SG

平成28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。

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　標的型攻撃メールの脅威と対策に関する次の記述を読んで，設問1，2に答えよ。

Y社は，事務用機器を主力商品とする販売代理店である。従業員数は1,200名であり，本社には営業部，情報システム部，総務部などがある。

〔PCのマルウェア感染〕

ある日，情報システム部は，Y社内の1台のPCが大量の不審なパケットを発信していることをネットワーク監視作業中に発見し，直ちに外部との接続を遮断した。

情報システム部による調査の結果，営業部に所属する若手従業員G君が，受信した電子メール（以下，電子メールをメールという）の添付ファイルを開封したことが原因で，G君のPCがマルウェアに感染し，大量のパケットを発信していたことが判明した。幸いにも，情報システム部の迅速な対処によって，顧客情報の漏えいなどの最悪の事態は防ぐことができた。

〔受信したメール〕

情報システム部のS主任は，営業部の情報セキュリティリーダであるE課長に，今回の事態に関する調査結果を報告した。次は，その時の会話である。

S主任　：G君が受信したメールは，いわゆる標的型攻撃メールと呼ばれるものです。標的型攻撃メールとは，［　a　］の組織や個人を対象として，受信者のPCにマルウェアを送りつけ，情報を窃取することなどを目的とするメールであり，［　b　］の組織や個人を対象として送られるウイルスメールとは異なるものです。

E課長　：最近は国内でも標的型攻撃メールに起因する情報漏えい事故が多数発生しており，大手企業や官公庁以外もターゲットになり得るので，営業部の従業員には十分に注意するよう言っていたのだが。

S主任　：標的型攻撃メールでは，注意していたつもりでも，気付かずにマルウェア感染が起こります。また，受信者が疑いをもたないように，メールの差出人を公的機関などに詐称したり，メールの件名や内容を受信者の業務に関連したものに偽装したりするといった，［　c　］を利用します。

E 課長　：G 君が受信したメールを具体的に説明してくれるかな。

S 主任　：メールの内容を図 1 に示します。この内容から，①受信者の疑いを低減させる手口や，受信者の動作を巧みに誘導する手口などが見受けられます。

S 主任は，②標的型攻撃メールによく見られる注意すべき特徴のうち，G 君が受信したメールに見られる特徴を説明した。

差出人：F <F@zz-freemail.co.jp>　　送信日時：2016/03/18 10:22
宛先　：info@y-sha.com
CC　　：
件名　：Re: Re: 【至急】製品導入に関する問合せ

添付ファイル：質問事項.exe

G様

お世話になっております。
先日，貴社の製品について問合せをしたX社のFです。
これまで，貴社の事務用機器に関する情報を提供していただき，
ありがとうございました。
弊社では，今回，貴社から提案していただいた製品について，
導入する方向で検討を進めております。
その中で，確認したい事項が幾つか出てきました。
つきましては，急なお願いで恐縮ですが，添付ファイルの質問内容を
ご確認の上，本日15時までに回答をいただけないでしょうか。
よろしくお願いいたします。

X社　調達部　F
E-mail: F@x-sha.co.jp
URL: http://www.x-sha.co.jp

図 1　G 君が受信したメールの内容

〔ヒアリング〕

S 主任からの調査報告を受けた E 課長は，G 君に対して，このメールを受信した際の状況及び対応に関してヒアリングをした。また，Y 社の情報セキュリティインシデント管理規程（以下，管理規程という）どおりには対応しなかった理由を G 君に確認した。

E課長がまとめたヒアリング結果を図2に，Y社の管理規程を図3に示す。

・X社は過去に取引がある会社であった。
・F氏と直接会ったことは無かったが，10日前から，製品の問合せが3回あり，メールでやり取りをしていた。
・メールの添付ファイルを開封した際は，見慣れないウィンドウが表示されただけでドキュメントは開くことができなかった。そこで，ファイルを再送してほしい旨を先方にメールで返信したが，15時までと急いでいた割にその後の返信が無く不審に思った。再度連絡しようと思っていたが，別件で多忙になり，確認ができなかった。
・その後，PCの処理速度が遅くなったり，見慣れないウィンドウが表示されたりするなどの不具合や不審な事象が発生していたが，その都度，PCを再起動するなどして解決を試みた。また，ウイルス対策ソフトが動作し，パターンファイルが最新になっていることを確認できたのでマルウェア感染はあり得ないだろうと考え，誰にも相談せず，報告もしなかった。
・以前に他の部のH君が，顧客から貸与されたUSBメモリをPCに接続してマルウェア感染が起きたことを上司に報告した際に，上司から大変厳しく叱責されたとH君本人から聞いていたので，マルウェア感染と確信できない限りは，報告したくないと思っていた。
・管理規程については，新入社員研修の際に一度見たことがある程度で，重要な規程とは思っていなかった。
・標的型攻撃メールについては，聞いたことはあったが理解はしていなかった。

