システム監査基準・システム管理基準の改訂における課題と対応策

Issues and Countermeasures in Revising the System Audit Standards and the System Management Standards

石島　隆
ISHIJIMA Takashi
法政大学　Hosei University

要旨: 経済産業省が公表しているシステム監査基準・システム管理基準は、2018 年 4 月に改訂が行われたが、その後の情報通信システムやシステム開発・運用技術の変化、デジタル・トランスフォーメーションに向けた様々な動きに対応して、改訂が必要となっている。本稿では、システム監査制度そのものと、システム監査基準・システム管理基準の改訂に関する論点について検討した。その結果、①システム監査制度と情報セキュリティ監査制度の統合、②システム監査企業台帳制度の見直し、③システム管理基準を廃止し、システム監査実施ガイドラインとして再構成するとともに、改訂の頻度を増やすことを提案した。なお、システム監査実施ガイドラインの作成に当たっては、Society5.0 におけるアジャイル・ガバナンスと情報品質特性を考慮する必要がある。

キーワード: システム監査基準、システム管理基準、サイバー・フィジカルシステム、国際標準、情報品質

Abstract: The System Audit Standards and the System Management Standards published by the Ministry of Economy, Trade and Industry (METI) were revised in April 2018, and the revisions are necessary to respond to the subsequent changes in information and communication systems, system development and operation technologies, and various movements toward digital transformation. In this paper, the system audit system itself and the issues related to the revision of the System Audit Standards and the System Management Standards are discussed. As a result, it was proposed that (1) the System Audit System and the Information Security Audit System be integrated, (2) the System Audit Corporate Ledger System be reviewed, and (3) the System Management Standards be abolished and restructured as a system audit implementation guideline, and that the frequency of revision be increased. In addition, it is necessary to consider the agile governance and information quality characteristics in Society 5.0 when developing the system audit implementation guidelines.

Keywords: System Audit Standards, System Management Standards, Cyber Physical System, International Standards, Information Quality

1. はじめに

経済産業省が公表しているシステム監査基準は、システム監査を実施する監査人の行為規範及び監査手続の規則を規定しており、また、システム管理基準は、システム監査人の判断の尺度を規定している（経済産業省，2018a）。

両基準は、2018 年 4 月に改訂が行われたが、その後の情報通信システムやシステム開発・運用技術の変化、デジタル・トランスフォーメーションに向けた様々な動きに対応して、システム監査関係諸団体により、改訂に向けた議論が始まっている。

そこで、以下においては、両基準の改訂に関する論点について検討するとともに、Society5.0 において求められるシステム監査の新たな機能について述べる。

なお、本稿は、システム監査学会第 34 回公開シンポジウム（2021 年 11 月 5 日開催）の発表論文に新たな観点を盛り込んで大幅に加筆修正したものである（石島隆，2021b）。

2. システム監査制度そのものに関する課題

システム監査は、「情報システムのライフサイクル」に着目して構築されてきたが、情報セキュリティ監査が対象としてきた「情報資産」の観点との統合が必要である。また、アジャイル・ガバナンスに貢献する監査の視点からは「情報」の信頼性を保証する機能が重要である。したがって、システム監査制度と情報セキュリティ監査制度を棲み分けするのではなく、IT に関連する監査制度として一本化することが望ましい。さらに、情報品質特性を定義することにより、一貫性・整合性のある体系化を図ることが必要である。詳細については、5.及び 6. で述べる。

また、システム監査基準に則ってシステム監査を行う企業（個人事業主を含む。）を登録するシステム監査企業台帳制度が運用されている。情報セキュリティ監査制度においても同様の制度があったが、現在は、情報セキュリティサービス審査登録制度に移行している（経済産業省，2018b and 2018c）。現状では、各システム監査企業の申告に基づいて情報が登録されているのみであり、各社のサービス品質の評価は行われていない。今後、登録制度の見直しが必要である。

3. システム監査基準の改訂に関する課題

システム監査基準は、システム監査を実施するにあたって順守すべき規範について定めている。システム監査基準の構成を表 1 に示した。

システム監査は、従来、組織体を単位として実施されてきたが、今日のサイバー・フィジカルシステムを前提とすると、業務系システムのみでなく、制御系システム、組込系システムなども対象として、組織体の単位を越えた監査の実施や監査主体間の連携が必要となっている。このため、監査人間の連携や他の監査人への依拠に関する定めの検討が必要である。

なお、システム監査は、内部監査人が実施する場合と外部機関に委託して実施する場合があり、監査人の独立性にも差異がある。内部監査の国際基準や公認会計士又は監査法人が実施する検証業務との関係をどのように監査基準に反映すべきかについての検討が必要である。

