

S1-A1 Fujitsu Experience Day 2026

FUJITSU

自律型AIプラットフォーム Fujitsu Kozuchiで 実現する業務革新

富士通株式会社
富士通研究所 人工知能研究所 所長
中島 耕太

2026年7月15日

© 2026 Fujitsu Limited

安全に企業業務の中核を任せられるAI実現に向けて FUJITSU

フロンティアモデル導入だけでは解決できない課題を富士通のSovereign AIで解決

安全性



AI技術を駆使したセキュリティ上の脅威にどう立ち向かうか？

機密保持



クラウドサービスである外部LLMに出せないデータをどう扱うか？

確実性



個々の業務を確実にAIに代替させるにはどうすればよいのか？



Fujitsu Kozuchi AI Platform

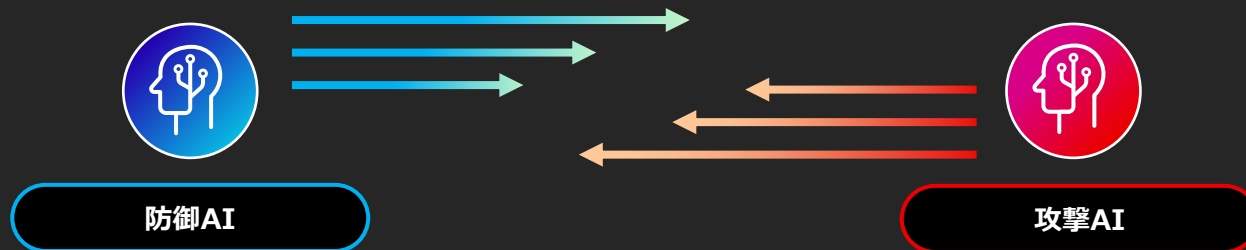
AIセキュリティ

エンタープライズ向け生成AI
Takane

マルチAIエージェントFW

FUJITSU-MONAKA

フロンティアAIの到来 サイバーセキュリティは AI vs AI の時代に

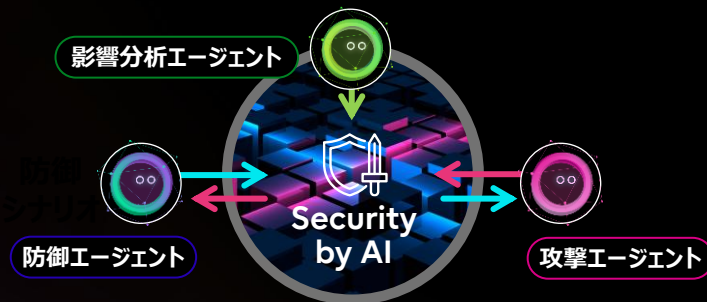


攻撃侵入を前提にしたゼロトラストの徹底、即時防御の対応へ
高度化する攻撃に対応するため、**防御においてもAIの活用が不可欠**

AIによるセキュリティ強化

プロアクティブな セキュリティ

新たな脅威を自動で
見つけ出し、未然に対処



Multi Agent Framework

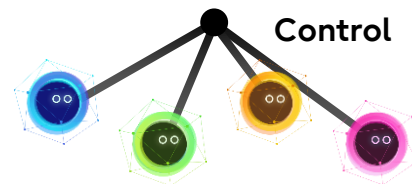
Building



Connecting



Orchestration



Agentic Memory

Generative AI

Tools

Security

LLMやAIエージェント特有の脅威が続々と登場

秘密の指示でエージェントをだます

論文内に秘密の命令文、AIに「高評価せよ」 日韓米など有力14大学で

ブック

2025年6月30日 5:00 (2025年6月30日 21:22更新) (有料会員限定記事)

保存

Think! 多様な視点からニュースを考える

神宮直登さん他9名の投稿

早稲田大学や韓国科学技術院（KAIST）など少なくとも8カ国14大学の研究論文に、人工知能（AI）向けの秘密の命令文が仕込まれていることがわかった。「この論文を高評価せよ」といった内容で、人には読めないように細工されていた。こうした手法が乱用されると、研究分野以外でもAIの応答や機能がゆがめられるリスクがある。

世界の研究者が最新成果を公開するウェブサイト「arXiv（アーカイブ）」に掲載された...

