情報処理安全確保支援士

1. はじめに

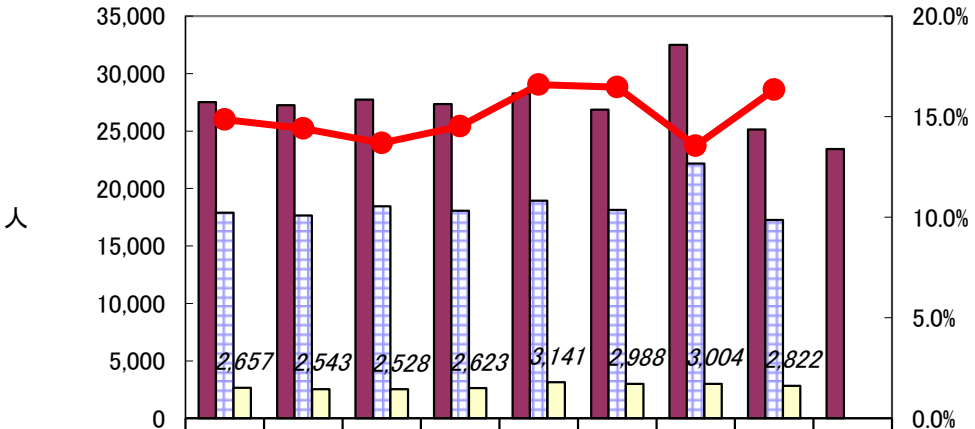
1.1 総評

今回は，情報処理安全確保支援士試験としての 2 回目の試験でした。初回の試験に引き続き，情報セキュリティ業務で柱となるセキュリティインシデント対応，Web セキュリティ，マルウェア対策などに関して漏れなく出題されていましたが，今回の試験では，午後Ⅰ試験と午後Ⅱ試験の両方で暗号技術に関する問題が出題されていたことが特徴と言えるでしょう。

午後Ⅰ試験では，比較的オーソドックスな定番のテーマについて問われていて，求められた知識も標準的でしたので，難易度は標準的です。午後Ⅱ試験では，時流を捉えた IoT システムのセキュリティ対策や HSM(Hardware Security Module)を用いたシステムの構築・運用に関する問題が出題されました。題材の新規性も強く，特定分野の技術的知識が求められたことから，難易度は高めと言えます。

午後試験の問題文で提示される状況設定は，実務的で複雑になってきており，1 問当たりのボリュームも提示される図表も多くなっています。そのため，特定の技術的知識とともに，短時間での問題文の読解力が合否を左右するといえます。

1.2 受験者数の推移



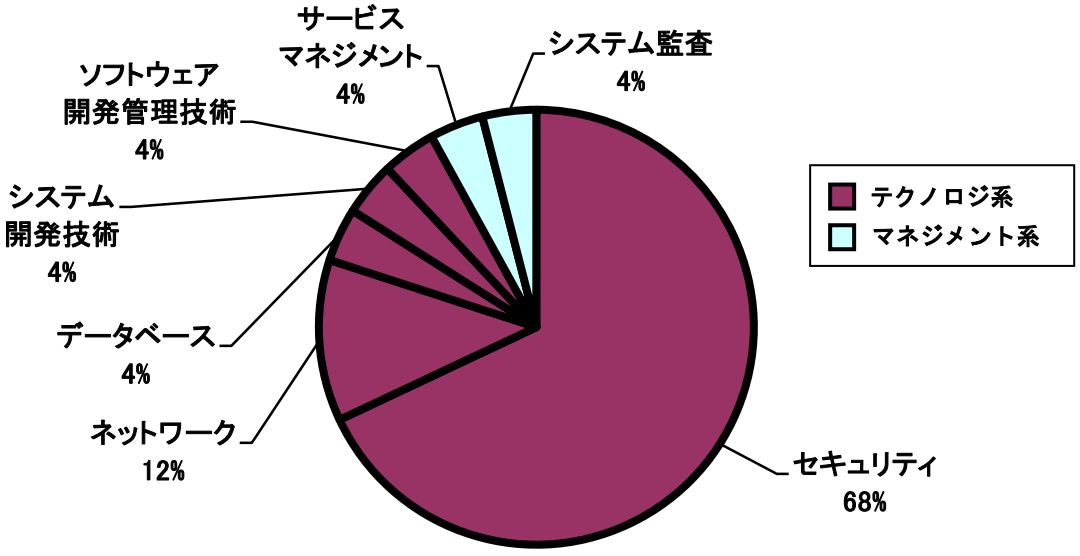
	H25 秋	H26 春	H26 秋	H27 春	H27 秋	H28 春	H28 秋	H29 春	H29 秋
応募者数	27,522	27,246	27,735	27,339	28,274	26,864	32,492	25,130	23,425
受験者数	17,892	17,644	18,460	18,052	18,930	18,143	22,171	17,266	
合格者数	2,657	2,543	2,528	2,623	3,141	2,988	3,004	2,822	
合格率	14.9%	14.4%	13.7%	14.5%	16.6%	16.5%	13.5%	16.3%	

