システム監査技術者

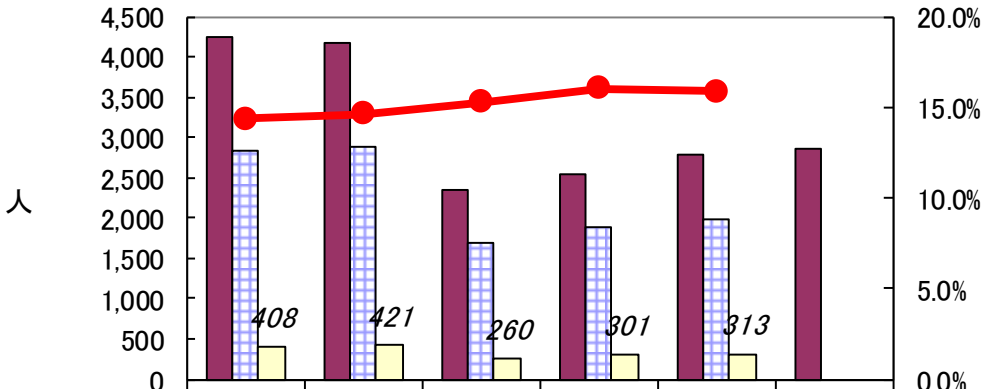
1.　はじめに

1.1　総評

システム監査基準やシステム管理基準，財務報告に係る内部統制基準類が本年改訂され，次回からいずれも新基準に基づく試験が実施されます。今回は，これらの現行基準下で実施される最後の試験となり，午前Ⅱ試験での基準類の扱われ方が注目されましたが，過去問が再出題されただけでした。今回の午後問題では，キャッシュレス化推進，DX 推進，クラウドサービス利活用の推進といった政府政策に深くかかわるような時宜を得た内容の問題が目立ちました。具体的には，クレジットカード情報の保護やローコード／ノーコード開発，ビッグデータの利活用，サイバーセキュリティといった出題テーマの問題です。

午前Ⅱ試験では，定番のシステム監査の基本業務や内部統制に関する知識はもちろんのこと，従来どおり，新しい法制度に関する知識も問われました。午後Ⅰ試験では，セキュリティの監査，企画・開発業務の監査，業務処理統制の監査といった出題分野のバランスがとれた問題構成となっており，しかも，最近の IT 技術を採用した題材が扱われています。 午後Ⅱ試験では，最近続いていたシステム監査業務自体に関する問題は出題されず，従来どおりのトピック的なテーマの問題が出題されました。2 問とも，経営陣が積極的に関与し，組織横断的な連携が求められる課題に関する内容であり，IT ガバナンスの枠組みや全体最適化という視点からの評価が求められるもので，難易度が高い問題といえます。

