News Release

経済産業省
Ministry of Economy, Trade and Industry

平成１６年１０月８日
経　済　産　業　省

新「システム監査基準」、「システム管理基準」の公表について

ＩＴ投資の目的が、単なる現場の合理化から経営革新へと大きく変化しつつある中、国際的な最新動向も踏まえつつ、経済産業省において、情報システムに係る新たな「システム管理基準」及び「システム監査基準」を策定しました。

具体的には、ＩＴ投資が企業全体の経営最適化に資するよう、経営戦略の観点や情報通信技術の最新動向を踏まえて基準を改訂しており、これら基準が企業に幅広く普及することによって、我が国産業の競争力が強化されることを期待しております。

情報技術の浸透や技術革新の影響により、企業経営におけるＩＴ投資の目的が、単なる現場の合理化から経営そのものの革新へと大きく変化しつつある中、経済産業省においては、国際的な最新動向も踏まえつつ、昭和６０年に策定した「システム監査基準」を改訂し、新たな「システム管理基準」及び「システム監査基準」を策定しました。

具体的には、情報化投資の全体最適化といった経営戦略の観点、情報通信技術の最新動向、また近年重要性を増している情報セキュリティ監査制度との整合性の観点を踏まえて改訂したものであり、当該基準が幅広く普及していくことを通じて、我が国産業の競争力が強化されることを期待しております。

なお、当該基準は、（財）日本情報処理開発協会に設置されたシステム監査基準検討委員会における検討結果を踏まえたものです。

(参考)
昭和６０年１月　システム監査基準策定
平成８年１月　　システム監査基準改訂
平成１６年１０月　システム監査基準を改訂し、システム監査基準・管理基準を策定

（本発表資料のお問い合わせ先）
商務情報政策局　情報セキュリティ政策室
担当者：田辺、大崎
電　話：０３－３５０１－０３９７（直通）

システム管理基準

平成16年10月8日策定

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

システム管理基準は、組織体が主体的に経営戦略に沿って効果的な情報システム戦略を立案し、その戦略に基づき情報システムの企画・開発・運用・保守というライフサイクルの中で、効果的な情報システム投資のための、またリスクを低減するためのコントロールを適切に整備・運用するための実践規範である。

システム管理基準は、本管理基準と姉妹編をなすシステム監査基準に従って監査を行う場合、原則として、監査人が監査上の判断の尺度として用いるべき基準となる。ただし、組織体が属する業界又は事業活動の特性等を考慮して、必要ある場合には、本管理基準の主旨及び体系に則って、該当する関係機関などにおいて、独自の管理基準を策定し活用することが望ましい。また、時々の関連技術動向、関連法令、及び社会規範などを考慮し、それらを反映した詳細なサブコントロール項目を策定することが望ましい。

なお、情報セキュリティの確保の観点から監査を実施する場合には、情報セキュリティ監査制度に基づく情報セキュリティ監査を行うことが要請される。一方で、システム管理基準においても情報セキュリティの確保に関連する項目が挙げられているが、それぞれの項目について、情報セキュリティ管理基準を活用して監査を実施することが望ましい。

システム管理基準(287項目)

Ⅰ. 情報戦略(47)

1. 全体最適化(18)

1.1 全体最適化の方針・目標(6)

⑴ ITガバナンスの方針を明確にすること。
⑵ 情報化投資及び情報化構想の決定における原則を定めること。
⑶ 情報システム全体の最適化目標を経営戦略に基づいて設定すること。
⑷ 組織体全体の情報システムのあるべき姿を明確にすること。
⑸ システム化によって生ずる組織及び業務の変更の方針を明確にすること。
⑹ 情報セキュリティ基本方針を明確にすること。

1.2 全体最適化計画の承認(3)

⑴ 全体最適化計画の立案体制は、組織体の長の承認を得ること。
⑵ 全体最適化計画は、組織体の長の承認を得ること。
⑶ 全体最適化計画は、利害関係者の合意を得ること。

1.3 全体最適化計画の策定(7)

