SG

平成28年度　秋期
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ません。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。

秋の情報処理技術者試験は，［ a ］月に実施される。

解答群　ア　8　　イ　9　　ウ　10　　エ　11

適切な字句は“ウ　10”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　オンラインストレージサービスの利用における情報セキュリティ対策に関する次の記述を読んで，設問1～4に答えよ。

J社は，従業員数150名の電気機器メーカである。顧客企業から提示される仕様に基づいて電気製品を設計，製造している。

J社では，1年前に最高情報セキュリティ責任者（CISO）及び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を定め，情報セキュリティ関連規程を整備した。情報セキュリティ委員会の事務局は，情報システム課が担当している。また，各部の部長は，情報セキュリティ委員会の委員及び部における情報セキュリティ責任者を務め，自部の情報セキュリティを適切に確保し，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する。

J社では，社内ネットワークとインターネットの間にファイアウォールを設置している。また，社外のWebサイトの閲覧は，全てプロキシサーバ経由とし，業務上不要と思われるWebサイトへの接続をコンテンツフィルタで制限している。制限されているWebサイトへの接続が必要になった場合は，接続するPCを限定して，情報システム課が一時的に制限を解除している。J社では，DHCPは使っておらず，PCのIPアドレスは固定である。

〔オンラインストレージサービス〕

50名の従業員が所属する製造部では，製造の一部を協力会社であるB社に委託している。製造部からB社へは，従来，USBメモリを使用して製品製造に関係するファイルを提供していたが，USBメモリを管理する手間や，顧客企業からの急な仕様変更への対応が課題であった。製造部は，これらの課題を解決するために，顧客企業各社の了解も得た上で，2年前から，X社が提供するオンラインストレージサービス（以下，Xサービスという）をB社へのファイル提供に利用している。Xサービスはインターネット上で提供されている。サービス仕様（抜粋）を次に示す。

・専用のドメイン名をもち，インターネット上のどこからでもアクセスできる。
・スマートフォンやタブレットなど，PC以外の端末からでも利用できる。
・インターネット上における盗聴や改ざんへの対策として，サービスへの接続に

HTTP over TLS（HTTPS）を使用している。

・利用アカウントの ID として電子メールアドレス（以下，メールアドレスという）を登録し，パスワードを設定すれば，Web ブラウザだけですぐに利用を始められる。

・利用アカウントごとに専用のフォルダが与えられ，ファイルの登録や，登録したファイルの閲覧，編集などの操作を行うことができる。フォルダ容量が 10 G バイトまでは無料である。

・ファイルの登録時，又は登録後に，ファイル共有先を指定し，共有権限を付与することによって，指定した利用アカウントにファイルの操作を許可したり，インターネット上の誰にでもファイルの閲覧を許可したりすることができる。ファイルの共有設定には表 1 に示す 4 種類がある。

表 1　X サービスにおけるファイルの共有設定

番号	ファイル共有の有無	ファイル共有先	付与できる共有権限	設定内容
1	ファイル共有あり	指定した利用アカウント	編集権限	指定した利用アカウントに対して，ファイルの閲覧，編集，削除を許可する。
2			閲覧権限	指定した利用アカウントに対して，ファイルの閲覧を許可する。
3		パブリック 1)	閲覧権限	利用アカウントがなくても，インターネットからのファイルの閲覧を可能にする。
4	ファイル共有なし	なし	権限なし	ファイルを登録した利用アカウント以外に，ファイル操作を許可しない。

注 1)　パブリックとは，インターネット利用者全般を意味する。

〔X サービス利用規則〕

2 年前，X サービスの利用開始に当たって，製造部では X サービス利用規則を作成し，部内に通知した。現在の X サービス利用規則を図 1 に示す。

なお，J 社の社内規程では，スマートフォンやタブレットの業務利用は認めていない。かつ，PC を社外に持ち出して使用することも禁止している。

1. X サービスを社外で業務利用することは禁止する。
2. X サービスに登録するファイルは，B 社に製造委託する製品の仕様とその関連情報に限定する。
3. メールアドレスを X サービス専用に一つ設け，J 社製造部が使用する利用アカウントの ID として登録する。また，当該利用アカウントのパスワードは，製造部の情報セキュリティリーダが設定し，製造部の従業員に通知する。
4. 当該利用アカウントのパスワードは半年ごとに更新し，秘密に管理する。
5. B 社にファイルを提供する場合は，当該ファイルのファイル共有先として B 社の利用アカウントを指定し，“閲覧権限”を付与する。

図 1　X サービス利用規則（抜粋）

〔事故発生〕

1 か月前，Q 社から J 社に連絡が入った。Q 社は J 社と取引関係はないが，Q 社従業員がインターネット検索を行っていたところ，J 社の社名が記載され，秘密情報と記されたファイルが X サービスで公開されているのを発見したので連絡したということであった。製造部の情報セキュリティリーダである S 主任が調査したところ，J 社が B 社に提供するために X サービスに登録している顧客企業の製品製造に関係するファイルの一つが公開されてしまっていることが判明した。問題のファイルは，ファイル共有先に［ a1 ］が指定され，かつ，共有権限に［ a2 ］が付与されていた。

S 主任から報告を受けた製造部の情報セキュリティ責任者である T 部長は，CISO に一報を入れるとともに，①直ちに X サービスに登録している全てのファイルを削除し，X サービスの利用を中止するように指示した。

今回の事故を重く見た CISO は，情報セキュリティ委員会を招集し，T 部長に事故原因の調査と対策の検討を指示した。また，情報システム課の U 課長には，製造部への支援を指示した。

〔原因調査〕

S 主任は，T 部長から指示を受けて事故原因の調査を開始し，X サービスの情報セキュリティに影響する問題，つまり外部からの攻撃やシステム障害などが発生しなかったか，対象ファイルの共有設定を変更した者は誰かなどを X 社に問い合わせた。X 社からは，X サービスの情報セキュリティに影響する問題は発生しておらず，また，

操作の履歴情報を開示できるのは法令に基づいた開示請求があった場合に限ると回答があった。

X社から調査協力を得ることができず，また，この時点で事件として警察に捜査を依頼することも難しいと思われたので，S主任はU課長と相談し，J社内の調査を進めることにした。U課長は②プロキシサーバを調査したが，不審な点は確認されず，また，製造部の全PCも調査したが問題点は見つけられなかったので，S主任は製造部の従業員全員に個別にヒアリングを行うことにした。

