宛パケットでは、宛先IPアドレスがグローバルIPアドレスからプライベートIPアドレスへ変換されます。
- プライベートIPアドレスを使用している内部ネットワーク環境のホストから、インターネットのような外部ネットワークにアクセスするために利用します。内部ネットワーク上のホストのIPアドレスを外部ネットワークに公開しないため、不正アクセスのリスクを低減するメリットもあります。



スタティックNAT

- プライベートIPアドレスとグローバルIPアドレスの1対1の変換を、ネットワーク管理者が手動設定で行います。
- 常にプライベートIPアドレスをグローバルIPアドレスに1対1で変換するため管理が容易というメリットはありますが、複数の端末から外部ホストに同時接続する場合は複数のグローバルIPアドレスが必要になるというデメリットがあります。



プライベートIPアドレスとグローバルIPアドレスの対応ルールを設定
192.168.100.2 ⇒ 200.1.1.2
192.168.100.3 ⇒ 200.1.1.3
192.168.100.4 ⇒ 200.1.1.4

NATテーブルに、通信時変換されたアドレス情報を保存

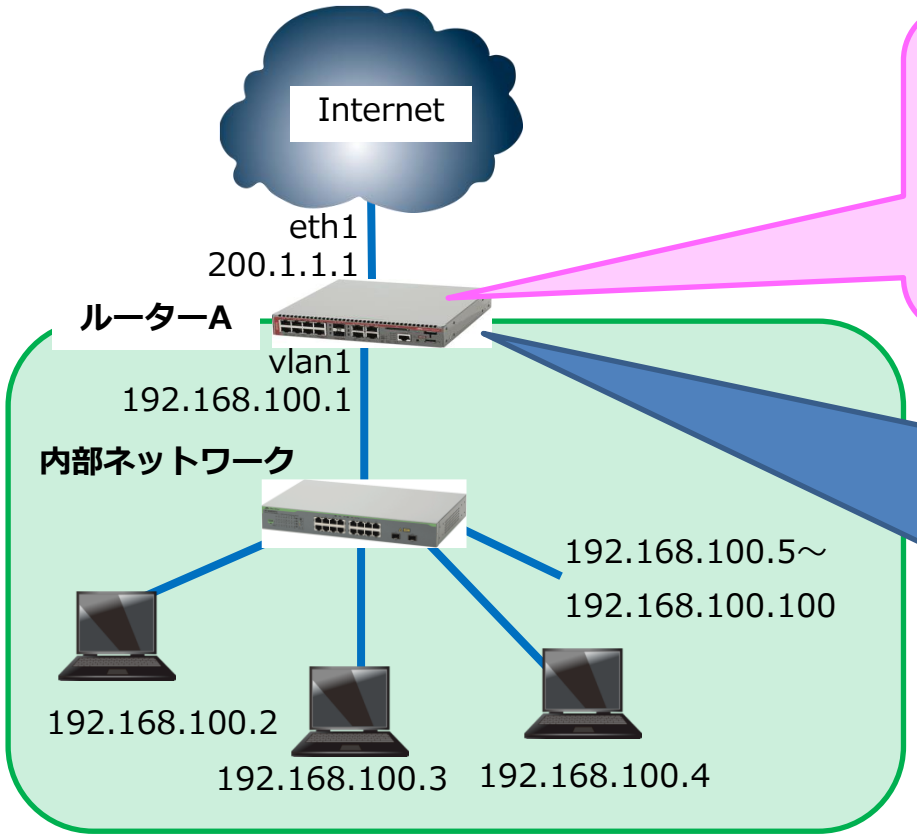
ルーターAのNATテーブル	
プライベートIPアドレス	グローバルIPアドレス
192.168.100.2	200.1.1.2
192.168.100.3	200.1.1.3
192.168.100.4	200.1.1.4

応答パケットはこの情報を元に、元のアドレスに変換される

（例）内部ネットワークからInternet宛パケットの送信元アドレスを192.168.100.2 から 200.1.1.2 へ変換後その情報をNATテーブルに保存します。Internetから内部ネットワーク宛応答パケットの宛先IPアドレスは、保存した情報を元に200.1.1.2 から 192.168.100.2 へ変換されます

ダイナミックNAT

- 複数のプライベートIPアドレスから、複数のグローバルIPアドレスへの多対多の変換を行います。
- 予め「どの範囲のプライベートIPアドレスをどの範囲のグローバルIPアドレスに変換する」という設定を行うことで、ルーターは指定されたプライベートIPアドレスのホストから送られてきたパケットを、空いているグローバルIPアドレスに変換して外部ネットワークへ転送します（グローバルIPアドレスは固定されません）。



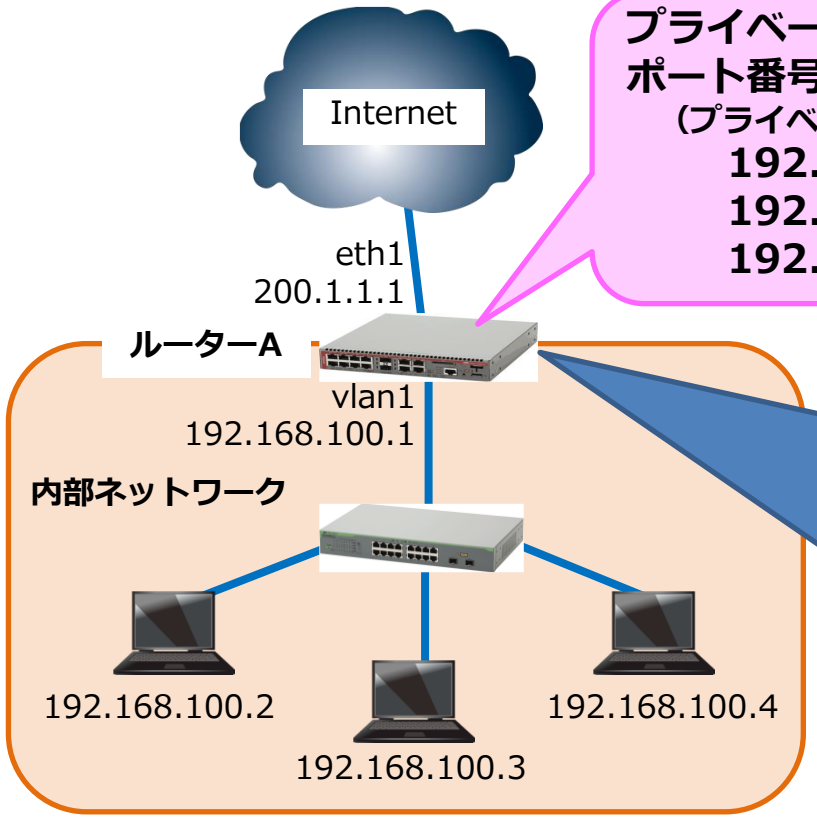
対象となるプライベートIPアドレスと変換するグローバルIPアドレスの対応ルールを設定
（変換対象のプライベートIPアドレス）：
192.168.100.2 ～ 192.168.100.100
（変換するグローバルIPアドレス）：
200.1.1.2 ～ 200.1.1.100

