デジタル社会推進実践ガイドブック DS-110

デジタル・ガバメント推進標準ガイドライン
解説書
（第３編第１０章 システム監査）

2023 年（令和５年）3 月 31 日

デジタル庁

〔ドキュメントの位置付け〕
Informative
参考とするドキュメント

〔キーワード〕
監査体制、監査実施計画書、監査手続書、監査調書、監査報告書

〔概要〕
標準ガイドラインの下位文書として、標準ガイドラインの記載の趣旨、目的等を理解しやすくするため、逐条的な解説等を記載した参考文書。

改定履歴

改定年月日	改定箇所	改定内容
2022年4月20日	第１０章１.	・府省ＣＩＯをデジタル統括責任者に修正
2020年11月27日	第１０章１.	・ODBに関する記載を削除
2020年3月31日	－	・解説書全体に合わせ、日付のみ更新
2019年2月27日	－	・初版決定

目次

第１０章　システム監査

ＰＭＯは、プロジェクトの目標を達成することを目的として、所管する情報システムにまつわるリスクに適切に対処しているかを客観的に評価するために、内部又は外部からの支援を得て、次のとおり監査を行う(1)ものとする。

なお、各府省の体制等の状況によって、ＰＪＭＯ等が直接監査を行うことを妨げない(2)。この場合においては、監査体制の確立、監査実施計画書の作成・調整・確定、監査の実施の主体はＰＪＭＯ等とする(3)。

1. はじめに

システム監査（以下、単に「監査」ということがある。）は、情報システムにまつわる様々なリスクに適切に対処しているかどうかを、独立かつ専門的な立場の監査体制により客観的に評価し、そこで発見された問題点の指摘やその改善案の提示を行うことにより、プロジェクト目標の達成に貢献するものである。

プロジェクトの活動は、情報システムの企画、設計・開発の段階に留まらず、情報システムの運用、保守の段階までを含めるものであり、プロジェクト目標を確実に達成するためには、運用及び保守段階をも対象とした監査を実施する必要がある。

本書では、システム監査とプロジェクトの他の活動との関係を図 10-1 のように想定している。

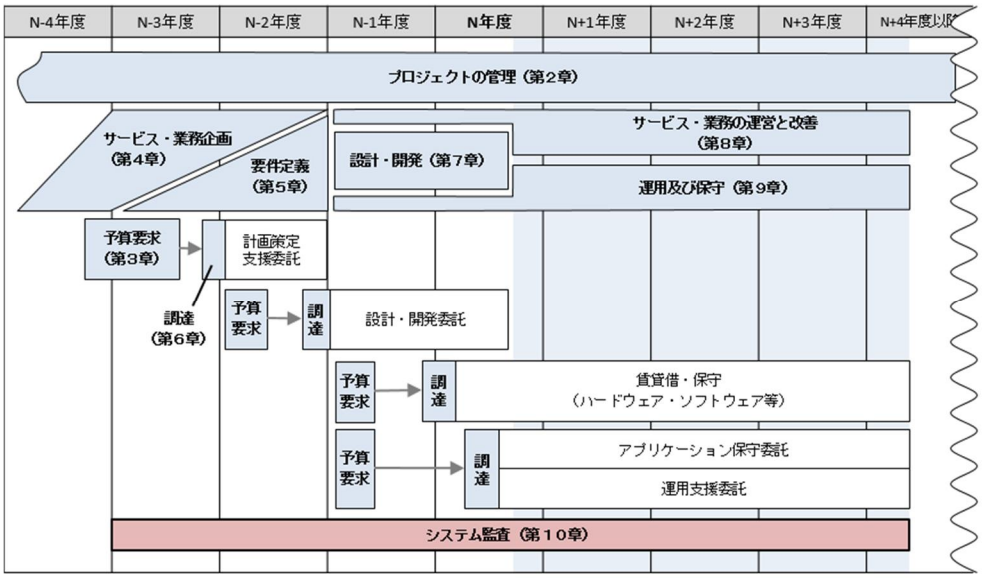


図 10-1
システム監査の実施と前後又は並行する工程との関係

2. 解説

(1)「ＰＭＯは、プロジェクトの目標を達成することを目的として、所管する情報システムにまつわるリスクに適切に対処しているかを客観的に評価するために、内部又は外部からの支援を得て、次のとおり監査を行う」

「所管する情報システムにまつわるリスクに適切に対処しているかを客観的に評価する」とは、各府省の定めるシステム監査計画に基づいて、所管する情報システムにまつわるリスクに対してプロジェクトが適切に対処しているかを、デジタル・ガバメント推進標準ガイドライン、各府省の規則・手順、プロジェクトの標準化ルール等に対する準拠性や妥当性の観点から客観的に点検・評価・検証することを指す。

なお、情報セキュリティリスクは「情報システムにまつわるリスク」に含まれることから、情報セキュリティ監査は、システム監査におけるテーマの一つである。システム監査と情報セキュリティ監査の関係については、標準ガイドライン「第２編第８章１．システム監査計画の策定」を参照すること。

