情報処理安全確保支援士

1.　はじめに

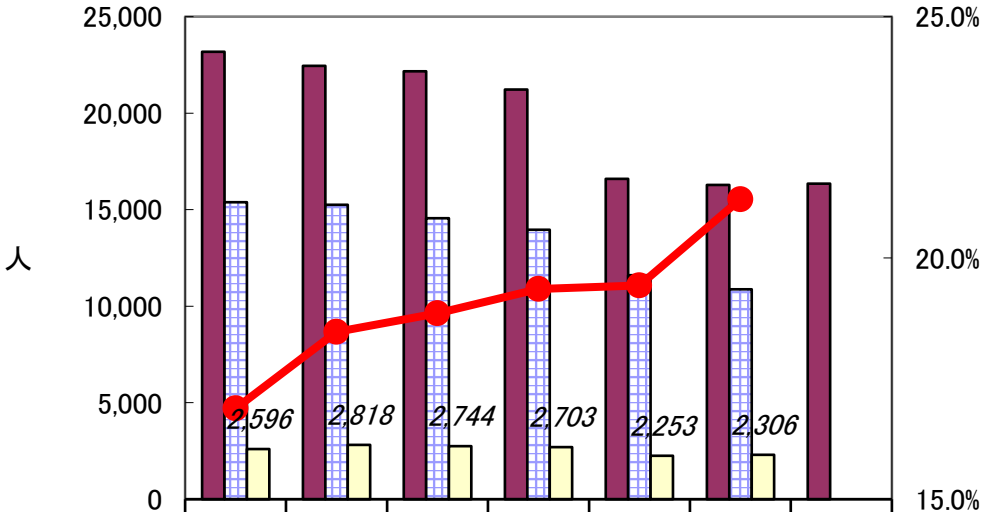
1.1　総評

今回の情報処理安全確保支援士試験(SC)は，出題テーマに特異なものはなく，全体として標準的な難易度だと思います。

午前Ⅱ試験は，技術レベルが最も高いレベル 4 に設定されているセキュリティ分野の新規問題が増えたことと，過去問題の再出題であっても SC 以外の試験区分の過去問題の数が例年よりも多かったことから，前回よりも難しく感じられました。

一方，午後Ⅰ・午後Ⅱ試験は，定番の情報セキュリティインシデント対応やセキュアプログラミング，このところ出題が増えている IDaaS などを含む問題が出題され，取り組みやすかったと思います。難易度としては，深いセキュリティ技術知識が問われる難問はなく，知識レベル・時間的なレベルともに標準的でしょう。

1.2　受験者数の推移



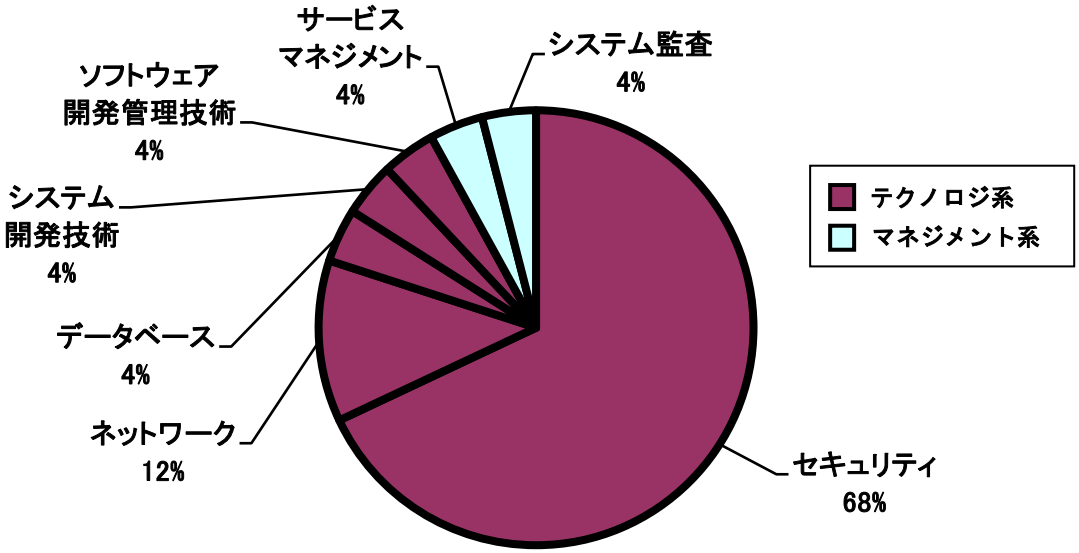
	H30春	H30秋	H31春	R1秋	R2 10月	R3春	R3秋
応募者数	23,180	22,447	22,175	21,229	16,597	16,273	16,354
受験者数	15,379	15,257	14,556	13,964	11,597	10,869	
合格者数	2,596	2,818	2,744	2,703	2,253	2,306	
合格率	16.9%	18.5%	18.9%	19.4%	19.4%	21.2%	

