

# AI事業者ガイドライン活用の手引き (案)

---

資料公開時に記入予定

令和8年（2026年）●月

総務省 経済産業省

# はじめに：本書「活用の手引き」について

AIの安全安心な活用の促進を目的とし、AIガバナンスの統一的な指針を示す「AI事業者ガイドライン」は、AIを取り巻く状況の変化に応じて、継続的に更新されています。

本書「活用の手引き」は、

**AI事業者ガイドラインの活用を補助する目的**で作成されており、AI事業者ガイドラインを用いてAIガバナンスの構築・実践に取り組む方々のうち、**特に、AIガバナンスの構築・実践をこれから始める皆様に向けたもの**となっています。

内容としては、

- AI事業者ガイドラインを活用する上で**前提となる考え方**
- AIガバナンスの構築時の準備・土台として**はじめに着手すると良いこと**
- AIガバナンスの実践時の**AI事業者ガイドラインの参照の仕方、活用例**をそれぞれ紹介する構成となっています。

本書は案の段階ですので、今後内容の見直しが実施される可能性があります。

# はじめに：AI事業者ガイドラインはいつ、何に役立つのか

AI事業者ガイドラインを活用している事業者の方々に、実際にAI事業者ガイドラインを活用している場面やメリットについて伺ったところ、以下のような声をいただいています。

## AI事業者ガイドラインを活用している場面

- 社内・部門のAIポリシー・規則を策定・更新する際に参照
- 社内のAIに関するガイドラインにおいて参照・引用
- AIに関するリスクの全体像や重要なリスクについて確認する際に参照
- AI製品・サービスについての配慮事項の整理やチェックリストの作成の際に参照
- AI製品・サービスに係る契約実務の整理の際に参照
- 組織内のAIについての勉強会の資料を作成する際に参照



## AI事業者ガイドラインを活用して感じたメリット

- AIガバナンスの土台となる概念を理解できた
- AIガバナンスの施策動向を知ることができた
- AIガバナンスにおいて考慮すべき点の不足に気付くことができた
- 社内・部門における取組のイメージを具体化できた
- 社員のAIガバナンス知識向上の役に立った
- 部門間・会社間のやり取りの共通言語となった
- AI事業者ガイドラインを参考としていることが対外的なアピールとなった



・上記は、事業者との個別のヒアリングの結果や総務省のAI事業者ガイドラインに関する事業者アンケートの結果\*に基づいて作成  
(\*[https://www.soumu.go.jp/main\\_content/001055180.pdf](https://www.soumu.go.jp/main_content/001055180.pdf))

# 目次

はじめに	p. 2
<b>1章</b> AI事業者ガイドラインに関する前提	p. 5
<b>2章</b> 本書の位置づけ	p.13
<b>3章</b> AIガバナンスの構築・実践	p.18
<b>1.</b> AIガバナンス構築時の準備事項	p.20
<b>2.</b> AIガバナンス実践時の参照事項	p.30

# 1章 AI事業者ガイドラインに関する前提

本書の内容の理解を助けるために、AI事業者ガイドラインに関わる基本的な考え方や用語を説明します。

---

- × AI事業者ガイドラインの記載事項の遵守は義務である
- ➔ AI事業者ガイドラインは義務を課すものではなく、事業活動においてAIを開発・提供・利用する全ての者を対象に、AIのリスクを正しく認識し、自主的に対策を講じるための考え方を示しているものです。
  
- × AI事業者ガイドラインに書いてあることは、全てそのまま自社に適用すればよい
- ➔ 自社の事業規模および状況等に合わせて過不足なく対応いただくことが重要です。
  
- × データ提供をする者や、個人でAIを利用する場合も対象になっている
- ➔ 「事業活動においてAIの開発・提供・利用を担う全ての者」を対象としており、「データ提供者」や、個人でAIを扱う「業務外利用者」は対象外です（AI事業者ガイドラインの内容自体はどのような立場の方にとっても参考となり得ます）。

---

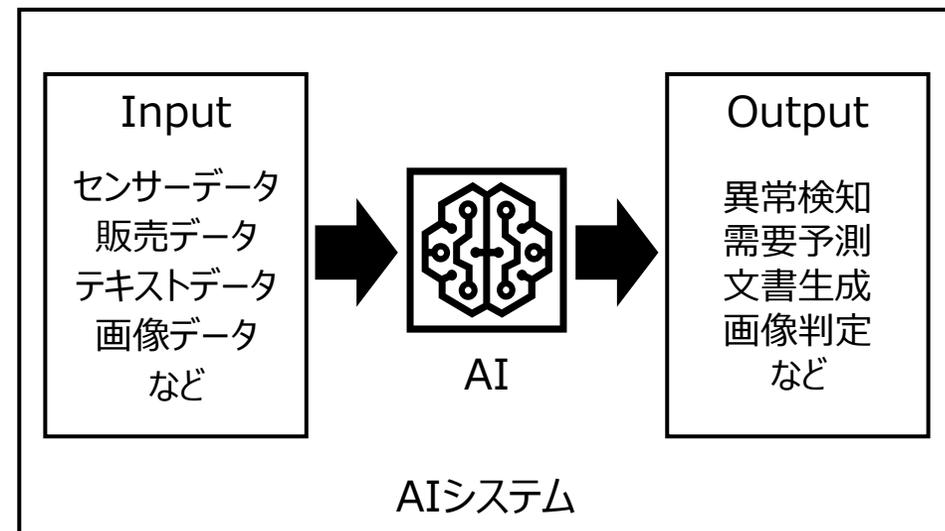
AI事業者ガイドラインの位置づけや活用の前提についての詳細な解説は以下を参照

- 本編はじめに (p.2~8)
- 別添.はじめに (p.2~5)

## AIシステムとは何か

AIは、社会において、需要予測システム、画像認識などで活用されています。

このようなAIを組み込んだシステムを、AI事業者ガイドラインでは、「AIシステム」として扱っております。



AIについての詳細な解説は以下を参照

- 本編第1部 関連する用語 (p.9~11)
- 別添1A.AIに関する前提 (p.6~14)

AIは、企業活動の全般にわたってその効果を発揮し、コスト削減や生産性向上、新たな価値創出などの便益が期待されています。

一方で、AIには偽・誤情報の拡散、個人情報の漏えい、バイアスによる差別的出力、悪用など、様々なリスクも存在します。

AIを活用する際は、これらのリスクを正しく認識し、適切な対策を講じることが重要です。

## AIの便益とリスク

## 便益



コスト削減  
生産性向上  
新たな価値創出

...

## リスク



偽・誤情報の拡散  
個人情報の漏えい  
悪用

...

## AIガバナンスとは

AIガバナンスとは、AIのリスクを適切に管理しながら、便益を最大限引き出すために、技術・組織・社会の各側面から必要な仕組みを作り、運用していくことです。

AI事業者ガイドラインでは、AIガバナンスを「AIの利活用によって生じるリスクをステークホルダーにとって受容可能な水準で管理しつつ、そこからもたらされる正のインパクト（便益）を最大化することを目的とする、ステークホルダーによる技術的、組織的、及び社会的システムの設計並びに運用」と定義しています。

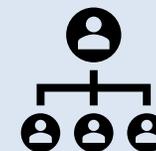
AIによるリスクを管理し、便益を最大化する  
仕組み作り・運用

## AIガバナンス



## 技術的システム

セキュリティ対策、  
品質管理の仕組みなど



## 組織的システム

社内ルール、教育体制、  
責任者の配置など



## 社会的システム

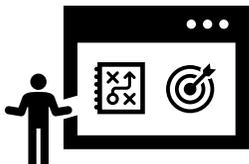
業界基準、法規制など

## Point

AIガバナンスは、経営陣やAIの責任者、IT部門などの組織が単独で考えるものではなく、関係者全員が関わっていることを理解する必要があります。

AIガバナンスについての詳細な解説は以下を参照  
本編第1部 関連する用語（p.9～11）、本編第2部E.AIガバナンスの構築（p.27～28）  
別添2.「第2部E.AIガバナンスの構築」関連（p.29～95）

