問2　インターネットを利用したシステムの情報セキュリティ監査対応に関する次の記述を読んで，設問1～5に答えよ。

K社は，従業員数200名の，半導体を中心とした電子部品の専門商社であり，本社と配送センタの二つの拠点がある。K社は，インターネットを利用した受発注システム（以下，受発注Webシステムという）及び配送センタのシステムを用いて，国内，国外の部品メーカや代理店から仕入れた電子部品を製品メーカに対して低価格，短納期で供給している。K社の組織を図1に示す。

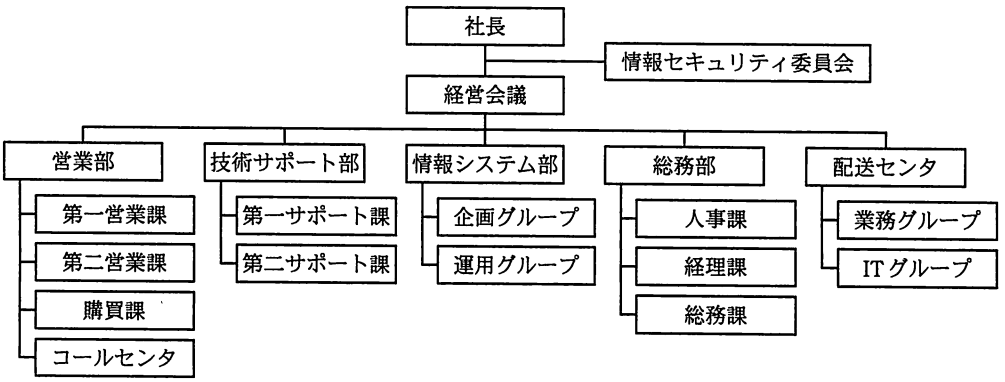


図1　K社の組織

これまで，K社では大きな情報セキュリティインシデント（以下，インシデントという）が発生したことはない。しかし，最近，K社では取引先から受発注Webシステムのセキュリティ対策についての質問を受けることが多くなった。K社は，取引先の製品メーカが使用する部品の重要な供給元であることから，K社で受発注Webシステムの長時間停止や，そこからの情報の漏えい，改ざんなどのインシデントが発生すると，K社だけでなく製品メーカにも影響が及ぶことが考えられる。

そこで，社長は，自社の情報セキュリティの問題点を洗い出し，見直しを図ることを経営会議に提示し，決定した。この作業を情報システム部が行うことになり，情報システム部のE部長は，部下のF主任とG君に見直しの具体的な方法について検討するよう指示した。

〔情報セキュリティの見直しと情報セキュリティ監査〕

次は，情報セキュリティの見直しについてのＦ主任とＧ君の会話である。

Ｇ君　：情報セキュリティの見直しといっても，新たに何を行ったらよいのでしょうか。技術的対策は一通り実施していると思いますし，既に情報セキュリティ基本方針，対策基準，実施手順などの情報セキュリティポリシ文書（以下，ポリシという）を整備し，それらが遵守されているかどうかの内部監査も毎年実施しています。

Ｆ主任：ポリシが遵守されていることは毎年の内部監査でチェックしているけれど，ポリシや対策の有効性についてはチェックしきれていない気がするので，外部の専門家に情報セキュリティ監査を依頼するとよいと思うよ。

Ｇ君　：情報セキュリティ監査ですか。経済産業省の情報セキュリティ監査制度に基づいて実施するものですね。

Ｆ主任：情報セキュリティ監査には，大きく分けると二つのタイプの監査があるが，今の時点で監査を受けるとしたら［　a　］型かな。その結果で得られる管理面，技術面の改善提言を基に情報セキュリティを改善していき，情報セキュリティ管理の成熟度が上がったら，次の段階として［　b　］型に移行していくのがよいだろうね。そうすれば，当社が明確な基準に適合するレベルで情報セキュリティ対策を実施していることを，部品メーカや製品メーカに対して示すことができるだろう。

