2011 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

2011 年 3 月 18 日 (株)アイテック 商品開発本部

■ 全体講評

午後Ⅰの選択問題は 4 問中 2 問選択です。選択する問題によって難易度のレベルにかなり違いがあります。やさしい問題や経験のあるテーマの問題で高得点を出せるように，問題内容から素早く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，流通小売業のポイント管理システムの監査が出題されています。実店舗と Web ショップのポイント交換の問題です。やや難しい設問もあり満点は少なく，平均点もあまり高くありません。

問 2 は，旅行業におけるモバイル営業支援システムの監査についての問題です。モバイル端末に関するセキュリティが中心となって出題されています。約半分の人がこれを選択して満点も出ており，比較的答えやすい問題です。

問 3 は，損保業における内部統制のシステム監査です。主に IT 業務処理統制に関する設問が中心です。「内部統制」というタイトルから敬遠する人が多かったように感じました。また低得点が目立ちます。

問 4 は，製造業における情報システム開発手順の監査についての問題です。要求定義書の内容など開発管理に関しての設問が中心となります。選択する人は少なく，平均点数も低い問題です。

短時間で問題を選ぶ注意点として，まず設問を読んで「何を要求されているか」を素早く理解することが重要です。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くなどして，設問内容を意識しながら，改めて問題文を読むとよいでしょう。

また，解答方法にも気を付けてください。何が問われているかを必ず確認するほか，不要な修飾語はできるだけ削除し，ポイントになる内容を分かりやすく記述することです。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，肝心のことが記入できていないようなものも数多く見受けられました。例えば，問 1 設問 2 では，要望を書かなければならないのに問題点を書く人がいます。これでは 0 点になります。

記述式の場合，答えは分かるが，どう書いてよいか分からないという人がいます。そのためか採点者が理解できない記述がかなりあります。この場合，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。何がキーワードか問題文を読みながら，印をつけていくとよいでしょう。また模擬試験などの経験を積むことが必要になるでしょう。

問1 流通小売業のポイント管理システムの監査

【採点基準】

［設問1］

(1)，(2) は，解答例どおりを各 5 点。その他は，基本的に 0 点。

［設問2］

(1) 要望は，解答例どおり又は別解として，「販売システムでは日次処理で蓄積ポイントを更新しているが，販売結果をすぐに反映してほしい」であれば，8 点。

(2) 機能は，解答例どおりが 8 点。その他は，基本的に 0 点。

［設問3］ 解答例どおりを 8 点。

［設問4］ 解答例に沿った内容が二つあれば各 8 点。その他は基本的に 0 点。

【講評】

流通業，サービス業を中心に CRM システムの一環として，広く使われているポイント管理システムは，リアルタイムでポイント更新をするシステムが多くありますが，大企業以外ではまだ日次更新のシステムが多いのが現状です。そのようなシステムを取り上げて，更新のタイミング，特別割増ポイント加算，Web ショップの扱いなどにおける，データ整合性と正確性についてのシステム監査をしています。

設問 1 では店舗と本社の蓄積ポイントの処理結果が合わない原因とその調査方法について記述します。(1)合わない原因は「店舗キャンペーンの加算率データの登録漏れや登録エラーがある」こと，(2)その調査方法は「キャンペーン計画書の入力帳票とシステム登録された計画内容とを，突合（照合）して内容を確認する」ことです。問題文中の「電話などの依頼によって仮登録が行われる」ことに注目すると，容易に解答例が得られます。

(1)で単なる「仮登録したから」とか「キャンペーン加算率が間違っていた」だけでは 0 点です。なぜ違ったかその原因として「登録漏れ，入力エラー」の記述が必要です。これ以外の記述で「複数店舗で金額値引きをしたから」，「本社から更新結果が送信されてない」，「営業本部長の承認がない」という解答は的外れになるため 0 点になります。

(2)監査証拠にキャンペーン計画の書類と入力された計画を用い，監査手法として両方を突合し確認します。仮登録のポイント率と登録された計画と照合することも正解としました。ここで「本部長の承認を確認する」

は不適切です。

設問 2 は，Web ショップで想定される顧客の要望・不満を考えます。解答例のように「Web 以外の店舗で購入したポイントもリアルタイムですぐに反映させてほしい」ということでしょう。別解として，「販売システムでは日次処理で蓄積ポイントを更新しているが，販売結果をすぐに反映してほしい」という要望も考えられます。それを実現する機能は「各店舗の購入ポイントをリアルタイムで蓄積ポイントの更新ができる機能」です。

設問ではデータ共有化に関しての要望が問われています。解答の間違えとして多いのは「Web 店舗のキャンペーン加算率もほしい」とか「おすすめ情報の提供」，「関連購買品情報の提供」などです。これらは設問の趣旨と違っています。

設問 3 は，顧客データベースの不正なアクセスが発見できるようにする調査方法を聞いています。解答例にあるように「顧客 ID とパスワードの認証は既に Web サーバで行われ，データベースサーバへのアクセス時には不正もその兆候も発見できない」となります。