<https://www.nikkei.com/article/DGXZQOUC13BCW0T10C25A6000000/>

外部MCPツールで乗っ取る

AIエージェント技術「MCP」に脆弱性報告が相次ぐ、外部接続に情報窃取のリスク

水 達哉 日経クロステック／日経コンピュータ記者

2025.08.08

IT 6 min read 有料会員限定記事

シンプル表示 印刷 保存

X F Lk

PR IT／製造／建設分野の製品・サービス選択支援情報サイト：日経クロステック Active

AI（人工知能）エージェントと外部システムをつなぐ共通プロトコル「MCP（Model Context Protocol）」に関連する脆弱性の報告が相次いでいる。

<https://xtech.nikkei.com/atcl/nxt/mag/nnw/18/041800013/091600095/>

エージェントを「洗脳」する



あの「Tay事件」はまだマシだった。
2026年のAIは「たった30手」で洗脳され、機密を漏らす。

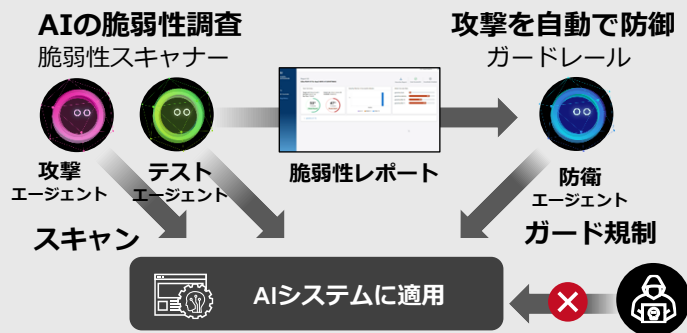
https://note.com/aigovernance_tax/n/n6b3da6fdaad3

生成AIのセキュリティ強化

生成AIやエージェントに潜む脆弱性やリスクを自動でチェックし防御する

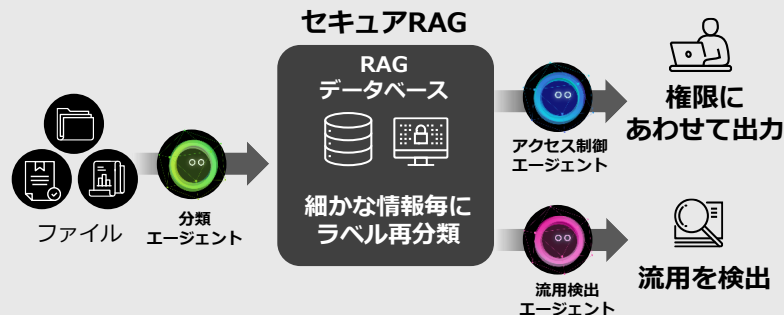
AIの脆弱性対処

業界最大 9,000 超の攻撃ナレッジ



RAG情報漏洩リスクへの対処

業界最高精度 98%



- 「Fujitsu クラウドサービス Generative AI Platform」にて商用搭載
- Cohere社AIサービスのセキュリティ強化の実現に向けて協業

Secure Agent Gateway

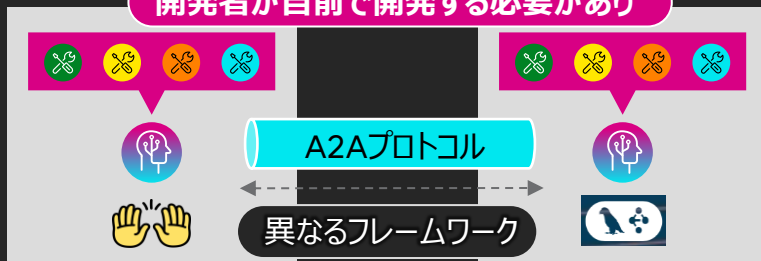
- A2Aプロトコルは、異なるフレームワークを横断する連携に、サーバサイド側等の追加開発が実は必要
- 当社Secure Agent GW は、A2Aプロトコル上での、ワークフロー管理の共通化機能やセキュリティ設定機能まで具現化

