2013 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

2013 年 3 月 26 日 (株)アイテック 情報技術教育研究部

■ 全体講評

午後Ⅰは 4 問中 2 問の選択になりますが，問題によって正答率に違いがあります。自分の専門にこだわらずに，解答しやすい問題を選んでください。例えば，問 3 は比較的やさしく正答率の高い問題でした。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。

それぞれ長文の問題を読んで，すぐに設問に答えなければならないので，時間が不足しがちです。短時間で解答が簡単な問題を選ぶのも，能力のひとつになります。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。そのためには，いきなり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問題文を読むことが重要です。

設問で何が問われているかを必ず確認し，ポイントとなる内容を分かりやすく記述することが必要です。今回の公開模試でも，設問で問われていること以外の内容を答えているものが多く見受けられました。これらの点は特に注意しましょう。

例えば問 3 の設問 2 では「発生する恐れがある問題点」を挙げよとあります。ここで現状の問題点を挙げるのは設問の意味を理解していない解答です。問 2 の設問 3「リスクを挙げよ」という設問に，改善提案を書くような解答では採点の対象になりません。

試験当日は，集中力，精神力，体力の勝負になるので，最後まであきらめず，必ず合格するという強い意識を持って臨むようにしましょう。

問1 SLA(サービスレベルアグリーメント)の監査

【採点基準】

［設問1］

(1)(2)それぞれ解答例どおりであれば各 8 点。(1)について，別解として「ユーザの意向を反映しないまま SLA が締結されてしまう」も正解です。

その他は，基本的に 0 点。

［設問2］

①②とも，分析内容と監査証拠が解答例どおりの表現であればそれぞれ 7 点と 2 点です。それ以外は，基本的に 0 点。①の監査証拠の別解として「操作性能調査レポート」の解答も認めます。

［設問3］

対策について①②とも解答例と同様の趣旨が適切に指摘されているものに対し各 8 点。その他は，基本的に 0 点。

【講評】

情報サービスなどアウトソーシングを利用する場合のサービス保証内容について合意を行うことが，SLA（サービスレベルアグリーメント）です。一般的な問合せ対応，トラブル発生時の対応，などについての保証内容，料金体系，運用時間などについて，きちんとした契約書の形にまとめる必要があります。

問題文の論点は，SLA の合意形成プロセスに関しての問題です。本問は，全体としてわかりやすい設問が多く，比較的正答率の高い問題でした。

設問 1(1)では，プロジェクトチームの合意形成の後段階で，発生する不具合を考えます。「SLA 項目の見直し・修正が必要になり手戻りになる」という解答が望まれます。「ユーザの意思を反映しないまま SLA が締結される」という解答も正解です。それ以外は不正解です。業務効率が低下する，用語の解釈が違うなど，「合意形成プロセスの不具合」以外はすべて不正解です。

(2) では，取締役会で確認すべき事項を考えます。「サービス品質と投資金額のバランスを考え，投資効率を判断する必要がある」という解答が望まれます。経営が成り立つためには，収益とのバランスが必要です。料金に関する記述があれば正解としました。業務効率が達成できないという解答は不正解です。

設問 2 では，分析の内容と必要な監査証拠を答えます。①では，性能テストの調査は遠方の営業所まで対象を広げて調査分析をする必要があります。全体にまで対象を広げたテストが記述されていなければ不正解になります。②では，「アクセスログを取りログ解析によって不正アクセスの有無を分析する」となります。不正アクセスの分析が対象ですので，「セキュリティ対策の分析」という解答では対象が広がり過ぎです。

それぞれの監査証拠となるレポート名は，①「システム稼働レポート」または「操作性能調査レポート」を挙げます。②の監査証拠は「アクセス解析レポート」がよいでしょう。ここでレポート名，文書名を書くように指摘されていますので，単に①レスポンスタイム，②アクセスログなどデータ名だけの解答は不正解です。

設問 3 は，ユーザ満足度を上げるための方策を書きます。クレーム①について，対応者によって同じ回答がで

きるようにするため，回答マニュアルの整備，FAQ，Q&A の整備が必要であることが分かります。データベースの作成も正解とします。

クレーム②については，たらい回しを避けるためには担当部署が明確になっている必要があるので，「担当部署を明記した業務分担マニュアルの整備が必要である」となります。教育徹底も必要です。「窓口の一本化」という解答は，設問の趣旨とずれているので不正解です。