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，攻撃手法や情報セキュリティ技術に関する「情報セキュリティ」からの出題が大幅に増えています。今回は，セキュリティ分野の新規問題が例年より多く 7 問もありましたが，そのうちの 5 問が「情報セキュリティ」の問題で，これが出題数増に影響したものと思われます。その他の小分類は，出題数の多い順に「セキュリティ実装技術」,「情報セキュリティ対策」となっており，ほとんどが技術知識を問う問題で占められているという傾向に変わりはありません。「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，それぞれ 1

問のみでした。

セキュリティ分野の小分類	出題数			
	R3 秋	R3 春	R2 10 月	R1 秋
情報セキュリティ	9 問	6 問	5 問	9 問
情報セキュリティ管理	1 問	1 問	3 問	1 問
セキュリティ技術評価	1 問	1 問	0 問	1 問
情報セキュリティ対策	2 問	4 問	3 問	0 問
セキュリティ実装技術	4 問	5 問	6 問	6 問

セキュリティ分野の新規問題のテーマは，次のとおりです。

・Adversarial Examples 攻撃
・Pass the Hash 攻撃
・PQC(Post-Quantum Cryptography)
・SAML 認証
・サイバーキルチェーン
・ファイアウォールのステートフルパケットインスペクション
・TLS1.3 の暗号スイート

このうち，初出題の用語は“Adversarial Examples 攻撃”，“Pass the Hash 攻撃”，“PQC”，“サイバーキルチェーン”の 4 つで，前回よりも 1 つ増えています。“Adversarial Examples 攻撃”は AI に誤認識させる新しい攻撃手法，“PQC”は量子コンピュータの出現によってもたらされる脅威に対抗するための新しい技術に関する問題です。また，TLS については過去にも出題されたことがありますが，“TLS1.3 の暗号スイート”では新しいバージョン 1.3 の知識が初めて問われました。過去問題を流用した問題の中にもバージョンが更新されているものがあり，“FIPS PUB 140-2”は“FIPS PUB 140-3”に更新され，“無線 LAN の暗号化通信の規格”の選択肢中の WPA2-Enterprise は WPA3-Enterprise に更新されています。このように，今回は，最新のセキュリティ動向に関する知識の有無を問うような問題が数多く出題されています。

その他の分野の新規問題は，ネットワーク分野の“VXLAN”と，ソフトウェア開発管理技術分野の“ブルーレイディスクのコンテンツ保護技術”の 2 問で，前回と同数です。2 問ともセキュリティと関連性のある出題テーマとなっています。

2.2 難易度の特徴

今回の午前Ⅱ試験は，前回よりも難しかったと思います。

その理由として，新規問題が前回よりも 2 問増え，しかも技術レベルが最も高いレベル 4 に設定されているセキュリティ分野の新規問題が前回の 5 問から 7 問へと増えたことが挙げられます。前述のように，この中には，最新のセキュリティ動向を注視していなければ解答が難しい用語に関する問題や，既出の用語であってもこれまでよりも深い知識が要求さ

れる問題が含まれ，これらは難易度が高いと判断しました。

また，これまでは過去問題の再出題はほとんどがSCの過去問題で，他の試験区分の過去問題は3問程度でしたが，今回は前回に引き続き5問と多くなっています。他の試験区分の過去問題演習までは行っていないという受験者も多いと考えられることから，そのような場合はさらに見たことがない問題が多いという印象を受け，難しく感じたでしょう。

過去問題の再出題率は，他の試験区分も含めると6割を超えていますが，SCに限定すると4割強で，直近5回分の中で最も低くなっています。これまでと比較すると低かったとはいえ，合格基準点が60点の試験において，過去問題演習を行っていれば40点以上を確実に得点できるということは，非常に効果的な学習方法であることに変わりありません。SCでは3回前の問題の再出題率が高い傾向があり，今回も3回前の令和元年度秋から4問出題されています。この回を含めて過去問題演習を行っていれば，明らかに有利だったと考えられます。