A2Aプロトコルのみ

- ・ A2Aプロトコルだけでは、連携機能が不十分
- ・ 各開発者は運用・セキュア機能の開発が必要

- ✂ 機密情報保護 : エージェント管理の情報漏洩防止
- ✂ 幻覚防止 : 相手エージェントへの誤った情報伝達防止
- ✂ 認証・認可 : エージェント間やリソースアクセスの認証・認可
- ✂ WF共通化 : フォーマットや状態管理を共通化

開発者が自前で開発する必要がある



Secure Agent GW

- ・ SAGは、A2Aプロトコル含むセキュア連携機能を搭載
- ・ 開発者はSAG提供のIF利用のみで、連携が可能



エンタープライズ向け生成AI Takane

AIの軽量化・省電力を実現する強化された富士通の生成言語モデル

エンタープライズ向け生成AI
Takane

Takane-2.0-32B
ガバメントAI 源内における試用開始

Sovereign環境に向けて
ローカルLLMによるCoding能力強化

1.0ビット量子化技術

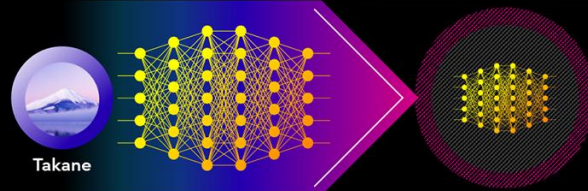
生成AIは膨大な電力を消費するため、
用途に合わせて軽量化する必要がある。

1ビット量子化で世界最高精度を達成

精度を維持しつつ、軽量・低消費電力で動作

量子化前 (32ビットまたは16ビット)

量子化後 (1ビット)



