AI品質合意フレームワークについて

2026年10月6日

妹尾 義樹

標準化オフィサー
知財・標準化推進部/インテリジェントプラットフォーム研究部門
産業技術総合研究所

AI品質マネジメントイニシアティブ　会長

内容

■機械学習AIの品質にまつわる課題

■ビジネスにおけるAI品質合意の重要性

■品質評価の難しさ

■リスクマネジメント

■エコシステムにまたがる品質管理

- AIQMI/WG3　AI合意フレームワーク

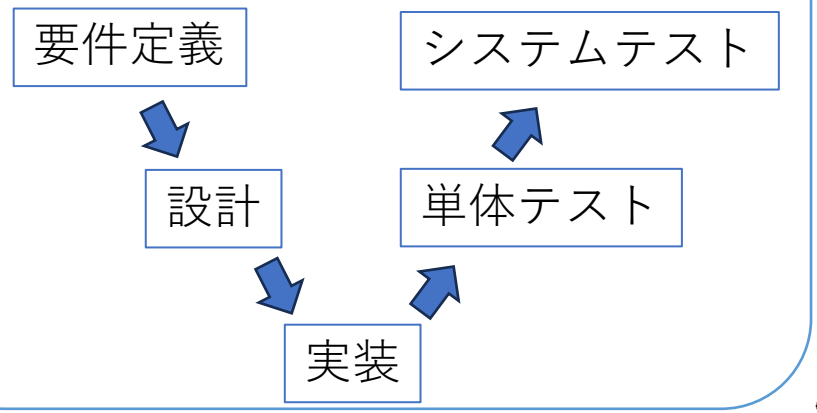
■まとめ

機械学習ＡＩの品質にまつわる課題

データ（お勉強の材料）が機能を決めるAIの品質管理をどうやるか？

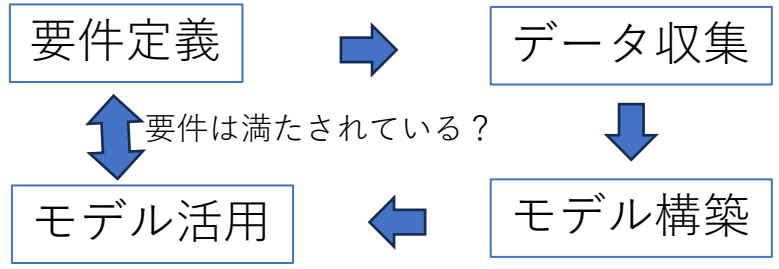
従来のソフトウェア品質保証
どうやればいいかを作りこみ確認

分析的アプローチ



機械学習AI
「お勉強」による機能の作りこみ

帰納的アプローチ





企業側のジレンマ：「一定の品質」を担保・説明できない

AI品質の難しさ：“猫問題”

例：画像中の猫を検出するプログラム

猫の画像、を定義するのは難しい
- 一般的猫の特徴（髭、目、耳、尻尾…）
- 猫の種類（三毛猫、ペルシャ猫、マンチカン…）
- 光の当たり方、撮影角度、猫の姿勢…
- 漫画、顔だけ、しっぽだけ

