

守れるから、任せられる。境界を超えて、価値をつなぐ。

「Trusted Data Fabric™」構想を始動

～組織の壁を越えて AI とデータを安全につなぎ、AI に任せられる業務とデータを拡大～

NTT ドコモビジネス株式会社(旧 NTT コミュニケーションズ株式会社、以下 NTT ドコモビジネス)は、AI とデータの信頼性を高め、安心して AI エージェントを活用できる環境の実現に向けて「Trusted Data Fabric™」構想(以下 本構想)を始動します。本構想は、企業の各組織が自らのデータを管理する権限を持ったまま、組織内外のさまざまな AI エージェントやデータと安全に連携できる環境の実現をめざすものです。「その AI は信頼して利用できるか」「誰が・何を・どこまで利用できるか」「データを守りながら活用できるか」という 3 つの視点から、AI とデータの信頼性向上を図ります。これにより、AI に任せられる業務や AI が活用できるデータの範囲を広げ、企業における AI 活用の高度化をめざします。

1. 背景

近年、生成 AI は、指示に応じて回答する段階から、自律的に判断・実行を行う AI エージェントへと進化しました。企業では、AI エージェントが業務システムや社内のデータを活用して、自ら業務を実行する段階へと利用が広がりつつあります。こうした中、一つの依頼を複数の AI エージェントが分担し、組織を横断して業務を進める場面も増えています。AI エージェントが業務のなかで高い価値を発揮するためには、組織にまたがるデータや AI を安全かつ信頼性の高い形で活用できる環境が求められます。

一方、AI エージェントの活用を重要な業務や価値あるデータにまで広げるにあたっては、2 つの課題があります。

第一に、AI エージェントの権限や判断の根拠を確認できないことです。人を前提とした従来の ID や承認の仕組みでは、どの AI エージェントが、誰の委任を受け、どこまでの権限で動いているのかを把握することが困難です。そのため、正規の認証や人の承認を経ている、判断の根拠や権限の流れを後から説明できない場合があります。

第二に、価値あるデータほど AI エージェントが活用できないことです。機微なデータを守りながら使う手段がないため、データを「使わせない」か「すべて見せる」かの二択になり、AI エージェントの活用は定型業務にとどまりやすくなります。

こうした課題を解決するためには、業務を担う主体として AI エージェントを管理し、データを守りながら活用できる新たな仕組みが必要です。

2. 本構想の概要

本構想では、管理・統制された AI エージェントが機微なデータも含めて活用しながら、これまで人が担う必要があった重要な業務を担えるようにすることをめざします。本構想は次の 3 つの領域で構成され、NTT ドコモビジネスは、それぞれの領域においてサービスの提供や技術開発を進めています。

(1) AI を安全に使うために判断と行動を統制する「Trusted AI」

AI エージェントが実行しようとする行動を直前に判定し、誤った行動を未然に止められるようにします。また、攻撃や乗っ取りから AI エージェントそのものを守るとともに、実行履歴を記録し、管理・監

査できるようにします。こうした統制を実現するサービスとして、企業専用の外部から切り離された環境で AI エージェントを利用できる「クローズド AI エージェント※¹」(2026 年 8 月提供開始)や、AI が不適切な回答や情報の取り扱いをしないよう、日本語の表現に対応して監視する「Chakoshi®※²」などを提供しています。

(2)「誰が・何を・どこまで使えるか」を管理する「Trusted Identity」

利用者や AI エージェントの本人性・真正性を確認し、あらかじめ許可された範囲でのみデータやシステムを利用できるようにします。この仕組みを支えるサービスとして、利用者の認証・権限管理を行う「SmartLiTA®※³」の対象を AI エージェントにも拡張して提供する予定です。加えて、AI エージェントの提供者や権限などの情報を登録・確認できる「AI エージェント属性情報レジストリ(仮称)※⁴」の実現に向けた検討を進めています。

(3)データを守りながら使う「Trusted Data Access」

機密情報や個人情報を含むデータを、データの保有者が管理権限を保持したまま、組織を越えた連携や分析に利用できるようにします。こうしたデータ活用を実現するサービスとして、データを秘匿したまま分析できる技術を用いた「析秘®※⁵」を提供しております。今後は機能拡張を進めるとともに、AI エージェントが機微なデータを扱うための新たな仕組みを検討します。

