

全体講評

新試験制度の導入に伴い、午後 試験は 4 問中 2 問選択になりました。今回は選択する問題によって難易度にかなり違いがあり、問 2、問 4 は比較的やさしい問題で高得点者が多く出ました。それに対し、問 1、問 3 はかなり難しい問題で低得点者が目立ちました。

このように、選択問題によって大きく得点に差が出るような場合、いち早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 はシステムのリプレースにおける投資計画の有効性と妥当性を監査する問題、問 2 は内部統制の監査に関する問題、問 3 は個人情報漏えい事故に対する対応の監査、問 4 は組込みシステムの開発過程の監査となっています。今回から新たにシステム監査試験の試験範囲となった「組込みシステム」に関する問題が出題されています。「組込みシステム」の問題といっても、システム開発管理やプロジェクトの進捗管理などは、通常システム開発と同様に考えればよいので、解答にあたっては従来とほとんど同じようなポイントを考えればよいでしょう。

全体的に長文の問題を読んで理解しなければならぬので、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、能力の一つになります。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。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。

「問題点を挙げよ」という設問(例えば、問 3 設問 2)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。

問1 システムのリプレース**【講評と採点基準】**

システム開発計画の有効性および妥当性を監査する問題です。有効性および妥当性を評価する場合は、開発の効果を定量的・定性的に分析します。定量的な分析としては、経営に与える効果として、経費削減額や人件費削減量、さらに売上高や利益の向上額などの数値が用いられます。定性的な分析には、顧客満足度の向上やサービスレベルの向上などといった感覚的なものが多く用いられます。人によって判断尺度が違うのが難点であり、

出来るだけ金額換算して定量化することが望まれます。

[設問 1]

計画書に書かれた〔達成すべき目標〕の達成状況を評価する項目として、サービス品質を評価する指標を挙げます。問題文中に〔達成すべき目標〕(3)現行システムに比べて「サービスレベルが低下することのないよう、高い品質を維持する」とあります。

サービスレベルとして用いられる指標には、平均故障間隔 (MTBF)、平均修復時間 (MTTR)、レスポンスタイム、解決件数などがあります。

「具体的な評価指標を挙げなさい」とあるので、抽象的な用語は不正解になります。例えば、単に「24 時間稼働するための高い信頼性、可用性」とか、「ユーザの高い評価」という解答は不正解です。

ここでは指標を書くことが要求されているのですが、多くの人が「高い信頼性を確保する」「現行と同じ稼働率を維持する」のように目標値を記述していました。このような表現は採点対象になりません。

[設問 2]

システム部門および利用部門の人件費として、不足している費用項目を挙げます。問題文中の〔費用の検討〕を見ますと、ここには人件費がほとんど考慮されていません。「システム部門」と「利用部門」のそれぞれの項目において発生する人件費を挙げます。

ここで求められているのは、システム再構築の費用についてであり、定常的な運用段階の費用ではないことに注意して下さい。運用のための人件費は不正解です。また、外部委託費には人件費が含まれているのが普通なのでこれは除外します。

[設問 3]

〔リスクの検討〕(2)(3)において検討不十分であったリスクを考えます。情報システムに関して言われるリスクとは「損失を生じさせる可能性」というのが一般的な意味であり、システム停止、災害の発生、情報の漏えい・盗難などの現実的な損失に結びつくものであることをしっかりと理解して下さい。

問題文中から解答に結びつく用語・表現は見あたらないので、自分の表現で書く必要があります。そのためいろいろな解答がありましたが、キーワードを外していない

い場合は正解にしました。

〔リスクの検討〕(2)では、一つのOSに統一することによる信頼性や安定性の低下がリスクとなります。ここでのキーワードは、信頼性・安定性です。なお、「プログラムの変換ミス」などはリスクには入れません。

〔リスクの検討〕(3)では、利用部門の業務運用において、業務上さまざまなトラブルが予想されます。サービスレベルの低下や業務効率が低下するということがキーワードになります。

「費用が増加するリスク」という表現は、上記リスクの定義にそぐわないので不正解になります。

問2 製造業における販売管理システムの内部統制監査

【別解】

[設問1]・管理者の責任権限を明確にできる。

【講評と採点基準】

この問題は内部統制を具体的な業務と結び付けて考えます。「内部統制」というテーマを見て「難しい」と敬遠した方も多いようですが、分かりやすい設問で解答は比較的簡単に導くことができ、高得点が続出しました。

〔設問1〕

内部統制の策定にあたってまず行うことが業務フローを作成することです。業務フローを図示化することのメリットを挙げます。

模範解答のとおりですが、ここで気をつけるのは「内部統制の効果に結びつくメリット」を挙げることです。このポイントから外れた解答が目立ちました。例えば、情報システムの分担が明確になることではありません。また、情報セキュリティの強化のためという解答も的外れになります。「他の担当者が業務の理解をしやすくなる」、「現状の業務プロセスを正確に明示する」という解答も内部統制の効果に結びつかない解答ですので、不正解になります。

〔設問2〕

「受注業務の処理手順」を見てみると、の部分の問題であることが分かります。要約すると「修正データは営業部員が修正して入力するが、責任者の承認を得ないまま集計処理と出荷処理に回される」ことが問題であり、この点を挙げて改善点を書けば良いので、大変分かりやすい設問であり、ほとんどの解答が正解でした。

なお、改善点が要求されているのに、現状の問題点を書く人もいました。注意して下さい。「管理機能が必要」などという解答がありました。抽象的で不十分な表現です。

〔設問3〕

「調査で発見した問題点」の中で、改善提案に取り入れられていない問題点は です。問題文中の問題点と改善提案を比較対照していけば、対応していない部分はおのずから明らかになってきます。この問題に対する改善提案として「関係者に対し、内部統制について周知徹底する」ということになります。分かりやすい設問で、ほとんどの解答が正解でした。

