情報品質の確保とシステム監査の役割

Role of system audits to ensure information quality

石島　隆
ISHIJIMA Takashi
法政大学　Hosei University

要旨： 現在、経済産業省が公表している「システム監査基準」及び「システム 管理基準」の改訂作業が行われている。本稿では、システム監査の定義と目的について述べた上で、システム監査を取り巻く環境変化について、①サイバー・フィジカルシステムと情報品質、②アジャイル・ガバナンスとトラストという２つの側面から検討する。その結果、今回の改訂のさらに先にある課題に対応するためのシステム監査の役割について検討し、さらに、情報の信頼性保証のためのシステム監査の可能性を検討する。今後、情報品質特性を切り口として、システム監査と情報セキュリティ監査に分かれている IT 関連の監査制度を統合し、Society5.0 の世界におけるアジャイル・ガバナンスの推進に資する監査制度を確立することが望まれるが、相当の期間を要すると考えられるため、民間団体によるシステム監査の実践に資するガイドラインを整備することにより、環境変化への対応をアジャイルに行っていくことを提案する。

キーワード: システム監査、アジャイル・ガバナンス、トラスト、情報品質

Abstract: Currently, the "System Audit Standards" and "System Management Standards" published by the Ministry of Economy, Trade and Industry (METI) are undergoing revision work. This paper describes the definition and purpose of systems auditing, and then examines the changing environment surrounding systems auditing from two aspects: (1) cyber-physical systems and information quality, and (2) agile governance and trust. As a result, the author will discuss the role of system auditing to address issues further beyond the current revision, and further examine the potential of system auditing for assuring the trustworthiness of information. In the future, it is desirable to establish an audit system that contributes to the promotion of agile governance in the Society 5.0 world by integrating IT-related audit systems that are divided into system audit and information security audit, using information quality characteristics as a starting point, but since this is expected to take a considerable period of time, private organizations However, since it is expected to take a considerable period of time, the author propose that private organizations respond to environmental changes in an agile manner by developing guidelines that contribute to the practice of systems auditing by private organizations.

Keywords: systems audit, agile governance, trust, 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，2018）。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、2022 年 9 月から「システム監査に関する検討会」が設置され、改訂案の検討が行われている。

本稿においては、システム監査の定義と目的について述べた上で、システム監査を取り巻く環境変化について、①サイバー・フィジカルシステムと情報品質、②アジャイル・ガバナンスとトラストという２つの側面から検討する。その結果を踏まえて、今回の改訂のさらに先にあ

る課題に対応するためのシステム監査の役割について検討し、さらに、情報の信頼性保証を行うためのシステム監査の可能性を検討する。

2. システム監査の定義と目的

現行のシステム監査基準において、「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。」と定義されている。すなわち、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たプロセスの有効性に関する監査である（経済産業省，2018）。

一方、情報セキュリティ監査基準において、「情報セキュリティ監査の目的は、情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備、運用状況を、情報セキュリティ監査人が独立かつ専門的な立場から検証又は評価して、もって保証を与えあるいは助言を行うことにある。」と定義されている。すなわち、情報セキュリティ監査は、情報資産のライフサイクルに着目して構築された情報セキュリティに係るリスクマネジメントのプロセスの有効性に関する監査である（経済産業省，2003）。

このように、システム監査、情報セキュリティ監査ともに、プロセスの有効性を評価するものであり、情報システムが取り扱うデータや情報も対象となるため、データや情報の信頼性を監査テーマとして、信頼性確保のためのプロセスの有効性を監査することは可能であるが、その組織体が処理して提供するデータや情報そのものの信頼性を評価し、保証するためのシステム監査を想定した制度ではない。したがって、公認会計士等が実施する財務諸表監査のように開示される情報の適正性について保証を行うための仕組みは整備されておらず、今後、ステークホルダーのニーズを見極めた上で実現方法の検討が必要である。

