SYSTEM OF SYSTEMS 運用ガイドライン：立命館版

2025 年 3 月 31 日（公開版）

# OIC に構築されるSystem of Systems の テストベッドを活用した 共同研究開発に関するガイドライン

立命館大学

目次

1　本ガイドラインの目的・概要 4
1.1　本ガイドラインの背景 4
1.2　SoS の特徴 6
1.2.1　SoS とは 6
1.2.2　SoS の性質 6
1.2.3　SoS と複雑システムとの異同 8
1.3　本共同研究開発における SoS 9
1.4　本ガイドラインの目的 9
2　用語定義 11
3　SoS ガバナンス 12
3.1　SoS ガバナンスの必要性 12
3.2　SoS ガバナンスの基本理念および基本方針 12
3.2.1　SoS ガバナンスの基本理念 12
3.2.2　SoS ガバナンスの基本方針 13
3.3　SoS ガバナンスの基本構造 14
3.3.1　アジャイル・ガバナンス 14
3.3.2　協調型ガバナンス 15
3.3.3　二階建て構造 15
3.4　補償を基礎とした SoS ガバナンス 16
4　SoS（テストベッド）におけるステークホルダー間の法的関係と各ステークホルダーの法的義務 18
4.1　ステークホルダー間の法的関係 18
4.2　各ステークホルダーの法的義務 18
5　ステークホルダーの役割と責任 19
5.1　SoS ガバナンス責任者：立命館大学 19
5.1.1　SoS 全体のガバナンス 19
5.1.2　データ管理 24
5.1.3　SoS の普及促進 25
5.2　SoS プラットフォーム開発者 26
5.2.1　学内におけるプラットフォームの開発 26
5.2.2　プラットフォーム開発への協力 29

5.3　SoS 提供者 ..... 30
5.3.1 SoS サービスにかかるガバナンス ..... 30
5.3.2.　SoS サービスにかかる監視 ..... 34
5.4　サービス提供者 ..... 35
5.5　サービス受益者（SoS サービスの提供を受ける主体） ..... 37
5.5.1　遵守事項 ..... 37
5.5.2　情報提供 ..... 38
5.6　潜在的サービス受益者（教職員・学生・地域住民） ..... 38
6　実証実験への対応 ..... 40
6.1　実証実験の実施における総則 ..... 40
6.2　実証実験を行う主体における遵守事項 ..... 40
7　テストベッドを含む SoS 運用のワークフロー ..... 42
7.1　陸上において SoS プラットフォームを利用する場合の運用にかかるワークフロー ..... 42
7.2　空中において SoS プラットフォームを利用する場合（配送ドローン等）の運用にかかるワークフロー ..... 44
7.3　SoS 運用終了後のワークフロー ..... 47
8　インシデントへの対応 ..... 48
8.1　事故・ヒヤリハットが発生した場合 ..... 48
8.1.1　事故が発生した場合 ..... 48
8.1.2　ヒヤリハットの場合 ..... 50
8.2　不具合・障害を検知ないし発見した場合 ..... 51
8.2.1　サービス受益者からの通報 ..... 51
8.2.2　監視業務を所掌する SoS 提供者からの通報 ..... 51
8.2.3　通報後のワークフロー ..... 51
8.3　サービス提供者が異常を検知した場合 ..... 52
8.4　外部の変化を検出した場合 ..... 52
8.5　SoS の構成要素を変更する場合 ..... 53
8.5.1　サービス提供者の求めに応じて SoS の構成要素を変更する場合 ..... 53
8.5.2　サービス受益者等からの情報提供により SoS を変更する場合 ..... 54
8.6　SoS の構成要素が故意または過失により毀損された場合 ..... 54
8.7　SoS サービス運営にかかる情報が漏えいした場合 ..... 55
8.7.1　個人情報に該当する収集データの漏えいの場合 ..... 55

8.7.2　その他情報統制について ..... 56
9　有害事象への対応 ..... 57
9.1　用語定義 ..... 57
9.2　SoS 運用時における有害事象への対応 ..... 57
9.3　重篤な有害事象への対応 ..... 58
9.3.1　SoS ガバナンス責任者を除く SoS 事業推進担当部署の対応 ..... 58
9.3.2　SoS ガバナンス責任者の対応 ..... 58
9.3.3　大学学長の対応 ..... 59
9.4　大臣への報告等 ..... 59
9.5　将来に向けた対応 ..... 60
10　ガイドラインその他関連規定の見直しまたは改正 ..... 61
10.1　通則 ..... 61
10.2　フィードバック・インシデント等発生後の見直し等にかかる特則 ..... 62
10.3　実証実験・テストベッド運用後の見直し等にかかる特則 ..... 62
11　補論：提言など ..... 63
11.1　学内規程等への反映 ..... 63
11.1.1　アジャイル・ガバナンスの理念を踏まえた学内規程の見直し方針 ..... 63
11.1.2　安全性・プライバシー保護等に関する既存ルールとの整合 ..... 64
11.1.3　ガイドライン運用結果のフィードバックと規程整備の継続的検討 ..... 65
11.2　ハードロー（法令等）への反映に向けた提言 ..... 65
11.2.1　リスク管理と補償制度の検討 ..... 65
11.2.2　制度設計・社会実装 ..... 65
11.3　今後の検討事項 ..... 66
12　参考文献 ..... 67

# 1 本ガイドラインの目的・概要

## 1.1 本ガイドラインの背景

我が国は、「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により、経済発展と社会的課題の解決を両立する人間中心の社会」を Society 5.0 と名付け、その実現を目指している。すなわち、CPS（Cyber Physical System）及び IoT（Internet of Things）に代表される SoS（System of Systems：データを介して異なるシステム同士が複雑につながるシステム）によるアーキテクチュアル・イノベーションによって、誰もが快適に質の高い生活を送れるような社会を目指している。アーキテクチュアル・イノベーションとは、ある製品システムが持つ構成要素の連結方法（つながり方）が変わることにより、アーキテクチャに関する知識が変わることである。クリステンセンの「イノベーションのジレンマ」には、インクリメンタル・イノベーションとラジカル・イノベーションが代表的なイノベーションとして記載されているが、それに水平統合（モジュールの統合）の概念を組み入れ、機能特性を変化することなく、相互依存性（関係性）のみ変化するイノベーションをアーキテクチュアル・イノベーションと呼ぶ。しかしながら、いわゆる自動運転システムやドローン運行管理システムを典型的な事例として、SoS の社会実装がなかなか進んでいないのが現実である。我が国の社会システムにおいては、他国に比して危険回避的なリスク選好の社会風土・社会制度が相まって、「何かが生じたとき」のレピュテーションリスク及び法的リスクが相対的に高い。このことが、イノベーションの足かせの一因になってしまっていると考えられる。

そのような風土を変えていくためには、イノベーターのディスインセンティブとなる様々な要因を制度の面から取り除いていくことがより肝要である。すなわち、各事業者にゼロリスクを求めるのではなく、一定のインシデントが発生する可能性をあらかじめ想定したうえで、万が一インシデントが生起した場合でも、事後の改善や迅速復旧を行うことを積極的に評価するようなガバナンスのあり方を考える必要がある。

あらゆるシステムがつながる SoS の時代において、開放的なシステムの振る舞いには常に不確実性が伴う。そのような状況では、従来の「予見可能性に基づく結果回避義務（注意義務）」を前提としたトップダウンによるハードローでの画一的・固定的な問題対処に限界がある。なぜなら、そもそも SoS 固有のインシデント（各システム固有のインシデントではなく各システムが相互作用した結果、SoS を構成することにより発生するインシデント）については、その生起が予見不能であり、事後的にも原因の特定が困難なことが多いため、注意義務の内容を事前に定めておくことが難しいからである。それにもかかわらず、無理やり（遡及的に）注意義務を措定するアプローチを採れば、インシデントに関与している関係者が罰則や責任をおそれて情報の開示に消極的になり、原因究明もままならない。

予見不能な状況を前提とした場合には、従来ハードローで担ってきた役割を、ボトムアップによるソフトローでの経験的・分権的な問題対処に委ねることの有効性が相対的に高まってくる。その有効性を高めるには、現況を正確に把握するための継続的なデータの収集・利活用の仕組みと、問題究明と対策

をマルチステークホルダーにより継続的に図ることのできるようなガバナンスの仕組みとインセンティブ設計が不可欠である。加えて、イノベーションを促進するインセンティブ付与の意味でも、ハードローのような処罰を伴う規定での厳格な管理よりは、ソフトローを中心に自主規制、自主順応、自主監査を促す仕組みにて PDCA サイクルを回す方法がより SoS に適している可能性がある。

SoS の時代にあって、マルチステークホルダーによる合意形成に基づき、ソフトローを上手く活用しながら、「安心・安全とイノベーションの両立」を図る社会の構築が我が国の社会的チャレンジである。すなわち、様々な社会システムにおいて、「環境・リスク分析」「ゴール設定」「システムデザイン」「運用」「評価」「改善」といったサイクルを、マルチステークホルダーで継続的かつ高速に回転させていくガバナンス・モデル――「アジャイル・ガバナンス」――の形成が我々のチャレンジのひとつである（経済産業省『アジャイル・ガバナンスの概要と現状』(2022)）。

アジャイル・ガバナンスのデザイン対象は、技術的なシステムだけではない。それをガバナンス（統治・管理）する組織の仕組みやこれに適用されるルールの創発的デザインのありかたである。創発的デザインとは、生命システムに見られる創発の特徴を有する人工物デザインのことであり、生命システムの創発と同様に、ボトムアップとトップダウンの双方向過程が共存するデザインのことである。このとき、ボトムアップの方は、新しくかつ多様なデザインの候補を生成するプロセスであり、トップダウンの方は、生成したそれぞれのデザインの候補を最適化するプロセスである。創発的デザインでは、この双方向のプロセスをトライ＆エラーを繰り返すことにより、斬新かつ多様なデザインの候補を導出する。また、アジャイル・ガバナンスの運用にあたっては、システムの状況について、リアルタイムデータ等を使って継続的にモニタリングしていくことが求められる。他方、影響を受けるステークホルダーに対して、自らのシステムのゴール、それを達成するためのシステムのデザイン、そこから生じるリスク、運用体制、運用結果、救済措置等について、適切な開示を継続的に行うことが不可欠である。

本ガイドラインは、そのようなアジャイル・ガバナンスの実現に向けたソフトローの端緒をあらわすものである。ポイントは、SoS 固有の各種インシデントに対する原因究明と技術面・ガバナンス面での評価、改善を繰り返しながら継続的なアップデートを図り、まさに「創発するソフトロー」として進化を遂げていく性質にある。

アジャイル・ガバナンスの実現に資するガイドラインの策定といっても、トップダウンのアプローチに依拠したガバナンスシステムを基礎としている日本社会において、一足飛びに、あるいは出島のような特区を抜きにしてその実効性は担保できない。そこで本ガイドラインでは、「立命館大学大阪いばらきキャンパス（OIC）に構築された SoS（テストベッド）の共同研究利用」において生じるリアルおよびバーチャル（シミュレーション上の）インシデントについて、

1） 既存のルール（ハードロー／ソフトロー）の適用・緩和により対応できること
2） 新たにアジャイル・ガバナンスを適用しなければならないこと、すなわち自律的システムが連携して新秩序を同一フィールドで共時的に生成するための二重ループを基礎とした上位のガバナンス体系とソフトローの内容をガイドラインに規定しつつ

3) 2)の場合は更に（ア）と（イ）に分類される。これらについては提言として本ガイドラインの補論に明記する

(ア) 私企業・組織が制度化可能なもの

私契約的にはかなり柔軟に設計できるが、刑法、道路交通法、旅客運送法、事故などが関係する場合は個別的な対処が求められる。

(イ) 国や自治体による新たな制度整備が望まれるもの

SoS のさらに効果的な運用にむけて、国や地方公共団体において新たな制度設計や社会実装が望まれる。

## 1.2 SoS の特徴

### 1.2.1 SoS とは

SoS とは、複数のシステムが連携することにより個々のシステムだけでは達成できない事項を提供するために構成されたシステム群のことをいう。SoS に関する国際規格としては ISO/IEC/IEEE 21841:2019, Systems and software engineering, Taxonomy of systems of systems があり、対応する日本産業標準として JIS X21841 がある。上記規格における SoS および SoS に属する構成システムの定義は、以下のとおりである。

| | |
|---|---|
| システム・オブ・システムズ（SoS） | それを構成する個々の構成システム自体では成し遂げられない特有の能力を提供するために、相互作用するシステムまたはシステム要素の集まり<br>注：システム要素は、SoS 内での構成システムの相互作用を容易にするために必要となる場合がある。 |
| 構成システム | SoS の一部分を形成する独立したシステム<br>注：構成システムは、一つ以上の SoS の一部分となることが可能である。個々の構成システムは、それ自体が有用なシステムである。独自の開発、管理、および利用がなされ、並びにゴールおよび、資源を持っている。しかし、SoS 内では相互に作用し、SoS に特有な能力を提供する。 |

### 1.2.2 SoS の性質

本共同研究開発プロジェクトがテストベッドとして運用する SoS は、各種サービスロボット、ドローン、データ管理プラットフォームその他の複数のシステムから構成される統合システムであり、以下の性質を有している。

1） 独立性（Independence）：SoS は、それぞれが完全な機能を有するシステム（構成システム）の集まりである。各構成システムは、互いに独立して存在し、他の構成システムから分離されても、自己完結的に動作する能力を持つ。また、独自の目標や運用基準を有し、他の構成システムや外部制御から独立して機能しうる。

2） 自律性（Autonomy）：SoS を構成する個々のシステムは、プログラムされた指示や決められたルールに依存することなく、環境や内部状態に応じて自力で動作を調整することができる。外部の介入なしに自己管理と自己制御を行う能力を有するため、予測不可能な環境の変化に柔軟に対応し、目標の達成に向けた活動を自律的に調整する。

3） 協働性（Collaboration）：SoS は、複数の構成システムが連携して、個々の構成システムでは達成できない高度な目標を実現することができる。各構成システムは、それぞれの能力（情報処理能力、感知能力等）やリソース（データベース、通信ネットワーク等）を他の構成システムと共有し、共通の目標の達成に向けて協調的に動作する。

4） 複雑性（Complexity）：SoS は、異なる機能、設計、目標を持つシステムから構成されているため、そのことによって生じる特有の複雑さを持つ。たとえば、各構成システムは、独自の開発サイクルや更新プロセスを持ち、設計、実装、統合、互換性、保守、セキュリティその他の技術的な課題に直面する。新たな要求や技術の進展があれば、SoS の構成や運用方法に変化が起こり、最適化の機会が生じるが、同時に不確実性や困難を来す可能性もある。各構成システムの目標の多様性も、SoS 全体の柔軟性と効率性を高めるが、その一方で、運用上の課題を増加させる要因ともなる。

5） 創発性（Emergence）：SoS は、統合された各構成システムが相互に作用することにより、個々の構成システムの性能を単純に足し合わせたものを超える機能を発揮し、より高次の目標を実現することができる。この「全体は部分の単純総和以上のものである」という性質（創発性）は、SoS の最大の長所の一つである。その反面、設計時には想定していなかった不具合や挙動により、システム全体のパフォーマンス（処理速度、信頼性、効率、正確性、ユーザー体験等）に影響が及ぶ可能性もある。

6） 拡張性・縮小性（Scalability）：SoS は、システム全体の規模や機能を柔軟に拡張し、または縮小することができる。新しい構成システムの追加や機能の拡充は、SoS 全体の機能を強化し、新たな課題に対応することを可能にする。その一方で、構成システムの削除や機能の縮小により、運用の効率化やコストの抑制を図ることもできる。この拡張性と縮小性（スケーラビリティ）は、創発性と並ぶ SoS の大きな長所であり、システム全体の持続可能性と進化を支える不可欠な要素である。

### 1.2.3　SoS と複雑システムとの異同

1)　複雑システムとの違い

SoS は単なる複雑システムではなく、その構成システム自体が複雑システムである場合もある。構成システムは基本的には自律分散型であり、異なるシステムオーナーが存在するため、中央制御方式を採用することは困難である。個々の構成システムによって形成されるネットワーク構造も時間とともに変動する可能性がある。

SoS においては、複雑システム間の関係が形成されているが、その連携具合には濃淡があり、それどころか、濃淡自体も時間とともに変化するため、そもそも全体システムの全容把握が困難である。また、SoS に属する構成システムのライフサイクルは異なり、各システムには独自のインテグレータや運用者が存在する。SoS とは、複数の独立・自立・自律したシステムの連合体の総称であり、タイプの分類が種々提案されてはいるものの、それを構成するシステムおよびシステム間の関係性により千差万別である。

このため、各システムから提供されるデータに関しても、それらの一元的な管理を前提としたマネジメントやガバナンスは現実的ではなく、むしろ、各システムにおけるデータの形式が異なることを想定した運用が必要である。コミュニケーションをとるシステム間に共通のプロトコルが存在するという点を除けば、データの管理と利用は各システムの特性に依存する。このため、多種多様なシステムから必要な情報を適切に収集し、その情報に基づいて全体のマネジメントやガバナンスを行うことが重要である。

2)　複雑システムとの類似点・留意点

複雑システムと同様、SoS も、その構成要素の単純な総和として理解されるものではない。構成システムを個別に分解・分析し、それぞれの機能、構造、振る舞いを把握して、それらを単純に組み合わせて全体像を捉えようとしても、各構成要素の動作のタイミングや構成要素間の関係性を含めた総合的、包括的な理解は極めて困難である。創発という言葉で表現されることもあるこの性質は、システムの本質を考えるうえで欠かせない要素である。とはいえ、システムを分解・分析せずに理解しようとすることもまた困難である。

完璧なシステムを構築することは現実的には不可能であり、どのようなシステムにも必ず何らかの障害が発生する可能性がある。この現実を踏まえ、システムの運用においては障害が発生することを前提とした体制を整える必要がある。そのためには、システムが正常に機能するための手順だけでなく、障害が発生した際の具体的な対応手順も定めるべきである。この対応手順には、障害を自動的に検知し、迅速に対応するためのシステムの自動モニタリング機能の構築が含まれる。また、障害が発生したときにユーザーや関係者からの通報にどのように対応するかも策定しておく必要がある。通報に対する迅速かつ効果的な対応は、システム運用において重要な要素である。さらに、障害対応に関する手順やポリシーを明確にルール化し、関係者全員がそれを理解し守ることができるようにすることも不可欠である。

これにより、予期せぬ事態に対しても組織として一貫した対応が可能になる。

## 1.3　本共同研究開発における SoS

SoS を実社会で構築・運用する際には、その複雑性や不確実性に対処するために、シミュレーション技術を活用するのが有用である。この技術は、SoS の構想から廃棄に至るライフサイクル全体で中核的な役割を果たし、サイバー空間と物理空間を円滑に行き来できるような双方向的な関係性の構築と維持を支える基盤となる。とくに、システムの全体像が初期段階では不明瞭な場合や機能が段階的に追加される際、あるいはサービスの変化によって各構成システムのライフサイクルマネジメントが異なる状況において、SoS の改修やソフトウェアの更新が全体に及ぼす影響を事前に分析するために用いられる。