ルーターAは、設定されたグローバルIPアドレスの中で、空いている（=現在通信で使用されていない）グローバルIPアドレスへ変換します

ルーターAのNATテーブル	
プライベートIPアドレス	グローバルIPアドレス
192.168.100.2	200.1.1.30
192.168.100.3	200.1.1.2
192.168.100.4	200.1.1.100

スタティックNAPT

- グローバルIPアドレス＋TCP/UDPポート番号とプライベートIPアドレス＋TCP/UDPポート番号の1対1の変換を、ネットワーク管理者が手動設定で行います。
- 端末数分のグローバルIPアドレスを用意する必要がないというメリットはありますが、ポートとIPアドレスの組み合わせを固定的に行うため、アプリケーションによっては対応できなかったり、ポートの衝突が発生しやすいというデメリットがあります。



プライベートIPアドレス、およびグローバルIPアドレスとポート番号の対応ルールを設定

（プライベートIPアドレス）		（グローバルIPアドレス）	（ポート番号）
192.168.100.2	⇒	200.1.1.3	60000
192.168.100.3	⇒	200.1.1.3	61500
192.168.100.4	⇒	200.1.1.3	62000

ルーターAは設定されたルールに従い、IPアドレスとポート番号を変換します。各端末との通信は、変換後のポート番号で識別します

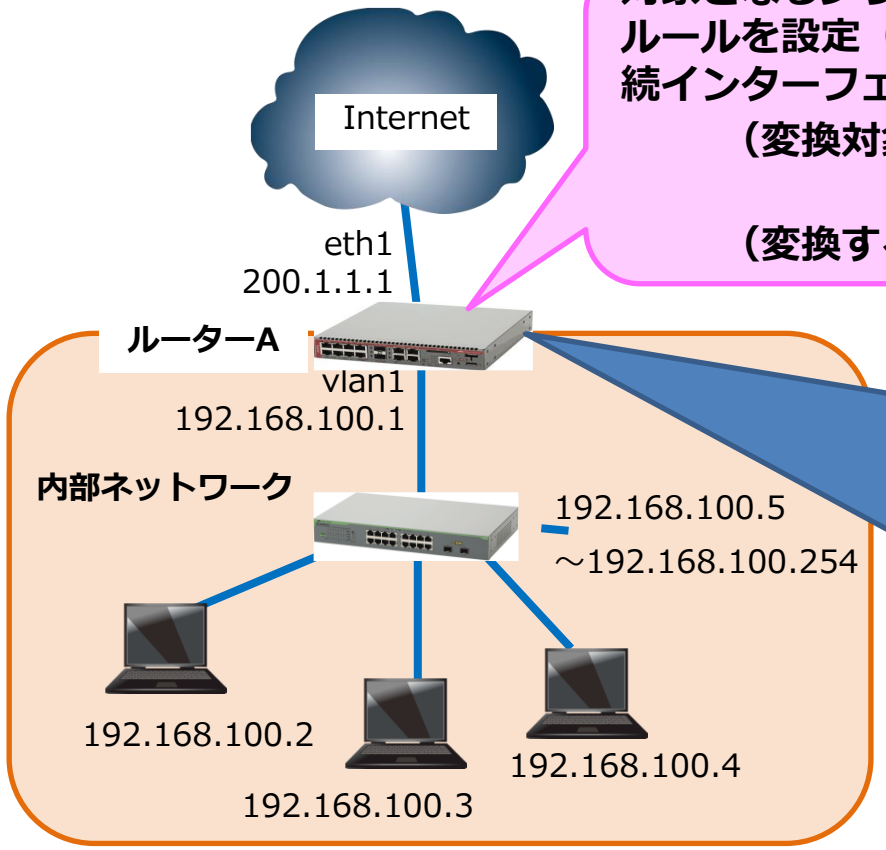
ルーターAのNATテーブル

プライベートIPアドレス	変換前ポート番号	グローバルIPアドレス	変換後ポート番号
192.168.100.2	49200	200.1.1.3	60000
192.168.100.3	49500	200.1.1.3	61500
192.168.100.4	49700	200.1.1.3	62000

※ NAPTはIPマスカレードとも呼びます。

ダイナミックNAPT

- 複数のプライベートIPアドレス＋TCP/UDPポート番号から、1つのグローバルIPアドレス＋複数のTCP/UDPポート番号への変換を自動的に行います。
- ダイナミックNAPTは動的にプライベートIPアドレスのポート番号が変化することから、セキュリティ面で非常に有効なため、多くのブロードバンドルーターで利用されているアドレス変換方式となります。



対象となるプライベートIPアドレスと変換するグローバルIPアドレスの対応ルールを設定（変換するグローバルIPアドレスに、ルーターAのWAN回線接続インターフェースのIPアドレスを指定することも可能）

（変換対象のプライベートIPアドレス）：
192.168.100.2 ～ 192.168.100.254

（変換するグローバルIPアドレス）：200.1.1.1(eth1)

ルーターAは設定されたルールに従い、IPアドレスとポート番号を変換します。グローバルアドレス変換時のポートは、空きポートを動的に割り当てます

ルーターAのNATテーブル

プライベートIPアドレス	変換前ポート番号	グローバルIPアドレス	変換後ポート番号
192.168.100.2	49200	200.1.1.1	49501
192.168.100.3	49500	200.1.1.1	55100
192.168.100.4	49700	200.1.1.1	63001

