情報処理安全確保支援士

1.　はじめに

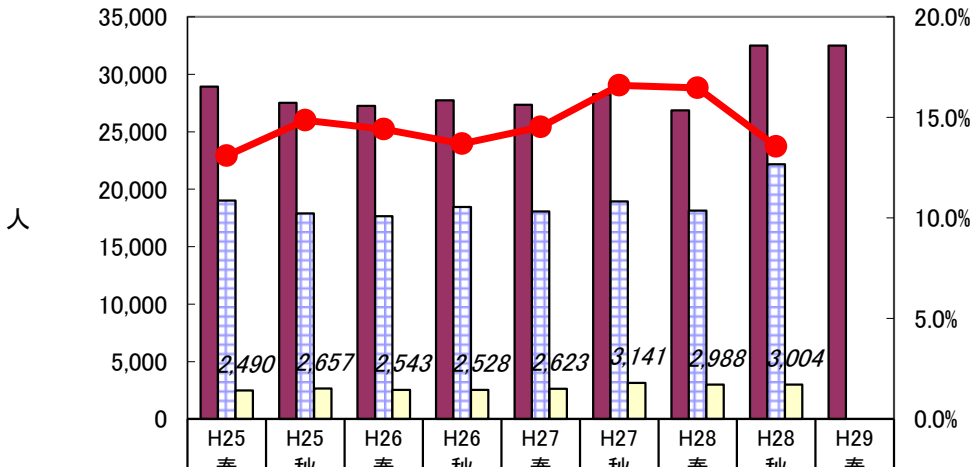
1.1　総評

情報処理安全確保支援士試験は，情報セキュリティスペシャリスト試験(以降，旧 SC 試験という)に代わって新たに創設されて初めての試験ということで注目が集まっていました。試験要綱やシラバスの内容は，いくつかの用語が追加された程度でほとんど変更がなかったことから,弊社では旧 SC 試験と大きく傾向が変わることはないと予想していました。結果は，出題形式や出題テーマに差異はなく，旧 SC 試験をそのまま踏襲しています。午前Ⅱ試験では攻撃手法や暗号化・認証技術が多く出題され，午後Ⅰ・午後Ⅱ試験ではセキュリティインシデント対応，Web アプリケーションのセキュリティなど旧 SC 試験の定番テーマが出題されました。セキュリティ技術の知識とその実務的な応用力を問う試験内容となっています。

試験全体の難易度は，直近の旧 SC 試験と比較するとやや難しかったと思います。午前Ⅱ試験と午後Ⅰ試験は標準的なレベルでしたが，午後Ⅱ試験は 2 問とも難易度が高い問題でした。必要とされる技術知識はネットワーク技術知識も含めて詳細度が高く，具体的な設定内容やログの抽出条件など実務に直結する設問が数多く含まれています。

今後も情報処理安全確保支援士として実務に対応できる高い技術知識と適応力が求められていくでしょう。

1.2　受験者数の推移



	H25 春	H25 秋	H26 春	H26 秋	H27 春	H27 秋	H28 春	H28 秋	H29 春
応募者数	28,930	27,522	27,246	27,735	27,339	28,274	26,864	32,492	32,493
受験者数	19,013	17,892	17,644	18,460	18,052	18,930	18,143	22,171	
合格者数	2,490	2,657	2,543	2,528	2,623	3,141	2,988	3,004	
合格率	13.1%	14.9%	14.4%	13.7%	14.5%	16.6%	16.5%	13.5%	

