情報処理安全確保支援士

1. はじめに

1.1 総評

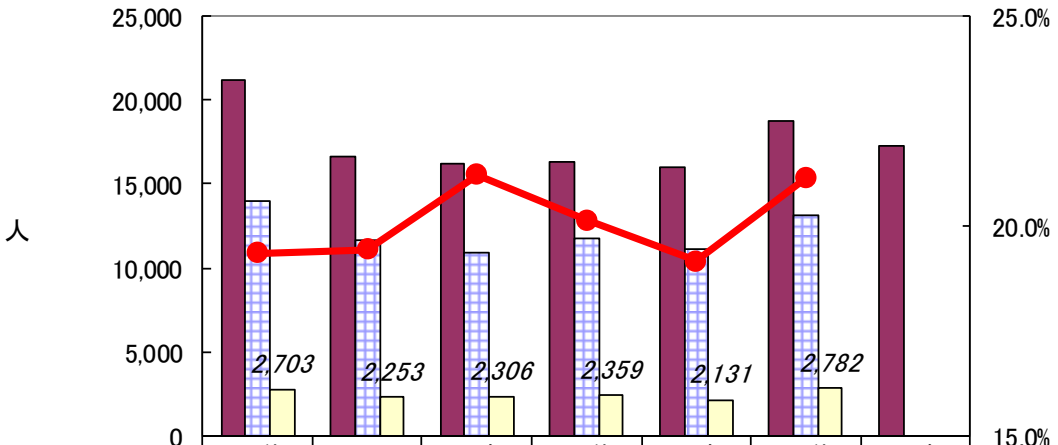
今回の情報処理安全確保支援士試験(SC)は，午後Ⅰ試験，午後Ⅱ試験の形式で行われる最後の試験です。情報セキュリティ実務で柱となるセキュリティインシデント対応，定番のWeb サイトのセキュリティ対策やセキュアプログラミングなどに関する出題のほか，特に，クラウドサービス関連のセキュリティに関する出題内容が目立つことが特徴です。また，最近よく扱われる認証連携に関する内容も継続して出題されています。

午前Ⅱ試験は，半分近くの問題が新作問題でしたが，セキュリティ分野では6割を超える問題が過去問題からの再出題でした。難易度は標準的です。

午後Ⅰ試験は，特定の技術的知識が問われる設問も含まれていて，具体的な技術的知識や対応が問われる場面の多い問題になっています。難易度は，やや高めです。

午後Ⅱ試験は,解答ボリュームのとても多い問題と深い技術的知識が問われる問題の2択となっていて，どちらを選んでも難易度は高かったと思われます。

1.2 受験者数の推移



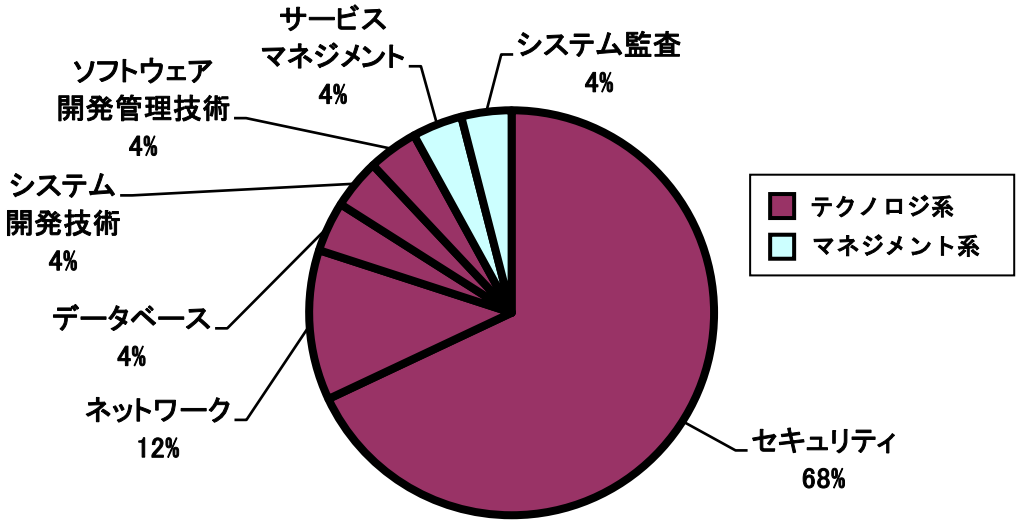
	R1秋	R2 10月	R3春	R3秋	R4春	R4秋	R5春
応募者数	21,229	16,597	16,273	16,354	16,047	18,749	17,265
受験者数	13,964	11,597	10,869	11,713	11,117	13,161	
合格者数	2,703	2,253	2,306	2,359	2,131	2,782	
合格率	19.4%	19.4%	21.2%	20.1%	19.2%	21.1%	