図2　G君へのヒアリング結果

第1章　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）の定義
・インシデントとは次のことをいう。
“不正アクセス”，“マルウェア感染”，“情報の漏えい”，“情報の改ざん”，“情報の消失”，
（省略）
第2章　インシデント検知時の報告及び対処
・従業員は，インシデントを発見した際には，速やかに情報セキュリティリーダに報告し，その指示に従うこと。
なお，インシデントであるかどうか判断がつかない疑わしい事象も，自己判断せず同様に報告すること。
・情報セキュリティリーダは，インシデントを認知した場合には，その状況を確認し，情報セキュリティ責任者に速やかに報告するとともに，情報システム部と連携し，被害の拡大防止を図るための応急措置及び復旧に係る指示又は勧告を行うこと。
・従業員は，各自の判断で復旧対応や解決を試みるのではなく，必ず情報セキュリティリーダの指示又は勧告に従うこと。
第3章　インシデントの原因調査及び再発防止
・情報セキュリティリーダは，情報システム部と協力してインシデントの原因を調査するとともに，再発防止策を検討し，報告書にまとめて情報セキュリティ責任者に報告すること。
（省略）

図3　管理規程

〔情報セキュリティ意識向上に向けて〕

次は，ヒアリング実施後のＥ課長とＳ主任との会話である。

Ｓ主任　：標的型攻撃メールによるマルウェア感染を完全に防ぐことは難しいので，被害を最小化するためには，メールの添付ファイルを開封した後に従業員が適切な対応を取ることが重要になります。

Ｅ課長　：そうだね。③今回の初動対応における問題点は二つあったと思う。本来であれば，管理規程に基づき，疑わしい事象を発見した従業員は，［　d　］に報告をしなければならない。また，報告に当たっては，［　e　］報告することも重要だ。

Ｓ主任　：おっしゃるとおりです。今回の問題点を解決するには，規程やルールは単に策定しただけでは不十分であり，それらが順守されるように［　f1　］，［　f2　］の２点を行うことが重要だと考えられます。

Ｅ課長　：今回のような標的型攻撃メールなどへの対策に当たっては，従業員一人一人の情報セキュリティ意識を向上させる地道な活動が必要だと思う。まずは，④実際に攻撃を受けた場合にも一人一人が適切に対応できるかを定量的に測定し評価できるようにしていきたい。そのための全社的な取組みも情報システム部で実施してもらえないだろうか。

Ｓ主任　：承知いたしました。検討し実施したいと思います。

Ｅ課長からの提案もあって，Ｙ社では，従業員の情報セキュリティ意識向上に着実に取り組むようになった。

設問1　〔受信したメール〕について，(1) ～ (4) に答えよ。

(1) 本文中の［ a ］，［ 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。

a，b に関する解答群

ア　海外	イ　架空	ウ　官界
エ　国内	オ　大企業	カ　中小企業
キ　特定	ク　不特定多数	ケ　民間

(2) 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　AES	イ　ゼロデイ攻撃
ウ　ソーシャルエンジニアリング	エ　トロイの木馬
オ　ヒヤリハット	カ　ブルートフォース攻撃

(3) 本文中の下線 ① について，今回の攻撃者が使った手口として考えられるものを二つ，解答群の中から選べ。

解答群

ア　製品を導入する方向で検討を進めているという趣旨を伝えた上で，質問の回答期限を指定することによって添付ファイルを開くよう誘導している。

イ　メールの本文に Y 社の従業員しか知り得ない情報を記載することによって疑いを低減している。

ウ　メールの本文に正当な URL を装ったリンクを記載した上で，その URL リンクをクリックするよう指示し，誘導している。

エ　メールのやり取りを数回行うことによって疑いを低減している。

(4) 本文中の下線②について，次の(i)～(iii)のうち，G君が受信したメールに見られる特徴だけを全て挙げた組合せを，解答群の中から選べ。

(i) 差出人のメールアドレスがY社の社内メールアドレスに詐称されている。

(ii) 差出人のメールアドレスと，本文の末尾に記載された署名のメールアドレスが異なる。

(iii) 実行形式ファイルが添付されている。

解答群

ア (i)	イ (i)，(ii)	ウ (i)，(ii)，(iii)
エ (i)，(iii)	オ (ii)	カ (ii)，(iii)
キ (iii)		

設問2 〔情報セキュリティ意識向上に向けて〕について，(1)～(5)に答えよ。

(1) 本文中の下線③について，次の(i)～(iv)のうち，今回の初動対応における問題点を二つ挙げた組合せを，解答群の中から選べ。

(i) PCの不具合に気付いても直ちに再インストールなどの復旧対応を行わなかった点

(ii) 問合せ対応を行うに当たって，X社との最近の取引記録を確認しなかった点

(iii) 不審な事象が起きたにもかかわらず，情報セキュリティリーダに報告しなかった点

(iv) 不審な事象が起きたにもかかわらず，マルウェアには感染していないと自己判断した点

解答群

ア (i)，(ii)	イ (i)，(iii)	ウ (i)，(iv)
エ (ii)，(iii)	オ (ii)，(iv)	カ (iii)，(iv)

(2) 本文中の［ 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。

d に関する解答群

ア　インシデントであると判断した後

イ　原因調査後

ウ　再発防止策を検討した後

エ　速やか

(3) 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　誤った報告を行わないよう，事象をインターネットや書籍などで確認して，類似の事例が確認できたものを

