NW

平成23年度　秋期
ネットワークスペシャリスト試験
午後Ⅱ　問題

試験時間	14:30 ～ 16:30（2時間）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. この注意事項は，問題冊子の**裏表紙**に続きます。必ず読んでください。
4. **答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。**
5. 問題は，次の表に従って解答してください。

問題番号	問1，問2
選択方法	1問選択

6. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) B又はHBの黒鉛筆又はシャープペンシルを使用してください。
   (2) **受験番号欄**に，**受験番号**を記入してください。正しく記入されていない場合は，採点されません。
   (3) **生年月日欄**に，受験票に印字されているとおりの**生年月日**を記入してください。正しく記入されていない場合は，採点されないことがあります。
   (4) **選択した問題**については，次の例に従って，**選択欄**の**問題番号**を○印で囲んでください。

   なお，○印がない場合は，採点の対象になりません。2問とも○印で囲んだ場合は，はじめの1問について採点します。

   〔問2を選択した場合の例〕

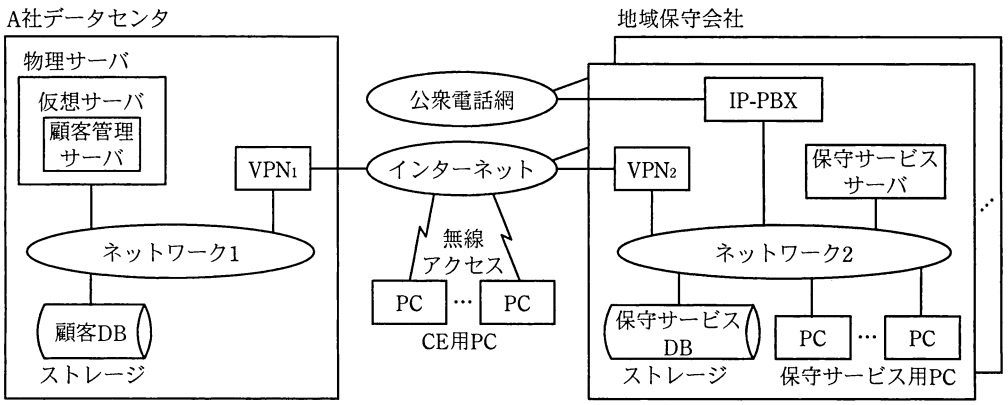
選択欄	
1問選択	問1
	問2

   (5) 解答は，問題番号ごとに指定された枠内に記入してください。
   (6) 解答は，丁寧な字ではっきりと書いてください。読みにくい場合は，減点の対象になります。

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

問1　保守サービスシステムの再構築に関する次の記述を読んで，設問1～5に答えよ。

A社は，OA用品の製造・販売会社である。A社ではこれまで，製品を購入した企業からの機能や修理の問合せへの対応（以下，保守サービスという）を，地域ごとの保守関連会社（以下，地域保守会社という）に委託していた。地域保守会社では，問合せに応じてカスタマエンジニア（以下，CEという）による出張修理の手配も行っている。これらの業務遂行を支援するシステム（以下，保守サービスシステムという）の現状構成を，図1に示す。



VPN1，VPN2：VPN装置　IP-PBX：VoIP対応PBX　DB：データベース

注記　ネットワーク1，2の詳細は省略している。

図1　保守サービスシステムの現状構成（抜粋）

問合せ電話の受付は，担当の地域保守会社で行っている。保守サービス用PCにはソフトウェアで電話機能を実現するソフトフォンがインストールされている。電話は，IP-PBXが受け，保守サービス用PCに転送される。CEの出動指示は，地域保守会社の受付者が，通話完了直後の後処理で行っている。問合せ電話の応対に必要な顧客情報は，顧客DBから，担当の地域保守会社へ夜間にバッチ転送され，地域保守会社にある保守サービスサーバの管理下にある保守サービスDBに取り込まれる。CEは，CE用PCを持ち，無線アクセスによって接続したインターネットを介して，保守サービスサーバにアクセスし，必要な情報をやり取りしている。

A社は，保守サービスの品質と効率の向上を図るために，業務の見直しと，それに伴うシステムの再構築を検討することになった。再構築に当たって，保守サービスシ

ステムを，A 社データセンタ内のシステムに統合することにした。これまで，保守サービス業務を行ってきた地域保守会社は，統合したシステムを共同利用することで，情報資産の一元化を実現できる。

保守サービスシステムの再構築の担当となった N 君は，次に示す具体的な検討項目を設定した。

(1) 作業効率を高めるための CE 用 PC の選定

(2) データ保存機能のない PC であるシンクライアント（以下，TC という）システムの検討

(3) 電話の着信場所の A 社データセンタへの統合化に伴う電話回線の必要数の算定

(4) 地域保守会社及び CE 用 PC から A 社データセンタへの接続ネットワークの検討

(5) 拡張性を考慮した A 社データセンタ内ネットワーク構成の検討

〔作業効率を高めるための CE 用 PC の選定〕

N 君はまず，CE 用 PC について検討した。保守サービスシステムでは，これまで CE 用 PC として，携帯電話用通信カードの入ったノート PC を利用してきた。しかし，最近では情報端末機能を備えた携帯電話やタブレット型の PC（以下，MPC という）などが普及しつつあり，CE 用 PC として使える可能性が出てきた。

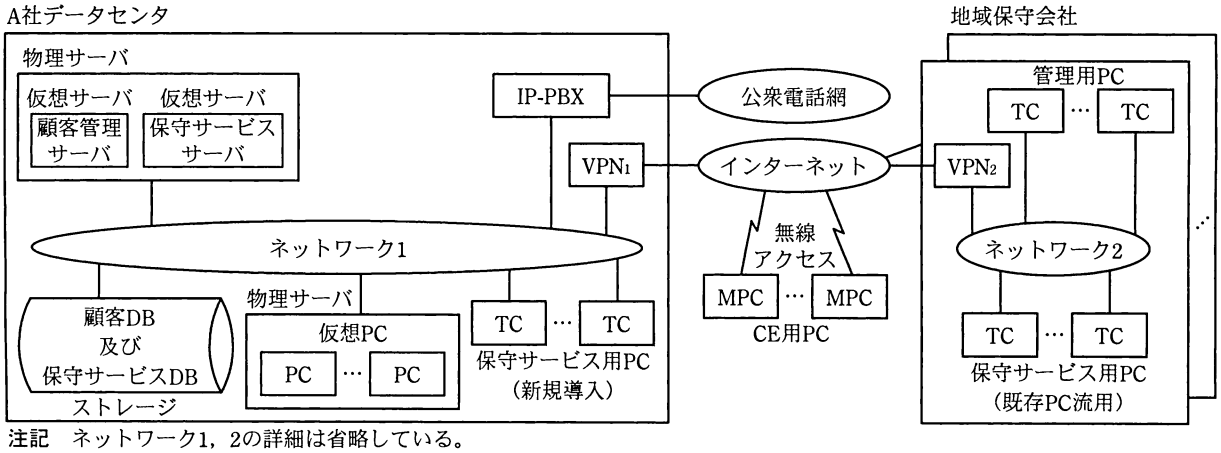
MPC には，駅などの公共施設にあるアクセスポイントを経由して，インターネットに接続できる［　ア　］機能をもった機種が多い。携帯電話網に直接接続する機能をもたない MPC でも，携帯電話端末のテザリング機能を使うと，携帯電話網を経由したインターネット接続が可能になる。

