新人エンジニアが学ぶ無線と IP ネットワーク

1. はじめに

新人エンジニアの皆さん、ネットワークの世界へようこそ。本書は、**無線 LAN** と **IP ネットワーク**の基本を学び、現場で活用できる知識を身につけるための入門書です。日常生活やビジネスでネットワークは欠かせない存在となっており、スマートフォンの Wi-Fi 接続から会社の社内 LAN まで、幅広く利用されています。本書では、無線通信の仕組みから IP ネットワークの構成要素、ネットワーク機器の役割、重要なプロトコル、セキュリティ対策、ネットワーク設計、トラブル対応、さらには運用・監視の基本まで、順を追って解説していきます。

目的: 本書の目的は、ネットワークに不慣れな新人エンジニアが基本概念を理解し、実務で活用できる土台を築くことです。専門用語はできるだけわかりやすい言葉で説明し、具体例や図解を交えて理解を助けます。読者の皆さんが本書を通じて、無線 LAN と IP ネットワークの全体像をつかみ、自信を持ってネットワーク構築やトラブルシューティングに取り組めるようになることを目指しています。

それでは、ネットワークの基礎の世界を一緒に学んでいきましょう。

2. 無線の基礎

はじめに、**無線**（ワイヤレス）による通信の基礎を学びます。無線通信とは、その名の通りケーブルなどの物理的な線を使わずに、電波を利用してデータを送受信する方法です。私たちが日常的に使う**無線 LAN（Wi-Fi）**もこの一種で、スマートフォンやノート PC がアクセスポイントを通じてインターネットに接続する際に利用されています。

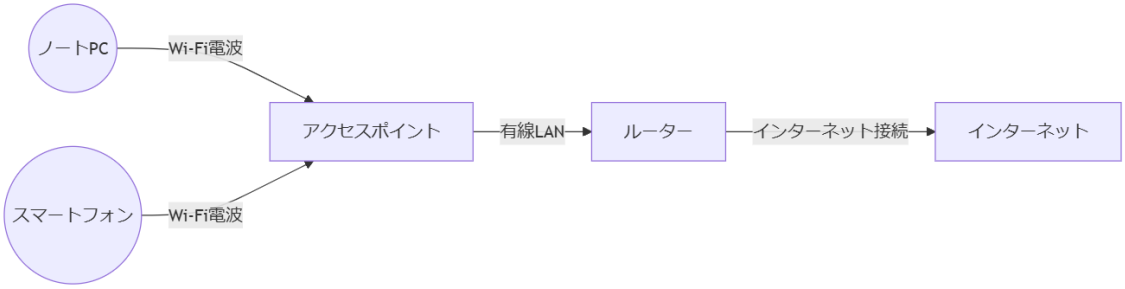
無線 LAN とは何か

無線 LAN は **Wireless LAN**（ワイヤレス・ラン）の略で、ケーブルの代わりに電波でデータ通信を行う LAN（Local Area Network）のことです。一般には **Wi-Fi**（ワイファイ）という名称で広く知られており、カフェや自宅、オフィスなど様々な場所で利用されています。Wi-Fi は技術規格の一つであり、例えば IEEE802.11 シリーズの規格に基づいて動作しています。無線 LAN を使うことで、ケーブル接続の制約がない自由なネットワーク接続が可能になります。

無線 LAN の基本構成要素:

1. **アクセスポイント（AP）:** 無線 LAN の基地局にあたる機器です。電波を利用して端末と有線ネットワークの橋渡しをします。家庭用の「Wi-Fi ルーター」は、無線 AP と有線ルータが一体となった装置が多いです。
2. **無線端末（クライアント）:** 無線 LAN に接続するデバイスを指します。スマートフォン、タブレット、ノート PC、ゲーム機、IoT 機器など、多様な端末が含まれます。
3. **電波:** データを運ぶメディア（媒体）です。無線 LAN では主に 2.4GHz 帯と 5GHz 帯の周波数の電波が使われ、空間を伝わって情報を届けます。

上記の要素がそろって初めて無線 LAN で通信ができます。例えば自宅の Wi-Fi では、スマホや PC（無線端末）が家の Wi-Fi ルーター（AP）に電波で接続し、その Wi-Fi ルーターがインターネットへ通信を中継しています。



上の図は、無線 LAN で端末がネットワーク接続する一般的な構成を表しています。ノート PC やスマートフォンが Wi-Fi 電波を介してアクセスポイント（Wi-Fi ルーター）に接続し、アクセスポイントは有線 LAN 経由でルーターとつながり、最終的にインターネットへアクセスします。

無線通信の仕組み

無線 LAN で端末が通信を行う基本的な流れは次のとおりです。

- **電波の検出と接続要求:** 無線端末は周囲に飛んでいる Wi-Fi の電波（SSID と呼ばれるネットワーク名を含む信号）を検出します。接続したい SSID を選択すると、端末はそのアクセスポイントに対して接続要求を送信します。
- **認証と暗号化の設定:** アクセスポイントは端末からの接続要求を受け取ると、事前共有キー（パスワード）や証明書を用いて端末の認証を行います。認証に成功すると、Wi-Fi の暗号化鍵の交換（ハンドシェイク）が行われ、安全に通信できる準備が整います。現在主流の暗号化方式は **WPA2** や **WPA3** で、通信内容を傍受されないよう強力に保護します（古い **WEP** は脆弱で、現在は使用推奨されません）。
- **通信の開始:** 認証・暗号化設定が完了すると、端末とアクセスポイント間でデータの送受信が可能になります。以降、端末からのデータは電波に変換されてアクセスポイントへ飛び、アクセスポイントで有線のデータに戻されインターネットへ送出されます。逆の方向の通信も同様で、インターネットからアクセスポイントに届いたデータが電波で端末に届けられます。

無線 LAN では、通信品質を保つために**周波数帯とチャネル**の管理も重要です。2.4GHz 帯では電波が遠くまで届きやすい一方で電子レンジなど他の機器とも干渉しやすく、5GHz 帯では高速通信が可能ですが遮蔽物や距離に弱い、といった特徴があります。そのため環境に応じて適切な周波数帯やチャネルを選択し、電波の混雑や干渉を避けるようにします。

無線通信技術の発展

無線 LAN は IEEE802.11 という標準規格に基づいて発展してきました。例えば、古くは **802.11b**（最大 11Mbps、2.4GHz 帯）や **802.11g**（54Mbps）といった規格が使われ、現在では **802.11n**（最大 600Mbps、2.4/5GHz 両対応）や高速な **802.11ac**、最新の**802.11ax (Wi-Fi 6)**などが登場しています。新しい規格になるほど通信速度の向上や同時接続の効率化、省電力化などが図られており、ネットワーク環境に求められる性能に合わせて機器を選定することが重要です。

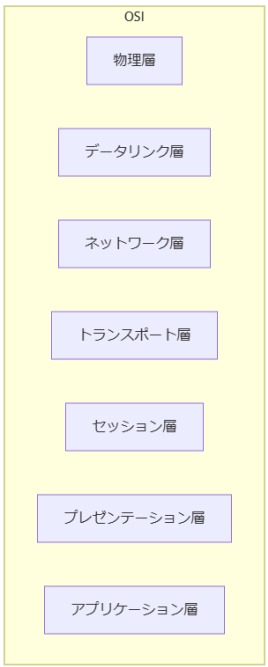
3. IP ネットワークの基礎

次に、**IP ネットワーク**について基礎を学びましょう。IP ネットワークとは、コンピュータ同士が**IP（Internet Protocol）**という共通のルールに従って通信を行うネットワークのことです。インターネットをはじめ、企業内 LAN や家庭内 LAN でも IP が使われています。IP ネットワークの理解は、ネットワークエンジニアにとって必須の知識です。

ネットワークの階層モデル

IP ネットワークを理解するには、通信の階層（レイヤー）概念を簡単に押さえておくと役立ちます。通信は大きく分けて **OSI 参照モデル**の 7 階層（あるいは TCP/IP モデルの 4 階層）で考えられていますが、ここでは主要な部分に絞って説明します。

- **物理層・データリンク層:** これは主にネットワークの**インフラ部分**です。ケーブルや無線電波でビットを送る物理層、その上で直接接続された機器同士が通信するデータリンク層があります。データリンク層では **MAC アドレス**という機器固有の番号を使って通信し、スイッチングハブ（スイッチ）などがこの層で機能します。
- **ネットワーク層:** ここが **IP 層**です。ネットワーク間の通信を可能にする層で、IP アドレスを使って世界中のネットワークを識別し、パケットを中継します。ルータはこの層で動作し、IP アドレスを見て適切な経路にデータを転送します。
- **トランスポート層:** ネットワーク層の上位にあり、通信をアプリケーションに届ける役割を担います。代表的なプロトコルに **TCP**（信頼性の高い接続型通信）と **UDP**（シンプルで高速なコネクションレス通信）があります。ポート番号を使って同一ホスト内のアプリケーションを区別します。



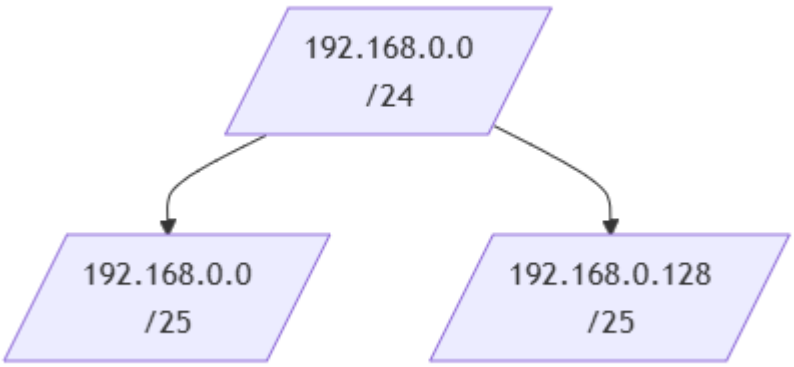
上記のように層に分けて考えることで、どの部分に問題があるか切り分けたり、役割の違う機器を整理したりしやすくなります。特に **IP ネットワーク**という場合、主に「ネットワーク層（IP）」とその周辺の仕組みに注目していきます。

