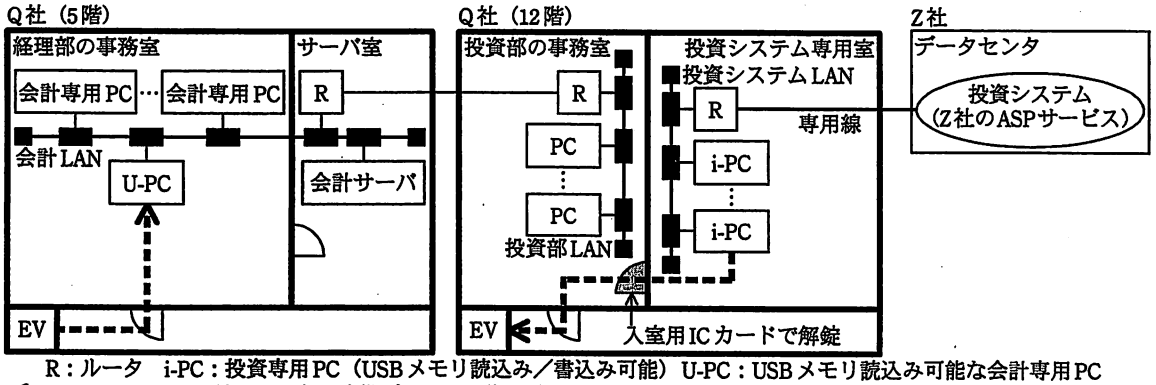
問4　財務報告に係る内部統制に関する次の記述を読んで，設問1～4に答えよ。

Q社は，従業員数500名の保険業を営む未上場会社であり，上場を目指している。2008年4月1日以後に開始する事業年度からは，財務報告の信頼性の確保を目的に，上場会社に対して内部統制報告書の作成が義務付けられた。そこで，Q社は，本年度から内部統制報告書を作成することにした。Q社は，内部統制報告書作成に際して，財務報告に係る内部統制のうち，特に情報システムに関する統制が有効であるかを評価するため，コンサルティング会社Y社にIT全般統制に関する状況の確認及び不備の指摘を依頼した。

Q社の資産運用を行う投資部には，投資部長の他に50名が所属しており，うち20名が投資システムを用いた業務を行う従業員（以下，投資担当者という）で，残りはその他の業務を行う従業員（以下，事務担当者という）である。投資部は12階にある。

現在利用中の投資システムは，証券会社を親会社にもつ情報システム会社のZ社がASPサービスとして提供しているものであり，Q社と専用線で接続されている。また，端末として投資専用PCが20台ある。多額の資金を運用することから，投資専用PCは，Q社の投資部LANとは分離されており，入室用ICカードでの入室管理が行われている投資システム専用室内に設置されている。入室及び投資専用PCの利用は，投資担当者20名及び投資部長1名だけに許可されている。

経理部は，投資部と同じビルの5階にあり，会計専用PCで会計サーバにアクセスして業務を行っている。投資部では，市場の取引終了後，財務報告のために，投資システムの特定のデータ（以下，会計連携データという）を抽出し，経理部にUSBメモリで運搬し会計サーバに入力している。経理部及び投資部関連の情報システムを，図1に示す。



R：ルータ　i-PC：投資専用PC（USBメモリ読込み／書込み可能）　U-PC：USBメモリ読込み可能な会計専用PC
<--- ：USBメモリを利用した会計連携データの運搬経路　　EV：エレベータ

図1　経理部及び投資部関連の情報システム

〔情報セキュリティガイドライン〕

投資部は，投資システム利用のための情報セキュリティガイドライン（以下，情報セキュリティガイドラインという）を作成し，情報セキュリティ上の事故が起こらないようにしている。情報セキュリティガイドラインを図2に示す。