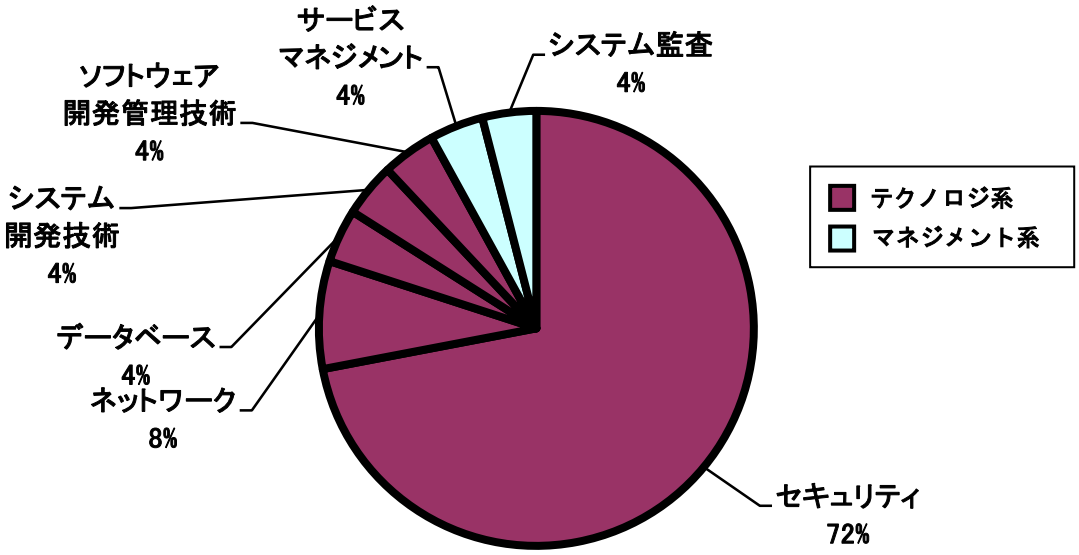
2.　午前Ⅱ問題の分析

2.1　問題テーマの特徴

直近の旧 SC 試験と比較すると，重点分野とされるレベル 4 の「セキュリティ」が 1 問増えて 18 問，「ネットワーク」が 1 問減って 2 問となっています。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，変動はありません。

セキュリティとネットワークの知識は，当然のことながら午後試験でも必須なので，午前Ⅱの出題比率が多少変化しても合否への影響はほとんどないでしょう。

出題分野	出題比率	出題数
セキュリティ	72%	18 問
ネットワーク	8%	2 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，さらに小分類にまで分類してその内訳を見てみると，攻撃手法や暗号化・認証技術が含まれる「情報セキュリティ」からの出題が多く，8 問となっています。次いで，セキュアプロトコルや認証プロトコルなどが含まれる「セキュリティ実装技術」，アクセス制御やマルウェア対策などが含まれる「情報セキュリティ対策」の

順となっています。毎回出題数の少ない，ISMS やセキュリティ組織などの「情報セキュリティ管理」と，JCMVP や CVSS などの「セキュリティ技術評価」からの出題は，それぞれ 1 問のみでした。今回は，より多くの攻撃の手口について問われたことが特徴として挙げられます。“SSL/TLS ダウングレード攻撃”，“サイドチャネル攻撃”など六つの攻撃について出題されています。前回および前々回では攻撃手法は 3 問のみだったので，倍増していることになります。その分，毎回必ず出題されていた認証局やディジタル証明書といった公開鍵基盤の問題が今回はありませんでした。

「ネットワーク」分野からの出題テーマは，旧 SC 試験では IP，TCP，DNS，HTTP，メールシステムなど午後問題を解くうえで前提となるような知識についての出題が多くとり上げられてきました。その点，今回出題された“Automatic MDI/MDI-X”は，異色ということができるでしょう。

その他の分野からの出題テーマは，セキュリティに関連するようなテーマから出題されています。

新規問題としては，「セキュリティ」分野からは“SSL/TLS ダウングレード攻撃”，“セッションフィクセーション攻撃”，“DNS 水責め攻撃”，“MITB 攻撃の対策”，“フォールスネガティブ”が出題されました。新規問題のほとんどが攻撃に関するものであるという特徴があります。これらのうち，“DNS 水責め攻撃”は異なる観点から過去に出題されたことがあります。また，“セッションフィクセーション攻撃”，“MITB 攻撃の対策”，“フォールスネガティブ”は午後問題で出題されたことがあります。したがって，目新しい用語は“SSL/TLS ダウングレード攻撃”のみです。そのほかの新規問題は「ネットワーク」分野から“Automatic MDI/MDI-X”，「システム監査」分野から“IT に係る保証業務の三当事者”が出題されました。

