

報道が描く「誤解」と、制度の「現実」

【誤解】「全学習データの一般公開が義務化された」

・営業秘密が
すべて奪われる

・オープンソースや
スタートアップの
開発が停止する

・違反すれば直ちに
著作権法違反で
罰せられる

【現実】「対象を絞った開示と、層状の透明性要求」

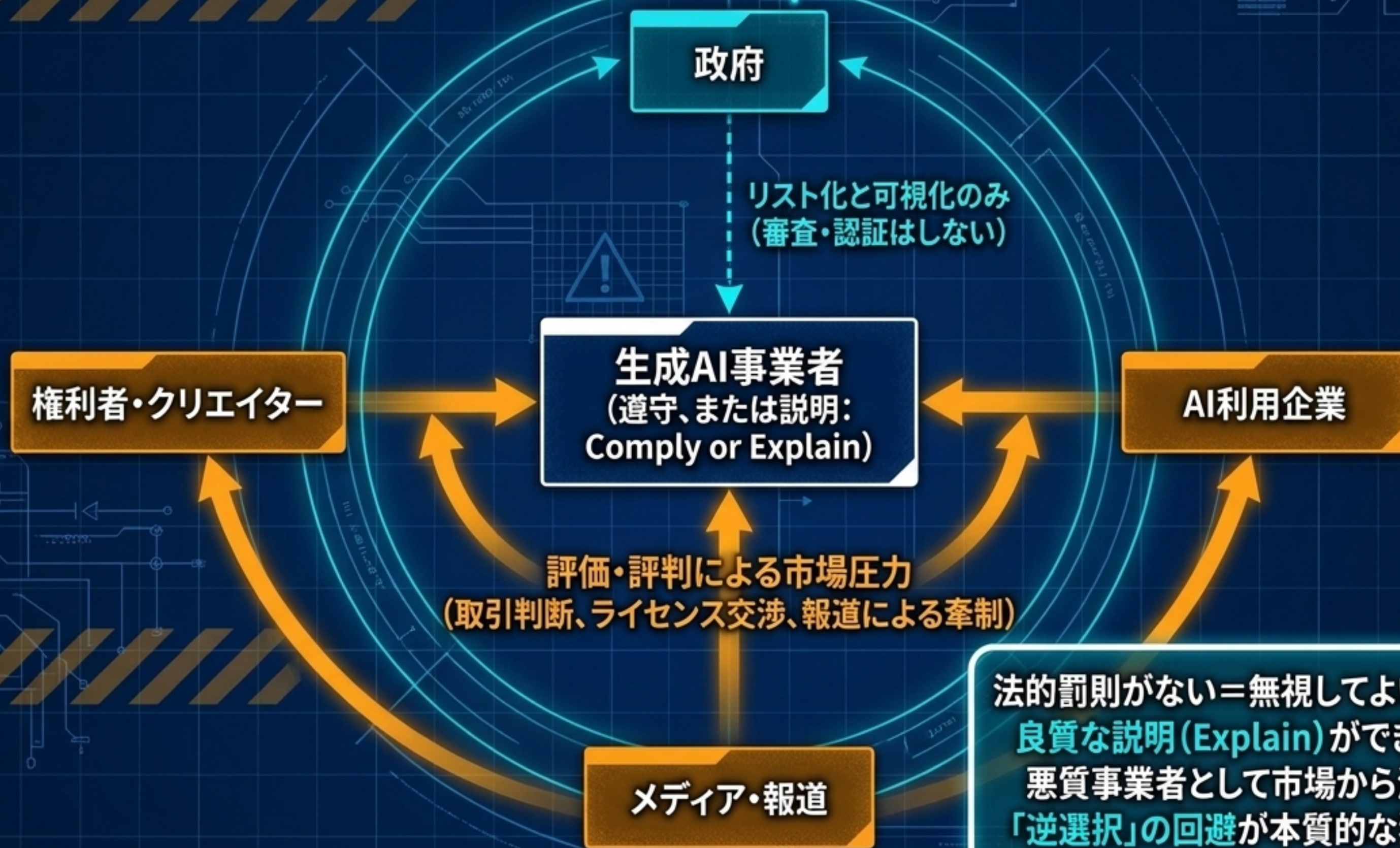
・一般公開されるのは
あくまで「概要」のみ

