

Globant ▶

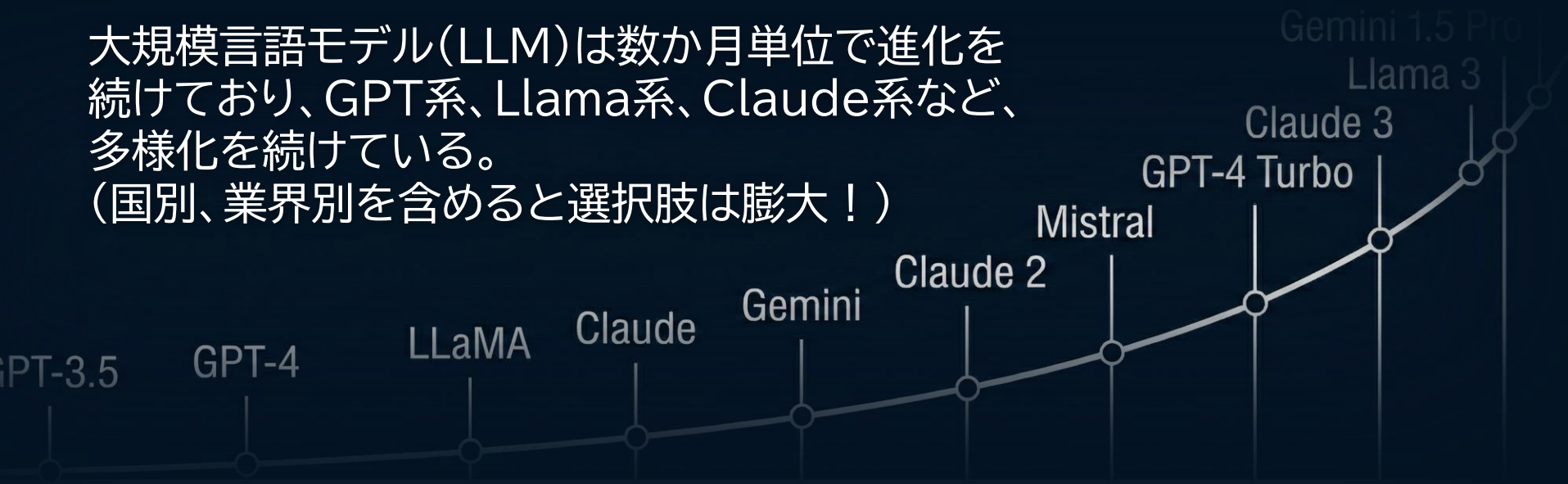
Enterprise AI

---

# エンタープライズシーンにおける 生成AI導入アーキテクチャの最前線

# 生成AIの進化は止まらない

大規模言語モデル(LLM)は数か月単位で進化を続けており、GPT系、Llama系、Claude系など、多様化を続けている。  
(国別、業界別を含めると選択肢は膨大！)





