経済産業省

システム監査基準・管理基準の改訂について

経済産業省 商務情報政策局

サイバーセキュリティ課

システム監査基準・管理基準について

昭和60年1月策定
平成8年1月、平成16年10月、平成30年4月改訂

- システム監査人がシステムの運用状況等を点検・評価し、ガバナンスやマネジメント等について一定の保証や助言を行うことで**システム監査は、システムの信頼性等を確保し、企業に対する信用を高める重要な取組**。
- 経済産業省では、**システム監査の品質の確保及び効果的な監査の実現のため、システム監査基準（システム監査人の行為規範及び監査手続の規則を規定）とシステム管理基準（監査の効率的・効果的遂行を可能にする判断の尺度を規定）を策定、公表**している。

システム監査基準：

監査人の行為規範や監査手続の規則を規定

Ⅰ．体制整備に係る基準	1　監査人の権限と責任等の明確化 2　監査能力の保持と向上 3　ニーズの把握と品質の確保
Ⅱ．監査人の独立性・客観性等に係る基準	4　監査人としての独立性と客観性の保持 5　慎重な姿勢と倫理の保持
Ⅲ．監査計画策定に係る基準	6　監査計画策定の全般的留意事項 7　リスクの評価に基づく監査計画の策定
Ⅳ．監査実施に係る基準	8　監査証拠の入手と評価 9　監査調書の作成と保管 10　監査の結論の形成
Ⅴ．監査報告とフォローアップに係る基準	11　監査報告書の作成と提出 12　改善提案のフォローアップ

システム管理基準：

監査の判断尺度となる情報システムに係る組織体制や開発・運用・保守等における基準（主旨・着眼点含む）を規定

Ⅰ　ITガバナンス
戦略方針・組織体制、資源管理等の評価・指示・モニタ等

Ⅱ　企画フェーズ
プロジェクト計画の管理、要件定義の管理、調達の管理

Ⅲ　開発フェーズ
設計・実装・テスト等の管理

Ⅳ　アジャイル開発
概要、人材の役割、プロセス

Ⅴ　運用・利用フェーズ
データ管理、ログ管理、インシデント管理等

Ⅵ　保守フェーズ
保守の実施、ソフトウェア構成管理、ライフサイクル管理等

Ⅶ　外部サービス管理
利用計画、委託先選定、契約と管理、サービスレベル管理

Ⅷ　事業継続管理
リスクアセスメント、業務継続計画・復旧計画の管理等

Ⅸ　人的資源管理
責任と権限の管理、業務遂行管理、教育・訓練の管理等

Ⅹ　ドキュメント管理
ドキュメントの作成、管理

システム監査基準・管理基準の改訂の背景・目的

- 昨今、本基準が参照する国際基準の改訂や技術の進展に伴う状況の変化等を踏まえ、**今年度、有識者や関係者を集めた検討会等を開催し、システム監査基準・管理基準の改訂・見直しを実施**。
- 改訂・見直しに当たっては、最新の技術革新や社会情勢の変化等を踏まえた監査が速やかに可能となるよう、**実施方法等の「実践部分」については切り離して別冊化し、システム監査に知見のある民間団体（日本システム監査人協会）においてアップデート等を図っていくことを予定**。

＜改訂に伴う管理等の変更＞

経済産業省

（現行）システム監査基準

（現行）システム管理基準

改　訂

●原則（What）、趣旨、解釈指針、達成目標、管理活動の例等

（改訂後）システム監査基準

（改訂後）システム管理基準

民間団体（日本システム監査人協会）

実践部分は別冊化

●実施方法（How）、実施・書式の例、管理活動例の着眼点（必要な観点や留意事項）等

システム監査基準ガイドライン

システム管理基準ガイドライン

システム監査基準の改訂案の概要①

- システム監査基準については、システム監査人の行為規範及び監査手続の規則として監査人の独立性・客観性等に関する基準や監査計画・監査報告などの監査全般に関する基準を規定。
- 今回、システム監査の意義・目的を達成するに当たり、**システム監査人の倫理が監査の前提となるものであることをより明確にするため、倫理規定部分について、基準から切り離して構成に整理**し、倫理に関して監査人が守るべき原則を明示するなどの改訂を実施予定。