1.2　受験者数の推移



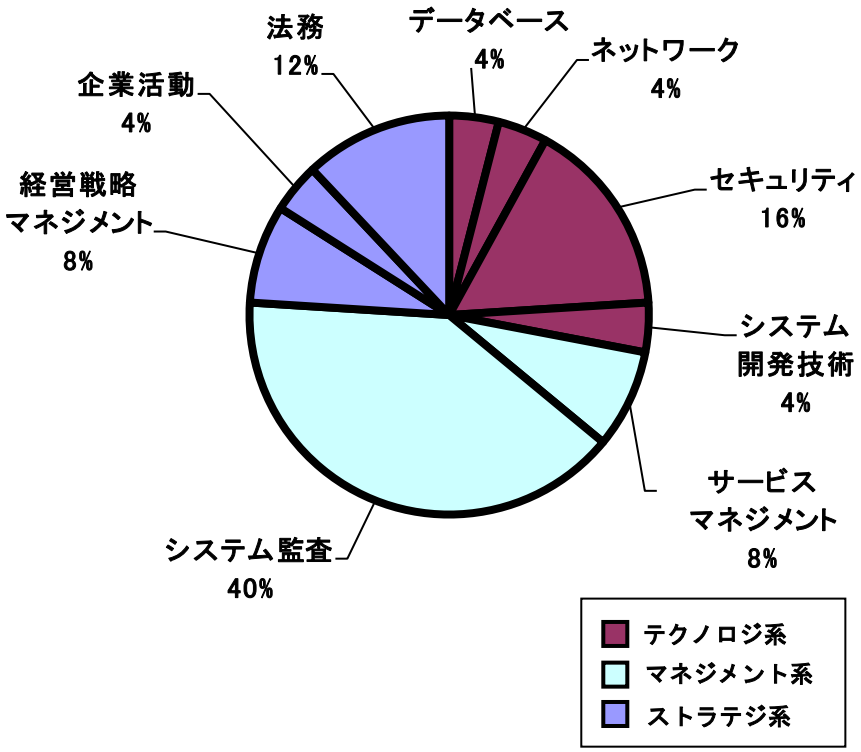
	H30春	H31春	R2 10月	R3秋	R4秋	R5秋
応募者数	4,253	4,175	2,350	2,552	2,792	2,851
受験者数	2,841	2,879	1,702	1,877	1,972	
合格者数	408	421	260	301	313	
合格率	14.4%	14.6%	15.3%	16.0%	15.9%	

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。今回は定番の『システム監査基準』『システム管理基準』『財務報告に係る内部統制の評価及び監査』に関する基準類からの出題が少なく，『システム監査基準(平成 30 年)』からの過去問題は 3 問のみの出題でした。これは，前述のとおり，旧基準下での出題が今回の試験で最後になるためと考えられます。

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,“AI システムが読み込む画像などの学習データの管理を対象としたシステム監査”の問題,“政府情報システムのためのセキュリティ評価制度(ISMAP)標準監査手続き”における監査対象期間に関する問題,“特定デジタルプラットフォームの透明性及び公正性の向上に関する法律(透明化法)”における特定デジタルプラットフォーム提供者に関する問題，アサエルの購買行動類型に基づく四つの製品タイプに対する消費者行動に関する問題などがまず目につきます。これらの新規問題は，法令の制定や改正・改訂を機に出題されるものや，現在の潮流を反映したテーマが多いといえます。

ISMAP については，ISMAP 管理基準の微改訂が昨年 4 月に行われ，さらに，リスクの小さな業務・情報の処理に用いる SaaS サービスを対象にした仕組みである“ISMAP-LIU(ISMAP for Low-Impact Use)の制度が昨年 11 月から新たに運用開始されたことが出題の動機と考えられます。また，透明化法については，デジタル広告分野を新たな対象に加える政省令が昨年 8 月に施行されたことなどが，出題動機の一つになっているともいえます。その一方で，監査調書や IT 全般統制などの従来の定番テーマの問題についても，新たな切り口で出題されています。全般的には，システム監査技術者試験の過去問の再出題が多く，特に令和 3 年度や令和 2 年度からの出題が多い印象を受けます。

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，レベル 4 の「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新規出題を除けば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，定番問題への対処に慣れれば解きやすい問題といえます。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。

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，過去の出題事例や常識的な判断から正解を類推できる問題もあるため，初見でもある程度の対応は可能です。今回の出題では，ISMAP や透明化法に関する問題など，知らないと正答し難い新規問題がある反面，アサエルの購買行動類型の問題を始め，初見でも正答しやすい問題も 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ます。そのため，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，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，ISMAP の問題や，過去問からの出題ですが，民法の契約不適合責任の問題などが挙げられます。

