2012 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

2012 年 2 月 15 日 (株)アイテック 情報技術教育研究部

■ 全体講評

4 問中 2 問の選択になります。選択する問題により難易度のレベルにかなり違いがあります。問 1 はよく出題される問題領域でもあり，比較的易しく高得点者が多く出ています。試験では問題を読んで素早く難易度を推定し問題を選択するという適切な判断が望まれます。

問 4 は「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，通常のシステム開発と同様に考えればよいので，解答するにあたっては従来とほとんど同じようなポイントと考えてよいでしょう。

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」を素早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。

「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。

＜午後Ⅰ＞

問1 サービス業における顧客情報システムの監査

【採点基準】

[設問1]

原因と対策について，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各 8 点。その他は，基本的に 0 点です。

[設問 2]

リスクとして，解答例のように二つ指摘してあれば各 7 点。その他は基本的に 0 点です。

[設問 3]

名称として，「文書管理規定」，または「機密文書取扱いに関する管理規定」などが書かれていれば，5 点。

セキュリティリスクとして，「機密文書がセキュリティ保護の対象にならず情報漏えいする恐れがある」または「機密情報を誤って開示する恐れがある」などが指摘されていれば 7 点。その他は基本的に 0 点です。

[設問 4]

解答例の通り書かれていれば 8 点。ここでは「事業継続計画」がキーワードになるので，そのキーワードの無い解答は基本的に 0 点です。

【講評】

情報管理の問題は過去にも何度も出題されており，過去問題を勉強している方にとっては解き慣れた問題です。多くの方がこの問題を選択しており，かつ高得点を取っています。

[設問1]

ユーザ ID/パスワードの管理に関しての設問です。アクセス権の設定のことではありませんので，注意して下さい。

(1) このような事態が発生した原因として考えられることは「ユーザ ID/パスワードの不適切な管理であり，その結果として退職者のユーザ ID を削除していない」ことになります。

ここでは「退職者のユーザ ID を削除してない」という事実が重要であり，単に「ユーザ ID 管理規定がない，管理ができていない」との指摘は半分正解です。

(2) 対策として ID 管理体制の確立と管理簿の保守点検を行い最新の状態に保つことの二つを書くとよいでしょう。保守という用語は，棚卸，突き合せも可とします。ただ単に「退職者のユーザ ID を削除する」というのは不正解になります。

ここで，ID 管理と直接関係ない解答，例えば，社員情報を定期的にとるなどの解答は 0 点です。

[設問 2]

磁気媒体の外部持出しに関する管理体制についてのリスクを二つ指摘します。

「顧客情報の不正コピーが行われ外部へ流出する危険性」および「USB メモリーの外部持出しにおける紛失・盗難の恐れ」を指摘して下さい。「不正コピーのリスク」と「外部持出しにおける紛失・盗難のリスク」というリスクの表現が必要です。

二つというので，顧客情報と社内機密情報や，パソコンと USB メモリーなど二つの対比する情報をあげた解答もありましたがいずれも的外れです。

なお，外へ持ち出した USB からウイルス感染することは情報漏えいリスクから外れますので，0 点です。

[設問 3]

機密文書の取り扱いに関する全社的な統一規定は何かという設問であり,「文書管理規定」「機密文書取扱い管理規定」となります。このような用語は常識ですので，すぐに解答が書けるようにしてください。

ここでは，文書が対象ですので「機密情報の管理規定」,「セキュリティポリシー」を挙げるのは不適切です。これらは機密文書だけではなく，より広い領域をカバーしているので，ここでは正解になりません。0点です。

この規定がないことで予想されるリスクは「機密文書の情報漏えい」です。このような解答のみ正解にしました。

[設問 4]

「事業継続計画を社内に周知徹底するための教育や広報活動」または「事業継続計画に関わる要員に対する教育や訓練活動」が指摘されていれば正解です。

別解として事業継続計画に関わる要員に対する教育や訓練活動としてもよいでしょう。事業継続計画（または BCP）がキーワードになります。それゆえ，一般的な「セキュリティ教育」や「情報漏えいした時の訓練」などという解答は不正解です。

問 2 キャッシングサービス関連システム監査

【採点基準】

[設問1]

③と④について，それぞれの理由が適切に指摘されているものに対し各 10 点。その他は，基本的に 0 点。

[設問 2]

リスクについて，解答例の通り書かれていれば10点。それ以外は0点。

[設問 3]

入出力画面およびログファイルにおいての保護対策が，解答例の通り書かれていれば各 5 点。その他は，0 点。

[設問 4]

解答例の通り書かれていれば10点。その他は，0点。

【講評】

問 2 は，金融機関のキャッシングサービスシステムにおいて，ユーザのアクセス制御をする場合のセキュリティ対策の問題です。一般的なセキュリティ対策として，ユーザ ID，暗証番号（パスワード）はもっとも基本的な対策であり，暗証番号についてその設定と変更などがきちんと管理されていることの監査が課題となっています。

[設問 1]

③について「閲覧したプログラム仕様書と現時点で実装されているチェック機能の合致を確かめる必要がある」ことを指摘すればよいでしょう。キーワードは「チェック機能の確認」であり，一般的な「プログラム仕様書通りにプログラムが作成されていることの確認」では抽象的なので正解にはなりません。

④について「暗証番号変更時のチェック機能が暗証番号設定ポリシに準拠しているか確かめる必要がある」ことを挙げます。ここでのキーワードは「暗証番号の設定ポリシ」です。キーワードを外した解答は 0 点です。単なる「ポリシ準拠」では正解になりません。

