問1　シンクライアント技術を利用したマルウェア対策に関する次の記述を読んで，設問1～5に答えよ。

A社は，従業員数20,000名の金融機関である。A社では，これまで，本店，国内支店及び海外支店で働く従業員間の情報共有，電子メール（以下，メールという）の送受信及びインターネット上のWebサイトアクセスのための環境を整備してきた。現在のPC，サーバ及びネットワーク（以下，OAシステムという）の構成を図1に示す。

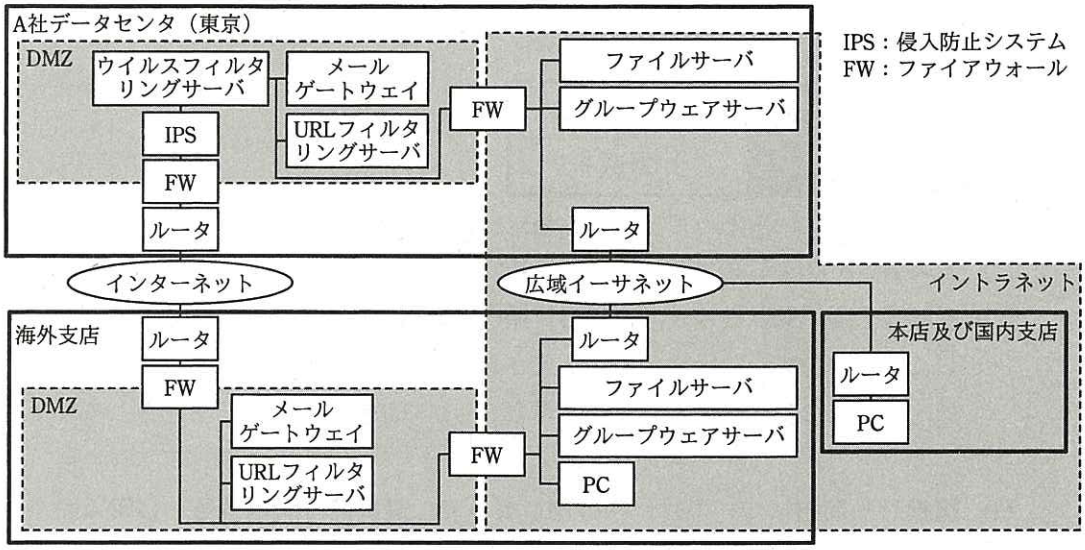

図1　現在のOAシステムの構成

PCには，クライアントアプリケーションソフトウェア（以下，クライアントアプリケーションという）としてWebブラウザ，グループウェアクライアント，オフィスソフトウェア及びPDFリーダが導入されている。グループウェアサーバは，メールサーバの機能ももっている。利用者は，グループウェアクライアントを利用して情報共有及びメールの送受信を行うことができる。ウイルスフィルタリングサーバは，HTTP通信及びSMTP通信においてファイルのウイルススキャンを行い，ウイルスが検出された場合は，直ちに当該通信を遮断し，ファイルを送受信した従業員と情報システム部の管理者に警告メッセージを送信する。URLフィルタリングサーバは，業務上必要がないWebサイトへのアクセスを禁止する。

A社は，情報システムのセキュリティ管理の強化及びコストの削減のために，本店及び全支店のPCをシンクライアント（以下，TCという）端末に段階的に移行し，A社データセンタ（東京）内にサーバを集約することにした。

〔マルウェア対策の要件〕

TC端末への移行及びサーバの集約に当たり，情報セキュリティ管理部は，情報システム部に対して，近年重大な脅威となっているマルウェア感染による情報漏えいについて対策を求めた。情報セキュリティ管理部が想定した，マルウェアによる情報漏えいのシナリオは次のとおりである。

