SG

平成31年度　春期
情報セキュリティマネジメント試験
午後　問題

試験時間	12:30 ～ 14:00（1時間30分）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. **答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。**
4. 問題は，次の表に従って解答してください。

問題番号	問1 ～ 問3
選択方法	全問必須

5. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) 答案用紙は光学式読取り装置で読み取った上で採点しますので，B 又は HB の黒鉛筆で答案用紙の**マークの記入方法**のとおりマークしてください。マークの濃度がうすいなど，**マークの記入方法**のとおり正しくマークされていない場合は読み取れないことがあります。特にシャープペンシルを使用する際には，マークの濃度に十分注意してください。訂正の場合は，あとが残らないように消しゴムできれいに消し，消しくずを残さないでください。
   (2) **受験番号欄**に**受験番号**を，**生年月日欄**に**受験票の生年月日**を記入及びマークしてください。答案用紙の**マークの記入方法**のとおり記入及びマークされていない場合は，採点されないことがあります。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入及びマークしてください。
   (3) **解答**は，次の例題にならって，**解答欄**にマークしてください。答案用紙の**マークの記入方法**のとおりマークされていない場合は，採点されません。

〔例題〕　次の［　　］に入れる適切な字句を，解答群の中から選べ。

春の情報処理技術者試験は，［ a ］月に実施される。

解答群　ア 2　　イ 3　　ウ 4　　エ 5

適切な字句は“ウ 4”ですから，次のようにマークしてください。

例題	a	ア	イ	●	エ	オ	カ	キ	ク	ケ	コ

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

全問が必須問題です。必ず解答してください。

問1　サイバー攻撃を想定した演習に関する次の記述を読んで，設問1～4に答えよ。

W 社は，自動車電装部品，ガス計測部品及びソーラシステム部品を製造する従業員数 1,000 名の企業である。経営企画部，人事総務部，情報システム部，調達購買部などのコストセンタ並びに自動車電装部，ガス計測部，及び昨年新規事業として立ち上げられたソーラシステム部の三つのプロフィットセンタから構成されている。ソーラシステム部は現在 30 名の組織であるが，事業を拡大させるために，毎月，3～4 名の従業員を採用しており，組織が拡大している。

W 社では，7 年前に最高情報セキュリティ責任者（CISO）を委員長とする情報セキュリティ委員会を設置し，情報セキュリティポリシ及び情報セキュリティ関連規程を整備して，ISMS 認証を全社で取得した。経営企画部が，情報セキュリティ委員会の事務局を担当している。また，各部の部長が，情報セキュリティ委員会の委員，及び自部における情報セキュリティ責任者を務めている。各情報セキュリティ責任者は，自部の情報セキュリティに関わる実務を担当する情報セキュリティリーダを選任している。

W 社は年に 1 回，人事総務部が主管となり，大規模な震災などを想定した事業継続計画の演習を実施している。サイバー攻撃を想定した演習は実施したことがないものの，サイバー攻撃などの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）の対応手順はあり，これまで，事業に深刻な影響を与えるようなサイバー攻撃は受けていない。

〔ソーラシステム部の状況〕

ソーラシステム部では，省エネルギーを推進しており，部で使用する全ての PC には，消費電力の少ないノート PC（以下，NPC という）を選定している。省エネルギー対策の一つとして，全ての NPC は，カバーを閉じると自動的にスリープモードに切り替わるように設定されている。また，情報セキュリティ対策の一つとして，全ての NPC では，USB ストレージなどの外部記憶媒体を使用できないように技術的対策を講じている。

ソーラシステム部の情報セキュリティ責任者は E 部長で，情報セキュリティリーダは F さんである。F さんは，最近，競合他社がサイバー攻撃を受け，その対応に手

間取って大きな被害が発生したとのニュースを聞いた。そこで，F さんは，ソーラシステム部内でサイバー攻撃を想定した演習を行うことを提案した。E 部長は提案を承認し，F さんに演習を計画するように指示した。

〔演習の計画〕

サイバー攻撃を想定した演習は，年 1 回行うことにした。演習は，一般的に表 1 に示すような机上演習と機能演習の 2 種類に大別される。機能演習の具体的な形式には，実際のサイバー攻撃に近い形で疑似的なサイバー攻撃を行う［　a　］が含まれる。

表 1　サイバー攻撃を想定した演習の種類

種類	説明	主な目的	具体的な形式
机上演習	議論主体の演習である。参加者の緊急時における役割，及び特定の緊急時の対応策について議論する。	参加者に気付きを与える。	・ワークショップ ・ゲーム
機能演習	作業主体の演習である。参加者の緊急時における役割及び責任を，シミュレーション環境で実践する。	作業手順，社内システム，代替施設などが適切に機能することを検証する。	・サイバーレンジトレーニング ・［　a　］

注記　本表は，NIST SP 800-84 や HSEEP（Homeland Security Exercise and Evaluation Program）などを基に，W 社が独自に作成した。

F さんは，机上演習と機能演習を比較検討した結果，今回は，参加者に気付きを与えられる机上演習として，ワークショップを実施することにした。演習終了後には，参加者からの意見を集めて次回の演習に反映することにした。

F さんは，机上演習のシナリオを検討するに当たり，サイバーキルチェーンを参考にすることにした。サイバーキルチェーンとは，サイバー攻撃の段階を説明した代表的なモデルの一つである。サイバー攻撃を 7 段階に区分して，攻撃者の考え方や行動を理解することを目的としている。サイバーキルチェーンのいずれかの段階でチェーンを断ち切ることができれば，被害の発生を防ぐことができる。サイバー攻撃のシナリオをサイバーキルチェーンに基づいて整理した例を表 2 に示す。

表2　サイバー攻撃のシナリオをサイバーキルチェーンに基づいて整理した例

段階	サイバー攻撃のシナリオ
1　偵察	①インターネット上の情報を用いて組織や人物を調査し，攻撃対象の組織や人物に関する情報を取得する。
2　武器化	攻撃対象の組織や人物に特化したエクスプロイトコード[1]やマルウェアを作成する。
3　配送	マルウェア設置サイトにアクセスさせるためになりすましの電子メール（以下，電子メールをメールという）を送付し，本文中の URL をクリックするように攻撃対象者を誘導する。
4　攻撃実行	攻撃対象者をマルウェア設置サイトにアクセスさせ，エクスプロイトコードを実行させる[2]。
5　インストール	攻撃実行の結果，攻撃対象者の PC がマルウェア感染する。
6　遠隔制御	（省略）
7　目的の実行	探し出した内部情報を圧縮や暗号化などの処理を行った後，もち出す。

注記　本表は，JPCERT コーディネーションセンター“高度サイバー攻撃への対処におけるログの活用と分析方法”などを基に，W 社が独自に作成した。

注[1]　脆弱性を悪用するソフトウェアのコードのことであり，攻撃コードとも呼ばれる。

[2]　この段階では，攻撃対象者の PC はマルウェア感染していない。

F さんは，次の二つの演習のシナリオを取り上げることにした。

シナリオ 1　標的型メール攻撃のシナリオである。W 社の取引先をかたった者から，W 社の公開 Web サイトが停止しておりアクセスできない旨の報告をメールで受信した。メールの本文には，W 社の公開 Web サイトを模した偽サイトの URL が記載されている。この場合の対応を行う。

シナリオ 2　標的型メール攻撃を受けた結果，マルウェア感染したというシナリオである。従業員の NPC のマルウェア対策ソフトからアラートが画面に表示された。アラートは，マルウェア感染らしき異常が認められたというものである。この場合の対応を行う。

