

[MAIN HEADING]

防衛インテリジェンスにおけるAI主権の確立と実証

Sakana AIによる公開情報（OSINT）
分析エージェントの全貌と戦略的意義

[AGENCY]
防衛省 / 防衛装備庁
(情報本部)

[VENDOR]
Sakana AI株式会社

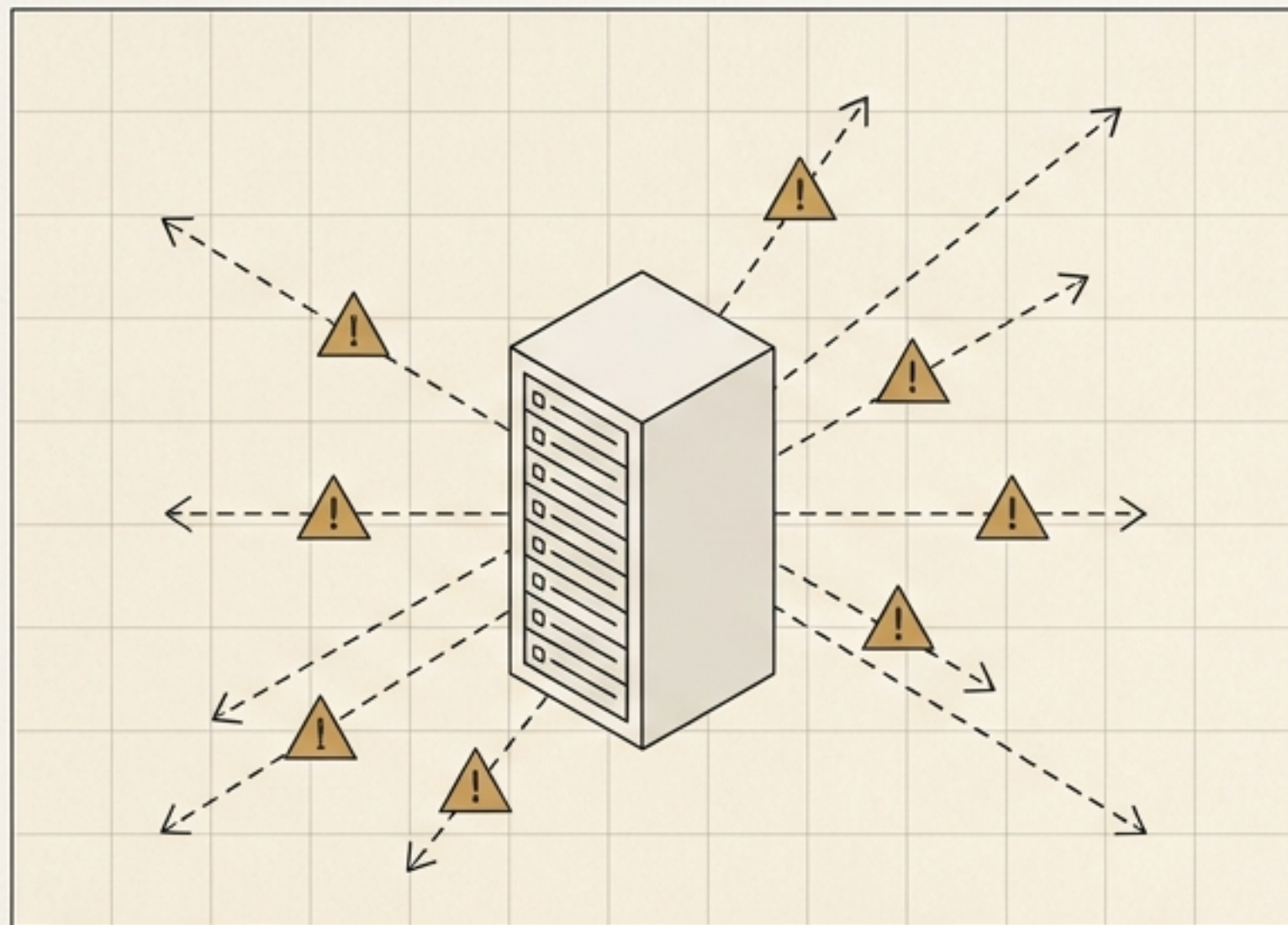
[CONTRACT_VAL]
