

令和2年度省エネルギー等に関する国際標準の獲得・普及促進事業
(国際ルールインテリジェンスに関する調査 (システムオブシステムズの安全性・信頼性確保))

報告書

令和3年3月31日

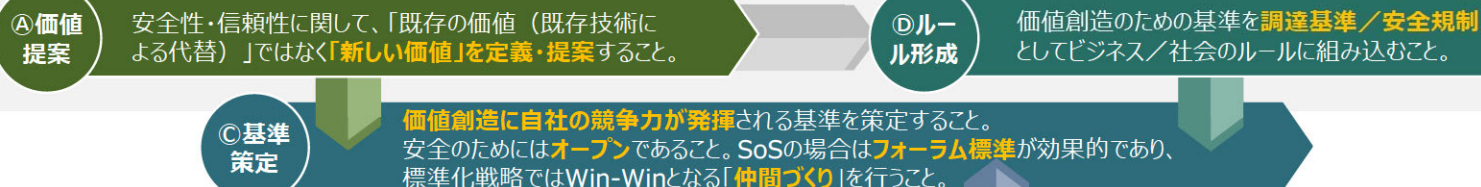
 株式会社三菱総合研究所

 **DEOS**  **astamuse**
company

報告書概要

Society5.0時代のシステムオブシステムズという新たな領域における安全性・信頼性に関する技術候補及び価値創造戦略の検討を行った。

国際標準化・価値創造戦略の検討



⑦競争力確保 競争力の源泉を特定（技術、マネジメントスタイル、価値観・ブランド、関係性）すること。対象テーマごとに課題解決に資する**日本の競争力の特定・創出を行うことは今後の課題**

SoSソリューション例

	①ヘルス&モビリティ	②IoTホーム	③HCD	④防災
特徴	モビリティとヘルスシステムという二つの独立なサブシステム間での協調的な安全性・信頼性の実現	家庭に導入される様々な住宅・家電システム等のサブシステム間での協調的な安全性・信頼性の実現	人間の属人的な特徴のばらつきによる意図しない安全性低下・信頼性低下の防止のためのしくみ	社会に導入されている様々なサブシステム間における、災害時の協調・連携のための機能
イメージ図				
価値提案	ヘルスシティ／シルバーシティ	安全な住まい	多様性・ダイバーシティ・人権	レジリエント
ルール形成 ステークホルダー	スマートシティ調達基準 デベロッパー	製品のマーク制度 メーカー（住宅、家電、）	（SDG's、国連）	スマートシティ調達基準、デベロッパー、JICA、ADB、UNDRR、JBP等
標準化	ISO26262, ISO/DIS21448 IEC62853	IEC 63168、(IoT住宅版SOTIF) IEC62853	ISO 13407, ISO9241シリーズ IEC62853	ISO 37123, ISO28000シリーズ ISO/TC268/SC1/WG6、 ISO/TC292
競争力	今後技術実証	今後技術実証	今後技術実証	ソリューションリストから選定

SoS要素技術

- ①安全要求定義／安全性解析技術 ②リアルタイムテスト技術 ③モジュラー化技術 ④攻撃防御モデル技術
⑤ロバスト制御技術 ⑥システムズレジリエンス技術 ⑦ホワイトボックス型AI 技術 ⑧ヒューマンファクター技術

スマートシティでの例



背景・目的

我が国が提唱するSociety5.0は「サイバー空間とフィジカル空間を高度に融合させたシステム」を前提としているように、我々の社会において、サイバー空間は、もはやリアルな空間に従属するものではなく、リアルな空間と対をなすもう一つの世界となりつつある。

このようなサイバー空間を構成するシステムについては、これまでのところ、単体のシステムを対象に安全性・信頼性に関する検討がなされてきた。他方で、Society5.0においては、データを介して異なるシステム同士が複雑につながることで、設計段階では予見しえない領域が拡大するため、単体では安全性・信頼性が確保されたシステムであっても、それらをつなげた際に予期しない挙動を行うようなケースも想定される。このため、今後、益々システムのコネクティ化が進む中においては、システム単体の安全性・信頼性のみならず、つながったシステム全体（システムオブシステムズ）としての安全性・信頼性を実現することが不可欠となる。サイバー空間とフィジカル空間とが融合し、ローカルなアクターの行為が国境を越えてフィジカル空間上に多大な影響を及ぼすようになると考えられるSociety5.0において、サイバー空間上のシステムの安全性・信頼性について国際的に統一的な標準を策定することは必要不可欠である。

また、これまでの機能安全に関する国際標準への対応においては、標準検討の中心を担った欧州の事業者がその後の標準対応も効率的に進められただけではなく、欧州各国が規制に国際標準を取り込むなど、バリューチェーン全体を通じたルール形成戦略を展開することで、実質的に欧州が関連する国際市場をリードする状況が生まれている。こうした状況に鑑みると、新たな領域において国際標準の策定から規制等との連携まで一貫して我が国が主導して検討を行うことは、Society5.0における日本企業の競争優位を実現する上で必須である。

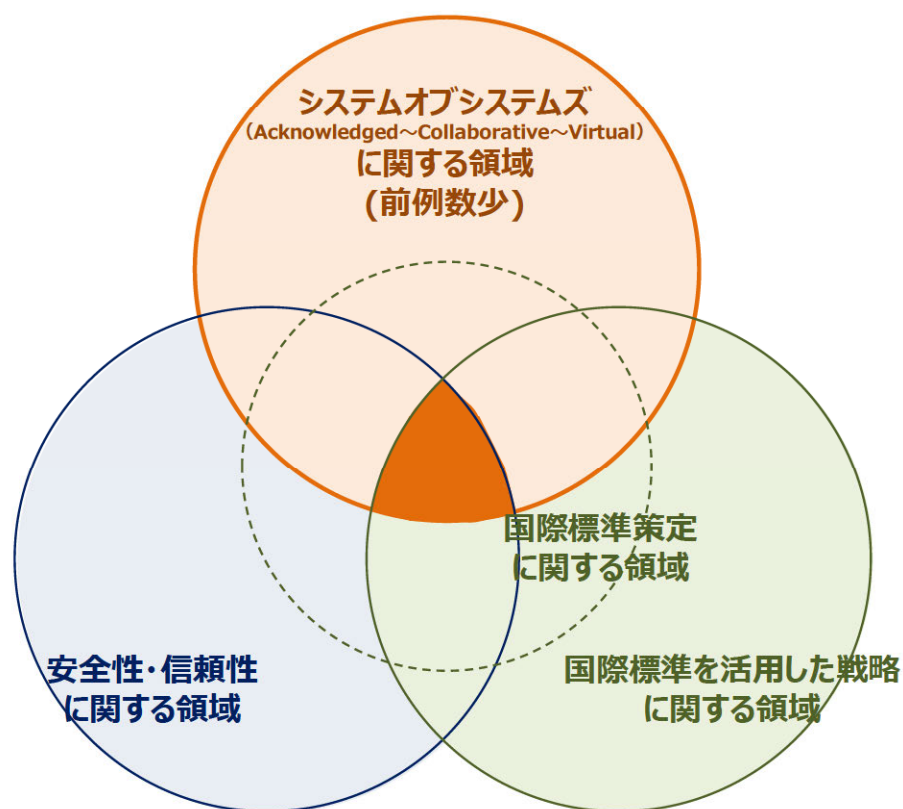
本検討にあたっては、異なるシステム同士がつながったシステム全体の安全性・信頼性を説明する仕組みを検討するものとする。

なお、業務に関しては、第2章「2. システムオブシステムズの安全性・信頼性の実現に向けた産業分野の検討」は一般社団法人 ディペンダビリティ技術推進協会、第1章の技術調査部分（「システムオブシステムズの安全性・信頼性担保に関する技術調査」に相当する内容、詳細は添付資料2）は株式会社アスタミューゼ、全体の取りまとめを三菱総合研究所が担当した。

検討スコープ^o

●本調査業務のスコープを以下に示す。

- Society5.0時代の「多くのシステムが繋がっていく社会（System of Systems）」を想定
- Society5.0時代における安全性・総合信頼性のあり方を検討
- Society5.0時代における安全性・総合信頼性に資する国際標準化の活用方法を検討（標準策定に留まらず）



目次構成

1. システムオブシステムズにおける今後の課題と関連取組事例	5
1. 1 システムオブシステムズに関する概念と課題の整理	5
1. 2 システムオブシステムズ及びシステム運用の工夫に関する先行研究及び先進技術の事例調査	16
2. システムオブシステムズの安全性・信頼性の実現に向けた産業分野の検討	70
2. 1 システムオブシステムズの安全性・信頼性の国際ルール形成を通じて競争優位を実現する産業分野の選定	70
2. 2 システムオブシステムズの安全性・信頼性の実現に向けた産業分野や技術の事例調査及びロードマップの策定	76
3. システムオブシステムズの安全性・信頼性の実現に向けた国際標準化戦略の検討	121
3. 1 国際標準を軸にした各国における戦略展開の調査、及びルール普及におけるポイント・課題の整理	121
3. 2 国際ルール形成を通じて競争優位を実現するのに適した産業分野や国際標準化戦略の検討	145
3. 3 国際標準等を活用したルール形成によって期待される経済的効果及びエネルギー効率化効果の試算例	159
4. 安全性・信頼性が担保されたシステムオブシステムズの実装に向けた提言	165
添付資料	
添付1 システムオブシステムズに関する補足資料	172
添付2 システムオブシステムズの安全性・信頼性担保に関する技術調査	182

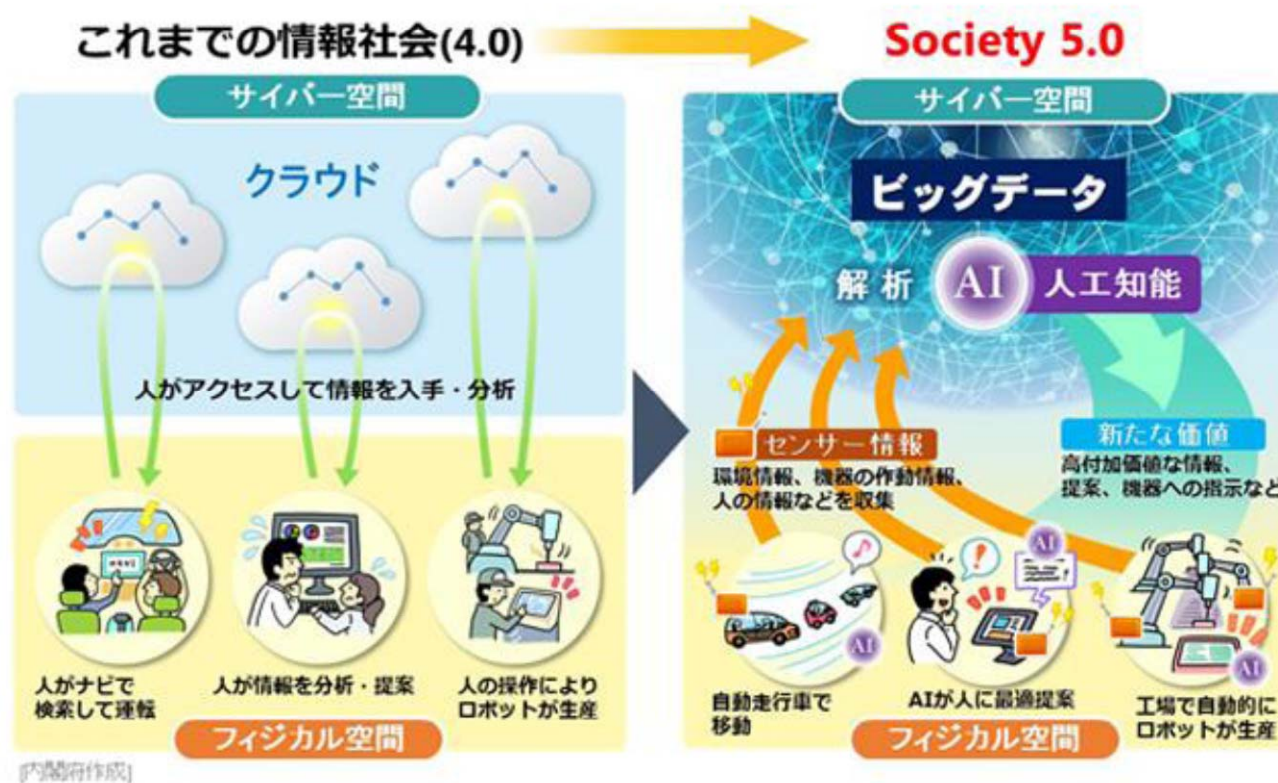
なお本報告書の出展について注記が無いものについては2021年3月に閲覧・確認した。

1. システムオブシステムズにおける今後の課題と関連取組事例

1. 1 システムオブシステムズに関する概念と課題の整理

Society 4.0の基本的な考え方と課題

- これまでの情報社会では、人がモノを使いこなすことで利便性が向上するという思想であった。サイバー空間とフィジカル空間で連携するが、個々のサービスは独立で開発・運用されていた。また、開発時の想定（制約設定）を中心とするモノづくりであった。
- このような社会では、サービスをまたぐ知識や情報の連携が困難であり、膨大な情報、複雑で多様なサービスを選び使いこなす能力が必要であった。そのため、社会問題の解決に繋がるような新しい技術やサービス（システムの利用を通じて、利用者が得られる体験）が生まれにくい状況が課題であった。



出所) 内閣府「Society5.0」(https://www8.cao.go.jp/cstp/society5_0/)、2021年3月閲覧

システムオブシステムズによるSociety 5.0の実現

- Society 5.0により、モノではなく、人の体験（コト）を中心にサービスを構築する世界となる。
- これにより、個々のシステムは独立して開発、運用されるが、柔軟に連携しながらサービスを実現する「システムオブシステムズ（SoS）によるサービス提供」が実現する。
- サービスのライフサイクル全体で、安全性や信頼性を担保する仕組みがより重要となる。あわせて、Society 5.0の社会的な視点だけでなく、産業、組織（企業・地方公共団体・コミュニティ）、個人に対する具体的な価値提供が必要となる。



**SoSによる
柔軟な
サービス提供**

階層ごとの価値提供

社会レベル

社会問題の解決

産業、組織レベル

利益目標、社会貢献

個人レベル

健康、成長、幸福感、安心、…

出所) IPA「Society5.0を実現するデジタルアーキテクチャ・デザインセンターの戦略」
(https://www.ipa.go.jp/dadc/seminar/pdf/ceatec2020_dadc_strategy_20201022.pdf)、2021年3月閲覧

システムオブシステムズ (SoS) の概念整理

- システムオブシステムズ (SoS) とは、あるシステムを構成するサブシステムがそのままでは達成できないサービスを提供するために、相互的に作用するサブシステムの集合体である (ISO/IEC/IEEE21841:2019)。
- ISO/IEC/IEEE21841:2019を踏まえると以下の4つに分類される (SoSでないSystemを“Monolithic System”と呼ぶ)。システム構成の自由度が高まるほど、安全確保 (管理) が難しくなる。

SoSの種類 (*-SoS)	定義 (ISO/IEC/IEEE21841:2019を意識)	目的	管理者	目的/管 理者	システム構 成自由度	安全確保 の難しさ	事例
Directed 統率された 中央集権的	- 共通の目的を達成するために構築・管理される - 各システムは個別に運用能力をもつが、通常運用時は、SoSに従属して共通の目的に従って動く	管理的存在が設定	存在する	SoSと独立していない	低	容易	IoT住宅 軍用システム
Acknowledged 承認された	- 全体として目標、管理者、資源を持つ - 各システムも所有権、目標、資金などを持つ - SoSと各システム間での協調的合意に基づいて変化	管理的存在が設定	存在する	SoSと独立している			モビリティ スマートグリッド IoT住宅
Collaborative 協調的	- 全体で合意された目的のために各システムが自発的に作用し合う - 個々のシステムが協調して、サービスをどう提供するか拒否かを決め、一貫性を遵守・保守する方法を提供する	相互作用で合意	存在しない (特定されない)	SoSと独立している			国際金融システム 鉄道システム
Virtual 仮想的	- 中央管理機関や、全体で合意された目的がない - 大規模な動きとして見えるが、表面には現れない仕組みで管理される	存在しない	存在しない	SoSと独立している	高	困難	道路交通 社会活動

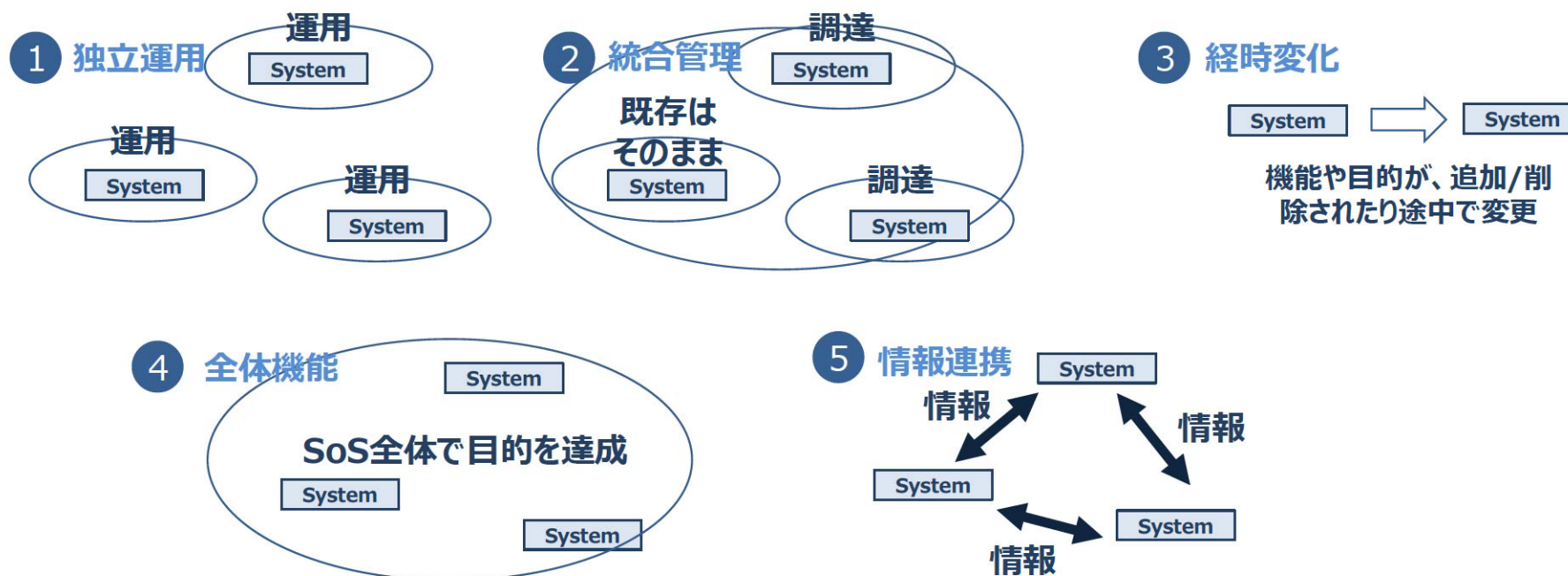
※本報告書では、Directed/Acknowledged/Collaborative/Virtual System of SystemsをそれぞれD-SoS/A-SoS/C-SoS/V-SoS、SoSではないMonolithic SystemをM-SoSと適宜略記する。

出所) ISO/IEC/IEEE21841:2019, Mark W. Maier (1998) “Architecting Principles for Systems-of-Systems”
IoT時代のシステム品質 (https://www.juse.or.jp/sqip/community/bucyo/8/files/shiryou_kouen.pdf)、2021年1月5日閲覧

システムオブシステムズ (SoS) の概念整理

- システムオブシステムズ (SoS) とは、以下の5つの特徴をもったシステムのことをいう。

1. 運用の独立性: SoSの構成システムは個別に運用
 2. 管理の独立性: 構成システムは別々に調達され、統合される。しかし、運用中の構成システムはそのまま運用
 3. 進化的開発: 機能や目的が、追加/削除されたり途中で変更されるなど、開発とシステムが進化的に変化
 4. 創発的振る舞い: 構成システム単独では実現できない目的をSoSとして実現
 5. 地理的な分散: 構成システムが離れており、構成システム間で質量やエネルギーの物理量ではなく、情報を交換
- ※6. データ集約、7. 異質性を定義に組み込んでいる文献もある



出所) IoT時代のシステム品質 (https://www.juse.or.jp/sqip/community/bucyo/8/files/shiryou_kouen.pdf)、2021年1月5日閲覧 等をもとに作成

システムオブシステムズ (SoS) の概念整理

- Monolithic System (M-Sys) と比較したシステムオブシステムズの特徴として、他にも以下のような整理がある。(ISO/IEC/IEEE21840:2019)
- 固定的な定義があるわけではないが、複数のステークホルダ・目的の存在、自律性と管理構造の独立性、情報連携、創発的振る舞いは共通。

SoSが持っている特徴

- ステークホルダが複数（興味が対立することもある）
- 目的が複数（対立することもある）
- 管理構造が独立しており、責任の所在も不明確
- 複数の運用プロパティ
- ライフサイクルも複数、調達もバラバラ
- 複数のオーナーがそれぞれのリソースの意思決定を実施

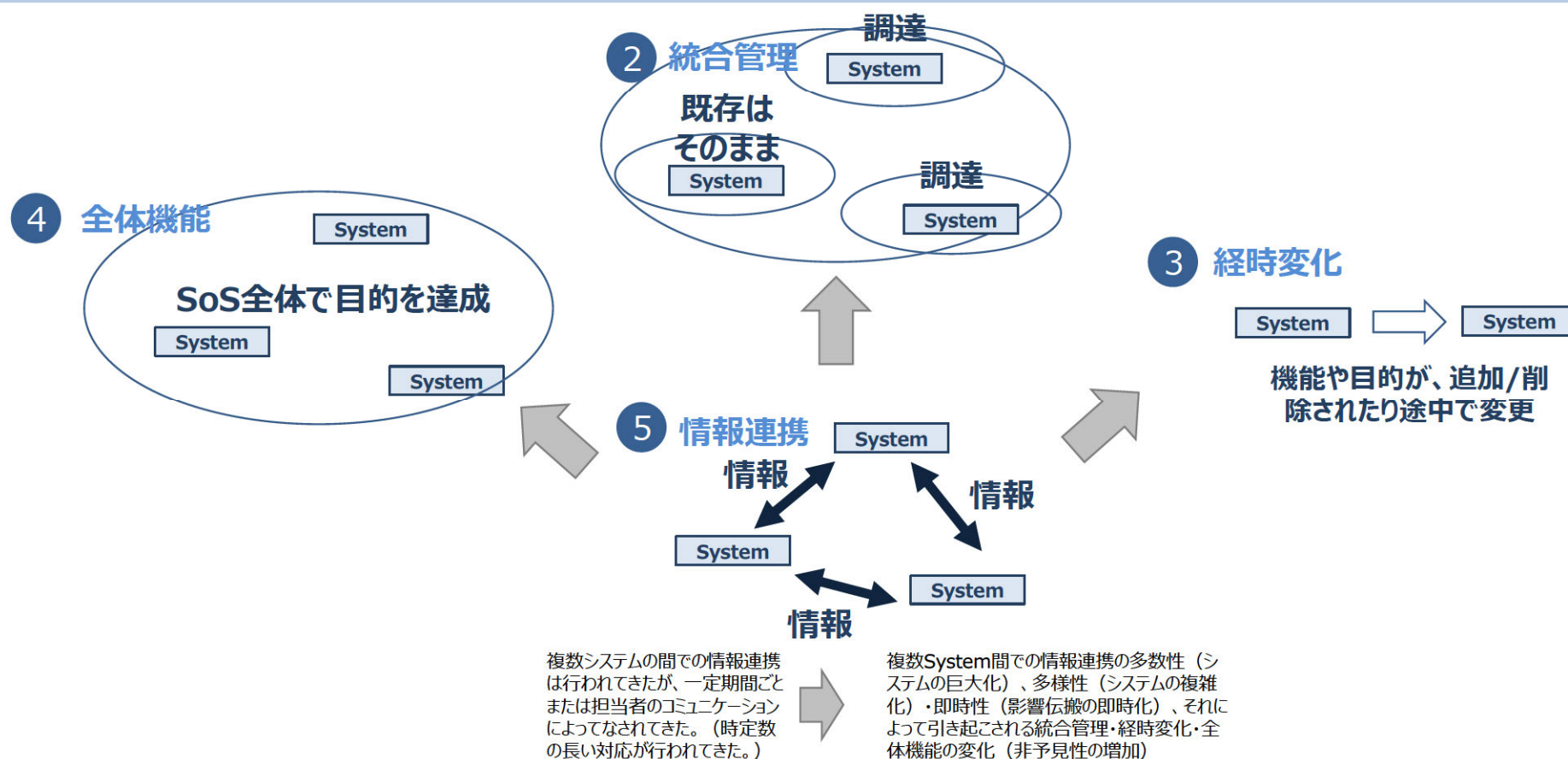
SoSが持っている特徴

- Autonomy：構成システムは自律的に動きつつ、SoSの目的を満たす。
- Belonging：構成システムは統合管理されているものもあれば、SoSを認識していないものもある。属し方はさまざま。
- Connectivity：SoSの可能性を高めるために構成システムがつながっており刻々と変化する。
- Diversity：自律性、所属、オープンコネクティビティによってダイバーシティが生まれる。
- Emergence：創発的なふるまいをする。

出所) ISO/IEC/IEEE21840:2019

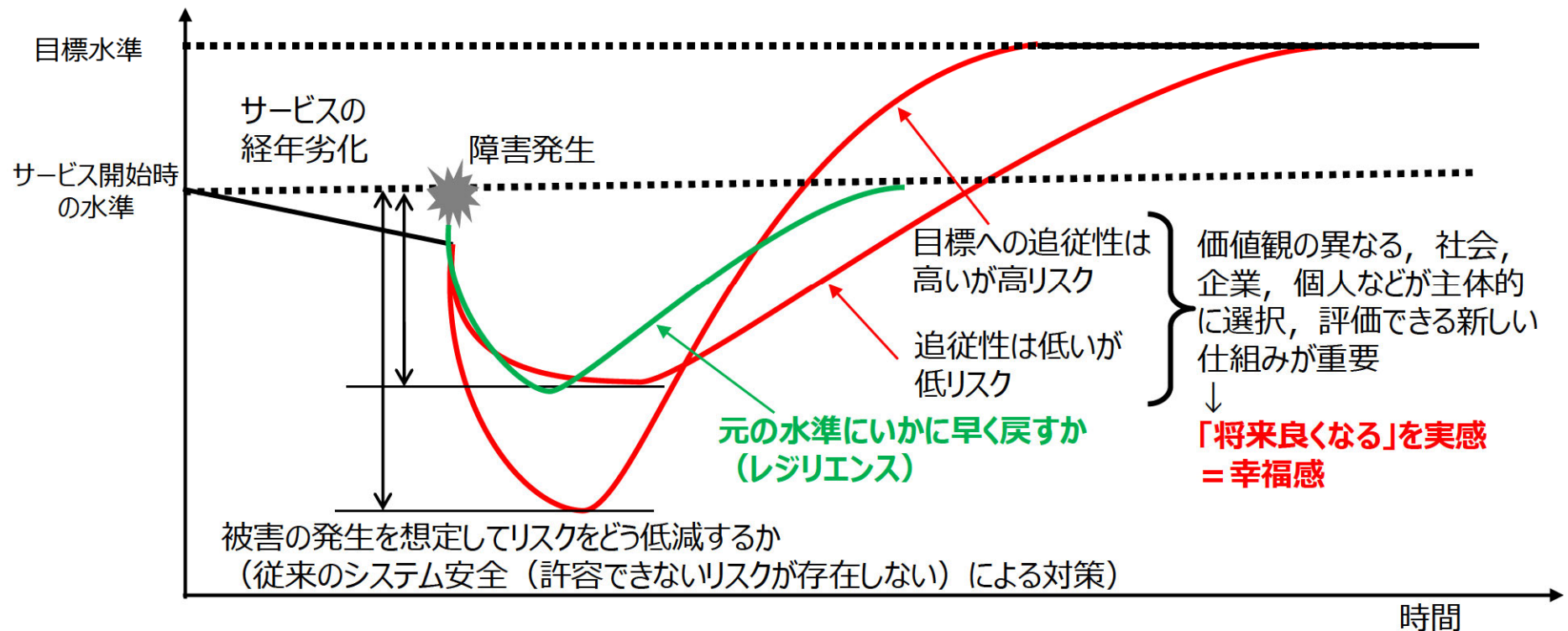
Society5.0で想定すべきシステムオブシステムズ (SoS)

- システムオブシステムズの特徴自体はこれまでの産業界及び社会現象の中でも既にみられている。
- Society5.0という文脈において特に注目すべきシステムオブシステムズの特徴として「複数システム間での情報連携の多数性（システムの巨大化）、多様性（システムの複雑化）・即時性（影響伝搬の即時化）、それによって引き起こされる統合管理・経時変化・全体機能の変化（非予見性の増加）」に注目し分析整理を行う。



目指す方向性（モノ中心からコト中心の安全へのポイント・新たな評価軸）

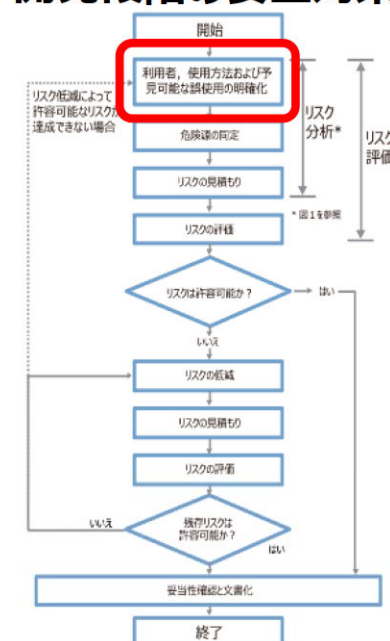
- システムオブシステムズの経時変化や複数の目的が混在する中で、目標とする水準に近づいていることを実感できる社会のためには3つのポイントが重要になる。
 - サービス提供者、システム開発者、利用者などのステークホルダが関与すること
 - ステークホルダ間で目標水準とそこに近づく戦略（受容リスク）を合意すること
 - 経過及び結果に関する説明責任を継続的に果たすこと
- 上記より、（システムオブシステムズにより実現される）サービスに求められる品質特性も、「レジリエンス」のような「時間軸」を加えたものが適切になる可能性がある。



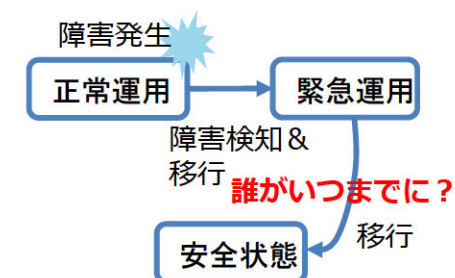
システムオブシステムズによって新たに発生しうるシステム開発上の技術的課題

- システムオブシステムズおよびそれを構成するシステムの開発段階では、以下の課題が生じる。
 - システム構成や動作目的（機能やサービス）の変更や追加に伴う、リスクの事前想定が困難
 - 開発時のリスク分析と評価に基づく安全対策だけでは、新たな障害に対応困難
 - 人手による将来予測に基づく開発の負担が大きい（網羅的なリスク分析、安全設計、テスト、品質確保、トレーサビリティ）
- システムの運用段階では以下の課題が生じる。
 - サービスを実現する一部のシステム障害の把握とその原因追求に時間が掛かり、全体の安全を担保する即時的な対応が困難
 - サービスを構成するシステム構成の複雑化・変化により、障害検知やサービス状態移行の時間保証と責任が曖昧に（保証からベストエフォートに？）
 - 事故や障害発生後、短期間で責任分解できず、裁判や保険等の仕組みの維持が困難（AI利用で難易度がさらに向上）

開発段階の安全対策



運用段階の安全対策



システムオブシステムズ (SoS)の安全性・信頼性担保における課題

- システムオブシステムズ (SoS) の安全性・信頼性担保における課題を整理した。①～④のほか、サイバー・フィジカルシステムの安全性担保における課題 (SoSになると課題が深刻化) として⑤⑥が挙げられる。

① SoSとしてのリスク想定困難性

- ✓ 個別システムの安全の積み上げではSoS全体の安全を確保するのは困難
- ✓ 外部環境の動的なシステムと接続される場合、予期できなかった新たな危険性が発生する可能性

② 運用時のシステムの変化への対応の困難性 (事前想定困難性)

- ✓ リスクの事前想定は困難であるため、運用段階 (ライフサイクル全体) での安全担保が必要

③ リスク事象発生時の対応の困難性 (→役割分担・責任の所在の不明確さ)

- ✓ システム複雑化に伴いシステム障害の把握とその原因追求が困難
- ✓ 障害検知や安全状態への移行に関する時間や責任が曖昧

④ 安全に関する目標設定・共有の困難性 (→役割分担・責任の所在の不明確さ)

- ✓ SoSにおける危険の許容「許された危険」の法規的な扱い方が不明確
- ✓ ステークホルダごとのメンタルモデルギャップ (リスク) の増大への対応が必要

⑤ AIによる判断の妥当性評価

⑥ サイバーセキュリティ担保の困難性

1. 1小括 SoSの特徴と目指す方向性・今後に向けた課題

Society5.0時代の特徴を理解するため、SoSの特徴から、目指すべき方向性と課題の整理を行った。

※本報告書では、Directed/Acknowledged/Collaborative/Virtual System of SystemsをそれぞれD-SoS/A-SoS/C-SoS/V-SoS、SoSではないMonolithic SystemをM-SoSと適宜略記する。

SoSの特徴

* - SoS	定義 (ISO/IEC/IEEE21841:2019を参照)	目的	管理者	目的/管理者	システム構成 自由度	安全確保 の難しさ	事例
Directed 統率された 中央集権的	- 共通の目的を達成するために構築・管理される - 各システムは個別に運用能力をもつが、通常運用時は、SoSに従属して共通の目的に従って動く	管理的存在が設定	存在する	SoSと独立していない	低	容易	IoT住宅 軍用システム
Acknowledged 承認された	- 全体として目標、管理者、資源を持つ - 各システムも所有者、目標、資金などを持つ - SoSと各システム間での協調的合意に基いて変化	管理的存在が設定	存在する	SoSと独立している			モビリティ スマートグリッド IoT住宅
Collaborative 協調的	- 全体で合意された目的のために、各システムが自律的に作用し合う - 個々のシステムが協調し、サービスをどう提供するか拒否かを決め、一貫性を遵守・保守する方法を提供する	相互作用で合意	存在しない (特定されない)	SoSと独立している			国際金融 システム 鉄道システム
Virtual 仮想的	- 中央管理機関や、全体で合意された目的がない - 大規模な動きとして見えるが、表面には現れない仕組みで管理される	存在しない	存在しない	SoSと独立している	高	困難	道路交通 社会活動

1. 運用の独立性

2. 管理の独立性

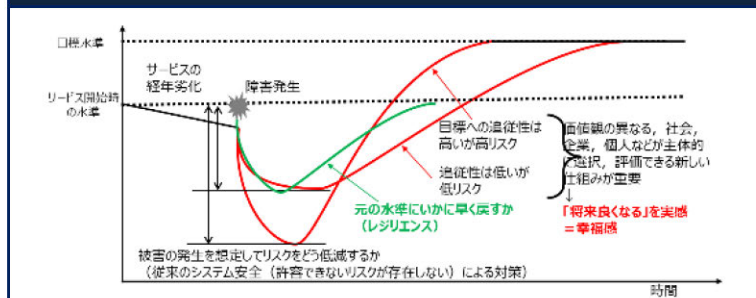
3. 進化的開発

4. 創発的振る舞い

5. 地理的な分散

目指す方向性

- サービス提供者、システム開発者、利用者などのステークホルダが関与すること
- ステークホルダ間で目標水準とそこに近づく戦略（受容リスク）を合意すること
- 経過及び結果に関する説明責任を継続的に果たすこと



SoSの特徴と安全性・信頼性担保に向けた課題

- ① SoSとしてのリスク想定の高リスク
- ② 運用時のシステムの変化への対応の高リスク
- ③ リスク事象発生時の対応の高リスク
- ④ 安全に関する目標設定・認識共有の高リスク
- ⑤ AIによる判断の妥当性評価
- ⑥ サイバーセキュリティ担保の高リスク

1．システムオブシステムズにおける今後の課題と関連取組事例

1．2 システムオブシステムズや、システム運用の工夫に関する先行研究**の調査(1イ)（取組事例）**

システムオブシステムズにおける今後の課題と解決のアプローチ

- 1.1で整理した課題への技術的・マネジメント的な対策、及び分野別の事例を整理した。
- これらの課題を踏まえ、日本の強みとなりうる課題・解決策×分野事例を整理、標準化検討に繋げる。

課題	概要	解決策（技術）	解決策（マネジメント）	【参考】分野事例
①全体リスク想定 の困難性	- 個別システムの安全の積み上げではSoS全体の安全を確保するのは困難 - 外部環境の動的なシステムと接続される場合、予期できなかった新たな危険性が発生する可能性		①安全要求定義／安全性解析 ②リアルタイムテスト技術 ③モジュール化 ⑤ロバスト制御 ⑥システムズレジリエンス ⑦ホワイトボックス化 ④攻撃防御モデル ⑧ヒューマンファクター ①SOTIF ②STAMP ③FRAM ④DEOSプロセス ⑤HCD ⑥DSM ⑦CPSF	電力交通医療住宅家電 ①サービスロボット JIS Y1001等 ②自動運転 Pegasus Project
②運用時の変化 対応の困難性	システム構成の変更や動作目的の変更によるリスクの事前想定は困難であるため、運用段階（ライフサイクル全体）での安全担保が必要			
③運用時の障害 対応の困難性	- システム複雑化に伴いシステム障害の把握とその原因追求が困難 - 障害検知や安全状態への移行に関する時間や責任が曖昧			
④ユーザ・ユース ケース想定 の困難性	- SoSにおける危険の許容「許された危険」の法規的な扱い方が不明確 - ステークホルダごとのメンタルモデルギャップ（リスク）の増大への対応が必要			
⑤AIの挙動の 不確実性	AIの不確実性への対応はSoSになるとさらに課題として顕在化			
⑥サイバー攻撃 への対処	サイバー攻撃への対処はSoSになるとさらに課題として顕在化			

課題およびその解決策の項目はそれぞれ重複するものが多い。また技術・マネジメントも互いに関係しているものも多い。

技術的な解決策

システムオブシステムズ関連の研究領域の構造化

- 前節で整理したシステムオブシステムズの安全性・信頼性担保における課題から研究領域を構造化し、8つの分野を設定した。
- システム全体のリスクの想定はユーザ・ユースケース想定を含み、また、運用時のシステムの変化には障害対応、及びサイバーセキュリティを含む。
- システムオブシステムズ関連の研究動向調査（特許、論文、グラント）を実施し、研究要素のキーワードを抽出するとともにその概要をまとめた。

大分類	1 システム全体のリスクの 想定困難性	2 運用時のシステムの 変化への対応困難性	3 AIによる 判断の妥当性
	① 安全要求定義／安全性解析技術 ② リアルタイムテスト技術 ⑧ ヒューマンファクターの考慮＊	③ モジュラー化技術 ④ 攻撃防御モデル技術 ⑤ ロバスト制御技術 ⑥ システムレジリエンス技術	⑦ ホワイトボックス型AI技術
中分類			
(課題)	① SoSとしてのリスク想定困難性	② 運用時のシステムの変化への対応困難性	⑤ AIによる判断の妥当性評価
	④ 安全に関する目標設定・認識共有の困難性	③ リスク事象発生時の対応困難性	
		⑥ サイバーセキュリティ担保の困難性	

①システム全体のリスクの想定（①安全要求定義、⑧ヒューマンファクターの考慮）

- システムオブシステムズでは、故障の社会的な影響も大きいことから、サブシステムの故障が他のサブシステムに影響しないよう分離した制御設計（故障許容設計や故障伝播抑制設計）、複数の専門家による依存関係の明示化・整合性確保が必要な項目の明確化が重要である。
- あわせて、システムの一要素として人間も考慮し、その特性や振る舞い、さらには意図の変化等を把握するためのヒューマンファクターの分析技術も重要である。

概要

具体例

1

安全要求定義
／安全性解析
技術

- ・ システム同士の故障許容設計や故障伝播抑制設計、複数の専門家の連携などの技術が含まれる
- ・ システムオブシステムズでは、複雑にシステムが絡み合い大きなシステムを構成しており、故障の社会的な影響も大きいことから、安全を確保するため以下のような技術が存在
 - ・ あるサブシステムの故障が他のサブシステムに影響しないよう、分離した制御設計
 - ・ 複数の専門家による依存関係の明示化・整合性確保が必要な項目の明確化
 - ・ STAMP/STPAやFTAなど確立された手法の適用から、新しい手法までが含まれる

- ・ 自動車のシステムやハードウェアの一部の故障が全体に波及することを抑止する技術
- ・ 一部の電線の故障が波及して大規模停電を誘発することを抑制する技術

8

ヒューマン
ファクターの
考慮

- ・ ヒューマンファクターとはシステムの安全性や有効性に影響を与える人間のふるまいや特性のこと
 - ・ AcciMaps、STAMP、Human Factors Analysis Classification System (HFACS)、Event Analysis of Systemic Teamwork (EAST)などの手法を用いて分析される

- ・ 高度道路交通システムにおける自動運転車と非自動運転車の共存
- ・ 危険な製造現場におけるロボットと人間の協調作業

①システム全体のリスクの想定（②リアルタイムテスト技術）

- システムオブシステムズにおいて創発的に発生するありとあらゆる事象に対して、システム実機ですべてのシナリオの検証を行うことは難しい。そのため、実機を仮想的に再現した環境でシミュレーションを行うことで、実機では困難な危険なケースのテストを網羅的に実施することができる。
- これをリアルタイムにシミュレーションを行うことで、設計段階のみならず運用段階でもフィードバックを行うことが可能となる。

概要

具体例

2

リアルタイム
テスト技術

- Hardware-in-the-Loop Simulation、Processor-in-the-Loop Simulationなどのシミュレーション技術が含まれる
- 実機を用いることなく、**実機を仮想的に再現した環境でシミュレーション**を行うことで、実機では困難な危険なケースのテストが可能
- また、不具合が発生する条件を把握し、不具合の出る環境を再現して繰り返しテストが可能
- 結果、ユーザーがデザインした制御モデルを迅速に実機テスト環境へと移行させ、実機テストを行うことが可能

- 電力網や石油・ガス、石油化学、水処理、原子力などのインフラにおいて、性能やサイバー攻撃の影響を知り、設計にフィードバックするためのシミュレーション技術

②運用時のシステムの変化への対応（③モジュール化、④攻撃防御モデル）

- システムオブシステムズでは、システム構成を柔軟に変化させることが必要になる。そのため、プラットフォームを構築する技術や、サブシステム間を接続する技術、また、サブシステム間の矛盾の把握や解消のための技術が重要である。
- また、ネットワーク化された大規模制御系に対する悪意のあるサイバー攻撃に対する対応も重要である。

概要

具体例

3

モジュール化 技術

- ・ プラットフォームの構築やサブシステム間の接続の技術が含まれる
- ・ システムオブシステムズではその定義により、運用開始後にサブシステムの追加が想定されるが、それらサブシステム間で挙動に矛盾があると、システム全体が不安定となる。そこで、プラットフォームを構築する技術や、**サブシステム間を接続する技術**、また、**サブシステム間の矛盾の把握や解消**のための技術が必要となる

- ・ 車両やデジタルホームのアプリケーションを構築するために必要なサポートを提供するプラットフォームの構築
- ・ システムオブシステムズのメカニズムを分析するゲーム理論

4

攻撃防御 モデル技術

- ・ システムオブシステムズでは、ネットワーク化された大規模制御系に対する悪意のあるサイバー攻撃に対して、通信や計算量の面で制約される環境においても、**セキュリティレベルや制御性能を保証**する必要がある。攻撃や防御のモデルを構築し、定量化する技術が存在
- ・ 多層フレームワークの構築技術、ブロックチェーン等の技術はセキュリティそのものに活用されている
- ・ 攻撃／防御のモデルを構築し、リスクの定量化

- ・ サイバーフィジカルシステムの攻撃と防御の間の相互作用のモデル化の研究
- ・ 無人航空機の攻撃を検知し、警告信号を送信するコンピュータプラットフォームの構築

②運用時のシステムの変化への対応（③ロバスト制御、④システムズレジリエンス）

- システムオブシステムズでは、一つのシステムの挙動の不安定性が伝播する可能性があるため、各システムはノイズに対して頑健（ロバスト）である必要がある。また、システムがたとえ故障したとしても、その後素早く回復するためのレジリエントな設計技術等も重要である。

概要

具体例

5

ロバスト制御 技術

- ・ 想定内の入力の揺らぎを制御するもので、ファジィ制御やモデル化誤差などのロバスト制御の技術が含まれる
- ・ システムオブシステムズでは、システムの入出力関係がノイズに対して安定するような設計が重要になる
- ・ 事前に、あり得る環境の全てを把握することは不可能であるが、安全とコストのバランスを考慮しながら、一定レベルはモデルに組み込む必要がある。また、そのモデルと多少異なっても制御性を損なわない制御をする必要がある

- ・ 再生エネルギーが導入された電力システムに対して系統安定度を向上するプラグイン型制御技術

6

システムズ レジリエンス 技術

- ・ 想定外と言えるような大規模な災害や事故が発生した際に、経済的な効率をある程度達成したうえで、システムオブシステムズの安全性および可用性を維持する必要がある
- ・ どこまでを想定内として事前に対策をとり、どこからを事後の対応とするのかという、安全とコストのバランスをとること、システムが壊れないことだけでなく、壊れた後いかに素早く回復するかというレジリエンスの手法が重要となっている
- ・ 大規模災害などを入れ込む計算モデルや、生物学にインスピレーションを得たネットワーク設計の技術が含まれる

- ・ 防災のための社会インフラや、サプライチェーンを含めた生産システムなどを大規模災害時でも使用できるよう設計する技術

③AIによる判断の妥当性（⑦ホワイトボックス型AI技術）

- インプットに対するアウトプットが説明しづらいブラックボックスAIの利用は、システムオブシステムズになるとますますその不確実性が増大するため、安全性担保の観点で説明可能性を高めることは重要である。
- 各変数のモデル挙動に対する寄与度を説明するための技術のほか、大域的な説明性を担保するための大規模シミュレーション技術も含む。

概要

7

ホワイトボ
ックス型AI技術

- AIモデルがデータのどの部分を根拠に結果を出力したのかや、入力と出力の関係性を理解するための技術
- AI技術は、パフォーマンスに優れる反面、モデルが複雑になるため、その解釈性や説明性が損なわれブラックボックス化する傾向にある
- システムオブシステムズにてAIを使用する場合、説明可能なAI（Explainable AI、XAI）・ホワイトボックス型AI技術を使用することが望ましい。主要な技術は以下の通り
 - 1回の予測に対して説明を行う（局所的な説明性）
 - LIME(Local Interpretable Model-agnostic Explanations)
 - SHAP(SHapley Additive exPlanations)
 - LRP(Layer-wise Relevance Propagation)
 - モデルの全般的な挙動を調べる（大域的な説明性）
 - SA(Sensitivity Analysis)

具体例

- 局所的な説明性
交通システムの一部となる自動運転システム。画像認識による交通標識の判別において、その「予測結果が正しいか」でなく、画像中の標識部分の「ピクセルを根拠に判断しているか」まで明らかにする
- 大域的な説明性
ニューラルネットワークを用いた山火事警報システム。
一般的にはブラックボックスであるニューラルネットワークに対して「降雨の発生」「10時間あたり燃料含水率」「月（Month）」が火災リスクに対して影響が大きいという説明性を与えた

【参考事例】①システム全体のリスクの想定（②リアルタイムテスト技術） 等

- 海上ナビゲーションおよび制御システムは個々のソフトウェア集約型サブシステムとセーフティクリティカルサブシステムのSoSであり、システム全体の構成の検証と妥当性確認に課題
- SoSのソフトウェアは運用中に変更される可能性あり、システムレベルでモジュールを変更するには、認証への準拠を再評価する必要あり
- SoSのモジュールを、拡張された安全契約を通じて対応する安全ケース仕様に関連付けて、展開前に変更の影響を検証する方法についてのアプローチ
 - 更新のタイプ（完全、修正、適応）ごとに、再評価する必要のある要素を特定
 - 開発されたアプローチの適用性を評価するために、海上交通警報および衝突回避システム（MTCAS）のセーフティクリティカルモジュールでケーススタディを実施

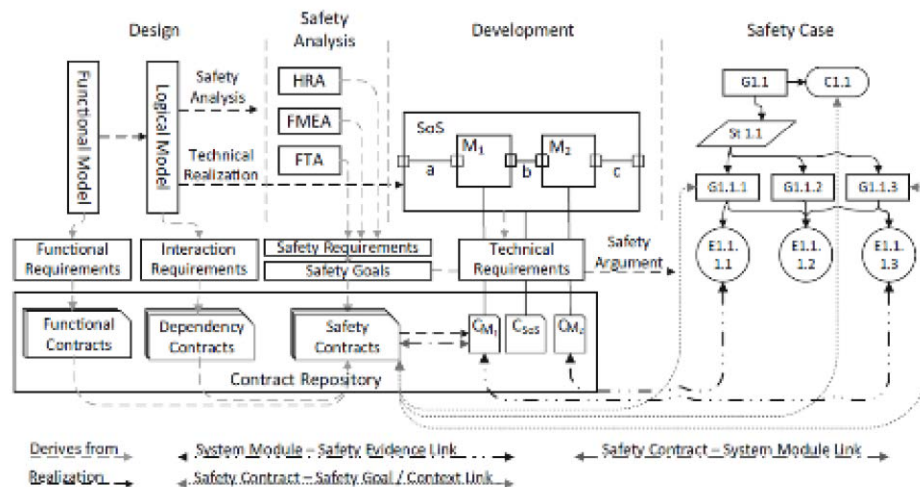


Fig. 3. Linking safety analysis, system development and the safety case via assume/guarantee-contracts

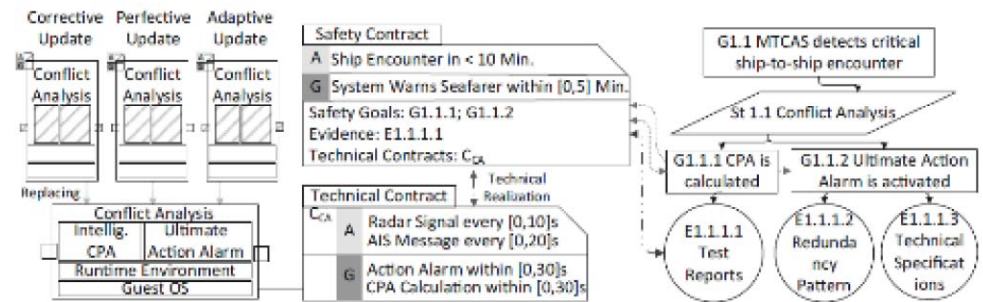


Fig. 5. Bidirectional dependency of conflict analysis module, safety contract and safety case

出所) A. Casimiro et al. (Eds.): SAFECOMP 2020, LNCS 12234, pp. 50–63, 2020. https://doi.org/10.1007/978-3-030-54549-9_4

【参考事例】①システム全体のリスクの想定（⑧ヒューマンファクターの考慮）等

- 自動運転車とその周辺システムを含む交通システム全体をSystem of Systems (SoS) と見なし、そのシステムモデルに基づき導出された安全性要求をもとにGSN (Goal Structuring Notation) によりアシュアランスケース記述を行うことでその妥当性確認を行うとともに、モデル検査を用いて検証を実施。
- モデル検査では、SoSの構成要素である自動運転システムとドライバ間の相互作用に関する安全性要求を検証するためCSP (Communicating Sequential Processes) モデルを利用。



図1 自動運転車を取り巻くSoSの相互接続の検証をもとにしたアシュアランスケース

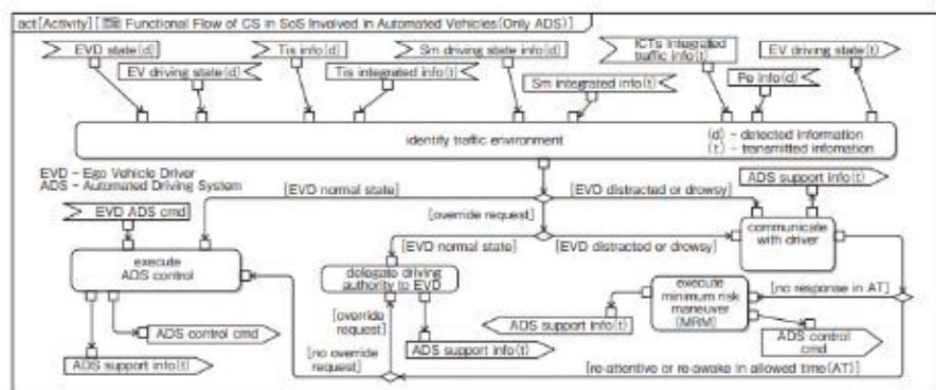


図2 自動運転システムの機能フローを示すアクティビティ図

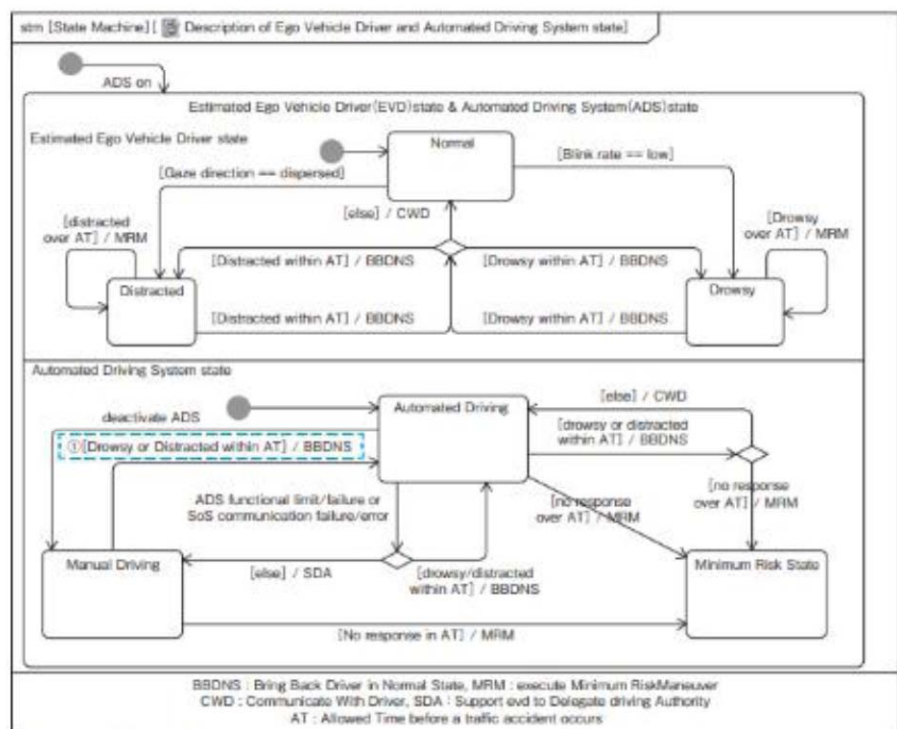
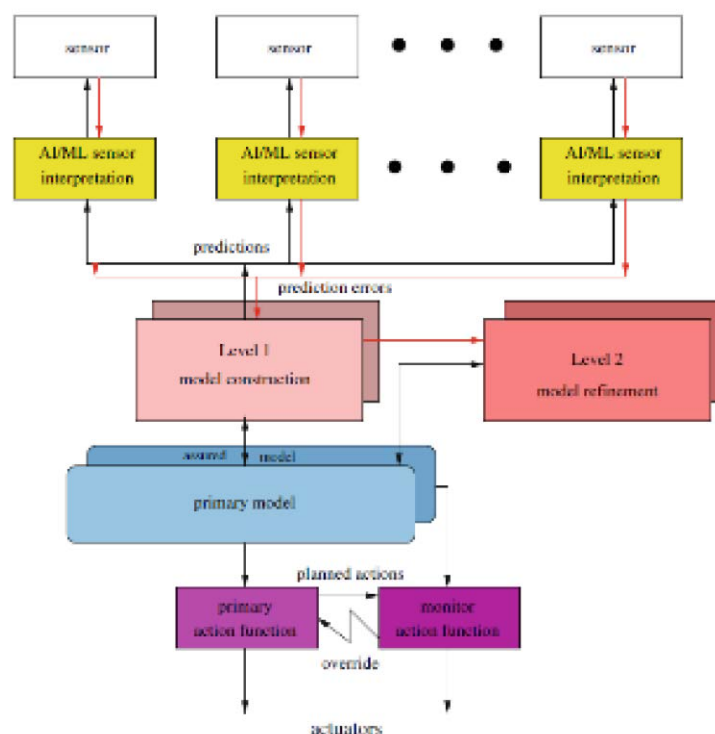


図4 自動運転車を取り巻くSystem of Systemでのドライバと自動運転システムの状態遷移

出所) 木下聡子ほか「自動運転車を取り巻く System of Systemsの安全性要求の妥当性確認と検証」, SEC journal Vol.12 No.4 Mar. 2017

【参考事例】②運用時のシステムの変化への対応（③ロバスト制御）

- 自律システムの「知覚」に使用されるワールドモデル（周辺環境）を構築・維持するためには「**モデルが時間の経過とともに変化する世界の正確な表現であること**」が必要。モデルが与えられた場合、アクションが安全（かつ効果的）であることも必要。
- AIとMLを使用して解釈するセンサーから派生したモデルの精度を確保するためのアーキテクチャと方法を提案。
センサー値からボトムアップにモデルを導出するのではなく、モデルを使用してセンサーの解釈を予測（小さな予測誤差であればモデル更新、大きな誤差であれば感知や解釈のエラー、または世界の予期しない変化として対応）。



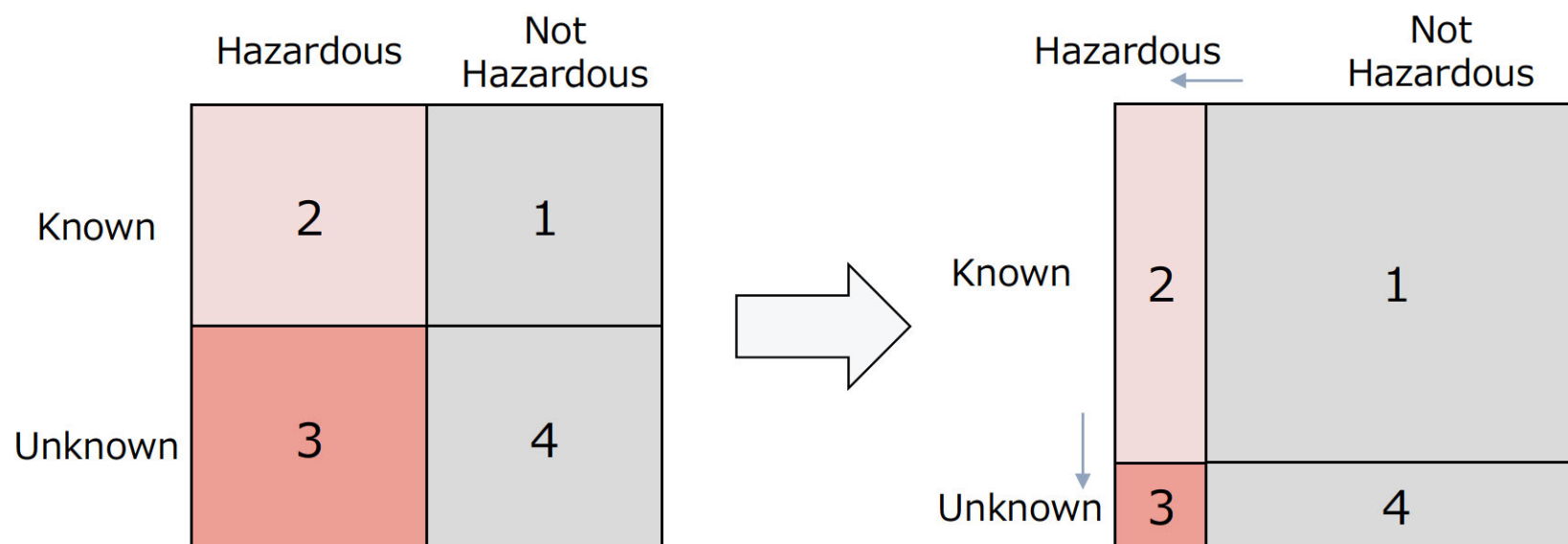
出所) Susmit Jha, John Rushby, Natarajan Shankar, "Model-Centered Assurance for Autonomous Systems", SAFECOMP2020

マネジメント的な解決策①

Safety of the Intended Functionality (ISO/DIS 21448)

Safety of the Intended Functionality (ISO/DIS 21448)

- 故障の回避、緩和を確認する機能安全（ISO26262）に対し、SOTIFは「意図した領域」内で適切に振る舞うことを確認する手法。ヒューマンエラーや性能限界（天候による影響などを含む）等、機器自体に故障が無くとも非安全に陥る部分を対象にしている。
- 事象をKnown/Unknown、Hazardous/Not Hazardousの4つのエリアで整理した場合、“Known”部分を増やし、対策を講じることで、“Unknown Hazardous”を減らす手法と捉えることもできる。
- System of systemsになると、このようなUnknownな事象が大きくなる。できるだけその部分を明確化させるための考え方と捉えることができる。

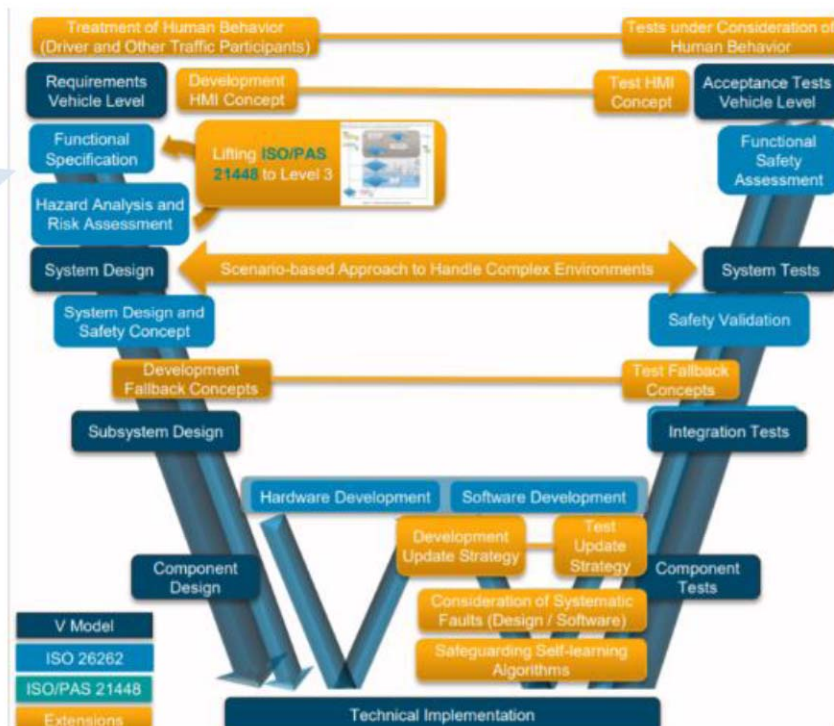


出所) ISO/DIS21448 (SOTIF) をもとに一部修正

Safety of the Intended Functionality (ISO/DIS 21448)

- ISO26262（機能安全）とは相補的であり、ISO26262で提唱されているVプロセスを補完する形で機能。
- 開発段階（Vの左側）で、システム・機能仕様、リスク評価、トリガーイベントの特定、機能の変更を行うとともに、検証段階（Vの右側）でKnown ScenarioのVerification（検証）およびUnknown Scenarioを含めたValidation（妥当性評価）を行う。
- 国際標準としてGSNをベースとした安全論証構造が提示。一般的なGSNに加え、Assurance Claim Pointを追加し、今後の検討課題を明確化している。なお、システム間の相互作用に伴う危険性を評価する手法として、STAMP（後述）が推奨技法になっている。

Pegasus Project（後述）のVモデルにもSOTIFが位置付けられている



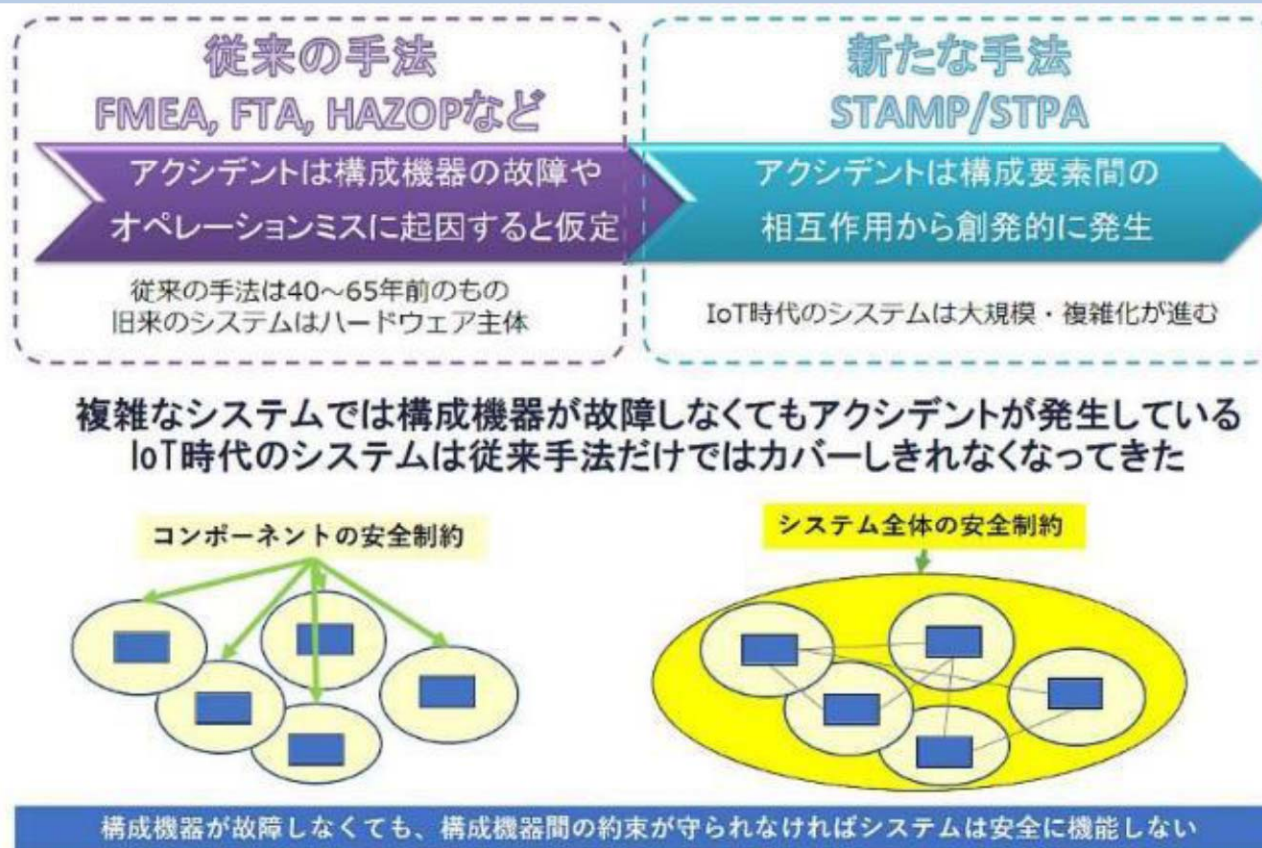
出所) Pegasus Symposium 2019 “V-Model and Process Analysis”
<https://www.pegasusprojekt.de/en/pegasus-symposium-2019/>, 2021年3月閲覧

マネジメント的な解決策⑧

STAMP/STPA

STAMP (Systems-Theoretic Accident Model and Processes)

- STAMP (Systems-Theoretic Accident Model and Processes : システム理論に基づくアクシデントモデル) とは、相互作用から創発的に発生するハザード要因にアプローチする安全性解析手法。従来のコンポーネントの安全制約の積み上げでは分析しづらくなったシステム全体の安全制約を評価する。マサチューセッツ工科大学のNancy Leveson氏により2012年に提唱された。



出所) IPA「国際安全規格におけるSTAMP/STPA適用可能性の考察」、第2回 STAMPワークショップ
(<https://www.ipa.go.jp/files/000063424.pdf>)、2021年1月5日閲覧

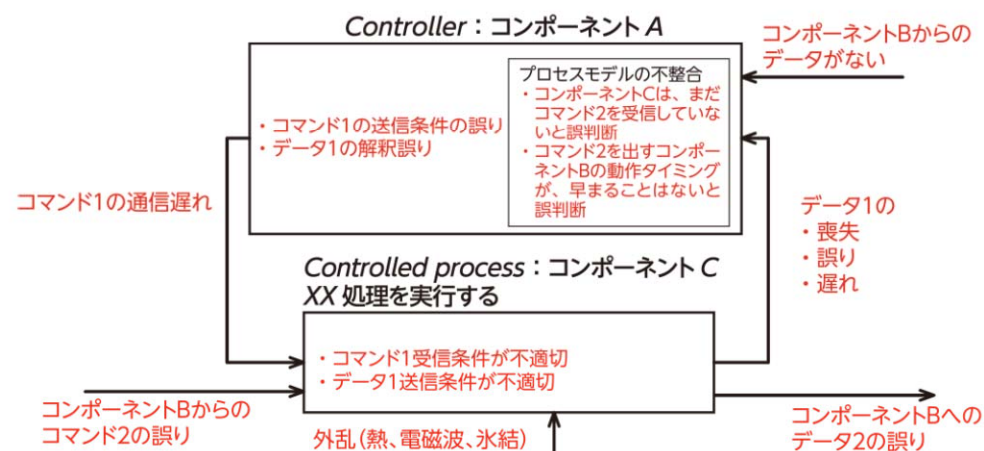
STPA (System-Theoretic Process Analysis)

- STPA (System-Theoretic Process Analysis) はSTAMPに基づく安全性解析の具体手法である。
- 以下のステップからなる。それぞれのステップにはガイドワードが整理されている。
 - Step 0: アクシデント、ハザード、安全制約の整理、コントロールストラクチャ（制御構造図）の構築
 - Step 1: Unsafe Control Action (UCA) の抽出
 - Step 2: Hazard Causal Factor (HCF) の特定
 - Step 3: 対策の立案
- システムオブシステムズになるとシステム間の相互作用を考慮する必要性は増加。システム全体のリスクへのアプローチが必要。

Step 1

コントロール アクション	非安全なコントロールアクション			
	与えられないとハザード	与えられるとハザード	早すぎ、遅すぎ、 誤順序でハザード	早すぎる停止、 長すぎる適用でハザード
コマンド 1	XX 条件下で、コマンド 1 が提供されない場合、ハザードに至る (UCA1)	コマンド 1 の内容が誤っていた場合、処理は停止するが、ハザードには至らない	コマンド 1 の提供が、コマンド 2 よりも遅れた場合、指示が書きされ、ハザードに至る (UCA2)	コマンド 1 が途中で停止した場合、ハザードには至らない
コマンド 2	コマンド 2 が提供されない場合、処理が開始しないが、ハザードには至らない	コマンド 2 の内容が誤っていた場合、処理は停止するが、ハザードには至らない	コマンド 2 の提供が、連続した場合、指示が累積され、ハザードに至る (UCA3)	コマンド 2 が途中で停止した場合、ハザードには至らない
コマンド 3	コマンド 3 が提供されない場合、処理が開始しないが、ハザードには至らない	コマンド 3 の内容が誤っていた場合、処理は停止するが、ハザードには至らない	コマンド 3 の提供が、遅れ／早い場合、処理開始がずれるが、ハザードには至らない	コマンド 3 が途中で停止した場合、ハザードには至らない

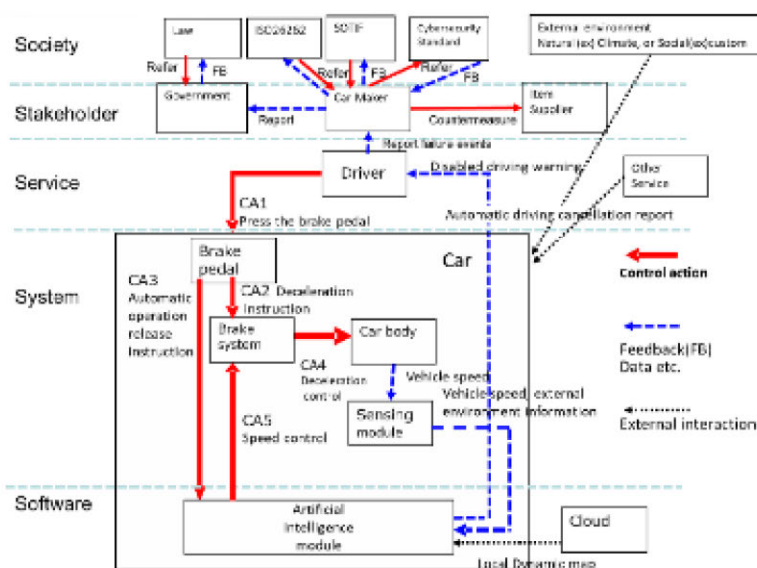
Step 2



出所) IPA「はじめてのSTAMP/STPA」Ver.1.0 (2016年3月)
(<https://www.ipa.go.jp/files/000051829.pdf>)、2021年3月閲覧

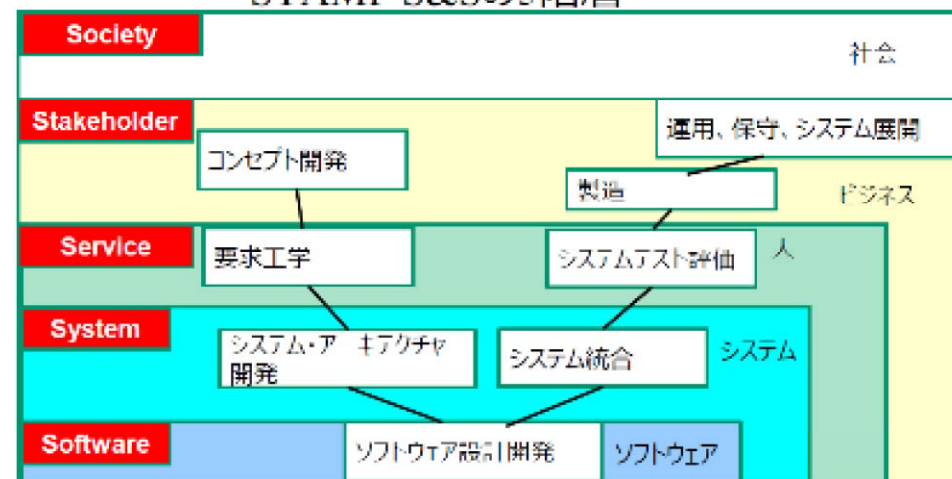
STAMP S&S

- STAMP S&Sはシステム理論に基づく安全性・事故分析などの様々な分析技術とその技術による取組。STAMPはSystem Theoretic Architecture Model and Processであり、S&Sは Safety、Securityの他、System、Software、Service、Stakeholder、Society、Specification、Standard、Scenarioの略称。
- STAMPの適用範囲の広さをベースにして、STAMPの各種分析方法等をより広範囲に異なる観点で適用することでSTAMPの可能性を引き出し、その具体的な適用方法を確立することを目的としている（機器＋システム＋人＋組織、多様なコンポーネントの相互作用を分析）。
- システムオブシステムズのモデル化には、このようなレイヤー別の整理が必要であると考えられる。



出所) 金子朋子「自動運転事例における機械学習の課題とヒアリング・アンケート結果」、第二回AI/IoTシステム安全性シンポジウム（2020年11月）

STAMP S&Sの5階層



Society（社会）、Stakeholder、Service（業務）、System、Softwareの5層に分けてコンピュータシステムが開発され、利用される世界をシステム思考でとらえることができる。

マネジメント的な解決策③

FRAM

FRAM (Functional Resonance Analysis Method: 機能共鳴分析)

- レジリエンス・エンジニアリングにおける安全分析のための手法。レジリエンス・エンジニアリングは、システムの安全は環境変動や意図しない入力に対する柔軟さによって達成されると考える。入力の変動に対して柔軟に変動できる能力の高さが安全性の高さ（成功要因）であると同時にリスク（失敗要因）でもある。
- FRAM はシステムの失敗事象を定義せずに分析を行うことに大きな特徴がある。まず個々の機能の詳細な定義から始め、分析の結果として全体ネットワークがモデル化され、システムの成功要因が導出される。

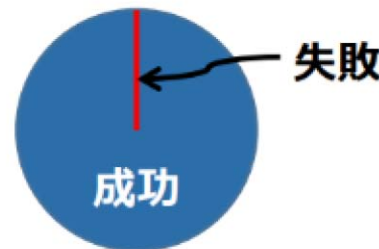
Safety-I

- ・ 悪い原因から悪い結果が生まれると定義する安全工学
- ・ **なぜ失敗するのかを分析してリスクを識別**

FTA
STAMP 等

Safety-II

- ・ 良い原因（成功）からも悪い結果が生まれると定義する安全工学
- ・ **なぜ成功するのかを分析してリスクを識別**



FRAM

出所) 道浦康貴「自動制御システムの安全性解析の最新手法」(<http://applmech.eng.niigata-u.ac.jp/jrail2017/doc/specialsession2.pdf>)、2021年1月5日閲覧

FRAM (Functional Resonance Analysis Method: 機能共鳴分析)

- 例えば、機能同士のインタラクションをFRAMにより分析する際には、やり取りされるデータの変化よりも機能そのものの変化に着目する。
- まれにしか発生しない問題の認識のためには、機能と機能との結び付き方は、矢印1本の関係で描画されるのではなく、結合の意味（セマンティクス）を伴うモデルの作成が必要になる。
- ヒューマンファクターを模擬するうえでも、セマンティクスも含めて模擬で切るという観点で適した表現方法である。

表1 機能の6要素

I: 入力	機能の動作トリガー
P: 前提	機能が動作開始するための事前条件
C: 制御	機能の挙動方法を操作する事後条件
R: 資源	機能の動作に必要な資源（事後条件）
T: 時間	機能実行可能時間（事後条件）
O: 出力	機能の出力

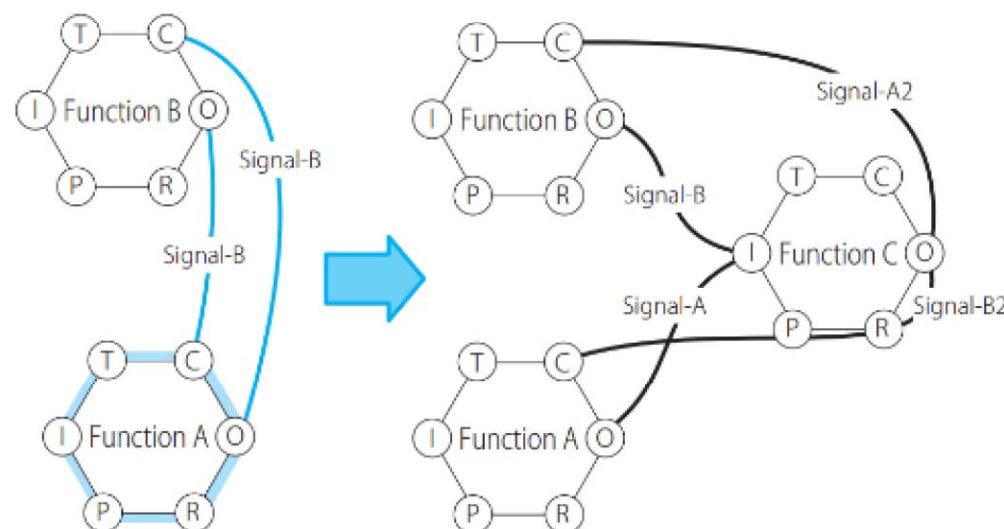


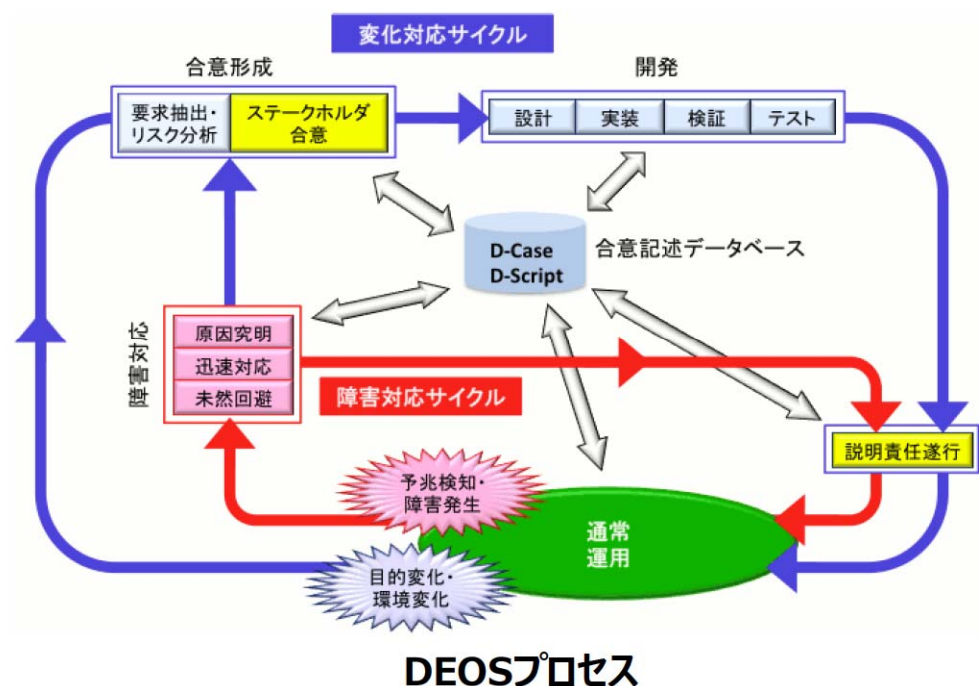
図 3.2.2-3 制御同士の競合を防止するための中間バッファの追加

出所) 野本秀樹ほか「FRAM (機能共鳴分析手法) による成功学に基づく安全工学」、SEC journal Vol.14 No.1 Aug. 2018
<https://www.ipa.go.jp/files/000068587.pdf>、2021年1月5日閲覧

マネジメント的な解決策④ DEOS プロセス (IEC 62853)

DEOS プロセス (IEC 62853) - 変化するシステムの総合信頼性確保を支援

- IEC 62853:Open Systems Dependabilityは開放系システムの総合信頼性に関する日本発の国際規格である。IEC TC56 Dependabilityで議論され、2018年5月に発行された。
- ディペンダビリティ技術推進協会の活動成果のうち、開放系システムの考え方と、総合信頼性を満たすための基本要件（4つのプロセスビュー）を標準化したものである。なお、ディペンダビリティの基本規格の1つで、分野規格や製品規格ではない。
- システムオブシステムズの安全性・信頼性確保に対しても適用可能であると考えられる。



