システム監査基準

経済産業省

平成 30 年 4 月 20 日

目次

前 文（システム監査基準の活用にあたって）

［1］システム監査の意義と目的

システム監査とは、専門性と客観性を備えたシステム監査人が、一定の基準に基づいて情報システムを総合的に点検・評価・検証をして、監査報告の利用者に情報システム[1]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の一類型である。

また、システム監査は、情報システムにまつわるリスク（以下「情報システムリスク」という。）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システム監査人が点検・評価・検証することを通じて、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、又は利害関係者に対する説明責任を果たすことを目的とする。

［2］システム監査基準の意義と適用上の留意事項

「システム監査基準」（以下「本監査基準」という。）とは、情報システムのガバナンス、マネジメント又はコントロールを点検・評価・検証する業務（以下「システム監査業務」という。）の品質を確保し、有効かつ効率的な監査を実現するためのシステム監査人の行為規範である。

本監査基準は、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、組織体の外部者に依頼するシステム監査においても適用される。

本監査基準は、情報システムの安全性、信頼性、準拠性のみならず、情報シス

---

[1] 情報システム：組織体及び組織体間の諸活動を支えるデータ・情報の収集、蓄積、処理、伝達、利用に関わる活動・仕組み・体系の総称である。情報(通信)技術、人間(行為)、制度・ルールなどによって実体論的もしくは存在論的に構成されるものである。情報技術(IT）は、情報システムを構成する物質的人工物である。

テムの戦略性、有効性、効率性等の監査もカバーし、かつ、中小規模の企業や、各府省庁、地方公共団体、病院、学校法人等、各種組織体が各種目的をもってシステム監査を行う場合にも利用できるように、汎用性のある内容となっている。

なお、組織体の内部監査人がシステム監査を実施する場合には、日本内部監査協会の「内部監査基準」又は内部監査人の国際組織 IIA の「専門職的実施の国際フレームワーク」を、また情報セキュリティ監査制度に基づく監査を実施する場合においては、「情報セキュリティ監査基準」をあわせて参照することが望ましい。

［３］システム監査上の判断尺度

本監査基準に基づくシステム監査においては、情報システムのガバナンス、マネジメント又はコントロールを点検・評価・検証する際の判断の尺度（以下「システム監査上の判断尺度」という。）として、原則として「システム管理基準」又は当該基準を組織体の特性や状況等に応じて編集した基準・規程等を利用することが望ましい。

なお、システム監査は各種目的あるいは各種形態をもって実施されることから、他のガイドラインや組織体独自の諸規程・マニュアル等を、システム監査上の判断尺度として用いることもできる。特に、情報セキュリティの監査に際しては、「システム管理基準」とともに、「情報セキュリティ管理基準」を参照することが望ましい。

［４］本監査基準改訂の背景と主要な改訂内容

本監査基準は、昭和 60 年（1985 年）１月に策定され、その後、平成８年(1996 年) 1 月及び平成 16 年（2004 年）10 月に改訂がされてきたが、その後、システム監査を巡る情報通信技術環境の劇的な変化や、システム監査に対するニーズの多様化がみられたことから、それらを踏まえて基準内容の見直しを行うこととした。

本監査基準の記述形式については、システム監査の実施に際して遵守が求め

られる「基準」を「しなければならない」と記述し、各基準の補足的な説明や、実務上の望ましい対応や留意事項を「解釈指針」として記述した。さらに、従来の本監査基準でみられた「一般基準」、「実施基準」、「報告基準」という体系は、基準の規定を分類・整理する意味しかないことから、今回の改訂では、システム監査実施の流れに沿って、適切な表題を付す方式を採用し、実務への適用を優先するようにした。

Ⅰ．システム監査の体制整備に係る基準

【基準１】　システム監査人の権限と責任等の明確化

システム監査の実施に際しては、その目的及び対象範囲、並びにシステム監査人の権限と責任が、文書化された規程等又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。

＜主　　旨＞

システム監査を効果的に実施し、監査の実施に係るトラブルを避け、監査実施へ協力を得るため、監査の実施に先立って、システム監査人に関する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、周知しておくこと、あるいは外部の専門家に依頼する場合は、契約に先立ち十分な事前協議を行うことが重要である。

＜解釈指針＞

１．　システム監査を組織体の内部監査人が行う場合には、内部監査規程等に、システム監査の内容及びシステム監査人の権限・責任等を適切に文書化するとともに、システム監査を適切に実施できるように組織体内部の適切なレベルでの承認を得る。

(1) 文書化すべき事項としては、例えば、以下のものが挙げられる。

- 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
- システム監査人の権限・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、監査要員、監査費用等）の確保に関する事項
- システム監査人の各種設備や情報資産等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

・システム監査人の守秘義務に関する事項

(2) 内部監査規程等の承認を行う主体は、組織体の個々の事情に応じて様々な形態をとりうる。例えば、内部監査部門を所掌する取締役等が選任されている場合には、内部監査規程等の承認は当該取締役等又は取締役会（監査委員会又は監査等委員会を含む。）等でなされるかもしれない。

２． 組織体の内部に適切なシステム監査人が存在しない場合、あるいは高度な技能を必要とする情報セキュリティの監査、遠隔地にあるデータセンタやクラウドサービスプロバイダに対するシステム監査などにおいては、システム監査 の全部又は一部を、組織体外部の専門事業者（監査法人等を含む。）に委託する場合がある。