IP アドレスとサブネット

IP アドレスは、IP ネットワーク上で各機器（ホスト）を識別するための番号です。IPv4 では 192.168.10.15 のように 0〜255 の数字を 4 つ組み合わせた形式（32 ビット）で表現されます。各 IP アドレスには**ネットワーク部**と**ホスト部**があり、ネットワーク部が同じアドレス同士は同一ネットワーク（サブネット）内にあるとみなされます。ネットワーク部の長さは**サブネットマスク**や**プレフィックス長**（例: /24 等）によって決まり、一般に同じネットワーク内ではサブネットマスクが共通です。

例として、アドレス 192.168.10.15/24 の場合、/24 は先頭 24 ビットがネットワーク部であることを意味します。このネットワーク部は 192.168.10.0 であり、この範囲に属する 192.168.10.xxx（xxx は 0〜255 の範囲）同士は直接通信できる関係にあります。一方、ネットワークが異なる（ネットワーク部が異なる）アドレス同士は直接には通信できず、後述する**ルータ**を経由する必要があります。

なお、IPv4 アドレスには**プライベート IP アドレス**と**グローバル IP アドレス**があります。プライベート IP は 192.168.x.x や 10.x.x.x など内部ネットワーク用に予約された範囲で、インターネット上では直接ルーティングされません。一方、グローバル IP はインターネットで一意に割り当てられるアドレスです。通常、家庭や企業内の端末はプライベート IP を使い、インターネットとの出入り口で **NAT**（後述）によってグローバル IP に変換しています。



デフォルトゲートウェイとルーティング

同一ネットワーク内の機器同士は直接やりとりできますが、異なるネットワークへの通信をする際には**ルーティング**が必要になります。各端末には**デフォルトゲートウェイ**という設定項目があり、これは「他のネットワークに行くときに経由するルータの IP アドレス」を指しています。例えば、自分の PC が 192.168.10.15/24 でデフォルトゲートウェイが 192.168.10.1 であれば、192.168.10.0/24 以外の宛先へのパケットはすべて 192.168.10.1（ルータ）に送るようになります。ルータは受け取ったパケットの宛先 IP を見て、次にどこへ転送すべきか判断します。

ルータは**ルーティングテーブル**を持っており、どのネットワーク宛の通信をどのインタフェースに送るかという経路情報を管理しています。小規模ネットワークでは経路はシンプルで、例えば「社内 LAN（例:192.168.10.0/24）は内部、その他のあて先はすべてインターネット側へ」といった具合に設定されます。これにより、LAN 内の通信は直接 LAN 内で完結し、外部への通信のみがルータに集約されてスムーズに運ばれます。

IP ネットワークの基礎として、**IP アドレス**の構造と役割、そして**ルータによる経路選択**について押さえました。次章では、有線と無線のネットワーク構成の違いについて詳しく見てみましょう。

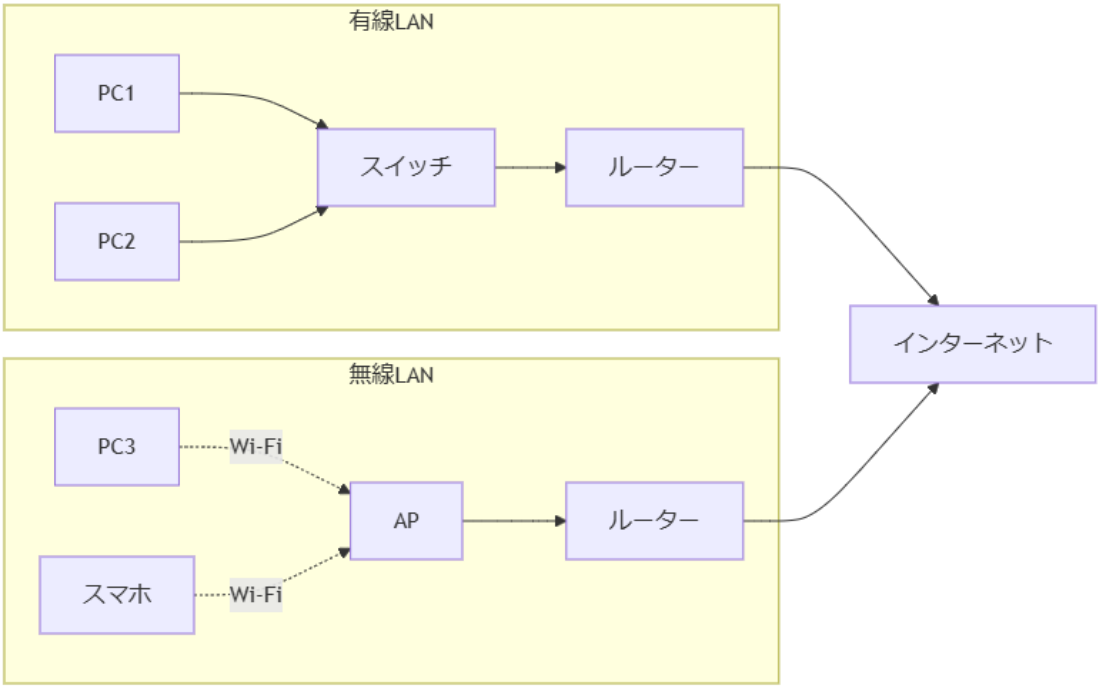
4. 無線 LAN と有線 LAN の構成比較

ここでは、**無線 LAN**（Wi-Fi による LAN）と**有線 LAN**（ケーブルによる LAN）の構成を比較し、それぞれの特徴や違いを理解します。どちらも LAN という点では共通ですが、接続形態や必要な機器、通信の性質に違いがあります。

接続形態の違い

- **有線 LAN:** 機器同士を**ケーブル（イーサネットケーブル）で直接接続するネットワークです。各端末（PC やプリンタなど）はハブやスイッチ**と呼ばれる集線装置にケーブルでつながり、通信します。有線 LAN では物理的に配線が必要ですが、一般に安定した速度と低遅延が得られ、外部から不正に電波を傍受される心配もありません。
- **無線 LAN:** 機器同士を**電波**で接続するネットワークです。各端末は空間に飛んでいる Wi-Fi 電波を介して**アクセスポイント（無線 AP）**に接続し、AP が有線ネットワークと無線端末を中継します。無線 LAN はケーブル不要で移動も容易ですが、電波状況に通信品質が左右されたり、セキュリティ設定をきちんとしないと通信を盗聴される危険があります。

下図は、有線 LAN と無線 LAN の典型的な構成例を比較したものです。左側は有線 LAN で、各 PC がスイッチにケーブルで接続されています。右側は無線 LAN で、PC やスマホが電波でアクセスポイントに接続しています。両者は最終的にルータ経由でインターネットに接続します。



有線 LAN では各機器が直接スイッチに繋がるため、**スター型トポロジー**（中央にスイッチ、そこから各端末へ配線）の構成になります。一方、無線 LAN では見た目上はスター型でも、実際の通信は共有された電波を介して行われます。つまり無線 LAN では**通信媒体を共有**しているため、一度に通信できる帯域を複数端末で分け合うことになります（これを**半二重通信**と呼びます）。有線 LAN のスイッチ接続では通常各ポートが専有帯域を持つ**全二重通信**（同時送受信可能）であり、衝突無く通信できます。

必要な機器の違い

- **有線 LAN に必要な機器:** 主に **LAN ケーブル**と**スイッチングハブ（スイッチ）です。各端末は LAN ケーブルでスイッチに接続されます。また外部ネットワークに出るにはルーター**が必要です。小規模環境では市販のブロードバンドルーターがスイッチ機能も内蔵している場合が多いです。
- **無線 LAN に必要な機器: アクセスポイント（AP）と、AP と有線側を繋ぐルーター**が必要です。一般的な Wi-Fi ルーターは、この AP とルーターの機能を一体化したものです（加えて内部にスイッチも持ち、LAN ポートが複数出ています）。企業環境では AP とルーターは分離され、複数の AP を**有線 LAN** 経由で一つのルータやコントローラに接続する構成をとります。

通信の特徴と使い分け

- **有線 LAN の特徴:** 高速かつ安定した通信が可能で、遅延も小さく、外部の電波干渉を受けません。大容量のデータ転送や遅延にシビアな用途（例えば動画配信サーバ、オンラインゲームの通信など）に適しています。ただし機器の配置替えや増設の際にはケーブル配線が必要になるため柔軟性に欠けます。
- **無線 LAN の特徴:** 配線不要で端末の持ち運び自由度が高く、スマートフォンなどモバイル機器の接続に欠かせません。一方で電波状況（距離、障害物、他の Wi-Fi との干渉）により速度低下や通信不安定が起こることがあります。また同一 AP に多数の端末が接続されるとスループット（実効速度）が頭打ちになる場合もあります。そのため無線 LAN は利便性が高い反面、安定性や速度の点で有線 LAN を完全には置き換えられないケースもあります。

使い分けのポイント: 基本的に、動かせない機器や高信頼・高速度が求められる通信には有線 LAN を、モバイル機器や配線困難な場所には無線 LAN を利用すると良いでしょう。現代のネットワークはこの両者を組み合わせて設計されるのが一般的です。

5. ルータとスイッチの基本機能

ネットワークを構成する上で重要な**ネットワーク機器**として**ルータ**と**スイッチ**があります。それぞれ役割が異なり、適切に理解することが大切です。この章ではルータとスイッチの基本機能と違いについて説明します。

