

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セキュリティ侵害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ーの作成、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しないと、いわゆる「足ぎり」となってしまう、残りの試験（午前Ⅱ、午後Ⅰ、午後Ⅱ）は採点されません。一方、試験全体としての可否と関係なく、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と確保してください。

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しないと，いわゆる「足ぎり」となってしまう，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 年春試験では，

- ・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。平年に比べると，PKI 関連の知識が多く問われていました。基本的な知識ですのでしっかり学習しておくべきテーマです。また，サイドチャネル攻撃，CRL，ルートキット，ベイジアンフィルタ，DNSSEC，DNSamp，SMTP-AUTH などの基本的な用語も多く出題されていました。これらの用語は過去に幾度も出題された用語でしたので，過去問演習をしっかりしておけば対応できました。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るのも策でしょう。

■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、スマートフォンに関するセキュリティなど、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）

問1はセキュアプログラミングの問題でしたが、プログラムコードが提示されておらず、プログラム言語についての知識がなくてもWebアプリケーションのセキュリティについての知識があれば解ける問題でした。また、HTTPのヘッダについての知識を問われていました。HTTPプロトコルそのものについて理解を深めておく必要があります。今回の様な題材について解けるように学習をしておくことで午後Ⅰ試験での問題選択の幅が広がります。

平成27年春試験は平年並の内容・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	H26 秋試験	H27 春試験
問1	スマートホンのセキュリティ ・バッファオーバーフロー ・スマホOS（脱獄）	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
問2	暗号技術の評価 ・暗号方式、ハッシュ関数 ・証明書の発行	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
問3	マルウェア感染とフィルタリング ・フィルタリングルールの設定 ・パスワード攻撃	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）

★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と把握して、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年春試験は、問1に1つだけセキュアプログラミングに関する問題が出題されていました。

しかし、プログラムコードは1行提示されていますので、プログラミング言語の知識は不要です。午後Ⅱ試験では、ネットワークセキュリティに関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	H26 秋試験	H27 春試験
問 1	認証システムの設計 ・シングルサインオン ・HTTP 認証	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
問 2	Web サイトのセキュリティ ・Web アプリケーションへの攻撃手法 ・ログの読解	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

■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。