表1 システム監査基準の構成

前 文（システム監査基準の活用にあたって）	
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 【基準２】 監査能力の保持と向上 【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
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 【基準５】 慎重な姿勢と倫理の保持
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 【基準７】 リスクの評価に基づく監査計画の策定
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 【基準９】 監査調書の作成と保管 【基準１０】 監査の結論の形成
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 【基準１２】 改善提案のフォローアップ

（出典）経済産業省（2018a）

4. システム管理基準の改訂に関する課題

システム管理基準は、システム監査の対象となる情報システムに関わるガバナンスとマネジメントのあり方について定めている。システム管理基準の構成を表 2 に示した。

新技術への対応に関しては、2018 年改訂時に「アジャイル開発」の章が設けられたが、アジャイル開発は、各種の開発メソッドの一つであり、システム管理基準の体系を崩している。アジャイル開発、AI（Artificial Intelligence）、IoT（Internet of Things）のような応用領域については、基準本体とは別冊にすることで、機動的な修正・追加を可能とする必要がある。

表 2 システム管理基準の構成

前文(システム管理基準の活用にあたって)
システム管理基準の枠組み
IT ガバナンスの定義
IT ガバナンスにおける EDM モデル※
IT ガバナンスにおける 6 つの原則
システム管理基準の前提となる組織体制
Ⅰ．IT ガバナンス
Ⅱ．企画フェーズ
Ⅲ．開発フェーズ
Ⅳ．アジャイル開発
Ⅴ．運用・利用フェーズ
Ⅵ．保守フェーズ
Ⅶ．外部サービス管理
Ⅷ．事業継続管理
Ⅸ．人的資源管理
Ⅹ．ドキュメント管理
用語定義
参考文献

（出典）経済産業省（2018a）

1985 年にシステム監査基準が制定された際には、実施基準の中に、監査の観点が記載されていたが、2004 年の改定時に、システム監査基準とシステム管理基準に分割された。

システム監査基準とシステム管理基準は、公認会計士等が実施する財務諸表監査における監査基準と会計基準の関係に相当するが、業務系システムのみでなく、制御系システム、組込系になどを含む情報システムは広範であり、様々な技術分野を包含・網羅した総合的な管理基準の作成には長い期間と労力を要するものと考える。

一方、情報システムに関連するガバナンス、マネジメント及びテクノロジーについては、国際標準である ISO 規格や日本の国家規格である JIS が制定されており、環境変化に対応して新たな規格の制定や規格の更新が行われている。

例えば、JIS においては、IT ガバナンスについて「JIS Q 38500：2015 情報技術 IT ガバナンス」が、システムライフサイクルプロセスに関連して「JIS X 0170：2020 システムライフサイクルプロセス」及び「JIS X 0160：2021 ソフトウェアライフサイクルプロセス」が制定されている。また、システム監査の隣接領域ともいえる品質管理の分野においては、日本発のソフトウェア品質管理知識体系である SQuBOK（Software Quality Body of Knowledge）が作成されており、現在第 3 版のガイドブックが刊行されている（飯泉紀子他，2020）。

このような情報システムに関連するガバナンス、マネジメント及びテクノロジーに関する規格や知識体系をさらにまとめ直すことよりも、システム監査基準を補完するものとして、システム監査実施ガイドラインを作成し、IT 環境やテクノロジーの変化に対応して、改訂頻度を増やすことが合理的と考える。

システム監査実施ガイドラインの構成については、全般的監査実施ガイドラインとテーマ別監査実施ガイドラインに大別し、以下のような体系を提案する。なお、テーマ別監査実施ガイドラインについては、前述の SQuBOK のソフトウェア品質の応用領域を参考にした（飯泉紀子他，2020）。

① 全般的監査実施ガイドライン

・IT ガバナンス監査実施ガイドライン

・システムライフサイクルプロセス監査実施ガイドライン

② テーマ別監査実施ガイドライン
・AI システム監査実施ガイドライン
・IoT システム監査実施ガイドライン
・アジャイル開発と DevOps 監査実施ガイドライン
・クラウドサービス監査実施ガイドライン
・オープンソース監査実施ガイドライン

具体的な監査実施ガイドラインの作成は、システム監査の実務家団体等の連合組織に委ね、改訂の頻度を増やすことを提案する。

また、情報システムに関わる技術進歩は著しく、サイバー・フィジカルシステムを社会に実装していくためのアジャイル・ガバナンスが提案されており、システム監査の対象にも大きな影響を与える（経済産業省，2021）。これらの観点については、5.及び 6.で述べる。

5. Society5.0 において求められるシステム監査の新たな機能

Society 5.0の世界では、サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムの利用により、ユーザの利便性の拡大が期待される。一方で、サイバー空間とフィジカル空間を融合させたサプライチェーンの拡大は、サイバー攻撃の機会の増大をもたらし、防御すべき範囲も急激に拡大することが懸念される。また、サイバー・フィジカルシステムにおいて流通・加工・創造される情報の品質確保も重要である。

