平成 21 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，電子メールからの情報漏えいとその対策事例における，規定とシステムの両面の改善策について出題した。全体として，正答率は想定どおりだった。

設問 2(2)は，漏えいした顧客の情報について，紛失した端末が携帯電話であるということに注意して，メールでやり取りしている価格表以外のものを解答してもらうものだったが，価格表と同類の“提案書”という解答が散見された。また，対策については，利用者の振る舞いに依存せず，漏えいした情報を短時間で特定できることが重要であることに着目してほしい。

設問 4(2)は，箇条と項番については正答率が高かった。しかし，対策については正答率が低く，だれがどのように徹底するかを記述していない解答が多かった。また，メール閲覧用の利用者 ID とパスワードを盗まれなくてもメールを閲覧されるシナリオを想起した上で対策を考えてほしい。

設問 5 は，事故の再発防止のために，規定面からの対策を問うた。5.13(2)が転送にかかわる規定なので，転送にかかわる内容を追記すべきである。

問 2

問 2 では，Java アプレットを用いたシステムを例にとり，サンドボックスに関する脆弱性とその対処方法について出題した。全体として，正答率は想定どおりだった。

設問 1 は，b の正答率が低かった。jar ファイルに対するディジタル署名の方式を問う問題であったが，誤った解答である RSA を選択する受験者が多かった。解答群の中からは，RSA と DSA の二つが候補となるが，本文中の署名の実現方式に関する記述から，DSA が正解となる。基本的な暗号技術については特徴を理解しておいてほしい。

設問 4(2)は，正答率が低かった。問題文の設定上，クライアント側とサーバ側の JRE のバージョンが異なるものとなることから，システム間の結合テストの実施を趣旨とした解答が多く見られた。問題文中の前提においては，結合テストで合格したからといって，サーバ側の JRE をバージョンアップしなくてもよいということにはならないことに注意してほしい。脆弱性の影響範囲を正確に把握して，必要かつ十分な対処の実践を期待したい。

問 3

問 3 では，IC カードを用いた認証システムのセキュリティ対策について出題した。全体として，正答率は想定どおりだった。

設問 1(1)は，正答率が低かった。IC カードのセキュリティ要件を問うたが，“偽造されていないこと”などのあいまいな解答やほかの要件と混同した解答が散見された。専門領域であるセキュリティ要件は正確に定義できてほしい。

設問 3 は，正答率が低かった。特に，設問 3(1)で問うた，PIN によるパスワードの保護について誤った解答が目立ったが，認証システムとして何を保護しなければならないかが理解できていなかったと推察される。

設問 5 は，残留リスクについては正答率が高かったものの，その低減措置については，印刷ログを取得するといった措置は通常の運用で行われているが，この問題の設定では不適切な解答が散見され，正答率は低かった。条件に応じて適切な措置が行えるような応用力を期待したい。

問4

問 4 では，社外で使用するノート PC からの情報漏えい対策について出題した。全体として，正答率は高かった。

設問 3 は，正答率が低かった。ハードディスク全体の暗号化対策について，本文中で“データの暗号化と復号を利用者に意識させることなく行う”ことを明示した上で，ノート PC のスリープ状態からの復帰にパスワードを設定しないと，だれもがスリープ状態から復帰させることができ，データが自動的に復号されるので情報漏えいにつながるという，現実に散見される問題点を問うた。“パスワード設定がないと問題である”ことを解答すればよいのだが，PC 起動時にハードディスク全体を一括で復号するという，処理能力上非現実的な仕組みを解答している受験者が少なくなかった。システムを総合的に考えた上で解答するようにしてほしい。

設問 5(1)は，正答率が高かった。ノート PC と鍵メモリを同時に持ち歩く業務がないと仮定した場合，P 社製品に優位点がある理由を問うたが，上記仮定と関係ない優位点を挙げる解答が見受けられた。セキュリティ対策においては，業務や制約条件を考慮した最適解の選定を求められる場面が多い。設定条件をよく理解して解答するようにしてほしい。

設問 5(2)は，正答率が低かった。TPM について問うたが，仕組みを理解していない誤った解答が目立った。利用が拡大しており，今後普及が見込まれるセキュリティ技術については，理解しておいてほしい。