情報処理安全確保支援士

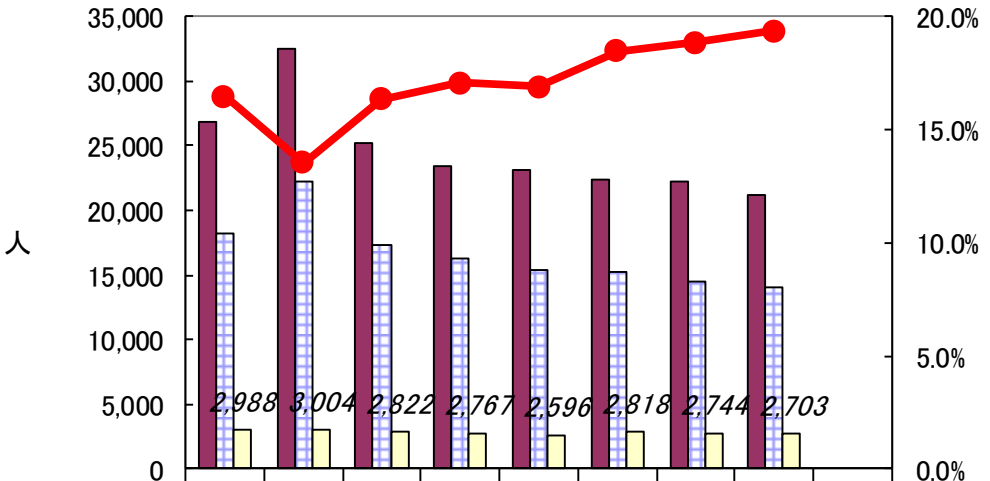
1.　はじめに

1.1　総評

今回の情報処理安全確保支援士試験は，出題テーマがこれまでとは傾向が多少異なり，全体的に難しかったと感じられます。

午前Ⅱ試験では，これまで攻撃に関する問題が多数出題されていましたが，今回は減り，代わりに情報セキュリティに関連する国の組織の新たな取組みや新たに策定されたフレームワークなどのセキュリティ管理面からの出題が増えました。また，午後Ⅰ・午後Ⅱ試験では，1回の試験で複数問出題されることもあった定番の情報セキュリティインシデント対応の出題がなく，情報システムの設計や開発におけるセキュリティ確保や利用時のセキュリティ対策に関する出題が中心でした。今回まったく新しいテーマが出題されたわけではありませんが，定番問題が出題されなかったことで難しく感じた受験者が多かったのではないかと思います。さらに午後Ⅱ試験は 2 問とも事例内容が複雑で，知識レベル・時間的なレベルともに難易度が高かったといえるでしょう。

1.2　受験者数の推移



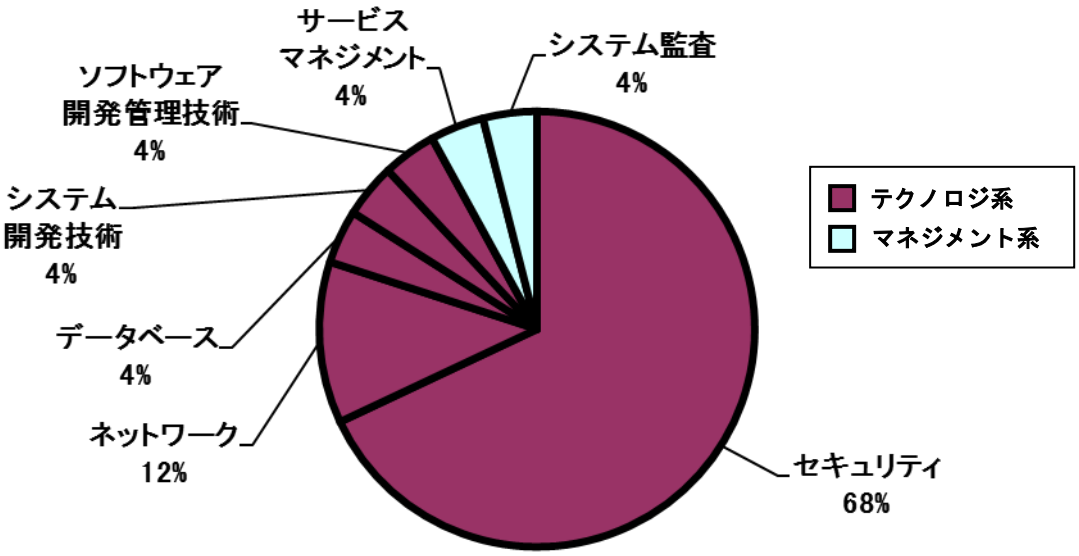
	H28春	H28秋	H29春	H29秋	H30春	H30秋	H31春	R1秋	R2
応募者数	26,864	32,492	25,130	23,425	23,180	22,447	22,175	21,237	
受験者数	18,143	22,171	17,266	16,218	15,379	15,257	14,556	13,964	
合格者数	2,988	3,004	2,822	2,767	2,596	2,818	2,744	2,703	
合格率	16.5%	13.5%	16.3%	17.1%	16.9%	18.5%	18.9%	19.4%	

