システム監査技術者

1.　はじめに

1.1　総評

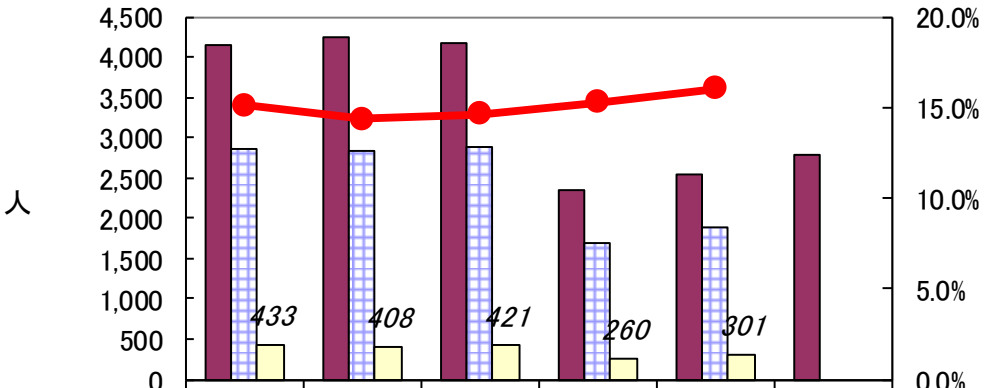
今回もシステム監査技術者に必要な専門知識や業務活動が幅広く問われるような試験でした。今回の出題には，AI や IoT，RPA といった巷間で注目を集めるようなトピック的なテーマはなかったため，新しさやインパクトは感じられなかったかもしれませんが，新基準や法改正，感染症対応やテレワーク推進など，現状を見据えた出題事項が随所に見受けられます。

午前Ⅱ試験では，システム監査や財務報告に係る内部統制に関する基準などをベースに，システム監査や内部統制に関する知識が多く問われました。

午後Ⅰ試験では，令和 4 年 4 月の改正個人情報保護法の全面施行を受けた個人情報保護の監査や，新型コロナウイルス感染症への対応としてのワークフローに関わるシステムの監査など，最近起きた世の中の変化に対応したシステム監査業務が題材となりました。

午後Ⅱ試験では，ここのところ毎年出題されていたトピック的なテーマの問題はありませんでしたが，昨年に引き続き，監査計画の策定に関する問題が出題されたことが特に目を引きます。近年，システム監査業務そのものに関する問題の出題が珍しくなっていたにもかかわらず，この分野の問題が 2 年連続して出題されたことは想定外でした。

1.2　受験者数の推移



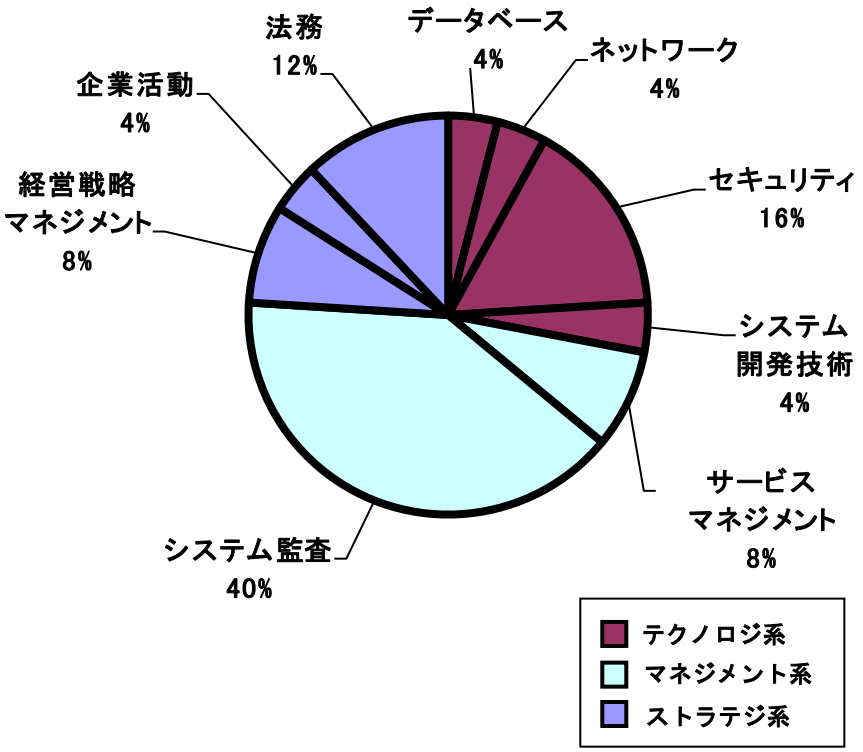
	H29春	H30春	H31春	R2 10月	R3秋	R4秋
応募者数	4,151	4,253	4,175	2,350	2,552	2,792
受験者数	2,862	2,841	2,879	1,702	1,877	
合格者数	433	408	421	260	301	
合格率	15.1%	14.4%	14.6%	15.3%	16.0%	

