2章 企業内ネットワーク構築

本章を学習することにより、P検1級の出題カテゴリー「企業内ネットワーク構築」を習得することができます。

＜本章で学習するスキル・詳細スキル＞

スキル	詳細スキル	ページ
（1）企業内ネットワークの設計ができる	1. 企業内ネットワークの倫理的な設計ができる	29頁
	2. 企業内ネットワークの物理的な設計ができる	33頁
（2）企業内ネットワークを構築することができる	1. 企業内の小規模ＬＡＮを構築できる	36頁
	2. ネットワークの分割ができる	40頁
	3. 複数拠点を接続するネットワークを構築できる	44頁

（1）企業内ネットワークの設計ができる

1．企業内ネットワークの論理的な設計ができる

システムがなくては仕事が成り立たない、という業種、業界が少なくない現代においては、社員がいつでも安心して利用できる、使い勝手のよい企業内ネットワークは、企業活動における生命線の一つです。しかし、ネットワーク利用の普及拡大と低価格ネットワーク機器類の登場により、比較的容易にネットワークを構築できるようになったため、しっかりとした設計も計画もなく、通信量の十分な調査なども行わないまま、結果的には、様々なリスクや課題を抱えたネットワーク環境で運用している企業が多いのが現状です。

本項では、自社内ネットワークを構築、または整備する際に、委託企業に提示する**RFP**に盛り込むべき内容として、現状のネットワークに関する問題解決と将来予測、**ユーザー**の使いやすさに加えてセキュリティ面でも安心して利用できるよう、全体最適の視点で企業内ネットワークを論理的に設計するためのポイントを、①現状調査と利用計画の検討、②基本方針の策定、③業務継続方法の策定の、大きな三つの流れに沿って解説します。

RFP
[Request For Proposal]
提案依頼書。システム化に関する業務を委託する際、どのようなことを依頼したいのか、システム概要、構成や調達の要件など具体的な内容を書いた文書のこと。

ユーザー（user）
一般的に利用する人を表す。システム利用者の場合は、そのシステムの利用権限を持つもので、この場合は、企業（自社）のネットワークの利用権限を与えられた人々のことを指す。

①現状調査と利用計画検討

まずは、「なぜ、企業内ネットワークを構築する必要があるのか」、その理由を明確にする必要があります。何かある度ごとに、ネットワークが不安定になったり、いつの間にか管理ができなくなってしまったり、という事態を招かないためには、ネットワークの利用に関する基本方針が必要です。ユーザーにとって使いやすく、また、基本方針に基づいて改善しながら、できるだけ長く使えるネットワーク環境の設計が理想です。

企業内ネットワーク構築の理由を明確にするために、現状調査を行います。具体的には、ユーザーはもちろん、将来予測のために経営者にもヒアリングを行います。それらの**ヒアリング**内容をもとに、現状の改善点と今後の利用計画までを検討します。次表に、ヒアリングで情報を収集し、最低限確認しておくべき点を記載します。

ヒアリング
特定の事柄に対して、決裁権者や利害関係者に質問をして、意見、考えを聞き出すこと。面談、インタビュー形式で実施する場合が多い。対象人数が多い場合は、アンケートをとったり、特定のテーマを設けた意見交換会を開いて、その場の意見をまとめる。

（メモ）　　年　　月　　日

＜現状調査・利用計画の検討にあたって入手すべき情報＞

ヒアリングの内容	設計要件
現状の問題とネットワークの利用に関する要望	改善点
ユーザーにとっての使いやすさ（ユーザーのネットワークの利用に関する基礎知識の有無、または、教育方針の確認）	
自社のセキュリティポリシー、具体的なルール、過去におきたセキュリティ関連の事故、被害等の確認	セキュリティ
ユーザーの数　①現在　②将来予測	ネットワーク規模
利用するアプリケーション　①現在　②将来予測	アプリケーションの優先度

表の通り、これらのヒアリング情報を整理することで、企業内ネットワークを構築する理由が明確化され、また、それぞれの情報が、企業内ネットワーク設計の要件にもなります。情報を整理する際は、**MECE**となるよう努めましょう。

MECE
［Mutually Exclusive and Collectively Exhaustive］
（4章-（1）-3参照）

②基本方針の策定

次に、ネットワーク設計の基本方針を策定します。基本方針は、下表の通り、次の四点を明確にします。

＜ネットワーク設計の基本方針：四つのポイント＞

ユーザーが利用するもの	ユーザーがネットワーク上で利用するアプリケーションを、前項で整理した内容を基に、重要度別（最重要、重要、通常などのレベル）にランク分けをし、確定する。
セキュリティ方針	情報へのアクセス権、ユーザー別の操作許可範囲、セキュリティ脅威とリスク対策、また、それらの維持運用管理方法。 ※詳細は1章情報セキュリティ管理-(1)項-2･3を参照ください。
冗長性	安定稼働の確保と障害発生時の問題の切り分け（そのための作業内容）を考慮した上で、ネットワーク・**トポロジー**に応じた冗長度を明確にする。
拡張性	通信量や接続先、収容機器の台数など、将来の増加予測をもとに、（どれくらい増やすのかを想定した上で）どの程度対応できる設計にするか確定する。

冗長［じょうちょう］
冗長とは、最低限必要なものに加えた予備や余分なものの意味。ネットワーク設計における冗長性とは、何らかの障害時でも問題なくネットワークが利用できることで、そのようなシステム構成にすることを冗長化という。

トポロジー［topology］
トポロジーは空間的要素の位置と接続関係を示す概念。
ネットワーク･トポロジー［network topology］はコンピュータネットワーク各種機器類をどのように接続するのか、接続形態を示す用語。代表例として、スター型、バス型、リング型などがある。

（メモ）　　年　　月　　日

≪参考≫ネットワークの構築

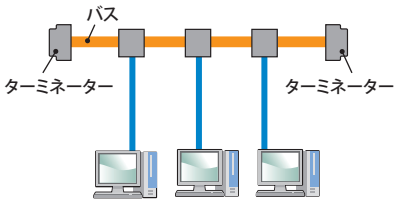
LAN接続形態と規格

LANの接続形態のことを**ネットワークトポロジー**といい、代表的なものにバス型、スター型、リング型があります。

ネットワークトポロジー
コンピューターネットワークの配線に各種機器がどのような形状で接続されているのかを表す用語。

バス型

バス（母線）と呼ばれるケーブル（伝送路）にコンピューターや周辺機器を接続する形態です。ケーブルの端には**ターミネーター**を取り付けます。1つの回線を複数のコンピューターが共有する形態のため、配線は簡単ですが、回線に障害が起きた場合はネットワーク全体に被害が及（およ）びます。規格としては、**イーサネット**が使われます。



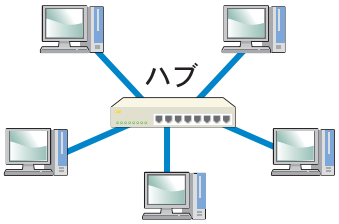
ターミネーター
コンピューターに周辺機器を接続したときの配線の終端（しゅうたん）に取り付ける抵抗器（ていこうき）のこと。終端で信号の反射を防ぎ、信号の乱れを防ぐ。

