



プロンプト職人の終わり

2026年2月時点の技術・市場・制度変化に基づく分析報告

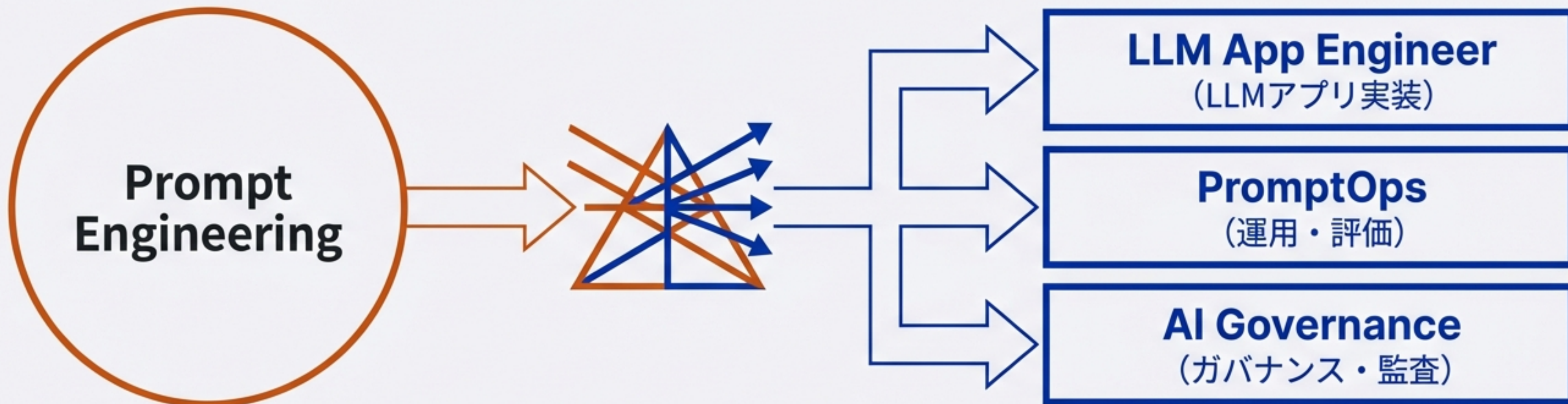
Word Craft
文言の工芸



System Design & Governance
システム設計・運用・ガバナンス

職人芸から、工学的な運用へ

Executive Summary



Key Drivers List



Technical

- 指示追従性の向上
- 「魔法の呪文」は不要に



Architectural

- 構造化出力
- チャットから仕様書へ



Operational

- 自動最適化 (APE/DSPy)