「内部又は外部からの支援を得て、次のとおり監査を行う」とは、ＰＭＯが主体者として、監査対象からの独立性及び客観性を担保した府省内の組織や者、外部委託事業者から監査体制を組成し、システム監査を行うことを指す。

なお、各府省において既に監査に関わる体制が確立・運用されている場合には、その体制の下、標準ガイドラインで求める内容を満たす監査を実施することができる。

標準ガイドラインにおける監査の全体体制は、次のとおりである。

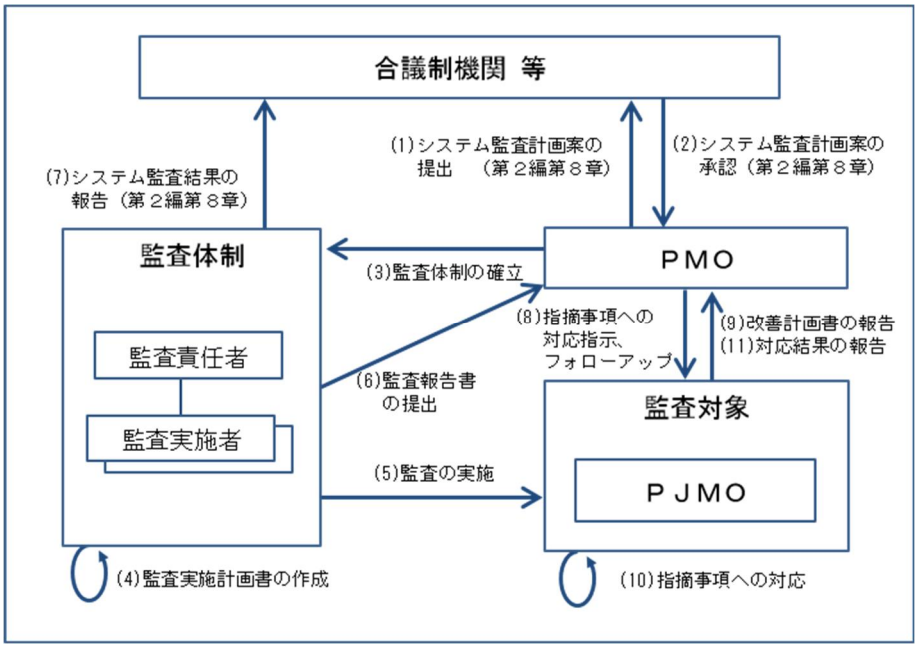


図 10-2
システム監査の全体体制

(2)「各府省の体制等の状況によって、ＰＪＭＯ等が直接監査を行うこと

を妨げない」

「ＰＪＭＯ等」とは、ＰＪＭＯに加え、府省により設置されている内部の監査部門を指す。

「ＰＪＭＯ等が直接監査を行うことを妨げない」とは、システム監査の体制は、独立性と客観性を保つため、監査対象の一部であるＰＪＭＯとは独立した組織が監査を行うことが望ましいことから、標準ガイドラインでは、ＰＭＯが実施することを想定して記載している。ただし、既に府省に設置されている監査部門や、人材確保等の実情を踏まえ、監査責任者及び監査実施者に一定の独立性を確保することを条件に、ＰＪＭＯ等が主体となって監査を行うことを許容するものである。

(3) 「この場合においては、監査体制の確立、監査実施計画書の作成・調整・確定、監査の実施の主体はＰＪＭＯ等とする」

「監査体制の確立、監査実施計画書の作成・調整・確定、監査の実施」とは、図 10-2 で示したシステム監査の全体体制のうち、ＰＪＭＯ等が実施主体となって監査体制が実施する役割を担うことを指す。このときにおいても、監査実施計画書及び監査結果について、ＰＭＯへ報告を行うことが必要である。