このような状況に対処するためには、サイバー・フィジカルシステムのサプライチェーン全体のリスク管理の実効性の担保と情報品質の確保の仕組みが必要になる。しかし、その実現には様々な障害があり、多様な仕組みを組み合わせて対処することが必要であるが、システム監査はその一翼を担う必要がある。

経済産業省が公表した「GOVERNANCE INNOVATION Ver.2: アジャイル・ガバナンスのデザインと実装に向けて」の中でも、監査に関連して、以下のような記述がある（経済産業省，2021）。これらは、システム監査において今後取り組むべき領域や制度の拡張・応用について、重要な示唆を与えている。

① サイバー空間上のデータ内容の信頼性の第三者による監査（経済産業省，2021，p.19）
② 内部監査におけるリアルタイム・モニタリング（経済産業省，2021，p.59）
③ コンプライアンス・モニタリングにおけるリスクに応じたアシュアランス（保証）の態様の活用（経済産業省，2021，p.99）

まず、データ内容の信頼性の監査については、財務諸表監査と同様に、提供される情報に信頼性を付与するものであり、信頼性付与のレベル、監査の実施主体、監査目標、監査手続等について基準の検討と制定が必要である。

次に、内部監査におけるリアルタイム・モニタリングについては、自動化が必須であり、モニタリングの対象、プロセス、結果の開示方法等の検討が必要である。

さらに、リスクに応じたアシュアランスの態様の活用とは、「自己チェック、ピアレビュー、内部監査、合意された手続、第三者によるレビューや監査等」の態様のことを意味しているが、現行のシステム監査基準においては、これらの態様について言及がないため、改訂時に記載の検討が必要である（経済産業省，2021，p.99）。

6. サイバー・フィジカルシステムと情報品質

6.1. サイバー・フィジカルシステムの構成要素

本稿において検討対象とするサイバー・フィジカルシステムとは、サイバー空間とフィジカル空間を高度に融合させたシステムを意味し、次のような 3 つの階層を有する（経済産業省，2019）。

第 1 層は、企業間のつながりの層であり、自組織におけるリスク管理・対応体制とサプライチェーンリスク管理が必要となる。

第 2 層は、フィジカル空間とサイバー空間のつながりの層であり、次の機能を果たす。

① フィジカル空間の物理事象を読み取り、一定のルールに基づいて、デジタル情報へ変換し、サイバー空間へ送る機能（転写機能）
② サイバー空間から受け取ったデータに基づいて、一定のルールによって、モノを制御したり、データを可視化したりする機能（制御・可視化機能）

第 3 層は、サイバー空間におけるつながりの層であり、次の機能を果たす。
① データを加工・分析する機能
② データを保管する機能
③ データを送受信する機能

6.2. サイバー・フィジカルシステムにおける情報品質特性の構成要素

著者は、2009 年に会計情報の品質特性を階層化して分類する考え方を提示した（石島隆，2009）。この考え方を基礎として、情報品質特性と IT の統制目標との関係を整理したものを表 3 に示した。さらに、前述のサイバーフィジカルセキュリティフレームワークの三層構造モデルと情報品質特性との関係を表 4 に示した。

ここにおいて、「目的適合品質特性」は、サイバー・フィジカルシステムの目的との適合性を意味するが、サービス提供者とサービス利用者の目的適合性に関する認識の相違が生じることも考えられる。そこで、これを補完するためには、サービスレベルアグリーメントのように、サービス提供者とサービス利用者が客観的に認識可能な指標を合意の上で設定することが必要となる。これを「基準準拠品質特性」と呼んでいる。

さらに、この品質特性を満たすためには、情報処理プロセスにおいて機能要件と非機能要件が満たされることが必要であり、これを「プロセス品質特性」と呼ぶことにした。ここで機能要件とは、サービスの目的を実現するために直接必要な機能を表す要件であり、非機能要件とは、セキュリティ要件のようにサービスの目的の実現の前提となる要件である。

