平成 30 年度　春期　情報セキュリティマネジメント試験　採点講評

午後試験

問 1

問 1 では，改正後の個人情報保護法の中から，情報セキュリティリーダとして留意すべき事項について出題した。

設問 1 は，b の正答率が低かった。個人情報を，本人から直接書面で取得するか，又はそれ以外の方法で取得するかによって，法が求める措置に違いがあることに留意してほしい。

設問 2 は，(2)の正答率が低かった。紛失・盗難に遭って回収できた PC を診断して，個人情報の漏えいの可能性を判定することは，説明責任を果たすためにも重要である。(1)は，漏えい自体を防ぐ対策であるのに対し，(2)は漏えいの可能性を検証するための対策であることを，正しく理解してほしい。

設問 3 は，匿名加工情報に関する出題であり，義務規定を問う(2)の正答率が低かった。自社のマーケティング分析のニーズを満たすためであっても，匿名加工情報から本人を再識別しようとする行為は禁止されている。法を順守するためにも匿名加工情報の取扱いルールを定め，外部委託先と取決めを結ぶことは，利用部門の役割である。

情報セキュリティリーダは，法の規定の理解と，個別事案への適用力を養ってほしい。

問 2

問 2 では，保険代理店で発生した内部不正事案を題材として，情報セキュリティリーダに求められる内部不正に関する基本的な知識を基に，事案について調査する能力や，事案が発生した背景・原因を分析する能力について出題した。

設問 1 は，おおむね解答できていた。

設問 2 の(1)は正答率が高く，不正のトライアングルに関してはよく理解されていた。しかし，(2)の g 及び h の正答率が低く，“組織における内部不正防止ガイドライン”で示された 10 の観点と対策，及び JIS Q 27001 附属書 A の管理策について理解を深めてほしい。

内部不正を防止するためには，技術的情報セキュリティ対策に加えて，組織の管理，人的管理，コンプライアンスなど，広範な領域についてきめ細かく対策をとる必要がある。情報セキュリティリーダには，内部不正防止に関する広範な知識と技能を身につけて，組織をリードしていくことを期待したい。

問 3

問 3 では，客先へのメール誤送信というトラブルを題材として，トラブルの根本的な原因を明らかにしながら，全社的な業務の効率化，情報セキュリティガバナンスの強化を図る能力について出題した。

設問 1 は，(1)の正答率が低かった。改正法の全面施行によって該当する規定が政令の条文から削除され，全ての事業者が個人情報保護法の適用対象となったことを，その経緯とともに理解してほしい。

設問 2 は，全体的に正答率が高く，よく理解されていた。情報セキュリティにおいても 1 件の重大な事故から会社の評判を落としてしまうだけでなく，事業継続に支障を来す場合もあるので，普段からヒヤリハット及び軽微な事故にも注意を払い，もし多いようなら対策を検討することが重要であることを理解しておいてほしい。

設問 3 は，(1)，(2)の正答率が低かった。(1)では，シャドーIT という用語だけでなく，シャドーIT がもたらす脅威についても理解しておいてほしい。(2)では，メールにおける証跡の調査方法だけに着目した解答が多く見受けられた。本文の状況設定と設問文をよく読んで解答してほしい。

情報セキュリティリーダは，トップダウン及びボトムアップの両アプローチを適宜組み合わせて，事業の目的及び戦略に合わせた情報セキュリティガバナンスの強化を図る能力を身に着けてほしい。