MPC の多くは，外出先での使用が前提とされているので，位置情報を取得する［　イ　］機能，カメラ機能，①インターネットを介してデータセンタにセキュアな VPN 接続を実現するための標準的な機能などが，実装されていることも多い。また，MPC はアプリケーションのダウンロード機能をもっているので，プログラムを追加することで各種の機能を追加できる。

N 君は，これらの利点から MPC を CE 用 PC として活用できると考え，今回の保守サービスシステムの再構築に合わせて導入することを提案し，了承された。

〔TC システムの検討〕

N 君が考えた再構築後の保守サービスシステムの構成概要を図 2 に示す。



注記　ネットワーク1，2の詳細は省略している。

図 2　再構築後の保守サービスシステムの構成概要

今回の保守サービスシステム再構築を機に，地域保守会社に分散していた保守サービスサーバと保守サービス DB を統合する。

A 社データセンタに保守サービス用 PC を新たに設置するが，繁忙期に対応するために，地域保守会社の既存 PC を利用し，地域保守会社でも保守サービス業務を行う。また，地域保守会社には，保守サービス業務以外で利用する管理用 PC を導入し，A 社データセンタ内のサーバにアクセスできるようにする。

ネットワーク経由で画面情報と操作情報の送受信だけを行う TC の実現方式としては，サーバベース方式（以下，SBC という）と仮想 PC 方式がある。SBC は，サーバで稼働させる PC のアプリケーションプログラムを，複数の TC で共用する方式である。一方，仮想 PC 方式は，PC の独立したプログラム実行環境（以下，仮想 PC という）を TC と 1 対 1 でサーバ上に用意する方式である。検討の結果，後者の方式を採用することにした。MPC にも，仮想 PC 方式に対応する機能をもつ機種を選定した。

IP-PBX で受けた問合せ電話に対して，TC で通話する場合，USB で接続したヘッドセット（以下，USB ヘッドセットという）を利用する。この USB ヘッドセットの利用方式については，USB リダイレクト方式と VoIP 対応 TC（以下，TC-V という）方式の，二つの方式がある。

USB リダイレクト方式は，TC に USB デバイスが接続されると，あたかも仮想 PC に USB デバイスが接続されたように動作させる機能を利用する方式である。

一方，仮想 PC に実装されたソフトフォンと TC の間で独自の制御を行うファームウェアが組み込まれた TC-V を利用するのが，TC-V 方式である。TC-V を利用した場合，呼制御は IP-PBX と仮想 PC 間で行うが，通話の音声を運ぶ RTP パケットは TC-V と IP-PBX 間で直接送受する。

USB リダイレクト方式と TC-V 方式の音声データの経路を，図 3 に示す。

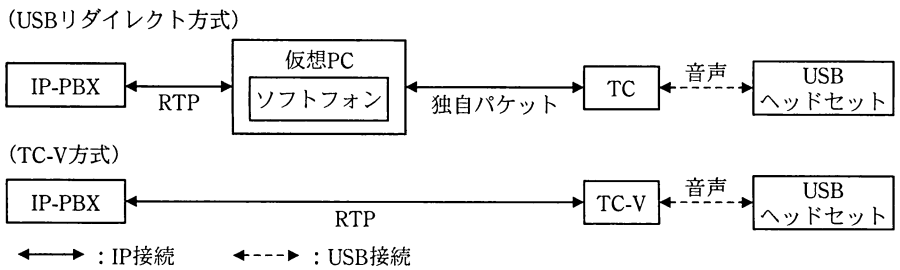


図 3　USB リダイレクト方式と TC-V 方式の音声データの経路

N 君は，TC を新規に導入する場合は音質を重視して TC-V を利用し，既存 PC を活用する場合は，導入の容易性・低コストの観点から，USB リダイレクト方式を利用することにした。

〔電話の着信場所の A 社データセンタへの統合化に伴う電話回線の必要数の算定〕

これまで地域保守会社に委託していた保守サービス業務は，一括して A 社データセンタに集約するので，再構築後の保守サービスシステムの電話回線数について，現在のシステムを分析し，その必要回線数について検討することにした。

現在のシステムの分析に当たり，まず，電話をかけても，回線がビジーとなってつながらない呼損状態が発生するモデル（待ち行列を作らないモデル）を想定した。呼損の発生確率を呼損率という。待ち行列理論では，待ち行列モデルを，“到着間隔の分布型／サービス時間の分布型／窓口数／待ち行列系の許容収容数”で表現するケンドール記法がよく使われる。この記法を使い，地域保守会社での受付のモデルを，ランダム到着（M），指数分布サービス（M）とし，M/M/s/s と考える。現在，地域保守会社は 10 社あり，地域ごとに受付回線 10 本で対応し，最繁時は 1 時間当たり 36 件の問

合せ電話がかかってくる。電話応対には，通話後の後処理時間を含め，1 件当たり平均 10 分掛かる。この場合，各地域の 1 時間当たりの到着率は［ a ］，サービス率は［ b ］，s の値は［ c ］となる。

再構築後，地域保守会社で受け付けていた問合せ電話を，②A 社で一括して受け付けるようにして，呼損率を従来と同等以下にするために，受付回線が何本必要となるかを，表 1 の呼損率表から求めることにした。

表 1　呼損率表

呼量＼回線数	10
6.0	4.3
6.7	6.7
7.0	7.9

呼量＼回線数	66	67	68	69	70	71	72
60.0	4.6	3.9	3.4	2.8	2.4	2.0	1.6
66.7	9.8	8.9	8.0	7.2	6.4	5.7	5.0
70.0	12.7	11.7	10.8	9.8	9.0	8.1	7.3

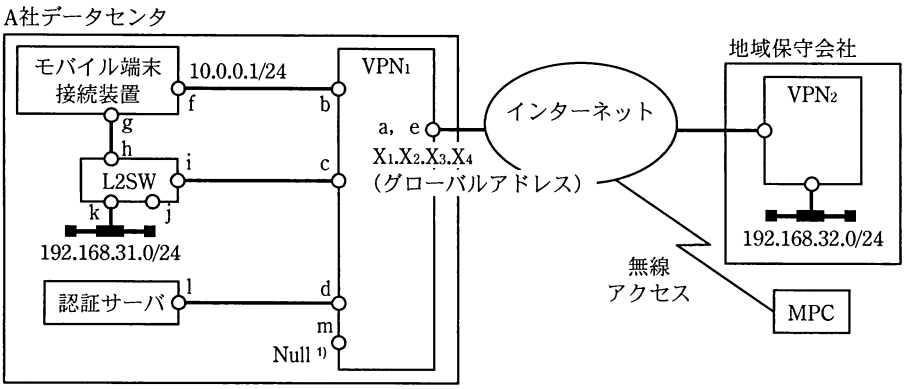
注記 1　呼量は単位時間（1 時間）当たりの通話時間の合計である。
注記 2　呼損率の単位は％であり，小数第 2 位を四捨五入している。

