2015 春 システム監査技術者 全国統一公開模試＜午後Ⅰ＞ 講評と採点基準

2015 年 3 月 20 日 (株)アイテック 教育研究開発部

■ 全体講評

3 問中 2 問の選択になります。問 1 は，食品製造小売り業のシステム開発計画の妥当性の監査についての問題，問 2 は，精密機器メーカの設計情報管理システムのセキュリティ監査についての問題，問 3 は，外部データセンタ利用システムの運用監査に関する問題です。業種やテーマが広範囲にまたがって出題されています。自分の経験や知識の活かせるテーマを選んで解答することが大事ですが，あまり専門にこだわらずに，解答しやすい問題を選んでください。

問題によって平均点にかなり違いがあります。問 1 は，開発計画の妥当性ということで取組みやすかったのか，大多数の方がこれを選んでいますが，やや難解な問題で解答に迷う方が多く，低得点が目立ちました。問 2 は，セキュリティということで選択する人が多数を占めています。この問題は高得点が多く目立ちました。

試験では，問題を読んで素早く難易度を推定し，問題を選択する適切な判断が望まれます。それぞれ長文の問題を読んで，すぐに設問に答えなければならないので，時間が足りません。短時間で解答しやすい問題を選ぶのも，能力の一つになります。設問をよく読んで「何が要求されているか」を素早く理解することが重要です。そのためには，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。

解答にあたっては，出題者の意図をよく考える必要があります。設問で何が問われているかを必ず確認し，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，設問で問われていないことを答えているものが多く見られました。

例えば，問 1 設問 4 で「改善勧告を述べよ」という設問に「問題点」を書く人がいますが，このような解答では高得点は望めません。また問 3 設問 1 で，「障害発生時には，自社要員で最低限行わなければならないことがある」としています。「最低限の範囲」とは何かを題意を踏まえて解答してください。最低限を超えている解答が目立ちました。十分に注意しましょう。

試験当日は，集中力，精神力，体力の勝負になるので，最後まであきらめずに必ず合格するという強い意識をもって臨むようにしましょう。

問1 システム開発計画の妥当性の監査

【採点基準】

［設問1］

監査室長が考えた(1)リスク及び(2)その原因について解答例の趣旨にあった解答であれば各 7 点。その他は，基本的に 0 点。

［設問2］

データモデルに関する(1)問題点及び(2)改善策が，解答例どおりの表現であれば各 8 点。それ以外は 0 点。

［設問3］

監査手続で参照する文書名及びその項目又は名称を二つ挙げる。解答例の趣旨にあった解答であれば各 6 点。それ以外は，基本的に 0 点。

［設問4］

非機能要件に関する改善勧告を挙げる。解答例の趣旨にあった解答であれば 8 点。それ以外は，基本的に 0 点。

【講評】

S 社と U 社の開発プロジェクトによって作成されたシステム化計画書についての監査を行っています。ユーザは S 社です。ユーザの視点に立っての設問が多いので，その観点からの解答が望まれます。設問 1 はどのリスクを解答するのがよいか，設問 2 はどのような問題点を書くか，解釈に迷うような比較的難しい設問です。低得点の方が目立ちました。

設問 1 では，問題文に「取締役会に報告事項として提出された」という表現があり，取締役会では報告事項であるから正式には承認されていないと考えて解答を考える必要があります。模範解答は次のとおりです。

(1)「後工程で経営トップの意向による仕様変更が発生する可能性がある」。経営トップの意向と答えなくとも「後工程で仕様変更が発生する可能性あり」とすれば正解とします。

(2)「システム化計画書が取締役会で正式に承認されていない」。取締役会と書かれていなくとも，正式決定がなされていないことが書けていれば正解とします。

なお，「ユーザが参加してない」という解答は不正解です。

設問 2 の問題点としては，「データの流れが分かりにくい」ではなく，「必要な情報が出力されないこと」です。改善策も，「E-R 図を理解してもらう」，「データモデルの妥当性を理解してもらう」ではなく，「ユーザや経営トップに必要な情報を確認してもらうこと」が大切

で，解答例のようになります。

設問 3 では，基盤チームの妥当性を確認するための文書名又は項目を挙げます。模範解答は次のとおりです。

(1)基盤チームのメンバの名前。又は，開発チームの体制表

(2)システム化計画書の開発スケジュール

これは多くの人が正解を書いています。やさしい設問といえます。(1)(2)のどちらか一つについて，二つ書いてある解答（例えば，メンバの名前と体制表など）は一つの解答にしました。

設問 4 の模範解答は「ユーザと経営トップの意向を確認して，非機能要件の妥当性を検証すること」となります。

「非機能要件について説明会を開く」，「S 社・ユーザに決めてもらう」でもよいでしょう。ここで，プロジェクトメンバに決めてもらうでは不正解になります。

ここでは，キャパシティや応答時間など非機能要件の内容をいっているわけではないことに注意してください。

問2 機密機器メーカの設計情報管理システムのセキュリティ監査

【採点基準】

［設問1］

情報漏えいの可能性があることを答える。解答例の趣旨であれば 8 点。その他は，基本的に 0 点。

［設問2］

(1)対応できないマルウェアについて，(2)情報漏えいを防止するシステム運用方針について，それぞれ解答例の趣旨であれば各 7 点。その他は 0 点。

［設問3］

監視強化策について，(1)提言の理由，(2)記録を保存する理由について，それぞれ解答を述べる。解答例どおりであれば各 7 点。その他は，基本的に 0 点。

［設問4］

承認プロセスの統制及び在庫管理の統制に関して確認対象となる文書や項目をそれぞれ 2 種類ずつ挙げる。解答例どおりであればそれぞれ 1 種類につき 3.5 点。その他は，基本的に 0 点。