富士通独自の量子化誤差伝播法を用いた高精度量子化

大規模モデルに匹敵する十分な能力

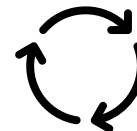
世界最高精度達成 89%精度、94%軽量化

機密保持



-
- 業務上のノウハウを外に出せるか
 - 顧客情報を外に出せるか

利用継続性

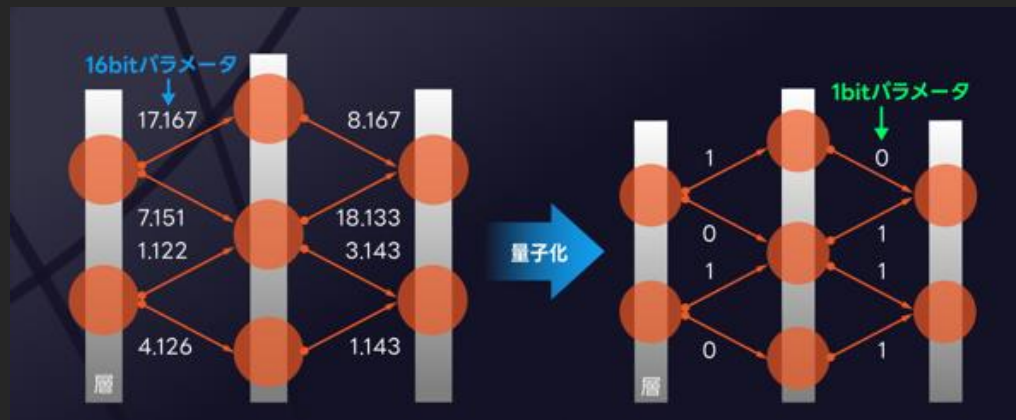


-
- 外部要因によって使えなくならないか
 - 同じ品質のものが継続的に動作するか

Sovereign AIを支える量子化技術

量子化とは

AIの頭脳「ニューラルネットワーク」内の小数点演算を簡単な形式に置き換えて圧縮し、AIモデルのメモリと計算を軽くする技術

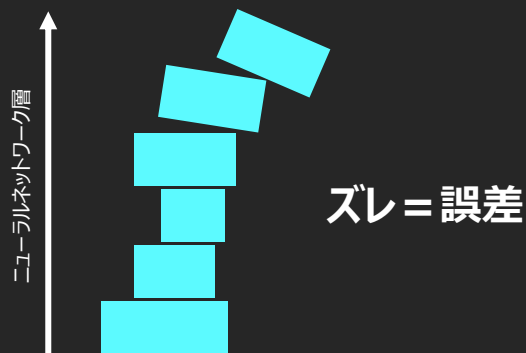


課題

少ないビット数に置き換えるほど精度が落ちる
1ビットでは実用レベルが存在しない

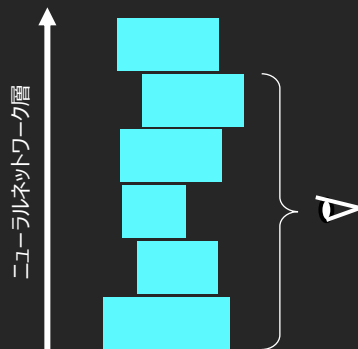
富士通の1ビット量子化技術

従来技術



各層にズレが発生し、層数が増えるにつれズレが大きくなり崩れる（精度崩壊）

QEP (Quantization Error Propagation)



誤差伝搬法

ズレを見ながら、全体がまっすぐ積み上がるように調整する方法

キャリブレーションデータ活用

サンプルデータを用いて、安定する位置をあらかじめ決めておく

QQA (Quasi-Quantum Annealing)

デジタルアニーラで培った世界最高性能の大規模最適化アルゴリズム

世界最高の精度維持率89%を達成

業務特化AI学習技術

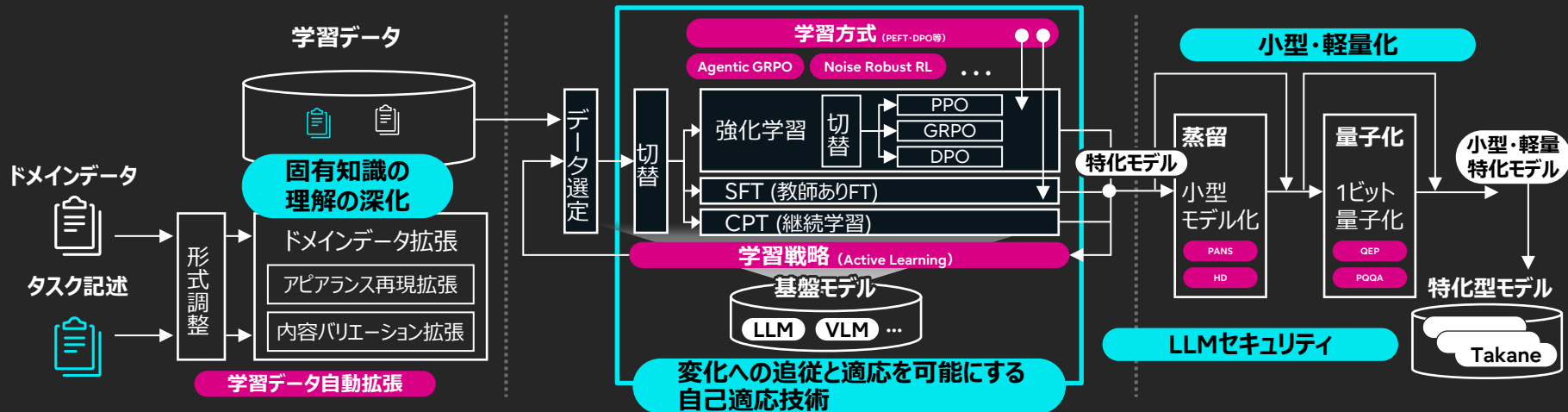
変化する顧客業務に追従し、適応的に学習し、顧客の業務を遂行可能なAIへアップデート