Ｇ君　：監査の範囲と対象も考えないといけないですよね。

Ｆ主任：今回は最初のケースだから，製品メーカの事業継続にも影響の大きい受発注Webシステムと配送センタのシステムを対象にするのがよいだろう。

Ｇ君　：監査の依頼先ですが，いつもシステム開発をお願いしているソフトウェアハウスのＹ社も監査サービスをやっているはずですから，Ｙ社に監査を依頼すればよいですか。

Ｆ主任：①今回のような場合，Ｙ社に監査を依頼すべきではないね。

Ｆ主任は，その理由を説明した。

G 君　：Y 社以外から選ぶとしたら，どういう企業を選ぶべきですか。

F 主任：経済産業省の情報セキュリティ監査 [c] に登録されている企業から選ぶのがよいだろう。得意とする監査対象の分野・業種，前年度の監査の実績などが経済産業省の Web サイトで検索できるから，何社か候補を挙げて問い合わせてみてくれるかな。情報セキュリティ監査の必要性を E 部長に説明する資料もお願いするね。

G 君　：分かりました。資料を作ってみます。後でチェックをお願いします。

E 部長は，F 主任と G 君の検討結果に合意した。経営会議で，E 部長が，情報セキュリティの見直しには情報セキュリティ監査が効果的であることを経営陣に説明したところ，賛同が得られ，外部の監査企業による情報セキュリティ監査を実施することが決まった。

K 社は数社の監査企業に提案を求め，比較した結果，監査企業 Z 社と監査契約を締結することにした。

〔Z 社との事前打合せ〕

監査を始めるに当たって，監査技法やスケジュールなどに関して事前に打合せを行うために，Z 社の監査人 V 氏と W 氏が K 社を訪問した。

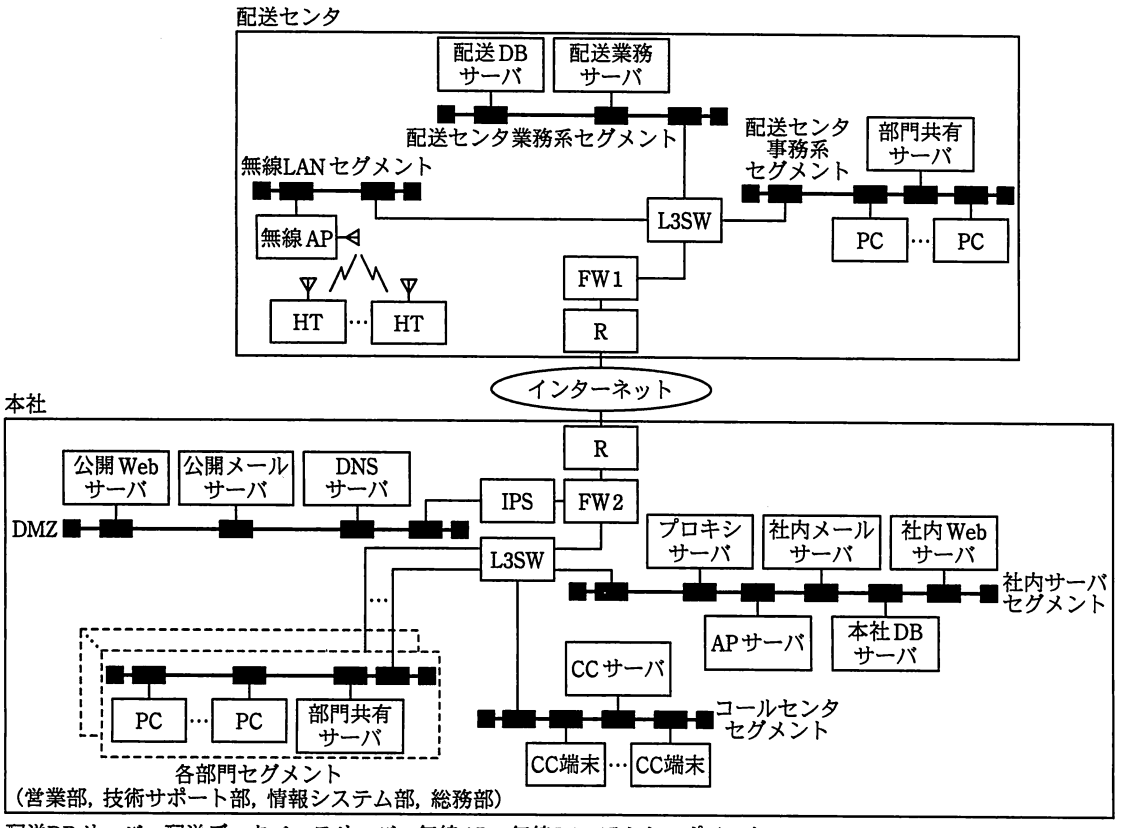
最初に，E 部長は K 社の情報資産と情報システムの概要を次のとおり説明し，受発注 Web システムと配送センタのシステムに関連するポリシと対策の有効性を確認することが今回の監査の目的であると述べた。