本共同研究開発は、このシミュレーション技術を活用し、AI を搭載したロボットやドローンを自動制御する SoS のテストベッドを運用することを目的としている。このテストベッドは、実際のキャンパス環境における自動制御ロボット等の動作やシステムの相互作用を評価するために設けられたシステムであり、AI を搭載したロボットやドローン、通信インフラ、ロボット等の運用状況を監視・制御するセンター、キャンパス内に設置されたセンサー、収集されたデータを管理・分析するシステムによって構成されている。これらのシステムを用いて、歩行者の動き、障害物、気象条件といった実環境下でのロボットの機能性、授業間の移動時間帯やインシデント発生時の動作、人や他のロボットとの協調性、通信状態、セキュリティおよびプライバシーの確保、システムの適応性と拡張性に至るまで、多岐にわたるテストが行われる。このテストベッドを通じて、実社会での運用に向けたロボット等の性能や安全性、利便性やエコシステムへの適合性を総合的に評価し、必要に応じて改善を重ねていく。

## 1.4　本ガイドラインの目的

本ガイドラインは、SoS（テストベッド）の共同研究開発プロジェクトに関与するすべてのステークホルダーに向けて、プロジェクトを適切に実施するための包括的なフレームワークを提示することを目的としている。具体的には、ガバナンス体制の確立、ステークホルダー間の法的関係および各ステークホルダーの法的義務、実証実験への対応、SoS 運用のワークフロー、インシデント発生時の迅速な対応手順、有害事象発生時の対応策の提供を行っている。本ガイドラインは、共同研究開発の目標達成を支援し、プロジェクトの参加者が共通の理解と目標に沿った行動をとるための指針である。

SoS の効果的な運用には、構成システム間で生じるギャップ、すなわち、個々の部分システムの機能と全体システムの目的との間に存在する調整不足や不整合を理解し管理することが不可欠である。このギャップは、予測可能なものに留まらず、予測できない形で動的に変化し続けるという特徴を持つため、これに柔軟に対応できるガバナンスの仕組みが求められる。このため、本共同研究開発では、アジャイル・ガバナンスを中核としたガバナンス・モデルを採用し、ダイナミックで不確実な環境下での変化に柔軟かつ迅速に対処し、未知のリスク（unknown-unknowns）にも適切に対応することを可能にして

いる。

意思決定のプロセスや運用の透明性（transparency）を確保することは、本プロジェクトの成功にとって不可欠である。透明性は、ステークホルダー間の情報共有を促進し、意思決定の妥当性を高めるだけでなく、ガバナンス全体の信頼性を向上させる重要な要素である。特に、SoS の運用においては、運用体制、データ管理、リスク対応の手順に関する明確な情報公開が求められる。これにより、ステークホルダー間の共通理解が深まり、連携が強化されるとともに、予期しないリスクに対する迅速かつ効果的な対応が可能となる。

本ガイドラインでは、SoS 全体の把握とその適切な運用を容易なものとすることにより SoS の持続可能な運用とイノベーションを促進するため、SoS を構成する各システムの責任主体、運用主体、データ管理主体を明確にし、それぞれの役割と責任についても示している。システム全体としての調和を図り、SoS を信頼できる（trustworthy）システムにすることが、本ガイドラインの究極の目的である。

# 2 用語定義

| 用　語 | 定　義 |
|---|---|
| SoS ガバナンス責任者 | 対象となる SoS のガバナンスに関する最終責任主体<br>SoS プラットフォーム開発者や SoS 提供者と密接に連携しながら SoS および SoS を用いて提供されるサービスに関するガバナンスを担う責任者<br>ただし、SoS を構成する各システムの自律性、分散性などが生来の性質により全責任を負うかについては状況に強く依存することに留意 |
| SoS プラットフォーム開発者： | 構成システムを組み合せ、統合して SoS を開発する主体<br>プラットフォームの構築の開発がメインとなることもあるが、 SoS におけるデータの流れなど要となる開発を担う |
| SoS 提供者 | SoS プラットフォーム開発者が開発・構築した SoS を施設・設備など使用環境も含めて提供する主体<br>サービス提供者の要求を汲んで、アプリケーションの作成など SoS の提供を行うとともに、利用者からのフィードバックの収集・評価を実施する<br>（SoS および各サービスに応じたアプリケーション開発では 、SoSプラットフォーム 開発者、サービス提供者とコミュニケーションし、合意形成する主体） |
| SoS 運用者 | 上に掲げる SoS ガバナンス責任者、SoS プラットフォーム開発者および SoS 提供者らの総体を指す。なお、本ガイドラインでは SoS 運用者によって構成される組織体を SoS 運用委員会（仮称）と定義する。 |
| サービス提供者 | SoS 提供者が提供する SoS を利用して、実際にビジネスとしてサービスを提供する主体 |
| サービス受益者 | サービス提供者が提供するサービスを受益する者 |
| 潜在的サービス受益者 | SoS との間に直接的な相互作用はないが、SoS の使用環境下に存在し、または存在する可能性のある者 |

# 3 SoS ガバナンス

## 3.1 SoS ガバナンスの必要性

SoS（テストベッド）の運用においては、SoS の特性を反映したガバナンスを構築することが不可欠である。多様なシステムや技術を統合する複雑な構造体を効率的かつ効果的に運用するためには、それに特化したガバナンスが必要となる。このため、本共同研究開発においては、アジャイル、協調型、二階建て構造といった 3 つの要素を基本とするガバナンスを確立している。このガバナンス・モデルは、システム間の一貫性と協調性を確保するとともに、SoS の持続可能な運用とイノベーションを促進する枠組みとして設計されている。一方、本共同研究開発においては、事故やヒヤリハット等のインシデントや有害事象が発生した場合に備え、迅速な救済を図る補償の仕組みを採用した。法的責任を前提としないこの仕組みは、事故原因の事後的な検証に必要な情報の提供にも資するものである。

本ガイドラインでは、ガバナンスを実行する際に依拠する基本理念と基本方針も定めている。基本理念は、プロジェクトのステークホルダーが根本的な価値観や信念を共有し、これに基づいて一貫した行動や意思決定を行うための指針である。本共同研究開発においては、人間中心の価値、多様性と包摂性、持続可能性といった理念を掲げている。プロジェクトを遂行するに際しては、その具体的な戦略やプロセス、準拠すべき規範を定める基本方針も重要となる。本ガイドラインでは、ステークホルダー間の合意形成をはじめとする 8 つの基本方針を提示している。

## 3.2 SoS ガバナンスの基本理念および基本方針

### 3.2.1 SoS ガバナンスの基本理念

1） 人間中心の社会（Dignity）：SoS の開発や運用においては、人間社会をより安全で安心できる快適な場とし、すべての人々に幸福と自己実現を追求できる環境を提供することが根本的な目的として優先されなければならない。SoS は AI を含む先進技術を駆使して構築されるものであり、これらの技術は広範な可能性を持つが、その一方で、技術の誤用が人間の福祉を脅かす恐れもある。技術の利点を活かしつつ、潜在的リスクを認識し、それを最小限に抑える努力が求められる。

2） 多様性を受容できる社会（Diversity & Inclusion）：SoS は、特定の集団の意見や需要だけに応えるのではなく、異なる文化的背景や社会的立場を持つ人々のニーズを幅広く考慮したものでなければならない。多様な意見と視点を取り入れ、多くのユーザーが等しく恩恵を受けられるような包摂的なアプローチを採用することが必要である。この取組みにより、多様な社会の多様なニーズに応え、より公平で包摂的な技術の展開が実現される。

3） 持続可能な社会（Sustainability）：必要となるエネルギーやその他のリソースについても十分に考慮する必要がある。持続可能性の推進には、環境への配慮とリソースの有効利用が重要であり、エ

ネルギーを効率的に使用し、廃棄物を減量化し、資源を再利用する運用プラクティスを採用することで、持続可能な人間社会の形成に寄与する。

### 3.2.2　SoS ガバナンスの基本方針

1) ステークホルダー間の合意形成：ステークホルダー間の明確な合意形成は、目標設定、システムデザイン、運用方針策定の各段階において極めて重要な要素である。共通の目標に基づいた行動を促進し、各ステークホルダーの期待を一致させるため、効率的な合意形成プロセスの構築とその推進が求められる。

2) ステークホルダー間の連携強化：SoS プロジェクトの成功を支えるために、ステークホルダー間での継続的なコミュニケーションと協力を促進する。情報共有のメカニズムを強化し、定期的なミーティングを開催することにより、ステークホルダー間の理解を深め、協力体制を構築する。

3) 透明性とアカウンタビリティの強化：意思決定プロセスの透明性を強化し、ステークホルダーが情報を容易に取得できる体制を構築することは、SoS（テストベッド）に対する信頼と各ステークホルダーの責任感を醸成するうえで不可欠である。速やかな情報公開と対応策の共有を通じ、ステークホルダーの役割と責任の明確化を図ることにより、説明責任と透明性を確保する必要がある。

4) セキュリティの確保：SoS の安全な運用を実現するためには、セキュリティ対策の強化が必要である。システムの設計段階からセキュリティを考慮に入れ、定期的なセキュリティ評価とアップデートを行うことが求められる。また、外部からの脅威（ハッキング、サイバー攻撃など）だけでなく、内部の脅威（内部不正、情報漏えいなど）に対しても効果的な対策を講じることが重要である。

5) リスク管理の強化：SoS 運用における様々なリスクを総合的に管理するため、具体的なリスク管理戦略を策定する。この戦略には、リスクの特定、評価、対応のプロセスが含まれる。リスクの早期発見と迅速な対応を可能にする体制の整備に加え、継続的な監視と改善の取組みを実施する。予期せぬ問題への対応力を向上させ、プロジェクトの安定性を保持する。

6) プライバシーの保護：個人のプライバシーを尊重し、保護することは SoS ガバナンスの重要な柱である。個人情報の取扱いに関しては、厳格な規制と透明性のあるプロセスを確立し、プライバシー侵害が起きないよう適切にデータ管理を行う必要がある。個人情報が適切に取り扱われるという信頼を醸成することは、SoS の持続可能な運用に不可欠である。

7) 教育とリテラシーの向上：すべてのステークホルダーが、SoS（テストベッド）の基礎から応用に

至るまでの知識と理解を深めることも、プロジェクトの持続可能な運用に直結する。ガバナンスの基本理念や基本方針に関する教育に加え、技術的知見の向上を目的としたトレーニングを実施し、ステークホルダーの能力向上を継続的に図っていく必要がある。

8) オープンイノベーションの促進：革新的なアイディアや技術を積極的に採用し、あるいは異なる分野間での協働を通じてオープンイノベーションを推進する。プロジェクト内での知識共有を活性化し、イノベーションの創出を加速する。

## 3.3 SoS ガバナンスの基本構造

### 3.3.1 アジャイル・ガバナンス

本共同研究開発の SoS は、AI を搭載したロボットやドローンが自律的に作業を行い、多様な技術やシステムの相互作用とステークホルダー間の連携によって生じる複雑な環境で運用される。このような状況に適切に対応するため、本共同研究開発では、予測不能な事態に迅速かつ柔軟に対処しうるアジャイル・ガバナンスを採用している。アジャイル・ガバナンスは、外部環境の変化に柔軟に対応し、迅速な意思決定と環境変化への適応を実現するための管理フレームワークであり、SoS の運用中に直面する潜在的な課題やリスクに対して柔軟に対処することが可能となる。

このフレームワークには、以下のプロセスがある。

1) 環境・リスク分析：学内で活用される SoS（テストベッド）は、物理的環境（キャンパスのレイアウト、ロボットが移動する際の障害物や障壁、気象条件など）や学内コミュニティのニーズといった外部環境の変化に強い影響を受ける。これらの要因を定期的に分析し、適切なリスク管理を実施する必要がある。

2) ゴール設定：SoS（テストベッド）は、キャンパス内での自律的なロボットやドローンの運用を通じて、効率的な物流やサービス提供の実現を目的としたものであり、これを実現するために具体的な目標が設定され、必要に応じて更新される。

3) システムデザイン：ガバナンスシステムを設計する際には、技術的要素だけでなく、組織構造やポリシーも考慮に入れる必要がある。この過程では、意思決定の透明性を高め、ステークホルダーが情報に容易にアクセスでき、問題発生時には迅速に対応できる体制を確立することが重要である。

4) 運用：SoS の運用はリアルタイムデータに基づいて行われ、システムの効率性と安全性の確保が優先される。問題が生じた場合は、速やかに原因を特定してステークホルダーに情報を提供し、対応策を講じる。このプロセスは、システムの持続可能性と安定性を保つために不可欠である。

5） 評価と改善：SoS の目標達成状況は定期的に評価され、システムの設計は必要に応じて見直される。外部環境の変化や新たなリスクの発生に対応するため、ガバナンスの目標は適宜再検討され、改善策が適用される。このサイクルを通じて、システムの効果と適応力を持続的に高めていく。

なお、SoS ガバナンスのプロセスは、現場レベルでのフィードバックサイクル（即時の問題解決を目的とする内側のサイクル）と、経営層レベルでのフィードバックサイクル（戦略的改善を目指す外側のサイクル）によって成り立っている。内側のサイクルでは、SoS の影響を評価し、適切な対応策を実行する。一方、外側のサイクルでは、長期的な視点で運用ポリシーを見直し、組織構造を最適化し、テストベッドを含む SoS の利用またはこれに付随するサービス（以下、「SoS サービス」という）の基盤を強化する。

### 3.3.2 協調型ガバナンス

本共同研究開発の SoS（テストベッド）においては、立命館大学と複数の企業が共同で一つの統合されたプラットフォームを形成している。このプラットフォーム内で、立命館大学および各企業は、独立性を維持し、それぞれの専門知識とリソースを活用しつつも、共通の目標達成に向けて協力する。協調型ガバナンスは、単独主体による一元的制御（完全なトップダウン方式）ではなく、各 SoS プラットフォーム開発者の協調的な行動による調整を促進するものである。

協調型ガバナンスは、各組織が独立して判断し行動しながらも、外部環境や内部要件の変化に柔軟に適応するため協力して調整を行うモデルである。これは、統合プラットフォームの目標が自動的に調整される「自己調整モデル」を採用するものではない。共通の目標と戦略の調整は、立命館大学を中心とする SoS プラットフォーム開発者の組織的な合意形成プロセスを通じて行われる。

### 3.3.3 二階建て構造

SoS（テストベッド）のガバナンスは、各構成システムの運用（一階部分）と SoS 全体の運用（二階部分）という二階建て構造で展開する。この役割分担の構造により、SoS の複雑性と動的な特性を考慮した効率的かつ効果的なガバナンスが可能となる。

一階部分では、各構成システムの独立性と自律性に配慮し、その性能、安全性および効率性を最大化することに注力する。各構成システムの管理責任者は、個々のシステムが独立して最適に機能し、SoS 全体の目標に貢献するように運用する責務を負う。システム間の連携やデータ共有を促進するプロトコル（共通言語や約束事）やインターフェースの整備も重要である。

これに対し、二階部分では、SoS 全体の目標に向けた運用に力点が置かれている。このレベルでは協調型ガバナンス（3.3.2.参照）が重要となり、技術的な面では、各構成システム間の協調動作と相互作用を促進することが求められる。ガバナンスの面では、共通の目標設定、リスク管理、戦略的意思決定、パフォーマンス評価が主な活動となる。SoS 全体の最適化を図り、環境変化や内部フィードバックに基

づく適応性を促進する。

## 3.4　補償を基礎としたSoSガバナンス

SoS は不確実性が高く、すべての事故を事前に予測することは不可能である。このため、現場の担当者やシステムの管理者が十分に注意を尽くしても、予期しない事故（有害事象）が発生するリスクが常に存在する。そこで、本共同研究開発では、SoS に関連する事故が発生した場合には、法的責任の有無にかかわらず、保険や基金を通じて迅速に補償を行う仕組みを採用している。

事故発生後は、基本的事実の確認を行ったうえで、詳細な事後検証に先立って補償を実施する。事後検証を先に行い、その結果に基づいて補償を行うという選択肢も考えられないわけではないが、そのような仕組みでは、被害者救済の遅れにつながり、損害の拡大や不信感の増大を招きかねない。長期の事後検証が事故対応への消極的な姿勢とみなされ、社会の信頼を損なう恐れもある。SoS の持続可能な運用のためには、迅速な補償により、被害者の救済を優先する必要がある。

この補償の仕組みは、一般的な民事不法行為責任に基づく賠償とは異なるものである。被害者救済の方法を賠償制度に限定すると、被害者がサービス提供者の故意または過失を立証する必要が生じ、その結果、被害者が救済されないことで SoS への信頼が損なわれ、SoS 全体の発展が阻害される可能性がある。 さらに、責任追及を恐れた関係者が先進的な試みや必要な情報共有を控える可能性もある。もとより、事後検証の結果、事故の発生が誰かの故意または過失によることが判明した場合には、当該者に対して、保険者または補償基金が求償を行うことになるが、それ以外の場合には、生じた損害は保険または基金が最終的に負担する[1]。

[1] ただし、求償を行う際には、AI や自動運転車などの事例において情報格差が障害となり、保険者が必要な情報を得られず求償が困難になる可能性が指摘されている。 そのため、事故調査や説明責任の観点から関係者の情報提供の責務を定めることが重要である。このような情報提供が関係者の求償リスクを高める可能性があるため、非協力的な姿勢が生じることも留意すべき点である。 また、この問題の解決には、立証責任の転換を含む法制度の見直しによって、関係者が説明責任を果たすインセンティブを高める必要があるとの指摘もある。

保険や基金を活用した補償は、SoS（テストベッド）の運用に伴うリスクを複数のステークホルダーで分散し、公平な責任分担を実現するだけでなく、リスクを金銭的に定量化することにより、将来に向けた計算可能性を高め、新たな試みに対する心理的障壁を低下させる効果も期待される。補償を基礎としたガバナンスは、SoS（テストベッド）の運用をより安定化させるための効果的な戦略として機能する。

# 4 SoS（テストベッド）におけるステークホルダー間の法的関係と各ステークホルダーの法的義務

## 4.1 ステークホルダー間の法的関係

SoS（テストベッド）の運用には、立命館大学と複数の企業を含む多くのステークホルダーが関与している。これらのステークホルダーの役割と責任は、本ガイドラインが定めるもののほか、ステークホルダー間の合意によって決定または調整される。

SoS プラットフォーム開発者は、共同研究開発に関する合意に基づき、SoS プラットフォームの運用を目的とした法的関係を形成する。各当事者は、自己の提供したシステムの最適化を目指しつつ、すべての当事者で決定する SoS（テストベッド）の目標を達成するために自律的な業務を行うことが求められる。換言すれば、各当事者の業務は、SoS（テストベッド）の目標によって規定される。各 SoS プラットフォーム開発者は、共同研究開発に関する合意により定められる SoS（テストベッド）の目標を達成するため、必要に応じて、第三者との間で契約を締結する。具体的には、SoS を構成する各システムの保守・点検業務を委託する契約、サービス提供者にテストベッドの試行と評価を委託する契約、SoS サービスのプロセスをデジタル化し、自動化するソフトウェア（アプリケーション）の開発を委託する契約、AI 搭載ロボットの製作供給を委託する契約などがある。各プラットフォーム開発者は、他のプラットフォーム開発者に対し、上記契約を締結する第三者について選任または監督上の注意義務を負う。

なお、本共同研究開発においては、サービス提供者の行為により第三者に損害が生じたときは、当該サービス提供者は、故意または重大な過失がない限り、法的責任を負わない。この場合の被害者救済もまずは補償によって行われ、立命館大学に監督上の注意義務違反があれば、保険者または基金は立命館大学に対して求償する。

## 4.2　各ステークホルダーの法的義務

SoS（テストベッド）に関与するすべてのステークホルダーは、本ガイドラインが定める基本理念および基本方針に従って行動する義務を負う。この要請は、具体的な技術や個別の運用手順を超えて、ガバナンスの枠組み、データ保護、知的財産権の管理、安全性およびセキュリティの確保にまで及ぶ。各ステークホルダーは、本ガイドラインが定める倫理的規範および行動基準を遵守しなければならない。