④PPPoE / IPoE

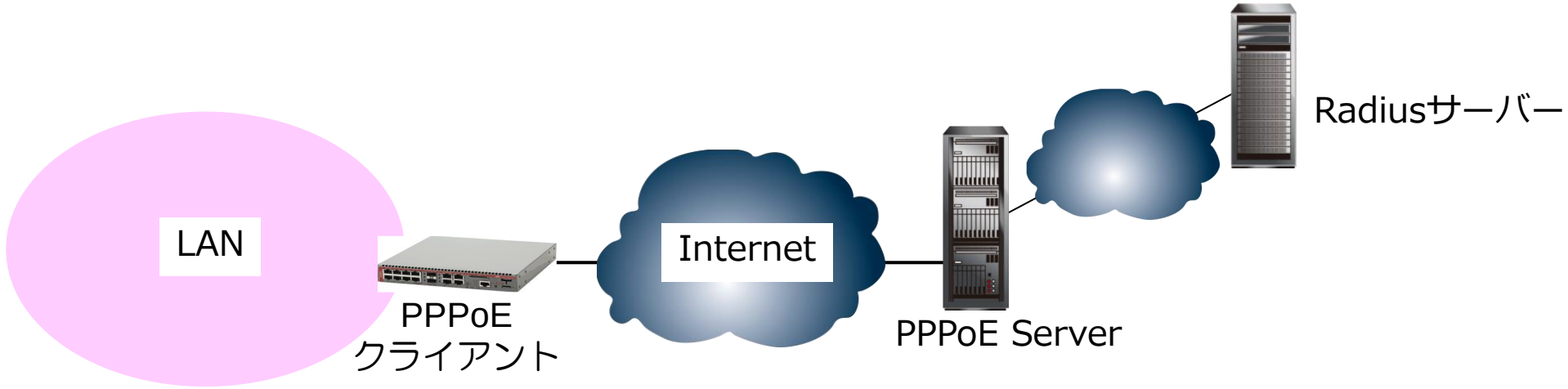
PPP(Point to Point Protocol)の概要

- PPPは、２点間で複数のプロトコルのデータを運ぶための手段で、いくつかのプロトコル群から構成されています。
  - LCP（Link Control Protocol）：LCPによってパスワード認証機能を提供して、リンクを確立します。
  - NCP（Network Control Protocol）：それぞれの通信プロトコルに必要な設定を行って接続を確立します。

- PPPのメリット
  - 複数のセッションを並行して確立できる
  - セッション単位の課金ができる（RADIUS Server等が必要）
  - 認証の仕組みが簡単で、ユーザー名とパスワードによるシンプルな認証方式
  - セッション単位での認証、暗号化と圧縮が可能
  - ネットワーク層プロトコルに依存しない。TCP/IP以外の通信プロトコルも利用できる
  - 標準化されているので、様々なベンダー機器で利用が可能（RFC1661で標準化）

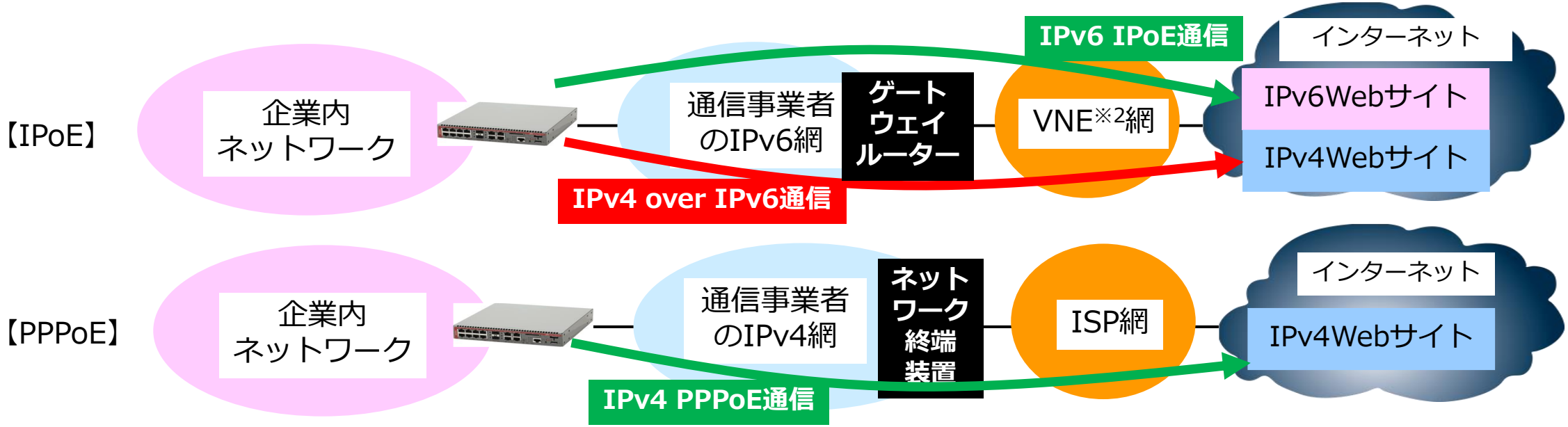
PPPoE(PPP over Ethernet)の機能

- PPPoEとは、イーサネットフレーム上にPPPをカプセル化する通信プロトコルで、RFC2516で定義されています。
- PPPの持つ認証機能が利用できますし、複数回線との同時接続も可能（マルチセッション）です。
- PPPoE使用時の注意点
  - PPPoEクライアントの明確化：最近ではルーターを利用することが主流
  - 認証におけるユーザー名とパスワードの設定
  - パケットサイズの設定（MTU）
  - 最低限のファイアウォール、ウイルス対策ソフトを導入してから接続する



IPoE(Internet Protocol over Ethernet)

- IPoEは、PPPoEと同様にインターネットへの接続方式の一つです。IPoEではインターネットへの接続に高速大容量のゲートウェイルーター(GWR)を使用するため、通信速度はPPPoEの10倍（最大10Gbpsまたは最大100Gbps※1）で、輻輳が発生しにくくネットワークの安定性が高いという特徴があります。
- IPoEでは、 IPv6アドレスのWebサイト(=IPv6網)にのみ接続可能です。IPv4アドレスのWebサイトに接続するためには、通信事業者が提供する「IPv4 over IPv6インターネット接続サービス」を利用する必要があります。IPv4 over IPv6は、IPv4パケットをIPv6でカプセル化する技術になります。



※1 通信事業者または使用する機器のインターフェースによって異なります。また、アクセス回線にベストエフォート型回線を使用する場合、通信速度はネットワークの混雑状況によって変わります。
※2 VNE(Virtual Network Enabler)とは、ISPにIPv6ネットワークを貸し出す事業者になります。ISPがIPv6ネットワークサービスを提供する場合にVNE事業者を利用することで、自前のIPv6ネットワーク設備を用意することなくサービスが提供できます。

