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。

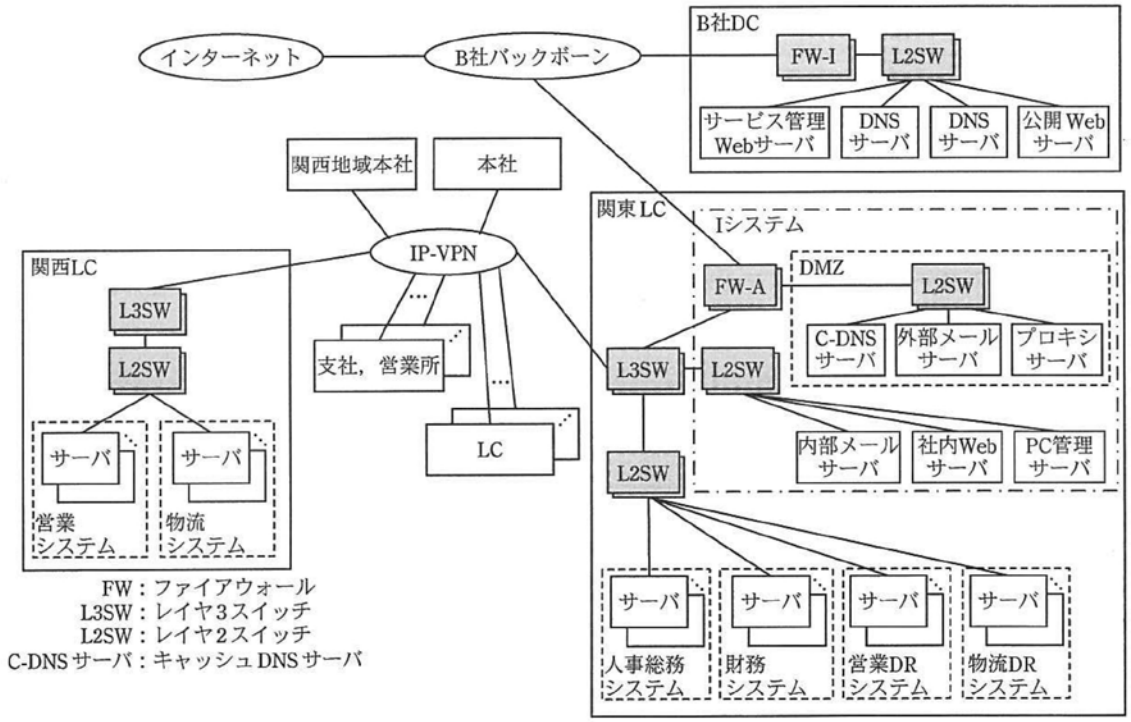
営業システム，物流システム，人事総務システム及び財務システムのサービス提供時間は，営業日の8～20時である。営業日は，年末年始を除く平日である。Iシステム及び社内ネットワーク設備のサービス提供時間は，24時間365日であるが，日曜日は保守のため停止することがある。

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。



FW：ファイアウォール
L3SW：レイヤ3スイッチ
L2SW：レイヤ2スイッチ
C-DNSサーバ：キャッシュDNSサーバ

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，ネットワークの幅輳を防げず，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。