このような場合には、委託契約書に、委託するシステム監査業務の内容及び責任等を明確に定める必要がある。

(1) 委託契約書の記載事項としては、例えば、以下のものが挙げられる。

・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

・委託者及び受託者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

(2) システム監査の全部又は一部を組織体外部の専門事業者に委託する場合であっても、当該専門事業者との適切な協働体制と、当該専門事業者に対する適切な監督体制を整えることが重要である。

【基準２】　監査能力の保持と向上

システム監査の品質を高め、組織体の状況やIT環境の変化等に対応して、効果的なシステム監査を実施するために、システム監査人は、適切な研修と実務経験を通じて、システム監査の実施に必要な知識・技能の保持及び向上に努めなければならない。

＜主　　旨＞

システム監査の信頼性を保つためには、専門的な観点からシステム監査が実施される必要がある。また、システム監査人には、組織体の状況変化やIT環境の変化に対応した付加価値の高いシステム監査を実施するために、情報システム及びシステム監査に関する専門的知識・技能が必要になる。また、論理的思考能力やコミュニケーション能力なども求められる。システム監査人は、継続的な研鑽を通じて、効果的かつ効率的なシステム監査を行えるよう、必要な知識・技能の向上を図ることが重要である。

＜解釈指針＞

１．　システム監査を効果的かつ効率的に実施するためには、システム監査に対するニーズを十分に考慮して、適切な知識・技能を有する者がシステム監査を実施する必要がある。

(1) 例えば、サイバー攻撃等の対策が効果的に実施されているかどうかの監査が求められる場合と、情報システムのガバナンスが適切に機能しているかどうかの監査が求められる場合とでは、システム監査人に求められる知識・技能は異なったものとなるであろう。したがって、システム監査のニーズを踏まえた適切な監査担当者をアサインする必要がある。

(2) システム監査の実施に必要な知識・技能の保持及び向上には、組織体内外の講習会等の活用とあわせ、OJT等を通じた実務経験も重要である。なお、組織体の内部で適切な知識・技能を有するシステム監査人を確保できない場合には、組織体外部の専門事業者の支援を考慮する必要がある。

２．　いかなる目的をもっていかなる対象についてシステム監査を実施するかによって一様ではないが、システム監査を効果的かつ効率的なものとし、システム監査の品質を高めるためには、情報システムとその管理、及びシステム監査に関する基礎的な知識・技能はもちろんのこと、経営戦略、ガバナンス、リスク管理、内部統制、及び関連法令等に関する幅広い関連知識を有していることが望ましい。

(1) システム監査人に求められる基本的な知識・技能を習得するためには、システム監査技術者、CISA（公認情報システム監査人）等の試験やCSA（公認システム監査人）の認定制度の活用も考えられる。システム監査に関する一定の専門的知識・技能を有することを認定された試験合格者がシステム監査を実施することは、システム監査の信頼性を担保することにもつながる。

(2) システム監査を効果的かつ効率的に実施するためには、CAAT（コンピュータ支援監査技法）の利活用に関する知識・技能が求められることから、当該技法の習得に努める必要がある。

３．　システム監査の実施に際しては、経営陣や監査対象の関係者とのコミュニケーションが求められる。したがって、システム監査人には、ロジカルシンキング及びロジカルライティングの能力、並びにプレゼンテーション技法及びインタビュー技法なども求められる。

４．　システム監査人は、システム監査の対象を巡る環境変化を常にキャッチアップし、新しい知識・技能を習得し続ける努力が求められることに留意する。特に、情報システムリスクの変化に対する認識を高めるように留意する必要がある。

【基準３】　システム監査に対するニーズの把握と品質の確保

システム監査の実施に際し、システム監査に対するニーズを十分に把握したうえでシステム監査業務を行い、システム監査の品質が確保されるための体制を整備しなければならない。

＜主　　旨＞

システム監査は、任意監査（法令等によって強制されない監査）であることから、基本的にはシステム監査の依頼者（通例、業務執行の最高責任者であるが、内部監査を所管する役職員、又はモニタリング機能を担う役職員等の場合もある。）がいかなるニーズをもっているかを十分に踏まえたものでなければならない。また、システム監査に対するニーズを満たしているかどうかを含め、一定の監査品質を確保するための体制の整備が必要である。

＜解釈指針＞

１．　システム監査を実施する場合、システム監査の依頼者のニーズによって、それに見合ったシステム監査の目的が決定され、システム監査の対象が選択される。

(1) 例えば、次のようなニーズに基づいて、システム監査の目的が決定される。

① 例えば、経営陣が、取引先等からの信頼を得るために、経営者による言明書の範囲内で、自組織の情報システムのマネジメントが有効に機能していることのお墨付きを得たいというニーズをもっている場合、「システム管理基準」に照らして情報システムのマネジメントの状況を評価・検証し、もって保証を目的としたシステム監査が行われる。

② 例えば、経営陣が、自組織のシステム開発管理に重大な不備があるのではないかと不安に思っており、もし不備があればそれを指摘してもらい、改善の具体的な方策を知りたいというニーズをもっている場合、「システム管理基準」に照らして現状のシステム開発管理の状況を評価・検

証し、指摘事項とともに改善提案を行う、助言を目的としたシステム監査が行われる。

なお、上記②の目的をもったシステム監査を行って成熟度が確認できた時点で、①の目的をもったシステム監査が行われることが通例である。

さらに、システム監査のニーズは、以上に限らず、例えば、委託先の管理レベルによって大きな損害を被る可能性があり、その管理レベルが自社の望むレベルであるか判断する材料として、第三者の評価が欲しいというシステム委託者のニーズ、システムを受託するに当たって、委託元が委託先の管理レベルを重視するようになり、委託元に自社のシステム管理レベルを判断してもらう材料として開示したいというシステム受託者のニーズ、社会的責任を負う重要インフラや多数の生命・財産に影響を及ぼす分野及び行政組織など、不特定多数の利害関係者に向けて、説明責任を果たすことを担保したいという社会的責任を負う者のニーズ等がある。

