システム監査入門

（システム監査の理解に向けて）

認定ＮＰＯ法人　日本システム監査人協会（ＳＡＡＪ）
（東北支部）

[Ver. 1.0　2025年 11月]

＜　前　文　＞

現「システム監査基準」（令和 5 年(2023 年)4 月 26 日）では、「システム監査とは、監査人が、一定の基準に基づいてＩＴシステムの利活用に係る検証・評価を行い、ガバナンスやマネジメント等について、一定の保証や改善のための助言を行うものであり、システムの信頼性等を確保し、企業等に対する信用を高める重要な取組である。」とあり、システム監査の専門家であるシステム監査人がシステム監査を行うための基準についての内容となっている。

また、専門家であるシステム監査人を対象とした基準であるため、専門家でない人たちには、構造・構成及び時系列の把握がしにくくなっていると思われる。

システム監査の主体は依頼者であることから、依頼側からのアプローチができるものが必要と考え、システム監査人の視点からではなく、監査を依頼する側の視点でシステム監査を把握できるようにするために、本書「システム監査入門」を作成した。

本書は、依頼者（経営者やシステム開発・運用等の依頼元等）やシステム監査に取り組もうとする人でもわかりやすいように、システム監査基準からポイントとなる部分を抜き出し、再編成して、加筆修正を行ったものである。

＜基となる資料＞

1）『システム監査基準』
（経済産業省、2023／令和 5 年 4 月 26 日）

2）『システム監査基準ガイドライン』
（特定非営利活動法人　日本システム監査人協会(SAAJ)、
2023／令和 5 年 8 月 10 日）

3）『システム監査基準テーマ別ガイドライン
リスク・アプローチによる IT マネジメントを対象とした
監査計画の策定方法に関するガイドライン』
（特定非営利活動法人　日本システム監査人協会(SAAJ)、
2025／令和 7 年 1 月 25 日）

4）『システム監査を知るための小冊子
～情報社会に不可欠なシステム監査～(改定第 4 版)』
（認定 NPO 法人　日本システム監査人協会(SAAJ)、
2025 年 2 月 21 日）

5）『保証型システム監査の実践
―システム監査業務の　さらなる深化に向けてー』
（NPO 法人　情報システム監査普及機構(J-AISA)、
2022 年 9 月 15 日）

6）『システム監査技術者試験（レベル４）シラバス（Ver.6.1)』
（独立行政法人　情報処理推進機構(IPA)、2023 年 12 月）

7）『情報システム監査　実践マニュアル（第 3 版)』
（認定 NPO 法人　日本システム監査人協会(SAAJ)、
2020 年 6 月 12 日）
（※「第 2 部　システム監査の実践方法」）

目　次

目　次

1．概要

1.1　ニーズ

現代社会において、ネットワークを含む情報システムは重要なインフラとなっている。ネットワークや情報システムに不具合が発生すると、そのまま、社会生活においても障害となってしまうことになる。（※ネットワークも通信システムと言える）

※例として

- 航空会社の情報システムの不具合による航空機による運航不能や電車の運行システムの不具合による電車の運行停止で移動ができなくなる
- 銀行の情報システムの不具合による ATM 停止で現金引出し等ができなくなる
- 携帯電話回線の不具合による通話や情報のやり取りができないことで業務が停滞する
- マイナンバー管理システムの不具合により他人の情報が引き出されることや自分の情報を引き出すことが出来ないことで病院や役所での処理ができなくなる

等々が挙げられる。

提供する情報システムは運用開始後に問題や障害が発生しないようにし、社内外の利用者が安全に信頼して使えるようにすることが重要である。

情報システムを提供する者は、情報システムの運用にあたって、利用者からの信頼を得ておくことが必要となってきている。

事前に情報システムの安全性や有効性を検証・評価し、明示することで利用者から信頼を得ることができる。

そのためには、情報システムを監査人等の第三者的立場の人によって検証・評価し、安全性、信頼性、さらに有効性、効率性について一定の保証を得ておくことが有効である。

つまり、

- 情報システムの運用にあたって、情報システムや運用体制に**問題点はないか**、運用開始後に**障害が発生するようなことはないか**を知りたい。

・情報システムの運用にあたり、**利用者や利害関係者の信頼を得たい**／信頼を回復したい。
・また、情報システムは業務の**効率化に寄与しているか**を知りたい。
・さらに、情報システムは組織体の**目標達成に寄与しているか**を知りたい。

などが求められており、これらのニーズに対応するためにシステム監査が必要となる。

尚、「システム監査基準」の「前文(2 段目)」には以下のように記載されている。

「今日社会での IT や情報システム、さらにはデータ・情報（ 本監査基準において、IT、情報システム、データ・情報をまとめた概念として「IT システム」という。）の利活用は、会社やその他組織体の諸活動全般に及んでいる。IT システムの戦略的利活用は、組織体の価値の向上や会社の競争力の維持、向上を図る上で不可欠である一方、それに伴いリスクも増大している。組織体が適切にリスク・マネジメントを行い、価値向上のために **IT システムの利活用を適切に行うことを確実にするため**に、システム監査が効果的・効率的に行われることが必要である。」

1.2　システム監査とは

「システム監査基準」の「前文」の「システム監査基準の意義と適用上の留意事項」には以下のように記載されている。

「システム監査とは、監査人が、一定の基準に基づいて IT システムの利活用に係る**検証・評価**を行い、ガバナンスやマネジメント等について、**一定の保証**や**改善のための助言**を行うものであり、**システムの信頼性等を確保**し、**企業等に対する信用を高める**重要な取組である。」