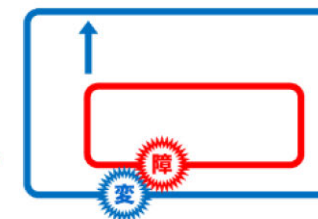
反復的アプローチ

- 目的や環境の変化に対してシステムを継続的に変更する変化対応サイクル
- 障害に迅速に対応する障害対応サイクル

合意形成と説明責任全うの支援

- 合意記述データベースによる、ステークホルダ間の合意形成
- 合意内容に基づく説明責任の全う
- 開発・運用フェーズの統合

DEOS二重ループ



出所) DEOS協会ウェブサイト (<http://deos.or.jp/index-j.html>)、2021年1月5日閲覧

【参考】Open System Dependabilityの概念整理

用語	出典	定義・説明
オープンシステム (Open System)	IEC 62853 p.8 3.12	system whose boundaries、 functions and structure change over time and is recognized and described differently from various points of view
信頼性 (Reliability)	JIS Z 8115 : 2019	アイテムが与えられた条件のもとで、与えられた期間、故障せずに、要求通りに遂行できる能力
総合信頼性 (Dependability)	JIS Z 8115:2019	アイテムが、要求されたときに、その要求どおりに遂行するための能力。アベイラビリティ、信頼性、回復性、保全性、及び保全支援性能を含む。適用によっては、耐久性、 安全性及びセキュリティのような他の特性を含むことがある。
開放系総合信頼性 (open systems dependability)	JIS C 62853:2020	期待されるサービスを要求されたときに要求されたように提供するために、目的、目標、環境及び実際のパフォーマンスの変化に対応し、説明責任を継続的に果たす能力 注釈 1 : パフォーマンスの意味には、実施、実績、性能、能力及び動作様態が含まれる。

用語	出典	定義・説明
安全 (Safety)	ISO/IEC Guide 51 : 2014	許容できないリスクが無いこと ("freedom from risk which is not tolerable")
	IEC 61508 : 1998	"freedom from unacceptable risk " part of the overall safety relating to the EUC* and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems、 other technology safety-related systems and external risk reduction facilities 被制御装置とその制御システムに関する安全のうち、電気・電子・プログラマブル安全関連系、他技術の安全関連系、外部のリスク低減装置の正常機能に依存する部分
	ISO 26262 : 2018	"absence of unreasonable risk" absence of unreasonable risk due to hazards caused by malfunctioning behaviour of E/E systems 電気・電子システムの機能不全時の動作に起因するハザードによる不合理なリスクがないこと

【参考】Open System Dependabilityの概念整理

- Society 5.0では、システムを取り巻く社会、環境、およびシステム自体も刻々と変化する。
- その変化を踏まえ、システムの安全に対する説明責任を継続的に果たすことが求められる。

Dependability (JIS Z 8115:2019)

- アイテムが、要求されたときに、その要求どおりに遂行するための能力。アベイラビリティ、信頼性、回復可能性、保全性、及び保全支援性能を含む。適用によっては、耐久性、安全性及びセキュリティのような他の特性を含むことがある。
 - アベイラビリティ：要求された通りの遂行状態にあるアイテムの能力（アイテムの信頼性、回復可能性、及び保全性を組み合わせた特性、ならびに保全支援性能に依存）
 - 信頼性：アイテムが与えられた条件のもとで、与えられた期間、故障せずに、要求通りに遂行できる能力
 - 回復可能性：アイテムが事後保全を実施せずに、故障から回復する能力
 - 保全性：与えられた運用・保全条件で、アイテムが要求通りに遂行できる状態に保持されるか、又は修復される能力
 - 保全支援性能：保全支援（アイテムを維持するための資源の共有）に関する組織の有効性

Open System Dependability (JIS C 62853:2020)

- 期待されるサービスを要求されたときに要求されたように提供するために、目的、目標、環境及び実際のパフォーマンスの変化に対応し、説明責任を継続的に果たす能力（注：パフォーマンスの意味には、実施、実績、性能、能力及び動作様態が含まれる）
 - アベイラビリティ、信頼性、保守性及び支援性を含め、ディペンダビリティ属性の概念自体は、オープンシステムについても従来のシステムと変わらない。しかし、オープンシステムでは、単独でシステム又はそのリスクを完全に理解する利害関係者はいないという文脈でこれらの属性を考える。

【参考】Open System Dependabilityの概念整理

- Dependability（総合信頼性）には安全性が包含されうる場合があるが、実質的には、安全要求（許容できないリスクを生じさせないこと）を達成するための能力（アベイラビリティ）が備わっているか、細分化された安全関連要求の信頼性が備わっているか、等、Dependする前提条件の一部としてSafetyがある、という関係性で捉えられるものであると考えられる。

Dependability (JIS Z 8115 : 2019)

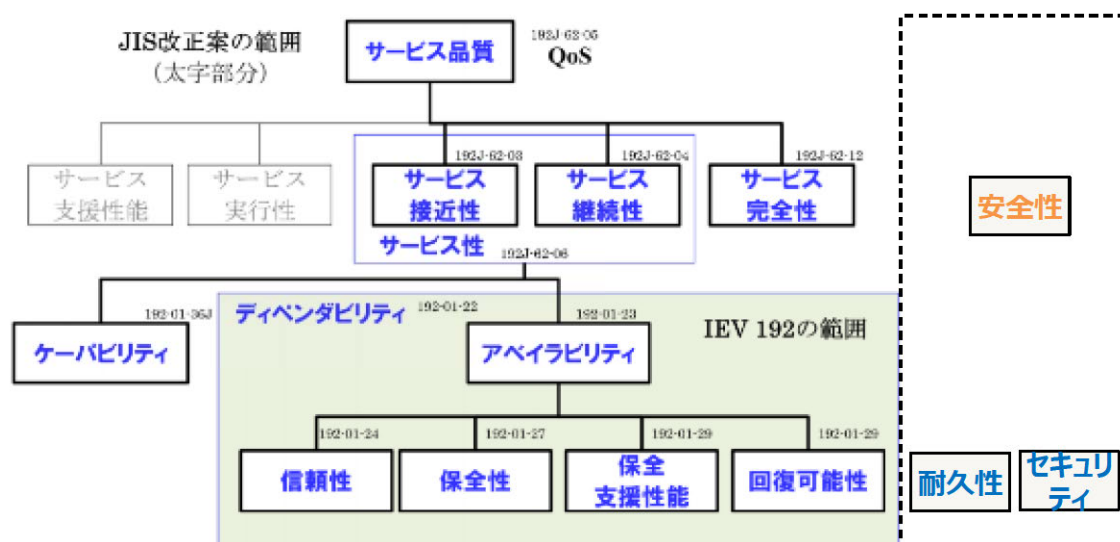
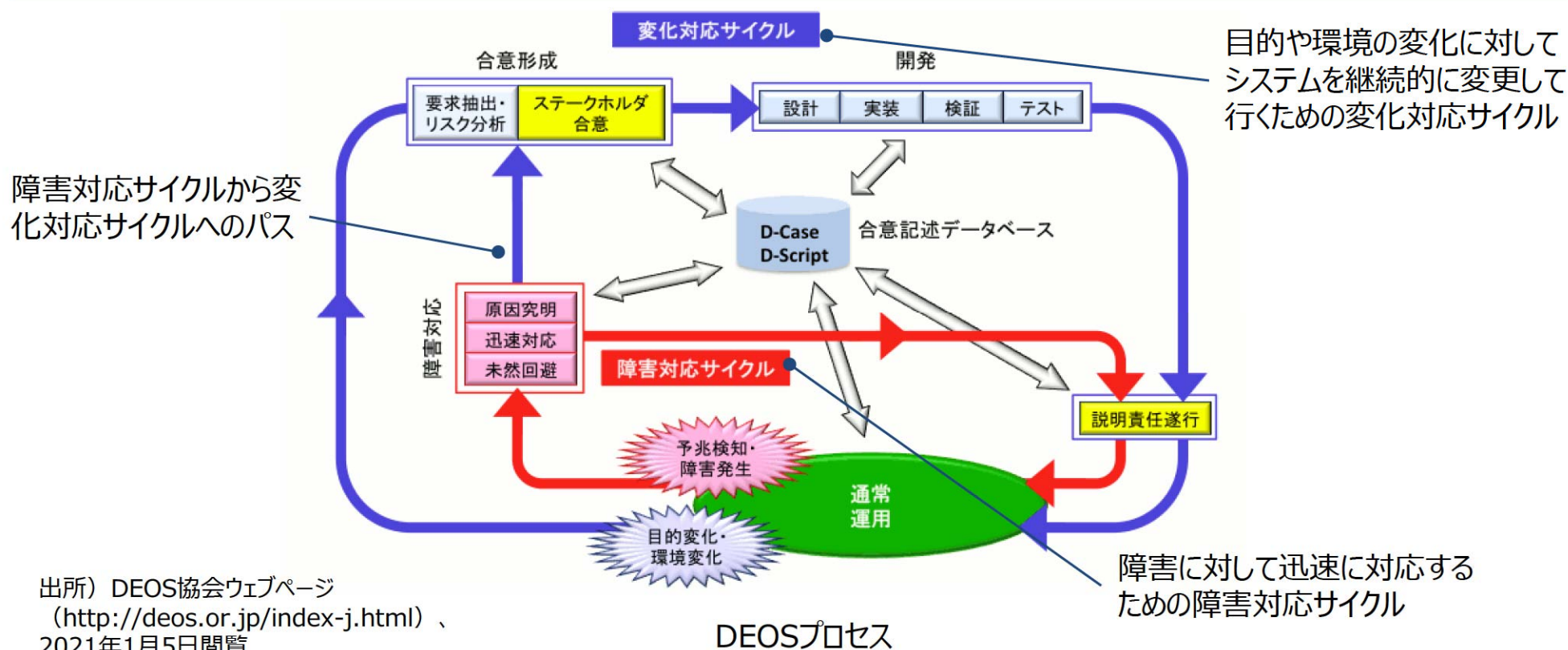


図6 IEC 60050-192 Ed.1 の適用範囲とJIS Z 8115 信頼性用語改正案の適用範囲 この図は、図5の構造を基にして、JIS改正案で採用している用語の範囲を示したもので、サービス関連用語を含む。四角枠の内部はIEC 60050-192 Ed.1 の範囲を示したもので、ディペンダビリティ関連用語に限定されている。

出所) 益田明彦「JIS Z 8115 ディペンダビリティ（信頼性）用語の現状と将来」、IEICE Fundamentals Review Vol.9 No.4
(https://www.jstage.jst.go.jp/article/essfr/9/4/9_318/_pdf)、2021年1月閲覧

DEOS プロセス (IEC 62853)

- DEOSプロセスにより、利用者がシステムに期待する便益を安全にかつ**継続的に提供**できる。
 - システム運用開始後の要求の変化に適応できる（変化対応）
 - システムの障害要因を顕在化する前にできる限り取り除くことができる（未然防止）
 - 障害が顕在化した後に迅速かつ適切に対応し、影響を最小とすることができる（障害対応）
- DEOSプロセスにより、ステークホルダーや社会への**説明責任を全う**できる。
 - 全ライフサイクルでの要求と実現に関する合意形成の構造的記録と履歴がある（合意履歴保持）
 - 合意に基づいたシステムの運用状況の監視と詳細な記録がある（監視と記録）

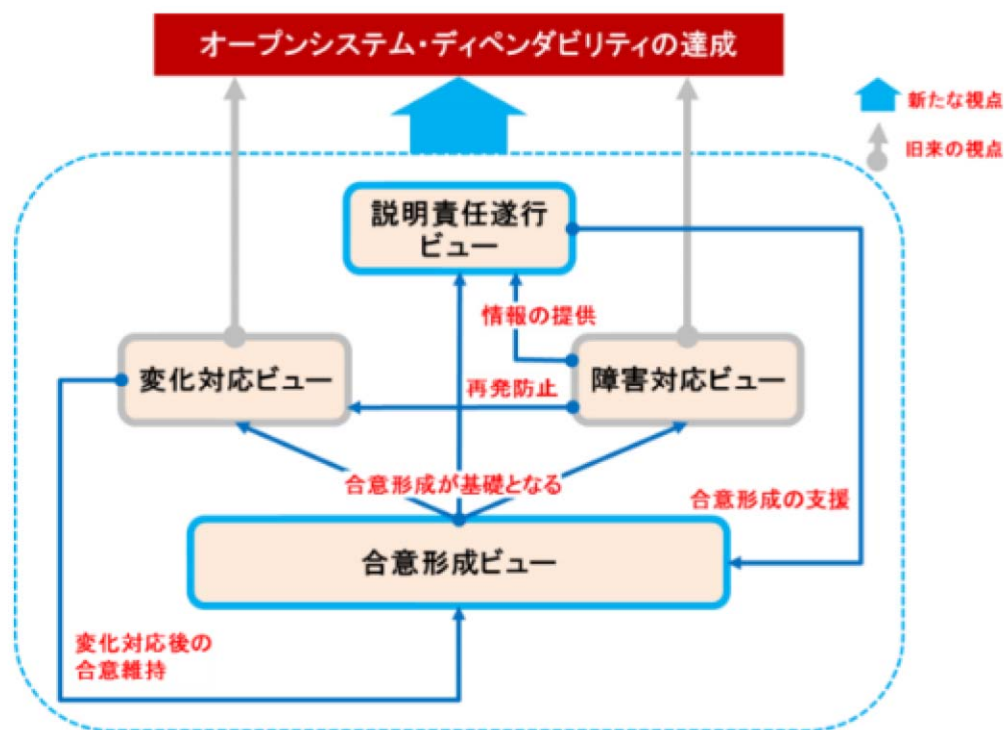


出所) DEOS協会ウェブページ
 (http://deos.or.jp/index-j.html) 、
 2021年1月5日閲覧

DEOSプロセス

DEOS プロセス (IEC 62853) - 4つのビュー

- 合意形成プロセスビュー：IEC15288 における合意プロセスに加え、OSD のプロセスがどのように実行されるかについての合意形成も含みまとめた観点
- 説明責任プロセスビュー：システム故障他のトラブルに関する説明責任の果たし方をまとめた観点
- 故障対応プロセスビュー：システム故障への即時・短期的対応のとり方をまとめた観点
- 変化対応プロセスビュー：故障への長期対応の他、システム環境やシステム目的の変化に対応する方法をまとめた観点

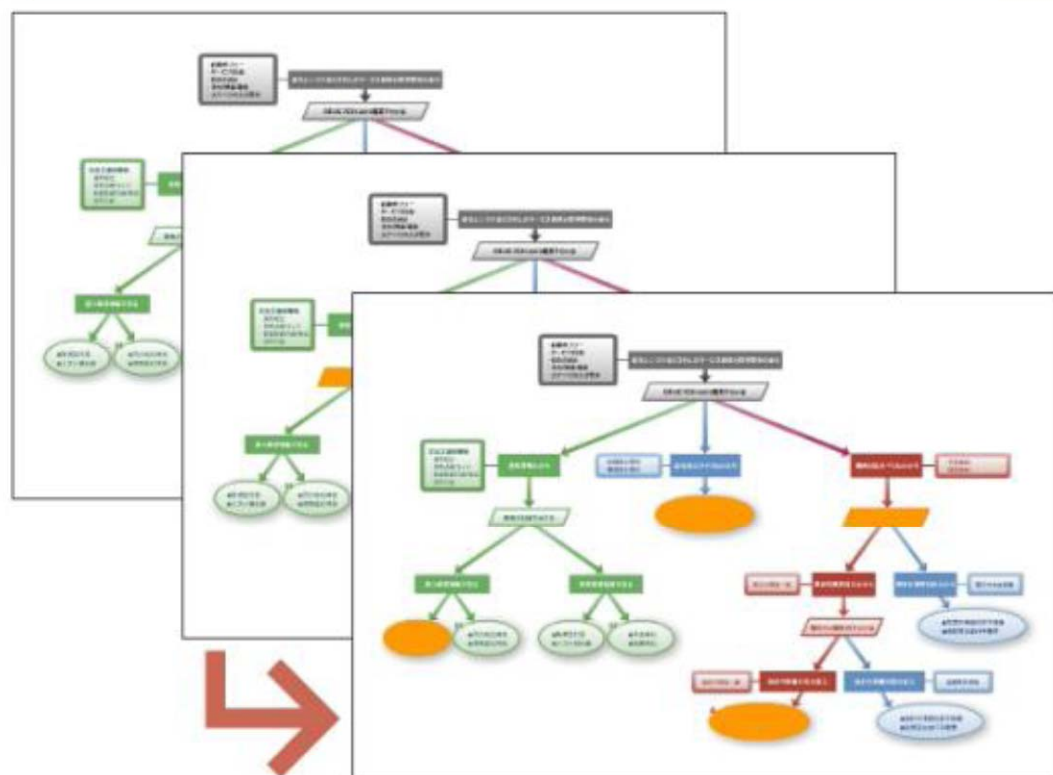


出所) DEOS協会ウェブページ
(<http://deos.or.jp/index-j.html>)、
2021年1月5日閲覧

4つのプロセスビューの関係

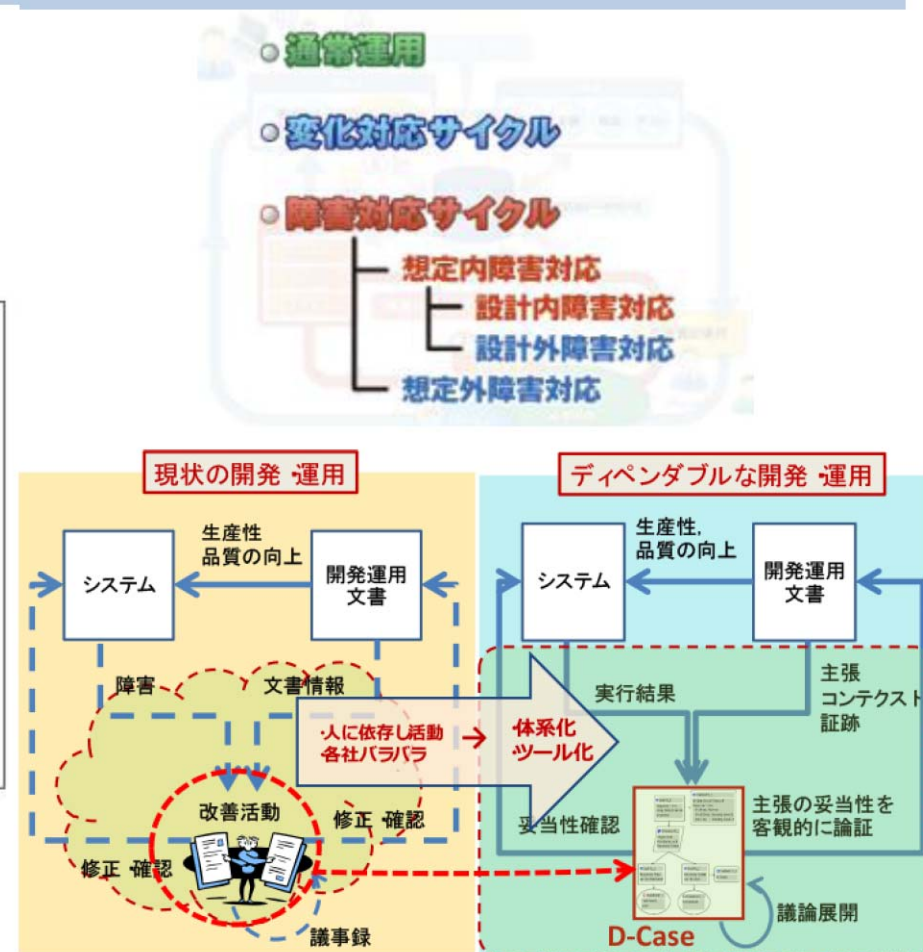
DEOS プロセス (IEC 62853) - D-Case

- ステークホルダ間の合意形成を支援する手法。Goal Structuring Notation (GSN) をベースに、関係者の要求を明確化し、議論の仮定と結果を可視化する。
- 通常運用、変化対応、障害対応に区分したDEOS基本パターンが用意されている。合意に基づく変更履歴が説明責任遂行を支援。



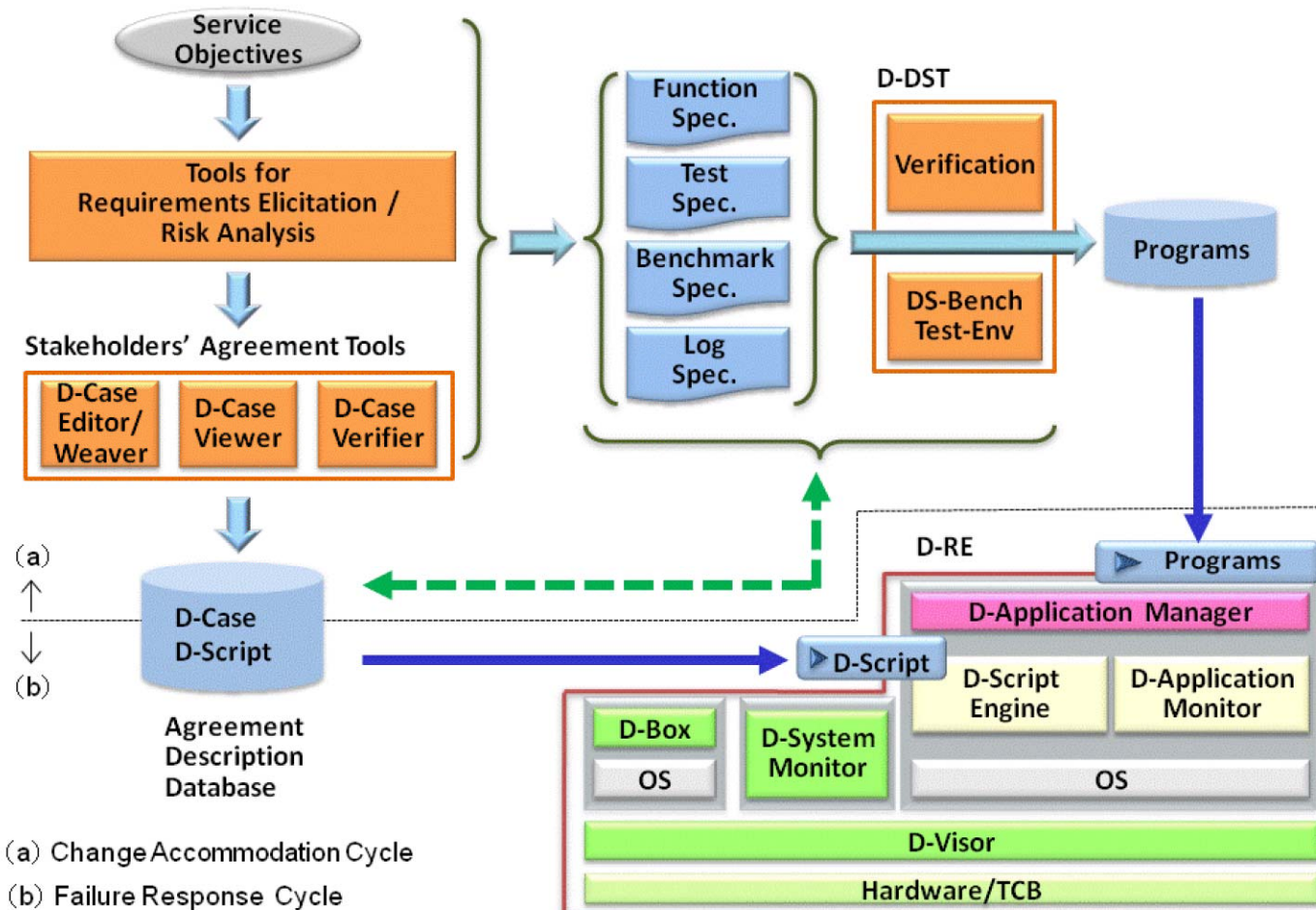
D-Case基本パターンとその更新

出所) DEOS協会ウェブページ (<http://deos.or.jp/index-j.html>)、
2021年1月5日閲覧



DEOS プロセス (IEC 62853) - DEOSアーキテクチャ

- D-Caseと連動してシステムを柔軟に変更するとともに、プログラムを検証し安全に実行する。障害や意図的な攻撃を監視し障害を未然に防ぐ。合意形成ツールとデータベースの構築が鍵となる。



出所) DEOS協会ウェブページ (<http://deos.or.jp/index-j.html>)、
2021年1月5日閲覧

マネジメント的な解決策⑤ 人間中心設計（UCD）

人間中心設計（UCD）

詳細は付属資料参照

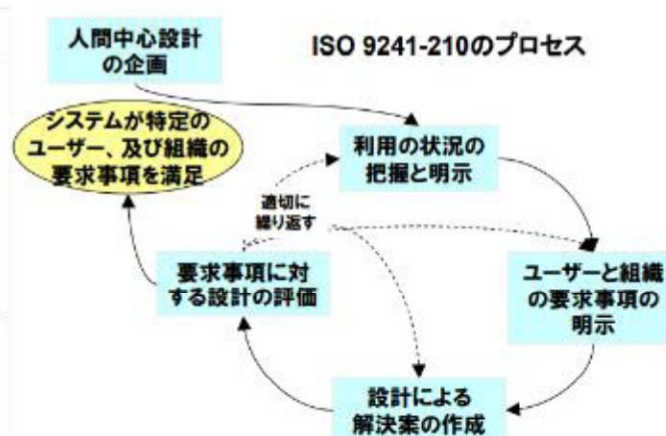
- ISO13407が1999年に発行、その改訂版ISO-9241-210が発行された。
- ユーザビリティ（ある製品が、指定されたユーザによって、指定された利用の状況（Context of Use）下で指定された目的を達成するために用いられる際の、有効さ、効率及びユーザの満足度の度合い、と定義されている）

インタラクティブ・システムの人間中心設計（HCD: Human-Centred Design）のプロセスに関する国際規格ISO 13407が1999年に発行され、翌年に日本工業規格JISとして制定されました。2010年には、その改訂版ISO 9241-210が発行されています。HCDは、ユーザー中心設計（UCD）と呼ばれることもあります。

ISO 13407: 1999
Human-centred design
processes for
interactive systems

JIS Z8530: 2000
インタラクティブシステム
の人間中心設計プロセス
(13407の翻訳JIS)

ISO 9241-210: 2010
Ergonomics of human-
system interaction
Part 210: Human-
centred design for
interactive systems



ISO 9241-11/JIS Z 8521のユーザビリティの定義

ある製品が、指定されたユーザーによって、指定された利用の状況下で、指定された目的を達成するために用いられる際の、有効さ、効率及びユーザーの満足度の度合い

関連用語の定義

ユーザー、利用の状況、目的等が異なると、ユーザビリティは変化する

- ▶有効さ(effectiveness): ユーザーが指定された目標を達成する上での正確さ及び完全さ
- ▶効率(efficiency): ユーザーが目標を達成する際に正確さと完全さに関連して費やした資源
- ▶満足度(satisfaction): 不快さのないこと、及び製品使用に対する肯定的な態度
- ▶利用の状況(context of use): ユーザー、仕事、装置(ハードウェア、ソフトウェア及び資材)、並びに製品が使用される物理的及び社会的環境

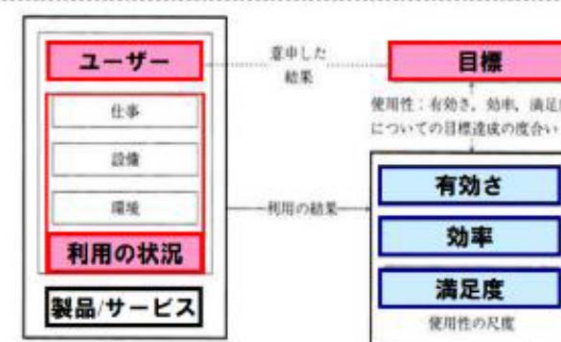


図1 使用性の枠組み

※インタラクティブシステムの人間中心設計プロセス(ISO 9241-210)等、関連のISO/JISでも同じ定義を採用しています

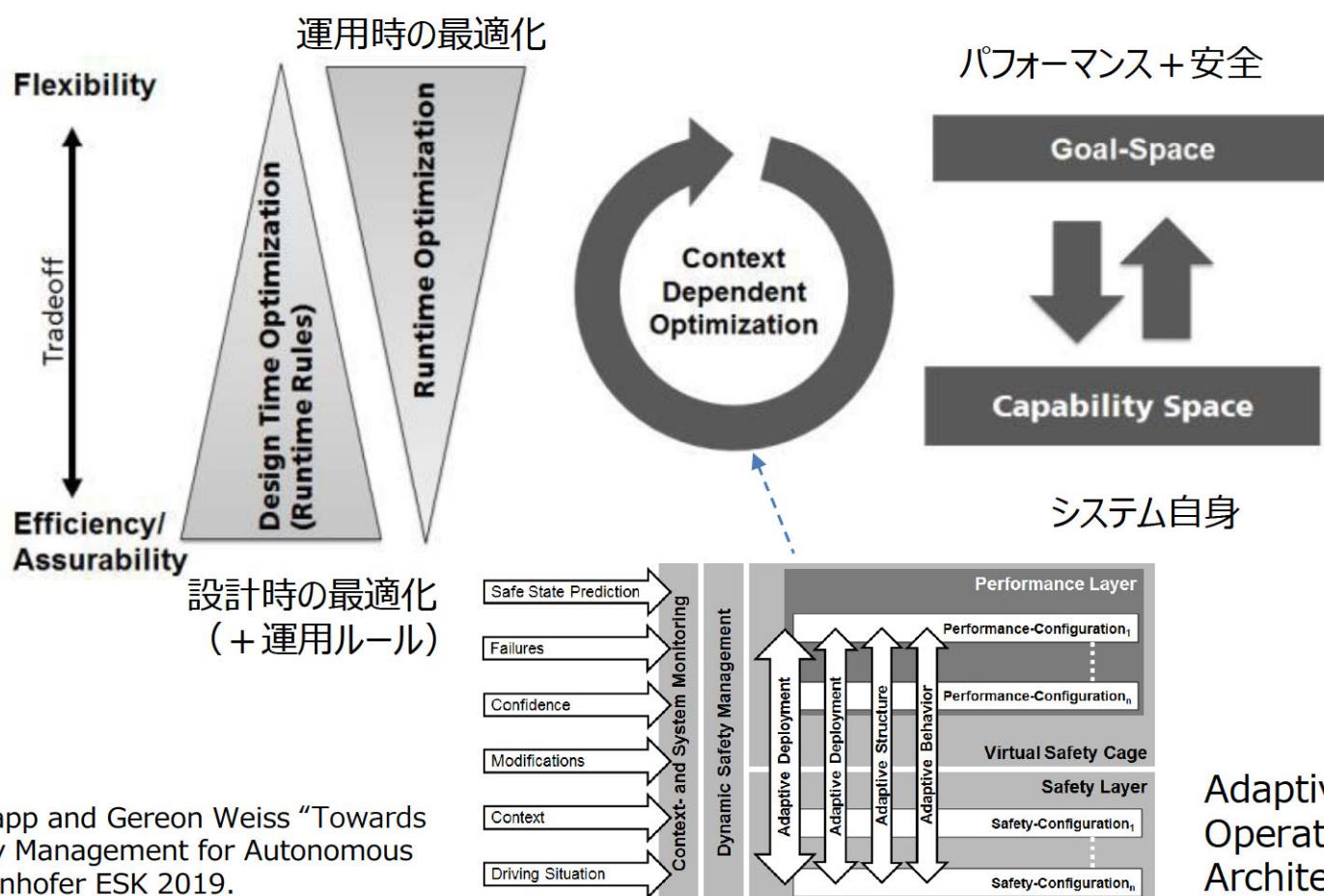
出所) 吉武良治「使いやすさ／利用時品質の考え方～開発技術者にとって重要なユーザビリティ、UXとは～」、ET2014 IPAブースプレゼン
(<https://www.ipa.go.jp/files/000044154.pdf>)、2021年3月閲覧

マネジメント的な解決策⑥

Dynamic Safety Management

Dynamic Safety Management (Fraunhofer IKS)

- Dynamic Safety Management (DSM) とは、設計時における最悪ケースの想定に縛られていては自律システムの安全性は担保できないため、運用時にリアルタイムのコンテキスト（外部環境）を見ることで安全かつ効率的な自律システムを実現する（Design Time/Static→Runtime/Dynamic）という考え方。Fraunhofer IKSが自動運転システムの制御を例に提唱している。

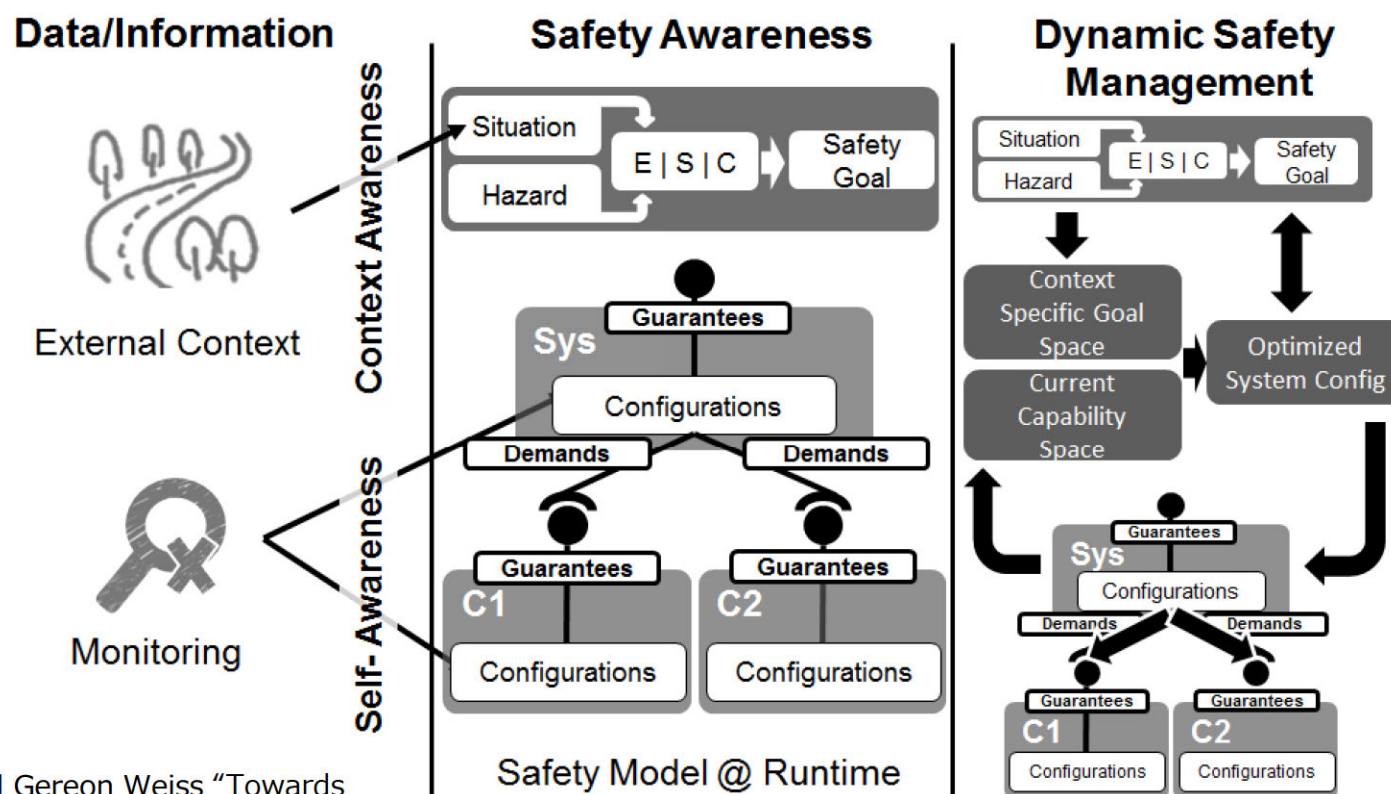


出所) Mario Trapp and Gereon Weiss "Towards Dynamic Safety Management for Autonomous Systems", Fraunhofer ESK 2019.

Dynamic Safety Management (Fraunhofer IKS)

- DSMとは、外部環境のモニタリングを通じた（将来も含む）リスク評価を用いてゴールを決定し、内部環境モニタリングを通じたケイパビリティ評価を踏まえそのゴールが達成されるかを把握しつつ、必要に応じてシステムの構造や挙動をリアルタイムに変化させること。
- DEOSプロセスの「変化対応サイクル」を実装したものと捉えることができる。

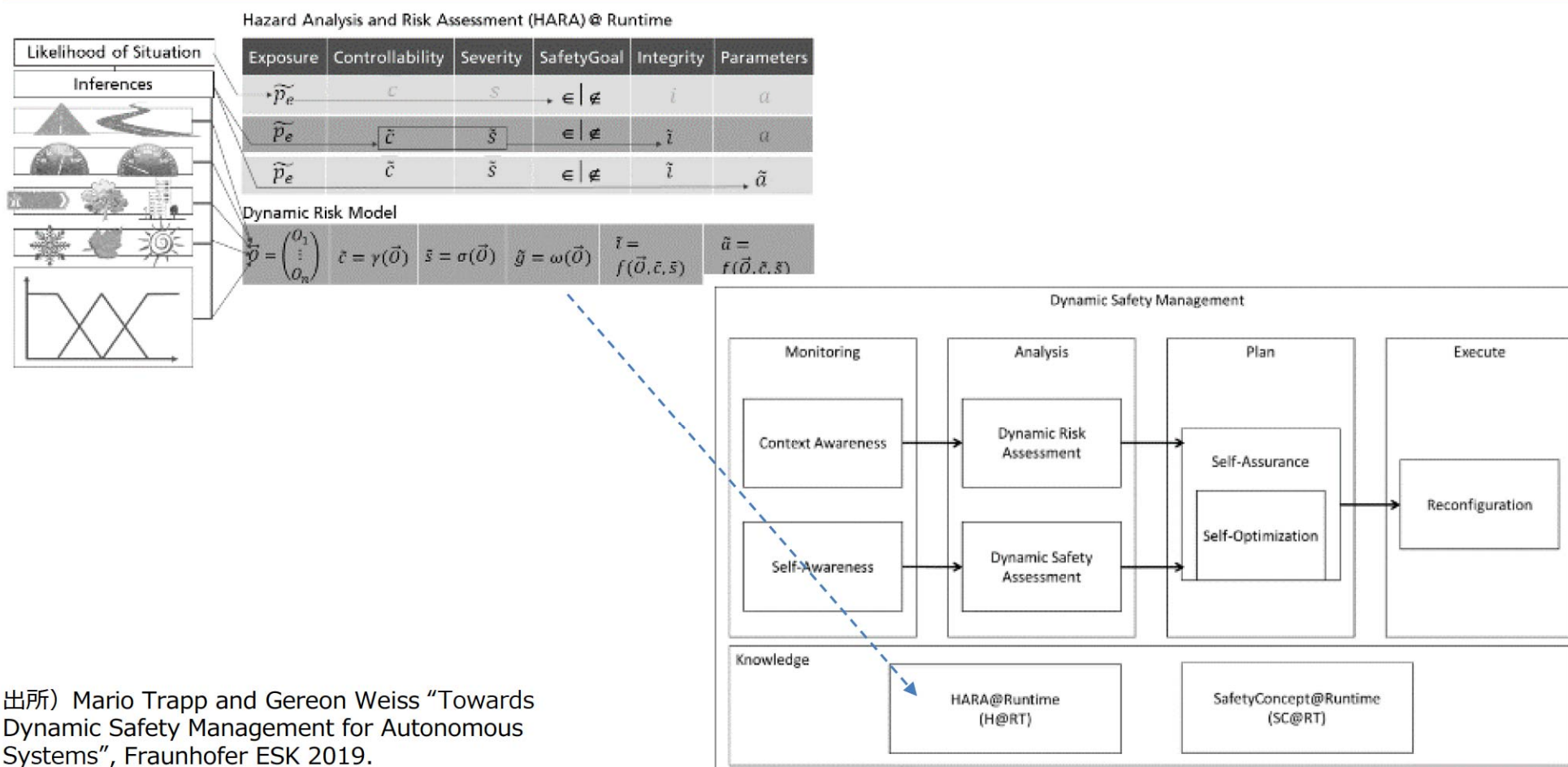
Basic Idea of Dynamic Safety Management



出所) Mario Trapp and Gereon Weiss "Towards Dynamic Safety Management for Autonomous Systems", Fraunhofer ESK 2019.

Dynamic Safety Management (Fraunhofer IKS)

- リスク評価を用いてゴールスペースを絞り込み（暴露、制御可能性、影響の大きさをもとにSafety Goalを設定）、システムがそれを満たしたうえで効率性を高めるための最適化・再配置を実施する。これはMAPE-K (Monitoring, Analysis, Plan, Execute + Knowledge) サイクルを回すことで可能になる。そのためにはODDの設定と、ベイジアンネットワーク等による発生事象の包括的モデル化が重要になる。

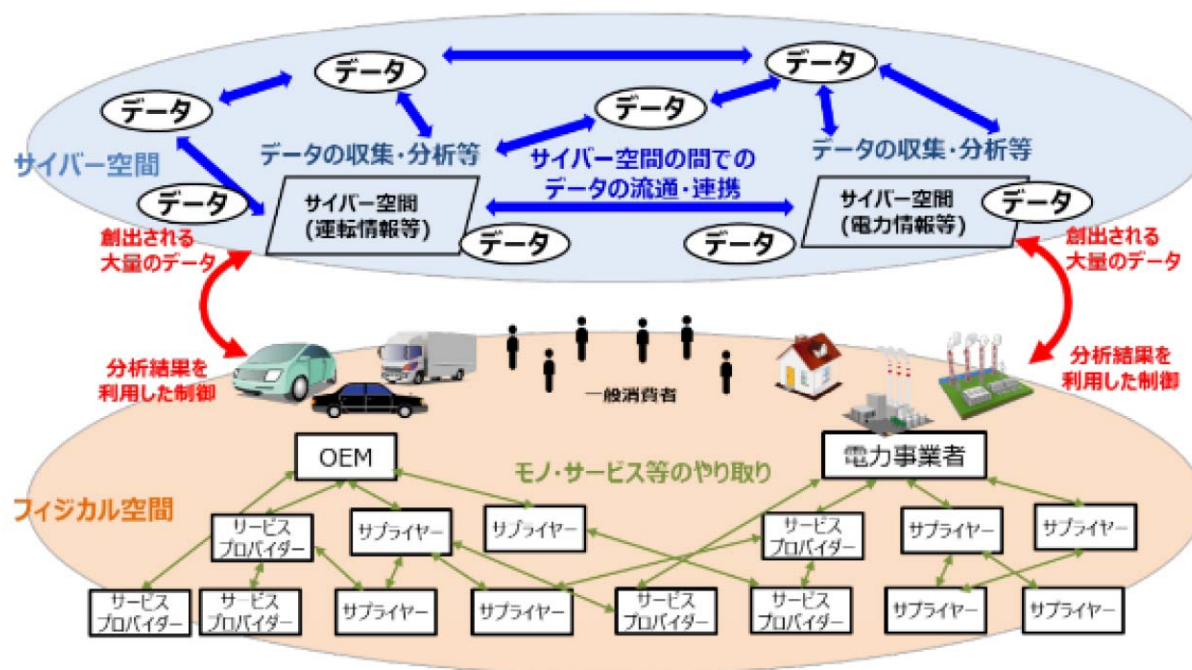


出所) Mario Trapp and Gereon Weiss "Towards Dynamic Safety Management for Autonomous Systems", Fraunhofer ESK 2019.

マネジメント的な解決策® CPSF

サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）

- 「Society5.0」では、データの流通・活用を含む、より柔軟で動的なサプライチェーンを構成することが可能。一方で、サイバーセキュリティの観点では、サイバー攻撃の起点の拡散、フィジカル空間への影響の増大という新たなリスクへの対応が必要になる。
- このため、産業サイバーセキュリティ研究会WG1において、「Society5.0」におけるセキュリティ対策の全体像を整理し、産業界が自らの対策に活用できるセキュリティ対策例をまとめた、『サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）』が策定された。



サイバー空間で大量のデータの流通・連携
⇒データの性質に応じた管理の重要性が増大

フィジカル空間とサイバー空間の融合
⇒フィジカル空間までサイバー攻撃が到達

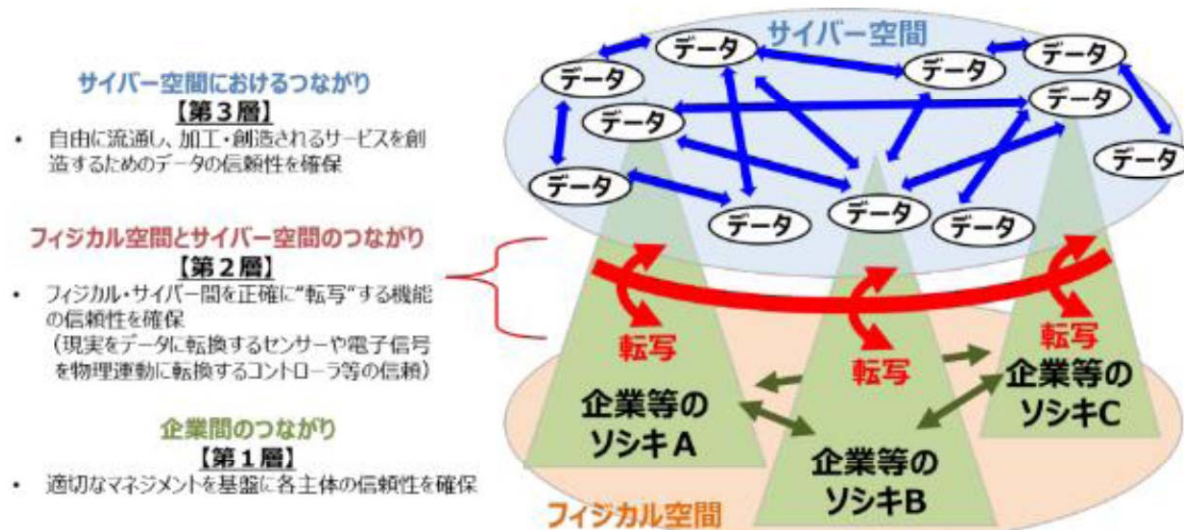
企業間が複雑につながるサプライチェーン
⇒影響範囲が拡大

Society5.0の社会におけるモノ・データ等の繋がりイメージ

出所) 経済産業省「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の概要」

サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）

- サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）は3層構造と6つの構成要素で整理されている。
 - 第1層：企業間のつながりにおける、企業（組織）のマネジメントの信頼性
 - 第2層：サイバー空間とフィジカル空間のつながりにおける、要求される情報の正確性に応じて適切な正確さで情報が変換される“転写”機能の信頼性
 - 第3層：サイバー空間のつながりにおける、データの信頼性

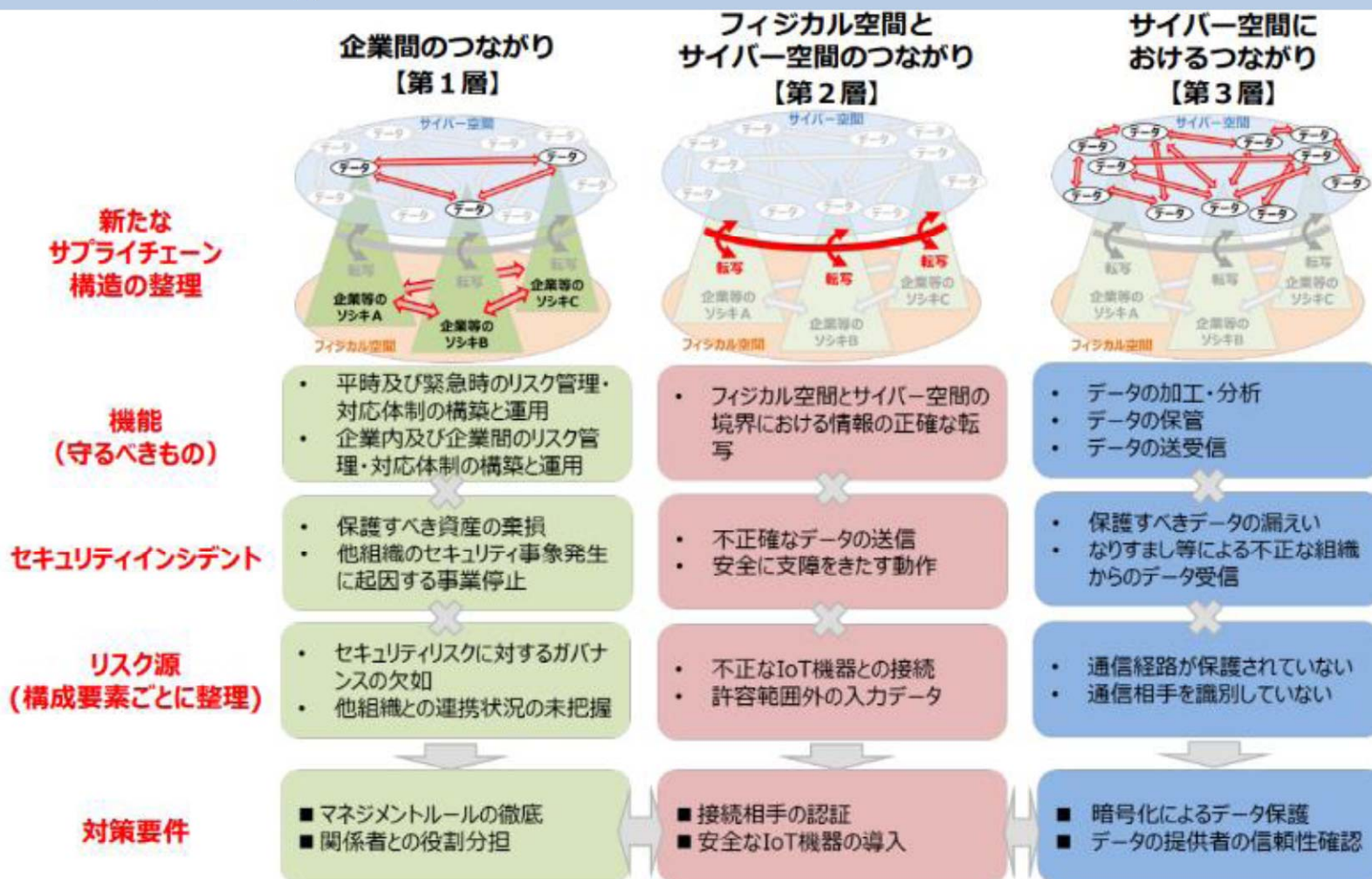


構成要素	定義	構成要素	定義
ソシキ	バリュークリエーションプロセスに参加する企業・団体・ソシキ	データ	フィジカル空間にて収集された情報及び共有・分析・シミュレーションを通じて加工された情報
ヒト	ソシキに属する人、及びバリュークリエーションプロセスに直接参加する人	プロセス	定義された目的を達成するために一連の活動を定めたもの
モノ	ハードウェア、ソフトウェア及びそれらの部品操作する機器を含む	システム	目的を実現するためにモノで構成される仕組み・インフラ

出所) 経済産業省「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の概要」

サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）

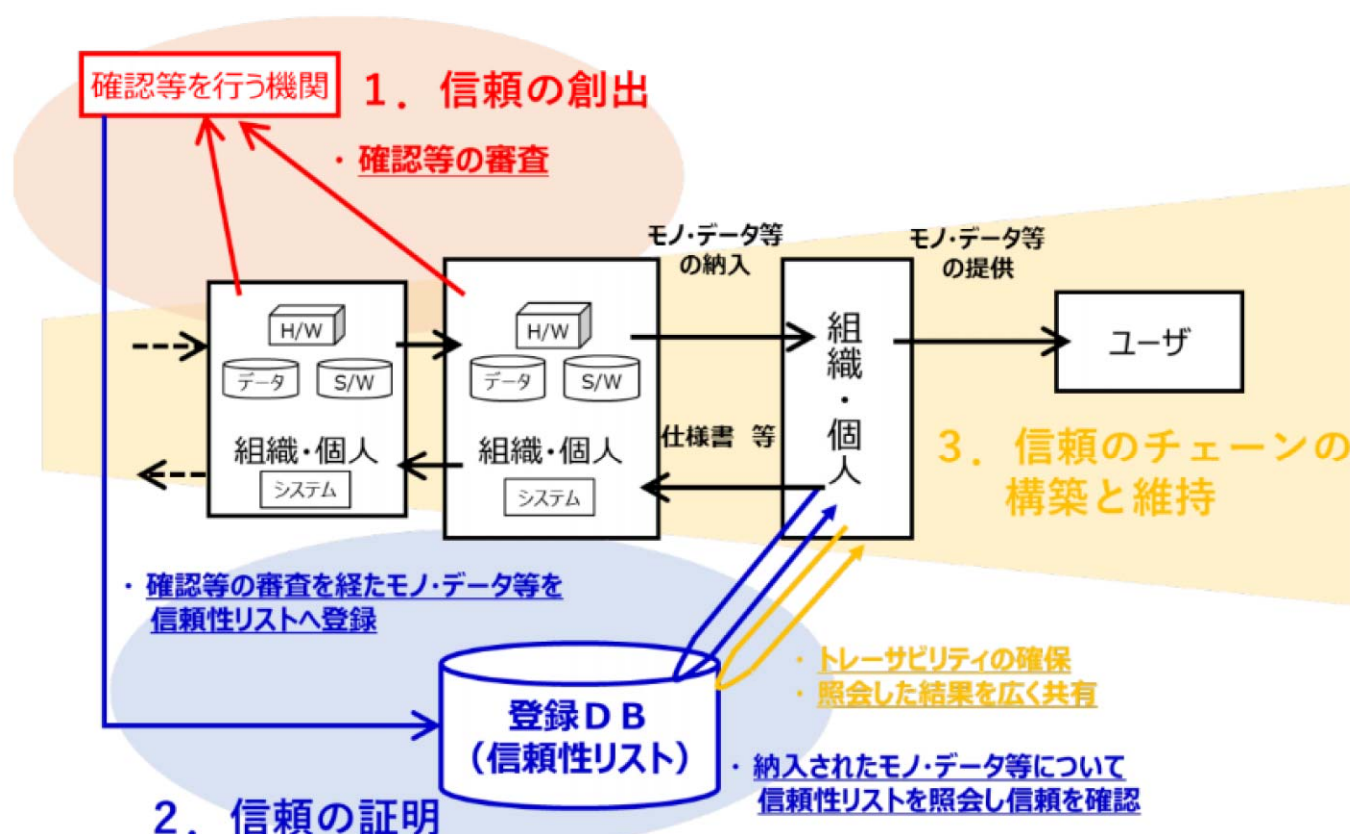
- 各層に対する対策を整理。第一層にはマネジメント・ガバナンス、第二層にはセンサやIoT機器、第三層にはデータそのものに対する要件となっている。



出所）経済産業省「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の概要」

サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）

- 各構成要素について必要なセキュリティ要件が満たされていることの確認（信頼の創出）、確認した主体以外の者による照会の仕組み（信頼の証明）により、それを繰り返し行い、広く共有して信頼のチェーンを構築、維持することが必要。
- このサイクルは、オープンシステムディペンダビリティを担保するためのDEOSプロセスとも親和性がある。



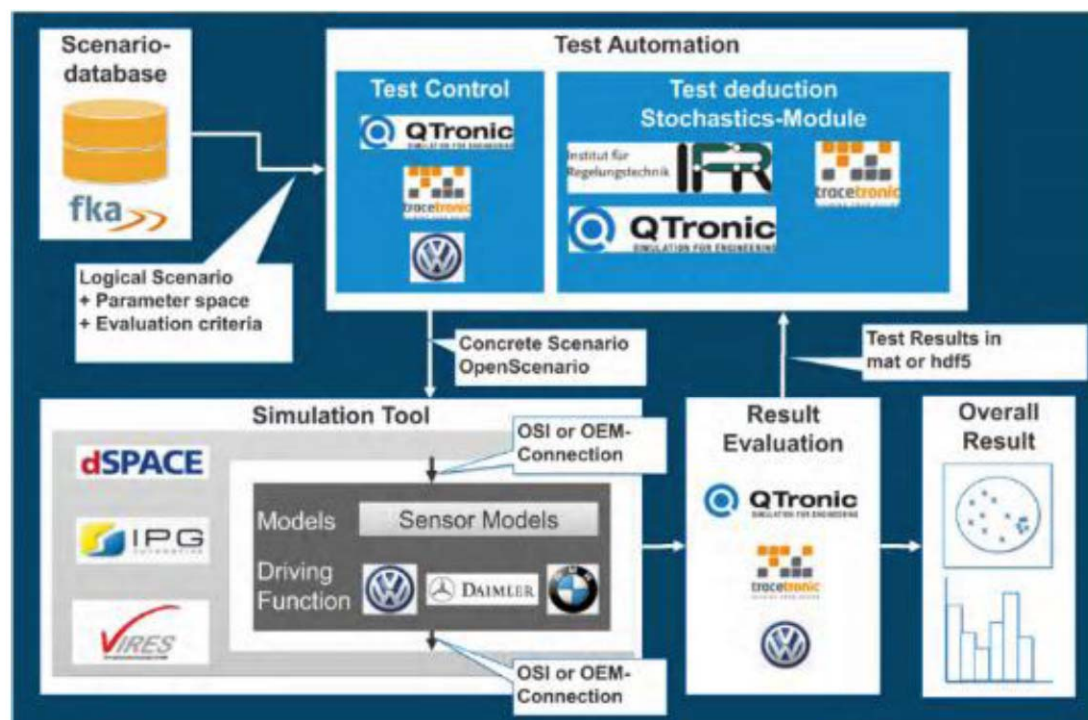
出所) 経済産業省「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の概要」

SoS課題解決の取組事例^ア

Pegasus Project

Pegasusプロジェクト

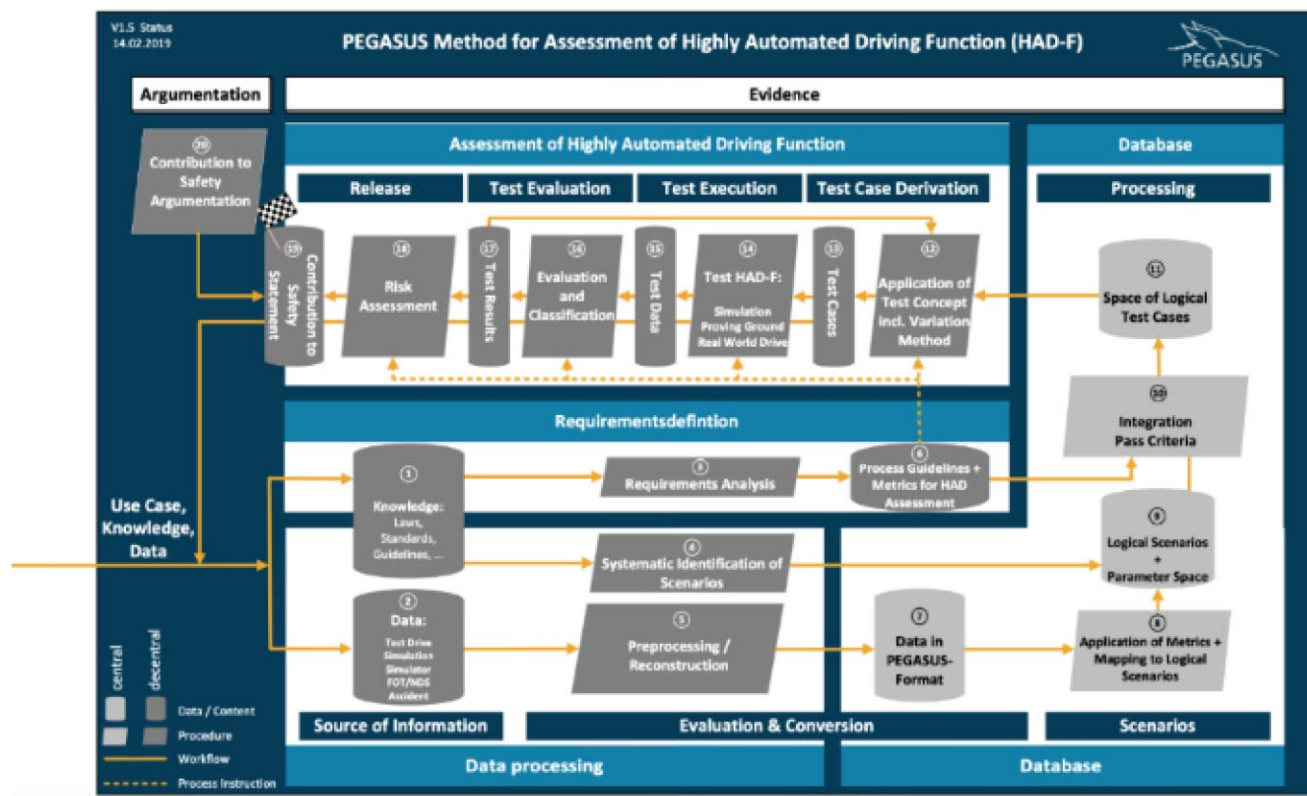
- Pegasusプロジェクトは、ドイツ経済エネルギー省が主導し、2016年～2019年に実施された産官学連携プロジェクト。「自動運転に必要な性能」、および「求められる性能を満たすことの確認方法」を確立することを目指して実施された。
- 自動車メーカー（BMW group、Daimler、Volkswagen、Audi等）、部品メーカー（Robert Bosch GmbHなど）、研究機関（German Aerospace Center、ダルムシュタット工科大学等）、認証機関（TUV）、ソフトウェアベンダーが参画。



出所) Pegasus Symposium 2019 “Introduction and Overview of 3.5 Years of PEGASUS”
 (<https://www.pegasusprojekt.de/en/pegasus-symposium-2019>), 2021年3月閲覧

Pegasusプロジェクト - Pegasus Method

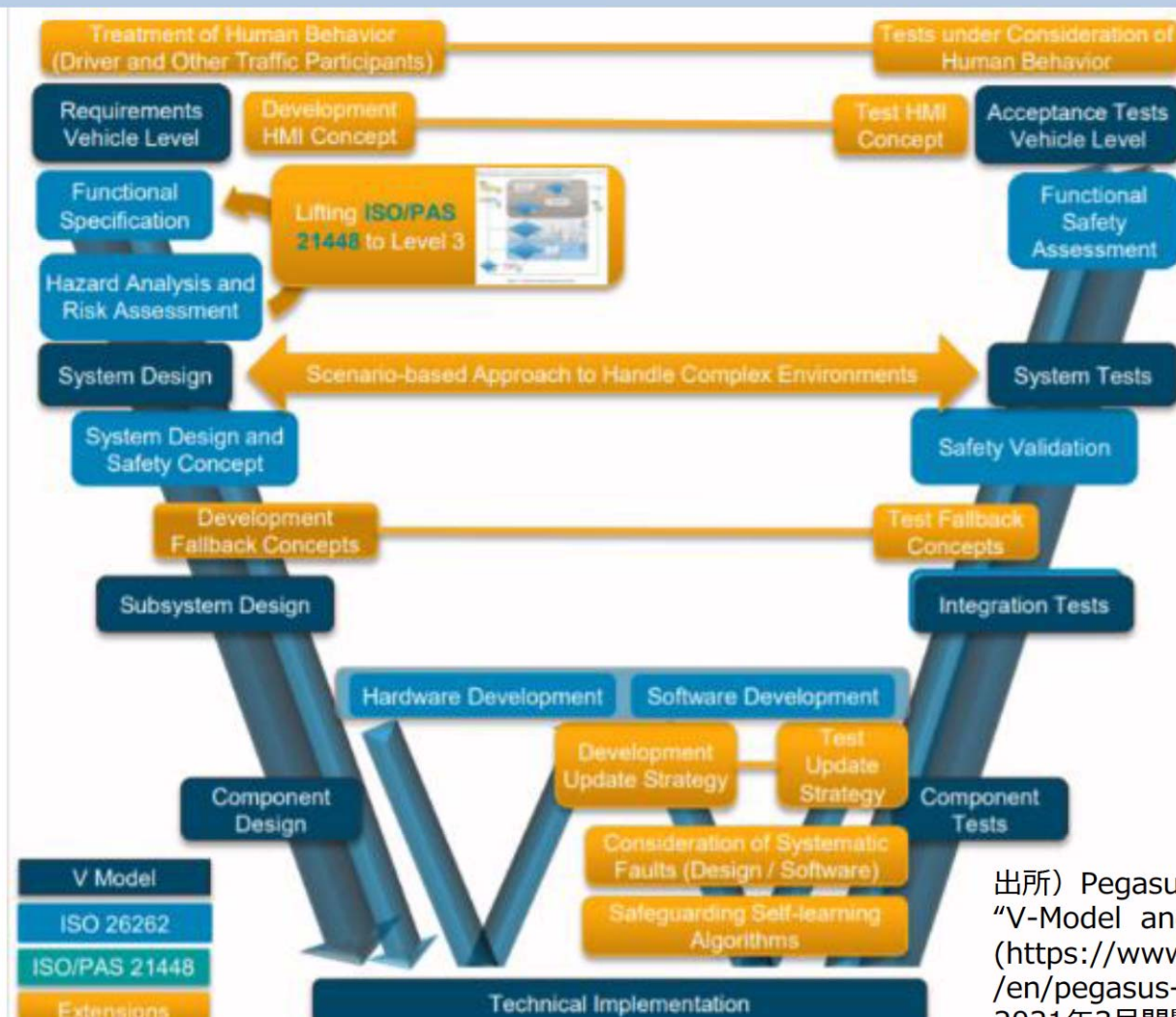
- 20ステップに及ぶ自動運転機能の評価フレームワーク（Pegasus Method）が提供された。
- 大きく「データ処理（シナリオ構築・フォーマット化）」「要求の決定」「データベース（テストシナリオ構築）」「アセスメントの実施」「論証」で構成される。
- 法律改正時などにアップデート可能とするためには自動化が必要であり、テキスト情報の知見のデジタル化および試験運転やシミュレーションデータの蓄積など、データドリブンのアプローチを採用している。



出所) Pegasus Symposium 2019 “Introduction and Overview of 3.5 Years of PEGASUS”
 (<https://www.pegasusprojekt.de/en/pegasus-symposium-2019>), 2021年3月閲覧

Pegasusプロジェクト - Vモデル

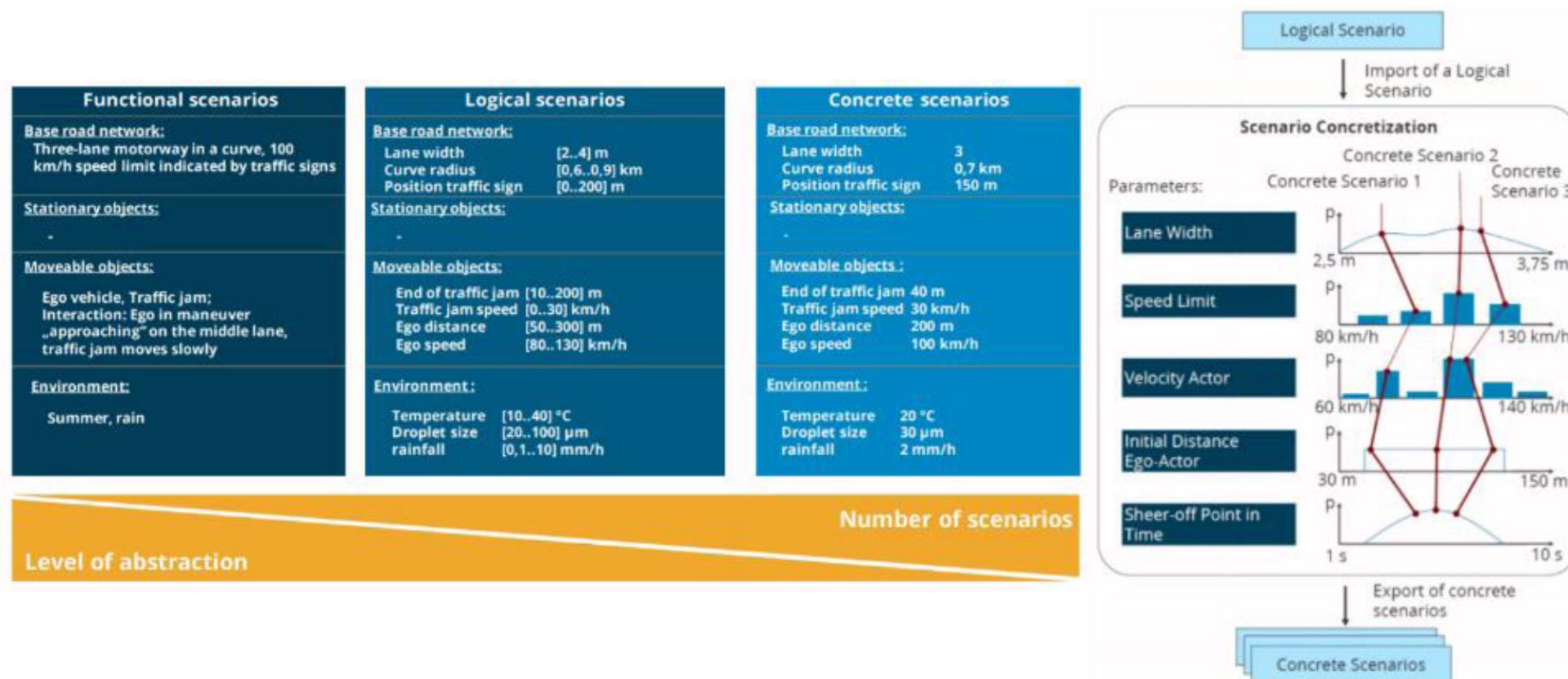
- 開発時にはISO26262（機能安全）への対応をベースにしながらも、ISO/PAS21448（現ISO/DIS21448、SOTIF）への対応を求めている。



出所) Pegasus Symposium 2019
 “V-Model and Process Analysis”
 (<https://www.pegasusprojekt.de/en/pegasus-symposium-2019>),
 2021年3月閲覧

Pegasusプロジェクト - 「テスト」の考え方

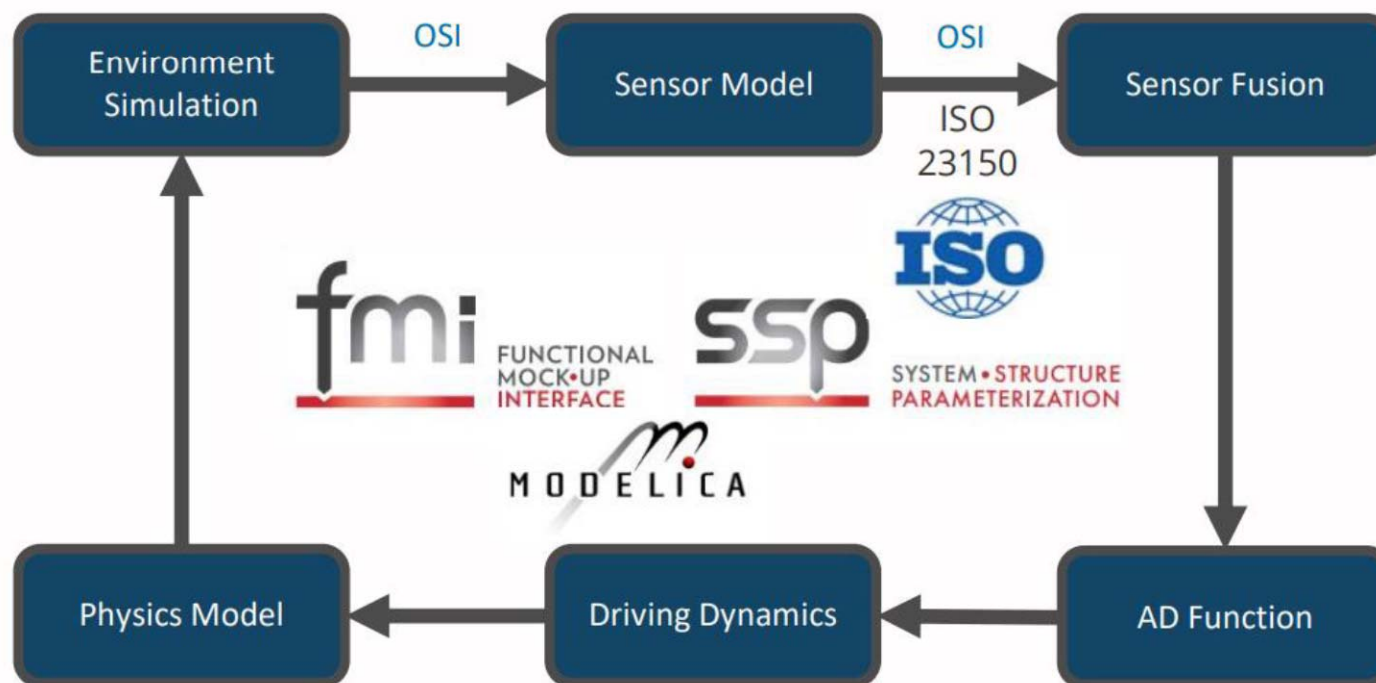
- テストを実施するうえでは「評価基準」、「シナリオ・パラメータスペース」「シミュレータでのテスト環境＋実域テスト環境（クリティカルケース対象）」を準備する必要がある。
- シナリオ構築手法として、Functional→Logical→Concreteとシナリオを具体化していくプロセスを提示している。このような安全論証のためのテストの考え方はシステムオブシステムズの評価においても参照されうる。



出所) Pegasus Symposium 2019 “Introduction and Overview of 3.5 Years of PEGASUS”
(<https://www.pegasusprojekt.de/en/pegasus-symposium-2019>), 2021年3月閲覧

Pegasusプロジェクト - 産官学の連携と標準化

- 自動運転用センサー（レーダー、LiDAR、カメラ、超音波センサー）とデータフュージョンユニット間のサービスインタフェースを定義した（ISO/FDIS 23150）。
- このようなシステムの評価体系を産業界で連携して確立したことで、今後技術開発を実施する各ステークホルダーにビジネスインセンティブをもたらす構造となっている。



出所) Pegasus Symposium 2019 "Sensor Models"
(<https://www.pegasusprojekt.de/en/pegasus-symposium-2019>), 2021年3月閲覧

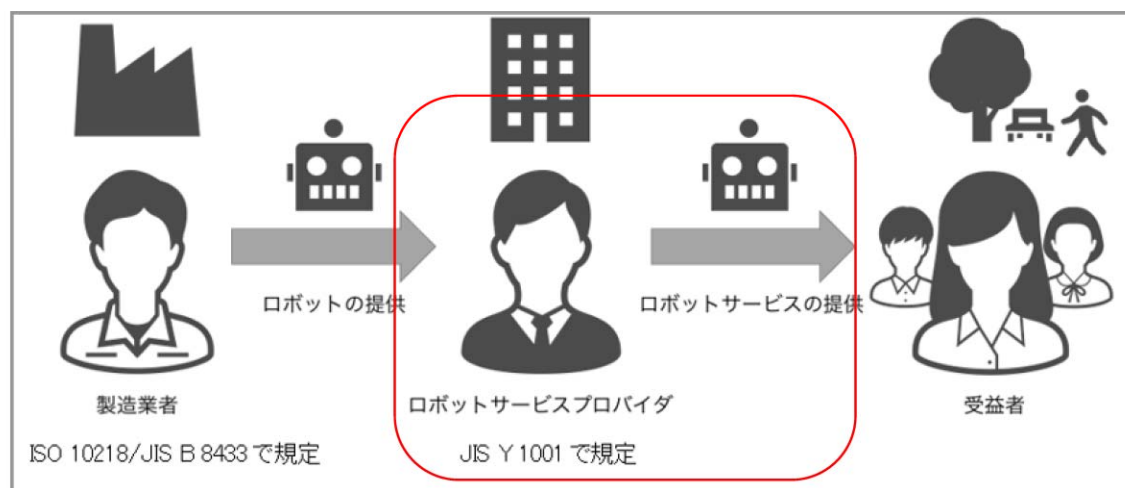
SoS課題解決の取り組み事例①

サービスロボット（JIS Y1001、自律移動型駅サービスロボット）

JIS Y1001（ロボットサービスの安全マネジメントに関する規格）

- サービスロボットに関しては、運用時の安全性保持のための規格が策定されていなかった状況にある。
- ロボット革命イニシアティブ協議会において産総研が中心となり議論を進め、成果を公表。
- 日本提案の新規格としてJIS Y 1001を作成し、ISO TC299に新規の標準化課題として提案中。

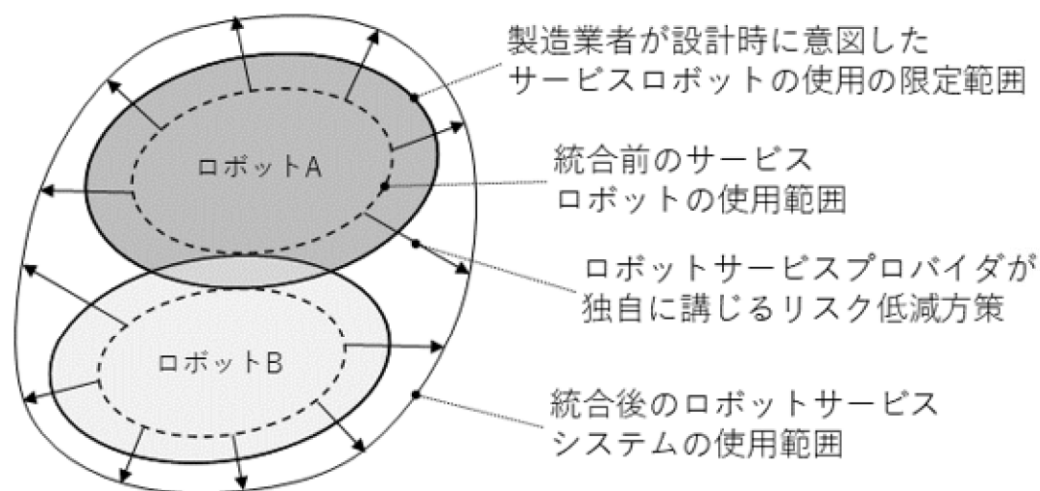
対象分野	ロボット本体（機械）の安全	ロボット運用時の安全
産業用ロボット	ISO 10218/JIS B 8433	ISO 45001/労働安全衛生法
サービスロボット	ISO 13482/JIS B 8445 及び JIS B 8446-1～3	従来なし ↓ 新規格（JIS Y 1001）



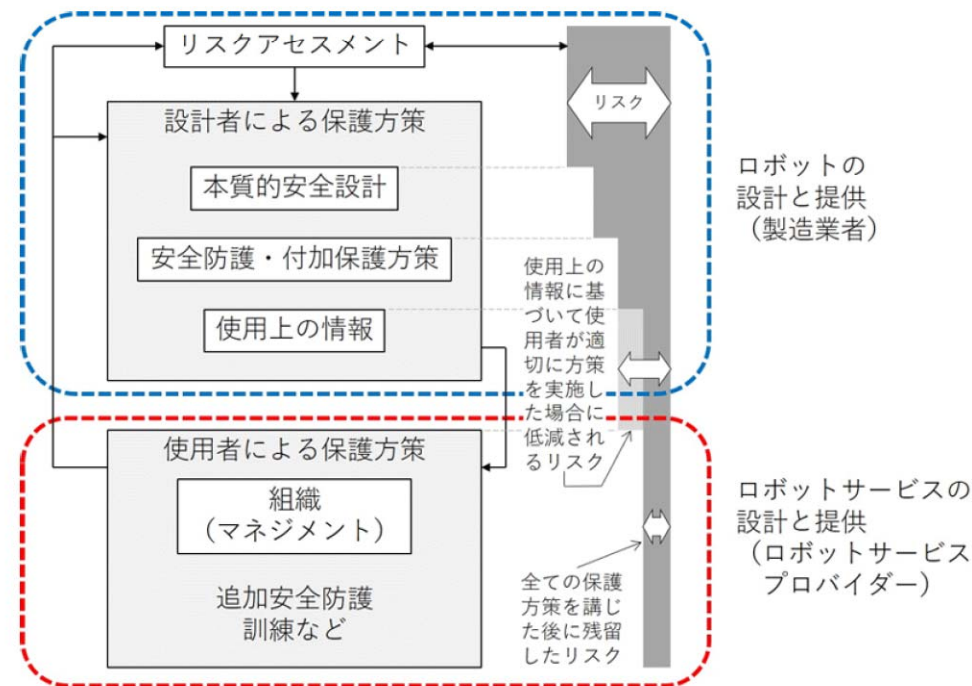
出所) 産総研ウェブページ (https://www.aist.go.jp/aist_j/press_release/pr2019/pr20190520/pr20190520.html)、2021年1月5日閲覧

JIS Y1001（ロボットサービスの安全マネジメントに関する規格）

- 異なる製造業者による複数のロボットを同じ場所でサービス提供する場合、使用範囲が広がるため製造時には想定していなかったリスクに対処する必要がある
- そのため、ロボットサービスプロバイダーが実施すべきリスクアセスメントやリスク低減方策などの安全管理とマネジメントについて規定を行っている。



複数ロボットの場合に重複範囲が発生

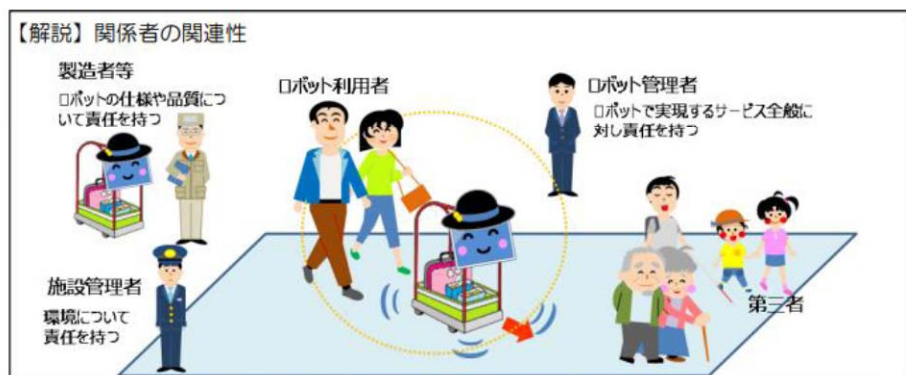


サービスプロバイダー部分のリスクマネジメントを検討する必要

出所) 産総研ウェブページ (https://www.aist.go.jp/aist_j/press_release/pr2019/pr20190520/pr20190520.html)、2021年1月5日閲覧

具体的なガイドライン：自律移動型駅サービスロボット

- (一社) 日本鉄道車両機械技術協会が、「自律移動型駅サービスロボットの安全性確保に関するガイドライン」を策定。これは、生活支援ロボット及びロボットシステムの安全性確保に関するガイドライン（第一版）、ISO規格等に合致し、駅特有の事情を考慮に入れて策定されたものである。
- 付表として「駅リスクの勘所」を付け、駅構内における箇所別に、想定されるリスクとリスク度合いを示した。



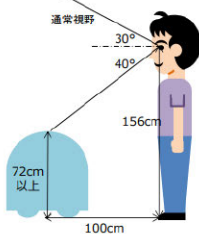
※事故発生時の過失割合は事故原因を元に判断される

【解説】

例えば低床型AGVなど、第三者の視界に入りにくい駅サービスロボットを運用すると第三者と接触する可能性が高まる。第三者から気づかれやすい全高であることやライトの点滅など気づかれやすい工夫をすること。

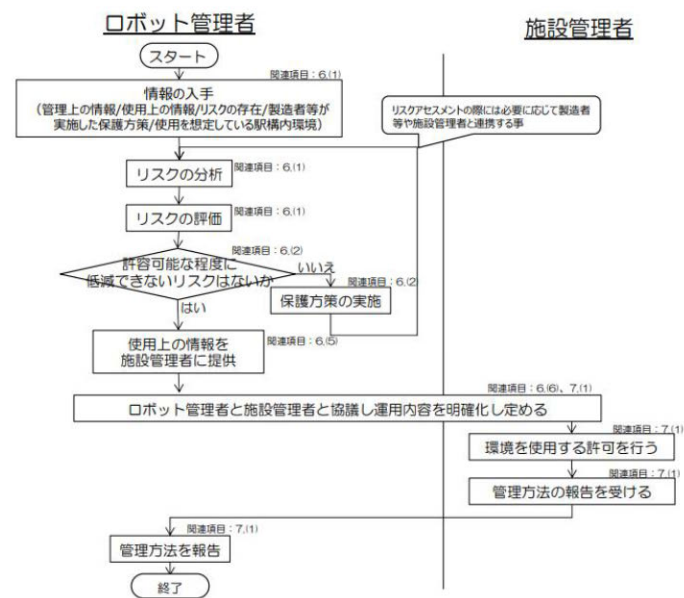
バリアフリー設備ガイドライン（旅客施設編）（平成19年7月 国土交通省）（以下、バリアフリーガイドライン）より、立位にて1mの距離より視認可能な全高72cm以上であることが望ましい。（立位の視点高（156cm）、通常視野内（下位40°））

