情報処理安全確保支援士

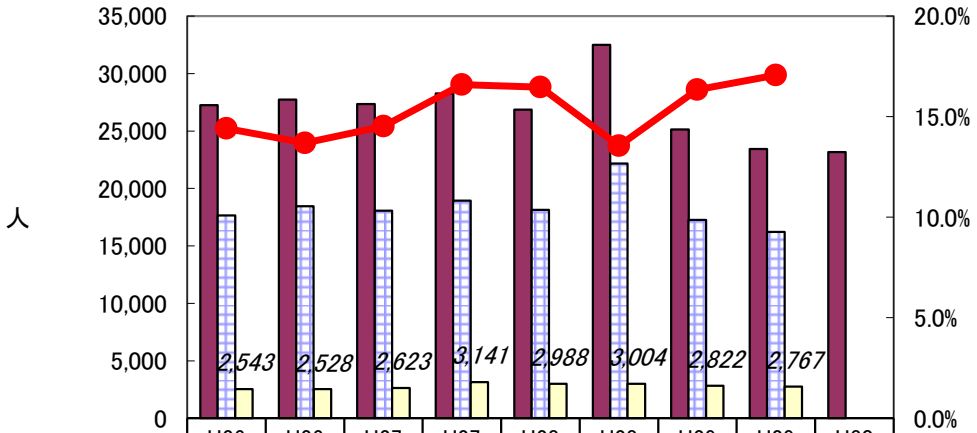
1.　はじめに

1.1　総評

今回の情報処理安全確保支援士(SC)試験は，過去 2 回の試験と比較すると易しかったという印象を受けました。これは，午後Ⅰ・午後Ⅱ試験で高度かつ詳細なレベルのセキュリティ技術知識があまり要求されなかったことと，頻出テーマがとり上げられ取り組みやすかったことが，理由として挙げられます。事例に対して基本的なセキュリティ技術知識を適用させ，具体的に解答表現するという設問が多くを占めています。午前Ⅱ試験では専門知識の有無が問われ，午後Ⅰ・午後Ⅱ試験では専門知識を応用させる思考力や問題読解力が要求される試験でした。

創設されてから 3 回の試験を終了した現時点では，試験の出題傾向として情報セキュリティスペシャリスト(旧 SC)試験との相違点は感じられません。新たに話題となっている脆弱性や攻撃をテーマとしてとり上げた問題も出題されていますが，新しい傾向というわけではなく，旧 SC 試験でもその時点で話題となっているテーマについて出題されています。新しい攻撃や対策が次々と出現する情報セキュリティの世界では当然のことといえるでしょう。難易度もその回によって異なり，どちらの試験のほうが難しいというような決まった傾向はありません。

1.2　受験者数の推移



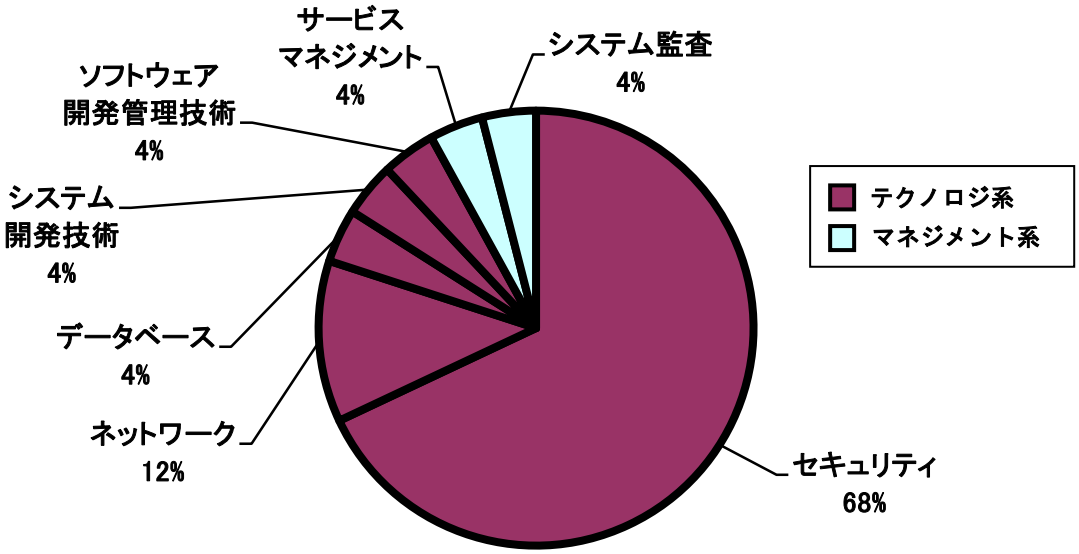
	H26春	H26秋	H27春	H27秋	H28春	H28秋	H29春	H29秋	H30春
応募者数	27,246	27,735	27,339	28,274	26,864	32,492	25,130	23,425	23,180
受験者数	17,644	18,460	18,052	18,930	18,143	22,171	17,266	16,218	
合格者数	2,543	2,528	2,623	3,141	2,988	3,004	2,822	2,767	
合格率	14.4%	13.7%	14.5%	16.6%	16.5%	13.5%	16.3%	17.1%	