ルータとスイッチの役割の違い

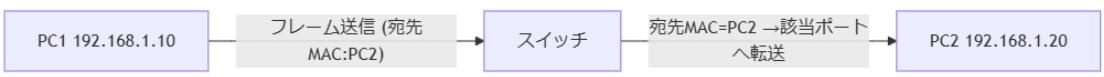
- **スイッチ（レイヤ 2 スイッチ）: LAN 内部の機器同士**を接続するための装置です。スイッチは受け取ったフレーム（データリンク層のデータ）の宛先 MAC アドレスを見て、適切なポートに転送します。ネットワーク内の各機器の MAC アドレスと接続されたポートの対応表（**MAC アドレステーブル**）を学習し、LAN 内の通信を効率よく行います。スイッチを使うことで各機器は直接通信したい相手だけと通信でき、不要なデータが他に漏れない仕組みになっています。原則としてスイッチは同一ネットワーク内（同一 IP サブネット内）の通信に用いられます。
- **ルータ: 異なるネットワーク間**を接続し、中継するための装置です。ルータは受け取ったパケット（ネットワーク層のデータ）の宛先 IP アドレスを見て、どのネットワークに転送すべきかを判断します。先述の通りルータはルーティングテーブルを持ち、宛先ネットワークごとの転送先（次ホップ）を管理しています。例えば社内 LAN とインターネットを接続するブロードバンドルーターは、社内向け（LAN 側）は内部に送り、その他（インターネット側宛）は WAN 側ポートに転送するといった動作をしています。また、多くのルータは IP アドレスを変換する **NAT 機能**や簡易なファイアウォール機能を備え、ネットワーク間の境界でセキュリティを提供する役割も担います。

簡単に言えば、**スイッチは LAN 内の交通整理役、ルータは LAN と外部（または LAN 同士）の橋渡し役**です。例えば家庭用の Wi-Fi ルーターの内部を見ると、LAN 側はスイッチ（複数の有線 LAN ポート）と無線 AP があり、それらをまとめて WAN 側（インターネット）へ中継する部分がルータになっています。

通信の流れの違い（スイッチ vs ルータ）

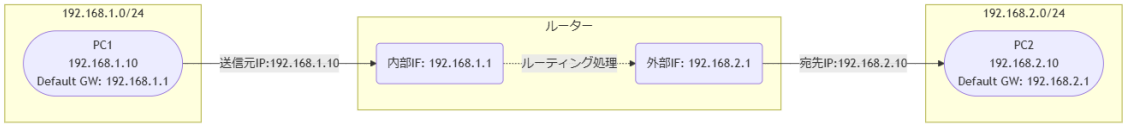
スイッチとルータで通信データの流れるイメージを比較してみます。

スイッチによる LAN 内通信: スイッチに接続された PC 同士が通信する場合、データはイーサネットフレームとして送信されます。送信元 PC は宛先 PC の MAC アドレスをフレームに記載し、スイッチに送ります。スイッチは自分の MAC アドレステーブルを参照し、その宛先 MAC が繋がっているポートがどれかを調べ、そのポートだけにフレームを転送します。こうして他のポートには不要なデータは流れず、宛先 PC だけがそのフレームを受け取ります。宛先 PC は自分宛の MAC アドレスがついたフレームを受信し、中身の IP パケットを処理します。同じネットワーク内であればルータを経由せず、このようにスイッチ内で通信が完結します。



上記の図では、PC1（IP:192.168.1.10）が PC2（192.168.1.20）にデータを送る際、スイッチ A が宛先 MAC（PC2 の MAC アドレス）を見て PC2 のポートにデータを届ける様子を示しています。

ルータによるネットワーク間通信: 異なるネットワークにいる PC 同士が通信する場合、データは送信元 PC のネットワークからルータに送られ、ルータで宛先ネットワークへ転送されます。例えば PC1(192.168.1.10)が別ネットワークの PC3(192.168.2.10)に通信する場合、PC1 はまず自分のデフォルトゲートウェイ（例:192.168.1.1）宛にパケットを送ります。スイッチ A を経由してルータに届いたパケットは、宛先 IP が 192.168.2.0/24 ネットワークであると判断され、ルータの別インタフェース（192.168.2.1 など）からネットワーク 2 側に転送されます。ネットワーク 2 側のスイッチ B を介して最終的に PC3 に届けられます。このように、ルータは IP アドレスに基づいてパケットを別ネットワークへ中継します。



図では、Network1 に属する PC1 から Network2 に属する PC3 へ通信する際に、ルーターR1 が両ネットワーク間でパケットを中継している様子を示しています。ルータは Network1 側に 192.168.1.1、Network2 側に 192.168.2.1 といった IP を持ち、それぞれのネットワークに参加しています。PC1 からのパケットを受け取った R1 は、宛先が 192.168.2.x であるため、自身の Network2 側インタフェースからそのネットワークにパケットを送り出し、PC3 に届けます。

ネットワーク機器選択時の注意

新人エンジニアとしては、シチュエーションに応じてルータとスイッチを正しく選択・配置することが重要です。LAN 内の機器増設にはスイッチを、ネットワーク間の中継やインターネット接続にはルータを使用します。また、昨今では**レイヤ 3 スイッチ**と呼ばれる高機能スイッチも存在し、これはスイッチにルーティング機能を統合したものです。大規模ネットワークでは L3 スイッチによって LAN 内の VLAN 間ルーティングを行い、外部接続は専用ルータで行うといった構成もあります。しかし基本的な原理は変わりませんので、まずはシンプルなスイッチとルータの動きを押さえておきましょう。

6. DHCP・DNS・NAT の基礎

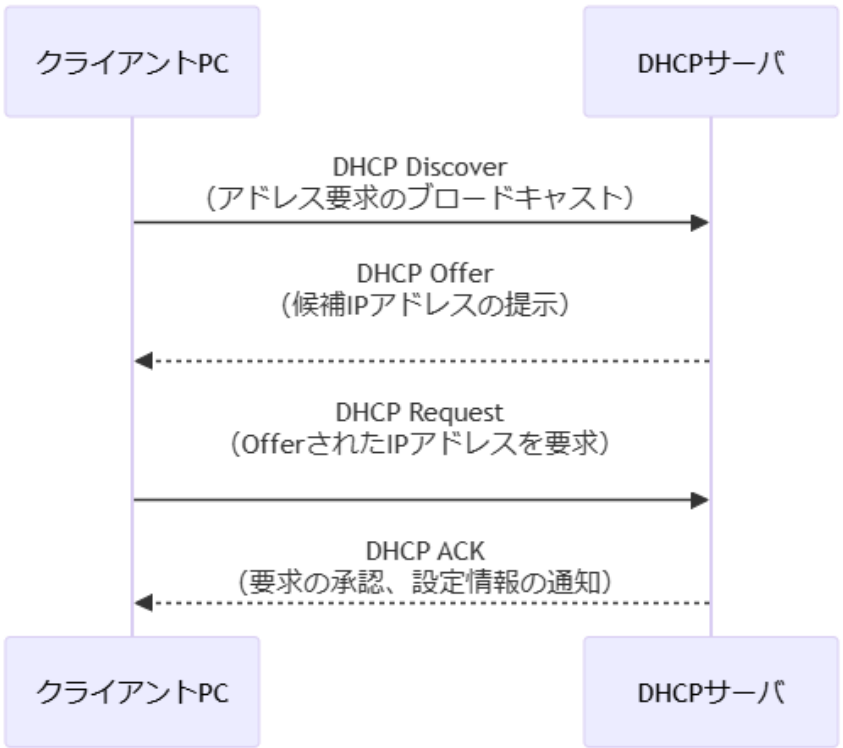
ネットワークが実際に動作するためには、各種の**ネットワークサービス**や**プロトコル**が重要な役割を果たしています。この章では、特に基本的かつ重要な「DHCP」「DNS」「NAT」という 3 つの仕組みについて、その目的と動作を解説します。

DHCP の基礎

DHCP（ディーエイチシーピー: Dynamic Host Configuration Protocol）は、ネットワークに接続された端末に対して、IP アドレスやサブネットマスク、デフォルトゲートウェイ、DNS サーバなどのネットワーク設定を自動的に割り当てるためのプロトコルです。DHCP サーバと呼ばれるサーバ（もしくはルータ内蔵の機能）がネットワーク上に存在し、各クライアント（PC やスマホ）は DHCP サーバと通信することで自身の設定を取得します。

DHCP を使うことで、管理者が手動で各端末に IP を設定する手間が省け、IP アドレスの重複設定ミスなども防止できます。例えばオフィスのネットワークに新しい PC を接続した際、DHCP が動作していれば自動的に未使用の IP アドレスが割り当てられ、すぐにネットワークを利用できるようになります。

DHCP の動作概要: クライアントとサーバ間の通信は以下の 4 つのステップで行われます（**DORA** と覚えます）。



1. **Discover（探索）:** クライアントがネットワーク上に DHCP サーバを探すための

ブロードキャストメッセージを送ります。「誰か IP アドレスをくれませんか？」という呼びかけです。

2. **Offer（提供）:** DHCP サーバはそれを受け取ると、割り当て可能な IP アドレスを選んでクライアントに提案します。「あなたにはこの IP を提供できます」という応答を返します。
3. **Request（要求）:** クライアントは提案された IP アドレスを使いたい旨をリクエストとしてサーバに送ります。複数サーバから Offer が来た場合、一つを選んで Request します。
4. **ACK（承認）:** DHCP サーバは Request を受けると、そのクライアントにその IP アドレスを確保したことを ACK 応答で知らせます。同時にサブネットマスクやデフォルトゲートウェイ、DNS サーバ情報といった付随のネットワーク設定もクライアントに提供します。

このやり取りによって、クライアント PC は IP アドレス設定を自動で完了します。DHCP で割り当てられた IP アドレスには有効期限（リース期間）があり、クライアントは定期的に延長要求を行い、使われなくなった IP はサーバに戻され再利用されます。

