ネットワークスペシャリスト

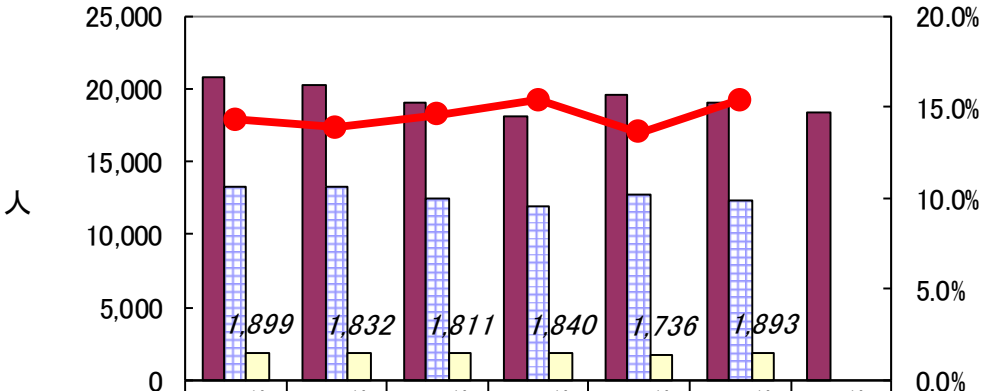
1.　はじめに

1.1　総評

今回のネットワークスペシャリスト試験は，午後試験でセキュリティについて大きく取り上げられたことが特徴として挙げられます。午後Ⅰ試験では「LANのセキュリティ対策」，午後Ⅱ試験では「ネットワークのセキュリティ対策」といった，問題テーマとして「セキュリティ対策」を打ち出した問題が出題されました。これまでも午後試験の一部でセキュリティについて問われることは当たり前のようになっていましたが，出題テーマにはっきりと表れることはあまりなく，ネットワークスペシャリストとしてセキュリティ対策を行うことができる知識や能力が必要であることを印象づける出題内容でした。

午前Ⅱ試験の難易度は，前回と変わりなく，やや易しいレベルでした。午後Ⅰ試験は，定番テーマからの出題が中心となっていましたが，具体的な設定内容を思考するものが多かったことを考え合わせると，標準的な難易度でしょう。午後Ⅱ試験は，セキュリティ対策の問題で新技術が取り上げられたこと，もう 1 問は実務経験者があまり多くないと考えられる IP 電話の知識が一部で要求される問題だったことから，難易度は標準レベルよりもやや高いでしょう。ただし，前回の午後Ⅱ試験が 2 問とも新しい技術を含む難易度の高い問題だったので，前回と比較すると難易度は抑えられているように思います。

