第1章

ネットワーク基礎知識と午後問題の解き方

ネットワークスペシャリスト試験の勉強をするにあたって，基礎を身につけることはとても大切です。本章ではまず，ネットワークの勉強を行う上で基本となる，通信の仕組みやOSI基本参照モデル，TCP/IPプロトコルや通信方式について学びます。
また，ネットワークスペシャリスト試験で合否を分けるのは午後試験です。第2章以降でそれぞれの技術分野に対応した午後問題を演習として取り上げますが，本章ではその前に，過去の午後Ⅰ問題と午後Ⅱ問題から1問ずつ取り上げ，それぞれについて，問題文の読み方と解き方のコツを詳しく解説します。

1-1 ネットワークとは

ネットワークスペシャリスト試験の対象となるコンピュータネットワークは，今も進化をし続けています。プライベートなネットワークからインターネットの接続まで，様々なレベルのネットワークについて全体像をつかみ，世界中の情報をネットワークで結ぶ手法や，その実践，管理などのスキルを身につける必要があります。

勉強のコツ

ネットワークの学習では，基本をしっかり押さえておくことが肝心です。
はじめての方はまず，この章で基礎知識を学習し，ネットワークの全体像をつかんでから，第2章以降の学習に進んでいきましょう。
すでにある程度知っている方は，「1-1　ネットワークとは」は飛ばしても大丈夫ですが，基礎を確認してから次に進むのもおすすめです。
また，「1-2　午後問題の解き方」では，午後問題の解き方を詳しく解説しています。次章以降の演習問題では午後問題が登場しますので，そちらに取り組む前に，ぜひ目を通しておいてください。

発展

インターネットはもともと，軍事技術の応用から発展していきました。アメリカの国防総省（DoD：United States Department of Defense）が中心となって，アメリカ西海岸の大学や研究所などの四つの拠点を結んだARPANET（Advanced Research Projects Agency Network）がインターネットの起源です。

ネットワークの進化

昔，コンピュータが普及し始めた頃には，コンピュータは1台1台，単独で使われていました。その利用形態を**スタンドアロン**といいます。しかし，コンピュータが進化するにつれて，複数のコンピュータを互いに接続することで情報の伝達や共有を行う**コンピュータネットワーク**が発明されました。

初期のコンピュータネットワークは，管理者が特定のコンピュータ同士を接続しただけのものでした。このようなネットワークを私的（プライベート）なネットワークといいます。それが徐々にプライベートなネットワーク同士を接続する公共（**パブリック**）のネットワークへと移行していきました。その一番大きなものが，世界中のネットワークが接続されたインターネットです。

1-1-1 通信の仕組み

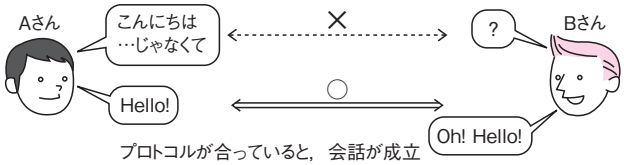
コンピュータネットワークでの通信では，コンピュータとコンピュータの間で情報を伝達します。人間同士が会話をする場合には，少しぐらい言葉を間違えても相手が適切に解釈して直してくれることが多いですが，コンピュータの場合はそのような融通は利かないので，きっちり，ミスのないように相手にデータを送る必要があります。

そのために，通信を行うときには，プロトコルと呼ばれる約束ごとをきちんと決めておき，それに合わせて相手にデータを送ります。

プロトコル

プロトコルとは，コンピュータとコンピュータがネットワークを利用して通信するために決められた約束ごとです。プロトコルをきちんと決めておくことによって，メーカやCPU，OSなどが異なるコンピュータ同士でも，同じプロトコルを使えば互いに通信することができます。

人間の会話に例えると，日本語や英語などの言語がプロトコルに相当します。そして，会話を通して話の内容（データ）を相手に伝えていきます。このとき，下図のように，受け手（Bさん）が日本語を知らず英語しか分からない場合には，話し手（Aさん）はデータを英語にして相手に伝えていく必要があります。



プロトコルを使った会話

コンピュータの場合は，会話の前後から意味を推測するといった高度なことはできないので，このプロトコルをしっかり決めておく必要があります。例えば，通信に障害が発生したらどうするかなど，通信中に起こりうる問題をあらかじめ考えておき，その

ときの対応なども一つ一つ決めておく必要があります。このように，コンピュータ間の通信では，**プロトコルをきめ細かく決めて，それを守ること**が大切です。

プロトコルの標準化

発展
プロトコルを独自のものにして別のメーカの機器とは通信できないようにすると，最もシェアの高い1位のメーカが圧倒的に有利になります。そのため，2位以下のメーカの中では早くから，メーカが異なっても互いに通信できるような互換性が大切だという認識が広まっていました。

コンピュータネットワークが広がり始めた当初は，プロトコルは各社が独自に開発していました。例えば，IBMは自社の通信技術を体系化したネットワークアーキテクチャ，SNA（Systems Network Architecture）を発表し，プロトコル群を体系化しました。しかし，このネットワークを使うためにはネットワーク上のすべての製品をIBM製にしなければならず，利用者にとって非常に不便でした。

そこで，メーカが異なっても互いに通信できるような互換性が重要であると認識されるようになり，プロトコルの**標準化**の必要性が言われるようになりました。

この問題を解決するために，国際標準化機構のISO（International Organization for Standardization）は，国際標準として**OSI**（Open Systems Interconnection：開放型システム間相互接続）と呼ばれる通信体系を標準化しました。

また，公共団体ではありませんが，大学などの研究機関やコンピュータ業界が中心となって推進してきた団体IETF（Internet Engineering Task Force）では，インターネットの標準である**TCP/IP**（Transmission Control Protocol/Internet Protocol）の提案や標準化作業が行われています。TCP/IPはインターネットの**デファクトスタンダード**であり，世界中で最も広く使われている通信プロトコルです。

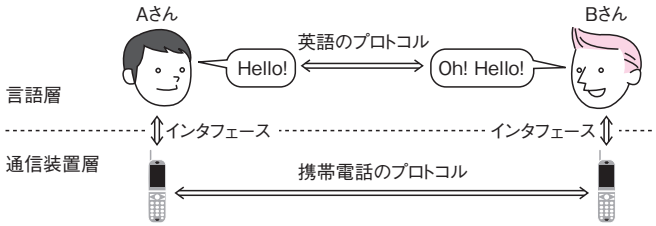
用語
デファクトスタンダード（De facto Standard）とは，国際機関や公的機関が定めた標準ではありませんが，事実上の標準として広まっているもののことです。

プロトコルの階層化

一つのプロトコルにいろいろな役割を詰め込みすぎると，プロトコルは複雑になりすぎてしまいます。そのため，プロトコルをいくつかの機能に分けて階層化するという考え方が提唱されました。次の節で紹介するOSI基本参照モデルは，その階層化の代表例です。

先ほどの会話の例で階層化を説明すると，直接会話をするのではなく携帯電話を使って2人が会話をする場合ということにな

ります。つまり，このとき，言語層と通信装置層という二つの階層ができるのです。



プロトコルの階層化

上の図では，会話をしているのはAさんとBさんなのですが，外から見ると，Aさんは携帯電話に話しかけているように見えます。この，Aさんと携帯電話の境界となる部分のことをインタフェースといいます。インタフェースを通じて，言語層から通信装置層にデータを渡し，通信装置の階層でのプロトコルを使って，データをBさんの携帯電話に伝送します。そこからまた，インタフェースを通じて，Bさんに会話内容を伝えるのです。

プロトコルを階層化しておくと，言語層，つまり会話をする言語を英語からフランス語に変えても，互いがフランス語を知っていれば会話は成立します。また，通信装置層，つまり通信装置を携帯電話から無線機や固定電話に変えても，両方が同時に変更すれば通信可能です。このように，プロトコルを階層化することによって，様々なプロトコルを組み合わせて通信を行うことが可能になります。

パケット

データを送るときに，大きなデータをそのまま送ると，ネットワークに負担がかかるうえ，時間がかかって大変です。そのため，コンピュータネットワーク上では，大きなデータを**パケット**と呼ばれる小さな単位に分割して送信する**パケット交換**という手法が用いられます。

データを送るときには，そのデータに，送信元コンピュータとあて先コンピュータの**アドレス**など，送るために必要な情報を書き込んで，ネットワークに送ります。その情報を書き込む部分が

関連

プロトコルの階層化は，ソフトウェアを開発するときのモジュール化の概念に似ています。例えば，OSI基本参照モデルでは，第1層から第7層までのモジュールを作ってそれをつなぎ合わせれば，通信が可能です。モジュールごとに独立していれば，それを取り替えることが可能という点でも似ている概念です。

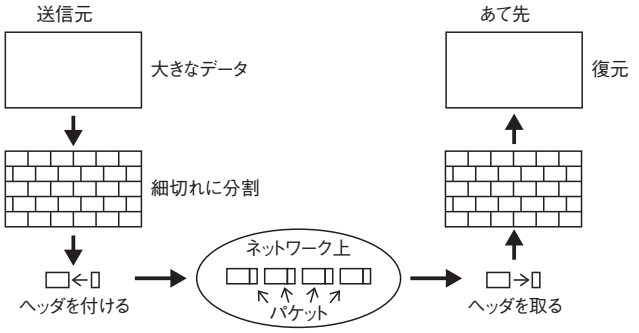
用語

アドレス（Address）とは，あるものの所在を指し示す情報のことです。一般的な社会でいうと，小包などに書く差出人や送り先の住所にあたります。
コンピュータネットワークの場合は，様々な種類のアドレスがあります。例えば，LANカードなどのネットワーク機器に割り当てられるMACアドレス，コンピュータを識別するために割り当てられるIPアドレスなどです。
様々な種類があり，また付け替えも頻繁に起こるため，ネットワークスペシャリスト試験の勉強では，このアドレスについての理解が大切になります。

用語

パケット交換という言葉は，パケットを交換して通信する仕組み一般を指します。以前はパケット交換網という通信サービスがありましたが，現在の通信サービスではほとんどパケット交換を行うので，わざわざパケット交換という呼び方はしなくなっています。

ヘッダです。パケット交換では，パケットごとにヘッダを付けて送り出すことによって，どのコンピュータ間の通信なのかをヘッダを見て判断することができます。



パケットを使った通信の様子

パケット交換で正しく通信するためには，パケットの送信元とあて先の両方で，ヘッダの内容を解釈するためのプロトコルが同じである必要があります。

覚えよう！

- □　**プロトコルは，通信の約束ごとで標準化し階層化**
- □　**パケットは，データを分割しヘッダを付けて送信**

コラム　人と人とを安全に結ぶためのネットワーク

ネットワークという言葉は，コンピュータネットワーク以外でも様々な場面で使われています。人や組織のつながりによる社会的なネットワークもありますし，鉄道路線や高速道路などの交通網のネットワークもあります。これらのネットワークの目的は，「人と人とを結びつける」ことにあります。

コンピュータネットワークは，最初はコンピュータ同士を結んで，より便利にすることが目的でした。しかし今では，ほかのネットワークと同様に，人と人とを結ぶことが目的になってきています。

インターネットが普及することで，FacebookなどのSNSを通じて友人などに近況を知らせたり，WebやYouTubeなどを通じて世界中の人に情報を発信したりすることができるようになりました。こうしたことが，日常生活や企業活動，学校やその他の場所での学習に大きな影響を与えています。

筆者も，本だけでなく，ブログやUstream，YouTubeなどで情報を発信しています。インターネットを通じて発表することで，試験を受ける人からのフィードバックも得ることができ，より双方向でつながることが可能になりました。

ただ，全世界の人がネットワークを通じて国境を越えて自由につながるということは，利便性が高まる一方，危険とつながる可能性も高くなります。世界にはいろいろな人がいますし，世界中の悪意をもった人ともつながるからです。コンピュータウイルスによる被害，インターネットを介した詐欺事件など，世界中で様々な事件が起きています。

そのため，今日のネットワークは，人と人とを自由につなぐことだけでなく，「安全につなぐ」ことも大切です。それには，セキュリティを考慮したネットワーク設計を行うことが不可欠です。様々なネットワーク技術を活用して，人と人とを安全につなぐネットワークを構築するスキルを身につけていきましょう。

勉強のコツ

ネットワークスペシャリスト試験の場合，ネットワーク技術を学習することはもちろん大切なのですが，それだけでは試験に合格できません。特に午後試験では，実際の会社での事例が出てきて，その会社に最適なネットワークを構築するといった設問があります。そのとき，「誰と誰がどのようなデータをやり取りしたいのか」に焦点を当てることがとても大切です。自由につながることと安全につながることはどちらも大切ですが，その重要度は，会社や扱うデータによって変わってくるからです。

ネットワークスペシャリストの午後試験では，いろいろな会社の多様な人物が登場してきます。その人物像をイメージしながらネットワークを想像していくと，より楽しく問題を解くことができます。

関連

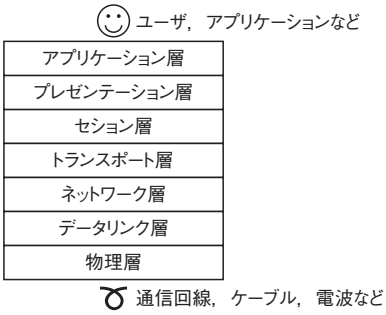
OSI基本参照モデルがそのまま，実際のネットワークシステムに実装されているわけではありませんが，ネットワークを設計するときの基礎になる考え方ですし，頭に入っていると様々な場面で役立ちます。ネットワークエンジニアの議論はOSI基本参照モデルを基に行われることも多いので，ネットワークエンジニアを目指すなら最初に身につけておくべき知識といえます。

1-1-2 OSI基本参照モデル

ネットワークでの通信に必要なプロトコルを七つの階層に分けてまとめたモデルが，OSI基本参照モデルです。OSI基本参照モデルでは，七つの階層でそれぞれ何を行うのかという役割について定義しています。実際の通信で使われるプロトコルは，この七つの階層のいずれかの役割をもっています。OSI基本参照モデルに当てはめて考えることで，プロトコルの詳細を知る前におおまかな役割について理解することができます。

OSI基本参照モデルの７階層

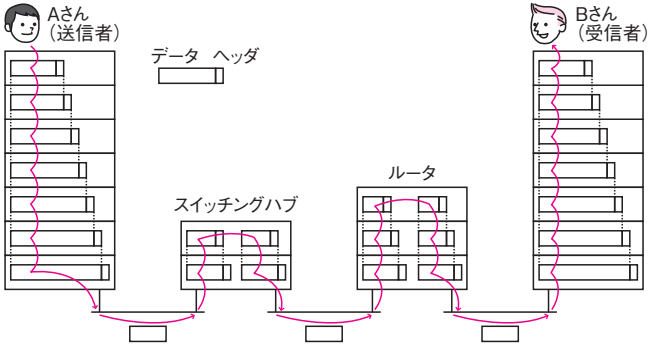
OSI基本参照モデルの階層は次のようになります。



OSI基本参照モデルの７階層

階層の一番上のアプリケーション層の上にあるのが，ユーザや，通信に関係ないアプリケーションなど，実際にデータを利用する人やシステムです。そして，一番下の物理層の下にあるのが，通信回線やケーブル，電波など，実際に電気信号を伝える物理的な媒体です。

