情報処理安全確保支援士

1.　はじめに

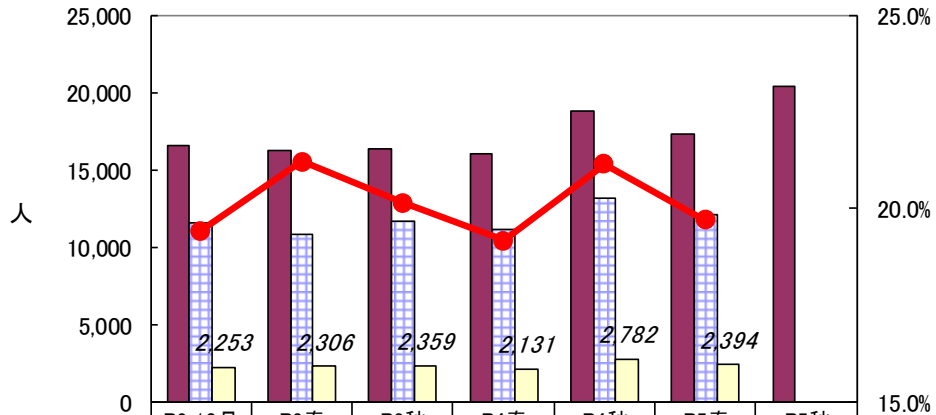
1.1　総評

情報処理安全確保支援士試験(SC 試験)は，これまでの午後Ⅰ・午後Ⅱ試験が今回から午後試験として統合され，記述式問題 4 問中の 2 問を 150 分で解答する出題構成に変更されました。午後の試験時間が 60 分短縮され，受験の負担はかなり減ったと考えます。

午後問題のテーマはさまざまに分散しており，技術者あるいは管理者などそれぞれの立場の人が選択しやすかったでしょう。特異なテーマはなく，公表されていたとおり，試験で問う知識・技能の範囲そのものに変更は見られませんでした。問題文のボリュームは，問題によって大きな差があり，最小のものはこれまでの午後Ⅰ問題と同等で，時間に余裕をもって解答できたと考えます。出題内容の点でも，これまでの午後Ⅱ問題のようにセキュリティ技術面とセキュリティ管理面の両面から幅広く問う総合問題は出題されず，4 問ともどちらかといえば午後Ⅰ問題に近いものでした。その他の特徴としては，解答の制限字数が大幅に長くなったことが挙げられ，正確な専門知識と応用力，解答表現力が求められています。

午前Ⅱ試験には変化はなく，総合的に判断すると，今回の SC 試験は前回よりも易しく，合格率は上がるでしょう。

1.2　受験者数の推移



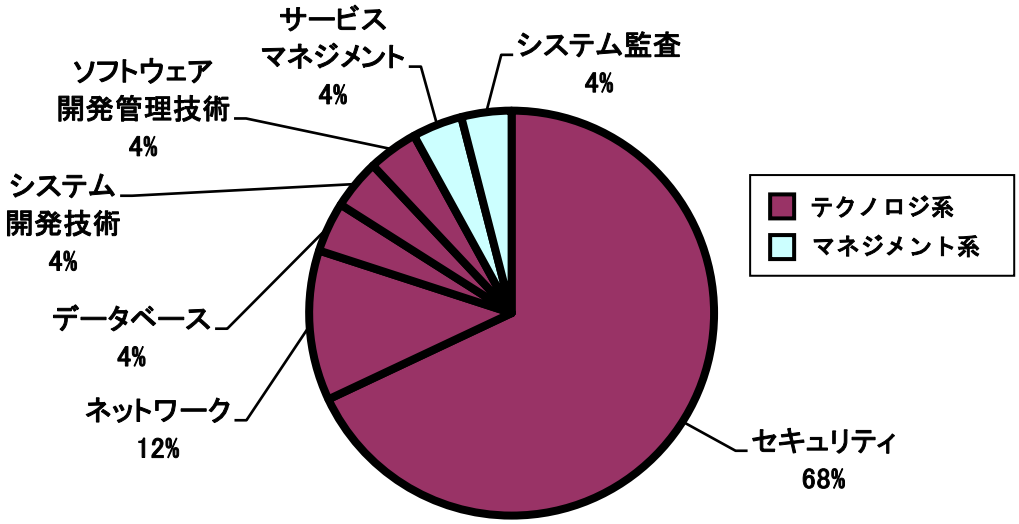
	R2 10月	R3春	R3秋	R4春	R4秋	R5春	R5秋
応募者数	16,597	16,273	16,354	16,047	18,749	17,265	20,432
受験者数	11,597	10,869	11,713	11,117	13,161	12,146	
合格者数	2,253	2,306	2,359	2,131	2,782	2,394	
合格率	19.4%	21.2%	20.1%	19.2%	21.1%	19.7%	

