

AWS Summit Japan 2026 ブースセッション

Amazon Bedrock AgentCoreで実現する セキュアなSaaS連携AIエージェントアーキテクチャ

2026年6月25日~26日

NTTデータ

ソリューション事業本部 デジタルサクセスソリューション事業部 AI&データアナリティクス統括部

目次

1. NTTデータが目指す生成AI活用の世界
2. Amazon Bedrock AgentCoreによるセキュアなSaaS連携
3. アマゾン ウェブ サービス（AWS）による生成AI開発プラットフォームの全体像

自己紹介

名 前： 田中 大貴 Daiki.Tanaka@nttdata.com

所 属： 株式会社NTTデータ ソリューション事業本部
デジタルサクセスソリューション事業部 AI&データアナリティクス統括部

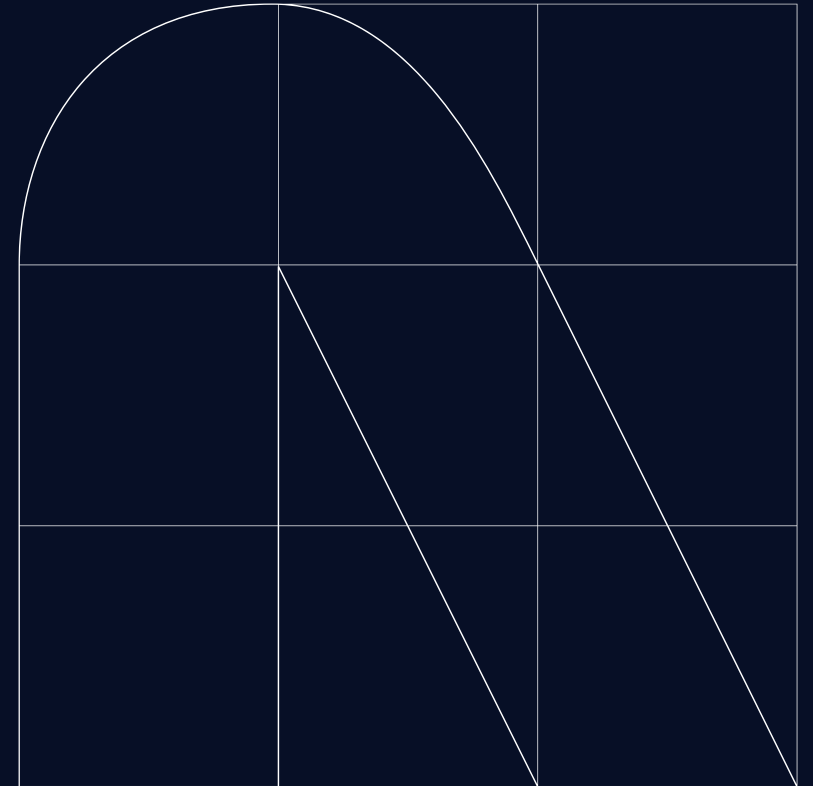
略 歴： 2023年にNTTデータへ入社後、
AWSを活用したデータサイエンスプラットフォームであるTDF-AM推進チームに所属
ITグランドデザイン領域のコンサルティング業務を経験する傍ら、
データ活用基盤の運用保守、AWSを用いた生成AI活用基盤の検討開発に従事



