問1　インターネット向けサーバの災害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 3,000 名の医薬品卸売会社である。東京に本社があり，大阪に関西地域本社がある。支社は，東京と大阪を含めた 7 都市にある。12 か所に物流センタ（以下，LC という）を置き，60 か所に営業所を置く。本社には，企画部，人事総務部，財務部及び情報システム部がある。関西地域本社には，営業本部，物流本部，人事総務部分室及び情報システム部分室がある。各支社には，営業部及び物流部がある。

〔A 社の情報システムの概要〕

A 社の情報システムには，営業システム，物流システム，人事総務システム及び財務システムに加えて，電子メール（以下，メールという）サーバ，プロキシサーバなどで構成されているインターネット接続システム（以下，I システムという）がある。営業システム及び物流システムは関西 LC に設置されている。人事総務システム，財務システム及び I システムは関東 LC に設置されている。営業システムは，社外の電子取引システム（以下，M-EDI という）と連携している。

営業システム，物流システム，人事総務システム及び財務システムのサービス提供時間は，営業日の 8～20 時である。営業日は，年末年始を除く平日である。I システム及び社内ネットワーク設備のサービス提供時間は，24 時間 365 日であるが，日曜日は保守のため停止することがある。

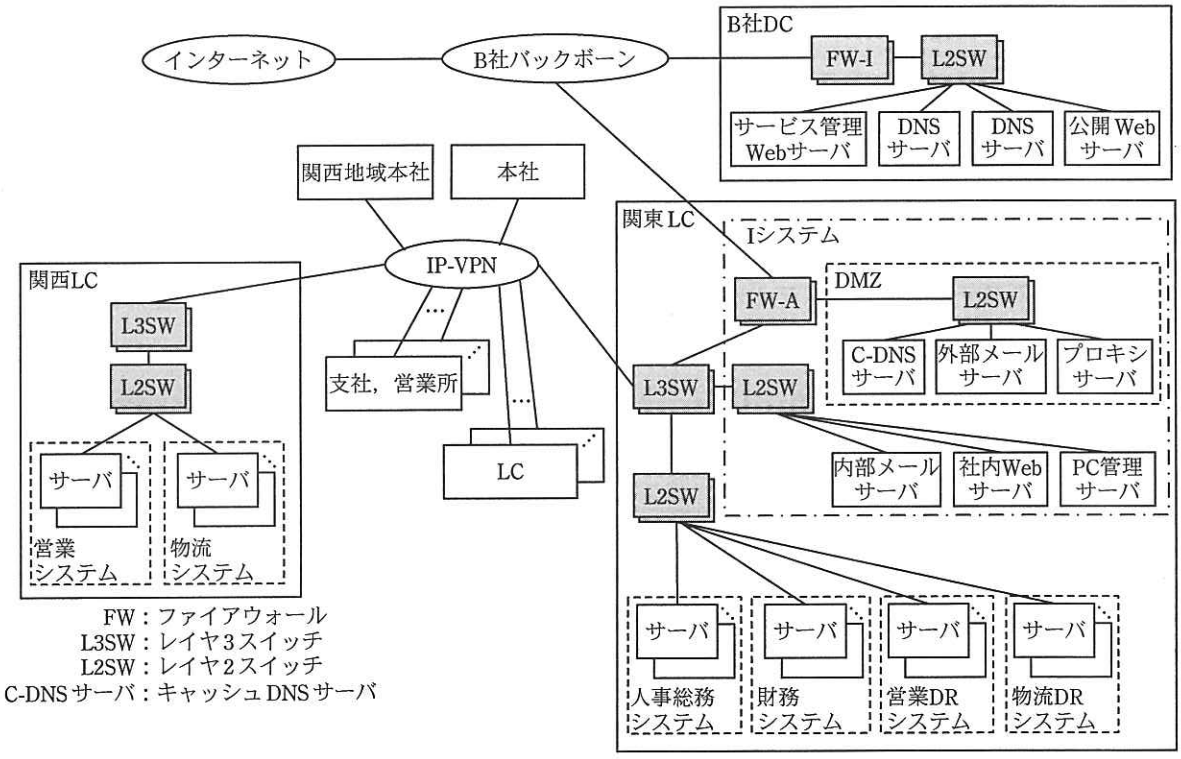
全ての従業員に 1 台ずつ PC を貸与している。事業所からの PC の持出しは禁止されているが，従業員が A 社の他の事業所へ出張している時，出張先で他の従業員の PC を借用して情報システムを利用することができる。

