JIPDECセミナー　講演資料

ISO/IEC 42001認証事例紹介「AIMSを通じたAIガバナンスの「実装」」

本資料は、JIPDECセミナー「AIのリスクマネジメントとAIマネジメントシステム（AIMS）認証の最新動向」（2026年4月20日までのオンデマンド配信）の資料です。
セミナーお申込み者様限定での配布となりますので、WEB、SNS等への掲載、転載はご遠慮ください。

GODOT

JIPDEC セミナー「AI のリスクマネジメントと AI マネジメントシステム(AIMS)認証の最新動向」

AIMSを通じたAIガバナンスの「実装」

株式会社Godot

2026.03.25

Agenda

01	株式会社Godotの紹介
02	Godotが取得に至った理由
03	AIMSのリスクベースアプローチ
04	AIMSがGodotへもたらした効果
05	AIによるAIガバナンスの強化

Agenda

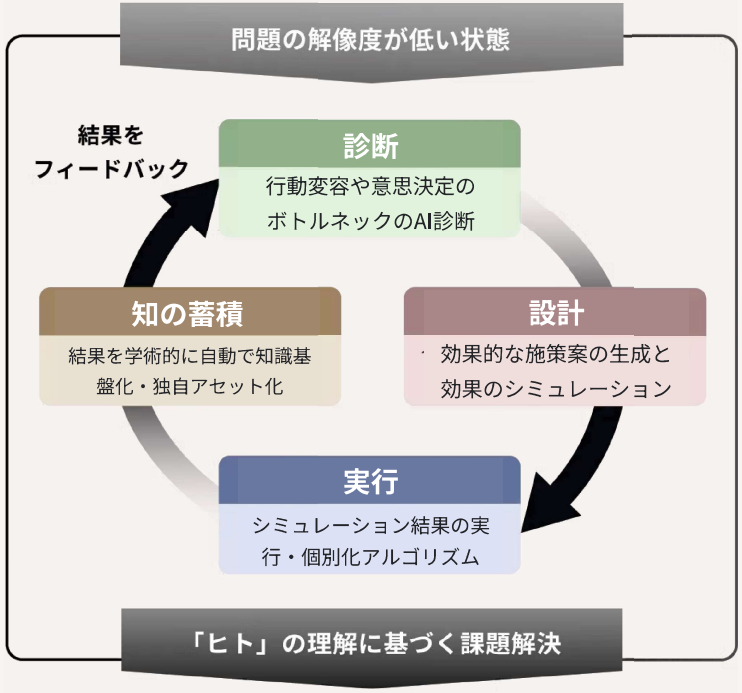
01	**株式会社Godotの紹介**
02	Godotが取得に至った理由
03	AIMSのリスクベースアプローチ
04	AIMSがGodotへもたらした効果
05	AIによるAIガバナンスの強化

株式会社Godotの紹介

行動原理の構造分析および行動変容を統合支援する学習型 AI システムを開発・提供するスタートアップ企業

社名	株式会社Godot
設立	2022年7月1日
代表者	代表取締役 森山健
本店	神戸市中央区浪花町56 KiP内
ﾒｲﾝﾊﾞﾝｸ	三井住友銀行 神戸営業部
事業概要	行動原理に関するAI・システム開発
取引先	神戸市、京都市、大阪市、読谷村 他 生損保、総合商社、食品大手 他
表彰等	『Forbes JAPAN』「2026年注目の日本発スタートアップ100選」、 「JAPAN'S AI 50」に選出

AIエージェントを活用したアプローチサイクル



Agenda

01	株式会社Godotの紹介
02	**Godotが取得に至った理由**
03	AIMSのリスクベースアプローチ
04	AIMSがGodotへもたらした効果
05	AIによるAIガバナンスの強化

Godotが取得に至った理由

信頼されるAIシステムの開発と運用

AIシステムの信頼性と透明性を確保し、ユーザーからの信頼を獲得する基盤づくり

持続可能で優しい技術の実装

人や環境、社会に悪影響を及ぼさない、持続可能なAI 技術の追求

責任あるAIへの向き合い方の可視化

企業ポリシーや理念に留まらず、国際的に認められる形でAI 倫理への取り組みを明示

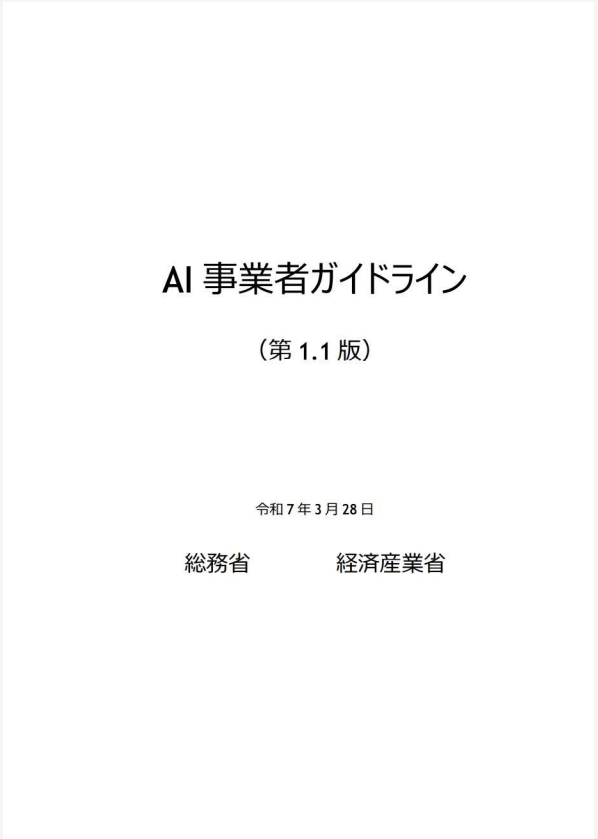
技術と倫理の架け橋

Godot が目指す「社会に受け入れられ、持続可能で多様性を包み込む技術」の具体的なリンクの一つ

Agenda

01	株式会社Godotの紹介
02	Godotが取得に至った理由
03	**AIMSのリスクベースアプローチ**
04	AIMSがGodotへもたらした効果
05	AIによるAIガバナンスの強化