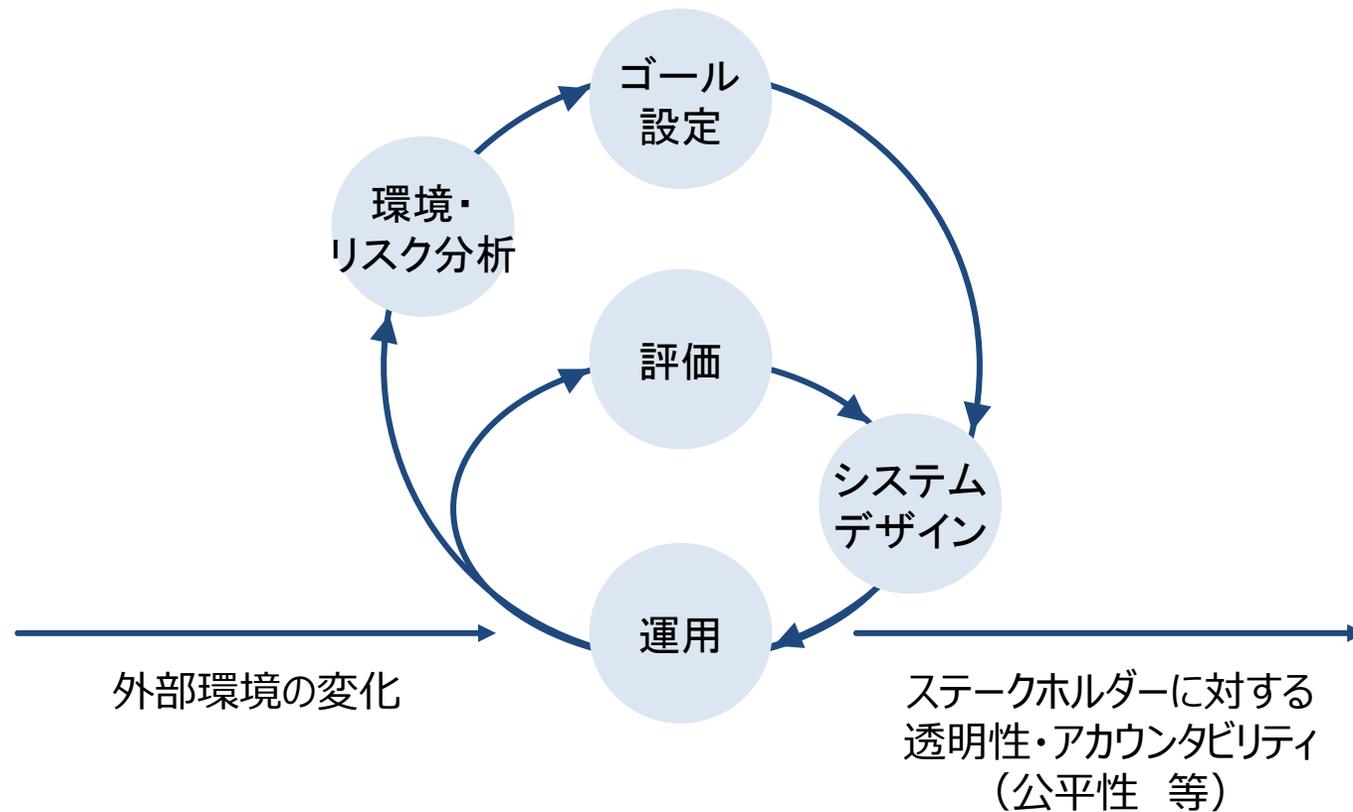
AIガバナンスの実践の要素は**環境・リスク分析**、**ゴール設定**、**システムデザイン**、**運用**、**評価**で構成されています。

環境・リスク分析	ゴール設定	システムデザイン	運用	評価
				
<p>把握する</p> <ul style="list-style-type: none"> <li>✓ AIの便益とリスク</li> <li>✓ AIの社会的な受容</li> <li>✓ 自社のAI成熟度</li> </ul>	<p>策定する</p> <ul style="list-style-type: none"> <li>✓ AIポリシー</li> <li>✓ 社内行動基準</li> </ul>	<p>設計・構築する</p> <ul style="list-style-type: none"> <li>✓ ゴールとの乖離の評価・対応方法</li> <li>✓ 組織間の連携体制</li> <li>✓ インシデント予防・対策</li> <li>✓ 社員の教育体制</li> </ul>	<p>説明可能な状態を確保しつつ、運用する</p> <ul style="list-style-type: none"> <li>✓ AIマネジメントシステム全体の運用状況</li> <li>✓ AIシステムごとの運用状況</li> </ul>	<p>チェックする・改善点を見つける</p> <ul style="list-style-type: none"> <li>✓ 第三者による評価</li> <li>✓ 関係者の意見収集・対応</li> </ul>

**Point**

上記の要素は単独で設定されていれば良いというものではありません。  
各要素がAIガバナンスの運用上どのように回るべきものは次のページで。

外部環境の変化に対応するため、環境・リスク分析、ゴール設定、システムデザイン、運用、評価のサイクルを回し続けることが重要です。



AIガバナンスの構築についての詳細な解説は以下を参照  
本編第2部E.AIガバナンスの構築 (p.27~28)  
別添2.「第2部E.AIガバナンスの構築」関連 (p.29~95)

# 主体区分とは

AI事業者ガイドラインではAIの事業活動を担う主体として、「**AI開発者**」、「**AI提供者**」及び「**AI利用者**」の3つの主体区分に大別し整理しています。

「データ提供者」および事業活動以外でAIを利用する「業務外利用者」は本ガイドラインの対象には含まれません

AI開発者	AI提供者	AI利用者
<p>AIシステムを<b>開発する事業者</b> (AIを<b>研究開発する事業者</b>を含む)</p>	<p>AIシステムを組み込んだ製品・サービスを<b>提供する事業者</b></p>	<p>事業活動において AIシステムまたはAIサービス を<b>利用する事業者</b></p>

## Point

事業者の企業単位の区分を示すものではなく、同一の事業者であっても、AI開発者とAI提供者など、複数の主体区分を兼ねる場合があります。

主体区分（AI開発者、AI提供者、AI利用者）についての詳細な解説は以下を参照

本編はじめに（p.4～8）

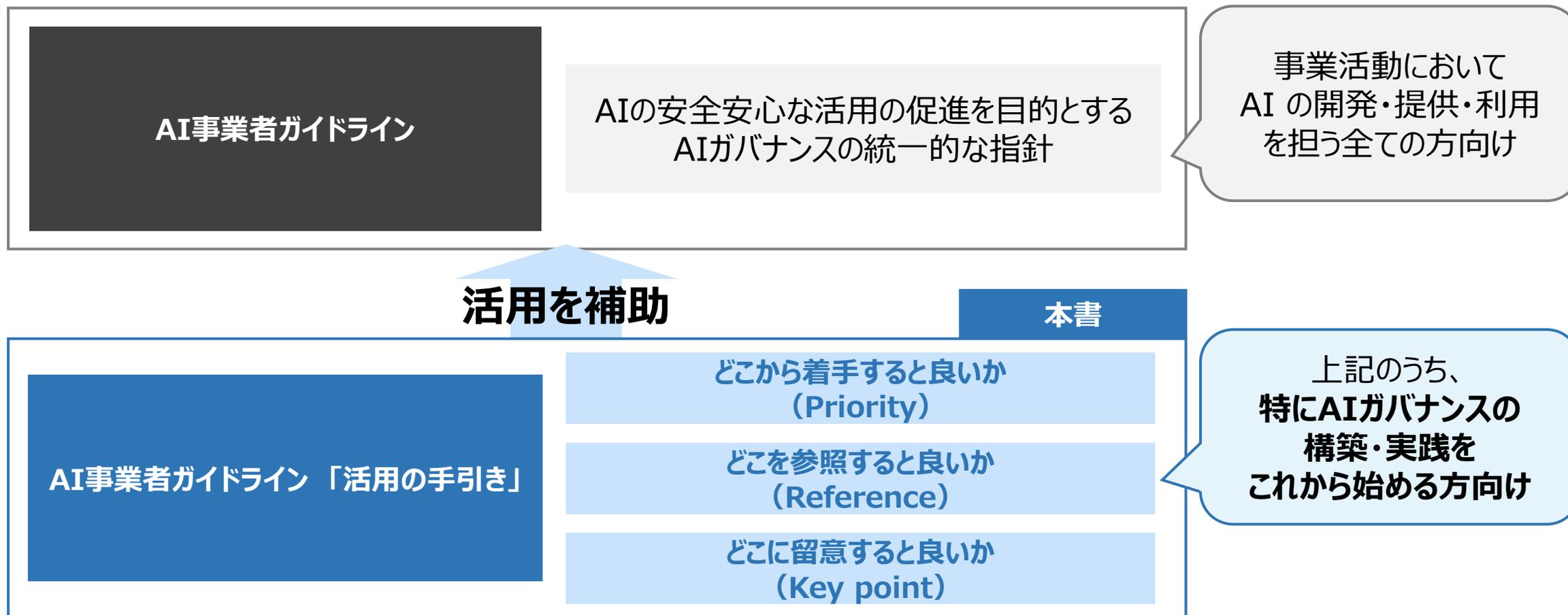
別添1A「AIの開発から利用までのバリューチェーン」、「AIシステム・サービスの例」及び「AI事業者のパターン」（p.9～15）

