平成 27 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，脆弱性検査の技能試験を題材に，Web サイトの脆弱性と対策について出題した。HTTP ヘッダインジェクションやセッションフィクセーションの脆弱性について，ある程度の知識が必要であったためか，全体として正答率は低かった。

設問 2(1)と(3)は，正答率が低かった。(1)は改行コードを二つ続ける HTTP ヘッダインジェクション攻撃に関する問題であったが，攻撃の仕組みを理解していないと思われる解答が多かった。(3)は改行コードの処理に関して，具体的な対策内容を期待したが，そのような解答は少なかった。

設問 3 は，正答率が高かった。セッションフィクセーションの脆弱性や対策については，よく理解されているようであった。ただし，(1)のような少し実践的な問題については，正答率が低かった。

問 2

問 2 では，運用担当者の PC へのマルウェア感染を題材に，侵入経路及び被害の調査から暫定対策実施までの情報セキュリティインシデント対応について出題した。全体として正答率は低かった。

設問 2 は，(1)，(2)共に正答率が低かった。ネットワーク構成を理解し，侵入及び漏えいの経路をあらかじめ想定しておくことは，インシデント対応だけでなくセキュリティ対策を考える上で重要である。ネットワーク上及び PC 上でのマルウェアと侵入者の動きを具体的にイメージできるよう，ネットワーク及びコンピュータの動作原理並びにそれらに対する攻撃手法への理解を深めてほしい。

設問 3(2) は，正答率が低かった。不正アクセスされる可能性はあるが，不正操作が行われた形跡はないサーバにおける，サービス停止が業務に大きく影響する場合の対策を問う問題であったが，サービス停止を伴う対策，又は実施までに時間が掛かる対策が解答として散見された。インシデント対応では，業務影響を抑えながら速やかに被害の拡大を食い止める対策を立案・実施することが重要であることを理解してほしい。

問 3

問 3 では，Web サイトに対するパスワード攻撃について出題した。全体として正答率は高かった。

設問 1 は正答率が低かった。ハッシュ化だけが施されたパスワードファイルに対する具体的な攻撃方法を問う問題であったが，ソルトなどの対策やレインボーテーブルを用いた攻撃が成功しない理由などを述べる解答が多かった。一般的な知見で解答するのではなく，本文に記載された事例に即して解答してほしかった。

設問 2(2)と(3)は，正答率が高かった。パスワード攻撃の検知について問う問題であったが，パスワード攻撃手法ごとの特徴や，その検知方法ついて，よく理解されているようであった。

設問 4 は正答率が高かった。パスワードリスト攻撃の具体的な方法を問う問題であったが，Web サイトに対するパスワード攻撃は，マスコミに取り上げられることも多かったので，理解が進んでいると思われる。