問1　メールシステムの情報セキュリティ対策に関する次の記述を読んで，設問1～5に答えよ。

P社は，従業員数300名のソフトウェア開発会社である。P社の主要事業は，ソフトウェア製品の開発及びWebアプリケーションの受託開発である。P社には，人事総務部，情報システム部，営業部及びシステム開発部がある。

P社のネットワーク構成を図1に示す。

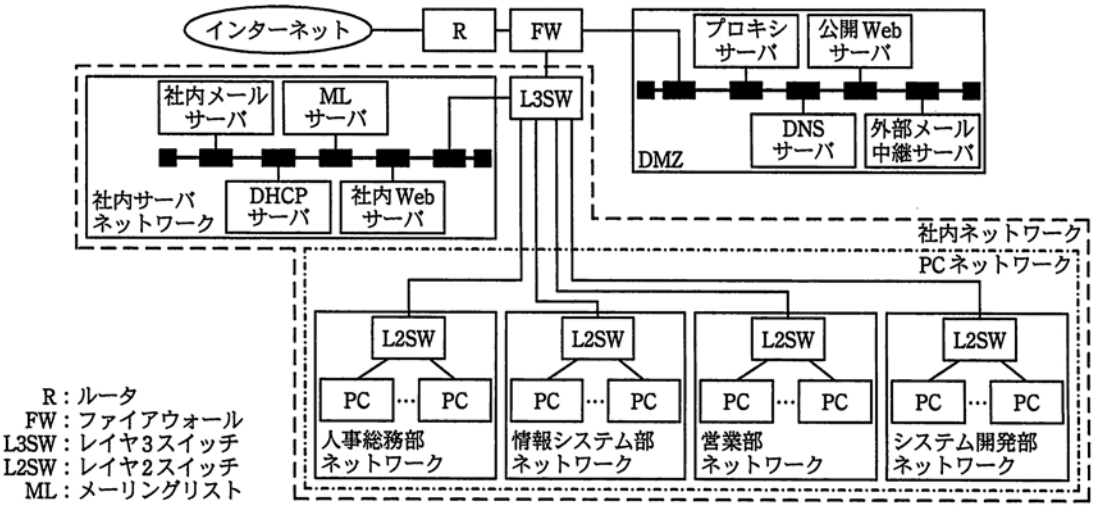

図1　P社のネットワーク構成

PCは，PCネットワークだけに接続されている。 PC へのIPアドレス割当ては，DHCPサーバ及びL3SWのDHCPリレーエージェント機能によって行われる。PCは，従業員がソフトウェア開発，資料作成，社内Webサーバへのアクセス，電子メール（以下，メールという）の送受信及びプロキシサーバ経由でのインターネットWebサイトの閲覧に使用している。P社では，各開発プロジェクト（以下，プロジェクトという）内の連絡にMLサーバを使用している。

FWのフィルタリングルール（以下，FWルールという）では，通信の送信元，あて先及びサービスの組合せによって，通信の許可又は拒否を指定している。FWルールを表1に示す。

FWでは，通信の許可及び拒否の状況をログとして記録している。各サーバでは，アクセス及びプログラムの動作結果をログとして記録している。

表1　FWルール

項番	送信元	あて先	サービス	動作
1	インターネット	外部メール中継サーバ	SMTP	許可
2	外部メール中継サーバ	インターネット	SMTP	許可
3	外部メール中継サーバ	社内メールサーバ	SMTP	許可
4	社内メールサーバ	外部メール中継サーバ	SMTP	許可
⋮	⋮	⋮	⋮	⋮
18	すべて	すべて	すべて	拒否

注記1　項番の小さいものから順に，最初に一致したルールが適用される。
注記2　項番5～17のFWルールは，SMTPに関連しないものである。

〔メールシステムの概要〕

P 社のメールシステムのサーバには，外部メール中継サーバ，社内メールサーバ及び ML サーバがある。それ以外のサーバ及び FW では，サーバ管理にメールを使用しているが，社外へのメールの送信は行わない。

P 社のメールアドレスのドメイン名には，P 社が取得したドメイン名（以下，P 社ドメイン名又は p-sha.cojp という）及びそのサブドメイン名（以下，P 社サブドメイン名という）を使用している。P 社ドメイン名は，各従業員に割り当てる従業員用メールアドレスのドメイン名と，postmaster や webmaster などをメールアドレスのローカル部として使用するサーバ管理用メールアドレスのドメイン名に使用している。P 社サブドメイン名は，ML アドレス用のドメイン名として使用する。ML アドレス用のドメイン名として，複数の P 社サブドメイン名の使用が可能である。現在は一つだけ作成し，使用している。P 社のメールアドレスのドメイン名及びメールアドレスは表 2 のとおりである。表 2 に基づいて DNS サーバの SPF（Sender Policy Framework）設定も行っている。

