ASI（超知能）時代の
デジタル主権のあり方とAIセキュリティ設計

栄藤　稔（えとう　みのる）
CXO Advisor, Netskope Inc.

2026-2027年：AGI到来のタイムライン

近くにある未来、汎用AI
(Artificial General Intelligence)

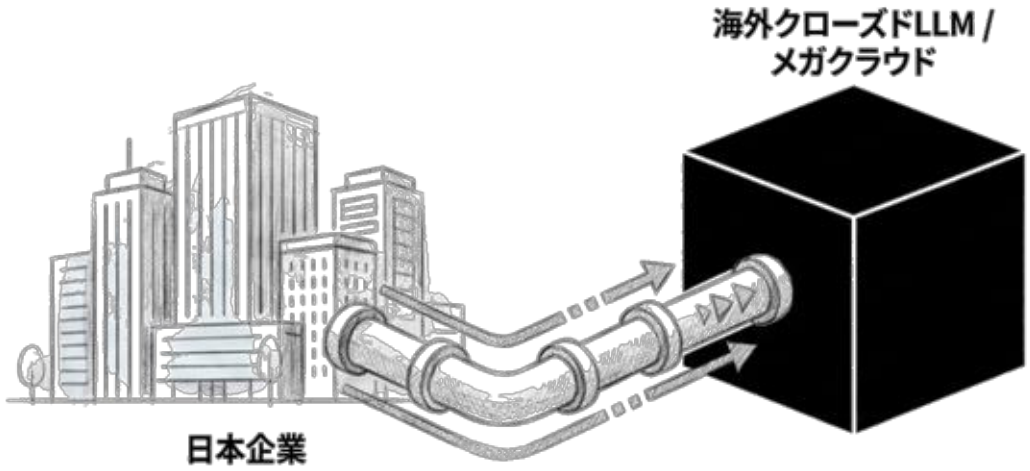
•敵対的な2時間のチューリング・テストに合格すること。

•知識・論理のQ&Aベンチマークで広範に成功すること。

•複雑な模型（モデルカー）の組立手順を正しく解釈し、実行できること。

Not Yet

「Fable 5]沈黙の悪夢：デジタル主権喪失の構造的リスク
平時の利便性が招く、戦時における国家・企業の「デジタル脳死」



アクセスリスク

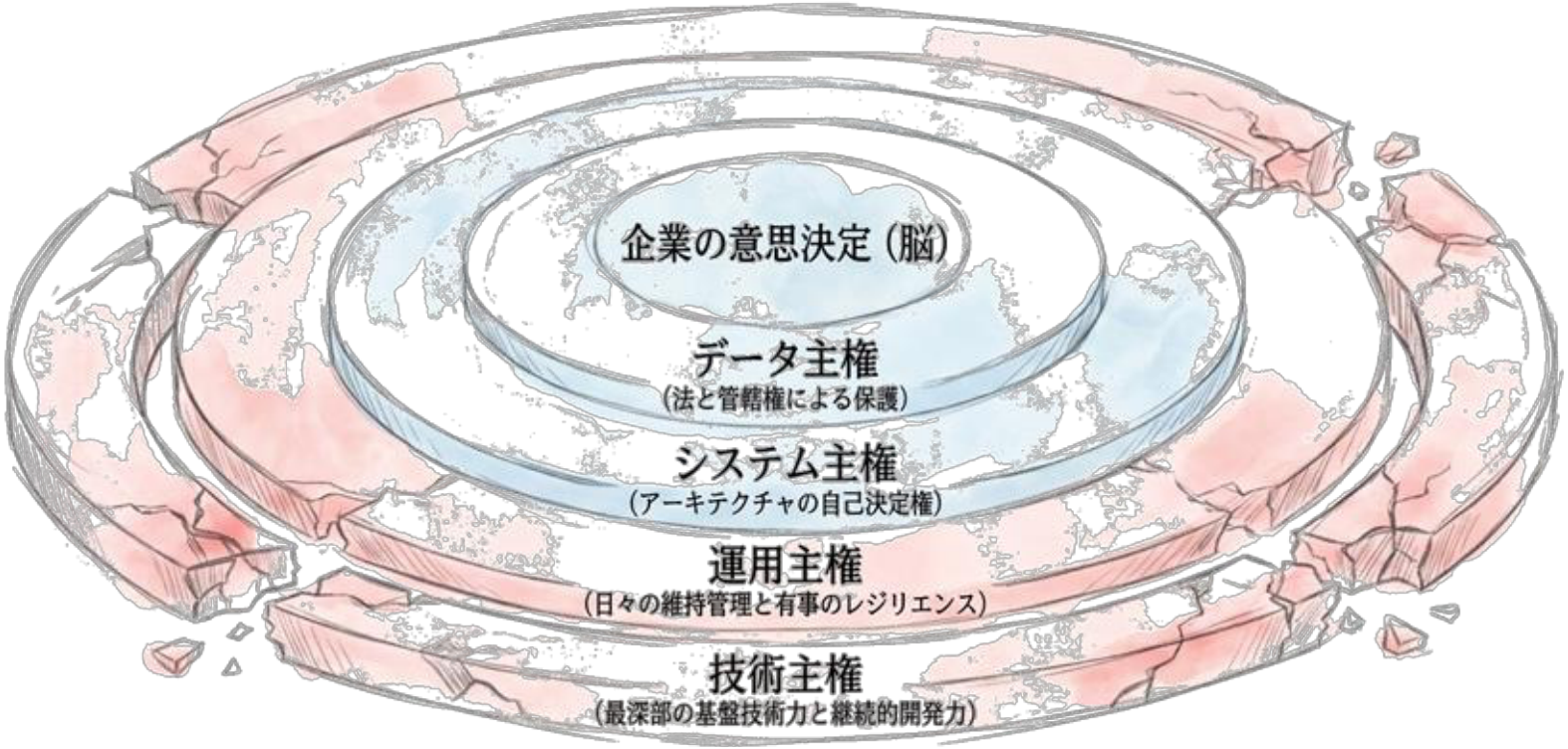
米国CLOUD Act等の域外適用。物理的に国内にあっても、法的義務による強制的なデータ開示要求。