⑤設定・管理機能

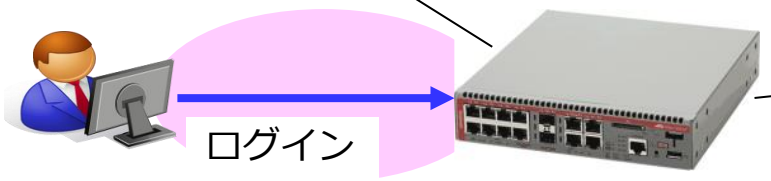
設定方法

- ルーターの設定方法には、「コンソール接続やtelnet接続によるコマンド(CLI)での設定」と「WebGUIインターフェースによるブラウザ画面での設定」があります。
- 基本的な設定はWebGUIインターフェースで行えますが、詳細な機能の場合はコマンド設定が必要になります。

【コマンド(CLI)によるIPアドレス設定】

```
awplus(config)# interface vlan10
awplus(config-if)# ip address 192.168.10.1/24
awplus(config-if)# ip address 192.168.11.1/24 secondary
awplus(config-if)# ip address 192.168.12.1/24 secondary
```

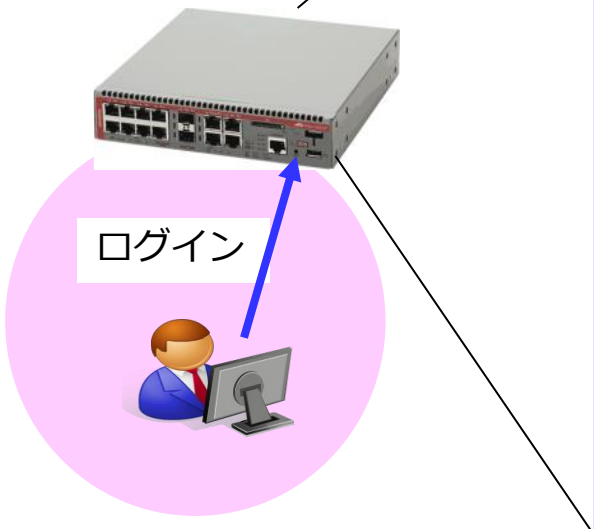
【WebGUIによるインターフェース設定画面】



AMF Plusマスター機能

- ルーター「AT-AR4050S-5G」および「AT-AR4050S」は、AMF Plusマスターライセンスの導入によりAMF Plusマスター機能が利用できるようになり、xシリーズスイッチ（AMF Plusメンバー）を最大20メンバー管理できます。リモートサイトの統合管理や小規模オフィスに最適です。
- 以下はAMF Plusマスターが管理しているAMF機器の一覧になります。

AT-AR4050S

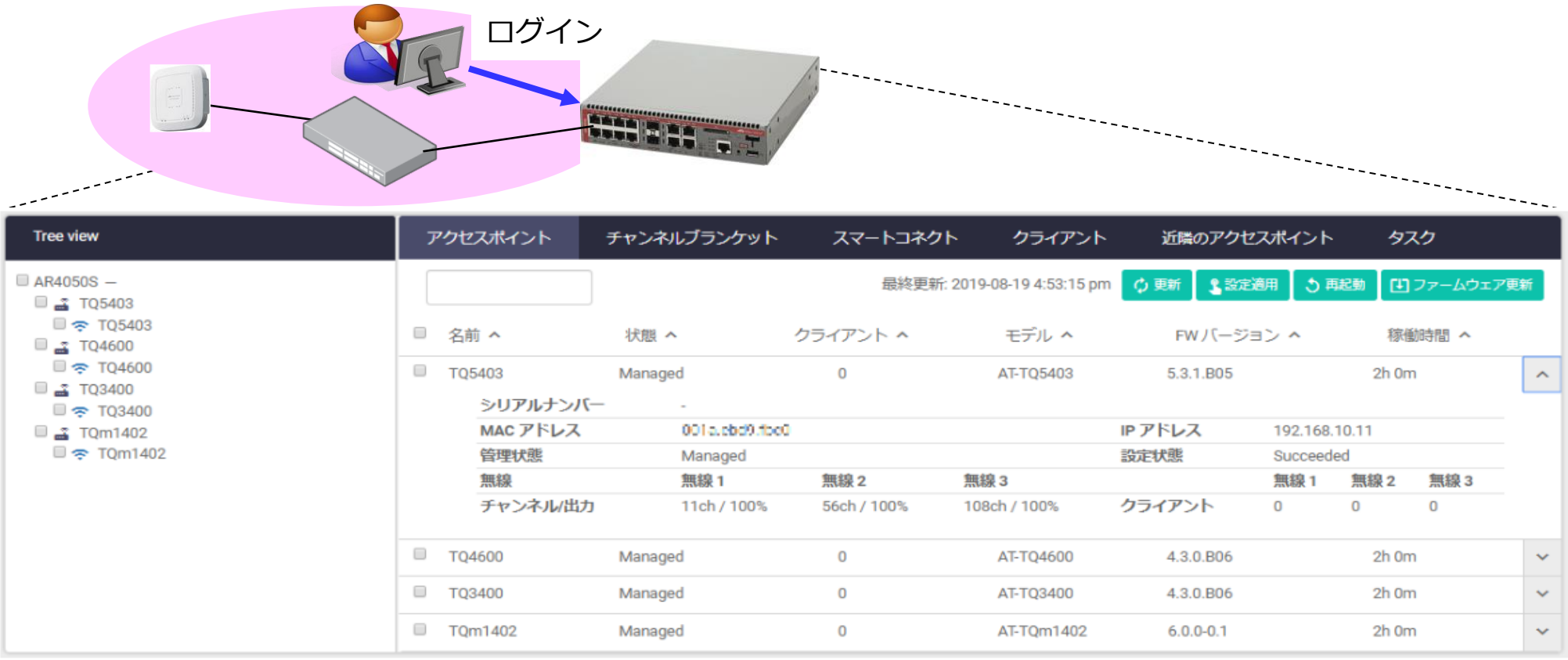


【AMF Plusノード管理】

```
SBx81# show atmf nodes

Node Information:

  * = Local device

 SC = Switch Configuration:
  C = Chassis    S = Stackable    N = Standalone

  Node                 Device             ATMF                          Node
  Name                 Type               Master  SC  Parent            Depth
-------------------------------------------------------------------------------
* SBx81                AT-SBx81CFC960       Y     C   none               0
  FSW242               x510-28GTX           N     S   SBx81              1
  FSW241               x510-28GTX           N     S   SBx81              1
  ESW231               x510-52GTX           N     S   FSW242             2

 Current ATMF node count 4
```