＜現行のシステム監査基準＞

前文

Ⅰ．体制整備に係る基準	1　監査人の権限と責任等の明確化 2　監査能力の保持と向上 3　ニーズの把握と品質の確保
Ⅱ．監査人の独立性・客観性等に係る基準	4　監査人としての独立性と客観性の保持 5　慎重な姿勢と倫理の保持
Ⅲ．監査計画策定に係る基準	6　監査計画策定の全般的留意事項 7　リスクの評価に基づく監査計画の策定
Ⅳ．監査実施に係る基準	8　監査証拠の入手と評価 9　監査調書の作成と保管 10　監査の結論の形成
Ⅴ．監査報告とフォローアップに係る基準	11　監査報告書の作成と提出 12　改善提案のフォローアップ

改訂

＜改訂案＞

前文
システム監査の意義と目的
監査人の倫理

Ⅰ．監査の属性に係る基準	1　監査に係る権限と責任等の明確化 2　専門的能力の保持と向上 3　ニーズの把握と品質の確保 4　監査の独立性と客観性の保持 5　監査能力及び正当な注意と秘密の保持
2．監査の実施に係る基準	6　監査計画の策定 7　監査計画の種類 8　監査証拠の入手と評価 9　監査調書の作成と保管 10　監査の結論の形成
3．監査の報告に係る基準	11　監査報告書の作成と報告 12　改善提案のフォローアップ

【改訂概要】

- 監査人が意識すべき**倫理に関する部分については基準と切り離す構成に整理し、守るべき原則として①誠実性、②客観性、③能力及び正当な注意、④秘密の保持**を明示
- 基準に**監査人のみならず、組織としての対応の在り方、デジタル技術・システム開発手法の変化によるリスクへの留意点**や**監査を効率的・効果的に進めるための手法（リスクアプローチ）**等を追記
- **アジャイル監査などの新たな監査手法例や監査における報告書書式例などはガイドラインとして別冊化**を予定

システム監査基準の改訂案の概要②

- 改訂案は、IIA国際基準、IIA倫理要綱等の最近の改訂を踏まえ、それらを参照のうえ記載を更新。
- DX、アジャイル開発等、システム監査を巡る情報技術環境の継続的な変化やシステム監査に対するニーズの多様化を踏まえ、基準の構成や内容を見直し、実施方法等のより具体的な内容はガイドラインに記載。

	<改訂案>	<基準・主旨・解釈指針への主な追加点>	<ガイドラインへの主な移行点>
	前文 システム監査の意義と目的 **監査人の倫理**	• 監査人の倫理として監査人が守るべき4つの原則（基準5から独立）	–
Ⅰ．監査の属性に係る基準	1　監査の権限と責任等の明確化	• 組織の責任の明示・システム監査の最終的な責任の所在 • システム監査の外部委託にあたっての利害関係の在り方	• システム監査に関する規程に記載する事項、規程の承認主体 • システム監査の外部への委託契約書等の文書に記載する事項
	2　監査能力の保持と向上	• システム監査を行う組織総体としての監査能力の具備	• システム監査に求められる知識や技能
	3　ニーズの把握と品質の確保	• システム監査終了後のアンケート調査等による品質の維持向上	• システム監査の目的決定の背景にあるニーズの具体例
	4　監査の独立性と客観性の保持	• 監査対象先から独立したシステム監査人による監査実施の必要性	• 組織体のケースごとのシステム監査人の独立性確保の具体例
	5　監査能力及び正当な注意と秘密の保持	• 専門的な知識・技能を有する監査人によるシステム監査の実施の必要性	• 「正当な注意」の具体的解説 • 職業倫理が求められるシステム監査関連団体の具体例

