システム監査技術者

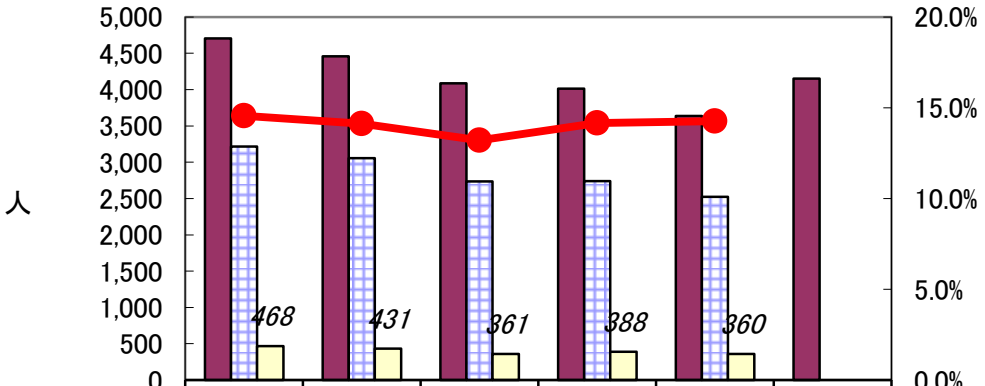
1.　はじめに

1.1　総評

今回はセキュリティ分野からの出題が目立つことが特徴です。午前Ⅱ問題では，従来の情報セキュリティに関する出題の強化・拡充の方針どおりに多めの出題が継続しており，午後Ⅰ問題では主題として制御システムの情報セキュリティの問題が扱われ，さらに午後Ⅱ問題はすべてセキュリティ監査の問題でした。特に，制御システムの情報セキュリティをはじめ，サイバーセキュリティ対策を意識した出題視点が多く見受けられます。2020 年の東京オリンピック・パラリンピックを控え，ライフラインなどの重要インフラへのサイバー攻撃が一層懸念される昨今，このようなセキュリティ分野の出題機運が高まっていたといえるでしょう。また，数年単位で情報セキュリティ関連の出題が集中する傾向も感じられ，本年はそのような年に当たったといえるかもしれません。

午前問題の難易度は標準的といえます。見慣れた題材も従来どおり多く，基本的な知識を押さえて過去問題に取り組んでいれば解答できる問題がほとんどです。また，午後Ⅰ問題は多彩な設問構成で特定分野の知識が要求される設問もあり，その意味ではやや難易度が高い部分も見受けられますが，全体的には標準的な難易度といえます。午後Ⅱ問題は，コントロール・監査手続を問う基本的な筋立ては崩されておらず，難易度は標準的といえます。

1.2　受験者数の推移



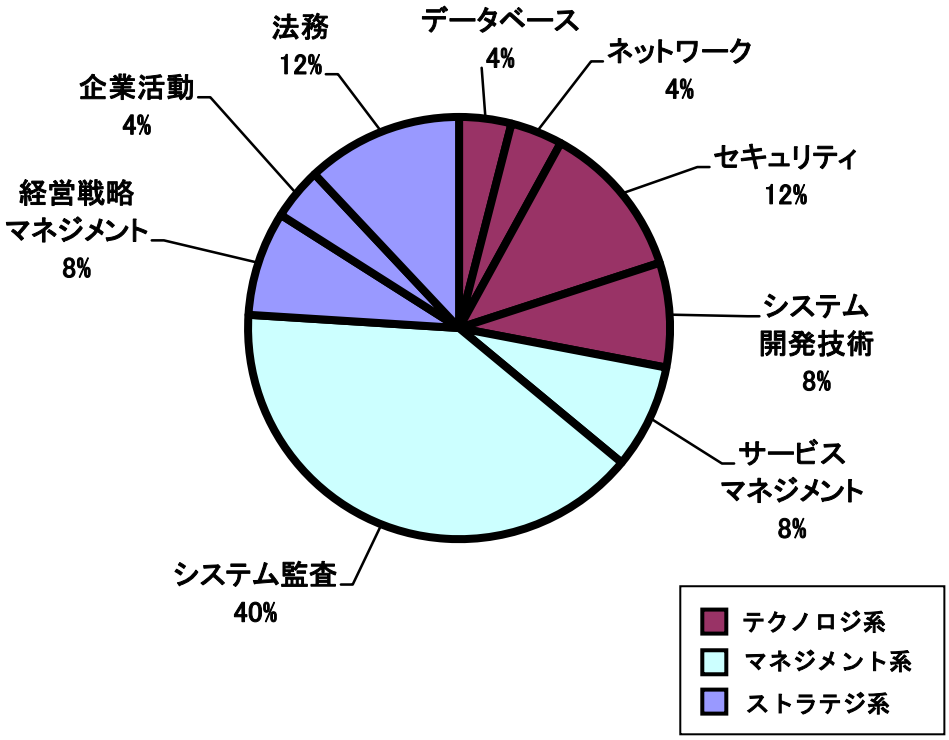
	H24春	H25春	H26春	H27春	H28春	H29春
応募者数	4,705	4,459	4,087	4,012	3,635	4,151
受験者数	3,216	3,053	2,733	2,740	2,524	
合格者数	468	431	361	388	360	
合格率	14.6%	14.1%	13.2%	14.2%	14.3%	