田中 大貴

1

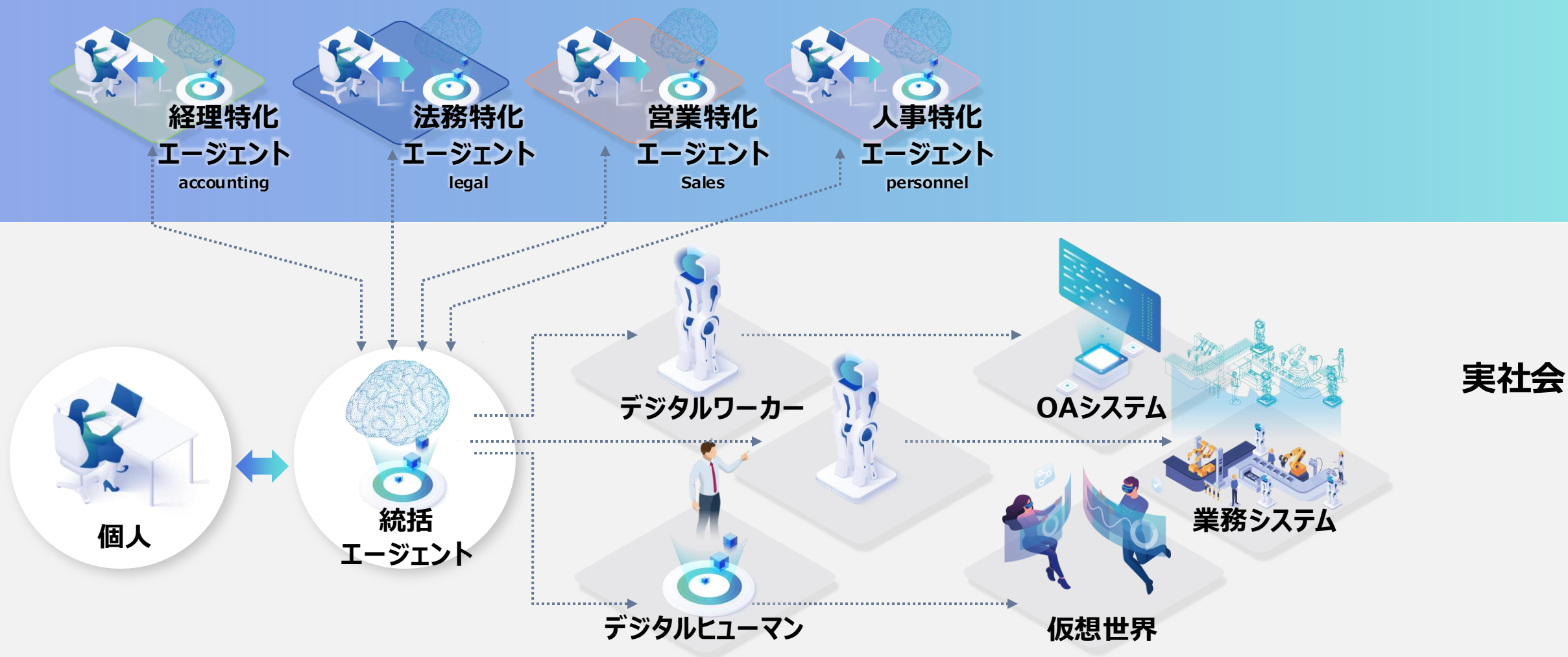
NTTデータが目指す生成 AI活用の世界



NTTデータが目指す世界

NTTデータでは、「**Smart AI Agent™**」を構想し、実現に向け取り組んでいます。

実際の業務に耐えうるだけの専門性を持ったエージェントが自律的に協働し、業務の抜本的変革を目指します。



Smart AI Agentの実現に向けて

Smart AI Agentの実現にはデータ連携・管理や改善サイクルに加え、セキュリティやガバナンスが担保された上での外部ツールとの連携が可能となる基盤が必要不可欠です。

自動化サイクル

一連の生成AIフローをワンストップで自動化。CI/CDパイプラインツールによって、一元管理されたログに基づく自動化サイクルを構築し、AIエージェントが継続的に学習・改善していく仕組み

データ連携・処理

ソースシステムとのデータ連携、分散処理およびノーコードETLツールを用いて、生成AIに利用するデータの前処理や変換を効率化。リアルタイム推論のためのデータ連携の仕組み

コスト管理・パフォーマンス最適化

I/O最適化や最適なクエリプランを自動適用。AIエージェントのスケールアップ/アウト。利用部門ごとのコスト管理の仕組み

データマネジメント（非構造データ）

RAGやトレーニングに利用する画像・テキストなどの非構造化データを安全かつ効率的に管理する仕組み。従来の構造化データのデータマネジメントと同様に、カタログによるメタデータ管理・リネージやデータ品質等の管理

セキュリティ・データマスキング

基盤、データ、APの各レイヤで適切なアクセス制御を行う。データアクセスやAPI呼び出しの履歴を集約・監査し、安全性とコンプライアンスを強化。トレーニングに用いるデータの匿名化や機密情報削除するためのマスキング機能

モデルの評価改善

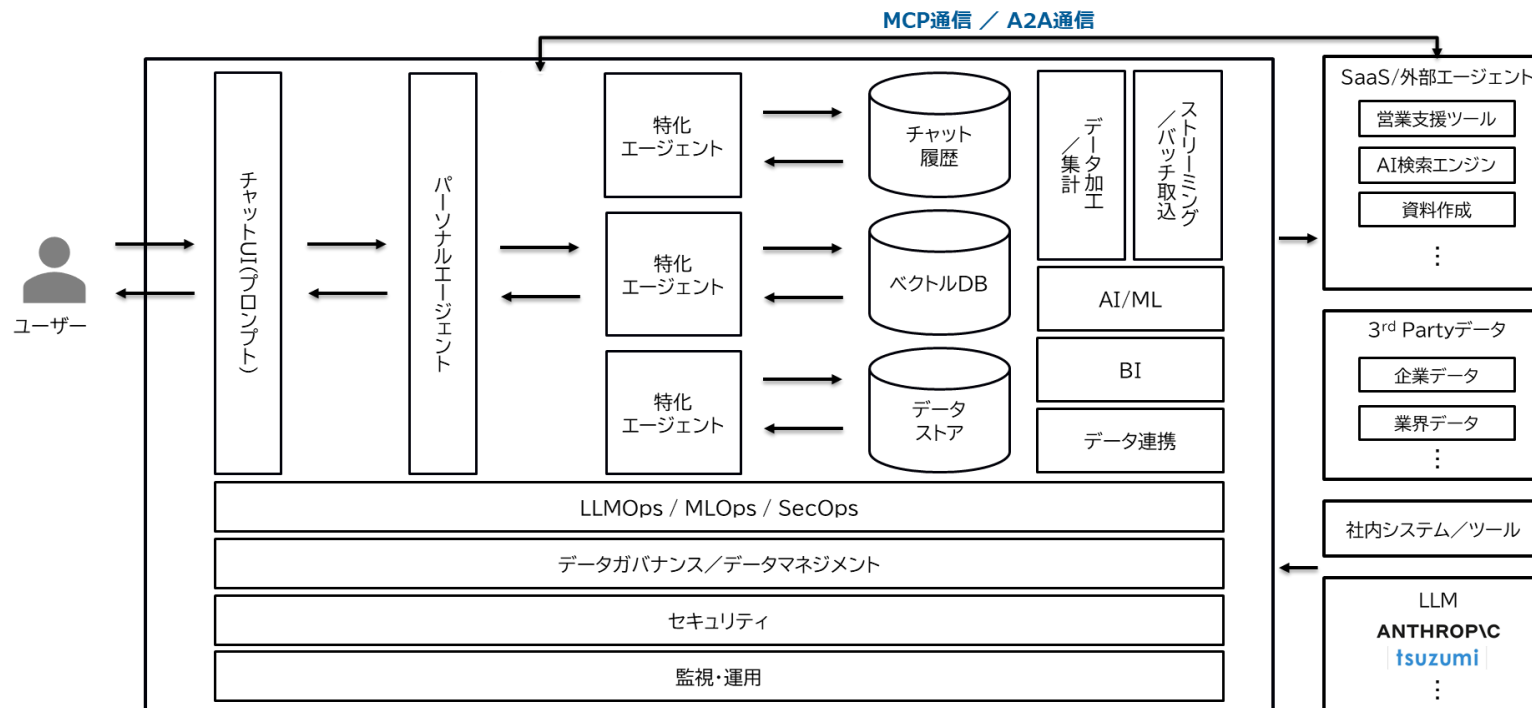
モデル品質を継続的に改善するための仕組み。モデルの評価、ユーザーフィードバック、モデル・特徴量管理など

