システム監査技術者

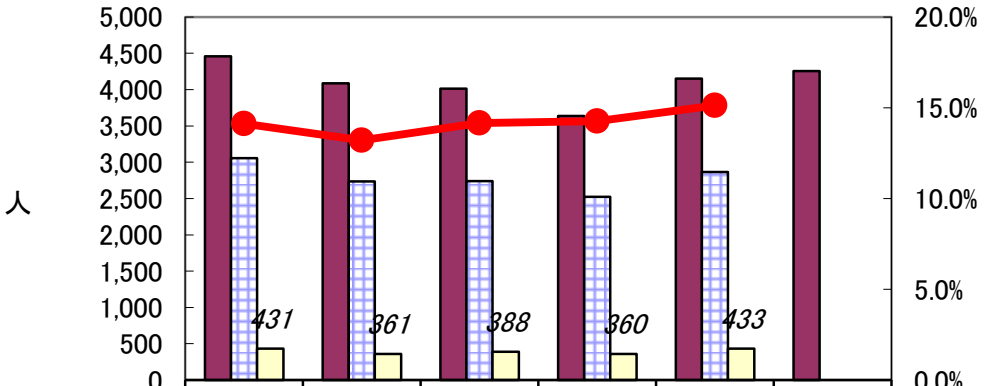
1.　はじめに

1.1　総評

今回は，情報戦略からシステムの企画・開発といったシステムライフサイクルに関する監査をテーマとする問題が多い試験でした。これらは基本となる出題テーマですが，ステージゲート手法による投資対効果検証やアジャイル型開発など，比較的ピンポイントなテーマ内容も扱われています。ステージゲート手法による開発とアジャイル開発手法は対照的な性格を持つものなので，両題材の同時出題によってバランスが取られている感じもします。また，前回はセキュリティ分野に大きく偏った出題でしたが，その反動からか，午後問題ではこの分野からの出題は皆無でした。また，午後Ⅰでは，業務処理統制が前回，今回と連続して出題され再び定番化したことなどが，気になる出題変動として挙げられます。午後Ⅱ問題については，今年4月20日に改訂された『システム監査基準』及び『システム管理基準』の改訂ポイントを先取りした内容が出題テーマとなったことが特徴です。

午前Ⅱ問題の難易度は標準的といえます。新規の出題といえるものは僅かですが，同区分からの過去問出題が少なく，他区分からの過去問出題や古い題材の出題によって，一見すると過去問出題が少ない印象を受ける内容でした。また，午後Ⅰ問題は，ピンポイント的な難しさはあるものの，解読しやすい問題構成で標準的な難易度の問題でした。午後Ⅱ問題は，論述テーマが比較的限定された出題のため，難易度が高めの試験となっています。

1.2　受験者数の推移



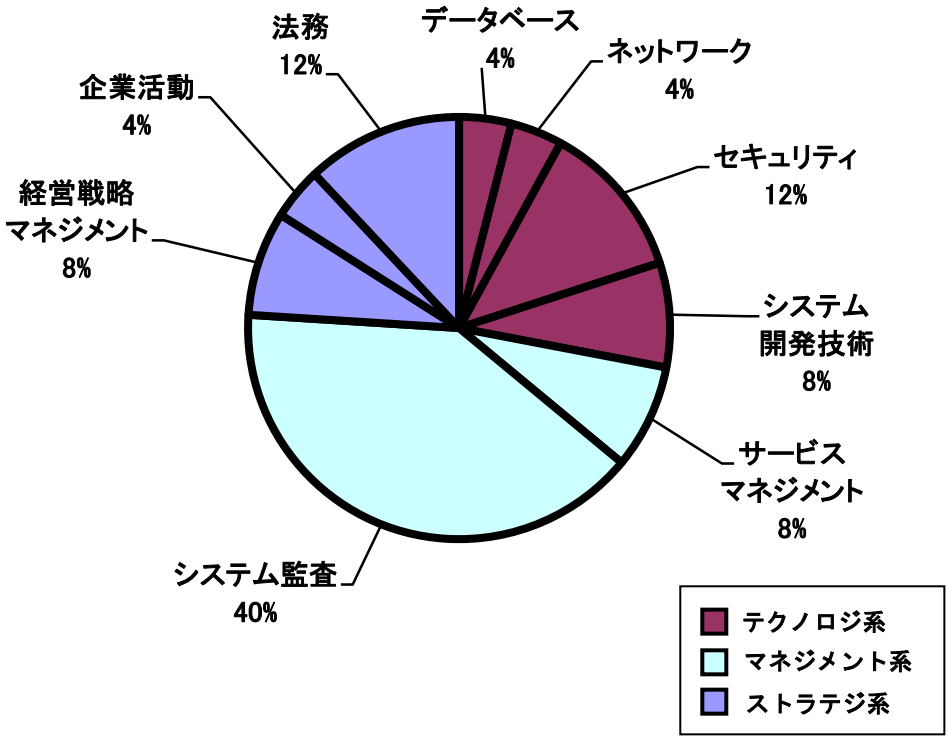
	H25春	H26春	H27春	H28春	H29春	H30春
応募者数	4,459	4,087	4,012	3,635	4,151	4,253
受験者数	3,053	2,733	2,740	2,524	2,862	
合格者数	431	361	388	360	433	
合格率	14.1%	13.2%	14.2%	14.3%	15.1%	