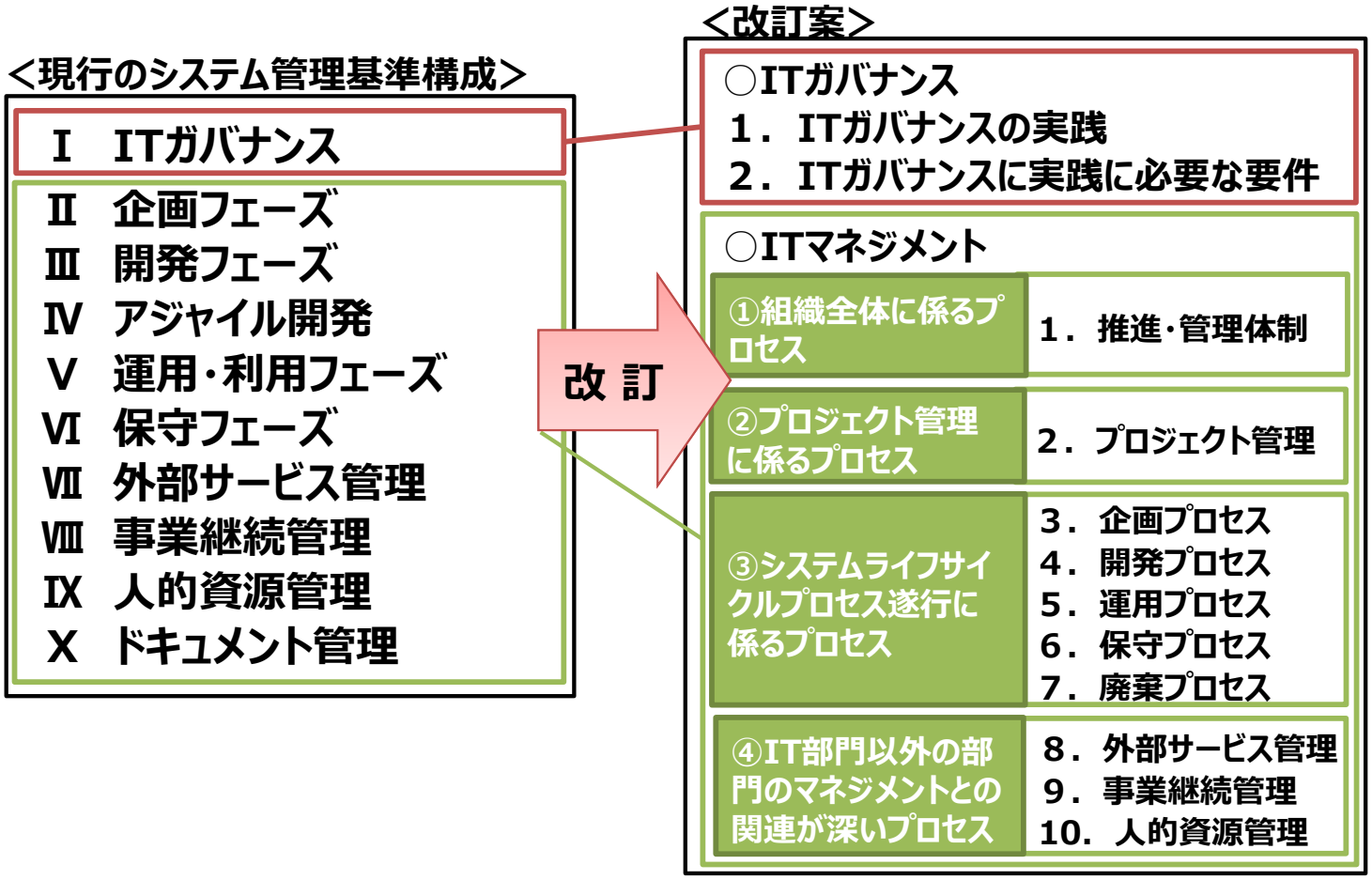
システム監査基準の改訂案の概要③

● （続き）

	<改訂案>	<基準・主旨・解釈指針への主な追加点>	<ガイドラインへの主な移行点>
2．監査の実施に係る基準	6　監査計画の策定	• リスク・アプローチに基づいた監査計画の策定（現行基準7から移動） • システム監査の対象範囲 • ガバナンス、マネジメント、コントロールの観点からの監査	• リスク・アプローチの解説、留意点（現行基準7から移動） • 監査計画を策定する利点の具体例 • システム監査対象範囲の具体例 • ガバナンス、マネジメント、コントロールの各観点の解説 • （アジャイル開発によるシステムの監査は個別のガイドラインを作成予定）
	7　監査計画の種類	• 中長期計画、年度計画、及び個別監査計画に分けた監査計画の策定	• 各監査計画に含まれる項目の具体例
	8　監査証拠の入手と評価	• 語句の見直し等	• 監査証拠の入手手続の解説、具体例、留意点
	9　監査調書の作成と保管	• 語句の見直し等	• 監査調書の作成と保管の解説、具体例、留意点
	10 監査の結論の形成	• 語句の見直し等	• 監査の結論を導くにあたっての解説、具体例、留意点
3．監査の報告に係る基準	11　監査報告書の作成と報告	• 語句の見直し等 • 監査の依頼者に加え、適切な関係者への監査報告書の配布	• 適切な関係者の具体例 • 監査報告書の作成にあたっての望ましい具体的報告事項、留意点
	12　改善提案のフォローアップ	• 語句の見直し等	• フォローアップの実施にあたっての望ましい具体的実施事項、留意点

システム管理基準の改訂案の概要①

- システム管理基準については、ITシステムの利活用のあるべき姿を示すIT戦略の方針や体制等のガバナンスに関する基準とITシステムの開発・運用等のマネジメントに関する基準を規定。