イーサネット
LANで接続された複数のコンピュータが、効率よく通信回線を利用できるように考えられた通信方法の一つ。現在、特殊（とくしゅ）な用途（ようと）を除いて、ほとんどはこの方式である。イーサネットには、1本の回線を複数の機器（*）で共有するバス型と、集線装置（ハブ）を介（かい）して各機器を接続するスター型の2種類がある。

＊この場合の機器は、コンピュータやハブ、ルーターなどで、これ等機器のことを「ノード」という。

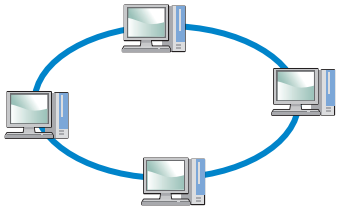
スター型

中央にHUB（ハブ）を設置してコンピューターや周辺機器を放射状に接続する形態です。他の接続形態に比べて配線の自由度が高いことなどから、LANの接続形態として広く利用されています。規格としては、イーサネットが使われます。



リング型

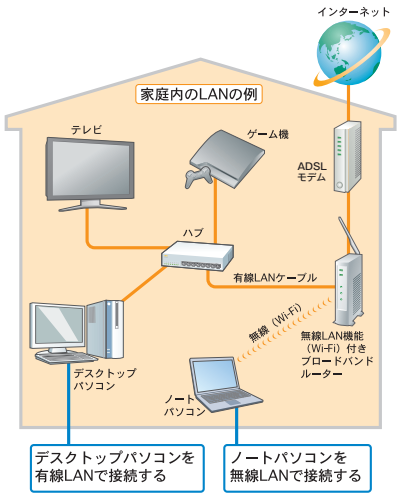
伝送路をリング状に配置し、コンピューターや周辺機器を接続する形態です。環状ネットワークともよばれます。規格としては、イーサネット以外のものが使われます。



LAN接続の種類

コンピューターをLANに接続するには、有線や無線などの方法があります。

有線	LANケーブルを使って接続します。
無線	電波や赤外線で接続します。 無線LANは、ハブの代わりに「アクセスポイント」という無線ルータの中継機器を使って、電波でデータのやり取りをします。各端末には無線LANカードが必要です。 
電話回線	外から、電話回線を使ってネットワークに接続するときなどに使われます。



（メモ）　　年　　月　　日

③業務継続方法の策定

既述の通り、ネットワーク設計は冗長性を考慮したものが必要ですが、万が一、機器類の故障など何等かの障害が発生し、ネットワークシステムが停止しても、業務を止めない代替案を策定しておくことが重要です。

代替案の策定においては、次の二つの視点から、ネットワーク障害時の影響範囲を想定し、ネットワークを利用せずに業務が遂行できる対応策を考えておくとよいでしょう。

1. 業務の**ワークフロー**を基に、ネットワーク環境に依存する部分を把握し、ネットワーク上の障害ポイントと照らし合わせて、ワークフロー上の該当業務から、その後の業務まで、影響を受ける範囲を想定します。

2. 顧客管理、会計管理、在庫管理など、**データベース**ごとに、影響を受ける業務内容を洗い出し、業務が止まらないよう、関連業務ごとのに障害時の対策をたてておきます。

ワークフロー［workflow］（業務フロー）
業務の内容や順番を吟味し、情報が円滑に流れるよう、業務に必要な処理手順を流れに沿って規定すること、また、規定した流れそのものを指す。
※業務フローの解説は3章-（4）-2参照。

データベース［database］
複数のユーザーやアプリケーションによって共有する集合した情報（データ）を指す。または、それらの情報（データ）を管理するシステムのこと。

P検1級対策

P検1級の問題では、企業内ネットワークを構築すべきか否か、企業内ネットワークを構築することによってどのような問題が解決できるのか、何が得られるのか、自社の現状と将来（経営戦略）を踏まえ、その目的を明確にできるかどうかが問われます。

（メモ）　　年　　月　　日

2. 企業内ネットワークの物理的な設計ができる

▼ネットワークの設計と構築における　物理設計

企業内ネットワークの構築にあたって考えなければいけないことは、論理設計と物理設計に大別されます。論理的な設計は前項で解説した通り、ネットワーク構築の目的と要件に基づいて、求める機能、役割を整理して、ネットワークの構成要素を確定し、構成要素間でのデータの流れを明らかにすることです。この論理設計をもとにして、購入するサーバーの台数、ソフトウェアや機器類の種類、数量、どこに設置して、どのようにつなぐのか、**ラック**や電源設備の確保、使用するケーブルと配線などを決めるのが物理設計です。

サーバーについては、設置スペースの問題や運用コストの問題から、複数台の導入が困難な場合もあるでしょう。その場合は、**仮想化**を行い 、1台のサーバーに複数の役割を持たせることも可能です。仮想化は、既存システムの一部が新しいサーバー OSに対応していないがそれ専用にサーバーを運用したくない、電源や保守等のランニングコスト面を抑えたいといった場合には有効な技術です。これらも理解した上で、最適なサーバー台数を検討するようにしましょう。

また､インターネットの出入点､拠点間通信をどう行うかといった将来の拠点間ネットワークの拡張性の面も考慮しつつ、物理設計を行いましょう。

企業内ネットワークは、たとえ小規模であっても、論理設計、物理設計の順に行い、それぞれを文書化･図式化しておくことが重要です。こうした情報を図式化した**LAN図（ネットワーク図）**も、設計に合わせ、論理構成図と物理構成図に分けて記載します。

論理構成図の情報要素としては、IPアドレス、サブネット（VLAN）、ルーティング、**ファイルサーバー**、**データベースサーバー**、**プリンタサーバー**、**DHCPサーバー**、**DNSサーバー**などのサーバー情報ですが、物理構成図には、文字通り、物理的な情報として、設置場所（フロアやラック）ごとの配線情報の他に接続ポート、イーサネットやケーブルについての情報を記載します。

LAN図を作成する目的は、構成を把握するため、トラブル回避･対策のため、ネットワーク拡張のため、など、使用する人やケースにより様々ですが、目的を考えずに、現状をただ記しておこうとすると、わかりづらいものになってしまいます。日々の運用のためのものなのか、配線工事のためのものなのか、目的に応じたLAN図（ネットワーク図）を作成しておくとよいでしょう。

また、購入したハードウェア類は、永遠に利用できるものではありません。機器としての寿命があるのはもちろんのこと、ドライバやライセンスなどソフト面での定期的なメンテナンスも必要です。論理構成図、物理構成図などのLAN図とともに、自社の資産として、購入年月日や仕様等を記載した**IT資産管理表**を作成し、運用、管理を行っていきます。

ラック
棚、台の意味。複数台のコンピューター（サーバーなど）を重ねて設置できる棚板がついているもの。

仮想化
疑似的にハードウエアが存在する状態をつくり、その機能、役割を提供できるようにすること。パソコンやサーバーなど装置全体から、メモリやCPUなど、装置の一部まで、様々な仮想化の技術がある。