１. システム監査

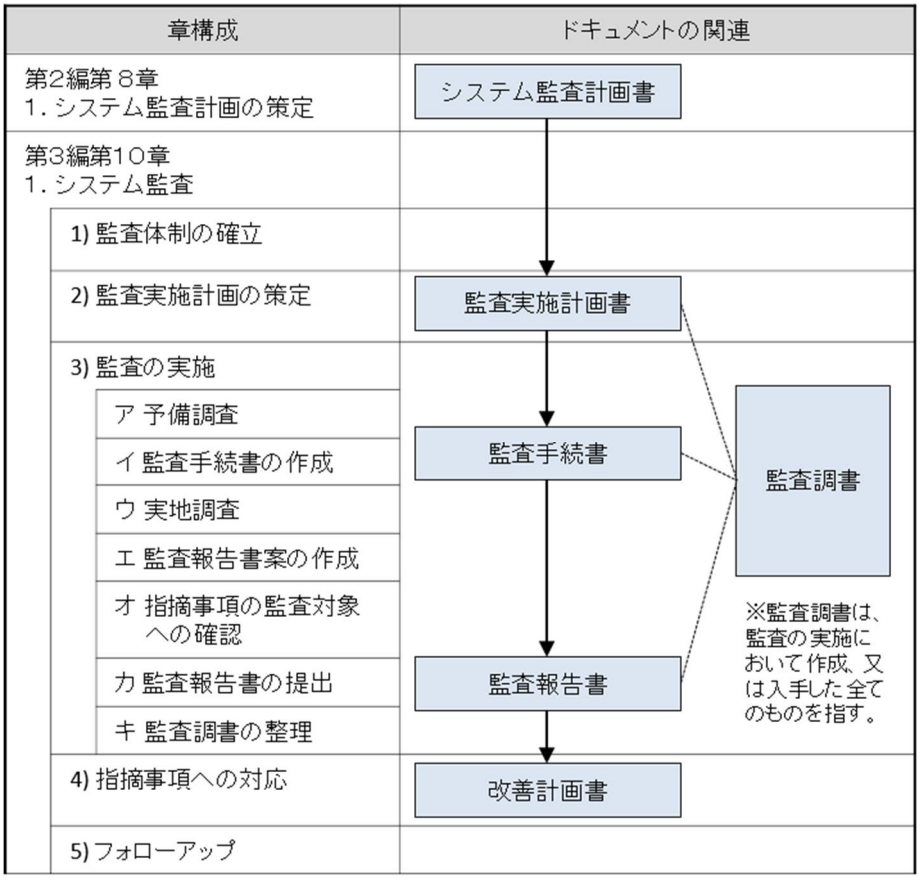
ＰＭＯは、システム監査計画（「第２編第８章 システム監査の計画・管理」参照）に基づき、次のとおり監査を行うものとする。なお、**システム監査計画に定めがない場合であっても、ＰＭＯが監査を行う必要があると判断したときは、監査を行う(1)**ものとする。

1. 趣旨

システム監査は、ＩＴガバナンスの視点で計画されたシステム監査計画に基づいて、効果的かつ効率的に実施する必要がある。

このため、ＰＭＯは、システム監査計画に基づいて、監査対象と指定されたプロジェクトに対して監査体制を組成して監査を実施するとともに、指摘事項に対する改善が確実行われるよう、ＰＪＭＯに対してフォローアップする。

システム監査で行う作業と作成ドキュメントの全体像を、次に示す。



← 図 10-3
システム監査で行う作業と作成ドキュメントの全体像

ドキュメントの概要は次のとおりである。

ドキュメント名	概要
監査実施計画書	システム監査の対象ごとに、詳細な計画を記載したもの。
監査手続書	各監査項目についての評価を行うための手続（入手する監査証拠及びその入手方法等）を記載したもの。

← 表 10-1
システム監査で使用するドキュメントの概要

ドキュメント名	概要
監査調書	監査実施者が監査の実施において作成し、又は入手した全てのもの。 次のものがこれに該当する。 • システム監査計画、監査実施計画書及びこれらの計画を作成するために収集した資料等 • 予備調査で確認した資料の名称や種類及びインタビュー対象者の氏名や役割、並びに把握した事項をまとめたもの • 監査証拠として採用したインタビュー記録（対象者、実施日時、実施場所等）、観察記録（対象内容、実施日時、実施場所等）、申請書、台帳、帳票、画面のハードコピー、その他の文書等 • 監査対象の概要把握、監査手続の作成等に利用した規程、マニュアル、その他の文書、記録
監査報告書	監査体制が、監査の結果に基づいて、作成するもの。

なお、監査調書は、ＰＭＯや監査対象からその監査結果についての根拠を求められた場合に必要なものである。また、次回以降の監査を効果的かつ効率よく実施するためにも用いられる。監査後においては、入手又は閲覧した資料の一覧を作成し、指摘事項と関係する監査証拠等のひも付けができるように、監査調書の整理を行っておく。

2. 解説

(1) 「システム監査計画に定めがない場合であっても、ＰＭＯが監査を行う必要があると認めたときは、監査を行う」

「ＰＭＯが監査を行う必要があると認めたとき」とは、例えば、次のような場合において、ＰＭＯがシステム監査の実施を判断することを指す。

- 工程レビューにおいて重大な問題が発見され、その対応についてシステム監査で確認した方が良いと思われる場合
- プロジェクト管理において、重大なリスク、課題等が挙げられた場合
- 情報システムの形態や、その利用する技術等が同様である他のプロジェクトにおいて重大な問題が発生した場合
- デジタル統括責任者等から指示を受けた場合