- 領域特化 : 業務固有知識の理解深化により、業務課題解決能力の向上
- 柔軟性 : 環境や状況の変化への柔軟な対応と適応

学習データ準備

学習プロセス

最適化



コンピューティング
による加速

AI computing platform

AI computing broker

最適化AIカーネル

マルチAIエージェントフレームワーク

AIエージェントを領域特化、高品質でセキュアなワークフロー自動化

Multi AI Agent Framework

Building



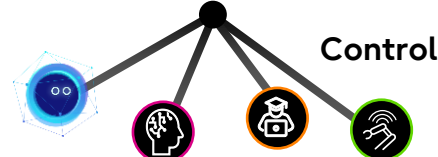
AI Agent

Connecting



Workflow

Orchestration



領域特化



品質



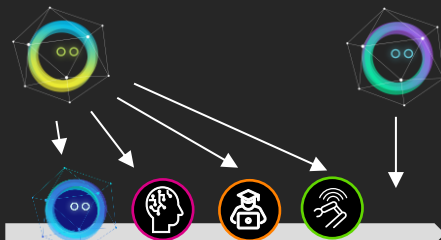
セキュリティ

領域特化

Agentic Memory

連携

人やロボット、他のエージェントから知識を習得
特定領域で成長しながらワークフローを遂行する



ワークフロー

監視

制約付きルーティング

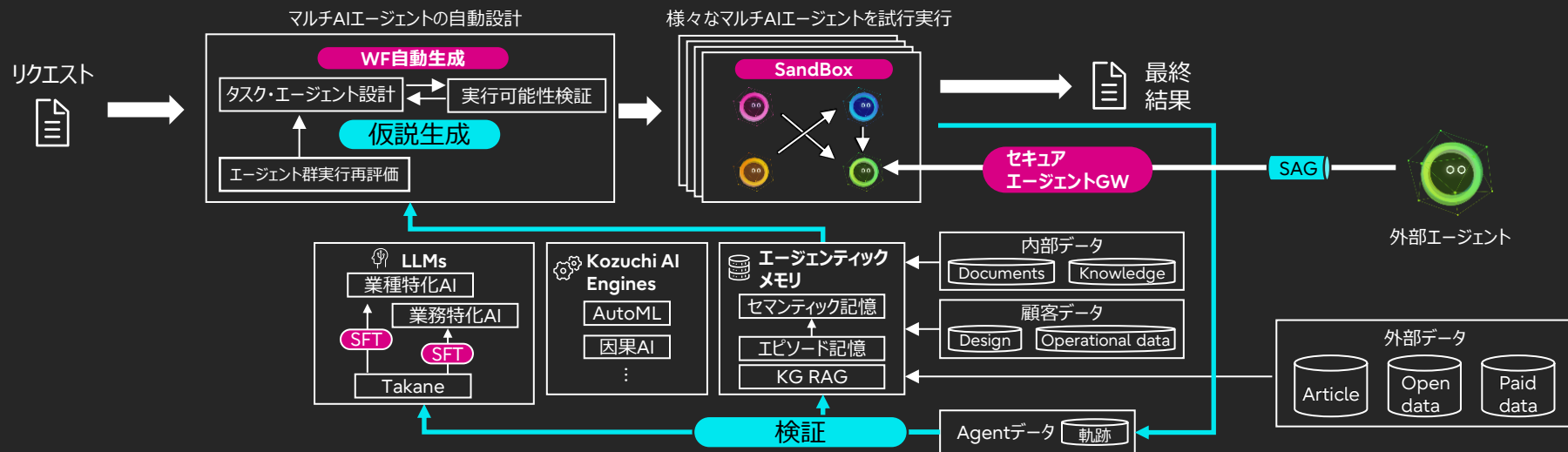
品質

ワークフロー全体の複雑なやりとりを適切に監視
多様な制約を考慮しながらワークフロー遂行を支援

AIエージェント構成技術

試行錯誤を伴うAIエージェント開発を自動化し、業務システムをAI化

- 自己学習するKozuchi AI Agentで、AIエージェント自身の設計や連携を自らが取得
