

4. 平成 24 年度秋期の試験に向けて

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 23 年度春期から平成 24 年度春期までの受験者数、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 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%)
平成 24 年度春期	29,756 (12.1%)	19,711 (66.2%)	2,707 (13.7%)

() 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 23 年度春期から平成 24 年度春期までの 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 年度秋期試験の 1 回限りです。

年 度	午前 I 試験	午前 II 試験
平成 23 年度春期	50.4%	74.9%
平成 23 年度秋期	69.1%	67.1%
平成 24 年度春期	57.1%	64.9%

図表 14 午前 I 試験と午前 II 試験の合格率の比較

平成 24 年度春期の午前 I 試験の合格率は、平成 23 年度秋期に比べると 12 ポイントも低下しましたが、同時期に実施された平成 23 年度春期に比較すると、6.7 ポイント向上しています。午前 I 試験の合格率は、最近、50%を超えるようになりましたが、以前は 40%に満たないこともありました。このため、午前 I 試験を受験する必要がある方は、図表 4 で示された、幅広い情報処理技術分野の知識を十分に把握して試験に臨むことが必要になります。なお、午前 I 試験に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という方法もあります。

午前 II 試験は、以前はおおむね 70%以上の合格率でしたが、最近、合格率の低下傾向が見られます。午前 II 試験は、過去問題から再出題される問題が多くありますが、最近の傾向として、新規の問題の出題比率が少しずつ高くなってきています。こうした要因などもあって、これまで 7 回実施された試験の中では、平成 24 年春期の 64.9%という合格率が最も低くなりました。

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 23 年度春期から平成 24 年度春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 23 年 春期	平成 23 年 秋期	平成 24 年 春期
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	7	7
	開発技術	3	2	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	2
ストラテジ系 (8 問)	システム戦略	3	3	4
	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

これまで、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でしたが、平成 24 年度春期試験でテクノロジ系が 17 問、マネジメント系が 4 問、ストラテジ系が 9 問という配分になりました。いずれにしても、午前 I 試験の出題範囲は極めて広いので、日ごろ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 23 年度春期から平成 24 年度春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 23 年 春期	平成 23 年 秋期	平成 24 年 春期
技術要素	セキュリティ	15	16	16
	ネットワーク	5	4	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 問の出題となっており、この比率は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 24 年度春期試験のデータ

(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。

高度試験共通の知識問題という位置付けから、出題される内容は特定種別に偏りのない非常にオーソドックスなものが多かったといえます。新傾向問題としては、次のような内容のものですが、出題数としては多くありませんでした。

問 4 コヒーレンシの対策が必要な書込み方式

問 15 電子メールの機密性を確保できる仕組み

問 18 EVM

問 22 災害や事故の発生後の対応

今回の午前 I 全体の傾向としては、定番問題といえるものが従来よりも少なく、次のようにやや細かい知識について問われる問題が増えていました。

問 2 パリティビットの付加で訂正できるビット数

問 5 RAID の分類方法

問 9 テクスチャマッピングの説明

問 17 モデレータが主導するレビュー技法

問 20 レプリケーションが有効な対策

問 23 情報戦略の投資対効果

(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、第 3 回（平成 22 年度春期）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、全体的な午前Ⅱ試験の難易度を評価すると、標準レベルといえます。

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 問のうち、14 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。セキュリティの新規問題としては、クリックジャッキング攻撃、サイドチャネル攻撃（タイミング攻撃）、PCI DSS、公衆無線 LAN サービスにおける不正利用、ベイジアンフィルタリング、DNS amp 攻撃が出題されていました。一方、平成 21 年度秋期から平成 22 年度秋期の過去 3 期で出題された問題の中から 9 問が出題されていたので、過去問題を十分に学習していれば、正解を得やすいといえます。

ネットワーク分野の 4 問は、いずれも基本的な問題でした。また、データベース分野では GRANT 文による権限定義の問題が出題されていましたが、標準レベルの問題です。

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 問ずつ出題されていましたが、いずれも過去問題からの再出題です。問 22（システム開発におけるアクティビティとテストの組合せ）は平成 21 年度春期、問 23（特許権の取得が可能なもの）は平成 21 年度秋期に出題されていました。

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。IT サービスマネジメントの情報セキュリティ管理プロセスと、システム監査において考慮すべき事項の問題で

