# 情報処理安全確保支援士

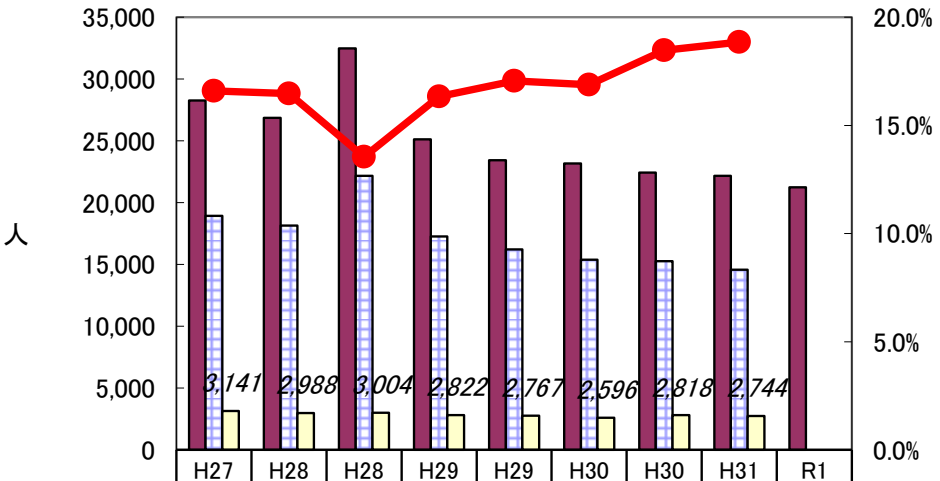
## 1.　はじめに

### 1.1　総評

今回は，情報セキュリティ実務で柱となるマルウェア対策，セキュリティインシデント対応や脆弱性対策，ネットワークセキュリティ対策などに関する出題のほか，特に，標的型攻撃に関しては，午後Ⅰ試験と午後Ⅱ試験の両方で出題されるなど目立っていました。また，ランサムウェア，マイニングマルウェア，標的型攻撃・APT 攻撃用マルウェアといったマルウェアへの対応に関しての出題も例年以上に多く感じます。さらに，最近では必ず出題されていた具体的なコードを提示してのセキュアプログラミングの出題がまったくなかった点も大きな特徴といえるでしょう。

情報処理安全確保支援士(SC)試験は，試験が開始された当初の難易度は高かったのですが，回を重ねるに連れて徐々に難易度が下がり，直近 2 回の合格率は以前の情報セキュリティスペシャリスト試験よりも高いものになっています。今回の試験も直近 2 回と同程度の合格率になると思われます。午後Ⅰ・午後Ⅱ試験で高度かつ詳細なレベルのセキュリティ技術知識があまり要求されておらず，頻出テーマが取り上げられたことが，理由として挙げられますが，インシデント対応の事例が増えて，より実務的な知識が問われる試験になっていますので，実務経験のない受験者は，ネットワークの知識やログの読み取りなどの対策をきちんとしておくことが必須の試験になっています。

### 1.2　受験者数の推移




| | H27 秋 | H28 春 | H28 秋 | H29 春 | H29 秋 | H30 春 | H30 秋 | H31 春 | R1 秋 |
|---|---|---|---|---|---|---|---|---|---|
| 応募者数 | 28,274 | 26,864 | 32,492 | 25,130 | 23,425 | 23,180 | 22,447 | 22,175 | 21,237 |
| 受験者数 | 18,930 | 18,143 | 22,171 | 17,266 | 16,218 | 15,379 | 15,257 | 14,556 | |
| 合格者数 | 3,141 | 2,988 | 3,004 | 2,822 | 2,767 | 2,596 | 2,818 | 2,744 | |
| 合格率 | 16.6% | 16.5% | 13.5% | 16.3% | 17.1% | 16.9% | 18.5% | 18.9% | |

