Contents

目 次

商標表示
各社の登録商標及び商標，製品名に対しては，特に注記のない場合でも，これを十分に尊重いたします。

Part 1　第2章　Chapter 2

システム監査技術者試験の出題傾向

2-1　システム監査技術者試験の概要

システム監査技術者試験を受けるに当たっては，試験の概要を把握する必要があることはいうまでもありません。

まず，システム監査技術者とは，「どんな人材で，どんな役割があるのか」を明らかにしておく必要があります。

独立行政法人 情報処理推進機構 IT 人材育成本部 情報処理技術者試験センターが発表した「情報処理技術者試験 新試験制度の手引」には，システム監査技術者の対象者像，業務と役割，期待する技術水準，レベル対応について，次のように記載されています。

(1)　対象者像（各試験区分の対象者像のシステム監査技術者）

高度 IT 人材として確立した専門分野をもち，被監査対象から独立した立場で，情報システムや組込みシステムに関するリスク及びコントロールを総合的に点検，評価し，監査結果をトップマネジメントなどに報告し，改善を勧告する者

これまでの対象者像と比較すると，平成 21 年度からのシステム監査技術者試験には，次の特徴があります。

・システム監査技術者を高度 IT 人材の確立した専門分野として位置付けた。
・我が国の国際競争力強化における組込みシステムの重要性の高まりに対応するため，情報システムに加え，組込みシステムを追加した。
・リスクアプローチの考え方を踏まえ，リスク及びコントロールを総合的に点検，評価するとした。

2-6　午後Ⅱ試験の出題状況

(1)　出題テーマ

次回の平成 26 年度から午後Ⅱ試験は，出題 2 問から 1 問を選択解答する試験となります。該当テーマについて，設問ア～ウから構成される論文（2,200～3,600 字）を 2 時間で作成する試験です。図表 2-5 に示すとおり，平成 25 年度までは，出題 3 問から 1 問を選択し解答する試験でした。

試験年度	出題テーマ
平成25年	問1　システム運用業務の集約に関する監査 問2　要件定義の適切性に関するシステム監査 問3　ソフトウェアパッケージを利用した基幹系システムの再構築の監査
平成24年	問1　コントロールセルフアセスメント（CSA）とシステム監査 問2　システムの日常的な保守に関する監査 問3　情報システムの冗長化対策とシステム復旧手順に関する監査
平成23年	問1　システム開発や運用業務を行う海外拠点に対する情報セキュリティ監査 問2　ベンダマネジメントの監査 問3　システム開発におけるプロジェクト管理の監査
平成22年	問1　情報システム又は組込みシステムに対するシステムテストの監査 問2　電子データの活用にかかわるシステム監査 問3　IT 保守・運用コスト削減計画の監査
平成21年	問1　シンクライアント環境のシステム監査 問2　システム監査におけるログの活用 問3　企画･開発段階における情報システムの信頼性確保に関するシステム監査
平成20年	問1　アイデンティティマネジメントに関するシステム監査 問2　内部統制報告制度におけるシステム監査 問3　外部組織に依存した業務に関する事業継続計画のシステム監査
平成19年	問1　システム監査における IT の利用 問2　情報システムの調達管理に関するシステム監査 問3　情報システムを利用したモニタリングとシステム監査
平成18年	問1　監査手続書の作成 問2　文書類の電子化とシステム監査 問3　情報漏えい事故対応計画の監査

図表 2-5　午後Ⅱ論述式試験の出題テーマ（平成 18～25 年）

平成 25 年度はありませんでしたが，平成 22 年度問 1，平成 23 年度問 3，平成

Part 2　Chapter 2

第2章 システム監査

2－1　システム監査とは

2.1.1　システム監査とは

システム監査は，情報システムを対象とする監査です。ここでは，参考として，監査と従来のシステム監査の定義を挙げておきます。

- **監査の定義**：独立かつ客観的立場で監査対象を評価基準に照らして点検・評価し，その結果を監査報告書に取りまとめ，組織体の長に提出することである（プライバシーマーク制度における監査ガイドライン；2000）。
- **システム監査の定義**：監査対象から独立かつ客観的立場のシステム監査人が情報システムを総合的に点検及び評価し，組織体の長に助言及び勧告するとともにフォローアップする一連の活動（1996 年版システム監査基準Ⅱ．用語の定義(1)システム監査）。