(1) 情報システムの企画，開発と運用

K 社の情報システムは，企画グループが企画を行い，設計，開発は主としてソフトウェアハウスの Y 社に委託している。

K 社の情報システムの構成は図 2 に示すとおりである。受発注 Web システムは，公開 Web サーバ，アプリケーションサーバ（以下，AP サーバという）及び本社データベースサーバ（以下，本社 DB サーバという）から構成され，AP サーバ上では部品メーカ，製品メーカ及び代理店から公開 Web サーバへのアクセスに対して受発注の処理を行うための Web アプリケーション（以下，Web アプリという）が稼働している。

K 社の主要な情報システムは，K 社の情報システムと同等と見なし得る機能及び構成の，Y 社の開発系プラットフォーム上で開発されている。また，情報システムの運用は，本社では運用グループが，配送センタでは IT グループが行っている。



配送DBサーバ：配送データベースサーバ　無線AP：無線LANアクセスポイント　L3SW：レイヤ3スイッチ
IPS：侵入防御システム　FW：ファイアウォール　HT：携帯端末
R：ルータ　CCサーバ：コールセンタサーバ　CC端末：コールセンタ端末

図２　K社の情報システムの構成

(2) 監査の対象とする情報資産

今回の監査の対象とするシステムは，製品メーカの事業継続にも影響の大きい受発注 Web システムと配送センタのシステムであり，監査の対象とする情報は，取引先に関する情報（以下，顧客情報という），取扱部品の単価及び受発注に関する情報である。

これらの情報は，主に Web アプリで入力され，本社 DB サーバに格納される。K 社ではこれらの情報を [d] に規定された営業秘密の要件を満たすよう管理している。

なお，部品の注文はコールセンタでも受け付けており，CC 端末からは本社 DB サーバ上の顧客情報や部品の受発注の情報が検索及び更新可能になっている。

(3) 本社の各部門での PC の利用形態

本社の各部門では，PC が各部門セグメントに接続され，部門共有サーバでファイルが共有可能である。各部門の PC からは社内サーバセグメントのプロキシサーバ，社内メールサーバ，社内 Web サーバにアクセス可能である。また，情報システム部の運用グループのメンバの PC からは，社内サーバセグメントのサーバを管理するためのアクセスが可能である。

(4) 配送センタのシステム

配送センタでは，入荷した部品の検品，入庫及び出荷作業（以下，入出荷作業という）を行っている。入出荷作業を迅速に行うために，配送センタでは図 2 のように HT を利用しており，HT と無線 AP の間の通信は無線 LAN のセキュリティ機能を用いて暗号化している。HT のアプリケーションは，ファームウェアとして Y 社が開発したものであり，入出荷作業によって生成される HT のデータは独自の通信プロトコルを用いて配送業務サーバに送信される。さらに，入出荷作業のデータは配送 DB サーバに格納され，本社 DB サーバにも反映されて，在庫管理などに活用されている。

(5) ネットワークセキュリティ対策

本社と配送センタのネットワークは，各拠点の FW を経由してインターネットに接続されており，FW の VPN 機能を用いて互いに接続されている。また，DMZ 上のサーバ群に対する不正なパケットは，IPS によって遮断している。

E 部長の説明を受け，V 氏は，ポリシとそれに関連する社内規程のほか，②K 社の現状の情報セキュリティ対策の具体的な内容を決定する際の根拠となった文書の提示を求めた。その上で，組織的な対策についてはポリシや社内規程などの文書の閲覧やヒアリングを中心とした監査手続を行うこと，技術的な対策についてはサーバなどに対する脆(ぜい)弱性検査を中心とした監査手続を行うことを説明した。