また、「システム監査基準」の「システム監査の意義と目的」には以下のように記載されている。

「システム監査とは、専門性と客観性を備えた監査人が、一定の基準に基づいてITシステムの利活用に係る検証・評価を行い、監査結果の利用者にこれらのガバナンス、マネジメント、コントロールの適切性等に対する保証を与える、又は改善のための助言を行う監査である。」

つまり、システム監査とは、専門性と客観性を備えた監査人が、一定の基準に基づいてガバナンス、マネジメント、コントロールの視点から、ITシステムの利活用に係る検証・評価を行い、利用者にこれらのガバナンス、マネジメント、コントロールの適切性等に対する保証を与える、又は改善のための助言を行う行為と言える。

※尚、監査による保証とは「Assurance」であり、「Guarantee」ではない。「Assurance」とは、定期健康診断や車検のように、「検証・評価時点で良好な状況」であることを明言したものであり、「Guarantee」は、家電における保証のように「製造・販売後の動作について問題が起きない」ことを明言したものである。

1.3　システム監査の目的

まず、「システム監査基準」の「システム監査の意義と目的」には以下のように記載されている。

「また、システム監査の目的は、ITシステムに係るリスクに適切に対応しているかどうかについて、監査人が**検証・評価**し、もって保証や助言を行うことを通じて、組織体の経営活動と業務活動の**効果的かつ効率的な遂行**、さらにはそれらの**変革を支援**し、組織体の**目標達成に寄与**すること、及び利害関係者に対する**説明責任を果たす**ことである。」

システム監査の目的としては、システム監査を通じて、

・情報システムや運用体制の問題点の洗い出しや障害発生リスクの事前の洗い出しを行い、運用開始前に情報システムや運用体制の**改善を行う**こと。

・情報システムの検証・評価の結果を明示することで、利用者から安心と信頼を得ることができるようになることや利害関係者に対する**説明責任を果たす**こと。
・また、情報システムを使うことで**業務を効果的、効率的に行うことができる**ようになること。
・さらに、それらの変革を支援し、組織体の**目標達成に寄与**すること。

などが挙げられる。　（※詳細は 1.4）

※「監査」とは、
・対象：企業や自治体などあらゆる組織体において、
・内容：経営や業務活動が適切に行われていることを、
法令や規程などに照らし合わせて点検・評価し、
・目的：その活動が適切でなければ指摘し、
正しい方向へ誘導すること。
（会計監査に代表される一部の監査では適切であることを
外部へ保証すること。）

※監査の種類
・主体による分類：「内部監査」「外部監査」
・対象による分類：「業務監査」「会計監査」など
・目的による分類：「助言型監査」「保証型監査」
保証型監査は独立した第三者の立場からの
監査（外部監査）が望ましい
（例：会計監査では財務諸表が適正に作成されていることを
株主に保証する必要がある、独立した第三者による
保証が必要）
（『システム監査を知るための小冊子』（SAAJ、2024）より）

1.4　目的別分類

・システム監査では、対象とする情報システムの開発・運用の状況により、実施する監査は「**助言型監査**」と「**保証型監査**」に分かれる。
・助言型システム監査は、情報システムの開発・運用の完成度が低い場合に、**是正や改善を行なうことを目的として**行われる。

・保証型システム監査は、情報システムの開発・運用の完成度が高い場合に、**内部および外部へ保証することを目的として**行われる。
・保証型システム監査を行うには、最初に助言型システム監査を行って情報システムの開発・運用の状況の完成度を高めておく必要がある。

・「システム監査基準」の【基準３】では、ニーズと目的別に監査パターンを記載している。

１）経営者がITシステムのマネジメント機能について保証を得るため（保証型）※J-AISAの経営者主導方式

２）経営者が自組織体のシステム管理について指摘や改善提案の助言を得るため（助言型）

３-1）委託者が委託先の管理レベルを判断するため（保証型）※J-AISAの委託者主導方式

３-2）受託者が自社の管理レベルを判断してもらえるようにするため（保証型）※J-AISAの受託者主導方式

３-3）社会的責任を負う組織体や行政組織が不特定多数の利害関係者に向けて説明責任を果たすため（保証型）※J-AISAの社会主導方式

※尚、助言型の監査パターンとしては、２種類が考えられる。

２-1）経営者が自組織体のシステム管理について指摘や改善提案の助言を得るため　（助言型の経営者主導方式）

２-2）委託者が委託先のシステム管理について指摘や改善提案の助言を得るため　（助言型の委託者主導方式：基準になし）（親会社が子会社のシステム管理について監督している場合、ホールディングス等）

※『保証型システム監査の実践』(情報システム監査普及機構 J-AISA、2022)では、「システム監査基準」の【基準３】を基に保証型監査を４つに分類して、詳細を記載している。

１）経営者主導方式：経営者が自組織体の状況を知るため

２）委託者主導方式：委託者が委託先の状況を知るため

3）受託者主導方式：受託者が自組織体の状況を委託先に知らせるため
4）社会主導方式　：経営者が自組織体の状況について説明責任を果たすため

・また、対象別に（監査の視点別に）、監査パターンを記載している。（保証型、助言型）

1）IT システムのガバナンスを対象とした監査
2）情報システムのマネジメントを対象とした監査
3）情報システムのコントロールを対象とした監査

（※「監査の視点」については 1.6）

1.5　実施方法別分類

・システム監査は監査計画を策定し実施すること。
・監査計画には、「**中長期計画**」「**年度計画**」「**個別監査計画**」がある。　・・・【基準６】

・また、システム監査の実施方法には「**単発型**」と「**定期型**」が考えられる。
・情報システムに大きな問題や障害があり早急に改善するために単発的にシステム監査が行われる。
（※疾病の発病に対する診察に似ている。）
・開発・運用している情報システムについて内部または外部に（一時的に）保証するために、単発的にシステム監査が行われる。　（※生命保険加入のための健康診断に似ている。）
・「単発型」では「個別監査計画」に基づいて監査が行われる。（「中長期計画」「年度計画」はない。）
・情報システムに大きな問題や障害はないがリスク管理の一部として定期的にシステム監査が行われる。
（※定期健康診断に似ている。）

