

システム監査技術者 講評**【総評】**

システム監査に関連する基準類(システム監査基準, システム管理基準, 財務報告に係る内部統制基準類)が令和5年に一斉に改訂され, 前回(令和6年度)の試験から新基準に基づく試験となりました。今回は新基準下の2回目の試験ということになります。午前Ⅱ試験では, これらの基準からの出題が前回にも増して多かったのが特徴的でした。午後Ⅰ・午後Ⅱの試験では, 毎回トピックとなる知識テーマが取り上げられますが, 今回は午後Ⅰ問1の「オープンAPI」や午後Ⅱ問2の「IT-BCP」がそれに該当するといえます。午後の試験では, クラウドサービスのセキュリティ, IT投資計画, リスク評価, 事業継続など, 幅広い観点における監査業務が取り上げられました。

【午前Ⅱ】

システム監査技術者の午前Ⅱ試験では, 基準や規格に基づく問題が多く出題される傾向がありますが, 今回は特に多く出題されました。出題の中心となる「システム監査」分野の出題は全部で10問ですが, このうち, システム監査基準から4問, システム管理基準から1問, 財務報告に係る内部統制基準類から2問, JIS規格から2問出題されました。つまり, 10問中9問が基準や規格に基づく問題ということになります。また, 午前Ⅱ試験全体を見ると JIS 規格に基づく問題が目立ち, 25問中6問も出題されています。そして, 「システム監査」分野では, システム監査基準にも登場する「スリー・ラインズ・モデル」が「3線モデル」(三つのラインモデル)として初めて出題されたのが特徴的です。

計算問題は1問もなく, ほとんどが知識問題でした。今回は新作問題が多く, 過去問題は他区分の問題が多かったことから, 受験者にとっては初めて見る問題が多かったと思います。新作問題は過去問題よりも深掘りされており, 基準や規格等の記述や用語を知っているだけではなく, その意味を正しく理解していないと解けないような問題が多く出題されました。総じて, 例年より難易度が高めという印象です。

【午後Ⅰ】

問1がオープンAPI態勢の監査, 問2がクラウドサービスのセキュリティ面の監査, 問3がIT投資計画の監査, というように, それぞれ全く異なる観点からの出題でした。問1は, 銀行のインターネットバンキングサービスの利便性向上のためにオープンAPI(Application Programming Interface)を導入する事例です。金融機関ではフィンテック事業者と連携したオープンAPIの活用が進められており, その取組みを反映した問題でした。問2は, IaaSのクラウドサービスを利用したシステムの監査の事例であり, 管理者権限の運用やクラウドサービス特有のセキュリティリスクについて考察する問題でした。問3は, 新たなオンラインショッピングシステムの構築計画をIT投資案件として, その投資計画の妥当性を監査で見えていく事例です。投資回収見込みの検討において不足している部分などを考察する内容でした。

問題文は3問とも4ページにまとめられており, 分量は少なめです。小問数(解答すべき項目の数)は問1と問2が6つ, 問3が5つで例年と大きく変わりません。前回に続き計算問題は1問もなく, 全て文章で

答える設問でした。

<午後Ⅰ問題テーマ>

- 問1 オープン API 態勢の監査
- 問2 クラウドサービスを利用したシステムの監査
- 問3 IT 投資計画の監査

【午後Ⅱ】

問1は新たなシステムの導入を決定する過程における「リスク評価」の監査がテーマです。対象システムに「特有のリスク」を把握してその大きさを評価し、リスクの顕在化の防止策や発見策(=コントロール)を講じ、その状況を監査する、という「リスク→コントロール→監査手続」の順に論述する、定番の流れの問題です。ただし、問題文に例示されている「特有のリスク」が「他国の個人情報を保有し、活用することで生じるリスク」というグローバルで特殊な内容でしたので、この例示に匹敵する水準の「特有のリスク」を持つ情報システムの題材を見つけるのは難しかったかもしれません。

問2は、企業が設定する事業継続計画(BCP)と整合をとって策定する情報システムの業務継続計画(IT-BCP)の監査がテーマです。震災やコロナ禍などを経てBCPの重要性が話題になり、午後Ⅰ問題でも何度か取り上げられていますが、今回は午後Ⅱの監査テーマとして取り上げられました。設問では、目標復旧時間、目標復旧レベル、目標復旧時点の設定とその妥当性、訓練の実施による実効性の確保、結果事象の見直し活動についても解答する必要があり、書くべき項目が多く、具体的な論述が求められています。また、設問イで「監査の着眼点」、設問ウで別の事柄を確認するための「監査手続」が問われており、定番の「リスク→コントロール→監査手続」の流れではないため、設問イと設問ウの対応をとりづらい面がありました。

なお、論述式試験では、今年の春期試験から、設問アの指示が「800字以内」から「400字以上 800字以内」に変わりました。システム監査技術者試験でも今回から同様に変更になりました。

<午後Ⅱ問題テーマ>

- 問1 情報システム導入の決定過程におけるリスク評価に関する監査について
- 問2 災害を想定した情報システムの業務継続計画の監査について

以上