情報セキュリティスペシャリスト

1.　はじめに

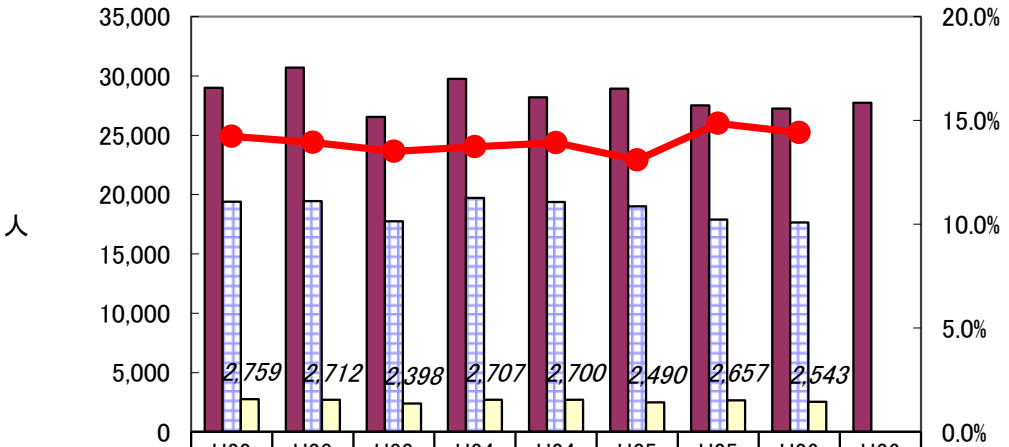
1.1　総評

今回の試験では，特定のセキュリティ技術の専門知識やその適用能力が問われる問題が目立ちました。特に，認証や暗号関連の技術知識が求められました。また，午後Ⅰ問題や午後Ⅱ問題の問題文で提示される状況設定が，全般的に実務的で複雑になっており，1問当たりのボリュームと提示される図表がともに増加しています。そのため，特定の技術的知識に加えて，問題文の読解力の有無が合否を左右するといっても過言ではありません。

今回の午後問題では，旧来はセキュアプログラミングの視点だけから扱われてきたバッファオーバフローの問題が，最近頻出されるようになったスマートフォンセキュリティの問題テーマとして扱われた点や，2010 年くらいから出題が少なくなっていた暗号アルゴリズムの等価安全性に関して出題された点，ID 管理や認証の統合などに関するアイデンティティマネジメント(IDM)関連の実務的な内容が出題された点などが特徴として挙げられます。また，個々の設問の大半が技術的な内容を問う問題で占められており，管理的な内容を問うものが少ないことも特徴です。

午前Ⅱ試験はセキュリティ分野での出題傾向がやや変化したため，難易度は前回に比べると高めです。午後Ⅰおよび午後Ⅱ試験でも，特定分野のテーマに絞り込んだ問題が多く出されていましたので，試験全体の難易度は高めと言えるでしょう。

