システム監査技術者

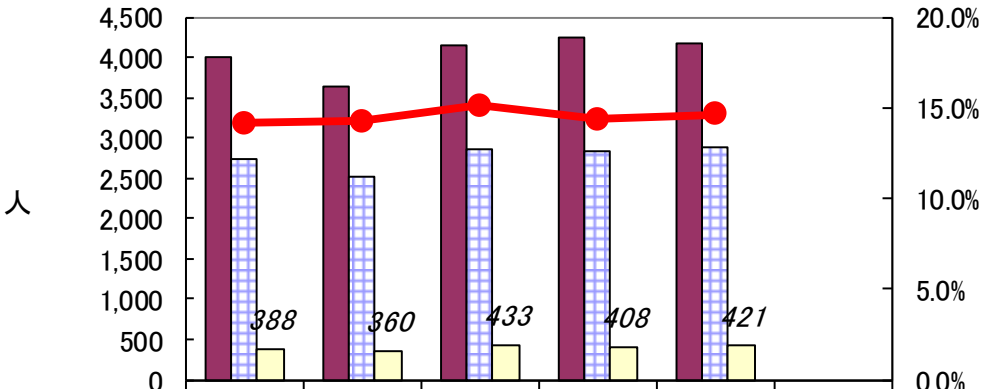
1.　はじめに

1.1　総評

今回は，『システム監査基準』及び『システム管理基準』（以下，両基準を新基準という）が平成 30 年 4 月に改訂されてから 2 回目のシステム監査技術者試験（以下，AU 試験という）でした。前回試験では，午前Ⅱ試験でこの二つの新基準の内容に基づく出題が 6 問出題され，新基準への移行が強く感じられる試験でした。今回は，新基準の内容に基づく出題はあったものの，新基準の特徴や旧基準との違いをきちんと押さえていないと解けないような問題ではなく，基準の改訂による大きな影響は感じられませんでした。また，午後試験では，総じて経営的視点が色濃く感じられる出題が多いことが特徴です。

AU 試験では，例年，世の中の動向や新技術を逸早く，積極的に取り上げる傾向が見受けられます。今回も，午後問題でデジタルトランスフォーメーション（DX）や AI を題材にした出題がありました。まさに，これからのシステム監査において重視されるであろう監査対象を扱ったテーマといえます。なお，今回は午後試験において，セキュリティ監査に分類される出題はありませんでした。

1.2　受験者数の推移



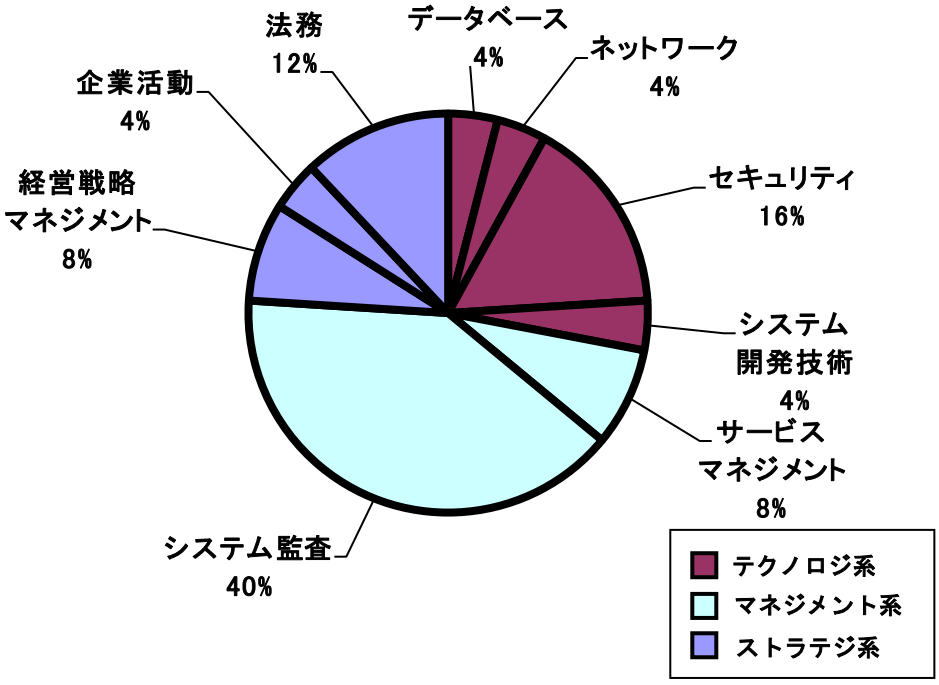
	H27春	H28春	H29春	H30春	H31春	R2
応募者数	4,012	3,635	4,151	4,253	4,175	
受験者数	2,740	2,524	2,862	2,841	2,879	
合格者数	388	360	433	408	421	
合格率	14.2%	14.3%	15.1%	14.4%	14.6%	

