

適合性評価サブワーキンググループ（適合性評価 SWG） 2025 年度活動報告書

令和 8 年 4 月 23 日

AISI Japan
AI Safety Institute

AI セーフティ・インスティテュート
事業実証ワーキンググループ
適合性評価サブワーキンググループ

目次

1.	はじめに.....	1
1.1.	背景・目的.....	1
1.2.	対象読者.....	2
2.	適合性評価の現状.....	3
2.1.	適合性評価について.....	3
2.2.	現状の適合性評価の取組について.....	3
3.	国内における AI に関する取組状況.....	6
3.1.	国内の活動概況.....	6
3.2.	諸外国との連携.....	9
3.2.1.	欧州（EU）.....	9
3.2.2.	米国.....	10
3.2.3.	韓国との連携の概況.....	10
4.	AI 適合性評価に係る取組について.....	12
4.1.	AI の国際標準化活動：ISO/IEC JTC 1/SC 42.....	12
4.2.	AI マネジメントシステム（ISO/IEC 42001）認証.....	14
4.3.	EU AI Act.....	15
4.4.	その他の動向など.....	16
5.	適合性評価 SWG における取組.....	17
5.1.	適合性評価 SWG について.....	17
5.2.	2025 年度の取組.....	20
5.3.	HMT の概要紹介.....	21
5.4.	HMT を題材に AI 適合性評価の在り方を検討.....	23
5.5.	今後の課題.....	25
6.	まとめと今後の活動について.....	26
7.	参加組織の紹介.....	30
7.1.	一般社団法人情報マネジメントシステム認定センター（ISMS-AC）の活動状況.....	30
7.2.	公益財団法人日本適合性認定協会（JAB）の活動状況.....	31
7.3.	一般財団法人日本規格協会（JSA）の活動状況.....	31
7.4.	独立行政法人製品評価技術基盤機構認定センター（NITE）の活動状況.....	32
7.5.	一般財団法人日本品質保証機構（JQA）の活動状況.....	33
7.6.	国立研究開発法人産業技術総合研究所（AIST）の活動状況.....	33

1.1. 背景・目的

AI が日常生活に広く浸透しつつあり、その影響が大きくなってきている。一方で、AI は巨大なブラックボックスでもあり、安全安心・快適な利活用を考える上ではルールを設定したうえでの自由な活動であること、すなわちイノベーションを促進させながら、同時に AI セーフティを確保する両輪を繋ぐ軸的な役割を、社会受容性も考慮しつつ実現する必要がある。

その軸的な役割の実現のために AI 分野における適合性評価が有用であると考え。AI の国際標準化を進めている ISO/IEC JTC 1/SC 42 において AI マネジメントシステム国際規格 (AIMS) である ISO/IEC 42001 が 2023 年 12 月に発行された。この規格は組織が AI を利活用するうえでのどのようなマネジメントシステムを構築するかについての要求事項を整理したものであり、ISO 9001 や ISO/IEC 27001 など各種マネジメントシステム規格と同様に第三者適合性評価 (認証) 制度が確立され、AIMS 認証が開始されている。

一方で、AI はサービス形態や運用体制とともに動的に変化し続け、サービスの提供においてはステークホルダーが多数いる場合が多く、そのためサプライチェーンやバリューチェーンをも含めて包括的にとらえることが必要となる。また、AI 技術は日々変化しており、AI マネジメントシステム認証だけで AI ガバナンスが十分に達成できていると言い切ることは出来ず、また従来の組織・製品・要員等の縦割りが一過性な適合性評価では、変化し続ける対象に対する評価に十分に対応しきれないという課題がある。このような状況を考えるに、従来の適合性評価の枠組みで、どこまでイノベーション推進と AI セーフティの確保に貢献できるのか検討が必要である。

このような課題意識からも、ISO/IEC JTC 1/SC 42 では、AI システムに対する適合性評価のハイレベル・フレームワークを規定する ISO/IEC 42007 の国際標準化が進行中ではあるが、その具体的な実装を考えると、検討、開発しなければならない事項は多い。欧州では、AI Act に順守していることを示す方法として適合性評価の適用が求められており、いわゆる整合規格の開発も進められている。我が国においても、国際規格等を実際に活用し、イノベーション推進と AI セーフティを確保するためには、少なくともいくつかの段階で具体化が必要となる。したがって、国内 AI 産業の活性化に資する実用的な適合性評価手法の開発、制度設計について、国際的な相互運用および相互承認も含めて検討する必要がある。

以上の経緯から、適合性評価 SWG は、AI セーフティ・インスティテュート (AISI) に設けられた事業実証 WG のうち分野横断 SWG の一つとして設置された。適合性評価 SWG では評価側・受審側組織とともに、ISO/IEC JTC 1/SC 42 での活動や AISI での取組を踏まえて具体的な適合性評価手法を開発するにあたり、AISI のガイドを踏まえて開発される評価ツール等を使ったヘルスケア SWG およびロボティクス SWG の具体的な取組などから、AI システムに関する要求事項等を導出し、自己適合性評価を含む AI に関する適合性評価手法と実行可能な運用手順の確立を目指す。

2025 年度における活動としては、自己適合性評価を含む AI に関する適合性評価手法と実行可能な運用手順の確立に向けて、既存の AI に限らない各分野の適合性評価制度・認証制度への取組状況、我が国の AI セーフティに関する現状と他国との連携状況、ISO/IEC JTC 1/SC 42 にて日本主導で標準化を進めている Human-Machine Teaming(HMT)を題材に AI 分野における適合性評価の在り方について、適合性評価 SWG において討議・検討した内容を整理するとともに AI 分野における適合性評価（AI 適合性評価）の課題を抽出した。最後に課題を踏まえた今後の活動方針について整理した。

1.2. 対象読者

- AI やデジタルに関する適合性評価などの制度設計に関心がある政策立案者
- 国際規格に基づく認定・認証を実施する機関
- AI 適合性評価の制度設計に関心がある方々
- AI 適合性評価により、AI の社会受容性の向上に関心がある方々
- 国際規格を活用して、守りの標準化から攻めの標準化戦略を立案したい組織、機関

2.

適合性評価の現状

2.1. 適合性評価について

適合性評価とは、製品、プロセス、サービス、システム、要員又は組織に関する規定・要求事項が満たされていることを示す。適合性評価における仕組みの一部として、適合性評価機関の能力を実証する「認定」と、認定された適合性評価機関が製品、プロセス、サービス、システム、要員又は組織を第三者が適合性評価する「認証」がある。

AIに限らず、様々な分野で「認証」と、適合性評価機関への「認定」が運用されている。適合性評価の「認証」には、評価要素について特定の要求事項を満たしていることを担保できるというメリットがあり、特に品質・セキュリティ・安全性などを評価する「認証」が様々な分野で活用されている。また、適合性評価は評価する内容（品質・セキュリティ・安全性など）だけでなく、評価対象も様々である。評価対象としては、「組織」、「製品」、「要員」などが主に想定される。

2.2. 現状の適合性評価の取組について

本節においては、「組織」、「製品」、「要員」の3つの評価対象に対する適合性評価の「認証」、「認定」に関する主な取組を紹介する。具体的には以下の表の取組について整理する。

表 2-1 適合性評価の取組

No	評価対象	取組名	規格・基準
1	組織	Information Security Management System (ISMS) 認証	ISO/IEC 27001 JIS Q 27001
2	組織	Quality Management System (QMS) 認証	ISO 9001 JIS Q 9001
3	製品	Common Criteria Recognition Arrangement (CCRA)	ISO/IEC 15408
4	製品	CE マーキング制度	EU 規制に対応する複数の欧州規格
5	製品	JC-STAR 制度	JC-STAR 適合基準
6	要員	IRCA の審査員制度	IRCA 1000 等
7	要員	JRCA の審査員制度	JRCA ME100 等

(1) Information Security Management System (ISMS) 認証¹

ISMS 認証は、組織の情報資産を保護するための情報セキュリティのマネジメントシステムに

¹ ISMS-AC、ISMS（情報セキュリティマネジメントシステム）とは、<https://isms.jp/isms/>

対する認証であり、情報セキュリティリスクを体系的に管理・低減することを目的とする。ISMS 認証の認証対象は企業や自治体等の組織で、国際規格 ISO/IEC 27001 (日本産業規格 JIS Q 27001) に基づき、リスクアセスメント、管理策の実装を含むリスク対応、内部監査、マネジメントレビュー、継続的改善などが審査される。ISMS 認証は国際的な制度であり、日本においては ISMS-AC や JAB が認定機関となり、認証機関が審査を実施している。IT 企業、金融機関、クラウド事業者、自治体など幅広い組織が認証を取得している。

(2) Quality Management System (QMS) 認証²

QMS 認証は、製品やサービスの品質を安定的に提供するためのマネジメントシステムに対する認証である。評価対象は製造業やサービス業などの組織で、ISO 9001 (JIS Q 9001) を基準に、顧客要求事項の把握、業務プロセス管理、品質目標の設定、内部監査、経営者によるレビューなどが審査される。QMS 認証は国際的な制度であり、日本においては JAB が認定を行い、認証機関が審査を実施している。自動車部品メーカーや建設会社、医療機関など多様な分野で認証取得事例がある。

(3) Common Criteria Recognition Arrangement (CCRA) ³

CCRA は、IT 製品のセキュリティ機能を国際的に相互承認する枠組みであり、ISO/IEC 15408 (Common Criteria) に基づいて評価が行われる。評価対象は OS、IC カード、ネットワーク機器などの IT 製品で、セキュリティ機能要件や保証要件、評価保証レベル (EAL) が審査される。日本では IPA が IT セキュリティ評価及び認証制度 (JISEC) の認証機関として運営を担い、登録評価機関が試験を実施する。IC カードや暗号モジュールなどが認証事例として挙げられる。

(4) CE マーキング制度⁴

CE マーキング制度は、EU 域内で製品を流通させるための法令適合表示制度であり、製品が EU 指令や規則に適合していることを製造者が宣言する仕組みである。評価対象は機械、医療機器、電子機器など多岐にわたり、安全性や電磁両立性、環境パフォーマンスなどが評価要件となる。該当分野では EU 指定機関 (Notified body) による適合性評価が必要な場合もある。日本企業も EU 市場向け製品で CE マーキングを取得している事例が多数存在する。

(5) JC-STAR 制度⁵

JC-STAR 制度は、IoT 機器のセキュリティ確保を目的として日本で整備が進められている制度である。評価対象はネットワーク接続機器等で、パスワード管理、ソフトウェア更新機能、脆弱性対応、ログ管理などのセキュリティ要件が確認される。国際的な技術基準も参照しつつ、日本では IPA が制度運営を担い、登録試験機関等が評価を行う。ルーターなど IoT 製品での認証事例

² JQA、ISO 9001 (品質)、https://www.jqa.jp/service_list/management/service/iso9001/

³ IPA、国際承認アレンジメント (CCRA) 概要、<https://www.ipa.go.jp/security/jisec/about/ccra.html>

⁴ JETRO、CE マーキングの概要：EU、<https://www.jetro.go.jp/world/qa/04S-040011.html>

⁵ IPA、セキュリティ要件適合評価及びラベリング制度 (JC-STAR)、<https://www.ipa.go.jp/security/jc-star/index.html>

が出始めている。

(6) IRCA の審査員制度⁶

IRCA (International Register of Certificated Auditors) の審査員制度は、英国の CQI (Chartered Quality Institute) が運営する国際的な審査員登録制度であり、マネジメントシステム審査員個人を対象とする、ISO/IEC 17024 の認定を受けた要員認証制度である。IRCA が定めるスキーム文書に基づき、審査員研修の修了、審査実績、専門知識、継続的能力開発 (CPD) などが評価される。世界的な認知度が高く、ISO 9001 や ISO 27001 の主任審査員などが登録され、国際案件で活用されている。

(7) JRCA の審査員制度⁷

JRCA (Japanese Registration of Certificated Auditors) の審査員制度は、日本要員認証協会が運営する国内の審査員登録制度であり、ISO/IEC 17024 の認定を受けたマネジメントシステム審査員の要員認証制度である。評価対象はマネジメントシステム審査員個人で、JRCA が定めるスキーム文書に基づき、所定の研修修了、審査経験、専門分野知識、継続教育の実施状況などが審査される。日本では JAB 及び ISMS-AC が認定機関となり、国内のマネジメントシステム認証制度の一端を担っている。

⁶ CQI/IRCA Japan、IRCA 審査員/監査員、https://japan.irca.org/IRCA_auditor.html

⁷ JRCA、マネジメントシステム審査員 評価登録センター (JRCA)、<https://www.jrca-jsa.or.jp/jrca/>

3.