供給停止リスク（Fable 5）

一方的なライセンス変更、予期せぬ輸出規制、有事の際の通信遮断によるインフラの突然死。

単にデータを国内に置くだけでは、国家の安全保障や企業の競争力は全く担保されない。

デジタル主権の四層



https://www.softbank.jp/business/content/blog/202506/digital-sovereignty
を参考に作成

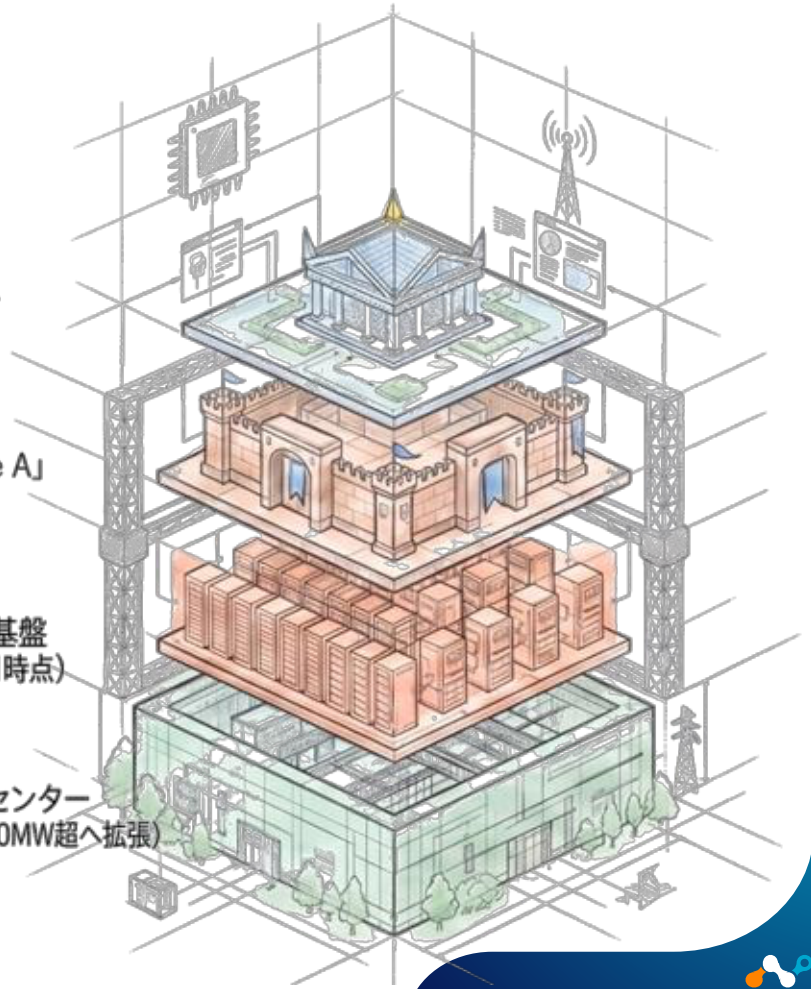
ソブリンAIインフラ：ソフトバンクによる垂直統合型主権インフラ ハードウェアからAIモデルまで全階層を自社管理下

Layer 4: Application
純国産LLM「Sarashina」シリーズ

Layer 3: Platform
ソブリンクラウド「Cloud PF Type A」
& Oracle Alloy

Layer 2: Compute
NVIDIA Blackwellを含むAI計算基盤
（全体で13.7 EFLOPS／2025年7月時点）

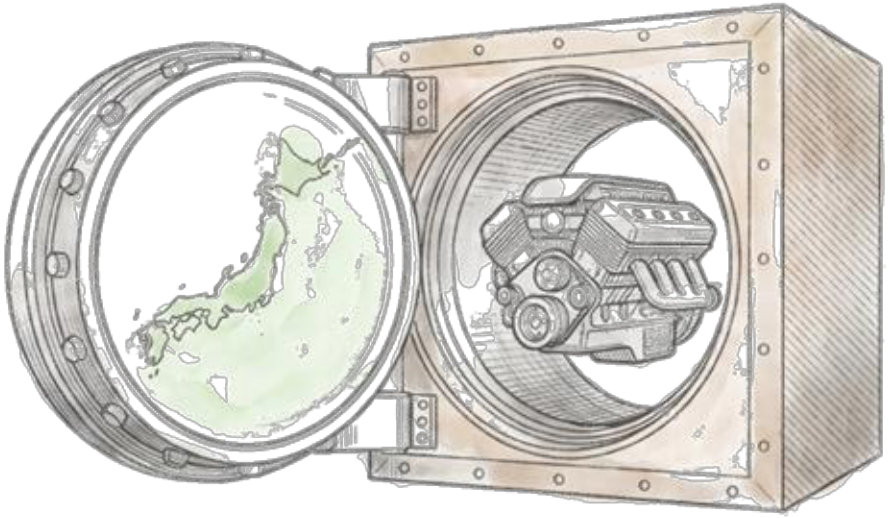
Layer 1: Facility
北海道苫小牧グリーンAIデータセンター
（2026年度開業・50MWから／将来300MW超へ拡張）



データの聖域化：Oracle Alloyを統合したソブリンクラウド

Cloud PF Type A:

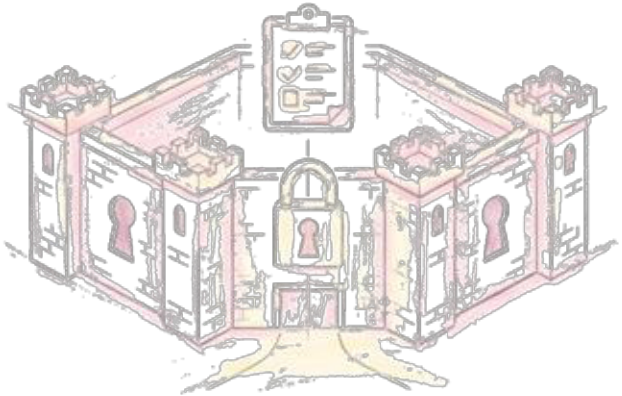
日本国内の法域と管理下でデータを完全に閉域運用。他国政府のアクセスリスクを構造的に排除。



Oracle Alloyの戦略的統合:

OCI (Oracle Cloud Infrastructure) のフルポートフォリオを、ソフトバンクの国内データセンターの閉域環境内で展開。

AIエージェントは壁の中にいる！
サイバー防衛戦略は「静的確認」から「動的統制」へ

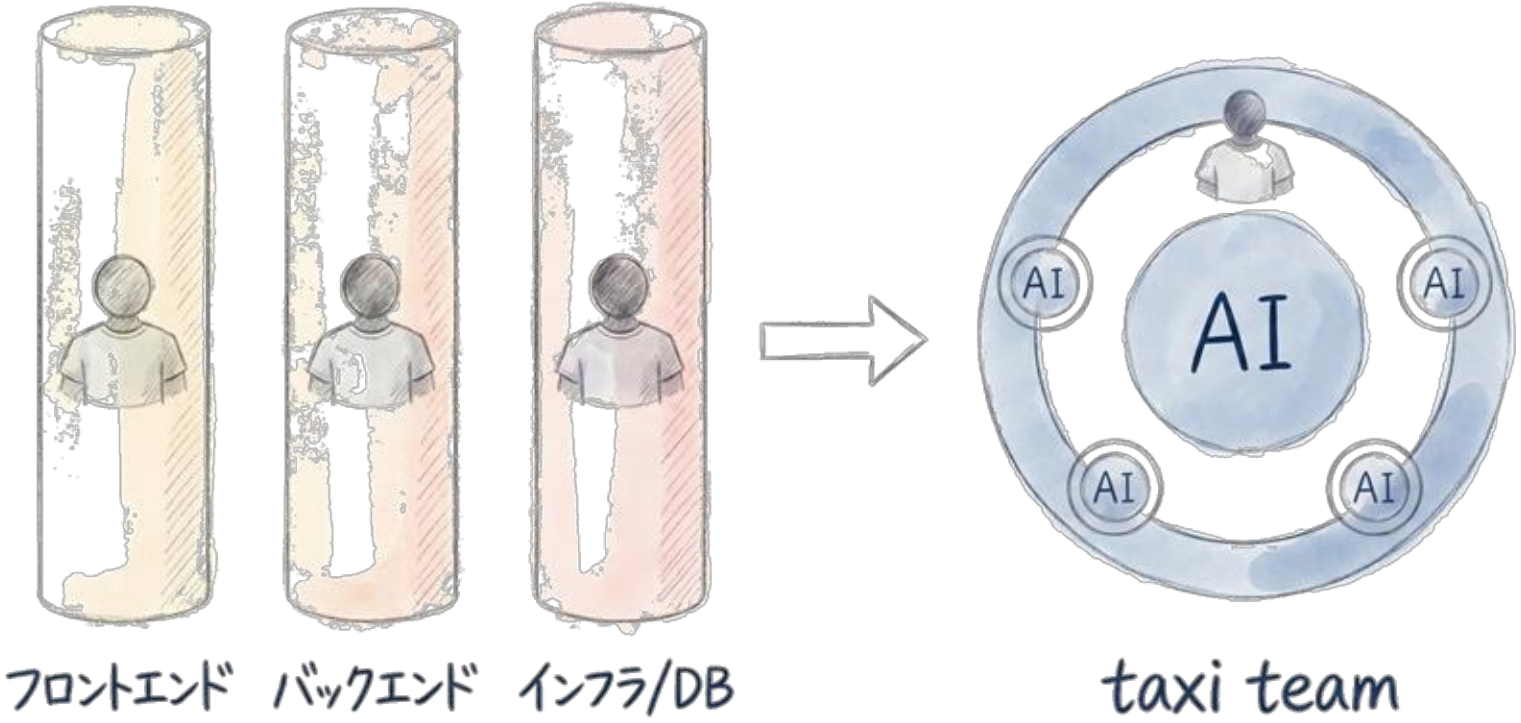


As-Is: 人間中心
UI/ブラウザ依存
静的な「ゼロリスクの確認」

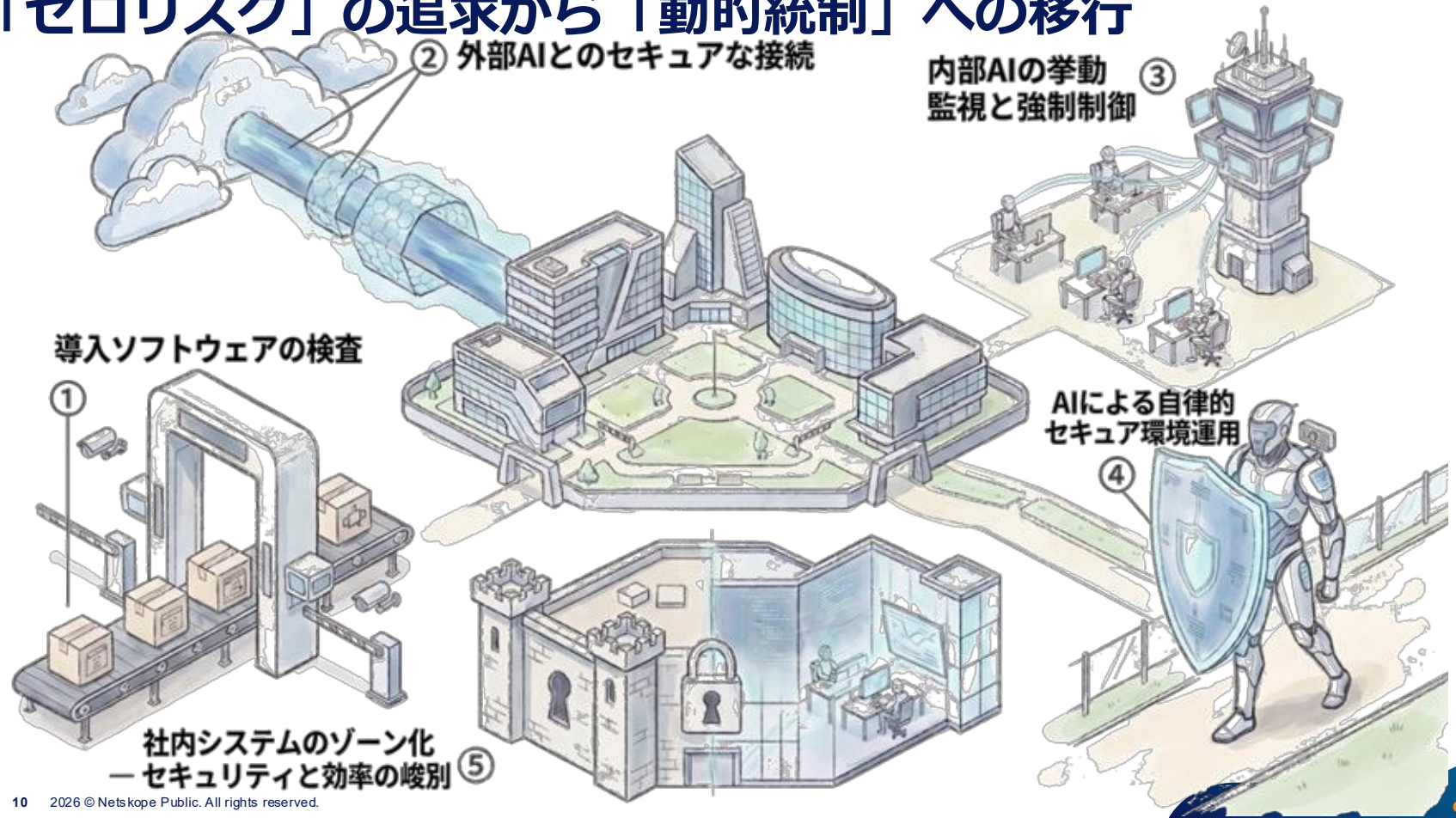
To-Be: エージェント間（M2M）通信
API主導
ミリ秒単位での「動的統制の確認」