AIMSのリスクベースアプローチ



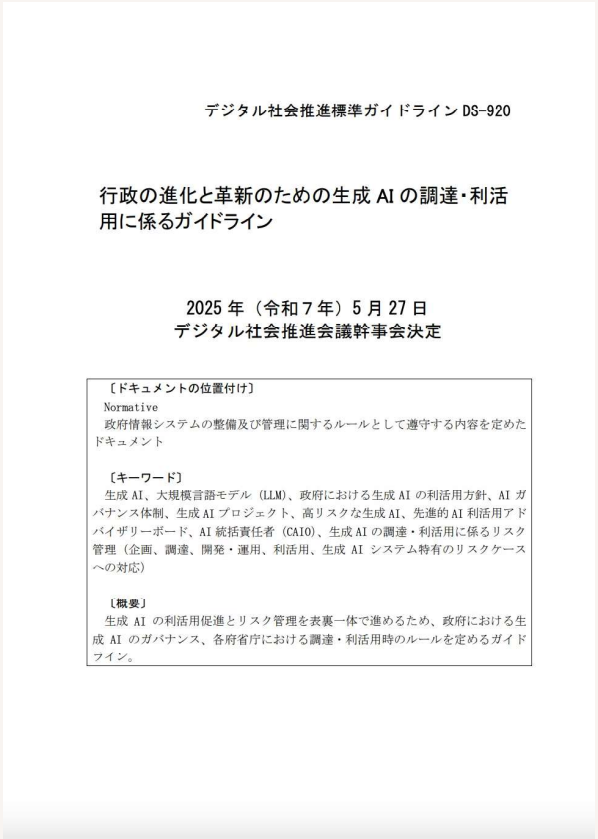
AI 事業者ガイドライン

（第 1.1 版）

令和 7 年 3 月 28 日

総務省　　経済産業省

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



デジタル社会推進標準ガイドライン DS-920

行政の進化と革新のための生成 AI の調達・利活用に係るガイドライン

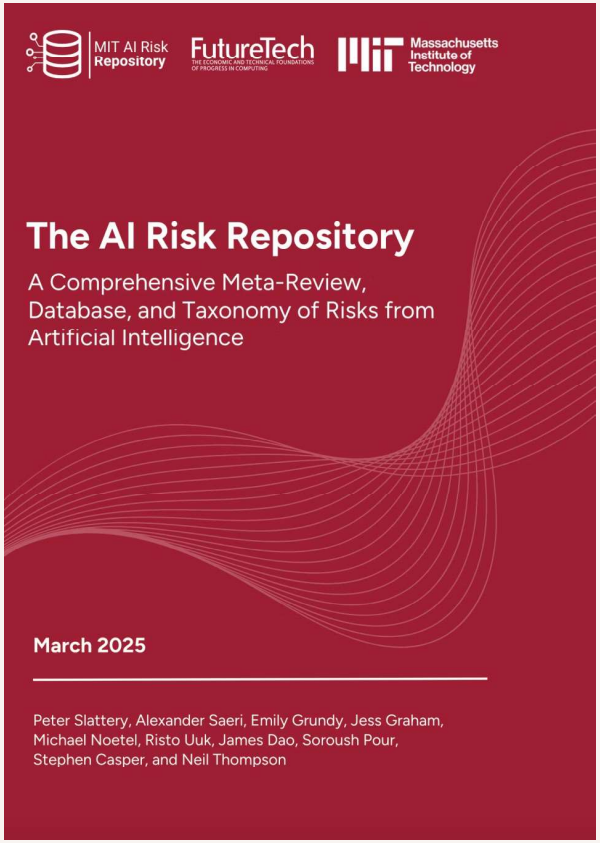
2025 年（令和 7 年）5 月 27 日
デジタル社会推進会議幹事会決定

〔ドキュメントの位置付け〕
Normative
政府情報システムの整備及び管理に関するルールとして遵守する内容を定めたドキュメント

〔キーワード〕
生成 AI、大規模言語モデル（LLM）、政府における生成 AI の利活用方針、AI ガバナンス体制、生成 AI プロジェクト、高リスクな生成 AI、先進的 AI 利活用アドバイザリーボード、AI 統括責任者（CAIO）、生成 AI の調達・利活用に係るリスク管理（企画、調達、開発・運用、利活用、生成 AI システム特有のリスクケースへの対応）

