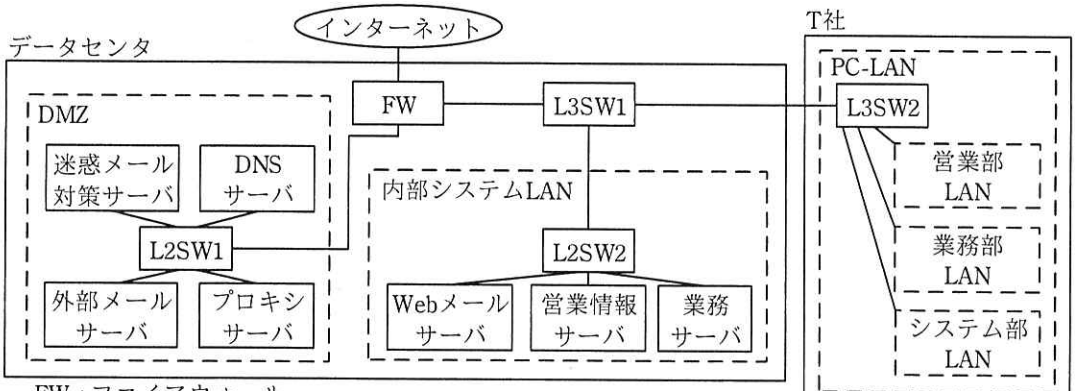
問2　情報セキュリティ対策の強化に関する次の記述を読んで，設問1～3に答えよ。

T社は，従業員数300名の小売業者である。

T社のネットワーク構成を図1に示す。



FW：ファイアウォール
L2SW：レイヤ2スイッチ
L3SW：レイヤ3スイッチ
注記　PCの記載は省略している。

図1　T社のネットワーク構成

T社は，全ての従業員にPCを1台ずつ貸与している。PCは全て，営業部LAN，業務部LAN及びシステム部LANのいずれかに接続されている。PC及び内部システムLANのサーバには，固定のプライベートIPアドレスを割り当てている。

T社では，電子メール（以下，メールという）の送受信及びWeb閲覧にインターネットを利用している。T社のドメイン名は，t-sha.co.jp（以下，T社ドメイン名という）である。また，全ての従業員は，T社ドメイン名のメールアカウントをもつ。

T社では，PC及びサーバを導入する際，システム部がアプリケーションソフトウェア，L社製マルウェア対策ソフト及びOS（以下，これらを併せてT社標準ソフトという）のインストール，脆弱性修正プログラムの適用，並びにマルウェア定義ファイルの最新化を行う。導入後のPC及びサーバは，プロキシサーバ経由でT社標準ソフトの各ベンダのサイトに毎月1回自動で接続し，それぞれの脆弱性修正プログラムを適用している。マルウェア定義ファイルは，1時間おきに最新化している。

〔内部システム LAN 上のサーバの概要〕

T 社の内部システム LAN とその LAN 上のサーバは，システム部の K さんが運用業務を担当している。内部システム LAN 上のサーバの機能の概要を表 1 に示す。表 1 に示す機能は全て有効にしている。

表 1　内部システム LAN 上のサーバの機能の概要（抜粋）

サーバ名	IP アドレス	機能の概要
Web メールサーバ	192.168.1.11	・SMTP で，迷惑メール対策サーバからのメールを受信するメール受信機能がある。 ・外部メールサーバに，SMTP でメールを転送するメール転送機能がある。 ・PC から Web ブラウザによってメールを送受信できるようにする Web メール機能，及びメールボックス機能がある。Web ブラウザとの通信プロトコルとして HTTP を用いる。 ・SMTP 通信及び HTTP 通信のマルウェアスキャンを行うマルウェアスキャン機能がある。 ・IP アドレス単位に，HTTP による接続を拒否することができる HTTP 接続拒否機能がある。その機能を用いて，内部システム LAN 上の他のサーバからの接続を拒否している。 ・送信メールについて，送信者メールアドレスをメールアカウントに対応付ける送信者メールアドレス詐称防止機能がある。 ・インターネットへの送信メールについて，送信者メールアドレスごとにインターネットへの送信の可否を設定できるインターネットメール送信制限機能がある。業務上，インターネットへの送信の必要がある者の送信者メールアドレスに対してインターネットへの送信を許可している。 ・DNS 機能がある。社内専用のドメイン名を管理する。インターネット上のドメイン名の名前解決は行わない。