また、ＰＪＭＯも、同様に必要と認めた場合には、自主的に監査を実施できる。

1） 監査体制の確立

ＰＭＯは、監査の独立性及び客観性の確保の観点から、監査実施前に、少なくとも次のアからエまでに掲げる事項を満たす監査体制を確立するよう努めるものとする。

ア　監査責任者及び監査実施者

監査体制は、監査責任者及び監査実施者により構成する(1)こと。

イ　独立性

監査体制の構成員は、監査対象となるプロジェクトや情報システムに関する業務等に関与していないこと(2)。なお、監査対象となるプロジェクト、情報システムに関する業務等に関与した者は、自らが監査対象となる業務の監査を行うことはできないこと。

ウ　監査能力

監査体制の構成員のうち少なくとも一人は、監査の実務経験を有すること(3)。

エ　専門性

監査体制の構成員のうち少なくとも一人は、監査目的に応じた技術的な知識及び実務経験を有すること(4)。

1. 趣旨

システム監査において客観的な点検・評価・検証を行うためには、システム監査を行う体制が監査対象から独立した立場であるという外観を確保する必要がある。

このため、ＰＭＯは、監査対象に対する独立性と客観性を確保することを目的として、本節に規定する監査体制の要件を満たすよう、監査体制を確立する。

2. 解説

(1) 「監査体制は、監査責任者及び監査実施者により構成する」

「監査体制」とは、ＰＭＯの下で監査実施計画書を作成し、それに基づき監査を実施する体制をいう。監査体制は、監査責任者１名と監査実施者（監査責任者の兼務可）により構成される。大規模プロジェクト等の場合には、サブチームを置き、それぞれにサブリーダを置く。

「監査責任者」とは、監査実施計画書を作成し、それに基づき監査の実施を監査実施者に指示し、監査結果の取りまとめを行う者を指す。監査責任者は、本項目の「イ　独立性」の要件を満たす者を選任することが望ましい。また、監査を外部委託する場合においても、監査責任者として府省内の者を置く。

(2)「監査体制の構成員は、監査対象となるプロジェクトや情報システムに関する業務等に関与していないこと」

「監査対象となるプロジェクト、情報システムに関する業務等に関与していない」とは、現在及び過去において当該プロジェクトのＰＪＭＯのメンバーでなく、当該情報システムの企画、設計・開発、運用、保守等のいかなる業務にも従事していないという意味である。なお、構成員が過去にＰＪＭＯのメンバーであったり、情報システムの業務に従事していたりする場合においても、業務従事時から１年以上経過している等、監査目的、監査対象期間等から構成員が客観的な評価を行うことができると考えられる場合は関与していないものとみなすことができる。

また、監査対象となるプロジェクト、情報システムに関する業務等に関与している構成員についても、監査手続の実施において、自らがインタビューを受ける立場になり得る、又は自らが作成等した証跡（自らが作成した資料・記録及び自らの行為・操作等を記録したログ等）が監査の対象となり得る場合には、当該監査手続の作成・実施、並びに監査調書及び監査報告書の作成に関与してはならない。

(3)「監査体制の構成員のうち少なくとも一人は、監査の実務経験を有すること」

「監査の実務経験を有する」とは、システム監査（情報セキュリティ監査を含む。）について、監査計画書の立案、監査手続の作成・実施、及び監査報告書の作成までの一貫した経験を有することをいう。

(4)「監査体制の構成員のうち少なくとも一人は、監査目的に応じた技術的な知識及び実務経験を有すること」

「監査目的に応じた技術的な知識及び実務経験を有すること」とは、監査目的を達成するために、専門的な技術知識（クラウドサービス、ネットワーク、情報システムの設計・開発手法等）や情報システムの整備業務に携わった経験（当該業務の監査経験を含む。）が必要と考えられる場合には、構成員のうち少なくとも一人は、その知識及び業務経験を有する者とすることを規定したものである。

2） 監査実施計画の策定

監査責任者は、システム監査計画書に基づいて、**次のとおり監査実施計画書を作成する(1)**ものとする。

ア　監査実施計画書の記載内容

監査実施計画書には、原則として次の[1]から[7]までに掲げる事項を記載する。

[1] 監査対象
[2] 監査目的
[3] 監査範囲
[4] スケジュール
[5] 監査体制
[6] 監査実施方法
[7] その他

イ　監査実施計画書の調整・確定

監査責任者は、**あらかじめ監査実施計画書の案をＰＪＭＯと調整し、ＰＭＯに報告する(2)**。

ＰＭＯは、監査実施計画書を確認し、確定するものとする。

なお、状況の変化等を勘案して監査実施計画書に変更が必要と判断されるときは、監査責任者は、ＰＭＯと相談して見直しを行うものとする。

1. 趣旨

システム監査計画は府省全体のシステム監査についての計画であり、実際のシステム監査に当たっては、効果的かつ効率的な監査が行えるよう、監査対象ごとに監査計画を具体化・詳細化する必要がある。

このため、監査責任者は、システム監査の実施に先立ち、監査対象ごとの監査実施計画書の案を作成し、監査対象のＰＪＭＯと調整の上、ＰＭＯに計画を報告し、内容を確定する。

