平成 26 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，ID 管理システム及び認証システムの設計及び運用上の考慮点に関する知識と対応能力について出題した。全体として正答率は低かった。

設問 1 は，認証システム及び利用者 ID 管理プロセスに関する問題である。(3)は，正答率が低かった。各地域の ID 管理プロセスを比較した上で，アジア地域における ID 管理プロセスの問題点を解答してほしかった。

設問 2 は，認証システムの方式比較に関する問題である。(1)と(2)は正答率が低かった。エージェント型と呼ばれる認証システムの方式の一般的な考慮点について理解しておいてほしい。

設問 3 は，ID 管理システムの設計に関する問題である。正答率は期待どおりだった。

設問 4 は，認証システムとポータルシステムの連携に関する問題である。地域は正答率が期待どおりだったが，サーバ名の正答率が低かった。通信シーケンスを理解した上で解答してほしかった。

設問 5 は，2 要素認証及びシンクライアントに関する問題である。正答率は低かった。一般的知識である，認証の 3 要素(記憶，所持，バイオメトリクス情報)，読取り装置を利用した 2 要素認証における考慮点，シンクライアントにおける考慮点について，理解してほしい。

設問 6 は，認証システムの統合に関する問題である。(2)は正答率が低かった。SPNEGO プロトコルを利用した統合認証について，本文中の通信シーケンス並びに PC 及び認証サーバに必要な設定内容を理解して解答してほしかった。複雑なシステムの設計においては，システムの動的な側面を通信シーケンスとして図示することによって，設計を検証することがしばしば行われる。セキュリティ技術者もこのような設計技法を身に付け，セキュリティシステムの設計で実践し，役立ててほしい。

問 2

問 2 では，SQL インジェクション，セキュリティ診断及び Web サイトの新しい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が，一部，正答率が非常に低い問題が見受けられた。

設問 1 は，SQL インジェクションに関する問題である。(1)と(2)は，正答率が期待よりも低かった。攻撃を受けた場合に，Web サーバのアクセスログがどのように残るかを理解しておいてほしい。

設問 2 は，Web サイトの脆弱性診断に関する問題である。(1)は，正答率が低かった。IPS や WAF が遮断するのは攻撃文字列を含む通信である。診断時には攻撃文字列と同じ文字列が送られることを理解して，解答してほしかった。(2)と(3)については，正答率は高かった。

設問 3 は，Web サイトの新しいセキュリティ対策に関する知識についての問題である。全体として正答率は低かった。(1)と(2)は，反射型の XSS と DOM ベースの XSS についての問題であったが，仕組みを正しく理解していない解答が目立った。クリックジャッキングは，数年前から問題視されてきた脆弱性であるが，対策を行っている Web サイトはまだ少ない状況である。これらの脆弱性や攻撃に関する知識を確認してほしい。