運用業務において，内部システム LAN 上のサーバへのログインには，SSH を利用している。

〔DMZ 上のサーバ及び FW の概要〕

DMZ 上のサーバには，固定のグローバル IP アドレスを割り当てている。DMZ 上のサーバで，プログラムが異常停止するなどのエラーが発生した場合，迷惑メール対策サーバを経由してシステム部の運用担当者のメールアドレス宛てに通知している。

DMZ 上のサーバの機能の概要を表 2 に示す。表 2 に示す機能は全て有効にしている。

表 2　DMZ 上のサーバの機能の概要

サーバ名	IP アドレス	機能の概要
迷惑メール対策サーバ	x1.y1.z1.2	・受信したメールを Web メールサーバに SMTP で転送する機能がある。 ・インターネットからのメールの受信において，SPF（Sender Policy Framework）を用いてメールの転送を許可又は拒否する機能がある。 ・インターネットからのメールの受信において，メールの件名及び本文の内容によって迷惑メールと判定したメールを破棄する機能がある。
DNS サーバ	x1.y1.z1.3	・インターネット向けの T 社ドメイン名を管理する機能がある。 ・インターネット上のドメイン名の名前解決を行う機能がある。 ・オープンリゾルバ防止機能がある。
外部メールサーバ	x1.y1.z1.4	・転送されてきたメールをインターネットに SMTP で転送する機能がある。
プロキシサーバ	x1.y1.z1.5	・PC 及びサーバからインターネットへの HTTP 及び HTTP over TLS（以下，HTTPS という）通信を中継するプロキシ機能がある。HTTPS 通信の中継には，CONNECT メソッドを利用する。 ・送信元 IP アドレスごとにプロキシサーバへの接続可否を設定できる接続元制限機能がある。現在の設定は，T 社のネットワーク内の IP アドレスからの接続だけを許可している。 ・送信元 IP アドレスごとに接続可能な URL を制限するアクセス制限機能がある。現在は，全ての URL への接続を許可している。 ・プロキシサーバからの接続を許可する宛先ポート番号を設定するポート制限機能がある。現在は，1023 以下の宛先ポート番号だけを許可している。

運用業務において，DMZ 上のサーバへのログインには，SSH を利用している。

DNS サーバに登録されている，T 社ドメイン名に対する TXT レコードの設定内容を図 2 に示す。

```
t-sha.co.jp.      IN TXT "v=spf1 +ip4:[    a    ] -all"
```

図 2　T 社ドメイン名に対する TXT レコードの設定内容

FW は，ステートフルパケットインスペクション型である。そのフィルタリングル

ールを表3に示す。

表3　FWのフィルタリングルール

項番	送信元	宛先	サービス	動作	ログ取得
1	インターネット	b	SMTP	許可	する
2	b	c	SMTP	許可	する
3	c	d	SMTP	許可	する
4	d	インターネット	SMTP	許可	する
⋮	⋮	⋮	⋮	⋮	⋮
25	全て	全て	全て	拒否	する

注記1　項番が小さいルールから順に，最初に合致したルールが適用される。
注記2　項番5～24はSMTP以外のサービスに関するルールであり，PC及び内部システムLAN上のサーバと，インターネットの間の通信を許可するものはない。

〔セキュリティ対策の見直し〕

同業他社で，運用担当者のPCがマルウェアに感染し，サーバに格納されていた個人情報が大量に漏えいする事故が発生した。T社の経営陣は事態を重く見て，現状の対策の点検と見直しをシステム部のJ部長に指示した。J部長は，サーバの設定の点検及び見直し並びに運用担当者のPCの利用方法の見直しを行うようにKさんに指示した。さらに，セキュリティ専門業者に助言を求めることにし，情報処理安全確保支援士（登録セキスペ）のW氏が担当することになった。