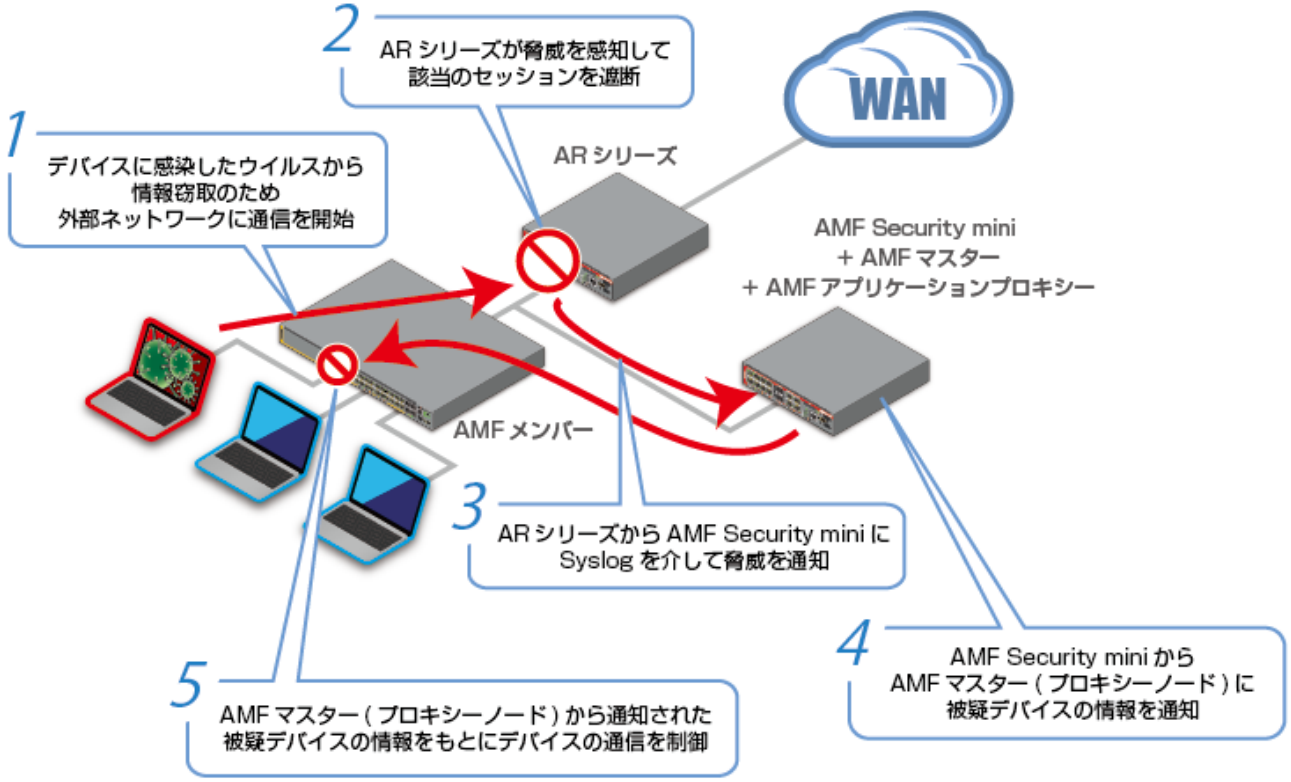
無線コントローラー機能

- ルーター「AT-AR4050S-5G、AT-AR4050S、AT-AR3050S、AT-AR2050V、AT-AR2010V」は無線コントローラー機能を持ち、標準5台の無線アクセスポイントを管理可能です。なお、AT-AR4050S-5GとAT-AR4050Sは、ライセンスの追加により最大25台まで無線アクセスポイントを管理可能です。
- 小規模オフィスでも容易に無線コントローラーを導入でき、外来波による影響を最小限にとどめ、最適な無線LANネットワークを維持します。
- 以下は、ルーターが管理している無線アクセスポイントの一覧画面です。



AMF-SECコントローラー機能

- ルーター「AT-AR4050S-5G」および「AT-AR4050S」は、AMF-SECurityコントローラーminiライセンスの導入によりAMF-SECコントローラーとして動作します。これにより、1台でAMF-SECコントローラー機能とAMF Plusマスター機能を提供します。※1
- AMF-SECurityは、セキュリティ・IT資産管理・人事などのアプリケーションをAMF-SECコントローラーと連携させることで、セキュリティリスクのある端末を自動で隔離する機能です。



※1 AMF Plusマスターとして動作するためにはAMF Plusマスターライセンスが必要です。また、UTM関連機能（ファイアウォールとNATは除く）とは併用不可となります。なお、ルーターのAMF-SECコントローラー機能はOpenFlowに対応していないため、OpenFlowによる制御はできません。

⑥製品紹介

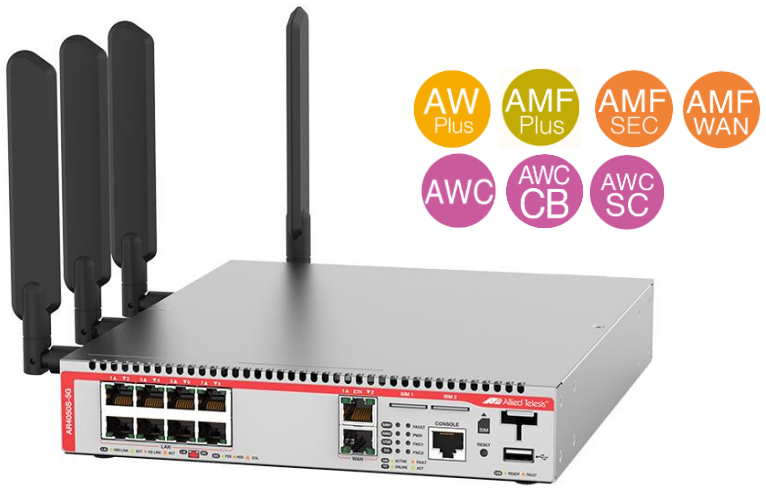
ルーター製品（一覧）

- 以下は、弊社のルーター製品の一覧になります。
- AT-AR4050Sは、ICSA(International Computer Security Association) Labs※のセキュリティテストの要件を満たし、「ICSA Labs Firewall Certification」認定を受けています。

※ ICSA Labsは、セキュリティやネットワーク接続機器の第三者テストおよび認定を行っており、世界トップクラスの多くのテクノロジーベンダーを対象に、製品のコンプライアンス、信頼性、性能の測定を行う機関です。

