

AI事業者ガイドライン案 概要

令和5年12月21日

総務省
経済産業省

AI事業者ガイドライン案（全体の構成、今後の進め方）

- 事業活動においてAIに関係する全ての者（企業に限らず、公的機関を含めた組織全般）を対象。事業者を①AI開発者、②AI提供者、③AI利用者（注）に大別（注）事業活動以外でAIに関係する者を含めない
- 3つの事業者カテゴリに共通の指針を括りだした上で（第2部C）、各カテゴリに特有、重要となる事項を整理（第3部～第5部）
- 簡潔な本編を補完するため、別添において詳細に解説

本編の構成

総論

第1部 AIとは

第2部 AIにより目指すべき社会と各主体が取り組む事項

A 基本理念

B 原則

C 共通の指針（一般的なAIシステム）

D 高度なAIシステムに関係する事業者に通じる指針

E ガバナンスの構築

各論

第3部 AI開発者に関する事項

データ前処理・学習時、AI開発時、AI開発後、国際行動規範の遵守

第4部 AI提供者に関する事項

AIシステム実装時、AIシステム・サービス提供後、国際指針の遵守

第5部 AI利用者に関する事項

AIシステム・サービス利用時、国際指針の遵守

別添

本編を補完する位置付けとして、次のような事項を記載

✓ AIシステム・サービスの例（各主体の関係性等を含む）

✓ AIによる便益や可能性、具体的なリスクの事例

✓ ガバナンス構築のための実践ポイント、具体的な実践例

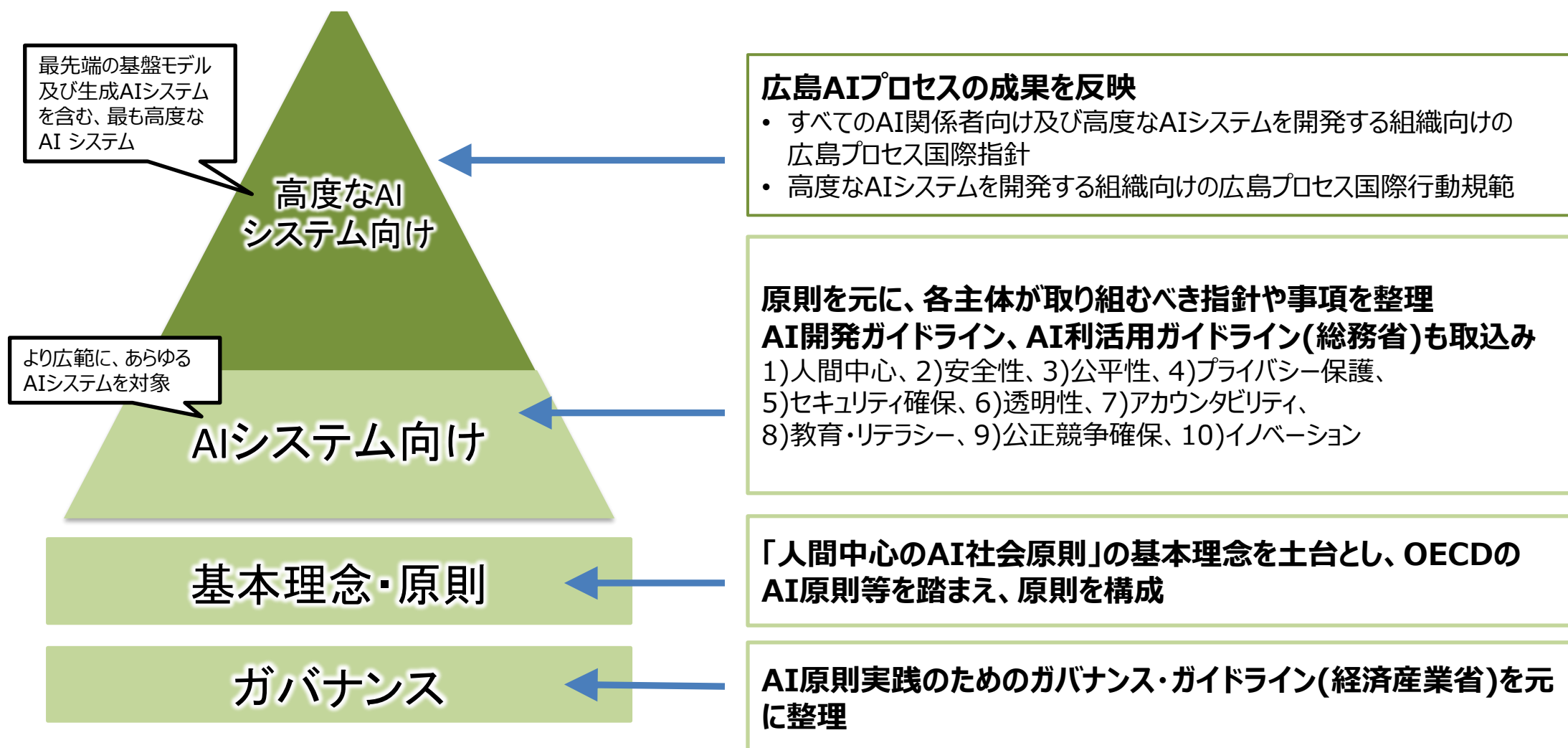
✓ 本編の各項目に関するポイント、具体的な手法の例示、
分かりやすい参考文献 等

