

AISIロボティクスSWG活動状況

ロボティクスSWG

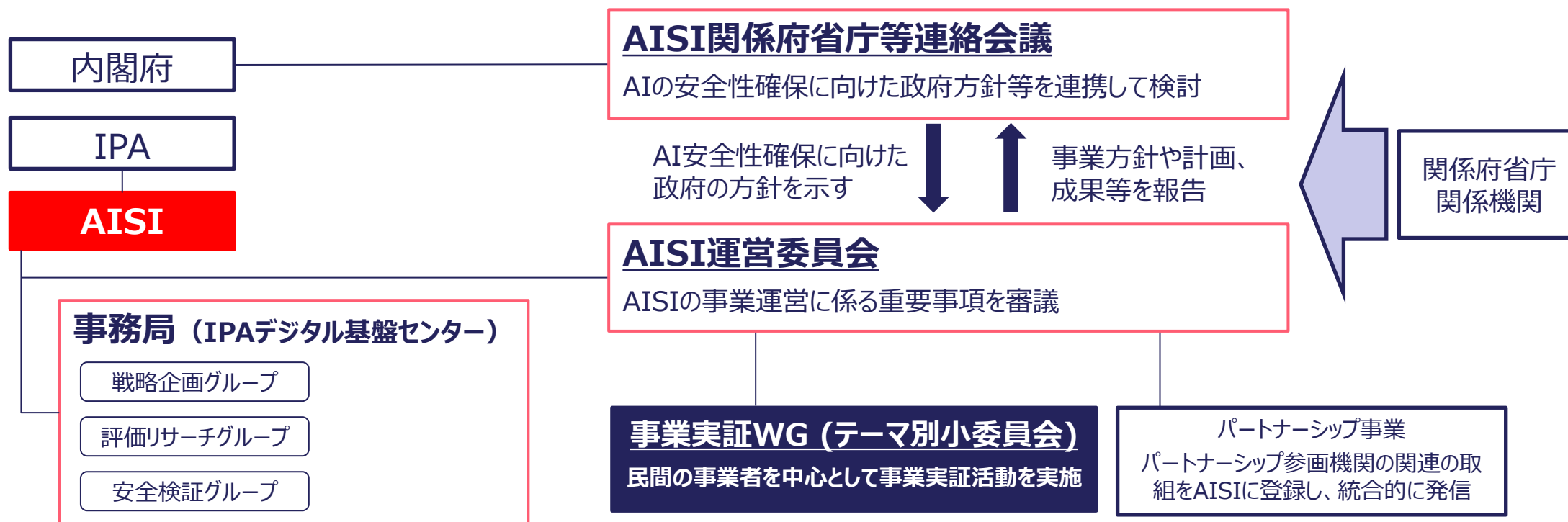
国立研究開発法人 産業技術総合研究所
ウェルビーイング実装研究センター
副研究センター長 中坊 嘉宏