A 社では，災害対策を目的として，情報システムの再構築を行ったばかりである。情報システムの再構築では，12 か所ある LC のうち関東 LC 及び関西 LC を重要拠点と位置付け，自家発電設備を導入した。災害時でも注文受付と物流が続けられるよう，営業システムの災害時用のバックアップとして営業 DR システムを，物流システムの災害時用のバックアップとして物流 DR システムを，それぞれ関東 LC に設置した。平常時，営業システムと営業 DR システムとのデータの同期及び物流システムと物流 DR システムとのデータの同期を行うことにした。さらに，M-EDI が使用できない場

合は，メールで注文受付を行うことにし，それらを踏まえた災害時の注文受付運用手順を作成した。

〔情報システムの構成〕

A 社では，DNS サーバ，公開 Web サーバなどの運用に，ISP の B 社が提供するデータセンタ（以下，B 社 DC という）を利用している。B 社 DC 及び A 社のネットワーク構成を図 1 に，I システムの機器と概要を表 1 に，B 社 DC の機器と概要を表 2 に示す。



注記 1　網掛けの機器はホットスタンバイ構成である。
注記 2　B 社バックボーン及び B 社 DC の機器には，B 社が高可用性対策及び災害対策を施している。
注記 3　PC は記載を省略している。

図 1　B 社 DC 及び A 社のネットワーク構成

表１　Ｉシステムの機器と概要

機器名称	概要
FW-A	フィルタリング機能：通信の送信元，宛先及びポート番号の組合せによって，通信の許可又は拒否を指定する。
C-DNS サーバ	DNS 機能：インターネット上のサーバの名前解決を行う。
外部メールサーバ	メール転送機能：インターネットと内部メールサーバの間でメールの転送を行う。 迷惑メール対策機能：メールの転送時に迷惑メールスキャンを行う。迷惑メール定義ファイルを迷惑メール対策ソフトのベンダの Web サーバから 1 時間ごとにダウンロードし，更新する。 DNS 機能：C-DNS サーバと同じ機能をもつ。
プロキシサーバ	プロキシ機能：PC からインターネット上の Web サーバへのアクセスを中継する。 キャッシュ機能：アクセスしたコンテンツを一時的に保管し，再利用することができる。 ウイルス対策機能：通信の中継時及びプログラムからのファイルアクセス時にウイルススキャンを行う。加えて，毎週月曜日の 3 時から全てのファイルのウイルススキャン（以下，フルスキャンという）を行う。ウイルス定義ファイルは，ウイルス対策ソフトのベンダの Web サーバから 15 分ごとにダウンロードし，更新する。 コンテンツフィルタリング機能：通信の中継において，フィルタリングを行う。フィルタリング定義ファイルは，フィルタリングソフトのベンダの Web サーバから 15 分ごとにダウンロードし，更新する。情報システム部と情報システム部分室の担当者が，フィルタリングする Web サーバの追加及び削除，フィルタリングするファイル種別の追加及び削除，並びにフィルタリングするキーワードの追加及び削除を行い，設定パターンとして保存することができる。
内部メールサーバ	利用者向け機能：PC によるメール送受信は，メールソフトではなくブラウザを通じて行う（以下，Web メールという）。利用者は，メールを選択してダウンロード及びアップロードすることができる。メールボックスは一つの利用者 ID につき 500M バイトである。平日の 3 時に，500M バイトを超えたメールボックスに対して，500M バイト以下になるように古いメールから順に削除処理を行う。 メール転送機能：外部メールサーバとの間でメールの転送を行う。 ウイルス対策機能：メールの転送時及びプログラムからのファイルアクセス時にウイルススキャンを行う。加えて，毎週月曜日の 3 時からフルスキャンを行う。ウイルス定義ファイルは PC 管理サーバから 15 分ごとに転送し，更新する。
社内 Web サーバ	社内通達を掲示する。全社通達の登録は，人事総務部の担当者が行う。各部門内の通達の登録は，各部門の担当者が行う。
PC 管理サーバ	OS 管理機能：PC の OS の更新プログラムについて，配布と適用状況の収集を行う。 ウイルス対策管理機能：PC 及び内部メールサーバへのウイルス定義ファイルの配布，PC の起動後に自動的に実施されるフルスキャンの結果，並びに PC のウイルス対策ソフトがウイルス検出時に送信する情報の管理を行う。ウイルス定義ファイルは，プロキシサーバを経由して，ウイルス対策ソフトのベンダの Web サーバから 15 分ごとにダウンロードし，更新する。