実際の通信では，次図のような流れで，Aさん（送信者）からBさん（受信者）にデータを届けます。



OSI基本参照モデルでのデータの流れ

通信経路の途中には，スイッチングハブやルータなど通信を中継する機器があります。それらの機器は7階層すべての役割をもつわけではなく，その機器に必要な階層（ルータならネットワーク層まで，スイッチングハブならデータリンク層まで）の機能をもち，パケットを中継します。

各層の機能や役割

OSI基本参照モデルの7階層それぞれの機能や役割は，以下のとおりです。

アプリケーション層（第7層）

通信に使う**アプリケーション**（サービス）です。電子メールを送ったりホームページを表示させたりするなど，実際の通信の目的を実現させるための機能をもちます。

プレゼンテーション層（第6層）

データの**表現**方法を，通信に適した形式にします。例えば，画像ファイルをテキスト形式に変換したり，データを圧縮したりします。

セション層（第5層）

通信するプログラム間で**会話**を行います。データの流れる経路である**コネクション**の開始や終了を管理したり，同期をとったりします。

関連

通信機器は，上の階層（アプリケーション層など）の機能をもたないものが多いですが，下の階層の機能は必ず備えています。
例えば，ルータはネットワーク層の機能を実現する通信機器ですが，データリンク層で伝送する機能，物理層で電気信号を変換する機能を合わせて必要とします。
「下だけがつながることはあっても，上だけがつながることはない」のが，OSI基本参照モデルの基本的な考え方です。

用語

コネクションとは，通信を行う相手との間で確保する仮想的な通信路のことです。
OSI基本参照モデルでは，コネクションの確立や解放をいつ行うのかという管理はセション層で行い，実際のコネクション確立はトランスポート層で行います。

トランスポート層（第４層）

コンピュータ内でどのアプリケーション（サービス）と通信するのかを管理します。また，通信網の品質の差を補完し，通信の**信頼**性を確保します。

ネットワーク層（第３層）

ネットワーク上でデータが**始点から終点まで**届くように管理します。ルータなどでネットワーク間を結び，ルーティングを行ってデータを中継します。

データリンク層（第２層）

ネットワーク上でデータが**直接接続された通信機器まで**配送されるように管理します。通信機器間で信号の受渡しを行います。データリンク層で作成されるパケットを**フレーム**と呼び，このフレームが実際に通信路を流れるデータとなります。

物理層（第１層）

物理的な接続を管理します。ディジタルデータを電気信号に変換したり，光に変換したりします。

それでは，次の問題で確認してみましょう。

問 題

OSI基本参照モデルのトランスポート層の機能として，適切なものはどれか。

ア　経路選択機能や中継機能をもち，透過的なデータ転送を行う。
イ　情報をフレーム化し，伝送誤りを検出するためのビット列を付加する。
ウ　伝送をつかさどる各種通信網の品質の差を補完し，透過的なデータ転送を行う。
エ　ルータにおいてパケット中継処理を行う。

（平成17年秋 テクニカルエンジニア（ネットワーク）試験 午前 問31）

解 説

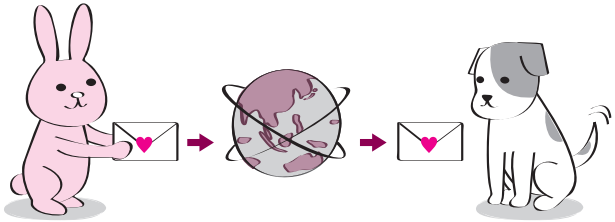
OSI基本参照モデルのトランスポート層では，通信の信頼性を確保します。そのため，伝送をつかさどる各種通信網の品質の差を補完し，透過的なデータ転送を行います。したがって，ウが正解です。アとエはネットワーク層，イはデータリンク層の機能です。

≪解答≫ウ

通信の例

それでは，実際の通信を例に，OSI基本参照モデルに対応してどのような処理が行われるのか見ていきましょう。

例えば，次の図のように，うさぎさんが犬くんにインターネットを通じてメールを送る場合を考えてみます。



うさぎさんから犬くんにインターネットメールを送る

アプリケーション層

うさぎさんはパソコン上でメールソフトを立ち上げて，犬くんに向けて「だいすき」とメールを打ちます。そして，「送信」ボタンを押してメールを送信したときにデータを送るのが，アプリケーション層の役割です。具体的には，電子メールを作成するメールソフト（アプリケーション）がその役割を果たします。

アプリケーション層（メールの送信）

アプリケーション層では，送信元がうさぎさんのメールアドレスで，あて先が犬くんのメールアドレスであることを示すヘッダなどがつけられます。

プレゼンテーション層

メールのデータは，そのままでは相手が読めるとは限りません。そのため，うさぎさんが書いた「だいすき」という文字を，誰もが読める「ネットワーク全体で統一された形式」に変換する必要があります。その役割を果たすのがプレゼンテーション層です。具体的には，メールを送るときの共通の形式である**MIME**形式などに変換します。

用語

MIME（Multipurpose Internet Mail Extension：多目的インターネットメール拡張）とは，様々な形式のデータを電子メールで送信するための規格です。日本語のテキストや画像，添付ファイルなど，様々な形式のデータをすべてテキストに変換します。MIME形式にすることで，ネットワーク全体で誰もが読めるようになります。

セション層

実際にメールのデータを送信するときに，通信路を確保して，データを送信する準備を行うのがセション層です。コネクションを管理し，両方のホストの間でどのようにデータを送れば効率良くやり取りできるかといった打合せが行われます。

トランスポート層

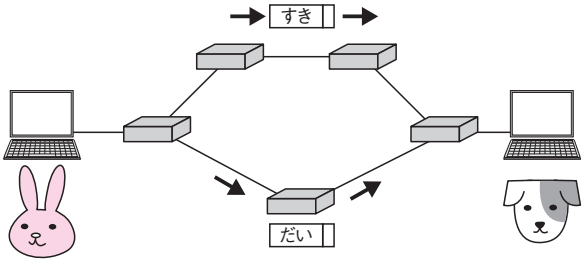
データを確実に相手に届けるために，通信相手との間にコネクションを確立します。具体的には，信頼性を確保するプロトコルである**TCP**（Transmission Control Protocol）を使って，コネクションの確立や切断を行います。

勉強のコツ

実際のネットワークに関する勉強では，トランスポート層とネットワーク層が中心になります。TCP/IPと呼ばれているとおり，トランスポート層のTCPと，ネットワーク層のIPは，通信の中核となる大切なプロトコルです。このTCPとIPをしっかり深く理解することが，ネットワークスペシャリスト試験合格の大切なポイントです。

ネットワーク層

ネットワーク層では，データを始点（うさぎさん）から終点（犬くん）まで届けます。そのとき，パケットを分割して「だい」と「すき」を別々に送っても，最終的に同じ場所に到達できるよう，ルータがルーティングして相手先に届けます。具体的には，あて先を見て始点から終点までのエンドツーエンドで中継するためのプロトコルとして**IP**（Internet Protocol）を使います。



ネットワーク層（メールの伝送）

データリンク層

データリンク層では，直接つながった機器間でデータ伝送を行います。例えば，うさぎさんのパソコンのLANカードから，家のルータまでのイーサネットケーブルの間での伝送などを管理します。パソコンからルータ，ルータから次のルータ……というかたちで，直接接続されたデータリンク間でのリンクバイリンクの通信を管理します。

物理層

物理層では，0や1で示されているディジタルデータを通信媒体に対応した形式に変換します。例えば，イーサネットのUTPケーブルなら電圧の高低に，光ファイバのケーブルなら光の点滅に変換します。

データを受け取った犬くんは，今度は逆に物理層の電気信号をディジタルデータにして，ヘッダから情報を解析して元のデータを復元し，下の階層から順に変換を行います。そして最後に，メールソフトでうさぎさんからの「だいすき」というメッセージを読むことができるのです。

このように，いろいろな役割をもつ各層が連携して役割を果たすことによって，実際の通信は成り立っています。

覚えよう！

- □　**トランスポート層は，通信の信頼性を確保**
- □　**ネットワーク層は始点と終点のエンドツーエンド，データリンク層は隣接間のリンクバイリンク**

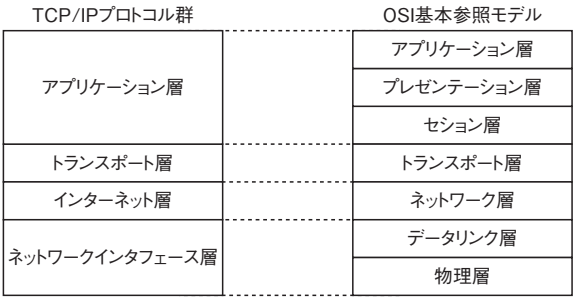
発展

OSI基本参照モデルは，ISOが考えた，理論的なモデルです。通信プロトコルに必要な機能を明確に定めているので，現実のプログラムとは必ずしも対応しません。逆に，TCP/IPプロトコル群は，実際にプログラムを組んで実装させることに重点を置いてきました。そのため，現在動いているインターネット上のサービスは，ほとんどがTCP/IPプロトコル群に準拠しています。

1-1-3 TCP/IPプロトコル群

現在のインターネットで使われている階層モデルとしては，TCP/IPプロトコル群があります。これは，インターネットで主に使用するTCPとIPを中心に，実際のアプリケーションに実装することを考えて作られたモデルです。

TCP/IPプロトコル群とOSI基本参照モデルとの対応関係は，以下のようになります。



TCP/IPプロトコル群とOSI基本参照モデルの対応関係

TCP/IPプロトコル群の方が階層は少ないですが，切り口は同じなので，TCP/IPプロトコル群のプロトコルをOSI基本参照モデルに対応させることができます。

TCP/IPプロトコル群での各層の機能や役割

TCP/IPプロトコル群での各層の機能や役割は，以下のとおりです。

アプリケーション層

OSI基本参照モデルのセション層以上に対応します。アプリケーションプログラムの中で実現されるそれぞれのサービスを実行させる役割です。例えば，Webを閲覧するときには，クライアントにはブラウザ，サーバにはWebサーバソフトが必要です。それらのアプリケーションが提供するサービスを実行するために，クライアントとサーバ間でやり取りをする際に用いられるプ

ロトコルが，HTTP（HyperText Transfer Protocol）です。

トランスポート層

OSI基本参照モデルのトランスポート層に該当します。代表的なプロトコルに，**TCP**（Transmission Control Protocol）と**UDP**（User Datagram Protocol）の二つがあります。

インターネット層

OSI基本参照モデルのネットワーク層に該当します。代表的なプロトコルに，IP（Internet Protocol）があります。

ネットワークインタフェース層

OSI基本参照モデルの物理層とデータリンク層に該当します。厳密には，物理層に該当するものをハードウェアととらえるので，ソフトウェアで実現する部分はほとんどはデータリンク層になります。例えば，LANカードを導入した場合，利用するためのドライバとなるソフトウェアなどがネットワークインタフェース層に該当します。

TCP/IPプロトコル群は現在，世界で最も普及しているモデルです。そのため，本書ではこの4階層に沿って，ネットワークの知識について深く学んでいきます。

TCP/IPプロトコル群の標準化

TCP/IPプロトコル群のプロトコルは，誰でも参加することができる**IETF**（Internet Engineering Task Force）という団体で決定されます。オープンであることが重視されるため，プロトコルはすべて公開されます。具体的には，プロトコルの議論は誰でも参加できるメーリングリストを通じて行われます。そして，仕様は**RFC**（Request For Comments）と呼ばれるドキュメントになり，インターネットで公開されます。

RFCになったドキュメントには番号がつけられます。例えば，TCPはRFC793やRFC3168，HTTP（バージョン1.1）はRFC2616です。

RFCで公開されるプロトコルは，実装することを考えて作成

発展

Webやメールのサービスを実現するソフトウェアには，TCP/IPプロトコル群のアプリケーション層に該当する機能が組み込まれています。つまり，OSI基本参照モデルでいうセション層，プレゼンテーション層，アプリケーション層の三つの役割がすべて盛り込まれているのです。例えば，HTTPのセッションを確立し，プレゼンテーション層に該当するHTMLのデータを交換するなどの機能が，ブラウザという一つのアプリケーションの中に詰め込まれています。

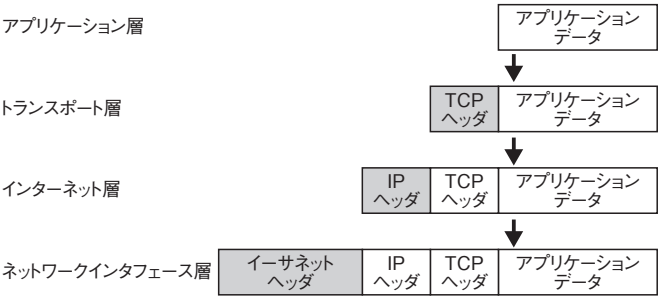
関連

RFCはほとんどが真面目なものですが，まれに冗談で作った「ジョークRFC」と呼ばれるものがあります。インターネットではエイプリルフールの悪ふざけは伝統ということで，4月1日前後に，ジョークと思われるRFCがいくつか発行されるのです。有名なものには，伝書鳩などを使ってインターネット上でデータ伝送をするためのプロトコルを定義したRFC1149などがあります。

されています。IETFでの議論では，実際に使えるプロトコルであることに重点が置かれます。そのため，RFCに沿ったプログラムを作成することで，異なるアプリケーション間での通信が可能になるのです。

TCP/IPプロトコル群でのパケット通信

TCP/IPプロトコル群では，各階層で送信されるデータにヘッダと呼ばれる情報が付加されます。例えば，アプリケーション層で作成されたデータをトランスポート層のTCPに送ると，TCPヘッダが付加されます。さらに，そのデータをインターネット層のIPに送ると，IPヘッダが付加されます。さらに，そのデータをネットワークインタフェース層のイーサネットに送ると，イーサネットヘッダが付加されるのです。



データにヘッダが順に付加される様子

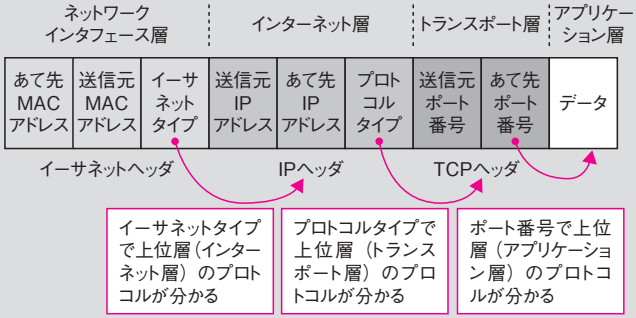
覚えよう！

- □ TCP/IPプロトコル群の仕様はRFCとして公開される
- □ 各階層で，ヘッダがデータに付加される

コラム

ダンプ解析のすすめ

ネットワーク上を流れるパケットは，データにヘッダが付加されていきます。そのため，実際に通信回線上を流れているパケットは以下のような様子になります。



それぞれのヘッダの内容はもう少し複雑ですが，パケットを最初から見ていくと，順番にすべての層のプロトコルが読み解けるようになっています。したがって，実際に流れているパケットをキャプチャ（採取）して解析すると，通信の様子を詳しく知ることができます。

パケットを解析するこの作業をダンプ解析といいます。ダンプ解析では，実際のパケットを基に，通信の流れを一つ一つ解析していきます。解析してみると面白いですし，トラブルシューティングにも役立ちます。ネットワークを肌で感じることができるので，試験対策だけでない実力アップにつながります。