1.2　受験者数の推移



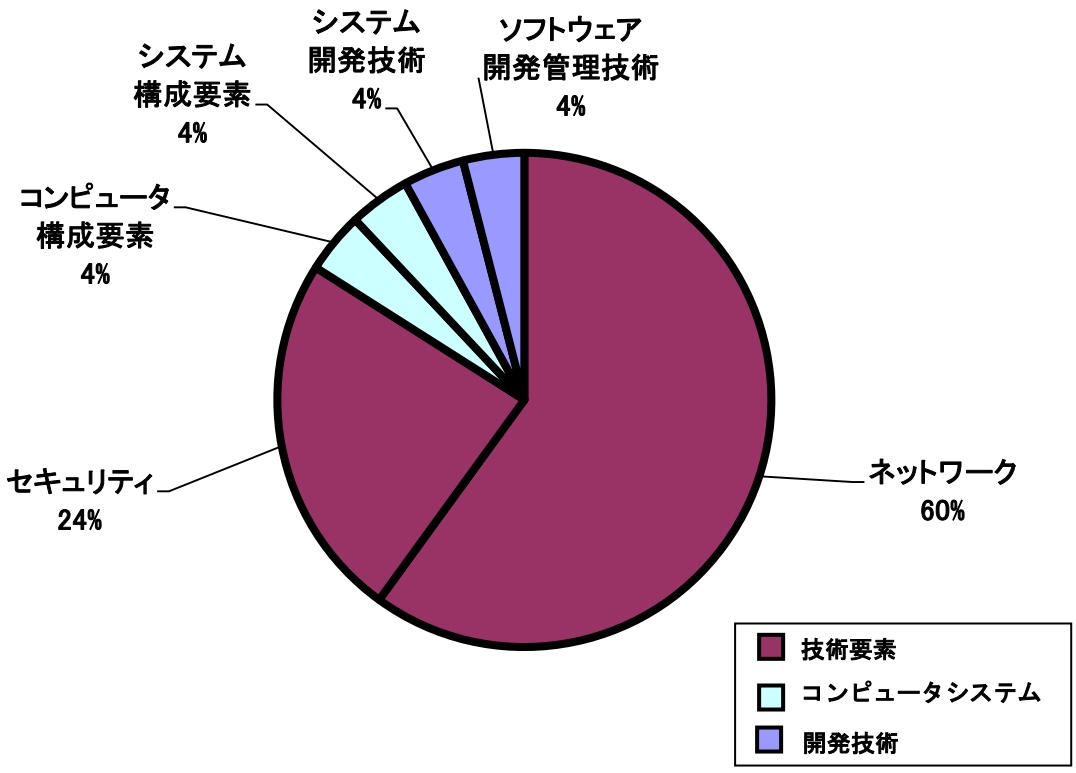
	H25秋	H26秋	H27秋	H28秋	H29秋	H30秋	R1秋
応募者数	20,803	20,220	18,990	18,096	19,556	18,992	18,345
受験者数	13,288	13,215	12,407	11,946	12,780	12,322	
合格者数	1,899	1,832	1,811	1,840	1,736	1,893	
合格率	14.3%	13.9%	14.6%	15.4%	13.6%	15.4%	

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例年通りで変化はありません。レベル 4 の重点分野である「ネットワーク」と「セキュリティ」で 8 割以上を占めています。

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，半数を占めており，例年通りです。ただし，その中でもルーティングプロトコルに関する出題が 3 問もあったことが特徴的です。ルーティングプロトコルは毎回必ず出題されるので，対策を取っていた受験者が多いと思われますが，今後も対策が必須という傾向は変わらないでしょう。そのほかの特徴としては，“SMTP

の EHLO コマンド”,“FTP の PASV コマンド”のように，コマンド名そのものを問う問題が 2 問も出題されたことが挙げられます。コマンドやメッセージが選択肢の文に含まれる問題は時々出題されますが,コマンドやメッセージそのものを直接問う問題は,平成 22 年に SNMP のメッセージが出題されて以来です。選択肢の文に含まれる問題より単純ですが，その分手がかりがなく，コマンドを知っているかどうかだけにかかってきます。今後は，プロトコルの概要だけでなく，やり取りされるコマンドやメッセージなども午前Ⅱ対策の段階から学習しておく必要があるでしょう。また，“OpenFlow”が 3 回連続で出題されたことも特徴の一つです。毎回異なる観点から“OpenFlow”の仕組みや特徴が取り上げられ，最近の注目のテーマであるといえるでしょう。

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，攻撃手法や脅威などを含む「情報セキュリティ」から最も多く出題されました。前回はセキュアプロトコルやネットワークセキュリティなどの「セキュリティ実装技術」が多く，前々回は不正アクセス対策やマルウェア対策などの「セキュリティ対策」が多かったので，出題されやすい小分野は特定できませんが，セキュリティ技術に関する問題がほぼすべてを占め，セキュリティ管理の問題はほとんど出題されない傾向が続いています。

2.2　難易度の特徴

今回の難易度は前回と同程度で，過去の平均から考えるとやや易しいレベルだったと思います。新規問題は前回と同じく 8 問で，難易度が高いと判断した問題数も前回と同じ 5 問です。

新規問題は，テーマとしては過去に出題されたことがあるものがほとんどを占めています。用語として初めて出題されたものは，ネットワーク分野の“SMTP の EHLO コマンド”,“Wi-SUN”,ソフトウェア開発管理技術分野の“CPRM”の 3 問です。“SMTP の EHLO コマンド”は 2 回前に SMTP コマンドの問題が出題されていますが，そのほかの 2 問は目新しく難しいと判断しました。“DNS の NS レコード”と“OpenFlow”はテーマとしては既出ですが，これまでよりも詳細度が上がっています。

