情報処理安全確保支援士

1.　はじめに

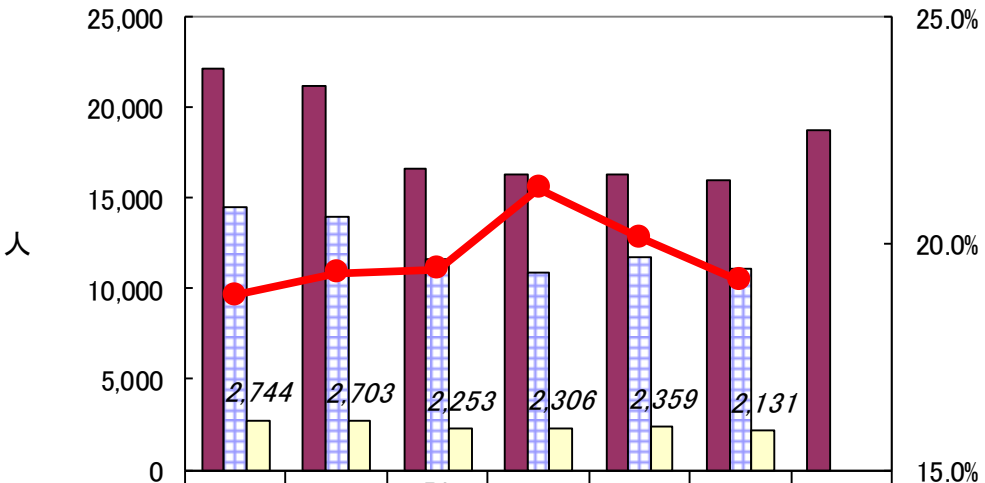
1.1　総評

今回の情報処理安全確保支援士試験(SC)は，午前Ⅱ・午後Ⅰ・午後Ⅱのいずれの試験も定番テーマからの出題が多く，前回より取り組みやすかったと思います。特に午後試験では頻出のセキュリティインシデント対応に関する問題が，午後Ⅰで2問，午後Ⅱでも1問出題され，過去問題演習で対策できていた受験者が多かったのではないかと考えられます。

今回の午後試験は詳細なセキュリティ技術知識が問われる難問はほとんどなく，思考力を重視した出題内容となっています。基本的なセキュリティ技術知識とセキュリティ管理知識，ネットワーク技術知識をもとに，問題事例の具体的な状況や設問の条件に従って思考しながら解答を導くものが多く出題されました。限られた時間内に事例内容を正確に読み取る必要がありますが，いずれの問題も時間的に厳しいということはないでしょう。

総合的に判断すると，今回の試験全体の難易度は標準的なレベルだと考えられます。

1.2　受験者数の推移



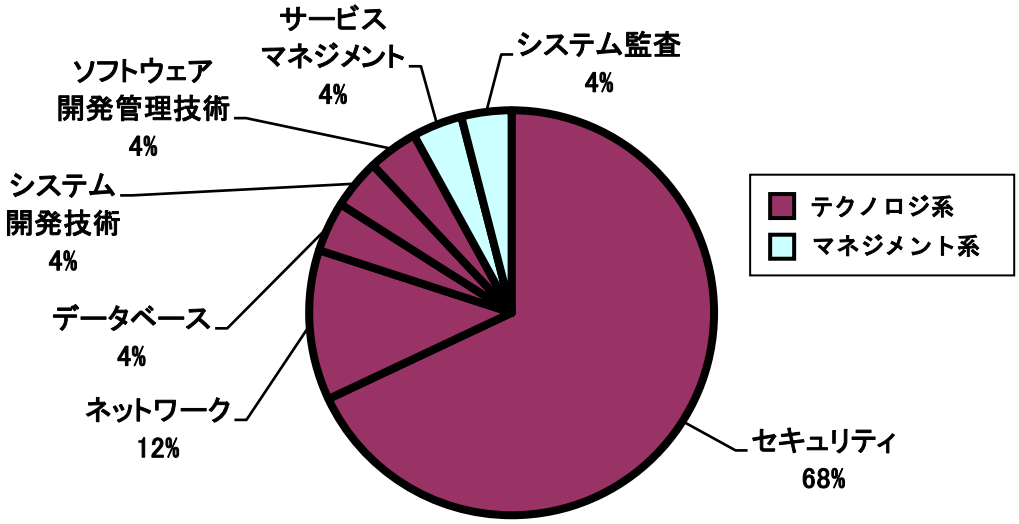
	H31春	R1秋	R2 10月	R3春	R3秋	R4春	R4秋
応募者数	22,175	21,229	16,597	16,273	16,354	16,047	18,749
受験者数	14,556	13,964	11,597	10,869	11,713	11,117	
合格者数	2,744	2,703	2,253	2,306	2,359	2,131	
合格率	18.9%	19.4%	19.4%	21.2%	20.1%	19.2%	