また、移動時には音声等を鳴らしながら移動することで注意喚起を促すことができる。音声・音響案内についてはバリアフリーガイドラインの定めに従い視覚障害者への配慮とともに騒音とならないよう必要最低限に留めるよう留意すること。また、バリアフリーガイドラインでは、ホーム上の階段における音響案内は鳥の鳴き声を模した音響とするなど標準例が定められている。駅サービスロボットの移動に関する音響案内についても、駅サービスロボットの種類に関わらず各箇所に共通とすることが望ましい。



【補足】ロボット管理者におけるリスクアセスメントのフローについて

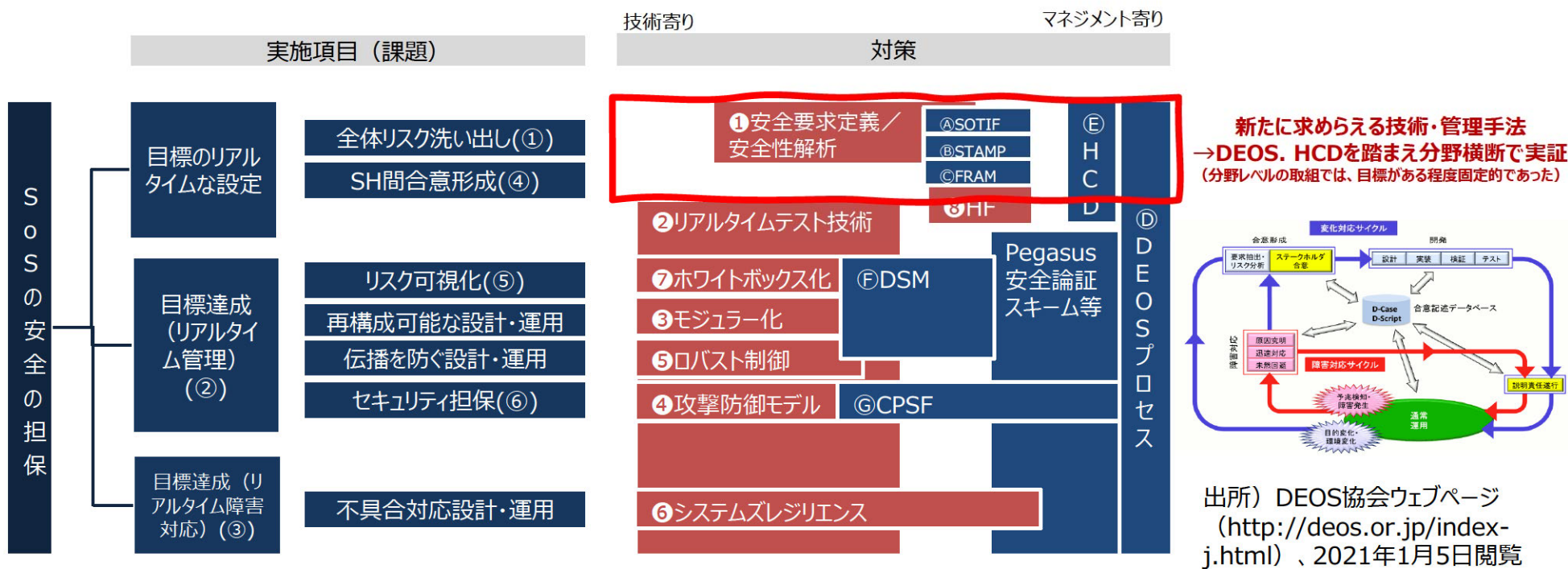
フロー1



出所) (一社) 日本鉄道車両機械技術協会「自律移動型駅サービスロボットの安全性確保に関するガイドライン 解説」
(http://www.rma.or.jp/robotguideline/files/pdf/robot_guideline_comment.pdf)、2021年3月閲覧

1. 2小括 システムオブシステムズにおける今後の課題と解決のアプローチ

- SoSの安全は「**目標のリアルタイムな設定**」と「**リアルタイム管理・障害対応（及びその説明）**」を通じて実現される。
- 「目標を達成（リアルタイム管理・対応）」する技術として、システムの再構成、不具合の伝播を防ぐための仕組み等といった個別技術が開発されつつある。（既存システムもSoS的な要素を大いに含んでいるため）
- 今後、より重要となるのは、「**目標のリアルタイムな設定**」を実現する技術にある。様々なステークホルダの意思のデータベース化、それを基にした目標設定の自動化等が求められる。（安全論証の上位部分のパターン化が必要であり、それはD-CaseのDEOS基本パターンが原型となり得る）
- これにより、**より高次元のサービス提供**が可能となる。（例えば都市レベルでは、「快適な移動サービスの機能を保ったまま道路工事を実施する」ことを明に要求する、ユーザを思いやる「おもてなし精神」を評価できる場を作る、等）



2. システムオブシステムズの安全性・信頼性の実現に向けた産業分野の検討

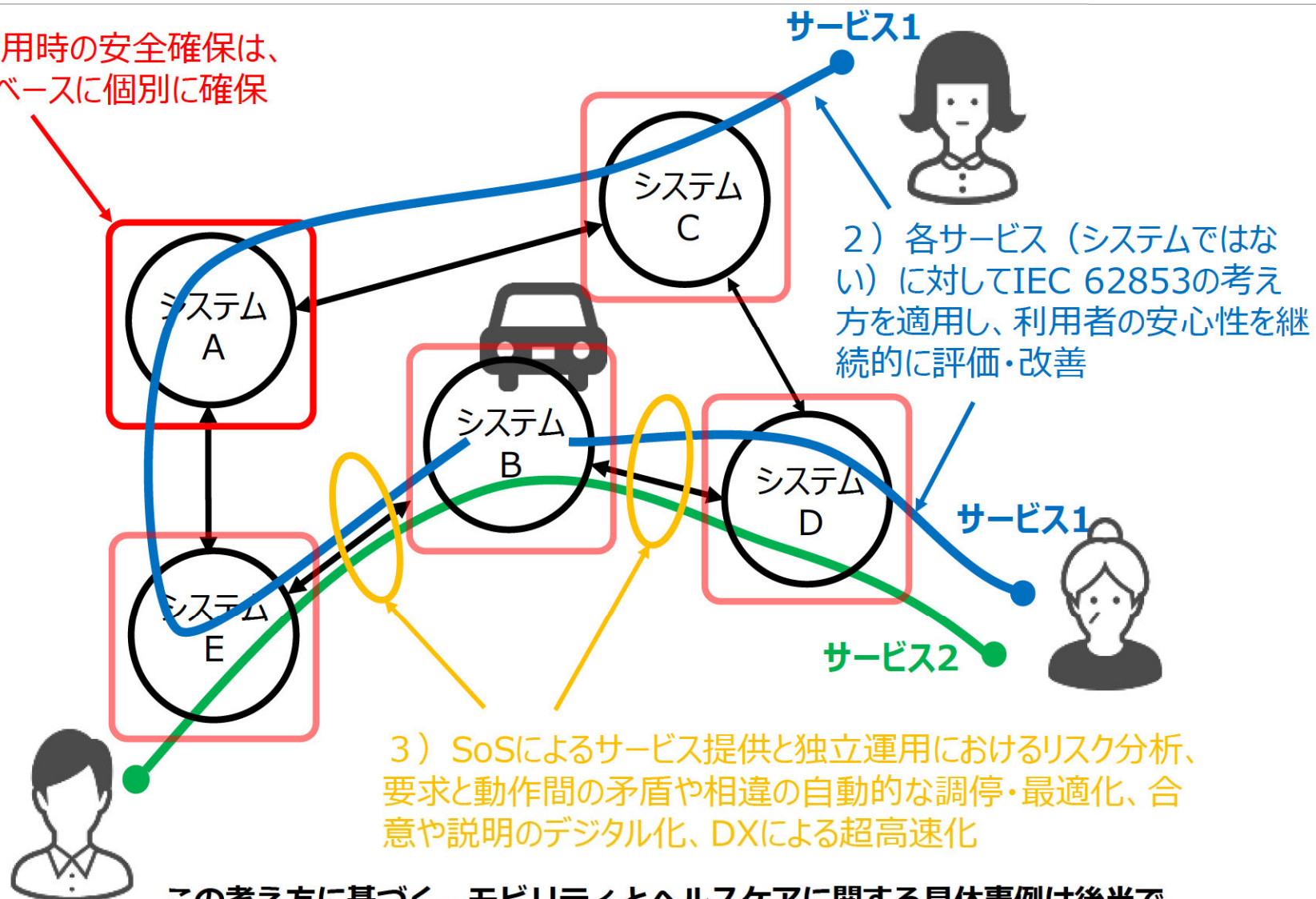
2. 1 システムオブシステムズの安全性・信頼性の国際ルール形成を通じて競争優位を実現する産業分野の選定

本節のポイント

- Society5.0の実現に向けては、サービスごとに別々のシステムを開発して、利用者がそれらを取捨選択して利用する選択方式ではなく、独立したサービスを提供する個々のシステム同士を柔軟に連携させ、新しいサービスを生み出す連携方式が望まれる
- 独立したサービスを提供するシステム同士を柔軟に連携させて構築するシステムは、システムオブシステムズ（SoS）と呼ばれるが、SoSの開発、運用に関する方法論や技術的課題、開発者や利用者といった人への影響については、十分に整理されていない
- 本資料では、SoSを対象に、安全確保の方法、人間中心設計、SoS運用時のルールやガバナンスの整備、という3つの視点から、潜在的に発生しうる課題と、それらを解決しながら生まれる**新しい価値**を検討する

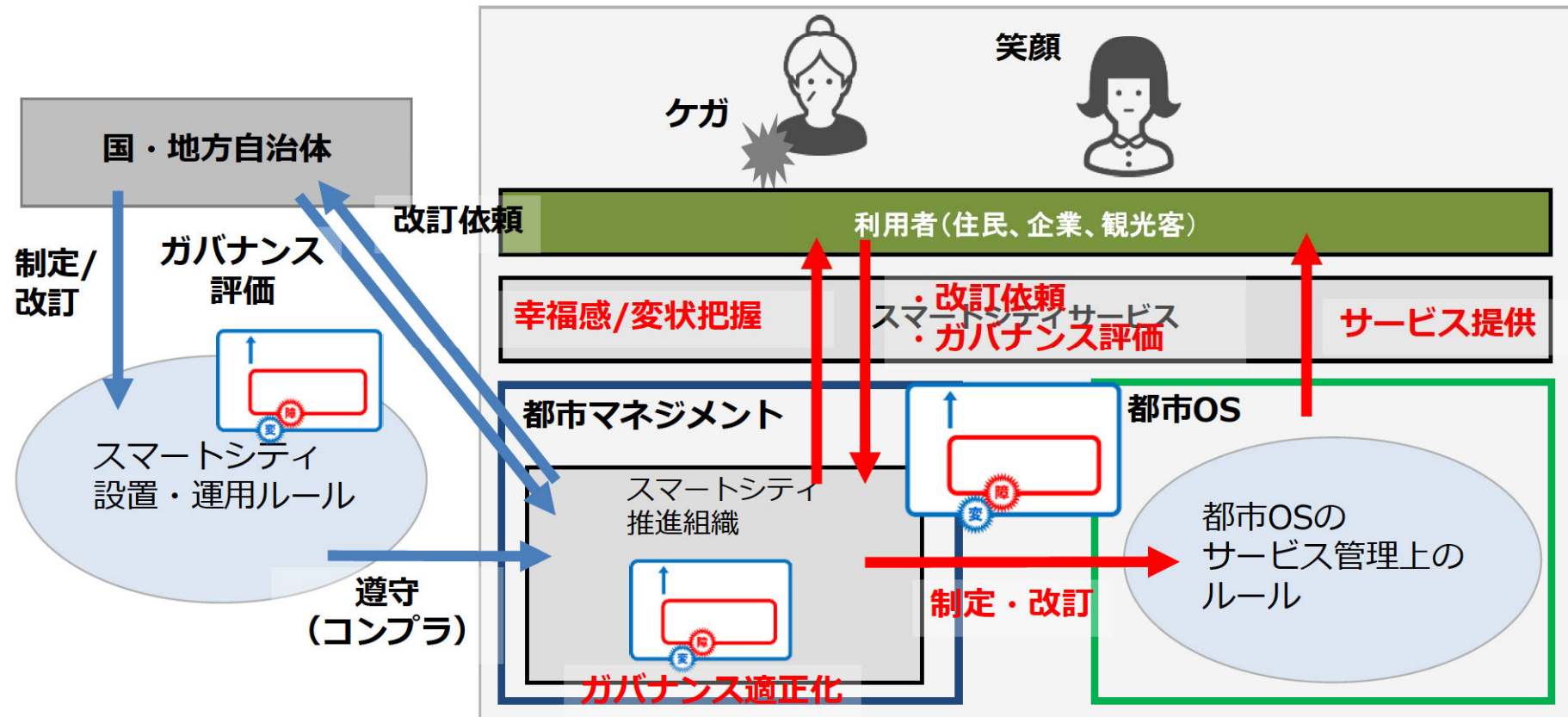
SoSにおける安全性確保（安全要求導出）の基本的な考え方（案）

1) 独立運用時の安全確保は、機能安全をベースに個別に確保



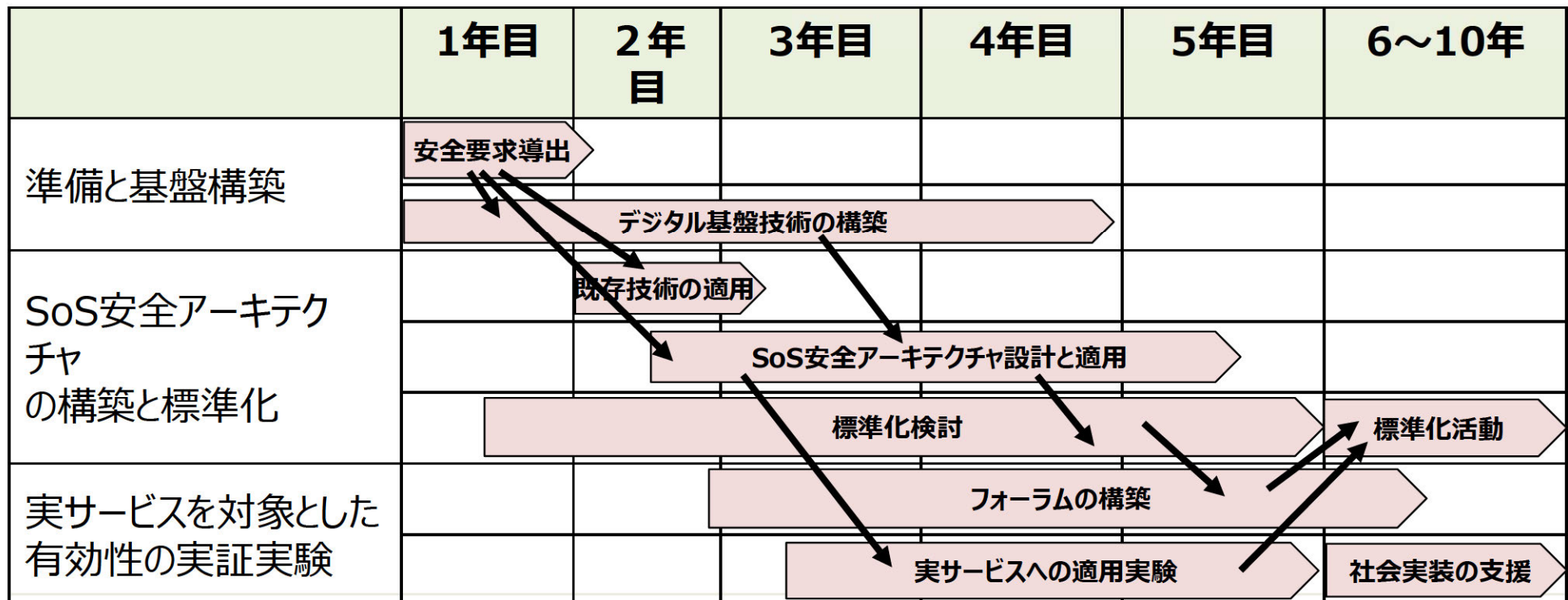
スマートシティのガバナンスとルール制定に関する提案

- 利用者と都市OSを維持、発展するための都市マネージメントの確立
- 都市マネージメントの継続的なガバナンス評価と適正化
- 利用者、都市OS、都市マネージメントにおいて発生する変化や障害だけでなく、利用者の幸福度の状況を把握して、ルールを迅速に改訂、適用する仕組み



フォーラム標準の構築に向けた活動項目とロードマップ案

- 実サービス（スマートシティ、ヘルスケア、ドローン等）を対象に安全要求導出を試行
- 安心性向上に向けて、IEC 62853の実運用を支えるデジタル基盤技術の構築
- 既存安全技術の有効性評価と、SoSにおける安全アーキテクチャの設計と標準化
- 実サービスの運用段階に対して、SoS安全アーキテクチャとデジタル基盤技術を適用した有効性の実証実験



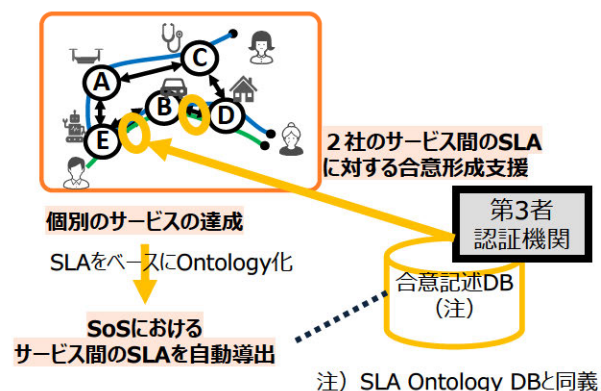
2. 1 小括 産業分野の選定

- システムオブシステムズの安全性・信頼性の国際ルール形成を通じて競争優位を実現する産業分野の選定として、以下の分野を選定した。

- ① スマートシティにおけるモビリティとヘルスケアの事例
- ② IoT住宅におけるSoSの事例
- ③ 人への影響分析（課題）と事例

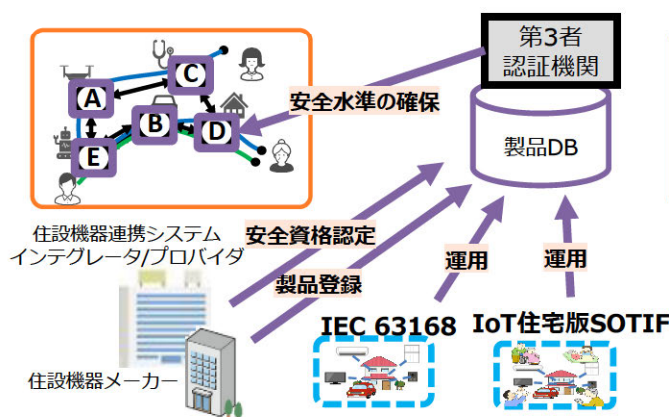
① モビリティとヘルスケア

異業種サービス連携を推進する合意形成支援技術



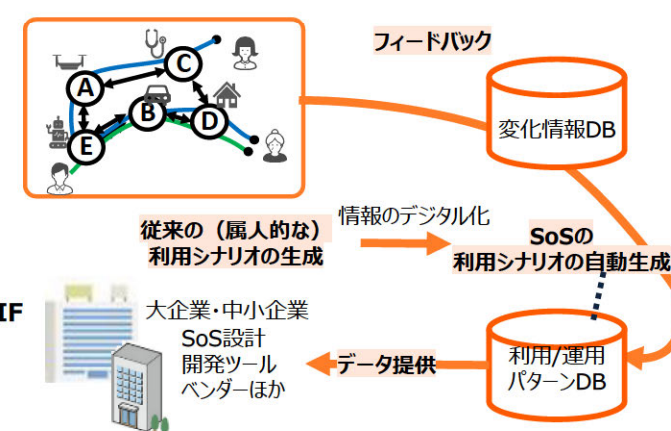
② IoT住宅

IoT住宅の住設機器連携における安全確保技術



③ 人への影響分析（HCD）

利用者の変化に対応するシミュレーション技術



2. システムオブシステムズの安全性・信頼性の実現に向けた産業分野の検討

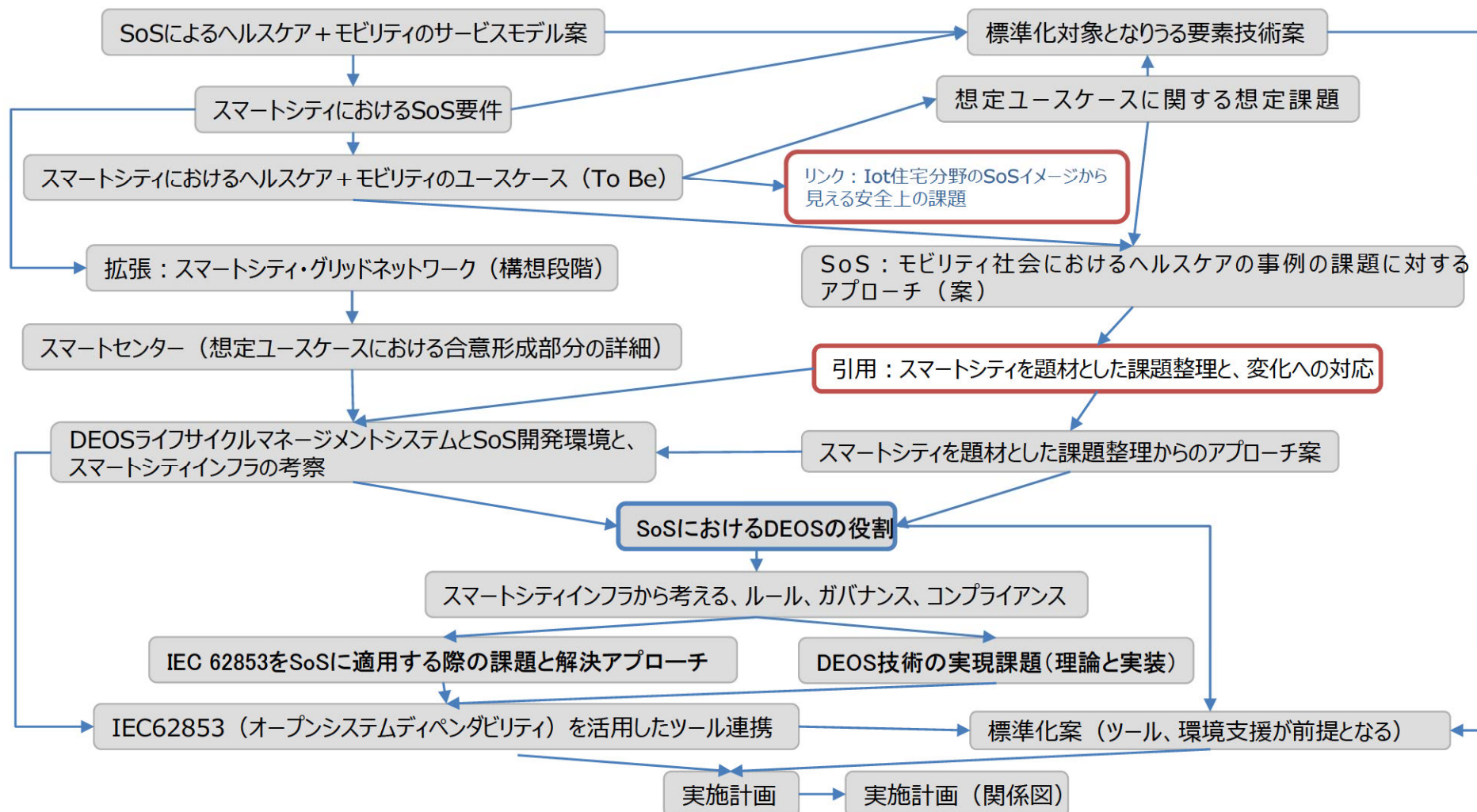
2. 2 システムオブシステムズの安全性・信頼性の実現に向けた産業分野や技術の事例調査及びロードマップの策定

①スマートシティにおける モビリティとヘルスケアの事例

本セクションの構成（ページ間の関連）

凡例：ページタイトル

- スマートシティ（ソサエティ5.0フィールド）におけるSoSの安全性、信頼性達成の考察ダイアグラム
- DEOSライフサイクルプロセスの適用課題、実施、具体的な計画案を検討



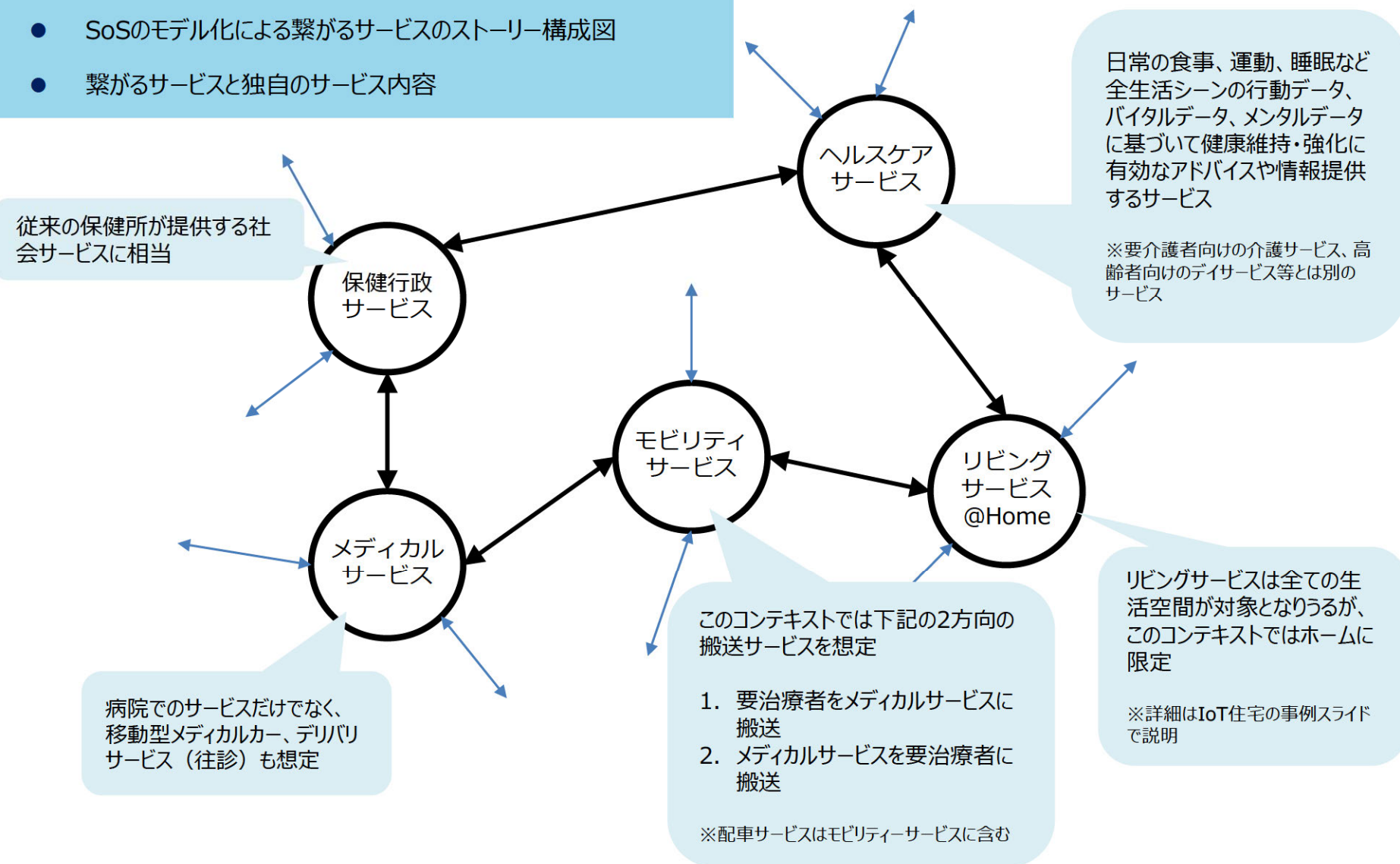
索引

● 用語の解説

用語	意味	注釈
Ontology	別添資料にて解説	OWL、DL Ontology
Terminology	別添資料にて解説	ISO704
SLA	サービスレベルアグリーメント：サービス提供者が、利用者に同意を求めるサービスの内容に関する右記述文書、あるいは契約書	https://www.meti.go.jp/policy/netsecurity/secdoc/contents/downloadfiles/080121saasgl.pdf
永続化	データベース等の技術により、データを保管、保護する技術	
合意形成	ステークホルダー、関係者によって合意される情報（意見の一致）とその形式	
合意モデル	合意を求める形式（例：ツールミンモデル、論証分析）	https://crd.ndl.go.jp/reference/modules/d3ndlcrdentry/index.php?page=ref_view&id=1000116055
情報銀行	総務省検討事案	https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/html/nd261250.html
都市オペレーティングシステム	ハードウェアのためのOSではない。スマートシティ上の膨大な情報空間を制御するためのアプリケーションプラットフォームを想定	出展：スマートシティリファレンスアーキテクチャホワイトペーパー第1版、SIP第2期ビッグデータ・AIを活用したサイバー空間基盤技術におけるアーキテクチャ構築及び実証研究事業、2020年3月31日
都市マネージメントライブラリ	上述のオペレーティングシステムが活用する、組織、ビジネスをルール&ガバナンスを持って駆動する情報群	

SoSによるヘルスケア＋モビリティのサービスモデル案

- SoSのモデル化による繋がるサービスのストーリー構成図
- 繋がるサービスと独自のサービス内容



スマートシティにおけるSoS要件

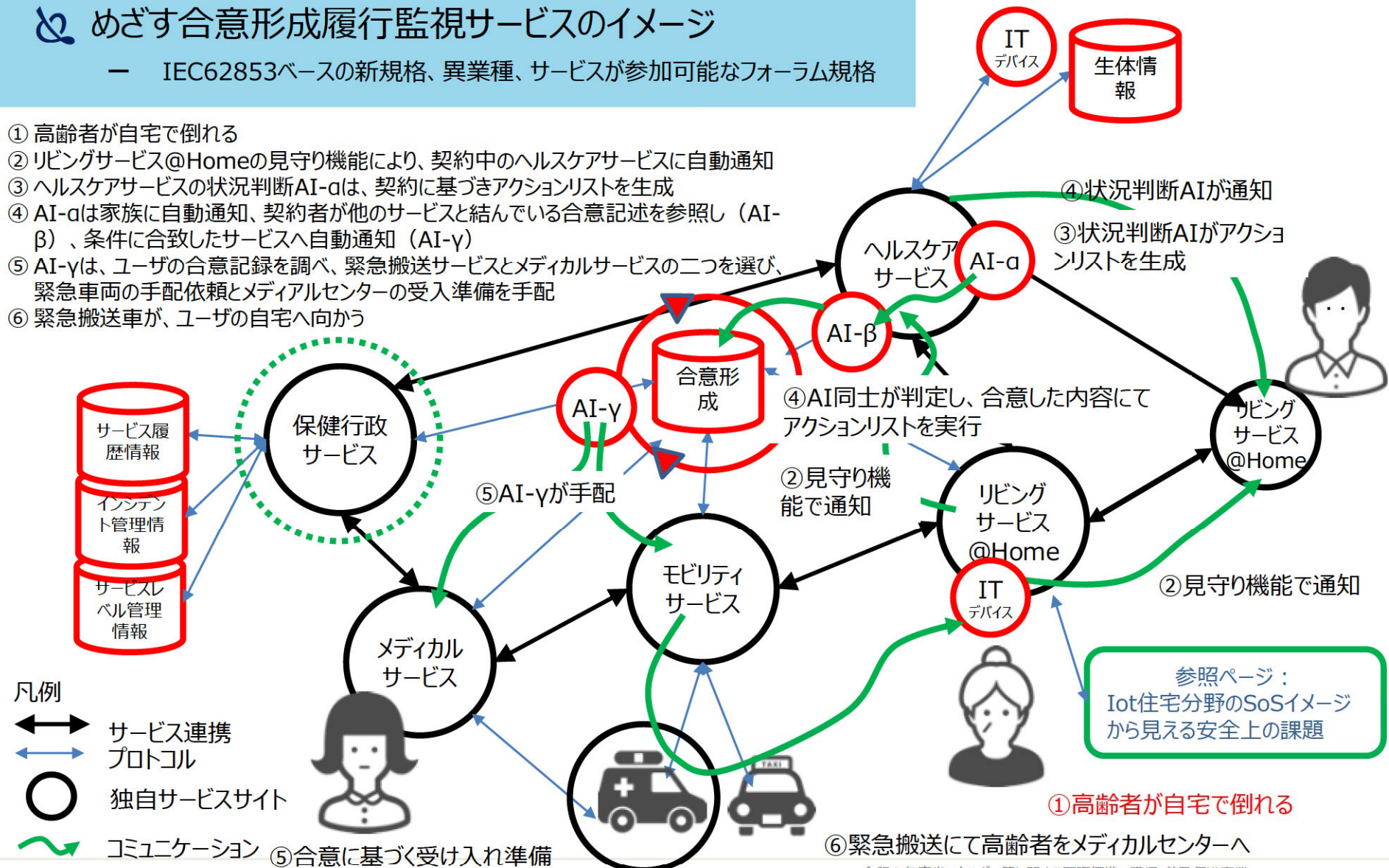
- スマートシティにおける独自サービスの存在
- 各サービスが連携して、さらに複数のサービスと状況を共有しながら、選択的サービスの実現
- サービス提供者とユーザの間でかわされるサービスの内容と契約条件等は、合意形成データベースによって扱われる。その合意に付帯する条件等のデータは、連携するデータベース間の接続によって分散化し、複数の合意における条件判定に用いられる
- 人の生活データ、生体データ、臨床データを時系列情報として永続化するプラットフォームが必要
- 生命維持の課題から分単位のサービスレベルの向上を目指し、AIの導入と、AI間の連携により複雑な条件における最適な選択を最短で実施できる
- 統合されたサービスの実施状況のモニタリングとサービス停止等の重篤なインシデントは、集中管理された後、再発防止と改善策の提出等を求める機構の存在

スマートシティにおけるヘルスケア＋モビリティのユースケース（To Be）

めざす合意形成履行監視サービスのイメージ

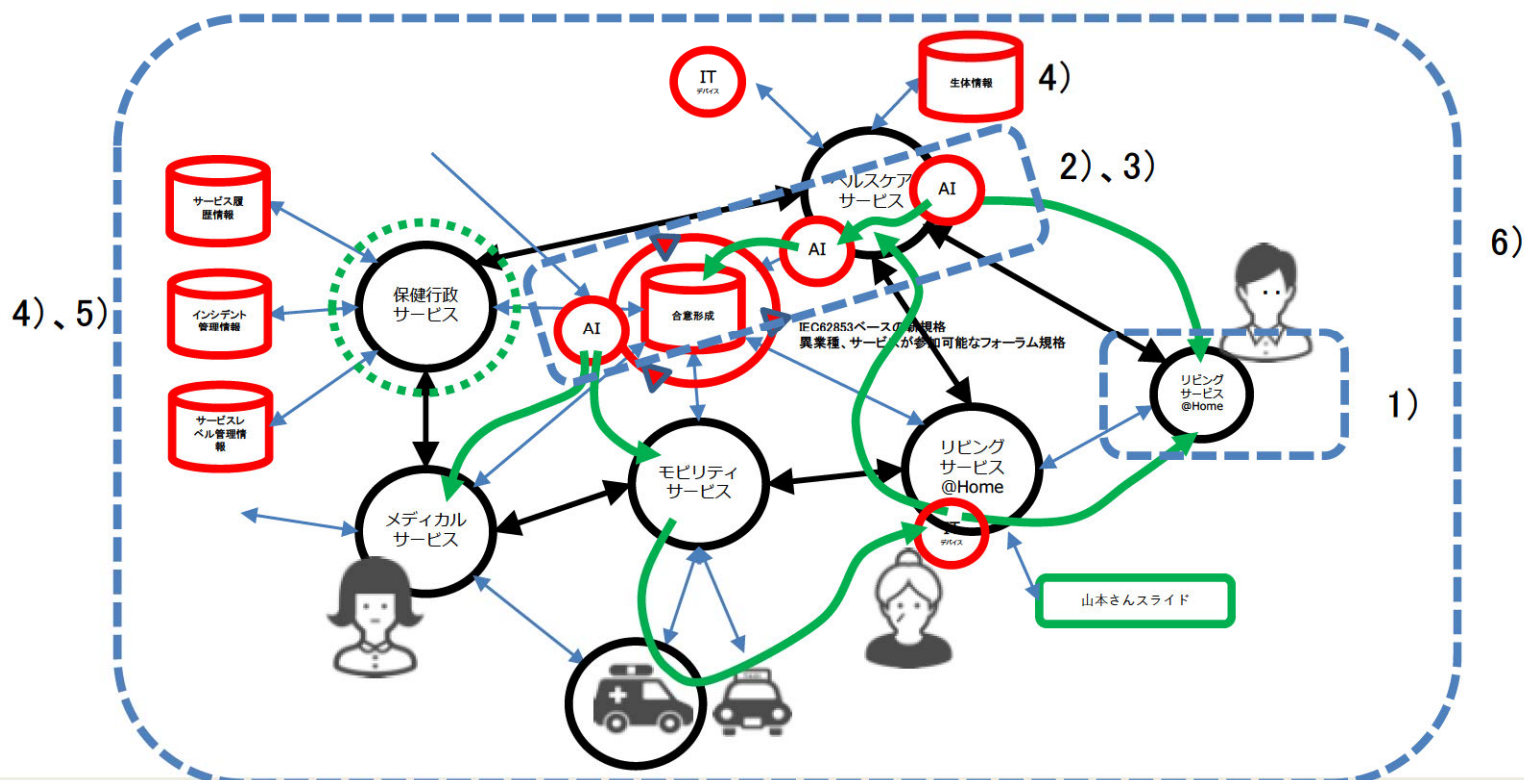
— IEC62853ベースの新規格、異業種、サービスが参加可能なフォーラム規格

- ① 高齢者が自宅で倒れる
- ② リビングサービス@Homeの見守り機能により、契約中のヘルスケアサービスに自動通知
- ③ ヘルスケアサービスの状況判断AI-aは、契約に基づきアクションリストを生成
- ④ AI-aは家族に自動通知、契約者が他のサービスと結んでいる合意記述を参照し（AI-β）、条件に合致したサービスへ自動通知（AI-γ）
- ⑤ AI-γは、ユーザの合意記録を調べ、緊急搬送サービスとメディカルサービスの二つを選び、緊急車両の手配依頼とメディカルセンターの受入準備を手配
- ⑥ 緊急搬送車が、ユーザの自宅へ向かう



想定ユースケースに関する想定課題

- 1) 独立運用時の安全確保は、機能安全をベースに個別に確保→〇の独立サービス領域
- 2) 独立サービス間の連携プロトコル（自動[AI等]による条件判別）
- 3) 複数のAI間協調判定の監視、または判定の合理性、妥当性検証
- 4) 個人情報の保全と開示条件（情報銀行）
- 5) サービス不履行等における回避機能（n次的サービスの監視）
- 6) 独立サービスのアップデートによるサービス継続の自動解析（合意記録の検証）



標準化対象となりうる要素技術案

- SoSスマートシティのターミノロジー
 - － テキスト、構造化：Terminology（ISO704）
- 文書：サービスアグリーメント
 - － 構造化文書：テキスト、数値、対象サービス
 - － 計算：Terminology（ISO704）を用いたOntology形式によるサービス妥当性証明（たぶんOWL）
- 文書：合意形成
 - － 構造定義：テキスト、論証分析によるOntology（OWL）、合意グラフ
- データ種：AI
 - － テキスト、ルールベース（YAML他）
- データ種：データベース
 - － SQL、NoSQL、意味グラフ形式（DL Ontology）、時系列データフォーマット（考案中）
 - － 構造化データ
- 監視
 - － 映像、写真、音声、音、イベント

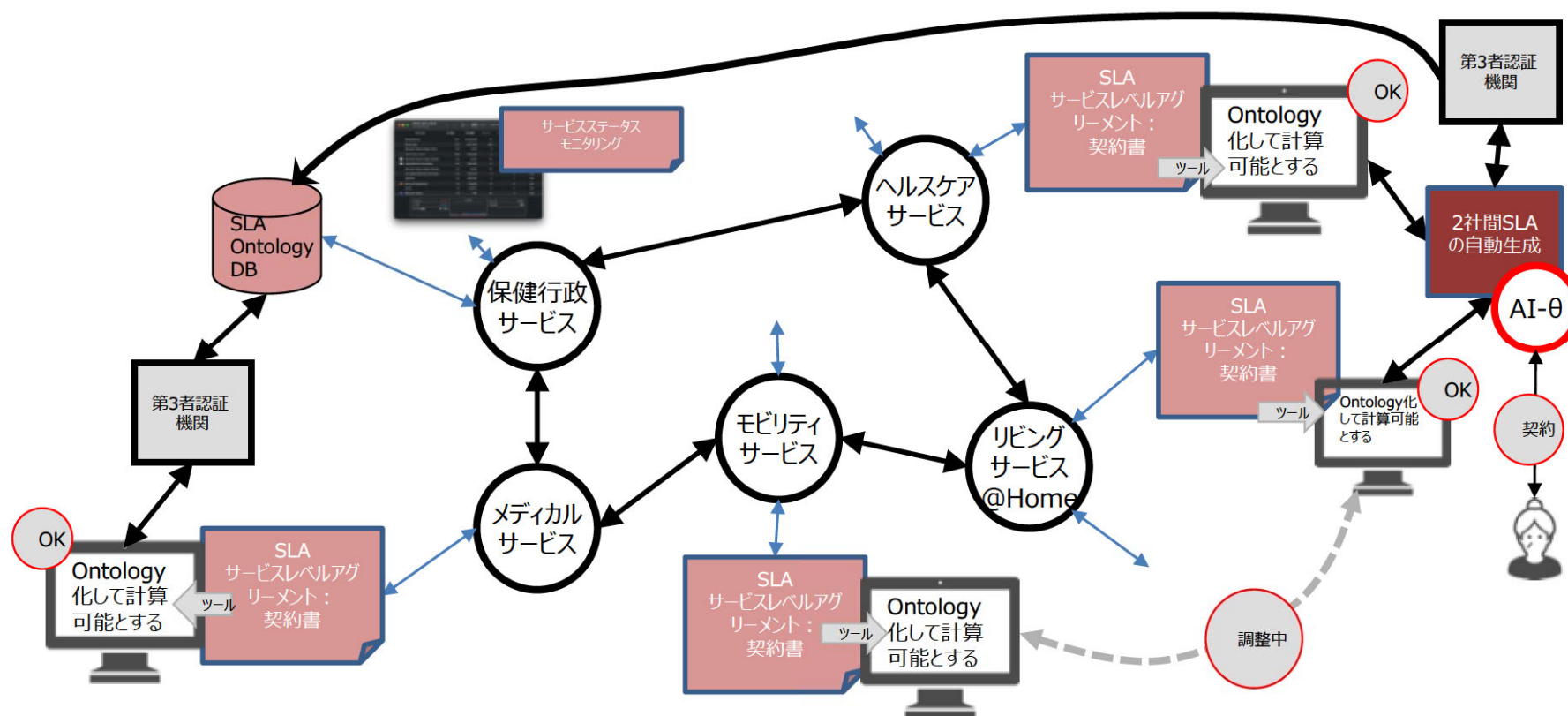
今後、SoS標準アプリの設計（プロトコル）の策定、アーキテクチャの表現手法と計算理論を検討

SoS : モビリティ社会におけるヘルスケアの事例の課題に対するアプローチ (案)

各個別システムのサービスレベルを第3者検証し認証する仕組みがベース

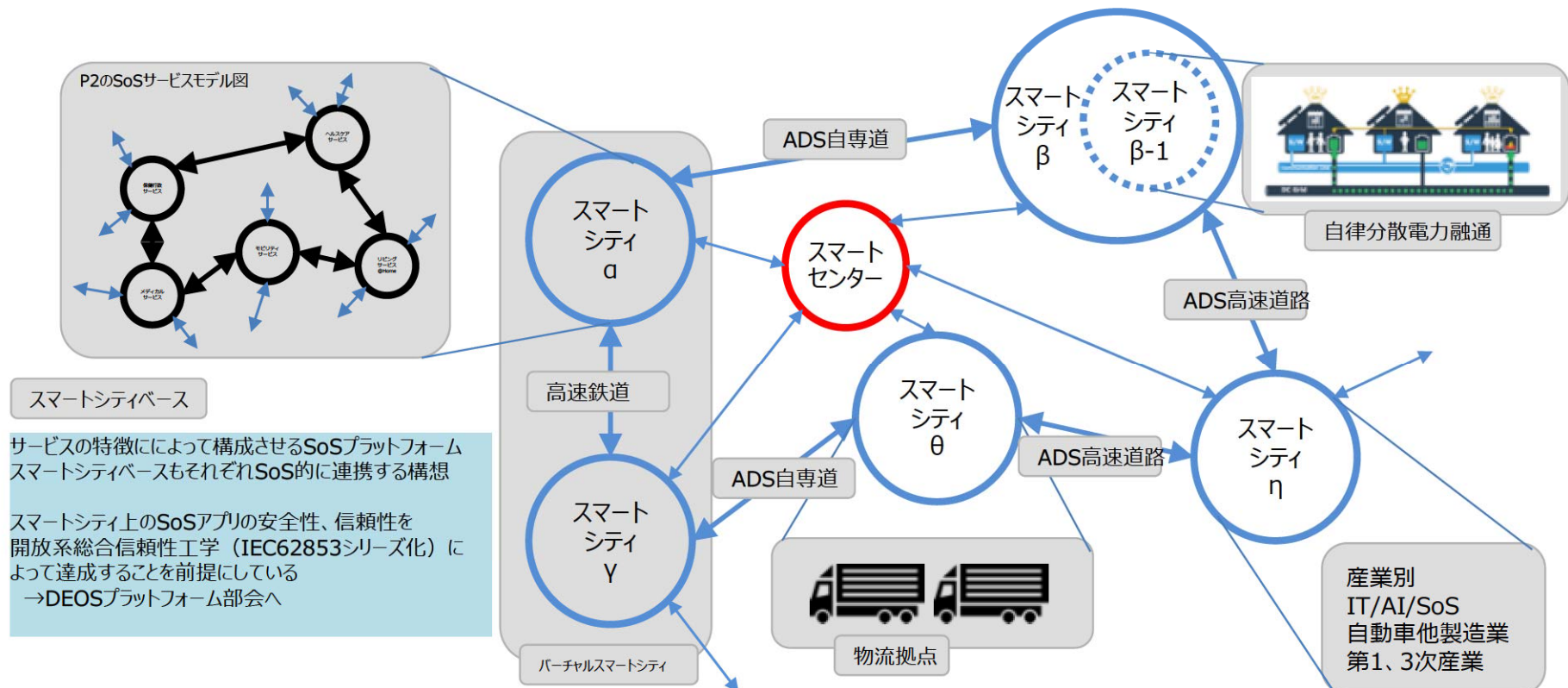
1. 個別サービスの達成をSLAをベースにOntology化して、妥当性検証を計算可能とする
2. 接続するサービス間のSLAを自動導出することで、2社間のサービスレベルの合意形成をおこなう
3. ユーザは、自動導出されたSLAに対して、契約をおこなうが、サービスエージェントが必要

➤ Ontologyは、スマートシティTerminologyを用いる前提であり、スマートシティTerminologyは、スマートシティアーキテクチャから定義されるものとする



拡張：スマートシティ・グリッドネットワーク（構想段階）

- スマートシティは、10数件のリビングサービス@Homeの規模から数十万人規模の中核都市までを想定して、それぞれサービスの特徴からスマートシティベースがあるものとする
 - スマートシティベースは、SoSのインフラ機能
 - インタースマートシティは、モビリティサービスで接続されている



スマートセンター（想定ユースケースにおける合意形成部分の詳細）

● めざす合意形成履行監視サービスのイメージ

- IEC62853ベースの新規格、異業種、サービスが参加

スマートセンター

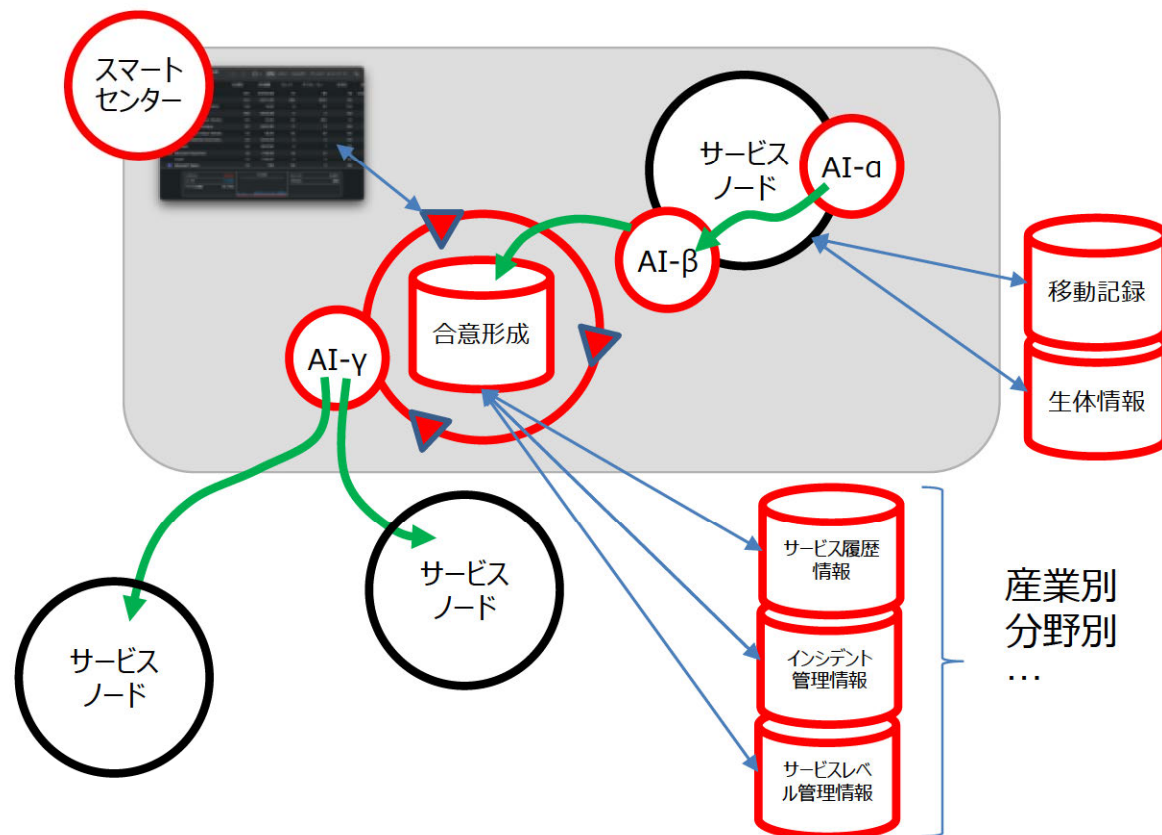
合意形成とその履行を監視する機構

運営監視
合意形成プロセス、ツールの提供
AI向けI/Fの提供
合意形成の履行監視（インターバル型）

ビジネスアナリシス

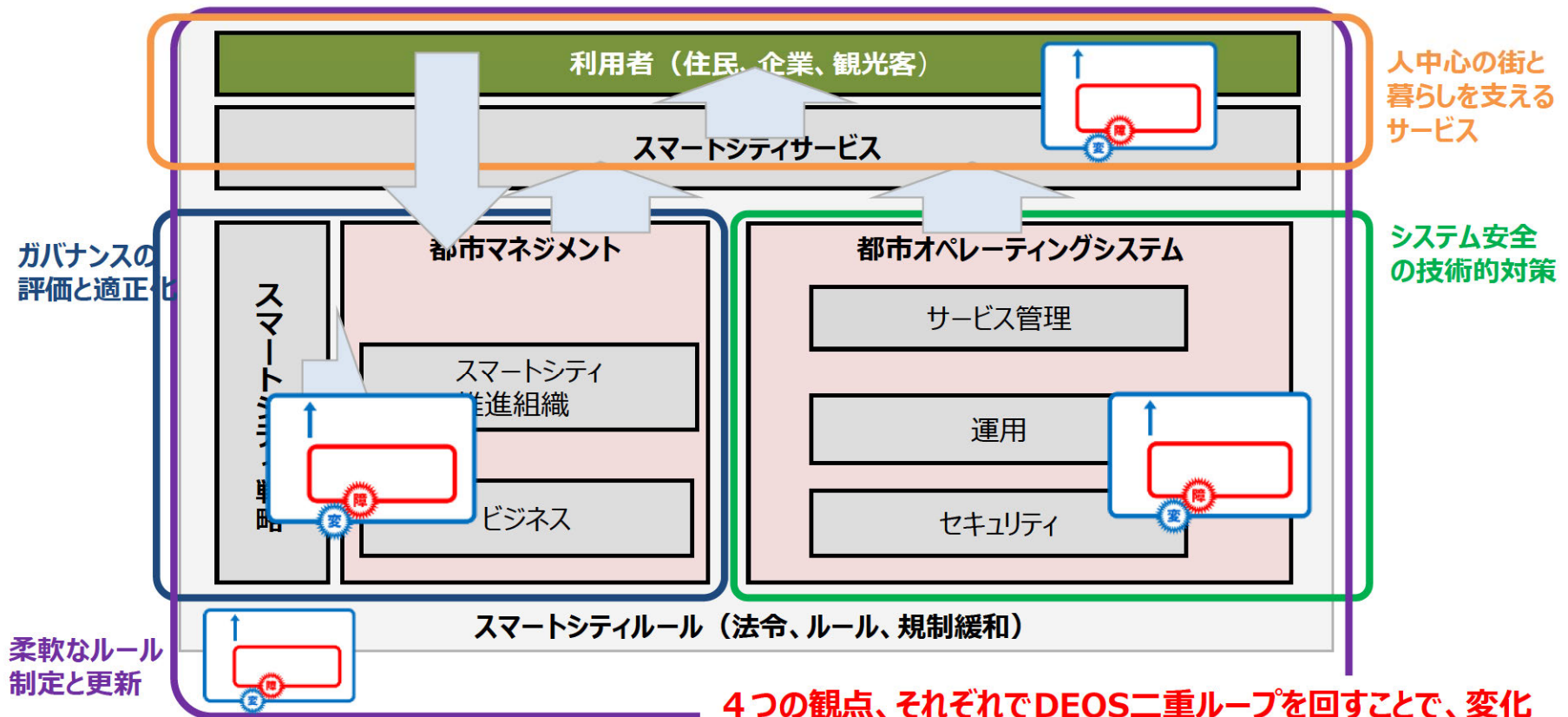
既存サービスの実効解析から、新規のサービスの発見

運用時系列データから、よりよい新サービスをAIが提案



スマートシティを題材とした課題整理と、変化への対応

- 「人中心の街と暮らしの継続的发展」を実現するための適切なサービス提供
- サービス連携時の安全を確保する技術的対策と方法論の確立
- 街運営のガバナンス評価と適性化、発展を促進に向けて柔軟なルール制定と更新



4つの観点、それぞれでDEOS二重ループを回すことで、変化に対応しながら継続的に街と暮らしを発展

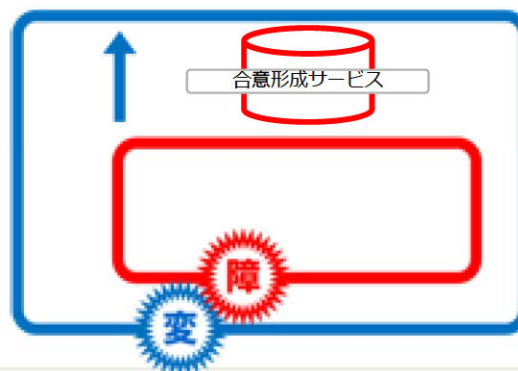
出所)「スマートシティリファレンスアーキテクチャ」を参考に独自に作成

スマートシティを題材とした課題整理からのアプローチ案

- スマートシティにおける安全を確保する技術的課題の整理と方法論の確立
 - SoSに適したアーキテクチャのモデリング設計と、制度、運用面から検討した柔軟性のあり方
- スマートシティに関係する人（住民、企業、観光客、管理組織）への影響分析
 - 生活様式からのニーズ・ウォンツのリストとサービスのギャップ分析、働き方多様化への業務規定の柔軟性、管理の自動化
- スマートシティの維持・発展を促進するルール、運営組織のガバナンス維持の課題
 - 変化、進化を促すルールの考案、想定課題を元にガバナンスシミュレーションを実行し、未然災害、人災への備え

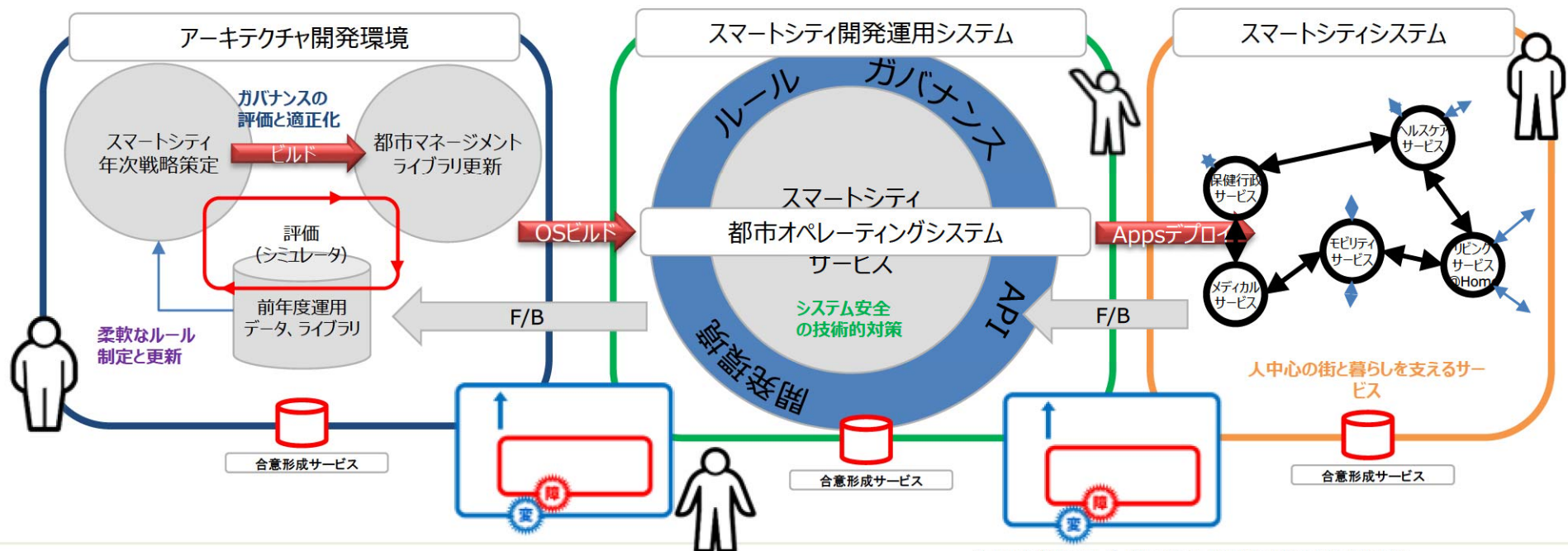


DEOSライフサイクルマネジメントを用いたソフトウェアの安全性・信頼性の構築環境ならびに実行、監視サービスの具体化（次頁に詳細）



DEOSライフサイクルマネジメントシステムとSoS開発環境と、スマートシティインフラの考察

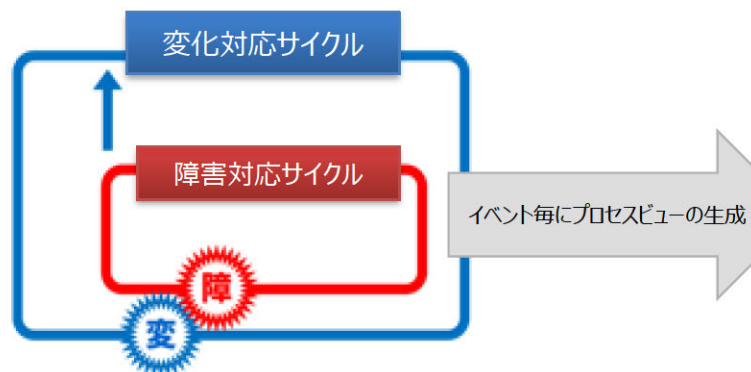
- アーキテクチャ開発環境を構築し、年次戦略をインプットすると、アーキテクチャを元に都市マネージメントライブラリをビルド
- アーキテクチャ開発環境は、自己分析解析機能を持っていて、前年度の実績（データ、有効ライブラリ）などをマトリックス化して、ビルド時のパラメータとする
- 計画された戦略は、シミュレータが解析して、前年度に対して有効性が確認されると、都市オペレーティングシステムをビルド
- 同時に、ルール、ガバナンスも半自動生成し、各サービスレベルを精査し、APIを生成
- 都市オペレーティングシステムを用いて、各サービスプロバイダーは、自社のサービス、他社との連携サービスを実装
- 実装後、認証を受けて、アーキテクチャ開発環境にフィードバックされ、アーキテクチャの更新が行われる
- 循環型SoS環境をDEOSライフサイクルにて環境一式を監視、サポート



SoSにおけるDEOSの役割

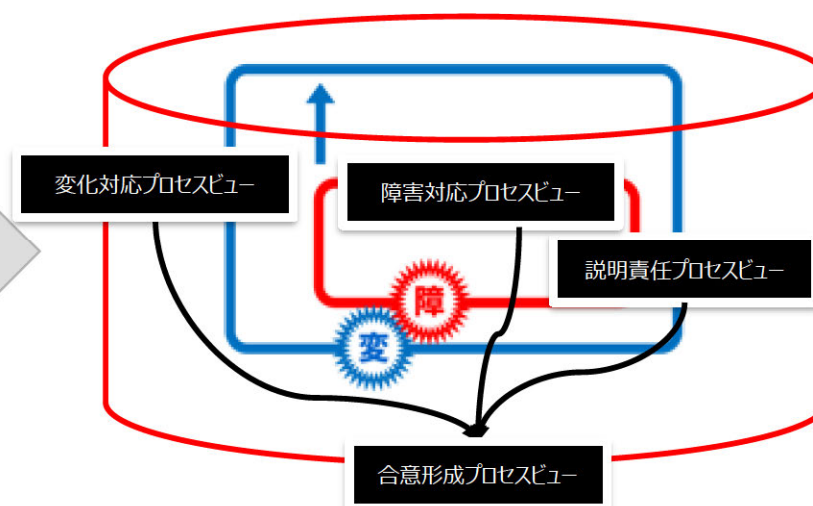
1. SoSへのDEOSライフサイクルの適応
 - 適応環境（スマートシティ）、サービスプロバイダー（ヘルスケア）、移動手段（モビリティ）で行われる事業開発、運用時の安全性、信頼性に関するエビデンスベースの妥当性検証
 - 推論、予兆検知にて、重大事故の未然回避
 - 重大事故の再発防止手段を提供
2. ルール、ガバナンス、コンプライアンスに貢献する合意形成手段（プロセスとツール化）
 - 次頁

DEOSライフサイクルマネジメント (通称DEOS2重ループ)



システムの設計・開発時、ならびに運用時におけるディペンダビリティ（総合信頼性）を確保するための基本プロセスを定義

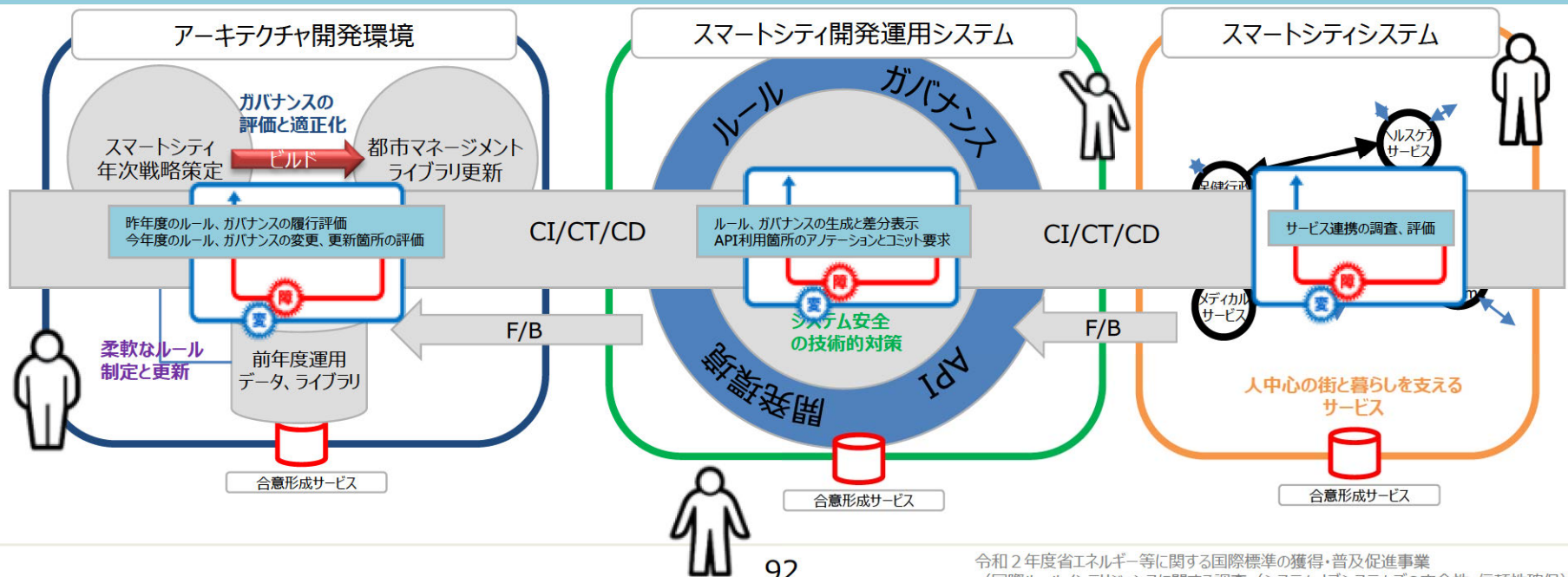
DEOSライフサイクルマネジメントの国際規格である、IEC62853（オープンシステムディペンダビリティ）では、4つのプロセスビューの作成を求めている



プロセスビュー内には常に合意を求めるイベントが発生し、ステークホルダーは、合意を繰り返しながら、ルール、ガバナンス、コンプライアンスを実行していく

スマートシティインフラから考える、ルール、ガバナンス、コンプライアンス

- SoSにおけるルール、ガバナンス、コンプライアンスは、新たな定義が必要である
- SoSにおける、
 - (スマートシティ運営組織の) ガバナンスとは統治のための機構、方法であることから、都市オペレーティングシステムを正しく実行されているかの監視と検証である
 - (サービスプロバイダーの) コンプライアンスとは、ルール、ガバナンスに基づき、遵守しているかどうかの証明であり、認証上のエビデンスである
 - ルールとは、(スマートシティ運営組織の) スマートシティ規範、(サービスプロバイダーの) 開発手順、リリース、更新に関する業務規約、(サービス受給者の) 利用原則であり、上位には法令、条例などが存在する
- ルール、ガバナンス、コンプライアンスと、上位に存在する法令、条例等は、それぞれ密接に絡み合い、正当性の検証を人間が行うには難しい。また、変更、更新時に相反を見つけ出したり、またある事象に関しての事案にて、どのルール、ガバナンス、コンプライアンスに抵触しているかを特定することをリアルタイムに発見するには不可能である
- 以下の考えは、ルール、ガバナンス、コンプライアンスをほぼ自動的にコンピュータ処理できるようにインフラ化するアイデアである



IEC 62853をSoSに適用する際の課題と解決アプローチ

- SoSにおける安全確保の要求事項（安全要求）が未規定
 - － 既存安全規格や考え方（例、Safety 2.0、Safety II、SOTIFやSaFAD等）の整理と評価→実証実験で試行
 - － SoSにおける安全確保の基本的な考え方と実現の仕組みを検討（次項）
- 膨大でかつ変化するステークホルダ間での合意・説明すべき内容とその方法が不明確
 - － 実サービスを対象に、要求事項、合意形成、説明責任の内容を具体化 → 実証実験でトライアル
 - － 変化対応と障害対応のために収集する運用情報（利用情報）の明確化 → HCDの観点から検討
 - － 上記に基づいて改善する仕組み → モビリティとヘルスケアの題材で検討し、さらに実証実験で確認
- 実サービスの運用を想定した基盤技術が確立していない
 - － 合意形成を支援（半自動化）し、その過程と結果が見える化 → モビリティとヘルスケアの題材で検討
 - － ステークホルダごとに適切な説明をするための支援（説明責任の支援） → HCDの観点で検討

DEOS技術による解決策の検討

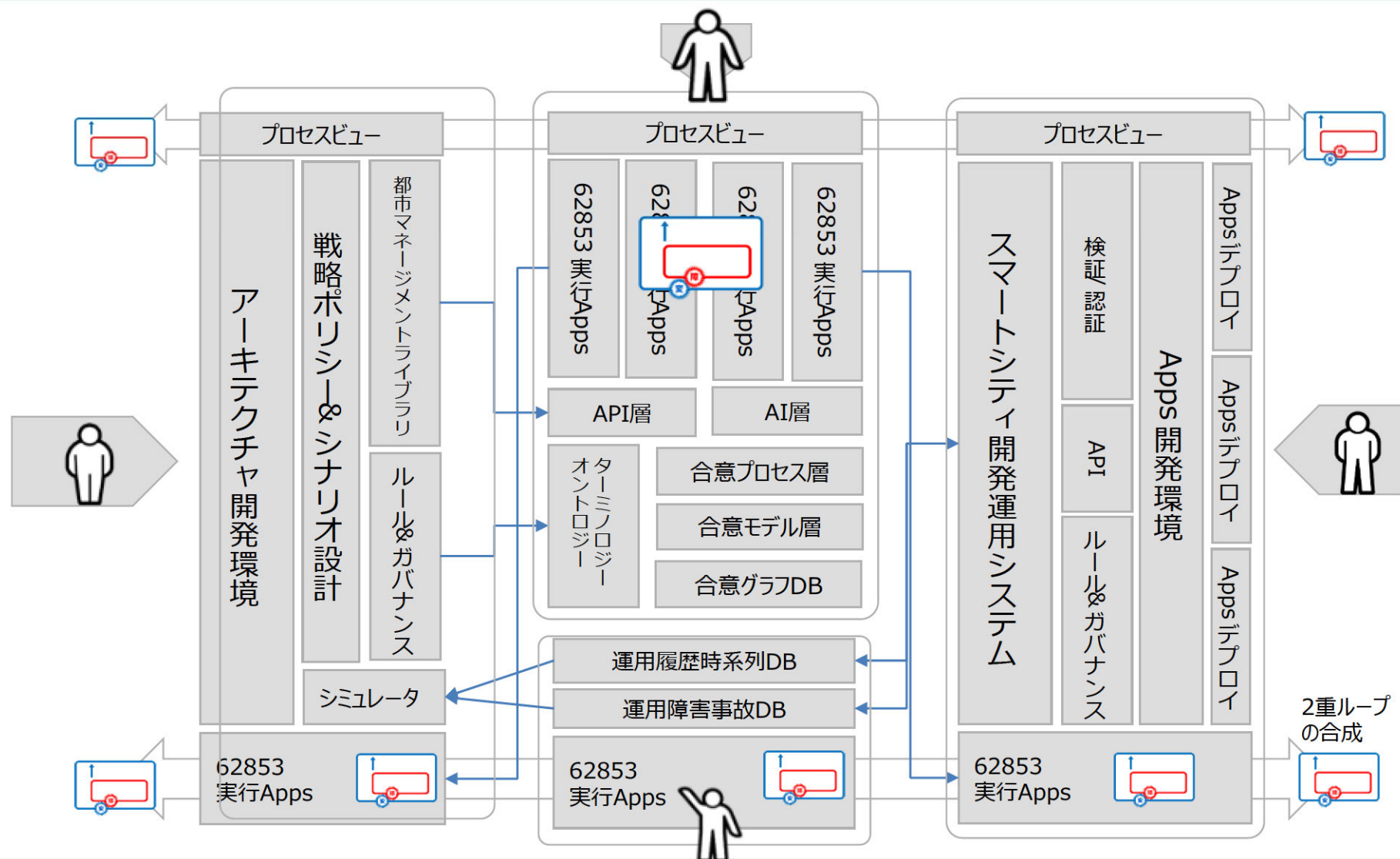
- SoSにおける安全確保のための考えを、定量化できる計算モデルを考案し検証する（1案としてSLAの妥当性計算理論）
- DEOSライフサイクル（IEC62853）を実行できる環境にて、合意形成と説明責任によるディペンダビリティの有効性を検証する（IEC62853の実験環境の整備）
- 運用時の大量データのリアルタイム処理の技術開発、因果を処理できるセマンティック解析技術の実現

DEOS技術の実現課題（理論と実装）

- SoSにおける安全確保のための考えを定量化できる計算モデルを考案し検証する（検証課題としてSLAの妥当性計算理論の考案）
 - DEOSライフサイクル（IEC62853）を実行できる環境にて、合意形成と説明責任によるディペンダビリティの有効性を検証する（IEC62853の実験環境の整備）
 - － CREST時代の検証実験は報告書有り
 - 運用時の大量データのリアルタイム処理の技術開発、因果を処理できるセマンティック解析技術の実現
- 次頁：「DEOSライフサイクルマネジメントシステムとSoS開発環境と、スマートシティインフラの考察」の実現系としてのソフトウェア構成検討
- 「DEOSライフサイクルマネジメントシステムとSoS開発環境と、スマートシティインフラの考察」の考えそれ自体がSoSにて実現されると仮定して、設計開発時にディペンダビリティ確保の実験を兼ねる
- スマートシティオペレーティングシステムとは、次頁（中央部分）IEC62853の実行をカーネルとした、分散アプリケーションサーバーとしての設計をめざす（難題としては分散環境におけるプロセス制御を実現する技術）
- 実施計画（開発スケジュール）と開発アイテム間の関係を示した。

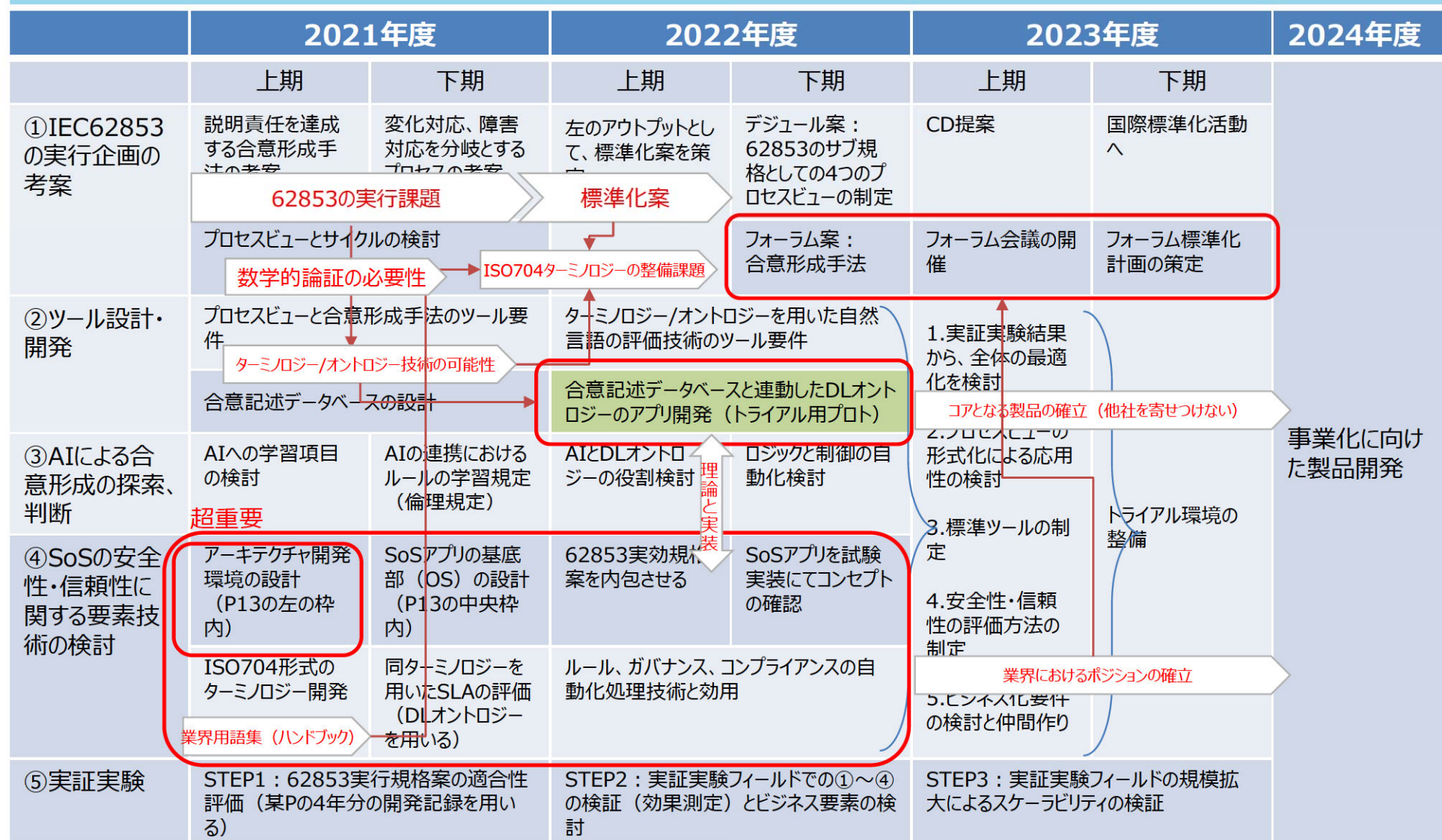
IEC62853（オープンシステムディペンダビリティ）を活用したツール連携

- 「DEOSライフサイクルマネジメントシステムとSoS開発環境と、スマートシティインフラの考察」をソフトウェア構成で記述



実施計画（関係図）

● テーマ間の関係性（研究開発の手順の説明）



標準化案（ツール、環境支援が前提となる）

1. IEC 62853の実行規格である、合意形成手法

- 注意：本件はSC 7での提案、議論が良いか？ また、IEC 62960 Ed.1:2020 **Dependability reviews** during the life cycleとの関係性を調査（IEC 62960は、2021年度JIS化が決定している（JIS化検討委員としてDEOSメンバーが参加））。
 - 説明責任を達成する合意形成手法の定義
 - システムのライフサイクルにおけるIEC 62853の4つのプロセスビューのそれぞれの関係性の定義、その関係性によって説明責任が達成できるかを明らかにする合意形成を目指す
 - 合意形成手法としてのプロセスとアウトプットを形式化する

1. SLA文書を用いた、サービス定義の妥当性証明技術

- スマートシティのルール、ガバナンスによりTerminologyを定義
 - 候補はISO704形式で構造化されたTerminology
- SLA(自然言語)をDL Ontologyで記述し、内容の妥当性評価をおこない、複数のSLAの結合を計算処理するフレームワークの定義
 - 計算とは、二つの異なる文書の結合、会話情報（意見、合意プロセス）における一致、不一致の同定です。

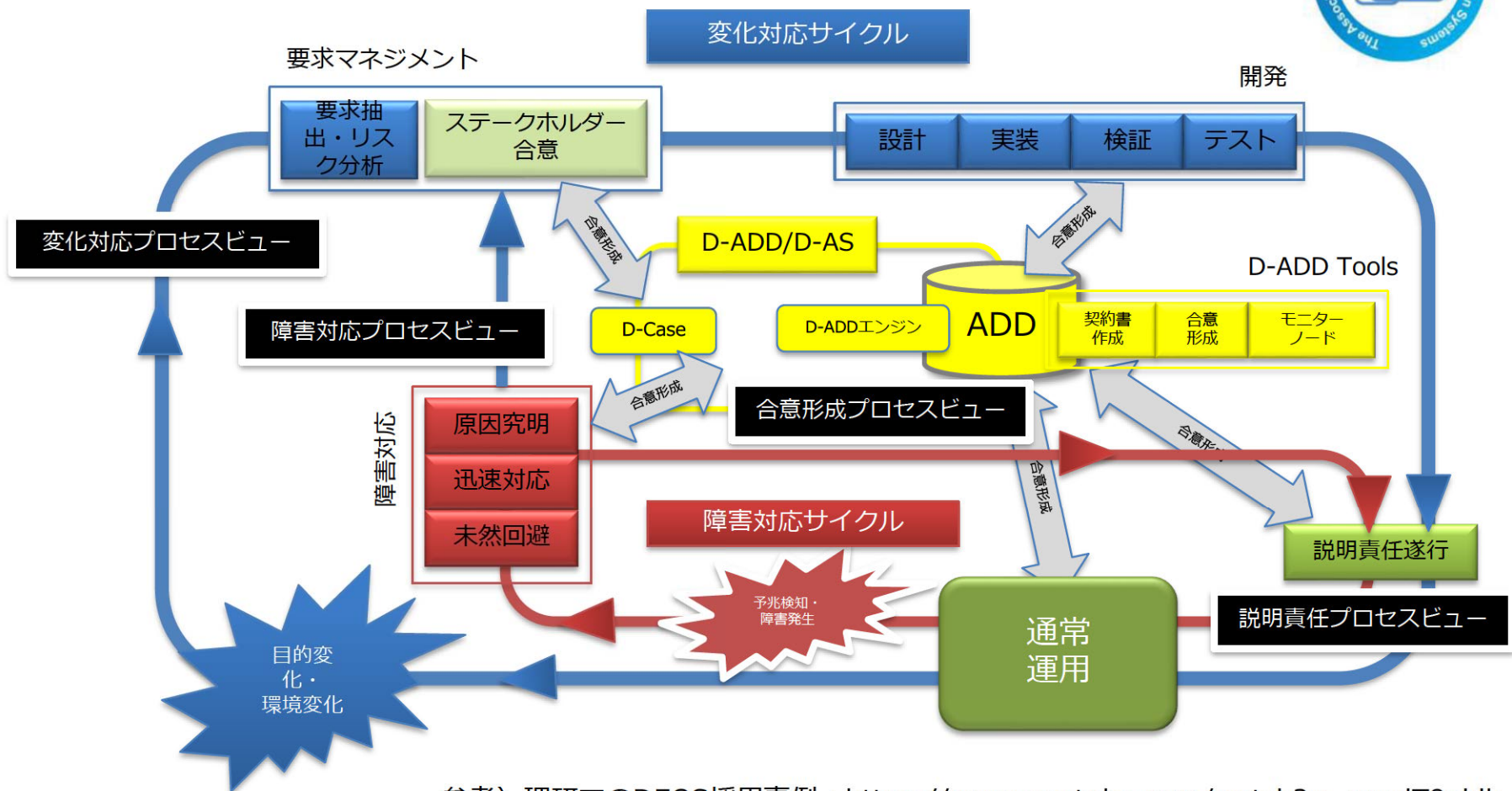


SC 7: <https://www.iso.org/committee/45086.html>

ISO/IEC JTC 1/SC 7

Software and systems engineering

参考 DEOSライフサイクルマネージメントとIEC62853（4つのプロセスビュー）の関係



参考) 理研でのDEOS採用事例 : <https://www.youtube.com/watch?v=rvyulT9aldk>

出所) JST-CREST「DEOSプロジェクト White Paper ver.3.0」 「図4 DEOSプロセス」を元に作成

②IoT住宅におけるSoSの事例

Iot住宅分野のSoSイメージから見える安全上の課題

● 安全上の課題を4つの視点で整理

1) 技術的な課題

- 装置が連携するシステムにおいて、各装置の要求がコンフリクトするとき危険な状態になる可能性がある。
- 人と装置が連携するシステムにおいて、人による誤操作が危険な状態を引き起こす可能性がある。連携規模が大きくなるほど利害関係者が増えるため、可能性も大きくなる。
- 人とAIの連携するシステムにおいて、AIによる誤判断が危険な状態を引き起こす可能性がある。