表2　B社DCの機器と概要

機器名称	概要
FW-I	フィルタリング機能：通信の送信元，宛先及びポート番号の組合せによって，通信の許可又は拒否を指定する。FW-Iのフィルタリングルールの設定はA社からの依頼に基づきB社が行う。
サービス管理Webサーバ	B社DCの設定用のWebサーバであり，DNSサーバの設定及び公開Webサーバのコンテンツ管理を行う。サービス管理WebサーバとPCのブラウザの間は暗号化のために［　a　］通信を使用している。FW-Iのフィルタリングルールの設定によって，送信元はプロキシサーバに限定している。A社情報システム部の担当者が使用する。
DNSサーバ	DNS機能：A社のドメイン名の情報を提供する。メール送信ドメイン認証技術の一つであるSPF（Sender Policy Framework）のレコードも設定している。
公開Webサーバ	A社の公開企業情報や医療従事者向け情報を提供する。

各ファイアウォールでは，通信の許可と拒否の状況をログとして記録している。各サーバでは，サーバへのアクセス及びプログラムの動作の状況をログとして記録している。

〔情報システムの運用〕

関東LCの機器の運用は情報システム部が行っている。関西LCの機器の運用は，情報システム部分室が行っている。両LCとも機器の起動，停止及び設定変更は，遠隔操作で行っている。設定変更時には機器のセキュリティに関する設定を行うこともあるので，遠隔操作には通信の暗号化が必要であり，TELNETやFTPではなく［　b　］を用いている。

〔地震発生とその影響〕

情報システムの再構築から半年後，月曜日の午前中に関東地方で強い地震が発生した。A社では，関東地区の一部の営業所と関東LCが被害を受け，業務遂行に支障が出た。直ちに，本社に災害対策本部を設置し，被害を受けた営業所と関東LCの復旧を行った。復旧のめどがついた1か月後，A社の経営会議は，今回の地震で起きた災害対策の問題点をまとめることを決めた。その決定を受けて，人事総務部長は，社内各部門に災害復旧対応と地震発生時の状況をヒアリングするよう，担当部員に指示した。担当部員がヒアリングした結果を図2に示す。

1. 災害復旧対応の状況
(省略)
2. 地震発生時の状況
(1) 被害を受けた地区の交通
ア 地震発生直後から翌日にかけて，被害を受けた営業所と関東 LC の周辺では鉄道とバスが運休した。
イ 地震発生直後から翌日にかけて，被害を受けた営業所と関東 LC の周辺では道路が渋滞した。
(2) 通信
ア 加入電話や携帯電話は通話規制のため，使用できない時間帯があった。
イ インターネットのメールの配送は最大 1 時間の遅れがあったものの，連絡手段として使用できた。
(3) 被害を受けた地区の注文受付
ア 一部の顧客で通信回線障害が発生し，M-EDI による注文ができなかった。
イ M-EDI の代替として営業所の担当者は，メールでの注文受付を行った。
(4) A 社の LC 及び B 社 DC の状況について
ア 関東 LC は次の状況であった。
・地震発生直後，停電が発生し，自家発電設備によって対応した。復電は 22 時間後であった。
・地震発生当日及び翌日は，関東 LC と B 社バックボーンを結ぶ回線の使用率がほぼ 100%となり，社内からインターネット上の Web サーバへのアクセスは困難であった。プロキシサーバのログを調査した結果，交通情報やニュースを提供している Web サーバへのアクセスが大多数であった。中でもニュース動画(ふくそう)へのアクセスが多く，プロキシサーバのキャッシュ機能は使用していたが，ネットワークの輻輳を防げず，メール配送の遅れの原因にもなったことが判明した。
・地震発生から 1 週間後，内部メールサーバのフルスキャンで同じウイルス（以下，X ウイルスという）を複数検出した。ベンダによれば，地震情報提供に見せかけた添付ファイル付きメールがあり，その添付ファイルを開くことでウイルスに感染するとのことであった。
イ 関東 LC 以外の LC には地震の影響はなかった。
ウ B 社 DC は次の状況であった。
・地震発生当日及び翌日は，公開 Web サーバへのアクセス数が平常時の 5 倍程度となり，応答が遅くなった。