単一モデルへの依存は数か月で陳腐化してしまう


# 導入を阻む多くの壁

## 技術面の課題

 認証認可:  
Oauth2.0/IDPとの統合


 データ連携:  
DB、Blob、文章(Word、PDF)  
REST API等データソースへの接続


 セキュリティ:  
ZeroTrust、既存システムとの統合

 性能・スケール:  
LLMレート制限、同時実行数制限

## 運用面の課題

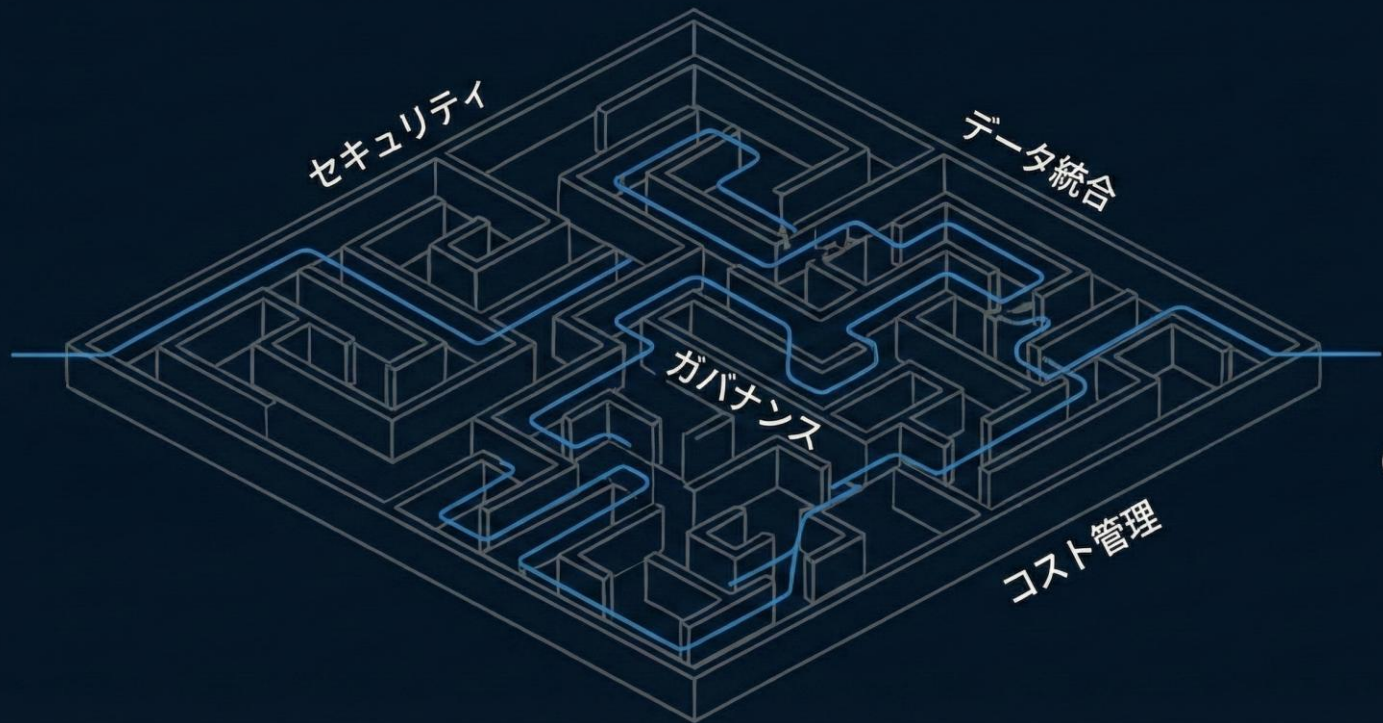
 ガバナンス:  
誰がどのLLMをどのように使えるか

 コスト管理:  
プロンプト単価x利用量を可視化し、  
予算を管理

 監査:  
全ての入出力をロギング、メタデータの  
記録管理する



Enterprise



セキュリティ

データ統合

ガバナンス

コスト管理



Generative AI