表２　Ｐ社のメールアドレスのドメイン名及びメールアドレス

種別	メールアドレスのドメイン名	メールアドレス
従業員用メールアドレス及びサーバ管理用メールアドレス	p-sha.co.jp	*user*@p-sha.co.jp [1]
ML アドレス	ml01.p-sha.co.jp	*project*@ml01.p-sha.co.jp [2]

注 [1] *user* は利用者やサーバ管理用途によって異なる。
[2] *project* はプロジェクトによって異なる。

外部メール中継サーバ，社内メールサーバ及び ML サーバには，オープンリレー対策が導入されている。オープンリレー対策では，表 3 に示すように，SMTP の転送元の IP アドレス又は IP アドレスブロック（以下，転送元 IP アドレスという）とメールの受信者ドメイン名の二つの組合せで，転送の許可又は拒否を判定する。受信者ドメイン名は，メールのエンベロープの受信者メールアドレスのドメイン名部分である。各メールサーバには，転送元 IP アドレスのうち受信者ドメイン名にかかわらずメールの転送を許可するもの（以下，許可アドレスリストという）が，登録されている。

表３　オープンリレー対策

転送元 IP アドレス	受信者ドメイン名	処理
許可アドレスリスト中のアドレス	社外のドメイン名	転送許可
	P 社ドメイン名 P 社サブドメイン名	転送許可
許可アドレスリスト以外のアドレス	社外のドメイン名	転送拒否
	P 社ドメイン名 P 社サブドメイン名	転送許可

社内メールサーバの許可アドレスリストには，PC ネットワークの IP アドレスブロックが登録されている。

転送が許可されたメールは，表 4 に示すように受信者ドメイン名ごとの処理が行われる。

表4　メールシステムの受信者ドメイン名ごとの処理

項番	サーバ	受信者ドメイン名	処理
1	外部メール中継サーバ	P社ドメイン名	社内メールサーバに転送
2		社外のドメイン名	DNSに登録されているメールサーバに転送
3		上記以外のドメイン名	転送を拒否
4	社内メールサーバ	P社ドメイン名	メールボックス保存プログラムに転送
5		P社サブドメイン名	MLサーバに転送
6		社外のドメイン名	外部メール中継サーバに転送
7		上記以外のドメイン名	転送を拒否
8	MLサーバ	P社ドメイン名	社内メールサーバに転送
9		P社サブドメイン名	同報プログラムに転送
10		上記以外のドメイン名	転送を拒否

社内メールサーバ及びPCにはウイルス対策ソフトが導入されている。社内メールサーバでのメール及びウイルス対策に関連した処理，並びにPCでのメール送受信処理は図2のとおりである。

(1) 社内メールサーバでのメール転送

［ a ］は，SMTPを使用し，メールを転送する。［ a ］のメール転送中に，ウイルス対策ソフトのウイルススキャン（以下，SMTPスキャンという）を行う。SMTPスキャンでウイルスを検知した場合，メール本文をウイルス検知通知に置き換える。次に，受信者ドメイン名ごとの処理を行う。

(2) 社内メールサーバでのメールボックス保存

P社ドメイン名あてのメールは，メールボックス保存プログラムである［ b ］によって，従業員用メールアドレス又はサーバ管理用メールアドレスごとのメールボックスに保存される。

(3) PCでのメール送受信

・メール送信

次の二つのどちらかを使用可能であるが，P社のPCでは(a)を使用している。

(a) PCの［ c ］は，SMTPで25番ポートを使用し，社内メールサーバの［ a ］にメールを送信する。

(b) PCの［ c ］は，SMTPで587番ポートを使用し，社内メールサーバの［ d ］にメールを送信し，［ d ］は，［ a ］にメールを転送する。

・メール受信

PCの［ c ］は，POP3を使用し，社内メールサーバのMRA（Mail Retrieval Agent）と通信し，従業員用メールアドレス又はサーバ管理用メールアドレスのメールボックスからメールを取り出す。

MRAのメール取り出し中に，ウイルス対策ソフトのウイルススキャン（以下，POP3スキャンという）を行うことも可能である。POP3スキャンでウイルスを検知した場合，メール本文をウイルス検知通知に置き換える。しかし，PCのウイルス対策ソフトに同等機能があるのでPOP3スキャンを使用していない。

(4) 社内メールサーバのウイルス対策ソフトのウイルス定義ファイル更新

15分おきに，次の処理を自動的に実行する。

・プロキシサーバ経由で，インターネット上のウイルス対策ソフトベンダのWebサーバに未更新ウイルス定義ファイルがあるかを確認し，未更新ウイルス定義ファイルがある場合はダウンロードを行い，更新を行う。