(1) 計画立案段階

・攻撃者が，A社従業員のメールアドレス，職場関連の情報を収集する。

(2) 攻撃準備段階

・攻撃者が，収集した情報を差出人やメール件名に使って，従業員がだまされやすい文面のメールを作成する。

・攻撃者が，C&C（Command and Control）サーバを準備する。

(3) 初期潜入段階

・攻撃者が，メールを従業員に送信する。

・メールの添付ファイル又は本文中のURLを従業員に開かせることによって，マルウェアを実行させる。

(4) 基盤構築段階

・マルウェアが，C&CサーバのIPアドレスを用いて，C&Cサーバとの通信を開始する。

(5) 目的遂行段階

・マルウェアが，ファイルサーバ又はグループウェアサーバから機密情報を含んだファイル（以下，機密ファイルという）を盗み出す。

・マルウェアが，盗み出した機密ファイルをC&Cサーバから指示されたインターネット上のサーバに送信する。

情報セキュリティ管理部は，マルウェアによってファイルサーバとグループウェ

アサーバ上の機密ファイルが，インターネット上のサーバに送信されることを防ぐために，情報漏えいのシナリオを踏まえた次の対策を新しいOAシステムの要件とした。

(1) マルウェア感染対策（初期潜入段階に対する対策）

要件1. PC及び各サーバにおいてウイルス対策ソフトを利用する。

要件2. ウイルスフィルタリングサーバによって，受信メールの添付ファイル及びWebサイトからダウンロードしたファイルに対するウイルススキャンを行う。

(2) マルウェア感染後の情報漏えい対策（基盤構築段階及び目的遂行段階に対する対策）

要件3. 認証プロキシサーバを新設し，利用者IDとパスワードによる利用者認証及びアクセスログの取得を行う。インターネット上のWebサイトへのアクセスは，必ず認証プロキシサーバを経由させる。

要件4. 基盤構築段階及び目的遂行段階で利用される通信を禁止する。

情報システム部のZ部長は，部下のYさんに，要件1～4を考慮したOAシステムの設計を行い，情報セキュリティ管理部のレビューを受けるよう指示した。

〔新しいOAシステムの設計〕

Yさんは，新しいOAシステムの設計案（以下，設計案1という）を作成した。設計案1の構成を図2に，設計案1における通信を表1に，それぞれ示す。

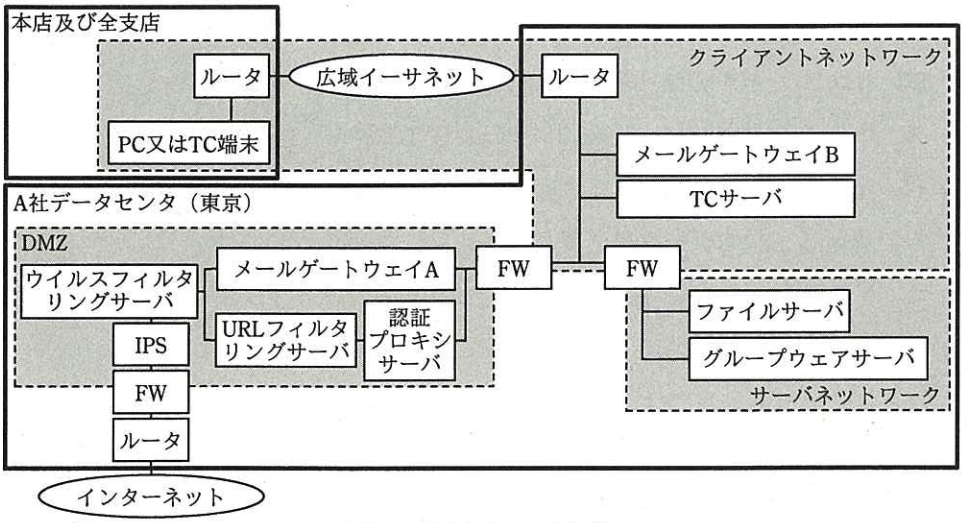

図２　設計案１の構成

表１　設計案１における通信

項番	送信元	宛先	プロトコル
1	PC 又は TC 端末	TC サーバ	TC サーバ製品の独自プロトコル
2	TC サーバ	ファイルサーバ	Windows ファイル共有プロトコル
3	TC サーバ	グループウェアサーバ	グループウェア独自プロトコル
4	グループウェアサーバ	メールゲートウェイ B	SMTP
5	メールゲートウェイ B	メールゲートウェイ A	SMTP
6	メールゲートウェイ A	インターネット上のメールサーバ	SMTP
7	インターネット上のメールサーバ	メールゲートウェイ A	SMTP
8	メールゲートウェイ A	メールゲートウェイ B	SMTP
9	メールゲートウェイ B	グループウェアサーバ	SMTP
10	TC サーバ	認証プロキシサーバ	HTTP 及び HTTP over TLS（以下，HTTPS という）
11	認証プロキシサーバ	インターネット上の Web サーバ	HTTP 及び HTTPS