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前回と同じで，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 問出題されました。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 問ずつとなっています。

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，さらに小分類にまで分類してその内訳を見てみると，例年どおり「情報セキュリティ」からの出題が多く，攻撃手法が 4 問，情報セキュリティ技術が 4 問の計 8 問となっています。ただし，これまでは新しい攻撃がとり上げられる傾向がありましたが，今回は出題されず，新規問題である“OS コマンドインジェクション”も用語としては既出です。次いで，セキュアプロトコルや認証プロトコルなどが含まれる「セキュリティ実装技術」，アクセス制御やマルウェア対策などが含まれる「情報セキュリ

ティ対策」の順となっています。「情報セキュリティ管理」からは“サイバー情報共有イニシアティブ(J-CSIP)”が，「セキュリティ技術評価」からは“CVSS の基本評価基準”が出題されました。2 問とも新規問題ですが，用語としては既出です。

セキュリティ分野の小分類	出題数			
	30 年春	29 年秋	29 年春	28 年秋
情報セキュリティ	8 問	8 問	8 問	8 問
情報セキュリティ管理，セキュリティ技術評価	2 問	3 問	2 問	1 問
情報セキュリティ対策，セキュリティ実装技術	7 問	6 問	8 問	8 問

「ネットワーク」分野からは 3 問中 2 問が新規問題で，“ICMP メッセージを識別するヘッダ”と“トランクポート”について出題されました。「サービスマネジメント」分野からは“可用性の計算”が，「システム監査」分野からは“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”が，新規に出題されました。

2.2　難易度の特徴

今回の午前Ⅱ試験は，例年どおりの標準的なレベルといえるでしょう。要求される知識レベルが特別に高い問題や，解答に多くの時間を要するような問題はありません。

「セキュリティ」分野の“CVSS の基本評価基準”は，三つの評価基準の違いを正しく把握しているかどうかが問われ，平成 28 年度春の午後Ⅱ問題で説明されていたような内容であることから，既出の CVSS の問題よりも難易度が高いと判断しました。“OS コマンドインジェクション”は，単純に攻撃の説明から用語を答える問題ではなく，攻撃の具体例が示されており，思考力を必要とする問題となっています。

「ネットワーク」分野の“ICMP メッセージを識別するヘッダ”と“トランクポート”は新規問題ということもあり，SC 試験での出題としてはやや難しかったと思います。

「サービスマネジメント」分野の“可用性の計算”は，計画停止時間の扱いがカギとなっています。

過去問題の再出題率は約 7 割で例年どおりですが，今回は応用情報技術者(AP)試験の過去問題から 3 問も出題されたことが特徴的です。過去問題演習を十分に行っていた受験者でも，他区分の過去問題演習まで行うことはあまりないと考えられることから，見慣れない問題で戸惑った受験者もいたと思います。AP 試験の技術レベルはレベル 3 までとなっていますが，“認証デバイス”と“エクストリームプログラミングにおけるテスト駆動開発”は，一度も目にしたことがなければ簡単には正解を得られないでしょう。

