○システム監査基準
昭和６０年１月公表
平成８年１月３０日改正公表

Ⅰ　主旨

本基準は、情報システムの信頼性、安全性及び効率性の向上を図り、情報化社会の健全化に資するため、システム監査に当たって必要な事項を網羅的に示したものである。

Ⅱ　用語の定義

本基準に用いている主な用語の定義は、以下のとおりである。

(1)　システム監査・・・・・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

(2)　システム監査人・・・次の知識及び能力を有し、システム監査に従事する者
①情報システムの基本的知識
②システム監査の知識
③システム監査の実施能力
④システム監査の実施に当たっての関連知識

(3)　信頼性・・・・・・・・・・・情報システムの品質並びに障害の発生、影響範囲及び回復の度合

(4)　安全性・・・・・・・・・・・情報システムの自然災害、不正アクセス及び破壊行為からの保護の度合

(5)　効率性・・・・・・・・・・・情報システムの資源の活用及び費用対効果の度合

(6)　被監査部門・・・・・・・システム監査を受ける部署

(7)　基本計画・・・・・・・・・当該年度に実施するシステム監査の全体的な計画

(8)　個別計画・・・・・・・・・基本計画に基づく個別のシステム監査業務に対する計画

(9)　リスク分析・・・・・・・情報システムを利用することに伴って発生する可能性のあるリスクを洗い出し、その影響度合を分析すること

(10)　指摘事項・・・・・・・・・システム監査人が自らの判断基準に基づき指摘した問題点

(11)　改善事項・・・・・・・・・指摘事項のうち、システム監査人が改善を必要と判断した事項

(12)　改善勧告・・・・・・・・・改善事項を緊急性を要する事項（緊急改善）とその他の事項（通常改善）に分けて整理した勧告

Ⅲ　基準の構成

本基準は、一般基準、実施基準及び報告基準から構成しており、その内容は以下のとおりである。

(1)　一般基準（９項目）

一般基準は、システム監査において基本となる監査計画及びシステム監査人に求められる要件等の原則を定めている。

(2)　実施基準（191項目）

実施基準は、システム監査の対象である情報システムの企画、開発、運用及び保守業務並びに共通業務に対する監査項目を定めている。

(3)　報告基準（８項目）

報告基準は、システム監査の結果をとりまとめるに当たっての必要事項及び結果に基づく措置を定めている。

Ⅳ　実施基準の考え方

(1)　実施基準は、集中処理又は分散処理のいずれにも適用できる。

(2)　実施基準は、開発方法に依存することなく適用できる。

(3)　企画業務は、情報戦略からシステム 分析・要求定義までを対象とする。

(4)　開発業務は、開発手順から移行までを対象とする。

(5)　運用業務は、情報システムの運用に係るソフトウェア、ハードウェア、ネットワーク、建物等の管理を対象とする。

(6)　保守業務は、ソフトウェアの変更に係る事項で、保守手順から旧情報システムの廃棄までを対象とする。

(7)　情報システムの大幅変更は、企画及び開発業務とする。

(8)　共通業務は、企画、開発、運用及び保守業務に共通するドキュメント管理、進捗管理、要員管理、外部委託及び災害対策から構成している。

(9)　企画、開発、運用及び保守業務の監査に当たっては、共通業務の基準についても考慮し、適用すること。

なお、共通業務の基準は、単独で適用することができる。

(10) 実施基準は、組織体の実態に応じ適切に適用すること。

Ⅴ　一般基準

1　体　制

(1)　組織体は、システム監査が適切に実施できる体制を整備すること。

2　監　査

(1)　システム監査人は、システム監査の基本計画及び個別計画を策定すること。

(2)　システム監査は、個別計画に基づき、予備調査、本調査及び評価・結論の手順により実施すること。

3　システム監査人の責任・権限

(1)　システム監査人は、自らの判断に対する根拠を明確にすること。

(2)　システム監査人は、被監査部門に対し資料の提出を求めることができる。

(3)　システム監査人は、組織体の長が被監査部門に改善を命令した事項について、実施状況の報告を求めることができる。

4　職業倫理

(1)　システム監査人は、客観的な評価者としての立場を堅持すること。

(2)　システム監査人は、自己に対する倫理的要請を自覚し、的確かつ誠実なシステム監査の実践を通じて、内外の信頼に応えること。

5　守秘義務

(1)　システム監査人は、正当な理由なく、業務上知り得た秘密を漏らし、又は不当な目的に利用してはならない。

Ⅵ　実施基準

イ　企画業務

1　情報戦略

(1)　情報戦略は、経営戦略との整合性を考慮して策定しているか。

(2)　情報システムの企画、開発、運用及び保守業務に係る標準化の方針を明確にしているか。