2) マネジメント的な課題

- 操作意思のない利用者が、操作意思を持つ利用者の操作やAIの判定による動作の影響で危害を被る可能性をどのように管理して低減するか体系的に決められていない。
- 装置の安全性は製造者が責任を負ってきたが、装置と人を組み合わせたシステムの安全はだれが責任を負うのか（住宅メーカーと住設メーカーの責任分解点：建てた直後と途中で追加更新したときの違い、変化前提のシステム）明確になっていない。

3) 文化的な課題

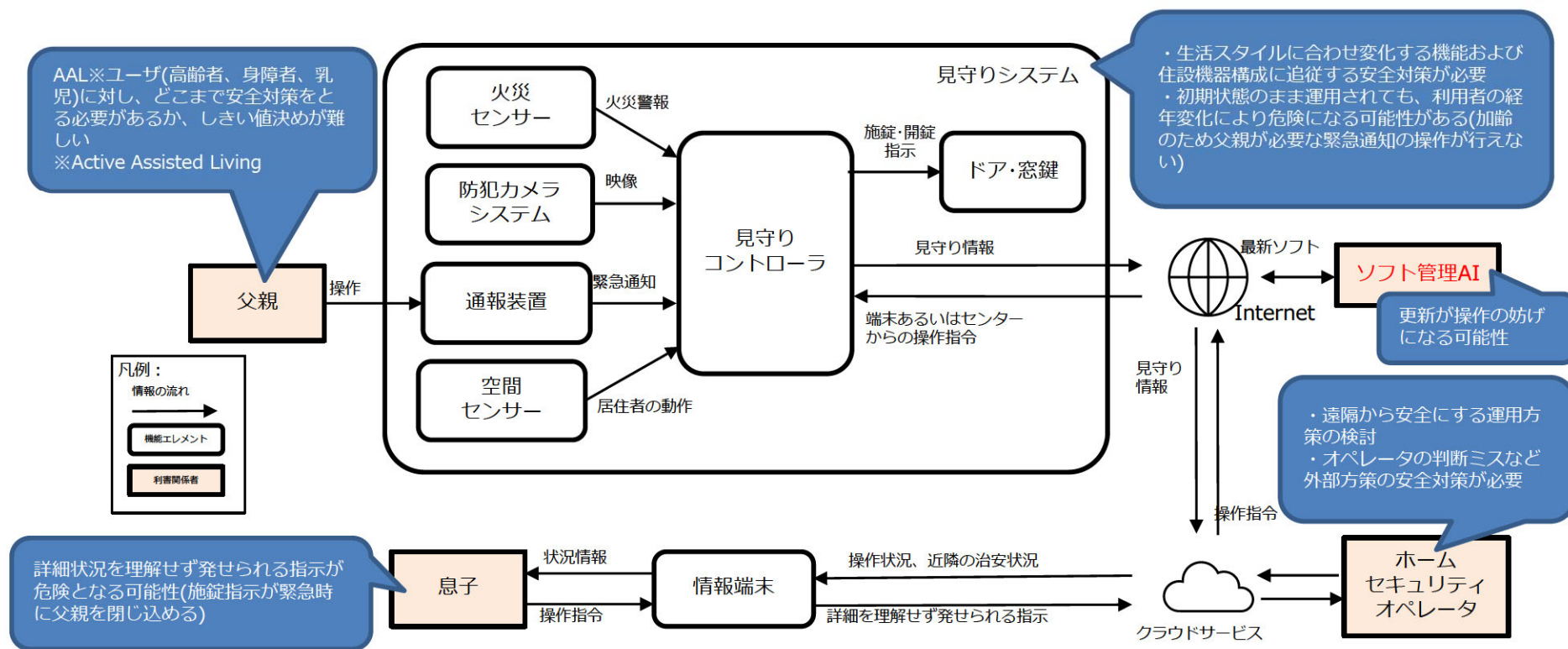
- 国や地域を跨ぐシステムにおいて、風習など文化差（例：靴を脱いで家に上がる、入浴時間の違い、認可される薬剤濃度の差）による危害の可能性はある。
- AAL※ユーザ(高齢者、身障者、乳児)に対するデメリットは、健常者にはデメリットにならないので、どこまで安全対策をとる必要があるか、しきい値を設定することが難しい。 ※AAL: Active Assisted Living

4) 規格化や、その普及に向けた課題

- 未知のリスクをとらえきれておらず、既知のリスクへの対策の正当性を示すことが難しい。運用してみて初めて発見されたリスクへの対処プロセスが決められていない。
- 個社の製品である装置が連携してシステムを構築することになるが、連携に際して各社が安全規格をどのように運用するかを立て付けができていない。
- 生活スタイルや経年変化により機能や機器構成が変化するため、リリース時点での安全性をより発展させた安全の検討が必要(利用者の行動予測、運用方策など)。

IoT住宅システムの危険事例(見守りシステム)

- 連携規模の高度化、複雑化により増える利害関係者に応じた安全性を検討する必要がある事例を示す

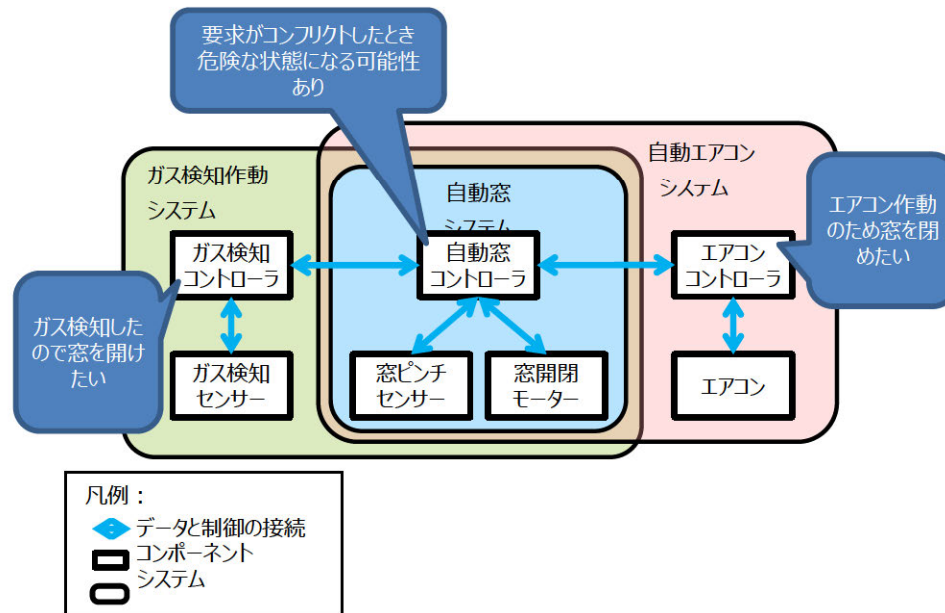


- ・ 見守りシステムは、複数のシステムが連携し高齢者である父親(AALユーザ)を遠隔から見守るシステム
 - ・ 利用者の生活スタイルや能力に変化に応じ、ソフト管理AIによりソフトウェアを最新に保つ機能を持つ
- 課題 1 : AALユーザにより安全対策の程度が異なるので、どこまで対策を行えば安全か、しきい値を決めるのが難しい
- 課題 2 : ソフトウェアの更新がその他のサブシステムの妨げになることが、運用するまでわからない場合がある
- 課題 3 : 理解せずにシステムを利用する人の行動が危険になる可能性(例：防犯目的の施錠操作で緊急時にAALユーザを閉じ込める)

Iot住宅分野のSoSイメージ例

● Iot住宅の連携システムと危険な状態の例を示す

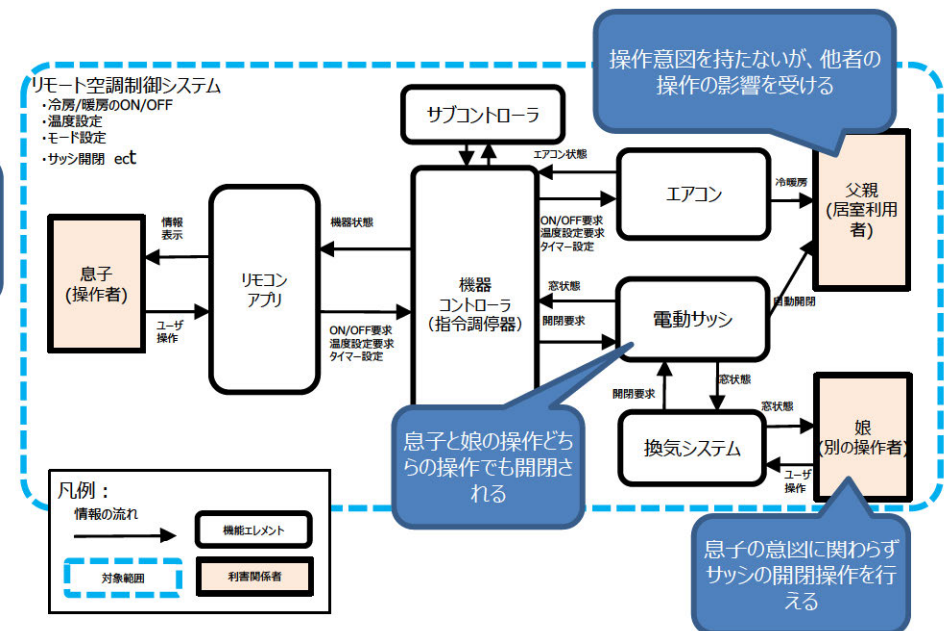
例1) 装置間の連携するSoSの例



自動窓システムは、サブシステムとしてガス検知作動システムと自動エアコンシステムにより共有される。これらは直接接続されないが、相互に連携する必要がある。

ガス検知作動システムの窓を開ける要求と、自動エアコンシステムの窓を閉める要求がコンフリクトしたとき、ガス検知時に窓をあける機能が働かず、危険な状態となる可能性がある

例2) 人間と装置が連携するSoSの例



利害関係者は互いの意図を理解しないことがある。例2の息子と娘は互いの意図を認識することなく共通の装置に対して異なる操作を行うことができる。

住宅の居住者以外にも、間接的な利用者が関連する。例2の父親が操作意図を持っていなくても、息子によるシステム操作の影響を受けることになる。

IoT住宅システムの安全規格

- IoT住宅の住設機器連携システムの安全規格(IEC 63168、IoT住宅版SOTIF※)策定中

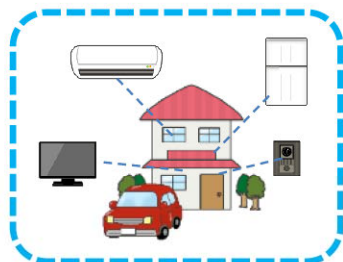
※Safety Of The Intended Functionality

【IEC 63168 住宅機能安全規格】

- 複数機器が連携するとき機器の故障による機能不全のリスクに対する安全の標準化
- 故障時のリスクを社会的に受容可能な範囲に抑えるための安全方策

【IoT住宅版SOTIF規格】

- 人のミス(誤使用・誤操作)と装置の設計上の限界(認識精度など想定外の要因)による機能不全のリスクに対する安全の標準化
- 人のミスと設計限界時のリスクを社会的に受容可能な範囲に抑えるための安全方策

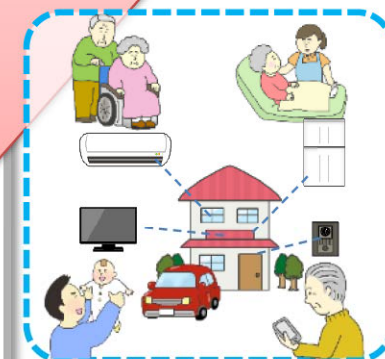


複数住設機器が連携するシステムの安全

機能不全

システム故障に起因する機能不全

人のミス、想定外の要因に起因する機能不全

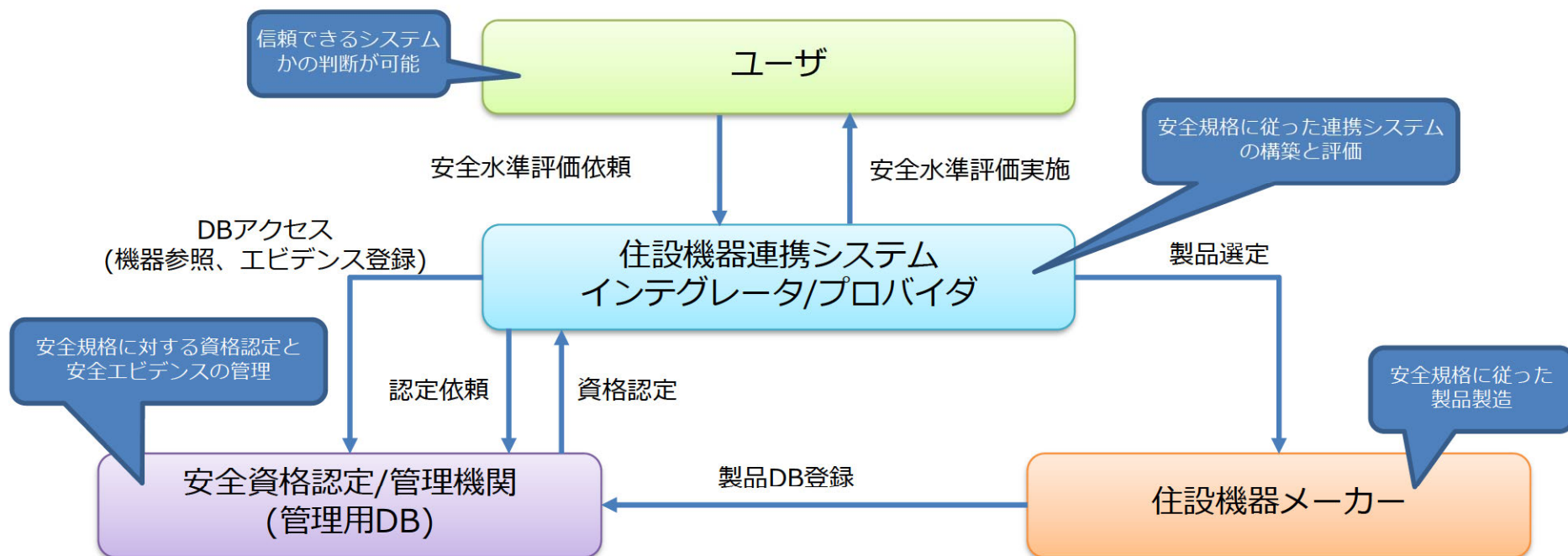


AALユーザの利用を踏まえたシステムの安全

- AALユーザの生活向上のため、住宅に導入される高機能化された電気/電子(E/E)システムが有効
- E/Eシステムによる制御に依存するIoT住宅における住宅設備機器連携の高度化と複雑化によって発生する安全上のリスクへの対策が重要課題
- 相補関係にあるIEC 63168およびIoT住宅版SOTIF規格を、IoT住宅の住設機器連携システムに適用する

IoT住宅システムの安全規格運用の立て付け例

- 安全規格(IEC 63168、IoT住宅版SOTIF)をどのように運用するかの例示

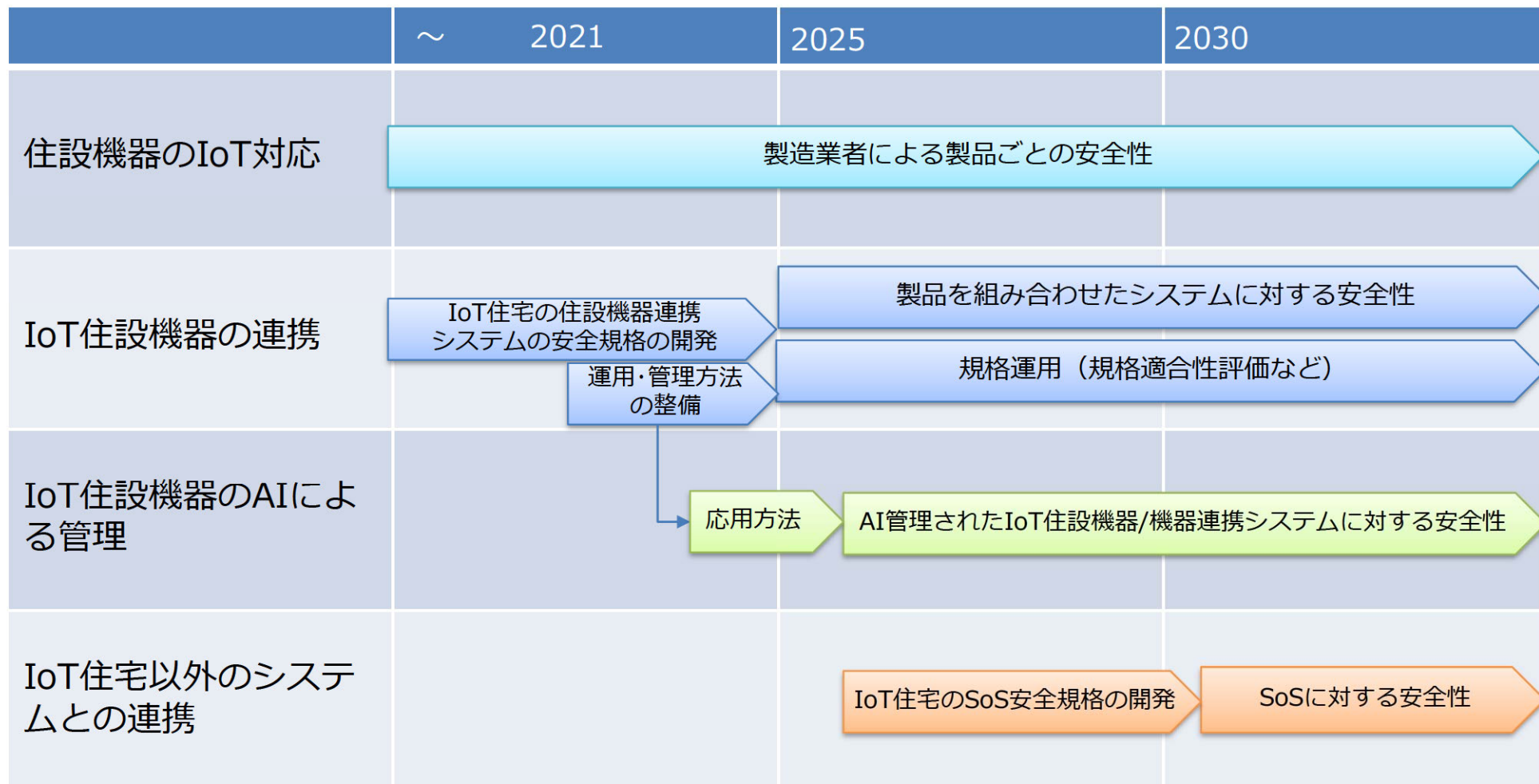


- 個別の住設機器メーカー（製造者）は、安全規格に従い製造された製品をDBに登録
- 住設機器連携システムインテグレータ/プロバイダーはDB登録製品から製品を選び、安全規格に従い連携システムを構築
- 安全資格認定/管理機関は安全資格の認定および登録製品の管理を実施
- ユーザは連携システムの安全性に関する判断基準を得られる

【課題】安全規格運用の立て付けは検討段階のものであり、管理方法も含め今後構築していく必要がある

ロードマップ°

- 複雑化するIoT住宅に係るシステムの安全性を確保するためのロードマップ



③人への影響分析（課題）と事例 ～人間中心設計（HCD）によるアプローチ～

本セクションの構成

●目次

※HCD: Human Centered Design (利用時品質、ユーザビリティを向上させる手段) ISO9241シリーズ

課題説明	System of systems (SoS) における利用時品質 (HCD※) の課題 SoSで利用時品質 (HCD) が低下、リスクの発生確率が高まる SoSに対する、HCD分野から見える安全上の課題
解決策	SoSにおける利用時品質の向上 (課題の解決) の手段にはHCDが有効 SoSにHCDを活かすための「利用者の変化に対応するシミュレーション技術」 SoS 4分類 に対応する「利用/運用パターン」をデータベース化し活用する 「利用者の変化に対応するシミュレーション技術」を適正に運用する
事例提示	スマートシティ「都市マネジメント」への対応例 モビリティ事例 (自動運転公共バスに一人暮らしの高齢者乗車時の課題) 同上 (同上 の対応)
規格/基準等 ロードマップ	HCD分野 (人間工学/ユーザビリティ/HCD関連) の主な規格の変遷 HCD分野の規格および業界ガイドラインの現状と今後への期待
付録	Safty2.0で提唱されている取組との整合性についての参考情報 HCD分野 有識者インタビュー情報 (6名分)
参考資料 (別資料)	・FAA情報 ・FDA情報 ・日本事務機械工業会 ・JISF0076_2004 船舶システムの安全設計評価に関する指針 ・航海機器100226a 設計ガイドライン案報告書 ・Discussion point for 25019_v3 Resolution

System of systems (SoS) における利用時品質 (HCD※1) の課題

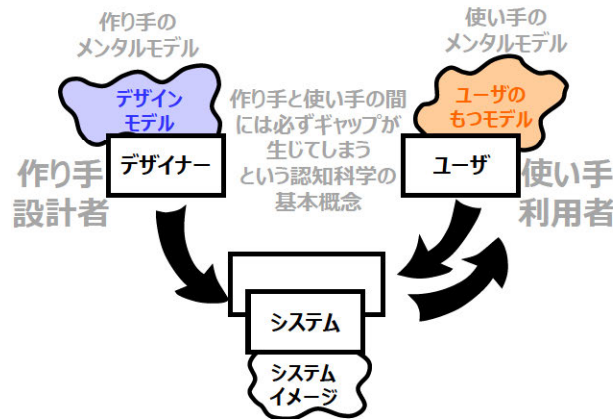
※1 HCD: Human Centered Design (利用時品質、ユーザビリティを向上させる手段) ISO9241シリーズ

●HCDの課題 (メンタルモデル※2ギャップの増大) により、SoSではリスクの発生確率が高まる

※2 メンタルモデル：本文内にて解説

従来継続する課題

- **作り手と使い手の間に生じる、メンタルモデル (意志/意識に影響する行動イメージ) のギャップを抑制できない**
単体の製品/サービス設計時に、作り手のメンタルモデル (設計者が想定する課題や解決に向けた着想) と、使い手のメンタルモデル (利用者が感じる課題や描く期待) とがすれ違う現象 (メンタルモデルギャップ) が利用時品質を低下させる原因である (D.A.Norman)
それを小さくするために適用するHCDの、スキル習得、マインド醸成、組織への定着などが継続的な課題である。HCDの具体的な取組としては、利用者の特定、人間特性の考慮、利用シナリオの想定などが必要。



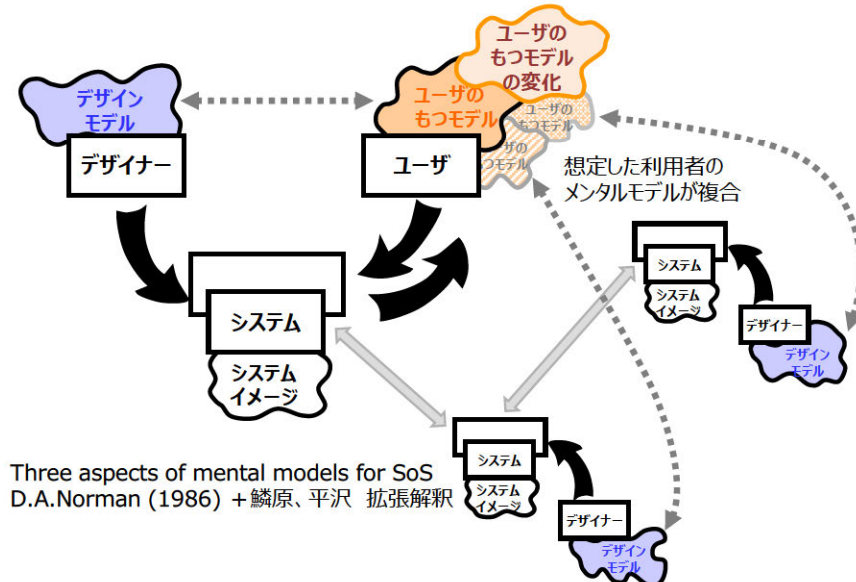
Three aspects of mental models D.A.Norman (1986) (原図)
The Design of Everyday Things Paperback – February 1, 1990
by Donald Norman (Author)

(グレー字は鱗原注釈 着色は説明用に施したもの)

付録にてインタビュー記録参照：HCD-Netビジネス支援事業部 自動運転社会におけるHAII検討委員会

SoSにおける新たな課題

- SoSでは、製品単体が想定した利用者のメンタルモデルが複合し、運用時にギャップが増加する
加えて、SoS運用時には、利用者のメンタルモデルも変化しギャップが増加する (下図参照) ことで利用時品質が低下するだけでなく、リスクの発生確率の増加にもつながる
- SoSにおける様々な利用シナリオ、利用者のメンタルモデルの研究が不足
- 製品単体の開発と比べ、SoSでは「人間特性の影響」を考察する方法が確立していない
SoSにおける「人」の扱い方が不明確
- 運用時のコンテキストの変容を、SoSのステークホルダーの誰が吸収するか責任の所在が不明確
このことは、戦略性の高いアーキテクチャから、具体的な製品のUI/UXを設計する、もしくは、抽象度の高い議論から具体化の議論へロジカルに繋げること、と同義であるが、この研究は未だ、できていない



Three aspects of mental models for SoS
D.A.Norman (1986) + 鱗原、平沢 拡張解釈

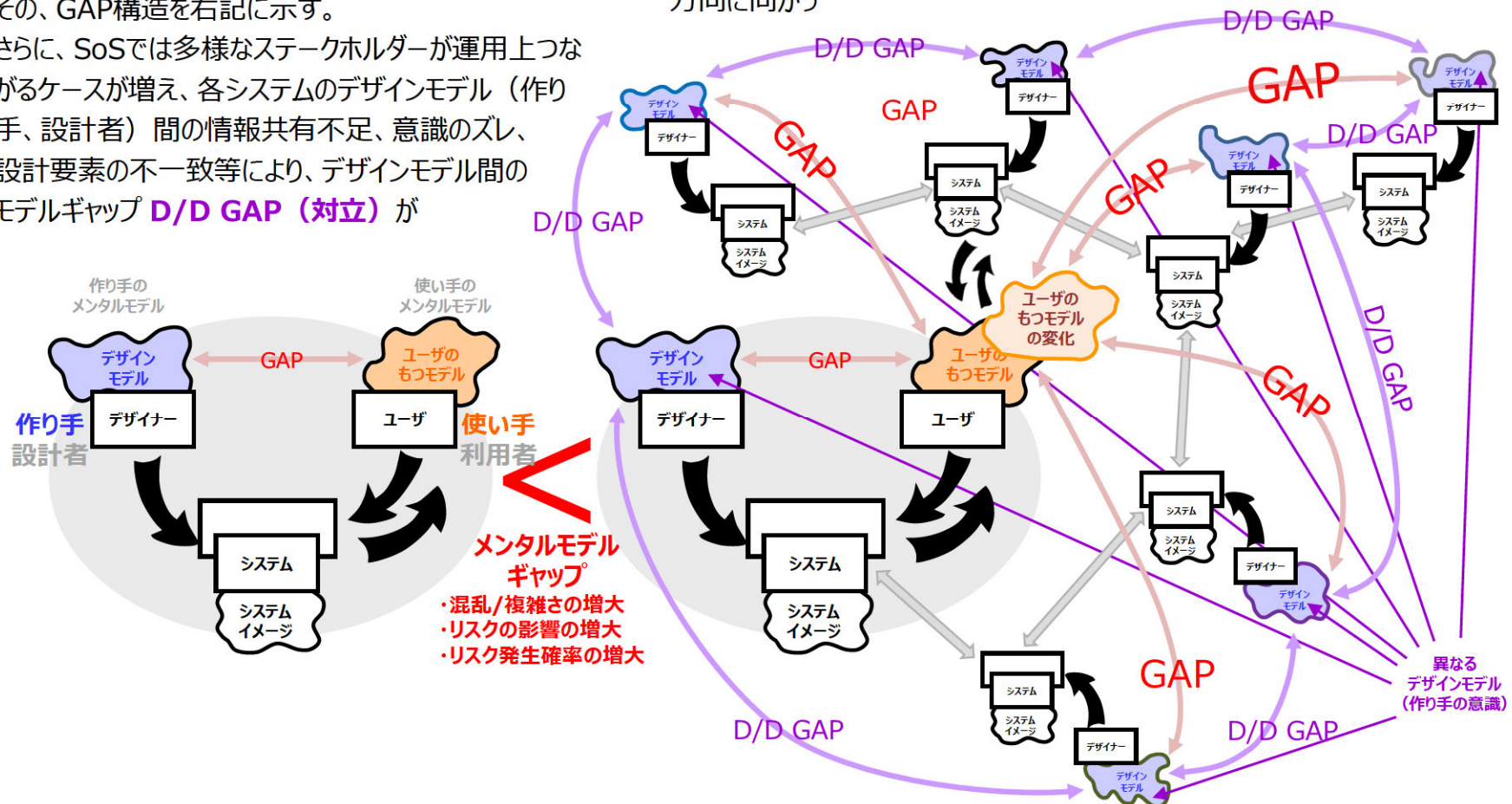
SoSで利用時品質（HCD）が低下、リスクの発生確率が高まる

- 「**作り手**と**使い手**のメンタルモデルギャップ」が利用時品質の低下を招く
- さらに、**作り手**と**作り手**のメンタルモデルギャップ（対立）により、混乱/複雑さも増加する

SoSでは「メンタルモデルギャップ」が必然的に増大する、その、GAP構造を右記に示す。

さらに、SoSでは多様なステークホルダーが運用上つながるケースが増え、各システムのデザインモデル（作り手、設計者）間の情報共有不足、意識のズレ、設計要素の不一致等により、デザインモデル間のモデルギャップ **D/D GAP（対立）** が

生じるため、ユーザにとっての混乱や複雑さが増し、結果としてリスクが高まる方向に向かう



SoSに対する、HCD分野から見える安全上の課題

●安全上の課題を4つの視点で整理（SoSへの対応策は未整備。今後の必要性について）

付録にてインタビュー記録参照：HCD-Netビジネス支援事業部 自動運転社会におけるHAI検討委員会

・技術的な課題

- 1) 公共インフラと自動制御システム間のリスクコミュニケーションが必要
 - 2) 自動制御システムと利用者間のリスクコミュニケーションが必要
 - 3) 利用者と利用者を支援するサービス間のリスクコミュニケーションが必要
- ※リスク増加の状況認識から各システムを安全側に制御することが必要
 ※様々な運用時の変化への対応（運用システムとしての変化対応）が必要

・マネジメント（運用）的な課題

- 1) 利用者は、常に自動制御システムを理解し対応することが基本運用
 - 2) 利用者の理解能力、意識、思考別のユーザータイプ分類に基づくことが必要
 - 3) 多様な認知/判断/行動の能力毎への対処、ヒューマンエラー（スリップ、ラプス等）発生時の想定が必要
- ※人間特性も含めた利用状況を網羅的に考えること(ISO25010)が前提条件
 ※一定空間内の日常的な行為/行動の状況認識を可能にすることが必要

・文化的な課題（ステークホルダー間コミュニケーション）

- 1) 地域毎に異なる文化、民族、メンタルモデル等の全体的な考察が必要
 - 2) 防犯、火事、地震、災害などに関連する行為/行動に関する情報共有については、SoSによるモノ同士の協調連携も含めて対応する
 - 3) 個人情報情報の漏洩には敏感だが、リスクマネジメントに有効であれば一定の情報開示も可能にする
- ※個人情報を省き、必要な情報に仕立てる、協調連携の状況を管理できるように
 ※総合的にスキルセットとマインドセットの両面での人材育成が必要

■ 便利な商品（システム）が、暮らす「場」に持ち込まれた時に起こり得る事象をモビリティ事例にて、HCD分野の対応策で考察してみる
 →自動運転車両内で一人暮らしの高齢者が倒れたことを想定（別記）

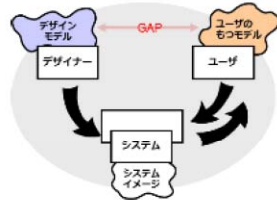
・規格化や、その普及に向けた課題

- 1) 自律性を持つAI製品/サービスに対する、人間工学系規格での扱いは、これからの議論
 ・SoSにおけるAIと人の関係については哲学的な議論も必要
 また、Tay問題を防ぐためには運用側での情報管理が必要
 ・世界（特にイギリス）の理解を得るためには、人をシステム（モノ）として扱う際の統合概念「情報化の影響分析（ソシオテクニカルアプローチ）」が必要になる
- 2) SoSに関与する全ての利用者にとって、どのような状況変化が生じて、その変化に対応し総合的に信頼できる必要がある
 ・全ての利用者とは、それぞれのsystemに関与する「operators、customers、responsible organization、public」であり、各利用者にとっての安全性、信頼性、Quality in useの向上が求められる
 ・規格情報の共有不足、周知徹底不足により、一定期間後にユースエラーを繰り返して誘発することを防ぐため、利用時品質はダイレクトユーザー（利用者）に加え、対象とする製品やシステム・サービスの利用に対して責任ある組織への影響、Societyへの影響等、社会へのインパクトを目指す。アクターや影響の規模を明確化する
- 3) SoSにおける危険の許容「許された危険注」の法規的扱い方が現段階では不明確
 ・注：財産の損失より便益が勝ることを許容して社会実装される様
- 4) リスクを見積もる「（例）危険見積（自衛隊用語）」の採用検討へ
 ・「責任の境界」を意識したリスクコミュニケーションにより危険見積を抑える等

SoSにおける利用時品質の向上（課題の解決）の手段にはHCDが有効

- 製品/サービス単位で、利用時品質を高めるためのHCDの効果は既に実証済み
- SoSでは、ビッグデータ/デジタル/AI技術により、よりHCDの有効性が高まる

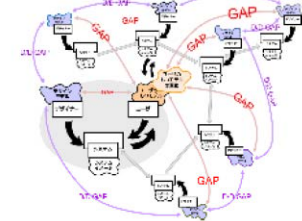
従来の検討対象/シミュレーション対象



・諸々の原則をベースに業界毎、市場毎に共通して適用できる工夫（下図中央）もされているが、専門性を必要とし、ツール等による分析/設計作業の効率化は実現していない。

・各手法は、SoSでも有効であるが、社会がデジタル化され、ビッグデータが利活用できるようになると、①作業効率の向上、②分析精度の向上、③多様化する利用者、④変化する利用者への対応（下図右）や、⑤複雑化する設計者間のモデルギャップの抑制効果（右図）が期待される。

SoSの検討対象/シミュレーション対象



従来のギャップ抑制への対応策（HCD分野の実績）

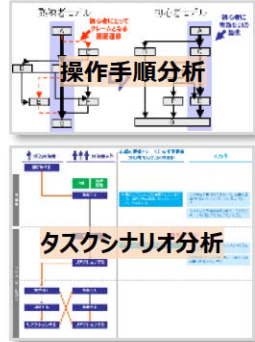
従来の製品/サービス単位の対応策

業界/市場共通の対応策

SoSにおけるギャップ抑制への対応策（想定）

ビッグデータ/デジタル/AI技術による対応策

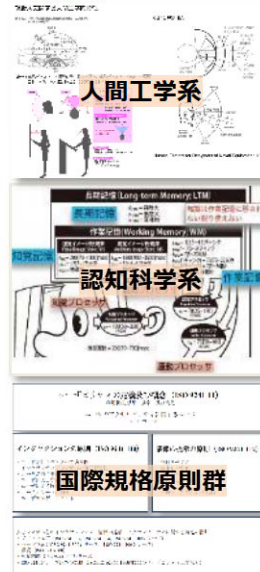
■タスク分析系



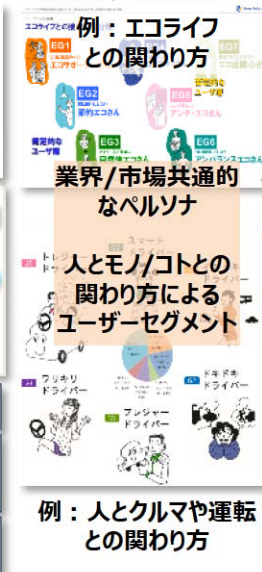
■人/状況の特長系



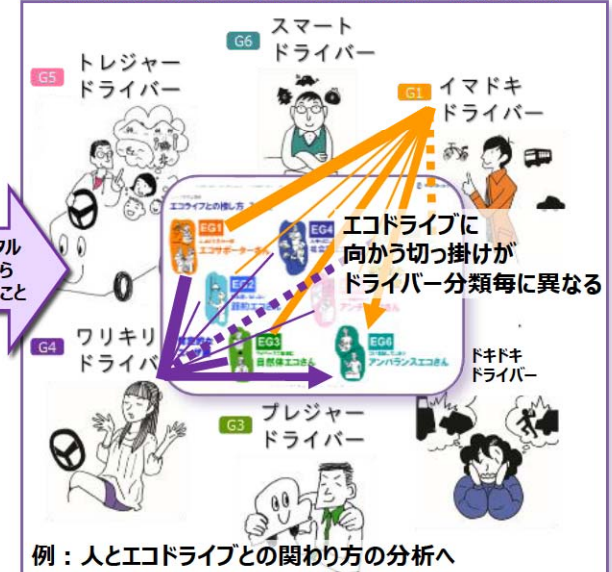
■原則系



■人とモノ/コト関係



■多様な価値観の組合せ、変化への対応（次頁参照）



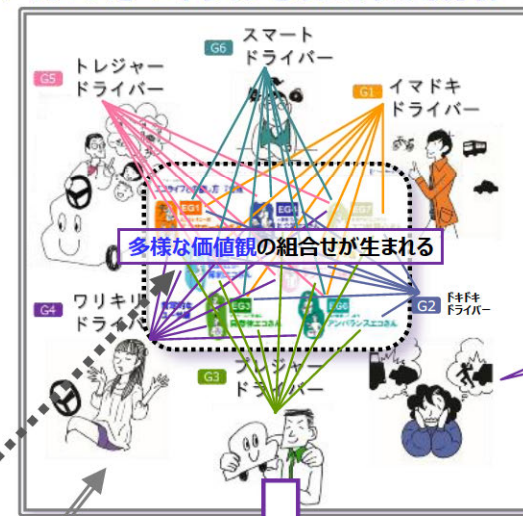
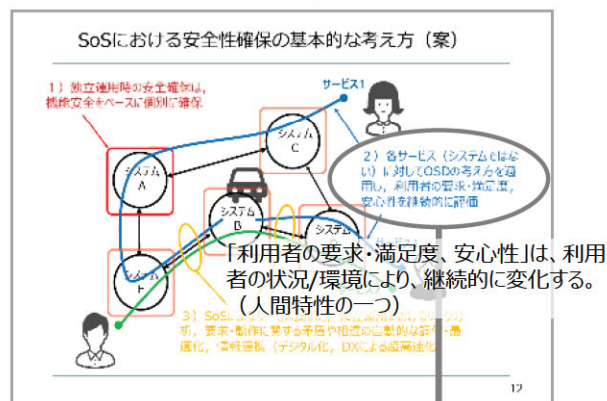
HCD分野の国際規格（ISO9241シリーズ等）および諸手法により、製品/サービス単位での利用時品質、安全、安心は管理されつつある。

SoSにHCDを活かすための「利用者の変化に対応するシミュレーション技術」

- SoSにおける、リスク減少 & ビジネス活性化に向けて、「利用者の変化に対応するシミュレーション技術」を構築し、以下の2つの状況（**多様な価値観**、**継続的な変化**）に対応する

- 1) 利用者の**多様な価値観**の組合せ、及び変化に対応
- 2) 運用時の状況/環境の**継続的な変化**に対応

→ 例：人とエコドライブとの関わり方の分析へ



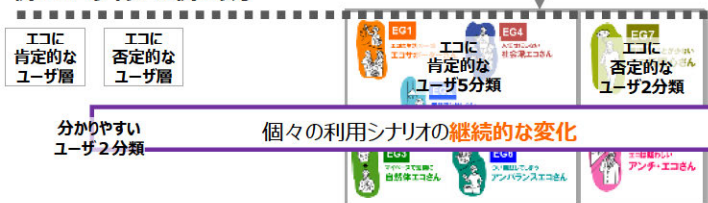
それぞれの価値観の組合せの影響を受けた利用者が

- ・情報を発信する
- ・サービスを受信する
- ・購買活動へ
- ・意図的な行動
- ・無意識な行為

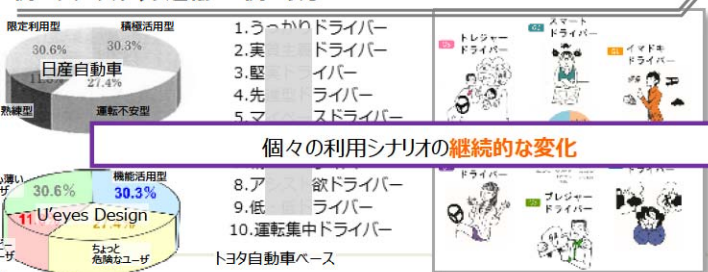
などなど...

の運用時の情報を、リアルタイムに自動で収集するデータから分析する

例：エコライフとの関わり方



例：人とクルマや運転との関わり方



価値観は**継続的に変化する**

変化する、SoS利用シナリオパターン
変化する、利用者の価値意識パターン
のデータベース化および専門家によるメンテナンス

SoS利用パターン	利用者のメンタルモデルパターン	社会規範/意識/行動
Directed (指示的)	「これは安全な運転方法だ」という意識	「安全運転」の意識を高める
Accompanied (伴走的)	「これは安全な運転方法だ」という意識	「安全運転」の意識を高める
Collaborative (協力的)	「これは安全な運転方法だ」という意識	「安全運転」の意識を高める
Virtual (仮想的)	「これは安全な運転方法だ」という意識	「安全運転」の意識を高める

(総称)
利用/運用パターンデータベース
↑
公的な利用シナリオ

利用者の変化に対応する
シミュレーション技術
の構築、Step UPへ

様々な変化情報から
各SoS分野
各コミュニティ
各シティ
に対して、安全/安心/効率化
の対策をシミュレーションできる
ようにする

SoSの定義&4分類に合わせて利用/運用パターンを整備する

(次頁参照)

SoS 4分類 に対応する「利用/運用パターン」をデータベース化し活用する

- SoS向け「利用（シナリオ）パターン」「利用者の価値意識パターン」を整備し、行為/行動の特徴点の変化情報を、AIにより常時収集、分析、更新されるデータベースを構築する
- 利用状況の変化と設計運用の整合性をシミュレーションし検証し続ける仕組みを構築する

変化する、利用/運用パターン		SoS利用（シナリオ）パターン	プラス 利用者の価値意識パターン	安全対策/事象/事故への対応
SoS4分類	SoS対象（適用範囲）例	SoSの利用範囲	利用者のタスク毎の価値意識パターン 利用者の行為/行動毎の価値意識パターン	
D-SoS 統率された	IoT住宅 IoT学校 IoT職場	・衣食住パターン ・伝える/学ぶパターン ・稼ぐ/組織への貢献パターン	・換気/寒暖の個体差への対応パターン ・理解力/感じ方/体験の仕方パターン ・働き方パターン	・ガス漏れ時の窓遮断を防ぐ ・情報の受容度を高める ・心身のストレス防止
A-SoS 認められた	デジカメとプリンター スマホと各種サービス	・画像を楽しむパターン ・健康管理パターン ・会場/施設利用パターン	・楽しみ方のパターン ・健康意識、健康への取組価値パターン ・会員/支払/セキュリティ意識パターン	・重要データの流出を防ぐ ・重症化、搬送先ミスマッチを防ぐ ・ビジネス機会損失を防ぐ
C-SoS 協調的	自動運転公共バス等が走る街 スマート/スーパーシティ	・自治体運営公共バス利用 ・多様な要請に対応できる宅配便	・安全/安心への価値感パターン ・交通円滑化への価値感パターン ・荷姿/配送/受取の価値感パターン	・交通事故防止 ・渋滞防止 ・誤配防止、効率配達の実現
V-SoS 仮想的	限定しない 地域 + 人々 + 行動環境下	・モビリティ社会活動 ・ヘルスケア社会活動	・社会活動への意識/行動パターン ・共通行動に対する意識/行動パターン ・社会貢献への意識/行動パターン	・緊急事態宣言下の良識行動の実現 ・扇動に冷静に対処できる ・スムーズなボランティア活動
SoS共通		・災害対応パターン ほか	・楽観的/心配性パターン ・消極的/積極的パターン ・我慢する/しないパターン ほか	・時間圧への冷静な対処 ・優先事項の的確な判断 ・多様な人への共通理解の実現

「利用者の変化に対応するシミュレーション技術」を適正に運用する

- 作り手と使い手のメンタルモデルを繋ぎ、「合意形成」を図る手段を、効果的に産業界に 提供し、かつ、ルール（規格、ガイドライン等）を整備、全ての設計開発者が参照できる
- SoS市場の受容性が継続的、飛躍的に高まるよう、商品/サービスの認証ビジネスを構築

SoSにおける、利用/運用パターンが、運用時の変化情報もリアルタイムに反映された上で、かつ、公的なデータベースで参照できる。大企業でなくても全産業界にて、また、従来のような属人性に頼らず、全ての設計開発者が活用できるようになる！



人間中心デザイン基礎知識体系図※を活用し、利用パターンの確からしさを確保する
 ※特定非営利活動法人人間中心設計推進機構
 ※「スマートシティファレンスアーキテクチャ 都市マネジメント スマートシティビジネス 体験デザイン」と同義

従来の利用シナリオの生成
 属人性の高いデザイン活動
 (HCD専門家による定性的/定量的考察) による、利用シナリオ (重要度、頻度) の生成

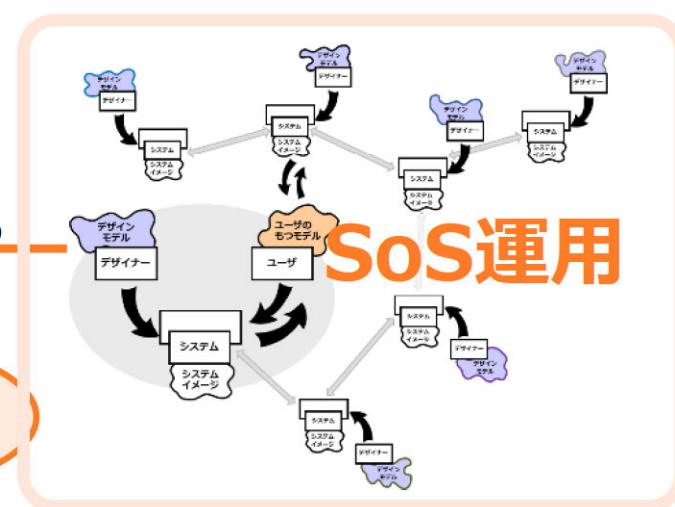
情報のデジタル化

SoSの利用シナリオの自動生成
 利用者の運用時のビッグデータ等、変化データに基づく利用シナリオ (重要度、頻度) の自動生成



変化状況を、SoSの運用時の情報からリアルタイムに把握する
 多様な利用者が、SoSの影響を受けて変化する、
 ・該当シナリオの重要度
 ・該当シナリオの発生頻度

DXレポート2のサマリ (企業のアクションと政策) 中長期～デジタル企業へ”迅速に変わりつづける能力”の獲得～への対応策とも繋がる仕組みづくりへ



検証し続ける仕組みの構築

運用時の利用者の変化情報、周辺状況の変化情報と、設計/変更案との整合性をシミュレーションした結果の検証
 SoS運用時の分析情報、AI情報 (変化情報) 等を、リアルタイムにデータベースへフィードバックする (DEOSプロセスの二重ループに相当する)

- ・行動モデルの検証サービス
- ・健全システムの認証サービスなど

変化情報データベース



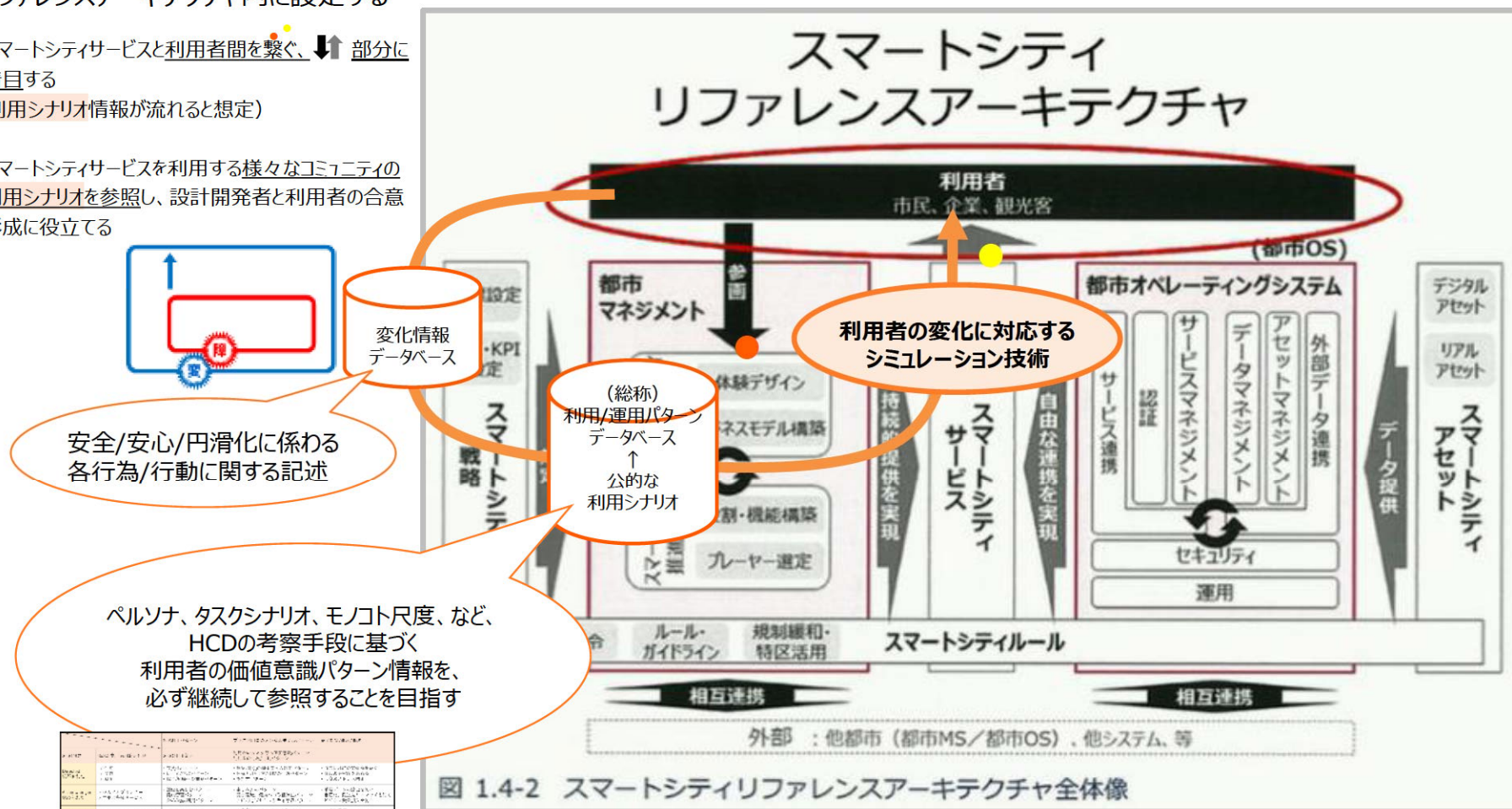
スマートシティ「都市マネジメント」への対応例

●「利用者の変化に対応するシミュレーション技術」をスマートシティサービス提供時に適用する

利用/運用パターン【SoS利用（シナリオ）パターン + 利用者の価値意識パターン】を、継続的にリアルタイムに参照する仕組みを、スマートシティリファレンスアーキテクチャ内に設定する

- スマートシティサービスと利用者間を繋ぐ、**↑↓** 部分に着目する
(利用シナリオ情報が流れると想定)

- スマートシティサービスを利用する様々なコミュニティの利用シナリオを参照し、設計開発者と利用者の合意形成に役立てる



出所）スマートシティリファレンスアーキテクチャホワイトペーパー 第一版（2020年3月31日）

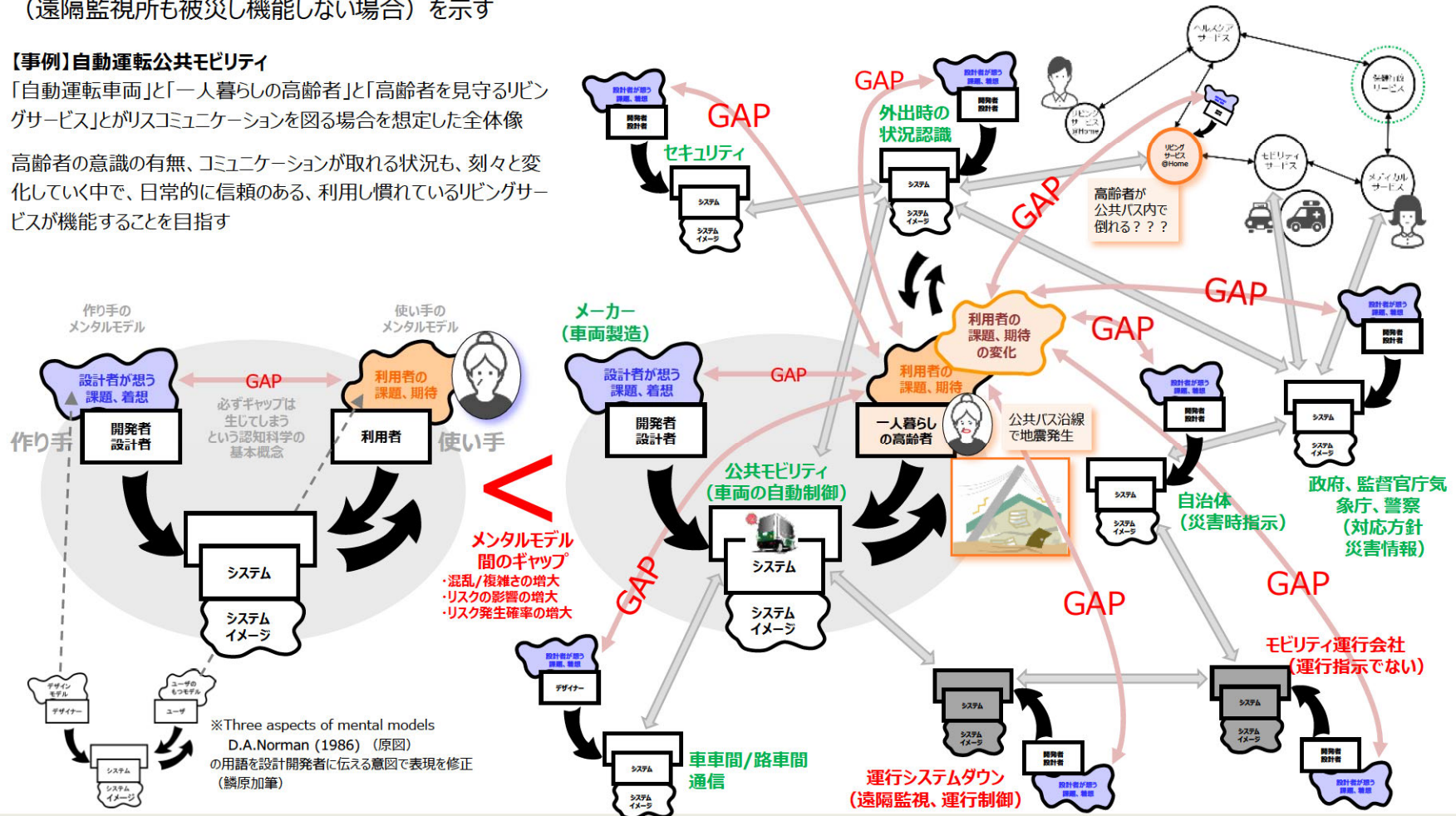
モビリティ事例（自動運転公共バスに一人暮らしの高齢者乗車時の課題）

● 「他に乗客がない状態で倒れる」 かつ 「災害が発生する」場合のリスク増大イメージ

一人暮らしの高齢者が自動運転公共バス乗車中に、原因不明で倒れ、かつ、地震発生により、バスが立ち往生する状況（遠隔監視所も被災し機能しない場合）を示す

【事例】自動運転公共モビリティ

「自動運転車両」と「一人暮らしの高齢者」と「高齢者を見守るリビングサービス」とがリスコミュニケーションを図る場合を想定した全体像
高齢者の意識の有無、コミュニケーションが取れる状況も、刻々と変化していく中で、日常的に信頼のある、利用し慣れているリビングサービスが機能することを目指す



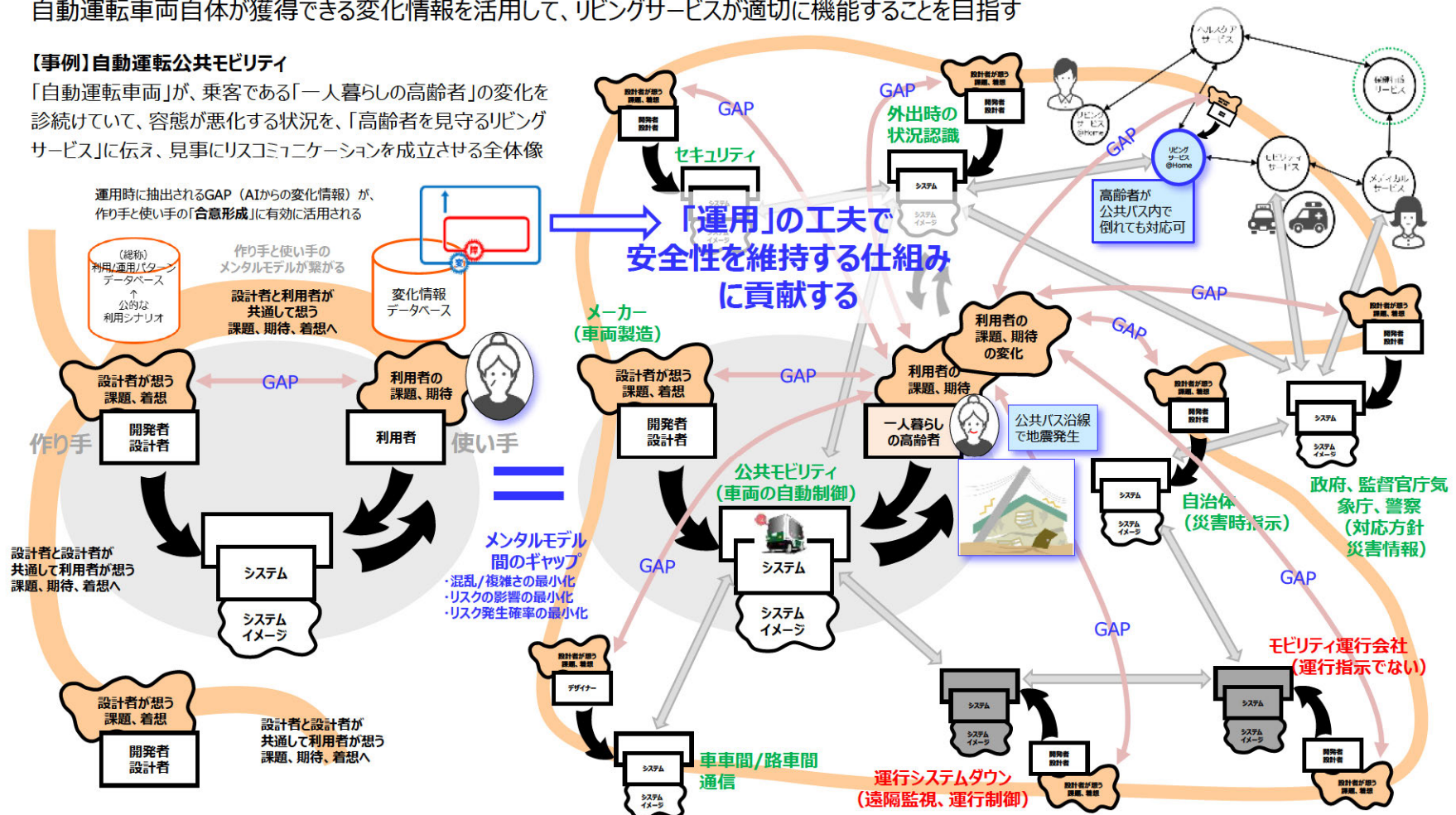
モビリティ事例（自動運転公共バスに一人暮らしの高齢者乗車時の対応）

- 「高齢者を見守るリビングサービス」が機能し、高齢者の安全が守られるイメージ

SoSで生じる「メンタルモデル間のギャップ」を最小化し、状況の変化により様々なリスク要因が重なる際の影響を想定、対応可能にする自動運転車両自体が獲得できる変化情報を活用して、リビングサービスが適切に機能することを目指す

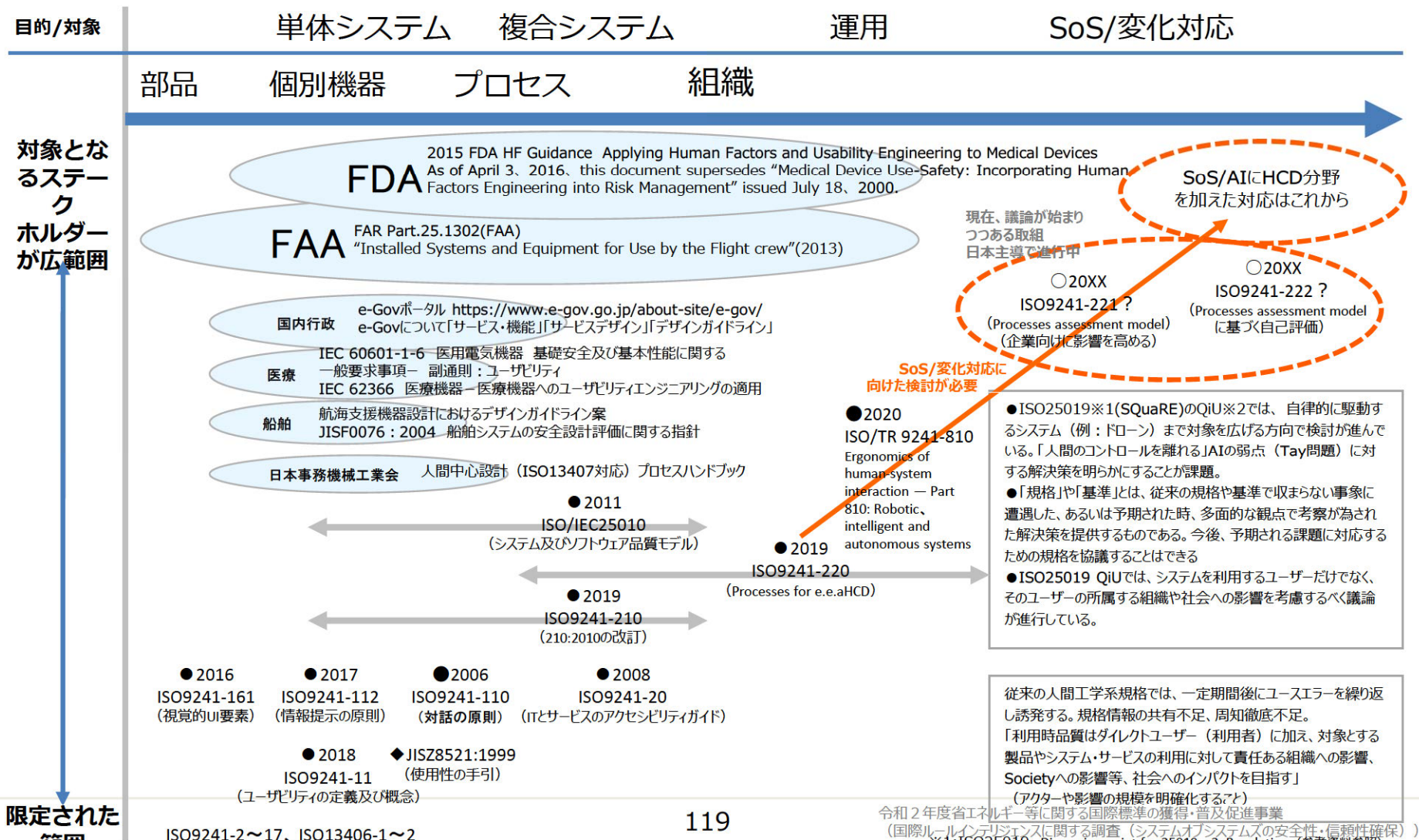
【事例】自動運転公共モビリティ

「自動運転車両」が、乗客である「一人暮らしの高齢者」の変化を診続けていて、容態が悪化する状況を、「高齢者を見守るリビングサービス」に伝え、見事にリスクコミュニケーションを成立させる全体像



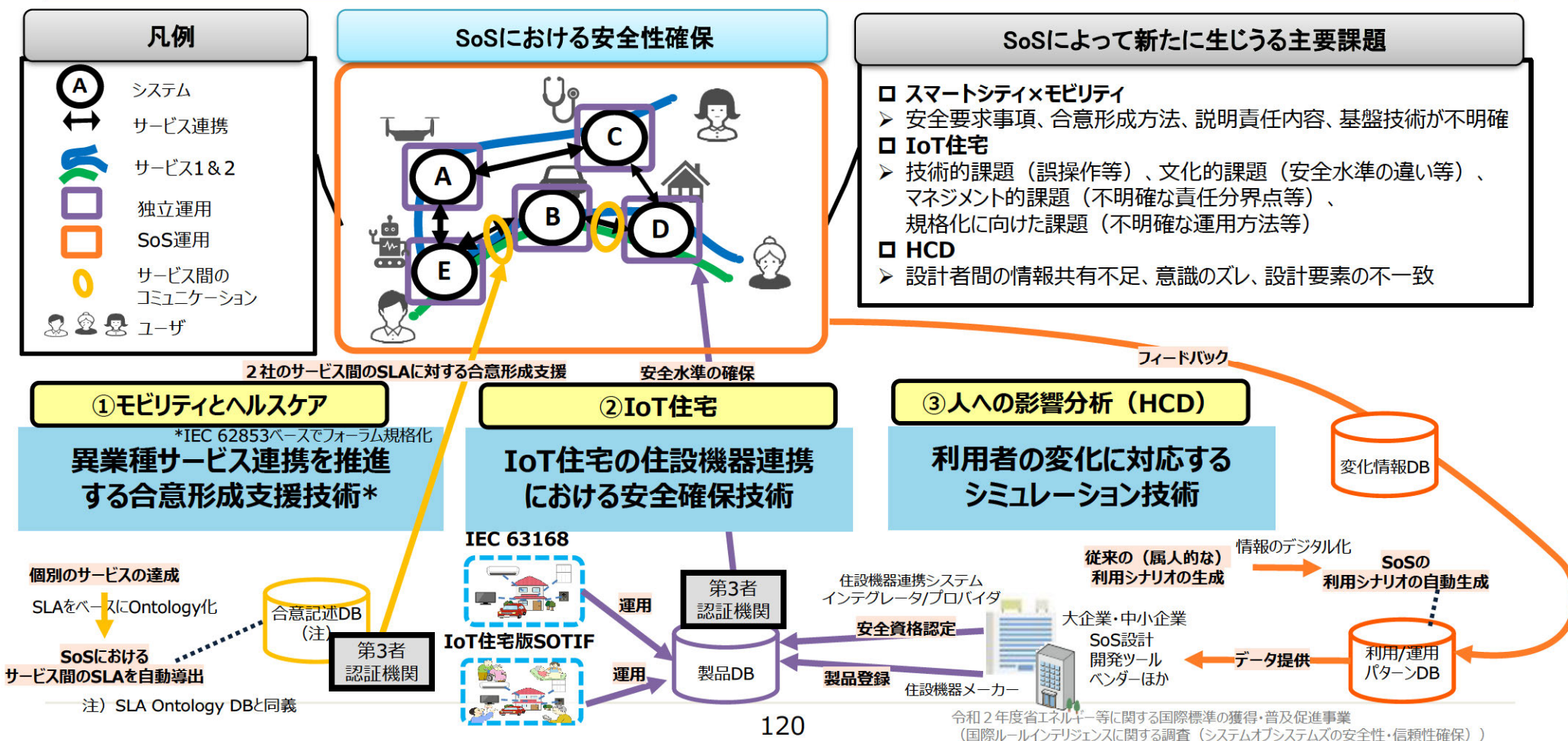
HCD分野の規格及び業界ガイドラインの現状と今後への期待

- SoS/変化対応に適用できるよう、新たな規格/基準が必要となる



2. 2小括 主要課題の解決アプローチ

1. SoSによって新たに生じる主要課題を、スマートシティ×モビリティ、IoT住宅、HCDの観点で整理
2. 解決策としてサービス間の合意形成支援技術、連携システムの安全確保技術、利用者変化に対応するSim技術を提案
3. 実現に向けてIEC62583ベースのフォーラム規格考案、DBやアプリ等のツール設計開発し、実証実験を行うことを提案
(まずはスマートシティ、ヘルスケア、防災、ドローン等を題材に安全要求導出を試行)



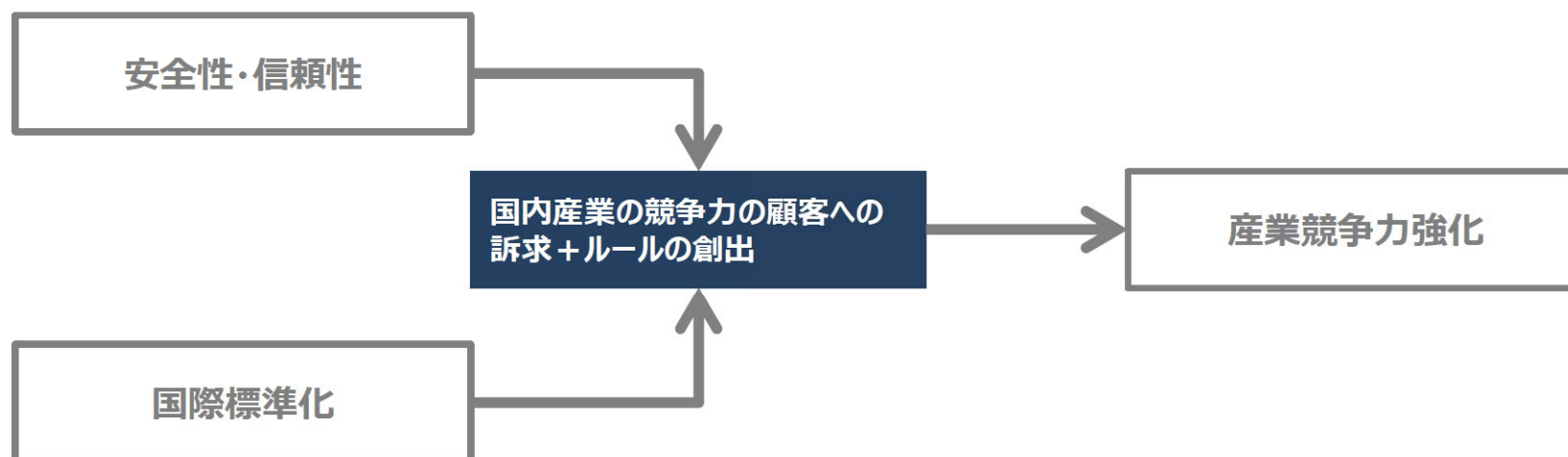
3. システムオブシステムズの安全性・信頼性の実現に向けた国際標準化戦略の検討

3. 1 国際標準を軸にした各国における戦略展開の調査、及びルール普及におけるポイント・課題の整理

※本節の調査検討においては有識者に対するヒアリング及びセミナーなどでの情報収集に基づき検討を行った。

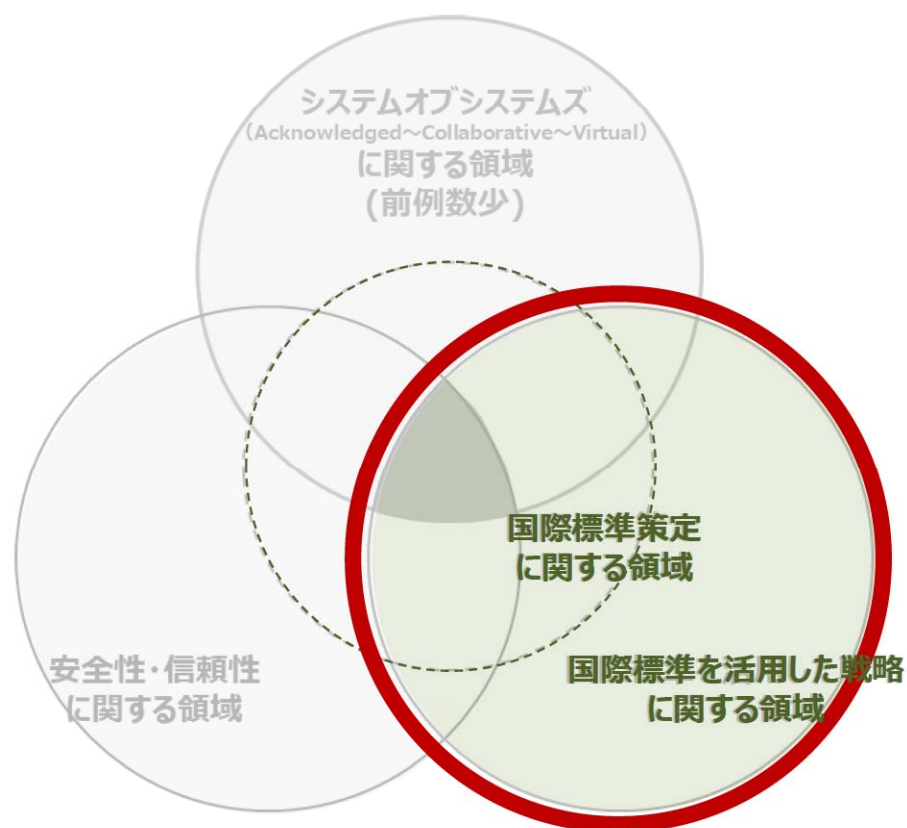
【前提】本事業において対象とする国際標準化戦略（＝産業競争力向上を指向）

- 産業競争力強化に繋がる安全性・信頼性に関する国際標準化戦略の検討を本事業の前提とする。
（対価を得られない**純ボランティアの社会貢献は本事業では対象外**とする。）
- 国際標準を活用した産業競争力強化は、国内産業の競争力の源泉を**価値化するためのルール形成を行うこと**によって実現される。



検討Step1：既存の国際標準化戦略

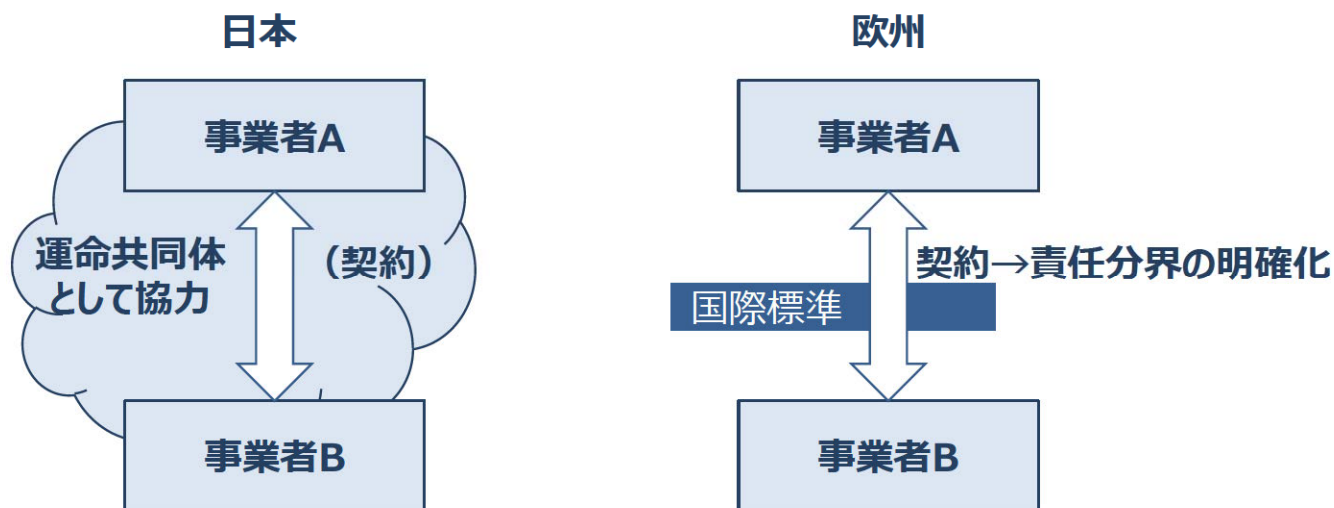
- まず下記について既存事例に基づいて整理を行う。
 - 国際標準策定に関する領域、及び国際標準を活用した戦略に関する領域



【前提】日本と欧米の違い／契約文化とその責任分担ツールとしての標準の位置づけ

- 欧州では同系統の宗教を共有する多民族社会の中で契約という行為が広く普及しており、更に欧州経済統合などの中で整備された欧州規格が契約文化に組み込まれるなど、相対的に均質であった日本国内とは事業環境が大きく異なっている。多様性のあるグローバル社会の姿は日本国内より寧ろ欧州のほうが近く、日本の今後の海外展開にあたっては、「**契約文化と国際標準という相手の土俵に乗る必要性**」がある。
- 特に日本企業においては、「良いものを作れば売れる」といった考え方だけに依存するだけではなく、契約文化における「ルール形成」の価値に着目した上で、**標準化戦略等に十分な経営資源を振り向ける必要**がある。

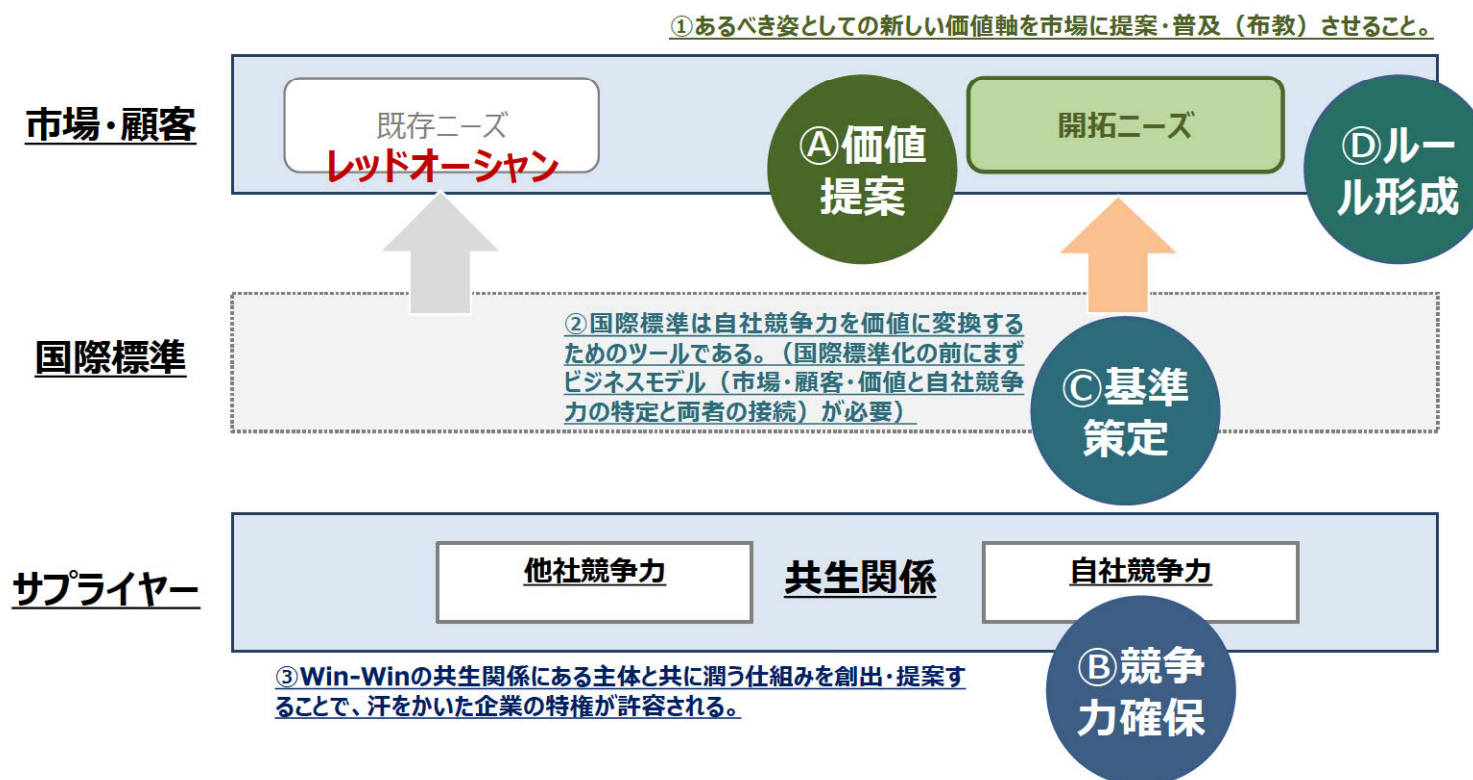
商習慣の違い



ルール形成戦略の考え方

● 国際標準が普及するためには**ビジネス上の差別化戦略に組み込まれることが必要**。

- ①あるべき姿としての新しい価値軸を市場に提案・普及（布教）させること。
- ②国際標準は自社競争力を価値に変換するためのツールである。
- ③Win-Winの共生関係にある主体と共に潤う仕組みを創出・提案することで、汗をかいた企業の特権が許容される。

