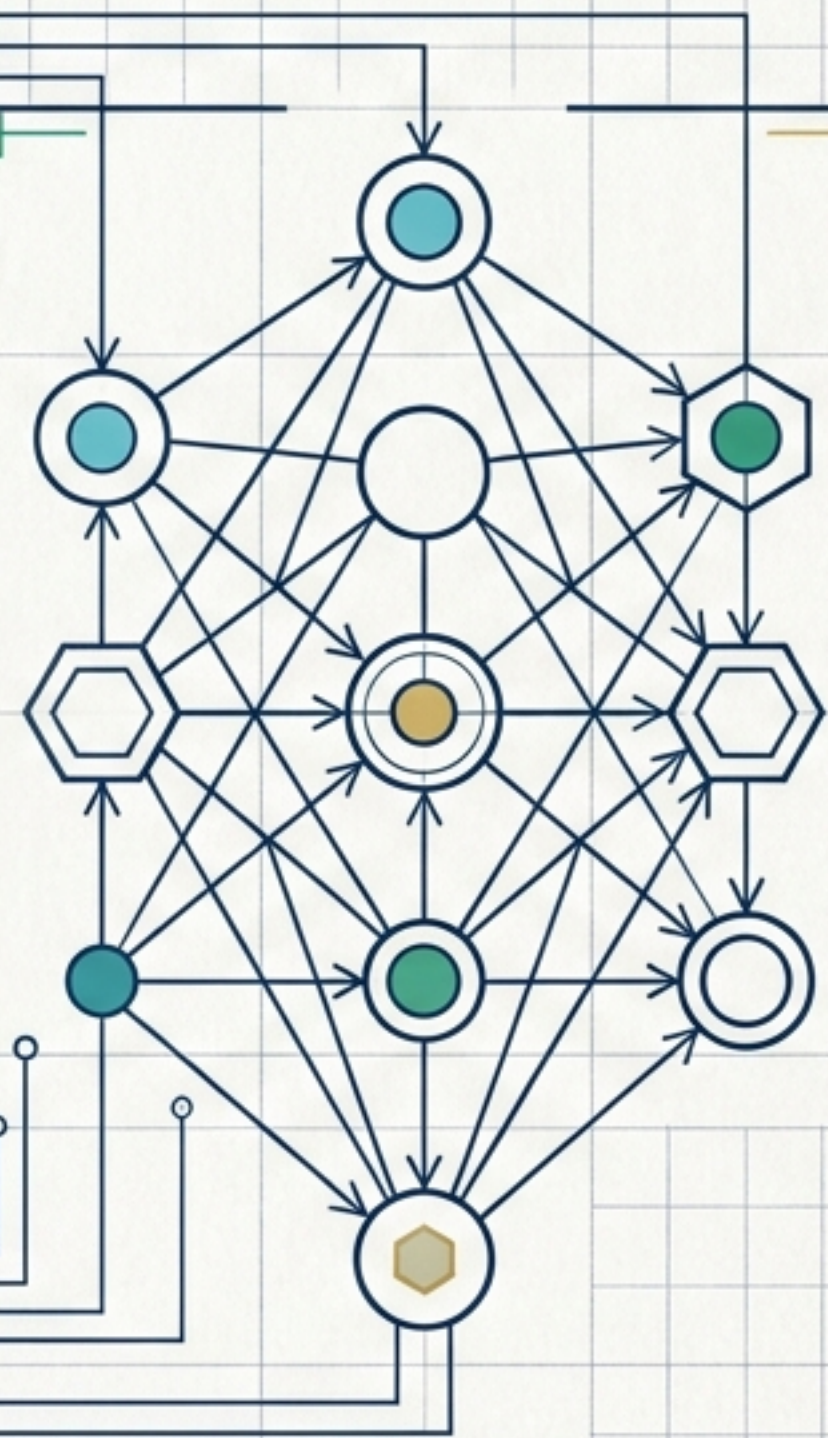




政策の青写真：AI悪用 リスクと知財ルール全般

日経新聞報道を起点とする、政府の横断的
AI規制と企業実務へのインパクト分析

2026年8月15日
政策知財戦略インスティテュート
AIガバナンス調査委員会



Executive Summary: 3つの核心的メッセージ



マクロの転換：著作権から 国家安全保障へ

- AI規制は単なる知財保護の枠を越境。
- サイバー防御・重要インフラを含む「省庁横断の4本柱」によるリスク管理ヘシフト。



