AU

平成28年度　春期
システム監査技術者試験
午後Ⅰ　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	2問選択

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) B又はHBの黒鉛筆又はシャープペンシルを使用してください。
   (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**を記入してください。正しく記入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してください。
   (3) **選択した問題**については，次の例に従って，**選択欄**の**問題番号**を**○印**で囲んでください。○印がない場合は，採点されません。3問とも○印で囲んだ場合は，はじめの2問について採点します。
   (4) 解答は，問題番号ごとに指定された枠内に記入してください。
   (5) 解答は，丁寧な字ではっきりと書いてください。読みにくい場合は，減点の対象になります。

〔問1，問3を選択した場合の例〕

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。

問1　情報セキュリティインシデント対応状況の監査に関する次の記述を読んで，設問1～4に答えよ。

B社は，中規模のインターネットサービス企業であり，買収した国内の子会社2社を含めて，B社グループとして事業を展開している。

〔B社グループの情報セキュリティインシデント対応体制〕

B社グループは昨年4月，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）への対応体制強化のために，B社CSIRT（Computer Security Incident Response Team）を設置した。B社グループにおけるB社CSIRTの位置付け，及び国内外の外部CSIRTなどの外部関連組織・外部Webサイトとの関係を，図1に示す。

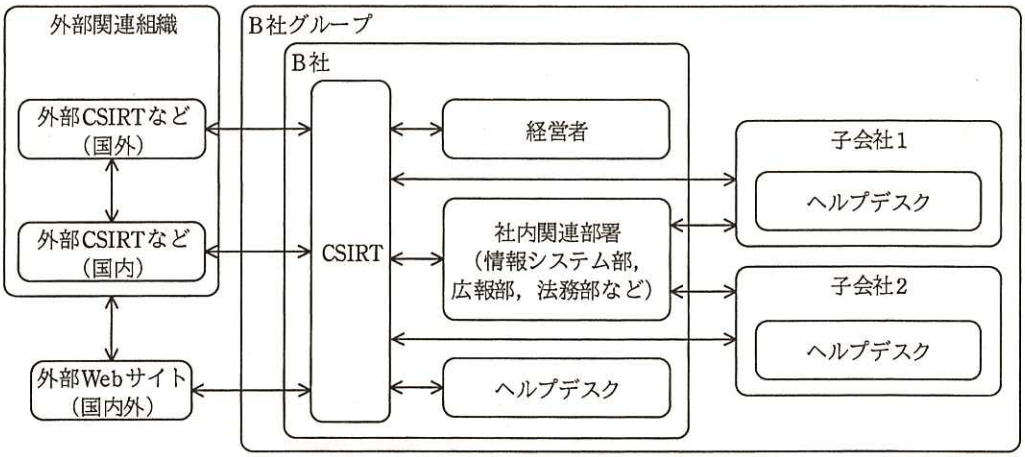

図1　B社CSIRTの位置付け及び外部関連組織・外部Webサイトとの関係

B社CSIRTは，B社の役員及び従業員で構成され，メンバは，最高責任者であるCIO，情報セキュリティに精通した専任社員（以下，専任社員という）2名，情報システム部との兼任社員（以下，情シ兼任社員という）2名，及びインシデント対応関連部署（広報部，法務部など）との兼任社員5名である。これらの兼任社員7名は，各子会社の対応する同部署との連絡窓口にもなっている。

B社CSIRTの対応範囲は，基本的にB社グループ内であるが，必要に応じて外部関連組織と連携して対応する場合がある。

〔インシデント対応状況の監査〕

年度監査計画に基づき，B 社内部監査部のシステム監査人 2 名が，設置後 1 年を経た B 社 CSIRT におけるインシデント対応状況の監査を行った。

監査の結果，判明した事項は，次のとおりである。

(1) B 社グループが共通で利用している電子メールシステム及びイントラネットを除き，B 社グループ各社の情報基盤は，IDS などの検知システムを含め，それぞれの情報システム部門が独自に管理している。検知システムは，B 社 CSIRT 設置以前に，B 社グループ各社が導入していたものである。

(2) B 社 CSIRT の最も重要な役割は，情報セキュリティイベント（以下，イベントという）の認知・連絡受付から通知・報告などに至る一連の活動（以下，インシデントハンドリングという）である。その内容を，表 1 に示す。

