情報セキュリティスペシャリスト試験　傾向と対策

(1) 情報セキュリティスペシャリスト試験の位置づけ

情報セキュリティスペシャリスト試験の受験者像は次のように考えられています。

業務と役割

セキュリティ機能の企画・開発・運用・保守を推進又は支援する業務，若しくはセキュアな情報システム基盤を整備する業務に従事し，次の役割を主導的に果たすとともに，下位者を指導する。

①情報システムの脅威・脆弱性を分析・評価し，これらを適切に回避・防止するセキュリティ機能の企画・要件定義・開発を推進又は支援する。

②情報システム又はセキュリティ機能の開発プロジェクトにおいて，情報システムへの脅威を分析し，プロジェクト管理を適切に支援する。

③セキュリティ侵犯への対処やセキュリティパッチの適用作業など情報システム運用プロセスにおけるセキュリティ管理作業を技術的な側面から支援する。

④情報セキュリティポリシの作成，利用者教育などに関して，情報セキュリティ管理部門を支援する。

期待する技術水準

情報セキュリティ技術の専門家として，他の専門家と協力しながら情報セキュリティ技術を適用して，セキュアな情報システムを企画・要件定義・開発・運用・保守するため，次の知識・実践能力が要求される。

①情報システム又は情報システム基盤のリスク分析を行い，情報セキュリティポリシに準拠して具体的な情報セキュリティ要件を抽出できる。

②情報セキュリティ対策のうち，技術的な対策について基本的な技術と複数の特定の領域における応用技術をもち，これらの技術を対象システムに適用するとともに，その効果を評価できる。

③情報セキュリティ対策のうち，物理的・管理的な対策について基本的な知識と適用場面に関する技術をもつとともに，情報セキュリティマネジメントの基本的な考え方を理解し，これを適用するケースについて具体的な知識をもち，評価できる。

④情報技術のうち，ネットワーク，データベース，システム開発環境について基本的な知識をもち，情報システムの機密性，責任追跡性などを確保するために必要な暗号，フィルタリング，ロギングなどの要素技術を理解している。

⑤情報システム開発における工程管理，品質管理について基本的な知識と具体的な適用事例の知識，経験をもつ。

⑥情報セキュリティポリシに関する基本的な知識を持ち，ポリシ策定，利用者教育などに関して，情報セキュリティ管理部門を支援できる。

⑦情報セキュリティ関連の法的要求事項などに関する基本的な知識を持ち，これらを適用できる。

（IPA 情報処理技術者試験ガイドブック，テクニカルエンジニア(情報セキュリティ)試験より抜粋）

(2)午前問題のテーマとレベル

午前試験は，午前 I，午前 II とあり，それぞれで“足きり”式の判定を行います。

★午前 I 試験

高度共通区分試験（午前 I ）は，4 肢択一式で 30 題出題されます。試験時間は，50 分間（9:30～10:20）です。また，合格基準は，正答数 60%（18 題正解）です。午前 I 試験で合格基準に達さないと，いわゆる「足きり」となってしまい，残りの試験（午前Ⅱ，午後 I ，午後Ⅱ）は採点されません。一方，試験全体としての合否と関係なく，午前 I 試験で合格基準に達していると，次回以降（2 年間）の午前 I 試験が免除されます。なお，応用情報技術者試験に合格していても合格時から 2 年間，午前 I 試験が免除されます。

試験問題は，同日に実施される応用情報技術者試験の午前問題から 30 題抜粋して作成されています。平成 21 年春，平成 21 年秋試験では，次の表に示す関係になっていました。

表 1. 応用情報技術者試験午前問題との関係

高度共通	応用情報		分野	高度共通	応用情報		分野
	H21春試験	H21秋試験			H21春試験	H21秋試験	
問1	問2	問1	テクノロジ	問18	問50	問51	マネジメント
問2	問3	問4		問19	問51	問53	
問3	問6	問5		問20	問55	問56	
問4	問12	問9		問21	問57	問57	
問5	問16	問15		問22	問59	問59	
問6	問19	問17		問23	問62	問61	ストラテジ
問7	問21	問21		問24	問64	問64	
問8	問24	問23		問25	問65	問67	
問9	問25	問25		問26	問67	問70	
問10	問28	問28		問27	問70	問71	
問11	問32	問31		問28	問71	問73	
問12	問36	問32		問29	問76	問77	
問13	問37	問37		問30	問79	問78	
問14	問40	問38					
問15	問41	問41					
問16	問44	問48					
問17	問48	問49					