(2) 例えば、次のようなニーズに基づいて、システム監査の対象が選択される。

① 例えば、経営陣が、経営戦略と IT 戦略との整合性、IT 利活用の有効性、企業グループ全体としてみた場合の IT 戦略の合理性についての保証又は助言を得たいというニーズをもっている場合、情報システムのガバナンスを対象とするシステム監査が選択される。

② 例えば、経営陣が、情報システムのサービスレベルの維持、より効率的な情報システムの維持管理、海外拠点に対するプライバシー規制等への対応状況について保証又は助言を得たいというニーズをもっている場合、情報システムのマネジメントを対象とするシステム監査が選択される。

③ 例えば、経営陣が、情報システムに実装された機能要件が、業務要件の変化に対応して、適切に維持管理が行われているかどうかについての保証又は助言を得たいというニーズをもっている場合、情報システムの

コントロールを対象とするシステム監査が選択される。

なお、上記の①、②及び③は、それぞれ別個の監査対象として明確に区別されて選択される場合もあれば、特に区別されずに組み合わせて選択される場合もある。

2． システム監査のニーズに応じて、公表されている各種基準・ガイドライン等を適切に選択し、必要に応じて組み合わせて、判断尺度とすることが望ましい。システム監査上の判断尺度を確定する際の客観的な参照基準として、「システム管理基準」及び「情報セキュリティ管理基準」が推奨される。

なお、システム監査のニーズによっては、「システム管理基準」又は「情報セキュリティ管理基準」の一部分、あるいは組織体の状況に適合するように適宜選択した項目群を監査上の判断尺度とすることもできる。ただし、採用される基準の範囲及び性質によっては、保証の範囲が限定されることに加え、保証の客観性が損なわれる可能性があることに留意する。

3． システム監査の実施に際しては、システム監査業務の品質を維持し、さらにはシステム監査業務の改善を通じてその品質を高めるために、内部監査部門内等での自己点検・評価（内部評価）、及び組織体外部の独立した主体による点検・評価（外部評価）を定期的に実施することが望ましい。

内部監査として実施するシステム監査の場合には、一般社団法人日本内部監査協会の「内部監査基準」やIIAの「内部監査の専門職的実施の国際基準」を参照して品質を高めるようにすることにも留意する必要がある。

システム監査業務の品質維持及び改善に際しては、システム監査に対するニーズにも十分に応えているかどうかという視点を組み込むことが重要である。

(1) システム監査人が自らの業務を継続的又は定期的に見直し、その結果をシステム監査業務の改善に結び付ける努力こそ、システム監査の品質を保ち、向上させるための鍵となることに留意すべきである。

(2) 自らの業務を本監査基準やベストプラクティス等に照らして見直し、改善のための工夫を凝らす試みは、システム監査人の能力向上にもつながる。

４． システム監査を外部の専門事業者に委託して実施する場合にも、委託先における監査の品質管理体制を確かめておくことが必要がある。

Ⅱ．システム監査人の独立性・客観性及び慎重な姿勢に係る基準

【基準４】　システム監査人としての独立性と客観性の保持

システム監査人は、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十分に配慮しなければならない。また、システム監査人は、監査の実施に当たり、客観的な視点から公正な判断を行わなければならない。

＜主　　旨＞

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。また、このようなシステム監査人としての組織上の外観への配慮のみならず、客観的な立場で公正な判断を行うという精神的な態度が求められる。

＜解釈指針＞

１．　システム監査人がその役割と責任を果たすためには、システム監査人は監査対象部門から独立している必要がある。システム監査人の所属する部門が、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。

(1) 組織体に内部監査部門が設置されている場合には、当該部門がシステム監査を実施することが望ましい。

(2) 組織体に内部監査部門が設置されていない場合には、監査対象の領域又は活動に直接従事していない者が実施するか、又は組織体外部の専門事業者への委託によって、外観上の独立性を確保することができる。

(3) システム監査人が、以前、監査対象の領域又は業務に従事していた場合、原則として、監査の任から外れることが望ましい。

２．　システム監査を外部の専門事業者に委託する場合、監査を担当する者が、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、システム監査人の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。

例えば、以前に、委託元組織体のシステム開発を担当していた者、又はシステムの保守に従事していた者がシステム監査人となる場合などは、身分上の利害関係を有するとの外観を呈する。

３．　システム監査人には、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を行う精神的な態度が求められる。もし公正不偏性が保持できない場合には、システム監査の客観性、ひいてはシステム監査の品質及び信頼性を著しく毀損することになるからである。

４．　システム監査人が、客観的な立場で公正な判断を行うためには、システム監査人としての高い倫理観が求められることから、外部からの圧力等を排除しつつ、自らも倫理観の高揚に努める必要がある。

５．　システム監査人が、客観的な立場で公正な判断を行うためには、システム監査人としての専門的な知識・技能が不可欠である。システム監査人が専門的な知識・技能を保持していないと、監査対象業務に責任を有する者や監査対象業務に従事する者の言いなりになるなど、自らの判断を委ねる可能性が高まるからである。また、システム監査人は、常に社内外の状況に目を向けて、組織体の論理や価値観だけで判断を行うのではなく、社会的な視点から見て公正な判断を行うように留意する必要がある。