2.2　難易度の特徴

要求されている知識レベルが特別に高いという問題はなく，午前Ⅱ試験として標準的なレベルといえるでしょう。

攻撃に関する新規問題の 4 問は，迷いやすい選択肢が含まれていることから，難易度が高いレベルに分類しました。例えば，“DNS 水責め攻撃”は，攻撃対象サーバがどこかということを正しく把握していないと解答に迷ったと思います。そのほかでは，“Automatic MDI/MDI-X”は，異色の出題だったことから，難しく感じた受験者が多かったでしょう。また，“OAuth2.0”は，過去問題を一部変更して再出題された問題ですが，比較的新しい技術であることから，難易度が高いとしています。

過去問題の再出題率は約 7 割です。旧 SC 試験では 6 割から 7 割程度であったことから，従来どおりといってよいでしょう。3 回前の平成 27 年度秋の旧 SC 試験からの再出題が多く，5 問出題されました。この「3 回前の過去問題から数多く再出題される」という傾向も旧 SC 試験と同じです。そのほか 4 回前から 2 問，5 回前から 3 問出題され，この 3 回分の合計は 10 問にもなります。6 割以上の正答率で合格する試験において全体の 4 割を占めていることから，これらの回の演習を行ったかどうかが難易度の感じ方に大きく影響するでしょう。

2.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	AES の特徴	B
2	SSL/TLS ダウングレード攻撃	C
3	サイドチャネル攻撃	A
4	TPM が持つ機能	B
5	セッションフィクセーション攻撃	C
6	DNS 水責め攻撃	C
7	FIPS PUB 140-2	A
8	クラウドサービスにおけるセキュリティパッチの管理と適用	B
9	リスク回避	A
10	CVE 識別子	B
11	MITB 攻撃の対策	C
12	OS コマンドインジェクション	A
13	フォールスネガティブ	A
14	OAuth2.0	C
15	OP25B の導入目的	B
16	サンドボックスの仕組み	A
17	IEEE802.1X と RADIUS の実装方法	B
18	ICMP Flood 攻撃	B
19	Automatic MDI/MDI-X 機能	C
20	CSMA/CA	A
21	SQL の GRANT 文	B
22	システム及び/又はソフトウェア製品の品質特性	B
23	DTCP-IP	B
24	データベースのバックアップと復旧	B
25	IT に係る保証業務の三当事者の組合せ	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 問題テーマの特徴

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ます。旧SC試験の直近5回の午後Ⅰ試験でも，セキュリティ技術知識を中心に問う出題傾向が定着しており，その出題傾向が引き継がれています。セキュアプログラミングの問題が1問出題された点も，旧SC試験と同じです。

問1は，セキュリティインシデント発生後の調査と対策について出題されました。マルウェアがARPポイズニングを用いた中間者攻撃によって利用者IDとパスワードを盗聴し，顧客情報を管理するサーバへの不正侵入を行おうとするまでの手順と，これを防ぐためのネットワーク構成やファイアウォールのフィルタリングルールの設定などが問われています。ARPポイズニングは，平成25年秋午後Ⅱ問1で出題されたことがあります。そのほか，LDAPやSSH，HTTP over TLSといったプロトコルがとり上げられています。

問2は，Webシステムにおけるクロスサイトスクリプティング(XSS)とクロスサイトリクエストフォージェリ(CSRF)の脆弱性に関するセキュアプログラミングの問題です。平成28年春午後Ⅰ問1で同様のテーマで出題されています。XSSやCSRFの脆弱性を用いた攻撃の仕組みと対策に関する知識とともに，HTMLの基本的なソースを読み取ることができる知識とイベントハンドラ属性の知識が必要です。