表 1 B 社 CSIRT が行うインシデントハンドリングの内容（抜粋）

項番	項目	内容
1	イベント認知・連絡受付	(1) 検知システムによって検知され，インシデントと自動判定されたイベントの認知 (2) B 社グループ内のヘルプデスク経由の連絡又は DNS などのディレクトリサービスを利用した外部連絡によるイベントの受付
2	トリアージ	(1) 認知又は連絡受付済みのイベントについて，B 社 CSIRT が対応すべきかどうかの判断及び必要に応じて行う連絡元への回答 (2) B 社 CSIRT が対応すべきイベントについて，インシデント判定マニュアルに基づく，インシデントかどうかの最終判定及び対応の優先順位付け
3	インシデントレスポンス	(1) B 社グループ内で発生したインシデントについて，当該会社のシステム管理者などとの連携及び被害の極小化・拡大防止を図るための対応 (2) 当該インシデントの影響が外部 Web サイトに及ぶおそれがある場合の，外部関連組織との情報交換及び必要な対応
4	B 社グループ内への通知・監督官庁への報告など	(1) B 社グループ内での被害の極小化・拡大防止を図るための注意喚起 (2) 必要に応じて行う監督官庁への報告，メディアや一般向けの公表など，外部への対応

(3) B 社 CSIRT は，イベントを“B 社グループの情報セキュリティに影響を及ぼし，重大な情報セキュリティ事故につながるおそれがある事象”と定義している。さらに，イベントの中でも“重大な情報セキュリティ事故に至り，B 社グループに多大な被害を与える事象”をインシデントと定義し，インシデントレスポンスの対象としている。

(4) B 社グループ各社の検知システムで検知されたイベントは，インシデントかどうか自動判定が行われ，インシデントと判定された場合には，B 社 CSIRT にも自動的に通知される。

このときに使用される，イベントの検知基準及びインシデントの自動判定基準は，検知システム上で設定されており，これらは，B 社 CSIRT 設置時に一度見直しが行われている。しかし，それ以降は検知システム上の設定が見直されておらず，検知システムで問題が発生するおそれがある。

(5) 専任社員及び情シ兼任社員は，B 社 CSIRT に常駐している。情シ兼任社員は，インシデントハンドリングにおいて，トリアージを含め，専任社員の職務を担当することもある。トリアージで使用するインシデント判定マニュアルには，判定のための確認事項及び確認方法が記述されている。このマニュアルは，トリアージについて高いスキルをもつ技術者向けに策定されているので，全ての確認事項について，詳細な確認方法が記述されているわけではない。

また，情シ兼任社員 2 名は，専任社員と同等のスキルをもっておらず，トリアージを常に正確に行うのは困難と判断される。このため，確認事項によっては，トリアージが適切に行われないおそれがある。

(6) 最近，B 社 CSIRT が，子会社の一つでインシデントレスポンスを行ったとき，一部のネットワーク機器が生成するログレコードの形式が，当該機器のバージョンアップで変更されており，そのまま使用することができなかった。その影響で，被害範囲の特定及び対応策の検討に時間を要し，結果的にインシデントハンドリングの完了が遅れた。

現在の運用のままでは，インシデントが発生した場合，再度インシデントハンドリングに支障を来すおそれがある。

(7) B 社 CSIRT 設置の際に外部関連組織との連携体制を構築して以降，定期的な情報交換や外部関連組織リストの更新などを行っていない。外部関連組織との連携体制の維持・強化は，B 社 CSIRT 運用規程で定められているが，日々発生するイベントの認知・連絡受付やトリアージに追われ，後回しになっている。

その結果，B 社グループ内又は外部でインシデントが発生した場合，外部関連組織との連携が迅速かつ有効に行われないおそれがある。

設問1　〔インシデント対応状況の監査〕の(4)について，システム監査人は，どのような問題が発生するおそれがあると考えたか。問題を一つ挙げ，35 字以内で述べよ。

設問2　〔インシデント対応状況の監査〕の(5)について，システム監査人は，どのような監査手続を実施した結果，“情シ兼任社員 2 名は，専任社員と同等のスキルをもっておらず，トリアージを常に正確に行うのは困難”と判断したか，45 字以内で述べよ。

設問3　〔インシデント対応状況の監査〕の(6)について，システム監査人は，B 社 CSIRT が，B 社グループ各社と連携してどのような対策を実施すべきと考えたか，40 字以内で述べよ。