ダンプ解析の詳しい方法はここでは割愛しますが，ダンプ解析を実際に行うという学習方法はおすすめです。

勉強のコツ

ダンプ解析は，実際に流れているディジタルデータのパケットをキャプチャして，それを解析することで行います。そのときに役立つのが，パケットキャプチャ用のソフトウェアです。LANアナライザやネットワークアナライザ，プロトコルアナライザとも呼ばれます。無料のものでは，Wireshark や Microsoft Network Monitorなどいろいろあるので，一度自分で実験してみるのも楽しいと思います。

ネットワークスペシャリスト試験の場合は，単に知っていることだけでなく，実践で体得した知識が大切になります。ダンプ解析は，そういった実践を補うツールとしても使えるのです。

勉強のコツ

通信方式の種類は，実際に具体的なネットワーク技術を学習するときに，「この技術はどこに分類されるのかな？」と意識してみると，理解しやすくなります。例えば，イーサネットはLANですが，広域イーサネットはWANに分類されます。TCPはコネクション型ですが，UDPはコネクションレス型です。対比して学習することで，より深く印象づけることが可能です。

用語

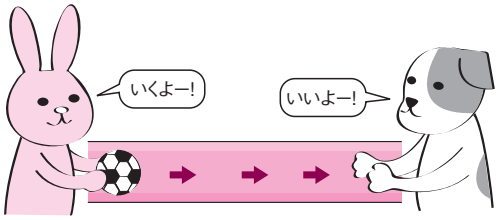
ネットワーク技術でのコネクションとは，コンピュータ間で通信を行うときに作られる論理的な通信路のことです。人間関係のコネクション（コネ）と同じように，2人の間でいろいろな言葉を交わし友好的な関係を作ってから，用件を実施します。

1-1-4 通信方式の種類

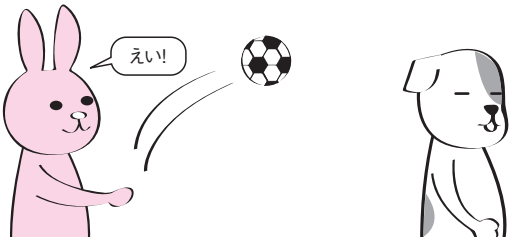
ネットワークを介した通信にはいろいろな方式があります。通信する方法やネットワークの種類，信頼を確保する方法など，様々な角度から分類できます。ここでは，その例をいくつか示します。

コネクション型とコネクションレス型

ネットワーク上でデータを配送する前に，送信者と受信者の間で専用の**コネクション**を張ってから通信する方式を**コネクション型**といいます。コネクション型の場合には，通信の前後にコネクションの確立とコネクションの解放を行う必要があります。コネクション確立などを行わず，いつでもデータを送信する方式を**コネクションレス型**といいます。



コネクション型



コネクションレス型

コネクション型は，手間がかかる分遅くなりますが，確実にデータを送る方式です。また，通信路が確保されるので，パケットの形にしなくても，単純にデータを順番に送信するだけの通信も可能です。

コネクションレス型は，通信は速く行えますが信頼性を確保できません。そのため，信頼性よりもスピードが要求される通信などに用いられます。また，コネクション型と組み合わせて通信を行うこともあります。例えば，有名なプロトコルでは，IPはコネクションレス型ですが，コネクション型のプロトコルであるTCPと組み合わせることによって，信頼性を確保しています。

回線交換とパケット交換

通信回線には，回線を完全に1対1でつなぐ回線交換と，複数のユーザで回線を共有するパケット交換の2種類があります。従来の電話などで利用されていたのが回線交換で，ユーザを1対1で接続するため，確実に一定の速度でデータを送る必要があります。パケット交換は，回線を複数のユーザで共有するため，通信速度はほかの人の通信に影響されます。また，相手を区別するためにあて先が必要なので，パケットにヘッダを付けて管理します。なお，複数のユーザが一斉に送信を行ったため回線にパケットがあふれて処理できない状態を**輻輳**（ふくそう）といい，この場合，パケットが喪失して相手に届かないことがあります。

LANとWAN

LAN（Local Area Network）は，一つの施設内など，ユーザが自分で管理できる範囲のネットワークです。それに対して**WAN**（Wide Area Network）は，都市間や国際間など，広い範囲に及ぶネットワークです。といっても，LANとWANの違いは，広さではなく，**電気通信事業者**が管理する必要があるかないかで，WANは電気通信事業者が管理しています。

LANとWAN

上の図のように，複数の拠点にあるLANを，WANを用いて接続するという形態が一般的です。

勉強のコツ

ネットワークスペシャリスト試験では，基本的に電気通信事業者そのものよりは，そのサービスを利用する立場の会社を題材とすることが多いので，詳しく出題される技術はLANが中心になります。WANについては，利用する立場から見た特徴や，通信量や通信速度などの計算に関する出題がほとんどです。

用語

電気通信事業者とは，電気通信サービスを提供する会社です。通信キャリアや通信事業者とも呼ばれます。電気通信事業法に基づき電気通信事業を営むので，事業に際しては電気通信事業者の登録を行うことが義務づけられています。

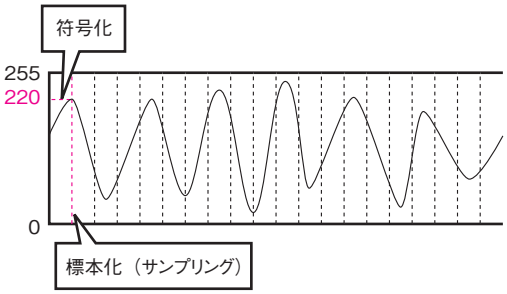
アナログとディジタル

もともとWANは，音声などのアナログ情報を扱う電話が中心であったため，アナログ回線が用いられていました。アナログ回線で通信データなどのディジタルデータを伝送するためには，アナログをディジタルに変換する**A/D変換**（Analog/Digital変換）を行う必要があります。

ディジタル回線が登場してからは，通信データはディジタルのままで送信できるようになりました。しかし逆に，音声などのアナログデータをディジタル回線で送る必要が出てきました。このときには，ディジタルをアナログに変換する**D/A変換**（Digital/Analog変換）を行います。

A/D変換，D/A変換を行うためには，**標本化**と**符号化**という二つの作業が必要です。標本化とは，連続したデータを一定の間隔を置いてサンプリングすることで，符号化は，サンプリングしたデータをディジタルに置き換えることです。

例えば，下図のような音の波があったときに，一定間隔でデータを取得することを標本化（サンプリング），それをディジタルのデータに置き換えることを符号化といいます。



標本化と符号化

標本化を行うときに必要なサンプリング周波数（1秒間に必要なサンプリング数）は，標本化定理によって求められます。**標本化定理**とは，ある周波数のアナログ信号をディジタルデータに変換するとき，それをアナログ信号に復元するためには，その周波数の**2倍のサンプリング周波数**が必要だという定理です。例えば，4kHzまでの音声データを復元させるためには，その倍の8kHz

発展

音を標本化し，符号化したデータを格納する方式の代表的なものにPCM（Pulse Code Modulation）があります。ディジタル回線であるISDNでは，符号化8ビット（256段階），サンプリング周波数8kHzのPCMが用いられています。

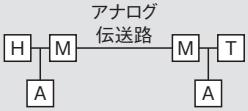
のサンプリング周波数が必要になります。

それでは，次の問題を解いてみましょう。

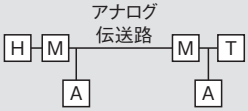
問題

ホストコンピュータ(H)と端末(T)を，モデム(M)を使用しアナログ伝送路を介して接続する。このとき，伝送中のデータを確認するためのプロトコルアナライザ(A)の適切な接続形態はどれか。

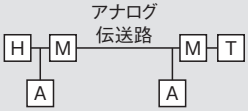
ア



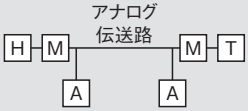
イ



ウ



エ



(平成17年秋 テクニカルエンジニア(ネットワーク)試験 午前 問45)

解説

ホストコンピュータ(H)からモデム(M)まではディジタルデータで，D/A変換してアナログデータになり，アナログ伝送路を流れます。端末(T)側では，ディジタルデータを受け取るため，T側のMでA/D変換して戻します。

プロトコルアナライザ(A)は，ディジタルデータをキャプチャして取得できるアナライザです。そのため，アナログ伝送路ではなく，D/A変換前，D/A変換後のディジタルデータを取得できる場所にAを接続する必要があります。したがって，アが正解です。

≪解答≫ア

用語

モデムはMOdulator DEModulatorの略で，A/D変換とD/A変換の両方を行う装置です。電話回線を使って通信を行う場合などに使用されます。

テキストデータとバイナリデータ

通信で伝送されるデータのうち，文字コードなど文字で表すことができるデータのみのものを**テキストデータ**といいます。そして，画像や音声などテキストデータ以外のものを**バイナリデータ**と呼んで区別します。

昔のパソコン通信などによるデータ伝送では，通信回線や手順などの都合でテキストデータしか送信できませんでした。そこで，バイナリデータを送るために，特別なプロトコルが必要になりました。

現在の通信手順ではほとんどの場合，バイナリデータを送ることができますが，安全のためテキストデータに変換して送るプロトコルも多くあります。電子メールを送るときにすべてのデータをテキストデータに変換するMIME（Multipurpose Internet Mail Extension）はその代表例です。

それでは，次の問題で確認してみましょう。

発展

昔の通信理論を勉強していると出てくるベーシック手順は，テキストデータしか送れない通信手順の1例です。その後，HDLC（High level Data Link Control）手順が登場し，バイナリデータを送ることが可能になりました。
現在よく使われる，イーサネットやPPPのパケットは，HDLC手順の考え方が基になっているので，バイナリデータ伝送が可能です。

勉強のコツ

ベーシック手順やHDLC手順については午前で出題されることがあるので，知っているに越したことはありませんが，午後ではまず出てきませんし，あまり重要事項ではありません。用語と概要を軽く押さえておけば十分です。

問 題

テキストデータ伝送とバイナリデータ伝送に関する記述のうち，適切なものはどれか。ここで，テキストデータは図形文字だけで構成されるものとする。

ア　対象データをテキストデータの文字列に変換することによって，テキストデータ伝送用の手順を使用してバイナリデータを送ることができる。

イ　テキストデータ伝送では7ビットの文字データに1ビットのパリティを付加して伝送し，バイナリデータ伝送では8ビットのデータに分割してそのまま伝送する。

ウ　テキストデータ伝送では無手順を使用し，バイナリデータ伝送ではベーシック制御手順を使用する。

エ　バイナリデータ伝送では，HDLC手順以外の伝送制御手順を使用することはできない。

（平成17年秋 テクニカルエンジニア（ネットワーク）試験 午前 問35）

解 説

バイナリデータでもテキストデータの文字列に変換することによって，テキストデータ伝送用の手順を使用して送ることができます。したがって，アが正解です。

イの7ビットの文字データに1ビットのパリティというのはベーシック手順の説明ですが，ベーシック手順ではバイナリデータを送ることはできません。そのため，ウも不正解です。また，バイナリデータ伝送はHDLC手順で行うことができますが，それ以外のPPPなどの伝送手順でも可能なので，エも不正解です。

≪解答≫ア

覚えよう！

- □ **LANは自分で，WANは電気通信事業者が設営・管理する**
- □ **アナログデータや伝送路を使うにはディジタルの変換が必要**

1-1-5 ネットワークの構成要素

ネットワークを実際に構築するときには，様々な機器やケーブルなどのハードウェアが必要です。

通信媒体と機器

ネットワークを接続するときには，ケーブルなどの通信媒体が必要です。ケーブルの種類としては，**ツイストペアケーブル**（より対線）や**光ファイバケーブル**などがあります。

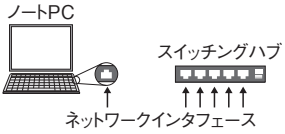
コンピュータとコンピュータをケーブルで直接接続すると，1対1で，しかもケーブルの届く範囲でしか通信ができません。そのため，ルータやスイッチングハブなどの**LAN間接続装置**を用いて，1度に複数台のコンピュータを接続したり，通信を増幅させて通信できる距離を増やしたりします。

関連

ツイストペアケーブルや光ファイバケーブルの種類など，LANケーブルの詳細については，「2-1-5　物理層」で詳しく学習します。

ネットワークインタフェース

コンピュータやLAN間接続装置をネットワークに接続するには，ネットワークに接続するための**ネットワークインタフェース**が装備されている必要があります。



ネットワークインタフェース

発展

ネットワーク機器の場合，新しい技術が登場した直後には，異なるメーカ同士の機器が接続できないといった相互接続性の問題が出ることがよくあります。ネットワークを導入するときには，機能だけでなく長時間運用された実績や相互接続性を確認することも大切です。

それぞれの通信プロトコルや方式に対応したネットワークインタフェースが用意されています。また，規格が同じなら他メーカの製品とも接続が可能なように，**相互接続性**も確保されている必要があります。

LAN間接続装置の種類

OSI基本参照モデルでは階層ごとに役割が違うので，ネットワークを接続するときに必要となる機器が異なります。それぞれの階層で必要な装置は以下のとおりです。

①リピータ（第1層　物理層）

電気信号を増幅して整形する装置です。リピータの機能では複数の回線に中継するハブ（**リピータハブ**）が一般的です。すべてのパケットを全端末に中継するので，接続数が多くなってくるとパケットの衝突が発生し，ネットワークが遅くなります。また，増幅や整形を繰り返すことでエラーが発生し，正常に通信されないこともあるので，ハブの段数（端末間に設置するハブの数）に制限があります。

リピータ

関連

リピータハブの段数制限は，10BASE-T では 4 段，100BASE-TX では 2 段です。なお，スイッチングハブやルータではこの段数制限はありません。

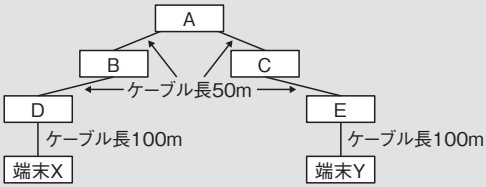
それでは，次の問題で確認してみましょう。

関連

10BASE-Tのツイストペアケーブルでは，ケーブル長の制限は100mです。ここまでは問題ありませんが，100mを超えると，減衰が大きく，通信できないこともあります。

問題

リピータハブ（A，B，C，D，E）とツイストペアケーブルで構成される図の10BASE-Tのネットワーク構成で，端末X，Yが正常に通信できなかった。その理由として適切なものはどれか。



ア　総ケーブル長が185mを超えている。
イ　端末とハブ間のケーブルが長すぎる。
ウ　ハブの段数が多すぎる。
エ　ルータがなく，ルーティングができない。

（平成20年秋 テクニカルエンジニア（ネットワーク）試験 午前 問45）

解説

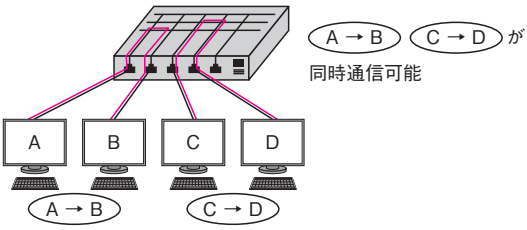
端末Xと端末Yは，端末X→D→B→A→C→E→端末Yというかたちでつながっているので，ハブの段数は，D，B，A，C，Eで5段です。これは，10BASE-Tのハブの段数制限である4段を超えているので，正常に通信できない可能性があります。したがって，ウが正解です。