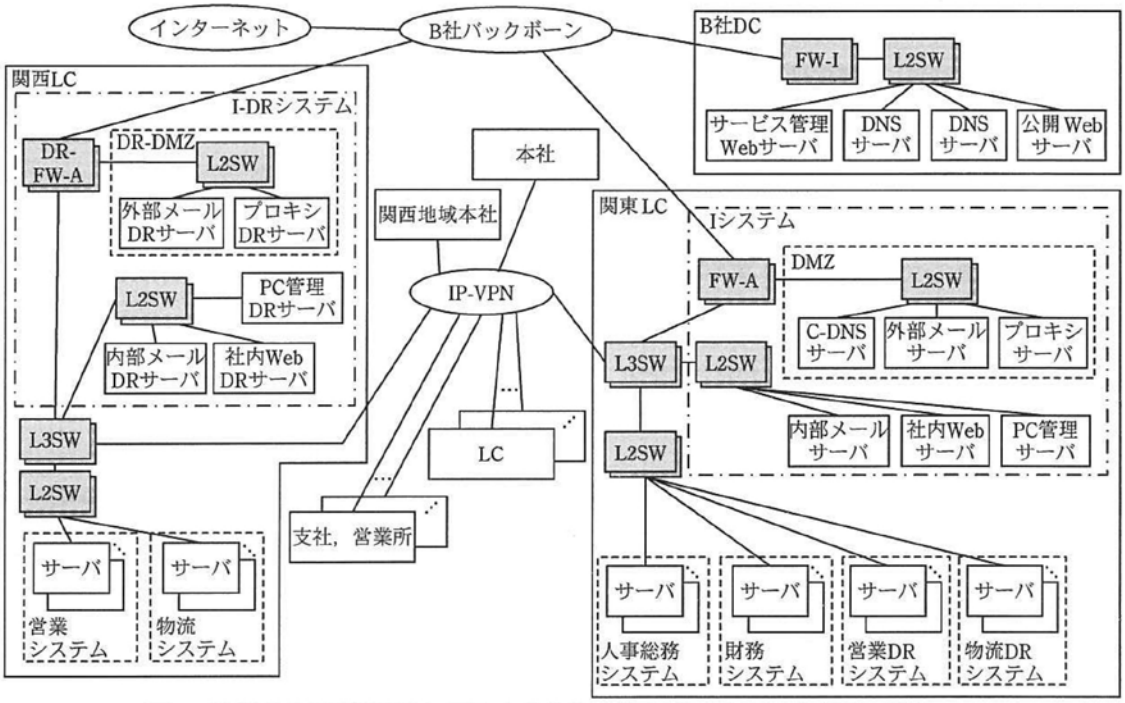


図 5　B 社 DC 及び I-DR システムを含む A 社のネットワーク構成（案）

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。

問 2 社内情報システムの移行に関する次の記述を読んで，設問 1～5 に答えよ。

R 社は，展示会やセミナなどのイベントを企画，運営する従業員数 90 名の企業である。

R 社では従業員に 1 台ずつノート PC が貸与されている。従業員は，貸与されたノート PC（以下，貸与 PC という）を用いて，電子メール（以下，メールという）の利用，プロキシサーバを介した Web サイトの閲覧，及び社内の情報システムの利用が可能になっている。顧客への訪問が多い営業部門やイベント会場での業務が多い会場運営部門には，社外に持ち出して利用するための PC（以下，持出 PC という）が数台用意されており，事前に上長が持出 PC 内のデータを確認した上で，一定期間社外に持ち出すことが許可されている。しかし，持出 PC では，社外から社内の情報システムへの接続や，社外でのインターネット接続が許可されておらず，そのため持出 PC を用いた社外でのメールの送受信はできない。また，持出 PC を返却する際には OS やアプリケーション以外のデータを全て消去することになっている。

貸与 PC 及び持出 PC にはウイルス対策ソフトが導入されており，そのウイルス定義ファイルは定期的に更新されている。また，ディレクトリサーバのもつ機能との連携によって，利用者パスワードの安全性やスクリーンセーバの設定などが一元管理され

ている。

貸与 PC 及び持出 PC では USB メモリが利用可能となっており，ファイルが自動的に暗号化される USB メモリが社内外で利用するために数個用意されている。

R 社の現行の情報システムの構成を図 1 に示す。

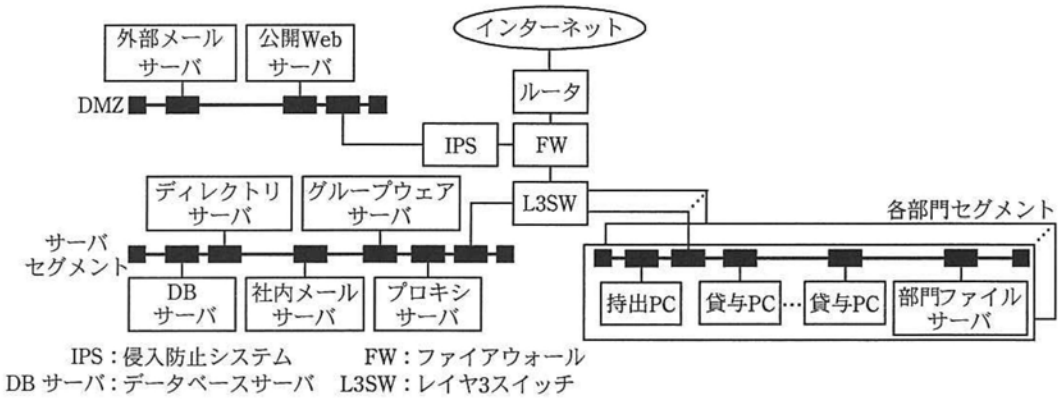


図 1　R 社の現行の情報システムの構成

R 社は従業員数が以前よりも増加しているので，現在のオフィスでは手狭になってきた。そのため，R 社はオフィスを半年後に移転することを決定し，各部門からメンバを集めて移転のためのプロジェクトチーム（以下，PJ という）を結成した。また，オフィスの移転を機に，現行の情報システムを見直して新たな情報システム（以下，新システムという）を構築することにした。情報システムを構築，運用している情報システム課からは，W 課長が PJ にメンバとして加わることになった。

〔新システムに対する要望〕

PJ 結成から 2 週間後の打合せの席で，各部門から出された新システムに対する要望は，図 2 のとおりである。

- 顧客からの問合せに迅速に対応するために，外出先や自宅からでもメールの送受信ができるようにしてほしい。
- スマートフォンやタブレット端末など，携帯端末を所有している従業員が増えてきた。現在は，個人所有の PC や USB メモリを社内の情報システムに接続することは禁止されているが，携帯端末の業務利用についての規定はない。しかし，セキュリティ上の問題点を解決し，業務利用についての規定が整備されれば，個人所有の携帯端末を業務に利用できるようになり，効率改善につながるのではないか。

図 2　各部門からの新システムに対する要望

W 課長は，クラウドコンピューティングを利用した外部のサービス（以下，グラウトサービスという）を利用することで，図 2 の要望を実現させることができるのではないかと考えた。自席に戻った W 課長は部下の S 主任を呼び，意見を聞いた。