SoS（テストベッド）が原因で契約外の第三者（学生、教職員、訪問者など）が損害を被ったときは、迅速な補償が優先される（3.4.参照）。事後検証の結果、損害発生の原因が特定され、その原因に法的責任を負う者がいると判断された場合は、その者に対して求償が行われる。求償の前提となる法的責任の有無は、共同研究開発に関する合意の趣旨および目的を踏まえ、民法（不法行為法）その他の法律の規定に基づいて判断される [2]。

[2] 注 1 に掲げる留意事項を参照。

# 5 ステークホルダーの役割と責任

本章は、SoS にかかるステークホルダーたる主体を分類し、その主体各々の役割ならびに所掌事務ないし遵守事項その他役割を例示的に列挙するものとする。

なお、本章で示されない unknown unknowns に該当するインシデントないしそのおそれなど新たな事象が生じた場合も考慮し、本章に掲げる各主体の所掌事務ないし遵守事項は、これらに限定されるものではないことに留意する必要がある。ただし、本章において新たに原則ないし役割、もしくは所掌事務ないし遵守事項を追加、修正もしくは削除を行う際には、アジャイル・ガバナンス方式に基づき、各主体間の協議によって遂行されるものとする。

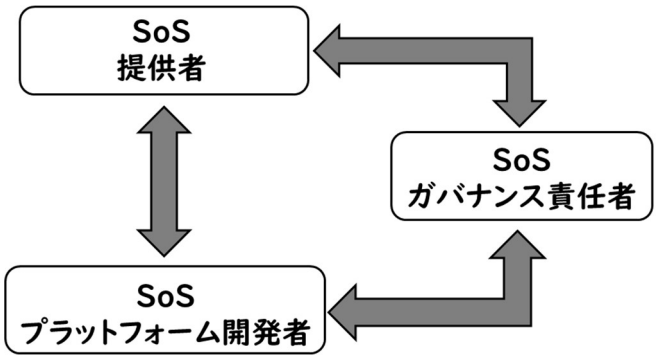
## 5.2 SoS ガバナンス責任者：立命館大学

社会、ステークホルダー、サービス、SoS システムのそれぞれに対する安全性、セキュリティ、プライバシー等に基づく信頼性（trustworthiness）が確保されるような体制を構築し、必要なデータの流れを制御ないし記録できるような関連組織を整備して、これを監督する。SoS のガバナンスにおいては、必要に応じて本ガイドラインおよびその下位規範（チェックリストなど）の改訂を行って、その質の維持・向上に努めるとともに、これらの規範ならびに関係法令に基づいて SoS が適切に運用されていることについて、最終的に責任を負う。

併せて、SoS 運用時に収集されるデータの管理責任者として、データを適正に収集するとともに、収集データに第三者の機密情報、個人情報または知的財産権に留意が必要なもの等が含まれている場合には、法令に従ってこれを適切に取り扱う体制を確立する。さらに、SoS 運用前および運用全体を通じて、データへのアクセスを管理する機能の導入を検討するなど、実用ないし現場レベルで適切な保護措置を実施する。

### 5.2.1 SoS 全体のガバナンス

1） SoS サービスの提供や SoS システムにかかるガバナンスの最終的な責任者として、SoS プラットフォーム開発者および SoS 提供者と連携して SoS サービス、SoS システムにつきアジャイル・ガバナンス方式を尊重しながら、これを遂行する。



2) 各ステークホルダー間の意思疎通が円滑に機能するための体系、すなわち指示系統ならびにエスカレーションルール（緊急事態発生時における報告ルートや責任者を定めたもの。下記参照）を確立する。この体系は、SoS から直接サービスを受けるサービス受益者からの不具合の通報や、潜在的サービス受益者からの情報提供への対応には限定されるものではない。

●このエスカレーションルールには、たとえば以下の事例が想定される。

例）配送ロボットサービス運用時における事故については、おおむね以下のワークフローに従う（後掲 8.1.1「事故が発生した場合[3]」を参照）。

8.1. 事故が発生した場合

①事故が発生した場合、その事故の客体が⑴本学学生、⑵本学教職員、⑶その他の一般人、⑷物によりアクションフローが異なるため、以下それぞれについて記載する。なお、本項目の主体は SoS 提供者または SoS 提供者補助員（実地監視者・統括監視者であるかは問わない）とするが、これには限定されない。

(1) 本学学生

① 配送ロボットまたは SoS 運用にかかる領域内掲示に記載された緊急連絡先から通報があった場合、または実地監視者・統括監視者が事故に気付いた場合、実地監視者が当該事故現場に赴く。このとき、作動している配送ロボット等の SoS 構成要素は一度停止するものとする。

② 当該事故の状況を速やかに統括監視者に報告し、傷害の程度が軽微と判断された場合には、保健担当部署に治療を求めるものとする。ただし、保健担当部署受付時間外に実証実験を含む SoS サービスを運用する場合には応急処置を施すものとし、その応急処置に必要な医療器具をあらかじめ準備しておくこと。

③ 傷害の程度が軽微でない場合は、速やかに 119 番通報を行うこと。

④ 事故の軽重にかかわらず「事故発生時の連絡票」を統括監視者は施設管理担当部署これに準ずる機関に送付すること。

⑤ キャンパス内で生じた本件事故が傷害を受けた者の過失であり、14 日の通院を要するものであれば、統括監視者は関連する学内機関に学生教育研究災害傷害保険の申請を行う。

⑥ 当該 SoS による事故が施設の瑕疵によるものであれば、統括監視者は施設賠償責任保険を施設賠償責任保険担当部署に申請する。その後、施設賠償責任保険担当部署は SoS ガバナンス責任者に通知する。

…

②実地監視員ないし統括監視員が①のワークフローにおいて事故の処理を行ったのちに、事故の軽重にかかわらず、当該事故の調査担当として SoS 提供者が当該事故の検証を SoS 事業推進担当部署と連携して行う。

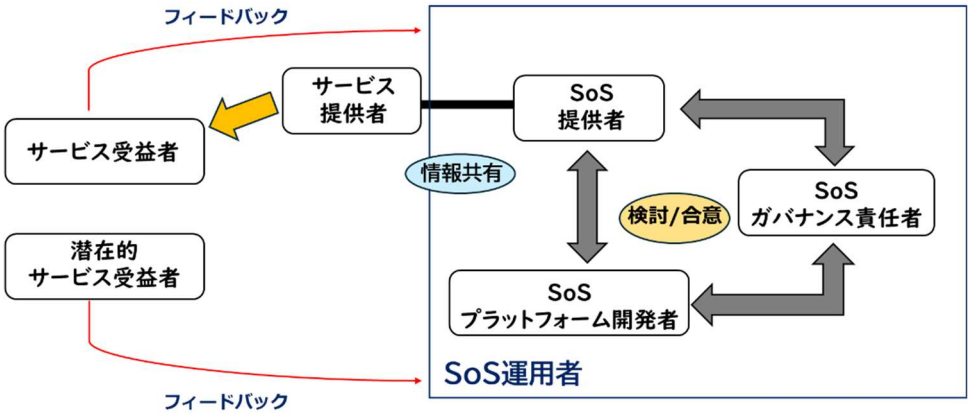
③②により事故原因にかかる情報を収集したのち、SoS 事業推進担当部署で構成される事故検討委員会を開催し、事故原因の特定および予後の改善策を記した事故報告書を作成するものとする。

3) ガバナンスの円滑な運用にかかるデータについては、学内に設置する SoS 事業推進担当部署と検

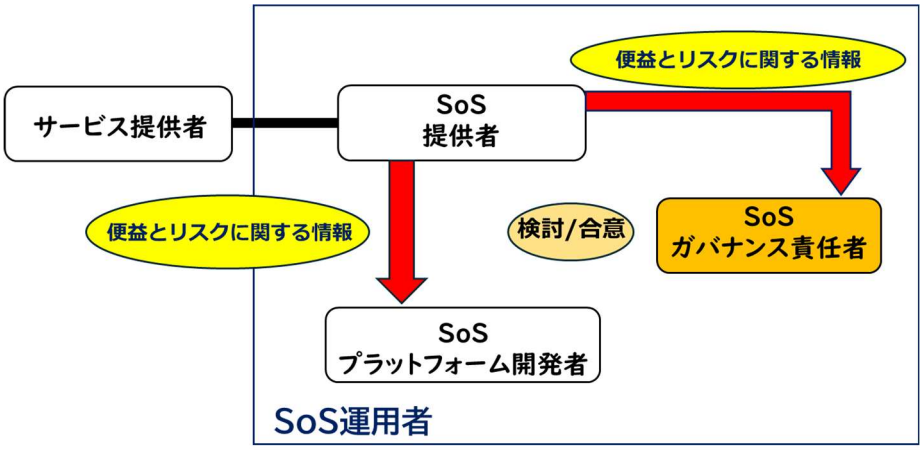
[3] 「事故」や「事故発生」にかかる定義は、SoS 事業推進担当部署の合意により決定されるものとする。ここでは、事故の関係者からの連絡、もしくは SoS プラットフォーム開発者によって事前に設定された条件に基づく判断の双方を含むものとするのが望ましい。

討・合意し、その決定事項を確実に遂行させる。

●この「ガバナンスに円滑な運用にかかるデータ」（たとえば SoS 運用中に発生したインシデントから得られた指揮系統に関する情報）について、ロボット配送の事例においては以下のように示される。




3） SoS サービスの便益とリスクについては、SoS 提供者から直接、またはサービス提供者を通じて、SoS 提供者から説明を受け[4]、他の SoS 事業推進担当部署と検討・合意するとともに、SoS サービス提供について SoS 提供者およびサービス提供者にその決定事項を確実に遂行させる。この場合においては、便益とリスクに関する情報のフィードバックも同時に行うものとする。




4） SoS 提供者の責任で分析される、Goal Structuring Notation(GSN)[5]を通じた SoS 全体の安全論

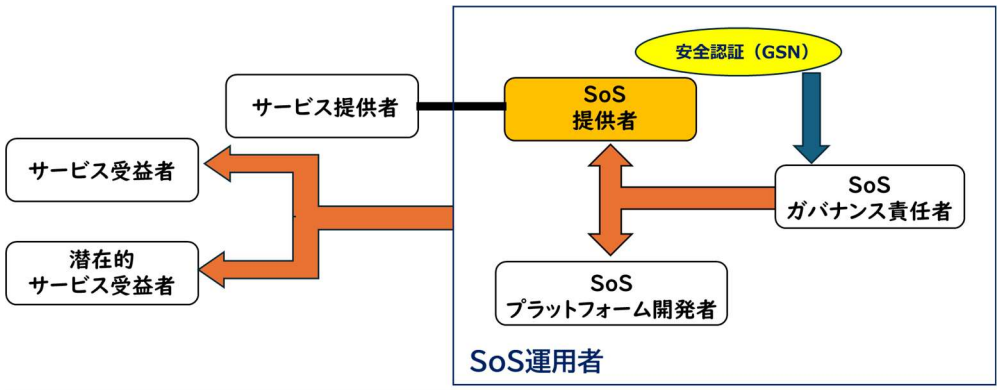
[4] この説明は、SoS サービスの運用を通じて得られた情報のうち、事後の運用に関する積極的または消極的な情報の双方を含み、また、必要に応じて当該サービスの停止や提供シナリオの変更に伴う利点・欠点の提示も行われる。

[5] GSN とは、議論をグラフィカルにあらわす表記法である。GSN は、目標や回答、文脈など議論の構成要素とそれらの

証を SoS ガバナンス責任者の責任において、SoS 事業推進担当部署、サービス提供者、サービス受益者ないし潜在的サービス受益者の順にステークホルダーに共有・公開し、説明責任を遂行する。

5) 提供する SoS サービスに関して、適切に運用されていること。障害・不具合が発生した場合においては、原因究明のための調査委員会の発足、説明責任の遂行など trustworthiness にかかるすべての事項に対する最高責任主体として、以下に掲げる責務を果たす。

① SoS 提供者、SoS プラットフォーム開発者を適時に監視および管理すること。その運用については、以下のようなものが考慮されるが、これには限定されない。




・SoS サービスが適正に運用されているか[6]
・SoS 構成要素であるシステムが適正に監視または運用されているか
・SoS 事業推進担当部署の所掌事務ならびに SoS サービスが関連法令に従って遂行されているか

② SoS 提供者、SoS プラットフォーム開発者から、SoS サービスないしプラットフォーム改善にかかる検討事項として提示された事項に対し、これらと協議のうえで最終決定を確定し指示を出すこと。その検討事項については、以下のようなものが考慮されるが、これには限定されない。

・SoS サービス運用中に SoS 提供者が気づいた配送ロボットの挙動に関する事項
・SoS サービスの運用前あるいは運用中のシミュレーション検証について実証実験を含む運用場所の工事、什器の配置の変更等、シミュレーションを構成する環境が変化した場合のシミュレーションへの反映

---

間の関係を明確に記述するために用いる。GSN で記述した議論は、システムやサービス、組織の安全性やセキュリティといったクリティカルな特性の保証を助ける。GSN では目標をいかにして満たすのかを、階層的に下位の目標に分割し、それ以上分割できない目標には根拠となる回答を示す。その他に、目標の分割をどのような方法で行うかを示す戦略や仮定、正当化の理由、および、その目標が成立つ文脈などを使って議論構造を可視化する。それらにより、主張の曖昧さや抜け漏れを把握しやすくすることで、第三者への説明も同時に円滑なものとすることができる。そのため、安全性の論証に限らず、セキュリティやディペンダビリティ、その他の議論構造の可視化などにも活用することができる。なおその詳細については、The Assurance Case Working Group (ACWG), Goal Structuring Notation Community Standard Version 3, 2021（https://scsc.uk/r141C:1）, pp.11-を参照されたい。

[6] この場合の「適正性」については、たとえば「データの信頼性が確保されている」ことが指標となりうる。

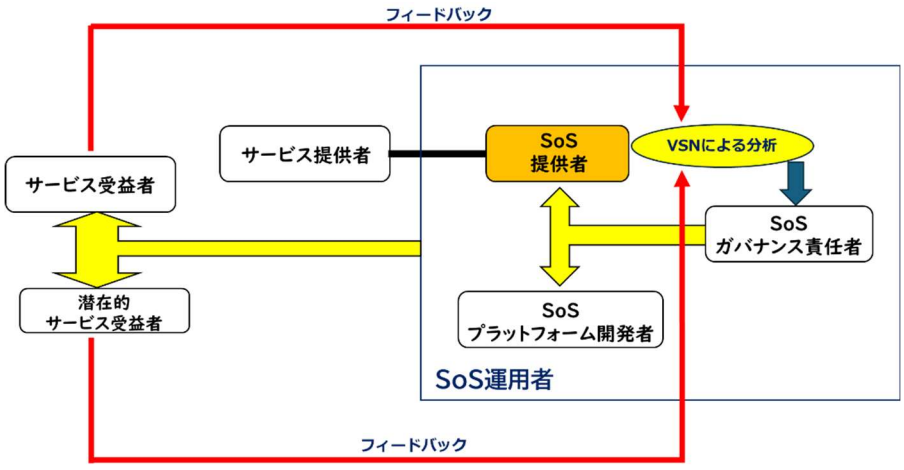
③　サービス提供者、サービス受益者ないし潜在的サービス受益者から提供された SoS サービスの運用にかかる事故・障害情報やその他改善に資する情報について SoS 提供者、SoS プラットフォーム開発者と協議し、最終決定を確定させたうえでこれを周知し、必要な対応措置について SoS 提供者、SoS プラットフォーム開発者に指示を出す。

たとえば、以下のようなケースが想定される。

| |
|---|
| ●SoS サービス運用後のアンケートにて、「商品受け取り待機場所の数メートル手前で配送ロボットが停止してしまった」というフィードバックが寄せられた。<br>→SoS プラットフォーム開発者側で蓄積されている人・ロボットの位置・軌跡に関するデータを参照し、事実確認を行うとともに、当該配送ロボットのメンテナンスを講じる。 配送ロボットのメンテナンス、カメラの動作、配送ルートの変更の検討（SoS 提供者）およびその変更を反映した配送ロボットサービスのシミュレーション（SoS プラットフォーム開発者）を行い、次の SoS サービス提供時までに上記協議にて決定した運用を実装できるようにする。 |

④　障害、不具合が発生した場合の SoS 事業推進担当部署ならびにサービス受益者、潜在的サービス受益者への説明責任を遂行する。その方法については 8 および 9 のワークフローに従い遂行するものとするのが望ましい。

7)　SoS ガバナンス責任者は、SoS 提供者によってサービス受益者ないし潜在的サービス受益者となる学生・教職員・一般市民の SoS に対する価値認識を Value Structuring Notation(VSN)[8]を通じて把握され、SoS の運用にかかるサービスの品質向上ないし unknown なリスクの発見を目的として得られた情報をもとにして提言された新たな対応策や改善策についての合意の可否を決定する。この場合において、提言された内容については、その採否にかかわらず他の SoS 運用者に共有されるものとする。




[8] VSN は、GSN の派生として、ユーザーがサービスをどのような用途で利用しているかという「サービスの意味」を、様々な文脈情報を用いて可視化するために使用されるものである。ここで言う「意味」とは、SoS が提供するサービスに対する意味をユーザーが創造するというものであり、提供者と利用者の相互作用によってサービスに対する意味を双方が共創したものと把握される。

8）7)において SoS ガバナンス責任者が SoS 提供者において提言されるべき当該対応策や改善策に合意した場合には、SoS 運用者らの協議・合意のもとで形成された方法により、サービス提供者、サービス受益者、潜在的サービス受益者に対してフィードバックされるものとし、サービス受益者および潜在的サービス受益者の便益向上に努めるものとする。

9）7)に掲げる価値認識の把握にかかる評価がそれを遂行する SoS 提供者の任意により遂行された場合には、SoS ガバナンス責任者は、その評価を遂行される旨を事前または事後においての同意の可否を決定するものとする。

### 5.2.2　データ管理

1）データにかかるライフサイクルマネジメントにおいては、セキュリティ対策も含めて、データの生成、収集、加工・編集、格納、廃棄に至るすべてのフェーズにおいて適切な管理を、SoS 提供者およびサービス提供者と連携し、SoS プラットフォーム開発者と協働して実行する。

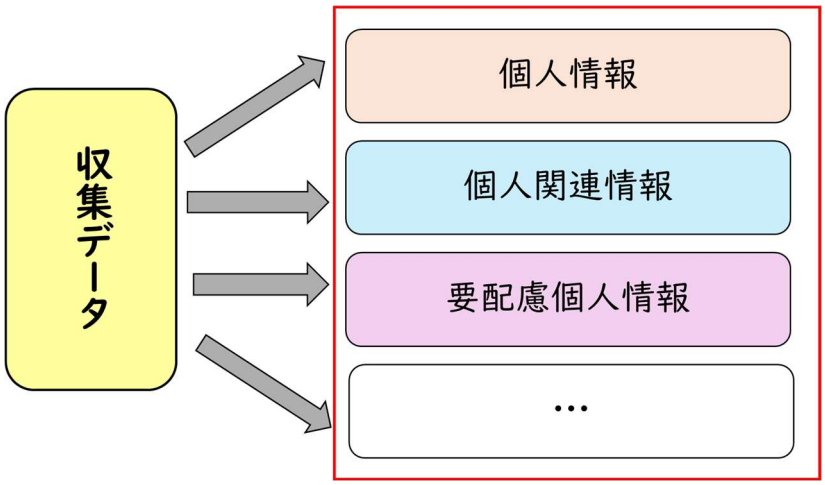
●上記におけるライフサイクルマネジメントの実行例としては、以下が考えられる。

> SoS の構成要素たるカメラによって収集した画像または映像データは、少なくとも 14 日間は SoS 事業推進担当部署において保持し、SoS サービス・SoS テストベッドの運用にかかる事故・ヒヤリハットの分析として活用できるものとする。