この処理は，手動による実行も可能である。プロキシサーバでは，キャッシュする対象からウイルス対策ソフトベンダのWebサーバを外している。

図2　社内メールサーバ及びPCでの処理

ML の管理及び処理は図 3 のとおりである。

・プロジェクトごとに ML アドレスを割り当てる。
・プロジェクト開始時に，プロジェクト管理者は情報システム部に ML アドレスの割当てを申請する。情報システム部は，ML アドレス及び ML アドレスごとの管理機能の利用者 ID（以下，ML アドレス管理者 ID という）とパスワードを設定して，プロジェクト管理者に通知する。
・プロジェクト管理者は，ML アドレスの管理機能を使用し，同報する受信者メールアドレス（以下，同報メールアドレスという）を同報リストに登録する。同報メールアドレスとして，従業員用メールアドレスだけが登録可能である。
・プロジェクト終了時に，プロジェクト管理者は情報システム部に ML アドレスの削除を申請する。情報システム部は，ML アドレス，ML アドレス管理者 ID 及び同報リストを削除する。
・ML サーバに ML アドレスあてのメールが届くと，同報プログラムが起動される。同報プログラムは，エンベロープの受信者メールアドレスを ML アドレスの同報リストの各同報メールアドレスに書き換えたメールを生成する。生成したメールを，SMTP を使用して社内メールサーバに転送する。

図 3　ML の管理及び処理

同報プログラムには，設定可能な項目があり，それら設定項目と現在の設定値は，表 5 のとおりである。

表 5　同報プログラムの設定項目と現在の設定値

設定項目名	説明	現在の設定値
ML アドレス管理者のメールアドレス	次のいずれかを選択する。 ・*project*-admin@p-sha.co.jp [1)] ・プロジェクト管理者の従業員用メールアドレス	プロジェクト管理者の従業員用メールアドレス
エンベロープの送信者メールアドレス	次のいずれかを選択する。 ・同報前のメールのエンベロープの送信者メールアドレス ・ML アドレス管理者のメールアドレス	同報前のメールのエンベロープの送信者メールアドレス
登録外メールアドレス制限	同報前のメールのヘッダの送信者メールアドレスが，登録された同報メールアドレス以外の場合にメールの同報を拒否する設定が可能である。	拒否する。
メールサイズ上限制限	あらかじめ設定した値を超える大きさのメールの同報拒否が可能である。	10M バイト

注 [1)]　*project* はプロジェクトごとに異なる。

〔PC の情報セキュリティ対策〕

PC には，表 6 に示す機能をもつウイルス対策ソフトが導入されている。PC 配布時には，各機能を利用できるように設定されている。

表 6　PC のウイルス対策ソフトの機能

機能の名称	機能の概要
ウイルス定義ファイル更新	PC 起動時及びその後 1 時間ごとに，次の処理を自動的に実行する。 ・プロキシサーバ経由で，インターネット上のウイルス対策ソフトベンダの Web サーバに未更新ウイルス定義ファイルがあるかを確認し，未更新ウイルス定義ファイルがある場合はダウンロードを行い，更新を行う。 この処理は，手動での実行も可能である。
定時スキャン	毎日，決められた時刻に PC の全ファイルのウイルススキャンを行う。ウイルスを検知した場合，ウイルスの駆除及びファイルの修復を行う。P 社では，正午に実行される。
メール送信スキャン	PC のメールソフトと連携し，メール送信時にウイルススキャンを行う。ウイルスを検知した場合，その通信を遮断する。
メール受信スキャン	PC のメールソフトと連携し，メール受信時にウイルススキャンを行う。ウイルスを検知した場合，メール本文をウイルス検知通知に置き換える。
⋮	⋮

P 社では，他社におけるメールアドレスの誤入力による情報漏えい事故の報道をきつかけに，情報漏えい対策の強化が必要であると認識し。情報システム部で対策を検討することにした。検討の結果，メールによる情報漏えいを防止する対策の一つとして，PC のメールソフトに装備されているあて先確認要求機能を使用することにした。この機能は図 4 のとおりである。

・環境設定
　あて先確認要求なしにメールの送信を許可するドメイン名（以下，許可済ドメイン名という）を社内 Web サーバに設定しておく。現在の許可済ドメイン名は表 2 のメールアドレスのドメイン名とすることにした。
・メールソフト起動時の処理
　メールソフト起動時に，社内 Web サーバから許可済ドメイン名をダウンロードし，PC に保存する。社内 Web サーバと通信ができない場合は，PC に許可済ドメイン名が保存されていたなら，それを参照する。
・メール送信時の処理
　メール送信時に，メールに入力した受信者メールアドレスのドメイン名と許可済ドメイン名とを照合する。一致した場合は，メールを送信する。一致しなかった場合は，受信者メールアドレスの確認を促すメッセージを表示する。確認ボタンを押すとメールを送信する。取消ボタンを押すと，メール編集画面に戻る。

