# 4．平成 21 年度秋期の試験に向けて

## 4-1　新試験について

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開発に移行しており，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 21 年度春期の受験者数，合格者数などを掲載します。

| 年　度 | 応募者数 | 受験者数 | 合格者数（合格率） |
|---|---|---|---|
| 平成 21 年春 | 25,377 | 16,094 | 2,580（16.0%） |

**図表 15　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 21 年度春期の試験結果から判断すると，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から，合格基準点をクリアすることが比較的難しく，午前Ⅱは，午後Ⅰがクリアできれば，その多くの受験者はクリアできるレベルものと考えられます。また，午前Ⅰで出題された 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ます。

こうしたことから，午前Ⅰ対策については，手を抜くことはできません。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。日頃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，関連する過去問を多く解いていくようにしましょう。しかし

ながら，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，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ようにしましょう。

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，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，システム監査の分野から出題されます。21 年度春期の出題数は，技術要素が 17 問，開発技術とサービスマネジメントが，それぞれ 4 問ずつです。技術要素のうちセキュリティ，ネットワーク，データベースについては，午後試験対策を行ううえで，必要な技術知識を吸収していく必要があります。午後試験対策が十分に実施できれば，ほぼ全問正解できるレベルになってきます。少なくとも 13 問は正解できますので，残りの 2 問以上を，開発技術とサービスマネジメント分野の計 8 問の中から正解すれば，合格基準点に達します。したがって，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つけていけば十分だと考えられます。

### (2) 午後Ⅰ試験，午後Ⅱ試験

午後Ⅰ試験の試験時間は 90 分で，4 問の中から 2 問選択して解答します。21 年度春期の出題内容は，それぞれの問題ごとに難易度の差があったように思われます。しかし，問題間における難易度の差については，個々の受験者が持ち合わせている技術レベルの差によるところも大きいので，できるだけ自分自身の得意とする分野の問題を選択していくことが必要です。また，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も必要です。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も多く，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。なお，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，試験を受験するにあっては，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さまざまな攻撃とその対策，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，SQL 文，RDB，データベースに対するアクセス制御方式，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。

午後Ⅱ試験の試験時間は 120 分で，2 問の中から 1 問選択して解答します。21 年度春期の午後Ⅱ試験は，問題の難易度が少しやさしかったので，次回の試験では難度が少し高くなるかもしれません。また，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も大切です。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つけていれば，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。

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，幅が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してください。なお，試験問題では，たん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ほうが多いので，問題で記述された内容を正しく理解し，その範囲内で考えていくようにしましょう。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つ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ようにしましょう。

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，次回の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 21 年度春期の試験のデータ

平成 21 年度春期に実施された情報セキュリティスペシャリスト試験を分析します。

### (1)　午前Ⅰ問題

新しい試験制度では，高度区分の試験は共通知識として午前Ⅰの 30 問，専門知識としての午前Ⅱの 25 問に分けて実施されることになりました。午前Ⅰ試験は，高度区分の試験すべて同じ共通の問題になります。受験者の IT 関連の基礎知識の理解度を評価するのに加えて，高度系の受験者にどのような知識を理解しておいてほしいかを示す指針にもなるため，その意味でも，どのような問題が出題されるか興味が持たれていました。

| 大分類 | 分類名 | 問題数 |
|---|---|---|
| 1 | 基礎理論 | 4 |
| 2 | コンピュータシステム | 4 |
| 3 | 技術要素 | 7 |
| 4 | 開発技術 | 2 |
| 5 | プロジェクトマネジメント | 2 |
| 6 | サービスマネジメント | 3 |
| 7 | システム戦略 | 3 |
| 8 | 経営戦略 | 3 |
| 9 | 企業と法務 | 2 |
| 合計 | | 30 |

**図表 16　高度午前Ⅰ試験　大分類別出題数**

出題比率について，初回はまんべんなく出題されると予想していましたが，基

礎理論が多めに出題され，開発技術は予想よりも少ない出題比率でした。技術要素の大分類には，ヒューマンインタフェース，マルチメディア，データベース，ネットワーク，セキュリティなど盛りだくさんの内容があるので，出題数が多いのは予想されていました。