システムアーキテクチャの根底に、人間を介在させない「論理的キルスイッチ」と「主権インフラ」を組み込むことが、ASI時代の絶対条件となる。

AI駆動開発　→ AIは企業システム内の同僚

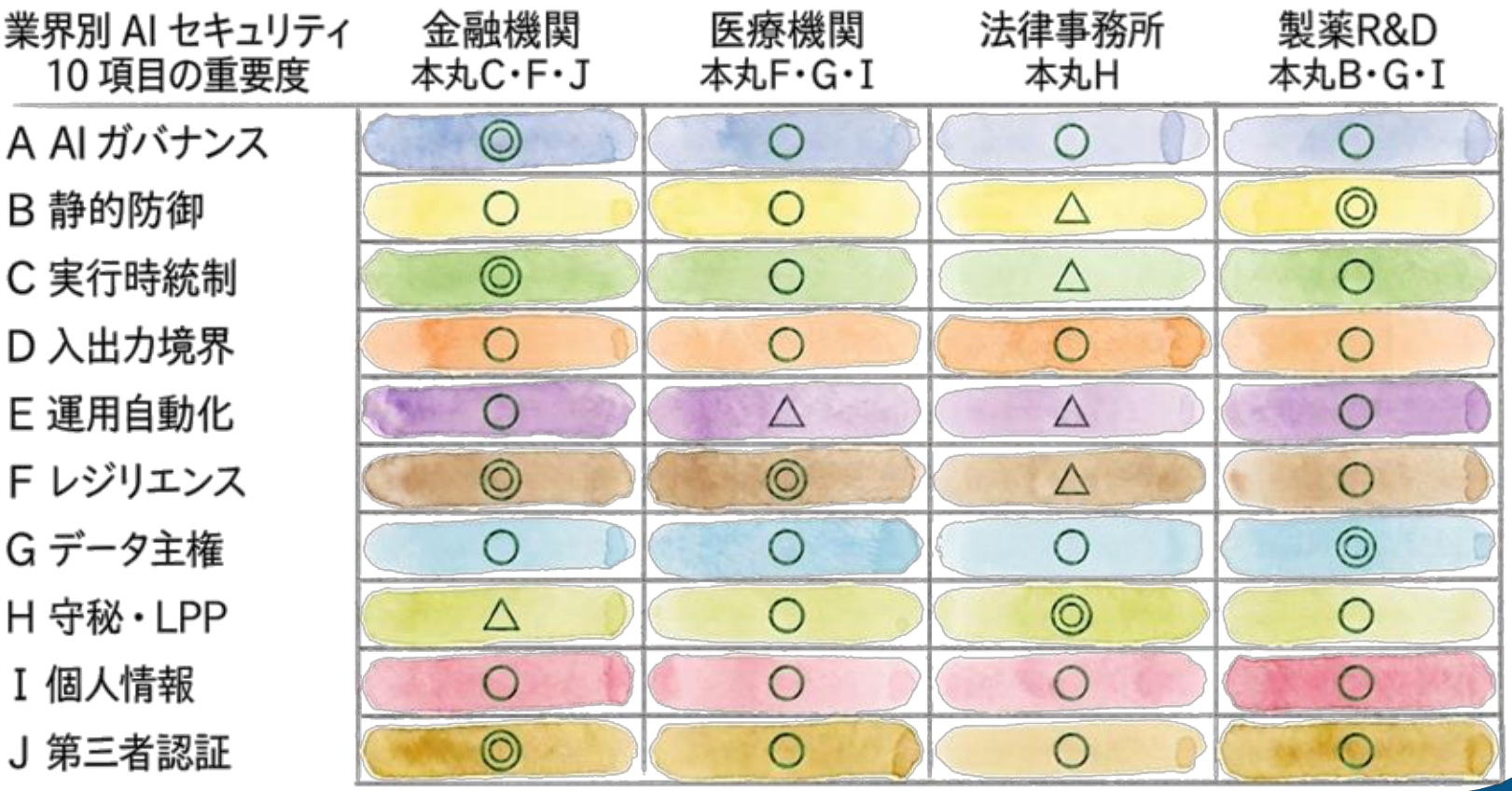


IT系スタートアップはAI駆動開発へ邁進：「ゼロリスク」の追求から「動的統制」への移行

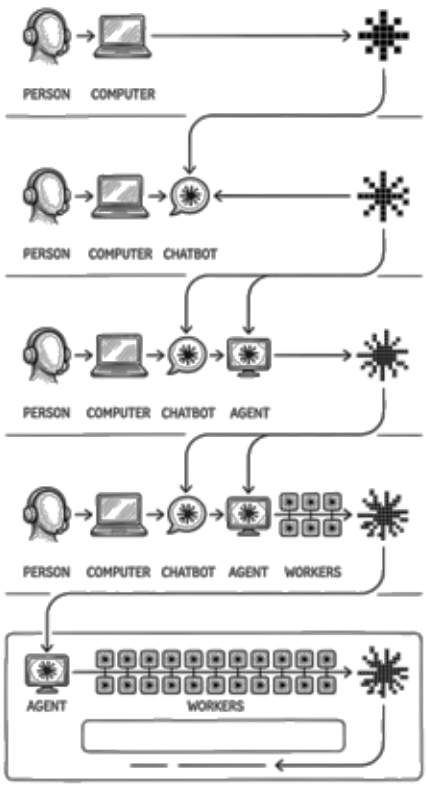


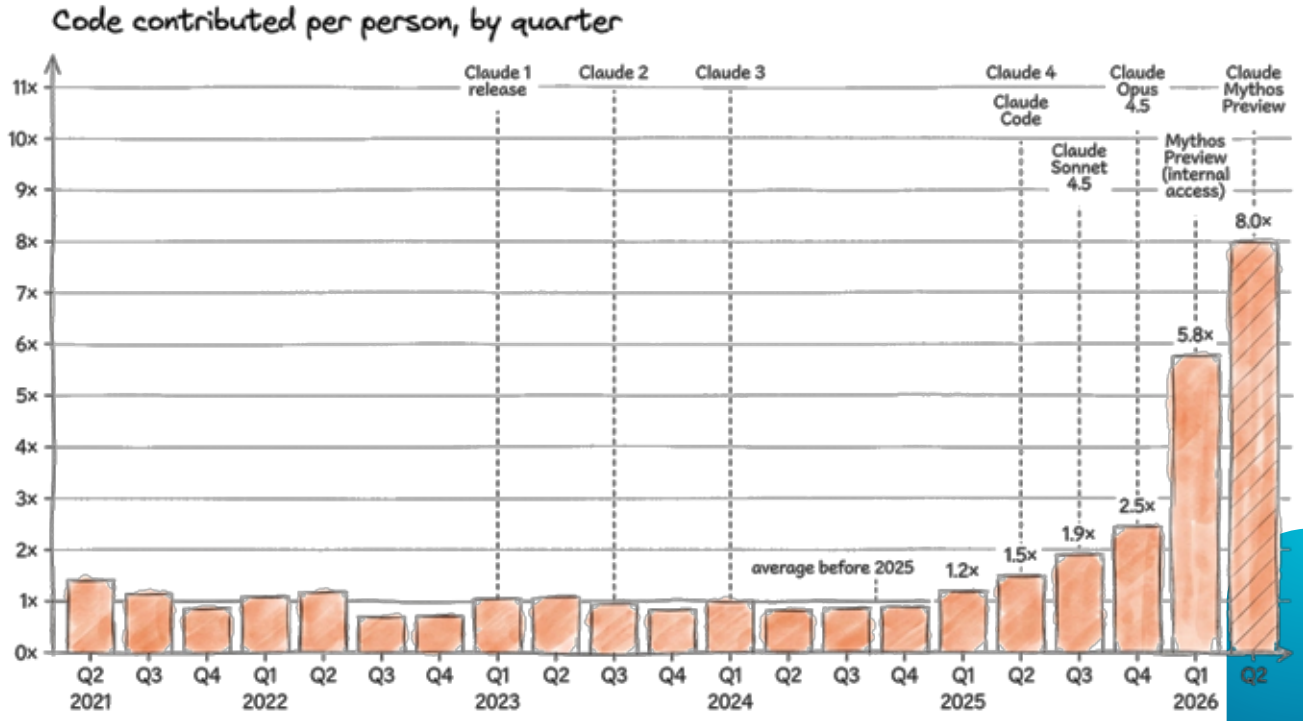
金融・医療・製薬・法律組織の現在位置を測る：AIセキュリティ評価シート　10の主要オプション