LAN図（ネットワーク図）
どこにどのような機器を設置したのかを示したLAN全体の構成図、ネットワークの配線を表したもの。機器類の配置と、どのケーブルで互いを接続しているのかなど、物理的な情報を記載する。

ファイルサーバー
クライアントユーザー同士のデータ共有やバックアップなど、データ保存を主目的として、ネットワーク上に設置するサーバー。

データベースサーバー
クライアントユーザーからの要求に応じ、データベースを操作する役割をもつ、データベースエンジンをインストールしたサーバー。

プリンタサーバー［printer server］
複数のコンピューターが、ネットワークで接続されたプリンターを、共用するためのサーバー。

DHCPサーバー［dynamic host configuration protocol server］
コンピューターをLANに接続する時、空いているIPアドレスを一時的に割り当て管理するサーバー。

DNSサーバー
ドメイン名システムを構成するサーバー。インターネット上のドメイン名とIPアドレスを一括管理しており、ドメイン名⇒IPアドレス、IPアドレス⇒ドメイン名等、インターネットに接続するコンピュータからの問合せに応える。

IT資産管理表
自社の情報化に必要なハードウェア、ソフトウェア類を一覧にしたもの。

（メモ）　　年　　月　　日

＜表1.　IT資産管理表項目例＞

機器類に共通した主な項目	資産管理番号、機種、IPアドレス、MACアドレス、コンピュータ名、OS、設置年月日、廃棄年月日
ハードウェアに関する項目	購入年月日、メーカー名、製品型番、製造番号、シリアルNo.、実装メモリ、ディスク容量
ネットワークに関する項目	ホスト名、ユーザー名、ドメイン、ワークグループ
設置場所や使用者に関する項目	設置場所、部名、課名、室名、使用者名
その他	リースの場合：リース契約番号、リース会社、
	リース契約日、リース期間（月）、リース開始・終了日 ハードウェア・ソフトウェアともにトラブル時の連絡先など

▼建築や内装への要求仕様策定と現場指示

サーバやルータなど情報機器類は、人通りが少なく、空調管理･施錠ができる独立したサーバールーム、もしくは、専用の隔離スペースへの設置が理想です。経営層に提案し、情報機器類の健全な運用とメンテナンスを行えるような環境を可能な限り確保しましょう。また、幹線など、動かないLANケーブルは、セキュリティの面からも、できるだけ壁の内側や床下に隠して見えないようにしましょう。これらを含めた要求仕様、論理構成図をもとに、オフィス内に機器やサーバ、PC端末の設置計画を立て、必要な配管、配線や電源を確保します。実際の設置場所を考える際は、建物について、配線、配管の有無、電源の引き込み状況（容量）を調査し、把握しておきます。

＜物理設計に関する確認ポイント＞

・ラック、サーバルームなど設置場所の確保
　（サーバルームは、空調管理ができるかもチェック）
・配線・配管の有無、数量
・設置場所への電源引き込み状況と容量

これらの情報確認は、場所によっては、工事が必要になる場合もあり、また、過去の資料が古い情報だったという場合もありますので、日数に余裕をもって行うようスケジュールをたてましょう。工事が必要な場合、費用と日数がネットワーク構築全体に影響します。

また、**無線LAN**を利用する場合は、アクセスポイントをどこにどれだけ設置すれば、データの送受信が問題なくできるのか、利用台数を想定したうえでの通信テストが必要です。

無線LAN
「有線」と違い、ケーブル（線）を使わずに、データの送受信を行うLANのこと。

IEEE 802. 11 a/b/g/n
規格に準拠した機器で構成するネットワークを指す場合が多い。また、データ送受信のための中継機器や、その機能をもったルータのことを、アクセスポイントと呼び、無線通信機能を持った端末がアクセスポイントを介してネットワークを形成する。

IEEE 802. 11 a/b/g/n
IEEE（米国電気電子学会）が策定した無線LANの標準規格。a,b,g,nは、規格種類のことで、下記の通り、通信速度が異なる。

IEEE 802. 11a
（54Mbps・5GHz）
IEEE 802. 11b
（11Mbps・2. 4GHz）
IEEE 802. 11g
（54Mbps・2. 4GHz）
IEEE 802. 11n
（300Mbps・2. 4GHz・5GHz）

（メモ）　　年　　月　　日

このように、小規模なネットワークの構築であっても、必ず現場に出向いて調査を行い、現状の正しい情報を把握したうえで機器類の配置計画を立てるようにします。

▼有線または無線LANとセキュリティ計画

小規模なLAN構築であっても、有線LANと無線LANが混在するケースが多く見受けられます。有線、無線各々にメリットデメリットがありますので、それらをしっかり理解し、自社の業務の性質に合わせて選択します。

＜表2.　有線LANと無線LANの特徴＞

有線LAN	無線LAN
・通信状態が安定している。 ・通信速度が速い。 ・セキュリティリスクは低い。 ・配線が必要。 ・機器類の設置個所（レイアウト）を十分に考えなければならない。 ・接続台数の上限＝ハブのポート数 ・**PoE**が可能。	・配線が不要なため見た目が美しく、レイアウトしやすい、移設や増設も容易。 ・電波が届く範囲は、どこからでもネットワークに接続できるが障害物などの影響を受けるため通信が不安定になりやすい。 ・セキュリティリスクが高い。 ・通信速度が有線LANに比べると遅い。 ・混信する（他のオフィスからも）

また、無線LANを導入した場合は、侵入のセキュリティリスクが高まります。社内のファイルサーバーにアクセスされ、顧客情報や機密情報を抜かれたり、システムを停止されたり、といった被害が及ばないように、暗号化や認証等の技術を使い、セキュリティ対策を講じる必要があります。最近では**スマートデバイス**や**クラウドサービス**を利用して業務の重要な情報をやり取りするケースも増えてきていますので、これらも含めたセキュリティ計画をたて、リスク管理を徹底することが重要です。

PoE［Power over Ethernet］
Ethernetの配線に使用するケーブルを利用してネットワーク機器に電力を供給する技術のこと。

スマートデバイス
ここでは、スマートフォンやタブレット等の総称として使用する。インターネットの利用、文書の閲覧など、パソコンと同じような使い方ができる。

クラウドサービス
データベース、サーバーなど、ソフトウェア、ハードウェアの各種リソースをインターネットを経由して利用するサービスの総称。ユーザーは、インターネットへ接続する環境があれば、これらのサービスを、自社で構築。運用するよりも、安価で容易に利用できるものがある。

P検1級対策

どんなに小規模であっても、無計画にLAN構築、機器類の設置をすることのないよう、論理構成と物理構成を十分に考えた上でLAN構築を行います。
P検1級の問題では、ネットワーク構築の目的を踏まえた上で、ニーズに応じた有線LAN、無線LANの選定を行っているかどうか、またセキュリティ計画が万全であるかが問われます。