2.　午前Ⅱ問題の分析

2.1　問題テーマの特徴

例年どおり，過去問題やその焼直しとみなせる出題が 7 割近くを占めています。今回は新監査基準・管理基準に関する問題が 3 問あり，関連基準に関する問題と合わせると，システム監査分野の半数を占めています。特に，関連基準については，令和元年に改訂された金融庁の『財務報告に係る内部統制の評価及び監査の基準』及び『財務報告に係る内部統制の評価及び監査に関する実施基準』からそれぞれ 1 問ずつ出題されています。

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	16%	4 問
システム開発技術	4%	1 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



新規出題としては，“情報システムを対象としたデューデリジェンス”の問題が，情報システム投資の評価に絡めてシステム監査分野の問題として出題された点，“JIS X 9251:2021 プライバシー影響評価のためのガイドライン”におけるプライバシー影響評価(PIA：Privacy Impact Assessment)に関する問題，環境適応の立場からの組織論としての“コンティンジェンシー理論”に関する問題，“JIS X 0153：2015　利用者用文書類の設計者及び作成者のための要求事項”における参照モードに関する問題などがまず目につきます。

前回試験に引き続き，基準等に基づく出題が多めに感じられます。なお，“バリューチェーンにおける支援活動”に関する問題など，経営戦略マネジメント分野ではITストラテジスト試験の過去問題が利用されやすいので，今後の試験対策としては，引き続き留意していく必要があります。

2.2　難易度の特徴

全体的には，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の差については，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」や「セキュリティ」の問題で，難問と感じられるものはほとんどないことから判断して，午前Ⅱ試験の難易度を左右するほどの影響は感じられません。この分野の問題は，問題作成の立場から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，新監査基準・管理基準に関する問題がある程度揃ってくれば，対応しやすくなってきます。そして，そのほかの問題の多くは出題例のある過去問やその類似問題となります。

今回の新規出題の問題中で難易度が高めの問題は半数以下です。そのような新規問題は，知らないと手も足も出ない問題も多いですが，過去の出題事例から正解を類推できる問題もあるため，ある程度の対応は初見でも可能です。今回の出題では，バックアップに必要な磁気テープ本数の算出など，条件を見誤ると正解し難く迷路に迷い込みかねない新規問題がある反面，初見でも正解が推定しやすい問題も 2，3 問は見受けられます。したがって，午前Ⅱ試験の全体的な難易度は標準的といえます。

情報処理技術者試験には，IT に関わる技術者が今知っておくべき事柄について，試験に出題することで広く啓蒙する役割もうかがわれ，法律の重要・改正ポイントや公表されたばかりの基準・ガイドラインの内容などが出題されるため，このような趣旨の問題の難易度が高めになりがちです。今回の出題では，JIS 規格関連の出題にこのような問題が 2 問ほど見受けられます。

2.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	デューデリジェンス	B
2	試査	A
3	システム管理基準：基準の活用における留意点	B
4	システム監査基準：フォローアップ	A
5	監査人の意見が分かれた場合の対応	B
6	個人情報管理台帳の取扱いの監査の指摘事項	B
7	JIS Q 27002：運用システムに対する監査の影響	B
8	システム管理基準：IT ガバナンスを成功に導く原則	B
9	財務報告に係る監査の基準：統制活動	A
10	財務報告に係る監査の実施基準：自動化統制	B
11	資金決済法	B
12	ウォームスタンバイ	B
13	バックアップに必要となる磁気テープ本数	C
14	JIS X 9251：個人識別可能情報の処理	C
15	特定商取引法	B
16	コンティンジェンシー理論	C
17	AES	B
18	公開鍵暗号方式の暗号通信での必要鍵数	B
19	ビヘイビア法	A
20	OP25B	B
21	トランザクション異常終了の際に行われる処理	A
22	DNSSEC	B
23	JIS X 0153：参照モード	C
24	バリューチェーンにおける支援活動	C
25	LTV の計算	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