イ　判断に迷う事象であっても自己判断せずに

ウ　部内の同僚と相談してから，報告するように勧められた事象を

エ　報告事項がそろうのを待って，レポートにまとめたものを

(4) 本文中の［ f1 ］，［ f2 ］に入れる，次の (i) ～ (iv) の組合せはどれか。f に関する解答群のうち，最も適切なものを選べ。

(i) 管理規程の内容に関する従業員への周知

(ii) 情報共有や報告が包み隠さず行われるような組織文化の醸成

(iii) 情報セキュリティにおけるクラッキング手法の教育

(iv) マルウェア感染時の迅速な復旧対応方法の指導

f に関する解答群

	f1	f2
ア	(i)	(ii)
イ	(i)	(iii)
ウ	(i)	(iv)
エ	(ii)	(iii)
オ	(ii)	(iv)
カ	(iii)	(iv)

(5) 本文中の下線 ④ について，E 課長の提案に応える取組みはどれか。解答群のうち，最も適切なものを選べ。

解答群

ア 標的型攻撃メールについて，従業員の PC がマルウェア感染しないために注意すべき事項を標語として作成して掲示する。

イ 標的型攻撃メールへの対策を題材とする DVD 上映会を年に 2 回開催し，従業員の出席率を確認する。

ウ 標的型攻撃メールを起因とするインシデントについて，他社で発生した事例を月に 1 回，イントラネット上の掲示板で紹介する。

エ 模擬の標的型攻撃メールを従業員に期間を空けて何回か送付し，添付ファイル開封後の報告完了率，報告完了までに要した時間などの変化を調査する。

問2　業務委託におけるアクセス制御に関する次の記述を読んで，設問1，2に答えよ。

A社は従業員数200名の通信販売業者である。一般消費者向けに生活雑貨，ギフト商品などの販売を手掛けており，商品の種類ごとに販売課が編成されている。

〔Z販売課の業務〕

現在，Z販売課は，商品Zについて顧客から電子メール又はファックスによる注文及び問合せを受け，その対応を行っている。商品Zの販売に関わる要員（以下，商品Z関連要員という）は，販売責任者であるZ販売課N課長，及びその管理下に5名の担当者，並びに業務委託先の管理者であるB社運用課L課長，及びその管理下に8名の担当者の，計15名で構成されている。商品Z関連要員の業務を図1に示す。

1. 受注管理業務
　顧客から届く注文を確認し，受注手続を行う。受注管理システム（以下，Jシステムという）を利用する。本業務は，A社のZ販売課の要員が担当する。
(1) 入力
　担当者は，届いた注文（変更，キャンセルを含む）の内容を確認し，不備があれば顧客に問い合わせる。不備がなければその情報をJシステムに入力し，販売責任者に承認を依頼する。
(2) 承認
　販売責任者は，注文の内容とJシステムへの入力結果を突き合わせて確認し，問題がなければ承認する。問題があれば差し戻す。
2. 問合せ対応業務
　顧客からの問合せに対応する。問合せ管理システム（以下，Tシステムという）を利用する。本業務は，業務委託先であるB社の運用課の要員が担当する。
(1) 入力
　担当者は，顧客から届いた問合せの内容を確認し，回答案をTシステムに入力して，管理者に承認を依頼する。
(2) 承認
　管理者は，回答案を確認し，問題がなければ承認する。これによってTシステムから顧客に回答が返信される。問題があればコメントを付記して差し戻す。

補足：Jシステム及びTシステムはA社の情報システム部が運用している。

図1　商品Z関連要員の業務（概要）

B社は，自社内にA社からの受託業務専用のオペレーションルームをもち，そこからA社のTシステムにアクセスしている。B社は，A社からの受託業務に必要な

設備及び管理体制を整えており，A 社が定める情報セキュリティ要件を満たしている。

〔J システム及び T システムの操作権限〕

Z 販売課では，J システム及び T システムについて，次の利用方針を定めている。

［方針 1］　1 人の利用者に，一つの利用者 ID を登録する。

［方針 2］　一つの利用者 ID は，1 人の利用者だけが利用する。

［方針 3］　ある利用者が入力した情報は，別の利用者が承認する。

［方針 4］　販売責任者は，Z 販売課の全業務の情報を閲覧できる。

J システム及び T システムでは，業務上必要な操作権限を利用者に与えるためにシステム上の役割（以下，ロールという）を定義する機能が実装されている。ロールには，業務上必要な操作権限の組合せが付与される。利用者 ID にロールを設定することによって，利用者の操作権限が決まる。一つの利用者 ID にはロールを一つだけ設定する。システム利用部署の長は，所属する利用者の利用者 ID に対するロール設定を情報システム部に依頼する。情報システム部が受けた依頼はシステムに登録され，翌営業日の朝 5 時に自動的にシステムに反映される。

J システム及び T システムにおいて，商品 Z 関連要員の利用者 ID に設定されているロールの種類とその操作権限を表 1 に示す。

表 1　ロールの種類とその操作権限

ロールに付与されている操作権限 / ロール	J システム			T システム		
	閲覧	入力	承認	閲覧	入力	承認
A 社販売責任者	○		○	○		
A 社販売担当者	○	○		○		
B 社管理者				○		○
B 社 T システム担当者				○	○	