（メモ）　　年　月　日

（2）企業内ネットワークを構築することができる

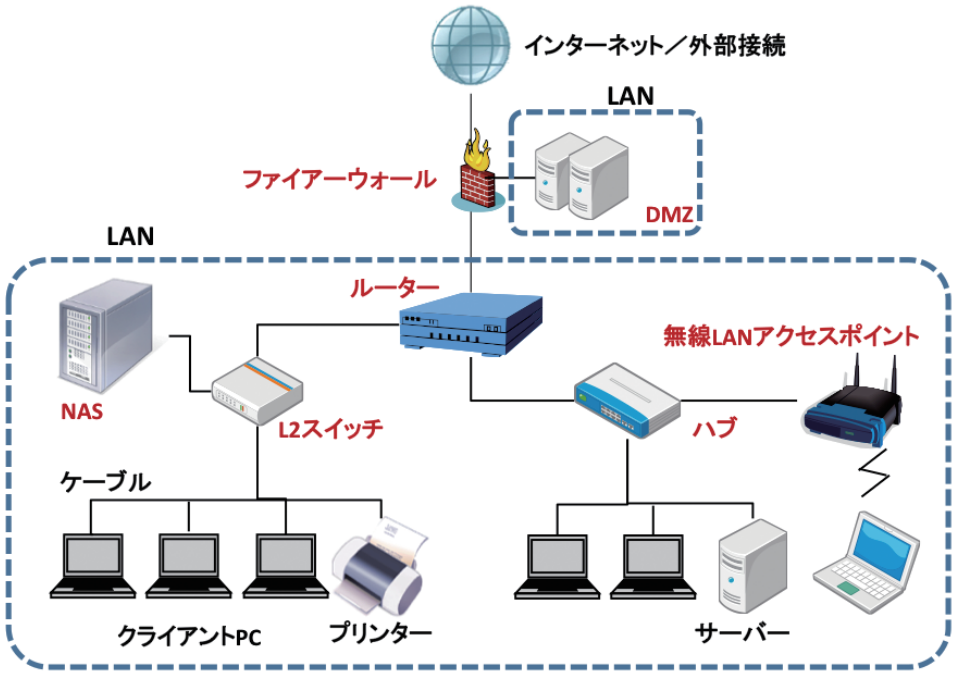
1．企業内の小規模LANを構築できる

前項までは、企業内でのネットワークを構築する際に必要な論理的な設計と物理的な設計についてのポイントを解説いたしました。本項では、それらの考え方に基づき、実際に、企業内で小規模な**LAN**を構築する際、必要となる機器と、それらの役割について、また、LAN構築後、どのような管理体制で運用をしていくべきか、それらのポイントについて解説いたします。

▼LANの構成要素

まずは、LANを構築するために、どのような役割を担う機器類が必要なのか、効率よく通信を行うLAN構築のための構成要素としての機器と役割について解説します。図Aが小規模LANの構成要素を表すイメージ図です。

＜図A　LAN構成イメージ図＞



LAN
［Local Area Network］
一般家庭、企業のオフィス、同じ施設内などにあるコンピューターやプリンター、通信機器などを接続した通信ネットワークのこと。

ファイアーウォール
外部ネットワークから社内ネットワークへの不正アクセスを防ぐための機能またはそれの機能を備えた装置。

DMZ
DeMilitarized Zoneの略。
非武装地帯。
インターネット接続環境において、公開サーバーを置くためにファイアーウォールによって外部・内部両方のネットワークから隔離されたセグメント。

ルーター
ネットワーク上のデータを、他のネットワークに中継する装置。ネットワーク層のアドレスによって、どの経路を通して転送すべきかを判断する経路選択機能がある。

ハブ
スター型物理トポロジーを取るネットワークにおいて、中心に位置する集線装置。

L2スイッチ
（レイヤ2スイッチ）
ネットワークの中継機器の一つで、データリンク層のデータで中継先を判断し、中継動作を行う。データリンク層がOSI参照モデルにおける第2層（レイヤー2）に属するため、L2スイッチと呼ばれている。

無線LANアクセスポイント
無線LANで端末を接続する際の中継親機。 Wi-Fiアクセスポイントということもある。

（メモ）　　年　　月　　日

図A の通り、小規模なLANでは、クライアントPCやサーバー、**NAS**等の情報端末、ハブ、L2スイッチ、ルーター等の各ネットワーク機器がケーブルや無線で接続され、**Ethernet（イーサネット）**という規格のもと、**TCP/IP**で通信を行っています。これらの各機器をケーブルで接続するLANを有線LANと言い、ケーブルを使用せず、無線LANアクセスポイント経由で無線で接続するLANを無線LANと言います。業務の性質や内容によって有線か無線かを使い分ける必要があります。

これらの規格に沿った機器の役割と選定のポイントについて解説します。

▼LAN構築に必要な機能と機器

前述の規格Ethernetの接続形態は、通信速度やケーブル最大長によっていくつかの種類にわけられます。

表3. 主なEthernetの種類

名称	最高伝送速度	ケーブル最大長
10BASE-T	10Mbps	100m
100BASE-T	100Mbps	100m
1000BASE-T	1Gbps	100m

現在、多くのパソコンに搭載のネットワークインターフェースは、1000BASE-Tと呼ばれ、ギガビットイーサネットに対応しています。しかし、接続する既存の資産が必ずしもギガビットイーサネットに対応しているとは限りませんので、接続する既存資産の仕様を再度確認し、それらに対応した通信機器を選定するようにしましょう。

また、業務に求められる用途（役割）を整理し、それに合わせた機器の選定も必要です。例えば、最近では、LANに直接接続し、共有ディスクとして使用できるNASの使用も増えています。NASは、アクセス権設定が可能なことから、共有ディスクやバックアップディスクとしての選択肢以外に、簡易的なファイルサーバーとしての運用の可能性もあります。

そして、各機器類の接続、という視点で見れば、接続機器と電源が遠い、配線スペースが不足している、といった問題がでてくることもあるでしょう。そのような場合は、PoE対応機器を使用するなどして、LAN経由で電源を供給するという解決策も考えられます。

NAS
[Network Attached Storage]
ネットワーク（LAN）上に接続できる記憶装置（ファイルサーバー専用機）。ネットワークインターフェースやOS、管理用ユーティリティなどが一体化されている。クライアントPCからは共有ディスクとして使用可能。

Ethernet（イーサネット）
一般家庭、企業のオフィス、同じ施設内などにあるコンピューターやプリンター、通信機器などを接続するための規格。

TCP/IP
インターネットやLANなどの標準プロトコル体系のひとつ。

10BASE-T
転送速度10Mbpsのツイストペアケーブルで、ハブを使って各機器を接続するスター型のEthernet。ハブの多段接続は4段階まで可能。

100BASE-T
転送速度100MbpsのEthernet。100BASE-T用の機器は10BASE-Tと互換性があるものが多いため、同じネットワークに混在させることができる。

1000BASE-T
最高伝送速度が1Gbpsで、Gigabit Ethernet（GbE）に対応した規格の中で最も普及している。

（メモ）　　年　　月　　日

▼アドレス体系と管理体制

LAN内の構成要素が決まったら、LANに接続する機器に、**IPアドレス**を割り当てます。IPアドレスは、体系を決め、計画的に割り当て、管理表を作成し、維持管理していく必要があります。アドレス体系は、

