# 企业级 Data Agent

# 技术架构与落地实践

从自然语言问数到可信多步骤分析

V1.0

2026 年 11 月

**技术架构白皮书**

# 目录

研究说明

执行摘要

1 Data Agent 的定义与边界

1.1 Data Agent 是什么

1.2 与传统 BI 的关系

1.3 与智能问数和 NL2SQL 的关系

1.4 与通用 Agent 的关系

1.5 四类系统的比较

2 企业级 Data Agent 六层参考架构

2.1 架构总览

2.2 交互意图层

2.3 任务规划层

2.4 业务语义层

2.5 工具与分析执行层

2.6 数据访问层

2.7 安全治理层

2.8 六层之间应传递什么

3 关键技术能力

3.1 多轮澄清

3.2 指标识别与语义映射

3.3 多步骤分析

3.4 图表与报告生成

3.5 分析回溯

4 可信分析与治理

4.1 准确性是分层指标

4.2 幻觉控制

4.3 权限与数据隔离

4.4 审计与证据链

4.5 人工复核与责任

4.6 安全测试

5 技术实现路线比较

5.1 路线一 直接 NL2SQL

5.2 路线二 通用 Agent 连接数据库和工具

5.3 路线三 调用 BI 能力的专业 Data Agent

5.4 路线四 混合架构

5.5 路线选择矩阵

6 从 POC 到生产的实施路线

6.1 第一步 选择可验证的业务任务

6.2 第二步 盘点数据与语义

6.3 第三步 设计工具和控制边界

6.4 第四步 建立 POC 题库

6.5 第五步 运行盲测与错误分析

6.6 第六步 小范围上线

6.7 第七步 持续运营

6.8 两条建设路线

6.9 Dora 与既有 FineBI 的实施前提

7 贯穿场景 从利润下降问题到可复核结论

7.1 场景说明

7.2 第一步 澄清问题

7.3 第二步 建立分析计划

7.4 第三步 执行与校验

7.5 第四步 组织答案

7.6 完整流程

8 典型场景与适用边界

8.1 经营分析

8.2 销售分析

8.3 财务分析

8.4 库存与供应链

8.5 Dora 作为具名实现例证

9 评测与验收方法

9.1 指标体系

9.2 POC 通过原则

9.3 上线后监控

10 挑战与发展趋势

10.1 可靠的长链路仍是核心挑战

10.2 语义资产将成为 Agent 的公共基础

10.3 工具协议会降低连接成本但不会消除治理

10.4 多智能体适合职责分工但会增加观测难度

10.5 从回答问题走向受控执行

11 实施建议

12 结论

术语表

参考资料

附录 A POC 检查清单

附录 B 正式发布前待补材料

本目录为静态目录，章节页码可在 Word 中更新字段后查看。

# 研究说明

## 研究问题

本白皮书回答四个问题：企业级 Data Agent 与通用 AI Agent、NL2SQL 和传统 BI 分别有什么边界；可信的数据分析智能体需要哪些架构层；企业应如何选择技术路线并完成 POC；既有 BI 体系怎样在控制风险的前提下引入 Agent 能力。

## 研究范围与方法

研究范围覆盖面向企业结构化数据分析的智能体，不讨论面向消费者的通用聊天助手，也不把所有具备自然语言界面的 BI 功能都归入 Data Agent。研究采用三类材料：一是公开论文和技术文档，用于解释 Agent、Text-to-SQL、工具调用与评测；二是 NIST、OWASP 和中国监管部门发布的风险治理材料；三是帆软 Dora、FineBI 的公开产品文档，用于核实产品能力及版本边界。资料检索截至 2026 年 11 月 2 日。

本文没有开展独立市场调查，也没有执行跨厂商同条件性能测试。因此，技术路线比较属于研究分析，不构成厂商排名；贯穿案例是说明性假设场景，不代表真实客户项目。正式对外发布前，应由产品、法务和案例负责人复核版本、部署条件和可披露范围。

## 证据标识

- **已验证事实**：可由公开的一手资料直接支持。
- **研究分析**：基于公开资料和架构原理作出的归纳，不能替代项目验证。
- **说明性假设场景**：用于说明流程和验收方法，数据与组织名称均为虚构。
- **待核实事项**：公开资料不足，需产品文档、POC 记录或客户授权材料补充。

## 执行摘要

1. Data Agent 的判断标准不是能否把自然语言转换为 SQL，而是能否围绕一个业务目标进行澄清、规划、受控调用分析能力、校验结果并保留可追溯记录。NL2SQL 可以成为其中一个工具，但不能单独承担指标口径、权限、长链路分析和结果解释。
2. 企业级架构应至少覆盖交互意图、任务规划、业务语义、工具与分析执行、数据访问、安全治理六层。六层之间需要传递用户身份、语义约束、执行参数、证据和审计信息，而不是只传递自然语言和最终答案。
3. 可信分析来自系统性约束。有效措施包括歧义澄清、受控指标和维度、最小权限、参数化工具、查询前检查、结果后验证、证据引用、人工复核和全链路日志。任何单一模型都不能替代这些控制。
4. 企业通常有四条实现路线：直接 NL2SQL、通用 Agent 连接数据库、调用 BI 能力的专业 Data Agent，以及混合架构。路线选择取决于数据复杂度、存量分析资产、实时性、监管强度和可接受的实施成本，不存在对所有企业都最优的方案。
5. 存量 BI 升级的价值在于复用已经治理的指标、数据模型、权限和看板，但复用并不等于自动获得可信结果。企业仍需确认 Agent 能看到什么数据、能调用什么工具、如何解释口径，以及错误怎样被发现和处理。
6. 帆软公开文档将 Dora 定位为企业级 Data Agent 平台，支持自然语言分析、任务规划与技能调用，并可接入 FineBI 的模型指标集、数据集、分析主题和仪表板。公开文档同时显示明确边界：当前数据模块主要连接 FineBI 资产与 Excel 类文件，部分高级能力受版本和部署条件约束。[1][2][3]
7. POC 不应只统计“回答是否像对的”。测试要覆盖答案正确性、指标口径、澄清行为、权限隔离、证据可追溯、失败恢复、延迟与成本，并保留每道题的输入、计划、工具调用、数据快照和人工判定。
8. 首个生产场景宜选择高频、可验证、可回退的分析任务。财务结账、供应链调度等高影响场景可以进入试点，但在稳定性、权限和复核机制成熟前，不宜让 Agent 自动执行不可逆业务动作。