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」からの出題は 6 問で，前回に比べると減っています。次いで「セキュリティ実装技術」から 5 問,「情報セキュリティ対策」が 4 問となっており，技術知識の問題が 15 問出題されています。「情報セキュリティ管理」を問う問題は 2 問で,「情報セキュリティ技術評価」からの出題はありませんでした。今回の試験は,「情報セキュリティ対策」からの出題が増えている点が目を引きますが，新作問題にこの分野の出題が 2 問含まれていた影響と思われます。

セキュリティ分野の小分類	出題数				
	R5 春	R4 秋	R4 春	R3 秋	R3 春
情報セキュリティ	6 問	8 問	6 問	9 問	6 問
情報セキュリティ管理	2 問	0 問	4 問	1 問	1 問
セキュリティ技術評価	0 問	1 問	0 問	1 問	1 問
情報セキュリティ対策	4 問	2 問	2 問	2 問	4 問
セキュリティ実装技術	5 問	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。

・ブロック暗号の CTR モード
・ISMAP 管理基準
・サイバーセキュリティフレームワーク：フレームコア
・WAF におけるフォールスポジティブ
・シグネチャ型 IPS
・証拠保全で優先すべき情報

このうち，初出題の用語は“ブロック暗号の CTR モード”，“ISMAP 管理基準”，“サイバーセキュリティフレームワーク：フレームワークコア”，“シグネチャ型 IPS”の 4 問で，前回の 1 問に比べて増えています。

その他の分野の新規問題は，ネットワーク分野の“代表ポート”と“ブロードキャストアドレス”，システム開発技術分野の“IoT 機器のペネトレーションテスト”，ソフトウェア開発管理技術の“プログラムの著作権”，サービスマネジメント分野の“問題管理で実施する活動”，システム監査分野の“リスクアプローチで考慮すべき事項”の 6 問です。このうち，ネットワーク分野の代表ポートの問題とディレクティッドブロードキャストとリミテッドブロードキャストに関する問題は，知識がないと正解するのは難しい問題といえます。

2.2　難易度の特徴

前回の午前Ⅱ試験は，新規問題が多く，また，過去問題の再出題の傾向に変化がみられたこともあり，ほぼ 85%を超えていた午前Ⅱ試験の突破率が 73%とかなり下がりました。

今回の試験も新規問題が多く，過去問題の再出題についても，3 回前の試験からの再出題は大きく減っています。前々回までは，3 回前の試験に偏った再出題がありましたが，前回の試験から，そのような特定の回からの偏った再出題はなくなりました。今回は，令和 3 年秋と平成 29 年秋から 3 問ずつ，令和 3 年春と令和元年秋から 2 問ずつ，残りは，平成 31 年春，平成 29 年春，平成 28 年秋からそれぞれ 1 問ずつという再出題になっています。