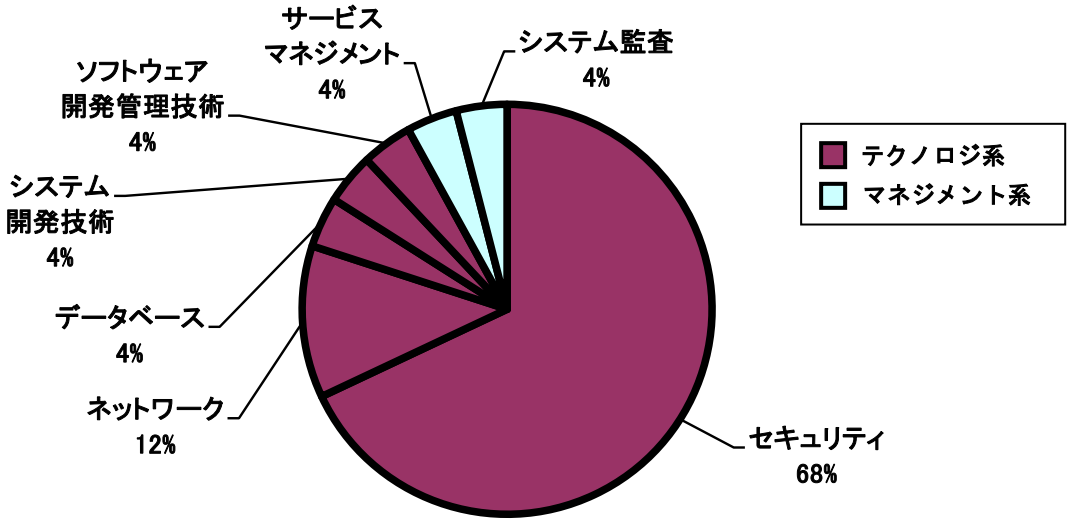
## 2. 午前Ⅱ問題の分析

### 2.1 問題テーマの特徴

今回の試験では,「セキュリティ」分野における再出題率は 17 問中 10 問と例年並みでした。また，最新のセキュリティトピックをテーマとした新規テーマの問題も出題されています。新規テーマとしては,FIDO アライアンスが規格化したパスワードレス認証の FIDO UAF, Bluetooth 機器の脆弱性を示す BlueBorne，脆弱性攻撃ツールである Exploit Kit などが挙げられます。重点分野以外の「データベース」分野では，NoSQL 系データベースの代表格であるドキュメント型データベースについて出題されました。データベーススペシャリスト試験でもほとんど出題されていない NoSQL について出題されたことは驚きです。

分野ごとの出題数には変化はみられず，重点分野でレベル 4 の「セキュリティ」が 17 問,「ネットワーク」が 3 問出題されました。

| 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ると，前回 11 問も出題されていた「情報セキュリティ」からの出題は，やや減って 9 問になっています。このうち脆弱性関連の 2 問は新規の問題テーマでした。また，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」と，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」からは昨年同様 6 問が出題されています。新規テーマとしては，常時 SSL/TLS のセキュリティ上の効果について問われていました。「情報セキュリティ管理」と「セキュリティ技術評価」からは 2 問が出題されていて，JIS Q 2701(情報セキュリティガバナンス)から“モニタ”について問われた新規テーマの問題と定番の CVSS についての問題が出題されていました。

| セキュリティ分野の小分類 | 出題数 | | | |
|---|---|---|---|---|
| | 元年秋 | 31 年春 | 30 年秋 | 30 年春 |
| 情報セキュリティ | 9 問 | 11 問 | 6 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 | 0 問 | 3 問 | 2 問 |
| 情報セキュリティ対策，セキュリティ実装技術 | 6 問 | 6 問 | 8 問 | 7 問 |

「ネットワーク」分野からの 3 問では，1 問が新規テーマの問題で，“IP パケットの再構築処理”について問われました。

## 2.2　難易度の特徴

今回の午前Ⅱ試験の難易度と過去問題の再出題率は，例年どおりの標準的なレベルといえるでしょう。要求される知識レベルが特別に高い問題や，計算問題のような解答に多くの時間を要する問題は出題されていませんでした。

再出題問題については，具体的には，「セキュリティ」分野 17 問中の 10 問が平成 30 年春～平成 27 年春の SC 試験からの再出題問題で，試験全体では，25 問中の 14 問が，平成 30 年春～平成 26 年秋の SC 区分の試験からの再出題問題でした。過去問題の学習度合いが難易度にも大きく影響することはいうまでもありません。また，FIDO や BlueBorne，Exploit Kit などの新規テーマの問題は用語知識の有無が問われる問題でした。

「ネットワーク」分野の“IP パケットの再構築処理”の問題は新規テーマの問題ということもあり，SC 試験での出題としてはやや難しかったと思います。

試験問題全体での他区分も含めた過去問題の再出題率は約 7 割で例年どおりですが，今回はシステム監査試験やシステムアーキテクト試験，サービスマネージャ試験といった論文系区分から再出題問題が選ばれていましたので，受験者にとっては他区分からの問題は，ほぼ新規問題に感じられたと思われます。