シナリオ 1 は，表 2 の“ b1 ”の段階での対応であり，シナリオ 2 は，表 2 の“ b2 ”の段階での対応である。

〔演習の実施〕

演習にはソーラシステム部の全メンバが参加した。F さんは，メンバを会議室に招集し，参加者を三つのグループに分けて，ワークショップを実施した。ワークショ

ップでは，F さんは，ファシリテータとして，参加者に対して二つのシナリオを提示した。参加者はグループごとに，W 社のインシデント対応手順に従って取るべきアクションを議論し，発表した。W 社のインシデント対応手順は，図 1 のとおりである。

1　検知
・インシデント又はインシデントのおそれを発見した場合は，直ちに自部の情報セキュリティリーダに報告する。
2　エスカレーション
・上記 1 の報告を受けた情報セキュリティリーダは，情報セキュリティ責任者，情報システム部及び関連組織に報告する。
・社外の利害関係者に連絡する場合は，次の手順に従う。
（省略）
3　原因の特定
（省略）
4　一次対応
　情報セキュリティリーダは，上記 3 で特定した原因に対して，必要に応じて情報システム部や関連組織の協力を得ながら，次の一次対応を行う。
・マルウェア感染が疑われる場合は，感染が疑われる NPC などをネットワークから切り離すことを最優先に実施する。
・ランサムウェア感染が疑われる場合は，上記の一次対応に加えて，電源の強制切断 1) を実施する。
（省略）
5　証拠保全
　情報セキュリティリーダは，上記 4 を実施後，証拠として，W 社証拠保全ガイドに従って，情報システム部や関連組織の協力を得ながら，インシデントに関係するコンピュータ，デバイスなどの機器を，操作せずに保管する。
　なお，必要に応じて，②証拠保全した機器の調査を情報システム部が外部のセキュリティ専門業者に依頼することがある。
（省略）
6　その他
　情報セキュリティリーダは，上記 2～5 の対応に当たり，インシデントに至る経緯や対応を，適宜，記録する。
（省略）

注 1)　通常の OS 終了処理やスリープモードへの切替えはせずに，機器側から電源ケーブルを抜くこと。NPC の場合は，電源ケーブルを抜いた上でバッテリを外すことも含む。

図 1　インシデント対応手順（抜粋）

各グループのワークショップの発表結果は，表3のとおりである。

表3　ワークショップの発表結果

シナリオ	グループ1	グループ2	グループ3
1	標的型メール攻撃であるか否かを確認するために，メール本文中の URL をクリックする。クリック後，もし NPC に異常が認められたら，情報セキュリティリーダにインシデントとして報告する。異常が認められなければ，何もしない。	怪しいメールと判断し，メール本文中の URL はクリックしない。インシデントのおそれありと考えられるので，情報セキュリティリーダに報告する。	怪しいメールと判断し，メール本文中の URL はクリックしない。メールをごみ箱に移してから完全に削除する。インシデントのおそれありとは考えられないので，報告は不要と判断する。
2	NPC をネットワークから切り離す。もし，ファイルが勝手に暗号化されるような兆候が認められた場合は，次のようにする。 ・NPC から電源ケーブルを抜く。 ・再起動をしてから，NPC のカバーを閉じて，バッテリを外す。	NPC をネットワークから切り離す。もし，ファイルが勝手に暗号化されるような兆候が認められた場合は，次のようにする。 ・NPC から電源ケーブルを抜く。 ・通常の OS 終了処理は行わず，NPC のカバーを開いたまま，バッテリを外す。	NPC をネットワークから切り離す。もし，ファイルが勝手に暗号化されるような兆候が認められた場合は，次のようにする。 ・NPC から電源ケーブルを抜く。 ・通常の OS 終了処理は行わず，NPC のカバーを閉じて，バッテリを外す。

F さんは，シナリオ1及びシナリオ2について，適切な対応方法を参加者に解説した。その中で，参加者から，なぜ，通常の OS 終了処理ではいけないのかと質問を受けたので，③その理由について説明した。また，演習後に，参加者にアンケートを実施した。

こうして，F さんは，無事にワークショップを終えた。

〔演習結果の振り返り〕

F さんが演習中に参加者から受けた質問と F さんの回答は表 4 のとおりであった。

表 4　参加者からの質問及び F さんの回答（抜粋）

シナリオ	質問	F さんの回答
1，2	サイバーキルチェーンの各段階の対策例を知りたい。	“1 偵察”段階の対策としては，次が考えられる。 ・SNS 利用におけるルールを作成する。 ・ c1 ・ c2 （省略）
1	もし，W 社の偽サイトが発見された場合，会社としてどのような対応を行うのか。	取引先及び顧客が被害に遭わないようにするために，次の対応を行う。 ・ d1 ・ d2 （省略）
2	（省略）	（省略）

〔演習結果の報告〕

F さんは，演習結果，参加者からの質問及び意見，インシデント対応手順の改善案並びに次回の演習に向けての改善案をまとめ，E 部長に報告した。また，F さんは，④ソーラシステム部の組織の状況などを考慮すると，年 1 回の演習だけでは十分とはいえないと考えて，演習の頻度を上げることを E 部長に提案した。E 部長は，F さんからの提案を受け，演習結果とあわせて提案内容を情報セキュリティ委員会に提出した。

情報セキュリティ委員会は，E 部長からの提案を受けて，全社としても，サイバー攻撃を想定した演習を実施することにした。

その後，ソーラシステム部は，大きなインシデントの被害もなく順調に事業を拡大し，W 社全体としても，更なる情報セキュリティの強化を図ることができた。

設問1　〔演習の計画〕について，(1) ～ (3) に答えよ。

(1) 本文中及び表 1 中の［ a ］に入れる具体的な形式はどれか。解答群のうち，最も適切なものを選べ。

a に関する解答群

ア　広域災害対策演習　　イ　情報セキュリティ監査
ウ　脆弱性診断　　エ　パンデミック対策演習
オ　ビジネスインパクト分析　　カ　ファジングテスト
キ　ホワイトボックステスト　　ク　マルウェア解析
ケ　リバースエンジニアリング　　コ　レッドチーム演習

(2) 表 2 中の下線①について，次の (i) ～ (v) のうち，該当する行為だけを全て挙げた組合せを，解答群の中から選べ。

(i) 攻撃者が，WHOIS サイトから，W 社の情報システム管理者名や連絡先などを入手する。

(ii) 攻撃者が，W 社の公開 Web サイトから，HTML ソースのコメント行に残ったシステムのログイン情報などを探す。

(iii) 攻撃者が，W 社の役員が登録している SNS サイトから，攻撃対象の人間関係や趣味などを推定する。

(iv) 攻撃者が，一般的な Web ブラウザからはアクセスできないダーク Web から，W 社のうわさ，内部情報などを探す。

(v) 攻撃者が，インターネットに公開されていない W 社の社内ポータルサイトから，会社の組織図や従業員情報，メールアドレスなどを入手する。

解答群

ア (i), (ii), (iii)　　イ (i), (ii), (iii), (iv)　　ウ (i), (ii), (iii), (v)
エ (i), (ii), (iv)　　オ (i), (ii), (iv), (v)　　カ (i), (iii), (iv), (v)
キ (i), (iv), (v)　　ク (ii), (iii), (iv), (v)　　ケ (ii), (iii), (v)
コ (iii), (iv), (v)

(3) 本文中の［ b1 ］，［ b2 ］に入れる段階の組合せはどれか。b に関する解答群のうち，最も適切なものを選べ。

b に関する解答群

	b1	b2
ア	1 偵察	2 武器化
イ	2 武器化	3 配送
ウ	2 武器化	4 攻撃実行
エ	3 配送	4 攻撃実行
オ	3 配送	5 インストール
カ	4 攻撃実行	5 インストール
キ	4 攻撃実行	6 遠隔制御
ク	5 インストール	6 遠隔制御
ケ	5 インストール	7 目的の実行
コ	6 遠隔制御	7 目的の実行