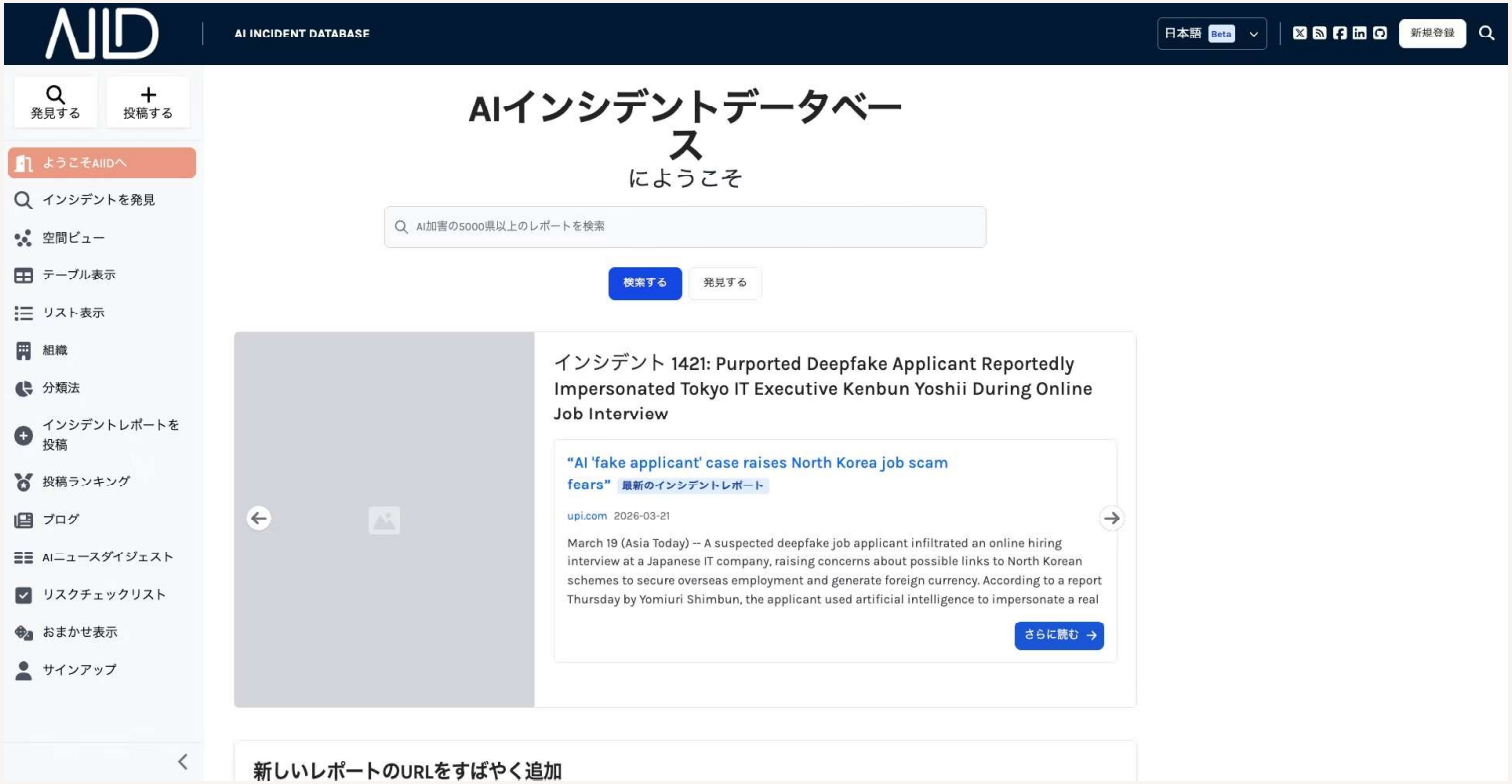
〔概要〕
生成 AI の利活用促進とリスク管理を表裏一体で進めるため、政府における生成 AI のガバナンス、各府省庁における調達・利活用時のルールを定めるガイドライン。

https://www.digital.go.jp/news/3579c42d-b11c-4756-b66e-3d3e35175623



https://airisk.mit.edu/

AIMSのリスクベースアプローチ



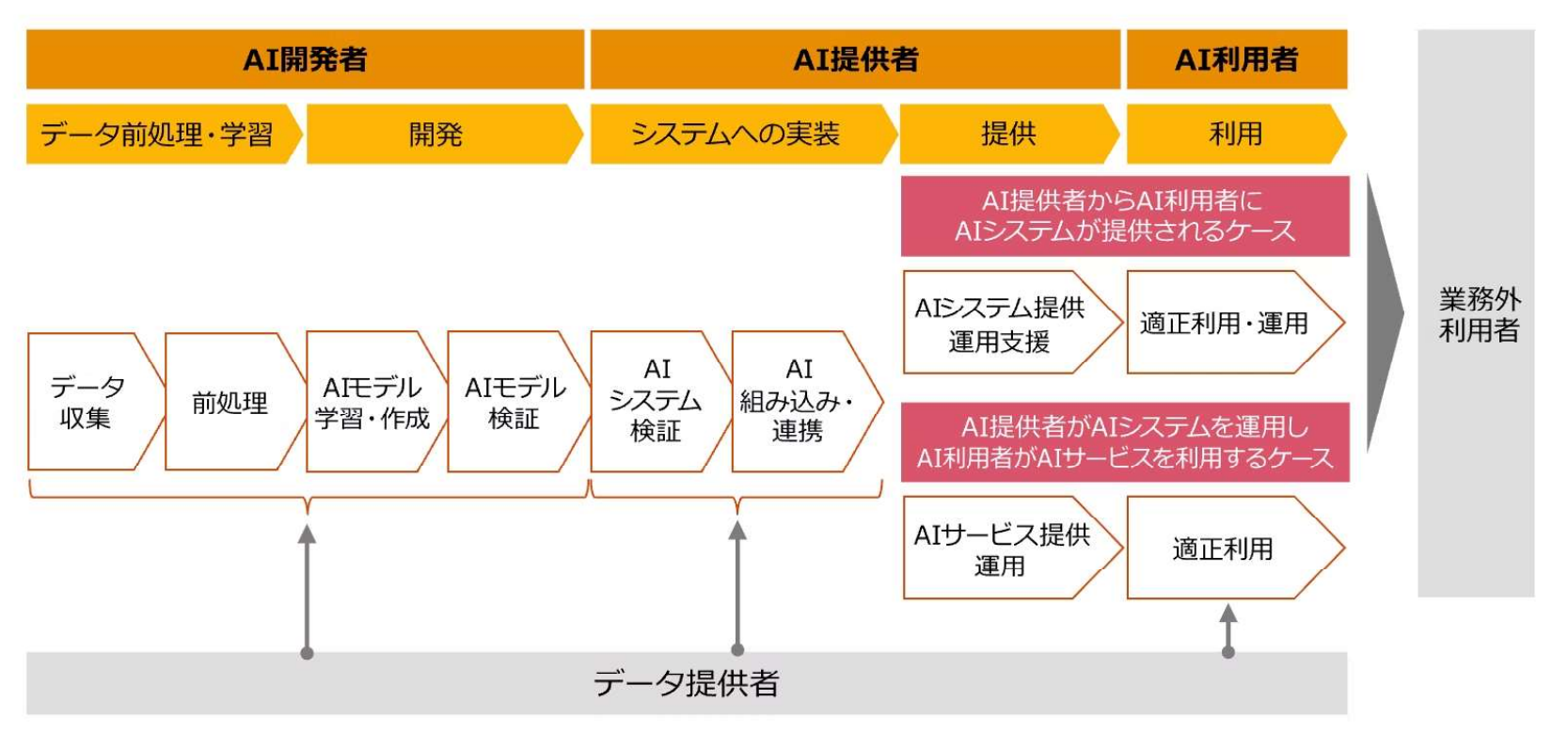
https://incidentdatabase.ai/ja/

AIMSのリスクベースアプローチ: 自社の役割

- 組織は、組織が開発、提供又は使用するAI システムの本来の目的を考慮し、これらのAI システムに関して自らの役割を決定しなければならない。
- 複数の役割を持つことはあり、役割に応じて考慮すべきリスクが異なる。
- 役割がAI顧客だけであってもAIMSの対象となる。