2.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	AI 学習データの管理の監査の指摘事項	A
2	ISMAP 標準監査手続における監査対象期間	C
3	JIS Q 19011：監査プログラムの定義	C
4	システム監査基準：予備調査の作業	A
5	システム監査基準：監査の結論の形成	B
6	内部監査人が実施する監査における監査調書	A
7	システム監査基準：十分かつ適切な監査証拠	B
8	固定資産管理システムの IT に係る全般統制	B
9	債権残高に関する異常の有無の検証方法	B
10	IT に係る全般統制	B
11	SLO，KPI，CSF の検討順序	B
12	TCO が最小となる新システム開発計画	B
13	フェアユース	A
14	特定デジタルプラットフォームの透明性及び公正性の向上に関する法律	C
15	民法の契約不適合責任	C
16	SL 理論	A
17	公開鍵基盤における CPS	B
18	サイバー情報共有イニシアティブ（J-CSIP）	B
19	JIS Q 27000：リスク評価	A
20	クリプトジャッキング	B
21	UML のデータモデルを実装する際の解釈	C
22	リンクアグリゲーション	B
23	レビューの名称の組合せ	A
24	ファイブフォース分析	B
25	アサエルの購買行動類型	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，ローコード／ノーコード開発ツールを利用したアプリ開発を題材とした企画・開発業務の監査に関する問題，人材管理システムの再構築を題材にした業務処理統制の監査に関する問題です。具体的な出題内容としては，令和3年4月の割賦販売法の一部を改正する法律の施行に伴って，そのセキュリティ対策義務の実務上の指針でもある“クレジットカード・セキュリティガイドライン”への遵守の視点や，DX 推進で期待される短期開発を実現するシステム開発プロセスと親和性が高い開発基盤としてのローコード／ノーコード開発ツール利用時に想定されるリスク及びコントロールの視点，クラウドサービスを利用したシステムの再構築など，キャッシュレス化推進，DX 推進，クラウド・バイ・デフォルト原則といったクラウドサービス利活用の推進といった政府政策に沿うような時宜を得た内容の問題が目立ちました。セキュリティ監査を主題とした問題は前回に引き続き，問1として出題されており，3年ぶりの出題となった業務処理統制をテーマとした問題が目を引きます。全体的には，セキュリティ監査，システム開発プロセスの監査，業務処理統制の監査という出題分野としてのバランスのとれた内容となっています。

設問レベルでは，全体的に，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どおり満遍なく問われています。

全体的に問題文は読み取りやすく，ページ数は3問ともにほぼ4ページ，図表の数が1つから2つで，問題文の分量は少なめです。AU の午後Ⅰ試験は，小問数(解答すべき事項の数)が他区分に比べて少なめであることが特徴です。その点，前回試験では，1問当たり6つから8つと多めでしたが，今回試験では例年どおりの5つから6つでした。問題文と小問数のいずれも，量的に大差はなく，解答記述量の面でも偏りがない出題となっています。

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，カード決済を行うECサイトに求められる情報セキュリティ対策及びカード情報保護対策に関する監査をテーマとした問題です。割賦販売法の改正に伴い改訂された“クレジットカード・セキュリティガイドライン”で義務化されたカード情報の非保持化や PCI DSS 準拠などの対応に絡めた内容や，ECサイト改ざんに備えたセキュリティ対策が問われています。全体的に，解答すべきポイントは問題文中で見つけやすく，今回の出題の中では最も易しく感じられる問題でした。

問 2 は，ローコード／ノーコード開発ツールを利用したアプリ開発のリスク低減のために策定された管理ルール案の監査をテーマとした問題です。ローコード／ノーコード開発ツールによるアプリ開発とそれに応じた管理ルール案(コントロール案)が提示され，その

内容に関連するリスクや監査ポイントを見い出すことに相当する設問で構成されています。特に，開発判断基準項目の追加項目など，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設問も含まれています。また，全体的に，解答のまとめ方に迷う設問も多く，難易度は高めの出題であったといえます。

