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Ver5.3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。

R06年秋試験では，

・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，AAA制御，AI画像認識への攻撃，ポスト量子暗号，Smurf，FIDO，SSO，量子暗号，DMARC，WAF，IPS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14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。

今回の午後試験では，**文章で解答する設問は全て字数制限がなくなりました**。答案用紙には罫線だけが示され，行数によってある程度の解答の分量は予想できますが，記述内容の自由度は高くなっています。これは他の試験区分の記述式試験にはない特徴です。問題の分量は，8～10 ページ程度です。解答数（小問数）は，今回は，4 問とも 11個～12個で，従来の午後Ⅰ試験問題と同程度です。しかし，解答の記述量が増え，文章で解答する問題が多くありました。

出題されたテーマは，インシデント対応や Webアプリケーションの脆弱性など，これまで度々出題されていたテーマでした。ただし，事例内容はより実務的になっており，設問では事例内容に基づいた具体的な解答を求めるものが増えています。セキュリティ技術をしっかり習得しておく必要があります。なお，今回は，規程や基準などのセキュリティ管理については問われませんでした。

R6秋試験の午後試験問題のテーマは，

問1　インシデントレスポンス
問2　ドメイン名変更
問3　クレジットカード情報の漏えい（セキュアプログラミング：ECMAScript）
問4　セキュリティ診断

です。セキュアプログラミングに関する問題は新午後試験になってから連続して出題されています。定番テーマになりそうです。（一方で，H31～R4まで，4年間出題されなかった時期もあったことを忘れてはいけません。作問者がネタ切れになれば，当然出題されないでしょう）

問1 は「インシデントレスポンス」というテーマで，定番のインシデント対応の問題です。今回はシンクライアント環境でのインシデント対応が取り上げられています。定番テーマではありますが，提示されている多くのログからマルウェアの動作を把握し，解析結果とも比較しながら具体的な解答を導くには，相応の時間が必要です。

問2 は「ドメイン名変更」というテーマで，ドメイン名変更に伴うメールセキュリティの問題です。SPF，DKIM，DMARC といった送信ドメイン認証技術に関する設問が中心で，第三者中継防止のルールについても出題されています。ドメイン名変更の移行作業中にどのように設定内容を変更させていけばよいかという具体策や，メーリングリストを利用する場合のSPFやDKIMの問題点についても問われています。直接的に知識を問う設問が多く，知識があれば解きやすかったと思います。

問3 は「クレジットカード情報の漏えい」というテーマで，Webアプリケーションの脆弱性によって偽フォームが表示され，クレジットカード情報が漏えいする事例です。ECMAScript（JavaScript）やHTMLのコードを1 行ずつ読み解く必要があるので，プログラミングの知識がない場合は，選択できない問題です。

問4 は「セキュリティ診断」というテーマで，Webアプリケーションの脆弱性とWeb APIのセキュリティについての問題です。Webアプリケーションの脆弱性としては，セッションフィクセーション，メールヘッダーインジェクションとHTTPヘッダーの不備について取り上げています。これらの脆弱性の修正方法や被害を軽減する効果などを具体的に答える必要がありました。

■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。

・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。

・近年，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。

・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！