PRESS RELEASE

報道関係者各位

2026 年 5 月 27 日

コグニザント、企業によるエージェント型システムの安全な拡張を支援する「Cognizant Secure AI Services」の提供開始を発表

企業全体に AI を活用した防御を提供する新サービスで、AI システムにおける「実証可能な信頼」の実践をサポート

コグニザント（NASDAQ: CTSH）は、企業が事業全体で AI やエージェント型システムを安全に保護、ガバナンス、拡張できるように設計された新しい統合サービス「Cognizant Secure AI Services」の提供を開始しました。

AI システムが全社的に導入されるようになり、組織は意思決定、自動化、顧客エンゲージメント、主要なワークフローに AI を組み込むようになりつつあります。このようなシステムは、企業のデータや各種システム、外部アプリケーションと連携しながら、推論や対話、業務実行を自律的に行うエージェント型機能を備えるようになっています。この変化は、ビジネスに変革をもたらす価値を秘めている一方で、従来のサイバーセキュリティモデルでは対応しきれないセキュリティ、ガバナンス、および実行時における新たなリスクも引き起こします。

従来のセキュリティは、あらかじめ動作が決められている決定論的なソフトウェアを前提として構築されてきました。一方、AI システムは確率に基づき状況に合わせて動作するため、従来型のセキュリティツールでは検知できない方法で悪用される可能性があります。改ざんされたモデルや悪意あるプロンプト、エージェントの誤作動などは、間違った行動を大規模に引き起こす恐れがあります。

今回発表したサービスは、企業がこれまでの「暗黙の信頼」から、証拠や追跡可能性、継続的な保証に基づく「実証可能な信頼（provable trust）」へ移行できるように設計されています。コグニザントは、AI システムに対する信頼性を構築と運用の二段階のアプローチで確保しています。第一に、構築段階では、導入前にモデル、データ、パイプラインを保護します。第二の運用段階では、本番環境で AI の挙動を継続的に監視し、不正な操作の検知や、安全性に問題のある動作の管理・軽減を支援するとともに、監査対応を支える証拠を保存します。

コグニザント サイバーセキュリティサービスライン グローバル責任者のヴィシャル・サルヴィ は、「AI は、企業システムの振る舞いを根本的に変えつつあります。これらのシステムは適応性があり、状況に応じて動き、ますます自律的になっています。それらを保護するためには、構築環境と実行環境の両方にまたがる継続的な保証が不可欠です。『Cognizant Secure AI Services』を通じて、私たちは企業が導入初日から AI システムに信頼を組み込み、システムが進化してもその信頼を維持し続けられるよう支援しています。」と述べています。

「Cognizant Secure AI Services」は、以下の 3 つの基盤をもとに構築されています。

- **「Agent Development Lifecycle（ADLC）」**

    - AI システムの設計、構築、テスト、導入、変更といった全ての段階にわたって保護機能が組み込まれています。
- **「Cognizant Neuro® Cybersecurity」**
    - 脅威への対応、相関分析、監査対応の証拠保全のために、AI と企業システム全体のシグナルを一元管理するシステムです。
- **「Responsible AI」**
    - 「Cognizant Trust™」を通じて提供される、継続的な信頼と保証のレイヤーです。AI システムの規模拡大に伴い、顧客が定義した要件に基づいて、追跡可能性、ポリシーの適用、およびコンプライアンス（法令遵守）への適合をサポートします。

これらの機能が連携することで、AI モデルやデータの保護、利用権限の管理、AI システムの安全な運用、AI エージェントの行動管理、生成 AI 利用時のリスク対策などを包括的にカバーし、企業が AI 運用のあらゆる段階でシステムを安全に管理できるようにすることを目指しています。

コグニザントはすでに、規制の厳しい業界を中心に世界 250 社以上の企業と協力し、AI 導入を含むデジタルトランスフォーメーション・プログラムの評価、保護、運用化を進めています。初期の導入事例では、ディープフェイクを利用した詐欺や AI モデルの改ざんの防止から、企業のワークフロー全体で稼働する自律型エージェントや生成 AI システムの保護に至るまで、今日の組織が直面する最も重大なリスクの一部に対処しています。同時に、規制環境下で責任を持って AI を拡張するために必要なガバナンスと監査の枠組みを、クライアントと共同で構築しています。

Everest Group プラクティスディレクターの アルジュン・チャウハン 氏は、「急速に変化する現在の環境において、組織は、AI セキュリティに対して個別のソリューションの寄せ集めではなく、より包括的なアプローチを求めるようになっています。構築フェーズから実行・運用ライフサイクルに至るまで、あらゆるリスクに対処できる統合フレームワークへの需要が高まっています。さらに、現実世界で確かな成果を上げるためには、最高クラスのテクノロジーを一貫した運用モデルに統合する能力が重要になってきています。強固な統合サイバーセキュリティ基盤を提供しつつ、AI 固有のセキュリティ機能へと柔軟に拡張できるプラットフォームは、企業規模で拡張可能な成果を提供する上で有利な立場にあると言えるでしょう。」と述べています。

企業の既存システムとの統合を前提に構築され、規制への準拠と運用の回復力をサポートする「Cognizant Secure AI Services」は、「実証可能な信頼」の実践を通じて、組織が AI を安全に拡張できるよう支援します。詳細については、「Cognizant Secure AI Services (英語)」をご覧ください。

コグニザントについて

コグニザント（NASDAQ: CTSH）は、AI Builder およびテクノロジーサービスプロバイダーとして、お客様にフルスタックの AI ソリューションを構築することで、AI 投資と企業価値を結ぶ架け橋となっています。業界、ビジネスプロセス、エンジニアリングに関する当社の深い専門知識を活かし、組織固有のビジネス環境をテクノロジー・システムに組み込みます。これにより、人間の可能性を最大限に引き出し、確かな成果を実現するとともに、急速に変化する世界においてグローバル企業が常に一歩先を行くための支援を行っています。
詳細については、www.cognizant.com をご覧いただくか、@cognizant をフォローしてください。

※本リリースは US 本社の Cognizant Launches Secure AI Services to Help Enterprises Safely Scale Agentic Systems を翻訳したものです。

コグニザントジャパンの詳細は下記ページをご覧ください。
https://www.cognizant.com/jp/ja/about-cognizant