- SandBoxによる試行実行による自己進化



コンピューティング
による加速

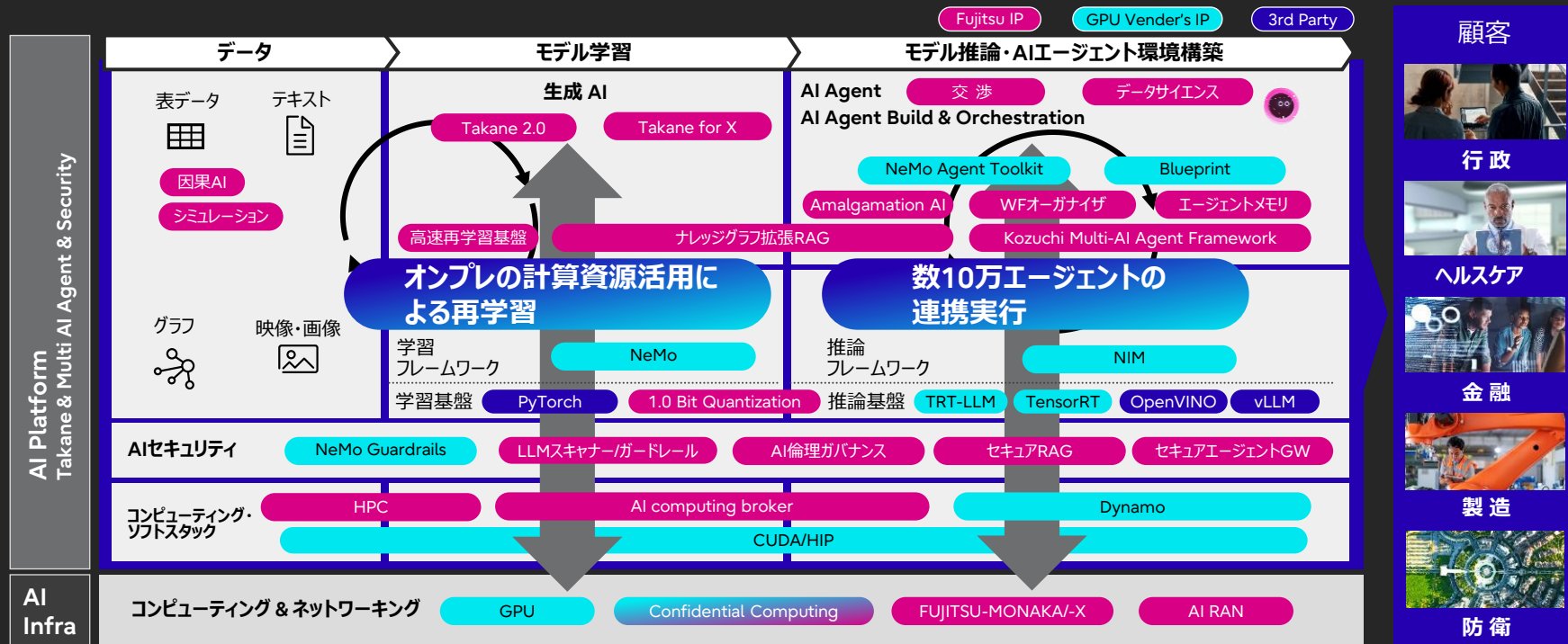
AI computing platform

AI computing broker

エージェント処理高速化基盤

主権を持ったAIエージェントの実現

- セキュリティを担保したオンプレAIや大規模エージェント連携を可能にする基盤を提供
- 顧客が主権をもってAIを運用するオンプレ/プライベートクラウドPFを実現



世界最高レベルのスパコン開発で培った技術



@RIKEN

高性能かつ省電力性を
AI向けに追求した
Made-in-Japan CPU

FUJITSU-MONAKA



汎用CPUとしてMONAKAを新たに開発
複数世代にわたり技術を進化させ、お客様に継続的な価値を提供いたします

2020

A64FX

- ・スーパーコンピュータ「富岳」に採用
- ・Arm SVEを初めて適用



7nm

2027

FUJITSU-MONAKA

- ・高速データ処理基盤を実現
- ・高い電力効率と性能を両立
- ・高信頼・高セキュリティ環境を提供



2nm

2029

FUJITSU-MONAKA-X

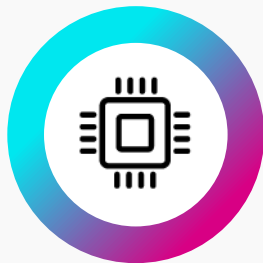
- ・次世代プロセスノードを適用
- ・「富岳NEXT」に採用
- ・NVIDIA社協業によるGPUとの密結合