次は，打合せにおける V 氏，W 氏，E 部長及び F 主任の会話である。

F 主任：Web アプリの脆弱性検査（以下，Web 検査という）について一つ心配なことがあります。運用中の公開 Web サーバは取引先のほか，部品メーカや代理店

からのアクセスがあるので停止させることができません。Web 検査によって公開 Web サーバが停止するようなことはないでしょうか。

W 氏　：公開 Web サーバに負荷を掛けるような検査項目は実施しないようにすることもできますが，それ以外の検査項目によってシステムが停止してしまう可能性がないとはいえません。Web 検査以外の脆弱性検査でも，IPS の運用に影響が出る可能性があります。もし，どうしても運用中の公開 Web サーバで脆弱性検査を行うことが難しいという場合には，Y 社の開発系プラットフォームで Web 検査を実施することも考えられます。

E 部長：なるほど。それについては運用グループの意見を聞いて検討しましょう。

V 氏　：分かりました。ところで，以前の提案の席で，今回の監査対象には他社の営業秘密の取扱いを含めないということをお聞きしました。監査手続にも関係してきますので，どのような情報があるのか，可能な範囲でお聞かせいただけますか。

E 部長：他社の営業秘密には，部品に関するノウハウや，他社との共同開発に関する情報があります。技術サポート部では，部品メーカから部品に関するノウハウの開示を受けているほか，部品メーカと共同で製品メーカの製品開発に参加し，三者間で新製品の技術情報を共有しています。他社から開示される営業秘密は，他社との秘密保持契約に従って管理しています。

W 氏　：参考までに，具体的にはどのような管理をされていますか。

F 主任：当社の営業秘密と同様，営業秘密の要件を満たすよう管理しています。具体的には，技術サポート部の部門共有サーバに保管し，製品担当者や，共同開発のプロジェクトの単位でアクセス制限を行っています。他社の営業秘密を基に当社で作成した情報についても同様です。他社との営業秘密の受渡しは暗号化した上で CD-R に書き込み，担当者が手渡しで行っています。

なお，部品メーカ及び製品メーカとの秘密保持契約の遵守状況は毎年内部監査で確認しており，その結果は各メーカに説明しています。したがって，他社の営業秘密は今回の監査対象には含めていません。

その後，K 社との数度の打合せを経て，Z 社は，経済産業省の定めた情報セキュリティ管理基準に照らして，K 社の業務やポリシを考慮した監査項目と，表 1 に示す監査計画を作成し，K 社に提示した。

表1　K社の監査計画（概要）

実施日	実施場所	監査手続	内容
1日目	Z社	DMZスキャン	DMZ上のサーバ群に対するZ社からのインターネット経由でのポートスキャン及び脆弱性スキャンの実施
2日目，3日目	Y社	Web検査	開発系プラットフォーム上でのWebアプリの脆弱性検査の実施
4日目～6日目	K社本社	管理状況ヒアリング	本社各部門での組織的及び技術的対策に関するヒアリングと現地調査
		サーバ，端末及びネットワークの検査	サーバ及び端末の管理状況の検査，並びにポートスキャン及び脆弱性スキャンの実施
7日目	K社配送センタ	管理状況ヒアリング	配送センタでの組織的及び技術的対策に関するヒアリングと現地調査
		サーバ，端末及びネットワークの検査	サーバ及び端末の管理状況の検査，並びにポートスキャン及び脆弱性スキャンの実施
		無線LAN検査	無線LANの設定及び管理状況の検査

〔監査手続〕

監査計画に従って，Z社による監査手続が開始された。1日目はDMZ上のサーバ群に対してZ社のネットワークからポートスキャンと脆弱性スキャンを実施したが，特に問題は発見されなかった。