企業セグメント毎のセキュリティ評価の濃淡（例）



ループが閉じる時：Recursive-Self-Improvement(RSI)

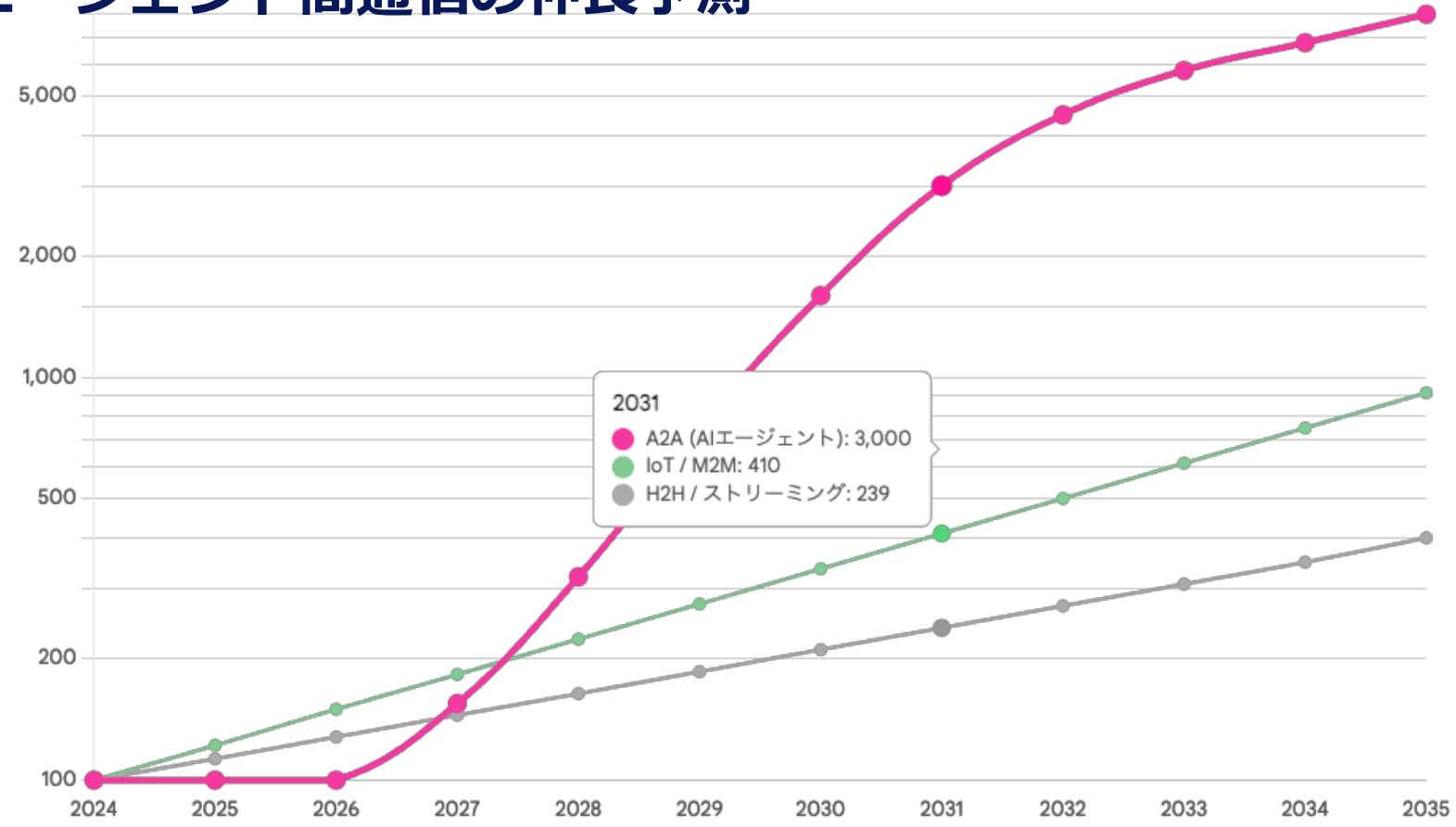




Claude開発者のコード開発量

https://www.anthropic.com/institute/recursive-self-improvement

エージェント間通信の伸長予測

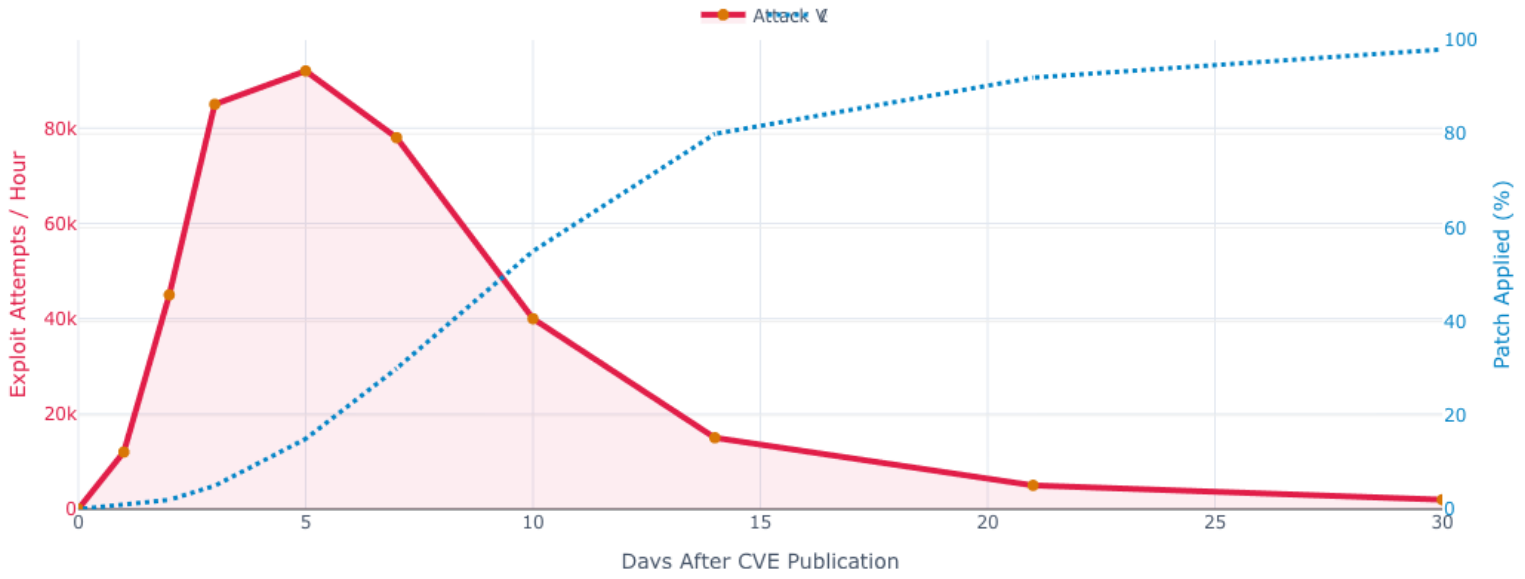


Cisco 『AI Impact on Wide Area Networks 2026』、 Nokia 『Advancing AI: Networks that self-operate』からの描画