ミクロのジレンマ：ソフト ローの限界と実装コスト

- 「プリンシプル・コード」は任意だが、遵守には膨大なデータ台帳や照会基盤が必要。
- 年間数千万～数十億円の実務コスト（FTE・システム費）を伴う経営課題。

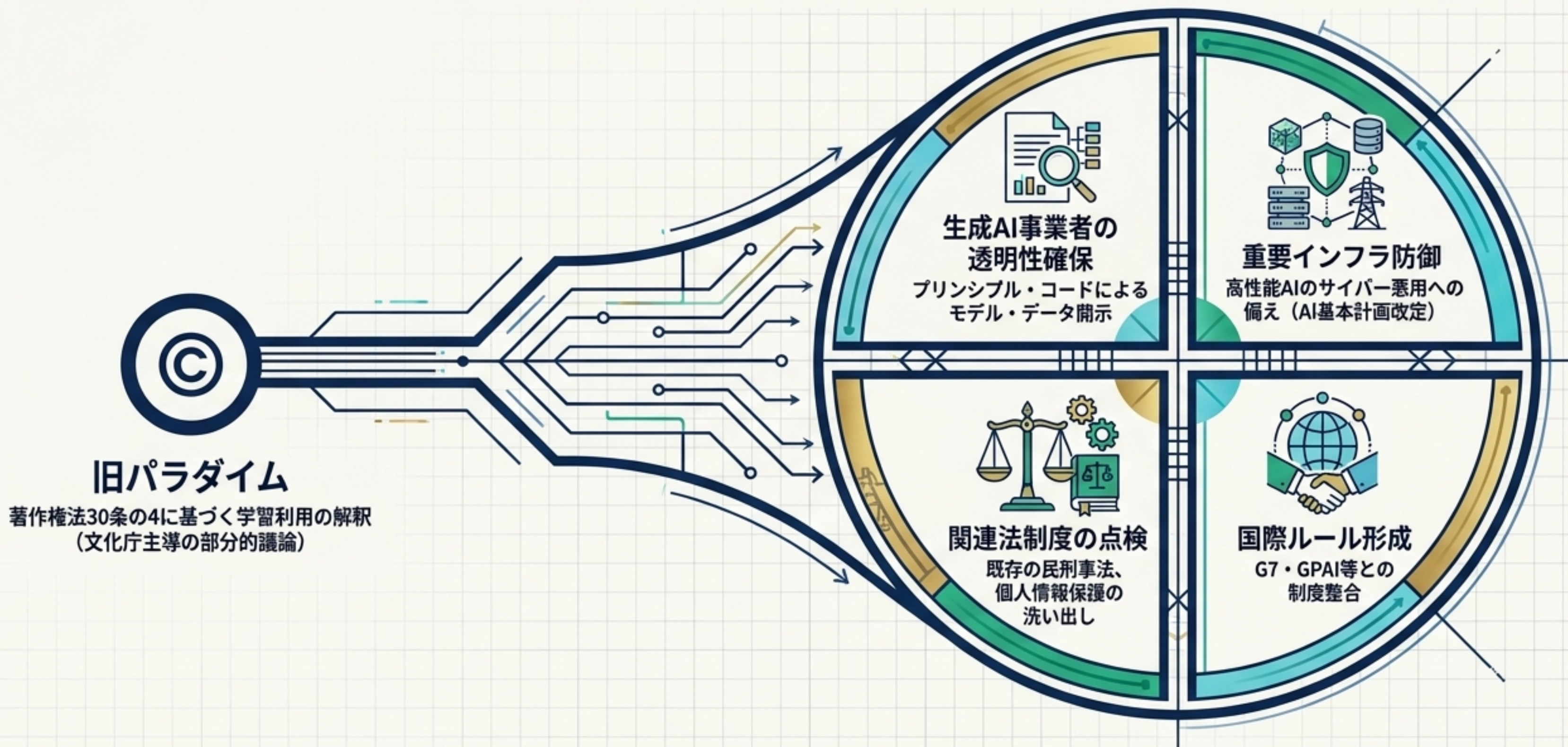


最適なアーキテクチャ： 二層型共同規制

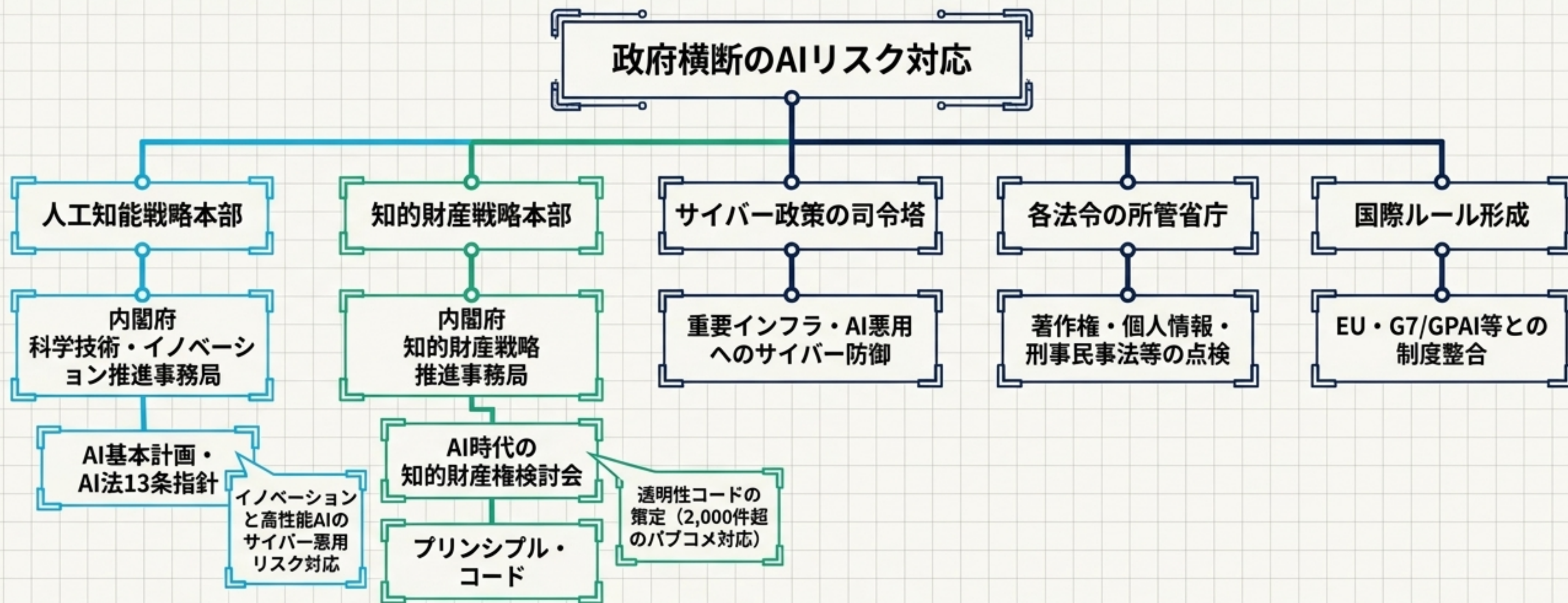
- 技術革新と機密保護の両立には新構造が不可避。
- 「最低限の法定化」と「第三者監査による限定開示」を組み合わせた制度設計へ。