実際の環境でクライアントの IP 設定を確認すると、DHCP から取得した情報が確認できます。例えば Windows のコマンドプロンプトで ipconfig コマンドを実行すると以下のように表示されます。

```
C:¥> ipconfig

   IPv4 Address. . . . . . . . . . . : 192.168.1.100

   Subnet Mask . . . . . . . . . . . : 255.255.255.0

   Default Gateway . . . . . . . . . : 192.168.1.1

   DNS Servers . . . . . . . . . . . : 192.168.1.1
```

この例では、192.168.1.100 という IP アドレスが DHCP によって払い出され、ゲートウェイや DNS も自動設定されています。

DNS の基礎

DNS（ディーエヌエス: Domain Name System）は、ドメイン名と IP アドレスを相互に変換する仕組みです。我々がウェブブラウザに入力する「www.example.com」のような人間に読みやすい名前を、コンピュータが通信に使う IP アドレス（例えば 93.184.216.34）に変換する役割を担っています。

DNS がないと、ユーザはサイトにアクセスするのに「93.184.216.34」のような数字を直接入力しなければならず非常に不便です。DNS はインターネットにおける「電話帳」のような役割を果たし、名前から番号（IP）を引き当てたり、その逆を行ったりします。

DNS の仕組み概要:

- 各端末には利用する DNS サーバの IP アドレスが設定されています（通常は DHCP で自動配布、もしくは手動設定）。例えば 192.168.1.1（ルータが DNS プロキシになる場合）や ISP 提供の DNS サーバ、公共 DNS（8.8.8.8 など）が使われます。

- ユーザがブラウザで「www.example.com」にアクセスしようとすると、PC はまず自分の DNS サーバに対し「www.example.com の IP を教えてください」というクエリを送ります。
- DNS サーバは自分がその名前を知っていればすぐに IP を返答します。知らない場合は、他の上位の DNS サーバに問い合わせ（再帰的問い合わせ）を行い、最終的に対応する IP アドレスを突き止めてクライアントに返答します。
- クライアント PC は受け取った IP アドレス（例: 93.184.216.34）宛に通信を開始し、目的のウェブサイトに接続できます。

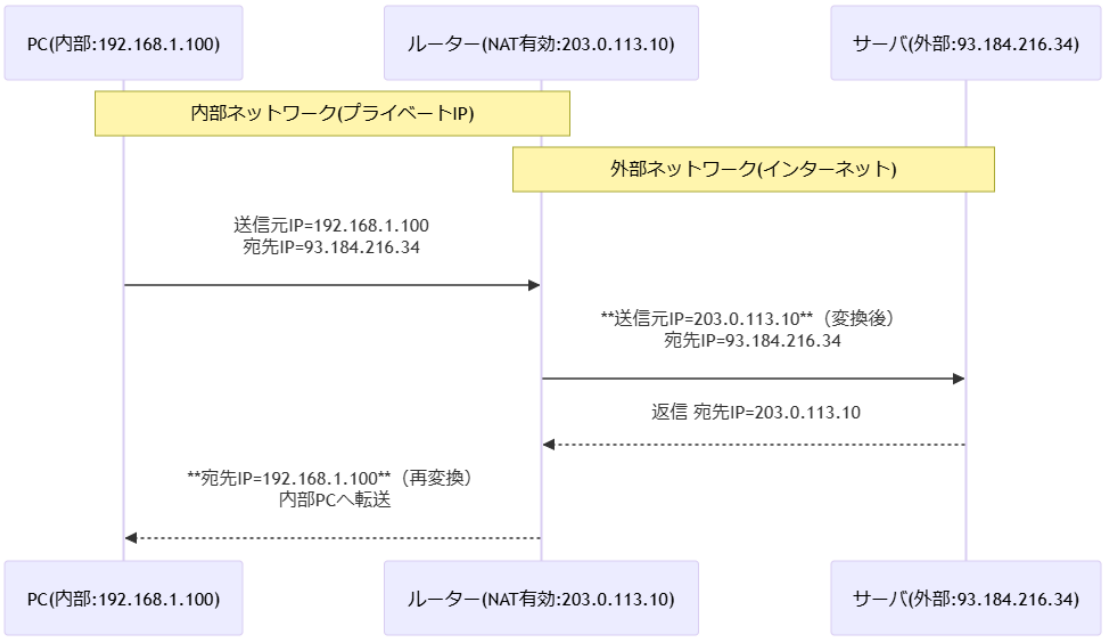
上記シーケンスは、PC が DNS サーバに対して名前解決を行う様子を示しています。DNS サーバは階層構造になっており、ルート DNS、TLDDNS、権威 DNS などを経て最終回答を得ますが、新人向けにはまず「DNS サーバに問い合わせると名前から IP が得られる」という点を押さえれば十分です。

DNS の補足: DNS には正引き（名前→IP）だけでなく逆引き（IP→名前）もあります。また、大規模なネットワークでは DNS サーバを冗長化したり、レスポンスを高速化するためにキャッシュ DNS サーバを設置したりします。DNS はネットワーク利用者にはあまり意識されませんが、裏で常に動いている重要なサービスです。

NAT の基礎

NAT（ナット: Network Address Translation）は、**ネットワークアドレス変換**とも呼ばれ、ネットワーク内部と外部で IP アドレスを変換する技術です。特に IPv4 アドレスの枯渇問題への対策として広く使われており、家庭や企業のルータはほぼ例外なく NAT 機能を備えています。

一番身近な NAT の例は、**家庭用ルータでのインターネット接続**です。自宅内の PC やスマホはプライベート IP（例:192.168.1.100 など）を持っていますが、そのままではインターネット上のサーバ（グローバル IP）と通信できません。そこで自宅ルータが NAT を行い、内部から外部への通信の際、送信元 IP アドレスを書き換えます。具体的には、例えば PC(192.168.1.100)からインターネット上のサーバ(93.184.216.34)に



アクセスするとき、ルータは送信元アドレス 192.168.1.100 を自分の持つグローバル IP（例えば 203.0.113.10）に変換して送り出します。戻ってきた応答については、宛先が自分のグローバル IP 宛になっているのを見て、対応する内部アドレス 192.168.1.100 に宛先を書き換えて LAN 内に転送します。これにより、多数の内部端末が少数のグローバル IP（多くの場合 1 つ）を共有してインターネットアクセスできるようになります。

上図は NAT（正確には NAPT、ポートも含めた変換）の動作を示しています。ルータ NAT は内部 PC ごとに通信のセッションを識別し、送信元アドレスとポート番号をグローバル側に置き換えて通信します。これにより外部からは多数の端末が **1 つのグローバル IP** から通信しているように見えます。

NAT の利点: IP アドレス節約の他に、内部ネットワークの端末が直接インターネットから見えなくなるため**セキュリティ向上**の効果もあります。外部から内部への直接通

信はデフォルトではできないため、不正アクセスのリスクを下げられます（必要な場合はポート開放やポートフォワーディング設定で特定の内部機器を公開します）。

注意: NAT 環境では、一部のアプリケーション（例えば P2P 通信やオンラインゲームなど）で特別な設定を必要とする場合があります。また、企業の拠点間通信などでは NAT を使わずグローバル IP を直接ルーティングするケースもあります。基本的な仕組みとして、NAT は「多数のプライベート IP を一つ（または限られた）のグローバル IP に見せかける」技術であると覚えておきましょう。

7. 無線 LAN セキュリティ

無線 LAN は便利である一方、電波を使う特性上、セキュリティに注意を払わなければなりません。この章では無線 LAN の基本的なセキュリティ対策と仕組みについて解説します。

無線 LAN における脅威

有線 LAN では物理的に接続しないとネットワークに参加できませんが、無線 LAN では電波が届く範囲にいれば理論的には誰でも信号を受信できます。そのため、適切に保護されていない Wi-Fi ネットワークでは、以下のような脅威があります。

- **盗聴:** 暗号化されていない Wi-Fi 通信（オープンな無線 LAN）では、第三者に通信内容を傍受される可能性があります。インターネット閲覧の内容や入力したパスワード等が漏洩する危険があります。
- **不正アクセス:** 無線 LAN に認証なしで接続できる状態だと、悪意ある人物がネットワークに侵入し、他の機器にアクセスしたり、インターネット経由で不正行為を働いたりする恐れがあります。
- **なりすまし:** 攻撃者が正規のアクセスポイントになりすまして（**悪意のあるホットスポット**）、ユーザを誘導し通信を傍受・改竄する（中間者攻撃）といった手口も考えられます。

暗号化と認証による保護

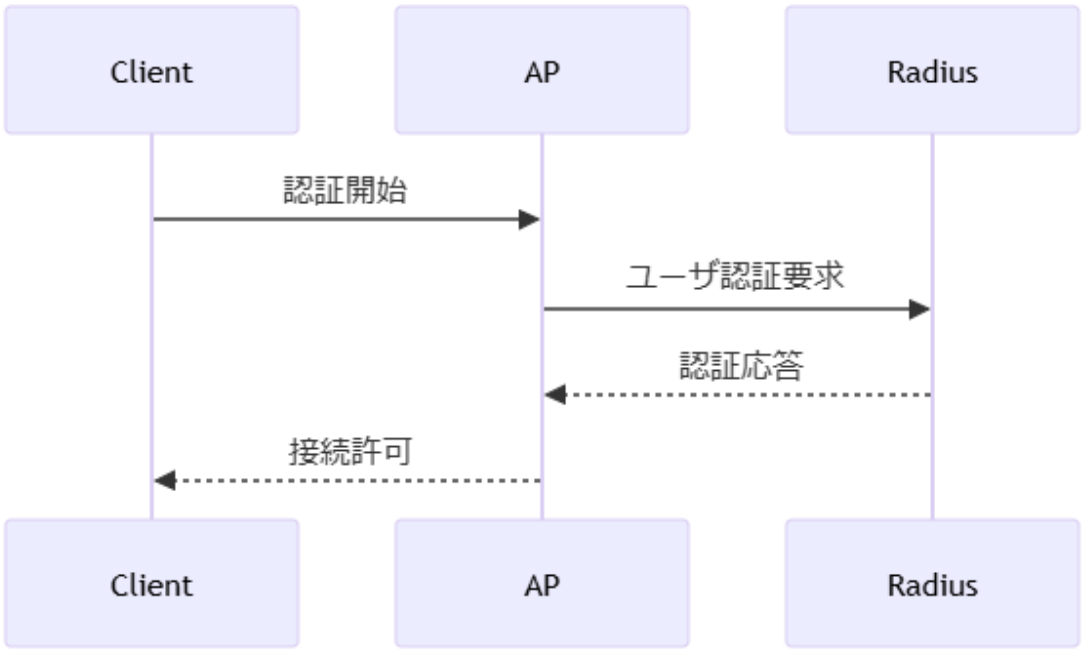
無線 LAN のセキュリティでもっとも基本となるのが、**暗号化されたセキュアな接続**を使うことです。現在一般的な Wi-Fi ルーターやアクセスポイントでは、以下のようなセキュリティモードが選択できます。

