平成 19 年度　秋期　情報セキュリティアドミニストレータ試験　採点講評

午後 I 試験

問 1

問 1 では，暗号技術と VPN に関する基本的な知識について出題した。全体として，正答率は高かった。

設問 1 b，c は，正答率が低く，IKE と DH の役割といった，IPsec や通信セキュリティの基本知識が不足していると推察された。情報セキュリティアドミニストレータとして，基本的な知識は身に付けておいてほしい。

設問 4 (1)は，利用者の観点から解答することを求めたが，この趣旨を違えた解答が散見された。問題文のケースでの IPsec VPN は，利用者への負担が最も少なく，ほかの方式で想定される操作が必要でないものがあることを指摘してほしかった。一方，(2)は，運用管理の観点から解答することを求めており，問題文から論理的に分析する技術的な問題であるが，正答率は低かった。与えられた技術的情報を，状況に応じて，論理的に分析することを心掛けてほしい。

問 2

問 2 では，電子メール，ファックス，USB メモリなどを例にとり，情報の身近な取扱いに潜むリスクについて出題した。全体として，正答率は高かった。

設問 2 では，想定されるリスクに対する情報セキュリティ対策を，抑止，予防，検知の各視点から解答することを求めたが，それらの視点を混同している解答が見受けられた。情報セキュリティ対策を検討する際には，各視点の意味を理解した上で，それらを組み合わせる対策検討が効果的であることを理解してほしい。

設問 4 は，正答率が高く，ほぼ題意は理解されているようだが，リスク回避策ではなく，リスク移転策を記述した解答が散見された。リスク対応の選択肢である，リスク回避，リスク低減，リスク移転などの考え方について，十分に理解してほしい。

問 3

問 3 では，機密に区分される電子文書の安全な管理について出題した。全体として，正答率は低かった。

設問 1 は，選択肢問題にもかかわらず，“必要の原則（need to know）”の正答率が低かった。“必要の原則”は，セキュリティマネジメントの原則の一つであり基本的な用語なので，知っておいてほしい。

設問 3 では，“公開鍵証明書の失効と再発行”とした誤った解答が目立った。問題文中の失効や再発行の条件を読めば，事業部統合時は該当しないことがすぐに分かるはずである。

設問 4 は，予想以上に正答率が低かった。“確認”は管理の基本である。不適切な権限設定によって引き起こされる問題の真の原因は，正しく設定されているかどうかの確認がなされていなかったことであることを読み取ってもらいたい。

設問 5 では，文書ごとの共通鍵の生成，文書の暗号化，生成した共通鍵の通知，通知された共通鍵による復号という一連の流れについて出題したが，(B)の通知内容として“生成した共通鍵”を答えていない解答が目立った。受験者の知識がまだ不十分であると思われる。

問 4

問 4 では，アカウント管理を例にとり，情報セキュリティの継続的改善について出題した。全体として，正答率は低かった。

設問 3 (1)では，評価値の精度を確保するためには，評価値の算出方法に問題がないことが重要であるということを理解してほしかったが，題意を正しく理解していない解答が目立った。例えば，周知の不徹底によって評価値の算出方法がサーバ管理者ごとに異なると，評価値の精度が確保できない。定量分析の実施に当たって重要なポイントが何かということを，問題文中の背景から十分に読み取ってほしい。

設問 4 (1)では，題意は理解されているが，原因としての記述になっていない解答が散見された。問題となっている事象を記述するのではなく，その原因を考察して記述してほしい。

設問 4 (2)では，アカウント付与の承認者を変更することは理解しているが，承認者として選んだ役職には不適当な解答が散見された。社内規程の修正に当たっては，問題点を解決するという視点にとどまることなく，修正された規則の実効性が十分であるかということにも留意してほしい。