実際の運用では呼損が発生すると，繰り返しかかってくる問合せ電話によって到着率が増大するので，回線が輻輳（ふくそう）し，呼損率が急増する。A 社では，その対策として，③自動音声応答用に回線を追加し，電話が着信して待ち状態になる場合は，自動音声応答機能でコールバックするための受付情報を取得して，直ちに切断する方式を導入することにした。登録された受付情報は，空きとなった受付者に順次割り当てられ，処理される。

〔地域保守会社及び MPC から A 社データセンタへの接続ネットワークの検討〕

再構築後の A 社データセンタ側には，地域保守会社との接続方法及び MPC との接続方法を用意する必要がある。N 君は，A 社と地域保守会社間の既設ネットワークの状況をチェックした上で，CE がアクセスするための仕組みを追加導入することにした。

図 4 は，図 2 中の地域保守会社及び MPC から A 社データセンタへの接続部分を抜き出し，より詳細に示したものである。



○：インタフェース　　a～m：インタフェース識別記号　　L2SW：レイヤ2スイッチ
注 1)　mはNullポートであり，Nullポートに送出されたパケットは転送されない。

図 4　地域保守会社及び MPC から A 社データセンタへの接続（抜粋）

地域保守会社と A 社データセンタ間，及び MPC と A 社データセンタ間は，インターネットを介して VPN で接続する構成とした。VPN_1 と VPN_2 は，A 社データセンタと地域保守会社の LAN 間を接続する VPN 装置であり，ファイアウォールを兼ねている。

MPC からの接続制御を行うモバイル端末接続装置は，VPN_1 の配下に設置する。VPN_1 のインターネット側インタフェース a のグローバルアドレス宛てに送られてきたパケットの中でポート番号 443 のパケットは，そのままモバイル端末接続装置に転送される。モバイル端末接続装置は，認証サーバに問合せを行い，認証サーバが MPC の認証を行う。認証が完了すると，モバイル端末接続装置では，MPC があたかもインタフェース g にいて，L2SW のインタフェース h に接続しているように動作する。

N 君が，今回の接続方法検討に当たり，VPN_1 のルーティングの設定を調べたところ，VPN_1 と VPN_2 間のインターネット VPN 接続のためのアソシエーションが確立できなかった場合，暗号化されないパケットがインターネット側に送出されてしまうことを発見した。現状では，あまり大事に至らないと考えたが，念のため，外部に送出されないよう代替ルートの設定を行うことにした。今回採用した VPN_1 と VPN_2 間の VPN 接続では，VPN のトンネルが確立すると，その VPN トンネルの仮想的なインタフェースが，ルーティング上，有効な経路として扱われる。

N 君が作成した再構築後の VPN_1 のルーティング設定の抜粋を，表 2 に示す。宛先の“0.0.0.0/0”は，デフォルトルートを示している。ゲートウェイに“0.0.0.0”を指定したときは，ゲートウェイを経由せず直接宛先ネットワークに到達可能であることを

示している。また，メトリック値は数値が小さいほど優先度が高い。

表2　VPN_1のルーティング設定（抜粋）

No.	宛先	ゲートウェイ	インタフェース	メトリック値
1	0.0.0.0/0	$Y_1.Y_2.Y_3.Y_4$ 2)	a	1
2	$X_1.X_2.X_3.X_4$ 1)	0.0.0.0	a	0
3	10.0.0.0/24	0.0.0.0	b	0
4	192.168.31.0/24	0.0.0.0	c	0
5	192.168.32.0/24	0.0.0.0	e	1
6	ウ	エ	m	オ

注 1)　$X_1.X_2.X_3.X_4$：グローバルアドレスを表す。

注 2)　$Y_1.Y_2.Y_3.Y_4$：インターネット側のデフォルトゲートウェイを表す。

〔拡張性を考慮したA社データセンタ内ネットワーク構成の検討〕

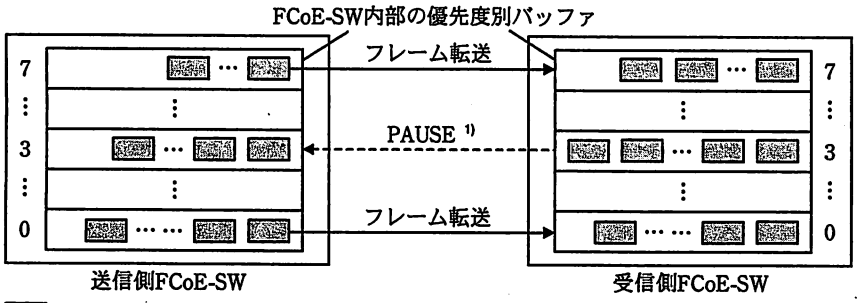
A社では，保守サービスシステムをデータセンタ内に統合するに当たり，今後のシステム拡張を容易にするためのネットワーク構成を検討することにした。データセンタでは，サーバの設置台数が増加し，中でも，ブレード型サーバの使用が増えている。ストレージは，FC（Fibre Channel）を使ったFC-SANが既に構築されていた。N君の調査によると，最近では，10Gビット／秒以上の高速イーサネットを使用し，FC-SANとLANを統合するFCoE（Fibre Channel over Ethernet）技術が登場している。この技術によって，FCプロトコル（以下，FCPという）をイーサネット上で動作させることができる。

FCの上位層であるSCSIは，パケットロスを前提としないプロトコルなので，SCSIの下位層では，パケットロスを防ぐ機能の実装が必要である。

パケットロスの要因としては，伝送路上でのビット誤りよりも，バッファの枯渇の方が大きいと考えられた。④FCでは，フロー制御の方法として，送信側と受信側の双方で，受信側の空きバッファ数を管理して送信を制御している。この方式を使うことによって，TCPで使われているような，ウィンドウサイズを用いたエンドシステム間の応答確認によるフロー制御では実現できないパケットロスの防止効果が得られる。

LANのMAC層でも，フロー制御の方法として，送信側に対してPAUSEフレームを送って送信を抑止する機能が，オプションとして規定されている。しかし，FCoEの実現には，この機能では不十分と考えられており，N君が調べたところ，FCoE対