## 2章 本書の位置づけ

AI事業者ガイドラインの本編・別添および本書の位置づけ、構成について解説します。

---

本書は、**AI事業者ガイドラインの活用を補助**することを目的としています。特に、AIガバナンスの構築・実践をこれから始める方々に向けて、AI事業者ガイドラインの参照箇所や留意点等を示しています。



## 「AI事業者ガイドライン」の本編・別添資料の位置づけ

本書「活用の手引き」を利用する上での前提として、AI事業者ガイドラインの構成についてまずは説明します。AI事業者ガイドラインは、大きく分けると本編および別添から構成されています。

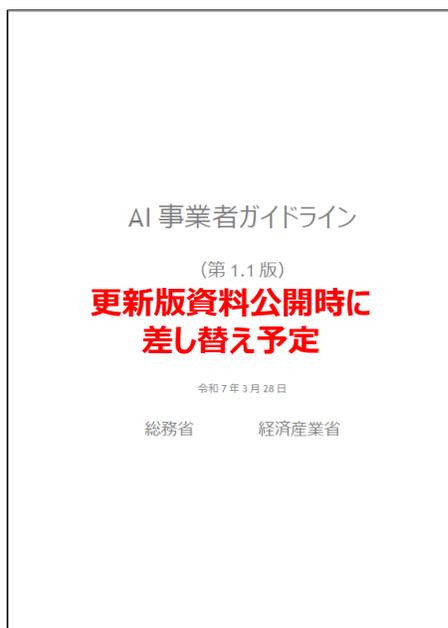
## 本編 (why, what)

どのような社会を目指すのか  
(基本理念=why)

どのような取組を行うのか  
(指針=what)

## 別添 (付属資料) (how)

どのようなアプローチで取り組むのか  
(実践=how)



