123.●ネットワークの基礎

✨123.●ネットワークの基礎

総務部門など非エンジニアの方でも「業者さんや情報システム部門と会話できる」ことを目的にした**ネットワークの基礎知識** を整理します。専門用語をなるべくわかりやすく噛み砕きます。

ネットワークの基礎知識（非エンジニア向け）

1. ネットワークの役割

- コンピュータや機器同士をつなげて情報をやり取りする仕組み
- 社内のパソコンから共有フォルダにアクセスしたり、インターネットを通じてクラウドサービスを使うのはすべてネットワークのおかげです。

---

2. ネットワークの種類

(1) **LAN（Local Area Network）**

- 社内や家庭など「限られた範囲」でのネットワーク
- 例：オフィス内のパソコン、プリンタ、サーバーを接続する

(2) **WAN（Wide Area Network）**

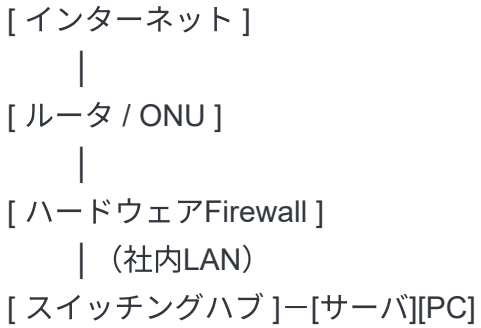
- 広範囲をつなぐネットワーク（インターネットを含む）
- 例：本社と支社を専用線やVPNで接続する

---

3. ネットワークを構成する機器

- **ルーター**：インターネットや社内LANとの“出入口”
- **スイッチ**：社内のPC・プリンタなどをつなぐ“配線の分岐点”
- **アクセスポイント（Wi-Fiルーター）**：無線LANを提供する装置
- **ファイアウォール**：不正アクセスを防ぐ“門番”

  イメージ図



　　│（社内LAN）
[アクセスポイント]ー[PC][プリンタ]

---

4. IPアドレスと名前解決

- **IPアドレス**：ネットワーク上の「住所」
  - IPv4（例：192.168.1.10）
  - IPv6（新しい規格、長い文字列）
- **DNS（Domain Name System）**：人間が覚えやすい名前（例：www.google.com）を、IPアドレスに変換してくれる仕組み

5. インターネット接続の仕組み

- 社内LAN → ルーター → プロバイダー（ISP） → インターネット → 接続先サイト
- 総務で理解しておくとよい視点：
  - **回線契約（光回線・モバイル回線）とプロバイダー契約**の両方が必要（ADSLはサービス終了）
  - 通信速度や障害時の責任分担を確認できるとよい

---

6. セキュリティの基本

- **ゼロトラスト**：「社内だから安全」という考え方をやめ、常に認証・監視する考え方
- **Wi-Fiの暗号化（WPA2/WPA3）**：通信内容を盗まれないようにする技術
- **VPN（Virtual Private Network）**：外部から安全に社内ネットワークへ接続する仕組み

  公共の道路（インターネット）の上に、自分専用の「秘密のトンネル（暗号化通信）」を作る技術

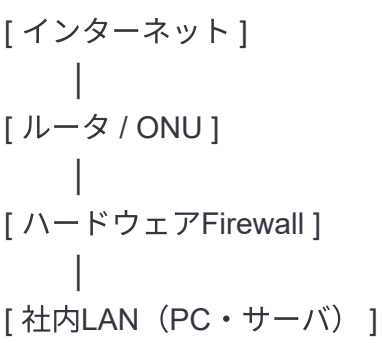
  Windows 10/11、macOS にはVPN接続機能（VPNクライアントアプリ）が標準搭載されている。
  会社側でVPNサーバを導入しクライアント側からサーバ情報を入力すれば利用可能となる。

  [自宅PC / スマ]（VPNクライアントアプリ）
  　　│ (暗号化トンネル=社内LAN)
  　　▼
  [インターネット]
  　　│ (暗号化トンネル=社内LAN)
  　　▼
  [会社のVPNサーバ]
  　　│
  　　▼
  [社内LAN（業務システム）]

