2008 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

2008 年 3 月 25 日 (株)アイテック 商品開発本部

■ 全体講評

4 問から三つ選んで解答しますが，問 1，問 2 は必須，問 3，問 4 は選択問題です。必須問題問 1，問 2 は比較的やさしく高得点者が多いのに反し，問 3，問 4 はかなり難易度のレベルが高く，低得点者が目立ちました。特に問 4 は長文で難しい設問でした。

全体に，過去問を勉強している人にとっては，とっつき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の経験をつむことが重要です。たとえば，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「コールセンタのリスク監査について」，問 2 は「システム変更手続きの監査のフォローアップについて」の問題です。

問 3 は「情報漏洩対策に関する問題」，問 4 は「内部統制の手続に関する問題」というテーマであり，非常に今日的な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。そのような場合は，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。

■ 問1 コールセンタのリスク監査について

【解説と採点基準】

情報セキュリティは出題されることの多い分野ですから，基本的なことはしっかりと理解しておきましょう。情報セキュリティの基本となる「受渡しルール」や不正アクセス対策としての「ID/パスワード管理」，および事業継続計画(BCP)の内容は，過去問でも何度も出されているテーマです。

緊急事態対応計画や事業継続計画(BCP)においては，緊急連絡のマニュアルがポイントになります。その内容を理解しておきましょう。

設問1

書類･情報の受渡しルールは，セキュリティ対策の基本です。情報の出し手，受け手の双方で授受の確認をすることを書く事が求められています。

現状の受渡しルールでは，(2)「一日分をまとめて」「担当者が直接」送付しています。(3)「送付表を添付しているが本社では到着確認をしていない」という状況です。

このうち問題とすべきは，「担当者が直接」送付していること，および「到着確認をしない」ことです。この点に着目すると，模範解答のような答えが出てきます。つまり，(2)コールセンタ全体でまとめて，かつ責任者が押印することによって確実な送付を行う。また，(3)無事に到着したことを責任者が確認し到着確認表の返送を行うことが必要です。

不正解として多いのは,(2)「問合せシートを作成したら直ちに送る」,「発生の都度送付する」という答えです。そのような必要性は文中には書かれていません。同様に，緊急度を分類して，重要なものは FAX 送信するという解答も不正解としました。

(3)で，単に「到着を確認する」,「確認を徹底する」という解答は答になっていないので不正解としました。やはり，この場合，フィードバック(返送すること)，又は「管理者の確認」という言葉がキーワードとして欲しいところです。

なお別解は，「現在手書きのシートを電子化する」ことで，通信システムで送付することができ，送付確認もできることです。

単に「メール添付で送信する」とか「送付内容をメールで通知する」という解答は，送付票の送付手段が変わっただけで，管理手段の変更ではないので，不正解です。

設問2

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。

文中の「不正アクセス対応の調査の結果」を見ると(1)から(5)までの結果から，(4),(5)の管理者権限を有する内部の犯行については対策不十分であることが分かります。

(4)管理者権限に関するユーザ ID が複数の人によって共有されていることは，不正アクセスにつながる可能性が高い。対策として，管理者権限のユーザ ID

は一人一人別々にして，管理をしなければならない。また，(5)部署の移動がない限り，管理者権限をそのままにしていることも大きな問題として，挙げなければならない。対策として，アクセス権限の定期的な見直しをすることです。

なお，(1)から(3)のユーザについての手続はほぼ完璧な対策を取っており，特段の問題点はないといえるでしょう。そのため，ここについて書かれた解答は不正解にしました。

例えば，パスワードの強制変更は３月でなく１月にすべきだとか，申請書は本人でなく上司が行うべきということは，その必然性が感じられないし，模範解答より重要度は低いといえるので，不正解としました。