出題内容については，すべての問題が応用情報技術者の試験問題と重複しており，レベル 3 の高度午前 I 対策は応用情報技術者試験の午前分野の内容を学習すればよいといえます。また，30 問のうち過去問が 18 問で 6 割あり，新試験といっても従来から出題されている良問を多く解くことが，従来と同様に有効といえます。

新試験では午前試験の出題分野が IT 全体に広がったため，例えばコンピュータ科学などの知識を含む基礎理論はマネジメント系や戦略系業務の人には難しく，逆にシステム・経営戦略や企業と法務といった問題は技術系の人には難しかったと思われます。

今回，出題された問題の中で，新傾向といえるもの，まだ定番になっていないものを挙げると次のとおりですが，初回としては予想よりも出題数が少なかったといえます。

問 7　代表的なオープンソースソフトウェア

問 9　パンくずリストと呼ばれる情報を表示する目的

問 11　概念データモデルの解釈（UML 記法）

問 15　不正侵入のための経路（バックドア）

問 27　TLO の説明

高度試験の午前 I は合否に関係なく，6 割正解できれば以降 2 年間の午前 I 試験の受験が免除されるという非常に便利な制度になりましたので，今回の午前 I 試験で 6 割正解できなかった人は，レベル 3 対応の午前試験用教材（アイテックの総合コースに付いているテキスト）で確実に内容を理解しておきましょう。

今回の出題内容から判断して，今後の午前 I 対策としては次の事項を学習しておくことをお勧めします。

・オープンソースソフトウェア（OSS）

・UML

・ISMS 適合性評価制度

・CMMI

・SLA

・共通フレーム

なお，プロジェクトマネジメント，サービスマネジメント分野の項目は，出題範囲を見るとそれぞれ，PMBOK，ITIL(v2)ベースになっていますが，直接的な出題は今回ありませんでした。今後はこれらの内容も出題されるようになると予想します。

個々の出題内容を見ると，専門外の内容は難しいものもありますが，過去問が6 割あったこともあり，全体としては難しい問題は少なく，予想されたよりも解きやすかったと思われます。

### (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 17 問，「開発技術」から 4 問，「サービスマネジメント」から 4 問という比率でした。ほぼ事前の予想どおりの比率であったといえます。

#### 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 分野です。分野別の出題数は，セキュリティが 12 問，ネットワークが 3 問，データベースが 2 問でした。セキュリティの 12 問のうち，10 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。内容的には，DNS キャッシュポイズニング，OP25B などの比較的新しい技術用語を問うものが出題されました。

ネットワーク，データベースの問題は，いずれも基本的な問題です。難易度的には，やや易といえます。

#### 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 分野です。分野別の出題数は，システム開発技術が 2 問，ソフトウェア開発管理技術が 2 問でした。なお，これらの問題は，情報セキュリティの専門知識を必要とするものではなく，それぞれの技術に関する一般的な知識問題です。

#### 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 分野です。分野別の出題数は，サービスマネジメントが 3 問，システム監査が 1 問でした。ITIL のインシデント管理，データベースサーバのハードディスク障害時にサービスを続行できるようにするための方策，アクセス権限を管理している利用者 ID リストから権限喪失者が削除されていることを検証する手続きなど，サービスマネジメント分野の問題は，比較的セキュリティに関する知識が要求されるような問題であったといえます。

### (3) 午後 I の問題

午後 I 試験は 4 問の中から 2 問の選択になりました。このため，1 問当たりの問題分量や設問数が基本的に増加しています。しかし，問題ごとの難易度や，一つの設問当たりの配点にばらつきが見られ，どの問題を選択し解答したかによって，合格基準点をクリアできるかどうかが大きく左右すると思われます。なお，情報セキュリティスペシャリスト試験の午後試験において合格基準点をクリアするには，セキュリティ技術の本質のほか，インターネットを構成する要素に対するさまざまな攻撃手法などの技術知識を十分に把握していることが要求されます。

