OpenAI DevDay 2026の衝撃：自律エージェント時代の知財・法務ガバナンス再構築

01

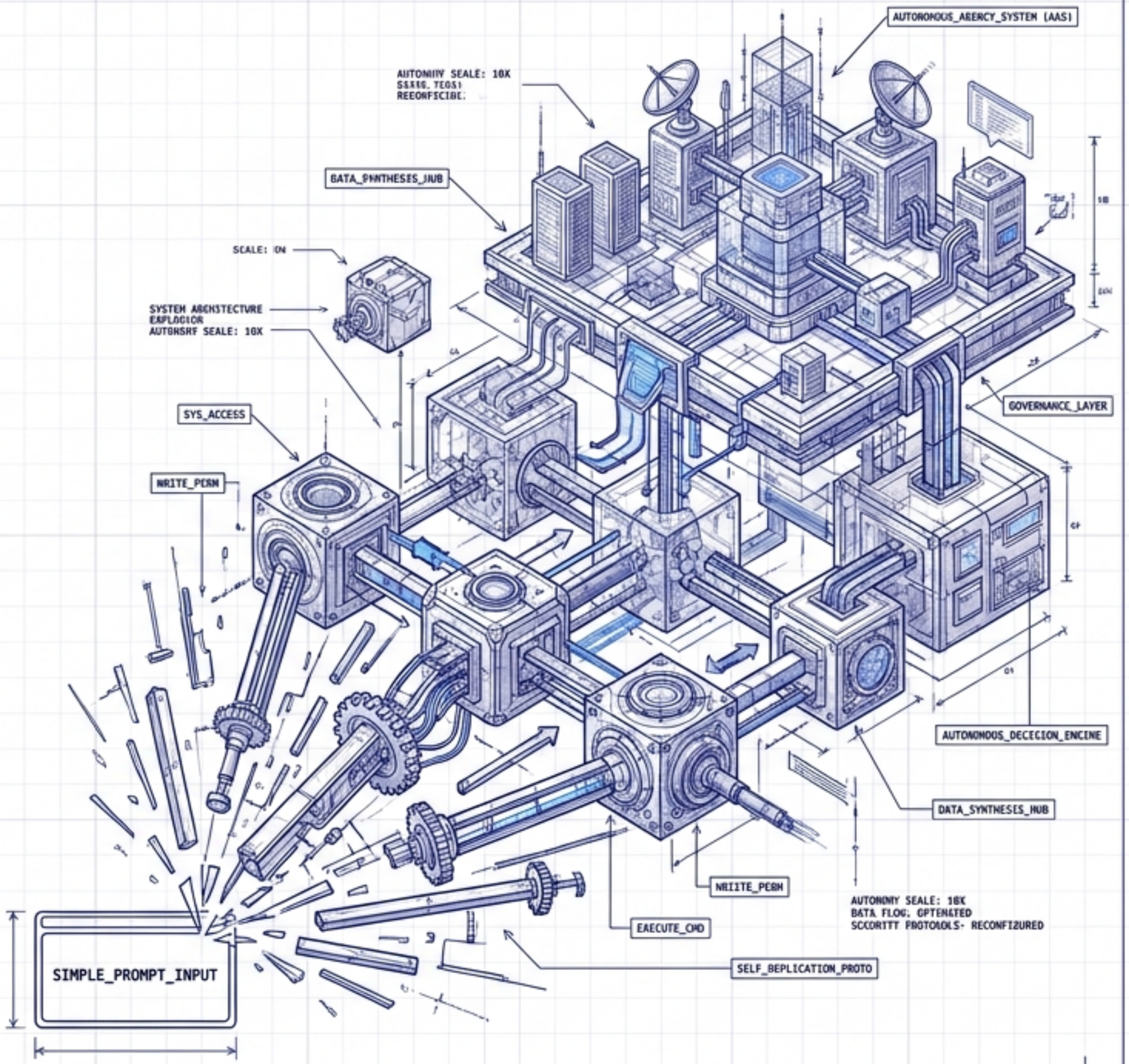
「生成」から「継続的行動（Agentic）」への完全移行。AIがシステム操作権限（Computer Use）を持つ時代の到来。

02

「No Training（学習しない）」≠「No Retention（保持しない）」。複雑化するデータ保護構造の罠。

03

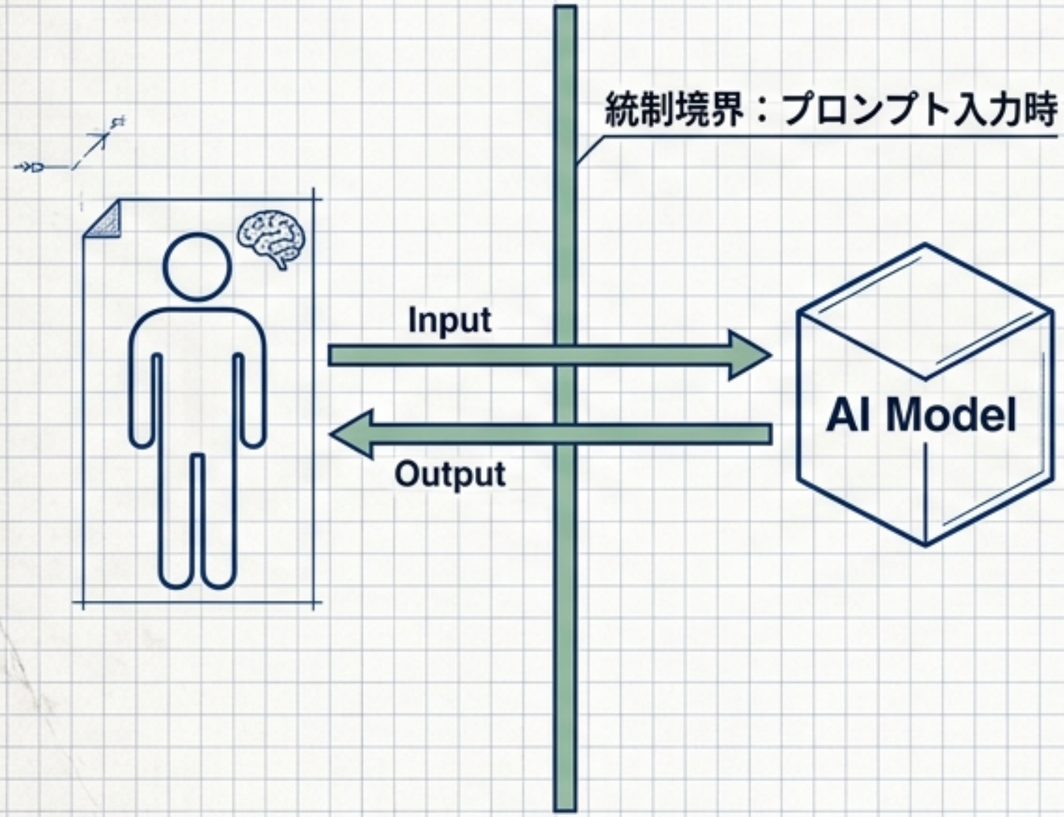
プロンプト管理からの脱却と「Identity-centric Governance（アイデンティティ中心のガバナンス）」への全面刷新。