- **AI提供者**　：AIプラットフォームの提供者、AI製品やAIサービス提供者など
- **AIプロデューサー**　：AI開発者・設計者・オペレータ・テスト実施者、ドメイン専門家など
- **AI顧客**　：AI利用者

AIMSのリスクベースアプローチ: AI開発ライフサイクル

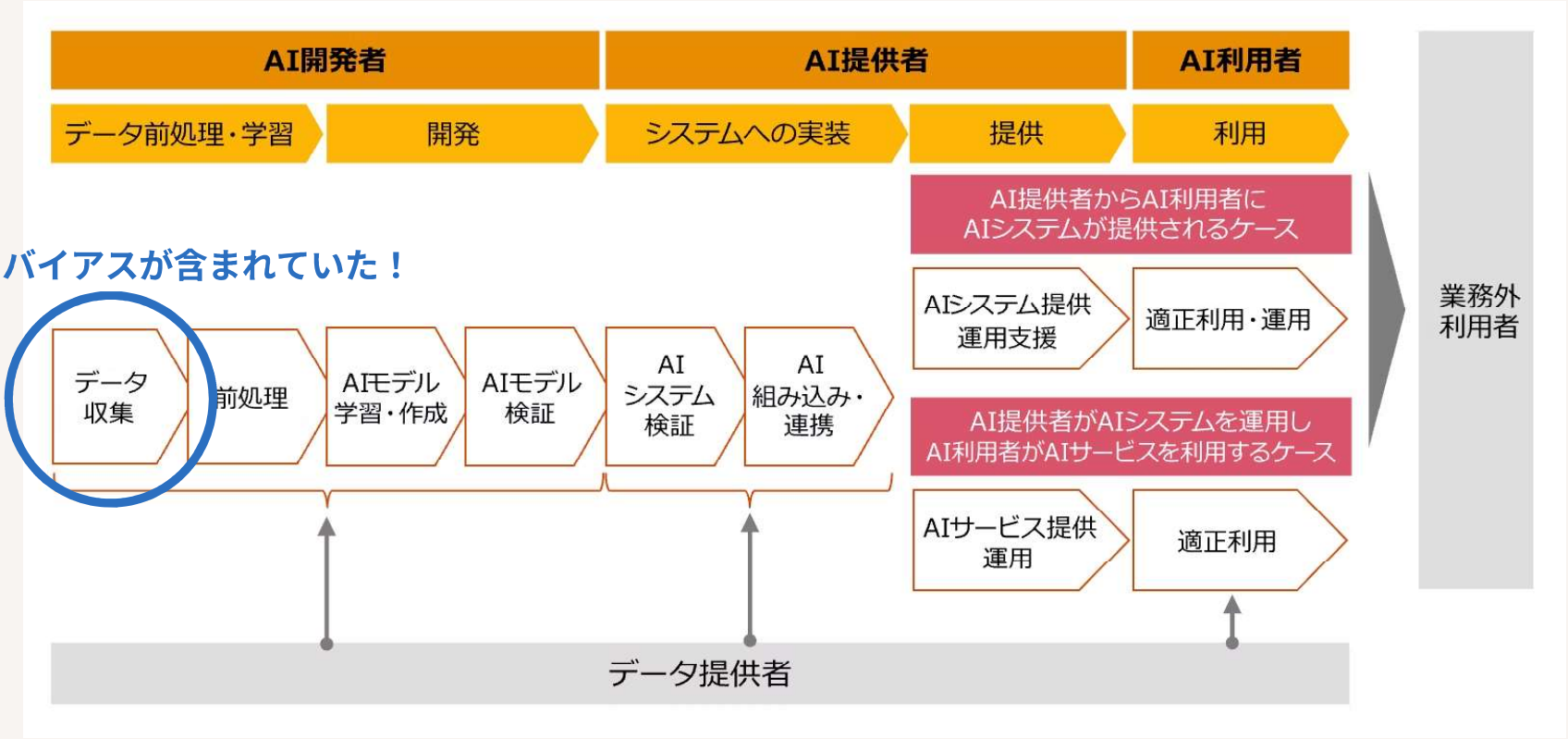


図の引用元

PwC 2024 『AIリスクをめぐる規制動向解説、日本企業はどのようにAIリスクと向きあうべきか』

https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/generative-ai-regulation11.html

