平成 30 年度　春期　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，Use-After-Free脆弱性を題材に，メモリ上の任意のアドレスへの書き込みから攻撃コードが実行される仕組みとその対策方法について出題した。全体として，正答率は低かった。

設問 6 は，正答率が低かった。実行コードが置かれることを想定していないメモリ領域であれば，全てデータ実行防止機能の保護対象にできる。一方，実行コードが置かれることを想定しているメモリ領域は，実行を防止するわけにはいかないので，通常は保護対象にできないことを理解しておいてほしい。

設問 7 は，正答率が低かった。シェルコマンドの実行に使われる system 関数について知っておいてほしい。

設問 8 は，正答率が低かった。メモリアドレスを特定するためには，何らかの手段でメモリアドレスを出力させる必要がある。メンバ関数一つ一つについて，メモリの内容を出力させられるかどうかを読み取れていれば，解答できる問題であった。

問 2

問 2 では，サーバの情報セキュリティ対策強化を題材に，サーバ及びファイアウォールの設定，並びに運用業務用 PC のセキュリティ対策強化について出題した。全体として，正答率は低かった。

設問 1(1)は，正答率が低かった。T 社におけるインターネットへのメール転送経路を理解した上で解答してほしかった。迷惑メール対策において，SPF（Sender Policy Framework）は重要であるので，よく理解しておいてほしい。

設問 2(2)は，図 3 に示した通信がプロキシサーバから外部メールサーバへの SMTP 通信であることを理解していない解答が散見された。インターネットとの通信でよく使用されるポート番号は，知っておいてほしい。

設問 3(2)は，正答率が低かった。運用業務用 PC であっても，脆弱性修正プログラムの適用やマルウェア定義ファイルの更新のためには，インターネット上の各ベンダのサイトとの通信が必要となることを理解しておいてほしい。

問 3

問 3 では，ネットワーク分離の設計について出題した。

設問 1 は，全体的に正答率が高かった。リスクアセスメントのプロセスについて，一定の理解がされていることがうかがわれる。

設問 3 は，全体的に正答率が高かったが，i では“研究開発 PC はマルウェアに感染しないから”という解答が一部に見られた。分離されたネットワークであっても，マルウェア感染は起き得ることを前提にセキュリティ対策を検討する必要があることを理解しておいてほしい。

設問 4 は，正答率が低かった。マルウェアが既にパスワードを窃取していることを読み取れていない，“再度パスワードを入力する”という解答が散見された。秘密情報を窃取するマルウェアは実際に存在するので，その仕組みを理解した上で対策を検討してほしい。