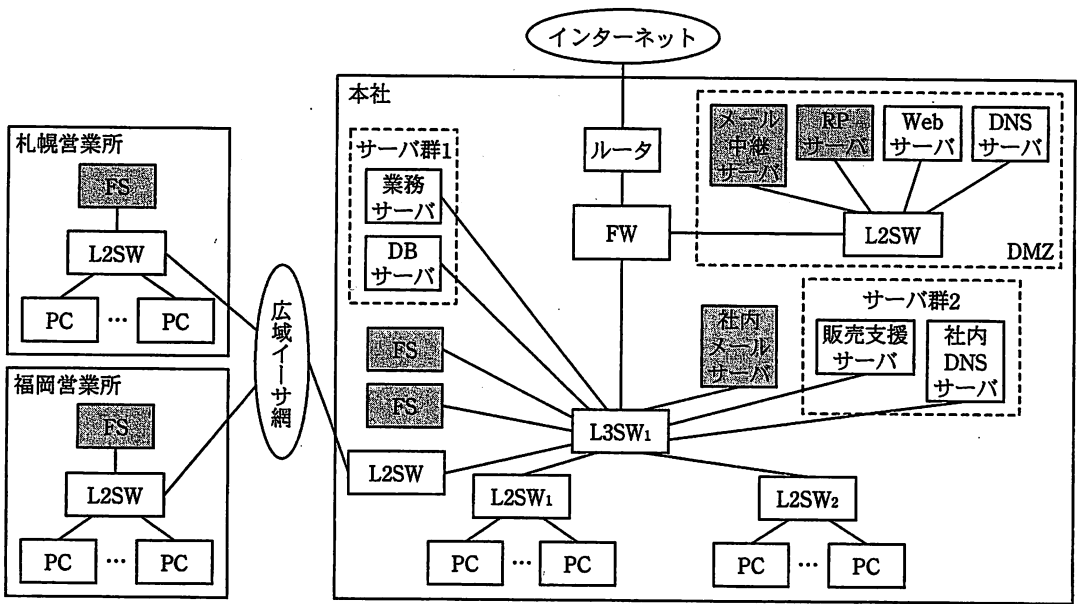
問2　IT環境の改善に関する次の記述を読んで，設問1～6に答えよ。

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。

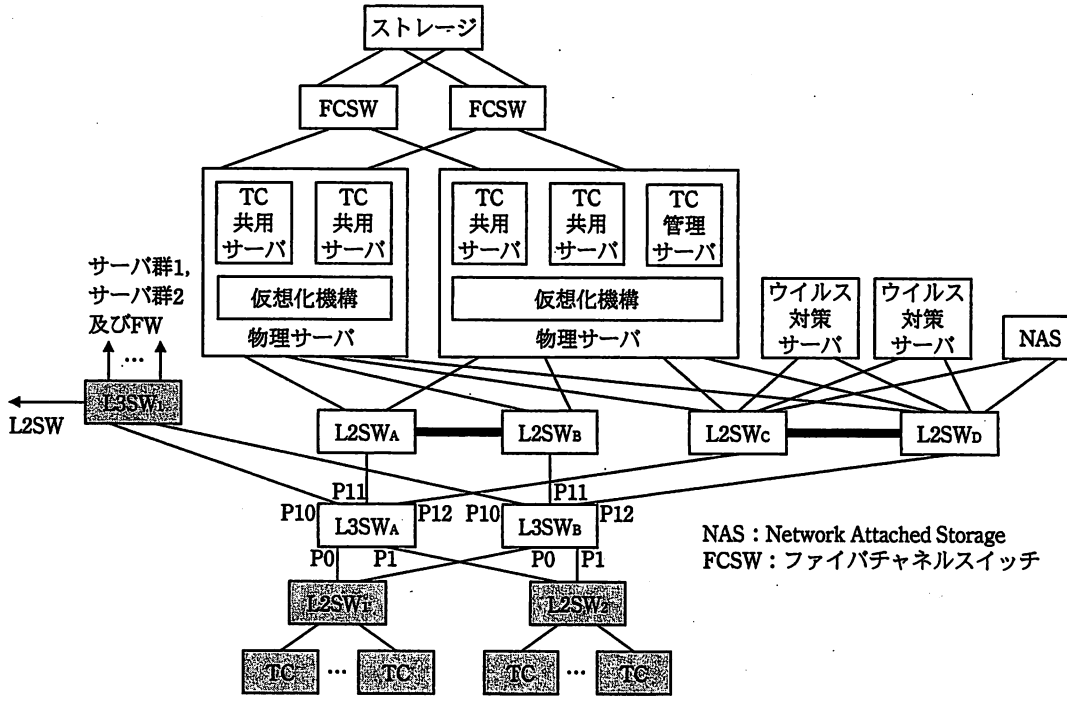
(1) TCシステムは，画面転送型のSBCとし，次の2段階に分けて導入する。

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	

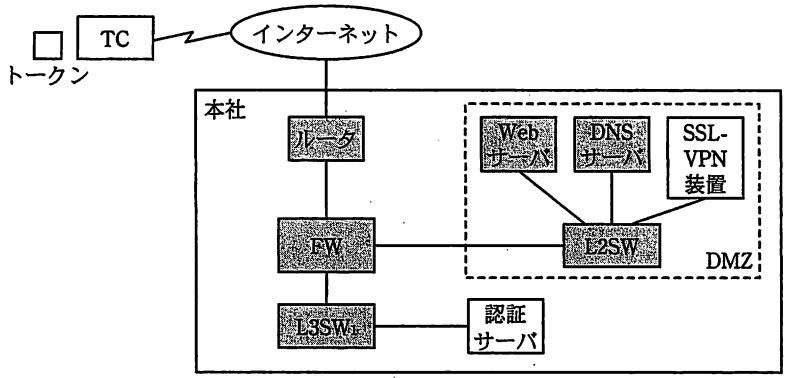
