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。