CDATA

ホワイトペーパー

MCP プラットフォームの優位性

エンタープライズでの AI 活用を実現するためのアプローチ

2026 年 7 月（日本語版）

CDATA

MCP プラットフォームの優位性：エンタープライズでの AI 活用を実現するためのアプローチ

エンタープライズ AI のアーキテクトは、5 年前には存在しなかったものを設計しようとしています。数十におよぶリアルタイムの業務データソースを横断しながら、質問に答え、ワークフローを実行し、自律的に動作する。これらすべてを同時に、しかもガバナンスを効かせ、コストを抑えながら正確に行うシステムです。これはモデルの問題でもデータパイプラインの問題でもなく、インフラの問題です。そしてアーキテクトと IT 部門の責任者がいま下す判断が、エンタープライズ AI が拡張していくのか、それとも停滞するのかを決めます。

判断の核心は次の二択です。データソース公式の Model Context Protocol (MCP) サーバーでアクセス・コントロールプレーンを自前で構築するのか、それとも対象となるすべてのデータソースを横断する集中管理型の MCP プラットフォームを採用するのか。この判断を左右する要因は主に 3 つあります。必要とされるデータのコントロール・コンテキスト・コネクティビティの水準、決定論的・非決定論的・自律的なワークフローを同時に成立させる必要性、そしてトークン消費を抑え込む圧力の強さです。

データソース公式の MCP で自前構築する道は、一見魅力的に映ります。しかし相応のコストとトレードオフがすぐに顔を出し、最終的にはエンタープライズ AI のアーキテクトと IT 責任者を集中管理型 MCP サーバーへと向かわせます。本ホワイトペーパーでは、AI アーキテクトが満たすべきインフラ要件を整理し、目前にある「作るか、買うか」の判断を具体的に示し、根本的に異なる 2 つのアプローチの検討事項とトレードオフを論じます。

エンタープライズ AI アーキテクトのミッション

エンタープライズ AI のデータインフラ要件は複雑に絡み合っており、そのすべてが同時に成り立っていなければなりません。拡張性のあるエンタープライズ基盤をつくるうえで、AI アーキテクトが両立させ、設計に織り込む必要のある中核的な目標は 6 つあります。

幅広く豊富な業務データソースへの、統制されたアクセスを LLM に与える。事業における AI の価値は、実際の業務データにどれだけアクセスできるかに比例します。Salesforce のレコード、NetSuite の財務情報、Jira のチケット、BambooHR のプロフィール、Zendesk のケースといったデータです。さらにこれらのデータは、クラウドアプリケーション、独自のデータソース、オンプレミスのネットワークドライブに散在していることが多く、いずれも LLM がアクセスできれば計り知れない価値を持ちます。すでに広く指摘されているとおり、このデータにアクセスできないモデルは当たり障りのない答えしか返しません。アクセスできるモデルは、具体性と一貫性、そして信頼を生み出します。

完全なコントロール、監査可能性、そして実効性のあるガバナンスを提供する。システムを横断して質問を投げ、アクションを起こせるのは、やり取りされるデータにガバナンスが効いている場合だけです。つまり、アクセス制御、ポリシーの適用、監査ログ、そして「どのデータに、誰が、どれだけのコストで触れたか」を把握できることが必要になります。Gartner の 2025 AI Ethics, Governance and Compliance の調査によれば、自社の AI ガバナンスに現時点で自信を持てている IT 責任者は 25% 未満にとどまります。このギャップは現場では次のように現れます。69% の企業で、従業員が禁止された生成 AI ツールを使い、データをスプレッドシートにコピーし、あるいは許可されていない経路で AI システムにアップロードしているのです。

非決定論的・決定論的・自律的なワークフローをまとめて支える。エンタープライズ AI は一枚岩ではありません。探索的な用途では、予測できない問い合わせに精度を落とさず対応できる柔軟なアーキテクチャが求められます。対極にあるのが決定論的なワークフローで、性質上より予測可能で反復可能ですが、データソース内部へのアクセスとガバナンスをより高い水準で必要とします。さらに自律型エージェントの展開も進んでおり、自由度の高い探索とビジネスロジックの理解の両方を相当量必要とし、ガバナンス・コントロール・監査可能性をいっそう高い水準で求めます。企業は当たり前のようにこの 3 つの自律モードすべてを求めており、それぞれを並行して支えるアーキテクチャを展開しなければなりません。