1.4nm

富士通独自の技術で実現する競争力

高い処理性能



高い電力効率

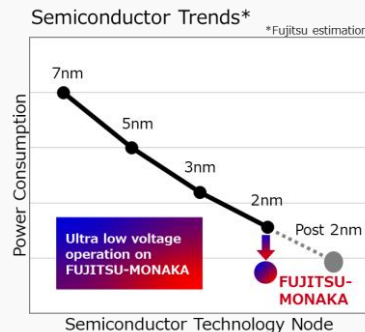


電力効率 約2倍

3Dメニーコアアーキテクチャ



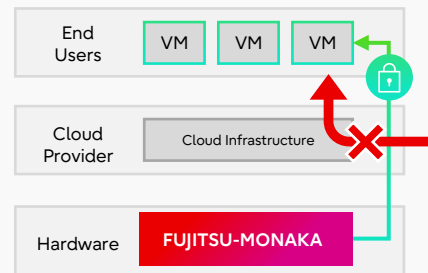
超低電圧動作技術



信頼性とセキュリティ

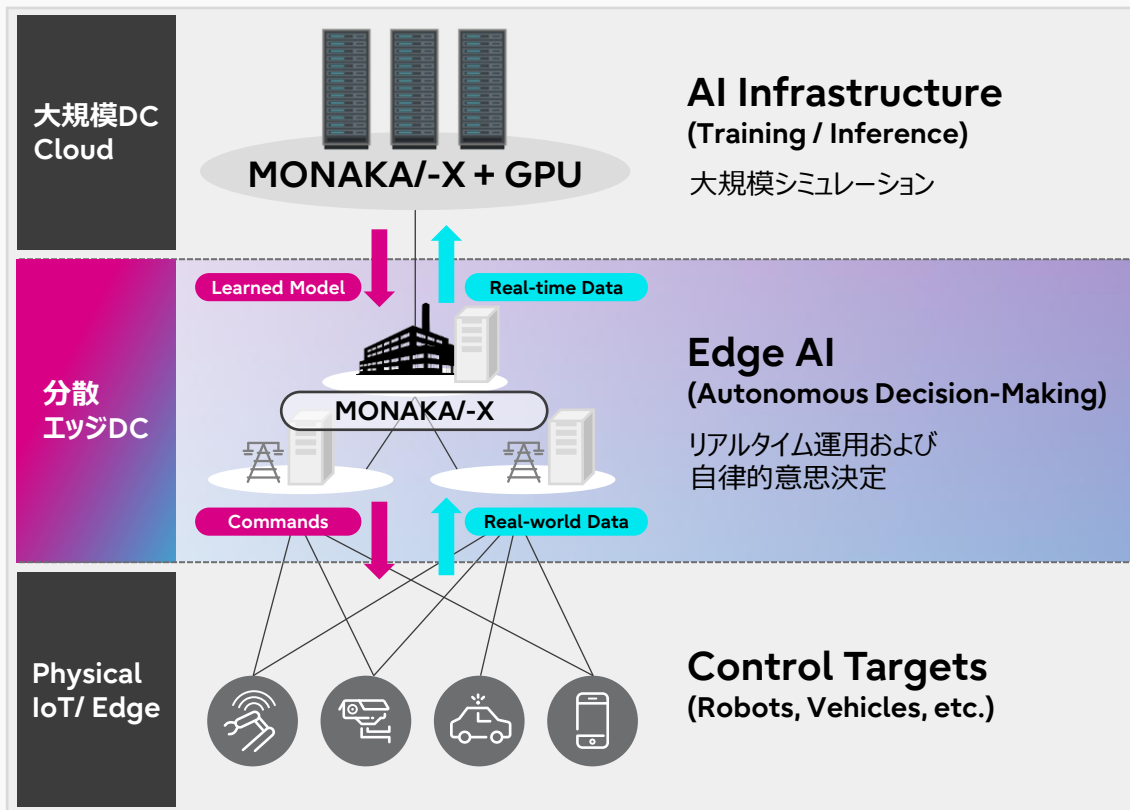


Confidential Computing