問2 ERP パッケージ導入によるシステム統合計画の監査

【採点基準】

［設問1］

解答例どおりであればそれぞれ 6 点。その他は，基本的に 0 点。

［設問2］

目的と内容について，解答例どおりのみ各 6 点。

その他は 0 点。

［設問3］

リスク内容が正しけ書けて入れば各 6 点，その他は，基本的に 0 点。

［設問4］

定量的な指標が正しく書かれていれば 8 点。その他は，基本的に 0 点。

【講評】

ERP パッケージ導入によるシステム統合は，業務改善を巻き込んで全社的に行われることが多く，IT だけにとどまらない全社的な視点で考える必要があります。今回の設問は，基幹業務を中心に社内体制も含めた変更を考えることが問われています。

設問 1 は,「システムライフサイクルコストの最小化」という観点で考えます。費用として(1)工場ごとの違いを反映したカスタマイズ費用,(2)冗長化システムを構成した場合のライセンス費用,(3)パッケージのバージョンアップ時にかかる費用の三つを挙げればよいでしょう。ここは，ほとんどの方が迷うことなく正解を書いています。ただし，(1)で単に「アドオン費用」，(3)で単に「保守費用」とするのは，言葉足らずで不正解とします。
この設問は正答率が高かったです。

設問 2 では，あくまで工場の生産現場のことがテーマですので，それ以外の解答は不正解になります。たとえば「全体の最適化をする」,「総合戦略を実施するため」,「全利用者のニーズを聞く」などの解答は範囲を広げ過ぎです。もっと絞り込んで解答する必要があります。

設問 3 は，「リスクを挙げよ」という設問です。ここに改善提案を書くような解答では採点の対象になりません。同様に「～すべき」という表現もリスクではありません。また，「全社的に影響が大きい」，「全社の業務がストップしてしまう」という抽象的な解答も不正解です。設問をよく読んで、求められている内容に沿った表現をしましょう。

設問 4 は，定量的な効果の指標をあげます。「納期問合せ」というキーワードが書かれていれば正解にします。具体的な数字で表すことができるものを定量的と言います。定量的な指標でない解答も目立ちましたが，すべて不正解です。

問3 顧客情報システムの情報管理体制の監査

【採点基準】

［設問1］

意識向上の方策および結果の確認方法について，解答例と同様の場合各 7 点。その他は，基本的に 0 点。

［設問2］

発生する恐れのある問題点について，解答例どおりのみ各 6 点。その他は，基本的に 0 点。

［設問3］

不正アクセスの有無を調査する手続きについて，適切な解答の場合 10 点。その他は，基本的に 0 点。

［設問4］

問題点および対策について，解答例と同様の場合各 7 点。その他は，基本的に 0 点。

【講評】

個人情報保護管理の問題は，監査の問題としてよく出題されます。印刷業，運送業など個人情報に関する業務を委託される企業では，業務に使用する顧客情報を厳密に管理する必要があるので，その管理体制を監査することが必要です。毎年出題され続けているテーマでもあり，的外れの解答はほとんど見当たらず，満点が続出する問題でした。

設問1は，意識向上の方策として，マニュアル作成と社員に周知徹底させる教育訓練を指摘すればよいでしょう。

行動マニュアル作成，情報保護の教育のどちらか一方の記述は半分正解になります。「セキュリティ方針の説明会を開催する」という漠然とした解答では不正解です。

結果の確認方法としては「アンケートまたはヒアリング調査で，情報保護の理解度を確認する」となります。理解度テストでも可とします。ただし，教育の開催実績回数とか，実施状況の調査という解答では，効果測定になりません。不正解です。

設問 2 では，宛名ラベルの出力帳票受け渡しプロセス

における「発生の恐れのある問題点」を挙げます。宛名ラベルについて「担当者がチェック印を記入して引き取ること」また,「外部の人が頻繁に出入りしていること」からヒントを得ます。つまり「取り間違いにより紛失する恐れがある」や「外部の人間による盗難が発生する恐れがある」として解答します。

