

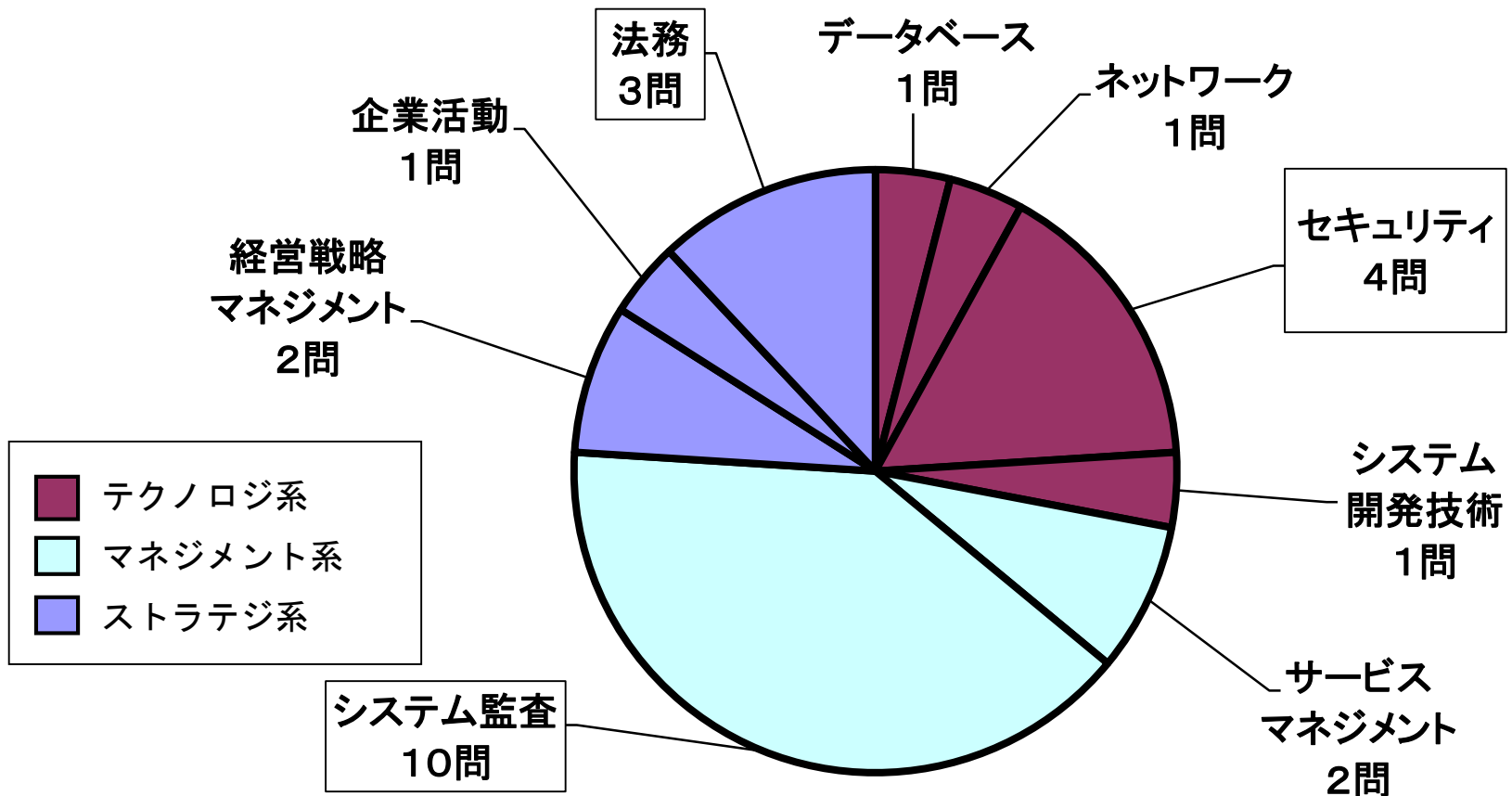
令和5年度 秋期試験 システム監査技術者(AU) 出題傾向分析

TAC株式会社



AU 午前Ⅱ 分野別出題数

- ・出題割合は変化なし。重点分野から17問



AU 午前Ⅱ 特徴と難易度

- 旧基準下での最後の試験
 - 改訂前の「システム監査基準」から3問
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基準類 が揃って改訂された
- “拠り所のある問題”が多く出題
 - 基準・規格・法律・フレームワークなどから9問
- 「セキュリティ」は管理面が中心
 - 公開鍵基盤, J-CSIP, JIS Q 27000, クリプトジャッキング
- 新作8問, 過去問題17問(うちAUから10問)
 - AUの過去問題が多く解きやすい。計算問題は1つだけ
⇒ 標準的(易しめ)

次回は新基準
から出題！

AU 午前Ⅱ 新作問題

・ 新作問題の目新しいテーマ

(監査) AI学習データの管理の監査における指摘事項

ISMAP標準監査手続における監査対象期間

JIS Q 19011: 監査プログラムの定義

(法務) 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)

(データベース) UMLのデータモデルを実装する際の解釈

(経営戦略) アサエルの購買行動類型

・ 定番テーマからの新作問題

(監査) 内部監査人が実施する監査における監査調書

ITに係る全般統制

⇒ 法令や政省令等の制定・改正を機にした出題が多い

AU 午後Ⅰ 特徴と難易度

- ・ テーマのバランスが取れた出題
 - 問1 セキュリティ監査
 - 問2 システムの企画・開発業務の監査
 - 問3 業務処理統制の監査
- ・ 政府政策に沿った、時世を反映した出題
 - キャッシュレス化推進 → クレジットカード情報保護
 - DX推進 → 開発ツールを活用した短期開発の実現
 - クラウド・バイ・デフォルト原則 → クラウドの利活用