問 3 は，クラウドサービスを活用したシステム再構築がテーマとなっていますが，実際には，人材管理システムの業務処理統制の問題であり，当然の如く，大半がデータインテグリティに関する設問となっています。問題文中の状況設定に応じて，データ不整合が生じるリスクやそのコントロールについて考えさせる設問内容であり，見つけ出した解答ポイントから，さらに一歩踏み込んで解答を作成しなければならない設問が多いため，難易度は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	クレジットカード情報保護の監査	B
2	ローコード／ノーコード開発ツールを利用したシステム開発の監査	C
3	人材管理システムの監査	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 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，今回の問題は両問とも，ある特定のシステムを対象とした監査というよりも，組織全体における IT 活用の仕組みやインフラの部分の監査に当たるため，組織全体からの視点での論述が求められています。特に，問 2 については，設問イと設問ウが全く同じ形式で，監査手続を監査の着眼点(ここでは監査要点の意味)や監査証拠とともに述べなければならず，記述量や時間配分の両面で手間がかかる問題といえます。

出題分野としては，問 1 はデータ利活用基盤の構築を題材にした IT マネジメントに関する推進・管理体制の監査やビッグデータ・AI の監査の分野からの出題，問 2 はサイバーセキュリティ管理態勢を題材にした情報セキュリティマネジメントに関する推進・管理体制の監査の分野からの出題でした。最近は，システム監査業務そのものの分野からの出題が続いていましたが，今回はありませんでした。

午後Ⅱ試験の平均的な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 問といった分類になります。今回は，問 2 のサイバーセキュリティ管理態勢に関する監査の問題が②に相当します。しかし，この問題は，金融分野のサイバーセキュリティ強化に向けた取組みの一環として，『金融分野におけるサイバーセキュリティ強化に向けた取組方針(金融庁)』が昨年 2 月にアップデートされたことや，サイバー攻撃から企業を守る観点から経営者が認識する必要がある事項等をまとめた『サイバーセキュリティ経営ガイドライン(経済産業省)』が本年 3 月に改訂されたことを契機に出題されたトピック的な問題とみなすこともできます。問題文の内容も，両文書の内容を色濃く反映したものとなっています。また，前回試験の問 2 の主題である「システム障害管理態勢に関する監査」と同様に，“体制”ではなく“態勢”が使用されている点も見逃せません。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あります。さらに問題文中で例示された「PDCA サイクルの実施」は，前回試験の問 2 の問題文で暗に提示された「障害管理マネジメントにおける PDCA サイクル」に呼応した「サイバーセキュリティ対策のフレームワーク(に基づくマネジメント)における PDCA サイクル」とみなすことができます。したがって，今回試験の問 2 は，前回試験の問 2 の関連出題ともいえるものです。一方，問 1 のデータ利活用基盤の構築に関する監査の問題は，ビッグデータの活用による経営戦略策定や市場分析などを想定した問題であり，トレンドに沿った問題テーマといえます。

今回の午後Ⅱ試験は，全体的に，問題設定が単純ではなく，ある程度の規模の組織が想定

されているため，関連する実務経験がないと，具体的な論述をその場で構成するのは難しい出題といえます。さらに，問題文中に解答すべき事項についての例示が少ない，あるいは全くないものもあり，出題テーマにおける具体的な知識が論述の前提として求められる場面も多く，その意味で難易度はかなり高めといえます。

4.2　各問題のテーマ，特徴

問 1 は，データ利活用基盤の構築の目的や必要とされる理由を踏まえて，構築に際して想定されるリスクやそれに対応して組み込まれたコントロールが適切に整備されているかを確かめるための監査手続が問われる内容となっています。問題文中に提示されているリスクは，個別に収集・保存されたデータの不整合やデータ品質に関するものだけで，例示されているコントロールは，データの品質維持やデータセキュリティ確保に関するものだけなので，問題文の記述だけでは，論述すべき内容のイメージが湧きづらいものでした。欲をいえば，全体最適化の観点から，品質・価値・リスクなどの認識の統一化，コード体系やデータ粒度などの標準化，それらの実効性を担保するためのシステム間連携・人材確保・組織体制の確立など，論述展開の足掛かりになるヒントがあると論述しやすい問題でした。その意味で，実務経験がないと論述がしづらく，難易度は高めといえます。