2）防犯カメラその他 SoS（テストベッド）運用の用に供されるカメラを通じて個人の肖像等プライバシーにかかわる情報を収集する場合は、これを学術研究の用に供する目的で取り扱う必要があるとき（当該個人情報を取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）に限定されるものとする。

3）収集データにかかるデータマッピングの作成を行う。

＊上記のデータマッピングについては、たとえば以下のようなものが考慮される。




4）SoS を構成するシステムに AI システムが含まれる場合は、学習データを含むデータの品質につい

て関連法規（個人情報保護法、不正競争防止法など）ならびに関連規格（ISO/IEC/IEEE 21839, ISO/IEC 42001 など）の定めに従い取り扱うこと。

5） 個人情報保護法に定める要配慮個人情報を含むもののほか、SoS 運用中に収集したデ　ータ管理の最終責任者として、SoS 事業推進担当部署と共同して当該データの管理を行う。なお、当該データの漏えい時においては、SoS プラットフォーム開発者、SoS 提供者ならびにサービス提供者にもその旨を共有し、個人情報保護法上、個人情報保護委員会への報告が要求される場合には、速やかに個人情報保護委員会への報告を行う（８.７.1 のワークフロー参照）。

6） SoS サービス運用中のデータ収集において、肖像または外見上、明らかに身体障害者福祉法（昭和 24 年法律第 283 号）別表に掲げる身体上の障害がある場合、要配慮個人情報として保護対象のデータとなりうる場合があることを考慮し、データ収集を実行している旨を「研究対象者等が容易に知り得る状態」で学内掲示等を通じて実施する。この「研究対象者等が容易に知り得る状態」とは、文部科学省「人を対象とする生命科学・医学系研究に関する倫理指針 ガイダンス」116 頁 2 に定める事項を準用する。

7） SoS 運用中のデータ収集においては、収集したデータを削除するというオプトアウトを保障しうる体制を構築する。とりわけ肖像を含む画像データを収集する場合は、対象者に対して、データの収集に同意または不同意である旨を示しうるような措置を講じなければならないことに留意しつつ、SoS サービス・SoS テストベッドの運用およびその周知にかかる HP または運用時における学内掲示等で当該措置を講じたうえで、 SoS ガバナンス責任者の責任においてこれを行うものとする。

8） SoS 運用時における収集データにかかる正当なオプトアウトの要求があれば、遅滞なく当該データを削除する。この運用においては、たとえば以下のフローが考慮される。

| |
|---|
| ⑴SoS サービス受益者または潜在的サービス受益者は、学内 HP または掲示に記載された二次元コードまたは URL にアクセスしてオプトアウト申請フォームにアクセスする。<br>⑵申請されたオプトアウトの情報は、SoS ガバナンス責任者の責任で管理し、SoS 事業推進担当部署にて共有する。<br>⑶⑵のフローの遂行とともに、遅滞なく収集したデータの削除を SoS ガバナンス責任者の責任で遂行する。 |

### 5.2.3　SoS の普及促進

SoS ガバナンス責任者およびこれにより指定される者は、本ガイドラインに掲げる SoS テストベッド運用の内容や、そのライフサイクルを通じて創出される価値に関する事項を、一般公衆に向けて発信す

ることに努めるものとする。

この発信方法には、ワークショップ、掲示、動画コンテンツ等一般公衆に提示する方式であれば任意に選択することができるものとし、発信対象となる属性に応じて任意に作成することができる。

## 5.3 SoSプラットフォーム開発者

SoS のプラットフォームを開発する主体であり、SoS の構成要素となる各システムを統合することにより、SoS それ自体の開発を実行する主体でもある。併せて、デジタルプラットフォームにかかわる法令を遵守し、あるいは公益デジタルプラットフォーム運営事業者認定制度における認定基準も参考にしながら、SoS を構築ないし改善する責任主体としての役割を担う。また、その構築においてデータ連携などプラットフォーム開発も兼務することができる。さらに、SoS を構成する各システムから取得するデータに関する責任者間の合意等にかかる記録の管理責任を担う。

また、SoS の改善のために協働して SoS プラットフォームの開発に資する役割を果たす。具体的には、リスクマネジメントとしてのコンフォーマンステスト（特定の基準や規格に適合しているかどうかを検証するテスト）や事故予測に必要なデータの連携、シミュレーションの提供などを行い、SoS にかかる SoS プラットフォームの改善を推進する。

さらに、リスクマネジメントとして事故発生時シミュレーションを行い、以後のサービス改善に努めるものする。加えて、事故発生時におけるその調査の視点から必要な情報あるいはデータを適時に SoS 提供者・SoS ガバナンス責任者と共有する。このプロセスにおいては、SoS プラットフォーム開発者間の相互連携により取り決められた目標ないしルールに従うことを主に留意する。

その所掌は、以下のとおりとする。

### 5.3.1 学内におけるプラットフォームの開発

1） SoS 提供者と連携して、通常運用におけるデータの取得、管理、補完を遂行する。この「通常運用におけるデータ」とは、たとえば配送ロボットが正常に挙動していることの論拠となるタイムログ、位置情報のデータのことを指すが、これには限定されない。なお、異なる定義を用いる場合は、SoS 事業推進担当部署との協議のうえで合意・決定しなければならない。

2） SoS サービスの運用時において異常ないし不具合が発生したとき、その原因を究明するために必要なデータ（ログ、監視カメラの画像データその他の必要なデータ）の証憑となる記録を SoS 事業推進担当部署と共有する。なお、この場合における「異常ないし不具合」の定義については 8 に示すもののほか、SoS 事業推進担当部署との事前の協議のうえで決定することができるものとする。

＊異常ないし不具合発生時のワークフローは、 8 を参照されたい。

3） SoS プラットフォーム開発にあたり新たな機能を追加するときは、SoS ガバナンス責任者または

SoS 事業推進担当部署に必要なデータを提供しなければならない。

4） SoS サービスの運用におけるガバナンスのためのデータにかかるライフサイクルマネジメントにおいては、そのセキュリティ対策も含め、データの生成、収集、加工・編集、格納、廃棄すべての段階において、適切な管理および体制の構築を遂行する。なお、本項における「データ」の定義ないし内容は、必要に応じて SoS 事業推進担当部署との協議のうえで決定することができるものとする。

5） 4)に掲げるセキュリティについては、その必要に応じて、ブロックチェーン技術等データの改ざんを防止するための技術的な機能を実装する（SoS 提供者が行う。ただし、立命館大学以外の SoS プラットフォーム開発者がこれを講じる際には、立命館大学の同意を得るものとし、緊急を要する場合には実装後に同意を得るものとする）。

6） SoS を構成するシステムに生成 AI を含む AI システムが含まれる場合は、特にその学習データを含むデータの品質について関連法規または関連規格に準拠することに留意しつつ、その状況を SoS 事業推進担当部署に必要に応じて提示するものとする。当該データの品質について関連法規または関連規格の要件を満たさないことが判明した場合は、遅滞なく SoS 事業推進担当部署に知らせるものとし、これらとの合意のうえでデータにかかる改善措置を講じるものとする。

7） SoS サービスの運用において、監視事務を所掌する SoS 提供者もしくはサービス提供者、またはサービス受益者もしくは潜在的サービス受益者から事故やヒヤリハット等の情報を得た場合は、当該 SoS プラットフォーム開発者の管轄において当該情報を取得し、原因究明や再発防止策を SoS 事業推進担当部署で検討・実施できる機能を実装するものとする[10]。なお、「事故」ならびに「ヒヤリハット」の定義および想定する具体的事例については、あらかじめ SoS 事業推進担当部署で定めた定義に従うものとする。

8） SoS サービスの運用中に生じた事故やヒヤリハット等の原因究明ならびに再発防止のために、SoS ガバナンス責任者の求めに応じて、実機やシミュレータ、ログデータその他の必要な情報を利用して解析し、その解析結果を、SoS 事業推進担当部署へ遅滞なく報告するものとする。

　SoS ガバナンス責任者の求めに応じなくとも、SoS プラットフォーム開発者の責任で自ら原因究明ならびに再発防止のために任意に解析を行うことができるものとするが、この場合においては、遅くとも解析結果を提供するまでに SoS 事業推進担当部署の合意を得なければならない。

9） SoS の新たな開発やサービスの追加、変更ないし削除において、人・モノ・データのそれぞれに対

[10] 事故やヒヤリハットの検証に要するデータとしては、人やロボットの位置・軌跡のデータが挙げられる。

して、その運用の効率も考慮した総合的かつ包括的な設計を図るとともに、SoS プラットフォーム開発において、外部環境も考慮したリスクアセスメントを実施する。この実施およびサービス追加・変更において、既存サービスの影響分析やリスクアセスメントの結果をサービス提供者から必要に応じて入手するものとする。

＊本項における「外部環境」は、たとえば SoS サービス運用時における以下のようなものを指す。

| |
|---|
| ・天候（とくに配送ロボット等運用時に用いられるカメラに影響を及ぼし得る雨量、風速・風向、温度、湿度、日照等） |
| ・日時（大学であれば開講期間の平日、休日または休暇期間の施設利用人数など） |
| ・人流（大学であれば教室、廊下、階段・エレベーター、トイレなど施設備品の配置） |
| ・道路交通（国道、都道府県道、市町村道および歩道、信号機、横断歩道等ならびに公園等公共施設等の配置） |

10）　9）に掲げるリスクアセスメントの手法ないし対象の具体的内容は、これを行う SoS プラットフォーム開発者の任意により決定することができる。ただし、その事前または事後において、当該リスクアセスメントの手法ないし対象の内容については SoS 事業推進担当部署その他これに準ずる機関の同意を得るものとする。

11）　9）に掲げるリスクアセスメントの結果が得られた場合においては、速やかに、SoS 事業推進担当部署または SoS 運用委員会に報告を行うこと。

12）　SoS サービス運用にかかる安全性、セキュリティ、プライバシーについては、堅牢なセキュリティ機能を SoS に実装し、適切に運用および監視する [7]。なお、この安全性確認には信頼性の確認も含むものとし、当該内容については、SoS プラットフォーム開発者の責任で定めたものを SoS 事業推進担当部署との協議・合意を経て決定されるものとする。

13）　立命館大学は、SoS サービス運用にかかる追加・変更などによる新規システム導入のために、コンフォーマンステストの項目を決定し管理を遂行する最終責任を負う。この場合における「コンフォーマンステスト」の項目内容ならびに管理にかかる手続については、SoS プラットフォーム開発者の責任で定めたものを SoS 事業推進担当部署と協議・合意することにより決定されるものとする。

14）　SoS サービスの運用開始前に、安全性や信頼性を確認するため、事前に策定された体制に基づ

[7] ここでの「堅牢性」とは、情報セキュリティにおける CIA(C: Confidentially[機密性]、I: Integrity[完全性]、A: Availability[可用性])を指すものとする。

いて実機やシミュレータその他の方法による試験方法を決定する。併せて、その試験結果を SoS 事業推進担当部署へ遅滞なく報告する。ただし、SoS 事業推進担当部署との合意において決められた方法による試験の遂行は、立命館大学の責任において行われるものとする。

15） SoS に関する新規システム導入やサービス追加・変更のプロセスは、SoS プラットフォーム開発者から提供されたシミュレータの活用を通じて行うものとし、コストおよび時間効率等を考慮しつつ、当該プロセスを構築するものとする [8]。ただし、考慮すべきコストや時間効率にかかる情報の提供は、SoS 提供者ないしサービス提供者、もしくは SoS ガバナンス責任者のいずれかが行わなければならず、その際には SoS 事業推進担当部署のすべてに当該情報を共有しなければならない。

16） 立命館大学は、SoS プラットフォーム開発者間の合意形成が円滑に行われるための体制を整備することに努めるものとする。

### 5.3.2 プラットフォーム開発への協力

1） SoS サービス運用中において得られた情報を送受信し、これを評価できる体制を構築したうえで、シミュレータを用いてコンフォーマンステストを行う。

2） 生起した事故にかかるデータ（位置情報・速度にかかる走行ログ、目撃者証言等）により事故状況を再現する。ただし、どの程度まで再現するのかについては SoS プラットフォーム開発者間で協働して決定するものとし、その一方が意思を示さない場合は他方の決定に合意したものとみなす。

3） あらかじめ SoS 運用者らで定義していない事故およびヒヤリハット事例をシナリオごとにシミュレーションし、将来に向けたサービス改善に努める。この場合においては、SoS 事業推進担当部署に対しシミュレーションの開始を通知したうえで合意を得るものとする。ただし、そのシミュレーション結果を提供するまでに SoS ガバナンス責任者ならびに SoS 提供者による意見が得られなかった場合は、合意があったものとみなす。

4） 前項のシミュレーションに必要なデータに関し、事故再現に必要な限度で取得データを開示し、立命館大学とともにこれを共有するものとする。また、シミュレーションの際は、以下に掲げる事項を尊重する。

---

[8] たとえば、SoS プラットフォーム開発者の一部または SoS ガバナンス責任者側でシミュレーションのシナリオを設計して、他の SoS プラットフォーム開発者にシミュレーションの実行を依頼し、その結果を受領するという運用が考えられる。

① 自律移動体のシステムに対してシミュレーション検証をすること
② 立命館大学内の諸規則その他ルールに対してシミュレーション検証をすること
③ 想定されうるシチュエーションに応じて都度検証をすること
④ シミュレーションにあたり、具体的なシミュレータを前項の通知書面に記載すること。

## 5.4 SoS 提供者

SoS 提供者は関連する法令を遵守しつつ、SoS ガバナンス責任者、SoS プラットフォーム開発者と連携して、アジャイル・ガバナンス方式により定義した SoS サービスの trustworthy な提供を遂行する。

SoS を構成する各システムの連携については、SoS 全体の運用が最適化されるように努め、変化を検知した場合には、迅速かつ適切に対応する。

併せて、SoS システムおよびサービスを常時モニタリングし、事前に定義した範囲からの逸脱の有無を監視する。また SoS を構成するシステムレベルで発見された異常に関する通知、サービス受益者や潜在的サービス受益者からの異常通知、ヒヤリハット情報、要望などを受け付ける窓口としても機能する。

SoS を構成する各システムにおいては、監視事務を所掌する者にモニタリング事務を移管し、そのモニタリングの結果をそれぞれ集計する。事前に定義した範囲からの逸脱を検出した場合その他 SoS プラットフォーム開発者側で検出された逸脱に関する情報を受領した場合は、警告を出すよう指示するとともに、SoS ガバナンス責任者ないし立命館大学、SoS プラットフォーム開発者に遅滞なく通知する。

### 5.3.1 SoS サービスにかかるガバナンス

1) SoS テストベッド運用が trustworthy なものとなるように SoS サービスの提供に貢献することに努める。

2) SoS に属するシステムの構成に従い、製造、販売、運用、保守、管理などの各活動および責任範囲等を統括する。

3) 個別システムおよび全体システム・サービスに対するアクション、相互作用、責任、契約関係を所掌する。

4) SoS サービスの企画段階において、システム構成要素でコミュニケーションを要するものについては、類型化 [9] などシステム構成の表現方法を明確にし、SoS 事業推進担当部署間と合意形成を行う。

[9] SoS は、共通の目的や管理方式に基づき、指向型、認識型、協調型、仮想型の 4 つの主要な形態に分類され、各構成要素間の連携や目的に応じて選択される（Loughborough University. (2020). Digitalization Transformation Solutions for a New Economy: Systems-of-Systems (SoS). Advanced VR Research Centre）。

5） SoS サービスの企画段階において、SoS 事業推進担当部署に対しデータ伝達のエスカレーションルールを明確化し、SoS システムの構成、挙動、機能を明確にする。

6） SoS サービスを新たに追加、変更ないし削除する場合は、それに伴う SoS の変更（システムの追加やシステム連携の変化への対応を含む）に関して、SoS プラットフォーム開発者およびサービス提供者（以下、本節においては「関係者」という）と既存サービスへの影響について、以下に掲げる事項を尊重し、既存 SoS との関係やシステム群としての影響について分析を遂行する。その際、関係者と連携するとともに、それらの活動を統括する。

① 追加・変更システムの使用環境について共有する情報の明確化
② 既存 SoS と通信等コミュニケーションをする場合はデータ連携
③ システムとしての連携または人を介した連携（運用面を含む）の再検証
④ 変更後の SoS サービスおよび SoS 自体に対して全体として整合がとれていることの確認
⑤ 上記にかかる運用マニュアルなどについての関係者に対する変更指示および周知
⑥ 追加・変更・削除にかかるすべての事項について SoS ガバナンス責任者、SoS プラットフォーム開発者に情報共有するとともに、SoS ガバナンス責任者の承認を得ること

7） 提供される SoS サービスの企画に先行し、SoS サービスを提供する SoS システムの 安全上の仕様および残留リスクが記載された書面を SoS プラットフォーム開発者から入手し、これを他の SoS 事業推進担当部署で管理する。この管理における最終責任者は SoS ガバナンス責任者とすることができる。

8） SoS 提供者の監視事務において、通常運用からの逸脱が検知された場合の対応要件を定義し、必要な機能を実装するために、これを SoS プラットフォーム開発者に遅滞なく通知する。この場合における必要な機能の実装にかかるコストの算定は、SoS 運用者らで行うものとする。

9） 記録するデータの内容に関し、SoS 事業推進担当部署と協議のうえで合意を行う。この場合において、記録するデータは SoS ガバナンス責任者の責任で管理するとともに、SoS プラットフォーム開発者を介して記録することに努めるものとする。

＊記録するデータとしては、以下のようなものが挙げられる。

| |
|---|
| ・SoS サービス評価に関するデータ |
| ・事故もしくはヒヤリハットに関するデータ |

10） SoS サービスを提供するにあたり、施設や場所の状況および運用にかかる体制を考慮した SoS サービスレベルでのリスクアセスメントを SoS プラットフォーム開発者と協力して行い、 安全性の確保を目的とした基本計画を立案し、当該計画に基づき SoS サービスの提供を実施するマネジメントを遂行する。その際、以下の要領で当該マネジメントを遂行する。

① 上述のリスクアセスメントにおいては、SoS システムの残留リスク（SoS システムおよびその運用も含む）が社会的に許容可能な程度にまで低減されたと判断されるまで、これを繰り返す。

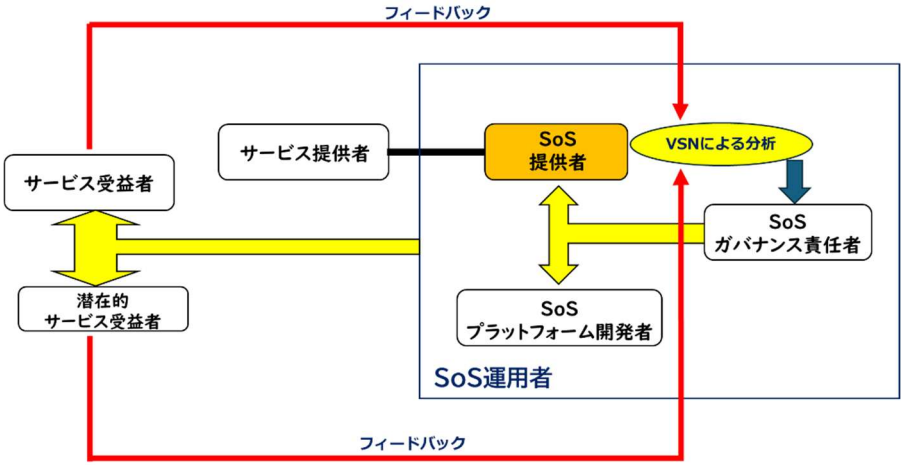
② リスクアセスメントの実施においては、関係者とともに各レベルにおけるリスクアセスメント、リスクマネジメントとの関係を明確にし、包括的かつ総合的に SoS サービスレベルでのリスクマネジメントを実施する。