(3)　情報戦略の有効性を評価しているか。

2　全体計画

(1)　全体計画の立案体制を組織的に確立し、組織体の長が承認しているか。

(2)　全体計画は、全体計画立案ルールに基づいて策定し、組織体の長が承認しているか。

(3)　全体計画は、情報化の効果、推進体制、費用等を明確にしているか。

(4)　全体計画は、情報システムの全体像を明確にしているか。

(5)　全体計画は、システム開発の優先度を明確にしているか。

(6)　全体計画は、システム開発によって生ずる組織及び業務の変更の方針を明確にしているか。

(7)　全体計画は、セキュリティ対策の方針を明確にしているか。

(8)　全体計画は、定期的な見直し及び経営環境等の変化に対応した見直しを行っているか。

3　開発計画

(1)　開発計画は、組織体の長が承認しているか。

(2)　開発計画は、全体計画との整合性を考慮して策定しているか。

(3)　開発計画は、内外の情報技術調査を実施して策定しているか。

(4)　開発計画は、目的、対象業務、費用対効果等を明確にしているか。

(5)　情報システムのライフサイクルを設定する条件を明確にしているか。

4　システム分析・要求定義

(1)　開発計画に基づいた要求定義は、開発及びユーザの責任者が承認しているか。

(2)　ユーザニーズの調査は、対象、範囲及び方法を明確にしているか。

(3)　実務に精通しているユーザが参画して現状分析を行っているか。

(4)　情報システムの導入に伴って発生する可能性のあるリスクを分析しているか。

(5)　情報システムに関連する法律、制度等を全て調査しているか。

(6)　情報システムの導入によって影響を受ける業務、管理体制、諸規程等は、見直し等の検討を行っているか。

(7)　ユーザ部門と情報システム部門の役割分担を明確にしているか。

(8)　開発計画及びユーザニーズに基づき、ソフトウェア、ハードウェア、ネットワーク等を選択しているか。

(9)　情報システムの目的を達成する実現可能な代替案を作成し、検討しているか。

(10)　開発方法は、開発の規模、期間及びシステム特性を考慮して決定しているか。

(11)　開発及び運用費用の算出基礎を明確にしているか。

(12)　情報システムの効果の定量的及び定性的評価を行っているか。

(13)　開発を遂行するために必要な要員、予算、設備、期間等を確保しているか。

ロ　開発業務

1　開発手順

(1)　開発手順は、開発の責任者が承認しているか。

(2)　開発手順は、開発方法に基づいて作成しているか。

(3)　開発手順は、開発の規模等から決定しているか。

2　システム設計

(1)　システム設計書は、開発及びユーザの責任者が承認しているか。

(2)　ユーザが利用しやすく入出力帳票、入出力画面等を設計しているか。

(3)　データベースは、業務の内容に応じて設計しているか。

(4)　データの保全性を確保しているか。

(5)　ネットワークは、業務の内容に応じて設計しているか。

(6)　情報システムの性能は、要求定義を満たしているか。

(7)　システム構成は、ピーク時を想定して設計しているか。

(8)　運用に必要な性能管理等の技術的な実現方法等を設計しているか。

(9)　情報システムの障害対策を講じているか。

(10)　不正防止、機密保護等の機能を設計しているか。

(11)　テスト計画は、目的、範囲、方法、スケジュール等を明確にしているか。

(12)　情報システムの利用に係る教育の方針、スケジュール等を明確にしているか。

3　プログラム設計

(1)　プログラム仕様書は、開発の責任者が承認しているか。

(2)　システム設計書に基づいて、プログラムを設計しているか。

(3)　プログラム設計時に発見したシステム設計の矛盾は、システム設計の再検討を行って解決しているか。

4　プログラミング

(1)　プログラム仕様書に基づいてプログラミングしていることを検証しているか。

(2)　プログラムテストの結果を記録及び保管しているか。

(3)　重要プログラムは、プログラム作成者以外の者がテストしているか。

5　システムテスト

(1)　テストデータの作成及びシステムテストは、テスト計画に基づいて行っているか。

(2)　システムテストは、公正かつ客観的立場の者が実施しているか。

(3)　システムテストは、ユーザが参画し、ユーザマニュアルに基づいて実施しているか。

(4)　システムテストの結果は、開発、運用、保守及びユーザの責任者が承認しているか。

(5)　システムテストの結果を記録及び保管しているか。

6　移　行

(1)　移行計画及び移行に伴う運用計画を策定しているか。

(2)　移行計画に基づいて、移行に必要な要員、予算、設備等を確保しているか。

(3)　移行完了の検証方法を明確にしているか。

(4)　移行後の運用の実行計画を策定しているか。