・接続する端末やサーバーは何台あるか
・将来どのような拡張を予定するか
・外部ネットワークとのやりとりは必要か（公開サーバーが必要か）
・全社で共有するものは何があるのか
・機材の交換や新規追加の可能性はあるか
・オフィスのフロア構成を考慮しているか
・部門、部署ごとに流通させる情報があるか
・拠点が複数ある場合、他拠点の管理はどうするか

などを留意して、計画を立てるようにしましょう。

＜表4.　IPアドレス割り振り（例）＞

接続端末台数（目安）	IPアドレス
1 ～ 100台	192.168.0.0 ～ 192.168.255.255/16
101 ～ 1000台	172.16.0.0 ～ 172.31.255.255/12
1001台以上	10.0.0.0 ～ 10.255.255.255/8

※必ずしもこの限りではありませんが、専門家の方が混乱しないIPアドレス割り振りの一例です。

現在、広く用いられているIPアドレスは**IPv4**と呼ばれるものが主流で、インターネットに接続する、世界で唯一のIPアドレスであるグローバルIPアドレスと、企業ネットワーク内で自由に使用できるプライベートIPアドレスに分かれます。いずれも利用できるアドレスの範囲が定められています。IPアドレスは、**サブネットマスク**によりネットワーク部とホスト部に別れて識別され、同一サブネット内に付与されるIPアドレスの個数も変わってきます。最近では、IPv4が枯渇し、**IPv6**を使うようになってきています。

IPアドレス
[InInternet Protocol Address]
インターネットやイントラネットなどのTCP/IPプロトコルを利用したネットワークにおける識別番号のこと。ネットワークに接続された個々のコンピュータに割り振られる。

IPv4
[Internet Protocol version 4]
現在普及している32ビットのIPアドレスを使用したインターネットの通信プロトコル。32ビットで識別できるコンピューターは2の32乗（42億9496万7296）台が最大のため、アドレス不足となり、近年128ビットで管理するIPv6［Internet Protocol version 6］への移行が進んでいる。

サブネットマスク
IPアドレス内のネットワークアドレス（ネットワークを識別する部分）とホストアドレス（個々のコンピューターを識別する部分）を判別するための表記。
サブネットマスク表記例：
255. 255. 0. 0　または　/16
255. 255. 255. 0　または　/24
255. 255. 255. 128　または　/25

IPv6
[Internet Protocol Version 6]
インターネットプロトコル（IP）のIPv4を拡張し、コンピューターに割り当て可能なIPアドレス数を拡大させたプロトコルのこと。IPv6ではアドレス情報を128ビットで表記しており、10の38乗という桁数のIPアドレスを識別することができる。これは実質上無限といえる数などで、パソコンだけでなく情報家電をはじめとしたあらゆる機器にIPアドレスを割り当ててもまだ余裕があると言われている。

（メモ）　　年　　月　　日

また、LANの規模が大きくになるにつれ、接続する機器やユーザー情報が増えてきますので、これらを一元管理できる仕組みも必要になります。この一元管理を**ドメイン**単位で実施する代表的な仕組みとして、Windows系サーバーの**Active Directory**があります。

ドメイン
ネットワークの管理単位。この文脈では、LAN上で同じデータを共有したり、権限をもつユーザーやコンピュータのグループを識別する名称の意味。

Active Directory（AD）
Microsoft社が提供するディレクトリ・サービス・システムで、Windowsサーバーに導入されている。ユーザーや接続機器、アクセス権限等を一括管理できる。Apple社のMacサーバーであれば、Open Directoryが同様の機能をもつ。

P検1級対策

LANを構成するための必要な機能や機器、特に、LAN内に構成するべき既存・新規機器の選別や、IPアドレスの具体的な割り当て計画を意図して行えるかどうかが問われます。そのためにIPアドレスの基本的な体系を理解しており、できるだけシンプルな管理、運用方法を選定することがポイントです。

（メモ）　　年　　月　　日

2. ネットワークの分割ができる

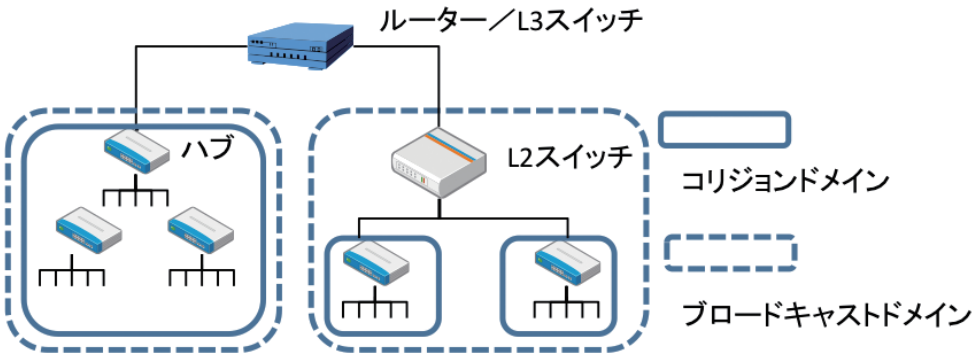
企業内ネットワークを効率よく運用するためのネットワーク分割について、目的や手法、具体的施策について解説します。

▼ネットワーク分割する目的や理由の策定

企業内ネットワークにおいて、例えば、

・接続台数が増え、ネットワークトラフィックが増えてきたので負荷分散したい。
・他部署から技術部と総務部への通信を制御したい。

など、ブロードキャストを代表とする通信トラフィックやアクセス権の制御が必要となる場合がでてきます。この場合、ネットワーク分割を行うのがより一般的で確実です。このネットワーク分割を行うためには、**コリジョンドメイン**と**ブロードキャストドメイン**、そしてネットワーク機器の機能を理解することが重要です。