表 3 情報品質特性と IT の統制目標

品質特性の区分		IT の統制目標	定　義
目的適合品質特性		有効性	情報がそれを利用するビジネスプロセスの目的に適合した適切なものであること
基準準拠品質特性		準拠性	情報が目的適合性の観点から設定された法令や組織内外の基準等に合致していること
プロセス品質特性	情報の内容に直接関わる品質特性（機能要件）	信頼性（ｲﾝﾃｸﾞﾘﾃｨ）	情報が組織の意思・意図に沿って承認され，漏れなく正確に記録・処理され，継続して利用が可能なこと ・正確性：情報がデータ項目に正確に記録され，提供されていること ・網羅性：情報が漏れなくかつ重複なく記録されていること ・正当性：情報が組織の意思・意図にそった承認手続を経たものであること ・維持継続性：必要な情報が最新の状態に正確に更新され，かつ継続使用が可能なこと
	情報システムとしての品質特性（非機能要件）	効率性	情報の提供が経営資源の最適な（最も生産的かつ経済的な）利用により行われること
		可用性	情報が必要とされるときに利用可能であること
		機密性	情報が正当な権限を有する者以外に利用されないように保護されていること
		原本性	作成者又は作成名義人の意思によって作成されたものであり（真正性）、かつ、作成後に変更、改ざん等が行われていないこと（完全性）
		透明性	説明責任を果たせるように適切な情報を提供すること

（出典）石島隆（2021a）一部修正。

表4　サイバー・フィジカル・セキュリティ・フレームワーク（CPSF）の三層構造モデルと情報品質特性

項　目		第１層	第２層	第３層
CPSF の三層の意味(注)		企業間のつながり	フィジカル空間とサイバー空間のつながり	サイバー空間におけるつながり
CPSF の各層における信頼性確保の内容(注)		適切なマネジメントを基盤に各主体の信頼性を確保	フィジカル・サイバー間を正確に“転写”する機能の信頼性を確保	自由に流通し、加工・創造されるサービスを創造するためのデータの信頼性を確保
CPSF の各層の機能(注)		リスク管理・対応体制の構築と運用	情報の正確な転写及び正確な転写の証明	データの加工・分析、保管及び送受信
目的適合品質特性		サービスの目的との適合性		
基準準拠品質特性		設定したサービスレベル（機能面及び非機能面）の達成度		
プロセス品質特性	**機能要件**	サービス品質管理体制の有効性	情報の転写の正確性	データの信頼性
	非機能要件	リスク管理・対応体制の有効性	情報の正確な転写の証明など	データの保護 通信相手の識別など

（出典）石島隆（2021a）に基づく。但し、(注)を付した各項目については経済産業省（2019）に基づいて記載した。目的適合品質特性、基準準拠品質特性およびプロセス品質特性の内容は著者が作成した。

7. おわりに

システム監査基準・システム管理基準の改訂については、様々な論点があるが、組織体の単位を越えたシステム監査への発展の基礎となるような基準の改訂が必要である。

本稿では、検討を行った結果、以下の3点について提案を行った。

① システムのライフサイクルに着目したシステム監査制度と情報資産のライフサイクルに着目した情報セキュリティ監査制度を統合すること。

② システム監査企業についても、情報セキュリティサービス審査登録制度に準じて、サービス品質の評価を実施する企業台帳制度として見直しを行うこと。

③ システム管理基準を廃止し、システム監査実施ガイドラインとして再構成するとともに、具体的な監査実施ガイドラインの作成は、システム監査の実務家団体等の連合組織に委ね、改訂の頻度を増やすこと。

なお、システム監査実施ガイドラインの作成に当たっては、Society5.0 におけるアジャイル・ガバナンスと情報品質特性を考慮すること必要がある。

文　献

飯泉紀子・鷲崎弘宜・誉田直美監修、SQuBOK 策定部会編（2020）『ソフトウェア品質知識体系ガイド第3版』，オーム社

石島隆（2009）『情報品質の研究』第7章 会計情報の品質特性と品質保証, 中央経済社, pp.144-157.

石島隆（2021a）「サイバーフィジカルシステムにおける情報品質とリスク管理に関わる諸制度の検討」，『第 26 回社会情報システム学シンポジウム講演論文集』,社会情報システム学研究会，Session 1-3.

石島隆（2021b）「システム監査基準・システム管理基準の改訂に関する課題」，システム監査学会第 34 回公開シンポジウム発表論文

経済産業省（2018a）「「システム監査基準」及び「システム管理基準」の改訂について」，https://www.meti.go.jp/policy/netsecurity/sys-kansa/h30kaitei.html (2021 年 7 月 31 日)

経済産業省（2018b）「システム監査制度について」，https://www.meti.go.jp/policy/netsecurity/sys-kansa/ (2021 年 8 月 1 日)

経済産業省（2018c）「情報セキュリティサービス審査登録制度」，https://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html (2021 年 8 月 1 日)

経済産業省（2019）「サイバー・フィジカル・セキュリティ対策フレームワーク」，https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html (2021 年 7 月 31 日)

経済産業省（2021）「「GOVERNANCE INNOVATION Ver.2: アジャイル・ガバナンスのデザインと実装に向けて」，https://www.meti.go.jp/press/2021/07/20210730005/20210730005.html (2021 年 8 月 1 日)