2日目と3日目は，V氏とW氏がY社に赴き，開発系プラットフォーム上でWeb検査を実施した。Web検査の主な検査項目と内容を表2に示す。

表2　Web検査の主な検査項目と内容

検査項目	検査する脆弱性の内容
オブジェクトの直接参照	存在を明示していないコンテンツやアプリケーションのデータファイルが，ディレクトリやファイル名，バックアップファイルなどを指定してアクセスされる脆弱性
e	HTML出力文字列のエスケープ処理が不適切な場合，攻撃者の作成した不正なリンクによってWebサイトを閲覧した利用者のブラウザ上でスクリプトが実行される脆弱性
f	利用者のブラウザによって，利用者の意図しないリクエストがWebサーバに送信され，ログイン中の利用者にだけ許可されたWebサイトの機能が勝手に実行される脆弱性
HTTPヘッダインジェクション	外部から渡されたパラメタをレスポンスのHTTPヘッダに反映する場合，不正なヘッダを生成されたり，レスポンスボディに不正な文字列を挿入されたりする脆弱性
SQLインジェクション・OSコマンドインジェクション	入力フォームのパラメタなどへの不正な文字列挿入によって，SQL文やOSのコマンドが不正に実行される脆弱性
不正メール送信	パラメタ文字列をメールヘッダに反映して電子メールを送信する場合，スパムメール送信などに利用される脆弱性
パス（ディレクトリ）トラバーサル	パス文字列の処理が不適切な場合，攻撃者の不正な入力によって，管理者がアクセスを想定していないファイルにアクセスされる脆弱性
不適切なセッション管理	クッキーなどを利用したセッション管理が不適切な場合，なりすましによる不正なアクセスが発生する脆弱性

Web 検査の結果，Web アプリの脆弱性として，不適切なセッション管理が行われていることが判明した。Web アプリには，SSL で保護された Web フォーム認証があり，利用者がパスワードを入力してログインすると，Set-Cookie ヘッダでセッション ID をブラウザに対して発行するようになっている。それ以降はセッション管理にこのセッション ID を利用するとともに，SSL による通信の暗号化が図られている。しかし，公開 Web サーバ内には SSL を利用していないページも存在し，HTTP 通信を盗聴することによってクッキーの情報を取得できることが判明した。この脆弱性を放置すると，[g] という攻撃手法によってなりすましによる不正アクセスが発生する可能性がある。

Web アプリ及び公開 Web サーバ以外では，Y 社の開発系プラットフォーム上の DB サーバに，数年前に K 社の本社 DB サーバに格納されていた顧客情報が格納されていることが判明した。

4 日目は本社の各部門での管理状況ヒアリングに移った。監査計画に従って，V 氏と W 氏は，まず情報システム部のヒアリングを行った。

次は，ヒアリングでの V 氏と E 部長の会話である。

V 氏　：顧客情報の取扱いについて，開発委託先である Y 社と何らかの取決めはされていますか。

E 部長：当社のシステム開発規程（以下，開発規程という）では，開発委託先との間の開発委託契約の中に，セキュリティに関する条項を含めることになっています。開発規程に従い，Y 社との開発委託契約には秘密保持条項を含めています。Y 社では，その秘密保持条項に従って顧客情報を適切に取り扱っているはずです。

V 氏　：秘密保持条項の内容について詳しくお話しいただけますか。

E 部長：漏えいや盗用を防止するための対策などが含まれていたと思います。

V 氏　：内容は後で拝見させていただきたいと思いますが，顧客情報を保護する観点から，必要に応じて開発規程と開発委託契約の内容を見直していただくことをお薦めします。

V 氏と W 氏が，E 部長から提示された開発規程と Y 社との開発委託契約を閲覧したところ，図 3 に示す，開発規程に定められている開発委託契約に関する要件が，開発委託契約の中に盛り込まれていることを確認した。

- 重要な情報の安全管理に関する事項
  - (a) 漏えいや盗用を防止するための対策の実施
  - (b) 委託範囲外での加工・利用・複製・複写の禁止
- 再委託に関する制限事項
- 重要な情報の取扱状況に関する K 社への報告の内容及び頻度
- 契約内容が遵守されなかった場合の措置に関する事項
- インシデントが発生した場合の報告・連絡に関する事項