国内における AI に関する取組状況

本章では、国内の AI に関する取組状況を概況し、OECD AI 原則および広島 AI プロセス等の国際的議論との接続関係を整理する。併せて欧州（EU）、米国、韓国との連携状況も整理する。

3.1. 国内の活動概況

本節では、まず我が国における AI の安全性・信頼性確保に向けた取組状況を概況しつつ、OECD AI 原則や広島 AI プロセス等の国際的議論との関係性を整理する。具体的には、国際的に共有される原則・指針が、国内の基本法や事業者向けガイドラインを介して、評価観点・評価手続・データ品質管理といった実装・評価実務へと段階的に落とし込まれていく流れを、「戦略・構想」「法律・規制」「ガイドライン」「手引き・フレームワーク」という階層構造として示す。

第一に、戦略・構想の層として、国際的な勧告である「OECD AI 原則⁸」が AI ガバナンスの議論の基礎を提供する。その後、広島 AI プロセスが、OECD AI 原則を議論の基礎と位置づけ、高度な AI システム（基盤モデル・生成 AI 等）を念頭に置いた「高度な AI システムを開発する組織向けの広島プロセス国際指針⁹」と、それを具体行動へ落とした「高度な AI システムを開発する組織向けの広島プロセス国際行動規範¹⁰」を整備し、さらに対象を「全ての AI 関係者」へ拡張した「全ての AI 関係者向けの広島プロセス国際指針¹¹」も整備した。国内においても、「人間中心の AI 社会原則¹²」が、日本社会の AI 活用の構想として存在する。

第二に、「法律・規制」の層として、国内の法律である「人工知能関連技術の研究開発及び活用の推進に関する法律（AI 基本法）¹³」が存在する。これは、人工知能関連技術の研究開発および社会実装を総合的かつ計画的に推進するため、国の基本方針や推進体制を定めるとともに、国際的な規範に即した指針整備等を位置付けた基本法である。本法律は、国際的な規範の趣旨に即した指針整備等を位置づけ、国内の推進体制を定める基本法である。制度設計にあたっては、広島

⁸ OECD, AI principles

<https://www.oecd.org/en/topics/ai-principles.html>

⁹ G7, Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI System

<https://www.mofa.go.jp/files/100573471.pdf>

¹⁰ G7, Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems

<https://www.mofa.go.jp/files/100573473.pdf>

¹¹ G7, 全ての AI 関係者向けの広島プロセス国際指針

<https://www.soumu.go.jp/hiroshimaaiprocess/pdf/document03.pdf>

¹² 内閣府, 人間中心の AI 社会原則会議 科学技術・イノベーション

<https://www8.cao.go.jp/cstp/ai/ningen/ningen.html>

¹³ e-Gov, 人工知能関連技術の研究開発及び活用の推進に関する法律

<https://laws.e-gov.go.jp/law/507AC0000000053>

AI プロセス等の国際的議論も踏まえつつ、国内の政策枠組みとして整理された¹⁴。

第三に、「ガイドライン」の層として、国内のガイドラインである「AI 事業者ガイドライン¹⁵」が存在する。AI 事業者ガイドラインとは、AI 基本法が掲げる「国際的な規範に即した指針の整備」という枠組みに基づき、AI を開発・提供・利用する事業者が自主的に講ずべき具体的な取組事項を、経済産業省及び総務省が整備したガイドラインである。また、産業技術総合研究所 (AIST) の「機械学習品質マネジメントガイドライン¹⁶」と「生成 AI 品質マネジメントガイドライン¹⁷」が、機械学習／生成 AI の品質確保を品質マネジメントとして整理し、評価に必要な品質計画・指標・テスト・運用監視等を構造化するガイドラインとなる。

第四に、「手引き・フレームワーク」の層として、AISI は、上位の政策・ガイドラインで示される取組事項を、組織が実装・評価し説明可能な形で整理する際に参照できる実務文書（評価観点、手順、成果物例等）を整備している。AISI 発行のガイドラインである「AI セーフティに関する評価観点ガイド¹⁸」、「AI セーフティに関するレッドチーミング手法ガイド¹⁹」、「データ品質マネジメントガイドブック²⁰」が存在する。これらのガイド群が、評価観点・評価項目例、レッドチーミングの手続と成果物、データ品質マネジメントという評価実務の具体を与える。あわせて、広島 AI プロセスの国際行動規範の適用促進・透明性確保の運用面として、OECD が支援する「G7 reporting framework²¹」が、組織が規範の順守状況を報告するためのフレームワークとして整備された。

また、AI に関する規格としては、経済産業省に設置された諮問機関である日本産業標準調査会 (JISC) の審議を経て、2025 年 8 月 20 日、「JIS Q 42001:2025 情報技術－人工知能－マネジメントシステム」が官報に公示された。これは、「ISO/IEC 42001 AI マネジメントシステム」の翻訳規格である。さらに、2026 年 3 月現在、AIMS の認証機関の基準である JIS Q 42006 が、ISO/IEC 42006 AI マネジメントシステムの審査及び認証を行う機関に対する要求事項の翻訳規格として策定中である。

上記で取り上げた関係性とその動向を下表と下図に示す。

¹⁴ 国会, 第 217 回国会 衆議院 内閣委員会 第 13 号 令和 7 年 4 月 11 日

<https://kokkai.ndl.go.jp/simple/detail?minId=121704889X01320250411&spkNum=0#s0>

¹⁵ 経済産業省, AI 事業者ガイドライン

https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/20240419_report.html

¹⁶ 産業技術総合研究所, 機械学習品質マネジメントガイドライン

<https://www.digiarc.aist.go.jp/publication/aiqm/>

¹⁷ 産業技術総合研究所, 生成 AI 品質マネジメントガイドライン

<https://www.digiarc.aist.go.jp/publication/aiqm/GenAIQuality-requirements-rev1.0.0.0019.pdf>

¹⁸ AISI, AI セーフティに関する評価観点ガイド

https://aisi.go.jp/output/output_framework/guide_to_evaluation_perspective_on_ai_safety/

¹⁹ AISI, AI セーフティに関するレッドチーミング手法ガイド

https://aisi.go.jp/output/output_framework/guide_to_red_teaming_methodology_on_ai_safety/

²⁰ AISI, データ品質マネジメントガイドブックの公開 Data Quality Management Guidebook

https://aisi.go.jp/output/output_information/250331_2/

²¹ Hiroshima AI Process, Reporting Framework

<https://www.soumu.go.jp/hiroshimaaiprocess/en/report.html>

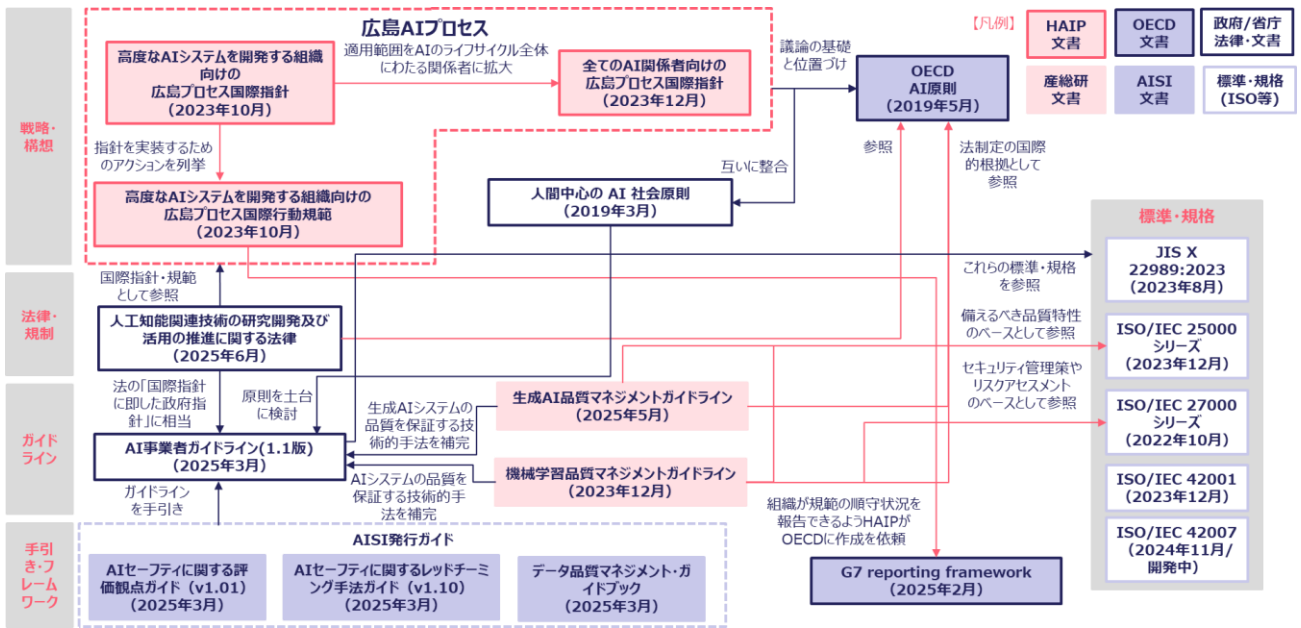


図 3-1 国内の AI に関する主な取組の状況

表 3-1 国内の AI に関する主な取組の一覧

分類	No	取組名	実施主体	発行年 (最終更新年)
戦略・構想	1	高度な AI システムを開発する組織向けの広島プロセス国際指針	G7 (広島 AI プロセス)	2023 年
	2	全ての AI 関係者向けの広島プロセス国際指針	G7 (広島 AI プロセス)	2023 年
	3	高度な AI システムを開発する組織向けの広島プロセス国際行動規範	G7 (広島 AI プロセス)	2023 年
	4	OECD AI 原則	OECD	2019 年
	5	人間中心の AI 社会原則	内閣府	2019 年
法律・規制	6	人工知能関連技術の研究開発及び活用の推進に関する法律	日本政府	2025 年
ガイドライン	7	AI 事業者ガイドライン	総務省・経済産業省	2024 年 (2025 年)
	8	機械学習品質マネジメントガイドライン	産業技術総合研究所	2020 年 (2024 年)
	9	生成 AI 品質マネジメントガイドライン	産業技術総合研究所	2025 年
手引き・フレームワーク	10	AI セーフティに関する評価観点ガイド	AISI	2024 年 (2025 年)
	11	AI セーフティに関するレッドチーミング手法ガイド	AISI	2024 年 (2025 年)
	12	データ品質マネジメントガイドブック	AISI	2025 年
	13	G7 reporting framework (HAIP レポート)	OECD	2025 年

