平成 28 年度　秋期　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，オンラインストレージサービスを例にとり，インターネット上で提供されるサービスを業務で利用する場合の課題や，事故発生時に情報セキュリティリーダが考慮すべき事項について出題した。

設問 2 は正答率が低かった。プロキシサーバを調査する目的が，今回発生した事故の原因となった PC を絞り込むことにあることを正確に理解できず，他の目的を含む選択肢を選んだ解答が多く見受けられた。

設問 3 (2) では，電子署名やハッシュ値に対する理解が不十分だと思われる解答が見受けられた。これらの技術は，ファイルの正当性や改ざんがないことを保証し，確認できるようにするためのものであり，第三者にファイルを読まれる可能性を下げるためのものではないことを理解してほしい。

設問 4 では，(4) の正答率が低かった。“オンラインストレージサービス業者との秘密保持契約見直し”を含む選択肢を選んだ解答が多く見受けられたが，今回発生した事故はオンラインストレージサービス業者からの情報流出が原因ではないことは，問題文をよく読めば分かるはずである。

インターネット上で提供されるサービスの業務利用は，今後ますます拡大すると予想される。情報セキュリティリーダは，そのような環境下でも部門の情報セキュリティを適切に管理，維持することが求められる。必要な対応を導き出す能力を身に着けてほしい。

問 2

問 2 では，従業員の外出先でのノート PC 紛失事象における情報セキュリティインシデント（以下，インシデントという）への対応について出題した。

設問 1 では，インシデント発生直後の初動対応を問うた。全体に正答率は高かった。組織が定めた初動対応の手順を，発生したインシデントに当てはめて，具体的に何をすべきかを検討する設問である。初動対応において事実関係を幅広く調査する能力を身に着けてほしい。

設問 2 では，情報セキュリティ対策の目的と効果及びインシデントの状況に応じた適切な対応を問うた。(3) は，ログの確認の目的が秘密鍵の漏えいの有無の調査にあることに着目して解答する必要があるが，正答率は平均的であり，おおむね理解されていた。(5) では，証拠保全の必要性を理解していない解答が見受けられた。

本問の解答に当たっては，まず，ノート PC の紛失から派生するリスクを想定する必要がある。その上で，実施済の情報セキュリティ対策とインシデントの状況を突き合わせて，対応を導く必要がある。情報セキュリティリーダは，業務で起こり得るインシデントを想定し，実施すべき対応を導く能力を身に着けてほしい。

問 3

問 3 では，不正プログラム感染を題材として，情報システムの利用部門における社内の関係者と協力したインシデント対応及び再発防止について出題した。

設問 1 では，インシデント発見後の初動対応について問うたが，正答率は平均的であり，おおむね理解されていた。インシデントの初動対応においては，会社の経営方針と基盤情報システム利用規程を考慮した上で，優先すべき対応を行い，状況に応じて適切な証拠保全を行うことが重要である点を理解しておいてほしい。

設問 2 は，正答率は高く，よく理解されていた。公開 Web サイトは改ざんされる可能性があり，かつ，誰もが改ざんされた公開 Web サイトを閲覧してウイルス感染の被害者になる可能性があることを理解しておいてほしい。

設問 3 では，インシデント対応を行う中で発見された課題の改善について問うたが，正答率は平均的であり，おおむね理解されていた。インシデント対応の中で発見された課題の改善だけではなく，リスクアセスメントを行い，バランスがとれた改善活動を行うことが重要であることを是非理解してほしい。

情報セキュリティリーダは，インシデント対応において，被害拡大防止及び証拠保全に適切に対応するための判断力と，再発防止のための具体策を検討する能力を身に着けてほしい。