何に使うか（＝要件）の定義が重要！

■機械学習を使えば、
- 検出ソフトウェアを容易に作成可能
- 訓練画像を集めて学習させるだけ！
  ⇒**判断基準は人には分からないまま**

■どこまで要件を精密に定義して確認するのか？
- 100%厳密に定義するなら演繹的プログラミングできる。









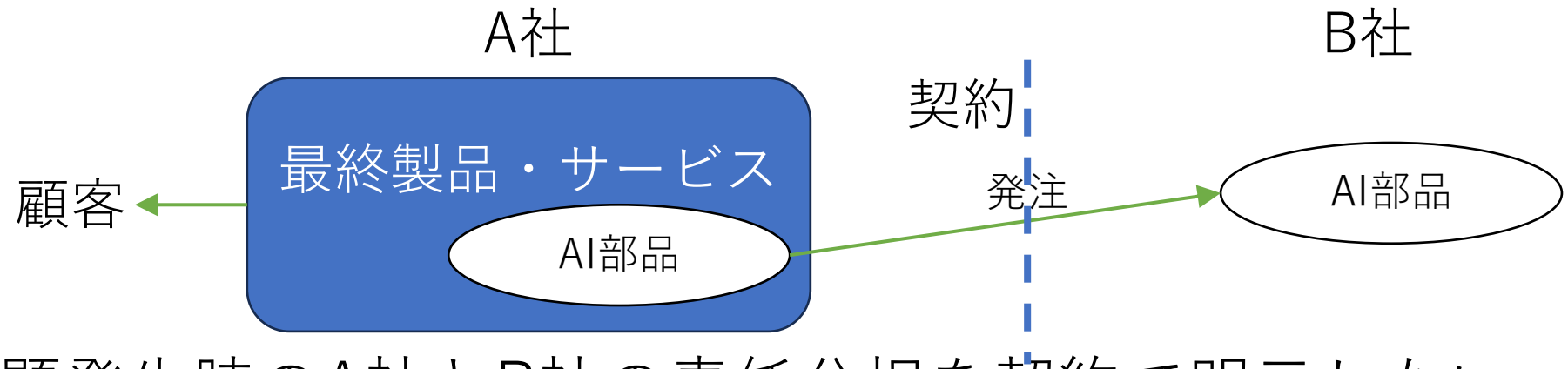


品質マネジメントの肝＝
訓練データが作りこむ機能と定義した要件をどうあわせるか？

ビジネスにおけるAI品質合意の重要性

■AIビジネスのサプライチェーンにおいて、問題発生時の責任分担の明確化（＝品質の合意）は必須の課題。

■例



■問題発生時のA社とB社の責任分担を契約で明示したい。

- 従来型ソフトウェアなら仕様の明確化で対応できるが、訓練データによって帰納的に仕様が定義されるAIの場合には難しい。
- この機能仕様をどのように明確化して合意するかが重要。

■他にも、保険、認証、法律対応などでも重要に。

AIソリューションの構築プロセス



合意形成まで繰り返し、必要に応じて前ステップに戻る
各ステップそれぞれに固有の合意形成が必要
また，全体プロセスの初期における合意も重要

合意できないと、次のステップに進めない

合意の明確化プロセス欠如が、AIソリューション、サービス、コンポーネントの
サプライチェーンでの流通を妨げ、AIビジネス拡大の足かせになる危険性

AIソリューション構築における「想定」とその合意の重要性

■学習データ採取時の環境を実運用時の環境に整合させるため



■問題の例

- スーパーの売上予測で過去1年間データで学習しモデル構築。
  - 先月、競合店が向かいにオープン。構築したモデルでの予測結果が合わない。
  - 先月、近くにオフィスビルが建った。オフィスの稼働日情報がないと弁当の売上予測が当たらない。
- 震災時を含むデータで学習→平常時の予測で問題発生

■想定した環境のモデルと現在の環境の整合性を評価する方法？

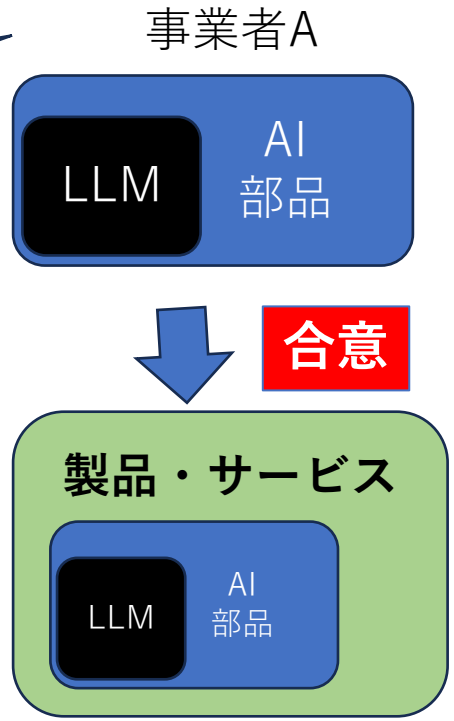
- 一般的には、PoCや実証実験の繰り返しにより整合性を高めるプロセスが必要。

合意の深堀（例）…想定の合意が鍵

■先の検討で洗い出したそれぞれの合意において、合意すべき双方の考え方と、合意に対する期待を深堀する。

事業者A（受注側）の期待

- 納入物の仕様（外部品質）を明確にして納入物の開発にかかるコストを最小化したい。
- 納入後の保守コストを最小化したい。問題発生時の問題切り分けコストを最小化したい。
- 納入後に問題があった場合の責任範囲を明確にして、リスクを最小化したい。
- 納入物の品質の良さを客観的指標で評価して、ベストプラックティスとして横展開したい。
- 納入物の価値を明確にしてできるだけ高く売りたい。強みのノウハウは非開示としたい。
- LLMなどの別部品を活用する場合には、そちらの不具合の責任を取りたくない。



