日本版AISIの体制強化とAIサイバー能力評価の最前線

日本版AISIの体制強化と日英米比較

予算88億円・将来200人体制を目指す抜本的強化

令和7年度補正予算で88億円を措置し、
段階的に人員を拡充予定。



日本 (Japan)
制度的基盤構築が途上



英国 (UK)



米国 (US)

200人規模の英国や先行アクセスを持つ
米国に対し、ギャップが存在



Safety
(安全性)



Security
(セキュリティ)

「Safety」から「Security」への重点転換

サイバー攻撃対応を重視し、独自の評価環境やテストベッド整備を推進。

AIモデルのサイバー能力評価と企業への示唆

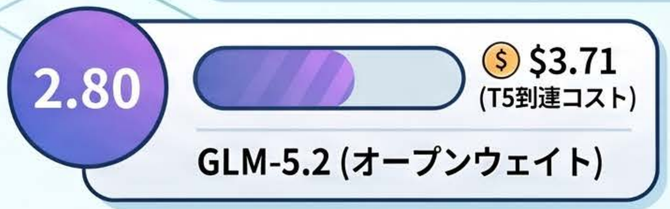


商用モデルがオープンモデルの性能を凌駕

ExploitBench評価でOpus 4.8が最高スコアを獲得。







オープンモデルへの高度能力拡散は未断定

GLM-5.2の最高到達はT3止まりで、
現状広汎な拡散とは言えず。

企業に求められるAI脆弱性対策と運用管理



既知脆弱性の修正
徹底



AI診断時の評価条件
記録・独自保護が必要



Gemini Notebook