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

Research on Various Systems Related to Information Quality and Risk Management in Cyber Physical Systems

石島　隆
Takashi Ishijima
法政大学　Hosei University

要旨: 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。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情報品質の確保とリスク管理の実効性の担保が必要となるが、その実現にはさまざまな障害がある。そこで、本稿では、サイバーフィジカルシステムの情報品質とリスク管理に関わる諸制度を検討した。この結果、従来から取り組まれてきたマネジメントシステムの確立やその定期的な第三者による検証に加えて、情報連携のためにデータの標準化が必要であり、さらにリアルタイムな監視により実効性を担保する必要性を指摘した。

キーワード: Society 5.0、サイバーフィジカルシステム、情報品質、リスク管理

Abstract: In the world of Society 5.0, user convenience is expected to expand by using a system that highly integrates cyber space (virtual space) and physical space (real space). On the other hand, there is a concern that the expansion of the supply chain that integrates cyber space and physical space will increase the chances of cyber attacks, and the range of defenses will rapidly expand. To cope with such a situation, it is necessary to ensure the information quality of the entire cyber-physical system supply chain and to ensure the effectiveness of risk management, but there are various obstacles to achieving this. Therefore, the author examined various systems related to information quality and risk management of cyber physical systems. As a result, in addition to the establishment of a management system that has been worked on in the past and its regular verification by a third party, it is necessary to ensure the effectiveness by standardizing data for information cooperation and real-time monitoring.

Keywords: Society 5.0, Cyber Physical System, Information Quality, Risk Management

1. はじめに

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。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情報品質の確保とリスク管理の実効性の担保が必要となるが、その実現にはさまざまな障害がある。そこで、本稿では、サイバーフィジカルシステムの情報品質とリスク管理に関わる諸制度の有効性を検討し、今後の制度等のあり方について述べる。

2. サイバーフィジカルシステムと情報品質

2.1. 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。

自組織におけるリスク管理・対応体制においては、「自組織に対する規制、法律、リスク、環境、運用上の要求事項を、管理し、モニタリングするためのポリシー、手順、プロセスが理解されており、経営層にサイバーセキュリティリスクについて伝えている」こと

が要求されている（NIST, 2018, ID.GV）

また、サプライチェーンリスク管理においては、「サイバーセキュリティ上の役割と責任が、内部の担当者と外部パートナーとで調整・連携されている」ことが要求されている（NIST, 2018, ID.GV-2）

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、以下の機能を果たす。

・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）
・サイバー空間から受け取ったデータに基づいて、一定のルールに基づいて、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。

・データを加工・分析する機能
・データを保管する機能
・データを送受信する機能

2.2. 情報品質特性の構成要素

著者は、石島（2009）において、会計情報の品質特性を次のように階層化する考え方を提示した。会計情報は、組織の活動状況を主として貨幣的評価に基づいて表現するものであるが、何をいつ、どのように表現するかについては、一定の仮定とルールを設定して行われる。このルールのことを「会計基準」と呼ぶ。会計基準に基づいて会計情報を作成することを「会計処理」と呼び、この会計情報を組織の内外に伝達するのが「会計報告」である。

このような会計基準を設定するためには、会計基準の設定主体が必要になる。会計基準設定主体は、会計情報の利用者の目的に合致した会計情報を提供するために、会計事象の変化の状況を反映して適切な会計基準を設定する必要があるが、実際に会計処理を行う組織における会計処理及び会計報告の実行可能性や監査による情報の保証可能性を考慮した会計基準を設定することが求められるため、その設定には、関係者間の調整が不可欠である。

したがって、会計情報の品質特性を検討するに当たっては、品質特性の持つ意味を会計基準の設定過程と会計処理及び会計報告の過程に即して捉える必要がある。

(1) 基準設定品質特性
会計事象をどのように会計処理し、会計報告を行うべきかを定める会計基準を設定するための会計情報の品質特性

(2) 準拠性品質特性
処理結果としての会計情報が会計基準に適合しているかどうか（準拠性）を示す会計情報の品質特性

(3) プロセス品質特性
会計処理と会計報告を行うプロセスにおいて要求される会計情報の品質特性

プロセス品質特性は、情報の内容に直接関わる品質特性（情報の信頼性：インテグリティ）と情報システム固有の品質特性からなる。

上記の分類によれば、会計情報の品質特性は、提供される会計情報の有用性に関する品質特性と、その会計情報を作成するプロセスの品質特性とからなる。最終的に提供され利用される会計情報の品質を確保するためには、会計処理及び会計報告に関わるシステムのプロセス品質特性の確保がなくてはならない。

