プロジェクト実践報告

System of Systems（SoS）運用ガイドライン：汎用版

髙村博紀[1)]，山本寛[2)]，稲葉光行[3)]，山田希[4)]，大場光太郎[5)]，日原拓哉[6)]，後藤智[7)]，冨山宏之[8)]，荒川明夫[9)]，上原哲太郎[10)]，羽深宏樹[11)]，髙橋圭[12)]，久米達也[13)]，徳田昭雄[14)]

要　旨

本研究は，立命館大学が受託した NEDO 補助事業「2022 年度～ 2024 年度 産業 DX のためのデジタルインフラ整備事業：複雑なシステム連携時に安全性及び信頼性を確保する仕組みに関する研究開発／ SoS 時代のシステムの安全性・信頼性とイノベーションの両立に向けたデジタルインフラ整備及びガバナンスのあり方に係わる研究開発」の成果のうち，System of Systems（SoS）の枠組みに基づくサービスの円滑な社会実装に向けて安全性，倫理性，制度的妥当性を備えた「SoS 運用ガイドライン」を纏めたものである。立命館大学では，リビングラボを中心とする実証環境を活かし，具体的かつ実践的なガイドラインを自主的に作成し，実証・改訂を重ねる中で，社会に開かれた運用モデルの構築を試みた。加えて，AI 事業者ガイドラインや公益デジタルプラットフォーム運営事業者認定制度といった外部制度とも連携し，それらとの整合性を自らの手で確認しながら，実効性あるガイドラインの作成に努めてきた。さらに，策定したガイドラインを関係者が確実に理解・運用できるよう，学習コンテンツの設計・作成・公開を積極的に進め，教育的支援の仕組みもあわせて構築している。

キーワード：System of Systems（SoS），デジタル・トランスフォーメーション，アジャイル・ガバナンス，マルチ・ステークホルダ，社会受容性，Value Structuring Notation（VSN）

1）一般財団法人日本品質保証機構　副参事，2）立命館大学情報理工学部　教授，3）立命館大学政策科学部　教授，4）立命館大学法学部　教授，5）立命館大学 OIC 総合研究機構　教授，6）大阪大学社会技術共創研究センター総合研究部門　特任助教（常勤），7）立命館大学経営学部　教授，8）立命館大学理工学部　教授，9）プライマルカラーズ合同会社　代表，10）立命館大学情報理工学部　教授，11）スマートガバナンス株式会社代表取締役 CEO，12）Kollect 京都法律事務所　弁護士，13）立命館大学財務部契約課　課長，14）立命館大学経営学部　教授

本稿（本ガイドライン）の目的・概要

は じ め に

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））[1)] 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。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予め想定した上で，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在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」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，それどころか事後的にも原因の特定が困難なことが多いため，結果回避義務を事前に決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（事後的に）結果回避義務を決めるアプローチを採れば，インシデントの原因に関与している関係者は罰則や責任をおそれて情報を積極的に開示しないがゆえに，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（『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。

本稿（以下，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 OIC（大阪いばらきキャンパス）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ールドで共時的に生成するための，2 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する。
③ ②の場合は更に（ア）と（イ）に分類される。

（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）三条委員会設置など国による前提全体条件が整わないと実行できないもの（訴追延期合意，損害賠償免責，公的保証）に分けて，特に（イ）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。

第 1 部　システム・オブ・システム（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である。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。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である。

システム・オブ・システム（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

注：システム要素は，システム・オブ・システム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

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。

SoS の性質

SoS の性質としては代表的なものとして①独立性，②自律性，③協働性，④複雑性，⑤創発性，⑥拡張性・縮小性があげられる。特に⑤創発性が Unknown-Unknows を産み出す原因になりうる。そのため，いかに④複雑なものを，①独立，②自律している部分がどこなのか明確にして，③協働させることにより，いい意味での想定外：想像以上に役に立つ，一見すると④複雑で⑥サービスの拡張や変更など柔軟に変化しどのように扱えばいいかわからないシステムとステークホルダが相互作用していけばいいのか，SoS についてルールをステークホルダ間で合

意しながら運用をすることが重要となる。

① 独立性（Independence）

SoS は，それぞれが完全な機能を持つシステム（要素システム）の集まりである。各要素システムは，互いに独立して存在し，他の要素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，他の要素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 を構成する各要素システムは，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，複数の要素システムが連携して，個々の要素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。各要素システムは，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）を他の要素システムと共有し，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，目標を持つ要素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。例えば，各要素システムは，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も直面する。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。各要素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，統合された各要素システムが相互に作用することにより，個々の要素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，又は縮小することができる。新しい要素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，要素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。

SoS の分類については 4 種：①指揮された SoS，②認められた SoS，③協調的な SoS，④仮想的な SoS と国際規格 ISO/IEC/IEEE 21839 で分類されている。

① 指揮された SoS

特定の目的を達成するために創出および管理された SoS であって，構成システムがその SoS に従うもの。構成システムは独立して稼働し，運用操作が可能な能力を保持する。しかしながら，通常の運用モードは一元的に管理された目的に従う。

② 認められた SoS

認識された目的，指定された管理者，および SoS の資源のある SoS。

構成システムは，それぞれに独立した所有権，目標，資金，開発および持続の取組み方を維持する。構成システムの変更は，SoS と構成システムとの間の協力的な合意に基づいている。

③ 協調的な SoS

合意済みの一元的な目的を達成するために，コンポーネントである構成システムが多かれ少なかれ自発的に相互作用する SoS。

構成システムは，サービスを提供または拒否する方法をまとめて決定し，それによって一貫性を強化および保守する手段を提供する。

④ 仮想的な SoS

一元的に管理する権限を欠き，一元的に合意した目的を持たない SoS。

大規模で広範的に創発的な振る舞いが発生すると（それは望ましいこともあるが），この種の SoS は他の種類の SoS と比べて見えにくいメカニズムに頼って SoS を維持する。通常，自己組織化している SoS のこと。

本ガイドラインは，前提として SoS を構成するシステムは自律・分散としているが，そのガバナンスの主体が明確となりうる（上記④以外の）場合について，ガバナンス責任者がおり，各構成システムとの関係性をどのように明確化しながら全体最適へと導くためのガイダンスを提供する。

SoS の形態としては①分散型，②集合型，③目的型，④進化型と区分されることがある。

① 分散型（Distributed）

各要素システムが高い独立性と自律性を持ち，中央集権的な管理や統制が最小限であるか，全く存在しない。各要素システムはそれぞれの目標に従って動作し，同時に全体としての目標達成に貢献する。この形態は，柔軟性が高く，変化に対して迅速に対応できるが，統合や協調動作の確保には特別な戦略や技術が必要となる。

② 集合型（Federated）

要素システムがより統一された目標のもとに集まり，中央集権的又は分権的な管理下で協調して動作する。特定の目標達成やプロジェクトの実行に適しており，効率的な資源配分や統一された方針の下での運用が可能である。

③　目的型（Directed）

特定の任務や目標を達成するために意図的に設計されたシステムの集合体である。強い統制構造のもとで運用され，各要素システムは全体の目標に貢献するために特定の役割を果たす。効果的な成果達成に向けた明確な計画と管理が特徴である。

④　進化型（Evolutionary）

時間とともに進化し，発展するシステムの集合体である。新しい技術や要求の出現に対応して徐々に拡張または改良される。長期的な持続可能性や発展性を視野に入れて，システムの進化や変化に柔軟にかつ迅速に対応できるよう，予測と準備を行う必要がある。

上記形態は，特定の状況や目標に応じて選択され，SoS の設計と管理において考慮されるべき重要な要素である。SoS の運用に当たっては，各形態の特性を踏まえ，その特性を活かした運用戦略を立案することが求められる。さらに，SoS ガバナンスを実行するうえで対象となる SoS がどのような形態となっているかについて分析するとともに，その形態が時間とともに変化することも考慮したガバナンスの仕組みを出来うる限り柔軟に設計する必要があり，変化に応じてガバナンスの在り方についても修正・変更していくような取組みこそが，SoS ガバナンスにおいて重要であることをステークホルダが理解し，そのうえで実行することが不可欠である。

SoS と複雑システムとの違いについて

SoS の場合，構成システムが複雑システムである場合をも考慮しなければならないことからも SoS が単なる複雑システムではないことを示しているが，さらに SoS に属している構成システムは基本的に自律分散型システムであり，システムオーナが異なるため SoS 全体システムとしては中央制御といった方式がとれないマルチオーナー，マルチステークホルダによる関与が避けられない点は SoS と複雑システムの差異として顕著なものである。またシステム間の連携に関しても濃淡があり，個々のシステムにより構成されるネットワーク構造がどうなっているのか，ネットワーク構造自体も変化する可能性がある。

SoS では，（統制が取れている）複雑なシステムを超えて，複雑システム間の関係，それもシステムとシステムで連携具合に濃淡があるばかりでなく，濃淡自体も時々刻々と変化するような形態をとり，全体システムの全容把握がそもそも困難である。また，SoS に属するシステムのライフサイクルは異なり，各システムにはインテグレータや運用者が存在する。それらの活動は一般的には自立，独立，自律している。SoS はタイプに分類されていたりはしているものの，原則的には複数の独立・自立・自律したシステムの連合体の総称であり，SoS といっても，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。そのため各シ

ステムから提供されるデータに関しても，一元的に収集して，すべてのシステムを制御するために必要なデータが完全に一元管理されることを想定して SoS をマネジメント・ガバナンスすることは現実的ではなく，むしろ，各システムでデータの形式も異なることを前提とすべきである。唯一，コミュニケーションするシステム間においては共通のプロトコルがあるだけと認識すべきであり，このような多種多様なシステムから，どのような情報がマネジメント・ガバナンスにおいて必要であり，その情報に基づいて判断することで，全体システムとしてマネジメント・ガバナンスするかが重要である。

ここで，マネジメントとガバナンスについて一言ふれておくと，SoS を構成するシステムにおいては，構成システムを管轄する組織が出来るだけマネジメントにより統制をとることが望まれる。SoS レベルでは構成システムが SoS との関係において濃淡があることからも，より高次なレベルで柔軟かつ包括的な対応，対策を内包した運用（運行）が重要となるため，本ガイドラインでは SoS マネジメントとはせずに，SoS ガバナンスとしている。

複雑システムとの類似点・留意点

複雑なシステムでも生じることではあることからも，構成システムにおいても考慮すべき事項として，システムはそれを構成する要素の単純な総和として理解することが出来ない。つまり，要素還元主義的にシステムの構成要素に分解をすすめるよう分析をし，構成要素の機能，構造，振舞いを理解したうえで，逆方向に単純に融合を試み結合しても，タイミングなど構成要素間の関係性をも含めて包括的，総合的に，かつ，網羅的に全体像をとらまえることが困難であることを意味している。それは創発という一言で説明される場合もあるが，システムを考えるうえで不可欠な本質的な事項である。しかし，複雑なシステムを分解，分析することなく理解すること／しようとすることもまた困難である。

また，完全なシステムを構築することは，SoS においても，複雑システムにおいても現実的には不可能であり，障害は発生するものであるという前提のもとでシステムを運用することが必要である。したがって，各システムに対して，ちゃんと機能し，障害が発生した場合の対応についても手順を定めておく必要があり，それをどこまでシステム化するか，つまりシステムを自動的にモニタリングして障害を検知して障害対応する仕組みをどうシステムに構築するか，また，障害が発生しているとユーザなどからの通報に対して，どのように対応するか，といった各種レベルから得られる障害に係る通報への対応をルール化しておくことが不可欠となる。

Cyber Physical Systems（CPS）としての SoS について：シミュレータの役割と重要性について

SoS を構築・運用するにあたり，シミュレーション技術の利活用は有用である。SoS の構想から廃棄にいたるライフサイクル全体においてシミュレータの役割を明確にするとともに，サイバー空間と物理空間を円滑に行き来できるような，双方向的な関係性を構築・維持するための仕組みを支える基盤としてシミュレーション技術をとらえることが SoS をガバナンスする

において不可欠であると考える。そもそも SoS においては下記にあげる不確定性が存在している。

✓ 全体像がはじめから明確になっていない。
全体観をえるために，抽象化してシミュレータを利用して全体システムの振舞い，人，モノ，データの流れの把握に利用する。

✓ 段階的に機能が追加される。
機能追加による既存システム，サービスへの影響を分析するため，まずはシミュレータを用いて影響分析し，追加する機能について分析，検討するための情報を提供する。

✓ 変化にともなう SoS の構成システムの改修，特にソフトウェアの更新等が各構成システムのライフサイクルマネジメントのサイクルが異なる。
そのため，各構成システムの改修が全体システムにどのような影響があるかについて，構成システムレベルではわからないため，シミュレーション技術等ももちいて，改修による全体システム（SoS レベル）での影響についてあらかじめ分析をしておくことで安定した運用が維持される。

SoS を理解するために留意すべきこと

全体システムと部分システムの総和の間に生じる Gap について考察し，それをどのようにガバナンスするか，また，ガバナンスにより全体システムの把握へとつなげていくことが出来るのかが，課題の解決へ道筋である。課題に対して明確な回答があるわけではなく，解決に向けてはベストエフォートで実施するよりない，難題である。変化し続け，完成形が明確でもない，この種の課題への取組みではアジャイル・ガバナンスが有効であると考える。SoS を構成するシステム，システムを開発，運用，保守する関係者に対して，ルールを定め／実行し／モニターをし，課題を抽出しカイゼンするというサイクルを回しながら実際にアジャイル・ガバナンスを実行することが上記 Gap を埋め，Unknown-Unknows を出来うる限り減らすために必須であり，これにより SoS における安全・安心・快適を実現する。SoS バナンスの仕組みをどう構築するかが重要となる。