≪解答≫ウ

②ブリッジ（第2層　データリンク層以下）

データリンク層の情報（**MACアドレス**など）に基づき，通信を中継するかどうかを決める装置です。ブリッジの機能で複数の回線に中継する**スイッチングハブ**（**レイヤ2スイッチ**）が一般的です。リピータの増幅，整形機能に加えて，**アドレス学習機能**と**フィルタリング機能**を備えています。送信元のMACアドレスを**アドレステーブル**に学習し，あて先のMACアドレスがアドレステー

ブルにある場合に，フィルタリングして，そのポートのみにデータを送信します。そのため，複数のホストが同時に通信可能です。



スイッチングハブ

③ルータ（第3層　ネットワーク層以下）

ネットワーク層の情報（**IPアドレス**）に基づき，通信の中継先を決めて転送する装置です。ルーティングテーブルを基に中継先を決めていく動作を**ルーティング**といいます。ルータは，異なるネットワーク，異なるデータリンクを相互に接続します。スイッチングハブの機能にルーティングの機能を備えた**レイヤ3スイッチ**もあります。

④ゲートウェイ（第4～7層　アプリケーション層以下）

トランスポート層以上でデータを中継する必要がある場合に用います。例えば，PCの代理でインターネットにパケットを中継する**プロキシサーバ**や，電話の音声をディジタルデータに変換して送出する**VoIPゲートウェイ**などは，ゲートウェイの一種です。また，電子メールなどは，あて先に直接送るのではなく，メールサーバなどのゲートウェイを中継してやり取りを行うのが一般的です。

それでは，次の問題で確認してみましょう。

発展

ブリッジやスイッチングハブは，アドレス学習を行ってアドレステーブルに記憶するため，ハブ内にCPUとメモリを備えて演算を行います。そのため，リピータハブよりも壊れやすいという特徴があり，スイッチングハブは冗長化することが推奨されます。

発展

ブリッジで区切られたネットワークの範囲をコリジョンドメインといいます。リピータで中継するだけだとコリジョン（衝突）が発生する可能性があるからです。ルータで区切られたネットワークの範囲をブロードキャストドメインといいます。ブリッジは，ブロードキャストパケット（すべての端末向けのパケット）を接続されているすべての端末に転送しますが，ルータは転送しないからです。

問題

複数のLANを接続するために用いる装置で，OSI基本参照モデルのデータリンク層のプロトコル情報に基づいてデータを中継する装置はどれか。

ア　ゲートウェイ　　イ　ブリッジ
ウ　リピータ　　エ　ルータ

（平成19年秋 テクニカルエンジニア（ネットワーク）試験 午前 問48）

解説

データリンク層のプロトコル情報に基づいてデータを中継する装置はブリッジです。したがって，イが正解です。アはトランスポート層からアプリケーション層，ウは物理層，エはネットワーク層でLANを接続する装置です。

≪解答≫イ

覚えよう！

- □　**リピータは物理層，ブリッジはデータリンク層，ルータはネットワーク層**
- □　**スイッチングハブにはアドレス学習機能とフィルタリング機能がある**

1-2 午後問題の解き方

過去問題，特に午後問題を解くことは，ネットワークスペシャリスト試験の対策としてとても有効です。ネットワークスペシャリスト試験の午後問題では，単に知識を問うだけでなく，会社（A社，B社など）での事例を基に，原因究明や問題解決を行います。そのため，基本的な知識を身につけた後は，実際の問題を解いて考えてみることが，試験での解答力を上げるために必須となります。また，午後問題で身につけた問題解決のスキルには実務に役立つ要素が多く含まれているので，しっかり理解しておくと仕事でも使えます。

ここでは，午後問題を演習する際に必要となる，午後問題の解き方について説明していきます。解き方を知り演習を繰り返すことで実力を上げていきましょう。

1-2-1 午後Ⅰ問題の解き方

午後Ⅰは，3問中2問選択で，1問が4～5ページある記述式の問題です。それぞれの問題で一つのテーマについて出題され，1問当たり40～45分で解答します。

過去3年で出題された午後Ⅰテーマは，以下のとおりです。

年度	問	テーマ	主に必要な知識（本書の対応する章）
平成22年秋	1	Webプロキシシステムの改善	Web（第5章），TCP（第4章）
	2	ネットワークの評価	WAN（第2章），運用管理（第8章）
	3	ネットワーク構成の見直し	セキュリティ（第6章），設計（第7章）
平成23年秋	1	宿泊施設へのLAN導入	物理層（第2章），設計（第7章）
	2	メールアーカイブシステム導入	メール（第5章），待ち行列（第7章）
	3	ネットワークの再構築	LAN（第2章），運用管理（第8章）
平成24年秋	1	Webサイトの構築	DNS（第5章），負荷分散（第7章）
	2	無線LANシステムの構築	無線LAN（第2章），設計（第7章）
	3	モバイル端末を利用したシステムの構築	無線LAN（第2章），Web（第5章）

この表からも分かるとおり，一つのテーマを解決するには複数の分野の知識を組み合わせる必要があります。そのため，解答の前提として，必要な知識の学習は必須です。実際の問題では現実に合わせた対応が求められるので，どのような場面でどの知識を使うかという実践的なスキルが必要です。

それでは，平成22年秋午後Ⅰ問1を例に，午後Ⅰ問題の解き方を見ていきましょう。

まずは問題文を読んで，必要な知識と概要について確認していきます。

問題　Webプロキシシステムの改善　CHECK ▶ □□□

「Webプロキシシステムについてがテーマ」ということを確認して，問題選択の目安にします。

Webプロキシシステムの改善に関する次の記述を読んで，設問1～3に答えよ。

A社では半年前から，2台のプロキシサーバを用いたWebプロキシシステムを利用している。A社のネットワーク構成を，図1に示す。

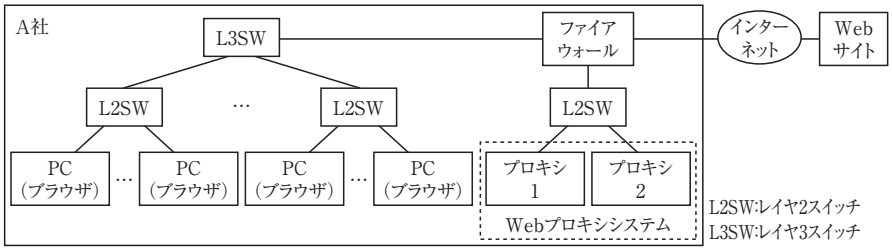


図1　A社のネットワーク構成（抜粋）

プロキシが2台あることと，それぞれの役割を確認します。2台のサーバを両方経由することから「サーバに負荷がかかりそうだな」と推測できれば完璧です。

プロキシ1はキャッシュとURLフィルタリング用のプロキシサーバ，プロキシ2はウイルスチェック用のプロキシサーバである。PC上のブラウザはプロキシ1へアクセスし，プロキシ1はプロキシ2へアクセスする。Webプロキシシステムのアクセス順序を，図2に示す。

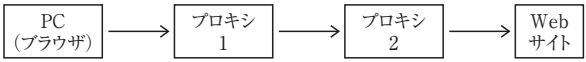


図2　Webプロキシシステムのアクセス順序

プロキシの定義を直接ブラウザに指定するのではなく，定義用のファイルを使う方法です。知らない場合は調べて確認しておきましょう。プロキシについては，「5-1-2　プロキシ」で説明します。

PC上のブラウザには，アクセスするプロキシ1のIPアドレスを定義する必要がある。A社では，定義用のファイル（以下，proxy.pacという）のURLをPCに登録している。proxy.pacはプロキシ1に格納されており，その中にプロキシ1のIPアドレスが登録されている。一方，プロキシ1には，アクセスするプロキシ2のIPアドレスが登録されている。

このWebサイトの応答に関する問題が，今回の問題のメインテーマです。すべてのPCで同時に発生するというあたりから，プロキシサーバの負荷が原因であることが推測されます。

最近，Webサイトの応答が極めて遅くなったり，止まったりするようになった。この問題は，すべてのPCで同時に発生し，数分後には自然に解消した。

この問題について，ネットワークとWebプロキシシステムを担当しているB君が，調査し改善することになった。

ログの解析から，問題が発生しているときには，プロキシ2が受け付けるTCPコネクション数が，設定の上限値まで増加していることが分かった。しかし，プロキシ1が受け付けるTCPコネクション数は上限値の半数以下であった。プロキシ1とプロキシ2の上限値は，ボトルネックとなるプロキシ2のサーバ性能から設計した値で，同一である。これらの事実から，プロキシ2の過負荷が応答性能に影響を与えていることは判明したものの，その原因は分からなかった。

このあたりの記述から，プロキシ2の方がボトルネックになっていて，TCPコネクション数が上限まで達して過負荷になっていることが分かります。問題では，その原因究明を行っていきます。

〔通信プロトコルに関する調査〕

B君は，Webサイトの応答性能に関係する通信プロトコルを調査した。

HTTPクライアントとHTTPサーバ間の通信では，大量のデータを一方向に転送するバルクデータ転送と，比較的少量のデータを交互に転送する対話型データ転送とが混在している。このうち，［ア］の応答性能は，ラウンドトリップ時間の影響を受ける。ラウンドトリップ時間とは，TCPコネクションにおけるパケットの往復時間である。一方，［イ］の応答性能は，ラウンドトリップ時間のほかに，ボトルネックとなる中継路の帯域幅と，確認応答を待たずに送信できるデータ量である［ウ］によっても変化する。ラウンドトリップ時間が同じでも帯域幅を広げれば，応答性能は向上し続けると思われがちであるが，TCPの通信プロトコル上，実効転送速度は，“［ウ］÷ラウンドトリップ時間”に抑えられる。

HTTPでの通信方式であるバルクデータ転送と対話型データ転送の説明です。このあたりは，問題文から知識を読み取れれば大丈夫です。

ラウンドトリップ時間についても，最初から知っている必要はありません。問題文から読み取って解答に用いることが大切です。

HTTP/1.0が公開されたころのHTTPの実装では，1組のリクエストとレスポンスごとに，TCPコネクションの確立と切断が行われていた。図3に，HTTPクライアントがGETリクエストを用いて，HTTPサーバからWebページの情報を取得する際の通信シーケンス例を示す。

図3において，利用者から見たHTTPサーバの応答時間（以下，TATという）は，t1 ～ t9の総和となる。HTTPクライアントの処理に着目すると，TATは次の三つに分割できる。

- TCPコネクションの確立完了までの時間：t1 ＋［エ］
- TCPコネクションの確立完了から，ダウンロードの完了までの時間：［オ］
- ダウンロードの完了から，TCPコネクションの切断と情報の表示がともに完了するまでの時間：［カ］＋t9

HTTPの通信シーケンスについては，頻出なので押さえておく必要があります。本書では，「5-1-1　HTTP」で説明します。

実は，この言葉を見落とさないようにすることが大切です。ここを見ないと，空欄エ～キを間違えてしまいます。

TCPの細かい知識については，ネットワークスペシャリスト試験の頻出事項です。ここがTCPの3ウェイハンドシェイクであることに気づくことは必須です。TCPについては，「4-2-1 TCP」で詳しく取り上げています。

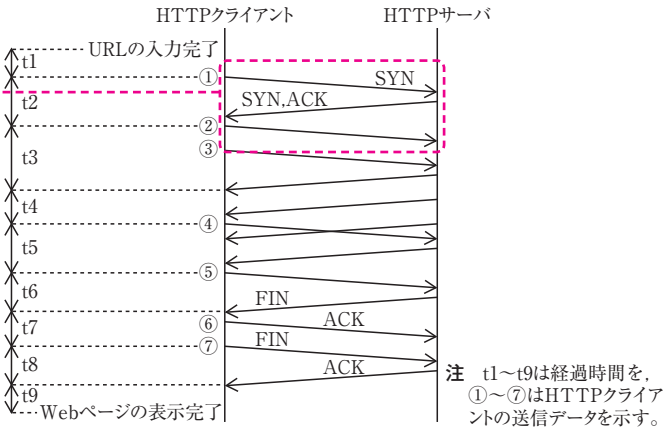


図3　HTTPに関する通信シーケンス例

HTTP/1.1において定義されている“永続的接続(Persistent Connections)”を用いると，複数組のリクエストとレスポンスが同一のTCPコネクションの中で実行できる。これによって，通信オーバヘッドが削減される。

多くのHTTPクライアントはキャッシュをもっており，取得する情報がキャッシュにある場合，その情報の最終更新時刻を付与したGETリクエストを送信する。キャッシュの情報が最新である場合，HTTPサーバは“304 Not Modified”のレスポンスだけを返す。これによってTATが短縮される。図3のHTTPクライアントがキャッシュをもち，問合せの結果，キャッシュにある情報が最新であると確認できた場合，そのTATは，図3で示されているTATに比べて，［　キ　］だけ短縮される。

先読み機能については，この説明で理解できればOKです。このあとの原因究明の要になります。

HTTPクライアントは，“先読み機能”を実装している場合もある。先読み機能とは，参照中のWebページに含まれるリンク情報を用いて，利用者が次に読み込む可能性のある情報を先読みし，キャッシュに蓄積しておく機能である。

このあたりから原因を推測できます。先ほどの「先読み機能」について読んだときにピンと来ていれば完璧です。

〔原因の究明と対策の実施〕

B君は，プロキシ2に関する通信データを調査した。その結果，特定のWebサイト(以下，Cサイトという)にアクセスするとき，プロキシ1からプロキシ2へのTCPコネクション確立要求が大量に発生

することが分かった。プロキシ2とCサイト間のTCPコネクションは一つだけで，HTTP/1.1の永続的接続が使われていた。

B君は，プロキシ1の仕様を再確認した。プロキシ1では先読み機能が実装されていた。また，設定によってこの機能を無効にすることができたが，A社では無効の設定を行っていなかった。B君は，PC上のブラウザやプロキシ2の仕様も再確認した。これらに先読み機能は実装されていなかった。B君は，次のように考えた。

Cサイトは，ほかのWebサイトへのリンク情報が多いので，プロキシ1の先読み機能が大量のTCPコネクションを発生させたと考えられる。プロキシ1の先読み機能を無効にすれば，問題は防止できそうである。無効にする作業は容易である。しかし，先読み効果がなくなるので，通常時の応答性能が悪化する可能性も否定できない。

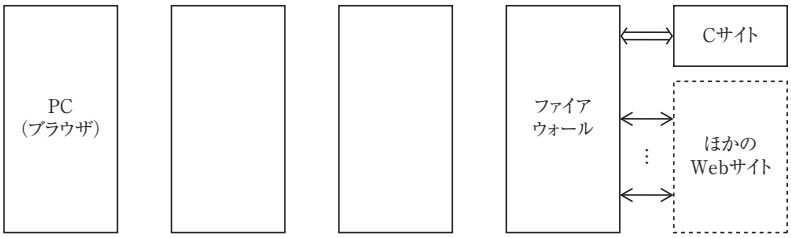
先読み機能を有効にしたまま，プロキシサーバのアクセス順序を変更する対策も有望である。しかし，複数の作業を同時に行わなければならない。例えば，プロキシサーバのIPアドレスを入れ替え，PC側の設定を変えない場合，プロキシサーバのIPアドレスを入れ替える作業のほかに，(Ⅰ)三つの変更作業が必要である。そのため，作業計画を作成し，変更作業を行う必要がある。また，この対策案では，プロキシ2のボトルネックは解消しても，(Ⅱ)別のボトルネックが発生する可能性がある。