出題分野としては，個人情報保護関連のセキュリティ監査に関する問題，ワークフローに関わるシステムの見直しを題材としたシステム企画業務の監査に関する問題，システムの運用管理や障害管理を題材としたシステム運用業務の監査に関する問題であり，出題テーマの枠組みとしては，比較的定番のテーマからバランスよく出題されています。とはいっても，具体的な出題内容としては，令和 4 年 4 月に全面施行された改正個人情報保護法の改正ポイントでもある仮名加工情報及び個人関連情報の活用や，新型コロナウイルス感染症や働き方改革への対応としてのワークフローの見直し，ペーパーレス化・脱印鑑の推進など，時宜を得た内容を絡めた問題が目立ちました。特に，セキュリティ監査を主題とした出題は5年ぶりで，個人情報保護の観点だけでなく，ログ管理やWebサイトセキュリティなど，セキュリティ関連の基本知識を前提とする問題構成となっています。なお，従来，午後Ⅰ問題としては定番であった，業務処理統制をテーマとした出題は，前回に引き続きありませんでした。

設問レベルでは，全体的に，リスクや監査ポイント，監査証拠や監査手続など，システム監査に関する重要な論点は従来通り満遍なく問われています。

近年の午後Ⅰ問題の小問数(解答すべき事項の数)は 5 つ程度であることが多く，他区分に比べて少なめであることが特徴でしたが，今回は 1 問当たり 6 つから 8 つの小問で構成されており，例年より小問数が増えました。小問数が多いと，1 小問当たりの配点が小さくなるので，出題者の意図に沿わない解答となったとしても，得点への影響が少なくて済みます。

各小問で問われている内容には，出題者の意図が読み取りづらいものや，まとめ方が難しいものも散見され，その意味では，難易度がやや高めの出題であったといえます。

3.2 各問題のテーマ，特徴

問 1 は，個人情報を取り扱うオンラインショッピングシステムにおける改正個人情報保護法への対応状況の監査をテーマとした問題です。改正個人情報保護法の改正ポイントでもある仮名加工情報及び個人関連情報の活用に絡めて，その活用リスクや情報漏えいリスクに関連する内容が問われています。特に，GPS 位置情報の活用については，継続的に収集される位置情報に関する問題点が問われており，出題者が意図する解答ポイントの選定やまとめ方が難しいものとなっています。また，検知機能としてのログ管理システムの活用や，ディレクトリトラバーサルの脆弱性に関する Web サイトセキュリティ上のリスクなど，セキュリティ分野の基本的な知識も問われていますが，やはり解答ポイントの選定やまとめ方に迷うものもあり，難易度は高めの出題であったといえます。

問 2 は，リモートワークや働き方改革の推進を背景に実施される申請書等のペーパーレス化を目的としたワークフローの見直しの監査をテーマとした問題です。問題としては素

直な構成で，実質的には監査ポイントを問う設問が多く，解答ポイントも問題文中で容易に見つけることができて解き易いため，3 問中では最も易しく感じられる問題でした。

問 3 は，金融機関のオンプレミスシステムの運用管理及び障害管理に関するシステム運用業務の監査をテーマとした問題です。特に，障害管理に関する監査の内容が中心となっており，委託元・委託先・再委託先との責任分担といった外部サービス管理に関する内容も含まれています。問題としては素直な構成で，実質的には監査ポイントを問う設問が多めですが，解答ポイントの選定やまとめ方に迷うものもあり，難易度はやや高めの出題であったといえます。

3.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	個人情報保護の監査	C
2	ワークフローに関わるシステムの監査	B
3	システム運用業務の監査	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 全体の出題傾向及び難易度について

例年とは出題形式が少し違うと感じられた方が多いと思います。システム監査技術者の午後Ⅱ問題は，特定のシステムを対象にして，「リスク→コントロール→監査手続」というシステム監査の基本的な流れに沿って設問が構成されている問題がほとんどです。しかし，今回の問題は一見すると，2 問とも従来の設問構成とは異なっているように感じる問われ方や表現方法が目に付きます。とはいっても，根幹となる基本的な流れから外れているという訳ではないので，従来通りの論述構成が可能です。

出題分野としては，情報システムの個別監査計画の策定と，制約及び監査リスクに応じた監査手続の設定を題材にしたシステム監査業務の分野からの出題と，情報システムの改変に伴うシステム障害管理態勢を題材にしたシステム運用業務の監査の分野からの出題でした。特に，昨年に引き続き，システム監査業務の分野からの出題があった点が注目されます。

