

ネットワークスペシャリスト

1. はじめに

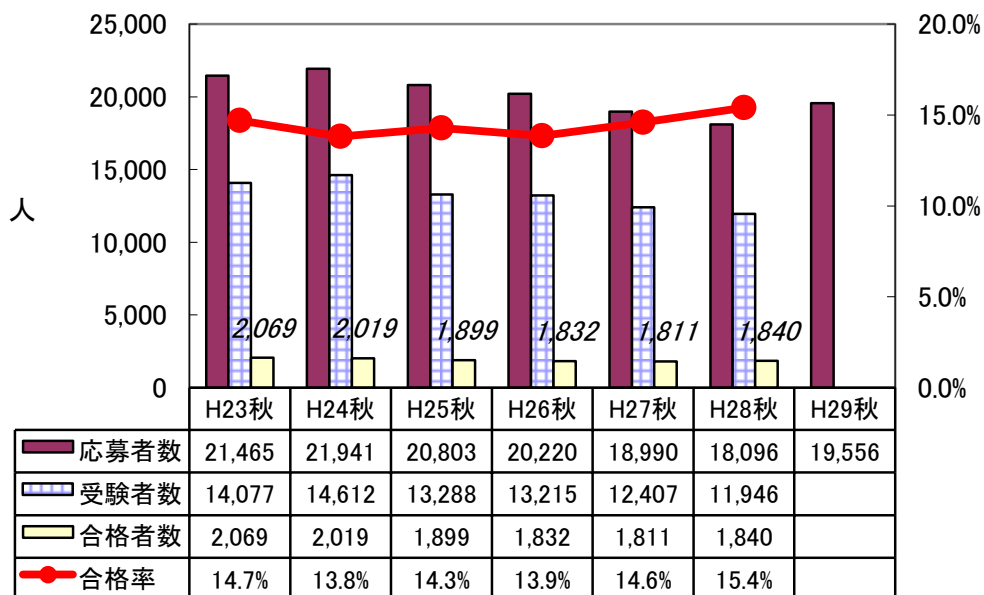
1.1 総評

試験全体の難易度は、前回よりやや高くなりました。これは、前回の午後Ⅰ・午後Ⅱ試験で比較的易しい問題があり、合格率が過去最高の 15.4%で他の高度区分の試験と比較しても 1%以上高かったことから、意図的に難易度を少し上げたのではないかと考えています。ただし、過去全体と比較すると、標準的なレベルの範囲内でしょう。

出題内容の特徴としては、午後Ⅰ・午後Ⅱ試験におけるセキュリティに関する出題が定着してきたことが挙げられます。今回は午後Ⅰ試験の全問と、午後Ⅱ試験の 1 問にセキュリティに関する設問が設定されていました。しかも、詳細なレベルまで問われ、午前Ⅱ試験のセキュリティ分野の知識レベルでは対応できない難しい設問がいくつかありました。今後もこの傾向は続く予想され、午後試験に対応できるセキュリティ技術知識の習得が必須となってきています。

また、新しいネットワーク技術について出題される傾向がある午後Ⅱ試験では、今回も“OpenFlow”や“CDN”，“EDNS-Client-Subnet”，“IEEE802.11ac”といった新しい技術が出題されました。