VRRP では，VRRP メッセージ（VRRP advertisement）がマスタルータから［　イ　］ルータへ送信され，マスタルータの稼働状態が報告される。VRRP メッセージは，宛先 IP アドレスが 224.0.0.18 の［　ウ　］キャスト通信である。Priority 値は，大小関係で優先順位が決まり，Preempt モードでは L3SW の起動タイミングに関係なく，最も［　エ　］値をもつルータが，マスタルータになる。

〔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。

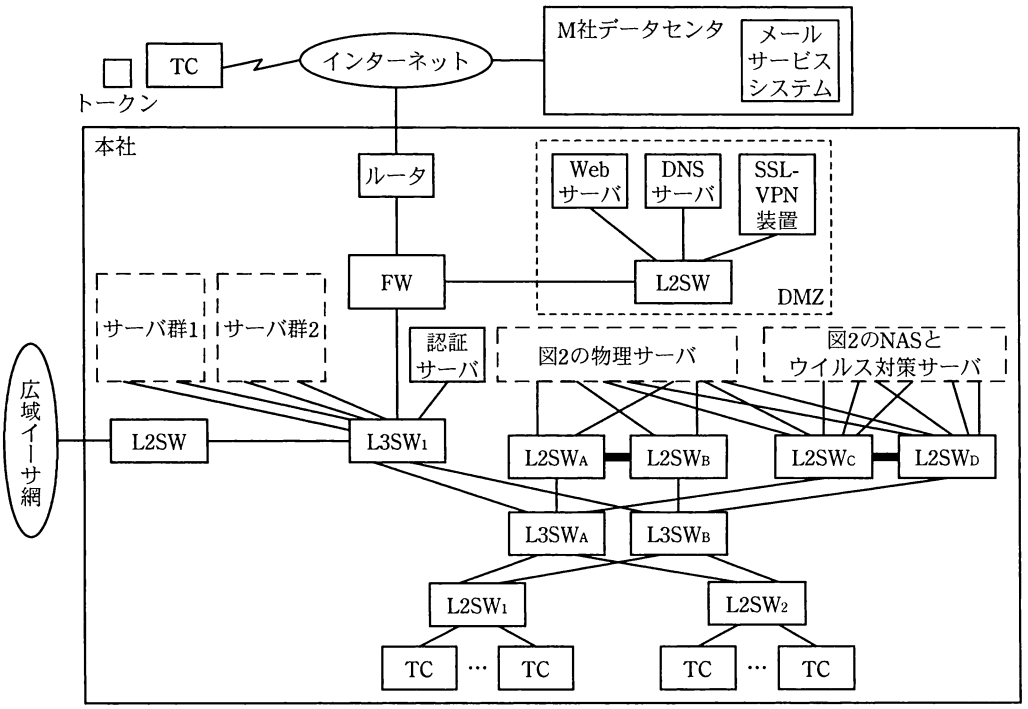


図5　IT環境改善後のネットワークシステム構成（抜粋）

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。