1.2　受験者数の推移



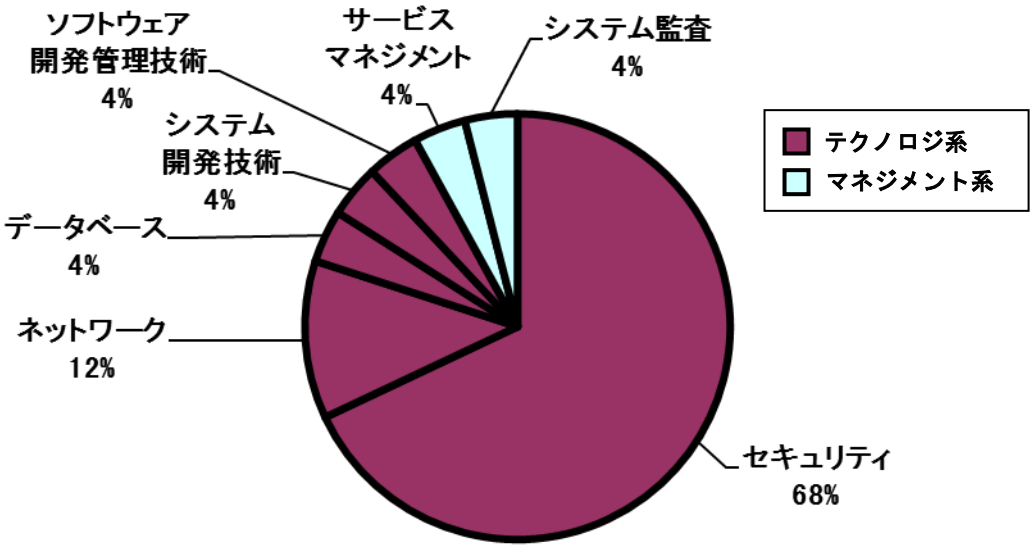
	H22 秋	H23 特別	H23 秋	H24 春	H24 秋	H25 春	H25 秋	H26 春	H26 秋
応募者数	28,989	30,704	26,539	29,756	28,188	28,930	27,522	27,246	27,735
受験者数	19,391	19,445	17,753	19,711	19,381	19,013	17,892	17,644	
合格者数	2,759	2,712	2,398	2,707	2,700	2,490	2,657	2,543	
合格率	14.2%	13.9%	13.5%	13.7%	13.9%	13.1%	14.9%	14.4%	

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比率は前回の春試験とまったく同様で，重点分野とされるレベル 4 の「セキュリティ」から 17 問，「ネットワーク」から 3 問が出題されたほか，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 問ずつが出題され，午前Ⅱ試験の出題範囲がすべてカバーされています。午前Ⅱ試験における「セキュリティ」強化が発表されて以降，2 回ともこの出題比率で出題されていますので，次回以降もレベル 4 の重点分野からの出題数が全体の 8 割を占める，重点分野に偏った出題構成の傾向は踏襲されると思われます。

出題分野	出題率	出題数
データベース	4%	1 問
ネットワーク	12%	3 問
セキュリティ	68%	17 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



しかし，17 問が出題された「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，直近 2 回の試験とは大きく傾向が異なっていました。次表は直近2回と今回のセキュリティ分野の17問について小分類レベルの出題数を示したものです。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」は直近の2回では約半分の8問が出題されていましたが，今回は5問にとどまりました。また，「情報セキュリティ管理」と「セキュリティ技術評価」の 2 分野については，直近の 2 回では 2 分野合わせて 1 問しか出題されていなかったのに，今回は 5 問と大幅に増えています。クラウドサービス利用のための情報セキュリティマネジメントガイドライン，FIPS 140-2，CSIRT，CVSS，CRYPTREC と，いずれも過去に出題された問題ではありますが，「情報セキュリティ」や「情報セキュリティ対策」に的を絞って学習していた受験者には厳しかったと思われます。

セキュリティの小分類	出題数		
	25 年秋	26 年春	26 年秋
情報セキュリティ	8 問	8 問	5 問
情報セキュリティ管理，セキュリティ技術評価	1 問	1 問	5 問
情報セキュリティ対策，セキュリティ実装評価	8 問	8 問	7 問

特に目新しい問題テーマとしては，「ネットワーク」分野の「RFC 5322 に準拠した電子メールのメッセージフォーマット」に関する問題と「ソフトウェア開発管理技術」分野の「コンテンツの不正複製防止方式の一つである DTCP-IP」に関する問題が挙げられます。

また，最近クラウドに関するセキュリティの新規問題が出題されるという傾向がありましたが，今回は，クラウドに関する問題は「情報セキュリティ管理」の分野から出題されてはいましたが，新作ではなく過去問題が再出題されていました。

2.2　難易度の特徴

「セキュリティ」分野の 17 問中，新作問題は 4 問のみで，12 問が平成 21 年度以降の情報セキュリティスペシャリスト(SC)試験から再出題された問題，1 問が応用情報技術者試験からの再出題問題となっていました。「セキュリティ」分野の過去問題の再出題率は 76%に上り，過去問題を学習したかどうかで得点が大きく左右されるでしょう。なかでも，平成 25 年春と平成 24 年秋の SC 試験からの再出題問題は，それぞれ 6 問，5 問となっていて，この 2 回についての学習をしていたかどうかが，難易度の感じ方にも，さらには合否にも大きく影響すると思われます。

