

# ブリュッセル効果への対応 **[第4回]** 日本企業はEU-AI法にどう備えるべきか

2025年5月12日(月) 17:30-18:30

【プログラム】

17:30-17:35 開会挨拶：飯田陽一（総務省）

17:35-18:00 公開アンケートの概要と日本企業が留意すべき対応の要点：  
工藤郁子（大阪大学）  
実積寿也（中央大学）

18:00-18:30 パネルディスカッションとQ&A  
パネリスト：  
工藤郁子（大阪大学）  
実積寿也（中央大学）  
根本宗記（NTT）  
大野健太（Preferred Networks）  
吉永和弘（NEC）  
司会：江間有沙（東京大学東京カレッジ）



ブリュッセル効果への対応：日本企業はEU-AI法にどう備えるべきか4  
**EU AI法とCoP、そして新たなガイドライン**

大阪大学 社会技術共創研究センター 特任准教授  
工藤郁子

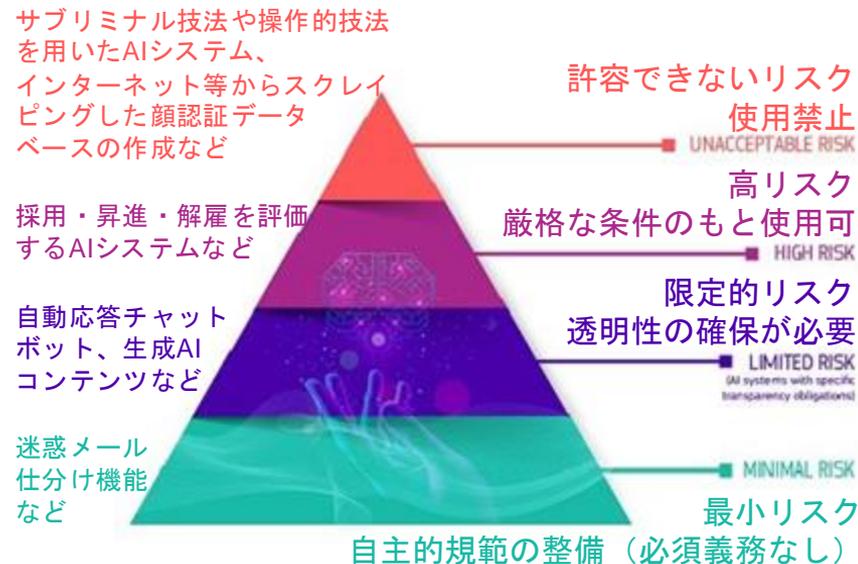
2025年5月12日



# EU AI法

本セミナー第2回  
報告資料より再掲

- ハードロー：世界で初めて包括的にAIを規制する法律
- リスクベースアプローチ：リスクの大きさに合わせた対応（右図参照）
  - 「リスク」とは、害が発生する確率とその害の重大性の組み合わせ(3条2号)
- 域外適用：日本企業も対象になりうる
  - EU域内で、AIシステムを市場投入、サービス提供している、または汎用目的AIモデルを市場投入しているプロバイダー（EUに所在しているかは問わない）（2条1項(a)）
  - アウトプットがEU域内で利用される場合、第三国に所在するAIシステムのプロバイダー及びデプロイヤー（2条1項(c)）
- 違反には多額の罰金（99～101条）

