【資料4-1】

AI事業者ガイドラインの更新に向けた検討

2026年10月30日

AIガバナンス検討会　事務局

1.「はじめに」の更新内容

- 更新ポイントと具体的な更新箇所（概要）

2.「AIによるリスク」の検討ワーキンググループ

- 検討内容の報告

3. 最新技術動向（AIエージェント・フィジカルAI）への対応

- 「対応方針」の記載について
- 「便益・ユースケース」の記載について

4. AIガバナンスに関する動向・事例の反映

- コラムに掲載する事例について

「はじめに」の更新ポイントと具体的な更新箇所（概要）

更新の目的・進め方

- 現在の「はじめに」は7ページあり、**利用者にとって、読みにくさや使いにくさに繋がっている**ため、必要な記載は残しつつも、分量の低減や構成の見直しによって改善を図る。
- 一部の有識者からご意見も伺った上で、**見直し方針の検討と修文案（初版）作成**を実施。
  （現状の修文案はあくまで初版であり、ガイドライン更新に向けて今後さらなる改善を実施予定）

見直しの方針

1. **分量の削減**
   章立ての変更や文章の見直し等
2. **末尾へ「ガイドライン策定経緯」を移動※及び改版履歴の追加**
   ※「本編」の末尾に移動
3. **AI事業者ガイドライン利活用ツール※の言及**
   ※ チェックリスト・ワークシート・チャットボット・活用の手引き
4. **その他個別内容の修正**
   脚注内容の見直し等

ご意見いただきたいポイント

上記「はじめに」の見直しの方針について（他に考慮すべき観点が無いか、等）

1.「はじめに」の更新内容
- 更新ポイントと具体的な更新箇所（概要）

2.「AIによるリスク」の検討ワーキンググループ
- 検討内容の報告

3. 最新技術動向（AIエージェント・フィジカルAI）への対応
- 「対応方針」の記載について
- 「便益・ユースケース」の記載について

4. AIガバナンスに関する動向・事例の反映
- コラムに掲載する事例について

「AIによるリスク」の検討ワーキンググループ

【資料4-2】参照

ご意見いただきたいポイント	「AIによるリスク」ワーキンググループにて検討中のリスクの一覧、リスクの分類について（過不足が無いか、等）

1. 「はじめに」の更新内容
   - 更新ポイントと具体的な更新箇所（概要）

2. 「AIによるリスク」の検討ワーキンググループ
   - 検討内容の報告

3. 最新技術動向（AIエージェント・フィジカルAI）への対応
   - 対応方針の記載について
   - 便益・ユースケースの記載について

4. AIガバナンスに関する動向・事例の反映
   - コラムに掲載する事例について

第1.2版（R8・3月公開）における主な更新箇所

AIエージェントとフィジカルAIについて、定義等を追記

【更新内容】

① AI事業者ガイドラインとしての定義の追加

✓ AIエージェントの定義（案）
本ガイドラインにおけるAIエージェントとは、特定の目標を達成するために、環境を感知し自律的に行動するAIシステムとする。

✓ フィジカルAIの定義（案）
本ガイドラインにおけるフィジカルAIとは、センサ等によるセンシングを通じて物理環境の情報を取り込み、AIモデルによる処理を経て、設定された目的を達成するための最適な方策を自律的に推論・判断し、アクチュエータ（駆動系）等を介して物理的な行動へとつなげるシステムであり、サイバー空間での処理に留まらず、現実世界に対して直接的な働きかけ（移動、操作、加工など）を行うことを特徴とするものとする。

② 便益の追加

✓ AIエージェント…複数のシステムと連携しながらの自律的行動による、調整・分析・意思決定等の業務効率化の便益を追加
✓ フィジカルAI…物理環境での自律的行動による、労働力不足の補完、安全性向上、介護・生活支援等の便益を追加

③ リスクに関する事項の追加

✓ 自律的行動による人間の意図しない動作、攻撃対象・攻撃手法の増加、複雑機構を持つことによる制御の困難化、悪意のあるコード生成等の事項を追加

④ 対応方針の追加

✓ 人間の判断を介在させる仕組みの構築や最小権限設定、ハードウェア残存データへの配慮等、留意すべき事項を追加

⑤ AIシステム・サービス例の追加

✓ 旅行先予約・提案エージェントや自律移動ロボット、AIエージェント作成サービス等のAIシステム・サービス例を追加

【主な更新箇所】

✓ 本編第1部.「AIとは」
✓ 別添1.「A.AIに関する前提」「B.AIによる便益／リスク」
✓ 別添3.4.5.「AI 開発者／AI提供者／AI利用者向け」

■人工知能基本計画 （令和8年7月14日 改訂） ※抜粋

第3章 AI関連技術の研究開発及び活用の推進に関し、政府が総合的かつ計画的に講ずべき施策 ※抜粋

第1節 AI利活用の加速的推進

エージェント型ＡＩを軸に、社会課題解決や産業競争力強化のためにＡＩを積極的に適用する。特にバーティカルＡＩ及びフィジカルＡＩを行政及び産業の現場に能動的に導入する。新しい事業や新たな産業の創出につながるＡＩ利活用を促進し、我が国のＡＩ市場を拡大する。公共性の観点から、医療・介護、福祉、農林水産業、社会インフラなどで社会課題の解決につながるＡＩ利活用を推進する。防衛、サイバーセキュリティ、防災、消防及び警察でのＡＩ利活用を戦略的に進める。ＡＩ利活用や開発の基盤にもつながるＡＩ駆動型の科学研究を推進する。

