平成 24 年度　秋期　情報セキュリティスペシャリスト試験　採点講評

午後Ⅱ試験

問 1

問 1 では Web サイトのセキュリティ対策について出題した。全体としては正答率が高く，対策についておおむね理解されているようであった。

設問 1(4)，(5)は，正答率が低かった。技術用語を問う問題だが，正確に記憶できていない受験者が多かった。

設問 2(1)は，正答率が低かった。“セッション ID の固定化”は，“ログイン時に新たなセッション ID が発行されていないこと”と“利用者に攻撃者があらかじめ用意したセッション ID を使わせること”の二つの条件がそろった場合に脆弱(ぜい)性となる。後者の条件をログイン時のリクエストとレスポンスから確認できれば，正解を導けるはずである。

設問 2(2)理由は，問題文中に“エスケープ処理を出力時に行っていましたが”という記述があるにもかかわらず，“エスケープ処理がされていなかったから”といった誤った解答が多かった。また，“二重引用符”だけは書かれていたが，具体的な理由が記載されていない解答も散見された。

設問 3(1)は，正答率が低かった。表 6 の項番 5 の“PC での操作”に記載のパラメタ，“操作の結果”，そして，図 3 の入力した値が次画面で取り扱われるものだけ診断可能という仕様を確認できれば，正解を導けるはずである。(2)の自動診断ツールの仕様と限界についても関連性を的確に解答してほしかった。

設問 4(1)は，脆弱性情報の入手についての改善案を問う問題である。今回，専門業者の診断で脆弱性を発見できたので，同様の効果が得られる運用を解答として期待していた。しかし，問題文中で修正プログラムの適用にはリスクがあるとしているにもかかわらず，“自動アップデート機能を利用する”という誤った解答が散見された。

日頃からセキュリティに関する知識を理解しておくことと，問題文をしっかりと読むことを期待する。

問 2

問 2 では，無線 LAN の導入を例にとり，社内ネットワークの構成変更が情報セキュリティ管理規程や既存のセキュリティ対策へ与える影響について出題した。全体として，正答率は高かった。

設問 2(2)では，“ノート PC からインターネットへの直接の通信を許可する”といった誤った解答が多かった。OA-LAN からインターネットへのアクセスと同様に，会議室 LAN からインターネットへのアクセスに対しても利用者認証や URL フィルタリングが必要である。そのため，会議室 LAN からインターネットへのアクセスもプロキシサーバを経由する必要があるということを，問題文から読み取ってほしかった。

設問 3(3)は正答率が低かった。単に“ノート PC を放置する”といった解答が多かったが，リスクの認識という点では不完全なので，第三者が操作可能な状態であることが具体的に分かるような説明を記述してほしかった。

設問 4(2)も正答率が低かった。プロキシサーバでの利用者認証を行うために，“ディレクトリサーバ上で利用者 ID を登録する”といった誤った解答が散見された。来客のデバイスがインターネットにアクセスする際はプロキシサーバを経由しないとなっていたので，問題文の設定をよく読み，解答してほしかった。