AIMSのリスクベースアプローチ: AI開発ライフサイクル



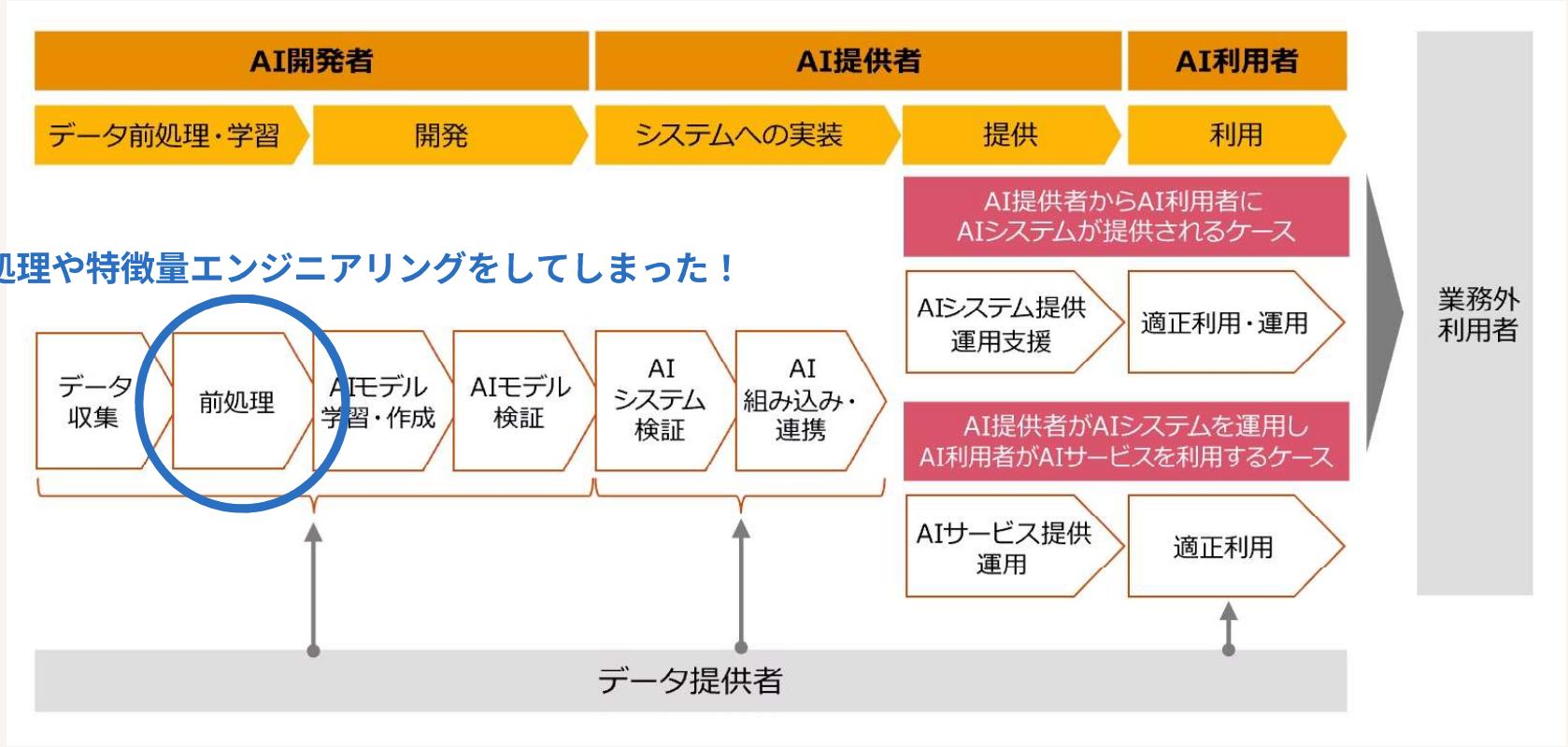
データにバイアスが含まれていた！

図の引用元

PwC 2024 『AIリスクをめぐる規制動向解説、日本企業はどのようにAIリスクと向きあうべきか』

https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/generative-ai-regulation11.html

