平成 29 年度　春期　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，マルウェアの解析について出題した。

設問 2 は，正答率が低かった。HTTPS のセッション開始時の仕組みが理解できていれば正答が導き出せる問題である。HTTPS は通信の安全の確保のため重要な技術であるので，確実に理解しておいてほしい。

設問 3 は，正答率が低かった。攻撃者は，マルウェアの発見を遅らせるために様々な技法を用いている。マルウェアの技術動向について学習を進めてほしい。

設問 4 及び設問 5 は，インシデントの終結に向けての対応について出題した。正答率は高かった。終結の手順はインシデント対応の中でも重要な点である。様々な状況を考えた上で机上演習を行うなど，学習を進めてほしい。

問 2

問 2 では，社内システムの情報セキュリティ対策強化を題材に，ネットワークセキュリティ及びマルウェア対策に関する設計と運用について出題した。

設問 1(1)は，正答率が低かった。セキュリティに関するプロトコルについて，名称だけでなく，その仕組みについて理解を深めてほしい。

設問 1(3)は，正答率が高かった。電子メールのオープンリレー対策について，受験者の知識が高いことがうかがわれる。

設問 2(2)h は，正答率が低かった。電子メールによる情報漏えいが疑われる場合，関連するメールサーバのログの調査が重要であることを理解して解答してほしかった。

設問 5 は，IDS の導入について述べている解答が散見された。IDS には，不審な通信を検知する機能はあるが，IPS とは異なり，不審な通信を遮断する機能はない。IDS と IPS の機能の違いを理解してほしい。