平成 21 年度　春期　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，自営 CA を利用したシステムの構築について出題した。全体として，正答率は想定どおりだった。

設問 1 では，a，b の正答率が低かった。暗号の 2010 年問題のような安全性に関わる環境変化に起因する話題や，暗号の強度や脆弱性についてもよく理解しておいてほしい。

設問 4 は，正答率が低かった。特に電子署名について，“ 推測した秘密鍵でメール本文を暗号化する ” など，正確には理解していないと思われる解答が散見された。

設問 5 では，(3)の正答率が低かった。自営 CA を利用したシステムでは，公開鍵証明書の発行者が鍵ペアの生成も行うことがあるが，その場合のリスクやリスク対応方法についても，理解しておいてほしい。

設問 6 は，正答率が低かった。自営 CA を利用したシステムを構築する場合，想定した範囲外で公開鍵証明書が使用されたときの影響についても考慮する必要があることを，理解しておいてほしい。

問２

問 2 では，衣料小売業者における情報セキュリティの見直しを例に取り，情報セキュリティ標準の知識，セキュリティ検査や Web アプリケーションの保護の手法などについて出題した。全体として，正答率は想定どおりだった。

設問 2(1)b は正答率が低かった。事業継続計画（BCP）は，事業継続管理（BCM）の中核を成し，組織が予期せぬ災害や事故，広範囲の伝染病などに遭遇した際の対応をあらかじめ定めておくものである。BCM は国際標準化が計画されているので，今後の動向を注目しつつ理解を深めてほしい。

設問 4(1)は正答率が低く，“ 回避 ” を選んだ解答が多かった。リスク対応の観点からは，リスクの原因を排除する “ 回避 ” は題意を満たさない。同様の考えからか，(2)においては “ トランザクションログを消去する ” という誤った解答が散見された。また，前提として問題文中に “ 暗号化を施してカード番号を判読困難にすることは難しい ” と記述されているのに，“ 暗号化を施す ” という解答も多かった。問題に含まれる条件をよく吟味して解答してほしかった。

設問 5 では，ISMS の審査の意義について考察が不足している解答が見られた。ISMS の審査の目的は，組織において PDCA サイクルが有効に機能していることを確認することにある。したがって，本文中で記述した様々な管理策を実行するだけではなく，講じた管理策に対する Check と Act が必要であることについて言及してほしかった。