・個別URL照会（原則2・3）は
特定条件下の限定対応

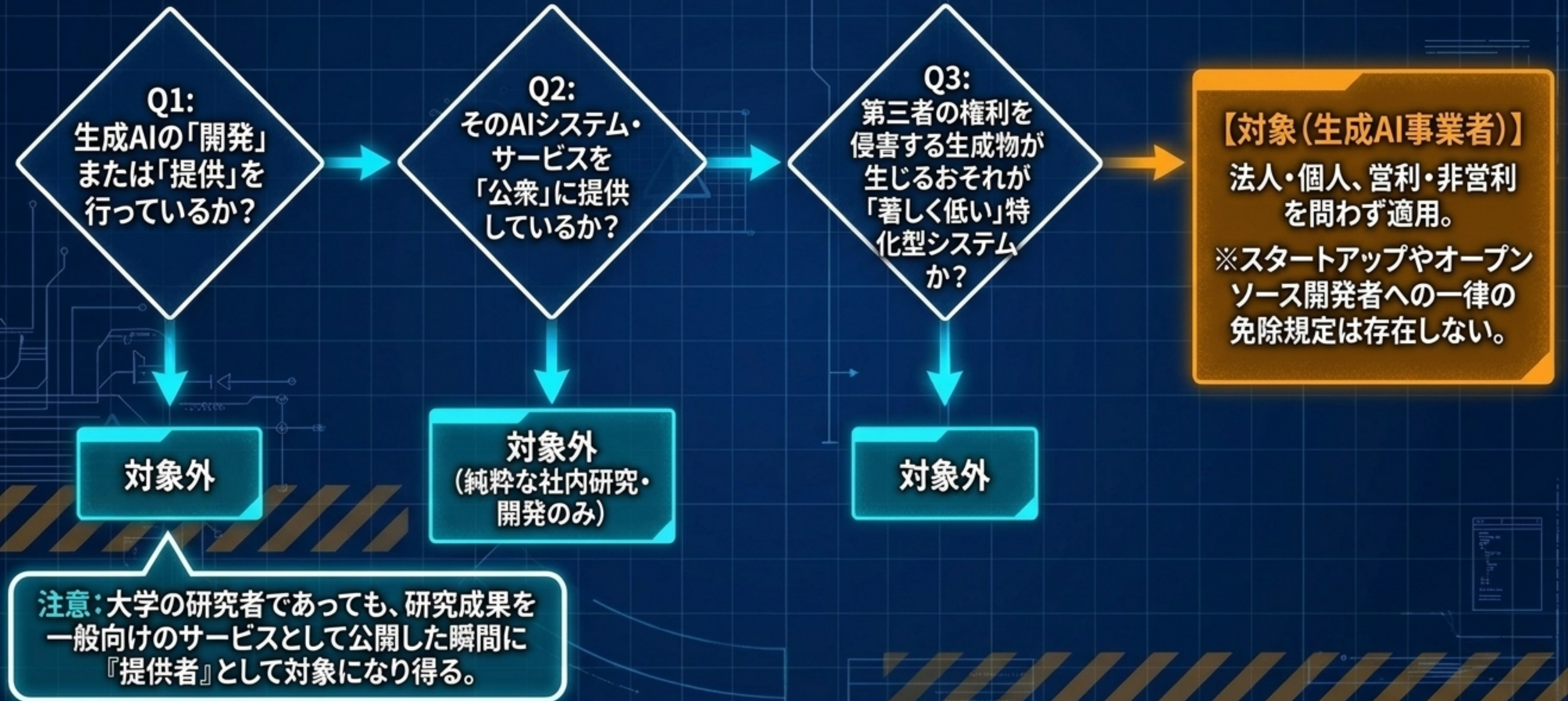
・「法的拘束力のないソフトロー」
であり実体法（著作権法）は不変

本コードは「学習データを丸ごと公開させる制度」ではない。
権利者とAI事業者の間の情報の非対称性を埋める「対話のためのインフラ」である。

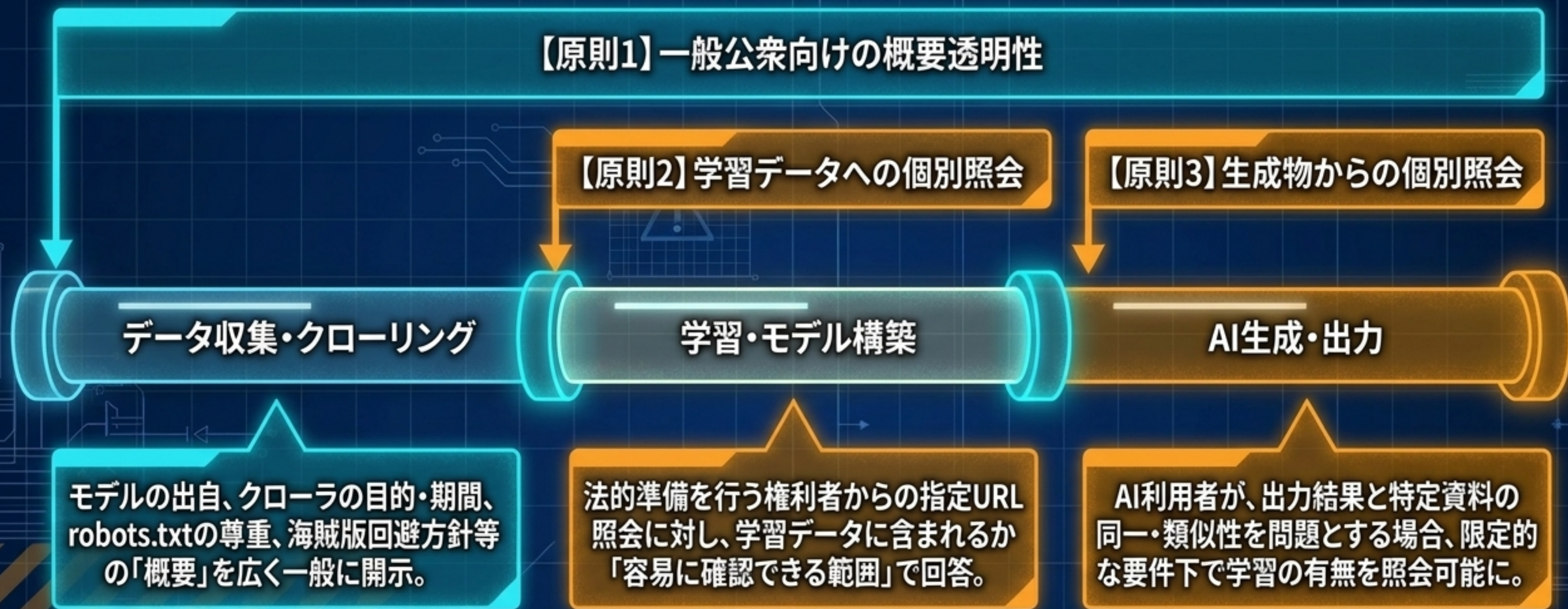
執行主体は政府ではなく「市場の評判」である



適用対象の境界線：誰がコードを遵守すべきか？



The IP & Data Flow Architecture : 3つの原則の介入点



Insight:「原則1(一般公開)」と「原則2・3(特定者への個別回答)」は全く別物である。
この二層構造の理解がコンプライアンスの第一歩となる。

グローバル規制ランドスケープ：日本の独自ポジション

広く、弱い (Wide but Weak)