セキュリティ分野は 6 問すべてが過去問題の流用でした。4 問が情報処理安全確保支援士(SC)試験の過去問題，2 問がネットワークスペシャリスト(NW)試験の過去問題です。“SSL/TLS ダウングレード攻撃”は SC 試験の過去問題であり，SC 試験まで広げて過去問題演習を行っていない場合を想定すると，迷いやすい選択肢が含まれていることから，難しいと判断しました。

そのほかの特徴としては，今回は 2 回前の平成 29 年の問題から 5 問出題されたことが挙げられます。直前に見直しをしていれば，すぐに正解を導くことができ，試験時間に余裕ができたでしょう。また，毎回必ず出題され，学習も進んでいたであろうルーティングプロトコルの問題が 3 問出題され，しかも 3 問とも過去問題の流用だったことは，得点源になったのではないかと思います。

2.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	IPsec	B
2	OSPF のコスト値	B
3	RIP-2 と OSPF の比較	A
4	スパニングツリープロトコル	B
5	BGP-4	A
6	CIDR	A
7	DHCP リレーエージェント	A
8	DNS の NS レコード	C
9	SMTP の EHLO コマンド	B
10	VRRP	A
11	ネットワークの制御	B
12	OpenFlow	C
13	FTP の PASV コマンド	B
14	WebDAV	A
15	Wi-SUN	C
16	SSL/TLS ダウングレード攻撃	C
17	Cookie の Secure 属性	B
18	ダークネットを利用した攻撃	B
19	ポートスキャン	B
20	ルートキット	A
21	DNS リフレクタ攻撃の踏み台防止策	B
22	プロセッサの構成要素	A
23	ピアツーピアシステム	B
24	UML のユースケース図	A
25	CPRM	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

今回の午後Ⅰ試験は，以前の出題傾向に戻った印象があります。前回は午後Ⅰ試験でも新技術について問われ，「午後Ⅰでは従来技術，午後Ⅱでは新技術」というそれまでの傾向と異なりましたが，今回は従来技術からの出題となっていました。

出題内容を見てみると，冗長化，負荷分散，ネットワークセキュリティといった，いずれも定番テーマからの出題でした。一見すると定番テーマで取り組みやすいように思いますが，詳細な知識が必要とされる設問もあり，決して易しいというわけではありません。また，3問とも事例に合わせた具体的な内容を問う設問が含まれ，知識だけでなくその応用力も求められています。午後Ⅰ試験全体としては，標準的な難易度でしょう。

3.2 各問題のテーマ，特徴

問1は「ネットワークの増強」というテーマで，回線やネットワーク機器の冗長化が出題の中心となっています。VRRPやVLANは頻出の知識項目で，前回も出題されています。リンクアグリゲーションもたびたび取り上げられていますが，動的に設定する際に利用するLACPプロトコルについては初出題です。静的に設定する場合と比較してLACPで実現可能なことを記述する難問が出題されました。そのほかには，ルーティングプロトコルやSNMP，Gratuitous ARP，pingなどの知識が必要とされ，3問の中では最も幅広い知識が求められていますが，いずれも直近5回以内の午後問題で出題された知識項目です。これらはほとんどが空欄穴埋め問題であり，午前Ⅱレベルの知識で対応可能なものもあります。

問2は「Webシステムの構成変更」というテーマで，Webアクセスの負荷分散について出題されました。DNSラウンドロビンによる負荷分散のセッション維持についてはこれまでにも複数回出題されており，過去問題演習を行っていれば解答しやすかったのではないかと思います。ただし，今回は通信が暗号化されていることと絡めて解答を導く必要があり，そこに気が付くことができたかどうかがポイントとなるでしょう。そのほかでは，WAFサービスを利用する場合と，利用しない場合でのDNSサーバのゾーンファイルの設定や，ファイアウォール(FW)の設定，負荷分散装置の設定など，具体的な設定内容が問われ，応用力が求められています。また，HTTPのSet-Cookieフィールド，Cookieフィールド，レスポンスのステータスコードなど，名称や値を覚えていなければ解答できないものもあります。このうち，Set-Cookieフィールドは平成27年午後Ⅰ問題で出題されていますが，うろ覚えの場合はHTTPリクエストとHTTPレスポンスのどちらのフィールドか迷ったでしょう。ステータスコードは初めての出題ですが，問題文中の図に示されていたことが何度かあります。HTTPのX-Forwarded-Forヘッダフィールドも初出題ですが，どのように利用するかは問題文中に説明されているので，その説明を理解できるだけの知識があれば支障はないと思います。