全体システム，サービスに関しての責任主体，運用主体，データ管理主体を明確にして，各役割に課せられる責任を明示する必要がある。また，全体システムを構成する各システムにおいても，個々のシステムに対して責任主体，運用主体，データ管理主体などを明確にし，それぞれの役割と責任について明示する必要がある。つまり，SoS の構成がどうなっているか明らかにすることと並行して，SoS の構成要素である各システムに関わる組織についても，組織間の関係性を含めて組織構成を明確化しなければならない。さらに，各階層における手順，取決めから発生する様々な事象を上の階層で吸収・処理できるような機構をシステム自体にも，それをマネジメント・ガバナンスする組織に対しても所持させる必要がある。各システムにおける運用を含めたマネジメント・ガバナンスに対して，どのように関係をつけて，全体システム

としてサービスを Trustworthy（ISO/IEC TR24028:2020 における“Trustworthiness”の定義は“ability to meet stakeholders’ expectations in a verifiable way”である。本ガイドラインでは，最低限，安全性，セキュリティ，プライバシー保護がなされていることを Trustworthy であるとして話を進めるが，これら 3 つの属性に限定されるものではない）に提供し続けることが出来る仕組みを体制，統制規則，エスカレーションルールを含めて，指揮系統の明確化，各担当における役割と責任の付与，全体システム，サービスに対しての合意と説明責任の遂行について構築する必要がある。

変化が発生したときの対応についても，緊急対応である障害対応，内外の変化への対応といった 2 観点からプロセスを定義し，Unknown-Unknowns をどのようにして減らしていくか，全体システムにおいて，システム境界，サービス境界，内部，外部さらに，それらの連携についてモニタリングやコミュニケーションを通じて方策を講じ続けなければならない。このモニタリングやコミュニケーションには，ステークホルダからのリクエスト，苦情，ヒヤリハット情報，環境，法律，技術，サービス提供で使用する外部リソースの変化などが含まれる。また，障害への対応においては，タイムラグ問題への対応をあらかじめ考えておく必要があるとともに，各自の判断におけるアクション，例えば，緊急停止ボタンの押下といった自らの判断で行うこと・自主的判断に基づく避難など，していいこと，してもいいこと，してはいけないことについても柔軟にルール化しておく必要がある。構成システムに対しては，Safety Of The Intended Functionality（SOTIF: 意図した機能の安全性）などシステムの設計限界，性能限界を考慮した設計をすること，また，協調安全といった人・環境・システムの関係性にも配慮した安全設計を考慮するなども必要である。

社会システムを分析するためのツールとしての SoS について

SoS について説明してきたが，なんだかよくわからない複雑怪奇なものととらえられてしまったら，大変残念である。むしろ，身の回りにある社会システムこそが SoS を形成しているととらえ，社会システムを分析するために利用し，そのうえでガバナンスやマネジメントをどうするかといった観点で考えるべきである。

社会システムを Quituple Helix として捉え，Open Innovation を起こそうとする欧州の動きを鑑みつつ，社会システムの構成要素を，組織（人）と人工物を対象として，自然の持続可能性への考慮についても当然考慮しなければならない。このような社会システムにおいては，多くの組織やコミュニティに属する人の間での合意形成プロセスが非常に大事であり，人工物を設計した組織（人）の意図や解釈をいかに正確に伝え，それらの多様で複雑なシステムや組織（人）で共創した新たな社会システムを実現し，安全かつ経済効果を有し，持続可能な運用体制を組めるかがアジャイル・ガバナンスに求められることである。そのためには，What や How だけではなく，設計者の意図にかかわる Why の部分の明確な言語化と合意形成が必要不可欠となる。

第 2 部　SoS ガバナンスにより目指す社会と全てのステークホルダが連携して取組む事項

社会システムを SoS ととらえ，分析すること，特にそのガバナンスをどうすべきか検討することは，より良い社会の実現の一方策を提供すると考えられる。つまり，社会的共通資本（社会インフラストラクチャー）として SoS をとらえることにより，SoS のあるべき姿について検討を進めること。

そのためには SoS においては，それを構成する，基本的に自律・分散で運用される構成システムをどのように全体最適に向けてガバナンスするかについて，各ステークホルダが連携していくことが不可欠であることからも，様々なレベルにおいてシステムとそれを運用する組織のマネジメントおよびガバナンスについてレベルを越えた連携についてもどうあるべきか検討することが必要となる。

SoS の分類と概要については，前述したが，国際規格 ISO/IEC/IEEE 21839 における分類，①指揮された SoS，②認められた SoS，③協調的な SoS，④仮想的な SoS とされているが，ガバナンスが十分に機能するには，①もしくは②である必要があり，③の場合では，後述の SoS プラットフォームが一般的なインターネットなどのインフラとなる可能性があり，SoS に係るガバナンスが複雑になる可能性がある。さらに④のように各構成システムが完全に独立・自律・分散している場合は，各構成システムのガバナンスをどのように連携させて SoS に係るガバナンスとして昇華，確立できるのかについて，構成システム間，ステークホルダ間のコミュニケーションを含めた，より高次で包括的な仕組みが必要になると考えられる。

ステークホルダについて

SoS ガバナンスにおけるステークホルダについて，SoS の形態に等に応じていろいろ考えることが出来るが，本ガイドラインにおいては以下のように定める。

また，SoS サービスとは，SoS を用いて提供されるサービスの総称である。（SoS 提供者が提供する）SoS を活用してサービス提供者が提供するサービスを指すことが多いが，これだけない場合があり，SoS プラットフォームが提供するインフラストラクチャー的サービス，SoS 提供者が提供する使用環境から得られる事項などが含まれることがある。

表 1

ステークホルダ	役割
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 SoS プラットフォーマや SoS 提供者と密に連携しながら SoS および構築された SoS を活用したサービスに関するガバナンスの責任者 ただし，SoS を構成する各システムの自律性，分散性などの性質により SoS ガバナンス責任者がどこまで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 プラットフォーマ	構成システムを SoS プラットフォームに接続しデータ連携する場合などにおけるインフラ整備の開発主体 SoS プラットフォームの構築がメインとなるが，構成システムを組合せ，インテグレーションするなどの IT システムとしての SoS における開発全判を担うこともある
SoS 提供者	SoS プラットフォーマが開発・構築した IT システムとしての SoS を施設・設備など使用環境も含めて提供する主体 サービス提供者の要求を汲み，アプリケーションの作成協力など含めて SoS の提供を行う（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 プラットフォーマ，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）
サービス提供者	SoS 提供者が提供する SoS を活用して，実際にビジネスとしてサービスを実施する主体。提供するサービスに対する主たる責任者となるが，必ずしもサービスに係るサービス（アプリケーション含む）を開発するとは限らない
サービス受益者	サービス提供者が提供するビジネスにより受益する者
潜在的サービス受益者	直接は SoS と相互作用や SoS を活用したサービスを利用はしないが，使用環境に（物理的に）存在している者

表 1，ステークホルダの分類は一般的なケースから導出されたものであり，対象となる SoS および，その関係者においては役割の重複やさらなる細分化が発生することは自然なことであり，状況に応じた役割分担・責任分界点の明示化（その時間における変化も考慮した）が重要である。また，SoS ガバナンス責任者，SoS プラットフォーマ，SoS 提供者の 3 組織は SoS レベルを，サービス提供者，サービス受益者，潜在的サービス受益者は，システムレベルでの事項であると考えると整理がしやすいかもしれない。

SoS ガバナンスとは

SoS ガバナンスの必要性について

AI 事業者ガイドラインにおいてもガバナンスの重要性については記載されているが，AI システムを包含する SoS においてもガバナンスこそが重要な事項であり，その基本方針は SoS においても同様であるとの理解のもと，SoS の文脈に読み替えたうえで AI 事業者ガイドラインに記載されている基本方針に則り，SoS ガバナンスの必要性について言及する。

「ステークホルダからの期待を鑑みつつどのような社会を目指すのか（基本理念 = why）」をステークホルダ間の合意に基づき，「SoS および提供されるサービスに関しどのような取組を行うべきか（指針 = What）」を明らかにすることが重要であり，また指針を実現するために，「具体的にどのようなアプローチで取り組むか（実践 = How）」を検討・決定し，実践すること

が SoS の安全・安心な活用に有用であり，不具合が発生した場合に対して緊急対応ができ，内外含めた変化に対しても迅速な対応がとれる，つまり変化に柔軟に対応・適応でき，かつ，説明責任を遂行できることが Trustworthiness の確立に重要となる。

実際の SoS サービスは目的・活用技術・データ・利用環境等によって多様なユースケースが存在する。また，技術の発展等，内部・外部の環境の変化も踏まえつつ，SoS プラットフォーマ，SoS 提供者，サービス提供者が連携して最適なアプローチを検討することが重要であり，常に変化を認識するとともに変化に対して柔軟に適応できるように考え続ける姿勢が重要である（Best Effort と継続的改善）。また，最終的な責任者である SoS ガバナンス責任者の積極的な全体最適化に向けた関与が SoS ガバナンスにおいて極めて重要な事項である。

基本理念

人間中心の社会：Dignity

SoS が，AI システムを含む高度な先進技術に基づき構築された構成システムからなるものであっても，その目的は人間社会をより安全・安心・快適にすることから逸脱することがないようにしなければならない。

多様性を受容できる社会：Diversity & Inclusion

SoS が，高度な先進技術に基づき構築されているとしても，一部の考えに基づいた画一的なモノとならないよう，多様な考え，意見を反映，需要する人間社会のために役立つものでなければならない。

持続可能な社会：Sustainability

SoS が高度な先進技術に基づき構築されているとしても，その運用に必要となるエネルギー等についても考慮する必要があり，持続可能な人間社会を形成するために役立たなければならない。

原則

各ステークホルダは基本的理念に基づき，人間中心の考え方を基軸として SoS ガバナンスを促進することで，SoS サービスの開発・提供・利用を推進し，社会課題の解決等にむけ，SoS および SoS サービスの目的を実現するように努めることが重要である。

このため各主体は SoS 活用にともなう社会的リスクを許容可能な範囲にまで低減を図るべく，安全・安心・快適といった価値を創造・確保することが重要である。

それには，個人情報などプライバシー保護，SoS の脆弱性等による可用性（Availability）の低下や攻撃等のリスクに対してセキュリティを確保するなど，継続したマネジメントおよびガバナンスが必要となる。

これらを実現するためには，各主体はシステムの検証と妥当性確認（V&V: Verification & Validation）の可能性を担保しつつ，ステークホルダに対して適切な情報を提供し透明性を向上するとともに，説明責任の遂行が重要である。そのためにはステークホルダ間での合意形成を明確にするなど追跡可能性の確保も必要となる。

加えて SoS がもつアーキテクチャの多様化・複雑性にともなうサプライチェーン・バリューチェーンの変化等により，各主体の役割・責任範囲が返答する可能性も考慮したうえで，各主体間の連携，サプライチェーン・バリューチェーン全体での最適化に努めることが重要である。

全てのステークホルダに共通の指針

① 人間中心：Human centric SoS
- ◇ 人間の尊厳と個人の自律。
- ◇ 各システムの自律分散，必要なときに連携できるための相互運用性の確保。
- ◇ ステークホルダ間の意思決定と合意形成：SoS ガバナンス管理者が，対話などを通しての合意形成の場を提供するとともに，合意形成にいたるプロセスを仕組みとして構築する。
- ◇ 多様性・包摂性の確保：公平性の確保＋ Digital 弱者や技術弱者への対策。

② 安全性：Safe SoS
- ◇ 生命・身体・財産・環境への配慮。
- ◇ ヒヤリハット情報や心配事，気付いた点等を声として集め，集めた声に対応する仕組み。
- ◇ 適正な利用と必要なリテラシー教育。

SoS サービスに対しては，サービス受益者は単なる受け手としてだけではなく，自分事として積極的に参加することが求められ，またサービス受益に係る相互作用を声としてフィードバックすることにより，サービス向上やイノベーション創出につながるような仕組みも，安全性を考慮しながら構築する必要がある。

③ プライバシー保護：SoS with Privacy protection
- ◇ 個人情報保護法等の関連法令の遵守。
- ◇ 各主体はプライバシーポリシーを定めること。

例えば，防犯カメラなどの情報を，事故分析に用いることができるなど柔軟かつプライバシー保護にも留意した運用方針の設定，ステークホルダ間合意の形成。

④ セキュリティ確保：Secure SoS
- ◇ SoS および SoS サービスに影響を及ぼすセキュリティ対策。
- ◇ 最新技術動向への留意，最新対策の適用。

⑤ 透明性：SoS with Transparency

◇ 検証と妥当性確認（V&V）の可能性の確保，第三者評価など。
◇ 関連するステークホルダへの情報共有，提供の仕組み。
◇ 合理的かつ誠実な対応，合理的予測可能な事態への対策。
◇ 関連するステークホルダへの説明可能性，解釈可能性の確保。

⑥ 説明責任 : SoS with Accountability
◇ 追跡可能性の確保共通の指針の対応状況の説明と情報共有の仕組み。
◇ 責任の明確化，責任分界点の明確化，関係者間の責任の分配ステークホルダへの具体的な対応記録，文書化。
➢ その Accessibility の確保合意形成プロセスとしての対話の重要性について理解すること（リスクコミュニケーションを含む包括的なコミュニケーション，それが可能となる場の提供を含む）。
◇ SoS を構築する技術は State of the Art であり，その運用は Best Effort により実施されていること。
◇ 責任分界点を明確にすることにより，リスクへの対応に対して抜け漏れがない（各ステークホルダの責任範囲を定めるのみならず，重複はあっても誰も対応できないような穴がない）ようにすること。
◇ 責任分界点は契約などにより明確化（明文化）すること。
◇ 契約などで明確化できない部分についても包括的に SoS ガバナンス責任者はとらえること不具合が発生した場合は迅速な対応とともに，原因究明を実施，再発防止がシステマティックに実現できるような仕組み（プロセス）の構築すること。
◇ 迅速な対応には，被害の拡大を防ぐこと，被害を受けた人への補償も含めること。