事業者B（発注側）の期待

- 納入物のコストパフォーマンスを最大化したい。（最小コストで最大機能）
- 納入後に発生する問題は、最小コストでAに対応してもらいたい。
- 提供する製品・サービスのリスクアセスメントを完全にやりたい。（納入されるAI部品にかかわるリスクを理解したい）
- 製品・サービス側（AI部品の外側）でやるべきガードレールやリスク回避機構の構築は最小にしたい
- 事業者A以外のベンダとコンペさせていい方を選択したい。
- 問題発生時に備えて事業者Aのガバナンスやマネジメント体制を確認しておきたい
- AI Act.など外部からの要件に対応したい

合意形成と標準，そして認証

■品質に関する合意形成に必要なこと

- 品質要件の合意：どのような品質について合意するのか＝What
- 要件の達成目標（達成基準）の合意：クリアすべき基準＝How Much
- 達成を判定方法の合意＝どうやって，どこまで確認するか＝How

■標準化の役割

- Whatと基準，確認方法などの標準化により，オーダーメードで合意項目を決めなくても，既製品の基準で合意プロセスが簡略化される.
- 基準が標準として設定されることで安心感が得られる.

■認証の役割

- 品質基準をクリアしていることを客観的に示せるようになる.

品質評価の難しさ～基準

■要件定義のあいまいさと出力の正しさの基準

■（例）数字認識の例



- 9の丸部分の大きさ：どこまでを9と認識するか？
- 閾値を明示的に示さないで、訓練データだけで閾値を作りこむ。どのように要件を定義して、どのように正しさを確認するか？

■上記以外にも沢山の同様の境界がある。

- ４や6の空間の大きさ
- 数字自体の大きさ、太さ、カスレ具合
- 数字の傾き

■AIQMガイドラインでは、丸部分の大きさをAttributeとして定義して、それに沿ったカバレッジや、正答率のチェックを要求している。

- どこまで、どうやればいいのか？リスクアセスメントでやるか？
- 郵便番号認識の例ではそこまでの厳密性は求められないが、自動運転向けなどの安全性にかかわるものの認識では厳密性が必要　⇒　どこまで求める？