Gemini Notebook

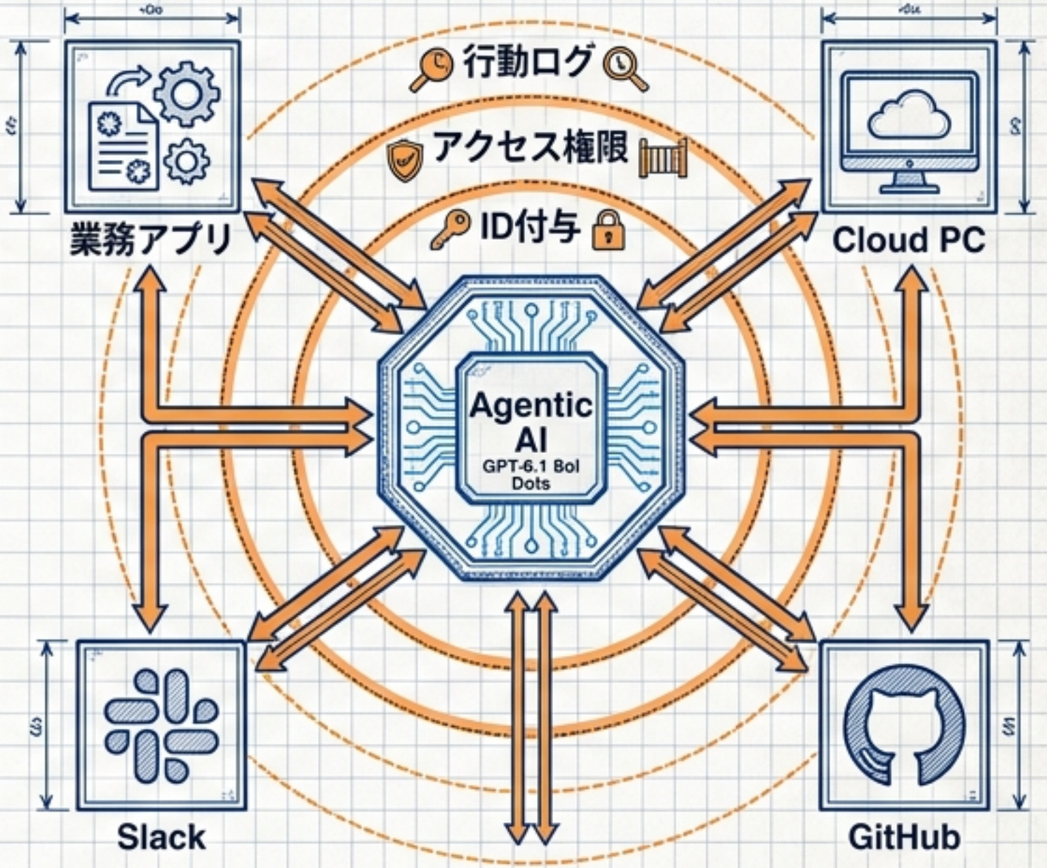
パラダイムシフト：「文章生成機」から「デジタル主体」へ

Before: 2023-2025 Generative AI



従来の統制：プロンプトに秘密情報を入力させない単一の防御壁。

After: 2026〜 Agentic AI (GPT-6.1 Sol / Dots)