事業部門の「市民開発者」を前提に設計する。いま AI 活用の支援を求めている事業部門（BU）は、要望と「じゃあこのアイデアはどうか」という相談で IT 部門のキャパシティを圧迫しています。すべての要望を引き受けて抱え込むのではなく、AI アーキテクトと IT 責任者は、事業部門が安心してツールを使える仕組みを設計するほうが得策です。新しいユースケースごとに中央の IT 部門が関与しなければならない仕組みでは、対応待ちの案件が際限なく積み上がっていきます。理想的な基盤は、コントロールとガバナンスを中央に残したまま、作る作業そのものは事業部門に任せられるものです。

LLM のコスト管理とトークンの ROI を維持する。トークン消費には、実際のコストがあり、しかも急速に膨らみます。未加工のデータセットをそのままモデルに送って要約させるのは、SQL クエリならごく一部の費用で先に用意できた答えを、高い金額で買う行為です。アーキテクトに必要なのは、分析処理をデータソース側に押し込み、モデルが実際に必要とするコンテキストだけを返せる仕組みです。

何よりも精度を担保する。素早く返ってくる誤答は、答えがないよりも悪い。ガバナンスの効いた業務環境では、不正確な AI の回答は時間を無駄にするだけでなく、誤った情報にもとづく意思決定を下流に生み出します。精度は「あると良いもの」ではなく、他のすべての目標が乗っている前提条件です。そして多段のワークフローやエージェントシステムが動き始めると、この誤差は積み上がっていきます。

> 精度の誤差は工程ごとに積み重なる
>
> 業界平均である 75% の精度で 5 工程のワークフローを回すと、正しく完了するプロセスはわずか 24% になります。

ミッションを果たす 2 つのアプローチ：作るか、買うか

エンタープライズ AI のデータ基盤をまだ検討中の AI アーキテクトは、たいてい次の 2 つの選択肢を比べています。

道筋 1：集中管理型の MCP プラットフォームを採用する

マネージド MCP プラットフォームとは、あらかじめ用意されたコネクタとコントロール群であり、MCP サーバーを通じて業務データソースを任意の AI クライアントやモデルに公開します。独自コネクタの開発やデータパイプラインの構築、継続的な保守は必要ありません。数百のデータソースを対象に、スキーマ解決、セマンティックコンテキスト、アクセス制御、クエリ最適化、監査ログを単一の設定レイヤーからまとめて扱えます。AI ツール、エージェント、自動化処理は、個々のデータソースではなく、ガバナンスが効いたセマンティック情報の豊富なデータレイヤーに接続します。

道筋 2：単一データソースの MCP で自前構築する

既存の SaaS ベンダーが MCP 標準を本格的に受け入れるまでには時間がかかりましたが、Salesforce や Atlassian といった主要プロバイダーは自社データソース向けの MCP サーバーを提供し始めています。こうしたデータソース公式の MCP は、自社データと AI クライアントを 1 対 1 でつなぐもので、データソースごとの連携がそれぞれ独立した実装・保守案件になります。あるいは、MCP サーバーを完全に自社開発する企業もあります。この場合、ガバナンス、アクセス制御、セマンティックな意味理解はデータレイヤーではなくアプリケーションレイヤーで管理することになり、追加の負担が生じ、ツールも別途必要になることが多いです。たとえばデータソース公式の MCP アーキテクチャでマルチソースの AI アプリケーションを実装するには、MCP ゲートウェイやセマンティック検索レイヤーといった追加のツールを設計し、実装し、管理しなければなりません。

どちらのアプローチも、条件を限れば機能します。しかし企業規模で見ると、判断はいくつかの要因とトレードオフに帰着します。以下の検討事項で順に見ていきます。

CDATA

すべてのエンタープライズ AI アーキテクトへの検討事項：コンテキスト、コントロール、コネクティビティ

マネージド MCP プラットフォームと、単一データソースの MCP を自前で組む方式との違いは、構築の初期段階では見えにくいものです。単一データソースの MCP はそれ自体に利用料がかからないことも多いのですが、コストはすぐに別の場所で発生し、トレードオフが明らかになります。ここからは、このトレードオフを 3 つの視点から見ていきます。コンテキスト（必要なデータをできるだけ完全かつ効率的に取り込む）、コントロール（データアクセスと、人間またはエージェントによる操作にガバナンスを効かせる）、コネクティビティ（対象データソースに安全かつ一貫して、リアルタイムでアクセスする）です。