・開発・運用している情報システムについて内部または外部に定期的に保証を行うために定期的にシステム監査が行われる。　（※車検やＱＣ認証、Ｐマーク認証等と似ている。）

・「定期型」では「中長期計画」「年度計画」「個別監査計画」に基づいて行われる。

1.6　システム監査の視点

・システム監査は、監査の目的に基づき、以下の視点から検証する。　・・・【基準６】

①．**ガバナンス**の視点：
取締役会等の経営監督状況を検証・評価する。
（取締役会等が経営者に対して、経営目的や経営戦略に沿うように、指示、監督、是正等を適切に行っているか）

②．**マネジメント**の視点：
経営者の経営管理状況を検証・評価する。
（経営者による方向づけに基づいて、PDCA サイクルが確率され、かつ適切に運用されているか）

③．**コントロール**の視点：
業務プロセス等の運用状況を検証・評価する。
（業務プロセス等において、リスクに応じたコントロールが適切に組み込まれ、機能しているか）

④．**総合**的視点：
上記①②③の視点に加えて、ガバナンス、マネジメント、コントロールの統合状況を検証・評価する。
（ガバナンス、マネジメント、コントロールが体系的に統合されて有効に機能しているか）

1.7　リスク・アプローチ

「システム監査基準」の【基準６】のリスク・アプローチをまとめると以下のようになる。

・システム監査におけるリスク・アプローチとは、
『ＩＴシステムに係るリスク』の大きさに応じて
「監査の人員や時間」を充てることにより、
監査を効果的かつ効率的に行う監査の実施方法である。

・リスク・アプローチとは、
監査の網羅性（監査対象全般に対するリスク評価）と
効率性（リスクに応じた監査の実施）を
両立させるための方法である。
（※保証を目的とした場合と助言を目的とした場合でリスク評価が異なる）

・「**システム監査に係るリスク**」:

１）「**監査対象に対するリスク**」

①．固有リスク：IT システムに係るリスク

②．統制リスク：固有リスクの発生防止、適時の発見、是正がされないリスク

③．残存リスク：固有リスクをコントロール実施後も残るリスク

２）「**監査実施に係るリスク**」

①．重要な影響のあるリスクを発見できないリスク

②．（監査リスクを）合理的に低い水準まで抑えられないリスク

・リスク・アプローチの監査を実施する前提となるのは、
「監査対象に対する適切なリスク」及び「監査実施に係る適切なリスク」の「識別」「分析」「評価」である。

1.8　システム監査の主な流れ（例）

1）「助言型監査」を単発的に行う場合の主な流れ
- 監査依頼（監査依頼契約）
- 個別監査計画の策定
- 監査（予備調査、本調査）　・・・(監査人)
- 監査報告書の作成　・・・(監査人)
- 監査報告会の開催
- 是正・改善
- フォローアップ　・・・(監査人)

2）「保証型監査」を単発的に行う場合の主な流れ
- 言明書の作成
- 監査依頼（監査依頼契約）
- 個別監査計画の策定
- 監査（予備調査、本調査）　・・・(監査人)
- 監査報告書の作成　・・・(監査人)
- 監査報告会の開催

3）「助言型監査」を定期的に行う場合の主な流れ
- 監査に関する規制の整備
- 中長期計画、年度計画の策定
- 監査依頼
- 個別監査計画の策定
- 監査（予備調査、本調査）　・・・(監査人)
- 監査報告書の作成　・・・(監査人)
- 監査報告会の開催
- 是正・改善
- フォローアップ　・・・(監査人)

4）「保証型監査」を定期的に行う場合の主な流れ
- 監査に関する規定の整備
- 中長期計画、年度計画の策定
- 言明書の作成
- 監査依頼
- 個別監査計画の策定
- 監査（予備調査、本調査）　・・・(監査人)
- 監査報告書の作成　・・・(監査人)
- 監査報告会の開催

2．監査計画

※前提：監査の対象となる情報システムの開発・運用についての管理規程がある（システム管理体制が整備されている）

2.1　監査に関する環境の整備

・システム監査の環境整備

(1) **組織的体制**の整備（独立組織の設置、社内啓発）

(2) **文書**の整備（システム監査規程等）

・・・【情報システム監査　実践マニュアル　第２部】

・システム監査を実施する意義、目的、対象範囲、並びに監査人及びシステム監査を行う組織の権限と責任は、**文書化された規程等**により定められていなければならない。

・・・【基準１】

・効果的かつ効率的なシステム監査を実現するための体制整備として、監査人及びシステム監査を行う組織の権限と責任を組織体の**内部監査規程等**によって明確にし、組織体全体に**周知**しておく必要がある。

また、システム監査を外部委託する場合には、委託先の権限と責任を契約書等の文書で明確に定めておく必要がある。

・・・【基準１】主旨

・システム監査を行う組織は、効果的かつ効率的なシステム監査を実現するため、**システム監査に関する規程を整備**する。

システム監査に関する規程は、組織体の内部監査規程の一部として、あるいは内部監査規程とは別に定められる。

システム監査に関する規程は、内部監査規程と同様の承認プロセスを経た上で、組織体全体に**周知**される。

・・・【基準１】解釈指針１．

＜システム監査に関する規程に記載する事項（例）＞

・システム監査の**目的**に関する事項

・システム監査の**対象範囲**に関する事項

・システム監査の**報告**に関する事項

・監査人及びシステム監査を行う組織の**権限・責任**に関する事項
・システム監査実施のための**監査資源**（監査時間、監査人、監査費用等）の確保に関する事項
・監査人の各種設備や情報資産へのアクセス権限に関する事項
・システム監査業務の**委託の可否**に関する事項
・監査人の**守秘義務**に関する事項