2. 午前Ⅱ問題の分析

2.1 問題テーマの特徴

分野ごとの出題数に変化はなく，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，さらに小分類に細分化してその内訳を見てみると，前回と前々回は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」からの出題が多くを占めていましたが，今回は出題傾向が異なり，「情報セキュリティ管理」からの出題数が増え，「セキュリティ技術評価」以外の各小分類から万遍なく出題されていました。特に新規問題として，前年度から総務省と NICT で実施されている“NOTICE”という取組みや，前年度に経済産業省が策定した“サイバー・フィジカル・セキュリティ対策フレーム

ワーク”など，国の組織の新たな取組みや新たに策定されたフレームワークが出題されたことが特徴的です。

そのほかの新規問題としては，セキュリティ分野からは“3D セキュア”，“ファイアウォールにおけるフィルタリングルールの変更”，“IP25B”が出題されました。“3D セキュア”は，ネットショッピングのオンライン決済におけるクレジットカード情報の不正利用が増加している中で，タイムリーな出題ということができるでしょう。

セキュリティ分野の小分類	出題数			
	R2	R1 秋	H31 春	H30 秋
情報セキュリティ	5 問	9 問	11 問	6 問
情報セキュリティ管理	3 問	1 問	0 問	1 問
セキュリティ技術評価	0 問	1 問	0 問	2 問
情報セキュリティ対策	3 問	0 問	1 問	2 問
セキュリティ実装技術	6 問	6 問	5 問	6 問

「ネットワーク」分野からは，“DHCP メッセージの宛先 IP アドレス”が新規に出題されました。DHCP メッセージについては，過去にメッセージの順序が出題されたことがあります。「システム開発技術」分野の “ペルソナ”は初出題ですが，新しい概念というわけではありません。「システム監査」分野の“個人情報管理台帳の取扱いの内部監査における指摘事項”も初出題ですが，監査における指摘事項に関する問題はこれまでに何度か出題されたことがあります。

また，2019 年 11 月に「情報処理安全確保支援士試験 シラバス 追補版（午前Ⅱ）」が Ver. 3.0 に改訂された際に「ソフトウェア開発管理技術」分野のアジャイルに関連する項目が大幅に増加したので，“レトロスペクティブを行うタイミング”は出題が想定されるテーマの問題でした。なお，本問は応用情報技術者試験で過去に出題されています。

2.2 難易度の特徴

これまであまり出題されなかった「情報セキュリティ管理」からの出題が増え，しかもそのうちの 2 問は新規問題だった点は，難易度を高めていると感じられます。また，“ファイアウォールにおけるフィルタリングルールの変更”は午後問題で出題されてもおかしくないような思考力を要する問題です。一方で，重点分野の一つである「ネットワーク」分野の 3 問中 2 問は，単純な用語選択の基礎的な内容でした。

過去問題の再出題率は 6 割を超え，前回と同じです。3 回前の平成 30 年度秋から 4 問，4 回前の平成 30 年度春から 4 問出題されています。これら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。

