2010 春 システム監査技術者 全国統一公開模試 講評と採点基準

2010 年 3 月 20 日 (株)アイテック 商品開発本部

■ 全体講評

4 問中 2 問選択になります。選択する問題による難易度のレベルに違いがあり，問 4 は比較的難しい問題で低得点者が多く出ています。試験では問題を読んですばやく難易度を推定し問題を選択する適切な判断が望まれます。

出題テーマとして，問 1 は保険業の営業管理システムの開発計画の監査について，問 2 は運用・保守業務の監査について，問 3 はサービス業における顧客情報システムの監査，問 4 は組込みソフトウェアの問題です。いずれもオーソドックスなテーマについての監査問題と思います。

最近の話題に沿ったタイムリーなテーマが揃っています。業務での実務経験だけでなく，幅広く学習している成果が試される出題です。

いずれも長文の問題を読んで理解しなければならないので，時間が不足気味です。問題を読んでいるうちに時間がなくなり，解答を満足に書くことができなかったという解答者もいたようです。受験テクニックを磨いてください。

短時間で解答が簡単な問題を選ぶ注意点として，設問をよく読んで「何を要求されているか」をすばやく理解することが重要です。いきなり頭から問題文を読むのではなく，まず設問から読むことが大切です。設問を読みながらポイントとなるところにアンダーラインを引いて，設問内容を意識しながら改めて問題文を読むことが重要です。

記述式の問題の場合，キーワードを明確に記述することが得点につながります。

問1 保険業の営業管理システム開発計画の監査

【採点基準】

[設問1]

(1)解答例のように「A 社の経営方針・経営戦略に合致した情報システムであること」が指摘されていれば 8 点。その他は基本的に 0 点です。

(2)番号としては，6 が書かれていれば 2 点。理由として，「社内にある既存のシステムとのデータ連携を考えなくともよい」点が指摘されていれば 7 点。その他は基本的に 0 店です。

[設問2]

不適切な活動として，解答例「営業管理に関するシステム連絡会に契約代理店の代表が出席していない」ことの指摘があれば 7 点。その他は基本的に 0 点です。

発生する不具合は「代理店の要望が取り入れられず，使いづらいシステムになる」，「稼働後ユーザから不満が出る」などが指摘されていれば 7 点。その他は基本的に 0 点です。

[設問3]

契約代理店において，使い勝手についてのアンケート調査，又はヒアリング調査が指摘されていれば 5 点。その他は基本的に 0 点です。

[設問4]

(1)「契約範囲と契約金額の決定の内容によって評価が異なる」ことや，「評価項目についての目標値や評価尺度が不明確のこと」が指摘されていれば 7 点。その他は基本的に 0 点です。

(2)「無料の保守業務の内容を確認すること」，又は「保守に関する費用分担，発生費用の内容を確認する」等の解答が指摘されていれば 7 点。その他は基本的に 0 点です。

【講評】

システム開発の方法として，自社開発と外部調達などの方法を比較検討する手順についての設問です。開発にあたってA社では四つの方式を検討しています。開発計画の承認プロセスについての理解度を確認する問題です。

設問 1 では，(1)情報システム開発方針の一番目に検討する事項を挙げます。やはりトップに来るのは「経営方針・経営戦略を考えること」になります。そのような趣旨の解答を書きます。

(2)は，開発方式を評価する項目と基準について考える問題です。文中に，今回の営業管理システムは，「社内にある既存のシステムとのデータ連携は考えなくともよいこととし」とありますので，この点を指摘することが必要です。不適当と判断される開発方針は 6 番です。理由は上記のとおりです。

設問 2 では，開発方式の検討プロセスを見ていくと，営業管理に関するシステム連絡会に A 社の関係者はほぼ出席しているが「代理店の代表がほとんど出席してない」ことが分かります。この点が不適切であるとされます。

その結果として起きる可能性がある不具合は，「代理店の要望が取り入れられないため，ユーザが使いづらいシステムになる」ということです。

ここでは，「業務実態が反映されてない」，「業務処理に不都合が発生する」などの一般的な解答は 0 点にします。

設問 3 では，まだ実現していないシステムについて，ユーザの使いやすさを調査する方法を考えます。

契約代理店の担当者にシステム概要を示し，又は試用の機会を作り，使いやすさについて，アンケート調査をとります。ヒアリング調査，書面調査などもよしとします。使いやすさ以外の調査についての解答は 0 点です。

設問 4 では，(1)の設問では「評価結果が変わる」ということの意味を理解する必要があります。具体的には，自社システムとして提案するか外部サービスを利用するかという判断がなされることを示しています。別な観点から解答すると，目標値と評価尺度が不明確ということも考えられるので，これも正解になります。

セキュリティ要件やサービス項目等の契約内容を聞いているのではありません。

(2)外部専門サービスの利用について，評価する項目として，保守コストの評価に影響する契約内容を考えます。

情報システムの無料で行われる保守業務について，その内容，又は保守費用の分担の形態などを確認する必要があります。保守契約の費用に関した記述であれば，正解とします。ただし，［障害時の対応コスト］など個別の保守項目についての記述は設問の趣旨とは異なるので不正解にします。

