情報処理安全確保支援士試験　本試験分析と傾向と対策

■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Ver5.4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）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**。

★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）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。

R07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，DRDoS攻撃（リフレクション攻撃），SAML，SHA，カミンスキー攻撃，デジタル証明書，コネクトバック，ISMAP，タイミング攻撃，OAurh2.0，OP25B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していれば，合格点は得点できるレベルの試験です。支援士試験からの再出題の問題は13問ありました。新出用語は，次回以降，午後試験のテーマとして取り上げられる可能性も視野に入れて，Webや専門書などで，詳しく学習しておくと良いです。

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よいです。**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確認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，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。

前回（R06秋）は，文章で解答する設問は全て字数制限なしでしたが，今回（R07春）は，字数制限のあるものと，ないものが混在していました。**この様子ですと，出題者として，字数制限なしで試験を実施していくという強い意志があるわけでもなさそうです**。字数制限の有無にかかわらず，上手に解答できるように練習してください。問題の分量は，8～10 ページ程度です。図表が多く含まれている問題もありますので，**読みごたえはあると考えてください**。旧試験の午後Ⅱ試験問題と同じような分量で出題されている問題もありましたので，問題本文を手際よく理解して解答を作成する力が必要です。実務経験や，専門知識を身に付けただけでは，苦戦します。試験対策として，問題を解き慣れる必要があります。

出題されたテーマに関しては，技術系の問題に比べて，管理系の問題が多く出題されていた点が特徴的でした。また，新制度になってから毎回出題されていた「プログラムコードが提示されるタイプのセキュアプログラミングをテーマにした問題」が出題されませんでした。

R6秋試験の午後試験問題のテーマは，

問1　サプライチェーンのリスク対策
問2　脆弱性管理
問3　スマートフォン用アプリケーションプログラムの開発
問4　IT資産管理及び脆弱性管理

です。

問1 は「サプライチェーンのリスク対策」というテーマで，セキュリティマネジメント系統の問題です。問題本文の出だしから，CI/CD（継続的インテグレーション/継続的デリバリー），SBOM（ソフトウェア部品表）という用語が登場します。これらは，ソフトウェア開発に関する用語です。応用情報技術者試験のシステム開発分野で学習します。**応用情報技術者試験合格レベルの知識がないと，門前払いされてしまう印象の問題**でした。全体としては，本文を読解して，その場で内容を理解し，本文に即して解答を書くタイプの問題です。

問2 は「脆弱性管理」というテーマで，主としてセキュリティマネジメント系統の問題です。技術的な要素としては，SQLインジェクションを題材に，定番のWebアプリケーションに関する知識も問われています。IPAが発行している「TLS暗号設定ガイドライン」に目を通したことがあるかが問われる問題もありました。IPAが発行するガイドライン類は，可能な限り目を通しておくことが大切です。全体としては，本文を読解して，その場で内容を理解し，本文に即して解答を書くタイプの問題です。

問3 は「スマートフォン用アプリケーションプログラムの開発」というテーマで，スマホアプリとWebサーバ，クラウドストレージサービスとの通信に関して，攻撃や対策を問う技術的な問題です。目立つ点としては，TLSハンドシェークについての出題です。ネットワーク関連の話題ですが，支援士のテキストにも登場する基本事項の一つですから，技術的なテーマが得意な方は，印象よく解き進めたと感じます。若干，プログラミング的な側面がありますが（図6にECMAScriptのコードが一行ある），この程度であれば，基本情報技術者試験や応用情報技術者試験合格レベルのプログラミング知識があれば対応できます。

問4 は「IT資産管理及び脆弱性管理」というテーマで，ドメイン管理とIT資産管理を合わせた問題です。ドメイン管理については，技術的なテーマといってもよいかもしれませんが，DNSサーバの設定が問われているのではなく，ドメインのドロップキャッチ，放置したWebサーバの乗っ取りなど，ありがちな管理に関するテーマが問われています。「調査方法を答えよ」といったタイプの問題は，自分で判断して答えを作り上げる問題です。**過去問演習と称して「答えを覚える」学習をしていても答えられません**。「答えを考え出す」練習が必要です。

■学習にあたって

・**応用情報技術者試験合格レベルの知識は確実に持ちましょう**。

・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。

・**答えが分からなくても，それっぽい内容の妥当な事柄をなんとか書く練習をしてください**。問題演習をするときに，空欄にしたまま，解答を見てはいけません。

・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，FIDO2（パスキー）など）は，重点的に学習してください。さらに，HTTP自体の知識もしっかり習得してください。

・REST API （Web API）について度々取り上げられています。REST の考え方や具体的な事例を学習しておきましょう。

・ここのところ，ソフトウェア開発に関連したテーマが多いです。ソフトウェア開発の技法を復習してください。可能であれば，自らで，簡単なWebアプリケーションを作成し，今（流行り）の開発手法を体験してみるとよいです。

・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よいです。

・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よいです。

・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！

・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。

・IPAのセキュリティサイト(http://www.ipa.go.jp/security)は必見です！