想定外！

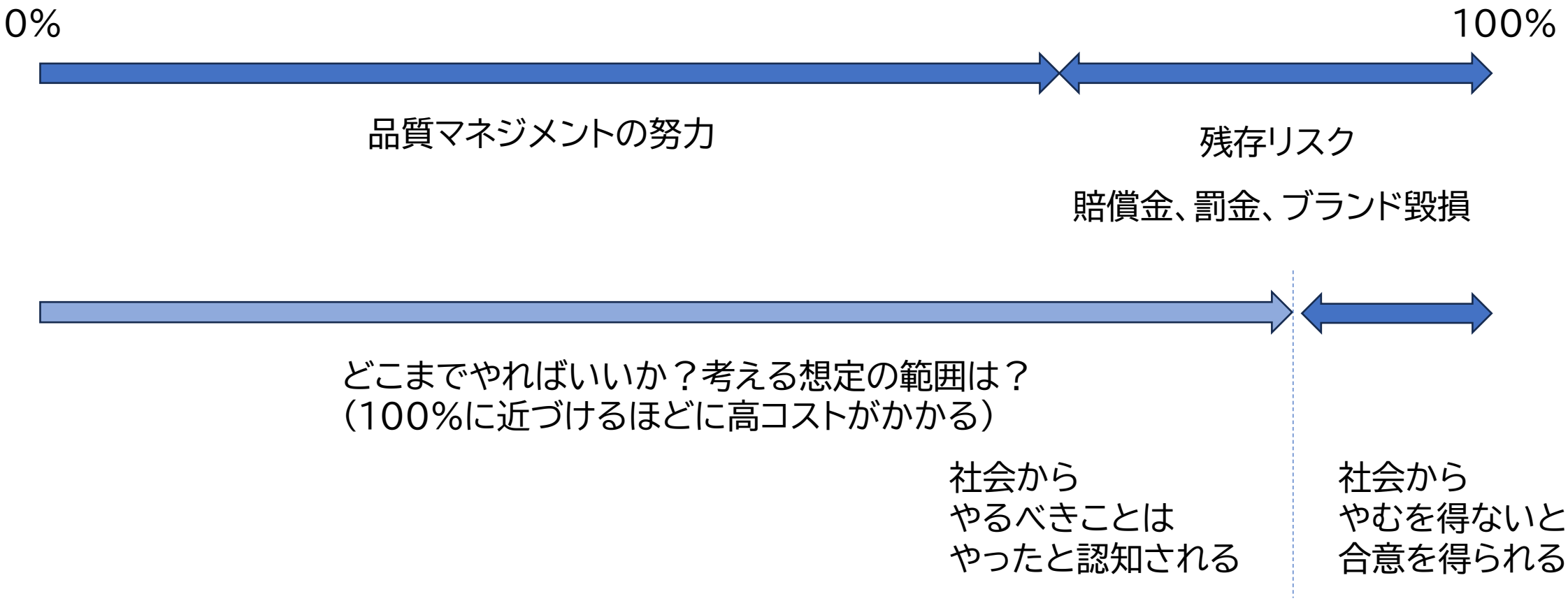


・想定外が来たということを少なくとも認識できる必要性！
・自動化は無理なので、人間との協調作業が必要。
・ライフサイクルにわたるサポートが重要。

リスクマネジメントと社会コンセンサス

「AIの品質マネジメントでは100%の品質保証は不可能」を合意してもなお残る

「どこまでやればいいのか」問題



エコシステムにまたがる品質管理

連携して品質管理し、リスクテイクするために

認証制度のあるべき姿とAIでの製品認証が困難な理由

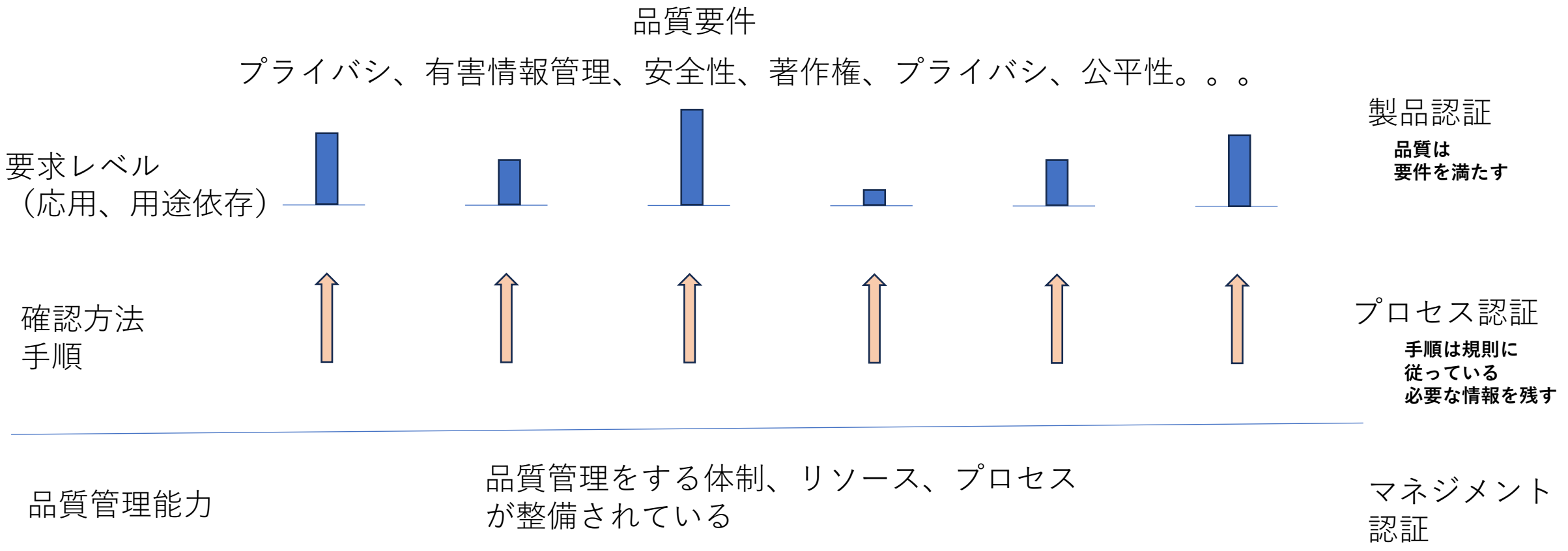
■認証制度は、ステークホルダー間での合意プロセスを「お墨付きを与える」ことで簡素化するためにある。
- 例，AI品質マネジメント標準（ISO/IEC 42001）の認証制度