また，「3 回前の試験から数多く再出題される」という傾向は続いており，3 回前の平成 30 年度春の SC 試験から 6 問が出題されていました。

## 2.3 問題テーマ難易度一覧表

| 問 | テーマ | 難易度 |
|---|---|---|
| 1 | FIDO UAF1.1 | C |
| 2 | サイドチャネル攻撃 | B |
| 3 | VA の役割 | A |
| 4 | XML ディジタル署名の特徴 | A |
| 5 | ダイナミックパケットフィルタリングの特徴 | A |
| 6 | X.509 における CRL の記述 | A |
| 7 | JIS Q 27014:2015 における“モニタ” | C |
| 8 | CRYPTREC 暗号リスト | B |
| 9 | CVSS | A |
| 10 | BlueBorne | C |
| 11 | Cookie の Secure 属性 | A |
| 12 | DKIM | A |
| 13 | マルチベクトル型 DDoS 攻撃 | B |
| 14 | 常時 SSL/TLS のセキュリティ上の効果 | B |
| 15 | Exploit Kit | C |
| 16 | EAP-TLS が行う認証 | B |
| 17 | SQL インジェクション対策(実装と実装以外) | A |
| 18 | DNSSEC | B |
| 19 | IPv4 ネットワークにおける IP パケットの再構築処理 | C |
| 20 | TCP で確認応答がない場合の処理 | B |
| 21 | ドキュメント型データベース | C |
| 22 | 状態遷移図の完成 | B |
| 23 | マッシュアップ | B |
| 24 | フェールソフト | B |
| 25 | 本番移行が失敗するリスクに対するコントロールの監査 | 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 全体の出題傾向及び難易度について

今回の午後Ⅰ試験では，このところ続いていたセキュアプログラミングの問題が出題されなかったという変化がみられました。また，久しぶりに，電子メールのセキュリティ対策を主題とした問題も出題されました。

問題テーマとしては，電子メールを悪用した攻撃への対策としての送信ドメイン認証技術，標的型攻撃に準じるマルウェア対応を含めたセキュリティインシデント対応とサイバーセキュリティ情報共有に関する問題，マルウェアを利用した標的型攻撃への対応が問われています。大枠のテーマ内容としては，電子メールのセキュリティ対策，インシデント対応，脆弱性やマルウェア対策などの頻出テーマが扱われていますが，具体的な技術的知識と対応が多く問われています。

情報システムやネットワークの構成，SPF や DKIM に関連する図表，フィルタリングルール，機器の詳細，調査結果，対応手順や対応記録といった関連図表に示された条件などに基づいて，具体的な状況判断や技術的対応力などを問う構成の問題で占められています。解答するうえで前提となる技術的知識はかなり特定の専門事項を要求する設問も見受けられますが，今回はセキュアプログラミング問題が出題されていませんでしたので，セキュアプログラミング問題を対象外にしている受験者も 3 問の中から自分の得意な問題を選択することが可能でした。問題による難易度の差はあまりなく，午後Ⅰ試験全体の難易度は標準的といえるでしょう。

## 3.2 各問題のテーマ，特徴

問 1 は，「電子メールのセキュリティ対策」というテーマで，SPF や DKIM，DMARC などの送信ドメイン認証技術の導入に関する問題です。午後問題で電子メールに関するセキュリティ対策が主題として出題されたのは，平成 26 年春の午後Ⅰ問題で「インターネット接続システムにおける迷惑メール対策」が出題されて以来のことです。今回は，SMTP の MAIL FROM コマンドや SPF の対応状況から想定した攻撃への効果の有無，DNS サーバに設定する TXT レコードや MX レコード，DMARC のタグ設定などについて問われています。これまでも，SPF や DKIM に関しては何度も出題されてきていますが，DMARC のタグ設定について問われたのは初めてです。

問 2 は，「セキュリティインシデント対応におけるサイバーセキュリティ情報の活用」というテーマで，標的型攻撃に準じたマルウェア対応を含めたセキュリティインシデント対応と，サイバーセキュリティ情報共有に関する問題です。

ISAC から提供された自社への攻撃計画に関する情報による調査と，その調査結果に基づいたマルウェアへの対策という事例になっています。マルウェアが行う情報持ち出しの C&C 通信が HTTP と DNS プロトコルを利用するという設定ですので，ネットワーク構成と FW のフィルタリングルールから HTTP 通信と DNS クエリがどのような経路を流れ，どこのログに

記録されるかをきちんと把握する必要があります。社内調査の結果について，ISAC に提供すべき情報を選ぶ問題は新しい視点の問題でした。また，C&C 通信の手法ごとの対策の中で，DNS トンネリングによる C&C 通信が問われたのは初めてで，難易度の高い問題といえるでしょう。この問題では，解答が発散しそうな設問には解答群が用意されるという配慮がされていました。

