情報セキュリティスペシャリスト試験　傾向と対策

■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・要件定義・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。

(IPA 試験要綱より抜粋)

■午前試験

★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。近年は，

・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

での出題です。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・ストラテジ系問題も4割以上を占めます。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。

テクノロジ分野についてのおおよその内訳は次の通りです。

・コンピュータ科学基礎（問1～3）
–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，流れ図）
–データ構造（リスト，ハッシュ，木，スタック，キュー），XML

・コンピュータシステム（問４〜10）
–ハードウェア（CPU，メモリ，キャッシュのヒット率，周辺装置）
–システム構成（マルチプロセッサシステム，稼働率，高信頼システム）
–ページング方式（ページフォルトの回数）
–オープンソース（オープンソースの定義など），OS（タスク管理）
–論理回路（論理演算），組込システム，符号化
–WEB 関連の技術（主にデザイン技術に関すること）
–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）
-ER 図，DBMS

・ネットワーク（問１２から１〜２題）
-IP 電話，IP アドレス，アプリケーションプロトコル

・セキュリティ（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）
–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，UML，知的財産権，産業財産権

★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 25 年春試験では，

・セキュリティ分野　　…16 題 (問 1〜16)
・ネットワーク分野　　… 4 題 (問 17〜20)
・データベース分野　　… 1 題 (問 21)
・システム開発分野　　… 3 題 (問 22〜24)
・監査分野　　… 1 題 (問 25)

での出題でした。平年と同じ構成です。セキュリティ分野，ネットワーク分野できちんと得点することが大切です。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です。
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，監査分野について，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，この二分野だけでも合格ラインには達せますから，おおざっぱに知識の復習を行う程度ですませておくのも策でしょう。

■午後試験

午後試験は，午後Ⅰ，午後Ⅱ試験とあります。どちらも，合格基準は 60 点の得点です。
午後試験問題共通の特徴として，テーマで取り上げている話題に関する知識があるか無いかで，解きやすさが全く違うという点が挙げられます。解答は，教科書的なものが多いので，なるべく最新のセキュリティテーマに触れ，どのように対策するのが一般的なのかといった知識を増やしてください。

★午後Ⅰ試験　（試験時間 90 分，3 題出題のうち 2 題を選択して解答する）

平成 25 年秋試験から，出題数が変更になります。これまで，4 題出題のうち 2 題を解答していましたが，次回からは，3 題出題に減ります。したがって，セキュアプログラミングの問題が 1 題出題されると，事実上選択の余地がなくなってしまうことも考えられますから注意してください。

平成 25 年春試験は，平年並の内容・レベルでした。今回は，午後Ⅰ試験には，セキュアプログラミングの問題は出題されていませんでした。

午後Ⅰ試験では，暗号技術や認証技術についての正確な基礎知識を問う問題や，ウェブサイトのセキュリティ，DNS サーバ，メールサーバのセキュリティといったテーマは定番テーマです。“セキュリティマネジメント”にかかわる問題もよく出題されます。“セキュリティマネジメント”がテーマの問題は第一印象は良いですが，文章をよく読んで，問われていることに正確に答える練習を積まないと，なかなか正解しませんので注意してください。

テーマ	H24秋試験	H25春試験
問 1	Webサイトの刷新 ・JSON，Javascript ・HTTP関する知識 ・フォーム認証	マルウェアの解析 ・FWのフィルタリングルールの読解 ・標的型攻撃の特徴 ・マルウェア感染の過程の把握
問 2	ログの管理 ・ログの分析に関すること ・ログ分析のの有効性，効率性	IPアドレス詐称対策 ・DNSプロトコルの特徴 ・DNSキャッシュポイズニング ・SPF
問 3	標的型攻撃 ・メールヘッダの分析 ・SPF ・標的型攻撃への対策	リモートアクセス環境のセキュリティ対策 ・物理的対策，盗難対策 ・リモートアクセス時のリスク
問 4	セキュリティインシデント対応 ・IDSの運用 ・FWでの通信制御 ・ログ管理	情報漏えい対策 ・不正競争防止法での営業秘密 ・ディジタルフォレンジック ・社外持ち出し用PCに対するリスク

★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ですが，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して，考えながら解くことが重要です。

平成 25 年春試験は，問 1 が Java 言語プログラムに関するセキュアプログラミングの問題でした。プログラム中のコメントを読めば，処理の内容は把握できますが，それでも，全くプログラム作成経験が無い受験者には，手に負えないと思われます。このことから，事実上，選択の余地無く問 2 を解答することになった受験者も多いように思います。

テーマ	H24秋試験	H25春試験
問1	Webサイトの診断と対策 ・HTTPリクエスト， HTTPレスポンスに関する知識 ・XSS ・SSH	業務パッケージの開発（Webアプリケーション） ・Javaによるセキュアプログラミング ・SQL文の組み立て ・脆弱性を把握する ・セキュリティ要件の決定
問2	無線LANの構築 ・無線LANの運用に関する知識 ・IEEE802.1x ・セキュリティポリシーの見直し	技術情報の管理 ・NTP ・メールサーバのセキュリティ DKIM，オープンリレー対策 ・タイムスタンプ技術 アーカイブタイムスタンプ

■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

・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

・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

・Web アプリケーションのセキュリティ，DNS サーバのセキュリティ，メールサーバのセキュリティは，重点的に学習してください。

・ネットワークセキュリティ（特に無線 LAN 関係）も学習を忘れずに！

・IPA のセキュリティサイト(http://www.ipa.go.jp/security)は必見です！

・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

・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。