平成 22 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，開発プロジェクトにおいて安全なシステム開発のために情報セキュリティスペシャリストが支援すべきテーマについて幅広く出題した。全体として正答率は想定どおりだった。

設問 2(1)は，プロジェクトマネジメント上の問題を問うたが，手戻りがあるとだけ解答したものが散見された。プロジェクトをセキュリティ面で支援するときには，納期やコストなどの問題を考慮して解答してほしかった。

設問 2(2)は，正答率が高かった。しかし，設計工程において求められる，セキュリティ要件の実現方法を設計するという観点が漏れている解答が散見された。脆弱性対策だけではなく，開発プロジェクトにおける工程ごとに行うべき作業を幅広く理解しておいてほしい。

設問 4(1)は，正答率が低かった。アクセス権の設定についての記述がない解答が散見された。SQL インジェクションは知っているものの，データベースのアクセス権に関する知識が十分活用されていなかった結果と思われる。本設問では，問題文の状況の下でマルチテナントのシステムにおけるデータベースの分離方法をセキュリティ面から検討している。これをきっかけにデータベースのアクセス権について理解しておいてほしい。

問２

問 2 では，組織内の認証システムの統合に関する技術及び統合におけるスケジューリングについて出題した。全体として正答率は想定どおりだった。

設問 2(1)は，正答率が低かった。チャレンジレスポンス認証は，ネットワークにおける認証の基本であるので，よく理解しておいてほしい。

設問 3(1)は，正答率が低かった。セキュリティレベルの異なる部門において同じ暗号化鍵を用いることが問題であることを，旧認証システムである A-SSO システムの設計及び問題文中の状況設定から理解してほしかった。

設問 3(2)は，正答率が低かった。SAML ではドメインをまたいだ Web アプリケーションの認証に SAMLResponse メッセージを用いていることに加えて，SAMLResponse メッセージでは，暗号化とディジタル署名を用いて，セキュリティを確保していることを理解しておいてほしい。