第3節 AIガバナンスの主導

エージェント型ＡＩの登場により、ＡＩがもたらすリスクは相当に複雑化・深刻化している。不具合の連鎖による大規模障害といった技術的リスク、責任の所在の曖昧化、雇用への影響といった社会的リスク、自律型のサイバー攻撃といった安全保障上のリスクが懸念され、適時適切の対応が一層求められる。特にサイバーセキュリティ上の脅威は、ＡＩによる自律型攻撃により未知の脆弱性の発見がされるなどの形で顕在化している。これらの脅威に対応し「信頼できるＡＩ」を実現するためにも、サイバー防御の強化が不可欠である。

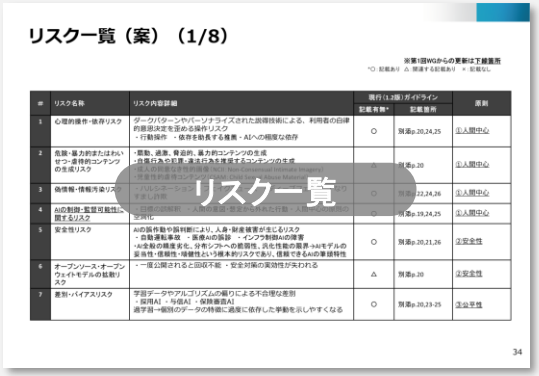
出典：https://www8.cao.go.jp/cstp/ai/ai_plan/aiplan_20260714.pdf

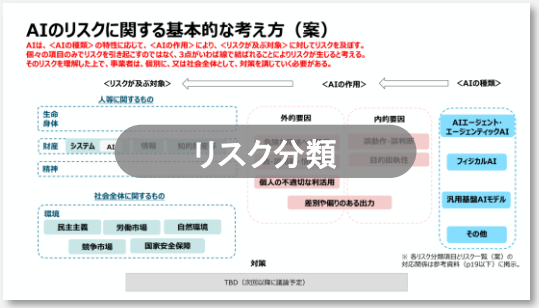
検討の方向性及び進め方

「AIによるリスク」のワーキンググループ、AIガバナンス検討会、及び技術動向調査結果の内容を整理しながら、リスク・対応方針・便益・ユースケースの具体的な検討を推進。

「AIによるリスク」の検討 ワーキンググループ

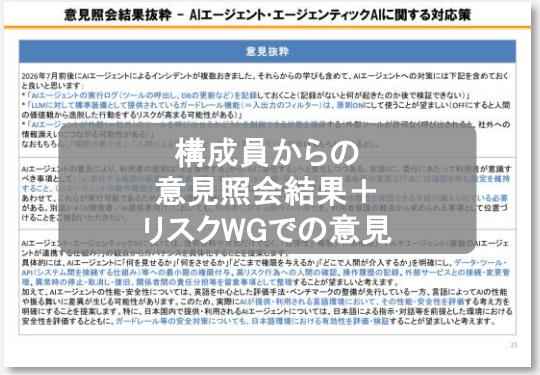
■AIエージェント・フィジカルAI・生成AI・従来型AI

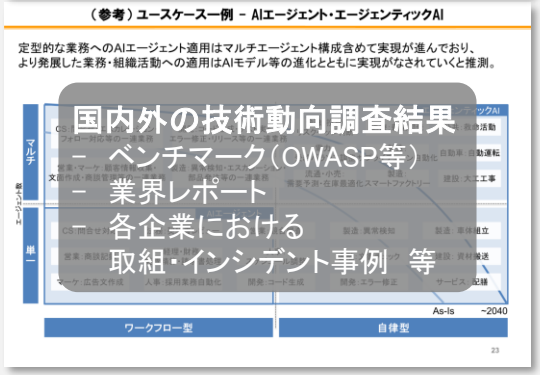




AIガバナンス検討会及び 技術動向調査結果

■AIエージェント・フィジカルAI





■生成AI・従来型AI

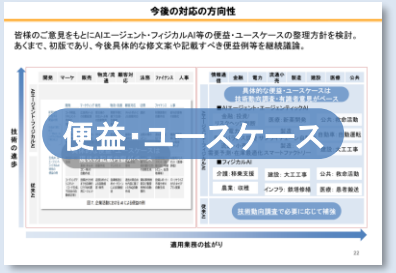
リスクWGでの意見

各種検討内容

■AIエージェント・フィジカルAI・生成AI・従来型AI







「対応方針」の記載について

現状の課題

■課題

第1.2版でHITLや必要最小限な権限設定等を対応方針として記載したが、基本的な記載に留まり、かつ従来型AI・生成AIの記載にアドオンする形のため体系立った整理ができていない



目標	• 現状記載のリスク（自律的行動による人間の意図しない動作、攻撃対象・攻撃手法の増加、複雑機構を持つことによる制御の困難化、悪意のあるコード生成等）及び新たに追加するリスク等を踏まえた対応策を追加し体系立てて整理する • 整理した内容の分かりやすい記載方法を検討する

追記する「対応方針」一覧（案） – AIエージェント・エージェンティックAI

構成員の意見やドキュメント調査を元にAIエージェント・エージェンティックAIで重視すべき対応方針（案）を整理。（あくまで今回の議論のための整理であり、AI事業者ガイドラインにおいて記載すべき項目や具体の文言については今後継続して議論。）

