平成 31 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，無線 LAN を侵入経路としたマルウェアへの感染を題材に，マルウェアの調査と対策について出題した。

設問 2 は，正答率が低かった。マルウェアは，発見されないよう自らの動作や存在の痕跡を消去することが多い。消去されたファイルも，セキュリティインシデント対応において，大きな手掛かりとなることが多いので，証拠保全の方法について理解しておいてほしい。

設問 3(1)は，正答率が低かった。WPA2 であっても，MAC アドレスが含まれるイーサネットフレームのヘッダ部は暗号化されないことを理解しておいてほしい。

設問 6 は，全体的に正答率が低かった。プロキシ経由の場合も含め，HTTPS（HTTP over TLS）のセッション確立までの手順と，その手順の中でディジタル証明書が果たす役割について理解しておいてほしい。また，HTTPS 復号機能は，外部との間で HTTPS 通信を行うマルウェアへの対策として有効であるが，一方で制約もあることも理解しておいてほしい。

問 2

問 2 では，セキュリティインシデントの対応を題材に，サーバの設定について出題した。

設問 1 は，正答率が低かった。完全性，可用性といった解答が散見された。企業では，営業秘密の管理は重要なので，営業秘密の要件は理解しておいてほしい。

設問 3(4)は，正答率が低かった。CRYPTREC では，安全な暗号アルゴリズムの一覧を掲載している。暗号アルゴリズムの選択の際に必要となるので覚えておいてほしい。

設問 5(4)は，正答率が低かった。A 社標準ソフトの脆弱(ぜいじゃく)性の検出といった解答が散見された。マルウェアに感染した PC が見つかった際に，他の PC 及びサーバでフルスキャンする目的について，理解しておいてほしい。

設問 6(1)は，正答率が低かった。A 社の内部システム LAN 上のサーバの機能と利用方法を理解した上で，解答してほしかった。

©2019　独立行政法人情報処理推進機構