3．平成 28 年度秋期の試験に向けて

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社会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試験が，情報セキュリティスペシャリスト試験です。

平成 28 年の第 190 回通常国会において，情報処理安全確保支援士に関する法律が成立し，平成 29 年 4 月から情報処理安全確保支援士の新しい試験が開始される予定になっています。これまでの情報セキュリティスペシャリスト試験は，経済産業大臣が認定する国家試験でしたが，情報処理安全確保支援士試験に合格すると，国家資格として正式に認められることになります。なお，情報セキュリティスペシャリスト試験の他，情報セキュリティアドミニストレータ試験，テクニカルエンジニアリング（情報セキュリティ）試験の合格者は，情報処理安全確保支援士となる資格を有する者とみなす予定になっていますので，所定の手続によって情報処理安全確保支援士になることができます。また，情報処理安全確保支援士試験は，情報セキュリティスペシャリスト試験をベースに新設することが検討されていますので，試験の名称にこだわることなく，1 期でも早く試験に合格するよう着実に準備を進めましょう。

参考までに，平成 27 年度春期から平成 28 年度春期までの受験者数，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，おおむね 13%台ないしは 14%台で推移してきましたが，平成 28 年度春期試験の合格率は，平成 27 年度秋期試験に続き 16.5%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 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%）	3,141（16.6%）
平成 28 年度春期	26,864（-5.0%）	18,143（67.5%）	2,988（16.5%）

（ ）内は，それぞれ対前期比増減率，受験率，合格率を示す。

図表 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 27 年度春期から平成 28 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試験の合格率を示すと，図表 11 のようになりますが，平成 28 年度春期試験では，午前Ⅰ試験と午前Ⅱ試験の合格率の差が，ほとんどなかったことが特徴といえます。

年　度	午前Ⅰ試験	午前Ⅱ試験
平成 27 年度春期	59.6%	61.4%
平成 27 年度秋期	51.2%	81.0%
平成 28 年度春期	65.8%	66.6%

図表 11　午前Ⅰ試験と午前Ⅱ試験の合格率の比較

平成 28 年度春期の午前Ⅰ試験の合格率は，平成 27 年度秋期に比べると約 15 ポイント向上し，1 年前に実施された平成 27 年度春期に比較しても 6 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 65.8%という数字は，最近の試験ではかなり良い結果でした。しかし，午前Ⅰ試験の合格率は，これまでの傾向から判断すると，かなり低い状態にあります。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です。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 26 年度秋期試験と平成 27 年度春期試験の 2 期連続で 60%台でしたが，平成 27 年度秋期試験では 81.0%と一気に跳ね上がりました。しかし，今回の平成 28 年度春期試験では，66.6%へと急激に低下しました。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していれば，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 28 年度春期試験では，3 期前に行われた平成 26 年度秋期試験の問題が 7 問出題されていたのもかかわらず，新規問題が前回の平成 27 度秋期試験より 2 問増加し，しかもレベル 4 に相当する問題が増えたことなどから，合格率が大きく低下する結果となりました。午前Ⅱ試験の対策としては，これまで 3 期前に行われた試験の問題（平成 28 年度秋期試験では平成 27 年度春期試験の問題）だけを重点的に学習しておくことが有効でしたが，新規問題が増加したり，レベル 4 の出題数が増加したりすると，合格率は低下する傾向が見られます。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 27 年度春期から平成 28 年度春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。

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

分　野	大分類	平成 27 年 春期	平成 27 年 秋期	平成 28 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	1
	サービスマネジメント	3	3	4
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

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。この他には，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 27 年度春期から平成 28 年度春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。

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。

大分類	中分類	平成 27 年 春期	平成 27 年 秋期	平成 28 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 13　午前Ⅱ試験　分野別出題数

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他，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。この他，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 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他，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 28 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，ここ数回同じ出題数です。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今回もこれまでと同じ 4 問で定着したといえます。

今回の試験で新傾向問題といえるものは例年よりも少なく，次の 2 問でした。

・問 5　ライブマイグレーションの概念
・問 21　クラウドサービス上の情報消失の予防に関するチェックポイント

問題の出題形式としては，文章の正誤問題が 19 問（前回 16 問），用語問題が 5 問（前回 6 問），計算問題が 2 問（前回 2 問），考察問題が 4 問（前回 6 問）で，前回と比べて文章の正誤問題が増え，考察問題が減っています。出題内容としては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。これは，ここ数回の傾向といえます。

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……26 進数，メッセージ符号化，流れ図の並列処理，SIMD，仮想記憶方式，DRAM，利用者の満足度，参照制約，トランザクションログ，スイッチングハブ，共通鍵暗号方式，WAF，Web ブラウザへの送信対策，IaaS，ソフトウェア品質特性，モジュール結合度
・マネジメント分野……工数見積り，サービスレベル管理，構成管理の導入メリット，監査手続
・ストラテジ分野……IT 投資評価，SOA，ビジネスプロセスを表記する UML 図法，チャレンジャ戦略，マーケティング要素 4C，製品開発のスピードアップ手法，ワーク・ライフ・バランス，個人情報保護法

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試験の午前問題を解き，余裕をもたせて 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，今後も変更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 年度秋期）と比較して，新規問題が前回より 2 問増加し，しかもレベル 4 に相当する問題が増えたことから，少し難しくなったといえます。このため，前回のような高い合格率（81.0%）になることはないと思われます。