〔個別ヒアリング〕

S主任は，自分とT部長を除く製造部の従業員48名一人一人に対して，Xサービスの利用状況を確認した。ヒアリング結果を図2に示す。

・Xサービス利用規則については，全員がその存在を認識していた。
・Xサービスを利用したことがある者は48名中45名であった。残り3名はB社に関係する業務がなく，Xサービスの利用方法も知らなかった。
・Xサービスを利用したことがある45名の中に，ファイルを公開したという認識をもつ者はいなかったが，一部の者はファイルの共有設定に関係する“指定した利用アカウント”，“パブリック”，“編集権限”，“閲覧権限”といった用語の意味を正しくは理解していなかった。
・Xサービスをスマートフォンやタブレット，自宅のPCなどから利用している者はいなかった。

図2　ヒアリング結果（抜粋）

Xサービスでは，ファイル登録時点の共有設定は，ファイル共有先“なし”，共有権限“権限なし”が初期値である。B社にファイルを提供するには，ファイル登録時，又は登録後に共有設定を変更する必要がある。S主任は，ヒアリング結果のうち［　b　］という製造部の状況では，“B社にファイルを提供する際に，Xサービスのファイル共有設定を間違える”という事故が起きやすいと考えた。そこで，従業員がXサービスの利用を開始する時点でXサービス利用規則と利用方法についての十分な教育を行うとともに，③万一間違った共有設定がなされても第三者にファイルを読まれる可能性を下げる対策をXサービス利用規則の中に定めておくべきであったと反省した。

〔問題点の整理，対策の検討〕

S主任は，一連の調査結果をT部長に報告した。T部長は，Xサービスの利用中止によってB社への製造委託に支障を来していることから，Xサービスの利用を早期に再開できるようにS主任に検討を指示した。S主任は，製造部の従業員による共有設定の誤り防止を含めた対策をU課長と相談した。U課長は，Xサービスを B社へのファイル提供に利用したこと自体が誤りであったとして，表2のように，Xサービスを業務で利用することの問題点とその理由を三つ指摘した。

表2　Xサービスを業務で利用することの問題点とその理由

番号	問題点	理由
1	c	今回の調査で判明したとおり，事故が発生した場合に原因を調べられないから。
2	従業員が自由にファイル共有を設定することができる。	個人向けサービスでは当然の機能であるが，従業員が自由にファイル共有を設定できると，e，f の予防が困難であるから。
3	d	インターネット上で提供される社外のITサービスを業務で利用する場合は，なりすましのリスクを軽減するために2要素認証などの強固な対策が必要であると，情報セキュリティ関連規程に定めているから。

次は，U課長とS主任の会話である。

U課長：製造部の業務を考慮すると，USBメモリを使ったファイル提供に戻すことは難しいのではないかと思いますが，何か代替案を考えていますか。

S主任：同じオンラインストレージサービスでも，法人向けに有償で提供されているサービスには管理機能を強化しているものが多いので，そうしたサービスを使うことを考えたいと思います。

U課長：利用するサービス自体を切り替えることによって，問題点1～3の解決を図るということですね。

S主任：はい。ただし，現在のXサービス利用規則の内容では，④事故発生時の原因特定は困難です。適切な法人向けサービスに切り替えるとともに，利用規則も作り直すつもりです。

U課長：今回の事故によって，全社の情報セキュリティ対策がまだ十分でないことに気付きました。情報セキュリティ委員会の事務局として，情報セキュリティ委員会に対して追加の⑤組織的対策を行うように働きかけた上で，情報システム課としても⑥技術的対策を進め，情報セキュリティの改善に努めます。

S主任は，新しい利用規則をどのように作成すべきか，U課長とともに検討した。また，法人向けサービスの選定方法についてU課長から技術的なアドバイスを受けた。

その後，S主任は問題点1～3に対応したオンラインストレージサービスとして，W社の法人向けオンラインストレージサービス（以下，Wサービスという）を選定し，Xサービスからの切替えについて，T部長の承認を得た。T部長は，情報セキュリティ委員会の承認と顧客企業各社の了解を得た上でWサービスの利用規則を新たに定め，製造部従業員への周知など十分な準備を行い，Wサービスを使ってB社へのファイル提供を再開した。

設問1　〔事故発生〕について，(1)，(2)に答えよ。

(1) 本文中の［ a1 ］，［ a2 ］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，適切なものを選べ。

aに関する解答群

	a1	a2
ア	B社の利用アカウント	閲覧権限
イ	B社の利用アカウント	編集権限
ウ	Q社の利用アカウント	閲覧権限
エ	Q社の利用アカウント	編集権限
オ	パブリック	閲覧権限
カ	パブリック	編集権限

(2) 本文中の下線①のように指示した理由はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア J社が使用しているXサービスの利用アカウントのIDとパスワードが漏えいしたことが明らかであり，J社がXサービスに登録している全てのファイルに被害が及ぶおそれがあったから

イ Xサービスがサイバー攻撃を受けたことが明らかであり，公開されたファイルの他にも，流出したファイルやマルウェア感染などの被害を受けたファイルが存在する可能性があったから

ウ Xサービスよりも機能が豊富であり，かつ，不正アクセスやマルウェアへの対策も十分な信頼できるサービスに早急に移行することを決定したから

エ 原因は不明だが，Xサービスに登録されている全てのファイルが公開されたことが明らかであり，J社としても早急に被害の拡大を防止する必要があったから

オ ファイルが公開された原因が不明であり，J社がXサービスに登録している他のファイルや，今後登録するファイルにも被害が及ぶおそれがあったから

カ ファイルがマルウェアに感染したことが明らかであり，J社がXサービスに登録している他のファイルや，今後登録するファイルにも被害が及ぶおそれがあったから

設問2　本文中の下線②について，次の(i)～(iii)のうち，調査を行う目的として適切なものだけを全て挙げた組合せを，解答群の中から選べ。

(i) Xサービス以外のオンラインストレージサービスが利用されていなかったかを確認するため

(ii) 情報システム課が一時的に制限を解除したWebサイトへの接続状況を確認するため

(iii) 製造部のPC以外のJ社PCの中に，Xサービスに接続したものがあるかを確認するため

解答群

ア (i)　　イ (i)，(ii)　　ウ (i)，(ii)，(iii)

エ (i)，(iii)　　オ (ii)　　カ (ii)，(iii)