【基準５】　慎重な姿勢と倫理の保持

システム監査人は、システム監査業務の計画、実施、及び結果の報告において、システム監査の専門家としての慎重な姿勢で臨むとともに、倫理観を保持し、誠実に業務を実施しなければならない。

＜主　　旨＞

システム監査人がシステム監査業務を行う際、システム監査人としての独立性及び客観性の保持と合わせて、システム監査の専門家として要求される慎重さをもって臨むことでシステム監査業務の品質を確保・向上させる必要がある。

＜解釈指針＞

１．　システム監査人としての慎重な姿勢とは、誤った監査上の判断や誤解に基づく監査上の判断がないよう、十分な注意を払うことをいう。

(1) システム監査人としての慎重な姿勢には、業務上の注意深さはもちろんのこと、とりわけ保証を目的とした監査においては、入手した監査証拠の十分性、適切性、正確性について精査するなど、建設的な検討を意識する態度の保持が含まれる。

(2) システム監査人としての慎重な姿勢は、システム監査に関する専門的な知識・技能にも左右されることから、システム監査人は、専門的な知識・技能の保持及び向上に努める必要がある。

(3) システム監査人としての慎重な姿勢は、あくまでも合理的な注意をもって監査を実施することを意味するから、監査上の判断に絶対に誤りのないことや、突出した成果を意味するものではないことに留意する。

２．　システム監査人として要求される慎重さには、職業倫理の遵守が含まれる。通常、下記の各団体に所属、又は専門資格を認定されているシステム監査人は、各団体で要求される専門職としての職業倫理の遵守が求められる。

・特定非営利活動法人日本システム監査人協会

・システム監査学会
・ISACA
・一般社団法人日本内部監査協会
・日本公認会計士協会

３．　システム監査人は、求められる倫理の一環として、業務上知り得た事項を正当な理由なく他に開示するなど、自らの利益のために利用してはならない。なお、システム監査人の守秘義務は、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。

Ⅲ．システム監査計画策定に係る基準

【基準６】　監査計画策定の全般的留意事項

システム監査人は、実施するシステム監査の目的を効果的かつ効率的に達成するために、監査手続の種類、実施時期、及び適用範囲等について、適切な監査計画を立案しなければならない。監査計画は、状況に応じて適時に変更できるように弾力的なものでなければならない。

＜主　　旨＞

システム監査を効果的かつ効率的に実施するためには、必要十分な時間をかけて監査計画を策定する必要がある。監査計画は、システム監査業務の進捗管理の手段となりうるが、状況に応じた適時な見直しを行うことも重要である。

＜解釈指針＞

１．　監査計画は、通例、中長期計画、年度計画、及び個別監査計画に分けて策定される。

(1) 中長期計画とは、システム監査の中長期における方針等を明らかにすることを目的として作成する。システム監査を経営に貢献するものとするために、又は利害関係者に対する説明責任を果たすために、情報システムの中長期計画と整合をとり、システム開発・更改計画やIT基盤の構築・更改などを踏まえて、中長期システム監査計画を策定する。

中長期計画には、例えば、次の事項が記載される。

・システム監査の中長期方針（情報システムの中長期計画との関係を含む。）

・システム監査の実施体制の整備（システム監査人材の育成等を含む。）

・システム監査の中長期方針に基づく主要な監査対象領域

・中長期にわたる監査資源への投資額の概算

(2) 年度計画とは、中長期計画に基づいて、システム監査の年間スケジュー

ルを内容とするものをいう。基本計画とも呼ばれる。

年度計画には、例えば、次の事項が記載される。

・システム監査の年間方針（年間を通じての重点課題、優先課題等）

・当該年度のシステム監査の目的

・当該年度に実施すべき監査対象（対象となる情報システム、業務、部門、テーマ等）

・上記事項を裏付けるためのリスクアセスメントの結果

・年間の監査スケジュール

・年間の監査費用の概算額

(3) 個別監査計画とは、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とし込んだ詳細計画書をいう。

個別監査計画には、例えば、次の事項が記載される。

・システム監査の目的

・システム監査の対象（年度計画に記載された監査対象から選択する。）とその重点課題及び着眼点

・上記事項を裏付けるためのリスクアセスメントの結果

・監査責任者及び監査担当者（担当者間の分担を含む。）

・監査日程（監査の開始日と終了予定日）等の詳細スケジュール

・監査場所

・利用する判断の尺度

・実施すべき監査手続の概要

・監査結果の報告予定時期

・監査費用の見積額（年度計画の監査費用概算を基に算出）

(4) アジャイル開発手法は、開発部門と利用部門の協調によって迅速かつ柔軟な反復的･継続的開発をすることが本来の意義である。したがって、アジャイル開発手法を採用するシステム開発プロジェクトなどでは、あらかじめ監査対象となる関係部門においてシステム監査の意義と必要性への十分な認識を培うとともに、アジャイル開発手法の本来の意義を損なわな

いように留意しつつ、監査実施のタイミング、サイクル、作業負荷、及び監査証拠の範囲･種類などを特定して計画を立案する。

２． 監査計画の前提としていた状況が変化した場合、システム監査の実施過程で新たな状況が発見された場合、又はやむを得ない事情により監査体制の変更が生じた場合には、適宜、計画を修正する必要がある。

３． 監査計画の策定にあたっては、監査対象が情報システムのガバナンスに関するものか、情報システムのマネジメントに関するものか、あるいは情報システムのコントロールに関するものかを考慮する。