次は，W 課長と S 主任の会話である。

W 課長：予算上の制約もあってこれまでなかなか情報システムの更改は難しかったが，今回のオフィス移転は良い機会だ。せっかく各部門から要望が挙がったのだ

から，できるだけ新システムに反映させたいね。その上でシステム管理の効率改善も図れたら言うことはない。要望を実現する手段だが，情報システムのうち幾つかをクラウドサービスに切り替えることも考えられる。クラウドサービスに切り替えれば，サーバの管理ミスや脆弱性対策の不備などに起因するリスクを外部に［ a ］するという観点や，管理コストを削減するという観点においてもメリットがあると思う。S 主任はどう思うかな。

S 主任　：イベント参加者のデータベースや経営情報など重要なデータをクラウドサービスに移すことには抵抗があります。また，現在のメールをクラウドサービスへ移行すると，①メールによってはこれまでと比較して，ある種類のリスクが高くなります。

W 課長：そのリスクについてはどう対策すればいいのかな。

S 主任　：メールの誤送信の対策に加え，添付ファイルの暗号化の徹底などが必要でしょうね。今は特に対策を行っていませんが，重要なデータを故意に外部へメールで送信することに対する抑止策も検討の価値があると思います。

W 課長：グループウェアの利用についてはどうだろうか。

S 主任　：現状では社内のスケジュール管理が中心で，そうしたデータは機密性が特に高いわけではなく，重要なデータとは言えませんが，顧客との打合せの予定などが書き込まれていますから，全体としては社外に公開できるものではありませんね。

それに，メールもそうですが，クラウドサービスへの切替えとなれば環境が大きく変わることになりますので，リスク［ b ］の結果に基づいて対応を行った上で，情報セキュリティポリシ（以下，ポリシという）の見直しを行い，必要な対策を実施するべきだと思います。

W 課長：そうだね。では次に，携帯端末の取扱いについて考えてみよう。現状では携帯端末に関する規定はないので，新たにポリシを設ける必要がありそうだ。それに，個人所有の携帯端末（以下，個人所有携帯端末という）を会社の業務に利用してよいかという議論もあるだろう。携帯端末といえば，S 主任は少し前からスマートフォンを使っているようだが，どう思うかな。

S 主任　:Web メールサービスを使っている経験から言うと，スマートフォンと PC の両方で同じようにメールを使えるのは大きなメリットですね。個人的には会社のメールとスケジュールくらいは個人所有携帯端末で確認できると確かに便利だと思いますが，セキュリティ上，心配な面もあります。もちろん，重要なデータに不正アクセスされるのは問題ですね。

個人所有かどうかは別として，携帯端末からの利用を含めてクラウドサービスの利用を考えるなら，次のような案が現実的ではないでしょうか。

S 主任は，表 1 のような情報システムの切替案を W 課長に示した。

表 1　情報システムの切替案

サービス名	クラウドサービスへの切替え	携帯端末からの利用	重要なデータの有無
メールサービス	実施	可	無
グループウェアサービス	実施	可	無
公開 Web サービス	現行のまま（新オフィスに移設）	可	無
その他のサービス	現行のまま（新オフィスに移設）	不可	有

W 課長：なるほど。各サーバで取り扱う情報の性質からすると，表 1 が妥当なところかもしれないな。リスクはいろいろあり，セキュリティ対策を実施しても最終的に残るものもあるだろう。その残るリスクをそのまま［ c ］してクラウドサービスに切り替えるかどうかは経営陣が判断することだ。2 週間後に次の PJ の打合せがあるので，それまでに表 1 の案を実現する上での検討課題をまとめてくれるかな。

S 主任　：分かりました。

S 主任は各部門からの要望を参考にしつつ，現行のポリシと情報システムを踏まえて図 3 のような新システムの検討課題の骨子をまとめ，順次検討していくことにした。

(1) クラウドサービスに切り替えた場合の管理とセキュリティの確保
(2) 携帯端末の管理とセキュリティの確保
(3) 新システムへの切替えに伴うポリシの改定
(4) 利用者に対する周知，教育

図 3　新システムの検討課題の骨子

〔クラウドサービスに切り替えた場合の管理とセキュリティの確保〕

S 主任は，まず，メールサービスとグループウェアサービスをクラウドサービスに切り替えた場合の管理，運用面の課題について検討することにした。クラウドサービスには大きく分けて SaaS（Software as a Service）型，PaaS（Platform as a Service）型，IaaS（Infrastructure as a Service）型の 3 種類があることから，それぞれの特徴を考慮して現行の自社運用との比較を行った。その結果を表 2 に示す。