（省略）
5. 投資システムの利用者IDの発行
(1) 新規の投資担当者は，申請書にアクセス権やその他の必要事項を記入し，投資部長の承認後，投資システム担当者に提出する。
(2) 投資システム担当者は，Z社に利用者IDの登録を依頼する（利用者IDの登録は，Z社だけが行う）。
(3) 投資システム担当者は，発行された利用者IDの情報をZ社から受け取り，申請した投資担当者に通知する。
6. 投資システムの利用者IDの削除
（省略）
7. 入室用ICカードの発行
（省略）
8. 入室用ICカードの返却
（省略）
9. 投資システムの利用者IDと入室用ICカードの発行対象
投資システムの利用者IDと入室用ICカードの発行対象は表1のとおりである。
（省略）
13. USBメモリの利用許可
投資部でのUSBメモリの利用は，次の三つの業務だけに認め，それ以外には許可しない。
(1) 分析のための投資システムのデータをダウンロードし，データを投資部の事務室のPCに移すこと
(2) 会計連携データを経理部の事務室に運搬し，会計サーバに入力すること
(3) 監査用データの提出を求められたときに，データ提出用に使用すること
14. USB管理簿
USBメモリの貸出しは，USB管理簿を使い，USB管理者が管理する。
なお，USB管理簿には，USB番号，利用者氏名，貸出日時，返却日時，目的，提出先名称の欄がある。USB管理簿の提出先名称の欄は，監査用データの提出時に利用する。
15. USBメモリの利用
(1) USBメモリの利用者は，利用前に，USB管理簿に必要項目を記入の上，USB管理者へ申請する。
(2) USB管理者は，USB管理簿の内容を確認の上，USB番号を記入し，USBメモリを貸し出す。
(3) USBメモリの利用者は，USBメモリ内のデータを消去してUSB管理者に返却する。
(4) USB管理者は，データ消去を確認し，USB管理簿に返却日時を記入の上，USBメモリを保管場所に格納する。
（省略）
21. 会計連携データの運搬
(1) 会計連携データの抽出担当者（以下，抽出担当者という）は，USBメモリの貸出しを受けて，i-PCから投資システムにアクセスし，その日の会計連携データを抽出し，USBメモリに保存する。
(2) 抽出担当者は，会計連携データ管理簿に当日の運搬を行う事務担当者の氏名と運搬依頼日時を記入し，USBメモリと会計連携データ管理簿を事務担当者に手渡す。
(3) 事務担当者は，USBメモリと会計連携データ管理簿を経理部まで運搬し，経理部の担当者に手渡す。
(4) 経理部の担当者は，経理部にあるU-PCを使用して，会計連携データを直ちに会計サーバに入力する。
(5) 経理部の担当者は，会計連携データ管理簿に自分の氏名と入力完了日時を記入し，事務担当者にUSBメモリとともに手渡す。
(6) 事務担当者は，USBメモリと会計連携データ管理簿を投資部まで運搬し，抽出担当者に返却する。
22. （以下，省略）

図2 情報セキュリティガイドライン

表1　投資システムの利用者 ID と入室用 IC カードの発行対象

役割名称	役割の説明	投資システムの利用者 ID	入室用 IC カード
投資部長	投資部のマネジメント。	あり	あり
投資担当者	投資システムでの株式売買を担当。	あり	あり
抽出担当者	会計連携データの抽出を担当。投資担当者の中の 1 名。会計連携データ管理簿を管理。	あり	あり
事務担当者	投資システムを用いない業務を担当。	なし	なし
USB 管理者	USB メモリの貸出し，返却のための USB 管理簿の管理を担当。事務担当者の中の 2 名。	なし	なし
投資システム担当者	Z 社との窓口を担当。投資担当者の中の 1 名。投資部の情報セキュリティ担当も兼務。抽出担当者とは異なるメンバ。	あり	あり

〔会計連携データの運搬〕

投資部では，情報セキュリティガイドラインに従い，USB 管理者から，投資部用に用意してある 5 個の USB メモリの一つの貸出しを受けて，市場の取引終了後の 16 時頃に，会計連携データの抽出を行い，終業前に経理部へ運搬する。

〔Y 社による IT 全般統制に関する状況の確認〕

Y 社は，Q 社の IT 全般統制に関する状況を確認する一環として，JIS Q 27002:2006 を参考に，情報セキュリティ対策の予備調査用の状況チェックリストを作成した。状況チェックリストの大項目を図 3 に，図 3 中の“7. [a]”に関する状況チェックリストを表 2 に示す。

1. 情報セキュリティポリシ	2. 情報セキュリティのための組織
3. 資産の管理	4. 人的資源のセキュリティ
5. 物理的及び環境的セキュリティ	6. 通信及び運用管理
7. [a]	8. 情報システムの取得，開発及び保守
9. 情報セキュリティインシデントの管理	10. 事業継続管理
11. 遵守	

