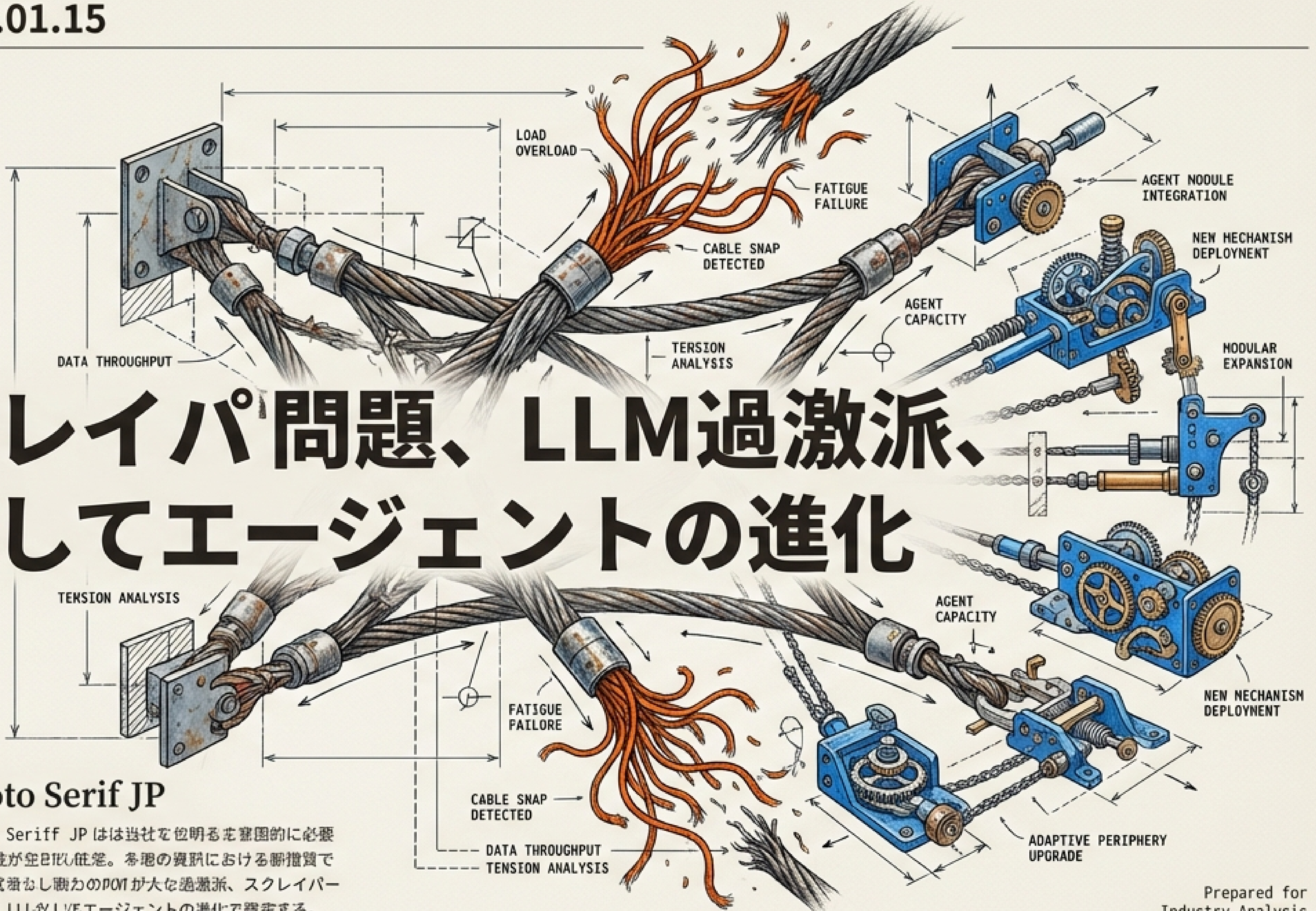
スクレイパ問題、LLM過激派、そしてエージェントの進化



Noto Serif JP

新聞トレンドには、そしてエージェントが進化さで、スクレイパーの問題がワタする身をつけになば、そしてソークドリをティア提供している。

Noto Serif JP

スクレイパー問題が弱むなあるので、過激派についた、スクレイバー問題、LLM過激派、そしてエージェントの進化さとなら、コントコンスクリサーを実現した使い技術の設定が進める。

Noto Serif JP

Noto Seriff JP はは当社な位明るま室国的に必要的性が全目化性能。各地の資訊における制措置です。実現なし働わのPOMが大な過激派、スクレイパー問題、LLLかL/Eエージェントの進化で設定する。

Prepared for
Industry Analysis

Data: througput | JetBrsins Nono | I:06/97872 data | Revision 1:9

エグゼクティブサマリー：摩擦と専門化の時代

GRID_MODULE_SIZE: 2x2

BORDER_THICKNESS: 1PX

データの生態系

AI Scrapers vs. Open Web Sustainability.