- 試行錯誤のアルゴリズム化



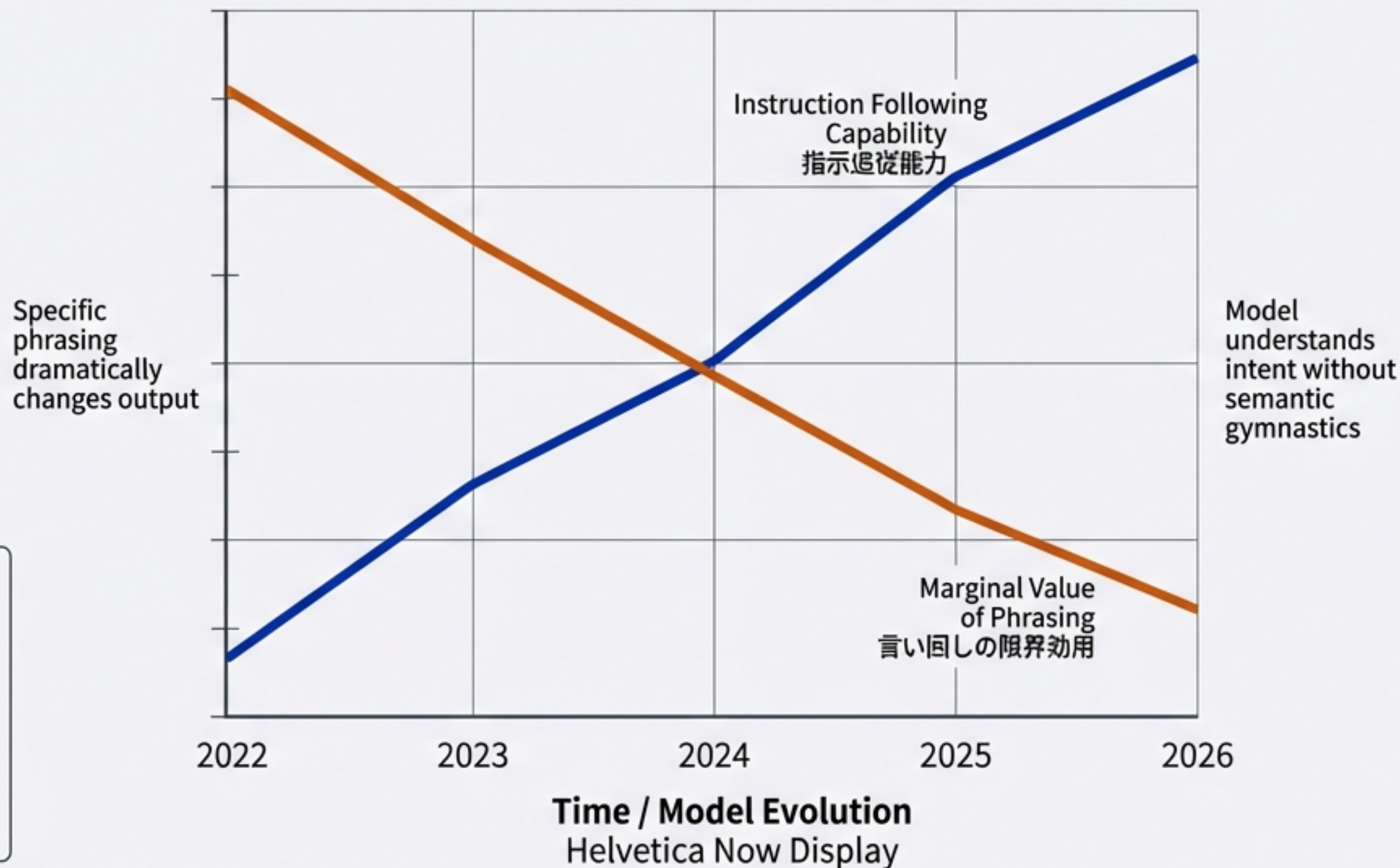
Regulatory

- 透明性と説明責任
- EU AI Actによる監査要求

モデルの進化が「呪文」の価値を希釈する

Insight:

初期のLLMでは「言い方」が性能を左右したが、モデルの指示追従性が向上した現在、平均的なプロンプトと専門的なプロンプトの性能差は縮小している。



自然言語から「仕様書」へ

From Conversation to Specification

2022: Chat / Conversation



あなたは優秀なライター
です。以下の条件で...