前回試験での再出題傾向の変化を受けて，その対策として幅広い年度の過去問題演習をきちんと行ったかどうかによって，過去問題演習の効果に差が生じたかもしれません。

とはいえ，試験で問われた内容そのものの技術的なレベルは，そこまで高いものではなく，例年と比べても標準的です。今回の午前Ⅱ試験全体の難易度は標準的といえます。

2.3 問題テーマ難易度一覧表

問	テーマ	分野名	難易度
1	CRYPTREC 暗号リスト	セキュリティ	A
2	Pass the Hash 攻撃	セキュリティ	A
3	SAML 認証	セキュリティ	B
4	衝突発見困難性	セキュリティ	B
5	DNS に対するカミンスキー攻撃への対策	セキュリティ	A
6	デジタル証明書	セキュリティ	B
7	ブロック暗号の CTR モード	セキュリティ	C
8	ISMAP 管理基準	セキュリティ	C
9	サイバーセキュリティフレームワーク：フレームワークコア	セキュリティ	C
10	WAF におけるフォールスポジティブ	セキュリティ	B
11	タイミング攻撃の対策	セキュリティ	B
12	シグネチャ型 IPS	セキュリティ	C
13	証拠保全で優先すべき情報	セキュリティ	B
14	無線 LAN の暗号化通信：WPA3-Enterprise	セキュリティ	B
15	DKIM	セキュリティ	B
16	OP25B 導入の目的	セキュリティ	A
17	SQL インジェクション対策	セキュリティ	A
18	同時使用できるクライアント数の計算	ネットワーク	B
19	代表ポート	ネットワーク	C
20	ブロードキャストアドレス	ネットワーク	C
21	GRANT 文による権限の付与	データベース	B
22	IoT 機器のペネトレーションテスト	システム開発技術	B
23	プログラムの著作権管理	ソフトウェア開発管理技術	B
24	サービスマネジメントの問題管理で実施する活動	サービスマネジメント	B
25	システム監査のリスクアプローチで考慮すべき事項	システム監査	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試験は，Webアプリケーションのセキュリティ・セキュアプログラミングの問題とセキュリティインシデント対応の問題，クラウドサービスの活用を題材にしたネットワークセキュリティの問題が出題されていて，いずれも定番テーマの問題です。ただ，セキュアプログラミングの問題を対象から外している受験者にとっては，選択の余地のない問題構成でもあります。

3問ともシステムやサービスの機能，設定内容，アクセスログ，ソースコード，調査結果といった関連図表に示された条件などに基づいて，具体的な状況判断や技術的対応力などを問う構成の問題になっています。問題分量は平均的ですが，3問ともに細かい図表の提示が多く，5～8 つの図表やその注記まで読み込む必要があり，読解に時間がかかったと思われます。また，解答するうえで前提となる技術的知識はかなり特定の専門事項を要求する設問も見受けられます。

以上のことから，知識面と時間的な面の両方から判断して，今回の午後Ⅰ試験の難易度はやや高めといえるでしょう。

3.2 各問題のテーマ，特徴

問1は，オフィス用品の受注システムを題材としたWebアプリケーションのセキュリティ・セキュアプログラミングに関する問題です。Java サーブレットプログラムを用いて，基本的な SQL インジェクション対策やディレクトリトラバーサル対策について出題されています。2回前の令和4年春にもSQLインジェクションやPreparedStatementに関して出題されていましたので，セキュアプログラミングを選択対象としている受験者にとっては取り組みやすい問題といえます。しかし，選択肢から選ぶ設問が一つもないという点で，難易度はやや高めです。特に，Java マルチスレッドプログラミングにおけるレースコンディションに関する問題は，SC試験の平成22年春の午後Ⅰ問題や平成25年春の午後Ⅱ問題で出題されて以来の出題でしたので，難しく感じられた受験者も多かったと思われます。問1の難易度は，やや高めです。