法的な執行力は持たないが、個別URL照会という極めて実務的・技術的な踏み込みを行っている世界でも特異な制度設計。

	日本 (本コード)	EU (AI Act + GPAI Code)	米国 (連邦 NIST + 州法 AB 2013)	英国 (政府検討中)
法的性格	ソフトウェア (Comply/Explain)	ハードロー (法定義務)	分散型 (州法はハード、 連邦は任意)	政策論争継続
学習データ 一般開示	概要開示	十分詳細な概要 (執行権限あり)	カリフォルニア州 で概要開示義務化	入力透明性を 検討中
個別URL 照会制度	★原則2・3で 明記	一般的な同型 制度なし	一般的な同型 制度なし	一般的な同型 制度なし

ステークホルダーの力学：2,000超のパブコメと最終版の妥協点

権利者側（新聞・アニメ等）

評価：一步前進だが任意では逆選択が起きる
要求：権利行使に資する透明性、将来的には
法制化を

AI産業側（BSA・新経連等）

評価：イノベーション阻害の懸念
懸念：営業秘密の漏洩、個別URL追跡の技術的
困難さ、事実上の義務化

最終コードに組み込まれた4つの安全弁

営業秘密・
セキュリティ
(機微情報の強制
開示は求めない)

過大負担
の回避
(合理的な判断に
基づく対応を許容)

法的拘束力
の否定
(著作権法適法性
とは別レイヤーで
あることを明記)

制度の不完全
性の承認
(原則は完全では
なく、技術動向に
応じ改定する)

営業秘密との両立：「二択」を避ける階層的情報ガバナンス



「営業秘密だから非公開」という一行のExplain（説明）は市場から評価されない。
「誰に対して、どの深度までなら安全に開示できるか」を設計することが求められる。

技術パラダイムの転換：Provenance-by-Designへの移行

【Before】性能・コスト最適化パイプライン



- 巨大なWebコーパスをそのまま投入。
- 「学習済みのモデルを後から調べても、どのURLを学習したか（記憶）を逆引きすることは技術的に困難。」

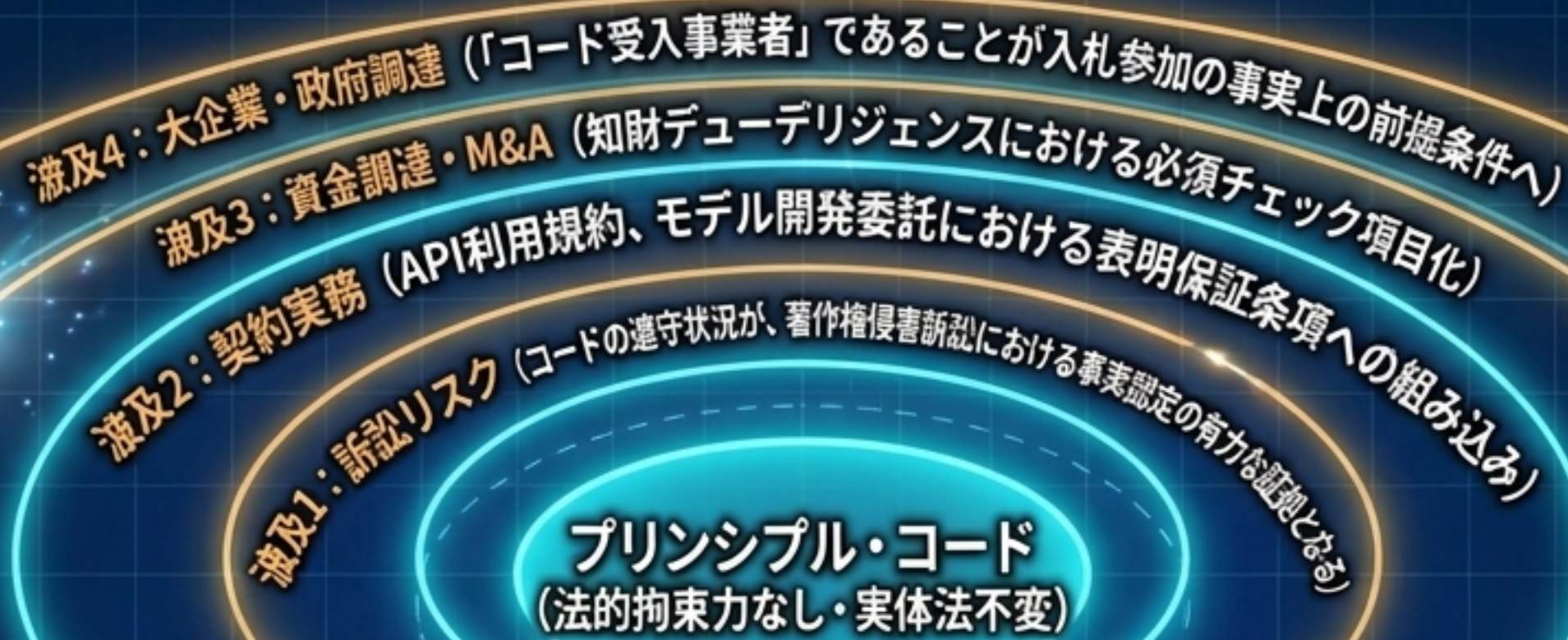
【After】来歴管理パイプライン (Provenance-by-Design)