対応方針カテゴリ		主体区分毎の対応方針詳細（案）		
		AI開発者	AI提供者	AI利用者
権限管理と不正利用の防止（NHI：Non-Human Identityの管理）	権限最小化	モデル参照データの制限	ツール・API利用等の権限最小化	権限逸脱等の定期確認
	識別・認証・認可	なりすまし等を考慮したモデル構築	NHIの管理・認証機能の組み込み	アカウントや資格情報の管理・運用
	動作ログの記録・監視	推論プロセス等のログ出力	実行環境全体での監視基盤の構築	動作ログの定期確認
自律行動に対する制御・対応	HITLの設計	HITLを考慮したモデル構築	HITLを意識した機能※の提供 ※チャットでの承認要求やワークフロー機能等	HITLプロセスの設計
	ガードレールの設計	モデルレベルでのガードレール設計	アプリ層でのガードレール設計	禁止事項等のルール整備
	異常な挙動の検知・停止	サーキットブレーカーの組み込み	サービス全体の監視	検知時の停止等の対応手順明確化
情報学習と記憶の健全性確保	データの信頼性評価	メモリ更新データの信頼性評価	メモリ管理ポリシーの策定	誤情報発見時の報告
エージェント連携環境における安全性の確保	外部サービスとの接続・変更管理	サービス変更を考慮したモデル構築	サービス間の接続の維持・管理	APIキーや認証情報等の管理
	エージェント間での統一したログ管理	推論プロセス等のログ出力	実行環境全体での監視基盤の構築	動作ログの定期確認
	インシデント報告体制の構築※	修正や事後学習等の体制整備	CSIRTの構築	エスカレーションフローの整備
AI過信・情報過多を防ぐための設計と教育施策	人間とAIの責任範囲の明確化	モデルの限界等の文書への明記	運用責任の分界点を明文化	責任を考慮した業務・ポリシー設計
	AIリテラシー教育	リスク・技術情報の整備	リスク・技術情報の整備	AI利用のリスク等の社内研修

※ 単一のエージェントの運用時も留意が必要ではあるが、マルチエージェント環境においてはより意識すべき事項として整理（ガイドラインへの記載方法は今後検討が必要）

ご意見いただきたいポイント

- 対応方針における上記整理について（他の整理軸はあるか、AI事業者ガイドラインのスコープとしてとしての妥当性、等）
- 対応方針の具体的な中身について（過不足の有無、既存の記載を踏まえ外すべき項目の有無、粒度は問題無いか、対応が難しいものは無いか、等）
- 既存の記載と章を分けて書くべきか
- マルチAIエージェントの観点を盛り込むべきか

（補足）AIエージェントの対応方針に関わる検討における参考情報例

ドキュメント名	記載内容（概要）
NSA及びFive Eyes「Careful Adoption of Agentic AI Services」	• 米NSAや英NCSCなどFive Eyes加盟国のサイバー防衛当局が共同発表した、エージェント型AI（自律型AI）の導入指針 • 最小特権の原則の徹底、不可逆・高リスク処理における人間の介入・監視（Human-in-the-Loop）、低リスク業務からの段階的導入等の対応に言及
OWASP「Agentic AI - Threats and Mitigations」	• 国際標準団体OWASPによる、エージェント型AI特有のセキュリティ脅威カタログと緩和策 • エージェントが持つ「目標の自律分解」「外部API・コード実行権限」「メモリ・セッションの永続化」を突く攻撃パターンやサンドボックス実行の義務化、ツール実行時の厳格な権限スコープ分離、エージェント間通信の検証といった防御策等に言及
NIST「AI Risk Management Framework」	• NISTが策定した、AIのライフサイクル全体を網羅するリスクマネジメントの国際的デファクト基準 • 「信頼できるAI」の実現を目的とした、リスク管理プロセスを統治、把握、測定、管理等の実践的なフレームワークを提供
NIST「IR 8596 Cybersecurity Framework Profile for AI」	• NIST CSF 2.0をAI環境向けに最適化した実践プロファイル • CSFの統治・防御・検知・対応プロセスの中に、モデル・プロンプト・訓練データの資産管理や、データポイズニング・モデル不正利用への対抗策を具体的にマッピング
MITRE「MITRE ATLAS（Adversarial Threat Landscape for AI Systems）（v5.4.0）」	• AI/機械学習システムを標的とする攻撃者の戦術・技術・手順（TTPs）を体系化したナレッジベース（AI版MITRE ATT&CK） • 実世界の攻撃事例や研究に基づき、モデル窃取、データポイズニング、敵対的サンプル入力、プロンプトインジェクション、間接的インジェクション等の攻撃手法を攻撃ライフサイクルに沿って分類
AISI「AIセーフティに関する評価観点ガイド」	• 日本のAIセーフティ・インスティテュートが公表した、AI開発者・提供者向けの実践的セーフティ評価指針 • エージェント型AIに対応し、「自律的な挙動」や「外部環境との相互作用」に対する観測・制御、人間の緊急停止・介入機能の妥当性評価等を言及
OECD「Agentic AI in organizations」	• 経済協力開発機構（OECD）による、企業・公共組織におけるエージェント型AIの導入インパクトとガバナンス課題の分析文書 • 単なる対話型支援から「複数業務の自律遂行」へと移行するエージェント型AIがもたらす生産性向上の便益やユースケース等に言及
Model AI Governance Framework for Agentic AI	• シンガポールIMDAによる、Agentic AI導入事業者向けにリスクとベストプラクティスを継続的に発信している文書 • 自律性・マルチエージェント化等に伴う、予測困難で連鎖的なインシデントのリスクに言及し、対応として、事前のリスク評価・人間の責任確保・技術的管理策・エンドユーザーの責任確保を継続的に回すガバナンス・フレームワークを提示

