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。平成 22 年春試験，平成 22 年秋試験ともに，

・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。

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）
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，流れ図）
問 3　　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）
問 4　　ハードウェア（CPU，メモリ，キャッシュのヒット率，周辺装置）

問５　　システム構成（稼働率，高信頼システム）
問６　　ページフォルトの回数，稼働率
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），組込システム
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　　ER 図，DBMS

・ネットワーク（問１２から１～２題）
問 12，13　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）
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，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 22 年秋試験では，

・セキュリティ分野　　…15 題 (問 1～15)
・ネットワーク分野　　… 5 題 (問 16～20)
・データベース分野　　… 1 題 (問 21)
・サービスマネジメント分野 … 4 題（問 22～25）
・システム開発分野　　…出題無し

での出題でした。平年とほぼ同じ構成です。今回は，前回，前々回には出題されていなかったデータベース分野の問題が出題されていましたが，1 題だけですから合否には関係ないと言えます。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と思います。

午前Ⅰ試験が免除の方は，サービスマネジメント分野について，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，4題出題のうち2題を選択して解答する）

平年並の内容・レベルです。ただし，今回は，セキュアプログラミングの問題が出題されていなかったことが特徴的です。なお，セキュアプログラミングは，経験の無い人が，一から学習することは荷が重く不利ですから，経験がある人向けと考えておいてください。

“セキュリティマネジメント”にかかわる問題も問2に出題されていました。一定レベルの技術的な事柄は問われますが，これらの問題は，状況が把握しやすく，比較的解きやすいと思われます。

さらに，WAFやマルウェアなど，近年良く扱われるテーマが出題されていたことも特徴的です。

テーマ	H22春試験	H22秋試験
問1	セキュアプログラミング ・主としてJavaサーブレット ・メモリリーク ・レーシング対策 ・強制ブラウズ	データ伝送のセキュリティ設計 ・SSL証明書 ・アクセス制限 ・事後確認の行い方 ・セキュリティポリシーとの整合性
問2	データの暗号化とバックアップ ・暗号化方式の検討 ・バックアップからの情報漏洩 ・TPM	利用者IDのライフサイクル ・UID管理システムの動きの把握 ・UIDの不正取得 ・確実なUIDの削除
問3	個人情報保護 ・S/MIME，PGP ・パスワードの運用	WAF ・セションハイジャック攻撃 ・SSL通信とWAFでのチェック
問4	ウイルス駆除・感染防止 ・ウイルスによる被害の把握 ・感染PCの特定 ・感染防止策	マルウェア対策 ・ガンブラーを想定したテーマ ・再発防止策の選定 ・被害を与えた顧客範囲の調査

★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。

H22秋試験では，Webアプリケーションの開発と，認証システムの統合を題材にした問題が出題されました。Webアプリケーションの開発の問題はセキュアプログラミングが絡んでくる問題で，プログラム開発の経験の無い方には解きづらいと思われます。

テーマ	H22春試験	H22秋試験
問1	サーバの対策 ネットワークセキュリティ ・DNSキャッシュ汚染対策…DNSsec ・メールサーバの対策…SPF ・アクセス制御，FWのルール設定	Webアプリケーションの開発 ・バインド機構を用いたコーディング ・アプリケーション設計時のセキュリティ ・SQLインジェクション対策
問2	情報セキュリティインシデントの対応 ・ログ管理のポリシー ・IPSの運用，ログ分析 ・従業員への周知・教育	社内認証システムの統合 ・チャレンジレスポンス認証 ・ケルベロス認証 ・シングルサインオン ・システムの移行に関する注意点

■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。