業務連携・ユーザビリティ

MCP通信やA2A通信を通じて、SaaSサービスや外部エージェントの連携するための仕組み。Salesforce等の業務ツールとの連携

AIガバナンス

テストツール：AIモデルの安全性やセキュリティなどをモニタリングし、異常がないかを評価
ガードレールツール：AIシステムの入出力を常時監視し、望ましくない入出力をブロック



Smart AI Agentの実現に向けて

本セッションでは、Smart AI Agentを実現する基盤の提供を見据えた取り組みとして、業務ツールをセキュアに利用することが可能な生成AIエージェント構築例をご紹介します。

自動化サイクル

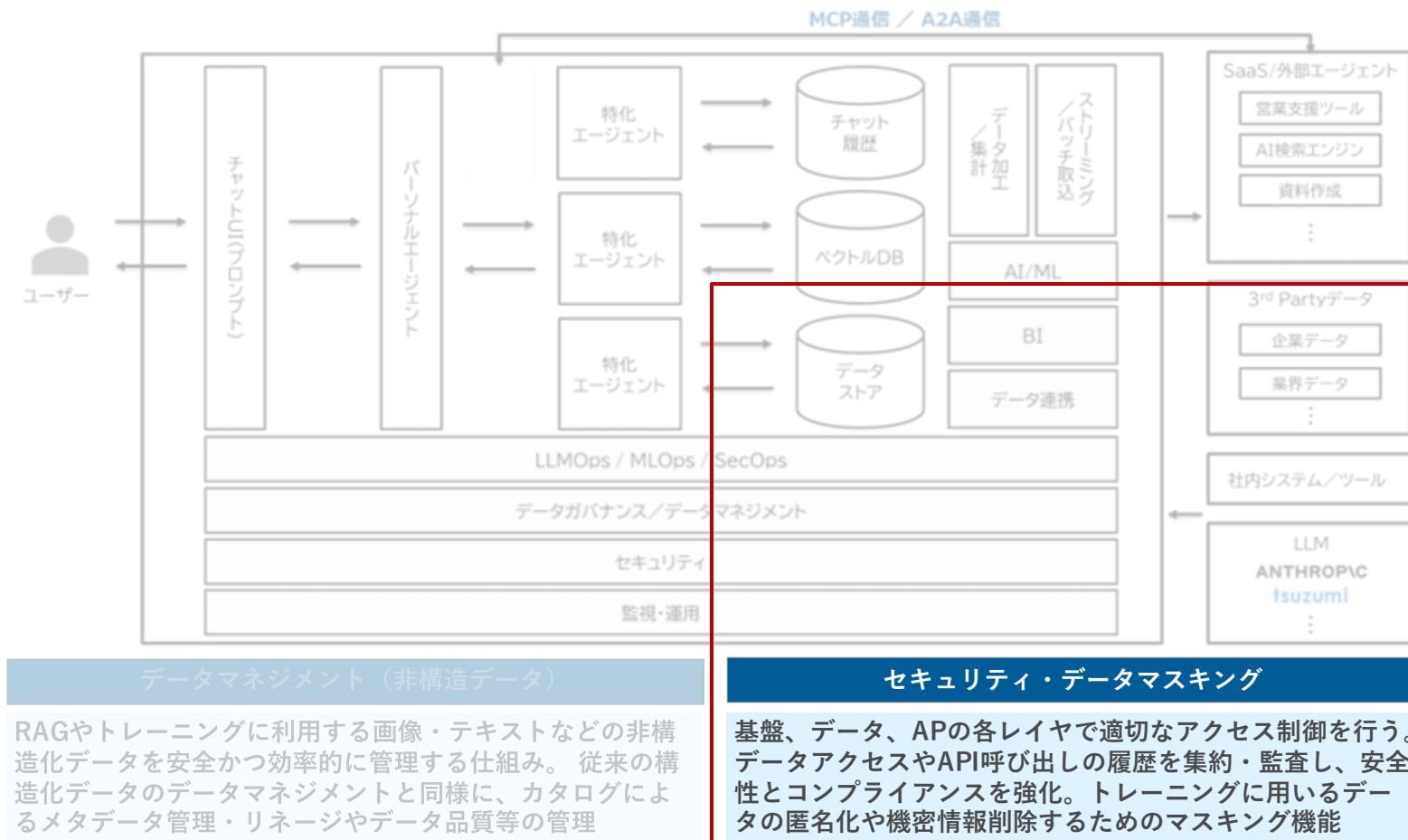
一連の生成AIフローをワンストップで自動化。CI/CDパイプラインツールによって、一元管理されたログに基づく自動化サイクルを構築し、AIエージェントが継続的に学習・改善していく仕組み