問 2 は,外部ネットワークとの接続を前提とするビジネスやサービスでのサイバーセキュリティ管理態勢が必要となる理由を踏まえて，その管理態勢における PDCA サイクルの実施の適切性を確かめるための監査手続と，インシデント発生時を想定した管理態勢の適切性を確かめるための監査手続が問われています。設問文では，監査の着眼点，入手すべき監査証拠，監査手続によって確かめるべき内容と分けて記述するように求められてはいますが，これらをすべて記述するということは，監査手続を書いていることと実質的に同じことです。また，［設問イ］や［設問ウ］で問われている「サイバーセキュリティ管理態勢における PDCA サイクルの実施」や「インシデント発生時を想定したサイバーセキュリティ管理態勢」については，問題文中では何も触れられていません。そのため，ここでの PDCA サイクルのフレームワークとしては，JIS Q 27001 の ISMS の枠組みを想定して論述する，または，『サイバーセキュリティ経営ガイドライン(経済産業省)』で提示されているような，NIST のサイバーセキュリティフレームワークに準じて論述する，どちらも有効だと考えられます。ただし，書きやすさという点では，サイバーセキュリティに特化した後者を想定したほうが有利ですし，出題者の問題作成のベースも後者側にあると考えられます。また，インシデント管理態勢については，CSIRT の設置などの緊急時の対応体制に触れるだけでなく，前回試験の問 2 と同様に,インシデント管理マネジメントの PDCA サイクルの実施の視点(対応計画，分析，低減，改善)などに触れておかなければ，管理態勢を監査していることにならない点に注意する必要があります。したがって，［設問イ］や［設問ウ］は，問われている内容が幅広いため記述量が多くなり，試験時間内にまとめることが難しく，難易度は高い問題といえます。

4.3　問題テーマ難易度一覧表

問	テーマ	難易度
1	データ利活用基盤の構築に関するシステム監査について	C
2	サイバーセキュリティ管理態勢に関するシステム監査について	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試験は，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「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，令和5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，監査基準に新たに設けられた，倫理に関して監査人が守るべき4つの原則(誠実性，客観性，監査人としての能力及び正当な注意，秘密の保持)を明示した倫理項目に関する事項や，他の監査やモニタリング活動とシステム監査との連携に関する事項などが挙げられます。また，両基準のより具体的な内容を整備した『システム監査基準ガイドライン』及び『システム管理基準ガイドライン』にも目を通しておきましょう。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（※今回午前Ⅱ試験で出題された)，バリューチェーン分析，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，今回は出題が見送られた『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』も本年改訂され，来年から施行されることになっているので，改訂ポイントなどを押さえておく必要があります。例えば，非財務情報の可視化，3 線モデル(スリーラインズモデル)の例示，経営者による内部統制の無効化に対する内部統制などが挙げられます。また，従来どおり，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，最近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」「不正競争防止法」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。

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，試験要綱の改訂時に設定される新しい知識項目から出題される傾向は変わりませんので，

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試験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開発プロセスの監査が挙げられ，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。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，ランサムウェアや標的型攻撃への対応やテレワーク環境の構築・運用時のセキュリティといったサイバー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」が一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。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，昨年 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，一昨年から「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。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』や総務省の『クラウドサービス利用・提供における適切な設定のためのガイドライン』なども参考になります。これらのクラウドセキュリティ監査に関連する基準類は，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，今回は人材管理でしたが，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。

システム開発プロセスの監査については，承認プロセスの不備や適切性を問われることが多く，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』『システム管理基準ガイドライン』『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.6.0)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（※今回関連問題が午後Ⅱ試験で出題された），サイバーセキュリティ対策の監査（※今回午後Ⅱ試験で出題された），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，不正調査などがあり，さらに，Ver.6.0 から付け加わった IT マネジメントに関する推進・管理体制の監査，プロジェクト管理の監査，アジャイル開発の監査，ワークエンゲージメントの監査などが挙げられます。

