令和３年度　秋期　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 アプリケーションプログラムを題材に，Content-Security-Policy（CSP）を利用した脆弱性対策と，SaaS に移行するときのリスク分析について出題した。全体として，正答率は平均的であった。

設問 2(2)及び(3)では，CSP がクロスサイトスクリプティング（XSS）脆弱性を防ぐ仕組みを理解できていないと思われる解答が一部に見られた。従来型のコンテンツに CSP を適用するためにはコンテンツの修正が必要ではあるが，XSS によって被害が発生する可能性は著しく低くなる。CSP の適用は，有効な手段であるので，この仕組みを理解しておいてほしい。

設問 5(2)は，全体的に正答率が高かったが，FIDO 認証器の利用状況を想定できていないと思われる解答が一部に見られた。リスク分析は，対象となる情報システムの利用状況に基づいて行うものであり，あらかじめよく整理しておくことを心掛けてほしい。

問２

問 2 では，テレワークに伴って発生したセキュリティインシデントを題材に，自社だけでなく，ガバナンスを効かせにくい他社を含む対応が求められる状況下におけるセキュリティ対処能力について出題した。全体として，正答率は平均的であった。

設問 3(4)は，正答率が高かった。本文中に示された確認ツールの仕様及びマルウェアの特徴を正しく理解し，遠隔操作機能が実行されていない挙動を適切に解答できていた。

設問 4(3)は，正答率が低かった。対処の優先度を上げるべき会員は，連携端末以外の機器へ感染が広がっている会員であるが，それを絞り込むための条件を明示できていない解答が散見された。マルウェア感染においては，最終的には被害対象について漏れなく対処すべきであるが，被害拡大を防ぐためにも優先度をつけて対処することが重要であることを理解してほしい。