注記１　DNS 及び Windows のディレクトリサービスの通信は，省略している。
注記２　表及び注記１に記載のない通信は FW によって禁止されている。
注記３　FW，ルータなど TCP コネクションを終端しない機器は送信元及び宛先として記載していない。

設計案１の概要は，次のとおりである。

・ネットワークを複数のネットワークに分け，FW でネットワーク間の通信を制限する。

・TC には，OS 及びクライアントアプリケーションを複数の利用者で共有する，画面転送型又はサーバベース方式と呼ばれる方式を採用する。

・TC サーバの OS 上で，クライアントアプリケーションが稼働する。
・PC にはビューア（TC 端末の機能を提供するソフトウェア）を導入するが，その後，本店及び支店ごとに段階的に PC から TC 端末へ移行する。
・TC 端末及びビューアから TC サーバまでの間は，TC サーバ製品独自のプロトコルで通信し，次のデータを送受信する。
  - デスクトップ及び TC サーバ上で動作するクライアントアプリケーションの画面
  - キーボード，マウスの操作情報
・認証プロキシサーバは，利用者 ID とパスワードによる利用者認証を行う。次のいずれかの利用者認証の方式を選択できるが，方式 2 を選択する。
  方式 1. 利用者が Web ブラウザを起動するたびに認証する。
  方式 2. 認証が成功すると，設定された時間が経過するまでは，クライアントの IP アドレスによって認証済みの利用者とみなす。

新しい OA システムは，次のように動作する。
・TC 端末又はビューアを起動して TC サーバにログオンすると，TC サーバが提供するデスクトップが表示される。デスクトップには，各クライアントアプリケーションを起動するためのアイコンがある。
・アイコンをクリックすると，クライアントアプリケーションが TC サーバの OS 上の一つのプロセスとして起動する。TC サーバには，仮想 IP アドレスプール（クライアントアプリケーションのプロセスが利用する仮想 IP アドレスの範囲）が定義されている。クライアントアプリケーションのプロセスは，仮想 IP アドレスプールの中から他のプロセスで利用されていない仮想 IP アドレスを一つ選択して利用する。クライアントアプリケーションのプロセスが終了すると，当該プロセスで利用されていた仮想 IP アドレスは解放され，他のプロセスが起動したときに再利用される。
・グループウェアクライアントの画面で受信メールの添付ファイルのアイコンをクリックすると，当該ファイルが開かれる。このとき，グループウェアクライアントは，グループウェアクライアントの実行環境である TC サーバの作業フォルダに，グループウェアサーバから添付ファイルをダウンロードし，OS の設定でファイル

タイプに関連付けられたクライアントアプリケーションを起動する。

・Web ブラウザ上でクリックしたリンクが，OS の設定でファイルタイプごとに関連付けられたインターネット上のファイルへのリンクであった場合，Web ブラウザは，インターネット上の Web サーバから Web ブラウザの実行環境である TC サーバ上の作業フォルダに当該ファイルをダウンロードし，該当するクライアントアプリケーションを起動する。

・各従業員には，TC サーバの設定によって，ファイルサーバのフォルダが一つずつ割り当てられている。クライアントアプリケーションの画面からファイル保存の操作を行うと，保存先を選択する画面に D ドライブとしてそのフォルダが表示される。D ドライブを保存先に選択すると，当該ファイルが，クライアントアプリケーションが稼働している TC サーバからファイルサーバに転送される。