最終的に，B君は，“対策として，プロキシサーバのアクセス順序を変更したい”と上司に報告した。その際，B君は，Cサイトへのアクセスによって発生するTCPコネクションについて，対策後の状態を図4に示し，この図を用いて対策の効果を説明した。

原因が判明しました。ここから，対応策を検討していきます。

先読み機能を無効にする，アクセス順序を変更するという二つの対策があることを読み取ります。

プロキシサーバのアクセス順序を変更する対策には，いろいろな影響がありそうです。このあたりを設問で考えていきます。



凡例　⟺ CサイトアクセスによるTCPコネクション
⟷ 先読みによるTCPコネクション

注　設定の関係上,一部を省略している。

図4　Cサイトへのアクセスによって発生するTCPコネクション(対策後)

その後，B君の報告どおりに変更作業が行われ，問題は発生しなくなった。

（平成22年秋 ネットワークスペシャリスト試験 午後Ⅰ 問1）

! 解答のポイント

この問題を簡単にまとめると，プロキシサーバが2台のWebプロキシシステムで応答性能に問題が発生したのでいろいろと検討した。そのとき，〔通信プロトコルに関する調査〕で，HTTPとTCPについて調査し，そして，〔原因の究明と対策の実施〕で，先読み機能が原因と判明し，アクセス順序を入れ替えて解決した，という流れです。

必要な知識は，**HTTP**と**TCP**，そして**Proxy**の各プロトコルについてです。それ以外は，問題文から読み取ることで対応できます。

それでは，設問を一つずつ確認していきましょう。

設問1

〔通信プロトコルに関する調査〕について，(1) ～ (3) に答えよ。

(1)　本文中の［ア］～［ウ］に入れる適切な字句を答えよ。

(2)　GETリクエストを図3中の①～⑦の中から選べ。

(3)　本文中の［エ］～［キ］に入れる適切な時間を，図3中のt1 ～ t9を用いた数式で答えよ。

解説

設問1は，**〔通信プロトコルに関する調査〕**についての問題です。したがって，問題文は，**〔通信プロトコルに関する調査〕**まで読めば解くことができます。問題文を全部一気に読むと大変なので，段落ごとに区切ってチェックしていきましょう。

(1)

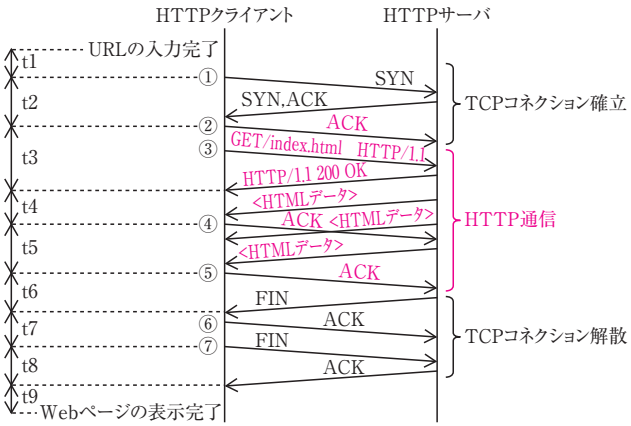
用語の穴埋め問題です。といっても，空欄アとイは，問題文中に書かれている「バルクデータ転送」と「対話型データ転送」について聞かれています。

この設問を解くのに必要な知識は，**TCPでの信頼性を確保したデータ転送の仕組み**です。TCPでは，信頼性を確保するために，シーケンス番号と確認応答で，パケットが相手にちゃんと届いたか確認します。このとき，確認応答を待たずに送信できるデータ量を**ウィンドウサイズ**といいます。大量のデータを送る際には，このウィンドウサイズを超えて一気に送ることはできないので，通信速度に制約がかかるのです。したがって，空欄ウが**ウィンドウサイズ**，その影響を受ける空欄イが**バルクデータ転送**，影響を受けない空欄アが**対話型データ転送**になります。

(2)

GETリクエストはどれかという問題です。この問題を解くためには，**HTTPの通信シーケンス**の流れと，その前後に**TCPのコネクション確立・解放**があるという二つについての知識が必要です。

図3の通信シーケンス例を省略せずに書くと，次のようになります。



したがって，GETリクエストは③になります。すべてを細かく覚えておく必要はありませんが，TCPコネクション確立の3ウェイハンドシェイクがあることと，HTTP通信はGETリクエストで始まることは知っておくと役立ちます。こういった流れを把握する意味でも，ダンプ解析を行って通信パケットを実際に見ることはおすすめです。

(3)

計算式の穴埋め問題です。(2)のTCPコネクションに関する知識があれば解けます。このとき，問題文の「HTTPクライアントの処理に着目すると」という記述を確認し，区切りを間違えないようにすることが大切です。

TCPコネクションの確立完了は，図3の②のパケットに該当します。HTTPクライアントの処理に着目すると，②のACKを送った時点でTCPコネクション確立完了です。したがって，空欄エは**t2**になります。

次に，ダウンロード完了まで，というのは，HTTP通信がひととおり終わるまでの時間です。HTTP通信の最後は⑤のACKを送った時点なので，②のパケット以降，⑤のパケットを送るまでの時間がHTTP通信です。したがって，空欄オは，**t3＋t4＋t5**となります。

TCPのコネクション解放は，FIN，ACK，FIN，ACKの4段階で行います。⑤のACKを送った時点から，TCPコネクションの解放までの時間は，t6＋t7＋t8となります。したがって，空欄カは**t6＋t7＋t8**です。

最後に，キャッシュがある場合のことを考えます。HTTPクライアントにすでにキャッシュがある場合には，③のGETリクエストに対する応答として，「200 OK」の代わりに「304 Not Modified」のレスポンスが返されます。その後のHTMLデータの伝送は必要ありません。図3でいうと，t4とt5の部分が不要になります。したがって，空欄キは**t4＋t5**となります。

≪解答≫

(1)　ア：対話型データ転送　　イ：バルクデータ転送　　ウ：ウィンドウサイズ

(2)　③

(3)　エ：t2　　オ：t3＋t4＋t5　　カ：t6＋t7＋t8　　キ：t4＋t5

それでは，次の設問2を見ていきましょう。

設問2

〔原因の究明と対策の実施〕について，(1)，(2)に答えよ。

(1)　本文中の下線(Ⅰ)について，三つの変更作業をそれぞれ30字以内で具体的に述べよ。

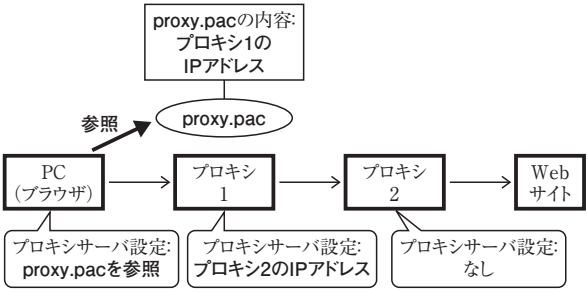
(2)　本文中の下線(Ⅱ)について，別のボトルネックを20字以内で述べよ。

解説

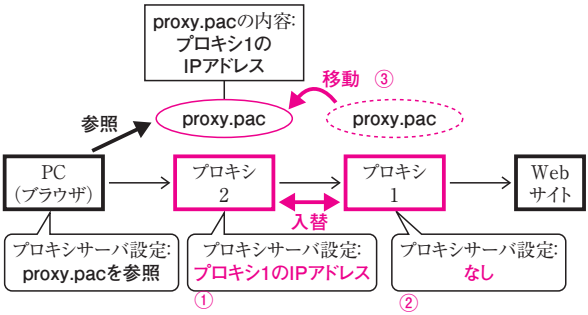
設問2は，〔原因の究明と対策の実施〕についての問題です。プロキシサーバのアクセス順序を変更する対策についての変更作業と別のボトルネックについて問われています。

(1)

図にすると分かりやすくなります。図2を基に，現在のWebプロキシシステムのアクセス順序とその設定をまとめると，次のようになります。



ここで，プロキシサーバのアクセス順序を変更する，つまりプロキシ2とプロキシ1を入れ替えると，プロキシサーバ設定は次のようになります。



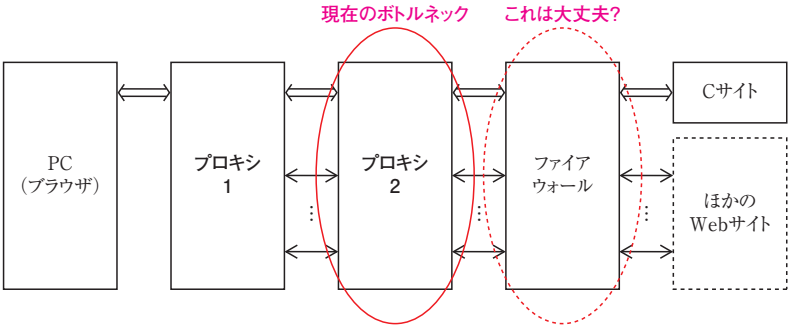
変更箇所は色文字で示しているところで，プロキシサーバのIPアドレスを入れ替える作業のほかに次の三つの変更作業が必要です。

① プロキシ2のプロキシサーバとしてプロキシ1を定義する。
② プロキシ1上のプロキシサーバの定義を削除する。
③ proxy.pacをプロキシ1からプロキシ2に移す。

したがって，この三つが解答となります。

(2)

設問3と合わせて考えると分かりやすくなります。設問で問われてはいませんが，対策前（入替え前）の図4を考えてみると，次のようになります。



Cサイトへのアクセスによって発生するTCPコネクション（対策前）

この状態だと，プロキシ2に，Cサイトアクセスによる TCP コネクションだけでなく，プロキシ1の先読みによる TCP コネクションの負荷も合わせてかかります。そのため，プロキシ2がボトルネックになります。

プロキシ1，プロキシ2を入れ替えると，プロキシ2には先読みによる負荷はかからなくなりますが，ファイアウォールの状況は変わりません。つまり，先読みの TCP コネクションを中継する必要があるファイアウォールの処理能力が足りないと，新たなボトルネックとなる可能性があるのです。したがって，(2) の解答は，**ファイアウォールの処理能力**になります。

≪解答≫

(1) ①・プロキシ2のプロキシサーバとしてプロキシ1を定義する。（27字）

②・プロキシ1上のプロキシサーバの定義を削除する。（23字）

③・proxy.pacをプロキシ1からプロキシ2に移す。（26字）

(2) ファイアウォールの処理能力（13字）

それでは，最後の設問を見てみましょう。

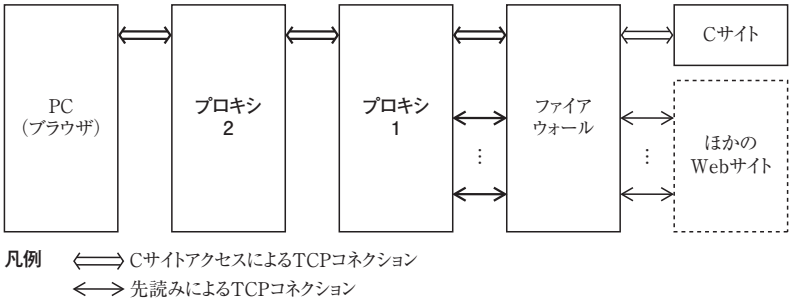
設問3

図4について，対策後の装置名とTCPコネクションを解答欄に記入せよ。

解説

問題文に従って，先ほどのCサイトへのアクセスによって発生するTCPコネクション（対策前）の図からプロキシ1とプロキシ2を入れ替えると，解答のようになります。問題文の指示どおりに考えれば，解答を導くことができるでしょう。

≪解答≫



以上，一つの問題を例に，午後Ⅰ問題を解いてみました。

このように，午後の問題は問題文の中に解答のヒントがたくさん詰まっています。用語や技術についての説明もあるので，しっかり読むことで専門分野の学習にも役立ちます。午後Ⅰの問題は長さも手頃なので，なるべく数多く解いて，合格に必要な実力を身につけていきましょう。

1-2-2 午後Ⅱ問題の解き方

ネットワークスペシャリスト試験の場合，最も難易度が高く，合否を分けるのは午後Ⅱです。一見，問題文が長いだけで知識はあまり要求されないので，読めば解けそうに思えますが，そうではありません。実際には，午後Ⅰより深い知識が要求され，しっかり考える必要があるのです。「午後Ⅱの難しさ」というのが体感できるようになれば，合格は近いと思います。

午後Ⅱ問題は，2問中1問選択で，1問10 ～ 12ページの記述式の問題です。内容的には，「事例解析」と呼ばれる，実際の会社の一連の事例について問われます。それぞれの問題で複数（だいたい4，5個）のテーマについて出題され，1問を120分かけて解答します。

過去3年で出題された午後Ⅱのテーマは，以下のとおりです。

年度	問	テーマ	主に必要な知識（本書の対応する章）
平成22年秋	1	業務システムの再構築	IP（第3章），セキュリティ（第6章），運用管理（第8章），ストレージ（第9章）
	2	ヘルプデスクシステムの構築	LAN（第2章），VPN（第6章），仮想化・ストレージ（第9章）
平成23年秋	1	保守サービスシステムの再構築	VoIP（第5章），VPN（第6章），設計（第7章），仮想化・ストレージ（第9章）
	2	IT環境の改善	STP（第2章），VRRP（第3章），メール（第5章），設計（第7章），仮想化（第9章）
平成24年秋	1	データセンタの分散化	LAN・スイッチ（第2章），設計（第7章），仮想化・SAN（第9章）
	2	ネットワークシステムの再構築	LAN・STP（第2章），IP・IPv6（第3章），設計（第7章），導入（第8章）

午後Ⅰまでの問題では，基本的に一つの知識が一つの問題に対応します。一方，午後Ⅱでは，複数の知識を組み合わせて問題を解く必要が出てきます。例えば，午後Ⅰでは，VRRP（Virtual Router Redundancy Protocol）やSTP（Spanning Tree Protocol）はそれぞれ単独で問題になりますが，午後Ⅱでは，二つを組み合わせたときの問題点や通信経路について問われます。そのため，問題演習を行いながら，一つ一つの知識を分解して確実にマスターしていくことが大切です。

それでは，平成22年秋午後Ⅱ問1を例に，午後Ⅱ問題の解き方を見ていきましょう。

まずは，問題文をざっと読んで概要を確認していきます。午後Ⅱは問題文が長いので，段落の見出し（〔システム基盤の設計〕など，〔 〕で囲まれている文言）だけに目を通して，何が書かれているか確認すると，全体の流れが見えてきます。