¥329,032,000

[TIMELINE]
2026.07 – FY2027 末

[SCOPE]
総合分析業務に必要な
AI機能の調査・実証

[STATUS]
ACTIVE_PROTOTYPING

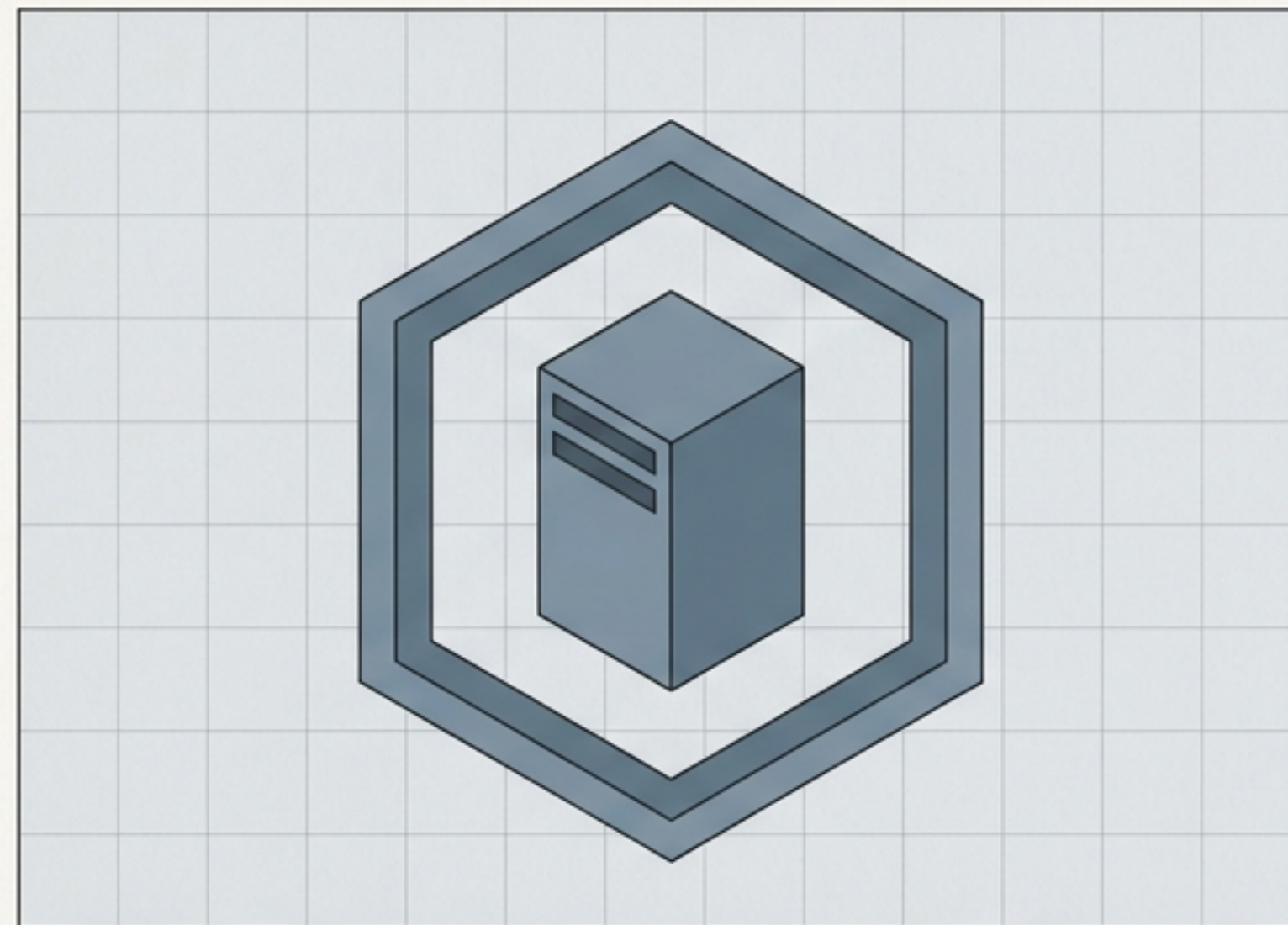
地政学的要請としての「AI主権 (AI Sovereignty)」



REF: VULNERABILITY-NODE

