

# AIがもたらす光と影、その対応を考える

～AIに関する各国の動向～

デロイトトーマツサイバーセキュリティ先端研究所 神菌 雅紀  
2023年7月12日

< Confidential >

# 各種AI原則やガイドラインから実際のオペレーションまで落とし込まれた手順・手法等を準備し課題を整理していく必要があります

## 規制法案と課題の整理

### AIに関する 規制法案

#### 具体例

原則・  
ガイダンス

- OECD AI 原則
- G20 AI 原則
- 人間中心のAI 社会原則（日本）

How

ガイドライン・  
基準・法令

- AI 倫理ガイドライン（EU）
- AI 原則実践のためのガバナンス・ガイドライン（日本）
- AI規制法案（EU）

How

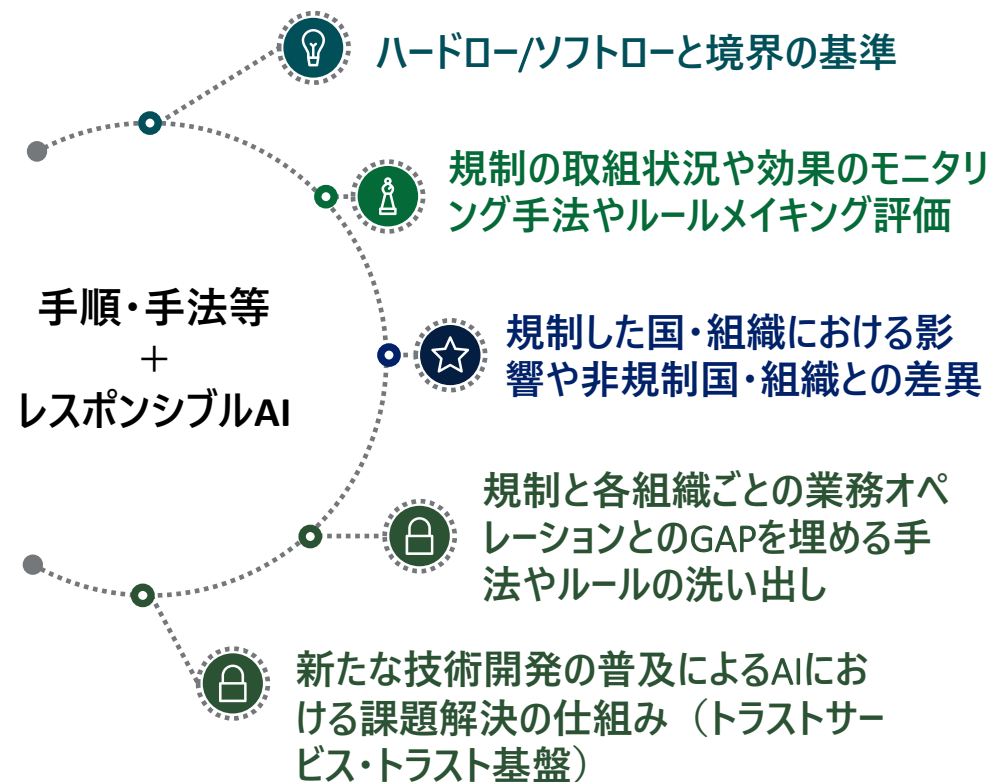
オペレーションに落とし  
込まれた手順・手法等

- AI モデルの透明性、信頼性を定量化するための仕組みやルール
- AI システムのセキュリティリスクを評価するための手法や技術
- AI の適切な監査と運用ルール
- AI生成物を検知する仕組みの実装

↑GAP

### 課題の整理

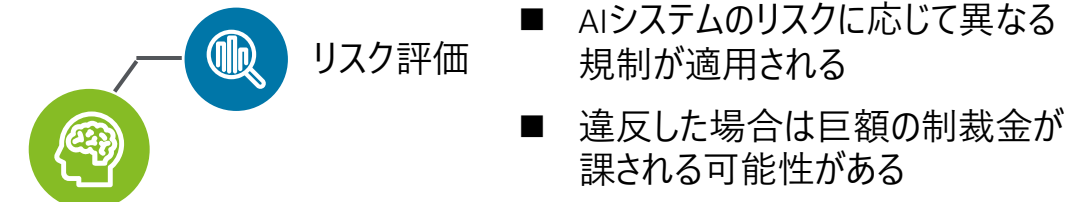
規制とオペレーションのGAPだけではなく、それぞれに対する課題も顕在化しています。それらを整理し解決に向けて進む必要があります。