図 3　開発規程に定められている開発委託契約に関する要件（一部）

5 日目，V 氏と W 氏は各部門での管理状況ヒアリングを終え，6 日目にかけて，K 社本社のサーバ，端末及びネットワークの検査に移った。技術サポート部の部門共有サーバとコールセンタの CC 端末を検査したところ，OS のセキュリティパッチの適用やウイルス対策など，セキュリティ対策の運用についても，ポートスキャン及び脆弱性スキャンについても特に問題は見当たらなかった。

7 日目は K 社配送センタでの監査手続に移った。V 氏と W 氏は，K 社配送センタのサーバ，HT 及び PC 並びにネットワークの管理状況についてヒアリングと技術的検査を実施したが，特に問題はなかった。

次に，V 氏と W 氏は表 3 に示す無線 LAN 検査に移った。

表 3　無線 LAN 検査の主な項目と内容

検査項目	検査内容
電波到達範囲検査	設置されている無線 AP の電波が屋外でどの程度の範囲で受信できるか確認する。
所有外無線 AP 検査	配送センタの内部で，K 社所有外の無線 AP 検出の有無を確認する。
無線 AP 設定情報確認検査	無線 AP の設定情報が設計どおりであることを確認する。
事前共有鍵強度検査	無線 AP と通信を行う HT の間で脆弱な事前共有鍵が使われていないことを確認する。

まず，電波到達範囲検査として，W 氏が検査用の PC を用いて配送センタの敷地を調査したところ，配送センタの敷地ほぼ全域にわたって，K 社所有の無線 AP の電波が通信を行うのに十分な強度で検出された。したがって，配送センタの敷地外にも無線 LAN の電波が到達しているものと推測された。

次いで，所有外無線 AP 検査に移った。配送センタのフロア内を移動して K 社以外の無線 AP 検出の有無を調べたところ，外壁近くでは微弱な電波が検出されたが，フロアの中心部ではほとんど検出されなかったので，K 社以外のアクセス可能な無線 AP は存在しないものと判断された。

無線 AP 設定情報確認検査では，K 社の設計資料と無線 AP の設定情報を突き合わせ，設計どおりに設定されていることを確認した。通信規格には WPA を採用し，認証方式に PSK を利用していた（以下，この通信規格と認証方式を併せて WPA-PSK という）。暗号化プロトコルには TKIP を利用しており，グループ鍵の更新間隔は 3,600 秒だった。

最後に，WPA-PSK で利用している事前共有鍵強度検査のために，W 氏は無線 AP と HT の間で取り交わされる無線パケットを取得した。辞書攻撃によって事前共有鍵の復元を試みる検査には時間が掛かることから，W 氏は取得したパケットのデータを Z 社に持ち帰って解析を行うこととし，V 氏と W 氏は K 社での監査手続を終了した。

〔監査報告会〕

表 1 の監査手続が終了して 1 か月後のある日，K 社で監査報告会が開かれた。この席で Z 社から提出された情報セキュリティ監査報告書を図 4 に示す。

情報セキュリティ監査報告書

（中略）

1. 検出事項
 (1) 受発注 Web システムにおけるセッション ID の取扱いに関する不備
 (2) 開発委託先 Y 社における顧客情報の取扱いの不備
 (3) 配送センタの無線 LAN における WPA-PSK 事前共有鍵の不備

2. 改善提言
 (1) 受発注 Web システムにおけるセキュリティ対策
  (1-a) ③セッション ID の取扱いに関するセキュリティ強化
 (2) 開発委託先に対する顧客情報の管理
  (2-a) ④顧客情報の取扱いに対する管理策の追加
 (3) 配送センタの無線 LAN のセキュリティ対策
  (3-a) WPA-PSK 事前共有鍵の強化
  (3-b) 無線 LAN 認証方式の強化

3. 検出事項と改善提言の詳細
（以下，省略）

図 4　情報セキュリティ監査報告書

V 氏が，受発注 Web システム及び配送センタのシステムに関連するポリシと対策はおおむね有効であるとの結論を述べた上で，W 氏が，今回の監査での検出事項と改善提言の内容を個々に説明していった。

