

平成 22 年度春 情報セキュリティスペシャリスト試験講評速報

2010,4,19 (株)アイテック 情報技術教育研究部

1. 試験全体講評

第 3 回情報セキュリティスペシャリスト試験の応募者数は 30,295 名で、第 2 回の情報セキュリティスペシャリスト試験の応募者数 (26,666 名) に比べると、13.6% と大きく増加しました。高度試験の中では最も応募者数の多い試験で、情報処理システムにおけるセキュリティの重要性が認知されていることを示しています。

午前 (共通知識) 試験は、幅広い分野からの出題であることには変わりはありません。その半面、平成 21 年度秋期の午前 試験の合格率 (36.1%) が低かったことから、全体的な難易度は、少しやさしくなったといえます。

午前 (専門知識) 試験の出題範囲は、技術要素のうち、セキュリティとネットワークが重点分野です。この 2 分野からの出題数は 20 問で前回と同じでしたが、今回は、更に、データベースからも 1 問出題されました。出題内容としては、情報セキュリティに関する個々の技術を問うものが大半を占めています。なお、問題の難易度は、ほとんどがレベル 3 と考えられ、合格基準点の 60% 以上をクリアすることは、比較的やさしいといえます。

午後 試験の出題テーマは、Java プログラミング、データの暗号化とバックアップ、転職サイトにおける個人情報保護、ウイルスの駆除及び感染防止でした。これまでの春期に実施されたテクニカルエンジニア (情報セキュリティ) 試験で出題されたような詳細な技術知識を要求されるものはあまりなく、基本的な技術知識が十分に身に付いていれば、解答できるようなレベルの問題だったと思います。その半面、穴埋め問題が減少し、記述式の問題が増加したので、思うように得点できないことが想定されます。したがって、全体的な難易度を評価すると、標準レベルといえます。

午後 試験の出題テーマは、インターネットに公開されているサーバの情報セキュリティ対策 (問 1)、情報セキュリティインシデント対応 (問 2) でした。問 1 は、DNS キャッシュポイズニングや SPF などについて理解していることが要求されますが、基本的な技術知識を十分に把握していれば、解答できるレベルです。問 2 は、情報セキュリティインシデント対応に関するものですが、記述式の小問数が多いので、正解できる小問には着実に正解し、得点を積み上げていくことが必要です。このため、問 1、問 2 とともに難易度はほぼ同じと考えられ、全体的に評価すれば、ほぼ標準レベルといえます。

2. 午前 試験 (高度試験共通) の講評

新試験制度になって 3 回目の試験実施ですが、前回の平成 21 年度秋期における高度試験午前 は午前免除対象者が受験者の半数前後いました。試験種別によって異なりますが、午前 を受験した人で合格点の 60 点以上取れた人は受験者の 4~5 割です。普段学習をしていないと簡単には 60 点を取れませんので、しっかり対策する必要があります。

共通知識として幅広い分野から 30 問が出題される午前 試験ですが、過去 2 回と同様に今回も応用情報技術者試験の 80 問からの抜粋になっていました。

出題内容に関して、前回試験では新傾向問題が増えましたが、今回はやや少なくなっています。難易度は前回に比べれば、少し易しかったといえます。

(新傾向問題)

- 問 3 整形形式の XML 文書が妥当である条件
- 問 9 経験則を基にした評価方法
- 問 14 LAN アナライザを使用するときの留意点
- 問 18 プロジェクトライフサイクルに共通する特性
- 問 20 ITIL v3 における問題管理プロセスの目標
- 問 26 企業の競争戦略におけるチャレンジャ戦略

3. 午前 試験講評

25 問のうち、分野別の出題数は、「技術要素」から 21 問、「開発技術」から 3 問、「サービスマネジメント」から 1 問という比率でした。第 2 回の出題数と比較して、技術要素が 1 問増えた関係で、サービスマネジメントが 1 問減少しました。全体的な難易度を評価すると、標準レベルといえます。

(1) 技術要素

技術要素からの出題範囲は、セキュリティ、ネットワーク、データベースの 3 分野です。分野別の出題数は、セキュリティが 17 問、ネットワークが 3 問で、データベースが 1 問です。セキュリティの 17 問のうち、15 問が情報セキュリティ技術に関するもので、情報セキュリティ管理(マネジメント系)は 2 問でした。内容的には、ハッシュ関数、デジタル証明書、ワンタイムパスワード、共通鍵の総数、ワームの侵入、ファイアウォールの設定、中間者攻撃、DKIM、SMTP-AUTH、セキュリティプロトコルなどの幅広い範囲からの出題となっており、バランスのとれた出題でした。ネットワークとデータベースの問題は、基本的な問題といえます。

