

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。平成 22～24 年春試験を通して，

- ・テクノロジー系問題 …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。テクノロジー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。

テクノロジー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など), OS (タスク管理)
- 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), システム構成
- 問10 コンピュータグラフィックス, 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24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 … 2題 (問22～23)
- ・サービスマネジメント分野 … 1題 (問24)
- ・監査分野 … 1題 (問25)

での出題でした。今回は、監査分野からも出題されましたが、平年とほぼ同じ構成です。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しますから、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。今回は Java 言語を利用したセキュアプログラミングの問題が出題されましたが，テーマは，Web アプリケーションにおけるセッション管理などについてでした。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。

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 1 題は出題される傾向にあります。“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	H23秋試験	H24春試験
問 1	セキュアプログラミング ・ C++, Java ・ SQLインジェクション ・ バッファオーバーフローの原因	セキュアプログラミング ・ クッキーの設定 ・ セッション管理 ・ エスケープ処理
問 2	セキュリティの観点での機能追加 ・ ハッシュ関数の名称 ・ ログイン処理の流れ ・ 仮パスワードを取得する手口	Webアプリケーションのセキュリティ対策 ・ 暗号方式（転置暗号，換字暗号など） ・ SQLインジェクション ・ XSS
問 3	SSL通信時のプロキシでのログ取得 ・ HTTPS通信時のロギングに関する問題点 ・ サーバ証明書の検証	保守作業の証跡確保 ・ ハッシュ関数による改ざん検出 ・ ログサーバの運用，ログ取得
問 4	ISMSと内部統制 ・ 物理的，環境的セキュリティ ・ アクセス制御 ・ データの完全性（正確性）の保証	情報セキュリティ技術者の育成 ・ 標的型攻撃（APT） ・ ウイルス感染からの復旧

★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と把握して，考えながら解くことが重要です。

テーマ	H23秋試験	H24春試験
問 1	セキュリティポリシーに従ったシステム開発 ・ 耐タンパ性 ・ アーカイブタイムスタンプ ・ BCP	インターネット向けサーバの災害対策 ・ ウイルス活動の調査，対処 ・ SPF ・ 災害時の情報提供
問 2	ログ管理システムの設計 ・ ネットワークセキュリティ ・ ログの取得，管理 ・ ログの分析	クラウドの利用とセキュリティ ・ 電子メールでの情報漏洩 ・ サービス停止時間の計算，バックアップ ・ モバイル（携帯）端末でのウイルス感染

■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
- ・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
- ・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。

！平成24年春期からセキュアプログラミングの言語が変わりました！

Perlが無くなり、JavaScript (ECMAScript) になりました。ご注意ください。
ECMAScriptは、JavaScriptやJScriptを標準化する目的で作られた言語です。