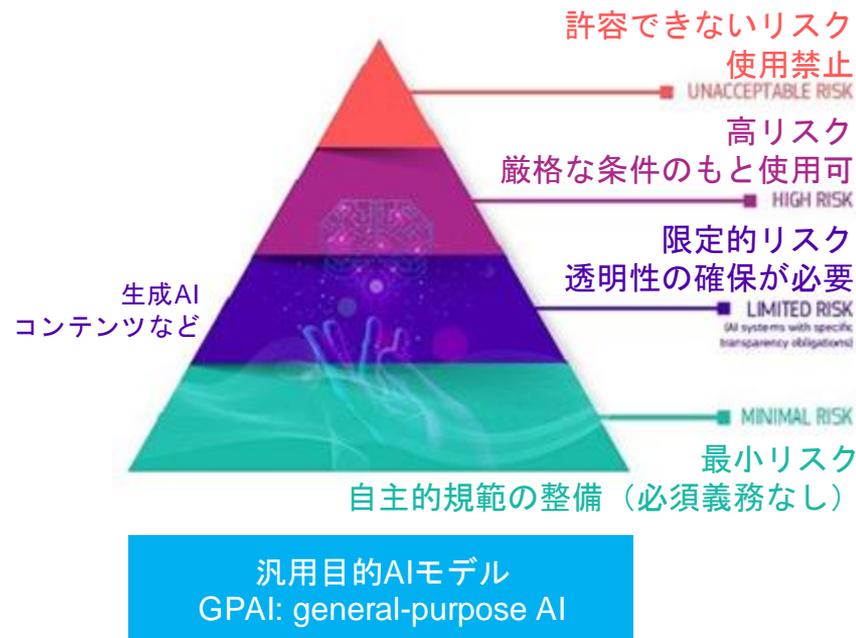


EUのウェブサイトの資料をもとに発表者作成  
<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

# EU AI法：汎用目的AIモデル

本セミナー第2回  
報告資料より再掲

- 4つのリスク類型に加えて、**汎用目的AI (GPAI: general-purpose AI) モデル**も別枠で規制
  - 生成AIのモデル等 (not 生成AIが出力したコンテンツ)
  - 経緯：2021年4月の法案公開後、2022年11月以降のChat GPT等の普及を受けて軌道修正
- 汎用目的AIモデル：顕著な汎用性を示し、多様で独立したタスクを適切に実行する能力を持ち、様々な下流のシステムやアプリケーションに統合可能なAIモデル (3条63号)
  - 「大量のデータを用いて学習されたAIモデルを含む」  
(が、それに限られないと解釈可能な文言)
  - 市場投入前の研究開発やプロトタイプ活動のために使用されるAIモデルは除外



EUのウェブサイトの資料をもとに発表者作成  
<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

# EU AI法：汎用目的AIモデル

本セミナー第2回  
報告資料より再掲(一部更新)

- 特定の条件を満たす汎用目的AIモデルは、「**システミックリスク**」があると見なされ義務が加重される

- システミックリスクは、例えば、化学兵器や生物兵器の開発障壁の低下、自律型汎用AIモデルに対する制御不能、有害な差別や偽情報の大規模化などを想定（前文110）

- システミックリスクの有無は適切な手法で判断されるとされ
- (1) **学習の累積計算量がFLOPで10の25乗より大きい場合は有と推定されることに加え（51条2項）**
- (2) EU当局による指定もある

システミックリスクが <b>ない</b> 場合の汎用目的AIモデルに関する義務（53条）	システミックリスクが <b>ある</b> 場合の汎用目的AIモデルに関する義務（55条）
<ul style="list-style-type: none"> <li>当局への情報提供（技術文書）</li> <li>下流プロバイダーへの情報提供</li> <li>EU著作権法遵守ポリシーの策定</li> </ul> <p>など</p>	<ul style="list-style-type: none"> <li><b>53条の義務に加えて</b></li> <li>標準化されたプロトコルによるモデル評価</li> <li>システミックリスクのアセスメントとリスク低減措置実施</li> <li>インシデント発生時における当局への報告</li> <li>サイバーセキュリティに関する保護措置の実施</li> </ul> <p>など</p>

# EU AI法とCoP

本セミナー第2回  
報告資料より再掲(一部更新)

- 汎用目的AIモデルについて「行動規範（Codes of Practice: **CoP**）」と呼ばれるガイドラインを策定（56条）
  - 法解釈を具体化するもので法的拘束力はないが、CoPへの準拠は、AI法への準拠を実証する手段となる（AI法への適合の推定ではない）
  - なお、ハイリスクAIなどを対象とする「CoC: Code of Conduct」（95条）とは別
  - さらにちなみに、G7日本議長国の下で始動した広島AIプロセスで策定されたのは「Code of Conduct」
- CoPは、マルチステークホルダー協議を経て、2025年5月までに策定予定**だった**
  - CoPの策定に参画するマルチステークホルダーは、2024年8月25日までEU内外から公募（現在は受付終了）  
**日本からの参加者はごく少数**：実積寿也（中央大学）、根本宗記（NTT）、工藤郁子（大阪大学）など？
- 2025年4月22日、汎用目的AIモデルに関する**CoPとは別のガイドライン案**（Commission Guidelines to Clarify the Scope of the General-purpose AI Rules in the AI）が公表され、5月22日まで意見公募中
  - 今回は誰でも意見提出可能！**

# 日本企業への影響

本セミナー第3回  
報告資料より再掲(一部更新)

- ・ 汎用目的AIモデルに関するルールは、日本企業にも影響
  - ・ 間接：開発受託をする場合、取引先から、開示義務の対象となる情報の提供や文書作成について協力を要請される可能性
  - ・ 直接：既存の汎用目的AIモデルを調整・ファインチューニングした主体が、新しいモデルのプロバイダーとして位置付けられる可能性あり（EU AI OfficeによるFAQ\*参照）
    - ・ CoPを起草する有識者チームは、ファインチューニング等によって新たに許容できないリスクが生じる可能性がないのであれば、義務の対象外とすべきと提言
    - ・ EU AI Office が本問題に関するガイドラインを近日中に公開することを期待すると述べていた
- CoPでは管轄外とされてきた問題が、**現在意見公募中のガイドライン**で整理される予定

\* <https://digital-strategy.ec.europa.eu/en/faqs/general-purpose-ai-models-ai-act-questions-answers>