〔マルウェア対策を考慮した修正〕

Y さんが設計案 1 について情報セキュリティ管理部のレビューを受けたところ，次の 3 点が指摘された。

指摘 1. 要件 2 のウイルススキャンが行われない場合がある。要件 2 を満たすように対策を強化する必要がある。

指摘 2. 要件 3 の認証プロキシサーバの方式選択について，方式 2 では要件 3 を満たせない。方式 1 を選択すべきである。

指摘 3. FW 及び IPS による通信の制限だけでは要件 4 を満たしていない。対策を追加する必要がある。

Y さんは，情報セキュリティ管理部の指摘を反映した修正案（以下，設計案 2 という）を作成し，情報セキュリティ管理部と Z 部長の承認を得た。設計案 2 では，TC サーバを，用途によってオフィス環境用 TC サーバ（以下，OA 用 TC サーバという）とインターネットアクセス用 TC サーバ（以下，IA 用 TC サーバという）に分けている。また，本店及び全支店でのメールによるファイル送信及びインターネット上の Web サイトへのファイルアップロードを，情報漏えい防止サーバ（以下，DLP サーバという）を使って制限する対策を追加している。DLP サーバの仕組みは次のとおりである。

・HTTP 通信及び SMTP 通信でインターネットに送信されるファイルに，住所，氏名，電話番号又は機密，個人情報などの区分を示す文字列が含まれていないかを検査する。