3.2. 諸外国との連携

3.2.1. 欧州（EU）

(1) 欧州（EU）の動向概況

EU では、リスクベースの包括規制である「AI Act²²」が 2024 年 8 月 1 日に発効し、段階的に適用される枠組みである。欧州委員会の整理では、禁止行為や AI リテラシーに関する規定は 2025 年 2 月 2 日から適用され、汎用目的 AI（GPAI）モデルに関する義務およびガバナンスは 2025 年 8 月 2 日から適用、AI Act の対象の多くは 2026 年 8 月 2 日から適用・執行開始となり、規制対象製品に組み込まれる高リスク AI については移行期間が 2027 年 8 月 2 日まで延長される可能性がある。これらの実装・執行に関しては、欧州委員会の European AI Office 等が中心的役割を担うとされる。なお、European AI Office は、欧州委員会内に設置された AI 専門性の中核組織であり、EU レベルでの一貫した AI ガバナンス体制の基盤として、AI Act の実施を支える役割を担う²³。また、AI Act の実施を支える「調和規格（Harmonised Standards）」について、欧州委員会は CEN/CENELEC（JTC 21）で高リスク AI 向けの規格策定が進んでいること、策定後に欧州委員会が評価し EU 官報（Official Journal）に引用することで、当該要求への適合が推定される（ただし適用は任意）という位置付けを示している²⁴。また、品質マネジメントに関する規格案（prEN 18286）が 2025 年 10 月に公衆審査（public enquiry）段階に入っている²⁵。

(2) 欧州（EU）との連携概況

日本政府等との連携については、日 EU デジタルパートナーシップ（2024 年 4 月 30 日、ブリュッセル）における共同声明で、EU 側の European AI Office と日本側の AISI の設立を踏まえ、将来の行政アレンジメントに基づく機関連携を進める意向が示されている²⁶。また、広島 AI プロセスの成果（国際行動規範等）を前進させ、AI ガバナンス枠組みの相互運用性を促進する観点から、欧州委員会の AI Act と日本の AI 事業者向けガイドライン等に関する情報共有を行う方針が明記されている。

²² EC, AI Act

<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

²³ EC, European AI Office

<https://digital-strategy.ec.europa.eu/en/policies/ai-office>

²⁴ EC, AI Pact

<https://digital-strategy.ec.europa.eu/en/policies/ai-pact>

²⁵ EC, Standardization of the AI Act

<https://digital-strategy.ec.europa.eu/en/policies/ai-act-standardisation>

²⁶ EC, Joint Statement of the second meeting of the European Union - Japan Digital Partnership Council

<https://digital-strategy.ec.europa.eu/en/library/joint-statement-second-meeting-european-union-japan-digital-partnership-council>

3.2.2. 米国

(1) 米国の動向概況

米国の動向として、NIST は「AI Risk Management Framework (AI RMF 1.0) ²⁷」を公表し、AI のリスク管理を「Govern/Map/Measure/Manage」の機能で整理して、組織が状況に応じて運用できる枠組みを提示している。さらに米商務省は、従来の U.S. AI Safety Institute を「Center for AI Standards and Innovation (CAISI)」へ再編する方針を示し、産業界の取組を支える形で、ガイドライン/ベストプラクティス整備や標準化への関与を強める方向性を打ち出している²⁸。

(2) 米国の連携概況

日本政府および関連組織との連携としては、「日米間の技術繁栄ディール (Technology Prosperity Deal)」協力覚書 (2025 年 10 月 28 日) ²⁹において、AI 分野で①イノベーションを促進する AI 政策の枠組みの推進、②AI スタック全体 (インフラ、ハード、モデル、ソフト、アプリ等) の輸出促進、③industry standards (産業標準) に関する共同作業、④両国のガイドライン/フレームワークの相互理解を進め、相互運用性の観点から必要に応じて実務を調和 (harmonizing practices) すること等が明記されている。また、研究開発面では AI for Science 等の応用を含む協力領域が例示されている。

日本の AISI との連携については、日本 AISI と米国 NIST が、日本の「AI 事業者ガイドライン」と NIST 「AI RMF」とのクロスウォーク (対応付け) を成果文書として公表している³⁰。さらに前記の協力覚書では、日本 AISI と米 CAISI のパートナーシップを前進・再焦点化し、AI の計測 (metrology) に関するベストプラクティスや industry standards 開発等を通じて、安全で信頼できる AI エコシステムを促進する旨が明記されている。

3.2.3. 韓国との連携の概況

韓国では、科学技術情報通信部 (MSIT) が、「AI 基本法 (AI Basic Act)」が 2024 年 12 月 26 日に国会本会議で可決され、2026 年 1 月 22 日に施行された。同法は、国家 AI 委員会や AI マスタープラン (3 年ごと) の枠組み、AI 産業支援 (R&D、データ、標準化等) に加え、市民の生命・身体・財産を AI リスクから保護する専門組織として AI Safety Institute を設置する法的根拠も位置付けている。これと整合する形で、韓国側の AI Safety Institute (Korea AISI) は 2024 年 11 月

²⁷ NIST, AI Risk Management Framework

<https://www.nist.gov/itl/ai-risk-management-framework>

²⁸ U.S. Department of Commerce, Statement from U.S. Secretary of Commerce Howard Lutnick on Transforming the U.S. AI Safety Institute into the Pro-Innovation, Pro-Science U.S. Center for AI Standards and Innovation

<https://www.commerce.gov/news/press-releases/2025/06/statement-us-secretary-commerce-howard-lutnick-transforming-us-ai>

²⁹ 内閣府, 日米間の技術繁栄ディールに関する協力覚書【令和 7 年 10 月 28 日】

<https://www8.cao.go.jp/cstp/kokusaiteki/nichibei/20251028.html>

³⁰ AISI, AI 事業者ガイドラインと米国 NIST AI リスクマネジメントフレームワーク (RMF) のクロスウォーク 2

https://aisi.go.jp/output/output_information/240918_1/

に設立され、AI 安全性評価や政策・技術研究、国際連携等を担う体制を掲げている

日本政府・関係機関との連携としては、外務省公表の日韓首脳会談³¹（2025年8月23日）で、両首脳が「水素・アンモニア、AI等」に関する協力を一層推進していくことで一致した旨が示されている。さらに、外務省は「AIに関する日韓外交当局間課長級協議³²」（2026年2月5日）を公表しており、両国の関心事項や協力の展望に加え、「安全、安心して信頼できる AI」ガバナンスや、広島 AI プロセス等を含む国際協力について意見交換し、定期協議を継続することで一致したとしている。

日本の AISI との関係では、日本 AISI は国際連携の枠組みの下で韓国を含む各国との意見交換を実施している旨を公表している³³。

³¹ 外務省, 日韓首脳会談

https://www.mofa.go.jp/mofaj/a_o/na/kr/pageit_000001_02331.html

³² 外務省, AI に関する日韓外交当局間課長級協議の開催（結果）

https://www.mofa.go.jp/mofaj/press/release/pressit_000001_03288.html

³³ AISI, 国際連携

https://aisi.go.jp/activity/activity_international/international/

4.

AI 適合性評価に関する取組について

本章では、AI 適合性評価に関する国内外の取組状況を紹介する。

4.1. AI の国際標準化活動：ISO/IEC JTC 1/SC 42

(1) ISO/IEC JTC 1/SC 42 (SC42) における活動³⁴

ISO/IEC JTC 1/SC 42 (SC42) は、2017 年に設立された委員会であり、AI に関する様々な規格の作成を行っている。日本より提案され策定された国際規格も多く、一部については JIS 規格化も進められている。

SC42 には 5 つの常設ワーキンググループ (WG) が設置されており、それぞれ、

WG1：用語や概念、マネジメントシステム規格等の基本規格の開発

WG2：データに関する規格等の開発

WG3：AI の特性（トラストワージネス）に関する規格等の開発

WG4：ユースケースとアプリケーションに関する規格等の開発

WG5：AI システムの計算手法と計算特性に関する規格等の開発

を担当している。

また、他のテクニカルコミッティ (TC) と共同で WG を設置することもあり、現在 6 つの JWG が活動している (JWG1 はプロジェクト終了のため休眠中)。

JWG2：AI ベースのシステムテストに関する規格等の開発

JWG3：AI を活用した保健医療情報に関する規格等の開発

JWG4：機能安全と AI システムに関する規格等の開発

JWG5：自然言語処理に関する規格等の開発

JWG6：AI における適合性評価に関する規格等の開発

JWG7：AI 対応金融システムに関する規格等の開発

適合性評価に関連する規格としては、AI マネジメントシステム規格である ISO/IEC 42001 が代表的なものであり、ISO/IEC 42001 を用いて認証活動をする機関（いわゆる認証機関）に対する要求事項を定めたものが ISO/IEC 42006 であり、ともに WG1 において開発された。これらは組織（のマネジメントシステム）を評価対象とする国際規格である。

認証対象としては、組織以外にも、製品と要員に関するものがある。AI 分野においても AI シ

³⁴ 6th Grand Canvas, AI 監査の展望：グローバル規制と ISO 標準から信頼のための実践的技術まで、
https://www.digiarc.aist.go.jp/event/6th_grand_canvas/pdf/20250917-6th-grand-canvas-01-cheng.pdf

システムを対象とした場合の適合性評価に関するハイレベル・フレームワーク規格 (ISO/IEC 42007) の開発が JWG6 にて行われている。ISO/IEC 42007 が直接的に適合性評価活動に用いられる可能性は高くはないが、各 WG や各 JWG において開発された／されている AI システムの (適合性) 評価に使える国際規格を組合せるなどにより AI 適合性評価についても議論が深化するものと考えられる。

(2) ISO/IEC 42001 について

ISO/IEC 42001 は、AI マネジメントシステム規格である。品質マネジメントシステムの国際規格 ISO 9001 や情報セキュリティのマネジメントシステム規格 ISO/IEC 27001 などと同様に組織におけるマネジメントシステムの要求事項である。

ISO/IEC 42001 の特色は、リスクベースアプローチを通じて AI システムを適切に開発・提供・利用するためのマネジメントシステム規格であることである。具体的には、AI リスクアセスメント・リスク対応、インパクトアセスメントの実施、データの取り扱いなどを含む。

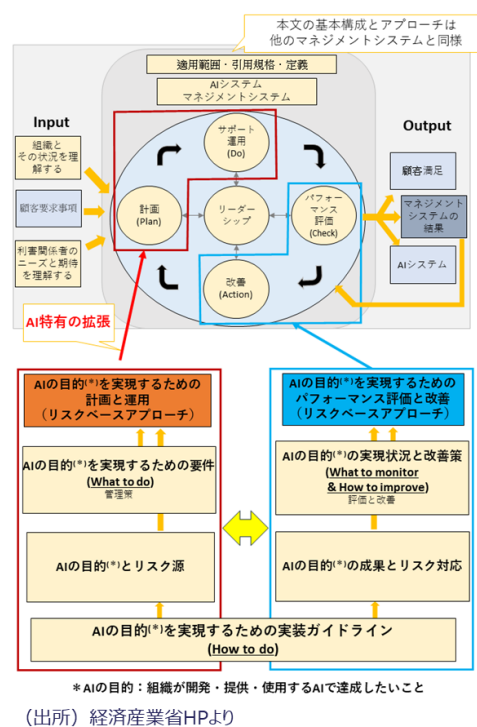


図 4-1 AI マネジメントシステムの構成³⁵

SC42/WG1 では、用語や概念に関する ISO/IEC 22989 など基本規格といわれるものを開発しているが、最近では ISO/IEC 42001 を中心に関連する規格群の開発が行われており、シリーズ規格として周辺規格が策定されている。この中には、いわゆる中小企業が AI マネジメントシステムを導入する際のガイドとなるハンドブックの作成も含まれており、また、組織における AI マネジ

³⁵ 経済産業省, AI マネジメントシステムの国際規格が発行されました、
<https://www.meti.go.jp/press/2023/01/20240115001/20240115001.html>