現行の平成 16 年版システム監査基準にはシステム監査の定義の記載はありません。次に挙げる「システム監査基準Ⅱ．システム監査の目的」に記載されている内容がシステム監査の定義に該当するといわれています。

「**システム監査の目的**は，組織体の情報システムにまつわるリスクに対するコントロールがリスクアセスメントに基づいて適切に整備・運用されているかを，独立かつ専門的な立場のシステム監査人が検証又は評価することによって，保証を与えあるいは助言を行い，もって IT ガバナンスの実現に寄与することにある」

特徴については，システム監査基準解説書に次のように記されています。

- 情報システムにまつわるリスクに対するコントロールについて監査を実施すること
- コントロールがリスクアセスメントに基づいて適切に整備・運用されているかを検証又は評価すること
- 監査には，保証型又は助言型の監査があること
- 最終的には IT ガバナンスの実現に寄与すること

演習問題

問2　システム監査の実施手順の説明として，適切な記述はどれか。

(865060)

ア　システム監査は，監査計画，本調査，予備調査，監査報告の手順で実施される。

イ　システム監査は，情報システムを対象とする監査なので，情報システムの形態によって，実施手順は異なる。

ウ　システム監査は，予備調査，監査実施，監査報告の手順で実施される。

エ　システム監査は，予備調査，本調査，評価・結論の手順で実施される。

解説

システム監査の実施手順についての理解度を問う問題です。システム監査は，予備調査→本調査→評価・結論の手順で実施されます。したがって，（エ）が適切です。

ア：予備調査は，本調査を効率的に実施するために実施します。

イ：システム監査の実施手順は，情報システムの形態によって異なるものではありません。

ウ：システム監査の大きな実施プロセスは，監査計画，監査実施，監査報告です。

解答－エ

2.2.2　システムの可監査性

(1)　システムの可監査性

システム監査の実施が可能である情報システムの性質をいいます。例えば，USBメモリの持出し禁止規定がコントロールとして存在し，その持出し禁止規定がその存在を確認・検証できるように文書化されている状況をいいます。

(2)　監査証拠

監査意見を立証するために必要な事実をいいます。システム監査の実施は，監査証拠を収集する行為です。監査証拠には物理的証拠，文書的証拠（電磁的証拠を含む），口頭的証拠などがあります。第三者として検証可能にするためには，監査証拠として監査調書に記載する必要があります。前述のUSBメモリでは，文書

Part 3　第2章　Chapter 2

情報システムのライフサイクルの監査に関する演習問題

2－1　はじめに

第1章では，午後Ⅰ試験内容の分析と解答のポイントについてお話ししました。

第2章以降は，午後Ⅰ記述式の過去の試験問題を受験者の取り組み易さを考え，見出しを中心におおまかに次の四つに分類し，演習問題として取り上げ解説します。

(1)　情報システムのライフサイクルの監査に関する演習問題（第2章）
(2)　アプリケーションシステムの監査に関する演習問題（第3章）
(3)　テーマ別システムの監査に関する演習問題（第4章）
(4)　システム監査の計画・実施・報告に関する演習問題（第5章）

2－2　情報システムのライフサイクルの監査

企画，開発，運用，保守の情報システムライフサイクルに関する演習問題です。システム管理基準の構成も，情報戦略，共通業務を別にすると，企画業務，開発業務，運用業務，保守業務に分類されています。平成24年度問4の「システムの移行計画の監査」も，企画業務の監査として，収録しています。

演習問題1	運用業務の監査	(H20春-AU 午後Ⅰ問1)
演習問題2	システム開発の監査	(H21春-AU 午後Ⅰ問4)
演習問題3	企画段階におけるシステム化効果の監査	(H22春-AU 午後Ⅰ問1)
演習問題4	システムの移行計画の監査	(H24春-AU 午後Ⅰ問4)
演習問題5	システム開発の企画段階における監査	(H25春-AU 午後Ⅰ問1)