3. サイバー・フィジカルシステムと情報品質

3.1. 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、情報品質特性を目的適合品質特性、基準準拠品質特性、情報の内容に直接関わる品質特性（機能要件）、及び情報システムとしての品質特性（非機能要件）に区分し、IT の統制目標との関係を表 1 に示した。

3.2. 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

次に、こ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 2 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、情報の内容に直接関わる品質特性と情報システムとしての品質特性を満たすことが必要である。前者は、システム設計における機能要件に対応し、後者は、非機能要件に対応する。

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。

これらの品質特性を IT の統制目標に対応させると、目的適合品質特性は有効性に、基準準拠品質特性は準拠性に、情報の内容に直接関わる品質特性（機能要件）は信頼性に、情報システムとしての品質特性（非機能要件）は効率性、可用性、機密性、原本性、透明性に対応する。品質特性の区分を IT の統制目標に対応させ、定義を含めて表 2 に示した。

4. アジャイル・ガバナンスとトラスト

経済産業省が「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」において提唱したアジャイル・ガバナンス・モデルは、「政府、企業、個人・コミュニティといった様々なステークホルダーが、自らのおかれた社会的状況を継続的に分析し、目指すゴールを設定した上で、それを実現するためのシステムや法規制、市場、インフラといった様々なガバナンスシステムをデザインし、その結果を対話に基づき継続的に改善していくモデル」である（経済産業省, 2021, v）。

アジャイル・ガバナンスは、ステークホルダー間のトラストの確立が前提であり、ガバナンスシステムの運用の結果を評価し、それを迅速にアップデートにつなげるため、ガバナンスの結果を当初設定したゴールに照らし合わせ、マルチステークホルダーでその評価を行っていくことが不可欠であり、評価の仕組みを作り上げることが必要である。そのためには、(1)評価手法の決定、(2)評価基準の決定、(3)ガバナンスの問題点の迅速なアップデートのプロセスの整備が必要となる（経済産業省, 2022, p.31）。

このうち、評価手法の決定については、マルチステークホルダーで理解・議論することを通じて、協創・決定されるべきであるとしており、以下の論点を提示している（経済産業省, 2022, p.31）。

① トラストの空白域がどこなのか。
　例：情報の信頼性、プロセスの信頼性 等
② どの程度の強さのトラストが必要とされるのか。
　例：自己言明、相互確認、第三者による評価 等
③ そのトラストを確保するためにどのような手法・アプローチが適切なのか。
　例：自主チェック、ピアレビュー、内部監査、外部監査、第三者による認証、第三者による格付、専門有識者、ユーザからの申告、内部・外部通報 等

また、トラストには様々な側面があるが、表 1 で示した情報品質特性との関連では、情報の内容に直接関わる品質特性としては、信頼性（インテグリティ）を挙げることができ、情報システムとしての品質特性との関連では、機密性及び原本性を挙げることができる。これらの品質特性を満たすためには、技術的対策の採用が必要であることはいうまでもないが、技術的対策の有効性評価を含む管理的対策が必要であり、さらにリスクの程度やステークホルダーのニーズに応じて、トラストの評価を行い、問題点の改善につなげることが必要である。

表1 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
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（2020）一部修正。

表2 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		
情報の内容に直接関わる品質特性(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	データ処理の信頼性
情報システムとしての品質特性(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（2020）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。

5. 今後求められるシステム監査の役割

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。

また、経済産業省（2021）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、今後、これらの態様についてのガイドラインの策定も必要となろう（経済産業省，2021，p.99）。

また、システム監査基準及びシステム管理基準の改訂後に、民間団体による「システム監査実践ガイドライン」の策定が計画されており、以下のようなテーマのガイドラインが候補となる。

監査手法に関するものとしては、リモート監査、組織間連携監査、アジャイル監査、継続的監査・モニタリングなどが挙げられる。

IT ガバナンスに関連するものとしては、IT ガバナンスのアセスメント、AI ガバナンス、データガバナンスなどが挙げられる。

技術領域に関連するものとしては、AI システム、IoT システム、アジャイル開発と DevOps、クラウドサービス、オープンソースソフトウェア利活用などが挙げられる。

