令和元年度　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，マルウェア感染及びその調査，並びに，開発・運用プロセスにおいてのセキュリティ対策について出題した。

設問 1(1)は，正答率が低かった。マルウェアには，目的の遂行のための機能だけでなく，発見されないように自らの動作や存在の痕跡を消す機能も組み込まれているものがある。今回のマルウェア X は，ワームであるので感染拡大機能をもつが，その機能によって，既に感染しているサーバが再度感染してしまう可能性がある。再度感染すると，例えばマルウェア X の処理が始めに戻ってしまい，目的の遂行の妨げになることがある。このようなマルウェアの機能の背景に関する知識も深めてほしい。

設問 2(1)は，正答率が低かった。表 2 に示された対策はいずれも典型的なものである。しかし，具体的にそれらの対策がどのような攻撃に対して効果を発揮するのかは，正確な理解を必要とする。様々な脅威と，対応するセキュリティ対策をしっかりと理解しておいてほしい。

設問 3(1)は，正答率が低かった。セキュリティに関する規格，標準，フレームワークなどは多数ある。それらの目的を正確に把握し，活用していってほしい。

問 2

問 2 では，OT と IT が混在する環境でのセキュリティ対策について出題した。

設問 1(1)は，正答率が低かった。社内に侵入したマルウェアを発見する手法の一つとして，社外と交換される HTTP メッセージを監視するという手法がある。HTTP メッセージの構造，ヘッダフィールドなどについての理解を深めてほしい。

設問 3 の g は，正答率が低かった。無線 LAN で利用される“MAC アドレス認証”は，これを認証技術としてみると明らかに欠点がある。工場などでは無線 LAN が利用されることも多いと思われるが，採用する技術の利点や欠点，限界を正しく理解し，有効な技術を採用することに留意してほしい。

設問 5(2)は，正答率が低かった。ネットワークの構成を工夫することで，リスクを回避，又は低減できるケースは多い。ネットワーク構成の変更の効果を正確に捉え，理解する力を高めてほしい。

設問 6(1)は，正答率が低かった。脆弱(ぜい)性情報について評価する際に役立つ CVSS についての設問であった。CVSS には基本値，現状値，環境値の三つがある。これらを正しく理解し，妥当かつ効果的な脆弱性対策の実現に有効活用してほしい。

設問 7(2)は，正答率が低かった。ネットワークやシステムの運用に責任をもつ部署が知るべきこと，判断に必要な情報について理解しておいてほしい。