図 2 ヒアリング結果

人事総務部長は，災害対策本部長及び全社の部長を集め，図 2 のヒアリング結果を報告し，対応策を検討した。議論の結果，次のとおりとなった。

・災害時，メールによる注文受付に切り替えても，停電が長時間になると営業業務と物流業務は継続できない可能性がある。それぞれの業務を継続するために，翌営業日の午前 8 時までに I システムを稼働できるようにする。

・X ウイルスのような，災害情報提供に見せかけた添付ファイル付きメールによって広まるウイルスへの対処が必要なので，X ウイルスに関する対処の経過と，そこから得られる知見をまとめる。

人事総務部長は，X ウイルスに関する対処の経過の報告を情報システム部の D 部長

に依頼するとともに，ヒアリング結果とそれに関する災害対策本部長及び全社の部長との議論の結果を経営会議で報告した。経営会議において，M-EDI 使用不能時の代替としてのＩシステムの重要性が認識された。

〔Ｘウイルスに関する対処の経過〕

Ｄ部長は，情報セキュリティ担当のＥ主任とＦさんに，Ｘウイルスに関する対処の経過をまとめるように指示した。Ｅ主任とＦさんは，図３に示すＸウイルスに関する対処の経過をＤ部長に報告した。

1. Ｘウイルス検出までの経過
   (1) 内部メールサーバのフルスキャンでＸウイルスが検出されたメールは，全て水曜日の１時から２時の間に内部メールサーバに届いた。
   (2) PC 管理サーバでは，金曜日の 20 時にウイルス定義ファイルをＸウイルスに対応したものに更新した。
   (3) 月曜日の３時に，内部メールサーバにおけるフルスキャンでＸウイルスを検出し，削除した。
2. Ｘウイルス検出後の措置
   (1) ウイルス対策ソフトのベンダへの照会結果
   - 画像を装ったファイルとしてメールに添付されている。
   - ファイルが開かれると，PC の画像閲覧プログラムの脆弱（ぜい）性を悪用し，感染する。脆弱性修正プログラムは，本資料作成時点ではリリースされていない。
   - 攻撃者が用意した複数の特定の Web サーバ（以下，特定 Web サーバという）と通信を行う。
   - 特定 Web サーバの IP アドレスのリストがＸウイルス内に定義されている。
   - 特定 Web サーバとの通信の際，ブラウザの設定情報を使うこともある。
   - 駆除には，専用のツールが必要である。
   (2) Ｉシステムのウイルス検査と対処
   - 一斉ウイルス検査を行うため，ウイルス検査開始時に PC 管理サーバに最新のウイルス定義ファイルを置き，各 PC のウイルス定義ファイルの更新とフルスキャンの実施を全従業員に依頼した。
   - FW-A と [c] のログを調査したところ，Ｘウイルスの活動がなかったことが確認できた。
   - PC 管理サーバのログを調査したところ，①フルスキャンの実施を確認できない PC が複数台あったので，その PC の利用者に実施を再度依頼した。再度の依頼から２週間後，フルスキャンが実施されたこととＸウイルスの感染がないことを確認した。

図３　Ｘウイルスに関する対処の経過

Ｄ部長は，内部メールサーバのフルスキャンでＸウイルスが検出されたメールボックスから利用者を調べれば，万が一ウイルスに感染した PC があったとしても，それをより早く特定して，対処を完了できるのではないかと指摘した。Ｅ主任は，Ｄ部長が指摘した調査方法では，②Web メールの性質上，ウイルスに感染した PC を特定できないことを説明した。Ｄ部長はＸウイルスに関する対処の経過を確認し，人事総務部長に伝えた。

〔I-DR システムの導入に関する検討〕

その後，経営会議において，関西 LC に I システムの災害時用のバックアップとして I-DR システムを導入することが決定された。I-DR システムの構築は情報システム部が担当することになり，D 部長は，E 主任に要件の検討を指示した。