# CoPと今回のガイドライン

## EU AI法：汎用目的AIモデルに関する条文

- ・ 汎用目的AIモデルの定義
- ・ システミックリスクがない場合の義務：透明性・著作権
- ・ 汎用目的AIモデルのうち、システミックリスクがあると推定する基準（閾値）：累積計算量がFLOPで10の25乗
- ・ システミックリスクがある場合の義務：リスク管理

など

など

## 意見公募中のガイドライン案

- ・ 汎用目的AIモデルの「汎用」とは？
- ・ 汎用目的AIモデルと推定する閾値：FLOPで10の22乗
- ・ 汎用目的AIモデルを調整・ファインチューニングした者はどのような場合に「プロバイダー」になる？
- ・ 学習や調整の「累積計算量」は、どう算出する？
- ・ 「市場投入」とは？オープンソースの適用除外を受けられるのはどのような場合？

など

## CoP草案（過去のセミナーで情報提供）

- ・ 透明性に関する技術文書作成のためのテンプレート
- ・ 安全性・セキュリティのフレームワークの策定手順
- ・ 事前のリスク評価、事後のモニタリングの手法

など

# 参考：EUで何が起きている？

本セミナー第3回  
報告資料より再掲(一部更新)

- ・ **国際競争力の強化のためのAI規制の見直し？**
- ・ 「ドラギレポート」の規制の簡素化 (simplify EU rules) 提言
  - ・ フォンデアライエン欧州委員長も受入れの姿勢
  - ・ 2025年2月、AI民事責任指令 (AI liability directive) 廃案
- ・ 2025年2月「AI Action Summit」での徴候
  - ・ マクロン仏大統領がインタビューで規制簡素化を主張
  - ・ ヴァンス米副大統領のAI規制批判
  - ・ 英米の共同声明署名拒否、英AISIの名称変更 (Safety → Security)
- ・ 2025年4月、**米国政府がCoP等の撤回を要請**
- ・ とはいえ、**AI法は発効済みで大きな方針変更は(でき)ない**



欧州は「AIの競争に参加していない」、マクロン仏大統領が危機感



via <https://news.ntv.co.jp/category/international/54c53a4ba3004af2aa1b1a3edfd0e565>  
<https://www.cnn.co.jp/world/35229256.html>

# 意見提出時のコツ

- ・ 今回は（法学や経済学の研究者というより）ビジネスやエンジニア視点からのフィードバックが有意義な場面ではないか
- ・ CoP草案のときの感触からすると、提出した意見は（意外なくらい）反映される
  - ・ ただし、AI法の条文については変更至難：「10の25乗」はすぐには変えられないが「10の22乗」は変更余地あり
- ・ 文言解釈上の疑問を尋ねるのではなく、「～とある箇所は…という趣旨だと理解したが、XXXの観点からは〇〇とすべき」などと具体的に提案するとよい

via <https://digital-strategy.ec.europa.eu/en/news/commission-seeks-input-clarify-rules-general-purpose-ai-models>

## Annex

### A.1. Compute used for training of models with approximately one billion parameters

The preliminary proposal for the threshold for a model to qualify as a general-purpose AI model proposed in Section 3.1.1 has been informed by the estimated amount of compute used in practice to train widely used models with approximately one billion parameters. While we do not refer to the models and their providers by name, we share the information relevant to our preliminary estimate in the following. The estimate is based on four models:

- Model A (a language model with 1.1 billion parameters):  $2 \cdot 10^{22}$  FLOP.
- Model B (a language model with 1 billion parameters):  $3 \cdot 10^{21}$  FLOP.
- Model C (a language model with 3.8 billion parameters):  $7.5 \cdot 10^{22}$  FLOP.
- Model D (an image diffusion model with 1 billion parameters):  $1.2 \cdot 10^{23}$  FLOP.

The above values have been obtained via the following calculations, which also serve to illustrate the two estimation methods described in Section 3.3.1.

#### **Model A:**

*Architecture-based approach:* Model A is a language model based on a transformer decode architecture with 1.1 billion parameters, trained on 3 trillion tokens. Applying the approximate formula for the training compute  $C$  from Section 3.4.1 yields

$$C \approx 6PD = 6 \cdot 1.1 \cdot 10^9 \cdot 3 \cdot 10^{12} = 1.98 \cdot 10^{22} \text{ FLOP}$$

*Hardware-based approach:* Model A's documentation also mentions that it took 3456 GPU hours to train it on 300B tokens using A100 GPUs, which implies 35,000 GPU hours for the full training run given the model was trained on 3 trillion tokens. This implies:

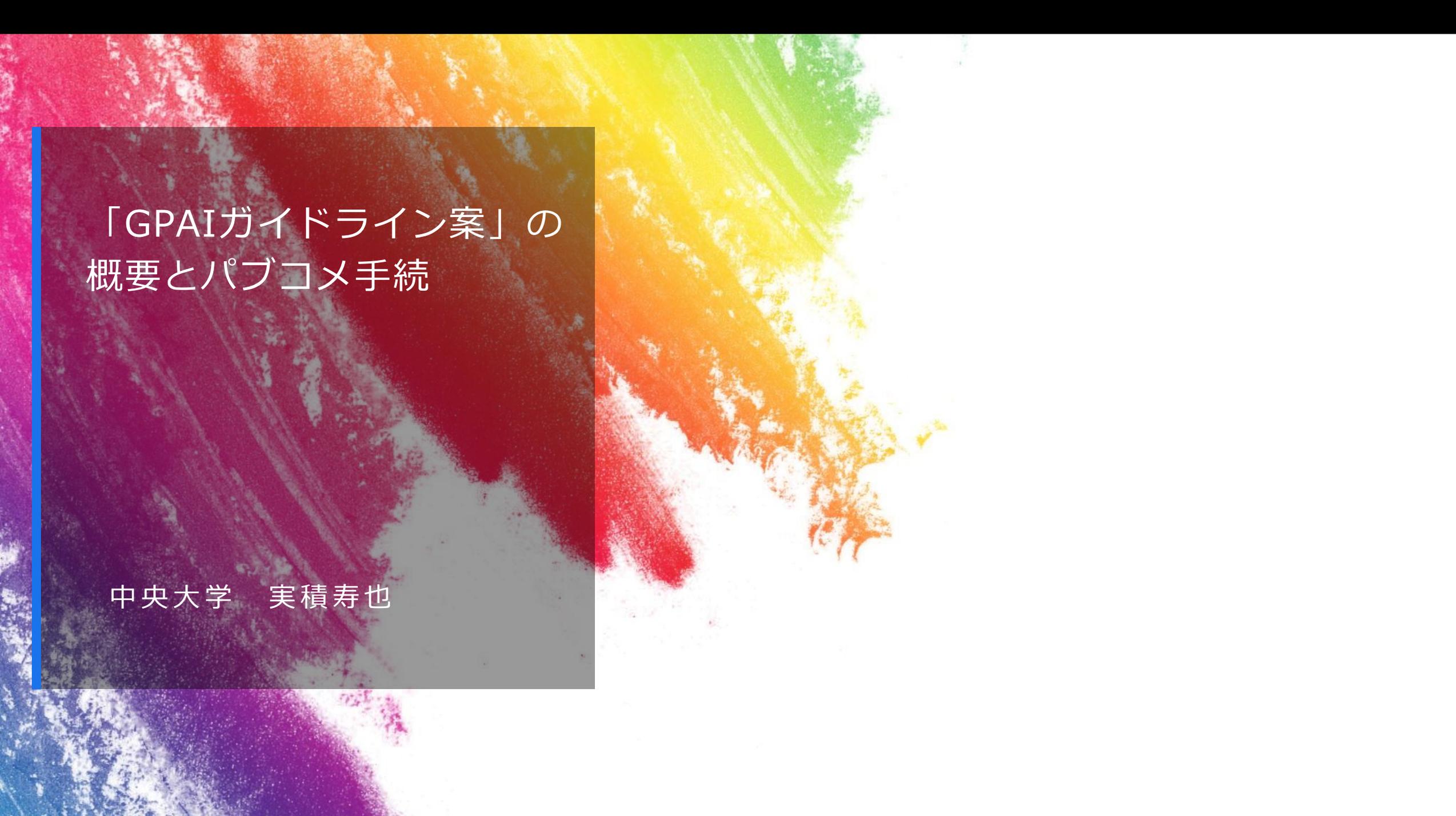
- a product  $NL$  of number of GPUs  $N$  and total training duration of  $L$  equal to  $NL = 35,000 \cdot 3,600$  seconds;
- a peak performance per GPU of  $H = 300 \cdot 10^{12}$  FLOP/second as per the NVIDIA A100 datasheet;<sup>6</sup>
- a GPU utilization of  $U = 56\%$  as indicated in model's documentation.

Using the hardware-based approach in Section 3.4.1, the total compute is then given by

$$C = N \cdot L \cdot H \cdot U \approx 2.1 \cdot 10^{22} \text{ FLOP}$$



Thanks!

