

4. 平成24年度春期の試験に向けて

4-1 情報セキュリティスペシャリスト試験について

インターネットの利用が、日常生活に利便をもたらした半面、ウイルス感染をはじめとし、数多くのセキュリティ問題が指摘されています。例えば、アプリケーションの多くが Web ベースのソフトウェアに移行しており、Web サーバなどの脆弱性をねらった攻撃が大きな問題になっています。こうしたセキュリティ問題に対し、適切に対応していくには、セキュリティ全般に関する技術知識が広く求められ、情報セキュリティ技術者に対する社会の期待も大きくなっています。この情報セキュリティ技術者としての実力を証明する公的な資格が、情報セキュリティスペシャリスト試験です。この資格は、ぜひ取得しておきたいものです。

参考までに、平成22年度秋期から平成23年度秋期までの受験者数、合格者数などの推移を図表13に示します。なお、合格率については、平成21年度秋期の合格率(18.5%)をピークに、その後、徐々に低下してきています。このため、情報セキュリティスペシャリスト試験を受験するに当たっては、受験対策を十分に行って試験に臨む必要があると考えられます。

年 度	応募者数	受験者数	合格者数
平成22年度秋期	28,989 (-4.3%)	19,391 (66.9%)	2,759 (14.2%)
平成23年度春期	30,704 (5.9%)	19,445 (63.3%)	2,712 (13.9%)
平成23年度秋期	26,539 (-13.6%)	17,753 (66.9%)	2,398 (13.5%)

() 内は、それぞれ対前期比増減率、受験率、合格率を示す。

図表13 応募者数・受験者数・合格者数の推移

4-2 出題予想

(1) 午前Ⅰ試験、午前Ⅱ試験

平成22年度秋期から平成23年度秋期までの3期にわたる試験から判断すると、午前試験については、次のようにいえます。まず、午前Ⅰ(共通知識)と午前Ⅱ(専門知識)を比較すると、午前Ⅰの出題範囲が広範囲にわたることなどから、合格基準点をクリアすることが難しく、午前Ⅱは、午前Ⅰがクリアできれば、その多くの受験者はクリアできるレベルのものと考えられます。ちなみに、午前

I 試験と午前II試験の合格率を比較すると、図表 14 のようになります。なお、午前I試験の合格率が、午前II試験の合格率を上回ったのは、平成 23 年度秋期が初めてです。

年 度	午前 I 試験	午前 II 試験
平成 22 年度秋期	37.1%	72.5%
平成 23 年度春期	50.4%	74.9%
平成 23 年度秋期	69.1%	67.1%

図表 14 午前 I 試験と午前 II 試験の合格率の比較

平成 23 年度秋期の午前 I 試験の合格率は、前回（平成 23 年度春期）、前々回（平成 22 年度秋期）と比較すると大きく向上しています。特に、1 年前の試験に比べると、32 ポイントも向上し、約 2 倍弱の合格率となっています。これに対し、午前II試験の合格率は、ここ 3 期の試験の合格率は、おおむね 70% 前後で推移しています。このため、平成 23 年度秋期試験で、初めて午前 I 試験の合格率が、午前II試験の合格率を上回るという結果になりました。これは、午前 I 試験から受験する必要がある受験者が、少なくとも午前 I 試験に合格し、次回の試験からは、専門分野の情報セキュリティ分野に絞った学習に専念して、次回の試験以降で合格をかち取りたいという意識などが強く働いたものと思われまます。なお、午前 I 試験の免除制度を利用できない受験者にとっては、午前 I 試験の出題範囲が極めて広範囲にわたることから、十分に準備して受験することが必要です。そこで、前述したように、初回の試験では手堅く午前 I 試験だけに合格し、2 回目以降の試験で午前II試験以降をすべて合格するという方法もよいでしょう。あるいは、午前 I 試験は免除制度がありますので、この制度を利用できるように、応用情報技術者試験に合格するか、いずれかの高度試験の午前 I 試験に合格しておくこともよいでしょう。