図 4　メールソフトに装備されているあて先確認要求機能

〔PC のリプレースとメールソフト誤設定に関する対策の検討〕

情報システム部では，PC のリース期間満了に合わせ，部ごとに PC のリプレースを行っている。

人事総務部の PC のリプレースでは，新しい PC の導入並びに OS 及びソフトウェアの設定に用いる手順書（以下，PC 導入手順書という）を情報システム部が作成した後，PC の納入ベンダが PC 導入手順書に基づいて PC の導入を行い，人事総務部がパスワードの設定を行った。

人事総務部の PC のリプレースが完了した翌日，人事総務部の S さんから情報システム部に，“午前中にメールを 1 通送信したが，相手に届いたメールの送信者メールアドレスが，人事総務部の A さんとなっていた”との申告があった。情報システム部の L 部長は，部下の M 主任と N さんに調査を指示した。M 主任と N さんは，DHCP サーバのログ及び A さんと S さんのメールアドレスを調査した。続いて，①メールシステムのサーバのログを調査し　S さんの申告どおりであることを確認した。さらに，S さんの PC の調査を行った。調査結果を図 5 に示す。

(1)　DHCP サーバのログ
　S さんの PC に割り当てた IP アドレスを特定した。
(2)　メールアドレス
　A さん　ato.taro@p-sha.co.jp
　S さん　sato.taro@p-sha.co.jp
(3)　メールシステムのサーバのログ
　（省略）
(4)　S さんの PC の調査結果
　PC のメールソフトの送信者メールアドレスの設定において，A さんのメールアドレスが設定されていた。納入ベンダに確認したところ，メールアドレス設定ツールで使用する設定情報一覧の作成時に，S さんのメールアドレスの先頭の“s”の入力が漏れ，一覧作成後の確認においても入力ミスを発見できなかったとの説明であった。

図 5　調査結果

M 主任と N さんは，調査結果，対策及び再発防止策を L 部長に報告し，対策及び再発防止策は実施された。

〔ウイルス感染とその対策に関する検討〕

大型連休明け，営業部長から L 部長に，“B さんの PC がウイルス感染した可能性があり，ネットワークから切り離した”との連絡があった。L 部長は，M 主任と N さんに調査を指示した。M 主任と N さんは，PC の調査と対処を行った。調査結果と対処を図 6 に示す。

(1) B さんへの聴取結果
午前 8 時 40 分ごろ　PC をロッカーから取り出し，起動した後，席を離れた。
午前 8 時 50 分ごろ　自席に戻り，PC を営業部ネットワークに接続した。
午前 9 時 20 分ごろ　メールを受信した。
午前 9 時 30 分ごろ　受信したメールのうち，題名に“メールソフトについての重要なお知らせ”と書かれたメールを同僚の C さんのメールアドレスあてに，メールソフトの転送機能を使用して送信した。
午前 9 時 55 分ごろ　C さんから“B さんが送信したメールがウイルス検知通知メールに置き換わって届いた”と電話連絡があった。
(2) B さんの PC のウイルス対策ソフトの設定
PC 配布後，B さんは，メールの送信及び受信が遅いという理由で，メール送信スキャン機能及びメール受信スキャン機能を使用しない設定に変更していた。
(3) DMZ 及び社内サーバネットワークに設置されているサーバ群のログ調査結果
午前 8 時 50 分　B さんの PC に営業部ネットワーク用の IP アドレスを割り当てた。
午前 9 時 20 分　同 IP アドレスで，メール受信が行われた。
午前 9 時 30 分　同 IP アドレスからメール送信が行われ，社内メールサーバで SMTP スキャンが動作した。
午前 9 時 40 分　②同 IP アドレスからのリクエストで，ウイルス定義ファイルのダウンロードが行われた。
(4) ウイルス感染
当該メールには，X ウイルスが添付されており，B さんの PC はこのメールの受信時に X ウイルスに感染した。X ウイルスに対応したウイルス定義ファイルは，大型連休最終日にリリースされていた。
(5) 対処
緊急対応ツールによって X ウイルスの駆除とファイルの修復を行った。さらに，メール送信スキャン機能とメール受信スキャン機能を使用するよう設定した。
X ウイルスに関する注意喚起情報を社内 Web サーバに掲載した。

図 6　B さんの PC の調査結果と対処

M 主任と N さんは，情報セキュリティ対策についての支援を委託している T 社の U 氏に調査結果と対処を説明し，対策についての助言を求めた。N さんは，今後の対策として，PC の利用に当たって，PC を起動後，メール受信前に手動でウイルス定義ファイル更新をさせようと考えていることを説明した。U 氏は，③PC での対策以外に，メールシステムのサーバでの対策もあると助言した。この助言に従い，N さんは新たな対策案を作成した。