問3は，クラウドサービスとLDAPサーバとの間でのSAMLを利用した認証連携に関する問題です。社員が社外からクラウドサービスにアクセスすることを防止するための認証連携の仕組みなどについて問われています。LDAPサーバでの利用者アカウント情報の一元管理は問1でも出題されていますが，旧SC試験でも最近時々とり上げられており，出題頻度が高くなっています。SAMLは午前Ⅱでは頻出テーマとなっていますが，午後問題で出題されるのは平成22年秋以来です。本問ではSAMLを用いた認証連携にブラウザを経由したHTTPリダイレクト方式を用いており，HTTPの基本的な仕組みと，ディジタル署名に関する知識も要求されています。

3.2 難易度の特徴

直近の旧SC試験では，その前年度に報告された重大な組込み機器の脆弱性をとり上げた新規性の高い問題が1問出題されました。しかし，今回の午後Ⅰ試験は3問とも過去に出題されたことがあるテーマが中心となっており，取り組みやすかったと思います。必要とされる知識レベルもそれほど高くはありません。しかし，問題文の事例を短時間で正確に把握し，事例内容に合わせた具体的な解答表現を導くためには，あいまいな知識では対応できません。セキュリティ技術とネットワーク技術の基本的な知識の正確性が求められています。また，直近2回の旧SC試験では，問題文のボリュームが抑えられ，時間的に厳しいということはありませんでしたが，今回の試験ではそれ以前のボリュームの大きい問題に戻り，時間的な余裕はありません。以上のことを考え合わせると，午後Ⅰ試験全体の難

易度は標準的なレベルでしょう。

問 1 は，ARP ポイズニングの仕組みを理解しているかどうかにかかっています。ARP は最も基本的なネットワーク技術の一つなので，ほとんどの受験者は理解できていると思います。本問では，ARP テーブルをどのように偽装すれば，通信の間に入って目的の利用者 ID とパスワードの盗聴を行うことができるかという攻撃者の立場で思考する必要があり，応用力が求められる内容です。そのほかでは，誰がどのホストにログインする場合にどのサービスを利用するかということを事例から正しく読み取るのに必要な知識と読解力も要求されます。知識レベルはいずれも基本的なものですが，決して易しい問題とはいえません。

問 2 は，XSS と CSRF はいずれも定番テーマで，しかも 2 回前にも出題されていたことから，学習していた受験者が多いと考えられます。午前Ⅱ試験レベルの知識では通用しませんが，それぞれの脆弱性を用いた攻撃の仕組みや対策についてひととおり学習していれば，解答を比較的容易に導くことができる設問が含まれています。難易度は標準的なレベルでしょう。

問 3 は，午後試験では久しく出題されていなかった SAML による認証連携ということで，一見難しそうに思うかもしれません。しかし，提示されているシーケンス図の空欄穴埋め問題には解答群がついており，容易に解答を導くことができます。そして，このシーケンス図をもとにすると，問題文に記述されている認証連携の動作内容を理解しやすくなり，難易度が抑えられています。注意深く読解すれば解答を導出できる設問もあり，知識レベルは高くありません。難易度はほかの 2 問と同様に標準的なレベルということができるでしょう。

3.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	社内で発生したセキュリティインシデント	B
2	Web サイトのセキュリティ対策	B
3	クラウドサービスの認証連携	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 問題テーマの特徴

午後Ⅱ試験は，2 問ともマルウェア感染の調査と対策を含む実務的な出題内容となっています。セキュリティ技術の知識とそれを実務に適用する応用力が問われています。直近の旧 SC 試験では，セキュリティ技術を中心に，一部で CSIRT の体制や共通脆弱性評価システム(CVSS)といったセキュリティ管理面から問われる内容となっていましたが，今回はセキュリティ管理面からの出題はありませんでした。出題範囲やシラバスにはリスク分析や人的管理などセキュリティ管理に分類されるような内容が含まれていますので，傾向が変わってセキュリティ管理面からの出題が一切なくなるというわけではないと考えています。