表 2　メールサービスとグループウェアサービスの管理と運用に関する比較

管理主体・管理内容	SaaS 型	PaaS 型	IaaS 型	自社運用（現行）
ハードウェア・ネットワークの管理主体（仮想化環境を含む）	事業者 1)	事業者	事業者	自社
OS，ミドルウェアの管理主体	事業者	［ d ］	自社又は事業者	自社
アプリケーションの管理主体	事業者	［ e ］	自社	自社
迷惑メール対策，ウイルス対策の管理主体	自社又は事業者	自社又は事業者	自社	自社
自社の管理工数	小	中	大	大
エンドユーザから見たサービスの稼働率	99.9%以上（SLA 2) に依存）	99.9%以上（予想）	99.9%以上（予想）	99.5%（実績）
ハードウェア保守対応	—	—	—	翌営業日対応

注 1)　サービス提供事業者
2)　Service Level Agreement：サービスレベル合意書

S 主任はこの結果から，管理工数や稼働率の面からみたとき，自社運用よりも SaaS 型サービスを利用する方が有利であると判断した。また，費用面についても，SaaS 型サービスの利用によって，自社運用よりも安価にメールとグループウェアのサービスを実現できると判断した。そこで，S 主任は W 課長と相談し，メールとグループウェアのサービスの SaaS での利用を前提に検討を進めることにした。

次に，S 主任は表 1 の切替案でグラウトサービスを利用する際のセキュリティ上の問題として，図 4 の(1)～(6)を想定し，それぞれについて R 社としての対策を検討することにした。

(1) 事業者から提供されるインタフェースの不備や機能の不足
(2) アカウント又はサービスの不正使用
(3) クラウドサービス上のデータの消失
(4) クラウドサービス上のデータの漏えい
(5) 事業者による不正行為
(6) リスク状況の非開示（リスクを算定するための情報が事業者から提供されないこと）

図 4　クラウドサービスを利用する際のセキュリティ上の問題

(1)については，具体的な例として，認証方式の不備，通信路の暗号化の欠如，監視やログ機能の不足といった問題が考えられるので，S 主任は事業者が提供するサービスの内容を更に詳しく調査することにした。(2)については，クラウドサービスを利用する R 社側でも認証に関する対策を行うことが必要と考えた。(3)については，②R 社においてデータのバックアップを行うことが必要になると考えた。

(4)～(6)については，事業者を選定する際に，事業者のプライバシーマーク付与，ISMS 認証，③受託業務に係わる内部に関する監査など，第三者による認証，監査などを受けている事業者を候補にしようと考えた。その中から更に契約，SLA の内容，サービスの実績などを詳細に比較検討して選定を行うことで，(4)～(6)への対策に代えることができるのではないかと S 主任は考えた。

各事業者のサービスを比較検討した結果，S 主任は C 社の SaaS 型クラウドサービスを選定するのがよいと判断し，W 課長に説明した。

次は，W 課長と S 主任の会話である。

W 課長：なるほど。C 社の SaaS 型サービスであれば実績も多いようだし，コスト面でも今より有利になるね。しかし，クラウドサービス上にメールとグループウェアのデータがあるので，アクセス元を限定できない C 社の SaaS 型サービスだと，持出 PC でも個人所有携帯端末でも，従業員が個人で所有している PC(以下，個人所有 PC という)でも，更にはネットカフェの PC などでも利用できるということになるね。それで本当に問題がないか，もう少し検討してみよう。

S 主任　：C 社の SaaS 型サービスでは，利用できる端末を限定できないので，確かに問題がありますね。

W 課長：自宅でメールを見たい場合もあるだろうから，個人所有 PC からの利用は許可するとしても，会社又は従業員個人の管理下にない PC についてはセキュリティ対策が不十分な可能性があるので，ポリシでクラウドサービスの利用を禁止した方がよさそうだ。

S 主任　：データに関しても，重要なデータは社内だけで利用すべきなので社内だけに

置き，社外からも利用してよいデータだけクラウドサービスに置く必要があります。表 1 の案はそのようになっています。

W 課長：そうだね。携帯端末を使う場合のセキュリティリスクについても引き続き検討してくれるかな。

S 主任　：分かりました。

〔携帯端末の管理とセキュリティの確保〕

W 課長の指示を受け，S 主任は携帯端末を利用する場合のセキュリティについて検討することにした。

携帯端末は，一般的に図 5 のような機能をもっており，ハードウェア面，ソフトウェア面で従来の携帯電話や PC とは違いがある。このため，利用する場合のセキュリティリスクにも大きな違いが想定される。

○基本機能
・音声通話（携帯電話事業者網経由）
○入出力機能
・ディスプレイ
・カメラ
・入力インタフェース（タッチパネル，キーボードなど）
○ネットワーク接続機能
・データ通信（携帯電話事業者網経由）
・無線 LAN 接続
○インターネット利用機能
・メール送受信
・Web ブラウザ（アクセス先は携帯電話専用サイトに限定されない）
○その他の機能
・利用者側で自由にアプリケーションを導入可能
・PC との連携（無線 LAN 又は USB 経由）

図 5　携帯端末の機能（主要なもの）

携帯端末は一般的なノート PC よりも携帯性が高い分，盗難や紛失のリスクが大きい。また，従来の携帯電話と異なり，携帯端末では自由にアプリケーションを導入することができる点が PC と同様であり，ウイルス対策や脆弱性対策が必要となる。通信の方法に関しても，携帯電話事業者の提供する携帯電話事業者網以外に，公衆無線 LAN などを利用することができるので，なりすましの防止や通信の暗号化などの対策が必要となる。さらに，携帯端末による社内の重要なデータの漏えいのリスクについても考慮する必要がある。