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，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,「情報セキュリティ対策」から 2 問となっており，技術知識がほぼすべてを占めています。「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 1 問のみで，前回 4 問も出題された「情報セキュリティ管理」からの出題はありませんでした。前回とだけ比較すると傾向が変わったように感じられますが，それ以前の分類を見ると，管理知識を問う問題は非常に少なく，前回が特異なケースだったことが分かります。

セキュリティ分野の小分類	出題数			
	R4 秋	R4 春	R3 秋	R3 春
情報セキュリティ	8 問	6 問	9 問	6 問
情報セキュリティ管理	0 問	4 問	1 問	1 問
セキュリティ技術評価	1 問	0 問	1 問	1 問
情報セキュリティ対策	2 問	2 問	2 問	4 問
セキュリティ実装技術	6 問	5 問	4 問	5 問

セキュリティ分野の新規問題は，次のとおりです。

・メッセージ認証符号付きメッセージの送信
・パスワードスプレー攻撃
・シングルサインオン
・ISO/IEC 15408
・クリックジャッキング攻撃対策

このうち，初出題の用語は“パスワードスプレー攻撃”の 1 問のみで，前回の 4 問から大幅に減少しています。

その他の分野の新規問題は，ネットワーク分野の“IPv6 の特徴”，データベース分野の“LEFT OUTER JOIN の実行結果”，サービスマネジメント分野の“投資利益率の計算”の 3 問です。IPv6 に関連する問題が出題されるのは平成 25 年春以来 9 年半ぶりです。データベース分野から SQL 文が出題されることは時々ありますが，その場合ほとんどは権限付与に関する GRANT 文であり,今回のようにセキュリティと関連性の薄い問題は珍しい出題です。

2.2 難易度の特徴

今回の午前Ⅱ試験は，新規問題であってもテーマとしては既出のものが多く，初出題の用語が減ったという点では，前回より難易度が高い問題が少なかったといえます。

一方で，過去問題の再出題に変化が見られ，過去問題演習の効果が例年ほど高くはありませんでした。これまでは，3～5 回前の過去問題から再出題される傾向があり，特に 3 回前からが多く，前回は 8 問も出題されました。そのため，3 回前を含めた過去問題演習を行うことは非常に効果的でした。しかし今回は，そのように偏った傾向は見られず，古い年度からの再出題や SC 試験以外の試験区分からの再出題が前回よりも増え，過去問題演習を行っていれば問題を見た瞬間に解答が浮かぶような再出題問題が例年より少なかったと思います。例えば，“未使用の IP アドレス空間を使った DoS 攻撃”，“前方秘匿性”，“IPsec”などはネットワークスペシャリスト試験や応用情報技術者試験で過去に出題された問題です。ただし，DoS 攻撃や IPsec は SC 試験でも過去に何度も出題されたことがあるテーマで，前方秘匿性も午後試験で取り上げられたことがある最近注目されているテーマなので，対応できた可能性は高いと考えられます。