2026年10月5日
AISI事業実証WG

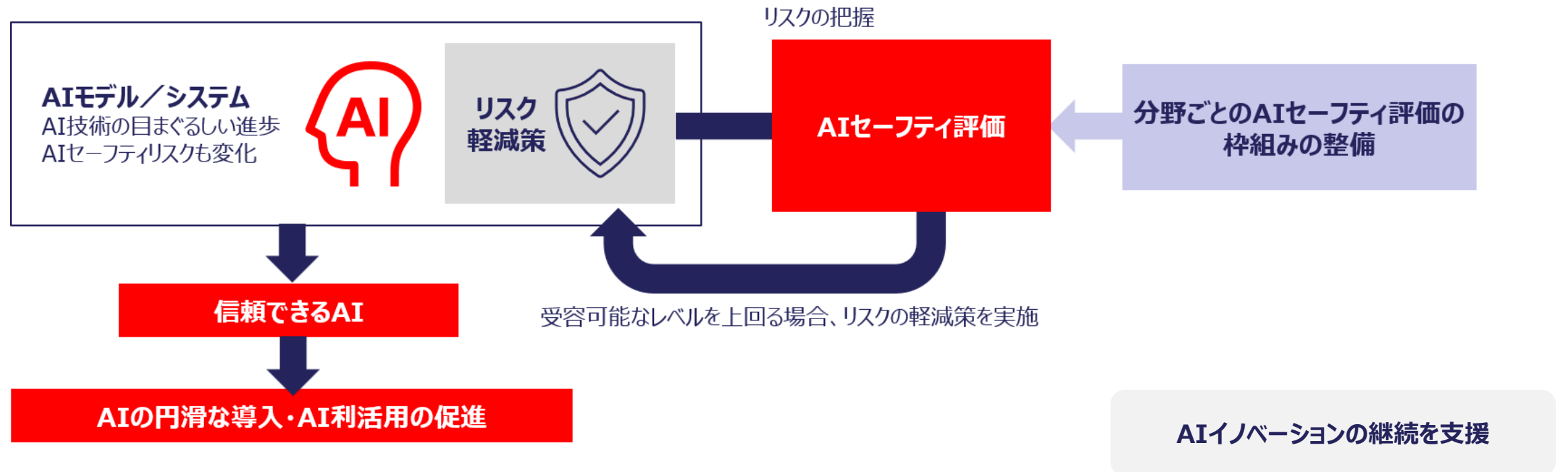
AISI Japan
AI Safety Institute

事業実証WGの設置

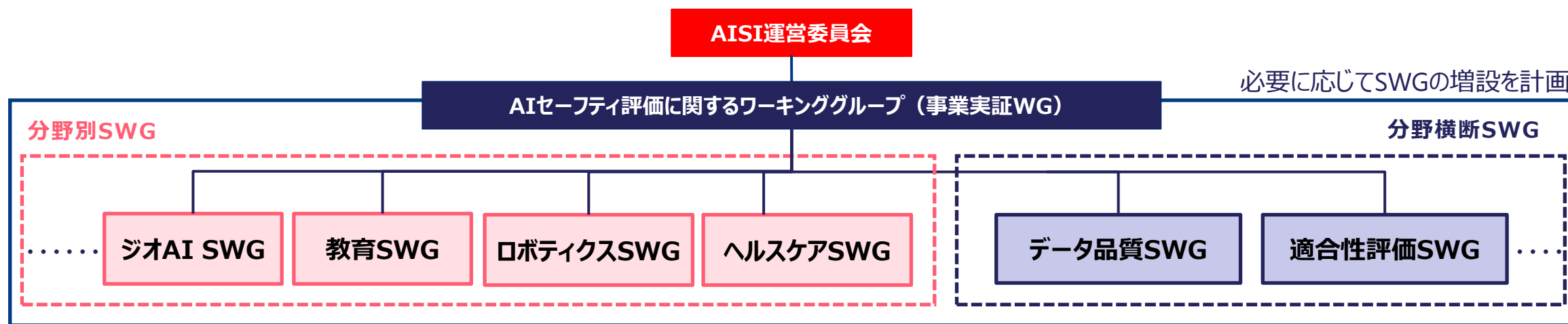
2025年3月、AISII運営委員会の下に、テーマ別小委員会として、「AIセーフティ評価に関するワーキンググループ」（事業実証WG）を設置



事業実証WGのゴールは、産業界・行政・専門家が協働して、AIの社会実装におけるAIセーフティの確保を支える仕組みを構築し、**利用者のリスク理解を前提としたAIセーフティ評価の枠組みを整備すること**



「信頼できるAI」を実現する実効的なAIセーフティ評価の枠組み構築に向けて、
分野別（Vertical）SWGと、分野横断（Horizontal）SWGを設置



WG運営事務局：三菱総合研究所

オブザーバ

内閣府（科学技術・イノベーション推進事務局） 内閣官房（国家安全保障局・国家サイバー統括室） 警察庁
デジタル庁 総務省 外務省 文部科学省 厚生労働省 農林水産省 経済産業省 国土交通省 防衛省
情報処理推進機構（IPA） 情報通信研究機構 理化学研究所 国立情報学研究所 産業技術総合研究所

AIロボティクスにおけるリスク・課題

- ◆ 従来のロボットにおける物理的リスクに加えて、AIが実装されることで人とのコミュニケーション等による心理的リスクや、個別の事故にとどまらない社会的リスクも想定される。
- ◆ 従来の機能安全を含めた新たな安全性評価、すなわちAIセーフティ評価に対する指針が求められる。