6. 情報の信頼性保証のためのシステム監査の検討

情報の信頼性保証のための監査の典型例は、公認会計士等が行う財務諸表監査である。財務諸表監査においては、監査人の行動規範としての監査基準と判断基準となる会計基準が長年にわたって体系的に整備されてきた。

監査対象となる企業の大半は、情報システムを利用して会計処理を行っており、財務諸表監査の一環として、必要に応じて情報処理プロセスの信頼性評価も実施されている。但し、財務諸表監査においては、資産の現物実査、棚卸立合、取引先に対する残高確認、取引先が発行した書類との照合など、監査対象組織外から入手した監査証拠（以下「外部証拠」という。）を用いた監査手続の実施も可能である。

ここに、財務諸表監査における監査証拠とは、「監査人が意見表明の基礎となる個々の結論を導くために利用する情報」をいう（日本公認会計士協会、2018、p.1）。また、監査証拠として利用する情報の要件は、適合性と信頼性からなる。適合性は、監査手続の目的と立証すべき命題（アサーション：財務諸表の適正性確保のための要件）との論理的

な関連性を意味し、目的適合性と言い換えることもできる。また、信頼性は、監査証拠自体の証明力を意味し、その証明力は「情報源及び情報の種類、並びに関連する場合には情報の作成と管理に関する内部統制を含む情報を入手する状況によって影響される」（日本公認会計士協会、2018、p.6）

一方、情報の信頼性保証のためのシステム監査は、情報システムによる処理結果としての情報の信頼性を保証するものであり、公共的な情報システムや共同利用する情報システムが提供する情報を対象とすることが考えられる。

保証対象とする情報の種類にもよるが、財務諸表監査のように外部証拠を用いた監査手続の適用が困難なケースには、並行シミュレーション法と呼ばれる「特定の監査目的を検証する機能を持ったプログラムを、システム監査人側で独自に準備し、それと監査対象プログラムに対して同一のデータを入力して、両者の実行結果を比較すること方法」により、情報処理結果の正確性を確認することも考えられる（日本情報処理開発協会, 1994）。

今後、情報の信頼性保証のためのシステム監査のユースケースと監査の方法について検討していきたい。

7. おわりに

本稿では、システム監査を取り巻く環境変化を検討し、その結果を踏まえて、今回の改訂のさらに先にある課題に対応するためのシステム監査の役割と情報の信頼性保証のためのシステム監査について検討した。

今後、情報品質特性を切り口として、システム監査と情報セキュリティ監査に分かれているIT 関連の監査制度を統合し、Society5.0 の世界におけるアジャイル・ガバナンスの推進に資する監査制度を確立することが望まれるが、相当の期間を要すると考えられるため、民間団体によるシステム監査の実践に資するガイドラインを整備することにより、環境変化への対応をアジャイルに行っていくことを提案する。

文　献

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（2020）「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.

経済産業省（2003）「情報セキュリティ監査基準 Ver.1.0」，https://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex04.pdf (2003 年 9 月 10 日閲覧)

経済産業省（2018）「システム監査基準」，https://www.meti.go.jp/policy/netsecurity/downloadfiles/system_kansa_h30.pdf (2022 年 2 月 9 日閲覧)

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 日閲覧)

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/2021/07/20210730005/20210730005-1.pdf (2021 年 8 月 14 日閲覧)

経済産業省（2022）「アジャイル・ガバナンスの概要と現状 GOVERNANCE INNOVATION Vol.3」，https://www.meti.go.jp/press/2022/08/20220808001/20220808001-a.pdf (2022 年 9 月 25 日閲覧)

日本公認会計士協会（2018）「監査基準委員会報告書 500 監査証拠」

日本情報処理開発協会（1994）『システム監査技術者育成カリキュラム』