問 1 は，マルウェアの詳細な解析用環境上での通信の観測による解析や，デバッガを用いた解析について出題されています。解析によってマルウェアの動作や影響範囲を特定し，応急措置と再発防止策を導くような流れになっています。旧 SC 試験において，マルウェアの解析ではログの調査がたびたび出題されてきましたが，今回はより詳細な解析方法が提示されています。そのほかに必要とされる知識は，サーバ証明書，URL フィルタリング，脆弱性修正プログラムの更新，ウイルススキャン，ディジタルフォレンジックスなどです。

問 2 は，業者とメールによる情報交換を行う環境でのマルウェア感染の調査と対策が問われています。マルウェアが保持している FQDN の TXT レコードを問い合わせた結果の文字列を指令として解釈して動作し，メール送信機能も持つという条件設定がなされており，メールシステムと DNS に関するネットワークの知識が要求されています。マルウェアに感染した PC，内部メールサーバ，外部メールサーバ，内部 DNS サーバ，外部 DNS サーバの間を，どこからどこへどの順にパケットが流れるかを問題文に記述されている内容を読み取って判断する必要があります。そのほか，プロキシサーバやウイルススキャンなどについて問われています。

4.2 難易度の特徴

午後Ⅱ試験は 2 問とも，要求されるセキュリティやネットワークの技術知識が高度かつ実務的です。旧 SC 試験の午後Ⅱ試験と比較しても，知識レベルの高い問題に位置づけられるでしょう。また，知識をそのまま解答する問題はほとんどなく，問題事例を踏まえたうえでの具体的な解答を求められているので，知識の応用力が必要とされます。さらに，問題文のボリュームが非常に大きかったことから，限られた時間内に問題事例を読み込んで設問要求に合った適切な解答を導くためには，素早い読解力も必須です。難易度はいずれも高かったといえるでしょう。

問 1 で出題されたマルウェア解析方法は，問題文を読み込むことである程度まで把握することができますが，マルウェアがデバッガ環境下であることを検知する方法など実務で経験したことがないと解答を導くことが難しく，専門的な知見が要求されるものもあります。実務経験の差が合否に結びつく可能性が高いと考えられます。また，脆弱性修正プロ

グラムの適用に関する設問では，同様の内容と対策が考えられ，それぞれの設問でどの問題点を解答すればよいか迷うことがあったかもしれません。

問 2 は，ネットワーク技術知識の有無に左右されるでしょう。マルウェアの動作を理解し，対策を講じるために必要とされる，メールシステムと DNS の知識は，午前Ⅱ試験レベルでは不十分です。特に DNS については，事例内容から内部 DNS サーバと外部 DNS サーバそれぞれに必要な設定は何かを見極める実務的な応用力が必要です。セキュリティ技術についての知識は十分に持っていても，ネットワーク技術の知識が欠如していると正解を導くのは難しい設問が複数あります。

4.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	マルウェアの解析	C
2	社内システムの情報セキュリティ対策強化	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

情報処理安全確保支援士試験の午前Ⅱ試験の出題傾向は，旧 SC 試験と比較して変化がなかったことから,午前Ⅱ対策もこれまでの旧 SC 試験での対策と同じでよいと考えられます。

直近の旧 SC 試験と比較すると，重点分野の「セキュリティ」と「ネットワーク」の出題比率が多少異なりますが，2 分野の合計が 8 割を占めることは同じです。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試験に合格できることになります。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行ったほうが，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りますので，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。

過去問題の再出題率が高いことから，知識習得後は過去問題演習が必須です。問題集や e-ラーニングによる問題演習を利用して，効率的に演習を行うようにしましょう。このとき，出題比率を念頭に置いて問題演習を行うと効果的です。具体的には，攻撃手法や暗号化・認証技術の出題比率が最も高いので，重点的に演習を行うとよいでしょう。問題演習を通じて自分の苦手な分野を洗い出し，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。過去問題演習は，直近 5 回分程度を目安にするとよいでしょう。特に 3 回前からの再出題が多いことから，試験直前に 3 回前の過去問題演習を行うことは非常に有効です。公開模試でもこの傾向を意識し，同じテーマについて同じ観点での問題，あるいは，同じテーマで異なる観点から出題された場合を想定した問題もとり入れて出題していますので，十分に活用してください。