・・・【基準１】ガイドライン１．

＜託契約書等の文書に記載する事項（例）＞

・委託業務の内容に関する事項
・委託期間に関する事項
・委託費用に関する事項
・監査日程及び監査結果（**成果物**）の提出に関する事項
・委託元及び委託先の**責任範囲**に関する事項
・各種設備や情報資産等への**アクセス権限**に関する事項
・**再委託**に関する事項
・**守秘義務**に関する事項
・委託業務の進捗管理及び品質管理に関する事項

・・・【基準１】ガイドライン５．

2.2　監査計画の策定

「システム監査基準」の【基準６】の監査計画の策定についてまとめると、以下のようになる。

１）監査計画の策定

・目的：システム監査を効果的かつ効率的に実施するため（監査の網羅性を確保し、かつ「**監査リスク**」を合理的に低い水準に抑えた効果的・効率的な監査を実施するため）

※「監査リスク」:
・誤った判断を行ってしまうリスク
・監査の目的を達成できないリスク
（『システム監査基準テーマ別ガイドライン
リスク・アプローチによる IT マネジメントを

対象とした監査計画の策定方法に関するガイドライン』）

・内容：（監査の方針）目的、目標、実施時期、適用範囲、監査方法等

・対象／範囲：原則として、組織体及びその集団におけるITシステムの利活用に係る経営活動及び業務活動の全て

※注意：監査依頼元の組織体及びその集団とは限らない。（委託先監査）

・検証のための監査の視点：

①．ガバナンスの視点
②．マネジメントの視点
③．コントロールの視点
④．総合的視点

2）監査計画は、主として**リスク・アプローチ**に基づいて策定する。

3）監査計画は、状況の変化に応じて見直し、変更する。

2.3　監査計画の種類

「システム監査基準」の【基準7】の監査計画の種類をまとめると以下のようになる。（ガイドラインを含めて）

・監査計画は、**中長期計画**、**年度計画**、**個別監査計画**に分けて策定する　（※「定期型実施」の場合）

（※「単発型実施」の場合、「中長期計画」「年度計画」は策定されない）

・原則として、中長期計画、年度計画、個別監査計画は全て、**リスク・アプローチ**により策定する。

1）中長期計画：

・内容：中長期的な対応が必要な事項

・目的1：システム監査の中長期における方針を明らかにするため

また、

・目的2：システム監査を経営に貢献するものとするため
利害関係者に対する説明責任を果たすため

・情報システムの中長期計画と整合を取り、システム開発・更改計画やIT基盤の構築・更改等を踏まえて策定する。

2）年度計画：

・内容1：リスク・アプローチに基づき、年間において監査を実施すべき事項

また、

・内容2：中長期計画に基づく年間スケジュール（基本計画）

3）個別監査計画：

・内容1：年間監査計画に基づいて、個々の監査のための計画

また、

・内容2：年度の基本計画に基づいて、個々のシステム監査対象ごとに、具体的な監査スケジュールまで落し込んだ詳細計画書

※『システム監査基準ガイドライン』の【基準7】では、各計画の記載事項についての詳細な記載がある。

2.4 改善提案（及び改善計画）のフォローアップ

・監査報告書に「**改善提案**」が記載されている場合は改善状況をモニタリングし、監査報告書に監査対象先が作成した「**改善計画**」が記載されている場合は実施状況をモニタリングする。

・システム監査は、監査報告書の作成と報告をもって終了するが、監査報告書に「改善提案」及び監査対象先が作成した「改善計画」、又はそのいずれかを記載した場合には、当該改善事項が適切かつ適時に実施されているかどうかを確かめておく必要がある。

（改善の実施が適切であるかどうかをフォローアップする。）

・フォローアップは、監査対象先の責任において実施される改善を監査人が事後的に確認するという性質のものである。
・監査人による改善計画の策定及びその実行への関与は、独立性と客観性を損なうことになる。

・・・【基準 12】

その他

・中長期計画、年度計画にフォローアップのスケジュールを組み込むこと。

2.5　年度計画の報告

・年度計画に対応して，当年度に実施した結果を年度報告書として作成する。　・・・【シラバス】3-7

（※報告書に記載する事項については、シラバスを参照のこと。）

2.6　監査業務の管理

・IPA の『システム監査技術者試験シラバス』には、「4 システム監査業務の管理」として、「進捗管理」、「品質の確保」、「監査業務の改善」、「監査体制の整備」が挙げられている。

(1) 「進捗管理」: 年度計画，個別監査計画，監査手続で計画された事項の進捗管理を行う。
(2) 「品質の確保」: 個別監査計画，監査手続，監査調書，監査報告書などの内容をレビューする。
(3) 「監査業務の改善」: 監査業務の作業実績値などを集計・分析し、監査業務の改善を図る。
(4) 「監査体制の整備」: システム監査部門の責任者は，中長期の視点からシステム監査技術者を計画的に育成する。

・・・【シラバス】4

３．(個別)監査の流れ（実施フロー）

3.1　監査の流れと資料

・監査における資料と流れ

①監査証拠／確かめた結果／監査人の所見

＞　「監査調書」(監査人が到達した結論)

②「監査調書」　＞　監査の結論

③監査の結論　＞　「監査報告書」(監査の結果)

１）(個別)監査計画の策定

・「言明書」の確認（保証型監査）

・「監査計画書」の作成

・監査手続の選定

２）監査（予備調査、本調査）

・「監査証拠」の入手

・「監査証拠」の評価

（＞「監査手続に基づき確かめた結果」)

