令和３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，インシデント対応体制の整備を題材に，情報セキュリティを構築し維持するための技術について出題した。全体として正答率は平均的であった。

設問 1(1)は，正答率が低かった。パスワードリスト攻撃の知識を問うたが，総当たり攻撃（ブルートフォース攻撃）やパスワードスプレー攻撃と区別ができていない解答が多かった。パスワードに対する各種攻撃がどのような攻撃なのか，是非知ってもらいたい。

設問 3 は，正答率が高かった。インシデント対応の体制やライフサイクルについて，よく理解していたと思われる。

設問 4 は，(1)の正答率が低かった。攻撃に悪用された IP アドレスを特定することは，効率的な追加調査や，脅威インテリジェンスについて外部と連携するためにも重要である。また，(3)と(5)の正答率がやや低かった。“/etc/hosts.allow”ファイルの設定やファイアウォールによる接続元制限は，よく使われる対策方法なので，よく理解してほしい。

設問 5 は，正答率が平均的であった。脆弱(ぜいじゃく)性管理は，サイバー公衆衛生とも呼ばれる基本的対策の一つである。脆弱性の評価の仕方をよく理解し，効果的かつ妥当な脆弱性管理を実現してほしい。

問 2

問 2 では，クラウドセキュリティを題材に，クラウドサービス利用を IT 統制していく上で必要な技術について出題した。全体として正答率は平均的であった。

設問 1(3)は，正答率が平均的であった。不正な DHCP サーバの検出方法を問うたが，不正な無線 LAN アクセスポイントの検出方法と混同している解答が散見された。設問文をよく読んで解答してほしい。また，DHCP の仕組みを理解していない解答も散見された。インシデントを分析する上で必要となる基本的なネットワーク技術を身に付けてほしい。

設問 2 は，正答率がやや低かった。情報漏えいがあった場合の最大の被害を想定する必要があったが，題意に沿わない解答が多かった。対象となるサービスの仕様と，本文中に明示してあるトラブルについての状況をよく読んで解答してほしい。

設問 3(2)は，正答率がやや低かった。IEEE 802.1X のシーケンスについて，DHCP サーバから IP アドレスを割り当てられるタイミングを問うたが，基本的なシーケンスの理解ができていない解答が多かった。主なネットワークプロトコルは概要を理解してほしい。

設問 6(1)は，正答率が低かった。個人所有機器の利用を禁止するために，秘密鍵を，会社が管理する PC からコピーできないようにする必要があるが，パスワードによる利用者認証など，効果のない解答が多かった。本文中に明示してある要件を正しく理解した上で，その要件を実現する方法を導いてほしい。