以上のことから，今回の午前Ⅱ試験はやや易しいと判断しました。

2.3 問題テーマ難易度一覧表

問	テーマ	分野名	難易度
1	メッセージ認証符号付きメッセージの送信	セキュリティ	C
2	PKI の RA の役割	セキュリティ	C
3	SAML	セキュリティ	A
4	Smurf 攻撃	セキュリティ	A
5	未使用の IP アドレス空間を使った DoS 攻撃	セキュリティ	B
6	パスワードスプレー攻撃	セキュリティ	C
7	シングルサインオン	セキュリティ	C
8	前方秘匿性	セキュリティ	B
9	ISO/IEC 15408	セキュリティ	B
10	CASB の効果	セキュリティ	B
11	クリックジャッキング攻撃対策	セキュリティ	B
12	ブロックチェーン	セキュリティ	B
13	IPsec	セキュリティ	B
14	SMTP-AUTH	セキュリティ	A
15	SPF 導入時の設定	セキュリティ	A
16	メール暗号化の公開鍵を用意する単位	セキュリティ	B
17	無線 AP のプライバシーセパレータ機能	セキュリティ	B
18	IPv6 の特徴	ネットワーク	C
19	クラス D の IP アドレス	ネットワーク	A
20	VRRP	ネットワーク	B
21	LEFT OUTER JOIN の実行結果	データベース	B
22	判定条件網羅のテストケースの組合せ	システム開発技術	A
23	SD メモリカードの著作権保護技術	ソフトウェア開発管理技術	B
24	投資利益率の計算	サービスマネジメント	A
25	SaaS へのアクセスコントロールの評価	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Ⅰ問題の分析

3.1 全体の出題傾向及び難易度について

午後Ⅰ試験は，セキュリティインシデント対応の問題が2問，Webアプリケーションの脆弱性の問題が1問という構成で，いずれも定番テーマからの出題です。過去問題演習を行っていた受験者にとっては取り組みやすいテーマといえるでしょう。

3問とも詳細なセキュリティ技術知識を要求するような設問はなく，セキュリティとネットワークの基本的な知識を事例に適用させて解答を導く応用力や思考力が問われるような試験でした。特にセキュリティインシデント対応に関する2問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。また，正確にインシデント内容を読み取るには読解力が必要とされますが，いわゆる国語力だけで読み取れるわけではなく，正確に読み取るためのベースとなる幅広いセキュリティ知識とネットワーク知識は必須です。知識的な面では，標準的な難易度でしょう。

問題文の分量は3問とも6ページで，平均的です。今回は3問とも細かい図表が多く提示されており，特に問2は図が2点，表が8点と午後Ⅰ問題にしては非常に多く，読解には多少時間がかかったかもしれません。

以上のことから，知識面と時間的な面の両方から判断すると，今回の午後Ⅰ試験の難易度は標準的でしょう。

3.2 各問題のテーマ，特徴

問1は，IoT製品の開発において各機能のセキュリティ対策や脆弱性について検討するという事例内容です。具体的には，ファームウェアアップデートにおけるDNSキャッシュポイズニング,製品のWebアプリケーションプログラムに対するOSコマンドインジェクション，クロスサイトリクエストフォージェリの3つの脆弱性を悪用した攻撃が取り上げられています。他の2問と比較すると，知識そのものを解答させる設問が多く，攻撃や脆弱性の名称，攻撃の仕組み，証明書の種類などがストレートに問われています。各攻撃の仕組みに関する設問は30～50字の記述式となっており，正確に表現できる知識レベルが求められますが，そのほかは3つの攻撃とも出題頻度が高いことや解答群が用意されているものもあることを考慮すると，容易に正解を導けるでしょう。したがって，時間的にも3問の中では最も余裕があり，難易度はやや易しいと考えられます。

問2は，脆弱性に起因するセキュリティインシデントへの対応というテーマで，インシデントが発生したサーバの調査，その他のサーバの調査，再発防止策の検討という流れになっています。インシデントが発生したサーバの調査では，サーバのプロセスとコネクション一覧からの通信先の特定や，利用しているソフトウェアの脆弱性及びそれを悪用した攻撃の内容とFWの通信ログの調査をもとにした攻撃の流れの把握などを行います。プロセス一覧，コネクション一覧，サーバのアクセスログ，FWの通信ログの4つの表から解答を導くための情報を読み取っていく必要があります。高い知識レベルは要求されていないものの，表か

ら必要な情報を読み取る知識，脆弱性と攻撃手法を理解する知識など，基本的なセキュリティとネットワークの知識は必須です。その他のサーバの調査では攻撃が失敗した理由などが問われ，再発防止策では URL フィルタリングルールの具体的な設定内容が問われています。このように，知識をそのまま解答するのではなく，事例内容を読み取り，思考しながら具体的な解答を導く思考力や知識の応用力を重視した問題となっています。以上のことから，難易度は標準的と判断しました。