■品質についての製品認証の効能
- 利用者（発注者）が利用する製品・サービス（納入物件）について、要求する品質が担保されていることを認証により確認できる。
- 開発者は認証（公的/Private）を取れば、個別の合意が必要な際に、第三者のお墨付き（公的/Private）を示して合意できる。
- 利用者（発注者）は第三者の認証により細部を自ら確認することなく安心して使える。

■困難な理由
- マネジメント認証は、開発者のCapabilityを確認することが主眼で、その確認が比較的容易だが、AIの製品認証は、要件が最終用途に大きく依存する。要件に多様性があるものについて、一括した認証フレームワークの構築は困難。
- AIは確率モデルに基づくため、100％の保証が難しい。どこまで確認すれば良いかの問題が付きまとう。
- どんどん進化するAI機能に品質確認手段が追い付かない。

製品認証と多様な品質要件への対応

■製品認証とマネジメント認証の間のプロセス認証

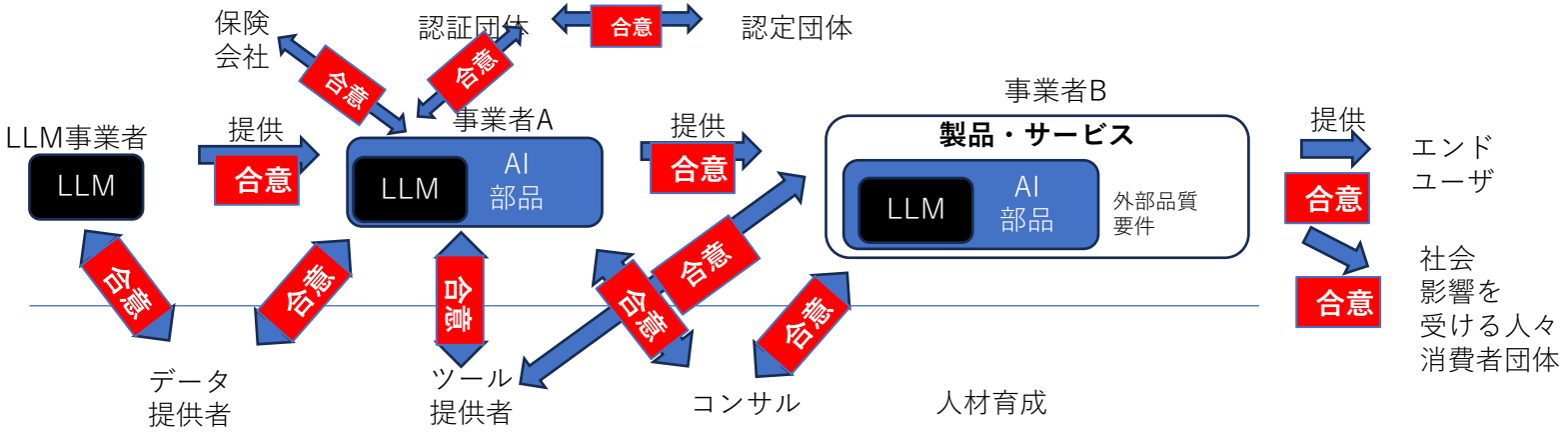


合意の構造

■ プレイヤー間の合意には構造がある。共通部分と特定機能。

■ 構造の要素

- 合意のレベル（どこまでの品質をどこまで確認するか？）
- 共通部分と特定部分の階層構造
- 合意の機能のグルーピング
- 開発・提供するサービスの内容や提供方法、利用形態（社内ユース/コンシューマ向け）。



