

Japan opens AI agent tools to 180,000 government staff and publishes the Gennai standard

Source copy kept by wheresthe.ai for the story “Japan opens AI agent tools to 180,000 government staff and publishes the Gennai standard” (<https://wheresthe.ai/d/jp-digital-agency-gennai-ai-agents-180000-staff-gennai-standard-2026-10/>).

Source: <https://www.digital.go.jp/policies/genai/agent-safety-standard>

Text saved 20 Oct 2026 (the page as published).

SHA-256 of the saved text: 25a8fc6bdd98721a0abf31b30307a306fbe1c5fc13a42f7ad60648eaf69f3e10

Documents the source offers: https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/b033337d-dad1-4493-9316-d929597e4667/9bbaf559/20261020_policies_genai_guideline_02.pdf; https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/b033337d-dad1-4493-9316-d929597e4667/4c25aead/20261020_policies_genai_guideline_01.pdf; https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/b033337d-dad1-4493-9316-d929597e4667/aaad4788/20261020_policies_genai_guideline_03.pdf

ガバメントAI 源内においてAI エージェント利用環境の提供を開始するとともに、「源内基準」を公表します

政府の業務には、情報収集や文書作成だけでなく、複数の工程を組み合わせる作業や、大量の資料をもとにした高度な調査・分析など、複雑で専門性の高いものが多くあります。しかし、こうした業務でAIを活かすには、既存のAIアプリケーションを使うだけでは十分ではありません。職員自らが業務の内容や目的に合わせてAIエージェントを作成・実行し、使いながら改善を重ねられる環境が必要です。このような環境でAIエージェントを活用することで、現場主導の業務改革、業務の効率化と質の向上、AI活用人材の育成を推進することが可能となります。そこで、デジタル庁は、ガバメントAI 源内において、約18万人の政府職員を対象に、2種類のAIエージェント利用環境の提供を開始します。本日から「エージェントチャット」を各府省庁等へ順次導入を進め、令和8年12月頃までに「源内工房」の導入を目指します。1.「エージェントチャット」：手軽にAIエージェントを作成・実行できる環境 2.「源内工房」：高度なAIエージェントを構築・実行できる環境 当庁の調査によれば、先進的なAIコーディングエージェント（自然言語の指示に基づき、コードの生成・修正、ファイル操作、コマンド実行、テスト等を自律的に進めるAI）に相当する高度なAIエージェント利用環境を、専門職員に限らず一般の職員も日常業務で利用できる政府共通基盤として、約18万人規模で導入する取組は、世界初の試みとなります。また、「エージェントチャット」及び「源内工房」については、地方公共団体や民間事業者等でも幅広く活用いただけるよう、だれでも利用・改変・再配布が可能な「源内OSS（オープンソースソフトウェア）Ver.2.0」として、令和9年2月頃を目途に、公開する予定です。あわせて、政府職員がAIエージェントを安全かつ適切に活用できるよう、関係者に求められる基本的な考え方や遵守事項を定めた「ガバメントAI 源内 ガバナンス・セキュリティ・セーフティに関する基準（「源内基準」）（PDF / 3,905KB）」（以下「源内基準」）を策定しましたので、公表します。AIエージェントは、従来のAIアプリに比べて機能が高度かつ複雑であり、実行できる処理の範囲も広がります。このため、セキュリティやガバナンス等を確保しながら、政府職員が主体的に活用できるルールが必要となります。源内基準では、「利用者」「管理者」及び「開発者」それぞれの立場に応じた責務・遵守事項を明確にしています。なお、源内基準は、AIの安全性に関する評価手法や基準の検討・推進を担う機関であるAIセーフティ・インスティテュート（AISI）の協力を得て策定しました。AIエージェント利用環境の導入を検討する地方公共団体や民間事業者等にとっても、安全性の確保と効果的な活用を両立するためのモデルケースとして、広く参考にしていただけるものと考えています。添付資料 ガバナンス・セキュリティ・セーフティに関する基準（「源内基準」）の策定・公表について（PDF / 857KB） ガバメントAI 源内 ガバナンス・セキュリティ・セーフティに関する基準（「源内基準」）（PDF / 3,905KB） ガバメントAI 源内における「AIエージェント」利用環境の導入（PDF / 1,567KB）