一方で，「3 回前の過去問題から数多く再出題される」という傾向は続いており，3 回前の平成 28 年度秋の旧 SC 試験から 7 問も出題されました。この回の問題演習を行っていれば有利だったことは明らかです。

2.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	CVSS の基本評価基準	C
2	OS コマンドインジェクション	C
3	XML ディジタル署名	B
4	エクスプロイトコード	B
5	シングルサイオンの実装方式	B
6	ダイナミックパケットフィルタリング	A
7	ディジタル署名に使う鍵	A
8	CRL	A
9	認証デバイス	C
10	サイバー情報共有イニシアティブ(J-CSIP)	B
11	cookie の secure 属性	A
12	DKIM	A
13	テンペスト攻撃	A
14	ダウンローダ型マルウェア感染後の対策	B
15	ルートキット	A
16	DNSSEC	A
17	SQL インジェクション対策	B
18	ICMP メッセージを識別するヘッダ情報	C
19	トランクポート	C
20	WebDAV	B
21	トランザクションのコミット完了のタイミング	B
22	シーケンス図	A
23	エクストリームプログラミングにおけるテスト駆動開発	C
24	可用性の計算	C
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	B

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試験の全体的な出題傾向としては，セキュリティ技術知識とその応用に重点が置かれ，例年どおりということができます。3問中1問がセキュアプログラミングの問題であることも変わりありません。

午後Ⅰ試験全体の難易度としては比較的易しかったと思われます。問 1 は，メモリ破壊を行う攻撃に利用されるUse-After-Freeという脆弱性に関するセキュアプログラミング問題です。新規性が高く，問 1 に限っていえば難易度は高いでしょう。そのほかの 2 問は，電子メールの送受信とWeb閲覧におけるセキュリティ，LAN分離による機密ファイルの漏えいとマルウェア感染拡大の防止，といったいずれも定番の出題内容です。多くの受験者が実務で直面したことがある，あるいは，問題演習を通して学習したことがあるような事例がとり上げられ，取り組みやすかったということができるでしょう。問題文は例年どおり分量が多いものの，理解しやすい事例内容だったことから，時間的に厳しいということもないと思われます。高度かつ詳細なセキュリティ技術知識は要求されず，例年と比較すると易しいでしょう。ただし，読み取り不足のまま解答を導いてしまうとミスにつながり，慎重に読解することが求められます。

3.2 各問題のテーマ，特徴

問 1 は，「ソフトウェアの脆弱性」というテーマで，メモリ破壊を行う攻撃に関する C++のセキュアプログラミング問題です。メモリ破壊を行う攻撃としては，バッファオーバフローが旧SC試験で3回出題されたことがありますが，今回はそれとは異なり，近年脆弱性の報告が増加しているUse-After-Freeについて出題され，新規性が高い問題でした。攻撃の仕組みは，問題文中で図を用いながら詳細に説明されていますが，メモリ領域の構造に関する知識やメモリ領域を操作するC++プログラムの知識を持っていないと，説明を正しく理解することは難しいでしょう。C++プログラミング経験の有無によって難易度のとらえ方が大きく異なる出題内容であり，問題を選択しなかった受験者が多かったと予想されます。

問2は，「情報セキュリティ対策の強化」というテーマで，電子メールの送受信とインターネット上の Web 閲覧におけるセキュリティ対策の強化がとり上げられています。必要とされる知識は，メール転送の仕組み，送信ドメイン認証の SPF レコード，ファイアウォールのフィルタリングルール，DNSサーバのオープンリゾルバ，プロキシサーバ経由のHTTPS通信とCONNECTメソッドなどです。午後Ⅰ・午後Ⅱ試験で必須の知識ばかりであることから，学習も進んでいたと考えられ，取り組みやすかったでしょう。必要な通信はどこからどこへの何の通信か，サーバの持つ機能は何か，といったことを正確に把握する読解力が要求されます。技術知識レベルとしては高いものは要求されておらず，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具体的に解答すればよく，易しい問題だったと考えられます。