問 3 は，「標的型攻撃への対応」というテーマで，標的型攻撃への対策実施後に発生したセキュリティインシデントへの対応と対応手順改善という事例で，事後調査に関する基本的なインシデント対応の問題です。不審 PC の電源を切らない理由や LAN から切り離さない場合に想定されるマルウェアの活動などは，これまでにも何度か問われてきました。ipconfig や systeminfo，tasklist，net view などのコマンドを攻撃者が使った目的，FW のログから確認すべきこと，FW のログでは感染を検知できない状態についての設問は，実務的な経験があるかどうかによって難易度に差が生じるかもしれませんが，全般的に難易度の高い設問は含まれていません。

## 3.3　問題テーマ難易度一覧表

| 問 | テーマ | 難易度 |
|---|---|---|
| 1 | 電子メールのセキュリティ対策 | B |
| 2 | セキュリティインシデント対応におけるサイバーセキュリティ情報の活用 | B |
| 3 | 標的型攻撃への対応 | 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 全体の出題傾向及び難易度について

午後Ⅱ試験では，午後Ⅰ試験と同様に，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が，技術面・管理面の両側面から解答を導き出すことが求められる設問テーマが多くなる傾向があります。また，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問題文にあるため，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だけでなく，幅広い分野について問う総合問題として出題されることが多いといえます。前回は管理面の設問が極端に少ない試験になっていましたが，今回は，技術面・管理面の設問テーマがバランスよく配置されていました。

問題テーマは，マイニングマルウェアやルートキットなどのマルウェア対応を含めたソフトウェア開発環境のセキュリティ対策と工場ネットワークでのランサムウェア感染・APT攻撃への対応やデータ転送の安全性確保を題材とした工場でのセキュリティ対策です。目新しい点としては，DevOps の実践の改善としてのコンテナ技術の活用について問われたことやセキュリティ対策の標準として，OWASP ASVS，CIS Benchmarks，FedRAMP の用語知識が求められたこと，データ転送の安全性確保策としてデータダイオードの活用などに関して出題されたことが挙げられます。

難易度については問題間で差が生じていました。問 1 は通常の試験対策ではあまり学習しないと思われる DevOps やコンテナ技術という項目が含まれていたことなどから，難易度が高いと判断しました。問 2 は工場ネットワークでのランサムウェアや APT 攻撃への対応やデータを安全に転送する仕組みといった基本的な問題でしたので，設問数や解答ボリュームは問 1 に比べるとかなり多くなっていますが，難易度は標準的です。

## 4.2 各問題のテーマ，特徴

問 1 は，「ソフトウェア開発におけるセキュリティ対策」というテーマで，マイニングマルウェアやルートキットなどのマルウェア対策でのソフトウェア開発環境のセキュリティ向上と DevOps におけるセキュリティ向上策，コンテナ技術活用について問われています。

インシデント発生後のフォレンジック調査でのルートキットの動作説明で，Linux で実行中のプロセスを表示するコマンド，そのコマンドがアクセスするディレクトリについての知識，構成管理や変更管理，リリース前の確認及び実行環境の更新に活用するコンテナ技術に関する知識が問われている点で，受験者を選ぶ難易度の高い問題だと感じました。

この問題では穴埋め問題が 21 と通常の倍近く出題されるという特徴もありますが，穴埋め問題の多くで解答群が用意されていました。また，マルウェアへの対策案として示された各対策が，マルウェアのどの機能への対策となっているのかが問われた問題は，過不足なく回答しなくてはいけない点で難しいといえるでしょう。

問 2 は，「工場のセキュリティ」というテーマで，システム部が管理する基幹ネットワークと各工場や部門が管理する部門機器や部門 NET が存在する中で，ランサムウェア感染と

いうインシデント発生を機にサイバー攻撃による生産設備の停止を防ぐための取組みを実施したという事例で，APT 攻撃のステップや工場の課題を調査し，課題への対処として工場ネットワーク構成の見直しやデータ転送の安全確保策を選ぶという流れです。