AIMSのリスクベースアプローチ: AI開発ライフサイクル



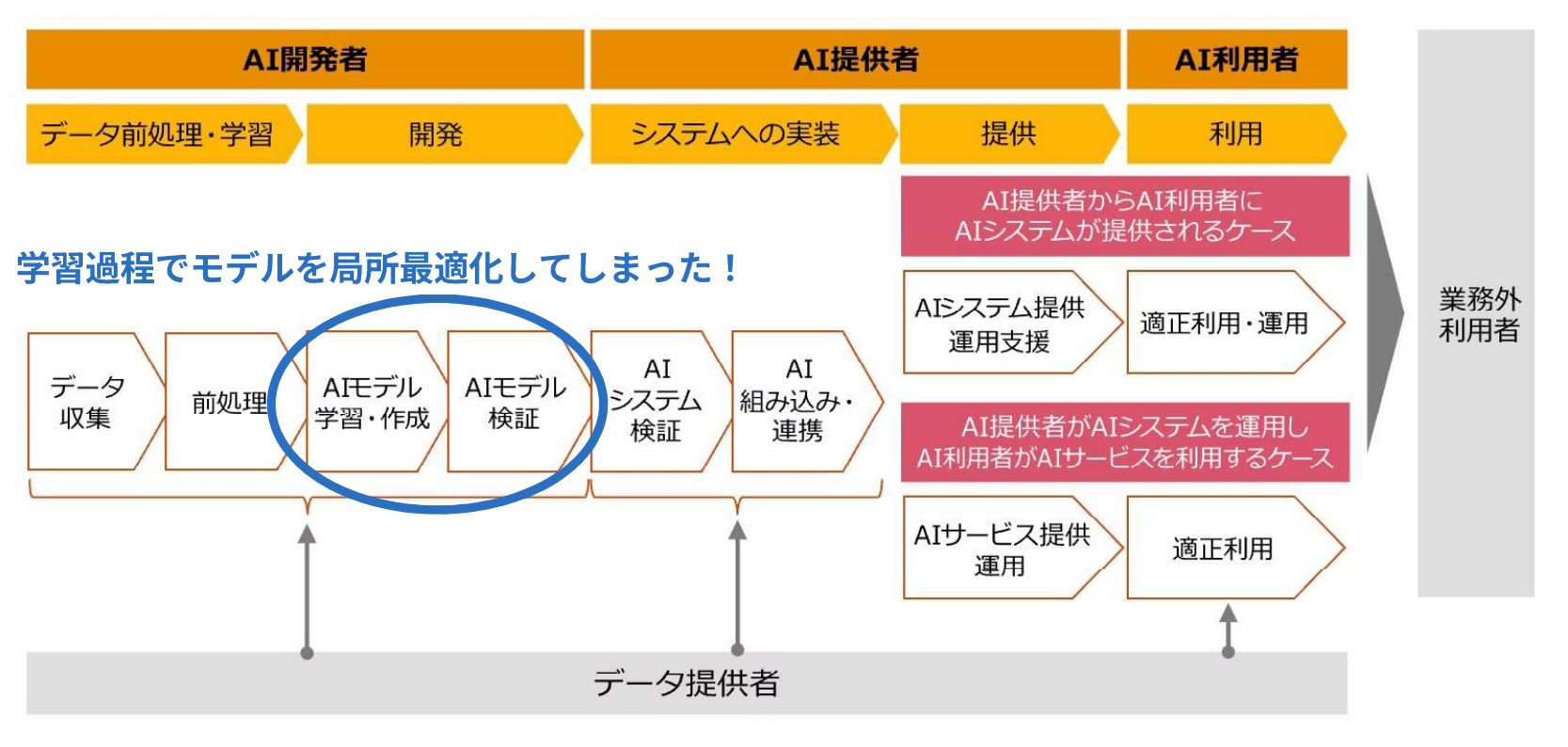
誤った前処理や特徴量エンジニアリングをしてしまった！

図の引用元

PwC 2024 『AIリスクをめぐる規制動向解説、日本企業はどのようにAIリスクと向きあうべきか』

https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/generative-ai-regulation11.html

AIMSのリスクベースアプローチ: AI開発ライフサイクル

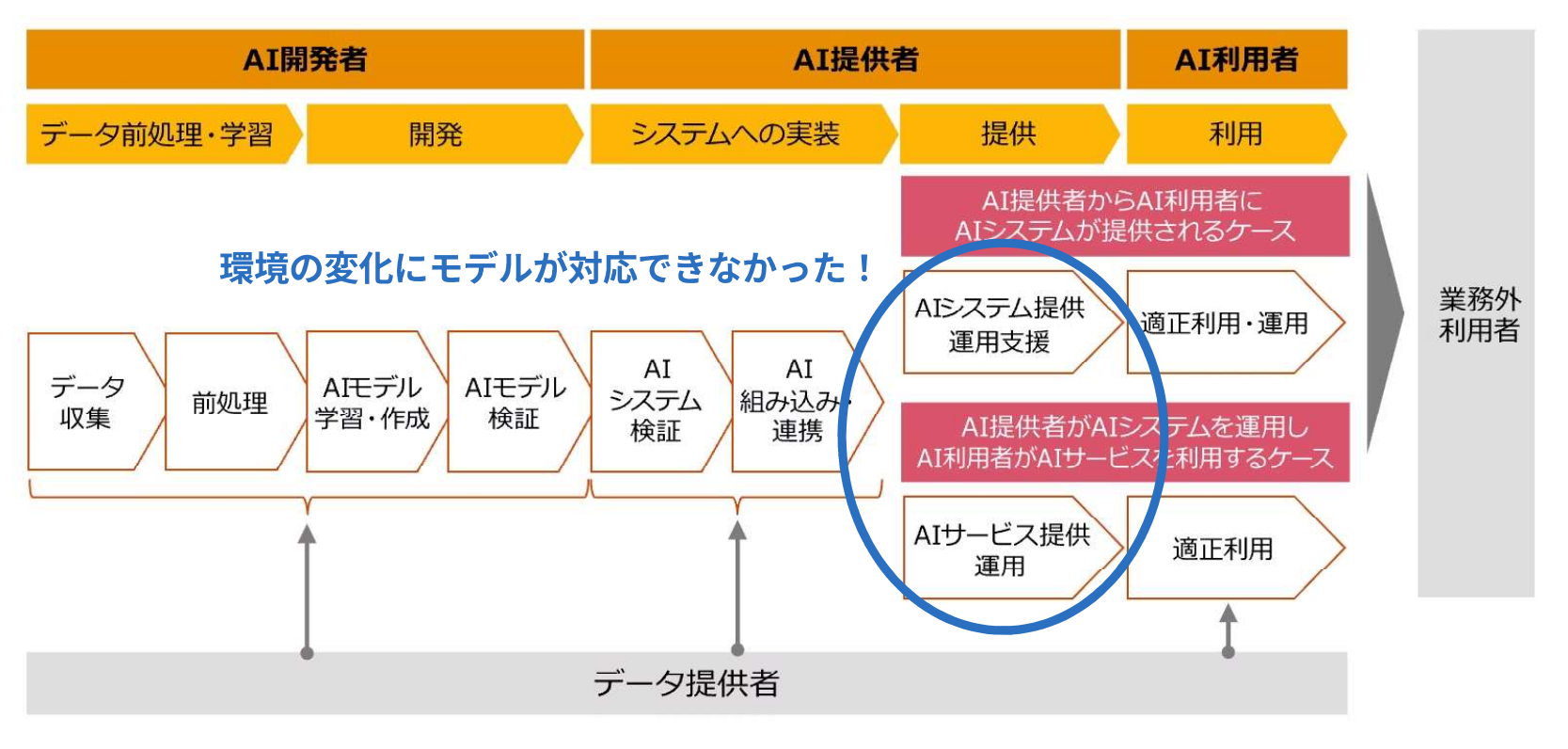


図の引用元

PwC 2024 『AIリスクをめぐる規制動向解説、日本企業はどのようにAIリスクと向きあうべきか』

https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/generative-ai-regulation11.html