The Paradigm Shift: 局地的な知財問題から 「国家レベルの横断的リスク管理」へ

新パラダイム：政府横断の4本柱

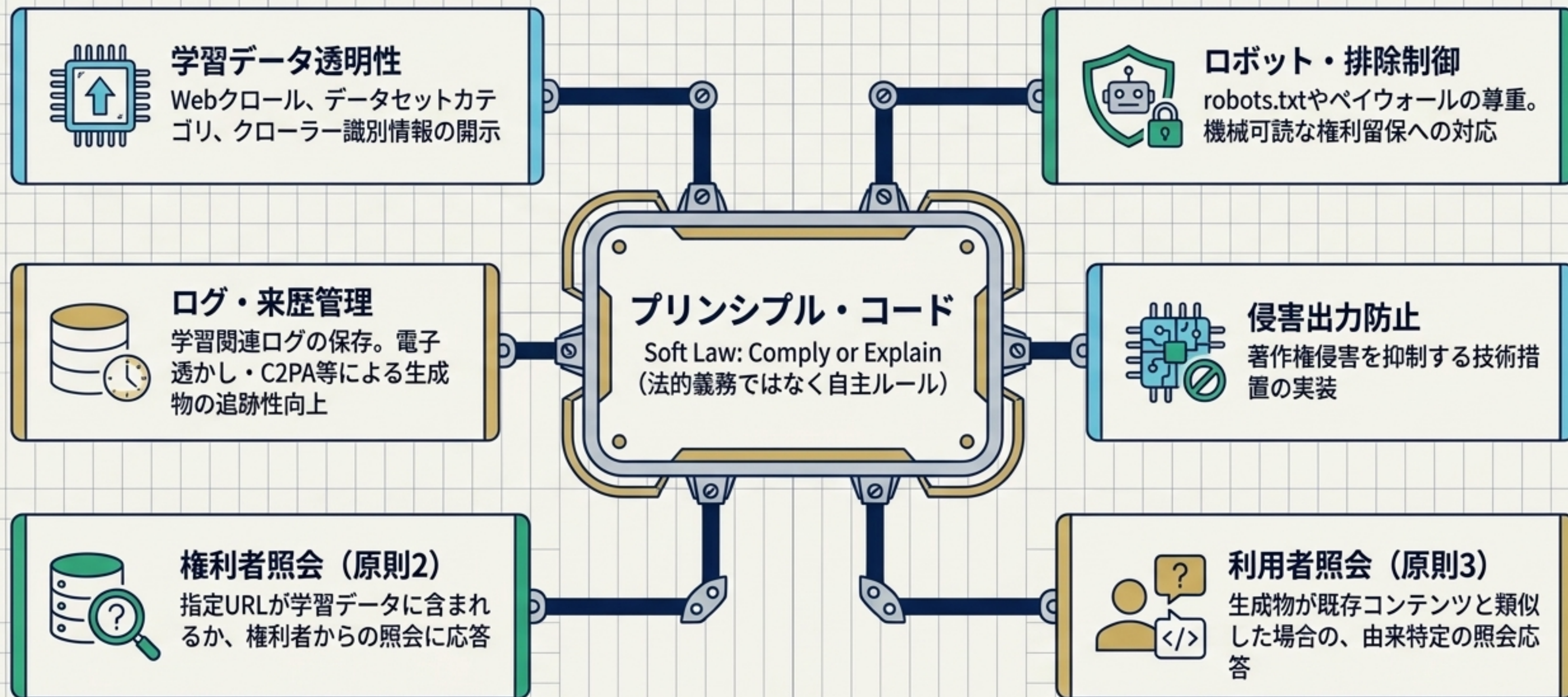


Dual Command Structure: 政策を牽引する政府内の「二重の司令塔」