総合的に判断すると，前回と比較してやや難しかったということができるでしょう。

2.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	OS コマンドインジェクション	C
2	SAML	A
3	エクスプロイトコード	A
4	サイドチャネル攻撃	B
5	ブロックチェーン	B
6	NOTICE	C
7	サイバー・フィジカル・セキュリティ対策フレームワークの目的	C
8	CRYPTREC の活動内容	B
9	3D セキュア	C
10	MITB 攻撃の対策	B
11	クラウドサービスのセキュリティ	B
12	cookie の Secure 属性設定時の Web サーバとブラウザの処理	B
13	ディジタルフォレンジックス	A
14	ファイアウォールのフィルタリングルールの変更	C
15	DNSSEC で実現できること	A
16	SMTP-AUTH の特徴	B
17	IP25B	B
18	DHCP メッセージの宛先 IP アドレス	B
19	RADIUS	A
20	スパニングツリープロトコル	A
21	DBMS のコミット処理完了のタイミング	A
22	ペルソナ	B
23	レトロスペクティブを行うタイミング	B
24	TCO が最小の案	A
25	個人情報管理台帳の取扱いの内部監査における指摘事項	C

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

2019年11月に午後の出題範囲とシラバスの改訂が行われ，午後の出題範囲は次のようになりました。

1 情報セキュリティマネジメントの推進又は支援に関すること
2 情報システムの企画・設計・開発・運用におけるセキュリティ確保の推進又は支援に関すること
3 情報及び情報システムの利用におけるセキュリティ対策の適用の推進又は支援に関すること
4 情報セキュリティインシデント管理の推進又は支援に関すること

改訂前と比較すると，セキュリティに関する近年の環境変化などを踏まえて，構成や表記が変更されていますが，出題内容に大きく影響を与えるようなものではないと考えられます。

今回の午後Ⅰ試験は，セキュリティ技術知識とその応用に重点が置かれているという点ではこれまでと同様です。大枠のテーマの特徴としては，定番の情報セキュリティインシデント対応の問題(出題範囲の4)が1問も出題されなかったことが挙げられます。また，長年にわたって必ず3問中1問出題されてきたセキュアプログラミングの問題(出題範囲の2に含まれる)が前回に引き続きありませんでした。今回は，情報システムの設計や開発におけるセキュリティ確保(出題範囲の 2)や，情報システムの利用におけるセキュリティ対策(出題範囲の3)から出題されています。

問1のスマートフォンを用いた決済は，IPAから公開されている「情報セキュリティ 10大脅威 2020」で個人編の脅威の1位となっており，最近のニュースでもたびたび取り上げられている新しいテーマといえますが，そのほかの2問には新規性はありません。

3問ともセキュリティ技術に関する知識をそのまま解答する設問は少なく，事例として提示されている記述や図表を読み取り，その内容や条件に合わせて知識を応用させて解答を導く設問がほとんどでした。このような問題を解くためには，深い思考力や実務に基づく経験が要求され，難易度のやや高い試験でした。前回は 3 問とも標準的な難易度だったことから，前回よりも難しかったといえるでしょう。

3.2 各問題のテーマ，特徴

問1は，スマートフォンを用いた決済のなりすましに関する問題です。バーコードやQRコードを用いた決済におけるセキュリティや無線 LAN サービス利用時の中間者攻撃，サーバ証明書の検証，パスワードリスト攻撃などについて問われています。バーコードやQRコードを用いた決済におけるセキュリティは，処理が提示され，なりすましを行う手段を考えさせる難しい問題となっています。また，パスワードリスト攻撃はこれまでにも出題さ

れたことがありますが，今回は攻撃者が効率的に攻撃を行うためのスクリーニングについて出題され，要求される知識レベルが高くなっています。難易度は高めの問題で，今回の3問の中ではもっとも難しいでしょう。

問2は，電子メールのセキュリティ対策としてのS/MIMEの活用に関する技術的知識を問う問題です。S/MIMEは，午前Ⅱ問題では最近も出題されていますが，午後問題では平成22年春の情報セキュリティスペシャリスト試験で一部取り上げられて以来です。また，今回のように事例において中心的な技術として出題されたのは初めてです。解答ポイントとして何を含めればよいか表現に迷う設問が含まれていたことから，難易度はやや高めの問題といえるでしょう。