ここで現状の問題を挙げるのは設問の意味を理解してない解答です。入退室管理がないことや，受け渡しのチェックがないことなど「何々してない」というのは「発生する恐れがある問題点」の正解になりません。設問をよく読んで，適切な表現の解答を書くようにしましょう。

設問 3 は，不正アクセスの有無を調査・確認する手続きを問うものです。これについては管理簿を使ってアクセスの記録がきちんと管理されていることを監査する必要があります。解答としては，「アクセスログの取得と定期的分析がなされ，不正と思われるアクセスの有無を調査する」となります。ここでは，アクセスログがキーワードになります。単に「操作ログ，ログを確認する」では不十分な解答です。

設問 4 は，バックアップの保管について考えます。問題点は「火事等の災害で日次と月次のファイルが一緒に破損する恐れがある」ことです。対策は「月次ファイルは情報システム室から離れた別の場所に保管する」。となります。

日次・月次の 2 つのバックアップ媒体が保管棚に一緒に保管されている状況を指摘して欲しいところです。情報システムと同じ場所の保管を指摘するのは、それに比べて重要度が落ちます。正解にはなりません。

月次バックアップファイルの保管場所の選定において情報システムや日次バックアップファイルの保管場所と離れた別の場所に保管されなければならないという解答が望まれます。

問 4 システム開発と運用の外部委託の監査

【採点基準】

[設問1]

解答例どおりであれば 9 点。その他は基本的に 0 点。

[設問2]

解答例どおりであれば 9 点。その他は基本的に 0 点。

[設問3]

(1)(2)について，解答例どおりのみ各 8 点。
その他は 0 点。

[設問4]

IT によらないコントロール，IT によるコントロールのそれぞれについて，解答例どおりのみ各 8 点。
その他は 0 点。

【講評】

業務処理などの業務を外部委託する場合，委託先との契約において気を付けることが多々あります。情報の保護管理の問題，更に下請けへ再委託をする場合の問題などがあります。今回は，どのような委託契約を結ぶかについて問われています。

設問 1 は，機密保持に関して契約に追記する項目です。「何が機密情報かを定義し，機密区分に応じた取扱情報を別途規定してそれを順守させる」が正解です。この正解は特に悩むことは無くすぐに書けるので，ほぼ全員が正解です。機密情報の定義，機密保持の手順の策定のどちらか一方しか書かれていない場合は，半分の部分点となります。

設問 2 では，「委託先を原則禁止にして，委託作業の管理を C 社が責任を持って実施する」が正解です。「再委託の原則禁止」が書かれていればすべて正解にしました。それ以外の解答でも「委託先を C 社が責任を持って管理する」とあれば正解です。ただし，「再委託の場合は B 社の許可承認を得る」「再委託先の従業員を厳密に管理する」などの解答は，方向が違うので不正解です。

設問 3 は，(1)「管理区域への入室は 1 回の認証で一人しか入室できないようにする」が正解です。個人別の ID 発行などで，共連れ（ともづれ）を防止する方策が書かれていれば，正解です。ここでは，退室時の記録を取るという解答は重要性が落ちるので，不正解とします。

(2)例外処理については「例外処理でも捜査記録としてログ情報が残るようにする」ことが正解です。「直接アクセスする権限を許可しない・禁止する」などの解答はこの設問においては重要度が低いので不正解です。

設問 4 は，IT によらないコントロールとして「指定した重要作業を行う際には複数担当者によるクロスチェックを義務付ける」または「C 社から作業結果の報告を定期的に受け，B 社側でその内容を実態に照らして確認する」が挙げられます。ここでは，作業結果の報告がキーワードになるので，この用語があれば正解にします。また，「SLA の定期評価と報告」も正解にします。しかし，ペナルティを決めておく，委託先の監督を徹底するなどの指摘は，正解にはなりません。

IT によるコントロールとして，「業務実施のログを取得して，定期的な管理者の確認を義務付ける」と解答すればよいでしょう。アクセスログでも正解とします。ここで「リストア手順書が更新されていない」ことまでは不要ですので，不正解になります。

以上