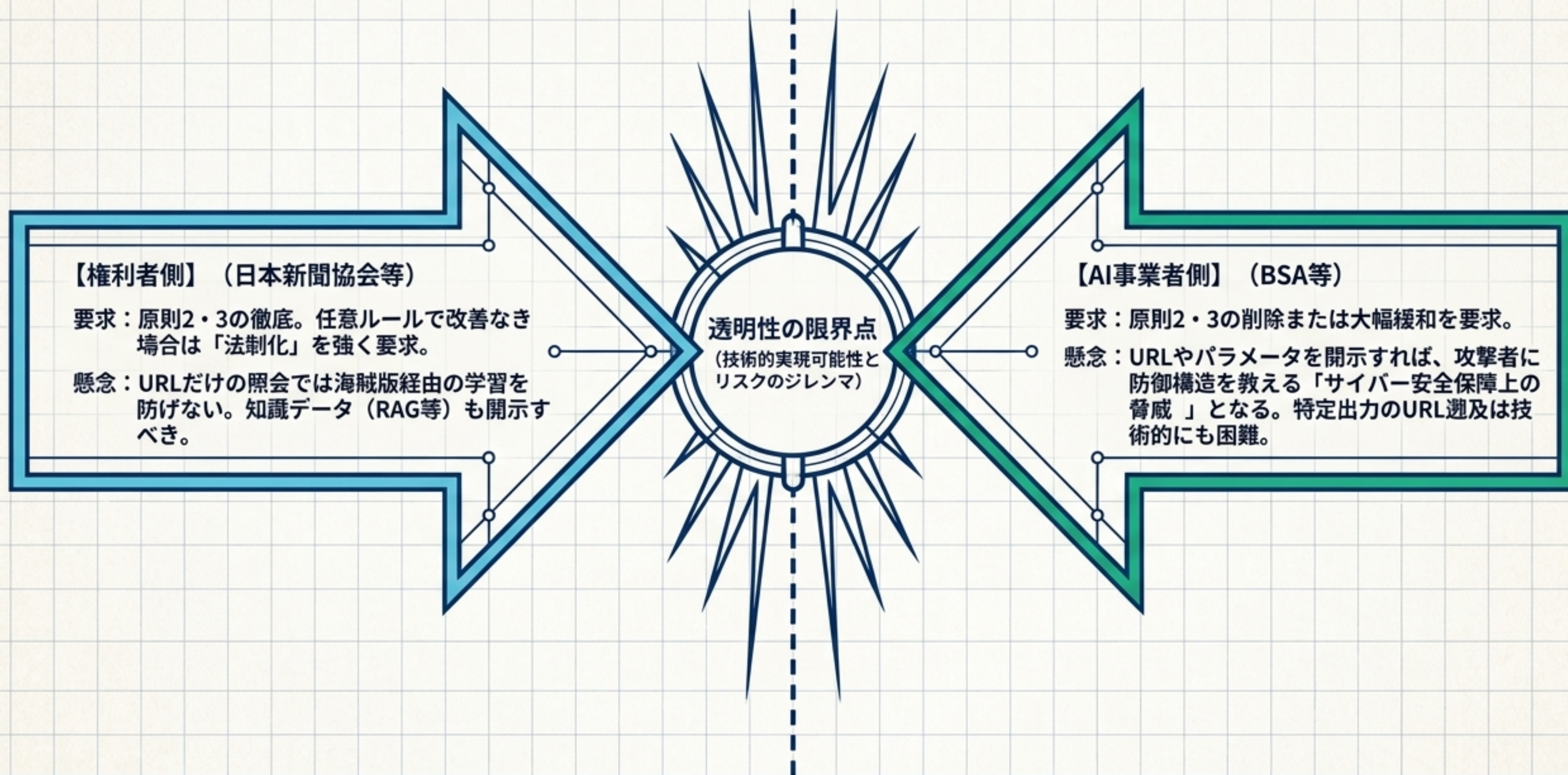


インサイト：知財の透明性コードを先行させつつ、他省庁が法制度の隙間を洗い直す
「第二段階のAIガバナンス構築」フェーズ

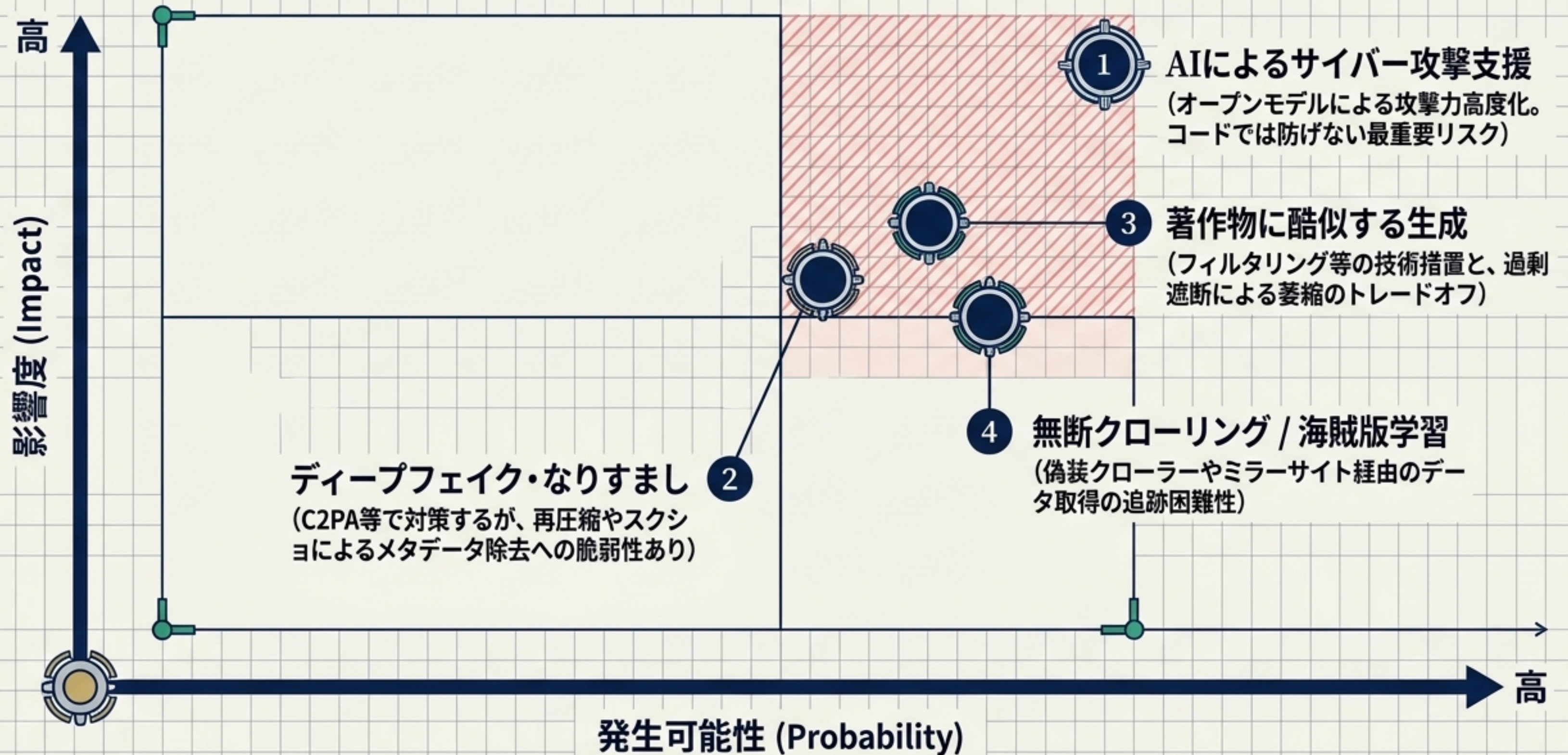
