平成 30 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，クラウド環境におけるセキュリティ対策について出題した。全体として，正答率は高かった。実務的な設問が多かったため，実務経験者にとっては解きやすい問題だったと思われる。

設問 1 は，正答率が低かった。欧州だけでなく，日本における個人情報保護にも影響を与える規則であるので，知識として知っておいてほしい。

設問 2(2)は，正答率は高かったが，要件や仕様を言葉で正確に表現できていない解答が多く見受けられた。文書において，要件や仕様を言葉で正確に表現する能力を身につけてほしい。

設問 4(2)は，正答率が低かった。この設問においても，不都合の内容を言葉で正確に表現できていない解答が多く見受けられた。文書において，言葉で正確に表現する能力を身につけてほしい。

設問 4(3)は，正答率が低かった。運用管理ツールの効果を正しく理解し，ツールを有効に活用する能力を身につけてほしい。

問 2

問 2 では，セキュリティインシデント（以下，インシデントという）対応の準備とインシデントの調査活動について出題した。

設問 2(2)i は，正答率が低かった。インシデント発覚時には，様々な機器が出力したログを見比べて，経緯などを調査する必要が生じる。各ログに記録された時刻が正しいこと，及び，時刻のタイムゾーンが同じであることが重要である。ログ間でタイムゾーンが異なると，認識違いによって，調査が難航する場合がある。

設問 3(2)及び(3)は，正答率が低かった。社内に侵入した遠隔操作機能をもつマルウェアは，攻撃者が準備した C&C サーバと通信して攻撃者の指示を受け取り，これに従って動作する場合が多い。この動作を正しく理解しておくことは，侵入の検知や被害の未然防止のために重要である。マルウェアが検知された PC をネットワークから即座に切り離すことには長所と短所がある。これを正しく理解した上で，マルウェア検知時の初動活動を設計してほしい。

©2019　独立行政法人情報処理推進機構