③ 残留リスクが社会的に許容可能な程度にまで低減されたと判断することが SoS 提供者および関係者のみで困難な場合は、必要に応じて専門的な知見を有する第三者も交えて対応する。

＊本項目におけるリスクアセスメントの評価項目として、以下のようなものが考慮される。

- ●安全計画の立案：配送ロボットサービスにおける事故・ヒヤリハットの内容、発生時の対応事項等
- ●残存リスクの社会的許容度：社会的許容度の基準（サービス受益者、周辺住民のアンケート状況等）
  - ① 当該サービスの利用あるいは利用の様子を通じてどのようなベネフィットが得られたか
  - ② リスクを低減するために行う取組みが適切に遂行されているか
- ●リスクアセスメントの実施体制
- ●リスクアセスメントの運用フロー

11） SoS の運用にかかるサービス受益者ないし潜在的サービス受益者となる学生・教職員・一般市民の SoS に対する価値認識を SoS 提供者による Value Structuring Notation(VSN)を通じて把握し、SoS の運用にかかるサービスの品質向上ないし unknown なリスクの発見に努め、そこで得られた情報をもとに、可能な限りで新たな対応策や改善策を提言する。この場合において、SoS 提供者において提言されるべき当該対応策や改善策は、SoS ガバナンス責任者の同意をもって他の SoS 運用者に共有され、SoS 運用者らの協議・合意のもとで形成された方法により、サービス提供者、サービス受益者、潜在的サービス受益者にフィードバックされるものとし、サービス受益者および潜在的サービス受益者の便益向上に努めるものとする。




12） 11)に掲げる価値認識の把握にかかる評価はそれを遂行する SoS 提供者の任意により行うことができるものとする。この場合において、当該評価のために SoS サービスを通じて得られた個人情報等の法的保護に値する情報の管理にかかる責任は当該 SoS 提供者が負うものとし、併せて評価を遂行する旨を事前または事後において SoS ガバナンス責任者の同意を得るものとする。

13）　SoS サービスの提供時に想定される事故の発生可能性を相当な程度において低減させるため、事故発生時の対応手順を SoS 事業推進担当部署との協議・合意に基づき策定する。当該手順策定にあたっては、SoS サービスを分析し、各システムにおける対応策やシステム構成要素における対応策を体系的に整理・詳細化することに努める。

14）　SoS サービスの提供中または SoS システムの運用中に事故もしくは重大な故障が発生し、または新たな危険源が判明した場合には、あらかじめ定義された方法により緊急対応を行うとともに、当該事故や故障の軽重にかかわらず、これらに関する情報を SoS 事業推進担当部署に遅滞なく通知して、原因究明と再発防止の対策を講じる。

15）　SoS テストベッドを用いたサービスの遂行の際、事故に基づく賠償責任を補償する包括的な保険に加入する。

16）　安全確保上の必要がある場合には、提供する SoS サービスに対して、サービス受益者に対する制約を明確にする（年齢、身長、体重または技能等を含む）。

17）　事故を防ぐために必要かつ十分な安全上の情報を広報すること。広報の対象となる情報については、SoS 事業推進担当部署との協議・合意に基づいて定め、必要に応じて SoS 提供者以外の SoS 事業推進担当部署も広報を行うことができるものとする。

18）　SoS サービスの運用時においては、SoS サービス受益者のみならず、潜在的サービス受益者に対しても学内掲示を通じて遵守事項の啓発を行う。

19）　情報提供を受ける際、「重大でない案件」と思われる場合には、アンケートフォームなどオンライン上での情報提供で完結できるよう、運用する SoS 構成要素に QR コードを貼付するなど、潜在的サービス受益者の負担軽減に努める。

＊上記の「重大でない案件」とは、以下のようなものが考慮される。

| ●配送ロボットがいわゆるチョコ停の状態となった場合 |
|---|

20）　情報提供を受ける際、事故が発生しているなど「重大な案件」と思われる場合には、たとえば SoS 構成要素に緊急連絡先電話番号を付すなどして、監視業務を所掌する SoS 提供者に直接情報を提供できる体制を構築する。この場合、情報提供を受けた SoS 提供者は、遅滞なく SoS ガバナンス責任者および監視業務を所掌する SoS 提供者に報告するものとする。

21)　緊急対応と並行して、遅滞なく事故の原因究明を行い、運用の修正だけでは解決しえない原因については、システム自体の改修を SoS プラットフォーム開発者またはその関連主体に指示する。その際、以下の事項に留意する。

① SoS ガバナンス責任者の責任のもとで、他の SoS 事業推進担当部署とともに、システム・サービスの修正・改善を検討し、合意に基づいて対応措置を講じること。

② 修正に必要なデータを SoS ガバナンス責任者ないし SoS プラットフォーム開発者から取得すること。

③ 必要に応じてサービス提供者に向けて 1)の合意内容に基づく指示を与えること。

④ 修正、復旧、カイゼン（作業の効率や品質を向上させるための継続的な改善活動）が完了したと認められる時点において、SoS システム全体の検証とその妥当性確認を実施する。この場合には、必要に応じて SoS プラットフォーム開発者ないし SoS ガバナンス責任者がその検証および妥当性確認の主体となることもできる。

⑤ 4）の実施結果を SoS ガバナンス責任者に報告するとともに、SoS 事業推進担当部署間で共有する。また、当該実施結果は、SoS ガバナンス責任者が適切に保管するものとする。

⑥ 1)から 5)に掲げる措置を講じる際に要した費用については、SoS プラットフォーム開発者その他システムに関連する主体により得られた情報に基づき、SoS 事業推進担当部署の合意のもとで算定するものとする。

### 5.3.2. SoS サービスにかかる監視

1) SoS サービス運用中の外部環境の変化をモニタリングする。

2) SoS サービスに対するモニタリングについては、SoS 提供者の責任で対象のレベルに応じて階層化し、それぞれに対応するレベルでのモニタリングを実施する主体を定め、モニタリングを実施させるルールを形成するとともに、緊急事態への対応等のエスカレーションルールを付記して手順書を書面ないし電磁的記録で作成するものとする。

ルール化した手続については、SoS 事業推進担当部署の合意を得るものとし、当該手続においてデータを収集する場合には SoS ガバナンス責任者にデータを提供し、これを SoS 事業推進担当部署で共有するものとする。

＊上記の「対象のレベルに応じた階層化」は、たとえば以下のようなものが考慮される。

【配送ロボット】
①本学開講期の平日（授業日である土日祝を含む）：監視者１名、実地監視補助者：３名
②本学開講期の土日祝日（授業日対象日を除く）：監視者１名、実地監視補助者：２名
③全年齢を対象とした実証実験開催時：監視者２名、実地監視補助者：５名

3) SoS サービスにかかるシステムが正常に運用されるよう、あらかじめ運行設計領域および運行計画等を設定し、これを逸脱していないことを確認する。

＊この「運行設計領域および運行計画等」とは、たとえば以下のようなものが考慮される。

・配送ロボットにかかる型式、車両番号および車台番号
・配送ロボットの運行の経路、実施日および時間、運送される人または物
・当該配送ロボットを管理する場所の所在地および連絡先

4） SoS サービス運用が事前の運行計画に従って提供されていることを確認する。

5） 監視システム、および、サービス提供者またはサービス受益者もしくは潜在的サービス受益者からの異常検知等の通知を受けられる体制を構築する。

6） 監視システムおよびサービス提供者またはサービス受益者もしくは潜在的サービス受益者の対応についてリアルタイムまたは適時に通知しうる体制を、SoS 事業推進担当部署との合意のうえで構築する。

＊この「リアルタイムまたは適時に通知しうる体制」とは、たとえば、モニタリング本部を設置し、実地に配置されている監視補助員と常時連絡を取るための通信機器を備えるとともに、本部の監視者が設定された運行領域内に配備されている監視カメラおよび３D マップを閲覧できる状況に置くことなどが考えられる。

7） サービス受益者からのサービスに対する不具合、苦情、リクエストに迅速に対応できる仕組みを構築する。

8） モニタリングにより逸脱を検出した場合において、迅速な障害対応のために SoS ガバナンス責任者へ遅滞なく連絡する。

9） 障害等が発生しない場合であっても、より良いサービスの提供・改善の実現のために、現に運用する SoS サービスとの差異について可能な限りモニタリングする。

10） 外部環境の変化を検出した場合に、その SoS への影響を分析しうるデータの収集を SoS ガバナンス責任者に要請する。この場合において、検出すべき外部環境の変化は、SoS 事業推進担当部署との合意のうえで定義するものとし、その検出体制の構築においては、必要に応じて SoS プラットフォーム開発者と協力して遂行することができるものとする。

## 5.5 サービス提供者

サービス提供者とは、その事業活動において、SoS または SoS サービスを利用する事業者である。SoS 提供者が意図する適正な利用および環境変化等に関する情報を、実地において適時かつ適切に SoS 提供者と共有し、正常な稼働を継続し、必要に応じて提供された SoS を運用する役割を担う。また、SoS の運用ないし活用において第三者に何らかの影響が及ぶことが考えられる場合は、当該者に対する SoS による意図しない不利益の回避や便益最大化の実現に努める役割を担う。本ガイドラインの策定時においてすでに SoS サービスを利用している事業者のほか、配送ロボットや警備ロボットの運用など、今後 SoS を活用する可能性のある事業者を広く含むものとする。

サービス提供者の所掌事務は、以下のとおりである。

1) 当該 SoS の利用について「7．テストベッドを含む SoS 運用のワークフロー」に基づき、SoS サービスにかかる計画書面を SoS 提供者に提出する。この計画に基づき SoS 事業推進担当部署による利用許可を得たうえで、SoS を利用したサービスを開始することができるものとする。

2) 1)の場合において、サービス提供者が虚偽または重大な瑕疵のある申告を行ったとき、その限度において生じた損害についてはサービス提供者がその責任を負うものとする。

3) SoS サービスの運用時において、SoS 提供者等による指示に従いつつ、サービス受益者に対して実地で SoS サービスを提供する。

4) 監視業務を所掌する SoS 提供者の体制ならびにインシデント発生時への対応（後述「8．インシデントへの対応」参照。以下同じ。）にかかる連絡系統を把握する。

5) 事故発生時等の対応およびアクションフローについて把握する。併せて、事故発生時においては、SoS 提供者等 SoS 事業推進担当部署の対応を待つことなく、インシデントへの応急的な対応を講じることができるものとする。この場合において、SoS 提供者に遅滞なく当該インシデントの状況を報告すること。

6) SoS サービスの運営改善に資する情報が、SoS サービスの提供を通じて得られたフィードバックを通じて得られた場合は、遅滞なく SoS 提供者に報告すること。ただし、その情報がサービス提供者における営業秘密（不競法 2 条 6 項）もしくは限定提供データ（同条 7 項）に該当する場合は、営業秘密もしくは限定提供データに該当する旨を SoS 提供者および SoS ガバナンス責任者に書面で告知することにより、必要な限度で情報の開示を制限することができる（SoS サービスの運営改善に資する情報が人の生命・身体ないし財産の保護に寄与する場合を除く）。

7) サービス提供者の提供を通じて得られたデータ（ 6）に掲げるものを含む）が SoS 運用者その他関係するステークホルダー以外の第三者に漏洩することのないようにセキュリティを確保する。

8) SoS 構成要素における不具合・故障に起因する事故発生時において、当該事故に関連する情報を有する場合は、前項の規定にかかわらず、遅滞なく SoS 提供者に報告する。

## 5.6　サービス受益者（SoS サービスの提供を受ける主体）

サービス受益者とは、SoS 運用時に提供されるサービスに対して直接指示を出すことにより、サービスを受益する者であり、SoS を業務としては直接使わないが、その便益、損失を被る可能性がある主体を指す。たとえば、学内に附設される施設からの配送サービス等を利用する、教職員・学生・地域住民といった利用主体を指す。サービス提供者から示された遵守事項に従いつつ、提供されたサービスに対するフィードバックを SoS ガバナンス責任者、SoS プラットフォーム開発者、SoS 提供者およびサービス提供者らに以後の SoS サービスの改善を促す主体でもある。SoS ガバナンス責任者から示された VSN に対するフィードバックも行い、SoS サービスの向上にも貢献する。

### 5.6.1　　遵守事項

1)　サービス受益時にはサービス提供者からの指示を遵守すること。

2)　サービス受益時でなくても、ワークショップ・説明会等において SoS ガバナンス責任者、SoS プラットフォーム開発者、SoS 提供者、監視業務を所掌する SoS 提供者から示された、サービス利用時における遵守事項を遵守すること。

3)　その他、サービス提供者または SoS 運用委員会（仮称）の掲示による遵守事項を遵守すること。

4)　前項の「遵守事項」とは、おおむね以下の事項を指す。

①　ステークホルダーの役割と責任を明確にした SoS の運用にかかわるポリシーと各ステークホルダーとの関係を理解すること。

②　信頼性（trustworthiness）を基礎とする SoS の特性と各ステークホルダーとの関係を理解すること。

③　SoS に適用される法令に関する情報収集と各ステークホルダーとの関係を理解すること。

④　SoS から生じる可能性のある潜在的な悪影響の収集と各ステークホルダーとの関係を理解すること。

⑤　SoS 技術が、自己の享受するサービスその他の様々な業務で活用されていることを理解すること。

＊上述の「遵守事項」について、たとえば配送ロボットの運行では、以下のようなものが考慮される。

| |
|---|
| 1）SoS ガバナンス責任者、SoS プラットフォーム開発者、SoS 提供者、サービス提供者、サービス受益者および潜在的サービス受益者の定義、およびその関係性（所掌事務の具体的内容は、この限りでない）を理解すること。<br>2)　1）で掲げた主体の所掌事務のうち、SoS 固有の特性が関連すると認められるものを理解すること。<br>3) 提供される SoS サービス（テストベッドを含む）に関連する法令、およびこれとサービス受益者が関連しうる事 |

例ならびに適用法令に基づき禁止される事項を理解すること。
4) 提供される SoS サービス（テストベッドを含む）の潜在的リスクに対する知識、およびそのリスクの対策のために講じられる措置のうち、監視カメラを通じたサービス受益者の肖像の映り込みなど、サービス受益者のプライバシー等の権利に一定の影響を及ぼしうるものがあることを理解すること。
5) 当該 SoS が配送ロボットに限定されず、清掃ロボットや警備ロボット、施設案内ロボットにも用いられていることを理解すること。

### 5.6.2　情報提供

おおむね以下の事項についての情報提供を行うことができるものとする。情報提供を行うに際しては、ロボットやドローンのような SoS 構成要素に貼付された緊急連絡先、または、SoS 提供者、SoS ガバナンス責任者および SoS プラットフォーム開発者に対する情報提供のために構築されたスキームを利用する。この場合において、以下に掲げる事項ならびに情報提供スキームは、SoS 事業推進担当部署による合意のうえで任意に作成、変更または修正されることがある。

① ヒヤリハット情報
② 急停止など不具合情報
③ サービスに対する要望や不満、満足など障害対応
④ その他 SoS システムないしサービスのカイゼンにつながる情報
⑤ SoS ガバナンス責任者から示された VSN に対するフィードバック

＊上記「VSN に対するフィードバック」には、この分析結果にサービス受益者がどのような目的を持って SoS サービスを利用しているか、SoS サービスに対してどのような価値認識（どのように使用されるか）を行い、どのような機能を求めているか、そこでどのようなリスクが存在するかという内容が含まれる。

＊かりにサービス受益者からフィードバック情報が得られなかった場合でも、情報提供が必要であるにもかかわらずこれがなされなかった限りで、SoS 事業推進担当部署の責任において当該状況の改善にかかる措置が講じられる。

## 5.7　潜在的サービス受益者（教職員・学生・地域住民）

潜在的サービス受益者とは、SoS 運用時に提供されるサービスに対して直接関与はしないものの、将来的に SoS サービスによる利益を享受する主体を指す。潜在的サービス受益者は、当該 SoS において事故、ヒヤリハットもしくは不具合が発生した場合における SoS 提供者等に対する通報、または第三者の観点による当該 SoS 運用に対するクレームもしくはフィードバックを行うこともできる。

この「潜在的サービス受益者」には、立命館大学の学内機関、教職員、学生のほか、大学周辺の地域住民も該当するが、学内機関については情報提供を必要な限りで提供するものとし、その他の

主体からの情報提供は任意によってもたらされることに留意する。

おおむね以下の事項についての情報提供を行うことができるものとする。情報提供を行うに際しては、ロボットやドローンのような SoS 構成要素に貼付された緊急連絡先、または、SoS 提供者、SoS ガバナンス責任者および SoS プラットフォーム開発者に対する情報提供のために構築されたスキームを利用する。この場合において、以下に掲げる事項ならびに情報提供スキームは、SoS 事業推進担当部署による合意のうえで任意に作成、変更または修正されることがある。

1） ヒヤリハット情報
2） 急停止などの不具合情報
3） その他 SoS システムないしサービスのカイゼンにつながる情報

# 6　実証実験への対応

本章は、SoS サービスを実用化に供するための実証実験において遵守すべき事項を示すものである。とりわけ、実証実験においては当該 SoS サービスの実用化に比較して期間・場所など当該 SoS サービス運用における外部条件が限定されるため、一般的な実用段階を想定する 5 における所掌事務に加えて、実証実験の実施ならびに実施者において遵守すべき事項および実証実験後にとるべきアクションは、以下に示される。

ただし、実証実験の実施者が 5 における SoS 提供者、SoS プラットフォーム開発者、SoS ガバナンス責任者となることを妨げない。

## 6.2　実証実験の実施における総則

一般参加者を対象とした外部向けの実証実験では、以下の事項の遵守に努めなければならない。

1）　実証実験の実施にあたっては、事前に SoS ガバナンス責任者を中心としたプロジェクトチームを組織し、実証実験を遂行する主体とともに実証実験の実施内容を検討し、プロジェクトとして管理できるよう組織体制も含めて計画立案をする。

2）　ヒヤリハット情報収集のための体制について実証実験を行う主体間で構築する。この場合において、SoS 運用者側で事前にこれを定めることができるものとする。

3）　実証実験を行う主体は、当該プロジェクトにかかる計画、実証実験の実施から終了までの記録を保管する。

## 6.3　実証実験を行う主体における遵守事項

実証実験の実施者は、以下の事項を実施または遵守するよう努めなければならない。

1）　被験者および被験者以外の第三者の生命、身体、財産、プライバシーその他の権利が侵害されないよう、細心の注意を払うこと。特に、実証実験内容に関して、これを実施する施設や場所の状況に即したリスクアセスメントを行い、安全性の確保を目的とした基本的な計画を立案し、必要に応じて倫理委員会（人対象倫理審査委員会、理工系安全管理委員会その他の当該実証実験にかかる専門的委員会を含む）の意見を聴取したうえで、同計画を実施すること。

2）　使用する SoS 構成要素である機器についてあらかじめ定めた、あるいは合意された選定基準に則り選定すること。

3） 実証実験に先立ち、SoS 構成要素の製造者等より、使用する機器の安全上の仕様および残留リスクが記載された書面を取得すること。

4） 安全確保上の必要があるときは、一定の年齢、身長、体重または技能等を備えた者を被験者とすること。この場合においては、個人情報保護法の規定に従いつつ、セキュリティを確保しながら SoS ガバナンス責任者とともに、当該データを適切に管理すること。

