平成 25 年度　春期　情報セキュリティスペシャリスト試験　採点講評

午後 I 試験

問 1

問 1 では，マルウェア解析を題材に，マルウェアや標的型攻撃へのセキュリティ対策について出題した。全体として正答率は高かった。

設問 1 は，全体的に正答率が低かった。設問 1 は，J 社の FW のフィルタリングルールと，ML2，ML3 の特徴を理解すれば，論理的に解が得られる設問である。本文の内容を丁寧に読んだ上で，解答してほしい。

設問 2 は，全体的に正答率が高かった。マルウェア解析後の暫定対策についての設問であったが，定石とされている対策内容であり，解答できた受験者が多かったようだ。

設問 3(1)は，正答率が低かった。マルウェアがもつ機能だけでなく，その機能の目的も考察した上で，解答してほしい。

設問 3(2)，(3)は，正答率が高かった。本文中から最も機密度が高い情報が何であるかを見極め，それを守るために J 社はどのようなネットワーク構成上のセキュリティ対策を実施しているかについて，Y 主任と S 氏との会話を通して出題したが，おおむね理解されているようであった。

問 2

問 2 では，DNS キャッシュポイズニング攻撃や SPF(Sender Policy Framework)を題材に，IP アドレス詐称対策について出題した。全体として正答率は低かった。

設問 1(1)は，正答率が高かった。基本的な用語については受験者の理解度が高いことがうかがえる。

設問 1(2)は，正答率が低かった。“送信元ポートを限定する”，“不要なポートを遮断する”などの誤った解答が多かった。根本的な対策である DNSSEC の導入が進んでいない状況下では，DNS キャッシュポイズニング対策として，DNS サーバからの問合せの送信元ポートを予測不能なものとすることが有効であり，そのためのパッチが DNS サーバベンダから提供されている。

設問 1(5)は，正答率が低かった。TXT レコードに関するキャッシュポイズニングが成功した場合には，SPF 検証機能の仕組上，偽装された SPF レコードに従って不正な発信元からメールを受信してしまうおそれがあることに気づいてほしかった。

現在の電子メールシステムは DNS と密接に関係している。電子メールのセキュリティ対策と関連付けて，DNS のセキュリティ対策についても理解を深めてほしい。

問 3

問 3 では，デスクトップ仮想化を題材に，リモートアクセス環境の情報セキュリティ対策について出題した。全体として正答率は低かった。

設問 1 は，正答率が高く，デスクトップ仮想化によって得られる基本的なセキュリティリスクの低減効果に対する理解は進んでいるようだ。

設問 3 は，リモートアクセス環境が不正接続された場合の，影響範囲が二つの案で違う理由を問う問題であったが，ゲートウェイサーバへの攻撃に言及する解答が散見された。図表をよく読んで二つの案の違いを理解した上で解答することを心がけてほしい。

設問 4(1)は，仮想化された PC へ接続する端末側のセキュリティ対策について問う問題であったが，仮想化された PC のセキュリティ対策と混同している解答が目立ち，正答率は低かった。

デスクトップ仮想化は，デスクトップ環境のセキュリティに効果がある技術であるが，リモートアクセス環境においては，仮想化された PC とそれに接続する端末の，両方のセキュリティを考慮しなければならないことを，是非理解してほしい。

問４

問 4 では，不正競争防止法を題材に，機密情報の保護管理を行う上で情報セキュリティ対策をどのように進める必要があるかという視点から出題した。全体として正答率は低かった。

設問 1 は営業秘密の 3 要件について出題した。正答率は低く，2 要件以上を正答できた受験者は少なかった。営業秘密の要件は企業が守るべき情報を明確化するために必要となる知識であり，理解しておいてほしい。

設問 3(2)は，不正アクセス，盗聴やウイルス感染のような，リスクではなくセキュリティインシデントそのものを解答している例もあり不十分な解答が多かった。リスクとセキュリティインシデントを明確に区別して答えられるようにしてほしい。

設問 4 は，電子媒体の機密情報に対する管理策について問うたが，正答率が低かった。電子媒体の機密情報に対する管理は基本的なことなので，知っておいてほしい。