S 主任は，以上の検討結果を踏まえて，携帯端末のセキュリティリスクへの対策を図 6 のようにまとめ，W 課長に提示した。

(1) 貸与 PC に加えて携帯端末からのクラウドサービスの利用を許可するが，利用者は特にセキュリティに留意する。
(2) 携帯端末を利用する場合には，紛失，盗難への対策を行う。
(3) 携帯端末を利用する場合には，ウイルス対策や脆弱性対策を行う。
(4) 携帯端末からクラウドサービスを利用する場合には，二要素認証など，強度の高い利用者認証を行う。
(5) 携帯端末からクラウドサービスを利用する場合には，SSL による暗号化を行う。
(6) 携帯端末から DMZ 以外の社内のネットワークへの接続は禁止する。

図 6　携帯端末のセキュリティリスクへの対策

S 主任は，新システムに図 6 のような対策を採り入れれば，メールとグループウェア以外の社内の重要なデータは，現在と同様に保護することができることを基本視点として挙げた。この方式を採用した場合，社内ネットワークに接続された貸与 PC からも携帯端末からもクラウドサービスに対して暗号化通信が可能である一方，携帯端末から FW を経由して DMZ 以外の社内のネットワークに直接アクセスすることはできない。これに対し，W 課長は，この方式を採用した場合でも，④携帯端末の機能を用いて従業員の貸与 PC 上のデータに直接アクセスが可能であることを指摘し，対策を行うよう指示した。

さらに，S 主任は，携帯端末の利用形態についても考察を進めた。申請によって個人所有携帯端末からのクラウドサービスの利用を許可する場合（以下，案 1 という）と，会社として特定機種の携帯端末を導入し，従業員に貸与する場合（以下，案 2 という）の二つを想定し，その差異を表 3 にまとめた。この後，S 主任は，重要なデータの保護についても検討し，経営陣に判断を仰ぐことにした。

表３　利用する携帯端末による差異

	案 1	案 2
費用負担	携帯端末代金と業務で使用する通信料その他の料金を従業員が負担する。	携帯端末代金と通信料を会社が負担する。
携帯端末のセキュリティ管理	従業員個人での管理が必要であり，一元管理は困難。	一元管理が可能。
携帯端末に導入するアプリケーションの制限	従業員個人での管理が必要であり，一元管理は困難。	R 社で許可しないアプリケーションのダウンロードを禁止でき，一元管理が可能。
携帯端末の脆弱性対策	従業員個人での管理が必要であり，⑤個々の個人所有携帯端末の脆弱性を一括で修正することは困難。	脆弱性の一括修正は基本的に可能だが，採用した機種に脆弱性があった場合，メーカ側の対策が完了するまで全従業員が携帯端末を利用できない可能性がある。
携帯端末上のデータ	私的データと会社で利用するデータが混在する。	本来は会社で利用するデータだけだが，私的利用によって私的データが混在する可能性がある。

〔新システムの構成案〕

以上の検討結果を基に，S 主任は W 課長とともに検討を進め，新システムの構成案を作成して PJ と経営陣に提案した。利用する携帯端末に関しては，経営陣の判断で案 1 が採用され，利用希望者には通信料の補助を行うことになった。携帯端末利用者向けに無線 LAN のアクセスポイントを社内に設けることも提案したが，経営陣からは，外部者による盗聴やネットワークへの侵入を憂慮する意見があり，オフィス移転後も現在と同様に有線 LAN だけを使用することになった。最終的に承認された新システムの構成を図 7 に示す。

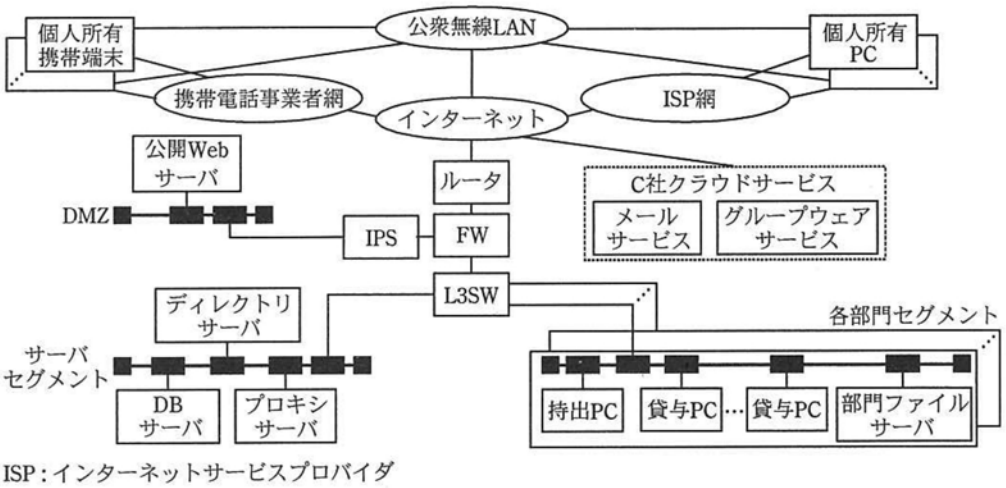


図 7　新システムの構成

〔新システムにおけるポリシの改定〕

新システムへの移行に伴い，W 課長は S 主任に対して現行のポリシを見直すよう指示した。S 主任は，現行のポリシに対し，図 8 の改定及び図 9 の追加を行う案を作成した。