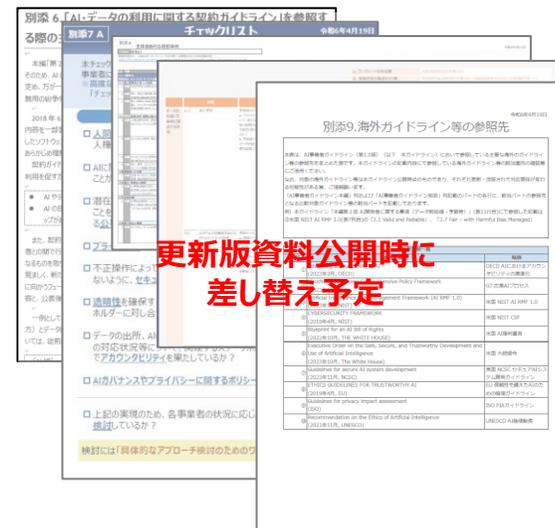
## 本編の解説資料

## 別添1~5



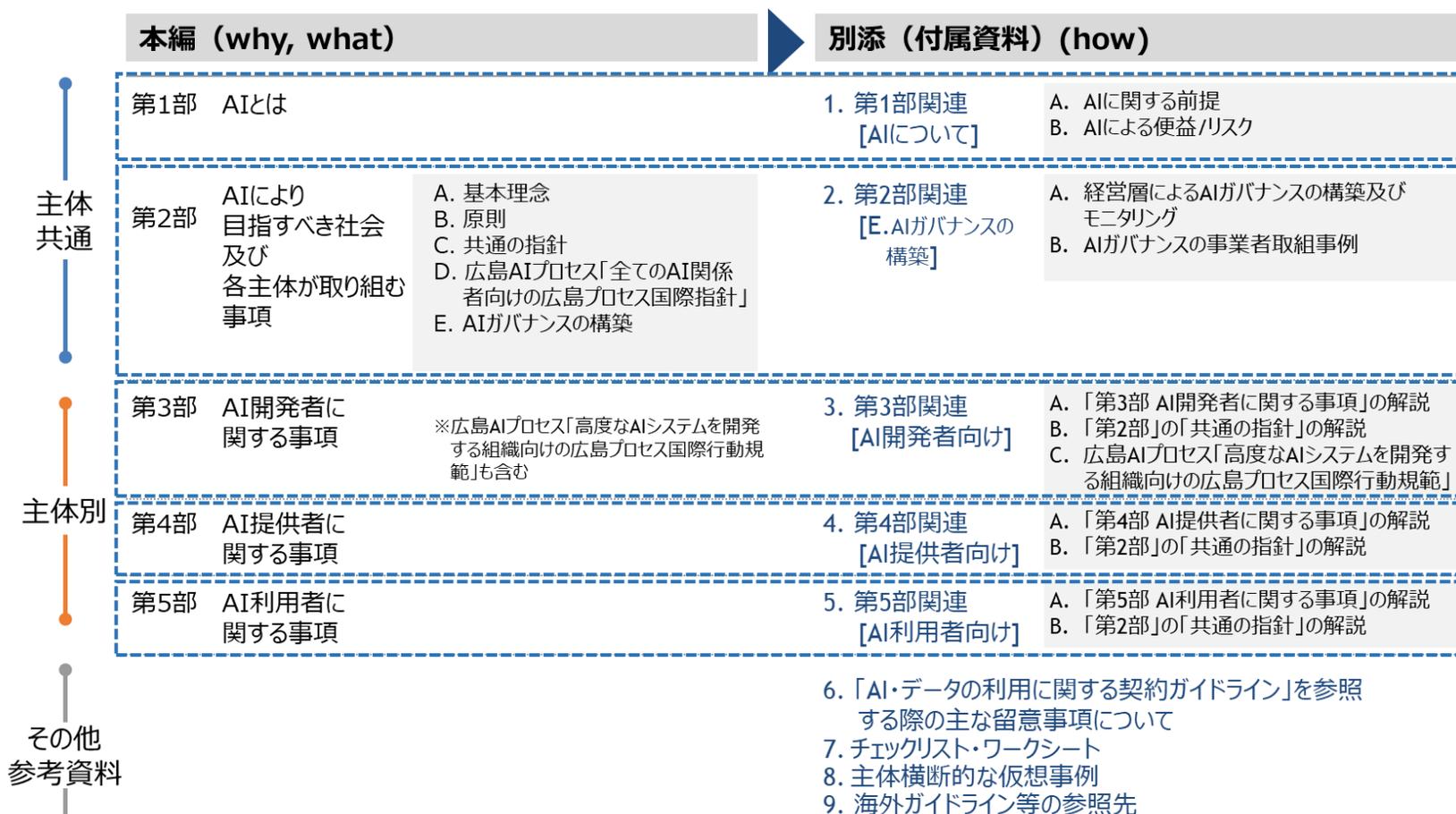
## ワークシート・その他補足資料

## 別添6~9



# 「AI事業者ガイドライン」の本編・別添資料の対応関係

AI事業者ガイドラインの本編の各部と、別添の各部はそれぞれ対応しています。  
別添は、本編の読解をサポートし、具体的な行動に繋げるための解説書です。



## 「AI事業者ガイドライン」の本編・別添資料の読み方

何を知りたいか、というポイント別に、AI事業者ガイドラインのどこを参照すると良いかを示します。

知りたいポイント別  
「AI事業者ガイドライン」の参照箇所



# 3章 AIガバナンスの構築・実践

AI事業者ガイドラインを用いてAIガバナンスの構築・実践をする際の準備、参照事項を説明します。

---

## 1. AIガバナンス構築時の準備事項

- ✓ AIガバナンス構築の準備・土台となる対応事項・要素について解説



☞ 上記の下線が引いてある各種見出しをクリックすると、概要のページに移動できます。適宜ご活用ください。

## 2. AIガバナンス実践時の参照事項

- ✓ AIガバナンス実践時につまずきやすい項目をいくつか取り上げ、AI事業者ガイドラインの参照の仕方・活用を解説

### AI事業者ガイドラインの参照箇所

#### 課題とAI事業者ガイドライン参照例

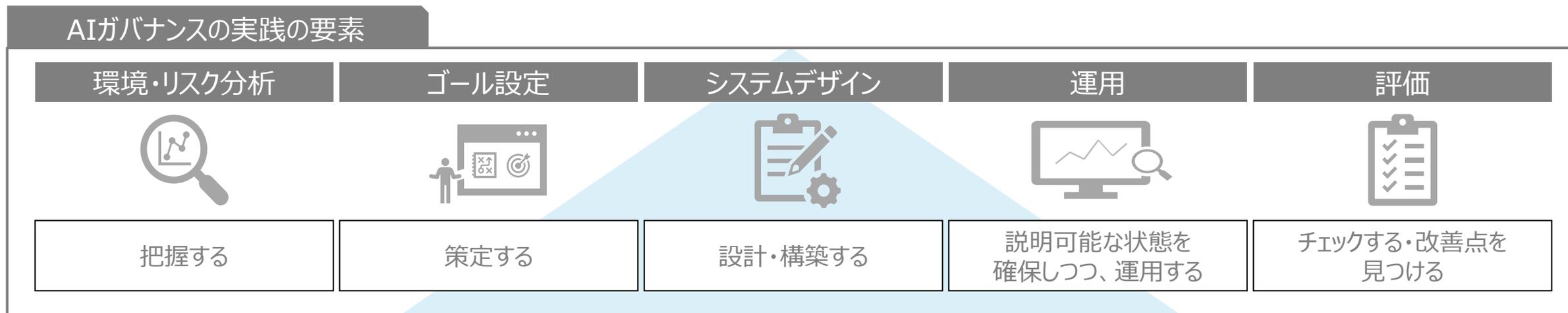
- ◆ リスク分類の整理
- ◆ リスクベースアプローチの採用
- ◆ 教育コンテンツの整理
- ◆ 契約に関する留意事項の把握

# 3章 1. AIガバナンス構築時の準備事項

これからAIガバナンスを構築する方向けに、はじめに対応すべきことを解説します。

---

AIガバナンスの構築時、実践の要素の土台として必要となる4つの事項について説明します。



### AIガバナンス構築時の準備事項



#### Point

P. 11のAIガバナンスの構築の要素は、それぞれ具体的取組に着目すると多数の項目があります。「AIガバナンス構築時の準備事項」はこれら全体に関わる準備・土台と考えてください。また、準備事項の取り組み順序については、事業者ごとの状況に応じて変わり得るため、並行して対応することも念頭に置き、ご判断ください。

## 1. AIガバナンス構築時の準備事項

- ✓ AIガバナンス構築の準備・土台となる対応事項・要素について解説



☞ 上記の下線が引いてある各種見出しをクリックすると、概要のページに移動できます。適宜ご活用ください。

## 2. AIガバナンス実践時の参照事項

- ✓ AIガバナンス実践時につまずきやすい項目をいくつか取り上げ、AI事業者ガイドラインの参照の仕方・活用を解説

### AI事業者ガイドラインの参照箇所

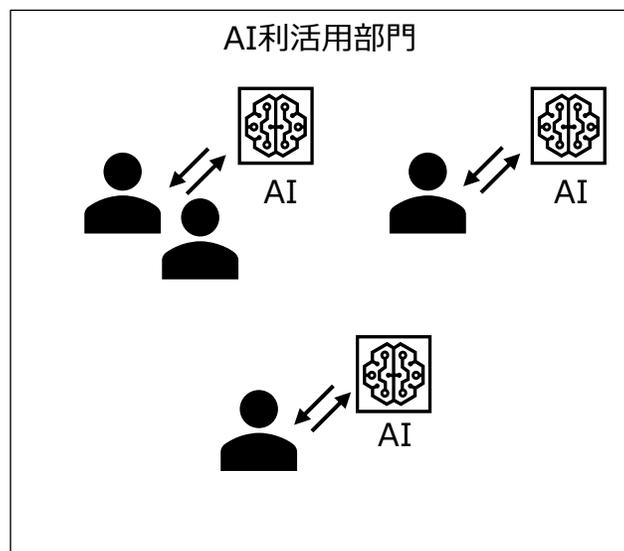
### 課題とAI事業者ガイドライン参照例

- ◆ リスク分類の整理
- ◆ リスクベースアプローチの採用
- ◆ 教育コンテンツの整理
- ◆ 契約に関する留意事項の把握

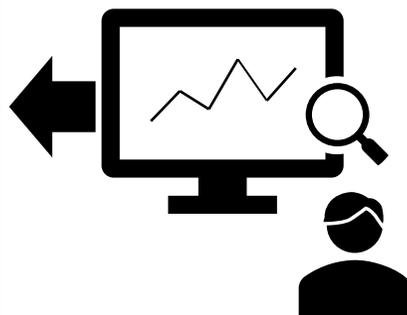
## 対応事項概要

組織内のAI開発・提供・利用の状況を適切に把握し、組織のAIリスク評価を適切に実施できる準備を整える。

組織内のAIの  
開発・提供・利用の状況



適切に把握・管理する



組織内のAI開発・提供・利用の状況を取得する仕組みを作る

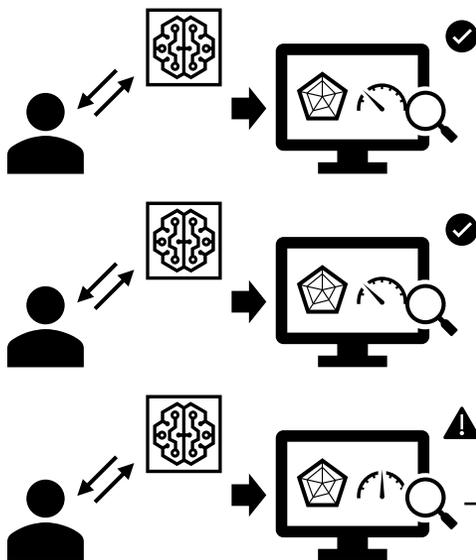
- ✓ **取得方法：**  
ユーザー側からの申請、定期アンケート/ヒアリング等を活用して、組織内のAI開発・提供・利用の状況を継続的に取得する
- ✓ **管理する項目：**  
どのような目的・用途で、どの部門が、どのようなAIを使っており、どのようなデータを用いているか等の情報を管理する

# リスク評価体制の構築

## 対応事項概要

リスク評価に関して相談できる体制を構築し、リスクベースアプローチの考え方で基準を設けて、窓口相談する場合とセルフチェックで良い場合を分けて対応する。

### 相談する基準を設ける



### 相談窓口を設置する



#### 相談窓口を設置する

現場で不足しているAIリスク評価・対策の知識・観点を相談できる窓口を設置する

#### 相談する基準を設ける

運用の負担を考慮し、すべてのユースケースを相談窓口へ寄せるのではなく、基準を設けて、ユースケースによって相談が必要な場合とセルフチェックで良い場合を分けて対応する（リスクベースアプローチ）

#### Point

既存の体制があれば、必ずしもAI活用のために体制を新規に構築する必要はありません。

# 参考) リスク評価体制の構築の参照箇所

## リスクコントロールの体制構築

行動目標 3-1【ゴール及び乖離の評価、並びに乖離対応の必須化】：  
 各主体は、経営層のリーダーシップの下、各主体のAIのAIガバナンス・ゴールからの乖離を特定し、乖離により生じる影響を評価し、リスクが認められる場合、その大きさ、範囲、発生頻度等を考慮して、その受容の合理性の有無を判定し、受容に合理性が認められない場合にAIの開発・提供・利用の在り方について再考を促すプロセスを、AIマネジメントシステム全体、及びAIシステム・サービスの設計段階、開発段階、利用開始前、利用開始後等の適切な段階に組み込むことが期待される。経営層は、再考プロセスについて基本方針等の方針策定、運営層はこのプロセスの具体化を行うことが重要である。そして、AIガバナンス・ゴールとの乖離評価には対象とするAIの開発・提供・利用に直接関わっていない者が加わるようにすることが期待される。なお、乖離があることを理由としてAIの開発・提供・利用を恣意的に不可とする対応は適当ではない。そのため、乖離評価はリスクを評価するためのステップであり、改善のためのきっかけにすぎない。

- 【実践のポイント】
- 各主体は、経営層のリーダーシップの下、以下に取り組む。
    - 「AIガバナンス・ゴール」からの乖離を特定し、リスクベースアプローチを用いて、リスクに対するコントロールを選択し、ユースケース、サービス又は製品ごとに適切なレベルの管理を実施
    - 現状のAIシステム・サービス及び「AIガバナンス・ゴール」からの乖離を特定・評価
    - リスクが認められる場合、その受容の合理性の有無を判定
    - 受容に合理性が認められない場合、開発・提供・利用の在り方を再考/再考するためのプロセス<sup>34</sup>の開発・提供・利用の適切な段階及び各主体内の組織における意思決定プロセスへの組み込み
    - 上記は経営層がリーダーシップを取って、その意思決定に責任を持ち、運営層が具体化した上で、継続的に実施
      - AIガバナンス、組織マネジメント及びプロジェクトマネジメントの仕組みを構築する責任は、運用責任と等しいことを認識し取り組む
  - 各主体内での認識の醸成を行うため、決定した乖離評価項目を各主体内で共有
    - 提供するAIの内容に応じて、各主体間で連携して乖離評価を実施