※ 上記参考情報に加えて、国内外の民間企業におけるAIエージェントに起因するインシデント事例やその対応方針例等の情報も参考としている。

追記する「対応方針」一覧（案）－ フィジカルAI

構成員の意見やドキュメント調査を元にフィジカルAIで重視すべき対応方針（案）を整理。（あくまで今回の議論のための整理であり、AI事業者ガイドラインにおいて記載すべき項目や具体の文言については今後継続して議論。）

対応方針カテゴリ		主体区分毎の対応方針詳細（案）		
		AI開発者	AI提供者	AI利用者
知覚・センサ層の対策（入力の保護）	物理的な保護	-	物理的なアクセスの検知機能や盗難追跡機能の組み込み	機器設置場所のアクセス制限・保護
	センサーデータの保護	特定の異常値による誤認識が軽減されるモデルの構築	センサーデータの改ざん防止・検知	定期的な清掃・点検・キャリブレーション（校正）作業
モデル・推論の対策（判断の保護）		AIエージェント・エージェンティックAIと同等の対策		
作業・制御・通信層の対策（出力の保護）	ガードレールの設計	安全領域を超えない物理的制約が組み込まれたモデルの構築	ソフトウェアから独立したハードウェア安全装置の設置	安全エリア設定、減速ゾーン、進入禁止領域などの設定
	通信・ネットワークの保護	-	各種通信の暗号化	社内ネットワークセキュリティの維持
安全設計とフェイルセーフ	異常な挙動の検知・停止	物理的な異常挙動を検知・判定するアルゴリズムの組み込み	フェイルセーフ機構・非常停止ボタン等の設計	運用・人手介入での制御
	デジタルツインによる事前学習・検証	シミュレーション上でのAIの安全性・堅牢性の反復検証・学習（Sim-to-Real）	仮想空間やクローズド環境での検証	機器設置場所のアクセス制限・保護

ご意見いただきたいポイント

- 対応方針における上記整理について（他の整理軸はあるか、AI事業者ガイドラインのスコープとしてとしての妥当性、等）
- 対応方針の具体的な中身について（過不足の有無、既存の記載を踏まえ外すべき項目の有無、粒度は問題無いか、対応が難しいものは無いか、等）
- 既存の記載と章を分けて書くべきか

（補足）フィジカルAIの対応方針に関わる検討における参考情報例

ドキュメント名	記載内容（概要）
NIST「Cyber-Physical Systems (CPS) Framework」	• NISTが策定した、物理制御とサイバー空間が融合した**CPS（サイバーフィジカルシステム）**の統合設計・セキュリティフレームワーク • 物理世界のセンサ・アクチュエータ（OT）とAI・情報通信（IT）が連動する環境において、「機能性」「安全性（Safety）」「セキュリティ（Security）」「プライバシー」「信頼性」の5面から多面的にリスク評価を実施することを推奨
OWASP「Robotics Security Testing Guide (RSTG)」	• OWASPが主導する、ヒューマノイド・自律走行ロボット・産業用ロボット向けのペネトレーションテスト（侵入・安全性テスト）標準ガイド • デジタル上の脆弱性が「物理的な破壊や人身危害」へ直結するリスクを対象
OWASP「Multi-Agentic System Threat Modelling Guide (MAESTRO)」	• 自律型エージェントAIが複数連携する環境（分散ロボティクス、スマートファクトリー等）を対象とした脅威モデリングガイド • AIが物理的なツールやアクチュエータ（搬送機、バルブ操作、API）を実行権限として持つ際の脅威をモデル化。エージェント間の通信汚染、目標の歪曲、誤認による物理機器の不正操作リスクの洗い出し手法に言及
MITRE「MITRE ATLAS」	• AI脅威カタログATLASにおける、フィジカル空間を介した機械学習モデルへの攻撃手口群 • 物理的敵対パッチ（Physical Adversarial Patches）やセンサスプーフィング等に言及
ENISA「AI in Autonomous Driving」	• 自動運転車や自律走行モビリティにおけるAIアルゴリズムのサイバーセキュリティ専門ガイド。 • 車載知覚AIのデータポイズニングや、物理環境からの入力ノイズによる意思決定の誤作動を分析。車両内の「AI推論系」と「操舵・ブレーキ等の物理アクチュエーション系」を隔離する多層防御アーキテクチャを提唱
WEF「After ChatGPT, "Physical AI" Is Next. Can We Afford Failures in the Real World?」	• 生成AIが、製造工場、物流拠点、建設現場、人型ロボットなどの「物理経済」へ進出する転換期において、経営層・政策決定者へ警鐘を鳴らしたオピニオン／提言レポート • 「リリースして後から直す（アジャイル）」の文化が、物理世界では人命に関わるため通用しないため、フィジカルAIの本格展開には、ハードウェアによる強制停止と厳格な安全ガバナンスが不可欠であることを提唱
日本ロボット工業会（JARA）「JIS B 8445 / 8446（生活支援ロボットの安全性）」	• 国際安全規格ISO 13482に基づく国内基準 • 人間と物理的に触れ合う介護・移動支援・搭乗型ロボットにおいて、AI制御ソフトウェアの欠陥が物理的挟み込みや衝突・転倒に繋がらないための機構的・電気的制約を定義

※ 上記参考情報に加えて、国内外の民間企業におけるフィジカルAIに起因するインシデント事例やその対応方針例等の情報も参考としている。

便益・ユースケース

便益・ユースケースに関する現状の記載内容

現状のAI事業者ガイドラインでは、便益を「企業活動×従来AIの便益 or 生成AI・AIエージェント・フィジカルAIの便益」というマトリクスで整理をしている

便益の例

以下の「図 7. 企業活動における AI による便益の例」は、企業活動における AI による便益のごく一例を示したものだが、企業活動の全般にわたり、効果を発揮しうる。