応のスイッチ（以下，FCoE-SW という）では，図 5 に示すような優先度付バッファ制御機能を実装していることが分かった。



注 1) 受信側バッファの枯渇を防止するために送出する。

注記 0～7の数字は，FCoE-SW内のバッファの優先度を示す。数字が大きいほど優先度が高い。

図 5 FCoE-SW の優先度付バッファ制御機能

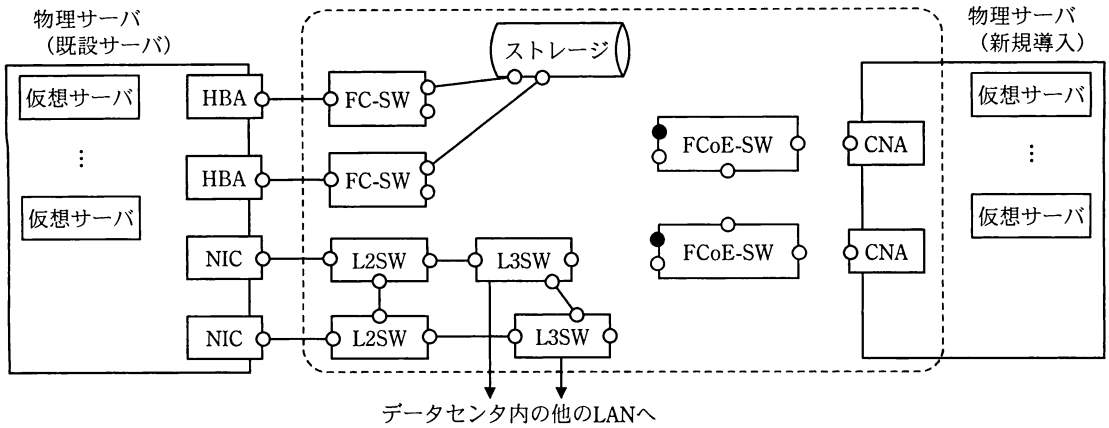
図 5 に示す方式では，⑤優先度別にバッファを用意し，受信バッファが枯渇したときには優先度別に送信を抑止するための PAUSE フレームを送出している。

N 君は，既設機器との接続性を確保しながら，SAN と LAN の将来の統合化に備えるために，CNA（Converged Network Adapter）と呼ばれるネットワーク接続アダプタ製品を使うことにした。この製品は，10 G ビット／秒のイーサネットと FCoE に対応しており，1 個のアダプタで HBA（Host Bus Adapter）と NIC を兼ねることができる。

加えて，CNA と接続する FCoE-SW は，IETF（Internet Engineering Task Force）で標準化が進められている TRILL（Transparent Interconnection of Lots of Links）に対応する製品とした。TRILL 対応の FCoE-SW に入ったフレームは，TRILL ヘッダでカプセル化され，出口の FCoE-SW でカプセル化が解除されて相手に届く。これによって，相互接続された複数の FCoE-SW が，一つの大きな FCoE-SW のように動作する。フレームの転送経路については，コストを評価して最短経路を決める SPF（Shortest Path First）というアルゴリズムを使用している。このアルゴリズムでは，経路を冗長化する場合，⑥経路のコストを適切に設計することによって，トラフィックを分散できる。その結果，冗長化のためにスパニングツリープロトコルを使った場合には得られない効果が期待できた。

今回導入することにした FCoE-SW には，FC と FCoE の相互変換機能が用意されて

いるということなので，既設のシステムに追加接続する形で，図 6 のような拡張性を考慮したネットワーク構成を考えた。ここで，二つの CNA は同時に使用する。



○：インタフェース　●：FCとFCoE相互変換機能のインタフェース　L3SW：レイヤ3スイッチ
注記　設問との関係で，一部の接続を表示していない。　FC-SW：FC対応スイッチ

図 6　拡張性を考慮したネットワーク構成

このようにして，N 君は，将来に向けて A 社データセンタの SAN と LAN の統合化に配慮しつつ，保守サービスシステムの再構築に向けての設計検討を終え，システムの構築作業に着手した。

設問 1　〔作業効率を高めるための CE 用 PC の選定〕について，(1)，(2)に答えよ。

(1)　本文中の［　ア　］，［　イ　］に入れる適切な字句を答えよ。

(2)　本文中の下線①について，CE が様々な場所からネットワーク接続を行う観点から，適切なプロトコル名を答えよ。

設問 2　〔TC システムの検討〕について，(1)，(2)に答えよ。

(1)　TC，TC-V に接続している LAN の音声転送用帯域は，TC-V 方式の方が少ない。使用するコーデックに関連して，その理由を 35 字以内で述べよ。

(2)　USB リダイレクト方式で，仮想 PC の処理によって発生する会話品質に影響を与える事象と，それに起因する音質劣化要因を組み合わせて二つ挙げ，答案用紙の空欄を埋めよ。

設問 3　〔電話の着信場所の A 社データセンタへの統合化に伴う電話回線の必要数の算定〕について，(1)～(3)に答えよ。

(1)　本文中の［　a　］～［　c　］に入れる適切な数値を答えよ。

(2) 本文中の下線②について，従来の呼損率は幾らか。また，従来と同等以下の呼損率を維持するための必要最小限の回線数を答えよ。答えは，表 1 中の数値で答えよ。

(3) 本文中の下線③について，対策後の方式は，どのような待ち行列のモデルとなるか。20 字以内で述べよ。

設問 4 〔地域保守会社及び MPC から A 社データセンタへの接続ネットワークの検討〕について，(1)～(4)に答えよ。

(1) 表 2 中，VPN トンネルのインタフェースはどれか。インタフェース識別記号で答えよ。

(2) 表 2 中 No.6 の行は，VPN トンネルが Active にならない状態で，暗号化されないパケットがインターネット側に送出されないようにする設定である。［ウ］～［オ］に当てはまるアドレスとメトリック値を答えよ。

(3) MPC がモバイル端末接続装置に接続できるようにするには，VPN_1 にどのような設定が必要か。60 字以内で述べよ。

(4) MPC のアプリケーションで使用するポートによって，送られてくるパケットを制限する設定は，A 社データセンタ内のどの機器で行う必要があるか。その機器名を答えよ。また，その機器に設定しなければならない理由を，50 字以内で述べよ。

設問 5 〔拡張性を考慮した A 社データセンタ内ネットワーク構成の検討〕について，(1)～(5)に答えよ。

(1) A 社データセンタのように，多数のブレードサーバを設置する環境で，SAN と LAN を統合することによって得られる設計上の効果を，40 字以内で述べよ。

(2) 本文中の下線④について，TCP で使われているようなウィンドウサイズによるフロー制御では実現できず，FCP のフロー制御方法によって可能になる，パケットロスの防止効果を，35 字以内で述べよ。