⑦ 教育・リテラシー : Evolutive SoS
◇ SoS にかかるリテラシー教育。
◇ Digital 対応のためのリスキリング・アップスキリング。
◇ ステークホルダへのフォローアップ
◇ 積極的に参加するような仕組み。
◇ 体験型の取組み：ハッカソンやアイデアソンなど。

⑧ 公平な競争確保 : SoS with Fairness
◇ 各主体は SoS を活用した新たなビジネス・サービスが創出されることにより，持続的な成長の維持と社会課題の解決等に努めることが期待される。
◇ そのためにも公正な競争環境の維持が重要となる。
◇ 新規参入が容易となる，参入障壁が低くなるような仕組み：プラットフォーム化，参入への標準的な手順の策定など。

⑨ イノベーション : Innovative SoS
◇ オープンイノベーションの推進。

◇ 相互接続・相互運用性の確保。
◇ 適切な情報提供。
◇ イベントなどにより，限定的に挑戦的かつステークホルダ参加型の取組みを実施し，それに基づき新たなサービスの創出など，イノベーション創出・価値創造につながるような仕組みづくり。

⑩ 持続可能性の確保 : Sustainable SoS
◇ グリーン対応。
◇ エネルギー対応。
◇ SX に向けた取り組み。
◇ SoS ライフサイクルマネジメントとして，SoS が技術の発展に呼応するように，ステークホルダのスキルやリテラシーも向上するように連動する仕組みの構築。
◇ 構築した仕組みがイノベーション創出へとつながるような仕掛け。
※なお，SoS サービスの提供に（高度な）AI システムが利活用される場合における事業者に共通の指針としては，AI 事業者ガイドラインを参考にした対策が強く望まれる。

SoS ガバナンスの構築：アジャイル・ガバナンスを基礎とした仕組み

各主体間で連携しバリューチェーン全体で「共通の指針」を実践し SoS および SoS サービスを安全・安心・快適に活用していくためには，SoS に関するリスクをステークホルダにとって受容可能な水準で管理しつつ，そこからもたらされる便益を最大化するための，SoS ガバナンスの構築が重要となる。

また，「Society 5.0」や「デジタル田園都市国家構想」を実現するためには，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（CPS）の社会実装を進めつつ，SoS および SoS サービスにおいてもその適切なガバナンスを構築することが不可欠である。後述するが SoS は社会システムをとらえる上で重要な役割を果たすと考えられ，その根幹にある CPS を基盤とする社会は，複雑で変化が速く，リスクの統制が困難であり，こうした社会の変化に応じて，SoS ガバナンスが目指すゴールも常に変化していく。そのため，事前にルールや手続が固定された SoS ガバナンスではなく，企業・法規制・インフラ・市場・社会規範といった様々なガバナンスシステムにおいて，「環境・リスク分析」「ゴール設定」「システムデザイン」「運用」「評価」といったサイクルを，マルチステークホルダで継続的かつ高速に回転させていく，「アジャイル・ガバナンス」の実践が有効であると考える。

アジャイル・ガバナンスを一言でいえば，変化に対する組織としての適切な対応のことである。変化は組織の内部・外部を問わず発生するものであり，その発生を検知するためのモニタリングの機構を組織として持つ必要がある。

SoSガバナンス：アジャイルガバナンスに基づいた実現

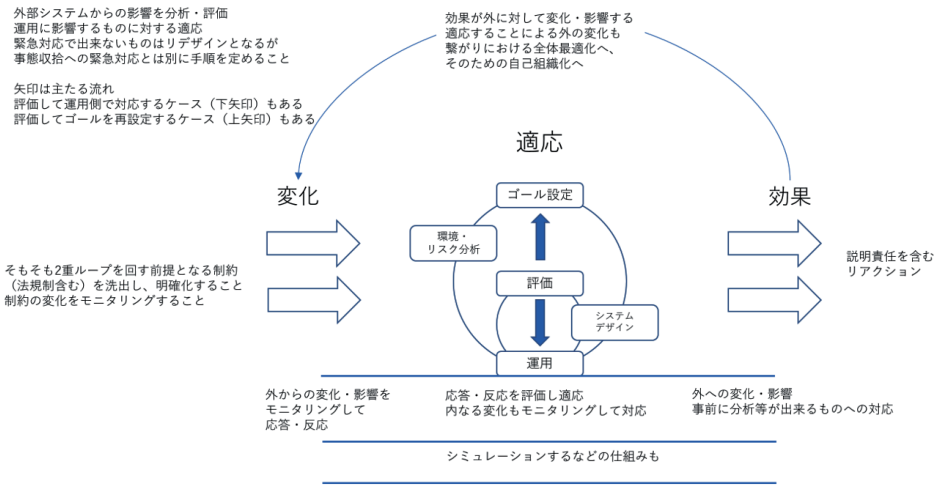


図 1

① SoS および SoS サービスがライフサイクル全体においてもたらしうる便益／リスクや開発・運用に関する社会的受容，「外部環境の変化」や SoS 習熟度等を踏まえ，対象となる SoS および SoS サービスに関連する「環境・リスク分析」を実施する。

（ア）アジャイル・ガバナンスの 2 重ループを回す前提となる制約（法規制含む）を洗出し，明確化すること。

（イ）制約の変化をモニタリングすること。

② ①を踏まえ，SoS および SoS サービスを開発・提供・利用するか否かを判断し，開発・提供・利用する場合には，SoS ガバナンスに関するポリシーの策定等を通じて「SoS ガバナンス・ゴールの設定」を検討する。なお，このゴールは，各主体の存在意義，理念・ビジョンといった経営上のゴールと整合したものとなるように設定する。

③ 更に，このゴールを達成するための「SoS ガバナンスの設計」を行った上で，これを「運用」する。その際には，各主体が，SoS ガバナンス・ゴールとその運用状況について外部の「ステークホルダに対する透明性，アカウンタビリティ（公平性等）」を果たすようにする。

（ア）外からの変化・影響をモニタリングして応答・反応すること。

（イ）外部システムからの影響を分析・評価。

（ウ）運用に影響するものに対する適応。

（エ）緊急対応で出来ないものはリデザインとなるが。

（オ）事態収拾への緊急対応とは別に手順を定めること。

④ その上で，リスクアセスメント等をはじめとして，SoS マネジメントシステムが有効に機能しているかを継続的にモニタリンし，「評価」および継続的改善を実施する。

（ア）応答・反応を評価し適応。
（イ）内なる変化もモニタリングして対応。
（ウ）外への変化・影響。
（エ）事前に分析等が出来るものへの対応。
（オ）説明責任を含むリアクション。

⑤ SoS および SoS サービスの運用開始後も，規制等の社会的制度の変更等の「外部環境の変化」をも踏まえ，再び「環境・リスク分析」を実施し，必要に応じてゴールを見直す。このなかでサービスの追加や変更，それにともないシステムデザインのリニューアルなど変化への適応をすること。

ここで注意が必要なのは，あくまでも図はイメージであり，矢印は主たる流れである。つまり，評価して運用側で対応するケース（下矢印）もあるし，評価してゴールを再設定するケース（上矢印）もある。また，SoS ガバナンスを実施していることによる効果が外に対して変化・影響することもあるため，適応することによる外の変化をも考慮したうえで，繋がりにおける全体最適化へ，そのための自己組織化へといった事項までをもガバナンスの範疇とすることが理想的である。つまり，全体最適に向けて

✓ バリューチェーン／リスクチチェーンの観点で主体間の連携を確保。
✓ データの流通をはじめとしたリスクチェーンの明確化と開発・提供・利用の各段階に適したリスク管理，SoS ガバナンス体制の構築を実施。

を行っていくことが重要である。これらを効果的な取組とするためには，SoS ガバナンスに対する責任者が，従来のリーダシップを越えた役割を担うことも重要であり，ファシリテータ役としてガバナンス主体としての役割を発揮することが重要である（必要があれば，これを Meta リーダシップ呼ぶ）。なお，その際は，短期的な利益の追求の観点からガバナンスを単なるコストと捉えるのではなく，各主体の持続的成長と中長期的な発展を志向した先行投資として捉えることが重要である。その Meta リーダシップの下，上記のサイクルを回しつつ，具体的に各組織の戦略や企業体制に SoS ガバナンスを落とし込んでいくことで，各組織の中で文化として根付かせることが重要となる。

SoS ガバナンスにおいては，関係するすべての事項について，ステークホルダの明確化と各ステークホルダがすべき事項について整理する必要がある。
SoS ガバナンスオーナはそれらを明確化するとともにルールを定め，SoS データ責任者や SoS サービス責任者など各ロールに対して何をさせ，自らも含めた責任分界点を定める必要がある。

また，各ロールにおいても，アジャイル・ガバナンスの考え方に基づき自らの担当分に関してマネジメントの仕組みを計画，実施する必要がある。つまり，各階層，各ロールにおいてアジャイル・ガバナンスの考え方に基づいたガバナンスが実施されるとともに階層間の関係をも

含む包括的なガバナンスの仕組みを，システムのライフサイクルが異なる SoS に対して適切に実施する計画，体制の構築が要求されることになる。つまり，アジャイル・ガバナンスを上図のようにとらえなおすとともの，各レベルにおいて各組織は 2 重ループを回すこと，それらが融合されたときに全体システムとして SoS ガバナンスとしてもまたアジャイル・ガバナンスが実現されていることが理想的なあるべき姿である。

契約と法的義務について

各ステークホルダは法令遵守，関係者との契約の締結とその遵守とともに，契約内容について，変化に応じて見直すこと

SoS の運用においては複数のステークホルダが関与しているため，これらのステークホルダについてルール（Rules）・役割（Roles）・責任（Responsibilities）の 3 つの R を定める必要がある。特に，役割と責任については契約により決定・調整される必要がある。また，各ステークホルダは自らの責任を全うするために補償を基礎としたガバナンスを実施する必要がある。

（以下，立命館大学版ガイドラインより転記・修正）

SoS は一元的に管理・統制されたシステムと比べて不確実性が高く，すべての事象（事故を含む）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 SoS における構成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。また，予期しない事象が発生した場合についても，その責任が追及できるかどうかも不確定な場合が生じる可能性を排除できない。そこで，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，被害者を救済することを推奨する。

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。事後検証の結果に基づく補償では，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[2)]。

第 3 部　各ステークホルダに関する事項

SoS ガバナンス実装の概要

SoS ガバナンスを実装するうえで重要なことは下図の赤枠を明確にすることである。

SoS運用ガイドラインに記載する事項　**赤枠**を明確にすること

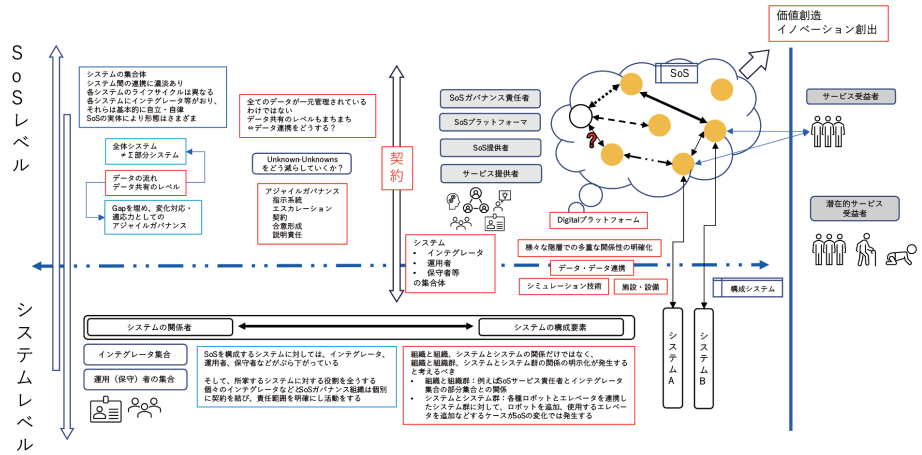


図 2

SoS のガバナンスにおいては，図 2 における赤枠に該当する部分を明確化していくことが重要である。また，一度明確化したから十分というわけではなく，変化に対してどのように対応・適応するかについても考えていかなければならない。特に Unknown-Unknowns をいかに減らして，安定したサービスを，安全・安心・快適に提供することを原則として，さらに，サービス受益者や潜在的サービス受益者からの声を集め，さらにカイゼンが進み，イノベーション創出や価値創造といったものをステークホルダ全体参加型で実現していく取組み自体が SoS ガバナンスにおいて考慮しなければならない要点であることを理解する必要がある。

（そのためには，不確定さや未知な事象，想定外も機会ととらえ，失敗を恐れずに挑戦する社会へと導くために SoS ガバナンスがあること，各人の個性に最大限の配慮をしつつ全員参加型で，より良い社会を形成するためのルールであることを周知する必要がある。）

ガバナンスやマネジメントと書くと，トップダウン型で与えられ，遵守すべき規制であると認識されがちであるが，SoS ガバナンスにおいては一方的に与えられ，守るためのルールではなく，ルールそのものに対しても参加者が作り，更新していくものであるとマインドセットをかえさせ，それが可能となるために，関係各所の声を集める仕組み，集めた声に対応する双方向型，ネットワーク型の相互作用と，循環構造を構築する必要もある。SoS サービスは魅力的なコンテンツを提供者のみならずサービス受益者も一緒になって作っていく取組みを確立することが SoS ガバナンスでは重要である。