〔I-DR システムに関する要件の検討〕

I-DR システムに関する要件の検討は，E 主任と F さん，情報システム部分室の G 主任から成る検討チームが行うことになった。業務の継続性の観点から，I-DR システムに関する要件を図 4 の（案）のように整理した。

(1) I-DR システムへの切替え
・I システムが使用不能になった場合，翌営業日の午前 8 時までに I-DR システムへの切替えが完了できること。
(2) I-DR システムから I システムへの復旧
・I システムの機能復旧を確認したら，営業日以外の日に I-DR システムから I システムへの切戻しが行えること。
(3) I-DR システムのメール機能
・内部メールサーバと同じメールアドレス，利用者 ID 及びパスワードを使用できること。
・既読及び未読の状態は引き継がなくてよい。
・少なくとも，切替えを行う日の前日の 22 時までに届いたメールを利用可能にすること。
・復旧後の一定期間（以下，並行運用期間という），I-DR システムのメールを参照できれば，I-DR システムから I システムへのメールボックスの復元を行わなくてよい。
(4) I-DR システムのメール以外の機能
・I システムと同じとする。
(5) I-DR システムのセキュリティ運用
・修正プログラムの適用及び設定変更は，常に最新の状態にする。

図 4　I-DR システムに関する要件（案）

検討チームは，I-DR システムに関する要件（案）を D 部長に報告し，承認を得た。続いて検討チームは，図 4 を基に，図 5 に示す B 社 DC 及び I-DR システムを含む A 社のネットワーク構成（案），並びに表 3 に示す I-DR システムの機器と概要（案）を作成した。