5） 実証実験中に事故が発生する可能性があると考えられる場合には、あらかじめ、事故発生時の対応手順を策定すること。

6） 5）における事故を回避するための必要かつ十分な安全上の情報を広報すること。

7） 実証実験を実施した結果、新たに判明した危険源やリスクの内容について得た知見を記録し、これを遅滞なく SoS ガバナンス責任者、SoS プラットフォーム開発者ならびに SoS 構成要素の製造者その他関係者に通知すること。

8） 実証実験実施上の事故に基づく損害賠償を補償する責任保険または損害保険に加入すること。

9） 実証実験を遂行する主体は、当該実証実験終了後に当該実証実験にかかるデータを保管および検証を行い、SoS サービスの向上に反映することに努める。この場合においては、SoS ガバナンス責任者の項（5.2）に記載する事項に従ってデータを管理すること。

# 7 テストベッドを含む SoS 運用のワークフロー

本章は、テストベッドを含む SoS 運用ならびに実証実験時に 5.2 から 5.7 に掲げたステークホルダーが果たす役割を示すものである。なお、本章の記載はあくまで例示であり、実際の運用にあたっては、関連法令を遵守しつつ、適宜 SoS 事業推進担当部署との合意のうえで任意に変更することができるものとする。

## 7.2 陸上において SoS プラットフォームを利用する場合の運用にかかるワークフロー

【SoS 運用前】

1） SoS 事業推進担当部署は、SoS 運用にかかる利用申請における当該 SoS テストベッドないし SoS サービスの運用の運行計画およびサービス受益者ならびに潜在的サービス受益者の遵守事項につき審査を行うものとする。この場合において、以下に掲げる事項を考慮するものとする。

**【共通事項】**

1)サービス提供に使用する SoS 構成要素(配送ロボット、清掃ロボット、施設案内ロボット、巡回警備ロボット等)の性能に関する情報
2)サービス提供者の人員に関する情報およびその指揮系統(現場責任者、サービス提供実施者その他補助者等の氏名)
3)運行経路
4)施設設備・周辺通路および道路の状況
5)運用日に予想される天候
6)サービス提供を行う日時において場所の周辺で開催されるイベント
7)サービス受益者となる者の年齢等の属性
8)サービス提供を通じて得られるデータの利用目的
9)サービス提供を通じて得られるデータのセキュリティ確保の手段
10) その他 SoS 提供者をはじめとする SoS 運用者(以下、「SoS 運用者等」という)が求める内容

＊なお、運用する SoS 構成要素であるロボットの用途、たとえば配送ロボット、清掃ロボット、コミュニケーションロボット（施設案内ロボット)、巡回警備ロボットおいては、それぞれにおいて対応する以下に掲げる事項も上記に加えて考慮することが推奨される。

**【配送ロボット】**

1） 配送対象物
2)(資金決済が生じる場合)配送対象物ないし配送にかかる決済に対する決済代行企業の提供するサービス含む資金決済方法
3)(資金決済が生じる場合)資金決済に対応する証憑(領収書・適格請求書その他財務会計上必要な書類)の仕様
4） その他効率的な物品配送を実現するために搭載される機能として SoS 運用者等が必要と認めるもの

**【清掃ロボット】**

1） 清掃に用いられる化学製品等に関する情報
2)【共通事項】の 3)運行経路に対応する運行時間
3)その他効率的な施設清掃を実現するために搭載される機能として SoS 運用者等が必要と認めるもの

**【コミュニケーションロボット】（※現時点では施設案内ロボット）**

1） 運行速度・運行可能領域
2） 運行時の画面表示およびユーザーインターフェース(UI)に関する以下の情報
①操作案内音声の有無(会話速度、音声の種類・数およびこれらが変更する機能の有無を含む)
②①の他に当該ロボット作動中に発せられる会話の内容

③多言語対応の有無(日本語以外の言語を用いる場合はどの言語を用いるかを明確にすること)
④運行経路表示(ナビゲーション表示)の有無
3)(利用者であるサービス受益者の音声を認識して操作するものである場合)音声認識感度に関する情報およびその操作案内の有無
4)エラー発生あるいは緊急時に利用者であるサービス受益者が SoS 提供者等当該サービスの管理者に連絡できる仕様となっているか。
5)その他利用者であるサービス受益者と円滑なコミュニケーションを図りつつ、効率的な施設案内を実現するために搭載される機能として SoS 運用者等が必要と認めるもの

**【巡回警備ロボット】**

1) 運行速度
2) 運行経路とそれに対応する運行時間
3) 当該巡回警備ロボットが異常を検知した場合における現場においてこの対応を遂行する者の氏名および従事時間
4) 緊急対応を要する場合の連絡・指揮系統
5)その他安心・安全な施設警備を実現するために搭載される機能として SoS 運用者等が必要と認めるもの

2) 上記計画においては、運用当日の人員配置を SoS 提供者ないしサービス提供者の合意のもとで定めることができる。この場合、SoS 運用の実地に配置する実地監視員（SoS 提供者補助員〔SoS 提供者を補助する者であり、SoS 提供者の指揮監督のもとでその補助業務を遂行する者〕が望ましい。なお、SoS 提供者がこれを兼任することを妨げない）および配送ロボットの挙動を遠隔で監視することができる統括監視員（SoS 提供者に限る）を適切に配置することに努め、必要に応じて 3D モデル等シミュレーションモデルの操作ならびに保守管理を遂行する SoS プラットフォーム開発者も置くものとし、これら主体がすべて「8 インシデントへの対応」に示すインシデントに対応しうるよう、連絡体制およびエスカレーションルールを構築するものとする。

3) 2)に掲げるほか、配送ロボットの挙動の不具合等が生じた場合に、サービス提供者に対して適切な指示を与えられるよう、事前のマニュアルおよび連絡体制を構築する。

4) 1)から 3)に掲げる事項を満たした場合に、法令（道路交通法、民法、個人情報保護法、電波法その他の関連法規）の遵守に関する誓約書の提出をもって、SoS ガバナンス責任者は運用を希望する SoS 提供者ならびにサービス提供者に対して当該 SoS の運用許可を出すものとする。

5) 運用当日において、SoS 事業推進担当部署の最終意思決定をなしうる主体としての SoS ガバナンス責任者は「8 インシデントへの対応」に掲げるインシデントに対する必要な対応を講じうるために実地の SoS 提供者または SoS プラットフォーム開発者と連携をとれるような体制を確立する。

【SoS 運用当日】

1) 実地の実地監視員（SoS 提供者または SoS 提供者補助員）は、①SoS（テストベッド）ないし SoS サービスの運用が上記１）から４）に定める事項を遵守したものであるか、②サービス受益者または潜在的サービス受益者が当該 SoS の運用にかかる遵守事項を遵守できている

かを常時確認できるようにする。このとき、SoS 提供者は、SoS 提供者補助員に対し、自らの責任でこの業務の一部を委ねることができる。

2) 実地の SoS 提供者と配送ロボットを監視する実地監視員は、統括監視員、SoS プラットフォーム開発者および SoS ガバナンス責任者が連携するためのハブとしての役割を果たし、連絡体制の維持に努めるものとする。ただし、実地監視員が SoS 提供者補助員である場合は、統括監視員がこの役割を果たすものとする。

3) インシデント発生時には、「8．インシデントへの対応」に記載される手順に従って実地監視員が対応を行う。

## 7.3 空中において SoS プラットフォームを利用する場合（配送ドローン等）の運用にかかるワークフロー

【SoS 運用前】

1) 立命館大学は、ドローン飛行許可証交付にあたり、以下に掲げる事項を明示するものとする。

| |
|---|
| ⑴ 100ｇ以下のドローンに関する学内ルール<br>⑵ 飛行可能場所・飛行禁止場所・飛行場所ごとの飛行高度その他の詳細なルールを示したマップを作成し、とくに建物上空・OIC フィールド内以外の飛行禁止、線路・高速道路付近における高度制限などを明示する。 |

2) 立命館大学は、学生・職員向けに大学敷地内でのドローン運用ルールについて講習を実施する。

3) SoS 事業推進担当部署は、事前に、航空法ならびに小型無人機等飛行禁止法その他の関連法令の定めに従い、サービス提供者による SoS 運用にかかる利用申請における当該 SoS テストベッドないし SoS サービスの運用の運行計画およびサービス受益者ならびに潜在的サービス受益者の遵守事項につき審査を行い、学内におけるドローン飛行許可証を発行するものとする。この場合においては、以下の事項を考慮するものとする。

1）使用するドローンの飛行経路・空域の決定について、人口集中地区[10]の飛行（航空法 132 条の 85 第 1 項 2 号参照）、空港等周辺空域・緊急用務空域[11]・150m 以上の上空など航空機の航行の安全に影響を及ぼすおそれの空域（航空法 132 条の 85 第 1 項第 1 号参照）など国土交通大臣の許可対象の飛行となるか否か
2）使用するドローンの情報（機体の縦横幅・重量）
3）使用するドローンの運航手順および運航者の技能（免許の有無を含む）
4）使用するドローンにかかるリモート ID、技適、登録機体番号の明記
5）使用するドローンが障害物センサーなど衝突回避機能を有しており、最大風圧抵抗は、10.7 m/s（スケール 5）以上の機体であるか否か
6）使用するドローンに鳥追い払い装置など、鳥獣対策の実施がなされているか否か
7）施設設備、周辺通路および道路・鉄道路線の状況
8）運用日に予想される天候
9）SoS 運用を行う場所とその周辺で開催されるイベント
10）配送ドローンの場合は配送対象物
11）学生・職員向けに大学敷地内でのドローン運用ルールに関する講習の受講の有無
12）サービス受益者となる者の年齢等の属性
13) 使用するドローンを通じて得られた情報の利用目的
14) その他の必要と認められる事項

4） 3)に掲げる計画においては、運用当日の人員配置を SoS 提供者ないしサービス提供者の合意のもとで定めることができる。この場合、SoS 運用の実地に配置する実地監視員（SoS 提供者補助員が望ましい。なお、SoS 提供者がこれを兼任することを妨げない）および配送ロボットの挙動を遠隔で監視することができる統括監視員（SoS 提供者に限る）を適切に配置することに努め、必要に応じて 3D モデル等シミュレーションモデルの操作ならびに保守管理を遂行する SoS プラットフォーム開発者も置くものとし、これら主体がすべて「8． インシデントへの対応」の章において示されるインシデントに対応しうるよう、連絡体制およびエスカレーションルールを構築する。

5） 4)に掲げるほか、配送等ドローンの挙動に不具合等が生じた場合に、サービス提供者に対して適切な指示を与えられるよう、事前のマニュアルおよび連絡体制を構築する。

6） 1)から 5)に掲げる事項を満たしたうえで、以下に示す条件に合致する場合において SoS ガバナンス責任者は、運用を希望する SoS 提供者ならびにサービス提供者に対して、当該 SoS の運用許可を出すものとする。

[10] 立命館大学大阪いばらきキャンパスが所在する大阪府茨木市全域および立命館大学衣笠キャンパスの敷地（京都市北区等持院北町 56-1）は、飛行許可申請対象地区の人口集中地区であることに留意されたい。なお、立命館大学びわこ・くさつキャンパスの敷地内（滋賀県草津市野路東 1 丁目 1−1）は、これに該当しない。

[11] 「緊急用務区域」に該当する場合は、許可があってもドローンを航行させてはならない。

⑴大学敷地内でドローンを飛行させる者について、国土交通省が発行する操縦者技能証明書の提示。
⑵法令（航空法、小型無人機等機飛行禁止法、道路交通法、民法、個人情報保護法、電波法その他の関連法規）の遵守に関する誓約書の提出。
⑶学内のドローン飛行許可申請書に加え、下記書類の添付。
①様式１　無人航空機の飛行に関する許可・承認申請書
②様式２　無人航空機の機能・性能に関する基準適合確認書
③飛行許可証
④通報計画の通報がわかるもの（DIPS 通報画面のスクリーンショット等）
⑥　技能証明書の写し

7） 運用当日において、SoS 事業推進担当部署の最終意思決定をなしうる主体としての SoS ガバナンス責任者は 8 に掲げるインシデントに対する必要な対応を講じうるために実地の SoS 提供者または SoS プラットフォーム開発者と常に連絡をとることができるようにしておく。

【SoS 運用当日】

1） SoS 運用当時、OIC の A 棟屋上に設置した風速計の値が風速 5m/s 以下である場合に限り、ドローンを運行させることができる。

2） SoS 運用当日に、降雨・降雪時またはゲリラ豪雨・落雷のおそれがある場合は、直ちに運行を中止する。

3） 実地の実地監視員（SoS 提供者または SoS 提供者補助員）は、当該 SoS テストベッドないし SoS サービスの運用が上記【SoS 運用前】にかかわる 1)から 6)に定める事項を遵守したものであるか、およびサービス受益者または潜在的サービス受益者が当該 SoS の運用にかかる遵守事項を遵守できているのかを常時確認できるようにする。このとき、SoS 提供者は、SoS 提供者補助員に対し、自らの責任でこの業務の一部を委ねることができる。

4） 実地の配送ドローンを監視する実地監視員は、統括監視員、SoS プラットフォーム開発者および SoS ガバナンス責任者が連携するためのハブとしての役割を果たし、連絡体制の維持に努めるものとする。ただし、実地監視員が SoS 提供者補助員である場合は、統括監視員がこの役割を果たすものとする。

5） 実地監視員は配送ドローンの運航経路にサービス受益者ないし潜在的サービス受益者がみだりに侵入しないようにするなど、これらの者の身体上の安全に最大限に留意して SoS の運営に努める。

6） インシデント発生時には、「8 インシデントへの対応」に記載される手順に従って実地監視員が初動対応を行う。この場合において、統括監視員や SoS プラットフォーム開発者その他の SoS 事業推進担当部署の構成員がこれを行うことを妨げない。

## 7.4 SoS 運用終了後のワークフロー

1） 運用終了後、SoS 提供者は、許可を受けた運行計画に従って当該 SoS の運用がなされていたのかについて、その運用に関与したサービス提供者、サービス受益者ないし潜在的サービス受益者からの情報提供またはフィードバックを考慮しつつ、事後評価を行うための報告を行う。
＊この事後評価においては、たとえば SoS テストベッド運用に関与したサービス受益者ないし潜在的サービス受益者となる学生・教職員・一般市民の SoS に対する価値認識を VSN で分析し、unknown なリスクの発見に努めることが考慮される。

2） 前項の報告を受けて、SoS 提供者および SoS 提供者補助員、SoS プラットフォーム開発者、SoS ガバナンス責任者により構成されるガイドライン検討委員会（10 参照）は、次回以降の運用について必要に応じて修正案（ガイドラインその他別添に掲げるチェックリスト等を含む）を検討し、これを本学研究部の同意のもとで修正を施すものとする。このとき、修正の必要がなくても、当該サービスに関する記録を保存するものとする。

3） ガイドライン検討委員会は、前項の同意を得た後に修正を施したガイドラインその他別添に掲げるチェックリストを遅滞なく公表するものとする。

4） 1)から 3)のほか、将来の SoS テストベッド運用において、新たな価値創造・イノベーション創出およびインセンティブに関する積極的な要素が見出された場合には、以降の SoS テストベッド運用にかかる運用計画ないしこれに付随する諸サービスに反映させるものとする。この場合において、必要に応じガイドラインその他別添に掲げるチェックリストに当該内容を反映し、これを公表することができるものとする。

# 8 インシデントへの対応

本章は、SoS におけるリスクマネジメントおよび社会受容性の確保を目的として、SoS サービス運用中（実証実験による運用を含む）において想定されるインシデントの対応を、以下において例示的に列挙する形式で示すものである。

なお、必要に応じて本章に記載される内容を具体化するための用語定義、数値基準の定義、具体的な担当者等その他必要な事項は、SoS ガバナンス責任者、SoS プラットフォーム開発者、SoS 提供者で構成される組織あるいはこれに準ずる組織との合意のうえで任意で決定することができるものとする。併せて、以下で示されない unknown unknowns に該当するインシデントないしそのおそれが生じたときは、SoS ガバナンス責任者、SoS プラットフォーム開発者、SoS 提供者らは、(ｱ)当該インシデントが発生した場合には遅滞なくその解決ならびに分析を遂行し、(ｲ)当該インシデントが発生するおそれが判明した場合には遅滞なくその分析を遂行し、当該インシデントに対するアクションフローを都度詳細版に追加あるいは修正するものとする。

この場合において、本ガイドラインにおいて具体化された事項については、本ガイドラインの改定に限られず、本ガイドラインの内容を補足するための補遺、規則文書その他の必要と認められる方法により本ガイドラインとは別に作成された文書により定めることができるものとする。

## 8.2 事故・ヒヤリハットが発生した場合

実証実験を含む SoS サービス提供時に各サービス受益者に事故もしくはヒヤリハットが生じた際における SoS 提供者等のアクションフローを示す。ただし、必要に応じて本項に掲げる事項は、サービス提供者、SoS ガバナンス責任者でも遂行することができるものとする。

### 8.2.1 事故が発生した場合

1）事故が発生した場合、その事故の客体が⑴本学学生、⑵本学教職員、⑶その他の一般人、⑷物のいずれであるかによりアクションフローが異なるため、以下それぞれについて記載する。なお、本項目の主体は SoS 提供者または SoS 提供者補助員（実地監視者・統括監視者であるかを問わない）とするが、これには限定されない。

(1) 本学学生

① 配送ロボットまたは SoS 運用にかかる領域内掲示に記載された緊急連絡先から通報があった場合、または実地監視者・統括監視者が事故に気づいた場合は、実地監視者が当該事故現場に赴く。このとき、作動している配送ロボット等の SoS 構成要素は一度停止するものとする。

② 当該事故の状況を速やかに統括監視者に報告し、傷害の程度が軽微と判断された場合には、保健担当部署に治療を求めるものとする。ただし、保健担当部署受付時間外に実証実験を含む SoS サービスを運用する場合には応急処置を施すものとし、その応急処置に必要な医療器具をあらかじめ準備

しておくこと。

③ 傷害の程度が軽微でない場合は、速やかに 119 番通報を行うこと。

④ 事故の軽重にかかわらず、統括監視者は「事故発生時の連絡票」を施設管理担当部署またはこれに準ずる機関に送付すること。

⑤ キャンパス内で生じた本件事故が傷害を受けた者の過失によるものであり、かつ、一定期間の通院を要するものであるときは、統括監視者は、関連する機関に学生教育研究災害傷害保険の申請を行う。

⑥ 当該 SoS による事故が施設の瑕疵によるものであるときは、統括監視者は、施設賠償責任保険を担当部署（以下、単に「施設賠償責任保険担当部署」という）に申請する。その後、施設賠償責任保険担当部署は SoS ガバナンス責任者に通知する。

(2) 本学教職員

① 配送ロボットまたは SoS 運用にかかる領域内掲示に記載された緊急連絡先から通報があった場合、または実地監視者・統括監視者が事故に気づいた場合は、原則として実地監視者が当該事故現場に赴く。このとき、作動している配送ロボット等の SoS 構成要素は一度停止するものとする。

② 当該事故の状況を速やかに統括監視者に報告し、傷害の程度が軽微と判断された場合には、保健担当部署に治療を求めるものとする。ただし、保健担当部署受付時間外に実証実験を含む SoS サービスを運用する場合には応急処置を施すものとし、その応急処置に必要な医療器具をあらかじめ準備しておくこと。