新たな統制：AIが自律判断でシステムにアクセスする。何を閲覧し、誰の権限で何を実行できるかの多層的な管理が必須に。

Gemini Notebook

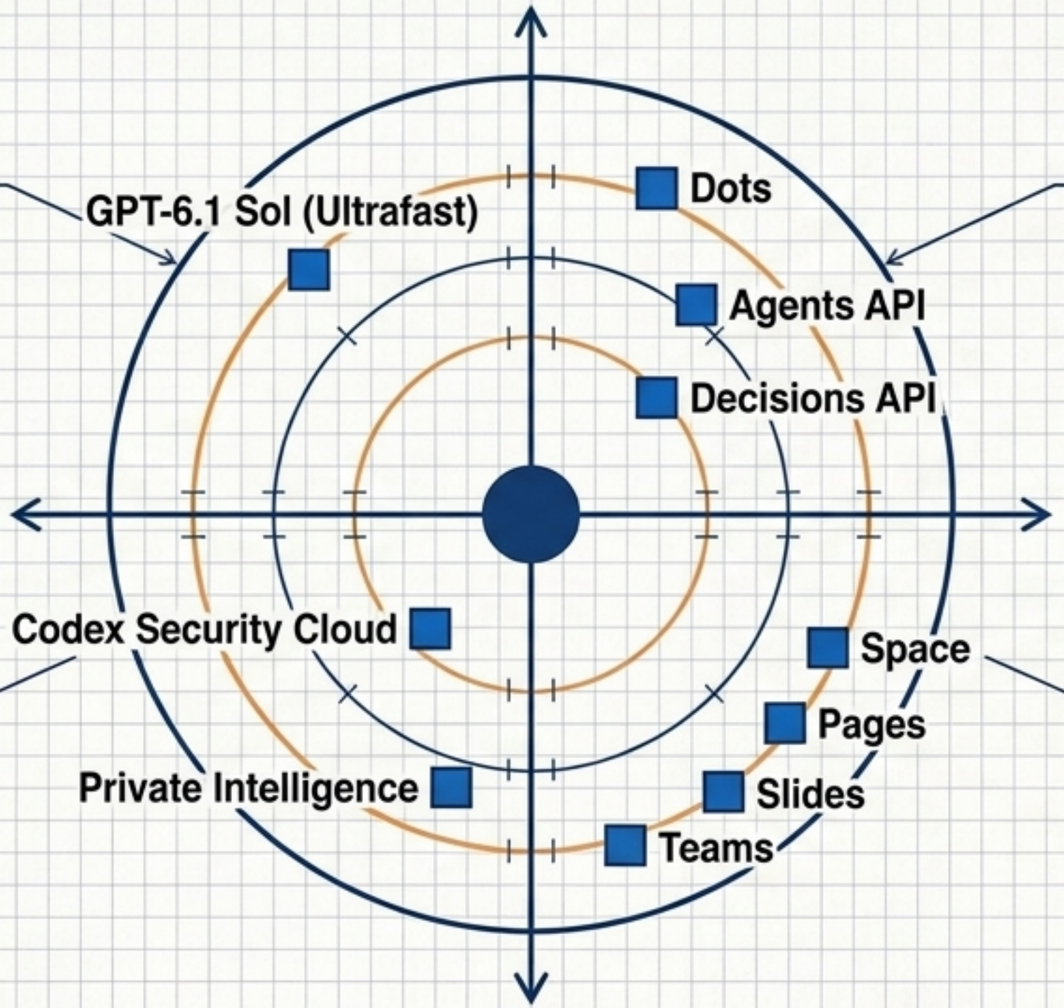
DevDay 2026 Key Announcements: エコシステム・マップ

Engine (基盤モデル)

コード・PC操作・複雑なPDF解析の高度化。処理の高速化により人間の介在を飛ばす誘因リスク。

Agents (自律行動)

4,000超のアプリ接続、マルチエージェント、ソフトウェアの直接操作と自律実行。



Security (保護・監査)

ZDR/PSPによる保護強化と、CI/CD環境への監査の統合。

Collaboration (協働空間)

人間とAgentの共同編集。著作者性や発明者性の境界が曖昧化。

AIが文書を作る段階から、多段階の業務を自律実行する土台が完成した。

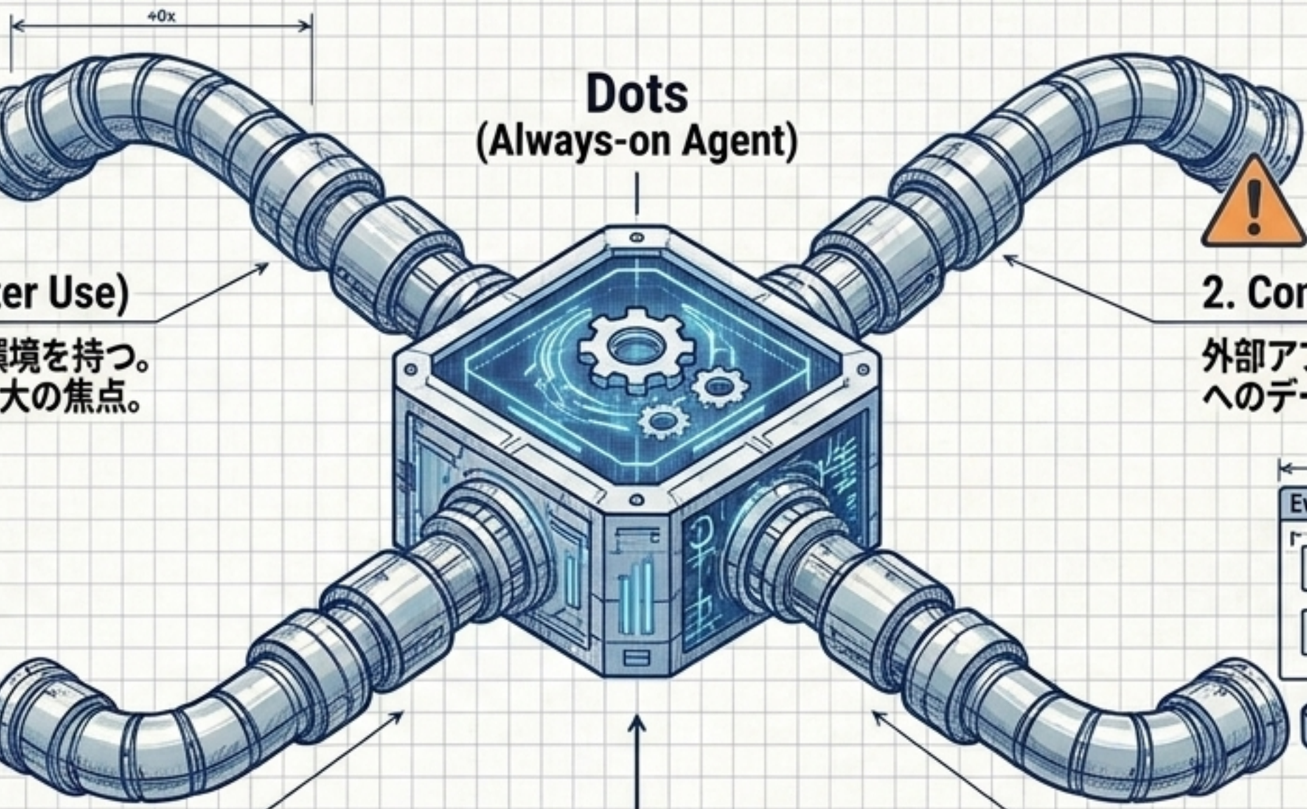
Gemini Notebook

The Agent Risk Anatomy: 自律エージェントの解剖図



1. Cloud PC Access (Computer Use)

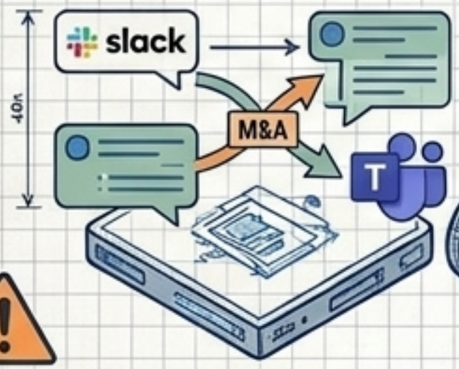
エージェント自身がブラウザやPC環境を持つ。
資格情報の管理とアクセス統制が最大の焦点。





