2010 春 システム監査技術者 総合実力診断模試 講評と採点基準

2010 年 2 月 17 日 (株)アイテック 商品開発本部

■ 全体講評

4 問から二つ選んで解答するが，問 1，問 2 は比較的易しく高得点者が多いのに反し，問 3，問 4 は少し難易度が高く，低得点者が目立ちました。

全体に，過去問を勉強している人にとっては，解答しやすい問題が多くあったと思います。どのように解答を書けばよいかを修得するため，経験を積むことが重要です。例えば，キーワードを明確に記述することが高得点につながります。

出題テーマとして，問 1 は「システム変更管理の監査手続について」，問 2 は，「顧客管理システムの認証業務について」の問題です。

問 3 は「ホスティングサービスの監査と ISMS」，問 4 は「内部統制の手続」に関する問題であり，システム監査によく出題される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ている出題です。

全体に長文の問題を読んで理解しなければならないので，時間が足りません。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。解答における注意点として，設問をよく読んで「何が要求されているか」をすばやく理解することが重要です。そのような場合は，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。

また，解答として要求されていることを正しく理解してください。解決策を求めている設問に，問題点を書いている人もかなりいる状況です。

問1 運輸サービス業におけるシステム変更管理の監査手続について

【採点基準】

〔設問1〕

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 10 点。「システム保守運用基準書の作成時期が明記されていない」でも正解としました。その他は，基本的に 0 点。「改善の納期を守っていない」とか「目標達成ができない」というのは現時点でいえることではないので 0 点としました。

また「改善の実施時期」に無関係な解答は 0 点としました。例えば「多忙な担当者に任せた」，「担当者が他部門へ移動したこと」などです。

なお，(2)システム開発部のところをみて，「データ修正を行う場合は，・・・」などと書いている人がいます。システム企画部の記述ではありませんので，不正解です。

〔設問2〕

「システム変更依頼書にユーザ部門責任者の承認がないこと」と同様の趣旨が適切に指摘されているものに対し 10 点。その他は，基本的に 0 点としました。

「システム開発部の責任者の承認」を挙げたのは 0 点になります。改善計画書の中で触れているのでこれは問題として挙げる必要はないでしょう。

また，「部署名の更新がされていない」とか「勉強会の周知徹底がない」，「緊急の場合のルール作成がない」などはシステム企画部についてのことで，システム開発部の記述ではないので 0 点としました。

〔設問3〕

「月に 1 回開催予定の勉強会がまだ 3 回して実施されず，理解度の調査をしていない」と同様の趣旨が適切に指摘されているものに対し 10 点。その他は，基本的に 0 点としました。

「システム変更／データ修正の事前承認が 4 割であった」という解答も 0 点になります。設問の趣旨から考えてシステム開発部の勉強会以外に関する解答は不適切です。また「規定類の修正がないまま勉強会を実施した」というのも，周知徹底状況には直接結び付かないので 0 点としました。

〔設問4〕

不適切な行動として，システム保守運用基準書の改訂を監査部の K 氏が作成することを承諾したことと同様の趣旨が適切に指摘されているものに対し 10 点。

理由として，改善計画の実施責任はシステム企画部長が持つべきことと同様の趣旨が適切に指摘されているものに対し 10 点。別解として，「独立的立場にあるべき監査部員が業務の基準書作りに携わるべきではないから」も 10 点です。

その他は，基本的に 0 点としました。

【講評】

システム変更手続の監査に関する問題ですが，内容的には一般的な「システム監査のフォローアップ」に

ついての問題です。システム運用･保守において変更管理という独立したステップが確立しています。システム変更の実施状況を自己点検するための内部監査が必要とされています。

監査の指摘事項を受けて改善計画が作られています。その改善計画書の内容及び実施状況について，監査部門と被監査部門の関係，監査人の立場，改善計画書に基づくフォローアップの実施などについての正しい理解をしているかどうかが問われています。

過去問を勉強した人にとっては，解き慣れた問題と思われ，高得点者が多数いました。

設問1の改善の実施時期については，監査概要の(2)③改善勧告で「システム保守運用基準書の作成時期について，遅くとも年度末までに行うこと」になっています。しかし，〔改善計画書の作成〕(1)システム企画部のところの記述をみると，「時間の余裕が出てきた段階で作成する」とあります。これが不適切な内容になります。