2.　午前Ⅱ問題の分析

2.1　問題テーマの特徴

システム監査技術者の午前Ⅱ問題の出題内容は，従来どおり標準的なものでした。出題分野としては，出題範囲で設定された分野を漏れなくカバーしています。出題分野の重点は，原則どおりに「システム監査」の分野であり，マネジメント系とストラテジ系からの出題が全体の 7 割強を占めています。なお，前回試験から，「システム監査」の分野の問題と「法務」の分野の問題の構成が，11 問と 2 問から，10 問と 3 問に変更された状況が継続しています。

出題分野	出題比率	出題数
データベース	4%	1 問
ネットワーク	4%	1 問
セキュリティ	12%	3 問
システム開発技術	8%	2 問
サービスマネジメント	8%	2 問
システム監査	40%	10 問
経営戦略マネジメント	8%	2 問
企業活動	4%	1 問
法務	12%	3 問



全体的には，過去問題やその焼直しとみなせる出題も多く，通常の午前対策の問題演習で十分に対応できる問題といえます。新規出題としては，“情報セキュリティ監査基準に基づく保証型監査の意見表明”に関する問題，“CSIRT(Computer Security Incident Response Team)”に関する問題，“CRUD マトリックスを用いたエンティティのライフサイクル分析”に関する問題などがまず目につきます。題材としては，各区分で従来から扱われてきた出題テーマであっても，視点を変えたり，より詳細な部分を問う新作問題が出てきています。CSIRT については，前回の午後Ⅰ試験でもインシデント対応の問題として出題されましたが，サイバーセキュリティ対策の動向とも関連が深く，午後Ⅰで扱われた制御システムに関するセキュリティインシデントなどもカバーできるように機能を拡大してきています。なお，今回の「SL 理論によるリーダシップの型」「マーケットバスケット分析」「ファイブフォース分析」など，企業活動や経営戦略マネジメント分野の問題について，IT ストラテジスト試験で先行出題されてきた過去問が多く流用されていることが目に付きます。

2.2　難易度の特徴

全体的に，標準的な難易度の問題が出題されています。午前Ⅱ試験の特徴の一つである出題技術レベルについては，最も高度なレベル(レベル 4)の出題も想定される「システム監査」の問題で少し変化が見受けられました。従来どおりの解きやすい過去問が含まれている一方で，“システム監査基準”や“情報セキュリティ監査基準”について，従来とは少し視点を変えた難易度が高めの新作問題が出題されています。もとより，「システム監査」分野の問題は，出題ポイントが固定化しやすいという性質があることから，問題作成において無理に難易度を高くすることは難しく，標準的な難易度に落ち着くことが普通です。そして，その多くは出題例のある過去問題やその類似問題となっていました。また，新規問題も，これまでは基本的な用語の意味さえ理解できていれば対応できる問題が多かったのですが，今回は基準類の読込みなどが求められる解き難い出題でした。新規問題以外が比較的簡単なものが多かったので，新規問題の難易度を高めに設定してバランスをとったのかもしれません。いずれにせよ，出題全体に占める過去問題やその類似問題の割合は 6 割強といってよい状況がまだ継続していますので，従来どおりに過去問題の演習が効果的な学習方法といえ，通常の午前対策の問題演習で合格可能な問題内容といえます。