物理的リスク

ロボットの動作が人身・物的被害に直結し得るリスク(衝突、挟圧、転倒等)



心理的リスク

対人応対やコミュニケーション等により、人の心理状態に影響を与えるリスク



社会的リスク

サイバーセキュリティ攻撃や権利侵害や不正利用などの個別の事故にとどまらないリスク



ミッション

- ◆ 社会がAIロボットを安全かつ安心して利活用することを促進するため、開発メーカーやシステム提供者、研究機関等と連携して、より実用に近い応用例からAIセーフティ評価の模擬環境と仮想シナリオによる実証を通じて、将来の標準的な評価の枠組みの確立を目指す。

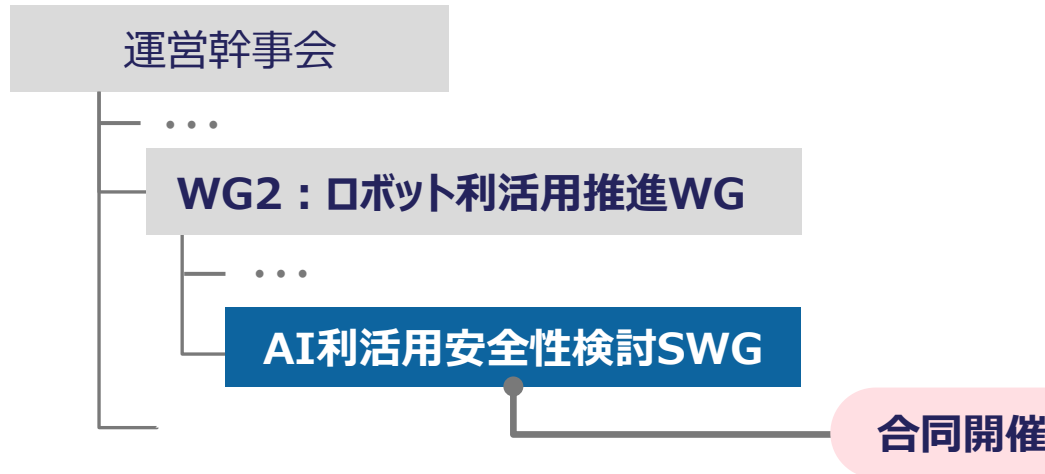
ロボティクスSWGの体制・参加組織



ロボット革命・産業IoTイニシアティブ協議会
Robot Revolution & Industrial IoT Initiative



ロボット革命・産業IoTイニシアティブ協議会（RRI）



AIセーフティ・インスティテュート（AISI）



★は本年度より新規参加

国研）産業技術総合研究所（SWGリーダー）

株式会社IHI

川崎重工業株式会社

一般社団法人セーフティグローバル推進機構

一般財団法人日本品質保証機構

富士通株式会社

三菱電機株式会社

サイバネットMBSE株式会社

株式会社日立製作所

パナソニック ホールディングス株式会社

株式会社Forcesteel Robotics★

セイコーエプソン株式会社★

株式会社ベリサーブ★

株式会社村田製作所★

一般社団法人日本ロボット工業会★

株式会社レゾナック★

NECネットエスアイ株式会社★

事務局：株式会社三菱総合研究所

本年度より産業競争力懇談会（COCN） フィジカルAIタスクフォースとも連携

清水建設株式会社

独立法人情報処理推進機構

東京科学大学

株式会社日立総合計画研究所

旭化成株式会社

日本電気株式会社

トヨタ自動車株式会社 など

ロボティクスSWGの昨年度（2025年度）の成果

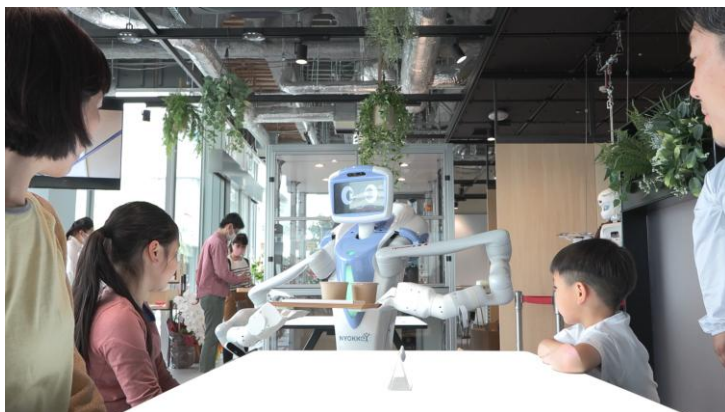
- AIを搭載し、人と空間を共有しながら移動、対話、搬送等を行うAIロボットを対象としたユースケースとして、「飲食店等における商品搬送ロボット」および「遠隔操作型の配送ロボット」の実証実験を実施。