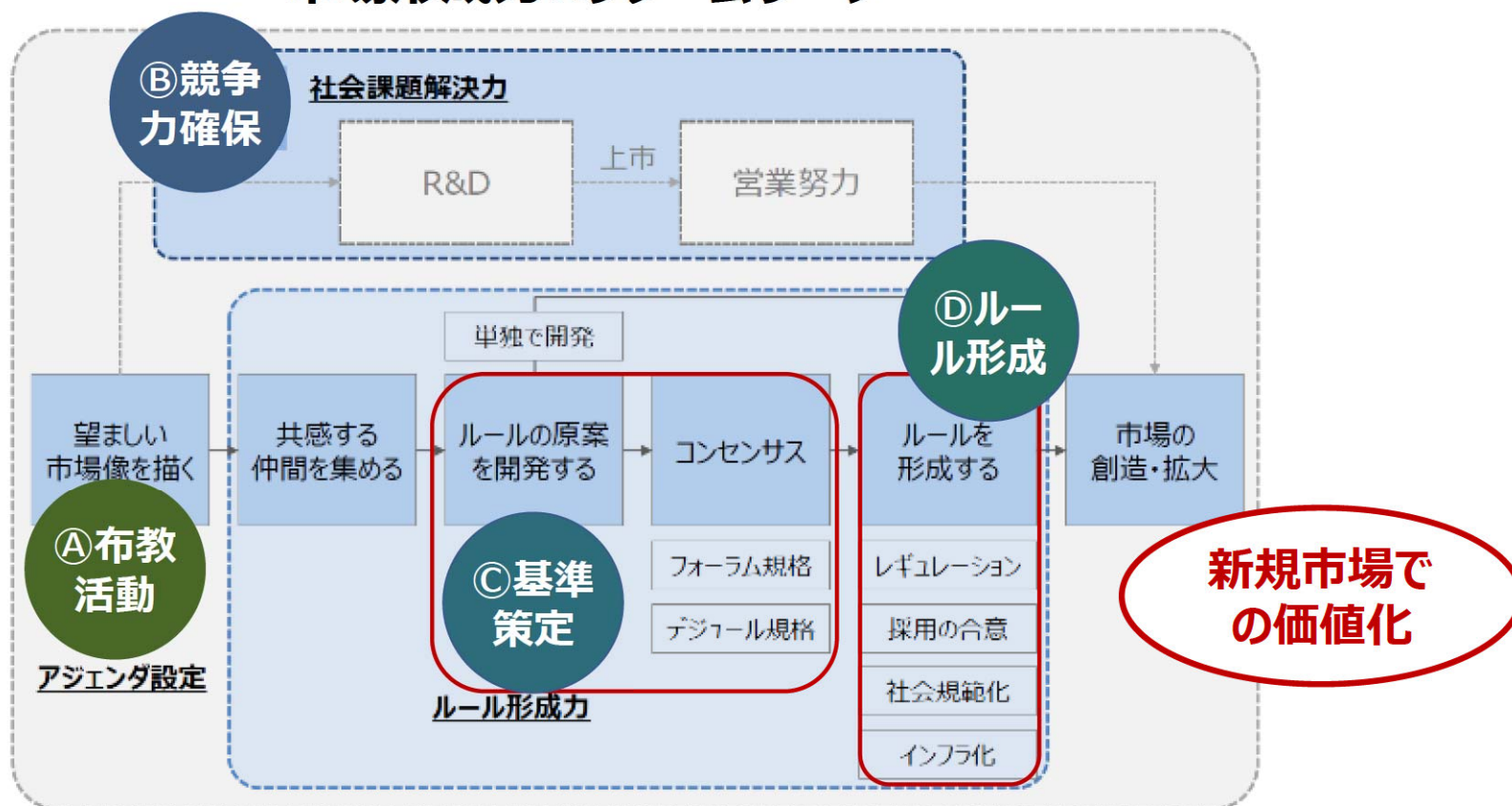


出典）基準認証政策課様ヒアリング内容を参考にMRI作成

ルール形成戦略の考え方

- 「国際標準の策定」は、全体的な「市場形成」×「ルール形成」戦略の一部として位置付ける必要がある。（産業競争力に裨益しない国際標準化は本事業の検討対象外とする。）

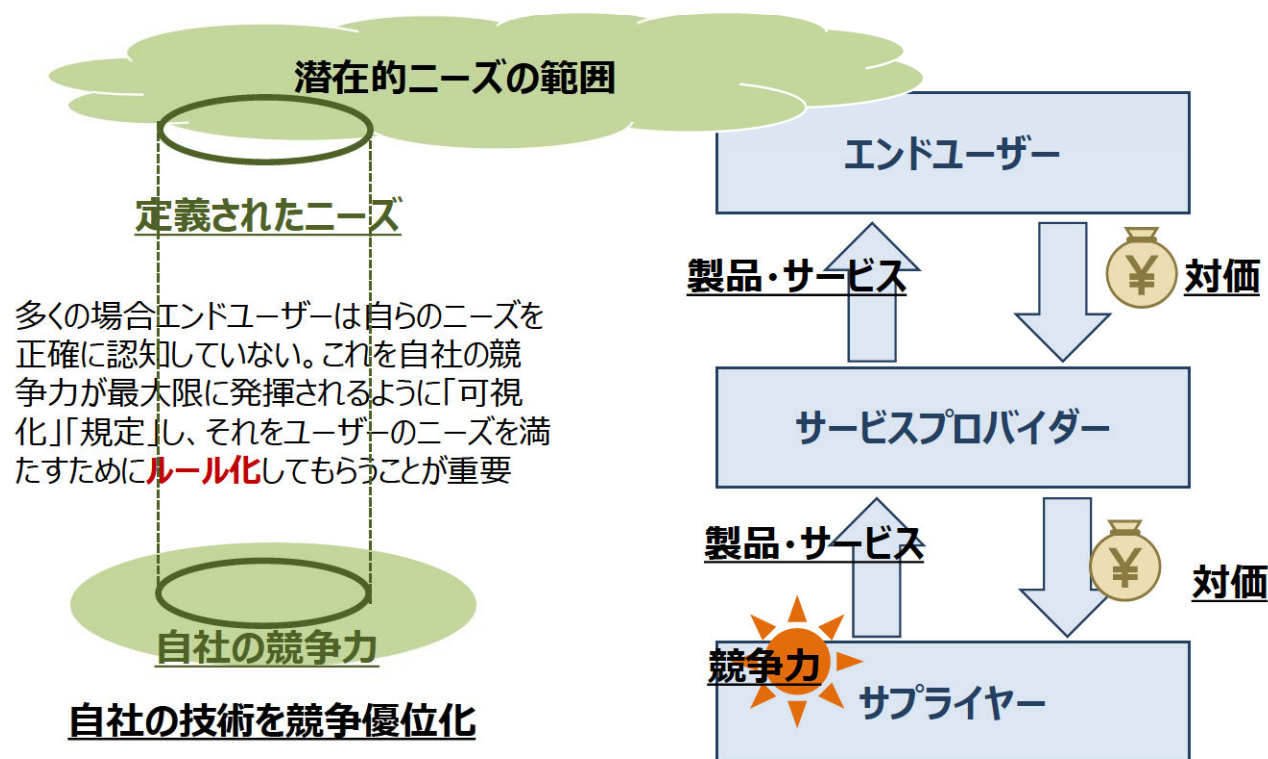
市場形成力×フレームワーク



出所) 経済産業省・日本規格協会「ビジネスを成功させるためのルール形成戦略セミナー」(2021年2月3日)

一般戦略①価値提案／アプローチ＝「新規市場の創出」＞「既存市場でのシェア拡大」

- 殆どの既存市場は既に成熟しておりシェア拡大はレッドオーシャンでの厳しい市場環境となる。
- 新規市場の創出において、ニーズが潜在的である段階においては、そのニーズは潜在顧客の中でも明確に自覚されていない場合が多く、**新規市場開拓と国際標準化によるルール形成を同時に進めていくことで大きな効果**を見込むことが出来る。
- その不確実なニーズを、**自社／自国の競争力を発揮できる部分を切り取り明文化**することによって、競争優位なニーズとして定式化することが出来る。この「**ニーズの定義・提案**」が最重要である。
- 個人以外の一般企業の調達や国の規制にあたっては、調達時にその価値の社会への説明・訴求が必要となる場合が多く、そのための**基準が「大義名分」として通用する「社会善」であることが望ましい**。



- ビジネスプロセスの設計では競争力を発揮するためのオープン・クローズ戦略が必要。

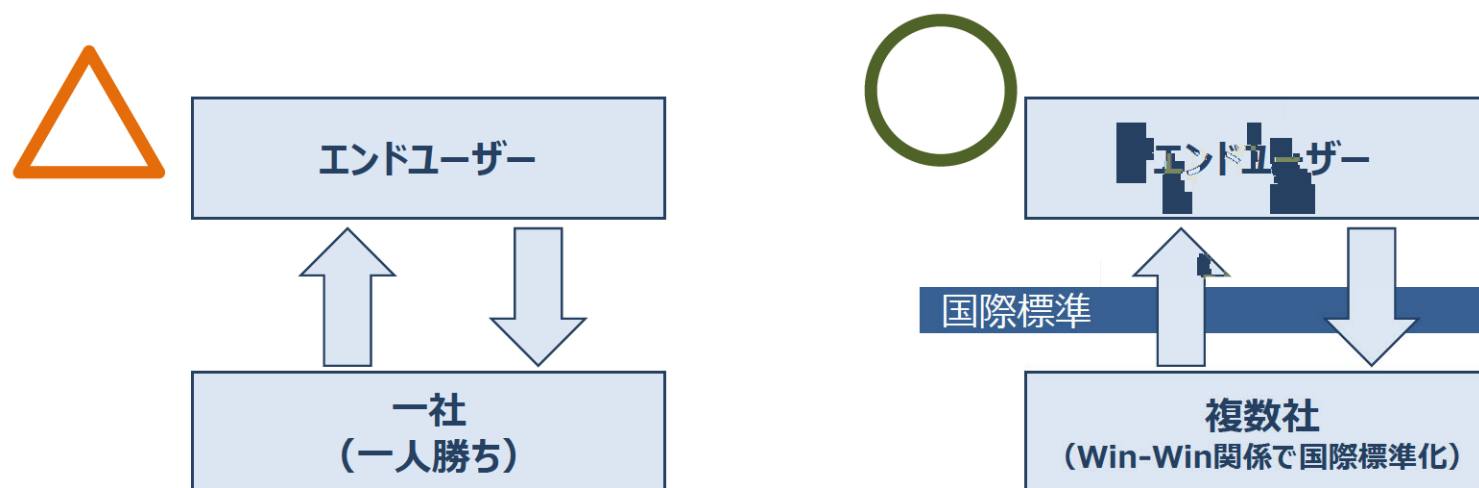
- 自社技術・製品の協調領域と競争領域を見極めた最適なオープン・クローズ戦略を踏まえ、事業戦略・標準化戦略と研究開発戦略・知財戦略と一体的に推進することが重要。



(<http://www.jfma.or.jp/FORUM/2019/doc/0221-1240-F-1.pdf>)、令和3年3月閲覧

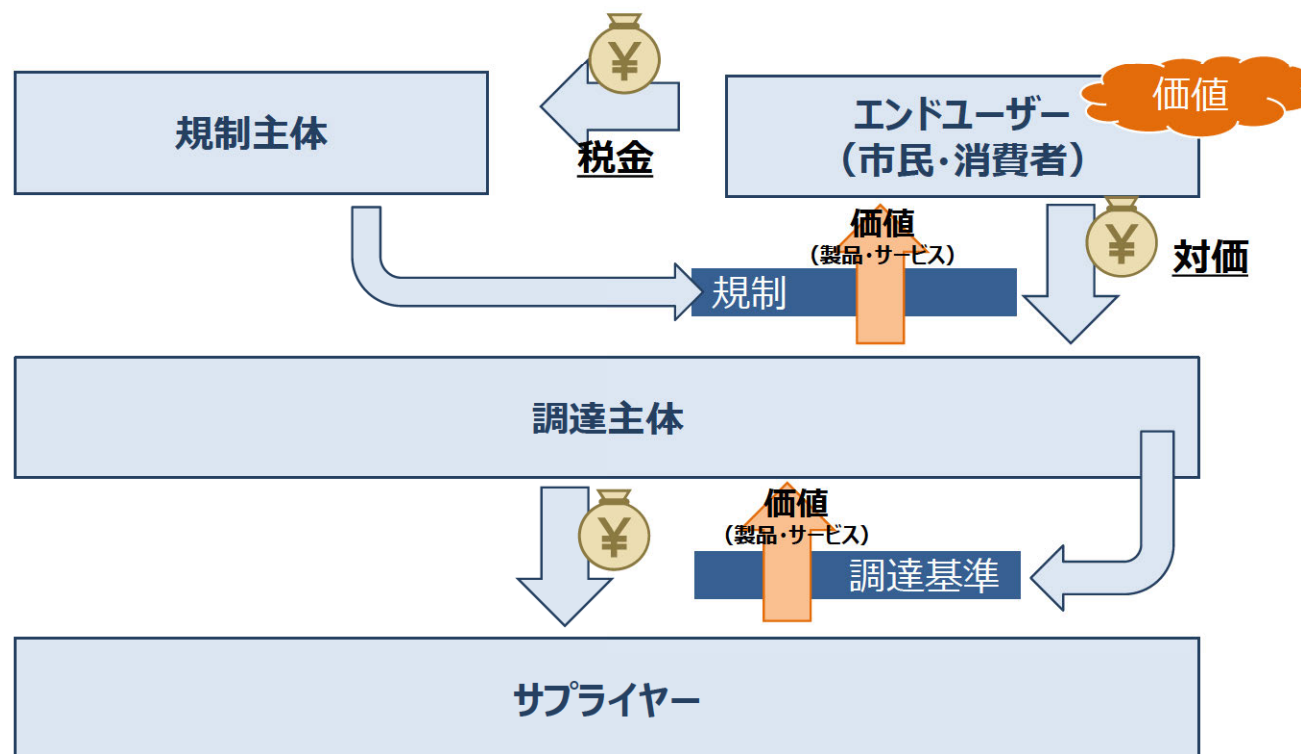
一般戦略◎基準策定／仲間を作る必要性

- 自社だけが持つ競争力を顧客の潜在価値と擦り合わせることが出来ればベスト
- しかし、新規市場創造は全ての国が狙う価値の源泉であり、他国とのルール争奪戦にならざるを得ず、「**一人勝ち**」が許される状況は通常創出されない。（過去の事例でも一人勝ちに見える事例は、相応の汗をかいた結果、他企業に許された分け前という位置づけになる）



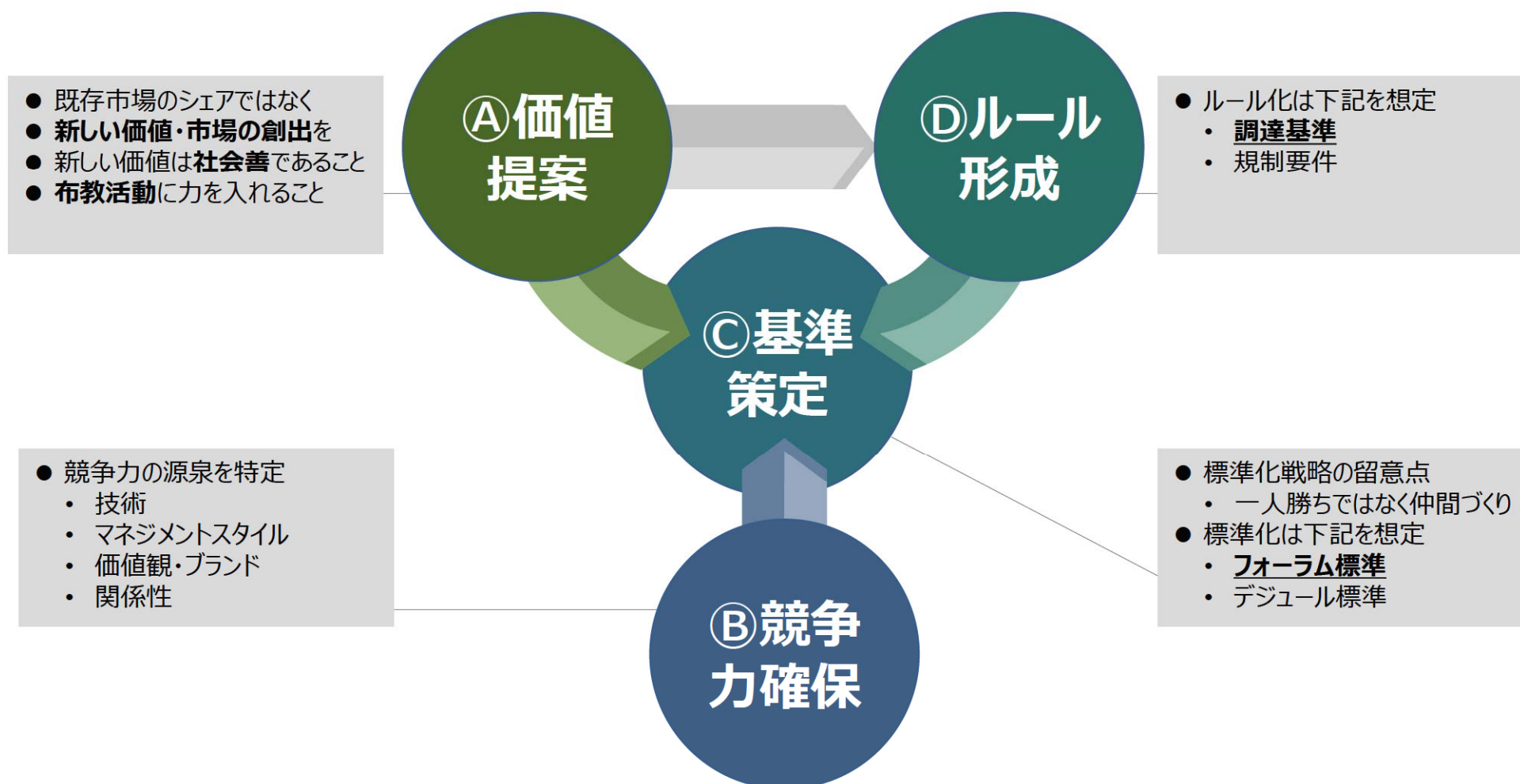
一般戦略④ルール形成／主に「①規制要件」「②調達基準」（又は③「認証マーク」）

- 産業競争力は如何に有利・競争力が発揮されるルールを構築するかが重要。
- ルールを規定する主体は基本的に「①規制主体」「②調達主体」の2種類。
- 「ルールを規定する主体が**大義名分のためにルールを策定する**」構造とすることが重要。
- また、明示的なルール以外の普及戦略としては「③認証マーク」を活用する方法もある。



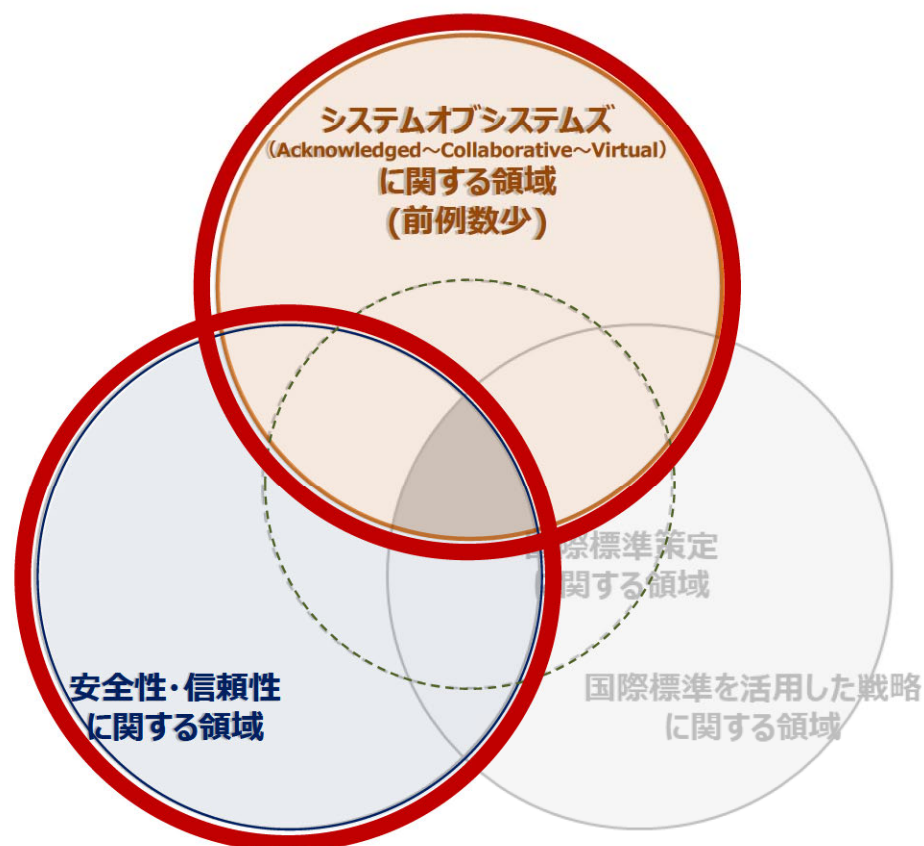
一般的なルール形成戦略の考え方

- 下記を関連付けて同時並行的に設計・具現化することが重要。
①価値提案、②競争力確保、③基準策定、④ルール形成



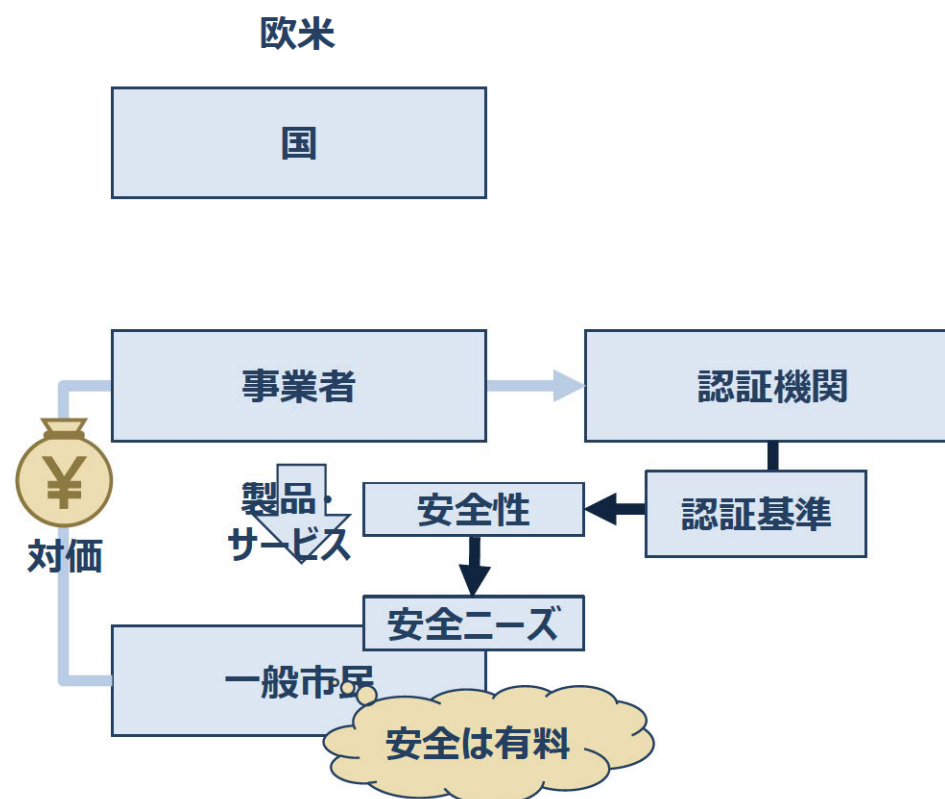
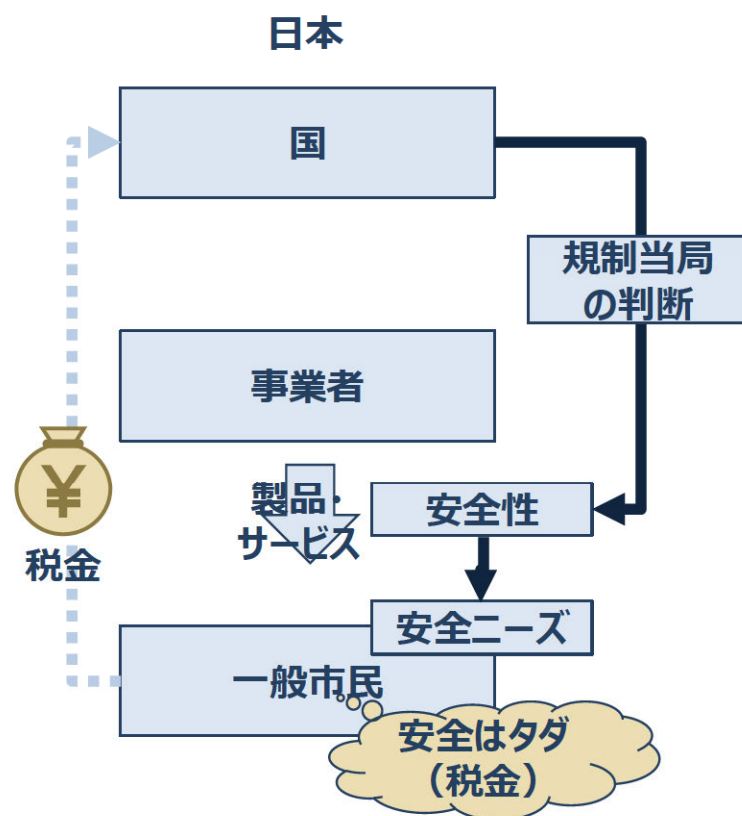
検討Step 2 : 安全性・信頼性とSoSの観点からの検討

- 次に安全性・信頼性とSoSの観点からの検討を行う。
 - Society5.0時代の「多くのシステムが繋がっていく社会（System of Systems）」を想定
 - Society5.0時代における安全性・信頼性のあり方を検討



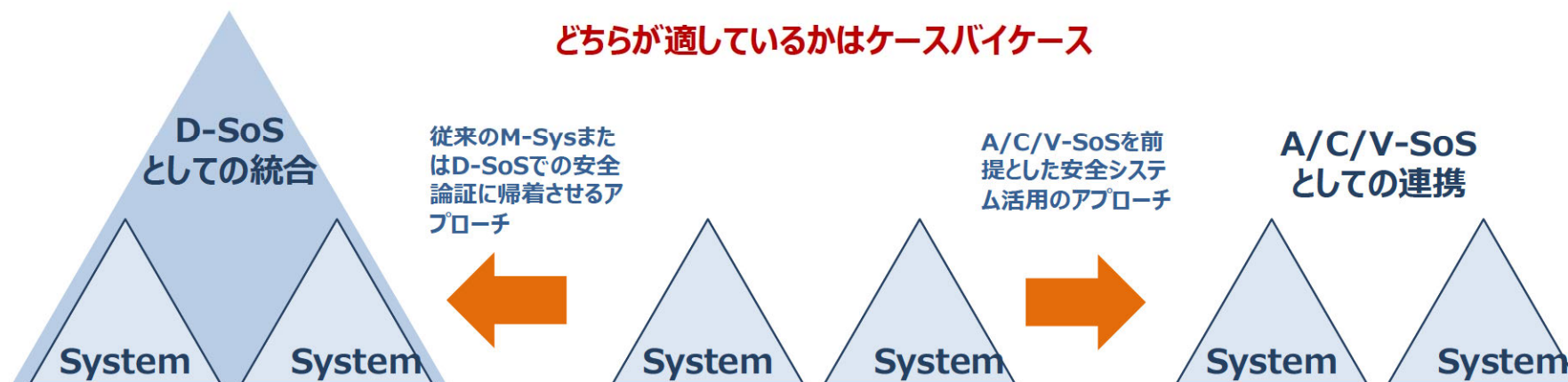
【前提】日本と欧米の違い／安全という価値に関する前提の違い

- 安全規制については基本的には地域性のある自国内の問題であるが、欧州などでは経済統合・市場一体化などの必要性から安全規制のための基準も域内の共通化が図られており、国際標準にもなっている。
- 安全規制も日本は国が規定する法令が中心であるが欧州では民間の認証機関の果たす役割が大きい。



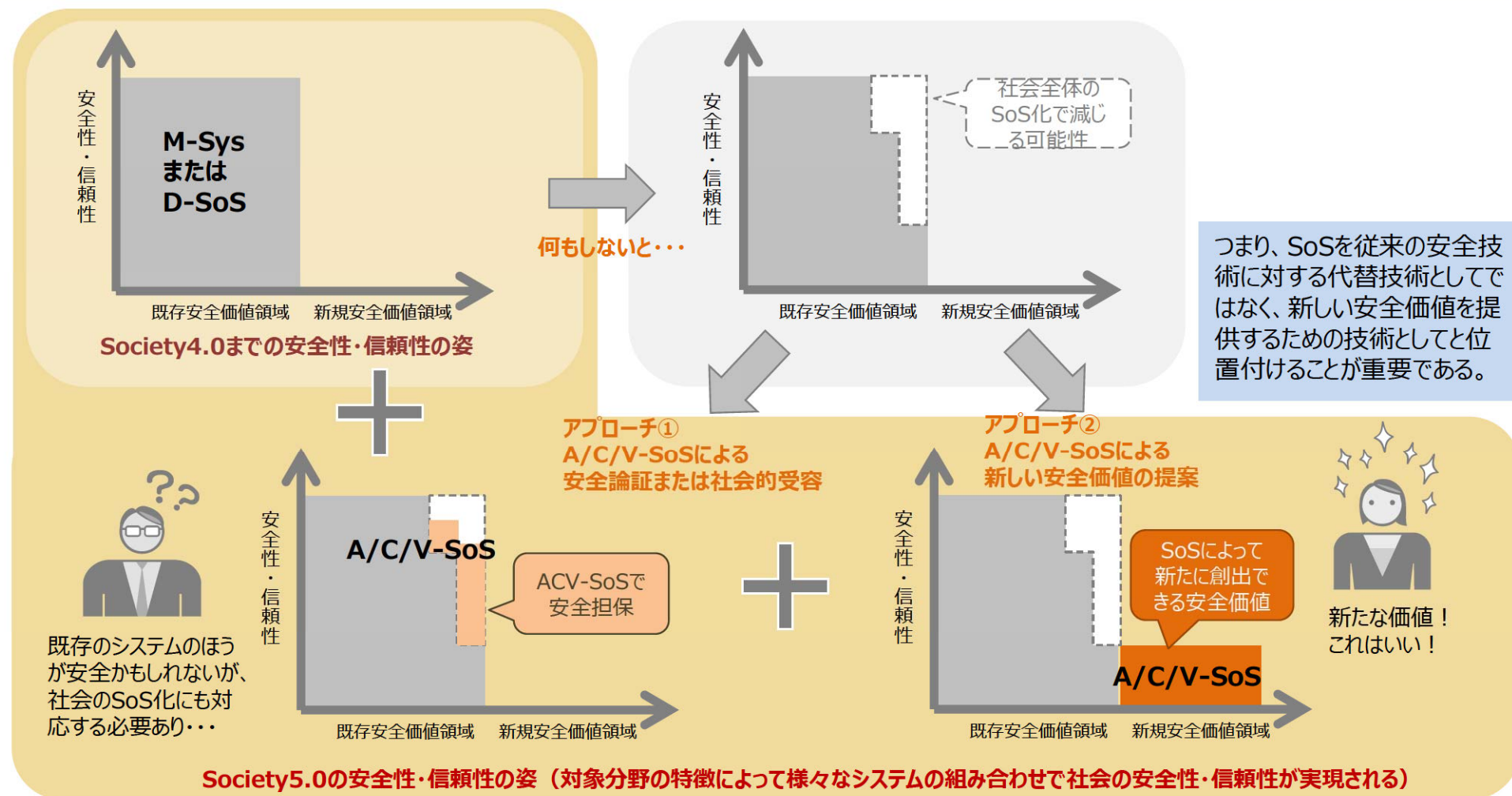
安全性・信頼性とSoS分野での④価値提案／新規価値創出

- 安全システムが担う「**人命に対する責任**」のもと、安全分野での新規技術導入に対するアプローチは、被害影響が大きい“**ミッションクリティカル**”な分野の場合にはM-SysまたはD-SoSでの**安全機能に対する高い信頼性を説明する従来の安全論証に帰着させるアプローチが必要**と考えられる。
- 一方で、安全分野におけるA/C/V-SoSの不確実性を伴うシステム導入に対して**社会的な責任負担・社会実装の道筋を描くことは今後の課題**である。**影響が局所的である場合には消費者の社会的受容性判断に委ねる方法**も一つのアプローチと考えられる。（アカウントビリティなどがポイント）



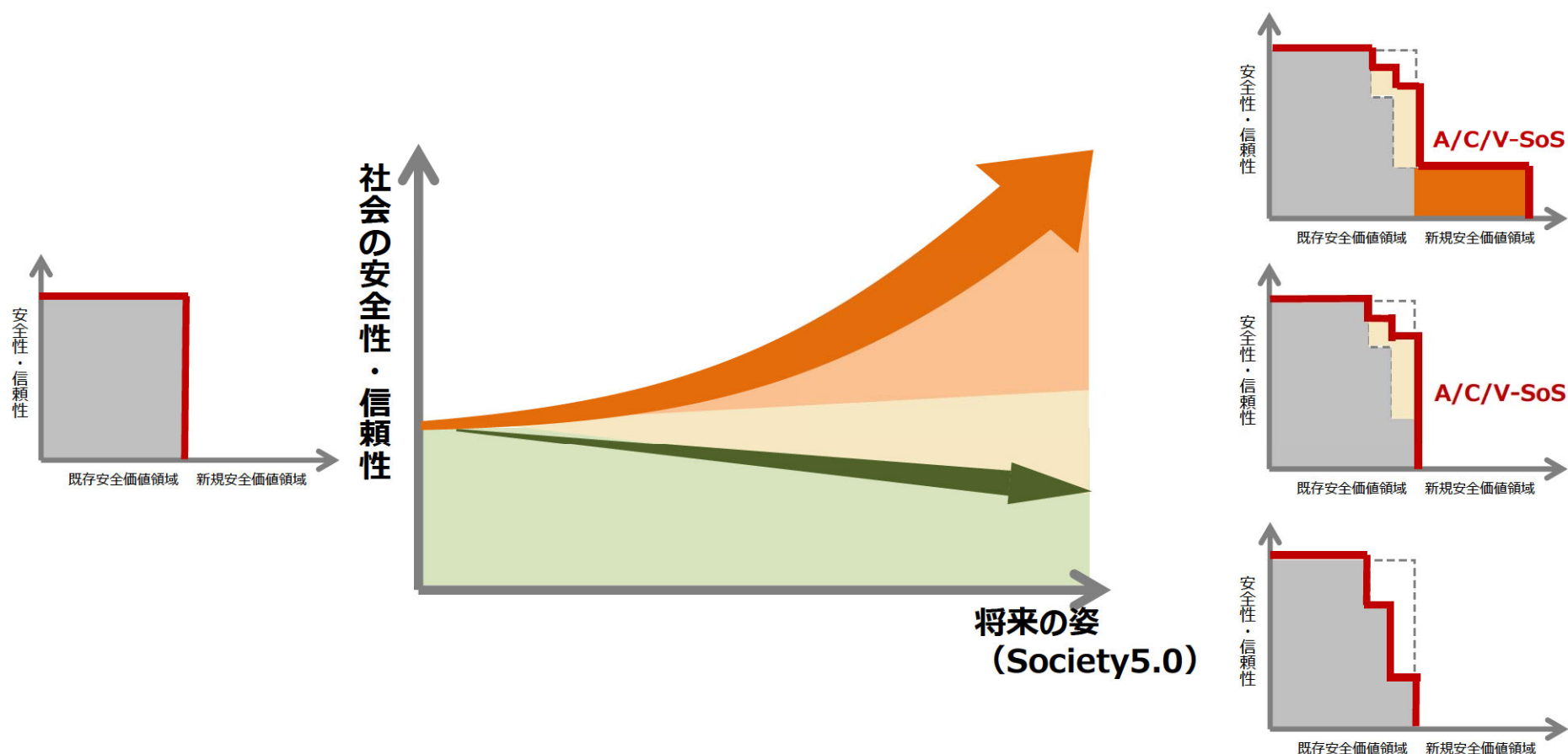
安全性・信頼性とSoS分野での①価値提案／新規価値創出

- 既に確立している安全価値領域のシステム（M-SysまたはD-SoS）の一部をA/C/V-SoS化すると安全機能の信頼性を懸念する声が根強い。安全価値創造戦略としては、①既存領域の安全価値を維持する、よりも寧ろ、②**新規領域の安全価値を拡大する、可能性を第一に目指すべき**と考えられる。



安全性・信頼性とSoS分野での①価値提案／新規価値創出

- これまで構築してきた安全性・信頼性をどれだけ死守しようとしても、一部は社会全体のSoS化の変化を受け入れざるを得ない可能性がある。むしろ社会の変化に対して、新しい安全性・信頼性の姿をプロアクティブに構築していく必要がある。具体的には、従来のM-Sys/D-SoSによる安全性・信頼性を、一部は①A/C/V-SoSに置き換える、②新しい安全性・信頼性の価値を創出していく（①のSoS技術を活用したA/C/V-SoSが含まれる）、といった取り組みが必要となる。

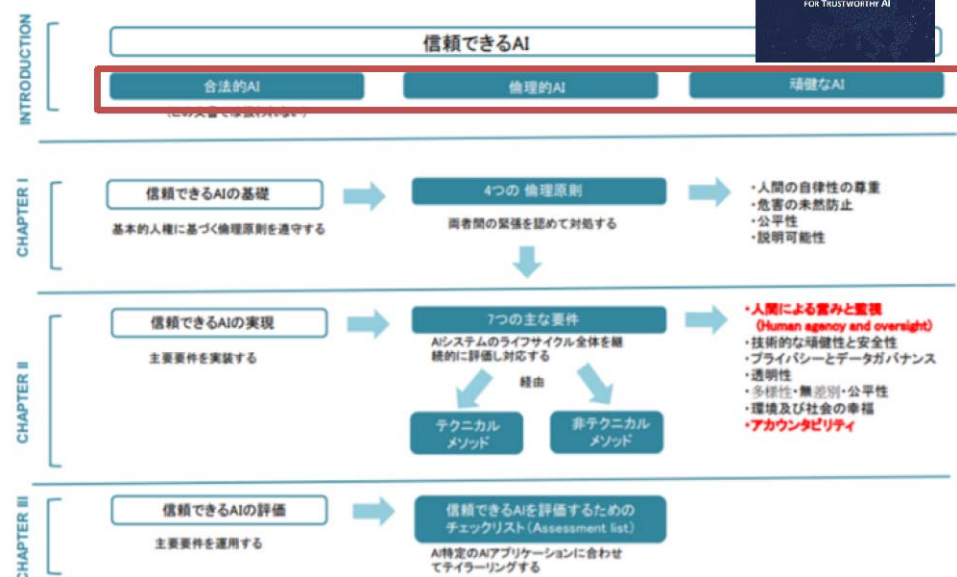


安全性・信頼性とSoS分野での④価値提案／新規価値創出

- 新しい価値創造として例えば下記が挙げられる。
 - AIの倫理、SDGs・ESG、カーボンニュートラル、人権、レジリエンス、...

信頼できるAIのための倫理ガイドライン

- 欧州委員会の高等専門家グループ「AI HLEG」にて信頼性を備えるAIを奨励する倫理ガイドラインを発行
- 信頼性を備えるAIとは、システムのライフサイクル全体で以下の3要素を保つもの（同ガイドライン規定）



出所) <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top>
<https://www.ieice.org/~swim/jpn/presentations/swim2019-24.pdf>、2021年3月閲覧

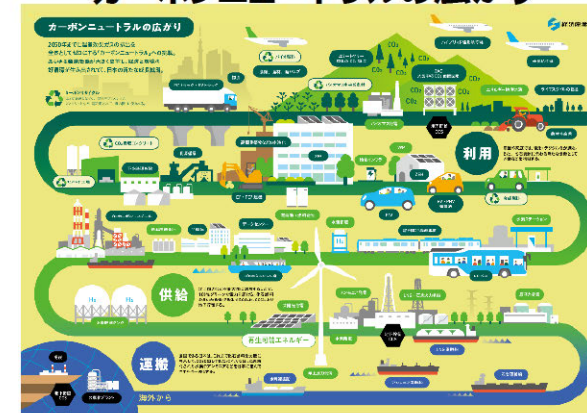
SDGs



出所)

https://www.unic.or.jp/activities/economic_social_development/sustainable_development/2030agenda/sdgs_logo/、2021年3月閲覧

カーボンニュートラルの広がり



出所) <https://www.meti.go.jp/press/2020/12/20201225012/20201225012.html>、2021年3月閲覧

令和2年度省エネルギー等に関する国際標準の獲得・普及促進事業
 (国際ルールインテリジェンスに関する調査(システムオブシステムズの安全性・信頼性確保))

安全性・信頼性とSoS分野での⑧競争力確保

- システムオブシステムにおいて競争力の源泉となる「技術」に関しては、「grant」「論文」「特許」等に対する技術調査の結果では海外に対して**競争力を持つ技術は特定が困難**であった。（添付資料2参照）

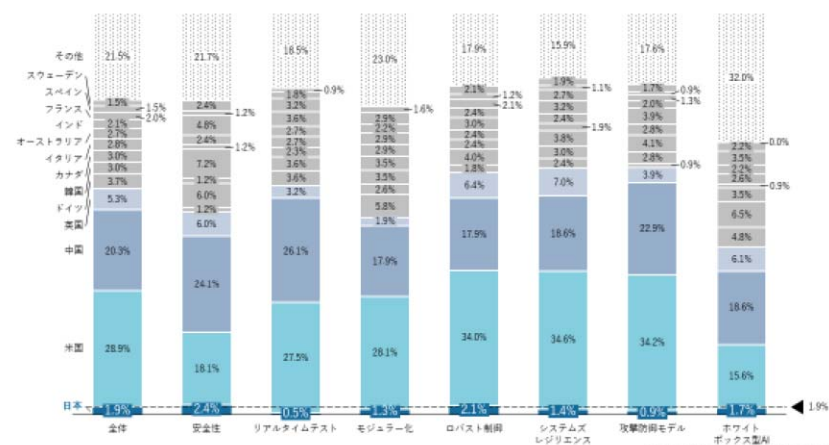
2 技術の定量評価や投資額動向等より重要領域・技術を特定

論文

astamuse
company

論文執筆者の国籍から国別の動向をみると、アメリカ・中国・イギリスが大半を占める。日本の研究が相対的に多いのは安全性やロバスト制御技術

分類ごとの論文執筆者の国籍割合



2 技術の定量評価や投資額動向等より重要領域・技術を特定

特許

astamuse
company

尚、特許に関しては日本の出願数は少ない。システムズレジリエンスやAI、セキュリティ関連については相対的に割合が高い領域

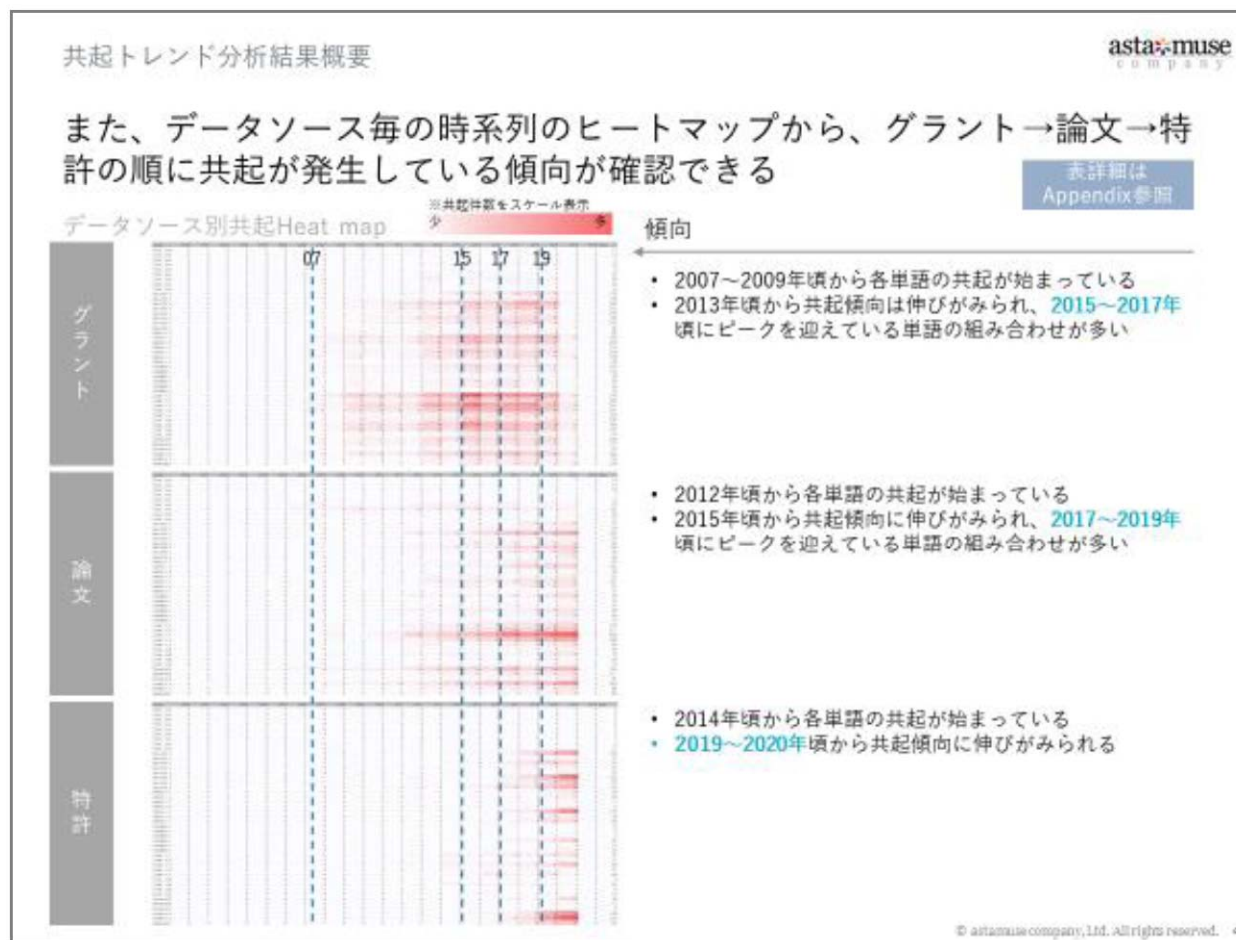
(参考) 分類別特許数と日本特許出願特許数

No.	分類	特許数	内、出願番号 JP始まりの特許	JP特許割合
1	安全要求定義/安全性解析	661	7	1.1%
2	リアルタイムテスト	29	0	0.0%
3	モジュール化	948	11	1.2%
4	攻撃防御モデル	1253	28	2.2%
5	ロバスト制御	178	1	0.6%
6	システムズレジリエンス	174	5	2.9%
7	ホワイトボックス型AI	167	4	2.4%

© astamuse company, Ltd. All rights reserved. 22

安全性・信頼性とSoS分野での⑧競争力確保

- SoS分野技術は、グラント→論文→特許の順でトレンド（共起）遷移が生起している。技術が競争力を持ち得る（実ビジネスで使えるようになる）ためには数年オーダーでの戦略的投資が必要と考えられる。（添付資料2参照）



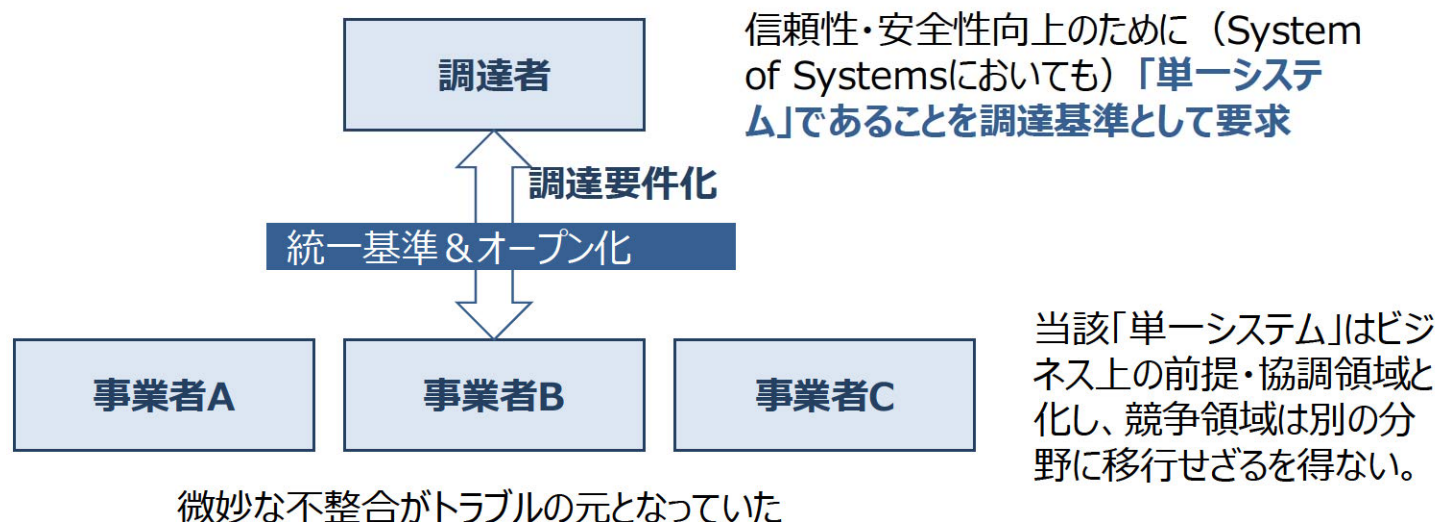
安全性・信頼性とSoS分野での⑥競争力確保

- 戦場は競争力のある分野とすべきであり、競争力のない分野で戦うべきではない。
- デジタル技術が普及した際の自国の競争力は何か。（DEOSプロセスだけでは競争力にはならない）
→**訴求すべき価値・分野によって異なる。これを特定することが重要。**

課題	概要	解決策（技術）	解決策（マネジメント）	【参考】分野事例
システム	①全体リスク想定 の困難性	①安全要求定義／安全性解析	①SOTIF ②STAMP ③FRAM	電力 交通 医療 住宅 家電
	②運用時の変化 対応の困難性	②リアルタイムテスト技術 ③モジュール化 ⑤ロバスト制御 ⑥システムレジリエンス	④DEOSプロセス	
	③運用時の障害 対応の困難性			
	④ユーザ・ユー スケース想定 の困難性	⑧ヒューマンファクター	⑤HCD	
コンポ ネント	⑤AIの挙動の 不確実性	⑦ホワイトボックス化 ⑥DSM		④サービスロボット JIS Y1001等
	⑥サイバー攻撃 への対処	④攻撃防御モデル	⑥CPSF	⑦自動運転 Pegasus Project

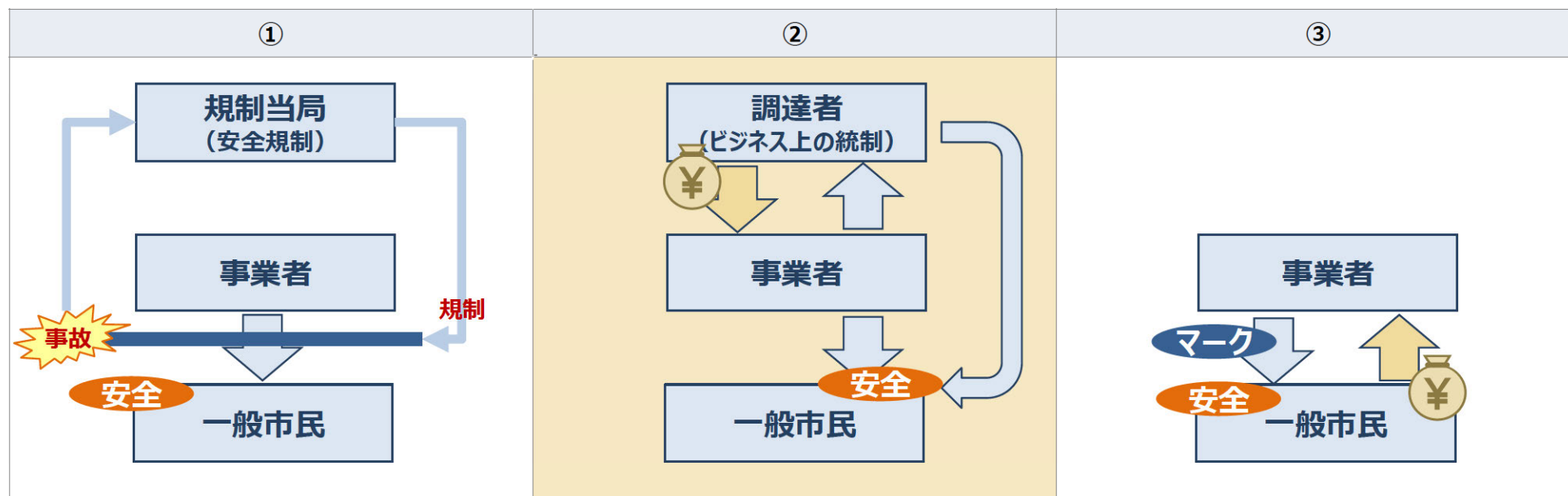
安全性・信頼性とSoS分野での◎基準策定／OPEN化という戦略

- System of Systems において総合信頼性を確保するための考え方は下記の2通り
- ① Systemsが多様である限り、欠陥はなくなる。欠陥を無くすための唯一の方法は、**単一のシステム**にすることである。SoSの複数ステークホルダーによる単一基準の策定のためには**オープン化が必須**。それは**SoSを対象とした場合にはフォーラム標準**の形となる。
- ② SoSの複数システムの**多様性を認めつつ**、安全性・信頼性を確保するための何らかの対策を行う。（高い安全性・信頼性のためには安全論証が必要となるがその技術開発は今後の課題）



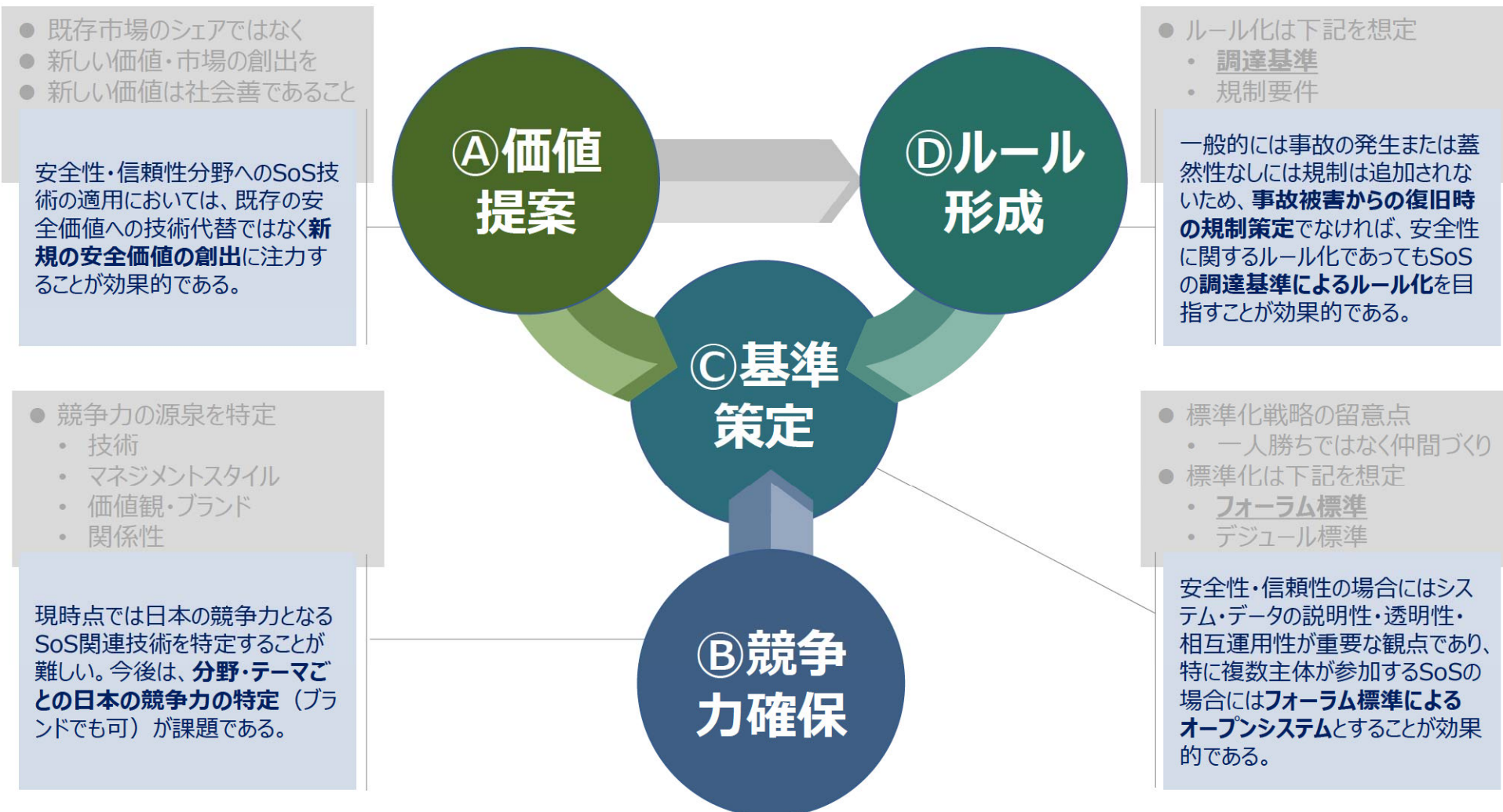
安全性・信頼性とSoS分野での①ルール形成／調達基準の活用

- ルール化は以下の3つが考えられるが、①は安全性・信頼性分野では現実的には事故後の復旧時期でないと規制強化にはならないこと、③は強制力が働きにくいことなどから、一般的には安全性であっても②を狙っていくべきであると考えられる。
- ① 規制当局による義務的安全規制要件化
- ② 調達基準で要件化することによるサプライチェーン上・相互接続インターフェース上での義務化
- ③ 消費者の購買行動での「認証マーク」による選別（個人消費行動を通じた社会的受容）
（③はマークの認証主体によって①②と組み合わせ可能）



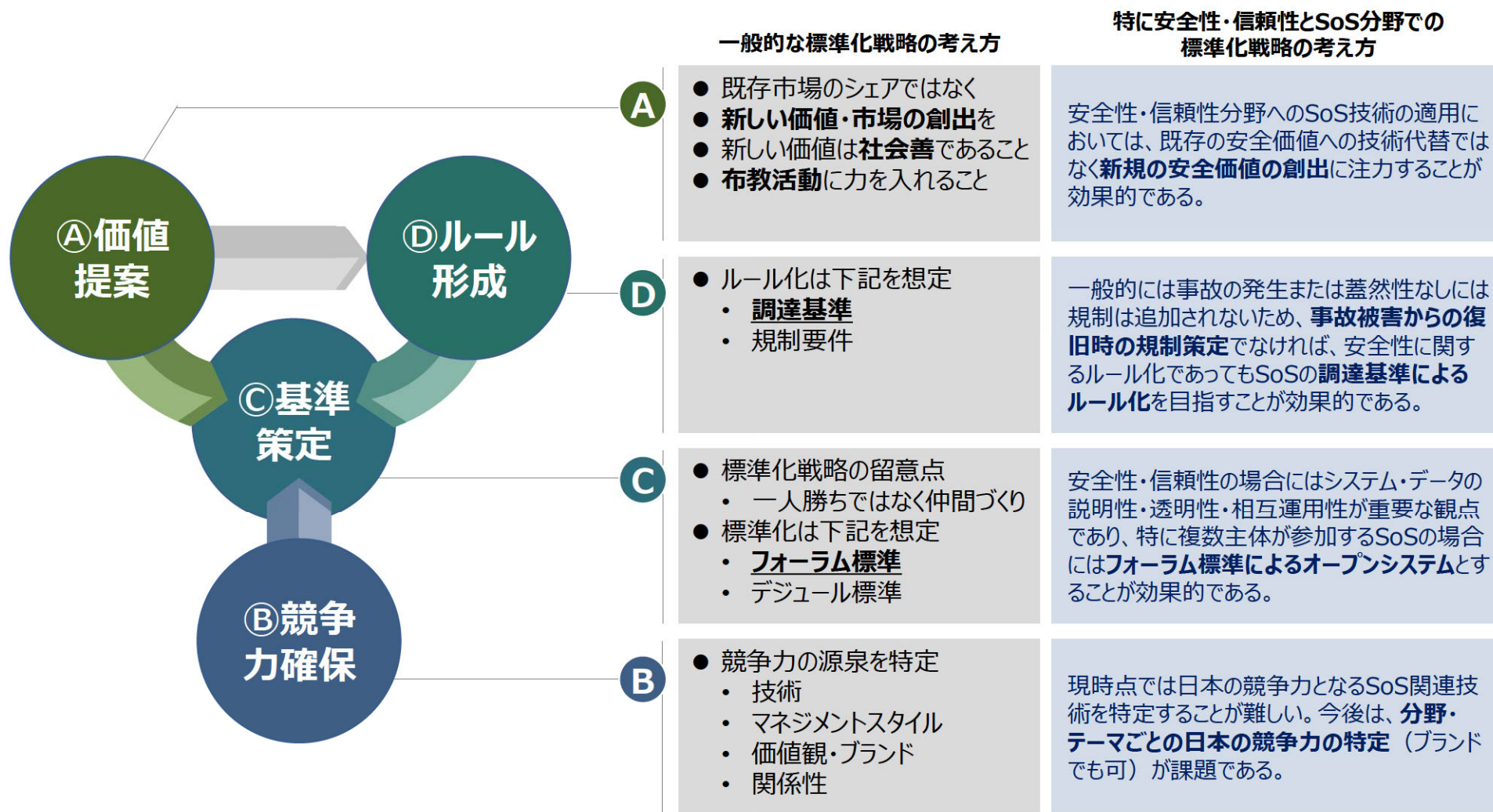
安全性・信頼性分野でのSoS活用における国際競争力確保のポイント

特に安全性・信頼性の分野で効果的なアプローチは以下と考えられる。④新規の安全価値の創出、⑤日本の競争力の特定（分野ごとの課題）、⑥フォーラム標準によるオープンシステム、⑦「可視化」すること



3. 1 小括 安全性・信頼性とSoS分野の標準化戦略において留意すべきポイント

安全性・信頼性とSoS分野の標準化戦略において留意すべきポイントを以下に整理した。

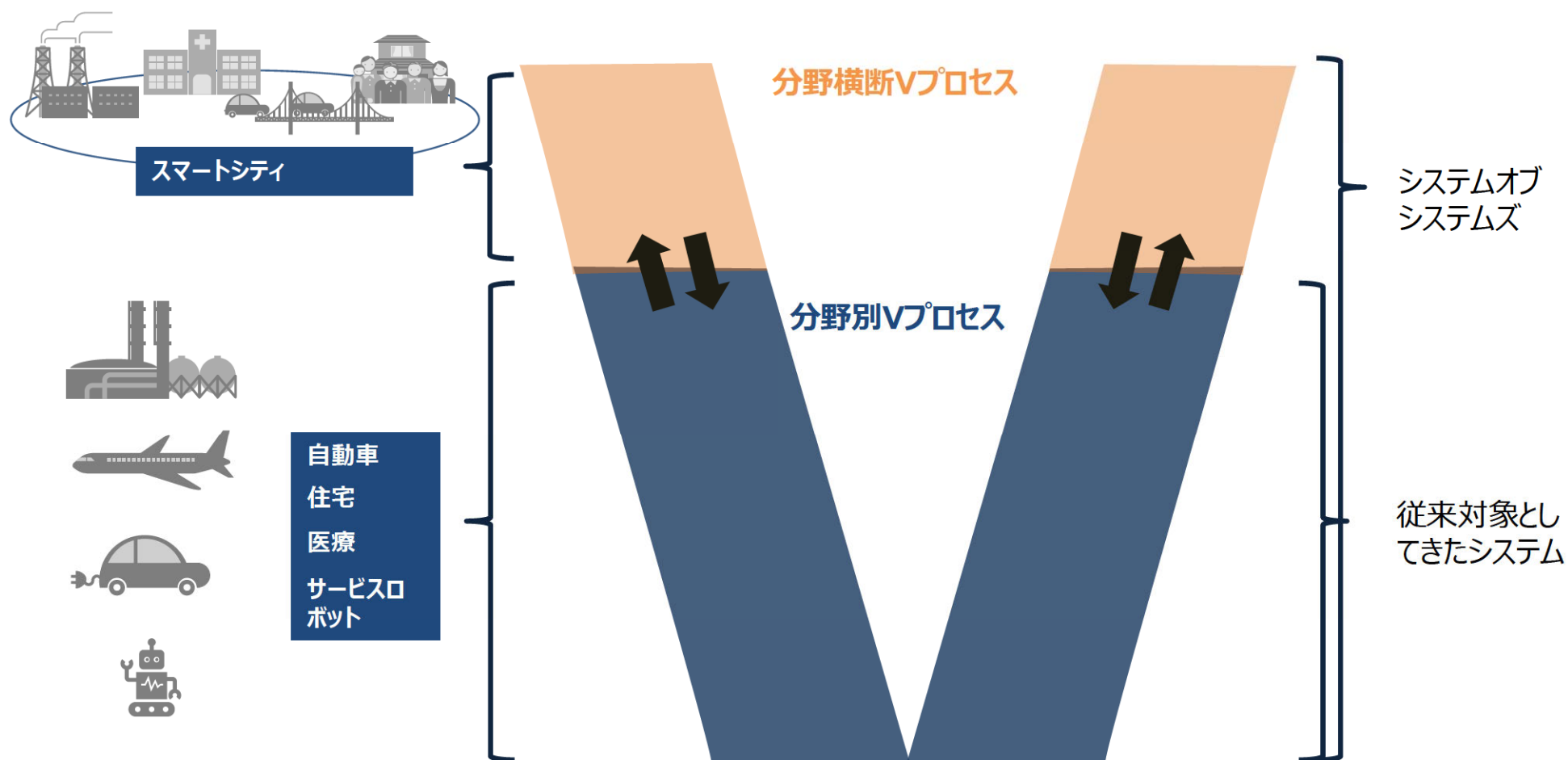


3. システムオブシステムズの安全性・信頼性の実現に向けた国際標準化戦略の検討

3. 2 国際ルール形成を通じて競争優位を実現するのに適した産業分野や国際標準化戦略の検討

システムオブシステムズの視点からのV&Vプロセス

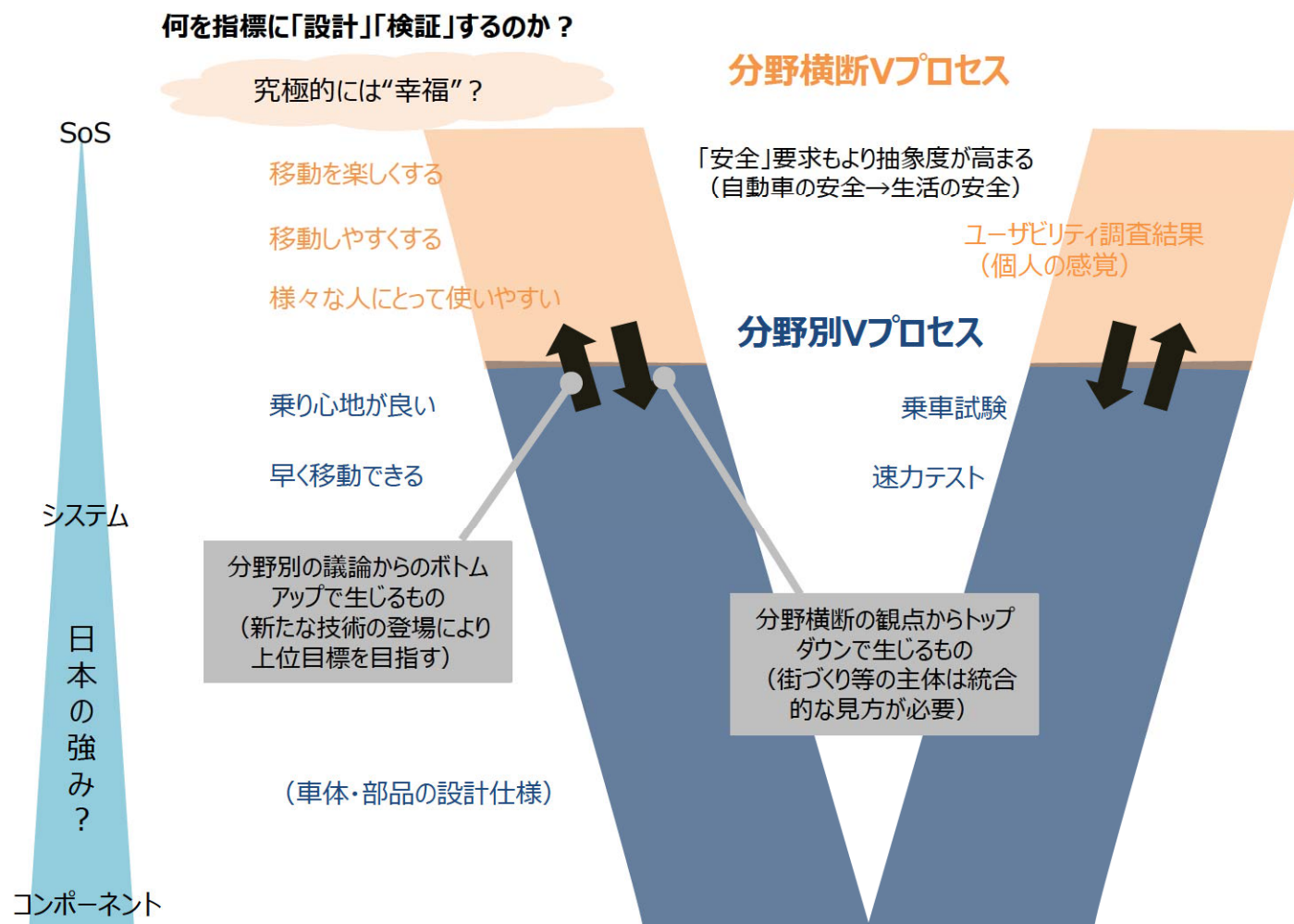
- 「システム」を対象とした従来の機能安全等の考え方（V&Vシステム）を、そのまま「システムオブシステムズ」に適用すると更に上位層の階層が追加される形となる。→“高次元目標を踏まえた設計・検証方法”



国際標準化戦略への展開イメージ

■ 最終的には「日本の強み」を生かせる戦略にする必要がある。

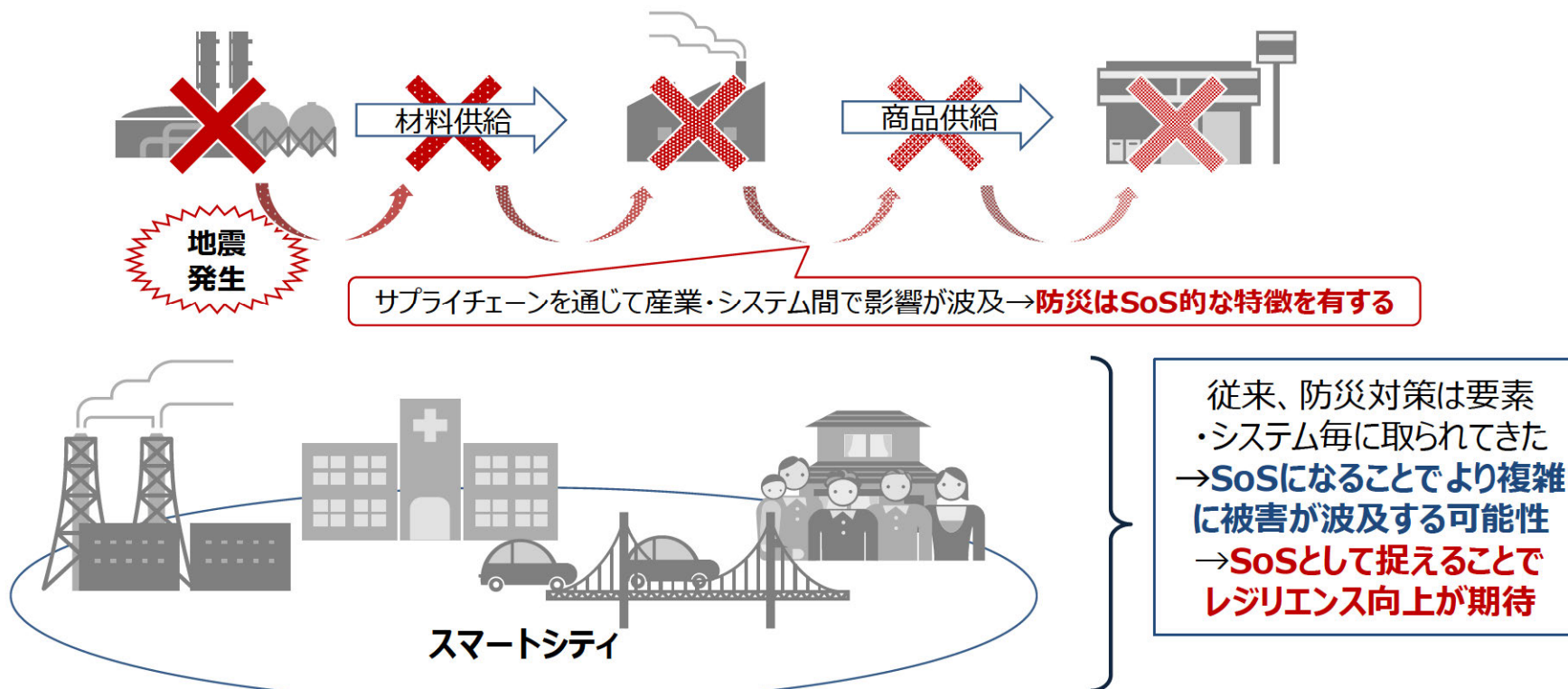
- 「日本の強み」の特定
- 解決策のシステム性能への落とし込み



国際標準化戦略の検討例：防災・レジリエンスの課題解決

スマートシティにおける防災上の具体的な課題（①価値提案）

- 災害はコントロール不可能な危険源であり、あらゆるシステムに影響を及ぼす。また、災害によって影響を受けたシステムは関係する産業やシステムに影響を及ぼすなど、**災害自体が既にSoS的な特徴を有しており**、SoSを考えるにあたって有益な知見があると見込まれる。
（例：インフラ被害により工場停止→その部品を使う工場や産業も停止するなど、サプライチェーンを通じて波及）
- スマートシティ、SoSにおいては、より地域単位で各機能・システムが密接に関わることで**サプライチェーンよりもさらに複雑な形で都市のレジリエンスが脅かされる**ことが懸念される。
- ただし、これまで地域を構成する機能・システム毎に考えられていた防災を、システムがつながった状態を前提として考えることで、防災上新たな価値をもたらしレジリエンスが向上しうる。

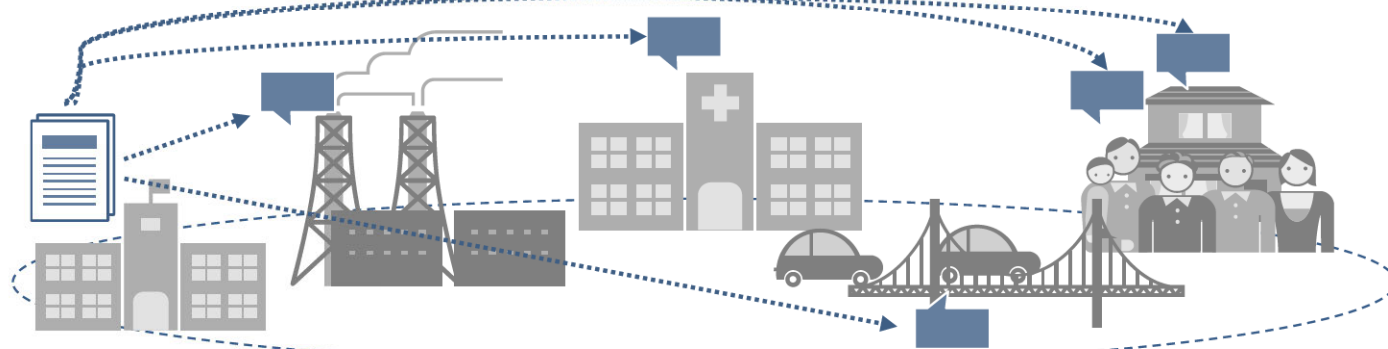


スマートシティにおける防災のあるべき姿（①価値提案）

- これまでは、自治体単位で地域防災計画が作られ、その上で都市機能・システム毎に防災対策が取られている。**自治体の計画と都市機能・システム、また都市機能・システム間での防災における連携や情報共有は限定的であった。**
- スマートシティにおいては、地域全体として備えるべき災害やリスクの情報が共有され、**防災における都市機能・システム間の影響の事前共有・把握**が期待される。さらに、各主体が求める防災を共有した上で、都市としてとるべき防災対策や**都市機能・システム間の互助等における主体間の連携**で、これまで望めなかった**高い水準での地域やその地域の住民・企業のレジリエンス向上**が期待される。

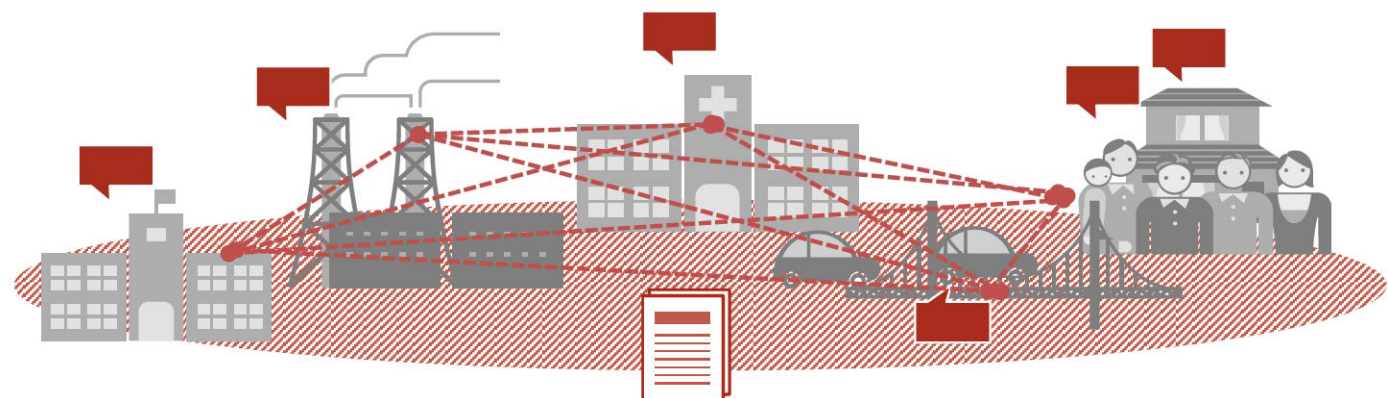
これまで

- 地域単位で地域防災計画等を策定
- 各事業者・個人で防災対策を実施
- 影響は各要素・システム間で干渉



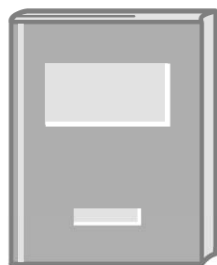
スマートシティ（SoS）

- 地域全体として備えるべき災害やリスクの情報を共有、互いに及ぼす影響をできる限り事前に把握
- 各主体の求める防災を共有し、地域として連携した防災対策を実施
- 有事にもそれぞれの被害状況を共有、地域全体で最適化

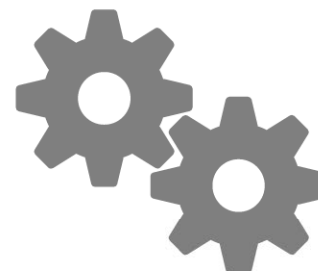


スマートシティにおける防災の日本の競争力（③競争力確保）

- SoSの一分野として、防災を日本が国際標準化し進めるメリットとして、**災害大国としての知見の蓄積、先進的な防災関連技術や取り組みを有しており、防災ブランドが国際的に認知されていることが挙げられる。**
- 東日本大震災の経験や、度重なる水害等の経験を多く有しており、様々な主体・場所で知見が蓄積されている。それらの知見は日本以外においても有効であるものも多い。
- 地震計や斜面防災技術等が以前より技術として存在しているが、昨今は**スマートシティ事業の一環で新たな防災技術・機能の開発・実証も進められている。**（参考に詳述）
- 仙台防災枠組みや日本に蓄積された知見をISO化することで、新しい技術なども共通の考えのもと導入ができ国際的な防災力向上が図られることが期待できる。現在、防災ISO化は日本が主導して開始されている。（参考に詳述）



- 災害の経験
- 仙台防災枠組
（防災ブランド）



- 地震計、斜面防災技術等
- スマートシティを通して開発・実証されている技術

防災の考え方・マネジメントと防災の技術を組み合わせることによって
「防災ソリューション」として日本の競争力をより発揮

(参考) 日本におけるスマートシティの防災の取り組み事例

- スマートシティの実証が様々な都市で行われており、その中で防災に関連する技術・機能も実証されている。
- 防災機能単体で検討されている場合が多いが、大手町・丸の内・有楽町地区での実証事業は、デジタルツインや都市OSを通じたデータ・機能間の連携等、SoSとしての都市をイメージした検討が行われている事例も存在する。
- 今後は、SoSとして振る舞う都市を前提とした防災の技術・機能の検討、またその検討を日本の競争力を活かしながら国際標準化することが、新たな社会の安全性確保及び日本の産業戦略としても重要である。

No	代表事例（スマートシティ関連事業）		参考URL
	自治体・地域・エリア	事業・プロジェクト名称、具体的な防災事業	
1	山口県宇部市	レジリエントで持続可能な社会を創る「スマートシティ宇部プロジェクト」 <防災意識を高めるスマート防災の推進> ・避難勧告時の携帯位置情報をAI分析し効果的に活用 ・自分事となる防災啓発効果の高いVR/AR教材を作成 ・ローカル 5 Gによる高度水害監視システムで4 Kカメラ・ドローン等の映像をリアルタイム伝送	https://www.mlit.go.jp/scpf/projects/docs/smartcityproject_co(1)%2031_ube.pdf
2	愛知県岡崎市	スマートシティ実現で増幅するエリアの引力 <浸水災害対策> ・外水、内水の水位把握と予測を、住民・来街者へ提供	https://www.mlit.go.jp/scpf/projects/docs/smartcityproject_mlit(2)%2012_okazaki.pdf
3	神奈川県横浜市	横浜みなとみらいスマートシティコンソーシアム <防災力・セキュリティ強化> (1) V P P 構築事業を展開し、災害時におけるエネルギーの確保を図るとともに、センサー等を設置し、災害時の被害リスクの予測と災害対応等に活用 ・V P P の構築、x E V 及び充放電器の普及 ・都市型浸水リスクの予測管理システムの導入 (2) 人流データ等を活用した災害発生時の効果的な避難誘導等の情報発信 ・デジタルサイネージを活用した緊急情報の発信 ・被災状況や負傷者搬送を俯瞰する「災害ダッシュボード」の活用 ・自動運転警備・清掃・運搬ロボット等の導入 ・MRデバイスの導入	https://www.mlit.go.jp/scpf/projects/docs/smartcityproject_mlit(2)%2006_minatomirai.pdf
4	東京都 大手町・丸の内・有楽町	大手町・丸の内・有楽町地区 スマートシティ推進事業 <レジリエンスの増強> ・災害ダッシュボード ・データライブラリ構築 ・都市OS構築	https://www.mlit.go.jp/scpf/projects/docs/smartcityproject_mlit(1)%2007_daimaruyu.pdf

(参考) スマートシティ関連規格に関する日本の動き

- 2020年11月、ISO/TC 268/SC 1/WG6（防災）が日本提案で設立。
「日本提案の防災フレームワークのTR開発」が進行中。
- 仙台防災枠組の趣旨に沿って、防災を推進させるための「防災ISO」の検討・開発を目指している。



出所) 今村文彦「防災ISO規格活動の開始 —防災イノベーションに向けて」, 産学官連携ジャーナル, 2020年9月
(https://www.jst.go.jp/tt/journal/journal_contents/2020/09/2009-03_article.html)、2021年3月25日閲覧

スマートシティにおける防災の基準策定（◎基準策定）

- 日本におけるスマートシティにおいて、防災の課題解決に資する技術実証等は進みつつある。
- 技術実証と並行し、防災の考え方・マネジメントについてもあわせて実証を行い、スマートシティの防災に求められるルール・基準等を官民で協調して検討をしていくことが有効である。
- そのルール・基準は、定性的な既存の規制文書のような内容のみならず、**APIの仕様等システムに求められる要件やアウトカムの測定等、サイバー空間におけるルール・基準**も検討されることが望ましい。システムに求められる要件は、国内外の既存システムとの連携なども見据え、可用性の高い形で検討されるべきである。
- あわせて、**ルール・基準への適合性の評価方法・体制**についても検討されるべきである。