2. 解説

(1) 「次のとおり監査実施計画書を作成する」

「監査実施計画書」とは、システム監査計画に定められた監査対象ごとに作成する監査の実施計画書を指す。

監査実施計画書の記載事項には、次の事項を記載する。

記載事項	記載内容
[1] 監査対象	システム監査計画に記載されている監査対象について記載する。
[2] 監査目的	システム監査計画に記載されている監査目的について記載する。
[3] 監査範囲	システム監査計画に記載されている監査範囲について記

← 表 10-2
監査実施計画書の記載内容

記載事項	記載内容
	載する。システム監査計画に記載された監査範囲をより具体化又は特定できる場合には、その内容を記載する。
［4］スケジュール	「3）監査の実施」に示す作業を基本として、監査の準備から終了後の監査調書の整理まで、工程ごとに詳細なスケジュールを記載する。 なお、ＰＪＭＯによる指摘事項への対応やフォローアップの期間も踏まえ、スケジュールを調整する。
［5］監査体制	監査責任者及びその他の監査実施者の所属及び氏名を記載する。なお、監査対象によりチームを分ける場合には、チームごとに記載する。
［6］監査実施方法	主たる監査手続で利用する監査技法について記載する。特に、監査手続を実施するために監査体制の構成員に技術的な能力が要求される情報システムを利用した監査技法又は実施に一定の準備が必要になるアンケートの実施等の監査技法を用いる場合には、その旨を明記する。また、主たる監査手続におけるインタビュー対象者の役割や人数、調査対象の書類の種類や数、監査実施場所等について記載する。本項目は、「3）監査の実施」の監査手続書の概要、特記事項等を示すものである。
［7］その他	上記[1]から[6]までに掲げる事項のほか、監査を実施するに当たっての留意事項等を記載する。例えば、外部委託先のデータセンタを監査する場合等における制約事項（データセンタ内に入室できる人数等）や留意事項（守秘義務の誓約書の必要性）が挙げられる。

(2) 「あらかじめ監査実施計画書の案をＰＪＭＯと調整し、ＰＭＯに報告する」

「監査実施計画書の案をＰＪＭＯと調整し」とは、ＰＭＯと監査実施計画書の内容を確定する前に、ＰＪＭＯに内容を共有し、監査を実施する上で支障となる要因を把握し、それらを排除するためのスケジュール変更や事前手続の実施等を指す。なお、監査実施計画書は、ＰＪＭＯとの調整及びＰＭＯへの報告に要する期間を踏まえて、計画的に作成することに留意する。

3） 監査の実施

監査責任者及び実施者は、次のアからキに示す手順で作業を行うものとする。

監査実施者は、監査手続書を作成した上で監査を行うものとし、その結果について監査調書（指摘事項等の監査証拠を添付すること。）を作成するものとする。

監査責任者は、監査結果について、ＰＭＯに報告するものとする。

ア　**予備調査(2)**

監査実施者は、監査対象を理解するために、監査対象である組織、業務、情報システムの概要について把握するための予備調査を実施する。

イ　**監査手続書の作成(3)**

監査実施者は、予備調査結果等に基づき、監査の手続（入手する監査証拠及びその入手方法等）を定めた監査手続書を作成する。

ウ　**実地調査(4)**

監査実施者は、監査対象先に赴いて、監査手続書に基づき監査を実施する。監査体制は、実施結果、入手した監査証拠、及び監査の実施に際し監査実施者が気付いた点等をまとめた監査調書を作成する。

エ　**監査報告書案の作成(5)**

監査実施者は、監査調書等を基に、監査結果や指摘事項等をまとめた監査報告書案を作成する。

オ　**指摘事項の監査対象への確認(6)**

監査実施者は、監査報告書案の指摘事項について、監査対象の担当者等に確認を行い、監査報告書に修正が必要な箇所を修正する。

カ　**監査報告書の提出(7)**

監査責任者は、ＰＭＯに監査報告書を提出した上で、ＰＪＭＯに通知する。また、監査責任者は、監査結果を合議制機関等に報告するものとする。（「第２編第８章　３．システム監査結果の報告」参照）

キ　**監査調書の整理(8)**

監査責任者は、監査調書を閲覧しやすいように整理する。

1. 趣旨

効果的かつ効率的にシステム監査を行い、適切な問題点の指摘及び改善案の提示を行うためには、結論を裏付けるために必要となる適切な監査証拠を十分に入手し、証拠に基づいて合理的な結論を導くとともに、その証拠及び結論に至った過程を明らかにする必要がある。

このため、監査責任者は、監査の実施に当たって、適切な監査証拠を入手するための監査手続書を作成し、監査手続書に従って証拠を入手するとともに、

監査調書として確実に記録を残し、監査報告書をまとめ、ＰＭＯに結果を報告する。

2. 解説

(1) 「予備調査」

「予備調査」とは、監査実施者が監査対象を理解するために、監査対象である組織、業務、情報システムの概要、プロジェクト推進に係るリスクなどについて把握するため、実地調査（監査対象のある場所に赴いて監査を行うこと。）を行う前に実施する調査のことを指す。