そのためには，① SoS ガバナンス責任者，② SoS プラットフォーマ，③ SoS 提供者，④サービス提供者といった SoS にかかるガバナンス，システム（プラットフォーム），サービス等を提供する側のアクション（理屈や思いも含む）だけではなく，それを受ける側である（⑤サービス受益者）および SoS の使用環境に（偶々も含む）存在する（⑥潜在的サービス受益者）からのリアクションも包括的にとらえて，図 3 の循環が仕組みとして組込まれていることが SoS のガバナンスにおいては重要である。そのためには関係者の全員参加を促す仕組みや相手の立場にたってヒアリングし続け，その声をシステムやサービスのアップデートに活用するための機構が必要となる。

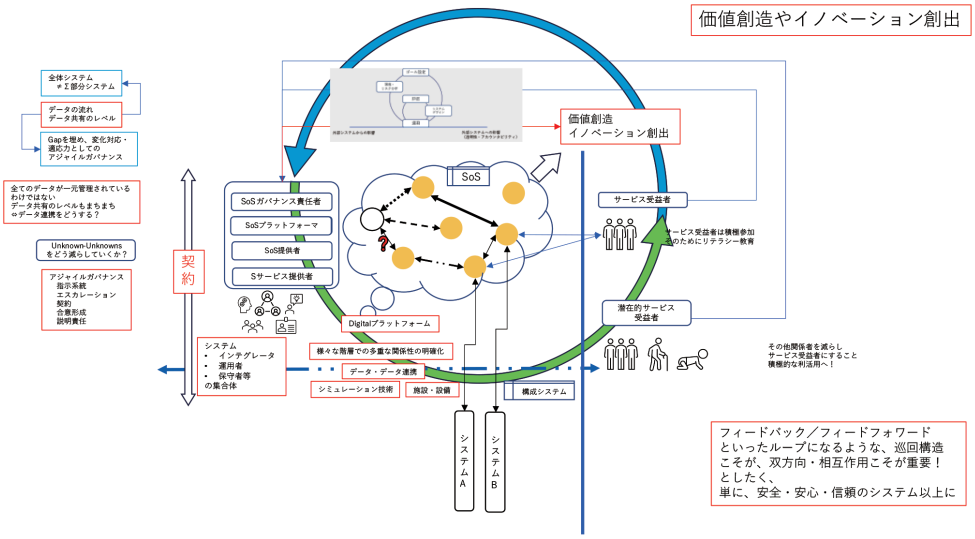


図 3

つまり，図 3 にあるような循環構造（緑青矢印の円環）をステークホルダが連携することにより実現することが SoS ガバナンスを実装するうえで本質的な事項となる。すべてのステークホルダは共通の社会課題の解決のため，自分事として課題と向き合うとともに積極的に参加することにより SoS サービスの提供側・受益側といった境界を越えて双方向な交流を実践することで全体最適，あらたな価値創造の役目を担っていると自覚する必要がある。また，全員参加による価値創造，スパイラルアップが実現されていることをステークホルダに感じてもらい，さらなる積極的な関与・参加を促すようなコミュニケーションを活性化するツールや価値の見える化，分析などのツールを SoS プラットフォームに実装して活用することも循環構造の構築に重要である。

SoS サービス提供側がすべき事項

SoS をガバナンス，構築，運用する組織および SoS を活用してサービスを提供する組織である：SoS ガバナンス責任者，SoS プラットフォーマ，SoS 提供者，サービス提供者の各ステークホルダがすべき事項を整理する。

はじめに断っておくが，4 組織が完全に独立して単独で実施する事項はなく，あくまでも実行主体として何をすべきかを分類したものであり，役割については重複があっても構わない。むしろ問題なのは，どの組織も担当していない事項が存在することであり，そうならないようにルール・役割・責任を決めていく必要がある。

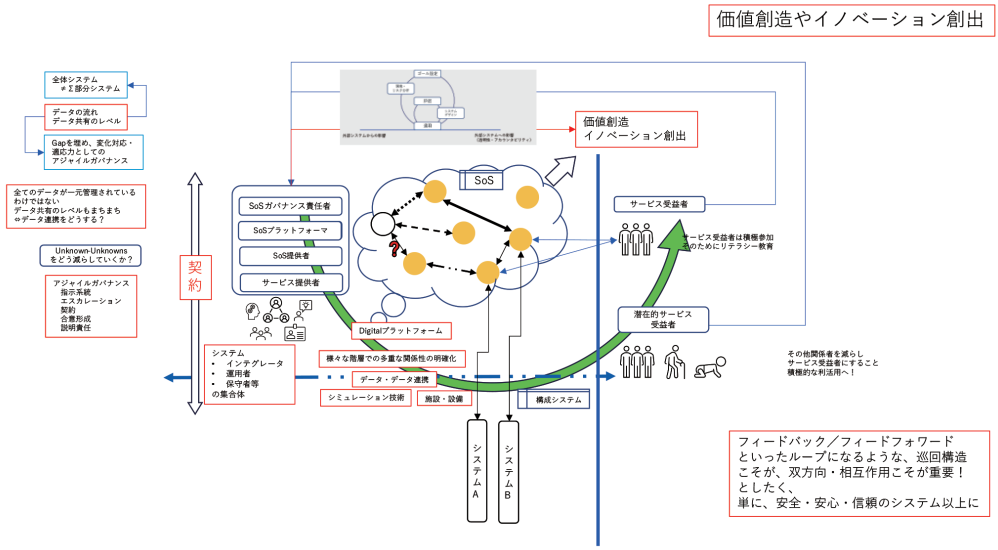


図 4

SoS を活用したサービスの提供においては，一方的な提供に留まらず，サービス受益者からのフィードバックをサービス強化や新サービスの創出へとつないでいく活動も重要である。そのためサービス受益者からの反応・声を集めて，それをサービスの向上などへとフィードバックをする仕組みをあらかじめ SoS の設計では考慮する必要がある。SoS レベルにいる 3 者：SoS ガバナンス責任者，SoS プラットフォーマ，SoS 提供者および SoS を活用してサービスを提供する 4 組織の関係（SoS サービス提供側と呼ぶ）図 5 のようになる。

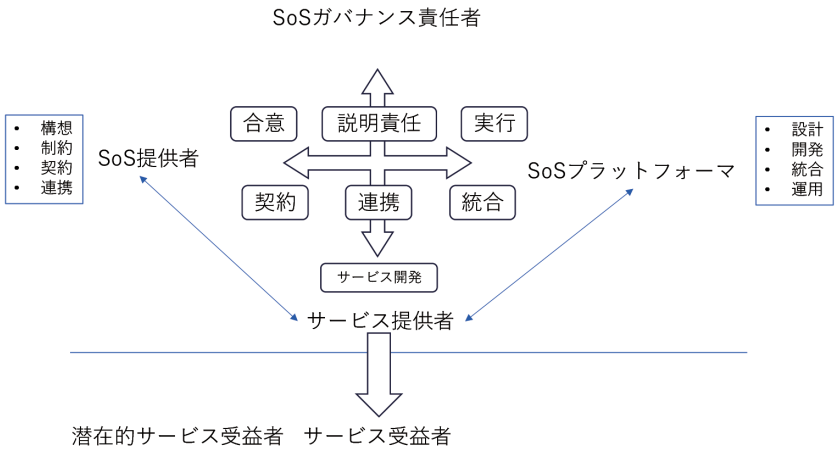


図 5

本ガイドラインでは，SoS レベルでのガバナンスの主体である SoS ガバナンス責任者，SoS プラットフォーマ，SoS 提供者とサービス提供者との間に契約関係を締結し，指揮系統およびエスカレーションルールを定めることにより全体システムとして SoS および SoS サービスを trustworthy に提供し続けるために各主体が実行すべき事項を整理している。構成システムレベルの話は従来のマネジメントの仕組みにより担保されていることを前提としている。SoS を活用してサービスを提供する，サービス提供者は従来のマネジメントの仕組みにより品質，安全は担保されていることを前提としている。サービス提供者が増え，サービスを追加，もしくは既存のサービス提供者がサービスを追加・修正する場合には，その変化を SoS として適切に取込み，連携することにより全体システムとしての SoS としての全体最適が重要となる。この SoS を共通の場としたときの SoS レベルでのガバナンスに関する各主体の取組むべき事項を整理したものである。そのため，SoS インテグレーションに関する組織間および構成システムレベルに係る組織と SoS レベルとの間でのガバナンスの主体との取決めを定めたうえで全体を包括するかたちでアジャイル・ガバナンスが行使できる仕組みを構築するために必要な要求を記載したものである。

SoS ガバナンス責任者（SoS および SoS サービスに係る最終責任者）

社会，ステークホルダ，サービス，SoS の各対象に対して，安全性，セキュリティ，プライバシー等（安全・安心・快適）を考慮し，それが確実に実施できるような体制を構築して，必要なデータの流れを制御，記録可能なように関連組織の状態を維持・監督する。

SoS のガバナンスに対して，そのルールを立案するとともに，ルールに基づいて SoS が運用されていることの最終判断と責任の主体を担う。

アジャイルがバンスを確保するためには，SoS ガバナンス責任者には，各ステークホルダ間の調整マネジメントリーダシップ能力だけではなく，欧州でよく言われる今までのリーダシップ能力とは異なる場をリードするリーダシップ能力（meta リーダシップ）が求められる。この能力により，心理的安全な場を形成しつつ，思い込みや思い違いをなくし，形式知化していない暗黙知てきな“あたりまえ”の部分を引き出し，合意形成するファシリテーション能力が必要である。

上記記載した役割を果たすために，SoS ガバナンス責任者は，以下を担当し，確実に遂行する必要がある。

- ✓ SoS の提供や SoS に係る最終的な責任者として，SoS プラットフォーマと SoS 提供者と連携して SoS サービス，SoS のガバナンスがアジャイル・ガバナンスの考え方に基づき実施されていることを合意・実施・説明責任遂行の仕組みを構築させ，最終責任者として説明責任を遂行すること。
- ✓ 各ステークホルダ間のコミュニケーションが円滑に機能するための仕組みを設計すること：指示系統，エスカレーションルールの確立。SoS に実装される機構については，SoS

プラットフォーマと SoS 提供者とともに構想から実装計画，構築を依頼すること。
これらの仕組みには，SoS から直接サービスを受ける受益者からの不具合の通報や，SoS の周辺にいる人からのヒヤリハット情報などへの対応も含まれる。

✓ ガバナンスに必要なデータについてステークホルダと検討，合意した内容に則り，SoS プラットフォーマと SoS 提供者に決定事項を確実に実装させ遂行させること。

✓ SoS の便益とリスクについて SoS 提供者（必要であれば SoS プラットフォーマとサービス提供者も）から説明を受け，検討，合意するとともに，SoS の提供について SoS 提供者とサービス提供者に決定事項を確実に実装させ遂行させること（必要であれば SoS プラットフォーマも含めた三者で内容について協議させること）。

✓ 対象とする SoS に係る最高責任者として，説明責任を遂行すること。

また，提供する SoS 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，trustworthy に係るすべての事項に対する最高責任主体として；

✓ SoS プラットフォーマ，SoS 提供者およびサービス提供者の活動をオーバーサイトする。

✓ SoS プラットフォーマ，SoS 提供者から検討事項として提示された事項に対して関係者と検討し，最終決定を確定し，指示を出すこと。

✓ SoS プラットフォーマ，SoS 提供者を飛越え SoS 運用者等からエスカレーションしてきた事項について関係者と検討し，最終決定を確定，周知し指示を出すこと。

✓ 障害，不具合が発生した場合のステークホルダへの説明責任を遂行し，社会的・倫理的責任を負うこと。

障害，不具合などが発生した場合には原因究明のための調査委員会を設置するなど，説明責任の遂行に対して，透明性，公平性，中立性などについても配慮すること。

上記役割をアジャイル・ガバナンスに基づき実現し，SoS サービスの trustworthy な提供に責任持つこと。

また，提供する SoS サービスに関しての価値創造に係るすべての事項に対する最高責任主体として；

✓ SoS プラットフォーマ，SoS 提供者と連携し，SoS の社会受容性を向上させること。

✓ SoS プラットフォーマ，SoS 提供者から提示されたサービス受益者および潜在的サービス受益者からの価値認識の分析結果に対して関係者と検討し，最終決定を確定，周知し指示を出すこと。

SoS プラットフォーマ（SoS Developer）

SoS を開発する事業者。SoS プラットフォームの開発者であり，IT システムとしての SoS に関する主体的な役割を担う組織である。

SoS の構成要素となるサービス提供者が提供するサービスおよびそれに必要なシステムを統

合・融合することによりSoSプラットフォームの開発を実行する。SoSプラットフォーム構築においてはデータ連携などシステム連携にかかるプラットフォームとしてのSoSサービスの構築，インテグレーション開発も含まれる。

プラットフォーマ，データマネジメントメントに関して

SoSを構成するサービス提供者が提供するサービスおよびそれに必要なシステムから取得するデータおよびステークホルダ間で合意し，合意した情報の収集・記録を行うこと。

- ✓ SoS提供者と連携して，通常運用におけるデータ（正常に挙動していることの論拠となるあらかじめ定義されたデータ）の取得，管理，補完をおこなうこと。
- ✓ 異常・不具合が発生したとき，その原因を究明するために必要となると合意されたログ，監視カメラの画像データなどの証拠となる記録を提出すること。
- ✓ リデザインの判断のためSoSガバナンス責任者にエスカレーションするに必要なデータを提供すること。

対象となるSoSに関連するデータに係るライフサイクルマネジメントの役割を担うこと。

- ✓ データに係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，廃棄にいたるライフサイクルすべての段階において適切な管理を体制構築とともに実行すること。
- ✓ データの改竄防止についてはブロックチェーンなどの技術も活用した仕組みを構築すること。安全性，セキュリティ，プライバシーを考慮したデザインと実装を行うこと。
- ✓ SoSを構成するシステムにAIシステムが含まれる場合は，特にデータ品質（学習データ含む）についても考慮すること。