（省略）

5.1　情報システム及びクラウドサービスへのアクセス

(1)　社内の情報システムへのアクセスは，貸与 PC 又は持出 PC から行う。当社が利用するクラウドサービスへのアクセスは，貸与 PC に加えて，当社が別途定める対策を行えば，個人所有 PC 及び個人所有携帯端末（以下，この二つを個人所有端末という）からも行ってよい。

なお，当社が利用するクラウドサービスは，メールサービス及びグループウェアサービスとする。

(2)　貸与 PC 及び持出 PC を社内のネットワークに接続するときは，別途指定するゲートウェイ及びプロキシの設定を実施する。

(3)　貸与 PC 及び持出 PC は，パスワードによるハードディスクの暗号化を行う。当社が利用するクラウドサービスにアクセスする個人所有端末に関しては，利用者の責任においてハードディスクその他の内部記憶媒体の機密性を高める。

（省略）

7.3 情報資産の管理

(1)　業務上利用する情報は，貸与 PC，持出 PC，サーバ又は別途定める媒体若しくは当社が利用するクラウドサービスに保存する。

(2)　クラウドサービス上で利用可能な情報については，個人所有端末に保存してもよい。

(3)　業務上利用する情報を保存した機器を社外で利用する場合は，“8.3 持出 PC”，“8.4 個人所有 PC”及び“8.5 個人所有携帯端末”に従う。

（省略）

図 8　ポリシの改定案（下線部分を改定）

8.4　個人所有 PC

当社が利用するクラウドサービスにアクセスする個人所有 PC では，次の対策を行う。

(1)　OS 及びアプリケーションに最新の脆弱性対策パッチを適用する。

(2)　ウイルス対策ソフトを導入し，ウイルス定義ファイルを最新に保つ。

(3)　ファイル共有ソフトを利用しない。

（省略）

8.5　個人所有携帯端末

当社が利用するクラウドサービスにアクセスする個人所有携帯端末では，次の対策を行う。

(1)　OS 及びアプリケーションに最新の脆弱性対策パッチを適用する。

(2)　ウイルス対策ソフトが利用可能な場合は，ウイルス対策ソフトを導入し，ウイルス定義ファイルを最新に保つ。

(3)　個人所有携帯端末の OS に対し，⑥インターネットに流布しているツールなどを利用した改造を行わない。

(4)　携帯端末メーカや携帯電話事業者のサイトなど，信頼できる提供元からだけアプリケーションを導入する。

（省略）

図 9　個人所有端末に関するポリシの追加案

さらに，グラウトサービスを利用するための細則は，図 10 のように定めた。

1.　クラウドサービスの利用者 ID とパスワード

(1)　クラウドサービスを利用するには，当社が指定するメールアドレスを利用者 ID として用い，これとパスワードを併用してログインする。

(2)　クラウドサービス用のパスワードは，社内の情報システム用のパスワードよりも更に安全なものにする。

(3)　クラウドサービス用のパスワードは，社内の情報システム用のパスワード及び［　f　］パスワードとは別のものにする。

2.　メールの利用

(1)　メールを利用するには，ブラウザを用いて当社の指定する URL にアクセスするか，メールソフトを用いて当社の指定するサーバにアクセスする。

(2)　メールソフトを利用するには，メールの送信プロトコルとして SMTP over SSL，メールの受信（バックアップ及びリストアを含む）のためのプロトコルとして［　g　］over SSL を用いる。

(3)　全てのメールはクラウドサービス上でアーカイブ及び送受信ログが取得されるので，それに留意する。

(4)　クラウドサービス上のメールは，必要であれば当社が指定するソフトウェアを用いて貸与 PC 上でバックアップを取得してもよい。

(5)　メールを業務と関係のないメールアドレスに転送しない。

3.　グループウェアの利用

(1)　グループウェアを利用するには，ブラウザを用いて当社の指定する URL にアクセスするか，グループウェアクライアントソフトを用いて当社の指定するクラウドサービスにアクセスする。

（省略）

図 10　クラウドサービスの利用細則

これらのポリシ及び利用細則は承認され，オフィスの移転と新システムへの移行の準備が進められた。

〔新システムへの移行後の情報セキュリティインシデント〕

新システムへの移行作業では多少の混乱はあったものの，S 主任が想定していたよりも作業はスムーズに完了した。また，携帯端末の利用申請者は全従業員の半数近くに及

び，S 主任は二度に分けて利用申請者への研修を行った。その後，個人所有端末で新システムを利用し始めた従業員からは，業務効率が向上したとの感想が寄せられた。

新システムへの移行作業を終えて 1 か月余りが経過したある日の昼休み，S 主任は昼食から戻り，自席で自分のスマートフォンを操作していた。ふと思いついた S 主任は，普段は会社で有効にしていないスマートフォンの無線 LAN 機能を有効にしてみたところ，数個の無線 LAN アクセスポイントが検出された。いずれも WEP による通信の暗号化が施されていたが，SSID の情報からは，携帯端末の無線 LAN 機能を有効にして無線 LAN のアクセスポイントとして利用している従業員が社内にいる可能性が考えられた。