この会計情報の品質特性における階層化の考え方を用いて、情報システム全般に適用可能な情報品質特性の階層化を行い、表１に対応表として示した。

会計基準の設定プロセスにおいては、会計情報の利用目的に適合するように利害関係者間の調整が行われるため、「基準設定品質特性」を「目的適合品質特性」と読み替えた。また、会計基準への準拠性は、目的に適合するように設定された基準に合致していることを意味するため、「準拠性品質特性」を「基準準拠品質特性」と読み替えた。さらに、プロセス品質特性のうち、「情報の内容に直接関わる品質特性」は、情報システムの設計においては、機能要件に該当するものであるため、これを「プロセス機能要件」と読み替え、「情報システム固有の品質特性」については、これを「プロセス非機能要件」と読み替えた。

これらの情報システム全般に適用可能な情報品質特性について、IT の統制目標との関係及び情報品質特性の定義を表２に示した。

次に、サイバー時代の情報処理プロセスとリスクの発生する箇所を図１に模式的に示した。まず、サイバー時代の情報処理プロセスにおいて、SaaS（Software as a Service）の利用を前提とすると、情報システムのユーザは、クラウドサービス（図１の「クラウドサービス１」）上のアプリケーションプログラムにアクセスして情報処理を行い、必要な情報を取得する。そのクラウドサービス自身も他のクラウドサービス（図１の「クラウドサービス 2」）にアクセスして情報の交換を行っている。その際には、まずユーザ自身の頭（人工知能や bot を含む）の中に目的やコンテキストがあり、これがクラウドサービスの目的やコンテキストと合致している必要がある。

さらに、そのクラウドサービス自身が連携する他のクラウドサービスとの目的やコンテキストの合致も必要となる。一方では、これらの情報処理システムを構成するユーザ、プログラム、データベース、ネットワークのそれぞれに様々なリスクが存在する。

まず、ユーザの目的やコンテキストとクラウドサービスが提供する機能や情報の内容が合致しないリスク、クラウドサービス間の連携において目的やコンテキストが合致しないことにより、情報処理の目的が達成されないリスクなど、目的やコンテキストに関連するリスクがある。

また、サイバー攻撃者がユーザになりすまして攻撃を仕掛けるリスク、不正なプログラムがインストールされ実行されるリスク、データベースの改ざんや情報漏洩のリスク、ネットワークの障害をもたらす攻撃のリスクなど、サイバー攻撃に伴うリスクがある。

この他、アクセス権限の設定ミス等で正当なユーザがアクセスできないリスク、プログラムのバグに伴うリスク、データベース内のデータの誤謬に伴うリスク、ネットワークの障害に伴うリスクなど、従来からの情報システムの構築と運用に関連するリスクのほか、自然災害に伴うリスクも挙げられる（石島隆, 2017, pp.41-42）。

なお、サイバーフィジカルシステムにおいては、図 1 のユーザは、人間に限られず、機器が自動操作されるケースが想定される。また、クラウドサービスを利用して、人間が遠隔地の機器に操作の指示を出すケースも想定される。

表 1　会計情報の品質特性と情報システム全般に適用可能な情報品質特性の対応表

会計情報の品質特性		情報システム全般に適用可能な情報品質特性	
基準設定品質特性		目的適合品質特性	
準拠性品質特性		基準準拠品質特性	
プロセス品質特性	情報の内容に直接関わる品質特性	プロセス品質特性	プロセス機能要件
	情報システム固有の品質特性		プロセス非機能要件