飲食店等における商品搬送ロボット

ロボットによる注文内容の把握（認知・判断）や配膳までの自律移動（行動の適切性や安全性）、注文者とのやり取り（インタラクションやプライバシー）を評価

協力企業・団体

川崎重工業、キビテク、サイバネットMBSE



出所) 川崎重工株式会社 Future Lab HANEDA

遠隔操作型の配送ロボット

複数の自律移動ロボットを人間が遠隔から監視・操作する際の運用・効率性や安全性を評価し、人とAIロボットの協働における課題を分析

協力企業・団体

産業技術総合研究所、パナソニックホールディングス



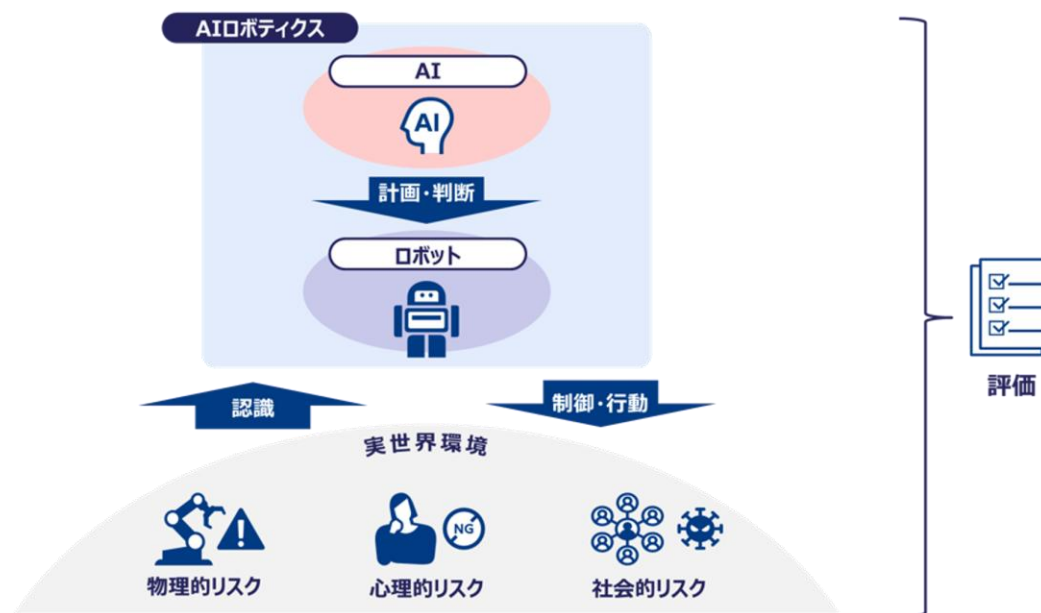
10台
1人



それぞれの実証実験に関する報告書は後日公開予定

ロボティクスSWGの昨年度（2025年度）の成果

- 「AIロボティクスに関するセーフティ評価観点ガイド」を2026年7月に発行。AIを活用し、人と空間を共有しながら移動、対話、搬送等を行うAIロボットを対象に、AIの利用に伴って新たに生じ得るリスクを特定・評価し、その結果に応じてリスク低減策を検討するための観点を示す。
- 実証実験を想定ユースケースとして、AIロボットの安全性を評価する際に確認すべき観点を9項目に整理