2.　午前Ⅱ問題の分析

2.1　問題テーマの特徴

今回の午前Ⅱ試験で特に注目していたのは，新基準からの出題数と，「セキュリティ」分野の出題数や難易度の変化の 2 点です。前者は，今回が新基準に移行してから 2 回目の試験であること，後者は，出題範囲の改訂によって今回から「セキュリティ」が重点分野に加わり，難易度のレベルも最も高度なレベルの出題が想定される「レベル 4」に上がったことからです。新基準からの出題数は 3 問で，前回の半分でした。出題内容も新基準ならではの特徴的なものではなく，基準の改訂に関する詳細な知識は要求されませんでした。

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



「セキュリティ」分野の出題数や難易度の変化に関しては，当分野からの出題は例年 3 問であったものが，今回は 1 問増えて 4 問になりました。情報処理安全確保支援士(SC)試験の過去問からの出題もありましたが，高度な技術的知識を問う出題は少なく，セキュリティに関する機関やフレームワークなど，セキュリティ政策の動向が取り上げられたのが特徴的です。よって，今回から「セキュリティ」分野が重視され，出題数は増えたものの，技術的な難易度は高くなかったといえます。なお，「セキュリティ」の 1 問増加により，「システム開発技術」からの出題が 2 問から 1 問に減りました。

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。過去問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練習で十分に対応できる問題といえます。他区分の過去問題が問題の後半に多く出題されていたので，後半は見慣れない問題が多く，難しく感じられがちかも知れませんが，この傾向は例年通りですので，午前Ⅱ試験の全体的な難易度は標準的といえます。

そのテーマが主題として扱われたという意味での新規出題としては，“SLA を作成する際の検討順序”，“職務発明に基づく特許の取扱い（特許法)”，“公開鍵基盤における CPS(認証局運用規程)”，昨年策定・公表された“サイバー・フィジカル・セキュリティ対策フレームワーク”，“VRIO 分析”などがありました。なお，今回の「コンピテンシモデル」「VRIO 分析」「SCM」など，企業活動や経営戦略マネジメント分野では IT ストラテジスト試験由来(最初にこの試験区分の午前Ⅱ問題で扱われた[解答選択肢含む]という意味)の過去問の内容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ごく僅かだけであることから判断して，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。特に，「システム監査」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の高い問題は約半数強です。そのような新規問題は，知らないと手も足も出ない問題が多く，午前試験が午後試験採点のための選別試験であることを改めて認識されられます。また，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，このような趣旨で法律の重要・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場合，問題の難易度が高めになりがちです。

2.3　問題テーマ難易度一覧表

問	テーマ	難易度
1	統計的サンプリング	B
2	システム監査基準：システム監査の品質	B
3	試査	B
4	ペネトレーションテストが適合するチェックポイント	A
5	内部統制監査におけるリスクアプローチ	B
6	システム監査基準：予備調査	B
7	システム監査基準：改善提案のフォローアップ	A
8	RFP によるベンダ選定手続の監査の指摘事項	B
9	データベースの直接修正に関する指摘事項	B
10	内部統制監査の実施基準：業務処理統制	A
11	SLA を作成する際に検討する順序	C
12	DA と DBA を別々に任命した場合の DA の役割	A
13	フェアユース	B
14	特許法：職務発明の取扱い	C
15	アーヴィング・ジャニスによる“心の警備”	B
16	コンピテンシモデル	B
17	AES の特徴	C
18	サイバーセキュリティ基本法に基づく NISC	B
19	公開鍵基盤における CPS	C
20	サイバー・フィジカル・セキュリティ対策フレームワーク	C
21	ビューを利用する目的	A
22	ブロードキャストストーム	C
23	教育効果の測定　カークパトリックモデルの 4 段階評価	C
24	VRIO 分析	B
25	SCM	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

出題分野の特徴は，経営構想の監査（DX 推進），システム監査業務そのもの（システム監査計画），システムの有効性の監査（IT ガバナンス），という異なる分野の問題テーマでしたが,3 問とも経営戦略･情報戦略といった経営的視点からの出題だったことです。そして，扱われた事例のベースとして，デジタルトランスフォーメーション（DX）の推進や AI システム・AI 技術への対応などの最近の話題が取り上げられているほか，改訂された『システム管理基準』で改めて位置付けが明確化された IT ガバナンスの実践が取り上げられていることも注目されます。DX の推進については，今期の他区分（PM）試験でも取り上げられており，一昨年末に経済産業省が策定・公表した『DX 推進ガイドライン』を意識したトピック的な出題ともいえます。