その中で，W 氏は，K 社配送センタで利用していた WPA-PSK の 8 文字の事前共有鍵が辞書攻撃によって復元できたことを伝えた。その上で，辞書攻撃への防御のために，WPA-PSK の事前共有鍵では少なくとも 21 文字程度の文字列を使うことが推奨されていることを説明した。その理由として，W 氏は，受発注 Web システムでも利用している Web フォーム認証と比較しながら，⑤事前共有鍵を用いる WPA-PSK は，その仕組み上，同じ長さのパスワードによる Web フォーム認証に比べて辞書攻撃に弱いことを指摘した。

これに加え，無線 LAN のアクセス制御の方式自体についても，EAP-TLS や PEAP による相互認証が可能な，IEEE [h] によるアクセス制御に変更することを提言した。

この提言に対し，E 部長は，現在の HT ではハードウェア上の制約があるので WPA-PSK を利用しているが，来年にも予定している配送センタのシステム更改のときに，新たに認証サーバを設置し，IEEE [h] が利用できる HT を導入したいと述べた。

そこで，W 氏は更改までの暫定的な対応として，現行の認証・暗号化方式を前提に，WPA-PSK の事前共有鍵は十分な長さのものを利用し，定期的に変更することを推奨した。

最後に，V 氏は，監査結果に対するフォローアップの重要性について述べるとともに，今回の監査では対象としなかった情報資産についても，今後，外部監査を行うことを推奨し，監査報告会を締めくくった。

この監査結果は，経営会議で報告され，社長からは，監査結果のフォローアップを確実に行うようにとの指示があった。

その後，⑥K 社では今回の監査での検出事項に対するフォローアップ監査が実施され，情報セキュリティ対策の改善が有効に行われていることを確認することができた。

設問1　〔情報セキュリティの見直しと情報セキュリティ監査〕について，(1)，(2)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5字以内で答えよ。

(2) 本文中の下線①について，Y社に監査を依頼すべきではないとF主任が述べた理由を，監査の原則の観点から40字以内で述べよ。

設問2　〔Z社との事前打合せ〕について，(1)～(3)に答えよ。

(1) 本文中の［　d　］に入れる適切な法令を解答群の中から選び，記号で答えよ。

解答群

ア　金融商品取引法　　イ　個人情報保護法　　ウ　著作権法

エ　特許法　　オ　不正競争防止法

(2) 本文中の下線②に該当する文書は，情報セキュリティマネジメントの中で実施される，ある作業の結果として作成されるものである。その作業とは何か。10字以内で答えよ。

(3) Z社は，受発注Webシステムの安全性を損なわずに表1中のDMZスキャンを実施するために，IPSの設定を一時的に変更するようK社に依頼した。その変更内容を，40字以内で述べよ。

設問3　〔監査手続〕について，(1)，(2)に答えよ。

(1) 表2中の［　e　］，［　f　］に入れる，脆弱性を表す適切な用語を答えよ。

(2) 本文中の［　g　］に入れる適切な字句を，15字以内で答えよ。

設問4　〔監査報告会〕について，(1)～(4)に答えよ。

(1) 本文中の［　h　］に入れる適切な字句を，10字以内で答えよ。

(2) 図4中の下線③に対応するための改善策を，35字以内で述べよ。

(3) 図4中の下線④に対応するために，図3中の“重要な情報の安全管理に関する事項”に追加すべき内容を30字以内で述べよ。

(4) W氏が本文中の下線⑤のように述べたのはなぜか。解答欄に従い，“WPA-PSKでは，……のに対し，Webフォーム認証では，……から”というように，それぞれ40字以内で述べよ。

設問 5　監査終了後のフォローアップ監査と他社の営業秘密のセキュリティ管理について，(1)，(2) に答えよ。

(1)　本文中の下線⑥について，図 4 中の検出事項 (1) 及び (3) に対する改善が図られていることをフォローアップ監査の監査人が確認できる証拠（エビデンス）には，Z 社が実施した監査手続によって得られる証拠以外に，どのようなものがあるか。それぞれ 30 字以内で具体的に述べよ。

(2)　Z 社による情報セキュリティ監査の対象としなかった情報資産として，他社との共同開発に関する情報がある。この情報を取り扱うときの管理策を定めるプロセスで，K 社はどのようなことを実施したと考えられるか。60 字以内で具体的に述べよ。