(1) 情報システムのガバナンスを監査対象とする場合、情報システムの利活用が経営目的に沿っているか、また、経営陣が経営戦略に沿うように管理者に適切な方向付けを行い、かつ、適切な是正措置が講じられているかどうかを確かめることに重点を置いた監査計画となる。例えば、経営戦略とIT戦略との整合性、並びに新技術及びイノベーションの経営戦略への組み込みなどの戦略リスクへの対応の状況に関する監査計画が必要となる。

(2) 情報システムのマネジメントを監査対象とする場合、経営陣による方向付けに基づいて、PDCAサイクルが確立され、かつ適切に運用されているかどうかを確かめることに重点を置いた監査計画となる。例えば、IT投資管理や情報セキュリティ対策が、PDCAサイクルに基づいて、組織体全体として適切に管理されているかどうかに関する監査計画が必要となる。

(3) 情報システムのコントロールを監査対象とする場合、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、機能しているかどうかを確かめることに重点を置いた監査計画となる。例えば、規程に従った承認手続が実施されているかどうか、異常なアクセスを検出した際に適時な対処及び報告がなされているかどうかなどに関する具体的な監査計画が必要となる。なお、ここでいうコントロールには、手作業によるコントロールと、情報システムに組み込まれた自動化されたコントロール

の双方が含まれることに留意する。

【基準７】　リスクの評価に基づく監査計画の策定

システム監査人は、システム監査を行う場合、情報システムリスク、及びシステム監査業務の実施に係るリスクを考慮するリスクアプローチに基づいて、監査計画を策定し、監査を実施しなければならない。

＜主　　旨＞

システム監査を効果的かつ効率的に実施するためには、リスクに基づく監査計画の策定（以下「リスクアプローチ」という。）が必要となる。ここでいうリスクアプローチには、２つの考え方がある。第１は、リスクの影響が大きい監査対象に重点的に監査資源を配分するというアプローチである。第２は、監査の結論を誤る可能性としての監査リスクを合理的に低い水準に抑えるというアプローチである。

＜解釈指針＞

１．　システム監査人は、情報システムリスクの特性及び影響を見極めた上で、リスクが顕在化した場合の影響が大きい監査対象領域に重点的に監査資源（監査時間、監査要員、監査費用等）を配分し、その一方で、影響の小さい監査対象領域には相応の監査資源を配分するように監査計画を策定することで、システム監査を効果的かつ効率的に実施することができる。

２．　情報システムリスクは、情報システムに係るリスク、情報に係るリスク、情報システム及び情報の管理に係るリスクに大別される。

(1) 情報システムに係るリスクとは、情報システムの入力、処理、保存、出力プロセスの信頼性、安全性、有効性、効率性等が確保できないとか、IT戦略と業務プロセスとの不整合などのリスクである。

(2) 情報に係るリスクとは、情報システムで処理、保存、出力される情報が、目的に従った利活用ができないとか、情報の機密性、完全性、可用性が確保できないなどのリスクである。

(3) 情報システム及び情報の管理に係るリスクとは、上記(1)及び(2)のリスクに対処するための体制・手続等に不備が含まれているリスクである。

システム監査人は、上記(1)及び（2）のリスク（固有リスクと呼ばれることもある。）と、それらに対応する(3)のリスク（統制リスクと呼ばれることもある。）を踏まえて、監査計画を策定する必要がある。

３． 情報システムリスクは常に一定のものではないため、システム監査人は、その特性の変化及び変化がもたらす影響に留意する必要がある。情報システムリスクの特性の変化及びその影響を理解したり、リスクに関する情報を更新したりする手法として、例えば監査対象部門による統制自己評価(Control Self-Assessment： CSA)や、システム監査人による監査対象部門に対する定期的なアンケート調査やインタビューなどがある。

４． システム監査人は、監査報告において指摘すべき監査対象の重要な不備があるにもかかわらず、それを見逃してしまう等によって、誤った結論を導き出してしまうリスク（監査リスクと呼ばれることもある。）を合理的に低い水準に抑えるように、監査計画を策定する必要がある。

(1) 監査は、時間、要員、費用等の制約のもとで行われることから、監査リスクを完全に回避することはできない。

(2) 監査リスクを合理的に低い水準に抑える監査計画の策定と監査の実施は保証の目的をもったシステム監査において重要となる。

Ⅳ．システム監査実施に係る基準

【基準８】　監査証拠の入手と評価

システム監査人は、システム監査を行う場合、適切かつ慎重に監査手続を実施し、監査の結論を裏付けるための監査証拠を入手しなければならない。

＜主　　旨＞

システム監査では、監査計画に基づく監査手続の実施の結果として監査証拠が入手され、それに基づいて監査の結論が形成される。監査手続に基づく監査証拠の入手は、監査の結論を得るために必要不可欠なものである。

＜解釈指針＞

１．　システム監査において、システム監査人は、個別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。

２．　監査手続は、監査対象の実態を把握するための予備調査（事前調査ともいう。）、及び予備調査で得た情報を踏まえて、十分かつ適切な監査証拠を入手するための本調査に分けて実施される。

(1)　予備調査によって把握するべき事項には、例えば、監査対象(情報システムや業務等)の詳細、事務手続やマニュアル等を通じた業務内容、業務分掌の体制などがある。なお、監査対象部門のみならず、関連部門に対して照会する必要　がある場合もある。

(2) 予備調査で資料や必要な情報を入手する方法には、例えば、関連する文書や資料等の閲覧、監査対象部門や関連部門へのインタビューなどがある。

(3) 本調査は、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をいう。十分かつ適切な監査証拠とは、証拠としての量的十分性と、確かめるべき事項に適合しかつ証明力を備えた証拠をいう。