品質レベル
どれくらいの品質を？

確認レベル
どこまで確認する？

特定個別機能

分別野共通　分別野共通　分別野共通

共通部分

産総研

AI品質マネジメントイニシアティブ
AI Quality Management Initiative

https://aiqm-initiative.cons.aist.go.jp/consortium.html

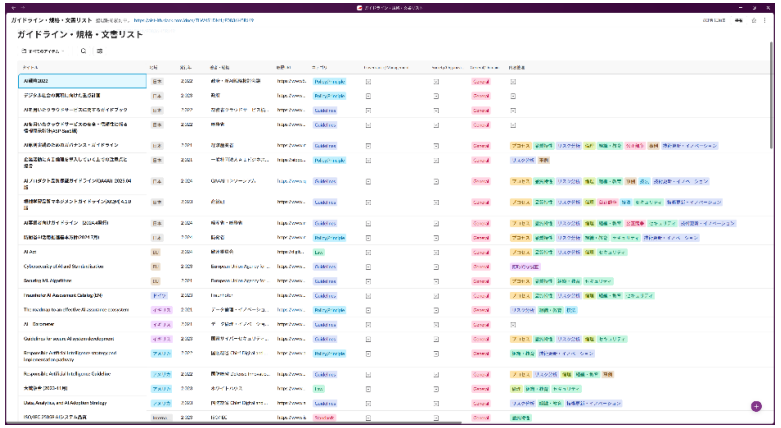
産業界メンバが協調領域について連携してAI品質マネジメントに取り組む

会長: 妹尾義樹(産総研)
副会長: 難波孝彰(産総研)
事務局長: 小西弘一(産総研)

50＋組織から100名以上が参加
2024年9月活動開始

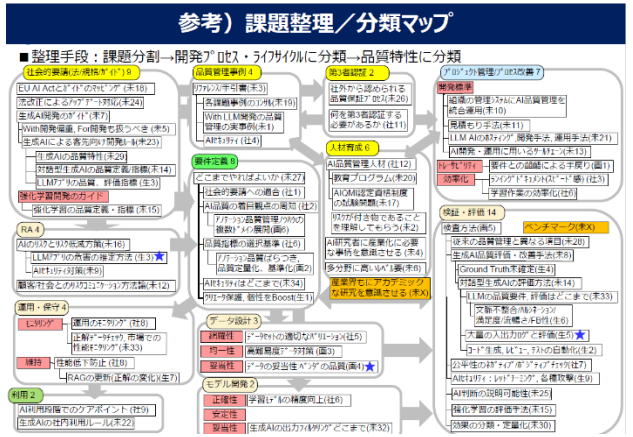
WG1:主査 新原敦介（日立）

To be Updated



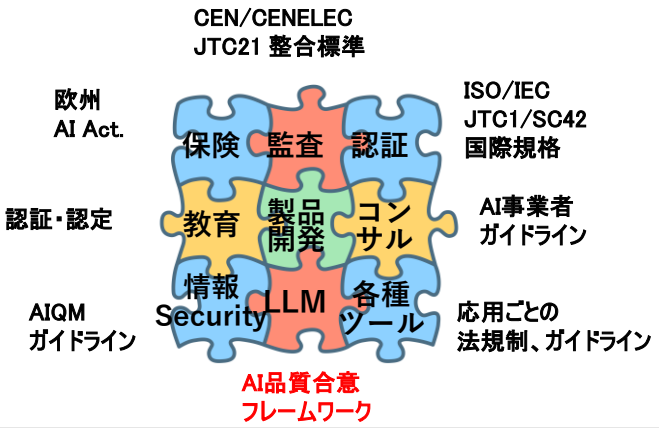
WG2:主査 三島浩一（DynamicRiskM.）

Problem Solving



WG3:主査 山田敦（IBM）

Ecosystem



AI品質合意フレームワークとそのねらい

https://aiqm-initiative.cons.aist.go.jp/pdf/ai_quality_framework_guide_rev1_0.pdf

■エコシステムのプレイヤー間（あるいは社内の部署間）で品質合意の全体像を共有するとともに、何が合意で来ていて、何が合意できていないのかを、連携活動のプロセスに応じて確認できる。品質管理プロセスそのものの合意にも使える。