問 3 は，「LAN 分離」というテーマで，LAN を分離することによって機密ファイルの漏えいやマルウェア感染の拡大を防ぐ方法がとり上げられています。午後 I 問題の 3 問の中で唯一，セキュリティ管理面からも出題され，JIS Q 31000:2010 リスクマネジメント-原則及び指針，JIS Q 31010:2012 リスクマネジメント-リスクアセスメント技法から，リスクアセスメントの定義が出題されました。ただし，出題の中心はセキュリティ技術知識とその応用です。インターネットへの通信を一切許可しない研究開発 LAN を分離し，社外の研究者とのファイルの共有を，ファイル転送サーバを利用して実現する事例です。その際に問題となるパッチやマルウェア定義ファイルの更新を行う配信サーバの配置，ファイアウォールの設定，リムーバブルメディアを利用してマルウェアに感染した場合でも機密情報が社外に漏えいしない仕組みなどについて問われています。問 2 と同様に，知識レベルとして高いものは必要とされておらず，セキュリティとネットワークに関する基本的な知識と読解力，解答表現力があれば十分に対応できるでしょう。

3.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	ソフトウェアの脆弱性	C
2	情報セキュリティ対策の強化	A
3	LAN 分離	A

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，午後Ⅰ試験と同様に，セキュリティ技術知識とその応用に重点が置かれていますが，問 2 の一部には，セキュリティ管理面からの出題も含まれています。問 1 でも，設問に直接関係はありませんでしたが，問題文中で“ISMS 適合性評価制度”という認証制度に触れています。技術面と管理面の両方から問われるのは，旧 SC 試験のときから午後Ⅱ試験でよく見られる傾向です。出題される 2 問のテーマはまったく異なる場合がほとんどですが，今回は 2 問ともに Web サイトのセキュリティと外部委託業者におけるセキュリティが盛り込まれており，類似性のある問題構成となっています。

過去 2 回の午後Ⅱ試験が難しかったので，新試験になってからの特徴かと注目していましたが，今回は 2 問とも易しく，旧 SC 試験と同様に難易度は回によって変動があるということが明らかになりました。2 問とも高度かつ詳細なセキュリティ技術知識やセキュリティ管理知識はあまり要求されていません。一方で，問題事例を踏まえたうえでの具体的な解答を求められているので，読解力と知識の応用力が必要です。高度な知識の有無を問うのではなく，実務に近い事例に適切に対処できる能力があるかどうかを見極めるような試験ということができるでしょう。特に問 1 は，設問の多くが問題文中に埋め込まれている解答の根拠をもとに解答を導く形式になっており，読解力の有無が大きく影響すると思われます。問 2 は，Web サイトのセキュリティに関する基本的な知識そのものを直接問うような設問が多く含まれていることから，Web サイトのセキュリティが得意な場合は問 2 を，そうでない場合は問 1 を選択したほうが解答しやすかったでしょう。

4.2 各問題のテーマ，特徴

問 1 は，「セキュリティ対策の評価」というテーマで，さまざまなセキュリティ対策の評価を行う事例がとり上げられています。クロスサイトスクリプティング(XSS)脆弱性の対策，共通管理者アカウントの対応，DB サーバの内部セグメントへの移設によるセキュリティ確保，外部委託におけるセキュリティ対策などについて問われています。XSS は前々回の SC 試験でも出題され，旧 SC 試験でも何度も出題されたことがある Web サイトのセキュリティの定番テーマです。今回は，XSS の手法の中でも“DOM Based XSS”と呼ばれる特殊な手法について出題されているため，やや高度な知識が必要とされます。問 2 と比較すると，Web サイトのセキュリティのほかにも，比較的幅広いセキュリティ技術知識項目について出題されています。共通管理者アカウントの対応については，問題文中のサーバへのアクセス権限やアクセス方法，サーバの持つ機能を正しく読み取ることができれば，正解を導くのは容易でしょう。DB サーバの内部セグメントへの移設によるセキュリティ確保については，午後Ⅰ試験の問 3「LAN 分離」と同様にファイアウォールのフィルタリングルール設定が出題され，必要な通信の流れを読み取ることができれば解答が見つかります。外部委託業者におけるセキュリティ対策では，業者の不正による機密情報の流出防止のための技術的対