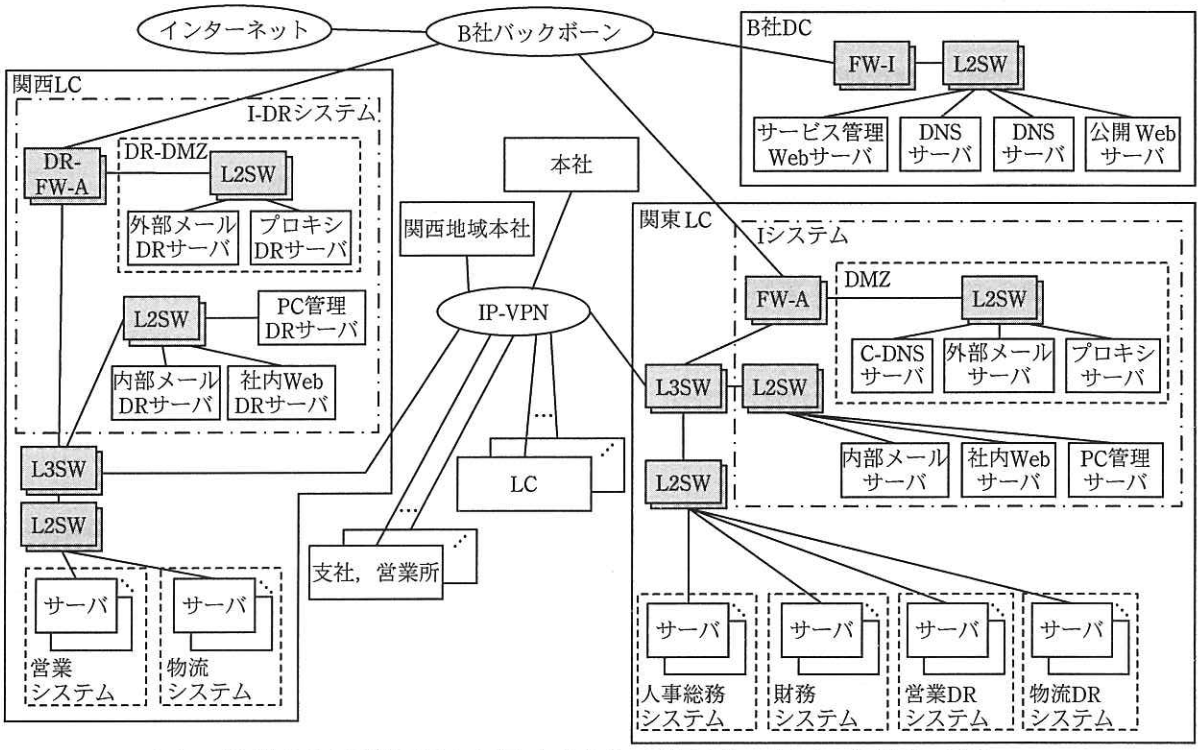


図５　B 社 DC 及び I-DR システムを含む A 社のネットワーク構成（案）

表３　I-DR システムの機器と概要（案）

機器名称	概要
DR-FW-A	FW-A と同じ機能をもつ。
外部メール DR サーバ	メール転送機能：インターネットと内部メール DR サーバの間でメールの転送を行う。 迷惑メール対策機能及び DNS 機能：外部メールサーバと同じ機能をもつ。
プロキシ DR サーバ	プロキシサーバと同じ機能及び C-DNS サーバと同じ機能をもつ。
内部メール DR サーバ	利用者向け機能：内部メールサーバと同じ機能をもつ。 メール転送機能：外部メール DR サーバとの間でメール転送を行う。 ウイルス対策機能：メールの転送時及びプログラムからのファイルアクセス時にウイルススキャンを行う。加えて，毎週月曜日の 3 時からフルスキャンを行う。ウイルス定義ファイルは PC 管理 DR サーバから 15 分ごとに転送し，更新する。
社内 Web DR サーバ	社内 Web サーバと同じ機能をもつ。
PC 管理 DR サーバ	OS 管理機能：PC 管理サーバと同じ機能をもつ。 ウイルス対策管理機能：PC 及び内部メール DR サーバへのウイルス定義ファイルの配布，PC の起動後に自動的に実施されるフルスキャンの結果，並びに PC のウイルス対策ソフトがウイルス検出時に送信する情報の管理を行う。ウイルス定義ファイルは，プロキシ DR サーバを経由して，ウイルス対策ソフトのベンダの Web サーバから 15 分ごとにダウンロードし，更新する。 情報同期機能：PC 管理サーバと情報を同期する。

注記　I システムとは機能が異なる箇所に下線を付す。

〔I-DR システムの方式設計〕

F さんが，I-DR システムの方式設計を行うことになった。まず，図 6 の I-DR システムのメールに関する方式設計（案）ができたので検討チームでレビューを行った。

(1) 外部メールサーバから外部メール DR サーバへの切替えについて
- 平常時は，DNS サーバの設定情報のうち MX レコード及び TXT レコードを I システム用に設定する。
- I-DR システムへの切替えは，DNS サーバの設定情報のうち，MX レコード及び TXT レコードを I-DR システム用に設定することで行う。

(2) 外部メール DR サーバについて
- 平常時は，外部メール DR サーバを停止しておく。
- I-DR システムへの切替時に，外部メール DR サーバを起動し，メールの転送設定を確認し，メールの転送の開始処理を実行したら，DNS サーバの設定情報を変更する。
- I システムの復旧後，並行運用期間の終了時に外部メール DR サーバを停止する。

(3) 内部メール DR サーバについて
- 平常時は，利用者向けの Web メール機能を停止しておく。
- I-DR システムへの切替時に Web メール機能を起動する。
- I システムの復旧時は，Web メール機能を起動したままとし，並行運用期間の終了時に Web メール機能を停止する。

(4) 平常時の内部メールサーバと内部メール DR サーバの連携について
- 内部メールサーバに届いたメールをメールボックスに保存するとともに，メールを複製して内部メール DR サーバに転送する。
- 毎日 20 時に，メールのアカウント及びパスワードの情報を内部メールサーバから内部メール DR サーバに転送する。

図 6　I-DR システムのメールに関する方式設計（案）（抜粋）

レビューの結果，③DNS の設定変更の直後は，外部メール DR サーバからインターネット上のメールサーバに転送したメールが SPF によって迷惑メールと判定される可能性があることが分かった。検討の結果，A 社のドメイン名のメールを送信することが許可されるサーバとして［ d ］と［ e ］の IPv4 アドレスを TXT レコードに登録しておけば，切替時には TXT レコードの設定変更が不要であることが分かり，図 6 の方式設計を修正した。

次に，F さんは，DR-FW-A，プロキシ DR サーバ，社内 WebDR サーバ及び PC 管理 DR サーバの方式設計を行い，レビューを行って問題がないことを確認した。