次に、午前 I 試験の出題分野についてです。出題分野は、テクノロジー系（基礎理論、コンピュータシステム、技術要素、開発技術）、マネジメント系（プロジェクトマネジメント、サービスマネジメント）、ストラテジ系（システム戦略、経営戦略、企業と法務）の全分野にわたりますので、幅広い分野に関する知識が要求されます。平成 22 年度秋期から平成 23 年度秋期試験までの分野別の出題数は、図表 15 に示すとおりです。なお、午前 I で出題される 30 問は、応用情報技術者

試験で出題された 80 問の中から抽出されていることが特徴です。

分野	大分類	平成 22 年 秋期	平成 23 年 春期	平成 23 年 秋期
テクノロジ系 (17 問)	基礎理論	3	3	3
	コンピュータシステム	5	5	5
	技術要素	6	6	7
	開発技術	3	3	2
マネジメント系 (5 問)	プロジェクトマネジメント	2	2	2
	サービスマネジメント	3	3	3
ストラテジ系 (8 問)	システム戦略	3	3	3
	経営戦略	3	3	3
	企業と法務	2	2	2
合計		30	30	30

図表 15 午前 I 試験 分野別出題数

図表 15 に示すように、午前 I の分野別の出題数は、テクノロジ系が 17 問、マネジメント系が 5 問、ストラテジ系が 8 問という比率で、毎回同じ比率になっています。このため、日頃から情報処理技術全般に関する知識を修得するとともに、出題数が多いテクノロジ系やストラテジ系に関連する過去問題を多く解いていくようにしましょう。しかし、午前 I の出題分野の全分野に関し時間を費やしていくことは、あまりお勧めできません。例えば、論理回路の問題などは、考え方を理解するのに少し時間がかかります。こうした問題に時間をかけても意味がありません。捨てる分野の問題を決めながら、効率的に学習していくことも必要になります。

次は、午前 II 試験です。午前 II 試験の出題数は 25 問、試験時間は 40 分です。出題の重点分野は、技術要素のうちセキュリティとネットワークです。このほかには、技術要素のうちデータベース、開発技術のうちシステム開発技術とソフトウェア開発管理技術、サービスマネジメントのうちサービスマネジメントとシステム監査の分野から出題されます。平成 22 年度秋期から平成 23 年度秋期試験までの分野別の出題数は、図表 16 に示すとおりです。

大分類	中分類	平成 22 年 秋期	平成 23 年 春期	平成 23 年 秋期
技術要素	セキュリティ	16	15	16
	ネットワーク	4	5	4
	データベース	1	1	1
開発技術	システム開発技術	1	1	1
	ソフトウェア開発管理技術	1	1	1
サービス マネジメント	サービスマネジメント	1	1	1
	システム監査	1	1	1
合 計		25	25	25

図表 16 午前Ⅱ試験 分野別出題数

午前Ⅱ試験の分野別出題数は、これまでの傾向から判断すると、セキュリティ分野とネットワーク分野とを合わせて 20 問、データベース分野が 1 問という比率になっています。このため、技術要素から 21 問、開発技術とサービスマネジメントは、それぞれ 2 問程度の出題になると考えられ、この比率が大きく変化することはないでしょう。

なお、技術要素のうちセキュリティ、ネットワークは、出題の重点分野であるほか、データベース技術を含めた技術知識については、午後試験対策を行う上で重要な位置付けにある技術知識です。このため、これらの三つの分野の技術については、十分に学習していくことが必要です。そうすれば、午前Ⅱ試験で出題される技術要素分野の問題は、ほぼ全問正解できるレベルになってくると考えられます。例えば、技術要素から 20 問出題された場合には、少なくとも 15 問以上は正解できるようになるでしょう。15 問正解できれば、合格基準点に達します。このため、午前Ⅱ試験は、特別な対策を実施する必要はなく、午後対策に必要な技術知識を十分に身に付けていくだけでよいと考えられます。