注記　○は，操作権限が付与されていることを示す。

例えば，N 課長の利用者 ID には“A 社販売責任者”というロールを設定して，J システムの閲覧及び承認並びに T システムの閲覧の権限をもたせている。

〔受注管理業務の委託〕

Z販売課では，受注管理業務を担当するA社の従業員の作業量が受注増によって増えていることから，この業務の入力作業をB社に対して追加で委託することにした。追加の業務委託で必要となるJシステムの操作権限の見直しを，A社の販売課全体の情報セキュリティリーダを務める販売管理課のM主任が支援することになった。

M主任は，受注管理業務におけるA社とB社の役割分担について，Z販売課のN課長からヒアリングした内容を次のとおり整理した。

［要求1］　B社が入力した場合は，A社が承認する。

［要求2］　A社の担当者が入力した場合は，現状どおりにA社の販売責任者が承認する。

これに基づきM主任が作成した新しい操作権限案を表2に示す。

表2　新しい操作権限案

ロールに付与される操作権限 / ロール	Jシステム			Tシステム		
	閲覧	入力	承認	閲覧	入力	承認
A社販売責任者	○		○	○		
A社販売担当者	○	○		○		
B社管理者	◎	◎		○		○
B社Tシステム担当者				○	○	
B社Jシステム担当者	◎	◎				

注記1　○は，付与される操作権限のうち，表1と同じものを示す。
注記2　◎は，付与される操作権限のうち，表1に比べて新しく追加したものを示す。

次は，この操作権限案についてのM主任とN課長との会話である。

M主任　：N課長の要求に従ってロールとその操作権限を見直してみました。

N課長　：確かに，要求どおりだ。ただ，販売責任者は私だけなので業務が停滞することが心配だ。B社で入力した情報はA社の担当者が承認すればよいので，“A社販売担当者”ロールに承認権限を追加できないだろうか。

M主任　：承認権限を追加すると，<u>①Jシステムで利用方針に違反してしまいます</u>。

N課長　：“A社販売担当者”ロールに承認権限を追加し，その上で，利用方針にも合

うようにしたい。例えば［ a ］ことはできるだろうか。

M主任 ：それならば，利用方針は順守できそうです。ただ，システムの改修が必要ですね。また，②［要求 2］を満たせません。別の案ですが，［ b ］ようにシステム改修するのはどうでしょう。

N課長 ：確かに，それなら［要求 2］も満たせる。早速，その方針で情報システム部にシステム改修の相談をしてくれないか。

M主任 ：承知しました。確認ですが，N 課長は，出張などで承認手続ができなくなるようなケースはありませんか。

N課長 ：今のところ問題ない。ただ，③来年度から毎年 2，3 回，2 週間ほどの海外出張に出る予定なので，誰かに代行してもらう必要が出てくる。この対応も検討したい。それと，B 社の L 課長からの話だが，一日の中でも問合せ数が少ない時間に，問合せ対応業務の担当者の一部が受注管理業務を応援できる運用を希望していたよ。あらかじめ担当者を任命して教育もしておくそうだ。

M主任 ：承知しました。すぐに B 社に詳細を確認して④必要な操作権限を与える方法を検討します。

M主任は，B社の管理者及びA社の情報システム部と調整して，N課長とともにJシステムの改修案，運用案を取りまとめた。

〔B社担当者の追加及び変更〕

A社情報システム部では，社内データベースに格納された情報を閲覧するための情報閲覧システム（以下，D システムという）を提供している。D システムで商品 Z 関連要員に付与されている閲覧権限を表3に示す。

なお，利用者 ID は，J システム及び T システムと共通である。

表3　商品Z関連要員に付与されている閲覧権限（抜粋）

情報のオーナ部署	情報	…	A社Z販売課の要員	B社運用課の要員
販売管理課	在庫情報	…	○	○
販売管理課	販売計画・実績情報	…	○	
サービス企画課	お客様情報	…	○	○
商品企画課	商品カタログ情報	…	○	○
商品企画課	問合せ履歴情報	…	○	○

注記　○は，閲覧権限が付与されていることを示す。

A社では，Dシステムの閲覧権限の付与について，次の手続を定めている。

(1)　各情報のオーナ部署の長が，閲覧権限を付与する対象者を決める。

(2)　情報システム部は，情報のオーナ部署の長の決定に従ってDシステムの閲覧権限を設定する。

(3)　利用部署の希望によって閲覧権限を付与する場合は，利用部署の長が，その情報のオーナ部署の長に申請して承認を得る。申請を承認した情報のオーナ部署の長は，情報システム部に対して閲覧権限の付与を依頼する。

(4)　利用部署が，業務委託先要員への閲覧権限付与を希望する場合は，［　c　］。

次は，B社の担当者の追加及び変更に関する，M主任とN課長の会話である。

M主任　：新しく追加されるB社Jシステム担当者に付与する閲覧権限について相談があります。［　d　］のリスクを低減するために，表3に示すDシステムの閲覧権限を見直して，必要最小限にした方がよいと思います。