問 3 もセキュリティインシデントへの対応がテーマとなっており，ゲームアプリの更新時にゼロデイ攻撃を受けたという事例内容が取り上げられています。問題文中に提示された各サーバの概要とゲームアプリの更新手順を把握したうえで，発生したインシデントによる被害の調査，再発防止策や被害低減策の検討を行うといった流れは，問 2 と似通っています。悪意のあるプログラムコードに攻撃者が指示した内容，被害の拡大を防止するための対処など，具体的な解答を導く思考力や知識の応用力を要求する設問が多く含まれている点も問 2 と共通しています。知識レベルもそれほど高くなく，コンテナ，REST API といった比較的新しい用語が問題文中に出てきますが，設問に大きく影響することはありません。以上のことから，問 3 も問 2 と同様に難易度は標準的でしょう。

3.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	IoT 製品の開発	A
2	脆弱性に起因するセキュリティインシデントへの対応	B
3	オンラインゲーム事業者でのセキュリティインシデント対応	B

注)難易度は 3 段階評価で，C が難，A が易を意味する。

4. 午後Ⅱ問題の分析

4.1 全体の出題傾向及び難易度について

午後Ⅱ試験は，セキュリティ技術に加えて，セキュリティ管理からの出題も含まれた総合問題となることが多い傾向があります。今回も，問 1 はマルウェアに感染した検体の調査という技術面での出題が中心でしたが，一部でログの取得の運用についての改善点が問われ，問 2 は定番のインシデント対応についてマルウェアの検知に関する技術面と運用体制に関する管理面の両面から問われる総合問題となっています。

午後Ⅱ試験も午後Ⅰ試験と同様に，詳細なセキュリティ技術知識が必要とされる設問はなく，セキュリティとネットワークの基本的な技術知識・管理知識を事例に適用させて解答を導く応用力や思考力が問われるような試験でした。知識レベルとしては 2 問とも標準的でしょう。

一方で，管理面での出題は，解答表現を一意に定めることが難しい傾向があり，今回の問 2 でも解答表現の作成に時間を要するものがありました。その点，問 1 は解答群から選ぶものが半数以上を占めていたため，解答表現に時間を費やすことはほとんどないでしょう。

問題文の分量は問 1，問 2 ともに 13 ページで平均より多いですが，前回のように 3 ページも差があるために受験者が得意なほうのテーマを選択するかどうか悩むといったことはなかったと思います。提示されている図表の数は 2 問とも非常に多く，図表間には関連性があるものもあり，脚注も含めて必要な情報を読み落とさないように慎重に読解していく必要があります。

以上のことから，午後Ⅱ試験全体としては標準的な難易度ですが，2 問を比較すると時間的な難易度の点から問 2 のほうがやや難しいと評価します。

4.2 各問題のテーマ，特徴

問 1 は，脅威情報を調査する部門における模擬攻撃試験を題材に，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，運用の改善提案などが問われています。解析作業手順については，ネットワーク構成や通信制御ルール，現在のファイル転送手順をもとに，マルウェア感染拡大を考慮した新しいファイル転送手順が問われています。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順に思考しながら解答を導きます。ARP スプーフィングについては，平成 29 年春の午後Ⅰ問題で取り上げられています。ARP の特徴や中間者攻撃を行うことが目的である点を理解しておく必要があります。解答数が多いため，この点を理解していないと大きく得点を落としてしまうことにつながるでしょう。パスワード攻撃対策としては，パスワードのハッシュ化で利用されるソルトは平成 27 年春以来の出題，ストレッチングは初出題です。問 1 では詳細なセキュリティ技術知識は要求されておらず，事例内容を正確に読み取ることができれば解答可能な設問が複数含まれています。問題文には図が 9 点と表が 10 点と非常に多くの図表が提示されており，それらを組み合わせながら解釈していく必要があります。難易度を知識面，時間的な