# EUのAI ActのようにAIがレスポンスブルであることを要件とする動きが加速しており、そのために評価すべき項目についてルールを策定し、第三者が精査できる仕組み作りが重要となります。

## AI規制とAI評価の仕組み

### EU AI Act (AI 規制法案)



AI システム	リスク区分	制限	補足
分類	許容できない AI	利用禁止	潜在意識への操作や子供を相手とする搾取行為等を禁止
	ハイリスク AI	規制 →事前適合性評価の準拠が条件	評価は原則自社評価だが一部例外あり
	限定リスクを伴う AI	情報/透明性の義務を条件	相手がAIであることの通知やAIによる生成物であることの明示
	最小/リスクなし AI	規制なし	規制なし

➡ GDPRと同様に日本でも当該規制の影響を受ける場合がある

### Responsible AIと評価

- AIシステムに求められる要件
    - AI Actでも見られるように、AIシステムの要件として透明性や説明責任 (Responsible AI/責任あるAI) が強く求められるようになってきています。
    - AIの開発者・サービスプロバイダは、AIシステムやサービスに求められる透明性や説明可能性、安全性等の要件が第三者によって評価できるような仕組み (ルール) を整えていく必要があります。
- ▼
- ResponsibleなAIに関連する動向
    - 一部のプラットフォームやテック企業は自社のHPで責任あるAIの取り組みに関するポリシー等を公開しています。  
ex) google : <https://cloud.google.com/responsible-ai>
    - スタンフォード大学の基盤モデル研究センター(CRFM)は、主要な基盤モデルがEU AI Actで求められる要件を満たしているかを評価し、その結果を公表しています。

# スタンフォード大学の調査ではテック企業10社の基盤モデルがEU AI Act (AI規制法案)の要件を満たすかを評価した結果、現段階では多くのモデルがEU AI Actに準拠できていませんでした

## EU AI Actへの準拠の状況

評価項目 (12項目)	OpenAI	cohere	stability.ai	ANTHROPIC	Google	BigScience	Meta	AI21 labs	ALEPH ALPHA	ELEutherAI	Totals
Draft AI Act Requirements	GPT-4	Cohere Command	Stable Diffusion v2	Claude	PaLM 2	BLOOM	LLaMA	Jurassic-2	Luminous	GPT-NeoX	
Data sources	● ○ ○ ○	● ● ● ○	● ● ● ●	○ ○ ○ ○	● ● ○ ○	● ● ● ●	● ● ● ●	○ ○ ○ ○	○ ○ ○ ○	● ● ● ●	22
Data governance	● ● ○ ○	● ● ● ○	● ● ○ ○	○ ○ ○ ○	● ● ● ○	● ● ● ●	● ● ○ ○	○ ○ ○ ○	○ ○ ○ ○	● ● ● ○	19
Copyrighted data	○ ○ ○ ○	○ ○ ○ ○	○ ○ ○ ○	○ ○ ○ ○	○ ○ ○ ○	● ● ● ○	○ ○ ○ ○	○ ○ ○ ○	○ ○ ○ ○	● ● ● ●	7
Compute	○ ○ ○ ○	○ ○ ○ ○	● ● ● ●	○ ○ ○ ○	○ ○ ○ ○	● ● ● ●	● ● ● ●	○ ○ ○ ○	● ○ ○ ○	● ● ● ●	17
Energy	○ ○ ○ ○	● ○ ○ ○	● ● ● ○	○ ○ ○ ○	○ ○ ○ ○	● ● ● ●	● ● ● ●	○ ○ ○ ○	○ ○ ○ ○	● ● ● ●	16
Capabilities & limitations	● ● ● ●	● ● ● ○	● ● ● ●	● ○ ○ ○	● ● ● ●	● ● ● ○	● ● ○ ○	● ● ○ ○	● ○ ○ ○	● ● ● ○	27
Risks & mitigations	● ● ● ○	● ● ○ ○	● ○ ○ ○	● ○ ○ ○	● ● ● ○	● ● ○ ○	● ○ ○ ○	● ● ○ ○	○ ○ ○ ○	● ○ ○ ○	16
Evaluations	● ● ● ●	● ● ○ ○	○ ○ ○ ○	○ ○ ○ ○	● ● ○ ○	● ● ○ ○	● ● ○ ○	○ ○ ○ ○	● ○ ○ ○	● ○ ○ ○	15
Testing	● ● ● ○	● ● ○ ○	○ ○ ○ ○	○ ○ ○ ○	● ● ○ ○	● ● ○ ○	○ ○ ○ ○	● ○ ○ ○	○ ○ ○ ○	○ ○ ○ ○	10
Machine-generated content	● ● ● ○	● ● ● ○	○ ○ ○ ○	● ● ● ○	● ● ● ○	● ● ● ○	○ ○ ○ ○	● ● ● ○	● ○ ○ ○	● ● ● ○	21
Member states	● ● ○ ○	○ ○ ○ ○	○ ○ ○ ○	● ● ○ ○	● ● ● ●	○ ○ ○ ○	○ ○ ○ ○	○ ○ ○ ○	● ○ ○ ○	○ ○ ○ ○	9
Downstream documentation	● ● ● ○	● ● ● ●	● ● ● ●	○ ○ ○ ○	● ● ● ●	● ● ● ●	● ● ○ ○	○ ○ ○ ○	○ ○ ○ ○	● ● ● ○	24
Totals	25 / 48	23 / 48	22 / 48	7 / 48	27 / 48	36 / 48	21 / 48	8 / 48	5 / 48	29 / 48	