N課長　：Jシステム担当者の作業は，届いた注文の確認と入力だ。商品カタログ情報とお客様情報の閲覧だけだな。

M主任　：では，N課長から［　e　］に対して，閲覧権限の付与を申請していただけますか。

N課長　：新しいB社担当者の名簿はできているかな。

M主任　：はい。B社から情報を受領しました。Jシステム担当者は3名です。

N課長　：Tシステム担当者に変更はないかな。

M主任　：あります。⑤来月中に1人が退任し1人が新規に着任すると聞きました。

引継ぎを兼ねて，おおよそ1週間は2人とも在籍してTシステムとDシステムを利用して業務を行う予定です。必要な権限を正しくシステムに登録するために，B社に担当者変更がある場合，原則2週間前に［ f ］から情報提供してもらうよう業務委託契約で定めています。後ほど，⑥正式に情報を受領します。

N課長　：分かった。今回，業務委託の対象システムも人員も増えるので，改めて情報漏えい対策に力を入れていきたい。頼りにしているよ。

こうしてN課長とM主任は必要な準備を進め，新しい体制で業務を開始することができた。

設問1　〔受注管理業務の委託〕について，(1)～(6)に答えよ。

(1)　本文中の下線①について，どの利用方針に違反するか。違反が考えられる利用方針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　［方針1］
イ　［方針1］，［方針2］
ウ　［方針2］
エ　［方針2］，［方針3］
オ　［方針3］
カ　［方針3］，［方針4］

(2)　本文中の下線①について，この利用方針違反はどのリスクを高めると考えられるか。解答群のうち，最も適切なものを選べ。

解答群

ア　正しく入力された注文が承認されず滞留してしまう。
イ　正しく入力された注文の情報が窃取されてしまう。
ウ　不正に入力された注文が差し戻されて滞留してしまう。
エ　不正に入力された注文が承認されてしまう。

(3) 本文中の［ a ］，［ b ］に入れる適切な字句を，解答群の中から選べ。

a，b に関する解答群

ア “A 社販売責任者”ロールを設定した利用者 ID を二つに増やす

イ “B 社 J システム担当者”ロール又は“B 社管理者”ロールを使って入力された注文だけを承認できる権限を追加する

ウ 自分が承認したい注文だけを検索できる機能を追加する

エ 承認できる利用者 ID を，入力者が指定する権限を追加する

オ 他の利用者 ID によって入力された注文だけを承認できる権限を追加する

(4) 本文中の下線 ② について，なぜ［ a ］では［要求 2］を満たせないのか。その理由を，解答群の中から選べ。ここで，［ a ］には正しい答えが入っているものとする。

解答群

ア “A 社販売責任者”ロールの利用者が，B 社で入力された情報を承認できなくなるから。

イ “A 社販売責任者”ロールの利用者が，自分宛ての承認依頼に気づくとは限らないから。

ウ “A 社販売担当者”ロールの利用者が複数人いるとき，1 人が入力し，別の 1 人が承認することができるから。

エ “B 社管理者”ロールの利用者が承認権限をもっているから。

(5) 本文中の下線③について，N 課長が出張中に他の者が代行するための措置のうち，利用方針に合致するものを，解答群の中から選べ。

解答群

ア “A 社販売責任者”ロールを設定した利用者 ID を一つ追加発行し，A 社の担当者の 1 人が，代行者として利用する。

イ A 社の担当者の 1 人を代行者に任命し，“A 社販売責任者”ロールの権限を追加で付与した新しいロールを作成して，代行者の利用者 ID に設定する。

ウ N 課長が，出張の期間に限り，自分の利用者 ID，パスワードを別の販売課の課長に貸す。

エ N 課長の上長に代行を依頼し，代行者の利用者 ID を J システム及び T システムに登録して“A 社販売責任者”ロールを設定する。

(6) 本文中の下線④について，情報システム部に依頼して必要な操作権限を与える方法はどれか。解答群のうち，最も適切なものを選べ。ここで，応援に回す B 社担当者を B 社応援担当者という。

解答群

ア “B 社 J システム担当者”ロールを設定した貸出し用の利用者 ID を準備し，応援の都度，B 社応援担当者にこの利用者 ID を利用させる。

イ “B 社 T システム担当者”ロールの権限と“B 社 J システム担当者”ロールの権限を併せ持つ新しいロールを定義し，B 社応援担当者の利用者 ID に設定しておく。

ウ B 社応援担当者の利用者 ID に対して“B 社管理者”のロールを設定しておく。

エ 応援の都度，B 社応援担当者の利用者 ID に設定されたロールを“B 社 J システム担当者”に切り替えてもらう。

設問2　〔B社担当者の追加及び変更〕について，(1)～(4)に答えよ。

(1)　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　業務委託先の管理者が，利用部署の長に名簿を提出するとともに，情報のオーナ部署の長に申請する

イ　業務委託先の従業員が，利用部署の長に申請し，利用部署の長が，情報のオーナ部署の長に申請する

ウ　利用部署の長が，業務委託先から提出された申請書を情報のオーナ部署の長に転送する

エ　利用部署の長が，業務委託先の管理者から提出された利用者の情報に基づき，情報のオーナ部署の長に申請する

(2)　本文中の［　d　］～［　f　］に入れる適切な字句を，解答群の中から選べ。

dに関する解答群

ア　内部不正　　イ　入力時のタイプミス

ウ　病欠

e，fに関する解答群

ア　B社の管理者　　イ　情報システム部

ウ　情報のオーナ部署の長

(3) 本文中の下線⑤について，対応するために必要な利用者 ID 管理の手続はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア 新任者がすぐに業務を開始できるよう，あらかじめ新任者用の利用者 ID の登録を情報システム部に依頼しておく。退任者の利用者 ID は削除しなくても支障はないのでそのままにしておく。