AT-AR4050S-5G

【 UTM＆VPN対応アクセスルーター】



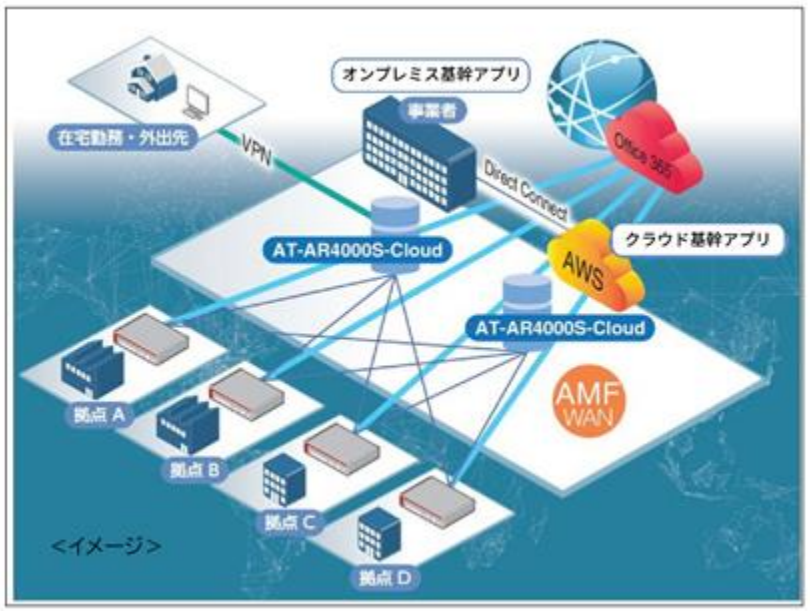
AT-AR4050S-5G

※延長用外部アンテナ AT-AR050 装着時

- **5G/LTE移動体通信接続サービスに対応**
  - AT-AR4050S-5Gはマルチキャリア（SIMフリー）対応の5G通信モジュールを内蔵し、SIMカードを挿入することで5G/LTE通信が可能になります。SIMカードを2枚同時挿入可能なデュアルSIMスロット対応のため、移動体通信回線のアクティブ・スタンバイでの運用も可能です。
- **ファイアウォール/UTM**
  - ステートフル・パケット・インスペクション型ファイアウォール（ゾーンベース）やIDS/IPSの基本となるセキュリティ機能に加え、レイヤー３ではIPアドレスブラックリスト、レイヤー７ではDPI（ディープパケットインスペクション）やURLフィルターなどに対応した、多重構造の強力なセキュリティを備えた次世代ファイアウォールです。
- **自律型無線LANソリューション AWC搭載**
  - AWCは、管理対象の無線LANアクセスポイント周囲の電波出力、チャンネルを常に認識し、最適化します。
  - 管理可能な無線LANアクセスポイント台数は標準5台で、ライセンス追加で25台まで拡張可能です。
  - AWC-CBおよびAWC-SCで最大5台の無線APを管理できます。
- **AMF/AMF Plusマスター機能対応**
  - AMF/AMF Plusマスターライセンスの導入により、AMF/AMF Plusマスター機能が利用できます。AMF/AMF Plusメンバーを最大20メンバー管理でき、リモートサイトの統合管理や小規模オフィスに最適です。
- **延長用外部アンテナ装着可能**
  - 延長用外部アンテナ(AT-AR050）でアンテナ部のみを3m延伸可能です。

AT-AR4000S-Cloud

【仮想アプライアンスルーター】



AT-AR4000S-Cloud

- **VPN（バーチャル・プライベート・ネットワーク）**
  - IPsec VPN接続でのIKEv2によるセキュアなIPsec通信やL2TPv3による柔軟な拠点間通信を実現できます。IPsec通信では最大3000セッションまでサポートします。
- **リモートアクセス（OpenVPN、OS標準VPNクライアント）**
  - テレワーク/在宅勤務や出張で、オフィスなど一定の場所に縛られずに、いつでもどこでも仕事ができる環境を構築できます。WindowsやiOSに標準搭載しているVPNクライアントソフトに加え、OpenVPNや、Androidのstrongswanと接続検証済みです。
- **ファイアウォール/UTM**
  - ステートフル・パケット・インスペクション型ファイアウォール（ゾーンベース）、IPアドレスブラックリストおよびDPI(ディープパケットインスペクション）などに対応します。UTM機能は以下をご利用いただくことができます。
    - ・IDS（侵入検知）/IPS（侵入防止）
    - ・アプリケーションコントロール
    - ・Webコントロール
    - ・IPレピュテーション
    - ・アドバンスドIPレピュテーション
- **AMF-WAN（SD-WAN）**
  - 以下のAMF-WAN機能に対応しています。
    - ・インターネットブレークアウト
    - ・SD-WANロードバランス
    - ・WANマップ/アプリケーショントラフィックの可視化

