令和５年度　春期　情報処理安全確保支援士試験　採点講評

午後Ⅱ試験

問１

問 1 では，Web サイトに対する脆弱性診断を題材に，脆弱性診断で注意すべき点と脆弱性に関する知識や対策について出題した。全体として正答率は平均的であった。

設問 2(2)は，正答率が低かった。“入力したスクリプトが二つ先の画面でエスケープ処理されずに出力”という具体的な事象に着目して，ツール V の設定を行う必要があった。脆弱性診断に使用するツールやマニュアルを正確に理解することは基本的なことである。脆弱性がある場合の Web アプリケーションの動き及びツールでの脆弱性を検知する方法も踏まえて，脆弱性診断を行ってほしい。

設問 2(3)は，正答率が低かった。診断対象 URL 自体を誤って解答した受験者が多かった。拡張機能を用いると，診断対象 URL の応答だけでなく，別の URL の応答も判定対象になる。データを入力する画面の URL とそのデータが出力される画面の URL が異なるということに着目してほしい。

設問 4(2)は，正答率が低かった。XSS を悪用した攻撃の手口は，様々あり，大きな被害にもつながり得る。対策を考える際にも必要な知識となるので，よく理解してほしい。

問２

問 2 では，Web サイトのクラウドサービスへの移行と機能拡張を題材に，権限設定及び認可に関連するセキュリティ対策について出題した。全体として正答率は平均的であった。

設問 3(2)q は，正答率がやや低かった。HTTP レスポンスである(8)と誤って解答した受験者が多かった。HTTP プロトコルの理解を深め，HTTP リクエストと HTTP レスポンスとのデータの違いをよく確認しておいてほしい。

設問 4 は，(1)，(2)ともに正答率が低かった。OAuth 2.0 のメカニズムについては，用語だけではなく，その具体的な方法を理解してほしい。また，ハッシュ関数など，暗号技術の基礎的な仕組みを理解しておくことが認証認可の中で使われる PKCE などのメカニズムを理解する上でも重要であることを知ってほしい。

設問 5(1)は，正答率が低かった。インシデントの再発防止では，受けた攻撃の経路を特定することが重要であることを知っておいてほしい。

設問 5 は，(2)，(3)ともに正答率がやや高かった。権限は，利用者には必要最小限しか与えないよう，慎重に検討することが求められる。業務などの要件と照らし合わせて，設定が必要最小限かどうかを確認してほしい。