Anatomy of the Principle Code: 生成AI事業者への透明性要求モジュール



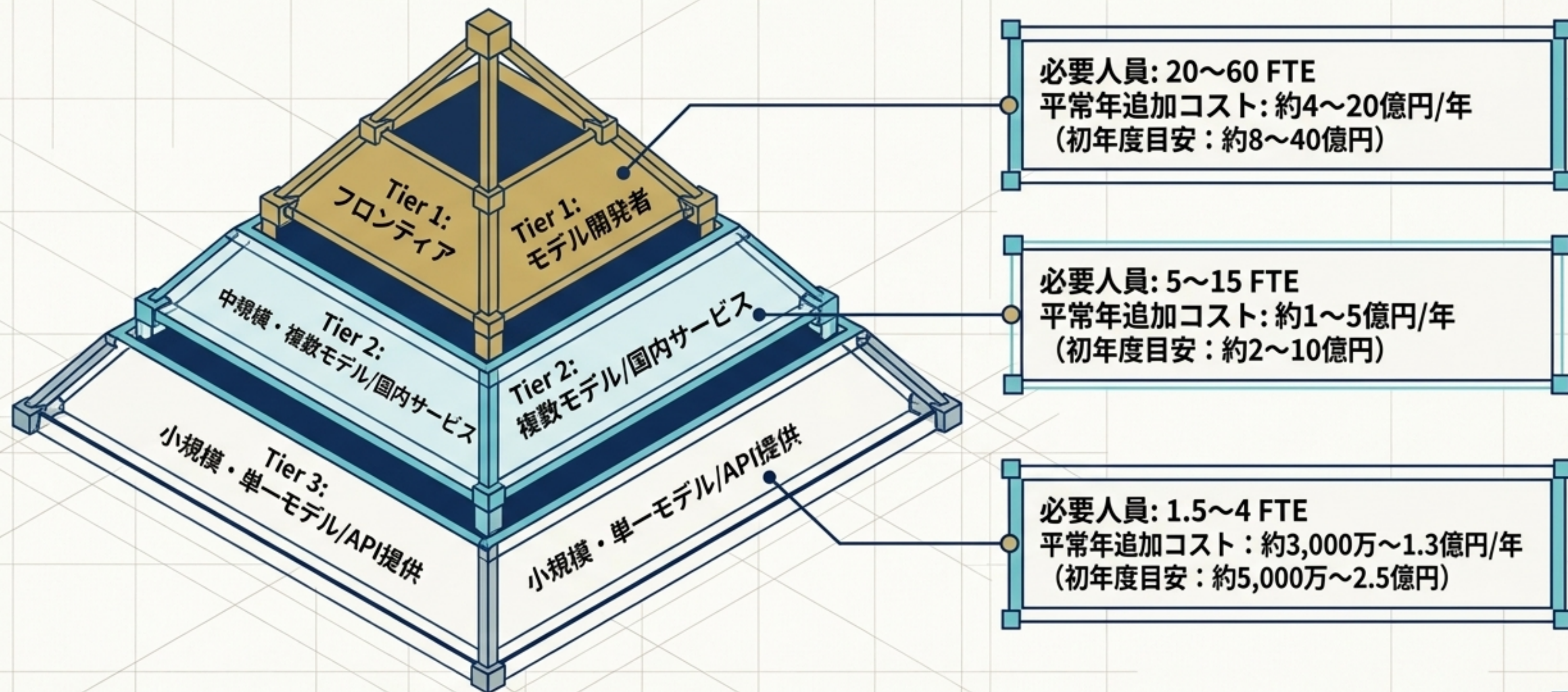
The Core Tension: 「権利者救済」と「サイバー防衛・営業秘密」の激突