- クローラー設定、URL、取得時点、除外リスト、ライセンス情報をデータ台帳として記録・保持。
- 「モデルの『記憶』を探るのではなく、データ収集の『記録』を検索可能なインフラとして構築しなければ、照会要請には応えられない。」

本コード対応で最もコストがかかるのは「文章を書くこと」ではなく、
「説明可能なデータ台帳」のシステム開発である。

The Ripple Effect : ソフトローの「事実上のハード化」メカニズム



「法的義務の不在」は、「実務上の影響の不在」を意味しない。コンプライアンスの重心は、**著作権法 (適法性)** から、**説明可能なデータ・ガバナンス (商取引標準)** へと移行した。

契約実務への波及：AIバリューチェーンにおける責任分配

契約上の論点	実務上の対応（条項の具体化）
データ透明性	上流ベンダーが公開するモデルカードや学習情報を、契約上の「仕様書」として特定・固定する。
原則2・3照会への協力	下流（サービス提供者）に権利者から照会が来た場合、上流（基盤モデル側）が合理的期限内にデータ履歴を調査・回答する協力義務を明記。
権利保証と補償	データ取得経路、robots.txtの尊重、権利留保対応に関する表明保証。知財クレーム発生時の防御協力と責任制限の配分。
証拠保全と監査	クローラーログ、データセットのバージョン履歴の保存期間の設定。「コード受入れ状況」を定期監査の対象とする。

下流企業にとって「APIの先はブラックボックスなので分かりません」は通用しなくなる。上流への情報提供要求が契約交渉の焦点となる。

The Action Blueprint: ステークホルダー別ロードマップ

	短期 (公表～1年以内:基盤構築)	中期 (1～3年:実効性検証と標準化)	長期 (3年超:限定的法制化の検討)
政府	良いExplain/悪いExplainの 具体例提示、中小企業向け 簡易様式の整備。	営業秘密を保護した実効 性KPIの測定。	【共通】効果検証に基づく 「連絡窓口」等の限定的ハ ードロー化検討。EU・米国 との国際的な制度調和と 相互運用基盤の確立。
AI事業者	対象性判定、データソース とクローラーの棚卸し、 公開/機密の分類、照会 窓口の設置。	Provenance-by-designの 開発、API契約の再設計。	
権利者・ 利用者	標準化された申出様式の 作成、濫用を避けたピン ポイントな照会。	機械可読な権利留保標準 (robots.txt以外)の策定、 作品IDの整備。	

新たな「市場のベースライン」の誕生

本コードは、権利者への「新たな法的請求権」を生み出すものではない。

また、AI事業者に対する「免罪符」でもない。

**これは、AI開発における「合理的な行動、説明、そして記録」の
事実上の市場標準 (De facto standard) を形成する試みである。**

普及すればソフトローとして成功し、普及しなければ強固な法制化(ハードロー)への圧力が加速する。
現在下されているのは、AIエコシステム全体の「自浄能力」に対するテストである。