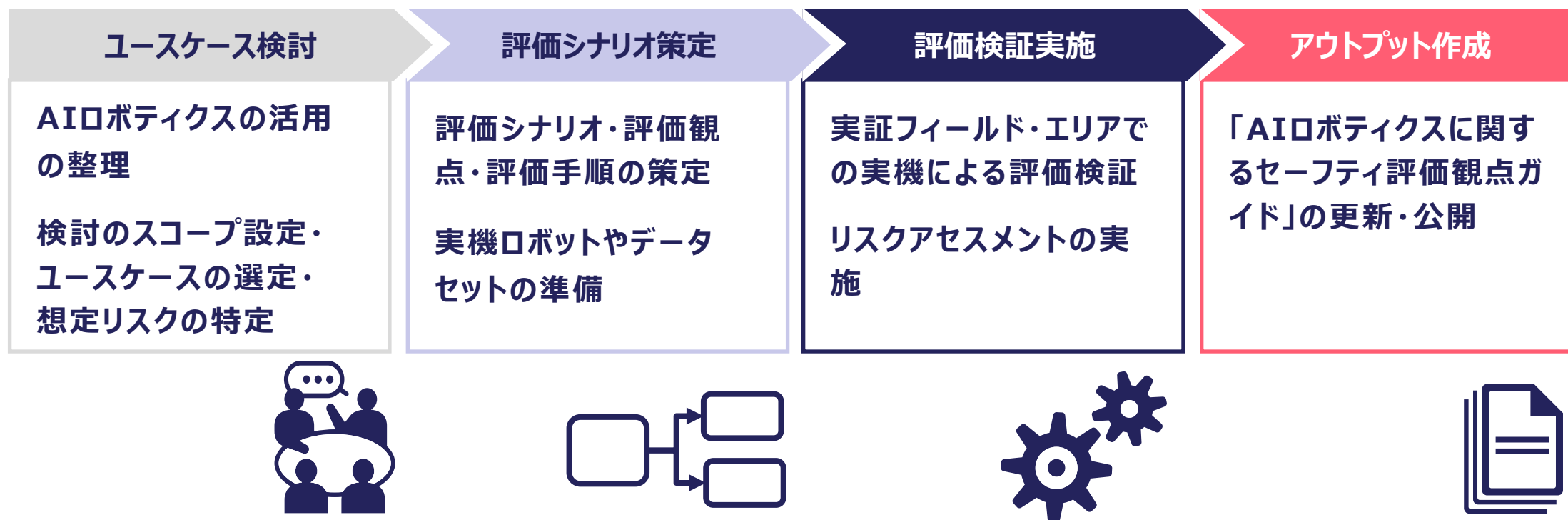


評価観点

- ✓ 物理的安全性
- ✓ 運用合理性
- ✓ 安定性
- ✓ 人間の適切な介在
- ✓ プライバシー保護
- ✓ 説明可能性
- ✓ 検証可能性
- ✓ 認知・判断の妥当性

2026年度上期の活動概要

- 上期は、AIロボティクスのユースケースを検討し、2件の評価実証を計画。
- ガイドの評価観点に基づき、評価シナリオと評価項目をSWGメンバーにて議論を行い、下期に実施予定の評価検証に向けて、具体的な評価方法や評価環境等を準備中。
- 評価検証の結果や今年度のSWGでの議論はガイドの次版に反映。



実証実験① 自律移動ロボットの公道走行実証

複数機種・複数台のロボットが、遠隔操作者の関与の下で、屋内外の多様な環境において人や車両交通を考慮しながら、AIにより自律的かつ安全に多様な移動を実現できることを検証