AI Risk Assessment: プリンシプル・コードが直面する「残余リスク」



Cost of Compliance: 「透明性」を実装するための実務コスト試算



Cost Drivers: 過去モデルのデータ台帳整備、照会DB構築、出力フィルター、法務・エンジニアリング対応

※本報告独自の感応度試算シナリオに基づく

Ripple Effects: エコシステム全体への波及と「比例原則」の必要性

AI利用企業 (B2B)

契約・調達要件への波及。ベンダー選定時のデューデリジェンス負担増（学習データの説明、IP保証、コード参加有無の確認）。

AI開発・提供者

直接的なコード遵守義務。
照会窓口運用、来歴技術の実装。

研究機関・スタートアップ

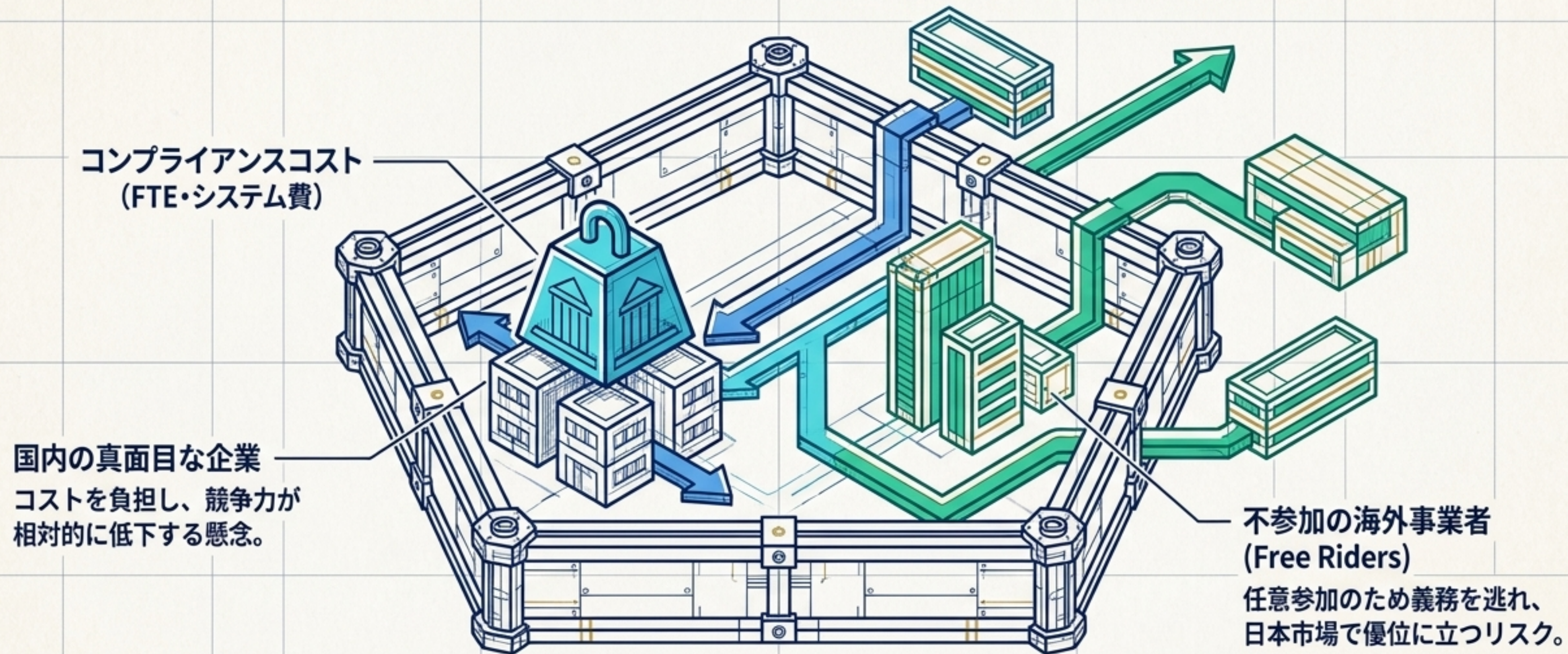
固定費増による研究萎縮リスク。
内部専用・閉域モデルを同列に扱わない「比例原則 (Proportionality)」による段階的義務化が不可欠。