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，攻撃者がサービス不能にしようとする標的（問 2），エクスプロイトコードに該当するもの（問 6），暗号の処理によって出力可能なもの（問 9），サイバー情報共有イニシアティブの説明（問 10），情報セキュリティリスクに関する定義（問 11），DNS キャッシュポイズニング攻撃の対策（問 12），電子メール暗号化プロトコルの組合せ（問 17）の 7 問でした。これに対し，過去問題からの出題は，平成 26 年度秋期から 7 問，平成 26 年度春期，平成 25 年度秋期，平成 24 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，DHCP メッセージの順序（問 19）は，DHCP メッセージの詳細を理解していることが必要ですから，レベル 4 の問題といえます。また，データベース分野では，不正アクセスを実行する入力パラメタ（問 21）が新規問題として出題されましたが，SQL 文の動作を理解していれば正解できるものです。

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，レベル 3 の標準的な問題といえます。

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 問ずつ出題されました。IT サービスマネジメントの情報セキュリティ管理プロセス（問 24），システム管理基準（問 25）のいずれも，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 問の選択です。Web システムに関連する問題は，問 1 に限られていましたので，全体としてバランスのとれた出題であったといえ

ます。また，詳細な知識を要求される問題が少なかったことから，基本的な知識を十分に身に付けて試験に臨んだ受験者にとっては有利だったと思われます。そして，それぞれの問題に丁寧に取り組んでいけば，比較的容易に合格基準点をクリアできると考えられます。しかしながら，各問題とも小問数が，これまでの試験に比べると少なかったことから，1 小問当たりの配点が高くなり，一つのミスが致命傷になる可能性があります。いずれにしても，午後問題に取り組む際には，問題文の記述内容や条件を考慮するとともに，設問で問われていることを確認しながら，解答を作成していくことが大切です。

問1　Web システムの開発

Web システムの画面遷移において発生する，クロスサイトスクリプティング（XSS）脆弱性とクロスサイトリクエストフォージェリ（CSRF）脆弱性に関するオーソドックスな問題です。Java や HTML などをよく知っている受験者にとっては，少し易しいレベルといえますが，その他の受験者にとっても，Web システムがもつ脆弱性などについて日ごろから十分に学習していれば，合格基準点をクリアできる点数を獲得することはそれほど難しいという訳ではありません。

問2　DMZ 上の機器の情報セキュリティ対策

DNS のセキュリティ及び迷惑メール対策の問題ですが，出題の比重は電子メールに関する知識に置かれています。電子メールのセキュリティなどについては，受験対策を十分に行っている方が多いと想定されますので，取組みやすい問題だったといえます。設問の中で，気を付ける必要があるものは設問 4 です。これは，問題を読んで安易に考えてしまうと，間違いやすいので，どのような電子メールが対象になるかをよく考える必要があります。全体の難易度を評価すると，少し易しいレベルといえます。

問3　スマートフォンアプリケーションの試験

問題のテーマはスマートフォンアプリケーションの試験となっていますが，出題の中心は，サーバ証明書の検証に関するものです。サーバ証明書の検証については，十分に学習されていると思いますので，解答を作成しやすかったのではないでしょうか。ただし，設問 1 の空欄 c に入れる字句は，サーバ証明書の有効期間を確認するには，有効期間の終了に設定する日付に注意することが必要です。

また，合格基準点をクリアできるかどうかは，設問 2 (1)の空欄 e ～ g のうち，幾つ正解できるかどうかがポイントになりそうです。全体の難易度を評価すると，少し易しいレベルといえます。

(4) 午後Ⅱの問題

午後Ⅱ試験は，問 1 が CSIRT 構築とセキュリティ設計，問 2 がテレワークのセキュリティというテーマですが，いずれもマルウェア感染にどのように対応していくかという観点からの出題となっています。問 1，問 2 とも，問題全文が 12 ページにわたっていますので，問題の記述内容はもちろんのこと，図や表で示された条件をよく確認し，的を射た解答を作成していくことが必要です。また，午後Ⅰ試験と同様に，これまでの試験と比較して，小問数が少なかったことから，1 小問当たりの配点が高くなり，一つのミスが致命傷になる可能性があります。記述式の問題は，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よく確認し，丁寧に解答を作成していくことを心掛けるようにしましょう。

問 1　CSIRT 構築とセキュリティ設計

本問では，インシデントの発生を契機として，社内に CSIRT の専門チームを構成する際に必要となる事項やその目的，脆弱性情報ハンドリングにおいて，各情報機器の構成管理情報を活用することによる効果，各部署との連携方法などが出題されています。リバースブルートフォース攻撃の検知方法を除き，前提知識が必要な問題はほとんどないので，問題の記述内容に照らし合わせて，丁寧に解答を作成していくとよいでしょう。なお，共通脆弱性評価システム（CVSS）に関する設問がありましたが，問題の条件を的確に考慮すれば，正解できるものです。全体の難易度を評価すると，少し易しいレベルといえます。

問 2　テレワークのセキュリティ

本問は，モバイル PC がマルウェアに感染したという事例を題材にして，侵入経路と被害状況などの調査と，未知のマルウェア対策を検討する問題です。未知のマルウェア対策では，VDI（仮想デスクトップ環境）の利用が検討対象になっていますので，VDI に関する知識があれば，取組みやすいといえます。なお，VDI については，平成 25 年度春期試験の午後Ⅰ問 3 として出題されたことがありま

すので，この内容を十分に把握していた受験者は有利だったと思われます。いずれにしても，問題の記述内容に照らし合わせて，丁寧に解答を作成していくことが必要です。VDI に関する知識が要求される分だけ，難度は問 1 より高く，全体の難易度を評価すると，標準レベルの問題といえます。

iTEC