全体的に，監査における評価の視点からは，戦略性や有効性の観点から問われる設問が多く，その意味では設問視点が偏っている感じは否めませんが，リスクや監査ポイント，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。特に今回は，監査手続を問う設問が多いことが目立ちます。

今回は 3 問とも，問題文と設問文で丁度 4 ページにまとめられ，1 問当たりの解答数も 5 つから 6 つに揃えられており，問題文の量や解答量に差はありませんでした。その意味では，問題文の読解や解答作成上の時間配分が楽な問題構成であったといえます。ただし，各設問で問われる解答ポイントのレベル（どこまで具体的に書くか）を判断し難いものも少なからず見受けられ，まとめ方・表現方法に迷う場面が想定されます。そのため，解答表現がバラけやすく，同じ解答ポイントが含まれている解答であっても，一見すると別物と判定されかねない状況が生まれやすいと考えられます。したがって，時間的・知識的な難しさはあまり感じ難く，「解答欄をすべて埋められて簡単だった」と思いがちですが，設問当たりの配点が大きいことも加わり，実際にはあまり得点できなかったという状況が生じかねません。そのため，表面的には，標準的な難易度の出題ばかりに思えても，実際の難易度はやや高めの出題と評価したほうが妥当と考えられます。

3.2 各問題のテーマ，特徴

問 1 は，DX 推進のための中長期経営計画における“デジタル経営構想”の推進状況の監査を題材とした，情報システム戦略やプロジェクト管理の監査をテーマとした問題です。PoC（Proof of Concept：概念実証，プロジェクト全体を新しく作り上げる前に実施する仮説の立案とその検証工程）やチャットボットなどの AI 技術の活用が取り上げられており，AI 技術導入時のリスク（PoC の結果が活かせない問題）を意識した設問なども含まれています。全体的に，問題文の条件から解答ポイントが推測できる設問で占められているといえますが，解答のまとめ方・表現に迷う設問もいくつかあり，難易度はやや高めの問題といえます。なお,AU 試験の午後Ⅰ問題では問題文中に会話文が含まれる出題形式は珍しく，

平成 30 年の試験で初めて登場し，今回試験で 2 回目となります。

問 2 は，監査対象をあまり明確に意識しなければならない問題ではなく，システム監査計画という切り口からの監査業務に関する問題です。監査業務そのものが問題テーマとなる午後Ⅰ問題の出題は珍しく，中長期計画，年度計画，個別監査計画の順に監査計画を落とし込む流れの事例が扱われています。この問題でも，前問と同様に，チャットボットなどの AI 技術の活用が取り上げられており，それに絡ませた監査要員の教育に関する設問などが設定されています。そのほか，監査対象の選定や監査用ソフトウェアの活用による監査業務の効率化などの設問で構成されており，解答ポイントの絞り込みや解答のまとめ方に迷うケースが想定されます。しかし，全体的には，標準的な難易度の問題といえます。

問 3 は，“システム有効性の監査”と題された，IT 投資計画に関する IT ガバナンスの監査の問題で，平成 30 年の『システム管理基準』で改めて定義された IT ガバナンスの実践が取り上げられており，新基準を意識した出題といえます。IT ガバナンスが大枠としてあるので，経営陣によるマネジメント・プロセスの評価・指示・モニタリングが求められることを意識しなければならない設問も含まれています。また，解答ポイントのレベルを判断し難い設問もあり，難易度はやや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	デジタルトランスフォーメーション推進プロジェクトの監査	C
2	システム監査計画	B
3	システムの有効性の監査	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

出題分野としては，最近何かと話題のAIシステムを対象とした企画・開発・運用業務の監査と，IT組織の役割・責任の変更を題材にしたITガバナンス・人的資源管理の監査の分野からの出題でした。

昨今，AI技術を利用したシステムの導入事例が増してきており，そのようなAIシステムの企画・開発・運用・保守におけるリスクを踏まえたAIシステムに対するシステム監査の実施が求められる機会がより多くなってきています。AI システムの監査の規範といえるような公的な基準がある訳ではありませんが，AI 関連の報告書やガイドラインは公的機関から公表されており，参考にできます。今回の出題もそのような標準的なAIシステム開発の枠組みを前提とした問題構成となっています。例えば，一昨年に公表された『AI・データ契約ガイドライン（経済産業省）』や昨年に公表された『AI利活用ガイドライン（総務省）』などが挙げられます。このような動向を踏まえると，AI システムの監査の問題はトピック的な出題といえます。

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AIシステムに関する監査の問題（問1）が①に相当し，IT組織の役割・責任に関する監査の問題（問2）が②に相当する出題と見なせますが，②についても，AIやIoTなどの新技術の導入を意識した出題となっていることが特徴です。

