

情報処理安全確保支援士試験 本試験分析と傾向と対策法

午後試験が1本化されました

■情報処理安全確保支援士試験の位置づけ

情報処理安全確保支援士は次の役割を担います。

業務と役割

情報セキュリティマネジメントに関する業務、情報システムの企画・設計・開発・運用におけるセキュリティ確保に関する業務、情報及び情報システムの利用におけるセキュリティ対策の適用に関する業務、情報セキュリティインシデント管理に関する業務に従事し、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 情報セキュリティ方針及び情報セキュリティ諸規程（事業継続計画に関する規程を含む組織内諸規程）の策定、情報セキュリティリスクアセスメント及びリスク対応などを推進又は支援する。
- 2 システム調達（製品・サービスのセキュアな導入を含む）、システム開発（セキュリティ機能の実装を含む）を、セキュリティの観点から推進又は支援する。
- 3 暗号利用、マルウェア対策、脆弱性への対応など、情報及び情報システムの利用におけるセキュリティ対策の適用を推進又は支援する。
- 4 情報セキュリティインシデントの管理体制の構築、情報セキュリティインシデントへの対応などを推進又は支援する。

(IPA試験要綱Ver5.2より抜粋)

■午前試験

★午前 I 試験

午前 I（高度共通区分）試験は、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、高度区分の情報処理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のように、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。

★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。

R05年春試験では、

・セキュリティ分野	…	17題 (問1～17)	《レベル4》
・ネットワーク分野	…	3題 (問18～20)	《レベル4》
・データベース分野	…	1題 (問21)	《レベル3》
・システム/ソフトウェア開発分野	…	2題 (問22, 23)	《レベル3》
・サービスマネジメント分野	…	1題 (問24)	《レベル3》
・システム監査分野	…	1題 (問25)	《レベル3》

での出題でした。例年と比べて分野ごとの出題数に変化はありません。

セキュリティ分野は、XMLデジタル署名、トランザクション署名、SAML、DNSSEC、OAuth、SSHなど、テキストで学習して知っているべき基本用語（知識）が主として出題されていました。テキストに掲載の用語を定着させ、過去問演習をしっかりとしていれば、合格点は得点できるレベルの試験です。再出題の問題が約7割でした。

最新の技術（とはいっても、すでに広く使われている技術）には日頃から興味を持って、理解を深めておくことが大切です。

午前I試験が免除の方は、システム/ソフトウェア開発、サービスマネジメント、監査分野について、一通りの知識整理をしておくといいです。セキュリティとネットワークに自信があれば、この2分野だけでも合格ラインには達せますから、おおよっぱに知識の確認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、事例問題、記述式の試験です。4問出題され、2問を選択して解答します。試験時間は150分、合格点は60点です。問題は、従来の午後I試験問題よりは分量が多く、午後II試験問題よりは分量が少なくなると予想されます。

午後試験問題の特徴として、テーマで取り上げている話題に関する知識があるかな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（電子メールによる攻撃）、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、組み込み機器のセキュリティ、クラウドサービスでの認証連携、インシデント対応などのテーマが好んで出題されます。近年は、特に、認証に関する問題が頻出です。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。

今回は、技術系の問題が3問（問1，問2，問3），管理系の問題が1問（問4）出題されていました。問題のテーマは、

- 問1 Webアプリケーションプログラムの開発
- 問2 セキュリティ対策の見直し
- 問3 継続的インテグレーションサービスのセキュリティ
- 問4 リスクアセスメント

です。問1はセキュアプログラミングに関する問題、問4はセキュリティマネジメントに関する問題でした。これらのテーマが毎回出題されるのかは、次回以降の様子を見ないと何とも言えません。

問1は、XSSの脆弱性に関する問題です。セキュアプログラミングを選択する人であれば、比較的解きやすい問題であったと言えます。

問2は、無線LAN，VLAN，ファイアウォールでのフィルタリング設定，サーバ証明書の検証など幅広く知識を問う問題です。多くのテーマを扱っていますが、どれも定番テーマですから、解きやすい問題といえます。

問3は、コンテナ仮想化，サーバ証明書の偽装，コードサイニング，WebAuthnなどの知識を問う問題です。コンテナ仮想化について正確な知識が備わっていないと解きづらかったと感じます。

問4は、「あなたの知見に基づき，答えよ」という珍しい形式の設問がありました。本文の状況設定に沿うように答えることが指示されていますので，答える内容は限られています。問題文の文脈を正しくとらえられているかが試されていると言えます。

■学習にあたって

- ・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
- ・午後試験は，問題文を正確に読んで，状況を的確に把握することが最も重要です。また，試験要綱の記載の支援士の役割を念頭に，解答の方向を察する練習してください。
- ・情報セキュリティマネジメントの視点でも知識整理をしておきましょう。
- ・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，認証認可技術（SAML，OAuth，Keycloakも注目かもしれません）は，重点的に学習してください。
- ・ログ調査，ログ分析などができるように，日頃から各サーバのログを見ておくといいです。
- ・仮想サーバの運用についても知識を持っておきましょう。特に，コンテナ型の仮想化は近年多く使われています。詳しく学習しておくといいです。
- ・ネットワークセキュリティ（VLAN，無線LAN，TLS1.3，VPNなど）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。
- ・過去問題演習は、PM I (1.5時間のまとまった時間が必要) → PM I → PM II (2.5時間のまとまった時間が必要) の繰り返しで演習するとよいです。AM II は、すきま時間を利用して演習しましょう。