TAC

令和5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】

情報処理安全確保支援士試験(SC 試験)は，これまでの午後Ⅰ・午後Ⅱ試験が今回から午後試験として統合され，今回から記述式問題 4 問中の 2 問を 150 分で解答する出題構成に変更されました。午後の試験時間が 1 時間短縮され，受験の負担はかなり減ったという印象を受けました。

午後問題のテーマはさまざまに分散しており，技術者あるいは管理者などそれぞれの立場の人が選択しやすかったでしょう。特異なテーマはなく，公表されていたとおり，試験で問う知識・技能の範囲そのものに変更はないといってよいでしょう。問題文のボリュームは，午後Ⅰ問題と午後Ⅱ問題の中間ぐらいになると予想していましたが，問題によって大きな差があり，最小のものはこれまでの午後Ⅰ問題と同等で，時間に余裕をもって解答できたと考えます。出題内容の点でも，これまでの午後Ⅱ問題のようにセキュリティ技術面とセキュリティ管理面の両面から幅広く問う総合問題は出題されず，4 問ともどちらかといえば午後Ⅰ問題に近いものでした。そのほかの特徴としては，解答の制限字数が大幅に長くなったことが挙げられ，正確な専門知識と知識の適用能力が必要とされています。

総合的に判断すると，今回の SC 試験は前回よりも易しく，合格率は上がるでしょう。

【午前Ⅱ】

分野ごとの出題数は前回と同じで，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 問出題されました。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。

新規問題は“クリプトジャッキング”，“SCAP”，“DNSSEC”，“OAuth 2.0”，“マルチキャスト通信で使用できる IP アドレス”，“IP アドレスの重複の確認に使用するプロトコル”，“DBMS のデータディクショナリ”，“カオスエンジニアリング”の 8 問です。ただし，テーマとしては既出のものがほとんどを占め，目新しい用語は“SCAP”と“カオスエンジニアリング”の 2 つです。

そのほかは過去問題の再出題で約 7 割を占めています。このうち SC 試験からの再出題は 11 問で，前回より 2 問減って全体の 4 割強です。他の試験区分からの再出題問題もテーマとしては既出のものがほとんどで，SC 試験での目新しい用語は“公開鍵基盤の CPS”のみです。

SC 試験からの再出題が 2 問減ったものの，目新しい用語が増えたわけではないことから，午前Ⅱ試験としては標準的な難易度でしょう。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，出題されたテーマや問われた知識の範囲を見ると，4 問ともこれまでの午後Ⅰ・午後Ⅱ試験との違いはありません。難易度を知識レベルの点から見ると，これまでの午後Ⅱ試験で出題されていた総合問題の事例内容の複雑さや必要とされる知識の幅や深さと比較すると易しくなりました。問題文のボリュームは，最小で 5 ページ，最大で 9 ページでした。午後Ⅰ問題と午後Ⅱ問題の間の分量とはいえ，この

ように問題ごとに大きな差があることは予想外でした。最小のものはこれまでの午後Ⅰ問題と同等のボリュームですが，解答にかけられる時間は1問当たり45分から75分へと増えたことから，時間的難易度は低くなっています。ボリュームの大きな問題2問を選択した場合は，読解に時間がかかり，解答時間に余裕はなかったかもしれません。知識レベルと時間的なレベルの両面から考えると，午後試験は易しくなったといえるでしょう。

これまでとは異なる点は，いずれの問題でも解答の制限字数が大幅に長くなり，特に問4は制限がまったくなかった点です。短い制限字数の場合は，さまざまな条件によって絞り込めるようにヒントとなる記述が問題文や設問文に設定されていることがあります。一方，長い字数で解答する場合は，仕組み，理由，攻撃方法などを適切に説明するだけの正確な専門知識と適用能力が必要とされ，解答の際にはこれまで以上に十分に練って解答表現することが求められます。

問1は，過去に毎回のように出題されてきたセキュアプログラミングの問題です。HTMLのソースとスクリプトが提示され，クロスサイトスクリプティング(XSS)脆弱性について取り上げられています。問題文が5ページと少なく，脆弱性は頻出テーマといえるXSSのみに絞られていることから，開発者にとっては取り組みやすい問題でしょう。

問2は，オフィスの無線LAN環境を悪用した攻撃を防ぐためのセキュリティ対策の見直しについて出題されました。無線LAN，VLAN，ファイアウォールのフィルタリング設定，サーバ証明書の検証，HSTS，EAP-TLS，TPMなどの知識が必要とされています。問題文が9ページありますが，知識レベルはそれほど高くありません。

問3は，クラウドサービスを利用したソースコード管理に関するインシデント対応の問題です。コンテナ仮想化，サーバ証明書の偽装，ドメインフロンティング，WebAuthn，コードサイニング証明書とコード署名などの知識が必要とされ，他の3問より知識レベルが高い問題です。

問4は，リスクアセスメントに関する管理寄りの問題です。企業のセキュリティ設定，リスクアセスメントの手順，リスクレベルの基準を読み取り，リスクアセスメントの結果表を完成させ，追加の管理策を問う流れになっています。リスク源による行為を解答する設問では，問題文の状況設定に沿う範囲で受験者の知見に基づいて答えるものがあり，制限字数の設定がなく，自由度が高いといえます。問題文が9ページあり，読解に時間を要する問題です。

＜午後問題テーマ＞

問1　Webアプリケーションプログラムの開発
問2　セキュリティ対策の見直し
問3　継続的インテグレーションサービスのセキュリティ
問4　リスクアセスメント

以上