M 主任と N さんは，調査結果，対処及び新たな対策案を L 部長に報告し，対策は即日実施された。

〔ML に関する検討〕

システム開発部では，あるプロジェクトで受託開発の一部を協力会社に再委託することになり，協力会社との間でプロジェクトにおいて扱うドキュメントなどのファイ

ルを暗号化して送受信するために，同報メールアドレスに協力会社のメンバのメールアドレスも登録可能にしてほしいという要望が，システム開発部長からL部長に伝えられた。L部長は，M主任とNさんに社外メンバのメールアドレスも登録可能なML（以下，社外メンバ登録MLという）の検討を指示した。

M主任とNさんは，要望内容と表4を基に検討を行い，表7のメールシステムの受信者ドメイン名ごとの処理変更案を作成し，U氏に相談した。P社のシステムにほかの変更はない。

表7　メールシステムの受信者ドメイン名ごとの処理変更案

項番	サーバ	受信者ドメイン名	処理
1	外部メール中継サーバ	P社ドメイン名	社内メールサーバに転送
2		P社サブドメイン名	MLサーバに転送
3		社外のドメイン名	DNSに登録されているメールサーバに転送
4		上記以外のドメイン名	転送を拒否
5	社内メールサーバ	P社ドメイン名	メールボックス保存プログラムに転送
6		P社サブドメイン名	MLサーバに転送
7		社外のドメイン名	外部メール中継サーバに転送
8		上記以外のドメイン名	転送を拒否
9	MLサーバ	P社ドメイン名	社内メールサーバに転送
10		P社サブドメイン名	同報プログラムに転送
11		社外のドメイン名	外部メール中継サーバに転送
12		上記以外のドメイン名	転送を拒否

U氏は，M主任とNさんの考えも聞きながら，表7のメールシステムの受信者ドメイン名ごとの処理変更案を基にレビューし，指摘事項を図7にまとめた。

(A)　あて先確認要求機能について
　メールソフトでは社外メンバ登録MLアドレスあて送信時に，あて先確認要求なしにメールが送信される。
(B)　メールシステムの受信者ドメイン名ごとの処理変更案について
　表7には，誤りがある。
(C)　ウイルス対策について
　社外メンバ登録MLで同報されたメールがウイルスに感染していた場合に，同報リストに登録された協力会社のメンバに連絡する手段が決められていない。
(D)　迷惑メールと判定されることについて
　協力会社のメールサーバが，迷惑メールの判定にSPFを使用している場合，P社からのメールが迷惑メールと判定されることがある。

図7　指摘事項

まず，M主任とNさんは，図7の(A)について検討し，④メールアドレスのドメイン名の使用方法も含めてMLサーバの設定を見直すとともに，社内Webサーバでの許可済ドメイン名の設定ルールとして明示する案を作成した。さらに，この見直しに伴うDNSサーバのSPF設定の変更は不要であることを確認した。U氏は，図7の(A)が解決されることを確認した。

次に，M主任とNさんは，図7の(B)について検討し，⑤表7の処理を2か所修正

し，社内メールサーバの許可アドレスリストに [e] の IP アドレスを追加する案を作成した。U 氏は，図 7 の(B)が解決されることを確認した。

続いて，M 主任と N さんは図 7 の(C)について検討し，連絡手段をメールとする案を作成した。U 氏は，⑥連絡手段をメール以外の方法とするように助言した。M 主任と N さんは，U 氏の助言に従い，発信者番号を通知した電話で連絡する案に修正した。

さらに，M 主任と N さんは図 7 の(D)について協力会社での SPF 利用状況について確認し，問題があるということが分かったので，対策を検討し，⑦ML サーバの設定を変更する対策案を作成した。U 氏は，図 7 の(D)が解決されることを確認した。

M 主任と N さんは，社外メンバ登録 ML の実現案を L 部長に説明した。L 部長は，システム開発部には複数のプロジェクトを担当している部員がいるので，社外メンバ登録 ML アドレスの取り違えによるメールの誤送信が起こる可能性があると指摘した。プロジェクトにおける情報交換での情報漏えい対策(以下，情報交換対策という)も併せて導入する条件で社外メンバ登録 ML の実現案を承認した。

〔情報交換対策に関する検討〕

M 主任と N さんは U 氏とともに，情報交換対策の検討を行った。U 氏は，P 社のメールシステムにおいては，社外メンバ登録 ML アドレスの取り違えによるメールの誤送信の防止が難しいことを指摘した。

検討の結果，次のような案を作成した。

社外メンバ登録 ML アドレスは，プロジェクトでの連絡手段としてだけ使用させ，ドキュメントなど重要情報の送信には使用させない。そこで，社外メンバ登録 ML アドレスあてのメールにファイルが添付されていたら，転送を拒否する機能をメールシステムに設定する。