(4)　本調査において証拠としての適切性を確保するためには、単にインタ

ビュー等による口頭証拠だけに依存するのではなく、現物・状況等の確認や照合、さらにはシステム監査人によるテストの実施、詳細な分析などを通じて可能な限り客観的で確証的な証拠を入手するよう心掛けることが重要である。

3． 監査手続の適用に際しては、チェックリスト法、ドキュメントレビュー法インタビュー法、ウォークスルー法、突合・照合法、現地調査法、コンピュータ支援監査技法などが利用できる。

(1) チェックリスト法とは、システム監査人が、あらかじめ監査対象に応じて調整して作成したチェックリスト（通例、チェックリスト形式の質問書）に対して、関係者から回答を求める技法をいう。

(2) ドキュメントレビュー法とは、監査対象の状況に関する監査証拠を入手するために、システム監査人が、関連する資料及び文書類を入手し、内容を点検する技法をいう。

(3) インタビュー法とは、監査対象の実態を確かめるために、システム監査人が、直接、関係者に口頭で問い合わせ、回答を入手する技法をいう。

(4) ウォークスルー法とは、データの生成から入力、処理、出力、活用までのプロセス、及び組み込まれているコントロールを、書面上で、又は実際に追跡する技法をいう。

(5) 突合・照合法とは、関連する複数の証拠資料間を突き合わせること、記録された最終結果について、原始資料まで遡ってその起因となった事象と突き合わせる技法をいう。

(6) 現地調査法とは、システム監査人が、被監査部門等に直接赴き、対象業務の流れ等の状況を、自ら観察・調査する技法をいう。

(7) コンピュータ支援監査技法とは、監査対象ファイルの検索、抽出、計算等、システム監査上使用頻度の高い機能に特化した、しかも非常に簡単な操作で利用できるシステム監査を支援する専用のソフトウェアや表計算ソフトウェア等を利用してシステム監査を実施する技法をいう。

なお、上記以外にも、コンピュータを利用した監査技法として、テストデータ法（あらかじめシステム監査人が準備したテスト用データを監査対象プログラムで処理し、期待した結果が出力されるかどうかを確かめる技法）、監査モジュール法（システム監査人が指定した抽出条件に合致したデータをシステム監査人用のファイルに記録し、レポートを出力するモジュールを、本番プログラムに組み込む技法）などが利用されることもある。ただし、これらの技法は、システムのバックアップ状況を確認して復元性を確保した上で利用することが望ましい。

さらに、サイバー攻撃を想定した情報セキュリティ監査などにおいては、ペネトレーションテスト法（システム監査人が一般ユーザのアクセス権限又は無権限で、テスト対象システムへの侵入を試み、システム資源がそのようなアクセスから守られているかどうかを確認する技法）などが利用されることもある。

4． アジャイル手法を用いたシステム開発プロジェクトなど、精緻な管理ドキュメントの作成に重きが置かれない場合は、監査証拠の入手において、以下のような事項を考慮することが望ましい。

(1) 例えば、採用されるフレームワークなどの開発手法そのものに、監査のために最低限必要となる情報をあらかじめ定義したり、自動化ツールを用いて、監査証拠を入手したりするなど、アジャイル手法を用いる開発現場に、監査対応のためだけのドキュメント作成に追加的な負荷をかけないような考慮が望ましい。

(2) 監査証拠の入手に自動化ツールを採用する場合、以下に掲げる事項を考慮する。

・入手したデータの完全性

・入手するデータの目的適合性

・入手過程における改ざん、改変からの保護

(3) 必ずしも管理用ドキュメントとしての体裁が整っていなくとも監査証

拠として利用できる場合があることに留意する。例えばホワイトボードに記載されたスケッチの画像データや開発現場で作成された付箋紙などが挙げられる。

(4) 必要となる監査証拠を適時に入手するためには、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、ルールが公式化され、常に適切に実践されていることを確認することが重要である。

なお、クラウドコンピューティングサービスを利用するような場合には、システム監査自体を実施することが困難なケースがあることに留意する。

5． 監査手続は、それぞれ単独で実施される場合もあるが、通常は、一つの監査目的に対して複数の監査手続の組み合わせによって構成される。

(1) 例えば、情報システムのアクセス権限付与の妥当性を監査目的とした場合の監査手続の組み合わせは、以下のようになる。

・アクセス権限付与のポリシー及び付与手続に関する規程類のドキュメントレビュー

・アクセス権限付与プロセスのウォークスルー

・アクセス権限付与を実施する担当者へのインタビュー又はチェックリストに対する回答の入手と検討

・情報システム上の実際のアクセス権限付与状況と、アクセス権限申請書との突合・照合

なお、無効となったアクセス権限を用いたテストデータを用いて、実際に拒絶されることをシステム監査人が直接確かめることが必要な場合もある。

(2) 例えば、委託管理の適切性を監査目的とした場合の監査手続の組み合わせは、以下のようになる。

・委託先選定基準や委託先決定にあたっての承認記録のドキュメントレビュー

・委託契約の条項（機密保持、監査権、再委託条項など）のドキュメント

レビュー

・委託先における情報セキュリティ管理状況に関するチェックリストに対する回答の入手と検討

・委託先からの業務報告書のドキュメントレビューを通じた業務内容と委託契約の条項との突合・照合、外部委託業者へのインタビュー

・（必要に応じて）外部委託業務実施拠点に対する現地調査

なお、委託先が第三者による保証又は認証を受けており、当該保証等報告書に依拠し、上記手続の一部を省略する場合、当該第三者の能力、客観性及び専門職としての正当な注意について検討を行った上で、委託業務の重要性とリスクを勘案する必要がある。