３)「監査調書」の作成

・「実施した監査手続」「入手した監査証拠」

「監査人が到達した結論」の記録

・「監査人の所見」の記載

４)「監査の結論」の導出

・指摘事項の選定

・不備・不足の事実確認（＞指摘事項）

・指摘事項の最終確認

５）監査報告書の作成

・助言型監査の場合の記載内容：監査の概要、監査の結果

・保証型監査の場合の記載内容：依頼者と監査人とが

同意した記載内容

６）監査報告

７）フォローアップ

（「監査報告書」に「改善提案」「改善計画」が記載して

ある場合）
・改善状況のモニタリング
（「改善実施状況報告書等」より）
・改善確認
・改善実施内容の検証・評価（「フォローアップ報告書」）

3.2 (個別)監査計画

3.2.1 言明書の確認

・保証型監査の場合には事前に確認しておく。
（※保証型監査における「言明書」については
『保証型システム監査の実践』(J-AISA、2023)を
参照のこと）

3.2.2 監査計画書の作成

・(個別)監査の実施前に作成する。

＜主な記載事項＞
・監査の目的
・監査の対象と範囲
・監査責任者及び監査担当者
・監査日程
・監査場所、監査対象部門
・実施すべき監査手続の概要
・監査費用の見積額
（年度計画の監査費用概算を基に算出）
・監査報告予定時期

・・・【基準７】ガイドライン４．

※留意点
・保証を目的としたシステム監査の内容と範囲は、監査人が決定する。
・助言を目的としたシステム監査の個々の助言業務の内容と範囲は、依頼者との合意による。

・・・【前文】監査人と取締役会等、経営者との関係

3.2.3　監査手続の選定

・ニーズと目的に合わせた確認内容の選定

・予備調査と本調査における証拠入手方法、手順の選定
（確認内容と証拠及びその検証・評価方法とに関連性があること。）

・監査手続は、それぞれ単独で実施される場合もあるが、一般的には、一つの監査目的に対して複数の監査手続の組合せによって構成される。
（※『ガイドライン【基準８】４.』に監査手続の組合せの例が記載されている。）

・予備調査後で本調査前に、監査手続の見直しを行うことがある。

3.3　監査

3.3.1　予備調査と本調査　・・・・【基準８】解釈指針２.

・監査手続は、「**予備調査**（事前調査）」と「**本調査**」に分けて実施する。

・予備調査：監査対象の実態を把握するプロセス

・本調査　：監査の結論を裏付けるために、十分かつ適切な監査証拠を入手するプロセス

3.3.2　監査証拠の入手

・監査計画に基づいて、監査手続を実施することによって、監査証拠を入手する。
・・・【基準８】解釈指針１.

・予備調査で必要な情報を入手する方法：
（例：関連する文書や資料等の閲覧、
監査対象部門のみならず関連部門へのインタビュー等）
・・・【基準８】解釈指針２.(2)

・十分かつ適切な監査証拠を入手する。

・・・【基準８】解釈指針２．(4)

・開発の関係者間の意思疎通を図る情報共有、コミュニケーションの仕組み、ルールが整備され、適切にルールが運用されているかを確かめることが重要である。

・・・【基準８】解釈指針６．

3.3.3　監査証拠の評価

・監査手続で入手した監査証拠から目的の到達状況を確かめる。

（＞「監査手続に基づき確かめた結果」）

・・・【基準８】

3.4　監査調書

・「実施した監査手続」「入手した監査証拠」「監査人が到達した結論」の記録

・監査の結論の基礎

・システム監査人の所見：監査結果の結論をまとめるための合理的根拠

・・・【基準９】

＜主な記載事項＞

・監査実施者及び実施日時

・監査の目的

・監査手続

・監査証拠

・監査手続に基づき確かめた結果

・発見事実（事態・事象、真因、影響等）及び発見事実に対する所見

・（監査調書のレビューが行われた場合）レビューアの氏名及びレビュー実施日

・・・【基準９】解釈指針２．

3.5 監査の結論

・監査調書の内容を詳細に検討し、合理的な根拠に基づいて、監査の結論を導く。　・・・【基準 10】

・監査の結論は、監査調書に基づいて、論理的に導く。
・・・【基準 10】解釈指針２.

・監査手続に基づき確かめた結果を、良好項目、懸案項目、非指摘項目、指摘項目に分け、監査人の所見を踏まえて、監査の結論を導く。

１）**良好項目**：監査実施時に、不備・不足がない項目

２）**懸案項目**：監査実施時に、不備・不足はないが、将来的に不備・不足となるリスクとなる項目

３）**非指摘項目**：・監査実施時に、不備・不足が発見されたが、リスクの大きさを評価した結果、問題がない・影響がないと判断した項目、
・優先順位が下位になった項目

４）**指摘項目**：監査実施時に、不備・不足があり、改善が必要な項目

・指摘事項の選定（指摘事項として改善を求めるかの判断）に当たっては、監査対象先と不備・不足についての事実確認を行い、指摘事項とすべきと判断した場合は、監査対象先に事実認識に相違ないかの最終確認を行う。
・・・【基準 10】解釈指針４.