イ 退任者が本当に業務を離れたことを確認してから，退任者の利用者 ID を新任者用に割り当てるよう，情報システム部に依頼する。

ウ 引継ぎ開始に当たり，新任者の利用者 ID を発行し，引継ぎ期間後，直ちに退任者の利用者 ID を無効化するよう，情報システム部に依頼する。

エ 引継ぎ開始に当たり，直ちに退任予定者の利用者 ID を無効化すると同時に，新任者の利用者 ID を発行するよう，情報システム部に依頼する。

(4) 本文中の下線⑥について，今回の担当者変更のために受領する情報としては**不要なもの**を，解答群の中から選べ。

解答群

ア 新任者の閲覧希望情報　　イ 新任者の着任予定日

ウ 退任者の退任予定日　　エ 退任者の利用者 ID

問３　情報セキュリティ自己点検に関する次の記述を読んで，設問１～４に答えよ。

R 社は従業員数 600 名の投資コンサルティング会社である。R 社では顧客の個人情報（以下，顧客情報という）を取り扱っていることから，情報セキュリティの維持に注力している。

R 社ネットワークでは URL フィルタリングを導入しており，フリーメールサービスを提供する Web サイトやソフトウェアのダウンロードサイトへのアクセスを禁止している。また，従業員にノート PC 又はデスクトップ PC のどちらかを貸与しており，それらの PC（以下，貸与 PC という）では USB メモリを使用できないようにしている。貸与 PC のうち，ノート PC だけが，リモート接続サービスによる社内ネットワークへの接続を許可されている。

海外営業部の部員は 10 人で，顧客は 500 人弱である。各部員は，担当顧客に，電子メールや電話を使って営業を行っている。海外営業部は他の営業部のオフィスとは離れた海外営業部専用のオフィスで業務を行っている。海外営業部で使用している顧客管理システム（以下，C システムという）は，海外営業部だけが使用している。C システムでは，アクセスログを 3 か月分保存している。海外営業部の部員は，出張がなく，全員がデスクトップ PC だけを使っている。

海外営業部では，情報システム部が運用管理を行っているファイルサーバを使用しており，各部員は顧客情報を含むファイルを当該ファイルサーバに一時的に保存する場合がある。その場合は，ファイルのアクセス権を各部員が最小権限の原則に基づいて設定することになっている。R 社では，顧客情報を保護するために，次の 2 点を各担当者が定期的に確認することとなっている。

・ファイルサーバに不要な顧客情報を保存していないか。
・ファイルのアクセス権は適切に設定されているか。

R 社では，情報セキュリティ推進部が実施する情報セキュリティ教育があり，海外営業部では，新たに配属された部員だけが受講することになっている。教育終了後には試験があるが，1 回では合格できず，再度教育と試験を受ける部員が時々いる。この教育資料は，世の中で新たなセキュリティ脅威が発見される都度，情報セキュリティ推進部で更新している。

〔海外営業部の簡易チェック〕

海外営業部のW氏は2か月前に情報セキュリティリーダに任命された。

海外営業部では，自部門の情報セキュリティを確保するために，独自の取組みとして，四半期に1回，海外営業部で作成した情報セキュリティ簡易チェックリスト（表1）を全部員に配布し，記入（以下，簡易チェックという）させている。表1のチェックリストは，5年前に作成されたものである。

表1　海外営業部の情報セキュリティ簡易チェックリスト

No.	チェック項目	OK/NG
ファイルサーバの顧客情報について		
1	業務上の必要がある人だけにアクセス権を付与している。 （全従業員にアクセス権が付与されている状態は不可）	
2	不要になった顧客情報は削除している。（3か月超の保存は不可）	
3	顧客情報は必要な属性だけ保存している。	
（省略）		
9	離席時にはPCの画面をロックしている。	

注記　チェック項目のとおりの場合はOK，チェック項目とは異なる場合はNGを記入する。

W氏が全部員にこのチェックリストを記入してもらったところ，全部員が全てのチェック項目にOKを記入して報告してきた。W氏は，念のため，数人に実施状況を確認したが，いずれも確かに報告のとおりであった。チェックリストは作成から5年も経過しており，情報セキュリティ事故のニュースを最近よく目にするようになったことから，W氏は，表2のチェック項目の追加を部長に提案した。

表2　W氏が作成した情報セキュリティ簡易チェックリスト追加項目案

No.	チェック項目	OK/NG
パスワードについて		
10	他人から容易に見えるところにパスワードを書いていない。	
電子メールの利用について		
11	不審な電子メールの添付ファイルを開いていない。	
情報セキュリティ事故への対応について		
12	情報セキュリティ事故が発生したときの連絡先を知っている。	
オフィスの情報セキュリティについて		
13	帰宅時は顧客情報を含む書類を施錠保管している。	

表2を見た部長は，①“部員がOKと記入してきたとしても，その結果が正しいか客観的に判断できないチェック項目がある”として，W氏に再検討するよう指示した。W氏は，次回の簡易チェックに向けて，チェック項目を見直すことにした。