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，紛らわしい選択肢はないかなどで判断しました。「ハッシュ関数の衝突発見困難性」は新作の問題で，まだ問われたことのなかったテーマでした。「電子メールのヘッダと本体の区別法」，「DTCP-IP」についても同様です。こちらの 2 問はセキュリティ以外の分野ということもあって，特に難しく感じたのではないでしょうか。

また，午後試験に対する対策として，攻撃手法とその対策や暗号化・認証技術セキュリティなどについては深く学習していますので，午前Ⅱ試験で「情報セキュリティ」や「情報セキュリティ対策」が中心に出題された場合の午前Ⅱ試験の突破率は高くなるという傾向が見られます。実際，「情報セキュリティ」や「情報セキュリティ対策」が多く出題された前回と前々回の試験では，午前Ⅱ試験の突破率は軽く 7 割を超えていました。しかし逆に，それらの分野からの出題が減ると，突破率は下がってしまいます。前表にも示しましたように，「情報セキュリティ」の出題が減っていますので，今回の午前Ⅱ試験の突破率は，65%前後になるのではないかと思われます。

以上のことから，午前Ⅱ試験の難易度は，前回に比べて少し高くなったといってよいでしょう。

2.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	PKI を構成する OCSP	A
2	ハッシュ関数の衝突発見困難性	C
3	クラウドサービス利用のための情報セキュリティマネジメントガイドライン	B
4	ディジタル証明書	B
5	FIPS 140-2	B
6	CSIRT	C
7	CVSS	C
8	CRYPTREC の活動内容	C
9	キャッシュポインズニング攻撃への対策	B
10	SAML	B
11	SSH	B
12	Smurf 攻撃の特徴	A
13	サイドチャネル攻撃	B
14	デジタルフォレンジックス	A
15	DKIM	B
16	EAP-TLS	C
17	サンドボックス	C
18	DNSSEC	B
19	RADIUS	B
20	電子メール　ヘッダと本体の区別法	C
21	デッドロックが発生している待ちグラフ	B
22	スタブとドライバ	B
23	DTCP-IP	C
24	JISQ20000-1 でのインシデント	B
25	情報セキュリティ管理基準に基づいた監査	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

前回の午後Ⅰ試験と同様に今回も，午後Ⅰ問題 3 問の中の 1 問でセキュアプログラミングの問題が出題されていましたが，今回は，スマートフォン(スマホ)のセキュリティに関する問題として，バッファオーバフロー攻撃について問われていました。また，残りの 2 問も，SSL クライアント認証や暗号関連の知識，通信のフィルタリング制御といった特定領域についての技術知識が求められる問題で，最近出題機会が少なくなっていた暗号アルゴリズムの等価安全性についても出題されていました。今回の試験の特徴は，セキュリティ全般の知識ではなく，問題ごとに特定のセキュリティ技術知識が求められたことといえるでしょう。

問 1 は「スマートフォン」というテーマで，個人所有のスマホから社内システムへのアクセスを許可した企業が，そのセキュリティ対策と利用規定を確認するという状況で，各種のバッファオーバフロー攻撃やスマホ関連のセキュリティに関する問題が出題されました。前回の試験でも C++のバッファオーバフローに関する出題がありましたので，2 回連続でバッファオーバフローに関して出題されたことになります。前回は整数オーバフローによるバッファオーバフローについての出題でしたが，今回は各種バッファオーバフロー攻撃とその対策についての詳細で具体的な知識や，スマホ OS に関連する知識が求められていました。

問 2 は代理店販売支援システムのセキュリティ強化を題材に，セキュリティ設計について問われています。具体的には，暗号アルゴリズムの等価安全性に関する問題や，SSL クライアント認証に用いるディジタル証明書の発行・更新・利用停止などの各種手順案について問われました。ハッシュ関数や等価安全性，PKI に関する基本的な知識が必要ですが，証明書管理における各種手順に関する設問の多くは，解答の根拠が問題文の中に埋め込まれていました。今回の 3 問中では，セキュリティ管理的な視点からの設問が比較的含まれている問題でした。