・機密や個人情報に該当すると判断した場合は，通信を遮断し，ファイル送信を行った従業員と情報システム部の管理者に警告メッセージを送る。

設計案 2 の構成を図 3 に，設計案 2 における通信を表 2 に，それぞれ示す。

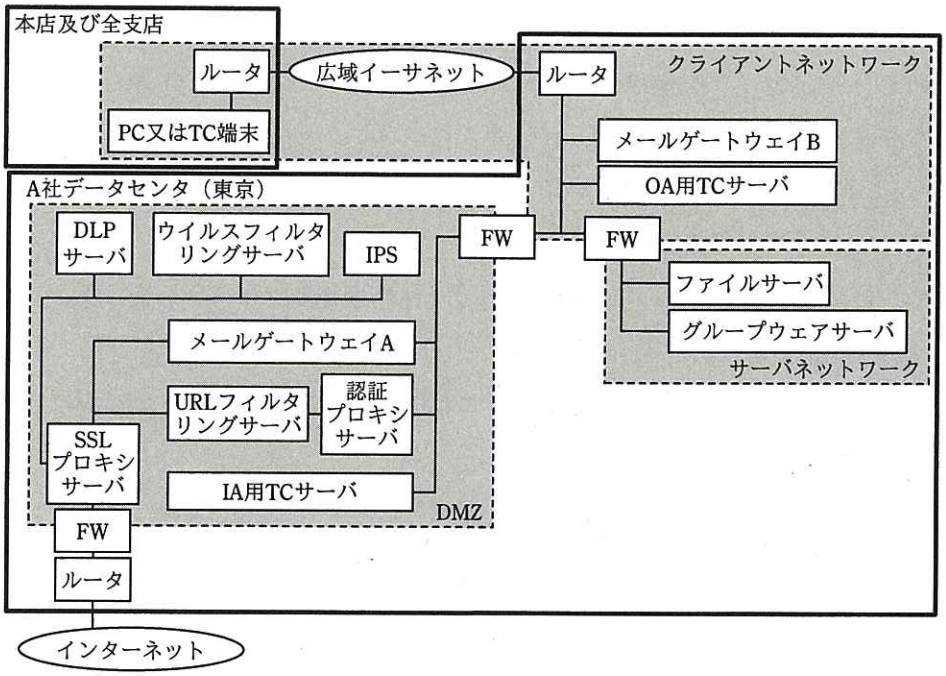

図 3　設計案 2 の構成

表2　設計案2における通信

項番	送信元	宛先	プロトコル
1	PC又はTC端末	OA用TCサーバ	TCサーバ製品の独自プロトコル
2	OA用TCサーバ	ファイルサーバ	Windowsファイル共有プロトコル
3	OA用TCサーバ	グループウェアサーバ	グループウェア独自プロトコル
4	グループウェアサーバ	メールゲートウェイB	SMTP
5	メールゲートウェイB	メールゲートウェイA	SMTP
6	メールゲートウェイA	インターネット上のメールサーバ	SMTP
7	インターネット上のメールサーバ	メールゲートウェイA	SMTP
8	メールゲートウェイA	メールゲートウェイB	SMTP
9	メールゲートウェイB	グループウェアサーバ	SMTP
10	PC又はTC端末	IA用TCサーバ	TCサーバ製品の独自プロトコル
11	IA用TCサーバ	認証プロキシサーバ	HTTP及びHTTPS
12	認証プロキシサーバ	SSLプロキシサーバ	HTTP及びHTTPS
13	SSLプロキシサーバ	インターネット上のWebサーバ	HTTP及びHTTPS

注記1　DNS及びWindowsのディレクトリサービスの通信は省略している。
注記2　表及び注記1に記載のない通信はFWによって禁止されている。
注記3　FW，ルータなどTCPコネクションを終端しない機器は送信元及び宛先として記載していない。

設計案2において，利用者が受信メール中のURLをクリックした場合，OA用TCサーバ上でWebブラウザが起動されるが，当該URLへのアクセスは失敗する。OA用TCサーバ及びIA用TCサーバの作業フォルダ中のファイルは，定期的に削除される。SSLプロキシサーバは，HTTPS通信の復号及び再暗号化に用いられる。

〔業務要件を踏まえた再修正〕

A社は，一部の国内支店において新しいOAシステムの試行運用を開始した。試行運用は成功し，A社は新しいOAシステムを本店及び全支店に展開することを決めた。展開に先立ち，情報システム部が本店及び全支店に新しいOAシステムについて説明したところ，海外支店Xから，他の金融機関との共同融資業務及び幹事業務のために，PC及び支店固有のインターネット接続回線を継続利用したいという要望が上がった。その業務とは，オンラインストレージとメールを使って，複数の金融機関との間で，融資案件の情報を共有し，参加する金融機関の募集を行うというものである。業務の具体的な内容は次のとおりである。

(1) 共同融資業務

a. 融資案件の幹事の金融機関から，融資案件に対する融資依頼のメールが送られ

てくる。オンラインストレージ上には当該融資案件に関するファイル（以下，案件ファイルという）が置かれており，メールにそれら案件ファイルのリストを含むページの URL が含まれている。

b. 融資依頼のメール中の URL をクリックしてリストにアクセスする。

c. リストから案件ファイルを選択し，ファイルサーバにダウンロードする。

d. 融資案件に融資する場合，幹事の金融機関に対して，返信メールで，参加表明と融資額を連絡する。

(2) 幹事業務

e. オフィスソフトウェアを使って案件ファイルを作成し，ファイルサーバに保存する。

f. ファイルサーバからオンラインストレージに案件ファイルをアップロードする。

g. 他の金融機関宛ての融資依頼のメールを作成し，オンラインストレージ上の案件ファイルのリストを含むページの URL を，Web ブラウザの画面からメール中にコピーして貼り付ける。

h. 融資依頼のメールを送信する。

1 融資案件当たりの案件ファイルの合計サイズは，最大 500 M バイトである。海外支店 X では，業務の最繁時間帯の 9:00～10:00 の間，100 名の従業員が，1 名当たり最大 3 件の共同融資業務を行っており，この業務スピードを維持する必要がある。融資案件への融資会社募集は，必要な資金が集まった時点で打ち切られ，幹事の金融機関によって融資先及び融資元との間の契約手続が開始されることから，利益率，リスクが好条件の案件ほど参加表明と融資額を早く連絡する必要がある。幹事業務は，9:00～10:00 の間は行われない。

Y さんは，マルウェア対策に加えて海外支店 X において他の金融機関との共同融資業務及び幹事業務を可能にする修正案（以下，設計案 3 という）を作成した。設計案 3 では，海外支店 X 専用に，ファイルサーバ及び TC サーバが追加されている。