ハ　運用業務

1　運用管理

(1)　運用管理ルールを定め、遵守しているか。
(2)　操作手順を標準化し、事故及び障害の対策を明確にしているか。
(3)　ジョブスケジュールは、業務処理の優先度を考慮して設定しているか。
(4)　オペレーションは、ジョブスケジュール及び指示書に基づいて行っているか。
(5)　例外処理のオペレーションは、運用管理ルールに基づいて行っているか。
(6)　オペレータの交替は、運用管理ルールに基づいて行っているか。
(7)　ジョブスケジュールとオペレーション実施記録の差異分析を行っているか。
(8)　情報システムの稼動実績を把握し、性能管理及び資源の有効利用を図っているか。
(9)　オペレーション実施記録は、運用管理ルールに基づいて一定期間保管しているか。
(10)　事故及び障害の内容を記録し、情報システムの運用の責任者に報告しているか。
(11)　事故及び障害の原因を究明し、再発防止の措置を講じているか。
(12)　識別コード及びパスワードの管理は、不正防止及び機密保護の対策を講じているか。
(13)　情報システムのセキュリティに関する教育及び訓練をユーザに対して実施しているか。

2　入力管理

(1)　入力管理ルールを定め、遵守しているか。
(2)　入力データの作成手順、取扱い等は、誤びゅう防止、不正防止及び機密保護の対策を講じているか。
(3)　データの入力は、入力管理ルールに基づいて行っているか。
(4)　データの入力の誤びゅう防止、不正防止及び機密保護の対策は有効に機能しているか。
(5)　入力データの保管及び廃棄は、入力管理ルールに基づいて行っているか。

3　データ管理

(1)　データ管理ルールを定め、遵守しているか。
(2)　データへのアクセスコントロール及びモニタリングは、有効に機能しているか。
(3)　データの利用状況を記録し、定期的に分析しているか。
(4)　データのバックアップの範囲及びタイミングは、業務内容、処理形態及びリカバリの方法を考慮して決定しているか。
(5)　データの授受は、データ管理ルールに基づいて行っているか。
(6)　データの交換は、不正防止及び機密保護の対策を講じているか。
(7)　データの保管及び廃棄は、不正防止及び機密保護の対策を講じているか。
(8)　データの複写は、不正防止及び機密保護の対策を講じているか。
(9)　データに対するコンピュータウイルス対策を講じているか。
(10)　データの知的財産権を管理しているか。

4　出力管理
(1)　出力管理ルールを定め、遵守しているか。
(2)　出力情報の作成手順、取扱い等は、不正防止及び機密保護の対策を講じているか。
(3)　出力情報の引渡しは、出力管理ルールに基づいて行っているか。
(4)　出力情報の保管及び廃棄は、出力管理ルールに基づいて行っているか。
(5)　出力情報のエラー状況を記録し、定期的に分析しているか。
(6)　出力情報の利用状況を記録し、定期的に分析しているか。
5　ソフトウェア管理
(1)　ソフトウェア管理ルールを定め、遵守しているか。
(2)　ソフトウェアへのアクセスコントロール及びモニタリングは、有効に機能しているか。
(3)　ソフトウェアの利用状況を記録し、定期的に分析しているか。
(4)　ソフトウェアのバックアップの範囲及び方法は、業務内容及び処理形態を考慮して決定しているか。
(5)　ソフトウェアの授受は、ソフトウェア管理ルールに基づいて行っているか。
(6)　ソフトウェアの保管及び廃棄は、不正防止及び機密保護の対策を講じているか。
(7)　ソフトウェアの複写は、不正防止及び機密保護の対策を講じているか。
(8)　ソフトウェアに対するコンピュータウイルス対策を講じているか。
(9)　ソフトウェアの知的財産権を管理しているか。
6　ハードウェア管理
(1)　ハードウェア管理ルールを定め、遵守しているか。
(2)　ハードウェアは、想定されるリスクを回避できる環境に設置しているか。
(3)　ハードウェアは、定期的に保守を行っているか。
(4)　ハードウェアは、障害対策を講じているか。
(5)　ハードウェアの利用状況を記録し、定期的に分析しているか。
7　ネットワーク管理
(1)　ネットワーク管理ルールを定め、遵守しているか。
(2)　ネットワークへのアクセスコントロール及びモニタリングは、有効に機能しているか。
(3)　ネットワークの利用状況を記録し、定期的に分析しているか。
8　構成管理
(1)　管理すべきソフトウェア、ハードウェア及びネットワークの対象範囲を明確にしているか。
(2)　ソフトウェア、ハードウェア及びネットワークの構成、購入先、サポート条件等を明確にしているか。
(3)　ソフトウェア、ハードウェア及びネットワークの導入並びに変更は、影響を受ける範囲を検討して決定しているか。
(4) ソフトウェア、ハードウェア及びネットワークの導入並びに変更は、計画的に実　施しているか。