策がとり上げられています。これについても問題文に解答の根拠が示されています。以上のように，問 1 は問題文中から解答の根拠を探して解答を導く形式の設問が主体となっています。解答字数が長いものが多く，解答ポイントを的確にとらえて解答表現できたかが合否の分かれ道となるでしょう。正確に問題文を読み取るだけのセキュリティとネットワークの基本的な知識と読解力があれば，十分に対応できる問題であると考えられます。

問 2 は，「Web サイトのセキュリティ」がテーマとなっており，Web アプリの診断項目や診断手順をもとにした，SQL インジェクション，XSS，アクセス制御の不備や認可制御の欠落，クロスサイトリクエストフォージェリ(CSRF)などの脆弱性診断と，外部委託業者におけるセキュリティ対策の実施について出題されています。それぞれの攻撃の具体的な方法と対策に関する知識が求められています。そのほか，Web サーバのアクセスログに記録される内容や，SSH の認証方式の知識などが必要です。外部委託業者におけるセキュリティ対策については，問 1 とは異なり，外部委託契約のセキュリティ面に関する検収条件や，Web セキュリティガイドの活用といった管理面からのセキュリティ対策が問われています。知識そのものを問う設問が多く設定されていますが，それほど高度な知識は要求されておらず，午前Ⅱ試験で出題されるような用語レベルの設問も一部含まれています。また，問題文が過去最長の 15 ページにわたりますが，ボリュームの割には事例が複雑にはなっておらず，順を追って読み取っていけば理解することができ，時間的な難易度も高くはないでしょう。

4.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	セキュリティ対策の評価	A
2	Web サイトのセキュリティ	A

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と思います。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りますので，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るでしょう。

過去問題の再出題率が 7 割前後と高いことから，知識習得後は過去問題演習が必須です。問題集や Web による問題演習を利用して，効率的に演習を行うようにしましょう。このとき，出題比率を念頭に置いて問題演習を行うと効果的です。具体的には，攻撃手法や暗号化・認証技術の出題比率が最も高いので，重点的に演習を行うとよいでしょう。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。また，問題演習を通じて自分の苦手な分野を洗い出し，あいまいな知識をテキストで再確認すると，弱点補強に役立ちます。過去問題演習は，少なくとも直近 5 回分は行うとよいでしょう。特に 3 回前からの再出題率が高いことから，試験直前に 3 回前の過去問題演習を行うことは非常に有効です。公開模試でもこの傾向を意識し，同じテーマについて同じ観点での問題，あるいは，同じテーマで異なる観点から出題された場合を想定した問題もとり入れて出題していますので，十分に活用してください。

また，昨年 10 月末に IPA から「情報処理安全確保支援士試験　シラバス追補版(午前Ⅱ)」が発表され，午前Ⅱにおける知識の細目が示されています。試験要綱よりも具体的に用語が追加されているので，特に重点分野については確認しておくとよいでしょう。

さらに，今回は出題されませんでしたが，新しい攻撃について出題されることがたびたびあることから，日頃から IT 関連のニュースに注目し，新しい攻撃についての情報収集を行っておくと役立つと思います。

非重点分野の「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」は，出題比率が低いことと，技術レベルはレベル 3 以下で，ほとんどの受験者は AP 試験に合格するだけの知識を持っていると想定されるので，対策は不要と考えています。あえて挙げるとすれば，トレンドとなっている開発技術や，新設または改訂された基準を把握しておくことと，計算問題で計算式を忘れていないか確認しておくことぐらいで十分でしょう。

5.2　午後Ⅰ対策

午後の出題範囲は，次のようになっています。

1　情報セキュリティシステムの企画・要件定義・開発・運用・保守に関すること
2　情報セキュリティの運用に関すること
3　情報セキュリティ技術に関すること
4　開発の管理に関すること
5　情報セキュリティ関連の法的要求事項などに関すること