設計案 3 の構成を図 4 に，設計案 3 における通信を表 3 に，それぞれ示す。

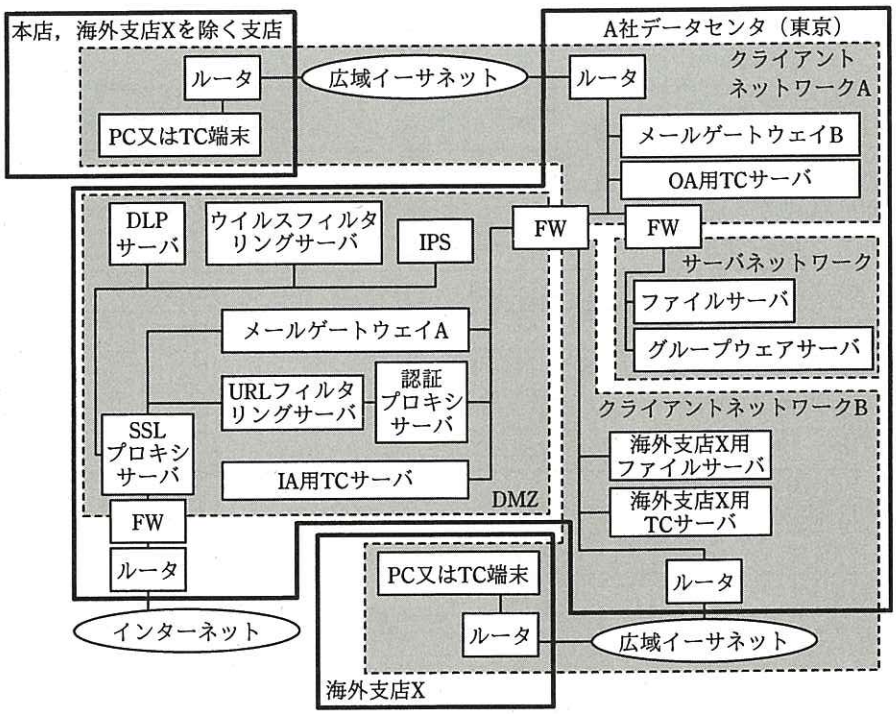
本店，海外支店Xを除く支店
ルータ
広域イーサネット
PC又はTC端末
A社データセンタ（東京）
ルータ
クライアント
ネットワークA
メールゲートウェイB
OA用TCサーバ
DLP
サーバ
ウイルスフィルタ
リングサーバ
IPS
FW
FW
サーバネットワーク
ファイルサーバ
グループウェアサーバ
メールゲートウェイA
URLフィルタ
リングサーバ
認証
プロキシ
サーバ
SSL
プロキシ
サーバ
IA用TCサーバ
DMZ
クライアントネットワークB
海外支店X用
ファイルサーバ
海外支店X用
TCサーバ
FW
ルータ
PC又はTC端末
ルータ
インターネット
ルータ
広域イーサネット
海外支店X

図 4　設計案 3 の構成

表3　設計案3における通信

項番	送信元	宛先	プロトコル
1	PC又はTC端末 （本店，海外支店Xを除く支店）	OA用TCサーバ	TCサーバ製品の独自プロトコル
2	OA用TCサーバ	ファイルサーバ	Windowsファイル共有プロトコル
3	OA用TCサーバ	グループウェアサーバ	グループウェア独自プロトコル
4	グループウェアサーバ	メールゲートウェイB	SMTP
5	メールゲートウェイB	メールゲートウェイA	SMTP
6	メールゲートウェイA	インターネット上のメールサーバ	SMTP
7	インターネット上のメールサーバ	メールゲートウェイA	SMTP
8	メールゲートウェイA	メールゲートウェイB	SMTP
9	メールゲートウェイB	グループウェアサーバ	SMTP
10	PC又はTC端末 (本店，海外支店Xを除く支店)	IA用TCサーバ	TCサーバ製品の独自プロトコル
11	IA用TCサーバ	認証プロキシサーバ	HTTP及びHTTPS
12	認証プロキシサーバ	SSLプロキシサーバ	HTTP及びHTTPS
13	SSLプロキシサーバ	インターネット上のWebサーバ	HTTP及びHTTPS
14	PC又はTC端末(海外支店X)	海外支店X用TCサーバ	TCサーバ製品の独自プロトコル
15	海外支店X用TCサーバ	海外支店X用ファイルサーバ	Windowsファイル共有プロトコル
16	海外支店X用TCサーバ	グループウェアサーバ	グループウェア独自プロトコル
17	海外支店X用TCサーバ	認証プロキシサーバ	HTTP及びHTTPS