ネットワーク分割により、トラフィック制御、アクセス権制御はもちろん、ネットワークアドレスや端末管理が容易になるといった管理上の利点もあります。

コリジョン
イーサネット上で同一伝送路上にある異なる端末が、同時に信号を送信した際に発生するデータの衝突現象。

コリジョンドメイン
イーサネットのネットワーク上で衝突信号が伝わる範囲。通信トラフィックの衝突、渋滞が影響する範囲。

ブロードキャスト
ネットワーク内で、不特定多数の端末にデータを送信すること。同報通信。

ブロードキャストドメイン
ブロードキャストが届く範囲

（メモ）　　年　　月　　日

▼ネットワーク分割する方法の理解

ネットワークを分割するための手段として、1）**サブネットマスク**を使ったサブネット分割と、2）VLAN　の2通りの方法について説明します。

1）サブネットマスクを使ったサブネット分割

IPアドレスは、ネットワークアドレス部とホストアドレス部に分かれて識別されます。

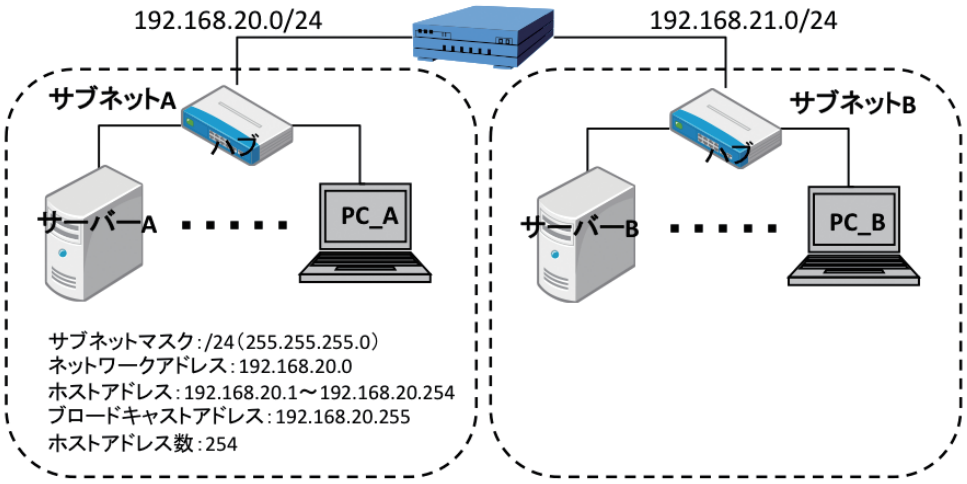
例）サブネットマスク　/24　の例

24ビット（ネットワークアドレス）	8ビット（ホストアドレス）

このIPアドレスのネットワークアドレス部分を使用し、複数の論理ネットワークに分割することを「サブネット化」と言います。そして、このネットワークアドレスを識別するための表記を「サブネットマスク」と言います。

サブネット分割では、分割したいネットワークに属する各機器を、物理的にわけて、ハブ、そしてそのハブを、スイッチやルーターに接続します。

＜図B　サブネット分割されたネットワーク図＞



PC＿A　→　サーバーA　アクセス可能　PC＿A　→　サーバーB　アクセス不可
PC＿B　→　サーバーA　アクセス不可　PC＿B　→　サーバーB　アクセス可能
サーバーAとPC＿A間で大量データのやりとりが発生しても、サーバーBとPC＿B間の通信に影響を与えない。

このように、サブネット分割をすると、物理的な関係を基本にしたネットワーク分割ができ、保守や障害対応を行いやすくなります。

サブネットマスク
IPアドレス内のネットワークアドレス（ネットワークを識別する部分）とホストアドレス（個々のコンピューターを識別する部分）を判別するための表記。
サブネットマスク表記例：
255. 255. 0. 0　または　/16
255. 255. 255. 0　または　/24
255. 255. 255. 128　または　/25

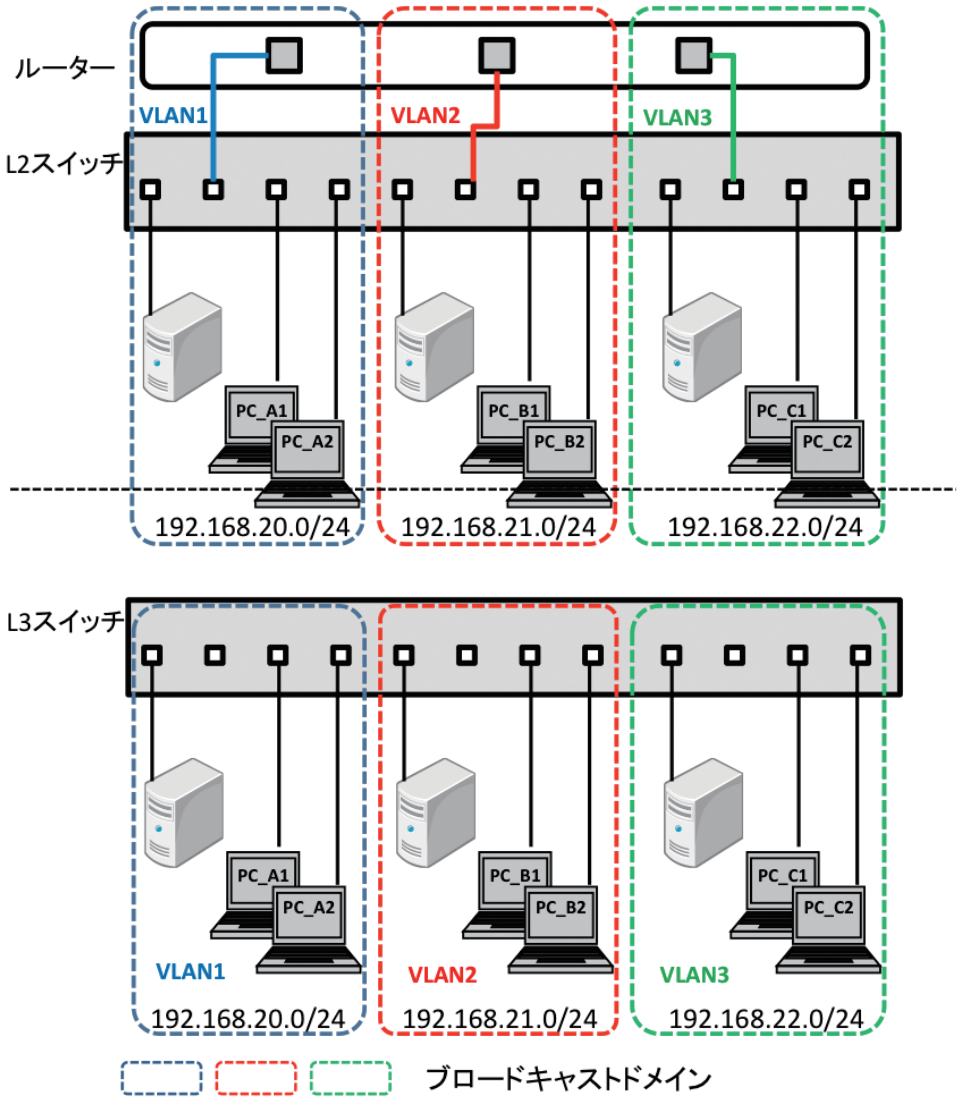
（メモ）　　年　　月　　日

2）VLAN（Virtual LAN｜仮想LAN）

VLANは、物理的な接続形態とは独立した、端末の仮想的なネットワークを実現します。VLANでは、**L2スイッチ**や**L3スイッチ**といった、回線やパケットの交換（スイッチング）機能を持った通信機器で構成します。L2スイッチはOSI参照モデルの第2層（レイヤ2）、L3スイッチは同じくOSI参照モデルの第3層（レイヤ3）で、通信を制御します。また、ネットワーク機器の一つである「スイッチングハブ」はL2スイッチに含まれます。

L2スイッチ／L3スイッチ
ネットワークを中継する機器。L2、L3は、それぞれOSI参照モデルのレイヤ2、レイヤ3を差す。

＜図C　VLAN＞



（メモ）　　年　　月　　日

このように、VLANでは、各ポートにVLAN番号（図CではVAN1 ～ VLAN3）を割り当てることでネットワークを分割します。この方式を、ポートVLANと言います。例えば、オフィスのレイアウト変更等で、VLAN3に接続されていた端末の一部をVLAN2に接続する場合は、ケーブルの配線をやり直すことなく、スイッチ上のVLAN定義の変更を行うだけなので、社内ネットワークの拡張・変更に柔軟に対応できる手法と言えます。最近では、このポートVLANに、**IEEE 802. 1Q**で標準化された**VLANタギング方式**（タグVLAN/タギングVLAN/VLAタグ方式ともいう）を組み合わせた構成がVLANの主流となっており、スイッチ間を通したVLAN設定が、より柔軟に行えるようになってきました。