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，同区分からの過去問出題が少ないという点で従来とは少し異なったものとなりました。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，最近の試験では,「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,10 問と 3 問に配分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



過去問題やその焼直しとみなせる出題がほとんどですが，今回は同区分からの過去問題の出題といえる問題が 2〜3 問程度しかありませんでした。最近，同区分からの過去問題の出題が多すぎる出題傾向が続いたので，その反動といえるかもしれません。

また，かなり過去に他区分で扱われた“サービスプロフィットチェーン”や“CE マーク”などの題材が焼き直されて新規出題されている点が目立ちます。そのほかの新規出題については，全体的な印象とは裏腹に特筆すべき題材がないことも今回の特徴です。しかし，他区分の過去問を見る機会のなかった受験者にとっては，目新しく感じられる出題が多いため，「システム監査」分野以外の出題の難易度が高く感じられたかもしれません。

全体的には，過去問題やその焼直しとみなせる出題が多く，通常の午前対策の問題演習で対応可能な問題といえます。

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」の問題で，難問と感じられるものはほとんど見当たら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，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自然です。そして，その多くは出題例のある過去問やその類似問題となっています。また，新規問題といえる問題であっても，今回のように，基本的な用語の意味さえ理解できていれば，対応できる問題ばかりです。出題全体に占める過去問やその類似問題の割合は 7 割近いといってよい状況ですので，従来どおりに過去問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練習で合格可能な問題といえます。

2.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	エディットバリデーションチェック	B
2	統計的サンプリング	B
3	監査人の意見が分かれた場合の監査チームの対応	A
4	改善勧告を行うまでの間に監査人が考慮すべき事項	A
5	監査調書	A
6	システム管理基準に示されている目的	A
7	試査	A
8	システム管理基準　追補版における IT 業務処理統制	A
9	債権残高に関する異常の有無の検証方法	B
10	内部統制に関係を有する者の役割と責任	B
11	JIS Q 20000-1 の“資源の運用管理”の要求事項	C
12	データセンタにおけるコールドアイル	B
13	CE マーク	C
14	アーヴィング・ジャニスの八つの兆候の“心の警備”	C
15	製造物責任法での免責事項	B
16	投資活動によるキャッシュフロー	B
17	媒体障害の回復時にトランザクションログを用いて行う操作	B
18	ファイル転送における FTP と HTTP の違い	B
19	サイドチャネル攻撃	B
20	SAML	B
21	OP25B によって遮断される電子メール	B
22	デザインパターンの Observer パターンを利用した実現事項	C
23	共通フレーム 2013 のシステム適格性確認テスト	B
24	LBO	C
25	サービスプロフィットチェーン	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　全体の出題傾向及び難易度について