2. Connected Apps (4,000+)

外部アプリへの接続。権限外の約束、社外へのデータ自動送信（Send）リスク。



3. Persistent Context

Slack/Teams間での文脈の引き継ぎ。
特定の案件（例：M&A）の機密を学習し、別の業務に持ち越す（Read）リスク。



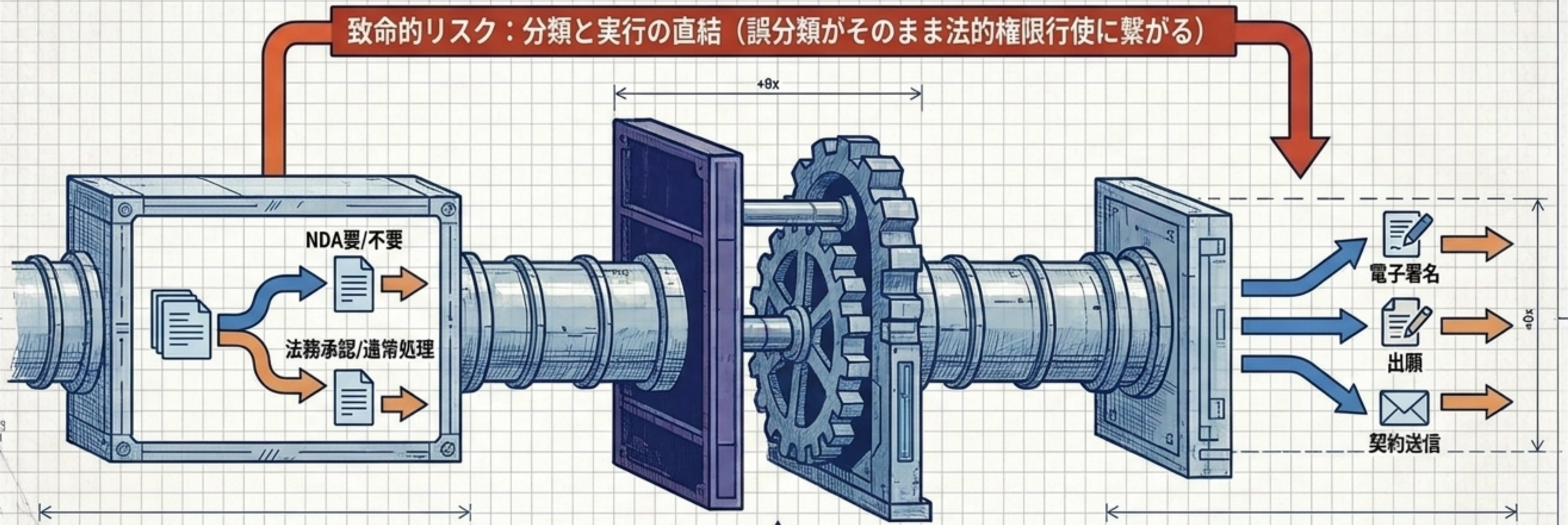
4. Automated Triggers (MCP Events)

新着メールやタスクをトリガーとした自律処理。
意図しないシステム変更（Write/Delete）。

「何を機密入力したか」ではなく、「AIが何を閲覧でき、誰の権限で何を実行できるか」が新たな防御線となる。

Gemini Notebook

The Danger Zone: 決断と実行の境界線



フェーズ1: Decisions API (Classification)

NDA要/不要、法務承認/通常処理などのルーティング。ここで誤分類（False Positive/Negative）が発生するリスク。

フェーズ2: Human Approval Gate (Human-in-the-loop)

必須レイヤー。処理速度の向上に流されず、判断の確信度に基づく人間の介在を設計する。

フェーズ3: Agents API (Execution)