2.　午前Ⅱ問題の分析

2.1　問題テーマの特徴

分野ごとの出題数は毎回同じです。重点分野で技術レベル 4 の「セキュリティ」が 17 問，「ネットワーク」が 3 問出題され，技術レベル 3 の「データベース」「システム開発技術」「ソフトウェア開発管理技術」「サービスマネジメント」「システム監査」の各分野は 1 問ずつの出題です。

出題分野	出題比率	出題数
セキュリティ	68%	17 問
ネットワーク	12%	3 問
データベース	4%	1 問
システム開発技術	4%	1 問
ソフトウェア開発管理技術	4%	1 問
サービスマネジメント	4%	1 問
システム監査	4%	1 問



セキュリティ分野について，小分類に細分化してその内訳を見てみると，暗号化や認証などの情報セキュリティ技術や攻撃手法に関する「情報セキュリティ」からの出題が約半数の 8 問となっています。次いで「セキュリティ実装技術」から 6 問出題されました。「情報セキュリティ対策」の技術的セキュリティ対策からは今回出題されませんでしたが，これら 3 つの小分類が該当する技術知識を問う問題がほとんどを占め，「情報セキュリティ管理」，「セキュリティ技術評価」といった管理知識を問う問題は少ないという傾向に変化はありません。

セキュリティ分野の小分類	出題数			
	R5 秋	R5 春	R4 秋	R4 春
情報セキュリティ	8 問	6 問	8 問	6 問
情報セキュリティ管理	2 問	2 問	0 問	4 問
セキュリティ技術評価	1 問	0 問	1 問	0 問
情報セキュリティ対策	0 問	4 問	2 問	2 問
セキュリティ実装技術	6 問	5 問	6 問	5 問

新規問題は，セキュリティ分野の“クリプトジャッキング”，“SCAP”，“DNSSEC”，“OAuth 2.0”の 4 問，ネットワーク分野の“マルチキャスト通信で使用できる IP アドレス”，“IP アドレスの重複の確認に使用するプロトコル”の 2 問，データベース分野の“DBMS のデータディクショナリ”， システム開発技術分野の“カオスエンジニアリング”の合計 8 問です。ただし，テーマとしては既出のものがほとんどを占め，目新しい用語は“SCAP”と“カオスエンジニアリング”の 2 つです。

そのほかは過去問題の再出題で約 7 割を占めています。このうち SC 試験からの再出題は 11 問で，前回より 2 問減って全体の 4 割強です。他の試験区分からの再出題問題もテーマとしては既出のものがほとんどで，SC 試験での目新しい用語は“公開鍵基盤の CPS”と“アジャイル開発手法のスクラム”の 2 つです。

そのほかの特徴として，SC 試験では，セキュリティ分野以外の分野からもセキュリティと関連性のある問題が出題されることがたびたびありますが，今回は，システムの耐障害性を高める手法である“カオスエンジニアリング”と，“データベースの直接修正に関するシステム監査の指摘事項”の 2 問にその傾向が見られます。

2.2　難易度の特徴

目新しい用語に関するものと，過去問題の再出題であっても久しぶりに出題され，かつ技術レベルが高いと考えられるものなどを難しいと判定しました。

SC 試験からの再出題が前回より 2 問減ったものの，目新しい用語の数は同数で，午前Ⅱ試験の難易度への影響はないといえます。

一方で，再出題される過去問題の年度の範囲が広くなり，過去問題演習の効果が以前と比較するとやや下がっています。以前は 3～5 回前の過去問題から集中的に再出題される傾向があり，過去 5 回分の問題演習は非常に効果的でした。しかし，昨年あたりからそのような偏った傾向は見られなくなり，3～10 回前から少しずつ再出題されるように変化しています。過去問題演習が効果的であることに変わりありませんが，古くまでさかのぼって過去問題演習を行っていなければ対応が難しいものもあります。例えば，“VA の役割”と“XML デジタル署名”はともに複数回出題されたことがありますが，直近で出題されたのは 7 回前です。しかも，紛らわしい選択肢が含まれること，技術レベルが高いことから，難易度は高いと判断しました。