⑴ 全体最適化計画は、方針及び目標に基づいていること。
⑵ 全体最適化計画は、コンプライアンスを考慮すること。
⑶ 全体最適化計画は、情報化投資の方針及び確保すべき経営資源を明確にすること。
⑷ 全体最適化計画は、投資効果及びリスク算定の方法を明確にすること。
⑸ 全体最適化計画は、システム構築及び運用のための標準化及び品質方針を含めたルールを明確にすること。
⑹ 全体最適化計画は、個別の開発計画の優先順位及び順位付けのルールを明確にすること。
⑺ 全体最適化計画は、外部資源の活用を考慮すること。

1.4 全体最適化計画の運用(2)

⑴ 全体最適化計画は、関係者に周知徹底すること。
⑵ 全体最適化計画は、定期的及び経営環境等の変化に対応して見直すこと。

2. 組織体制(9)

2.1 情報システム化委員会(5)

⑴ 全体最適化計画に基づき、委員会の使命を明確にし、適切な権限及び責任を与えること。
⑵ 委員会は、組織体における情報システムに関する活動全般について、モニタリングを実施し、必要に応じて是正措置を講じること。
⑶ 委員会は、情報技術の動向に対応するため、技術採用指針を明確にすること。
⑷ 委員会は、活動内容を組織体の長に報告すること。
⑸ 委員会は、意思決定を支援するための情報を組織体の長に提供すること。

2.2 情報システム部門(2)

⑴ 情報システム部門の使命を明確にし、適切な権限及び責任を与えること。

⑵ 情報システム部門は、組織体規模及び特性に応じて、職務の分離、専門化、権限付与、外部委託等を考慮した体制にすること。

2.3 人的資源管理の方針(2)

⑴ 情報技術に関する人的資源の現状及び必要とされる人材を明確にすること。

⑵ 人的資源の調達及び育成の方針を明確にすること。

3. 情報化投資(6)

⑴ 情報化投資計画は、経営戦略との整合性を考慮して策定すること。

⑵ 情報化投資計画の決定に際して、影響、効果、期間、実現性等の観点から複数の選択肢を検討すること。

⑶ 情報化投資に関する予算を適切に執行すること。

⑷ 情報化投資に関する投資効果の算出方法を明確にすること。

⑸ 情報システムの全体的な業績及び個別のプロジェクトの業績を財務的な観点から評価し、問題点に対して対策を講じること。

⑹ 投資した費用が適正に使用されたことを確認すること。

4. 情報資産管理の方針(4)

⑴ 情報資産の管理方針及び体制を明確にすること。

⑵ 情報資産のリスク分析を行い、その対応策を考慮すること。

⑶ 情報資産の効率的で有効な活用を考慮すること。

⑷ 情報資産の共有化による生産性向上を考慮すること。

5. 事業継続計画(5)

⑴ 情報システムに関連した事業継続の方針を策定すること。

⑵ 事業継続計画は、利害関係者を含んだ組織的体制で立案し、組織体の長が承認すること。

⑶ 事業継続計画は、従業員の教育訓練の方針を明確にすること。

⑷ 事業継続計画は、関係各部に周知徹底すること。

⑸ 事業継続計画は、必要に応じて見直すこと。

6. コンプライアンス(5)

⑴ 法令及び規範の管理体制を確立するとともに、管理責任者を定めること。

⑵ 遵守すべき法令及び規範を識別し、関係者に教育及び周知徹底すること。

⑶ 情報倫理規程を定め、関係者に教育及び周知徹底すること。

⑷ 個人情報の取扱い、知的財産権の保護、外部へのデータ提供等に関する方針を定めること。

⑸ 法令、規範及び情報倫理規程の遵守状況を評価し、改善のために必要な方策を講じること。

Ⅱ. 企画業務(23)

1. 開発計画(9)

⑴ 開発計画は、組織体の長が承認すること。

⑵ 開発計画は、全体最適化計画との整合性を考慮して策定すること。

⑶ 開発計画は、目的、対象業務、費用、スケジュール、開発体制、投資効果等を明確にすること。
⑷ 開発計画は、関係者の教育及び訓練計画を明確にすること。
⑸ 開発計画は、ユーザ部門及び情報システム部門の役割分担を明確にすること。
⑹ 開発計画は、開発、運用及び保守の費用の算出基礎を明確にすること。
⑺ 開発計画はシステムライフを設定する条件を明確にすること。
⑻ 開発計画の策定に当たっては、システム特性及び開発の規模を考慮して形態及び開発方法を決定すること。
⑼ 開発計画の策定に当たっては、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、検討すること。