問題　業務システムの再構築　CHECK ▶ □□□

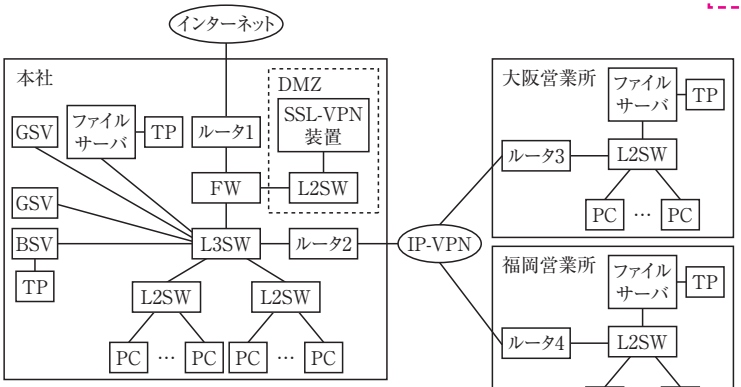
業務システムの再構築に関する次の記述を読んで，設問1～6に答えよ。

大きなテーマです。システム再構築に関する一連の流れについての問題です。

T社は，コンピュータ関連製品の卸売会社である。従業員数は400名で，東京に本社が，大阪，福岡に営業所がある。T社の営業員200名及び技術員100名は，外出先で活動することが多い。営業員は，担当する販売代理店への営業活動を行い，技術員は，自社の取扱商品の技術サポートを行っている。営業員と技術員は，外出先にデータ通信カードを装着したPCを携帯し，インターネット経由でSSL-VPN装置に接続して，T社内のシステムを利用している。

T社では，販売，購買，会計などの業務システムを運用している。現在のネットワークシステム構成を，図1に示す。

T社では，社内システムに外部からアクセス可能で，SSL-VPNをすでに利用していることが分かります。このような技術的な説明は要チェックです。



FW ：ファイアウォール　　L2SW ：レイヤ2スイッチ
GSV ：業務サーバ　　L3SW ：レイヤ3スイッチ
TP ：テープ装置　　BSV ：GSVで稼働する業務システム用のバックアップサーバ

注　IP-VPNの回線速度は,すべて10Mビット／秒である。

図1　現在のネットワークシステム構成（抜粋）

T社では，業務システムの機能強化を目的に，システムの再構築を行うことにした。機能強化策の一つとして，取扱商品を大幅に増やすために，商品マスタを50万レコードに拡大する。併せて，以前から改善が求められていた，ファイルサーバのデータバックアップの見直しも行う。これらを推進するためのプロジェクトマネージャと

この二つが，T社の業務システムの再構築で行うことです。ネットワークだけにとらわれず，「今回，何をしようとしているのか」について，忘れずに押さえておきましょう。設問を考えるときの助けになります。

して，情報システム部のＷ部長が任命された。Ｗ部長は，販売，購買，会計などの業務の責任者及びシステム基盤設計，構築，運用の責任者を選出して，新業務システム開発プロジェクトを発足させた。

新業務システムの概要設計完了後，Ｗ部長は，部下のＹ課長に対してシステム基盤と運用管理方式の設計を指示した。Ｙ課長は，環境の変化に柔軟に対応できるようにすることと，運用負荷を抑えるために，新業務システムを稼働させるシステム基盤に，サーバ仮想化技術を活用することにした。

サーバ仮想化技術を活用することと，その目的が書かれています。技術だけにとらわれるのではなく，その目的も押さえておきましょう。

段落1

〔システム基盤の設計〕

サーバの仮想化を実現させる仕組み（以下，仮想化機構という）を動作させるサーバのことを，物理サーバという。仮想化機構によって，物理サーバ上に作成されるサーバ機能を，仮想サーバという。仮想サーバは，物理サーバ上に複数作成できる。仮想サーバが使用するディスクは，物理サーバのローカルディスクとSANに接続されたディスク装置（以下，SANストレージという）に作成することができる。仮想サーバが使用するディスクをSANストレージに作成すると，複数の仮想サーバで共用できる。

穴埋めで，IP-SANについての知識を問われています。
このような知識は知っているに越したことはありませんが，全体のテーマとはあまり関係がありません。分からなくても必要以上にこだわらず，本文を読み進めていきましょう。

SANには，FC-SANと［a］がある。［a］を構成する代表的な技術がiSCSI（internet SCSI）である。最近は，iSCSIプロトコルがPCとサーバOSに実装されているので，iSCSIを容易に利用できるようになった。iSCSIは，信頼性のあるデータ通信を行うために［b］プロトコルを使用する。iSCSIでは，サーバで稼働し，［c］コマンドを発行して処理を要求するイニシエータと，ストレージ装置で稼働して，その処理を実行する［d］間で，ブロックデータの入出力を実現させている。今回は，稼働実績を重視して，FC-SANを利用することにした。

APサーバは仮想サーバですが，DBサーバでは仮想化機構は利用しません。このあたりの区別をしっかり押さえておかないと，勘違いして解答を書いてしまいがちなので，注意しましょう。

新業務システムは，アプリケーションサーバ（以下，APサーバという），データベースサーバ（以下，DBサーバという）及びSANストレージで構成する。APサーバは，仮想サーバで稼働させる。DBサーバは，APサーバのアプリケーションプログラムから使用される。Ｔ社では，仮想化機構を活用したシステム構築は初めての経験だったので，DBサーバは，2台でアクティブスタンバイ型のクラスタシステムを構成し，仮想化機構を利用しないことにした。クラスタシ

ステムでは，ハートビートパケットで各サーバの生存を確認するが，①各サーバが稼働しているにもかかわらず，ハートビートパケットを受信できなくなると，サービスを正常に提供できなくなる危険性がある。この障害を避けるために，②各サーバの生存確認を確実に行うための対応策を実施する。

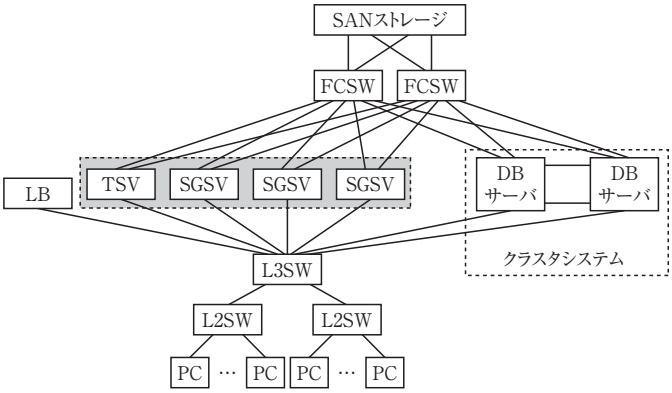
仮想化機構には，物理サーバの障害時や負荷増大時の対策機能が備わっている。しかし，この機能だけでは不十分なので，負荷分散装置（以下，LBという）を利用して，APサーバの冗長性を高めるとともに，［　e　］も向上させることにした。利用するLBには，負荷分散時に送信元IPアドレスをLBのものに付け替えるソースNAT機能があるが，APサーバを使用するPCを特定するために，この機能は利用しない。また，LBによるAPサーバの稼働状態管理を確実に行うために，APサーバからの返送パケットは，LBを経由させることにする。

APサーバを稼働させる物理サーバ（以下，SGSVという）は，障害時の影響を低減させるために，3台構成にする。各SGSVでは，APサーバを2台ずつ，全体で6台を稼働させて，能力面で余裕をもった構成にする。そのほかに，テスト用の物理サーバ（以下，TSVという）も用意する。新業務システムの構成を，図2に示す。

APサーバ，DBサーバ両方の生存確認がテーマです。運用管理などで，ハートビートパケットなどを用いて生存確認を行うというテーマは頻出です。
OSI基本参照モデルの各段階における生存確認の方法を知っておくと，このような問題に役立ちます。

仮想化機構だけでなく，負荷分散装置（LB）も使用します。LBの動作を詳しく見ていく問題は，午後Ⅱでは定番です。

LBの動きについての説明です。このような説明を確実に読み，パケットの動きを想像することが大切です。



注1　網掛け中の物理サーバでは，仮想化機構が稼働する。　　FCSW：ファイバチャネルスイッチ
注2　各SGSVでは，2台のAPサーバが稼働する。
注3　LBは，SGSVで稼働するAPサーバの負荷分散だけを行う。
注4　TSVでは，テスト用のAPサーバとDBサーバが稼働する。

図2　新業務システムの構成

段落2

〔データバックアップの検討〕

今回の再構築では，バックアップを本社に集めるというのが大きなテーマです。そのためには，ネットワークをどうするかが大切なポイントになります。

現在，営業所ごとにファイルサーバのデータをTPにバックアップしており，テープの管理やエラー時の対応などで，営業所員に負担を強いている。この問題を解決するために，TPへのバックアップを止め，すべての営業所のバックアップデータを本社に集めて，新業務システムのデータバックアップと統合するのが効果的と判断した。

遠隔地にバックアップする場合は，バックアップとリストアを高速化するために，通信帯域の確保が必要になる。そこで，通信帯域をあまり必要としないバックアップ方式を調査したところ，重複除外機能をもつバックアップシステムを利用すれば，バックアップデータ量を飛躍的に削減できることが分かった。

重複除外機能は，今回のバックアップシステムに特有の機能です。事前に知っておく必要はないので，問題文から仕組みを読み取ることが大切です。

重複除外機能は，サーバデータをブロックに分割し（以下，ブロックデータという），更新されたブロックデータが既にバックアップサーバに存在した場合，そのブロックデータをバックアップしない働きをもつ。重複除外機能をもつバックアップシステムは，バックアップ対象のデータをもつサーバに導入されるエージェントと，バックアップデータを保存するバックアップサーバから構成される。バックアップ対象のサーバでの重複除外処理の概要を，図3に示す。

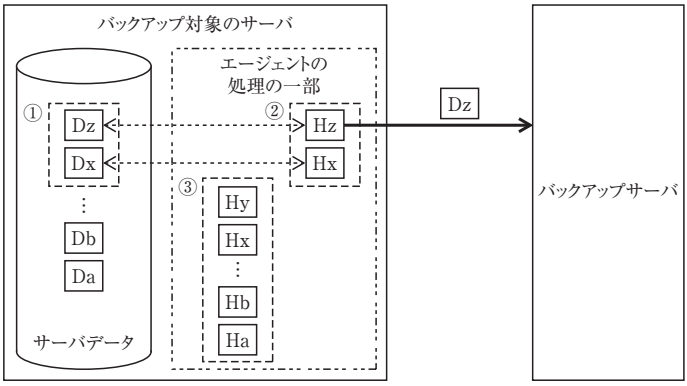


図3　バックアップ対象のサーバでの重複除外処理の概要

エージェントは，ハッシュ値同士の比較によって，更新されたブロックデータがバックアップ済かどうかをチェックする。図3中に示した②のHxとHzのうち，Hxは，③のハッシュ値の中に存在するので，Dxはバックアップされない。Hzは，③のハッシュ値の中に存在しないので，Dzがバックアップサーバに送られて，バックアップされる。このように，更新されたブロックデータから生成されたHxとHzが，③のサーバデータのハッシュ値に存在するかどうかをチェックすることで，DxとDzが，既にバックアップされたブロックデータと重複しているかどうか判断される。

ハッシュ値は，低い確率ではあるが，③ハッシュ値の衝突が発生するので，発生確率を更に低くするために，様々な対応策が考えられている。今回使用する重複除外機能をもつバックアップシステムでは，独自の対応策が実施されている。

ハッシュ値で改ざんを検知する仕組みを応用しています。このあたりを理解するためには，セキュリティ技術，特に改ざん検知について知っておく必要があります。

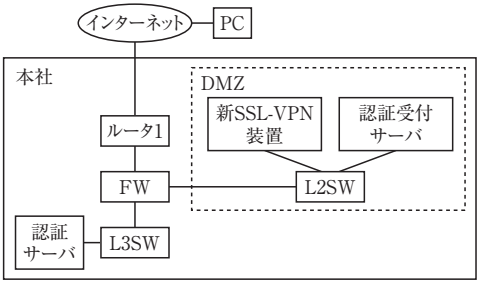
段落3

〔セキュリティ強化策と回線の検討〕

外出先からT社内のシステムを利用するときの認証は，ログインIDと固定パスワードだけで行われているので，セキュリティ上の問題を洗い出し，強化策を検討することにした。

調査した結果，ワンタイムパスワード方式の認証システムを導入し，既設のSSL-VPN装置の代わりに，PCのセキュリティチェック機能をもち，認証システムと連携も可能なSSL-VPN装置（以下，新SSL-VPN装置という）を導入すれば，少ない変更でセキュリティを強化できることが分かった。認証システムは，認証受付サーバと認証サーバで構成される。認証システムと新SSL-VPN装置の構成を，図4に示す。

ここでは，すでにあるSSL-VPN装置を新SSL-VPN装置に変更します。単に，SSL-VPNの利点ではなく，「何が変わったのか」を明確に理解しておく必要があります。



注1　認証受付サーバは,ワンタイムパスワード方式の認証機能と認証データを新SSL-VPN装置に引き渡す連携機能をもつ。
注2　認証サーバは,ランダムな数表の発行や認証処理を行う。RADIUSサーバ機能ももつ。

こういった図の注釈にも，重要な情報が隠されています。注2の，認証サーバはランダムな数表の発行を行う，という記述は，設問4(1)を解くときに必要です。

図４　認証システムと新SSL-VPN装置の構成

新SSL-VPN装置と認証システムの連携処理手順を，次に示す。

(i)　利用者は，PCのブラウザで，新SSL-VPN装置に接続する。

(ii)　新SSL-VPN装置は，セキュリティポリシに従って，PCをチェックする。

このあたりから，新SSL-VPN装置が，単にVPNを構築するだけでなくセキュリティ機能をもつ，という意味を確認します。検疫サーバの役割も請け負うのです。

チェック項目には，セキュリティパッチ，稼働プロセス，ウイルス対策ソフトなどが設定できる。チェック結果が正常のときには，認証受付サーバにリダイレクトされる。チェック結果が異常のときには，PCとの接続が切断される。

(iii)　認証受付サーバによって，ログインID入力画面がPCに表示される。

利用者が，ログインIDを入力すると，認証受付サーバは，ログインIDを基に，ランダムな数表を取得し，次の処理に移る。

(iv)　認証受付サーバによって，認証画面が表示される。

ワンタイムパスワードの一手法です。図4の注2で，数表が認証サーバにあることに気づくと，認証受付サーバと認証サーバで通信が必要なことが分かります。

利用者は，PCに表示されたランダムな数値で構成される数表から，事前に決めた数表の位置に表示されている数値をパスワードとして入力する。入力された数値がチェックされ，正しければ，新SSL-VPN装置にリダイレクトされ，ログインIDとパスワードが，新SSL-VPN装置に送信される。

(v)　新SSL-VPN装置は，受信したログインIDとパスワードを基に，RADIUSプロトコルで，認証サーバに対し認証を要求する。

新SSL-VPN装置は，ログインIDとパスワードを取得し，それで改めて，RADIUSプロトコルを使って認証を行います。

認証後，接続可能なサーバ一覧などをPCに表示する。

(vi)　利用者が，サーバ一覧の中から接続したいサーバを指定する

と，PCと新SSL-VPN装置間でVPNが設定され，本社のサーバに接続できる。

次に，本社と各営業所間の回線が，継続して利用できるかどうかを検討した。

ルータ2のログから送受信データ量を確認したところ，本社と営業所間で発生するトラフィックは，日中最大となり，7Mビット／秒であった。このうち，既存の業務システム利用のトラフィックが40%である。このトラフィックは，新業務システムの利用で，1.3倍になることが見込まれる。これらの条件から，本社と営業所間の最大トラフィックは，［ア］Mビット／秒であり，増加量は少ないことが判明した。

