平成 20 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 II 試験

問 1

問 1 では，システムの新規開発時や更改時におけるリスクアセスメントの実施と，その結果に基づくセキュリティ要件の検討を題材に，情報セキュリティアドミニストレータに求められる知識と経験を問う出題とした。全体として，正答率は高かった。

設問 1(1)は，基本的な用語を理解していない解答が見受けられた。“検知”や“予防”は，情報セキュリティに関する基本的な用語なので，十分に理解しておいてほしい。

設問 2(2)は，正答率が比較的低かった。既に実施済の対策を記述した解答や，購買管理システムの改修を必要としない運用上の工夫を記述した解答が見受けられた。本文及び設問文をよく読んで，落ち着いて解答するよう心がけてもらいたい。

設問 4(1)は，本文中の字句を用いていない解答や，本文中の字句を用いているものの発注入力処理時に取得するログに記録すべき項目としてふさわしくない解答が見受けられた。責任追跡性を確保するためには，どのような項目をログに記録すべきかについて理解を深めてほしい。

設問 5(2)は，特権 ID の運用上の問題点をどのように解決するかについて解答を求めたが，対策の方向性は間違っていないものの，対策の内容としては不十分な解答が見受けられた。最小特権や権限分離といった考え方を十分に理解してほしい。

問 2

問 2 では，情報セキュリティインシデントへの対応に関する知識，及び対応体制の整備についての知識と経験を問う出題とした。全体として，正答率は高かった。

設問 1 イは，“フィッシングサイトへ誘導する”といった，フィッシングサイトの偽装に寄与しない動作の解答が多く，正答率が低かった。ここで問われている，既知の攻撃手法の概要は，情報セキュリティアドミニストレータがインシデント対策の立案や対策の有効性についての評価を実施する際に必要となる知識であり，ぜひ知っておいてもらいたい。

設問 4 は，電子署名や公開鍵証明書の仕組みと役割に対する理解が十分でない解答が多く，正答率が低かった。PKI において，文書の真正性や本人確認がどのような仕組みで行われることになるのか，理解しておいてほしい。

設問 5 は，問題文の状況を踏まえた解答を期待したが，(1)と(4)の正答率が低かった。(1)では，機会損失など Y 社の事情を考慮した解答が，(4)では，既に実施済の対応を無視した解答が，それぞれ少なからず見られた。いずれも，設問の趣旨を取り違えた解答であるが，問題文を読み込めば，設問の趣旨を理解できたはずである。