出題分野としては，情報化投資やその検証システムの有効性の監査，データ分析システムの有効性の監査，販売管理システムの業務処理統制・企画業の監査など，システムライフサイクル全般に関する監査をテーマとする問題でした。

今回の出題の特徴としては，設問レベルまで含めてセキュリティに関する出題がほとんど見受けられない点や，稼働中システムの導入目的の達成状況の監査という有効性評価の視点が監査目的として重なった点，近年出題されることが少なくなっていた業務処理統制の題材が 2 年連続で扱われた点などがまず挙げられます。特に，研究開発や事業化・商品化の管理活動として普及しているステージゲート手法が扱われた点が注目されます。本手法を用いたプロジェクト運営も注目されるようになっていることから，この問題テーマでの出題は，トピック的な出題ともいえます。また，業務処理統制の問題では，会話形態の空欄設定型の出題形式が採られていることが注目されます。他の試験区分ではこの出題形式が多用されることもありますが，システム監査技術者試験では，過去に例のない初めての出題形式でした。

全体的に監査手続に関する設問が多いため，解答記述量が多めの印象となっていますが，難易度は例年と大きく変わりません。ただし，各問ともに，少なくとも一つは，解答ポイントの選択やまとめ方に迷う設問が含まれており，その判断で時間を浪費するという意味で，ピンポイント的な難しさは感じられる出題といえます。

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。

3.2　各問題のテーマ，特徴

問 1 は，ステージゲート手法システムの投資対効果の検証制度を題材とした，情報化投資やその検証システムの有効性の監査をテーマとした問題で，主にシステム開発プロジェクト全般の監査に関する問題といえます。

“ステージゲート手法”になじみのない受験者の方にとっては，選択し難い問題といえますが，ウォータフォール型開発における各フェーズのレビュー判定に相当するゲート審査での意思決定が，厳格にトップダウンで行える体制となっていると考えればよいだけで，特に“ステージゲート手法”ならではの知識や視点が問われている問題ではありません。むしろ，問題文での費用項目のまとめ方の解釈や監査要点での現状事項と予定事項の切分けなどの点で，解答ポイントの絞り込みに迷うケースが想定される問題です。その意味から，難易度は高めの問題といえます。

問 2 は，社内の各種活動のためのデータ分析システムを題材とした有効性の監査をテーマとした問題で，主に障害管理などのシステム運用業務の監査に関する問題といえます。

本問では，障害管理での可用性の視点や個人情報に関わるコンプライアンスなど，今回の午後試験で唯一，セキュリティの視点ともいえる設問が僅かに含まれています。

設問レベルでは，主に運用におけるリスクとコントロールを答えさせる問題であり，難易度としては標準的な問題といえます。しかし，通常の災害対策や耐障害性確保の目的ではなく，負荷分散の目的でレプリケーションサーバを構築する点や，問題文中の運用上のリスクの視点が絞り込み難い点などから，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る問題です。その意味から，難易度はやや高めの問題といえます。

問 3 は，EDI 発注機能を持つ販売管理システムの開発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，要件定義段階でのシステム開発業務の監査の側面もある問題といえます。

販売管理に関するコントロールはよくある一般的なものであり，全体的には解答しやすい問題といえますが，問題文表現の解釈に迷うことで，解答の方向性が見極めにくい設問も一部に含まれています。全体的には，標準的な難易度の問題といえます。

3.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	システムの投資対効果の検証制度を対象とした監査	C
2	データ分析システムの監査	C
3	販売管理システムの監査	B

注）難易度は 3 段階評価で，C が難，A が易を意味する。

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，非ウォータフォール型開発手法として一般的になってきたアジャイル型開発手法を題材とした開発業務(開発手順)の監査と，財務諸表監査では一般的であるリスクアプローチに基づいたシステム監査計画の策定を題材とした監査業務自体の分野からの出題でした。