演習問題　1

(H20 春-AU　午後Ⅰ問 1)

問 1　運用業務の監査に関する次の記述を読んで，設問 1 ～ 3 に答えよ。

A 社は，中堅の通信機器メーカである。A 社では，システムの重要性を認識し，内部監査部がシステム監査を定期的に実施してきた。本年のシステム監査については，内部監査部内で検討した結果，システム運用部を対象に実施することになった。内部監査部の一員である B 君は，その主担当者に指名された。

〔A 社のシステムとシステム関連部門〕

A 社の販売管理システムや在庫管理システムなどは，メインフレームで運用されている。一方，会計システムや経費管理システムなどは，分散環境で運用されている。これらのシステムは，A 社のデータセンタに設置されており，システム運用部が運用を担当している。システムの開発は，システム開発部第一課が担当している。

〔システム運用部の概要〕

システム運用部は，オペレーション課や基盤管理課などの複数の課で構成されている。オペレーション課は，システムの稼働状況の監視や本番機のオペレーションなどを担当し，基盤管理課は，OS，ミドルウェア，プログラムなどの本番環境の資源を導入・管理している。

オペレーション課には，本番機の稼働監視及びオペレーションを担当するオペレータとオペレーション管理者がいる。オペレータは 3 交代勤務となっており，それぞれ 2 名一組の体制で運用に当たっている。オペレーション管理者は，日中だけの勤務であり，出勤時に前日のオペレーション日誌の確認を行っている。

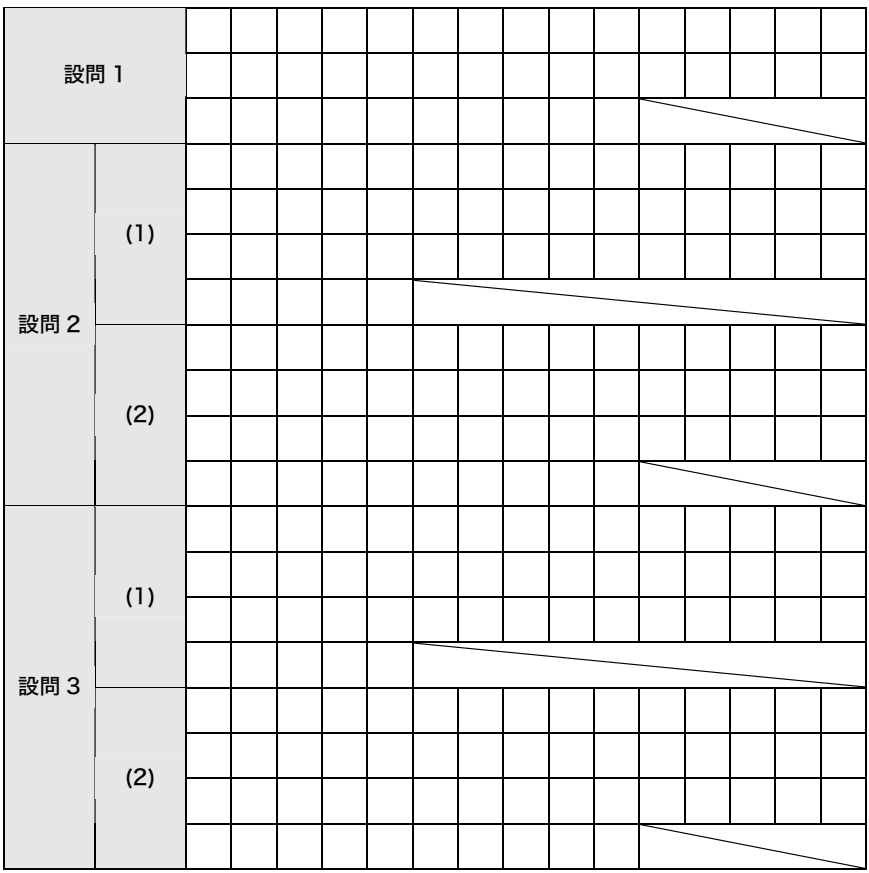
〔運用支援ツールへのオペレーションの登録〕

A 社のシステムには，ベンダが提供する運用支援ツールが導入されており，バッチジョブ及びコマンドの時間起動やメッセージ起動，ジョブネットの設定が可能である。A 社では，オペレータによる本番機への直接オペレーションをできるだけ防ぐために，運用支援ツールの機能を利用している。

