

情報処理安全確保支援士 講評

【総評】

今回の情報処理安全確保支援士試験(SC 試験)の問題では、最新の出題範囲の改訂に基づき、開発や運用時のセキュリティに関する用語や技術に関する内容が多く扱われています。午前問題については、セキュリティ関連文書の改訂ポイントなどに関する出題が目を引きます。午後問題については、4 間の出題テーマがバランスよく分散され、技術者や管理者などいずれの立場の受験者の方でも選択し易い出題構成となっています。出題内容としては、脆弱性管理に関するものが多く、さまざまな脆弱性管理指標に関する具体的な知識が求められています。特に、技術的知識だけでなく、管理的知識についても、知識の有無で解答できるか否かが決まる設問が多く、図や表から読み取らなくてはならない条件設定なども多岐にわたっており、難易度は高めの試験といえます。

【午前Ⅱ】

出題分野については、重点分野とされるレベル4の「セキュリティ」から17問、「ネットワーク」から3問出題されたほか、レベル3の「データベース」「システム開発技術」「ソフトウェア開発管理技術」「サービスマネジメント」「システム監査」の各分野から1問ずつ出題され、出題範囲をすべてカバーしています。出題分野については、レベル4の重点分野からの出題数が全体の8割を占め、重点分野に偏った出題構成が定着しています。

情報処理安全確保支援士の午前Ⅱ問題としては、出題内容、難易度ともに標準的なものであったといえます。過去問題あるいはその変形と思える問題は、7割以上を占めています。このうちSC 試験からの再出題は14問で、特に今回は令和5年の春期試験及び秋期試験からの出題が多くなっています。見慣れた問題が多いため、過去問演習を行っていれば、合格点の6割を超えることは難しくないと考えます。

今回の新規出題としては、問3のSHA-512/256に関する問題、問12のNISTの“サイバーセキュリティフレームワーク(CSF) 2.0”のコア機能の改訂ポイント(GOVERNの追加)に関する問題、問13のIoC(Indicator of Compromise; 侵害指標)に関する問題、問22のOSSツール(SonarQube)に関する問題などが目立ちます。

【午後】

今回の午後試験は、受験者の負担や出題内容の観点から見ると、最初の1問以外は読解や解答に手間かかる問題が多いように感じられるものでした。問題文のボリュームは、最小でも8ページあり、10ページに及ぶ問題もあります。全体的に細かい設定が多く、管理系の問題でも問題文の読解に時間がかかるため、解答時間に余裕はなかったかもしれません。

問1はソフトウェア開発プラットフォームの機能を利用した資産管理や脆弱性管理に関する問題であり、SBOMやSASTツールの活用といった技術的・管理的知識が問われています。

問2はさまざまな脆弱性評価指標(CVSSv3やEPSS)を活用した脆弱性管理を中心とした問題であり、ブランドSQLインジェクションやOpenSSHの脆弱性、鍵交換プロトコルのビットセキュリティ基準など、具体的な技術的知識も問われています。IPAの公表文書に基づく出題視点が多いことも特徴です。

問3はスマートフォンのアプリとWebサーバやクラウドストレージサービス間の通信や関連する処理における攻撃方法やその対策などに関する技術的な問題です。

問4は検索エンジン型で公開IT資産を洗い出す資産管理手法を中心とした問題であり、具体的な洗い出し手順まで問われる作り込まれた内容となっています。脆弱性管理については、CVSSのほか、KEVカタログなども題材として扱われています。

＜午後問題テーマ＞

問1 サプライチェーンのリスク対策

問2 脆弱性管理

問3 スマートフォン用アプリケーションプログラムの開発

問4 IT資産管理及び脆弱性管理

以上