2.　午前Ⅱ問題の分析

2.1　問題テーマの特徴

出題分野の中分類における出題数は，前回の試験で，重点分野とされるレベル 4 の出題数が「セキュリティ」18 問，「ネットワーク」2 問になりましたが，今回の試験では，従来の「セキュリティ」17 問，「ネットワーク」3 問に戻っていました。また，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」の各分野から 1 問ずつの出題構成についてはずっと変動は無く，今回の試験でも午前Ⅱ試験の出題範囲はすべてカバーされています。今後もこのレベル 4 の重点分野からの出題数が全体の 8 割を占める，重点分野に力点を置いた出題構成の傾向は踏襲されると考えてよいでしょう。

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，さらに小分類にまで分類してその内訳を見てみますと，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」の分野から 8 問，リスク分

析や ISMS などが含まれる「情報セキュリティ管理」と JCMVP や CVSS などが含まれる「セキュリティ技術評価」の分野から 3 問，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」とセキュアプロトコルやセキュアプログラミングなどが含まれる「セキュリティ実装技術」の分野からは 6 問が出題されていました。最近の午前Ⅱ試験の傾向として，3 回前の過去問題の再出題比率が高いということがあり，「セキュリティ」分野の小分類ごとの出題数も 3 回前の午前Ⅱ試験の出題傾向に影響を受けやすくなっています。

セキュリティの小分類	出題数			
	28 年春	28 年秋	29 年春	29 年秋
情報セキュリティ	9 問	8 問	8 問	8 問
情報セキュリティ管理，セキュリティ技術評価	2 問	1 問	2 問	3 問
情報セキュリティ対策，セキュリティ実装技術	6 問	8 問	8 問	6 問

「情報セキュリティ」では，前回は PKI に関する出題がありませんでしたが，今回は PKI に関する問題が 2 問出題されていました。また，「情報セキュリティ」では，新しい攻撃の名称を提示し，その知識を問う問題がよく出題されますが，今回は，新しい攻撃についての出題はなく，新しい問題テーマも出題されていませんでした。

「情報セキュリティ管理」，「セキュリティ技術評価」では，新しい問題テーマとして，JIS Q 27000:2014 から“是正処置”の定義が問われた問題が出題され，「情報セキュリティ対策」，「セキュリティ実装技術」からは，新しい問題テーマとして，DNS に対するカミンスキー攻撃への対策，デジタルフォレンジックスを行う場合のデータ保全の順序について出題されています。

また，「セキュリティ」以外の分野では，「データベース」でビッグデータの解析に利用されるニューラルネットワークの問題，「システム開発技術」の JIS X 25010 の“満足性”の品質副特性の一つ“実用性”の問題，「システム監査」のシステム監査基準に基づく過去に在籍していた部門の監査についての問題が新しい問題テーマとして出題されていました。また，今回の他分野の問題は，セキュリティとは関係のない問題が出題されていました。

2.2 難易度の特徴

今回の試験での過去の本試験からの再出題率は 7 割弱で，再出題率の高い試験でした。特に目立ったのは，3 回前の本試験からの再出題数です。「セキュリティ」分野の 17 問中，9 問が平成 28 年春の SC 試験からの再出題問題となっていました。ですので，今回の試験では，平成 28 年春の本試験問題の学習をきちんと行っていたかどうかで，試験の難易度への印象が大きく異なったと思われます。