注記1　DNS及びWindowsのディレクトリサービスの通信は省略している。
注記2　表及び注記1に記載のない通信はFWによって禁止されている。
注記3　FW，ルータなどTCPコネクションを終端しない機器は送信元及び宛先として記載していない。

〔パフォーマンス検証〕

Yさんは，設計案3について，情報セキュリティ管理部とZ部長の承認を得た後，海外支店Xに対して説明会を開いた。海外支店Xは，設計案3が共同融資業務での業務スピード維持に必要なパフォーマンス要件を満たせるのかどうかについて検証を求めた。

Yさんが試算したところ，パフォーマンス要件を満たすには，インターネット接続回線の帯域幅を確保するために大きなコストが必要になることが判明した。Yさんは，海外支店Xについては例外的に，TC端末に移行せずに，システム運用とセキュリティ管理も含めてPC及び支店固有のインターネット接続回線を図1の現状のまま継続利用せざるを得ないと結論付けた。Yさんは，設計案3を更に修正した設計案（以下，設計案4という）を作成し，その内容と修正理由を情報セキュリティ管理部とZ部長に説明した。設計案4の構成を図5に示す。

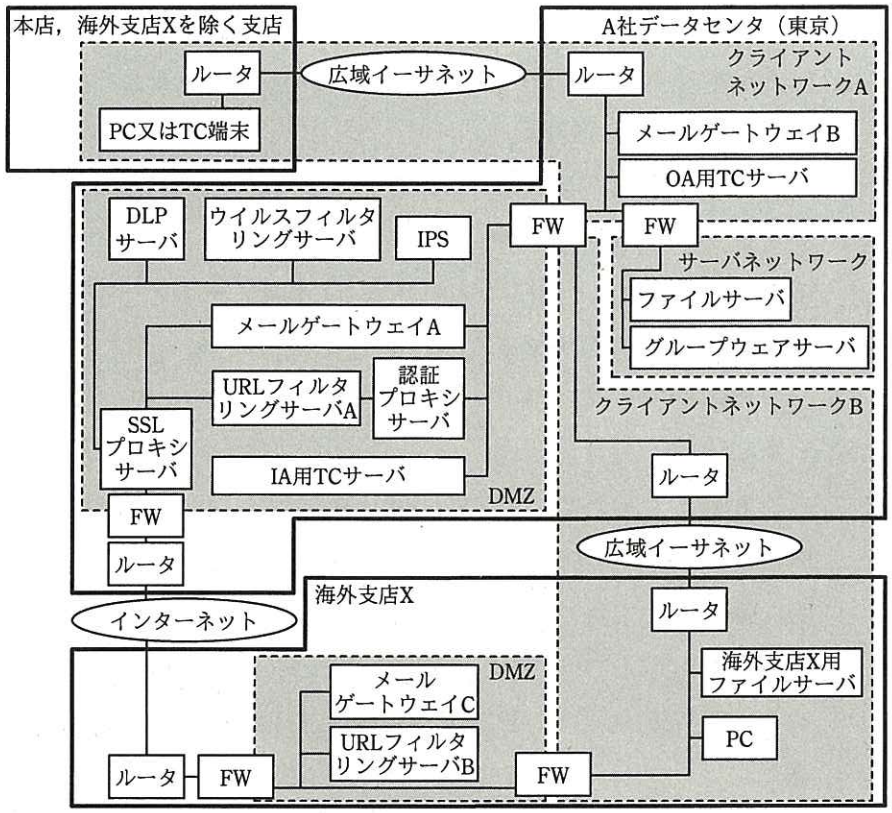

図 5　設計案 4 の構成

情報セキュリティ管理部と Z 部長は，海外支店 X のインターネット接続におけるセキュリティ対策について，次の二つを条件として，設計案 4 を承認した。

・①他の支店と同等の技術的対策を行うこと

・新しい OA システムは，国内，海外ともに情報システム部が構築，運用及びセキュリティ管理を行い，情報セキュリティ管理部がセキュリティ管理状況を定期的に監査すること