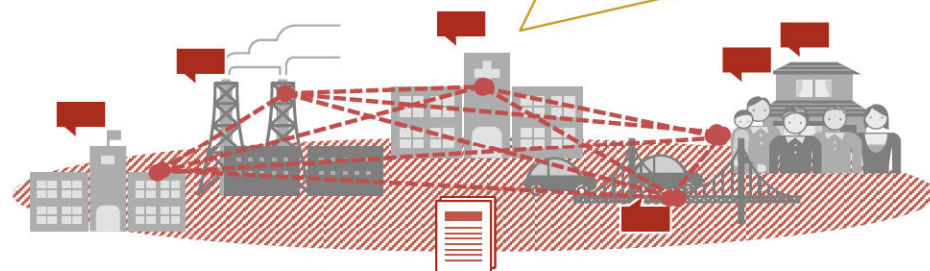
- 災害の経験
- 仙台防災枠組



- 地震計、斜面防災技術等
- スマートシティを通して開発・実証されている技術

破壊された平常時通信環境の中であって、発災時の都市に必要な機能・データの優先順位に応じて各システムが協調的に機能を再構築するしくみ

スマートシティの各機能との総合運用性等含めたスマートシティに求められる防災の検討・実証

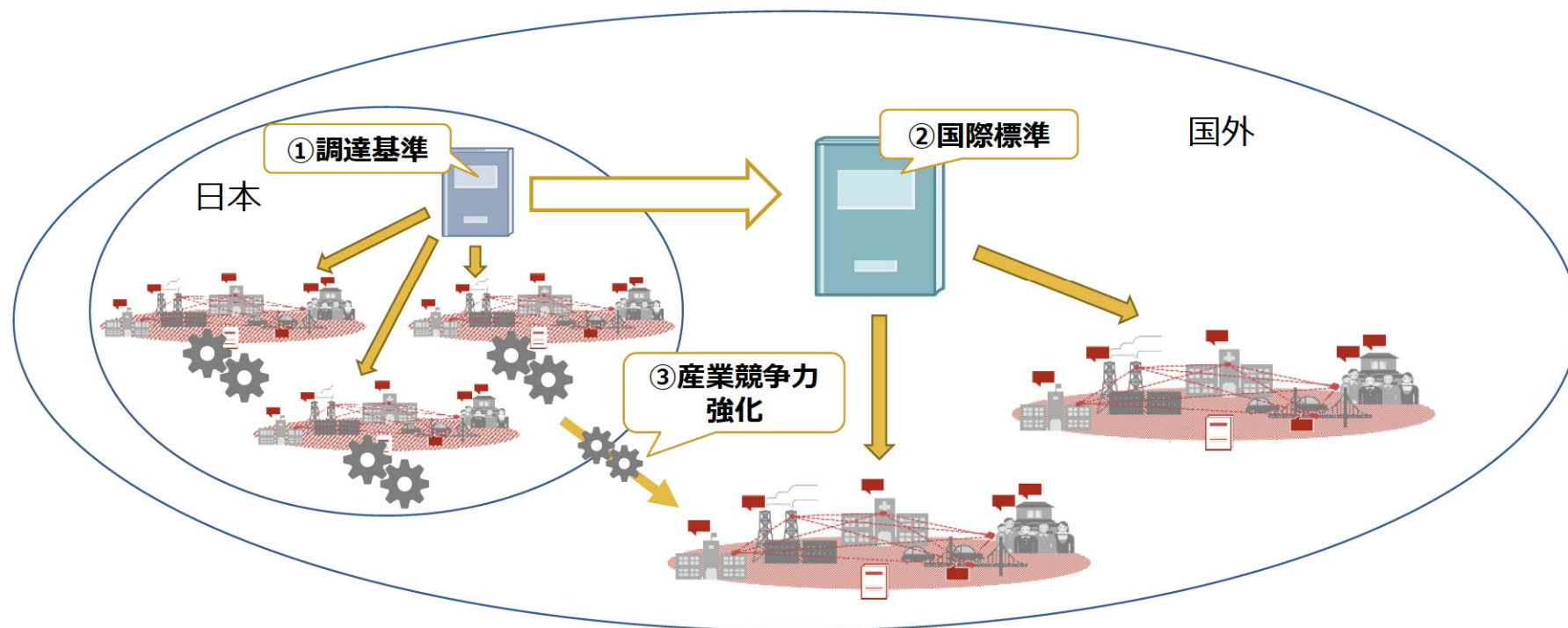


スマートシティの防災のルール・基準を官民連携で検討・策定



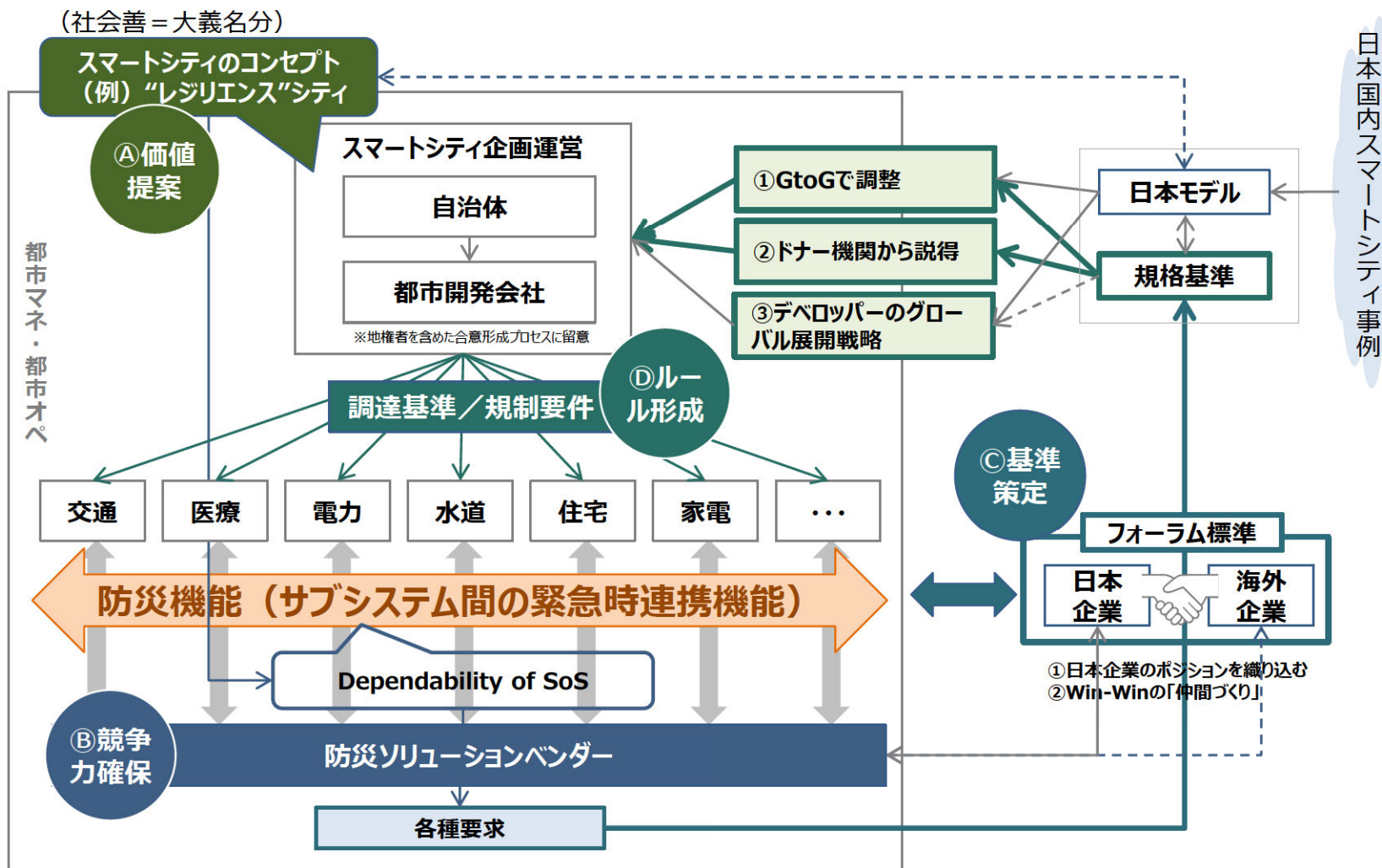
スマートシティにおける防災の国内外におけるルール形成（④ルール形成）

- スマートシティにおける防災のルール・基準は、まずもって**国内のスマートシティの調達基準**として設定することで、国内での普及を目指す。国内での普及により、各地の防災力向上とあわせて、技術の高度化もはかれることが期待される。
- 国外においても**国際標準化**を通して国際的な基準策定を行い、**国内外の都市システムにおける防災の調達基準**とすることを目指す。これにより、日本の防災の考え方・マネジメントと技術に基づいたスマートシティの防災を普及し、産業競争力の強化につながることを期待される。
- 国内外ともに、**ルール・基準への適合性の評価方法・体制**についても並行して整備されることが重要である。



SoSの典型例としてのスマートシティに関するルール形成戦略の考え方

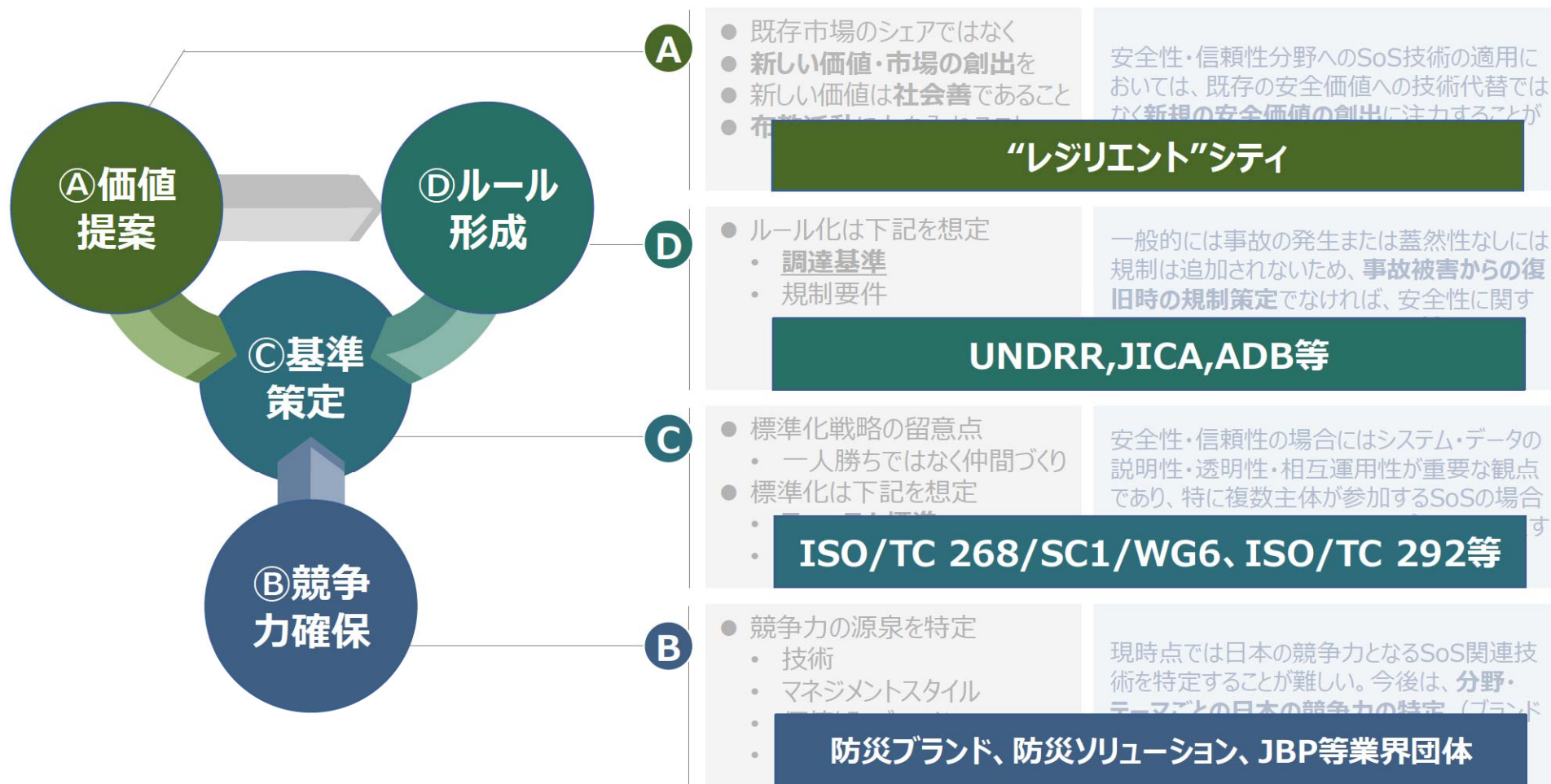
スマートシティにおいて防災レジリエンスの価値訴求を行うための標準化戦略のポイントを以下に整理する。



スマートシティにおいて防災レジリエンスの価値訴求を行うための標準化戦略のポイントを以下に整理する。

3. 2小括 防災分野のシステムオブシステムズでの価値化戦略

スマートシティにおいて防災レジリエンスの価値訴求を行うための標準化戦略のポイントを以下に整理する。



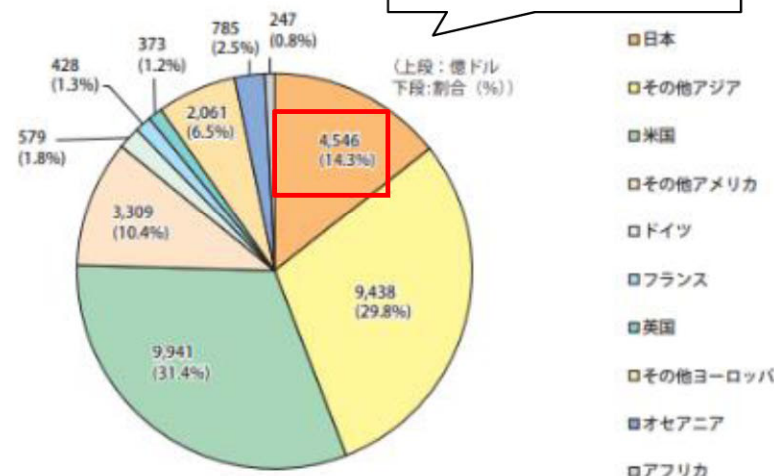
3. システムオブシステムズの安全性・信頼性の実現に向けた国際標準化戦略の検討

3. 3 国際標準等を活用したルール形成によって期待される経済的効果及びエネルギー効率化効果の調査

世界的な防災市場

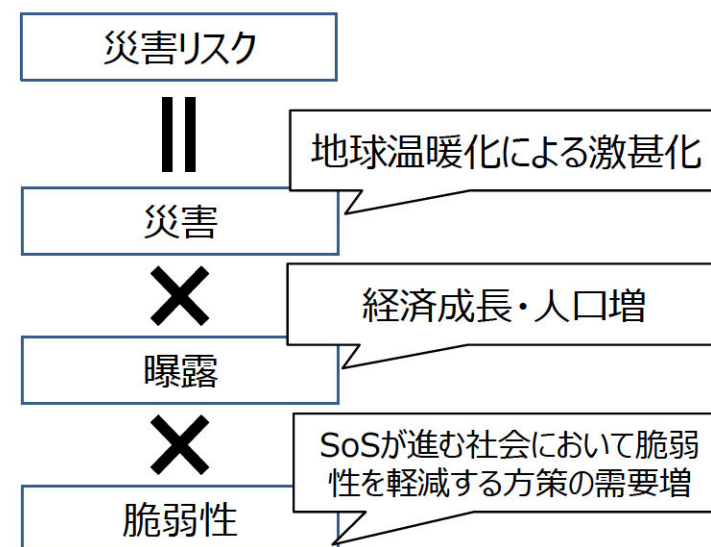
- 今後システムオブシステムズの実装が進むと思われる分野として「防災」分野を取り上げ、安全性・信頼性に関する国際標準等の国際ルールが策定された場合の経済的効果を算出した（建物・インフラなどへの影響を包含）。
- 日本は自然災害による被害が大きな国の一つであるが、世界における被害額のうち、日本の占める割合は約1/7である。アジアや米国、欧州等でも日本と同様にスマートシティにおける防災の標準化の需要は存在すると考えられる。
- また、アジア・アフリカ等、今後の経済成長や人口増が予想される地域では災害へのリスクの上昇も想定され、防災へのニーズの上昇が見込まれる。2011年のタイ洪水のように工業団地の浸水が日系企業に影響を与えるケースの被害軽減にもつながる。
- 地球温暖化による豪雨等災害リスクの増加も、設計外の規模の自然災害に対するレジリエンスが今後求められる理由の一つである。

第3-2-2図 世界における自然災害被害額と被害額の割合



資料：ルーバン・カトリック大学疫学研究所災害データベース（EM-DAT）より中小企業庁作成
 (注) 1. 1985年～2018年の自然災害による被害額を集計している。
 2. 2018年12月時点でのデータを用いて集計している。
 3. EM-DATでは「死者が10人以上」、「被災者が100人以上」、「緊急事態宣言の発令」、「国際救援の要請」のいずれかに該当する事象を「災害」として登録している。

災害リスクの今後の変化



スマートシティにおける防災の標準化による経済的利点

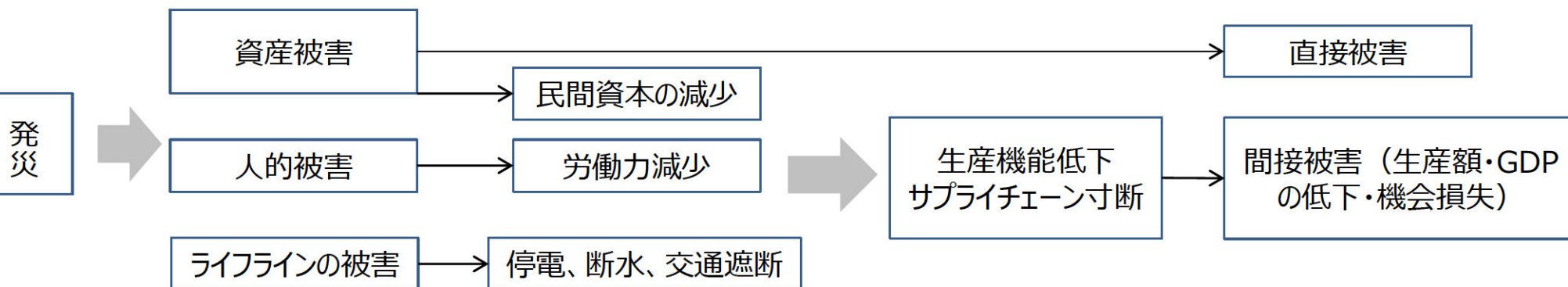
- スマートシティに防災の標準化を導入することにより、都市の防災システムとして**ステークホルダー間での情報共有**や**効果的な情報発信**が見込まれる。
- その結果、防災上の利点として**組織間の円滑な連携**や、リスク等情報の可視化による**意思決定の高度化**、適切な情報発信による**住民のリスク認知改善**等が可能となり、被災者の社会復帰や被災後の経済回復を早める効果（**レジリエンスの向上**）から**間接被害額の減少**が期待される。

スマートシティ（SoS）における防災システムが持つ機能

- ・ 地域全体として備えるべき災害やリスクの情報を共有、互いに及ぼす影響をできる限り事前に把握
- ・ 各主体の求める防災を共有し、地域として連携した防災対策を実施
- ・ 有事にもそれぞれの被害状況を共有、地域全体で最適化

レジリエンスの向上に資する事例

- ・ 避難者を適切に誘導し物資を分配することで、被害者の社会復帰が早まる。
- ・ SoS全体でリスクの特定、復旧作業の優先順位の把握が容易となり、ライフライン・交通インフラ等サブシステムの復旧が早まる。また、事業者の迅速な経営状態の回復も見込まれる。
- ・ 事前の準備によってシステム同士の繋がりに沿った被害の波及を最小限にとどめる。（接続先のエラーによるシステムの暴走防止等）



災害による経済被害の概要

出所）中央防災会議 首都直下地震対策検討ワーキンググループ「首都直下地震の被害想定項目及び手法の概要 ～経済的被害～」
http://www.bousai.go.jp/jishin/syuto/taisaku_wg/pdf/syuto_wg_keizai.pdf , 2021年3月24日閲覧

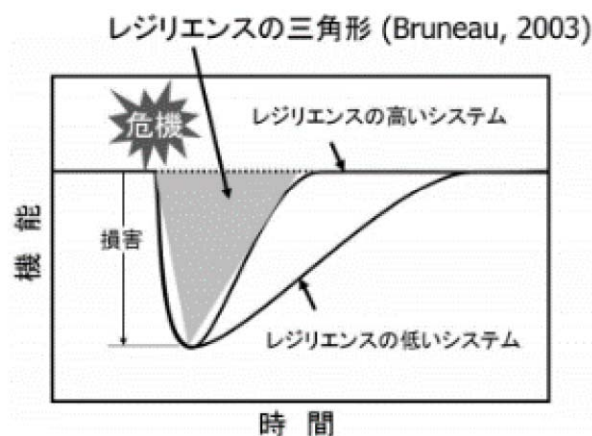
スマートシティにおける防災の経済被害軽減効果の試算①

- 防災分野におけるレジリエンスは左図のように表され、**損害からの回復が早い（レジリエンスの三角形が狭い）システムがレジリエンスの高いシステム**となる。
- 災害の間接被害の算出においても、縦軸を生産性とした同様のグラフ（右図）を用いて、生産額の減少分（レジリエンスの三角形の面積）を求める手法が用いられる場合がある。^{出所 1}
- 下記の計算における仮定の下で一年あたりの経済被害軽減効果を試算すると、**約4600億円**となった。

出所 1：損害保険料率算出機構、「巨大災害リスクに関する研究」, 第2章 東海地震の被害想定をベースとした間接被害額の算出例, 2003年7月,
https://www.giroj.or.jp/publication/earthquake_research/No04_2.pdf, 2021年3月24日閲覧

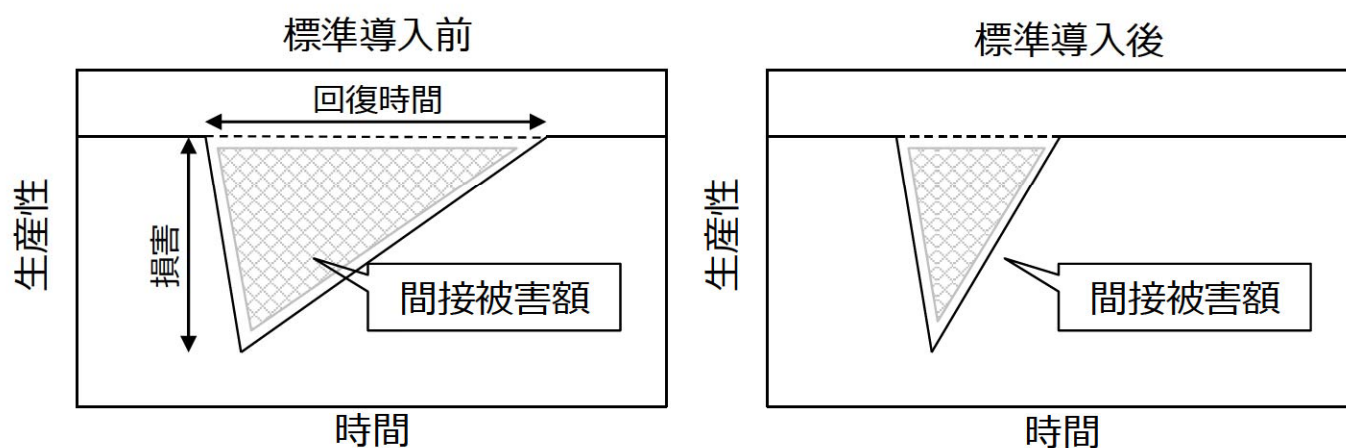
計算における仮定

- 防災の標準化では前スライドの通り回復力の向上が見込まれ、ここでは標準の普及により回復時間が1%減少すると仮定する。右図のように線形なレジリエンスカーブを仮定すると、最大の損害が同等の場合、間接被害額も回復時間と同様に1%減少する。被害軽減効果は全国一律とする。
- 今後30年における日本の主な災害を南海トラフ地震と首都直下地震とし、30年における一年あたりの経済被害軽減効果を試算する。



防災分野におけるレジリエンスカーブ

出所) 古田一雄 and 菅野太郎. "レジリエンス工学の誕生と展望." システム/制御/情報 60.1 (2016): 3-8.



スマートシティにおける防災の標準導入前後における間接被害額の変化

スマートシティにおける防災の経済被害軽減効果の試算②

- 防災分野におけるレジリエンスは左図のように表され、**損害からの回復が早い（レジリエンスの三角形が狭い）システムがレジリエンスの高いシステム**となる。
- 災害の間接被害の算出においても、縦軸を生産性とした同様のグラフ（右図）を用いて、生産額の減少分（レジリエンスの三角形の面積）を求める手法が用いられる場合がある。^{出所 1}
- 下記の計算における仮定の下で一年あたりの経済被害軽減効果を試算すると、**約4600億円**となった。

出所 1：損害保険料率算出機構,「巨大災害リスクに関する研究」,第2章 東海地震の被害想定をベースとした間接被害額の算出例, 2003年7月,
https://www.giroj.or.jp/publication/earthquake_research/No04_2.pdf, 2021年3月24日閲覧

計算式

$$（１年あたりの経済被害軽減効果）＝（想定間接被害額※１）×（標準化による軽減率※２）×（一年あたりの災害が生じる確率※３）$$

※ 1：土木学会レジリエンスの確保に関する技術検討委員会「『国難』をもたらす巨大災害対策についての技術検討報告書」^{出所 2}より、南海トラフ地震の間接被害額を1240兆円、南海トラフ地震の間接被害額を731兆円とした。

※ 2：上記仮定の通り、間接被害額が1%減少すると仮定し0.01を代入した。

※ 3：内閣府HP^{出所 3}より、両地震の30年以内の発生確率を70%として計算した。

出所 2：レジリエンスの確保に関する技術検討委員会,「『国難』をもたらす巨大災害対策についての技術検討報告書」,土木学会, 2018年6月7日,
<https://committees.jsce.or.jp/chair/node/21>, 2021年3月24日閲覧

出所 3：内閣府 防災情報のページ 地震災害, <http://www.bousai.go.jp/kyoiku/hokenkyousai/jishin.html>, 2021年3月24日閲覧

本節では、2章で検討した複数の分野①～③を包含する観点としての「防災」に着目した上で、国際標準等を活用したルール形成によって期待される経済的効果の推計を行った。

3. 3小括 防災分野のシステムオブシステムズでの効果試算

- スマートシティに防災の標準化を導入することにより、都市の防災システムとしてステークホルダー間での情報共有や効果的な情報発信が見込まれる。
- その結果、防災上の利点として組織間の円滑な連携や、リスク等情報の可視化による意思決定の高度化、適切な情報発信による住民のリスク認知改善等が可能となり、被災者の社会復帰や被災後の経済回復を早める効果（レジリエンスの向上）から間接被害額の減少が期待される。
- 一定の仮定の下で一年あたりの経済被害軽減効果を試算すると、**約4600億円**となった。

＜参考＞ 国際標準及び関連戦略により生じる経済的効果の例

機能安全規格ISO26262への準拠の有無で、開発ライフサイクルの「概念設計～システム設計」における設計作業工数を見積った実験によると、とあるシステム設計工程で合計で2.9 人月の作業が追加された一方、システム設計仕様書の不具合（16 件）が見過ごされ、後工程で発見されたと仮定した場合の作業工数の増加分は 3.5 人月と想定された。このように、安全関連規格の普及による開発工程全体の工数削減効果は一定程度あると想定される。

出所）IPA「ソフトウェア品質説明力の強化に伴い発生する開発工程負荷の評価・分析実施報告書」（2013年2月）
（<https://www.ipa.go.jp/files/000026866.pdf>）、2021年3月閲覧

4. 安全性・信頼性が担保されたシステムオブシステムズの実装に向けた提言

4. 安全性・信頼性が担保されたシステムオブシステムズの実装に向けた提言

まとめ①

● SoSの安全性・信頼性に関する国際標準化戦略の考え方

- ✓ 一般的に国際標準化戦略では、以下の4つの観点について**事前に計画**することが重要である。特にSoSの安全性・信頼性確保に関する技術の社会実装において重要なポイントについても合わせて以下に示す。

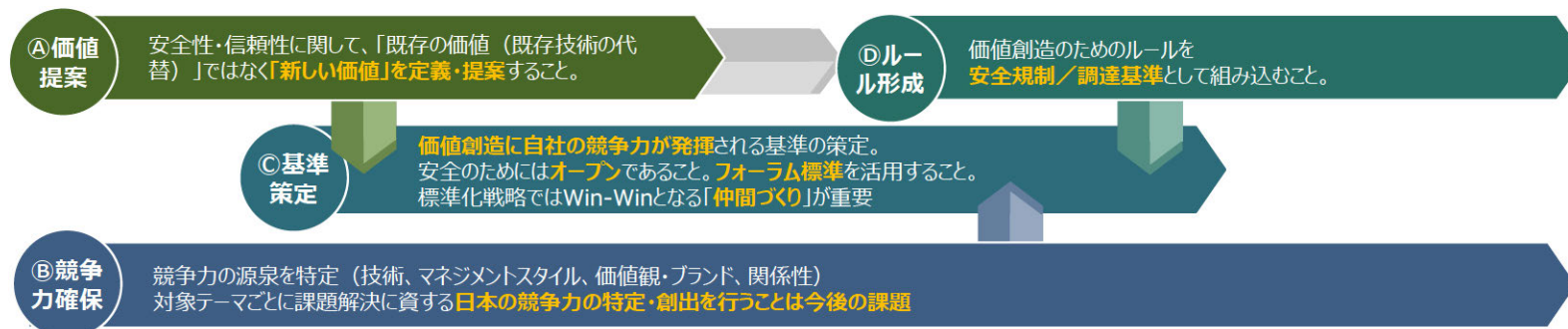
①**価値提案**：SoS技術は既存の安全性・信頼性の価値における技術代替よりはむしろ**新たな安全性・信頼性の価値創出・市場創造を行う**ことが効果的と考えられる。また、他者を巻きこむルール形成も見据えた場合には提案される価値は「**社会善**」である必要がある。

②**競争力確保**：技術調査の結果によると、現時点では日本の競争力となるSoS関連技術を特定することが難しい。今後は、**産業界のグローバルマインドの醸成**及び国の支援が必要である。

③**基準策定**：特に安全性・信頼性の分野においては**オープン化**が重要であり、且つ複数のステークホルダーが関連するSoS分野においては**フォーラム標準**による国際標準化（**仲間づくり**）が必要である。

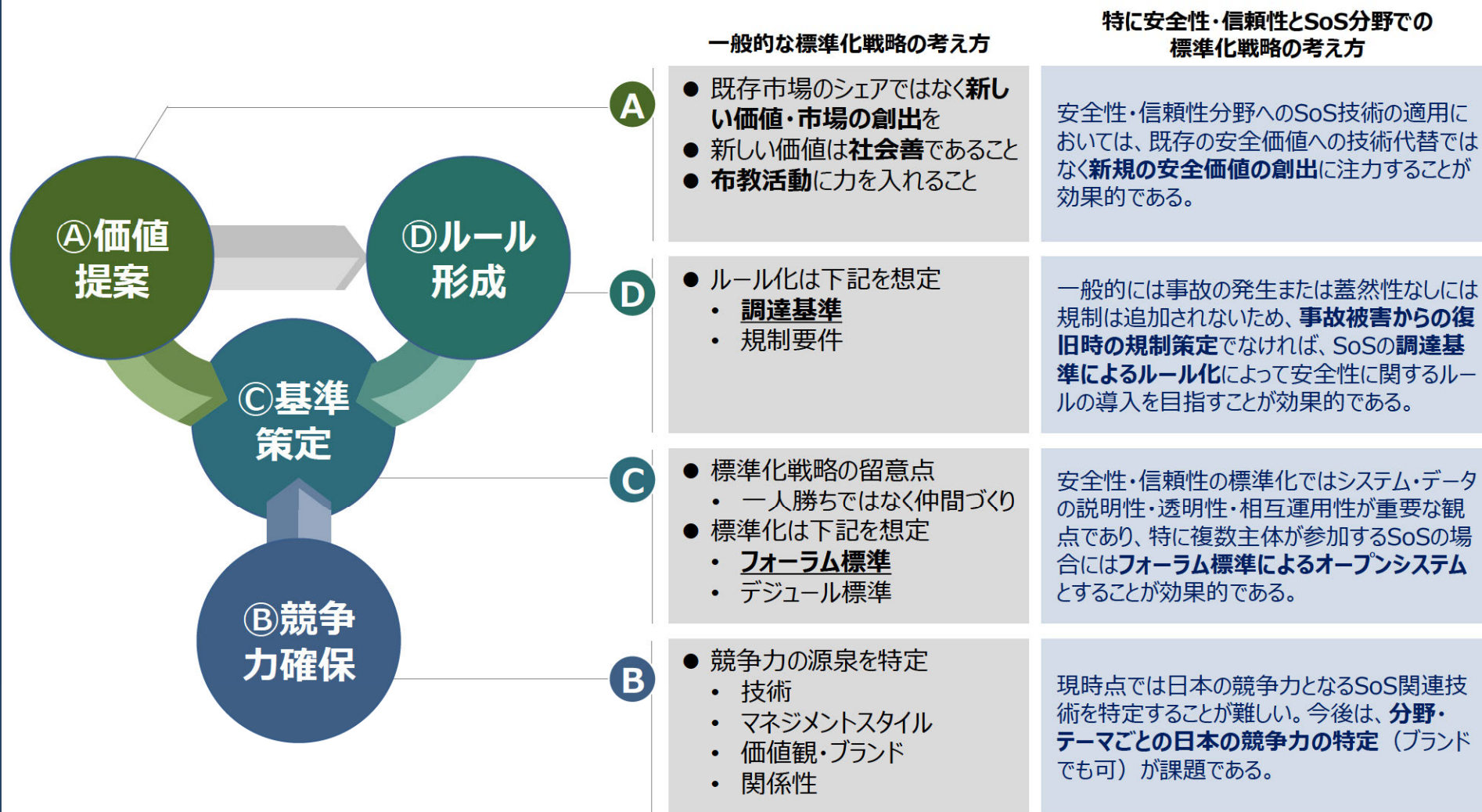
④**ルール形成**：基本的にはルールを「**調達基準**」に組み込むことが必要である。例えばスマートシティであれば都市計画にドナー機関・標準化機関等を巻き込んだ働きかけが効果的であると考えられる。

- ✓ 産業力向上の戦略としては**課題特定や基準策定だけでは不十分**である。特に日本企業においては、①価値提案・④ルール形成、②競争力確保にも留意した上で、十分な経営資源を振り向けることが必要である。



まとめ②

- SoSの安全性・信頼性に関する**国際標準化戦略の考え方**を以下に示す。



まとめ③

● SoSの安全性・信頼性に関する**技術開発の考え方**

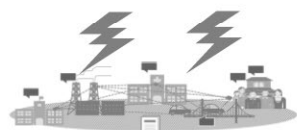
- ✓ 安全性・信頼性とSoS分野の国際標準化戦略テーマ案として、下記①～③の3テーマを前出のロードマップと共に提案する。ただしこれらのテーマについては、具体的な競争力の特定及びルール化戦略（ステークホルダーの特定）が課題であり、今後は日本産業の「競争力」としてこれらの**技術実証を行いつつ**、安全性・信頼性に関する**新しい価値提案・市場創出**を行っていくことが期待される。

①「モビリティとヘルスケア」

②「IoTホーム」

③「HCD」

- ✓ また、①～③の社会実装の基盤となるスマートシティとも親和性が高く、日本が競争力を有すると考えられる「防災」をテーマ④として追加した。

	①ヘルス&モビリティ	②IoTホーム	③HCD	④防災
特徴	モビリティとヘルスシステムという二つの独立なサブシステム間での協調的な安全性・信頼性の実現	家庭に導入される様々な住宅・家電システム等のサブシステム間での協調的な安全性・信頼性の実現	人間の属人的な特徴のばらつきによる意図しない安全性低下・信頼性低下の防止のためのしくみ	社会に導入されている様々なサブシステム間における、災害時の協調・連携のための機能
イメージ図				
④価値提案	ヘルスシティ/シルバーシティ	安全な住まい	多様性・ダイバーシティ・人権	レジリエント
④ルール形成 ④ステークホルダー	スマートシティ調達基準 デベロッパー	製品のマーク制度 メーカー（住宅、家電、..）	（SDG's、国連）	スマートシティ調達基準、デベロッパー、JICA、ADB、UNDRR、JBP等
④標準策定	標準化	ISO26262, ISO/DIS21448 IEC62853	IEC 63168、(IoT住宅版SOTIF) IEC62853	ISO 13407, ISO9241シリーズ IEC62853
④競争力確保	競争力	今後技術実証	今後技術実証	ソリューションリストから選定

まとめ④

● SoSの安全性・信頼性に関する**技術開発の考え方**

- ✓ 具体的に競争力のある技術を開発するためには、個社企業が国際標準化戦略等に対して十分な経営資源を振り向けることが重要である。また、技術調査においてグラント→論文→特許の順で競争力が具現化されている実態を考慮すると、国の中長期的な産業戦略も合わせて必要と考えられる。

③競争力確保

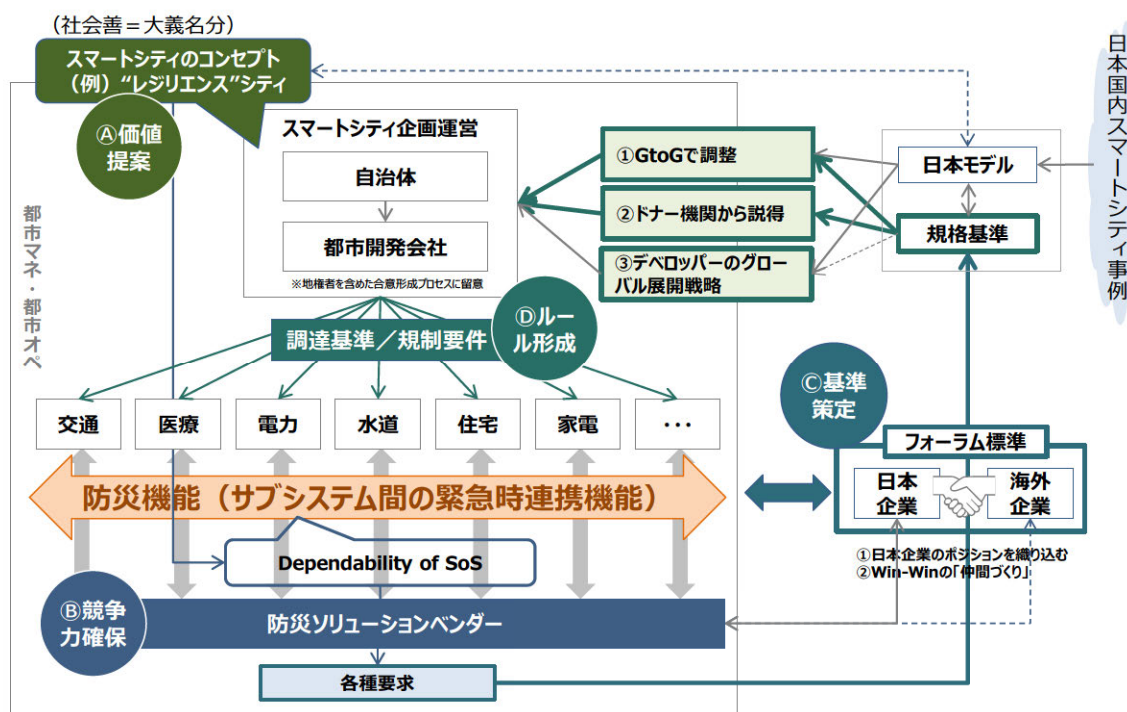
システム

コンポーネント

課題	概要	解決策（技術）	解決策（マネジメント）	【参考】分野事例
①全体リスク想定 の困難性	- 個別システムの安全の積み上げではSoS全体の安全を確保するのは困難 - 外部環境の動的なシステムと接続される場合、予期できなかった新たな危険性が発生する可能性		A SOTIF B STAMP C FRAM ①安全要求定義／安全性解析	
②運用時の変化 対応の困難性	システム構成の変更や動作目的の変更によるリスクの事前想定は困難であるため、運用段階（ライフサイクル全体）での安全担保が必要	②リアルタイムテスト技術 ③モジュラー化 ⑤ロバスト制御 ⑥システムレジリエンス		
③運用時の障害 対応の困難性	- システム複雑化に伴いシステム障害の把握とその原因追求が困難 - 障害検知や安全状態への移行に関する時間や責任が曖昧		④DEOSプロセス	
④ユーザ・ユース ケース想定 の困難性	- SoSにおける危険の許容「許された危険」の法規的な扱い方が不明確 - ステークホルダごとのメンタルモデルギャップ（リスク）の増大への対応が必要	⑧ヒューマンファクター	⑤HCD	④サービスロボット JIS Y1001等
⑤AIの挙動の 不確実性	AIの不確実性への対応はSoSになるとさらに課題として顕在化	⑦ホワイトボックス化	⑥DSM	
⑥サイバー攻撃 への対処	サイバー攻撃への対処はSoSになるとさらに課題として顕在化	④攻撃防御モデル	③CPSF	⑦自動運転 Pegasus Project

まとめ⑤

- スマートシティを対象とした場合の**標準化戦略の具体的なアクションイメージ**を以下に示す。
- ✓ 「防災」の分野は、それ自体が社会善となる新たな安全性・信頼性の価値であり、**スマートシティのデベロッパー・地権者・ドナー機関等と共に調達基準の開発**を行うことで、システムオブシステムズにおける安全性・信頼性のしゅみを社会実装することが可能となる。特に今後は、**日本の「防災ブランド」を競争力**としながら、より具体的なステークホルダーによる体制の組成と基準化（国際標準化）の取り組みを推進することが期待される。



令和2年度省エネルギー等に関する国際標準の獲得・普及促進事業
(国際ルールインテリジェンスに関する調査(システムオブシステムズの安全性・信頼性確保))
報告書

2021年3月



株式会社三菱総合研究所
東京都千代田区永田町二丁目10番3号
☎080-6771-9258



一般社団法人 ディペンダビリティ技術推進協会
京都市中京区烏丸通二条上ル蒔絵屋町280
☎075-213-7075



アスタミューゼ株式会社
東京都千代田区神田小川町3丁目9-2 BIZCORE神保町4F
☎03-5148-7181

令和2年度省エネルギー等に関する国際標準の獲得・普及促進事業
(国際ルールインテリジェンスに関する調査 (システムオブシステムズの安全性・信頼性確保))

添付資料 1 システムオブシステムズに関する補足資料

令和3年3月31日

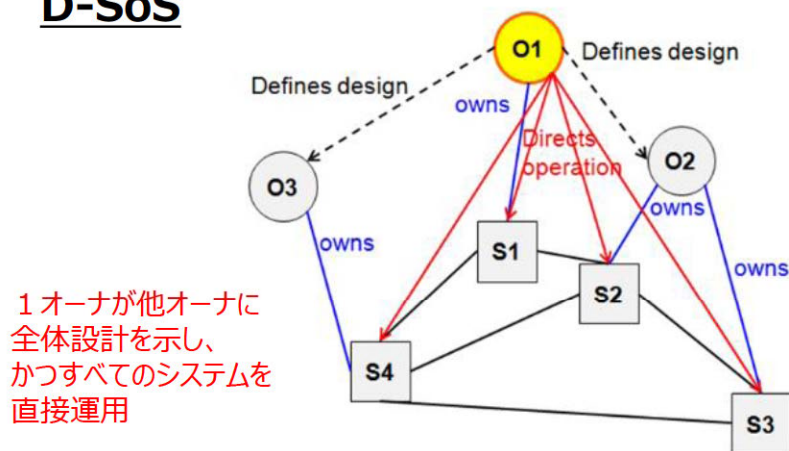
付録：システムオブシステムズ（SoS）の定義（学術的な原型）

出典	定義
Mark W. Maier、 Architecting Principles for Systems-of- Systems、(1998)	以下の5つの特徴をもったシステムをSystem of Systems (SoS)と呼ぶ。 1. 運用の独立性: SoSの構成システムは個別に運用 2. 管理の独立性: 構成システムは別々に調達され、統合される。しかし、運用中の構成システムはそのまま運用 3. 進化的開発: 機能や目的が、追加/削除されたり途中で変更されるなど、開発とシステムが進化的に変化 4. 創発的振る舞い: 構成システム単独では実現できない目的をSoSとして実現 5. 地理的な分散: 構成システムが離れており、構成システム間で質量やエネルギーの物理量ではなく、情報を交換 SoSでないSystemを“Monolithic System”と呼ぶ。（本報告書ではM-Sysと標記）

参考：学術論文で示されているSoSの例

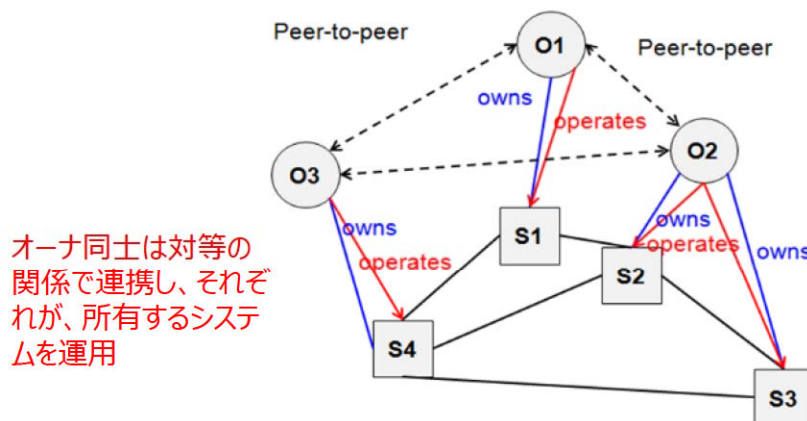
O: System owner、S: System

D-SoS



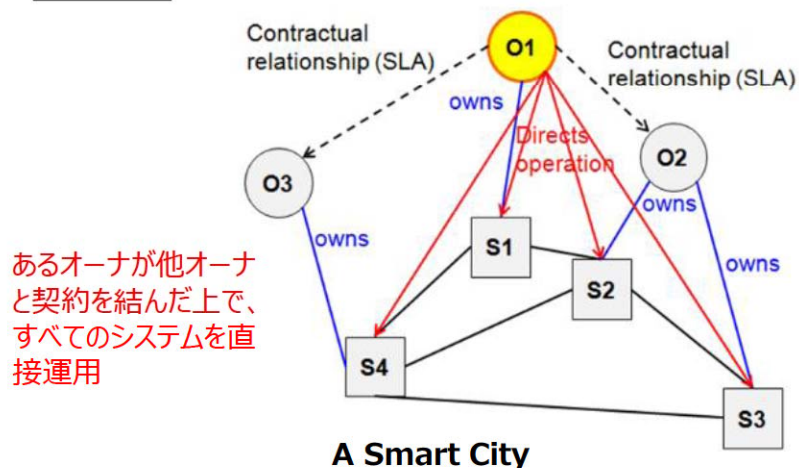
NexGen – US Air Traffic Management System

C-SoS



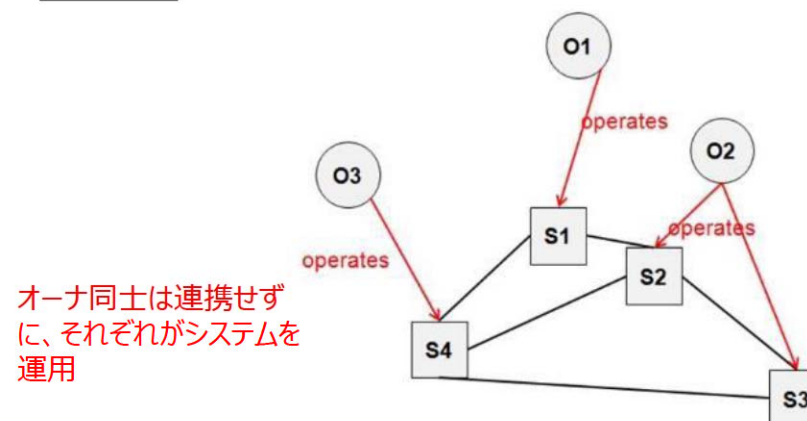
The Global Financial System

A-SoS



A Smart City

V-SoS



A Crisis Management System

出所) C. Ncube et al., "On Systems of Systems Engineering: a Requirements Engineering Perspective and Research Agenda", IEEE 26th International Requirements Engineering Conference, 2018

Safety 関係の用語定義

規格	safety	functional safety
ISO/IEC Guide 51 : 2014	freedom from risk which is not tolerable	-
IEC 61508 : 1998	freedom from unacceptable risk	part of the overall safety relating to the EUC* and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems、 other technology safety-related systems and external risk reduction facilities 被制御装置とその制御システムに関する安全のうち、電気・電子・プログラマブル安全関連系、他技術の安全関連系、外部のリスク低減装置の正常機能に依存する部分
ISO 26262 : 2018	absence of unreasonable risk	absence of unreasonable risk due to hazards caused by malfunctioning behaviour of E/E systems <u>電気・電子システムの機能不全時の動作に起因するハザード</u> による不合理なリスクがないこと

システム＝モノを前提とした定義になっている
→ヒトを含むシステムを扱いたい

Dependability の用語定義

規格	用語	定義
JIS Z 8115:2019	総合信頼性 (Dependability)	アイテムが、要求されたときに、その要求どおりに遂行するための能力。アベイラビリティ、信頼性、回復性、保全性、及び保全支援性能を含む。適用によっては、耐久性、安全性及びセキュリティのような他の特性を含むことがある。

Open Systems Dependability

規格	用語	定義
JIS C 62853:2 020	オープンシステム、開放系 (open system)	その境界、機能及び構造が時間とともに変化し、様々な視点に応じて異なった認識及び記述のされ方を するシステム 注釈1 システムの変化には、特定の目的をもった適応だけでなく、自然発生的な進化も含まれる。例えば、 管轄の異なる複数の領域にまたが（跨）るシステムの内部における、自然発生的かつ非協調的なものが 含まれる。 注釈2 オープンシステムの境界、機能及び構造は時間とともに変化するだけでなく、どの時点においても曖 昧で、異なる利害関係者によって異なって認識され得る。オープンシステムの定義は、所与の抽象レベル及 び視点に対するJIS Z 8115におけるシステムの定義を精緻化するものである。ある抽象レベルでは明確に 定義可能な境界も、より詳細なレベルではより曖昧になり得る。ある目的に対して、又はある利害関係者 にとって、どのレベルの詳細さが必要となるかは、あらかじめ定めることが可能であるとは限らず、そのレベルの 詳細さを得られるという保証もない。 注釈3 オープンシステムは、他のシステム又は環境と境界とをまたが（跨）ってリソースを交換する。場合に よっては境界自体を変化させる。 注釈4 相当規模のシステムであれば、必ずオープンシステムとしての側面及び従来型システムとしての側面 の両側面をもつ。オープンシステムという用語はシステムの分類には用いられない。この用語がシステムに 適用されるのは、そのシステムのオープンな側面がシステムの課題検討において重要な意味をもつときで ある。 注釈5 ソフトウェアシステムは、“オープンソース”であり得るが、それはそのシステムがオープンシステムである かどうかとは関係がない。ただし、オープンソースソフトウェアであることは、権限の一元化に欠けるなどのオープ ンシステムの側面を必然的にもたらす。
	開放系総合信頼性 (open systems dependability)	期待されるサービスを要求されたときに要求されたように提供するために、目的、目標、環境及び実際のパ フォーマンスの変化に対応し、説明責任を継続的に果たす能力 注釈 1 : パフォーマンスの意味には、実施、実績、性能、能力及び動作様態が含まれる。

人を含むシステムが掲げるゴールの例

用語	定義	文献
レジリエンス (resilience)	一般：困難や良くないことが発生した後に、再び幸福、成功などになる能力。歪んだり、伸ばしたり、押されたりした後に、もとの形状に戻ろうとする能力 (Cambridge Dictionary) ビジネス：ビジネス機会、需要、混乱、脅威などの内的あるいは外的な変動に迅速に適応・応答し、その影響を限定的にとどめて事業継続する能力([1]) 生態学：生態系が変化や擾乱（じょうらん）を吸収して生物の個体数など諸変数の関係を維持する能力([1]) 工学：外乱や外圧に対するシステムの回復力([1])	[1]レジリエンス工学の誕生と展望： https://www.jstage.jst.go.jp/article/isciesci/60/1/60_3/_pdf/-char/ja
Positive Risk Balance	自動運転車によって、交通参加者の残存リスクが、より低減されることによるリスクベネフィット評価の結果。つまり、リスクは残るものの、最終的に、人間の能力と比較して社会的な被害が減ること(社会にとってプラス)を目指す考え方。	SaFAD (SAFETY FIRST FOR AUTOMATED DRIVING)

参考：対象システムの特性に対する既存概念の適用可能範囲（広めに捉える）

安全確保の考え方 システムの特性		これまでの安全規格 Guide 51 機能安全規格	Safety 2.0 (tripartite system)	SOTIF規格 自動運転 ISO 21448	開放系の総合信頼性 IEC 62853 ※安全確保方法論は 他規格と連携
境界、機能、 構造の変化	知識、リスク、 説明の網羅性				
Fixed/ Closed	Well-known	○	○	○	○
Fixed/ Closed	Unknown		△ (AI) ?	○	○
Flexible/ Opened	Well-known		○		○
Flexible/ Opened	Unknown		?		○

※Safety 2.0とは？

人、機械、環境の3者に注目し、互いに連携しながら安全を確保する考え方（Collaborative safety）。3者それぞれ変化し、3者と外部との境界も変化しうるが、それらの関係性は完全に明確化できることが前提。安全の基本的な考え方を規定するGuide 51を拡張する。

参考文献：IEC white paper、“Safety in the future”、2020.11

<https://etech.iec.ch/issue/2020-06/iec-publishes-white-paper-on-safety-20>

参考：SoSの分類と既存概念（主な適用範囲）との対応関係（提案）

システムの構造→ ↓システムの特性		単一System (M-Sys)	System of Systems			
境界 機能 構造	知識 リスク 説明性		Directed (D-SoS)	Acknowledged (A-SoS)	Collaborative (C-SoS)	Virtual (V-SoS)
Fixed/ Closed	Well-known	これまでの安全規格				
Fixed/ Closed	Unknown	SOTIF規格（自動運転） ISO 21443		既存の安全に関する考え方 + IEC 62853 をベースに 課題を整理し、適用可能性を検討		
Flexible/ Opened	Well-known					
Flexible/ Opened	Unknown	IEC 62853				
SoS関連規格 ISO/IEC/IEEE 21840:2019		ISO/IEC/IEEE 15288	ISO/IEC/IEEE 21839:2019 SoS considerations for systems ISO/IEC/IEEE 21841:2019 SoS considerations			

参考：M-Sys/D-SoSとA/C-SoSによるサービス実現の特徴

	M-Sys/D-SoS	A/C-SoS
人（特にサービス利用者）	- サービス提供者とその責任範囲が明確 - システム全体が完成するまで提供されない - 複数のサービスを柔軟に組み合わせることが難しい	（品質は今ひとつかも知れないが）動くサービスからどんどん提供していく - 必要なサービスを柔軟に連携 - 利用するサービスによって、品質や価格等の違いが生まれやすい
システム開発者（安全確保）	- サービスと責任範囲が明確なので、安全や品質を確保しやすい - システム全体が完全に設計されて完成するまでサービスを提供できない - システムが複雑化してくると、全体の品質担保が困難に - システムの部分的な改修が難しい（もしくは、部分的な改修を事前に想定した仕組みが必要）	（品質は今ひとつかも知れないが）動くサービスからどんどん提供できる - システムの部分的な改修は容易 - 全体の品質を均等にしたり、高いレベルでの品質を担保するのは難しい（方法論が研究されている）
システム管理者（ルール・ガバナンス）	- ガバナンスを維持、改善する仕組み自体は考えやすく、構築しやすい - 全体管理の負荷は高い - ルール改訂に時間が掛かる	- 迅速なルール改訂が可能 - 全体を統括する仕組みがないので、ルールの矛盾を見つけて、一貫性を保つような運用時の仕組みが必要

Society 5.0では、A/C-SoSによる柔軟で高速なサービス提供が必須となるので、早急に（安全性を含む）品質確保のための手法を確立すべきである

令和2年度省エネルギー等に関する国際標準の獲得・普及促進事業
(国際ルールインテリジェンスに関する調査 (システムオブシステムズの安全性・信頼性確保))

添付資料 2

システムオブシステムズの安全性・信頼性担保に関する技術調査

令和3年3月31日



システムオブシステムズの 安全性・信頼性担保に関する技術調査

2021年3月17日

asta**muse**
c o m p a n y

アスタミューゼ株式会社
東京都千代田区神田小川町3丁目9-2
BIZCORE神保町4F
TEL : 03-5148-7181 (代表)

プロジェクト全体像	．．．	2
1. 網羅的な情報収集による全体感把握と対象技術定義	．．．	5
2. 技術の定量評価や投資額動向の整理	．．．	15
3. 技術キーワードの共起分析結果からみるトレンドの把握	．．．	41
4. 各領域の研究開発・実装状況の具体的調査	．．．	50
Appendix	．．．	86

- 本プロジェクトではシステムオブシステムズの安全性・信頼性担保に関する技術調査を行うことで、システムオブシステムズにおける一般的な課題解決の方向性を示すことを目的とした
- 調査にあたっては、弊社特許・論文・グラントデータベースから技術キーワードを抽出の上、大きく8領域に構造化を行った
- グラント配賦額から見える中長期的な投資額と、ベンチャービジネスの調達額から見える短期的な投資額を総合的に鑑みると、安全要求定義／安全性解析は勿論のこと、「運用時のシステムの変化」に対して対応する技術に投資が集まっており、これらの技術については今後の課題解決の方向性に資する技術である
- また、安全要求定義／安全性解析の中の概念でも、safetyとsecurityについては近年特許でも急速に共起で現れている用語であり、今後はsecurityだけでなくsafetyの概念も含めた社会実装が期待される

以下の手順で技術調査を進める

1

網羅的な情報収集 による全体感把握と 対象技術の定義

- システムオブシステムズ関連の研究動向調査（特許、論文、グラント）を実施し、研究要素のキーワードを抽出
- コアとなる技術・概念をブレイクダウンし構造化することによって同領域を俯瞰

2

技術の定量評価や 投資額動向等より 重要領域・技術を特定

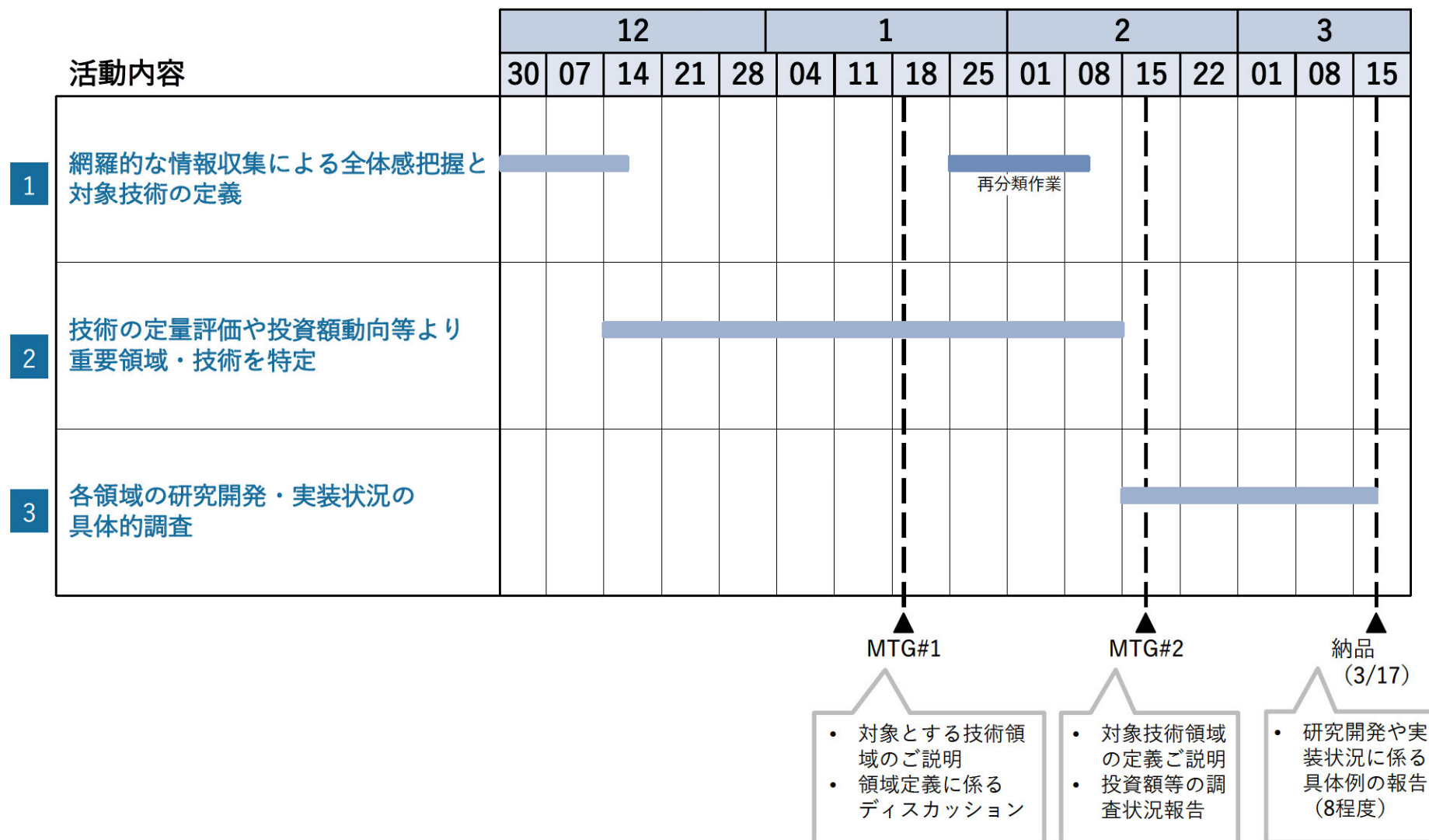
- 1にて俯瞰した領域ごとに特許、論文、グラントのスコアリングを実施し、技術の定量評価を実施
- 併せて、ベンチャー投資額、ベンチャー設立動向等を整理することで領域ごとの市場の期待値・可能性を整理
- 上記動向、及び領域における日本の競争力を踏まえ、特に重要と想定される技術を特定
※重要とすべき技術・概念に関しては要議論

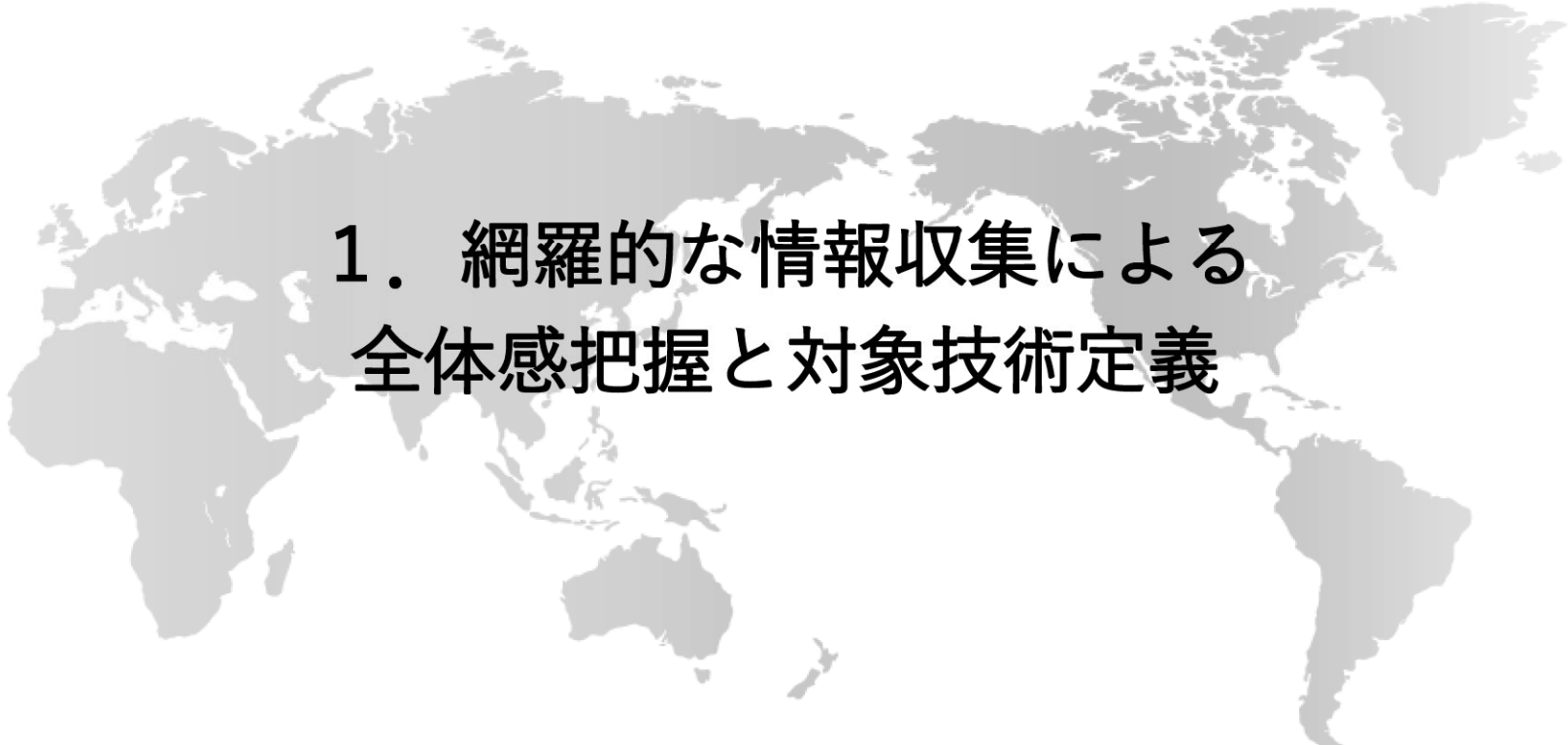
3

各領域の研究開発・ 実装状況の具体的 調査

- 2にて特定した重要技術・概念に関する具体的な研究開発状況・動向や実装状況を調査・整理
- 場合によっては当該研究者・有識者に対するヒアリング等を実施

調査スケジュールは以下の通り





1. 網羅的な情報収集による 全体感把握と対象技術定義

1 羅的な情報収集による全体感把握と対象技術の定義

システムオブシステムズの安全性・信頼性担保に資する技術・概念につき、各種ソースを活用し研究動向を把握した上で、関連要素のKWを抽出する

研究動向調査アプローチ



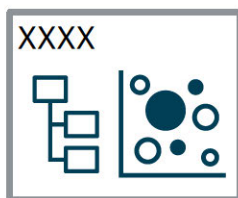
グラント・論文

- 研究投資総額から、注目すべき領域を把握
- 論文についても、引用数の多いものを中心に調査



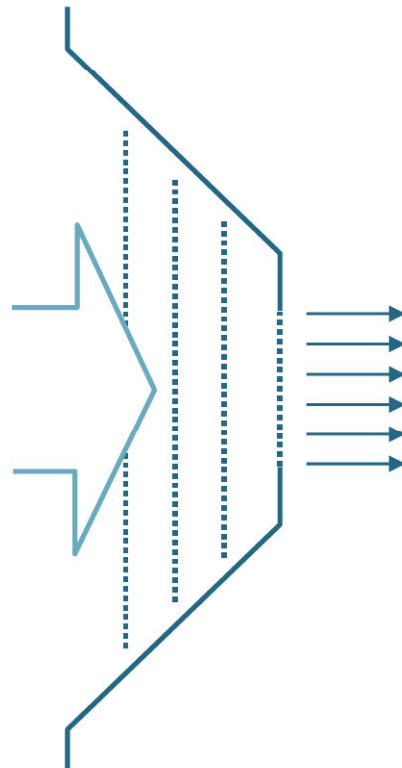
特許

- アスタミューゼ独自のロジックに於いて評価の高い特許をピックアップ
- 実用化を見据えた技術活用について、理解を深める



研究展望資料

- 各国の動向がマクロ視点で追える一覧性の高い報告資料なども、全体感把握に活用



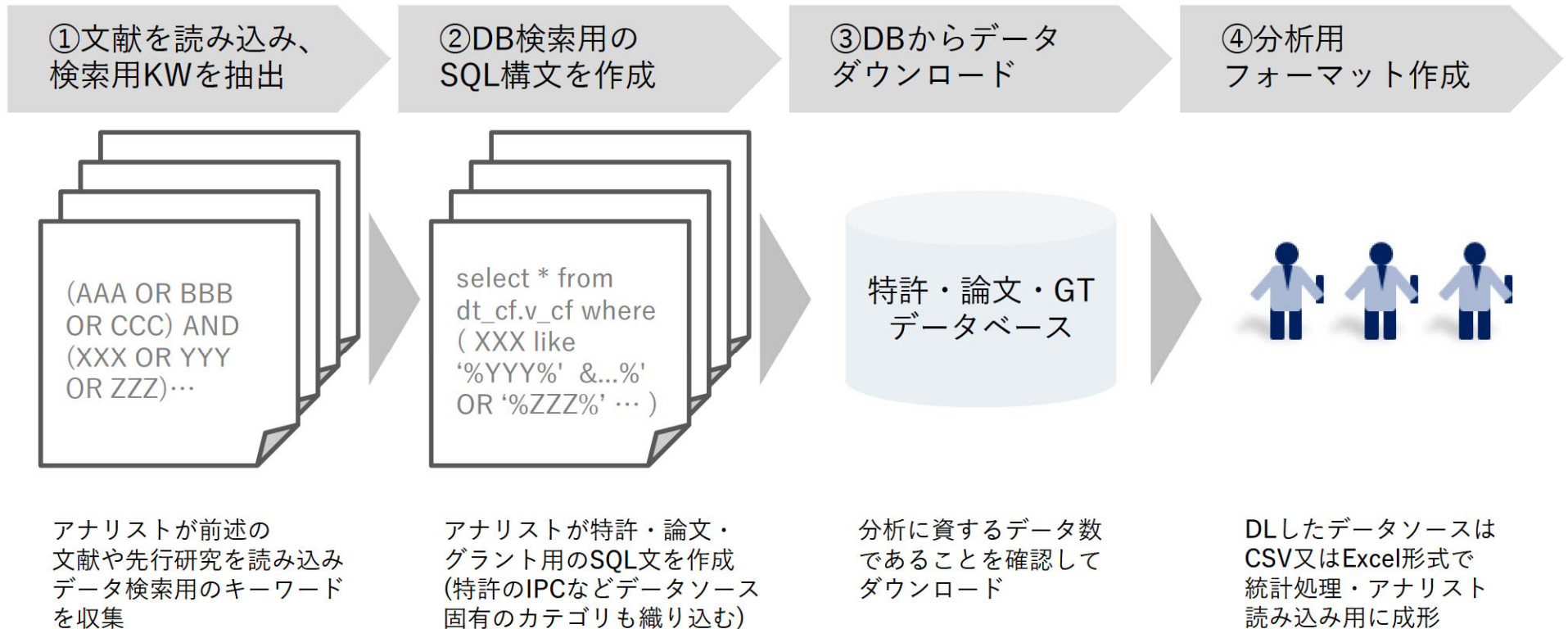
技術ワードの棚卸し (イメージ)

- 統合監視技術
- 認証技術
- XXX
- XXX
- XXX
- XXX
- XXX
- XXX...