1.2 受験者数の推移

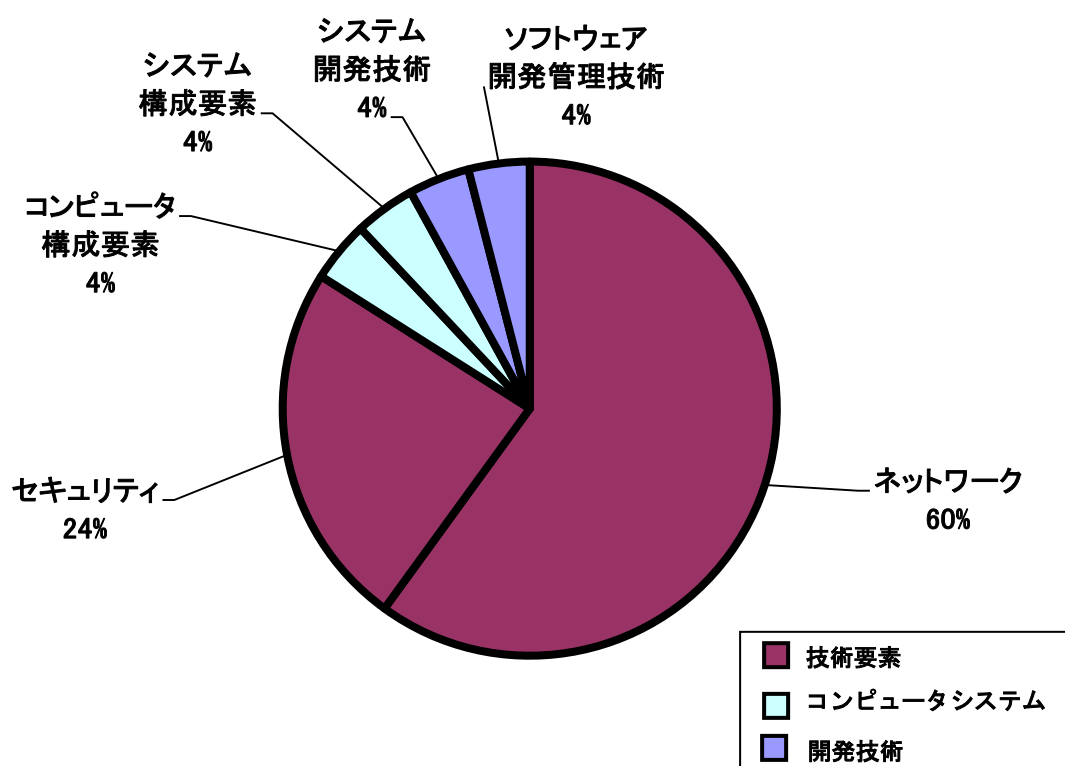


2. 午前Ⅱ問題の分析

2.1 問題テーマの特徴

分野別の出題比率は過去3回と同じです。レベル4の重点分野である「ネットワーク」が15問、「セキュリティ」が6問出題され、レベル3の「コンピュータ構成要素」「システム構成要素」「システム開発技術」「ソフトウェア開発管理技術」はそれぞれ1問ずつとなっています。試験要綱の改訂がなければ、今後も出題比率に変化はないと考えられます。

出題分野	出題比率	出題数
ネットワーク	60%	15 問
セキュリティ	24%	6 問
コンピュータ構成要素	4%	1 問
システム構成要素	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



「ネットワーク」分野を出題範囲の小分類に従って分類すると、TCP/IP を中心とする「通信プロトコル」に関する出題が最も多く出題されており、約半数を占めています。次いで、データリンク制御やルーティング制御が含まれる「データ通信と制御」となっており、従

来と大きな変化はありません。

もう一つの重点分野である「セキュリティ」分野からの出題を小分類に従って分類すると、「セキュリティ対策」から多く出題されており、前回と同様です。そのほかの分野からの出題は、毎回1問であることもあり、はっきりとした出題傾向は認められません。

今回は新規に作成された問題が増えたことが特徴として挙げられます。過去の午前Ⅱ試験における新規問題の割合は約3割ですが、今回は4割が新規問題となっています。特にネットワーク分野で新規問題が多く、5割以上を占めています。ただし、新規問題のテーマを見てみると、これまでに出版された問題と同一テーマのものもあり、新しい知識項目といえるのは、“VLANのVID(VLAN Identifier)”，“OpenFlow”，“FTPのパッシブモード”，“VDI(Virtual Desktop Infrastructure；仮想デスクトップ基盤)”，“MLC(Multi-Level Cell)フラッシュメモリ”の5問で、前回の午前Ⅱ試験での初出題の問題数と同じです。このうち“OpenFlow”は、平成28年10月に発表された出題範囲の改訂によって、ネットワーク分野では唯一付け加えられたネットワーク仮想化からの出題です。

2.2 難易度の特徴

今回は新規問題の出題比率が高く、一見難しそうに思えるかもしれません。しかし、新規の出題であってもテーマは過去に出題されたものもあります。また、過去の出題を午後Ⅰ・午後Ⅱ試験にまで広げて見てみると、“MLCフラッシュメモリ”以外は過去に出題された知識項目であり、目新しいというわけではありません。

