4．平成 25 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，実際の被害なども発生しています。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 年度秋期から平成 24 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 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%）
平成 24 年度秋期	28,188（−5.3%）	19,381（68.8%）	2,700（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 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 年度秋期から平成 24 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，

比較的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 年度秋期	69.1%	67.1%
平成 24 年度春期	57.1%	64.9%
平成 24 年度秋期	41.3%	60.6%

図表 14　午前Ⅰ試験と午前Ⅱ試験の合格率の比較

平成 24 年度秋期の午前Ⅰ試験の合格率は，平成 24 年度春期に比べると約 16 ポイント，1 年前に実施された平成 23 年度秋期に比較すると，実に約 28 ポイントも低下しています。午前Ⅰ試験の合格率は，最近，50%を超えていましたが，今回は 41.3%にすぎません。このため，午前Ⅰ試験を受験する必要のある方は，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よいでしょう。

午前Ⅱ試験は，以前はおおむね 70%以上の合格率で推移していましたが，最近，合格率がかなり低下しています。今回の合格率は 60.6%にすぎず，これまで 8 回実施された午前Ⅱ試験の中では，最も低くなりました。午前Ⅱ試験は，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いますが，出題の中心は，過去問題からの再出題です。しっかり学習すれば，午前Ⅱ試験は比較的に容易に合格できますが，その半面，あまり軽視しないようにすることも必要です。

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

午前Ⅰの分野別の出題数は，基本的にテクノロジ系が 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。唯一の例外は平成 24 年度春期試験で，そのときの配分は，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 問でした。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 年度秋期から平成 24 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 23 年 秋期	平成 24 年 春期	平成 24 年 秋期
技術要素	セキュリティ	16	16	16
	ネットワーク	4	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ことが必要です。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，ディジタル署名，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ことが必要です。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。さらに，情報セキュリティポリシ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ことが必要です。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

共通知識として出題範囲全体から 30 問がまんべんなく出題される午前Ⅰ試験ですが，従来どおり，全ての問題が応用情報技術者試験の 80 問からの抜粋になっています。高度系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いといえます。

今回出題された問題は，テクノロジ分野が 17 問，マネジメント分野が 5 問，ストラテジ分野が 8 問で，前回に比べてマネジメントが 1 問増加し，ストラテジが 1 問減っています。出題内容に関しては，応用情報技術者試験が従来よりも新傾向問題が多かった影響を受けたと思われますが，例年よりも新傾向問題が多く，例えば，次のようなものが出題されています。

問 10　データウェアハウスに業務データを書き出すツール（ETL ツール）
問 11　非同期通信技術を利用した検索候補の逐次表示（Ajax）
問 15　Web アプリケーションへの攻撃と対策
問 28　PLM の目的
問 30　国際的な標準の会計基準（IFRS）

午前Ⅰ全体の傾向としては，新傾向問題が少し増えましたが，その他の問題は定番問題といえるものがほとんどです。計算問題や用語問題，考える必要のある問題が前回（平成 24 年度春期）よりも少なくなり，文章の正誤を判断する問題

が増えました。

次に示す内容は新傾向問題以外の主な内容で，これまでも繰返し出題されています。基礎知識として確実に理解していることが求められます。

・テクノロジ分野……集合，ハミング符号，スタック，命令の並列実行，キャッシュメモリの書込み動作，稼働率の計算，主記憶管理（仮想記憶），ストアドプロシージャ，SSL 通信手順，暗号方式，分析・設計技法（決定表），著作権

・マネジメント分野……アローダイアグラム，EVM，インシデント管理，可用性管理，システム監査人の責任

・ストラテジ分野……BPO，非機能要件，RFI，競争戦略，プロダクトライフサイクル（PLM），QC 七つ道具（親和図）

（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，今後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，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，SEO（Search Engine Optimization）ポイズニング，クラウドサービス利用のための情報セキュリティマネジメントガイドライン，ダイナミックパケットフィルタリング，ポリモーフィック型ウイルス，ICMP Flood 攻撃，SSL に対するバージョンロールバック攻撃などが出題されていました。一方，直近の過去問題と全くの同一問題の出題が前回よりも減少しましたが，類題が多く出題されることに変わりはなく，過去問題を十分に学習していれば，正解が得られやすいといえます。

ネットワーク分野の 4 問のうち，3 問は基本的な問題あるいはセキュリティ関連プロトコルの問題でした。残りの 1 問は，IPv6 のサブネットに関する新規問題

でした。データベース分野の問題は，データベース更新の異常終了時の処理に関する定番問題でした。

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問ずつ出題されていました。オブジェクト指向における情報隠蔽（問 22）と特許権に関する問題（問 23）で，難易度は標準レベルといえます。