2.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	システム監査におけるサンプリング（試査）	B
2	監査証拠	A
3	システム監査基準の前文に記載の利用目的	A
4	ITF 法	B
5	システム監査基準に基づいて作成されたシステム監査報告書	C
6	テストデータ法を監査手続として使用する上での留意点	B
7	監査証跡	A
8	情報セキュリティ監査基準に基づく保証型監査の意見表明	C
9	固定資産管理システムに係る IT 全般統制	B
10	“全社的な内部統制”としての“IT への対応”	B
11	JIS Q 20000-2:2013 による SLA の作成指針	C
12	データ管理者の役割	B
13	プログラム著作物の著作権	B
14	下請代金支払遅延等防止法	B
15	特定商取引法	B
16	SL 理論によるリーダシップの型	C
17	SQL 文(LEFT OUTER JOIN)	B
18	サブネットワークアドレス	B
19	CSIRT	A
20	ブルートフォース攻撃	A
21	ペネトレーションテスト	A
22	JIS X 25010　システム／ソフトウェア製品の品質特性	B
23	CRUD マトリックス	A
24	マーケットバスケット分析	B
25	ファイブフォース分析	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 問題テーマの特徴

出題分野としては，システム開発プロジェクトにおける品質管理やデータ移行に関する監査，制御システムに関するセキュリティ監査，在庫管理システムの業務処理統制の監査など，幅広い分野からの出題といえます。

今回のセキュリティ監査の問題では，石油プラントという重要インフラの制御に用いられる制御システムへのサイバー攻撃を想定した，制御システムの情報セキュリティの内容が初めて扱われたことが特徴です。制御システムのセキュリティマネジメントシステム(CSMS：Cyber Security Management System for IACS[Industrial Automation and Control System])に関する第三者認証制度も2014年から開始されており，その意味ではトピック的な出題といえます。また，業務処理統制の監査の問題については，単純な在庫管理に関する内容だけでなく，システム統合プロジェクトでのデータ移行に関する内容に在庫移管の話を絡めた問題であることが特徴です。

設問レベルでは，リスク，監査要点，コントロール(対策)，監査手続などが，さまざまな形態で問われています。したがって，設問テーマ設定という観点からは偏りのない問題であったといえます。

問 1 は，企業合併及び工場と物流センタの再編に伴う在庫管理システムの統合を題材とした業務処理統制(アプリケーションコントロール)の監査をテーマとした問題で，システム開発プロジェクトにおけるデータ移行の監査や有効性監査の側面もある問題といえます。

問 2 は，システム開発プロジェクトにおける設計工程からテスト工程の品質管理の監査をテーマとした問題で，品質評価の適切性をかなり具体的に検証・評価させる内容となっています。昨年の午後Ⅱ問題の問 2 が“情報システムの設計・開発段階における品質管理に関する監査”であったこととの関連性も想像されるような問題テーマでした。

問 3 は，製油所の石油精製制御システムを題材とした制御システムのセキュリティ監査をテーマとした問題で，まさに重要インフラへのサイバー攻撃を想定した問題といえます。制御システムならではのセキュリティ管理や脆弱性対応で重視されるポイントを検証・評価する設問テーマで構成されています。

3.2 難易度の特徴

いずれの問題も，監査の過程が監査対象の概要とともに効率よくまとめられており，読みやすいものでした。出題内容としては，問題文で明解に対応付けられたリスクとコントロールを踏まえた設問が多く，設問に該当する問題文箇所は見つけ易い問題が多かったといえます。しかし，解答ポイントは分かっても，どのレベルまでどのような表現で解答すべきかで迷う設問が複数見受けられます。その部分を除けば，全体的な難易度は標準的といえます。問題文量や解答記述量については，特定の問題に偏ることなくほぼ均一で，いずれも適切な量であり，この意味での解答時間確保の難しさはありません。

問 1 は，業務処理統制の問題なので他の問題に比べて問題文がやや長めですが，対象業務に関して丁寧に記述されており，問題文をよく読めば解答ポイントがつかめる設問が多いといえます。ただし，解答表現に迷う設問が多く，その意味での難易度は高いといえます。表現の仕方によっては，解答すべきポイントからずれ過ぎたり，広がり過ぎたりしかねないおそれもあります。

問 2 は，指摘密度などの具体的な評価指標を用いた品質管理を検証・評価する細かい内容でしたが，なじみ深いテーマでもあることから，比較的容易に解答ポイントが見い出せる設問が多く，難易度は標準的な問題といえます。

