TAC

平成28年度春期情報処理技術者試験

情報セキュリティマネジメント　講評

【午前】

午前問題 50 問の内訳をおおまかに整理すると，次のようになります。

・問 1～11　(計 11 問)

情報セキュリティ管理やリスク分析，人的セキュリティ対策など，主に組織の ISMS(情報セキュリティマネジメント)プロセスに関する出題。

JIS Q 27001/27002 や IPA“組織における内部不正防止ガイドライン”など，標準的なガイドラインに拠った出題も多く含まれていました。

・問 12～30　(計 19 問)

暗号技術や認証技術，攻撃手法と対策など，主に技術的(テクニカル)な要素に関する出題。

各種攻撃手法に関する用語の意味を問う問題が目立ちました。また，不正や漏えいを防止するための具体策について問うものも数問出題されています。

・問 31～36　(計 6 問)

各種ガイドラインや法律など，法務に関する出題。

個人情報保護法や特定電子メール法といったセキュリティ関連の法規を中心に，知的財産権や労働取引関連なども含めて，シラバス(知識細目)の中から万遍なく出題されています。

・問 37～50　(計 14 問)

システム構成や要素技術，各種マネジメント・戦略などの「その他の分野」に関する出題。

システム監査とサービスマネジメントの分野から 2～3 問ずつ，システム構成やネットワークなどのテクノロジ系からは各分野ごとに基礎的な知識問題が 1 問ずつ出題されている印象です。

重点分野であるセキュリティと法務が全体の 70%強を占め,その他の分野は 30%弱というバランスでした。次回以降に変更される可能性もありますが，まずはこの比率を意識して対策するのがよいでしょう。

出題形式としては，用語に関する知識，及び簡単な状況判断を答えさせるものが大部分で，数値の計算や図表の読取りなどの複雑な手順を必要とするものはほとんど見られませんでした。時間的な負荷は少なく，多くの受験者が時間内に余裕をもって全問に解答できたでしょう。

また，過去の既存区分の試験からの流用は，50 問中 20 問程度見られました。セキュリティ分野ではそれほど目立ちませんでしたが，「その他分野」では流用の度合いが半数程度と，かなり高めでした。

初回ということで難易度評価は困難ですが，既存の試験区分との比較も含めて

難易度 A：IT パスポート(IP)試験及び基本情報技術者(FE)試験への対策学習，
及び一般常識を活用することで平易に解答できる

難易度 B：FE 試験の視点から見て標準的

難易度 C：FE 試験の視点から見てもやや難解

という尺度で見てみると，50 問分の内訳は，おおよそ

難易度 A：40%程度　　難易度 B：45%程度　　難易度 C：15%程度

と評価できます。深い知識が要求される問題も散見されますが，平易な問題の割合も多いため，FE の対策学習を進めていた受験者であれば，合格点を獲得するのはさほど困難ではなかったと評価できます。

【午後】

午後問題3問の内容は次のようなものでした。

問1：標的型攻撃メールの脅威と対策

標的型攻撃メールの受信を発端としたマルウェア感染というインシデント事例を用いて，

・各攻撃手法の特徴に関する知識

・初動対応の問題点

・管理規定及び運用の改善点

などを考察させる問題です。

ボリュームもそれほど大きくなく，各設問で問われている内容も平易なものが多いため，短い時間で高い正答率を得られた受験者が多いと思われます。

問2：業務委託におけるアクセス制御

販売業務システムを題材に，各ロール(役割)に設定する適切なアクセス操作権限，及びユーザIDも含めた管理運用の方法を考察させる問題です。

各設問の解答に予備知識はさほど必要としませんが，代わりに登場人物や使用システム，考慮すべき方針や要求などが多数提示されているため，時間をかけて丁寧に整理・読解することが求められます。

問3：情報セキュリティ自己点検

顧客情報の扱いを題材に，各種リスクの洗出しやコントロールの評価を考察させる問題です。

CSA(統制自己評価)というやや難解な概念が登場し，その特徴を問う設問も登場します。ただし，十分に理解できていなくとも，セキュリティ監査について基礎的な理解があれば，一般常識と考え合わせて各設問に答えることは十分に可能です。

評価についての設問では，与条件から適切な評価を導くだけでなくその根拠との整合性も考察させるなど，問い方に工夫がみられます。

全体として，暗号化やセキュリティプロトコルといった技術的(テクニカル)な知識を要する部分はほとんど無く，情報セキュリティの基本的な概念をベースに与えられた条件を丁寧に読み解く読解力，分析力が重視されている問題セットだったと評価できます。テーマも「インシデント対応」「アクセス制御」「リスク分析・対応」といったように，出題が十分予想された標準的なものが並んでいました。

時間的な負担の視点で見ると，問1がかなり軽く，問2・問3が重めのバランスでした。問2・問3には1問当たり40分程度を要してしまった受験者も多かったかもしれません。

以上を考え合わせた総合的な難易度としては，FE試験の午後問題対策を行っている受験者であれば，さほど難解ではない平易な問題であり，時間配分さえしっかりできればかなりの確率で合格点に到達できたのではないかと評価できます。ただし，マネジメント系やストラテジ系の「長文読解」タイプの問題が苦手な受験者にとっては，思ったよりも手強く感じられた可能性もあります。

今回の出題傾向，問題ごとのボリュームバランスが意図的なものか，今後も継続するかは不明ですので，引き続き注視していきたいところです。

【予想配点】

〔午前〕

問 1～50：各 2 点

〔午後〕

問 1：34 点

設問１　(1)　a，b　…　各 3 点　×　2

(2)　c　…　3 点

(3)　…　4 点

(4)　…　4 点

設問２　(1)　…　4 点

(2)　d　…　3 点

(3)　e　…　3 点

(4)　f　…　4 点

(5)　…　3 点

問 2：34 点

設問１　(1)　…　3 点

(2)　…　3 点

(3)　a，b　…　各 2 点　×　2

(4)　…　3 点

(5)　…　3 点

(6)　…　3 点

設問２　(1)　c　…　3 点

(2)　d，e，f　…　各 2 点　×　3

(3)　…　3 点

(4)　…　3 点

問 3：34 点

設問１　…　4 点

設問２　…　4 点

設問３　(1)　a　…　4 点

(2)　b　…　4 点

(3)　c　…　4 点

(4)　d　…　3 点

(5)　…　3 点

設問４　(1)　e　…　4 点

(2)　f　…　4 点

（午後試験の合計は上限を 100 点とする）

以上