2. 分析（8）
⑴ 開発計画に基づいた要求定義は、ユーザ、開発、運用及び保守の責任者が承認すること。
⑵ ユーザニーズの調査は、対象、範囲及び方法を明確にすること。
⑶ 実務に精通しているユーザ、開発、運用及び保守の担当者が参画して現状分析を行うこと。
⑷ ユーザニーズは文書化し、ユーザ部門が確認すること。
⑸ 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分析を実施すること。
⑹ 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うこと。
⑺ 情報システムの導入効果の定量的及び定性的評価を行うこと。
⑻ パッケージソフトウェアの使用に当たっては、ユーザニーズとの適合性を検討すること。

3. 調達（6）
⑴ 調達の要求事項は、開発計画及びユーザニーズに基づき作成し、ユーザ、開発、運用及び保守の責任者が承認すること。
⑵ ソフトウェア、ハードウェア及びネットワークは、調達の要求事項を基に選択すること。
⑶ 開発を遂行するために必要な要員、予算、設備、期間等を確保すること。
⑷ 要員に必要なスキルを明確にすること。
⑸ ソフトウェア、ハードウェア及びネットワークの調達は、ルールに従って実施すること。
⑹ 調達した資源は、ルールに従って管理すること。

Ⅲ. 開発業務 （49）

1. 開発手順（4）
⑴ 開発手順は、開発の責任者が承認すること。
⑵ 開発手順は、開発方法に基づいて作成すること。
⑶ 開発手順は、開発の規模、システム特性等を考慮して決定すること。
⑷ 開発時のリスクを評価し、必要な対応策を講じること。

2. システム設計（15）
⑴ システム設計書は、ユーザ、開発、運用及び保守の責任者が承認すること。
⑵ 運用及び保守の基本方針を定めて設計すること。
⑶ 入出力画面、入出力帳票等はユーザの利便性を考慮して設計すること。

⑷ データベースは、業務の内容及びシステム特性に応じて設計すること。
⑸ データのインテグリティを確保すること。
⑹ ネットワークは、業務の内容及びシステム特性に応じて設計すること。
⑺ 情報システムの性能は、要求定義を満たすこと。
⑻ 情報システムの運用性及び保守性を考慮して設計すること。
⑼ 他の情報システムとの整合性を考慮して設計すること。
⑽ 情報システムの障害対策を考慮して設計すること。
⑾ 誤謬防止、不正防止、機密保護等を考慮して設計すること。
⑿ テスト計画は、目的、範囲、方法、スケジュール等を明確にすること。
⒀ 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すること。
⒁ モニタリング機能を考慮して設計すること。
⒂ システム設計書をレビューすること。

3. プログラム設計(5)
⑴ プログラム設計書は、開発の責任者が承認すること。
⑵ システム設計書に基づいて、プログラムを設計すること。
⑶ テスト要求事項を定義し、文書化すること。
⑷ プログラム設計書及びテスト要求事項をレビューすること。
⑸ 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すること。

4. プログラミング(4)
⑴ プログラム設計書に基づいてプログラミングすること。
⑵ プログラムコードはコーディング標準に適合していること。
⑶ プログラムコード及びプログラムテスト結果を評価し、記録及び保管すること。
⑷ 重要プログラムは、プログラム作成者以外の者がテストすること。