	開発	マーケティング	販売	物流・流通	顧客対応	法務	ファイナンス	人事
従来から存在する便益の例	コード検証、ドキュメント作成の自動化	広告用メールの自動配信	受注後の対応メール等の自動発信	需要予測に基づく生産・在庫数最適化	チャットボットによる自動対応	翻訳	財務諸表の自動作成	給与計算等の自動化
生成AIで更に向上（一部AIエージェントやフィジカルAIで更に向上）	類似コード・データの抽出・検証	データに基づいたパーソナライゼーション広告	チャネル別、ニーズ別の売上予測	配送ルート最適化	顧客の成約・解約率予測	法務文章のレビュー	過去実績にもとづいた将来予測、不正検知	職務経歴書等に基づいた人材需要マッチング
生成AI、AIエージェント、フィジカルAI特有の便益の例	学習データの生成	販売促進（マーケティング素材・キャッチコピー等）の自動作成	営業トークスクリプトの自動作成	物流条件交渉のアシスタント	対応内容の自動生成、要約	規定に基づいた契約書ドラフトの自動生成	経費精算アシスタント（自動仕訳、申請レビュー、証憑取得等）	AI採用アシスタント（面接・評価）
	コーディングアシスタント（コード生成、不具合の自動修正等）	投稿から分析までを自律的に行うSNS運用エージェント	店頭ロボットによる自動接客・販売	自律搬送ロボット・ドローンによる自動配送	過去の問合わせ内容に基づいたFAQ自動作成	類似事例検索及び重要判例の自動要約	投資レポート・市場分析の自動生成	パーソナライズされたキャリアプラン提案

図 7. 企業活動における AI による便益の例

例えば、物流の領域では、AI を用いたロボットによる配送の自動化及び需要予測によるバリューチェーンの最適化、人事の領域では、給与計算の自動化及び職務経歴書にもとづいた人材需要マッチング等、データを活用した効率化に AI が活用され、多様な用途で業務の効率化・最適化が行われている。

また、企業以外においても、行政における手続きの自動化、センサ及び画像情報等を用いた農場での作業支援システム、診療履歴等の利用による医療分野への活用等も行われている。

さらに、B2C の領域では、チャットボット、自動運転、検索システム、音声アシスタント等、多岐にわたるサービスが展開されている。

加えて、AI の活用による便益は社会にも波及し得る[7]。

加えて、AI エージェントの登場により、ユーザーの意図を理解し、自律的にタスクを遂行することで、複雑な業務プロセスを効率化し、人的負荷を大幅に削減できる。単なる指示実行にとどまらず、複数のシステムやアプリケーションと連携し、状況に応じた判断や最適化を行うことで、従来は人手に依存していた調整・分析・意思決定を自動化することが可能となる。最後に、フィジカル AI は、少子高齢化による労働力不足を補い、人と協働して生産性を向上させることで、あらゆる産業や現場の自動化と効率化に寄与することが期待される。危険な環境で人の代わりに作業を行い、安全性を高めつつリスクを低減するほか、介護や生活支援を通じて人々の自立と QOL 向上に寄与し、福祉や医療などの分野で新たな支援の創出にもつながり得る。

グローバルの激しい競争を勝ち抜くためにも、生成 AI を積極的に取り入れる形でデジタル戦略の見直しを行う等、自身が享受できる便益を正しく理解し、可能性を模索するとともに、積極的な姿勢を持つことが期待される。

解消したい課題

- **エージェンティックAI、フィジカルAIの便益（及びユースケース）は、「共通的な企業活動への適用」から「業界固有の業務への適用」も増えてくるため、現状の分類ではマッピングしづらいユースケースも存在**
- **研究段階のものから実装段階のものまで混在**