- **WEP (Wired Equivalent Privacy):** 古い方式の暗号化。鍵（パスワード）の強度にもよりますが、既に脆弱性が発見されており、ツールを使えば比較的容易に解読されてしまいます。**現在では使用非推奨**です。
- **WPA/WPA2 (Wi-Fi Protected Access):** WEP の後継として標準化された暗号化方式で、TKIP や AES といった暗号プロトコルを使います。特に **WPA2-AES** は長らく強固なセキュリティを提供してきました。家庭用では事前共有鍵（パスフレーズ）方式が一般的です。
- **WPA3:** 最新の Wi-Fi セキュリティ規格で、より強力な暗号化手法（SAE: Simultaneous Authentication of Equals）を採用しています。WPA2 の脆弱性を改善し、パスワードに対するオフライン辞書攻撃への耐性などが向上しています。

現状では **WPA2-PSK (AES) または可能なら WPA3** を使用し、十分に推測されにくい強度の高いパスフレーズを設定することが必要最低限のセキュリティ対策です。アク

セスポイントに初期設定で弱いパスワード（例えば「password」や電話番号など）を使っていると、破られる可能性が高まります。

また、企業などでは **802.1X 認証**を用いた WPA2-Enterprise/WPA3-Enterprise モードが使われます。これは認証サーバ（RADIUS サーバ）と連携し、各ユーザごとに認証（証明書や ID/パスワード）を行ってネットワーク接続を許可する仕組みです。エンタープライズモードでは一人ひとりに異なる資格情報が与えられるため、社員の入れ替わりなどでも対応しやすく、セキュリティを高く保てます。



その他の無線セキュリティ対策

暗号化以外にも、無線 LAN の安全性を高めるための設定や対策があります。

- **SSID の隠蔽（ステルス SSID）:** アクセスポイントのネットワーク名(SSID)をブロードキャストしないように設定できます。隠したからといって安全になるわけではありませんが、目に見えるネットワークが減るため攻撃対象になりにくくする効果は多少あります。ただし専門的なツールを使えば隠れた SSID も検出されてしまうため、過信は禁物です。
- **MAC アドレスフィルタリング:** 無線 LAN に接続してくる端末の MAC アドレスをあらかじめ登録しておき、リストにない端末からの接続を拒否する方法です。管理コストがかかる割に、MAC アドレスは偽装可能なため、これも強い防御策ではありません。**補助的な手段**として使われます。
- **電波出力の調整と物理的対策:** 電波の出力を必要以上に強くしない（必要なエリアを少し出るくらいに抑える）ことで、建物の外に電波が漏れにくくし、外部からの不正接続リスクを下げることができます。また、AP を物理的に安全

な場所に設置し、リセットボタン等から不当に設定初期化されないようにすることも重要です。

公衆無線 LAN 利用の注意

新人エンジニア個人としても、公衆無線 LAN（フリーWi-Fi スポットなど）を利用する際にはセキュリティに気を付ける必要があります。暗号化されていないネットワークでは機密情報のやり取りは避ける、VPN（仮想プライベートネットワーク）を利用して通信を暗号化する、怪しいアクセスポイントには接続しない、といった心構えが大切です。

無線 LAN のセキュリティは、設定項目が多岐にわたるため最初は難しく感じるかもしれません。しかし**「暗号化による保護」と「適切な設定管理」**というポイントを押さえておけば、大きな間違いは避けられます。常に最新のセキュリティ情報にも目を配り、ルータのファームウェア更新なども怠らないようにしましょう。

8. VLAN とルーティングプロトコルの概要

この章では、ネットワークのより発展的な概念として**VLAN** と**ルーティングプロトコル**について概要を学びます。これらは中級以上のトピックですが、概要を理解しておくことでネットワーク設計や運用の幅が広がります。

VLAN の概要

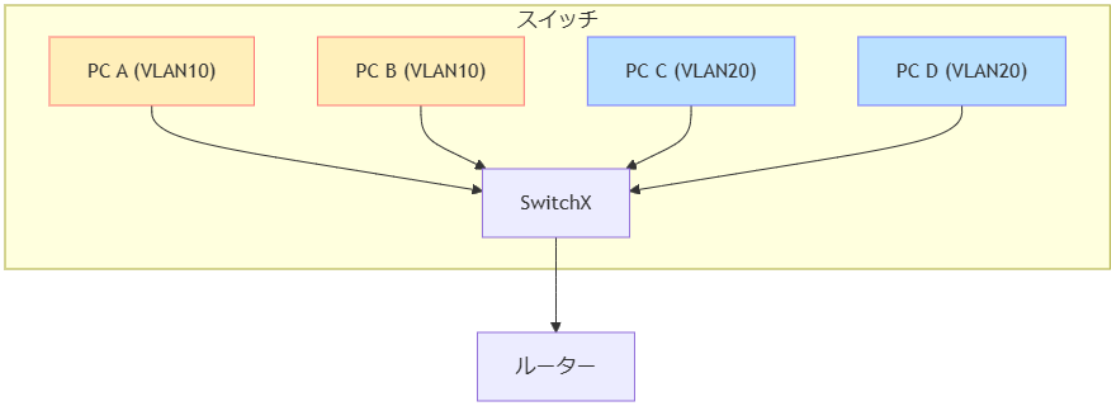
VLAN（ブイラン: Virtual LAN）は、スイッチ上で論理的にネットワークを分割する技術です。物理的には同じスイッチや LAN 上に接続されている機器を、設定によって複数の仮想的な LAN に分けることができます。こうすることで、ネットワークを論理的に分離し、セキュリティ向上やトラフィック制御、柔軟なネットワーク構成を実現できます。

VLAN の主なポイント:

- VLAN ごとに別のネットワーク（IP サブネット）を構成し、原則として同じ VLAN 内の機器しか直接通信できません。異なる VLAN 間の通信は、ルータもしくは L3 スイッチで中継する必要があります。
- 一つのスイッチで複数の独立した LAN を実現できるため、機器の配置換えや部門追加などの際にもケーブル配線を変えずに論理構成を変更できます。
- VLAN には ID（番号）を割り振ります。例えば「VLAN10=営業部 LAN、VLAN20=開発部 LAN」のように決めておき、スイッチのポート毎にどの VLAN に所属させるか設定します。これにより、営業部と開発部の PC は同じスイッチにつながっていても別ネットワークとして隔離されます。

例えば、下図のように 1 台のスイッチに 4 台の PC が接続されている状況で、VLAN によって 2 つのグループにネットワークを分離することができます。

上記の図では、vSwitch(Virtual Switch)上で VLAN10（黄色）と VLAN20（青色）が設定され、それぞれ PC A/B、PC C/D が所属しています。同じ色同士（同じ VLAN）の PC はスイッチ上で直接通信できますが、異なる色（別 VLAN）同士の通信はスイッチ内では遮断されます。代わりに、スイッチから接続された Router（ルーターまたは L3 スイッチ）が VLAN 間を中継する役割を果たします。Router は VLAN10 用と VLAN20 用にそれぞれインタフェース（またはサブインタフェース）を持ち、両ネットワークに参加してルーティングを実施します。



VLAN の利点と使用例:

- セキュリティ: 部門間や役割間でネットワークを分離し、不用意なアクセスを防ぐ（例: ゲスト用 Wi-Fi を社内 LAN とは別 VLAN にする）。
- トラフィック制御: ブロードキャストドメイン（ネットワーク内のブロードキャストが届く範囲）を分割し、無関係なブロードキャストが他部署に飛ばないようにする。
- 柔軟性: 物理配置に縛られずネットワークグループを構成できる（設定変更で対応可能）。

VLAN を使うには、スイッチやルータが VLAN 機能（IEEE802.1Q タグなど）に対応している必要があります。ほとんどの企業向けスイッチは対応していますが、廉価なアンマネージドスイッチ（設定機能のないスイッチ）では VLAN は使えません。新人エンジニアとしては、まず「VLAN＝仮想的にスイッチを分割して別ネットワークを作る仕組み」と理解しておき、実際の設定や運用については徐々に経験を積んでいくとよいでしょう。

ルーティングプロトコルの概要

ネットワーク間を接続するルータ同士が、お互いに経路情報を交換するためのルールが**ルーティングプロトコル**です。前章までで扱ってきたルーティングは、主にスタティック（静的）なものでした。スタティックルートでは管理者が手動で「この宛先ネットワークはあのルータへ」と設定します。一方、ネットワーク規模が大きくなると手動設定は煩雑になるため、ルータ同士が自動的に情報交換して経路を学習・更新する仕組みが用いられます。