5. システムテスト・ユーザ受入れテスト(13)
⑴ システムテスト計画は、開発及びテストの責任者が承認すること。
⑵ ユーザ受入れテスト計画は、ユーザ及び開発の責任者が承認すること。
⑶ システムテストに当たっては、システム要求事項を網羅してテストケースを設定して行うこと。
⑷ 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うこと。
⑸ システムテストは、本番環境と隔離された環境で行うこと。
⑹ システムテストは、開発当事者以外の者が参画すること。
⑺ システムテストは、適切なテスト手法及び標準を使用すること。
⑻ ユーザ受入れテストは、本番同様の環境を設定すること。
⑼ ユーザ受入れテストは、ユーザマニュアルに従い、本番運用を想定したテストケースを設定して実施すること。
⑽ ユーザ受入れテストは、ユーザ及び運用の担当者もテストに参画して確認すること。
⑾ システムテスト及びユーザ受入れテストの結果は、ユーザ、開発、運用及び保守の責任者が承認すること。
⑿ システムテスト及びユーザ受入れテストの経過及び結果を記録及び保管すること。

⑬ パッケージソフトウェアを調達する場合、開発元が品質テストを実施したことを確認すること。

6. 移行（8）

⑴ 移行計画を策定し、ユーザ、開発、運用及び保守の責任者が承認すること。
⑵ 移行作業は文書に記録し、責任者が承認すること。
⑶ 移行完了の検証方法を移行計画で明確にすること。
⑷ 移行計画に基づいて、移行に必要な要員、予算、設備等を確保すること。
⑸ 移行は手順書を作成し、実施すること。
⑹ 移行時のリスク対策を検討すること。
⑺ 運用及び保守に必要なドキュメント、各種ツール等は開発の責任者から引き継いでいること。
⑻ 移行は関係者に周知徹底すること。

Ⅳ. 運用業務（73）

1. 運用管理ルール（4）

⑴ 運用管理ルール及び運用手順は、運用の責任者が承認すること。
⑵ 運用管理ルールは、運用設計に基づいて作成すること。
⑶ 運用手順は、運用設計及び運用管理ルールに基づいて、規模、期間、システム特性等を考慮して作成すること。
⑷ 運用設計及び運用管理ルールに基づいて、担当責任者を定めること。

2. 運用管理（16）

⑴ 年間運用計画を策定し、責任者が承認すること。
⑵ 年間運用計画に基づいて、月次、日次等の運用計画を策定すること。
⑶ 運用管理ルールを遵守すること。
⑷ 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すること。
⑸ 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うこと。
⑹ 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うこと。
⑺ オペレータの交替は、運用管理ルールに基づいて行うこと。
⑻ ジョブスケジュール及びオペレーション実施記録を採り、ジョブスケジュールとの差異分析を行うこと。
⑼ 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すること。
⑽ 事故及び障害の影響度に応じた報告体制及び対応手順を明確にすること。
⑾ 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すること。
⑿ 事故及び障害の原因を究明し、再発防止の措置を講じること。
⒀ 情報システムのユーザに対する支援体制を確立すること。
⒁ 情報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すること。
⒂ 情報システムの稼動に関するモニタリング体制を確立すること。
⒃ 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ること。

3. 入力管理（5）

⑴ 入力管理ルールを定め、遵守すること。

⑵ データの入力は、入力管理ルールに基づいて漏れなく、重複なく、正確に行うこと。
⑶ 入力データの作成手順、取扱い等は誤謬防止、不正防止、機密保護等の対策を講じること。
⑷ データの入力の誤謬防止、不正防止、機密保護等の対策は有効に機能すること。
⑸ 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うこと。

4. データ管理 (10)
⑴ データ管理ルールを定め、遵守すること。
⑵ データへのアクセスコントロール及びモニタリングは、有効に機能すること。
⑶ データのインテグリティを維持すること。
⑷ データの利用状況を記録し、定期的に分析すること。
⑸ データのバックアップの範囲、方法及びタイミングは、業務内容、処理形態及びリカバリの方法を考慮して決定すること。
⑹ データの授受は、データ管理ルールに基づいて行うこと。
⑺ データの交換は、不正防止及び機密保護の対策を講じること。
⑻ データの保管、複写及び廃棄は、誤謬防止、不正防止及び機密保護の対策を講じること。
⑼ データに対するコンピュータウイルス対策を講じること。
⑽ データの知的財産権を管理すること。