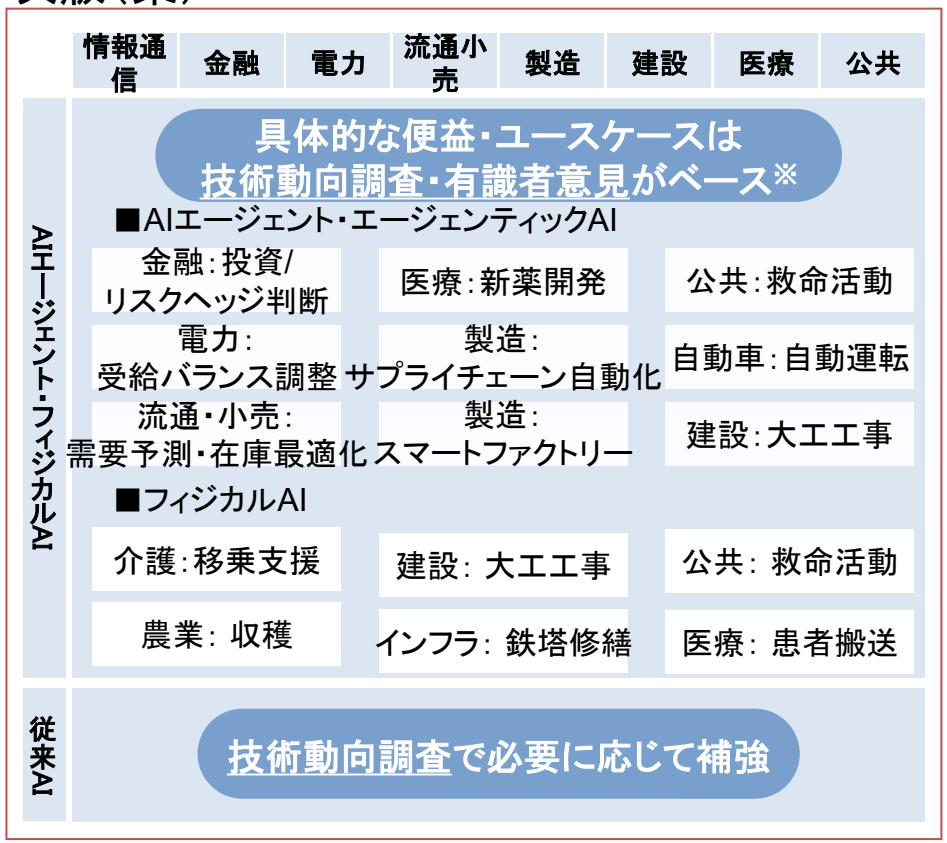
今後の対応の方向性

構成員の意見等を元にAIエージェント・フィジカルAI等の便益・ユースケースの整理方針を検討。
今後具体的な修文案や記載すべき便益例等を継続議論。

第1.2版



次版（案）



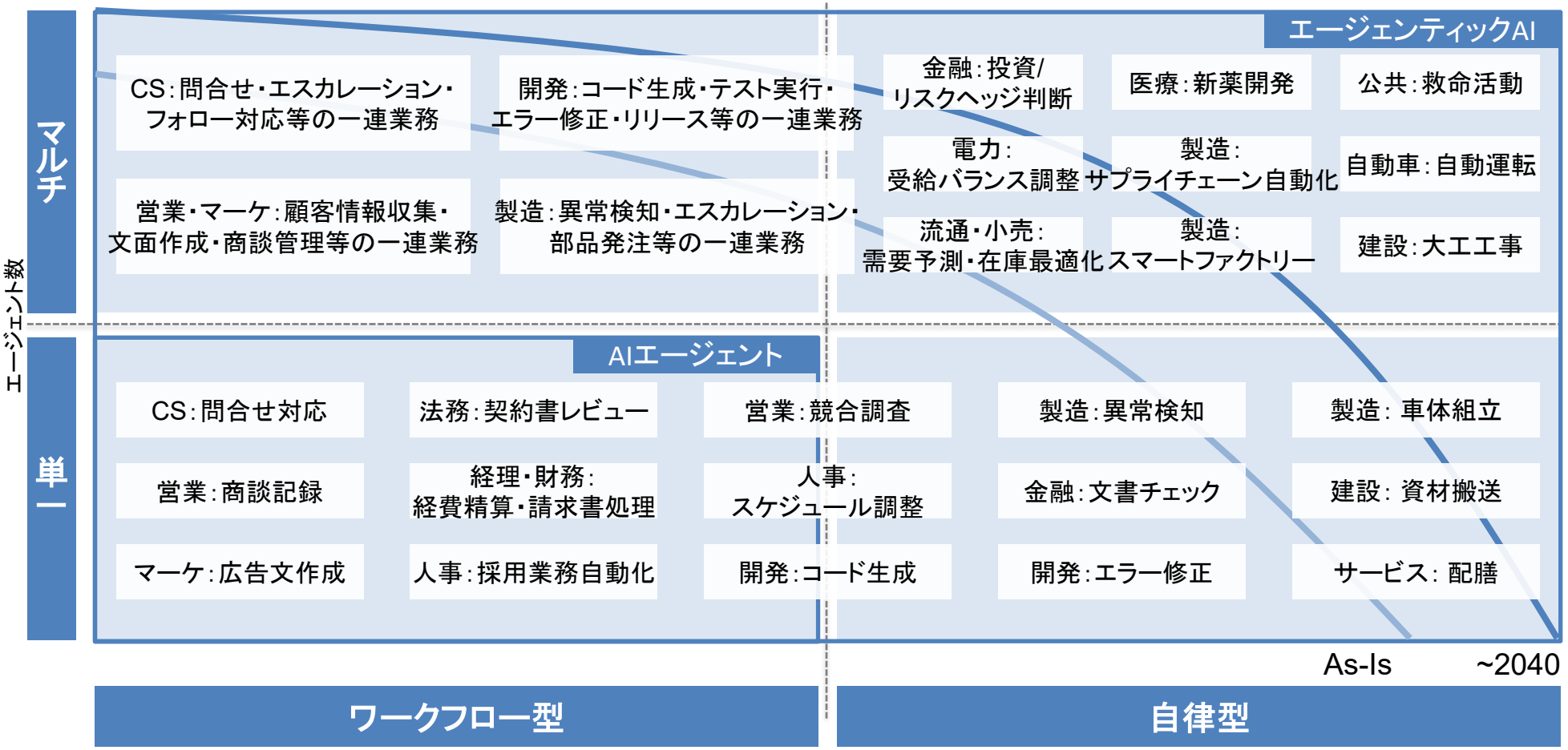
※ 既に実装・浸透している例をマトリクスとして整理、
今後推進される例は必要に応じて参考情報として文章で補記する想定

ご意見いただきたいポイント

・便益・ユースケースの上記整理について
・（整理方法を踏まえて、）どのような便益・ユースケースを追加すべきか（重点を置くべき業界・ユースケースはあるか、等）

（参考）ユースケース一例 – AIエージェント・エージェンティックAI

定型的な業務へのAIエージェント適用はマルチエージェント構成含めて実現が進んでおり、
より発展した業務・組織活動への適用はAIモデル等の進化とともに実現がなされていくと推測。



（精査は必要であるが、既に実現・浸透している例をマトリクスとして整理、今後推進される例は重要なものだけを必要に応じて文章で補記する想定）

※ 国内外の各事業者におけるAIエージェント・エージェンティックAIの実際の活用事例や実証実験例に加えて、
OECD「Agentic AI in organizations」やWEF「Transforming Consumer Industries in the Age of AI」等の各種ドキュメント（ドキュメントからは主に将来的なユースケースを参考）をベースに整理