コンテキスト

マルチソースのセマンティックフェデレーション vs. 単一データソースのデータパイプライン。公式 MCP のアプローチは、一度に 1 つのデータソースを、そのデータソース固有のセマンティクスのまま公開します。フェデレーション型のプラットフォームは、すべてのデータソースをまとめて、一貫したセマンティックモデルに正規化した形で公開します。営業アナリストが Salesforce と NetSuite と BambooHR に同時にまたがる質問を投げたとき、フェデレーション型なら、システム間の用語の細かな——しかし放置すれば答えを狂わせる——違いを踏まえた、筋の通った回答が返ります。公式 MCP 方式では、あらかじめ作り込んだパイプラインか、不整合なスキーマをモデル自身が突き合わせられることが前提になります。後者は当てにできる前提ではなく、しかも後述するようにコストのかかる代替手段です。

ツール呼び出し：データソースから継承したツール vs. 汎用ツールレイヤー。公式 MCP がモデルに渡せるのは、データソース側のベンダーが公開すると決めたツールだけです。Connect AI のようなマネージドプラットフォームは、データソース固有のツールに加えて、データソースを横断する汎用ツール、さらに自社固有のワークフロー向けにカスタムツールを追加する手段も提供します。違いは、AI でできることの範囲をベンダーだけが決めるのか、自社の意向も反映できるのか、という点です。

スキーマ、メタデータ、権限、リネージ——生データだけでは足りない。AI モデルは、扱っているデータの中身だけでなく構造まで理解しているときに、より優れた判断を、より効率的に下します。マネージド MCP プラットフォームは、接続されたすべてのデータソースについて、行と列そのものに加えて、データスキーマ、フィールド単位のメタデータ、関連性のコンテキスト、権限構造を届けます。

非決定論的・決定論的・自律的なワークフローをまとめて支える。先に述べたとおり、理想的な AI アーキテクチャはこの 3 つのワークフローモードをすべて支えます。データソース公式の MCP サーバーは、そのデータソースのシステム内に収まる決定論的なユースケースで最も力を発揮しますが、他の 2 つのモードを実質的に支えるだけの外部コネクティビティとガバナンス機能を欠いています。システム間の接続を橋渡しし、データをセマンティックにフェデレーションして正規化し、アクセスとアクションの権限を中央で制御することで、マネージド MCP サーバーは 3 つのモードを同時に適切に支えるアクセス・コントロールプレーンを提供します。

コントロール

プラットフォーム側のロールベースアクセス制御＋データソースから継承した権限。公式 MCP は、認証されたユーザーまたはサービスアカウントの権限を継承する場合があります。出発点としては悪くありませんが、ガバナンスモデルとしては不完全です。マネージドプラットフォームなら、データソースのシステムに手を入れずに、その上へ追加のコントロールを重ねられます。具体的には、ロールベースアクセス制御（RBAC）、属性ベースアクセス制御（ABAC）、行レベルのポリシー、個人情報（PII）に対する列マスキングです。

データレイヤーでのポリシー適用。規制業種や機密性の高い業界の多くでは、PII マスキング、データレジデンシー要件、フィールド単位の伏せ字処理を、データがモデルに届く前に済ませておく必要があります。これらのポリシーをプロンプトやアプリケーションレイヤーで効かせようとすると、壊れやすく、一貫せず、エンドユーザー規約に違反するおそれもあります。データアクセスレイヤーで効かせるほうが、確実で監査もしやすい道筋です。

読み取り専用 vs. エージェント制御付きの読み書き。データソースのシステムに書き込むエージェント型のワークフローには、読み取り専用のクエリとは異なるガバナンスが必要です。マネージドプラットフォームなら、書き込み権限をエージェント単位、データソース単位、ワークフロー単位でスコープを切れますし、定めた閾値を超える書き込み操作には人間の承認を必須にできます。自前構築の場合、そのロジックは各エージェントのコードの中に置いて管理し、人手で監視することになります。