メントシステムの内部監査のための規格 ISO/IEC 42114 は日本主導で開発されていく見込みである。

(3) ISO/IEC 42007 について

ISO/IEC 42001 が組織を対象としたマネジメントシステム規格であるのに対して、ISO/IEC 42007 は AI システムの適合性評価に関するハイレベル・フレームワークを規定した規格として、ISO/CASCO との共同 WG である JWG6 にて開発中の国際規格である。こちらは ISO/CASCO で改定中の ISO/IEC 17067 と連動する形で開発が進められている。ISO/IEC 17067 は製品認証についての要求事項を規定している ISO/IEC 17065 に対する認証スキームに関する規格であったが、現在の改定では製品認証に対する適合性評価スキームだけではなく、全ての適合性評価スキームへと拡大し開発をしている。

4.2. AI マネジメントシステム (ISO/IEC 42001) 認証

ISO/IEC 42001 に基づく AIMS 認証の評価対象は、AI システムの開発・提供・利用を行う組織である。

ISMS 等のマネジメントシステム認証を含む認定機関による国際的な協力体制である APAC や IAF 等では、加盟認定機関による相互評価を通じて、各認定機関が行う認定の同等性が確認されている。これにより、加盟認定機関の間で、認定された認証機関が発行する認証が国際的に同等であることを示すのが相互承認協定である。

AIMS 認証についても、国際規格の開発とともに同様の国際的枠組みの整備が進められている。2024 年 7 月にアラブ首長国連邦 (UAE) で開催された APAC の相互承認協定 (MRA) 諮問会議において、AIMS 認証機関に対する要求事項である ISO/IEC 42006 の発行後、APAC の相互承認協定 (MRA) に、ISO/IEC 42001 に基づく AIMS 認証に対する認定を追加することが合意された。これにより、将来的には APAC に加盟する認定機関が認定した認証機関による AIMS の認証の国際的な同等性が担保される見込みであり、既に APAC AIMS MRA の署名に向けて準備している海外認定機関があるとみられる。また、2025 年 10 月にバンコクで開催された IAF 技術委員会 (IAF TC) において、相互承認協定に AIMS も含めることを新団体 Global Accreditation Cooperation Incorporated において継続検討することが示された。

一方で、AI マネジメントシステムに対する関心の高まりを背景として、ISO/IEC 42006 の発行前から、一部の国・地域では既に AIMS に関する認証及び認証機関の認定の取組が先行的に進められてきた。例えば、米国、韓国、インド、オランダ、シンガポールなどにおいて ISO/IEC 42006 発行前から AIMS 認証機関の認定及び AIMS の認証が開始されており、Microsoft、Google、Samson 等が認証を取得している。

日本では ISMS-AC が 2025 年 7 月の ISO/IEC 42006 発行に伴い AIMS 認証機関の認定を開始し、既に 2 つの機関を AIMS の認証機関として認定している。また、これらの認定を受けた認証機関によって日本国内で複数の組織が AIMS 認証を取得している。

4.3. EU AI Act

EU AI Act³⁶ではリスクベースで AI システムに対する要求事項が整理されており、そのうち特にハイリスク AI システムに対しては、法規制に紐づく形で適合性評価が求められている。EU AI Act におけるハイリスク AI とは以下のような分野で利用されている AI を示している。

- 医療機器
- 重要インフラ
- 雇用・採用
- 教育評価
- 法執行
- 司法分野
- 信用評価 など

ハイリスク AI に対する適合性評価で評価される項目としては、以下の項目が想定されている。

- リスクマネジメント体制
- データガバナンス
- 技術文書
- 記録保持
- 透明性・利用者への情報提供
- 人間の監督
- 精度・堅牢性・サイバーセキュリティ要件

一方で、適合性を確認する標準は EU において作成中の段階である。欧州委員会から欧州標準化機関における CEN/CENELEC JTC21 に対して規格開発要求 (Standard Request) が 10 項目出ている。現在開発中の調和規格 (Harmonised Standard) については、JTC21 の HP³⁷にて公開されている。

5.3 節で示した ISO/IEC 42001 認証は国際的な枠組みで実施されているが、それ単体で強制性をもつものではなく、いわゆるボランタリーな (規制への対応ではない) 活動である。欧州においては、各規制当局 (例えば DG CONNECT 等) において規制 (法) が定められ、それに準拠するための一つの方策としての整合規格を活用する場合がある。これらの枠組みについては、特に CE マーキング制度において顕著になっており、NLF (New Legislative Framework) とよばれる製品の安全性と市場監視を強化することを目的に 2010 年より開始した法制枠組みのなかで実装

³⁶ EU Artificial Intelligence Act, The AI Act Explorer

<https://artificialintelligenceact.eu/ai-act-explorer/>

³⁷ CEN/CENELEC JTC21

<https://jtc21.eu/>

されている。EU AI Act においても NLF の枠組みのなかで、既に公表されている ISO/IEC などの内容も考慮して、システムティックに法と標準と適合性評価に関する対応が策定される。

4.4. その他の動向など

新たな適合性評価に関する提案として、EY と Microsoft から Joint Certification に関する白書³⁸が提出されている。これはプライバシーマネジメントシステム規格である ISO/IEC 27701 において規格本文にあたる部分は従来のマネジメントシステム認証としてとらえ、付属書にある管理策については製品認証の枠組みである ISO/IEC 17065 に基づく評価を考慮することでより自然な評価が行えるのではないかという発想であり、これを可能とするには現行の ISO/IEC 17067 を拡張すべきであり、これはプライバシーマネジメントシステム規格のみならず他のマネジメントシステム規格、特に、ISO/IEC 42001 にも適用すべきではないかといった提案である。実際に ISO/IEC AI workshop において Joint Certification に関するプレゼンテーションも行われている。プライバシーマネジメントシステムや AI マネジメントシステムを構築する際に、IT システムや AI システムが組織において活用されることを考えると、使用する IT システムや AI システムが適切なものであることを保証することは健全なマネジメントシステムの構築では自然なことである。また、Microsoft は SC42 や CASCO の活動にも積極的に参加しており、SC42 ウィーン総会において米国のエキスパート（Microsoft 所属）とオーストラリア代表の共同提案という形で WG1 内においてプレゼンテーションが行われた。その後も継続した活動が続けられその影響が顕在化している。事実、ISO/IEC 17067 は製品認証スキームだけではなく、全ての適合性評価スキームへと拡張する形で改定が進んでおり、ISO/IEC 42007 の開発においても ISO/IEC 17067 と連動する形で開発されており、実際の国際標準化活動として Joint Certification への活動が進行していると考えられることができる。

ここで Joint Certification を製品評価と組織評価と同時に行うものであるとだけとらえては本質的な事項を見失う可能性があることを指摘しておく。JIS 制度においても、CE マーキング制度においても対象は製品ではあるものの、製品が適切に（大量）生産することが可能となる組織のマネジメントシステムも併せて評価する。つまり、製品と組織の両方を評価するだけでは、特に新規性はない。マネジメントシステムの構築に IT システムや AI システムの活用が不可欠であるという事実とともに、マネジメントシステムを運用する上でも IT や AI システムを使用しなければならないというなかでの、当該システムに関する評価の必要性に端を発したものであるとともに、IT システムや AI システムなどアップデートが従来の製品よりも頻繁におこなわれる対象に対して適合性評価がどうあるべきなのかといった点からも Joint Certification をとらえなければならない。

³⁸ LinkedIn, Kim Lucy

https://www.linkedin.com/posts/kimberlylucy_a-joint-certification-approach-for-digital-activity-6914989025967689728-fm-r/?utm_source=linkedin_share&utm_medium=member_desktop_web

5.

適合性評価 SWG における取組

5.1. 適合性評価 SWG について

本文書の背景でも記載したが、AI はサービス形態や運用体制とともに動的に変化し続け、サービスの提供においてはステークホルダが多数いる場合が多く、そのためサプライチェーンやバリューチェーンをも含めて包括的にとらえる必要があり、従来の製品・人・組織単位の縦割りかつ一過性な適合性評価では、変化し続ける対象に対する評価に対応しきれないのではないかという問題意識がある。そのため、イノベーション推進と AI セーフティの確保に役立つ AI 適合性評価の検討が必要であり、その検討には、相互運用や相互承認も含めることが重要であるため、国際標準化や諸外国における関連する活動も考慮する必要がある。

AI適合性評価

AISI Japan AI Safety Institute

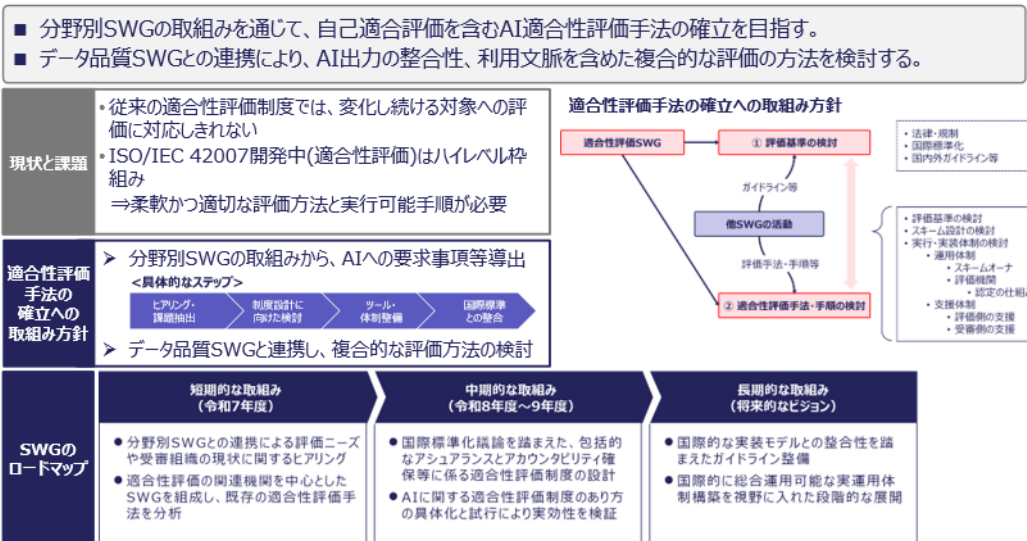
- AI法においても標準の活用がうたわれており、標準に準拠していることを示すには適合性評価が重要
 - 欧州における法規制とその実装のための標準（整合規格）の活用（NLF）が知られているが、標準は法に比べて、まだ、柔軟に改定ができる（Amendmentも含め）
 - 特にAIなど技術革新のスピードが速く、社会的影響が大きいものに対しては法と標準の関係を明らかにしつつ、法に準拠していることを、関連する標準への準拠に置き換えていく必要がある
 - AIを含むDigitalプロダクト／サービスに対する適合性評価を考えると、
 - **変化が前提**：対象が変化し続ける、環境の変化も発生、それに応じてガバナンス・マネジメントも変化せざるを得ない
 - **関係者が多様**：マルチステークホルダ、サプライチェーンのみならず、リスクチェーン、バリューチェーンなども考慮する必要がある
- ↓
- **問い**：組織／要員／製品と縦割りでの適合性評価でAIセーフティを担保できるのか？

14

図 5-1 AI 適合性評価の概要

このような問題意識と課題解決に向け、AISI 事業実証 WG に分野横断 SWG の一つである適合性評価 SWG を設置した。適合性評価 SWG では、適合性評価に携わっている国内の認定機関、標準開発機関（ISO/CASCO、SC42 で活動されている機関）の有識者、専門家からなる有識者委員会を組成して、既存の適合性評価の整理とともに AI 適合性評価の在り方について検討している。検討にあたっては、SC42 にて規格開発が進められている人と AI（マシン）が協働してチームをなしサービス等を提供する仕組みである Human-Machine Teaming（HMT）を題材にし、HMT を評価対象としたときの AI 適合性評価の在り方、課題、問題点の抽出を実施した。HMT では、チームの評価をどうすべきか、提供されるサービスを評価する場合にどうすべきか等、従来の適合性評価の枠組みだけでは対応できない部分が出現すると考えたからである。