（補足）AIエージェントの便益・ユースケースに関わる検討における参考情報例

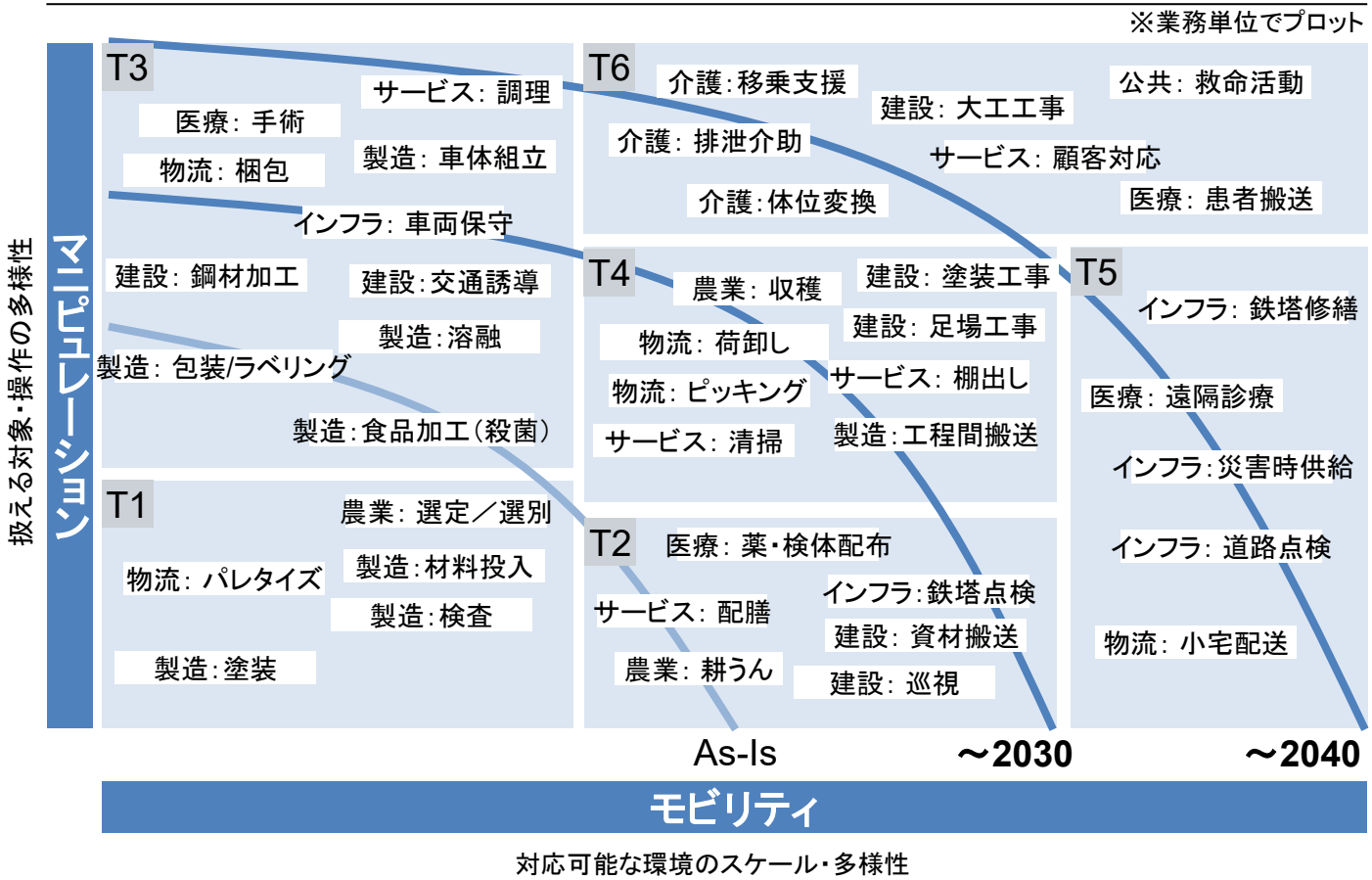
ドキュメント名	記載内容（概要）
OECD「Agentic AI in organizations」	• 経済協力開発機構（OECD）による、企業・公共組織におけるエージェント型AIの導入インパクトとガバナンス課題の分析文書 • 単なる対話型支援から「複数業務の自律遂行」へと移行するエージェント型AIがもたらす生産性向上の便益やユースケース等に言及
WEF「Transforming Consumer Industries in the Age of AI」	• 世界経済フォーラム（WEF）による、消費財・小売・流通産業におけるAI変革とビジネス戦略レポート • 需要予測、サプライチェーン自動化、パーソナライズされた購買体験など、バリューチェーン全域にわたるAIの活用価値を解説

※ 上記参考情報に加えて、国内外の民間企業におけるAIエージェントの活用事例の情報も参考としている。

（参考）ユースケース一例 – フィジカルAI

フィジカルAIの適用領域は、マニピュレーションとモビリティの汎用性向上に応じ、
単純で限定的な作業から、多様な環境での高度な作業や人協働への範囲が拡大していく

Physical AIのユースケース (抜粋)