問2は，DMZ上のサーバへの不正アクセスに関するログ調査を題材にしたセキュリティインシデント対応の問題です。FTPの接続モードの視点は定番の設問であり，攻撃者による不正コードの設置についての，C&Cサーバとの接続モードごとの差が問われた設問は，関連図表を注意深く紐解けば比較的解答しやすいものでした。また，DNSをC&C通信として悪用する攻撃手法であるDNSトンネリングについては，SC試験の令和元年秋の午後Ⅰ問題で一度，取り上げられてはいますが，今回はより具体的な出題内容となっていました。

TCPのウェルノウンポートやFTPのパッシブモード，psコマンドやnetstatコマンドについてのある程度の知識を必要とする問題であることを考慮すると，難易度はやや高めといえます。

問 3 は，複数のクラウドサービス利用時の認証連携や在宅勤務のリモート接続におけるクラウドサービスの活用を題材としたネットワークセキュリティの問題です。クラウドサービスの機能設定が主体の問題は，問題文中の条件を正しく把握することができれば，比較的順当に解答が導ける標準的な難易度の設問が並んでいます。ただし，多要素認証機能の選択など，要件の意図を読み誤ると選択を誤りかねない設問も含まれていました。

問 3 の難易度は，標準的といえるでしょう。

3.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	Web アプリケーションプログラム開発	C
2	セキュリティインシデント	C
3	クラウドサービス利用	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る総合問題となることが多い傾向があります。今回も，問 1 についてはDAST ツールによる脆弱性診断を通した Web サイトセキュリティの総合問題，問 2 についてもクラウドサービス活用に関する総合問題といえ，両問ともに技術面・管理面の設問テーマが出題されています。

求められた技術的知識については，問 1 は，クロスサイトスクリプティング(XSS)や SQL インジェクションなどの知識が求められていますが，高度な技術的知識が必要な設問は含まれていません。問題文を正しく読み解くことができれば，対応可能といえる問題でした。一方，問 2 の OAuth2.0 に関しては，送信されるデータのパラメータなどからフロー図のどの部分のものであるかを答えさせる設問や，令和 4 年春に出題された OAuth 2.0 の拡張機能である PKCE(Proof Key for Code Exchange)を利用した認可コード横取り攻撃への対策に関する内容が再出題され，具体的な検証方法を述べることが求められた設問などは，高い技術的知識が求められた設問といえます。

問題文の分量は 11 ページと 12 ページと平均的でしたが,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多く，図表の注記など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。

今回の試験で目を引いたのは，問 1 の解答分量の多さです。制限字数を加算すると，430 字にもなります。令和 4 年の午後Ⅱ問題の 1 問当たりの解答分量の平均が 225 字であることを考えると，今回の問 1 の解答分量は通常の問題の 2 倍にもあたることが分かります。これは，そのまま解答群の提示された設問が少ないことにも結びつきますので，問 1 は，時間的な難易度の高い問題ということができるでしょう。

以上のことから，問 1 は時間的な難易度の高い問題，問 2 は技術的難易度の高い問題といえます。

4.2 各問題のテーマ，特徴

問 1 は XSS，SQL インジェクションといった脆弱性の診断や対策に関する Web サイトセキュリティの総合問題です。Web サイトの脆弱性診断ツールの設定に関する設問や，代表的な脆弱性の内容に関する設問，診断業務における組織的管理策に関する設問などで構成されています。脆弱性診断ツールの設定に関する設問については，解答要件が読み取りづらい設問が含まれています。診断用データに関する設問は最近よく出題されていますが，今回は SQL インジェクションにおける検出パターンの違いによるレスポンスの差異に着目した出題になっていました。組織的管理策に関する設問は，解答ポイントを比較的容易に想定できるものでした。

問 1 は，技術的知識や管理策についての知識は基本的なレベルで対応可能で，問題文を正しく読み解くことができれば解答ポイントを見つけることが可能な問題です。しかし，前述

したように解答ボリュームが通常の 2 倍もあることから，他の問題よりも解答を的確にまとめる力や，解答をまとめるための時間を多く必要とする時間的な難易度の高い問題といえます。

