

**【午前】**

50問の内訳は以下のとおりであり、前回(平成28年秋期)とほぼ同様でした。数値計算などの複雑な手順を要するものが無いという傾向は従来と同様ですが、前回及び前々回と比較すると、単純な用語定義を問う問題がやや減少し、踏み込んだ知識が必要になる問題が若干増えている印象を受けます。

問1～12：組織のISMSに関する出題

問13～30：技術的(テクニカル)な要素に関する出題

問31～35：法務に関する出題

問36～50：その他の分野に関する出題

過去試験からの流用改変は50問中28問程度で、前回と比べると微増しています。その中には単純な流用ではなく、問題文の一部や選択肢を改変しているものも多く含まれていました。ISMS関連では新作が多く、技術的な要素やその他分野については流用が多いという傾向は継続しています。

難易度については、前々回 → 前回 → 今回と少しずつ上昇してきた印象です。「FE試験の対策に相当する学習を進めていけば十分に合格点を獲得できる」という基本的な評価は変わりませんが、合格をより確実にする(高得点を見込む)ためには、AP試験やSC試験で用語問題として問われているような、やや高度な内容についても触れておくことより望ましい、という見方もできます。

**【午後】**

午後問題3問の内容は次のようなものでした。インシデントへの対応を主題にした問題と、リスク分析などの計画を主題にした問題がミックスされ、全体としてはバランスのとれた内容になっています。

問1：マルウェア感染への対応

ランサムウェアに感染した事例を用いて、調査分析の考え方や企業としての対応について考察する。

問2：クラウドサービスの導入と運用

メール送受信に関するクラウドサービスの導入事例を用いて、外部サービス利用時のセキュリティ面での留意点、及び当該サービスにおけるアクセス制御(アクセス権設定)について考察する。

問3：オフィスの物理的セキュリティ

オフィスレイアウトの変更を題材に、機密性の確保手段や共連れ対策、施錠方式などを考察する。

各問とも情報量は従来どおり多めですが、各設問の内容から「どの部分の記述を重点的に考察すればよいか」が比較的分かりやすくなっており、解答に要する時間は前回よりも少なく済んだ人が多いかもしれません。

その代わり、個々の設問で問われる内容はしっかりした知識と論理的な考察を必要とするものも多く、求められるスキルのレベルは前回よりも上がった印象を受けます。“Tor(匿名ネットワーク)”や“アンチパスバック”など、FE試験でもあまり問われていない知識が必要になる設問も含まれていました。午後問題全体としての難易度は前回並みか、やや上がったと評価できるでしょう。

## 【予想配点】

[午前]

問 1～50 : 各 2 点

[午後]

問 1 : 34 点

設問 1 (1) a … 4 点

(2) 4 点

(3) 4 点

設問 2 (1) b, c … 各 3 点 × 2

(2) 4 点

設問 3 (1) 4 点 (完答)

(2) 4 点

(3) 4 点

問 2 : 34 点

設問 1 (1) a … 4 点

(2) 5 点

(3) b … 4 点

(4) c … 4 点

設問 2 (1) d ~ f … 各 4 点 × 3

(2) 5 点

問 3 : 34 点

設問 1 (1) a ~ c … 各 3 点 × 3

(2) 2 点

(3) ② ~ ⑤ … 各 2 点 × 4

設問 2 d … 3 点

設問 3 e ~ h … 各 3 点 × 4

(午後試験の合計は上限を 100 点とする)

以上

この講評の著作権は TAC(株)のものであり、無断転載・転用を禁じます。

Copyrights by TAC Co.,Ltd.2017