※ 本編を元にしたチェックリストも含む（参考を参照）

⇒ 来年1月以降パブリックコメントを実施し、3月を目途に策定・公表予定。最新の動向等も踏まえつつ、4月以降も随時更新予定

AI事業者ガイドライン案（対象範囲）

- 広島AIプロセスでとりまとめられた高度なAIシステムに関する国際指針及び国際行動規範を反映しつつ、**一般的なAIを含む（想定され得る全ての）AIシステム・サービスを広範に対象**
- 実際のAI開発・提供・利用においては、本ガイドラインを参照し、**各事業者が指針遵守のために適切なAIガバナンスを構築するなど、具体的な取組を自主的に推進することが重要**



各主体が取り組む主な事項の例（抜粋）

第2部

AIにより目指すべき社会と各主体が取り組む事項

- 法の支配、人権、民主主義、多様性、公平公正な社会を尊重するようAIシステム・サービスを開発・提供・利用し、関連法令、AIに係る個別分野の既存法令等を遵守、人間の意思決定や感情等を不当に操作することを目的とした開発・提供・利用は行わない
- 偽情報等への対策、AIモデルの各構成技術に含まれるバイアスへの配慮
- 関連するステークホルダーへの情報提供（AIを利用しているという事実、データ収集・アノテーション手法、適切/不適切な利用方法等）
- トレーサビリティの向上（データの出所や、開発・提供・利用中に行われた意思決定等）
- 文書化（情報を文書化して保管し、必要な時に、入手可能かつ利用に適した形で参照可能な状態とする等）
- AIリテラシーの確保、オープンイノベーション等の推進、相互接続性・相互運用性への留意等
- 高度なAIシステムに関係する事業者は、広島AIプロセスで示された国際指針を遵守（開発者は国際行動規範も遵守）
- 「環境・リスク分析」「ゴール設定」「システムデザイン」「運用」「評価」といったサイクルを、マルチステークホルダーで継続的かつ高速に回転させていく、「アジャイル・ガバナンス」の実践 等

第3部

AI開発者に関する事項

- 適切なデータの学習（適正に収集、法令に従って適切に扱う）
- 適正利用に資する開発（AIモデルの調整（ファインチューニング）の目的に照らしてふさわしいものか検討）
- セキュリティ対策の仕組みの導入、開発後も最新動向に留意しリスクに対応
- 関連するステークホルダーへの情報提供（技術的特性、学習データの収集ポリシー、意図する利用範囲等）
- 開発関連情報の文書化
- イノベーションの機会創造への貢献 等

第4部

AI提供者に関する事項

- 適正利用に資する提供（AI開発者が設定した範囲でAIを活用等）
- 文書化（システムのアーキテクチャやデータ処理プロセス等）
- 脆弱性対応（サービス提供後も最新のリスク等を把握、脆弱性解消の検討）
- 関連するステークホルダーへの情報提供（AIを利用していること、適切な使用方法、動作状況やインシデント事例、予見可能なリスクや緩和策等）
- サービス規約等の文書化 等

