

午後 試験

問 1

問 1 では、自動化や監視を行うツールを使ったシステムの運用業務に対する監査について出題した。全体として、正答率は低かった。

設問 2 (1) は、作業をするオペレータ自身がログの出力も行っており、モニタリングの有効性に問題があることに気が付いてほしかった。(2) は、その点に気が付けば、簡単に解ける問題である。

設問 3 (1) は、コントロールを実施する側の立場に立って、全件調査すべきであるという解答が多かった。コントロールにかかわる証拠の閲覧（承認印の確認）だけでは状況によって必ずしも十分な監査手続とは言えないことを理解していれば、解答できる問題である。監査は、コントロールが実施されているかどうかをサンプリングなどの監査手続で確かめるものなので、サンプリングの利用自体が間違いとは言えない。(2) は、コントロールの運用状況の評価手続と登録ミスを防ぐコントロール自体を混同している解答が多かった。

問 2

問 2 では、キャッシングサービス関連システムの監査について出題した。全体として、正答率は高かった。

設問 1 は、おおむね正答率が高かった。しかし、の理由として、“キャッシングサービス関連システムにおいて、他人が容易に推測できる暗証番号を設定していないように制限しているか”という監査手続のねらいから外れた解答が散見された。

設問 2 については、暗証番号の入力に関する脆弱性<sup>ぜい</sup>だけではなく、その結果生じるリスクについても解答してほしかった。

設問 4 については、調査対象の数が少ないことを記述している解答が散見された。また、カード会員番号の非表示の方法や、@ネットシステムに関するセキュリティ対策といった、題意から外れた解答が見られた。“ATM 利用明細票上のカード会員番号が非表示になっているか”という監査手続のねらいを適切に理解してほしかった。

問 3

問 3 では、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出題した。全体として、正答率は低かった。

設問 1 (1) では、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の記述を期待したが、単にコールセンタ内の LAN の脆弱性を指摘しただけの解答が多かった。設問 2 でも問うているところであるが、リスクの識別は、監査を行う上で不可欠な能力であるから、是非身につけておいてもらいたい。

設問 3 (2) では、監査上の着眼点について、〔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たが、通話録音システムのログとディスク上の音声記録との整合性といった、題意を理解していない解答が散見された。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た。これらの明確な区別は、監査を行う上での基本的な知識であるので、是非理解しておいてもらいたい。

問 4

問 4 では、契約管理システム導入後の監査について出題した。全体として、正答率は高かった。

設問 1 は、ID の不正使用のような、件数の減少理由とならない解答が一部に見られた。契約管理に関してシステム導入前に発生していた問題点を理解し、指定された資料からシステムの目的が達成されていない可能性を考えて解答してほしかった。

設問 3 は、不正な利用や承認ルートの追加・変更の業務遅延のような、問合せの増加につながらない問題点についての解答が散見された。サポート担当である情報システム部への問合せが多い理由（例えば、システムへの理解不足や教育不足）と問題点（例えば、操作ミスや作業の遅延）の両者を十分に考えて解答してほしかった。

設問 4 は、社内ネットワークへアクセスする ID 及びパスワードに関する監査項目や抽象的な監査項目（例えば、申請時の承認が適切であること）についての解答が散見された。システムの特徴を踏まえて、リスクを十分に考えて解答してほしかった。