問3は，Webシステムのセキュリティ診断について出題されました。Webサーバの脆弱性診断やネットワーク型・ホスト型 IPS の活用に関する技術的知識が問われています。診断をネットワーク上のどこから行うか，稼働中のセキュリティ機器の設定をどのように変更して診断する必要があるかといった診断計画についても具体的に問われています。セキュリティ診断は，午後Ⅰ・午後Ⅱ問題の一部で脆弱性検査あるいはセキュリティ評価などとしてたびたび出題されています。問題文で提示された条件を漏らさずに読み解くことができれば解答可能な問題であり，標準的な難易度の問題といえるでしょう。

3.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	スマートフォンを用いた決済	C
2	電子メールのセキュリティ対策	C
3	Webシステムのセキュリティ診断	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試験の出題範囲は午後Ⅰ試験と同じです。午後Ⅱ試験においても出題範囲やシラバスの改訂の影響と考えられるような変化はありませんでした。

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という傾向があります。今回は，セキュリティ技術中心の出題内容となっており，セキュリティ管理面では問 1 の一部で個人情報の取扱いについて問われただけでした。大枠のテーマについては，午後Ⅰ試験と同様に午後Ⅱ試験でも，定番の情報セキュリティインシデント対応の出題がなく，情報システムの設計や開発におけるセキュリティ確保や，情報システムの利用におけるセキュリティ対策から出題されています。

2 問とも幅広い高度なセキュリティ技術知識と深い思考力が要求され，必要とされる知識レベルの高い問題です。また，事例内容が複雑で読み解くのに時間を要し，時間的な難易度も高い問題です。総合的に判断すると，今回の午後Ⅱ試験は 2 問に難易度の差はなく，2 問とも難しかったといえるでしょう。前回は 2 問中 1 問が易しかったことから，前回と比べても難しかったといってよいでしょう。

4.2 各問題のテーマ，特徴

問 1 は，百貨店の合併に伴う複数の Web サイトの統合がテーマです。その中でも，サイト間でのアカウント連携の設計が中心となっています。アカウント連携に関する例外処理を中心とした Java コードレビュー，パスワード失念時処理の脆弱性やリスク，SAML によるシングルサインオンの通信フローなどに関する幅広い高度なセキュリティ技術知識が問われています。SAML は午前Ⅱ試験の定番問題ですが，午後試験でも平成 30 年秋の午後Ⅱ問題，平成 29 年春の午後Ⅰ問題で出題されており，このところ出題頻度が増えている技術の一つです。セキュリティ管理的知識としては，事業承継に伴って取得した個人情報の取扱いについて，個人情報保護法に定められている禁止事項を 70 字以内の長文で解答する設問があり，正確に記述するのは難しいと思われます。複数のサイト間でのアカウント連携の複雑な記述の読取りや，Java ソースコードを含む多くの図の読取りに時間を要することから，時間的な難易度も高い問題です。

問 2 は，クラウドサービスを活用したテレワーク環境という，現在対応を迫られている企業が増加していると思われるテーマについて出題されました。クラウドサービスの仮想デスクトップでテレワーク環境を構築・運用する際のクラウドサービス間の認証連携や TOTP の脆弱性，モバイル端末のセキュリティになどに関する高度なセキュリティ技術知識が要求されています。クラウドサービスの認証連携は，平成 30 年秋の午後Ⅱ問題や平成 29 年春の午後Ⅰ問題でも出題されており，出題頻度が増えています。事例では利用目的ごとに多くのクラウドサービスを利用しており，クラウドサービス間の認証連携には OpenID Connect の認可コードフローを利用する場合と Implicit フローを利用する場合があるなど

複雑になっています。この複雑な事例を読み解くのにはかなりの時間を要します。また，知識を応用させて事例に合わせた解答を，出題者が意図する解答ポイントは何かを見極めながら記述する必要がある設問が多くを占め，深い思考力が要求される難しい問題です。

4.3　問題テーマ難易度一覧表

問	テーマ	難易度
1	百貨店における Web サイトの統合	C
2	クラウドサービスを活用したテレワーク環境	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，攻撃と 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。PKI についても，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。また，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，新しい攻撃についての情報収集を行っておくと役立つでしょう。今回のように，国の組織の新たな取組みや新たに策定された基準などが出題されることも考えられ，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，今回は出題されませんでしたが，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読取り，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と思います。

セキュアプログラミングに関する問題は，毎回 1 問出題されていましたが，前回と今回は出題されませんでした。今後も出題されないとは限らないので，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。例えば，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。