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），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試験要綱より抜粋)

変わりました！

■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（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確保してください**。

テクノロジ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）
　–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）
　–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4～8）
　–ハードウェア（CPU，メモリ，キャッシュのヒット率，周辺装置）
　–システム構成（マルチプロセッサシステム，稼働率，高信頼システム）
　–ページング方式（ページフォルトの回数）
　–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）
　–論理回路（論理演算），組込システム，符号化
　–WEB関連の技術（主にデザイン技術に関すること）
　–コンピュータグラフィクス，動画・画像フォーマット（MPEG1,2,4，JPEGなど）
・ヒューマンインタフェース，コンピュータグラフィックス（問8：出題なしの場合もある）
　–アクセシビリティ，パンくずリスト，SMILなど
　–メタボール，ラジオシティ，シェーディング，テクスチャマッピングなど
・データベース（問9　1～2題）
　–ER図，正規化，DBMS
・ネットワーク（問10，11　1～2題）
　–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12～16）
　–鍵の利用法（主に公開鍵），PKI，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。

R01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，サイドチャネル攻撃，XMLディジタル署名，ダイナミックパケットフィルタリング，CRL，CRYPTREC暗号リスト，クッキーのSecure属性，CVSSなどテキストや問題集で基本事項を学習しておけば正解できる問題（頻出テーマ問題）が多く出題されていました。今回は，FIDO(Fast IDentity Online)，BlueBorneなどの新用語が出題されていました。従来から出題される用語をきちんと正解できれば，新用語については間違えても気にする必要はありません。セキュリティのテーマについては，日頃からウェブなどで情報収集することも大切です。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，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。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）

R01年秋試験には，セキュアプログラミングは出題されませんでした。H31春試験でも，セキュアプログラミングに関する問題は，コードが4行提示されているだけの規模でした。セキュアプログラミングは以前ほど重点を置かない分野になった可能性もあります。少々注意が必要かもしれません。

R01年秋試験の問題のテーマは，①電子メールのセキュリティ，②セキュリティインシデント対応，③標的型攻撃への対応といった内容でした。いずれも基本知識に忠実な標準的な問題です。問題文の分量は，前回まで（H31春）とほぼ同じです。事前対策学習（過去問題演習，分析）を十分に行えば解きやすい問題が多いですが，事前対策学習をしっかりせずに簡単に解けるほどやさしくはありません。

午後Ⅰ試験では，暗号技術や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。ネットワークセキュリティの問題も出題されますので，ネットワークの知識（データリンク層レベルの技術が手薄になりがちです）もしっかり習得しておきましょう。

問番号	H31春試験	R01秋試験
問1	Webサイトのセキュリティ ・サイト間での情報伝達 ・CORS ・HTTPヘッダ	電子メールのセキュリティ対策 ・SPFの効果 ・DKIMの仕組み，効果 ・DMARC
問2	クラウドサービスのセキュリティ ・HSTS ・無線LANのセキュリティ ・OTP	セキュリティインシデント対応 ・ファイアウォール ・マルウェアの活動調査 ・コードサイニング ・プロキシ認証，BASIC認証
問3	IoT機器の開発 ・認証トークンの設計 ・クライアント証明書 ・TPM，耐タンパ性	標的型攻撃への対応 ・初期調査で行う内容 ・マルウェア感染の検知法の改善 ・ログ

★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）

問題のテーマは，①ソフトウェア開発におけるセキュリティ対策，②工場のセキュリティでした。問1は，空欄に単語を補充する問題が大変に多かった点が特徴的です。選択肢から単語を選んで答えるものもありました。

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少なくなりましたが，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。https://www.ipa.go.jp/security/vuln/ssl_crypt_config.htmlで「SSL/TLS暗号設定ガイドライン」が公開されています。参考にするとよいです。また，メールヘッダやHTTPヘッダの解析もできるようにしておきましょう。

問番号	H31春試験	R01秋試験
問1	マルウェア感染と対策 ・インシデント発生とその追跡 ・IEEE802.1x，EAP ・共通鍵方式の暗号モード(ECB，CTR) ・HTTPS復号機能	ソフトウェア開発におけるセキュリティ対策 ・Linuxにおけるコマンドの利用 ・FWフィルタリングルールの設定 ・ファイルの改ざん検知 ・コンテナ技術の活用
問2	情報セキュリティ対策の強化 ・営業機密の要件 ・推奨されている暗号アルゴリズム ・インシデントの調査 ・不正ログイン対策	工場のセキュリティ ・ランサムウェアへの感染 ・APT攻撃の段階 ・データの安全な転送手段の検討 ・セキュリティ規程の見直し

■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。

・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

・**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。**

・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詳しく学習してください

・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，TLS/SSL，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。