**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。

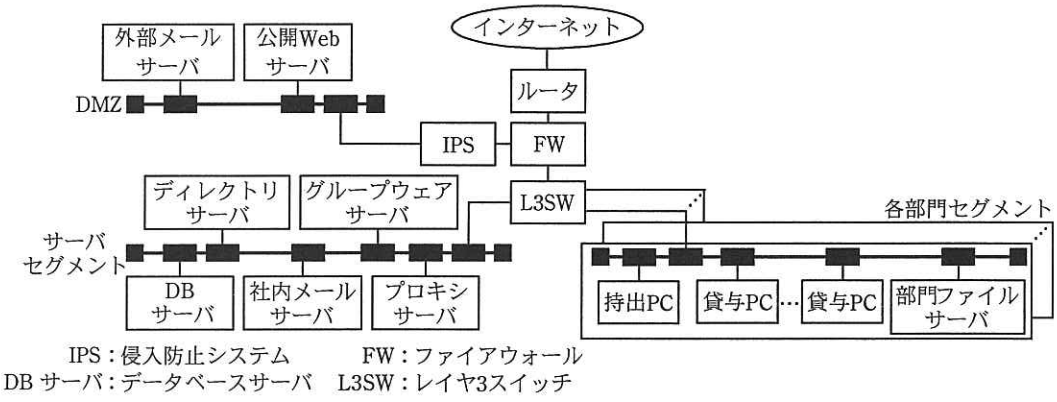



**図1　R社の現行の情報システムの構成**

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，クラウドサービスという）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(ぜい)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受託業務に係る内部統制に関する監査など，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。

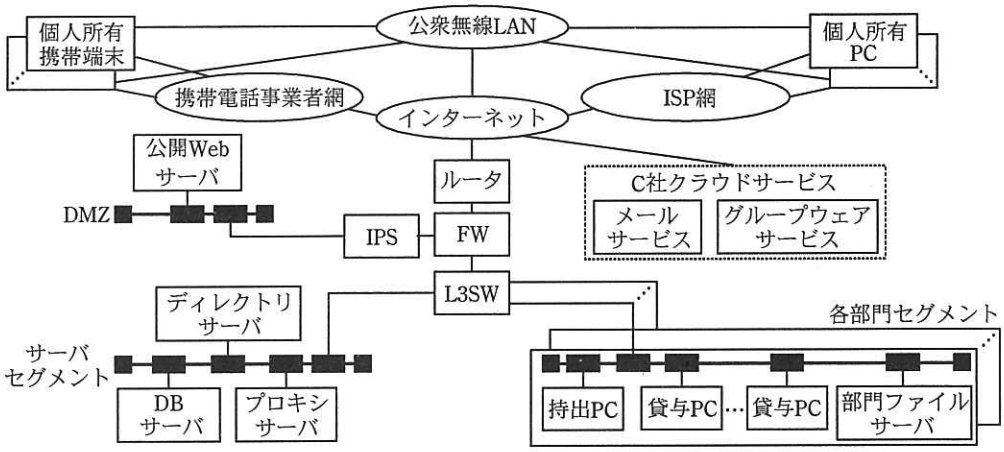
さらに，S 主任は，携帯端末の利用形態についても考察を進めた。申請によって個人所有携帯端末からのクラウドサービスの利用を許可する場合（以下，案 1 という）と，会社として特定機種の携帯端末を導入し，従業員に貸与する場合（以下，案 2 という）の二つを想定し，その差異を表 3 にまとめた。この後，S 主任は，重要なデータの保護についても検討し，経営陣に判断を仰ぐことにした。

**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。




ISP：インターネットサービスプロバイダ

**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，クラウド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 ISO/IEC 20000　　イ PCI DSS

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。