# LLMの進化に対応する最適解：マルチLLM抽象化アーキテクチャ

アプリケーションと多様なLLM群の間に「**抽象化レイヤー**」を設けることで、複雑さを吸収し、将来のモデル変更を柔軟に対応できる基盤を構築する！

モデルの選択：

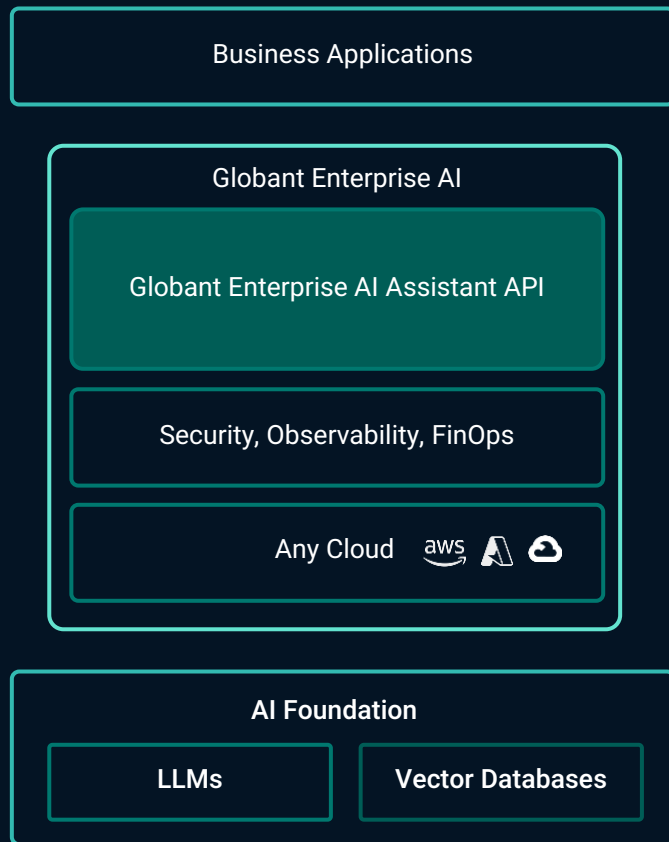
用途(コスト、性能、言語特性)に応じて最適なLLMを選択できる

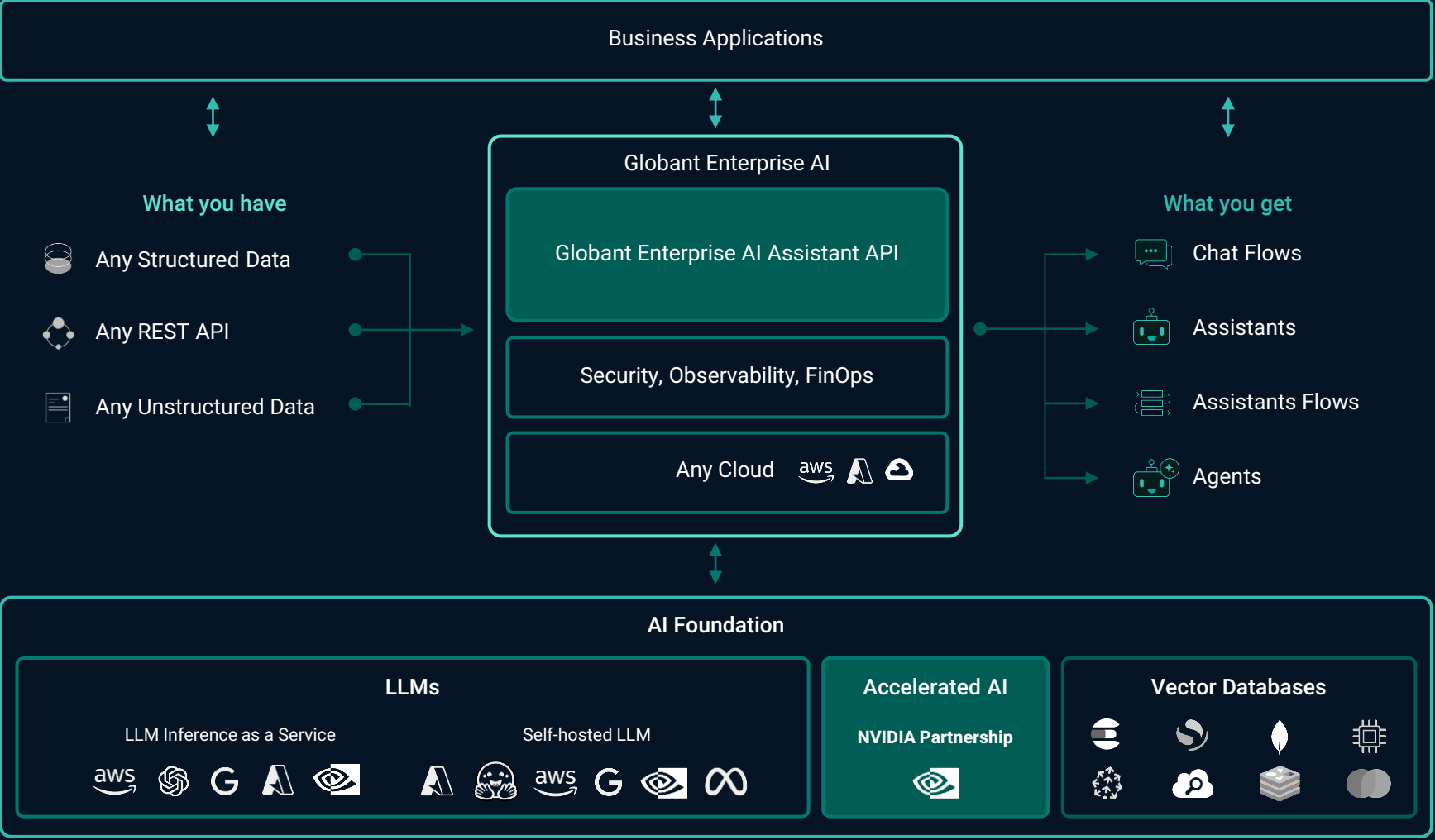
開発の加速：

統一されたAPI/SDKにより、アプリケーション開発者はモデル固有の仕様を意識する必要がない

ベンダーロックインの回避：

特定のLLMベンダーに依存することなく、常に最良の選択肢を確保





# AI基盤がもたらす柔軟性と統制



## LLM抽象化と柔軟素

ベンダーロックインの回避：  
最適なLLMをコストや性能に  
応じて自由に切り替える。

ロードバランシング：  