- 今回、IT利活用による新たな開発技術やボーダーレスとなっているIT環境のボーダーレス化等の現状を踏まえ、**アジャイル開発やAI活用等の新たな手法・技術等にも対応できるよう、国際規格の考え方なども踏まえながら、各プロセスを細分化して再整理**するなどの改訂を実施予定。



【改訂概要】

- **ITガバナンス部分につき、**国際規格の考え方も踏まえ、**実践のための直接的な活動に係るプロセスと実践に当たって必要となる要件に係るプロセスに分類し再整理**
- **ITマネジメント部分につき、**国際規格のプロセス区分も参考にしつつ、**新たな手法・技術等にも対応できるよう、各プロセスを細分化し再整理**
- **アジャイル開発を含む様々なプロセスモデルや情報システムの導入形態に対応する留意点**については、**ガイドラインとして別冊化**を予定

システム管理基準の改訂案の概要②

- ITガバナンス編の章構成・ITマネジメント編との関連、記載のポイントを以下に示す。

※同一の＜タグ名＞の記載がある項目について関連があることを意味する

大分類（編）	中分類（章）	小分類（節）	II. ITマネジメント編との関連※	記載のポイント
I. ITガバナンス	1. ITガバナンスの実践	1.1 経営戦略とビジネスモデルの確認	＜IT戦略ビジョン＞（経営戦略とビジネスモデル及びそのビジネス成果はITマネジメント全体と関連）	経営陣によるITガバナンスの実践のための直接的な活動に関わるプロセスを記載
		1.2 IT戦略の策定	＜IT戦略（ITガバナンス方針とIT基本計画）＞	
		1.3 効果的なITパフォーマンスの確認と是正	＜ITパフォーマンス評価＞	
		1.4 実行責任及び説明責任の明確化		
	2. ITガバナンス実践に必要な要件	2.1 ステークホルダーへの対応	＜IT戦略＞	ITガバナンスの実践を支える活動に関わるプロセスを記載
		2.2 取締役会等のリーダーシップ		
		2.3 データ利活用と意思決定	＜ITガバナンス方針＞	
		2.4 リスクの評価と対応	＜ITリスク管理方針＞ ＜事業継続に関する方針＞	
		2.5 社会的責任と持続性	＜ITガバナンス方針＞	