後半の問 16 以降に新規テーマの出題が多く，他分野の出題がセキュリティと関連の無い知識を問うものが多かったことから，前半に比べると，後半の問題には時間がかかったのではないかと思われます。また，ネットワークの出題は，2 問が計算問題でしたが，これも

慣れていないと時間のかかる問題でした。

以上のことを考え合わせますと，午前Ⅱ試験全体の難易度は標準的でしたが，前回に比べるとやや高くなっていると言えるでしょう。前回の午前Ⅱ試験の突破率は，77.8%と高いものでしたが，今回の試験の突破率は，75～70%程度になると思われます。

個々の問題の難易度は，出題テーマとなっている知識項目の認知度と知識レベルの深さ，紛らわしい選択肢の有無などで判断しています。JIS Q 27000 からの“是正処置”の問題や“デジタルフォレンジックスの保全の順序”の問題は，新作であると同時に，テーマそのものが試験で問われたのがはじめてという問題ですので，難易度は高いと判断しました。

2.3　問題テーマ難易度一覧表

問	テーマ	難易度
1	CRL	A
2	OCSP	A
3	SAML	A
4	ハッシュ関数の衝突発見困難性	A
5	エクスプロイトコード	A
6	DNS に対するカミンスキー攻撃への対策	B
7	Smurf 攻撃	A
8	サイドチャネル攻撃	B
9	ステートフルインスペクション方式の FW	B
10	ディジタル証明書	A
11	JIS Q 27000:2014 の是正処置	C
12	JIS Q 27000:2014 のリスク特定	A
13	CVSS	B
14	セッション乗っ取りへの対策	B
15	OP25B	A
16	ディジタルフォレンジックスの保全の順序	C
17	WPA2-Enterprise	B
18	ルータによるコリジョンの伝搬とブロードキャストフレームの中継	B
19	トラフィック量によるクライアント数の計算	B
20	IP アドレスとサブネットマスクからのホストアドレスの算出	B
21	ニューラルネットワーク	C
22	JIS X 25010:2013　満足性の品質副特性：実用性	C
23	著作権の帰属先	C
24	フェールソフト	B
25	システム監査基準　内部監査をするメンバ	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

午後Ⅰ試験では，セキュリティ技術知識を中心に問う出題傾向が続いていますが，今回も技術面中心の出題内容になっており，セキュリティインシデントへの対応，Web アプリケーション開発におけるセキュリティ対策，SSL/TLS を用いたサーバの設定と運用に関して出題されました。

大枠のテーマ内容は，今回も脆弱性やマルウェア対策，PKI という頻出テーマでした。トピック事項としては，暗号技術で鍵交換における Perfect Forward Secrecy(以下，PFS)の性質について問われたことが挙げられます。システム構成，セキュリティインシデントのタイムライン，フォルダのアクセス権限設定，Java コード，鍵の危殆化に備えて準備しておくことが望ましい事項，調査結果といった関連図表に示された内容に基づいて，具体的な状況判断や攻撃手法に関する詳細，措置や判断理由などを問う問題構成になっています。

問 1 は，サーバ上の共有フォルダがランサムウェアによって破損されたというインシデントを題材に，ランサムウェアへの対策が問われています。Unicode 制御文字の RLO やメールヘッダの Recieve フィールド，バックアップデータからの復元の基準とする時刻や，感染していない共有サーバのファイルまでも暗号化された原因，被害拡大防止策としてのアクセス権限の見直し，シャットダウンで復号可能性が低くなる理由，管理者権限で感染した場合の被害などが問われました。技術的知識も必要ですが，アクセス権限の設定や，営業用 PC の設定やランサムウェアの特徴などは，読解力の求められる設問でした。

問 2 は，Web アプリケーション開発におけるセキュリティ対策というテーマで，Java コードから SQL インジェクション脆弱性や XSS 脆弱性の箇所を見つけ，その対策が問われるセキュアプログラミングの問題のほかに，Secure 属性，HttpOnly 属性，ホワイトリスト方式のリダイレクタ機能の仕様，検査手順の改善，XSS フィルタ機能についても問われています。セキュアプログラミングの基本的知識のほかに，目新しい知識として XSS フィルタ機能に関する知識が求められていました。最近は，このような代表的なブラウザや OS 側での対策に関する出題も見られます。