一部、誤解して「コンピュータウイルスを挙げている人もいましたが、これは安全管理対策に入っていますので、問題に挙げる必要はありません。

問3 外部委託企業の個人情報漏えい事故への対応の監査

【講評と採点基準】

個人情報保護の責任が増している状況から、情報処理を外部委託する場合にも、社内と同等の管理レベルを委託先に求める企業が増えています。X社の場合は、社内の情報管理規程があるので、それに基づいて「外部委託する場合には、委託先選定基準に基づき選定評価する」こととなります。

この問題では、個人情報保護対策に関する一般的な知識を求めています。設問2,3では、不備な点、不足している内容など、問題文に書かれていない項目を考えて書く必要があります。自分の知識・経験を整理していないと、解答が書けません。また、よく問題文を読まないでピントが外れた解答になります。そのため、低得点が目立ちました。

〔設問1〕

「X社情報取扱規程」に規定されている利用者の責任を確認する資料にどんなものがあるか、必要な記録の名称を答えます。解答の通り「情報取扱規程」の中から該当するものを列挙してください。ほとんどの解答は正解でした。

ここで不正解となったのは、「文書持出し記録・管理簿」とか「利用目的申請書」などしか書かれていない解答です。「重要な文書・機密文書の持出し記録」と明確にして下さい。持出しの対象は重要書類なのか、利用申請とは何の利用申請なのかを明確にしていない解答は不正解としました。

また、設問の趣旨は「利用者の責任」を確認するものであり「システム運用者の責任」を確認するものではありません。その意味から「アクセス権限の付与・記録」について書かれていたものは不正解です。

なお、委託先選定基準、委託先選定結果を書いた解答もありましたが、これらは管理記録ではありません。

[設問 2]

「委託先選定基準」に記載されている 3 点について、安全性を確認する上で不十分な点を挙げます。解答のように記述すればよく、あまり迷うことはなかったと思われます。

ここで不正解となった解答を挙げてみます。 について、理解度の測定尺度がない、理解度の測定が困難など。

について、漏えい事故だけでなく他の事故も調べる、事故発生時の対応体制・報告体制がないなど。 について、再委託の選定基準がない、委託先の理解を確認する手続きがない、再委託先に対して情報取扱基準の教育が必要など。これらの解答は、不正解です。

この設問で注意すべき点は「不備な内容」を挙げることです。「 をしていない」と書くべきで、「対策」を書くと不正解となるので注意してください。

[設問 3]

「X 社情報取扱規程に基づく委託先での情報取扱基準」に記載されている内容について不足する項目を挙げます。

現在 X 社から Y 社へ委託している業務内容は、請求書と通知書を併せて封入、検査封げんし、配送業者へ渡すことです。このことから考えると、「データを受け渡しする場合」の配慮が不足していることは、容易に気付きます。それ以外にも、再委託の場合の記録と管理、外部委託する場合の X 社の事前了解、漏えい事故が発生した場合の報告・分析などが不足項目として思いつくでしょう。

それ以外については全て不正解になります。不正解になった解答では次のようなものが挙げられていました。外部委託する場合の事前評価、入退室管理、データ保管ルール、配送業者との情報取扱いルール、顧客情報の社外持ち出し禁止ルールや保管のルール、などです。これらは、問題文の趣旨「現在 Y 社へ委託している業務の内容」に合わないので不正解としました。単に「情報漏えい事故の対策を取る」などは範囲が広すぎて採点対象になりません。

問4 組込みシステム開発過程のシステム監査

【講評と採点基準】

組込みシステムの開発過程の監査という今年から新たにシステム監査試験の試験範囲となった分野の問題です。「組込みシステム」は「装置や機器に組み込まれた、それらを制御するコンピュータシステム」という定義があります。その監査業務は、システムの企画・開発・運用・保守に関するリスクの理解とコントロールの理解

など、通常のシステム開発と同様に考えればよいので、解答にあたっては従来の知識が生かされるはずで、過去問を勉強した人にとっては、解きなれた問題で、高得点者が多くいました。

[設問 1]

開発標準に定められた手続きへの違反を指摘する設問です。問題文中〔システム監査人の把握した事実〕(3)(4)の記述を見ると、違反内容はすぐに分かります。その違反が製品にもたらす影響は、解答のとおりですが、ここで「開発する製品にもたらす影響」とあるので、開発プロセスへの影響より品質に関する指摘をした方がよいと思われます。

プロセスへの影響としては、追加作業が発生すること、スケジュール遅延になることなどが考えられます。

[設問 2]

プロジェクト管理上の問題点は、問題文中〔システム監査人の把握した事実〕(6)を見ると、追加作業やテスト障害発生などが作業進捗の報告から洩れていることが分かります。

もう一つの問題点は、本文中の記述から、調整会議など X 社が主体的に管理を行わず A 社に依存した体制になっていることです。

ここでは、プロジェクト管理について書く必要があるので、開発標準が通用していない、徹底していないという解答は不正解です。また、プロジェクト進捗会議の形骸化などの抽象的な表現ではなく、具体的な内容を書くことが求められています。

[設問 3]

A 社に委託すべき役割として上記設問 1 と設問 2 に対応した内容を挙げると良いでしょう。設問 1 で挙げた問題点を解決するためには、仕様整合性確認調整と、テスト結果の確認という品質確保の役割が必要になります。また、設問 2 で挙げた問題点を解決するためには、進捗状況把握と必要な回復対策の立案という総合的進捗管理の役割が求められています。

ここでは、モニタリングや報告会議などで報告させるとした解答は不十分です。

以上