平成 21 年春試験・秋試験ともに,

・テクノロジ系問題 …17 題
・マネジメント系問題… 5 題
・ストラテジ系問題 … 8 題

での出題でした。今後ともに，この傾向は続くものと考えられます。テクノロジ系問題が若干多いですが，マネジメント・ストラテジ系問題との割合はほぼ半数と言えます。したがって，両分野ともにしっかりと学習して対策をしておく必要があります。

レベルは，応用情報技術者試験からの抜粋であることから明らかなように，応用情報技術者試験と同一レベルです。応用情報技術者試験（ソフトウェア開発技術者試験）の受験経験の無い方は，午前Ⅰ試験対策に，ある程度(かなり)の時間を要します。この分の学習時間をしっかり確保してください。

なお，テクノロジ分野については，次の内訳です。

・コンピュータ科学基礎（問 1～3）

問 1，2　　基礎理論（2 進数，オートマトン，浮動小数演算の誤差，情報数学）

問 3　　データ構造（リスト，ハッシュ，木，スタック，キュー）

・コンピュータシステム（問 4～10）

問 4　　ハードウェア（CPU，メモリ，周辺装置，外部バスの規格）

問 5　　システム構成（稼働率，高信頼システム）

問 6　　計算問題（ページフォルトの回数，稼働率，キャッシュのヒット率）

問 7　　オープンソース（オープンソースの定義，オープンソースのソフトウェア），GPL

問 8　　論理回路（論理演算）

問 9　　WEB 関連の技術（主にデザイン技術に関すること）

問 10　　コンピュータグラフィクス，動画・画像フォーマット（MPEG1,2,4，JPEG など）

・データベース（問１１から１～２題）

問 11㈱
問 11，12㈱ ER 図，DBMS

・ネットワーク（問１２から１～２題）

問 12，13㈱
問 13㈱　　IP 電話，IP アドレスの割り当て，アプリケーションプロトコル

・セキュリティ（問１４～15）

問 14，15　鍵の利用法（主に公開鍵），脅威・攻撃手法，ISMS などの基準に関すること

・システム開発（問１６～１７）

問 16，17　CMMI，品質特性，データ中心設計，プロセス中心設計，開発技法の特徴

★午前Ⅱ試験

午前Ⅱ試験は，4 肢択一式で 25 題出題されます。試験時間は，40 分間（10:50～11:30）です。また，合格基準は，正答数 60%（15 題正解）です。午前Ⅱ試験で合格基準に達さないと，いわゆる「足きり」となってしまい，残りの試験（午後Ⅰ，午後Ⅱ）は採点されません。試験時間も短く慌ただしい試験になります。ゆっくり解いているとすぐに時間が経ってしまいますので注意しましょう。

平成 21 年秋試験では，

・セキュリティ分野　　…14 題（問 1～14）

・ネットワーク分野　　… 6 題（問 16～21）

・システム開発分野　　… 3 題（問 15，22，23）

・サービスマネジメント分野… 2 題（問 24，25）

・データベース分野　　…出題無し

での出題でした。平成 21 年春試験と比較するとセキュリティの問題が増加しています。また，今回はデータベース分野が出題されませんでした。多少の増減はあるものの，おおよそこのくらいの比率であると考えてください。なお，レベルは，セキュリティ，ネットワーク分野がレベル４で，他の分野はレベル３です。レベル３は，応用情報技術者試験の午前問題と同じレベルです。

午前Ⅰ試験を受験する方は，午前Ⅱ試験は，午前Ⅰの延長ととらえて構わないと思います。

午前Ⅰ試験が免除の方は，システム開発，サービスマネジメント，データベースの各分野について，知識整理をしておく必要があります。セキュリティとネットワークに絶対の自信があれば，この２分野だけでも合格ラインには達せますから，他の分野はほどほどの学習ですませておくのも策でしょう。