(3) 本文中の下線⑤について，優先度別制御をすることによって，どのような通信状態の発生を回避するのか。50 字以内で述べよ。

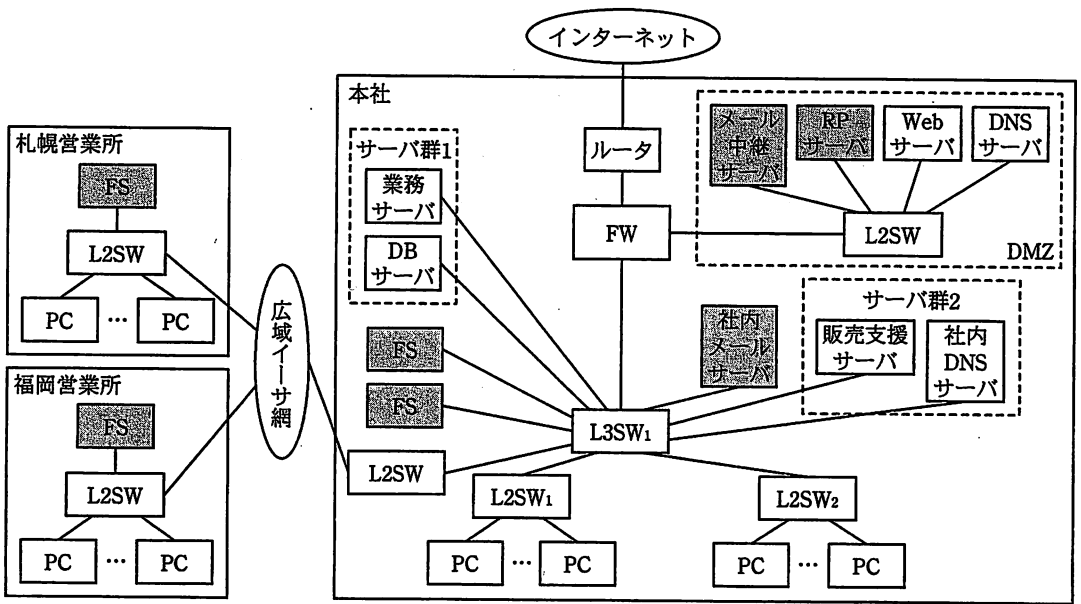
(4) 本文中の下線⑥を可能にする経路のコスト設計を，25 字以内で述べよ。また，スパニングツリープロトコルでは実現できず，この設計で得られる効果は何か。20 字以内で述べよ。

(5) 図 6 中の破線で囲まれた部分の接続について，不足している線を追加して，答案用紙の図を完成させよ。

問2　IT環境の改善に関する次の記述を読んで，設問1～6に答えよ。

Y社は，従業員400人のコンピュータ関連製品の販売会社で，東京に本社，札幌と福岡に営業所がある。Y社では，全社員が資料作成，インターネット利用などにPCを活用している。営業員は，外出時にPCを携帯して，顧客先での製品説明に活用するとともに，本社のDMZに設置されているリバースプロキシサーバ（以下，RPサーバという）経由で，販売支援サーバを利用している。

Y社のIT基盤である，現在のネットワークシステム構成を，図1に示す。



注記　網掛け部分は，IT環境改善後に撤去する予定のサーバである。
L3SW：レイヤ3スイッチ　　FW：ファイアウォール
L2SW：レイヤ2スイッチ　　FS：ファイルサーバ
広域イーサ網：広域イーサネットサービス網

図1　現在のネットワークシステム構成（抜粋）

情報システム部のF部長は，PCからの情報漏えいと，電子メール（以下，メールという），ファイルデータなど個人が管理しているデータの消失の危険性が内在する，社内のIT環境に不安を抱いていた。

その不安が現実のものとなる事故が発生した。営業員が，外出先で不注意からPCを落とし，破損させてしまったのである。このPCに保存されていたのは，営業活動

に欠かせないデータであり，困り果てた営業員は情報システム部に助けを求めてきた。情報システム部では，データ復旧サービスを利用して，PC に保存されたデータを回復させようとしたが，結局，ほとんどのデータが失われてしまった。F 部長は，このような事故を回避するために，ネットワーク担当の G 主任とサーバ・PC 担当の H 君に改善策を検討させることにした。

G 主任と H 君は，PC にデータを保存することが，情報漏えいとデータ消失リスクを大きくしていると考え，データを PC に保存しないシンクライアント（以下，TC という）システムを導入すべきであると判断した。また，メールサーバの運用にも改善すべき課題があったので，メールを一括してサーバに保管できる，外部のメールサービス（以下，メールサービスという）を活用するとともに，懸案であったメールアドレスのドメイン名の変更も提案することにした。二人は，これらの 2 点を改善策としてまとめ，F 部長に報告した。F 部長はこの報告を基に，IT 環境の改善に関する企画書を作成して取締役会で提案し，承認された。そこで F 部長は，早速，G 主任と H 君をメンバとする IT 環境改善プロジェクトを発足させ，TC システムの設計及びメールサービスへの移行方法の設計を指示した。

指示を受けた G 主任と H 君は，今後のプロジェクトの進め方と役割分担を決めた。

〔TC システムの設計〕

TC システムの設計を担当することになった H 君は，まず，TC について調査した。調査結果は，次のとおりである。

TC システムには複数の形態があり，その中で，画面の情報を TC に転送する形態（以下，画面転送型という）が，ネットワークへの負荷が少ないことが分かった。

画面転送型 TC システムには，サーバベース方式（以下，SBC という）と仮想 PC 方式がある。SBC は，サーバで稼働させる PC のアプリケーションプログラム（以下，AP という）を，複数の TC で共用する方式である。一方，仮想 PC 方式は，仮想化機構を組み込んだサーバに，PC の独立したプログラム実行環境を TC と 1 対 1 で用意する方式である。