設問2 〔演習の実施〕について，(1) ～ (4) に答えよ。

(1) 図1中の下線②を表すものはどれか。解答群のうち，最も適切なものを選べ。

解答群

ア Web アプリケーションの脆弱性診断

イ 技術動向の監視

ウ 従業員の情報セキュリティ教育や啓発

エ セキュリティ製品やソリューションの評価

オ セキュリティツールの開発

カ ディジタルフォレンジックス

(2) 表 3 のシナリオ 1 の発表結果について，W 社のインシデント対応手順に沿った対応であるか否かを示す組合せはどれか。解答群のうち，最も適切なものを選べ。ここで，“正”は手順に沿った対応であることを示し，“誤”は手順に沿った対応ではないことを示す。

解答群

	グループ 1	グループ 2	グループ 3
ア	誤	誤	誤
イ	誤	誤	正
ウ	誤	正	誤
エ	誤	正	正
オ	正	誤	誤
カ	正	誤	正
キ	正	正	誤
ク	正	正	正

(3) 表 3 のシナリオ 2 の発表結果について，W 社のインシデント対応手順に沿った対応であるか否かを示す組合せはどれか。解答群のうち，最も適切なものを選べ。ここで，“正”は手順に沿った対応であることを示し，“誤”は手順に沿った対応ではないことを示す。

解答群

	グループ 1	グループ 2	グループ 3
ア	誤	誤	誤
イ	誤	誤	正
ウ	誤	正	誤
エ	誤	正	正
オ	正	誤	誤
カ	正	誤	正
キ	正	正	誤
ク	正	正	正

(4) 本文中の下線③の理由について，次の (i) ～ (v) のうち，該当するものを二つ挙げた組合せを，解答群の中から選べ。

(i) 通常の OS 終了処理を行うと，記憶媒体に異常が生じることがあるから

(ii) 通常の OS 終了処理を行うと，その間にもファイルが暗号化され，被害が拡大することがあるから

(iii) 通常の OS 終了処理を行うと，調査に必要な情報の一部が失われることがあるから

(iv) 通常の OS 終了処理を行うと，バッテリやマザーボードが故障することがあるから

(v) 通常の OS 終了処理を行うと，メーカのサポートを受けられなくなることがあるから

解答群

ア (i), (ii)	イ (i), (iii)	ウ (i), (iv)
エ (i), (v)	オ (ii), (iii)	カ (ii), (iv)
キ (ii), (v)	ク (iii), (iv)	ケ (iii), (v)
コ (iv), (v)		

設問３　〔演習結果の振り返り〕について，(1)，(2)に答えよ。

(1)　表4中の［ c1 ］，［ c2 ］に入れる，次の(i)～(vii)の組合せはどれか。c に関する解答群のうち，最も適切なものを選べ。

(i)　インシデント発生後に迅速な対応ができるように，社内に CSIRT を構築する。

(ii)　インターネット上の匿名掲示板などに社内情報を書き込まないように，従業員に対して情報セキュリティ教育を行う。

(iii)　攻撃者に有用な情報を渡さないように，外部のセキュリティ専門業者に，SNSや匿名掲示板などの監視を依頼する。

(iv)　攻撃者の偵察を検知するために，W 社の社内 Web サーバやプロキシサーバへのアクセス内容をログに記録する。

(v)　実行形式のファイルが添付されたメールを受信したら直ちに削除するように，従業員に対して情報セキュリティ教育を行う。

(vi)　情報漏えいの被害を低減させるために，W 社のファイルサーバのファイルを全て暗号化する。

(vii)　マルウェア感染の被害を低減させるために，W 社の全ての NPC に対して，マルウェア対策ソフトのマルウェア定義ファイルを更新する。

c に関する解答群

	c1	c2
ア	(i)	(ii)
イ	(i)	(vii)
ウ	(ii)	(iii)
エ	(ii)	(iv)
オ	(iii)	(iv)
カ	(iii)	(vi)
キ	(iv)	(v)
ク	(v)	(vi)
ケ	(v)	(vii)
コ	(vi)	(vii)

(2) 表 4 中の [d1] , [d2] に入れる，次の (i) ～ (v) の組合せはどれか。d に関する解答群のうち，最も適切なものを選べ。

(i) 偽サイトが閉鎖されるまでの間，W 社の公開 Web サイトを閉鎖する。

(ii) 偽サイトにアクセスしないように，その存在と危険性について外部に公表する。

(iii) 偽サイトにアクセスできないように，Web フィルタリングを設定する。

(iv) 偽サイトを攻撃するように，外部のセキュリティ専門業者に依頼する。

(v) 偽サイトを閉鎖するように，偽サイトの IP アドレスの割当てを管理しているプロバイダに依頼する。

d に関する解答群

	d1	d2
ア	(i)	(ii)
イ	(i)	(iii)
ウ	(i)	(iv)
エ	(i)	(v)
オ	(ii)	(iii)
カ	(ii)	(iv)
キ	(ii)	(v)
ク	(iii)	(iv)
ケ	(iii)	(v)
コ	(iv)	(v)

設問4　本文中の下線④について，F さんが考えた理由はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　ISMS 認証を取得しているから

イ　オフィスの省エネルギーを推進しているから

ウ　事業に深刻な影響を与えるようなサイバー攻撃を過去に受けたことがあるから

エ　プロフィットセンタであるから

オ　毎月，3～4 名の従業員を採用しているから

問2　企業における情報セキュリティ管理に関する次の記述を読んで，設問 1～4 に答えよ。

X 社は，機械製品及び産業用資材の輸入及び国内販売業務を行う従業員数 1,000 名の商社であり，機械営業部，資材営業部，総務部，情報システム部などがある。

X 社は，数年前に同業他社で発生した情報セキュリティ事故を機に，情報セキュリティ管理に力を入れるようになり，JIS Q 27001 に基づく情報セキュリティマネジメントシステム（以下，X 社 ISMS という）を構築し，ISMS 認証を取得している。

X 社 ISMS では，副社長である最高情報セキュリティ責任者（CISO）を委員長とする情報セキュリティ委員会を設置し，各部の部長が情報セキュリティ委員会の委員を務めている。また，各部の部長は自部の情報セキュリティリーダを指名する。情報セキュリティ委員会は X 社 ISMS の年間活動計画を決定する。

X 社 ISMS の活動の実務は，各部の情報セキュリティリーダから構成される ISMS ワーキンググループ（以下，ISMS-WG という）が行っている。ISMS-WG のリーダは，情報システム部の S 課長である。ISMS-WG は，年間活動計画に基づき活動するほか，X 社 ISMS 規程などの文書（以下，X 社 ISMS 文書という）の改定案の検討を行う。

〔X 社 ISMS の年間活動計画〕

4 月のある日，今年度初めての ISMS-WG 会合が開催され，その席上で，表 1 に示す X 社 ISMS の年間活動計画が提示された。また，6 月に実施される情報資産目録の見直しについて S 課長から説明があった。X 社 ISMS では各部において情報資産の名称，管理責任者，重要度，保管場所，保管期間を記した情報資産目録を作成し，毎年見直すことになっている。しかし，毎年見直し後に幾つかの記載の過不足が見つかっていることから，見直し後の記載に過不足がないことをよく確認するよう，改めて S 課長が ISMS-WG のメンバに対して注意を促した。

表1　X社ISMSの年間活動計画（抜粋）

時期	内容
5月	ISMS-WGメンバ向け情報セキュリティ教育の実施
6月	各部における①情報資産目録の見直し
8月	全社を対象にした情報セキュリティリスクアセスメントの実施及びリスク対応計画の策定
12月	従業員向け情報セキュリティ教育の実施
1月	X社ISMS規程の順守状況に関する内部監査の実施
3月	情報セキュリティ委員会への年間活動報告及び情報セキュリティ委員会の審議事項の取りまとめ
随時 1)	情報セキュリティリスクアセスメントの実施及びリスク対応