5. 出力管理 (7)
⑴ 出力管理ルールを定め、遵守すること。
⑵ 出力情報は、漏れなく、重複なく、正確であることを確認すること。
⑶ 出力情報の作成手順、取扱い等は、誤謬防止、不正防止及び機密保護の対策を講じること。
⑷ 出力情報の引渡しは、出力管理ルールに基づいて行うこと。
⑸ 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うこと。
⑹ 出力情報のエラー状況を記録し、定期的に分析すること。
⑺ 出力情報の利用状況を記録し、定期的に分析すること。

6. ソフトウェア管理 (9)
⑴ ソフトウェア管理ルールを定め、遵守すること。
⑵ 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、有効に機能すること。
⑶ ソフトウェアの利用状況を記録し、定期的に分析すること。
⑷ ソフトウェアのバックアップの範囲、方法及びタイミングは、業務内容及び処理形態を考慮して決定すること。
⑸ 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うこと。
⑹ ソフトウェアの保管、複写及び廃棄は、不正防止及び機密保護の対策を講じること。
⑺ 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ること。
⑻ ソフトウェアの知的財産権を管理すること。
⑼ フリーソフトウェアの利用に関し、組織体としての方針を明確にすること。

7. ハードウェア管理 (6)
⑴ ハードウェア管理ルールを定め、遵守すること。
⑵ ハードウェアは、想定されるリスクに対応できる環境に設置すること。

⑶ ハードウェアは、定期的に保守を行うこと。
⑷ ハードウェアは、障害対策を講じること。
⑸ ハードウェアの利用状況を記録し、定期的に分析すること。
⑹ ハードウェアの保管、移設及び廃棄は、不正防止及び機密保護の対策を講じること。

8. ネットワーク管理(6)
⑴ ネットワーク管理ルールを定め、遵守すること。
⑵ 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、有効に機能すること。
⑶ ネットワーク監視ログを定期的に分析すること。
⑷ ネットワークは、障害対策を講じること。
⑸ ネットワークの利用状況を記録し、定期的に分析すること。
⑹ ネットワークを利用したサービスについて、組織体としての方針を明確にすること。

9. 構成管理(4)
⑴ 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、管理すること。
⑵ ソフトウェア、ハードウェア及びネットワークの構成、調達先、サポート条件等を明確にすること。
⑶ 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すること。
⑷ 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、計画的に実施すること。

10. 建物･関連設備管理(6)
⑴ 建物及び関連設備は、想定されるリスクに対応できる環境に設置すること。
⑵ 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ること。
⑶ 関連設備は、適切な運用を行うこと。
⑷ 関連設備は、定期的に保守を行うこと。
⑸ 関連設備は、障害対策を講じること。
⑹ 建物及び室への入退の管理を記録し、定期的に分析すること。

Ⅴ. 保守業務(19)

1. 保守手順(3)
⑴ 保守ルール及び保守手順は、保守の責任者が承認すること。
⑵ 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すること。
⑶ 保守時のリスクを評価し、必要な対応策を講じること。

2. 保守計画(3)
⑴ 保守計画はユーザ及び保守の責任者が承認すること。
⑵ 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うこと。
⑶ 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すること。

3. 保守の実施(3)
⑴ システム設計書、プログラム設計書等は、保守計画に基づいて変更し、ユーザ及び保守の責任者

が承認すること。
⑵ 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すること。
⑶ 変更したプログラム設計書に基づいてプログラミングしていることを検証すること。

4. 保守の確認(5)
⑴ 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うこと。
⑵ 変更したプログラムは、影響範囲を考慮してテストを行うこと。
⑶ 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すること。
⑷ 変更したプログラムのテストの結果は、ユーザ、運用及び保守の責任者が承認すること。
⑸ 変更したプログラムのテストの結果を記録及び保管すること。

5. 移行(3)
⑴ 移行手順は、移行の条件を考慮して作成すること。
⑵ 変更前のプログラム及びデータのバックアップを行うこと。
⑶ 運用及び保守の責任者は、他の情報システムへ影響を与えないことを確認すること。

6. 情報システムの廃棄(2)
⑴ 旧情報システムは、リスクを考慮して廃棄計画を策定し、ユーザ、運用及び保守の責任者の承認を得て廃棄すること。
⑵ 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すること。

VI. 共通業務(76)

1. ドキュメント管理(9)

