4．平成 27 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狙った攻撃や，電子メールを利用した標的型攻撃など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 25 年度秋期から平成 26 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 年度秋期試験の合格率（18.5%）をピークに，その後，徐々に低下し，平成 25 年度春期試験の 13.1%で底打ち状態となりました。その後 2 期連続で 14%台の合格率になりましたが，平成 26 年度秋期試験では，再び 13%台に低下しました。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，午後試験で合格基準点をクリアすることが必要ですから，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 25 年度秋期	27,522（-4.9%）	17,892（65.0%）	2,657（14.9%）
平成 26 年度春期	27,246（-1.0%）	17,644（64.8%）	2,543（14.4%）
平成 26 年度秋期	27,735（1.8%）	18,460（66.6%）	2,528（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 25 年度秋期から平成 26 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 25 年度秋期	54.1%	78.0%
平成 26 年度春期	62.0%	73.6%
平成 26 年度秋期	56.2%	65.0%

図表 14　午前Ⅰ試験と午前Ⅱ試験の合格率の比較

平成 26 年度秋期の午前Ⅰ試験の合格率は，平成 26 年度春期に比べると約 6 ポイント低下した半面，1 年前に実施された平成 25 年度秋期に比較すると約 2 ポイント向上しています。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 56.2%という数字自体は決して高いものとはいえません。このため，午前Ⅰ試験を受験する必要のある方は，図表 4 で示した，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，平成 23 年度秋期試験以降，60%台で推移していましたが，平成 25 年度秋期と平成 26 年度春期の 2 期連続で，70%を超えました。しかし，平成 26 年度秋期試験では，再び 60%台に低下しました。これは，平成 26 年度秋期試験では，過去問題のうちレベル 4 の問題が多く選ばれていたこと，セキュリティ分野以外の分野で新規問題が出題されたことなどの要因によるものと考えられます。しかし，午前Ⅱ試験の出題内容は，過去問題からの再出題が多いことが特徴ですから，過去問題を中心に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。とはいっても，平成 21 年度春期の 88.8%や，平成 21 年度秋期の 81.4%には及ばないので，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 25 年度秋期から平成 26 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試験で出題される 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 25 年秋期	平成 26 年春期	平成 26 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	4	4
	技術要素	7	8	8
	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	2	3	3
	経営戦略	4	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試験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，「情報セキュリティ」に関する出題の強化・拡充が実施された結果，情報セキュリティ

分野の問題は 3 問から 4 問に増加しています。

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 25 年度秋期から平成 26 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 25 年秋期	平成 26 年春期	平成 26 年秋期
技術要素	セキュリティ	16	17	17
	ネットワーク	4	3	3
	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 1 問増加し，その分，ネットワークの問題が減少していますので，次回の試験以降は，平成 26 年度春期試験の出題数がベースになるでしょう。

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おくこと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 26 年度秋期の午後Ⅰ試験は，平成 26 年度春期と同じように，セキュアプログラミングに関する問題は 3 問中 1 問だけでしたが，平成 25 年度秋期試験のように，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が出題されることもあります。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であるといえます。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おけ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ス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 26 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。

今回の試験は，平成 25 年 10 月に発表された“セキュリティ分野の出題強化”の方針で行われた 2 回目の試験で，午前 I 試験でのセキュリティ問題の出題数は 4 問で前回と同じでした。

出題された問題は，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。

今回の試験で新傾向問題といえるものとしては，次の問題がありました。

問 6　Linux カーネルの説明

問 15　WPA2 で利用される暗号化アルゴリズム

問 21　目標復旧時点（RPO）を定めているもの

問 27　コア技術の事例

問題の出題形式としては，文章問題が 16 問（前回 21 問），用語問題が 5 問（前回 2 問），計算問題が 4 問（前回 2 問），考察問題が 5 問（前回と同じ）で，前回と比べて文章問題が減り，用語問題と計算問題が増えています。基礎理論とセキュリティの問題でやや難しい問題があったため，全体としては少し難しく感じられた問題だったといえます。

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，基本情報技術者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，新傾向問題以外の主な内容を示します。定番問題もありますが，下線を引いた問題は高度午前 I 試験ではあまり出題されていない内容です。これらの問題は解答に少し時間がかかるので，基礎知識を確実に理解しておく必要があります。

・テクノロジ分野……カルノー図，M/M/1 待ち行列モデル，グラフの最短所要時間，ライトバック方式のキャッシュ，稼働率の計算，フリップフロップ回路，コードの桁数計算，関係の候補キー，通信プロトコル，サブネットワーク，SMTP-AUTH，DNS キャッシュポイズニング，セキュリティ上の脅威と対策，ブラックボックステスト，著作権帰属先の記載がない契約

・マネジメント分野……構成管理の対象，ファストトラッキング，SLA の記載内容，在庫データの網羅性チェック

・ストラテジ分野……バランススコアカード，SOA の説明，請負型契約，リードタイムの短縮，コンカレントエンジニアリング，問題解決のための図，不正競争防止法

(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。なお，全体的な難易度を評価すると，前回（平成 26 年度春期）よりも少し難しかったといえるでしょう。それは，セキュリティ分野の新規問題の出題が減少した半面，レベル 4 に相当する過去問題が再出題されたことや，その他の分野では，そのほとんどが新規問題であったからです。