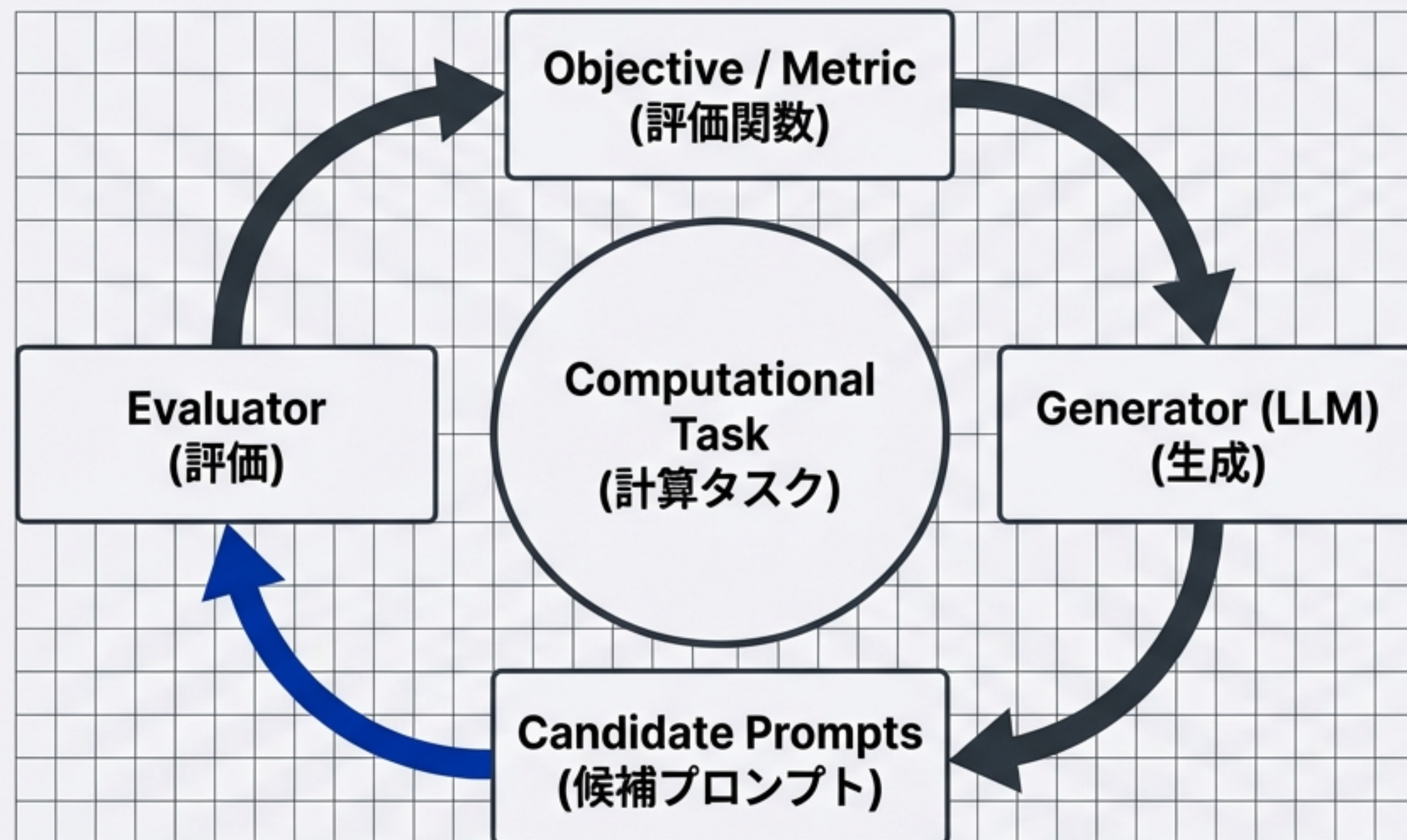
2026: Executable Schema

```
{  
  "role": "system",  
  "tools": ["calculator", "search_api"],  
  "response_format": { "type": "json_object" },  
  "constraints": "no_hallucination"  
}
```

プロンプトはもはや単なるテキストではない。入力データ、利用可能ツール（API）、出力スキーマ、制約条件を定義する「実行可能な仕様書」である。

試行錯誤のアルゴリズム化

Automatic Prompt Engineering & DSPy



Key Technologies List

- **APE (Automatic Prompt Engineer)**
 - プロンプト生成を探索問題として処理
- **DSPy**
 - プロンプトをプログラマ的に最適化・コンパイル
- **PromptBreeder**
 - 進化的アルゴリズムによる世代交代

「職人の直感は、エンジニアの評価関数に置き換わる」

「操作UI」から「監査対象」への変質

EU AI Act & Security Governance



Transparency (透明性)

EU AI Act (2026.08～)

誰が書き、どのデータを使い、どう決定したか。完全な文書化義務。

Security (セキュリティ)