問 3 は「マルウェア感染への対応」というテーマで，標的型メール攻撃によるマルウェア感染を契機にマルウェア対策を見直すという状況で，メールのフィルタリングルールや，バックドア通信の遮断のためのプロキシサーバのアクセス制御ルール，サーバへのマルウェアの不正アクセス軽減のための L3SW のフィルタリングルールと，パスワードに関連してハッシュ値の計算コストやソルトについて問われました。設問の大半がフィルタリングルール関連の問題で，ここまで集中的にフィルタリング制御について問われた問題ははじめてでした。

3.2 難易度の特徴

今回の午後Ⅰ試験でも，問題文の長大化，詳細な図表数の増加，実務レベルに近い複雑な条件設定といった最近の傾向どおりの問題が出題されていました。問題文は 5～6 ページ

にわたるうえに，1 問当たり 3～7 もの図表が提示されていて，それらの図表の内容を的確に読み取ることが求められています。設問の大半は，問題文中に示されたプログラムコードやメモリ配置，証明書の新規発行手順案と補足情報，暗号アルゴリズムの安全性，FW や L3SW のフィルタリングルールといった関連図表に示された条件などに基づいて，具体的なセキュリティ技術やセキュリティ対策を詳しく問うものです。

また，問題テーマの特徴でも述べましたように，今回の試験は，特定の技術に関して特化して問われる問題となっています。ですので，出題領域に関する知識を有する受験者にとっては有利ですが，そうでなければかなり厳しい試験になったと思われます。

問 1 のスマホに関するバッファオーバフロー攻撃とその対策についての問題は，スタックバッファオーバフロー攻撃の防止策やインジェクションベクタによる攻撃の抑止策，インターネットからの Web サーバへのバッファオーバフロー攻撃への対策，スマホ OS についての知識などが具体的に問われていて，3 問の中で一番難易度の高い問題といえるでしょう。

問 2 では，久しぶりに暗号アルゴリズムの等価評価について出題されていましたが，基本的知識があれば回答可能な問題でした。手順案や補足情報についての穴埋め問題も素直な問題が多く，高い専門知識が必要な問題もありませんでしたので，取り組みやすい問題といえるでしょう。セキュリティ設計の不備に関する修正案についての設問は問題文中に解答の根拠となる情報が提示されているものが大半です。ただし，問題文や図表が多く，特に図 1 と図 2 の読み取りに時間がかかる問題でした。内容的な難易度はやや易しめといえますが，時間的な難易度が高いので，総合的に普通と判定します。

問 3 は，フィルタリング設計について重点的に問われた問題でしたが，提示されたフィルタリングルールについて，正しく読み取ることができれば対応可能な問題で，高い専門知識は要求されてはいません。最後の設問で，パスワードの総当り攻撃のための，ハッシュ値を計算すべき最大数を求めるシグマ関数を用いた計算式についての穴埋め問題が出されています。時間的な余裕があれば，それほど難しい問題ではありませんが，いきなり数式を提示されて焦ってしまった受験者も多かっただろうと思います。この問題も基本的な知識で対応可能な問題でしたが，求められた知識が特定領域に集中していたことや，問題文の分量・図表が一番多く，時間的な意味での難易度が高めといえることを勘案して，総合的な難易度は普通と判定します。

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	C
2	代理店販売支援システム	B
3	マルウェア感染への対応	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 1 問を 2 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，通常は，単にセキュリティ技術を問う設問テーマだけでなく，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テーマも出題されます。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るため，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らず，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。今回の問題も基本的には総合問題といえますが，初めから大枠のテーマ自体が絞り込まれているために，これまでの午後Ⅱ試験に比べると設問テーマの幅が狭く特定領域に特化している問題と言えるでしょう。また，設問の大半が技術的な内容を問うものでした。

問 1 はグローバルな観点からの複数の ID 管理システムやシングルサインオン(SSO)システムの統合設計に関する問題で，様々な観点から ID 管理と認証システムについて問われる問題です。問題文に示された日本，欧米，アジアの各地域における認証システムについて，利用者認証の通信シーケンス図と説明文に基づいて理解した上で，統合設計で採用した認証方式の理由，必要な調整，不備などに応えることが求められています。Kerberos 認証やエージェント型とリバースプロキシ型の SSO の仕組みについての知識が必要です。