問3は「LANのセキュリティ対策」というテーマで，LAN通信制限の実現策としてDNSスヌーピングを用いる方法とARPスプーフィングを用いる方法が取り上げられました。DNSス

ヌーピングは平成25年の午後Ⅰ問題で出題されましたが，今回はポートの設定という知識レベルが一段高い問題が出題されました。また，ARPスプーフィングは初めての出題で，中間者攻撃と同様の仕組みで監視を行うことを理解していないと難しかったでしょう。また，通信制限装置の接続といった機器の接続の問題は頻出問題ですが，問題文の記述内容をどうとらえればよいのか悩む問題でした。一方で，不正PCを接続するセグメントとの通信を許可する機器や，そのセグメントを追加することによって設定に変更が生じる機器と変更内容といった問題は，問題文を慎重に読み取れば対応可能な問題です。

以上のことから，問3はセキュリティの深い知識を要求されるなど高度な知識が必要な設問が複数あることから，やや難しいと判断しました。問1と問2は難しい設問も一部にありましたが，知識の習得と過去問題演習という対策を取っていれば対応可能な問題のほうが多いと思われることから，標準的なレベルでしょう。

3.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	ネットワークの増強	B
2	Webシステムの構成変更	B
3	LANのセキュリティ対策	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 全体の出題傾向及び難易度について

午後Ⅱ試験は，幅広い知識が要求される総合問題として出題されることがよくあります。しかし今回は，問1がIP電話システムを含むネットワークシステムの移行の問題，問2がネットワークのセキュリティ対策の問題となっており，2問とも出題範囲が限定的でした。このように，2問とも限定的なテーマで出題されることは珍しいですが，平成26年の午後Ⅱ試験で今回と同様のテーマの組合せで出題されたことがあります。

また，午後Ⅱ試験では新しいネットワーク技術について出題される傾向があります。今回もセキュリティ対策の問題の中で，攻撃を防ぐための新しい技術が複数取り上げられました。

IP電話システムの業務経験がある人はそれほど多くないと考えられ，問2を選択した人のほうが多いのではないかと予想しています。しかし，SIPやIP-PBXなどIP電話システムに関する知識レベルは，平成26年の問題ほど高くなく，基礎知識さえ持っていれば問題文を読み取って解答できる設問も複数ありました。

一方，これまで新技術についての出題では，新技術そのものの知識が問われることはほとんどなく，問題文に記述されている新技術についての説明を読み取り，従来技術の知識を応用させて理解したうえで解答を導くようになっていました。しかし，今回の問2では，新しい技術そのものの動作を説明する難易度の高い問題が出題されました。

前回は2問とも新技術を含み難易度が高かったことと比較すると，今回は標準的か，やや高いレベルに収まっていると思います。

4.2 各問題のテーマ，特徴

問1は「クラウドサービスへの移行」がテーマとなっています。システムの移行はこれまでにも何回か出題されたことがありますが，今回はIP電話システムを含むネットワークシステムの移行が対象となっており，SIPの通信シーケンスなどに関する知識も要求されています。利用するクラウドサービスは，IaaSのほか，PBXサービスも含まれており，これに伴ってシステム構成を変更し，機器の切替えや設定の変更を行う手順と変更内容などが具体的に問われています。IP電話機間の通話だけでなく，社内や外出先でのスマートフォンを活用した通話や保留転送を行う仕組みは，初めての出題です。また，本社と支店間の通話，公衆電話網を介した取引先との通話など，場合分けしながらそれぞれの通信経路や移行手順を理解する必要があります。いずれも知識レベルはそれほど高くはありませんが，問題文を正確に読み取る読解力が要求され，両者を考え合わせると標準的な難易度といえるでしょう。

問2は「ネットワークのセキュリティ対策」というテーマで，さまざまなセキュリティ対策技術が出題されました。この中で取り上げられたSYNフラッド攻撃とDNSキャッシュポイズニング攻撃は，平成26年の午後Ⅰ問題で出題されたことがありますが，今回のように