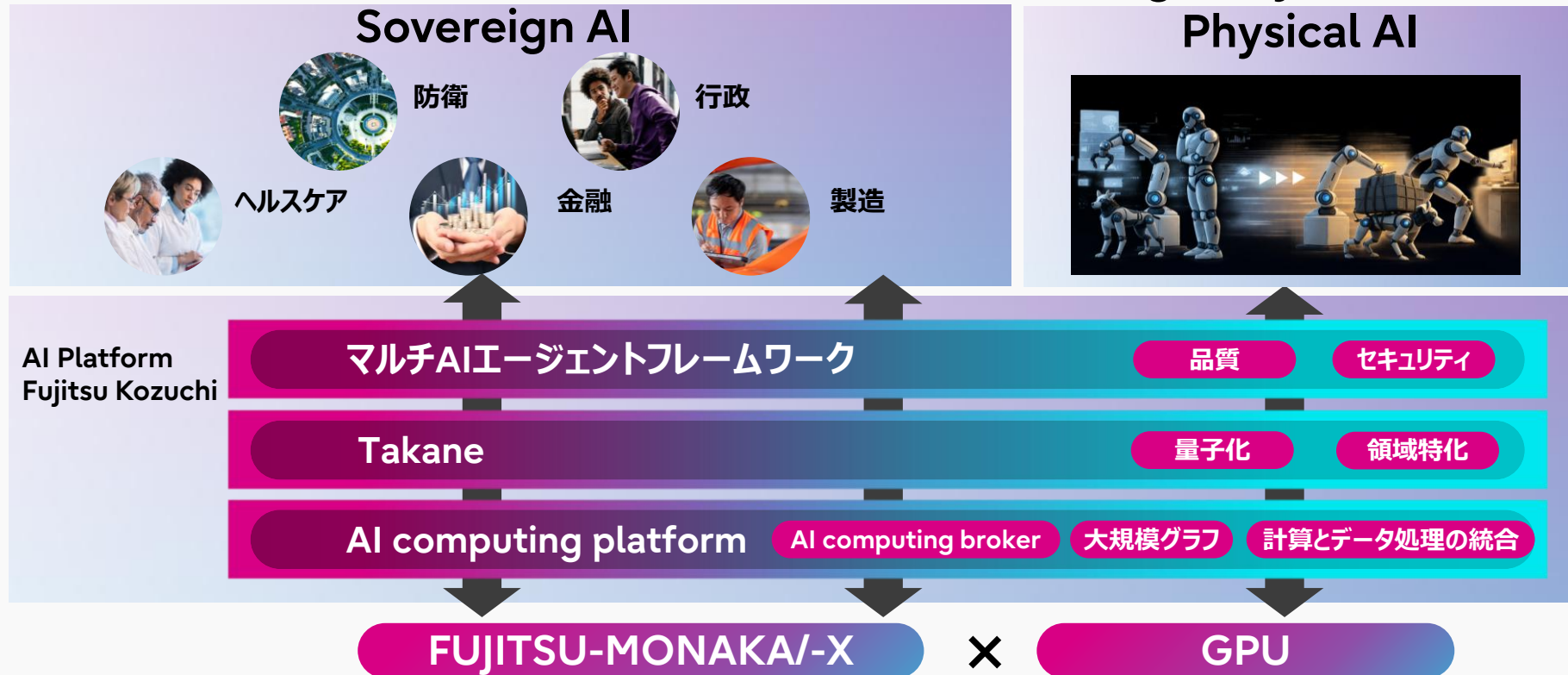
プロセッサが信頼の基点->国産であることの信頼性

Agentic AI時代の分散型DCの社会実装に寄与



自律型AIプラットフォームFujitsu Kozuchi

コンピューティングとの有機的垂直統合で現場で使えるSovereign/Physical AIを提供



お問い合わせ

本資料に関するお問い合わせは
以下までお気軽にご連絡ください。



contact-events-fed@cs.jp.fujitsu.com

Thank you