設問4　〔インシデント対応状況の監査〕の(7)について，システム監査人が想定した，“外部関連組織との連携が迅速かつ有効に行われない”ことによる影響を，次の(1)及び(2)の観点から，それぞれ 50 字以内で述べよ。

(1)　B 社グループ内に及ぼす影響

(2)　B 社グループ外に及ぼす影響

問２　システムの移行判定の監査に関する次の記述を読んで，設問1～4に答えよ。

D社は，クレジットカード会社であり，現在，同業E社との合併に伴うシステム統合プロジェクト（以下，本プロジェクトという）を推進している。

D社は，5年前にも同業F社との合併に伴うシステム統合を行っている。そのときには，移行判定が不十分なまま本番移行を実施した結果，大規模なシステム障害が発生した。こうした経験を踏まえて，D社内部監査部長は，システム監査チームに対して，本プロジェクトにおける移行判定の適切性を監査するよう指示した。

〔本プロジェクトの概要〕

システム監査チームが予備調査で把握した本プロジェクトの概要は，次のとおりである。

(1) システム統合委員会は，本プロジェクトの重要事項を決定する会議体であり，D社及びE社（以下，両社という）役員，両社システム部門長，両社利用統括部門長などで構成される。

(2) システム統合は，E社のシステムをD社のシステムに片寄せして行う。

(3) システム統合スケジュールの概要は，図1のとおりである。

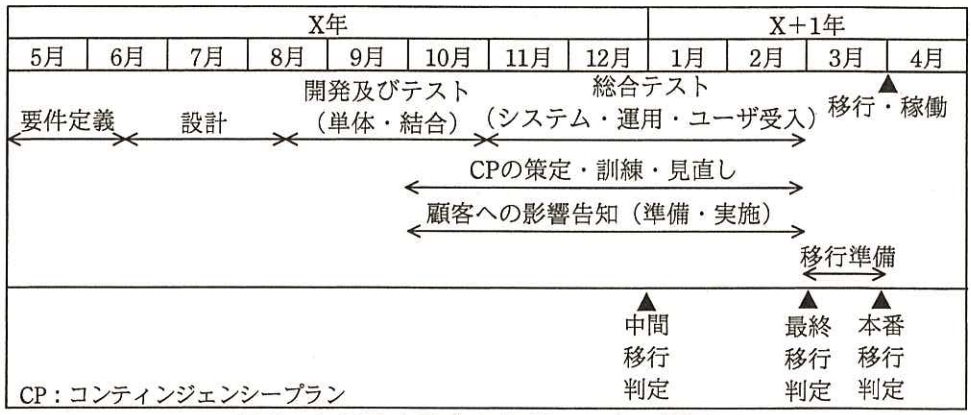

図1　システム統合スケジュールの概要

(4) 各移行判定の概要は，次のとおりである。

① 移行判定は3段階に分け，中間移行判定は12月末，最終移行判定は翌年2月末，本番移行判定は3月末に実施する。

② 各移行判定では，判定項目，判定条件，及び必要とする判定根拠資料で構成される各移行判定基準が策定され，各移行判定の 10 日前までにシステム統合委員会が承認する。

③ 各移行判定基準のほか，判定項目ごとに判定条件を満たしているかどうか，判定根拠資料に基づいて確認するために，各移行判定手続が策定される。

④ 各移行判定結果は，システム統合委員会が承認する。

なお，各判定根拠資料について，本プロジェクトの管理基準では，“本プロジェクトの各プロセスについて，部門長などの責任者が承認した証跡を，各判定根拠資料に記録する”と定めている。

(5) 統合後のシステムは，両社の合併当日（4 月 1 日）から稼働させる。

(6) 両社システム部門担当者は，システム統合に伴う顧客への影響告知の必要性を検討し，その結果に基づき，顧客影響一覧を作成した。表 1 にその一部を示す。表 1 に関する両社システム部門担当者の判断は，次のとおりである。

① 表 1 の項番 1，2 については，両社利用部門担当者に対して，顧客への影響に関する告知計画書の作成を依頼する。

② 表 1 の項番 3 については，顧客への影響が極めて限られているので，顧客への影響告知は不要である。

表 1 顧客影響一覧（一部）

項番	顧客への影響	顧客への影響告知
1	E 社のクレジットカード利用代金の口座振替日は，毎月 5 日から毎月 10 日に変更される。	必要
2	E 社のクレジットカード利用明細は，システム統合の 2 か月後まで参照できない。	必要
3	本番移行日深夜の約 2 時間，両社発行のクレジットカードは利用できない。	不要