1.1 作成(5)
⑴ ドキュメントは、ユーザ部門及び情報システム部門の責任者が承認すること。
⑵ ドキュメント作成ルールを定め、遵守すること。
⑶ ドキュメントの作成計画を策定すること。
⑷ ドキュメントの種類、目的、作成方法等を明確にすること。
⑸ ドキュメントは、作成計画に基づいて作成すること。

1.2 管理(4)
⑴ ドキュメントの更新内容は、ユーザ部門及び情報システム部門の責任者が承認すること。
⑵ ドキュメント管理ルールを定め、遵守すること。
⑶ 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、更新履歴を記録すること。
⑷ ドキュメントの保管、複写及び廃棄は、不正防止及び機密保護の対策を講じること。

2. 進捗管理(6)

2.1 実施(3)
⑴ 進捗計画に基づいて方法、体制等を定め、ユーザ、企画、開発、運用及び保守の責任者が承認すること。

⑵ ユーザ、企画、開発、運用及び保守の責任者は、進捗状況を把握すること。
⑶ 進捗の遅延等の対策を講じること。

2.2 評価(3)
⑴ 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、責任者が承認すること。
⑵ 評価結果は、次工程の計画に反映すること。
⑶ 評価結果は、進捗管理の方法、体制等の改善に反映すること。

3. 品質管理(4)
3.1 計画(2)
⑴ 品質目標に基づいて品質管理の計画を定め、ユーザ、企画、開発、運用及び保守の責任者が承認すること。
⑵ 品質管理計画は、方法、体制等を明確にすること。

3.2 実施(2)
⑴ 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、責任者が承認すること。
⑵ 評価結果は、品質管理の基準、方法、体制等の改善に反映すること。

4. 人的資源管理(13)
4.1 責任･権限(3)
⑴ 要員の責任及び権限は、業務の特性及び業務遂行上の必要性に応じて定めること。
⑵ 要員の責任及び権限は、業務環境及び情報環境の変化に対応した見直しを行うこと。
⑶ 要員の責任及び権限を周知徹底すること。

4.2 業務遂行(4)
⑴ 要員は、権限を遵守すること。
⑵ 作業分担及び作業量は、要員の知識、能力等から検討すること。
⑶ 要員の交替は、誤謬防止、不正防止及び機密保護を考慮して行うこと。
⑷ 不測の事態に備えた代替要員の確保を検討すること。

4.3 教育･訓練(4)
⑴ 教育及び訓練に関する計画及びカリキュラムは、人的資源管理の方針に基づいて作成及び見直しを行うこと。
⑵ 教育及び訓練に関する計画及びカリキュラムは、技術力の向上、業務知識の習得、情報システムの情報セキュリティ確保等から検討すること。
⑶ 教育及び訓練は、計画及びカリキュラムに基づいて定期的かつ効果的に行うこと。
⑷ 要員に対するキャリアパスを確立し、業務環境及び情報環境の変化に対応した見直しを行うこと。

4.4 健康管理(2)
⑴ 健康管理を考慮した作業環境を整えること。
⑵ 健康診断及びメンタルヘルスケアを行うこと。

5. 委託･受託(25)

5.1 計画(3)

⑴ 委託又は受託の計画は全体最適化計画に基づいて策定し、責任者が承認すること。
⑵ 委託又は受託の目的、対象範囲、予算、体制等を明確にすること。
⑶ 委託又は受託は、具体的な効果、問題点等を評価して決定すること。

5.2 委託先選定(3)

⑴ 委託先の選定基準を明確にすること。
⑵ 委託候補先に必要な要求仕様を提示すること。
⑶ 委託候補先が提示した提案書の比較検討を行うこと。

5.3 契約(8)

⑴ 契約は、委託契約ルール又は受託契約ルールに基づいて締結すること。
⑵ コンプライアンスに関する条項を明確にすること。
⑶ 再委託の可否について明確にすること。
⑷ 知的財産権の帰属を明確にすること。
⑸ 特約条項及び免責条項を明確にすること。
⑹ 業務内容及び責任分担を明確にすること。
⑺ 契約締結後の業務内容に追加及び変更が生じた場合、契約内容の再検討を行うこと。
⑻ システム監査に関する方針を明確にすること。