スタック全体にわたる監査ログ。公式 MCP の監査ログは、たいていツール呼び出しだけを記録します。マネージド MCP サーバーは、データクエリ、ユーザー別・ユースケース別のトークン消費、ユーザーとエージェントの ID、ポリシーの判定結果を、すべて 1 カ所に取得して記録します。

エージェントアクセスのためのサービスアカウント。人間のユーザーは ID プロバイダーを通して認証します。エージェントはサービスアカウントを通して認証します。この両方を対等なアクセス方式として扱い、それぞれに独立したガバナンス機能を持つプラットフォームは、AI エージェントに向けて作られています。人間のアクセスしか扱えないもの――公式 MCP ではこちらが一般的です――は、AI エージェント向けには作られていません。

コネクティビティ

単一データソース vs. マルチソースのコネクティビティ。単一のデータソースに収まるユースケースもあります（「Salesforce で製品 X のエンタープライズ向け商談のうち、進行中のものをすべて探す」など）。しかし実際には、クエリもエージェント型のワークフローも、複数のデータソース、そして複数のクラウド環境やオンプレミス環境を短時間に次々とまたぐコネクティビティを求めるようになっています。単一データソースの MCP は定義上 1 対 1 の関係であり、たいていは自社のクラウドアプリケーションの中に閉じています。マネージド MCP プラットフォームは、稼働環境を問わずデータソースを横断するコネクティビティを提供します。

データソース側でのトークンコスト最適化。マネージド MCP の分析処理は、Connect AI 独自のセマンティック SQL レイヤーを通じてデータソース側で走り、要約済みの結果を返します。このときモデルが受け取るのは生データの塊ではなく、狙いを絞った答えです。1 万行のデータセットをモデルに送って要約させるのは、SQL がすでに計算し終えた 3 文の要約を送るよりも、トークン費用がはるかに高くつきます。エンタープライズ規模では、これはトークン消費とレイテンシーの両面で無視できないトレードオフです。

メタデータと関連性のコンテキスト。「進行中の商談のうち、直近 30 日間に活動のないものはどれか」に答えるには、テーブルから行を取ってくるだけでは足りません。Salesforce における商談レコード、活動レコード、タイムスタンプの関連性を理解する必要があります。データソースを理解したコネクタはその関連性を把握し、セマンティックレイヤーがそれをデータソース横断でフェデレーションします。

時間経過にともなう MCP の保守。公式 MCP サーバーは、データソース側のベンダーが保守します。Salesforce が MCP エンドポイントを変更し、NetSuite が API を更新し、Zendesk がツールを廃止すれば、接続はそれぞれ独立に壊れます。自前構築のアーキテクチャでは、社内の誰か——多くの場合はチーム 1 つ丸ごと——が、すべてのデータソースについて、各ベンダーの都合に合わせたタイミングでその保守を背負います。マネージドプラットフォームはその保守を引き取ります。接続と認証トークンが常に最新の状態に保たれているのは、プラットフォームがそれを継続的に更新しているからです。

LLM とベンダーの中立性。特定の SaaS ベンダーや LLM プロバイダーに密結合したアーキテクチャはロックインを生み、モデルの勢力図が変わったときに高くつきます。そして勢力図はこの 2 年で何度も変わり、落ち着く気配もありません。モデルに依存しない MCP プラットフォームなら、ユースケースに合ったモデルへクエリを振り分けたり、プロバイダーを乗り換えたりする際に、データレイヤーを作り直す必要がありません。

Connect AI はエンタープライズのコンテキスト・コントロール・コネクティビティにどう応えるか

CData の Connect AI は、エンタープライズ AI のデータ基盤がコネクティビティ・コンテキスト・コントロールを同時に満たさなければならない、という認識のうえに作られています。3 つのうちどれか 1 つでも弱いと、精度が落ちます。しかも自律的に推論するモードでは、不正確さは誰かが介入する前に結果を生んでしまいます。