IEEE 802. 1Q／VLANタギング方式
各社が独自方式で開発実装していたVLANの相互運用性を確保するため、IEEEによって標準化された規格。ポートVLANでは、スイッチ間を接続するために、VLANの数だけ、それぞれのスイッチにポートを確保する必要があったが、VLANタギング方式では、パケットにタグと呼ばれる数BytesのVLAN情報を付加して一つのポートを複数のVLANに所属させることができる。そのため、構成の変更や拡張がより容易になる。

▼ネットワーク分割計画の策定と実施

ネットワーク分割は、ネットワークの物理的構成（OSI参照モデルのレイヤ1の物理層、レイヤ2のデータリンク層のネットワーク、つまり、ケーブルの配線やPCの配置、VLANの設定）と論理的構成（レイヤ3のネットワーク層以上のネットワーク、つまり、ルーターを中心とした構成）を把握し、

・接続する端末台数と将来的な拡張性
・セキュリティ確保の必要性
・費用

等、解決すべき課題の優先度を考慮して行いましょう。

また、ネットワーク分割では、柔軟なネットワーク構成が可能になる反面、ネットワーク構成を複雑にしてしまうデメリットもあります。特に、ネットワーク規模が拡大してくると、フロア間、拠点間通信などで発生する通信障害を迅速に切り分けるために、通信経路に**インテリジェントハブ**を設置して、**SNMPマネージャー**と組み合わせ、リモートからの集中管理を行う仕組みも視野に入れましょう。

インテリジェントハブ
スイッチングハブにネットワーク管理機能を搭載した製品。SNMPマネージャーと組み合わせることで、LANやWAN上にあるインテリジェントハブの一ヶ所集中管理が可能となる。

SNMP/SNMPマネージャー Simple Network Management Protocol
ネットワーク経由で機器を管理するためのアプリケーション層のプロトコル。ルーター、スイッチなど、TCP/IPネットワークに接続された通信機器をSNMPエージェントと言い、それらを管理するソフトウェアをSNMPマネージャーと言う。

P検1級対策

最近の企業内ネットワークでは、VLANを使ったりL3スイッチを使ったりすることが主流となっています。L ANを分割する目的や理由を明確にし、LAN分割の方法について、それぞれの違いとそれらを構成するために必要な機器についてしっかりと理解しましょう。

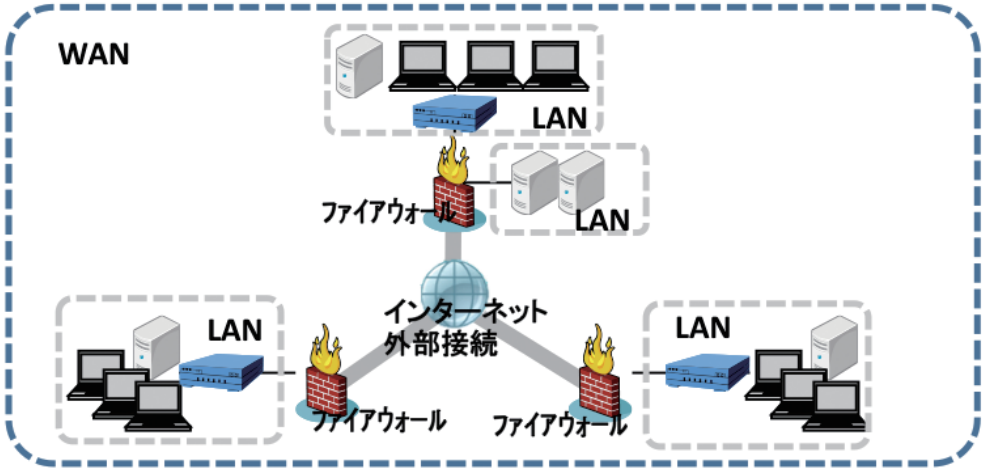
（メモ）　　年　　月　　日

3. 複数拠点を接続するネットワークを構成できる

複数拠点を有する企業では、拠点単位でのサーバー設置、インターネット接続を行っているケースも多く見られます。しかし、業務効率化や情報共有、セキュリティといった観点から、拠点内ネットワーク（LAN）同士を接続する拠点間ネットワーク（**WAN**）の設計・構築が必要です。

WAN
Wide Area Network　の略。
広域通信網と訳される。地理的に離れた拠点間のLANを接続しているネットワークのこと。

＜図D　．WANイメージ図＞



拠点間ネットワークの設計では、「通信事業者のサービスを使用する」必要があり、その点が、LANの設計と大きく異なります。通信速度・性能・費用が異なる、様々なWANサービスの中から、自社に最も適したサービスを選定し、設計･構築を行わなければなりません。

▼流通調査と利用計画と利用アプリケーション策定

自社に適したサービス選定のためには、LANと同様、自社の現状を踏まえた利用計画が必要です。利用計画にあたっては、次の三つの視点で情報を整理しておきます。

1）WAN経由で利用するアプリケーション

e-mail、ファイル共有、ブラウザといった情報系アプリケーション、ERP、SFA等の基幹システム、**VoIP**、テレビ会議等、各事業所が利用したり今後導入を検討したりしているアプリケーションを整理し、業務遂行に必要な帯域算出のための基本情報とします。

VoIP
Voice over Internet Protocol の略。
IPネットワーク上で音声データを伝送する技術。SIPやH. 323という規格がある。VoIP対応アプリケーションとしては、Skype,LINE、Google Voice等がある。PC以外に、スマートフォン対応のアプリも充実してきている。

2）利用端末数と既存回線接続状況（現状と今後の増減見込み）

接続端末数と今後の情報量の増減見込み、ADSL,光回線接続といった、現在の回線契約接続状況を整理します。

（メモ）　　年　　月　　日

3）現状の問題点の洗い出し

ある特定の時間帯に通信が極端に遅くなる、ネットワーク接続が切れる、といったネットワークトラフィックの問題を洗い出します。

上記三点に加え、拠点間ネットワークを導入することで、何か特別な操作が必要になるなど、操作性が大きく変更されることのないよう、利用ユーザーの操作性の面からの検討も必要です。物理面では、拠点間ネットワーク構築によってあらたに配置する機器やケーブル、電源、配線ルート等もあらかじめ確保しておくとよいでしょう。

▼各サービス理解

複数拠点間ネットワークの構築に際しては、通信事業者（キャリアとも言います）が提供している固定電話、ISDN、専用線、**ATM**、IP-VPN、広域イーサネット、といった広域通信網のサービスを利用することが前提です。各サービスの違いをよく理解し、速度、品質、費用、等を総合的に判断して、既存機器の再利用や、単一サービスなのか、複数サービスを組み合わせるのかも含め、自社に最適なサービスを選択します。