### 問 1　パケットログ解析

DNS サーバに対する DNS reflection 攻撃や，ボットの挙動などに関する技術的な問題です。DNS プロトコルをはじめとしたネットワークに関する詳細な技術知識が要求されるので，全体的に難度が高いといえます。例えば，穴埋め問題と語句選択として 9 問が出題されていましたが，この 9 問に全問正解することはかなり難しいといえます。また，記述式問題は 4 問ありましたが，比較的に容易に解答できるものは，設問 3 (2)に限られます。この問題において合格基準点の 30 点をクリアすることは，厳しいと考えられます。

### 問 2　ソフトウェアの脆弱性への対応

Web 販売システムにおけるサーバソフトウェアが持っている脆弱性対策の問題です。問題を一見すると，難しそうに感じられます。しかし，問題に記述されている内容をよく読んでいけば，正解を導き出せるものもあります。合格基準点をクリアするという観点では，標準レベルの問題といえます。ただし，セキュリティに関し，一定レベルの技術知識を持っているということが条件です。

### 問３　アプリケーション開発時の脆弱性対策

セッション ID の生成に関する注意事項，パスワードを突き止められないようにするハッシュ値の算出方法などの基本的な問題が出題されています。そのほかには，Perl 言語，HTML タグの属性に関するものです。HTML タグの属性は，属性を知らなければ答えようがありませんが，そのほかの設問は比較的取り組みやすいといえます。ただし，設問数が最も少ないので，記述式の設問の配点が高くなっていると考えられます。ミスをしてしまうと，一気に得点が減少しますので，合格基準点をクリアすることは難しくなってきます。問題の難易度を全体的に評価すると，標準レベルといえます。

### 問４　情報システムの特権管理

午後Ⅰの 4 問の中では，比較的，マネジメント系を中心とした問題です。出題内容は，特権 ID の利用，ログの取得内容，ログによって確認すべき事項などの基本的な問題が多く出題されています。問題の記述内容を十分に把握しながら，解答を作成していけば，正解を導きやすいといえます。合格基準点をクリアするという観点では，比較的やさ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 が技術系，問 2 がマネジメント系というように，出題内容としてはほぼバランスが取れていたように思われます。両方の問題とも，最近のセキュリティ動向などを十分に把握していることが必要です。しかし，設問で問われていることについては基本的なものが多く，情報セキュリティに関し，一定レベル以上の知識を有していれば，正解できるものが多いといえます。このため，十分に準備して試験に臨んだ受験者は，合格基準点をクリアできると考えられます。なお，午後Ⅰと午後Ⅱを全体的に比較すると，午後Ⅰがやや難，午後Ⅱがやや易という評価になると思います。

### 問１　公開鍵基盤の構築

設問 1 は，米国政府調達基準で現在調達可能で 2011 年以降調達できなくなる暗号アルゴリズムに関するものなどが問われていますので，かなり難度が高く，4 問中 2 問の正解が得られるかどうかです。その半面，記述式の問題は全体的にやさしいレベルであるといえます。例えば，設問 2 は，問題の記述内容から正解

を導くことができますし，設問 3 は，秘密鍵の取扱いに関し，一定の知識があれば，正解できる問題です。設問 4 は，解答字数が多いので，解答作成に苦労するかもしれませんが，公開鍵証明書の仕組みを把握していれば，適切に解答を作成することができます。また，設問 5 は，公開鍵証明書の取扱いに関するもの，設問 6 は，通信相手の公開鍵がない場合，署名の検証に失敗することに気付けば，比較的容易に正解を導くことができます。合格基準点の 60 点をクリアするという観点では，比較的やさしいレベルの問題といえます。

**問２　インターネット販売を行う企業の情報セキュリティ管理**

ほとんどの設問は，PCI DSS（データセキュリティ基準）で示されている要件をベースにして，F 社の販売システムの脆弱性の改善事項に関する F さんと G 部長の会話の内容をもとにしています。しかし，設問で問われている内容は，基本的な技術知識の問題が多く，多くの設問に対し解答を作成しやすいといえます。強いて難しい設問を挙げるとしたら，WAF におけるシグネチャを作成することが難しい理由を答える設問 3 の(1)や，トランザクションログに対する代替管理策を答える設問 4 の(1)などを挙げることができます。いずれにしても，合格基準点をクリアすることは，問 1 と同様に比較的やさしいといえます。