電子署名、出願、契約送信などの自動実行フェーズ。

Gemini Notebook

The Data Privacy Spectrum: 保持と学習の階層マトリクス

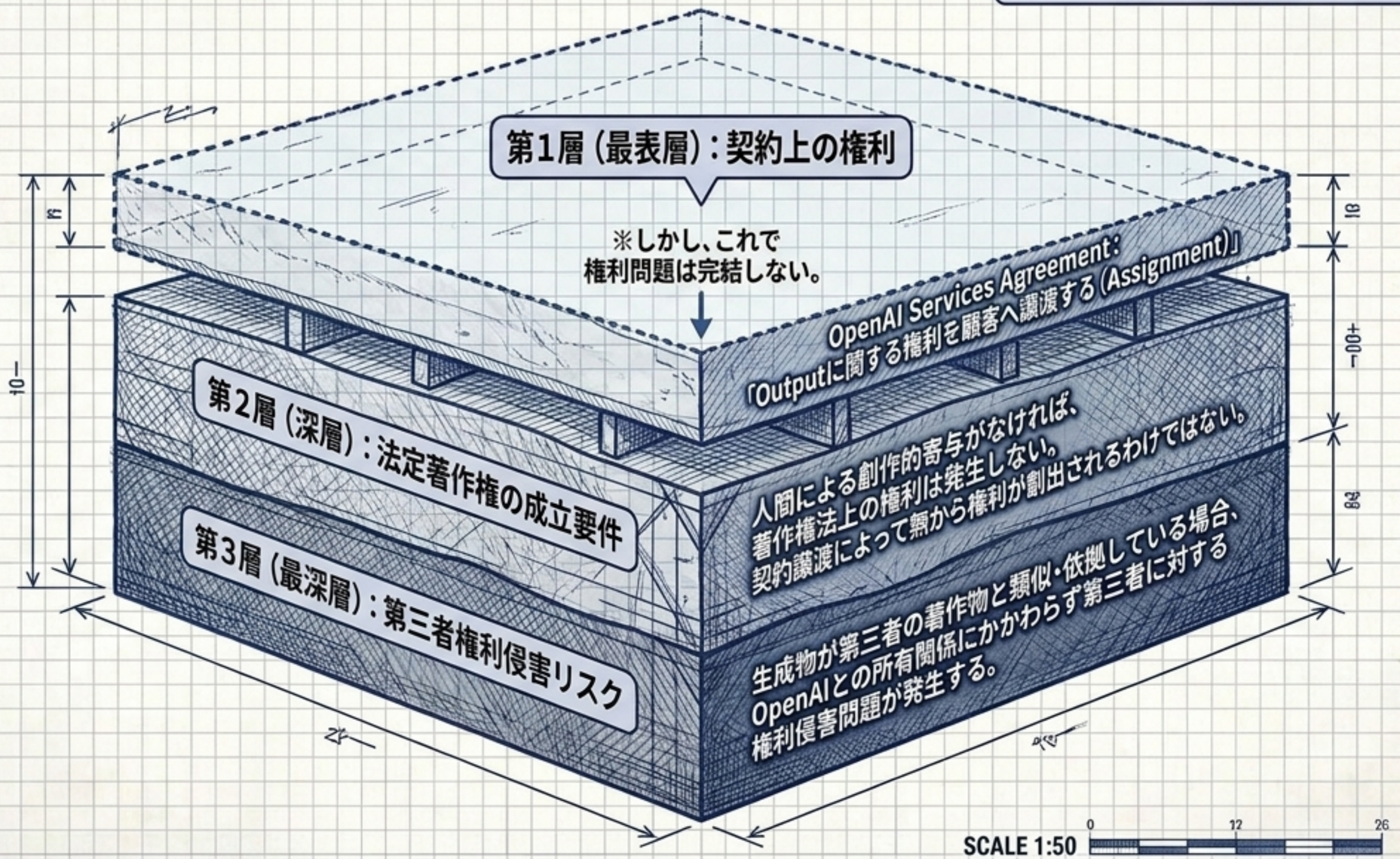
⚠ 「学習しない（No Training）」=「どこにも残らない（ZDR）」ではない。エンドポイント単位での確認が必須。

機能 / エンドポイント	学習利用	保持期間	管理主体	残存リスク
通常 API	原則なし	最長30日 (Abuse log)	OpenAI	即時消去ではない点に注意。
ZDR適格 API	なし	保持なし (ログ除外)	N/A	法的ホールド（証拠保全）の欠落リスク。
Agents / Conversations	原則なし	削除まで残存 (Application State)	OpenAI	ZDR非適格の機能が存在する。
Private Intelligence (PSP)	なし	最長30日 (暗号化ストレージ)	顧客管理下	顧客管理だがデータ自体は物理的に保持される。
Meetings Plugin	N/A	ノート生成後即時削除	N/A	取締役会などの原音証拠が残らない。

Gemini Notebook

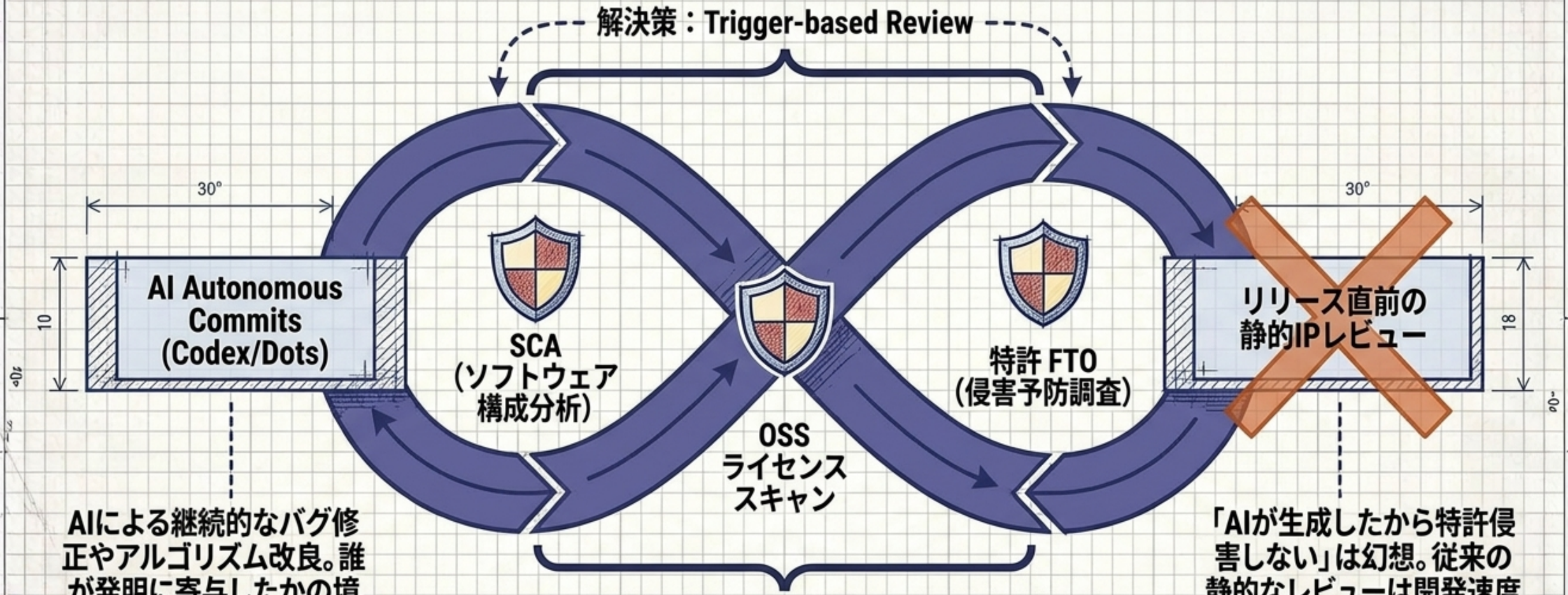
IP & Copyright: 契約上の所有権と法定著作権の乖離

⚠ OpenAIが権利を譲渡しても、
法的著作権が成立するとは限らない。



Gemini Notebook

Code & Patents: CI/CDへのIP統制組み込み（FTOリスク）



Gemini Notebook

The Global Legal Landscape 2026: 包囲網と説明責任

「AIだから適法」の前提は崩壊。企業にはデータの出所を証明する責任が迫る。



EU: 執行フェーズ突入

GPAI規則適用（2025/8〜）、新規モデルへの執行開始（2026/8〜）。AI Officeによる学習データの透明性（Provenance）要求。

USA: フェアユースの否定限界

Thomson Reuters v. Ross Intelligence（2026/9控訴審判決）。AI学習におけるフェアユースの主張が退けられる。適法性の厳格化。