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 17 問，ネットワークが 3 問，データベースが 1 問でした。次回以降の試験も，この出題比率がベースになっていくものと考えられます。

セキュリティ分野の 17 問のうち，15 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。新規問題は，ハッシュ関数の衝突発見困難性（問 2），キャッシュポイズニング攻撃への対策（問 9），サイドチャネル攻撃の説明（問 13），認証にクライアント証明書を用いるプロトコル（問 16）の 4 問でした。これに対し，過去問題からの出題は，平成 25 年度春期から 6 問，平成 24 年度秋期から 4 問，平成 24 年度春期から 1 問，その他から 2 問が出題されていました。

ネットワーク分野の 3 問は，新規問題が 2 問，平成 24 年度秋期の過去問題が 1 問という内訳でした。新規問題のうち，電子メールで，ヘッダと本体を区別する方法（問 20）はレベル 4 の問題といえます。また，データベース分野では，トランザクションの待ちグラフ（問 21）が新傾向問題として出題されましたが，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。いずれも新規問題です。コンテンツの不正な複製を防止する方式の DTCP-IP の説明（問 23）は，DTCP-IP とは何かを知っている必要があります。

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。サービスマネジメントの問 24（JIS Q 20000-1 で定義されるインシデント）は新規問題ですが，システム監査の問題は，最近の午前 I 試験に出題されたことのあるものでした。

(3) 午後 I の問題

午後 I 試験は，3 問の中から 2 問を選択して解答します。このため，セキュアプログラミング問題を選択対象外として臨んだ受験者は，問 2 と問 3 を自動的に選択することになったと思われます。いずれの問題も，問題文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必要です。制限時間の中で，どこまで記述内容を理解して，要点をまとめて文章化できたかどうかが 60 点をクリアするためのポイントになると思われます。なお，これまでの午後 I 試験では，毎回，設問数が極端に少ない問題が見られましたが，今回の試験では，全ての問題とも多くの設問が設定されていました。このため，正解できそうな設問は必ず正解し，着実に点数を積み上げていくことが必要ですが，設問数の少ない問題は，一つ答えられないものがあると，大きく点数を失いますので，問題の出題傾向としては望ましい方向に改善されていると評価できます。

問 1　スマートフォン

セキュアプログラミングと端末管理に関する問題で，プログラミング言語は前回（平成 26 年度春期試験）から連続して C++です。バッファオーバフロー攻撃が主なテーマですが，バッファオーバフローに関する脅威の概要と防御技術に関する知識のほか，スマホアプリの特性などの知識が必要です。セキュアプログラミング技術のほか，スマホアプリに関する脆弱性問題も出題されていますので，難易度的には，やや難の問題といえます。

問 2　代理店販売支援システム

SSL クライアント認証を使用する端末認証に関する問題です。暗号アルゴリズムの強度に関する考察，端末廃棄時における処理，証明書の新規発行手順，利用停止手順，更新手順などを考察するものが出題されています。特定の前提知識は不要ですが, 証明書や SSL クライアント認証の特徴を把握できていると解答しや

すかったと思われます。難易度はやや易しめといえます。

問３　マルウェア感染への対応

マルウェア感染への対応に関する問題で，通信の制御方法のほか，OS がパスワードを格納する方法に関するものなどが出題されています。具体的には，マルウェアの入口対策として送信元を詐称したメールをフィルタリングする方法のほか，バックドア通信を遮断する方法，マルウェアから内部サーバへの不正アクセスを軽減させるためのフィルタリングルール，ハッシュ化したパスワードに関する扱いなどの問題が出題されました。過去問題の類題を演習した受験者にとっては，取り組みやすい問題だったといえます。

(4)　午後Ⅱの問題

午後Ⅱ試験は，問 1 が ID 管理システムと認証システムの様々な技術的課題を考察する問題，問 2 が Web サイトの脆弱性診断と対策を検討する問題です。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。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　利用者 ID 管理システム及び認証システムの設計

利用者 ID 管理システム及び認証システムの設計をテーマとしており，複雑な図を多く用いて問題が展開されています。このため，問題を一見すると，難度の高い問題に思えますが，表 1（N 社の各地域における利用者認証方式の概要）をしっかり押さえた上で，それぞれの設問に取り組んでいけば，解答作成に必要なキーワードは問題文に記述されているので，正解を導きやすい問題といえます。なお，問題文を読みこなしても，少し考える必要がある設問は，設問 5 (2)及び(3)に限られるので,合格基準点をクリアすることは比較的容易であると思われます。

問２　Web サイトのセキュリティ

Web サイトのセキュリティに関する技術的な内容を主体とした問題です。具体的には，SQL インジェクション攻撃のログの分析と対策，Web サイトの診断ガ

イドラインの考察や診断の目的，DOM（Document Object Model）ベースの XSS の対策，クリックジャッキングの対策，HSTS（HTTP Strict Transport Security）の使用時において利用者が注意すべき事項や中間者攻撃を受ける状況などの問題が出題されています。DOM ベースの XSS などは，これまでセキュアプログラミング問題で出題されてきた内容ですが，問 1 を断念し，問 2 を選択した受験者もいたと想定されることなどから，難しく感じた受験者も少なからずいたと思われます。設問 1 (1)と(2)をスムーズにクリアできれば，後続の設問も順調に正解できると思われますが，難易度を全体的に評価すると，やや難しめの問題といえます。