情報処理安全確保支援士試験　本試験分析と対策法

■情報処理安全確保支援士とは

サイバー攻撃の急激な増加により，企業などにおけるサイバーセキュリティ対策の重要性が高まる一方，サイバーセキュリティ対策を担う実践的な能力を有する人材は不足しています。そこで，サイバーセキュリティに関する実践的な知識・技能を有する専門人材の育成と確保を目指して、国家資格「情報処理安全確保支援士」制度が創設されました。

「情報処理安全確保支援士（以下，支援士）」はサイバーセキュリティに関する専門的な知識・技能を活用して企業や組織における安全な情報システムの企画・設計・開発・運用を支援し，サイバーセキュリティ対策の調査・分析・評価やその結果に基づく指導・助言を行います。

(http://www.ipa.go.jp/siensi/index.htmlより抜粋)

■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Ver5.0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。

R04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》
・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，MAC（メッセージ認証符号），CAの登録局，SAML，Smurf攻撃，SSOの方式，PFS，クリックジャッキング，IPsec，SMTP-AUTH，SPF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。初出の用語は「パスワードスプレー攻撃」だけでした。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。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必要があります。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，午後Ⅰ，午後Ⅱ試験とあります。どちらも，合格点は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，オンラインストレージの利用，組込み機器のセキュリティなど，近年話題になっているテーマが好んで出題されます。近年は，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。

★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）

R04年春試験には，久しぶりに（令和になって初めて）セキュアプログラミングの問題が出題されましたが，今回のR04秋試験では出題されませんでした。セキュアプログラミング分野は，他のテーマと同等の単なる「1分野」にすぎない扱いになったといえます。

R04年秋試験の問題のテーマは，①IoT製品の開発に関するセキュリティ，②，③セキュリティインシデント対応といった内容でした。3問とも，詳細なセキュリティ技術知識を答えさせる設問はなく，セキュリティとネットワークに関する基本知識を用いて解答を導く，応用力や思考力が試される問題でした。特に，問2，問3のセキュリティインシデント対応に関する問題ではその傾向が強く，知識をそのまま解答する設問はほとんどありませんでした。インシデント内容を正確に読み取るには，読解力が必要とされますが，国語力だけで読み取れるわけではなく，**幅広いセキュリティ知識とネットワーク知識**が必須です。

午後試験は，事例として提示されている本文や図表を読み取って，問題文に即して答えを考えるという試験ですから，事前対策学習（過去問題演習，分析）を十分に行えば解ける問題が多いです。

午後Ⅰ試験では，認証技術の利用についての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，ログ調査といったテーマが定番です。SSHやUNIX系OS(Linux)のコマンドについても度々登場しますので，Unix系OSの管理についての実務経験があると相当程度に有利です。

★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）

今回のテーマは，①脅威情報調査（マルウェアの検体調査），②インシデントレスポンスチームでした。

問1は，マルウェアに感染した検体の解析作業手順，ARPスプーフィング，パスワード攻撃について扱っています。問題文中で提示されている図表を正しく解釈できる基本知識が備わっていれば，難なく解けました。ある作業が何のために行われるのか，どの作業の前に行うべきかを丁寧に考えながら答えることがポイントです。

問2は，技術的な観点での設問と，セキュリティマネジメントの観点での設問がありました。問1と同様に，問題文中で提示されている図表を正しく解釈できる基本知識と，思考力が試される問題でした。セキュリティマネジメントの観点での設問では，インシデント対応で対応完了までに日数を要した事例から改善点を読み取り，体制を見直すタイミングを考えさせていました。問1よりも技術的な内容が少ないので，こちらの方が解きやすいと感じる受験者もいたかと思います。

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もあります。試験の直前に細かい数値などを復習しておくとよいです。

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をしっかり把握して，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。近年は，情報セキュリティマネジメントだけ

を題材にした問題はありませんが，**情報セキュリティマネジメントを絡ませた問題が出題されることは多くなりました**。

午後II試験では，ネットワークセキュリティに関係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，TLS(SSL)については詳細に学習しておいてください。

■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

・午後問題は，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よいです。

・ネットワークセキュリティ（VLAN，無線LAN，TLS1.3，IPsec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。

・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。