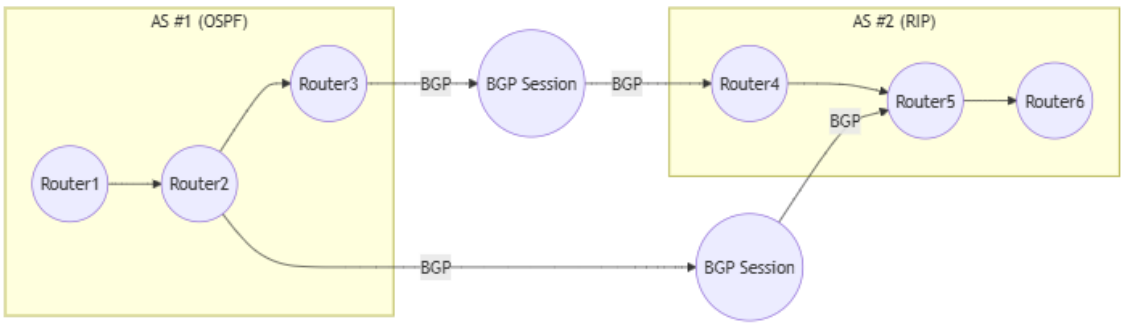
主なルーティングプロトコル:

- **RIP (Routing Information Protocol):** 古典的なプロトコルで、小規模向き。ホップ数を指標に経路選択しますが、遅収束やホップ数制限(最大 15 ホップ)など制約があります。
- **OSPF (Open Shortest Path First):** 中〜大規模ネットワークで広く使われるプロトコル。リンク状態型で、各ルータがお互いの接続状況を伝え合い、最短経路を計算します。収束が速くスケーラブルで、多数のルータが参加する企業ネットワークで標準的に採用されています。
- **BGP (Border Gateway Protocol):** 主にインターネット（AS と AS の間）で使われる経路制御プロトコル。経路のポリシー制御が可能で、ISP 間の経路選択などに利用されています。企業内というより、インターネット全体の経路交換に使われる特殊な例ですが、ネットワークエンジニアなら名前は覚えておくべきでしょう。

これら以外にも EIGRP（シスコ独自)、IS-IS（主に通信事業者で利用）など様々なルーティングプロトコルがありますが、まずは **OSPF** が内部向けプロトコルの代表、**BGP** が外部向けの代表と覚えておくと良いです。

ルーティングプロトコルの動作イメージ: 例として OSPF では、ネットワーク内の各ルータがお互いに **LSA**(Link State Advertisement)というパケットを送信して、自身に繋がるネットワークやルータの情報を知らせ合います。全ルータがリンク状態のデータベースを持ち、それを基にアルゴリズム（Dijkstra の最短経路木）で経路を計算します。障害が起きてリンクがダウンすると、直ちにその情報がネットワーク内に知れ渡り、各ルータが経路を再計算して新しいルートに切り替えます。これにより動的に最適なルーティングが維持されます。

新人レベルでは、詳細なプロトコルの仕組みよりも**「ルータ同士が自動で経路情報をやり取りしている」**ことを理解する程度で十分です。小規模ネットワークでは静的ルート設定で済む場合が多いですが、将来的に大規模ネットワークや ISP 関連の業務に携わるなら、OSPF や BGP の知識が必要となるでしょう。



9. ネットワーク設計と機器選定

ネットワークの基礎知識を踏まえ、実際にネットワークを設計する際の考え方と、適切な機器を選定するポイントについて解説します。新人エンジニアが最初に任されるネットワーク構築は、小規模なオフィス LAN や部門 LAN であることが多いですが、基本的なアプローチは規模に関わらず共通です。

ネットワーク設計のポイント

1. **要件定義:** まず、ネットワークを利用する目的と要件を明確にします。例えば「社員 50 名が利用する社内ネットワーク」「来客用のゲスト Wi-Fi を提供」「社内サーバへのアクセスとインターネット接続を提供」等です。必要な接続台数、アプリケーションの種類、必要な帯域（スループット）、カバーすべき物理範囲（フロアや建物）などを洗い出します。

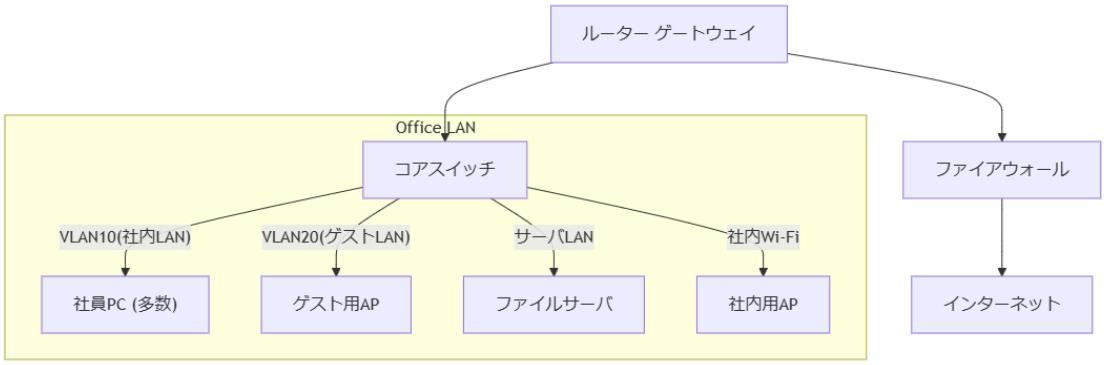
2. **ネットワーク構成の設計:** 要件を満たすネットワークの構成を考えます。有線・無線 LAN の組み合わせ、どこにスイッチや AP を配置するか、どのようにルータで接続するかを決めます。中小規模ではシンプルに 1 台のルータと必要な数のスイッチ・AP という構成でしょう。部署ごとにネットワークを分ける必要があれば VLAN の設計も行います。また将来的な拡張（例えば人数増加や機器追加）も見越し、余裕あるポート数や IP アドレス計画を立てます。

3. **IP アドレス・ネットワークアドレス設計:** IP アドレスの範囲を決め、サブネットを設計します。小規模で一つの LAN なら 192.168.x.0/24 をひとつ使う程度ですが、部門別に VLAN で分けるならそれぞれに /24 を割り振るなど計画します。**アドレス計画表**を作って、どの機器にどの IP を割り当てるか（静的 IP が必要なサーバやプリンタ、DHCP レンジの範囲など）を整理しておくと管理が容易です。

4. **トポロジー設計:** 機器間の接続構成（トポロジー）を図に描いてみます。スイッチとルータの接続関係、冗長構成を取るなら冗長リンクや予備機も含めて示します。中規模以上では**コア・ディストリビューション・アクセス**層の三層モデルを考慮する場合もありますが、小規模なら単一のスイッチ層で十分です。

5. **セキュリティと管理:** ファイアウォールの設置、無線 LAN の暗号化設定、各機器の管理アクセス方法（例: ルータの管理画面にパスワード設定、SNMP 有効化等）も設計段階で検討します。特にインターネットと接続するネットワークでは、**外部から内部への不正アクセス防止**が重要なので、ルータの ACL 設定や UTM の導入なども検討に入ります。

以上を経て、一連のネットワーク構成図と仕様書を作成し、それに基づいて機器を用意・設定する流れになります。下図は、小規模オフィスネットワークの一例を示したものです。



この図では、中央にコアスイッチを置き、社員 PC や社内 Wi-Fi AP、ゲスト Wi-Fi AP、ファイルサーバなどがぶら下がっています。ルーターが上流でインターネット（ISP）に接続し、必要に応じてファイアウォールを経由しています。また、社員 LAN とゲスト LAN を VLAN で論理分離している例です。実際の構成は環境に応じて様々ですが、**ネットワーク図を書くこと**は設計内容を確認する上で非常に有効なので、新人のうちから練習しておくとよいでしょう。

機器選定のポイント

ネットワーク機器（ルータ、スイッチ、アクセスポイント等）を選ぶ際には、以下の観点を考慮します。

- **性能と規模:** 接続する端末数や要求される通信速度に耐えられるスペックか確認します。スイッチであればポート数、ポート速度(Gigabit, 10Gig など)、バックプレーン帯域。ルータであればスループット（NAT 処理能力や VPN 処理能力)、同時セッション数、メモリ量。AP であれば対応する Wi-Fi 規格(802.11ac/ax など)、同時接続端末数の目安、帯域幅などです。例えば 50 人が使うオフィスなら企業向けの高性能 AP を複数台設置する、などが必要になります。
- **機能:** 企業ネットワークでは VLAN や PoE(Power over Ethernet)給電、SNMP 管理、ループ検知、QoS など様々な機能が求められます。スイッチには**レイヤ 2 スイッチ**と**レイヤ 3 スイッチ**がありますが、小規模なら L2 で十分な場合も多いです。ルータには VPN 接続機能、ファイアウォール機能、NAT 越え機能、冗長構成対応（VRRP 等）などを備えるものがあります。自分たちのネットワークに必要な機能を洗い出し、それを満たす機器を選定します。
- **信頼性とサポート:** 重要なネットワークでは、機器の冗長構成（予備機や二重化）が求められます。加えて、ベンダーのサポート体制や保守契約も考慮します。障害発生時にすぐ交換対応してもらえるか、ファームウェア更新が安定提供されているか、ドキュメントは充実しているか等です。有名メーカー（シスコ、アライド、ヤマハ等）の製品は値段が高い反面、信頼性と情報の豊富さで安心感があります。一方、小規模・低予算なら民生用上位機種や中堅メーカーの製品も検討します。
- **コスト:** 予算内で最大の効果が得られる構成を目指します。高機能な機器ほど高価になるので、本当にその機能が必要か吟味します。例えば将来の拡張を見据えて高価な L3 スイッチを入れるより、当面は安価な L2 スイッチ＋必要にな

った時にルータを追加、の方が良い場合もあります。見積を取り、費用対効果を比較検討しましょう。

機器選定の実例: 先ほどの小規模オフィスを例にすると、以下のような機器リストが考えられます。

- ルータ: N 社製の UTM 一体型ルータ（1Gbps 対応、VPN 機能あり）を 1 台。
- スイッチ: 24 ポートギガビット L2 スイッチ（PoE 対応、VLAN 対応）を 1 台。
- 無線 AP: 天井取付型のデュアルバンド対応 AP を 2 台（社員用とゲスト用、各 SSID 別 VLAN 紐付け）。
- ファイアウォール: ルータに内蔵されていれば省略。必要なら専用ファイアウォールを追加。
- その他: 予備のスイッチ 1 台（故障時の即時交換用）、ラックや配線モール、UPS（無停電電源）などの付帯設備。