9　建物・関連設備管理

(1)　建物及び関連設備は、想定されるリスクを回避できる環境に設置しているか。

(2)　建物及び室への入退の管理は、不正防止及び機密保護の対策を講じているか。

(3)　関連設備は、定期的に保守を行っているか。

(4)　関連設備は、障害対策を講じているか。

ニ　保守業務

1　保守手順

(1)　保守に必要なドキュメント等は、引継ぎルールに基づいて開発の責任者から引継いでいるか。

(2)　保守手順は、保守の規模、期間、システム特性等を考慮して決定しているか。

(3)　保守手順は、保守の責任者が承認しているか。

2　保守計画

(1)　保守計画を策定し、保守及びユーザの責任者が承認しているか。

(2)　変更依頼等に対し、保守の内容及び影響範囲の調査並びに分析を行っているか。

(3)　保守のテスト計画は、目的、範囲、方法、スケジュール等を明確にしているか。

3　保守の実施

(1)　システム設計書、プログラム仕様書等は、保守計画に基づいて変更し、保守及びユーザの責任者が承認しているか。

(2)　プログラムの変更は、保守手順に基づき、保守の責任者の承認を得て実施しているか。

(3)　変更したプログラム仕様書に基づいてプログラミングしていることを検証しているか。

4　保守の確認

(1)　変更したプログラムのテストの実施は、保守のテスト計画に基づいて行っているか。

(2)　変更したプログラムは、新規開発と同程度のテストを行っているか。

(3)　変更したプログラムのテストは、ユーザが参画し、ユーザマニュアルに基づいて実施しているか。

(4)　変更したプログラムのテストの結果は、開発、運用、保守及びユーザの責任者が承認しているか。

(5)　変更したプログラムのテストの結果を記録及び保管しているか。

5　移　行

(1)　移行手順は、移行の条件を考慮して作成しているか。

(2)　変更前のプログラム及びデータをバックアップしているか。

(3)　運用の責任者は、他の情報システムへ影響を与えていないことを検証しているか。

6　旧情報システムの廃棄

(1)　旧情報システムは、廃棄計画を策定し、運用及びユーザの責任者の承認を得て廃棄しているか。

(2)　旧情報システムの廃棄方法及び廃棄時期は、不正防止及び機密保護の対策を考慮して決定しているか。

ホ　共通業務

ａ　ドキュメント管理

１　作　成

(1)　ドキュメント作成ルールを定め、遵守しているか。

(2)　ドキュメントの作成計画を策定しているか。

(3)　ドキュメントの種類、目的、作成方法等を明確にしているか。

(4)　ドキュメントは、作成計画に基づいて作成しているか。

(5)　ドキュメントは、情報システム部門及びユーザ部門の責任者が承認しているか。

２　管　理

(1)　ドキュメント管理ルールを定め、遵守しているか。

(2)　情報システムの変更に伴い、ドキュメントの内容を更新し、更新履歴を記録しているか。

(3)　ドキュメントの更新内容は、情報システム部門及びユーザ部門の責任者が承認しているか。

(4)　ドキュメントの保管及び廃棄は、不正防止及び機密保護の対策を講じているか。

(5)　ドキュメントの複写は、不正防止及び機密保護の対策を講じているか。

ｂ　進捗管理

１　実　施

(1)　進捗管理の方法､体制等を定め､企画､開発､運用及び保守業務の責任者が承認　しているか。

(2)　企画、開発、運用及び保守業務の責任者は、進捗状況を把握しているか。

(3)　進捗の遅延等の対策を講じているか。

２　評　価

(1)　業務の工程終了時に、計画に対する実績を分析及び評価しているか。

(2)　評価結果は、次工程の計画に反映しているか。

(3)　評価結果は、進捗管理の方法、体制等の改善に反映しているか。

ｃ　要員管理

１　責任・権限

(1)　要員の責任及び権限は、企画、開発、運用及び保守の業務の特性に応じて定めているか。

(2)　要員の責任及び権限は、情報環境の変化に対応した見直しを行っているか。

(3)　要員の責任及び権限を周知徹底しているか。

２　業務遂行

(1)　要員は、権限を遵守しているか。