REF: VULNERABILITY-NODE

VS



REF: SOVEREIGN-CORE

REF: SOVEREIGN-CORE

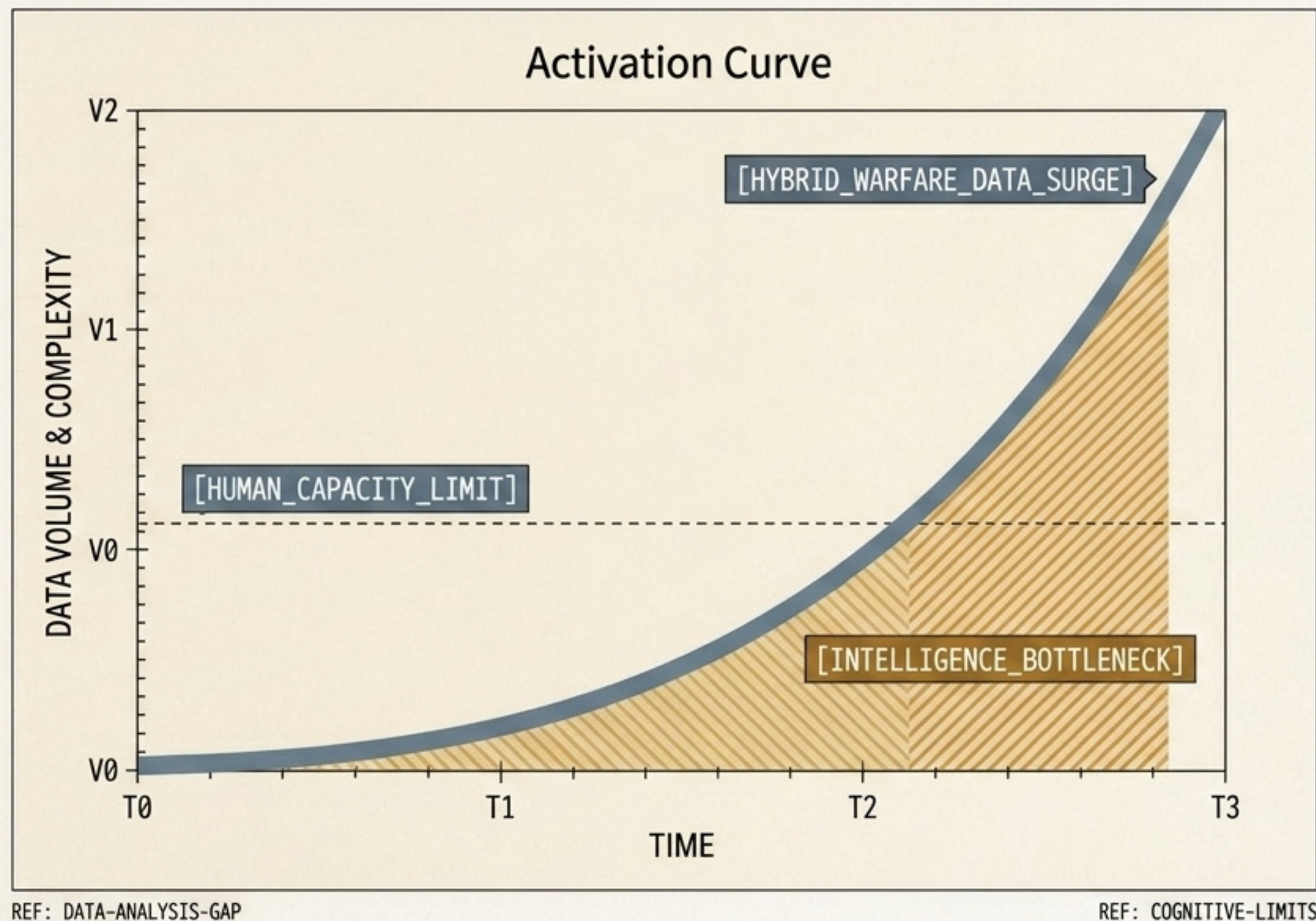
〔外国製モデルの脆弱性〕

- 輸出管理規則や特定モデルの外国人利用制限による供給途絶リスク。
- 海外クラウドへのデータ送信に伴う、法制・運用上の制約と情報漏洩リスク。

