Universal AI Agent Platform　DOC-ID: UAA-JP-2026-V3

Universal AI Agent サービス概要・システム構成＆導入ガイド

システム改修不要・最短3日で社内データベースと安全に直結する次世代MCP準拠エンタープライズAIエージェント

APPI / Zero Data Retention

MCP Read-Only Protocol

01. エグゼクティブサマリー（導入目的と期待ROI）

Universal AI Agentは、企業が保有する既存データベース（SQL Server / PostgreSQL / MySQL / SQLite）へ読み取り専用（Read-Only）で直結し、「24時間リアルタイム接客・購買促進」と「経営・現場データの自然言語分析」を単一基盤で実現するB2B SaaSプラットフォームです。

定型問い合わせ自動解決率

80%

Webウィジェット＋Messenger統合対応



有人オペレーター回答作成時間

-70%

AIコパイロットによる返信下書き自動生成



初期接続検証（無料PoC）期間

最短3日

初期構築費用 0円・既存API改修不要



02. システム連携構成図＆コア安全設計

FLOW 01 接点・認証

顧客 / 社内メンバー

Webウィジェット（Cookie自動認証）やFB Messengerから自然言語で質問。

FLOW 02 第1防壁・AI推論

高速Regex＋自己検証

危険語句を遮断し、ビジネス辞書とLangGraph Reflectionで正確なSQLを生成。

FLOW 03 第2防壁・権限制御

SQL AST検証＆RLS分離

構文木解析でSELECT以外を100%遮断。ロールとUser Scopingで閲覧範囲を制限。

FLOW 04 TLS 1.3 直結

社内既存データベース

外部へデータを複製せず（Zero Retention）、Read-Onlyで安全に照会。

SECURITY 01 二層DBガードレール＆完全Read-Only接続

高速Regexフィルターと SQL AST（抽象構文木）解析の二層防御により、SELECT文以外の変更クエリ（INSERT / UPDATE / DELETE / DROP）をDB到達前に100%遮断します。

SECURITY 02 行レベル権限（RLS）・ロール連動・データ非保持

既存DBのrole_tableおよびUser Scopingを自動認識し、役職・顧客ごとの閲覧範囲と回答トーンを厳格に分離。Zero Data Retentionにより外部AI学習への利用は0%です。

ENGINE 03 LangGraph自己検証（Reflection）ループ＆リッチUI生成

AIが生成したSQLと取得結果を自己検証（Self-Correction）してハルシネーションを抑止。画像付商品カードやKPI集計表を自動生成して即座に表示します。

STUDIO 04 4つのAI自動検出エンジン＆ビジネス辞書定義

画像結合（Image JOIN）・ロール構造・User Scoping・テーブル権限の4項目をAIが自動検出。テーブル・カラムの業務定義（ビジネス辞書）とライブプレビューで非エンジニアでも設定可能です。

03. ノーコード管理画面・設定ガイド（3ステップ画面イメージ）

専門的なプログラミング知識は一切不要。管理画面のウィザードに沿って最短3ステップで設定・稼働できます。

SCREEN 01 DB接続ウィザード＆AI推奨テーブル選択 — Read-Only 接続OK (18ms)

- PostgreSQL / SQL Server / MySQL / SQLiteを選択して接続テスト
- AIが業務に重要なテーブル（products, orders等）を自動推奨
- 機密テーブル・カラム（パスワード・原価等）をチェック1つで除外

```
対象テーブル: ☑ products ☑ orders ☐ admin_secrets (除外)
```

SCREEN 02 4つのAI自動検出＆ビジネス辞書マッピング — AI Auto-Detect 完了

- ワンクリックで「画像JOIN」「ロール表」「User Scoping」「権限」を自動検出
- カラム名に社内用語（例: total_amt → 売上金額（税込））を定義
- 役職ごとの回答トーン（経営層向け・CS向け）をノーコード設定

```
辞書定義: orders.total_amt → 「売上金額（税込・送料別）」
```

SCREEN 03 ライブ検証＆1行スクリプトタグ埋込 — 本番稼働・Copilot有効

- 管理画面内のテストチャットでSQL推論プロセスと商品カードを事前検証
- Cookie / LocalStorage顧客トークン連携と事前ヒアリングを設定
- 発行された1行の<script>タグを既存Webサイトに貼るだけで即時稼働

```
<script src="https://.../widget.js" data-id="ag_jp01" async></script>
```

04. システム仕様・対応環境一覧

対応データベース	Microsoft SQL Server / PostgreSQL / MySQL / SQLite（完全Read-Only接続）
接続プロトコル・構成	Model Context Protocol (MCP) 準拠 / クラウド（AWS・Azure・GCP）およびオンプレミスVPN対応
対応チャネル・受信箱	Webチャットウィジェット（1行スクリプト埋込）＋ Facebook Messenger（統合受信トレイ対応）
顧客認証・事前ヒアリング	ブラウザCookie / LocalStorageトークン自動認証、チャット開始前フォーム（氏名・敬称設定）
セキュリティ・法令準拠	個人情報保護法（APPI）準拠 / ISO/IEC 27001 (ISMS) 基準準拠 / TLS 1.3・AES-256暗号化 / 完全監査ログ

05. 無料POC（概念実証）導入ロードマップ

STEP 01 Day 1

要件整理（30分）

対象DB種別と自動化したい接客・社内分析シナリオを整理（秘密保持契約NDA締結対応）。

STEP 02 Day 2

3ステップDB接続（半日）

Read-Onlyアカウントで安全接続。AI推奨テーブル選択とビジネス辞書をMCPインデックス同期。

STEP 03 Day 3〜

AI設定・プレビュー検証

ライブプレビュー画面でペルソナ・業務ルール・Image JOINカード・RLS権限を実データ検証。

STEP 04 最短30秒

1行タグ埋込・本番稼働

既存サイトへ1行の<script>タグを貼るだけで本番稼働。有人引き継ぎ・AIコパイロットも即時利用可能。

06. 開発・運営会社概要（ベンダー情報）

会社名	BK HIGHTECH Co., LTD
設立	2022年
共同創業者	Dr. Dang Hoai Phuong, Tan Nguyen, Dung Nguyen
R&D顧問・学術連携	Dr. Dang Thien Binh（ダナン工科大学 / DUT 応用研究連携）
所在地	ベトナム・ダナン市ハイチャウ区ハイホー K96/17 (K96/17 Hai Ho, Hai Chau, Da Nang, Viet Nam)
連絡先・Web	+84 816 946 355 / contact@bkhightech.vn / https://bkhightech.vn

© 2026 BK HIGHTECH Co., LTD. All rights reserved. — Universal AI Agent Platform (DOC-ID: UAA-JP-2026-V3)