(2)　作業分担及び作業量は、要員の知識、能力等から検討しているか。

(3)　要員の交替は、不正防止及び機密保護を考慮して行っているか。

(4)　不測の事態に備えた代替要員の確保を検討しているか。

3　教育・訓練

(1)　教育及び訓練のカリキュラムは、情報戦略に基づいて作成及び見直しを行っているか。

(2)　教育及び訓練のカリキュラムは、技術力の向上、業務知識の習得、情報システムのセキュリティ確保等から検討しているか。

(3)　教育及び訓練は、カリキュラムに基づいて定期的かつ効果的に行っているか。

(4)　要員に対するキャリアパスを確立し、情報環境の変化に対応した見直しを行っているか。

4　健康管理

(1)　健康管理を考慮した作業環境を整えているか。

(2)　健康診断及びカウンセリングを行っているか。

d　外部委託

1　委託計画

(1)　委託計画を策定し、委託の責任者が承認しているか。

(2)　委託の目的及び対象範囲を明確にしているか。

(3)　委託は、具体的な効果、問題点等を評価して決定しているか。

2　委託先選定

(1)　委託先の選定基準を明確にしているか。

(2)　委託先が提案した受託条件の比較検討を行っているか。

3　委託契約

(1)　委託契約は、委託契約ルールに基づいて締結しているか。

(2)　不正防止、機密保護等の対策を明確にしているか。

(3)　知的財産権を明確にしているか。

(4)　特約条項及び免責条項を明確にしているか。

4　委託業務

(1)　委託業務の実施内容は、契約内容と一致しているか。

(2)　委託業務の進捗状況を把握し、遅延対策を講じているか。

(3)　委託先における不正防止、機密保護等の対策の実施状況を把握し、必要な措置を講じているか。

(4)　成果物の検収は、委託契約に基づいて行っているか。

(5)　委託した業務の結果を分析及び評価しているか。

e　災害対策

1　リスク分析

(1)　地震等のリスク及び情報システムに与える影響範囲を明確にしているか。

(2)　情報システムの停止等により組織体が被る損失を分析しているか。

(3)　業務の回復許容時間及び回復優先順位を定めているか。

2　災害時対応計画

(1)　リスク分析の結果に基づき、災害時対応計画を策定し、組織体の長が承認しているか。

(2)　災害時対応計画の実現可能性を確認しているか。

(3)　災害時対応計画に基づいた訓練を定期的に行っているか。

(4)　災害時対応計画は、見直しを行っているか。

3　バックアップ

(1)　情報システム、データ及び関連設備のバックアップ方法並びに手順は、業務の回復目標に対応して定めているか。

(2)　運用の責任者は、バックアップ方法及び手順を検証しているか。

4　代替処理・復旧

(1)　運用及びユーザの責任者は、復旧までの代替処理手続き及び体制を定め、検証しているか。

(2)　運用及びユーザの責任者は、復旧手続き及び体制を定め、検証しているか。

Ⅶ　報告基準

1　報告書作成

(1)　システム監査人は、システム監査報告書を作成すること。

(2)　システム監査報告書は、情報システムの信頼性、安全性及び効率性についての評価を記載すること。

(3)　システム監査報告書は、指摘事項を記載すること。

(4)　システム監査報告書は、改善勧告を記載すること。

(5)　システム監査報告書は、改善勧告について提示できる改善案を記載すること。

(6)　システム監査人は、その他必要と認めた事項は、システム監査報告書に記載すること。

2　報　告

(1)　システム監査報告書は、組織体の長に提出し、報告すること。

3　フォローアップ

(1)　システム監査人は、改善勧告に基づく措置について、改善の実施状況の把握及び改善の促進に努めること。

Ⅷ　留意事項

(1)　安全対策の実施状況の監査については、「情報システム安全対策基準」を活用すること。

(2)　コンピュータウイルス対策の実施状況の監査については、「コンピュータウイルス対策基準」を活用すること。

(3)　ソフトウェアの利用状況の監査については、「ソフトウェア管理ガイドライン」を活用すること。