予備調査の方法は、プロジェクト計画書、業務分析資料、要件定義書等の各種文書を査閲するのが一般的な方法であるが、監査対象の担当者にインタビューを行う方法もある。

また、監査手続書を作成するために、監査実施者は監査対象に関わる規定等の文書やプロジェクト推進に係るリスクなどを確認する。さらに、監査対象からどのような監査証拠を入手できるかを確認するため、監査対象における監査証跡（監査証拠になる可能性のある記録類等）を把握する。

(2) 「監査手続書の作成」

「監査手続書の作成」とは、実地調査に使用するため、各監査項目についての監査を行うための手続（入手する監査証拠及びその入手方法等）を監査手続書に記述することを指す。

なお、監査手続書は、次の手順で作成する。

表 10-3
監査手続書の作成手順

手順	内容
監査項目の決定	システム監査計画書に記載されている監査の方針を基に、監査項目を決定する。監査項目とは、監査目的を達成するために必要となる評価項目である。監査目的に照らして、監査の方針に基づいて適切な監査項目を選定し、監査目的に合うよう内容を修正する。
入手すべき監査証拠及び監査技法の決定	監査証拠とは、監査項目を評価するために必要な証拠であり、最終的に監査結果を裏付けるものである。 監査証拠を入手する方法を監査技法という。監査技法には質問、査閲、照合、分析、観察等がある。監査証拠と監査技法は併せて検討する。 一般に、証拠能力の高い監査証拠を入手するためには、監査実施者に高度な知識・経験が必要になる。また、入手に手間を要する場合が多い。さらに、情報システムや業務において確保される監査証跡（システムのログ、承認された申請書等）は、証拠能力が高いにもかかわらず、情報システムの仕様として監査証跡が確保されていない場合もある。 よって、監査実施者は、監査目的等に照らし合わせ、どの程度の証拠能力が必要かを検討しつつ、監査証跡の確保の状況、監査実施者の知識・経験、実地調査に費やせる時間等を考慮の上、入手すべき監査証拠を決定する必要がある。 なお、監査範囲として監査対象期間が設定されている場合には、インタビューにより確認する事項の発現時期、査閲する記録類の作成時期等が監査対象期間内であることについても留意する必要がある。
サンプリング対象及びその数の決	監査証拠をどの程度入手するかを決定する。 サンプリングは、主に準拠性評価を行う際に必要になる。例えば、保守段階におけるアプリケーションの変更について、アプリケーション

手順	内容
定	変更依頼と変更記録を照合する場合に、どのアプリケーションを対象にするのか、また、確認する変更記録の数を決定する。 サンプリング数は、監査目的における当該監査手続の重要性や、その手続に関わる監査実施者の数、手続にかけられる時間等の監査資源によって決定する。 サンプリング対象及びその数は、監査手続の実施時に決定し、その時の対象や数を監査調書に記載する方法もある。 なお、全数調査を妨げるものではない。
その他必要事項の記載	監査手続を実施する上での着眼点、留意点等を記載する。

(3) 「実地調査」

「実地調査」とは、監査実施者が監査対象先に赴き、監査手続書に基づいて監査を実施することを指す。監査を実施した結果、入手した監査証拠、及び監査の実施に際し監査実施者が気付いた点等を監査調書にまとめる。

(4) 「監査報告書案の作成」

「監査報告書案の作成」とは、監査実施者が監査調書等を基に監査結果をまとめ、監査報告書案を作成することを指す。

監査報告書には、監査の実施概要、監査結果の概要（総論）、指摘事項、改善提案を記述する。

記載事項	記載内容
監査の実施概要	監査実施計画書の内容を簡潔に記載する。
監査結果の概要（総論）	監査目的で記載した監査対象における対策の適切性について、監査結果から得られた監査責任者の結論を記載する。 ただし、一般的には、監査目的で確認する管理や対策の状況を「適切」又は「適切でない」かのいずれかで判断するのは難しいため、監査実施者の感想、主要な指摘事項、それによって生じる可能性がある問題点、必要な対策等について、報告先が理解しやすいように記載する。
指摘事項	各監査手続を実施した結果、判明した問題点を記載する。指摘事項を記載する際には、指摘事項の重要度、指摘した事項によって生じる可能性がある問題点を記載する。
改善提案	指摘事項を改善するための案及び実施期限等を記載する。改善提案、改善期限等は、あくまで監査体制としての提案である。実際の改善内容は、ＰＪＭＯが監査体制の改善提案等を参考にして検討し、ＰＭＯと調整の上、決定・具体化されていくことになる。

← 表 10-4
監査報告書の記載内容

(5) 「指摘事項の監査対象への確認」

「指摘事項の監査対象への確認」とは、監査体制が作成した監査報告書案の指摘事項について、監査実施者が監査対象の担当者等に確認を行うことを指す。確認するのはあくまで事実関係であり、指摘事項の記載の可否や記述の仕方ではないことに留意すること。