再出題された問題の過去の出題年度を見てみると、ネットワークスペシャリスト試験はこれまで、広い年度から少しずつ出題され、旧試験制度のテクニカルエンジニア(ネットワーク)試験から出題されることもありましたが、しかし今回は、2回前の平成27年から4問、3回前の平成26年から5問と新しい年度に集中しており、過去問題演習を行って午前Ⅱ対策をしていれば、高い確率で解いていた問題だと考えられます。

以上のことから、新規問題が増えた影響はそれほど大きくなかったと考えられ、前回より若干難易度が上がった程度でしょう。前回はやや易しかったので、今回は標準的なレベルといえるでしょう。

2.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	ZigBee	B
2	呼量	A
3	RIP-2 と OSPF の相違点	B
4	VLAN の VID のビット長	B
5	スパニングツリープロトコル	B
6	DNS の MX レコード	B
7	ICMP メッセージ	B
8	IPv6 アドレス	C
9	SMTP	C
10	UDP を使用するプロトコル	A
11	ネットワークの制御	B
12	サブネットのブロードキャストアドレス	A
13	OpenFlow	B
14	FTP のコネクション確立	C
15	IP 電話の音声品質指標	B
16	ビヘイビア法	A
17	ダークネットへの SYN/ACK から想定される攻撃	C
18	デジタルフォレンジックス	A
19	DNSSEC	A
20	VDI を用いたセキュリティ対策の設定条件	C
21	DNS amp 攻撃の踏み台防止対策	B
22	MLC フラッシュメモリ	B
23	待ち行列理論	B
24	ソフトウェアの使用性向上施策	A
25	ペアプログラミング	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 問題テーマの特徴

今回の午後 I 試験は、3 問すべてにセキュリティに関連する設問が含まれていたことが特徴として挙げられます。これは前々回あたりから顕著になってきた出題傾向です。ネットワーク技術だけでなく、セキュリティ技術についての学習も深く掘り下げて行っていたかどうかのカギを握っていると考えられます。

問 1 は、SSL-VPN に関する問題です。SSL/TLS コネクション開設時のメッセージと決定される暗号スイートの利用目的、SSL-VPN の三つの方式と特徴などに関する汎用的な知識と、SSL-VPN と VLAN を用いたネットワーク構成の事例に合わせたファイアウォールのルール設定、レイヤ 3 スイッチのアクセスリストの設定などの実務的な知識が問われています。SSL-VPN は平成 25 年の午後 I 試験でも出題されましたが、そのときと比較すると、今回は SSL/TLS の暗号スイートの利用目的といったセキュリティに一步踏み込んだ設問や、不正アクセスを防御するためのアクセス制御の設定など、セキュリティ関連の設問の割合が増えています。

問 2 は、午前 II 試験でも出題された VDI の導入に関する問題です。導入前後の通信経路の違いやネットワーク帯域の違い、帯域制御方法など、ネットワーク技術に関する設問が中心の問題です。VDI については、平成 22 年の午後 I 試験でとり上げられています。セキュリティに関する設問としては、仮想 PC におけるマルウェア感染時の初期対応や、UTM のフィルタリングルールの設定といったネットワークシステム運用時のセキュリティ管理について出題されました。

問 3 は、クラウドサービスとのネットワーク接続がテーマです。インターネット VPN は過去にたびたび出題されていますが、その方式として、IP in IP でトンネルを構成して IPsec で暗号化を行う方式が初めてとり上げられました。前回の午後 II 試験では GRE over IPsec が出題され、MTU の調整について問われましたが、今回も MTU の調整に関連する出題がありました。そのほか、BGP や OSPF といったルーティングプロトコル、ネットワーク監視などについての知識が必要とされています。ルーティングプロトコルは OSPF については前回の午後 II 試験でもとり上げられましたが、BGP と OSPF の二つのプロトコルを利用する事例は初めてです。

3.2 難易度の特徴

問 1 の SSL-VPN に関する問題では、次のような詳細なセキュリティ技術知識が要求されました。

- ・十分な安全性を確保するための TLS のバージョン
- ・SSL/TLS のハローメッセージで決定される暗号スイートの利用目的

これまでもセキュリティ技術に関する設問は出題されてきましたが、このように深いレベルまで問われたことはありませんでした。一方で、実務的な知識を問う設問は、SSL-VPN