複数LLMやインスタンスにリク  
エストを分散しレート制限を緩和。

障害対策：  
特定のモデル障害発生時に、  
代替のモデルへと切り替える。



## 堅牢なセキュリティとガバナンス

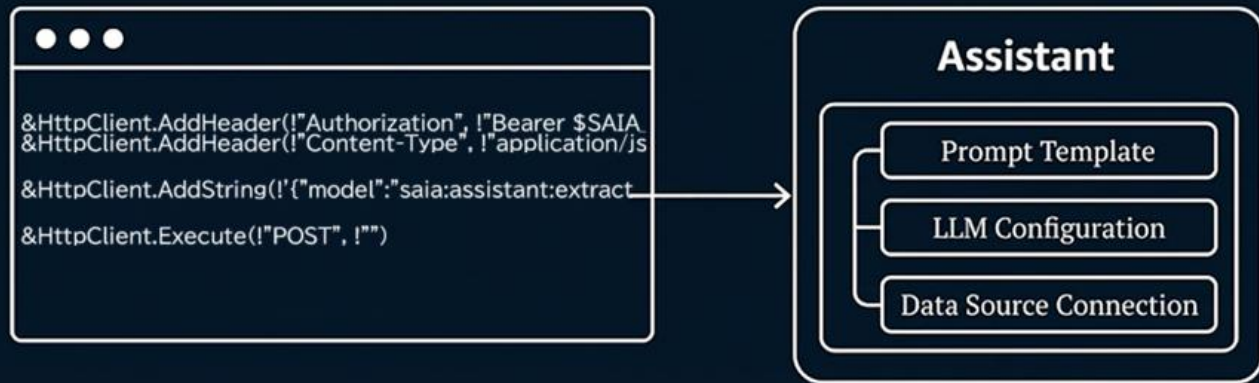
統合認証：  
OAuth2.0を利用したIDの統  
合運用。企業IDでのLLM利用  
を実現。

ガードレール機能：  
プロンプトインジェクション対  
策や不適切な入出力を監視、  
制御。

可観測性：  
モデルごとのコストと利用状況  
を詳細に追跡・監視。



# Assistant:特定のタスクを「AI関数」としてカプセル化



AI Assistantは、特定の目的(例:「契約書からリスク項目を抽出する」)を達成するためのプロンプト、LLMモデル設定、データソースを一つの単位としてパッケージ化し、APIとして公開する機能。