キ (iii)

設問３　〔個別ヒアリング〕について，(1)，(2) に答えよ。

(1)　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　X サービスの利用方法を知らない従業員が 3 名いた

イ　X サービス利用規則の存在を従業員全員が認識していた

ウ　X サービスをスマートフォンやタブレット，自宅の PC などから利用している従業員がいなかった

エ　ファイルの共有設定に関係する用語の意味を正しくは理解していない従業員がいた

(2)　本文中の下線 ③ について，次の (i) ～ (iv) のうち，該当する対策だけを全て挙げた組合せを，解答群の中から選べ。

(i)　登録するファイルに電子署名を付与する。

(ii)　登録するファイルを暗号化する。

(iii)　ファイル登録後，B 社だけに，登録したファイルのハッシュ値を連絡する。

(iv)　ファイル登録後，B 社だけに連絡し，B 社のダウンロードが完了次第直ちに削除する。

解答群

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

エ　(i)，(iii)　　オ　(i)，(iii)，(iv)　　カ　(i)，(iv)

キ　(ii)，(iii)　　ク　(ii)，(iii)，(iv)　　ケ　(ii)，(iv)

コ　(iii)，(iv)

設問4　〔問題点の整理，対策の検討〕について，(1) ～ (4) に答えよ。

(1)　表 2 中の［ c ］，［ d ］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，d に関する解答群

ア　スマートフォンやタブレットから利用できる。

イ　操作の履歴情報が提供されない。

ウ　通信中の情報が暗号化されない。

エ　登録したファイルに対するウイルスチェック機能をもたない。

オ　メールアドレスとパスワードだけで利用できる。

(2)　表 2 中の［ e ］，［ f ］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，f に関する解答群

ア　DDoS 攻撃	イ　意図的な公開	ウ　クラッキング
エ　誤操作	オ　スパムメール	カ　中間者攻撃
キ　なりすまし	ク　フィッシング	ケ　紛失

(3)　本文中の下線 ④ について，図 1 のどの項番が事故発生時の原因特定を困難にしているか。解答群のうち，最も適切なものを選べ。

解答群

ア　1	イ　2	ウ　3
エ　4	オ　5	

(4) 本文中の下線 ⑤ 及び ⑥ について，次の (i) ～ (viii) のうち，今回の事故を受けて情報セキュリティ委員会と情報システム課が行うべき対策を三つ挙げた組合せはどれか。解答群のうち，最も適切なものを選べ。

［情報セキュリティ委員会が行うべき組織的対策］

(i) オンラインストレージサービス業者との秘密保持契約を見直し，情報流出の予防に関する条項を強化する。

(ii) 業務に関係がないインターネット利用を禁止する旨を情報セキュリティ関連規程に定める。

(iii) 社外の IT サービスの導入について，全て情報セキュリティ委員会の承認を必要とすることを情報セキュリティ関連規程に定める。

(iv) 情報システムの利用アカウントの共有を禁止する旨を情報セキュリティ関連規程に定める。

［情報システム課が行うべき技術的対策］

(v) X サービスの利用アカウントの ID に登録していたメールアドレスを廃止し，新たに選定する法人向けのオンラインストレージサービスの利用アカウントの ID として登録する専用のメールアドレスを新たに用意する。

(vi) 新たに選定する法人向けのオンラインストレージサービスに登録する全てのファイルを，定期的にバックアップする。

(vii) 新たに選定する法人向けのオンラインストレージサービスに登録するファイルに電子署名を付与するために，電子証明書を準備する。

(viii) オンラインストレージサービスは，情報セキュリティ委員会の承認を得たものだけ接続を許可するようにコンテンツフィルタを設定する。

解答群

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

問2　情報機器の紛失に関する次の記述を読んで，設問1，2に答えよ。

Z社は，従業員数2,000名の生命保険会社であり，東京に本社をもち，全国に支社が点在している。以下，本社及び各支社を拠点という。

Z社では，拠点の営業員が，会社貸与の持出し用ノートPC（以下，NPCという）を携帯して顧客を訪問し，商品説明資料，見積書，契約書の作成などを行っている。Z社の本社情報システム部は，NPCの情報セキュリティ対策とその持出し管理のために，表1に示すルールを定めている。

表1　NPCの情報セキュリティ対策と持出し管理ルール

全PCのための情報セキュリティ対策	・次の情報セキュリティ対策を行う。 (a) OSへのログインパスワード設定 (b) BIOSパスワードの設定 (c) CD及びDVDからの起動禁止設定 (d) OS，ソフトウェアの最新化（脆弱性対応） (e) ウイルス対策ソフトのパターンファイル最新化及び定期的なフルスキャン (f) 5分間無操作でスクリーンをロックし，パスワード入力要求 (g) 外部記憶媒体の接続制限（Z社が従業員に貸与するUSBメモリだけが接続可）
NPCのための情報セキュリティ対策	・(a)～(g)に加えて，次の情報セキュリティ対策を行う。 (h) ハードディスクドライブ（以下，HDDという）全体の暗号化 (i) クラウドサービスで提供される契約管理システム（以下，Lシステムという）を利用するためのクライアント証明書[1]のインストール ・(h)，(i)の情報セキュリティ対策を施したNPCに“対策済NPC”の文字列と有効期限日（最長6か月）を記載したシールを貼り付ける。
NPCによる情報の持出し管理	・NPCに情報を保存して持ち出す場合は，本社情報システム部が運用するNPC持出し申請システムを利用して，その都度，所属する部課の長の承認を得る。その際，持ち出すファイルのリストをNPCから出力し，NPCの資産管理番号と合わせて申請する。 ・NPCの持出し頻度が高く，都度申請では支障が生じる場合には，部課の長は，最長1か月の“NPC期間持出し”を承認することができる。

注[1]　Lシステムでは，クライアント認証とパスワード認証の組合せによる2要素認証の仕組みが提供されている。クライアント認証は公開鍵暗号方式を利用する。NPC上のクライアント証明書と秘密鍵は，NPCの故障などに備えるためにエクスポート可能にしている。Lシステムの利用アカウントは本社情報システム部が管理している。Lシステムでは顧客情報を含む契約書を管理している。

Z社は，各拠点に情報セキュリティ管理責任者とその配下の情報セキュリティリー

ダを置いている。また，各拠点に配置された情報システム担当は，各拠点で利用するPC などの情報機器の貸出し，表 1 に示した情報セキュリティ対策の設定と維持，持出し管理の実施指導，本社情報システム部と連携した情報システムの運用管理，利用支援などを行っている。