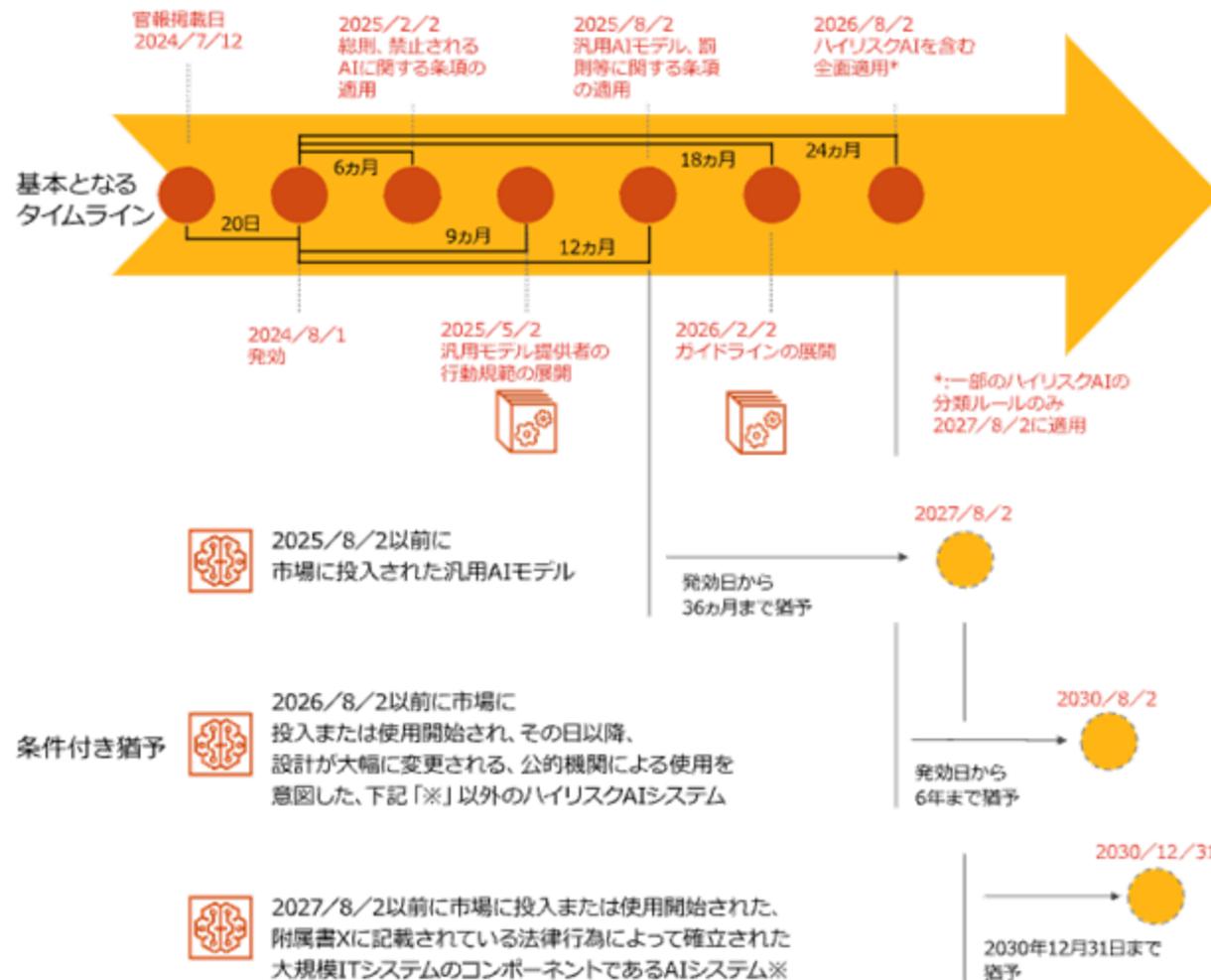


# 「GPAIガイドライン案」の 概要とパブコメ手続

中央大学 実積寿也

# EU AI法とパブリックコメントの背景

- EU AI法の適用開始：
  - 2025年8月に施行（Regulation (EU) 2024/1689）
  - 特に汎用AIモデル（GPAI）への新たな義務が導入される
- ガイドラインに係るパブコメの目的：
  - 2025年8月2日のGPAIルール適用開始を控え、実務ガイドラインの策定に向けて、多様な意見を収集
  - CoPとともに本年5 - 6月に公表予定
  - 日本を含む非EU企業にも影響大：ファインチューニングのみの利用でも規制対象となる可能性



# GPAIガイドライン

- 正式名称：AI法における汎用AI規則の範囲を明確にするための委員会ガイドライン
  - Commission Guidelines to Clarify the Scope of the General-purpose AI Rules in the AI Act
- 目的
  - 「汎用AIモデル」とは何か、「汎用AIモデルの提供者」とは何か、「汎用AI市場投入」とは何か、汎用AIモデルの学習に使用される計算資源をどのように見積もるのか、といった主要概念の明確化。
  - CoPを補完する文書としての位置付け
  - 法的拘束力はないが、欧州委員会にとって重要な判断基準となる
- カバーしているトピック
  1. 汎用AIモデル（GPAIモデル）とは
  2. GPAI モデルの提供者とは誰か、下流でモデル修正を行う事業者（downstream modifier）の取り扱い
  3. GPAI モデルの市場投入とは何か、オープンソース適用除外について
  4. モデルの学習や修正に使用される計算リソースの見積もり
  5. 経過措置、グランドファーザー制度、遡及適用
  6. CoP遵守と署名の効果
  7. GPAIルール of 監督と実施

# パブリックコメントの主な設問

## 1. GPAIモデルの定義

- GPAIであるか否かの閾値として「 $10^{22}$ FLOP」という計算量基準は適切か？
- 代替基準はありうるのか？

## 2. 提供者の範囲と下流改変者の義務

- Downstream Modifierが「提供者」となる計算量基準の適切性（例： $3 \times 10^{21}$ 、 $3 \times 10^{24}$  FLOP）

