3. 平成 28 年度春期の試験に向けて

3-1　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 年度秋期から平成 27 年度秋期までの受験者数，合格者数などの推移を図表 10 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%台で推移してきましたが，平成 27 年度秋期試験の合格率は，久々に 16.6%という高いものとなりました。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%）
平成 27 年度秋期	28,274（3.4%）	18,930（67.0%）	3,111（16.6%）

（　）内は，それぞれ対前期比増減率，受験率，合格率を示す。

図表 10　応募者数・受験者数・合格者数の推移

3-2　出題予想

(1)　午前Ⅰ試験，午前Ⅱ試験

平成 26 年度秋期から平成 27 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 11 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 年度秋期	56.2%	65.0%
平成 27 年度春期	59.6%	61.4%
平成 27 年度秋期	51.2%	81.0%

図表 11　午前Ⅰ試験と午前Ⅱ試験の合格率の比較

平成 27 年度秋期の午前Ⅰ試験の合格率は，平成 27 年度春期に比べると 8 ポイント以上も低下し，1 年前に実施された平成 26 年度秋期に比較しても 5 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 51.2%という数字は，最近の試験ではかなり低い結果に終わったといえます。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 年度秋期試験と平成 27 年度春期の 2 期連続で 60%台に低下しましたが，今回の試験では，合格率が 81.0%と一気に跳ね上がりました。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。平成 27 年度秋期試験では，3 期前に行われた平成 26 年度春期試験の問題が 7 問出題されていたことなどから，合格率が向上したと考えられます。つまり，これまでは 3 期前に行われた試験の問題（平成 28 年度春期試験では平成 26 年度秋期試験の問題）だけを重点的に学習していれば合格基準点をクリアすることは

容易でしたが，このパターンが変更されると，合格率は低下する可能性があります。このため，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 年度秋期から平成 27 年度秋期試験までの分野別の出題数は，図表 12 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 年秋期	平成 27 年春期	平成 27 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	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 12　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 年度秋期から平成 27 年度秋期試験までの分野別の出題数は，図表 13 に示すとおりです。

大分類	中分類	平成 26 年 秋期	平成 27 年 春期	平成 27 年 秋期
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 13　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，TLS/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。

3-3　平成 27 年度秋期試験のデータ

(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 問が出題される試験です。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。また，出題された問題は，従来どおり全て同時期に実施された応用情報技術者試験 80 問から選択された問題になっています。

平成 26 年春期試験から重点的に出題されているセキュリティ分野の問題はこれまでと同様に 4 問でしたが，法規分野でサイバーセキュリティ基本法が出題されているため，5 問の出題があったと考えることができます。

今回の試験で新傾向問題といえるものとしては,次のような問題がありました。

・問 9　ディジタルハイビジョン対応の映像圧縮符号化方式
・問 25　環境ガイドラインによる環境表示
・問 26　M&A による垂直統合
・問 30　サイバーセキュリティ基本法の対象

問題の出題形式としては，文章問題が 16 問（前回 19 問），用語問題が 6 問（前回 3 問），計算問題が 2 問（前回 6 問），考察問題が 6 問（前回 2 問）で，前回と比べて文章問題と計算問題が減り，用語問題と考察問題が増えています。出題内容としては最近の傾向として基礎理論の問題がやや難しく，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……集合の包含関係，パリティチェック，ハッシュ関数の衝突，並列処理方式，クラスタリングシステム，デマンドページング方式（仮想記憶），分周期の値，コード設計，DB の障害回復，伝送時間計算，公開鍵暗号方式，

ゼロデイ攻撃，ブルートフォース攻撃，ペネトレーションテスト，DFD のデータストア，共通フレーム

・マネジメント分野……EVM の管理対象，日程管理，問題管理プロセス，予備調査で実施する作業，受注伝票の監査手続

・ストラテジ分野……情報システム全体の最適化目標，RFI，デルファイ法，意思決定

出題される内容は，過去に何度も出題されている基本的な問題が大半を占めます。高度系試験で専門分野の力を発揮するのは午前Ⅱ試験からになりますが，午前Ⅰ試験はそのための“入場券に当たる”ので，試験対策としては，過去の応用情報技術者の午前試験問題を解き，7 割以上正解できるよう確実に実力を付けてください。

(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 27 年度春期）とほぼ同レベルといえますが，過去問題の比率が高かったことから十分に学習し試験に臨んでいれば，前回の合格率を上回ると思われます。