問1は論述対象がAIシステムに限定されており，携わった経験のない受験者の方は敬遠されたのではないかと思われます。それに対して，問2はIT組織に関する問題であり，どこのIT部門でも直面している課題内容なので，身近な問題として比較的取り組みやい題材であったと思われます。

論述内容については，両問ともに，状況の変化，リスク，コントロールに対する監査手続といった標準的な論点が求められており，論述構成の観点からは取り組みやすい設問構成となっています。

まとめると，今回の午後Ⅱ試験は，問 1 は題材が限定されて選択し難く難易度が高めの問題で，問2は題材が身近で選択しやすく書きやすい難易度が標準的な問題といえます。

4.2 各問題のテーマ，特徴

問1は，AIシステムの利用段階で想定されるリスクを踏まえて企画・開発段階で実施すべき監査手続が問われる内容となっています。AI システム開発に関するリスクとして，アルゴリズムの不透明化のリスク，収集データの十分性や網羅性のリスク，成果物（学習済みモデル）の機能・性能などの品質リスク，開発手法に起因する要求・完了条件・成果物などの不明確化リスク，収集データの加工（学習用データセット生成）のためのコスト・

工数リスク，成果物・派生データの権利帰属・利用条件設定のリスクや責任分配のリスクなどに関するヒントが問題文中に具体的に例示されており，論述しやすくなるような配慮はなされていますが，実際に具体的な論述をするためには，相応の知識や経験が求められる内容になっています。その意味で，難易度は高めの問題と評価できます。

問2は，クラウドサービスの利用拡大やAI・IoT等の新技術導入といったIT環境に対応するためのIT組織の役割・責任の変更に伴うリスクを踏まえて，対応策(コントロール)やその監査手続が問われる内容となっています。企業のIT部門の役割・責任は，旧来のシステム開発から，システムの管理，そしてシステムの企画・戦略立案へと重心が移ってきました。つまり，より経営的な視点が求められる立場に変わってきています。特に，DX推進が叫ばれる昨今では，企業が経営戦略を実現するためには最新のIT技術を活用することが不可欠となっており，IT部門はそれを推進するうえで中心的な役割・責任を担うことが求められています。そのような役割・責任を果たすためには，自社の業務内容やその課題に対する理解，最新のIT技術を活用・評価するための知識，経営陣・利用部門・委託先と合意形成するステークホルダマネジメントといった知識・経験に基づくスキルが求められます。

IT組織の役割・責任が変更されると，要員に求められるスキル構成も変わるため，求める人材像を明確にしたうえで，要員の育成（教育，訓練，キャリアパス確立等）や新規要員の採用などの対応策を講じる必要があります（このような内容は，今回の午後Ⅰの問1でも扱われていました)。このような対応策（コントロール）を挙げることや，その取組状況(整備・運用状況)を確かめるための監査手続が求められる内容になっており，論じやすい内容なので，難易度は標準的な問題と評価できます。

4.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	AI技術を利用したシステムの企画・開発に関する監査について	C
2	IT組織の役割・責任に関するシステム監査について	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，新基準の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，今回は過去問の再出題でしたが，リスクアプローチや監査リスクモデルに関する問題などが挙げられます。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 ストラテジストで重視される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」「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「特許法」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」など，最近改正された法律・基準類には留意しておく必要があります。

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，今回試験から，重点分野に加わり，難易度レベルも最も高度なレベル 4 からの出題が可能となったことから，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従来よりも増してきました。

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，昨年からの出題傾向は，セキュリティ監査が大枠テーマの出題はなく，RPA，AI，DX など，DX 推進関連のトピック的な出題が顕著になっています。これは，DX の実現やその基盤となる IT システムの構築を実現するうえで経営者が押さえるべき事項を明確にした『デジタルトランスフォーメーションを推進するためのガイドライン（DX 推進ガイドライン)』が平成 30 年 12 月に経済産業省から公表された契機によるものと考えられますが，今後も引き続き DX 推進のための基盤となる RPA，AI，IoT などの技術に絡む問題は出題される可能性は高いと考えられます。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。

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，今回試験でも問 2 での監査対象となったマイナンバーを含む個人情報を扱う顧客管理システムなど，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，今期の他区分（SC）でも出題された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。さらに，脱印鑑の流れも加わり，申請・承認業務や紙文書の電子化などのテーマも今後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，クラウドセキュリティ監査などが挙げられます。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，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』や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及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。

今回出題された午後Ⅰ試験の DX の監査や AI 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.4.6)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，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，事業継続計画（BCP）に関する題材が挙げられます。テレワークや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）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。