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Ⅰ試験

問1

問 1 では，電子メールのセキュリティ対策について送信ドメイン認証技術を中心に出題した。なりすましメールによる被害が多数発生している。その技術的対策である送信ドメイン認証技術として，SPF，DKIM，DMARC が標準化されている。SMTP，DNS に加えて，それぞれの仕組みや特徴を理解してほしい。

設問 1 は，正答率が低かった。SPF は SMTP の MAIL FROM コマンドで指定された送信者メールアドレスのドメインを認証することを理解してほしい。

設問 2 は，全体的に正答率が高かったが，(3)は正答率が低かった。SPF の認証の仕組みを理解していない解答が散見された。

設問 4 は，正答率が低かった。N 社取引先になりすまして送信する方法を具体的に説明できていない解答が散見された。

問2

問 2 では，サイバーセキュリティ情報（脅威インテリジェンス）の活用と，C&C 通信への対策手法について出題した。全体として，正答率は低かった。

設問 1 は，全体的に正答率が高かったが，(3)は正答率が低かった。具体性が不十分な解答が多かった。

設問 2(2)は，マルウェアがプロキシ認証情報を窃取する手法を理解していない解答が散見された。

設問 2(4)は，全体的に正答率が低かった。C&C 通信には，よく使われるプロトコルや仕組みが悪用されることが多い。今回出題した DNS トンネリングと呼ばれる手法は，組織内に存在するフルサービスリゾルバとして動作する DNS を悪用する C&C 通信手法であり，悪用される事例が増加している。DNS 及び DNS を悪用する C&C 通信の仕組みや特徴を理解しておいてほしい。

問3

問 3 では，マルウェア感染後のインシデント対応方法について出題した。本問にある R システムは，最近利用が広がり始めた EDR を想定している。EDR を含め，マルウェアの最新の検知手法，インシデント対応方法について，理解を深めてほしい。

設問 2 は，全体的に正答率が高かった。PC の管理の経験が少しあれば，なじみのあるコマンドであり，よく理解されていた。

設問 3 は，全体的に正答率が高かったが，(2)は，正答率が低かった。マルウェアに感染した PC が，C&C サーバと接続していないのは，ネットワークから切り離された状態（ネットワークケーブルを抜く，又は電源の切断）かマルウェアが初期偵察状態であり，当該 PC や周辺 PC からの情報収集中であることが考えられる。実際のマルウェア関連のインシデント対応でも，本問のように分析することは多いので，よく理解しておいてほしい。