問 3 は，セキュリティ監査という頻出テーマの問題ですが，製油所の制御ネットワーク・制御システムという監査としては特殊な事例設定であり，制御システムの情報セキュリティの知識が全くないと，解答すべきポイントの絞り込みや解答の表現レベルなどにとまどう設問がいくつか含まれています。その意味で，3 問中最も難易度が高めの問題といえます。

3.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	在庫管理システム統合計画の監査	B
2	システム開発における品質管理の適切性の監査	B
3	制御ネットワーク及び制御システムの監査	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

出題分野としては，組織の内部不正に対する技術的対策や組織的対策と，標的型攻撃などの情報システムの運用段階での脅威を想定した情報セキュリティ管理を題材としたセキュリティ監査の分野のみからの出題でした。一昨年も両問ともほぼセキュリティ監査といえる出題でしたが，両問とも完全にセキュリティ監査をテーマとした出題であったことはこれまでなく，珍しい年といえます。また，個人情報や営業秘密などの企業内の重要情報の漏えいを意識した出題となっていることから，“個人情報保護法”の改正や経済産業省の“営業秘密管理指針”の改訂，IPA の“組織における内部不正防止ガイドライン”の改訂など，最近のセキュリティ法規の動向を踏まえた出題ともいえます。

出題テーマとしては，両問とも比較的絞り込んだテーマ内容ですが，対象にできる情報システムは限定されておらず，いずれかは選択可能な出題構成といえます。

最近の問題テーマの構成は，①最新のトピックに絡めた問題が 1 問，②平均的な受験者が選択しやすい比較的オーソドックスなシステム監査の問題が 1 問といった出題が基本となってきています。今回の出題構成では，問 1 が前記①と②にまたがった問題，問 2 が前記①に分類できる問題とみなすことができます。

問 1 は，組織の内部不正対策の監査をテーマとした問題です。内容的には，誰にでも心当たりがある書きやすい問題テーマであったといえます。監査対象となる内部不正対策が法令などに準拠して行われているかどうかという準拠性の監査の側面もある問題です。なお，ここ 2～3 年前から相次いで発生している内部不正による大量の情報漏えい事件を受け，経済産業省が IPA の“組織における内部不正防止ガイドライン”の周知徹底を図っており，その意味では，トピック的な出題ともみなせます。

問 2 は，標的型攻撃などの情報システムの運用段階での脅威を想定して，組織として確保すべきセキュリティレベルを維持するための情報セキュリティ管理を題材としたセキュリティ監査をテーマとした問題です。最新の攻撃手法やインシデント対応などを想定した実務的なテーマ内容であり，トピック的な出題といえます。

4.2 難易度の特徴

論述内容については，基本的には，リスクやコントロールに対する監査手続といった標準的な設問で構成されており，解答しやすい形態となっています。ただし，昨年の問 1 と同様に，設問イとウがそれぞれ同形の出題形式(監査手続)となっている問題もあり，まとめ方や記述量の割振りに迷う場面もあったかもしれません。なお，最近の出題で設問文に明示されることの多かった監査証拠への言及が今回は全くありませんでしたが，監査手続を記述するうえでは本来必須の事項であり，難易度に及ぼす影響はありません。

問 1 は，組織の内部不正対策の監査ということで，内容的には，誰にでも心当たりがある選択しやすい問題テーマであったといえます。設問形式は，設問イと設問ウでともに監

査手続が問われており，コントロールや監査要点が設問文で明示的に求められていないので，まとめ方に迷った受験者の方もおられたかもしれません。また，技術的対策が問題文に例示されていないので，どのようなレベルで書くべきかで迷った受験者の方もおられたかもしれません。しかし，通常どおりの設問構成になっていなくとも，コントロール(対策)や監査要点のまとめ方が変わる訳ではなく，例示がない部分は逆に自由に書けることになるので，内容的には大きな影響はないと考えられます。むしろ，設問イと設問ウでコントロールと監査手続を分けて問われる場合よりも，挙げるべきポイントが少なくて済むともいえます。よって，これらの変則的な設問構成の難易度への影響はほとんどないと考えられます。このような点から，総体的には，標準的な難易度の問題といえます。

問 2 は，最新の攻撃手法やインシデント対応などを想定した実務的なテーマ内容であることから，やや専門的な内容といえ，特定のセキュリティ分野の知識や関連実務に携わっていないと書きにくい面がある問題といえます。また，設問アでまずセキュリティレベルが問われているので，それをどのように設定し表現するか，そして，設問イ以降とどのように整合を取っていくかなどを適切にまとめていかなくてはならず，その意味では難易度がやや高めの問題といえます。