## 管理体制構築の参考事例



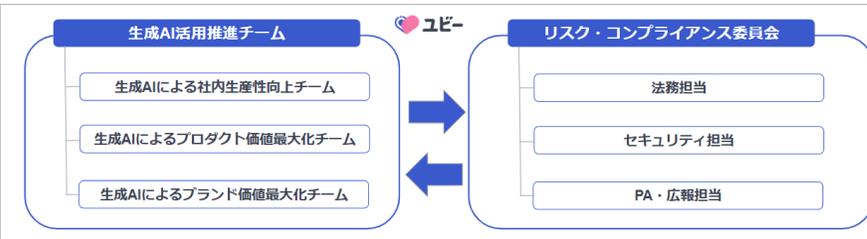
別添 図9. AIガバナンスの推進体制



別添 図20. AIガバナンス推進実行体制



別添 図17. AI倫理ガバナンスの体制



別添 図 26. Ubie株式会社におけるAIガバナンス体制

別添2A.行動目標3-1【ゴール及び乖離の評価、並びに乖離対応の必須化】（p.43～51）を参照

別添2B.AIガバナンスの構築に関する実際の取組事例（p.73～95）を参照

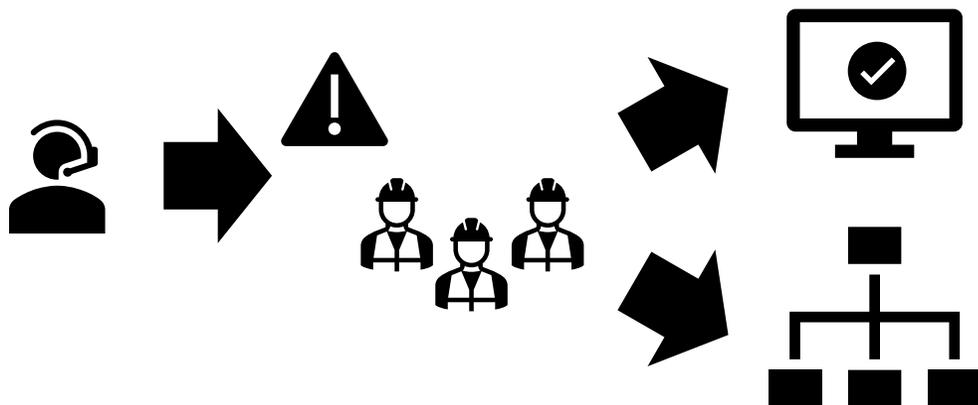
# インシデント報告体制の構築

## 対応事項概要

インシデントが発生した場合にも、適切な対応が取れるよう体制およびプロセスを整備する。

### 連絡窓口を設置する

### インシデント対応プロセスを事前に検討する



#### 連絡窓口を設置する

インシデントが発生した場合、速やかに報告できる窓口を設定する

#### インシデント対応プロセスを事前に検討する

インシデントの評価・分析や応急措置だけでなく、社内外への説明・報告フローについても事前検討、予行演習しておくことで、速やかな対応の準備をする

#### Point

既存の体制があれば、必ずしもAI活用のために体制を新規に構築する必要はありません。

## インシデント関連の負担軽減

**行動目標 3-4【予防・早期対応による AI 利用者及び業務外利用者のインシデント関連の負担軽減】：**  
各主体は、経営層のリーダーシップの下、インシデントの予防及び早期対応を通じて AI 利用者及び業務外利用者のインシデント関連の負担を軽減することが期待される。

## [実践のポイント]

各主体は、経営層のリーダーシップの下、以下に取り組むことが期待される。

- システム障害、情報漏洩、クレームの発生等のインシデントの予防及び早期対応
- ライフサイクル全体を通じてインシデントを予防し、又は発生した場合に早期に対応できる体制を構築

インシデントを予防し、又は発生した場合に早期に対応できる体制の構築の際には以下の点に留意する。

- 過去事例の蓄積及び行動目標 3-3 で収集した情報の活用による予防策・事前準備策の検討
- 関連する主体間での責任の分配（リスクを軽減できる者への分配）
- 確率的に一定の経済的損失が発生する用途に対応する保険の活用を通じた経済的な損失への早期の対応

- 別添2A.行動目標3-4【予防・早期対応によるAI利用者及び業務外利用者のインシデント関連の負担軽減】（p.58）を参照

## インシデント発生時の対応の事前検討

## 行動目標 3-4-2【インシデント発生時の対応の事前検討】：

各主体は、経営層のリーダーシップの下、AI インシデント発生時に、AI 利用者及び業務外利用者への説明、影響範囲、損害の特定、法的関係の整理、被害救済措置、被害拡大防止措置、再発防止策の検討等を速やかに実施するため、対応方針の決定及び計画の策定を検討するとともに、当該対応方針又は計画に関して適宜実践的な予行演習を実施することが期待される。

## [実践のポイント]

各主体は、経営層のリーダーシップの下、以下に取り組むことが期待される。

- AI インシデント発生時の対応方針及び計画を策定
- 上記について、適宜実践的な予行演習を実施

AI インシデント発生時に備え以下のような体制をあらかじめ整備することが期待される。

- 連絡受付窓口の設置
- 対応担当役員のアサイン
- 対応担当者個々の役割分担
- 対応アプローチ・プロセス
- リスク管理部門等の社内関係者への連絡体制
- 顧問弁護士等の社外関係者及び専門家への連絡体制
- ステークホルダーに対して通知するプロセス等

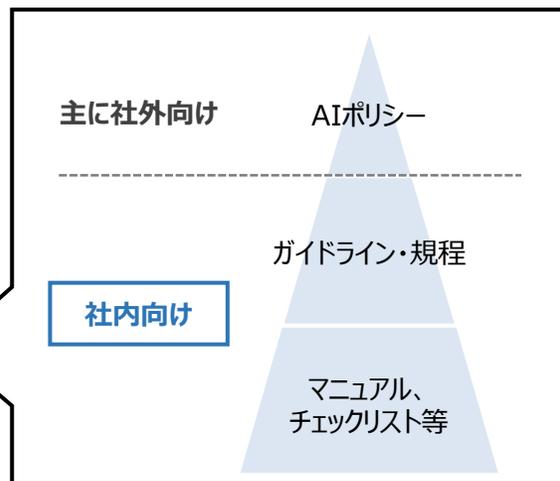
なお、AI システム・サービスの AI インシデントの事業への影響が大きい場合は、事業継続計画（BCP）を実際に発動させる際の重大要素として、AI インシデントを盛り込むことも検討する。

- 別添2A.行動目標3-4-2【インシデント発生時の対応の事前検討】（p.61～62）を参照

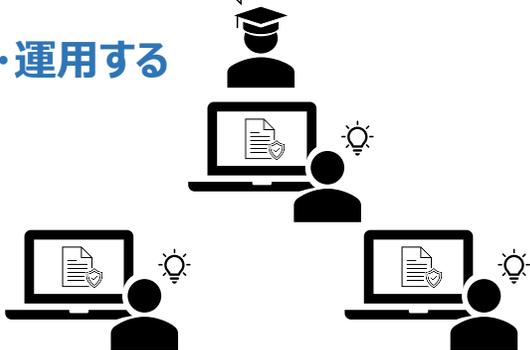
## 対応事項概要

組織が扱うAIに対する考え方について共通認識を持てるように、ルールを整備し、周知する

## ルールを整備する



## 周知・運用する



## ルールを整備する

ルールを明文化することで、社内の共通認識を形成する

## 周知・運用する

ルールがしっかり遂行されるよう、社内教育含め、組織を構成するメンバーにルールを浸透させる

## 組織内の情報共有

## 行動目標 3-3-2【環境・リスク分析のための日常的な情報収集・意見交換の奨励】:

各主体は、経営層のリーダーシップの下、日常的に、AIシステム・サービスの開発及び運用に関するルール整備、ベストプラクティス、インシデント等の情報を収集するとともに、社内外の意見交換を奨励することが期待される。