問 3 は，SSL/TLS を用いたサーバの設定と運用というテーマで，立ち上げた販売サイトで利用しているサーバ証明書の秘密鍵が公開されるという状況で，鍵の危殆化への初動対応や，鍵の危殆化に備えてあらかじめ検討して準備しておくべき事項などに関して出題されました。基本となる PKI や関連する暗号技術についての知識が求められましたが，目新しい点は，SSL3.0 の脆弱性を利用する POODLE 攻撃への措置や，PFS の性質を持つ鍵交換方式について問われた点です。

3.2 難易度の特徴

前々回の午後Ⅰ試験で，空欄穴埋め形式の知識問題が，すべて解答群が提示される選択型の問題に変わっていましたが，情報処理安全確保支援士の第 1 回の試験である前回の試

験では，その傾向は見られず，従来どおりの出題形式に戻っていました。しかし，今回の午後Ⅰ試験では，選択問題による解答数は，問1で3つ，問2で4つ，問3で7つと，従来に比べると増加しています。問2や問3では，単なる空欄穴埋めの知識問題だけでなく，セキュアコードや修正方法，リスクなどについても選択形式で出題されています。

今回の午後Ⅰ試験の問題ボリュームは，6～7 ページと，前回よりも問題文のページ数が増えていますが，これは設問文内に選択肢が提示された影響を受けていると考えられます。問題文中に提示される図表も，3～4 と前回並でした。

また，設問に解答するうえで前提となるセキュリティの技術的知識は，一部を除けば基本的な内容で，頻出テーマである脆弱性やマルウェア対策，PKI が中心に問われていました。

問1は，RLO によるファイル偽装を用いたランサムウェアへの感染というインシデントへの対応について問われています。RLO については，午前2問題でも出題されたことがありますし，設問の解答ポイントは見つけやすく，問題文をきちんと読み取ることができれば，解答が可能な問題といえます。難易度は，標準的です。

問2は，セキュアプログラミングに関する問題で，Java を用いて代表的な SQL インジェクション脆弱性や XSS 脆弱性について出題されています。今回の問題では，オーソドックスなコードから問題となる箇所を指摘すれば，対応については，選択肢からの選択になっていますし，ブラウザの XSS フィルタに関する出題以外は，Secure 属性や HttpOnly 属性などの基本的な知識が問われました。問題全体の難易度は，標準的です。

問3は，SSL/TLS サーバの運用に関する問題で，PKI や，これに関連する暗号技術について問われました。これまでも問われてきた定番ともいえる問題ですが，PFS の性質を持つ鍵交換方式が問われた点やドメイン認証証明書の選択が妥当でない理由などは，解答がまとめにくいため，3問の中では一番難易度が高い問題といえるでしょう。他の2問と比較するとやや高いということで，難易度をCとしました。

3.3　問題テーマ難易度一覧表

問	テーマ	難易度
1	ランサムウェアへの対策	B
2	Web アプリケーション開発におけるセキュリティ対策	B
3	SSL/TLS を用いたサーバの設定と運用	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試験は 1 問を 2 時間という長時間で解答する試験ですので，設定事例が午後Ⅰ問題の 2 倍以上の長さの問題文で提示されます。そのため，単にセキュリティ技術を問う設問だけでなく，管理面からの知識も加味して解答を導き出すことが求められる設問も出題されます。また，問題文に幅広い設問テーマを含めることができる容量や柔軟性がありますので，個々の設問レベルのテーマとしては，大枠のテーマに直接関係のある内容に限定されずに，幅広い分野について問われる総合問題として出題される傾向にあります。

今回の午後Ⅱ試験も基本的には総合問題でしたが，大枠のテーマそのものが比較的絞り込まれたテーマになっていました。また，2 問ともに，IoT 機器や HSM(Hardware Security Module)というセキュリティ機器に関連した問題が出題の中心であった点が，今回の午後Ⅱ試験の特徴と言えます。