[設問 2]

暗証番号の誤入力が無制限に許容されることで，正しい暗証番号を入手されるリスクを挙げます。

誤入力の回数制限がないと総当り番号を発生させる脅威があります。ここで「不正に暗証番号が解読される」とだけしかない記述は不正解です。

[設問 3]

①入力画面において「のぞき見」対策として隠し文字（マスキング），または非表示になっている必要があります。②ログファイルの保護として，ログファイルを誰が見るかわからないので，たとえ見られても盗難されないよう，暗証番号が暗号化されていること，または暗証番号そのものが保存されていないことを確認します。ログファイルにおいて非表示とする解答がありましたが，それではログをとる意味がありません。

[設問 4]

ATM 利用明細表のテスト印字結果について，十分な監査が行われていないことを問題としているので，解答としては，対象とした金融機関が 3 機関では少ないこと，それ以外の ATM 利用明細票のカード会員番号も調査することを示せば正解とします。

「別解」として，テスト印字結果の閲覧だけではなく，実際の運用段階における印字状況の確認をすることも正解にします。

問 3 コールセンタシステムの監査

【採点基準】

[設問1]

(1) リスク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 10 点。

(2) そのリスクを回避するためのコントロールについて，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。

[設問 2]

顧客満足度の低下について，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12点。その他は0点。

[設問 3]

(1) 電子メールの抽出条件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。

(2) 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 12 点。その他は，基本的に 0 点。

【講評】

再構築後のコールセンタシステムの有効性の監査についての問題です。

[設問 1]

(1) 顧客満足度の低下といったシステムの有効性にかかわるリスクについて考えます。社内 LAN の障害時に顧客が問合せできないという解答になります。「トラフィック増大による品質低下」を記述する解答もありますが，やや的外れになります。

(2) では，LAN セグメントの冗長化という解答が正解です。いずれも，正解率が高く，本文を読めば簡単に正解にたどりつくものと推測できます。

[設問 2]

IVR になったため顧客満足度が低下した理由を考えると，オペレータとの会話を希望している顧客にとっては IVR になったために保留が多くなる，手間がかかるようになったということが解答として浮かび上がります。

分かりやすい内容で，正解者の多い設問でした。

[設問 3]

(1) 顧客の苦情が発生するメールの条件を考えると，容易に「メール回数や終了までの時間」を考えつくと思います。この設問も比較的簡単な設問です。

(2) では，通話の記録が確実に記録・保存されているかに関する監査上の着眼点について述べます。音声記録のディスクの容量管理が正解ですが，設問の意図を読み取れる人が少なく，ほとんど正解はありませんでした。

むしろ，通話記録がきちんと保存されていることのチェック方法についての解答が多く，すべて不正解となりました。

〔監査手続の追加〕で述べられている内容に基づいた記述を期待していましたが，題意を理解していない解答が多く，また監査上の着眼点，すなわち監査視点ではなく，監査手続を記述した解答も多く見られました。結果として，不正解者の多い設問です。

問 4 組込みシステム開発過程のシステム監査

【採点基準】

[設問 1]

①と②それぞれについて，違反内容とそれが製品にもたらす影響について解答する。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 5 点。①，②共に計 10 点ずつ。その他は，基本的に 0 点。

[設問 2]

プロジェクト管理上の問題点として，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各 7 点。その他は，基本的に 0 点。

[設問 3]

提言事項にて，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。

【講評】

組込みシステムの開発過程の監査についての問題です。

[設問 1]

二つの違反を挙げます。

開発標準に定められた手続への違反を指摘する設問です。文中〔監査人の把握した事実〕の(3)(4)の記述を見ると，違反内容はすぐに分かります。

①詳細設計書について，違反は，監督者の確認印がないまま次のステップに進んでいること。その影響は，基本設計書の内容と詳細設計書の内容に不整合が発生することです。

②B 社の単体テストの結果について，違反は監督者のレビューを受けていないこと。その影響は，テストが不十分なため，プログラムモジュールの品質が悪くなることです。

内容的にはここで，本文の記述から推測できるので，それほど悩む問題ではないでしょうが，キーワードを外さないようにしましょう。①のキーワードは監督者の確認印，②のキーワードは監督者のレビューです。

その影響についても，①二つの設計書の不整合，②テストが不十分ということを外さなければ，正解に達します。

その違反が製品にもたらす影響は，「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（例えば，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）より品質に関する指摘をした方が良いと思われます。

[設問 2]

プロジェクト管理上の問題点は，文中〔監査人の把握した事実〕の(6)を見ると，次の 2 点が挙げられま

す。

①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事。

②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事。

このような解答が書かれていれば，正解です。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表現ではなく，具体的な内容を書く事が求められています。

模範通りの解答はほとんどありませんでした。「調整会議」と「進捗会議」についての問題を挙げていれば正解にしました。

個別の細かい不具合を挙げる解答もありますが，例えば，調整会議に出席していない，調整会議の報告が不十分などは，すこし内容がずれているので不正解になります。

[設問 3]

A 社に委託する内容です。A 社の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 に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 に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。このような解答があれば正解とします。

この設問も解答する立場をどう考えるか，悩むところです。大きく言えば，A 社とのプロジェクト管理契約になり，小さく言えば，B 社の進捗管理などとなります。どの視点で解答を書くか判断が難しいですが，模範解答は，その中間レベルで品質管理と進捗管理としてまとめています。それゆえ，このレベルの解答を正解としました。B 社の品質管理，納期管理は立場が違うので，不正解とします。