外部からアクセス可能な Web サーバと，アクセス不可能なデータベースサーバの区別ができていればすぐに分かる内容です。顧客データベースへのアクセスログ記録を顧客 ID と照合しても不正アクセスの有無は確認できません。

「ID やパスワードを盗まれてなりすましが起きる」ということや「企画部員の内部犯行を防げない」ではありません。これらの解答は 0 点です。

この設問は難しかったためか，正解者が少ない結果となりました。

設問 4 は，リスク分析表にある「不正コピー，データの紛失，盗難」というリスクに対して，リスク対策を考える設問です。「不正もち出し，内部犯行」という脅威が書かれているので，対策は比較的すぐに思い浮かぶはずです。

解答例のように「外付け記憶媒体へのコピー禁止」，「機密データの外部もち出しの禁止」，「機密データの外部もち出しの管理体制を厳しくする」という内容の他，「ダウンロードの禁止」，「ダウンロードのログの監視」も正解にしています。

ここでは外部持ち出しに注目してください。「セキュリティポリシ」，「セキュリティ教育」，「暗号化」などは，広義の情報漏えい対策になり，本設問の解答には不適切です。「アクセスログをチェックする」は的外れのため 0 点です。

問2 旅行業におけるモバイル営業支援システム

【採点基準】

［設問1］

（1）不具合の内容は，解答例どおりの場合 7 点。

（2）対応策は，解答例どおりの場合 8 点。それ以外の場合は，基本的に 0 点。

［設問2］ 画面の内容をのぞき見，盗み見され情報が流出すると書かれていれば 10 点。その他は 0 点。

［設問3］

（1）確認すべき項目は，解答例どおりの場合 7 点。

（2）確認方法は，解答例どおりの場合 8 点。その他は，基本的に 0 点。

［設問4］ 解答例どおりだけ 10 点。その他は 0 点。

【講評】

問 2 はモバイル営業支援システムとして，データ送信における信頼性と安全性に関する問題です。設問 1，3 はやや難しいですが，設問 2，4 は正答率が高く，全体的に平均点を上げています。満点者もかなり出ていました。

設問 1 では，不具合として「モバイル端末に情報が残った場合に登録が完了していないと思って二重登録してしまう」を答えます。その対策として「登録受け付けの際に既に登録された案件情報と同じ内容の場合に登録を拒否する機能を用意する」です。

モバイル側ではなく，サーバ側で行う対策を記述することに注意してください。「端末に通信エラーを通知する」，「サーバ側のデータを上書きする」，「サーバ側で前のデータを消去し更新前の状態に戻す」等の解答は，適切な対策とはいえないので不正解にしました。

設問 2 は，「画面を第三者に覗き見される」，「盗み見される」と書かれた解答が正解です。こちらはほとんどの方が正解の記述をされていました。

設問 3 は，モバイル端末からの情報流出がないことを確認する項目とその方法を述べます。解答例のように確認すべき項目は「モバイル端末に残された情報が画面に表示されて流出していないこと」，又は「端末にアクセスしていないこと」となります。その確認方法は「モバイル端末に残されたログを閲覧して，紛失時間中に成功したログインがなかったことを確認する」となります。この点は，問題文中の「モバイル端末へのログイン／ログアウトの履歴情報はモバイル端末内に保存され…」という文章を読めばすぐに解答に結び付けられます。

確認項目と確認方法を，確認項目に「ログイン／ログアウトの履歴情報を閲覧」と書いている解答もありました。併せて一つの解答として 8 点です。

設問 4 は，活用効果を測定する指標を書きます。非定

形業務の効率向上の効果となっているので，文中から，電子メールとグループウェアの活用であることが分かります。正解は「モバイル端末を使った電子メールとグループウェアのアクセス件数を社内 PC と比較する」となります。社内 PC と比較することは必ずしも必須ではありませんので，上記活用情報を収集するという記述でも正解にします。ほとんどの方は正解をしています。なお，「訪問件数の増加指標」，「社員同士のコミュニケーション指標」などは不正解です。

問3 損害保険業における内部統制のシステム監査

【採点基準】

［設問1］ a,b,c は，解答例どおり「エ，オ，イ」だけ各 4 点。その他は 0 点。

［設問2］ 問題点と改善点は解答例と同じであれば，各 6 点。その他は，基本的に 0 点。

［設問3］ 問題点と改善点は解答例と同じであれば，各 6 点。その他は，基本的に 0 点。

［設問4］ 必要な施策とその効果を確認する監査手続について，解答例と同じであれば，各 7 点。その他は，基本的に 0 点。

【講評】

内部統制に関する問題は，システム監査の問題として最近多く出題されるようになっています。しっかりと理解しておく必要があるテーマです。COSO レポートによると，内部統制とは「業務の有効性・効率性，財務諸表の信頼性，関連法規の遵守に分類される目的を達成するために，合理的な保証を提供することを意図した，取締役会，経営者及びそのほかの職員によって遂行される一つのプロセスである。」と定義されています。このプロセスに従ってどのような統制が行われるかの理解が必要でしょう。低得点が目立つ問題でした。