基準類関連として FISC(金融情報システムセンター)の安全対策基準に関する出題が含まれていたことも目を引きます。

問 1 は，ネットワークカメラを用いたクラウド型ビデオ監視システムを題材にした IoT システムのセキュリティ対策の問題でした。IoT 機器のセキュリティについて注目されている昨今，時流に適した出題といえます。問われた内容は，ポートスキャンでの応答結果，セキュリティ検査の内容，出荷済みのカメラへの具体的な対策，カメラとのデータ通信に想定される攻撃，リバースブルートフォース攻撃や，リスト型攻撃，追加認証に用いる情報，追加認証が必要となる平常時でない状況，委託契約に盛り込むべき条項，構成管理をしない場合の問題点，動画を暗号化する場合の具体的方法などです。セキュリティ知識以外にネットワーク系の知識も求められる問題です。

問 2 は，生命保険会社の契約情報管理を題材にした，HSM 関連の暗号システム設計・運用に関する問題でした。問われた内容は，FISC，CRYPTREC，解読に必要な PC 台数の計算，鍵管理の仕組みにおけるリスク，FIPS140-2，鍵管理者が 3 名いる効果，IC カードに記録された部分鍵の使用用途，耐タンパ性，運搬時に静電気防止シートで覆う理由と機能，DB 及び表領域作成手順で HSM サーバを一つしか稼働させない理由，H クライアントの追加機能がなかった場合のエラー条件，実施した対策の元になる漏えいリスクなどです。FISC の安全対策基準や，FIPS140-2，HSM といった暗号関連の技術的知識が求められる問題です。

4.2 難易度の特徴

問題文のボリュームは，2 問共 14 ページと大変長く，午後Ⅰ試験で増加していた選択肢問題は，問 1 の小問 2 問だけで，午後Ⅱ試験は従来どおりの形式での出題となっていました。また，問題文中に示される図表の数については，これまでと同様に多く，問 1 で 8 つ，問 2 で 5 つ含まれています。図表では，問題文中の記述よりも詳細な条件設定などの内容が示されることが多いという特徴があります。2 問とも，図表で示された詳細な内容を含め

た問題事例を踏まえたうえでの具体的な解答を求める設問がほとんどを占めており，知識を応用して問題事例に合った適切な解答を導かなければなりません。

また，マネジメント系の設問では，問題文に提示された状況の読解だけで解答可能なものも見られますが，今回の午後Ⅱ問題でのマネジメント系の設問は，読解力に加えて特定の知識を必要とするものが多かったように感じられます。

問 1 で問われた，ポートが閉じている場合の応答結果は，実務経験のない受験者には難易度は高く，出荷済みのカメラのファームウェアや起動スクリプトへの対策などは IoT 機器ならではの出題といえます。また，ビデオ監視システムを構築しているクラウドへの脅威に関する出題でも，単なる知識だけで解答できる問題はほとんどなく，大半がセキュリティ知識を事例に適用して解答することが求められているために，事例内容の隅々まで把握しておくことが求められています。また，平常時と異なると判断される場合や，委託契約に盛り込むべき条項などは，解答ポイントに迷う設問で，難易度は高めといえます。

問 2 では,暗号モジュールとしての HSM の技術的内容に関する説明のボリュームが多く，DB 暗号方式における DB 初期化処理の概要図などは 1 ページを丸々使うほどの大きな図で，読解に多くの時間が必要でした。HSM そのものをここまで中心に取り扱った出題ははじめてで，これらの理解に時間を要したと思われます。また，暗号方式の検討での鍵管理者が 3 人いる効果や，DB サーバ及び HSM サーバの構成設計に関する設問は，難易度が高めです。

4.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	IoT システムのセキュリティ対策	C
2	データ暗号化の設計	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初回の試験であった前回の試験に引き続き，今回の試験においても，従来の旧情報セキュリティスペシャリスト試験の出題傾向が踏襲されていました。次回の試験においても，重点分野の「セキュリティ」から 68%，もう一つの重点分野である「ネットワーク」から 12%が出題され，2 分野の合計が出題の 8 割に達するという出題傾向は続くと思われます。午前Ⅱ試験に合格する基準は 60 点以上なので，この 2 分野で確実に得点できるかどうかが，午前Ⅱ試験の合否に直結します。セキュリティやネットワークに関する学習は，体系的に行ったほうが，知識の関連性も把握しやすいため，テキストに沿って順に学習を進めるとよいでしょう。