SoSプラットフォーマは，SoSガバナンス責任者，SoS提供者と連携を密にして，人・モノ・データの流れを明らかにするとともに，システムとしてのSoSにおけるライフサイクルマネジメントの主体である。この活動にはサービス提供者とのサービスに係る調整も含まれ，また，SoSプラットフォーマが基盤となるプラットフォームを構築しているため，SoSインテグレータとしての役割も全うしなければならない。

そのためには，SoSガバナンス責任者，SoS提供者，必要ならばサービス提供者からのneedsやwantsを汲み，咀嚼しデザインとして，SoSの構想を関係者間に提示，明示化することから始める必要がある。関係者間の合意形成を円滑にすすめるために，デザイン思考などを活用して，6W2Hについて，関係者と合意をはかる必要がある。

- ✓ SoS開発において，外部環境をも考慮したリスクアセスメントをSoS提供者と実施すること，SoSガバナンス責任者にその結果を報告，リスクマネジメントに対して合意すること。
  - ➢ 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をSoSサービス提供者とともに実施すること。
  - ➢ 安全性，セキュリティ，プライバシーについては，しっかりとした対策をSoSに機

能として備えると共に，対策を計画し，システムとして制御すること。また，安全性の確認は，信頼性の確認も含めること。

- ➢ サービス追加・変更などによる新規システム導入の為に，コンフォーマンステストの項目を決定すると共に，コンフォーマンステストを管理すること。
- ➢ 安全性や信頼性の確認は，運用が開始される前に，検討された対策を基に実機やシミュレータによる試験方法を決定し試験すること。また，試験結果を管理者へ報告すること。
- ➢ 新規システム導入する場合は，コンフォーマンステストを実施すること。また，試験結果を管理者へ報告すること。
- ➢ 新規システム導入やサービス追加・変更のプロセスは，シミュレータを活用するなど，コストや時間効率も含めて構築すること。
- ➢ 関係者の合意形成する仕組みを整備すること。

また，運用後にも検証可能となるように，あらかじめ SoS の機能としてログの取得や分析はもとより，意思決定（判断）に至るまでの過程の明確化などについても考慮した設計をすることが強く勧められる。

設計，開発においては Evidence based System Engineering の考えに基づいて，議論の過程も含めた開発にかかる証跡を残し，運用を見据えた Dev（Sec/Safe/ML）Ops などを考える必要がある。

- ✓ アジャイル開発をベースとした柔軟な開発を実施するとともに，検証についても確実に遂行できるようなプロセスと体制をサービス提供者と連携して構築すること。
- ✓ データ収集を安全などに活用するだけではなく，新たな価値創造に使うことも考えること。
  - ➢ そのためにデータ提供者から情報が集まりやすいような仕組み（SNS との連携）をすること。
- ✓ 開発においてシミュレータを活用して，シミュレータでの動作確認などを徹底するとともに，関係者間の合意形成のツールとしても活用すること。
- ✓ 運用において，SoS 監視者から事故やヒヤリハットの情報を得た場合は，原因究明と再発防止策を実施すること。
- ✓ 原因究明において，実機やシミュレータ，ログデータなどを使用して解析すること。また，解析結果を SoS 提供者へ報告すること。
- ✓ 再発防止についても検討し，実機やシミュレータで試験すること。また，試験の結果を SoS 提供者へ報告すること。
- ✓ 新たにサービスを追加するなど変化への対応においても，シミュレータを活用して，コスト，時間効率も含めた開発プロセスを構築すること。

シミュレーション技術について

シミュレーション技術は開発のみならず，運用において不具合の原因究明の支援や，サービスの追加を考えたときの影響分析など，物理世界での検証とは違ったレベルでの抽象度や自由度が高い分析を可能とする重要な技術である。それだけでなく，SoS ガバナンスにおける中心的な役割を果たす，SoS ガバナンス責任者，SoS プラットフォーマ，SoS 提供者の間の合意形成をスムーズにはかるためのツールとしても活用することを推奨する。

また，サービス提供者との間でどのようなサービスを実現するか，その意思決定においてもシミュレーション技術を活用して，ニーズから要求事項を適切に抽出するなど，活用の場面は多岐に渡る。このことからも，シミュレーション技術を活用することは SoS ガバナンスにおいて（特に，CPS として SoS をとらえ，開発・運用するにあたっては）必須のツールである。

SoS のモニタリング

SoS プラットフォーマは SoS および SoS サービスを常時モニタリングし，あらかじめ定めた範囲からの逸脱がないか監視する主体である。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やサービス受益者や SoS および SoS サービスの周辺に存在する関係者からの異常通知，ヒヤリハット情報，要望などの窓口としての役割をサービス提供者とともに有する。

SoS を構成する各システムにおいては，それぞれの担当にモニタリング自体は移管し，各レベルにおけるモニタリングの結果を集計し，あらかじめ定めた範囲からの逸脱を検出した場合は警告を出すよう指示するとともに，SoS 提供者，SoS ガバナンス責任者に通知するとともに，連携して対応すること。

- ✓ 外部の変化（特に潜在的サービス受益者の声）もモニタリングすること：SoS 提供者とサービス提供者と連携してシステムレベルでのモニタリングについて合意しておくこと。
- ✓ システム・サービスに対するものモニタリングについては，対象のレベルにあわせて階層化し，それぞれのレベルでのモニタリング主体を決め，モニタリングを実施させるとともに，緊急事態への対応としての通知手続き等をルール化すること。ルール化した手続きについては SoS ガバナンス責任者の承認を得て，SoS 提供者と共有すること。さらに，収集したデータに関して，特に事故情報など重要な意思決定に必要なものは SoS ガバナンス責任者にデータを提供すること。
- ✓ プラットフォームとして，SoS が正常に運用されていることを Operational Range などを設定して逸脱していないことを確認すること。
- ✓ サービスが予定された通りに提供されていることを確認すること：サービス提供者が提供するサービスに関する確認。
- ✓ サービス提供者からの異常検知などの通知を受けられるよう体制構築すること。

✓ サービス提供者の対応についてリアルタイム，もしくは時間差を最低限にして連絡がくるような仕組みを構築すること。
✓ サービス受益者からのサービスに対する不具合，不満，リクエストに迅速に対応できる仕組みをサービス提供者とともに構築すること。
✓ モニタリング中に逸脱を検出したら迅速な障害対応のため SoS 提供者へ連絡すること。
✓ 障害が発生していなくても，より良いサービスの提供，在るべき姿の実現のために何が現状と差があるかモニタリングすること。
✓ 外の変化を検出した場合に，その SoS への影響を分析するにたるデータの収集へと SoS 提供者へ連絡すること。

SoS 提供者（SoS Provider）

SoS プラットフォーマが構築した SoS をアプリケーションや製品もしくは既存のシステムやビジネスプロセス等に組み込むことにより，サービス提供者（SoS Business User）が提供するサービスを支える SoS を提供する事業者であり，設備等の物理的な主体も含めて提供する組織である。

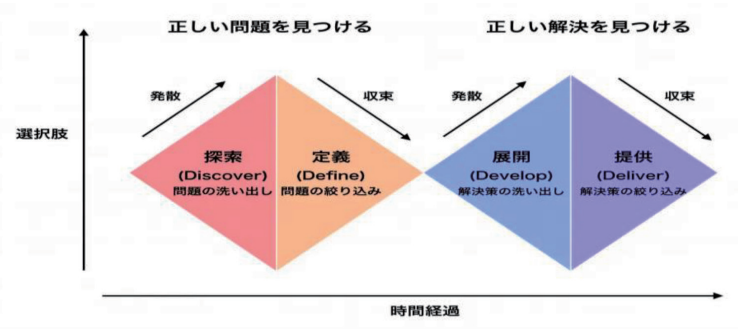
SoS ガバナンス責任者と同一の組織であることもあるが，SoS 運用の責任主体として，SoS プラットフォーマと連携を密にして，安定した SoS を活用したサービス（SoS サービス）をサービス提供者が提供できるように努める責任がある。

SoS 検証と妥当性確認，他システムとの連携の実装に関する SoS プラットフォーマへの要求事項の整理，使用環境を含めた SoS の提供および，サービス提供者が提供するサービスの共同開発や開発支援，そのサービスが正常に稼働のためのサービス提供者（SoS Business User）側の運用サポートや場合によっては AI サービスの運用の一部を担う。

SoS の提供に伴い，ステークホルダとのコミュニケーションが求められることがあるが，その際には SoS ガバナンス責任者とともにステークホルダ間のコミュニケーションを円滑にするための活動を担当する。ステークホルダ間のコミュニケーションは，各ステークホルダの背景知識などが異なるため，思い込み，思い違いが潜在的に存在する可能性が排除できないため，それら障害をなくす・軽減するためにはステークホルダ間での対話が必須であり，そのために求められる活動を SoS ガバナンス責任者とともに実施する。ステークホルダ間のコミュニケーションにおいては，何かを決める事も大事ではあるが，その前の形式知化されていない暗黙知の部分をいかに対話で引き出す対話のプロセスが必須であり，いわゆるアイスブレイクのような活動も含まれることに留意されたい。

（IDEO のデザイン思考などに書かれている，ダブルダイヤモンドの一つ目のダイヤモンドの，与えられた課題自体を再探索する過程に類似。ダブルダイヤモンドは，2005 年に英国デザイン協議会で初めて導入された，2 つのダイヤモンドを描くように発散と収束を行う課題解決方法であり，1 つ目の「正しい問題を見つけるダイヤモンド」では，「探索（Discover）」「定義

（Define）」に分けて問題点の発散と収束を行い，2つ目の「正しい解決を見つけるダイヤモンド」では「展開（Develop）」「提供（Deliver）」に分けて解決策の発散と収束を実施する。）



図は，https://uxdaystokyo.com/articles/glossary/doublediamond/ より

図 6

SoS 提供者は，SoS ガバナンス責任者および SoS プラットフォーマと連携して，アジャイル・ガバナンスの考え方に基づきサービス提供者が提供するサービスを Trustworthy にするための支援主体である。後述のサービス提供者が提供するサービスに関して，一緒にサービス開発を担当する役割を併せ持つ（開発自体は SoS プラットフォーマなど他組織に依頼するケースが想定されるが，その契約などマネジメントにおける主体である）。SoS を構成する各システムの連携について全体最適に向かうように常に作用し続け，変化を受け取った場合には対応する主体でもある。最終責任は SoS ガバナンス責任者となる。

- ✓ SoS サービスの便益とリスクについて分析し，Trustworthy な SoS サービスをサービス提供者，SoS プラットフォーマとコミュニケーションをしてサービスを構築支援し導入すること。
- ✓ サービス提供者に提供する SoS を構成するシステムやサブシステムに基づいて，SoS プラットフォーマ，サービス提供者と構成要素の製造，販売，運用，保守，管理などシステムレベルにおける各ロールの活動，責任範囲などを統括すること。
- ✓ システムレベルにおける各ロールの全体システム・サービスに対するアクション，相互作用，責任，契約を司ること。
- ✓ システム構成要素でコミュニケーション（通信）をとるものはグループ化するなどシステム構成の表現方法を明確にし，ステークホルダと合意すること。
- ✓ SoS におけるデータの流れについて明確化し，SoS の構成，振舞い，機能を明確にすること。
- ✓ SoS サービスを追加，変更する場合は，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）に関して，関係者と既存サービスへの影響について，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おこなうこと。

- ➢ その際に，使用環境について何を共有しているのか明確にすること。
- ➢ 既存 SoS と通信などコミュニケーションをする場合はデータ連携について検討すること。
- ➢ SoS として連携する（システムとしての連携）部分と，人を介して運用も含めた連携に関して再検証すること。
- ➢ 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取れていることの妥当性確認を実施すること。
- ➢ 上記に係る運用マニュアルなどの変更を関係者に指示するとともに周知すること。
- ➢ 変更にかかるすべての事項について SoS ガバナンス責任者，SoS データ責任者，SoS 監視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。

✓ SoS サービスの企画に先立ち，SoS サービスを提供する SoS 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 プラットフォーマおよびサービス提供者から入手し，サービス提供者に提供すること。サービス提供者と SoS プラットフォーマと三者で協議すること。

✓ SoS モニタリングに関しては，SoS プラットフォーマと連携して，何をモニタリングするかについて協議し，その結果を SoS ガバナンス責任者の承認のもとで実施すること。また，通常運用からの逸脱が検知された場合の対応について定義しておくこと。

✓ 記録するデータの管理に関して SoS プラットフォーマと協議し，SoS ガバナンス責任者と合意・承諾をえること。合意した内容がデータとして取得できるように SoS プラットフォーマ協議のうえ SoS に仕組みとして実装すること。

✓ SoS サービスを構築支援するにあたり，“施設 や場所の状況”および‘‘運用に係る体制“を考慮した SoS レベルでのリスクアセスメントを SoS および SoS サービスに対して実行し，安全性の確保 を目的とした 基本計画を立案し，同計画に基づき SoS サービスの提供を実施するマネジメントの実施主体であること。

- ➢ 上述のリスクアセスメントにおいては，SoS の残留リスク（SoS のみならず，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，この過程を繰り返すこと。
- ➢ リスクアセスメントの実施では，関係者（SoS インテグレータ，運用者，（保守者）を含む）を集め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こと。
- ➢ 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 サービス責任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こと。

✓ 事故の発生する可能性はゼロにすることは不可能であるため，あらかじめ，事故発生時の

対応手順を SoS プラットフォーマとともに策定すること（すべてのステークホルダが参加するような仕組みを構築すること，対応手順は全てのステークホルダに周知させ，要求とすること），事故が発生した場合は主たる関係者として対応にあたること。
SoS ガバナンス責任者の承認を得ること。