(3)午後問題のテーマ

★午後Ⅰ試験　（試験時間 90 分，4 題出題のうち 2 題を選択して解答する）

H21 春試験よりも，問題で扱う事例規模が大きくなっており，設問の分量も明らかに増えています。前回の試験よりも問題自体の難易度は上がったと言えます。しかし，合格ラインが 60%の正解でよいことと，1 題 45 分かけられることを考えると，前回試験が簡単であった感も否めません。今回の試験くらいの分量が標準と考えられます。文章を記述する設問が増えていますから，文章で要点を表現する練習は以前にも増して重要になっています。

H21 秋試験のテーマは，“セキュリティマネジメント”の色合いが濃かったように思います。しかし，これは単純に今回そうであったというだけで，次回以降の試験の傾向とは言えません。技術的色合いの濃い問題とマネジメント的色合いの濃い問題は同程度出題されると考えてください。

テーマ	H21春試験	H21秋試験
問1	パケットログの解析 ・ログの読み取り ・DNSへの攻撃	電子メールからの情報漏洩 ・規定の遵守違反の箇所 ・携帯電話の紛失 ・携帯電話でのメール取り扱い
問2	ソフトウェアの脆弱性への対応 ・HTTPでのGET，POST ・IPS ・修正プログラムの適用時の注意	Javaアプレット （セキュアプログラミング） ・アプレットの署名 ・JREのバージョン依存の問題
問3	Webアプリのセキュリティ （セキュアプログラミング） ・Perl DBI ・セッションの識別 ・XSS	ICカード認証 ・ICカードのセキュリティ要件 ・チャレンジレスポンス認証 ・ICカードの失効方法
問4	情報システムの特権管理 ・特権ID管理の運用 ・アラートに関する設計	ノートPCの情報漏洩 ・ノートPCの持ち運びに際しての問題 ・導入予定製品の評価

★午後Ⅱ　（試験時間 120 分，2 題出題のうち 1 題を選択して解答する）

午後Ⅱ試験では，技術的に細かい点を空欄補充形式で問われることが多いです。しかし，合否に関係するほどは空欄数は多くないですし，また，全体的な配点割合も少ないので，さほど気にしなくても良いでしょう。

午後Ⅱ試験は，問題文の分量が多いこと以外には，午後Ⅰ試験と難易度は変わりません。問題文で提示されている事例のストーリーをしっかり把握することがとても重要です。

H21 秋試験では UML(ユースケース図)を読解させる問題が出題されていました。セキュリティ要件を定める際に必要となる一連の開発知識，技能を問う点が特徴です。応用情報技術者試験レベルの一通りの知識が定着していると有利でしょう。

テーマ	H21春試験	H21秋試験
問１	公開鍵基盤の構築 ・暗号アルゴリズム ・署名の利用における問題点 ・プライベート認証局の運用	認証・認可基盤構築の実施計画 ・UML(ユースケース図) ・SAMLのメッセージフロー ・LDAP
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 ・JIS Q 27001 ・セキュリティ要件の提示 ・ISMSの継続的改善	社内LANの見直し ・IEEE802.1X ・EAP ・ファイアウォールの設定 ・無線LANのセキュリティ

(4)学習に当たって

・午前試験は，試験を受けるための受験資格をもらうものと考えよ！

・午前試験は，過去問演習で攻略可能です。出来る限りたくさん演習しましょう

・暗記は通用しない，原理・理由を**理解**すべし

・午後問題には，ストーリー性があります。解答の方向を察する学習をしてください

・言いたいことを日本語で簡潔に表現する練習をしましょう

・セキュアプログラミングは，経験者のみ解答可能な問題と考えてください。内容は，難しくはありませんが，テキストなどで学習できる事柄ではありません。実際の経験が必要です。経験不足の方は，自宅でサーバを作って，日曜プログラマになりましょう

・暗号アルゴリズムの特徴やセキュリティプロトコルについて徹底的に学習してください

・セキュリティに関する情報を日頃から幅広く集めることは，この職種にかかわる者として必須です。実践しましょう。