適合性評価SWGの概要



20

図 5-2 適合性評価 SWG の概要

適合性評価 SWG は内閣府の「研究開発と Society 5.0 との橋渡しプログラム (BRiDGE)」における「AI 分野における Joint Certification の検討」と連動する形で進めている。BRiDGE では、以下の 4 点の実施を予定している。

- ① AI 分野における Joint Certification に関する調査
- ② 勝ち筋シナリオの策定
- ③ パイロット評価の検討と関係機関との調整
- ④ AI 標準化及び適合性評価人材育成プログラムの検討

今年度は①と②を実施、特に②については適合性評価 SWG と合同で AI 適合性評価について我が国の勝ち筋シナリオの策定のための議論を行った。また、①については、海外の関係者 (SC42 及び CEN/CENELEC JTC21) と意見交換を実施した。加えて、京都大学との共同研究 (京都大学と IPA 及び AISI) においては Software Defined Society を支えるためのリーガルエンジニアリング (LE4SDS) の中で、法と標準と適合性評価の関係を明確にし、法が正しく機能していることの証跡としての適合性評価の役割について検討した。

BRIDGE標準活用加速化支援事業の取組み

AI分野に対するJoint Certificationの検討

- ◆ 調査：海外関係機関との意見交換と連携
- ◆ AI適合性評価の検討（パイロット評価等）、勝ち筋シナリオの検討（適合性評価SWGと合同委員会）
- ◆ 京都大学と共同研究（IPA・AISII）：Legal Engineering for Software Defined Society
 - ・ AIセーフティ評価とAI適合性評価の関係整理／既存の適合性評価再考
 - ・ 相互運用／相互承認に向けて

AI適合性評価

- ・ AI法においても標準の活用がたわわており、標準に準拠していることを示すには適合性評価が重要
 - ・ 欧州における法規制とその実装のための標準（整合規格）の活用（NLF）が知られているが、標準は法に比べて、まだ、柔軟に改定ができる（Amendmentも含め）
 - ・ 特にAIなど技術革新のスピードが速く、社会的影響が大きいものに対しては法と標準の関係を明らかにしつつ、法に準拠していることを、関連する標準への準拠に置き換えていく必要がある
 - ・ AIを含むDigitalプロダクト／サービスに対する適合性評価を考えると、
 - ・ **変化が前提**：対象が変化し続ける、環境の変化も発生、それに応じてガバナンス・マネジメントも変化せざるを得ない
 - ・ **関係者が多様**：マルチステークホルダー、サプライチェーンのみならず、リスクチェーン、バリューチェーンなども考慮する必要がある
- ⇓
- ・ 問い：組織／要員／製品と権限での適合性評価でAIセーフティを担保できるのか？

体制・参加組織

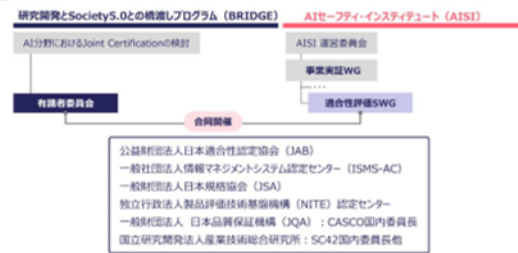


図 5-3 BRIDGE との連携

次年度以降も、AI 国際標準化活動（SC42 をメインに）と連動しながら、欧州 AI 法と整合規格、適合性評価手法などを分析しながら進めていく計画である。

翻って、AI 適合性評価を考える場合、考慮すべき事項は多岐に渡り、その制度設計を考えたとき、我が国だけのルール（ガラパゴス化）とならないように国際的な相互運用と相互承認を考える必要があり、その点においても国際規格を活用することが重要となる。

AI適合性評価：考えるべき事項

・ 制度設計に向けた検討

相互運用・相互承認

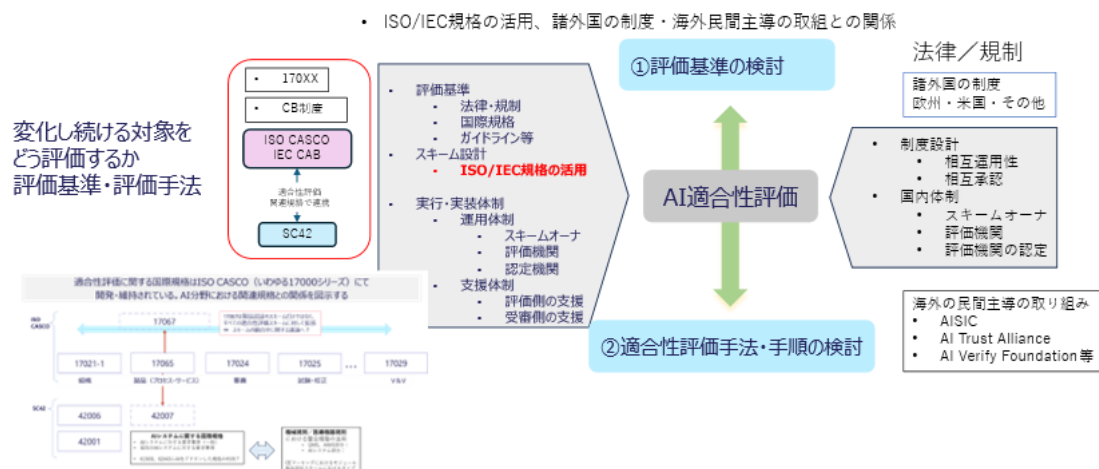


図 5-4 AI 適合性評価において考えるべき事項

5.2. 2025 年度 of 取組

ここまでの整理を踏まえると、国内の AI に関する取組においては「戦略・構想」や「法律・規制」はあるが、基本的にはガイドライン等をベースにソフトローな枠組みを構築していることが確認できた。そのため、ソフトローな枠組みで AI の安全性を確保することができるような適合性評価手法・運用手順を検討、開発していくことが重要である。

そのような検討を目指すうえで、AI 適合性評価に関する様々な観点の検討が必要である。例えば、下図に示す通り、AI 適合性評価においては、多様な評価対象が検討され、多様な評価対象に対する適合性評価スキームが必要である。そのため、AI 適合性評価における評価対象の在り方や、多様な評価対象の認証スキームの統合化に向けた各機関との協働の在り方などを検討する必要がある。これらに加えて、評価側と AI サービス提供者（受審）側との密なコミュニケーション、国内の法律・ガイドラインとの対応、国際調和などの観点も考慮しつつ、AI セーフティに資する適合性評価の在り方を検討する必要がある。

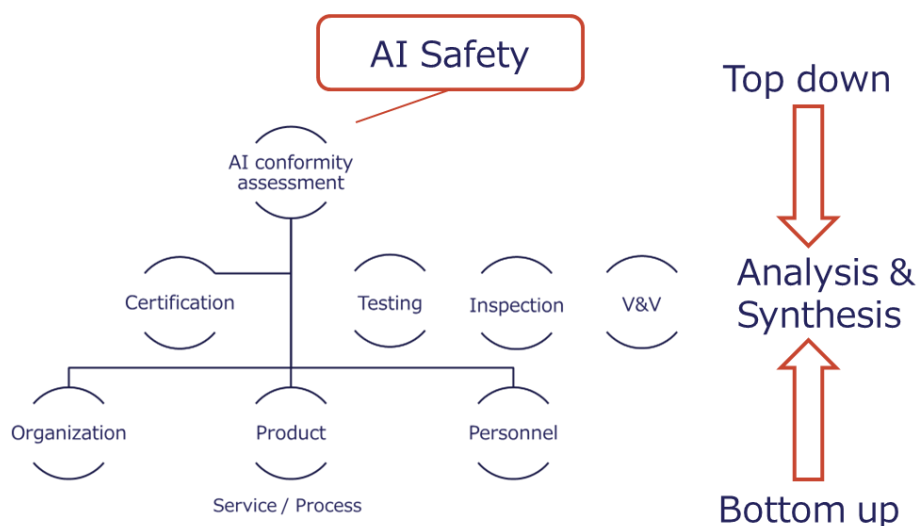


図 5-5 AI 適合性評価のイメージ図

検討すべき観点を踏まえて、2025 年度としては、「既存の適合性評価の整理」と「AI 適合性評価の在り方」について検討を実施した。「既存の適合性評価の整理」については、4 章の通りである。「AI 適合性評価の在り方」については、AI 適合性評価における評価対象の在り方を整理するために、Human-Machine Teaming(HMT)を題材に検討を行った。

1. 既存の適合性評価の整理

適合性評価 SWG の参加組織の活動に関連する適合性評価活動、標準化活動について報告し、それを整理することにより既存の適合性評価（制度）をまとめた。

2. AI 適合性評価の在り方について検討

SC42 にて開発中の人と AI が連携してチームとなりサービス等を提供する HMT を題材にして、評価対象とその評価方法、課題などについて専門的知見から意見を募り、整理した。

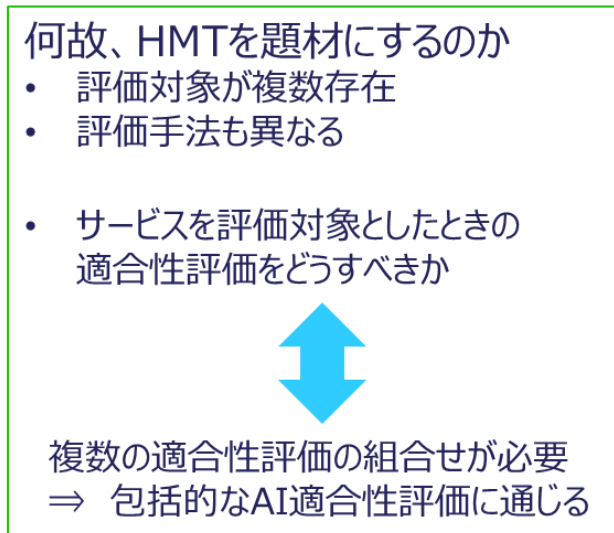


図 5-6 HMT を題材とする理由

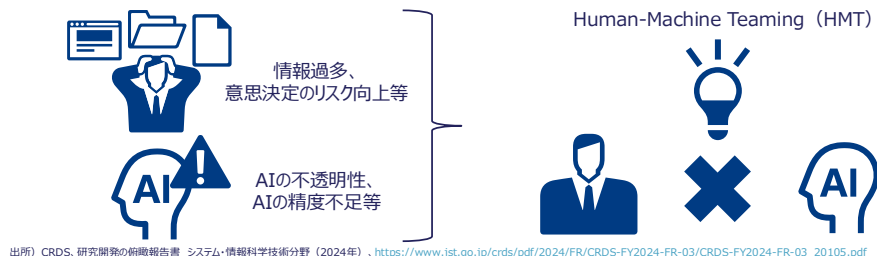
5.3. HMT の概要紹介

5.1 で紹介した SC42 では、AI において重要な概念である HMT に関する国際標準化が進められている。

Human-Machine Teaming (HMT) とは

AISI Japan AI Safety Institute

- Human-Machine Teaming (HMT) は、ISO/IEC 22989:2022「Artificial intelligence concepts and terminology」において、「Integration of human interaction with machine intelligence capabilities」として定義された概念である。
- 日本語では、「人・AI協働」とほぼ同義であり、目的達成に向けて人とAIが協力して取り組むことを示している。
- 本概念が生まれた背景として、情報化社会において人間のみで意思決定を行うことが難しいと同時に、情報処理に長けている一方でAIも精度が不十分である場合があり、人とAIが協働することの必要性が確認された。
- 上記の背景の中、人とAIの最適な協働の在り方を検討するためにHMTの概念が定義、人とAIの協働が類型化されている。