問 2 は SQL インジェクション，DOM ベースのクロスサイトスクリプティング(XSS)，クリックジャッキングなどの攻撃手法に対する対策や最近 RFC 化された HSTS プロトコルなどを含めた Web アプリケーションセキュリティの問題でした。具体的には，アクセスログの読み取り，Web サイトの診断ガイドライン，反射型の XSS と DOM ベース XSS の診断方法や，診断方法が異なる理由，クリックジャッキング対策の HTTP 応答ヘッダの指定，HSTS を有効にする HTTPS の応答ヘッダに関する問題，などについて問われました。

4.2 難易度の特徴

今回の午後Ⅱ試験は，問 1 が ID 管理と認証システムに，問 2 が Web アプリケーションセキュリティに特化していますので，受験者の有している知識領域によって難易度の感じ方に差が出るといえます。また，問題文の分量が問 1 は 13 ページと特に長く，文章や図表の形で提示される多くの情報の中から必要な情報を漏れなく見つけ出し，専門知識を適用して解答を導き出すための読解力は，午後Ⅰ試験よりもさらに必要とされています。

今回の午後Ⅱ試験は，知識領域が特定の分野に集中していることに併せて，問題分量の点でも前回の試験より多くなっています。したがって，前回の午後Ⅱ試験と比較した場合の難易度は，問 1 はかなり高く，問 2 は若干高めといえるでしょう。

実は，情報セキュリティスペシャリスト試験では，H23 年の秋以降，午後Ⅰ試験の突破率よりも午後Ⅱ試験の突破率のほうが 6～15%ほど高くなっています。午後Ⅰ試験の突破率が 42～52%で推移しているのに対して，午後Ⅱ試験の突破率は 52～59%もあるからです。し

かし，今回の試験では，午後Ⅰ問題と午後Ⅱ問題の突破率は同じくらい，あるいは午後Ⅱ試験の突破率のほうが低くなってしまうかもしれません。

問１は，問題文が 13 ページと長いうえに，図表も 9 つと多く，また，問題文中に“(以下，○○という)”という置き換えが頻出しているために，問題文がとても読みづらく，読解に時間を要するタイプの問題でした。また，問題文の構成が解答の根拠を導出しにくいタイプのもので，全体像を理解するのに何度も読み返す必要がありました。SSO の認証システムについての知識も必須で，過去数回の午後Ⅱ試験の中でもかなり難易度の高い問題になると思います。

問２は，Web サイトのセキュリティについての専門的な技術的知見が必要な問題です。問題文は 11 ページで図表も 8 つとボリュームがありますが，午後Ⅱ試験としては通常のレベルです。攻撃手法とその対策を要求するタイプの問題ですので，問 1 に比べると問題文の読解にはそれほど多くの時間をとられることはなかったと思われます。アクセスログから脆弱性のある URI を見つける問題や HSTS を有効とする HTTPS 応答ヘッダの指定など，問われている知識は簡単なものではありません。ですが，問 1 との比較において明らかに難易度に差があるため，こちらの問題の難易度は標準と判定します。

4.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	利用者 ID 管理システム及び認証システムの設計	C
2	Web サイトのセキュリティ	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

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 割に達しています。午前Ⅱ試験に合格する基準は，60 点以上ですので，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」分野について，午前の出題範囲の小分類に細分化して見てみますと，今回，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」が直近 2 回の 8 問から 5 問に減っていました。しかし，攻撃手法や暗号化・認証技術は情報セキュリティ試験の要ともいうべき分野です。次回以降，増えることはあってもこれ以上減ることはないと考えられます。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」については，前 2 回と同じくらい出題されています。今回，出題傾向に変化が見られましたが，これらの二つの小分類について重点的に学習する必要があることには変わりありません。今回の試験で出題が増えたのが「セキュリティ技術評価」の分野です。全問が過去問題の再出題でしたので，過去の本試験問題を学習する際に，この分野についてもきちんと押さえるようにする必要があると思われます。