システム監査業務自体の基本問題がテーマとして出題されたのは久しぶりで，平成 26 年に午後Ⅱ問題の出題数が 3 問から 2 問に変更されてからは初めての出題となります。出題数が 3 問であった時代には，システム監査業務自体の基本問題が 1 問含まれるケースがよく見受けられましたが，出題数が 2 問となってからは，全く出題されなくなっていました。また，アジャイル型開発手法を題材とした午後問題も，平成 25 年に午後Ⅰで出題されて以来の扱いとなります。その頃とは異なり，アジャイル型開発に関わる機会も格段に増えてきていることとは思われますが，問題テーマとしては『システム監査基準』及び『システム管理基準』の改訂内容を先取りしたトピック的なものと受け取れます。

今回は例年と異なり，これまで見られなかった論点で，しかもやや大きな視点からの問題テーマばかりの出題であることから，問題選択に困った受験者の方も多かったと思われます。出題テーマに準じた経験を全く持たない受験者の方にとっては，取り組み難い問題テーマばかりであり，その意味では，難易度は高かったといえます。また，昨年が両問ともにセキュリティ監査の分野のみからの出題でしたので，問題・設問レベルのテーマともに，セキュリティを扱う部分はありませんでした。

4.2 各問題のテーマ，特徴

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，問 2 の両問ともに，前記①に分類できる問題といえます。問 2 は，かつて出題数が 3 問であった時代に出題されていた，システム監査業務自体に関する基本問題に該当するものが一時的に復活したとみるよりは，『システム監査基準』及び『システム管理基準』の改訂内容を反映した出題とみるべきでしょう。問 1 についても，両基準が“アジャイル開発手法”への対応を考慮した内容となっている点を反映したものといえます。

問 1 は，アジャイル型開発におけるリスクやその手法による開発を進める上での体制・スキル・開発環境などに関するコントロール，それらに対する監査手続などを問う問題です。論述内容については，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いるので，解答しやすい形態となっていますが，アジャイル型開発ならではの特徴，例えば，ペアプログラミング，継続的なデプロイ，テスト駆動といった手法や，進捗管理，見積り，要員などのリスクに関する知識がないと扱い難く，難易度が高めの問

題テーマといえます。もっとも，問題文にはヒントや例示があることで，問 2 よりは選択しやすい問題です。ちなみに，今回の TAC 模試「問 1　短期開発プロジェクト～」は，アジャイル型開発を論述対象の一つとしています(解説の論述例の一つはアジャイル)ので，模試をアジャイル開発で書いていれば本番でも対応できたことと思われます。

問 2 は，いわゆるリスクアプローチに基づく監査の問題であり，システム系の受験者の方には，なじみのない方も多かったことと思われます。財務諸表監査・会計監査では一般的ですが，システム監査ではこれまで題材に挙げられる機会があまりなかった問題テーマです。ただ，システム監査技術者試験のシラバスでは，“リスクアプローチによって中長期監査計画や基本計画を策定する能力”への要求が明示されており，既出の財務諸表に係る内部統制監査の路線をシステム監査でも踏襲しようとする流れも不自然なものではありません。また，新システム監査基準においても，【基準 7】として，“リスクの評価に基づく監査計画の策定”について明示されることになりました。

本問は，個別の監査案件ではなく，年度監査計画の策定における監査対象の選定や監査目的の設定であることから，上位の視点が求められているところが特徴で，この視点で準備しているような受験者の方はまずいなかったと考えられます。設問の要求事項についても，リスクアプローチによる監査対象選定や監査目的設定の手順や留意点，利点，問題点，必要な措置など，変則的な設問構成となっています。それらに関連する問題文中の例示も少なく具体性に欠けるので，出題意図に沿った論述をするのは難しいと考えられます。このように，論述テーマの狭さや変則的な出題形式という面から，難易度は高いといえます。

4.3　問題テーマ難易度一覧表

問	テーマ	難易度
1	アジャイル型開発に関するシステム監査	C
2	リスク評価の結果を利用したシステム監査計画の策定	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。特に，今年改訂された『システム監査基準』及び『システム管理基準』からの出題は，今後増えることが予想されます。例えば，リスクアプローチや監査リスクモデルに関する問題やITガバナンスにおけるEDMモデルの問題などがまず挙げられます。

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」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「製造物責任法(PL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。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。

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，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 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，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。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，今年改訂された『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。

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，今回の出題のように変則的なケースも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，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。