5.4 委託業務(7)

⑴ 委託業務の実施内容は、契約内容と一致すること。
⑵ 契約に基づき、必要な要求仕様、データ、資料等を提供すること。
⑶ 委託業務の進捗状況を把握し、遅延対策を講じること。
⑷ 委託先における誤謬防止、不正防止、機密保護等の対策の実施状況を把握し、必要な措置を講じること。
⑸ 成果物の検収は、委託契約に基づいて行うこと。
⑹ 業務終了後、委託業務で提供したデータ、資料等の回収及び廃棄の確認を行うこと。
⑺ 委託した業務の結果を分析及び評価すること。

5.5 受託業務(4)

⑴ 受託業務の実施内容は、契約内容を遵守すること。
⑵ 受託内容の進捗状況を把握し、リスク対策を講じること。
⑶ 成果物の品質管理を行うこと。
⑷ 契約に基づき、受託業務終了後、提供されたデータ、資料、機材等を返却又は廃棄すること。

6. 変更管理(6)

6.1 管理(3)

⑴ 変更管理ルールを定め、ユーザ、開発及び保守の責任者が承認すること。
⑵ 仕様変更、問題点、ペンディング事項等の変更管理案件が生じた場合、他システムの影響を考慮して決定すること。

⑶ 変更管理案件は、提案から完了までの状況を管理し、未完了案件は定期的に分析すること。

6.2 実施(3)

⑴ 変更管理案件は、変更管理ルールに従って実施すること。
⑵ 変更管理案件を実施した場合に、関連する情報システムの環境も同時に変更すること。
⑶ 変更の結果は、ユーザ、開発、運用及び保守の責任者が承認すること。

7. 災害対策(13)

7.1 リスク分析(3)

⑴ 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すること。
⑵ 情報システムの停止等により組織体が被る損失を分析すること。
⑶ 業務の回復許容時間及び回復優先順位を定めること。

7.2 災害時対応計画(6)

⑴ リスク分析の結果に基づき、事業継続計画と整合をとった災害時対応計画を策定すること。
⑵ 災害時対応計画は、組織体の長が承認すること。
⑶ 災害時対応計画の実現可能性を確認すること。
⑷ 災害時対応計画は、従業員の教育訓練の方針を明確にすること。
⑸ 災害時対応計画は、関係各部に周知徹底すること。
⑹ 災害時対応計画は、必要に応じて見直すこと。

7.3 バックアップ(2)

⑴ 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ること。
⑵ 運用の責任者は、バックアップ方法及び手順を検証すること。

7.4 代替処理・復旧(2)

⑴ ユーザ及び運用の責任者は、復旧までの代替処理手続き及び体制を定め、検証すること。
⑵ ユーザ及び運用の責任者は、復旧手続き及び体制を定め、検証すること。

附則

1. 情報セキュリティに関連する項目については、情報セキュリティ管理基準を活用することが望ましい。
2. その他、関連する基準を活用することが望ましい。

システム監査基準

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「報告基準」からなっている。

システム監査基準は、組織体の内部監査部門等が実施するシステム監査だけでなく、組織体の外部者に監査を依頼するシステム監査においても利用できる。さらに、本基準は、情報システムに保証を付与することを目的とした監査であっても、情報システムの改善のための助言を行うことを目的とした監査であっても利用できる。

システム監査の実施に当たっては、組織体における情報システムにまつわるリスクに対するコントロールの適否を判断するための尺度が必要である。システム監査は、本監査基準の姉妹編であるシステム管理基準を監査上の判断の尺度として用い、監査対象がシステム管理基準に準拠しているかどうかという視点で行われることを原則とする。しかし、システム管理基準に基づく監査に限らず、各種目的あるいは各種形態をもって実施されるシステム監査においても本監査基準を活用することができる。

システム監査基準は、昭和 60 年（1985 年）1月に策定されたもので、その後平成8年(1996 年)1月に改訂され、今回は2度目の改訂である。今回の改訂は、昨年4月に創設された情報セキュリティ監査基準との整合性を図り、従来の実施基準の主要部分を抜き出し、システム管理基準として独立させ、それぞれに大幅な加筆・修正を行ったものである。