Z 社の情報セキュリティ管理規程では，顧客情報を含め Z 社が秘密として管理している情報（以下，秘密情報という）の漏えい及びその可能性がある情報セキュリティインシデント（以下，情報セキュリティインシデントをインシデントという）が発生した場合の対応手順を定めている。そのうち，従業員に貸与している情報機器の紛失・盗難が発生した場合の対応手順は図 1 のとおりである。

1. インシデントの発生

紛失・盗難の発生又はその可能性がある事象を発見した従業員は，直ちに，所属する部課（以下，当該部課という）の長に報告する。報告を受けた長は，直ちに，その時点で確認した事実関係を，当該部課がある拠点（以下，当該拠点という）の情報セキュリティ管理責任者に報告する。情報セキュリティ管理責任者は，情報機器への不正なアクセスのおそれ，秘密情報の紛失・漏えいの発生又はその可能性があると判断した場合には，インシデントの発生を宣言する。

2. 初動対応

情報セキュリティ管理責任者は，配下の情報セキュリティリーダに対して，直ちに，初動対応の体制の編成及び初動対応の開始を指示する。情報セキュリティリーダは，当該拠点の情報システム担当と協力して，インシデントの事実関係を整理し，情報機器に保存されていた情報の内容及び量，並びに暗号化，アクセス制御などの情報セキュリティ対策の実施状況を確認する。保存されていた情報に情報システムのアカウント情報が含まれる場合は，パスワードの変更やアカウントの停止を行うなど，インシデントの影響拡大を防止する措置をとる。情報セキュリティリーダは，確認結果と防止措置を当該拠点の情報セキュリティ管理責任者に報告する。情報セキュリティリーダは，必要に応じてインシデントの対応に当たるメンバを指名することができる。

以下省略（“3. 調査”，“4. 通知，報告及び公表”，“5. 復旧”，“6. 事後対応”が続く）。

図 1　情報機器の紛失・盗難発生時の対応手順（抜粋）

〔情報機器の紛失〕

R 支社は，従業員数 100 名の支社であり，営業員が 60 名いる。R 支社では，支社長が情報セキュリティ管理責任者を務め，各部課の長が情報セキュリティリーダを務めている。

10 月 12 日（水）10 時 30 分頃，R 支社の営業部 1 課の F さんが，客先から R 支社

に戻る途中，電車の網棚にかばんを置き忘れるという事象が発生した。かばんの中には，NPC が入っていた。

報告を受けた R 支社長は，インシデントの発生を宣言し，営業部 1 課の情報セキュリティリーダである K 課長に対して，直ちに初動対応を開始するよう指示した。また，R 支社長の指示によって，K 課長，各部の部長，及び R 支社の情報システム担当として初動対応に当たる W 主任が出席して，インシデント対策会議が開催されることとなった。

幸い，当日の 15 時頃にかばんとその中の NPC を回収することができた。しかし，紛失している間に，外部の者によって NPC を操作されたり，NPC から情報を窃取されたりした可能性は否定できない。K 課長は，調査を継続しつつ，16 時 30 分に開催予定のインシデント対策会議に向けてインシデント報告書案を作成することにした。

〔インシデント報告書案の作成〕

K 課長は，まず，F さんが置き忘れた情報機器（以下，紛失機器という），紛失機器に保存されていた情報，及び紛失機器における情報セキュリティ対策の実施状況を表 2 のとおり整理した。

表 2　インシデント報告書案（抜粋）

紛失機器	・NPC（1 台） 資産管理番号：ZR00XXXX NPC 持出し申請システムにおいて，10 月 3 日に，1 か月間の NPC 期間持出しを承認した記録あり。 ・補足：会社貸与のスマートフォンは紛失していない。 当日，会社貸与の USB メモリなどの外部記憶媒体は持ち出していない。
紛失機器に保存されていた情報の内容及び量	・NPC 持出し申請システムにおいて，会社紹介資料，商品説明資料の持出し申請の記録あり。どちらも自社 Web サイトで社外に公開している資料。 ・持出し申請以後に保存した情報は調査中。
紛失機器における情報セキュリティ対策	・全 PC 及び NPC のための情報セキュリティ対策は，本社情報システム部が定める手順に従い正しく実施されていたことを，PC 管理ツールが NPC 紛失当日の朝に収集した情報を基に，W 主任が確認した。 なお，F さんのログインアカウントには情報セキュリティ対策を変更する権限はない。 ・“対策済 NPC” シールは 7 月 25 日に発行されたものである。

続いて，K 課長は，インシデント報告書案の一部として，インシデント発生とその初動対応の経緯を図 2 のとおり整理した。

NPC の紛失から初動対応及び NPC の回収までの経緯		
(1) インシデントの発生及び報告		
09:45	F さん	訪問先を出る。
10:00	F さん	会社に戻るために，○○駅から××線に乗車。混んでいたので，立ったまま，かばんを目の前の網棚に置く。会社貸与のスマートフォンで電子メールを閲覧。
10:05	F さん	目の前の座席が空いたので，座る。かばんは網棚に置いたまま。
10:20	F さん	△△駅に到着。下車した後，網棚にかばんを置き忘れたことに気付く。
10:30	F さん	△△駅の係員にかばんの紛失を届ける。内容物は NPC，パンフレット，筆記用具など。その時点で，駅において該当する拾得物の届出はなし。
10:45	F さん	スマートフォンを使って，K 課長に，かばんの紛失を電話で連絡。 紛失した状況，かばんに NPC が入っていたこと，その NPC は持出しを承認されているが，紛失時にどのような情報を保存していたかは定かではないことを報告。
	K 課長	F さんに対し，警察に連絡するように指示。
10:55	K 課長	R 支社長に対し，第一報として，F さんからの報告内容を報告。
	R 支社長	インシデントの発生を宣言。K 課長に，直ちに体制を編成して初動対応を開始するように指示。
(2) 初動対応		
11:00	K 課長	関係者を召集して状況説明。初動対応を次のとおり開始。 (a) K 課長の実施内容 ・紛失物の捜索活動の支援 ・情報機器紛失時の状況など，事実関係の確認 ・［ a ］ (b) W 主任の実施内容 ・紛失機器の特定 ・紛失機器における［ b ］ ・［ c ］システムの特定 ・上記で特定したシステムにおいて F さんのアクセス権の無効化 ・上記で特定したシステムにおいて［ d ］
11:10	K 課長	R 支社長に電話で状況報告。
	R 支社長	対応の継続を指示するとともに，15:00 にインシデント対策会議を開催することを決定し，事実関係を整理するよう指示。
	W 主任	NPC 持出し申請システムにおける F さんの持出し申請記録を確認し，K 課長に連絡。
11:15	F さん	最寄りの警察署に，遺失届出書を提出。
11:20	W 主任	L システムにおいて F さんのアクセス権が無効化されたことを K 課長に報告。

