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]