1 体系的な情報収集による全体感把握と対象技術の定義

弊社DBに格納されている英訳済みの特許・論文・グラントデータに対して、対象技術の検索式を作成し、SQLで分析対象データを取得する

特許・論文・グラント母集団作成手順



KWから母集団を作成。後続分析対象とする各データソースの母集団は以下の通り

母集団の概要

	特許	論文	グラント
対象年度	2000～2020年出願	2000～2020年発表	2000～2020年に開始された研究
取得対象	Global (JP/EP/US/WO/CN等)	Global ^{*1}	Global (26カ国/35機関)
取得件数	3,567件	2,770件	1,388件
スコアリング基準日	2021/4/1		

*1 論文についてはMicrosoft Academic, CrossRef, PubMed等主要データソースをカバー

1 網羅的な情報収集による全体感把握と対象技術の定義

システムオブシステムズの安全性・信頼性担保における課題（調査ポイント）から研究領域を構造化し、8つの分野を設定した

システムオブシステムズ関連の研究領域構造化

大分類	1 システム全体のリスクの 想定困難性	2 運用時のシステムの 変化への対応困難性	3 AIによる 判断の妥当性
	1 安全要求定義／安全性解析技術 2 リアルタイムテスト技術 8 ヒューマンファクターの考慮*	3 モジュール化技術 4 攻撃防御モデル技術 5 ロバスト制御技術 6 システムレジリエンス技術	7 ホワイトボックス型AI技術
中分類			

* 分析母集団としては①安全要求定義／安全性解析技術に含めている

1 網羅的な情報収集による全体感把握と対象技術の定義

各領域の概要及び具体例は以下の通り。安全要求定義／安全性解析技術に含めて考えていたヒューマンファクターの考慮についても分析を行う

1 システム全体のリスクの想定の困難性

概要

具体例

1

安全要求定義
／安全性解析
技術

- システム同士の故障許容設計や故障伝播抑制設計、複数の専門家の連携などの技術が含まれる
- システムオブシステムズでは、複雑にシステムが絡み合い大きなシステムを構成しており、故障の社会的な影響も大きいことから、安全を確保するため以下のような技術が存在
 - あるサブシステムの故障が他のサブシステムに影響しないよう、分離した制御設計
 - 複数の専門家による依存関係の明示化・整合性確保が必要な項目の明確化
 - STAMP/STPAやFTAなど確立された手法の適用から、新しい手法までが含まれる

- 自動車のシステムやハードウェアの一部の故障が全体に波及することを抑止する技術
- 一部の電線の故障が波及して大規模停電を誘発することを抑制する技術

8

ヒューマン
ファクターの
考慮

- ヒューマンファクターとはシステムの安全性や有効性に影響を与える人間のふるまいや特性のこと
 - AcciMaps、STAMP、Human Factors Analysis Classification System (HFACS)、Event Analysis of Systemic Teamwork (EAST)などの手法を用いて分析される

- 高度道路交通システムにおける自動運転車と非自動運転車の共存
- 危険な製造現場におけるロボットと人間の協調作業

ヒューマンファクターはシステムオブシステムズの安全性・安定性に影響を与える要素の1つであるため、後段の具体的な技術事例として別途確認を実施する(分析の都合上、①の母集団内に⑧が含まれている)

1 網羅的な情報収集による全体感把握と対象技術の定義

リアルタイムテスト技術は仮想環境等で迅速に繰り返しシミュレーションを行いフィードバックする技術と定義

1 システム全体のリスクの想定困難性

概要

2

リアルタイム
テスト技術

- Hardware-in-the-Loop Simulation、Processor-in-the-Loop Simulationなどのシミュレーション技術が含まれる
- 実機を用いることなく、**実機を仮想的に再現した環境でシミュレーション**を行うことで、実機では困難な危険なケースのテストが可能
- また、不具合が発生する条件を把握し、不具合の出る環境を再現して繰り返しテストが可能
- 結果、ユーザーがデザインした制御モデルを迅速に実機テスト環境へと移行させ、実機テストを行うことが可能

具体例

- 電力網や石油・ガス、石油化学、水処理、原子力などのインフラにおいて、性能やサイバー攻撃の影響を知り、設計にフィードバックするためのシミュレーション技術

1 網羅的な情報収集による全体感把握と対象技術の定義

モジュラー化は運用時に増加する複数のサブシステムの接続関連、攻撃防御モデルはSoSに対するセキュリティの保証が中心となる技術

2 運用時のシステムの変化への対応の困難性

概要

具体例

3 モジュラー化 技術

- プラットフォームの構築やサブシステム間の接続の技術が含まれる
- システムオブシステムズではその定義により、運用開始後にサブシステムの追加が想定されるが、それらサブシステム間で挙動に矛盾があると、システム全体が不安定となる。そこで、プラットフォームを構築する技術や、サブシステム間を接続する技術、また、サブシステム間の矛盾の把握や解消のための技術が必要となる

- 車両やデジタルホームのアプリケーションを構築するために必要なサポートを提供するプラットフォームの構築
- システムオブシステムズのメカニズムを分析するゲーム理論

4 攻撃防御 モデル技術

- システムオブシステムズでは、ネットワーク化された大規模制御系に対する悪意のあるサイバー攻撃に対して、通信や計算量の面で制約される環境においても、セキュリティレベルや制御性能を保証する必要がある。攻撃や防御のモデルを構築し、定量化する技術が存在
- 多層フレームワークの構築技術、ブロックチェーン等の技術はセキュリティそのものに活用されている
- 攻撃／防御のモデルを構築し、リスクの定量化

- サイバーフィジカルシステムの攻撃と防御の間の相互作用のモデル化の研究
- 無人航空機の攻撃を検知し、警告信号を送信するコンピュータプラットフォームの構築

1 網羅的な情報収集による全体感把握と対象技術の定義

運用時の想定内の変化へ対応するロバスト制御技術と、想定外の変化からの回復技術等のレジリエンス技術をそれぞれ定義

2 運用時のシステムの変化への対応の困難性

概要

具体例

5

ロバスト制御 技術

- 想定内の入力の揺らぎを制御するもので、ファジィ制御やモデル化誤差などのロバスト制御の技術が含まれる
- システムオブシステムズでは、システムの入出力関係がノイズに対して安定するような設計が重要になる
- 事前に、あり得る環境の全てを把握することは不可能であるが、安全とコストのバランスを考慮しながら、一定レベルはモデルに組み込む必要がある。また、そのモデルと多少異なっても制御性を損なわない制御をする必要がある

- 再生エネルギーが導入された電力システムに対して系統安定度を向上するプラグイン型制御技術

6

システムズ レジリエンス 技術

- 想定外と言えるような大規模な災害や事故が発生した際に、経済的な効率をある程度達成したうえで、システムオブシステムズの安全性及び可用性を維持する必要がある
- どこまでを想定内として事前に対策をとり、どこからを事後の対応とするのかという、安全とコストのバランスをとること、システムが壊れないことだけでなく、壊れた後いかに素早く回復するかというレジリエンスの手法が重要となっている
- 大規模災害などを入れ込む計算モデルや、生物学にインスピレーションを得たネットワーク設計の技術が含まれる

- 防災のための社会インフラや、サプライチェーンを含めた生産システムなどを大規模災害時でも使用できるよう設計する技術

1 網羅的な情報収集による全体感把握と対象技術の定義

複数のシステムが繋がる中では、AIによる判断や決定に説明性を与えることが重要であるため、ホワイトボックス型AI技術を定義

3 AIによる判断の妥当性

概要

具体例

7

ホワイトボ
ックス型AI技術

- AIモデルがデータのどの部分を根拠に結果を出力したのかや、入力と出力の関係性を理解するための技術
- AI技術は、パフォーマンスに優れる反面、モデルが複雑になるため、その解釈性や説明性が損なわれブラックボックス化する傾向にある
- システムオブシステムズにてAIを使用する場合、説明可能なAI (Explainable AI, XAI) ・ホワイトボックス型AI技術を使用することが望ましい。主要な技術は以下の通り
 - 1回の予測に対して説明を行う（局所的な説明性）
 - LIME(Local Interpretable Model-agnostic Explanations)
 - SHAP(SHapley Additive exPlanations)
 - LRP(Layer-wise Relevance Propagation)
 - モデルの全般的な挙動を調べる（大域的な説明性）
 - SA(Sensitivity Analysis)

- 局所的な説明性
交通システムの一部となる自動運転システム。画像認識による交通標識の判別において、その「予測結果が正しいか」でなく、画像中の標識部分の「ピクセルを根拠に判断しているか」まで明らかにする
- 大域的な説明性
ニューラルネットワークを用いた山火事警報システム。一般的にはブラックボックスであるニューラルネットワークに対して「降雨の発生」「10時間あたり燃料含水率」「月 (Month)」が火災リスクに対して影響が大きいという説明性を与えた



2. 技術の定量評価や投資額動向の整理

2 技術の定量評価や投資額動向等より重要領域・技術を特定

取得した特許・論文・グラントデータ1件1件をスコアリングし、他者からの技術的注目度が高い技術を優先的に読み込む

特許・論文・グラントスコアリング手順

特許・論文・グラントの母集団

詳細分類A

詳細分類B

詳細分類C

異なる技術領域に含まれる技術のスコアを比較することはできないため、いくつかの技術区分ごとにスコアリングを実行する

イメージ

公報番号	公報発行日	出願番号	出願日	知財力スコア	有効余命
US8831677B2	20140909	US13373368A	20111110	133.60	11.45
US20130073387A1	20130321	US13439761A	20120404	115.79	0.00
US20110130636A1	20110602	US2010870117A	20100827	109.83	0.00
US8620841B1	20131231	US13601890A	20120831	109.07	12.26
US20110153368A1	20110623	US2009641128A	20091217	102.22	0.00
US8089356B2	20120103	US2009422953A	20090413	102.10	0.00
US8325034B2	20121204	US13279270A	20111022	101.10	0.00
US8457873B2	20130604	US2009653770A	20091216	98.70	11.46
US10027711B2	20180717	US13413586A	20120306	97.83	11.08
US8571731B2	20131029	US2009653769A	20091216	97.81	11.00
US20100306533A1	20101202	US2010790285A	20100528	96.81	0.00
US20100129357A1	20100527	US2009502581A	20090714	96.69	0.00
US9073554B2	20150707	US2009592276A	20091120	93.47	13.10
US8264345B2	20120911	US2009627031A	20091130	91.19	9.54
US9395707B2	20160719	US13214057A	20110819	90.82	10.66
US20130226624A1	20130829	US13776208A	20130225	90.48	0.00
US20100150829A1	20100617	US2009624778A	20091124	89.82	0.00
WO2010065079A2	20100610	WO2009US6274A	20091124	89.12	0.00
WO2011066371A2	20110603	WO2010US57981A	20101124	88.27	0.00

特許スコアは他社への技術的排他権としての被引用数評価を中心に、地理的な権利範囲、残存期間などを重み付けして総合的に算出

特許スコアリングロジック

スコアリングの特徴

特許が持つ情報をパラメタとして重みづけして偏差値を導出することで、任意の技術母集団内での優位性が算出可能

- 他国・他機関への排他権としてのインパクト評価を中心に、更に地理的な権利範囲、権利の時間的な残存期間などを重み付け
 - ✓ 他国・他機関への排他権は被引用文献数等で評価
 - ✓ 地理的な権利範囲はファミリー文献数等で評価
 - ✓ 権利の時間的な範囲として、特許ステータス、残存年数等で評価
- 被引用文献数に対するウェイト調整
 - ✓ 経済規模(GDP)と特許重要度(損害賠償額)が大きな国の特許を牽制している企業のスコアが高くなるように調整
- 推定有効期限の算出
 - ✓ 推定有効期限について、国毎の特性及び領域毎の技術の陳腐化スピードを反映し、算出

他社評価ロジックとの違い (経済性評価)



論文スコアは、以下の通り掲載されたJournalの評価と論文自体の評価とを掛け合わせて算出を行った

論文スコアリングロジック

掲載Journal自体の評価

Journalの領域補正済みImpact Factor

論文単体の評価

被引用回数+1

要素	意味合い
領域補正済みImpact Factor × 被引用回数	- Clarivate社が定めているJournal評価指標で、以下の計算式で計算 $\frac{n\text{年における}A, B\text{の延べ引用回数}}{A(n - 2\text{年の掲載論文数}) + B(n - 1\text{年の掲載論文数})}$ - Category間の値のアンバランスさが課題（医療系はI/Fが高めに算出等） - 領域を跨いだ比較が可能となるよう、I/FとJournal全体の被引用回数の両方を用いて補正 - Journalに1つもしくは複数付与されているCategoryごとに、重複を許してJournal全体の被引用数の平均を計算する - 被引用数の平均が最も大きいCategoryを筆頭Categoryとする 1の結果に対し、（各Categoryの平均）/（全Categoryの平均の合計）でCategoryごとの係数を計算し、筆頭CategoryとI/Fと掛ける - 論文単体の被引用回数が0の場合スコアが0になるのを避けるため1を加算 - 権威あるJournalに掲載されたが被引用回数0の論文と、I/Fが0のJournalに掲載された論文とを分けて評価する目的

グラントスコアは、研究者1人あたりに均した配分金額と、研究期間の残存年数との積により算出

グラントスコアリングロジック

$$\begin{array}{c} \text{投資額} \\ \boxed{\text{採択案件の1人あたり採択金額}} \end{array} \times \begin{array}{c} \text{時間的範囲} \\ \boxed{\text{残存年数}} \end{array}$$

要素	意味合い
1人あたり 採択金額	• どういった研究にどれだけ投資されているかを確認することで、対象となる研究の有望性を判断 • 採択金額を担当研究者の数で除した値を使用 (研究者単位でも同様のスコアリングを可能なよう、汎用的に定義を行っているため) $\frac{\text{採択案件の金額}}{\text{担当研究者数}}$ • 金額については、採択案件の開始日に一括で計上し計算を行った
残存年数	• 基準日時点の研究期間の残存年数を使用 • 過去の研究ではなく、現在稼働している研究のみを集計することで、現在から近未来の動きを捉えることが可能

特許スコアリング結果の一例。スコア上位には単一システム内での技術に注目していると思われる特許が並ぶ一方…

スコア上位3特許及び日本のスコア上位特許概要

KW分類	特許名称	概要	国	スコア
安全性解析	System and method for assessing the security posture of a network and having a graphical user interface	グラフィカルユーザーインターフェイスを用いてネットワークを複数回分析する必要なしに、ネットワークのセキュリティ脆弱性を評価するデータ処理システム・方法	US	146.97
攻撃防御モデル	Automated and adaptive model-driven security system and method for operating the same	複雑なIT環境でセキュリティポリシーを適切に管理するための、アクセス制御などの方法及びシステム	US	121.60
ロバスト制御	Method of Secure Electric Power Grid Operations Using Common Cyber Security Services	一般的なサイバーセキュリティサービスを使用して、電力網の制御システムから送電、配電のデバイスまで、安全に接続する	US	121.42
モジュラー化	人工知能を有するシステム	オープンな環境における情報交換を行う人工知能モジュールと、その人工知能モジュールの動作をモニターし、クローズドな環境で情報交換に伴う処理を行う別の人工知能モジュールを有するシステム	JP	56.20

…中位にはSoSやCPS関連の特許も存在しており、例えば動作不能となったシステムを同機能の別システムに置き換えるといった技術は深堀可能か

スコア中位のSoS/CPS関連特許概要

KW分類	特許名称	概要	国	スコア
安全性解析	System, method and computer program product for developing a system-of-systems architecture model	各システムアーキテクチャの協調的設計方法や、システム構造及び動作を直感的に捕捉可能にするための視覚的な描写（モデリング）技術	US	105.92
ロバスト制御	robust testing for discrete-time and continuous-time system models	CPSにおいて異なるシステムの接続により、浮動小数点演算等の複雑な計算が悪影響をもたらさないよう、離散時間・連続時間それぞれのモデルでプログラムの頑健性を検証	US*	87.22
システムズレジリエンス	Methods, systems and computer program products for determining systems re-tasking	SoSの可用性を最大化するため、経時的にシミュレーションを行い、動作不能（故障）となったシステムは同機能を保持する別システムに置き換える方法及びシステム	US	77.12
攻撃防御モデル	Method and apparatus for resilient end-to-end message protection for large-scale cyber-physical system communications	システム間で、スケーラビリティやend to endのセキュリティを損なうことなく、メッセージ認証や鍵の管理を行う技術	US	76.92

*USではあるが、NEC Laboratories America Inc.の特許

尚、特許に関しては日本の出願数は少ない。システムズレジリエンスやAI、セキュリティ関連については相対的に割合が高い領域

(参考) 分類別特許数と日本特許庁出願特許数

No.	分類	特許数	内、出願番号 JP始まりの特許	JP特許割合
1	安全要求定義／安全性解析	661	7	1.1%
2	リアルタイムテスト	29	0	0.0%
3	モジュラー化	948	11	1.2%
4	攻撃防御モデル	1253	28	2.2%
5	ロバスト制御	178	1	0.6%
6	システムズレジリエンス	174	5	2.9%
7	ホワイトボックス型AI	167	4	2.4%

特許としての排他性に加え、経済・財務的観点にも鑑みて保有特許や特許ポートフォリオを定量的に評価

特許毎	パテントインパクトスコア Patent impact score	◆「他社への技術的脅威（他社拒絶査定引用回数など）」 ◆「権利の地理的範囲（出願国など）」 ◆「権利の時間的範囲（権利の経過年数など）」 <u>他社への排他権としてのインパクト評価</u>を中心に、更に地理的な権利範囲、権利の時間的な残存期間などを重み付けした定量的な評価指標 ・対象母集団（技術分類、市場分類）毎に偏差値化 ・経済規模と特許重要度（特許侵害リスク）が大きな国の特許を侵害している企業のスコアが高くなるように調整 ・国ごとの特性や領域ごとの技術の陳腐化スピードを考慮し推定有効期限を設定
企業毎	トータルパテント アセット Total patent asset	各社の <u>特許ポートフォリオとしての総合的な競争力を計る指標</u> として使用 $= \Sigma [\text{パテント インパクト スコア } (\geq 50) \times \text{特許権利残存年数}]$
	パテントエッジスコア patent edge score	競合他社に対して大きな脅威となりうる突出した特許(1件)があるかどうかの指標として用いる $= \text{MAX}[\text{パテント インパクト スコア}]$

特許スコアリング結果では、アメリカや中国の企業／大学・研究機関のスコアが相対的に高い。HWとSWを組み合わせた特許が多く、他者へのインパクトが高いことが理由の1つと想定

特許スコアリングの結果概要

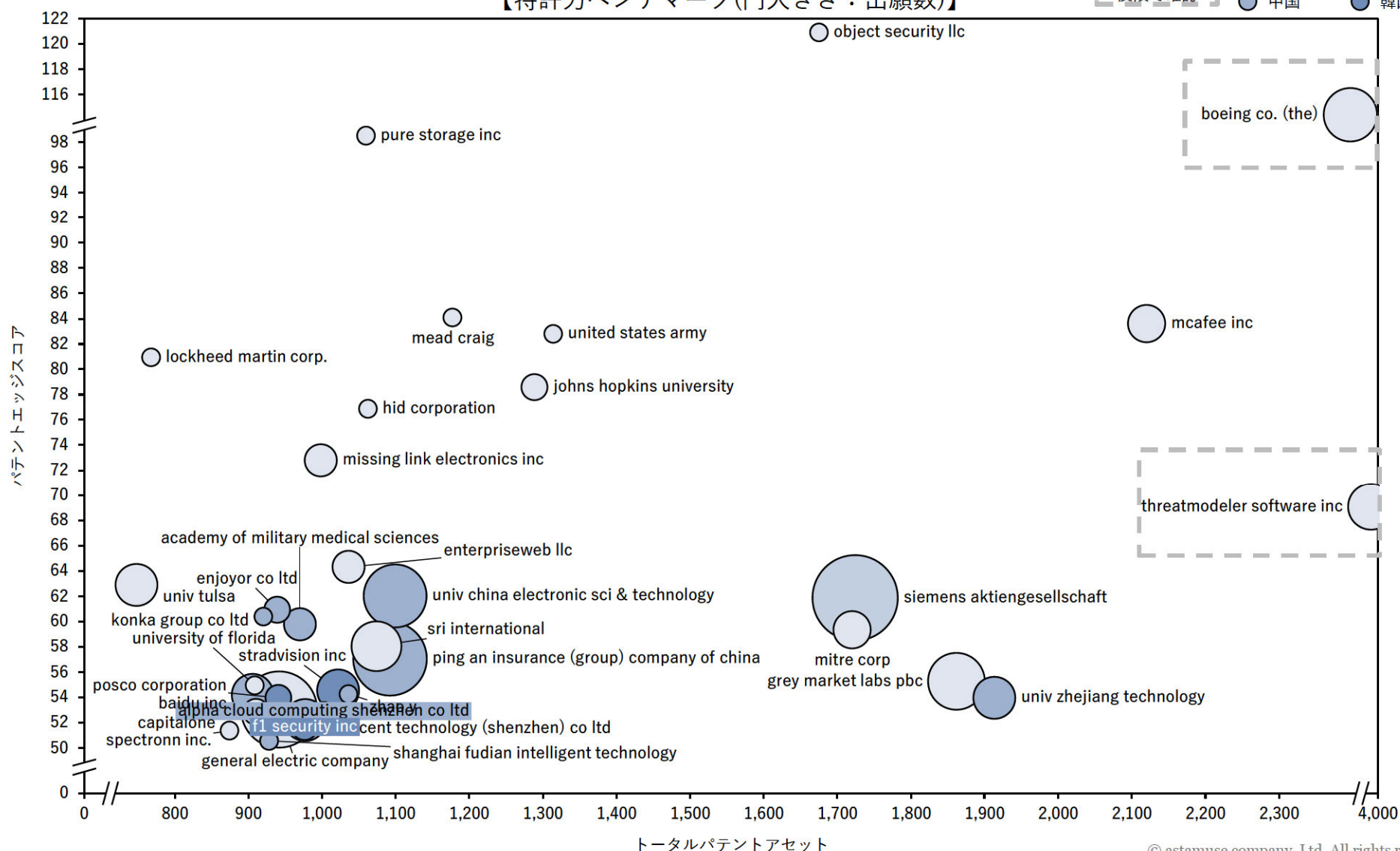
- 概観
 - アメリカや中国、ドイツ、韓国の企業／大学・研究所のスコアが比較的高位に位置する
 - 日本の出願も存在するものの、上位には入ってこない傾向にある
- 企業関連
 - 例えば、Boeing、General Electricを例にとると、2000年代は「航空機の飛行時の地図の表示方法」などデータを処理する特許が多く出願されていたが、2010年代以降は「UAVを用いた貨物の空中配送」など、ハードとソフトが融合したシステムの特許が増加している
 - 他方、NECや東芝では、上記海外企業と比較して、ハードとソフトが融合したシステムの特許の出願が少ない傾向が伺える
- 大学・研究所関連
 - 浙江工業大学（univ zhejiang technology）は中国浙江省の主要総合大学であり、2012年頃よりシステムの特許出願が急増している。具体的な実装を目的としたデータを処理する特許が多く出願されており、例えば画像処理に基づく「労働者の疲労状態検出」や「交通状況識別」などが挙げられる
 - また、テキサス大学の特許数は2000年代初頭より緩やかな増加傾向となっており、2000年代はデータ処理、2010年代になりハードとソフトの融合という傾向がみられる
 - 国内で見ると、東京大学も特許数は緩やかな上昇を示しており、当初はデータ処理の特許を出願しているが、ここ数年でハードとソフトの融合の特許が出願されている

①安全要求定義・安全性解析関連技術で総合力が高いのはアメリカ企業で、中でもboeingが総合力、突出力とも上位に位置する

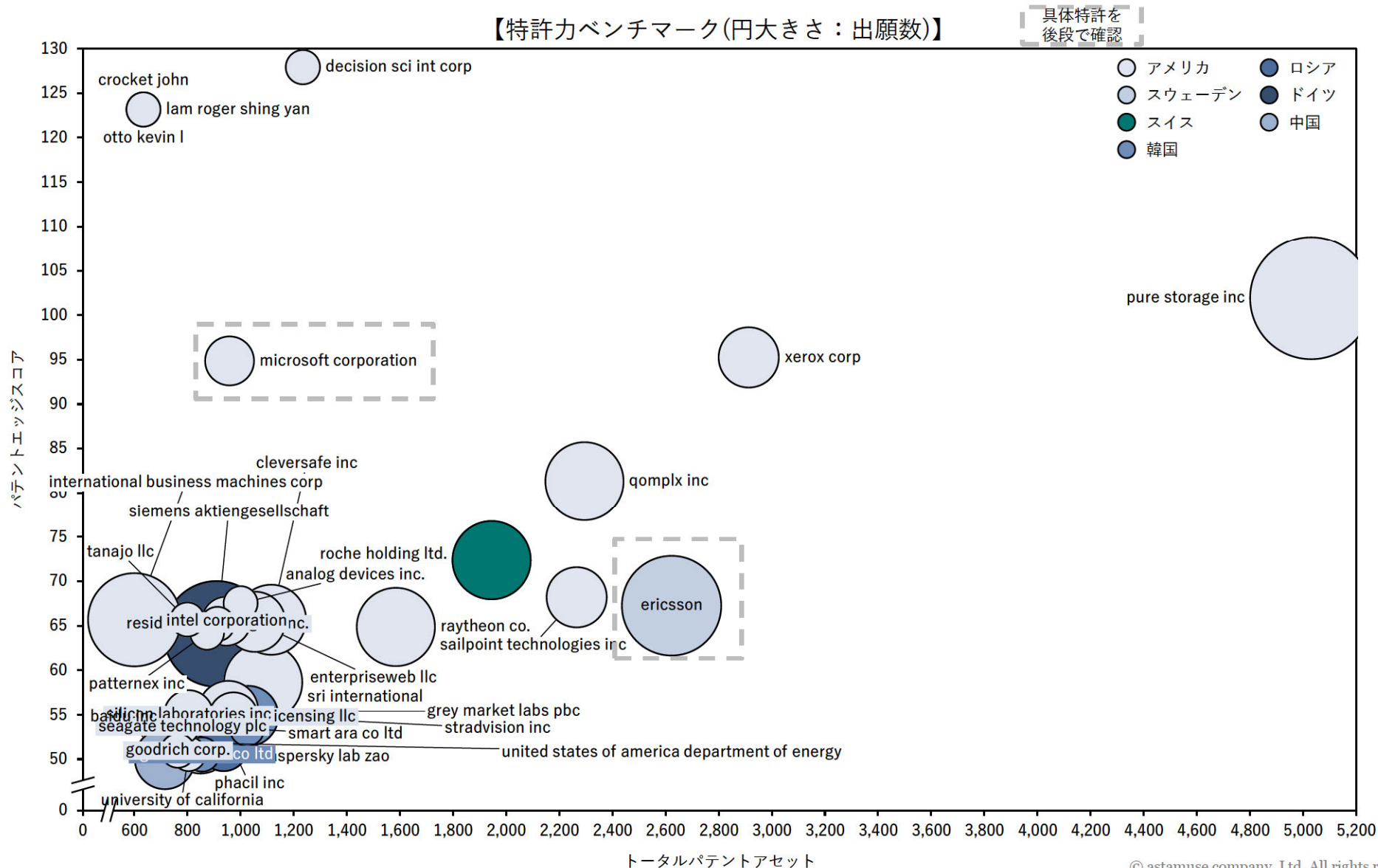
【特許力ベンチマーク(円大きさ：出願数)】

具体特許を
後段で確認

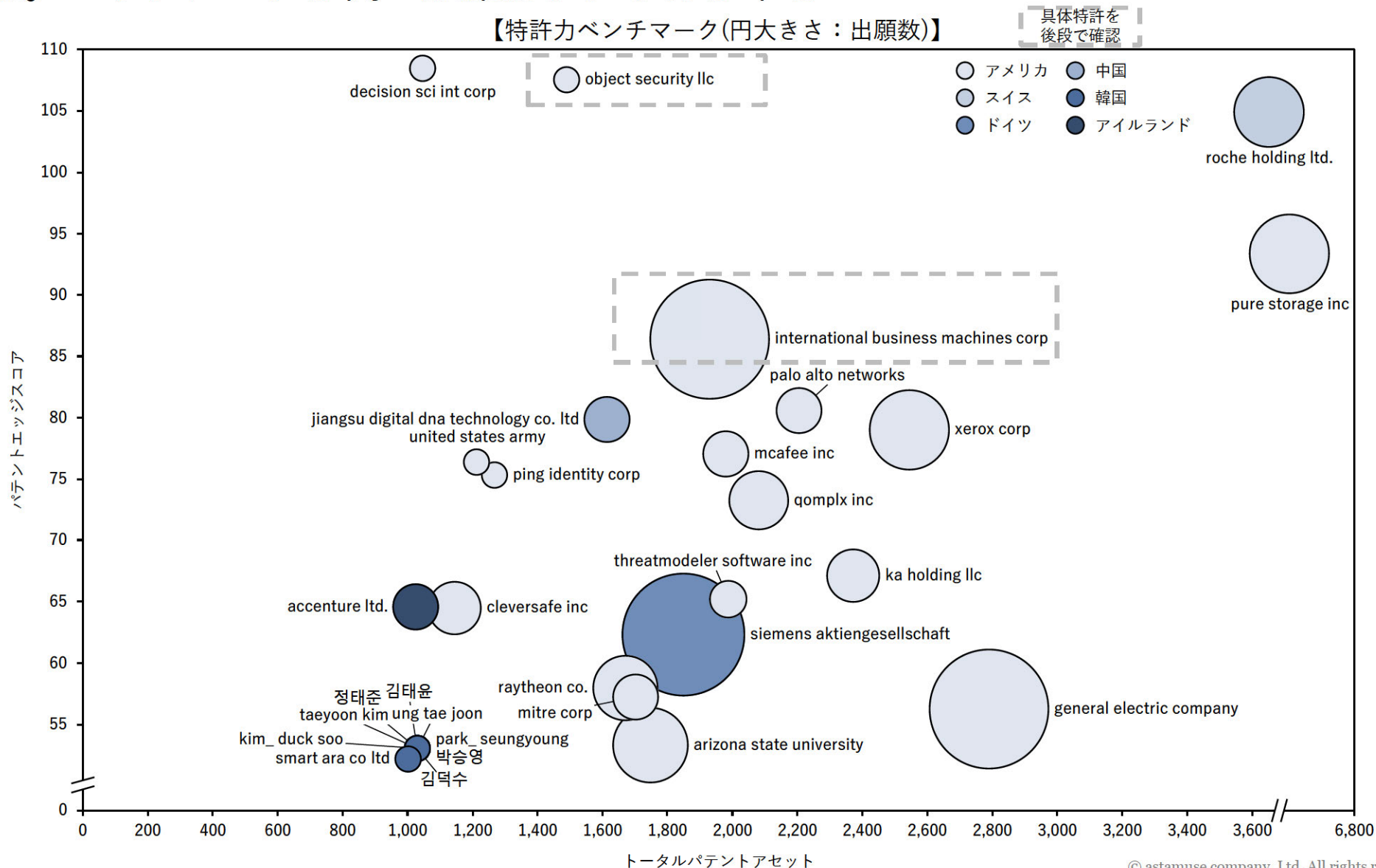
○ アメリカ ○ ドイツ
● 中国 ● 韓国



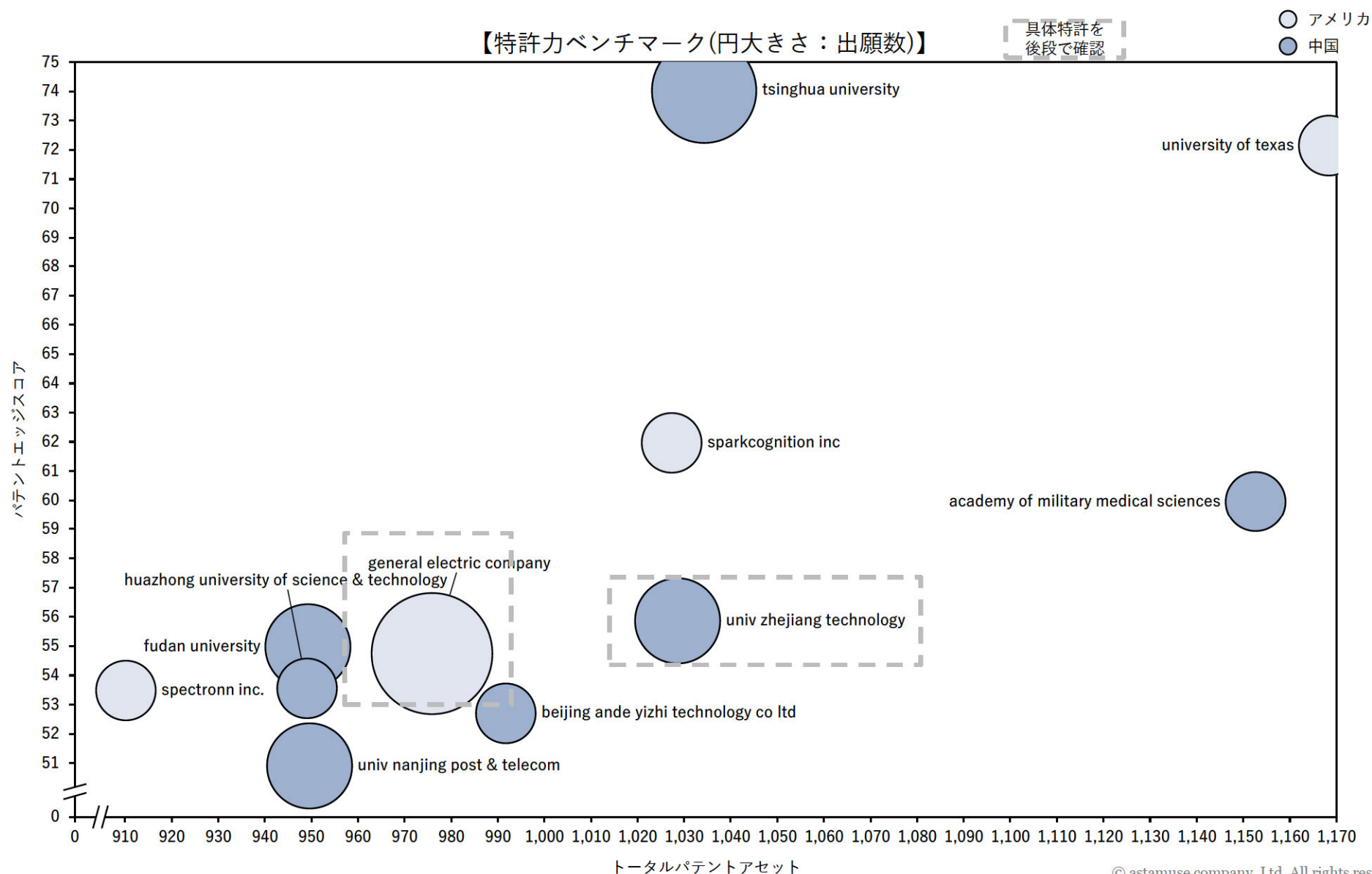
③モジュラー化技術は他技術に比べて、国籍に幅が存在



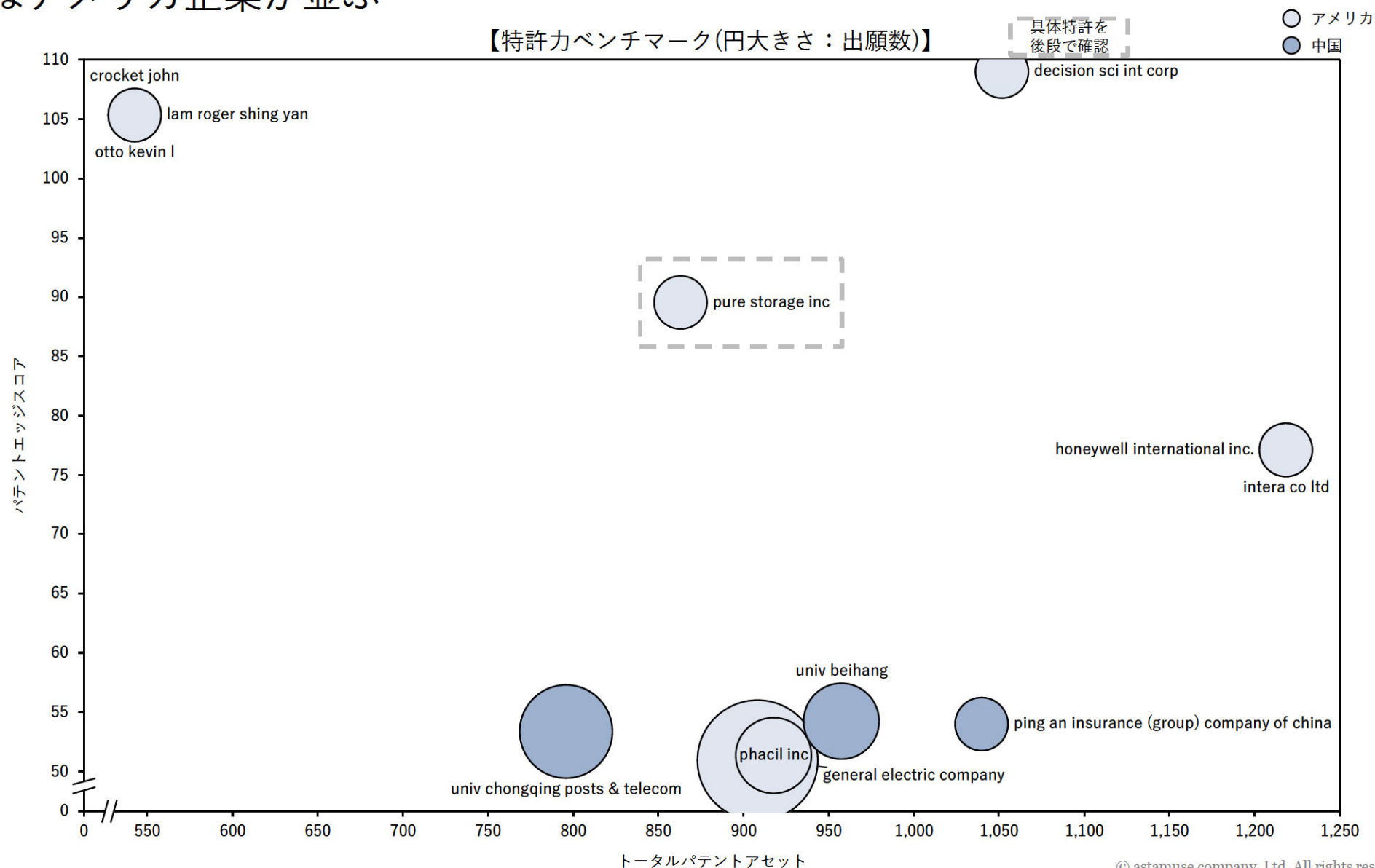
④攻撃防御モデル技術はIBMやGE等の関連特許出願が多く、IBMは中上位に存在。エッジスコアが高い企業はアメリカが中心



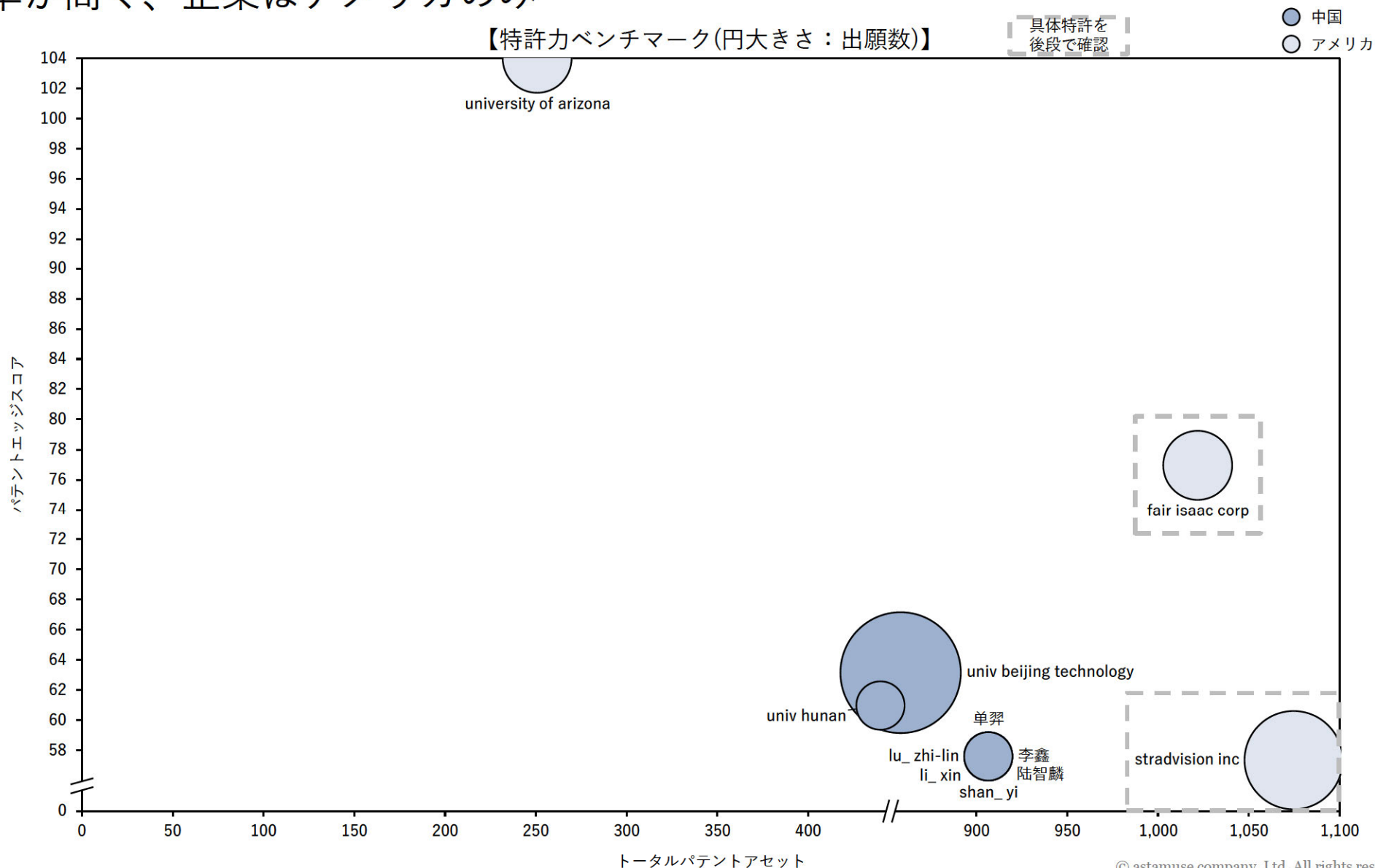
⑤ ロバスト制御技術は中国の大学や研究機関が多く出現している



⑥システムズレジリエンス技術はプレイヤー数は少ない。総合力・突出力上位にはアメリカ企業が並ぶ

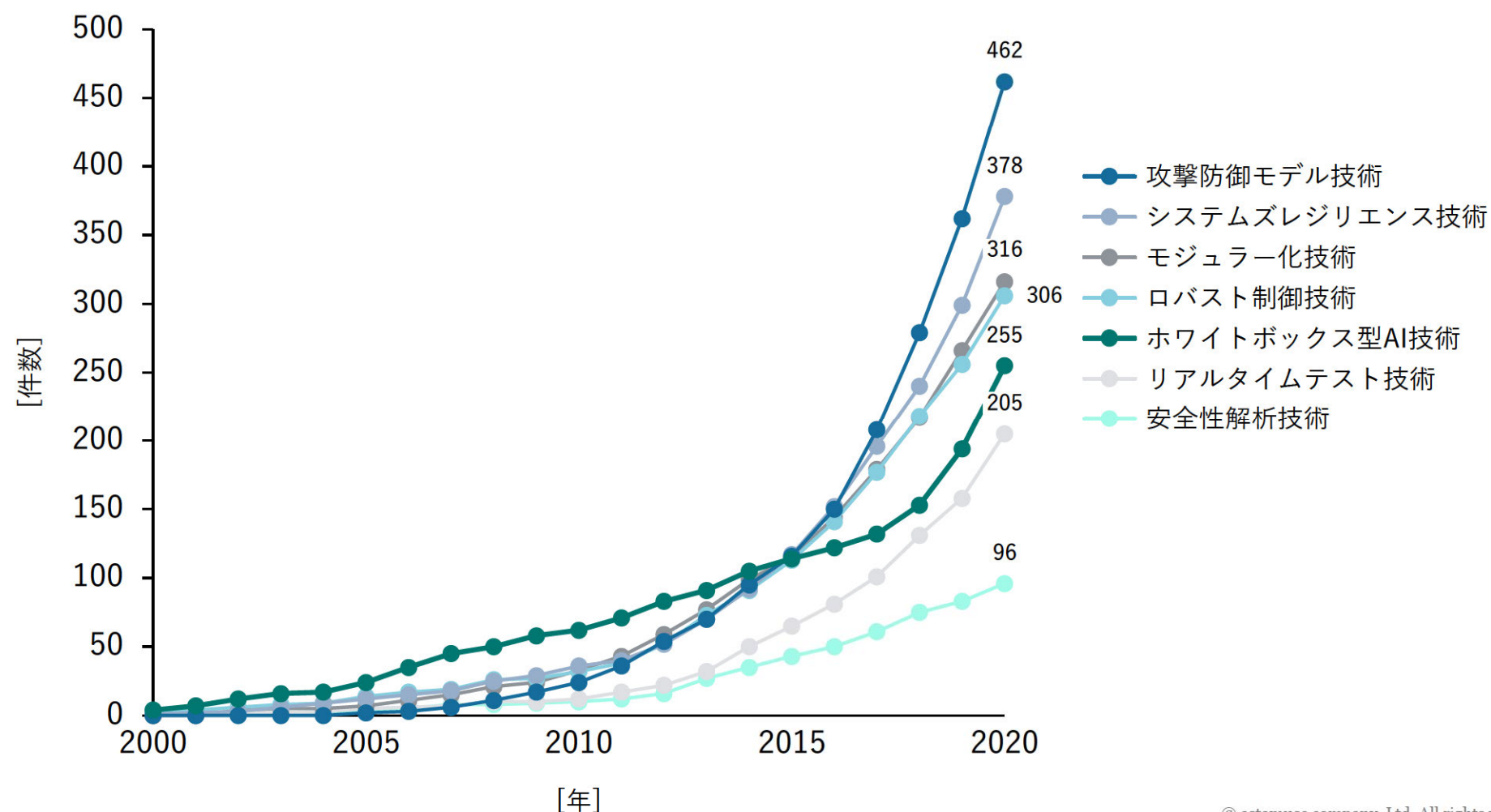


⑦ホワイトボックス型AI技術については、プレイヤー数は僅少。大学の特許の比率が高く、企業はアメリカのみ



各分類における論文発表数の推移は以下の通り。攻撃防御モデルやレジリエンス技術に関する論文中心

分類ごとの論文発表数（累積, 件数）



論文スコアリング結果の一例

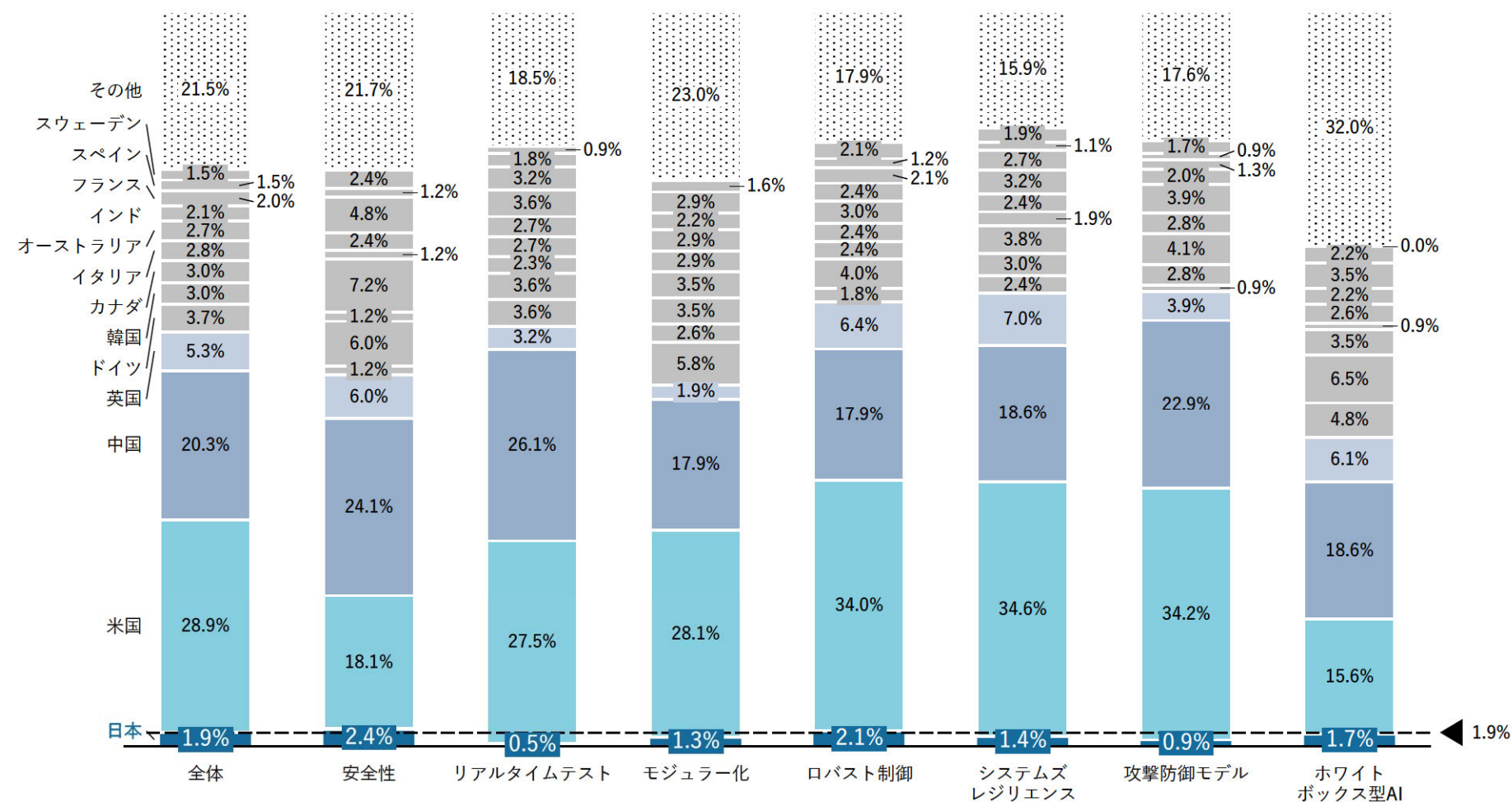
スコア上位3論文及び日本のスコア上位論文概要

KW分類	グラント名称	概要	国	スコア
攻撃防御 モデル	Cyber-Physical System Security for the Electric Power Grid	スマートグリッドにおけるサイバー攻撃に対するセキュリティの研究。アプリケーション・インフラ等の階層化によりセキュリティを担保する	US	36.08
モジュラー 化	Modeling Cyber-Physical Systems	航空機車両管理システムを例に、ハイブリッドシステムのモデリングやシミュレーション、コンカレントまたはヘテロジニアスな計算モデルなどを研究	US	25.89
システムズ レジリエン ス	Secure estimation and control for cyber-physical systems under adversarial attacks	攻撃により一部のセンサーまたはアクチュエーターが破損した場合に、システムの状態を推定しシステムを再構築する研究	US	20.25
ロバスト 制御	Robust Design of System of Systems Using Uncertainty Assessment Based on Lattice Point Approach: Case Study of Distributed Generation System Design in a Japanese Dormitory Town	システムオブシステムズの、不確実であり非線形であるという課題を回避するため、格子点を用いたロバスト最適化を研究	JP	0.02

スコア上位には、セキュリティやシステム予測のため、モジュール化や階層化されているシステムのモデリングを行う研究が並ぶ。また、説明可能なAIの研究として個別のAIのインプットとアウトプットの繋がりを研究するものも多い

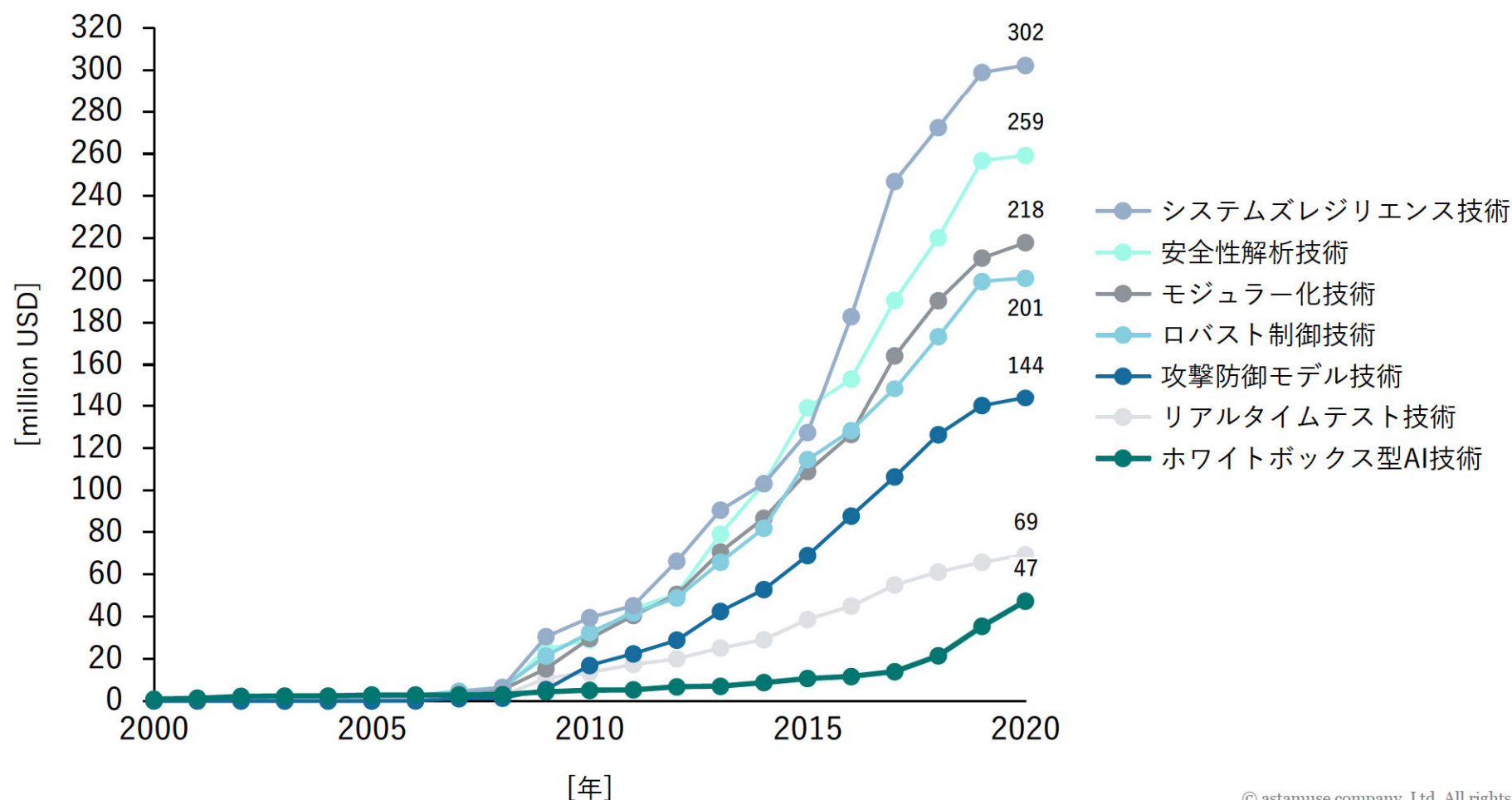
論文執筆者の国籍から国別の動向をみると、アメリカ・中国・イギリスが大半を占める。日本の研究が相対的に多いのは安全性やロバスト制御技術

分類ごとの論文執筆者の国籍割合



各分類におけるグラント調達額の推移は以下の通り。システムズレジリエンスや安全性解析、モジュラー化技術に関連する研究に注目が集まる

分類ごとのグラント配賦額（累積,millionUSD）



グラントスコアリング結果の一例

スコア上位3グラント及び日本のスコア上位グラント概要

KW分類	グラント名称	概要	国	スコア
安全性解析	EPSRC Centre for Doctoral Training in Autonomous Intelligent Machines and Systems	End to end の自律システムを構築するという目的に向け、AIやCPS、制御・検証等の研究を実施	GB	24,574,063
攻撃防御モデル	Cyber Security CDT Phase Two	big data security, assurance, CPS, real time securityといったテーマで幅広く研究を実施	GB	10,648,148
システムズレジリエンス	Serendipity - Säkra och pålitliga plattformar för autonomi	信頼性の高い既存（単一システムでの）セキュリティ技術を活用し、オープンで異種のシステムが繋がるCPS上で、スケーラブルなセキュリティを担保する技術の研究	SE	6,266,587
ホワイトボックス型AI	システム知の循環に基づく受容可能な知能システムの創生	現在のAIはブラックボックス化されており、システムの理解と検証に必要な知識抽出が困難。システム自らがシステム知を分析・説明・制御し、循環させる構造の研究	JP	155,419

スコア上位では自律したサービスのためにシステム全体として自己監視、自己修復、自己再構成などの機能を持たせる研究が存在。また、説明可能なAIのため、モデルの予想を理解する方法や検証方法も研究されている

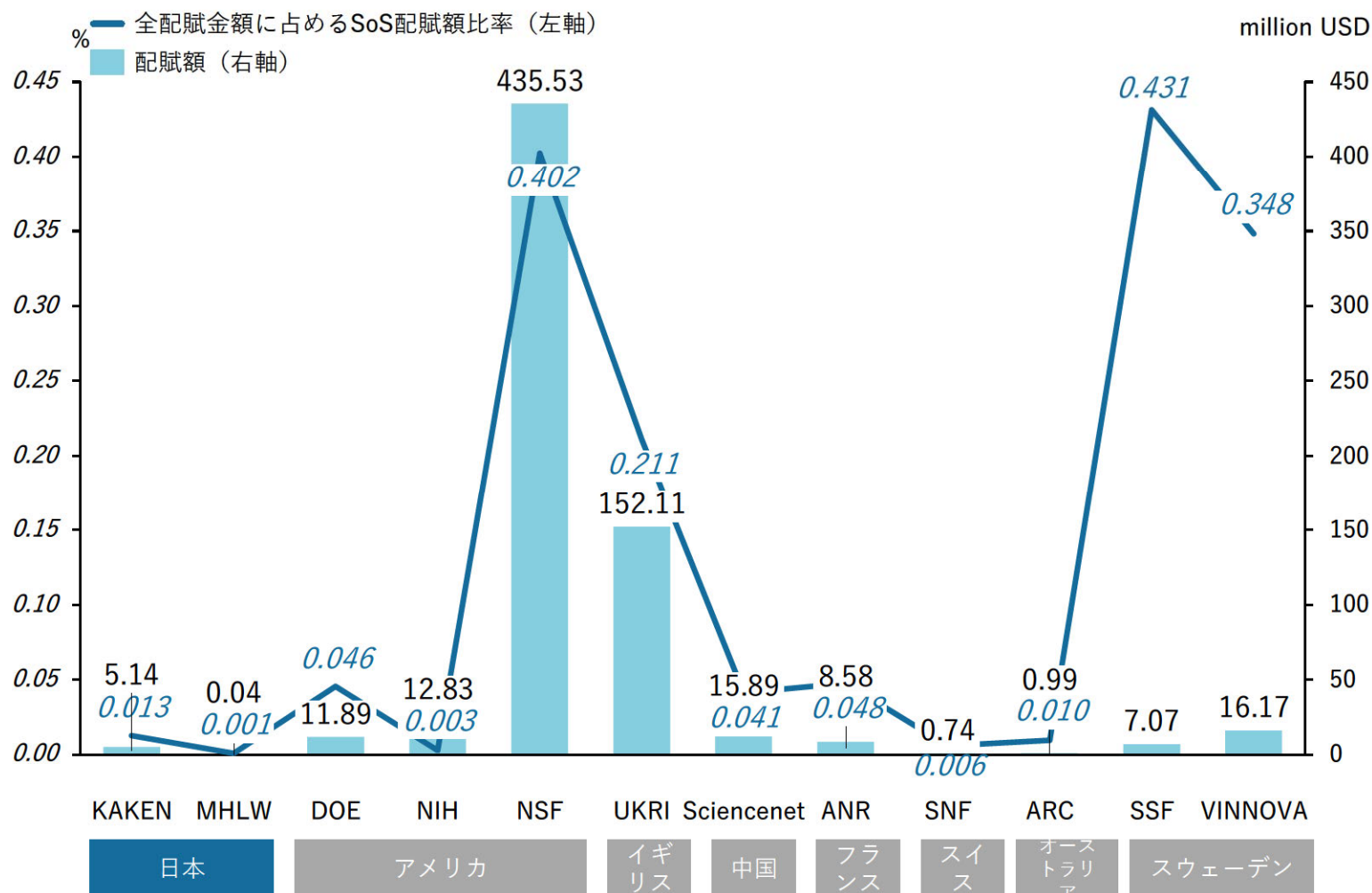
システムオブシステムズ関連の研究配賦は、日本、アメリカ、中国、オーストラリア、欧州各国の計8カ国、12機関でみられた

グラント機関一覧（システムオブシステムズ関連配賦あり）

国	機関略称	機関名
日本	KAKEN	科学研究費助成事業データベース
日本	MHLW	国立保健医療科学院/厚生労働省（厚労科研費）
アメリカ	DOE	U.S. Department of Energy
アメリカ	NIH	National Institutes of Health
アメリカ	NSF	National Science Foundation
イギリス	UKRI	United Kingdom Research and Innovation
中国	Sciencenet	ScienceNet（化学網）
フランス	ANR	Agence Nationale de la Recherche
スイス	SNF	Swiss National Science Foundatio
オーストラリア	ARC	Australian Research Council
スウェーデン	SSF	Swedish Foundation for Strategic Research
スウェーデン	VINNOVA	Swedish Agency for Innovation Systems

金額ベースではアメリカ・イギリスが圧倒するものの、比率からはスウェーデンが当該領域へ注力していることがわかる

【機関別システムオブシステムズ関連グラント配賦額累計及び割合（集計期間：2000-2020）】



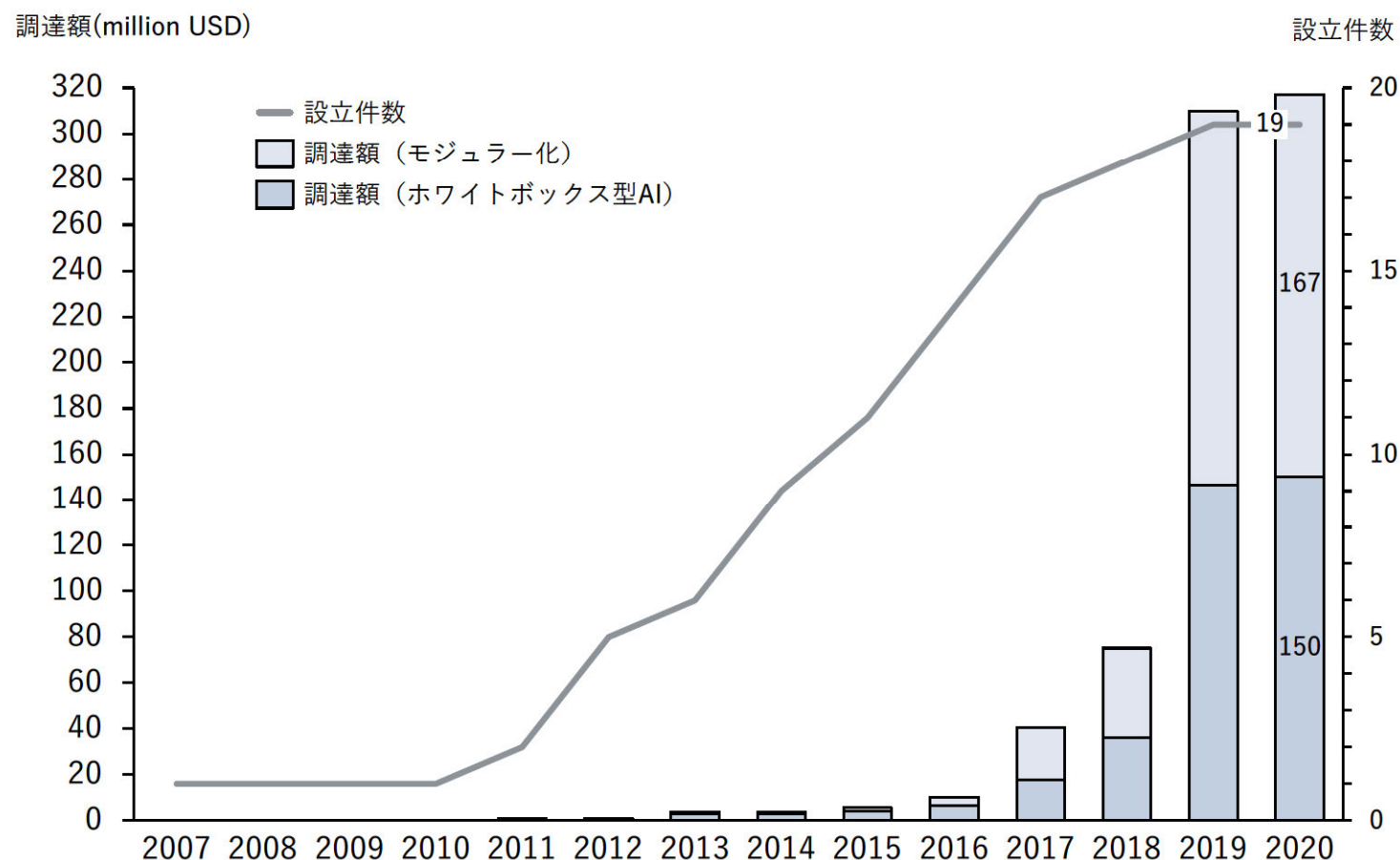
各国とも直近5年で投資額が増加傾向にある。日本の研究配賦は2015年以降特に伸びている中、アメリカやフランス、スウェーデンでは若干先行して配賦が行われている

【機関別システムオブシステムズ関連グラント配賦額（2000-2020; million USD）】 ※投資額を機関別にスケール表示

Source		2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
日本	KAKEN	0.02	0.05	0.03	0.17	0.03	0.18	0.00	0.00	0.00	0.08	0.03	0.26	0.31	0.33	0.25	0.65	0.84	0.34	0.67	0.89	0.00
	MHLW	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.04	0.00	0.00	0.00	0.00
アメリカ	DOE	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	7.14	0.69	0.00	0.00	1.97	1.87	0.21
	NIH	0.55	0.00	0.81	0.00	0.00	0.25	0.00	0.00	0.00	1.32	0.70	0.21	0.39	0.00	0.00	1.31	0.00	0.00	3.58	3.00	0.73
	NSF	0.30	0.41	0.00	0.00	0.00	0.15	0.30	6.66	3.92	35.65	33.22	19.99	28.31	40.32	31.48	55.33	30.20	46.08	42.66	51.89	8.66
イギリス	UKRI	0.00	0.00	0.00	0.00	0.00	0.00	0.96	9.30	0.72	1.02	0.00	0.95	0.48	3.56	0.90	10.23	48.60	44.02	11.66	11.08	8.65
中国	SCIENCENET	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.00	1.66	2.07	2.66	3.88	2.38	3.22	0.00	0.00
フランス	ANR	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	2.50	0.37	2.41	1.63	0.00	0.90	0.34	0.43	0.00
スイス	SNF	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.26	0.00	0.00	0.49	0.00	0.00	0.00
オーストラリア	ARC	0.00	0.00	0.09	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.28	0.37	0.24
スウェーデン	SSF	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	2.01	0.00	0.00	0.00	0.00	0.00	0.31	3.57	0.91	0.26
	VINNOVA	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	2.94	4.72	1.42	2.71	2.62	1.77	0.00

各分類におけるベンチャー投資額の推移から、モジュラー化技術、ホワイトボックス型AI技術は展開が早期に進むと想定

関連ベンチャー設立動向と分類毎の調達額累計（累積,millionUSD）



短期・中長期の資金流入動向を踏まえると、安全性解析や攻撃防御モデル、ロバスト制御やシステムレジリエンス関連の技術については今後注目に値すると考えられる

投資額等サマリ

	短期的期待値 (VB投資額) million USD	中長期期待値 (GT投資額) million USD	サイエンス 注目度(論文数)	有望技術 領域
① 安全要求定義／安全性解析技術 ⑧ ヒューマンファクターの考慮	N/A	259	96	✓
② リアルタイムテスト技術	N/A	69	205	
③ モジュール化技術	167	218	316	✓
④ 攻撃防御モデル技術	N/A	144	462	✓
⑤ ロバスト制御技術	N/A	201	306	✓
⑥ システムレジリエンス技術	N/A	302	378	✓
⑦ ホワイトボックス型AI技術	150	47	255	✓



3. 技術キーワードの共起分析結果からみる トレンドの把握

データソースそれぞれにつき、頻出度が高い単語を抽出。抽出された単語から定型語や汎用語を除外した上で、共起の時系列変化を確認する

共起分析実施手順

2000～2020年の各母集団から
頻出単語を上位30件ずつ抽出

rank	patent	grant	paper
1	network	systems	systems
2	system	research	cyber
3	method	project	system
4	invention	infrastructure	security threats
5	data	development	cps components
6	user	design	paper
7	device	data	physical systems
8	information	system	safety
9	attention	cps	technical analysis
10	model	impact	attacks
11	systems	cyber	model
12	plurality	time	approach
13	image	technologies	cpss
14	time	tools	data
15	learning organization	science environment	time
16	architecture	cities	study
17	communication	control	reliability models
18	timing vector	models	framework
19	processor	methods	information
20	level policy	impacts	development
21	computer screen	approach	results
22	module	services	method
23	identification	communities	sos
24	output	applications	control
25	memory	energy	system design phase
26	devices	world	challenges
27	network model	training	issues
28	input	students	performance
29	security posture	generation	communication networks
30	policy set	representatwater	methods

定型語や汎用語の除外

ソース内定型語（例）

- 特許：invention
- グラント：research, project, approach
- 論文：paper, approach, study, result

汎用語（例）

- development
- method
- data

キーワード設定・共起分析

以下10語を選定し分析実施

- cps, cyber physical system
- cyber
- sos, system of systems
- security
- safety
- reliability
- framework
- model
- application
- user

組み合わせパターンは45通り。3ソース分実施し、計135件がOutputとなる

(参考) 各データソースの頻出語について

データソース毎の頻出上位20語は以下の通り。今回のPJテーマにも鑑みて
SoS、CPSと安全性・信頼性に関係する用語を選定

定型用語等

選定キーワード

rank	特許	グラント	論文
1	[('network', 0.025423626363201165),	[('systems', 0.019342036949306942),	[('systems', 0.02769132767474545),
2	('system', 0.019768028748633797),	('research', 0.015240384793590946),	('cyber', 0.02301212380421603),
3	('method', 0.01904601462832604),	('project', 0.013176992682994531),	('system', 0.02079535900619998),
4	('invention', 0.014791512085284734),	('infrastructure', 0.009981526704196532),	('security threats', 0.01806151694011345),
5	('data', 0.013398050652178398),	('development', 0.006721631226573133),	('cps components', 0.014225298248930424),
6	('user', 0.013187668421733908),	('design', 0.006704306340865518),	('paper', 0.012604239008158904),
7	('device', 0.01123921065655214),	('data', 0.005823770195049545),	('physical systems', 0.012579896542266676),
8	('information', 0.009686470940719002),	('system', 0.005610632518946246),	('safety', 0.009367378466594719),
9	('attention', 0.007837777687102757),	('cps', 0.00540097047571732),	('technical analysis', 0.007488830342732799),
10	('model', 0.007455495510206491),	('impact', 0.0052926194373378145),	('attacks', 0.006836407436088791),
11	('systems', 0.006376194164593632),	('cyber', 0.005253706924259554),	('model', 0.006745819385094132),
12	('plurality', 0.005026304755986803),	('time', 0.004886144807732964),	('approach', 0.0064244283404455045),
13	('image', 0.004818393058034487),	('technologies', 0.004452470626812117),	('cpss', 0.006317685719633675),
14	('time', 0.004793264416763609),	('tools', 0.004427625773517253),	('data', 0.006194893687376732),
15	('learning organization network intrusion', 0.004666531266023441),	('science environment', 0.0040013713775043465),	('time', 0.005311999147902911),
16	('architecture', 0.004236508660452873),	('cities', 0.003929141565381122),	('study', 0.004960919694833447),
17	('communication', 0.0041284491334176434),	('control', 0.003911299414343844),	('reliability models', 0.004894404514855756),
18	('timing vector', 0.004058379672187445),	('models', 0.003704170539050791),	('framework', 0.004687595641253111),
19	('processor', 0.004039110476782568),	('methods', 0.0034975173359841905),	('information', 0.004500649947191406),
20	('level policy', 0.00391465522308266),	('impacts', 0.0034544000853028336),	('development', 0.0044144425663782015),
21	('computer screen', 0.0038394773139938648),	('approach', 0.0033632105999826844),	('results', 0.0043382910963109325),
22	('module', 0.003772398547806175),	('services', 0.0033609170599271814),	('method', 0.004162152364447564),
23	('identification', 0.0037611921478367745),	('communities', 0.0033558628753579344),	('sos', 0.003921377053776897),
24	('output', 0.0037488551326958436),	('applications', 0.0032455810248450375),	('control', 0.003736786470583787),
25	('memory', 0.0037151857322974386),	('energy', 0.003236045621035322),	('system design phase', 0.0036876956531632717),
26	('devices', 0.0036118912994973066),	('world', 0.003212432372459424),	('challenges', 0.0036194479487886154),
27	('network model', 0.00353175167987971),	('training', 0.0031979297657479663),	('issues', 0.0034616966631768444),
28	('input', 0.0033765706172205604),	('students', 0.003117862377749721),	('performance', 0.0033046876452126313),
29	('security posture', 0.0033578940125735895),	('generation', 0.003101426578673069),	('communication networks', 0.003064782648767527),
30	('policy set representations', 0.0033091468993258766)]	('water', 0.003067298847807805)]	('methods', 0.0029924825117679664)]

全体的にグラント→論文→特許の順に件数が蓄積されている傾向にある。尚、System of Systemsとの共起は少なく、上位はCPSやcyberが中心

共起の累積件数（集計期間：2000－2020）上位60件

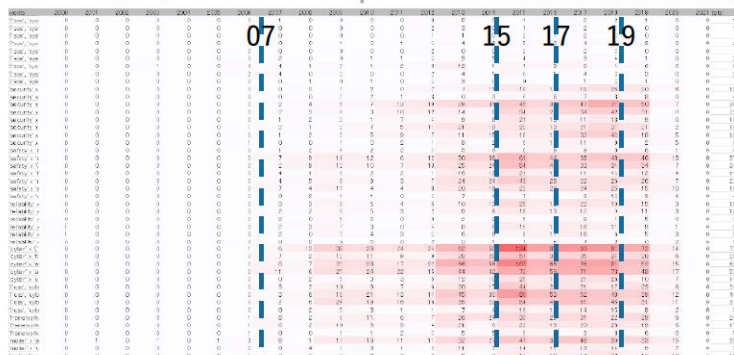
words	source	total(00-20)	words	source	total(00-20)
'cyber' x 'cps', 'cyber physical system'	グラント	734	'cyber' x 'user'	グラント	147
'cyber' x 'model'	論文	634	'safety' x 'model'	特許	145
'cyber' x 'model'	グラント	622	'security' x 'safety'	特許	142
'cyber' x 'application'	グラント	531	'model' x 'application'	特許	138
'cps', 'cyber physical system' x 'model'	グラント	443	'cyber' x 'cps', 'cyber physical system'	論文	136
'safety' x 'cyber'	グラント	376	'safety' x 'cyber'	論文	129
'cps', 'cyber physical system' x 'application'	グラント	375	'security' x 'safety'	グラント	128
'security' x 'cyber'	グラント	365	'safety' x 'model'	論文	121
'model' x 'application'	グラント	352	'safety' x 'framework'	グラント	114
'model' x 'application'	論文	347	'framework' x 'application'	論文	111
'framework' x 'model'	論文	323	'security' x 'framework'	グラント	106
'safety' x 'cps', 'cyber physical system'	グラント	304	'application' x 'user'	グラント	104
'cyber' x 'framework'	グラント	290	'reliability' x 'cps', 'cyber physical system'	グラント	103
'cyber' x 'application'	論文	284	'cyber' x 'model'	特許	99
'security' x 'cyber'	論文	254	'model' x 'user'	グラント	99
'framework' x 'model'	グラント	240	'reliability' x 'model'	グラント	99
'safety' x 'model'	グラント	236	'reliability' x 'cyber'	論文	97
'model' x 'user'	特許	223	'application' x 'user'	特許	92
'security' x 'cps', 'cyber physical system'	グラント	222	'reliability' x 'model'	論文	92
'cyber' x 'framework'	論文	215	'security' x 'application'	論文	92
'cps', 'cyber physical system' x 'framework'	グラント	205	'cps', 'cyber physical system' x 'user'	グラント	91
'safety' x 'application'	グラント	194	'model' x 'user'	論文	87
'security' x 'model'	特許	189	'security' x 'application'	特許	86
'security' x 'model'	グラント	183	'security' x 'cyber'	特許	86
'security' x 'application'	グラント	181	'reliability' x 'application'	グラント	82
'framework' x 'application'	グラント	177	'safety' x 'application'	論文	81
'sos', 'system of systems' x 'model'	論文	161	'cyber' x 'user'	論文	79
'security' x 'model'	論文	160	'cyber' x 'cps', 'cyber physical system'	特許	75
'reliability' x 'cyber'	グラント	155	'cps', 'cyber physical system' x 'model'	論文	72
'security' x 'user'	特許	151	'security' x 'framework'	論文	68

また、データソース毎の時系列のヒートマップから、グラント→論文→特許の順に共起が発生している傾向が確認できる

表詳細は
Appendix参照

データソース別共起Heat map ※共起件数をスケール表示
少 多

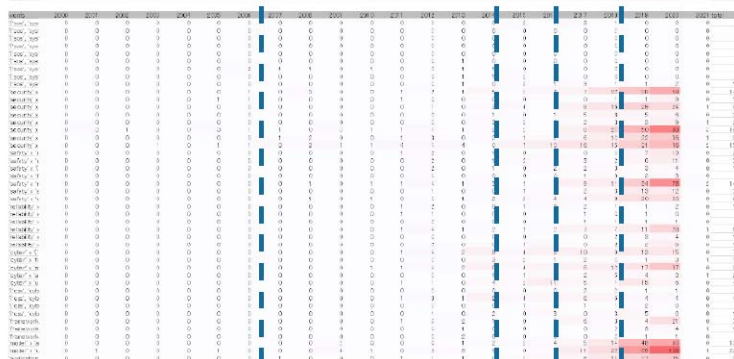
グラント



論文



特許

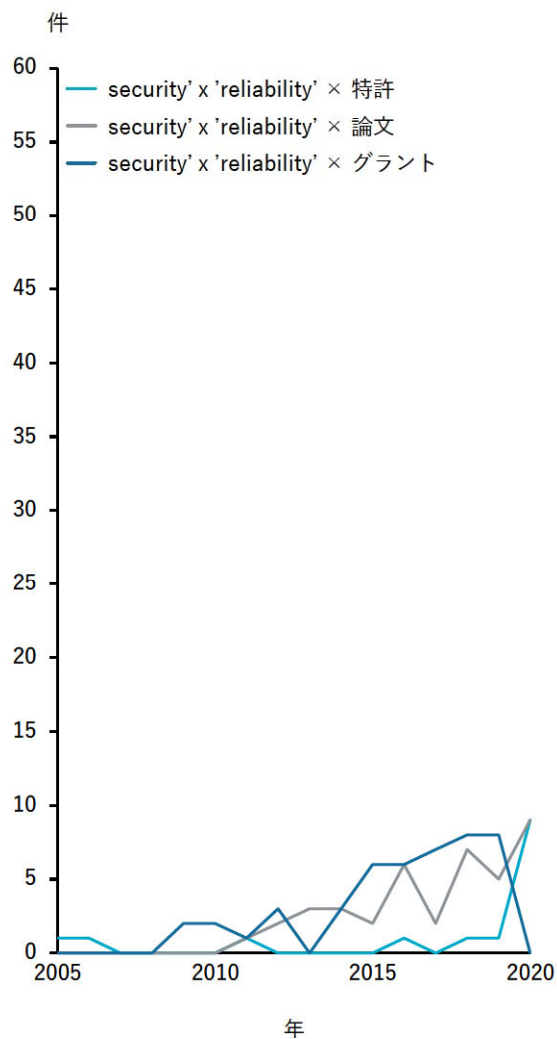
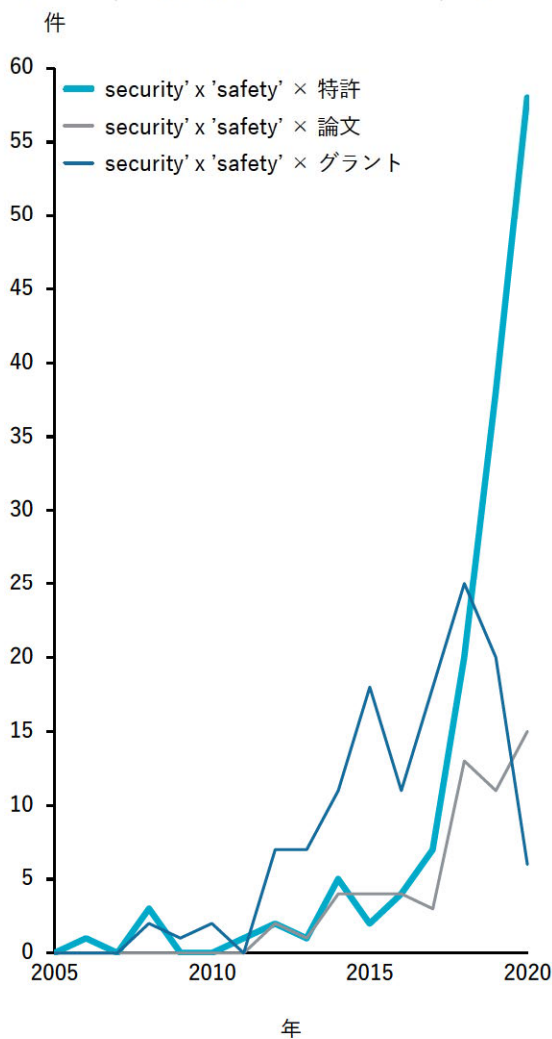
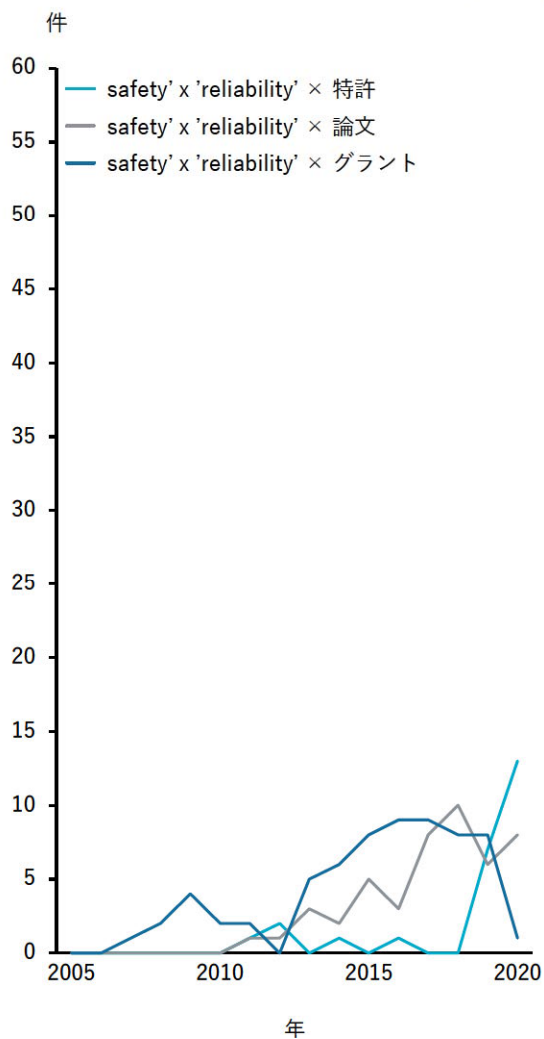


傾向

- 2007～2009年頃から各単語の共起が始まっている
- 2013年頃から共起傾向は伸びがみられ、**2015～2017年**頃にピークを迎えている単語の組み合わせが多い
- 2012年頃から各単語の共起が始まっている
- 2015年頃から共起傾向に伸びがみられ、**2017～2019年**頃にピークを迎えている単語の組み合わせが多い
- 2014年頃から各単語の共起が始まっている
- 2019～2020年**頃から共起傾向に伸びがみられる

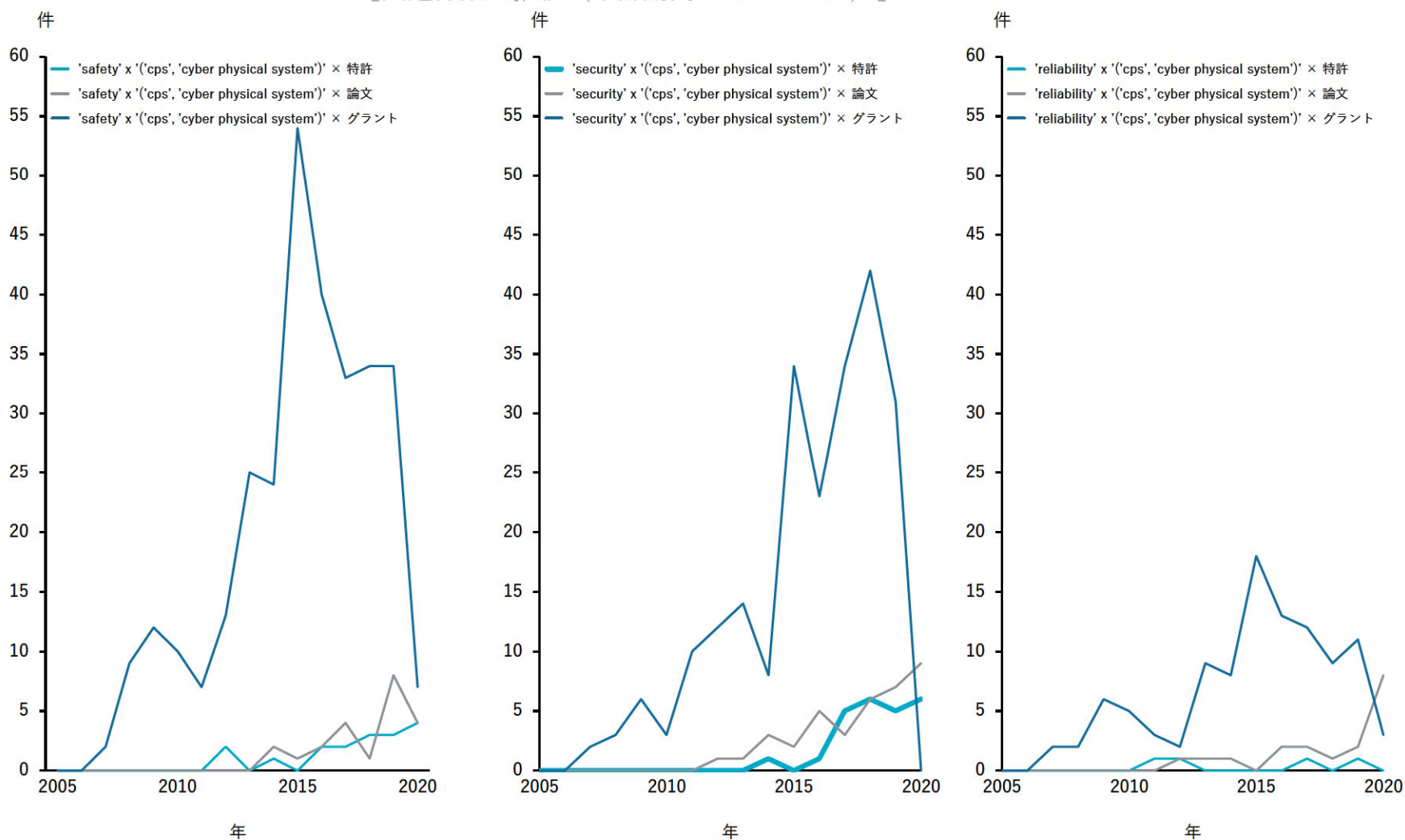
'17年以降急速にsafetyとsecurityが同時に論じられるようになってきている。また、信頼性(reliability)と同時に論じた研究は相対的に少ない

【共起件数の推移（集計期間：2000-2020）】



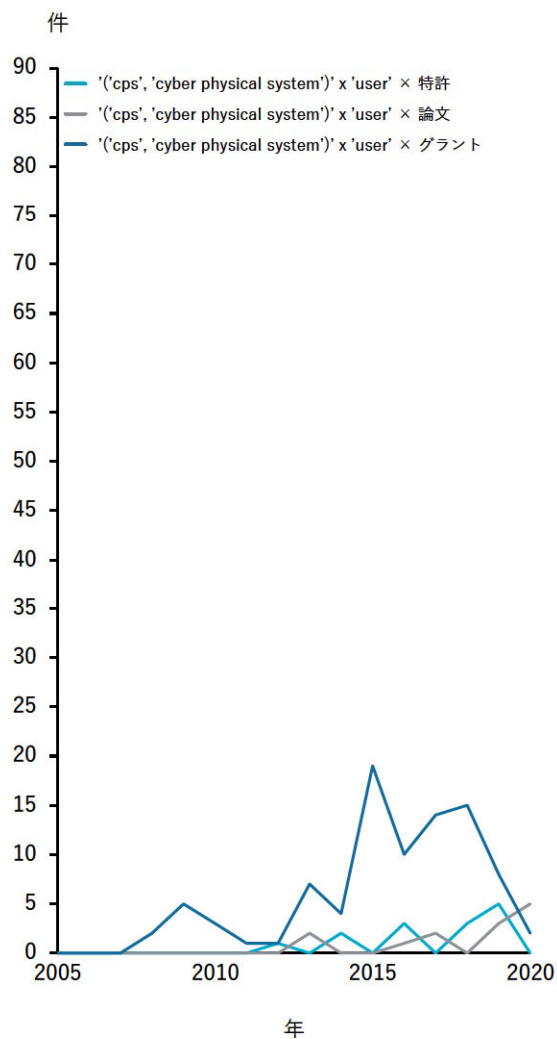
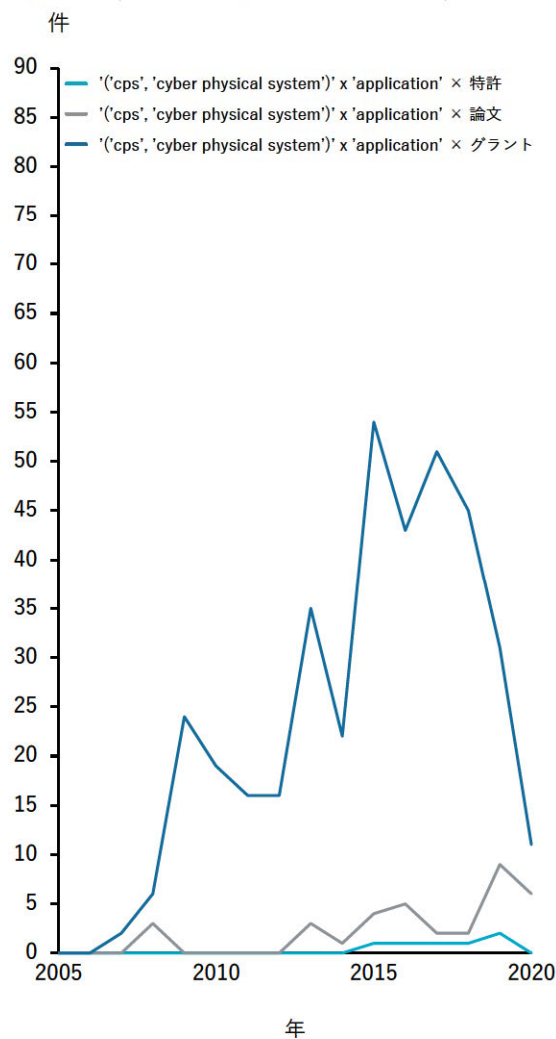
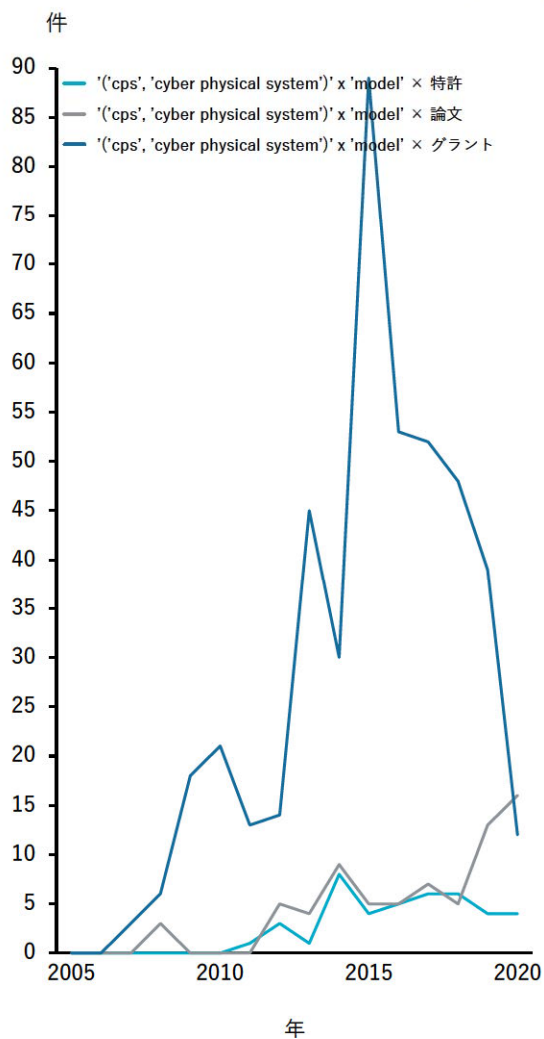
CPSとの関連ではsafety, security, reliabilityの順に共起が発生。グラントはそれぞれ一定数出現するが、特許での出現が多いのはsecurity関連技術

【共起件数の推移（集計期間：2000-2020）】



modelの共起は特許・論文にも多少見られる一方、application, user等のより実装段階に近いと想定される用語はグラントを除き出現が少ない

【共起件数の推移（集計期間：2000-2020）】



今後は単なるセキュリティだけではなく、安全性（safety）も含めた技術の社会実装が期待される

- 頻出語の観点
 - 論文においては、safety, security, reliabilityといった安全性や信頼性を論じるものが多くみられることから、**学術的に安全性・信頼性が重要なファクターであると認識されている**と考えられる
 - 他方で、特許では同様の単語はsecurityを除いて上位には出現せず、**ビジネス上（アプリケーション上）はsecurity関連の技術を中心に確立されている**と想定される
 - その意味で、ヒューマンファクター等の概念にも通ずるsafety関連の技術の実用化は今後期待すべき観点
- 共起の観点
 - 各単語の共起の推移から、概ね「**グラントによる国の予算配賦**」→「**論文による実証**」→「**ビジネスでの実装（特許）**」という時間軸で推移している傾向が見て取れる
 - とりわけ、safetyとsecurityは2017年以降急速に特許で共起が発生しており、頻出語でsecurityが多いことも踏まえると、**今後はビジネスの文脈でもsafetyにより軸足が置かれる**と想定
 - また、モデルやフレームワークといった（比較的）抽象的な用語の共起の方が、アプリケーション等の用語に比べて多く起きている
 - ただ、**アプリケーションやユーザ**といった用語についても**グラントでの共起は上昇傾向であるため、今後は個別具体的な技術開発が想定される**



4. 各領域の研究開発・実装状況の具体的調査

コンポーネントのフォルトツリー解析をシステムのモデルに統合して、SoS全体の障害の伝播を直感的に捕捉可能

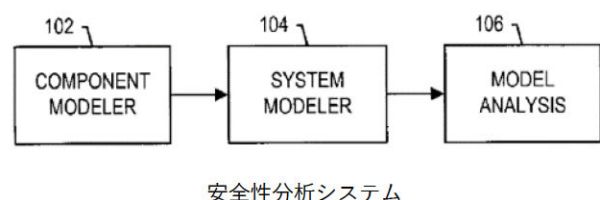
会社概要

会社名	Boeing
所属国	米国
業種	航空宇宙、軍需
売上（2020年）	58,158(百万ドル)
Webサイト	https://www.boeing.com/

事業概要

- 民間航空機と防衛・宇宙・セキュリティシステムの製造、それらのアフターマーケットサービスを提供

技術概要



- フォルトツリー解析(FTA)を使用した、航空機のような複雑なシステムの安全性分析
- コンポーネントのフォルトツリーをシステムのモデルに統合して、障害の伝播を直感的に視覚化

参考文献

タイトル	Safety analysis of a complex system using component-oriented fault trees
出願日	2013/11/18
出願番号	US14082506A
出願人	Boeing Co.