(2) 午後Ⅰ試験、午後Ⅱ試験

午後Ⅰの試験時間は 90 分で、4 問の中から 2 問を選択して解答します。選択の幅が広いので、できるだけ自分自身の得意とする分野の問題を選択していくことが必要です。また、一度選択した問題については、最後までやり抜くようにすることも必要です。それは、問題文をよく読んでいけば、問題の中にヒントが記述されていることが多く、それらを手掛かりにして正解を導いていくことが可能だ

からです。なお、ヒントを見つけることができるかどうかについては、各自が持ち合わせている知識が多いか少ないかなどの差によって決まります。

そこで、試験を受験するに当たっては、できるだけ技術レベルを向上させておく必要があります。例えば、セキュリティ技術では、Web アプリケーションなどに対するセキュアプログラミングをはじめ、メッセージ認証、本人認証、デジタル署名、電子証明書の検証方法、暗号化技術、ネットワークやデータベースに対する様々な攻撃とその対策、セキュリティプロトコル、VPN 技術、ファイアウォールの設定、IDS や IPS、迷惑メール対策など、多くの技術知識を吸収していく必要があります。また、ネットワーク技術分野では、TCP/IP (HTTP, HTTPS, IPsec, SSL など) やインターネット利用・接続技術、DNS の仕組み、電子メールの配送の仕組みなど、データベース技術分野では、データベースに対するアクセス制御、SQL 文、RDB、データベースの排他制御やリカバリなど、幅広い技術を修得していく必要があります。更に、情報セキュリティポリシーやリスク分析などのマネジメント系の問題に加えて、フィッシングやフォレンジックなど最新のトピックも含めて出題されるので、幅広く知識を吸収していく必要があります。また、JIS Q 27001 や JIS X 5070 などの標準化動向の把握も忘れないようにしましょう。

次に、午後Ⅱ試験です。試験時間は 120 分で、2 問の中から 1 問を選択して解答します。午後Ⅱは、問題分量が 10 ページ以上にわたりますので、問題をよく読んで、解答を導いていくという基本的な姿勢を貫いていくことが大切です。そうすれば、正解を導くことができる問題が必ず出てきます。情報セキュリティに関する一定の技術知識を身に付けた上で、午後Ⅱ試験では、「あわてず、あせらず、あきらめず」という精神で臨むことが必要です。

また、午後問題の特徴は、出題内容が一つの技術に絞ったものよりも、複合的な観点から出題されます。この傾向は、午後Ⅱ問題では特に顕著になります。そこで、セキュリティと、ネットワークあるいはデータベースの相互に関連した総合問題に対応できる技術力を養っていくことが必要になります。しかし、幅広いこれらの技術を十分に修得していくには、かなりの時間が必要です。試験の直前になってあせらないように、あらかじめ多くの学習時間を見込んでおき、計画的に学習していくことが必要です。また、一度、理解しても繰り返し技術知識をインプットしていかないと、すぐに忘れてしまいます。工夫をしながら継続的に学

習していく姿勢を確立するようにしましょう。なお、試験問題では、単なる技術的な知識から解答する問題はそれほど多くありません。問題文に記述された内容に従って解答する問題の方が多いので、問題の記述内容を正しく理解し、その範囲内で考えていくとよいでしょう。そのためには、問題文に記述された内容を理解できるだけの基本的な技術力をまず身に付けていくことが必要です。また、午後試験は数十字程度の記述式で解答します。記述内容については、考え方や根拠を明確に示すほか、キーワードをしっかりと押さえた解答を作成することが必要です。

以上のように、情報セキュリティスペシャリストの資格を取得するためには、それなりの努力が要求されます。したがって、この資格を保有することは、それだけ価値が高いということになります。学習計画をしっかりと立てて、試験では必ず合格するように努力していきましょう。