A 社は，条件を満たすように見直した設計案 4 に基づき，新しい OA システムの本格運用を開始した。

設問1　〔新しいOAシステムの設計〕について，(1)，(2)に答えよ。

(1) 設計案 1 について，次の(a)～(c)の場面で利用される全ての通信を，それぞれ表1中の項番で答えよ。

(a) 本店の TC 端末を利用して，グループウェアサーバ上のファイルをファイルサーバに転送する。

(b) インターネットから A 社にメールが届き，そのメールを国内支店の TC 端末を利用して閲覧する。

(c) 海外支店の PC を利用して，インターネット上の Web サイトにアクセスする。

(2) 設計案 1 において，受信メールの添付ファイルを海外支店の TC 端末から開いてマルウェアに感染した場合，マルウェアはどの構成要素上で動作するか。図 2 中の用語で答えよ。また，その後，マルウェアがファイルサーバ上のファイル及びグループウェアサーバ上のファイルを盗み出してインターネット上の Web サーバに送信するのに利用する全ての通信を，表 1 中の項番で答えよ。

設問2　〔マルウェア対策を考慮した修正〕について，(1)～(5)に答えよ。

(1) 指摘 1 について，ウイルススキャンが行われないのはどのような場合か。二つ挙げ，それぞれ25字以内で述べよ。

(2) 指摘 2 について，方式 2 が要件を満たせない理由を，技術的要因を含めて75字以内で述べよ。

(3) 設計案 2 において，利用者がインターネット上の Web サイトのファイルを閲覧してマルウェア感染が起きた場合，マルウェアはどの構成要素上で動作するか。図3中の用語で答えよ。

(4) 設計案 2 において，利用者が受信メールの添付ファイルを開いてマルウェア感染が起きた場合，マルウェアはどの構成要素上で動作するか。図 3 中の用語で答えよ。

(5) 設計案 2 におけるマルウェア対策について，目的遂行段階でマルウェアが利用する二つの通信のうち，FW によって禁止されているのはどの通信か。マルウェアの実行がインターネット上の Web サイトのファイルを閲覧して起きた場合，及び受信メールの添付ファイルを開いて起きた場合のそれぞれにつ

いて，送信元，宛先及びプロトコルを答えよ。

設問3　〔業務要件を踏まえた再修正〕について，(1)，(2)に答えよ。

(1)　海外支店 X の共同融資業務及び幹事業務のうち，設計案 2 では実現できない項目を全て挙げ，本文中の a～h の記号で答えよ。

(2)　設計案 3 において，海外支店 X の PC からインターネット上の Web サイトのファイルを閲覧してマルウェアに感染した場合，及び受信メールの添付ファイルを開いてマルウェアに感染した場合，それぞれマルウェアはどの構成要素上で動作するか。図 4 中の用語で答えよ。

設問4　〔パフォーマンス検証〕について，(1)，(2)に答えよ。

(1)　パフォーマンス要件を満たすために必要な回線速度は何 M ビット／秒か。小数第 1 位を四捨五入して整数で答えよ。ここで，回線使用率は 70%とする。また，1M バイト=10^6 バイト，1M ビット／秒=10^6 ビット／秒とし，制御データ及びエラーによる再送については，回線使用率の前提条件で考慮されているものとする。

(2)　本文中の下線①を実現するために，図 5 中の海外支店 X の DMZ に追加すべき構成要素を解答群の中から全て選び，記号で答えよ。

解答群

ア　DLP サーバ	イ　IA 用 TC サーバ
ウ　IPS	エ　OA 用 TC サーバ
オ　SSL プロキシサーバ	カ　TC サーバ
キ　ウイルスフィルタリングサーバ	ク　認証プロキシサーバ

設問5　設計案 4 において，監査とセキュリティ管理の役割を一つの組織にもたせた場合，どのような不都合が起こるか。30 字以内で述べよ。