AT-NFV-APL-GTX / AT-NFV-APL-GT

【アドバンスト・セキュアVPN センター・ルーター】

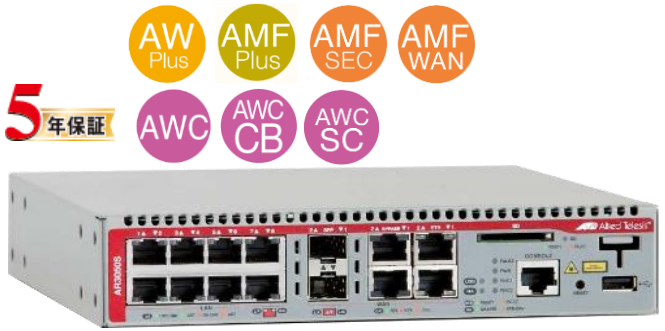
AT-NFV-APL-GTX

AT-NFV-APL-GT

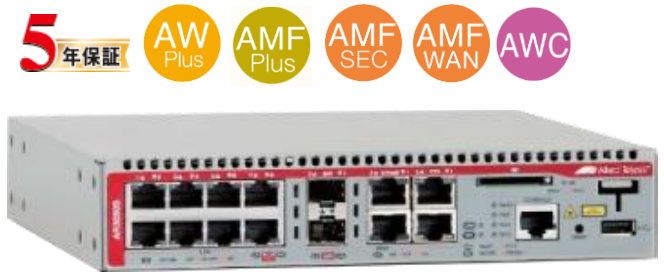
- **10Gインターフェース搭載（AT-NFV-APL-GTXのみ）**
  - 100/1000/10GBASE-T規格に対応したポート(オートネゴシエーション)を4ポート搭載し、最大37Gbps(IPv4ルーティング時)の高スループットを実現します。
- **ファイアウォール/UTM**
  - ステートフル・パケット・インスペクション型ファイアウォール（ゾーンベース）やIDS/IPSの基本となるセキュリティー機能に加え、レイヤー3ではIPアドレスブラックリスト、レイヤー7ではDPI（ディープパケットインスペクション）やURLフィルターなどに対応した多重構造の強力なセキュリティーを備えた次世代ファイアウォールです。
- **VPN（バーチャル・プライベート・ネットワーク）**
  - IPsec VPN接続を利用した仮想網で、拠点間通信が安全に行えます。また、IKEv2の対応により、よりセキュアなIPsec通信が可能なだけでなくL2TPv3による柔軟な拠点間通信を実現できます。
  - IPsec通信において最大3000セッションをサポートするため、本製品をセンタールーターで多拠点ネットワークを構成可能です。
- **リモートアクセスVPN**
  - PCやスマートフォンなどの端末と本製品をVPN接続し、外部から社内ネットワークへのアクセスを可能とするリモートアクセスVPNに標準で対応します。
  - Windows 10や iOSに標準搭載しているVPNクライアントソフトに加え、マルチプラットフォームでより高度なセキュリティに対応したOpenVPNや、AndroidでIPsecIKEv2を用いて接続可能なVPNクライアントソフトstrongSwanを利用して、自宅からの在宅勤務やシェアオフィスからのモバイルワークに最適なリモートアクセス環境を実現できます。

AT-AR4050S / AT-AR3050S

【UTM＆VPN対応ルーター】



AT-AR4050S



AT-AR3050S

- **セキュアなVPN接続**
  - IPsec VPN接続を利用した仮想網で、拠点間通信が安全に行えます。IKEv2でよりセキュアなIPsec通信が可能なだけでなく、L2TPv3による柔軟な拠点間通信を実現できます。AT-AR4050Sでは、IPsec通信において最大1000セッションまでサポートし、多拠点ネットワークを構築することが可能です。
- **高セキュリティ**
  - ステートフル・パケット・インスペクション型ファイアウォール（ゾーンベース）やIDS/IPSの基本となるセキュリティ機能に加え、レイヤー３ではIPアドレスブラックリスト、レイヤー７ではDPI（ディープパケットインスペクション）やURLフィルターなどに対応した、多重構造の強力なセキュリティを備えた次世代ファイアウォールです。
- **SD-WANロードバランス**
  - 複数のWAN回線をロードバランスし帯域を有効に利用することが可能な機能です。常時回線状態を監視し、新たなセッションを結ぶ際、品質のよい回線を選択してロードバランスするといった先進的な負荷分散が可能です。送信元IP、宛先IPやポート番号と組み合わせることでアプリケーション単位でロードバランスすることも可能です。
- **AMF/AMF Plusマスター機能対応（AT-AR4050Sのみ）**
  - AMF/AMF Plusマスターライセンスの導入により、AMF/AMF Plusマスター機能が利用できます。AMF/AMF Plusメンバーを最大20メンバー管理でき、リモートサイトの統合管理や小規模オフィスに最適です。

AT-AR2050V/AT-AR2010V

【VPN対応ルーター】

AT-AR2050V

AT-AR2010V

＊DC（12～24V）電源対応

■ ファイアウォール

- ステートフル・パケット・インスペクション型ファイアウォール（ゾーンベース）をはじめ、IDS/IPS、各種攻撃検出機能や、特定のURLに対するアクセス許可・拒否を制御可能なカスタムURLフィルターに対応。外部からの脅威や社内からの情報漏洩などを防ぎ、安全なインターネット接続環境を構築できます。

■ セキュアなVPN接続

- IPsec VPN接続を利用した仮想網で、拠点間通信が安全に行えます。また、IKEv2の対応により、よりセキュアなIPsec通信が可能なだけでなく、L2TPv3による柔軟な拠点間通信を実現できます。

■ SD-WANロードバランス

- 複数のWAN回線をロードバランスし帯域を有効に利用することが可能な機能です。常時回線状態を監視し、新たなセッションを結ぶ際、品質のよい回線を選択してロードバランスするといった先進的な負荷分散が可能です。送信元IP、宛先IPやポート番号と組み合わせることでアプリケーション単位でロードバランスすることも可能です。

■ AC/DC電源対応（AT-AR2010Vのみ）

- 機器内部で使用しているDC電源（12-24V）を使用することができます。もちろんACアダプターを使用することでAC電源からも給電可能です。

AT-AR1050V

【VPN対応ルーター】

AT-AR1050V

■ インターネットVPN

- IPsecを利用したVPN（3DES/AES）をサポートし、安価なインターネットサービスを利用したセキュアな企業間ネットワークが構築可能です。

■ ファイアウォール

- ステートフル・パケット・インスペクション型ファイアウォール（ゾーンベース）をはじめ、IDS/IPS、各種攻撃検出機能や、特定のURLに対するアクセス許可・拒否を制御可能なカスタムURLフィルターに対応。外部からの脅威や社内からの情報漏洩などを防ぎ、安全なインターネット接続環境を構築できます。

■ WebベースGUIおよびCLI設定

- Webブラウザーからの簡単設定や、機器やトラフィックの状態をダッシュボードから一元管理・監視などが行えます。操作言語は使用するWebブラウザーの言語設定に応じて日本語/英語の自動切り替えが可能です。また、業界標準のコマンド体系に準拠したCLIにも対応し、多数の機器を効率よく設定できます。

■ NAT（アドレス変換）

- スタティックNAT、ダイナミックNATに加えエンハンスドNAT（NAPT）に対応し、限られたIPアドレスを有効に利用できます。さらに、PPTP（GRE）、L2TP、IPsec（ESP、IKE）のプロトコルに対してはパススルーが可能です。

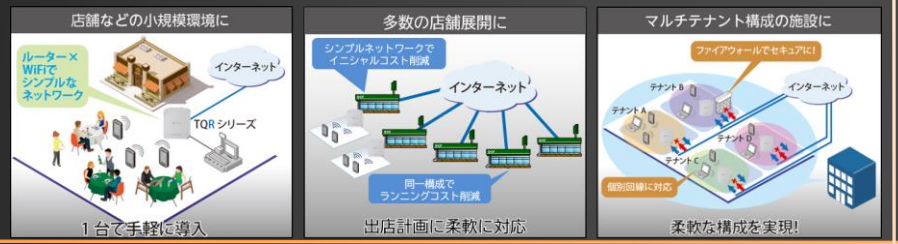
Appendix：各種販促情報のご案内

各種販促情報のご案内

新製品のご紹介(Wi-Fi6対応無線LANルーター)