数値が出てきたときには，チェックしておきます。計算問題では，基本的にこの数値を用いることで答えを求めることができます。

各営業所のデータバックアップは，夜間に行う。各営業所のファイルサーバのデータ量は1Tバイトである。2回目以降のバックアップデータ量は，ベンダの情報によれば，重複除外機能によって全体の0.5%以下に削減される。これらの条件から，許容時間内にバックアップを完了できる見込みである。

以上の検討によって，本社と各営業所間の回線が，継続して利用可能と判断した。

段落4

〔システムの運用管理方式の設計〕

新業務システムでは，統合監視システムを利用して，ネットワーク機器とサーバの稼働状態の監視を行う。

(1) ネットワーク機器の監視

統合監視システムには，④監視対象機器を発見して，接続構成図を自動作図する機能があるので，管理者は，接続構成図の中から，監視するネットワーク機器を選択することができる。ネットワーク機器の監視はSNMPで行われ，ネットワーク機器の稼働状態を，MIB情報の定期的な収集によって監視するとともに，Trapの受信によって異常を検知する。

ネットワーク機器の監視システムの機能です。実際の監視ソフトを知っていると，イメージしやすくなります。

(2) サーバの監視

サーバの監視は，あらかじめ設定された間隔で，各サーバから監視対象の情報を収集して行う。収集した情報の中に異常が発見されたときには，その内容がメッセージ表示画面に表示される。

監視項目には，CPU，メモリなどの使用率，サービスとプロセスの稼働状態及びイベントログの内容がある。仮想サーバを活用したシステムでは，仮想サーバの稼働状態監視だけでは十分でないので，⑤通常のサーバ監視よりも複雑な監視が必要になる。イベントログの監視では，フィルタ機能の活用が必要になり，フィルタの条件設定には，⑥運用後のチューニングが必要になる。

通常のサーバの監視に加えて，仮想サーバを用いるときならではの監視も必要です。

図1との違いを確認して，新業務システム構築後の変更点をチェックしておきましょう。

新業務システム構築後のネットワークシステム構成を，図5に示す。

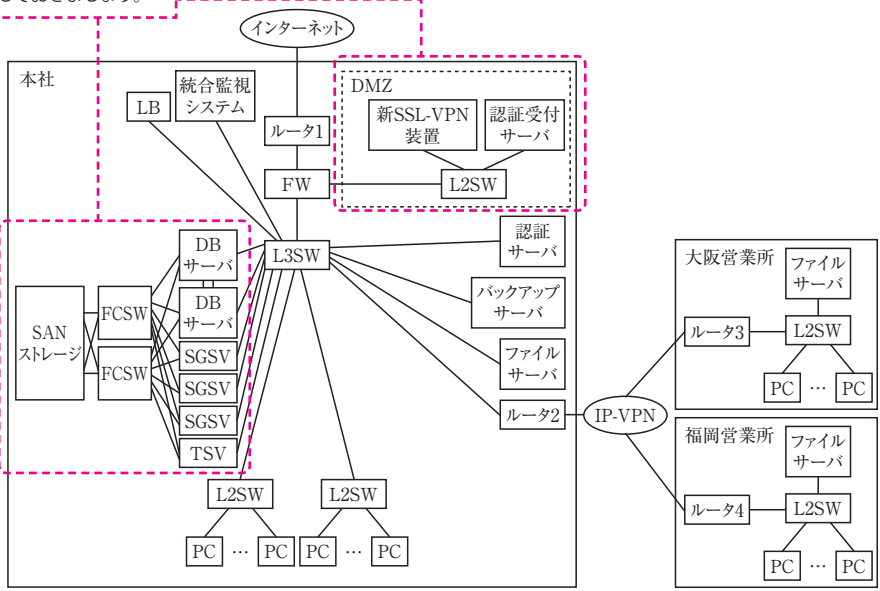


図５　新業務システム構築後のネットワークシステム構成（抜粋）

段落5

〔システムの切替え〕

W部長は，プロジェクトメンバと共同で，システム切替えまでの準備作業のスケジュールと，切替時の作業スケジュール（以下，システム切替スケジュールという）を立案した。そして，W部長は，プロジェクトメンバを各作業の責任者として，システム切替えまでの準備作業を実施させた。

各種テストの終了後，受注から代金回収までの，一連の業務の流

れに沿って処理を進める方式で，総合テストを実施し，問題なく完了した。

負荷テストは，Y課長が担当した。負荷テストでは，新業務システムの処理能力を確認するために，本番と同じ6台のAPサーバを稼働させて実施した。LBには，処理を平均的に分散させるために，ラウンドロビン方式が設定されている。

現在の負荷分散方式は，ラウンドロビン方式です。このあたりを読み取るには，負荷分散に関する知識が必要になります。

負荷テストは，11：00から12：00までの間に，主要業務の販売と購買のシステムを利用する社員に，日常的に行われる業務を処理してもらって行った。負荷テストは順調に進み，ほぼ期待どおりの結果が得られ完了した。負荷テストにおける，ある時間内でのCPU使用率を，表に示す。

表　負荷テストにおける，ある時間内でのCPU使用率

単位　%

測定項目	物理サーバ1		物理サーバ2		物理サーバ3	
	仮想サーバ1	仮想サーバ2	仮想サーバ3	仮想サーバ4	仮想サーバ5	仮想サーバ6
CPU使用率	10～40	20～60	50～100	60～100	20～50	10～50

表と文章から，負荷が均等に振り分けられていない状況を読み取ります。

負荷テストで，6台の仮想サーバに処理が振り分けられたことを確認できた。しかし，CPU使用率の高い状態が続いた仮想サーバが存在していた。振り分けられた処理との関係を調べたところ，メモリに読み込んだ商品マスタの大量のデータに対して，検索を伴う処理を実行した仮想サーバが，高負荷になることが判明した。新業務システムの中には，仮想サーバに大きな負荷を与えるプログラムがあるので，このようなプログラムを実行するサーバに負荷を集中させることなく，負荷を平準化するために，負荷分散方式の見直しを行うことにした。

負荷分散方式の問題は定番です。どのような負荷分散方式があるのかを知っておくと，対処法はすぐに浮かびます。

データ移行テストでは，既存の業務システムから新業務システムへのトランザクションデータの移行が，正しく行えるかどうかを確認する。データ移行は，移行データの作成，移行データの取込み，及び移行データの確認の3段階で行われる。移行データは，既存の業務システムからトランザクションデータを抽出し，各種マスタとテーブルを参照して，加工処理が施されて作成される。移行データの取込みでは，取込みプログラムで，移行データを新業務システムに取り込む。移行データの確認では，新業務システムに取り込まれ

データ移行テストの手順についてチェックします。データ移行テストで何をしようとしているのかを読み取ります。

たデータの正当性を，新業務システムのプログラムでチェックする。データ移行テストを何回か繰り返した結果，問題なくデータ移行を行えることが確認できた。

以上の準備作業を行った後，システム切替え当日，システム切替スケジュールに従って，作業を実施した。システム切替スケジュールを，図6に示す。

作業内容	月末(金曜)	稼働2日前(土曜)	稼働1日前(日曜)
月締め処理	→		
移行データの作成	⟶	⟶	
移行データの取込み	⟶	⟶	→
移行データの確認			⟶
業務開始準備			⟶

図6　システム切替スケジュール

システムの切替えは，月末の金曜日から3日間掛けて実施した。金曜日の業務終了後に，月末の締め処理を行い，その後にデータ移行作業を開始した。移行データの確認後，月曜日の業務開始のための準備作業を行い，システム切替作業を終了した。データ移行作業の途中で問題が幾つか発生したが，必要な対応措置をとり，無事に新業務システムを稼働させることができた。

(平成22年秋 ネットワークスペシャリスト試験 午後Ⅱ 問1)

! 解答のポイント

設問を解く前に問題文を整理しておきます。段落の見出しを中心に，問題全体の流れと対応する設問をまとめると，以下のようになります。

段落（見出し）	対応する設問
〔システム基盤の設計〕	設問1，設問2
〔データバックアップの検討〕	設問3
〔セキュリティ強化策と回線の検討〕	設問4
〔システムの運用管理方式の設計〕	設問5
〔システムの切替え〕	設問6

業務システムの再構築という大きなテーマで，基盤設計からシステム切替えまで，五つのサブテーマについて順に考えていきます。問題文を少しずつ読み進めながら設問を一つずつ解いていくと，無理なく解き終えることができます。

それでは，設問を一つずつ確認していきましょう。

設問1

本文中の［ a ］～［ e ］に入れる適切な字句を答えよ。

解説

空欄穴埋め問題です。**空欄a～dについてはSAN，空欄eについては負荷分散装置の知識問題**です。詳しい技術解説は，SANについては「9-2-1　SAN」で，負荷分散については「7-1-4 負荷分散」に記載しているので，そちらを参照してください。

SANには，経路に専用のファイバチャネルを使うFC-SANと，通常のIPネットワークを使うIP-SANの2種類があります。したがって，空欄aは**IP-SAN**です。IP-SANの代表的なプロトコルiSCSIは，その名のとおり，ハードウェアのインタフェースであるSCSI技術の応用です。信頼性を確保するためにトランスポート層にTCPを利用し，SCSIコマンドを発行して，イニシエータとターゲットの間で，データの入出力を行います。したがって，空欄bは**TCP**，空欄cは**SCSI**，空欄dは**ターゲット**になります。

負荷分散装置のメリットは，「冗長性が高くなることによる可用性の向上」「サーバに分散させることによる負荷軽減（性能低下防止）」「サーバを増やして性能を向上できる拡張性（スケーラビリティ）」の三つです。このうち，冗長性と負荷増大時の対策については，すでに問題文中

に挙げられているので，残りは拡張性になります。したがって，空欄eは**スケーラビリティ**（又は**拡張性**）です。

≪解答≫

a：IP-SAN　　b：TCP
c：SCSI　　d：ターゲット
e：スケーラビリティ　又は　拡張性

設問2

〔システム基盤の設計〕について，(1)，(2)に答えよ。

(1)　本文中の下線①の状況の発生で，サービスが正常に提供できなくなるDBサーバの状態を，40字以内で述べよ。また，下線②の対応策の内容を，25字以内で述べよ。

(2)　図2で，PCからの処理要求がAPサーバとDBサーバで処理されて，処理結果がPCに転送されてくる経路を，次の【転送経路】に示す。(a)，(b)に入れるサーバと機器を，図2中の名称を用いて，【転送経路】の表記方法に従い，すべて記述せよ。

【転送経路】
PC→［　(a)　］→APサーバ→L3SW→DBサーバ→
L3SW→APサーバ→［　(b)　］→PC

解説

設問が二つありますが，いずれも〔システム基盤の設計〕についての問題です。知識というより問題文から推測する問題なので，**問題文の最初の図2までをしっかり読めば答えられます**。

(1)

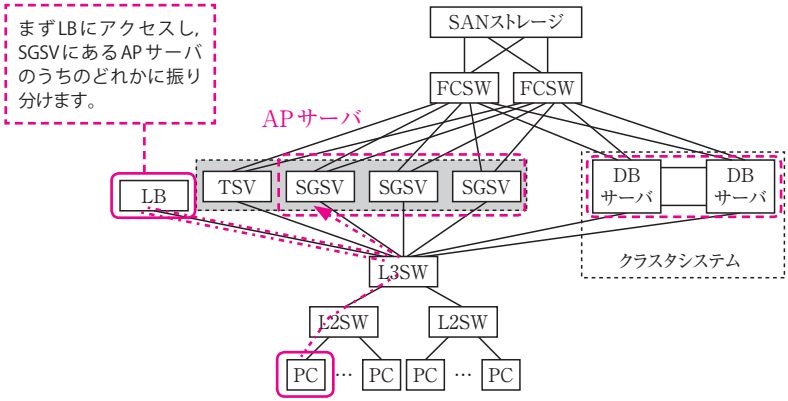
まず，下線①「各サーバが稼働しているにもかかわらず，ハートビートパケットを受信できなくなる」という状況の発生で，サービスが正常に提供できなくなる**DBサーバの状態**について問われています。問題文にもあるとおり，DBサーバは，仮想化機構を活用せず，2台でアクティブスタンバイ型のクラスタシステムを構成しています。つまり，2台のクラスタシステムで1台のノード（ネットワークの構成要素。この問の場合はDBサーバ）がアクティブに稼働し，もう1台のノードは稼働せずスタンバイ状態で待機しています。スタンバイノードは，アクティブノードからのハートビートパケットを受信することで生存確認をしています。スタンバイノードは，ハートビートパケットを受信できなくなると，アクティブノードが故障したと判断して，サービスを起動させてアクティブになります。このとき，アクティブノードは稼働していてパケットが届かなかっただけという場合には，サービスが複数起動してしまうため，サービスを正常

に提供できなくなります。したがって，サービスが正常に提供できなくなるDBサーバの状態は，**一つのサービスが，クラスタシステム内の複数のノードで同時に起動する**状態です。

このとき，下線②「各サーバの生存確認を確実に行うための対応策を実施する」の対応策の内容を考えます。ハートビートで生存確認を行っているので，ハートビートパケットを確実にスタンバイノードに届けるための対策が必要です。最も一般的な対策としては，ハートビートのやり取りを行う回線を冗長化して可用性を高めるというものがあります。したがって，対応策の内容としては，**ハートビートのやり取りの回線を複数にする**となります。

(2)

【転送経路】を求める問題です。図2から，PCからの処理要求がAPサーバとDBサーバで処理されて，処理結果がPCに転送されてくる経路を考えます。問題文中に，APサーバの冗長性を高めるためにLBを利用するという記述があるので，PCからはまず，LBにアクセスしてからAPサーバに接続します。



したがって，PCからAPサーバへの経路は，PC→L2SW→L3SW→LB→L3SW→APサーバになるので，空欄(a)は，**L2SW→L3SW→LB→L3SW**となります。

また，APサーバからの返送パケットについては，問題文中に，「また，LBによるAPサーバの稼働状態管理を確実に行うために，APサーバからの返送パケットは，LBを経由させることにする」とあります。つまり，APサーバからPCに直接返すのではなくLBを経由させるので，行きの経路を逆に辿ります。したがって，APサーバからPCへの経路はAPサーバ→L3SW→LB→L3SW→L2SW→PCとなり，空欄(b)は，**L3SW→LB→L3SW→L2SW**となります。

≪解答≫

(1)　状態：一つのサービスが，クラスタシステム内の複数のノードで同時に起動する。（34字）

対応策：ハートビートのやり取りの回線を複数にする。（21字）

(2)　(a) L2SW→L3SW→LB→L3SW

(b) L3SW→LB→L3SW→L2SW

設問3

〔データバックアップの検討〕について，(1) ～ (3) に答えよ。

(1)　重複除外処理にハッシュ関数を利用する利点を，30字以内で述べよ。

(2)　本文中の下線③の衝突によって引き起こされる問題を，30字以内で述べよ。

(3)　上記 (2) の問題の発生確率を更に低くする方法について，考えられる方法を，50字以内で述べよ。

解説

設問3では，〔データバックアップの検討〕について問われています。重複除外処理機能をもつバックアップシステムでのバックアップの仕組みがテーマです。**セキュリティ技術，特にハッシュ関数についての知識**が必要です。ハッシュ関数についての技術解説は，「6-1-1　暗号化技術」を参照してください。

(1)