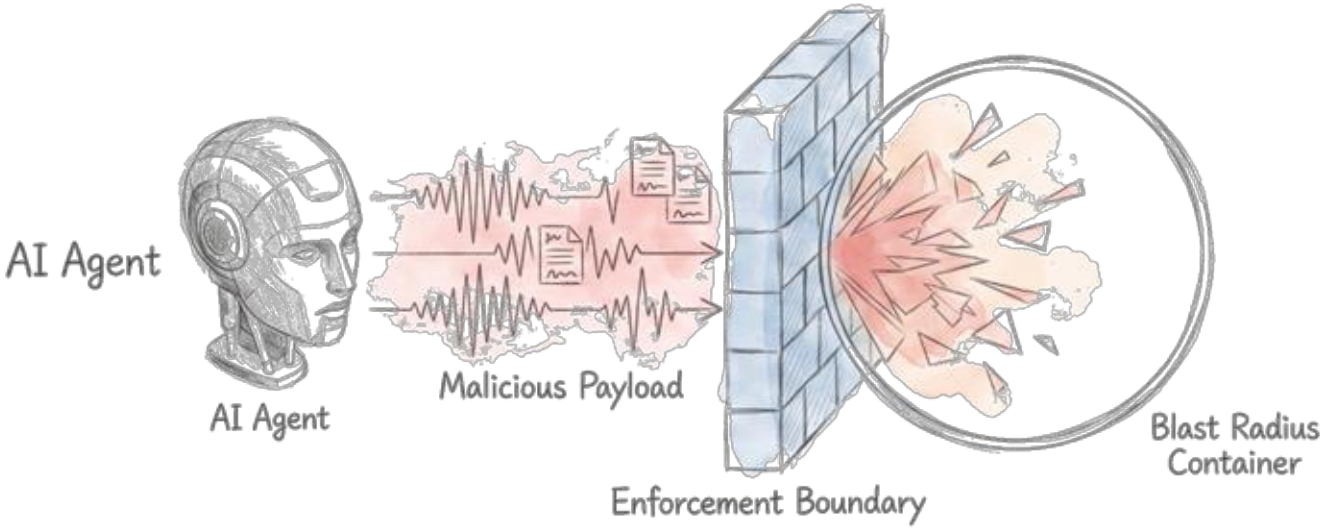
Mythos of Cyber Warfare:Zero-Day AI vs Auto-Patching

⚔️ 3. CVE情報のパラドックス（コインの表裏）

脆弱性情報（CVE）の公開は、防御側にパッチを促す目的で行われますが、現在では「AIへの攻撃ターゲット指示書」として機能しています。脆弱性が公表された瞬間から、世界中の攻撃AIがPoC（概念実証）コードを生成し、数分から数時間以内に大規模なスキャンと攻撃を開始します。パッチ適用が完了するまでの「兵器化ウィンドウ」が攻撃者の最大の狩場となっています。



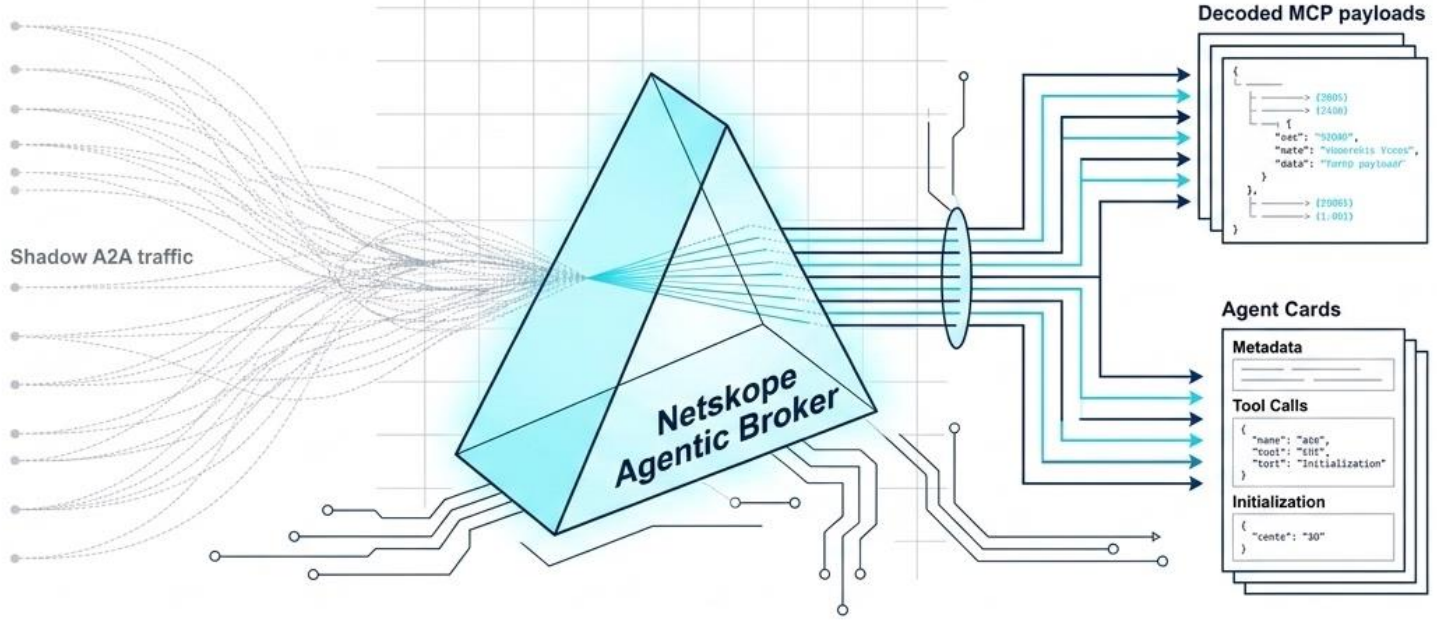
Runtime Enforcement(実行時強制制御)



1. 可視化 (Visibility) → 2. 検証 (Validation) → 3. 実行時強制制御 (Run-time enforcement)