3.6 監査報告書

3.6.1 監査報告書の作成

・監査の目的の応じた適切な形式で作成する。
・・・【基準 11】

・監査報告書の作成に際しては、正確性、客観性、簡潔性、明瞭性、理解容易性、適時性に留意
・図表等のビジュアルを利用すると効果的
・表現は建設的なものとすること。
・・・【基準 11】解釈指針１．

・保証型監査の場合の記載内容（例）
・監査概要（監査の目的、
監査の対象範囲、
監査の実施期間、
監査の実施者、
監査手続きの概要）
・監査結果（結論、
指摘事項、
改善提案、
改善計画・・・(監査対象先が作成)、
総合意見）
・・・【基準 11】解釈指針４．
・助言型監査の場合：依頼者と監査人とが同意した記載内容
・・・【基準 11】解釈指針５．
（※「3.2.2　監査計画書の作成」の留意点も参照のこと）

・取締役会等に提出するシステム監査報告書は、詳細な監査報告書とは別に、ポイントを簡潔にまとめた要約監査報告書として作成する。
要約監査報告書では、監査の専門用語、及び実施した監査の詳細な記載はできる限り避ける。
・・・【基準 11】ガイドライン１．(1)

3.6.2　改善提案

・監査報告書に指摘事項を記載した場合に、指摘事項に対しての改善提案を記載することがある。

＊指摘事項と改善提案（及び改善計画）とは、
それぞれが対応するように記載する必要がある。
＊改善提案の記載に際しては、**重要改善事項**と**通常改善事項**等、あるいは**緊急改善事項**と**中長期改善事項**等、その重要度や緊急度に区別して記載する。
・・・【基準 11】ガイドライン４．＜例２＞

・『システム監査技術者試験（レベル４）シラバス（Ver.6.1)』の「3-2 改善提案の記載」には以下の記載がある
・監査報告書には，指摘事項を改善するために必要な事項を改善提案として記載する。
・改善提案は，改善の重要性及び緊急性を判断して，「**緊急改善**」と「**通常改善**」に分けて記述する。
(1) 緊急改善：システムに重大な欠陥が生じており、そのまま放置できないと判断される事項
(2) 通常改善：重大な欠陥ではないがシステムの改善が図れると判断される事項
・改善提案には，改善内容，改善実施部門，他の改善提案との整合性などを盛り込む。

3.6.3 改善計画

・改善計画は、監査報告前に作成する場合と、監査報告後に作成する場合がある。
１）（監査報告に際し監査対象先が作成する場合）
監査対象先又は改善責任部門は、指摘事項の最終確認後で、監査報告書の完成前に、監査報告書に記載される改善提案に対する改善計画を作成し、監査人に提出する。

（監査人は提出された改善計画を監査報告書に記載する）

2）（監査報告語後に監査対象先が作成する場合）
監査対象先又は改善責任部門は、監査報告書の提出（報告）を受けた後に、監査報告書に記載される改善提案に対する改善計画を作成する。
（後日、フォローアップのために監査人に提出）

・監査対象先又は改善責任部門は、関係先又は関係部門と協議の上、改善計画を作成する。

＜記載内容＞
・具体的な改善内容と方法、
・実施体制と責任者、
・進捗状況又は今後のスケジュール　等
・・・【基準 12】解釈指針１.

＊指摘事項と改善提案（及び改善計画）とは、それぞれが対応するように記載する必要がある。
・・・【基準 11】ガイドライン４. ＜例２＞

3.7　監査報告

・報告の種類
１）監査報告書・要約監査報告書の提出・回付
（緊急を要する場合は口頭で、後日提出）
２）監査報告会の開催

・監査の依頼者や適切な関係者に報告
・・・【基準 11】

・監査の依頼者である取締役会等及び経営者等や監査対象先等を含む適切な関係者に報告
・・・【基準 11】主旨.

・取締役会等には、詳細な監査報告書とは別に、ポイントを簡潔にまとめた要約監査報告書で報告
・・・【基準 11】ガイドライン１．(1)

・システム監査が IT ガバナンスに関連する場合、取締役会等及び経営者、監査役会等に対する報告と併せて、組織体のガバナンス機能に関わる機関にも提出
・・・【基準 11】解釈指針２．

・監査対象先に対しては写しを回付
監査対象部門以外にも必要に応じて回付
・・・【基準 11】解釈指針３．

3.8 フォローアップ

3.8.1 改善状況モニタリング ・・・【基準 12】解釈指針２．

１）「監査報告書」に「改善提案」が記載してある場合

・監査人は、監査対象先又は改善責任部門から、一定期間以内に、「改善計画書」を受領し、適宜、「改善実施状況報告書」等によって、改善状況をモニタリング

２）「監査報告書」に「改善計画」が記載してある場合

・監査人は、適宜、「改善実施状況報告書」等によって、改善状況をモニタリング

3.8.2 改善確認

・監査人は、監査対象先の責任において実施される改善を事後的に確認する。・・・【基準 12】解釈指針２．

・監査人は、当該改善事項が適切かつ適時に実施されているかどうかを確かめる。

・監査人は、改善の実施が適切であるかどうかを確かめる。　・・・【基準 12】主旨

・監査対象先から提出された改善実施状況報告書により、改善内容の妥当性、改善体制、改善の進捗状況等を確認する。　・・・【基準 12】解釈指針３.

3.8.3　改善実施内容の検証・評価

・監査人の改善提案の基となった指摘事項の重大性等を総合的に勘案して、検討する。

１）追加的な検証が必要か

２）次回以降の監査に反映すべき点がないか

・・・【基準 12】解釈指針３.

3.8.4　改善対応の再要求

・以下の場合は、再度の改善対応を要請する。

１）監査対象先又は改善責任部門が実施した改善策が不十分

２）改善提案に基づく問題解決がなされないまま

・さらに、改善が適切かつ適時に行われない場合のリクを明確にして、取締役会等及び経営者等に報告する場合もある。

・・・【基準 12】解釈指針４.

3.8.5　報告

・フォローアップの終了後、「フォローアップ報告書」を作成する。

・監査対象先又は改善責任部門に回付する。

・重要度に応じ経営者、取締役会等にも報告する。

・・・【基準 12】解釈指針５.