15

図 5-7 HMT の概要

HMT は、ISO/IEC 22989:2022 「Artificial intelligence concepts and terminology」において、「Integration of human interaction with machine intelligence capabilities」として定義されている。日本語では、「人・AI協働」とほぼ同義であり、目的達成（サービス提供等）に向けて人とAIが

協力して取り組むことを示している。本概念が生まれた背景として、情報化社会において人間のみに意思決定を行うことが難しいと同時に、情報処理に長けている一方で AI も精度が不十分である場合があり、人と AI が協働することの必要性が確認されたことによる。上記の背景の中、人と AI の最適な協働の在り方を検討するために HMT の類型化がされている³⁹。

AI において HMT を検討することでもたらすメリットとしては、下図の通り大きく 5 点あげられる。これらが実社会に与える影響としては、AI 社会における人間の職の増加、医療などの法制度の AI 利用と適合する、利用者側の AI システム利用への反発の低減、AI 出力の説明の一部容易化などが挙げられる。

相互補完による 性能・柔軟性の向上	人間の直感・倫理判断・文脈理解とAIのデータ分析能力を組み合わせ、柔軟な判断やAIの性能を向上させる。
意思決定の質の向上	AIのデータを用いた客観性に人間の社会的・倫理的背景を加えることで、透明性・説明責任を持つ意思決定を行うことが可能となる。
安全性・信頼性の向上	完全自律のAI、人間のみの判断と比較して、誤作動や倫理的逸脱のリスクを低減することが可能となる。
ユーザからの 信頼性の向上	完全自動化に対して不安を持つユーザーに対し、「協働」によってユーザーの心理的受容性を高めることが可能である。
学習・適応の促進	人間がAIを学ぶ、AIが人間を学ぶという相互適応の仕組みを構築することで、AI・人間共に成長することが可能である。

図 5-8 HMT がもたらすメリット

HMT においては AI と人間の関係性に応じて、下図の通り 5 つの類型化が検討されている。類型に応じてメリットが異なるため、ユースケースに応じて適切な HMT の在り方を選択することが求められる。

類型	AIと人間の関係性	行動の主体	ユースケース例	メリット
Human supervisor	人間がAIの上位	AI	・ 検索エンジン、経路探索など	・ 安全性・倫理性の担保 ・ AIの暴走リスクを抑制
Human mentor	人間がAIのやや上位	主にAI	・ 画像認識AIを用いた製品検査	・ AIの学習段階から人間の価値観をインプット可能 ・ 必要に応じて人間が手出し可能
Peer	人間とAIが同等	両方	・ 医療用AIと臨床医による高度医療	・ 相互補完・相互学習が可能
Machine mentor	AIが人間のやや上位	主に人間	・ 接客におけるAIのサポート	・ AIが広範な知識を人に提供可能 ・ 人のトレーニングが効率的に可能
Machine supervisor	AIが人間の上位	人間	・ スーパーにおけるAIの商品リコメンド	・ 大規模な効率化が可能 ・ エラー検出・最適化が可能

↑
意思決定の人間の関与度

図 5-9 HMT における AI と人間の協働の類型化

³⁹ JST, 人・AI 共生社会のための基盤技術

<https://www.jst.go.jp/crds/pdf/2024/WR/CRDS-FY2024-WR-08.pdf>

5.4. HMT を題材に AI 適合性評価の在り方を検討

(1) 適合性評価の対象としての HMT

HMT を対象として適合性評価を検討した場合、AI だけでなく、人間、AI と人間の協働関係、サポートする組織など様々な評価対象が存在する。2025 年度の適合性評価 SWG では、以下の 6 点を HMT の評価対象として議論を行った。

- サービス : エンドユーザーに提供される AI が活用されているサービス
- マシン : 実際の AI または AI が搭載されたマシン
- 人 : マシンと連携してサービスを提供する人
- チーム : サービスを提供する人とマシンのチーム
- 組織 : サービスとそれを提供するチームをサポートする組織
- 相互作用 : マシンと人の相互作用

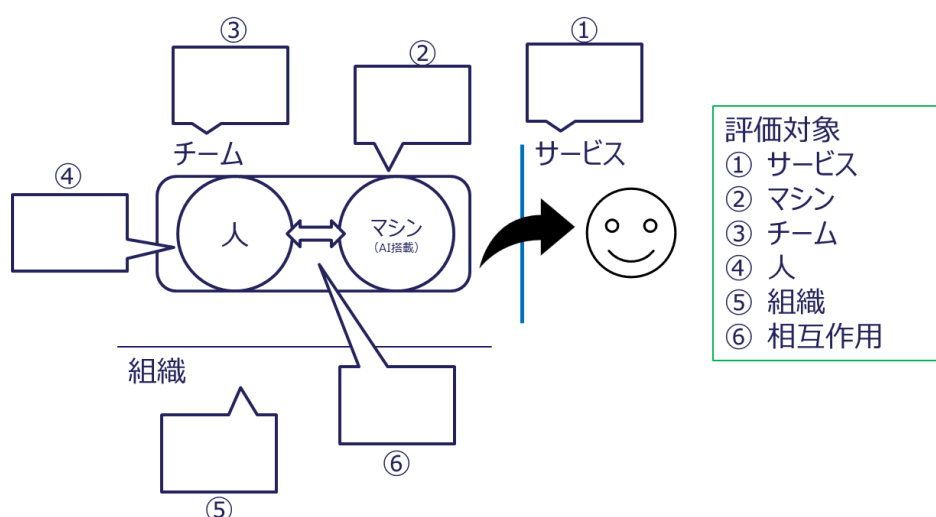


図 5-10 HMT における評価対象

(2) 適合性評価 SWG における HMT を踏まえた AI 適合性評価に関する意見

各評価対象において、起こってほしくないこと、起こってほしいこと、評価対象において参照できる評価方法・関連規格に関する SWG メンバーの意見を以下の通りに整理した。

サービスという観点では、エンドユーザーに対するアウトプットの正しさ（精度・信頼性）、エンドユーザーのアウトプットに対する透明性（安全性・倫理性・説明責任）など、エンドユーザーに届くアウトプットを評価することに対する意見を確認できた。アウトプットを評価するうえでの課題として、プロセスの合理性・運用性以外の観点の評価の可能性、アウトプットの正しさや透明性を測定することが難しい（「適切」などの言葉の定義が難しい）、サービスによってアウトプットが違い共通的に評価できない、という点が挙げられた。

マシンという観点では、マシン（AI）の透明性、人（Human Expert）への有用な情報提供、予測不可能な行動が起きないことなど、サービスと同様にマシンのアウトプットの評価に加えて、よりマシン自体の安全性・信頼性の評価が必要ではないかという意見を確認できた。課題として、

行動の主体(≒HMT の類型)に応じて基準/レベルを変動させる必要があるという意見があった。

チームという観点では、人と AI が協働すること自体への評価(技術的な依存度、生産性の向上など)に加えて、協働における責任の所在を評価する必要性に関する意見を確認できた。課題としては、エンドユーザーにとってはチームの評価は重要性が低く、他の観点の中で評価することで十分ではないかという意見があった。

人という観点では、人がマシン(AI)の判断を適切に評価できる点、人がマシン(AI)の特性を理解できている点など、人がどの程度マシン(AI)を理解できたうえで判断できる能力を持っているかという観点の評価に関する意見が多くあった。また、課題としては、人の能力を図る際には、知識・技能を扱う能力に対する評価や適格性以外での評価の必要性等に関する意見があった。

組織という観点では、マシン(AI)の学習などに関する管理、人に対する計画、チームにおける責任分界など、組織がチームを管理するうえで必要な観点の評価に関する意見が多くあった。また、課題としては、既にある AI マネジメントシステムに関する規格である ISO/IEC 42001 との連携に関する意見があった。

相互作用という観点では、人とマシンの役割分担やその役割分担に応じた連携の関連での評価に関する意見があった。課題としてはチームの観点と同様に、エンドユーザーにとってはチーム(協働)の評価は重要性が低く、他の観点の中で評価することで十分ではないかという意見があった。

その他の意見として、AI システムにおける責任という観点では、提供者または運用者(≒組織)が担う前提となっているため、組織を評価することが重要ではないかという意見が複数あった。また、HMT を踏まえた評価がエンドユーザーのアウトプットの評価にどうつながるかという点、HMT の類型によって評価基準が変動する可能性があるなど、HMT における評価についての意見も複数あった。

(3) 適合性評価 SWG における意見の取りまとめ

全体を通して、エンドユーザーに提供するアウトプットのセーフティ(安全性・信頼性等)を保つことが重要であるという意見が多くあった。そのため、HMT を踏まえた評価では、「①サービス」のセーフティを評価するうえで、②～⑥の評価を実施するという整理になると考えられる。

一方で、整理した 6 つの観点を全て評価する必要がないという意見も確認された。特に「③チーム」や「⑥相互作用」に関しては明確な評価は必要ではないという意見があると同時に、「⑤組織」において重要視されている評価観点と類似していることから、「⑤組織」の観点に「③チーム」や「⑥相互作用」を含めることも一案だと考えられる。

また、現行の「ISO/IEC 42001」は、「③チーム」、「④人」、「⑤組織」、「⑥相互作用」が全体的に含まれているという意見もあり、今後は「②マシン」の評価ができる認証と連携することが重要だと考えられる。加えて、「④人」に関しては、適合性評価ではない方針も検討できるという意見があった。

現在の適合性評価 SWG の意見を取りまとめると、「HMT における「①サービス」の評価には、「ISO/IEC 42001」における「⑤組織」(「③チーム」、「⑥相互作用」含む)の評価に加えて、「②

マシン」の評価、「④人」の評価を連携したスキームが必要」という考えが一案だと考えられる。

また、ロボティクス SWG で検討している配膳ロボットを HMT で捉えると、レストラン側の管理者 (Human expert) と配膳ロボットがチーム (Human-machine team) を構成し、Human supervisor type の関係性になると思われる。この関係性に対する要求事項は ISO/IEC 25589 (Framework for human-machine teaming) に規定されている。加えて、客 (Human end user) との関係も含めた安全確保 (客が配膳ロボットの通り道に突然現れたり立ち塞がったりしない) も論点となり、これについても間接的な要求事項として規定されているところである。このあたりの動向も踏まえて議論すべきではないかという意見があった。

5.5. 今後の課題

今年度、HMT を評価対象としたときの AI 適合性評価の課題や問題点について確認できた。次年度以降は、より詳細な分析を進めるとともに、具体的な AI 適合性評価の制度設計にも着手して行くことを検討する。その際に、誰が制度の主体 (スキームオーナー) となるべきかについても検討が必要となるが、これは適合性評価 SWG の活動を越える論点となるため、関係府省庁も交えながら進めていく必要がある。

本報告書は AI 適合性評価のあり方について AISI 事業実証 WG における適合性評価 SWG において有識者と検討した（現時点での）結果を整理したものである。AI を取り巻く状況は日々アップデートされているため、報告書の内容もそれに合わせてアップデートしていく必要がある。

また、来年度の適合性評価 SWG の活動としては、今年度の適合性評価 SWG 参加メンバー以外にも、評価機関（認証機関や試験機関）および受審側組織（業界団体等）にも参加を促し、拡大した形で進めていく予定である。

AISI 事業実証 WG には分野別 SWG としてヘルスケア SWG とロボティクス SWG があり、それぞれ AI セーフティに関するガイドラインなどを提供している。それらの SWG と連携を深くすることとし、AI セーフティ評価を支えるための AI 適合性評価についても議論を深めていく必要がある。AI セーフティのあるべき姿については、従来の安全性を超えて、より広い立場から考えていく必要がある。

— 安全性(Safety)とAIセーフティ



- ◆ 安全性(Safety) ~ISO/IEC GUIDE 51:2014(E)~
 - Safety: Freedom from risk which is not tolerable
 - 安全とは、**許容不可なリスクがないこと。**
- ◆ AIセーフティ ~AIセーフティに関する評価観点ガイド~
 - **人間中心**の考え方をもとに、
AI活用に伴う社会的リスク(※)を低減させるための**安全性・公平性**、
個人情報の不適正な利用等を防止するための**プライバシー保護**、
AIシステムの脆弱性等や外部からの攻撃等のリスクに対応するための**セキュリティ確保**、
システムの検証可能性を確保し、
適切な情報提供を行うための**透明性** が保たれた状態。
※社会的リスクには、物理的、心理的、経済的リスクも含む。

AIセーフティとは？ / AIセーフティ評価とは？

17

図 6-1 安全性と AI セーフティ

AI セーフティを考えるうえでは、包括的 (Holistic) なアプローチが不可欠であると考えられる。現状の適合性評価においては、組織・製品・要員といったともすると縦割りの評価に留まっていることもあり、それらの適合性評価の結果をどう組み合わせ、AI セーフティを支えるために必要で本質的な AI 適合性評価とは何かを、原点に回帰して考える必要がある。幸いにも、変化し続けるシステム (サービス) のディペンダビリティに関する研究プロジェクトやアジャイル・ガバナンスに関する報告書、複数のシステム、組織が連携してサービスを提供する場合のガバナンス: SoS (システムオブシステムズ) ガバナンスに関する研究プロジェクトなど関係が深いと考

えられる知見があるため、こちらを AI 分野にアップデートすることで課題解決に向け活動を進めていく予定である。

課題解決のヒントとして: System Thinking, etc.