図 2　インシデント発生とその初動対応の経緯

11:45	F さん	R 支社に帰社。
	K 課長 W 主任	事実関係を確認するために F さんにヒアリング。
12:30	K 課長	この時点までに確認した事実関係と対応状況を R 支社長に報告。
(3) NPC の回収		
14:10	F さん	△△駅からかばんが見つかった旨の電話連絡を受ける。□□駅で，乗客が届けてくれていた。
	K 課長	R 支社長にインシデント対策会議延期を申し入れ，16:30 開始に決定。
14:50	F さん	□□駅でかばんとその中身を確認し，受領。
	K 課長	すぐに NPC を受け取る。
15:05	K 課長	R 支社長に電話で報告。

図 2　インシデント発生とその初動対応の経緯（続き）

〔インシデントの影響及び対応〕

16 時に，K 課長は W 主任に声を掛け，インシデント対策会議の事前確認のための打合せを行った。次はその時の会話である。

K 課長 ：F さんは，NPC にはどのような情報が入っていたか定かではないと言っていました。契約書などの顧客情報は入っていたのでしょうか。

W 主任 ：NPC の持出し申請の時点では，顧客情報は含まれていませんでした。ただし，①持出しの承認の後でも，NPC に顧客情報を追加で保存できてしまいます。

K 課長 ：分かりました。②当社で定めた手順のうち，NPC 紛失時に NPC の中の情報を盗まれるリスクを低減する手順は，施されていたでしょうか。

W 主任 ：はい。もちろんです。

K 課長 ：紛失時点で顧客情報が NPC に保存されていたかどうか，紛失後に NPC に誰かがアクセスしていたか，確認をお願いします。ところで，今，F さんは L システムにアクセスができない状態ですね。

W 主任 ：はい。F さんの NPC 内にあるクライアント証明書と秘密鍵が盗用される可能性を考慮した措置です。もし，F さんの利用アカウントで認証に成功したとしたら，F さんが担当する全ての顧客の情報にアクセスできてしまいます。

K 課長 ：すばやく対応してくれましたね。

W 主任：秘密鍵の漏えいの有無を調査するために，何者かが F さんの秘密鍵を使い，クライアント認証して［ e1 ］が L システムの［ e2 ］のログ中にないか確認しました。確認したログの範囲では，不審な点はありませんでした。F さんがまた L システムにアクセスできる状態にするために，［ f ］，アクセス権を有効にする予定です。

K 課長 ：F さんの NPC は，今後どのようになるのでしょうか。

W 主任 ：一時的にでも自社の管理を離れたことによって情報が盗まれたり，マルウェアが入れられたりした可能性があるので，［ g1 ］。

K 課長 ：［ g2 ］。

こうして K 課長はインシデント対策会議に臨み，インシデント報告書案に沿って事実関係，対応状況及び今後の調査予定を報告し，R 支社長の了解を得た。

2 日後，W 主任から，NPC 内に顧客情報は追加保存されていなかったこと，及び F さんが NPC を紛失していた間に NPC がアクセスされた痕跡はなかったことの報告があり，このインシデントは収束が宣言された。

設問1　〔インシデント報告書案の作成〕について，図2中の［ a ］～［ d ］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。

aに関する解答群

ア　Fさんが紛失した情報の内容及び量の特定

イ　Fさんが持ち出した情報の持出し方法の特定

ウ　インシデントによる損害額の検討

エ　インシデントの再発防止策の策定

bに関する解答群

ア　“対策済NPC”シール発行記録の確認

イ　Fさんの利用記録の確認

ウ　資産管理番号とFさんへの貸与記録の確認

エ　情報セキュリティ対策の実施状況の確認

cに関する解答群

ア　Fさんがオフィスで使っている

イ　Fさんが外出先からアクセスできる

ウ　Fさんが顧客情報を保管している

エ　Fさんが顧客訪問の際に画面を見せてもらったことがある

dに関する解答群

ア　Fさんが当日訪問した顧客に関する顧客情報がダウンロードされていないかどうかに絞った確認

イ　社外から操作ログが改ざんされていないかどうかの確認

ウ　社外からパスワードリスト攻撃が行われていないかどうかの重点的な確認

エ　社外から不審なアクセスがないかどうかの幅広い確認

設問2　〔インシデントの影響及び対応〕について，(1) ～ (5) に答えよ。

(1) 本文中の下線 ① について，どのような方法が考えられるか。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) 1 か月間の NPC 期間持出しの承認を得るとその期間中に，NPC を会社に持ち帰り，追加で保存できる。

(ii) NPC の持出しとは別に，会社貸与の USB メモリに保存して持ち出すことによって，NPC に保存できる。

(iii) 外出先から L システムにアクセスして，NPC にダウンロードして保存できる。

(iv) 外出先で，公衆無線 LAN に接続して，インターネット上で他社の公開 Web サイトを閲覧し，NPC にダウンロードして保存できる。

(v) 顧客訪問先で，顧客から借りた USB メモリからコピーして保存できる。

解答群

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

(2) 本文中の下線 ② について，表 1 に記載されている対策のうち，NPC 紛失時に，NPC 内のデータが読み取られるリスクを低減するための対策として最も効果的なものを，解答群の中から選べ。

解答群

ア (a)	イ (b)	ウ (c)
エ (d)	オ (e)	カ (f)
キ (g)	ク (h)	ケ (i)

(3) 本文中の［ e1 ］，［ e2 ］に入れる字句の組合せはどれか。e に関する解答群のうち，最も適切なものを選べ。

e に関する解答群

	e1	e2
ア	アクセスを試みた形跡	本日 00:00 から 11:20 まで
イ	アクセスを試みた形跡	本日 00:00 から 15:30 まで
ウ	情報をダウンロードした形跡	本日 00:00 から 11:20 まで
エ	情報をダウンロードした形跡	本日 00:00 から 15:30 まで

