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Ⅰ試験

問１

問 1 では，IoT 製品の開発を題材に，ファームウェアの改ざん対策及び Web アプリケーションプログラムのセキュリティについて出題した。全体として正答率は平均的であった。

設問 1(4)は，正答率が低かった。HTTPS を利用して攻撃者のサーバから偽のファームウェアをダウンロードさせない実装を問う問題であったが，暗号化を行うという解答や，サーバ証明書の確認に触れていない解答が散見された。安全な通信を行うための TLS について理解を深めてほしい。

設問 3 は，(1)，(2)ともに正答率が低かった。リスク評価及び脆弱性の対策立案において，攻撃を受ける具体的な脅威を想定することは重要である。POST メソッドを用いたクロスサイトリクエストフォージェリ攻撃の仕組みとその攻撃を防ぐための対策について理解を深めてほしい。

問２

問 2 では，ソフトウェアの脆弱性に起因するセキュリティ侵害を題材に，攻撃の痕跡の調査から再発防止策の検討までのセキュリティインシデント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(1)は，正答率は平均的であったが，プロセスの起動順序を説明した解答が散見された。不審なプロセスの調査においては，プロセスの親子関係について調査することの必要性も認識しておいてほしい。

設問 3(1)は，正答率が低かった。報告されている脆弱性情報から，実際のシステムについて影響を受ける条件を把握し，影響を評価することは，脆弱性への対処を行う上で重要なので，その手法について理解を深めてほしい。

問３

問 3 では，オンラインゲーム事業者でのセキュリティインシデント対応を題材に，ソフトウェアのサプライチェーンに起因する攻撃への対処について出題した。全体として正答率は平均的であった。

設問 1(2)は，正答率が平均的であったが，マルウェアである prog がコンテナ中で実行されるに至った経緯を踏まえていない解答が散見された。C&C 型のマルウェアによる攻撃の一連の流れについて理解を深めるとともに，コンテナ環境であっても被害が発生しうることに留意してほしい。

設問 3(4)は，正答率が平均的であったが，ソースコードサーバがレジストリサーバにゲームイメージを登録することを見落としている解答が一部に見られた。本問に示した，継続的インテグレーションと呼ばれる手法は，ソフトウェア開発の現場で広く活用されている。安全に運用できるように，よく理解しておいてほしい。