この運用支援ツールへのオペレーションの登録は，オペレーション開始の前週までに原則すべて行われる。登録の流れは，次のとおりである。

〔解答用紙〕

コピーして活用してください。



解答作成のポイント　Point

＜解答の方針＞

本問は，運用業務に関するシステム監査に関する問題です。

冒頭の運用業務に関する監査と設問が3問あることを念頭において，ページをめくり設問1～3を読み，各設問の内容を把握してから本文を読みます。

設問1　運用支援ツールにオペレーションを登録する手続について，予定した作業が漏れなく，正確に登録されていることを保証する重要なコントロールを40字以内で解答する。

設問2　〔登録が間に合わなかった作業依頼手続〕中のコントロールだけでは，オペレータの作業にかかわるリスクが十分低減されない状況について，

(1)　低減されないリスクを50字以内で解答する。

(2)　(1)のリスクを低減するコントロールを55字以内で解答する。

設問3　障害関連メッセージの登録手続について，

(1)　B君が実施した監査手続だけでは，基盤管理課の登録ミスを防ぐコントロールの運用状況を評価する上で不十分な理由を50字以内で解答する。

(2)　B君が実施すべき監査手続を55字以内で具体的に解答する。

問題の概要を整理してみましょう。

・中堅の通信機器メーカA社
・システムの重要性を認識→内部監査部による定期的なシステム監査の実施
・本年度のシステム監査→監査対象：システム運用部，監査人：主担当者B君

＜A社システム関連プロフィール＞

・販売管理システム，在庫管理システム：メインフレームで運用
・会計システム，経費管理システム：分散環境で運用
・データセンタに設置，システム運用部による運用，システム開発部第一課が担当
・システム運用部の概要：オペレーション課，基盤管理課などの複数の課で構成
→オペレーション課：システムの稼働状況の監視や本番機のオペレーション