〔中間移行判定後の監査〕

システム監査チームは，中間移行判定結果の適切性を確認するために，中間移行判定後の 1 月上旬に，表 2 の中間移行判定基準，判定結果などを閲覧し，関係者にインタビューを行った。

表2　中間移行判定基準と判定結果（抜粋）

中間移行判定基準				判定結果
項番	判定項目	判定条件	判定根拠資料	
1	顧客への影響告知についての準備状況	システム統合に伴う顧客への影響についての検討結果に基づき，告知計画書を作成している。	顧客影響一覧 告知計画書	可
2	システムテスト（以下，STという）の状況	ST が計画どおり実施されていることを，両社システム部門長が承認している。	ST 計画書 ST 中間報告書	条件付で可
3	ユーザ受入テスト（以下，UATという）の状況	UAT が計画どおり実施されていることを，両社利用統括部門長が承認している。	UAT 計画書 UAT 中間報告書	条件付で可

監査結果は，次のとおりである。

(1)　両社利用部門担当者にインタビューしたところ，表1の項番3について，顧客への影響告知を行うべきであると考えていることが分かった。続いて，追加の監査手続を行った結果，顧客影響一覧が適切に作成されていないことが判明した。

(2)　ST で検出された不具合の一部（以下，ST 不具合という）が，未対応であった。その結果，システム統合委員会は，表2の項番2の判定として，“ST 不具合への対応を完了し，両社システム部門長が1月末までに承認することを条件として可とすること”を承認していた。

(3)　UAT 中間報告書には，“テストケースの実施率が12月末時点の目標に対して，約50%にとどまっている”と記載されている。すなわち，最終移行判定までに全てのテストケースを実施することは困難な状況であった。その結果，システム統合委員会は，表2の項番3の判定として，“テストの項目・方法・スケジュールなどの計画を見直し，両社利用統括部門長が1月末までに承認することを条件として可とすること”を承認していた。

〔最終移行判定前の監査〕

システム監査チームは，各移行判定の概要，中間移行判定結果などを踏まえて，監査目的を次のように設定し，2月上旬に監査を実施した。

(1)　最終移行判定基準案の判定項目，判定条件，及び必要とする判定根拠資料は，整合がとれているか確認する。

(2) 中間移行判定でも使用された判定根拠資料の内容が，［　a　］

(3) 最終移行判定基準案が適切に策定されていることを確認するだけでなく，［　b　］

監査において，システム監査チームが閲覧した最終移行判定基準案は，表 3 のとおりである。

表 3　最終移行判定基準案（抜粋）

項番	判定項目	判定条件	判定根拠資料
1	UAT の完了	UAT が計画どおり完了したことを，両社利用統括部門長が承認している。	UAT 計画書 UAT 結果報告書
2	CP の実効性の確保	訓練を行い，CP の実効性を確保している。	CP 訓練結果報告書

監査における主な指摘事項は，次のとおりである。

(1) 〔中間移行判定後の監査〕の監査結果(3)への対応結果について，両社利用統括部門長が承認したことは，システム統合委員会議事録には記録されているが，UAT 計画書には記録されていない。表 3 の項番 1 の判定手続においては，適切な UAT 計画書を用いる必要がある。

(2) 表 3 の項番 2 については，訓練が行われたことを確認する判定手続だけでは，判定条件を十分に満たしていない。追加の判定手続が必要である。

設問 1　〔中間移行判定後の監査〕の監査結果(1)について，システム監査チームが追加の監査手続において確認したと考えられる事項を，50 字以内で述べよ。

設問 2　〔中間移行判定後の監査〕の監査結果(2)について，システム監査チームが閲覧したと考えられる監査資料を二つ挙げ，それぞれ 15 字以内で答えよ。

設問 3　〔最終移行判定前の監査〕の監査目的(2)，(3)中の［　a　］，［　b　］に入れる適切な字句を，それぞれ 35 字以内で述べよ。

設問 4　〔最終移行判定前の監査〕の指摘事項(2)について，システム監査チームが必要と考えた追加の判定手続を，判定根拠資料と確認事項を含めて 50 字以内で述べよ。