## 3. 「市場投入」の定義とオープンソース例外

- 無償公開・再配布など例外条件の妥当性

## 4. 学習・修正時の計算量の見積もり方法

- GPU使用ベース／モデル構造ベースなどの計算式

## • 意見提出締切

- Thursday, 22 May, 12:00 (noon) CET.  
日本時間 5月22日午後8時



ブリュッセル効果への対応：日本企業はEU-AI法にどう備えるべきか 4

# EU AI法 GPAIガイドラインについて

2025年5月12日

日本電気株式会社

# 「FLOP」と「FLOPS」の違い

## ■ FLOP (floating point operations) : 浮動小数点演算数

- 浮動小数点演算の**総量**を示す指標
- 自動車に例えると、積算距離計 (オドメーター)



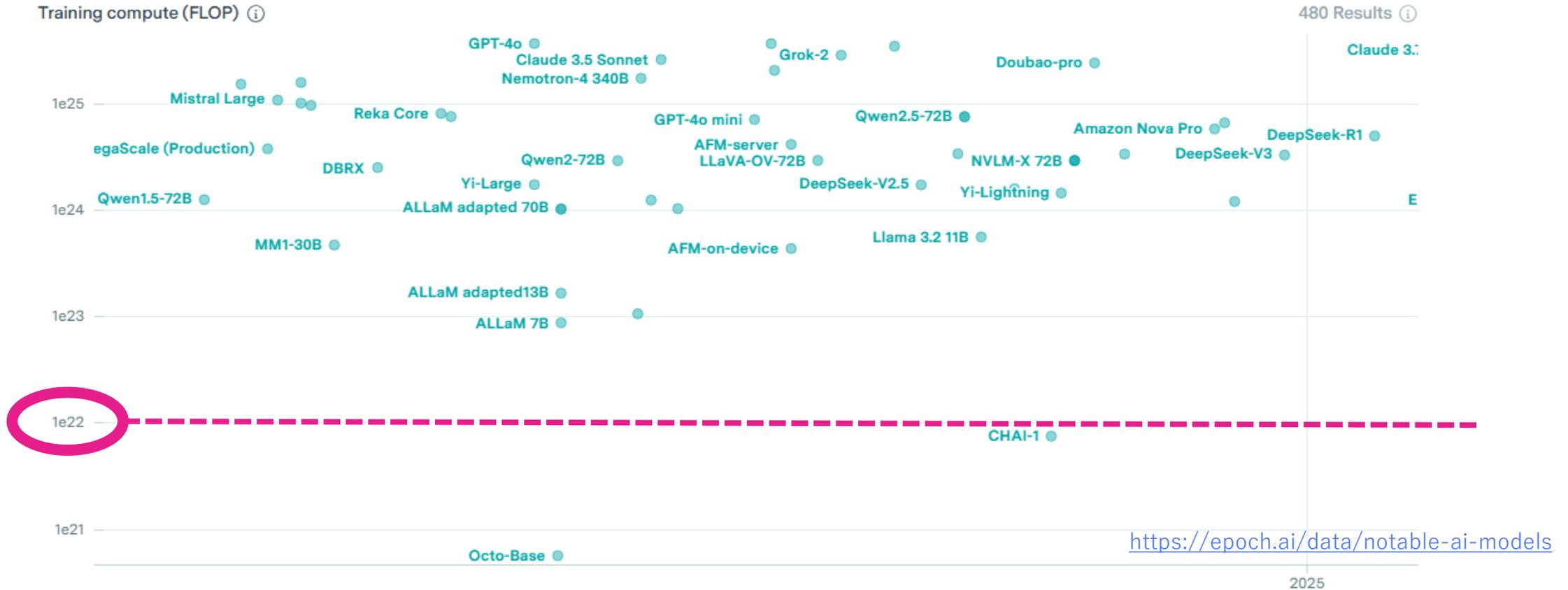
## ■ FLOPS (floating point operations per second) : 1秒間あたりの浮動小数点演算数

- **1秒間に**浮動小数点演算が何回できるかの指標。主にCPUやGPUといったコンピュータのハードウェア性能を評価
- 自動車に例えると、速度計 (スピードメーター)



- EU AI法では、**GPAIモデルのトレーニング量を測るために前者の指標を用いている**が、後者の指標のほうがメジャーであるため、**国内外の解説記事でも混同しているケースがある**。また、前者を「FLOPs」(小文字のsで複数形)と表記しているケースもあるため注意が必要 (EU AI法もドラフト版ではこの表記を使用)