AIMSのリスクベースアプローチ: AI開発ライフサイクル

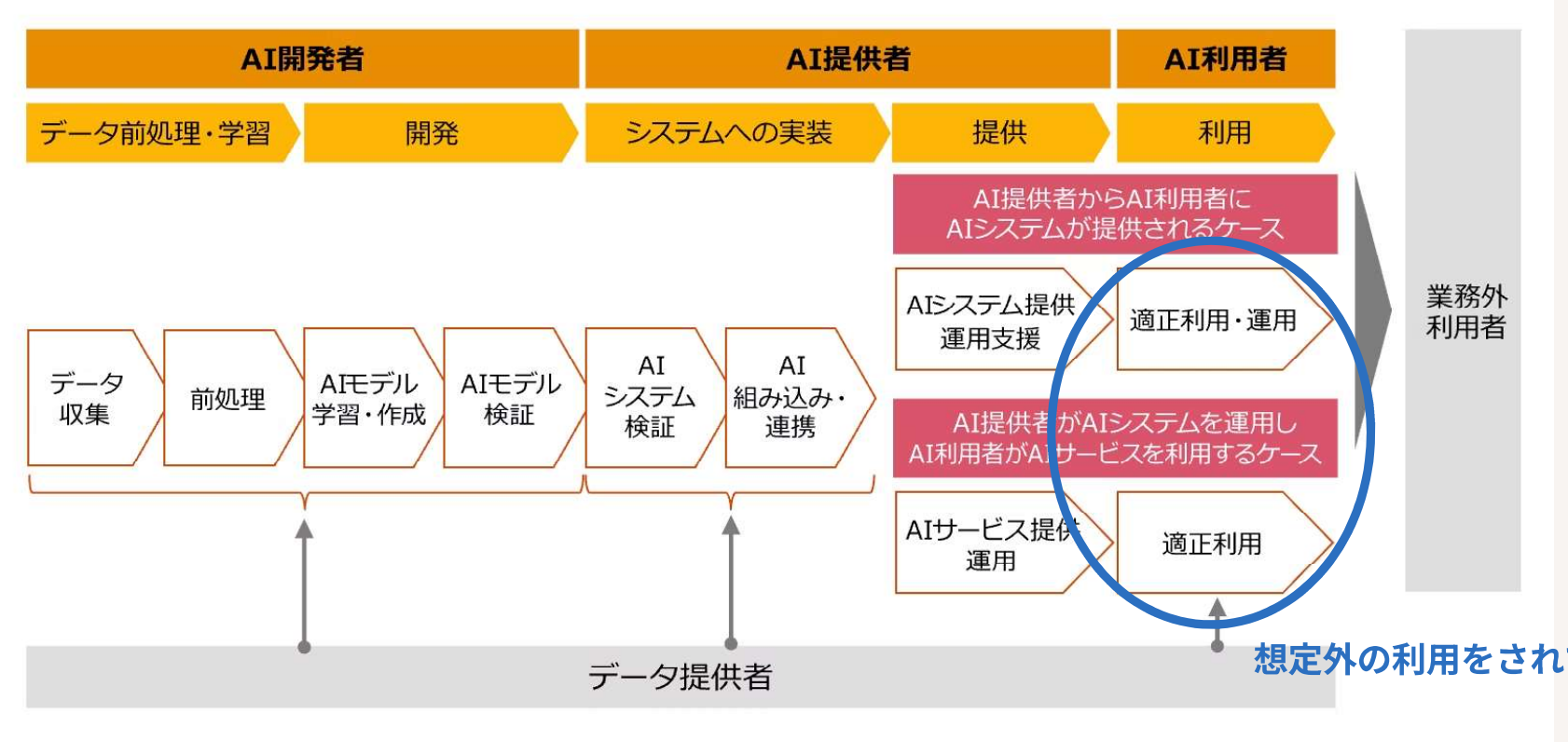


図の引用元

PwC 2024 『AIリスクをめぐる規制動向解説、日本企業はどのようにAIリスクと向きあうべきか』

https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/generative-ai-regulation11.html

AIMSのリスクベースアプローチ: AI開発ライフサイクル



図の引用元

PwC 2024 『AIリスクをめぐる規制動向解説、日本企業はどのようにAIリスクと向きあうべきか』

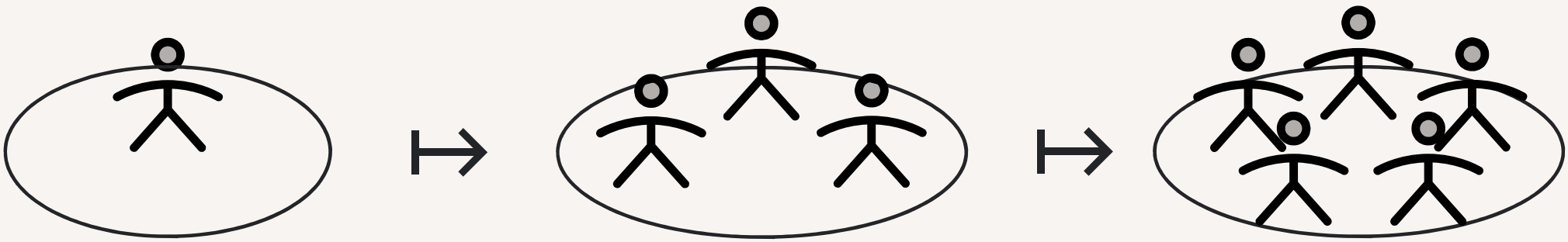
https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/generative-ai-regulation11.html

AIMSのリスクベースアプローチ: AIアセット分類によるリスク検討

AIアセットを分類することでリスクを管理しやすくする。

- **AIモデル**　：GPT系、Gemini系、Claude系などのクローズドモデルや、Llama系、Qwen系などのオープンモデル等
- **AIシステム**　：LLM等のAIを用いたアプリケーション・システム
- **AIデータ**　：AIモデルの学習・ファインチューニング、システム稼働のためのデータ
- **AIインフラ**　：AIモデルの学習・ファインチューニングのためのインフラ、AIシステムのインフラ
- **AIツール**　：ChatGPTやClaude、Vibe Coding等のAIツール

AIMSのリスクベースアプローチ: リスクと影響範囲



予見可能なAIシステムの誤用

個人、組織・コミュニティへの潜在的影響

社会への潜在的影響

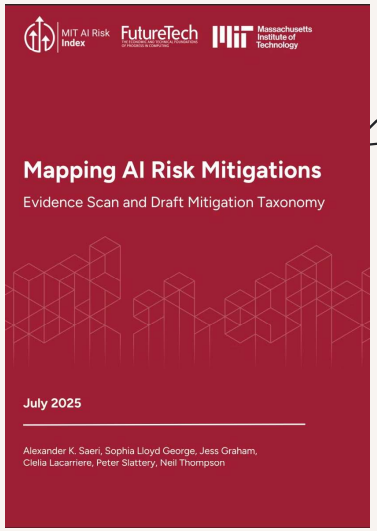
AIMSのリスクベースアプローチ: リスク検討

カテゴリ	利用対象者	AIシステム	システムの目的・意図	システムの達成目標	予見可能なAIシステムの誤用	個人、組織・コミュニティへの潜在的影響	社会への影響
利用	自社従業員	ChatGPT	社内業務効率の向上	ChatGPTを活用することで業務効率が向上し、顧客に対する提供価値を向上させること	誤情報や偽情報を活用してしまう	ビジネスの上の重要な意思決定の誤りによる経済的損失	世間の誤った認識の拡大
						当社への不信感の増加	メディア情報への信頼性低下

