4．平成 26 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 24 年度秋期から平成 25 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，徐々に低下していましたが，平成 22 年度秋期試験以来，久々に 14%台の合格率になりました。情報セキュリティスペシャリスト試験で合格を目指すには，午後試験をクリアする必要がありますので，受験対策を十分に行って試験に臨むことが大切です。

年　度	応募者数	受験者数	合格者数
平成 24 年度秋期	28,188（-5.3%）	19,381（68.8%）	2,700（13.9%）
平成 25 年度春期	28,930　（2.6%）	19,013（65.7%）	2,490（13.1%）
平成 25 年度秋期	27,522（-4.9%）	17,892（65.0%）	2,657（14.9%）

（　）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 24 年度秋期から平成 25 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 24 年度秋期	41.3%	60.6%
平成 25 年度春期	48.7%	66.9%
平成 25 年度秋期	54.1%	78.0%

図表 14　午前Ⅰ試験と午前Ⅱ試験の合格率の比較

平成 25 年度秋期の午前Ⅰ試験の合格率は，平成 25 年度春期に比べると約 5 ポイント，1 年前に実施された平成 24 年度秋期に比較すると約 13 ポイントも向上しています。午前Ⅰ試験の合格率は，変動幅が大きいことが特徴ですが，今回の 54.1%という数字自体は決して高いものではありません。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試験の合格率は，このところ 60%台で推移していましたが，今回の試験では，久々に 78.0%という高い合格率になりました。午前Ⅱ試験の出題内容は，過去問題からの再出題が多いので，しっかり学習すれば，午前Ⅱ試験は比較的容易に合格できると考えられます。しかし，平成 21 年度春期の 88.8%や，平成 21 年度秋期の 81.4%には及びませんので，初めて情報セキュリティスペシャリスト試験を受験される方は，あまり軽視しないようにしましょう。

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 24 年度秋期から平成 25 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 24 年 秋期	平成 25 年 春期	平成 25 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	3	3
ストラテジ系 （8 問）	システム戦略	3	3	2
	経営戦略	3	3	4
	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。情報処理技術分野の知識だけではなく，プロジェクトマネジメントやシステム戦略，経営戦略などの知識も要求されます。このため，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。なお，平成 25 年 10 月に IPA（独立行政法人 情報処理推進機構）から情報処理技術者試験の出題構成の見直しが発表されました。それによると，「情報セキュリティ」に関する出題の強化・拡充が実施されますので，情報セキュリティ分野の問題が現行の 3 問から 4 問に増える可能性はあります。

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 24 年度秋期から平成 25 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 24 年秋期	平成 25 年春期	平成 25 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。しかし，前述したように，情報処理技術者試験の出題構成の見直しを受け，セキュリティ分野の出題数が 17 ないしは 18 問に増え，その分，ネットワークあるいはデータベースの問題が減少する可能性があります。

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 21 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方が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，3 問の中から 2 問を選択して解答します。平成 25 年度秋期の午後Ⅰ試験では，3 問のうち，2 問がセキュアプログラミングや HTML（XML）に関連する知識が要求される問題でしたから，セキュアプログラミングの問題を選択対象から外して準備した受験者は苦戦を強いられたと思われます。このため，できるだけセキュアプログラミング関連の知識を身に付けておくことが必要となってきています。このほか，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が必要です。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。しかし，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 25 年度秋期試験のデータ

(1)　午前Ⅰの問題

共通知識として出題範囲の全分野から 30 問が出題される午前Ⅰ試験ですが，出題分野の内訳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，ここ数回同じ内訳です。

従来どおり，30 問全てが同時期に実施された応用情報技術者試験 80 問からの抜粋になっています。前回の試験では，この 80 問からやや難しめの問題を選んでいる傾向があり難易度も高かったのですが，今回は基本的な問題が選ばれていて，全体に解きやすかったといえます。

今回の試験で新傾向といえる問題は例年より少なく，次の 2 問でした。

問 23　IT ポートフォリオの説明

問 27　プロダクトイノベーションの例

問題の出題形式としては，文章問題が半数の 15 問（前回と同じ），用語問題が 6 問（前回よりも 1 問増），計算問題が 4 問（前回よりも 1 問増），考察問題が 5 問（前回より 2 問減）でした。前回と比べて考察問題が減っており，その分，解きやすかったと思います。難易度としては前回よりもやや易しくなったといえるでしょう。

高度情報処理技術者の午前 I 試験は出題範囲が広い中からの 30 問なので，対策としては日ごろから基本情報から応用情報技術者試験レベルの問題を少しずつ解いて基礎知識を維持することが大切です。

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……桁落ち，ハッシュ関数，流れ図の穴埋め，キャッシュメモリの平均アクセス時間，フェールセーフ，稼働率の比較，ガーベジコレクション，DRAM の特徴，ストアドプロシージャ，データの正規化，サブネットマスク，TCP/IP プロトコル（UDP），ディジタル署名，情報セキュリティ基本方針，E-R 図