Global Regulatory Landscape: 各国アプローチの比較マトリクス

国・地域	主要制度	透明性義務	生成物表示	強制力
日本	プリンシプル・コード	モデル・データ概要、クローラー、照会	C2PA・電子透かし等推奨	● 現段階で完全自主的（ソフトロー）
EU	AI Act + GPAI Code	GPAI提供者に透明性・著作権対応義務	2026年8月からArt 50適用	● 法的強制 + 任意コード
米国（加州）	Training Data Transparency Act	データセット高水準サマリー公開義務	-	● 州法強制
英国	政府報告にて複数案評価中	法的透明性義務を検討中	-	● 検討中
中国	AI生成合成内容標識弁法	コンテンツ生成・流通の追跡が主眼	明示・暗示標識の要求	● 行政規制・強制標準

インサイト：EUは「法的義務」と「技術コード」を組み合わせた構造。日本の「完全任意コード」アプローチは国際的に見ても強制力の弱さが際立つ。

The Japanese Dilemma: 「完全任意コード」がもたらす競争歪曲リスク



Strategic Imperative: 日本向けサービスを展開する海外事業者に対しても、
公共調達等の「市場アクセス条件」としてコード適合を実質的に要求するメカニズムが不可欠。

Evaluating Policy Options: 政策アーキテクチャの診断と評価

政策オプション	権利保護	実効性	R&D負担	国際整合	評価コメント
A: 現行ソフトローのみ	△	△～低	◎	○	フリーライダー問題の温床
B: 最低限法定＋詳細コード	◎	◎	○	◎	[推奨案] EUに近い二層型
C: 全面的事前許諾法制	◎	◎	低	△	イノベーションへの悪影響大
D: 市場・技術中心	△	◎	○	○	交渉力弱者の保護に難あり
D: 独形の製者監査モデル					イノベーションの保護に難上
E: 独立第三者監査モデル	○～◎	◎	○	◎	[推奨案] B案と組み合わせ 営業秘密を保護

結論：最も合理的なアプローチは「B（共同規制）」と「E（独立監査）」の統合モデルである。

Synthesis - The Optimal Blueprint:

機密保護と透明性を両立する「3層分離アーキテクチャ」



Layer 1:
Public Info
(完全公開)

対象：モデル概要、クローラーID、データセット概要
法的拘束力のある最低限の開示基準（法定化）



Layer 2:
Limited Disclosure
(限定開示)

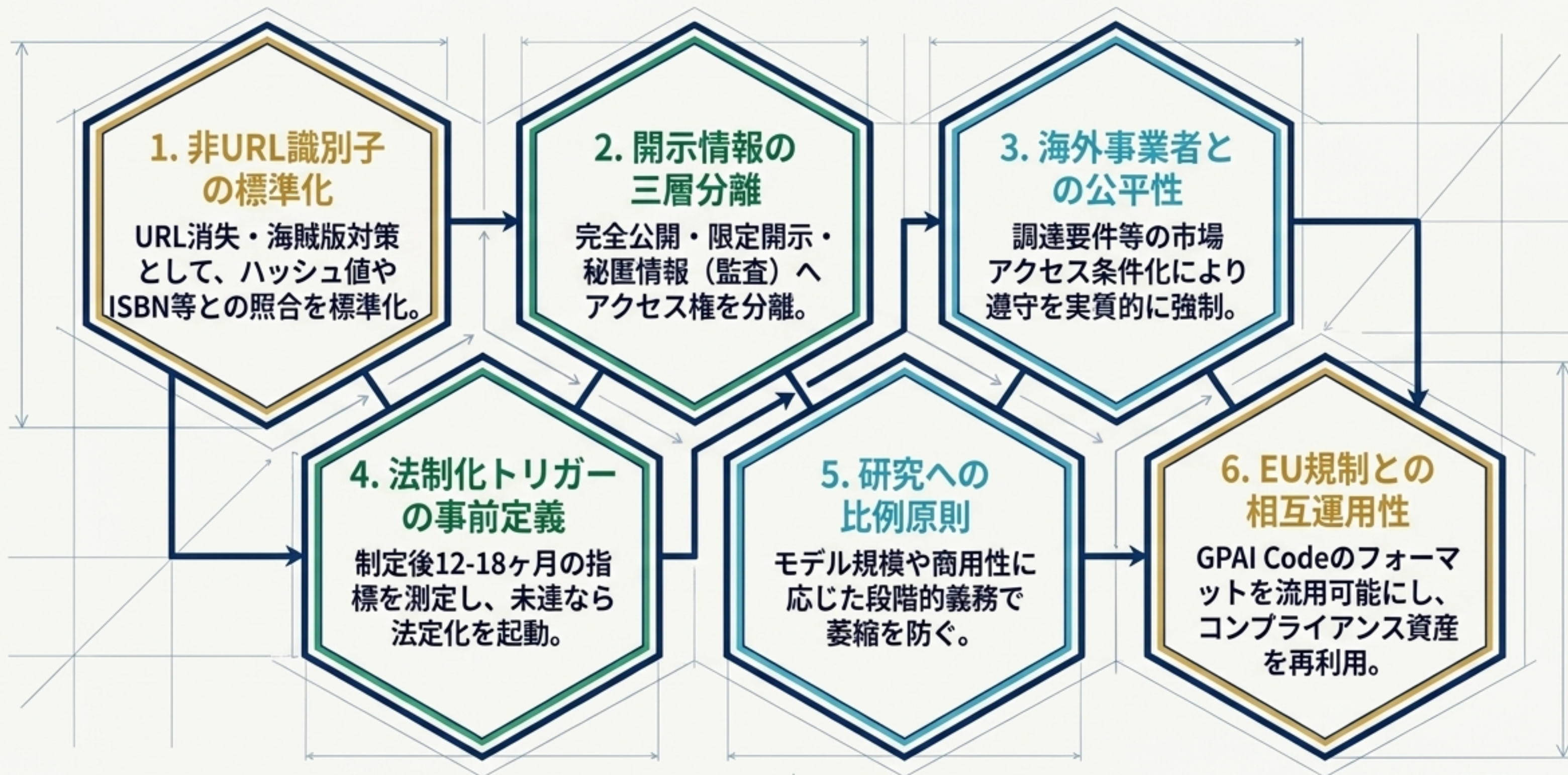
対象：認証済み権利者への照会回答（作品の包含有無）
標準化された照会プロセスと濫用防止