この設問のように「対応すべき統制」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下さい。

設問3

「緊急時の連絡体制」について不適切な点及びその変更提案うぃ書きます。

不適切な点として，「通報者は最初に上司へ連絡をとること」「公的機関へ連絡する場合は経営者の承認を得ること」「担当者の呼出しは 24 時間以内とする」ことがあります。それに対する変更提案は「上司への連絡は，緊急処置の後でもよい」「緊急の場合は経営者の承認を得なくて公的機関へ連絡する」「復旧の担当者はできるだけ早く呼出しをする」です。

公的機関とは，消防署や警察など緊急を有する連絡を想定して下さい。担当者の判断で緊急連絡をすることが望ましいでしょう。

間違いとして多かった答えとして「上司への連絡がとれない場合の対策が不明確である」がありましたが，それよりも重要で明白な不備な事項を挙げておくほうが良いでしょう。また同様に「広報活動は，経営者の承認を得なくともできる」という解答がありましたが，マスコミなどへの対応は経営問題ですので，経営者の関与は不可欠としました。

この設問は「(1)緊急連絡体制」についての設問であるのに，(2)BCP 運用体制について答えを書く人が一部います。例えば「BCP の理解度，徹底度が低い」などの解答です。このような解答は不正解です。

また，解答欄が「不適切な内容」を書く欄と「変更提案」を書く欄に分かれていることに注意して下さい。この欄を取り違えて，往々にして「不適切な内容」に「変更提案」を書く人がいますが不正解となります。記入欄の取り違えをしているようでは高得点は望めません。

■問2　システム変更管理のフォローアップ監査手続きについて

システム変更手続き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，およ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，解き慣れた問題です。高得点者が多数いました。

【解説と採点基準】

設問1

改善の実施時期に関する問題です。文中〔改善計画書の作成〕の(1)システム企画部のところの記述を見ると，ここで指摘された事項は「①システム保守運用基準書の作成時期について，年度末までに行うこと」になっています。それに対し「時間の余裕が出てきた段階で作成する」とあるのは不適切です。

別解の「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。

実施時期に関しては，目標達成状況を判定するためにきわめて重要な情報です。

「改善の実施時期」に関係ない解答は，不正解としました。例えば，「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見て，「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

改善計画書で書かれていない点を述べます。〔システム監査の概要〕に記載されている点について見てみます。(3)システム開発部の監査　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」ことを解答として挙げます。ほぼ全員が正解を書いております。改善計画書の中には「システム開発部の責任者の承認」につ

いては触れているのでこれは問題ないでしょう。

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不正解です。

設問3

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回して実施されていないこと」があります。これでは，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。

かなりの方が「システム変更／データ修正の事前承認が4割であった」ことを挙げています。これは，ユーザ部門も含まれた状況であり，システム開発部の結果だけとはいえないので，不正解としました。設問の趣旨から考えた場合，システム開発部の勉強会に関する解答が望まれます。

設問4

K氏の不適切な行動を挙げます。改善提案を実施した部署が問題になります。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氏が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」，「客観性」，「公平性」**です。このようなキーワードが書かれていれば正解としました。

■問3　サービス業／流通業（物販）の顧客管理システムにおける情報漏洩対策の監査

【解説と採点基準】

情報漏洩対策として個人情報保護対策が中心となっています。個人情報保護としては，個人情報保護法を中心としたセキュリティポリシの内容をしっかりと理解しておきましょう。個人情報のライフサイクルや情報漏えいのリスク分析は，基本的な知識です。また，自社内の対策だけではなく外注委託先の個人情報保護管理体制の監査も重要です。

解答には，一般的な解答を要求することもありますが，設問1にあるように「B社の現状に即して」という場合は，問題文をよく読んでその中から解答文を見つけて下さい。問題文中の表現を使うことが要求されています。

設問1

設問では「重大な漏洩事件・事故とはどのような場合をいうか」とありますが，ここでは情報漏洩の重大な事故と判断される基準となる状況を記述します。〔外部委託企業の個人情報漏洩事故対応の監査の実施〕からA社の委託先選定基準について解説しているところから出題されています。