目新しい技術としては，前述したデータダイオード方式がありますが，具体的な内容については詳細に説明されています。また，脆弱性管理プロセスの中で行う深刻度評価が CVSS の基本値，現状値，環境値のどれにあたるのかを選ぶ問題などは単に用語を知っているだけでは答えられない問題です。また，工場ネットワークの見直し案によって，どのようなセキュリティ上の効果があるかが問われた設問や認証サーバの設置位置が問われた設問は，ネットワーク上の通信の流れを読み取ることが求められています。しかし，基本的なセキュリティ知識で十分に対応が可能で，解答ポイントの期待が外れることのない素直な設問が多いことから，問題そのものの難易度はやや易しめといえるでしょう。ただ，問題分量や設問数，解答ボリュームが設問１に比べるとかなり多くなっている点を踏まえて難易度は標準的と判断しました。誰もが取り組みやすい問題でした。

## 4.3　問題テーマ難易度一覧表

| 問 | テーマ | 難易度 |
|---|---|---|
| 1 | ソフトウェア開発におけるセキュリティ対策 | C |
| 2 | 工場のセキュリティ | 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

午前Ⅱ試験は，重点分野の「セキュリティ」と「ネットワーク」の 2 分野の合計が 8 割を占めます。午前Ⅱ試験に合格する基準は 60 点以上なので，この 2 分野でしっかりと得点できれば，午前Ⅱ試験に合格できます。したがって，「セキュリティ」と「ネットワーク」の 2 分野に的を絞って学習することをお勧めします。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知識を習得することが大切です。その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からです。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しておくことで，午前Ⅱ対策から午後対策への移行もスムーズに行えるでしょう。

過去問題の再出題率が 7 割前後と高いことから,知識習得後は過去問題演習が必須です。問題集や Web による問題演習を利用して,効率的に演習を繰り返し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。演習後は正解した場合でも必ず解説を読み，誤答の選択肢についての知識も確認しておくと，知識が広がり，類似問題が出題された場合にも対応できるようになります。また，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，少なくとも直近 5 回分は行うとよいでしょう。特に 3 回前からの再出題率が高いことから，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取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，IPA のホームページに掲載されている「情報処理安全確保支援士試験（レベル４）シラバス追補版（午前Ⅱ）Ver2.0」に午前Ⅱにおける知識の細目が示されています。試験要綱よりも具体的に用語が列挙されていますので，特にセキュリティ分野の用語については，一つ一つを確認し，分からない用語があった場合には，学習しておくとよいでしょう。

さらに,新しい攻撃についてもたびたび出題されていますので,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ちます。

## 5.2 午後Ⅰ対策

午後の出題範囲は，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，この中に IT の技術動向として IoT 機器やビッグデータ，AI なども含まれています。「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。

セキュアプログラミングに関する問題は，今回は出題されていませんでしたが，これまでは毎回 1 問出題されていましたので，次回以降に出題される可能性は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，選択しない方が賢明です。その場合，残りの 2 問を必ず選択することになりますので，苦手なテーマ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問題を選択する可能性がある場合は，これまで 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多く出題されていますので，教材の一つとして利用するとよいでしょう。

また，セキュリティインシデント対応の事例が午後Ⅰ・午後Ⅱともに頻繁に出題されていることから，インシデント対応の流れに沿った学習も欠かせません。インシデント対応に関する過去問題をピックアップして集中的に演習を行うのも効果的です。そして，異常が発生している PC を特定するのに必要となるログの見方やネットワークコマンドの表示結果の見方，証拠を保全するための手順や注意点，マルウェア感染範囲や感染経路を特定するためのファイアウォールのルールの読み取り，マルウェア対策ソフトや脆弱性修正プログラムの運用上の注意点，出口対策としてのフィルタリングの設定などの共通的な知識を洗い出しておくと，さまざまなインシデント対応事例の問題に活用できると思います。これには，ネットワーク技術知識の習得が前提となります。例えば，よく出題されるファイアウォールのフィルタリングルールに関する問題では，ネットワーク構成図や事例内容から，何のパケットがどこからどこへ流れていくか，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いえるでしょう。

午後Ⅰ対策では，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。実務で経験したことがない事例

については特に，さまざまな問題演習を通して疑似体験をしておくことは非常に有効です。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が，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だけ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

午後Ⅱ対策は基本的には午後Ⅰ対策と同じです。追加で行うべき対策としては，セキュリティ管理面の知識を強化しておくことが挙げられます。午後Ⅰ対策で提示した，午後の出題範囲の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，まず，ISMS に関する JIS Q 27000:2014，27001:2014，27002:2014 や，サイバーセキュリティ基本法，個人情報保護法，不正競争防止法などを学習し，余裕があれば，米国 NIST の“重要インフラのサイバーセキュリティを向上させるためのフレームワーク”，“コンピュータセキュリティインシデント対応ガイド”などについての概要も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。