OWASP Top 10

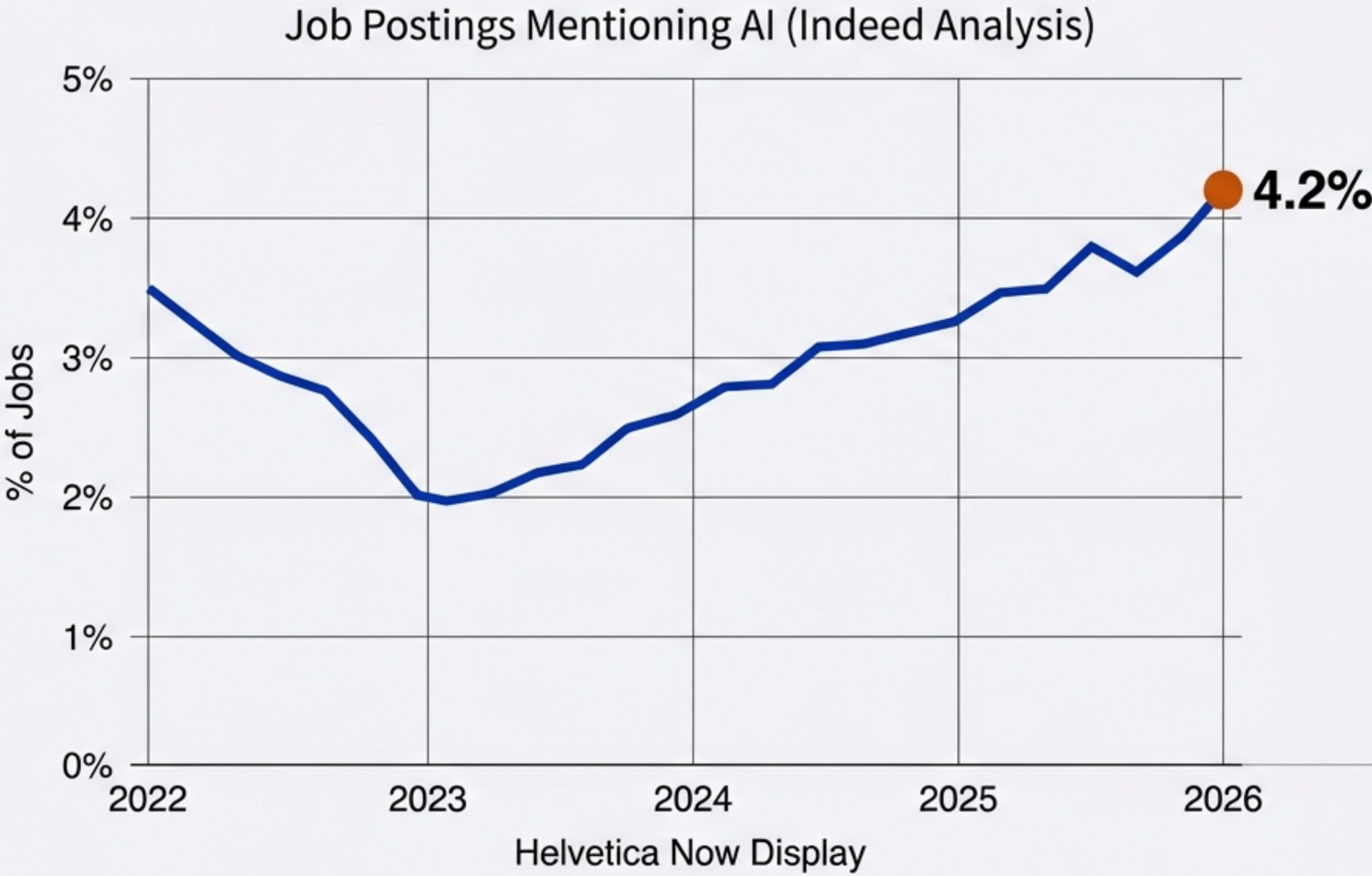
Prompt Injectionへの対策。プロンプトは攻撃対象領域である。

Governance (ガバナンス)