TC システムを導入するときは，データの移動が必要になる。また，TC では，AP の使用方法が少なからず変わるので，一時的には業務の混乱を招くことが予想される。

H 君は，調査結果，現状のネットワークシステムの構成及び PC 利用の状況を SI 業

者のS社に説明して，TCシステムの提案を求めた。S社からは，次の2点を骨子とする提案を受けた。

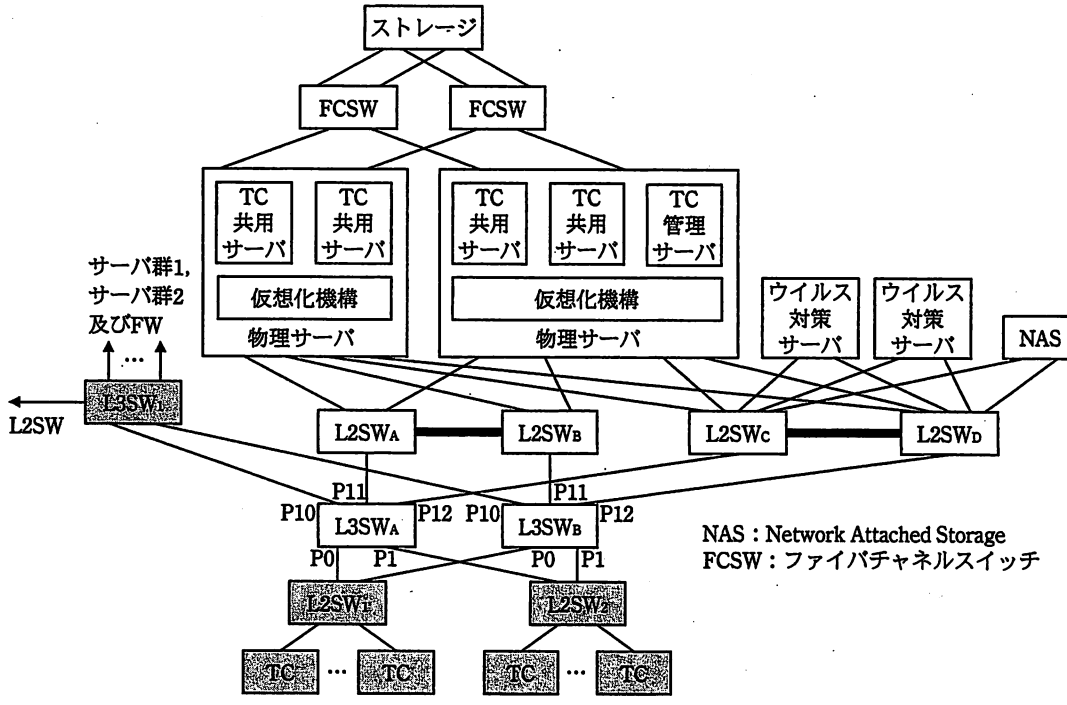
(1) TCシステムは，画面転送型のSBCとし，次の2段階に分けて導入する。

第1段階は，PCの持出し時の事故による，情報漏えいとデータ消失のリスクが大きい営業員のうち，本社所属の80人に導入する。

第2段階は，第1段階の導入，運用経験を生かして，全社に展開する。

(2) 使用中のPCは，更新時までTCとして活用する。

S社から提案を受けた，TCシステムの構成を，図2に示す。



注記1 L2SWAとL2SWB，L2SWCとL2SWDを接続する太線は，スタック接続を示す。
注記2 L3SWのP0，P1，P10，P11，P12は，ポート番号を示す。
注記3 TCは，既設のPCを流用する。
注記4 網掛け部分は，既設の機器を示す。

図2 TCシステムの構成

TCシステムは，TC共用サーバ，TC管理サーバなどで構成される。

TCをTC管理サーバに接続すると，ログインパスワードの入力が求められる。ログ

インパスワードを入力して TC 管理サーバで認証されると，TC は TC 共用サーバに接続され，利用可能になる。このとき，TC は最も低負荷の TC 共用サーバに接続され，TC 共用サーバの負荷が平準化される。

次は，TC システムの構成に関する，S 社の I さん，G 主任及び H 君の会話である。

I さん ：TC システムは，仮想化機構によって作成された仮想サーバ上で稼働させます。第 1 段階では，物理サーバを 2 台導入して，TC 共用サーバと TC 管理サーバを稼働させます。第 1 段階の導入では，既設のサーバ，$L3SW_1$ 及び FW の IP アドレスの変更は伴いませんが，本社の PC の IP アドレスの変更と $L3SW_1$ への IP アドレスの追加設定が必要になります。

H 君 ：構成については分かりました。NAS は，どんな用途に使用するのですか。

I さん ：用途は，二つあります。一つは，利用者ごとの TC 利用環境を作るための情報を記録したファイル（以下，プロファイルという）を保管します。プロファイルの働きによって，①TC 共用サーバにログインすると，ログインした利用者の TC 利用環境が作られます。二つ目は，TC 利用者が作成したファイル類を保管します。第 1 段階で，本社の FS を NAS に統合します。

H 君 ：FS のデータバックアップ作業が負担になっていましたから，助かります。営業所の FS も NAS に統合しますよね。

I さん ：それは，第 2 段階で行うことを提案します。

H 君 ：そうですか。

G 主任：サーバとネットワーク機器の冗長化は，どのような方法で行うのですか。

I さん ：$L2SW_A$ と $L2SW_B$，$L2SW_C$ と $L2SW_D$ は，スタック接続して一つのスイッチとして扱えるようにします。これらの L2SW から，サーバ，NAS 間の接続には，リンクアグリゲーションを設定します。サーバと NAS の NIC には，チーミング機能を設定して 2 本の回線に負荷を分散させ，［　ア　］と冗長化を図ります。$L3SW_A$，$L3SW_B$ 及び $L3SW_1$ では，静的経路制御を行わせます。$L3SW_A$ と $L3SW_B$ における VRRP 関連の設定内容は，表 1 のとおりです。

G 主任：$L2SW_1$，$L2SW_2$，$L3SW_A$，$L3SW_B$ 間でループが発生しませんか。

I さん ：表 1 の構成なので，ループは発生しません。また，②ポートやケーブルの障害時には，全ての VRRP が同期して，同じ L3SW がマスタルータになります。

G 主任：分かりました。

表1　$L3SW_A$ と $L3SW_B$ における VRRP 関連の設定内容（抜粋）

項目	設定1		設定2		設定3	
VRRP グループ ID	1		2		3	
VLAN ID	VLAN1		VLAN2		VLAN3	
仮想 IP アドレス	IPVIP10		IPVIP20		IPVIP30	
所属ポート	P0		P1		P10	
仮想 MAC アドレス	00-00-5e-00-01-01		00-00-5e-00-01-02		00-00-5e-00-01-03	
Priority 値	$L3SW_A$	$L3SW_B$	$L3SW_A$	$L3SW_B$	$L3SW_A$	$L3SW_B$
	100	80	100	80	100	80
監視対象インタフェース	P1, P10, P11, P12		P0, P10, P11, P12		P0, P1, P11, P12	
障害検出時の Priority 値	50		50		50	

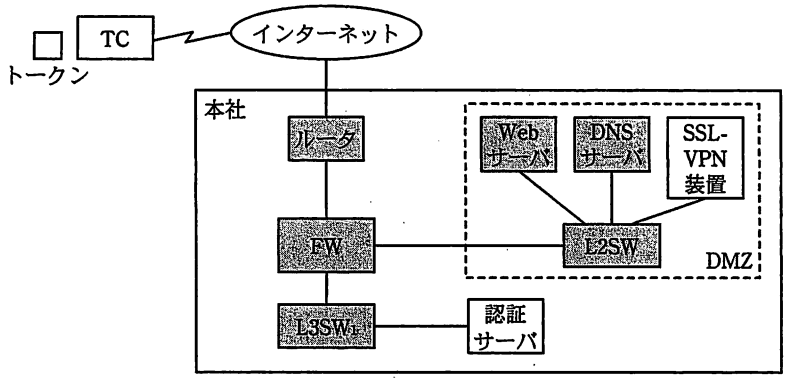
VRRP では，VRRP メッセージ（VRRP advertisement）がマスタルータから［　イ　］ルータへ送信され，マスタルータの稼働状態が報告される。VRRP メッセージは，宛先 IP アドレスが 224.0.0.18 の［　ウ　］キャスト通信である。Priority 値は，大小関係で優先順位が決まり，Preempt モードでは L3SW の起動タイミングに関係なく，最も［　エ　］値をもつルータが，マスタルータになる。

〔社外での TC 使用時のセキュリティ対策〕

社外で TC を使用しても，社内と全く同じ処理ができる。そこで G 主任は，社外での TC 使用時には，どのようなセキュリティ対策を講じるのかを，I さんに確認した。

