

125.●ネットワーク導入の仕様

125.●ネットワーク導入の仕様

○中小企業向けネットワーク導入仕様（社員100名程度）

規模感（社員数 20～100 名程度）を想定し、典型的な社内 LAN 環境・インターネット接続・セキュリティ・運用管理などを含めた、**基本仕様例**をまとめます。

1. ネットワーク全体像

- **構成**：インターネット回線 → ファイアウォール/UTM → コアスイッチ → 各フロアスイッチ → PC・サーバ・プリンタ
- **方式**：有線 LAN + 無線 LAN（業務用 Wi-Fi）
- **IP 管理**：DHCP サーバで自動割り当て（範囲を部門ごとに分ける）

2. インターネット回線

- **回線種別**：光回線（1Gbpsベース、利用人数次第で 10Gbps も検討）
- **冗長化**：可能ならプロバイダを分けて 2 回線（業務継続性のため）

3. セキュリティ機器

- **ファイアウォール/UTM**
 - FortiGate、WatchGuard、Palo Alto など中小向けモデル
 - 機能：外部からの不正アクセス防止、VPN、Web フィルタリング、IPS、アンチウイルス
- **VPN**：テレワーク用に SSL-VPN または IPsec-VPN を提供
- **MFA（多要素認証）**：VPN・クラウドサービスへの接続時は必須

4. LAN 機器

- **コアスイッチ**：L3スイッチ（VLAN設定可、10Gbpsアップリンク）
- **アクセススイッチ**：PoE対応（Wi-Fi APやIP電話用）
- **冗長化**：コアスイッチは2台冗長化が理想

5. Wi-Fi

- **規格**：Wi-Fi 6 (IEEE 802.11ax)
- **SSID分離**：
 - 社員用（社内リソースにアクセス可）
 - ゲスト用（インターネットのみ）

- 認証：社員用は RADIUS 認証（AD/LDAP連携）、ゲストは共通パスワード or 一時発行コード

6. サーバ環境

- オンプレミス（必要に応じて）
 - Active Directory（ユーザー・端末管理）
 - ファイルサーバ（NAS も可）
 - プリントサーバ
- クラウド併用
 - Microsoft 365 / Google Workspace
 - クラウドストレージとオンプレNASの併用

7. IPアドレス設計（例）

- ネットワークアドレス：192.168.0.0/24
 - 192.168.0.1：GW(ファイアウォール・ルータ)
 - 192.168.0.2～50：サーバ類
 - 192.168.0.100～200：PC・プリンタ（DHCP）
 - 192.168.0.201～254：Wi-Fi端末

（部門ごとに VLAN を切るなら「192.168.10.x 営業」「192.168.20.x 経理」などに分割）

8. 運用・管理

- 監視：SNMP監視 or クラウド型監視（Zabbix, PRTG, 監視SaaS）
- ログ管理：ファイアウォール・サーバ・ADのログを集中管理
- バックアップ：NAS + クラウドストレージ併用
- セキュリティポリシー：USB利用制限、MFA必須、定期パスワード変更禁止（長期強固パス推奨）

9. 導入コスト目安（社員 50 名規模）

- 回線：光回線 1Gbps（月額 5万～10万円／冗長化すると倍）
- UTM/Firewall：50～200万円（年額ライセンス費用あり）
- スイッチ類：1台 20万～50万円
- Wi-Fi AP：1台 5万～10万円 × 複数
- サーバ/NAS：50万～200万円
- 運用（監視・保守契約）：月額 5万～15万円

👉 初期導入コスト合計：約 140～490 万円程度このように「インターネット・セキュリティ・LAN/Wi-Fi・サーバ管理・運用保守」のバランスを考えて仕様を決めるのがポイントです。

○小規ネットワーク導入仕様（社員 10 名規模・安価重視）

規模感（社員数 10 名程度）を想定し、典型的な社内 LAN 環境・インターネット接続・セキュリティ・運用管理などを含めた、**基本仕様例**をまとめます。

ここでは「信頼性は確保しつつ、過剰投資は避ける」方向で設計します。

1. インターネット回線

- 光回線 1Gbps（単回線で十分）
- プロバイダは法人向けでなくても可（ただし固定IPが必要ななら法人契約推奨）

2. セキュリティ／ルータ

- 家庭用ルータではなく、小規模法人向けルータを導入
 - 例：Yamaha RTX シリーズ、NEC IX シリーズ
- ファイアウォール機能：標準搭載で十分
- VPN：テレワーク用に設定可（必要があれば後付けでOK）

👉 **UTM（統合脅威管理）**：ファイアウォールやセキュリティ機能をまとめて1台で実現する機器）

ファイアウォール、VPN、IPS/IDS（侵入防止・検知システム）、アンチウイルス / アンチマルウェア、アンチスパム、Webフィルタリング、アプリケーション制御、ログ・レポート機能はコストが高いため要検討（数十万円＋年額ライセンス）だが、あった方が無難。代替案はセキュリティソフトやクラウドメールセキュリティで補完。

3. LAN 機器

- スイッチ
 - L2スイッチ（ギガビット対応、8～16ポート）
 - VLAN分割は不要（人数が少なくネットワークが混雑しないため）
- 配線
 - 有線LAN（カテゴリ6）を基本とし、プリンタやNASは有線接続
 - 社員のPCは固定でもDHCPで自動割り当て

4. Wi-Fi

- 無線LANアクセスポイント（法人向け1～2台）
 - 例：Buffalo 法人向けAP、Aruba Instant On
- SSID
 - 社員用（社内リソース接続可）
 - ゲスト用（インターネットのみ）

👉 家庭用 Wi-Fi ルータでも動くが、業務環境なら法人向けの安定品がおすすめ。

5. サーバ環境

- NAS（2ベイ RAID1 構成）をファイルサーバ兼バックアップ先に
 - 例：Synology、QNAP、Buffalo TeraStation
- Active Directory サーバは不要（10名規模ならローカルアカウント＋クラウド管理で十分）
- クラウドサービス（Microsoft 365 / Google Workspace）を中心に利用

6. IPアドレス設計（シンプル）

- ネットワーク：192.168.1.0/24
 - 192.168.1.1：ルータ（デフォルトゲートウェイ）
 - 192.168.1.2：NAS
 - 192.168.1.10～：PC（DHCP割り当て）
 - 192.168.1.200～：プリンタ

7. 運用・管理

- ネットワーク監視は不要（10名なら管理者が定期チェックで十分）
- NASはクラウドに自動バックアップ（OneDrive/Google Drive/S3など）
- ウイルス対策は各PCに**エンドポイントセキュリティ**＝「社員のPCやスマホを直接守るセキュリティ」導入

8. 導入コスト目安

- 光回線：月額 5,000～8,000円程度
- UTM：7～10万円（FortiGate FGなど）
- ルータ：5～10万円（Yamaha RTX1210など）
- スイッチ：1～3万円（8～16ポート ギガビットL2）
- Wi-Fi AP：2～5万円 × 1～2台
- NAS：5～15万円（HDD込み）

👉 初期導入コスト合計：約20～50万円程度

9. 構成図

- ✅ 小さく始めて大きく発展させる

社員10名規模なら「**光回線＋法人ルータ＋L2スイッチ＋Wi-Fi＋NAS**」で十分ですが、後々のことを考えてUTMは導入した方がより安心です。

最初はVLANや10Gbpsバックボーンは不要で、クラウドサービスを中心にした方が運用コストも削減できます。

規模を大きくする場合は、この構成を基本にしてコアスイッチを加え部門ごとのネットワークをL2ないしはL3のSwitchで増設していくのが良いでしょう。