そこで，S 主任がプロキシサーバのログを確認したところ，在席して貸与 PC からクラウドサービスや外部のサイトにアクセスして業務を行っているはずの従業員のうち，数名がプロキシサーバに対して数日間アクセスしていないことが判明した。また，該当する従業員は携帯端末の利用申請を行っていた。

S 主任は，これらの従業員が携帯端末の無線 LAN 機能を利用してプロキシサーバへのアクセスを回避しているのではないかと考えた。

このような事態を放置した場合に，⑦重大なセキュリティ事故が発生することを危惧した S 主任は，W 課長と相談し，疑いのある従業員にヒアリングを行うことにした。

その結果，S 主任の考えたとおり，どの従業員も貸与 PC と携帯端末とを無線 LAN 機能で接続し，貸与 PC から携帯端末及び携帯電話事業者網経由でクラウドサービスや外部のサイトにアクセスしていたことが判明した。

ポリシに不備があったので，これらの従業員に対する処分は見送られたが，ポリシの改定と技術的対策を行い，利用者への周知，教育を再度実施することによってこの問題の再発防止を行うことにした。

その後，R 社では大きなトラブルもなくクラウドサービス及び携帯端末を利用して業務を行っている。

設問 1　〔新システムに対する要望〕について，(1)～(3)に答えよ。

(1)本文中の [a] ～ [c] に入れる適切な字句をそれぞれ解答群の中から選び，記号で答えよ。

解答群

ア　移転　　イ　回避　　ウ　受容

エ　対応　　オ　低減　　カ　分析

(2)本文中の下線①について，どのようなメールについてどのようなリスクが高まるか。 30 字以内で答えよ。

(3)図 3 の検討課題について，利用者に対して周知，教育すべき事項を二つ挙げ，それぞれ 25 字以内で答えよ。

設問 2　〔クラウドサービスに切り替えた場合の管理とセキュリティの確保〕について，(1)～(4)に答えよ。

(1)表 2 中の [d] ， [e] に入れる適切な字句を，それぞれ 3 字以内で答えよ。

(2)表 2 について，ある事業者が提供するサービスにおいて，保証するサービスの稼働率が 99.9%であるとき，1 か月間での最大停止時間は何分になるか。秒以下は切り捨てて分単位で答えよ。ただし，1 か月は 30 日とし，1 日のサービス提供時間は 24 時間とする。

(3) 本文中の下線②について，メールやグループウェアのサービスを SaaS 型サー

ビスで利用する場合，メールやグループウェアのデータ以外に，R 社においてバックアップを行う必要があると考えられるデータは何か。 25 字以内で答えよ。

(4) 本文中の下線③の監査において用いられる監査基準を解答群の中から選び，記号で答えよ。また，プライバシーマーク付与や ISMS 認証なども含め，第三者による認証，監査などを受けている事業者を候補とすることで，事業者にはどのようなことが期待できるか。 40 字以内で述べよ。

解答群

ア　lSO/IEC 20000　　イ　PCIDSS

ウ　SAS 70 （SSAE 16）　　エ　情報セキュリティ監査基準

設問 3　〔携帯端末の管理とセキュリティの確保〕について，(1)，(2) に答えよ。

(1) 本文中の下線④について，携帯端末側から貸与 PC 上のデータにアクセスするには具体的にどのような方法が想定されるか。25 字以内で述べよ。

(2) 表 3 中の下線⑤に対応するため，従業員に個人所有携帯端末の詳しい脆弱性情報を提供することが考えられる。各従業員に必要かつ十分な脆弱性情報を提供するには，従業員の個人所有携帯端末の利用申請時にどのようなことを行う必要があるか。40 字以内で述べよ。

設問 4　〔新システムにおけるポリシの改定〕について，(1)，(2) に答えよ。

(1) 図 10 中の [f] ，[g] に入れる適切な字句を，[f] は 15 字以内，[g] は 5 字以内で答えよ。

(2) 図 9 中の下線⑥に示す改造によって，携帯端末がウイルスに感染しやすくなる理由を，60 字以内で述べよ。

設問 5　〔新システムへの移行後の情報セキュリティインシデント〕について，(1)，(2) に答えよ。

(1) 本文中の下線⑦について，どこにあるどのようなデータがどのような経路で漏えいすることが想定されるか。50 字以内で具体的に述べよ。

(2) S 主任が発見したセキュリティ上の問題の再発を防ぐために，図 9 の個人所有端末に関するポリシの追加案に更に追加すべき項目と，R 社内の情報システムにおいて実現可能と考えられる技術的対策を，それぞれ 40 字以内で述べよ。

解答例

問 1

《出題主旨》

災害復旧対応では，災害発生時の状況を想定し，有効かつ具体的な計画を作成しておくことが重要であ　る。インターネットに接続されたサーバは，災害復旧対応に重要な役割を果たすが，同時に十分な情報セキュリティ対策も求められる。