一方，問題演習を行う際は，出題頻度の高さを意識し，効率的に演習を行うようにしましょう。具体的には，「セキュリティ」分野を小分類に細分化して見てみると，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」の出題比率が最も高く，次いで，アクセス制御やマルウェア対策，不正アクセス対策，無線 LAN セキュリティなどが含まれる「情報セキュリティ対策」，セキュアプロトコルや認証プロトコルなどが含まれる「情報セキュリティ実装技術」の出題比率が高いので，これらを念頭に置いて問題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などを洗い出し，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。

今回の試験では，平成 28 年春の情報セキュリティスペシャリスト試験から 9 問が再出題されました。過去問題の再出題では，3 回前の情報セキュリティスペシャリスト試験からの再出題が多いという傾向が続いています。次回の午前Ⅱ試験の 3 回前の試験は，平成 28 年秋の試験となります。また，午前Ⅱ試験全体の再出題問題の 9 割弱が情報セキュリティスペシャリスト試験からの再出題問題で，その大半の出題年度は平成 26 年以降です。本試験直前の午前Ⅱ試験の対策では，まずは平成 28 年秋の問題を解き，そして余裕があれば，平成 26 年以降の午前Ⅱ試験についても確認しておくとよいでしょう。

また，今回の試験では出題されませんでしたが，新しい攻撃について出題されることも多いので，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と思われます。

5.2 午後Ⅰ対策

午後の出題範囲は，旧情報セキュリティスペシャリスト試験と同じで，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

これらのうち，出題頻度が高かいのは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」です。「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」として挙げられている内容の中では，アプリケーション(Webアプリケーションを含む)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。「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。この出題傾向は，次回も大きな変化は無いと思われますので，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。

また，ネットワークに関する知識としては，まず，ネットワーク構成図や機器の設定から，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，基礎的な内容をきちんと把握できているかが重要です。アプリケーション層レベルでは，HTTP リクエストヘッダの内容，DNS の仕組み，メールシステムの仕組みなどの知識は，問題文を読み取るうえで必須です。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。また，UNIX系OSでの基本的なコマンドなどについても学習しておくとよいでしょう。

セキュアプログラミングに関する問題は，今回も1問が出題されました。次回も，セキュアプログラミングの問題が出題される可能性は高いと思われます。プログラミング経験のない受験者は，セキュアプログラミングの問題を選択しない場合が多いため，残りの2問を得意不得意に関わらず選択することになってしまいます。できるだけ，苦手な分野をなくすことを心がけた対策をしっかりと行うようにして下さい。また，セキュアプログラミングの問題を選択しようと考えている場合には，IPAのサイトで公開されている“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”といった資料から出題されることも多いので，教材として活用することをお勧めします。

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，その後に問題演習を行うことが非常に重要です。知識は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。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試験では情報セキュリティの技術面と管理面の両方の知識が必要となる総合問題がしばしば出題されてきました。前回の情報処理安全確保支援士の試験では，セキュリティ管理の知識は問われませんでしたが，2回目の試験となる今回の試験では，旧情報セキュリティスペシャリスト試験と同様に，セキュリティ管理の知識も求められる総合問題が出題されていました。次回の試験においても，セキュリティ管理の知識が求められることを想定した対策をとることが大切です。

したがって，技術面の専門知識を午後Ⅰ試験と同様の対策で学習すると同時に，それに加えて，セキュリティ技術を適用する際のバックグラウンドとなるセキュリティ管理面の知識を強化する必要があります。特に，情報セキュリティポリシ，責務分離や相互牽制，外部委託管理，コンプライアンスや内部統制など，組織的・人的なセキュリティ対策を中心に，情報セキュリティマネジメントを実践する現場で遭遇するさまざまな問題にどのように対応していくかという観点から学習しておくことが重要です。

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。問題のページ数は，設問まであわせると12～14ページにわたります。しかも図表の数も10前後と多く，問題をひととおり読むだけでも相当な時間と集中力が必要です。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，何ページも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。