■ビジネス視点での合意と技術視点での合意をシームレスにつなぐ。

■外部要因を勘案して、合意が必要なものを容易に選択できる。

■アジャイル的な繰り返し開発プロセスでの合意のプロセスを管理できる。

■共通のフレームワークで取引相手と合意できる。

- 現在、AIの品質（特にリスク管理）については、各社が個別のチェックシートなどを作成して対応している。

■問題発生時の責任分担を明確にできる。

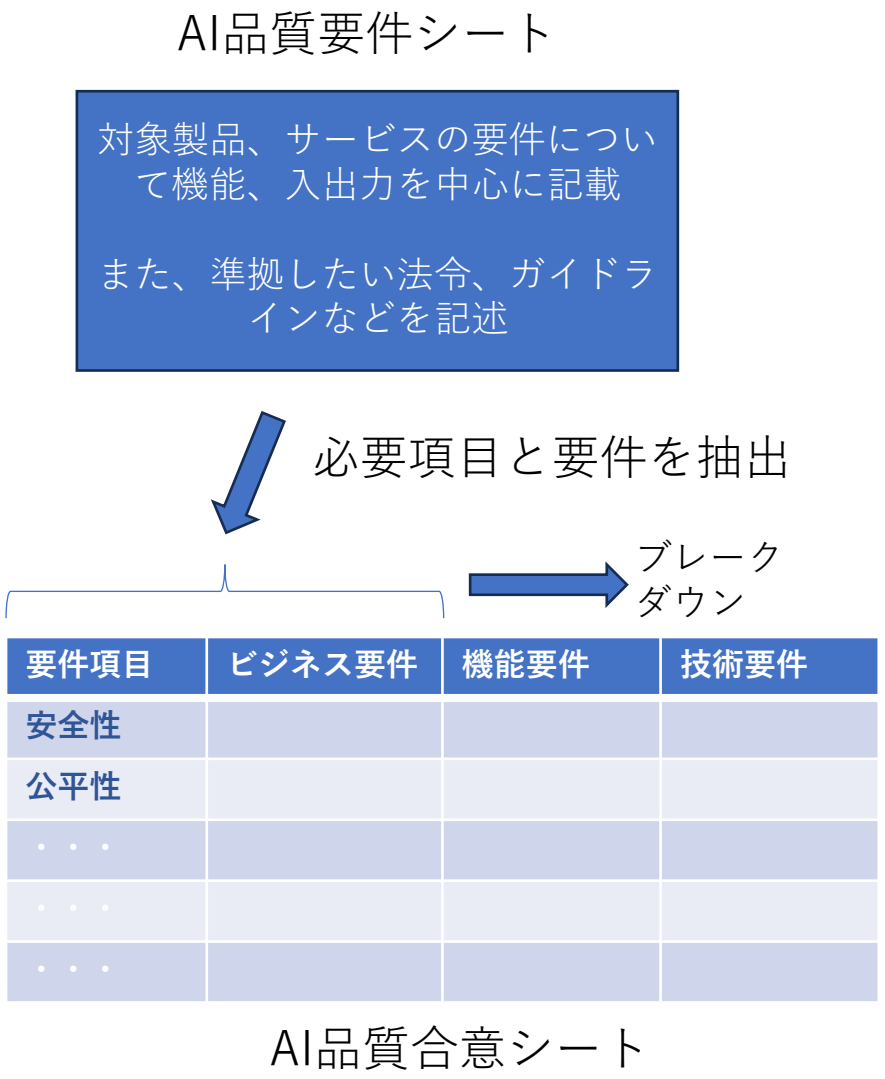
AI品質合意フレームワークの構成

■AI品質要件シート

- 対象製品・サービスの要件を記載
- AI品質要件の膨大な候補リストから合意すべき項目（合意シートのビジネス要件）を容易に抽出できるようにする。
- 企業間の契約書で案件を記載するレベル。