(4) 本文中の［ f ］に入れる適切な字句を，解答群の中から選べ。

f に関する解答群

ア　F さんの L システムの利用アカウントのパスワードを変更した後

イ　F さんの従来のクライアント証明書を失効させてから，新しい鍵ペアを生成しクライアント証明書を発行し直した後

ウ　F さんの秘密鍵のバックアップを取り寄せた後

エ　本社情報システム部で L システムのログを保全した後

(5) 本文中の［ g1 ］，［ g2 ］に入れる字句の組合せはどれか。g に関する解答群のうち，最も適切なものを選べ。

g に関する解答群

	g1	g2
ア	HDD を複製し，今日中には返却します	入念な調査をお願いします
イ	証拠保全をした上で調査しています	F さんには新しい NPC を手配しましょう
ウ	直ちに HDD を取り出し，データを消去した上で，破壊し，破棄します	情報漏えいがないように，確実にお願いします
エ	直ちに NPC を初期化して，OS から入れ直します	それなら安心ですね
オ	返却前に，F さんに NPC の中のファイルを点検してもらいましょう	私も立ち会います

問３　業務用 PC での Web サイト閲覧に関する次の記述を読んで，設問１～３に答えよ。

P 社は，従業員数 1,000 名の消費者向け健康食品製造会社であり，経営方針として自社のブランドイメージを重視している。P 社のマーケティング部では，社外向け Web サイトのコンテンツのうち，製品紹介情報，IR 情報，CSR 情報などの管理を行っている。マーケティング部には 20 名が在籍し，二つの課がある。マーケティング 1 課は，ブランドマーケティング戦略を担当している。マーケティング部では，情報セキュリティ責任者を A 部長が，情報セキュリティリーダをマーケティング 1 課の B 課長が務めている。

P 社では全従業員が基盤情報システムを利用して日々の業務を行っている。基盤情報システムは，会社貸与の業務用 PC（以下，PC という），LAN 及びインターネット接続から成るネットワークサービス，ディレクトリサービス，社内ファイル共有サービス，電子メールサービスなどから構成されている。P 社従業員は，LAN に接続された各自の PC から各サービスを利用している。また，LAN からのプロキシサーバを経由しないインターネット接続はファイアウォールによって遮断されている。

P 社には，基盤情報システム以外にも勤怠管理システム，交通費精算管理システム及び人事管理システムがある。P 社従業員は，出勤時と退勤時に各自の磁気ストライプカード型の従業員証をタイムレコーダに通すことになっており，出退勤時刻が勤怠管理システムに記録される。P 社の課長以上の職位の者は，直属の部下について，勤怠管理システムを用いて出退勤時刻などの勤怠管理情報を，交通費精算管理システムを用いて交通費精算情報を，人事管理システムを用いて人事評価情報を確認できる。

基盤情報システム，勤怠管理システム，交通費精算管理システム及び人事管理システムは同じタイムサーバに基づいて時刻同期がなされている。それらの情報システム及び自社 Web サイトの構築と運用管理は，情報システム部が行っている。

情報システム部の C 部長が，P 社の最高情報セキュリティ責任者（CISO）を務めている。情報システム部には運用管理課があり，基盤情報システムに対して図 1 に示す設定と運用管理を行っている。また，利用については図 2 に示す P 社基盤情報システム利用規程（以下，利用規程という）を整備している。

1. 設定
・PC 上のハードディスクドライブ（以下，HDD という）全体を暗号化
・PC 上の Web ブラウザで，プロキシサーバを利用するように設定
・社内ファイル共有サービスでの共有フォルダの設定は，次のとおり
　- ディレクトリサービスを利用してアクセス権の設定を管理
　- アクセス権は，各利用部門からの申請に応じて設定単位を変更可能
　- アクセス権の設定単位は，次のいずれか一つを選択
　　部単位：特定の部に属する従業員だけがアクセス可能
　　課単位：特定の課に属する従業員だけがアクセス可能
　　職位単位：特定の部に属する部長，課長，主任のいずれかの職位以上の従業員だけがアクセス可能
　　従業員単位：特定の従業員だけがアクセス可能
　- デフォルトのアクセス権は，課単位
2. 運用管理
・PC 上の OS，オフィスソフト，Web ブラウザ，ウイルス対策ソフトなどのソフトウェアのインストール，パッチ適用及びアップデートを一括で運用管理
・一括運用管理対象のソフトウェアのパッチ及びアップデートがベンダからリリースされた場合は，適用要否の確認を速やかに行い，適用が必要と判断したものを適用
・PC の管理者権限は，PC 運用管理担当者だけに付与
・各利用部門からの情報システム利用に関する各種申請について，利用規程にのっとった承認を得たものだけを受理

図 1　P 社基盤情報システムにおける設定と運用管理（抜粋）

1. パスワードは，使用できる文字種（大小英字，数字，記号）全てを組み合わせて 8 文字以上，かつ，他人に推測されにくいものとし，他人に知られないよう適切に管理すること。
2. 機密性が高い電子データには，暗号化を施し，適切なアクセス権を設定すること。
3. 各利用部門から情報システム部への情報システム利用に関する各種申請については，所属部門長及び情報セキュリティリーダの承認を得ること。
　なお，機密性が高い情報の取扱いに関連する申請内容については，CISO の承認を得ること。
4. 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）の発生時には，その対応として第一に被害拡大防止に努め，第二に証拠保全に努めること。
　なお，所属部門の情報セキュリティリーダ又は情報システム部からの指示があった場合には，その指示に従うこと。

図 2　利用規程（抜粋）

〔インシデントの発見と初動対応〕

9 月 26 日（月）10 時，運用管理課の H さんが基盤情報システムを運用監視していたところ，9 月 23 日（金）20 時から 25 日（日）にかけての社内からインターネットへの通信量が前週の金曜日から日曜日にかけてのものと比較して大幅に増えていることを発見し，直ちに運用管理課の D 課長に報告した。D 課長は不審に思い，プ

ロキシサーバのログを調査するよう H さんに指示した。その結果，図 3 に示すことが判明した。

・大量の通信は，同一の社外 IP アドレス（以下，アドレス Y という）へのアクセスであった。
・POST メソッドから始まって CONNECT メソッドが連続した HTTP over TLS（HTTPS）通信であった。
・発信元はマーケティング 1 課に所属する入社 2 年目の E さんの PC（以下，E-PC という）であった。