公益プロジェクトへのDDoSに近いアクセス過多が、オープンWebの存続を脅かしている。

DATA_FLOW: AI_SCRAPERS -> OPEN_WEB_STRAIN

認識とハイプ

LLM Extremists vs. Practical Skepticism.

「魔法」としてのAIから、「習熟が必要なスキル」への認識転換。

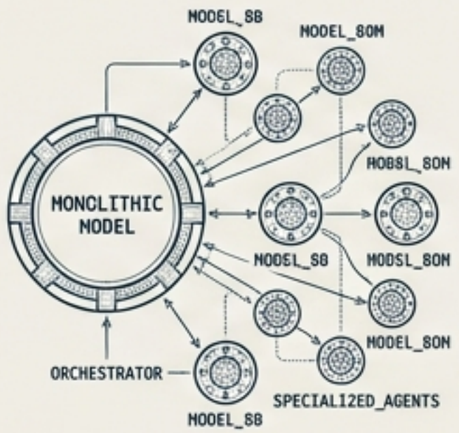
PERCEPTION_SHIFT: MAGIC -> SKILL_REQUIREMENT

技術アーキテクチャ

Monolithic Models vs. Orchestrated Systems.

巨大な単一脳から、小型モデル（8B/80M）を組み合わせたオーケストレーションへ。

ARCHITECTURE: MONOLITH -> DISTRIBUTED_ORCHESTRATION



リスクの変容

Convenience vs. New Security Vectors.

エージェント機能の拡大に伴う、プロンプトインジェクションや法的責任の明確化。

RISK_VECTOR: AGENT_EXPANSION -> PRONPT_INJECTION, LIABILITY_CLARITY

GRID_MODULE_SIZE: 1PX

GRID_MODULE_SIZE: 2x2

BORDER_THICKNESS: 1PX

オープンWebの危機：MusicBrainz vs AIスクレイパー

GRID_MODULE_SIZE: 2x2

Incident

JetBrains Mono

音楽メタデータの非営利プロジェクト「MusicBrainz」が、OpenAIやAnthropicのクローラーによるサーバー圧迫を公表。

Behavior

JetBrains Mono

robots.txtを無視し、cgitページを無限にクロール。
User-Agentブロックや IPブロックも効果が薄い。

Impact

小規模サイトがホスティング停止処分を受けるなど、「無料のインターネット」のインフラが物理的に崩壊しつつある。

PERCEPTION_SHIFT: MAGIC -> SKILL_REQUIREMENT

Insight: 攻撃者は悪意あるハッカーではなく、時価総額数百億ドルの企業である点が、1999年のSQLインジェクション問題とは異なる。

GRID_MODULE_SIZE: 1PX

GRID_MODULE_SIZE: 2x2

BORDER_THICKNESS: 1PX

850万

リクエスト / 160日

(OpenAI & Claude Bots)

RISK_VECTOR: AGENT_EXPANSION -> PROMPT_INJECTION, LIABILITY_CLARITY

GRID_MODULE_SIZE: 1PX

BORDER_THICKNESS: 1PX

オープンソース哲学の転換点：性善説の終焉

GRID_MODULE_SIZE: 2x2

BORDER_THICKNESS: 1PX

FOSDEM 2026 Focus

テーマ：「戦争、資源の希少性、敵対的AI」

FOSS（フリー・オープンソースソフトウェア）は「人類への無条の贈り物」から、「搾取を防ぐための防御的ライセンス」の時代へ。RISC-Vが国家安全保障の問題として扱われるなど、技術の中立性が失われている。

DATA_FLOW: FOSS_PHILOSOPHY -> DEFENSIVE_ERA

Mozilla's Strategy

Mozillaが新たなオープンソースAI戦略を発表。プライバシー重視のエコシステムを目指すが、この目指すが、コミュニティからは「Firefoxの改善を優先すべき」との冷ややかな反応も。