以上のことから，今回の午前Ⅱ試験の難易度は標準的といえます。過去問題演習を行って

いれば，合格基準の 6 割を超えることは難しくないでしょう。

2.3 問題テーマ難易度一覧表

問	テーマ	分野名	難易度
1	OS コマンドインジェクション	セキュリティ	A
2	TLS1.3 の暗号スイート	セキュリティ	B
3	VA の役割	セキュリティ	C
4	XML デジタル署名	セキュリティ	C
5	クリプトジャッキング	セキュリティ	A
6	マルウェア Mirai	セキュリティ	B
7	トランザクション署名	セキュリティ	B
8	SAML	セキュリティ	B
9	公開鍵基盤における CPS	セキュリティ	C
10	NOTICE	セキュリティ	B
11	JIS Q 27000 における情報セキュリティリスクに関する記述	セキュリティ	B
12	SCAP	セキュリティ	C
13	DNSSEC	セキュリティ	B
14	OAuth 2.0	セキュリティ	C
15	SSH	セキュリティ	A
16	IMAPS	セキュリティ	A
17	ファイアウォールのフィルタリングルールの変更	セキュリティ	A
18	サブネット分割時のサブネットマスク	ネットワーク	A
19	マルチキャスト通信で使用できる IP アドレス	ネットワーク	A
20	IP アドレスの重複の確認に使用するプロトコル	ネットワーク	B
21	DBMS のデータディクショナリ	データベース	B
22	カオスエンジニアリング	システム開発技術	C
23	アジャイル開発手法のスクラム	ソフトウェア開発管理技術	C
24	内部監査	サービスマネジメント	B
25	データベースの直接修正に関するシステム監査の指摘事項	システム監査	A

注)難易度は 3 段階評価で，C が難，A が易を意味する。

3. 午後問題の分析

3.1 全体の出題傾向及び難易度について

今回の午後試験は，午後Ⅰ・午後Ⅱ試験が統合されてから初めての午後試験でした。これまで午後Ⅰ試験では技術知識中心に問われ，午後Ⅱ試験では管理知識も含めた総合問題となる傾向がありました。今回，総合問題は出題されず，技術知識中心が3問，管理知識中心が1問という出題構成でした。これは，情報処理安全確保支援士試験の前身である情報セキュリティスペシャリスト試験が，さらにその前身である技術寄りのテクニカルエンジニア(情報セキュリティ)試験と管理寄りの情報セキュリティアドミニストレータ試験が統合された試験だったことからも妥当であると考えています。情報セキュリティスペシャリスト試験の午後Ⅰ試験は，平成25年度春までは4問出題中，2問解答する形式で，技術知識中心が3問，管理知識中心が1問という構成で出題されることが多かったことから，それが再現されているような印象を受けました。

出題された大枠のテーマは，Webアプリケーションの脆弱性，セキュリティ対策の見直し，インシデント対応，リスクアセスメントの4問で，いずれも過去に午後Ⅰ・午後Ⅱ試験で取り上げられたことがあるテーマです。2022年12月のSC試験における出題構成等の変更の発表時に，試験で問う知識・技能の範囲そのものに変更はないことが明示されていたとおり，今回問われた知識・技能の範囲に変化はありませんでした。

難易度について知識レベルの点から見ると，これまでの午後Ⅱ試験で出題されていた総合問題での事例内容の複雑さや，知識の幅や深さはなく，4問ともどちらかといえば午後Ⅰ問題に近いといえます。これまでとは異なる点は，いずれの問題でも解答の制限字数が大幅に長くなり，特に問4は制限がまったくなかった点です。短い制限字数の場合は，さまざまな条件によって絞り込めるように，ヒントとなる記述が問題文や設問文に設定されていることがよくあります。一方，今回のように長い字数で解答する場合は，仕組み，理由，攻撃方法などを適切に説明できる，より正確な専門知識と思考力が必要とされ，解答表現力も求められます。要求される知識の正確性といった点で，これまでの午後Ⅰ試験より，やや難しいと考えられます。