(2) 開発技術

開発技術からの出題範囲は、システム開発技術とソフトウェア開発管理技術の 2 分野です。今回の出題数は、システム開発技術が 2 問、ソフトウェア開発管理技術が 1 問でした。SOA に関する問題(問 23)が、やや難という印象を受けますが、選択肢の内容を消去法によって絞っていけば正解できると思われます。

(3) サーマネジメント

サービスマネジメントからの出題範囲は、サービスマネジメントとシステム監査の 2 分野ですが、今回の出題数は、システム監査の 1 問だけでした。情報セキュリティ監査基準の位置付けに関するものが出題されましたが、これは平成 20 年度の情報セキュリティアドミニストレータ試験で出題されたものです。

4. 午後 試験講評

午後 試験は 4 問の中から 2 問の選択です。各自が得意する問題を、うまく選択できたかどうかポイントになると考えられます。また、技術的に高度の内容が問われているものは少なく、問題の記述内容や条件をうまく考慮しながら、解答を作成していくことが要求されるような問題でした。なお、各問とも、字句の穴埋め問題が減少し、数十字で解答する記述式の問題が増加した半面、問 2 や問 4 は記述式の小問数が少ないので、記述式の配点が高く設定されと考えられます。正解できる設問は、確実に得点し、ミスをしなことが 60 点をクリアするための条件といえます。

問 1 Java プログラミング

セキュアプログラミングに関する問題として、前回に引き続き Java が出題されました。これまでは、Perl、C++、Java を変更しながらの出題になっていましたので、今回は読みが外される出題となりました。なお、この問題の選択者は、Java を理解している受験者やセキュアプログラミングが得意な受験者などに限られると思われれます。こうした面を考慮し、難易度を評価すると、ほぼ標準レベルといえます。

問 2 データの暗号化とバックアップ

暗号化の基本的な考え方などを中心とした問題です。問題で提起された内容を十分に把握しながら、設問の誘導にうまく乗っていくことができれば、比較的高い得点が得られると思われれます。設問 1、設問 2 は基本的な問題なので、ほぼ全問正解できるでしょう。設問 3 の小問のうち、どれだけ正解できるかがポイントです。難易度を全体的に評価すると、比較的やさしいといえます。

問 3 転職サイトにおける個人情報保護

個人情報保護というテーマですが、パスワードの管理や設定方法に関する内容の問題です。専門知識が必要なものは、PGP における証明書のフィンガプリントを確認する小問程度です。そのほかの小問について、問題の条件を十分に確認した上で、何がセキュリティホールになっているかなどに気付けば、比較的多くの小問に対し正解を導いていくことができると思われれます。全体的な難易度は、比較的やさしいといえます。

問 4 ウイルスの駆除及び感染防止

ウイルス感染の問題は、少し考えにくいところがありますが、問題の条件を十分に確認しながら解答を作成していくことが必要です。この問題は、記述式の小問数が特に少なく、配点が高くなる可能性があります。一つの小問のミスが致命傷になるので、難易度を全体的に評価すると、標準レベルといえます。

5. 午後 試験講評

午後 試験は、問 1 がネットワークセキュリティを中心とした技術系、問 2 がマネジメント（管理）系に比重が置かれていた問題といえます。また、午後 試験では、問題の記述内容のほか、図や表で示された条件を考慮しながら、解答を作成していくことが重要です。このため、問題の条件などを十分に加味し、分かりやすい文章表現で解答を作成できたかどうかなどが、合格基準点の 60 点以上に達するかどうかの分かれ目になると考えられます。

問 1 インターネットに公開されているサーバの情報セキュリティ対策

SSH 接続、DNS キャッシュポイズニング、SPF（Sender Policy Framework）による迷惑メール対策など、最近の技術動向に関する知識が要求される問題です。しかし、個々の小問に関しては、技術的に高度な内容を求めているものはあまり多くありません。むしろ、基本的な問題や対策などを十分に把握していれば正解できるものの方が多いといえるでしょう。このため、全体的な難易度は比較的やさしいといえますが、小問数が全体的に少ないので、確実に正解できる問題にはミスをしないことが必要です。

問 2 情報セキュリティインシデント対応

情報セキュリティインシデント対応というテーマです。全体的に情報セキュリティマネジメントに関する知識が要求されるほか、ネットワークセキュリティに関する技術知識が必要な問題です。記述式の問題が多いことから、思うように得点できないことも考えられます。難易度を全体的に評価すれば、ほぼ標準レベルといえます。

以上