問3　プロジェクト管理の監査に関する次の記述を読んで，設問1～5に答えよ。

A法人は，ある地方公共団体の外郭団体である。A法人では，現行の基幹システムの老朽化と保守サポートの期限切れに伴い，新たに基幹システムを開発することになった。現在，要件定義工程が終了したところである。

A法人のシステム部門は要員が少なく，開発規模が大きいことから，基幹システム再構築プロジェクト（以下，Sプロジェクトという）では，開発及びプロジェクト管理支援業務を外部に委託することにした。

監査部のシステム監査チーム（以下，監査チームという）は，今年度の監査計画に従い，Sプロジェクトの管理業務及び体制の妥当性の確認を目的とするシステム監査を実施した。

〔プロジェクトの体制〕

基本設計工程以降のSプロジェクトの体制は，図1のとおりである。

(1) ステアリングコミッティは，Sプロジェクトの重要な意思決定を行う組織であり，システム担当役員，情報システム部長及び各利用部門の担当役員で構成されている。

(2) プロジェクトマネージャ（PM）には，情報システム部のT課長が任命されている。

(3) 開発委託先は，サブシステムごとに分割し，W社，X社，Y社及びZ社に発注されている。

(4) PMOの業務は，P社に委託されている。

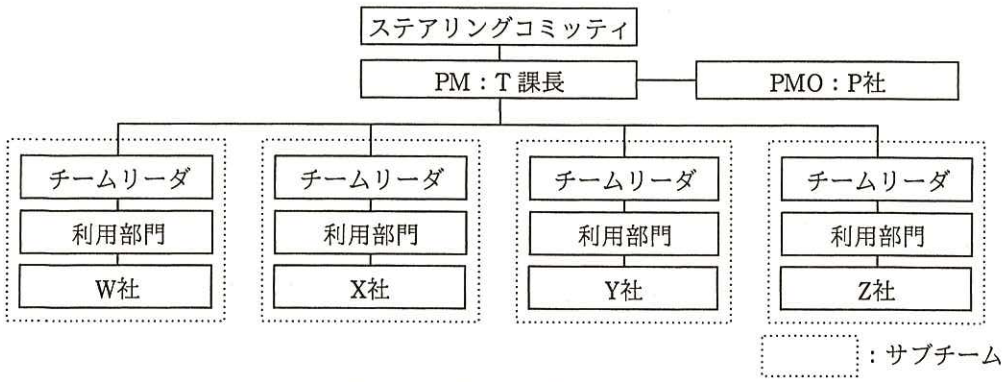

図1　Sプロジェクトの体制

〔プロジェクト管理基準の概要〕

A法人は，システム開発の経験が少ないことから，独自のプロジェクト管理基準を保有していない。そこで，P社のプロジェクト管理基準をベースにし，A法人の要望を取り入れた，Sプロジェクト用のプロジェクト管理基準（以下，管理基準という）を作成し，使用することにした。管理基準は，表1のとおりである。

表1　管理基準（抜粋）

項番	管理項目	管理内容
1	プロジェクトの体制と役割	・PMがプロジェクト管理業務を円滑に実施できる体制とすること
2	ステアリングコミッティの役割	・マイルストーン，開発スケジュール，スコープ，予算などの重要事項は，ステアリングコミッティが承認すること
3	PMOの役割	・PMOは，各サブチームから定型フォーマットで進捗報告書を収集すること ・PMOは，プロジェクトに関わる進捗報告及び課題を整理し，PMに報告すること
4	成果物の管理	・各工程の成果物のうち，あらかじめ指定されているものは，PM及び利用部門の責任者が承認すること ・各工程の成果物は，次工程に漏れなく引き継ぐこと

〔システム監査の計画〕

システム監査計画の中で策定した監査要点及び監査手続の概要は，表2のとおりである。

表2　監査要点及び監査手続の概要

項番	監査要点	監査手続
1	プロジェクトの体制が管理基準に従っていること，及びT課長がPMとしての役割を果たしていること	①　体制図を閲覧し，関係者にインタビューして，プロジェクトの体制が管理基準に従っているか確認する。 ②　進捗会議の議事録を閲覧し，T課長の出席状況を確認する。 ③　T課長にインタビューし，Sプロジェクトの円滑な管理に問題がないか確認する。
2	ステアリングコミッティが，管理基準に記載されている役割を果たしていること	①　T課長にインタビューし，ステアリングコミッティが役割を果たしているか確認する。
3	PMOが，管理基準に従って課題管理及び進捗管理を行っていること	①　進捗会議の議事録の閲覧及びP社へのインタビューで，PMOが，管理基準どおり役割を果たしているか確認する。
4	成果物が，管理基準に従って次工程に引き継がれていること	①　P社を含む各委託先にインタビューし，要件定義工程の成果物が委託先に引き継がれ，要件の説明を受けているか確認する。