〔高機密ソブリン環境の必須要件〕

- 外部ネットワークから物理的に隔離された「エアギャップ」環境での完結。
- 最高度機密を自国データセンター内で処理可能な軽量・高効率な国産基盤（二層構造アーキテクチャ）の確立。

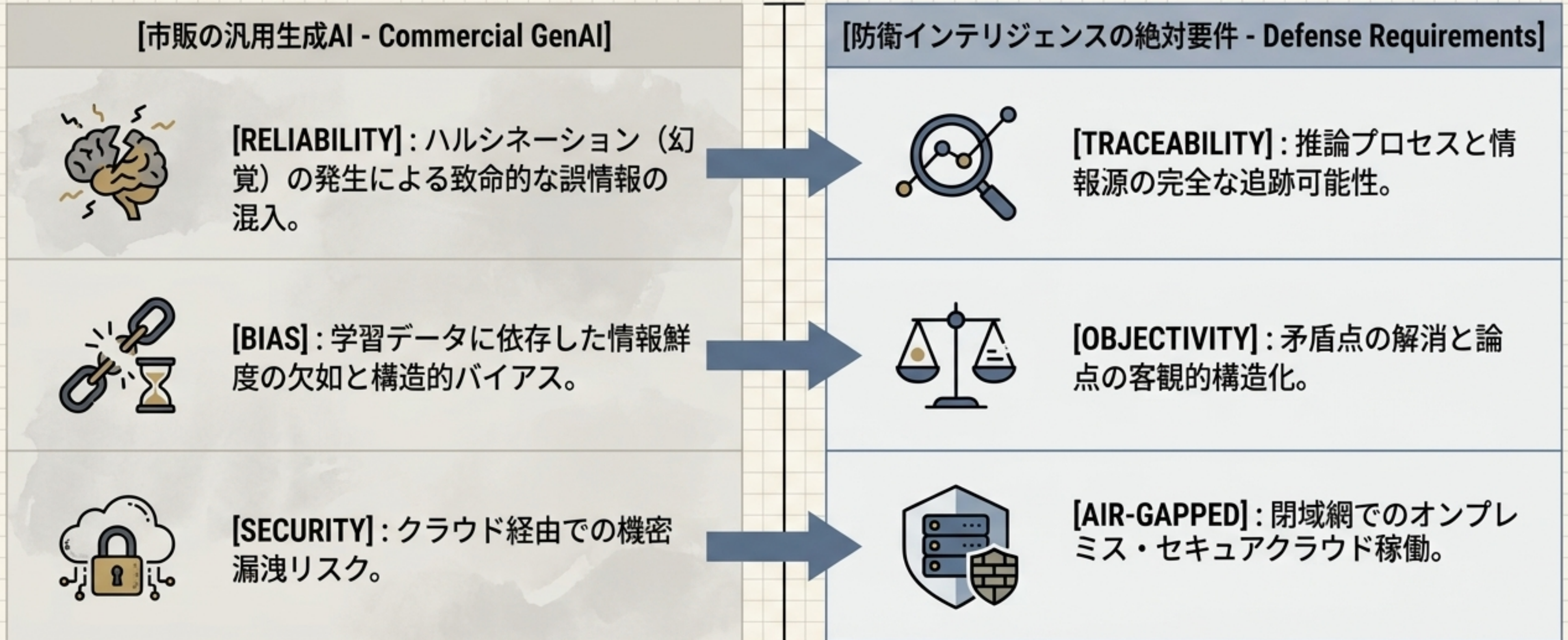
現代ハイブリッド戦がもたらす情報処理の物理的限界



[総合分析業務の逼迫]