Ⅱ. システム監査の目的

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。

Ⅲ. 一般基準

1. 目的、権限と責任

システム監査を実施する目的及び対象範囲、並びにシステム監査人の権限と責任は、文書化された規程、または契約書等により明確に定められていなければならない。

2. 独立性、客観性と職業倫理

2.1 外観上の独立性

システム監査人は、システム監査を客観的に実施するために、監査対象から独立していなければならない。監査の目的によっては、被監査主体と身分上、密接な利害関係を有することがあってはならない。

2.2 精神上の独立性

システム監査人は、システム監査の実施に当たり、偏向を排し、常に公正かつ客観的に監査判断を行わなければならない。

2.3 職業倫理と誠実性

システム監査人は、職業倫理に従い、誠実に業務を実施しなければならない。

3. 専門能力

システム監査人は、適切な教育と実務経験を通じて、専門職としての知識及び技能を保持しなければならない。

4. 業務上の義務

4.1 注意義務

システム監査人は、専門職としての相当な注意をもって業務を実施しなければならない。

4.2 守秘義務

システム監査人は、監査の業務上知り得た秘密を正当な理由なく他に開示し、又は、自らの利益のために利用してはならない。

5. 品質管理

システム監査人は、監査結果の適正性を確保するために、適切な品質管理を行わなければならない。

Ⅳ. 実施基準

1. 監査計画の立案

システム監査人は、実施するシステム監査の目的を有効かつ効率的に達成するために、監査手続の内容、時期及び範囲等について、適切な監査計画を立案しなければならない。監査計画は、事情に応じて適時に修正できるように弾力的に運用しなければならない。

2. 監査の手順

システム監査は、監査計画に基づき、予備調査、本調査及び評価･結論の手順により実施しなければならない。

3. 監査の実施

3.1 監査証拠の入手と評価

システム監査人は適切かつ慎重に監査手続を実施し、保証又は助言についての監査結果を裏付けるのに十分かつ適切な監査証拠を入手し、評価しなければならない。

3.2 監査調書の作成と保存

システム監査人は、実施した監査手続の結果とその関連資料を、監査調書として作成しなければならない。監査調書は、監査結果の裏付けとなるため、監査の結論に至った過程がわかるように秩序整然と記録し、適切な方法によって保存しなければならない。

4. 監査業務の体制

システム監査人は、システム監査の目的が有効かつ効率的に達成されるように、適切な監査体制を整え、監査計画の立案から監査報告書の提出及び改善指導（フォローアップ）までの監査業務の全体を管理しなければならない。

5. 他の専門職の利用

システム監査人は、システム監査の目的達成上、必要かつ適切と判断される場合には、他の専門職による支援を考慮しなければならない。他の専門職による支援を仰ぐ場合であっても、利用の範囲、方法、及び結果の判断等は、システム監査人の責任において行われなければならない。

6. 情報セキュリティ監査

情報セキュリティ監査については、原則として、情報セキュリティ管理基準を活用することが望ましい。

Ⅴ. 報告基準

1. 監査報告書の提出と開示

システム監査人は、実施した監査の目的に応じた適切な形式の監査報告書を作成し、遅滞なく監査の依頼者に提出しなければならない。監査報告書の外部への開示が必要とされる場合には、システム監査人は、監査の依頼者と慎重に協議の上で開示方法等を考慮しなければならない。

2. 監査報告の根拠

システム監査人が作成した監査報告書は、監査証拠に裏付けられた合理的な根拠に基づくものでなければならない。

3. 監査報告書の記載事項

監査報告書には、実施した監査の対象、実施した監査の概要、保証意見又は助言意見、制約又は除外事項、指摘事項、改善勧告、その他特記すべき事項について、証拠との関係を示し、システム監査人が監査の目的に応じて必要と判断した事項を明瞭に記載しなければならない。

4. 監査報告についての責任

システム監査人は、監査報告書の記載事項について、その責任を負わなければならない。

5. 監査報告に基づく改善指導（フォローアップ）

システム監査人は、監査の結果に基づいて所要の措置が講じられるよう、適切な指導性を発揮しなければならない。