リスクスコア = 発生可能性 + 影響度

閾値以上の場合、リスク対応策を実施

AIMSのリスクベースアプローチ: リスク対応



https://airisk.mit.edu/blog/mapping-ai-risk-mitigations

Mitigation Category	Mitigation Subcategory
1. Governance & Oversight Controls *Formal organizational structures and policy frameworks that establish human oversight mechanisms and decision protocols to ensure human accountability, ethical conduct, and risk management throughout AI development and deployment.*	1.1 Board Structure & Oversight
	1.2 Risk Management
	1.3 Conflict of Interest Protections
	1.4 Whistleblower Reporting & Protection
	1.5 Safety Decision Frameworks
	1.6 Environmental Impact Management
	1.7 Societal Impact Assessment
2. Technical & Security Controls *Technical, physical, and engineering safeguards that secure AI systems and constrain model behaviors to ensure security, safety, alignment with human values, and content integrity.*	2.1 Model & Infrastructure Security
	2.2 Model Alignment
	2.3 Model Safety Engineering
	2.4 Content Safety Controls
3. Operational Process Controls *Processes and management frameworks governing AI system deployment, usage, monitoring, incident handling, and validation, which promote safety, security, and accountability throughout the system lifecycle.*	3.1 Testing & Auditing
	3.2 Data Governance
	3.3 Access Management
	3.4 Staged Deployment
	3.5 Post-Deployment Monitoring
	3.6 Incident Response & Recovery
4. Transparency & Accountability Controls *Formal disclosure practices and verification mechanisms that communicate AI system information and enable external scrutiny to build trust, facilitate oversight, and ensure accountability to users, regulators, and the public.*	4.1 System Documentation
	4.2 Risk Disclosure
	4.3 Incident Reporting
	4.4 Governance Disclosure
	4.5 Third-Party System Access
	4.6 User Rights & Recourse

参考にしつつ自社にあったリスク対応策を検討・実行する

AIMSのリスクベースアプローチ: リテラシー向上研修

AIMS認証取得後、運用1年を経て発展的なリテラシーの社内展開を開始。

1

AIの基礎

事業に関連するAIについての基本的な知識を身につける

2

ISO/IEC42001について

AIMSの国際規格リスクベースアプローチを理解する

3

AIリスクの基礎

AI開発ライフサイクルに沿ったAIリスクを理解する

4

生成AIのリスク

他のAIとは異なる生成AI固有のリスクを理解する

5

AIインシデント事例

AIにまつわるリスクを事例とともに理解する

6

AIMS内部監査の基礎

内部監査担当者向けの研修

エンジニア向け研修の一例

- LLMの継続事前学習
- LLMのファインチューニング
- LLMのデプロイメント

ビジネス向け研修の一例

- AIプロジェクトマネジメント
- 会社で取り扱うAI技術の概要
- 機械学習工学

Agenda

01	株式会社Godotの紹介
02	Godotが取得に至った理由
03	AIMSのリスクベースアプローチ
04	**AIMSがGodotへもたらした効果**
05	AIによるAIガバナンスの強化

AIMSがGodotへもたらした効果

認証取得はゴールではなく、Godot のAI システムが進むべき方向性を示すスタートライン。
取得動機を満たすことに加えて、3つの効果が見られた。

01

倫理的思考の文化醸成

制度的な正しさだけでなく、
社員一人ひとりが、「なぜ必要か？」「倫理的リスクはないか」を主体的に考える文化が醸成

02

問い続ける力の育成

問い続ける力を育むプロセスが、組織の競争力そのものに直結

03

自律的判断・対応力

社会や法規制の変化に合わせて自律的に判断・対応できるチームはどんな環境でも信頼され選ばれ続ける

Agenda

01	株式会社Godotの紹介
02	Godotが取得に至った理由
03	AIMSのリスクベースアプローチ
04	AIMSがGodotへもたらした効果
05	**AIによるAIガバナンスの強化**

AIによるAIガバナンスの強化

工数負荷大
→ 検討の抜け
漏れリスク

AS-IS

完全マニュアル

リスクの洗い出し → **リスクの評価** → **リスク対応策の検討・実施**

予見可能なAIシステムの誤用、個人、組織・コミュニティへの潜在的影響、社会への影響を洗い出す

発生可能性と影響度の高さをふまえてリスクを評価する

リスク評価の結果、必要な場合は対応策を検討し実行する

AIによるAIガバナンスの強化

工数負荷大
→ 検討の抜け
漏れリスク

AS-IS

完全マニュアル

リスクの洗い出し

予見可能なAIシステムの誤用、個人、組織・コミュニティへの潜在的影響、社会への影響を洗い出す

リスクの評価

発生可能性と影響度の高さをふまえてリスクを評価する

リスク対応策の検討・実施

リスク評価の結果、必要な場合は対応策を検討し実行する

AIによる効率化とHITLによる質の担保

TO-BE

AI Workflow

HITL

AIによるリスクの洗い出し

予見可能なAIシステムの誤用、個人、組織・コミュニティへの潜在的影響、社会への影響を洗い出す

人の確認

AIによるリスクの評価

発生可能性と影響度の高さをふまえてリスクを評価する

人の確認

AIによるリスク対応策の検討

リスク評価の結果、必要な場合は対応策を検討し実行する

人の確認・実行へ

GODOT

株式会社Godot