問2 運用・保守業務の監査

【採点基準】

[設問1]

解答例の「登録結果リストとジョブ登録予定表を照合して，内容が一致しているか確認する」が指摘されていれば 10 点。その他は基本的に 0 点です。

[設問2]

(1)「ジョブ登録予定表や作業依頼書に記載のない作業を，Z 社の担当者が行っても発見できないリスク」又は「Z 社の担当者が作業ミスや改ざんを行っても発見できないリスク」が指摘されていれば 10 点。その他は基本的に 0 点です。

(2)「Z 社責任者が運用支援ツールのログにより依頼された作業だけが行われていることを確認する」が指摘されていれば 10 点。その他は基本的に 0 点です。

[設問3]

「運用支援ツールのログを閲覧して，作業依頼書の報告内容と一致することを確認する」が指摘されていれば 10 点。その他は基本的に 0 点です。

[設問4]

解答例「障害の原因を究明して，再発防止の措置を講じること」が指摘されていれば 10 点。その他，細かい障害時の確認項目などは基本的に 0 点です。

【講評】

本問は，卸売業の基幹システムについて，その運用・保守業務に関する問題です。

設問 2 はリスクを挙げることが要求されています。リスクは，損失の発生する可能性をいうので解答にはそれに適した表現をするように留意してください。

設問 1 では，登録結果がジョブ登録予定表のとおり行われているかどうかを確認します。登録結果リストと予定表の内容が一致しているかを確認すればよいことになります。

この設問はほとんどの人が正解を書いています。ここで「ジョブ実行結果の確認」だけの解答では表現不足です。

設問 2 では，(1)リスクとして，Z 社の担当者がジョブ登録予定表や作業依頼書に記載のない作業を行っても発見できないこと，作業ミスや改ざんを起こしても発見できないリスクを書きます。

(2)コントロールとして，Z 社責任者が運用支援ツールのログによって作業内容を確認することが解答です。誰が（Z 社責任者が），何を用いて（運用支援ツールのログによって）確認するかを明確にしてください。

設問 3 では，監査手順として，運用支援ツールのログを閲覧して，作業依頼書の報告内容と一致することを確認することを指摘します。

ここでは作業依頼書の内容と一致することをどうやって確認するかが記述されます。「ログの確認」ということがポイントになるでしょう。全数チェックは必要ありません。

設問 4 では，システム管理基準の運用管理項目は細かく覚えていないと思われますが，障害発生という場面を想定すれば，解答は限られています。すぐに思い浮かぶ解答として，「障害の原因究明」と「再発防止策」の二つが書かれていればよいでしょう。障害発生

時の細かい確認事項は，ここで記述することはないと思います。

問3　サービス業における顧客情報システムの監査

【採点基準】

[設問1]

解答例「ユーザ ID の管理が不適切であり，退職者のユーザ ID を削除してない」，又は「ユーザ ID 管理規定がない，管理ができていない」が指摘されていれば 8 点。対策として「ユーザ ID の管理体制を確立し，頻繁に保守を行い最新の状態に保つ」ことが指摘されていれば 8 点。その他の解答は 0 点です。

[設問2]

二つのリスクとして，解答例の「顧客情報の不正コピーが行われ外部へ流出する危険性」及び「USB メモリの外部持出しにおける紛失・盗難のおそれ」を指摘してあればそれぞれ 7 点。その他は基本的に 0 点です。

[設問3]

名称として，文書管理規定，又は機密文書取扱いに関する管理規定などが書かれていれば，5 点。

セキュリティリスクとして，「機密文書がセキュリティ保護の対象にならず，情報漏えいするおそれがある」又は「機密情報を誤って開示するおそれがある」などが指摘されていれば 7 点。その他は基本的に 0 点です。

[設問4]

解答例「事業継続計画を社内に周知徹底するための教育や広報活動」又は「事業継続計画にかかわる要員に対する教育や訓練活動」が指摘されていれば 8 点。ここでは「事業継続計画」がキーワードになるので，その解答以外は基本的に 0 点です。

【講評】

設問の主眼は，アクセス管理とユーザ ID，パスワードの管理体制です。管理簿を使ってその設定と変更などがきちんと管理されていることを監査します。

また，情報システムの事故発生など緊急事態が発生したときの業務分担と連絡体制を明確にする等の対策を策定したものとして，事業継続計画（BCP：ビジネス・コンティニュイティ・プラン）があります。対策が十分に社内へ浸透するよう文書化して社内に周知徹底する必要があります。

このような情報管理の問題は過去にも何度も出題されており，過去問を勉強している方にとっては解きなれた問題です。多くの方がこの問題を選択しており，かつ高得点をとっています。

設問 1 では，ユーザ ID/パスワードの管理に関して，解答例のように記述してください。アクセス権の設定のことではありませんので，十分に注意してください。

(1)このような事態が発生した原因として考えられることは解答例のようにユーザ ID/パスワードの不適切な管理であることになります。

(2)対策として ID 管理のことを書くとよいでしょう。頻繁に管理簿の保守点検を行い最新の状態に保つことが必要です。ここで，ID 管理と直接関係ない解答は 0 点です。例えば，社員情報を定期的にとるなどの解答がありました。不正解です。

