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。なお，セキュリティ分野が 4 問ありますので重点学習分野です。

・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 4～8）
　–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９　１～２題）
-ER 図，正規化，DBMS

・ネットワーク（問１０，１１　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１２～１５）
–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 27 年秋試験では，

・セキュリティ分野	…17 題 (問 1～17)
・ネットワーク分野	… 3 題 (問 18～20)
・データベース分野	… 1 題 (問 21)
・システム開発分野	… 2 題 (問 22，23)
・サービスマネジメント	… 1 題 (問 24)
・監査分野	… 1 題 (問 25)

での出題でした。ポリモーフィック型ウイルス，水飲み場型攻撃，ICMPFlood，ダウンローダ型マルウェアなどの日頃からウェブなどで情報収集をしていれば知っているような基本的な知識が多く出題されていました。テキストだけではなく，自主的に情報セキュリティに関する情報収集をしているかを試す問題と考えられます。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，合格点は 60 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。標的型攻撃，Web アプリケーションを狙った攻撃，スマートホンに関するセキュリティ，オンラインストレージの利用など，近年話題になっているテーマが好んで出題されます。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 27 秋試験ではセキュアプログラミングが出題されませんでした。今回も HTTP のメソッドを取り上げた問題が出題されていました。HTTP プロトコルそのものについて理解を深めておくことは必須であるといえます。HTTP のメソッド，レスポンスステータスコード，クッキー，HTTP ヘッダ中の情報についてしっかり理解しておくことが大切です。

平成 27 年秋試験も平年並の内容・レベルでした。しかし，セキュリティスペシャリストの試験は問題文が長く，図表も多いので，これらをしっかり把握する力が必要です。問題のレベルは決してやさしくはありません。

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，スマホのセキュリティ，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。“情報セキュリティマネジメント”をテーマとした問題は減ってきており，技術色が濃くなっています。

問番号	H27 春試験	H27 秋試験
問 1	Web サイトの脆弱性と対策 ・セッションクッキーの扱い ・HTTP ヘッダインジェクション	ソフトウェアの脆弱性への対応 ・HTTP リクエストの検証 ・WAF
問 2	情報漏洩インシデントの調査 ・フィルタリングルールの読み取り ・ログ管理	特権 ID の管理 ・アクセスしたユーザの特定 ・ID 管理の方法
問 3	パスワードへの攻撃 ・パスワードの設定 ・パスワードの保管(ハッシュ値とソルト)	Web サイトにおけるインシデント対応 ・ログイン履歴の分析 ・FW のフィルタリングルール ・HTTP リクエスト，ステータスコード

★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，このような空欄は合否に関係するほどは多くないですし，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よいでしょう。午後Ⅱ試験は問題文の分量が多いですが，午後Ⅰ試験と技術的な知識の要求レベルは変わりません。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，総合的に考えながら解くことが重要です。また，午後Ⅱ問題は複数のテーマを組み合わせた問題になっていることも特徴です。テーマの変わり目を適切に判断できると解きやすくなります。

平成 27 年秋試験は，セキュアプログラミングに関する問題は出題されませんでした。一方で，セキュリティマネジメントの観点からセキュリティ関連法規について知識を問われていた点が特徴的で

した。セキュリティ法規関連のテーマは手薄になりがちなテーマですから，整理し直しておくとよいでしょう。午後 II 試験では，ネットワークセキュリティに関係する問題もよく出題されますから，ネットワークの知識についても万全にしておく必要があります。特に，SSL については詳細に学習しておいてください。また，メールヘッダの解析もできるようにしておきましょう。

問番号	H27 春試験	H27 秋試験
問 1	ウイルス対策 ・DNS，SMTP ・URL フィルタリングの設定 ・Web フォームの悪用	マルウェア対策 ・マルウェアの感染 ・ウイルススキャン ・FW で遮断する通信 ・パフォーマンス検証(回線速度計算)
問 2	製造業におけるネットワーク構築 ・マルウェアの感染 ・証明書発行の手続き ・セキュリティポリシー，実施規定	データの取り扱い ・オンラインストレージの利用 ・セキュリティ関連法規，営業秘密 ・ディスク暗号化方式

■学習に当たって

・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，標的型攻撃は，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 と SSL）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。内容はさほど難しくはありませんが，短期間で学習できるテーマではありません。実際の経験が必要です。もし，プログラミング未経験（入門レベル）の方が学習するのであれば，自宅やクラウド上にサーバを作って日曜プログラマになって学習する意気込みが必要です。

・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。