✓ 手順策定にあたっては SoS サービスを分析し，各システムにおいて実施すべき対応，システム構成要素として対応すべきこと等に各階層における対応策を体系化，詳細化すること（SoS プラットフォーマとサービス提供者に対する要求でもあることに留意）。
✓ SoS サービス提供中又は SoS の運用中，事故 若しくは 重大な故障が発生し，又は 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するとともに，再発防止のため原因を究明のためこれらに関する 情報を関係者に通知し，原因究明と再発防止の対策を講じること。
✓ 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こと（SoS プラットフォーマとサービス提供者に対する要求でもあること）。
✓ 安全確保上の必要がある場合には，提供するサービスに対して，利用者に対する制約を明確にすること（年齢，身長，体重 又は 技能等を含む）。
✓ 事故を避けるため必要かつ十分な安全上の情報を広報すること。
✓ 事故が発生した場合は，速やかに定義された対応手順に基づく緊急対応を実施すること，あわせて SoS 運用者などに対して適切な指示を出すこと。
✓ 緊急対応と並行して（時間差はある），原因究明をおこない運用を修正するだけでは解決しない原因についてはシステム側の改修をおこなうため，SoS ガバナンス責任者の承諾を得たのちに，修正の指示を下位階層へ出すこと。
  ➢ 意思決定は SoS ガバナンス責任者の責任の下，関係者と合意し，その決定事項を受けて全体システム・サービスのどこを修正するのか検討すること。
  ➢ 修正にあたり必要なデータを SoS プラットフォーマや関係者から取得すること。
  ➢ 下位階層のどこに指示をだすか，全体システム・サービスを的確に分解・分析して分担に関して依頼すること。
  ➢ SoS 提供者や SoS プラットフォーマが修正，合成・融合し復旧，カイゼンされた全体システム・サービスとしての検証と妥当性確認を実施すること。
  ➢ 上記実施結果を SoS ガバナンス責任者に報告し，記録を SoS データ責任者に渡し格納すること。

SoS 提供者は，SoS ガバナンス責任者および SoS プラットフォーマと連携して，アジャイル・ガバナンスの考え方に基づき SoS の運用・保守などライフサイクルにかかるマネジメント主体であること。サービス提供者が提供する SoS サービスの便益を継続的に高めるためにサービス提供者と連携して，以下を実行すること。

✓ SoS サービスの便益を継続的に高め，社会受容性の向上に責任を負うこと。

✓ SoS データ管理者と連携し，SoS ユーザおよび非ユーザに関するデータを継続的に取得すること。
✓ サービス受益者および潜在的サービス受益者から提供されるデータを継続的に分析し，SoS サービスの価値認識の理解と，そこから想定される要求機能とリスクを明らかにすること。
✓ SoS サービスの想定される要求機能をサービス提供者に公開し，サービス提供者のサービス改善に貢献すること。
✓ SoS サービスの価値認識に従って，サービス提供者同士を連携させ，新たな便益創造に貢献すること。
✓ SoS サービスの想定されるリスクを SoS ガバナンス責任者に共有すること。
✓ SoS プラットフォーマが実施する SoS モニタリングの結果を受けて SoS ガバナンス責任者と SoS プラットフォーマと 4 者で協議のうえ対応を考えること

※サービスの価値認識

サービスの価値認識とはユーザがそのサービスが何をするためのものなのかという個々のユーザの認識である。ユーザはこの価値認識に沿って，そのサービスの利用という行動を起こす。サービスがその行動をより満足させる機能を提供することでユーザの便益の評価が行われる。さらに，その行動にはリスクが伴うので，そのリスクの対処を事前に実施する必要がある。価値については，ステークホルダの立場によって同じ対象に対して異なる認識となることがある。この認識のズレ（差異）がサービス提供側と受益側で大きくなるとサービス自体が利活用慣れなくなる恐れが発生する。そのため，価値の見える化，特に異なる立場にあるステークホルダの価値認識を把握することが重要となる。

サービス提供者（SoS Business User: SoS を活用してサービスを提供する者）

事業活動において，SoS プラットフォームを利用したサービス（SoS サービスと呼ぶ）をアプリケーションとして計画，構築，実装ののち提供する組織。なお，SoS サービスの計画，構築，実装から提供までのすべてを担当するとは限らない。

サービス提供者は，SoS 提供者から安全安心で信頼できる SoS の提供（SoS プラットフォームおよび，それから提供されるサービス，物理的な設備などを含む，以下，SoS および SoS サービスと呼ぶ）を受けながら，自らの事業活動として SoS サービスをサービス受益者に提供する。そのためには，SoS プラットフォーマおよび SoS 提供者と密に連携しコミュニケーションをとる必要がある。

SoS 提供者が意図した範囲内で，継続的に SoS を適正に利用して，自らが考える理想のサービスをサービス受益者に提供することが重要である。また，サービス受益者の反応を適切に集め，サービス向上や新サービスの開発へと継続的なカイゼン活動が通常の運用に組み込まれるように運用プロセスを構築する必要がある。これにより業務効率化や生産性，創造性の向上等

SoS によるイノベーションの最大の恩恵を関係者が受けることが可能となる。また，人間によるオーバーサイト（Human Oversight）を導入することにより，人間の尊厳や自律を守りながら予期せぬ事故を防ぐことも可能となる。

サービス提供者は，社会やステークホルダから 提供したサービスに関して説明を求められた場合には，SoS 提供者等のサポートを得てその要望に応え理解を得ることがアカウンタビリティの観点からも重要であり，より効果的な SoS 利用のために必要な知見習得や SoS 理解のための取組みも期待される。

- ✓ SoS 提供者が意図している適正な利用および環境変化等の情報を SoS 提供者と共有し SoS サービスの提供を正常に継続すること。
- ✓ 必要に応じて提供された SoS を活用する役割を担うこと。
  SoS の活用において業務外利用者に何らかの影響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，SoS による便益最大化の実現に努める役割を担うこと。
- ✓ 自らの事業として提供する SoS サービスについて責任を持つこと。
- ✓ 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こと。
- ✓ SoS プラットフォーマ，SoS 提供者と意思疎通を密にして，アプリケーション開発など SoS サービスの提供に必要な事項を計画，実行すること。
- ✓ ビジネスのフィードバックについてもあらかじめ考慮して SoS を利用すること。
  つまり，どこまでデータを SoS プラットフォーマ，SoS 提供者に共有するのか定めること。
- ✓ ヒヤリハット情報のみならず，改善ポイントへとつながるサービス受益者の声をどう集めるのか（その仕組みが SoS プラットフォームおよび SoS 提供者側にある場合は調整すること）。
- ✓ サービス受益者の声のみならず，潜在的サービス受益者からの声も集める仕組みとその利用について SoS プラットフォーマ，SoS 提供者と三者で合意して実装すること。

安全を考慮した適正利用

- ✓ SoS 提供者が定めた利用上の留意点を遵守して，SoS 提供者が設計において想定した範囲内で SoS および SoS サービスを利用すること。
- ✓ 正確・必要な場合には最新性（データが適切であること）等が担保されたデータの入力を行うこと。
- ✓ SoS サービスの出力について精度やリスクの程度を理解し，様々なリスク要因を確認した上で SoS を運用する。
- ✓ SoS サービスのアウトカムを理解するため，サービス受益者からの声を集める仕組みをサービスに取り組むこと。

個人情報の不適切入力とプライバシー侵害への対策

✓ SoS および SoS サービスへ個人情報を不適切に入力することがないよう注意を払うこと。
✓ サービス開発においては，サービス受益者に対して，個人情報などに関する取扱いについて明示し，関係者と合意したうえでサービスを提供すること。
✓ サービス受益者の個人情報を適切に管理すること。
✓ SoS および SoS サービスにおけるプライバシー侵害に関して適宜情報収集し，防止を検討すること。

セキュリティ対策

✓ SoS 提供者によるセキュリティ上の留意点を遵守すること。

関連するステークホルダへの情報提供・説明

✓ 著しく公平性を欠くことがないよう公平性が担保されたデータの入力を行い，バイアス等にも留意して SoS および SoS サービスから出力結果を取得すること。
✓ そして，出力結果を事業判断に活用した際は，その結果を関連するステークホルダに周知すること。
✓ 関連するステークホルダの性質に応じて合理的な範囲で，適正な利用方法を含む情報提供を平易かつアクセスしやすい形で行うこと。
✓ 関連するステークホルダから提供されるデータを用いることが予定されている場合には，SoS の特性や用途，提供先との接点，プライバシーポリシー等を踏まえ，データ提供の手段，形式等について，あらかじめ当該ステークホルダに情報提供すること。
✓ SoS の出力結果を特定の個人又は集団に対する評価の参考にする場合は，SoS を利用している旨を評価対象となっている当該特定の個人又は集団に対して通知すること。
✓ データの取扱いについては，関連するガイドラインが推奨する出力結果の正確性や公正さ，透明性等を担保するための諸手続きを遵守すること。
✓ 自動化バイアスも鑑みて人間による合理的な判断のもと，評価の対象となった個人又は集団からの求めに応じて説明責任を果たすこと。
✓ 利用するシステム・サービスの性質に応じて，関連するステークホルダからの問合せに対応する窓口を設置し，SoS 提供者とも連携の上説明や要望の受付を行うこと。

提供された文書の活用と規約の遵守

✓ SoS 提供者から提供された SoS および SoS サービスについての文書を適切に保管・活用すること。
✓ SoS 提供者が定めたサービス規約を遵守すること。

サービスの改修，新サービスの開発などに関して，SoS 提供者，SoS プラットフォーマとコミュニケーションを密にするとともに，他のサービス提供者ともコミュニケーションが取れるようなコミュニティを形成することが望ましい。

SoS サービスを受ける側がすべき事項

SoS においては，サービス提供側から一方的にサービスを受けるだけではなく，受けたサービスから何が得られたのか，より良いサービスにするためには何ができるのか，双方向なコミュニケーションが重要である。また，SoS においては構成システムに AI システムも含む，高度な技術内容が含まれるケースがあるため，サービスの提供を受ける側に対しても，ある程度のリテラシーが求められることにも注意が必要である。

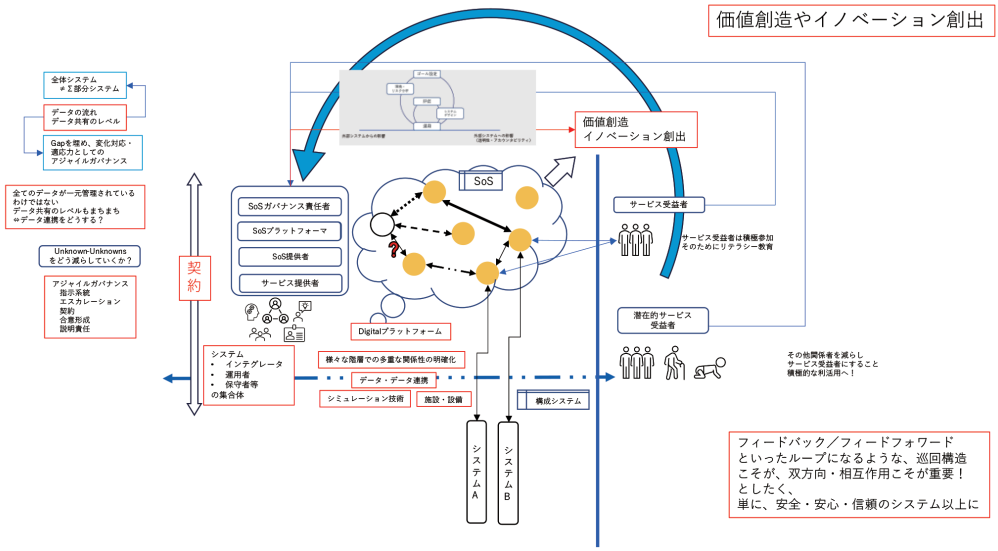


図 7

さらに，SoS サービスを受ける側は一方的にサービスを提供されるだけではなく，提供されたサービスについて評価し，フィードバックをすることでより良いサービスをサービス提供側と一緒に作っていくような取組みへ参加することが望ましい。もちろん，そのためにはサービス提供側のほうで，受け手側の声を集めるための仕組みをあらかじめ構築している必要がある。SoS の強みとしては，ガチガチにルールが決まっており，それを変えることを許容しない（故に安全がある程度担保され，サービス提供側の責任とすることになりがちである）のではなく，関係者が全員参加することにより，新たな価値創造やイノベーションの創出へとつながっていくことでもある。

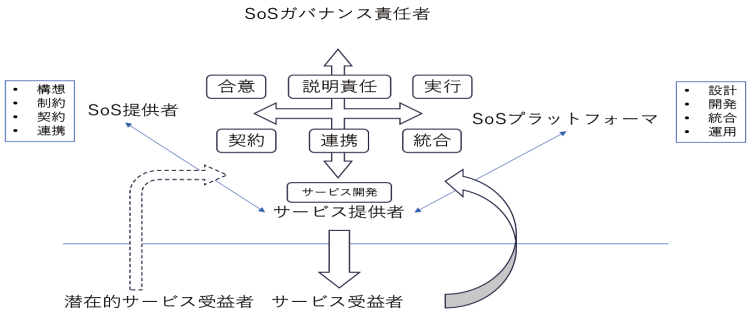


図 8

そのためには，サービス受益者側で，

◇　守るべきこと

◇　発信すること

に関して，適切に理解し対応していくことが重要である。

また，サービス提供においても，①利用前に，サービス内容を理解すること，必要なリテラシーを身に着けておくこと。そのためにアプリの適正なダウンロード方法，適正利用を遵守するために必要な事項を洗い出しておくこと。利用で発生する責任について，リスクと便益について合意（契約）しておく必要がある。②利用中・利用後のリアクションとして，気づいた事項については発信し，サービス向上につなげる活動へと参加すること。