注 1)　業務若しくは情報資産の大きな変更，又は情報セキュリティインシデントが発生した場合。

〔販路拡大のための施策〕

最近になって，主な取引先である海外のY社が，新製品として個人向けの3Dプリンタ（以下，3DPという）を開発した。これまでX社は個人向けには製品を販売していなかったが，機械営業部では3DPの個人向け販売を販路拡大の機会と捉え，そのための施策を検討した。その結果を表2に示す。

表2　販路拡大のための施策

施策	内容
個人向け通信販売	インターネットを利用して，3DPの個人向け通信販売を行う。
X社Webサイトの改修	購入者が3DPの関連情報を参照したり利用者登録をしたりできるよう，X社Webサイトを改修する。
SNSによる情報提供	一般に広く使われている，短文の投稿及び写真の掲載が可能なSNSを利用し，新たに登録するX社公式アカウントを通じて3DPの使い方のコツ，ファームウェアの更新情報，利用事例などを紹介する。

機械営業部の情報セキュリティリーダであるT課長は，これらの施策に係る情報セキュリティリスクアセスメントの実施とリスク対応が必要と考え，S課長に相談したところ，表3のようなアドバイスを受けた。

表3　S課長のアドバイス

施策	アドバイス
個人向け通信販売	・通信販売の開始によって，②適用される法令への対応と，それに伴うX社ISMS文書の見直しが必要になる。 ・クレジットカードによる決済への対応として，次の二つの案が考えられる。 案1　X社Webサイトを改修し，X社でクレジットカード決済を行う。［　a　］への準拠が必要になるので，X社ISMSに管理策を追加する。 案2　通信販売は行うが，X社としてクレジットカード情報を非保持化する。クレジットカード決済には外部のオンラインショッピングサイトを利用する。
X社Webサイトの改修	（省略）
SNSによる情報提供	・X社ISMSにおいては，業務用PCでのSNSの利用が禁止されている。業務でSNSを利用するのであれば，SNSのリスクについて検討した上で，X社ISMS文書を見直す必要がある。

S課長のアドバイスを受け，T課長は個人向け通信販売については，案2を採用し，外部のオンラインショッピングサイトを利用するのがよいと考えた。利用するシステムの詳細が固まった後に改めて情報セキュリティリスクアセスメントを行い，ISMS-WGに確認してもらうことにした。

次に，S課長とT課長はSNSを利用した情報提供に起因するリスクについて検討することにした。S課長は，T課長に次のリスクを説明した。

リスク1　X社の従業員が，X社公式アカウントを用いてX社の信用及び評判を低下させるような投稿を行う。

リスク2　第三者がX社公式アカウントを装い，X社の信用及び評判を低下させるような投稿を行う。

リスク3　第三者がX社公式アカウントを乗っ取り，X社の信用及び評判を低下させるような投稿を行う。

S課長の説明を聞いたT課長は，機械営業部だけでこれらのリスクに対応することは困難と判断した。そこで，SNSを利用した情報提供に起因するリスクについては，全社的な対策を立案するようS課長に依頼した。

また，S課長は，業務外でのSNSの個人利用についても，次のようなリスクがあることをT課長に説明した。

リスク 4　X 社の従業員が，X 社の信用及び評判を損なうような不用意な投稿を行う。

リスク 5　X 社の従業員が，その投稿から③X 社及び従業員の情報を攻撃者に推測され，X 社に対する標的型攻撃の手掛かりにされるような不用意な投稿を行う。

これらのリスクを踏まえ，T 課長は，業務外での SNS の個人利用についても，従業員向けに何らかの指針を示すのがよいのではないかと S 課長に提言した。S 課長は，SNS の利用に関するルールを立案し，ISMS-WG で検討することにした。

〔SNS の利用に関する情報セキュリティ対策〕

数日後，S 課長は X 社公式アカウントの運用に関する情報セキュリティ対策の案を作成した。その内容を表 4 に示す。

表 4　X 社公式アカウントの運用に関する情報セキュリティ対策（案）

項目	内容
利用目的の限定	X 社公式アカウントの利用は，製品情報の発信，お客様からの問合せへの返信などの業務目的に限定する。
発信者の限定	X 社公式アカウントを利用する担当者（以下，SNS 担当者という）を限定する。
X 社からの公式な情報発信であることの明示	X 社公式アカウントについて，次の事項を実施する。 ・ b1 ・ b2 ・ b3
アカウント乗っ取りの防止	SNS 担当者に対して，次の事項を徹底させる。 ・ c1 ・ c2 ・ c3

また，S 課長は，SNS の個人利用に関する指針を策定し，12 月に実施する従業員向け情報セキュリティ教育の内容に含めることにした。SNS の個人利用を一律に禁止することは適切でないので，この指針では，法令及び雇用契約上の要求事項の観点から従業員が順守すべき事項と，SNS の利用に当たって従業員が実施することが推奨される事項に分けて記載することにした。その概要を表 5 に示す。

表5　SNSの個人利用に関する指針（概要）

項目	内容
順守すべき事項	SNSの個人利用においては，次の事項を順守する。 ・ d1 ・ d2 ・ d3 （省略）
推奨される事項	SNSの個人利用においては，次の事項を実施することが推奨される。 ・ e1 ・ e2 ・ e3 （省略）

X社公式アカウントの運用に関する情報セキュリティ対策及びSNSの個人利用に関する指針は，ISMS-WGでの検討を経て情報セキュリティ委員会において承認された。

〔オンラインショッピングサイトの利用〕

機械営業部は，大手通信販売業者であるZ社のオンラインショッピングサイト（以下，Zショップという）を利用して個人向けに3DP及びオプション品を販売することにした。Zショップでは，消費者向けサイト以外にも各出品者用にポータルサイトを提供している。

X社には，Z社からX社専用のポータルサイト（以下，X社ポータルという）へのアクセス権が付与され，X社ポータルを利用する業務担当者用アカウントを追加又は削除可能な管理者用アカウントが一つ設定された。この管理者用アカウントでは，X社ポータルの他の機能を利用する個々の業務担当者用アカウントの管理だけを行うことにした。X社ポータルで業務担当者用アカウントを追加すると，その業務担当者のメールアドレスに対して電子メールが送信され，初期パスワードの変更が促される。

X社ポータルで利用可能な機能とその内容を表6に示す。

表6　X社ポータルの機能と内容

機能	内容
商品登録	・Zショップに出品する商品の情報の登録，修正及び削除
在庫管理	・Zショップに出品した商品の在庫数及び販売価格の管理
受注管理	・Zショップで受注した商品の納期，配送先の氏名，住所などの受注情報の確認 ・受注情報のCSV形式でのダウンロード ・購入者への発送通知
売上管理	・取引ごとの売上情報の確認 ・Z社に支払う手数料及びZ社からの入金に関する情報（以下，決済情報という）の確認 ・売上情報及び決済情報のCSV形式でのダウンロード
アカウント管理	・X社ポータルにアクセスできる別の業務担当者用アカウントの追加 ・システム上の役割（以下，ロールという）の登録，削除 ・X社ポータルの機能と次のいずれかの利用権限の組合せの，ロールへの付与 編集：情報の閲覧，ダウンロード及び編集ができる。 閲覧：情報の閲覧はできるがダウンロードと編集はできない。 ・アカウントへのロールの設定

機械営業部では，X社ポータルで表7に示すロールを新たに登録することにした。

表7　X社ポータルに新たに登録するロールと主な作業

新たなロール	X社ポータルで行う主な作業
商品担当者ロール	・出品する商品の情報を管理する。 ・在庫状況を反映する。
発送担当者ロール	・受注情報をダウンロードし，それに基づく商品発送を行う。 ・発送が完了したら，発送通知を行う。
経理担当者ロール	・売上情報及び決済情報をダウンロードし，X社の会計システムに入力する。