〔解答例〕

［設問１］

基盤管理課長が実施する運用スケジュール表と登録結果リストの内容の照合確認

［設問２］

(1)　オペレータが本番作業依頼票で指示された以外の作業を本番機で実施しても発見されないリスク

(2)　オペレーション管理者が自ら該当オペレーションログを出力して，依頼された作業だけが行われたかを確認する。

［設問３］

(1)　基盤管理課長による本番リリース依頼書に基づくメッセージ登録照合が正確であることを確認できない。

(2)　本番リリース依頼書と登録内容表を照合し，登録されたメッセージが本番リリース依頼書と同一であることを確認する。

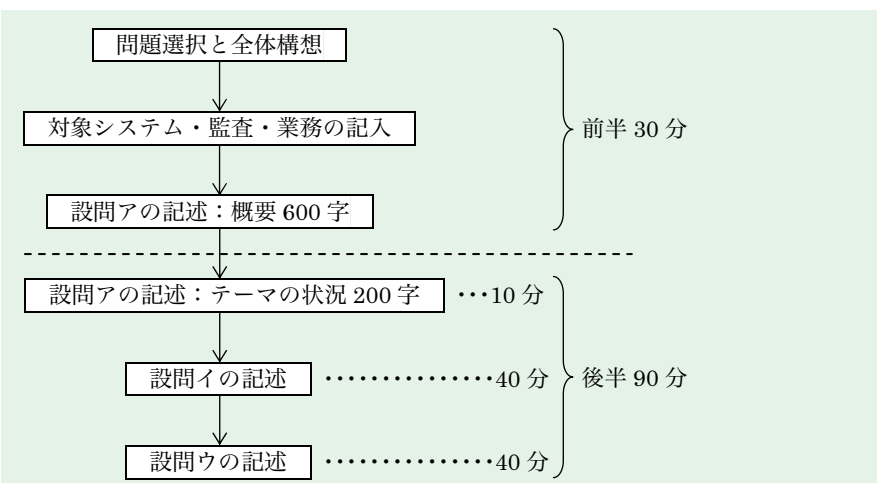
Part４　第３章　Chapter３

本番対策と合格予想論文

３－１　本番対策

本番の試験は，2 時間（120 分）ですが，解答する問題を選択し，記述する対象のシステム，監査，業務について所定の様式（第 4 部第 1 章図表 1-1 の 6(2)“あなたが携わったシステム監査，システム利用又はシステム開発・運用業務の概要”の答案用紙）に記入し，本番の論文を合格ラインの 2,400 字（推奨 2,800 字）以上を記述するにはあまりに短い時間といえます。

したがって，準備した下書き論文を利用して，効率良く記述していくためには，あらかじめ時間配分を考えておく必要があります。時間配分は，皆さんが準備した下書き論文の構成にも影響を受けると思いますが，ここでは標準的な論文構成と時間配分を図表 3-1 に示します。



図表 3-1　標準的な論文構成と時間配分

論文作成の手順は，前半の 30 分と後半の 90 分に大きく分けることができます。

〔事例1〕

組込み型システムの監査について　(865315)

自動車やカーナビ，携帯電話やデジタルカメラなどコンピュータを内蔵した情報関連機器が氾濫している。また，最近特に話題になっているロボットも工場にあっては様々な形で実用化されより人間に近いロボットを目指し，インテリジェント性をいかに確立し，労働不足や高齢化社会への貢献をするかなどの観点からも研究されている。

これらは，いずれもコンピュータを中心にした組込みシステムをベースとしている。組込み型システムは，エンベデッドシステムとも呼ばれ，マイクロチップと制御プログラムを組み込み，特定用途に専用化されたシステムであり，ITをマイクロチップに搭載した情報システムともいえる。

特定用途とはいえ，汎用的にチップオンボード化しているため，情報システムとしての信頼性，安全性，効率性は欠かせないが，不安定な振舞い事例も報告されている。

今後，ますます高速化されたマイクロチップが大量に組み込まれた情報家電などが普及することは明らかであり，安定的・継続的稼働は欠かせず，システム監査の観点からの点検・評価が求められている。

あなたの経験と考えに基づいて，設問ア～ウに従って論述せよ。

設問ア　あなたが携わった組込みシステムの概要と，当該組込みシステムの特徴について，800字以内で述べよ。

設問イ　設問アで述べた組込みシステムの内包するリスクと，該当リスクを逓減するための対策を700字以上1,400字以内で具体的に述べよ。

設問ウ　組込みシステムについて監査するとき，監査のチェックポイントと監査手続ついて700字以上1,400字以内で具体的に述べよ。

〔解説〕

本問は，「組込み型システムの監査について」がテーマです。監査対象分野としては，組込みシステムというテーマの観点からは，テーマ別監査に分類される出題ですが，組込みシステムアプリケーションのシステム監査と考えれば，アプリ

ケーションシステムとしても記述可能です。

設問アでは，「あなたが携わった組込みシステムの概要と，当該組込みシステムの特徴」が出題テーマです。組込みシステムの概要と特徴がテーマですので，見出し構成としては次のようになります。

Ⅰ．組込みシステムの概要と特徴
　Ⅰ.1　組込みシステムの概要
　　(1)　組込みシステム開発の目的
　　(2)　組込みシステムの概要
　Ⅰ.2　組込みシステムの特徴

解答例では，カーオーディオプロトタイプシステムを対象としましたので，カーオーディオプロトタイプシステムの概要の見出しになっています。

設問イについては，設問アで述べた組込みシステムに対するリスクと当該リスクに対する対策について記述することを求めています。見出し構成としては，次のような構成になるでしょう。解答例では，カーオーディオプロトタイプシステムを監査対象としましたので，カーオーディオプロトタイプシステムに及ぼすリスクとして記述しています。

Ⅱ．組込みシステム関連リスクとその対応
　Ⅱ.1　組込みシステムに及ぼすリスク
　Ⅱ.2　組込みシステム関連リスクへの対応

設問ウについては，組込みシステムついてシステム監査する場合の監査のチェックポイントを求めています。ここでは，監査手続も記述に加えて，見出し構成は次のような構成としています。出題は設問ア，イについての記述がないので，一般論としての記述も可能なように見出し構成に具体的な組込みシステムの記述を含めていません。