重複除外処理にハッシュ関数を利用する利点を問われています。図3の重複除外処理でハッシュ関数を利用すると，ブロックデータDxがハッシュ値Hxに変換されます。ハッシュ関数で算出するハッシュ値は固定長なので，データのサイズはDx＞＞Hxになります。そのため，データが同一かどうかをチェックするときには，Dxを比較するよりHxを比較する方が，サイズが小さく高速になります。したがって，ハッシュ関数を利用する利点は，**データが同一かどうかのチェックが高速化できる**点になります。

(2)

本文中の下線③「ハッシュ値の衝突が発生する」によって引き起こされる問題について問われています。ハッシュ関数では，ある一定の確率で，異なるデータから同じハッシュ値を求めることができます。つまり，実際のデータが変更されていても，同じデータと判断される可能

性が残ります。したがって，引き起こされる問題は，**異なったデータを同じデータと判断してしまう問題**です。

(3)

(2)の問題の発生確率を更に低くする方法について問われています。ハッシュ関数が一つだけだと衝突が発生する可能性は一定なので，これを減らすためには，ほかの方法を組み合わせる必要があります。例えば，従来からパケットなどのエラーチェックに使われているCRC(Cyclic Redundancy Check)を組み合わせて，ハッシュ値とCRCの両方をチェックするという方法があります(CRCについては，「7-2-1　符号化・データ伝送技術」を参照)。したがって，問題の発生確率を更に低くする方法には，**ブロックデータのCRCも合わせて生成し，ハッシュ値とCRCの両方を比較して判断する**方法があります。

また，ハッシュ値の計算単位を二つに分けることなどで複数チェックを行うようにしても，発生確率を低減できます。例えば，**ブロックデータを2分割し，それぞれのハッシュ値を生成して，それらをつなぎ合わせて比較する**といった方法も可能です。

発生確率を更に低くする方法として実効性があれば，**この二つ以外の解答でも正解になります**。午後Ⅱでは特に，答えが一つとは限らない設問が多いので，問題文を基に「妥当な解」を考えていきましょう。

≪解答≫

(1)　データが同一かどうかのチェックが高速化できる。(23字)

(2)　異なったデータを同じデータと判断してしまう問題(23字)

(3)　・ブロックデータのCRCも合わせて生成し，ハッシュ値とCRCの両方を比較して判断する。(42字)

・ブロックデータを2分割し，それぞれのハッシュ値を生成して，それらをつなぎ合わせて比較する。(45字)

設問4

〔セキュリティ強化策と回線の検討〕について，(1)～(4)に答えよ。

(1)　手順(ii)のPCのチェックは，すべてのPCに対して行われる。新SSL-VPN装置がPCに対して行う処理を，25字以内で述べよ。また，認証受付サーバと認証サーバ間の通信が発生する箇所を，連携処理手順(i)～(vi)の中から，すべて選んで答えよ。

(2)　セキュリティ強化策によって，セキュリティ面で改善される点を二つ挙げ，それぞれ25字以内で述べよ。

(3)　認証システムを導入したときに，FWに新たに許可設定すべき通信を二つ挙げ，それぞれ送信元とあて先を明確にして，25字以内で答えよ。

(4)　本文中の［　ア　］に入れる数値を求めよ。答えは，小数点以下を切り上げて整数で求めよ。

解説

設問4では，〔セキュリティ強化策と回線の検討〕について問われています。**(1)は実務的な知識が必要**ですが，**(2)以降は問題文を読むことで解くことが可能**です。

(1)

手順(ii)「新SSL-VPN装置は，セキュリティポリシに従って，PCをチェックする(以下略)」ときに，新SSL-VPN装置がPCに対して行う処理について問われています。手順(ii)に，「チェック項目には，セキュリティパッチ，稼働プロセス，ウイルス対策ソフトなどが設定できる」とありますが，このようなチェックは，PC内でのOSの状態を調べる必要があるので，外部からアクセスしただけでは分かりません。そのため，PCに検疫のためのプログラムをダウンロードし，そのプログラムを実行させて情報を提供してもらうという形態をとります。したがって，新SSL-VPN装置がPCに対して行う処理は，**検疫のためのプログラムをダウンロードする**処理になります。こういった問題を解くためには，ハードウェアやOSの知識，製品の知識など，**ネットワークの勉強以外のスキルが必要**です。

また，(1)の続きで，認証受付サーバと認証サーバ間の通信が発生する箇所を考えます。(i)では，PCのブラウザと新SSL-VPN装置間の通信のみです。(ii)では，セキュリティチェックが正常なら認証受付サーバにリダイレクトされるので，PCと認証受付サーバに通信が発生します。(iii)では，認証受付サーバによって，ログインID入力画面がPCに表示されます。このときに，利用者がログインIDを入力すると，「認証受付サーバは，ログインIDを基に，ランダムな数表を取得し」とあります。図4の注2によると，ランダムな数表の発行を行うのは認証サーバなので，ここで認証受付サーバと認証サーバ間の通信が発生していることが分かります。同様に(iv)でも，認証画面で「入力された数値がチェックされ」とありますが，このチェック，つまり認証処理は，図4の注2より，認証サーバで行われます。したがって，ここでも認証受付サーバと認証サーバ間の通信が発生しています。(v)は，新SSL-VPN装置が直接，認証サーバにアクセスして認証を要求しています。(vi)では，PCのブラウザと新SSL-VPN装置間の通信のみです。したがって，認証受付サーバと認証サーバ間の通信が発生する箇所は，**(iii)，(iv)**になります。

(2)

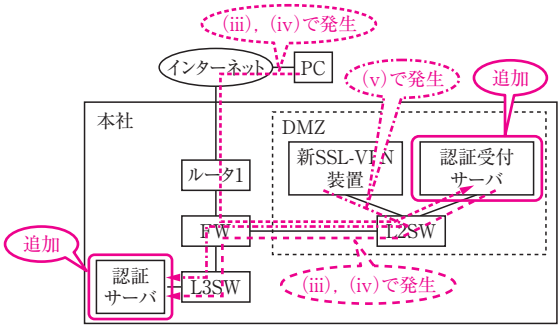
セキュリティ強化策によって，セキュリティ面で改善される点を二つ聞かれています。今回のセキュリティ強化策で変更されたのは，次の2点です。

①認証がログインIDとパスワードから，ワンタイムパスワード方式になった。
②新SSL-VPN装置でセキュリティチェック機能が利用できるようになった。

したがって，改善された点としては，①より**パスワードの安全性が高まる**点が一つあります。また，②より**PCのセキュリティチェックが行われる**点も挙げられます。この二つが解答です。

(3)

認証システムを導入したときに，FWに新たに許可設定すべき通信を二つ挙げます。(1)で連携処理手順(i) ～ (vi)で通信内容を考えてきたので，それを基に，新たに発生する通信について考えます。図1と図4を比べると，図4で新たに加わったのは，認証受付サーバと認証サーバです。



これらの新しいサーバとの通信のうちFWを経由するものを考えると，(iii)，(iv)で発生するPCから認証受付サーバへと，認証受付サーバから認証サーバへの通信があります。また，(v)では，新SSL-VPN装置から認証サーバへの通信があります。したがって，FWに新たに許可設定すべき通信には，以下の三つがあります。

- **インターネットから認証受付サーバへの通信**
- **認証受付サーバから認証サーバへの通信**
- **新SSL-VPN装置から認証サーバへの通信**

このうちの二つが指摘できていれば正解です。

(4)

計算問題です。空欄アに入れる数値（本社と営業所間の最大トラフィック）を求めます。問題文から数値を確認すると，現在のトラフィックは7Mビット／秒で，このうちの40%のトラフィックが新業務システムで1.3倍になります。したがって，

$$7\ [\text{Mビット／秒}] \times (0.4 \times 1.3 + (1 - 0.4)) = 7 \times 1.12 = 7.84 \fallingdotseq 8\ [\text{Mビット／秒}]$$

となります。小数点以下を切り上げるので，空欄アは**8**になります。

≪解答≫

(1)　PCに対して行う処理：検疫のためのプログラムをダウンロードする。（21字）
　　通信が発生する箇所：(iii)，(iv)

(2)　①・パスワードの安全性が高まる。（14字）
　　②・PCのセキュリティチェックが行われる。（19字）

(2)　※次のうちから二つを解答
- インターネットから認証受付サーバへの通信（20字）
- 認証受付サーバから認証サーバへの通信（18字）
- 新SSL-VPN装置から認証サーバへの通信（21字）

(4)　ア：8

設問5

〔システムの運用管理方式の設計〕について，(1) ～ (3) に答えよ。

(1)　本文中の下線④の発見方法を，50字以内で述べよ。

(2)　本文中の下線⑤の監視では，性能管理を効果的に行うために，どのような監視方法が必要か。50字以内で述べよ。

(3)　本文中の下線⑥のチューニング内容を，25字以内で述べよ。

解説

設問5では，〔システムの運用管理方式の設計〕について問われています。ネットワーク機器とサーバの稼働状態の監視を行います。**運用管理についての基本的なスキルと知識が必要**で

す。詳しくは「8-1-1　運用管理」を参照してください。

(1)

下線④「監査対象機器を発見して」の発見法が問われています。一般的なネットワーク監視システムには，ネットワークの範囲を指定すると，そのネットワーク内にある機器を発見する機能があります。手法は原始的で，そのネットワークに存在する可能性のあるIPアドレスに対し，一つ一つpingを発行し，応答があるかどうかでホストの有無を判断します。したがって，発見方法は，**指定された範囲内のIPアドレスあてにpingを発行し，応答の有無でホストの存在を判断する**というものです。

(2)

下線⑤「通常のサーバ監視よりも複雑な監視」で，性能管理を効果的に行うために必要な監視方法について問われています。今回の新業務システムでは，仮想サーバを活用しているので，仮想サーバと物理サーバの両方を監視することが大切です。このとき，単に両方を管理するだけでなく，仮想サーバと物理サーバを対比して管理すると，性能管理をより効果的に行うことができます。したがって，必要な監視方法は，**仮想サーバと，仮想サーバが稼働する物理サーバの稼働状態とを対比して監視できるようにする**というものになります。

(3)

チューニング内容について問われています。下線⑥の周辺に「イベントログの監視では，フィルタ機能の活用が必要になり，フィルタの条件設定には，運用後のチューニングが必要になる。」とあるとおり，聞かれているのは，フィルタの条件設定です。イベントログは，すべてを確認すると量が多すぎて，障害に結びつくログを見落としてしまいます。そのため，フィルタの条件設定をチューニングして，障害に結びつくログだけを検出するようにします。したがって，チューニング内容は，**障害に結びつくログだけを検出するようにする**ことになります。

≪解答≫

(1)　指定された範囲内のIPアドレスあてにping を発行し，応答の有無でホストの存在を判断する。（45字）

(2)　仮想サーバと，仮想サーバが稼働する物理サーバの稼働状態とを対比して監視できるようにする。（44字）

(3)　障害に結びつくログだけを検出するようにする。（22字）

設問6

〔システムの切替え〕について，(1) ～ (3) に答えよ。

(1)　負荷テストで判明した状況を基に，負荷分散効果をより高められる負荷分散方式を，30字以内で答えよ。

(2)　データ移行テストの目的を，25字以内で述べよ。

(3)　システム切替スケジュールの立案において明確にすべき事項を，問題発生時の措置の面から二つ挙げ，それぞれ40字以内で述べよ。

解説

設問6では，〔システムの切替え〕について問われています。最後の総まとめなので，今まで変更してきた内容を踏まえての出題です。**(1) は負荷分散，(2) はデータ移行についての知識が必要**です。負荷分散については「7-1-4　負荷分散」で，システム移行については「8-1-2　システムの導入，現行システムからの移行」で取り上げているので，そちらを参考にしてください。

(1)

負荷分散効果をより高められる負荷分散方式について問われています。現在の負荷分散方式はラウンドロビン方式で，表の負荷テストでのCPU使用率を見ると，仮想サーバ3と4に負荷が偏っているのが分かります。問題文に，「新業務システムの中には，仮想サーバに大きな負荷を与えるプログラムがあるので，このようなプログラムを実行するサーバに負荷を集中させることなく，負荷を平準化するために，負荷分散方式の見直しを行う」とあり，これを満たす負荷分散方式を考えます。今回は，CPU使用率に偏りがあるのが問題なので，CPU使用率を平準化するためには，CPU使用率が最も少ないサーバに振り分けるCPU負荷分散（CPU Load）という方法が適当です。したがって，負荷分散効果をより高められる負荷分散方式は，**CPU使用率の低いAPサーバに処理を振り分ける**方式になります。

(2)

データ移行テストの目的について問われています。問題文中より，「データ移行テストでは，既存の業務システムから新業務システムへのトランザクションデータの移行が，正しく行えるかどうかを確認」します。このとき，「移行データは，既存の業務システムからトランザクションデータを抽出し，各種マスタとテーブルを参照して，加工処理が施されて作成される」ことから，この，**データ抽出，加工ロジックの正当性の確認**を行い，データの移行が正しく行えるかどうかを確認します。また，「移行データの取込みでは，取込みプログラムで，移行データを新業務システムに取り込む」ことから，取り込まれるデータが正確に移行されていることを確認する必要があります。そのため，**新業務システムにおけるマスタデータの完全性の確認**を

行い，データが正しいことを確認します。また，実際のシステム切替は図6のスケジュールに従って行うので，この時間内に移行が終わるかどうかを確認する必要があります。そのため，**データ移行に要する時間の確認**を行い，図6で設定された時間でシステム切替えが実行可能なことを確認します。

(3)

システム切替スケジュールの立案において明確にすべき事項を，問題発生時の措置の面から二つ挙げます。設問に，「問題発生時の措置の面から」とあるので，問題が発生した場合を想定して解答を考えます。システム移行時に事前に考えておくべきことには，次の二つがあります。

①事前に考えられる問題やリスクを可能な限り洗い出しておき，対応策も考えておく。
②システム移行に失敗した場合に，確実に元に戻せるようにする。そのため，失敗の判断基準と，それを決定するタイミングをあらかじめ決めておく。

したがって，明確にすべき事項としては，**①データ移行時に予測できる問題を事前に明確化して，対応策を作っておく**ことと，**②システム切替えを断念するときの判断基準と，それを決定する時間を明確化する**ことになります。

≪解答≫

(1)　CPU使用率の低いAPサーバに処理を振り分ける。（24字）

(2)　・データ抽出，加工ロジックの正当性の確認（19字）
　　・新業務システムにおけるマスタデータの完全性の確認（24字）
　　・データ移行に要する時間の確認（14字）

(3)　①・データ移行時に予測できる問題を事前に明確化して，対応策を作っておく。（34字）

　　②・システム切替えを断念するときの判断基準と，それを決定する時間を明確化する。（37字）

以上，一つの問題を例に，午後Ⅱ問題を解いてみました。

午後Ⅱ問題は午後Ⅰに比べて設問が多くて大変ですが，設問ごとに考えていくと，最後まで解くことができます。また，知識については，午後Ⅰと同様，様々な分野が複合して出題されます。また，事例解析なので，一連の問題を解いていくことによって実際の業務の流れが分かります。

ほかの問題を演習するときにも，単に設問を解いて覚えるのではなく，背景にある知識を調べる，全体の流れで何をしようとしているのか確認する，などによって，学習効果は格段に上がります。過去問演習をなるべく多く行って，確実に実力を身につけていきましょう。