メールによる情報交換の代替手段として，情報交換のための Web サーバ(以下，PJWeb サーバという）を DMZ に導入する。PJWeb サーバでは，利用者の認証を行い，ドキュメントなどのアップロード及びダウンロードによる情報交換を実現する。加えて，アクセス状況をログとして記録する。 PJWeb サーバへの通信を FW で制限する。⑧これらのほかに、メールシステムの機能及び利用計画を踏まえ、PJWeb サーバに必要な情報セキュリティ機能を追加する。

PJWeb サーバの運用は，次のようにする。

プロジェクト管理者は，プロジェクト開始時にプロジェクトの名称，期間，協力会社情報，メンバなどのプロジェクト情報を添えて登録申請を行い，プロジェクト終了時に削除申請を行う。情報システム部は，申請内容に基づき，PJWeb サーバへの利用者 ID，パスワード及び格納領域の登録又は削除設定を行う。さらに，DMZ に設置されているサーバと同様に，定期的な PJWeb サーバの脆弱性検査及び修正プログラムの適用を行う。⑨これらのほかに，情報システム部は，PJWeb サーバの情報セキュリティ対策にかかわる運用も行う。

M 主任と N さんは，この情報交換対策案を L 部長に説明し，承認を得た。3 か月後，情報交換対策は導入され，社外メンバ登録 ML の運用が開始された。

設問 1　〔メールシステムの概要〕について，図 2 中の [a] ～ [d] に入れる適切な字句を解答群の中から選び，記号で答えよ。

解答群

ア　MDA（Mail Delivery Agent）　　イ　MSA（Mail Submission Agent）

ウ　MTA（Mai1Transfer Agent）　　エ　MUA（Mail User Agent）

設問 2　〔PC のリプレースとメールソフト誤設定に関する対策の検討〕について，(1)，(2) に答えよ。

(1) PC のメールソフトの送信者メールアドレスを誤って設定しても，社内メールサーバが PC のメールソフトからのメールの送信を拒否しない理由を，40 字以内で述べよ。

(2) 本文中の下線①のログ調査結果を得るために調査したサーバの名称を図 1 中の字句を用いて答えよ。また，確認した内容を 50 字以内で述べよ。

設問 3　〔ウイルス感染とその対策に関する検討〕について，(1)，(2) に答えよ。

(1) 図 6 中の下線②のログ調査結果を得るために調査したサーバの名称を図 1 中の字句を用いて答えよ。

(2) 本文中の下線③について，U 氏が助言した対策を 30 字以内で述べよ。

設問 4　〔ML に関する検討〕について，(1) ～ (5) に答えよ。

(1) 本文中の下線④について，ML サーバの設定の見直し案を 45 字以内で，許可済ドメイン名の設定ルール案を 35 字以内で述べよ。

(2) 本文中の下線⑤について，表 7 中の修正箇所 2 か所の項番と修正後の処理を答えよ。

(3) 本文中の [e] に入れる適切なサーバの名称を図 1 中の字句を用いて答えよ。

(4) 本文中の下線⑥について，U 氏が連絡手段をメール以外の方法に変更するように助言した理由を 40 字以内で述べよ。

(5) 本文中の下線⑦について，SPF によって P 社からのメールが迷惑メールと判定されないために ML サーバの設定を変更する対策案を 50 字以内で述べよ。

設問 5　〔情報交換対策に関する検討〕について，(1)，(2) に答えよ。

(1) 本文中の下線⑧について，PJWeb サーバに必要な情報セキュリティ機能として追加すべきもののうち，情報漏えい対策に効果があるものを二つ挙げ，具体的な内容を，それぞれ 40 字以内で述べよ。

(2) 本文中の下線⑨について，PJWeb サーバの情報セキュリティ対策のうち，情報漏えい対策として，情報システム部が行うべき運用方法を，想定するリスクを含めて，60 字以内で具体的に述べよ。

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。

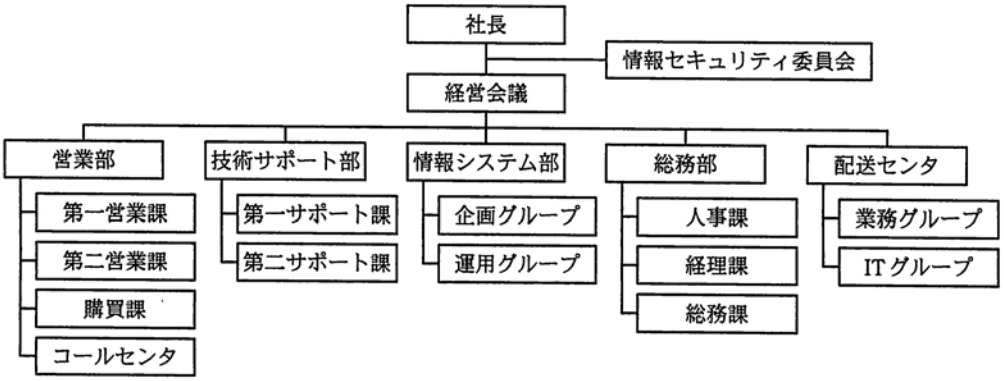

図１　K社の組織

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時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。