- ・ 1問当たりの小問数は例年通り(5～6つ)
 - 配点が高い → ミスすると失点が大きい

AU 午後Ⅰ 各問題の特徴と難易度(問1)

- ・ 問1 クレジットカード情報保護の監査
 - カード業界の基準やガイドラインへの準拠
 - 店舗側のカード情報の非保持化の実現
- ※「EC店舗がカード情報を持たないから安心」ではない！
- 過去の情報の管理は？
- 外部委託先(決済代行業者)のセキュリティは？
- ECサイトへの攻撃への対策は？
- ・ 侵入防御システムの導入 → 誤検知への対応
 - ・ Web改ざん検知システムの導入 → 監視対象の選定
- 内容をイメージしやすく, 3問中最も解きやすい。

⇒ 標準的

AU 午後Ⅰ 各問題の特徴と難易度(問2)

- ・ 問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
 - － 利用部門が主体のアプリ開発
 - ・ 開発ツールの利用(短期開発, 開発コスト削減)
 - ・ 「管理ルール案」の適切性の監査
 - － 監査の観点
 - ・ テストやドキュメント作成によってコスト・期間が増大?
 - ・ アプリ開発の開発判断基準の検討
 - ・ システム部が利用している開発標準を流用できるか
 - ・ 設計ドキュメントの適切性(後任者が保守できるか?)
 - ・ 操作ログの改ざん・消去対策
 - － 出題意図をつかみづらい設問あり ⇒ 難しい

AU 午後Ⅰ 各問題の特徴と難易度(問3)

- ・ 問3 人材管理システムの監査
 - クラウドサービスを利用した人材管理システムの再構築
 - 監査の観点(データインテグリティ中心)
 - ・ 人事情報の閲覧権限が適時に更新されない問題
(セキュリティ面／業務遂行面)
 - ・ 受講歴の情報の網羅性の確保
 - ・ 検索性(新資格のマスタ登録, 名称統一)
 - ・ 虚偽の情報入力(自身の評価を上げるため)
 - ・ 新たに発生した作業負荷を加味した効果の算定
 - 解答ポイントから一步踏み込んだ解答が求められる