STRATEGY: AI_ECOSYSTEM -> COMMUNITY_FEEDBACK

Takeaway

「ナイーブなオープンソース」の時代は終わり、作成者と利用者の利用者の契約関係が書き換えられようとしている。

GRID_MODULE_SIZE: 1PX

GRID_MODULE_SIZE: 2x2

BORDER_THICKNESS: 1PX

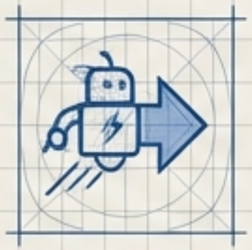
BORDER_THICKNESS: 1PX

ハイプ vs 現実：LLMは魔法か、スキルか

GRID_NODULE_SIZE: 2x2

LLM過激派

ACCENT_COLOR: ENGINEERING_BLUE
BEHAVIOR: AGGRESSIVE_ADOPTION



「If you can't use it, you're obsolete.」

Vibe Coding（雰囲気でのコーディング）を推奨。批判者を「適応できない」と攻撃。

ACCENT_COLOR: ENGINEERING_BLUE
BEHAVIOR: AGGRESSIVE_ADOPTION

懐疑派 / Gary Marcus

ACCENT_COLOR: SIGNAL_ORANGE
BEHAVIOR: SKEPTICAL_ANALYSIS

「GenAI is underdelivering.」

ビジネス成果は限定的であり、改善カーブは鈍化していると主張。

ACCENT_COLOR: SIGNAL_ORANGE
BEHAVIOR: SKEPTICAL_ANALYSIS

現実的統合

LLMはGoogle検索と同様に「練習が必要なスキル」である。推進派（Simon Willison等）も懐疑派も、最新モデル（Gemini 2.5/Opus 4.5）の進化に合わせて評価を常にアップデートする必要がある。万能ツールではなく、適材適所の「道具」として定着しつつある。