I さんの説明を，次に示す。

社外で TC を使用するときには，トークンを使ったワンタイムパスワード（以下，OTP という）方式の認証でセキュリティを確保する。OTP の認証処理を行う認証サーバは，新たに導入して $L3SW_1$ に接続する。また，認証から TC 共用サーバへのログインまでの，一連の処理を自動化する機能をもつ SSL-VPN 装置を，DMZ に設置する。社外で TC を使用するための認証システム構成を，図3に示す。



注記　網掛け部分は，既設の機器を示す。

図3　社外でTCを使用するための認証システム構成

社外で TC を使用するときには，まず TC を SSL-VPN 装置に接続させると，SSL-VPN 装置から，利用者 ID，ログインパスワード，OTP の入力が求められる。これらを入力すると，SSL-VPN 装置の連携機能によって，OTP の認証，ログインパスワードの認証及び TC 共用サーバへのログインが自動的に行われる。ログイン後，TC にはデスクトップ画面が表示され，必要な AP を使用することができる。

OTP は，時刻同期方式を利用する。社員に，あらかじめトークンと呼ばれるパスワード生成器を配布する。トークンが生成する数字は 1 分経過ごとに変化し，一度しか使用できない。本方式では，時刻のずれが発生するので，ずれの許容範囲を設定する。認証サーバは，許容範囲内で認証を試みて，認証できたらトークンとの時刻のずれを推定して記憶し，次回の認証時に，記憶したずれを基に時刻の補正を行う。

次に，G 主任と H 君は，メールサービスの利用について検討した。

〔現在のメールシステムの構成と利用状況〕

まず，G 主任は H 君に対して，図 1 に示した現在のメールシステムの構成と利用状況を，次のように説明した。

DMZ に，Y 社ドメイン（以下，y-sya.example.co.jp という）宛てのメールを受信するメール中継サーバがあり，社外へのメールも，このサーバが中継している。社内には，社員が送受信に使用する社内メールサーバがある。

DMZ に設置された，DNS サーバのゾーンデータファイルの内容を，図 4 に示す。

```
$TTL 86400 ; 1日
@ IN SOA ns.y-sya.example.co.jp. hostmaster.y-sya.example.co.jp. (
        2011090101 ; serial番号
        43200      ; refresh 時間（12時間）
        1800       ; retry 時間（30分）
        604800     ; expire 時間（7日）
        10800 ）   ; negative cache 時間（3時間）
    IN NS ns.y-sya.example.co.jp.
    IN MX 10 mail.y-sya.example.co.jp.
```

図 4　DNS サーバのゾーンデータファイルの内容（抜粋）

Y 社では，メール消失事故を防ぐために，数年前に IMAP4 の使用を推奨した。しかし，強制をしなかったので，現在でも多くの社員が POP3 を使用している。IMAP4 の利用者は，社内メールサーバに作成したフォルダにメールを保存している。POP3 の利用者は，PC に作成したフォルダにメールを保存し，メールボックスのメールは，メーラでダウンロード後に消去されるように設定している。Y 社では，PC のフォルダに保存したメールの障害時に備えた対応作業は，社員に任せている。

POP3 と IMAP4 の違いは，メーラを使っているだけではほとんど意識されない。しかし，③複数の PC で同じメールアカウントを使用するときには，違いが分かる。

〔メールサービスへの移行方法の設計〕

メールサービスについては，サービス料金，機能，保存可能なメール容量，セキュリティ対策状況などを調査し，M 社のメールサービスを利用することにした。

二人が設計した，IT 環境改善後のネットワークシステム構成を，図 5 に示す。

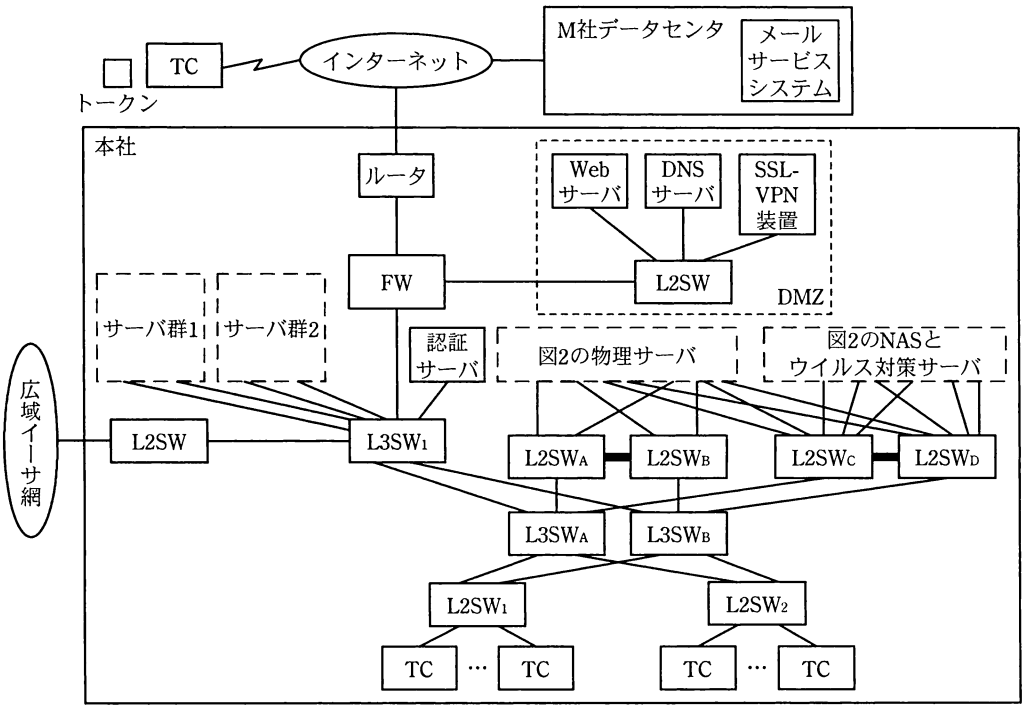


図5　IT環境改善後のネットワークシステム構成（抜粋）

次に，二人は，M社のメールサービスへの移行方法の設計を行った。

M社のメールサービスでは，メールを長期間保存できるだけの容量とアーカイブサービスが提供されているので，メール消失リスクを回避できる。メールサービスでは，使用中のメーラを継続して使えるだけでなく，Webブラウザのメーラ（以下，Webメールという）も提供されている。M社のWebメールは，使用中のメーラと同等の操作性なので，運用の容易さを重視し，TCではWebメールを使用させることにする。Webメールでは，社内メールサーバ及びPCに作成されたフォルダは使用できないので，Webメール使用前に，使用中のメーラを使って，必要なメールをメールサービスに移動させる。社内メールサーバに登録されているメーリングリスト（以下，MLという）には，社内用，社外向けに公開しているものなど多種のものがあり，それらの中には，利用されていないものも多い。MLのメールサービスへの登録は，移行ツールが提供されていないので，個別に登録する必要がある。そこで，MLは，メールサービス利用開始後に，必要性を精査して登録することにする。

M社のメールサービスでは，メールサービスの利用契約を締結した後に，統一するY社の新しいドメイン（以下，y-sya.example.comという）が設定され，M社のDNS