AT-TQ6702 GEN2-R

- **Wi-Fi6とVPNルーターの機能を1台で提供**
- **エンタープライズ向け機能を搭載**
  - FirewallやダイナミックENAT、IPsec、VAP、Captive Portal、WPA3など各種エンタープライズ向け機能を搭載
- **AMF Plusによる一元管理に対応**
- **様々なネットワークに適用可能**
  - 小規模ブランチオフィス、コンビニエンスストアやレストランなどの店舗向けのネットワークなど、様々なネットワークをAT-TQ6702 GEN2-R 1台のみでシンプルな構成を組むことが可能



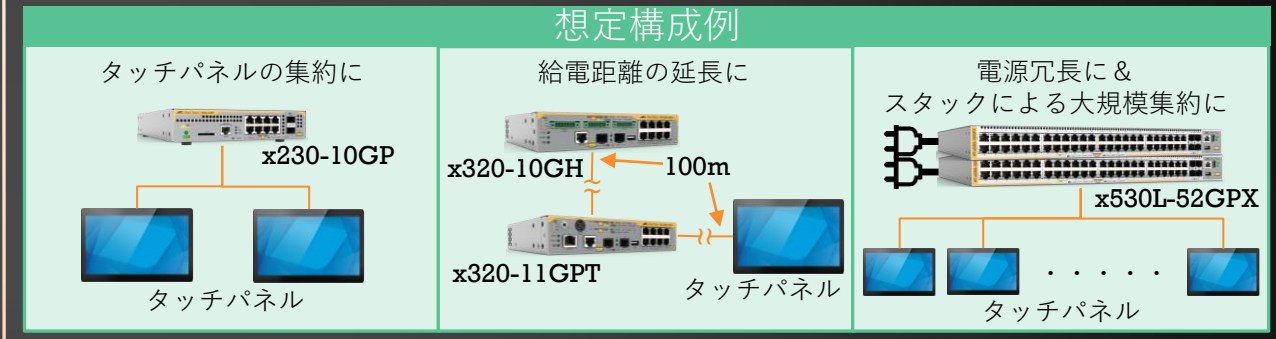
スイッチ製品協業ベンダーのご紹介

協業先：**タッチパネル・システムズ株式会社**

PoE対応タッチパネルと接続検証を実施！

検証機器：**x530L・x320・x230・AT-7101GHTm**

https://www.allied-telesis.co.jp/news/newsrelease/nr230324.html



Allied Labのご紹介

Allied Lab で検索！

アライドテレシスの技術を製品担当が分かりやすく紹介。

…第十回目：**Wi-Fi6**対応アクセスポイント比較検証
「失敗しない**Wi-Fi6**選びの手引き」

…第十一回目：統合型ネットワーク管理ソフトウェア
「**AT-Vista Manager EX**で**Network**管理者のお悩み大解決！」

…第十二回目：ネットワーク統合管理
「ネットワーク管理の手間をごそっと削減！」

…他、多数！

ビデオデータシートのご紹介

各種製品名 で検索！

製品の特長やユースケースなどを動画でご紹介します。

…**PoE++**対応マルチギガビットスイッチ
x530L GHXm シリーズ紹介

…オール**10G**レイヤー**2**スイッチ
XS910/8 紹介

…マルチギガビット対応**PoE++**インジェクター
AT-7101GHTm紹介

…他、多数！

5Gルーター製品の標準価格改定

大規模災害発生時でも大切な通信インフラを確保する5Gルーターを、2023年7月から新標準価格でご提供します。

法人向け5G/4G LTE対応VPNルーター

AT-AR4050S-5G

相互接続性：NTTドコモ、KDDI、Softbank

5年保証

新標準価格(税抜) **¥259,000**
(税込) **(¥284,900)**

約30% OFF

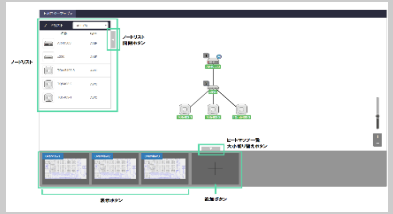
旧標準価格(税抜) ~~¥368,000~~
(税込) ~~(¥404,800)~~

コードNo.	製品名	標準税込価格	概要
4668R	AT-AR4050S-5G	¥284,900	5G/4G LTE通信対応VPNセンタールーター本体
4668RZ1	AT-AR4050S-5G-Z1	¥294,910	5G/4G LTE通信対応VPNセンタールーター本体（デリスタ保守1年付）
4668RZ5	AT-AR4050S-5G-Z5	¥327,690	5G/4G LTE通信対応VPNセンタールーター本体（デリスタ保守5年付）
4668RZ7	AT-AR4050S-5G-Z7	¥361,900	5G/4G LTE通信対応VPNセンタールーター本体（デリスタ保守7年付）

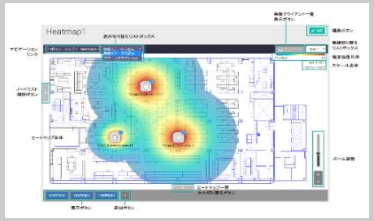
（注）UTMなどの機能追加ライセンスは、別途費用が発生します。

VISTA MANAGER mini

トポロジーマップ表示



Wi-Fiのヒートマップ表示



標準で5台の無線APを管理、追加ライセンスにより25台まで拡張可能

できる！緊急避難所ネットワーク
～通常の学校ネットワークの資産を有効活用～

WAN回線をバックアップ

WANインターフェースは有線ポートに加えてSIMカードスロットを搭載し、5Gあるいは4G LTEのSIMを利用して有線の回線をバックアップする構成を構築可能です。

無線LANコントローラー

大規模災害発生時に無線LANサービスの開放が必要な場合、標準搭載の無線LANコントローラーは、予約されたSSIDをUSBメモリーを使って即座に開放可能です。

ファイアウォール

本製品のファイアウォールはアプリケーションベースでの通信制御に対応したDPI機能を標準搭載し、緊急時においてもWANの安全性や冗長性を高めます。

ご清聴ありがとうございました。

Allied Telesis

今回ご紹介しましたネットワーク製品に関して、
別途個別に相談がございましたら、お気軽に弊社
営業までお問い合わせください。