選定後は、各機器の設定を行い実際にネットワークを構築します。**ドキュメント化**（構成図、IP リスト、設定手順書）は後日のトラブル対応や拡張時に役立つので必ず残しておきましょう。

10. トラブルシューティング

ネットワーク運用において、**トラブルシューティング（障害対応）**は避けて通れない重要なスキルです。この章では、ネットワークに問題が発生した際に新人エンジニアが取るべき基本的な対応の流れと、よくある問題例について紹介します。

トラブルシューティングの基本アプローチ

ネットワーク障害の原因を突き止め復旧するには、体系立てたアプローチが有効です。以下のステップを踏みながら問題を切り分けていきます。

1. **現象の確認:** まず具体的に何が「できない」のかを明確にします。例：「インターネットに接続できない」「特定のサーバにアクセスできない」「無線 LAN に繋がらない」など。また影響範囲も確認します。一台の PC だけなのか、複数のユーザが同様の問題か、全社的か。
2. **物理層・接続の確認:** 次に基本中の基本として、物理的な接続状況をチェックします。有線ならケーブルが抜けていないか、ポートのリンクランプは点灯しているか。無線なら端末が SSID に接続済みか、電波強度は十分か等。また端末側の Wi-Fi スイッチがオフになっている、ケーブル断線など意外と初歩的な原因も多いので見逃さないようにします。
3. **IP アドレス設定の確認:** 端末が正しい IP アドレスを取得・設定できているか確認します。ipconfig（Windows）や ifconfig/ip addr（Linux）コマンドで IP、サブネットマスク、デフォルトゲートウェイをチェックします。ここで IP が割り当てられていない、もしくは誤ったアドレスになっている場合、DHCP サーバの問題や設定ミスが疑われます。例えば 169.254.x.x のようなアドレスになっていたら、DHCP サーバと通信できず APIPA と呼ばれる自動アドレスが振られた状態です。
4. **経路の疎通確認（疎通テスト）:** IP が正しく設定されていれば、次はネットワーク経路のどこで問題が起きているか調べます。典型的には **ping** コマンドを使

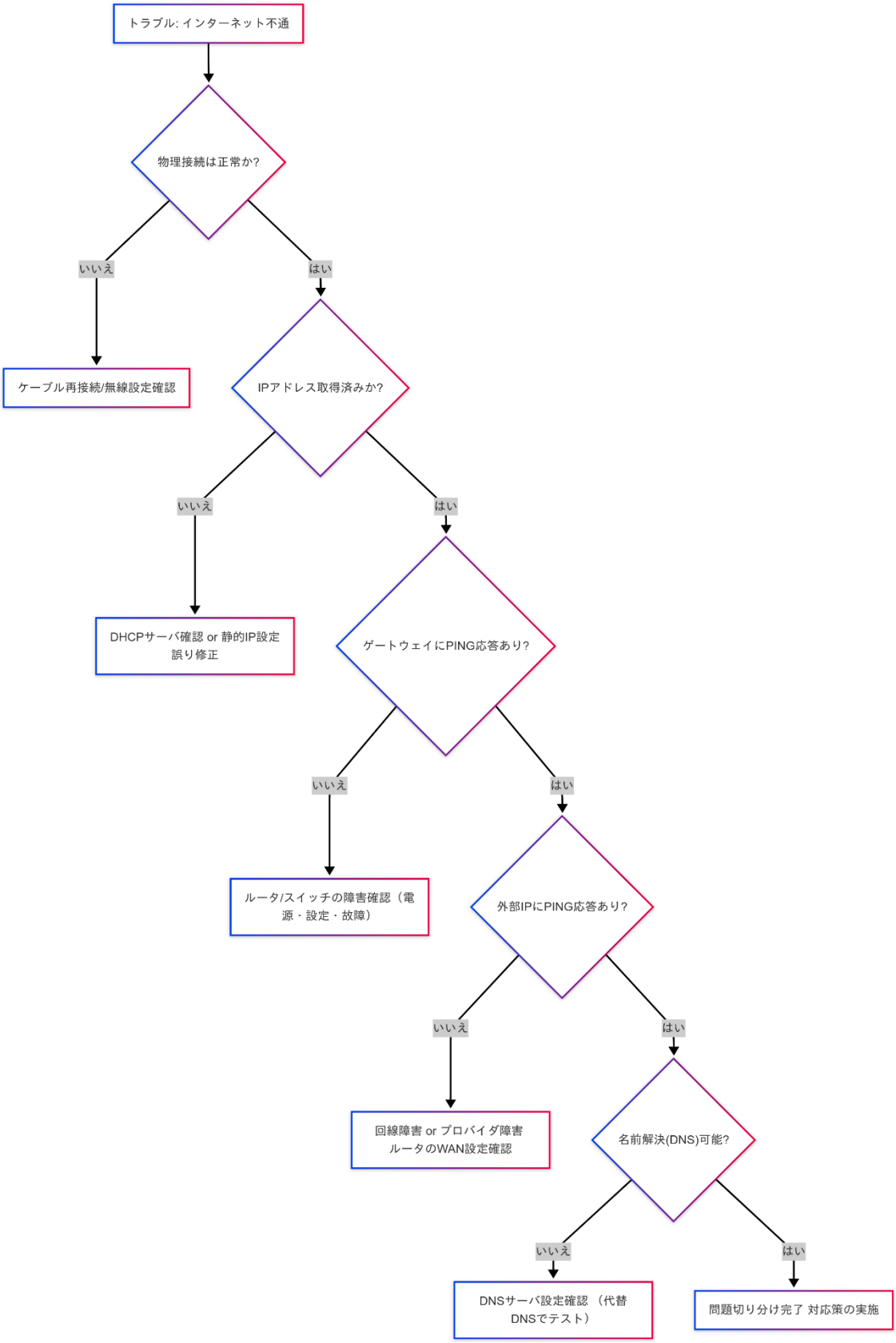
った疎通確認です。まずデフォルトゲートウェイ（ルータ）に ping を実行します。ping 192.168.1.1 など。ここが応答しなければ LAN 内部の問題です（ルータ故障、スイッチ不良、ケーブル断など）。

    - ゲートウェイに ping が通れば、次にインターネット上の安定した IP（例えば 8.8.8.8 など Google DNS）に ping します。これが通らなければインターネット接続に問題（ルータの WAN 側や ISP 側の障害）が考えられます。
    - IP アドレス宛の ping が通るのに、例えば ping www.google.com などドメイン名では通らない場合、DNS の問題が疑われます。

5. **ネットワーク機器の状態確認:** クライアント側の問題でなければ、スイッチやルータなどのネットワーク機器側を調べます。機器のステータス LED、ログメッセージ（syslog や機器内ログ）、CPU 使用率やメモリ状況、インターフェースのエラー統計などを確認します。例えばルータの WAN 回線がダウンしていないか、スイッチポートに異常（コリジョンやループによるブロードキャストストームなど）が起きていないかなどを見ます。
6. **原因の特定と対策:** 情報を総合して原因を推測し、対策を講じます。設定ミスなら正しい設定に修正、機器故障なら交換、ケーブル不良なら張り替え、などです。DNS サーバがダウンしていたなら再起動するか予備に切り替える、など具体的な手を打ちます。対策後は問題が解決したか確認します。
7. **再発防止と記録:** 解決したら、なぜその問題が起きたのか整理し、再発を防ぐ措置が必要なら実施します。また障害の経緯と対応を記録（報告書など）してナレッジを蓄積します。これは今後チームで共有し、同様のトラブル時に迅速な対応をする助けとなります。

上記の流れを実践することで、多くのネットワークトラブルに対処できます。特に ping や traceroute、nslookup など基本ツールの使い方は習熟しておきましょう。

以下のフローチャートは、典型的な「インターネットに繋がらない」問題の切り分け手順をまとめたものです。



この図のように段階を追って Yes/No で分岐しながら原因を絞り込んでいきます。全て

「はい」で進んだ場合でも問題が残るケース（例えば特定のサービスだけ利用不可など）は、さらに上位層（ファイアウォール設定やアプリケーションの問題）の調査が必要ですが、大まかな方針は同じです。

よくあるネットワークトラブルの例

- **ケーブル抜け・断線:** ネットにつながらない原因のトップです。思いがけないところでケーブルが抜けていたり、清掃などで断線したりします。まず疑うべき基本ポイントです。
- **IP アドレス競合:** 誰かが固定 IP を設定したが既存 DHCP 範囲と被ってしまい、他の PC とアドレス重複して両者通信不良になるケース。IP 重複時は Windows なら警告が出ます。
- **DNS の不調:** インターネットには ping が通るのにウェブ閲覧不可、メール送受信不可という場合、DNS 名前解決に問題があるかもしれません。社内 DNS サーバが止まっていたり、ルータの DNS 転送機能がハングすることもあります。
- **無線 LAN の接続不良:** 電波干渉やチャンネルの混雑で著しく速度低下・切断が発生するケース。AP 再起動やチャンネル変更で改善することがあります。また新たに電子レンジや他の AP が近くに設置されて干渉が強まる例もあります。
- **機器の CPU 高騰:** ルータや L3 スイッチの CPU が何らかの要因で 100%近く使われていると、パケット処理が追いつかず全体の通信が遅延・途絶します。スパニングツリーループや DDoS 攻撃など、トラフィックの異常発生が背景にある場合もあります。
- **ルータ設定ミス:** 新しい静的ルートを入れ忘れた、NAT 設定を間違えた、フィルタの順序ミスで通信をブロックしていた、など人的ミスも起こりえます。変更を加えた直後に問題が起きた場合は設定を疑います。