重大な漏洩事件を示している場合とは，模範解答に示すように，「個人情報管理体制の不備」，「運用点検・確認の不備」，「タイムリーな報告の不備」，「社内の過失が認められる場合」，「顧客に直接被害を与えた場合」などです。

この設問の解答は「判断基準」を書くのであって情報漏洩の状況を書くのではありません。それゆえ「インターネットへの個人情報の流出」，「宅配業者の誤配送」，「ＰＣの盗難」，「ウイルスやファイル共有ソフトウェアによる個人情報の漏洩」などという解答は不正解です。

設問 1 は，解きやすい問題ですが，解答の表現として何を書くべきか，迷う問題です。問題文中の文章でない解答は不正解としました。かなりの方が不正解でした。

設問2

表中の空欄を埋める問題です。ライフサイクルについては，文中の〔個人情報保護手順のリスク評価〕に情報のライフサイクルとして「取得から消去」までという記述が見つかるので，a には「取得」が入ります。ｂには表の記述欄に「第三者の定義」とあるので，ここから，「第三者提供」を記述します。ｂを「第三者認証」と取り違えた人がかなりいました。

同様に，リスクｃ，リスクｄには，文中〔外部委託企業の個人情報漏洩事故対応の監査の実施〕に記述されたリスクとして「情報漏えい，改ざん，利用不可，目的外利用，作業ミス，ウイルス感染」の中から，リスクｃに「改ざん，利用不可」，リスクｄに「目的外利用，作業ミス，ウイルス感染」を選ぶとよいでしょう。リスクｄに改ざんを書いている人が多いですが，不正解です。

設問3

設問は「これまでの委託先評価に問題があったので，これからどうするか」ということですが，「今後の選定見直し時に，および毎年の更新時に」という言葉を

補って考えるとよいでしょう。

本文中の〔委託先選定基準と評価実施〕の最後の部分に次のような文があります。「第三者認証の取得を準備中のため，具体的な内容をチェックしていない」「長年の取引先で目立った事故が発生していないので毎年見直し評価していない」。これが問題点です。

ここから改善策として「第三者認証を取得していても，具体的な内容をチェックする」，「長年の取引先で事故が発生していなくても毎年見直し評価する」，および「委託先評価は，選定時だけでなく，毎年見直し評価する」という解答がだされます。

ここで単に「委託先評価基準に即しているかチェックする」という解答だけでは不備です。**「毎年」，「定期的」**にというキーワードが重要です。

その他，「委託先への教育」や「損害賠償の契約」などの解答もありましたが，不正解です。

■問4　製造業における内部統制システムについて

【解説と採点基準】

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 法とも言われる金融商品取引法の成立により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ないます。

この問題は問題文が長いので敬遠した方も多いのですが，つぼにはまれば解答は比較的簡単に導かれます。しかし，長文でもあり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，問題文のどこを見て解答を書けばよいかに迷った解答者が多く，特に設問 3 は多くの人がまった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

ID/パスワード管理の内容を答えます。〔情報の取扱に関する各種規程〕の記述をみると，解答が得られる文章が載っています。それが，「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」，「社員が異動や職務を変更した場合は削除する」，「派遣社員，協力会社社員には契約時に発行し，契約終了時に削除する」という解答となります。

これ以外にもいろいろな解答が考えられますが，模範解答以外の表現は不正解にしました。一般的な ID/パスワード管理の内容はここでは不正解です。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」などです。

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，いずれも不正解です。

設問2

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。普通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ということになります。顧客マスターの内容を考えて下さい。

顧客コードを入力して，顧客マスター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。マスター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ます。

設問3

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あり，この設問に対して何を解答すればよいか迷う人が多かったようです。コントロールのポイントですから，まず承認行為がどこにあるかを考えて見ましょう。

〔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。

これが正解です。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，非常の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下さい。

不正解として多かったのは「計算上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」などなど，すべて設問の趣旨からはずれており，不正解です。

以上