面の両方から判断すると，標準的でしょう。

問 2 は，マルウェアの検知というインシデントに対して，解析や再発防止策などの技術的な面と，インシデントの重大さを考慮した運用体制の組替えといった管理的な面から出題されています。マルウェアの検知では 2 種類のマルウェアについて取り上げられており，混同しないように読み進めていく必要があります。EDR 製品で記録されたイベント情報をもとにマルウェアを解析する設問では，どのファイルからどのファイルへ感染拡大していくかが具体的に問われています。運用体制については，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などの管理的な知見が求められています。問 1 と同様に詳細な知識は問われておらず，知識レベルとしては標準的でしょう。問 1 のように ARP スプーフィングといった特定の技術知識が要求されていない分，問 2 のほうが取り組みやすいと感じる受験者もいるかもしれません。一方で，問 2 では，マルウェアを検知するための EDR の検知ルールを問う設問が 4 問出題されており，これをどう表現するかが難しいといえます。何を検知すればよいかは比較的容易に判断できますが，それを EDR の検知ルールの仕様に基づいてルール化する段階で思考力が要求されます。このように解答に時間を要する設問も含まれていますが，時間的な難易度が高いというほどではなく，総合的に判断すると，問 2 の難易度も標準的でしょう。

4.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	脅威情報調査	B
2	インシデントレスポンスチーム	B

注)難易度は 3 段階評価で，C が難，A が易を意味する。

5. 今後の対策

5.1 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試験に合格する基準は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。

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。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が 6〜7 割と高いことから，知識習得後は過去問題演習が必須です。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。できるだけ多くの過去問題演習を行うのに越したことはありませんが，少なくとも直近5回分は繰り返し行ってください。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。これまでは特に3回前からの再出題率が高い傾向があったことから，試験直前に 3 回前の過去問題演習を行うことをお勧めしていましたが，今回はそのような傾向は見られませんでした。古い年度からの再出題や SC 試験以外の試験区分からの再出題が前回よりも増え，例年ほど過去問題演習の成果が直結しなかったかもしれません。しかし，出題テーマが大きく変わったわけではないことから，過去問題演習の効果は間違いなくあるといえます。

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。

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。

5.2　午後Ⅰ対策

午後Ⅰ対策で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。たとえ，問題文中に解答のヒントとなる記述があっても，気付くことさえできないかもしれません。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。

また，セキュリティインシデント対応の事例が午後Ⅰ・午後Ⅱ試験ともに頻繁に出題されていることから，インシデント対応の流れに沿って学習することも欠かせません。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。

最近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認証などは認証の仕組みを手順も含めて把握しておいてください。

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，活用するとよいと思います。そのほか，C++ではバッファオーバフローについて出題されています。その対策技術としては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くとよいでしょう。

午後Ⅰ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。今回はIP，ARP，UDP，DNS，HTTP，LDAPなどの知識が必要とされましたが，そのほかTCP，SMTP，NTP，DHCP，SSH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ですので，午後問題演習に入る前にネットワークの知識の再確認をするとよいでしょう。

そして，午前Ⅱ対策と同様に，午後Ⅰ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，FW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，数多くの午後Ⅰ問題演習を行うとよいでしょう。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。

5.3　午後Ⅱ対策

午後Ⅱ対策は基本的には午後Ⅰ対策と同じです。追加で行うべき対策としては，セキュリティ管理面の知識を強化しておくことが挙げられます。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，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。

セキュリティ技術知識については，出題される範囲は午後Ⅰ試験と同一ですが，より詳細なレベルまで問われることがあります。問題演習を行う場合は，午後Ⅰ問題とは別に午後Ⅱ問題の演習も必ず行い，習得した技術知識のレベルが必要とされる技術知識のレベルに達しているかを確認しておくとよいでしょう。

そのほか，午後Ⅱ問題特有の長文問題に対する短時間での読解に慣れておく必要があります。細かい図表が多く提示される場合もあり，問題事例を把握するだけでも相当な時間と集中力が必要になります。午後Ⅱ問題では午後Ⅰ問題以上に設定条件も複雑になり，読解力が大きなカギを握っています。問題文や設問文で提示された条件や要求事項の関係がどのようになっているのかを整理し，誤りなく見極めることに留意して問題演習を行うことが重要です。問題文の分量が多いため，何度もページをめくることになり，ポイントとなる記述を見落としがちになります。また，ポイントとなる記述が複数箇所に埋め込まれており，何ページか離れた図の注記に記されているようなこともあります。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，印をつけたりするなど，ポイントを見落とさない工夫を自分なりに見つけて問題演習を行うとよいでしょう。

午後Ⅱ問題演習を行う際は，最初は時間を意識しなくてもよいと思いますが，次の段階として制限時間内に解答できるかも確認するようにしてください。本番の試験では問題選択や見直しの時間も考慮する必要があるので，1 問 100 分を目標に問題演習に取り組むとよいでしょう。