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Ⅰ試験

問１

問１では，リモート保守のセキュリティインシデント対応を題材に，被害範囲の調査並びにSSHサーバ及びファイアウォール設定の見直しについて出題した。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。“接続先のサーバが稼働していない”という誤った解答が散見された。SSHサーバのフィンガプリントの確認は，実運用で疎かにされやすいが，接続先サーバの確認のために重要なことであるので，その目的をよく理解してほしい。

設問3(1)は，正答率がやや低かった。秘密鍵と公開鍵を混同した解答や“秘密鍵のパスフレーズをSSHサーバに送信するため”といった解答が散見された。適切に鍵ペアを管理するためにも，SSHにおける公開鍵認証の仕組みをよく理解してほしい。

問２

問2では，設計文書の管理及びIRM（Information Rights Management）製品の導入を題材に，秘密情報の漏えいのリスクと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，正答率が高かった。IRM-Lがファイルをどのような仕組みで保護しているのかについて，よく理解されていた。

設問2(4)は，正答率がやや低かった。“ブルートフォース”のように，ログイン試行回数を制限する対策がされていることと，推測が容易なパスワードを利用者が設定してしまうという前提条件を考慮していない解答が散見された。利用者認証に対する攻撃手法には様々なものがあるが，それぞれの特徴と有効な対策をよく理解してほしい。

問３

問3では，PCのマルウェア感染を題材に，マルウェア感染拡大防止策，ログの調査並びに，ファイアウォール及びサーバ設定について出題した。全体として，正答率は平均的であった。

設問2(1)は，正答率が高かった。通信要件からFWフィルタリングルールをどのように設定すべきかについて，よく理解されていた。

設問3(2)は，正答率が低かった。実行ファイルの変化について述べた解答が散見された。実行ファイルが変化した場合は，ハッシュ値があらかじめ登録したハッシュ値とは異なるので，Yソフトによって実行を禁止される。実行を許可されているファイルを悪用するマルウェアには，どのようなものがあるかを考えて解答してほしかった。