# 「GPAIモデル」への該当基準について



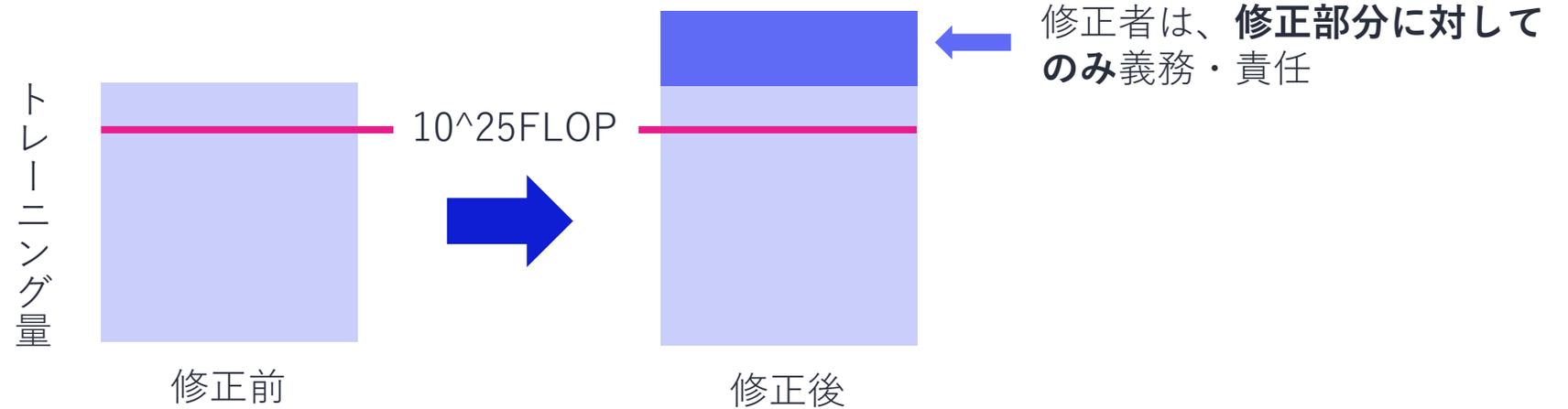
- 2024年以降にリリースされたほとんどすべてのAIモデルのトレーニング量はGPAIモデル該当基準である $10^{22}$  ( $1e22$ ) FLOPを超えている
- AlibabaのQwen2.5-0.5Bなど一部の小規模モデルは $10^{22}$ FLOPを若干下回る模様。しかし、パラメータ数も1B (10億) を下回っており、EU AI法 前文98の基準 (1B以上がGPAIモデル) に照らし合わせても「GPAIモデル」には該当しない
- このため、これまでの「GPAIモデル」の該当判断に大きな影響を及ぼすものではない (=妥当と考える)

# 「修正」によるGPAIモデル「プロバイダ」への該当基準について

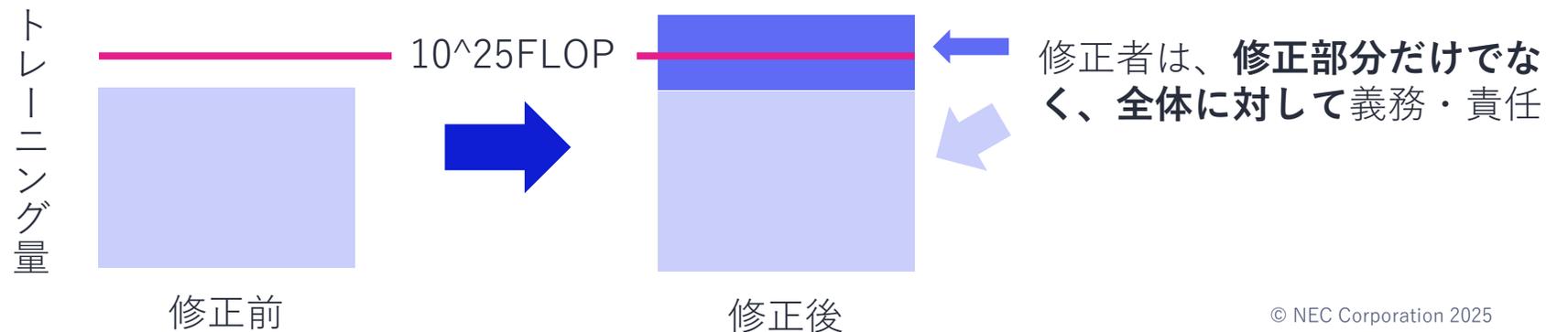
- ファインチューニングなどの「修正」に要するトレーニング計算量が約 $3 \times 10^{21}$ FLOP（GPAIモデル基準の3分の1）以上となった場合は、「新しいGPAIモデル」やそのプロバイダとみなされうる
- 「修正」に要するトレーニング計算量が約 $3 \times 10^{24}$ FLOP（システミックリスクGPAIモデル基準の3分の1）以上となった場合は、「新しいシステミックリスクGPAIモデル」やそのプロバイダとみなされうる（ガイドライン案6ページ目）
  - これまでは、小規模なファインチューニングを行った場合もプロバイダとみなされるうるのではないかという懸念があったが、かなり大規模な修正・再トレーニングをおこなった場合に限定されることが判明
  - 一方で、システミックリスクGPAIモデル基準（ $10^{25}$ FLOP）にわずかに及ばないAIモデル（例えばMeta Llama3-70Bが $7.9 \times 10^{24}$ FLOP）を修正・再トレーニングした結果、システミックリスクGPAIモデル基準を超えてしまった場合、修正・再トレーニングした者がシステミックリスクGPAIモデルプロバイダとみなされる可能性がある（9、10ページ目）。このため、このようなぎりぎりのAIモデルの活用が進まなくなる可能性がある。日本の産業界においては、LlamaなどのオープンソースのAIモデルを再トレーニングして活用するケースは多いと考えられるため、影響が懸念される