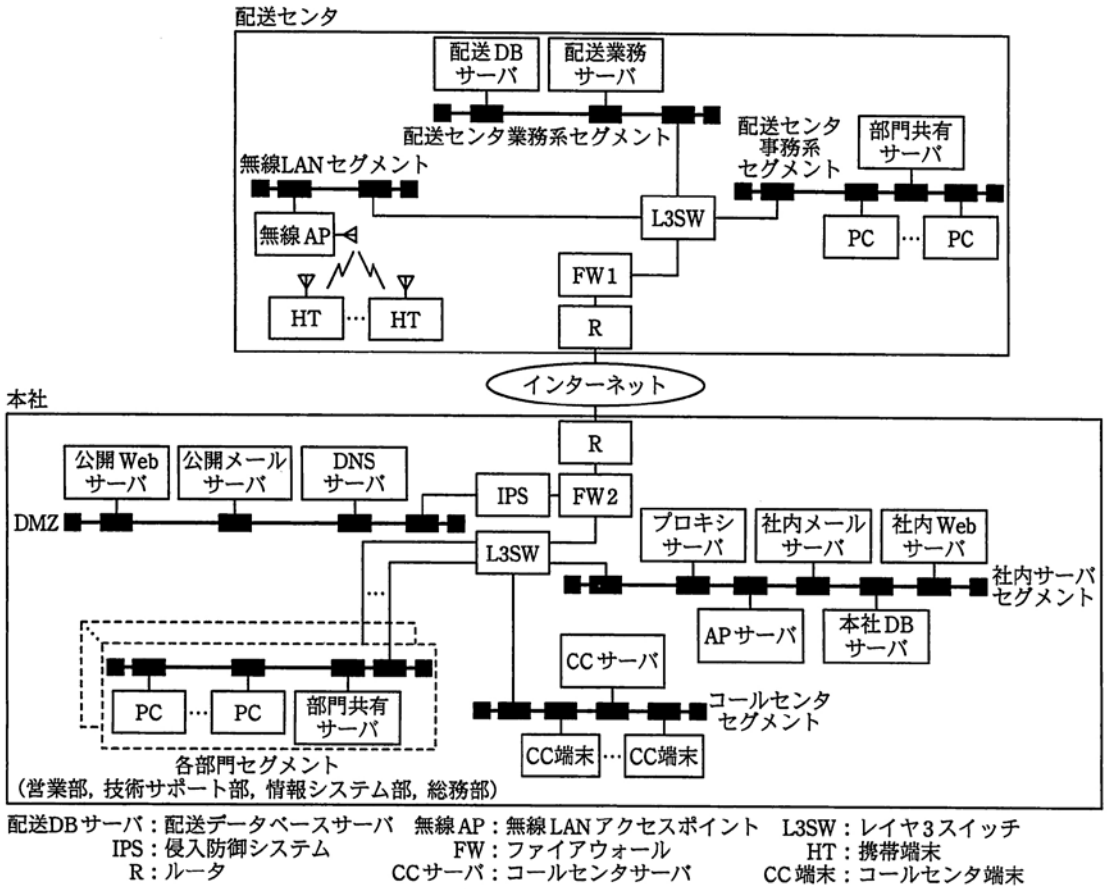

図２　K社の情報システムの構成

(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 を使用し，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，IEIEE [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。

解答例

問 1

出題趣旨

電子メールは，コミュニケーションに有用かつ必須な手段となっている。 しかし，メール誤送信による情報漏えいやウイルス感染の危険性がある。さらに，メーリングリストにおける同報機能によって危険性が高まり，情報セキュリティ対策が重要となる。

本問では，メールシステムの情報漏えい対策の強化を題材にして，電子メールに関する知識と設計能力及びメールシステムに関する情報セキュリティ対策の実施能力を問う。

設問 l　a　ウ
　　b　ア
　　c　エ
　　d　イ

設問 2　(1) 送信者メールアドレスは，送信の許可と拒否の判定には使用しないから

(2) **サーバの名称**　社内メールサーバ
　　確認した内容　S さんの PC の IP アドレスから，送信者メールアドレスが A さん用であるメールを送信したこと

設問 3　(1) プロキシサーバ

(2) 社内メールサーバの POP3 スキャンを使用する。

設問 4　(1)　**見直し案**　社外メンバ登録 ML のドメイン名として，新たな P 社サブドメイン名を使用する。
　　設定ルール案　社外メンバ登録 ML のドメイン名を許可済ドメイン名に含めない。