5.3　午後Ⅱ対策

今後の午後Ⅱ試験は，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。前々回と前回のような，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。その題材としては，午前Ⅱ対策でも触れたような，3 線モデルを絡めた他の監査やモニタリング活動とシステム監査との連携に関する問題などが想定されます。

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。そのほか，午後Ⅰ対策で挙げたような，システム監査技術者試験のシラバスに追加されてきたテーマでの出題も今後想定されます。

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開発プロセスの監査，外部サービスの監査，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。

令和6年度春期の情報処理技術者試験・情報処理安全確保支援士試験の対策もTACにお任せください！

＜企業ご担当者様へ人気のおススメコースをご紹介＞

合格に必要な知識を効率よくマスターできるコンテンツ

情報処理安全確保支援士Webコース

情報処理安全確保支援士受験のためのベーシックコースです。少ない時間で効率的に学習ができるように専門知識の重要論点を集約したポイント講義（Web動画）は、20テーマ（1テーマあたり30分）を配信します。

試験対策	42,000円（10%税込）
午前Ⅰ免除	36,000円（10%税込）

充実した添削指導の午後Ⅱ対策が合格のポイント

ITストラテジストWebコース

午前・午後の試験に対応したアウトプットトレーニングで、知識の定着を図ります。講義動画（全4回、1回あたり30分）は午後Ⅰの分析と解法テクニック、論述式問題への取組み方を具体的な問題で解説します。

試験対策	54,000円（10%税込）
午前Ⅰ免除	48,000円（10%税込）

合格に必要な知識を効率よくマスターできるコンテンツ

ネットワークスペシャリストWebコース

少ない時間で効率的に学習ができるように工夫されたコースです。専門知識（午前Ⅱ）の重要論点を集約したポイント講義は、20テーマ（1テーマあたり30分）を配信します。

試験対策	42,000円（10%税込）
午前Ⅰ免除	36,000円（10%税込）

充実した添削指導の午後Ⅱ対策が合格のポイント

ITサービスマネージャWebコース

午前・午後の試験に対応したアウトプットトレーニングで、知識の定着を図ります。講義動画（全4回、1回あたり30分）は午後Ⅰの分析と解法テクニック、論述式問題への取組み方を具体的な問題で解説します。

試験対策	54,000円（10%税込）
午前Ⅰ免除	48,000円（10%税込）

充実した添削指導の午後Ⅱ対策が合格のポイント

システムアーキテクトWebコース

午前・午後の試験に対応したアウトプットトレーニングで、知識の定着を図ります。講義動画（全4回、1回あたり30分）は午後Ⅰの分析と解法テクニック、論述式問題への取組み方を具体的な問題で解説します。

試験対策	54,000円（10%税込）
午前Ⅰ免除	48,000円（10%税込）

知識の総整理を短期間で行う問題演習中心のコース

応用情報技術者 徹底演習コース

学習経験者、再受験者対象の午後試験対策コースです。午後試験の出題分野ごとに出題頻度や重要度の高いテーマを精選しました。その解法を学び、短期間で効率よく知識の総整理と得点力アップを目指します。

23,100円（10%税込）

※上記コースは2024年春試験向けコースとなります。各コース名はTAC法人向け人材教育サービス紹介サイト「TAC.biz」の当該コース紹介ページへのリンクとなっております。なお、2024年秋試験向けコースにつきましては、別途ご案内いたします（2024年春頃を予定しています）。

お問合せはこちら

TAC株式会社 法人事業部

東日本エリア：東京都千代田区神田三崎町3-2-18 | 03-5276-9802

東海・北陸エリア：名古屋市中村区則武1-1-7 NEWNO名古屋駅西8F | 052-977-1051

西日本エリア：大阪府大阪市北区中崎西3-4-12 梅田センタービル5F | 06-6371-1075