2.3 問題テーマ難易度一覧表

問	テーマ	分野名	難易度
1	Adversarial Examples 攻撃	セキュリティ	C
2	Pass the Hash 攻撃	セキュリティ	C
3	PQC(Post-Quantum Cryptography)	セキュリティ	C
4	SAML 認証	セキュリティ	C
5	サイバーキルチェーン	セキュリティ	C
6	ファイアウォールのステートフルパケット インスペクション	セキュリティ	A
7	FIPS PUB 140-3	セキュリティ	A
8	CRL(Certificate Revocation List)	セキュリティ	A
9	JIS Q 27017:2016	セキュリティ	C
10	cookie の Secure 属性	セキュリティ	A
11	IoT 機器での TCP23 番ポートへの攻撃	セキュリティ	B
12	証拠保全の順序	セキュリティ	B
13	テンペスト攻撃	セキュリティ	A
14	ルートキット	セキュリティ	A
15	無線 LAN の暗号化通信の規格	セキュリティ	A
16	EAP-TLS 認証	セキュリティ	A
17	TLS1.3 の暗号スイート	セキュリティ	C
18	VXLAN	ネットワーク	C
19	ルータによるコリジョン伝搬とブロードキャス トフレーム中継の可否	ネットワーク	A
20	利用可能なホスト数	ネットワーク	A
21	参照制約によって拒否される操作	データベース	A
22	探索的テスト	システム開発技術	B
23	ブルーレイディスクのコンテンツ保護技術	ソフトウェア開発管理 技術	C
24	フェールソフトの例	サービスマネジメント	A
25	クラウドサービスの導入検討プロセスに対する システム監査	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，定番の情報セキュリティインシデント対応の問題が2問，情報漏えい対策の問題が 1 問という構成でした。前回と前々回は情報セキュリティインシデント対応の問題が1問も出題されず，出題傾向に変化がありましたが，今回は元に戻ったような印象を受けました。

3問とも深い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が問われるような試験でした。単純に技術や攻撃の名称を問うような設問は 1 問もなく，空欄穴埋め問題もすべて事例内容に基づいて思考した解答が求められています。いずれの問題も正確に事例内容を読み取る読解力が必要とされますが，正確に読み取るためには正確な知識が必要です。知識レベルが高くないからといって曖昧な知識で通用するわけではありません。暗号化，認証，フィルタリングなどの正確な知識が要求されています。

問題文の分量は3問とも6ページで，提示されている図表の数も6点ずつで同じです。

以上のように，問題ごとの難易度の差は感じられず，いずれも標準的でしょう。

3.2 各問題のテーマ，特徴

問1は「セキュリティインシデント」というテーマで，不正アクセスによる顧客情報漏えいのセキュリティインシデント対応について出題されました。ファイアウォールのフィルタリングルールの設定，アクセス権限の種別，ログの分析，SSH 接続のフィンガプリント，SSH接続時のパスワード認証と公開鍵認証などについて問われています。セキュリティインシデント対応の問題では，フィルタリングルール，アクセス権限，ログなどの基本的な知識は必須です。深い知識は求められていませんが，事例に合わせた具体的な設定内容や設定理由などを解答する必要があるため，読み落とさないように慎重に読解しなければなりません。SSH接続のフィンガプリントは平成22年春の午後Ⅱ問題で問われて以来11年ぶりの出題です。そのときと同様に，フィンガプリントを確認する目的が問われています。SSH接続時のパスワード認証と公開鍵認証は過去に何度か出題されていますが，毎回同じ論点が問われているので，過去問題演習を行っていれば容易に解答できたと思います。以上のことから，難易度は標準的と判断しました。

問2は「システム開発での情報漏えい対策」というテーマで，IRM(Information Rights Management)製品を用いた設計秘密の情報漏えい対策に関する問題です。IRM が出題されたのは初めてですが，そのセキュリティ機能については問題文中に記述されており，その内容を読み取って設計秘密の管理の問題をどのように解決できるかを思考することが求められています。具体的には，アカウントの種類に応じた権限の設定，プロジェクト離任者が出た場合の対応，暗号化ファイルの解読に要する計算量，パスワードクラッキングとその対策，マルウェア感染による設計秘密の不正取得方法などについて問われています。計算問題は

過去にほとんど出題されたことがありませんが，べき乗の計算なので難しいわけではありません。ただし，この箇所に正誤があり，記述が追加され，その記述によって解答が異なるので，確認漏れに気をつける必要があります。問 1 と同様に高度な知識が求められていないことから，問 2 も難易度は標準的でしょう。

