平成 25 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 I 試験

問 1

問 1 では，クロスサイトスクリプティングについて出題した。全体として正答率は低く，広く知られた脆弱性のはずだが，正確には理解されていないようであった。

設問 1(1)では判定基準と対策との関連性について出題した。選択問題にもかかわらず，正答率が低かった。

設問 1 の(2)～(4)，設問 2(1)～(3)，(5)，(6)ではそれぞれ原因箇所，問題の種類，対策方法を出題した。原因箇所を正しく特定できると正解を導き出せる。また，原因箇所の特定ができなくても，問題文中の診断結果をよく読めば，問題の種類を特定でき，対策方法を導き出せる。これらの関係を別々に考えるのではなく，一組として理解できれば，さらに正答率が高まるはずである。

設問 2(4)では，対策に用いるメソッド名をプログラム中から読み取ることについて出題した。正答率は高かった。

設問 2(7)では，特定した原因箇所を修正することについて出題した。無解答が多かった。できるだけ修正範囲を限定した上で，プログラムを修正する能力をつけてほしい。

この問題では，IPA が公表している脆弱性対策資料を題材にした。この資料を活用して，試験だけではなく，実際のアプリケーション開発時も脆弱性への対策を正確かつ確実に実施してほしい。

問 2

問 2 では，スマートフォンアプリケーション（以下，スマホアプリという）を用いたサービスにおいてセキュリティ上考慮すべき点について出題した。全体として正答率は低かった。

設問 1 では，スマホアプリの利用者認証について出題した。(2)は選択問題にもかかわらず，正答率は低かった。暗号方式やハッシュ関数について正確に覚えておいてほしい。

設問 2 では，スマホアプリを利用したサービスにおける問題点の改善案について出題した。正答率は高かった。アドレス帳の全件データを送信しなくても要件を満たせる手段を考えれば，正解を導けるはずである。

設問 3 では，スマホアプリからのリクエストを処理する Web アプリケーションの問題点について出題した。(1)では二つのパラメタのうち“DateTime”を“AuthKey”と誤って解答した受験者が多かった。各パラメタの役割をよく理解して，正解を導いてほしかった。各パラメタの役割を理解できれば，(2)の追加する仕様として“YoyakuCode”と“AuthKey”との対応をチェックしなければならないということも導けるはずである。

今後普及が見込まれるものも含め，スマホアプリのセキュリティについては，IPA が公表している情報セキュリティ対策資料なども参考にして，体系的に学習しておいてほしい。

問 3

問 3 では，パブリッククラウドサービスの業務利用を題材に，2 要素認証の利用と事業継続について出題した。

設問 1 では，2 要素認証の利用を開始するプロセスについて出題した。2 要素認証は，パスワードだけを用いた認証に比較すると安全性を格段に高めることが可能であるが，運用が不適切であるとその目的は達成できない。2 要素認証の利用開始プロセスにおいてどのようなリスクがあるかを認識し，正しいプロセスを設計することが重要である。

設問 2 では，2 要素認証に利用している携帯電話に盗難，紛失があった際の対応について出題した。不正使用が継続してしまう理由については正答率が高かった。一方，その対策についての正答率は低く，クッキーに関する対応を答えた受験者が多く見受けられた。クッキーに関する対応では効果は限定的である。認証に利用している要素（この場合は携帯電話）の盗難・紛失に対しては，管理者が速やかに対応できるように，確実に届け出させることが必要であることを認識してほしい。

設問 3 では，パブリッククラウドサービスを用いた業務の事業継続に関して出題した。正答率は高かった。パブリッククラウドサービスを利用する際には，可用性についても検討を行い，必要な対策をあらかじめ実施することが必要であるという点については理解されていたようだ。