実証エリア（お台場）

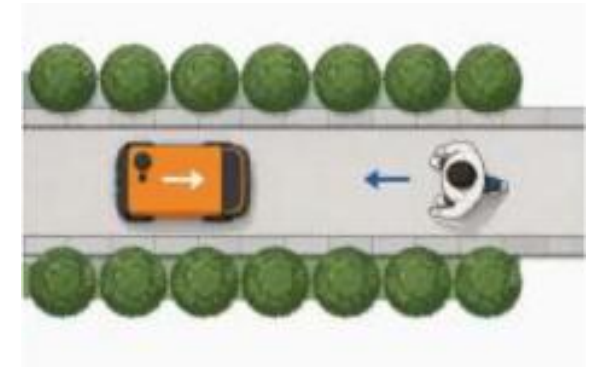


主な評価観点

・ 物理的安全性



- ・ 認知・判断の妥当性
- ・ 人間の適切な介在



・ 運用合理性

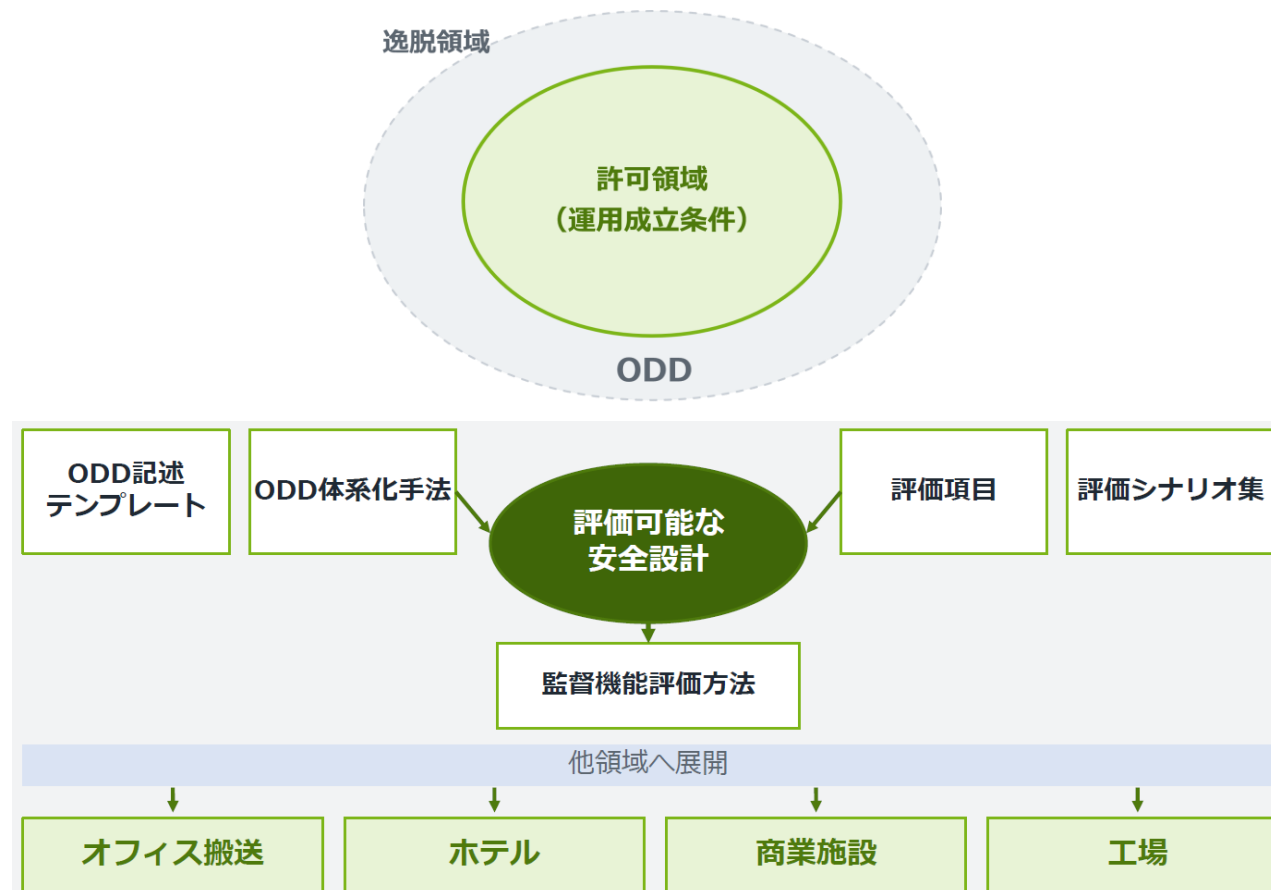
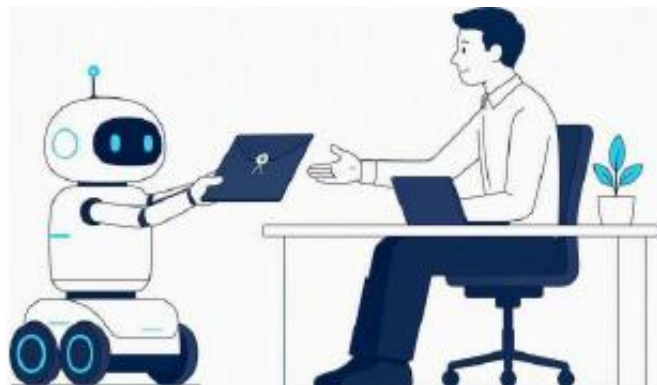