データ連携・処理

ソースシステムとのデータ連携、分散処理およびノーコードETLツールを用いて、生成AIに利用するデータの前処理や変換を効率化。リアルタイム推論のためのデータ連携の仕組み

コスト管理・パフォーマンス最適化

I/O最適化や最適なクエリプランを自動適用。AIエージェントのスケールアップ/アウト。利用部門ごとのコスト管理の仕組み



モデルの評価改善

モデル品質を継続的に改善するための仕組み。モデルの評価、ユーザーフィードバック、モデル・特徴量管理など

業務連携・ユーザビリティ

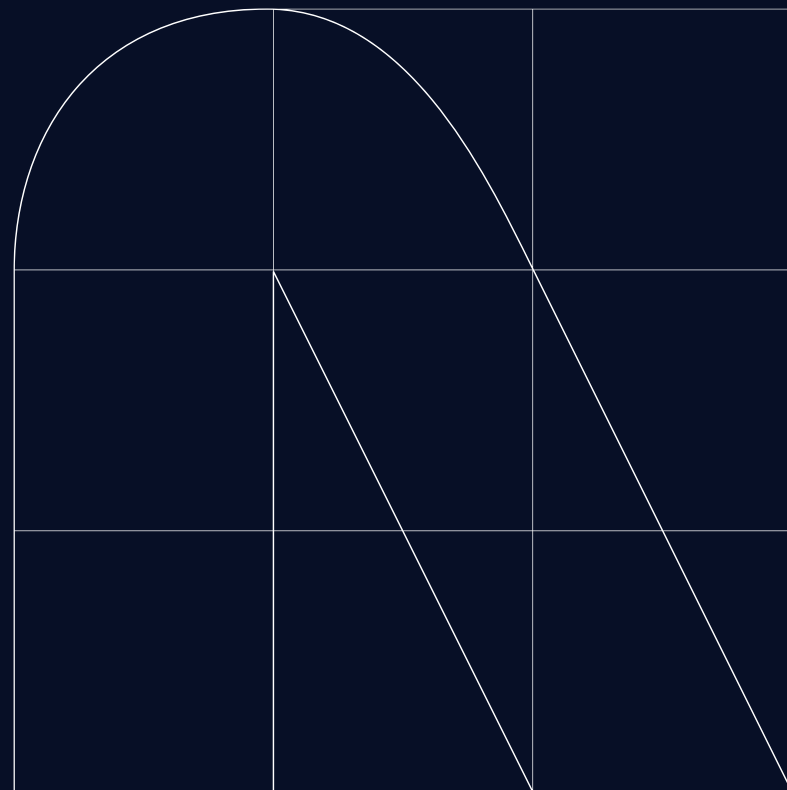
MCP通信やA2A通信を通じて、SaaSサービスや外部エージェントの連携するための仕組み。Salesforce等の業務ツールとの連携

AIガバナンス

テストツール：AIモデルの安全性やセキュリティなどをモニタリングし、異常がないかを評価
ガードレールツール：AIシステムの入出力を常時監視し、望ましくない入出力をブロック