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。次回以降の試験も，この出題比率は維持され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，ステートフルインスペクション方式のファイアウォール（問 3），IT セキュリティ評価及び認証制度の説明（問 6），水飲み場型攻撃の手口（問 8），不正のトライアングルの構成要素（問 9），OAuth 2.0 の動作（問 17）の 5 問でした。これに対し，過去問題からの出題は，平成 26 年度春期から 7 問，平成 25 年度秋期，平成 25 年度春期，平成 24 年度秋期，平成 23 年度春期，平成 21 年度秋期からそれぞ

れ 1 問の出題となっています。

ネットワーク分野の 3 問は，新規問題が 1 問，過去問題が 2 問という内訳でした。新規問題の，TFTP の特徴（問 20）は馴染みが少ないプロトコルと思われるので，レベル 4 の問題といってもよいでしょう。また，データベース分野では，データウェアハウスの構築に必要な処理（問 21）が新規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 問ずつ出題されました。いずれも，平成 24 年度秋期試験の過去問題でした。

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。入出力データの管理方針（問 24），システム監査における監査証拠（問 25）は，いずれも新規問題ですが，レベル 3 の問題といえます。

(3) 午後 I の問題

午後 I 試験は，3 問の中から 2 問を選択して解答します。問 1 と問 3 は，その内容から Web サーバソフトに携わっている受験者にとって，取組みやすい問題であったといえます。その半面，Web サーバソフトについて，あまり経験のない受験者にとっては，問 2 を選択したものの，問 1 と問 3 の選択に迷ってしまい，時間に追われた受験者も多かったものと想定されます。

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，問題の記述内容をどこまで理解して，要点をまとめて文章化できたかどうかが 60 点をクリアするポイントになったと思われます。

問 1　ソフトウェアの脆弱性への対応

2014 年に大きな話題になった，オープンソースソフトウェアの Web アプリケーションフレームワークの Struts の脆弱性への対応を題材とした問題です。情報

セキュリティの 3 要素で重視するもの，攻撃手法の理解，WAF の方式検討やルール設計，動作検証，誤検知に関する用語などが出題されました。WAF のルール設計については，正規表現の知識が必要です。難易度は，標準レベルといえます。

問２　特権 ID の管理

システム保守の外部委託先の技術者による顧客情報の不正持出し対策を題材とした問題です。特権 ID を管理するツールの運用の考察，サーバへのアクセス者の特定に関する考察，ファイアウォールの設定見直し，不正操作の検知に関する考察，資産管理に関する考察などが出題されました。アクセス者を特定できない理由を答える設問は，過去に類題がありましたが，やや難しめだったかもしれません。全体の難易度は，標準レベルといえます。

問３　Web サイトにおけるインシデント対応

取引先に対して公開している Web サイトにおける，不正侵入のインシデント対応を題材とした問題です。侵入順序の考察，アクセスログに基づく攻撃の考察，ファイアウォールのフィルタリングルールの見直し，各種の対策が防止する攻撃に関する考察などが出題されました。サーバのアクセス制御の対策によって防御する攻撃内容を答える問題は，やや難しめだったかもしれません。全体の難易度は，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 がマルウェア対策の様々な設計案を考察する問題，問 2 がデータの暗号化方式などを考察する問題です。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　シンクライアント技術を利用したマルウェア対策

標的型攻撃におけるマルウェア対策を題材として，業務で必要な通信の考察，

マルウェアによる通信や動作の考察，ファイアウォールで禁止しているマルウェア通信，業務要件を踏まえたシステム設計案の考察，回線速度の計算，セキュリティ監査などが出題されました。複数の設計案と業務要件及びマルウェアの動作を総合的に考察して，解答としてまとめることが求められています。ネットワーク系の出題が目立ちますが，標的型攻撃対策の問題は８回連続の出題であることから，取組みやすかった方が多かったと思われます。難易度は，標準レベルといえます。

問２　データの取扱い

クラウドベースのオンラインストレージサービスの利用を題材として，サービスの利用方法の見直しや追加する機能の考察，関連法規，ブロック暗号アルゴリズムの考察，フォルダの暗号方式の考察，パスワード強度の計算，ファイルのマルウェア感染への対策の考察などが出題されました。パスワードの強度については，午後Ⅰ試験と合わせて３回連続の出題でした。暗号化に関する設問が目立つため，暗号技術が得意な受験者が積極的に選択したと思われます。逆に，暗号技術が苦手な受験者は，苦戦したと思われます。難易度は，標準レベルといえます。