## 【実践のポイント】

各主体は、経営層のリーダーシップの下、以下に取り組むことが期待される。

- 日常的な、ルール整備、ベストプラクティス、インシデント等の情報収集
- AIマネジメントチームを社内に設置している場合であっても、社内の他部門との議論及び勉強会を開催したり、他社も参加する団体活動に関与

- 別添2A.行動目標3-3-2【環境・リスク分析のための日常的な情報収集・意見交換の奨励】(p.57)を参照

## AI利活用ガイドラインの策定

「別添2B. AIガバナンスの構築に関する実際の取組事例」で紹介している事例のうち、以下2事業者はガイドラインを公開しているため適宜参照

コラム 8 : 富士通グループの AI ガバナンスに関する取組<sup>64)</sup>

同社は、AIの開発・提供企業として、AIに関する懸念や予期せぬ不都合の解消と適切な技術活用による持続可能な社会の創造を責務とし、広島 AI プロセス「報告枠組み」への参画、AI ガバナンスの国際的な議論への積極的な参加に加え、後述の AI の倫理審査や開発プロセスにおけるリスク管理などの社内ガバナンスの取組を推進している。さらには、AI ガバナンスの取組紹介や生成 AI 利活用ガイドラインの公開、AI 倫理の重要性を喚起する「Fujitsu AI 倫理かるた<sup>67)</sup>」の公開など、社外への普及の取組にも力を入れている。<sup>68)</sup>

2018年に加盟した欧州コンソーシアム「AI4People」が提案する5原則を参考に、2019年に「富士通グループ AI コミットメント」を策定、さらにその実践のために、AIの利活用方法に応じた具体的な判断基準や手順を整備した(「図 16. 富士通グループ AI コミットメント」参照)。また、AI ガバナンスの取組に対する客観的な評価を得るべく、「富士通グループ AI 倫理外部委員会」を設置し、AI 技術のほか、生命医学、生態学、法学、SDGs、消費者問題など多様性を重視した外部の専門家その委員として招聘している。社長をはじめ経営陣がオブザーバーとして参加する同委員会における活発な議論を提言として取りまとめ、これを取締役会へと共有することで、AI 倫理を「企業経営上の重要課題」としてコーポレートガバナンスに組み込んでいる。<sup>69)</sup>

「コラム 8 : 富士通グループの AI ガバナンスに関する取組」

## コラム 12 : 神戸市における AI 活用のためのルール整備

神戸市は、政令指定都市であり、人口約 150 万人(政令市 7 位)、市職員数は約 2 万人(教員含む)。同市は、一定のルールで AI を効果的かつ安全に活用することを目的として、「神戸市における AI の活用等に関する条例」(以下「AI 条例」という)を制定している。対象は、神戸市及び市の業務を請負・委託等する事業者となる。AI 条例を策定する際には、AI 事業者ガイドライン及び EU の「AI 法 (Artificial Intelligence Act)」をもとに、同市が AI 利用者として果たすべき責務を盛り込んだ。ガイドラインや法規制等の単語をそのまま利用するのではなく、市職員が理解しやすい単語に置き換えて利用する等の工夫を行っている。

AI 条例は、市が行政処分等に AI を用いようとする場合にリスクアセスメントを行うことを定める。AI の持つリスクをゼロとすることは現実的ではなく、職員が AI の持つリスクを正しく認識し、そのリスクに対処する仕組みを設けることが重要である。また、「リスクベースアプローチ」の考え方を参考に、行政処分等の市民の権利利益に重大な影響を与え得る判断に AI を活用する際には、リスクに応じた慎重な手続きを課し、それ以外には簡便なチェックとすることで、AI 活用の推進と安全確保のバランスを保つことに配慮している。

「コラム 12 : 神戸市における AI 活用のためのルール整備」

- 別添2B. AIガバナンスの構築に関する実際の取組事例 (p.73~95)を参照

## 3章 2. AIガバナンス実践時の参照事項

AIガバナンスの実践におけるAI事業者ガイドラインの活用の仕方、参照箇所を説明します。

---

## 1. AIガバナンス構築時の準備事項

- ✓ AIガバナンス構築の準備・土台となる対応事項・要素について解説



☞ 上記の下線が引いてある各種見出しをクリックすると、概要のページに移動できます。適宜ご活用ください。

## 2. AIガバナンス実践時の参照事項

- ✓ AIガバナンス実践時につまずきやすい項目をいくつか取り上げ、AI事業者ガイドラインの参照の仕方・活用を解説

### AI事業者ガイドラインの参照箇所

#### 課題とAI事業者ガイドライン参照例

- ◆ リスク分類の整理
- ◆ リスクベースアプローチの採用
- ◆ 教育コンテンツの整理
- ◆ 契約に関する留意事項の把握

## AIガバナンスの実践の要素

環境・リスク分析



ゴール設定



システムデザイン



運用



評価



AIガバナンスの実践時にはAI事業者ガイドラインの以下の箇所を特に参照してください。

AIガバナンスの実践の各要素に関連するポイントや事例（本編第2部Eおよび別添2）

主体毎の留意事項（本編第3～5部および別添3～5）

行動目標1-1【便益/リスクの理解】：

各主体は、経営層のリーダーシップの下、AIの開発・提供・利用の目的を明確化したうえで、AIから得られる便益だけでなく意図しないリスクがあることについて、各主体の事業に照らして具体的に理解し、これらを経営層に報告し、経営層で共有し、適時に理解を更新する。

【実践のポイント】

【実践のポイント】

各主体は、経営層のリーダーシップの下、以下に取り組む。

- 事業における価値の創出、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
- 自社の事業に結びつく形で、「便益」及び意図せざるものを含めた「リスク」を具体的に理解
- その際に、回避すべき「リスク」及び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便益を確保、リスクを削減
- 迅速に経営層に報告/共有する仕組みを構築

実務的な観点も  
掲載しています

行動目標

各種AIガバナンスの実践の要素に対して、一般的かつ客観的な目標を記載

実践ポイント・実践例

各行動目標のポイントを記載・仮想事例に基づく事例を記載

A. 本編「第3部 AI開発者に関する事項」の解説

【本編の記載内容（再掲）】

データ前処理・学習時

D-2) i. 適切なデータの学習

- ◇ プライバシー・バイ・デザイン等を通じて、学習時のデータについて、適正に収集するとともに、第三者の個人情報、知的財産権に留意が必要な等が含まれている場合には、法令に従って適切に扱うことを、AIのライフサイクル全体を通じて確保する（「2」安全性、「4」プライバシー保護、「5」セキュリティ確保）
- ◇ 学習前・学習全体を通じて、データのアクセスを管理するデータ管理・制限機能の導入検討を行う等、適切な保護措置を実施する（「2」安全性、「5」セキュリティ確保）

各主体の留意事項  
を記載

【ポイント】

- AIモデルの質の向上のために、AI開発者は、AIの学習等に用いるデータの質に留意することが重要となる。
- 利用するAIの特性及び用途を踏まえ、AIの学習等に用いるデータの質（正確性及び完全性等）に留意する<sup>85</sup>
- また、AIの学習等に用いるデータの質を向上させるため、想定

実務的・技術的な観点も  
掲載しています留意事項に関する  
各主体の具体的な  
アプローチを記載

次のページ以降でAIガバナンス実践時に想定される課題に対して参考となる箇所について紹介します。

## 課題

自社のリスク分類に過不足がないか判断がつかない

## AI事業者ガイドラインの活用ポイント

AI事業者ガイドラインにおけるリスク分類と、自社内でのリスク分類・観点を比較する

## ■ AI事業者ガイドラインで提供している共通指針の活用

👉 リスクの洗い出しに活用できるフレームワークを整理・活用する  
AI事業者ガイドラインで紹介している10の「共通指針」を活用し、自社内でのリスク分析・評価の枠組みと比較する。

## 10の「共通指針」

各主体が 取り組む事項	1) 人間中心	社会と連携した 取組が 期待される事項	8) 教育・リテラシー
	2) 安全性		9) 公正競争確保
	3) 公平性		10) イノベーション
	4) プライバシー保護		
	5) セキュリティ確保		
	6) 透明性		
	7) アカウンタビリティ		

AIの共通指針についての詳細な解説は以下を参照  
本編第2部 AIにより目指すべき社会及び各主体が取り組む事項 (p.12～28)

