R&Dフェーズ｜研究　**実用化時期**｜FY28-

Mehr Licht!
More Photonics for Intelligence

#A06

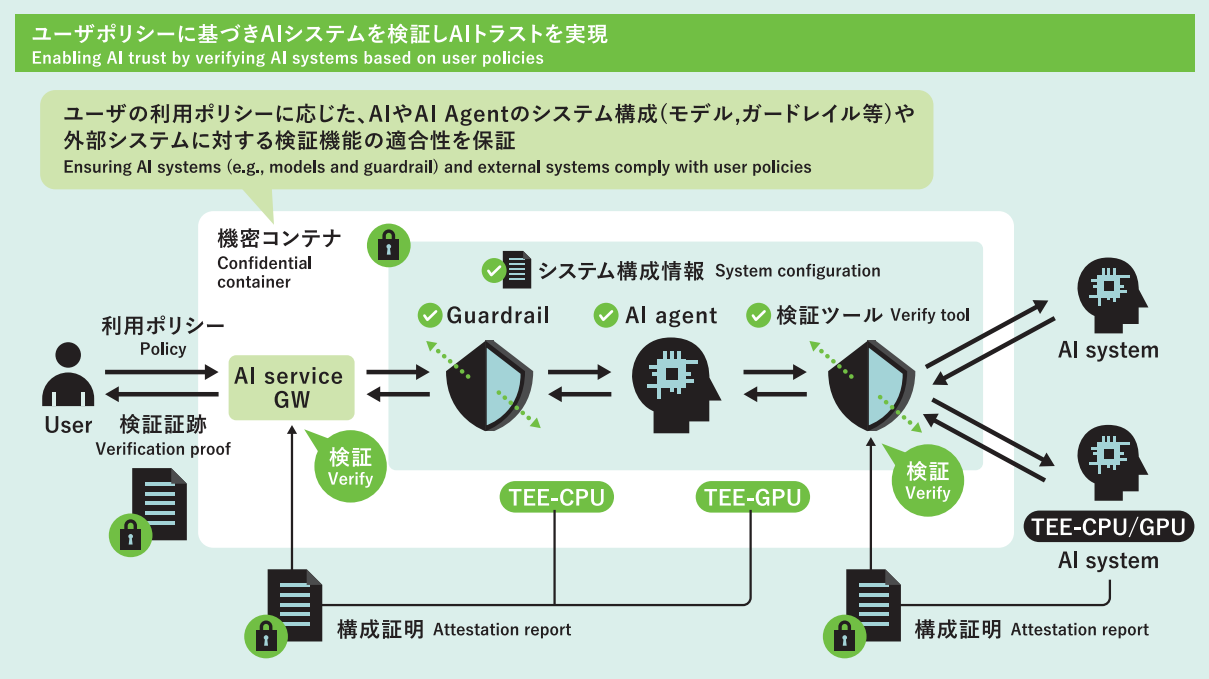
#AI・光量子基盤#AI倫理・責任あるAI#安心・安全

AIのトラストを実現するコンテナ実行環境

利用するAIやAIエージェントが期待通りの構成・動作であり安全であることを検証します

技術課題・ゴール

AIの利用拡大が期待される一方、入力した個人情報等が意図に反して利用されないか、AIが想定外の動作をしないかといった不安が、安心して利用する上での課題です。従来は利用者自身がその安全性を確認することが困難でした。AI及びAI-Agentの実行環境やモデル、データ利用方針、安全機構などを技術的に検証可能にし、提供者を暗黙に信頼することなく安心して利用できる社会を実現します。



技術ポイント

要素技術

・TEE-CPU/GPU対応の機密コンテナによる、AIやAI-Agentのデータ機密性とアプリケーション完全性の技術的保証
・アプリケーションの改修不要で、複数コンテナ構成や機密性を保ったデータ永続化にも対応する汎用基盤

市中技術差異点

・提供者を暗黙に信頼せず、利用者自身がAIやAI-Agentの構成と安全性を検証できる仕組み
・特定のAIに依存せず、市中のAI-AgentやLLMなどのAIモデルの任意の実装を検証できる汎用的な仕組み

適用ビジネス/ユースケース

コミュニケーションサービス

予約・購買等を代行するAI-Agentについて、個人情報が外部送信や学習に使われないか、安全性等が確認されたAIモデルが実際に使われているか、想定外の動作を防ぐ仕組みがあるかを検証し、安心してデータや操作を任せられる環境を実現します。

出展組織
NTT株式会社 ネットワークサービスシステム研究所

関連情報URL
https://www.rd.ntt/ns/inclusivecore.html