・マネジメント分野……リスク転嫁，ミッションクリティカルシステム

・ストラテジ分野……IT ポートフォリオ，業務のあるべき姿，デルファイ法，マーケティング要素 4P，EDI の情報表現規約，減価償却，著作権法

(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。全体的な難易度を評価すると，新規問題が少なめで過去問題からの出題が多くあったことから，難易度は少し易化したといえます。

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，今回は 16 問全て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）に分類されるものはありませんでした。

セキュリティの新規問題としては，RLO（Right-to-Left Override）を利用した手口，JVN（Japan Vulnerability Notes）などで採用されている CVE（Common Vulnerabilities and Exposures）の識別子の説明，hosts ファイルの確認事項などが出題されました。しかし，多くの問題が，平成 22 年度春期から平成 24 年度春期までの本試験で出題されたものの再出題ですから，過去問題を十分に学習していれば，難なく正解が得られると思います。

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が，TCP のサブミッションポートの説明は新規問題です。また，データベース分野では，分散データベースシステムにおける分割に対する透過性が出題されていましたが，標準レベルの問題といえます。

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。いずれも標準レベルの問題といえます。

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 問ずつ出題されていました。問 24（問題管理プロセスにおけるプロアクティブな活動），問 25（SaaS のアクセスコントロールを評価する対象の ID）は，いずれも新傾向の問題で，用語の知識や考察力を求められるものです。

(3) 午後 I の問題

平成 25 年度秋期の午後 I 試験から，出題数が 4 問から 3 問に減り，その中から 2 問を選択して解答する形式に変更されました。セキュアプログラミングの問題を選択対象外として臨んだ受験者は，自動的に問 2 と問 3 を選択せざるを得なく，思わぬ苦戦を強いられたのではないでしょうか。また，問 3 は設問数が少なかったので，これも苦戦の原因になったものと思われます。なお，午後 I 試験で

は，問題の記述内容や条件を考慮しながら，解答を作成していくことが基本となっています。このため，考察型の設問では，問題文をよく読み取って，設問で問われていることに的確に解答することができたかどうかが，合格基準点をクリアするポイントになると考えられます。

問１　Web システムのクロスサイトスクリプティング対策

セキュアプログラミングの問題で，プログラミング言語は Java です。クロスサイトスクリプティング（XSS）対策がテーマですから，XSS に関する脅威の概要とセキュアコーディングの知識が必要です。セキュアコーディングの知識があり，過去問題を演習した受験者にとっては，標準レベルの問題といえます。

問２　スマートフォンアプリケーション

設問１と設問２は，端末（スマートフォン）の認証に関する問題です。内容的には認証強度の考察や鍵への攻撃に関することが問われていますが，問題の記述内容に基づいて解答を考えることが必要です。なお，鍵付きハッシュ関数については用語の知識が必要です。これに対し，設問３は，スマホアプリケーションにおいて不正に情報を取得する手口と，その対策を考察する問題ですから，得点差が生じやすいと思われます。難易度を全体的に評価すると，やや難といえます。

問３　パブリッククラウドサービスの安全な利用

設問１と設問２は，クラウドサービスの利用において，認証機構の脆弱性と認証を強化する方法を検討する問題です。クッキーに関する知識が必要ですが，難易度は標準レベルといえます。設問３は，クラウドサービス停止時の事業継続方法を考察する問題で，事業継続の一般的な考え方が必要です。難易度を全体的に評価すると，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がインシデント対応としての調査やネットワークセキュリティ分野の様々な技術的内容を考察する問題，問２がリモートアクセス環境におけるリスクと対策を検討する問題です。今回の午後Ⅱ問題は，いずれもネットワークセキュリティに関する知識が要求され，出題内容としては，少し偏ったものになったといえます。なお，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大切です。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ことなどから，設問で問われていることを十分に理解した上で解答を作成していくことが重要になってきます。

問１　マルウェア感染への対策

マルウェア感染の検知を契機とするインシデントの初期対応の目的や行動の問題点，調査における留意点，メールヘッダの分析，ログの調査，LAN における通信の盗聴，セキュリティ対策としてのソフトウェアのアップデート，マルウェアからの外部への通信の監視や防御，PC クライアントへの対策内容など，様々な観点からの問題が出題されています。前半の設問は，問題の記述内容に従って考察すれば，解答を作成しやすいと思われます。後半の設問では，ネットワークセキュリティのほか，修正パッチを適用する際に事前に確認することが必要となるものや，APT などの攻撃に関する対策についての基本的な知識を把握していれば，解答を導きやすいといえます。

問２　スマートフォンを利用したリモートアクセス環境

スマートフォンによる許可していないアクセス方法，盗難紛失時の問題，ファイアウォールのルール，自社で管理できる対策の範囲，スマートフォンのデータ消去に関する制約，利用手続の見直し，セキュリティの監視，従業員の同意書の内容などの問題が出題されています。リモートアクセスに関する技術知識を有していれば，取り組みやすい問題です。また，設問２や設問３は，情報セキュリティマネジメント系の問題といえますが，問題の記述内容に従って解答していくことがポイントです。特に，設問３のスマートフォン利用に当たって，従業員から事前に得ておく同意内容については，基本的な事項となっているものです。