問 3 は「PC のマルウェア対策」というテーマで，PC のマルウェア感染のインシデント対応について出題されました。インシデント発生時の初動対応，フルスキャン実施前のマルウェア定義ファイルの更新方法，ファイアウォールのフィルタリングルールの設定変更，マルウェア感染リスク低減のための実行ファイルのハッシュ値チェックの問題点などが問われています。インシデント発生時の初動対応は過去に何度も問われたことがある論点です。マルウェア定義ファイルやフィルタリングルールについては，事例を正しく読み取ることができれば容易に解答できるでしょう。一方で，実行ファイルのハッシュ値チェックの問題点は最近新たな脅威として注目されているファイルレスマルウェアについて問われていますが，新しい攻撃などに関する情報を日頃から収集していないと思いつかなかったかもしれません。以上のことから，問 3 の難易度は標準的と判断しました。

3.3　問題テーマ難易度一覧表

問	テーマ	難易度
1	セキュリティインシデント	B
2	システム開発での情報漏えい対策	B
3	PC のマルウェア対策	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でISO/IEC 27017とISO/IEC 27018について,問2で独自のガイドラインやテレワークセキュリティ規程について取り上げられ，技術面と管理面の両面から問われる総合問題となっています。大枠のテーマとしては，定番の情報セキュリティインシデント対応やセキュアプログラミング，このところ出題が増えているIDaaS，タイムリーな話題でもあるテレワークなどが中心となっており，取り組みやすく感じられるテーマだと思います。ただし，プログラミング経験がない場合は，セキュアプログラミング問題を含む問1ではなく，問2を選択したのではないかと考えられます。

午後Ⅰ試験と同様に，午後Ⅱ試験も詳細な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知識を事例に適用させて解答を導く応用力が問われるような試験でした。問題文の分量は2問とも12ページで，提示されている図表の数も14点ずつと非常に多く，午後Ⅰ試験よりもさらに読解力が必要となります。難易度は，知識的なレベル・時間的なレベルの両方から考えて，2問とも標準的でしょう。

4.2 各問題のテーマ，特徴

問1は「協力会社とのファイルの受渡し」というテーマで，システムの脆弱性診断及び対策とクラウドへの移行について出題されました。クロスサイトスクリプティング(XSS)脆弱性に関するセキュアプログラミング，SaaSへの移行時の注意点，SIEMを利用したログからの不正アクセス検知，ISO/IEC 27017，ISO/IEC 27018，IDaaSとの連携による多要素認証実現方式のうちFIDO認証についてなど，幅広い知識が要求されています。ISO/IEC 27017は今回の午前Ⅱ問題で出題され，そのときは正解できなかった場合でも試験直後に見直していれば，午後Ⅱ問題では得点できた可能性があります。XSSについては，過去に何度か問われたエスケープ処理の教科書的な内容が出題されたほか，Content-Security-Policyを用いた対策が初めて出題されました。SIEMも初出題でしたが，ここで取り上げられたパスワード攻撃は平成29年秋の午後Ⅱ問題で問われた論点と同じでした。FIDO認証の利用者認証の流れを示す図は平成31年春の午後Ⅰ問題で取り上げられたものと同じで，問われた論点も同様のものでした。このように幅広い基本的なセキュリティの知識が必要ですが，過去に問われた論点が複数含まれていることから，難易度は標準的と判断しました。

問2は「マルウェア感染への対処」というテーマで，社外の組織が会員となっている団体を運営する企業におけるマルウェア感染による秘密情報漏えいのセキュリティインシデント対応について出題されました。テレワーク導入時のセキュリティ規程の作成，CRYPTREC暗号リスト，UTMを利用したC&Cサーバへの通信の遮断方法，マルウェアの感染範囲の絞り込みなどについて問われています。このうち，UTMの機能の一つとして取り上げられたDNSシンクホール機能は初めての出題です。問1ほど幅広い知識は要求されませんが，事例に合わ

せた具体的な解答が求められており，事例内容を的確に把握して知識を適用させる能力が必要です。例えば，マルウェアの特徴の記述から感染範囲を読み取り，不足している対策を解答するといった思考力が要求されています。以上のことから，問 2 の難易度も標準的と判断しました。

4.3　問題テーマ難易度一覧表

問	テーマ	難易度
1	協力会社とのファイルの受渡し	B
2	マルウェア感染への対処	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 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，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 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。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。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効果的です。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)Ver3.1」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でしょう。

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。よく出題されるテーマは，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見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ファイアウォールのルールの設定，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。

セキュアプログラミングに関する問題は，以前は毎回 1 問必ず出題されていましたが，最近は出題されないこともあり，また今回のように出題されても問題の一部に限られることが増えています。バッファオーバフロー，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”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，活用するとよいと思います。

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。IP，ICMP，ARP，TCP，UDP，HTTP，DNS，SMTP，LDAP，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，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特におろそかになりがちかもしれません。試験に慣れるためにも，多くの午後Ⅰ問題演習を行ってください。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されているので，解説をしっかり読むことも大切です。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。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，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。