また，毎回新しい攻撃について出題されていることから，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と思います。

5.2 午後Ⅰ対策

午後試験の出題範囲は，旧 SC 試験と同じで，次のようになっています。

1 情報セキュリティシステムの企画・要件定義・開発・運用・保守に関すること
2 情報セキュリティの運用に関すること
3 情報セキュリティ技術に関すること
4 開発の管理に関すること
5 情報セキュリティ関連の法的要求事項などに関すること

午後Ⅰ試験では，セキュリティ技術寄りの出題傾向が強く，1～3 の「情報セキュリティシステムの企画・要件定義・開発・運用・保守に関すること」,「情報セキュリティの運用に関すること」,「情報セキュリティ技術に関すること」の出題頻度が高くなっています。具体的には,「情報セキュリティシステムの企画・要件定義・開発・運用・保守に関するこ

と」の中では，アプリケーションのセキュリティ対策，セキュアプログラミング，ネットワークセキュリティ対策，サーバ・クライアント・セキュリティ装置などのシステムセキュリティ対策などが主に出題されています。また，「情報セキュリティの運用に関すること」の中では，情報セキュリティポリシ，脆弱性分析，不正アクセス対策，インシデント対応などが出題されやすく，「情報セキュリティ技術に関すること」の中では，アクセス管理技術，マルウェア対策技術，暗号化技術，認証技術，PKI，ログ管理技術などの出題頻度が高くなっています。したがって，午後Ⅰ試験対策としては，これらを中心に深い知識を習得しておく必要があります。

特に，旧 SC 試験ではセキュアプログラミングに関する問題がほぼ毎回 1 問出題されており，今回も出題されたことから，今後も出題される可能性は非常に高いと考えてよいでしょう。セキュアプログラミングの問題は，プログラミング経験のない受験者は選択しないことが考えられます。その場合，残りの 2 問を必ず選択することになるので，ほかに苦手な項目を作らないようにより一層しっかりと対策を行うことが求められます。セキュアプログラミングを選択する場合は，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，教材の一つとして利用するとよいでしょう。

また，ネットワーク技術知識の習得も重要です。ネットワーク構成図や事例内容から，何のパケットがどの経路で流れていくか，パケットの送信元 IP アドレスは何かなどを読み取る基礎的な知識が必要です。TCP/IP のプロトコルとしては，インターネット層では IP，ICMP，ARP，トランスポート層では TCP と UDP，アプリケーション層では HTTP，DNS，SMTP，LDAP，SSH などが問題文を読み取るうえで必須の知識となります。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，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，午後Ⅰ対策は，テキストを中心とした知識の習得が不可欠であることはもちろんですが，その後に必ず問題演習を行うことが非常に重要です。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がよくあります。その最大の要因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。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していますので，問題演習を行った後に解説をしっかり読むことが大切です。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

今回の午後Ⅱ試験では，セキュリティ管理の知識が問われませんでしたが，旧 SC 試験ではセキュリティ技術とセキュリティ管理の両方の知識が必要となる総合問題が出題されることがありました。今後も一部でセキュリティ管理の知識が要求されることが考えられま

すので，セキュリティ管理面の知識を補充しておく必要があります。午後Ⅰ対策で提示した，午後試験の出題範囲の4と5の「開発の管理に関すること」「情報セキュリティ関連の法的要求事項などに関すること」が該当します。「開発の管理に関すること」の中では，ソフトウェアの配布と操作，人的管理手法，脆弱性情報収集管理などが比較的出題されやすいと考えられます。「情報セキュリティ関連の法的要求事項などに関すること」の中では，ISMSに関するJIS Q 27000，27001，27002や，サイバーセキュリティ基本法，個人情報保護法，不正競争防止法についての概要を習得しておいてください。

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，必要とされる技術知識のレベルと習得した技術知識のレベルが合っ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，問題文の読解力が大きなカギを握っています。問題本文と設問文中で提示された条件や要求事項との関係がどのようになっているかを整理し，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ったり戻ったりすることになり，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中に示されているようなこともよくあります。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。