問 2 はクラウドサービスの選定・移行・運用を題材にして，そのサービス間連携に応じ，リポジトリサービスを活用して開発されるモジュールの開発時のセキュリティまで含めた総合問題です。複数のクラウドサービスの仕様を誤りなく読み解くことを要求する設問が並んでいます。ただし，付与権限の設定に関する設問など，サービス内容の先入観に捉われると誤りやすいものも含まれています。また，令和 4 年春の午後Ⅱ試験で出題された OAuth 2.0 の拡張機能である PKCE(Proof Key for Code Exchange)を利用した認可コード横取り攻撃への対策に関して，より具体的な内容で出題されていることから，認証連携関連のセキュリティに関する出題への対応の重要性が再認識されます。OSS リポジトリサービスを活用して開発されるモジュールの開発時のセキュリティに関する設問は，アクセス権限管理に関する設問が主体ですが，解答の表現やまとめ方に多少迷う設問も含まれています。

問 2 は，技術的難易度の高い問題です。

4.3　問題テーマ難易度一覧表

問	テーマ	難易度
1	Web セキュリティ	C
2	Web サイトのクラウドサービスへの移行と機能拡張	C

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的です。

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，IEEE802.1X や今回も出題された SAML 認証は定番の問題といえます。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。

今回の試験では，過去問題の再出題率はやや下がりましたが，それでも 6 割近くは再出題の問題ですので，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。以前は，3 回前の試験からの再出題率が高いという傾向がありましたが，ここ 2 回の試験では，特定の回からの試験の再出題率が特別に高いということはなくなっています。そのため，3 回前～12 回前の過去問題の演習を繰り返し行うことをお薦めします。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などで再確認すると，弱点補強に役立ちます。古い年度からの再出題が増えているため，以前よりも過去問題演習の成果が直結しにくくなっているかもしれません。しかし，出題テーマが大きく変わったわけではないので，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試験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　午後対策

次回の試験から，これまで午後Ⅰ試験と午後Ⅱ試験に別れていた試験が，午後試験に一本化されます。問題数は4問で，そのうち2問を選んで解答します。試験時間は150分ですので，1問当たり75分の問題が出題されることになります。試験時間や問題数といった出題構成は変更されますが，これは問題選択の幅と時間配分の自由度を拡大する変更であり，**“試験で問う知識・技能の範囲そのものに変更はありません”**と，IPAが表明しています。

ですので，午後試験対策としては，これまでと同様の対策を行えばよいと考えます。

午後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，クラウドセキュリティなどです。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。

同時に，セキュリティ管理面の知識の学習として，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の知識を習得してください。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，セキュリティインシデント対応の事例が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。

セキュアプログラミングに関する問題は，令和4年春以降，出題が増加傾向にあります。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。ARP，DNS，FTP，HTTP，IP，ICMP，NTP，SMTP，SSH，TCP，UDP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試験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，それがおろそかになってしまうこともよく起こります。試験に慣れるためにも，数多くの午後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。

午後試験の問題は，次回の試験ではじめて出題されますので，問題演習は，過去の午後Ⅰ問題や午後Ⅱ問題を利用することになると思われます。午後試験の試験時間は 1 問 75 分ですので，試験時間から推測すると，現在の午後Ⅰ問題よりは長く，午後Ⅱ問題よりは短い問題になるのではないかと思われます。問題演習を行う場合，最初は午後Ⅰ問題から始めて，ある程度の読解力がついてから，午後Ⅱ問題を行うようにしてください。午後Ⅰ問題で記述式試験に慣れれば，午後Ⅱ問題での対策は不要と考える方もいらっしゃるかもしれませんが，これまでの午後Ⅰ問題では，管理的な知識が問われることはほとんどなかったために，管理的な問題を解くためには，午後Ⅱ問題を解く必要があります。午後Ⅱ問題の問題分量が多いため，敬遠しがちになると思われますが，少なくとも，管理面での設問だけでも過去の午後Ⅱ問題を利用して取り組むようにしてください。