を問う。

本問では，インターネット向けサーバの災害復旧対応を題材として，システムの設計及び運用に関する能力を問う。

設問 l　a　・ HTTP over SSL
・SSL
b　SSH

設問 2（1）c　プロキシサーバ
（2）PC 及びプロキシサーバから特定 Web サーバへの通信がないこと
（3）①　・電源が入っていない状態
②　・LAN に接続していない状態
（4）他の従業員の PC を借用し，Web メールを使用した場合

設問 3　(1)　d　外部メールサーバ　　順不同
e　外部メール DR サーバ
(2)　参照する DNS サーバのキャッシュに切替え前の情報が保持されている。
(3)　プロキシ DR サーバからサービス管理 Web サーバへの通信を許可するように FW－I の設定を追加する。

設問 4　（1）画像情報を最小限にし，文字主体にする。
（2）フィルタリングするファイル種別に動画を追加する。

設問 5　（1）迷惑メール定義ファイルを最新にする。
（2）I-DR システムの機器だけに行った設定の反映及び最新の修正プログラムの適用を，I システムの機器に行う。

問 2

《出題主旨》

近年，スマートフォンやタブレット端末などの携帯端末の普及が急速に進む中，クラウドサービスに代表される企業内外の情報リソースを有効に利活用するために BYOD（Bring Your Own Device），すなわち個人所有の携帯端末の企業での利用が注目されている。

本問では，イベント運営会社における社内システムのクラウドサービス利用への移行及び個人所有の携帯端末の導入を題材に，クラウドサービス及び携帯端末を業務で利用する際のセキュリティ上のリスクとその対応について問う。

設問 1　(1)　a　ア
b　カ
c　ウ
(2)　機密性の高い社内のメールが外部に流出するリスク
(3)　①・新システムへの切替えに伴うポリシの改定点
②・グラウトサービス及び携帯端末の安全な利用方法

設問 2　(1)　d　事業者

e　自社

(2)　43

(3)　クラウドサービス利用者のアカウント情報

(4)　**記号**　　ウ

期待できること　事業者の定めた管理策が，適切なマネジメントに基づいて運用されていること

設問 3　(1)　携帯端末を PC の USB ポートに接続する。

(2)　従業員の個人所有携帯端末の機種と OS のバージョンを申請させる。

設問 4　(1)　f　個人所有携帯端末用の

g　IMAP4

(2)　携帯端末メーカの設定したセキュリティ機構が無効化され，一般のアプリケーションが本来利用できない権限で動作　　**することが可能になるから**

設問 5　(1)　貸与 PC の中にある重要なデータが無線 LAN と個人所有携帯端末を経由して社外に故意に送信される。

(2)　**項目**　　個人所有携帯端末と貸与 PC を無線 LAN で接続しない。

技術的対策　ディレクトリサーバとの連携によって貸与 PC の無線 LAN 機能を無効にする。

採点講評

問 1

問 1 では，インターネット向けサーバにおける災害対策を題材にして，そこで必要となる情報セキュリティ対策について出題した。全体として正答率は高かった。

設問 3(1)は，メールの転送を行わないサーバやインターネットとの間でメールの転送を行わないサーバを挙げた解答が散見された。本文及び図表をよく読めば正答を導けるはずである。

設問 3(2)は，正答率が低かった。 SPF (Sender Policy Framework)の仕組みの説明が誤っている解答や，SPF 以外の手法を述べた解答が目立った。 SPF は迷惑メールに対する有効な対策の一つである。 SPF の仕組みをよく理解しておいてほしい。

設問 4(2)は，プロキシサーバ及びプロキシ DR サーバの機能を用いた解答を求めたにもかかわらず，存在しない機能を述べた解答が目立った。本文，図表及び設問をよく読み，求められていることを理解した上で解答してほしかった。

問 2

問 2 では，社内システムのクラウドサービスへの移行及び個人所有の携帯端末の導入を題材に，グラウトサービス及び携帯端末を業務で利用する際のセキュリティ上のリスクとその対応について出題した。全体として正答率は低かった。

設問 1(2)は，正答率が低かった。グラウトサービスへの移行によってメールサーバが社外に置かれるということを考慮せずに，社外へのメールの誤送信や平文でのメールの送信を挙げた解答が多かった。

設問 4(2)は，改造ツールに脆弱性が含まれる可能性について述べた解答が多かった。改造ツールをインストールした携帯端末に感染するマルウェアが存在することも事実ではあるが，そうしたマルウェアも携帯端末に導入されているセキュリティ機構が無効化されて初めて動作が可能となることに気づいてほしかった。

設問 5(2)は，技術的対策として，ファイアウォール又は IPS によるアクセス監視や，プロ

キシの設定の強制によるアクセスの制限を挙げた解答が散見された。前者では無線 LAN での通信を防ぐことはできず，後者ではブラウザを利用しない外部との通信を防ぐことができない。本文に記述された前提や設問で触れられた条件に注意した上で，どのような対策が最も効果的かを十分に吟味して解答してほしかった。