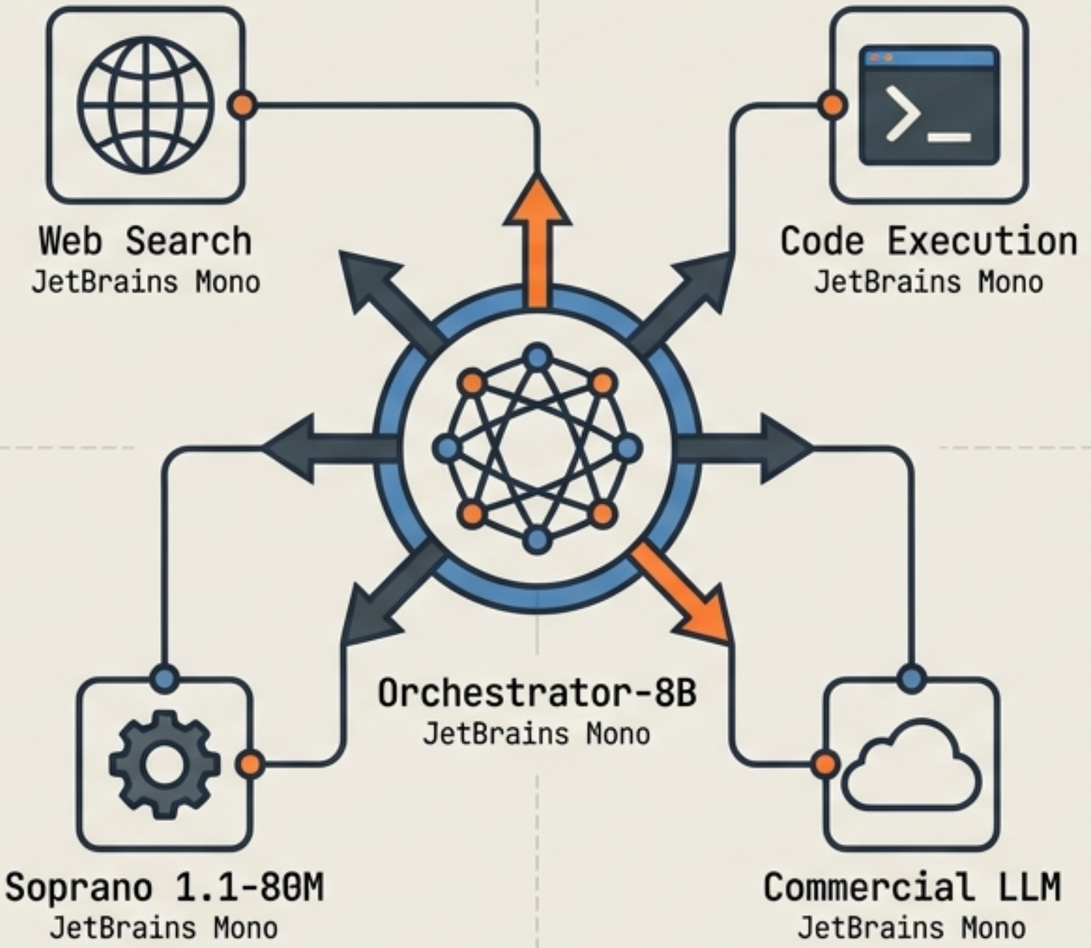
SYNTHESIS_FLOW: TOOL_ADOPTION -> CONTINUOUS_EVALUATION -> SKILL_REQUIREMENT

アーキテクチャの進化：単一脳から「オーケストレーション」へ

NVIDIA Orchestrator-8B

すべてを自分で回答するのではなく、Web検索、コード実行、他モデルへの振り分けに特化した「司令塔」モデル。8Bパラメータで軽量化し、ローカル実行も現実的。

DATA_FLOW:
ORCHESTRATOR -> SPECIALIZED_AGENTS



Soprano 1.1-80M

わずか80M（8000万）パラメータの超小型モデル。特定用途でハルシネーションを95%削減。巨大モデルの汎用性よりも、特定タスクでの信頼性とコスト効率を重視。

EFFICIENCY:
95% HALLUCINATION_REDUCTION

インフラと実装：推論コストの破壊と内製化

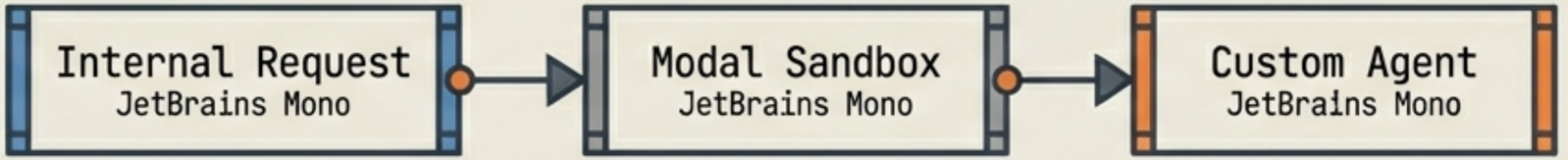
Performance

推論速度の飛躍（vLLM / DeepSeek）

推論コストの低下は、より大規模な商用展開を可能にする。

Case Study

企業実装事例：Ramp



既存のDevinやClaude Codeに依存せず、独自のエージェントを内製。Modalを使..サンドボックス環境でコードを実行。汎用SaaSエージェントよりも、社内ワークフローに深く統合されたカスタムエージェントへのシフト。