設問 1 では，解答例に従って順に，IT 全社的統制，IT 全般統制，IT 業務処理統制と理解します。

設問 2 では，契約プロセスの問題点を考えます。問題点は「営業員の詳細な報告を受けないまま上司が承認を与えている」ことで，別解として「営業員が個人的な判断で算定している」，「自由裁量で判断している」も正解にします。営業員の報告だけで営業所の上司が承認を与えている点は大きな問題です。

改善策としては，営業員からの報告が必須なように業務プロセスを改善することですので，「営業員からの詳細な報告を文書等で確認して上司が承認する」となります。

間違いとして多い解答はチェックリストに関する答えです。設問にあるように「内部統制上の…」という条件を考えてください。改善策に「チェックリストの項目を充実させる」だけでは不十分です。上司への報告と承認を考えてください。

設問3は，現金収納における内部統制上の問題を考えます。問題点は「経理部は営業員の自己申告だけで現金収納を行っている」こと，改善策は「収納金額について顧客からの確認を取るようにする」ことです。ここでも，設問にあるように「内部統制上の…」という条件を考えてください。「通し番号をつける」などの伝票の工夫ではありません。「契約申込書との突合せ」でもありません。「顧客に渡した領収書の控えを添付する」などの解答は，本当に渡した領収書の控えかどうかが確認できないので正解になりません。やはり顧客へ直接確認することが必要です。営業所の上司は現金収納に関して直接かかわっていないので，統制上の問題は考えません。

設問4は，営業員の問題意識を改善する施策と，その効果を確認する監査手続です。(1)施策として「未納問題を解決することの重要性について教育・研修を行い徹底する」こと，監査手続は「適切な対象者に対するアンケート又はヒアリング調査で，教育の理解度を確認する」です。

(2)効果を確認する監査手続として，適切な対象者を選定して，アンケート又はヒアリング調査で，教育の理解度を確認することが必要です。

ここで「契約解除の数が減少している」という解答は間違いです。営業員の問題意識の改善効果に限定してください。同様に，「教育が行き渡っていることを受講者名簿で確認する」のも意識改善の効果を測定するものとしては不適切です。

問4 製造業における情報システム開発手続の監査

【採点基準】

［設問1］ 解答例と同様の内容であれば 12 点。その他は，基本的に 0 点。

［設問2］ 解答例と同様の内容であればあれば 12 点。その他は，基本的に 0 点。

［設問3］ 解答例どおりだけ 12 点。その他は，基本的に 0 点。

［設問4］ トラブルと回避策は解答例と同じであれば，各 7 点。その他は，基本的に 0 点。

【講評】

問 4 は，情報システム開発手順に関する問題です。正答率は全体的に低くなりました。

設問 1 では，情報システム要件定義書のレビュー項目を書きます。解答として「業務要求定義書の要求項目がすべて情報システム要件定義書に記載されていること

を確認する」です。これは，問題文中の「情報システム開発手順の標準フロー」では前工程に当たる業務要求定義の内容になります。解答はすぐに発見でき，ほぼ全員が正解を書いていました。その他，生産方式，全体最適，信頼性などに関する解答は的外れの解答になり，不正解です。

設問 2 は，生産部門が要求した機能を採用しないと判断するために必要な検討項目を述べます。「要求された機能を実装しない場合でも人手による業務遂行が可能なことを確認する」ことです。

設問の趣旨が理解できないせいか的外れの解答が多く，正解者の非常に少ない設問でした。「システム全体の導入目的が果たせていればよい」，「完成納期が守られていればよい」，「個別買いとまとめ買いのコスト比較をする」，「複数製品にひも付けた共通部品の発注頻度」などは的外れ解答ですべて 0 点です。

設問 3 は，製造部門の製造指示発行機能について，開発手続上確認すべきことを考えます。「製造部門の要望が業務要求定義の内容と矛盾しないか経営企画室を交えて確認する」という解答が書ければよいでしょう。その他の解答として，「機能決定に関して経営企画室の関与手続を確認する」とか「生産計画に影響を与えないか確認する」，「購買部門の影響を与えないか確認する」などはいずれも不正解です。関与する部署を指摘するのではなく「情報システムの企画は経営企画室が立案するのであるから経営企画室が承認していることを確認する」ことが必要です。

設問 4 は，計画どおりのサービス開始ができないトラブルを考えます。そのトラブルは「運用テスト工程で利用者の要求が満足されないことが発覚して手戻りが多発する」ことです。

ただし，設問にあるようにサービス開始が困難なトラブルですので，「利用者の要求が実現せずシステムが利用されないリスク，目標達成できないトラブル」はシステムが開発され，サービスが開始された後の説明であり，不正解です。システムサービスが提供する前の運用テストの段階で発見されるトラブルであることが必要です。

そしてその回避策は「情報システム設計の工程でプロトタイプを作成して利用部門から設計内容の承認を得る」ことです。回避策として，プロトタイプというキーワードがあれば正解としました。

以上