ロボットの分類

T1	定型作業（据置）	手順や手配が標準化され、繰り返し性が高い据置型の作業
T2	搬送・巡回	物品や資材の搬送、エリア内の見回り・巡回などの移動中心の作業
T3	高度作業（据置）	設備内で行う高精度・高信頼の加工、組立など。高度なマニピュレーションを要する
T4	移動作業	現場を移動しながら実行する作業。屋内外で環境の変動が大きい
T5	広域作業	広域にまたがる範囲で、連続的に状況を把握しながら遂行する作業
T6	人協働	人と同一空間で協調して行う作業。指示の理解・柔軟な役割分担・安全確保を重視

（精査は必要であるが、既に実現・浸透している例をマトリクスとして整理、今後推進される例は重要なものだけを必要に応じて文章で補記する想定）

※ 国内外の各事業者におけるフィジカルAIの実際の活用事例や実証実験例に加えて、内閣府「ムーンショット目標」や
WEF「『After ChatGPT, "Physical AI" Is Next. Can We Afford Failures in the Real World?』」等の各種ドキュメント（ドキュメントからは主に将来的なユースケースを参考）をベースに整理

（補足）フィジカルAIの便益・ユースケースに関わる検討における参考情報例

ドキュメント名	記載内容（概要）
内閣府「ムーンショット目標」	• 「フィジカルAI」そのものを中核に据えた国家プロジェクト • デジタル空間のAIにとどまらず、センサとアクチュエータ（身体）を持つロボットが実世界で試行錯誤しながら学習する技術を開発。2030年ターゲットとして「現場でタスクを完遂する汎用自律人型AIロボット」の確立、2050年には人の介護・家事支援から宇宙・深海・災害現場での完全自律活動までを言及
WEF「After ChatGPT, "Physical AI" Is Next. Can We Afford Failures in the Real World?」	• 生成AIが、製造工場、物流拠点、建設現場、人型ロボットなどの「物理経済」へ進出する転換期において、経営層・政策決定者へ警鐘を鳴らしたオピニオン／提言レポート • 「リリースして後から直す（アジャイル）」の文化が、物理世界では人命に関わるため通用しないため、フィジカルAIの本格展開には、ハードウェアによる強制停止と厳格な安全ガバナンスが不可欠であることを提唱

※ 上記参考情報に加えて、国内外の民間企業におけるフィジカルAIの活用事例の情報も参考としている。

1. 「はじめに」の更新内容
   - 更新ポイントと具体的な更新箇所（概要）

2. 「AIによるリスク」の検討ワーキンググループ
   - 検討内容の報告

3. 最新技術動向（AIエージェント・フィジカルAI）への対応
   - 「対応方針」の記載について
   - 「便益・ユースケース」の記載について

4. AIガバナンスに関する動向・事例の反映
   - コラムに掲載する事例について

AIガバナンスに関する動向・事例の反映

- AI事業者ガイドラインの別添（p73～p94）では、事業者による実際のAIガバナンスに関する取組事例をコラムとして紹介（全11事例）。
- AI事業者ガイドライン次版以降、以下に取り組む事としたい。

大分類	小分類	詳細
①事例コラムの追加 （AIエージェント・フィジカルAI等、多様なAIが様々な事業者に導入されつつある現況を踏まえた更新）	業種の拡大	現在の事例コラムはICT企業の事例が多いため、他業種の事例の拡充を図る。 ※拡充対象の業種は日本成長戦略・バーティカルAIの重点領域（市場性・公共性）から着手する事も一案。 https://www.cas.go.jp/jp/seisaku/nipponseichosenryaku/pdf/rm2026.pdf ⇒P16 -市場性：製造、物流・交通、情報通信、金融、創薬 -公共性：医療・介護・福祉、農林水産、建設、教育、行政、エネルギー
	AI利用者の事例の拡充	現在の事例コラムではAI開発者・AI提供者の事例が多いため、AI利用者のAIガバナンスに関する実践・取り組み事例の記載の充実化を図る。
	企業規模の多様化	大手企業からスタートアップ・中小企業まで幅広く取り組み事例を記載する。
	最新のAI動向の反映	最新技術動向を踏まえ、AIエージェント（エージェンティックAI）・フィジカルAI等に関する事業者のAIガバナンスに関する実践・取組事例を追加する。
②事例コラムの整理 （事業者の読みやすさ、利用しやすさを意識した更新）	事例コラムの別冊化	今後の事例拡充を見据え、コラムをAI事業者ガイドライン（別添）から切り離し、別冊化する。
	事例コラムの分類	取り組み事例の分類（軸は要検討）を行い、検索性を向上させる。（既存の事例についても分類を図る）。

ご意見いただきたいポイント　**事例コラムの追加・整理の方針について（他に考慮すべきポイント、積極的に収集すべき事例等はあるか）**

第32回AIガバナンス検討会 ご意見をいただきたいポイント

1.「はじめに」の更新内容

ご意見いただきたいポイント	「はじめに」の見直しの方針について（他に考慮すべき観点が無いか、等）

2.「AIによるリスク」の検討ワーキンググループ

ご意見いただきたいポイント	「AIによるリスク」ワーキンググループにて検討中のリスクの一覧、リスクの分類について（過不足が無いか、等）

3. 最新技術動向（AIエージェント・フィジカルAI）への対応

ご意見いただきたいポイント	・対応方針における整理について（他の整理軸はあるか、AI事業者ガイドラインのスコープとしてとしての妥当性、等） ・対応方針の具体的な中身について（過不足の有無、既存の記載を踏まえ外すべき項目の有無、粒度は問題無いか、対応が難しいものは無いか） ・既存の記載と章を分けて書くべきか ・マルチAIエージェントの観点を盛り込むべきか

4. AIガバナンスに関する動向・事例の反映

ご意見いただきたいポイント	事例コラムの追加・整理の方針について（他に考慮すべきポイント、積極的に収集すべき事例等はあるか）