問題文のボリュームは，最小で5ページ，最大で9ページでした。これまでの午後Ⅰ問題は概ね5～6ページ，午後Ⅱ問題は11～13ページだったことから，両者の間の分量であるとはいえ，このように問題ごとに大きな差があることは予想外でした。最小のものはこれまでの午後Ⅰ問題と同等のボリュームですが，解答にかけられる時間は，(問題選択に要する時間を考慮しなければ)1問当たり45分から75分へと増えたことから，時間的難易度は低くなっています。一方，ボリュームの大きな問題2問を選択した場合は，読解に時間がかかり，解答時間に余裕はなかったかもしれません。

以上のことから，今回の午後試験は，知識面，時間的な面ともに前回の午後Ⅰ・午後Ⅱ試験全体と比較すると，易しくなりました。

3.2　各問題のテーマ，特徴

問1は「Webアプリケーションプログラムの開発」というテーマで，過去に毎回のように出題されてきたセキュアプログラミングの問題です。HTML のソースとスクリプトが提示され，クロスサイトスクリプティング(XSS)の脆弱性について取り上げられています。問題文が 5 ページと少なく，脆弱性は頻出テーマといえる XSS のみに絞られていることから，開発者にとっては取り組みやすい問題でしょう。XSS は前回の春にも午後Ⅱ試験で出題されています。プログラムの処理内容や，攻撃者が情報を取得する方法を長文で解答させる問題が含まれ，HTML とスクリプトのプログラムを読み取る能力は必須です。プログラム経験の有無によって，難易度の感じ方は両極端となると考えられることから，標準的な難易度と判断しました。

問2は「セキュリティ対策の見直し」というテーマで，オフィスの無線LAN環境を悪用した攻撃を防ぐためのセキュリティ対策の見直しについて出題されました。無線 LAN，VLAN，ファイアウォールのフィルタリング設定，サーバ証明書の検証，HSTS，EAP-TLS，TPM など，午後試験 4 問の中では最も幅広い知識が必要とされていますが，いずれも頻出の知識項目であることから，知識レベルはそれほど高くありません。問題文が9ページあり，ファイアウォールのVLAN設定やフィルタリング設定，アクセスポイントの設定など，多くの図表が提示されていることから，時間的な難易度はやや高めですが，事例に設定されている条件を丁寧に読み取っていけば解答できるものが多く含まれています。したがって，難易度は標準的と判断しました。

問3は「継続的インテグレーションサービスのセキュリティ」というテーマで，クラウドサービスを利用したソースコード管理に関するインシデント対応の問題です。コンテナ仮想化，サーバ証明書の偽装，ドメインフロンティング，WebAuthn，コードサイニング証明書とコード署名，FIPS 140-2 Security Level 3 などの知識が必要とされ，他の3問より知識レベルが高い問題です。初出題の知識は，ドメインフロンティングと FIPS 140-2 Security Level 3 の2つです。FIPS 140-2 は午前Ⅱ試験でたびたび出題されていますが，レベルまで問われたことはなく，レベルを考慮しないと誤った解答になってしまう可能性があります。コンテナ仮想化は，平成30年春の午後Ⅱ試験で出題されたことがあり，そのときはコンテナの特徴や利用イメージが問題文中で説明されていましたが，今回はまったくなく，知識レベルが上がっています。このように，複数の知識レベルの高い設問が含まれていますが，そのほかの知識項目は，過去に何度か出題されており，同一の論点が問われたものもあることから，ある程度対応できたと考えられます。また，問題文が6ページと少なく，解答時間が足りないということはないでしょう。以上のことから，難易度はやや高いと判断しました。

問4は「リスクアセスメント」というテーマで，顧客情報を扱う配送業務を委託している企業におけるリスクアセスメントに関する管理寄りの問題です。リスクアセスメントの出題は，平成28年秋の午後Ⅱ試験以来です。企業のセキュリティ設定，リスクアセスメントの手順，リスクレベルの基準を読み取り，リスクアセスメントの結果表を完成させ，追加の管理策を問う流れになっています。特徴としては，リスク源による行為を解答する設問が，