〔サーバの設定の点検及び見直し〕

Kさんは W氏の支援を受けて，表4に示すサーバの設定のチェックリストを作成した。

表4　サーバの設定のチェックリスト（抜粋）

サーバ名	機能名	チェック内容
DNSサーバ	オープンリゾルバ防止機能	DNSサーバがeを許可するのは，DMZ上の他のサーバからだけであること
プロキシサーバ	接続元制限機能	DMZ上のサーバ，内部システムLAN上のサーバ及びPC-LAN上のPCだけが，プロキシサーバに接続可能であること
	ポート制限機能	接続を許可すべき宛先ポート番号を設定していること

表 4 に基づいて点検していたところ，プロキシサーバのポート制限機能に問題があることが分かった。次は，プロキシサーバのポート制限機能の利用方法に関する，W 氏と K さんの会話である。

W 氏　：プロキシサーバの設定をみると，CONNECT メソッドの悪用を防ぐ制限がなされていませんね。

K さん：CONNECT メソッドを悪用すると，どういう問題が生じるのでしょうか。

W 氏　：図 3 に示すように，CONNECT メソッドを悪用してトンネルを確立させることで，Web メールサーバの機能を回避できます。そして，①この回避によっていくつかの問題が生じます。

K さん：ポート制限機能に関する設計の見直しと設定変更案を作成します。

```
CONNECT x1.y1.z1.4:25 HTTP/1.1
```

図 3　CONNECT メソッドを悪用したリクエスト

K さんと W 氏は，サーバの点検を続け，他に問題がないことを確認した。

〔運用担当者の PC の利用方法の見直し〕

引き続き K さんと W 氏は，運用担当者の PC の利用方法の見直しを行った。

運用担当者は，運用担当者の PC からサーバに特権 ID でログインしているので，PC がマルウェアに感染した場合，サーバの重要な情報が窃取されるおそれがある。また，メールの送受信やインターネットの Web 閲覧は，マルウェア感染のリスクが高い。そこで，次の対策を実施することにした。

・運用担当者には，運用担当者の PC の他に，運用業務専用の PC（以下，運用 PC という）も貸与する。

・サーバの運用業務は，運用 PC だけで行うルールとする。

・運用 PC では，メールの送受信及びインターネットの Web 閲覧を技術的に制限する。

・L3SW2 に接続する運用 PC-LAN を新設し，そこに運用 PC を接続する。

その上で，次の設定を変更することにした。

・L3SW1 及び L3SW2 での IP アドレス指定によるフィルタリング設定

・②Web メールサーバの HTTP 接続拒否機能の設定

・③プロキシサーバのアクセス制限機能の設定

K さんは，運用 PC の利用方法案並びにサーバ及び L3SW の設定変更案を作成して，J 部長に説明し，了承を得た。K さんは，運用 PC の導入に着手し，サーバ及び L3SW の設定変更を行った。

設問 1　〔DMZ 上のサーバ及び FW の概要〕について，(1)，(2)に答えよ。

(1) 図 2 中の［ a ］に入れる適切な字句を答えよ。

(2) 表 3 中の［ b ］，［ c ］及び［ d ］に入れる適切なサーバ名を図 1 中の字句を用いて答えよ。

設問 2　〔サーバの設定の点検及び見直し〕について，(1)，(2)に答えよ。

(1) 表 4 中の［ e ］に入れる適切な通信の内容を 30 字以内で述べよ。

(2) 本文中の下線①について，回避によって生じる問題を二つ挙げ，それぞれ 40 字以内で具体的に述べよ。

設問 3　〔運用担当者の PC の利用方法の見直し〕について，(1)，(2)に答えよ。

(1) 本文中の下線②について，設定内容の変更点を 30 字以内で具体的に述べよ。

(2) 本文中の下線③について，設定内容の変更点を 55 字以内で具体的に述べよ。