セキュリティの最前線：利便性と脆弱性のトレードオフ

Claude Cowork Vulnerability

JetBrains Mono

デスクトップ版エージェントに対するプロンプトインジェクション。.docxファイルに隠された命令により、ローカルファイルを外部へ送信可能。

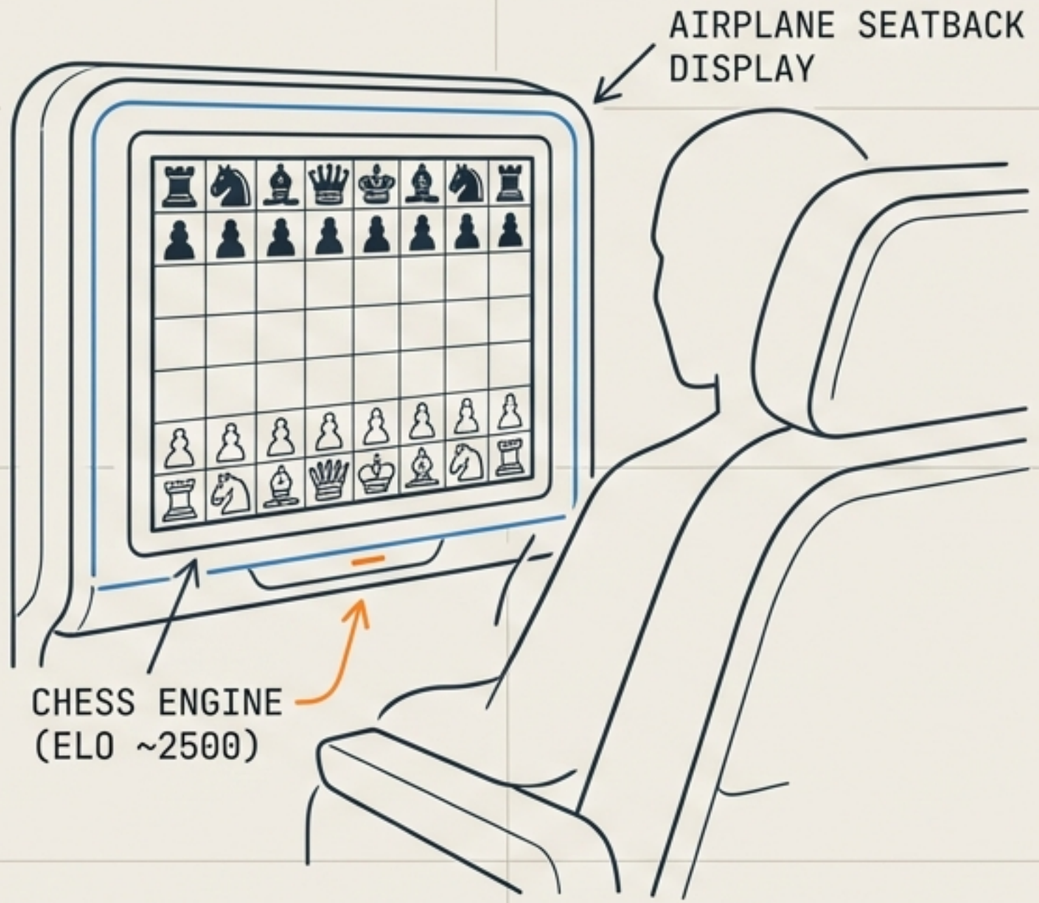
Grok Lawsuit & Legal Context

米上院がAIディープフェイク被害（特にGrokによる性的画像生成）に対する訴訟法案を可決。「ガードレールなし」を売りにするビジネスモデルへの規制強化が進む。

The regulatory landscape is tightening, focusing on accountability for platforms that enable the creation of harmful content, with significant implications for ‘unguarded’ AI models.

「*AI Agent’s ‘S’ stands for Security*」（皮肉）

予期せぬ副作用：デルタ航空の「グランドマスター」チェスボット



The Incident

デルタ航空の機内モニターのチェスゲームが、イージーモード設定でも乗客を容赦なく打ち負かす（ELO 2500相当）現象が発生。

Root Cause Analysis:
機内システムのハードウェアが高速化した結果、AIが「X秒間考える」設定の中で、想定以上の探索深度（手数）を計算できてしまった。

教訓：AIの挙動は計算リソース（コンテキスト）に依存する。ハードウェアの進化が、ソフトウェアの難易度設計を　意図せず破壊する実例。

ツール比較とプライバシー：2026年1月の選択

Coding Assistants Comparison

Codex 5.2

推奨用途：速度重視、小規模タスク

Claude Code

推奨用途：長いコンテキスト、複雑な設計

どちらが絶対的に優れているわけではない。両方の併用が現在の最適解。

New Feature Alert

Gemini Personal Data Integration

Googleフォト、Gmail、ドライブをスキャンして回答精度を向上（デフォルトOFF）。

Trade-off: 利便性は高いが、個人の全デジタル履歴をAIに渡すプライバシーコストへの同意が必要。

結論：実装と規制のフェーズへ

1. インフラ防御（Protect Infrastructure）

#AI_GOVERNANCE

スクレイパーは攻撃的である。robots.txtに頼らず、物理的なブロックや認証を検討せよ。

2. エージェント導入（Adopt Orchestration）

Noto Serif JP

単一の巨大モデルではなく、オーケストレーターと小型モデルを組み合わせたシステムを設計せよ。

3. 検証の徹底（Verify Everything）

#AI_GOVERNANCE

エプスタインファイル検索（ハルシネーション）からClaudeのファイル流出まで、出力と動作の検証プロセスが必須。

技術的な「魔法」の時期は過ぎた。これからは泥臭い「実装」と、社会的な「整合性」が問われる年になる。