アカウントにロールを設定された業務担当者は，自分の業務用PCでX社ポータルにアクセスし，利用権限を付与された機能を利用して作業を行う。

機械営業部では，表6及び表7を基に，各ロールに付与する利用権限を検討することにした。その案を表8に示す。

表8　各ロールに付与する利用権限（案）

機能／ロール	商品登録	在庫管理	受注管理	売上管理	アカウント管理
X社ポータル管理者ロール[1)]	◎	◎	◎	◎	◎
商品担当者ロール	◎	◎	×	×	×
発送担当者ロール	○	◎	◎	×	×
経理担当者ロール	×	○	○	◎	×

注記　◎は編集の利用権限が付与されることを，○は閲覧の利用権限が付与されることを，×は利用権限が付与されないことを示す。

注[1)]　あらかじめ管理者用アカウントに設定されている。

X 社 ISMS では，今回のように業務を大きく変更する場合は，情報セキュリティリスクアセスメントを実施し，リスク対応を行うことになっている。そこで，この案について，T 課長が S 課長に相談したところ，次の指摘を受けた。

指摘 1　発送担当者ロールを割り当てられた業務担当者は業務で購入者情報を扱うので，その業務担当者の業務用 PC に購入者情報が蓄積されるおそれがあり，対策が必要である。

指摘 2　X 社ポータル管理者ロールの利用権限が過大であり，不正が起こるおそれがある。X 社ポータル管理者ロールの利用権限を分割すべきである。

これらの指摘を受け，T 課長は，指摘 1 については，発送担当者ロールを割り当てられた業務担当者に対して業務用 PC に蓄積された購入者情報の利用後の削除を徹底させるとともに，購入者情報が蓄積されていないことを上長に定期的に点検させることにした。また，指摘 2 については，表 8 を見直して X 社ポータル管理者ロールの利用はやめるとともに，アカウント管理を含む X 社ポータルの各機能の利用状況のモニタリングを行うために，新たなロールを追加することにした。追加する新たなロールとそのロールに付与する利用権限の案を，表 9 に示す。

表 9　追加する新たなロールとそのロールに付与する利用権限（案）

機能 / ロール	商品登録	在庫管理	受注管理	売上管理	アカウント管理
アカウント管理ロール	（省略）			f1	f2
モニタリングロール				g1	g2

これらの案は ISMS-WG で検討され，情報セキュリティ委員会の承認を得て，Z ショップで 3DP の販売が開始されることになった。

その後，Z ショップからの新製品の販売は順調に進んでいる。

設問1　表1中の下線①について，該当する作業を三つ，解答群の中から選べ。

解答群

ア　新たに追加された情報資産の名称と管理責任者を記載する。

イ　記載された情報資産の重要度が適切であるか確認する。

ウ　記載された情報資産のリスクを低減する。

エ　情報資産目録に対するアクセス権を設定する。

オ　情報資産目録の情報セキュリティパフォーマンス及びX社ISMSの有効性を評価する。

カ　廃棄された情報資産を情報資産目録から削除する。

設問2　〔販路拡大のための施策〕について，(1)～(3)に答えよ。

(1)　表3中の下線②について，適用される法令，及び見直しが必要なX社ISMS文書の組合せはどれか。解答群のうち，最も適切なものを選べ。

解答群

	法令	X社ISMS文書
ア	個人情報の保護に関する法律	情報セキュリティ方針
イ	個人情報の保護に関する法律	適用宣言書
ウ	個人情報の保護に関する法律	適用法規制一覧
エ	電気通信事業法	情報セキュリティ方針
オ	電気通信事業法	適用宣言書
カ	電気通信事業法	適用法規制一覧
キ	特定商取引に関する法律	情報セキュリティ方針
ク	特定商取引に関する法律	適用宣言書
ケ	特定商取引に関する法律	適用法規制一覧

(2) 表3中の [a] に入れる適切な字句を，解答群の中から選べ。

aに関する解答群

ア JIS Q 15001　　イ JIS Q 20000

ウ JIS Q 27017　　エ NIST SP 800-171

オ PCI DSS　　カ 情報セキュリティサービス基準

(3) 本文中の下線③に当てはまる攻撃手法はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア キーロガー　　イ クリプトジャッキング

ウ サイドチャネル攻撃　　エ セッション固定攻撃

オ 総当たり攻撃　　カ ソーシャルエンジニアリング

キ ディレクトリトラバーサル　　ク パスワードリスト攻撃

ケ バッファオーバフロー攻撃　　コ レインボー攻撃

設問３　〔SNS の利用に関する情報セキュリティ対策〕について，(1) ～ (4) に答えよ。

(1) 表 4 中の［ b1 ］～［ b3 ］に入れる，次の (i) ～ (v) の組合せはどれか。b に関する解答群のうち，最も適切なものを選べ。

(i) SNS アカウントのプロフィールにおいて，X 社のアカウントであることを明示する。

(ii) SNS 担当者の個人アカウントと X 社公式アカウントとの相互フォローを行う。

(iii) SNS の提供業者に審査を申請し，認証済みアカウントであることを表示してもらう。

(iv) X 社 Web サイトに，X 社公式アカウントのページへのリンク及び X 社公式アカウントの運用方針を明示する。

(v) X 社のメールサーバで，SPF（Sender Policy Framework）を用いた送信ドメイン認証を行う。

b に関する解答群

	b1	b2	b3
ア	(i)	(ii)	(iii)
イ	(i)	(ii)	(iv)
ウ	(i)	(ii)	(v)
エ	(i)	(iii)	(iv)
オ	(i)	(iii)	(v)
カ	(i)	(iv)	(v)
キ	(ii)	(iii)	(iv)
ク	(ii)	(iii)	(v)
ケ	(ii)	(iv)	(v)
コ	(iii)	(iv)	(v)

(2) 表 4 中の [c1] ～ [c3] に入れる，次の (i) ～ (v) の組合せはどれか。c に関する解答群のうち，最も適切なものを選べ。

(i) X 社公式アカウントによる投稿への，利用者からのアクセス状況をレビューする。

(ii) X 社公式アカウントのパスワードを他のサービスのものと共用しない。

(iii) X 社公式アカウントの利用者 ID を広く宣伝し，認知度を高める。

(iv) X 社公式アカウントへの投稿については，社内の定められた業務用 PC からだけ行う。

(v) X 社公式アカウントへのログインには，記憶を利用した認証と所持しているものを利用した認証を併用する。

c に関する解答群

	c1	c2	c3
ア	(i)	(ii)	(iii)
イ	(i)	(ii)	(iv)
ウ	(i)	(ii)	(v)
エ	(i)	(iii)	(iv)
オ	(i)	(iii)	(v)
カ	(i)	(iv)	(v)
キ	(ii)	(iii)	(iv)
ク	(ii)	(iii)	(v)
ケ	(ii)	(iv)	(v)
コ	(iii)	(iv)	(v)

(3) 表 5 中の [d1] ～ [d3] に入れる，次の (i) ～ (v) の組合せはどれか。d に関する解答群のうち，最も適切なものを選べ。

(i) 業務上の守秘義務に反する投稿を行わない。

(ii) 業務用 PC では SNS の個人利用を行わない。

(iii) 自分の投稿は X 社の公式見解である旨を SNS のプロフィールに明示する。

(iv) 投稿に当たっては，著作権，肖像権などの他人の権利の侵害に注意する。

(v) 取引先の従業員とは SNS 上での私的な交流は行わない。

d に関する解答群

	d1	d2	d3
ア	(i)	(ii)	(iii)
イ	(i)	(ii)	(iv)
ウ	(i)	(ii)	(v)
エ	(i)	(iii)	(iv)
オ	(i)	(iii)	(v)
カ	(i)	(iv)	(v)
キ	(ii)	(iii)	(iv)
ク	(ii)	(iii)	(v)
ケ	(ii)	(iv)	(v)
コ	(iii)	(iv)	(v)