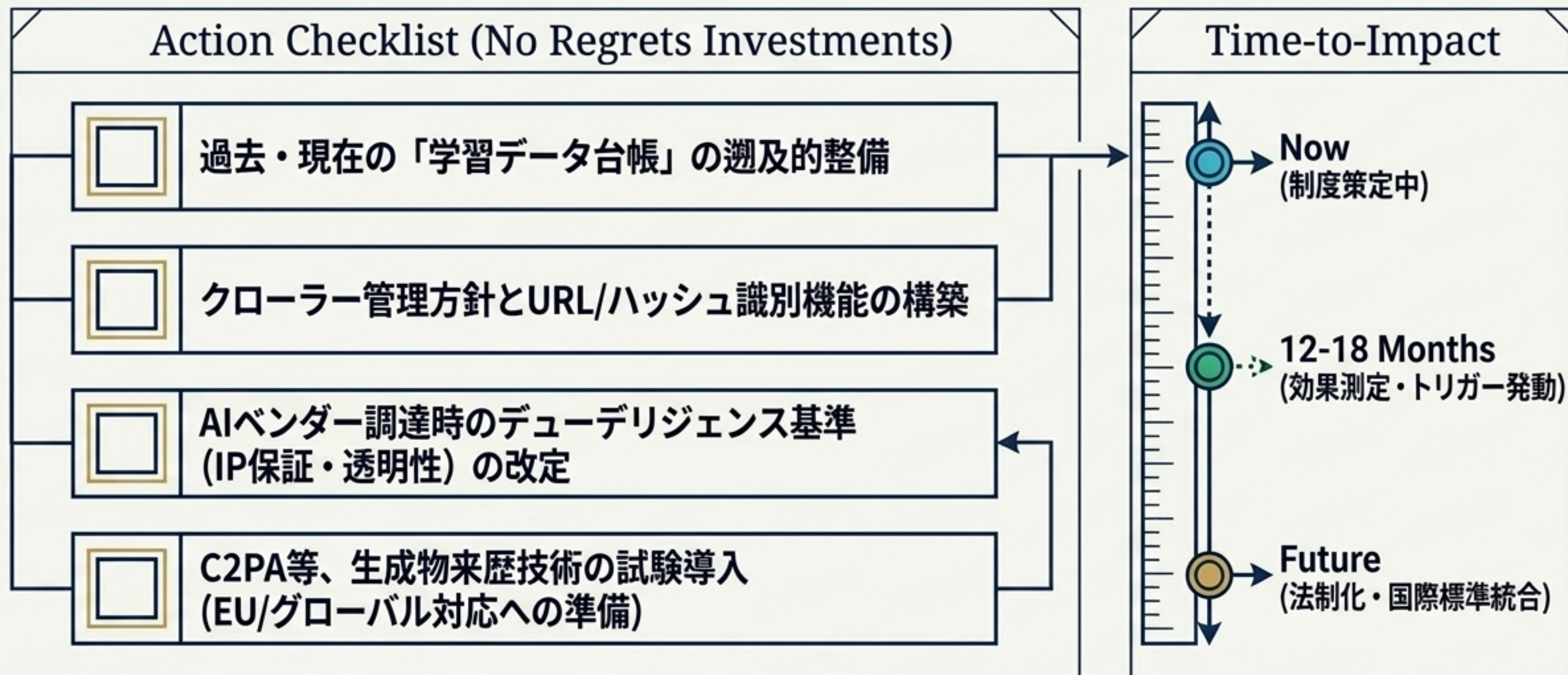
Layer 3:
Confidential Info
(秘匿情報 / 第三者監査)

対象：セキュリティ防御用URL、詳細パラメータ、営業秘密
裁判所・独立監査人・規制当局のみへの開示。
サイバー安全保障リスクを遮断。

6 Key Design Principles: 実効性確保のためのシステム要件



Conclusion & Next Steps: 制度確定を待たずに着手すべき「基盤投資」



Takeaway: 最終的な法律の条文や期限を待つべきではない。どの案に落ち着いても、AI開発・活用において「データプロベナンス（来歴）基盤」は今後の必須要件となる。