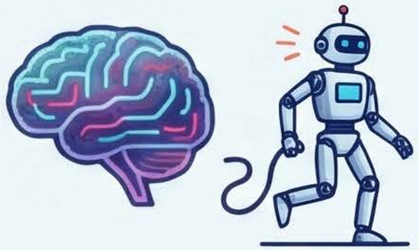
AI「爆速進化」に抗うガバナンス：日本が選ぶべき「AI主権」への道

AIの技術進化（月単位）と法整備（年単位）の速度差を前提に、AIを「罰する」のではなく、人間側の「組織・インフラ設計」を再定義する日本独自の戦略を解説します。

生成AIがもたらす3つの主要リスク



AI自体の「誤作動」と「エージェント化」

幻覚（ハルシネーション）に加え、AIが勝手に動き出す自律性のリスクが上昇中。

攻撃の「武器」としての悪用

サイバー攻撃の敷居を下げ、専門知識がなくても高度なハッキングが可能に。

社会を揺るがすシステミックリスク

先進国の雇用の60%がAIに曝露し、格差や力の集中を招く。

主要国・地域のAIガバナンス戦略の比較

	優先性	方法
米国	膿条力・国家安全保障	大統縲令・調連・輸出管理
EU	基本槙・安全・透明性	AI法（ハードロー）・罰全
中国	産業振興・国家管理	登録制・行政指導
日本	利活用促進・国際視籍	促進法・ガイドライン・評価

日本の「AI主権」戦略と3年計画

「国産AI」から「AI主権」への転換

全自前主義ではなく、外部モデルを使いつつ管理・監査権を確保する。

ソフトロー（指計）による柔軟な統制

罰則より、情報の共有とアップデートを重視した機動的なルール作り。

[TIMELINE_EVENT]

実効性を高める3カ年ロードマップ

1年目
利用台帳化

2年目
分野別指計

3年目
責任・保険制度の確立