主なWANサービスとしては、専用の回線で直結する直結回線と、多数の利用者で共有する共用回線があります。

表5. 直結回線のWANサービス

回線の種類	特徴
専用回線	地上や地下に敷設された銅線や**光ファイバー**を使い、特定の拠点間を結ぶWANサービス。一般に「専用線」と言う。ユーザー専用の帯域が確保されている専用回線で、安定性、品質は高い。料金は、通信速度や距離に依存し、一般的に高額。専用のインターフェースを持った機器（主にルータ）が必要。
公衆回線	距離と通信速度、通信時間で料金が決まる従量制。大別すると、公衆回線網に代表されるアナログ網回線とISDNに代表されるデジタル回線に分けられる。公衆回線網はモデムを必要として、最近ではほとんど利用されていない。**ISDN**も減少傾向にあるが、バックアップ回線（次表参照）として採用されるケースがある。
ダークファイバ	企業等が敷設している光ファイバーのうち、使用せずに余っている線を他の事業者に貸出し、接続する伝送装置や中継器などは事業者側で用意する形態のサービス。

ATM
Asynchronous transfer modeの略。B-ISDN（広帯域ISDN）の伝送方式で、音声、データ、映像といったマルチメディア通信を広帯域で実現する技術。キャリアのバックボーンとして利用されるケースが多い。

光ファイバー
光を使った通信ケーブル。大容量のデータを長距離伝送できる。

ISDN
Integrated Services Digital Networkの略。電話やFAX、データ通信を統合して扱うデジタル通信網。従量課金制。

（メモ）　　年　月　日

図E. 直結回線

表6. 共用回線のWANサービス（バックボーン回線）

回線の種類	サービス名	特徴
バックボーン	広域 イーサネット	企業ネットワーク構築においてメジャーなサービスの一つ。LAN接続と同様にイーサネットのポートを提供するサービスで、レイヤー2をベースとする。接続用機器として、ルーター以外に、L2スイッチ・L3スイッチが使用可能。
	IP-**VPN**	通信業者の閉域IPネットワーク網を共用利用したIPプロトコルを使ったネットワーク。
	インターネットVPN	インターネット上でIPプロトコルを使ったネットワーク。他と異なり、インターネットを使用するため、データ盗聴や成りすまし対策として、**PPTP**や**IPsec**といった**トンネリング**プロトコルを使用して通信するのが一般的である。

表7. 共用回線のWANサービス（アクセス回線）

回線の種類	サービス名	特徴
アクセス	FTTH	光ファイバを伝送路として、データ通信はもとより、電話、テレビ、動画配信など統合的な通信サービスの総称。加入者側には**ONU**が設置される。
	ADSL	電話線を使い、高速なデータ通信を非対称通信で行う技術。よって上りと下りの速度が異なることに留意する必要がある。ADSLで用いるモデムをADSLモデムと言う。

VPN
Virtual Private Network の略。企業内ネットワークの拠点間接続などに使われ、あたかも専用回線であるかのように利用できるサービス。VPNには、IP-VPN,インターネットVPN、レイヤ2VPN、SSL-VPNなどがある。

PPTP
Point-to-Point Tunneling Protocolの略。Microsoft社によって提案された暗号通信プロトコル。リモート アクセス用に設計されたPoint-to-Point プロトコル（PPP：Point-to-Point Protocol）を**カプセル化**して通過させる

カプセル化
転送パケットにヘッダ情報を付加し、元の通信プロトコルとは別の通信プロトコルとして送る技術。

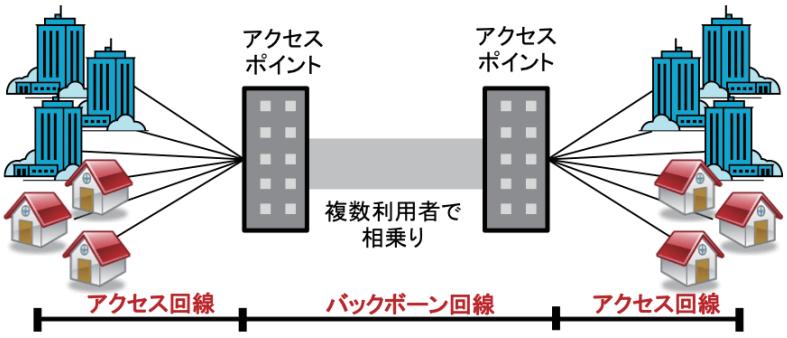
IPSec
Security Architecture for Internet Protocol 。パケット通信で改ざん防止や秘匿機能を提供するプロトコル。

トンネリング
元の通信プロトコルをカプセル化して、異なる通信プロトコルとして透過的に伝送する技術。

ONU
Optical Network Unitの略。光回線終端装置。

（メモ）　　年　　月　　日

図F.　共用回線におけるバックボーン回線とアクセス回線



▼冗長性や代替案の策定

「ただ接続すればよい」「コストをあまりかけられないのでこの位のサービスで」「最新だから」など、安直な考えで拠点間ネットワークの設計・サービスの選定を行うと、後々トラブルを引き起こす原因となります。まずは、利用するアプリケーションの重要度、優先度を整理し、拠点間ネットワーク導入後、それらのアプリケーションを使用することで社内の課題がどのように解決され、業務がどう改善されるのかを理解・共有することに注力しましょう。そして、LAN構築と同様、運用保守面を考慮し、冗長性の確保も検討します。拠点間ネットワークの冗長化を行うポイントとして、以下の視点を持っておくとよいでしょう。

・バックアップ回線

ネットワーク停止による機会損失を最小限にとどめるための予備回線を持つ。若干遅くても、通常業務を継続させる。尚、予備回線は、主回線と別業者、別経路を採用する方がよい。

・負荷分散

一時的なトラフィック高負荷によるレスポンス低下等、ネットワーク遅延に対する対策。いつどのような負荷が何のためにおきるのかの事前予測も必要。

また、拠点間ネットワークの運用を考えた場合、遠隔で解決できるサービスやツールを用いるなど、迅速な障害対応に対する対策も必要です。そして、ハブやスイッチ、ルーター等、各種接続機器の技術革新に伴い、WANサービスも、新しいサービスが次々に展開されています。以前のように、一度構築したら5年、10年現状維持でよい、というわけにはいきません。常に通信量や利用状態を把握し、今後の通信量の予測をたてながら、帯域を増減したり新サービスに移行したりするなど、PDCAを行いながら運用し、社内の最適な通信状態を確保、維持していきます。

P検1級対策

キャリアの最新サービスには、敏感に、常に情報のアンテナをはっておき、より安定した運用管理の選択肢として考慮しておくことが重要です。P検1級の問題では、これらの選択肢の中から、自社の課題解決、目的にあったサービス選定を意図して行っているかが問われます。

アクセス回線
事業所や自宅など利用者宅から通信事業者が提供するアクセスポイントまでを接続する回線。

バックボーン回線
ネットワーク通信の中枢として集線装置間や拠点間、あるいは事業者間、などを結ぶ大容量の通信回線網。幹線ネットワーク、コアネットワークとも言う。

（メモ）　　年　　月　　日