トラブル対応は経験値がものを言います。一つひとつの事例を糧に、「似た現象のときは前こうだったな」という引き出しを増やしていきましょう。焦らず基本に立ち返って調査することが解決への近道です。

11. 運用・監視の基礎

ネットワークは構築して終わりではなく、その後の**運用管理**が非常に重要です。安定したネットワークサービスを提供し続けるために、日々の監視やメンテナンスを適切に行う必要があります。この章では、ネットワーク運用と監視の基本について説明します。

運用の基本

ネットワーク運用とは、構築したネットワークを安定的に稼働させるための継続的な作業全般を指します。具体的には以下のような業務があります。

- **設定管理とバックアップ:** ルータやスイッチ、ファイアウォール等の設定を管理します。設定変更を行った際は内容を記録し、万一の機器故障に備えて設定のバックアップ（コンフィグファイルの保存）を定期的に取得しておきます。新人エンジニアでも、設定変更の前後で差分をとって記録する習慣を持ちましょう。
- **機器のソフトウェア更新:** ネットワーク機器のファームウェアや OS には不具合修正やセキュリティ改善のアップデートがリリースされます。適切なタイミングでこれらを適用するのも運用の仕事です。ただし、更新によって不具合が生じるリスクもあるため、内容を精査しバックアップを取った上で計画的に実施します。
- **利用状況の把握:** ネットワークのトラフィック量、帯域使用率、各機器の CPU/メモリ使用率などを把握しておきます。日常的な利用状況を知っておくことで、異常時の早期発見や、将来的な増強（キャパシティプランニング）の判断材料となります。
- **問い合わせ・トラブル対応:** ユーザからの「ネットが遅い」「繋がらない」といった問い合わせに対応するのも運用の一部です。前章で学んだトラブルシューティングの手順を活かして対処します。また、問題が再発しないよう恒久対応策を検討することも重要です。
- **ドキュメント維持:** ネットワーク構成図、IP アドレス管理表、配線図、機器リスト、設定値一覧などのドキュメントを最新状態に保ちます。ネットワークは変更が発生するものなので、都度情報を更新しないと実態とドキュメントが食い違ってしまいます。新人のうちは先輩から「ドキュメントを更新しておいて」と頼まれることも多いでしょう。

運用において大切なのは**継続的な注意と整備**です。小さな問題を放置すると大きな障害につながることがあります。例えば「このスイッチのログに時々出るエラーは気になるが放置」という状態が、ある日スイッチダウンという重大事故になるかもしれません。日頃からログやアラートをチェックし、予兆があれば先回りして対策する姿勢が求められます。

監視の基本

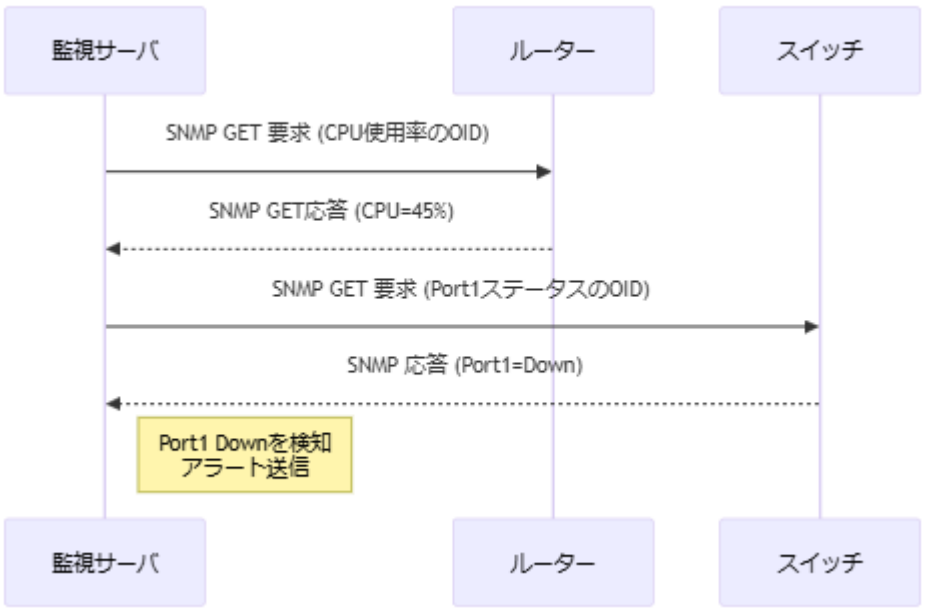
ネットワーク監視とは、ネットワークや機器の状態を常時モニタリングし、異常があれば検知・通知する仕組みや行為のことです。監視により問題の**早期発見・迅速対応**が可能となります。

監視する主な項目:

- **死活監視:** ルータやサーバなどが動作しているか（応答があるか）を確認します。典型的には定期的に ping を送って応答が返ってくるかを見る方法があります。応答がなければダウンしている可能性が高いので、すぐ管理者にアラートが上がるようにします。
- **リソース監視:** 機器の CPU 使用率、メモリ使用率、温度、電源ユニットの状態などを監視します。閾値を超えた場合に通知します。例えばルータ CPU が 80%を超え続けたら異常トラフィック発生を疑って調査する、といった具合です。
- **インターフェース監視:** スイッチやルータの各ポートの状態（Up/Down）やエラーの発生、トラフィック量を監視します。誤りパケットやコリジョンが急増していないか、帯域使用率が高すぎないかなどを見ることで、回線故障や輻輳を検知できます。
- **ログ監視:** ネットワーク機器は syslog 等で様々なログを出力します。重要なエラーログ（インターフェースダウン、経路変化、認証失敗など）が出たら検知するような設定も行います。また FW/UTM ではセキュリティログ（不正アクセスの試行など）も監視対象です。

監視の方法とツール:

- 小規模ネットワークでは、定期的な手動チェックと主要機器への PING 監視（バッチスクリプトや簡易ツール）程度でも運用できます。しかし規模が大きくなると、人手では難しいため専用の監視ツール/ソフトウェアを導入します。
- オープンソースでは **Zabbix**、**Nagios**、商用では **SolarWinds**、**PRTG**、**Datadog** など、多くのネットワーク監視ソリューションがあります。これらは WEB ダッシュボードでネットワーク全体の状態を可視化し、閾値超過時にメールや SMS で通知するなど高度な機能を備えています。
- **SNMP（Simple Network Management Protocol)**という標準プロトコルがあり、多くの機器が対応しています。SNMP を使うと機器の各種情報（インターフェース統計値や CPU 温度など）を取得できます。監視ツールは内部で SNMP によって機器から情報を収集しています。新人エンジニアは、まず SNMP で何ができるかを押さえ、必要に応じて SNMP の設定（コミュニティ名や SNMP バージョン、許可 IP の設定など）を行えるようになると良いでしょう。



上記シーケンスは監視サーバが SNMP を使って機器情報を取得し、異常を検知する様子の一例です。実際の監視製品はこれを自動かつ継続的に行い、大量のデータを蓄積・分析しています。

定期点検とレビュー: 監視システムに頼るだけでなく、定期的にネットワーク全体を見直すことも重要です。例えば月次でトラフィックレポートを作成し、どのリンクが逼迫しているか、応答時間の変化はないかなどを分析します。これによりボトルネックや将来の課題を早めにキャッチできます。

運用・監視は地味に見えますが、ネットワークの安定稼働を支える縁の下の力持ちです。新人のうちは構築よりも運用作業の比重が大きいかもしれません。その中で是非、「ネットワークの健康状態」を常に意識して、問題の芽を摘む習慣を身につけてください。

12. まとめ

お疲れさまでした。本書を通じて、**無線 LAN と IP ネットワークの基礎**について一通り学習しました。新人エンジニアの方に向けて、現場で役立つ知識を意識しながら以下のポイントを解説してきました。

- **無線の基礎:** Wi-Fi（無線 LAN）の仕組み、電波を使った通信の特徴、基本構成と接続手順、暗号化の重要性などを学びました。無線は便利ですが有線と異なる注意点があることを理解いただけたと思います。
- **IP ネットワークの基礎:** IP アドレスとは何か、ネットワークとサブネットの概念、ルータによる経路選択など、ネットワークの根幹となる IP 技術について学びました。デフォルトゲートウェイや DNS の役割も押さえました。
- **ネットワーク機器:** スイッチとルータの違いや役割分担を理解し、それぞれが LAN 内部とネットワーク間接続で必要不可欠であることを確認しました。また、DHCP が IP 設定を自動化し、DNS が名前解決を担い、NAT がアドレス

変換で IPv4 利用を支えている仕組みも習得しました。

- **セキュリティと高度な話題:** 無線 LAN セキュリティの基本対策（暗号化・認証）や、VLAN でネットワークを論理分割する手法、OSPF/BGP のようなルーティングプロトコルの存在にも触れ、ネットワークの安全性・拡張性を高める考え方に触れました。
- **設計・運用:** 小規模ネットワーク設計の流れや機器選定の勘所を学び、さらに日常の運用・監視で注意すべき点、トラブルシューティングの基本手順も習得しました。ネットワークは設計・構築して終わりではなく、適切に管理・改善していくサイクルが大事であることを理解できたでしょう。

ネットワーク技術は日進月歩で、新しい技術や製品が次々登場します。しかし、基礎的な原理原則は大きく変わりません。**物理層からアプリケーション層までの流れ**、**データ転送の仕組み**、**機器の役割**といった基本をしっかり身につけておけば、新しい知識にも対応しやすくなります。

最後に、実践あるのみです。可能であれば職場のネットワーク機器の設定を先輩に見せてもらったり、自宅に小型ルータやスイッチを用意して実験してみたり、手を動かして体験することで理解が深まります。また、トラブル対応した経験は大きな財産となります。失敗を恐れず、しかし慎重に計画・検証しながら、ネットワークエンジニアとしての第一歩を踏み出してください。

本書で得た基礎知識が、皆さんの今後の活躍に役立つことを願っています。ネットワークの世界へようこそ、そしてこれからも学びを続けていきましょう！