TAC

令和6年度秋期　情報処理安全確保支援士試験

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)は，旧来の午後Ⅰ・午後Ⅱ試験が午後試験として統合され，記述式問題 4 問中の 2 問を 150 分で解答する出題構成に変更されてから 3 回目の試験でした。初回の試験では，問題ごとに問題分量に大きな開きがあり，設問の問われ方も 4 問中 1 問だけ字数制限がないなど統一感がありませんでしたが，回を重ねるにつれてこのような問題ごとの差が縮まってきています。今回は問題分量が 8 ページ～10 ページで，旧来の午後Ⅰ・午後Ⅱ試験のちょうど中間です。また，文章で解答する設問には字数制限はなく，答案用紙に行数のみが設けられる形式に変わりました。一方で，出題されたテーマは，インシデント対応や Web アプリケーションの脆弱性など，旧来の試験でもたびたび出題されていたテーマで変化はありません。ただし，事例内容はより実務的になっており，設問では事例内容に基づいた具体的な解答を求めるものが増えています。4 問とも深いセキュリティ技術知識が必要とされ，規程や基準などのセキュリティ管理知識については問われませんでした。これは前回と同様で，今後もセキュリティ技術中心の出題が続く可能性があります。

【午前Ⅱ】

分野ごとの出題数には変化はありません。重点分野でレベル 4 の「セキュリティ」が 17 問，「ネットワーク」が 3 問出題され，全体の 8 割を占めています。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」の各分野は 1 問ずつとなっています。

レベル 3 の分野からはセキュリティと関連性がある問題が出題されることもあり,今回は「システム監査」で“アクセス管理に関する内部統制”が出題されました。

新規問題は 7 問で，テーマとしては既出のものと午後問題で出題されたことがあるものを除くと，“MITRE ATT&CK”，“パスキー認証における生体情報の受信”，“ SOAR (Security Orchestration, Automation and Response) ”，“DTLS”，“ネットワークタップ”の 5 問となり，前回と同数です。

午前Ⅱ試験としては標準的な難易度で，過去問題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。

【午後】

今回の午後試験は，いずれも定番のテーマでの出題で，インシデント対応，メールセキュリティ，そして Web アプリケーションの脆弱性が 2 問です。新しい攻撃や脆弱性，新しいセキュリティ技術の出題はなく，過去問題演習を行っていれば，解く手掛かりとなったのではないかと考えます。ただし，単語で解答するものはわずかで，文章で記述するものがほとんどを占め，しかも実務的な事例内容に基づいた具体的な解答が要求されており，容易ではありません。文章での解答は行数での制限に変わり，字数制限がないため，これまでよりも解答表現の自由度が高くなっている反面，対策や理由，攻撃方法などを適切に記述するだけの正確な専門知識と応用力が必要とされ，解答の際にはこれまで以上に十分に思考・検討して解答表現することが求められます。

問題文は8ページ～10ページ，解答数(小問数)はいずれも11問～12問となっており，構成面での問題ごとの差はあまりなく均一でした。構成面にとらわれずに得意なテーマ2問を選択できたでしょう。

問1は,過去に毎回のように出題されてきたインシデント対応の問題です。提示されているログを読み取ってマルウェアに感染している範囲やインターネットに送信されたファイルを特定することや，追加の調査内容や対策を具体的に解答することが求められています。

問2は，ドメイン名変更に伴うメールセキュリティの問題です。第三者中継防止のルールのほか，SPF，DKIM，DMARC といった送信ドメイン認証技術に関する設定内容を含む詳細な知識が必要です。ドメイン名変更の移行手順や，メーリングリストを利用する場合のSPFやDKIMの問題点についても出題されています。

問3は，Webアプリケーションの脆弱性によって偽フォームが表示され，クレジットカード情報が漏えいする事例が取り上げられています。HTMLが書き換えられた偽フォームの画面全体を図示するといったSC試験では珍しい設問も含まれています。

問4もWebアプリケーションの脆弱性に関する問題で，脆弱性診断が取り上げられています。主にセッションフィクセーションとHTTPヘッダーの不備について，脆弱性の修正方法や被害を軽減する効果などが具体的に問われています。

＜午後問題テーマ＞

問1　インシデントレスポンス
問2　ドメイン名変更
問3　クレジットカード情報の漏えい
問4　セキュリティ診断

以上