と VLAN を用いたネットワーク構成図を理解するのに必要な基礎知識と、問題文を正確に読み取る読解力があれば、解答を導くことができるような比較的易しいレベルでした。以上のことから、問 1 全体としては標準的な難易度と判断しました。

問 2 の VDI の導入に関する問題は、VDI の動作概要などが説明されているので、実務で VDI の経験がなくてもある程度対応できたと思われます。しかし、空欄穴埋め問題が、必要帯域を計算する、フィルタリング設定を答えるなど、いずれも思考力を要するものとなっており、単純に基礎知識をそのまま解答すればよいような設問がほとんどありませんでした。以上のことから、標準的な難易度の設問が中心の問題ということができそうです。

問 3 のクラウドサービスとのネットワーク接続の問題では、BGP と OSPF の二つのルーティングプロトコル間での経路情報の再配布時にループを防止する経路制御といった難易度の高い設問がありました。BGP、OSPF それぞれのプロトコルに関する知識は持っていても、二つのルーティングプロトコルを利用するという問題事例は、平成 17 年の旧テクニカルエンジニア(ネットワーク)試験の午後 I 試験で RIP-2 と BGP が出題されて以降これまで出題されていなかったことから、実務で経験していないと正解を導くのは難しかったと思われます。また、インターネット VPN の方式として、IPsec はたびたび出題されてきましたが、IP in IP のパケットに IPsec を利用する方式は初出題でした。以上のことから、やや難しい問題と判断しました。

また、今回の午後 I 試験は問題文の分量が多くなったことも特徴の一つです。問題文が長いということは、読解に時間がかかるだけでなく、事例が複雑になりやすく、それだけ難易度が高くなることにつながります。

午後 I 試験全体としては、前回は易しい問題が 1 問あったことを考え合わせると、前回より難しくなったといえるでしょう。

3.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	SSL-VPN の導入	B
2	仮想デスクトップ基盤の導入	B
3	社内ネットワークとクラウドサービスとのネットワーク接続	C

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 問題テーマの特徴

午後Ⅱ試験では新しいネットワーク技術がとり上げられる傾向がありますが、今回は、問1でOpenFlowやCDN(Content Delivery Network)、EDNS-Client-Subnetといった新しい技術について出題され、問2では新しい無線LAN規格のIEEE802.11acがとり上げられました。問2では、午後Ⅰ試験と同様にセキュリティ技術についても問われたことが特徴として挙げられます。

問1は「SDNとクラウドの活用」が出題テーマとなっています。午前Ⅱ試験でも出題されたOpenFlowについては、OpenFlowコントローラがOpenFlowスイッチの接続情報を収集する仕組みに関する基礎知識、OpenFlowを採用したネットワーク構成での通信におけるパケットのヘッダ情報や、Flow-ModメッセージによってOpenFlowスイッチに登録される内容などが問われています。OpenFlowは平成25年の午後Ⅱ試験でも出題されています。そのほか、自社運用とクラウドサービス利用切替え時のDNS設定、CDNでEDNS-Client-Subnetを導入した場合の利点、CDN適用によるTAT(Turn Around Time)の改善理由、IaaS環境のバックアップを自社運用にする場合とクラウドにする場合の比較などが問われました。

問2は「無線LANシステムの導入」が出題テーマとなっています。無線LAN規格としてはIEEE802.11nとIEEE802.11acがとり上げられています。IEEE802.11acは、午前Ⅱ・午後Ⅰ・午後Ⅱ試験を通して初めての出題で、使用する周波数帯やチャネルボンディング、MIMO技術について出題されました。また、無線LANの暗号化方式のWEP、WPA、WPA2はいずれも過去に出題されたことがあります。今回は、TKIPのキーストリームの構成要素や、CCMPのカウンタモードによる暗号化／復号手順など、詳細なセキュリティ技術知識が必要とされています。そのほかには、無線LANアクセスポイントの配置設計、無線LANコントローラの導入による利点と障害発生時の問題点、PoEとPoE+、EAP-TLSで使用するクライアント証明書の配布に関する問題点などについて問われています。