4-3 平成 23 年度秋期試験のデータ

(1) 午前 I の問題

共通知識として幅広い分野から 30 問が出題される午前 I 試験ですが、過去 3 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、前回試験と同様に新傾向問題の数は多くありませんでした。また、今回は計算問題や考える必要のある問題が例年よりもやや少なく、難易度は前回に比べて少しやさしかったのではないかと考えられます。なお、新傾向問題としては、次のようなものがあります。

問 17 知的財産権戦略

問 28 GPL のルールに則した対応

出題内容を見てみると、テクノロジー分野の基礎理論の問題で前回よりも細かい内容が出題されており、少し難しかったかもしれません。この分野のそれ以外の問題は、全体に用語選択と文章の正誤判定問題がほとんどで解答の絞込みもできることから、難易度は高くないと考えられます。

マネジメント系、ストラテジ系分野では、難しい問題はなく、新試験制度になってから出題された過去問題も多いので、解きやすい内容だといえます。なお、午前 I 試験が免除になっている人も、出題された内容は確認しておき、午前 I 試験で要求される知識レベルについては常に把握しておきましょう。

(2) 午前Ⅱの問題

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 2 問、「サービスマネジメント」から 2 問という比率でした。この比率は、平成 22 年度春期試験以降、同じですから、これからも変化はないと考えられます。なお、全体的な難易度を評価すると、比較的やさしいレベルといえます。

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、分野別の出題数は、セキュリティが 16 問、ネットワークが 4 問、データベースが 1 問でした。セキュリティの 16 問はすべて技術的な問題で、情報セキュリティ管理（マネジメント系）の問題はありませんでした。内容的には、DNS セキュリティ関連が 2 問、暗号認証技術が 2 問、SSL や IPsec などセキュリティプロトコル関連が 3 問、メールセキュリティが 2 問、攻撃手法や脅威に関するものが 5 問、データベースセキュリティ関連が 1 問、ウイルス対策が 1 問です。ほとんどが過去問題の再出題です。主なものとしては、22 年度春期から 6 問、21 年度春期から 2 問でした。なお、新傾向問題としては、問 7 の「IP アドレスと MAC アドレスに係る攻撃」や問 9 の「Smurf 攻撃の特徴」、問 16 の「不正にシェルスクリプトを実行させる攻撃」などがあります。ネットワーク分野は、オーソドックスな問題が出題されました。

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、それぞれ 1 問ずつ出題されました。いずれも過去問題における定番テーマですので、基本を理解していれば両問とも正解できると思われます。

サービスマネジメント

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、それぞれ 1 問ずつ出題されました。問題は、フェールソフトとリスク分析手法ですが、リスク分析の問題は、情報セキュリティ管理（マネジメント系）分野の問題ともいえます。

(3) 午後 I の問題

午後 I 試験は 4 問の中から 2 問の選択です。各自が得意とする問題を、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。また、数十字で解答する記述式の問題が大半を占めていますので、ポイントとなる記述を正確に表現することが必要です。いずれにしても、正解できそうな設問は、確実に得点し、ミスをしたことが 60 点をクリアするための条件といえます。

問 1 セキュアプログラミング

プログラミング言語として C++ と Java の二つが取り上げられました。SQL インジェクションをはじめとする定番テーマが多く、比較的取り組みやすいといえます。ただし、コード内の変数名をすべて選ばせるなど、解答方法を細かく指定している設問があり、ケアレスミスをしないように注意する必要があります。この問題の選択者は、C++ や Java を理解している受験者が中心になると考えられるので、難易度を総合的に評価すると、標準レベルといえます。

問 2 販売システムへの機能追加設計

安全なログイン処理やパスワードの初期化機能をテーマとした問題です。同様のテーマを取り上げた問題は、平成 22 年度秋期試験の午後 I 問 2 (利用者 ID のライフサイクル管理) などがありました。過去問題を十分に理解していれば、取り組みやすかったと思いますが、ログイン処理の問題は流れ図を穴埋めする形式のため、流れ図を書いたことのない受験者は戸惑ったと考えられます。なお、パスワード初期化機能の問題では、制限時間の中で問題文から関連する箇所を的確に読み取って考察することが要求されます。難易度を全体的に評価すると、やや難のレベルといえます。