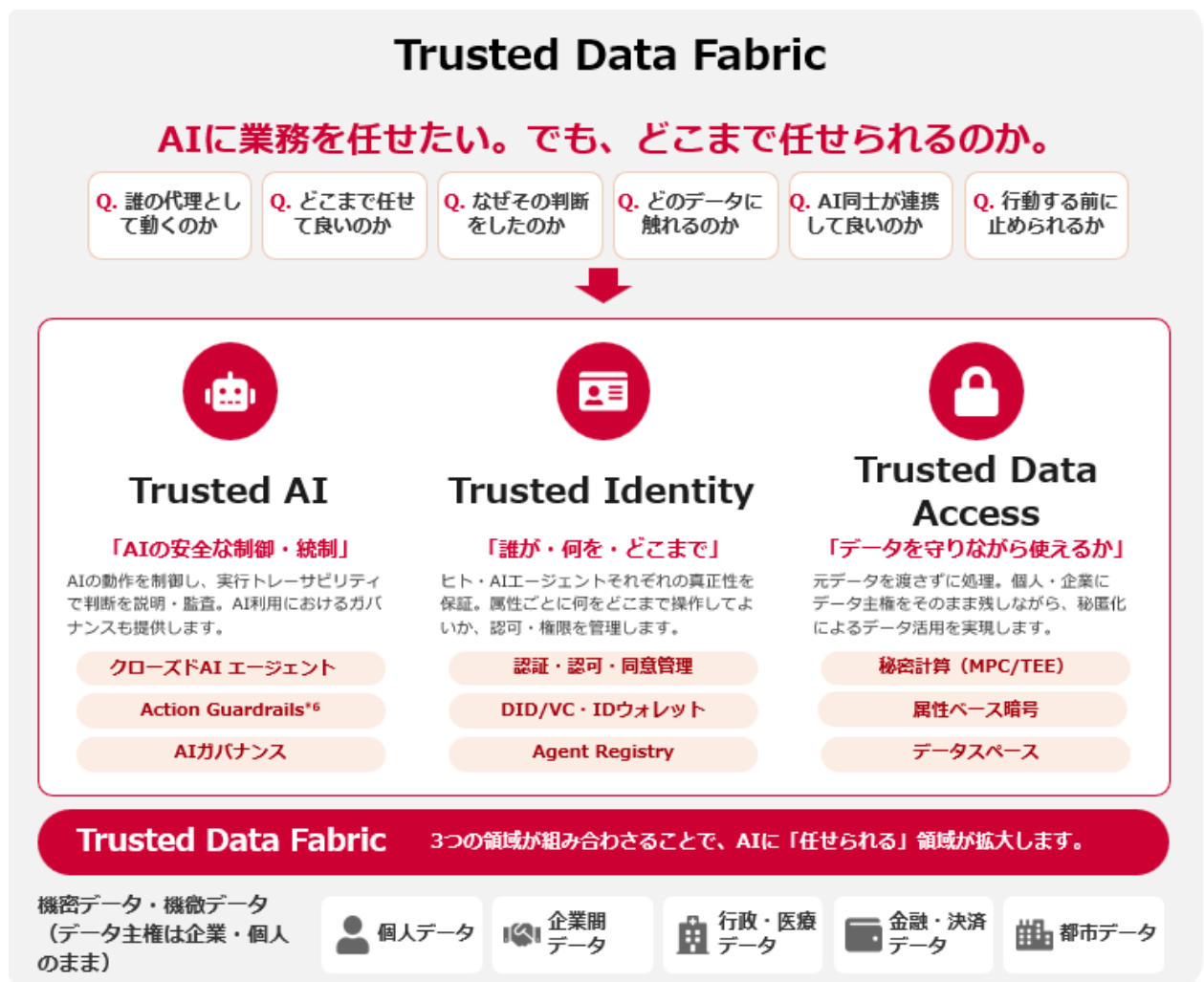


図 1. Trusted Data Fabric を構成する 3 つの Trust

3. 今後の展開・ロードマップ

「Trusted AI」「Trusted Identity」の各領域において、2026 年度中に、AI エージェントの行動を実行前に判定して止める機能(Action Guardrails^{※6})や、AI エージェントの認証・権限管理を行う機能(SmartLiTA[®]の AI エージェント向け拡張)の提供をめざします。あわせて、AI を法令や社内規程に沿って適切に管理・運用するための取り組みを進めます。

「Trusted Data Access」の領域において、データを外部に出すことなく活用する技術や、ハイブリッド・ソブリンクラウド^{※7}を通じて、企業や組織が自らのデータを管理する権限を持ったまま、組織を越えてデータを活用できる環境を整備します。

パートナー企業との連携を拡大しながら、金融、スマートシティ、教育、医療、製造、公共、インフラなどさまざまな分野への展開を進め、将来的には、企業や業界の垣根を越えて AI エージェントとデータが安全に連携できる環境へと発展させていきます。

さらに、AI 時代に最適な次世代 ICT プラットフォーム「AI-Centric ICT プラットフォーム^{®※8}」の機能の一つとして本構想を組み込むことも検討しています。

「NTT コミュニケーションズ株式会社」は 2025 年 7 月 1 日に社名を「NTT ドコモビジネス株式会社」に変更しました。私たちは、企業と地域が持続的に成長できる自律・分散・協調型社会を支える「産業・地域 AX のプラットフォーマー」として、新たな価値を生み出し、豊かな社会の実現をめざします。

つながる。驚きを。幸せを。



<https://www.ntt.com/about-us/strategy.html>

※1：クローズド AI エージェントとは、Trusted Data Fabric を構成するソリューションの一つで、企業専用の閉域環境で AI エージェントを利用できるサービスです。

<https://www.ntt.com/about-us/press-releases/news/article/2026/0817.html>

※2：Chakoshi とは、NTT ドコモビジネスが開発した日本語特化型の AI ガードレールです。

<https://chakoshi.ntt.com/>

※3：SmartLiTA とは、認証認可・同意管理・本人確認を統合した ID 管理プラットフォームです。

<https://www.ntt.com/business/dx/socialinnovation/healthcare.html>

※4：AI エージェント属性情報レジストリ(仮称)とは、AI エージェントの提供者や機能、権限などの属性情報を管理し、AI エージェントの信頼性向上を目的とした基盤です。

<https://www.ntt.com/about-us/press-releases/news/article/2026/0512.html>

※5：析秘とは、機密性の高い情報を秘匿化したまま保管・加工・分析するセキュアなデータ利活用サービスです。

<https://www.ntt.com/business/services/secihi.html>

※6：Action Guardrails とは、AI エージェントが何かを実行する直前に「本当に実施してよい行動なのか」をチェックする仕組みのことです。

※7：ハイブリッド・ソブリンクラウドとは、データ主権を確保する「ソブリン環境」と、ハイパースケーラーが提供するパブリッククラウドを組み合わせた運用形態のことです。

※8：AI-Centric ICT プラットフォーム[®]とは、企業が AI を活用して、生産性の抜本的改善、競争力強化やビジネスモデル変革を進める AI 時代に最適な次世代 ICT プラットフォームのことです。

<https://www.ntt.com/business/lp/aicentricictpf.html>