【基準９】　監査調書の作成と保管

システム監査人は、監査の結論に至った過程を明らかにし、監査の結論を支える合理的な根拠とするために、監査調書を作成し、適切に保管しなければならない。

＜主　　旨＞

監査調書は、システム監査人が実施した監査のプロセスを記録したものであり、かつ、監査の結論の基礎となるものであることから、秩序ある形式で、監査調書として記録、適切に保管しておく必要がある。

＜解釈指針＞

１．　システム監査人は、すべてのシステム監査において、実施内容の客観性等を確保するために、監査調書を作成する。

２．　監査調書の記載事項は、システム監査の目的等によって一様ではないが、システム監査においては、通常、以下の事項を含む。ただし、これらに限定されない。

- 監査実施者及び実施日時
- 監査の目的
- 実施した監査手続
- 入手した監査証拠
- システム監査人が発見した事実（事象、原因、影響範囲等）及び発見事実に関するシステム監査人の所見
- 監査調書のレビューが行われた場合には、レビューアの氏名及びレビュー日

３．　監査調書に記載されたシステム監査人の所見は、システム監査人の意見形成のための合理的な根拠となる。

４．　監査調書は、組織の文書管理規程に従って体系的に整理し、後日、容易に参照、活用できるように保管する必要がある。

５．　監査調書には、組織体の重要情報や機密情報が含まれていることが一般的であり、通常、電子媒体で保管されることから、監査調書の受け渡しや持ち出し等のルールを定めるとともに、未承認アクセスに対する防止対策、及び適切なバックアップ対策を講じるようにし、監査調書の散逸、改ざん等に十分に留意する。

【基準１０】　監査の結論の形成

システム監査人は、監査報告に先立って、監査調書の内容を詳細に検討し、合理的な根拠に基づき、監査の結論を導かなければならない。

＜主　　旨＞

システム監査人は、監査報告に先立って、監査調書に基づいて結論を導く必要がある。保証を目的としたシステム監査であれ、助言を目的としたシステム監査であれ、結論の報告は合理的な根拠に基づくものでなければならない。

＜解釈指針＞

１．　システム監査人は、結論を表明するための合理的な根拠を得るまで監査手続を実施することで、十分かつ適切な監査証拠を入手し、結論表明のための合理的な根拠を固める必要がある。

２．　システム監査人は、監査調書に基づいて結論表明のための合理的な根拠を固める必要があり、論理の飛躍がないように心掛ける必要がある。

３．　システム監査人は、監査調書の内容から明らかになった、情報システムのガバナンス、マネジメント、又はコントロールの不備がある場合、その内容と重要性から監査報告書の指摘事項とすべきかどうかを判断する必要がある。

その場合、システム監査人は、監査調書に記載された不備の全てを監査報告書における指摘事項とする必要はない。また、監査報告書の指摘事項とすべき場合であっても、その内容と重要性に基づいて、事前に順位付けを行っておく必要がある。

４．　監査報告書における指摘事項とすべきと判断した場合であっても、監査調書に記録されたシステム監査人の所見、当該事実を裏づける監査証拠等につ

いて、監査対象部門との間で意見交換会や監査講評会を通じて事実確認を行う必要がある。

Ⅴ． システム監査報告とフォローアップに係る基準

【基準１１】　監査報告書の作成と提出

システム監査人は、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。

＜主　　旨＞

システム監査人は、監査報告書を作成し、監査依頼者に提出する必要があるが、報告すべき内容を理解しやすい方法で報告することが重要である。

＜解釈指針＞

１． システム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、適時性に留意する。また、図（アプリケーションシステムの関係図、処理プロセス図など)、表、グラフ、イラスト、写真などを利用することも効果的である。さらに、表現が敵対的になることを避け、建設的なものとすることを心掛ける必要がある。

(1) システム監査報告書は、システム監査の依頼者が当該報告書の主要読者となる点に留意し、経営陣を宛先とする場合には、詳細監査報告書とは別に、要約監査報告書として作成・報告するなどの工夫が望ましい。なお、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ことが望ましい。

(2) システム監査報告書の作成に際して、業務監査に関する監査報告書と一体のものとして作成することが効果的な場合がある。

(3) システム監査報告は、文書で作成することを原則とするが、緊急を要する場合には口頭で報告を行うこととし、後日、監査報告書を提出することができる。

(4) なお、組織体によっては、ペーパレス化を行っているので、プレゼンテーションソフトを利用したり、電子ファイルで作成することもある。組織

体の状況に応じて工夫する必要がある。

2．　システム監査の依頼者が業務執行の最高責任者である場合、最高責任者に対する報告とあわせて、取締役会、監査委員会（監査等委員会）又は監査役会等、組織体のガバナンス機能を担う機関にも監査報告書を提出することが望ましい場合がある。とりわけ、情報システムのガバナンスを対象としたシステム監査報告書や、監査報告書において情報システムのガバナンスに言及しているなど、監査報告の内容が組織体の経営に直結するとか、経営を脅かす重要なリスクとなりうるような場合にも、ガバナンス機能を担う機関に対してシステム監査報告書を提出することが望ましい。