(4) 表 5 中の [e1] ～ [e3] に入れる，次の (i) ～ (v) の組合せはどれか。e に関する解答群のうち，最も適切なものを選べ。

(i) SNS 上で投稿を削除しても，その投稿が拡散されてしまう可能性があることに留意して投稿する。

(ii) SNS を利用する個人所有の端末について，適切な物理的及び技術的対策を実施する。

(iii) 投稿に URL を含めるときは，URL 短縮サービスを利用する。

(iv) 面識のなかった人から SNS を通じて“友達”関係の形成など交流の申出を受けた場合には，積極的に受諾し，人間関係の拡大に努める。

(v) 利用する SNS ごとに，発信する情報の公開範囲を適切に設定する。

e に関する解答群

	e1	e2	e3
ア	(i)	(ii)	(iii)
イ	(i)	(ii)	(iv)
ウ	(i)	(ii)	(v)
エ	(i)	(iii)	(iv)
オ	(i)	(iii)	(v)
カ	(i)	(iv)	(v)
キ	(ii)	(iii)	(iv)
ク	(ii)	(iii)	(v)
ケ	(ii)	(iv)	(v)
コ	(iii)	(iv)	(v)

設問4　〔オンラインショッピングサイトの利用〕について，(1)，(2) に答えよ。

(1)　表 9 中の［ f1 ］，［ f2 ］に入れる記号の適切な組合せを，f に関する解答群の中から選べ。ここで，◎，○及び×は表 8 の注記と同一である。

f に関する解答群

	f1	f2
ア	◎	◎
イ	◎	○
ウ	◎	×
エ	○	◎
オ	○	○
カ	○	×
キ	×	◎
ク	×	○
ケ	×	×

(2)　表 9 中の［ g1 ］，［ g2 ］に入れる記号の適切な組合せを，g に関する解答群の中から選べ。ここで，◎，○及び×は表 8 の注記と同一である。

g に関する解答群

	g1	g2
ア	◎	◎
イ	◎	○
ウ	◎	×
エ	○	◎
オ	○	○
カ	○	×
キ	×	◎
ク	×	○
ケ	×	×

問3　情報セキュリティの自己点検に関する次の記述を読んで，設問1～6に答えよ。

マンション管理会社 Q 社は，マンションの管理組合から委託を受けて管理業務を行っており，契約している管理組合数は 3,000 組合である。東京の本社には，経営企画部，営業統括部，人事総務部，経理部，情報システム部，監査部などの管理部門があり，東日本を中心に 30 の支店がある。従業員数は，マンションの管理人（以下，管理員という）3,300 名を含めて 3,800 名である。管理業務の内容は，管理組合の収支予算書及び決算書の素案の作成，収支報告，出納，マンション修繕計画の企画及び実施の調整，理事会及び総会の支援，清掃，建物設備管理，緊急対応，管理員による各種受付・点検・立会い・報告連絡などである。

Q 社は 3 年前に全社で ISMS 認証を取得しており，最高情報セキュリティ責任者（CISO）を委員長とする情報セキュリティ委員会を設置し，JIS Q 27001 に沿った情報セキュリティポリシ及び情報セキュリティ関連規程を整備している。CISO は情報システム担当常務が務め，情報セキュリティ委員会の事務局は情報システム部が担当している。また，本社各部の部長及び各支店長は，情報セキュリティ委員会の委員，及び自部署における情報セキュリティ責任者を務め，自部署の情報セキュリティを確保し，維持，改善する役割を担っている。各情報セキュリティ責任者は，自部署の情報セキュリティに関わる実務を担当する情報セキュリティリーダを選任している。

U 支店には，支店長，主任 2 名，管理組合との窓口を務めるフロント担当者 10 名が勤務している。U 支店の情報セキュリティ責任者は B 支店長，情報セキュリティリーダは第 1 グループの A 主任である。U 支店に勤務する従業員には，一人 1 台のノート PC（以下，NPC という）が貸与されている。NPC にはディジタル証明書をインストールし，Q 社のネットワークに接続する際に端末認証を行っている。U 支店では，Q 社の文書管理規程に従い，顧客情報などの重要な情報が含まれる電子データは，U 支店の共有ファイルサーバの所定のフォルダに保管する運用を行っている。U 支店の共有ファイルサーバは，1 日 1 回テープにバックアップを取得し，1 週間分のテープを世代管理している。

U 支店が契約している管理組合数は 80 組合であり，フロント担当者 1 名当たり 5～10 の管理組合を担当している。U 支店が担当する管理組合のマンションはそれぞれ，管理事務室が 1 か所設置されており，管理員が 1～2 名勤務している。管理事務室には，管理員以外に，Q 社従業員，マンション居住者が立入ることがある。多くの

マンションでは，管理事務室の入室にマンションごとの暗証番号が必要である。暗証番号はおおむね 2 年ごとに変更される。管理事務室には，管理組合の許可を受けた上で，管理員と U 支店の連絡用に，LTE 通信機能付き NPC を 1 台設置し，インターネット VPN 経由で Q 社のネットワークと接続している。①管理事務室に複数の管理員が勤務する場合には，管理員間で NPC，利用者 ID，パスワード，メールアドレスを共用している。

〔自己点検の規程及びチェック項目〕

Q 社では，自己点検規程及び内部監査規程を，表 1 のとおり定めている。

表 1　自己点検規程及び内部監査規程（概要）

項目	自己点検規程	内部監査規程 [1)]
実施者	管理員を含めた全従業員自らが実施する。	監査部が実施する。監査人は，専門職としての知識及び技能を保持し，監査対象部署からの［a1］を確保しなければならない。
報告先	情報セキュリティリーダが自部署の従業員の回答を評価し，情報セキュリティ責任者が確認の上，その結果を情報セキュリティ委員会に提出する。	監査責任者は，監査手続の結果とその関連資料から作成された監査調書に基づき，監査報告書を作成し，CISO に提出する。
実施頻度	月 1 回実施する。	年 1 回実施する。また，自己点検の結果に応じて適時実施する。
対象	管理員を含めた全従業員を対象とする。	監査対象をサンプリングによって抽出する。
評価の観点	［a2］を遵守して ISMS を運用しているかを点検する。点検する項目は，各部，各支店では，情報セキュリティ責任者が，情報セキュリティ委員会の定めた自己点検における標準チェック項目を基に自己点検チェック項目（以下，チェック項目という）として設定している。	［a2］を遵守して ISMS を運用しているか，［a2］が，情報セキュリティポリシに準拠しているか，また法令の改正や，環境の変化に合わせて適切に改定されているかを評価する。
評価の手法	（省略）	規程文書などを確認して準拠性を評価し，［a3］への質問・閲覧・観察などによって遵守性を評価する。
結果に対する改善	自己点検の結果に基づき，改善が必要な場合には，情報セキュリティ責任者が，情報セキュリティの改善及びチェック項目の見直しを行う。	（省略）

注 [1)]　本規程は，経済産業省“情報セキュリティ監査基準”及び“システム監査基準”を基に Q 社が作成した。

また，U支店では，チェック項目を図1のとおり設定している。

1　クリアデスクを実施している。
2　クリアスクリーンを実施している。
3　NPCのOSの更新履歴によって，自動更新の正常終了を確認している。
4　NPCのアプリケーションソフトウェア（以下，アプリケーションソフトウェアをアプリという）のバージョンが最新かをヘルプメニューで確認している。
5　退出時にNPCをセキュリティケーブルでロックしている。
6　退出時に顧客情報などの重要な情報を含む書類をキャビネットに施錠保管している。
7　プリンタに印刷物を放置していない。
8　顧客情報などの重要な情報が含まれる電子データを，NPC上ではなくU支店の共有ファイルサーバの所定のフォルダに保管している。
9　個人所有PCを業務で使用していない。
（省略）