AI事業者ガイドラインでは、共通指針の枠組みに沿って、各資料、各章が構成されています。詳細を確認し、自社のリスク分類・観点の過不足のご確認に活用下さい。

表 1. 「共通の指針」に加えて主体毎に重要となる事項

	第2部. C. 共通の指針	「共通の指針」に加えて主体毎に重要となる事項		
		第3部. AI 開発者 (D)	第4部. AI 提供者 (P)	第5部. AI 利用者 (U)
1) 人間中心	① 人間の尊厳及び個人の自律 ② AIによる意思決定・感情の操作等への留意 ③ 偽情報等への対策 ④ 多様性・包摂性の確保 ⑤ 利用者支援 ⑥ 持続可能性の確保			
2) 安全性	① 人間の生命・身体・財産、精神及び環境への配慮 ② 適正利用 ③ 適正学習	i. 適切なデータの学習 ii. 人間の生命・身体・財産、精神及び環境に配慮した開発 iii. 適正利用に資する開発	i. 人間の生命・身体・財産、精神及び環境に配慮したリスク対策 ii. 適正利用に資する提供	i. 安全を考慮した適正利用
3) 公平性	① AIモデルの各構成技術に含まれるバイアスへの配慮 ② 人間の判断の介入	i. データに含まれるバイアスへの配慮 ii. AIモデルのアルゴリズム等に含まれるバイアスへの配慮	i. AIシステム・サービスの構成及びデータに含まれるバイアスへの配慮	i. 入力データ又はプロンプトに含まれるバイアスへの配慮

## 参考) リスク分析の参照事項

## AIによるリスク例の紹介

## AIによるリスク

便益が広がる一方で、利用の拡大及び新技術の台頭に伴い、それらが生み出すリスクも増大している。特に生成 AI の普及に伴っては、偽情報・誤情報の生成・発信等リスクの多様化・増大が進むほか、知的財産権の尊重を求める声が高まっている。

- ・下表はAIのリスクを網羅したものではなく、想定に基づく事案も含んでおり、あくまで一例として認識することが期待される
- ・下表には政府等の公的機関も含めた社会全体での対応・議論が必要となるリスクも含まれる

リスク例	関連する共通の指針	「共通の指針」に加えて主体毎に重要となる事項		
		第3部 AI開発者	第4部 AI提供者	第5部 AI利用者
データ汚染攻撃等のAIシステムへの攻撃	5) セキュリティ確保	i. セキュリティ対策のための仕組みの導入 ii. 最新動向への留意	i. セキュリティ対策のための仕組みの導入 ii. 脆弱性への対応	i. セキュリティ対策の実施
バイアスのある出力、一貫性のない出力等	1) 人間中心 ①人間の尊厳及び個人の自律 ③偽情報等への対策			
ハルシネーション等による誤った出力	2) 安全性	i. 適切なデータの学習 ii. 人間の生命・身体・財産、精神及び環境に配慮した開発 iii. 適正利用に資する開発	i. 人間の生命・身体・財産、精神及び環境に配慮したリスク対策 ii. 適正利用に資する提供	i. 安全を考慮した適正利用
	3) 公平性	i. データに含まれるバイアスへの配慮 ii. AIモデルのアルゴリズム等に含まれるバイアスへの配慮	i. AIシステム・サービスの構成及びデータに含まれるバイアスへの配慮	i. 入力データ又はプロンプトに含まれるバイアスへの配慮
	8) 教育・リテラシー			
ブラックボックス化、判断に関する説明の不足	6) 透明性	i. 検証可能性の確保 ii. 関連するステークホルダーへの情報提供	i. システムアーキテクチャ等の文書化 ii. 関連するステークホルダーへの情報提供	i. 関連するステークホルダーへの情報提供
	7) アカウンタビリティ	i. AI提供者への「共通の指針」の対応状況の説明	i. AI利用者への「共通の指針」の対応状況の説明	i. 関連するステークホルダーへの説明

- ・ 別添1B.AIによる便益/リスク (p.17~28) を参照

## 「環境・リスクの分析」における実践のポイント・実践例の紹介

## A.経営層による AI ガバナンスの構築及びモニタリング

## 1.環境・リスク分析

行動目標 1-1【便益/リスクの理解】:

各主体は、経営層のリーダーシップの下、AIの開発・提供・利用の目的を明確化したうえで、AIから得られる便益だけでなく意図しないリスクがあることについて、各主体の事業に照らして具体的に理解し、これらを経営層に報告し、経営層で共有し、適時に理解を更新する。

【実践のポイント】

各主体は、経営層のリーダーシップの下、以下に取り組み<sup>18)</sup>。

- 事業における価値の創出、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
- 自社の事業に結びつく形で、「便益」及び意図せざるものを含めた「リスク」を具体的に理解
- その際に、回避すべき「リスク」及び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便益を確保、リスクを削減
- 迅速に経営層に報告/共有する仕組みを構築

「リスク」としては、具体的には以下のようなものが挙げられ、これらのリスクに起因して、レピュテーションの低下及び法令違反を理由とした制裁金並びに損害賠償責任の負担等による損失が生じる可能性もある。リスクについての詳細は、別添 1.【B.AIによる便益/リスク】を参照いただきたい。

- AI全般に共通するリスク
  - バイアスのある結果及び差別的な結果の出力、フィルターバブル・エコーチェンバー、偽情報、不適切な個人情報の取扱い、データ汚染攻撃、ブラックボックス化、機密データの漏洩、AIシステム・サービスの悪用、エネルギー使用量及び環境の負荷、バイアスの再生成 等
- 生成 AI により顕在化したリスク
  - ハルシネーション、誤情報を鵜呑みにすること、著作権等の権利及び資格との関係 等
- 組織・管理に起因するリスク
  - 製品又はサービスに AI が含まれていることの不認識、ガバナンスにおける AI に関する考慮不足、環境認識又は計画等が不足したことによる不適切、偏在的な AI の活用、仕事の棲み分け、人間と AI との関係性の整理不足 等

なお、バリューチェーン/リスクチェーン全体での便益の確保、リスクの削減に努めるために重要な複数主体にまたがる論点として、例えば、以下のものが挙げられる。

- 主体間、又は主体内の責任分配
- AIシステム・サービス全体の品質向上
- 各 AIシステム・サービスが相互に繋がることによる新たな価値の創出の可能性 (System of Systems)
- AI利用者・業務外利用者のリテラシー向上

- ・ 別添2A 1.環境・リスク分析 (p.31~39) を参照

## 課題

リスクの大小をどのように判断すべきかの基準がない

## AI事業者ガイドラインの活用ポイント

リスクの大きさ（影響の大きさ・可能性）を把握したうえで、その対策の程度をリスクの大きさに対応させる「リスクベースアプローチ」の考え方を採用する

## ■リスクベースアプローチの採用

👉 **リスクレベルを定義して、影響の大きさや可能性に応じた対応を定める**

## リスクレベル定義

## 対応方針

ハイリスク

- **リスク評価組織で対応策を検討の上、承認が必要。**

その他

- **部署内でのセルフチェックで対応**

別添2A.行動目標3-1【ゴール及び乖離の評価、並びに乖離対応の必須化】(p.43~46)を参照

AI事業者ガイドラインの「実践例」ではユースケースごとにリスクレベルを定義し対応を定める、リスクベースアプローチの採用事例も紹介しています。

## 【実践例 vi：リスクベースアプローチによるAIの提供及び利用に関する活動】

当社では、AIの提供及び利用の際のリスクベースアプローチの考え方として、透明性の確保、公平性の確保、信頼性の確保、AI利用の公表、知的財産の保護、その他の計6つの検討項目を定め、各検討項目において、潜在的なリスクと、その潜在的リスクに対するコントロール手法（最低限の対処）を定めている。例として、透明性の確保では、潜在的リスクとして、「モデルのバージョンを保存せず、AIの判断に起因する事象発生時や、検証が必要な際にAIの事後検証ができなくなるリスク」を挙げ、これに対するコントロール手法として、「AIモデル開発に用いた学習データを保管」を規定している。そして、実際のAIの提供及び利用部門が、リスクの有無とそれに対する具体的なコントロール手法の評価を行い、その結果をリスク評価部門が更に評価することで総合的にリスクへの対応の妥当性を判断している。

検討項目		潜在的なリスク	その他固有リスク①	コントロール手法	その他コントロール手法②	妥当性評価	判断
大項目	中項目		記入欄 業務担当部門		記入欄 業務担当部門		
透明性の確保	データ・学習済モデルの管理	・学習・推論データ・学習済モデルのバージョンを保存せず、AIの判断に起因する事象発生時や、検証が必要な際に判断根拠の事後検証ができなくなるリスク	左記以外のリスク無し	・AIモデル開発に用いた学習データを保管 ・使用した推論データおよび推論結果の保管 … (例外規定：～であるデータは保管の対象外とする)	左記のとおり対応	①において、○○○○というリスクも考えられるではないか	差し戻し ①において、考慮すべき観点の異なる検討
…	…	…	…	…	…	…	…