システム管理基準の改訂案の概要③

- ITマネジメント編の章構成・ITガバナンス編との関連、記載のポイントを以下に示す。

※1 赤字は現行基準にも存在するプロセス、青字はJIS X 0170に存在しないプロセス
※2 同一の＜タグ名＞の記載がある項目について関連があることを意味する

大分類（編）	中分類（章）	小分類（節） ※1	I. ITガバナンス編との関連 ※2	記載のポイント
II. ITマネジメント	1. 推進・管理体制	1.1 体制と機能	＜IT戦略ビジョン＞ ＜IT戦略＞	現行基準のITガバナンスの記載事項から体制に関する事項を移動
		1.2 システムライフサイクルモデル管理		
		1.3 ITアーキテクチャ管理		
		1.4 資源配分管理		
		1.5 品質管理体制		
		1.6 知識資産管理		
	2. プロジェクト管理	2.1 プロジェクト計画の策定と承認	＜IT戦略ビジョン＞ ＜IT戦略＞	
		2.2 プロジェクト実行と管理		
		2.3 プロジェクト意思決定管理		プロジェクトレベル（業務上）の意思決定管理について記載
		2.4 プロジェクトリスク管理	＜ITリスク管理方針＞	
		2.5 調達管理	＜IT戦略＞	
		2.6 外部委託管理	＜IT戦略＞	
		2.7 構成・変更管理		
		2.8 情報管理	＜ITガバナンス方針＞	
		2.9 ドキュメント管理		
		2.10 プロジェクトの生産性等の測定		品質、コスト、納期などの指標に基づく測定プロセスについて記載
		2.11 情報システムの品質保証		

システム管理基準の改訂案の概要④

- （続き）

※1 赤字は現行基準にも存在するプロセス、青字はJIS X 0170に存在しないプロセス
※2 同一の＜タグ名＞の記載がある項目について関連があることを意味する

大分類（編）	中分類（章）	小分類（節） ※1	I. ITガバナンス編との関連 ※2	記載のポイント
II. ITマネジメント	3. 企画プロセス	3.1 ビジネス分析	＜IT戦略＞	成果物：ビジネス要件仕様
		3.2 業務要件定義		成果物：業務要件仕様
		3.3 システム要件定義		成果物：システム要件仕様（機能・非機能要件仕様）
		3.4 基本設計		成果物：基本設計仕様
		3.5 詳細設計		成果物：詳細設計仕様
		3.6 実現可能性及び効果の分析		技術面のアセスメントに必要な情報を提供するプロセスについて記載
	4. 開発プロセス	4.1 実装		
		4.2 統合		実装されたシステム要素を組み立てるプロセスについて記載
		4.3 検証		「正しく製品が作られた」ことを判断するプロセスについて記載
		4.4 ユーザ受入テスト		「正しい製品が作られた」ことを判断するプロセスについて記載
		4.5 本番環境への移行		
		4.6 稼動後評価と報告	＜ITパフォーマンス評価＞へのフィードバック	稼働したシステムの評価については、「稼働後評価と報告」を通じてITガバナンスへフィードバックされる