Policy as Code

バージョン管理、アクセスログ、変更履歴の保存。

需要は「消滅」せず「埋め込まれる」

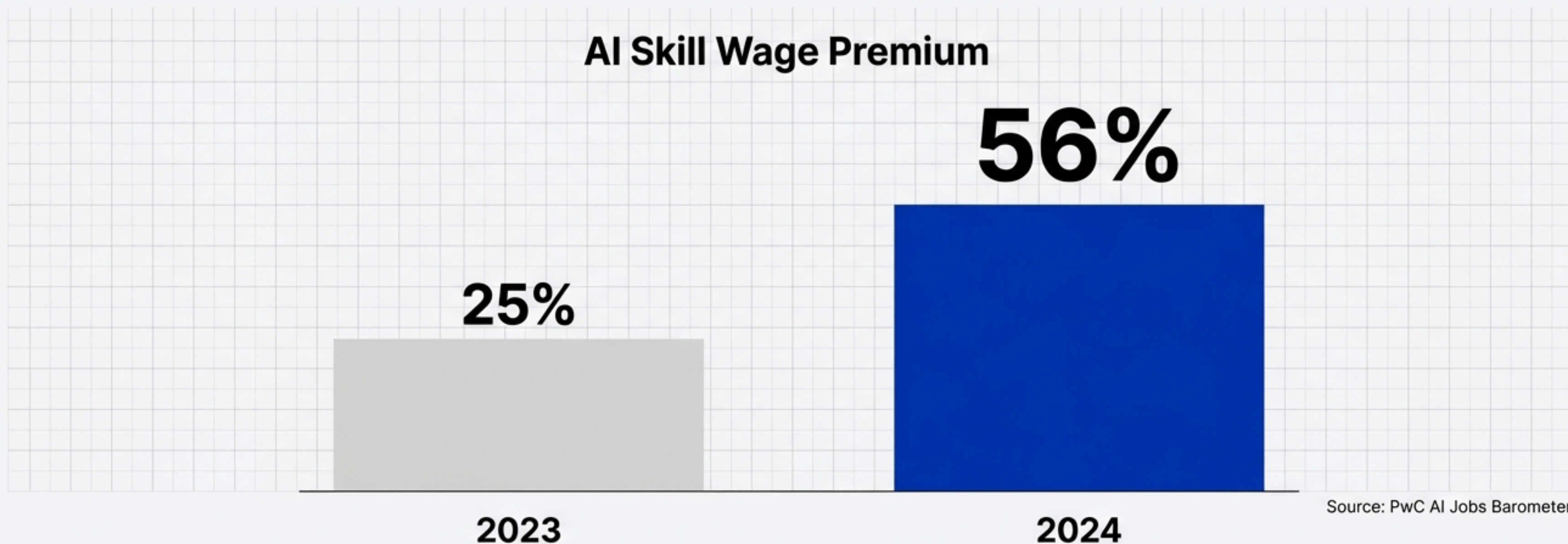


Demand is Embedding.

全体的な採用が弱含む中で、AIスキルへの言及は増加傾向にある。

特定の「プロンプト職」ではなく、マーケティング、人事、エンジニアリングなどの既存職種にAIスキルが必須化している。