表 2　情報システム全般に適用可能な情報品質特性の分類

品質特性の区分		IT の統制目標	情報品質特性の定義
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	プロセス機能要件	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
	プロセス非機能要件	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
		説明責任	経営者が説明責任を果たせるように適切な情報を提供すること

次に、これらの検討結果を前提として、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との関係を表 3 に示した。

「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である。これを「基準準拠品質特性」と呼ぶことにした。

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。

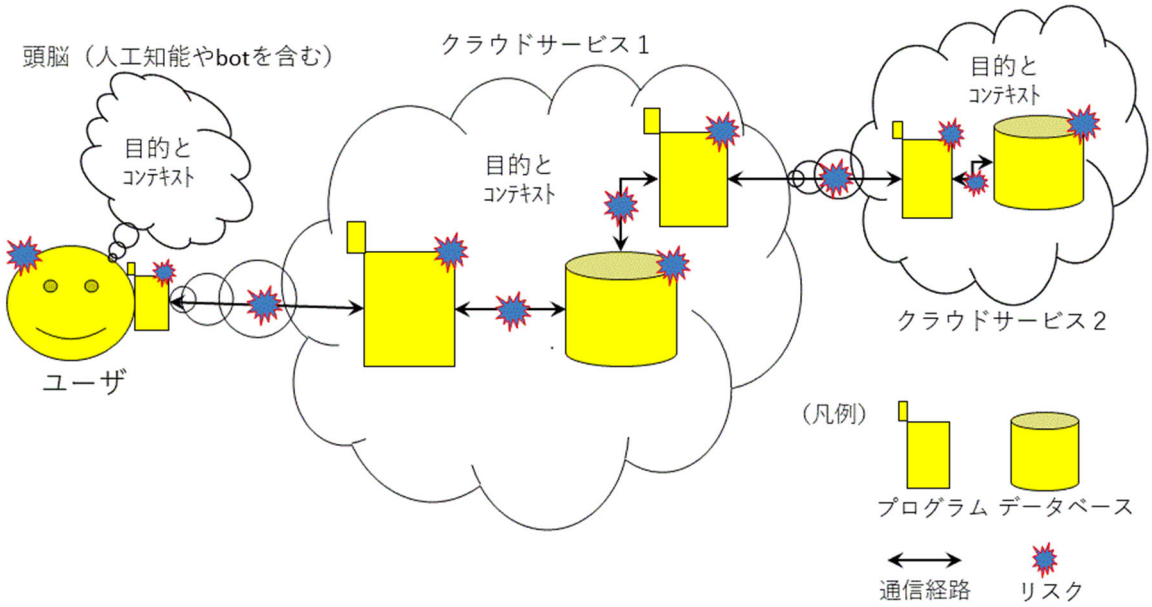

図１　サイバー時代の情報処理プロセス

（出典）石島隆 (2017) p.42

表３　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

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）（注）は、経済産業省 (2019) に基づいて記載。目的適合品質特性、基準準拠品質特性、プロセス品質特性の内容は、著者が作成。

3. 情報品質とリスク管理に関する制度等

3.1. セキュリティに関するガイドライン

サイバーセキュリティに関して、我が国では、「サイバーセキュリティ戦略」が 2015 年に閣議決定されており、2019 年には、米国 National Institute of Standards and Technology (NIST) のフレームワークを参照して、経済産業省が「サイバー・フィジカル・セキュリティ対策フレームワーク」を公表している（経済産業省, 2019）。表 4 に当該フレームワークの対策要件のカテゴリーを示した。

また、第 2 層の IoT (Internet of Things) のセキュリティに関しては 2016 年に「IoT セキュリティガイドライン」が公表されている（IoT 推進コンソーシアム・総務省・経済産業省, 2016）。また、これを参照して、「安全な IoT システムのためのセキュリティに関する一般的枠組」が公表されている（内閣府，2016）。さらに、一般社団法人重要生活機器連携セキュリティ協議会（以下「CCDS」という。）は、