設問 2 では，問題点への対応が改善計画書で触れられていない点を述べます。〔システム監査の概要〕(3)システム開発部の監査の②発見事項で指摘された内容は「システム変更・データ修正依頼書にユーザ部門の責任者又はシステム開発部の責任者の承認印がないケースが多数見つかった」ことです。

この問題への対応がとられていない点として「ユーザ部門の責任者のことが触れられていない」ことが解答になります。ほぼ全員が正解でした。

設問 3 は，部内へ規約類を周知徹底する状況を監査するための手続に関する問題です。監査報告書の提出から半年が過ぎているのに，「勉強会がまだ 3 回しか実施されていないこと」とあり，十分な周知徹底状況とはいえないでしょう。また，「回数だけでなく勉強会の内容や理解度の調査をしていないこと」も周知徹底活動の問題として重要です。

設問 4 は，K 氏の不適切な行動として，改善提案を実施した立場が問題になります。改善指摘事項について，システム企画部が監査人 K 氏に「システム保守運用基準書」の改訂を依頼し，K 氏はそれを受けたことは監査人としての独立性を損ねることになります。

システム企画部が作成すべき「システム保守運用基準書」修正案を監査部の K 氏に作成依頼し，K 氏がそれを受けたことは，たとえシステム企画部からの依頼とはいえ，独立的立場を要求される監査部員として不適切です。ここのキーワードは，監査人の「独立性」です。このキーワードが書かれていれば正解としました。

問2 「顧客管理システムの認証業務について」

【採点基準】

〔設問1〕

(1)a，b は，解答例どおり各 4 点。

b として，別解「次回監査計画」も考えられます。a，について，単なる「監査結果」は 0 点としました。

〔設問2〕

次の三つを指摘します。

①監査チームメンバの中に，受信企業の担当部長がいる

②個別計画書と基本計画書の承認順序が逆

③問題点を指摘した後は，それに対応した改善策が提言されていない

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それぞれ 8 点です。

その他は，基本的に 0 点としました。

〔設問3〕

解答例は次の二つです。それぞれに対し 9 点です。

①B 社の審査担当者が Z 社から送付された IC カードと PIN メモを，送付先のチェックや内容を確認せずに会員へ直接送付している

②B 社の担当者は，会員からの失効申請を本人確認しないまま処理をしているので，悪意的な申請の妨害や失効を防ぐことができない

その他は，基本的に 0 点としました。

【講評】

この問題は，監査報告書の内容項目と監査手順についての知識を問う問題です。比較的易しい問題ですが，認証システムの図があったので敬遠した人が多いと思われます。これらの項目は一般的な監査報告書の基本知識として認識されなければならないでしょう。

設問 1 は，「システム監査基準」の報告基準によると，報告書には，指摘事項，改善勧告，改善案を記載すること，となっています。この改善提案は⑦総合評価の前にくるべきものであり，a「問題点と改善対策」が正解となります。b「フォローアップ計画」又は「次回監査計画」です。

解答として目立ったのは，b のところの「問題点と改善対策」を書く人が多いことです。順序からいえば総合評価の前になければならないのですが，これは，一応正解としました。監査のプロセスは十分に理解してください。

設問 2 は，監査手続に問題があることを，問題文を読んで抽出します。次の 3 点を指摘します。

①監査チームメンバの中に，受信企業の担当部長がい

ます。本来システム監査は，監査対象から独立かつ客観的な立場のシステム監査人が行うものです。監査チーム内に被監査企業の部長が入っているのは，問題点としてすぐ分かることです。
②個別計画書と基本計画書の承認順序が逆です。基本計画書と個別計画書の理解があれば，この解答はすぐに導かれるでしょう。
③「システム監査基準」では，システム監査人は「情報システムを総合的に点検評価し，組織体の長に助言及び勧告するとともに，フォローアップする一連の活動」をするとあります。監査で問題点を指摘した後は，それに対応した改善策が必要であるのですが，提言していないことが分かります。