・ インタラクションの適切性



実証実験② 運用・利用者目線での安全性検証

- 書類・小物をオフィス内で搬送するAIロボットを対象として、依頼から受け渡し、例外対応までの一連の流れにおける**AIロボット運行設計領域（ODD）**を定義し、逸脱しないか監督する機能を評価
- AIロボットのためのODDの体系化手法等の安全設計や監督機能を標準化可能な形にして、産業ロボット分野、サービスロボット分野を問わずAIロボット全般への展開を目指す。



- ロボティクスSWGでは、SWGメンバからテーマを持ち寄り、今年度の新規テーマとして**AIロボットの自律性**や**フィジカルAIのセキュリティ**等について議論を開始。
- 合同開催のRRIの他WG会議との連携、またAIロボティクスに関する国内外の動向調査を実施中。

マニピュレータの自律性に関する 情報要件と機能構造の整理



Pick & Place を対象として

マニピュレータ小WG 2025年度活動報告



2026年6月
ロボット革命・産業IoTイニシアティブ協議会
ロボットイノベーションWG
ソフトウェアアーキテクチャ調査検討委員会

検討状況

サイバーセキュリティに関連する主な取組

日本



一般的なサイバーセキュリティ要件に留まる

- 経産省・総務省は2026年3月、AI事業者ガイドライン第1.2版でフィジカルAIを定義。AI事業者ガイドラインではライフサイクル全体のサイバーセキュリティ対策を求める。

欧州



一般的なサイバーセキュリティ要件に留まる

- サイバーレジリエンス法（CRA、規則(EU)2024/2847）が2024年10月採択。脆弱性・インシデント報告義務は2026年9月11日開始、全面適用は2027年12月11日。

米国



外国製AIロボットに対して事実上の輸入規制

- 2026年7月、米連邦通信委員会（FCC）が外国製のロボットを対象機器リストに追加しFCCの機器認証を取得できなくなった。サイバーセキュリティ・サプライチェーンリスクを理由に事実上の輸入規制に踏み切る。

中国



国家標準内でセキュリティについて言及

- 工業情報化部が「人型ロボットとエンボディッドAI標準化技術委員会」を通じ国家標準体系HEISを2026年2月に発表。サプライチェーン・ライフサイクル全体のセキュリティを包含。

韓国



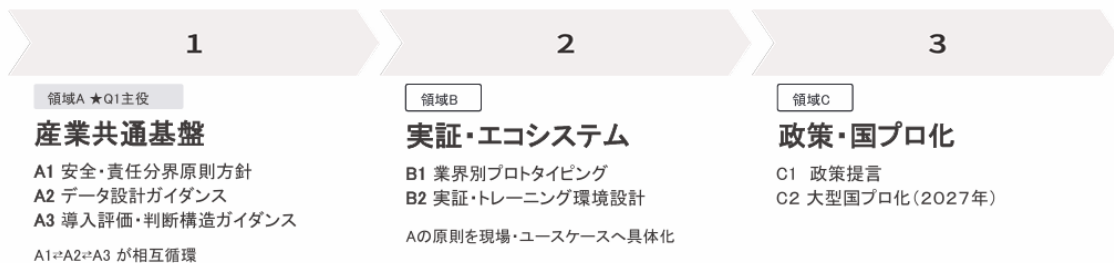
一般的なサイバーセキュリティ要件に留まる

- 科学技術情報通信部(MSIT)傘下の韓国インターネット安全保障庁（KISA）が2025年に「AIセキュリティガイド」を公表、AIライフサイクル全体で113のセキュリティ要件を規定。