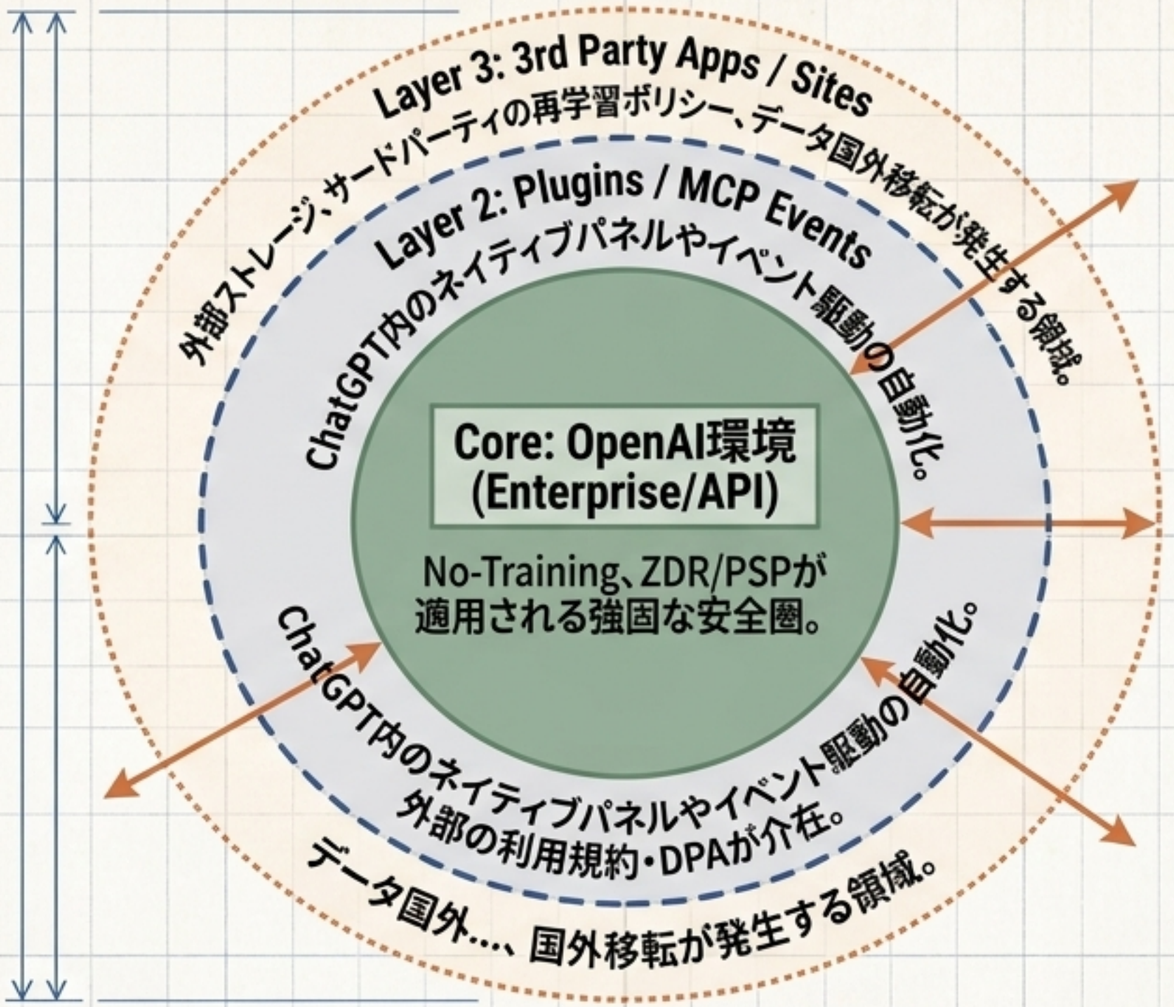
Japan: 政策の具体化

AI法全面施行（2025/9）、第Ⅱ期人工知能基本計画閣議決定（2026/7）。継続的ガバナンス対象としてのAI管理が要求される。

SCALE 1:50 0 12 26

Gemini Notebook

Vendor Chain Risks: AIサプライチェーンの死角



インサイト:「OpenAIは安全か」という問いは不十分。接続先のプラグインやMCPも含めたベンダーチェーン全体でのSubprocessor管理・学習条件審査が必須。