4.2 難易度の特徴

問1で出題されたOpenFlowは新しい技術で、とり組みにくいと感じる受験者が多かったと考えられます。詳細な図表を提示しながら、OpenFlowの通信メッセージや通信シーケンスにおける動作などが丁寧に説明されていますが、予備知識がなければ限られた時間内で正確に把握するのは難しいと思われます。過去に一度出題されたことがあるので、この過去問題演習を行ったかどうかの影響は大きいでしょう。また、解答数が多く、ほとんどが事例に合わせた具体的な解答を要求されていることから、問題文の丁寧な読み込みと知識を応用させる思考が必要となり、解答を導くまでに時間がかかります。一方、後半のDNSやCDN、IaaS環境のバックアップの設問は、必要とされる知識レベルはそれほど高くなく、問題文をよく読み取れば解答を導くことができると思います。しかし、前半に時間を取られ、最後にたどり着くまでに時間切れになってしまった受験者もいたでしょう。以上のことが

ら、難易度は高いと判断しました。

問 2 では、無線 LAN の暗号化プロトコルの TKIP や CCMP についての設問は、必要とされる知識レベルが高かったと思います。一方、無線 LAN アクセスポイントの配置設計、無線 LAN コントローラの導入による利点と障害発生時の問題点、PoE と PoE+については、易しい問題ではないものの、平成 25 年の午後Ⅱ試験や平成 24 年の午後Ⅰ試験の無線 LAN に関する問題で類似内容が出題されたことがあり、これらの過去問題演習を行っていれば比較的とり組み易く感じたでしょう。以上のように、知識レベルが高い設問は一部に限られていたことなどから、難易度は標準的なレベルと考えられます。

午後Ⅱ試験全体としては、前回と同様に難易度が高い問題 1 問と標準的なレベルの問題が 1 問という組合せとなり、前回と難易度に差はないといえます。

4.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	SDN とクラウドの活用	C
2	無線 LAN システムの導入	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試験の分野別の出題比率は、ネットワーク分野が 60%、セキュリティ分野が 24% となっています。この 2 分野に的を絞って学習すれば、基準点(60 点)を突破することは十分に可能となります。それ以外の出題分野からは 1 問ずつしか出題されないことや、応用情報技術者試験に合格してステップアップしてきた受験者であればすでに知識を持っているはずの問題が出題されることが多いことから、時間をかけて特別の対策をとる必要はないでしょう。効率的に学習し、午後対策の時間を確保するほうが得策です。

最初にテキストをひととおり読んで、ネットワーク技術とセキュリティ技術の知識を体系的に習得してください。午前Ⅱ試験は 4 者択一式なので、最初から問題演習のみで知識を習得していけば十分だと思われかもしれませんが、それでは解答を丸暗記するだけになりやすく、理解したとはいえません。また、断片的な知識の集まりとなり、知識の関連性が分かりません。

体系的に知識を習得した後に、過去問題演習を行うことは必須です。過去問題の再出題率は 6 割から 7 割もあります。再出題される問題の多くは、過去 5 年以内に出題されたネットワークスペシャリスト試験の問題です。特に今回は 2 回前と 3 回前からが集中して再出題されており、9 問となっています。前回は 3 回前から 5 回前が多く、それより前は広い年度から少しずつ出題されていたので、次の再出題が高い年度を予測するのは難しいですが、少なくとも直近 5 回分は演習しておきましょう。また、セキュリティ分野では旧情報セキュリティスペシャリスト試験の過去問題から再出題されることもあるので、旧情報セキュリティスペシャリスト試験のセキュリティ分野の問題演習を行うことも有効です。

問題演習を行う際の注意点は、必ず解説を読むということです。不正解だった場合はもちろんのこと、正解できた場合でも、他の選択肢の解説から関連知識を得ることができます。このようにすれば、1 問の演習でより多くの知識を習得することができ、違う視点から問われた場合にも対応できるようになります。スキマ時間を有効に活用して問題演習を繰り返し行い、確実に得点に結びつけましょう。

5.2 午後Ⅰ対策

午後Ⅰ試験は、午前Ⅱ試験のように単純に技術知識を問う問題は少なく、事例に知識を適用させて具体的に解答するものがほとんどです。午後Ⅰ問題を解くためには、さらに深い知識とその応用力が必要不可欠です。知識がないということは、事例内容を正しく把握することができない、ヒントとして埋め込まれている記述に気がつかない、読取りに時間がかかるなど、問題文を読解する時点ですでに大きなマイナス要因となります。まずは知識の再習得を行い、レベルアップを図りましょう。