2

Amazon Bedrock AgentCoreによるセキュア なSaaS連携



取り組み概要

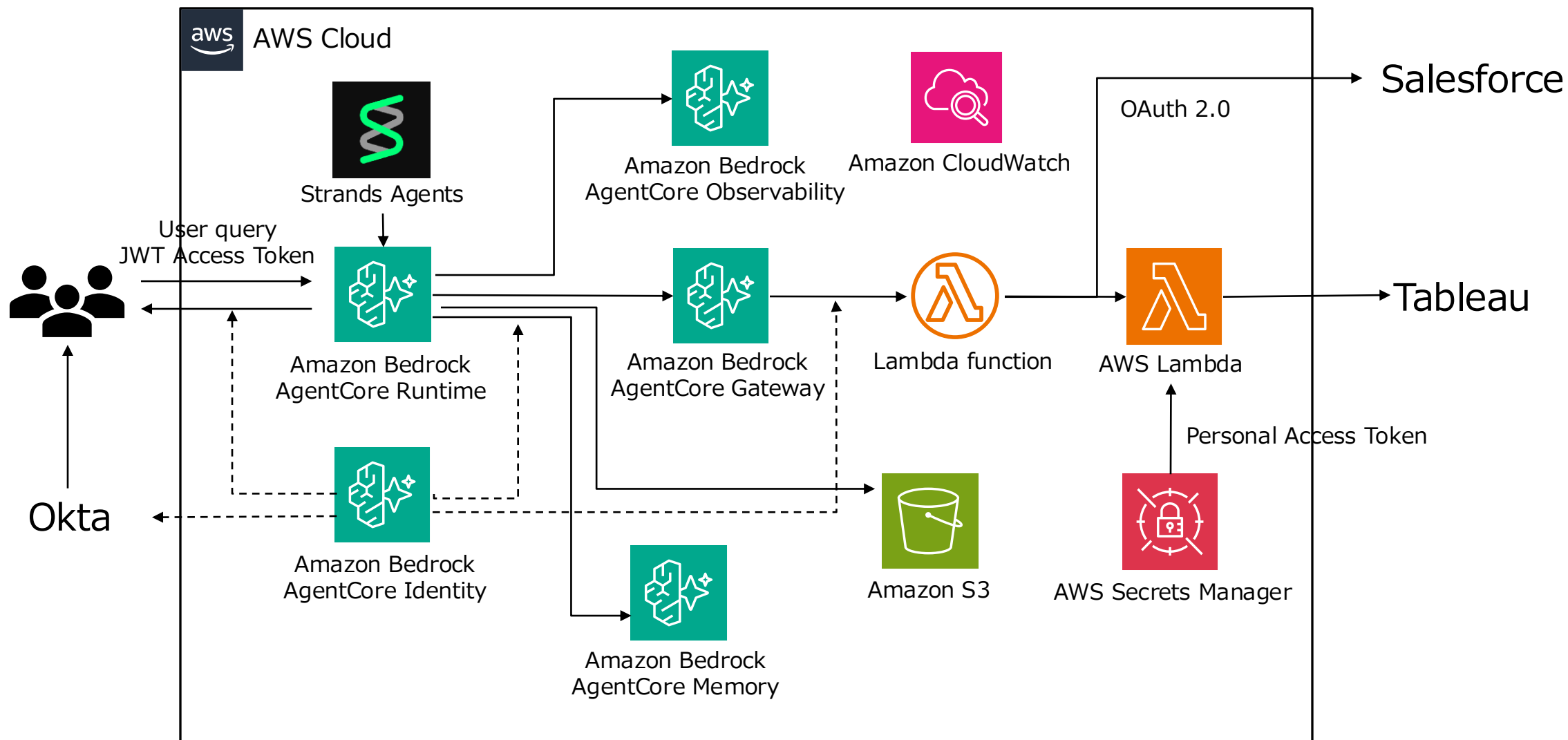
営業部門における「生成AIを用いたレポート作成およびデータ分析自動化」の実現というユースケースを想定した取り組みをご紹介します。外部SaaSとしてSalesforceとTableauから情報を取得し、自然言語による問い合わせに基づいてレポートを生成するAIエージェントをAmazon Bedrock AgentCoreをベースに構築しました。

主なポイント

- Amazon Bedrock AgentCore Runtimeによるセキュアな環境での生成AIエージェント実行
- Oktaによるユーザー認証を利用した生成AIエージェント呼び出し
- Amazon Bedrock AgentCore GatewayによるセキュアなSalesforce・Tableau接続

