

4. 平成 23 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 22 年度春期から平成 23 年度春期までの受験者数、合格者数などの推移を図表 14 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 年度春期	30,296 (13.6%)	19,951 (65.9%)	3,045 (15.3%)
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%)

() 内は、それぞれ対前期比増減率、受験率、合格率を示す。

図表 14 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 年度春期から平成 23 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。午前 I 試験と午

前Ⅱ試験の合格率を比較すると、図表 15 のようになります。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。

年 度	午前Ⅰ試験	午前Ⅱ試験
平成 22 年度春期	60.1%	69.4%
平成 22 年度秋期	37.1%	72.5%
平成 23 年度春期	50.4%	74.9%

図表 15 午前Ⅰ試験と午前Ⅱ試験の合格率の比較

平成 23 年度春期の午前Ⅰ試験の合格率は、前回（平成 22 年度秋期）と比較すると大きく向上していますが、1 年前の試験と比べると、約 10 ポイントも低下しています。これに対し、午前Ⅱ試験の合格率は、平成 22 年度春期から徐々に向上していますし、過去問題などを十分に学習しておけば、特段の対策は必要ないといえます。しかし、午前Ⅰ試験の合格率は、春期試験は比較的良い半面、秋期試験の合格率は 40% 以下という状態（平成 21 年度秋期は 36.1%）が続いていますので、平成 23 年度秋期試験は要注意であるといえます。特に、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。あるいは、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、免除制度を利用できるようにしておくといよいでしょう。

午前Ⅰ試験の出題分野は、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 年度春期から平成 23 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。

分野	大分類	平成 22 年 春期	平成 22 年 秋期	平成 23 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	7	6	6
	開発技術	2	3	3
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 16 午前 I 試験 分野別出題数

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。なお、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ようにしましょう。

次に、午前 II 試験です。出題数は 25 問、試験時間は 40 分となっています。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、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 年度春期から平成 23 年度春期試験までの分野別の出題数は、図表 17 に示すとおりです。

大分類	中分類	平成 22 年 春期	平成 22 年 秋期	平成 23 年 春期
技術要素	セキュリティ	17	16	15
	ネットワーク	3	4	5
	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 17 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、平成 22 年度春期試験における出題比率がベースになってくると考えられます。つまり、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ます。

技術要素のうちセキュリティ、ネットワークは、出題の重点分野ですから、この 2 分野からの出題数は 20 問近くなります。また、技術要素のうちセキュリティ、ネットワーク、データベースについては、午後試験対策を行う上で、必要な技術知識を十分に吸収していくことが必要になります。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きます。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。したがって、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けば十分だと考えられます。

(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」という精神で臨む必要があります。

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必要があります。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ため、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。

出題内容に関しては、平成 22 年度秋期試験と同様に新傾向問題の数は多くありませんでした。しかし、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多く、難易度は前回に比べて少し難しかったと評価していましたが、SC の受験者の合格率は前回よりも向上していました。なお、新傾向問題としては、次のようなものがあります。

問 10 マルチメディアコンテンツに関する W3C 勧告

問 14 ゼロデイ攻撃の特徴

問 25 受注管理システムの非機能要件

問 27 技術進化過程を表すもの

出題内容を見てみると、新傾向問題の内容について詳しく知らない人もいたと思われるが、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、難易度は高くはないと考えられます。その他の問題は、基本情報技術者試験や応用情報技術者試験で従来から出題されている内容でした。いずれにしても、午前 I 試験は、幅広い情報処理技術分野における基礎知識を確実に理解することが大切です。

また、マネジメント系、ストラテジ系分野では、特に難しい問題はなく、新試

験制度になってから出題された問題を理解していれば解答できる内容といえます。なお、午前Ⅰ試験免除対象になっている人も、出題された内容は確認しておき、午前Ⅰ（共通知識）で要求される知識レベルを常に維持しておきましょう。

（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、問題の難易度は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 分野です。分野別の出題数は、セキュリティが 15 問、ネットワークが 5 問、データベースが 1 問です。セキュリティの 15 問のうち、13 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、AES、EAP-TLS の認証方式、TPM、暗号アルゴリズムの危殆化、SMTP-AUTH、CRL、デジタル証明書、ウイルスの検出手法及び調査手法、通信の暗号化、メールの第三者中継、耐タンバ性などでした。暗号化や認証技術に関する出題が多かったことが特徴といえます。ネットワーク分野では、トラフィックの計算問題と、通信プロトコルで使用されるデータ形式の問題は、意外な出題であったといえます。

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。基本的な知識さえあれば、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 問ずつ出題されていました。ITIL の管理プロセスと、データ受渡しの正確性と網羅性を確保するコントロールの問題です。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。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比較的少なく、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、設問数が少ないので、1 解答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、ミスをしなことが 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

セキュアプログラミングに関する問題は、これまで Perl と Java から出題されてきましたので、今回は、順当に C++からの出題となりました。URL のパーセントエンコード、ナル文字終端、バッファオーバーフローの要因などの知識があれば、比較的取り組みやすいといえます。しかし、設問数が少ないので、ミスをすると、致命傷になると思われます。なお、この問題の選択者は、C++を理解している受験者が中心になると考えられるので、本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 ソフトウェア資産管理

問題のテーマは、ソフトウェア資産管理ですが、内容的にはソフトウェアのライセンス契約、ソフトウェアの脆弱性によるウイルス感染などを中心とした問題です。穴埋め問題については、一部、専門用語を理解していることが要求されます。また、問題の大半を占める記述式の設問は、問題文の条件をどのように考察し、それらを評価していくかがポイントになります。このため、難易度を全体的に評価すると、標準レベルといえます。

問 3 情報漏えい対策

情報漏えい対策に関する問題は、これまでも出題されていますので、比較的取り組みやすい問題であったといえます。また、問題の記述内容から何がセキュリティホールになっているかなどを見極めていけば、正解を導くことができる設問が多いと思われます。このため、難易度については、少しやさしめといえます。

問4 Webサイトのセキュリティ対策

SSHの技術的な知識、ファイアウォールのログ監視、ファイルのアクセス権限、ログインの試行回数など、幅広い分野の問題から出題されています。正解できそうな設問には、確実に解答を作成していくことが必要です。なお、難易度を全体的に評価すれば、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がメールの仕組みやウイルス対応などの情報セキュリティ技術を中心とした問題、問2が情報セキュリティ監査を中心とした問題です。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。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 メールシステムの情報セキュリティ対策

メール転送及びメーリングリストの仕組みのほか、SPF (Sender Policy Framework) などの技術知識を十分に把握しておくことが必要です。中でも、メーリングリストに関する設問が多く、問題の記述内容を十分に理解し、解答を作成していくことが求められます。なお、問題の記述内容及び図や表で示された条件を的確に把握した上で、解答を作成すれば正解を導くことができる設問が多いと思いますが、制限時間内にすべての条件を整理し、考察することができたかどうかのポイントです。難易度を全体的に評価すれば、標準レベルと想定されます。

問2 インターネットを利用したシステムの情報セキュリティ監査対応

情報セキュリティ監査に関する全般的な知識のほか、一部、Webアプリケーションに対する攻撃手法、IPS、無線LANのセキュリティに関する技術知識が必要な問題です。穴埋め問題については、比較的基本的な用語を答える問題が多いので、記述式の問題に対する解答を、問題の記述内容に従って考察し作成していくかどうかのポイントになると思われます。難易度を全体的に評価すれば、標準レベルといえます。