COCN（産業競争力懇談会）にて活動中の「フィジカルAIタスクフォース」における“安全・責任分界原則”に関するテーマで連携開始

全体構造・推進スケジュール 概観図

推進領域A/B/Cの連携構造と2027年4月大型国プロ化までの流れを一目で示します。



A1・A2・A3 相互循環の詳細

A1 安全・責任分界原則

- 安全と責任の基本原則
- 何を見て、どこで止め、誰が引き受けるか

→ A2へ: 安全上見るべき対象を規定

A2 データ設計ガイド

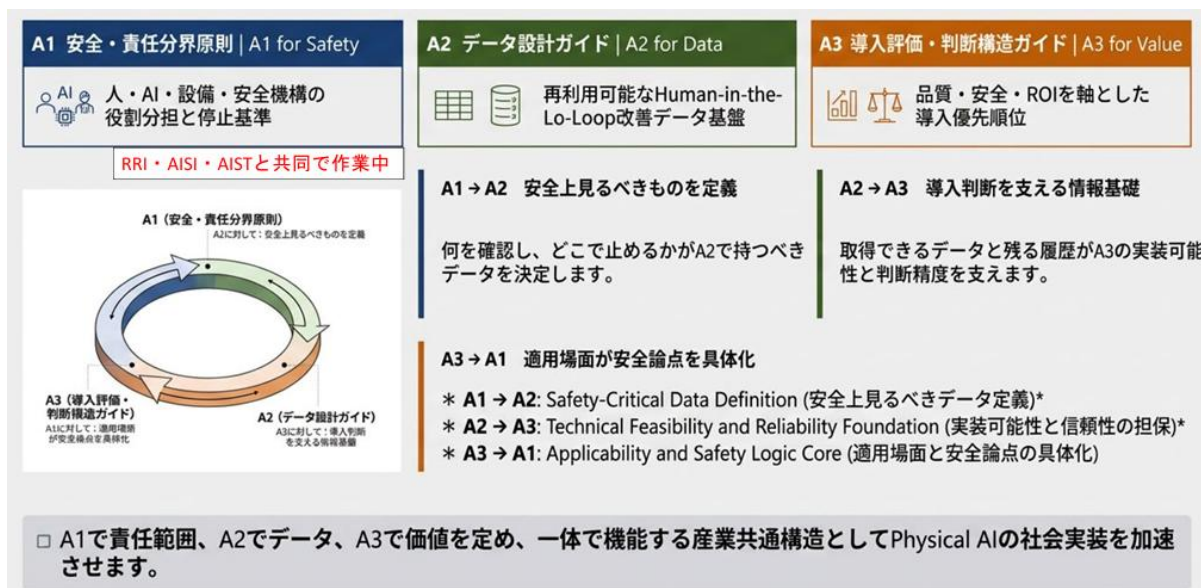
- データの持ち方・残し方・特微量整理
- Human-in-the-Loop 改善が回る設計
- データが集まる仕組み

→ A3へ: 取得可能データがA3を支える

A3 導入評価・判断構造ガイド

- どこに入れると価値が出るか
- 導入判断と優先順位の整理

→ A1へ: 導入先がA1の安全論点を具体化



出所) COCNフォーラム2026「[COCNフィジカルAIタスクフォース活動内容](#)」

「第44回日本ロボット学会学術講演会 (RSJ2026)」(金沢大学、2026年9月1～4日)のオープンフォーラム (OF)、および企業・団体展示にて、AISIIやロボティクスSWGの活動を紹介。

第44回日本ロボット学会学術講演会 (RSJ2026) @金沢大学角間キャンパス 自然科学本館
一般向けオープンフォーラム (OF)
場所: 108 (講演室J)
日時: 2026/09/01 17:00-18:30

OF4: AIロボットの安全をみんなで考える

主催: ロボット革命・産業IoT イニシアティブ協議会 (RRI)
オーガナイザー: 三好 崇生 (サイバネットMBSE)

出所) [20260901 OF4 AIロボットの安全をみんなで考える min](#) (見逃し配信中)



技術の進展と課題

AIの技術進歩のスピードは想像以上に早い。一方で、人が活動する物理世界に拘束されるロボティクス分野では、まだ乗り越えるべきAI技術のハードルがある。

間近に迫るAIロボットの実現

人と同じように対話し、判断して作業できるAIロボットの実現はかなり間近に迫っており、その実現によるインパクトとAIロボットへのニーズや期待は極めて大きい。

日本の議論を先導する

日本がAIロボティクスの「研究開発」と「利活用」において先頭を走ることができるように、AIロボットの社会受容について徹底的に突き詰めて検討し、議論を先導していきたい。

AISI

Japan AI Safety Institute