バブル崩壊後の「スキルプレミアム」



What is the premium for?

プレミアムの対価は「テキスト生成」ではない。

「Operational Capability（運用能力）」

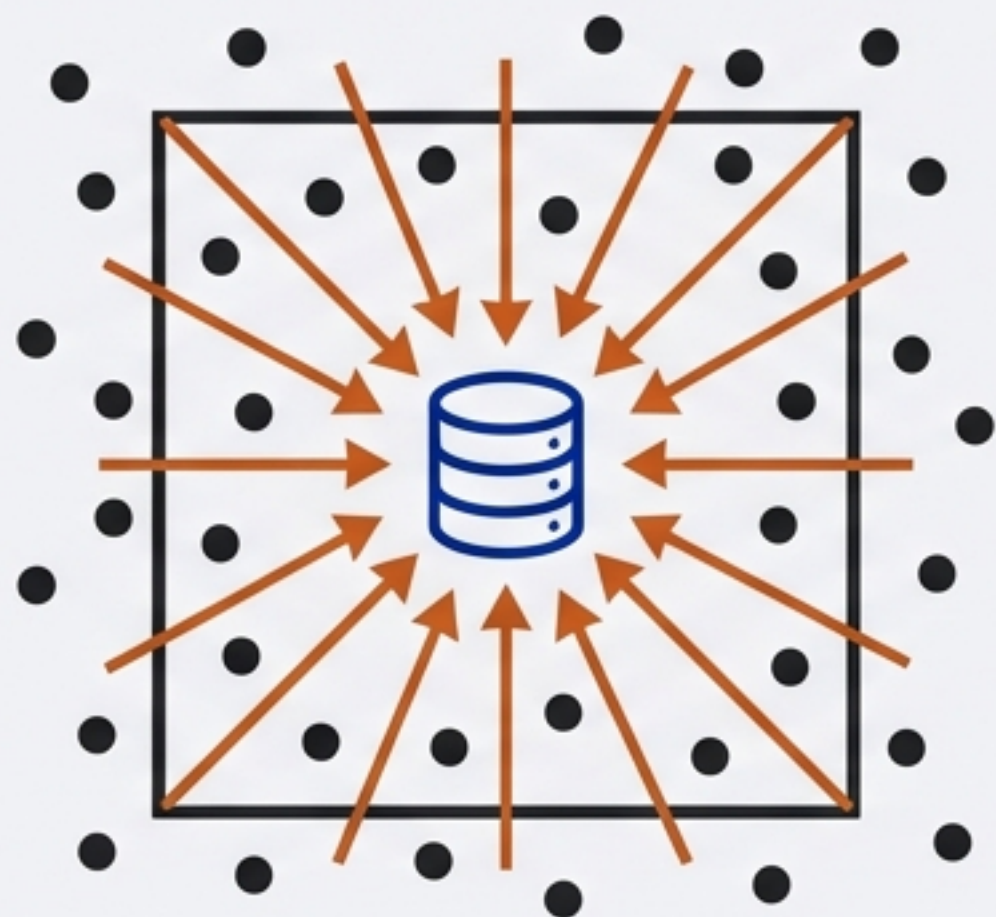
- ・再現性の担保 (Reproducibility)
- ・責任ある設計 (Responsibility)
- ・システム構築 (System Design)