図 8. リスクベースアプローチの例

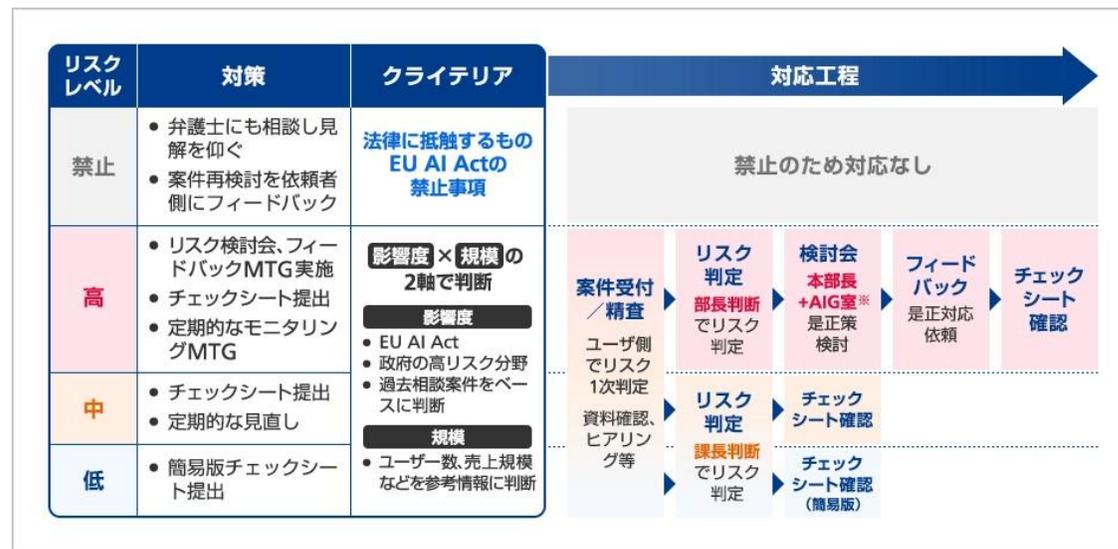
## リスクベースアプローチの考え方

## B.AIによる便益/リスク

AIは、新規ビジネスを生み出したり、既存ビジネスの付加価値を高めたり、生産性を向上させたりする等の便益をもたらす一方で、リスクも存在する。

このリスクについては可能な限り抑制することが期待される。一方で、過度なリスク対策を講じることは、コスト増になる等、AI活用によって得られる便益を阻害してしまうことから、リスク対策の程度をリスクの性質及び蓋然性の高さに対応させるリスクベースアプローチの考え方が重要である。

## リスクベースアプローチの実践例



別添図 23.ソフトバンクのリスクベースアプローチ

- 本編はじめに (p.3~4) を参照
- 別添1B.AIによる便益/リスク (p.17~28) を参照

- 別添2A.行動目標3-1【ゴール及び乖離の評価、並びに乖離対応の必須化】(p.43~46)、行動目標5-1【AIマネジメントシステムの機能の検証】(p.67~69)を参照
- 別添2B.AIガバナンスの構築に関する実際の取組事例 (p.73~95) を参照

## 課題

社員のAIリテラシーをどうやって向上させたらよいかわからない

AI事業者ガイドライン  
の活用ポイント

リテラシー向上のための施策例を確認する

## ■ 教育リテラシー向上のための施策例の確認

👉リテラシー向上のためのアプローチや教育コンテンツの活用事例を参考に、自社に合った教育カリキュラムを設定する。

AI事業者ガイドラインの「実践例」では外部教材等を活用した教育例も紹介しています。

## 行動目標 3-2【AI マネジメントシステムの人材リテラシー向上】：

各主体は、経営層のリーダーシップの下、AI マネジメントシステムを適切に運営するために、外部の教材の活用も検討し、AI リテラシーを戦略的に向上させることが期待される。例えば、AI システム・サービスの法的・倫理的側面に責任を負う役員、マネジメントチーム、担当者には、AI 倫理及び AI の信頼性に関する一般的なリテラシー向上のための教育を、AI システム・サービスの開発・提供・利用プロジェクトの担当者には AI 倫理だけではなく生成 AI を含む AI 技術に関する研修を、全者に対して AI マネジメントシステムの位置づけ及び重要性についての教育を提供することが考えられる。

## [実践のポイント]

- 各主体は、経営層のリーダーシップの下、以下に取り組むことが期待される。
- 外部講師によるものを含め、役職及び担当に適した研修及び教材を用い、AI リテラシーの向上を図ること
  - その際、各者の果たすべき役割に応じて適した研修及び教材の活用
  - 特に重要となる AI 倫理については全社員に受講させる等の工夫

## ■ AI事業者ガイドラインの実践例で紹介されている外部リソースの採用例

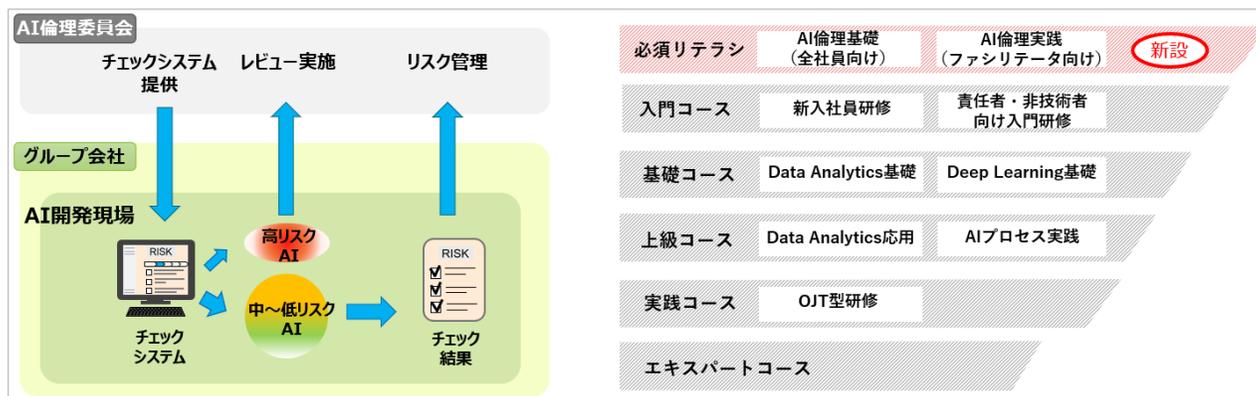
## 経済産業省の提供コンテンツ

- マナビ DX
- マナビ DX Quest など

## 資格試験

- ITパスポート
- G検定 など

## 教育コンテンツの検討例



別添図14. AIガバナンスの体制 概要



別添 図22. ソフトバンクのAI倫理・ガバナンス教育の推進活動

- 別添2B.AIガバナンスの構築に関する実際の実践事例 (p.73~95) を参照

## 課題

既存の契約ひな形等でAI固有の論点をカバーしきれていない

## AI事業者ガイドラインの活用ポイント

特に、AI特有のリスク対策を整理した上で、契約者間で役割分担し、契約内容に反映する。

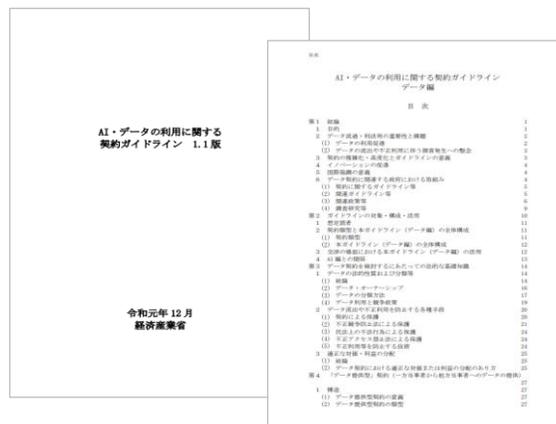
### AIガバナンス上必要な事項を契約内容に反映するまでの流れ



### その他の法的論点の確認

- 「別添6.『AI・データの利用に関する契約ガイドライン』に記載の留意事項について」では、契約の検討に有益なガイドラインを紹介しています。
- 個人情報や知的財産権などの個別の留意事項については、別添6でも紹介している以下ガイドラインに詳述されています。
  - AI・データの利用に関する契約ガイドライン
  - 契約チェックリスト

### ● AI・データの利用に関する契約ガイドライン



### ● 契約チェックリスト



別添6.「AI・データの利用に関する契約ガイドライン」を参照する際の主な留意事項について (p.183~187) を参照