図1　U支店のチェック項目

〔アプリの更新漏れ〕

A主任は情報処理推進機構（IPA）の情報セキュリティサイトを見た際に，PDF閲覧ソフトにおいて任意のコードが実行されるという深刻な脆弱性に対する注意喚起が，2週間前から掲載されていることに気付いた。そこで，A主任が第1グループメンバのNPCについて，PDF閲覧ソフトのバージョンが最新かを確認したところ，最新ではないNPCが2台あった。1週間前に実施した自己点検では，チェック項目4に全員が“はい”と回答していた。A主任が2台のNPCの利用者に確認したところ，他のアプリの更新は確認していたが，PDF閲覧ソフトの確認が漏れていたことが判明した。

A主任が，IPAの情報セキュリティサイトの参考情報から，脆弱性対策情報データベースを確認したところ，図2のとおり記載されていた。

JVNDB-20XX-XXXXXX
PDF 閲覧ソフトにおける任意のコードを実行される脆弱性
CVSS v3 による深刻度
[b] 値[1]：9.8（[c]）
・攻撃元区分[2]：ネットワーク
・攻撃条件の複雑さ：[d1]
・攻撃に必要な特権レベル：[d2]
・利用者の関与：[d3]
・機密性への影響（C）：高
・完全性への影響（I）：高
・可用性への影響（A）：高

注[1] 値は，0～10.0 で表現される。
[2] 区分には，ネットワーク，隣接，ローカル及び物理がある。

図 2　PDF 閲覧ソフトに対する CVSS v3 の脆弱性評価結果（抜粋）

次は，図 2 についての情報システム部の R 課長と A 主任の会話である。

R 課長：CVSS v3 の [b] 評価基準は，脆弱性そのものの特性を評価する基準であり，評価には，攻撃の容易性及び情報システムに求められる三つのセキュリティ特性である，機密性，完全性，可用性に対する影響といった基準を用います。[b] 評価基準は，時間の経過や利用環境の差異によって変化せず，脆弱性そのものを評価する基準です。図 2 を見ると，この PDF 閲覧ソフトの脆弱性の深刻度は [c] であり，“攻撃条件の複雑さ”，“攻撃に必要な特権レベル”，“利用者の関与”の全てにおいて，攻撃が成功するおそれが最も高い値を示しています。したがって，PDF 閲覧ソフトは早急に更新が必要です。

A 主任：アプリのバージョンが最新かを，簡単にチェックする方法はありませんか。

R 課長：方法は二つあります。一つ目は，“MyJVN バージョンチェッカ”という IPA から無償提供されているソフトウェアを使う方法です。各利用者が NPC にインストールされているアプリのバージョンが最新かを簡単にチェックすることができます。二つ目は [e] を導入する方法です。情報システム部で，各 NPC のアプリのバージョンが最新かを管理し，一括してチェックすることが可能ですが，導入には費用が掛かります。実は，“MyJVN バージョンチェッカ”を全社で利用する準備のために，試用部署を探していました。

しかるべき手続を経て，情報セキュリティ委員会の承認を受けるので，U 支店で試用してもらえませんか。

A 主任は，B 支店長の許可を得て“MyJVN バージョンチェッカ”の試用を開始し，“MyJVN バージョンチェッカ”がフロント担当者や管理員の IT リテラシでも問題なく使用できることを確認し，B 支店長と R 課長に報告した。

報告を受けた B 支店長は，“MyJVN バージョンチェッカ”を全社に先駆けて U 支店で継続して試用することについて，情報セキュリティ委員会の承認を受けた。

〔個人所有スマートフォンの業務利用〕

最近，フロント担当者の K さんが仕事中に度々個人所有スマートフォン（以下，スマートフォンをスマホという）を使っているので，A 主任が K さんに尋ねたところ，個人所有スマホを業務に使うことがあるとのことであった。

K さんは，②スマホの個人利用者向けチャットアプリ（以下，M アプリという）を利用して，K さんが担当する P マンションの管理組合（以下，P 組合という）の理事からの問合せに回答したり，業務に関する情報を送信したりしているとのことであった。P 組合の理事長から，次の理由で，M アプリの使用を求められて，やむを得ず従ったとのことであった。

・P 組合では，理事同士の情報共有に M アプリを利用している。
・問合せに対する K さんの返信がいつも遅く，おおむね 3 営業日以上掛かっている。M アプリを利用すれば，K さんがいつメッセージを読んだかが把握できる。

なお，Q 社は，③従業員が個人所有スマホを業務に利用することを，会社として許可していない。

A 主任は，K さんが個人所有スマホを業務利用していること，及びスマホ用アプリの業務利用によって問題が発生することについて，B 支店長に報告した。

〔チェック項目の見直し〕

これまでの報告を受けて，B 支店長は，図 1 のチェック項目の見直しが必要であると判断し，A 主任に対して見直しを指示した。④A 主任が示した見直し案を B 支店

長が承認し，見直されたチェック項目が翌月から使用されることになった。

〔M アプリの調査〕

K さんは，P 組合に M アプリが使用できなくなったことを連絡したが，P 組合は，M アプリの利用を強く要望するとのことであった。相談を受けた A 主任が，M アプリの機能と特徴を調べたところ，図 3 のとおりであった。

・M アプリの連絡先（以下，AP 連絡先という）に登録された相手とだけ，メッセージの送受信ができる。
・送信相手がいつメッセージを読んだかを確認できる。
・M アプリのメッセージは，スマホに保存される。
・M アプリのアカウントは，スマホの電話番号に対応付けて登録される。
・スマホのアドレス帳（以下，アドレス帳という）に登録された相手と，自分の双方が M アプリを使用し，かつ，それぞれの M アプリに，アドレス帳へのアクセス許可を与えている場合，M アプリのアカウントが相互の AP 連絡先に自動登録される。
・宛先グループを作成し，宛先グループ全員にメッセージを同時に送信できる。また，そのメッセージを宛先グループの各メンバがいつ読んだかを確認できる。
・写真，音声，ビデオ，ファイル，URL などを，メッセージに添付して送信できる。
・メッセージに JPEG ファイルを添付した場合，撮影時に格納される各種データは自動的に削除される。
・現在地の位置情報を自動的に取得して，メッセージに添付して送信できる。

図 3　M アプリの機能及び特徴（抜粋）

A 主任は，図 3 から，⑤M アプリを業務連絡に利用することには，幾つかのリスクがあると考えた。更に調査したところ，M アプリに業務用の機能を追加したアプリ（以下，BM アプリという）が存在することが分かった。BM アプリで追加された機能は，図 4 のとおりである。

・他のスマホの M アプリ又は BM アプリとの間でメッセージを送受信できる。
・BM アプリを導入した組織において，BM アプリの管理者を指定できる。
・管理者が，AP 連絡先の管理を行え，AP 連絡先の自動登録を禁止できる。
・管理者が，BM アプリのデータを遠隔から消去できる。
・管理者が，BM アプリを導入したスマホでのスマホ用アプリの利用を制限できる。
・誤って送ったメッセージの送信を取り消すことができる。

図 4　BM アプリで追加された機能（抜粋）

A 主任は，図 4 から，BM アプリには適切なセキュリティ機能が備わっていると考

え，情報システム部に，個人所有スマホ及び BM アプリの業務利用について検討を依頼した。

情報システム部は，個人所有スマホの業務利用に対する情報セキュリティリスクアセスメント及び⑥BM アプリの利用に対する情報セキュリティリスクアセスメントを実施した。さらに，その結果を情報セキュリティ委員会に報告し，許可を受けた上で BM アプリを試験導入し，問題がないことを確認した。