③ 傷害の程度が軽微でない場合は、統括監視者は速やかに 119 番通報を行うこと。

④ 当該教職員勤務時間中の事故と認められる限りで労災保険が適用されるため、統括監視者は、当該教職員にこの保険を適用する旨を通知すること。

⑤ 当該 SoS による事故（当該教職員の勤務時間中の事故に限定されない）が施設の瑕疵によるものであるときは、統括監視者は施設賠償責任保険を施設賠償責任保険担当部署に申請し、施設賠償責任保険担当部署は SoS ガバナンス責任者に通知する。

(3) その他一般人

① 配送ロボットまたは SoS 運用にかかる領域内掲示に記載された緊急連絡先から通報があった場合、または実地監視者・統括監視者が事故に気づいた場合は、実地監視者が当該事故現場に赴く。このとき、作動している配送ロボット等の SoS 構成要素は一度停止するものとする。

② 当該事故の状況を速やかに統括監視者に報告し、傷害の程度が軽微であれば、実地監視者が応急処置を施すこと。この場合、当該応急処置に必要な医療器具はあらかじめ準備しておく。

③ 傷害の程度が軽微でない場合は、統括監視者は速やかに 119 番通報を行う。

④ 当該 SoS による事故が施設の瑕疵によるものであるときは、統括監視者は施設賠償責任保険を施設

賠償責任保険担当部署に申請し、施設賠償責任保険担当部署は SoS ガバナンス責任者に通知する。

⑤ 施設管理部署が受付窓口となり、遅滞なく SoS ガバナンス責任者へ通知する。

⑷ 物

① 配送ロボットまたは SoS 運用にかかる領域内掲示に記載された緊急連絡先から通報があった場合、または実地監視者・統括監視者が事故に気づいた場合は、実地監視者が当該事故現場に赴く。このとき、作動している配送ロボット等の SoS 構成要素は一度停止するものとする。

② 当該事故の状況を速やかに統括監視者に報告し、運用に関与するすべての主体の安全確保を行うとともに、SoS ガバナンス責任者に遅滞なく通知し、当該物損事故にかかる情報共有を SoS 事業推進担当部署で行う。

③ 当該 SoS による事故が施設の瑕疵によるものであるときは、統括監視者は施設賠償責任保険を施設賠償責任保険担当部署に申請し、施設賠償責任保険担当部署は SoS ガバナンス責任者に通知する。

2）実地監視員ないし統括監視員が 1）(1)～(4)に掲げる①のワークフローにおいて事故の処理を行ったのち、SoS 提供者は、事故の軽重にかかわらず、当該事故の調査担当として当該事故の検証を他の SoS 事業推進担当部署と連携して行う。

3） 2)により事故原因にかかる情報を収集したのち、SoS 事業推進担当部署で構成される事故検討委員会を開催し、事故原因の特定および将来の改善策を記した事故報告書を作成するものとする。

4）必要に応じて、学生を含むサービス受益者に当該事故の経緯報告を行うものとする。併せて、必要に応じて SoS 運用（SoS テストベッドを含む）にかかる安全評価基準等の修正をガイドライン検討委員会もしくは SoS ガバナンス責任者の求めに応じて構成される委員会により行うものとする。

5）事故により損害が生じた場合は、遅滞なく被害者に対して補償を行わなければならない。

### 8.2.2 ヒヤリハットの場合

1） 事故には至らないヒヤリハットの情報が、配送ロボットに記載された緊急連絡先から通報された場合、または実地監視者・統括監視者が事故に至らないヒヤリハット気づいた場合は、実地監視者が当該ヒヤリハット現場に赴くものとする。このとき、作動している配送ロボットないし配送ドローン等の SoS 構成要素は一度停止するものとする。

2） 実地監視者は、当該ヒヤリハットの状況および事情をその関係者から聴取し、これを統括監視

者に遅滞なく報告する。

3） 統括監視者は、SoS プラットフォーム開発者と協同して、３D モデル等を用いて当該ヒヤリハットの原因を特定するための分析を行う。

4） 3)の分析により特定されたヒヤリハットの原因分析結果については、遅滞なく SoS ガバナンス責任者に報告するものとし、SoS 事業推進担当部署で当該分析結果にかかる情報を共有する。

## 8.3 不具合・障害を検知ないし発見した場合

### 8.3.1 サービス受益者からの通報

サービス受益者が、普段のサービスとの差異、サービスの低下、ロボットの挙動に異常のある SoS についての不具合もしくは障害を発見した場合、または、運用されている各種モビリティに不具合もしくは懸念事項を発見して通報した場合は、通報ルールに基づいて、サービスやサービス提供にかかるモビリティなどの不具合を、監視業務を所掌する SoS 提供者に通知するものとする。

### 8.3.2 監視業務を所掌する SoS 提供者からの通報

監視事務を行う SoS 提供者または当該監視事務に関与する SoS プラットフォーム開発者が、普段とのサービスの差異、サービスの低下、ロボットの挙動に異常のある SoS についての不具合・障害を発見した場合、または、運用されている各種モビリティに不具合や懸念事項を発見して通報した場合は、通報ルールに基づいて、サービスやサービス提供にかかるモビリティなどの不具合を、他の SoS 提供者に遅滞なく通知する。

### 8.3.3 通報後のワークフロー

1） 通報窓口である監視業務を所掌する SoS 提供者は、通報を受けて関係者に通知を行い、緊急対応に入る。

2） 実地監視者、統括監視者、サービス提供者等実地にいる者は、必要に応じて避難指示を出し、誘導する。

3） 当該障害が収拾した場合は、SoS 事業推進担当部署は、障害の原因究明を検討委員会にて遂行する。

4） SoS 提供者および SoS プラットフォーム開発者は、障害の発生源の特定に努め、障害の発生源が判明した場合は、該当者が当該箇所に対する緊急対応を施す。

5） SoS ガバナンス責任者は、障害原因にかかる報告書を速やかにサービス受益者や潜在的サービス受益者に公開することにより、説明責任を遂行する。

## 8.4 サービス提供者が異常を検知した場合

1） サービス提供者がシステムに異常を検出したときは、SoS 提供者への連絡を相互に迅速に行う。

2） 避難が必要である場合は、実証実験責任者またはサービス提供者等の実地の関係者は、サービス受益者等の誘導対応も行う。

3） サービス提供者または SoS 事業推進担当部署は、迅速な障害対応を実施すること。この場合においては、当該異常の検知に伴う他の影響についても考慮する。

4） SoS 事業推進担当部署は障害の発生源を特定し、緊急の対応を行う。

5） サービス提供者または SoS 提供者は、サービス受益者に対し、当該 SoS に不具合が生じていること、またはその影響について可能な限り現状を報告する。

6） SoS ガバナンス責任者、SoS プラットフォーム開発者、SoS 提供者は、障害の原因究明を実施する。

7） 当該異常の検知にかかるインシデントが収拾した場合は、SoS ガバナンス責任者は、速やかにサービス受益者をはじめとするすべての SoS に関与するステークホルダーに対し、説明責任を遂行する。

## 8.5 外部の変化を検出した場合

1） 外部の変化（SoS 事業推進担当部署を構成するある主体が他の主体の意思に関係なく SoS サービスにかかる構成要素を任意に改変させた場合を含む）を SoS 事業推進担当部署が検出した場合は、事前に定義したルールにより、アジャイル・ガバナンスの方式で対応するものとする。
2） SoS 事業推進担当部署はこれを協議し、必要な対応について合意したのち、指示系統に従い、指示を出す。

3） 必要に応じて、SoS に変更ないし修正を加え、当該 SoS 変更後のマネジメントおよびガバナンスが

正常に機能することを検証する。

4) SoSガバナンス責任者は、SoSについて実施した上記3)の内容について、ステークホルダーに対する説明責任を遂行する。
5) SoSサービスにかかる運用手順に変更がある場合は、その変更の限りにおいて当該SoS運用に係る手順書、事前計画書その他の関連文書の更新を行う。

6) サービスに変更が生じた場合、またはサービス提供の手順などに変更が生じた場合は、サービス受益者などに対して、当該変更について周知する。

## 8.6 SoSの構成要素を変更する場合

### 8.6.1 サービス提供者の求めに応じてSoSの構成要素を変更する場合

1) SoSの利用を希望するサービス提供者の求めに応じてSoSの構成要素が変更する、あるいは変更が必要となる場合は、窓口である監視業務を所掌するSoS提供者は、その旨を他のSoS事業推進担当部署に遅滞なく報告する。

2) 1)の手続により提供された情報に即して、あらかじめ定めた安全基準等SoS運用にかかる基準に照らして、SoS事業推進担当部署は速やかに検討および審査を行う。

3) 2)による審査の結果、SoSの構成要素を変更することが合意されなかった場合は、サービス提供者に対してその理由を文書または口頭により遅滞なく示すものとする。この場合において、SoS事業推進担当部署は、サービス提供者による申請に対してSoS事業推進担当部署で定めた基準に適合するための方法を教示することに努めるものとする。
4) 2)による審査の結果、SoSの構成要素を変更することが合意された場合は、SoS事業推進担当部署に対し指示系統に従い指示を出し、その変更につき担当することのできるSoS事業推進担当部署は、当該箇所に対して変更対応を実施する。

5) 4)の変更対応を行ったSoS事業推進担当部署は、当該対応が適切になされた旨の検証を実施する。

6) 変更が適切に実施された場合もしくは変更をしなかった場合のいずれにおいても、SoSガバナンス責任者は、すべてのステークホルダーに対して当該SoSの構成要素の変更の旨およびその結果についてその旨の公表または周知等の方法を通じて説明責任を遂行する。

### 8.6.2　サービス受益者等からの情報提供により SoS を変更する場合

#### 8.6.2.1　ワークフロー

1) サービス受益者からリクエスト、クレーム、ヒヤリハットないしフィードバックにかかる情報（以下、「情報」とする）が提供された場合は、窓口である監視業務を所掌する SoS 提供者は、SoS 事業推進担当部署に遅滞なく報告する。

2) 潜在的サービス受益者から情報提供がなされた場合は、窓口である施設管理部署は SoS 事業推進担当部署に連絡する。

3) SoS 事業推進担当部署は、提供された情報について分析・検討を行う。

4) 3)による検討の結果、SoS に対して変更することが合意された場合は、SoS 事業推進担当部署に対し指示系統に従って指示を出す。

5) 4)により指示を受けた SoS 事業推進担当部署は、当該箇所に対して変更対応を実施する。

6) 5)の変更対応を行った SoS 事業推進担当部署は、当該対応が適切になされた旨の検証を実施する。

7) 変更が適切に実施された場合もしくは変更をしなかった場合のいずれにおいても、SoS ガバナンス責任者は、すべてのステークホルダーに対してその旨の公表または周知等の方法を通じて説明責任を遂行する。

#### 8.6.2.2　通報システムの運用

1) 情報提供を受ける際、「重大でない案件」と思われる場合には、アンケートフォーム制などオンライン上での情報提供で完結できるよう、運用する SoS 構成要素に QR コードを貼付するなど、潜在的サービス受益者の負担軽減に努める。
2) 情報提供を受ける際、事故が発生しているなど「重大な案件」と思われる場合には、運用する SoS 構成要素に緊急連絡先電話番号を付すなど、監視業務を所掌する SoS 提供者に直接提供できるような体制を構築する。この場合、情報提供を受けた SoS 提供者は遅滞なく SoS ガバナンス責任者および監視業務を所掌する SoS 提供者に報告するものとする。

## 8.7　SoS の構成要素が故意または過失により毀損された場合

1) 監視業務を所掌する SoS 提供者は、サービス受益者をはじめとする第三者の安全確保を行いつつ、

当該 SoS にかかる毀損事故に関する証拠の保全を適切かつ適時に行うこと。ただし、監視業務を所掌する SoS 提供者が即時に対応できない場合には、サービス提供者が必要な限度でこれらを行い、可能な限り即時に監視業務を所掌する SoS 提供者に当該毀損事故の報告を行う。

2) 監視業務を所掌する SoS 提供者は、証拠の保全を行ったのち、当該毀損事故に関する事項を SoS 事業推進担当部署に報告する。

3) 報告を受けた SoS 提供者は、SoS ガバナンス責任者の指示に従い、必要に応じて警察に通報し、被害届を提出する。

4) SoS ガバナンス責任者は、必要に応じて SoS 事業推進委員会の構成員を含む事故調査委員会を立ち上げる。

5) 前項に掲げる事故調査委員会および SoS 事業推進担当部署を通じて損害と損害額の確定および賠償請求を行う。

6) 前 5 項に掲げるほか、運用中の SoS 構成要素であるシステムに対して不正侵入や不正利用等情報セキュリティ事故（法人の情報資産のうち、デジタルデータの機密性、完全性および可用性を維持することを損なう、または損なう可能性のある事象のことを指す）があったと認められる場合には、関連する内部規定に従って情報セキュリティ事故の対処を行わなければならない。

## 8.8 SoS サービス運営にかかる情報が漏えいした場合

### 8.8.1 個人情報に該当する収集データの漏えいの場合

1) SoS 運用中に収集したデータのうち、個人情報保護法において保護を受ける個人情報に関するデータ（SoS サービス提供中に収集した顔画像、身長、またはそれらが要配慮個人情報に該当する場合、ないしはサービス受益者から収集した氏名、連絡先電話番号またはメールアドレスその他の個人を特定するに足りる情報）が漏えいした場合は、個人情報保護委員会に遅滞なく報告する。

2) 流出した個人情報データが 1000 件以上であるときは、SoS ガバナンス責任者は、調査委員会を立ち上げて、個人情報保護委員会に報告する。

3) 流出した個人情報データの件数にかかわらず、倫理委員会が「不適合の程度が重大」と判断した場合は、立命館大学の名義で個人情報漏えいの旨を公表し、遅滞なく個人情報保護委員会に報告する。

### 8.8.2　その他情報統制について

1）SoS 事業推進担当部署は、SoS サービス運用中ないし実証実験中において事故が発生した場合にそのサービスとは無関係な周囲の人間（潜在的サービス受益者を含む）に対して撮影・録画をしないように啓発するように努める。

2）SoS 事業推進担当部署は、SoS サービスないし実証実験についてのレピュテーションリスクを考慮しつつ、当該 SoS サービスないし実証実験に関する SNS 上の情報に留意することにも努める。

# 9 有害事象への対応

本章は、以下に定義する有害事象への対応をあらかじめ手順化することにより、当該有害事象への迅速な解決を図るとともに、SoS の社会的受容の観点から信頼回復を図ることを目的とする。併せて、当該有害事象にかかる民事責任ないし刑事責任の根拠となりうる過失の構成を妨げる、注意義務の内容およびその履行を構成しうる基準を示すものとする。

## 9.2 用語定義

本章における用語の定義は、以下のとおりとする。

1) 「有害事象」とは、実施された研究との因果関係の有無を問わず、研究対象者に生じたすべての好ましくない、または意図しない傷病もしくはその徴候（臨床検査値の異常を含む）をいう（文部科学省・厚生労働省・経済産業省「人を対象とする生命科学・医学系研究に関する倫理指針」第 2 用語の定義 (36)参照）。

2) 「重篤な有害事象」とは、有害事象のうち、①死に至るもの、②生命を脅かすもの、③治療のための入院または入院期間の延長が必要となるもの、④永続的または顕著な障害・機能不全に陥るもの、⑤子孫に先天異常を来すものをいう（前掲「人を対象とする生命科学・医学系研究に関する倫理指針」第 2 用語の定義 (37)参照）。

3) 「予測できない重篤な有害事象」とは、重篤な有害事象のうち、SoS 運用にかかるあらかじめ定められた SoS の運用計画書[12]、またはインフォームド・コンセントの説明文書等において記載されていないもの、または記載されていてもその性質もしくは重症度が記載内容と一致しないものをいう（前掲「人を対象とする生命科学・医学系研究に関する倫理指針」第 2 用語の定義 (38)参照）。

## 9.3 SoS 運用時における有害事象への対応

1) SoS ガバナンス責任者ならびに SoS 提供者は、SoS の運用実施にかかる必要な情報を取得するなど、その適正な実施および運用結果の信頼性の確保に努めなければならない。

2) SoS ガバナンス責任者は、SoS の運用にかかる倫理的妥当性または科学的合理性を損なう、またはそのおそれがある事実を知り、または情報を得た場合であって、その運用の継続に影響を与えると考えられるものを得た場合には、遅滞なく、大学学長に報告し、必要に応じて、SoS の運用を停止し、もしくは中止し、またはその計画を変更しなければならない。

---

[12] 「7．SoS（テストベッド）運用のワークフロー」に掲げられる運行計画を指すものと解釈してもよい。

3) SoS ガバナンス責任者は、SoS の運用実施において、当該運用により期待される利益よりも予測されるリスクが高いと判断される場合、または当該運用により十分な成果が得られた、もしくは十分な成果が得られないと判断される場合には、当該運用を中止しなければならない。

4) SoS ガバナンス責任者は、SoS 運用にかかる事前の計画に定めるところにより、その進捗状況およびその実施に伴う有害事象の発生状況を倫理委員会（6.2 参照）および大学学長に報告しなければならない。

5) SoS ガバナンス責任者は、SoS プラットフォーム開発者、SoS 提供者およびサービス提供者に対し、当該 SoS 運用に関連する必要な情報を共有しなければならない。

6) 大学学長は、2)または 4)による報告を受けた場合には、必要に応じて、倫理委員会の意見を聴き、速やかに SoS の運用の中止、原因究明等の適切な対応をとらなければならない。この場合、倫理委員会が意見を述べる前においては、必要に応じ、SoS ガバナンス責任者に対し、その運用の停止または暫定的な措置を講ずるよう指示しなければならない。

## 9.4 重篤な有害事象への対応

### 9.4.1 SoS ガバナンス責任者を除く SoS 事業推進担当部署の対応

SoS ガバナンス責任者を除く SoS 事業推進担当部署は、重篤な有害事象の発生を知った場合には、次項 1)および 3)の規定による手順書等に従い、サービス受益者等への説明等、必要な措置を講ずるとともに、遅滞なく SoS ガバナンス責任者に報告しなければならない。

### 9.4.2 SoS ガバナンス責任者の対応

1) SoS ガバナンス責任者は、あらかじめ定められた SoS の運用計画書に、重篤な有害事象が発生した際の SoS 事業推進担当部署（SoS ガバナンス責任者を除く）が実施すべき対応手順を記載し、当該手順に従って適正かつ円滑に対応が行われるよう必要な措置を講じなければならない。

2) SoS ガバナンス責任者は、SoS の運用実施において重篤な有害事象の発生を知った場合は、速やかに、当該有害事象や運用の継続等について倫理委員会に意見を聴いたうえで、その旨を大学学長に報告するとともに、1)および 3)の規定による手順等に従い、適切な対応を図らなければならない。また、速やかに当該 SoS 運用の実施に携わる SoS 事業推進担当部署（SoS ガバナンス責任者を除く）に対して、当該有害事象の発生にかかる情報を共有し、事故調査委員会を立ち上げなければならない。

3) SoS の運用実施において予測できない重篤な有害事象が発生し、当該運用との直接の因果関係が否定できない場合は、SoS ガバナンス責任者は、本学の長に報告したうえで、速やかに、2)の規定による対応の状況および結果を厚生労働大臣に報告し、公表しなければならない。

### 9.4.3 大学学長の対応

大学学長は、あらかじめ、SoS の運用時に重篤な有害事象が発生した際に SoS 事業推進担当部署（SoS ガバナンス責任者を除く）が実施すべき事項に関する手順書を作成し、当該手順書に従って適正かつ円滑に対応が行われるよう必要な措置を講じなければならない。