図 3　プロキシサーバのログの調査結果

D 課長はその旨を C 部長に報告の上，B 課長に連絡した。連絡を受けた B 課長は利用規程にのっとり，①E さんに初動対応を指示し，併せて A 部長に報告した。

B 課長は，自席の PC を利用して E さんの［ a1 ］を調査した。E さんは市場調査業務を担当しているので，P 社の競合情報，消費者動向などについての様々なインターネット上の Web サイトを日々閲覧している。次に情報システム部の協力の下，B 課長による調査結果と E-PC から［ a2 ］へのアクセスログとを突き合わせたところ，大量の通信が記録されていた時刻の中には，E さんが［ a3 ］時刻が含まれていた。さらに，E さんへの聞き取り調査を行ったところ，E さんは，P 社が入居するオフィスビルの法定点検に基づく停電時以外は離席，外出又は帰宅の際，E-PC にログインしたままにしていたことが判明した。これらのことから，今回の不審なアクセスは，E さん自身によるものではないと推定された。

B 課長と D 課長による協議の結果，同日 15 時に，情報システム部による調査及び対応が開始された。情報システム部における調査の結果を図 4 に，各事象の発生日時を表 1 に示す。

・E-PC は，不正プログラム V に感染していた。
・不正プログラム V は，E-PC にインストールされていたソフトウェア Z（以下，ソフト Z という）の脆弱性 M を突いて侵入するものであった。ソフト Z は，インストールされて以来，パッチが適用されていなかった。
・E-PC 上では，ウイルス対策ソフトが起動しないように管理者権限を用いて設定されていた。

図 4　情報システム部における調査の結果（抜粋）

表1　各事象の発生日時

日付	時刻	事象
7月4日	11:00	E さんが，業務の都合から，しばらくの間，E-PC 上のウイルス対策ソフトが起動しないように設定してほしいと H さんに依頼
	11:30	H さんが，E-PC 上のウイルス対策ソフトが起動しないように管理者権限で設定
8月2日	15:00	ソフト Z の開発元が脆弱性 M の対策パッチをリリース
8月4日	10:00	ウイルス対策ソフトの開発元が，不正プログラム V に対応するパターンファイルをリリース
9月23日	20:00	E-PC がアドレス Y に向けた通信を開始
9月26日	10:00	H さんが通信量の大幅増加を発見，D 課長に報告 H さんがプロキシサーバのログを調査開始
	13:30	H さんがプロキシサーバのログの調査結果を D 課長に報告 D 課長が C 部長に報告，B 課長に連絡
	13:45	B 課長が E さんに初動対応を指示，A 部長に報告後，E さんへの聞き取り調査などを開始
	14:30	B 課長と D 課長が協議
	15:00	②情報システム部が，次に示す調査及び対応を開始 ・社内からアドレス Y への通信を遮断 ・E-PC の HDD 内のデータを証拠保全 ・E-PC からの大量の通信の原因の把握

注記　日付は全て同年のものである。

〔情報システム部による調査結果の中間報告〕

情報システム部による E-PC の調査結果の中間報告が，9 月 27 日（火）13 時から行われた。次は，その時の D 課長と B 課長の会話である。

D 課長 ：マーケティング部と情報システム部の間では，ソフト Z に対するパッチ適用を含めた運用管理について何も取決めがない状態でした。マーケティング部からのソフトウェアインストール申請書には，パッチ適用などの運用管理についての依頼は記載されていませんでした。

B 課長 ：すみません，依頼内容が不十分でしたね。

D 課長 ：他にもこれらと同じようなことがあったら問題なので，引き続き調査をします。ところで，7 月 4 日から昨日までのログ中の通信先を解析したところ，ウイルス対策ソフトの開発元などによって悪意ある Web サイトと判断された URL 又は IP アドレスに該当するものはありませんでした。感染原因は，電子メールの添付ファイルや USB メモリからと考えられますが，も

し，感染原因がインターネット上の Web サイトへのアクセスだとしたら，E さんがアクセスしたのは，閲覧するだけで不正プログラムに感染するように，企業の［ b ］の公開 Web サイトが［ c ］されたものだったとも考えられます。

B 課長 ：［ b ］の URL ということであれば，悪意ある Web サイトだとは思わないので，防ぎようがないですね。Web サイトが［ c ］されたことによって，その Web サイトの所有者たる企業は［ d ］となるだけでなく，Web サイト閲覧者に対しても不正プログラムによる被害が及ぶので，［ e ］の立場になってしまうおそれがあり，非常に怖いですね。③私自身の職務からも人ごとではないので，すぐに対策を検討しましょう。D 課長，協力をお願いします。

〔課題の改善〕

内容が不明なデータが E-PC から社外に大量に送信されたことから，［ f ］が起きたおそれもあると B 課長は考えた。そこで E さんにヒアリングした。その結果，マーケティング 2 課へのヒアリングも必要と考えられたので，マーケティング 2 課のプレゼントキャンペーン担当を務めている G 主任にもヒアリングを行った。それらの結果を図 5 に示す。

1. E さんへのヒアリング結果
・マーケティング 2 課が 8 月に募集した，P 社製品購入者向けプレゼントキャンペーンの匿名アンケート結果に関するファイル（以下，アンケートファイルという）を，9 月 8 日（木）頃，社内共有フォルダ N 内で発見した。
・④いつか業務に役立つかもしれないと考え，アンケートファイルを社内共有フォルダ N から E-PC 内にコピーした。
・E-PC 内には，暗号化されたアンケートファイルを復号したものはなかった。また，アンケートファイル以外には機密性が高い情報を含んだファイルはなかった。
2. G 主任へのヒアリング結果
・アンケートファイルの暗号化には，マーケティング部内の共有パスワードを利用していた。
・アンケートファイルは，G 主任を含めたマーケティング 2 課のプレゼントキャンペーン担当者 3 名が共同作業できるように，社内共有フォルダ N に保存していた。
・アンケート結果には，P 社製品の味や食感，健康食品としての有用性などへの批評や競合会社製品との比較による辛らつな意見が書かれていた。

