令和４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，セキュリティ関連会社での脅威情報調査及び CTF を題材に，マルウェアの動的解析システムの，安全な運用方法の設計能力，及び攻撃者の攻撃手法を想定した事前対策の立案能力を問うた。全体として正答率は平均的であった。

設問 2 は正答率がやや低かった。従来のファイル転送手順を，ファイルシェアサーバの感染リスクを低減する新しいファイル転送手順に並び替える問題であったが，内部モードへの切替えを前半に実施するといった，誤った解答が散見された。マルウェア転送は慎重に行う必要がある。作成したファイル転送手順案が，与えられた方針に全て従っているかを，よく確認してほしい。

設問 3 は，(1)，(2)，(3)ともに正答率が高かった。ARP スプーフィングによる，ARP テーブルの MAC アドレスの変化や，通信パケット上の MAC アドレスの変化が正しく理解されていた。

問２

問２では，EDR（Endpoint Detection and Response）を利用した未知マルウェア対策を題材に，EDR で記録したイベントの分析，ルールの作成及び EDR で検知したインシデントへの対応について出題した。全体として正答率は平均的であった。

設問 2 は，正答率が高かった。インシデント対応では，イベントの記録を基にタイムラインを整理することが重要である。問題中に示した EDR のイベントの記録から，マルウェアの挙動が正しく読み取られていることがうかがわれた。

設問 6 は，正答率が低かった。問題中のインシデント対応において，どこで無為に時間が過ぎているかに注目して考えてほしかった。インシデント対応については，幾つかのガイドラインが発表されているので，インシデント対応の全体像を理解できるよう，これらを参照して学習してほしい。