監査実施者は、確認結果に誤りがある場合は、確認結果に基づき、監査報

告書案を修正する。

(6) 「監査報告書の提出」

「監査報告書の提出」とは、監査責任者がＰＭＯに、監査報告書を提出することを指す。監査報告書の提出に当たっては、ＰＭＯ、監査対象のＰＪＭＯ、及び関係者等を集めて報告会を行う等により、監査結果の内容や指摘事項等が適切に理解されるよう努める。

合議制機関等に対する監査結果の報告は、標準ガイドライン「第２編第８章３．システム監査結果の報告」を参照のこと。なお、監査資源の不足、監査対象である情報システムのスケジュール遅延等によりシステム監査計画に記載された監査又はＰＭＯから指示した監査が実施できなかった場合には、その旨を合議制機関等に報告する。

(7) 「監査調書の整理」

「監査調書の整理」とは、監査責任者が、事後の監査結果の検証や、次回以降の監査における今回の監査結果の活用等に向け、監査調書を閲覧しやすいように整理することを指す。

4） 指摘事項への対応

ＰＪＭＯは、**監査結果により指摘された事項については、これを課題として認識の上、改善計画を立案し、監査責任者及びＰＭＯに報告する(1)**ものとする。また、ＰＪＭＯは、改善計画に基づいて、指摘事項への対応を行い、**当該対応の結果について、監査責任者及びＰＭＯに報告する(2)**ものとする。

なお、指摘事項への対応を行った結果、プロジェクト計画書との差異が発生した場合は、プロジェクト推進責任者は、プロジェクト計画書に反映し、当該計画書の内容を更新する。

1. 趣旨

監査責任者より報告された指摘事項は、プロジェクトの目標達成を確実なものとするため、監査報告書の改善提案の内容を踏まえて、監査対象において適切かつ確実に対応される必要がある。

このため、ＰＪＭＯは、指摘事項に対する改善計画を立案し、責任を持って対応し、対応結果を監査責任者及びＰＭＯに報告する。

2. 解説

(1) 「監査結果により指摘された事項については、これを課題として認識の上、改善計画を立案し、監査責任者及びＰＭＯに報告する」

「改善計画を立案し、監査責任者及びＰＭＯに報告する」とは、ＰＪＭＯが、監査結果の指摘事項に対する改善計画を策定し、監査責任者及びＰＭＯに報告することを指す。また、システム監査計画に基づく監査又はＰＭＯの指示による監査の場合にあっては、ＰＭＯに改善計画書を提出し、承認を受ける。ＰＪＭＯは、改善計画書の内容について監査責任者に確認し、必要な助言を受ける。

改善計画の記載事項を、次に示す。

記載事項	記載内容
指摘事項への対応内容	指摘事項への対応方法等を記載する。指摘事項に対応しない場合にはその理由を明記する。 また、対応内容が指摘事項に係るリスクを十分に担保しない場合においても、その理由を明記する。
実施時期又は実施期限	改善計画を実施する時期又は実施期限を記載する。 実施時期が監査体制の提案する実施期限よりも遅くなる場合には、その理由を明記する。
対応責任者	改善計画を実施する責任者を記載する。

← 表 10-5
改善計画の記載内容

(2) 「当該対応の結果について、監査責任者及びＰＭＯに報告する」

「当該対応の結果について、監査責任者及びＰＭＯに報告する」とは、ＰＪＭＯが、改善計画書に記載された事項の対応を全て完了したとき、監査責

任者及びＰＭＯにその旨を報告することを指す。ただし、当該完了日が監査報告書の受領日から起算して３か月を超えるときは、３か月単位で途中経過の報告を行う。

5） フォローアップ

システム監査計画に基づく監査又はＰＭＯの指示による監査の場合は、ＰＭＯは、当該監査の結果への対応について、フォローアップを行う(1)ものとする。

1. 趣旨

指摘事項に対する改善内容は、指摘した問題が確実に対処されている必要があるため、対応内容及び対応結果は、客観的に評価される必要がある。

このため、ＰＭＯは、ＰＪＭＯの作成した改善計画の内容、対応状況、対応結果をフォローアップし、対応が確実に行われるようにする。

2. 解説

(1) 「当該監査の結果への対応について、フォローアップを行う」

「フォローアップ」とは、指摘事項に対する対応状況や対応結果を確認し評価することを指す。

指摘事項のフォローアップを、次に示す。

種類	内容
改善計画のフォローアップ	ＰＭＯは、ＰＪＭＯが作成した改善計画について、指摘事項が網羅的かつ正確に理解された上で検討されているか、また、その検討結果が適切に改善計画に反映されているかを確認する。 システム監査計画及びＰＭＯの指示による監査にあっては、最終的な改善計画及びその実施時期は、監査対象が作成した案を、ＰＭＯが承認することにより確定する。 監査責任者は、改善計画及びその実施時期について、ＰＪＭＯによる改善計画の策定及びＰＭＯの承認に対して助言を行う。
実施状況のフォローアップ	ＰＭＯは、ＰＪＭＯが実施する改善計画に基づいた指摘事項に対する改善の状況確認を行う。 フォローアップは、改善計画書に記載された個別の改善項目が対応されるごとに、できるだけ早く実施することが望ましい。なお、監査を外部委託する場合においては、フォローアップまで含めて調達範囲とすることが望ましい。 ＰＭＯは、システム監査計画にフォローアップを盛り込む。