## LLM非依存:

アプリケーションはAssistantAPIを呼び出すだけで、動作するLLMを変更してもアプリケーション側の変更は不要。

## バージョンング:

プロンプトの変更履歴を管理し、AIソリューションとしての品質を常に最新に保つ。

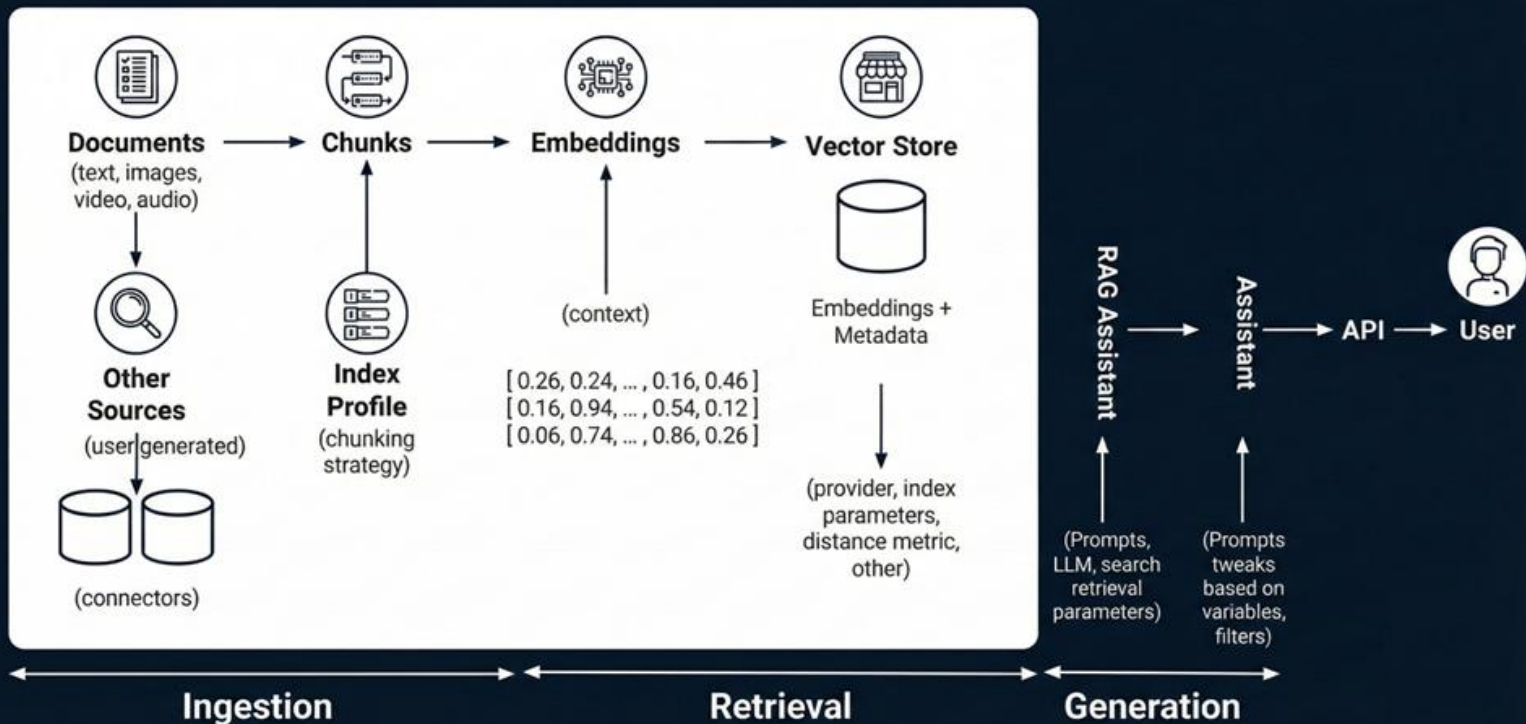
## 再利用性:

一度作成したAssistantは、様々なアプリケーションから「AI関数」として呼び出しが可能。



# RAG Assistant: 企業内ナレッジを安全にAIへ統合する

## GeneXus Enterprise AI - RAG Architecture



# The Lab (Agents): 自律的なタスク遂行フレームワークへ

Agentsは生成AIを「関数」や「定義済プロセス」から、自律的にタスクを計画・実行する「実行モデル」へと拡張する概念です。大規模で複雑な目的を達成するために、複数のAIEージェントが協調して動作します。