- ◆ 合成の誤謬 (Fallacy of Composition)
- ◆ Total Optimization ≠ Σ Local Optimization
- ◆ Systems are connected: System of Systems, Open systems

"A system is a way of looking at the world."
 "... a system, any system, is the point of view of one or several observers."
 Gerald M. Weinberg (1975)
 An Introduction to General Systems Thinking

木を見て森を見ず ⇒ 木も見て森も見る
 群盲評象 ⇒ 全容 (貌) 把握



PICARD Theory of Systems



From the Point of View of an Observer

Holistic Approach to Finding the Whole Solution: Using Systems Principles & Concepts, James N Martin

- DEOS Project (JST CREST、研究統括 所 真理雄): Dependable Engineering for Open Systems
 成果の一つとして IEC 62853 Open Systems Dependability 2018

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

https://www.kindaikagaku.co.jp/book_list/detail/9784764904613/

- Agile Governance (METI)

<https://www.meti.go.jp/press/2022/08/20220808001/20220808001.html>

https://www.meti.go.jp/shingikai/mono_info_service/governance_model_kento/index.html

https://www.meti.go.jp/shingikai/mono_info_service/governance_model_kento/pdf/20250930_1.pdf

- SoS Governance guideline (NEDO 産業DX、立命館大学: 研究統括 徳田昭雄)

<https://www.ritsumei.ac.jp/research/idx-agpf/250515-0039-01.pdf> 20

図 6-2 AI セーフティにおける課題解決のヒント

これらの知見を活用しながら、AI サービスが安全・安心・快適に提供されていることをどのように評価するか、その中で AI 適合性評価がサポートできる部分について、今後さらに検討を深めていく。

AI サービスが安全・安心・快適に提供されていること

TrustworthyなDependableなサービスが継続的に提供されていること

Wants and Needs ⇒ Requirements is NOT easy

What is truly wanted and needed for conformity assessment in AI Safety?



This painting is commonly known as the "Selling-Tree Story." It is a very famous illustration that has long been used in software engineering, first appearing in the newsletter of the University of London Computer Centre in 1973.

本質的なもの (要件) を抽出して、AI セーフティ評価、それを (部分的に) サポートする AI 適合性評価の枠組みを構築すること!

Currently activities for AI Conformity Assessment is

Conformity Assessment SWG is examining conformity assessment procedures when HMT is the subject of evaluation.

- Human-Machine Teaming (HMT) : 「Integration of human interaction with machine intelligence capabilities」(ISO/IEC 22989, Artificial intelligence concepts and terminology: 2022)
- HMT has 5 types; Human supervised, Human mentor, Peer-Peer, Machine mentor, and Machine supervised

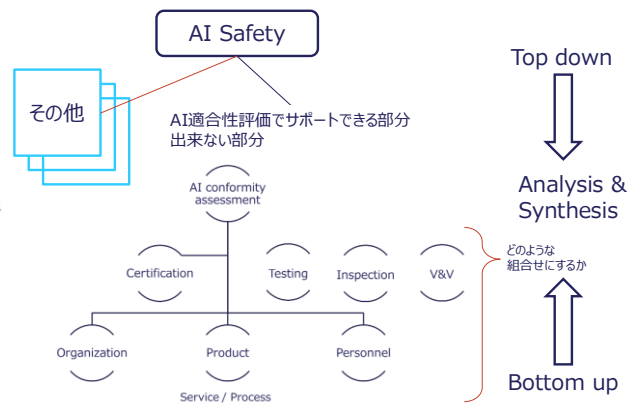


図 6-3 AI サービスが安全・安心・快適に提供されていること

AI 適合性評価の制度設計をするうえでは、審査する側とされる (受審) 側の継続的なコミュニ

ケーションが不可欠であり、評価についても一過性のものではなく AI サービスのライフサイクルを通じた継続的な評価の確立が必要となると考えている。また、受審側の自発的な AI セーフティに関連する活動（HAIP レポート、OECD のガイドライン等への準拠、AI 事業者ガイドラインや AISI のガイドライン等への準拠）も重要となる。一方向ではなく、関係者のすべてが当事者としての意識を持ち、関係者のすべてにとって良し（N方良し）となるような制度設計に向けて活動を継続して行く所存である。

2026年度に向けた活動方針

AISI Japan
AI Safety
Institute

- AI適合性評価の制度設計には、評価側と受審側の継続的なコミュニケーションが不可欠であり、2025年度のメンバーに加えて、適合性評価機関や受審側組織に拡大して進めていく予定である。
 - 評価側としては、AIサービスのライフサイクルを通じて継続的に評価できるAI適合性評価手法の開発を目指すことが望まれる。
 - 受審側としては、自発的なAIセーフティに関連する活動（HAIPレポート、OECDのガイドライン等への準拠、AI事業者ガイドラインやAISIGガイドライン等への準拠とそれらの証跡の確保）も重要となる。
- 2026年度では、評価側・受審側の両方の意見を踏まえて、適切な制度設計を検討していく。

今後の活動：包括的なAI適合性評価制度の構築に向けて、各種適合性評価手法をモジュールとして組合せる方法論の確立へ

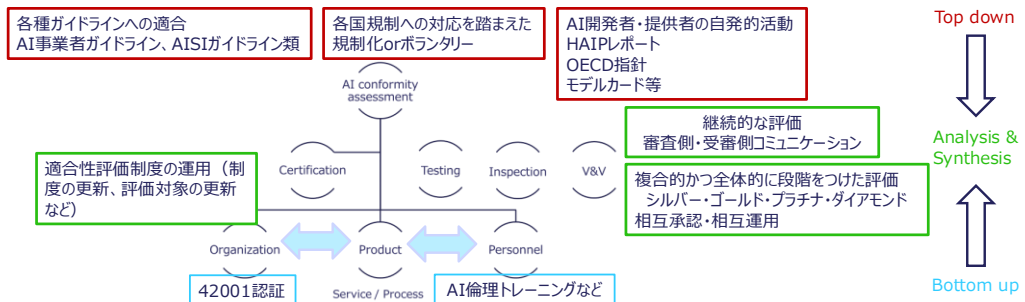


図 6-4 2026 年度の活動方針と AI 適合性評価の制度設計の方針の一例

今後目指していく AI 適合性評価の姿としては、各組織内の評価のみならず、組織間（サプライチェーン・バリューチェーンなど）についても考慮したうえで、組織及びその活動と関係する事項を含めて評価が行えるような、組織及びその活動だけの評価でなく、それらの関係性をも評価できるような、より大きな（一段高いレベルの評価も含めて）枠組みの中でのあるべき姿について検討を進めていく。最終的には、組織内・組織間の評価を総合して、グレードを示す等柔軟な仕組みの構築や、実現可能性について検討を進めていく。

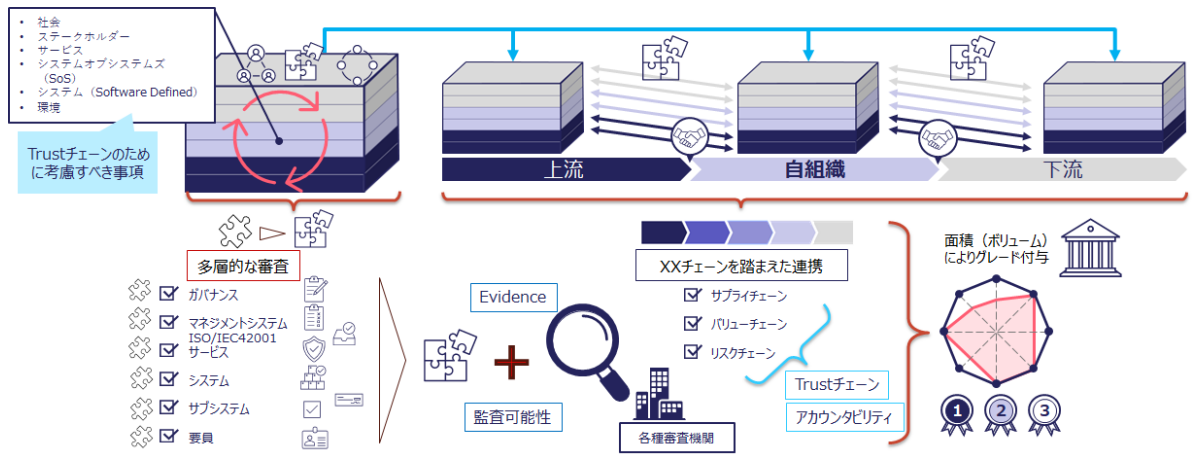


図 6-5 目指していく AI 適合性評価の姿

本章では、今年度の適合性評価 SWG への参加組織と活動状況を紹介する。

7.1. 一般社団法人情報マネジメントシステム認定センター（ISMS-AC）の活動状況

一般社団法人情報マネジメントシステム認定センター（ISMS-AC）⁴⁰は、ISMS 等のマネジメントシステム認証に関する認定機関（Accreditation Body）として、認証機関（Certification Body）が国際規格に基づき適切に審査・認証を実施できる能力と体制を有するかを審査し、認定する役割を担っている。

特に ISMS 適合性評価においては、ISO/IEC 27001 に基づく情報セキュリティマネジメントシステム（ISMS）認証に関し、ISO/IEC 17021-1 および ISO/IEC 27006-1 等に基づき認証機関を審査、認定するとともに、認定した認証機関の一覧および認証取得組織数を公表することにより、情報セキュリティ分野における第三者による認証制度の透明性および信頼性の確保に資する取組を行っている。

また、ISMS-AC は、IAF（International Accreditation Forum: 2026 年 1 月より ILAC と統合し Global Accreditation Cooperation Incorporated へ移行）のアジア太平洋地域における下部組織である APAC（Asia Pacific Accreditation Cooperation、旧 PAC）に 2006 年に加盟、2007 年には IAF に加盟するとともに、その後発足した ISMS の相互承認協定（APAC では MRA と呼ぶ）に署名した。MRA の枠組みの下で他の APAC MRA 署名認定機関から定期的に評価を受けることにより、その認定活動が認定機関に対する要求事項である ISO/IEC 17011 に適合し、他の MRA 署名認定機関と同等に信頼できることが認められている⁴¹。