脅威モデルの作成を簡易化／迅速化するテンプレート化技術は、連鎖的なシステムにおいても適用可能であり、SoS全体の脅威の波及を捕捉可能

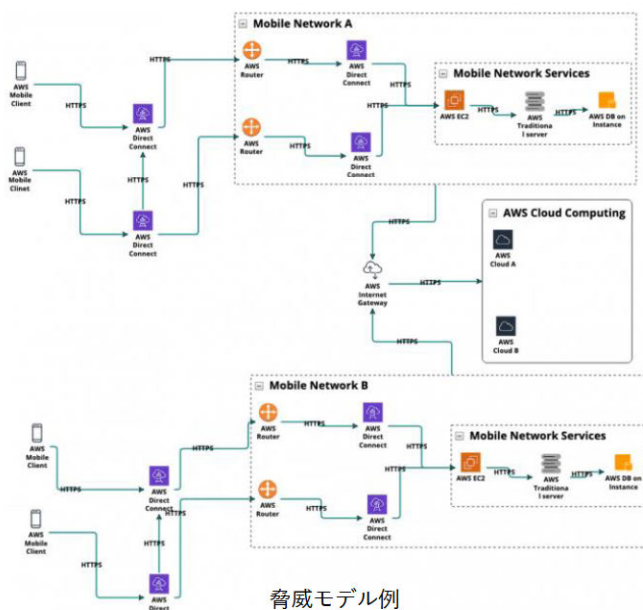
会社概要

会社名	ThreatModeler
所属国	米国
業種	情報通信
売上（2020年）	-
Webサイト	https://threatmodeler.com/

事業概要

- 2010年に設立されたスタートアップ企業であり、脅威モデリングプラットフォームを提供

技術概要



- 一般的に使用される脅威モデルを脅威モデルテンプレートとして保存
- 新しい脅威モデルを作成するための基盤として、わずかな変更を加えて再利用可能
- システムやコードの変更が頻繁に発生する環境において、迅速にセキュアな環境を構築できる
- 外部システムやインフラ等の共有コンポーネントとの相互作用に関しても連鎖的にモデルを構築できるため、それぞれの脅威がシステム全体にどのように影響するかの把握も可能

参考文献

タイトル	Systems and methods for automated threat modeling of an existing computing environment
出願日	2020/8/17
出願番号	US16947798A
出願人	Threatmodeler Software Inc.

人が複数のタスクを同時に行う際の作業負荷モデルの開発により、タスクやワークロードが整理され、SoSのパフォーマンスが向上

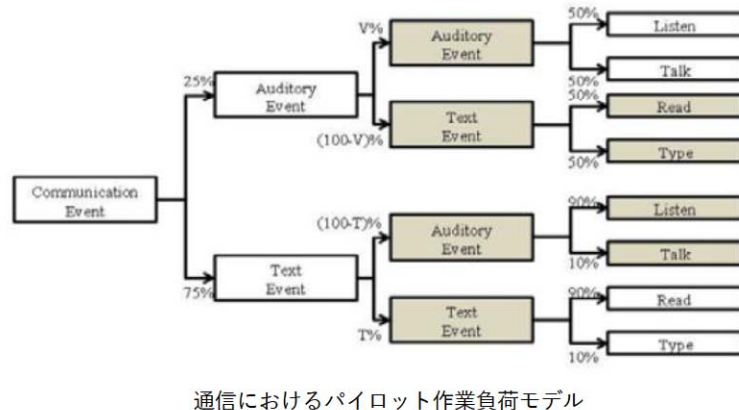
論文情報

研究者	John M. Colombi; Michael E. Miller; Michael F. Schneider; Major Jason McGrogan; David S. Long; John Plaga
所属国	米国
掲載雑誌	Systems Engineering
掲載年	2012
Webサイト	https://www.afit.edu/bios/bio.cfm?facID=34

研究概要

Predictive mental workload modeling for semiautonomous system design: Implications for systems of systems

技術概要



(研究されている技術の概要)

- Multiple Resource Theory (人が複数のタスクを同時に行う際には、単一の認知資源を複数のタスクに割り当てるのではなく、複数の認知資源を利用していると考えられる理論)を使用して作業負荷モデルを作成
- システム設計における人間の作業負荷分析の組み込み

(研究成果や今後の方向性)

- タスクの要求、タスク間の競合、ワークロードの低減の検討による、SoSのパフォーマンス向上

人と自律的なサイバーフィジカルシステムの協働についてのフレームワークを用いて、適切に人を自律ループに組み込んだシステムを設計

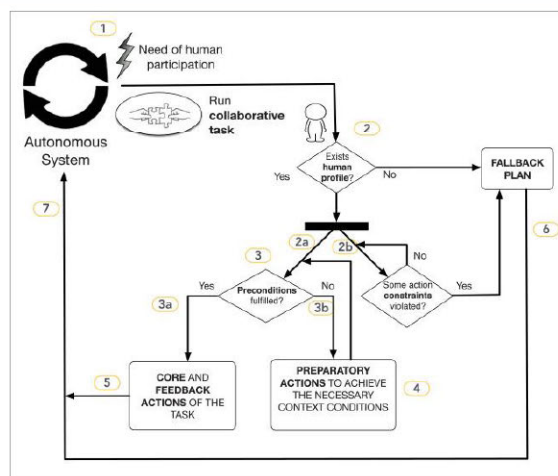
論文情報

研究者	Miriam Gil; Manoli Albert; Joan Fons; Vicente Pelechano
所属国	スペイン
掲載Journal	International Journal of Human-Computer Studies
掲載年	2019
Webサイト	http://www.upv.es/ficha-personal/vpelecha

研究概要

Designing human-in-the-loop autonomous Cyber-Physical Systems

技術概要



人間と自律的なCPSの協働

(研究されている技術の概要)

- 自律的なサイバーフィジカルシステム(CPS)においても、より適切にタスクを実行するため人間の介入が必要

- 人をCPSの自律ループに統合することの技術的な課題や制約を特定し、CPSにおける人と自律的なCPSの協働についてのフレームワークを示し、そのフレームワークを設計に用いる方法を提供

(研究成果や今後の方向性)

- フレームワークを適用して自動運転車のプロトタイプを作成し、このプロトタイプで人間の統合が仕様で定義されているとおりに動作するかどうかを確認

人が関わるインシデントの分析に用いられる各種手法の有用性を評価して、事故発生後の遡及的な検証において適切な分析手法を確認

論文情報

研究者	Neville A. Stanton; Laura A. Rafferty; Alison Blane
所属国	英国
掲載雑誌	Journal of Battlefield Technology
掲載年	2012
Webサイト	https://www.southampton.ac.uk/engineering/about/staff/ns4c08.page

研究概要

Human factors analysis of accidents in system of systems

技術概要

(研究されている技術の概要)

- インシデントの分析に用いる、AcciMaps、Human Factors Analysis Classification System(HFACS)、Systems Theory Accident Model and Process(STAMP)、Event Analysis of Systemic Teamwork(EAST)の4つの分析手法を11の基準に従って評価

(研究成果や今後の方向性)

- 事故発生後の遡及的な検証だけでなく事故予測等のプロスペクティブな検証にも使用できる分析手法の確認

Barrier certificateなどの技術を用いて、安全性を確保しながらリモートで試験可能なマルチロボット制御技術

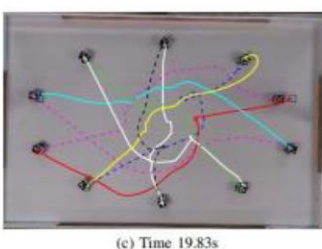
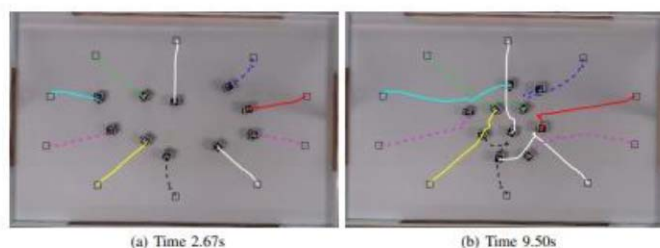
研究機関情報

研究機関	Georgia Institute of Technology
所属国	米国
代表研究者	Magnus Egerstedt
配分額	1,000(千ドル)
研究期間	2015～2018
Webサイト	http://magnus.ece.gatech.edu/index.html

研究概要

CPS: TTP Option: Synergy: Safe and secure open-access multi-robot systems

技術概要



Barrier certificateを用いたポジション交換

(研究されている技術の概要)

- モバイルロボットが協調的に行動を調整できるマルチロボットの実証実験において、Barrier certificateなどを用いて、安全性を担保する
- 現地のオペレータの負傷や機器の損傷を回避できるように安全性を担保しながら、ロボットのアルゴリズムをリモートでリアルタイムにテストできるような検証環境の構築を行う

(研究成果や今後の方向性)

- 米国の機関のロボット工学者が世界クラスのマルチロボット実証実験環境を利用可能に

交通にかかわるサイバーフィジカルシステムでは、複数の既存のサブシステムをテストするモデルの統合により、より良いシミュレーションを達成

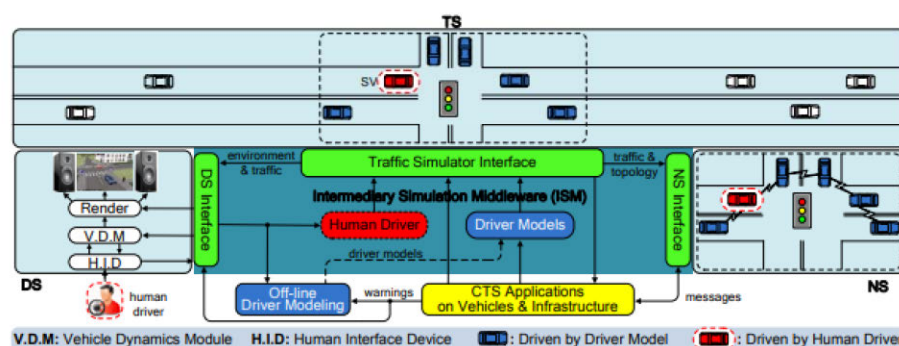
論文情報

研究者	Yunfei Hou; Yunjie Zhao; Aditya Wagh; Longfei Zhang; Chunming Qiao; Kevin F. Hulme; Changxu Wu; Adel W. Sadek; Xuejie Liu
所属国	米国、中国
掲載論文	IEEE Transactions on Vehicular Technology
掲載年	2016
Webサイト	https://www.csusb.edu/we-define-the-future/spotlight/532739

研究概要

Simulation-based testing and evaluation tools for transportation Cyber-Physical Systems

技術概要



統合シミュレーション

(研究されている技術の概要)

- 輸送サイバーフィジカルシステム(TCPS)については、土木工学、コンピュータサイエンス、及び関連分野でさまざまな独自のシミュレーションモデルが提案されている
- 特に、輸送、通信、及び人的要因で使用するモデルを組み合わせることで、よりよいシミュレーション手法を開発する

(研究成果や今後の方向性)

- ヒューマンファクターのより良いモデルの入れ込みにより、更なる精度向上が期待できる

モジュールプロセス固有のデータから仮想モジュールを作成し、それらを通信を介して結合して、システム全体のシミュレーションを実行

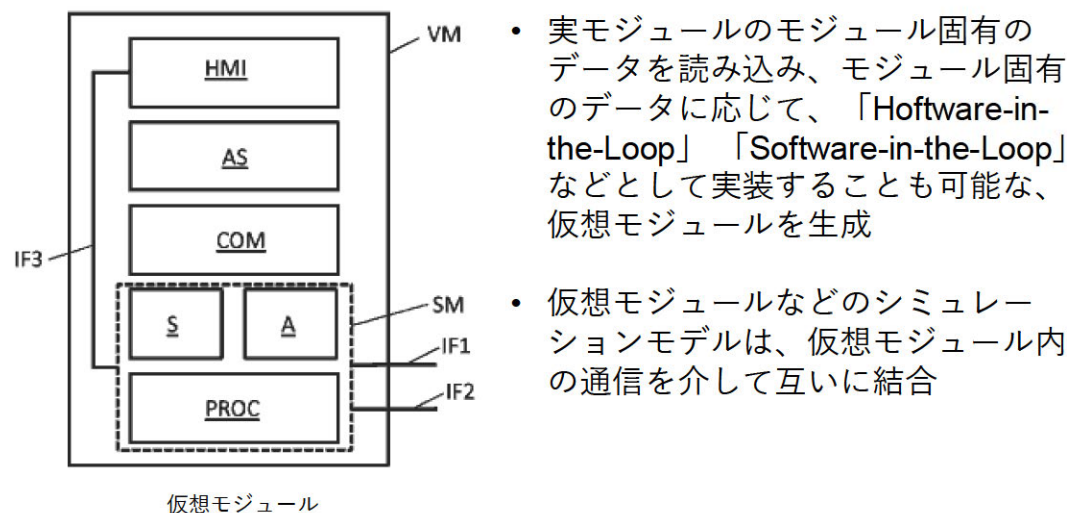
会社概要

会社名	Siemens
所属国	ドイツ
業種	電気機器
売上（2020年）	68,300(百万ドル)
Webサイト	https://new.siemens.com/jp/ja.html

事業概要

- 電子機器、情報通信、インフラ、モビリティ、ヘルスケア等の分野における製造／システムソリューション事業
- さまざまなシステム、機器、デバイスを組み合わせ、産業界に新しい価値を創造

技術概要



参考文献

タイトル	Method and device for computer-assisted simulation of a modular technical system
出願日	2019/10/30
出願番号	WO2019EP79651A
出願人	Siemens Aktiengesellschaft

人間や環境を含むインフラや都市に関するデータを取得し、モデリングや可視化を可能にし、シミュレーション用テストケースを提供

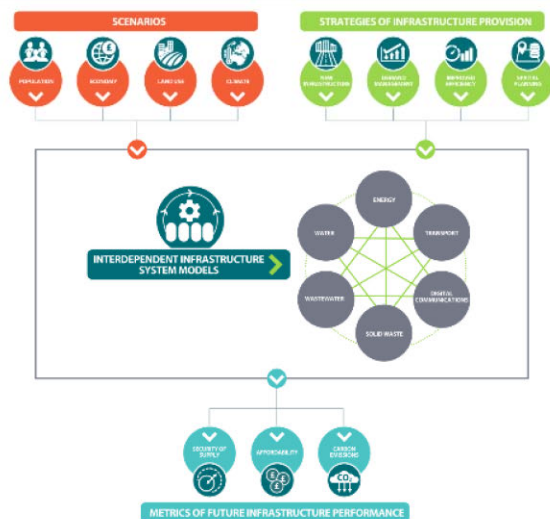
研究機関情報

研究機関	University of Oxford
所属国	英国
代表研究者	Jim William Hall
配分額	10,796(千ドル)
研究期間	2017～2021
Webサイト	https://www.eci.ox.ac.uk/people/jhall.html

研究概要

UKCRIC National infrastructure database, modelling, simulation and visualisation facilities

技術概要



インフラシステムオブシステムモデリングプラットフォーム

(研究されている技術の概要)

- インフラや都市に関するデータの取得と分析により、複雑なインフラ／都市のモデリングや可視化を研究している
- インフラ資産とネットワーク、人間と自然環境に関する基本的なデータセットとシミュレーション用のテストケースを提供

(研究成果や今後の方向性)

- 高性能コンピュータやシミュレーションモジュールの開発により、システムオブシステムズのシミュレーションを可能とする
- 複雑かつ高次元のシミュレーションを実施し、可視化を想定
- 人口増加や技術革新、気候変動等の変化に対して、都市インフラがどのように機能するか、といったシミュレーションを活用することで、政府や当局の戦略的意思決定に資することが目的

より安価にロバストを考慮したシミュレーションを可能にするハイブリッドサロゲート/メタヒューリスティックベースのアルゴリズムを開発

論文情報

研究者

Amir Parnianifard; Ali Zemouche;
Ratchatin Chanchaen; Muhammad
Imran; Lunchakorn Wuttisittikulij

所属国

タイ、フランス、英国

掲載論文

PloS one

掲載年

2020

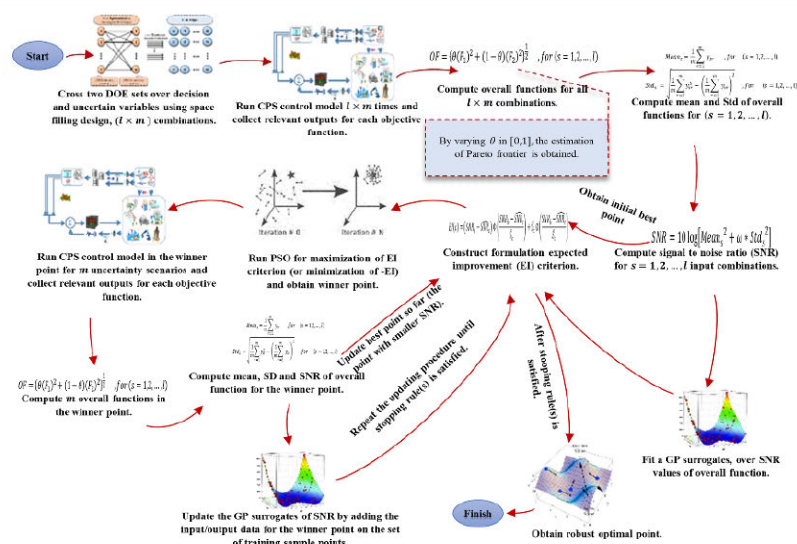
Webサイト

<https://www.eng.chula.ac.th/en/staff/assoc-prof-lunchakorn-wuttisittikulij-ph-d>

研究概要

Robust optimal design of FOPID controller for five bar linkage robot in a Cyber-Physical System: a new simulation-optimization approach

技術概要



(研究されている技術の概要)

- コンピュータシミュレーションにおいて、ロバストを考慮したより安価な最適化の計算方法を開発する

(研究成果や今後の方向性)

- 効率的な大域的最適化におけるサロゲートモデルの利点と最適な結果の収束におけるメタヒューリスティックの利点をもつ、新しいハイブリッドサロゲート/メタヒューリスティックベースのロバストシミュレーション最適化アルゴリズムを開発する

ロバストシミュレーション最適化のアプローチ

システムのどの部分にモジュラー性をもたせるかは必要な機能とコストの兼ね合いとなり、最適レベルを決定するフレームワークが開発されている

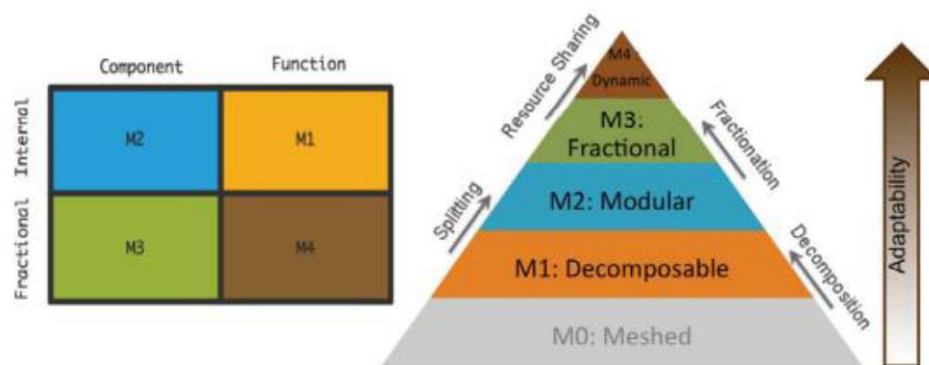
論文情報

研究者	Babak Heydari; Kia Dalili
所属国	米国
掲載論文	Procedia Computer Science
掲載年	2012
Webサイト	https://www.stevens.edu/

研究概要

Optimal system's complexity, an architecture perspective

技術概要



モジュラー設計の最適レベルを決定するためのピラミッドモデル

(研究されている技術の概要)

- 複雑なシステムにおける、モジュラー設計の最適レベルの検討のための、環境の空間的及び時間的異質性、システムの適応性、及びモジュール性のためのコストが組み込まれた設計フレームワークの開発

(研究成果や今後の方向性)

- モジュラー設計の最適レベルを決定するための、モジュール性の機能的及び物理的次元を考慮に入れた4レベルのピラミッドを開発

共通のプラットフォームに、障害に対する保証のレベルが異なるアプリケーションを効率的に統合するための、切り分けと結合のバランス

研究機関情報

研究機関	University of York
所属国	英国
代表研究者	Alan Burns
配分額	1,033(千ドル)
研究期間	2013～2016
Webサイト	https://www.cs.york.ac.uk/people/burns

研究概要

Mixed criticality embedded systems on many-core platforms

技術概要

(研究されている技術の概要)

- 障害に対する保証のレベルの異なるアプリケーションを共通のプラットフォームに統合するために、安全性を保証するための「パーティション化」と効率的なリソース使用のための「共有」のバランスを調整
- メニーコアプラットフォームにおいて、適切なスケジューリングスキームやランタイム制御を開発し、検証や効果のシミュレーションを実施

(研究成果や今後の方向性)

- リソース使用率の大幅な向上と消費電力の削減

サブシステムのモジュールとしての切り分け方により、サブシステムの性能のパフォーマンスのトレードオフを改善することができる

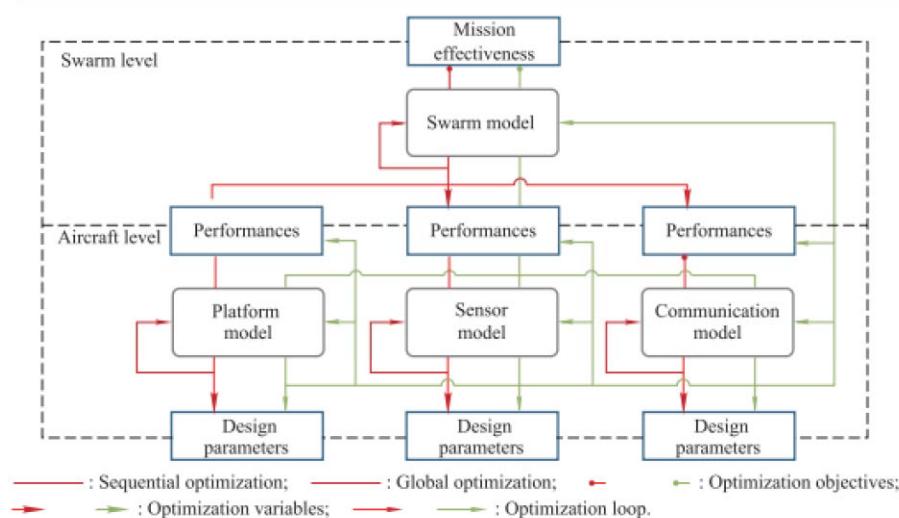
論文情報

研究者	Zhang Ruiwen; Song Bi-feng; Pei Yang; Yun Qijia
所属国	中国
掲載論文	Journal of Systems Engineering and Electronics
掲載年	2019
Webサイト	https://en.nwpu.edu.cn/

研究概要

Improved method for subsystems performance trade-off in system-of-systems oriented design of UAV swarms

技術概要



設計フレームワーク

(研究されている技術の概要)

- マルチUAVの設計におけるサブシステムのパフォーマンスのトレードオフの改善のため、サブシステムの分解を伴う設計フレームワークを開発

(研究成果や今後の方向性)

- プラットフォーム、センサー、及び通信を同等に重要なサブシステムとして扱い、運用戦略をトレードオフに統合

モジュールの接続に用いられるAPIのプロバイダとクライアントのスムーズな相互作用のため、検証プラットフォームが開発されている

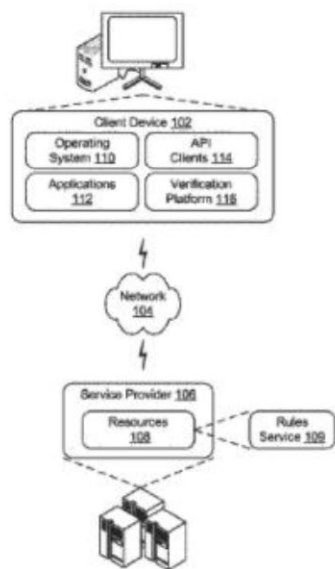
会社概要

会社名	Microsoft
所属国	米国
業種	ソフト開発、システム運用
売上（2020年）	143,015(百万ドル)
Webサイト	https://www.microsoft.com/ja-jp

事業概要

- デバイスからクラウドサービスまで多種多様な製品・サービスの開発・提供

技術概要



ステートフルルール検証プラットフォーム

- ステートフルルール検証プラットフォーム。仕様言語を実装して、APIプロバイダとAPIクライアントを提供する中央モジュールを持つターゲットシステムのテストに使用されるルールの定義を提供。ルールは、APIプロバイダとAPIクライアント間の相互作用に関連する状態要素の遷移に関して定義できる
- 仕様言語に従って定義されたルールにより、ランタイム検証が可能になり、チェックを実装するランタイムコードが自動的に生成され、インターセプトされたシステムコールの動作をテストするために挿入される

参考文献

タイトル	API Rules Verification Platform
出願日	2013/6/14
出願番号	US13918851A
出願人	Microsoft Technology Licensing LLC

SoSでは様々な階層における安定した通信が重要になり、本特許では運搬系SoSの車両に安定した無線リソースを割り当てる方法について記載

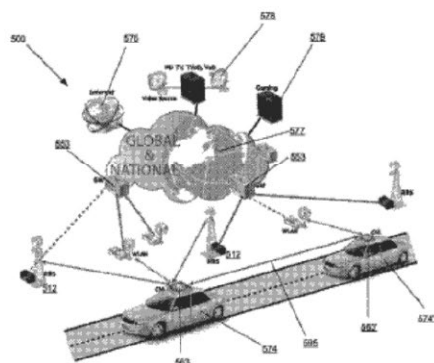
会社概要

会社名	Ericsson
所属国	スウェーデン
業種	通信機器
売上（2020年）	-
Webサイト	https://www.ericsson.com/en

事業概要

- ・ 移動及び固定通信業者へ通信機器・サービスを提供

技術概要



複数の移動通信モジュールを含む無線ネットワーク

- ・ 無線端末を備えた無線通信ネットワークで無線リソースを割り当てる方法
- ・ 無線接続は、車両に関連付けられた移動通信モジュールを介して、無線端末ユニットと無線通信ネットワークのノードとの間に確立できる。車両は経路に沿って移動し、移動体通信モジュールは、経路に沿った異なるタイプのネットワークに関連付けられた少なくとも2つのネットワークノードとの無線接続を確立するように構成され得る。ネットワークカバレッジを持たないエリアを検出し、車両が検出されたエリアに入る前に所定の数のパケットをバッファリングして、無線通信システムへの接続の中断がないように構成され得る

参考文献

タイトル	Methods for assigning radio resources for mobile devices connected to a mobile communication module and related systems and devices
出願日	2011/8/4
出願番号	US13198605A
出願人	Ericsson

特許では、モデル駆動型のセキュリティシステムにより、セキュリティ要件を自動的にモデル化するものが目立つ

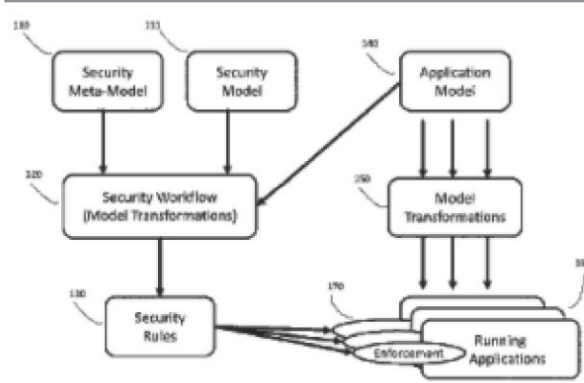
会社概要

会社名	Object Security
所属国	米国
業種	情報通信
売上（2020年）	-
Webサイト	https://objectsecurity.com/

事業概要

- セキュリティポリシーの自動化、サプライチェーンのリスク分析の自動化などセキュリティの簡素化・自動化を提供するプロバイダ

技術概要



モデル駆動型セキュリティシステム

- セキュリティ要件を高レベルの抽象化でモデル化
- 入力はドメイン固有言語(DSL)で表現され、人間の介入を最小限に抑えて、強制可能なセキュリティルールに変換

参考文献

タイトル	Automated and adaptive model-driven security system and method for operating the same
出願日	2015/1/22

出願番号 US14602935A

出願人 Object Security LLC

プログラムコードの特定のユニットをテストするように自動的に構成されたユニットテストを用いて、効率的な分析を行う

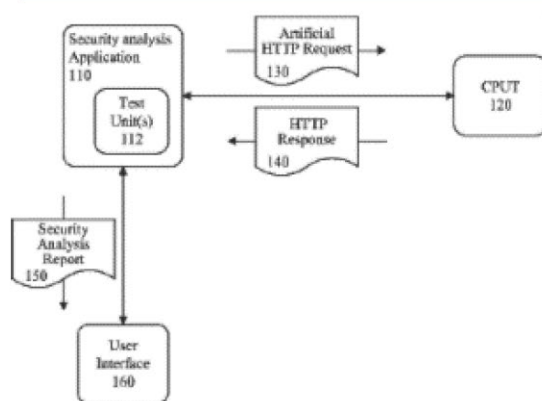
会社概要

会社名	International Business Machines
所属国	米国
業種	IT・通信
売上（2020年）	73,620(百万ドル)
Webサイト	https://www.ibm.com/jp-ja

事業概要

- ITソリューション導入
- ソフトウェア／ハードウェアの開発・製造・保守・運用

技術概要



ユニットテストを自動的に成するためのシステム

- テスト対象のコンピュータプログラム (CPUT) を分析して、潜在的なセキュリティの脆弱性に関連するデータを特定
- 潜在的な脆弱性に関連するデータを識別するため、プロセッサを介したCPUTの分析や、CPUT内のプログラムコードの特定のユニットをテストするように構成された自動的に合成されたユニットテストを用いる
- CPUTのセキュリティ脆弱性を特定し、セキュリティ分析レポートを出力

参考文献

タイトル	Automatische synthese von einheitentests fuer sicherheitstests
出願日	2013/1/17
出願番号	DE112013000485A
出願人	International Business Machines Corp

フィジカルとサイバーの両方で脅威をモデリングして、シミュレーションにより攻撃防止及び軽減の方法を得る

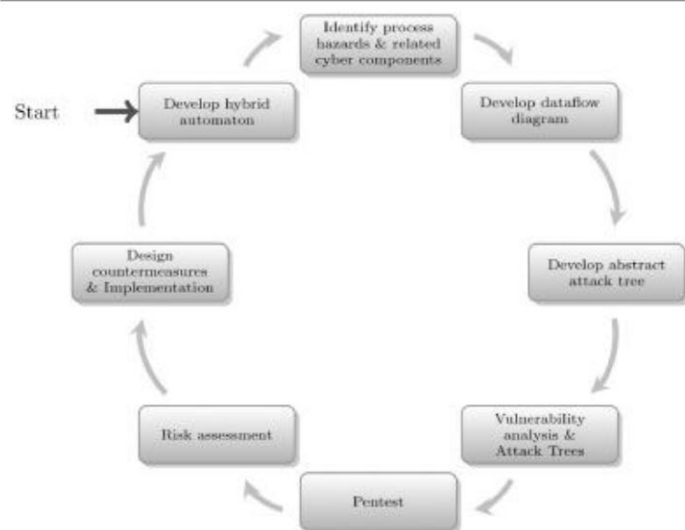
論文情報

研究者	Ashraf Tantawy; Sherif Abdelwahed; Abdelkarim Erradi; Khaled Bashir Shaban
所属国	米国、カタール
掲載論文	Computers & Security
掲載年	2020
Webサイト	http://qufaculty.qu.edu.qa/khaled-shaban/

研究概要

Model-based risk assessment for cyber physical systems security

技術概要



リスク評価フロー

(研究されている技術の概要)

- 実際の産業用コントローラーと通信プロトコルを備えたサイバーフィジカルシステム(CPS)検証環境を利用して、CPSのセキュリティリスクを評価するための統合アプローチの開発

(研究成果や今後の方向性)

- リスク評価は、最初に物理的な脅威を特定し、ハイブリッドオートマトンを使用して数学モデルを導出し、システムの潜在的な危険な状態を列挙。次に、ネットワーク及びデータフローモデルを使用してサイバーシステムを分析し、特定された危険につながる可能性のある攻撃シナリオを作成。最後に、攻撃シナリオが検証環境で実行され、攻撃を防止及び軽減するために取り得る方法が観察される

確立ゲームモデルに基づいたセキュリティ意思決定アプローチで、攻撃者と防御者の間の相互作用を特徴付け、最適な防御戦略を作成

論文情報

研究者	Kaixing Huang; Chunjie Zhou; Yuanqing Qin; Weixun Tu
所属国	中国
掲載論文	IEEE Transactions on Industrial Electronics
掲載年	2020
Webサイト	http://english.hust.edu.cn/

研究概要

A game-theoretic approach to cross-layer security decision-making in industrial Cyber-Physical Systems

技術概要

(研究されている技術の概要)

- 現状の産業用サイバーフィジカルシステム(ICPS)のセキュリティ対策には、高度に組織化されたサイバー攻撃から防御するための積極的な意思決定機能がない
- 確率ゲームモデルに基づくセキュリティ意思決定アプローチで、ICPSにおける攻撃者と防御者の間の相互作用を特徴付け、システムの損失を最小限に抑えるための最適な防御戦略を生成

(研究成果や今後の方向性)

- ICPSのクロスレイヤーセキュリティゲームモデルを構築する実用的な方法を提供し、Hardware-in-the-Loopシミュレーション環境を用いたケーススタディを実行し、実現性を示した

安全なデータ転送を可能にするブロックチェーン技術は価格、拡張性、遅延等の課題によりSoSへの利用が困難だったが、課題が克服されつつある

研究機関情報

研究機関	Grid7
所属国	米国
代表研究者	David Cohen
配分額	1,149(千ドル)
研究期間	2018～2020
Webサイト	https://taekion.com/

研究概要

E-Blockchain: A scalable platform for secure energy transactions and control

技術概要



Taekionセキュアファイルシステム

(研究されている技術の概要)

- 産業用IoTで展開され则认为られている膨大な数のインターネット接続デバイスは、現状の集中型の管理のアプローチでは、サイバーセキュリティの脅威に適切に対処することができない
- 信頼できるデータの作成を支援できるブロックチェーンテクノロジーであるが、現状では、過剰なトランザクション料金、スケーラビリティの問題、許容できない遅延などの課題があり、サイバーフィジカルシステムに適さない

(研究成果や今後の方向性)

- 電力システムとIoTデバイス間のサイバーセキュアトランザクションをサポートする、ブロックチェーンベースのソフトウェアとサイバーセキュリティプラットフォームのアプリケーションを開発

ロバスト制御のアプローチのひとつ「冗長センサ」からの信号を予想される信号と比較するなどして冗長センサの障害を自動で判別

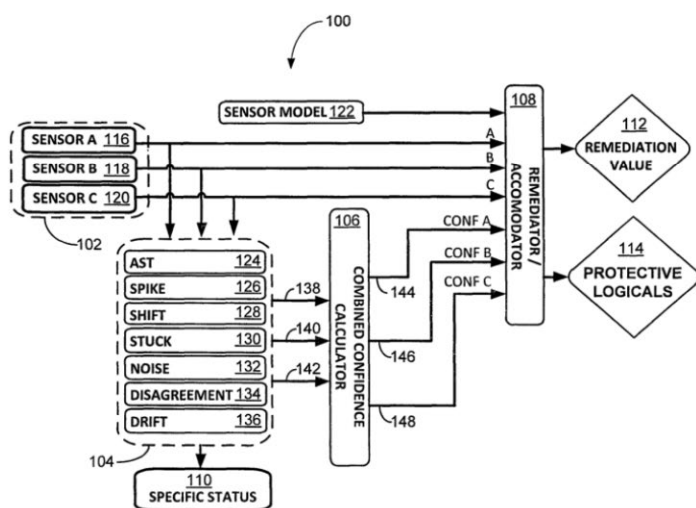
会社概要

会社名	General Electric
所属国	米国
業種	重工業、航空宇宙産業、電気機器
売上（2020年）	79,619(百万ドル)
Webサイト	https://www.ge.com/jp/

事業概要

- ソフトウェア融合型の産業機器とソリューションの提供

技術概要



障害検出、分離、及び修復システムのブロック図

- 発電所などのロバスト性を高めるためのアプローチとしてセンサを冗長化する方法があるが、(人の手を介さず)自動的に障害のタイプを判別することが困難
- それに対して、冗長化されたセンサからの信号を予想される信号と比較するなどして、通信の喪失やチャネルの故障など、障害のタイプを区別

参考文献

タイトル	Systems, methods, and apparatus for detecting shifts in redundant sensor signals
出願日	2013/4/8
出願番号	US13878396A
出願人	General Electric Company

イベントベースのスケジューリングを採用するサイバーフィジカルシステムにおいて、高速フィードバックを特徴とするモデル予測制御を行う

論文情報

研究者	Jianhua Wang; Yan Song
所属国	中国
掲載雑誌	IEEE Transactions on Industrial Informatics
掲載年	2020
Webサイト	https://en.usst.edu.cn/index.htm

研究概要

Resilient RMPC for Cyber-Physical Systems with polytopic uncertainties and state saturation under TOD scheduling: an ADT approach

技術概要

(研究されている技術の概要)

- 伝送負荷を軽減するため、Try-Once-Discardプロトコル(決定論的イベントベースのスケジューリングプロトコル)を採用しているサイバーフィジカルシステムにおいて、復元性やロバスト性、指数安定性が保証されるようにコントローラを設計して、ロバストモデル予測制御(高速に最適化問題を計算してフィードバック制御)を行う

(研究成果や今後の方向性)

- リアプノフ関数(系の微分方程式を解くことなしに系の安定性を論ずる)や平均滞留時間(ADT)を用いて制御を可能にする

ファジイ理論で用いられるメンバシップ関数の設計と分析を容易にして、モデル学習時のアルゴリズムのロバスト性をより容易に確立

論文情報

研究者	Mohit Kumar; Yihua Mao; Yuhao Wang; Taorong Qiu; Yang Chenggen; Weiping Zhang
所属国	中国、ドイツ
掲載雑誌	Information Sciences
掲載年	2017
Webサイト	https://www.uni-goettingen.de/en/prof.+dr.+mohit+kumar/605765.html

研究概要

Fuzzy theoretic approach to signals and systems:
Static systems

技術概要

(研究されている技術の概要)

- すべてのシステム変数とパラメータを不確実であると想定し、システム変数とパラメータのメンバシップ関数(あいまいな量を表現するのに使用し、その概念にどの程度属しているかを0から1で出力)の設計と分析を容易にするための数学的理論、パラメータを推定するためのアルゴリズムを開発

(研究成果や今後の方向性)

- ノイズの影響を受ける多入力単一出力の静的システムにおいて、方法論を適用して、適応フィルタアルゴリズムを得、時間領域分析を行い、アルゴリズムのロバスト性と収束特性を確立
- モデルの学習時の不確実性に対処可能な技術

自動運転における標識の誤認識などに利用され得る、人工的摂動による攻撃を、遺伝的アルゴリズムを用いて作成したサンプルを利用して防御

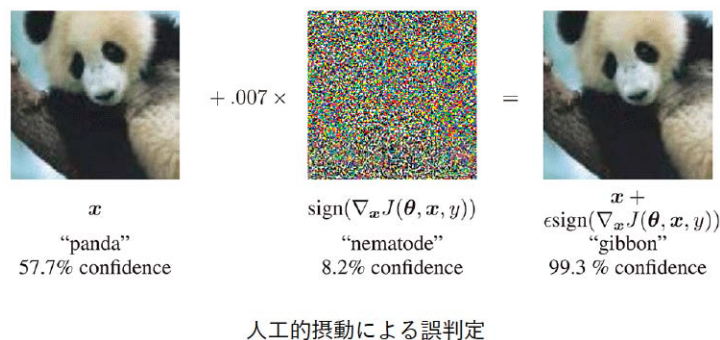
会社概要

会社名	Zhejiang University of Technology
所属国	中国
業種	大学・研究所
売上（2020年）	-
Webサイト	http://www.wsc.zjut.edu.cn/zjuten/index.jsp

事業概要

- 浙江省の主要大学であり、工学、科学、教養、法、経済学、薬学、管理、教育など、さまざまな科目のプログラムを提供

技術概要



- 画像上の人工的摂動 (小さな攪乱) に基づく画像分類器に対する攻撃への防御
- 遺伝的アルゴリズムにより、効果の高い摂動とそれに対抗するサンプルを得、分類器の学習に使用

参考文献

タイトル	Image classifier adversarial attack defense method based on disturbance evolution
出願日	2018/4/4
出願番号	CN201810299242A
出願人	Univ Zhejiang Technology

自動運転において、人間の思考/行動を活用しロバストなアルゴリズムを開発する研究開発事例も存在し、同様技術はCPSにも展開が可能

研究機関情報

研究機関	Cornell University
所属国	米国
代表研究者	Mark Campbell
配分額	1,399(千ドル)
研究期間	2017～2021
Webサイト	https://campbell.mae.cornell.edu/

研究概要

S&AS: INT: Inference, reasoning, and learning for robust autonomous driving

技術概要

(研究されている技術の概要)

- 人間は詳細な地図や高精度のGPSやセンサがなくても運転可能で、ガイダンスに必要な情報は少なく、学習を通じて運転技術を向上させることができる
- 一方、自動運転では上記の情報なしには運転不可能
- 人間のドライバーをガイドとして活用することで、リアルタイムで状況を認識して後の行動を予測可能なアルゴリズムを開発する
- 当アルゴリズムの特徴として、短期(リアルタイム)と長期(学習)の両方でミスを検出して克服するロバスト性を持つことが挙げられる

(研究成果や今後の方向性)

- 検出、シーン推定、予測、及び異常/間違いの検出と学習のためのロバストな知覚パイプラインの開発
- 自動運転にとどまらず、本PJの成果はロボット工学やサイバーフィジカルシステムにも転用が可能

現状のSoSのレジリエンスの向上には非線形にコストがかかるが、生物学に着想を得たネットワーク設計により有利にSoSの回復力の向上を見込む

論文情報

研究者	Bryan C. Watson; Stephen M. Malone; Marc J. Weissburg; Bert Bras
所属国	米国
掲載論文	Journal of Mechanical Design
掲載年	2020
Webサイト	https://ecdm.gatech.edu/

研究概要

Adding a detrital actor to increase system of system resilience: A case study test of a biologically inspired design heuristic to guide sociotechnical network evolution

技術概要

(研究されている技術の概要)

- 障害後のSoSのパフォーマンスは、SoSのハード(物理設計)またはソフト(人間の介入)による向上が考えられるが、レジリエンスを向上させるための現在のアプローチでは、SoSスケールとともにコストと人の手の必要性が非線形に増加する
- 生物学的に着想を得たネットワーク設計によるSoSの回復力の向上と、そのシステム回復力を新しく開発したSystem of System Resilience Measurement(SoSRM)で測定

(研究成果や今後の方向性)

- 生物学的に着想を得たネットワーク設計が社会技術的なSoSのレジリエンスを向上

外乱を吸収するイベントトリガ制御のためのフィルタを開発し、SoSへの予期せぬサイバー攻撃への対応力を増強

論文情報

研究者	Zhou Gu; Xiaohong Zhou; Tao Zhang; Fan Yang; Mouquan Shen
所属国	中国
掲載Journal	ISA transactions
掲載年	2019
Webサイト	https://www.qust.edu.cn/

研究概要

Event-triggered filter design for nonlinear cyber-physical systems subject to deception attacks

技術概要

(研究されている技術の概要)

- ファジーモデルベースのサイバーフィジカルシステムにおけるイベントトリガ制御(計測データの送信や制御入力 of 更新を必要なときだけ行う制御法)のフィルタ設計
- イベントトリガ制御で、サンプリングデータに予期しない外乱から生じる急激な変化がある場合、従来のイベントトリガ制御では意図しないイベントがトリガされる可能性があるが、これを防ぐ

(研究成果や今後の方向性)

- フィルタが設計され、フィルタリングエラーシステムを漸近的に安定させる十分条件が確立
- サイバーフィジカルシステムにおけるサイバー攻撃に対応可能

SoS全体としての可用性を高める為、各システムの可用性の定量化を行い必要に応じて他システムでの代替を判断可能な技術

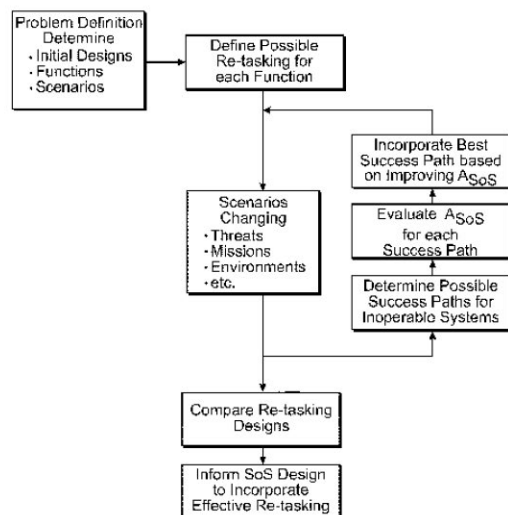
会社概要

会社名	Sandia National Laboratories
所属国	米国
業種	大学・研究所
売上（2020年）	-
Webサイト	https://www.sandia.gov/index.html

事業概要

- 国家安全保障に関わる研究
(戦略分野：核兵器、国家安全保障プログラム、エネルギー、グローバルセキュリティ)

技術概要



re-taskingの効果的な設計を決定するための方法

- SoS内での効果的なre-tasking(代替可能性や冗長性)を決定し、システムを組み立てるプログラム技術
- SoSの可用性を定量化して、その最大化のために、動作しなくなった、または損傷したシステムを同じ機能を満たすことができるシステムに置換することが可能
- SoSの全体的な運用可用性や、未知の条件／変化に対する適応性と回復力の向上に資する技術である

参考文献

タイトル	Methods, systems and computer program products for determining systems re-tasking
出願日	2014/10/22
出願番号	US14521285A
出願人	Honeywell International Inc.(Sandia National Laboratoriesの運営会社)、Intera Co Ltd

サイバーフィジカルシステムをオンデマンドでカスタマイズできる機能は不測の事態に対する備えとなる

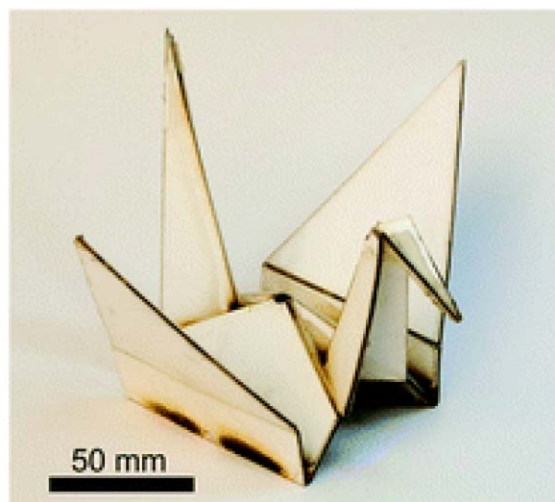
研究機関情報

研究機関	Massachusetts Institute of Technology
所属国	米国
代表研究者	Daniela Rus
配分額	6,600(千ドル)
研究期間	2012～2019
Webサイト	http://danielarus.csail.mit.edu/

研究概要

Collaborative research: an expedition in computing for compiling printable programmable machines

技術概要



セルフフォールディングする複合材料

(研究されている技術の概要)

- 物理的なパーツ自体ではなく、デザインのみをデジタルで保存して、サイバーフィジカルシステムをオンデマンドでカスタマイズすることを目指す

(研究成果や今後の方向性)

- デバイスの組み立てと動作の望ましい機能を提供するためのツール及び制御アルゴリズムの設計や、専門家でないユーザーが作成したプログラムにセーフガードを提供して、マシンを安全に操作できるようにする、デバイス固有及びタスク固有のプログラミング環境を生成する方法などを確立
- 不測の事態の他にも、遠隔地で人道援助や災害救援に従事する救助隊の後方支援の必要性を抑えるなどで有用

当然ながら、複数のシステムの連環構造においてはデータ／ストレージの物理的な隔離や冗長化、素早い復旧はレジリエンス上重要なファクタ

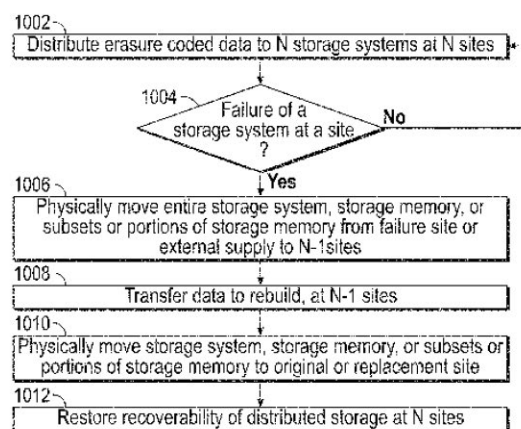
会社概要

会社名	Pure Storage
所属国	米国
業種	IT・情報通信
売上（2020年）	1,643(百万ドル)
Webサイト	https://www.purestorage.com/jp/

事業概要

- ディスクによる記憶装置にかわるオールフラッシュ・ストレージ・システムの製造、販売

技術概要



分散ストレージのディザスタリカバリ方法のフロー

- 複数のサイトにあるストレージシステムの1つに障害が発生した場合に、他のストレージシステムからデータを回復できるように、イレイジャーコーディングを採用
- ディザスタリカバリの際には、データを再構築するため、複数のストレージデバイスを物理的に移動し、データを転送することにより素早い復旧を見込む

参考文献

タイトル	Disaster recovery for high-bandwidth distributed archives
出願日	2018/1/31
出願番号	US15885670A
出願人	Pure Storage Inc.

意味決定システムに不可欠な説明可能性AI

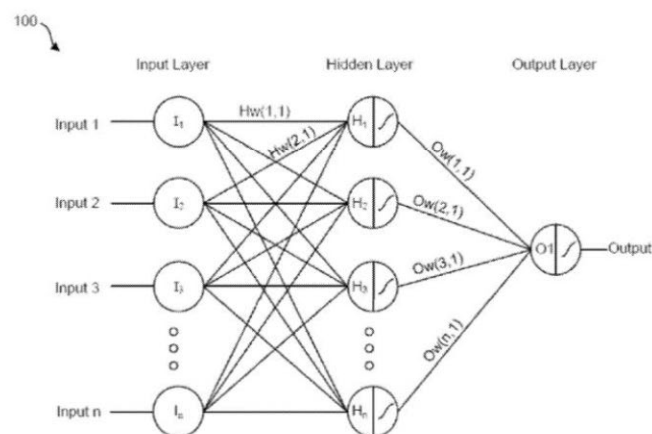
会社概要

会社名	フェア・アイザック
所属国	米国
業種	情報通信業
売上（2020年）	136,818（百万円）
Webサイト	https://www.fico.com/

事業概要

意思決定システム、収集代行システム、不正利用防止システム、信用度スコアリングシステム（FICOスコア）の開発・運用

技術概要



計算の複雑性の軽減が可能な
ニューラルネットワークのノード構造

- 意思決定や不正利用防止など、説明性の求められるアプリケーションに感度分析（Sensitivity Analysis）を適用
- 感度分析における計算の複雑性を軽減する技術
- 信用度スコアリングシステムにおいて、ホワイトボックス型AIであるFICO® Responsible AIを展開

参考文献

タイトル	Reduction of computation complexity of neural network sensitivity analysis
出願日	2013/09/18
出願番号	US14030834A
出願人	FAIR ISAAC CORPORATION

自動運転技術のための説明可能なAI

会社概要

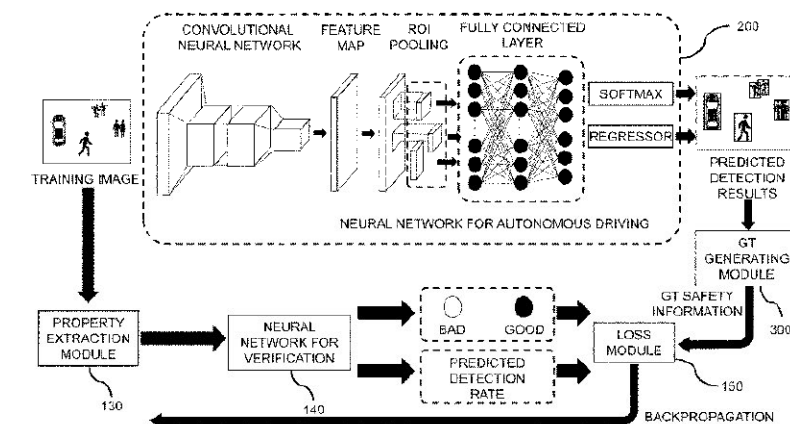
会社名	STRADVISION
所属国	韓国
業種	情報通信業
売上（2020年）	N/A
Webサイト	https://stradvision.com/

事業概要

自動車業界において画像処理技術のソリューションを提供。完全自動運転車の実用化を目指す

技術概要

- 自動運転等の生命に関わる技術では、AIの信頼性が特に求められる
- ドライバーに危険を知らせるアラートシステムにおいて、結果出力までの過程を検証する手法を開発
- 同社画像認識モデル「SVNet External」はレベル2~4の自動運転車両に導入されている



取得された画像に対して、画像の信頼性等をリアルタイムで検証することができる

参考文献

タイトル Learning method for providing functional safety by warning driver about potential dangerous situation by explainable AI which verifies detection processes of neural network for autonomous driving, involves learning device for verification

出願日 2019/12/23

出願番号 US16724428A

出願人 stradvision inc

ドメインフリーな機械学習モデルの信頼性評価技術

研究機関情報

研究機関	カリフォルニア大学アーバイン校
所属国	米国
代表研究者	Padhraic Smyth, Mark Steyvers
配分額	\$1,199,898
研究機関	2019/10/1-2023/9/30
Webサイト	https://www.ics.uci.edu/~smyth/index.html

技術概要

研究概要

Assessment of Machine Learning Algorithms in the Wild

- ・ AIには、ブラックボックス性があり、結果出力までのプロセスを理解することが難しい
- ・ これは、自動運転や医療診断などクリティカルな領域へAIを適用する際の障壁になる
- ・ 本プロジェクトでは、ブラックボックスモデルの信頼性を評価するアルゴリズムを開発
- ・ ResNet（画像データ）、BERT（テキストデータ）など産業界で既に利用されているモデルへの適用する論文を発表

深層学習型AIとも知識型AIとも異なる第三極のAI

研究機関情報

研究機関	名古屋大学
所属国	日本
代表研究者	鈴木 達也
配分額	44,330千円
研究機関	2019/04/01-2022/03/31
Webサイト	http://www.suzlab.nuem.nagoya-u.ac.jp/suzuki/index.html

研究概要

他者とのインタラクションを考慮したモデル予測型知能の創出と自動運転車両への実装

技術概要

- ・ 「モデル予測型知能」を提案
- ・ インタラクションにより、他者から行動データを取得し、そのデータを用いて他者行動モデルを構築・更新するフレームワーク
- ・ 他者行動モデルにより、相手の行動を予測した上で、自己の行動を最適化する
- ・ 既存の深層学習とは異なる安全性や他者との協調性に優れたアプローチ
- ・ 汎用的な技術であるが、自動運転システムをターゲットに設定

AIデバイスにおけるサイバー衛生

研究機関情報

研究機関	グリニッジ大学
所属国	英国
代表研究者	Georgios Loukas
配分額	£830,139
研究機関	2020/12-2023/11
Webサイト	https://www.gre.ac.uk/people/rep/las/george-loukas

技術概要

研究概要

CHAI: Cyber Hygiene in AI enabled domestic life

- 電子メールやウェブサイトには既知のサイバー攻撃対策がある一方、新興技術であるスマートデバイスにおいては、対策が十分でない（知見の不足及び機能の不足）
- そのために以下の4つの機能を提供する
 - サイバー攻撃対策リスクの評価
 - 説明可能性AIを用いたリスク診断情報の提供
 - ユーザーへの対策方法の提示
 - 説明可能性AIを使用するユーザーへのトレーニングの提供
- 特にサイバー攻撃を受けた際のリスクの高い住宅に関連するAI（温湿度センサーを利用するAIなど）をターゲットに設定
- ガススマートメータ会社など数社と提携実績あり



（参考）特許スコアリングにあたり、母集団作成に使用した検索式の一例

条件1	・タイトル／抄録／請求項に “System of systems” または “Cyber Physical Systems” が含まれる
条件2	・タイトル／抄録／請求項に “Security”、“Reliability”、“Safety Assurance”、“Safety Verification” 等安全性に関する単語が含まれる
条件3	・テキストフィールドに以下のような関連キーワードが含まれ、 かつIPCがG06（「計算または計数」に関する技術）で始まる ・ modeling ・ STAMP／STPA ・ robustness ・ systems resilience ・ real time alert ...
条件4	・ 出願年が2000年以降

(参考) 各母集団スコアリング結果基本統計量

母集団毎のスコアリング結果基本統計量

母集団のスコアリング結果基本統計量

	特許	論文	グラント
平均値	50.00	0.304	86,601
中央値	48.76	0.005	0
最大値	146.96	36.084	24,574,063
最小値	14.75	0	0
標準 偏差	9.99	1.391	793,483

(参考) 共起分析 グラント年次推移

※共起件数をスケール表示

少 多

words	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	total
'(sos', 'system of systems)' x 'security'	0	0	0	0	0	0	0	1	0	0	0	0	3	5	0	1	2	2	2	1	0	0	17
'(sos', 'system of systems)' x 'safety'	0	0	0	0	0	0	0	0	0	0	0	0	2	3	0	1	2	2	0	0	0	0	10
'(sos', 'system of systems)' x 'reliability'	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	2	1	2	0	0	0	0	7
'(sos', 'system of systems)' x 'cyber'	0	0	0	0	0	0	0	0	0	1	0	1	0	4	0	5	2	4	4	3	0	0	24
'(sos', 'system of systems)' x '(cps', 'cyber physical system)'	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	2	2	2	0	0	0	0	8
'(sos', 'system of systems)' x 'framework'	0	0	0	0	0	0	0	2	0	0	1	1	0	3	1	4	2	3	4	1	0	0	22
'(sos', 'system of systems)' x 'model'	0	0	0	1	0	0	4	4	1	3	1	2	3	12	1	7	8	9	4	6	0	0	66
'(sos', 'system of systems)' x 'application'	0	0	0	0	0	0	2	4	0	2	0	0	2	4	1	6	1	4	0	3	0	0	29
'(sos', 'system of systems)' x 'user'	0	0	0	0	0	0	0	0	1	0	1	0	0	3	0	0	1	1	0	1	0	0	8
'security' x 'safety'	0	0	0	0	0	0	0	0	2	1	2	0	7	7	11	18	11	18	25	20	6	0	128
'security' x 'reliability'	0	0	0	0	0	0	0	0	0	2	2	1	3	0	3	6	6	7	8	8	0	0	46
'security' x 'cyber'	0	0	0	0	0	0	0	2	4	6	7	13	19	29	31	45	34	47	71	50	7	0	365
'security' x '(cps', 'cyber physical system)'	0	0	0	0	0	0	0	2	3	6	3	10	12	14	8	34	23	34	42	31	0	0	222
'security' x 'framework'	0	0	0	0	0	0	0	1	2	2	1	7	4	9	8	21	13	11	18	9	0	0	106
'security' x 'model'	0	0	0	0	0	0	1	2	1	2	7	5	11	21	18	22	18	21	31	21	2	0	183
'security' x 'application'	0	0	0	0	0	0	0	1	2	3	5	9	7	11	15	18	15	32	40	18	5	0	181
'security' x 'user'	0	0	0	0	0	0	1	0	0	1	0	2	1	9	2	9	10	11	9	2	5	0	62
'safety' x 'reliability'	0	0	0	0	0	0	0	1	2	4	2	2	0	5	6	8	9	9	8	8	1	0	65
'safety' x 'cyber'	0	0	0	0	0	0	0	7	9	14	12	6	12	30	36	61	44	38	48	46	13	0	376
'safety' x '(cps', 'cyber physical system)'	0	0	0	0	0	0	0	2	9	12	10	7	13	25	24	54	40	33	34	34	7	0	304
'safety' x 'framework'	0	0	0	0	0	0	0	4	1	6	2	2	1	16	12	21	12	11	10	12	4	0	114
'safety' x 'model'	0	0	0	0	0	0	0	4	5	8	9	3	7	24	24	43	28	22	26	26	7	0	236
'safety' x 'application'	0	0	0	0	0	0	0	7	4	11	4	4	8	20	18	22	22	24	25	15	10	0	194
'safety' x 'user'	0	0	0	0	0	0	0	0	2	1	1	0	0	7	4	7	3	3	10	3	4	0	45
'reliability' x 'cyber'	0	0	0	0	0	0	0	3	3	9	5	4	5	10	13	29	15	22	19	15	3	0	155
'reliability' x '(cps', 'cyber physical system)'	0	0	0	0	0	0	0	2	2	6	5	3	2	9	8	18	13	12	9	11	3	0	103
'reliability' x 'framework'	0	0	0	0	0	0	0	2	0	5	2	0	3	2	2	5	1	8	4	5	0	0	39
'reliability' x 'model'	1	0	0	0	0	0	0	2	3	7	3	0	4	8	8	16	10	16	11	9	1	0	99
'reliability' x 'application'	1	0	0	0	0	0	0	2	0	7	4	3	0	6	9	9	11	16	6	5	3	0	82
'reliability' x 'user'	0	0	0	0	0	0	0	0	2	0	0	0	0	3	1	1	5	4	2	0	2	0	20
'cyber' x '(cps', 'cyber physical system)'	0	0	0	0	0	0	1	6	13	38	29	24	24	62	50	134	83	93	91	72	14	0	734
'cyber' x 'framework'	0	0	0	0	0	0	0	7	2	12	11	9	9	28	28	51	30	35	34	28	6	0	290
'cyber' x 'model'	0	0	0	0	0	0	0	8	7	23	28	17	20	66	56	107	66	76	81	52	15	0	622
'cyber' x 'application'	0	0	0	0	0	0	0	11	6	27	24	22	15	44	42	72	59	71	73	48	17	0	531
'cyber' x 'user'	0	0	0	0	0	0	0	0	2	5	3	3	5	12	10	25	18	21	26	10	7	0	147
'(cps', 'cyber physical system)' x 'framework'	0	0	0	0	0	0	0	3	2	10	9	7	6	20	17	44	20	21	17	23	6	0	205
'(cps', 'cyber physical system)' x 'model'	0	0	0	0	0	0	0	3	6	18	21	13	14	45	30	89	53	52	48	39	12	0	443
'(cps', 'cyber physical system)' x 'application'	0	0	0	0	0	0	0	2	6	24	19	16	16	35	22	54	43	51	45	31	11	0	375
'(cps', 'cyber physical system)' x 'user'	0	0	0	0	0	0	0	2	5	3	1	1	7	4	19	10	14	15	8	2	0	91	
'framework' x 'model'	0	0	0	0	0	0	1	8	2	9	11	6	7	26	24	33	25	31	22	29	6	0	240
'framework' x 'application'	0	0	0	0	0	0	1	6	2	10	9	9	4	21	6	22	19	20	23	19	6	0	177
'framework' x 'user'	0	0	0	0	0	0	1	0	0	1	1	2	0	5	5	9	9	3	8	6	0	0	50
'model' x 'application'	1	1	0	1	0	1	3	8	1	17	19	11	11	32	27	47	37	48	39	33	15	0	352
'model' x 'user'	0	0	0	0	0	0	2	0	4	1	3	1	2	11	7	14	11	13	14	9	7	0	99
'application' x 'user'	0	0	0	0	0	0	1	0	0	2	2	2	0	9	3	17	12	14	22	10	10	0	104

(参考) 共起分析 論文年次推移

※共起件数をスケール表示

少 多

words	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	total
'(sos', 'system of systems')' x 'security'	0	0	0	0	0	0	0	0	3	1	1	0	2	0	0	2	1	0	1	3	0	0	14
'(sos', 'system of systems')' x 'safety'	0	0	0	0	0	0	2	0	0	0	0	0	0	0	2	3	2	0	2	2	1	0	14
'(sos', 'system of systems')' x 'reliability'	0	0	0	0	0	0	0	0	1	0	0	1	3	3	0	1	2	0	1	2	1	0	15
'(sos', 'system of systems')' x 'cyber'	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	2	0	0	0	2	1	0	7
'(sos', 'system of systems')' x '(cps', 'cyber physical system)'	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
'(sos', 'system of systems')' x 'framework'	0	0	0	0	0	1	4	5	2	2	1	2	4	6	7	6	1	6	1	5	3	0	56
'(sos', 'system of systems')' x 'model'	0	0	0	0	0	2	7	5	9	14	9	9	13	13	12	19	11	13	9	9	7	0	161
'(sos', 'system of systems')' x 'application'	0	0	0	0	0	0	0	0	1	4	2	0	3	1	1	4	5	3	3	0	3	0	30
'(sos', 'system of systems')' x 'user'	0	0	0	0	0	0	0	1	2	0	0	1	1	1	0	0	1	3	0	0	2	0	12
'security' x 'safety'	0	0	0	0	0	0	0	0	0	0	0	0	2	1	4	4	4	3	13	11	15	0	57
'security' x 'reliability'	0	0	0	0	0	0	0	0	0	0	0	1	2	3	3	2	6	2	7	5	9	1	41
'security' x 'cyber'	0	0	0	0	0	0	0	0	1	0	3	1	10	6	16	12	24	39	43	43	56	2	256
'security' x '(cps', 'cyber physical system)'	0	0	0	0	0	0	0	0	0	0	0	0	1	1	3	2	5	3	6	7	9	0	37
'security' x 'framework'	0	0	0	0	0	0	0	1	0	0	1	0	2	4	2	11	7	10	7	10	13	1	69
'security' x 'model'	0	0	0	0	0	0	0	1	2	0	3	4	6	5	10	10	10	20	28	31	30	2	162
'security' x 'application'	0	0	0	0	0	0	0	1	0	1	1	3	4	4	4	6	10	14	14	14	26	0	92
'security' x 'user'	0	0	0	0	0	0	0	0	2	0	0	1	2	1	1	2	0	2	3	6	12	0	32
'safety' x 'reliability'	0	0	0	0	0	0	0	0	0	0	0	1	1	3	2	5	3	8	10	6	8	0	47
'safety' x 'cyber'	0	0	0	0	0	0	0	0	0	0	1	1	4	4	7	6	7	16	27	29	27	0	129
'safety' x '(cps', 'cyber physical system)'	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1	2	4	1	8	4	0	22
'safety' x 'framework'	0	0	0	0	0	0	1	1	1	0	2	0	1	6	3	6	5	3	5	6	11	0	51
'safety' x 'model'	1	0	0	0	1	0	2	0	0	1	1	0	2	10	9	12	12	13	18	18	21	0	121
'safety' x 'application'	0	0	0	0	1	0	0	0	0	1	1	1	1	3	5	8	4	7	17	15	17	0	81
'safety' x 'user'	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	3	1	0	1	3	6	0	15
'reliability' x 'cyber'	0	0	0	0	0	0	0	0	0	0	0	1	8	8	6	6	8	11	8	18	23	2	99
'reliability' x '(cps', 'cyber physical system)'	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	2	2	1	2	8	0	18
'reliability' x 'framework'	0	0	0	0	0	0	0	0	0	0	0	0	1	4	3	2	2	5	3	3	7	1	31
'reliability' x 'model'	0	0	0	1	0	0	0	0	1	0	1	3	7	8	5	8	8	7	10	16	17	3	95
'reliability' x 'application'	0	0	0	0	0	0	0	0	0	0	1	3	4	4	4	7	2	7	7	8	16	1	64
'reliability' x 'user'	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	1	1	0	2	7	0	14
'cyber' x '(cps', 'cyber physical system)'	0	0	0	0	0	0	0	0	3	0	0	0	6	9	10	12	12	17	19	22	26	1	137
'cyber' x 'framework'	0	0	0	0	0	0	0	0	3	0	2	1	8	10	10	16	17	41	28	38	41	2	217
'cyber' x 'model'	0	0	0	0	0	0	0	0	6	1	6	7	33	27	38	46	59	98	84	107	122	5	639
'cyber' x 'application'	0	0	0	0	0	0	0	0	3	0	2	5	7	13	19	18	27	36	43	50	61	1	285
'cyber' x 'user'	0	0	0	0	0	0	0	0	1	0	0	2	4	8	2	3	6	11	11	11	20	1	80
'(cps', 'cyber physical system)')' x 'framework'	0	0	0	0	0	0	0	0	2	0	0	0	3	0	4	2	2	4	4	5	7	0	33
'(cps', 'cyber physical system)')' x 'model'	0	0	0	0	0	0	0	0	3	0	0	0	5	4	9	5	5	7	5	13	16	0	72
'(cps', 'cyber physical system)')' x 'application'	0	0	0	0	0	0	0	0	3	0	0	0	0	3	1	4	5	2	2	9	6	0	35
'(cps', 'cyber physical system)')' x 'user'	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	1	2	0	3	5	0	13
'framework' x 'model'	1	0	1	0	0	4	7	8	6	6	8	5	16	23	28	26	23	47	24	40	50	2	325
'framework' x 'application'	0	0	1	0	1	0	0	1	2	2	2	1	3	7	9	10	7	18	14	14	19	0	111
'framework' x 'user'	0	0	0	0	0	0	0	1	0	0	1	0	1	2	3	2	3	2	2	4	10	0	31
'model' x 'application'	0	1	2	2	2	3	3	4	6	5	6	12	9	15	27	22	36	38	37	44	73	2	349
'model' x 'user'	0	0	0	1	0	0	1	1	2	0	3	2	3	6	7	6	9	9	8	12	17	1	88
'application' x 'user'	0	0	0	2	0	1	0	1	0	0	0	3	2	4	3	4	5	5	5	9	10	1	55

(参考) 共起分析 特許年次推移

※共起件数をスケール表示

少 多

words	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	total
'(sos', 'system of systems)' x 'security'	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1	3	1	0	0	0	0
'(sos', 'system of systems)' x 'safety'	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
'(sos', 'system of systems)' x 'reliability'	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
'(sos', 'system of systems)' x 'cyber'	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
'(sos', 'system of systems)' x '(cps', 'cyber physical system)'	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
'(sos', 'system of systems)' x 'framework'	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
'(sos', 'system of systems)' x 'model'	0	0	0	0	0	0	2	1	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0
'(sos', 'system of systems)' x 'application'	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	2	0	0	0	0	0	0	0
'(sos', 'system of systems)' x 'user'	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	2	1	3	1	1	2	0	0
'security' x 'safety'	0	0	0	0	0	0	1	0	3	0	0	1	2	1	5	2	4	7	20	38	58	0	0
'security' x 'reliability'	0	0	0	0	0	1	1	0	0	0	0	1	0	0	0	0	1	0	1	1	9	0	0
'security' x 'cyber'	0	0	0	0	0	0	0	0	0	0	0	0	1	0	3	4	1	8	16	29	24	1	0
'security' x '(cps', 'cyber physical system)'	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	5	6	5	6	0	0
'security' x 'framework'	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	2	0	2	3	3	9	1	0
'security' x 'model'	0	3	1	0	0	3	1	1	0	3	1	1	4	1	2	2	0	8	20	50	88	3	0
'security' x 'application'	0	0	0	0	0	0	0	1	2	0	0	1	3	0	2	1	2	6	10	22	36	1	0
'security' x 'user'	0	0	0	1	0	1	1	3	3	4	1	4	4	4	0	7	10	16	15	31	46	2	0
'safety' x 'reliability'	0	0	0	0	0	0	0	0	0	0	0	1	2	0	1	0	1	0	0	7	13	0	0
'safety' x 'cyber'	0	0	0	0	0	0	0	0	0	0	0	0	2	0	1	2	3	3	2	6	11	0	0
'safety' x '(cps', 'cyber physical system)'	0	0	0	0	0	0	0	0	0	0	0	0	2	0	1	0	2	2	3	3	4	0	0
'safety' x 'framework'	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	3	2	3	0	0
'safety' x 'model'	0	0	0	0	0	0	0	0	1	0	1	1	4	1	3	1	1	9	11	34	78	2	0
'safety' x 'application'	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	2	2	3	13	12	0	0
'safety' x 'user'	0	0	0	0	0	0	0	0	1	0	1	0	0	1	2	2	4	4	8	20	20	0	0
'reliability' x 'cyber'	0	0	0	0	0	0	0	0	0	0	0	1	2	0	0	1	3	2	1	1	2	0	0
'reliability' x '(cps', 'cyber physical system)'	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	1	0	1	0	0	0
'reliability' x 'framework'	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0
'reliability' x 'model'	0	0	0	0	0	0	0	0	0	0	0	1	4	1	2	1	2	7	7	11	28	1	0
'reliability' x 'application'	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	2	3	4	0	0
'reliability' x 'user'	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	4	0	2	2	9	0	0
'cyber' x '(cps', 'cyber physical system)'	0	0	0	0	0	0	0	0	0	0	0	1	4	2	9	4	8	10	9	13	15	0	0
'cyber' x 'framework'	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	2	1	2	0	1	3	1	0
'cyber' x 'model'	0	0	0	0	0	0	0	0	0	0	1	1	4	2	8	4	7	8	10	17	37	0	0
'cyber' x 'application'	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	4	2	5	4	3	1	0
'cyber' x 'user'	0	0	0	0	0	0	0	0	0	0	0	1	1	0	4	2	11	5	4	15	6	0	0
'(cps', 'cyber physical system)')' x 'framework'	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	1	1	0	0
'(cps', 'cyber physical system)')' x 'model'	0	0	0	0	0	0	0	0	0	0	0	1	3	1	8	4	5	6	6	4	4	0	0
'(cps', 'cyber physical system)')' x 'application'	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	2	0	0	0
'(cps', 'cyber physical system)')' x 'user'	0	0	0	0	0	0	0	0	0	0	0	0	1	0	2	0	3	0	3	5	0	0	0
'framework' x 'model'	0	0	0	0	0	0	0	0	0	0	0	1	0	2	1	0	0	6	3	4	21	0	0
'framework' x 'application'	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	2	3	4	1	0
'framework' x 'user'	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	1	1	0	0
'model' x 'application'	0	0	0	0	0	0	0	0	0	2	0	0	0	1	2	2	4	5	14	48	60	0	0
'model' x 'user'	0	1	0	0	0	1	0	0	0	4	1	0	2	3	1	0	2	11	22	69	106	1	0
'application' x 'user'	0	0	0	0	0	0	0	1	0	0	0	1	1	1	0	2	4	6	14	27	35	0	0

二次利用未承諾リスト

報告書の題名 令和2年度省エネルギー等に関する国際標準の獲得・普及促進事業（国際ルールインテリジェンスに関する調査（システムオブシステムズの安全性・信頼性確保））報告書
 委託事業名 令和2年度省エネルギー等に関する国際標準の獲得・普及促進事業（国際ルールインテリジェンスに関する調査（システムオブシステムズの安全性・信頼性確保））
 受注事業者名 株式会社三菱総合研究所

頁	タイトル、内容等
6	Society 5.0のしくみ（内閣府ウェブページ）
7	Society5.0を実現するデジタルアーキテクチャ・デザインセンターの戦略（IPAウェブページ）
25	Hake G. et al. "Towards Recertification of Modular Updates in Integrated Maritime Systems of Systems", SAFECOMP 2020.
26	木下聡子ほか「自動運転車を取り巻く System of Systemsの安全性要求の妥当性確認と検証」, SEC journal Vol.12 No.4 Mar. 2017
27	Susmit Jha, John Rushby, Natarajan Shankar, "Model-Centered Assurance for Autonomous Systems", SAFECOMP2020
30, 62	Pegasus Symposium 2019 "V-Model and Process Analysis"
32	IPA「国際安全規格におけるSTAMP/STPA適用可能性の考察」、第2回 STAMPワークショップ
33	IPA「はじめてのSTAMP/STPA」Ver.1.0（2016年3月）
34	金子朋子「自動運転事例における機械学習の課題とヒアリング・アンケート結果」、第二回AI/IoTシステム安全性シンポジウム（2020年11月）
36	道浦康貴「自動制御システムの安全性解析の最新手法」
37	野本秀樹ほか「FRAM（機能共鳴分析手法）による成功学に基づく安全工学」, SEC journal Vol.14 No.1 Aug. 2018
39, 44, 69	DEOSプロセス（DEOS協会ウェブページ）
42	益田明彦「JIS Z 8115 ディペンダビリティ（信頼性）用語の現状と将来」, IEICE Fundamentals Review Vol.9 No.4
45	4つのプロセスビューの関係（DEOS協会ウェブページ）
46	D-Case基本パターンとその更新（DEOS協会ウェブページ）
47	DEOSアーキテクチャ（DEOS協会ウェブページ）
49	吉武良治「使いやすさ／利用時品質の考え方～開発技術者にとって重要なユーザビリティ、UXとは～」, ET2014 IPAブースプレゼン
51-53	Mario Trapp and Gereon Weiss "Towards Dynamic Safety Management for Autonomous Systems"
55-58	経済産業省「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の概要」
60, 61, 63	Pegasus Symposium 2019 "Introduction and Overview of 3.5 Years of PEGASUS"
64	Pegasus Symposium 2019 "Sensor Models"
66,67	ロボットサービスの安全マネジメントに関する規格（産総研ウェブページ）
68	（一社）日本鉄道車両機械技術協会「自律移動型駅サービスロボットの安全性確保に関するガイドライン 解説」
116	スマートシティファレンスアーキテクチャホワイトペーパー 第一版（2020年3月31日）
126	経済産業省・日本規格協会「ビジネスを成功させるためのルール形成戦略セミナー」（2021年2月3日）
128	経済産業省「国際標準化の動向とルール形成戦略について」
137	EU「信頼できるAIのための倫理ガイドライン」
137	経済産業省「カーボンニュートラルの広がり」
153	今村文彦「防災ISO規格活動の開始 一防災イノベーションに向けて」, 産学官連携ジャーナル, 2020年9月
160	中小企業庁「中小企業白書 2019年版」, 第3部第2章
162	古田一雄 and 菅野太郎. "レジリエンス工学の誕生と展望." システム/制御/情報 60.1 (2016): 3-8.
174	C. Ncube et al., "On Systems of Systems Engineering: a Requirements Engineering Perspective and Research Agenda", IEEE 26th International Requirements Engineering Conference, 2018

二次利用未承諾リスト

報告書の題名 令和２年度省エネルギー等に関する国際標準の獲得・普及促進事業（国際ルールインテリジェンスに関する調査（システムオブシステムズの安全性・信頼性確保））報告書
 委託事業名 令和２年度省エネルギー等に関する国際標準の獲得・普及促進事業（国際ルールインテリジェンスに関する調査（システムオブシステムズの安全性・信頼性確保））
 受注事業者名 株式会社三菱総合研究所

頁	タイトル、内容等
234	安全性分析システム Source : US14082506A
235	脅威モデル例 Source : Threatmodeler https://threatmodeler.com/threat-model-templates/
236	通信におけるパイロット作業負荷モデル Source : Procedia Computer Science 8, 242-248, 2012
237	人間と自律的なCPSの協働 Source : International Journal of Human-Computer Studies, 130, 21-39, 2019
239	Barrier certificateを用いたポジション交換 Source : arXiv : 1609.04730 https://arxiv.org/pdf/1609.04730.pdf
240	統合シミュレーション Source : IEEE Transactions on Vehicular Technology 65(3), 1098-1108, 2016
241	仮想モジュール Source : WO2019EP79651A
242	インフラシステムオブシステムモデリングプラットフォーム Source : Infrastructure Transitions Research Consortium https://www.itrc.org.uk/nismod/
243	ロバストシミュレーション最適化のアプローチ Source : PloS one https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0242613
244	モジュラー設計の最適レベルを決定するためのピラミッドモデル Source : Procedia Computer Science 12, 63-68, 2012
246	設計フレームワーク Source : Journal of Systems Engineering and Electronics, 30(4), 720-737, 2019
247	ステートフルルール検証プラットフォーム Source : US13918851A
248	複数の移動通信モジュールを含む無線ネットワーク Source : US13198605A
249	モデル駆動型セキュリティシステム Source : US14602935A
250	ユニットテストを自動的に成するためのシステム Source : DE112013000485A
251	リスク評価フロー Source : Computers & Security 96, 101864, 2020
253	Taekionセキュアファイルシステム Source : Grid7 https://taekion.com/home/solutions-alpha-06/
254	障害検出、分離、及び修復システムのブロック図 Source : US13878396A
257	人工的摂動による誤判定 Source : arXiv:1412.6572v3 https://arxiv.org/pdf/1412.6572v3.pdf
261	re-taskingの効果的な設計を決定するための方法 Source : US14521285A
262	セルフフォールディングする複合材料 Source : Soft Matter, 9, 7688-7694, 2013
263	分散ストレージのデザスタリカバリ方法のフロー Source : US15885670A
264	計算の複雑性の軽減が可能なニューラルネットワークのノード構造 Source : US14030834A
265	自動運転技術のための説明可能なAI Source : US16724428A

令和2年度省エネルギー等に関する国際標準の獲得・普及促進事業
(国際ルールインテリジェンスに関する調査 (システムオブシステムズの安全性・信頼性確保))
報告書

2021年3月



株式会社三菱総合研究所
東京都千代田区永田町二丁目10番3号
☎080-6771-9258



一般社団法人 ディペンダビリティ技術推進協会
京都市中京区烏丸通二条上ル蒔絵屋町280
☎075-213-7075



アスタミューゼ株式会社
東京都千代田区神田小川町3丁目9-2 BIZCORE神保町4F
☎03-5148-7181