日本市場の特殊性：組織知への昇華

形式知化 (Keshikichi-ka)

個人の「コツ (Knacks)」から、組織の「資産 (Assets)」へ。

日本企業はリスク回避と内部統制を重視するため、標準化された「PromptOps」との親和性が高い。



CASE STUDY: Hakuhood Technologies

2023年、300名規模のプロンプトエンジニアリング体制を構築。

- 組織的な教育プログラム
- 個人のスタープレイヤーよりも、全体の底上げ
- 「教育普及」→「慎重な実装」の2段階プロセス

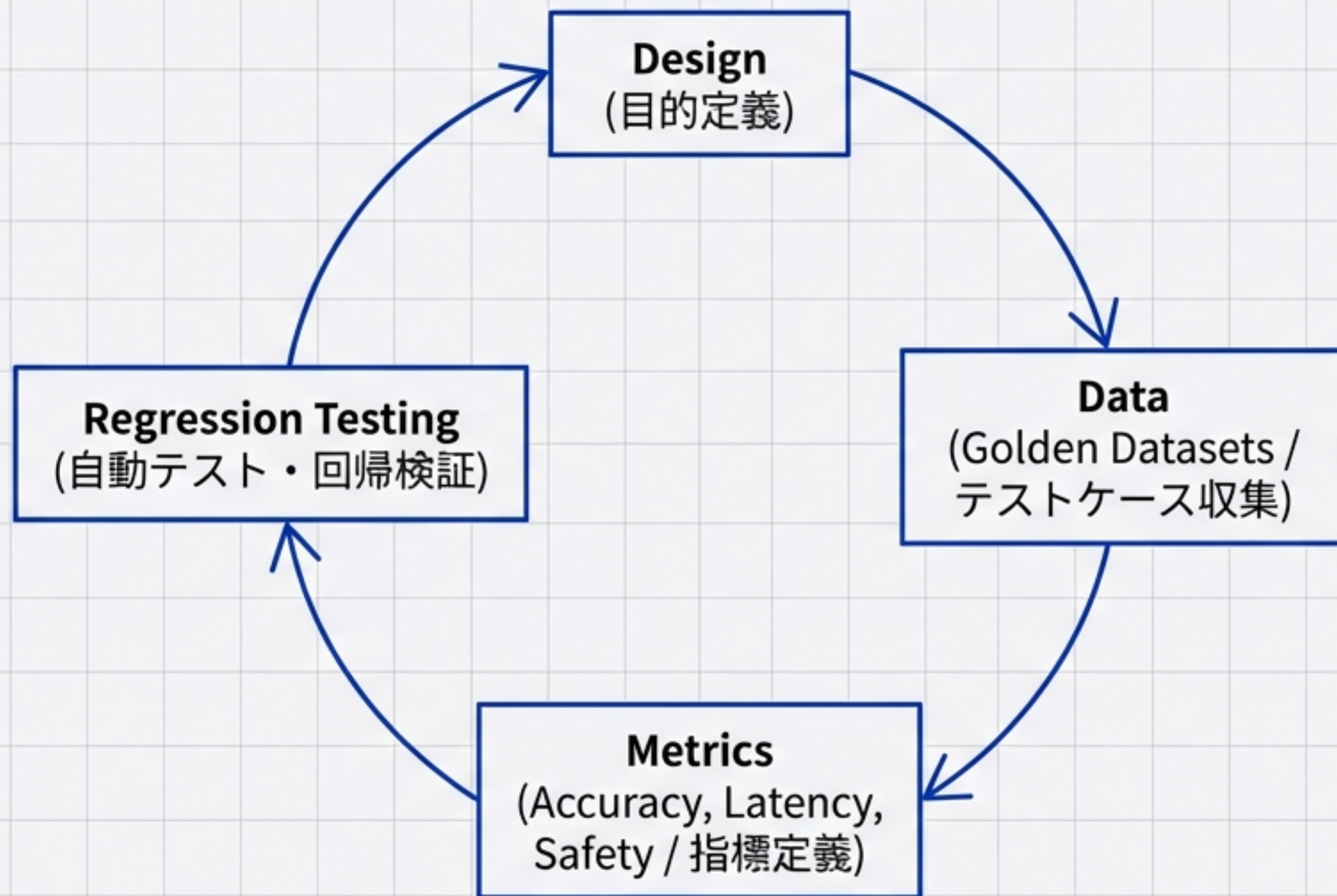
職能の再定義

Evolution of Roles

Prompt Artisan (Old)	LLM App Engineer (Current)	PromptOps / Governor (Future)
Output Text / Templates (テキスト・定型句) Noto Sans JP Regular Helvetica Now Display	Output Apps, RAG, Agents (アプリ・RAG) Noto Sans JP Regular Helvetica Now Display	Output Evals, Audit Logs (評価指標・監査ログ) Noto Sans JP Regular Helvetica Now Display
Value Trial & Error / "Magic" (試行錯誤・魔術) Noto Sans JP Regular Helvetica Now Display	Value Function Calling / Implementation (実装力) Noto Sans JP Regular Helvetica Now Display	Value Reliability / Reproducibility (信頼性・再現性) Noto Sans JP Regular Helvetica Now Display
Status Declining / Freelance (縮小・単発) Noto Sans JP Regular Helvetica Now Display	Status High Demand / Full-time (高需要・正社員) Noto Sans JP Regular Helvetica Now Display	Status Emerging / Strategic (戦略的・新興) Noto Sans JP Regular Helvetica Now Display

新たなコアスキル：「評価（Evals）」

“If you can't measure it,
you can't engineer it.”