第5部

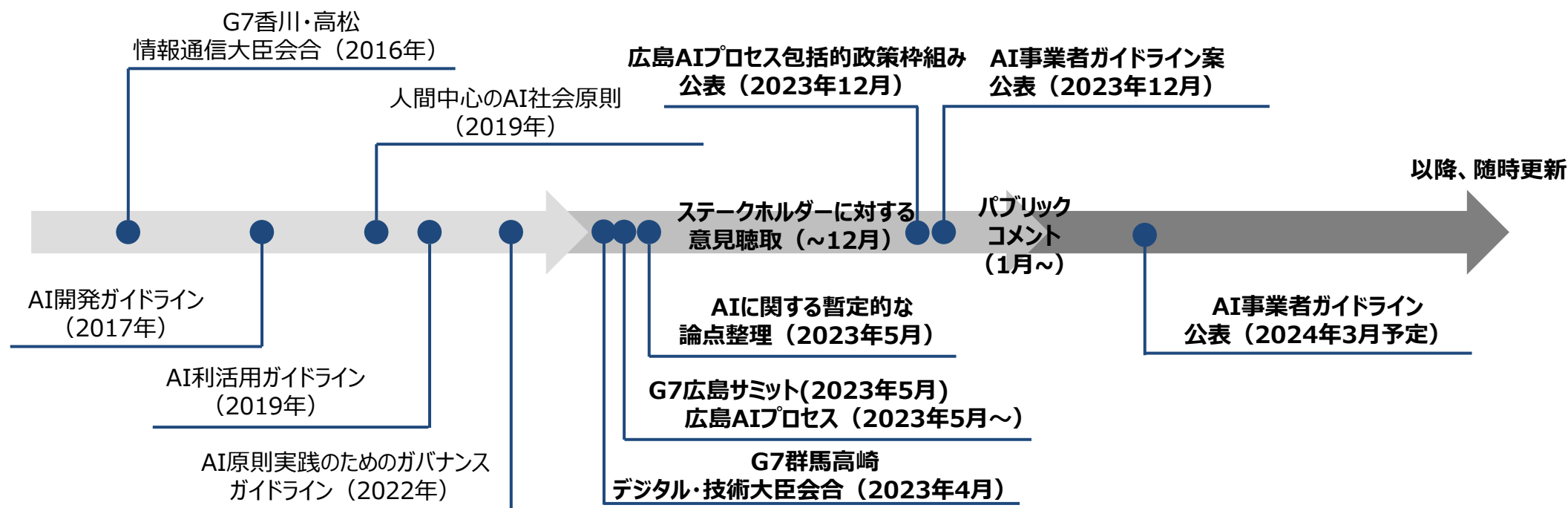
AI利用者に関する事項

- 安全を考慮した適正利用（提供者が示した適切な利用範囲での利用）
- バイアスに留意し、責任をもって出力結果の利用を判断
- プライバシー侵害への留意（個人情報等を不適切に入力しない等）
- セキュリティ対策の実施
- 関連するステークホルダーへの情報提供（利害関係者に平易かつアクセスしやすい形で示す等）
- 提供された文書の活用、規約の遵守 等

AI事業者ガイドライン案（背景・経緯）

- 我が国は従前より、世界に先駆けて、AIに関する議論を主導（G7香川・高松情報通信大臣会合(2016年)、人間中心のAI社会原則(2019年、内閣府)）。今般、「**AIに関する暫定的な論点整理**」（2023年5月、AI戦略会議）を踏まえ、**総務省・経済産業省が共同事務局として、既存のガイドラインを統合・アップデート**（注）し、**広範なAI事業者向けのガイドライン案**をとりまとめ
- 作成にあたっては**広島AIプロセスの議論やマルチステークホルダー・アプローチを重視**。総務省の「AIネットワーク社会推進会議」、経済産業省の「AI事業者ガイドライン検討会」及び各検討会下のWGを活用し、**産業界、アカデミア及び市民社会の多様な意見を聴取**

（注） AI開発ガイドライン（2017年、総務省）、AI利活用ガイドライン（2019年、総務省）、AI原則実践のためのガバナンスガイドライン（2022年、経済産業省）



参考：チェックリスト

- ①全主体（ガバナンス）、②開発者、③提供者、④利用者に大別
- ガイドライン「本編」の各項目に対応した「確認事項」を全般的に提示し、各事業者がカスタマイズして活用できる形式を検討（Excel形式での公表を想定、各事業者が「別添（付属資料）」の事例等を参照しつつ具体的な取組内容について検討可能な様式）
- 事業者にとって使いやすいものになるよう、引き続き検討

本編に対応した確認事項				各事業者が関連する事項、他の主体との関係を検討して記載		各事業者が別添を参照し、具体的な取組事項を検討して追記	
	分類	確認事項 (ガイドライン「本編」を基に記載)	対応箇所	各自の事業に関連する事項 (該当しない場合はその理由)	他の主体との関係についての事項	✓ 具体的な取組内容 (別添(付属資料)該当箇所を基に検討)	最終検討日 (見直し日)
1. 環境・リスク分析	1-1 便益/リスクの理解	a. 事業における価値の創出や社会課題の解決等のAIの開発・提供・利用の目的を明確に定義したか？ b. 自社の事業に結びつくかたちで、「便益」や、意図せざるものを含めた「リスク」の性質を具体的に理解したか？ c. その際に、回避すべき「リスク」や、複数主体にまたがる論点に留意し、バリューチェーン/リスクチェーン全体での便益を確保、リスクを削減したか？ d. 迅速に「経営層に報告/共有する」仕組みを構築したか？	別添2.			□	
	1-2 AIの社会的な受容の理解	a. 潜在的なステークホルダーも含めたステークホルダーを特定したか？ b. 特定した上で、「社会的な受容」の理解に努め、AIを開発・提供・利用したか？ c. 提供開始後も、急速に変化する外部環境を考慮し、必要に応じて適時にステークホルダーの意見を再確認したか？	別添2.			□	
	1-3 自社の習熟度の理解	a. 各主体の事業領域や規模等に照らして「AI習熟度」の評価の必要性を検討したか？ b. 必要であると判断した場合、AIのリスクへの対応力を見える化し、AI習熟度（AIシステム・サービスの開発・提供・利用時に求められる準備がどれだけできているのか）を評価したか？ c. 必要ではないと判断した場合、その理由を整理したか？	別添2.			□	