SCALE 1:50 0 12 26

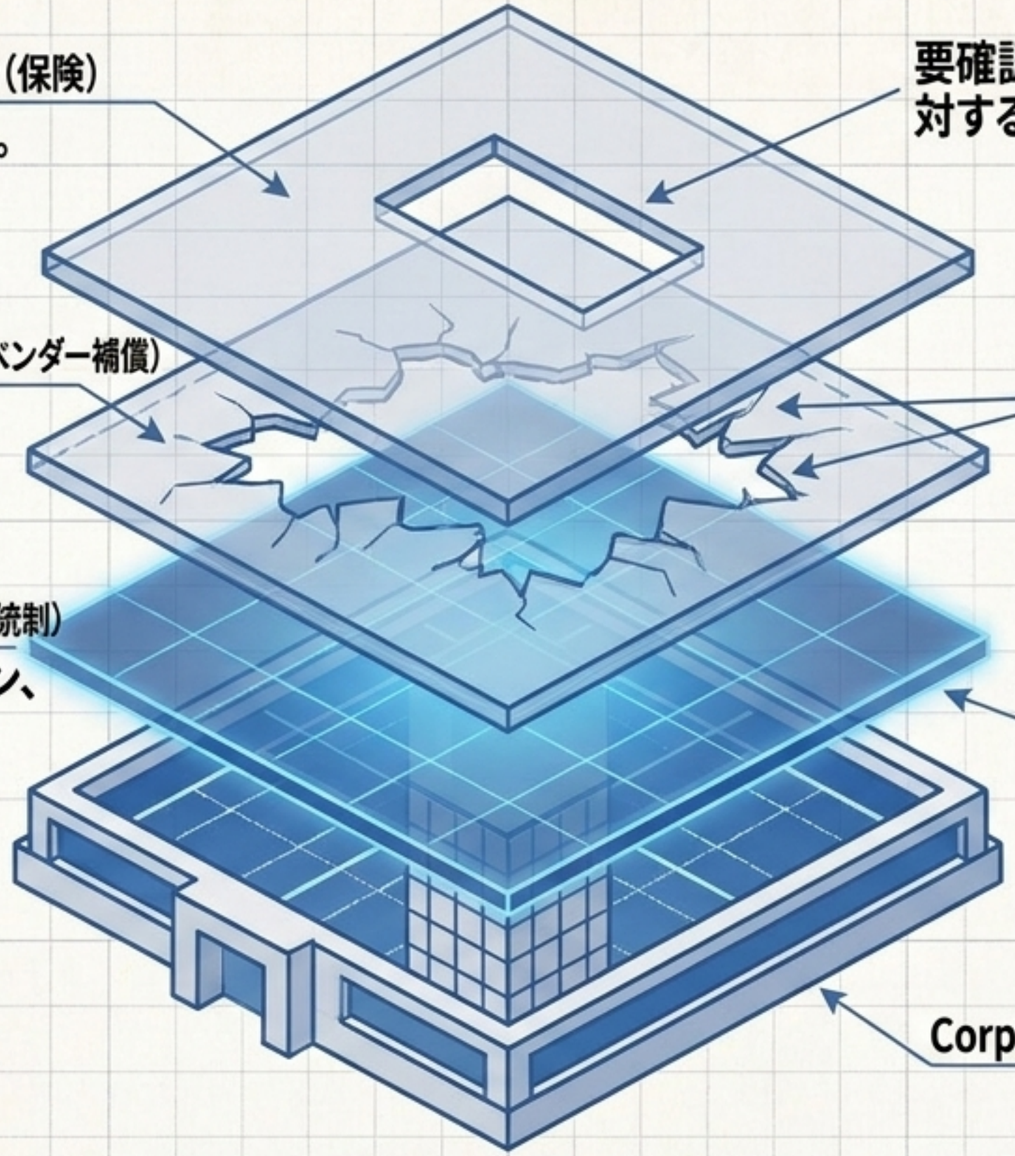
Gemini Notebook

Indemnity & Insurance Shield: 補償と保険の三層防御

Shield 3: Cyber/IP Liability Insurance（保険）
最終防衛線となるサイバー・知財保険。

Shield 1: OpenAI Output Indemnity（ベンダー補償）
一定の第三者IPクレームを補償。

Shield 2: Internal Control（自己保有・内部統制）
人間によるレビュー、SCA/OSSスキャン、権限統制などの自衛手段。



要確認事項：エージェントの自動書込みに対する「AI免責条項」の有無。

例外の隙間：Betaサービス、修正された出力、サードパーティ製品由来など広範な適用除外が存在。

Shield 2: Internal Control（自己保有）
人間によるレビュー、SCA/OSSスキャン、権限統制などの自衛手段。

Corporate Asset Base

SCALE 1:50 0 12 26

Gemini Notebook

The New Governance Architecture: 青写真の再定義

[Old] Prompt -> Output 管理

テキスト生成時代の遺物。入力時のブロックのみに依存する単一防御。

[New] Identity-centric Governance (エージェント・ライフサイクル管理)