４．監査関係者

・監査関係者（当事者）としては、「利用者／監査依頼者」「監査人／監査受託者」「プロセス・オーナー／監査対象関係者」が挙げられる。
・監査では、「利用者」が「監査人」に監査を依頼する。
・監査依頼を受けた「監査人」は「プロセス・オーナー」を含む「監査対象先」の監査を行う。

・監査の目的（保証型、助言型）や監査対象（視点／ガバナンス、マネジメント、コントロール）により、当事者は異なる。

4.1　当事者

・内部監査人や外部監査人は、取締役会等（取締役会、理事会等）や経営者からの委託により、IT システムに係る監査を実施し、その結果を報告することによりガバナンス、マネジメント、コントロールに役立つ監査を行うことになる。
なお、取締役会等からの指示や監査役（会）等からの依頼により内部監査人や外部監査人がガバナンスに対する監査を行うこともあり得る。
・・・【前文】監査人と取締役会等、経営者との関係

・また、監査業務は保証を目的としたシステム監査と助言を目的としたシステム監査から成り立っている。
・・・【前文】監査人と取締役会等、経営者との関係

4.1.1　保証型システム監査

・保証を目的としたシステム監査には、監査対象となる組織体、業務、機能、プロセス、情報システム等（以下、「監査

対象先」という。）について、監査の意見又は結論を得る基礎として、監査人が入手した証拠を客観的に評価することが含まれる。

・・・【前文】監査人と取締役会等、経営者との関係

・一般的には、次の三者が当事者となる。

(1) プロセス・オーナー：
事業体、業務、機能、プロセス、システム若しくはその他の監査対象事項に直接関わる者又はグループ

(2) 監査人：
評価を行う者又はグループ

(3) 利用者：
評価結果を利用する者又はグループ

・・・【前文】監査人と取締役会等、経営者との関係

・システム監査においては、
プロセス・オーナーには監査対象先(関係者)が、
監査人には内部監査人や外部監査人が、
利用者には経営者や取締役会等が一般的には該当する。

・なお、外部監査の場合には、
組織体外部の第三者にシステム監査の実施を依頼する者がおり、取締役会、経営者等がその監査の依頼者となる。

・また、監査役（会）等の監査においては、
プロセス・オーナーには取締役や監査対象先(関係者)が、
監査人には監査役（会）等が、
利用者には株主が一般的には該当する。

・・・【前文】監査人と取締役会等、経営者との関係

4.1.2　助言型システム監査

・助言を目的としたシステム監査の性質は、助言に加えて提案や相談の提供であり、一般に、依頼者からの具体的な要請に基づいて実施される。

・・・【前文】監査人と取締役会等、経営者との関係

・一般的には、助言を目的としたシステム監査では、次の二者が当事者となる。

(1) 監査人：
助言を提供する者又はグループ

(2) 依頼者：
助言を必要として、これを受ける者又はグループ

・・・【前文】監査人と取締役会等、経営者との関係

・ただし、監査の性格においては、当事者が増加ないし変化する場合がある。

助言業務を実施するに当たっても、監査人は、客観性を維持すべきであり、また、管理者としての職責を負ってはならない。

・・・【前文】監査人と取締役会等、経営者との関係

4.2　権限と責任

・システム監査を実施する意義、目的、対象範囲、並びに**監査人及びシステム監査を行う組織の権限と責任**は、文書化された規程等により定められていなければならない。

・・・【基準１】

・効果的かつ効率的なシステム監査を実現するための体制整備として、**監査人及びシステム監査を行う組織の権限と責任**を

組織体の内部監査規程等によって明確にし、組織体全体に周知しておく必要がある。

また、システム監査を外部委託する場合には、**委託先の権限と責任**を契約書等の文書で明確に定めておく必要がある。

・・・【基準１】主旨

※監査人及びシステム監査を行う組織に対しての監督も重要

・システム監査の全部又は一部を組織体外部の専門家に委託する場合、当該専門家と密接に連携し、当該専門家に対する適切な**監督**を行うことが重要である。

・・・【基準１】解釈指針２．(1)

＜システム監査に係る権限（例）＞

・システム監査の遂行に必要な全ての**記録や資料の閲覧が可能**であること。

・システム監査の遂行に必要な全ての**設備や情報資産へのアクセスが可能**であること。

・監査対象先の責任者や担当者に**面接**し、**質問**し、又は**事情説明**を**求める**ことができること。

・・・ガイドライン【基準１】２．

4.3　監査倫理

・システム監査は、監査人の誠実性及び専門的な能力を信頼し依頼されるものであり、監査人はその期待に応え、責任を果たすことが求められ、業務に関する説明責任を果たすこととなる。

さらに、システム監査が結果として、広く社会的な信用につながるには、個々の利用者・依頼人の要請を満たすだけではなく、監査人が独立した立場において、社会的役割を自覚し、自らを律し、かつ社会の期待に応え、公共の利益に資することができなければならない。

IT の進展をはじめ、監査の対象となるシステムを巡る環境変化が激しいこともあり、監査の方法の選択や監査結果の判断に関して、種々の価値観の中で適切な意思決定をするためには、監査人の倫理が重要である。加えて、IT 利活用の高度化により、システム監査においても機密性の高い情報に触れる機会が増加しており、倫理に関して社会的な要請が高まっていることを意識しなければならない。

・・・【監査人の倫理】

＜倫理に関して監査人が守るべき４つの原則＞

○**誠実性**：

監査業務において、常に**正直な態度**を保持し、**強い意志**をもって適切に行動すること。監査人が**誠実**であることによって信頼が築かれることから、誠実性は、自らの判断が信用される基礎となる。