■AI品質合意シート

- AIビジネス要件、AI機能要件、AI技術要件の3段階で合意対象と、その要件を記載。
- 合意、充足の状態を管理
- 改版履歴を管理



AIビジネス要件、AI機能要件、AI技術要件について

要件対象の合意をAIビジネス要件、AI機能要件、AI技術要件の3段階でブレークダウンして管理。

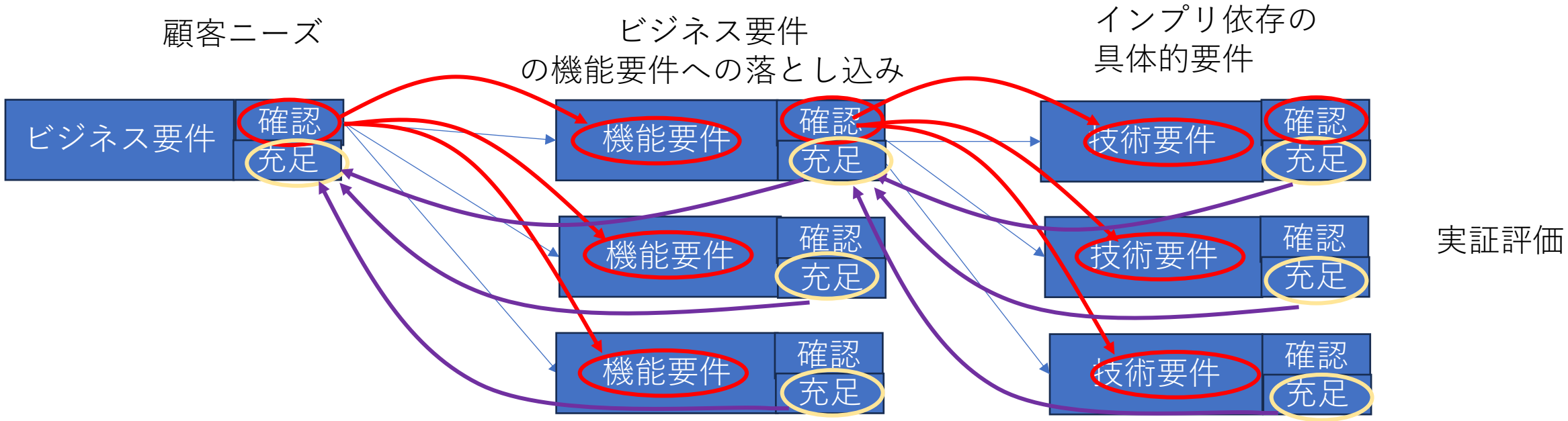
■AIビジネス要件：最終的に構築するサービス/製品に必要な要件を記載。サービス/製品の構築に用いるAIの機能に関連するものを記載。技術内容には踏み込まない。
⇒AI事業者ガイドラインの「開発者にとっての重要な事項」の記載レベル

■AI機能要件：サービス/製品の構築に使われるAIコンポーネントの要件について、AIビジネス要件の充足を確認し、合意するためのものを記載。主に、AIコンポーネントの入出力にかかわる要件を記載する。ただし、インプリメンテーションの詳細には踏み込まない。また、AI技術要件の導出に必要な情報を記載する。
⇒産総研AIQMガイドラインの外部品質のレベル。

■AI技術要件：AI機能要件の充足を確認するための技術要件をインプリメンテーションに踏み込んで、KPIと達成基準の組を列挙する形で記載する。評価方法や用いるテストデータについても明確化する。
⇒産総研AIQMガイドラインの内部品質のチェックを念頭にKPIと達成基準および確認方法を定める。

合意状態について

■それぞれの要件については、要件そのものについて合意できると「確認」、その要件について技術要件など下位の要件の達成によって、当該要件の達成が確認されると、それを「充足」とする。すべてのビジネス要件の「充足」が品質管理プロセスのゴールとなる（運用品質管理は別途必要）



現在のAI合意フレームワークの検討状況

■AI品質合意フレームワーク解説書 Rev1.0を公開
- https://aiqm-initiative.cons.aist.go.jp/pdf/ai_quality_framework_guide_rev1_0.pdf

■具体例に基づいて，AI合意フレームワークの有効性を確認中
- AI合意フレームワークを用いた「産総研チャットボット開発」
- 開発委託側と受託側での合意がうまくできるか確認
- フレームワークの改善，拡張

■他の応用についても実例検証を計画中

■逐一変化する合意を管理するのが困難であることが判明
- GitHubなどのツールを活用した合意管理を検討中

まとめ

■AIの品質マネジメントについて，特にエコシステムでの品質管理のために，ステークホルダー間での合意が非常に重要.

■認証制度により，上記合意が容易になるが，AIで100％が難しいことおよび，AIは水平技術なので，製品認証が困難.

- 製品認証を行うのであれば，応用ドメインで，応用特化型での認証とすべき.

■AIで満たすべき最低限の共通の要件についての製品認証はできるかもしれない.

■プロセス認証の一形態として，合意フレームワークの標準化に大きな可能性を感じている.

END