製品分野別（車載分野、スマートホーム分野、金融端末(ATM)分野、決済端末(POS)分野など）のガイドラインを公表している。

表 4　サイバーフィジカルセキュリティフレームワークの対策要件のカテゴリー

機能	カテゴリー	
特定	AM	資産管理
	BE	ビジネス環境
	GV	ガバナンス
	RA	リスク評価
	RM	リスク管理戦略
	SC	サプライチェーンリスク管理
防御	AC	アイデンティティ管理、認証及びアクセス制御
	AT	意識向上及びトレーニング
	DS	データセキュリティ
	IP	情報を保護するためのプロセス及び手順
	MA	保守
	PT	保護技術
検知	AE	異変とイベント
	CM	セキュリティの継続的なモニタリング
	DP	検知プロセス
対応／復旧	RP	対応計画
	CO	伝達
	AN	分析
	MI	低減
	IM	改善

（出典）経済産業省(2019) の対策要件のカテゴリーを NIST (2018)の機能に対応させて著者が分類。

3.2. 第三者による検証制度

クラウドサービスのセキュリティの検証制度としては、米国公認会計士協会が定めた検証制度である SOC2 保証報告書や米国における FedRAMP (Federal Risk and Authorization Management Program) を挙げることができる。

SOC2 保証報告書は、受託業務を対象として、セキュリティ、可用性、処理のインテグリティ、機密保持及びプライバシーに関連する内部統制が米国公認会計士協会が定めた Trust サービス規準（必要に応じて追加規準の設定が可能）を満たしているかどうかを検証した報告書である。世界的な大手クラウドサービス事業者は、大手会計事務所による SOC2 保証報告書を利用者に提供している。

一方、FedRAMP は、米国政府全体のプログラムであり、クラウドの製品やサービスに対するセキュリティ評価、認証、継続的監視に関する標準的なアプローチを提供している。この制度では、NIST SP 800 シリーズを使用しており、クラウドサービスプロバイダーは、認証が連邦情報セキュリティマネジメント法 (FISMA) に準拠していることを保証するために、第三者評価機関（Third-Party Assessment Organization：3PAO)が実施する独立したセキュリティ評価を受ける必要がある (AMAZON, 2019)。

3.3. 製品認証制度

第 2 層に関連する認証制度として、2019 年 10 月に CCDS が IoT 機器としての共通要件について「IoT 機器向けサーティフィケーションプログラム」を開始しており、HD メモリーカメラレコーダー、国内向け ATM、決済端末、住宅用窓シャッター、給湯リモコンの各製品にサーティフィケーションマークが付与されている。

また、第 3 層に関連する認証制度としては、日本文書情報マネジメント協会が「電子帳簿保存法スキャナ保存ソフト法的要件認証」及び「電子帳簿ソフト法的要件認証」を行っている。ソフトウェアの認証に当たっては、そのソフトウェアのマニュアル、取扱説明書などで公開されている機能をベースに、公正な第三者機関でチェックし、必要な機能を全て備えていることを確認したうえで認証審査委員会において審議し、認証が行われている（日本文書情報マネジメント協会, 2020）。

3.4. 脆弱性検査

脆弱性検査とは、ソフトウェアやシステムに対してセキュリティ上の脆弱性がないかどうかを検査するものである。

情報処理推進機構 (2013) は、開発フェーズにおける脆弱性検査では、ソフトウェアのソースコードに作りこんでしまった脆弱性がないかを検査する「ソースコードセキュリティ検査、ソフトウェア等に対して脆弱性を発現させやすいデータやファイルを送り込み、脆弱性の有無を検査する「ファジングによる検査」、サーバやクライアント、組込み機器に対して、既知の脆弱性がないかを点検する「システムセキュリティ検査」、そして、脆弱性を検出するためのリクエストをウェブアプリケーションに送ることで、主として既知の脆弱性を検出する「ウェブアプリケーション検査」を紹介している。

また、運用フェーズにおける脆弱性検査については、「ウェブアプリケーション検査」及び「システムセキュリティ検査」の他に、組織のサーバやネットワークに対して攻撃者が実際に侵入できるかという点に着目