- **FireWall**：ネットワークを外部の接続から守るために設置される「関所」のような役割

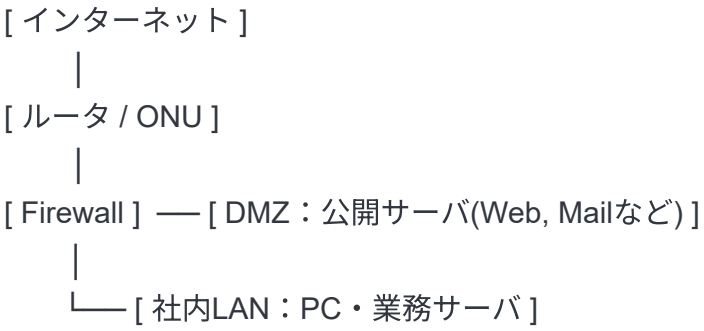
  ◯基本的な最小構成

社内ネットワーク（LAN）とインターネット（WAN）の境界
最も一般的で基本的な配置は、インターネット回線（ルータやONU）と
社内ネットワークの間 にファイアウォールを置きます。
外部からの攻撃を遮断し、内部から外へ出ていく通信も制御できます。



◯セキュリティ強化の構成

DMZ（非武装地帯）の構築
Webサーバやメールサーバなど、外部公開が必要なサーバを
DMZ（DeMilitarized Zone） と呼ばれる領域に置く場合があります。
ファイアウォールを使って「外部公開サーバ」と「社内LAN」を厳密に分離します。



---

7. ネットワーク障害の典型例とチェックポイント

- **インターネットがつながらない**
  → ルーターの電源確認 → 回線事業者の障害情報 → 社内配線の確認
- **プリンタに接続できない**
  → IPアドレスが正しいか → スイッチやLANケーブルの確認
- **Wi-Fiが遅い**
  → 接続人数過多、距離・壁の影響、チャンネル干渉、周波数（2.4GHz、5GHz）

---

8. 総務部門向けチェックリスト

✅ 社内LANとインターネットの違いを説明できる
✅ ルーター・スイッチ・アクセスポイントの役割を理解している
✅ IPアドレスとDNSの役割を知っている
✅ 回線契約とプロバイダー契約の違いを理解している

✅ VPN・Wi-Fi暗号化の意味を知っている
✅ 障害時の初期確認手順を把握している

まとめ

ネットワークの専門的な設計はエンジニアが行いますが、
「どの機器がどんな役割か」「トラブル時にどこを確認するか」「業者との会話で最低限の用語を知っているか」
これだけ理解しておくと、総務部門の方も導入・運用の場面で大きく役立ちます。

NAS（Network Attached Storage）の基礎知識

1. NASとは？

- **Network Attached Storage** の略で、「ネットワークにつながる外付けハードディスク」のようなもの。
- 通常の外付けHDDは **USBケーブルで1台のPCに接続** しますが、
  NASは **LANケーブル（またはWi-Fi）で社内ネットワークに接続** するため、複数のPCやスマホから同時にアクセスできます。

---

2. NASの役割

- 社内の「共有フォルダ」として機能
- ファイルサーバー代わりに使える（特に中小企業でよく採用される）
- バックアップ先として利用できる

---

3. NASのメリット

- **データ共有が簡単**
  → 同じファイルをみんなで利用できる
- **導入が容易**
  → 専用サーバーより安価で、設定もシンプル
- **データの安全性向上**
  → RAID機能（複数HDDに分散保存）により、HDDが1台壊れてもデータを守れる機種が多い
- **リモートアクセス可能**（クラウド連携機能付きモデル）
  → 外出先やテレワーク時に社内NASへ接続できる

---

4. NASの注意点

- **障害リスク**
  → 機器自体が壊れるとアクセスできなくなるため、別途バックアップが必要
- **セキュリティ**
  → インターネットからアクセスできる設定にすると、不正侵入のリスクが高まる

- **速度**
  → ネットワーク環境が遅いとNASも遅く感じる

---

5. NASとクラウドストレージの違い

項目	NAS	クラウドストレージ（例：Google Drive, OneDrive）
データの保存場所	社内（機器）	インターネット上（外部サーバー）
管理責任	自社	クラウド事業者
初期費用	機器購入が必要	契約次第（低〜中）
セキュリティ	自社対策が必要	サービス側のセキュリティを利用
利便性	社内LANで高速アクセス	どこからでもアクセス可能

---

6. 総務部門が押さえるべきNASのポイント

✅ 「社内の共有フォルダ」として使える機器である
✅ 複数人でのファイル共有に便利だが、バックアップも必要
✅ RAID機能やクラウド連携の有無が製品選定のポイント
✅ 外部アクセス（リモート接続）を有効化する際はセキュリティ対策が必須

まとめ

NASは **「社内に置ける小さなファイルサーバー」** です。
クラウドと比べて **社内ネットワーク内での高速性と自社管理のしやすさ** がメリットですが、セキュリティとバックアップの管理を怠ると危険です。