最近の問題テーマの構成は，その性質から，①最新技術など世の中のトピックに絡めた問題が 1 問，②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 問といった分類ができるような出題パターンといえます。今回は，前掲のシステム障害管理態勢に関する監査の問題が②に相当します。そして今回は，①に相当する問題の替わりに，監査計画や監査手続の策定というシステム監査業務そのものに関する問題が出題されています。午後Ⅱ問題が 3 問中 1 問選択の形式で出題されていた頃には，3 問中 1 問がこのような監査業務に関する問題であるケースが多かったのですが，2 問中 1 問選択の形式になってからは，このような問題の出題頻度はかなり低くなっていました。それにもかかわらず，2 年連続しての出題となりました。システム監査業務そのものに関する問題については，近年，“監査計画”を題材に含める事例が多く，今回も，“個別監査計画”を扱った題材となっています。さらに，“監査リスク”といった，平成 30 年のシステム監査基準の改訂で改めて重視されるようになった，“リスクアプローチに基づく監査計画の策定”という路線に沿った出題となっています。

②に相当するシステム障害管理態勢に関する監査の問題については，“体制”ではなく“態勢”を使用した意図も汲み取る必要があります。つまり，環境変化に応じて，動的に運用・改善が行われ，実際に機能している状態にあるかという点，すなわち実効性のあるものが構築されているかが重視されています。このような言い回しは特に金融関係のシステムで好んで用いられることが多く，さらに問題文中で例示された「API 連携のための情報システムの改変」については改正銀行法対応に基づく金融機関の API 開放の推進と無関係であるとも思えず，今回の午後Ⅰ問 3 の金融機関システムの障害管理を含む出題との関係性がうかがわれます。

全体的に，論述すべき要求事項が多く，各事項についての問題文での例示が少ないので，出題意図に沿った論述を完結するのは難しいかもしれません。従来とは異なる要求事項については，具体的な論述が難しい内容も多く，その意味で今回の午後Ⅱ試験の難易度はやや

高めといえます。

4.2　各問題のテーマ，特徴

問 1 は，情報システムの個別監査計画の策定における重点項目・着眼点の設定やその監査上の制約を踏まえた監査リスクとそれに対応するための監査手続が問われる内容となっています。監査対象とする情報システムについては自由に選択できる反面，「制約があって実施できない監査手続」や「それによって生じる監査リスク」といったイレギュラーな内容が問われているため，論述内容の事前準備は困難で，実務経験がないと具体的な論述がしづらい難問といえます。問題文中では，監査上の制約として，「テレワーク環境や監査資源」が例示され，監査リスクに対応するための監査手続として，「PDF ファイルの原本性確保に必要な監査証拠の入手」が例示されています。これらは，テレワーク環境の推進や改正電子帳簿保存法のへの対応・脱印鑑といった流れと無関係とはいえず，問題テーマとして表立つことはなくとも，時宜にかなった内容の問題となっています。

問 2 は，情報システムの改変とそれに対応する障害管理態勢を踏まえて，管理態勢の実効性を確かめるために設定すべき着眼点及びその設定理由，着眼点に応じて入手すべき監査証拠，証拠に基づいて確かめるべき具体的内容などが問われる問題となっています。ここで，着眼点は監査項目や監査目標(必要なコントロールの裏返し，広めの監査要点)，設定理由はコントロールが必要なリスク，監査証拠に基づいて確かめるべき具体的内容は詳細な監査要点を含めた監査手続と考えれば，従来通りの設問内容とみなすことができ，「リスク→コントロール→監査手続」というシステム監査の基本的な流れを意識できる論述構成が可能となります。本問は，設問アで「情報システムの改変の内容」が求められているように，情報システムの改変ありきの問題であり，改変に伴う障害管理態勢を書く必要があります。そして，問題文中に「障害に対する基本方針，体制，訓練，見直しなどのシステム障害管理態勢の構築」,「実効性のあるシステム障害管理態勢が構築されているかどうか」とあることや前述した点も含め，“実効性”がキーワードとなり，それを確保するための障害管理マネジメントにおける PDCA サイクルの監査という側面もあることを意識する必要があります。出題テーマとしては，障害管理というオーソドックスなものなので，受験者にとっては問 1 よりも選択しやすく論述しやすいのですが，以上のような洞察を踏まえると，難易度は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	情報システムの個別監査計画と監査手続について	C
2	システム障害管理態勢に関する監査について	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。特に，平成30年に改訂された『システム監査基準』及び『システム管理基準』の両基準内容からの新作問題に備えておく必要があります。例えば，改訂基準で重視されるITガバナンスに関する内容は，最近連続して出題されているので，注意が必要です。ストラテジ系の出題に対しては，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」のほか，ITストラテジスト試験で出題済みの経営戦略策定のフレームワーク(PEST 分析，ファイブフォース分析，バリューチェーン分析[今回出題された]，VRIO分析，3C分析，SWOT分析など)，「法務」分野では，「著作権法」「特許法」「労働者派遣法」「個人情報保護法」「請負契約の法務」「下請代金支払遅延等防止法」などが挙げられます。また，今回出題された『財務報告に係る内部統制の評価及び監査に関する実施基準(令和元年改訂)』に基づく，「自動化されたITに係る業務処理統制(ITAC)の運用状況の評価」など，最近，改訂・改正された法律・基準類には留意しておく必要があります。特に，昨年から今年にかけて改正された未出題の関連法律として，「電子帳簿保存法」「個人情報保護法」「著作権法」「プロバイダ責任制限法」などがあり，これらの改正ポイントを把握しておくとよいでしょう。