## 9.5 大臣への報告等

1) 大学学長は、当該研究機関が実施している、または過去に実施した研究について、この指針に適合していないことを知った場合には、速やかに倫理委員会（6.2 参照）の意見を聴き、必要な対応を行うとともに、不適合の程度が重大であるときは、その対応の状況および結果を厚生労働大臣（文部科学省の所管する研究機関にあっては文部科学大臣および厚生労働大臣。経済産業省の所管する研究機関にあっては厚生労働大臣および経済産業大臣。以下、単に「大臣」という）に報告し、公表しなければならない。

2) 前項における「不適合の程度が重大であるとき」とは、研究ごとに倫理審査委員会の意見を聴いて、当該研究の倫理的妥当性および科学的合理性が損なわれるほどに著しくこの指針から逸脱しているかという観点で判断される。ただし、下記各号に掲げる場合は、当該 SoS 運用の内容にかかわらず、不適合の程度が重大であるとみなし、大臣に報告し公表しなければならない。

   ① 倫理審査委員会の審査または本学長の許可を受けずに SoS の運用を実施した場合
   ② 必要なインフォームド・コンセントの手続を行うことなく SoS 運用を実施した場合
   ③ SoS の運用内容の信頼性を損なう程度の運用結果のねつ造や改ざんが発覚した場合
   ④ SoS の運用に関連する情報が漏えい（情報が外部に流出すること）、滅失（情報の内容が失われること）または毀損（情報の内容が意図しない形で変更されることや、内容を保ちつつも利用不能な状態となること）の報告を受けた場合
   ⑤ 研究の参加について研究対象者の自発的な意思決定が制限された場合、重大な有害事象が発生した場合その他の研究の継続に影響を与えるような情報を知り得た場合（これに類似する研究対象者等の人権を尊重する観点または研究の実施上の観点から重大な懸念が生じた場合においてこれに関連する報告を受けた場合を含む）

3) 大学学長は、当該研究機関における研究がこの指針に適合していることについて、大臣またはその委託を受けた者が実施する調査に協力しなければならない。

## 9.6　将来に向けた対応

1）　本学学生を含むサービス受益者に対する当該有害事象の経緯報告は、遅滞なく行われなければならない。

2）　当該有害事象を受け、 SoS の運用にかかる安全評価基準、監視対象データ、ガイドラインその他別添に掲げるチェックリスト等の修正をガイドライン検討委員会（10 参照）もしくは SoS ガバナンス責任者の求めに応じて構成される委員会により遅滞なく行わなければならない。

# 10　ガイドラインその他関連規定の見直しまたは改正

本章は、本ガイドラインその他関連規定の見直しまたは改正にかかるプロセスを規定するものである。このプロセスは、インシデントや有害事象の発生における事故等調査結果のみならず、実証実験や SoS テストベッド運用から得られたフィードバックを基調として、SoS ガバナンス責任者、SoS プラットフォーム開発者その他 SoS ガバナンス責任者が指名する者によって構成されるガイドライン検討委員会（以下、「ガイドライン検討委員会」とする）によって遂行されるものとする。

## 10.2 通則

1） ガイドライン検討委員会の委員長は、原則として SoS ガバナンス責任者とする。

2） 本ガイドラインその他関連規定の見直しまたは改正（以下、「見直し等」という）にかかる議案は、ガイドライン検討委員会の構成員によって提出することができる。

3） 2)に掲げる議案の審議にあたっては、ガイドライン検討委員会の構成員によって遂行されるものとする。ただし、SoS ガバナンス責任者が認めるときは、ガイドライン検討委員会の構成員でない者も参加することができる。

4） 2)に掲げる議案の採決にあたっては、議案採決時に出席するガイドライン検討委員会の構成員全員の同意により行われるものとする。ただし、欠席した構成員の見解に関してガイドライン検討委員会の構成員全員の同意がある場合においては、これを採用することができるものとする。

5） 4)における採決において可決された案は、本ガイドラインに反映させ、これを公開するものとする。

6） ガイドライン検討委員会は、次節に掲げるインシデント等の発生時または実証実験・テストベッド運用後を除く場合において、2 ヵ月に 1 回の間隔でガイドラインの見直し等にかかる定例の委員会（以下、「定例会」とする）を開催するものとする。

7） 定例会の日程は、あらかじめ本学事業年度の初月において年次単位で決定するものとする。ただし、ガイドライン構成員全員の同意がある場合（ガイドライン委員会の構成員が定められた期限内に意思を表明しなかった場合は、同意があったものとみなす）においては、決定された任意の定例会を非開催とすることができる。

## 10.3 フィードバック・インシデント等発生後の見直し等にかかる特則

1） SoS ガバナンス責任者ないし SoS 提供者によって SoS の運用にかかるサービスの品質向上ないし unknown なリスクの発見のために得られた情報をもとに提言された新たな対応策や改善策が SoS 運用者らに共有された場合、ガイドライン検討委員会は本ガイドラインその他関連規定の見直し等にかかる委員会をすみやかに開催するものとする。

2） インシデント等（「8 インシデントへの対応」の各節に掲げるもの、および「9 有害事象への対応」に掲げる有害事象を指す。）発生後の事故調査報告その他の報告またはフィードバックを受けたガイドライン検討委員会は、本ガイドラインその他関連規定の見直し等にかかる委員会を遅滞なく開催するものとする。この場合、必要に応じてガイドライン検討委員会の構成員でない当該インシデントの関与者も、当委員会の審議に参加することができる。

3） 2）に掲げるインシデントのうち、ヒヤリハットに関する事項においては、相当期間内に本ガイドラインその他関連規定の見直し等にかかる委員会を遅滞なく開催することができるものとする。

## 10.4 実証実験・テストベッド運用後の見直し等にかかる特則

実証実験およびテストベッド運用後のフィードバックあるいはその報告を受けた場合その他必要と認められる場合は、ガイドライン検討委員会は、相当期間内に本ガイドラインその他関連規定の見直し等にかかる委員会を開催することができるものとする。ただし、SoS ガバナンス責任者が必要と認めた場合は、これを遅滞なく開催しなければならないものとする。

実証実験およびテストベッド運用後のフィードバックあるいは報告を受けたガイドライン検討委員会は、相当期間内に本ガイドラインその他関連規定の見直し等にかかる委員会を開催することができるものとする。ただし、SoS ガバナンス責任者が必要と認めた場合は、これを遅滞なく開催しなければならないものとする。

# 11 補論：提言など

本ガイドラインは、立命館大学の施設内で運用される SoS のテストベッドを学内外のステークホルダーが協力して安心・安全・快適に活用しながら、そこで得られた知見をもとに、学内における SoS の動作環境やガバナンスの質を向上させるだけでなく、社会全体の SoS 基盤整備にも貢献することを企図している。その実効性を高めるためには、SoS の運用を通じて生起した課題を踏まえ、学内の規程や運用ルールを適宜見直し、テストベッドの円滑な運用を支えるとともに、SoS の社会的普及をも視野に入れて、法制度（いわゆるハードロー）の整備や社会受容性の向上に向けた提言を継続的に行っていく必要がある。そこで本章では、SoS の運用を通じて蓄積される知見を学内規程等に反映させる際に考慮すべき視点を示すとともに、法制度の整備や社会受容性の向上にも資する継続的な取り組みと今後の検討課題を整理する。

## 11.2 学内規程等への反映

### 11.2.1 アジャイル・ガバナンスの理念を踏まえた学内規程の見直し方針

立命館大学の学内規程は、改廃を大学の方針決定を担う会議体が担い、大学代表者の統括のもとで運営されるなど、トップダウン型の要素が強い。特に、リスクマネジメント、情報セキュリティ、個人情報保護、防犯対策などの領域では、明確なルールが設定され、関係者は既存規程に基づいて行動することが求められる。一方で、各キャンパスや部局ごとに管理責任者が配置され、運用レベルでは一定の裁量を持って対応することが可能な仕組みも組み込まれている。

SoS（テストベッド）の運用を通じて得られる知見は、学内規程の実効性を向上させるうえで有益な示唆を提供する可能性がある。とくに、新しい技術や運用実績がもたらす課題の明確化、リスクマネジメントの精緻化、学内外のステークホルダーとの調整の在り方といった側面については、慎重な検討が求められる。こうした視点を踏まえ、以下の三点について、既存の規程の適用可能性や補完的な運用の在り方を検討する余地がある。

1） 不確実な状況下での柔軟な対応を可能にする規程の構造

SoS の運用では、新技術の実装や社会的受容性の変化に即応することが求められる。このため、状況変化に応じた調整がしやすい規程のあり方や、既存規程の枠組みの中で柔軟な運用を行うための工夫が考えられる。具体的には、リスクマネジメント規程や情報セキュリティ事故対応ガイドラインとの関係性について整理し、適切な連携を確保することが重要である。

2） 学内外ステークホルダーとの協調を促進するルールの整理

SoS の共同研究開発・実証実験には外部企業・研究者・行政などが関与するため、学内規程と

の整合性や運用面での調整が不可欠となる。既存の規程を活用しながら、協力関係を円滑に進めるための合意形成の手続や責任分担の明確化について、どのような整理が可能か検討することが望ましい。

3） 実証実験の結果を学内規程の運用に反映する仕組みの検討

ロボット・ドローンなど自律制御システムが複数連動する SoS 運用では、既存の情報セキュリティやリスクマネジメントの枠組みが想定していない事故類型やリスクが生じる可能性がある。こうした知見を学内で適切に活用し、リスク管理や事故対応の実効性を高める方策について、関連部局と共有しながら検討を進めることが有益である。

### 11.2.2 安全性・プライバシー保護等に関する既存ルールとの整合

本ガイドラインで示される安全性やプライバシー保護、インシデント・有害事象への対応方針は、学内の情報セキュリティ規程、個人情報保護規程、リスクマネジメント規程、防犯カメラ管理規程など、既存の規程類との整合を図ることが重要である。SoS（テストベッド）の運用では、複数のシステムや運用主体が連携するため、物理的被害とデジタル被害が複合的に発生するリスクも想定される。このような特性を踏まえ、既存規程の適用可能性や補完的な運用のあり方について検討することが求められる。

1） 安全管理上の考慮事項

SoS の実証実験では、ロボット・ドローンなどの自律制御技術による新たなリスクが想定される。既存の情報セキュリティ事故対応ガイドラインやリスクマネジメント規程との関係を整理し、安全管理の実効性を高める方策について議論を深めることが有益である。

2） プライバシー保護との整合性

SoS の運用において、学術研究目的でないデータ活用や機器の稼働ログ・映像記録の利用が想定される場合、既存の個人情報保護規程との関係を整理し、適切な取り扱いを確保することが望ましい。プライバシー保護の観点から、関係部局と協力しながら適用範囲や運用ルールの検討を進めることが重要である。

3） 複数規程・委員会間の調整の必要性

情報セキュリティ関連の関係部局との連携ルールを整理し、新たなリスクが確認された場合に迅速な対応ができる仕組みを整備することが有益である。

### 11.2.3　　ガイドライン運用結果のフィードバックと規程整備の継続的検討

本ガイドラインは、インシデント発生時の事後検証やテストベッド運用後の見直しなど、継続的なフィードバックの仕組みを重視している。このプロセスで得られた知見を、学内規程の運用に適切に活用し、未知のリスクや新たな技術進展にも対応できるようにするための検討が求められる。

1）インシデント情報の共有と分析

「Digital 事故」などの新概念を適切に扱うための補償体制や運用フローについては、関係部局と議論を深め、学内での活用可能性を探ることが有益である。

2）フィードバック・ループの確立

SoS 運用で得られた知見（安全性向上策、プライバシー保護対策など）を、学内規程の運用改善に活かすための情報共有の仕組みを確立することが望ましい。

## 11.3 ハードロー（法令等）への反映に向けた提言

学内規程の改訂だけでは対応できない課題の中には、国や地方公共団体と連携しながら検討を進める必要があるものも含まれる。ここでは、SoS（テストベッド）の運用から得られる知見をもとに、今後の制度設計や社会実装に向けた考え方を整理する。

### 11.3.1　　リスク管理と補償制度の検討

AI 搭載ロボットやドローンなどが関与する「Digital 事故」「Digital インシデント」の概念整理と、それに対応するリスク管理の枠組みが求められる。具体的には、デジタル事故の報告義務の在り方や、事故データの収集・分析の仕組みを整備することにより、原因究明と再発防止に資する体制の構築が期待される。予測困難なリスクに対処するため、補償・賠償責任の在り方についても、制度設計の検討が必要である。また、事故発生時の迅速な情報開示を促進するためには、情報提供者に対する訴追免除や減免措置の導入可能性についても議論が求められる。

### 11.3.2　　制度設計・社会実装

SoS の普及と制度化に向けては、技術標準化や社会受容性の向上が不可欠である。SoS プラットフォームの評価基準を整備し、国内外の標準化団体との相互承認や認証スキームの形成を進めることが、広範な技術基盤の確立に資する。SoS の試験結果を社会の制度設計や運用基準の策定

に活かすこともまた、技術実証と社会実装のギャップを埋めるとともに、安全性・信頼性の向上に寄与という観点から期待される。加えて、大学が公的機関の認定制度（例：公益デジタルプラットフォーム認定）とどのように連携できるかを議論し、SoS の社会実装を促進するための制度設計に貢献することも期待される。

## 11.4 今後の検討事項

SoS（テストベッド）の運用を通じて得られる知見を、学内規程の適用状況の検証や社会実装の議論に活かしていくため、今後も以下の課題に取り組む。

- 「Digital 事故・インシデント」関連の新ルール が円滑に適用されているかを、学内の関連部局や関連委員会と連携し、定期的に検証して必要に応じた調整を行う。
- インシデント対処や補償制度運用の実績を整理し、産官学の各種フォーラムで知見を共有するなど、ハードロー整備や社会受容性向上に向けた議論を深める。
- AI・ロボット技術の進展に伴い、学内外の規程や法制度の見直しが求められる場面に適応できる仕組みを検討する。
- Unknown-Unknowns の判定基準、社会受容性評価、SoS トラストワースネス（安全性・セキュリティ・プライバシー保護）のアセスメント手法など、継続的な更新プロセスを設計する。
- 公益デジタルプラットフォーム認定などの制度を活用し、SoS の運用実績をモデルケースとして提示し、学外の関係者と協力しながら、制度的インセンティブのあり方についても議論を進める。

# 12 参考文献

本ガイドラインは、「SYSTEM OF SYSTEMS 運用ガイドライン：汎用版」をもとに作成したものである。そのほか、本ガイドラインの作成に際して、以下の文献を参考とした。

**【府省庁ガイドライン等】**

**<内閣府>**

- **Society 5.0**
  https://www8.cao.go.jp/cstp/society5_0/
- **AI 戦略**
  https://www8.cao.go.jp/cstp/ai/index.html

**<経済産業省>**

- **Society5.0 における新たなガバナンスモデル検討会**
  https://www.meti.go.jp/shingikai/mono_info_service/governance_model_kento/index.html
- **アジャイル・ガバナンス関係：GOVERNANCE INNOVATION Ver.3**
  https://www.meti.go.jp/shingikai/mono_info_service/governance_model_kento/20220808_report.html
- **技術情報管理認証制度**
  https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/

**<厚生労働省>**

- **機能安全テキスト、ボイラー登録制度：機能安全による機械等の安全確保について**
  https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000140176.html

**<総務省・経済産業省>**

- **AI 事業者ガイドライン**
  https://www.soumu.go.jp/main_sosiki/kenkyu/ai_network/02ryutsu20_04000019.html
  https://www.meti.go.jp/press/2024/04/20240419004/20240419004.html

**<デジタル庁>**

- **資料アーカイブ**
  https://www.digital.go.jp/resources

- **デジタル社会推進標準ガイドライン**

  https://www.digital.go.jp/resources/standard_guidelines

**＜個人情報保護委員会＞**

- **法令・ガイドライン等**

  https://www.ppc.go.jp/personalinfo/legal/

**【情報処理推進機構（IPA）の出版物・ガイドライン】**

- **書籍・刊行物**

  https://www.ipa.go.jp/publish/index.html
- **公益デジタルプラットフォーム認定制度**

  https://www.ipa.go.jp/digital/dx/dpf-nintei.html
- **ウラノス・エコシステム・データスペーシズ リファレンスアーキテクチャモデル ホワイトペーパー**

  https://www.ipa.go.jp/digital/architecture/reports/ouranos-ecosystem-dataspaces-ram-white-paper.html

**【ロボット革命・産業 IoT イニシアティブ】**

- **オンラインライブラリー**

  https://www.jmfrri.gr.jp/onlinelibrary/item/

**【DEOS プロジェクト（JST）・DEOS 協会】**

- **DEOS：変化しつづけるシステムのためのディペンダビリティ工学（近代科学社）**

  https://www.kindaikagaku.co.jp/book_list/detail/9784764904613/
- **Open Systems Dependability: Dependability Engineering for Ever-Changing Systems (CRC Press)**
- **Open Systems Dependability: Dependability Engineering for Ever-Changing Systems, Second Edition (CRC Press)**

  https://www.routledge.com/Open-Systems-Dependability-Dependability-Engineering-for-Ever-Changing/Tokoro/p/book/9781498736282
- **DEOS 協会**

  http://deos.or.jp/index-j.html

**【国際規格】**

**＜ロボット関係（ISO TC299）＞**

- **ISO 10218-1, ISO 10218-2, ISO 11161**（産業用ロボット、ロボットシステム、統合システム規格）
- **ISO 13482**（サービスロボット規格）
- **ISO 31101（JIS Y1001）**（サービスロボットのサービス提供者向けマネジメントシステム規格）
- **シンガポール国家規格：SS TR108**（病院向けサービスロボット統合システム規格）

**＜ドローン関係（ISO TC20 SC16, SC17 など）＞**

- **JIS Y1011**（ドローンサービス提供者向けマネジメントシステム規格）

**＜システム・SoS 関係＞**

- **オープンシステム・ディペンダビリティ**（IEC 62853, DEOS プロジェクトの成果）
- **システムアーキテクチャ**（ISO/IEC/IEEE 42010）
- **ライフサイクルマネジメント**（ISO/IEC/IEEE 15288）
- **SoS 関連規格**
    - **ISO/IEC/IEEE 21839**（SoS のライフサイクル段階における考慮事項）
    - **ISO/IEC/IEEE 21840**（ISO/IEC/IEEE 15288 の SoS 工学への適用ガイドライン）
    - **ISO/IEC/IEEE 21841**（SoS の分類）

**＜ソフトウェア・データ・AI 関係＞**

- **ソフトウェア**（ISO/IEC 25000 シリーズ, ISO/IEC 12207）
- **データ関係**（ISO 8000 シリーズ, ISO/IEC 5259 シリーズ）
- **AI 関係（ISO/IEC JTC1 SC42）**（ISO/IEC 42001, ISO/IEC 22989, ISO/IEC 38507, ISO/IEC 5338 など）

**＜安全性・セキュリティ・プライバシー＞**

- **安全性**（ISO 12100, ISO 13894-1, -2, IEC 61508, IEC 62061）
- **セキュリティ**（IEC 62443 シリーズ, IEC 15408, ISO/IEC 27000 シリーズ）
- **プライバシー**（ISO/IEC 27701）
- **システム・ソフトウェア保証**（SO/IEC/IEEE 15026-1:2019 (JIS X 0134-1:2021), ISO/IEC/IEEE 15026-2:2022 (JIS X 0134-2:2024), ISO/IEC/IEEE 15026-3:2023, ISO/IEC/IEEE 15026-4:2021（JIS X 0134-4:2024））