サーバで公開される。

二人がまとめた，メールサービスへの切替スケジュールを，図6に示す。

項番	作業名	作業者	作業開始からの経過							
			1週	2週	3週	4週	5週	6週	7週	8週
1	アカウントの登録，中継設定	情報システム部	→	→						
2	パスワードの設定，接続設定	利用者			→	→				
3	メールアドレスの変換設定	情報システム部				▲	（夜間に実施）			
4	メールサービスへの切替え設定	利用者				▲	（業務開始前に実施）			
5	フォルダ，メールの移行	利用者					→	→		
6	MLの登録	情報システム部					→	→		
7	中継設定の解除	情報システム部							▲	
8	MXレコードの変更	情報システム部							▲	
9	メールサーバの撤去	情報システム部								▲

図6　メールサービスへの切替スケジュール

図6中の項番で，各作業者が行う具体的な作業内容を，次に示す。

1. メールサービスに，社員のアカウントを登録する。個人のメールアドレスのユーザ名は，使用中のものをそのまま使う。また，メールサービスが y-sya.example.co.jp 宛てのメールを受信したとき，そのユーザのアカウントが登録されていれば，メールサービスのメールボックスに配信され，登録されていないアカウントや ML のときは y-sya.example.co.jp に中継されるように，あらかじめ設定しておく。
2. メールサービスのツールで，パスワードを設定する。また，使用中のメーラでメールサービスへの接続設定を行う。社内メールサーバと PC に保存されたメールをメールサービスに移動させるために，メール読出しは IMAP4 を使用する。これらの設定によって，使用中のメーラで，メールサービスと社内メールサーバの両方でメール送受信を行えるようになる。この段階では，メールの送受信を社内メールサーバで行うように設定する。
3. 社内メールサーバが受信したメールを，メールサービスに配送させるために，社内メールサーバに，メールアドレスの変換設定を行う。この変換は，メールアドレスの y-sya.example.co.jp を y-sya.example.com に書き換えるもので，ML に関しては，個人アドレスに展開された後に，この変換が行われる。宛先ドメインが書き換えられたメールは，メールサービスに配送されることになる。

4. メールの送受信をメールサービスに切り替える。
5. 社内メールサーバとPCに保存されたメールをメールサービスに移動する。
6. MLを見直して，メールサービスに登録する。
7. 項番1でメールサービスに設定した，y-sya.example.co.jpへの中継を解除する。
8. DNSサーバのMXレコードを変更し，y-sya.example.co.jp宛てのメールをメールサービスに配送させる。
9. 社内メールサーバとメール中継サーバを撤去する。

なお，TCシステムの導入には，ファイルの移動と既設のPC，ネットワーク機器の設定変更などが必要になることから，メールサービスに移行した後，TCシステムを導入することにした。

G主任とH君からの設計内容の説明を受けたF部長は，TCシステムの方式とその導入ステップ及びメールサービスへの切替手順に問題がないと判断し，プロジェクトメンバに改善への取組みを指示した。

設問1　本文中の［　ア　］～［　エ　］に入れる適切な字句を答えよ。

設問2　〔TCシステムの設計〕について，(1)～(5)に答えよ。

(1) 本文中の下線①を実現させるためには，何と何が対応付けられる必要があるかを，15字以内で答えよ。

(2) 営業所のFSのNASへの統合を第2段階で行うのは，どのような問題の発生を避けるためか。その問題の内容を，25字以内で述べよ。

(3) 図2中の$L2SW_1$，$L2SW_2$，$L3SW_A$，$L3SW_B$間でループは発生しない。表1を参照し，その理由を，25字以内で述べよ。

(4) 本文中の下線②の動作のために設定している項目を，表1から答えよ。また，その項目を設定した場合，障害発生時のVRRPの動作を，50字以内で述べよ。

(5) VRRPメッセージに含まれる情報を，表1中の項目で，三つ答えよ。

設問3　〔社外でのTC使用時のセキュリティ対策〕について，(1)，(2)に答えよ。

(1) トークンが生成する数字を変化させる時間間隔を長くすると，トークンに表示された数字を正しく入力しても，不正パスワードになるケースが発生するこ

とがある。その理由を，20字以内で述べよ。

(2) 本文中の時刻同期方式で，ずれた時刻を認証サーバが推定する方法を，50字以内で述べよ。

設問4 〔現在のメールシステムの構成と利用状況〕について，(1)～(3)に答えよ。

(1) 社員に任せている，障害時に備えた対応作業の内容を，30字以内で述べよ。

(2) 本文中の下線③のときに，POP3で発生する問題を，30字以内で述べよ。

(3) 図4において，セカンダリDNSサーバが，ゾーンデータファイルをコピーすべきか否かをチェックする時間間隔を答えよ。

設問5 〔メールサービスへの移行方法の設計〕について，(1)～(3)に答えよ。

(1) 図6中の項番2の作業期間中，メール送受信を社内メールサーバだけで行わせる理由を，50字以内で述べよ。

(2) 図6中の項番3の作業の代わりに，社内メールサーバがメールを受信したときに，そのメールをそのままメールサービスに転送させる中継設定を行ったとする。この場合，メールサービスにアカウントが存在しないメールアドレス宛てのメールで問題が発生する。その問題を，40字以内で述べよ。

(3) 図6中の項番4の実施後，項番6でMLが登録されるまでの間に，社内から，Y社の社員だけが登録されているML宛てに送信されたメールは，どのように転送されてメールサービスのメールボックスに配信されるか。メールサーバ名又はメールサービスを，【転送経路】の表記方法に従い，経由する順に全て列挙せよ。

【転送経路】

経由する順に全て列挙	→ メールサービス → メールボックス

設問6 第1段階のTCシステム導入時の作業と変更について，(1)，(2)に答えよ。

(1) 移動すべきデータを二つ挙げ，それぞれの移動先とともに答えよ。

(2) 本社の既設のPCと$L3SW_1$に設定されているネットワーク関連情報のうち，機器のインタフェースのIPアドレス以外に，変更されるべき情報を二つ挙げ，それぞれ20字以内で述べよ。

〔 メ モ 用 紙 〕

7. 退室可能時間に途中で退室する場合には，手を挙げて監督員に合図し，答案用紙が回収されてから静かに退室してください。

退室可能時間	15:10 ～ 16:20

8. **問題に関する質問にはお答えできません。**文意どおり解釈してください。
9. 問題冊子の余白などは，適宜利用して構いません。
10. 試験時間中，机上に置けるもの及び使用できるものは，次のものに限ります。
なお，会場での貸出しは行っていません。
受験票，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（アラームなど時計以外の機能は使用不可），ハンカチ，ティッシュ，目薬
これら以外は机上に置けません。使用もできません。
11. 試験終了後，この問題冊子は持ち帰ることができます。
12. 答案用紙は，いかなる場合でも提出してください。回収時に提出しない場合は，採点されません。
13. 試験時間中にトイレへ行きたくなったり，気分が悪くなったりした場合は，手を挙げて監督員に合図してください。