詳細まで問われるのは初めてです。新しい技術として，uRPF，SYN パケットのディレイドバインディング，SYN クッキーなど複数の技術について問われ，難易度がやや高い問題です。特に uRPF については，動作そのものを説明する問題が出題され，知識がなければまったく解答できない難問です。SYN クッキー技術については，TCP コネクション確立時の 3 つのパケットのシーケンス番号と確認応答番号がどのように設定されるかという基本的な知識を持っていれば対応可能なはずですが，慎重に解答しないと混乱しやすいでしょう。DNS キャッシュポイズニング攻撃の対策では，FW のフィルタリングルールを読み取る能力や，攻撃の仕組みを理解したうえでの DNS パケットのヘッダ情報の知識が求められています。そのほか，マルウェア侵入対策を取り上げた問題文では，C&C サーバ側が用いる Fast Flux という手法や Domain Flux という手法について説明されています。いずれも SC 試験でも出題されたことがない手法が，NW 試験で出題されたことに驚きます。ただし，設問で問われているのは，C&C サーバへアクセスするときの FQDN や，プロキシ認証で記録されるログ，プロキシサーバを経由するときと経由しないときの DNS 問合せの経路などで，NW の試験範囲を逸脱するようなものではありません。DNS 問合せの経路は正しく把握していないと FW の設定で不正な通信を遮断できないので，しっかりと理解しておくことが求められています。

4.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	クラウドサービスへの移行	B
2	ネットワークのセキュリティ対策	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。

最初にテキストを用いて学習し，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。このとき，用語を丸暗記するのではなく，仕組みをきちんと理解しておくと，午後対策にスムーズに入ることができるでしょう。

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 割を占めています。今回は 2 回前の NW 試験から 5 問も出題されました。ただし，何回前からの過去問題が多く出題されるかは毎回異なるので，少なくとも直近 5 回分は演習しておきましょう。また，今回のようにセキュリティ分野では SC 試験の過去問題から再出題されることもたびたびあります。NW 試験の過去問題に加えて，SC 試験のセキュリティ分野の過去問題も演習を行っておくとよいでしょう。

問題演習を行う際には，必ず解説を読むということが大切です。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。午前Ⅱ問題演習は移動時間や短い空き時間でも行うことができるので，このようなスキマ時間を有効に活用して間違える問題がなくなるまで演習を繰り返しましょう。試験直前にも忘れていないか確認するために再演習を行うと効果的です。

5.2 午後Ⅰ対策

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。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。知識がなければ，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。まずはテーマごとに個々の知識を掘り下げて学習しましょう。

TCP/IP の各層における主要なプロトコルは，コマンドやメッセージ，パラメタ，属性などに至るまで詳細な知識を習得し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，セキュリティも重要テーマの一つとなっています。暗号化と認証，アクセス制御，VPN，PKI，迷惑メール対策，ウイルス対策などの知識は必須です。今回はサイバー攻撃についての知識も要求されたことから，主要な攻撃手法とその対策も学習しておくとよいでしょう。

知識を深めた後に，習得した知識を事例に適用させる応用力が身についているかを確認するために，過去問題演習を行うことは必須です。今回は過去に問われた論点と同一の論点が多く出題され，過去問題演習の効果が非常に高かったと考えられます。少なくとも過去5回分の午後Ⅰ問題演習を行い，時間に余裕があれば，さらにさかのぼって問題演習を行うようにするとよいでしょう。過去 5 回分の午後Ⅰ問題をすべて解いて理解するには相応の時間が必要となりますが，合格を勝ち取る手段としては最適です。

また，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。過去問題演習を行うことは，知識の応用力を養うだけではなく，読解力や解答表現力を養うことにも役立ちます。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。弱点分野を把握し，強化すべき分野を洗い出すようにするとよいでしょう。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り，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，より広い範囲にわたって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。今回は例外もありましたが，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。新しい技術についての特別な知識を持っていなくても，多くの場合は解答できるようになっていますが，説明を理解するまでにかなりの時間がかかります。知識を持っていれば読解時間を短縮でき，明らかに有利です。最近は SDN や IoT に関連する技術がよく出題される

ので，これらの技術について概要を把握しておくとよいでしょう。

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るため，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よいでしょう。