3．　監査対象部門に対しては、監査依頼者たる経営陣の了承を得たうえで、監査報告書の写しを回付することが望ましい。とりわけ、監査報告書に指摘事項及び改善提案を記載した場合には、当該事項に関係する監査対象部門に対しては、当該監査に限定した監査報告書を提出するなどの工夫を行うことが望ましい。また、監査対象部門以外であっても、当該指摘事項及び改善提案と密接に関連する部門等があれば、必要に応じて当該部門等に対しても、写しを回付することが望ましい。

4．　システム監査報告書の記載事項やその記載方法は、監査の目的、あるいは監査報告書の提出先等に応じて一様ではないが、以下に例示するような記載を行うことが望ましい。

(1) 監査の概要

以下に例示する事項を簡潔明瞭に記載する。

・監査の目的（ニーズ、根拠、背景等でもよい。）

・監査の対象（その選定根拠等を含むことが望ましい。）

・監査の実施期間

・監査の実施者

・（必要に応じて）採用した監査手続の概要

(2) 監査の結論

例えば、以下のように記載する。なお、下記は、その一例にすぎず、記載の形式や記載の文言について標準的となるものはないので、システム監査人が適宜工夫を行うことで、活用される監査報告書とすることが重要である。

＜例１＞ 監査対象に保証を付与する場合

x 年 x 月 x 日から y 年 y 月 y 日の期間（時点の場合には、x 年 x 月 x 日現在と記入する。）に係る AAA（対象としたシステム等を記入する。）は、BBB（「システム管理基準」等の判断の尺度を記入する。）に照らして適切であると認められる（又は重要な指摘事項は見当たらなかった)。

＜例２＞ 監査対象について助言を行う場合

AAA（対象としたシステム等を記入する。）について、BBB（「システム管理基準」等の判断の尺度を記入する。）に照らして監査手続を実施した結果、以下の検出事項が発見されたので、その改善勧告を含めてここに報告する。 記 １．指摘事項　xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx ２．改善勧告　xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

＊ 指摘事項と改善勧告とは、それぞれが対応するように記載する必要がある。

＊ 指摘事項の記載に際しては、リスクの重大性など、指摘事項の根拠となった事項をあわせて記載することが望ましい。

＊ 改善勧告の記載に際しては、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こと。あわせて、改善に責任を有する担当部署を明確にする必要がある。

＊ 改善勧告の記載に際しては、改善事項のみならず、改善によって期待される効果等を記載することが望ましい。

＊ 監査対象について保証の付与と助言をあわせて行う場合、助言については、別途「助言報告書」等の表題を付した個別の報告書を作成することが望ましい。

(3) その他特記すべき事項

システム監査の概要や結論につき、システム監査人が、下記の例のように、特に監査報告書読者の注意を喚起する必要性を認めた場合には、その他特記すべき事項として記載する。

・IT 戦略や IT 投資方針の変更
・情報システム運用体制の大幅な変更
・情報システムの重大な障害の発生

５． 組織体の会計監査人、監督官庁、取引先等、組織体の外部者からシステム監査報告書の提出又は開示要請があった場合、監査依頼者の了解が必要であることはいうまでもなく、提出又は開示先の限定、開示内容の範囲と粒度、開示の制限に関する契約上の義務等を勘案して慎重に対応する必要がある。

【基準１２】　改善提案のフォローアップ

システム監査人は、監査報告書に改善提案を記載した場合、適切な措置が、適時に講じられているかどうかを確認するために、改善計画及びその実施状況に関する情報を収集し、改善状況をモニタリングしなければならない。

＜主　　旨＞

システム監査は、監査報告書の作成と提出をもって終了するが、監査報告書に改善提案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。なお、システム監査人は、改善の実施そのものに責任をもつことはなく、改善の実施が適切であるかどうかをフォローアップし、システム監査の依頼者たる経営陣に報告することになる点に留意する。

＜解釈指針＞

１．　システム監査人は、監査報告書に記載した改善提案への対応状況について監査対象部門又は改善責任部門等から、一定期間以内に、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を記載した改善計画書を受領し、適宜、改善実施状況報告書などによって改善状況をモニタリングする必要がある。

(1) 監査報告書の発行前に、監査の指導機能により、監査対象部門の自発的な取り組みによって発見された不備への改善が実施される場合もあるが、それはフォローアップとは区別されなければならない。

(2) フォローアップは、発見された不備の重要性、改善対応に要する期間を含む改善の難易度、その他監査対象部門の状況に応じて弾力的に実施することが望ましい。

(3) 監査対象部門による所要の措置には、改善提案のもととなった指摘事項の重要性に鑑み、当該指摘事項に関するリスクを受容すること、すなわち改善提案の趣旨を踏まえた追加的な措置を実施しないという意思決定が含まれる場合もある。

２．　フォローアップは、監査対象部門の責任において実施される改善をシステム監査人が事後的に確認するという性質のものであり、システム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留意すべきである。

３．　監査対象部門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し、システム監査人の改善提案のもととなった指摘事項の重大性等を総合的に勘案して、追加的な検証が必要かどうか、あるいは次回のシステム監査に反映すべき点がないかどうかを検討することが望ましい。

４．　監査対象部門又は改善責任部門が実施した改善策が不十分であるか、又は改善提案に基づく問題解決がなされないまま放置されている場合は、当該部門に対して、再度の改善対応を要請する必要がある。また、改善が適切かつ適時に行われない場合のリスクを明確にして、システム監査の依頼者たる経営陣に報告することが必要な場合もある。

５．　フォローアップの終了後、フォローアップ報告書を作成し、システム監査の依頼者たる経営陣に報告し、その写しを監査対象部門又は改善責任部門に回付する必要がある。