サービス受益者

SoS ユーザが提供するサービスに対して，直接リクエストを出すことにより，サービスを受益する人：SoS を業務としては直接使わないがその便益（場合によっては損失）を被る可能性がある人のこと。

安全を考慮した適正利用

✓　サービス提供者が定めた利用上の留意点を遵守して，サービス提供者が設計において想定した範囲内で SoS および SoS サービスを利用すること。

✓　正確・必要な場合には最新性（データが適切であること）等が担保されたデータの入力を行うこと。

✓　SoS サービスの出力について精度やリスクの程度を理解し，様々なリスク要因を確認した上で SoS を利用すること。

✓　SoS サービスの向上を助けるため，提供されたサービスに対して反応を示すこと。

個人情報の不適切入力とプライバシー侵害への対策

✓　個人情報を不用意に入力しないよう注意を払うこと。

✓ 個人情報などに関する取扱いについて確認し，合意したうえでサービスを利用すること。
✓ 個人情報を適切にマネジメントすること。
✓ SoS および SoS サービスにおけるプライバシー侵害など不利益なないことを事前に確認したうえでサービスの利用を検討すること。

セキュリティ対策
✓ セキュリティ上の留意点を遵守すること。
✓ 不安があった場合はサービス提供者を含む，SoS サービス提供側に問合せをすること。

関連するステークホルダへの情報提供・説明
✓ 著しく公平性を欠くことがないよう公平性が担保されたデータの入力を行い，バイアス等にも留意してすること。
✓ 提供したサービスにより，ポジティブなこと，ネガティブなこと含めて気づいたことがあれば，声として関連するステークホルダに発信すること。

提供された文書の活用と規約の遵守
✓ SoS 提供者から提供された SoS および SoS サービスについての文書を適切に保管・活用すること。
✓ SoS 提供者が定めたサービス規約を遵守すること。

データ提供（ポジティブ・ネガティブ）
✓ ヒヤリハット情報，軽微なサービスの停止（いわゆるチョコ停）などの不具合情報。
✓ サービスに対する要望や不満，満足など。
✓ 障害対応，カイゼン対応につながる情報の提供。

リテラシー教育に関して

SoS を利用するにあたり，サービス受益者は一方的にサービスの提供を受けるだけでは不十分である。SoS を利用したサービスに関する一定レベルの理解がなければサービスの価値を十分に享受できない場合があり，特にサービスを利用するにあたり提供する情報（個人情報など）については自衛の意味でも一定のリテラシーが必要となるからである。リテラシー教育については，単なる座学やインタビューでは潜在的な暗黙知的な情報は引き出せない。高度なファシリテーション能力（Meta ファシリテーション）を有する人材を確保し，どう育成するかが大事。コミュニティの声を聞く方策としては，インタビューだけではなく，ワークショップや参加型のフェス形式などとなるような配慮も効果的である。

潜在的サービス受益者

直接 SoS サービスと相互作用する主体ではないが，使用環境にいる存在

まず，自身がいる環境について，どのようなロボットやドローンなどが共存しているかについて積極的になること。その上で，直接サービスの授受など相互作用はないまでも，物理的な積極などを含めて，被害者にならないこと，加害者にならないように SoS が運用されている環境やルールに対する理解を自発的に行うこと。

✓ 警告などについて目を通すこと：掲示，看板など環境情報の把握　注意義務について理解しておくこと。
✓ 何かあった場合は関係者の指示にしたがうこと。
✓ ヒヤリハット情報など気になったことを通知すること。

データ提供（ポジティブ・ネガティブ）

✓ ヒヤリハット情報，チョコ停などの不具合情報。
✓ サービスに対する要望など。
✓ どうなったら，どういったサービスなら参加するか。
✓ 何が参加へのハードルになっているのか等の情報。
✓ 障害対応，カイゼン対応につながる情報の提供。

イベントなどへの対応について：期間・場所等が限定されるもの

イベントなど通常の SoS の運用，ガバナンスを踏まえつつも，次なるサービスの開発，イノベーション創出・価値創造へのチャレンジととらえること。イベント開催中に関係者とのコミュニケーションからニーズやウォンツを集め，要求へと，それに基づいた新サービスの開発，システム開発へ昇華させることを念頭におくこと。

サービス提供者，サービス受益者，潜在的サービス受益者などの声をどう反映させるか考えたうえでイベントを開催すること。それがイノベーション創出・価値創造へとどう繋がるのか，繋げるようにしたいのかを明確にすること。

期間・場所等が限定されているイベント　⇒　挑戦的な取組みを試す特別な「場」と考える。

✓ 届出など，通常とは違う，より（挑戦的）参加を促すようなイベントを開催することにより，通常の運用ではできていなかったことにチャレンジすること。
✓ 参加型イベントとして，双方向にコミュニケーションをとること。
✓ 潜在的サービス受益者をサービス受益者など SoS と直接関係するステークホルダへと行動変容させることにより，社会受容性を高めることを目的とすること。
✓ その際に，社会受容性について調査するなども忘れないようにすること。

提供したサービスに対して，反応してもらうためには，魅力的なサービスであることが大前

提であり，コミュニケーションを円滑にして参加者の声を集めるためには，双方向性，巡回構造，スパイラスアップ構造を組み込むようにすること。

単なる利便性がいいから使ってみたいから，楽しいから使いたい，もっといいサービスにするために何が要るか，積極的に発信，一緒に開発，一緒に作る「場」としてイベントをとらえる（共創のため）。

そのために，あそび場（体験型，参加型）であり，ステークホルダのコミュニケーションの場（デザイン思考の活用）としてのイベントの構想・企画立案が重要である。

一般人が参加の外部向けのイベントについて

イベントの実施については，事前に SoS ガバナンス責任者を中心として関係者で内容の検討し，プロジェクトチームを立上げ，プロジェクトとして管理できるよう体制等も含めて計画立案すること。当該プロジェクトに係る計画，イベントの実施から終了までの記録を残すこと。

➢ ヒヤリハット情報収集のための仕組みを用意すること。

サービスロボット安全ガイドラインから

✓ イベントの実施者は，次の事項を実施又は遵守するよう努めなければならない。
✓ イベント内容の安全性分析など。
✓ 使用する機器はあらかじめ定めた選定基準に則り選定すること。
✓ イベントに先立ち，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。
✓ 被験者および被験者以外の第三者の生命，身体，財産，プライバシー権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等の意見を聴取したうえ，同計画 を実施すること。
✓ 安全確保上の必要があるときは，一定の年齢，身長，体重又は 技能等 を備えた者を被験者とすること。
✓ イベント中に事故の発生する可能性がある場合には，あらかじめ，事故発生時の対応手順を策定すること。
✓ 事故を避けるため必要かつ十分な 安全上の情報を広報すること。
✓ イベントを実施した結果，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，これを製造者等に通知すること。
✓ イベント実施上の事故に基づく賠償責任を補償する保険に加入すること。
✓ イベント終了後に，イベントに係るデータを保管して，SoS サービスの向上などに反映すること。

おわりに　社会受容性を高めるために

SoS におけるサービスの提供においては，新しいサービスや仕組み（ロボットやドローンとの共生）が内在されることからも，社会に受け入れられるような仕組みを考える必要がある。最先端の技術を目の当たりにした場合，便利であることを理解する前に，躊躇して避けてしまわれないように，とりあえず使ってみようと積極的な行動へと誘う必要も SoS が社会に浸透する際に必要である。とはいうものの，実際に SoS を運用してみて，サービス受益者などからのフィードバックを分析し，カイゼンするサイクルを回してみなければわからない部分が多くあるため，現時点では，これこそが社会受容性を高めるためのソリューションですと提供する段階にまでは到達していない。したがって本章では，現時点で，こうしたら良いのではないかという仮説のもと我々の主張を以下述べさせていただく。今後，SoS を実運用するなかで得られた知見により，適宜修正加筆をしていく予定であり，その意味で本章はリビングドキュメントであり，未完であることをあらかじめご了承いただくとともに，こうしたら良いのではないかといったご意見・コメントもあわせて頂戴できれば幸いである。

VUCA から BANI へ

VUCA（Volatility: 変動制，Uncertainty: 不確実性，Complexity: 複雑性，Ambiguity: 曖昧性）の時代といわれてから久しい。世界（社会）には不確定な要素が増加しており，それらが社会的不安や社会情勢の混乱を招いている。このような世界においては，その対応として OODA ループに注目が集まった。OODA ループは，観察（Observe）− 情勢への適応（Orient）− 意思決定（Decide）− 行動（Act）− ループに Implicit Guidance & Control, Feedforward ／ Feedback Loop をあわせるによって，健全な意思決定を実現するというものである。VUCA も OODA も，もともとは軍事用語である。VUCA は 1990 後半から言われだし，20 世紀末には，ビジネス，経営などの分野でも使われるようになった。OODA も軍事的な範疇を越えてあらゆる分野に適用できる一般論と認識されている。しかし，OODA は小規模で変化に対応できる現場などでは有効ではあるが，ある程度の規模になると適用が難しいとの指摘もある。何故ならば，OODA ループは，そもそも個人の意思決定，判断などパイロットの能力の分析から得られたものであり，その意味において個人の状況適応モデルと考えられ，その有用性については適用範囲も考慮する必要がある。この点について，野中郁次郎は，OODA ループは個人の状況適応モデルであるとし，組織の知識創造やイノベーション能力をスパイラルアップするものとして，個人から組織へと，暗黙知を形式知として組織に対して結晶化させるプロセスとして SECI モデルを提案したといわれている。そして，変化が穏やかなときは PDCA サイクル，激しいときは OODA ループが適していると分析している。また，堀義人は，VUCA には VEDA で対応することが有効と提唱している。ここでいう VEDA とは，Vision，Education，Dialogue，

Action のことであるが，VEDA とはサンスクリット語で「知識」を表すことからも，面白い表現である。

最近は，VUCA の時代から，BANI も加わり，より混沌となってきたともいわれている（Jamais Caisco 氏が論説“Facing the Age of Chaos”において提唱）。BANI とは，Brittle: 脆い，Anxious: 不安，Nonlinear: 非線形，Incomprehensible: 不可解の頭文字を並べてものであるが，当初は COVID19 のパンデミックにより，世界がより混沌と不安になってきた様相を表す用語として使われた。COVID19 への対応は一応の落ち着きをみせてきていると思われるが，未知のウイルスによるパンデミックの脅威，世界情勢の不安定さ，国家間，人同士の連携の脆さなど，人類への課題は残されたままでもある。さて，この混沌とし，（漠然とした）不安な世界を生き抜くには，Resilience，Agile，Mindfulness そして直観力がカギであるとされている。

ここで，ともすると古典ともなりつつある PDCA サイクルについて一言ふれておきたい。まず，当初から綿密かつ完全な計画（P）を立てることは上述の VUCA，BANI な世界において現実的とは言い難い。そのため，まずはわかっていること，見えていることから計画を立案し，アジャイル型に進め，モニタリングを通じてカイゼンを進めながら，段階的に拡大，修正できるような柔軟で拡張性が高いデザインが必要となる。そのために PDAC をしっかり実現するためには，Policy, Design, Concept, Architecture がなければならない。また，これらが揃ったとしても，関係者が実現できなければ絵に描いた餅でしかなく，その意味では，皆が安心・安全で，夢があって，快適であり，達成可能であること，つまり，Peaceful，Dreamy，Comfortable，Achievable（Attainable）でなければならない。また，PDAC の対象となるモノ・コトには，物理世界，デジタル（データ），サイバー空間，自律性といった Physical, Digital, Cyber, Autonomous について考慮していく必要がある。つまり，モノ・コトとしてのサイバーフィジカル空間である CPS があり，サイバー空間とフィジカル空間（物理世界）を往来するためのデータとそれを利活用するためのデジタル技術，CPS 上で挙動する自律分散システム，その部分空間としての SoS について考察を進めることが重要となる。その中で，上述の PDCA が達成できているか検証していく必要があると考える。

【質問】

では，このような VUCA，BANI な世界のなかで，さらに多様性や包摂性が求められるなかで，社会受容性とはどうあるべきであり，どう向上させることができるのであろうか。

多様性と包括性を考える場合には，大量生産に代表されるような“マス XX”ではなく，カスタマイズされ，個人の趣味嗜好に応じたテーラーメイドなサービスへのニーズへの対応が重要となると考える。これは，個別化・差別化といった他との比較ではなく，私だけのサービスといった“一意性”こそが，個として異なる各人にとって重視されるようになってきているとも考えられるからである。

【回答】現時点における我々の主張は以下となる。

VUCA や BANI といわれる社会において，社会受容性とは個々を（が）受け入れることができる**寛容度**であり，社会受容性を向上させる仕組みとしては，アジャイル・ガバナンスの図に加筆した。