← 表 10-6
フォローアップの種類

２. システム監査に関する調達の特例

ＰＭＯは、監査業務を委託する場合、「第６章 調達」の規定に従うものとする。このほか、特例として、監査に関する調達仕様書を作成するときは、次の1）から3）までに掲げる事項を盛り込むものとする。

1）　作業の実施に当たっての遵守事項

監査事業者等は、**監査結果及び監査で知り得た情報を監査体制の構成員以外の者と共有してはならないこと**(1)。

2）　入札制限

監査対象である情報システムの調達案件（監査業務案件を除く。）に関与した事業者は、監査の独立性及び客観性の確保の観点から、当該情報システムの監査に関する調達案件の入札に参加できないものとすること(2)（「第６章３．1)クb）入札制限」参照）。

3）　再委託に関する事項

原則として、監査業務の再委託は行ってはならないこと(3)。

1. 趣旨

監査業務を委託する場合は、業務の特性から、「第６章　調達」で規定された内容に加え、特例を盛り込む必要がある。

このため、監査業務に係る調達仕様書には、情報の守秘義務の範囲や、監査業務を調達する際の入札制限について規定する。理由としては、監査実施者が監査対象の情報システムの開発事業者であるなど、何らかの利害関係を有する場合、監査報告書の独立性及び客観性に疑義が生じることになるからである。

また、監査業務においては、機密情報に触れる場合も多いため、関係する事業者をできるだけ限定すべく、再委託の制限についても規定する。

2. 解説

(1) 「監査結果及び監査で知り得た情報を監査体制の構成員以外の者と共有してはならないこと」

「監査結果及び監査で知り得た情報」とは、情報セキュリティインシデントに繋がる情報や非常に秘匿性の高い情報等を指す。したがって、委託先の監査事業者等においても、当該情報を第三者に漏らしてはならないのみならず、事業者内における情報共有には必要最低限の範囲内にとどめるといった細心の注意を払わせる必要がある。

よくあるケースでは、監査の改善提案を作成する場合に、当該改善案に関係する技術的な知識を有する者で監査体制の構成員以外のものに支援を求めることがある。このような場合においても、機密情報の開示を行わないのみならず、委託元名、具体的な業務、情報システム構成等を伏せた上で、助言を求めることとする。

(2)「監査対象である情報システムの調達案件（監査業務案件を除く。）に関与した事業者は、監査の独立性及び客観性の確保の観点から、当該情報システムの監査に関する調達案件の入札に参加できないものとすること」

「監査対象である情報システムの調達案件（監査業務案件を除く。）に関与した事業者」とは、当該情報システムの企画（調査、要件定義等）、開発、運用、保守等の業務のいずれかに携わった事業者を指し、プロジェクト管理支援事業者を含む。

なお、監査対象が情報システムの運用、保守業務であった場合、当該情報システムの開発事業者は、一見、監査の独立性及び客観性を脅かさないようにも考えられる。しかし、監査の実施において開発段階での瑕疵等が発見される場合もあるため、直接、監査対象の業務に関係しない開発事業者等であっても入札制限の対象とすべきである。

(3)「原則として、監査業務の再委託は行ってはならないこと」

「原則として、監査業務の再委託は行ってはならない」とは、監査業務を調達する場合において、受託事業者が再委託を行うことを禁止することをいう。監査業務においては、機密情報に触れる場合も少なくないため、関係する事業者をできるだけ限定する必要がある。また、システム開発等の調達と異なり、監査業務においては、多くの要員は不要であることから再委託を行う必要性が高くない。

ただし、単独の事業者で監査目的を達成することが難しい場合、又は、単独の事業者で実施する場合よりも再委託を行って実施した方が監査の品質を高めることができる場合には、例外として、監査業務の再委託を認める。

例えば、「情報セキュリティ対策の適切性を確認する」という監査目的を達成するために、脆弱性検査、ペネトレーションテスト（侵入テスト）等の特殊な技術を用いた実証的な監査手続を実施した方が良い場合がある。監査サービスを提供する事業者の中には、脆弱性検査、ペネトレーションテストを行っていない事業者も多い。よって、一般的な監査が得意な事業者と技術的な監査が得意な事業者を組み合わせて監査を行った方が、より品質の高い監査を実施することができると考えられる。