システム管理基準の改訂案の概要⑤

- （続き）

※1 赤字は現行基準にも存在するプロセス、青字はJIS X 0170に存在しないプロセス
※2 同一の＜タグ名＞の記載がある項目について関連があることを意味する

大分類（編）	中分類（章）	小分類（節）※1	I. ITガバナンス編との関連 ※2	記載のポイント
II. ITマネジメント	5. 運用プロセス	5.1 運用体制の整備	＜IT戦略＞	管理活動の例は、JIS Q 20000も参考にして記載 システムの運用効果については、「運用の評価と報告」を通じてITガバナンスへフィードバックされる
		5.2 運用計画		
		5.3 運用の実施		
		5.4 運用における構成・変更管理		
		5.5 インシデント・問題管理		
		5.6 サービスレベル管理		
		5.7 運用の監視と記録		
		5.8 運用の評価と報告	＜ITパフォーマンス評価＞へのフィードバック	
	6. 保守プロセス	6.1 保守体制の整備	＜IT戦略＞	システムの保守作業実施結果については、「実施結果の記録と報告」を通じてITガバナンスへフィードバックされる
		6.2 保守計画		
		6.3 保守作業の実施		
		6.4 保守作業の検証		
		6.5 本番環境への適用		
		6.6 実施結果の記録と報告	＜ITパフォーマンス評価＞へのフィードバック	

システム管理基準の改訂案の概要⑥

- （続き）

※1 赤字は現行基準にも存在するプロセス、青字はJIS X 0170に存在しないプロセス
※2 同一の＜タグ名＞の記載がある項目について関連があることを意味する

大分類（編）	中分類（章）	小分類（節）※1	I. ITガバナンス編との関連 ※2	記載のポイント
II. ITマネジメント	7. 廃棄プロセス	7.1 廃棄計画	＜IT戦略＞	
		7.2 廃棄の実施		
		7.3 廃棄結果の検証		
	8. 外部サービス管理	8.1 外部サービス利用計画の策定	＜IT戦略＞	クラウドサービスを含む外部サービスの利用において留意すべき特有の事項をまとめて記載 外部サービスの利用効果については、「外部サービスの評価」を通じてITガバナンスへフィードバックされる
		8.2 外部サービスの選定と契約		
		8.3 外部サービスの運用管理		
		8.4 外部サービスの評価	＜ITパフォーマンス評価＞へのフィードバック	
		8.5 サービスレベル管理		
	9. 事業継続管理	9.1 リスクアセスメント	＜事業継続に関する方針＞	従来は、業務継続管理を対象としていたため、JIS Q 22301等を参考にして節を見直し 事業継続管理の結果については、「業務継続計画の評価及び見直し」を通じてITガバナンスへフィードバックされる
		9.2 業務継続計画の策定		
		9.3 業務継続計画の管理		
		9.4 訓練、演習及びテストの実施		
		9.5 業務継続計画の評価及び見直し	＜ITパフォーマンス評価＞へのフィードバック	

システム管理基準の改訂案の概要⑦

- （続き）

※1 赤字は現行基準にも存在するプロセス、青字はJIS X 0170に存在しないプロセス
※2 同一の＜タグ名＞の記載がある項目について関連があることを意味する

大分類（編）	中分類（章）	小分類（節） ※1	I. ITガバナンス編との関連 ※2	記載のポイント
II. ITマネジメント	10. 人的資源管理	10.1 人的資源管理計画	＜IT戦略ビジョン＞ ＜IT戦略＞ ＜ITパフォーマンス評価＞へのフィードバック	人的資源管理は、JIS X 0170にもあるが、より幅広い観点で記載 人的資源管理の結果については、「人的資源管理計画」の「評価、検証及び見直し」を通じてITガバナンスへフィードバックされる
		10.2 責任と権限の管理		
		10.3 業務遂行の管理		
		10.4 教育・訓練の管理		
		10.5 健康管理		
		10.6 要員のエンゲージメント向上		

改訂スケジュール予定

- **①システム監査基準及び③システム管理基準については、意見公募手続を経て、2022年度中に改訂予定。**
- **①～④の公表時期は、**国際規格の動向等を踏まえる必要がある**②システム監査ガイドライン及び④システム管理ガイドラインの改訂完了時期に合わせ、2023年度前半を予定（改訂版の施行時期は準備期間等を考慮し、2023年度後半を予定）。**