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。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い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習得しておくとよいでしょう。特に，「セキュリティ」分野では，難易度レベルがレベル 4 からも出題されるようになり，情報処理安全確保支援士(SC)の午前Ⅱ過去問の学習なども視野に入れる意味が十分出てきました。

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。しかし，セキュリティ監査が大枠テーマの出題が長く途絶え，今回ようやく個人情報保護法の改正ポイントと絡めて出題されました。また，最近盛んに出題される傾向にあった，DX 推進のための基盤となる RPA，AI，IoT などの技術に絡む出題にも引き続き備えておく必要があります。AI 技術に関しては，監査対象が AI システムという場面だけでなく，AI を活用した監査という視点も取り上げられる可能性があります。なお，RPA や AI などの新技術を導入したシステムを念頭においた次世代監査に関する資料として，2019 年に『次世代の監査への展望と課題』が日本公認会計士協会から公表されており参考になります。

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。そのほか，注目度の高いテーマとしては，テレワーク環境の構築・運用のセキュリティに関する問題が挙げられます。IPA による「情報セキュリティ 10 大脅威」の組織部門で「テレワーク等のニューノーマルな働き方を狙った攻撃」が昨年からランクインし，テレワーク推進下での組織のセキュリティガバナンス・コンプライアンスの低下や，関連ルールの整備や運用を支えるマネジメント力の低下が指摘されています。また，「デジタル改革関連法」による「押印・書面の交付等を求める手続きの見直し」や脱印鑑の潮流から，今回出題されたワークフローシステムや電子署名システムで実現されるような承認業務の電子化などのテーマも引き続き扱われる可能性があります。個々の問題テーマについては，公的機関や民間団体から公表されている基準・ガイドライン類に目を通しておくことが有効です。基本的な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』や平成 29 年 4 月に内閣官房内閣サイバーセキュリティセンターが策定・公表した『情報セキュリティ監査実施手順の策定手引書』などが参考になります。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，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。内部不正対策に関連しては，平成 30 年の『不正競争防止法』の改正や，それを受けた経済産業省の『営業秘密管理指針』の改訂が翌年続けて行われているほか，IPA の『組織における内部不正防止ガイドライン』も個人情報保護法の改正やテレワーク環境に対応するため，今年 4 月に改訂されています。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。最近の動向としては，「政府情報システムにおけるクラウドサービスの利用に係る基本方針」において，クラウドサービスの利用をデフォルトとする「クラウド・バイ・デフォルト原則」が打ち出されたことを受けて，昨年から「政府情報システムのためのセキュリティ評価制度(ISMAP)」が開始されています。

このような評価を実施する際には，クラウドサービスに関する評価基準が重要となります。例えば，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。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)も近年発行されており，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，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 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。

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『COBIT』などのガイドラインの内容が参考になります。

AI 関連システムの監査の問題は，システム監査技術者試験のシラバス(試験における知識・技能の細目)の Ver.3.1 から Ver.4.4 で付け加わった(現在は Ver.5.0)未出題テーマであり，この類のテーマとしては，ビッグデータの監査，サイバーセキュリティ対策の監査，スマートフォンの監査，個人情報保護監査，事業継続計画・管理の監査，不正調査などが挙げられます。

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，従来どおりに，①最新のトピックに絡めた問題と，②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。今回のような，監査業務そのものに関する出題頻度については今後の出題動向から判断するしかありませんが，基本的には，数回に 1 回程度の出題割合と想定されます。

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，テレワーク環境の構築・運用・セキュリティ，ビッグデータの活用，マイナンバー制度や改正個人情報保護法，GDPR など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，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。

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。