〔監査部による情報セキュリティ監査〕

R社監査部は，1年に1回，CSA（Control Self Assessment：統制自己評価）方式による情報セキュリティ監査を実施している。CSAとは，監査部が被監査部門を直接評価するのではなく，被監査部門が，自部門の活動を評価することを指す。R社監査部では，被監査部門にCSAの実施を依頼し，その結果を活用して監査を実施している。

R社では，5年前，監査の方式を決定するに当たり，②監査部が各部門を直接監査する方式とCSA方式の利点，欠点を比較評価した。その結果，R社にとってはCSA方式の方がメリットが大きいと判断し，CSA方式を採用した。

R社の監査実施の手順を図1に示す。

1. 監査部が各部門にCSAシートを配布し，CSAの実施と結果の提出を依頼する。
2. 各部門は，CSAシートを用いてCSAを実施する。
3. 監査部が各部門から提出されたCSA結果を検証し，不明な点は当該部門に確認する。
4. “NG”の評価項目がある場合，及び改善が必要と監査部が判断した場合は，当該部門に改善計画の策定と提出を依頼する。

（改善が必要になった場合は次を行う。）

5. 改善が必要な部門は，改善計画を監査部に提出する。
6. 監査部は，提出された改善計画が適切か確認する。
7. 当該部門は，改善計画に基づき改善を実施する。
8. 改善後，当該部門は監査部に改善結果を報告する。
9. 監査部は改善された状況を確認し，適切であれば改善完了とする。

図1　R社の監査実施の手順

〔CSAの実施〕

海外営業部にも監査部からCSAを実施するよう依頼があり，W氏が海外営業部の評価を行うことになった。W氏は，監査部から送付されてきたCSAシートに従って，職場の状況を観察したり，部員にヒアリングしたりして評価を行った。評価結果を表3に示す。CSAシートの評価結果は次のルールに従って記入する。

・評価項目どおりに実施している場合：“OK”
・評価項目どおりには実施していないが，代替コントロールによって，“OK”の場合と同程度にリスクが低減されていると考える場合：“(OK)”（代替コントロールを具体的に評価根拠欄に記入する。）
・評価項目どおりには実施しておらず，かつ，代替コントロールによって評価項目に関するリスクが抑えられているわけではないと考える場合：“NG”
・評価項目に関するリスクがそもそも存在しない場合：“NA”

表 3　CSA シート（海外営業部の評価結果）（抜粋）

No.	評価項目	評価結果	評価根拠
4	新たな脅威について全員が教育を受けている。	a	
10	貸与 PC には会社が許可したソフトウェアだけがインストールされている。	OK	全部員に口頭で確認した。
11	リモート接続のためのパスワードを 90 日ごとに変更している。	b	
19	ファイルサーバ上の顧客情報のアクセス権は最小権限の原則に基づいて設定されている。	c	
25	業務用アプリケーションの利用者 ID の登録・変更・削除をルールどおり実施している。	OK	承認済みの利用者 ID 登録申請書を証跡として添付。
26	d	(OK)	少人数の専用オフィスであり，常に誰かが在席しているので，部外者が従業員に気付かれずに入ることは難しい。また，最終退出者はオフィスの出入口を施錠している。
29	業務用アプリケーションの利用者 ID 棚卸をルールどおり 3 か月に一度実施している。	OK	利用者 ID 棚卸記録を証跡として添付。

W 氏が，CSA 結果を監査部に提出したところ，監査部から電話があり，評価結果について質問を受けた。

最初の質問は，表 3 の No. 26 の評価根拠欄についてであった。W 氏は，記載内容が事実であることを説明したところ，それであれば監査部としての評価結果も“(OK)”にすると言われた。

次の質問は，No. 29 の証跡として提出した利用者 ID 棚卸記録に，棚卸の際に不要と判断された利用者 ID が 5 個あることについてであった。W 氏が部内で事実を確認すると，いずれも棚卸の 1 か月以上前から，部員の退職又は異動で不要になっていた。これについては W 氏も改善が必要であると考え，③改善計画を策定して監査部に提出したところ，適切であるとの連絡があった。

〔新たな指摘についての改善計画〕

CSA の評価結果及びその後の事実確認に基づき，監査部から新たな指摘を受けた。それは，“C システムにおいて，利用者は自分の担当外の顧客情報に対してもアクセスが可能であり，最小権限の原則が守られておらず，社外への顧客情報の漏えいを防止できるようになっていない”というものであった。そこで，部長と W 氏は改善計画について検討を行った。次は部長と W 氏の会話である。

部長 ：新たな指摘に対応するために，［ e1 ］が必要だね。

W 氏 ：はい，そのために全部員に担当顧客を確認しますので，2 週間ほど時間を下さい。

部長 ：分かった。その間のリスクを低減するために，［ e2 ］を実施しておくというのはどうだろう。

W 氏 ：はい，分かりました。他にも，万が一顧客情報の漏えいが発生してしまったときのことを考えると，［ e3 ］も有効だと思います。

部長 ：それも実施しよう。他に，前から気になっていたのだが，部員が顧客情報を不適切に変更しないように，顧客情報の追加・修正・削除の権限についても考える必要があるね。