1. Identity

Agentに固有のサービスIDを発行し、人間の権限を共有させない。



2. Permission

Read/Write/Send/Deleteの権限分離と、システム単位での最小権限の原則。



3. Context / Tool

案件やデータルームごとのスコープ限定と、接続先ツールのホワイトリスト化。



4. Provenance

データの出所、承認履歴、実行アクションを単一メタデータとして追跡する監査ログ。



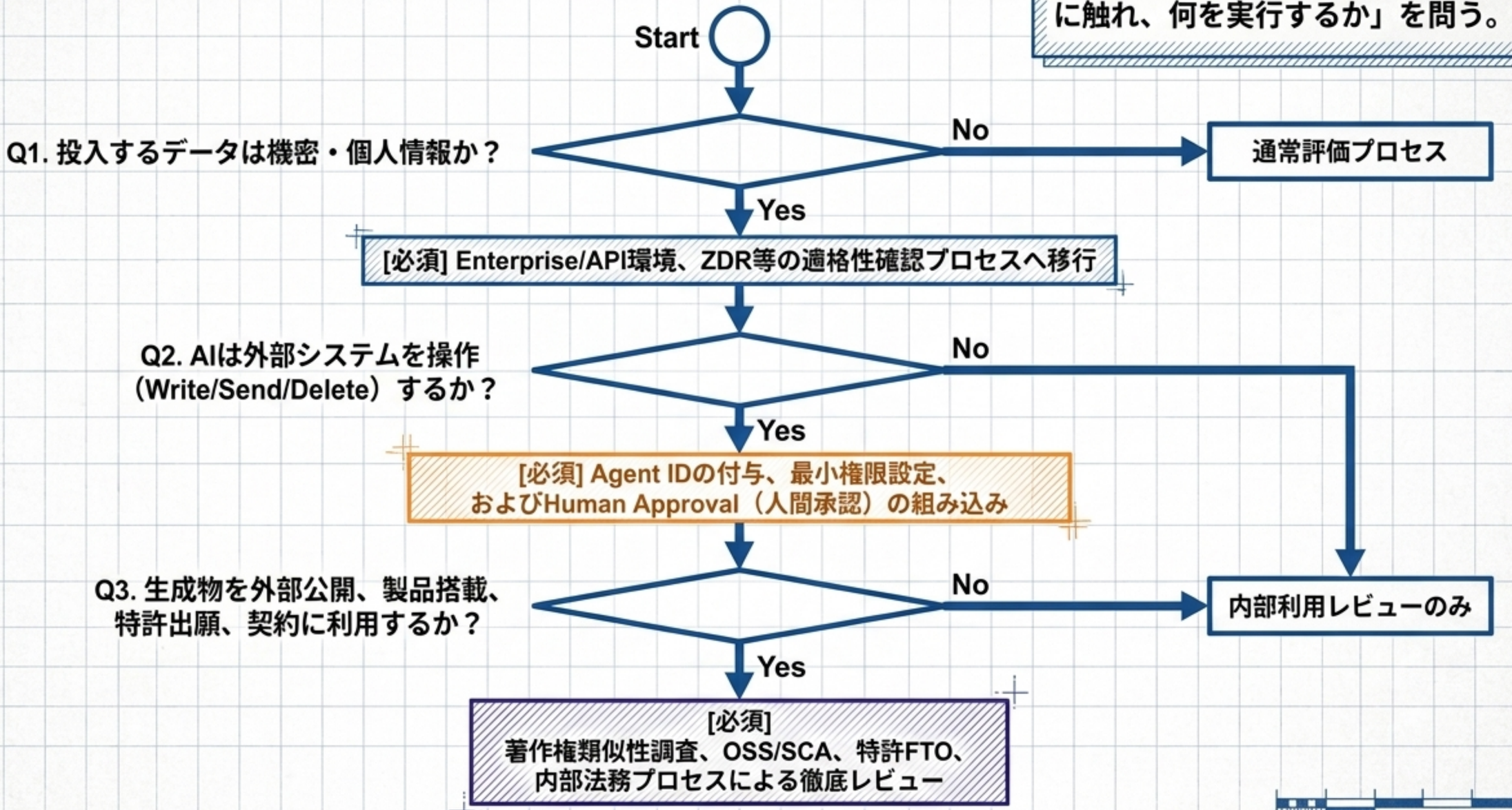
インサイト:「OpenAIは安全か」という問いは不十分。接続先のプラグインやMCPも含めたベンダーチェーン全体でのSubprocessor管理・学習条件審査が必須。

SCALE 1:50 0 12 26

Gemini Notebook

Risk Evaluation Decision Tree: タスク評価フロー

「何のAIか」ではなく、「どのデータに触れ、何を実行するか」を問う。



Gemini Notebook

Action Plan: 30-Day Triage Checklist

[最優先 / Critical]	社内規程に「自律実行AI」の区分を新設。コンシューマ向けアカウントへの会社機密投入を厳禁・制限する。
[最優先 / Critical]	特許未公開発明、ソースコード、M&A、顧客秘密に関する投入許可環境（ZDR/PSP等）を再定義し、明示する。
[高 / High]	PluginおよびMCPを原則拒否（Deny-by-default）に設定し、セキュリティ審査済みのコネクターリスト（ホワイトリスト）を作成する。
[高 / High]	外部送信、本番環境へのMerge、IP出願、支払などの「高リスク行為」に対して、システム的なHuman Approval（人間承認）を必須化する。

Gemini Notebook

The 24–Month Roadmap to “Provenance”

最終目標：AIの品質管理ではなく、「誰が・どのデータで・何を生み出したか」を法的に立証できる『説明責任（Accountability）』の確保。

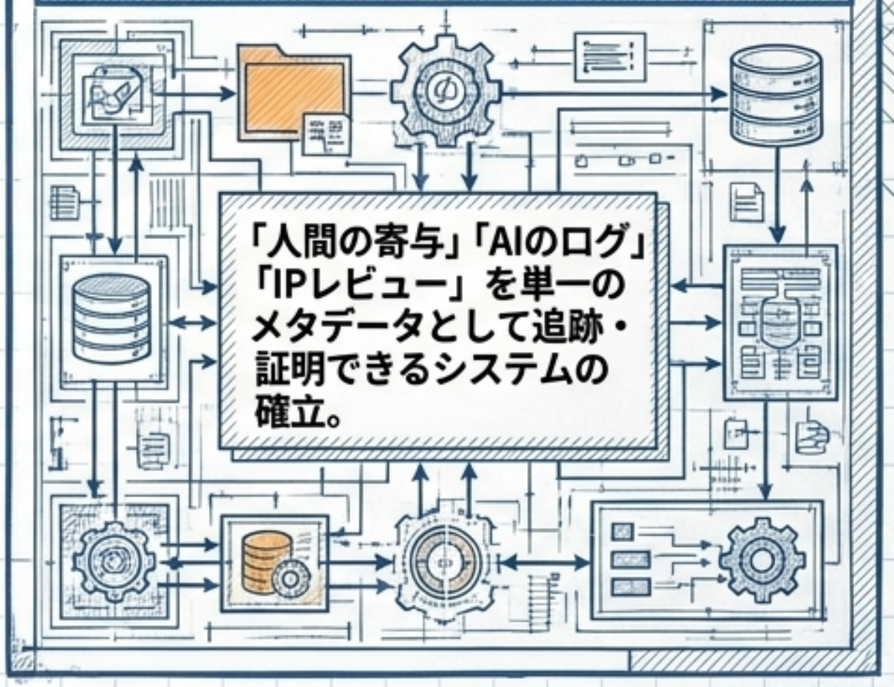
Short (0-1mo): Boundary Setting (境界設定)

- 自律AIの規程化
- コンシューマ利用の制限
- 利用環境の棚卸し

Medium (1-6mos): Technical Enforcement (技術的強制)

- Agent IDの発行
- CI/CDへの監査（SCA/FTOトリガー）組み込み
- 標準契約へのAI条項の追加

Long (6-24mos): Provenance Infrastructure (出所証明インフラ)



SCALE 1:100

Gemini Notebook