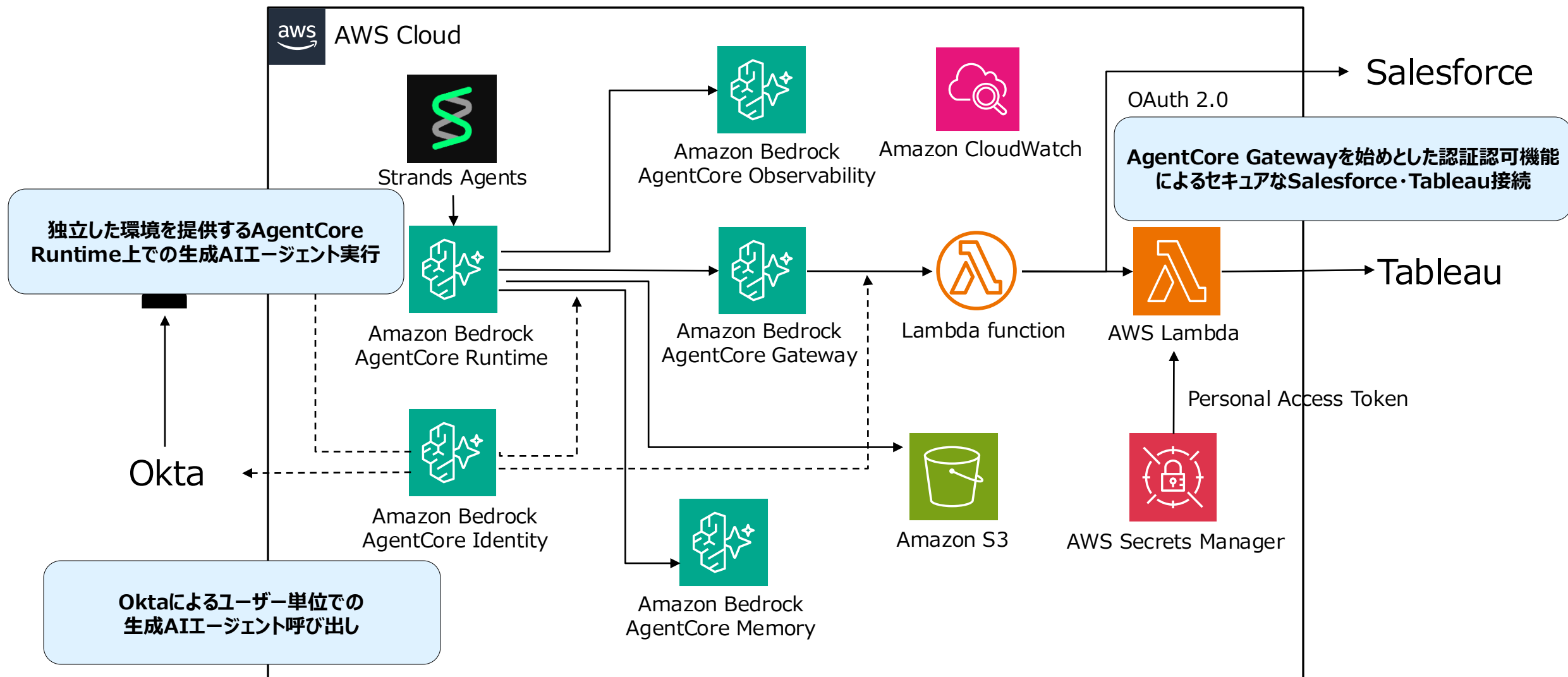
アーキテクチャ構成

Oktaによりユーザー認証され呼び出された生成AIエージェントが、認証認可を通してSalesforceやTableauからデータを参照・解析するアーキテクチャ構成となります。



アーキテクチャ構成

Oktaによりユーザー認証され呼び出された生成AIエージェントが、認証認可を通してSalesforceやTableauからデータを参照・解析するアーキテクチャ構成となります。