問題文の状況設定に沿う範囲で“受験者の知見に基づいて答える”という記述式問題では珍しい出題形式となっており，制限字数の設定もなく，自由度が高いといえます。複数の正解例が出されることも考えられますが，この設問に関連する設問がほかに 6 問あるので，最初の設問が不正解の場合，全て不正解となる可能性があります。技術的知識レベル，管理的知識レベルともに高くはありませんが，持っている知識を総動員して問題事例にどの知識を結びつけるべきか慎重に考える必要があります。問題文が 9 ページあり，読解にも時間を要する問題です。したがって，難易度はやや高いと判断しました。

なお，各問題の難易度は，これまでの午後Ⅰ問題と比較した場合で評価しています。

3.3 問題テーマ難易度一覧表

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

注)難易度は 3 段階評価で，C が難，A が易を意味する。

4. 今後の対策

4.1 午前Ⅱ対策

午前Ⅱ試験は，重点分野の「セキュリティ」と「ネットワーク」の 2 分野の合計が 8 割を占めます。午前Ⅱ試験の合格基準は 60 点以上なので，この 2 分野で取りこぼすことなく確実に得点できれば，午前Ⅱ試験に合格できます。したがって，「セキュリティ」と「ネットワーク」の 2 分野に的を絞って学習するほうが効率もよくお勧めです。そのほかの分野については，技術レベルが 3 であることも考慮すると，話題となっている用語をチェックしておく程度でよいでしょう。

セキュリティやネットワークに関する学習は，まずはテキストを用いて体系的に知識を習得することが大切です。そのほうが知識の関連性も把握しやすく，単独の知識を詰め込むよりも学習効果が高いでしょう。この 2 分野の知識はそのまま午後試験でも必須の知識となるので，一度体系的な学習を行っておくことで，午前Ⅱ対策から午後対策へとスムーズに移ることができます。特に出題されやすいのが，攻撃，認証技術，PKI です。さまざまな攻撃手法とその対策について，暗記するのではなく，仕組みをよく理解するように学習してください。例えば，同じ攻撃を取り上げていても視点を変えて出題されることがよくあり，丸暗記しただけでは対応できない可能性があります。認証技術では今回出題された SAML や IEEE802.1X は定番となっています。PKI については，認証局の役割のほか，認証局の階層構造に基づいて証明書の信頼性を保証する仕組み，証明書の構成，証明書発行手順，失効確認など，午後対策も見据えて体系的に学習しておくとよいでしょう。

過去問題の再出題率は，他の試験区分も含めると約 7 割と高く，SC 試験に限定しても 5 割近くあることから，知識習得後に過去問題演習を行うことは必須です。過去問題演習も「セキュリティ」と「ネットワーク」の 2 分野に絞って効率的に行うとよいでしょう。以前は 3～5 回前の過去問題から集中的に再出題される傾向がありましたが，最近は範囲が広がり，3～10 回前から少しずつ再出題されるように変化してきているため，過去 10 回分程度は演習しておくとよいでしょう。演習後は正解した場合でも必ず解説を読み，誤答の選択肢についての知識も確認しておくと，知識が広がり，類似問題が出題された場合にも対応できるようになります。問題演習を通じて苦手なテーマを洗い出し，あいまいな知識をテキストなどで再確認すると，弱点補強に役立ちます。

また，IPA のホームページに掲載されている「情報処理安全確保支援士試験　シラバス追補版(午前Ⅱ)」には，午前Ⅱにおける知識の細目が示されています。具体的な用語例が掲載されているので，確認しておくとよいでしょう。特にシラバス改訂時に追加された用語は出題されやすい傾向があるので，注意してください。

さらに，新しい攻撃や認証技術について出題されることがたびたびあるので，日頃から IT 関連のニュースに注目し，新しい攻撃やセキュリティ技術についての情報収集を行っておくと役立つでしょう。IPA や NICT のホームページで公開されているセキュリティ情報もチェックするとよいと思います。

