

知財AIエージェントの安全運用を支える「ハーネス設計」の6大原則

知財業務におけるAI活用では、LLMの賢さ以上に「モデルを信用しなくても事故が起きない統制層（ハーネス）」の設計が最重要。
未公開発明や営業秘密等の漏えいを防ぎ、法的効果を生む誤操作を防止する原則と構造。