- 自律型AIの暴走・権限悪用を実行時に、まさにその場で停止させる。
- 突破時の影響を限定するBlast Radius最小化（分散化・セグメンテーション）。

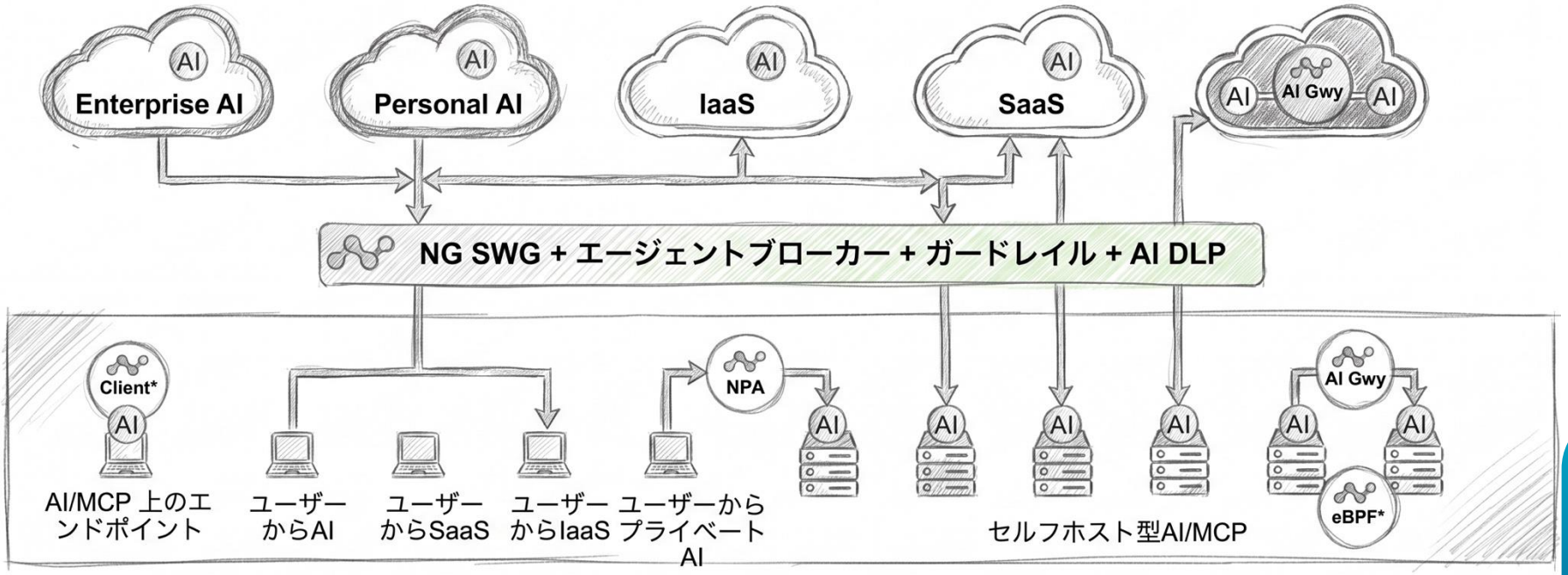
Agentic Broker (for the north-/southbound axis in SDN)



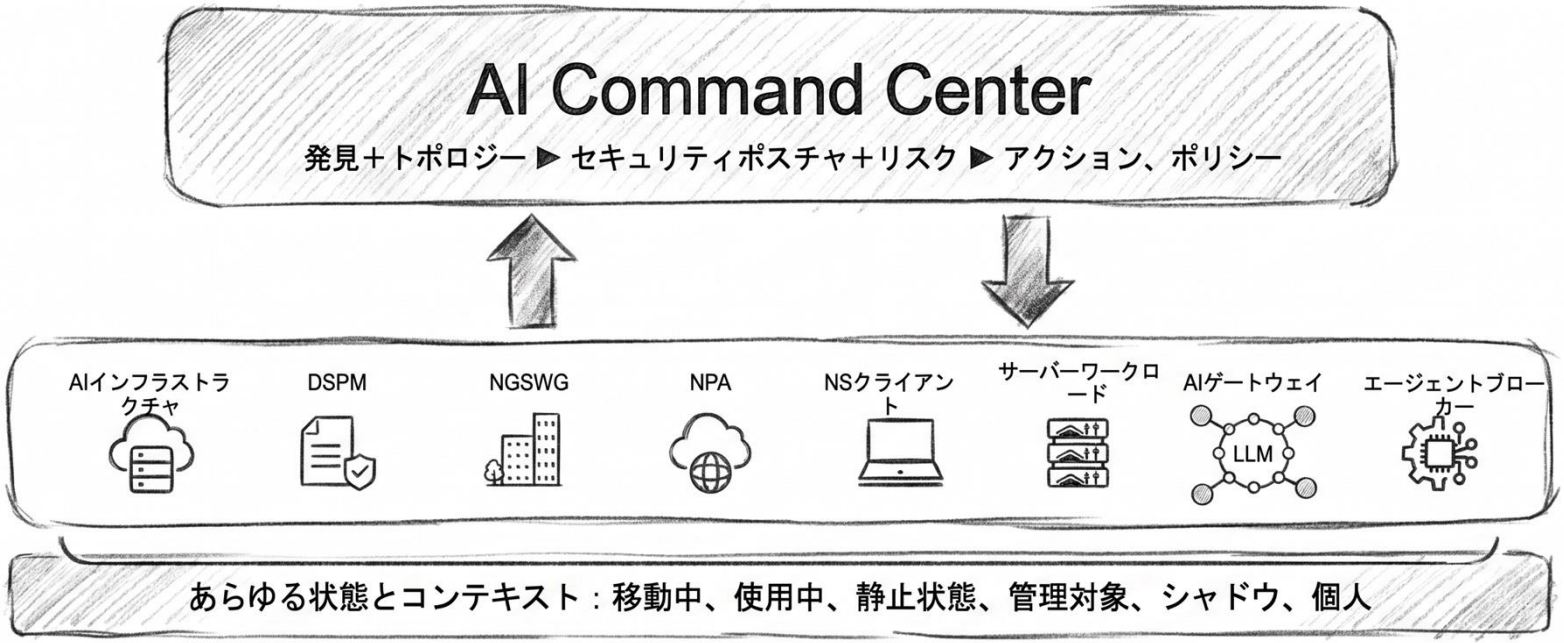
The Solution:
Netskope One Agentic Brokerがプロキシとして介在し、これまでブラックボックスだった非人間トラフィック（MCP/A2A）をリアルタイムでデコード。

Capabilities:
エージェントのセッション初期化、Tool Calls、Agent Cardのメタデータを解読し、インベントリ化。Shadow Agentic AIの全容を完全に可視化する。