○**客観性**：

監査業務において、**バイアス（先入観等）、利益相反を排し**、個人や組織等から**不当な影響を受けることなく**、監査人としての判断を行うこと。監査人としての判断が不当な影響を受ける場合、当該業務を引き受けてはならない。

○監査人としての**能力**及び**正当な注意**：

監査業務において、**必要な知識、技能を習得し、維持する**こと、及び誤った監査上の判断がないように、システム監査の基準に従って、監査人として**当然払うべき注意を払う**こと。

○**秘密の保持**：

監査業務において、取得した情報の秘密性を尊重し、業務上知り得た**秘密を守る**こと。法令等による守秘義務の解除を除き、依頼人又は所属する組織との関係が終了した後も、**秘密の保持**が求められる。

・・・【監査人の倫理】

4.3.1　独立性と客観性

・システム監査は、監査人によって**誠実**かつ、**客観的**に行われなければならない。
さらに、監査人が監査対象の領域又は活動から、**独立かつ客観的な立場**で監査が実施されているという外観にも十分に配慮されなければならない。
・・・【基準４】

・システム監査は、**客観性、誠実性の保持**として、客**観的な立場**で公正な判断を行うという精神的な態度を堅持する監査人によって行われなければならない**（精神的独立性）。**
監査人の精神的独立性は当然であるが、さらにシステム監査は、組織体の内部監査部門で行われるものであれ、外部の専門事業者によって行われるものであれ、監査対象先から**独立した立場**で実施されているという外観が確保される必要がある**（外観的独立性）。**
・・・【基準４】主旨

・　システム監査の実施に当たり、精神的独立性が堅持できない場合には、システム監査における客観性、ひいてはシステム監査の品質が維持できず、信頼性を著しく毀損することになることに留意する。
・監査人に外観的独立性が欠けるという疑いや印象を与えないために、システム監査は**監査対象先から独立**した監査人によって行われる必要がある。
所属する部門が、監査対象の領域又は活動と同一の指揮命令系統に属する場合、**組織的な独立性**が毀損されているとの外観を呈することに留意する。

・システム監査を外部の専門事業者（専門家）に委託する場合、システム監査を担当する者が、専門家としての能力を有しているか、独立性に問題がないかを確かめることが求められる。

委託元組織体と身分上の密接な利害関係を有することは、独立性が毀損されているとの外観を呈することに留意する。

（システム監査を外部に委託する場合の独立性については、【基準１】解釈指針 2.(2)参照のこと）。

・・・【基準４】解釈指針１．～３．

・外部委託先の専門家は、原則として、委託元の組織体と身分上又は経済上の特別な利害関係を有してはならない。特別な利害関係を有する者を外部委託先とする場合は、システム監査業務に影響を及ぼさぬよう適切な措置を講じなければならない。

・・・【基準１】解釈指針２．(2)

4.3.2　正当な注意

・システム監査は、専門的能力の維持・向上を図るとともに、監査業務において**正当な注意**を払って実施する監査人によって行わなければならない。また、監査人は秘密の保持をしなければならない。

・・・【基準５】

4.3.3　秘密の保持

・システム監査の実施に当たり、業務上知り得た事項を正当な理由なく他に開示したり、自らの利益のために利用したりしてはならないことが監査人に求められる。

なお、秘密の保持は、所属する職業団体や会社における倫理規程、契約、就業規則等によって要求される場合もある。

・・・【基準５】解釈指針２.

4.3.4　専門的能力

・適切な教育・研修と実務経験を通じて、システム監査に必要な**知識、技能及びその他の能力を保持**し、その**向上に努め**なければならない。
また、組織体のシステム監査を行う組織の長は、効果的かつ効率的なシステム監査に必要な**知識、技能及びその他の能力**を、システム監査を行う組織が**総体として備えている**か、又は**備える**ようにしなければならない。

・・・【基準２】

＜システム監査に求められる知識や技能の例＞

- 情報システムに関する知識
- システム開発の上流から下流に至る、開発手法等に関する知識
- プロジェクトマネジメントに関する知識
- 情報セキュリティに関する知識
- システムが対象とする業務（会計、サプライチェーン等）に関する知識
- システムの運用に関する知識
- 外部委託先の管理に関する知識
- 監査手続、監査技法等に関する知識

・・・【基準２】ガイドライン１.

・システム監査は、**専門的能力の維持・向上を図る**とともに、監査業務において正当な注意を払って実施する監査人

によって行わなければならない。また、監査人は秘密の保持をしなければならない。

・・・【基準５】

・システム監査の実施に当たり、客観的な立場で公正な判断が行われるために、**専門的な知識・技能を有する**監査人によって行わなければならない。

専門的な知識・技能を習得し、維持することは、監査人としての能力をもって依頼者に保証・助言を提供するために、適切な判断をすることが求められるからである。

・・・【基準５】解釈指針１．

【付録：システム監査　簡易チェックリスト】

確　認　項　目		確認
A.前提	1.システム開発・運用についての管理規程がある （システム管理体制が整備されている）	
B.準備	2.監査の目的が明確になっている	
	3.監査の種類決定している（保証型、助言型）	
	4.監査のレベルを選定している （ガバナンス、マネジメント、コントロール）	
	5.監査の対象範囲（システム）が選定されている	
	6.監査についての規程等が整備されている	
	7.監査時期が明確になっている	
	8.監査費用が準備されている（予算）	
	9.監査担当部門がある（監査担当者がいる）	
	10.（保証型監査の場合）言明書が作成されている	
C.実施	11.システム開発・運用についての記録がある （開発経緯、運用状況についての記録がある）	
D.監査人	12.独立した立場にある	
	13.監査のスキルがある（知識、資格、実績）	

システム監査入門

（システム監査の理解に向けて）

Ver. 1.0　2025.11.1

NPO 法人　日本システム監査人協会
（東北支部）