4.2　午後対策

これまで，午後Ⅰ試験では技術知識中心に問われ，午後Ⅱ試験では管理知識も含めた総合問題となる傾向があったことから，午後Ⅰ対策としては技術知識中心に学習し，午後Ⅱ対策としてはそれにプラスして管理知識を補強することをお勧めしてきました。統合された午後試験では，試験で問う知識・技能の範囲そのものに変更はなく，今回は技術知識中心の問題が 3 問と管理知識中心の問題が 1 問出題されたことから，午後対策としてはこれまでの午後Ⅱ対策と同様に，技術知識中心に学習を行い，それにプラスして管理知識を補強する方法がよいでしょう。

まず必要となるのは，より深い知識の習得です。午前Ⅱレベルの知識だけでは，問題事例の内容を正しく理解することはできません。今回のように長文で解答する形式が今後も続くことが考えられ，より正確な深い知識が必要となります。よく出題される技術は，アクセス管理，マルウェア対策，暗号技術，認証技術，ログ管理，ネットワークセキュリティ，Web アプリケーションセキュリティ，メールシステムのセキュリティ，DNS のセキュリティ，PKI，無線 LAN セキュリティ，TLS，プロキシサーバなどです。これらについて，重点的に学習し，理解を深めておいてください。

最近特に出題が増えているのがアイデンティティ管理の問題です。IDaaS を用いた SAML 認証や FIDO 認証，WebAuthn などは認証の仕組みを手順も含めて把握しておきましょう。

Web アプリケーションの脆弱性も頻出テーマの一つです。クロスサイトスクリプティング，クロスサイトリクエストフォージェリ，SQL インジェクションなどを中心に学習しておくとよいでしょう。IPA の“安全なウェブサイトの作り方”に掲載されている内容から出題されることがよくあるので，活用すると効果的です。そのほか，C++ではバッファオーバーフローについて出題されており，その対策技術として DEP などいくつかの技術が繰り返し問われていますので，ひととおり確認しておいてください。プログラム経験がない場合はセキュアプログラミング問題を選択しないというのも一つの方法ですが，Web アプリケーションの主な脆弱性に関する知識は持っておきましょう。

セキュリティ管理面の知識としては，ISO や JIS のセキュリティ関連の規格は最近出題が増えているので，確認しておくとよいでしょう。そのほか，人的管理，リスク管理，脆弱性評価指標，サイバーセキュリティ基本法，個人情報保護法，不正競争防止法などについて，知識を習得しておいてください。セキュリティ関連法規は，午前Ⅱ試験では出題範囲外ですが，午後試験では出題範囲に含まれているので，注意が必要です。

また，午後対策としては，ネットワーク技術知識の習得も重要です。問題事例には多くのプロトコルが出てきます。IP，ARP，TCP，UDP，DNS，HTTP，SMTP，NTP，DHCP，SSH，LDAP などの知識は，問題文を読み取るうえで必須となります。午前Ⅱで出題されるような用語説明レベルの知識では不十分なので，ネットワークの知識の再確認を行い，知識の補充をするとよいでしょう。

そして，午前Ⅱ対策と同様に，午後対策でも必ず問題演習を行うことが重要です。実務経験が少ない場合は特に，さまざまな問題演習を通して実務に近い事例を見ておくことは非

常に有効です。事例には，ネットワーク構成図が提示されることもよくあります。通信の流れがどのようになっているかを，事例中の記述，ファイアウォールのルール，ネットワーク構成図を照らし合わせて把握できるようにしておきましょう。

知識を持っていても問題事例に合わせて知識を適用させることができない場合は，読解力不足であると考えられます。また，事例内容とは異なる自分の経験だけから解答を導いてしまい，正解を得られないこともあります。「問題文を図表も含めてよく読む」「設問文の要求に答える」ということは当たり前のことですが，久しぶりに受験する場合はおろそかになりがちです。試験に慣れるためにも，数多くの過去問題演習を行うとよいでしょう。午後Ⅰ・午後Ⅱ試験の過去問題は，問題文のボリュームが午後試験とは異なりますが，事例の流れや問われるポイントは共通点が多く，午後Ⅰ・午後Ⅱ試験の過去問題演習は学習効果が高いと考えます。知識不足で不正解だった場合は知識の補充を行うなど，演習後に復習することが大切です。正解できなかった設問をチェックしておき，時間を空けて同じ問題を繰り返し解くことも効果的です。