P 組合から強い要望を受けてから半年後，情報セキュリティ委員会は，必要な情報セキュリティ関連規程を整備し，チェック項目を再度見直した上で，全社的に個人所有スマホの業務利用を BM アプリなど会社が認めたスマホ用アプリに限定して許可した。これによって，Q 社は P 組合の要望に応えることができた。また，BM アプリの利用を広げたことによって，Q 社と顧客との間の連携が強化された。

設問 1　本文中の下線①について，次の (i) ～ (iv) のうち，共用することによって高くなるリスクはどれか。該当するものだけを全て挙げた組合せを，解答群の中から選べ。

(i) NPC を操作した者を特定できないという状況を狙われて，不正に操作されるリスク

(ii) 異動者や退職者など，利用資格を失った者に NPC を不正に操作されるリスク

(iii) 共用者の 1 人がパスワードを変更した際に，他の共用者に変更後のパスワードを伝えるためのメモを書き，そのメモからパスワードが漏えいし，不正に操作されるリスク

(iv) クリアスクリーンをし忘れ，その隙に不正に操作されるリスク

解答群

ア (i)　　イ (i), (ii)

ウ (i), (ii), (iii)　　エ (i), (ii), (iv)

オ (i), (iii)　　カ (i), (iii), (iv)

キ (i), (iv)　　ク (ii), (iii)

ケ (ii), (iv)　　コ (iii), (iv)

設問2　〔自己点検の規程及びチェック項目〕について，(1)，(2)に答えよ。

(1)　表1中の［a1］～［a3］に入れる字句の組合せはどれか。aに関する解答群のうち，最も適切なものを選べ。

aに関する解答群

	a1	a2	a3
ア	機密性	情報セキュリティ関連規程	監査対象部署
イ	機密性	情報セキュリティ関連規程	監査部
ウ	機密性	文書管理規程	監査対象部署
エ	責任追跡性	情報セキュリティ関連規程	監査対象部署
オ	責任追跡性	情報セキュリティ関連規程	監査部
カ	責任追跡性	文書管理規程	監査対象部署
キ	独立性	情報セキュリティ関連規程	監査対象部署
ク	独立性	情報セキュリティ関連規程	監査部
ケ	独立性	文書管理規程	監査対象部署

(2)　図1中のチェック項目3～8のうち，NPCにおけるランサムウェアの脅威に対する管理策だけを全て挙げた組合せを，解答群の中から選べ。

解答群

ア　3，4，5　　イ　3，4，8

ウ　3，5，7　　エ　3，6，7

オ　4，5，6　　カ　4，6，8

キ　4，7，8　　ク　5，6，7

設問3　〔アプリの更新漏れ〕について，(1) ～ (4) に答えよ。

(1)　図 2 及び本文中の［ b ］に入れる字句はどれか。解答群のうち，最も適切なものを選べ。

b に関する解答群

ア　環境　　イ　基本　　ウ　現状

(2)　図 2 及び本文中の［ c ］に入れる字句はどれか。解答群のうち，最も適切なものを選べ。

c に関する解答群

ア　危険　　イ　緊急　　ウ　警告　　エ　重要

オ　注意　　カ　レベル 4　　キ　レベル 5

(3)　図 2 中の［ d1 ］～［ d3 ］に入れる字句の適切な組合せを，d に関する解答群の中から選べ。

d に関する解答群

	d1	d2	d3
ア	高	低	不要
イ	高	低	要
ウ	高	不要	不要
エ	高	不要	要
オ	低	高	不要
カ	低	高	要
キ	低	低	不要
ク	低	低	要
ケ	低	不要	不要
コ	低	不要	要

(4) 本文中の［ e ］に入れる字句はどれか。解答群のうち，最も適切なものを選べ。

e に関する解答群

ア BI ツール

イ CASB（Cloud Access Security Broker）

ウ IT 資産管理ツール

エ UEBA（User and Entity Behavior Analytics）

オ ソフトウェア構成管理ツール

カ 特権 ID 管理ツール

キ ポートスキャナ

設問4 本文中の下線②及び下線③のような行為を表す字句の適切な組合せを，解答群の中から選べ。

解答群

	下線②	下線③
ア	グリーン IT	BYOD
イ	グリーン IT	CDN
ウ	グリーン IT	VPN
エ	サンクション IT	BYOD
オ	サンクション IT	CDN
カ	サンクション IT	VPN
キ	シャドーIT	BYOD
ク	シャドーIT	CDN
ケ	シャドーIT	VPN

設問5　本文中の下線④について，次の (i) ～ (iii) のうち，A 主任が見直しを行った図1のチェック項目と見直しの内容だけを全て挙げた組合せを，解答群の中から選べ。

(i)　3 と 4 を“MyJVN バージョンチェッカによって，NPC のアプリのバージョンが最新かを確認し，最新でなければ更新している。”に統合する。

(ii)　4 を“NPC のアプリのバージョンが最新かを MyJVN バージョンチェッカで確認し，最新でないアプリは，MyJVN バージョンチェッカの指示に従って更新する。”に修正する。

(iii)　9 を“PC やスマホなどの個人所有端末を業務で利用していない。”に修正する。

解答群

ア　(i)　　イ　(i)，(iii)

ウ　(ii)　　エ　(ii)，(iii)

オ　(iii)　　カ　当てはまるものはない

設問6　〔Mアプリの調査〕について，(1)，(2)に答えよ。

(1)　本文中の下線⑤のリスクについて，次の(i)～(iii)のうち，該当するものだけを全て挙げた組合せを，解答群の中から選べ。

(i)　業務と関係のない宛先グループや友人とも M アプリでやり取りできるので，業務と関係のない友人や宛先グループに，誤って業務情報を送付してしまうリスク

(ii)　写真（JPEG ファイル）を添付した場合，写真には撮影場所を特定できるものが写っていなくても，撮影場所が特定されるリスク

(iii)　見知らぬ人が AP 連絡先に登録されてしまう場合があるので，見知らぬ人にメッセージを送ってしまうリスク

解答群

ア　(i)　　イ　(i)，(ii)

ウ　(i)，(ii)，(iii)　　エ　(i)，(iii)

オ　(ii)　　カ　(ii)，(iii)

キ　(iii)　　ク　当てはまるものはない

(2)　本文中の下線⑥で実施することについて，次の(i)～(v)のうち，該当するものだけを全て挙げた組合せを，解答群の中から選べ。

(i)　リスク共有

(ii)　リスク特定

(iii)　リスク評価

(iv)　リスク分析

(v)　リスク保有

解答群

ア　(i)，(ii)，(iii)，(iv)　　イ　(i)，(ii)，(iii)，(iv)，(v)

ウ　(i)，(iii)，(iv)　　エ　(i)，(iii)，(iv)，(v)

オ　(i)，(iii)，(v)　　カ　(ii)，(iii)，(iv)

キ　(ii)，(iv)　　ク　(iii)，(iv)

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

6. 退室可能時間中に退室する場合は，手を挙げて監督員に合図し，答案用紙が回収されてから静かに退室してください。

退室可能時間	13:10 ～ 13:50

7. **問題に関する質問にはお答えできません。**文意どおり解釈してください。
8. 問題冊子の余白などは，適宜利用して構いません。ただし，問題冊子を切り離して利用することはできません。
9. 試験時間中，机上に置けるものは，次のものに限ります。

   なお，会場での貸出しは行っていません。

   受験票，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（時計型ウェアラブル端末は除く。アラームなど時計以外の機能は使用不可），ハンカチ，ポケットティッシュ，目薬

   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 答案用紙は，いかなる場合でも提出してください。回収時に提出しない場合は，採点されません。
12. 試験時間中にトイレへ行きたくなったり，気分が悪くなったりした場合は，手を挙げて監督員に合図してください。