【講評】

セキュリティに関する出題です。専門的な知識が必要になります。マルウェアについてあまり一般的なことを書いても得点にはなりません。ヒントとなる文章が書かれているので簡単に解答に結びつけることができ，高得点の方が多くいました。ただし設問 2 (2)はかなり狭い範囲に限定した解答であり，正解者はほとんどいません。

設問 1 は，情報漏えいの可能性とは「設計情報系 LAN から OA・基幹業務系 LAN 上のクライアント PC を経由して情報が漏えいする」を答えます。一般的な「マルウェアの侵入経路」では題意にそぐわないので 0 点です。「PC を経由して流出」とするのが正解です。

設問 2 は，一般的なウイルス対策ソフトで，(1)対応できないマルウェアとは，(2)情報漏えいを防止するシステム運用方針とは，を解答します。模範解答は次のとおりです。

(1)パターンファイルが用意されない未知のマルウェア

(2)通常業務では行わないようなシステム間アクセスを拒否する。

(1)については，ほとんどの解答者が正解です。ゼロデイ攻撃など特定する必要はありません。(2)では設問に「マルウェアの侵入を防げない場合，その対策のための運用方針」を問われているので，暗号化などの技術的な対策は答えになっていません。運用対策でも「不審なメールは開かない」はマルウェアの侵入を防ぐ対策ですので，題意に合いません。「ウイルス感染の疑いがある場合はすぐ報告する」は，やや的外れの解答になります。「システム間アクセスを拒否する」という解答を書いた人は非常に少ない設問でした。

設問 3 は，監視行動についての設問です。

(1)監視強化策を提言する理由として，「該当社員が在席していない時間帯のアクセスは不正アクセスと考えられるため」が模範解答です。

(2)ログイン記録を保存する理由について，「サイバー攻撃があった場合，何回もログインを試みることが考えられるため」となります。総当たり攻撃，パスワードハッキングなども正解にします。(2)で「不審なアクセスがないか」を調べるというのは一般的な監視行動で，不正確な解答になります。

設問 4 の模範解答は，(1)承認プロセスの統制に関しては，突合せの書類として，

①外部記憶媒体使用の承認記録

②外部記憶媒体へのアクセスログ

となります。①は外部媒体使用承認書でも可。

(2)在庫管理の統制に関しては，

①外部記憶媒体管理台帳の数量

②実際の外部記憶媒体数量（外部記憶媒体の現物）

を挙げます。

(2)①は外部記憶媒体管理台帳でも可。ただし，外部記憶媒体管理台帳上の購入数量と廃棄数量は別々に書いてあっても一つの解答としました。②では「外部記憶媒体」としか書かれていない解答は質問の趣旨に合ってい

ませんので不正解です。ほとんどの解答者が正解でした。

問3　外部データセンタ利用システムの運用の監査

【採点基準】

［設問1］

自社で行わなければならないことを挙げる。解答例の趣旨で書かれていれば 10 点。それ以外の情報については，0 点。

［設問2］

リスクの回避策として有効な対策を挙げる。解答例どおりの場合 10 点。その他は，基本的に 0 点。

［設問3］

(1) (2)についてどのような状況かを適切に挙げていること，解答例どおりの場合各 8 点。その他は，基本的に 0 点。

［設問4］

サーバに関して情報項目を二つ挙げる。解答例どおりであれば各 7 点。その他は，基本的に 0 点。

【講評】

外部データセンタ利用システムのリスク管理に関する問題です。常識に頼る部分が多く，解答は比較的やさしいため高得点者が多い状況です。

設問 1 の“障害発生時に自社で行わなければならないこと”は，「障害原因の切分けを行い，適切な業者に連絡する」ことです。適切な業者とは X 社，Y 社とは限らないので限定すると不正解になります。また「最低限行うこと」ですので，「障害発生の原因究明と再発防止策の策定」までは求めていません。これはもっと大きな管理レベルの話です。同様に「データの受渡し」も不要です。

なお，自社で行うこととして「会計・人事など社内向けの関係部署への連絡」を書いた人が多いですが，設問文では「自社要員で最低限行わなければならないこと」となっており，題意にそぐわない解答になります。この設問は，正解者はほとんどいませんでした。

設問 2 では，「別の ISP と契約して，C 社とデータセンタの通信経路を二重化する」を記述すればよいでしょう。「バックアップセンタとの契約で別の ISP と二重化する」でもよいでしょう。「通信回線の冗長化が行われること」を書けばよいので，ほとんどの解答者が正解です。なお「専用回線を施設する」は題意に合わないので不正解です。

設問 3 (1)は，「データセンタ自身が被災して，二重化された機器の両方がダウンする場合」が模範解答です。単に「電源がなくなる障害が発生する」では解答として不備です。

(2)は，「データセンタが火災等の被害にあって，バックアップメディアも消失する場合」が模範解答です。ここでは「バックアップメディアが消失する」ことが重要なので，これが書かれていなければ不正解になります。「予備のディスクも災害にあう」も正解です。

設問 4 は，サーバの性能，容量に関する解答が必要で，

①サーバの CPU の使用率

②サーバのメモリの使用率

となります。

ディスクの空き容量，ディスクの使用率は，正解とします。

設問文に“サーバに関して必要となる情報項目として考えられるもの”とあるので，業務上の項目として「応答時間・レスポンスタイム」，「処理件数」，「データ容量」を挙げてもこれは正解にはなりません。

以上