問 3 プロキシ経由の Web アクセス

プロキシ経由の HTTPS 通信と、HTTPS 通信におけるサーバ証明書の検証という二つのテーマを取り上げた問題です。HTTPS とプロキシを連携させる場合の技術的特徴や課題、ブラウザによるサーバ証明書の検証処理などについての知識が要求されます。読み取り型の問題ではなく、技術的知識を前提とする考察型

問題のため、知識の有無で得点差がつくと考えられます。難易度は、標準レベルといえます。

問 4 財務報告に係る内部統制

情報セキュリティ管理に関する出題で、ISMS 管理策、USB メモリ内のデータ保護、外部委託先の内部統制の評価という三つのテーマを取り上げた問題です。ISMS 管理策については、JIS Q 27002 などの用語を解答する問題が複数あり、知識で差がつかます。技術的対策や管理的対策を解答する問題では、問題文の情報セキュリティガイドラインなどの記述を踏まえて解答することがポイントになります。難易度については、標準レベルといえます。

(4) 午後Ⅱの問題

午後Ⅱ試験は、問 1 が医療情報システムの要件定義と設計を題材とするセキュリティ設計を中心とした問題、問 2 がログ管理システムの設計を題材とする問題でした。午後Ⅱ試験に取り組むに当たっては、問題の記述内容のほか、図や表で示された条件を十分に考慮しながら、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るかどうかなどが、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 医療情報システムの要件定義と設計

設問のテーマとして、IC カードに格納する秘密鍵の保護やデジタル署名、タイムスタンプなどの技術的な内容のほかに、アクセス制御の検討、医療情報の機密性・真正性・可用性保護の考え方、非常時の業務継続や BCP に盛り込む内容の検討などが取り上げられています。デジタル署名に関する一部の設問を除いて高度な知識は要求されていません。情報セキュリティの基本的な考え方を踏まえた上で、問題文の記述に沿って、一つ一つ丹念に解答を作成していくことが求められます。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。

問2 ログ管理システムの設計

特権 ID に関連するログ管理に関する問題です。設問のテーマとしては、ログの記録項目、取得・保存方法、ログデータ量や伝送速度の計算、ログ分析方法、ログ管理の運用設計などが取り上げられています。特定領域の高度な知識が要求される問題はなく、問題文の条件を基に考察する問題がほとんどです。問1と同様に問題文の記述に沿って、一つ一つ丹念に解答を作成していくことが求められます。難易度を全体的に評価すれば、標準レベルといえます。

4-4 午前解答マークシートと、午後解答シートをダウンロードして、何度も問題を解いてみよう！

本書に収録されている問題を繰り返し解くことが、合格するための重要な学習になります。不得意分野の問題は、できるようになるまで何度も解きましょう。その際、次の方法で答案用紙を活用しましょう。

① 午前解答マークシート

午前解答マークシートを本書の巻末に収録しました。適宜、拡大コピーして活用してください。

② 午後解答シートをダウンロード

午後解答シートをアイテックのホームページ (<http://www.itec.co.jp>) からダウンロードしてみましょう。

アイテックのホームページ上部の「学習・受講中の方」をクリックし、次に「解説・解答シートダウンロード」の「詳しくはこちら」をクリックします。「解答シートダウンロード」の「徹底解説 本試験問題シリーズ」から希望する解答シートをご選択ください。

制限時間を守って解答し、解答・解説編で確認した後、巻末の「午後Ⅰ、午後Ⅱ問題 予想配点表」で、自己採点してみましょう。

午前は70%以上、午後は65%以上、正解できることを目標にしてください。