⇒ 難しい

AU 午後Ⅱ 特徴と難易度

- ・ 定番の出題形式の応用形
 - 組織全体におけるIT活用の仕組みやインフラ部分の監査
 - 「リスクーコントロールー監査手続」の変形
 - ・ 問1 コントロールが問われていない
 - ・ 問2 コントロールの代わりに「監査の着眼点」
「監査の着眼点」と「監査手続」×2（設問イ, ウ）
- ・ 論述すべき観点が多く、時間が足りないおそれあり
 - ・ 問1 ビッグデータレベルの大規模なデータ利活用基盤
 - ・ 問2 ①セキュリティ管理態勢のPDCAサイクルの適切性
②インシデント発生時の管理態勢の適切性
の両方の監査を述べる

AU 午後Ⅱ 各問題の特徴と難易度(問1)

・ 問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

コントロールが
問われていない

設問ア: データ利活用基盤の構築の概要, 目的,
その基盤が必要となる理由

設問イ: データ利活用基盤の構築に際して,
システム監査人はどのようなリスクを想定すべきか

設問ウ: データ利活用基盤が適切に構築されているかどうか
を確かめるための監査手続

かなり大がかりな基盤

- ビッグデータ活用による経営戦略策定や市場分析を想定
- ヒントが少ない(例示の観点だけでは足りない)

⇒ **難しい**

AU 午後Ⅱ 各問題の特徴と難易度(問2)

・ 問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

設問ア: システム又はサービスの概要,
サイバーセキュリティ管理態勢が必要となる理由

設問イ: サイバーセキュリティ管理態勢におけるPDCAサイクルの実施の適切性を確かめるための監査の着眼点,
入手すべき監査証拠, 監査手続によって確かめる内容

設問ウ: 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の適切性を確かめるための監査の着眼点,
入手すべき監査証拠, 監査手続によって確かめる内容

- － 設問イ・ウでそれぞれ別の監査を書かなければならない。
- － 論点が多いが、例示が少ない。 ⇒ 難しい

AU 今後の対策（午前Ⅱ）

<午前Ⅱ対策>

－ 基準の改訂に着目！

- ・ 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の基準
- ・ 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

すべて今年改訂されました。

来年は新基準から出ます！

TACテキストも刷新します！

※最新版を押さえておこう！

－ 過去問題の演習は有効！

- ・ 再出題率が高いので、解いたうえで新基準と比較しよう！

AU 今後の対策（午後Ⅰ）

<午後Ⅰ 対策>

－ 主要3テーマについて過去問題演習を

- ① システム開発関連の監査
- ② 業務処理統制の監査
- ③ 情報セキュリティ監査

特に①がよく出ます！
企画～開発～運用まで

テーマ別に、過去問題で取り上げられた観点を押さえておく

－ 最新トピックが出やすいので、リスクと対策を押さえておく

- ・ DX, AI, IoT, テレワーク環境の構築・運用・セキュリティ,
携帯デバイスの業務利用のセキュリティ, マイナンバー,
個人情報保護管理, クラウドコンピューティング,
事業継続計画(BCP), RPA など

午後Ⅱにも出ます！

AU 今後の対策（午後Ⅱ）

<午後Ⅱ 対策>

- 過去問題を使ってさまざまな題材での論述演習を
 - ・ 論述の中で、「リスク, コントロール, 監査手続」の対応がしっかり取れているかを常に意識する
- 新技術に関する問題への準備
 - ・ その技術に起こるリスクを知り、監査する場合の着眼点を想定しておく
- 監査経験がなくても大丈夫！
 - ・ 「もし自分が監査を行うならこうする」という視点で書く
 - ・ 問われたことに正面から「解答する」ことを意識する

今回のような応用形でも
この対応を意識して！