W 氏 ：［ f1 ］はどうでしょう。

部長 ：それでは業務が回らなくなるのではないかな。［ f2 ］が，効率が良いのではないだろうか。

W 氏 ：そうですね。しかし，ベンダに開発をお願いするので，半年は掛かります。対策が有効になるまで，負担は増えますが，［ f3 ］を行うのはどうでしょうか。

部長 ：そうだな，ちょっと大変だが実施しよう。今までの話をまとめて監査部に報

告しておいてくれ。

W氏 ：分かりました。

W 氏が改善計画を監査部に提出したところ，監査部から，“内容に問題がないので，計画に基づいて改善を実施するように”と連絡がきた。

その後，W 氏が再検討した簡易チェックリストは部長に承認され，使われることになった。また，情報セキュリティ監査結果に基づく改善も計画どおりに完了し，海外営業部の情報セキュリティレベルは大きく改善された。

設問1 本文中の下線①について，部長が再検討を指示したチェック項目はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア 10　　イ 11　　ウ 12　　エ 13

設問2 本文中の下線②について，CSA 方式の利点を二つ，解答群の中から選べ。

解答群

ア 関連法規への準拠性が担保できる。

イ 業務内容の十分な理解に基づいて評価できる。

ウ 証跡を提出する必要がない。

エ 独立的な立場から公正に評価できる。

オ 評価実施者に対する意識付けや教育として役立つ。

設問3 〔CSA の実施〕について，(1)～(5)に答えよ。

(1) 表3中の［ a ］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

	評価結果	評価根拠
ア	OK	情報セキュリティ推進部の資料を使った教育が行われている。
イ	NG	新たなセキュリティ脅威に関する教育を受けていない部員がいる。
ウ	NG	教育後の試験を1回で合格できない部員がいた。
エ	NA	新たなセキュリティ脅威に対抗することはできないので教育は不要である。

(2) 表3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

	評価結果	評価根拠
ア	OK	会社のルールで決められている。
イ	NG	誰も1回も変更をしていない。
ウ	NG	リモート接続ができない。
エ	NA	部内ではリモート接続は誰も行わない。

(3) 表3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

	評価結果	評価根拠
ア	OK	簡易チェックで，アクセス権の付与状況について確認している。
イ	OK	簡易チェックで，アクセス権を適切に設定するルールが存在することを確認している。
ウ	NA	顧客情報をファイルサーバに保存することは禁止されている。
エ	NA	ファイルサーバは情報システム部が運用しているので，情報システム部が回答する。

(4) 表3中の［ 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。

dに関する解答群

ア　PCを社外に持ち出す場合はあらかじめ許可を得ている。

イ　入退室管理システムが導入され，関係者だけ入室可能になっている。

ウ　必要な場所に監視カメラを設置して毎日 24 時間撮影し，映像を記録している。記録した映像の保存期間を1か月以上にしている。

エ　部内で情報セキュリティ啓発活動をしている。

(5) 本文中の下線③について，策定する改善計画の概要を，解答群の中から選べ。

解答群

ア　C システムから出力された利用者 ID の一覧を使って，3 か月ごとに利用者 ID の棚卸を実施する。

イ　部員の退職又は異動の際は，利用者 ID の削除申請と C システムからの削除を速やかに行うよう，管理職一人一人に周知する。

ウ　利用者 ID 棚卸の実施者を上位の役職者に変更する。

エ　利用者 ID 登録時，申請されたアクセス権限が業務上必要か確認する。

設問4　〔新たな指摘についての改善計画〕について，(1)，(2)に答えよ。

(1)　本文中の［ e1 ］～［ e3 ］に入れる，次の[対策 1]～[対策 3]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。

[対策 1] アクセスログの保管期間を3年間に変更するという対策

[対策 2] 営業部員に対し，担当顧客以外の顧客情報を閲覧しないように周知し，牽制するという対策

[対策 3] 担当する顧客の顧客情報だけにアクセスできるようにアクセス権を設定するという対策

eに関する解答群

	e1	e2	e3
ア	[対策 1]	[対策 2]	[対策 3]
イ	[対策 1]	[対策 3]	[対策 2]
ウ	[対策 2]	[対策 1]	[対策 3]
エ	[対策 2]	[対策 3]	[対策 1]
オ	[対策 3]	[対策 1]	[対策 2]
カ	[対策 3]	[対策 2]	[対策 1]

(2) 本文中の［ f1 ］～［ f3 ］に入れる，次の [対策 4]～ [対策 6] の組合せはどれか。f に関する解答群のうち，最も適切なものを選べ。

[対策 4] 顧客情報の追加・修正・削除の権限は管理職だけに付与するという対策

[対策 5] 部員による顧客情報の追加・修正・削除は，システムのワークフロー機能を使って上長が承認することによって，データベースに反映されるようにするという対策

[対策 6] 顧客情報の追加・修正・削除のログを上長が定期的に確認するという対策

f に関する解答群

	f1	f2	f3
ア	[対策 4]	[対策 5]	[対策 6]
イ	[対策 4]	[対策 6]	[対策 5]
ウ	[対策 5]	[対策 4]	[対策 6]
エ	[対策 5]	[対策 6]	[対策 4]
オ	[対策 6]	[対策 4]	[対策 5]
カ	[対策 6]	[対策 5]	[対策 4]

〔 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。
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。