〔システム監査の結果〕

システム監査計画に基づいて実施した監査の結果は，次のとおりである。

(1) 表 2 の項番 1 の監査要点について，T 課長は現行システムの運用の責任者を兼務していることを，体制図の閲覧及び関係者へのインタビューによって確認した。P 社との間では週次で進捗会議が実施されており，T 課長は，毎回進捗会議に参加している。T 課長はインタビューで“兼務していても特に支障はない”と答えている。監査チームは，これらの監査手続を実施した結果，T 課長が管理業務を円滑に実施できていると判断した。

(2) 表 2 の項番 2 の監査要点について，T 課長にインタビューした。T 課長は，“要件定義工程終了後，スケジュールの変更が発生したので，ステアリングコミッティの開催を要請し，対面で報告しようとした。しかし，出席者の都合がつかず，書面によって審議することになり，承認されるまでに約 2 週間を要した”と説明した。

(3) 表 2 の項番 3 の監査要点について，監査チームは，管理基準，及び進捗会議の議事録を閲覧し，PMO が管理基準に記載されている役割を果たしているか確認した。次に，P 社にインタビューし，P 社がプロジェクトの推進に苦慮していることを把握した。

(4) 表 2 の項番 4 の監査要点について，P 社にインタビューした。その結果，要件定義書の次工程への引継ぎに問題があり，基本設計に遅れが発生していることが分かった。このときの P 社の説明は，次のとおりである。

① 要件定義工程では，現行システムの保守を担当している G 社が業務分析を行った。

② G 社は，現行システムの機能を基に要件を洗い出し，要件定義書を作成した。

③ 情報システム部長と T 課長が要件定義書をレビューし，承認した。

④ 要件定義書に関しては，基本設計の開始前に G 社から各委託先に説明があったが，G 社は基本設計の開始後，現行システムの保守に追われ，余分の期間と要員を確保できなかった。その影響で，各委託先の疑問に対して，G 社からは回答が速やかに得られないことが多かった。

〔システム監査の報告〕

監査チームは，監査結果を基に，監査報告書を作成した。その内容は，次のとおりである。

(1) 〔システム監査の結果〕(2)について，ステアリングコミッティが十分に役割を果たしているとはいえないので，このままの体制で開発を進めた場合はリスクが大きい。

(2) 〔システム監査の結果〕(3)について，S プロジェクトの管理業務は P 社への依存度が高い。開発工程が進むに従って，進捗会議での報告内容は変化し，解決すべき課題も蓄積されていくと考えられる。それに伴い，発注者側の責任者である T 課長は，進捗報告の粒度，タイミングなどの管理業務の内容を改善していく必要がある。監査チームとしては，進行中の S プロジェクトの管理状況の適切性を確認するために，今後も随時フォローアップする。

(3) 〔システム監査の結果〕(4)について，要件定義を担当した委託先とは異なる委託先に開発を委託する場合には，基本設計工程の計画段階で考慮しておくべきことがある。今回は，スケジュールへの影響に対する考慮が不十分であったと考えられる。

設問 1 〔システム監査の結果〕(1)について，T 課長が S プロジェクトを円滑に管理できているか判断するために必要な，表 2 の項番 1 の①～③以外の監査手続を，40 字以内で述べよ。

設問 2 〔システム監査の結果〕(3)について，図 1 の体制に起因して監査チームが把握したと思われる課題を，30 字以内で述べよ。

設問 3 〔システム監査の報告〕(1)について，監査チームが考えたリスクを，45 字以内で述べよ。

設問 4 〔システム監査の報告〕(2)について，監査チームがフォローアップとして確認すべき内容を，45 字以内で述べよ。

設問 5 〔システム監査の報告〕(3)について，監査チームが基本設計工程の計画について確認したと考えられる内容を，50 字以内で述べよ。

〔 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。
13. 午後Ⅱの試験開始は **14:30** ですので，**14:10** までに着席してください。

午