テキストでとり上げられている TCP/IP の各層における主要なプロトコルは、それぞれ深く掘り下げて学習し、詳細な知識を身につけておく必要があります。そのほかの出題頻度

が高いネットワーク技術としては、レイヤ 2 スイッチの機能、無線 LAN、負荷分散などが挙げられます。設問では、事例に合わせた具体的な設定内容や運用方法を解答することが要求されます。実務での経験がない場合は、問題演習によってさまざまな事例の中で経験を積んでください。

また、セキュリティに関する出題割合が高くなってきており、重要テーマの一つといえます。セキュリティ関連の出題は今後も続くと考えられます。暗号化と認証、アクセス制御、セキュアプロトコル(SSL/TLS, IPsec, SSH など)、PKI、迷惑メール対策、ウイルス対策などの知識は必須です。セキュリティ技術についても、今回のように詳細なレベルまで問われる可能性は高いので、深く掘り下げて十分に学習しておきましょう。

さらに、午後Ⅰ試験では、問題文を正確に読み取り、設問文で要求されている内容を正しく理解する読解力や、解答表現を適切な形でまとめる表現力も要求されます。問題文に提示されているネットワーク構成図やフィルタリングルールの表などの図表の読取りも非常に重要です。過去問題や模試などを利用して問題演習を積み重ねることによって、それらの能力を身につけましょう。問題演習を行う際には、正解の表現と自分の解答表現を比較し、間違えた原因は知識不足なのか、読解力不足なのか、表現能力の欠如なのかなどを見極め、それに応じた対策をとることも大切です。また、解いた後は必ず解説をよく読み、解答を導く過程が正しいかも確認するようにしてください。同じ問題を繰り返し解くことも有効です。そうすることによって、問題文を解読するときのポイントや、解答表現を導くためのポイントがつかめるようになっていくと思います。

5.3 午後Ⅱ対策

午後Ⅱ対策は、基本的には午後Ⅰ対策と同様です。午後Ⅱ問題は、問題文の量がただ長いだけではなく、事例の設定条件が複雑になる、複数の技術について問われる総合問題となるという特徴があります。したがって、より多くの深いレベルの知識が要求されるとともに、読解力も午後Ⅰ問題以上に必要とされます。特に、午後Ⅱ問題では多くの図表が提示され、それらから必要な情報を得ることも大切なポイントです。これらの能力を身につけるには、やはり問題演習を数多くこなし、午後Ⅱ問題に慣れることが重要です。

学習すべき具体的な知識項目も午後Ⅰ対策と同様ですが、午後Ⅱ問題では新しい技術を含めて出題されやすいという傾向があります。その場合、新しい技術についての知識が直接問われるのはほとんどが用語レベルです。詳細な仕組みは問題文中に説明されており、その説明を読み取りながら、新しい技術の中で従来技術がどのように使用されているかを考え、従来技術の知識を適用させて解答していくような形式となっています。したがって、新しい技術については、詳細レベルまで理解しているに越したことはありませんが、問題を解くうえでは必ずしもそこまでは要求されず、新しい技術のベースとなっているさまざまな従来技術の知識をより正確に詳細レベルまで習得しておくことのほうがかえって重要です。

また、午後Ⅱ問題では、システムの再構築などをテーマとして、ネットワークシステム

の設計から移行・運用までを通して出題されることがあります。機器の設置や配線，設定情報，テストすべき項目，作業手順などに関するスキルやノウハウはテキスト中心の学習ではなかなか得ることができません。実務経験がない場合は，問題演習を通じて，より多くの事例に接しておくことが有効な対策となります。

問題演習を行う際の注意点としては，解答のポイントとなりそうなキーワードや文章にマークをつけたり，線を引いたりして見落とさないように工夫しながら問題文を読むということです。午後Ⅱ問題では，問題文が長いことから，解答の前提条件やヒントとなる記述が分散していることがよくあります。しかも，問題文中だけでなく，図表や設問文中にもそれらが埋め込まれています。そのため，重要な条件を見落とすというケアレスミスが起きやすくなります。問題演習の段階から，図表の脚注などの細かい部分まで見落とさないように注意深く読み取る習慣を身につけておくといよいでしょう。