不正解になった解答として「問題点について受信企業を交えて確認した」があります。監査では普通に行われている行動であり特に問題はありません。

設問 3 は，B 社における会員登録の受付と発行処理，及び失効処理手続上の問題点を挙げます。
①B 社の審査担当者は，Z 社から送付された IC カードと PIN メモを送付先のチェックや内容の確認せずに，会員へ直接送付しています。間違えた相手に送ることがあっては，重大な機密情報の漏えいにつながります。
②B 社の担当者は，会員からの失効申請を本人確認しないまま処理をしています。なりすましによる悪意のある申請の妨害や失効を防がなければならないので，少なくとも，コールバックなどの手段で本人確認をすべきと思われます。

不正解とした答えには次のようなものがあります。

①について，「IC カードと PIN メモを一緒の封筒に入れて送付している」「普通郵便で送付している」「登録申請について書類チェックだけである。管理者の承認を得ていない」などは，間違いではないが，正解の答えに比べて必要性が薄いと思われるので 0 点としました。

②について，「CRL の公開まで時間がかかるので，会員は Z 社に直接連絡すべきである」は正解としませんでした。問題文からそのような時間短縮の必然性は読み取れません。

問3 ホスティングサービスの監査とISMS

【採点基準】

〔設問1〕

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採点します。別解が多く示されています。この中から，2 例を選んで，解答することでそれぞれに 10 点となります。

その他は，基本的に 0 点とします。

〔設問2〕

別解を含めた四つの解答例の中から 2 例を解答することで，それぞれに対し 8 点。その他は，基本的に 0 点としました。

〔設問3〕

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 14 点。その他は，基本的に 0 点としました。

【講評】

情報処理業務を委託している企業への監査をする場合の設問です。ホスティングサービスを提供する A 社は，その顧客である M 社からの要求事項にどのように対処するか，監査報告の開示について及び ISMS 認証と内部監査との関係を問われています。セキュリティを中心とした ISMS 認証は，公式的な基準に沿った監査であるということをよく理解する必要があるでしょう。

ISMS は情報セキュリティマネジメントシステムの略で，システム運用に関する JIS 規格となっています。規格に基づく要求事項を満たすことで認証が行われます。

設問 1 は，M 社からの要求を「すべて受け入れること」が，他に悪影響が出る可能性があり，これが問題点です。模範解答のような別解も含めた解答となるでしょう。
①障害が発生した場合に，M 社の指示に従って対策を講じると，他の顧客の業務に悪影響を与える可能性がある
②障害発生時に個別の顧客に対応することによって，提供サービスの標準運用が崩れ，コスト高になる
③障害発生時に個別の顧客に対応することによって，提供サービスの標準運用が崩れ，ミスの発生の可能性が高くなる
④アクセスログを部分的に削除することは，ログの連続性及び完全性を損ねることになり，ログの信頼性がなくなる

不正解となった解答には，「M 社にだけ不正アクセスを日次報告することは，公平性，公正性に欠ける」などがあります。ログの保管期間，保管・保存容量に関する解答も 0 点にしました。

設問 2 は，B 部長が監査結果を開示した根拠は，報告書に記載された内容の影響度合い及び M 社に対し監査結果を開示する場合の社内手続がなかったことに起因すると判断できます。したがって，顧客に監査結果を開示する場合の条件として，監査結果の開示を承認する

ルール及び開示先での取扱契約のことを記述してあれば，よいことになります。
①監査報告のうち，顧客に関連する開示対象範囲はどの部分かを定めておく
②開示した監査報告書の開示先での取扱条件を定め，契約を取り交わしておく
③開示の可否を決定する手順，開示の判断基準を A 社内で定めておく
④電子データで監査報告書を提供する場合は，修正できないようにする

この中から 2 例を挙げればよいでしょう。この設問は分かりやすかったせいか，ほとんどの人が正解です。

この設問のように「対応すべき対策」を聞かれているのですが「現状の問題点」を書く人がいます。設問に合った解答をしてください。

設問 3 は，ISMS が認証基準について準拠しているかどうかの監査である点を理解していればすぐに解答は導けると思います。つまり，ISMS 認証の審査は「あらかじめ定められた規格の要求事項に対する適合性の評価」であり，M 社の要求している保証レベルなどに合わせて変更ができないことがポイントです。また，個々のサービス品質に対する基準を評価することは，ISMS 認証基準に含まれていないため，M 社の要求を満たしていることを認証所得で証明することはできません。