CData の AI データコネクティビティの現状レポートでは、企業の技術責任者が AI のデータ連携における優先事項を次のように挙げました。42% がリアルタイムのコネクティビティ、34% がセマンティックデータレイヤー、60% がガバナンスとリネージです。この 3 つはコネクティビティ・コンテキスト・コントロールにそのまま対応しており、実務者が本番環境で感じているギャップは、マネージド MCP サーバーのアプローチなら埋められる一方、公式 MCP アーキテクチャでは埋まらないことが多い、という裏付けになっています。

コンテキストと精度について。Connect AI は、モデルが動く前にスキーマ・構造・関連性を解決するセマンティックレイヤーを公開します。あるフィールドが何を意味するのか、2 つのオブジェクトがどう関係するのかを、モデルが推測する必要はありません。あらかじめ伝えられているからです。その直接の効果は、測定可能なかたちで高まる回答精度、短くなるレイテンシー、そして大幅に向上するトークン効率です。これが規模の面で精度にどうつながるのかの詳細な分析は、CData の AI 精度ホワイトペーパーにまとめています。

コントロールとセキュリティについて。Connect AI は、アクセスポリシー、RBAC、PII マスキング、監査ログをプラットフォームレイヤーで適用し、同時に各データソースアプリケーションからユーザーとサービスアカウントの権限をパススルーで継承して反映します。どのモデル、どのエージェント、どのインターフェースからのリクエストであっても、ガバナンスは効き続けます。このコントロールレイヤーのアーキテクチャは、CData のセキュリティベストプラクティスガイドで解説しています。

コネクティビティと保守について。Connect AI は、SaaS アプリケーション、データベース、オンプレミスシステム、クラウドプラットフォームにまたがる 300 以上の業務データソースへの接続を提供し、保守しています。カスタムフィールド、カスタムオブジェクト、複雑なリレーショナル構造にも対応します。コネクタの全ラインアップは jp.cdata.com/drivers でご覧いただけます。

この基盤が実際に動く様子は、複数のエンタープライズシステムを横断して動作する order-to-cash エージェントのライブデモを含め、Microsoft との共催ウェビナー「AI agents and the future of digital work」でご覧いただけます。

基盤は一度で作る

単一データソースの MCP サーバーは、エンタープライズ対応の AI アーキテクチャを構築する道として、表面上は魅力的に見えます。一部のプロトタイピングには適した選択でしょう。しかし、規模を拡げても意味のあるエンタープライズ AI の価値を出すために必要なコネクティビティの広さ、コンテキストの深さ、ガバナンスとコントロールの水準を前にすると、データソース公式の MCP アーキテクチャはたいてい本番環境に到達しません。

集中管理型の MCP プラットフォームに投資することで、AI アーキテクトとエンタープライズ IT の責任者は、現在を動かしながら将来に備えられます。このアプローチを採れば、ガバナンスが効き、フェデレーションされ、セマンティクスを備えたデータレイヤーを 1 つ、事業側に届けられます。AI はその上で、あらゆるワークフローについて、あらゆる自律レベルで直接動作でき、新しいユースケースが出てくるたびに基盤を作り直す必要もありません。

それが、AI のアクセス・コントロールプレーンの実体です。それをどう作るかという判断は、後から覆すのが極めて難しく、しかも高くつく、数少ないアーキテクチャ上の選択のひとつです。

今すぐ CData Connect AI を試す

Connect AI が AI と業務プロセスをどう合理化し、リアルタイムのインサイトとアクションにつなげるのかを、ぜひご確認ください。無料トライアルは jp.cdata.com から。

jp.cdata.com

AI のためのデータレイヤー。エージェント、アプリケーション、チームに、業務データへの信頼できるリアルタイムアクセスを。

CData は AI のためのデータレイヤーとして、AI をより正確に、効率的に、柔軟にします。ひとつのプラットフォームで数百の業務システムのリアルタイムデータに接続し、AI が正確に応答するためのセマンティックコンテキストを付与し、AI とデータのやり取りをすべて統制します。エージェント開発でも、アプリケーションへのデータアクセス組み込みでも、業務システムへのセルフサービスアクセス提供でも、CData は業務データを AI で使える状態に整えます。CData は Salesforce、Databricks、Microsoft、Google、Palantir をはじめ、世界中 10,000 社を超えるお客様の AI ワークロードを支えています。