4．平成 27 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，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 26 年度春期から平成 27 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 年度秋期試験の合格率（18.5%）をピークに，その後，徐々に低下し，最近では，おおむね 13%台ないしは 14%台で推移しています。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 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%）
平成 27 年度春期	27,339（-1.4%）	18,052（66.0%）	2,623（14.5%）

（　）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 26 年度春期から平成 27 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，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 回しかありません。

年　度	午前Ⅰ試験	午前Ⅱ試験
平成 26 年度春期	62.0%	73.6%
平成 26 年度秋期	56.2%	65.0%
平成 27 年度春期	59.6%	61.4%

図表 14　午前Ⅰ試験と午前Ⅱ試験の合格率の比較

平成 27 年度春期の午前Ⅰ試験の合格率は，平成 26 年度秋期に比べると約 3 ポイント向上した半面，1 年前に実施された平成 26 年度春期に比較すると約 2 ポイント低下しています。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 59.6%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，平成 27 年度春期試験では 61.4%と，平成 24 年度秋期の 60.6%に次ぐ低さでした。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 26 年度春期から平成 27 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 26 年春期	平成 26 年秋期	平成 27 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	4	4	4
	技術要素	8	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	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 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数は 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 26 年度春期から平成 27 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 26 年春期	平成 26 年秋期	平成 27 年春期
技術要素	セキュリティ	17	17	17
	ネットワーク	3	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，ネットワーク分野の問題が減少しています。これからの試験では，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。最近の傾向としては，3 問のうち，1 問はセキュアプログラミングに関する問題が出題されます。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いえますが，問題を解くレベルまで到達するには，相当の時間と努力が要求されます。問題選択に当たっては，あらかじめセキュアプログラミングに関する問題を選択するかどうかを決めておくとよいでしょう。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 27 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 年の 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 3 回目の試験で，午前試験でのセキュリティ問題の出題数は 3 回連続で 4 問あり，ほぼ定着していると考えられます。

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。なお，新傾向問題といえるものとしては次の問題があり，前回より増えています。

問 5　物理サーバのスケールアウト
問 8　拡張現実の例
問 13　JIS Q 31000 における残留リスクの定義
問 14　NIST 定義によるクラウドサービスモデル
問 25　IT 投資ポートフォリオの目的
問 26　コモディティ化の説明

問題の出題形式としては，文章問題が 19 問（前回 16 問），用語問題が 3 問（前回 5 問），計算問題が 6 問（前回 4 問），考察問題が 2 問（前回 5 問）で，前回と比べて用語問題と考察問題が減り，計算問題と文章問題が増えています。出題内容としては基礎理論の計算問題がやや難しく，その他の分野もこれまであまり出題されていない内容が幾つかあったため，全体として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……待ち行列（平均待ち時間），確率の計算，ハッシュ関数，スーパスカラ，ラウンドロビン方式，3 入力多数決回路，トランザクションの原子性，CSMA/CD 方式，回線のビット誤り率，パスワードの総数，ディレクトリトラバーサル攻撃，品質副特性における信頼性，エクストリームプログラミング
・マネジメント分野……所要日数を短縮する施策，リスク対応戦略の転嫁，可用

性と信頼性の KPI，エディットバリデーションチェック，バックアップデータ
・ストラテジ分野……情報戦略の投資効果，エンタープライズアーキテクチャ，プロセスイノベーション，EDI の情報表現規約，ロットの品質と合格率の関係，開発委託における著作権の帰属

(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，新規問題の出題数が平成 26 年度秋期試験よりも 1 問増加しましたが，レベル 4 に相当する問題が減少したことなどから，難易度は前回並みといえます。

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 17 問，ネットワークが 3 問，データベースが 1 問でした。この比率は，平成 26 年度春期試験から同じです。

セキュリティ分野の 17 問は，全て情報セキュリティ技術に関するものでした。新規問題は，Organization Name に記載されるもの（問 1），VA の役割（問 4），CRYPTREC 暗号リストの説明（問 8），NTP サーバの踏み台攻撃に対する対策（問 10），ダークネット（問 11），DNSSEC で実現できること（問 14）の 6 問です。これに対し，過去問題からの出題は，平成 25 年度秋期から 6 問のほか，平成 25 年度春期，平成 24 年度秋期，平成 24 年度春期，平成 23 年度春期，平成 22 年度春期からそれぞれ 1 問ずつで，3 期前に当たる平成 25 年度秋期からの出題数が最も多かったことが特徴ですが，過去問題を十分に学習していれば，正解が得られるものが多かったと思います。

