第 32 回公開シンポジウム　総括講演

サイバーフィジカルシステムにおける情報品質の確保とシステム監査

Information quality assurance and systems audits in cyber physical systems

石島　隆
Takashi Ishijima

法政大学経営大学院
Hosei business school of Innovation　Management

Society5.0 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が前提となる。それらの空間をつなぐためにはさまざまなレベルの情報システムやネットワークが必要となり、そこで利用基盤となる共通のプラットフォームを介する形態が想定される。

本講演は、シンポジウムの総括講演として、当日の講演や研究発表の内容を踏まえ、Society5.0 に関わるプラットフォームの情報品質の確保とそのシステム監査について、どのような取組みが必要かについて述べられている。

要旨は以下のとおりである。

1．情報品質の確保とシステム監査

情報品質の特性と IT の統制目標との関係を見てみると、品質特性の区分を「目的適合品質特性」「基準準拠品質特性」「プロセス品質特性」に分けた場合、「目的適合品質特性」は IT 統制目標の「有効性」に、「基準準拠品質特性」は「準拠性」に該当する。また「プロセス品質特性」では、情報の内容に直接かかわる部分は「信頼性（インテグリティ）」に、情報システムとしての品質特性は「効率性」「可用性」「機密性」「説明責任」に当てはまると考えられる。また、機能要件と非機能要件で分類すると情報システムとしての品質特性は非機能要件であり、それ以外は機能要件となる。

データのインテグリティと IT 統制の関係では、過去の J-SOX 時代の統制対象はユーザ、プログラム、データのそれぞれであったが、現在のサイバー時代では、ユーザはネットワーク上にあるデータにクラウドサービスを介してアクセスすることで目的を実現することが多くなっており、それらを総合した環境（コンテキスト）を重視した情報インテグリティが重要となる。コンテキストには、技術の状況、データの状況、スキルと知識、組織と文化、事業体の戦略的目標などが含まれる。

情報インテグリティリスクとしては主題リスク、利用リスク、情報設計リスク、情報処理ライフサイクルリスクが考えられるが、Society5.0 においては、情報ポータビリティにおける課題として、コンテキストの変更や、コントロール品質にバラツキがあるシステムを経由した伝達などを考慮する必要がある。

情報品質確保のための監査として、プロセス品質に関する監査は当然欠かせず、従来はこれを重視してきたが、これからは提供される情報やサービスの品質に関する監査も必要である。またプラットフォーム品質確保のためのシステム監査も Society5.0 では重要な観点であり、規模の拡大やグローバル化に応じて組織の枠を超えた品質確保が必要である。こうした品質保証の枠組みや、第三者による検証制度の構築が今後の課題であり、ここにシステム監査が貢献できる可能性がある。

2．サイバーフィジカルシステムとシステム監査

システム監査の目的は、情報システムリスクに対して適切に対応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・検証することにより、最終的に組織体の目標達成に寄与し、利害関係者に対する説明責任を果たすことにある。Society5.0 では、この対象が「組織体」

から「組織体を含む共同体、プラットフォーム」になる。またITガバナンスにおいても、多数の参加者が利用するプラットフォーム全体のガバナンスが課題となる。

サイバー時代の情報処理プロセスは、さまざまな情報がサプライチェーン（＝プラットフォーム）を通じて収集される。情報セキュリティリスクもネットワーク上やクラウド上それぞれのポイントに存在するが、これに対し経済産業省のサイバー・フィジカル・セキュリティフレームワーク（CPSF）では、三層構造のモデルが提示されている。

第1層は企業間のつながりであり、自組織におけるリスク管理・対応体制やサプライチェーンリスク管理が重要となる。第2層はフィジカル空間とサイバー空間のつながりであり、フィジカル・サイバー間の情報の“転写”の信頼性が重要となる。また第3層はサイバー空間におけるつながりであり、データの加工、保管、送受信などの機能が重要で、これらが監査のポイントとなる。

CPSFではサプライチェーンリスク管理として11の対策要件を挙げているが、これらを監査で直接的にみるだけでなく、他制度と関連して効率的に実施して水準を保つことも重要である。クラウドサービス事業者に対する第三者評価もあり、監査法人によるSOC2報告書などがポピュラーである。事業者によってはユーザに開示していたり、金融機関向けの事業者ではFISCの安全対策基準とマッピングした資料を提供しているところもある。その他、米国での第三者評価プログラムとしてのFedRAMPや日本文書マネジメント協会の認証制度といったものもある。

さらにCPSFでは対策要件をNISTのCybersecurity Framework v1.1の機能に対比させて分類した資料も添付されており、どのようなリスクに対してどのような対策要件があるのかも参照できる。これを見ると、第1層ではガバナンスやサプライチェーンといった人や組織に関するものが多く、第2層ではシステムやプロシージャに関するものが増える。第3層はデータの流通であるため、サプライチェーンの要件が多くみられる。これらを詳細に分析し、それぞれ自分たちのプラットフォームのシステムにおける重要点や注力すべきポイントにブレイクダウンしていくことが必要となる。

サイバーフィジカルシステムのシステム監査は、プラットフォームという観点をもって、自組織だけでなくサプライチェーンのリスク管理・対応体制の有効性評価も行うこと、およびそこで提供されるサービスの目的への適合性、サービスの品質とセキュリティ目標の達成度評価を行うことが重要であり、そこに第三者認証制度の活用などを考慮することも考えられる。

システム監査学会でも今後、研究プロジェクトなどを通じて具体的な議論に取り組んでいきたい。

（内藤　裕之　記）
（2019年10月25日開催）