B 社 DC については，サービス管理 Web サーバの使用に当たって，事前に B 社に依頼しておくべき事項があることが分かり，I-DR システム構築時にその依頼を行うことになった。

〔災害時の情報提供と情報収集の手段の確保〕

次に，公開 Web サーバについて，災害時の情報提供のあり方を検討した。地震発生当日及び翌日の公開 Web サーバのログを分析したところ，ページの構成を工夫することで，アクセス量が平常時の 5 倍程度になっても応答が遅くならないようにできることが分かった。そこで，災害時に公開 Web サーバの Web ページに盛り込む内容を見直すことにした。

続いて，④災害時は，情報収集の手段としてインターネット上の Web サーバへのアクセスを認めるが，図 2 の状況が発生しないように，プロキシサーバ及びプロキシ DR サーバの機能を用いて対応することに決まった。

D 部長と人事総務部長は，以上のように検討した内容を I-DR システム導入（案）として経営会議に報告し，承認を得た。

〔I システム及び I-DR システムの災害対応訓練の実施〕

情報システム部は，I-DR システム構築が完了した 1 か月後の日曜日に，訓練として，I-DR システムへの切替え，I-DR システムの運用及び I システムへの切戻しを行った。

訓練の実施後，情報システム部は反省会を開いた。反省会において，外部メール DR サーバの起動後，メールの転送を開始するまでの間にセキュリティ確保のために実施すべき事項が図 6 以外にもあることが分かり，切替手順を修正することにした。

検討チームは，I システムの復旧まで 3 か月という想定で，復旧手順を検討した。検討の結果，I システムの復旧において，I システムの機器に関する情報セキュリティ対策として行うべき事項があることが分かり，復旧手順に盛り込んだ。

それから更に 1 か月後の日曜日に，修正した復旧手順に基づいて再び訓練を行い，問題がないことを確認した。

その翌月の経営会議では，災害対策への習熟度を高めることを目的に，訓練を年 2 回実施することにし，必要に応じて，切替手順，切戻手順及び復旧手順の見直しを行うことが決まった。

設問 1　表 2 中の [a]，本文中の [b] に入れる適切な字句をそれぞれ英字で答えよ。

設問 2　〔X ウイルスに関する対処の経過〕について，(1)～(4)に答えよ。

(1)　図 3 中の［　c　］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。

(2)　X ウイルスの活動がなかったことを確認するには，FW-A で何を調べればよいか。35 字以内で述べよ。

(3)　図 3 中の下線①のように，フルスキャンを実施したかどうかを確認できない PC があった。PC がどのような状態にある場合に確認できないのか。その状態を二つ挙げ，それぞれ 20 字以内で具体的に述べよ。

(4)　本文中の下線②について，従業員がどのように Web メールを使用した場合，PC を特定できないか。30 字以内で述べよ。

設問 3　〔I-DR システムの方式設計〕について，(1)～(3)に答えよ。

(1)　本文中の［　d　］，［　e　］に入れる適切なサーバ名をそれぞれ図 5 中の字句を用いて答えよ。

(2)　本文中の下線③について，インターネット上のメールサーバが外部メール DR サーバから転送されたメールを SPF によって迷惑メールと判定する条件を 40 字以内で述べよ。

(3)　サービス管理 Web サーバの使用に当たり，B 社に依頼しておくべき事項を 50 字以内で述べよ。

設問 4　〔災害時の情報提供と情報収集の手段の確保〕について，(1)，(2)に答えよ。

(1)　災害時の情報提供について，公開 Web サーバの Web ページに盛り込む内容を見直した結果について，25 字以内で具体的に述べよ。

(2)　本文中の下線④について，プロキシサーバ及びプロキシ DR サーバにおいて対応した内容を 30 字以内で述べよ。

設問 5　〔I システム及び I-DR システムの災害対応訓練の実施〕について，(1)，(2)に答えよ。

(1)　外部メール DR サーバの起動後，メールの転送を開始するまでの間に実施すべきことを，図 6 以外の事項について，30 字以内で述べよ。

(2)　I システムの復旧において，I システムの機器に関する情報セキュリティ対策として行うべき事項を 55 字以内で具体的に述べよ。