- ハイブリッド戦や情報空間の複雑化により、多言語の海外報道、論文、SNSなどの情報量が加速度的に増大。
- 網羅的な情報収集、迅速・正確な分析、知見の体系的管理を人手のみで完結させることは既に限界に達している。

なぜ市販の汎用生成AIは防衛実務で破綻するのか

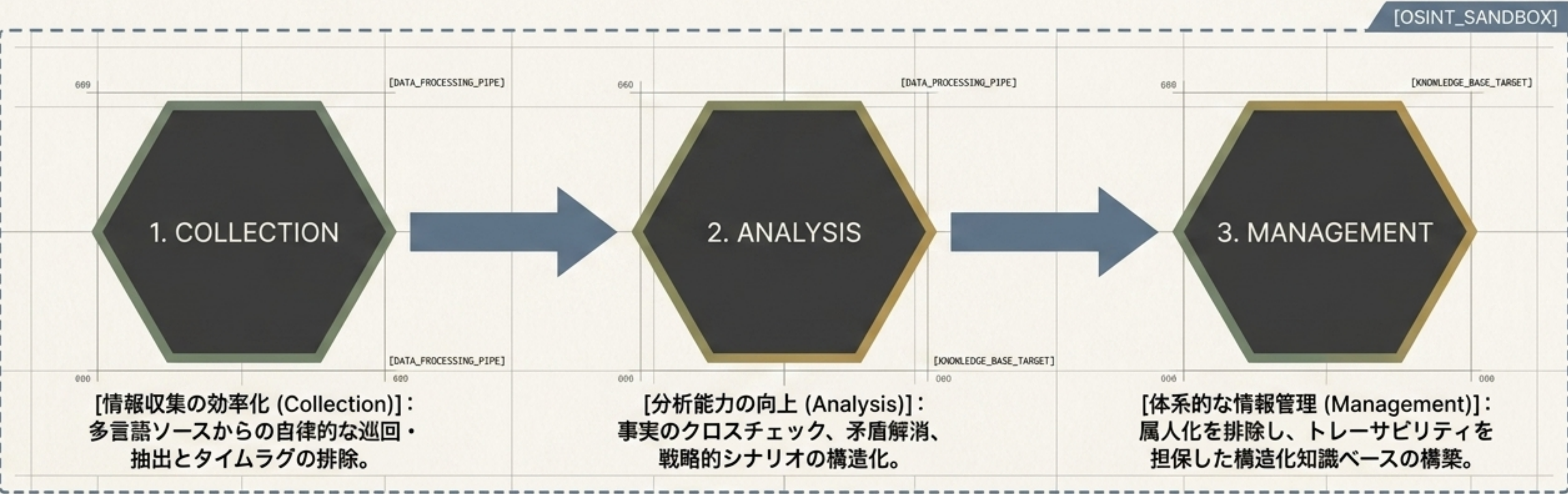


REF: TRANSFORM-PATHWAY

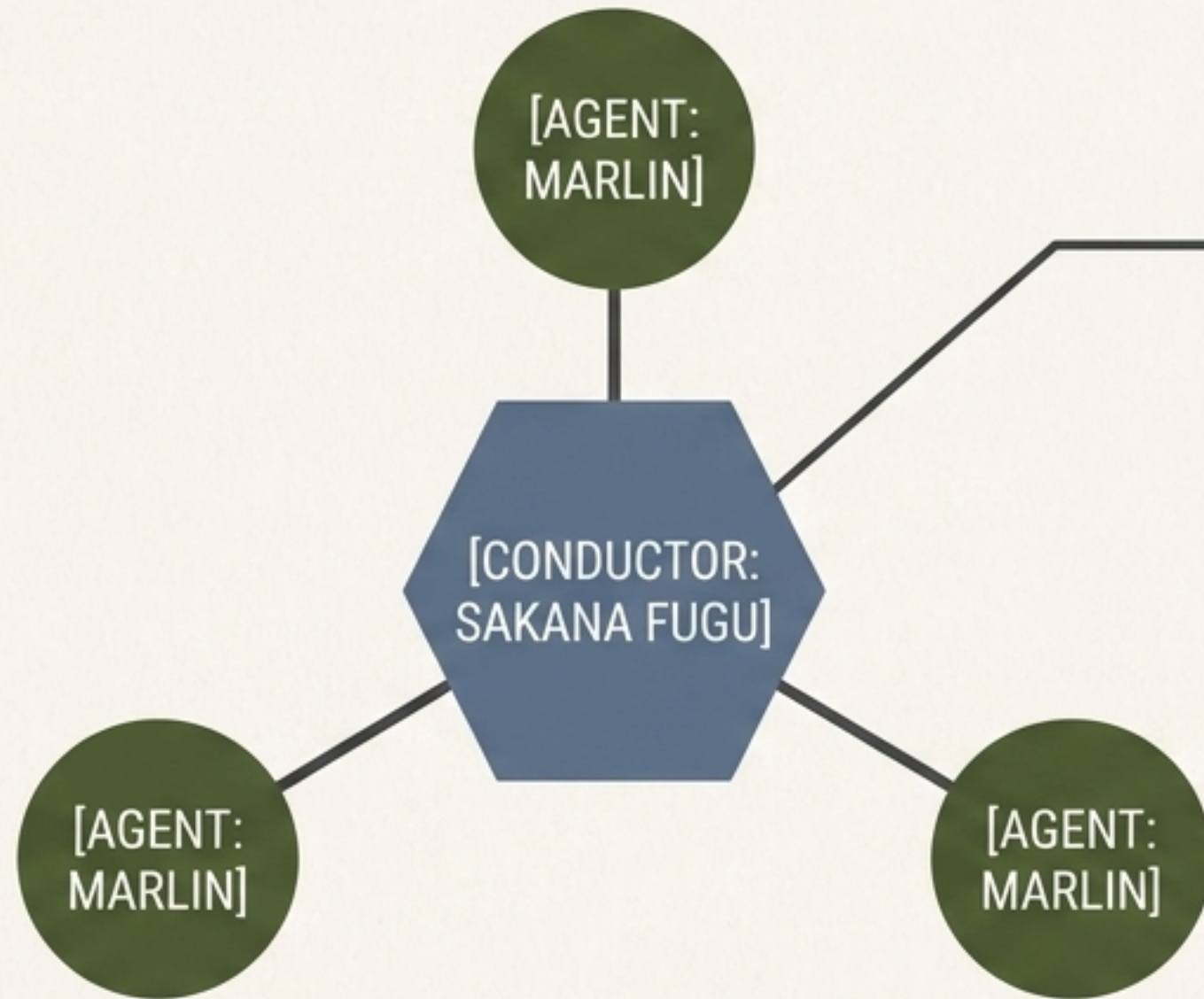
REF: DEFENSE-INTELLIGENCE-MATRIX

3.2億円の戦略投資：公開情報（OSINT）を起点とした安全な実証

機密性の高い情報（SIGINT/GEOINT）を直接AIに投入せず、外部公開情報の処理プロセスでセキュリティリスクを極小化しつつ実用性を検証。



技術的コア：マルチモデル・オーケストレーションと推論時計算量



[Conductor アーキテクチャ]:

単一の巨大モデルに依存せず、タスクに応じて専門モデルを動的に編成・協調させる「Conductor (Fugu基盤)」。

[長時間自律推論 (Inference-time Compute)]:

- 最大8時間におよぶ自律的仮説探索を実行するリサーチエージェント (Marlin)。
- AI自身が情報の収集、検証、仮説構築のループを回し続ける。

 [PROVEN_CAPABILITY] - 2026年7月「Diver OSINT CTF 2026」にて、Fugu-Ultra 1.1を活用したエージェントが850チーム中5位の実績。

総合分析業務のトランスフォーメーション：人手からエージェントへ

Legacy

Agentic

[収集 (COLLECTION)]

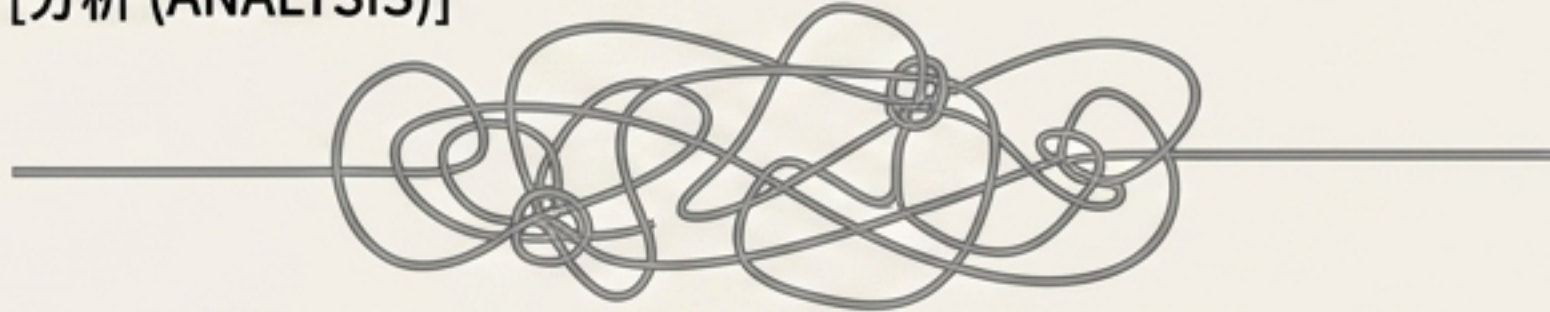


Legacy: 検索漏れ、多言語の壁、情報のタイムラグ。



Agentic: 専門エージェント群が多言語ソースを常時自律巡回し、重要情報を即座にフィルタリング・集約。

[分析 (ANALYSIS)]



Legacy: 認知バイアス、ノイズ混入、因果関係整理の過負荷。

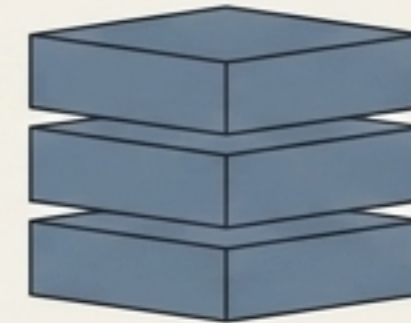


Agentic: 長時間推論によるクロスチェックで矛盾を解消し、戦略的選択肢を構造化。

[管理 (MANAGEMENT)]