特に，セキュリティインシデント対応の問題が午後Ⅰ・午後Ⅱ試験で頻繁に出題されていたことから，インシデント対応の流れに沿って学習することは欠かせません。インシデント対応に関する過去問題をピックアップして集中的に演習を行うのも効果的です。そして，異常が発生しているPCを特定するのに必要となるログの解析の仕方やネットワークコマンドの表示結果の見方，証拠を保全するための手順や注意点，マルウェア感染範囲や感染経路を特定するためのFWルールの設定，マルウェア対策ソフトや脆弱性修正プログラムの運用上の注意点，出口対策としてのフィルタリングの設定など，共通的な知識を洗い出して習得しておくと，さまざまなインシデント対応事例の問題に活用できるでしょう。

午後問題を解くときの注意点としては，重要と考えられる字句や，関連性があると思われる記述には線を引いたり，しるしをつけたりするなど，ポイントを見落とさない工夫をするということです。問題文の余白を活用するのもよいでしょう。過去問題演習を行う段階から意識して自分なりのルールを決めておくことをお勧めします。

令和6年度春期の情報処理技術者試験・情報処理安全確保支援士試験の対策もTACにお任せください！

＜企業ご担当者様へ人気のおススメコースをご紹介＞

合格に必要な知識を効率よくマスターできるコンテンツ

情報処理安全確保支援士Webコース

情報処理安全確保支援士受験のためのベーシックコースです。少ない時間で効率的に学習ができるように専門知識の重要論点を集約したポイント講義（Web動画）は、20テーマ（1テーマあたり30分）を配信します。

試験対策	42,000円（10%税込）
午前Ⅰ免除	36,000円（10%税込）

充実した添削指導の午後Ⅱ対策が合格のポイント

ITストラテジストWebコース

午前・午後の試験に対応したアウトプットトレーニングで、知識の定着を図ります。講義動画（全4回、1回あたり30分）は午後Ⅰの分析と解法テクニック、論述式問題への取組み方を具体的な問題で解説します。

試験対策	54,000円（10%税込）
午前Ⅰ免除	48,000円（10%税込）

合格に必要な知識を効率よくマスターできるコンテンツ

ネットワークスペシャリストWebコース

少ない時間で効率的に学習ができるように工夫されたコースです。専門知識（午前Ⅱ）の重要論点を集約したポイント講義は、20テーマ（1テーマあたり30分）を配信します。

試験対策	42,000円（10%税込）
午前Ⅰ免除	36,000円（10%税込）

充実した添削指導の午後Ⅱ対策が合格のポイント

ITサービスマネージャWebコース

午前・午後の試験に対応したアウトプットトレーニングで、知識の定着を図ります。講義動画（全4回、1回あたり30分）は午後Ⅰの分析と解法テクニック、論述式問題への取組み方を具体的な問題で解説します。

試験対策	54,000円（10%税込）
午前Ⅰ免除	48,000円（10%税込）

充実した添削指導の午後Ⅱ対策が合格のポイント

システムアーキテクトWebコース

午前・午後の試験に対応したアウトプットトレーニングで、知識の定着を図ります。講義動画（全4回、1回あたり30分）は午後Ⅰの分析と解法テクニック、論述式問題への取組み方を具体的な問題で解説します。

試験対策	54,000円（10%税込）
午前Ⅰ免除	48,000円（10%税込）

知識の総整理を短期間で行う問題演習中心のコース

応用情報技術者 徹底演習コース

学習経験者、再受験者対象の午後試験対策コースです。午後試験の出題分野ごとに出題頻度や重要度の高いテーマを精選しました。その解法を学び、短期間で効率よく知識の総整理と得点力アップを目指します。

23,100円（10%税込）

※上記コースは2024年春試験向けコースとなります。各コース名はTAC法人向け人材教育サービス紹介サイト「TAC.biz」の当該コース紹介ページへのリンクとなっております。なお、2024年秋試験向けコースにつきましては、別途ご案内いたします（2024年春頃を予定しています）。

お問合せはこちら

TAC株式会社 法人事業部

東日本エリア：東京都千代田区神田三崎町3-2-18 | 03-5276-9802

東海・北陸エリア：名古屋市中村区則武1-1-7 NEWNO名古屋駅西8F | 052-977-1051

西日本エリア：大阪府大阪市北区中崎西3-4-12 梅田センタービル5F | 06-6371-1075