

午後 試験

問 1

問 1 では、リスクに応じたセキュリティ対策やセキュリティ事故への対応方法について出題した。
設問 2 及び設問 3 は、正答率が高かった。緊急時の対応方法や Web アプリケーションに対する当面の予防措置は、従来議論されている一般的なセキュリティ対策でよいので、おおむね理解されていた。
設問 4 (3) の必要な作業とは、本文中に明記した、Web サイトや書籍に記載されている一般的な対策事項をそのまま抜き出しているという不適切な作業の改善を期待したものであるから、A 社受注システムの実態を踏まえたリスク分析である。また、この作業を行わないことによって生じる問題として、“事故が起きること”という誤った解答があったが、本文で設定した状況を踏まえ問題事項を具体的に解答するようにしてほしい。
設問 5 は、本問で設定した事態に対する改善を論点としていることから、事故情報の収集、それに基づく自社システムへの影響度評価、脆弱な箇所への措置のような事前の備えなど、アプリケーションレベルのセキュリティ対策としてなすべき具体的な行動を解答してほしい。事故が起こった場合の緊急対応体制整備やマニュアル整備など抽象的な表現ではなく、もう一步踏み込んで、具体的な事前の備えに言及してほしい。

問 2

問 2 では、企業内部での情報セキュリティ自己点検について出題した。全体としては正答率が高く、情報セキュリティ対策や自己点検について理解できているようであった。
設問 1 (2) d の個人情報保護法における委託先の監督については、正答率が極めて低かった。情報セキュリティアドミニストレータは、情報セキュリティや個人情報に関連する法令等について正しい知識をもっていてほしい。
設問 4 では、情報セキュリティマネジメントに関し、業務を担当している部署と情報システム部で担う役割について問うた。本文を読んで、状況を理解したうえで、それぞれの担うべき役割を解答してほしかったが、情報セキュリティ教育や研修についてなど、本文と無関係に答えられる一般論だけ述べている受験者も少なからず見られた。