令和５年度　春期　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，Web アプリケーションプログラム開発を題材に，セキュアプログラミングについて出題した。全体として正答率は平均的であった。

設問 1(3)は，正答率が低かった。“PreparedStatement”とすべきところを“Statement”と解答した受験者が多かった。“PreparedStatement”を使う方法は，セキュアプログラミングの基本であり，理解してほしい。

設問 2(3)は，正答率が低かった。“レースコンディション”は個人情報漏えいなどにつながる可能性があるので，設計，実装，テストでの対策を確認しておいてほしい。

設問 2(5)は，正答率がやや高かったが，“注文番号”と解答した受験者が見受けられた。注文番号は既に抽出条件に入っているので，E-R 図と Java ソースコードから，保険的対策として適切な抽出条件を導き出す方法を理解してほしい。

問２

問 2 では，セキュリティインシデントを題材に，ログ及び攻撃の痕跡の調査について出題した。全体として正答率は平均的であった。

設問 1 は，正答率が低かった。FTP 通信の動作を理解し，“アクティブモード”，“パッシブモード”のデータコネクションがそれぞれ FW のログにどのように記録されるかについて理解してほしい。

設問 2 は，(3)，(4)ともに正答率が高かった。攻撃の調査では，マルウェアの“バインドモード”，“コネクトモード”のそれぞれの通信の方向を理解した上で，プロセスの起動，ポートの利用，FW の通信記録など複数の情報の関連性を正しく把握する必要がある。複数の情報を組み合わせて調査することの必要性を認識してほしい。

設問 3(2)は，正答率が平均的であった。時間の経過とともに URL 上のファイルが変わっている可能性があることを認識し，証拠保全や不審ファイルの取扱方法について理解を深めてほしい。

問３

問 3 では，クラウドサービスの導入を題材に，プロキシのクラウドサービスへの移行に伴うネットワーク構成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 3(1)は，正答率が低かった。“見直し前”と“見直し後”の通信経路について理解していないと思われる解答が散見された。クラウドサービスのセキュリティを確保するためには，クラウドサービスとの通信経路を把握する必要があるので，ネットワーク構成の見直しによってどのように通信経路が変わるかを理解してほしい。

設問 3(5)は，正答率が平均的であった。表 5 の番号 1 と番号 2 について，逆に解答した受験者が散見された。適用されるルールの順番によって動作が変わってしまう。セキュリティ製品のフィルタリングルールでは，適用の順番に注意してほしい。