「セキュリティ」分野の問題 17 問中の 76%が過去問題の再出題でした。H21 年度の問題が 1 問ありましたが，それ以外は全て H24 年春以降の問題からの再出題でした。ですから，「セキュリティ」と「ネットワーク」に関する基礎知識をすでに持っている場合は，H24 年以降の過去問題の演習を中心に学習するのが効率的です。過去問題の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ようにしましょう。

また，普段から IT 関連のニュースに注目し，新しい技術動向についての知識を習得する習慣をつけておきましょう。例えば，スマートフォンやクラウドコンピューティングにまつわるセキュリティや，IPv6 環境のセキュリティに関連する事項などについて，押さえておくとよいと思われます。

今回の試験では， H25 年春と H24 年秋の情報セキュリティスペシャリスト試験からそれぞれ 6 問と 5 問が出題されていました。3 回前や 4 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比較的多い傾向がみられますので，次回も必ずそうとは限りませんが，試験直前の見直しや確認など，短時間で過去問題の演習をする場合には，それらの回を中心に行うとよいでしょう。

5.2 午後Ⅰ対策

出題数が 3 問に減って 3 回目の試験になりました。4 問中 2 問選択だった時は，セキュリティ技術寄りが 2 問，セキュリティ管理寄りが 2 問のように出題されることが多く，セキュリティ技術が得意な受験者もセキュリティ管理が得意な受験者も問題選択に困ることはあまりなかったと思います。しかし，出題数が 3 問に減って以降，セキュリティ管理寄り

の問題は出題されていません。毎回，セキュアプログラミングの問題が 1 問出題されていますので，セキュアプログラミングの問題を選択しないと決めているような受験者は，残りの 2 問を選択するしかありません。したがって，セキュリティ技術を中心に，幅広く満遍なく学習をすることが以前にも増して重要となっています。

午後Ⅰ試験の出題分野として扱われる頻度が高いものとして，試験要綱における出題範囲の「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」の分野では，ネットワークセキュリティ対策やサーバ・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，セキュアプログラミング，同じく「情報セキュリティの運用に関すること」の分野では，脆弱性分析，インシデント対応，不正アクセス対策，同じく「情報セキュリティ技術に関すること」の分野では，アクセス管理技術，マルウェア対策技術，暗号技術，認証技術，PKI などが挙げられ，これらの学習が午後Ⅰ対策の基本となります。

ネットワークセキュリティやシステムセキュリティについては，話題となっている攻撃手法やその対応方法を把握し，関連事項を含む問題演習などを通じてその理解度を高めておく必要があります。特に，脅威・脆弱性・攻撃手法・対策とそれらに関連するセキュリティ技術は，どのような分野の問題への対処においても役立つことが多いので，バラバラに覚えるのではなく，一連の知識として習得しておくことをお奨めします。

また，スマートフォンやクラウドサービスなどの新しいシステム利用形態におけるセキュリティが出題されはじめていますので，対策の一つに加えて基礎知識を習得しておく必要があります。

セキュアプログラミングについては，試験で使用するプログラム言語については，C++，Java，ECMAScript のいずれかであることが公表されています。まず，SQL インジェクションやクロスサイトスクリプティングといった Web アプリケーションにおける代表的な脆弱性やその対策を理解したうえで，Java などによるセキュアプログラミング上の留意点などを把握しておく必要があります。なお，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新たに追加された項目は出題される可能性が比較的高いので，時折チェックしておくとよいでしょう。

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，それだけでは不十分です。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往々にしてあります。その最大の要因は読解力不足であると考えられます。繰り返し問題演習を行い，正解表現と自分の解答表現の違いを比較し，解説を読んで見直すことで，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出題されることがしばしばあります。したがって，技術面の専門知識については，午後

Ⅰ試験と同様の対策が必要ですが，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しておく必要があります。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。具体的な学習方法としては，情報セキュリティ分野の過去の午後Ⅱ問題のうち，管理面を中心とする問題テーマの演習を数多く解いておくことが有効といえるでしょう。

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。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るので，重要と考えられる記述には線を引いたり，しるしをつけるなど，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。

〔MEMO〕