# 「修正」によるGPAIモデル「プロバイダ」への該当基準について

## ■ システミックリスクGPAIモデルを修正した場合



## ■ システミックリスク基準（10<sup>25</sup>FLOP）を下回るGPAIモデルを修正し、基準を超えた場合



# 「GP」 AIモデルの基準について

- トレーニング計算量がGPAIモデル基準（ $10^{22}$ FLOP）を超えている場合であっても、**実行できるタスクが限定されている場合は「GP（汎用目的）」AIモデルとはみなされない可能性がある**（5ページ目）
  - ・ ガイドライン案での例示
    - ・ コードのみを含み、他の種類のテキストを含まない特殊なデータセットでトレーニング
    - ・ 音声をテキストに書き起こすタスク専用トレーニング
    - ・ 画像の解像度を上げるタスク専用トレーニング
- 日本のAI企業が注力している、**業界・業種・業務特化型のAIが、「実行できるタスクが限定されているAI」とみなされるかどうか**で、日本の産業界への影響が変わる

# まとめ

1. 「GPAIモデル」への該当基準（ $10^{22}$ FLOP）については、大きな影響はない
2. 「修正」によるGPAIモデル「プロバイダ」への該当基準については、**システミックリスクの基準を若干下回るAIモデルを修正するケース**において要注意
3. 「GP（汎用目的）」AIモデルの基準については、どこまでが「**実行できるタスクが限定されているAI**」とみなされるか（GPAIから除外されるか）の明確化が必要

**NEC**

\Orchestrating a brighter world



TOKYO COLLEGE

ブリュッセル効果への対応:日本企業はEU-AI法にどう備えるべきか4

# EU-AI法 汎用目的AI ガイドラインについて

2025年5月12日

日本電信電話株式会社

技術企画部門 AIガバナンス室

根本 宗記

# ガイドライン案における累計計算量の基準

対象

基準

システミック リスク

学習の累積計算量:  $10^{25}$  乗 FLOP

汎用目的AIモデル

学習の累積計算量:  $10^{22}$  乗 FLOP

汎用目的AIモデルの微修正・調整

学習の累積計算量:  $3 \times 10^{21}$  乗 FLOP

# モデルA ハードウェアアプローチの計算方法

## モデルAの条件

---

使用GPU:	NVIDIA A100 ピーク性能 BFLOAT16 300×10の12乗 FLOP/秒
学習の累積計算時間:	35000時間
GPU使用率:	56%
パラメータ数:	11億
学習トークン数:	3兆トークン

## 計算式

---

$$35000\text{時間} \times 3600\text{秒/時間} \times 300 \times 10\text{の12乗 FLOP/秒} \times 0.56$$

$$= 2.1 \times 10\text{の22乗 FLOP}$$

※みなさんでも計算されることをお勧めします

## 考察

---

計算方法は非常に分かり易い

モデルAは、汎用目的AIモデル 10の22乗 FLOPを超える例

35000時間は1458日なので、A100 10枚で計算していたら145.8日(5か月弱)の期間

# 論点: FLOP基準で良いのか？

## 気になる点

---

CPUでもそうだったが、GPUの浮動小数計算性能はアプリケーションの処理性能に直結しない。NVIDIA H100は、A100より6倍強のBFLOAT16性能があるが、学習レベルの性能はそんなには上がらない。

新しい・性能が良いGPUで計算していくと10の22乗や10の25乗といった基準は実質的に下がっていく

## 代替基準

---

使用GPUによる影響が大きすぎる浮動小数計算性能によらない代替基準案

パラメータ数  $B$ (ビリオン)  $\times$  学習トークン数  $T$ (トリリオン)

モデルAの場合は、 $1.1 B \times 3 T = 3.3 B \cdot T$

## コメント案(現時点)

---

基準が簡単な計算式で算出できることは非常に良い

使用GPUによる大きな影響が抑えられる代替基準案を提案する

アルゴリズムによっても累積計算量はかなり変わるため、基準値は定期的見直しを行った方が良い  
そもそもAIモデルの学習量と社会リスクの大きさの関係性は、不明点が多いと認識している

# *Innovating a Sustainable Future for People and Planet*