(2)　①　**項番**　2
　　修正後の処理　社内メールサーバに転送
　　②　**項番**　11
　　修正後の処理　社内メールサーバに転送
（①，②は順不同）

(3) e　ML サーバ

(4) メールからウイルスが広まった場合，メールを連絡手段として使えなくなるから

(5) エンベロープの送信者メールアドレスに ML アドレス管理者のメールアドレスを設定する。

設問 5　(1) ①・アップロード時に，情報の取り違えに関する表示を行い，確認を促す機能
　　②・プロジェクトごと及び利用者ごとのアクセス権限を設定する機能
　　・PJWeb サーバへの通信を暗号化する機能
　　・アップロードされたドキュメントを一定時間の経過後に削除する機能

(2)・プロジェクト終了後，削除申請されないと PJWeb サーバを不正に利用されるので，プロジェクト管理者に確認を行う。
　　・PJWeb サーバのアクセスログを定期的に分析し，不正なアクセスの有無を確認する。

問 2

出題趣旨

組織体の情報資産に関わるリスクのマネジメントを効果的に実施する手法として，情報セキュリティ監査がある。情報セキュリティ監査人による独立かつ専門的な立場からの検証又は評価によって，組織体のマネジメントの向上を図ることが可能となる。

本問は，専門商社における情報セキュリティ監査を題材に，情報セキュリティ監査制度の知識，Web アプリケーション検査の技術，無線 LAN の強化，セキュリティ改善の手法などについて問う。

設問 1　(1) a　助言
　　b　保証
　　c　企業台帳
　(2) Y 社は K 社の開発委託先であり，監査の独立性を確保することが難しいから

設問 2　(1) d　オ
　(2) リスクアセスメント
　(3) Z 社の IP アドレスからのスキャンは遮断の対象としない。

設問 3　(1) e　クロスサイトスクリプティング
　　f　クロスサイトリクェストフォージェリ
　(2) g　セッションハイジャック

設問 4 (1) h　802.1X
　(2) セッション管理用のクッキーに secure 属性を付与する。
　(3)・テスト時の実データの利用禁止
　　・顧客情報の確実な返還，削除又は廃棄
　(4) **WPA-PSK では，**一度情報を傍受された後は無線 AP に接続せず高速に試行を繰り返されてしまう**のに対し，**
　　Web フォーム認証では，攻撃を受けた場合，後続する試行を遅らせることができる**から**

設問 5　(1) **検出事項（1）**・受発注 Web システムの改修に関する計画書
　　・受発注 Web システムの受入れテストの結果
　　検出事項（3）・無線 AP 及び HT の事前共有鍵変更に関する作業の記録
　　・配送センタのシステム更改に関する計画書
　(2)・他社から求められたセキュリティ要件が K 社の管理策のレベルを超える場合，リスク分析を実施して他社と対応を協議する。
　・ある会社の営業秘密が，K 社を経由して他の会社に漏えいしないよう，秘密保持契約の内容を検討する。

採点講評

問 1

問 1 では，メールシステムの情報漏えい対策の強化を題材にして，電子メールに関する知識，設計能力及び Web サーバの情報セキュリティ対策について出題した。全体として，正答率は想定どおりだった。

設問 2 は，正答率が高かった。メールのオープンリレーに関する理解が高いことがうかがわれた。

設問 4(2)は，正答率が低かった。問題中の記述と図表をよく読めば正答を導けるはずである。メールシステムの設計においては，メール機能以外の条件も考慮する必要があることを理解しておいてほしい。

設問 4(5)は，エンベロープについての言及がない解答が目立った。 SPF (Sender Policy Framework)は迷惑メールに対する有効な対策である。 SPF の仕組みをよく理解しておいてほしい。

設問 5(2)は，情報漏えい対策として，情報システム部が行うべき運用方法についての解答を求めたにもかかわらず，機能を述べた解答が目立った。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い。

問 2

問 2 では，無線 LAN や Web アプリケーションに関する技術的対策や，PDCA サイクルに代表されるマネジメント面での対策を題材にして，企業における情報セキュリティ監査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(1)は，正答率が低かった。平成 15 年に経済産業省の情報セキュリティ監査制度が開始されてから既に 8 年が経過しているが，受験者の知識がまだ不十分であることがうかがわれた。

設問 4(2)は，HTTPS と HTTP でクッキーを使い分けるという解答や，全てのページを暗号化するという解答が多かったが，それに加えて HTTPS で利用するクッキーに secure 属性を付与することまで踏み込んだ解答は少なかった。セッション管理は Web アプリケーションの技術的セキュリティ対策において重要な要素なので，代表的な対策についてよく理解しておいてほしい。

設問 5(2)は，管理策を策定するプロセスについての解答を求めたにもかかわらず，管理策を策定した後の実施状況の確認や内部監査について述べた解答が目立った。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い。