すが、いずれも標準レベルの問題といえます。

(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。それぞれの問題とも、詳細な内容が問われているものが多いので、各自が得意とする問題を、うまく選択できるかどうかポイントです。その上で、問題の記述内容や条件を十分に考慮しながら、解答を作成していくことが要求されます。なお、各問とも、設問数が少ないので、1 問当たりの配点が高くなっていると想定されます。また、数十字で解答する記述式の問題が大半を占めているので、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 脆弱性検査の結果とその後の対策

Java に関するセキュアプログラミングが取り上げられていますが、主にクッキーやセッション ID、HTML の生成などに関する技術的な知識が要求される問題です。設問 1 の穴埋め問題は基本的なものですから、正解できるレベルのもので。一方、設問 2 の記述式問題は、どのような接続環境を思い浮かべるかなどによって正解できるかどうかが決まってくると考えられます。設問 3 は、JavaScript におけるエスケープ処理を行うべき文字と、置換後の文字列の知識を有しているかどうかです。なお、この問題の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 Web アプリケーションのセキュリティ対策

Web アプリケーションのセキュリティについて、SQL インジェクション、不正ログインとその対策、パスワードの格納方法などに関する問題が出題されています。表 1 の「Web サーバの HTTP アクセスログ（不正アクセスに関連する部分の抜粋）」を読み取っていけば、正解を導くことができるものもあります。また、日ごろから注意すべきセキュリティ問題に関しての知識を有しているかどうかポイントです。

問 3 保守作業の証跡確保のための対策検討

ログ管理を中心とした問題です。操作ログに対するセキュリティの問題を十分

に把握していれば、比較的取り組みやすい問題であるといえます。しかし、記述式の問題が多いことや、問題の記述内容や表1の「案1及び案2の実現方式概要」などを十分に把握することが必要であることから、思ったように得点することができないかもしれません。正解できる設問には、確実に正解し、得点を積み上げていくことが必要であるといえます。難易度を全体的に評価すれば、標準レベルといえます。

問4 情報セキュリティ技術者の育成

ウイルス感染と、IPSで異常を検出した際の対応方法などの問題です。フィッシングメールや標的型攻撃メールなどに関する知識があれば、取り組みやすい問題といえます。しかし、設問で問われていることに対し、的確に解答を作成する必要があることのほか、記述式の解答数が5問しか設定されておらず、1問当たりの配点が高いため、少しでもミスをすると、合格基準点をクリアすることが難しくなります。いずれにしても、キーワードを押さえた解答を作成できるかどうかポイントです。

(4) 午後Ⅱの問題

午後Ⅱ試験は、問1がサーバ切替え時などに発生する技術的な課題を考察する問題、問2がスマートフォンにおけるセキュリティ問題などの知識を主に問うような問題です。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。今回の午後Ⅱ試験では、問題の条件などが比較的シンプルでしたから、解答を作成しやすかったものと思われます。しかし、記述式の問題では、自分自身が意図した内容を的確に文章で表現することが難しいので、設問で問われていることを十分に考慮した上で解答を作成できるかどうかなどが、合格基準点をクリアできるかどうかの分かれ目になると考えられます。

問1 インターネット向けサーバの災害対策

穴埋め問題は、基本的な用語や問題の記述内容に従って考えるものですから、正解が得られやすいと思います。記述式の問題についても、高度な技術知識を要求されるようなものが少なく、問題の記述内容を十分に確認しながら解答を作成すれば、比較的正確な解答を導きやすいと考えられます。平成22年度春期の午後Ⅱ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) や平成 23 年度春期の午後Ⅱ問 1 (メールシステムの情報セキュリティ対策) に比較すると、取り組みやすく、比較的やさしい問題であるといえます。

問 2 社内情報システムの移行

スマートフォンやタブレット端末の利用を前提にし、クラウドコンピューティングを利用した外部のサービスを利用する場合のセキュリティ問題を考えるものです。スマートフォンと PC の連携機能、情報漏えい対策などの知識を十分に保有していること、携帯端末がウイルスに感染しやすくなる理由などを理解していることが要求されますが、全体的には問題の記述内容に従って考察し、的確に解答を作成していけるかどうかポイントになると思われます。難易度を全体的に評価すると、標準レベルといえます。

itec