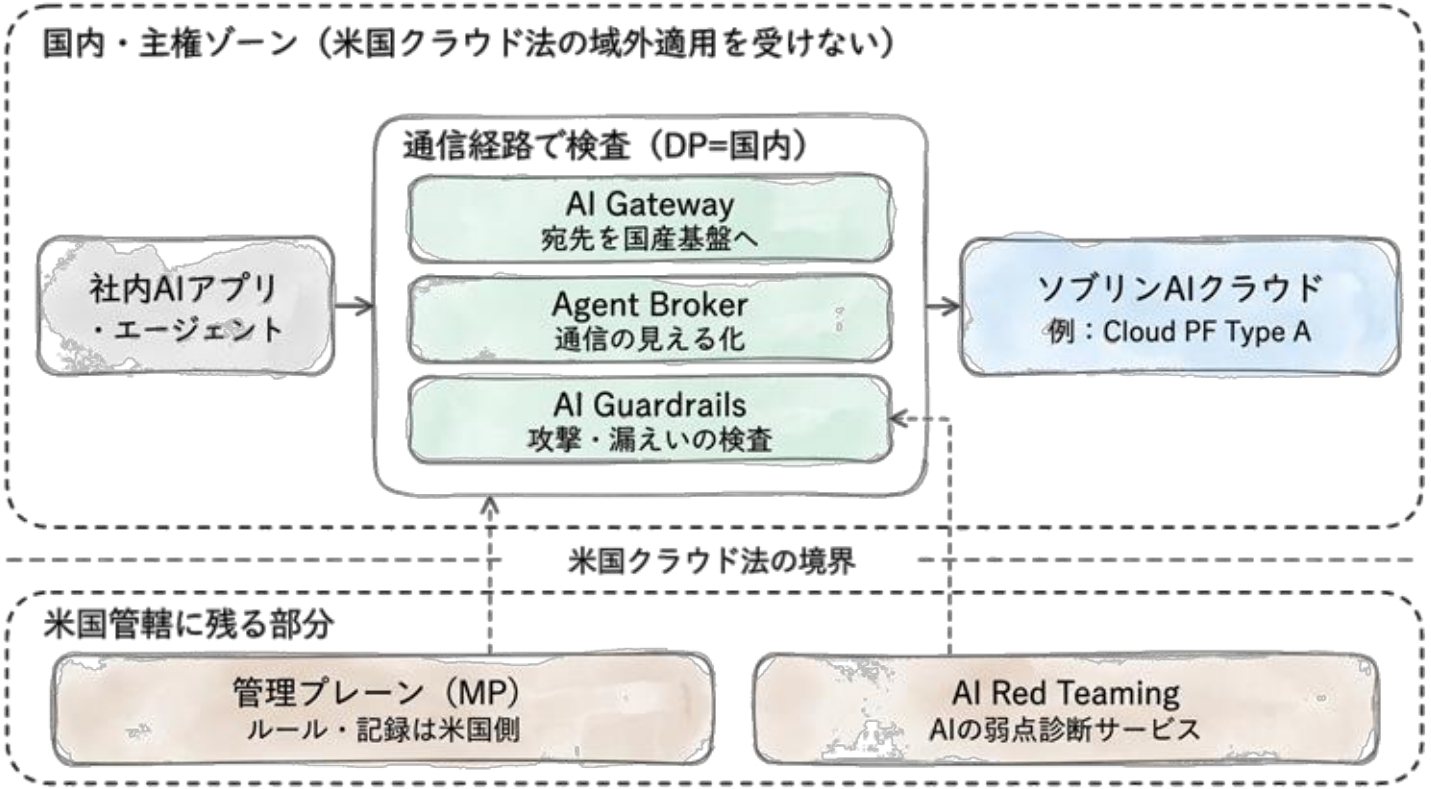
組織全体を保護するNetskope One AI Security



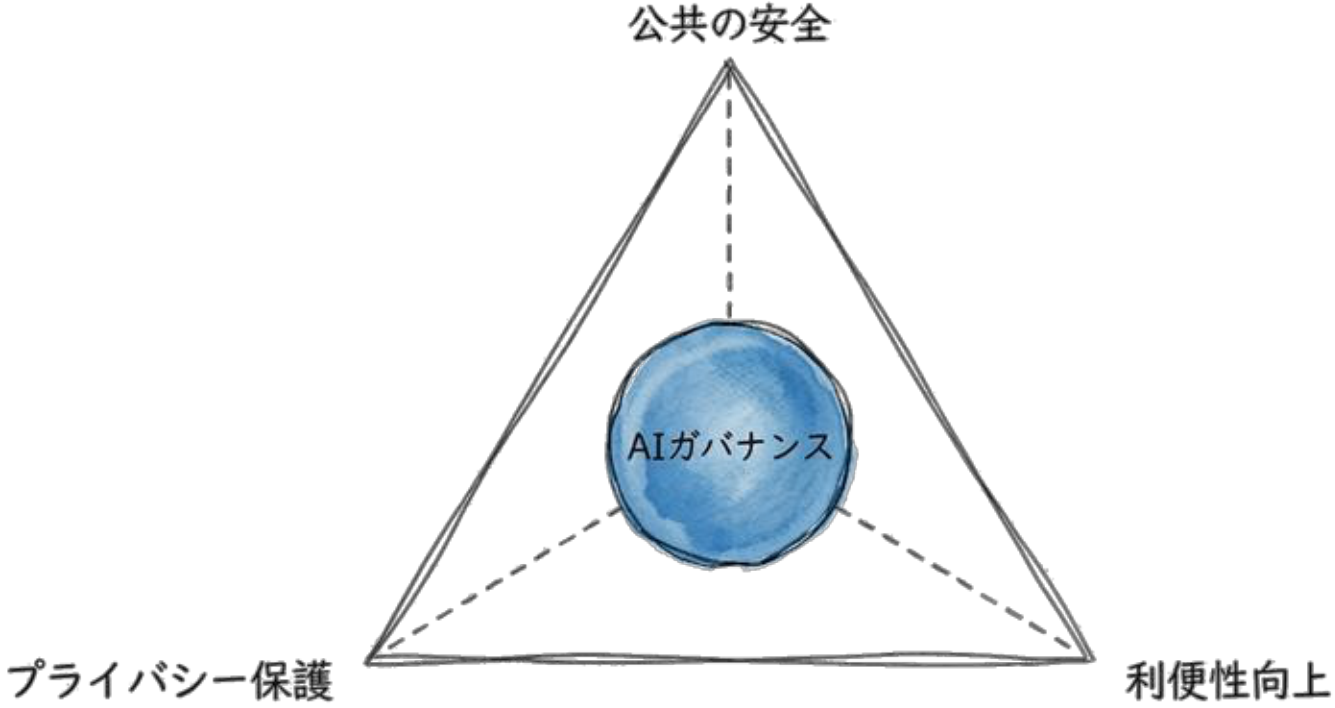
現在ベータ版：　Netskope One AI Command Center



Netskope、データ主権対応を24カ国へ拡大する — 業界の水準を引き上げる(5/28)



AIガバナンスの使命：トリレンマの最適設計



見えないものは、守れない。

Netskopeは、AIエージェントのすべてを見て、すべてを制御する。
Agentic AI時代の安全と秩序は、ここから始まります。

データ主権
どこを移動・処理・保管？

- 通信を国内事業者で
- 処理・保管を国内で
- メタデータも国内に

運用主権
誰がアクセスできる？

- 顧客管理の暗号鍵
  KMIP HSM
- アクセス制御
  RBAC・データ難読化
- 監査ログ
  全アクセスを記録

技術主権
インフラを自分で制御？

- オンプレ型DP
  自社環境に設置
- キャリア組込み型DP
  Orange等と提携
- ローカルZTNA
  ブローカーを国内に

残る論点：運用主体のコーポレート管轄（米国クラウド法）
ただし顧客管理鍵により、取り出せるのは暗号文に限定

	データ主権	運用主権	技術主権
AI Gateway 自社環境で実行	○	○	○
AI Guardrails 置き場所次第	○ / △	○ / ×	○ / ×
Agent Broker クラウドで実行	△	×	×

○ 主権あり　△ 部分的　× なし（運用はNetskope側）

AI Guardrailsは自社環境なら○、クラウドなら△/×（左/右）