して検査する「ペネトレーションテスト」を紹介している。

3.5. クラウドセキュリティ可視化サービス

クラウドセキュリティ可視化サービスは、リアルタイムにクラウドサービスへのアクセスの監視を行うサービスである。このサービスは、ガートナー社が 2012 年に提唱したコンセプトに基づいて、CASB（Cloud Access Security Broker）と呼ばれている。

その基本的な考え方は「ユーザと複数のクラウドプロバイダーの間に単一のコントロールポイントを設け、ここでクラウド利用の可視化や制御を行うことで、全体として一貫性のあるポリシーを適用できるようにする」ことである（サイバネットシステム, 2020）

3.6. データの標準化

利用者が自らの目的とコンテキストに適合したクラウドサービスを利用するためには、データの共通フォーマットやデータが表す概念についての共通に認識が必要である。

政府 CIO ポータルでは、政府として公開を推奨するデータと、そのデータの作成にあたり準拠すべきルールやフォーマット等を取りまとめた「推奨データセット」を公開している（政府 CIO ポータル, 2020）。

また、IMI 情報共有基盤事業では、「共通語彙基盤」と「文字情報基盤」の 2 つの基盤の整備と普及推進に取り組んでいる（IMI 情報共有基盤事業, 2020）。

4. おわりに

本稿では、サイバーフィジカルシステムの情報品質とリスク管理に関わる制度等を検討した。この結果、従来から取り組まれてきたマネジメントシステムの確立やその定期的な第三者による検証に加えて、情報連携のためにデータの標準化が必要であり、さらにリアルタイムな監視により実効性を担保する必要性を指摘する。

そして、図 2 は、サイバーリスクに対処するための内部統制の構成要素間の関係を示したものであるが、このような全体像を描いた取り組みが望まれる。

今後、ユースケース毎の制度やサービスの組み合わせについて、具体的に研究していきたい。

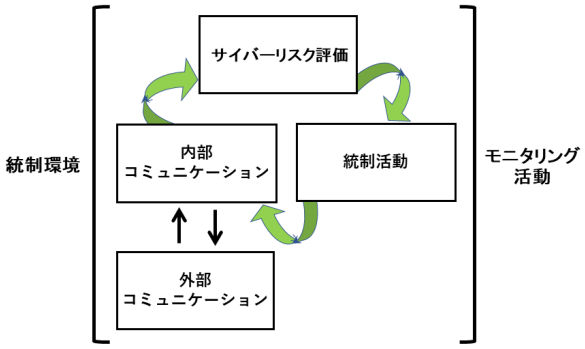

図 2　サイバーリスクに対処するための内部統制の構成要素

（出典）COSO (2015) p.4

文　　献

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2015), *COSO IN THE CYBER AGE.*

National Institute of Standards and Technology (NIST) (2018), Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

AMAZON (2020), “FedRAMP” https://aws.amazon.com/jp/compliance/fedramp/ (2020.1.22 閲覧)

IMI 情報共有基盤事業 (2020), 「IMI とは」, https://imi.go.jp/imi/ (2020 年 1 月 24 日閲覧)

IoT 推進コンソーシアム・総務省・経済産業省(2016), 「IoT セキュリティガイドライン」

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, pp.144-157.

石島　隆 (2017), 「サイバー時代の内部統制と三線防御モデル」, 『商学論究　第 64 巻第 5 号』, 関西学院大学商学研究会.

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」

サイバネットシステム (2020), 「CASB とは」, https://www.cybernet.co.jp/netskope/casb/ (2020 年 1 月 24 日閲覧)

重要生活機器連携セキュリティ協議会 (2019), 「IoT 機器向け　サーティフィケーションプログラムキックオフイベントのご案内」

情報処理推進機構 (2013), 「脆弱性検査と脆弱性対策に関するレポート」

政府 CIO ポータル (2020), 「推奨データセット」, https://cio.go.jp/policy-opendata (2020 年 1 月 24 日閲覧)

内閣府サイバーセキュリティセンター (2015), 「サイバーセキュリティ戦略」

同（2016）「安全な IoT システムのためのセキュリティに関する一般的枠組」

日本文書情報マネジメント協会 (2020), 「JIIMA 認証」, ttps://www.jiima.or.jp/activity/certification/