図3　状況チェックリストの大項目

表2　状況チェックリスト（抜粋）

項番	チェック項目		
	名称	概要	詳細
7.2.1	利用者登録	（省略）	（省略）
7.2.2	特権管理	（省略）	（省略）
7.2.3	利用者パスワードの管理	（省略）	（省略）
7.2.4	利用者のアクセス権のレビュー	（省略）	（省略）
7.3.1	パスワードの利用	（省略）	（省略）
7.3.2	無人状態にある利用者装置	（省略）	（省略）
7.3.3	[b]・クリアスクリーンポリシ	書類及び取外し可能な電子記憶媒体に対する[b]ポリシ，並びに情報処理設備に対するクリアスクリーンポリシを適用しているか。	(1) 重要な業務情報は，必要のない場合，特に部屋が無人状態のときには，施錠して保管をしているか。 (2) サーバ及びPCは，離席時にはログオフ状態にしておくか，若しくはパスワード，[c]又は類似の利用者認証機構を使用した[d]で保護しているか。また，使用していないときには，施錠，パスワード，又は他の対策で保護しているか。 (3) 重要な業務情報を含む文書は印刷後，[e]いるか。

Y社のコンサルタントは，状況チェックリストを基にしたアンケートを使って，投資システム担当者に予備調査を行った。その上で，現場の状況の確認及び投資システム担当者へのヒアリングも行い，他の確認結果と併せて，IT全般統制の状況についての報告をまとめた。

〔IT全般統制に関する指摘〕

Y社から，投資システムのIT全般統制の状況に関して報告があった。その中で，情報セキュリティ対策について，次の3点の指摘があった。

指摘1：会計連携データを運搬中のUSBメモリ内のデータ保護対策がとられておらず，財務情報の正確性確保の観点からみて不十分である。

指摘2：投資システム利用中の離席時に，不正利用の防止のために行うべき手続が定められておらず，操作者特定の観点からみて不十分である。

指摘3：投資システムへのアクセス権の付与状況を管理するために必要な，アクセス権付与状況の一覧表が作成されておらず，アクセス権管理の観点からみて不十分である。

〔Z 社の統制状況〕

指摘 3 のアクセス権管理については，情報セキュリティガイドラインに項目を追加し，アクセス権の付与状況を一覧表で管理できるようにした。ただし，投資システムのアクセス権管理については，Z 社の統制状況についても確認の必要な項目が存在する。しかし，Z 社は，データセンタへの取引先の立入りを認めていない。そこで，Q 社は，Z 社に対して，①Q 社としての確認が必要な項目を含む，Z 社の統制状況に関する報告書を［ f ］の立場の専門家に作成してもらい，提出するよう依頼した。

その後，Z 社から報告書が提出され，Q 社は，Y 社のコンサルタントからの指摘に対応して，無事に上場の準備を整えることができた。

設問 1　本文中及び図 3 中の［ a ］に入れる適切な字句を答えよ。

設問 2　表 2 中の［ b ］～［ e ］に入れる適切な字句を，［ b ］，［ c ］については 10 字以内で，［ d ］については 15 字以内で，［ e ］については 20 字以内で答えよ。

設問 3　〔IT 全般統制に関する指摘〕について，(1)～(3) に答えよ。

(1) 指摘 1 は，どのようなリスクに対する対策の不備を指摘しているか。解答群の中から一つ選び，記号で答えよ。

解答群

ア　DDoS　　イ　ウイルス感染　　ウ　改ざん

エ　盗難　　オ　漏えい

(2) 指摘 1 について，どのような技術的対策が効果的か。30 字以内で述べよ。

(3) 指摘 1 について，悪意をもった事務担当者による不正行為を防止できない。このためにどのような管理的対策が効果的か。情報セキュリティガイドラインの改定を前提として 30 字以内で述べよ。

設問 4　〔Z 社の統制状況〕について，(1)，(2) に答えよ。

(1) 本文中の［ f ］に入れる適切な字句を 10 字以内で答えよ。

(2) 本文中の下線①について，図 2 中の 5. (2) に関して確認が必要な，具体的な項目を一つ挙げ，30 字以内で述べよ。