Ⅲ．組込みシステムの監査チェックリストと監査手続
　Ⅲ.1　組込みシステムの監査チェックリスト
　Ⅲ.2　組込みシステムの監査を行う際の監査手続

なお解答例では，一般論として組込みシステムの監査を行う際のチェックリストと監査手続として記述しています。

〔事例1　解答論文例〕

本文（設問ア）　800字以内で記述してください。

Ⅰ.カーオーディオプロトタイプシステムの概要と特徴

私は工作機械メーカK社に10年勤務し，現在は機械工作設計課で組込みシステムの設計に従事している。

Ⅰ.1　カーオーディオプロトタイプシステムの概要

本システムは，カーオーディオシステムにおいて，CDやチューナのソフトウェアをチップに実装するためのプロトタイプシステムである。実装に当たっては，C言語をベースに32ビットCPU上でOSはμITRONを用いて開発した。

一般的に組込みソフトウェアは，ユーザによる多様な利用の仕方が考えられるケースが多く，複数タスクや割込みにも適切に対応する必要があるため，複雑な内部構造をもつケースが多い。本システムでも，そうした多数のイベント発生の非常に多くの順序や組合せに対して正しく振る舞うために網羅的な検証システムが欠かせない状況であった。本システムでは，そうした状況に対しリアルタイムOSのサービスコール利用を含む方式でモデル化を行い，モデル検査を行う検証エンジンを作成した。

Ⅰ.2　カーオーディオプロトタイプシステムの特徴

本システムの構成は，デバイスを制御するドメイン，ユーザによるボタン操作を制御するドメイン，各種機構を制御するドメイン，CDやチューナのアプリケーションを制御するドメイン，各ドメイン間インタフェースの五つのドメイン構成とした。

処理の流れとしては，ユーザの入力操作を条件判定し，CD，チューナ，音量，表示，メニューといった制御をイベント制御によって切り替える方式となっており，各種ユーザ操作に対応可能なポリモーフィズム構成となっている。

私は，本組込みシステムの開発に企画段階から参加し，検証チームのサブリーダとして，網羅性検証の全責任を負った。

システム監査基準

システム監査基準
経済産業省
平成 16 年 10 月 8 日改訂

Ⅰ．前文

今日，組織体の情報システムは，経営戦略を実現するための組織体の重要なインフラストラクチャとなっている。さらに，それぞれの情報システムがネットワーク化されることにより，社会の重要なインフラストラクチャとなってきている。一方，情報システムはますます多様化，複雑化し，それに伴い様々なリスクが顕在化してきている。また，情報システムに係わる利害関係者も組織体内にとどまらず，社会へと広がっている。従って，このような情報システムにまつわるリスクを適切にコントロールすることが組織体における重要な経営課題となっている。システム監査は，組織体の情報システムにまつわるリスクに対するコントロールが適切に整備・運用されていることを担保するための有効な手段となる。また，システム監査の実施は，組織体の IT ガバナンスの実現に寄与することができ，利害関係者に対する説明責任を果たすことにつながる。

組織体が情報システムにまつわるリスクに対するコントロールを適切に整備・運用する目的は，以下の通りである。

・情報システムが，組織体の経営方針及び戦略目標の実現に貢献するため
・情報システムが，組織体の目的を実現するように安全，有効かつ効率的に機能するため
・情報システムが，内部又は外部に報告する情報の信頼性を保つように機能するため
・情報システムが，関連法令，契約又は内部規程等に準拠するようにするため

システム監査基準は，システム監査業務の品質を確保し，有効かつ効率的に監査を実施することを目的とした監査人の行為規範である。本監査基準は，監査人としての適格性及び監査業務上の遵守事項を規定する「一般基準」，監査計画の立案及び監査手続の適用方法を中心に監査実施上に枠組みを規定する「実施基準」，監査報告に係わる留意事項と監査報告書の記載方式を規定する「報告

Index 索 引

英字

あ行

か行