午後Ⅰ試験では，セキュリティ技術寄りの出題傾向が強く，1～3 の「情報セキュリティシステムの企画・要件定義・開発・運用・保守に関すること」，「情報セキュリティの運用に関すること」，「情報セキュリティ技術に関すること」の出題頻度が高くなっています。具体的には，「情報セキュリティシステムの企画・要件定義・開発・運用・保守に関すること」の中では，アプリケーションのセキュリティ対策，セキュアプログラミング，ネットワークセキュリティ対策，サーバ・クライアント・セキュリティ装置などのシステムセキュリティ対策などが主に出題されています。また，「情報セキュリティの運用に関すること」の中では，情報セキュリティポリシ，脆弱性分析，不正アクセス対策，インシデント対応などが出題されやすく，「情報セキュリティ技術に関すること」の中では，アクセス管理技術，マルウェア対策技術，暗号技術，認証技術，PKI，ログ管理技術などの出題頻度が高くなっています。したがって，午後Ⅰ試験対策としては，これらを中心に深い知識を習得しておく必要があります。

セキュアプログラミングに関する問題が毎回 1 問出題されており，今後も出題される可能性は非常に高いと考えてよいでしょう。セキュアプログラミングの問題は，プログラミング経験のない受験者は選択しないことが考えられます。その場合，残りの 2 問を必ず選択することになるので，ほかに苦手なテーマを作らないようにより一層しっかりと対策を行うことが求められます。セキュアプログラミング問題を選択する可能性がある場合は，IPA の“安全なウェブサイトの作り方”や“セキュアプログラミング講座”に掲載されている内容から出題されることが多いので，教材の一つとして利用するとよいでしょう。

また，ネットワーク技術知識の習得も重要です。例えば，よく出題されるファイアウォールのフィルタリングルール設定の問題では，ネットワーク構成図や事例内容から，何のパケットがどこからどこへ流れていくか，パケットの送信元 IP アドレスは何かなどを読み取る基礎的な知識が必要です。TCP/IP のプロトコルとしては，インターネット層では IP，ICMP，ARP，トランスポート層では TCP と UDP，アプリケーション層では，HTTP，DNS，SMTP，LDAP，SSH などが問題文を読み取るうえで必須の知識となります。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，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。そのほかセキュリティインシデント分析などを行う際にも利用される主要なネットワークコマンドについては，出力される情報などを把握しておいてください。

そして，午後Ⅰ対策は，テキストを中心とした知識の習得が不可欠であることはもちろ

んですが，その後に必ず問題演習を行うことが非常に重要です。実務で経験したことがない事例については特に，さまざまな問題演習を通して疑似体験をしておくことは非常に有効です。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がよくありますが，その最大の要因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。解説には，その問題を解くうえでの技術知識の説明だけでなく，解答を導出するまでのポイントも説明していますので，問題演習を行った後に解説をしっかり読むことが大切です。繰り返し問題演習を行い，解答解説から正解表現と自分の解答表現の違いや解き方の違いを把握し見直すことで，問題文や設問文で見落としやすいポイントを学ぶと同時に，解答表現力を養ってください。

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。午後Ⅰ対策で提示した，午後の出題範囲の4と5の「開発の管理に関すること」「情報セキュリティ関連の法的要求事項などに関すること」が該当します。「開発の管理に関すること」の中では，ソフトウェアの配布と操作，人的管理手法，脆弱性情報収集管理などが比較的出題されやすいと考えられます。「情報セキュリティ関連の法的要求事項などに関すること」の中では，ISMS に関する JIS Q 27000:2014，27001:2014，27002:2014 や，サイバーセキュリティ基本法，個人情報保護法，不正競争防止法についての概要を習得しておいてください。

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，必要とされる技術知識のレベルと習得した技術知識のレベルが合っ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，問題文の読解力が大きなカギを握っています。問題本文と設問文中で提示された条件や要求事項との関係がどのようになっているかを整理し，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ったり戻ったりすることになり，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中に示されているようなこともよくあります。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，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自分なりに見つけて問題演習を行うとよいでしょう。