4.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	情報システムに関する内部不正対策の監査	B
2	情報システムの運用段階における情報セキュリティに関する監査	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の出題分野の中心となるマネジメント系とストラテジ系の問題を攻略することが基本となります。特に，過去問題の演習が効果的で，出題割合の最も多いマネジメント系の「システム監査」分野の問題を確実に解けるように学習しておいてください。学習内容の重点は，システム監査業務における基本用語の概念，『システム監査基準』『システム管理基準』『情報セキュリティ監査基準』『情報セキュリティ管理基準』などの基本的事項，コンピュータ支援システム監査技法，内部統制の評価・監査の基本的事項などが挙げられます。また，ストラテジ系では，頻出事項への対応を講じておくとよいでしょう。例えば，頻出事項として，「経営戦略マネジメント」分野では，「バランススコアカード」や「PPM」など，「法務」分野では，「労働者派遣法」「個人情報保護法」「請負契約の法務」や今回出題の「著作権法」「下請代金支払遅延等防止法」などが挙げられます。新試験制度が始まってからは，TOC(制約条件理論)や SECI モデルのように，新制度下で設定された出題範囲の知識項目からの出題も見られますので，他区分の午前Ⅱ問題を通じて学習しておくとよいでしょう。特に，企業活動や経営戦略マネジメント分野の問題については，IT ストラテジスト試験の午前Ⅱ問題の過去問題が参考になることが，今回の出題事例からも明らかです。ただし，数問の得点のためだけに学習労力を費やすよりは，出題の重点分野である「システム監査」と「法務」の 2 分野についての学習に絞ったほうが得策であることは改めて言うまでもありません。そのほか，試験要綱改訂時に追加された事項のうち，IFRS(国際財務報告基準)，刑法(特にウイルス作成罪)，クリエイティブコモンズ等のライセンス形態なども注目すべき題材といえます。

テクノロジ系の「データベース」「ネットワーク」「セキュリティ」「システム開発技術」の各分野や，そのほかの出題分野への対応については，午前Ⅰ対策と基本的に同等ですが，少しずつ新制度下で設定された出題範囲の知識項目からの出題に移行してきている傾向が見受けられますので，過去の頻出事項を中心に学習したうえで，余裕があれば，その時々で注目度の高い技術的事項の知識を取得しておくとよいでしょう。

5.2 午後Ⅰ対策

午後Ⅰの出題分野として扱われる頻度が高いものとして，セキュリティ監査，業務処理統制の監査，システムの開発業務や運用業務などのシステムライフサイクルの監査が挙げられ，これらの設問事項への対応が午後Ⅰ対策の基本となります。

セキュリティ監査関連の問題では，ID 管理やログ活用の視点を問われることが多いので，この出題事項の学習は不可欠です。この際，監査対象となる情報システムとしては，顧客情報や社員情報を扱う情報システムが筆頭に挙げられます。なお，セキュリティ監査の監査手続については，平成 21 年 7 月に経済産業省が策定・公表した『情報セキュリティ監査手続ガイドライン』が参考になります。このほか，スマートフォンやタブレットなどの携

帯デバイスの業務利用の際のセキュリティの問題，知的財産の窃取や情報システムの破壊による事業活動妨害を目的とした特定組織への攻撃の脅威など，セキュリティ監査の分野では，注目すべき題材が豊富にあります。例えば，今回出題されたようなサイバー攻撃への対応や，今回午後Ⅱ問題で出題された内部不正による情報漏えいへの対応などが挙げられます。午後Ⅰ問題テーマと前年の午後Ⅱ問題テーマの関連がうかがえる出題事例も時々見受けられますので，内部不正対策や標的型攻撃対策などに関するセキュリティ監査の問題には着目しておくべきでしょう。内部不正対策に関連しては，平成 27 年に，『不正競争防止法』の改正や経済産業省の『営業秘密管理指針』の全面改訂が行われているほか，IPA の 『組織における内部不正防止ガイドライン』も改訂されています。また，クラウドセキュリティ監査も注目される題材の一つです。クラウドセキュリティ監査制度における基準となる『クラウド情報セキュリティ管理基準』は，情報セキュリティ監査制度における主体別・業種別管理基準として，平成 24 年に JASA(日本セキュリティ監査協会)から公表されています。また，日本提案の ISO/IEC 27017(クラウドサービスの情報セキュリティ国際規格)が最近発行されており，クラウドセキュリティの国際認証も開始されていることからも，この分野の注目度は高いといえます。JIPDEC(日本情報経済社会推進協会)では，昨年から，ISMS 認証に追加する形態(アドオン認証)での ISO/IEC 27017 によるクラウドセキュリティ認証が開始されており，認証規格も昨年末に JIS Q 27017:2016 として JIS 化されています。そして，『クラウド情報セキュリティ管理基準』に先立ち公表された，経済産業省の『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』も最近改訂され，それと同時にその活用ガイドブックが公表されています。これらのクラウドセキュリティ監査に関する基準類は，クラウドコンピューティングにおけるセキュリティ監査の視点を学ぶうえで役立つことでしょう。