図 5　B 課長による，E さん及び G 主任へのヒアリング結果

B 課長は，A 部長にこれまでの調査結果の報告を行うとともに，図 6 に示す項目の検討が必要であると進言した。

1. 調査結果から発見された，改善すべき課題
  1-1 ソフト Z の運用管理についてマーケティング部と情報システム部の間で取決めがなかった。
  1-2 E さんと H さんの当事者間だけで E-PC 上のウイルス対策ソフトの停止を決めていた。
  1-3 H さんが E-PC 上のウイルス対策ソフトを起動するように設定を戻すのを忘れていた。
  1-4 E さんが業務と直接関係ないマーケティング 2 課の管理下のアンケートファイルを E-PC 上に保存していた。
  1-5 アンケートファイルの暗号化のパスワードが，部内の共有パスワードであった。
2. 情報システム部の調査から［ f ］が発生したことが確かになった場合の対処
  2-1 P 社所在地管轄の警察署や関係機関への届出又は報告
  2-2 アンケートファイルの関係者へのおわびと説明，社外への公表

図 6　検討が必要な項目

B 課長は，社内関係者の協力を得て課題の改善を実施した。また，中間報告以降の情報システム部の調査結果から［ f ］が発生したおそれは低いことが分かった。

B 課長は，改善すべき課題が図 6 の 1-1 から 1-5 の他にもないかの確認を A 部長に提案し，了承を得た。

B 課長は，改善すべき課題が他にもないか，［ g ］を実施した。その結果，他の課題が発見され，マーケティング部内で改善策の検討が開始された。

A 部長は，マーケティング部内での他の課題の発見に至った B 課長の提案を高く評価した。発見された課題とその改善策を A 部長が P 社経営陣に報告したところ，これらの提案は，全社的な改善活動に発展した。

設問1　〔インシデントの発見と初動対応〕について，(1)～(3)に答えよ。

(1) 本文中の下線①について，次の(i)～(v)のうち，B課長がEさんに指示すべき初動対応だけを全て挙げた組合せを，解答群の中から選べ。

(i) E-PCのHDD内のフォルダとファイルに対して何も操作をしない。

(ii) E-PCの電源を強制切断し，かつ，電源ケーブルを電源コンセントから外す。

(iii) E-PCをLANから切り離す。

(iv) E-PCを再起動する。

(v) E-PCを使ってEさんの基盤情報システムへのログインパスワードを変更する。

解答群

ア (i)　　イ (i)，(iii)　　ウ (i)，(iv)，(v)

エ (ii)，(iii)　　オ (ii)，(v)　　カ (iii)，(iv)，(v)

キ (iii)，(v)　　ク (iv)，(v)

(2) 本文中の［ 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	勤怠管理情報	インターネット	退勤していた
イ	勤怠管理情報	ディレクトリサービス	休暇を取得していた日の
ウ	交通費精算情報	社内ファイル共有サービス	外出していた
エ	交通費精算情報	ディレクトリサービス	出張していた日の
オ	人事評価情報	インターネット	無断欠勤していた日の
カ	人事評価情報	社内ファイル共有サービス	残業していた

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

(i) E-PCのHDDを別のHDDにフルコピーし，その別のHDDを“秘密”とラベルに書いた資料保存用紙封筒に入れ，封印し，Eさんが管理するマーケティング部の鍵付きロッカーに保管

(ii) E-PCのHDDを別のHDDにフルコピーした上で，最新のパターンファイルを搭載した別のPCに，その別のHDDを接続してフルスキャンを実施

(iii) アドレスYへの通信をプロキシサーバで遮断し，ファイアウォールではインターネットへの通信のうち，プロキシサーバを経由しないものだけを許可

(iv) 他の作業に先駆けて最初にE-PCにOS及びアプリケーションのクリーンインストールを実施した上で，E-PCをEさんに返却

(v) プロキシサーバなどのネットワーク機器上のログとE-PC上のイベントログなどを時系列に沿って整理及び分析

解答群

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

設問2 〔情報システム部による調査結果の中間報告〕について，(1)，(2)に答えよ。

(1) 本文中の［ b ］～［ 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。

b，cに関する解答群

ア 改ざん	イ 偽装	ウ 正規
エ 設計	オ 非正規	カ ボット化

d，eに関する解答群

ア 加害者	イ 首謀者	ウ 助言者
エ 扇動者	オ 第三者	カ 被害者

(2) 本文中の下線③について，B課長とD課長はどのような対策を検討したか。解答群のうち，最も適切なものを選べ。

解答群

ア 自社Webサイトのアクセシビリティを見直し，自社Webサイトの閲覧者に対する利便性と安全性を確保することによって，自社のブランドイメージの向上を図る。

イ 自社Webサイトの改ざんを防ぐために，自社Webサーバを情報システム部に依頼して速やかに停止させ，自社 Web サーバを社外のパブリッククラウド上に移行し，他者とのリスク共有（リスク移転）を図る。

ウ 自社 Web サイトの脆弱性検査を定期的に実施して，問題があれば修正する。また，新たな脆弱性が発見された場合にも必要な対応をとる。

エ 自社 Web サイトのトップページ上において，重要なお知らせとして，自社 Web サイトにドライブバイダウンロードが仕掛けられた可能性があると公表し，自社Webサイトの閲覧者に対して注意を喚起する。

設問3 〔課題の改善〕について，(1)～(3)に答えよ。

(1) 本文中及び図6中の［ f ］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。

fに関する解答群

ア E-PC への DDoS 攻撃　　イ E-PC への辞書攻撃

ウ E-PC への総当たり攻撃　　エ 情報改ざん

オ 情報破壊　　カ 情報漏えい

(2) 図5中の下線④について，社内共有フォルダNのアクセス権の設定単位はどのようになっていたと考えられるか。解答群のうち，最も適切なものを選べ。

解答群

ア 課単位　　イ 従業員単位　　ウ 職位単位　　エ 部単位

(3) 本文中の［ g ］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。

g に関する解答群

ア　情報システムのうち，マーケティング部内の従業員が利用しているものに対し，脆弱性検査

イ　マーケティング部内で取り扱っている全ての情報資産とその取扱い状況を可視化した上で，リスクアセスメント

ウ　マーケティング部内で取り扱っている全てのファイルの所在と所有者を洗い出し，各ファイルのアクセス権限の見直し

エ　マーケティング部における，E-PC 以外でのウイルス対策ソフトを停止させたままの PC 又はパッチ適用並びにアップデートが行われていない PC の有無の確認

オ　マーケティング部における，E-PC 以外でのソフト Z がインストールされた PC の有無と利用状況の確認

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

6. 退室可能時間に途中で退室する場合には，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。