ネットワーク分野の 3 問は，以前に出題された過去問題から 2 問と，新規問題として HTTP のヘッダ部で指定するもの（問 20）が出題されていました。いずれも基本的な問題ですから，3 問とも正解できるレベルと思われます。また，データベース分野では分散トランザクション処理で利用される 2 相コミットプロトコルが出題されていましたが，これも基本的な問題といえます。

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が，マッシュアップの例（問23）は平成25年度秋期の応用情報技術者試験で出題された問題です。

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。データセンタにおけるコールドアイルの説明（問24）は新規問題でしたが，標準レベルの問題といえます。また，正確性・網羅性を確保するコントロール（問25）は，平成23年度春期試験で出題された問題です。

（3） 午後Ⅰの問題

午後Ⅰ試験は3問の中から2問を選択します。どの問題も，詳細な知識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になると考えられます。今回の試験では，Webサイトのセキュリティに関する問題が1問だけでしたので，問題選択はスムーズに行われたものと思われます。その一方，各問とも，記述式の設問数が比較的多かったので，記述内容や条件をうまく考慮しながら解答を作成できたかどうか，あるいはポイントとなるキーワードを的確に指摘しているかどうかなどがポイントになってきます。いずれにしても，正解できそうな設問に対しては，確実に得点し，ミスをしないことが合格基準点の60点をクリアするための条件といえます。なお，問3は比較的，解答数が少なかったので，一つ答えられないものがあると，大きく点数を失うので，注意が必要であったと思われます。

問1　Webサイトの脆弱性と対策

Webサイトの脆弱性と対策というテーマですが，出題内容としてはWebサイトで行うセッション管理や，クッキーのsecure属性などに関する基本的な問題が出題されています。これらの知識に加え，URLエンコードの仕組み，HTTPヘッダインジェクションの内容を理解していれば，多くの設問に正解することができると思われます。これまでのセキュアプログラミングを主体とした問題に比べ

ると，プログラミングの専門知識を必要としない分だけ取組みやすい問題です。問題の難易度としては，やや易しいレベルといえます。

問２　情報漏えいインシデントの調査

情報漏えいインシデントの調査というテーマですが，マルウェアに感染する契機，マルウェア感染を防ぐための詳細な知識が必要とされます。また，問題文の量は 7 ページに達しているので，図表類を含め，問題の条件を正確に確認するだけでも大変な作業になります。また，一部専門的な知識を要求される設問もありましたので，難易度を全体的に評価すると，やや難のレベルといえます。

問３　パスワードへの攻撃

パスワード破りとそれに対応する方法などに関する問題です。平成 26 年度秋期試験で出題されたソルトを用いる効果の問題が出題されていますので，取組みやすいと思われます。しかし，今回は，ソルトを用いることによって防ぐことができる攻撃方法が問われていますので，注意が必要です。このほか，問題の条件を確認しながら，丁寧に問題に取り組んでいくことが必要です。難易度を全体的に評価すると，標準レベルの問題といえます。

(4)　午後Ⅱの問題

午後Ⅱ試験は，問 1 が DNS サーバやメールサーバのウイルス対策，プロキシサーバにおける URL フィルタリング，PC のウイルス感染対策などに関する問題，問 2 がマルウェア感染を防止するために必要となる対策やセキュリティポリシなどに関する問題でした。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。特に，問 1 は，問題全文が 13 ページにわたるほか，問題の条件などが少し複雑でしたから，安易に解答を作成しないことが必要です。いずれにしても，記述式の問題では，自分自身が意図した内容を採点者に分かってもらえるように的確に表現することが難しいので，設問で問われていることに対して必要なキーワードを押さえた答案になっているかどうかなどが，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　ウイルス対策

問１の出題内容は，DNS，SMTP，HTTP などのネットワークセキュリティに関する技術知識から答えるものと，問題の記述内容及び図表類で設定された条件を考慮しながら必要となるセキュリティ対策を考察するものとに大別されます。ネットワークセキュリティについて一定の技術知識を習得していれば，技術系の問題の多くに正解することはできますが，設問の多くは記述式の問題となっています。このため，設問で問われていることを表面的にとらえるのではなく，問題の記述内容や図表類に示された条件に従って論理的に考えていくことが必要です。問題の条件が少し複雑に絡み合っていますので，何がポイントになっているかをしっかりと見極めることが必要です。

問２　製造業におけるネットワーク構築

問２は，マルウェア感染を防止するために必要となる情報セキュリティ対策に関する問題です。ネットワークを物理的に分割することによってマルウェア感染を食い止めることができるかどうかを考察するもの，パスワード管理における基本的な知識，クライアント証明書に関する知識問題などが出題されています。問題の条件があまり複雑でないことから，問題文からマルウェアが感染していく方法を的確に把握していけば，正解を導き出すことは比較的容易であると考えられます。