業務処理統制の監査については，販売管理・購買管理・在庫管理・生産管理といった基本的な業務処理システムを監査対象とする事例が多いといえます。通常，業務処理統制をテーマとした問題では，データインテグリティおよびそれに関連するセキュリティの視点が設問事項となりますので，代表的な業務処理システムにおいて，データ不整合が生じるポイントやセキュリティ上の問題が生じるポイントについて学習しておくことは有効です。また，内部統制の評価・監査の視点から，財務報告に係る内部統制の IT への対応部分に関わる業務処理統制(IT 業務処理統制)が出題される機会も増えてきました。これについては，『システム管理基準』の追補版として，経済産業省から公表されている『システム管理基準 追補版 (財務報告に係る IT 統制ガイダンス)』の内容などが参考になります。そのほか，受託業務については，86 号監査の財務報告以外の部分を対象とした『受託業務のセキュリティ・可用性・処理のインテグリティ・機密保持に係る内部統制の保証報告書』の原則及び規準をまとめた《付録 4》文書などが日本公認会計士協会から最近公表されており，財務報告に限らない内部統制(受託会社側)のポイントを知るうえで参考になります。

システムライフサイクルの監査については，承認プロセスの不備や適切性を問われることが多いといえます。コントロールの視点からは，全般統制の監査ともいえます。全般統

制は,『システム管理基準』や最近改訂された『COBIT』などのガイドラインの内容が参考になります。

このほか，あらゆる組織で事業継続計画(BCP：Business Continuity Plan)の見直しが進められており，事業継続マネジメントシステム(BCMS)の国際規格である ISO 22301(JIS 規格では JIS Q 22301 に相当)も最近発行されていることから，試験対策上の重要性は増しています。

5.3 午後Ⅱ対策

今後の午後Ⅱの出題構成のパターンとしては，多少の変動はあるかもしれませんが，①最新のトピックに絡めた問題と，②平均的な受験者が選択しやすい比較的オーソドックスなシステム監査の問題との組合せが出題構成の基本形となっていくものと予想され，その路線で出題される問題への対応や受験時の問題選択の方針の決定が試験対策上重要といえます。

論述で求められる視点には，新しい情報技術やビジネスモデル，法制度などの知識が要求される機会が多く，受験者の方は，これらに関する最新の潮流をよく把握しておく必要があります。

前記①に分類される問題としては，マイナンバー制度開始や個人情報保護法改正動向を踏まえた個人情報保護管理，クラウドコンピューティング，外部委託業務における内部統制監査の効率化，情報セキュリティ関連(例えば，今回扱われたような内部不正対策や標的型攻撃による諜報活動への対応)，事業継続計画(BCP)に関する題材が挙げられます。クラウドコンピューティングの監査関連では，午後Ⅰ対策として挙げたような基準類を参考に監査の視点を養っておくことは，試験対策として有効です。そのほか，監査証跡と証拠保全などに関するディジタルフォレンジックスに関する問題なども重要です。

前記②に分類される比較的オーソドックスなシステム監査の問題については，企画業務・開発業務・運用業務などに関するシステムライフサイクルの監査，ソフトウェアパッケージの監査，委託・受託業務の監査，変更管理の監査，ドキュメント管理の監査などが挙げられます。

午後Ⅱ対策では，このような想定される問題テーマについて，監査対象となる情報システムや業務における問題点(リスク)は何か，それに対するコントロール(対応策)にはどのようなものがあるか，その整備状況や運用状況をチェックする監査手続はどのようにすればよいか，といった流れをさばけることが攻略上のポイントになります。