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。IT サービスマネジメントのリポジトリを構築する理由（問 24）と，システム監査の統計的サンプリングの問題（問 25）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がポイントです。また，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も必要です。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，ミスをしないことが 60 点をクリアするための条件といえます。

問1　インターネット Web サイトの刷新

ECMAScript に関するセキュアプログラミングの問題です。ただし，プログラムコードを分析するような設問はありません。マッシュアップ技術を利用する Web サービスにおける脅威とセキュリティ対策の知識が必要です。マッシュアップ関連のセキュリティについては，IPA のセキュアプログラミング講座でも解説されています。事前に学習をして試験に臨んだ受験者の方は，比較的解答しやすかったと考えられます。また，設問2では SSL のクライアント認証に関する知識が必要です。問1は，解答数が少ないので，穴埋め問題でも配点が高くなるので，

ミスをしないことが必要です。

問２　ログの管理

ログ管理をテーマとする情報セキュリティ管理分野の問題です。設問 2 のモニタリングを周知する目的や，モニタリング条件を開示しない理由を問う問題は，情報セキュリティ管理の一般的な考え方を知っていると解答しやすいといえます。そのほかの多くは，前提知識が不要で，問題文の記述から考察する問題です。したがって，時間が十分にあれば正答できるはずですが，制限時間内で問題文をいかに正確に読み取れるかがポイントになりそうです。

問３　標的型攻撃メールへの対応

平成 24 年度春期試験に続き，標的型攻撃への対応が出題されました。設問 1 と設問 2 は，メールヘッダの分析や SPF の詳細を問うメールセキュリティ分野の問題ですから，技術的な知識が必要です。設問 3 は，最近のサイバー攻撃に対する出口対策の考え方と，ファイアウォールや IDS に関する基本的な知識を応用させる問題です。設問 3 の記述式問題は，問題文の記述から解答を特定しますので，設問の主旨を的確に押さえて，問題文の記述を踏まえて解答することがポイントです。正確な技術知識が要求される分だけ，難度は少し高いといえるでしょう。

問４　情報セキュリティインシデント対応

インシデント対応をテーマとして，LB や IDS，FW，Web サーバにおける複数のログに関して，インシデントの分析やログ管理の暫定対策，恒久対策を考察する問題です。通信の制御や監視に関する基本的な知識のほか，図や表で示された条件を的確に読み取っていく必要があります。問題文の記述から解答を特定できる設問が多いので，解答を導きやすいといえますが，どれだけ問題文を正確に読み取れるかがポイントになりそうです。

(4)　午後Ⅱの問題

午後Ⅱ試験は，問 1 が複数の Web サイトにおける脆弱性対応を技術面，管理面から考察する問題，問 2 が無線 LAN のセキュリティに関する脆弱性や対策を技術面，管理面から考察する問題です。技術的な問題では，知識が問われるもの

もありますが，多くの問題は本文の記述内容のほか，図や表で示された条件から解答を作成していきます。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　Web サイトの診断と対策

大きなテーマは二つです。一つ目は，Web アプリケーションシステムにおける脆弱性に対する分析や対応を問う技術的な問題です。二つ目は，脆弱性情報の収集や修正プログラムの適用などに関するマネジメント系の問題です。技術的な問題では，特に XSS（クロスサイトスクリプティング）の知識が必要です。セッション固定化攻撃は，午後問題で本格的には初登場ですが，問題文の説明から考察可能になっています。また，多くの問題は XSS に関する問題です。問題文に HTTP のメッセージが多く示されていますので，マネジメント系を得意とする受験者には，問題文が難しく見えたと思われます。その半面，Web サイトの構築を経験している受験者にとっては，比較的やさしかったかもしれません。

問２　無線 LAN の構築

無線 LAN を中心とするネットワークセキュリティ分野の問題です。テクニカル系の問題では，MAC アドレスフィルタリングや，SSID のステルス化，WPA2 など，無線 LAN のセキュリティに関する知識が必要です。そのほか，ファイアウォールの設定や OS のネットワーク設定を問う問題では，問題文の記述を基に考察します。マネジメント系の問題では，従業員の退職時などにおける事前共有鍵の扱い，私物の機器を利用するときのセキュリティ対策への影響，ネットワーク接続ポリシに抵触する事項などに関する問題が出題されています。基本的な問題が多いので，無線 LAN に関する知識を保有していれば，合格基準点をクリアすることは比較的容易かもしれません。