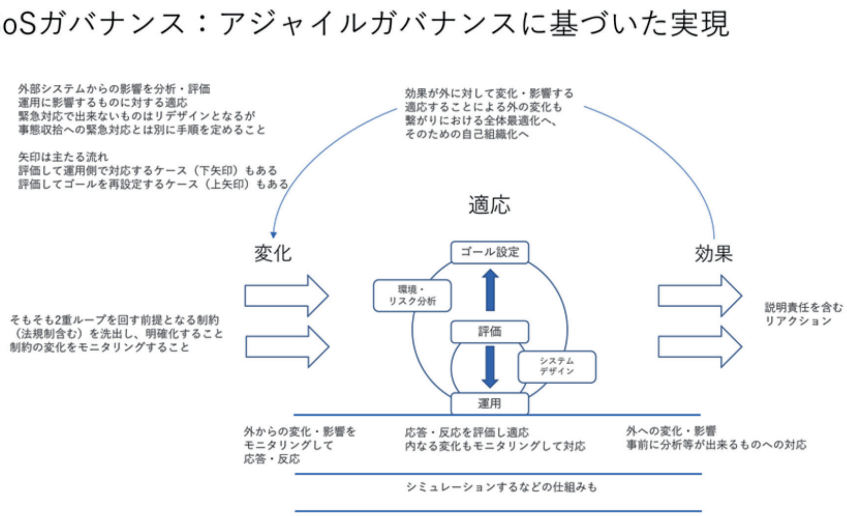


図 1

および，本稿で，赤枠を明確にし，循環構造（緑青矢印の円環）をステークホルダが連携することにより実現することすることがSoS ガバナンスの実装の本質であるとした。

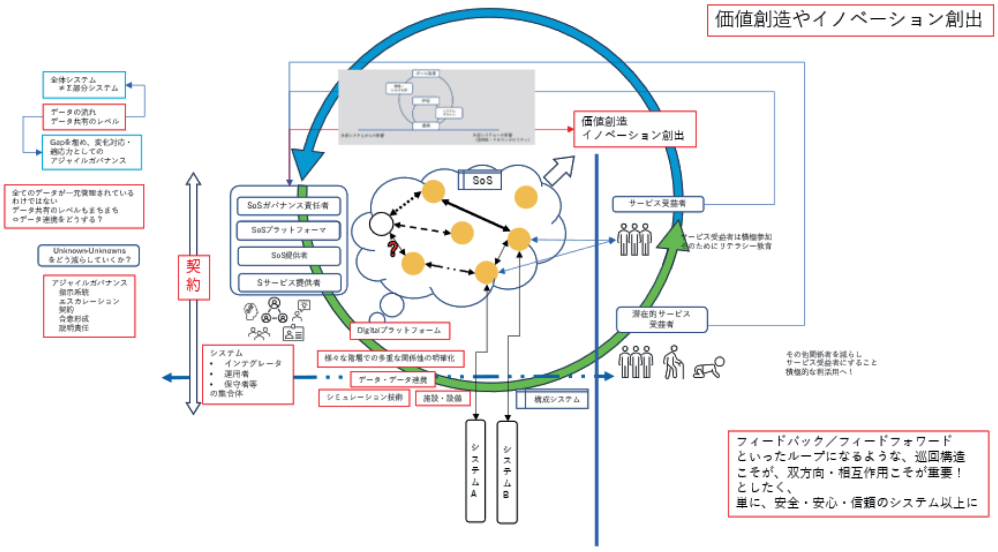


図 3

図 3 を連動させ，相互の関係を詳らかにしながら，上述した PDCA に関する分析を組み入れる形でスパイラルアップし続けることが社会受容性の向上に寄与する仕組みである。

【確認すべきこと】

- 双方向型：図 3（円環）をスパイラルアップに回すための仕組みがあるか。
  SoS に実装するもの，各構成システムでのマネジメントとして構築するもの，SoS ガバナンスとして各構成システムとの連携を含めて構築するもの等，レベルに応じた仕組みを明確化されているか？
- 全員参加型：他人事ではなく，自分事としてステークホルダは SoS と相互作用するための仕掛けがあるか？
  参加することで得られるメリットとともに，参加するためには最低限のリテラシーが必要であり，その取得が，過程も含めて Well Being に通じるような仕掛けが存在するか？
- 全体最適化：ステークホルダが全員満足するための運用と評価，カイゼン
  共存共栄，全体観といった一歩ひいた，俯瞰した立場からの社会全体最適に向けた各人の行動へと行動変容を促し，その活動が評価されるような仕組みがあるか？
- コミュニケーションの重要性：リスクとベネフィットについてステークホルダが理解していることを確認したか？
  多様性や包摂性の重要性，その実現にコミュニケーションが必要不可欠な事項であること。コミュニケーションを円滑にするための仕組み。あわせて，ポジティブ・ネガティブ両面から物事をとらえるために多様な人々との意見交換の実現があるか？
- SoS だからこそ出来ること，したいことが明確になっているか？

全ステークホルダにとって意味ある，価値あるようになっているか

- Win × N となるような仕組みとなっているか？
  参加者全員がハッピーに Well Being を！となるような仕組みがあるか？
- 実機を使う前にシミュレータの活用　→　メタバースにおけるアバター活用
  将来的には，物理的な存在を仮定しなくてもサイバー空間におけるアバターなども含めたメタバースにおける SoS といった形をも考慮しつつ，最低限のガバナンスとは何なのか，基本的人権の尊重や多様性，包摂性はどうあるべきなのかについて皆で知恵を出しながらよりよい社会の実現へと導くための「場」としての SoS の在り方と，そのガバナンスの方法論の確立を目指す取り組みがあるか？
- コミュニティの活用：たて・よこ・つながる　縦横にネット枠型に階層も超えたモノ・コトの往来（随伴関係の確立）と高次元化がされているか？

各ステークホルダがそれぞれで，アジャイル・ガバナンスを回せていること

- アジャイル・ガバナンスの輪をステークホルダ間でさらに大きく，関係者全体のレベルでのアジャイル・ガバナンスへと昇華させるようになっているか。
  小さなアジャイル・ガバナンスをより大きなアジャイル・ガバナンスへと。

小さなアジャイル・ガバナンス　≒　各ステークホルダレベル

大きなアジャイル・ガバナンス　≒　全ステークホルダによる共創，協働，協創のサイクル

各レベルにおけるアジャイル・ガバナンスの環を連携・連動させる meta な仕組みの提供へ。

そのためには，Data Driven であり Evidence Based である仕組みを SoS および SoS サービスにあらかじめ組込んで（Build In）しておくこと。

データについて

・　データが物理的空間とサイバー空間を Digital 技術で橋渡しとなっているか？

・　データが期待（予想）と現実のギャップを認識し，それを埋めるために活用する要素となっているか？

補　　論

汎用版に記載したことを実施するにあたり，法律など含めて制度設計しなければならない事項などについて整理する。

・　Digital 事故・Digital インシデントの定義

・　事前回避・事故検知・事故対応の一般的な枠組み

・　Digital 事故の報告と事故情報（再発防止策含む）の蓄積と共有の仕組

・　補償・賠償の原則と仕組み：法整備

・　情報提供者への訴追免除・減免措置について：法整備

・　上記項目の見直しプロセスの設定（アジャイル・ガバナンス的に回す仕組み）

基準，要求事項の整理

⇒　Digital 事故調査委員会の設置に向けた検討

・　SoS アジャイル・ガバナンス評価の仕組み，基準，チェック項目の整理

・　動的に変化する責任分界点を考慮した契約の在り方，既存法との関係等の分析

・　Unknown-Unknowns の判定基準

・　社会受容性の評価手法の確立

・　SoS トラストワージネス（安全性・セキュリティ・プライバシー保護）レベルの決定方法とアセスメント方法の構築

・　国際協調，国際連携について：相互承認の仕組みなど検討（国際標準化を含む）

・　スマートキャンパス評価：キャンバス OS の定義，成熟度評価

・　公益デジタルプラットフォーム認定などを活用して，SoS プラットフォーマの要件定義と

認定制度の検討

【注】

1）SoS とは，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。SoS サービスは，SoS を用いて提供されるサービスの総称。後述の SoS 提供者が提供する SoS を活用して提供されるサービス提供者のサービスを指すことが多いが，SoS プラットフォームにより提供されるインフラストラクチャー的サービス，SoS 提供者が提供する使用環境から得られる事項などが含まれる場合もある。SoS ガバナンスは，SoS を構成する各システム，SoS プラットフォームを活用して，構成システムより提供されるサービスについて構成システムのレベルではなく，上位な立場から SoS および SoS サービスに関（対）するガバナンスのこと。以下，SoS ガバナンス責任者，SoS プラットフォーマ，SoS 提供者，サービス提供者，サービス受益者，潜在的サービス受益者は，ステークホルダの項目にて定義。

2）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 の運用に伴うリスクを複数のステークホルダで分散し，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 運用をより安定化させる（根底で支持）ために必要不可欠な要素である。まず，優先されるべきは被害者を救済することである。民事不法行為責任利用者がサービス提供者の故意または過失を立証しなければいけないことの真の問題は，関係者から情報が集まらず立証までに時間がかかることにより，直ちに被害者が救済されないことにより，SoS への信頼が損なわれ発展しなくなり，イノベーションが阻害されることであると考える。そのため，公益デジタルプラットフォーム認定のように，国が SoS プラットフォームとして認定した SoS については国が救済制度を設けるなども検討が必要である。その際には，情報を提供する（説明責任の一環としても）ことによる組織へのインセンティブを作り出すことが可能となるような制度設計が必要となると考える。

【参考文献】

府省庁ガイドラインなど

- ➢ 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

- ➢ 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
- ➢ 9 主務省庁
  - ◇ 技術情報管理認証制度
    https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/
- ➢ 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（一部）

- ➢ 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）／一般社団法人　ディペンダビリティ技術推進協会

- ➢ 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

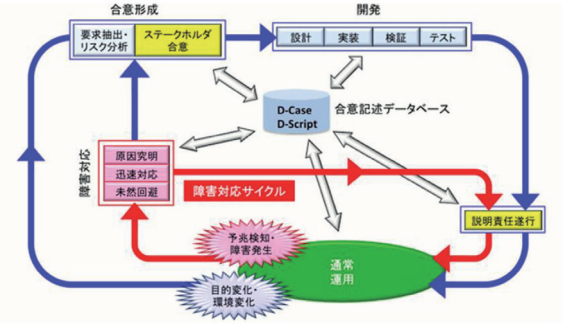


図 9

図 9 は，DEOS プロジェクトにおいて提唱された障害対応サイクル（赤矢印）と変化対応サイクル（青矢印）をあわせもつ DEOS ループである。重要なのはステークホルダで合意した内容を実施し，必要な証跡を合意記述データベースに格納，必要に応じて確認しながらシステムを運用し，サービスの継続を考え，常に説明責任が遂行できるようにしておくことである。各ステークホルダは自らが所掌する部分（システム，運用等）について，この DEOS ループを円滑にまわすように考え続けなければならない。

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，統合システムの安全規格
  - ISO 13482：サービスロボット安全規格
  - 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，ソフトウェア関係
  - 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の一つ）
  - システムアーキテクチャ：ISO/IEC/IEEE 42010: Architecture description
  - ライフサイクルマネジメント：ISO/IEC/IEEE 15288
  - SoS 関係
    - ISO/IEC/IEEE 21839: System of systems (SoS) considerations in life cycle stages of a system
    - ISO/IEC/IEEE 21840: Guidelines for the utilization of ISO/IEC/IEEE 15288 in the context of System of Systems (SoS) Engineering
    - ISO/IEC/IEEE 21841: Taxonomy of System of Systems
  - ソフトウェア工学：ISO/IEC JTC1 SC7
    - ISO/IEC 25000（SQuaRE）シリーズ，ISO/IEC 12207 など
  - データ関係
    - ISO 8000 シリーズ，ISO/IEC 5259 シリーズ等
- 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：機械安全・機能安全 ISO 12100，ISO 13894-1，-2, IEC 61508，IEC 62061 など
  - セキュリティ：IEC 62443 シリーズ，IEC 15408 シリーズ，ISO/IEC 27000 シリーズなど
  - プライバシー：ISO/IEC 27701 など

“System of Systems Operational Guidelines: General Edition”

Hiroki Takamura[1)], Hiroshi Yamamoto[2)], Mitsuyuki Inaba[3)], Nozomi Yamada[4)], Koutaro Oba[5)], Takuya Hihara[6)], Satoshi Goto[7)], Hiroyuki Tomiyama[8)], Akio Arakawa[9)], Tetsutaro Uehara[10)], Hiroki Habuka[11)], Kei Takahashi[12)], Tatsuya Kume[13)], Akio Tokuda[14)]

Abstract:

This study summarizes the outcomes of the NEDO-funded project commissioned to Ritsumeikan University: *“FY2022–FY2024 Digital Infrastructure Development for Industrial DX: Research and Development on Mechanisms to Ensure Safety and Reliability in Complex System Integration / Research and Development on Digital Infrastructure and Governance for Balancing Safety, Reliability, and Innovation in the SoS Era.”*

Specifically, it presents the “SoS Operational Guidelines,” designed to ensure safety, ethical integrity, and institutional validity for the smooth social implementation of services based on the System of Systems (SoS) framework. Leveraging a living lab-centered demonstration environment, Ritsumeikan University independently developed concrete and practical guidelines, repeatedly tested and revised them, and sought to build an open operational model for society.

In addition, the project actively aligned with external frameworks such as AI Business Operator Guidelines and the Certification System for Public Digital Platform Operators, verifying consistency with these systems to ensure the effectiveness of the guidelines. Furthermore, to guarantee that stakeholders can fully understand and apply the guidelines, the team proactively designed, developed, and published learning content, while also establishing an educational support mechanism.

Keywords:

System of Systems, Digital Transformation, agile governance, multi-stakeholder, social acceptance, Value Structuring Notation

1) Deputy Counselor, Japan Quality Assurance Organization 2) Professor, College of Information Science and Engineering, Ritsumeikan University 3) Professor, College of Policy Science, Ritsumeikan University 4) Professor, College of Law, Ritsumeikan University 5) Professor, Research Organization of Open Innovation and Collaboration, Ritsumeikan University 6) Specially Appointed Assistant Professor, The Research Center on Ethical, Legal, and Social Issues, Osaka University 7) Professor, College of Business Administration, Ritsumeikan University 8) Professor, College of Science and Engineering, Ritsumeikan University 9) CEO, Primal Colors LLC. 10) Professor, College of Information Science and Engineering, Ritsumeikan University 11) CEO, Smart Governance Ltd. 12) Attorney, Kollect Kyoto Law Office 13) Administrative Manager, Office of Purchasing and Contracts, Division of Financial Affairs, Ritsumeikan University 14) Professor, College of Business Administration, Ritsumeikan University