Max
Min

出所：スタンフォード大学の基盤モデル研究センター(CRFM)「Do Foundation Model Providers Comply with the Draft EU AI Act?」

# Deloitte.

## デロイト トーマツ

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイト ネットワークのメンバーであるデロイト トーマツ 合同会社ならびにそのグループ法人（有限責任監査法人 トーマツ、デロイト トーマツ コンサルティング 合同会社、デロイト トーマツ ファイナンシャル アドバイザリー 合同会社、デロイト トーマツ 税理士 法人、DT 弁護士 法人およびデロイト トーマツ グループ 合同会社を含む）の総称です。デロイト トーマツ グループは、日本で最大級のプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスク アドバイザリー、コンサルティング、ファイナンシャル アドバイザリー、税務、法務等を提供しています。また、国内約30都市に約1万7千名の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループ Web サイト（[www.deloitte.com/jp](http://www.deloitte.com/jp)）をご覧ください。

Deloitte（デロイト）とは、デロイト トウシュート マツ リミテッド（“DTTL”）、そのグローバル ネットワーク 組織を構成するメンバー ファーム およびそれらの関係法人（総称して“デロイト ネットワーク”）のひとつまたは複数を指します。DTTL（または“Deloitte Global”）ならびに各メンバー ファーム および関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。DTTL および DTTL の各メンバー ファーム ならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファーム または関係法人の作為および不作為について責任を負うものではありません。DTTL はクライアントへのサービス提供を行いません。詳細は [www.deloitte.com/jp/about](http://www.deloitte.com/jp/about) をご覧ください。デロイト アジア パシフィック リミテッドは DTTL のメンバー ファーム であり、保証有限責任会社です。デロイト アジア パシフィック リミテッドのメンバー およびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィック における100を超える都市（オークランド、バンコク、北京、ベンガルール、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、ムンバイ、ニューデリー、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、監査・保証業務、コンサルティング、ファイナンシャル アドバイザリー、リスク アドバイザリー、税務、法務などに関連する最先端のサービスを、Fortune Global 500® の約9割の企業や多数のプライベート（非公開）企業を含むクライアントに提供しています。デロイトは、資本市場に対する社会的な信頼を高め、クライアントの変革と繁栄を促し、より豊かな経済、公正な社会、持続可能な世界の実現に向けて自ら率先して取り組むことを通じて、計測可能で継続性のある成果をもたらすプロフェッショナルの集団です。デロイトは、創設以来175年余りの歴史を有し、150を超える国・地域にわたって活動を展開しています。“Making an impact that matters”をパーパス（存在理由）として標榜するデロイトの約415,000名の人材の活動の詳細については、（[www.deloitte.com](http://www.deloitte.com)）をご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、DTTL、そのグローバル ネットワーク 組織を構成するメンバー ファーム およびそれらの関係法人が本資料をもって専門的な助言やサービスを提供するものではありません。皆様の財務または事業に影響を与えるような意思決定または行動をされる前に、適切な専門家にご相談ください。本資料における情報の正確性や完全性に関して、いかなる表明、保証または確約（明示・黙示を問いません）をするものではありません。またDTTL、そのメンバー ファーム、関係法人、社員・職員または代理人のいずれも、本資料に依拠した人に関して直接または間接に発生したいかなる損失および損害に対して責任を負いません。



IS 669126 / ISO 27001



BCMS 764479 / ISO 22301

Member of  
Deloitte Touche Tohmatsu Limited