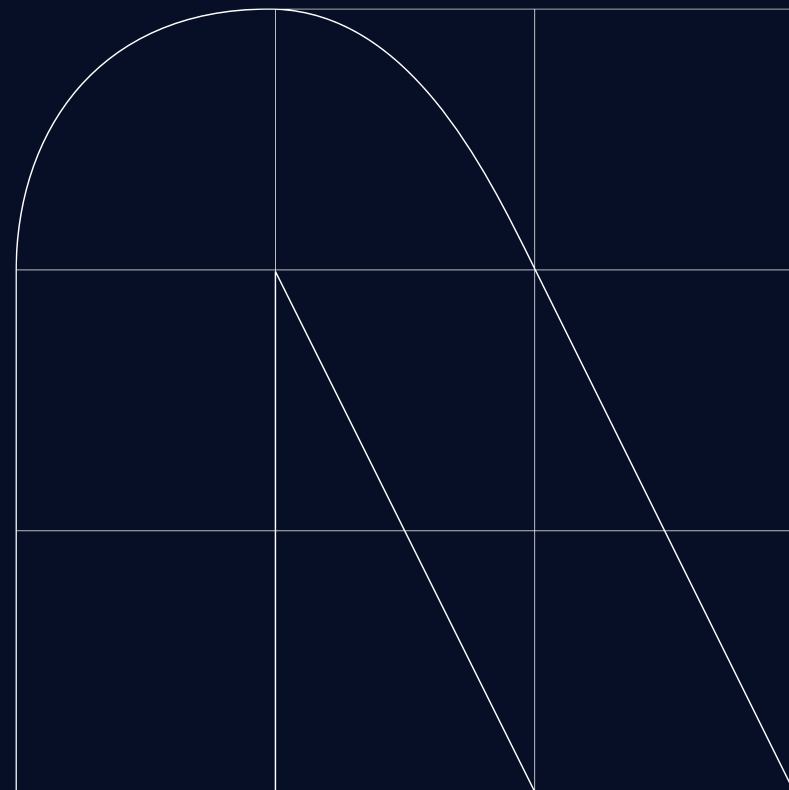
実装デモ

実装した生成AIエージェントの動作を、デモにてご紹介します。

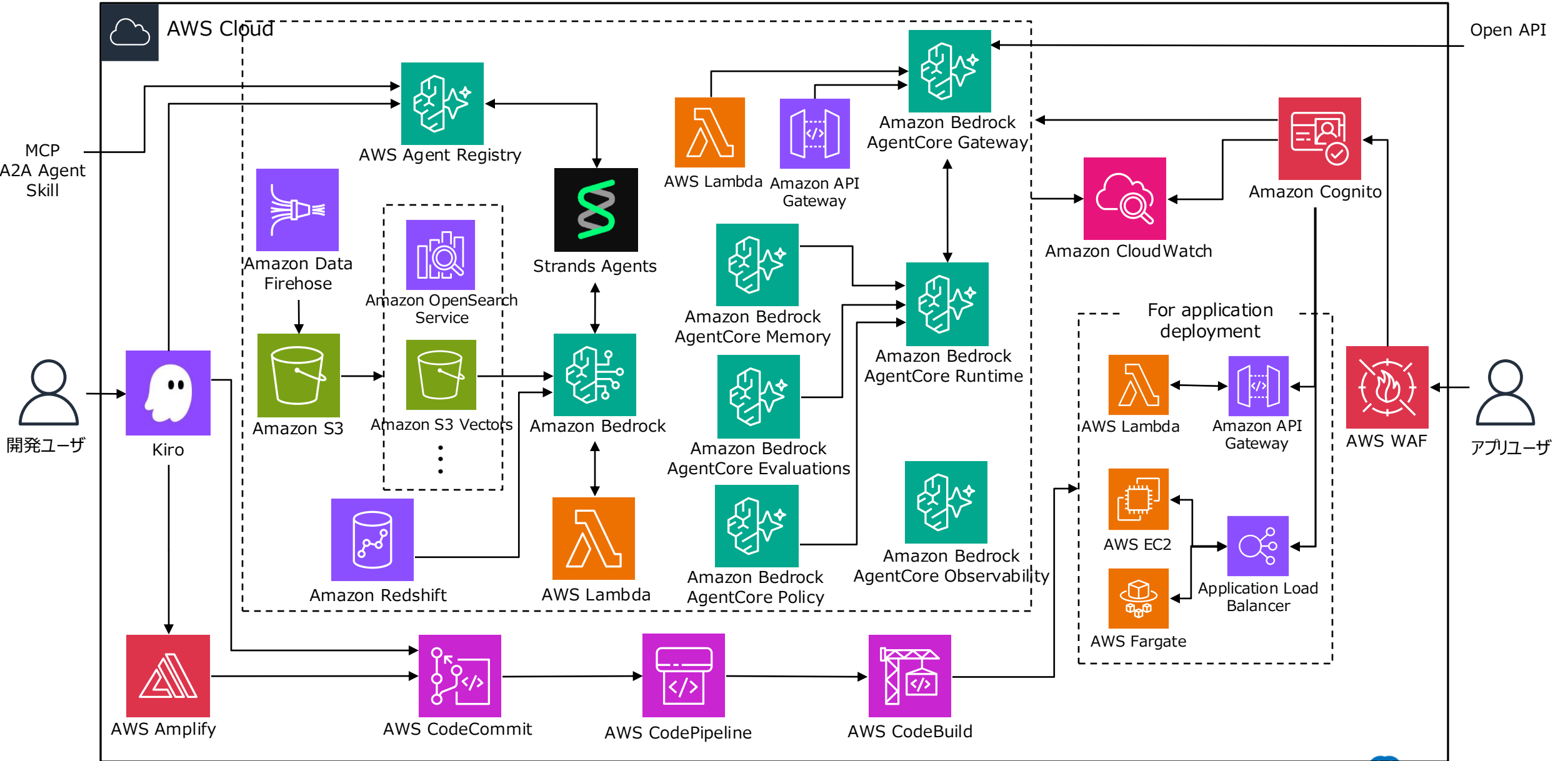


3

AWSによる生成AI開発 プラットフォームの全体像



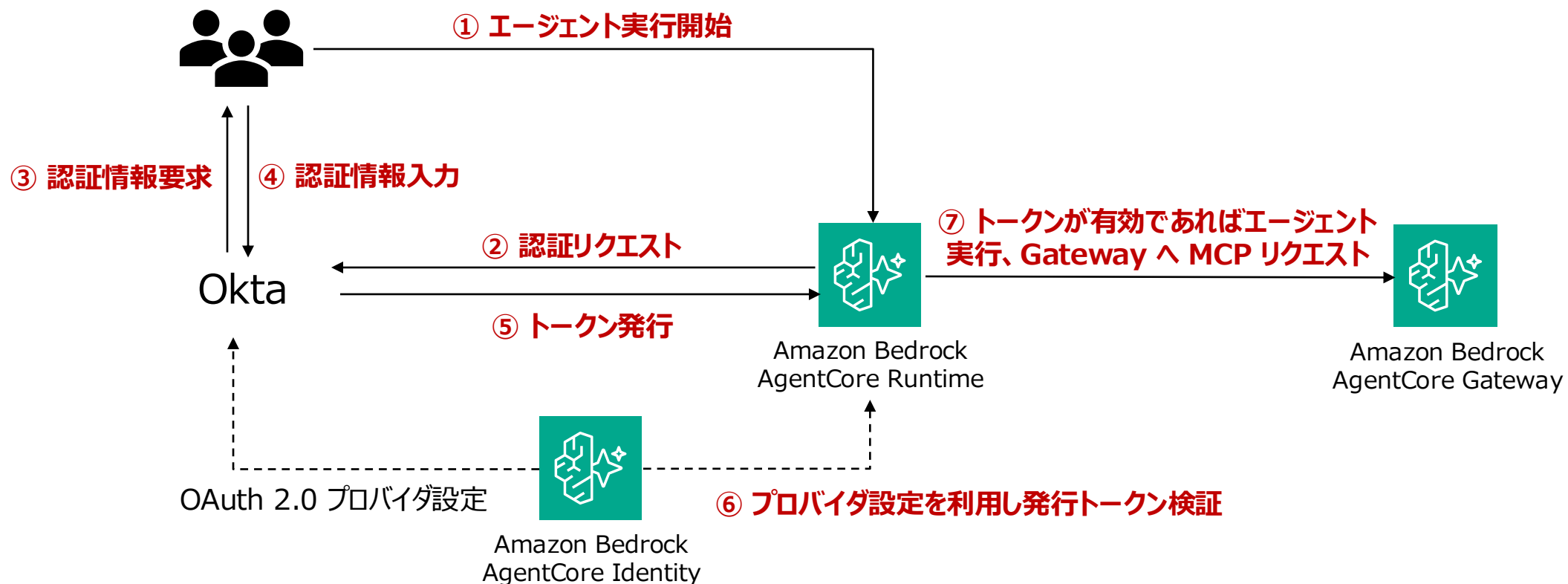
生成AI開発プラットフォーム例





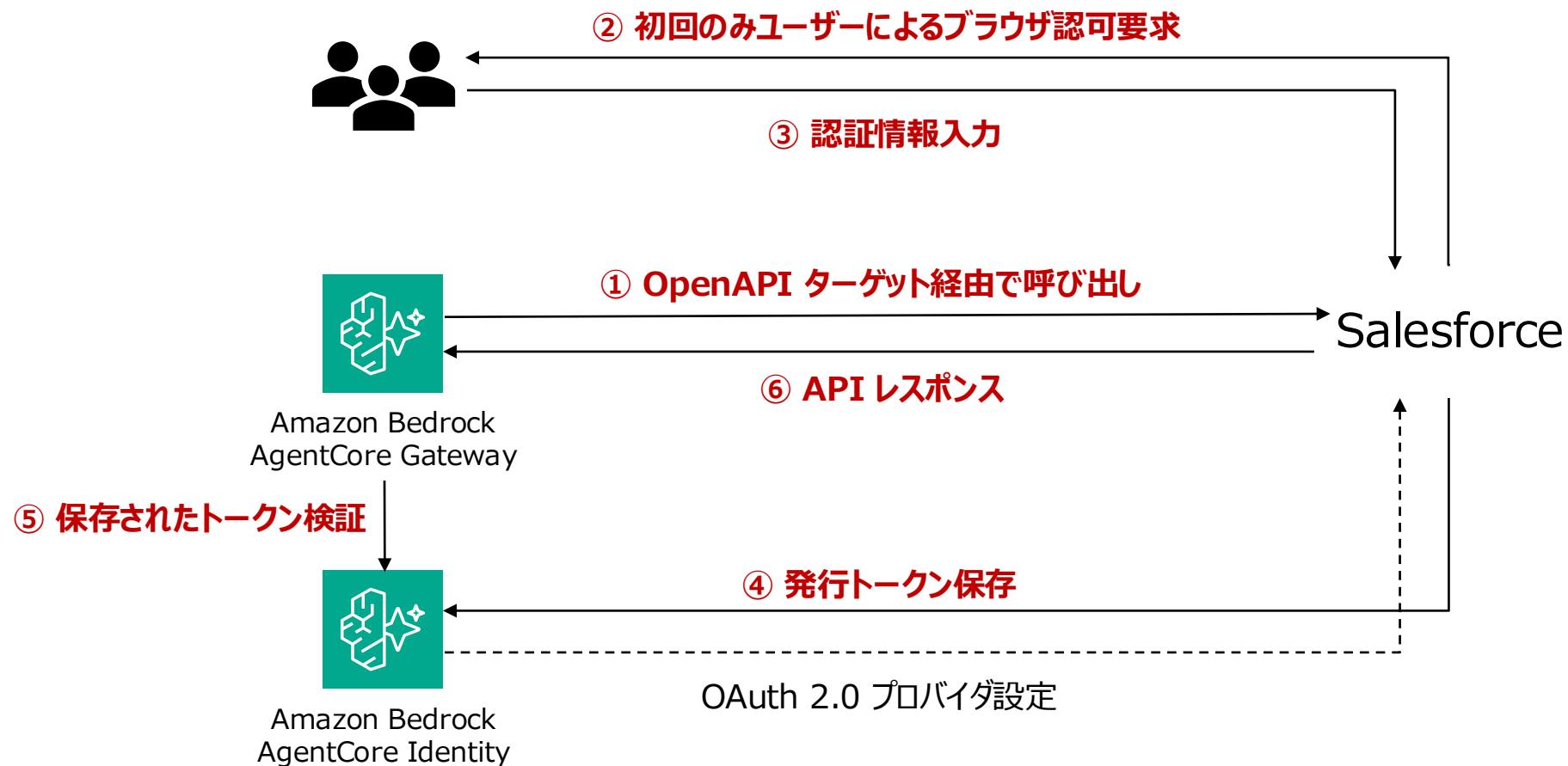
Okta認証

Oktaで発行されたJWTアクセストークンをAgentCore Runtime 側で検証する構成により、生成AIエージェントは認証済みユーザーコンテキストで実行され、後続の SaaS API 呼び出し時にもユーザー情報を引き継ぐことができます。



Salesforce連携

Salesforceとの連携には、OpenAPI定義を介したOAuth 2.0 Authorization Code Flowを利用しています。
AgentCore Gatewayが主体となって管理し、生成AIエージェントはトークン管理の詳細を意識しない設計となっています。



Tableau連携

TableauはPersonal Access Token（PAT）による認証方式を採用しています。Amazon Bedrock AgentCoreの標準機能ではPATによる認証認可ができないため、Gateway Interceptorsを活用したカスタム認証で連携しています。