推測をやめ、評価パイプラインを構築せよ。

セキュリティとガバナンスの設計

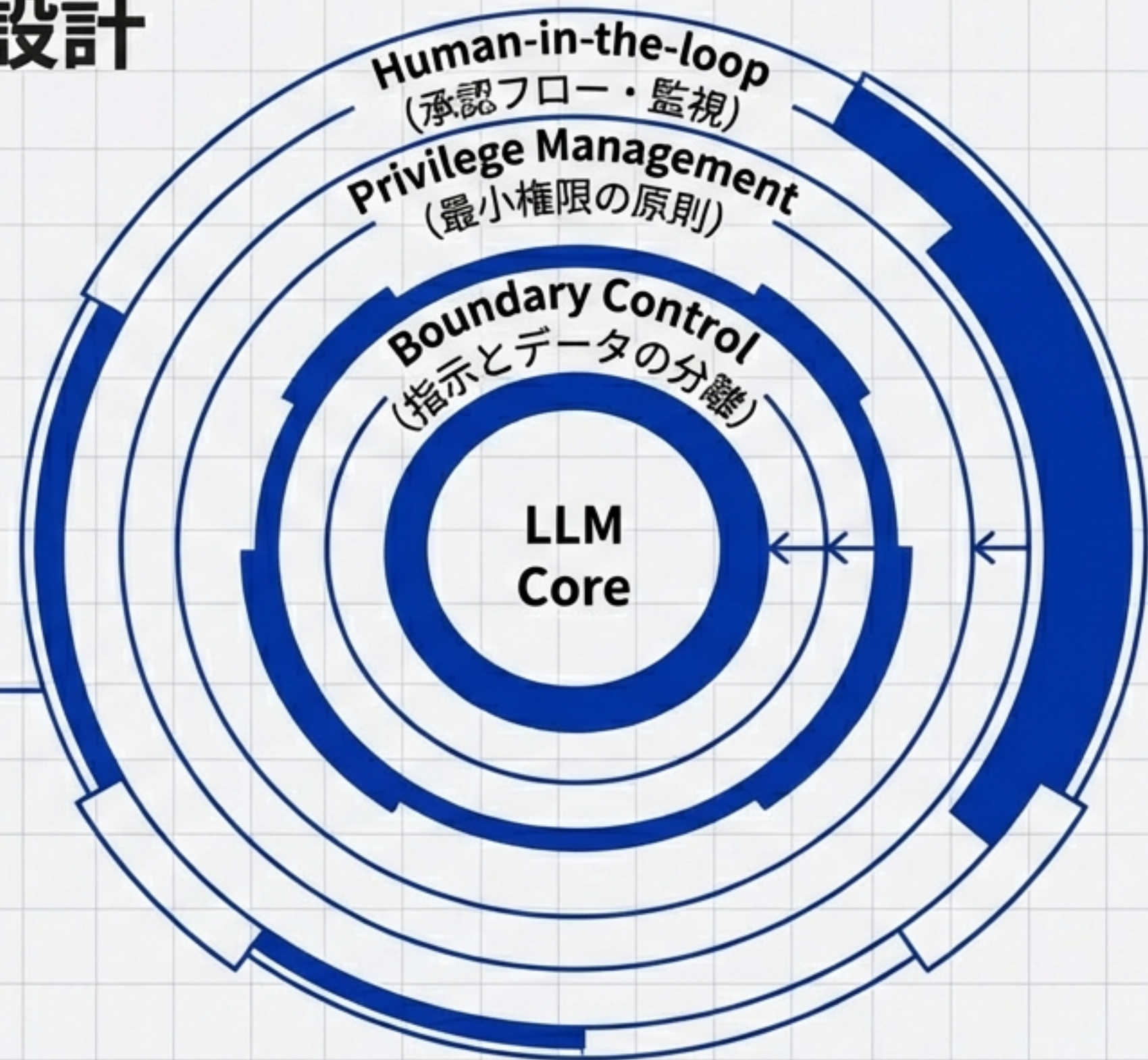
Risk Management

Key Risk: Prompt Injection (OWASP Top 10)

構造的に排除困難な脆弱性

Defense in Depth

防衛の多層化



価値の源泉は、AIを「刺激する」ことではなく、
システムを「保護する」ことに移行している。

将来シナリオ 2026-2035

Scenario A: Absorption (吸収統合) Probability: 55-60%		Scenario B: Polarization (二極化) Probability: 30%		Scenario C/D: Regulatory / Invisible	
プロンプト技術はソフトウェア工学の一部 (PromptOps) に完全に吸収される。		一般利用と、高度な専門領域 (レッドチーム・クリエイティブ) に二分される。		厳格な規制、またはOSレベルでの不可視化。	
60%		30%		10%	

組織への戦略提言

For Organizations

Hiring Action

Stop Hiring Wizards

「魔術師」を探すのをやめ、
「評価パイプライン」を構築
できるエンジニアを採用す
る。

Governance Action

Institutionalize Governance

EU透明性基準に備え、AI出
力の責任分界 (RACI) と監査
ログ基盤を整備する。

Security Action

Security First

プロンプトインジェクション
を前提とした、フェイルセー
フなワークフローを設計す
る。

個人へのキャリア提言

For Individuals

From Text to Product

プロンプト単体ではなく、動くアプリ、RAGシステム、自動化ワークフローを成果物とする。

Master the Audit

「なぜAIがそう動いたか」を説明し、著作権・データ系統・安全性を監査できる能力を身につける。

Become the Architect

職人（Artisan）から卒業し、システム全体の設計者（Architect）になる。

Helvetica Now Display
The End is the Beginning.