設問 2 では，磁気媒体の外部持出しに関する管理体制についての不備を指摘します。

顧客情報を外付け磁気媒体へコピーすること，USB メモリを外部に持ち出すことの両方についてのリスクを指摘してください。解答例のように，事故につながる事態が想定されること，つまり「不正コピーのリスク」と「外部持出しにおける紛失・盗難のリスク」の二つが重要です。この 2 種類のリスクを書いてください。

なお，外へ持ち出した USB からウイルス感染することも考えられますが，ここでは情報漏えいのリスクがはるかに重要ですので，それ以外の解答は 0 点です。

設問 3 では，機密文書の取扱いに関する全社的な統一規定は何かという設問であり，「文書管理規定」又はもっと丁寧にいうと「機密文書取扱い管理規定」となります。

ここでセキュリティポリシを挙げるのは不適切です。セキュリティポリシは，機密文書だけではなく，より広い領域をカバーしているので，ここでは正解にしません。0 点です。

(2)この規定がないことで予想されるリスクは「機密文書の情報漏えい」です。このような解答のみ正解にしました。

設問 4 では，事業継続計画を社員に周知徹底させる教育訓練が解答になります。

事業継続計画を社内に周知徹底するための教育や広報活動，別解として事業継続計画にかかわる要員に対する教育や訓練活動としてもよいでしょう。事業継続計画又は BCP がキーワードになります。

問4　組込みソフトウェア開発の監査

【採点基準】

[設問1]

問題点として「プロジェクトの規模や重要性を考慮せず，監査対象を無作為に決めている」が指摘されていれば 6 点。

改善策として「規模の大きなプロジェクトや重要度の高い製品を重点的に監査対象とする」が指摘されていれば 7 点。その他は基本的に 0 点です。

[設問2]

項番として，3-2 が指摘されていれば 5 点。理由として「テスト終了後にテスト仕様書の承認が行われるのでは遅すぎる」が指摘されていれば 7 点。その他は基本的に 0 点です。

[設問3]

項番として，4-5 が指摘されていれば 5 点。理由として「各種異常ケースに対するシステム動作は機能要件であり，非機能要件ではない」が指摘されていれば 7 点。その他は基本的に 0 点です。

[設問4]

コントロール目標は「企画部門の製品企画書の開発目的を反映して要件定義書が作成していること」が指摘されていれば 6 点。監査方法は「要件定義書の要求項目が，製品企画書の内容を引用しているかを査読によって確認する」が指摘されていれば 7 点。その他は基本的に 0 点です。

【講評】

組込みシステムを題材にした問題は取り組みにくいと思われるためか，この問題を選んだ人は非常に少数でした。また，設問 2，設問 3 については，正解率が低かったといえます。組込みシステムといっても，システム開発やシステム監査の基本は同じですので，それほど専門的な知識を問う問題は出題されていません。組込みシステムを開発する製造業の背景を理解していれば，他業界の人でも取り組める問題となるはずです。この問題は，有効性監査を目的とした監査の内容を扱っています。

設問 1 は，プロジェクトの選択方法の問題点です。「規模や重要性を考慮せず，監査対象を無作為に決めている」ことが問題です。ここでは，各課のバランスをとることを指摘する必要はありません。各課を均等に選択していることは別に問題とはなりません。

改善策として「規模の大きなプロジェクトや重要度の高い製品を重点的に監査対象とする」が指摘されていればよいでしょう。

設問 2 では，コントロール目標を達成していないと判断される項目を挙げます。

項番として，正解である 3-2 を指摘した人は非常に少なく，不正解の解答 1-1，1-2 等の指摘も多い状況です。

3-2 を選ぶ理由として「テスト終了後に仕様書の承認が行われている」が指摘されます。明らかに，このプロセスの順番はおかしいので，正解になります。

1-1 を選ぶ理由は，「固有リスクに対するコントロールがない」ことですが，設問 2 の趣旨とはずれていることが分かります。

設問 3 では，コントロール目標の項目に対応していない項目を選びます。コントロール目標 4 は非機能要件を取り上げているので，機能要件が記載されていればそれを指摘します。正解として，項番 4-5 が指摘されていればよいでしょう。この設問も正解者が少ない状況です。

4-5 が指摘される理由として「各種異常ケースに対するシステム動作は機能要件であり，非機能要件ではない」が指摘されます。

設問 4 では，D 社の製品開発の問題点を解決するコントロール目標を考えます。D 社の製品開発の問題点とは，「製品企画部で企画した製品のコンセプトが，開発された製品に十分に盛り込まれていない」ことです。

これを解決するコントロール目標は「企画部門の製品企画書の開発目的を反映して要件定義書が作成していること」を指摘します。ここで必要なのは「コンセプトを盛り込んだ製品を開発する」ことではありません。コンセプトを盛り込んだ要求定義書を作成することがコントロール目標になります。

監査方法は「要件定義書の要求項目が，製品企画書の内容を引用しているかを査読によって確認する」を指摘します。

以上