## 主要なコンポーネント

### Agent & TOOLS:

ビジネスリーダーから技術者まで、誰もが直感的にプロセスを設計可能。

### Agentic process:

LLMによる確率論的な判断と、API等による決定論的な処理を一つのワークフローに混在させることで、柔軟性と信頼性の両立を図る。

### Flows:

フローにより、各組織の特定のニーズに合わせた対話型ソリューションの作成が可能。各アシスタントやAIEエージェントの統合を容易にします。



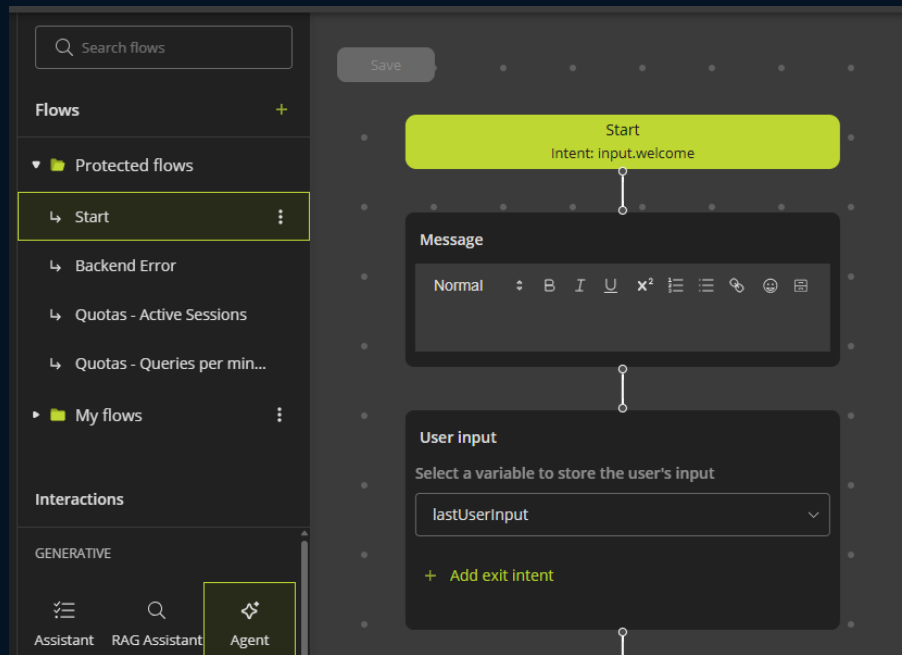
# Flows:複数のAI AssistantやAgentを組み合わせ自動化

Flowsは、複数のAI AssistantやAgentをドラッグ＆ドロップで組み合わせ、条件分岐/スクリプト実行/外部API連携などを交えて、複雑な業務フローを自動化する機能です。

## 主な利点

**ノーコードUI:**  
ビジネスリーダーから技術者まで、誰もが直感的にプロセスを設計可能。

**確率論と決定論の融合:**  
LLMによる確率論的な判断と、API等による決定論的な処理を一つのワークフローに混在させることで、柔軟性と信頼性の両立を図る。



# Flowsで実現する対話型UIとバックプロセスの革新

## ChatFlowsの導入例



顧客サポート(E-コマース)  
注文状況の確認、返品手続き  
を24時間自動で対応する。



予約アシスタント(観光)  
パッケージの選択から予約  
までを対話形式でサポート



アポイント調整(医療)  
患者の予約状況や医師の空き  
状況案内を自動化し、管理業  
務を削減。

## AgenticProcessの導入例



市場調査の自動化  
-「SNS情報収集Agent」  
-「感情分析Agent」

⇒「レポート生成Agent」に  
連携し、素早く情報を収集



保険契約管理の自動化  
-「契約書情報収集Agent」  
-「翻訳Agent」

⇒「システム入力Agent」に  
連携し、データ登録を省力化



サポート対応の高度化:  
-「問い合わせ内容分析Agent」  
-「社内ナレッジ検索Agent」

⇒「メール回答作成Agent」が  
最終回答を生成

## 再整理

- LLMは今後も多様化・進化を続けるため、マルチモデル前提のアーキテクチャが必須。
- エンタープライズ導入には、認証、セキュリティ、データ連携、ガバナンスを組み込んだAI基盤が不可欠。
- RAG、Assistant、Flow、AI Agentといった様々な要素を実際の業務フローへと統合できる。
- 目指すべきは「利用するLLMモデルは変わってもアーキテクチャは変わらない」設計思想である。

AI利用をPoC止まりにしないためには  
基盤選定、設計こそ重要

マルチLLM x  
セキュアなエンタープライズ基盤

Globant▶

Enterprise AI





# GeneXus Day 2026

Thank you