AI 分野では、ISO/IEC 42001:2023（AI マネジメントシステム）に基づく AIMS 認証に対応する認定業務を開始し、認証機関に対しては ISO/IEC 42006 に基づき審査・認定を実施している。2026 年 1 月 14 日付で、SGS ジャパン株式会社およびテュフ ラインランド ジャパン株式会社を AIMS 認証を提供する認証機関として認定した⁴²。

今後、ISMS-AC は、APAC における AIMS に係る相互承認協定の発足を見据えて、それへの加盟の準備を進めようとしているところである。

⁴⁰ ISMS-AC, 情報マネジメントシステム認定センター（ISMS-AC）

<https://isms.jp>

⁴¹ ISMS-AC, 認定機関の国際的な協力体制

<https://isms.jp/ov/i1tqjm00000065eh.html>

⁴² ISMS-AC が国内の認証機関に対して初の AIMS 認定！

<https://www.jipdec.or.jp/news/pressrelease/20260114.html>

7.2. 公益財団法人日本適合性認定協会（JAB）の活動状況

公益財団法人日本適合性認定協会（JAB）は、適合性評価機関（認証機関、試験所、検査機関等）を審査し、認定する認定機関として活動している⁴³。

JAB の認定の対象分野はマネジメントシステム認証機関、製品認証機関、要員認証機関、温室効果ガス（GHG）妥当性確認・検証機関、ならびに試験所、臨床検査室、検査機関、標準物質生産者、技能試験提供者等に及ぶ。各分野では、認定機関としての運用を定める ISO/IEC 17011 を基礎に、例えばマネジメントシステム認証（ISO/IEC 17021-1）、製品認証（ISO/IEC 17065）、要員認証（ISO/IEC 17024）、試験所（ISO/IEC 17025）等の国際規格に基づいて審査を行う。

また JAB は、国際相互承認の枠組み（IAF、ILAC 等）に基づくピア評価を受け、一定周期で国際的な審査を受けることにより、JAB の認定の国際的な受容性を担保している。認定取得後も、定期審査（サーベイランス）や更新審査を通じて、適合性評価機関の力量およびマネジメントの維持を確認する仕組みを採っている⁴⁴。

7.3. 一般財団法人日本規格協会（JSA）の活動状況

一般財団法人日本規格協会（JSA）は、我が国最大級の総合的な標準化機関として、規格の開発から提供（販売・情報提供）までを担い、標準化政策にも関与している⁴⁵。

JSA グループは、標準化機関である JSA に加え、標準・書籍の提供、研修、組織認証（主としてマネジメントシステム認証）等を担う日本規格協会ソリューションズ株式会社（JSA-SOL）、要員認証（審査員評価登録、翻訳者評価登録、標準化人材登録等）を担う一般財団法人日本要員認証協会（JRCA）等から構成される。これにより、標準の策定・普及に加え、認証（Certification）および要員認証（Personnel Certification）といった適合性評価の実務に関連するサービスもグループ内で提供している。

JSA は、ISO 適合性評価委員会（ISO/CASCO）をはじめとする国内審議団体の運営を通じ、適合性評価に関わる国際規格・指針の国内審議にも関与する。さらに、スタンダード・コンサルティングセンター（SCC）を相談窓口として、企業・団体が標準化に取り組む際の課題整理や、規格・基準開発の支援を行っている。SCC は NEDO、産総研、NITE 等を含む多数のパートナー機関と連携し、関連規格のリスト化や規格間対比（リファレンス整備）、標準化戦略に基づく助言等の支援メニューを示している。

加えて、標準化情報提供サービス（グローバルリサーチセンター）による調査・分析、ならびに企業向け研修・資格制度（国際標準化人材育成講座等）を通じて、標準・適合性評価に関わる

⁴³ JAB, 公益財団法人 日本適合性認定協会(JAB)

<https://www.jab.or.jp/>

⁴⁴ JAB, UPDATE 2023

https://www.jab.or.jp/cms/files/JAB_UPDATES_2023.pdf

⁴⁵ JSA, トップページ

<https://webdesk.jsa.or.jp/>

人材育成と情報基盤整備を行っている。

7.4. 独立行政法人製品評価技術基盤機構認定センター（NITE）の活動状況

独立行政法人製品評価技術基盤機構認定センター（NITE）は、国内の認定機関の一つとして、適合性評価機関（試験所、製品認証機関等）の能力と運用体制を審査し、認定を行っている⁴⁶。認定は、NITE 内の認定センターで行われ、International Accreditation Japan（IAJapan）と呼ばれている。

政策・市場ニーズに応じた認定プログラムの創設・拡充の事例として、NITE は ASNITE（製品評価技術基盤機構認定制度）における製品認証分野で、繊維製品の「Textile Exchange（TE）認証」に係る認定プログラム（2020 年度創設）がある。TE 認証では、認証機関が ISO/IEC 17065 に基づく認定を受けることが求められるとされ、IAJapan は日本国内の認定機関としてスキームオーナー（Textile Exchange）に登録された認証機関に対し認定サービスを提供する。加えて、バイオマス燃料（PKS）認証（2023 年度創設）の事例では、スキームオーナー（一般社団法人農産資源認証協議会）が運営する PKS 認証制度において、認証機関が ISO/IEC 17065 に基づき認定される枠組みが示されている。また、IoT 機器のセキュリティ確保を目的として日本で整備が進められ、IPA が制度運営を行っている JC-STAR 制度において、IAJapan は、IoT 製品の評価を行う試験機関の能力等を認定するプログラム（ASNITE-T(IT)）⁴⁷を運営している。

制度横断の連携として、NITE 資料は日本認定機関協議会（JAC）の枠組みを紹介している。JAC は 2006 年に日本産業標準調査会（JISC）の要請を受けて設置され、IAJapan が事務局⁴⁸を担当している。JAC は国内の複数の認定機関で構成され、運営委員会・メンバー会議および分野別 WG（試験所等を扱う TC1 WG、認証機関等を扱う TC2 WG、戦略 WG）により、認定制度に関連した基盤的課題や戦略的課題の検討を行う体制が示されている。

人材・情報基盤の整備として、NITE は「社会実装・規格活用」実現化人材育成プログラムを掲げ、適合性評価の基礎知識やスキーム構築の技能習得を目的とする講座を開講している企業・業界団体等が参加可能なプログラムとして位置付けられ、受講者アンケート結果等も示されている。さらに、NITE 内に「我が国全体の適合性評価を推進」する組織の設置を検討し、行政・自治体・業界団体・企業等からの相談対応と施策提案を進める方針が示されている。国際的枠組みについては、IAJapan が認定スコープに対応して APAC、グローバル認定協力機構（IAF および ILAC が統合した組織）に関与し、国際相互承認の枠組みの維持に向けた対応状況が示されている⁴⁹。

⁴⁶ NITE, 適合性認定

<https://www.nite.go.jp/iajapan/index.html>

⁴⁷ NITE, IoT 製品のセキュリティ機能・対策の評価を行う機関に対する認定プログラムを開始

https://www.nite.go.jp/iajapan/asnite/information/info_news20260210.html

⁴⁸ NITE, 日本認定機関協議会(JAC)

<https://www.nite.go.jp/iajapan/jac/index.html>

⁴⁹ NITE, 認定機関 NITE 認定センター（IAJapan）の取組-これまでの対応実績と今後の国際・国内展開

https://www.meti.go.jp/policy/economy/hyojun-kijun/std_w_ninsho/pdf/8-7.pdf

7.5. 一般財団法人日本品質保証機構（JQA）の活動状況

一般財団法人日本品質保証機構（JQA）は、製品、システムおよび環境等に関する品質保証を担う機関である。JQA は、適合性評価の業務類型として、試験・検査・認証・校正・検証を掲げ、電気・電子／医療機器／車載機器の認証・試験、マネジメントシステムの認証、計測器の校正・検定、JIS マーク認証、地球環境に関する審査・評価・支援、ロボット安全評価・ドローンサービス品質評価、マテリアル試験等を実施している⁵⁰。

制度・スキーム形成への関与事例として、生活支援ロボット分野における国際標準(ISO 13482) 開発に参画し、認証制度を立上げ、認証サービスを提供している。また、ISO 13482 の IDT 規格である JIS B 8445 が JIS マーク認証の対象となり、認証範囲を拡大している⁵¹。さらに、ドローンサービスについては、サービス品質を保つプロセス要求事項を規定した JIS Y 1011: 2024 の策定に参画し、当該規格に基づく認証制度の立上げ支援と適合性評価を担う⁵²。

サイバーセキュリティ分野では、欧州サイバーレジリエンス法に関連する整合規格検討の動向等を踏まえ、2025 年 4 月からサイバーセキュリティに係る IECCE CB 証明への適用範囲を拡大した⁵³。また、国内では IPA が運営する JC-STAR 制度（セキュリティ要件適合評価およびラベリング制度）における「検証事業者」としてのサービス提供を開始している。

AI に関しては、ISO/IEC 42001（AI マネジメントシステム）の審査サービスを 2026 年 1 月より開始している⁵⁴。

7.6. 国立研究開発法人産業技術総合研究所（AIST）の活動状況

国立研究開発法人産業技術総合研究所（AIST）は、ISO/IEC JTC 1/SC 42 “Artificial intelligence” に関連する国際標準化活動に関与しており、国内委員長を AIST の研究員が務めており、国内委員会を牽引している⁵⁵。同委員会において国際コンベンナ（Convenor）を 4 件確保し、日本提案の国際規格を 15 件成立させた旨が示されている⁵⁶。

また、AIST は AI に関するデータ品質の国際標準である ISO/IEC 5259 シリーズ（第 1 部～第

⁵⁰ JQA, 一般財団法人日本品質保証機構（JQA）

<https://www.jqa.jp/>

⁵¹ JQA, 生活支援ロボットに関する JIS マーク表示制度の認証機関として認証範囲拡大

https://www.jqa.jp/service_list/jis_a/topics/topics_jis_76.html

⁵² JQA, 「DSPA のドローンサービス品質認証制度」開始のお知らせ

https://www.jqa.jp/service_list/fs/topics/topics_fs_73.html

⁵³ JQA, サイバーセキュリティ分野における CB 証明書発行業務開始のお知らせ

https://www.jqa.jp/service_list/safety/topics/topics_safety_649.html

⁵⁴ JQA, ISO/IEC 42001（AI マネジメントシステム）審査サービス開始のお知らせ

https://www.jqa.jp/service_list/management/topics/topics_ms_569.html

⁵⁵ ITSCJ, 委員会一覧

<https://itscj.ipsj.or.jp/committee-activities/committee-list.html>

⁵⁶ 経済産業省, 令和 7 年度 産業標準化事業表彰 経済産業大臣表彰 受賞者インタビュー

<https://www.meti.go.jp/policy/economy/hyojun-kijun/keihatsu/hyosho/interview/R7/20251021-10.html>

5 部) の発行に貢献したことを公表している⁵⁷。同リリースでは、データの収集から利用までのライフサイクル全体における品質向上に資すること、機械学習に特有のデータセット品質課題（バイアス等）を踏まえた指針を提供すること、ならびにリスク管理や法規遵守の支援につながることを示されている。

さらに、安全性が重視される産業分野での AI 利活用に関して、国際技術報告書 ISO/IEC TR 5469:2024 (Functional Safety and Artificial Intelligence) の出版に共同エディタとして貢献した旨を公表している⁵⁸。同リリースでは、AI の特性を踏まえた安全確保の考え方や、従来システムと AI システムを組み合わせる際の留意点等を整理したことが示されている。

⁵⁷ 産業技術総合研究所, 信頼できる人工知能 (AI) 開発に向けて

https://www.aist.go.jp/aist_j/press_release/pr2025/pr20250327/pr20250327.html

⁵⁸ 産業技術総合研究所, 安全性に掛かる産業分野における AI 技術の利用を標準化が後押し

https://www.aist.go.jp/aist_j/press_release/pr2024/pr20240410/pr20240410.html