Legacy: 個人の属人化、調査履歴のサイロ化。



Agentic: 根拠情報のトレーサビリティを担保した再利用可能な構造化知識ベース。

絶対原則「Human-in-the-Loop（人間参加型）」の維持



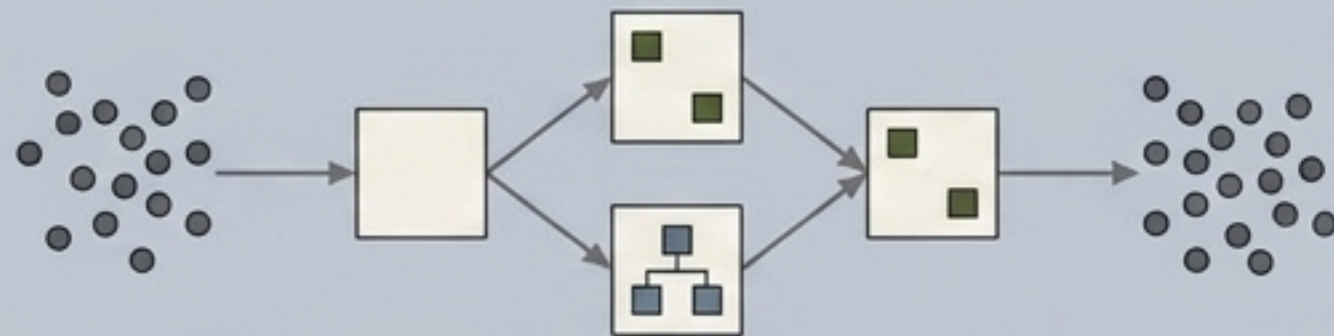
[分析官・指揮官の役割]:

AIによる自動交戦や完全自律型の判断は行わない。最終的な情勢評価、価値判断、意思決定の責任は人間が100%負う。

[COGNITIVE_FILTER_BARRIER]

[AIエージェントの役割]:

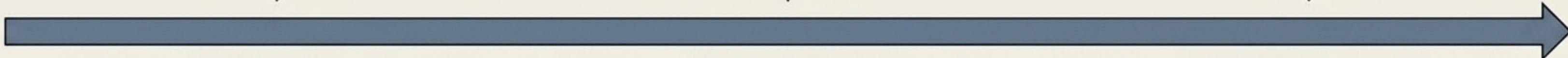
膨大な情報のスクリーニング、クロスチェック、複数のシナリオ・選択肢の構造化提示。
認知的負荷（Cognitive Load）の徹底排除。



日本の防衛AI戦略：マルチレイヤー・エコシステム・マトリクス

	運用レイヤー	対象データ	ベンダー	採用技術
L1	戦略インテリジェンス (国家政策レベル)	公開情報 (OSINT) 総合分析	Sakana AI (本実証事業)	エージェント/ オーケストレーション
L2	作戦計画立案 (司令部運用レベル)	文書・地理空間情報、 作戦シミュレーション	Preferred Networks (PFN)	PLaMo 3.0 Prime
L3	戦術・指揮統制基盤 (C2レベル)	ドローン/センサー等の 制約下前線データ統合	Sakana AI (DISI委託)	小規模エッジVLM / 複数AI統合
L4	全ドメイン統合防衛 アーキテクチャ	基幹システムへの組み 込み、アセット統制	三菱重工業 等	(System Integration)

社会実装に向けた複数年ロードマップ



[MILESTONE_01]

[MILESTONE_02]

[MILESTONE_03]

2027年度初頭 - プロトタイプ展開
と現場検証

- 実証用プロトタイプモデルの提供。
- 情報本部分析官による実業務シナリオに即したテスト試用。
- オンプレミスとセキュアクラウドのハイブリッド環境の適合性評価。

2027年度中盤 - アルゴリズム
改修と高度化

- 実務フィードバックに基づく機能改修。
- マルチモーダル処理の強化と、偽情報・認知戦対策機能の統合。

2027年度末 - 最終報告と実装
判断

- 技術評価を取りまとめた最終報告書の策定。
- 本格的な基幹システムへの社会実装（移行）判断。

最終展望：OSINTから 「全ドメイン情報融合」への進化

安全なサンドボックスでの証明

- 公開情報に基づく大局的な兆候察知と、
AIエージェント基盤の実用性・安全性の担保
(現在のフェーズ)。

機密インテリジェンスとの有機的結合

- 確立された基盤を、閉域ネットワーク内の
電波情報 (SIGINT) や衛星画像 (GEOINT)
等の機密センサーとシームレスに統合。

[KEY TAKEAWAY / SYNTHESIS]:
OSINT実証は、究極の目標である「全ドメイン
情報融合」を実現し、日本の防衛におけ
る即応性と精度を飛躍させるための戦略的足
場 (トロイの木馬) である。