解答は「ISMS 認証は情報資産を適切に管理し，機密を守るための監査基準があらかじめ決められているので，ISMS 認証では M 社の要求事項を満たすことを示すことはできない」又は「ISMS 認証は ISMS 認証基準への準拠性を審査するだけで，セキュリティレベルの工程は評価しないので，M 社の要求するセキュリティレベルを評価することはできない」となります。ここで 0 点にしたのは「ISMS はセキュリティだけの基準である」とか「内部監査と基準が違う」という解答です。

問4 製造業における内部統制システムについて

【採点基準】

〔設問1〕

ID／パスワード管理の内容について，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 8 点。その他は，基本的に 0 点としました。

〔設問2〕

解答例のように，顧客名称，顧客住所，販売価格，支払条件，出荷先住所が指摘されているものに対しそれぞれ 3 点。その他は，基本的に 0 点としました。

〔設問3〕

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それぞれ 7 点。その他は，基本的に 0 点としました。

【講評】

一般的な内部統制システムの問題です。内部統制は，日本版 SOX 法ともいわれる金融商品取引法の成立によって近年急速に注目されています。内部統制を整備するためには，実務の中からコントロールに必要な項目を選び出し，管理ルールや体制等を明文化して必要な統制を行います。

この問題は長文のためポイントを見つけるのに苦労した人が多いようです。また設問の趣旨は理解しても，問題文のどこをみて解答を書けばよいかを迷った解答者が多く，特に設問 3 は多くの人が全く方向違いの解答を書いています。その結果，低得点が目立ちました。

設問 1 は，ID／パスワード管理の内容を求めています。〔情報の取扱に関する各種規程〕の記述をみると，解答に結び付く文章が載っています。「社員が入社した時に ID を発行し，パスワードは半年ごとに見直し変更設定させる」，「異動や退職時に削除する」，「派遣社員や協力会社社員についても契約時に発行し，契約終了時に削除する」ということが解答となります。

これ以外にもいろいろな解答が考えられますが，「規定に記述されていない」ことなど模範解答以外の表現は 0 点にしました。一般的な ID／パスワード管理の内容もここでは 0 点としました。例えば，「過去に使った ID／パスワードは使わない」「申請時には上司の承認印がいる」「パスワードの設定時に推定されやすい文字列は避ける」などの解答は 0 点としました。また，申請から承認までのプロセスを書いている解答もありますが，いずれも 0 点としました。

設問 2 は，受注入力に当たってデータの誤入力や捏造を防ぐための方策を書きます。通常は顧客コードを入力するので，それ以外の顧客基本情報を挙げればよいでしょう。

顧客コードを入力して，顧客マスタから引き出す項目として，顧客名称，顧客住所，受注価格，支払条件，出荷先住所などがあります。マスタに事前に登録しておかれる情報です。

ここで多かった間違いは，割引率，申請者，与信限度額などです。これらの用語は，一元管理の基本情報という設問から外れているので，0 点としました。

設問 3 は，監査時に確認すべきコントロールのポイントとなる業務処理内容を挙げます。非常に難しい

設問ですが，コントロールのポイントですから，承認行為がどこにあるかを考えてみましょう。

〔受注・出荷・在庫管理業務の流れ〕の中に，業務処理手続を示しているので，コントロールとして「承認行為」に注目して探すと容易に解答できます。

監査時に確認するコントロールのポイントを〔受注・出荷・在庫管理業務の流れ〕の表中から“承認”している部分を抽出します。

①販売価格はこれまでの取引実績による割引額・割引率を考慮し営業部門が承認する

②需給調整の優先度は，これまでの取引実績を考慮し営業部門が承認する

③与信チェックで出荷停止された注文の出荷には，経理部門の承認が必要

この三つの業務が正解です。多くの人は，問題文中のどの部分が当てはまるか，ポイントを探すのに苦労したようで，非常に正解率の低い問題でした。コントロールとは，内部統制の機能であることの意味をきちんと理解してください。

不正解として多かったのは「現物棚卸在庫とシステム上の在庫が一致すること」，「注文と出荷が一致すること」，「入金処理の承認」など，これらは設問の趣旨から外れており 0 点としました。

以上