# 1 Data Agent 的定义与边界

## 1.1 Data Agent 是什么

**直接回答：** Data Agent 是面向数据任务的智能体系统。它接收业务人员用自然语言表达的目标，在必要时澄清需求，基于企业语义和用户权限规划分析步骤，调用数据查询、指标计算、统计分析、可视化或报告工具，并把结果、依据和限制返回给用户。

这个定义包含四个必要条件。第一，系统处理的是业务目标，而不只是单次查询。第二，系统能够选择和组合工具，执行路径不必完全固定。第三，系统在企业约束中运行，包括身份、权限、指标、数据时效和审计。第四，输出可以被验证，至少能够回到数据来源、查询条件或执行记录。

ReAct 研究将推理与行动交替组织，使模型可以根据环境反馈更新计划；Anthropic 的工程总结则区分了预定义代码路径的工作流与由模型动态决定过程和工具使用的 Agent。[4][5] 企业 Data Agent 可以同时使用两种模式：对规则稳定、风险较高的任务采用固定工作流，对问题拆解和探索路径保留受控的动态规划。把所有环节都交给模型会扩大不确定性，把所有环节都写死又会失去 Agent 对复杂问题的适应性。

## 1.2 与传统 BI 的关系

传统 BI 的优势是稳定、可重复和易于治理。数据团队预先建模，业务人员通过报表、看板、筛选器和自助分析界面获取结果。它适合高频管理指标、固定经营节奏和需要统一呈现的场景。其限制主要体现在分析入口和交付速度：用户需要理解数据模型或等待分析人员制作内容，临时追问往往跨越多个报表与系统。

Data Agent 不应取代经过验证的 BI 资产。更稳妥的做法是把指标、分析主题、看板、权限和可视化组件当作受控工具，让 Agent 负责意图识别、任务分解、工具选择、追问和结果组织。这样，BI 提供确定性较高的分析能力，Agent 提供面向目标的交互和编排。

## 1.3 与智能问数和 NL2SQL 的关系

智能问数通常把自然语言问题转换为结构化查询，再返回数字或图表。NL2SQL 是其中常见的技术路径。它降低了写 SQL 的门槛，但企业问题中的关键难点往往不在语法，而在业务语义。例如“本月利润下降原因”至少需要确认利润口径、组织范围、时间比较基线、内部交易处理、数据是否已结账，以及允许展开到哪些明细。

Text-to-SQL 研究已经把歧义、欠说明、模式映射、评测和错误分析列为完整生命周期问题。[6] 在企业环境中，还要增加权限、指标版本、数据时效和多步骤诊断。由此可见，NL2SQL 可以解决“怎样查询”，却不能独立解决“应该查询什么、结果是否可用、谁能看见什么”。

## 1.4 与通用 Agent 的关系

通用 Agent 通常面向广泛任务，可调用搜索、代码、文件和业务 API。它的长处是适应性强，适合研究、内容处理和跨工具协作。但企业数据分析需要稳定的业务语义、行列级权限、可复核计算和一致的展示方式。若通用 Agent 直接获得数据库高权限，提示注入、错误工具选择和越权访问的后果会放大。

专业 Data Agent 的核心不是使用了不同的大模型，而是对数据、语义、工具、权限和验证进行专门设计。它可以使用通用模型，也可以接入 MCP 等工具协议，但工具协议只解决标准化连接，不能自动解决数据权限和业务口径。[7]

### 1.5 四类系统的比较

| 维度 | 传统 BI | NL2SQL 问数 | 通用 Agent | 专业 Data Agent |
| --- | --- | --- | --- | --- |
| 主要输入 | 看板操作与字段选择 | 单个自然语言问题 | 开放任务描述 | 业务分析目标与连续追问 |
| 执行方式 | 预建模型和固定交互 | 生成并执行 SQL | 动态选择通用工具 | 结合语义、计划和受控分析工具 |
| 业务语义 | 由模型和指标体系承载 | 常依赖模式描述或提示词 | 通常需要额外接入 | 作为核心层持续治理 |
| 多步骤分析 | 依靠人工切换和判断 | 较弱 | 较强但不一定懂业务口径 | 围绕数据任务受控执行 |
| 权限治理 | 通常成熟 | 取决于查询代理层 | 容易因工具权限过大而失控 | 应贯穿身份、数据、工具与结果 |
| 结果追溯 | 可回到报表和数据模型 | 可回到 SQL 与结果集 | 取决于日志设计 | 应保留语义、计划、工具、查询和证据 |
| 适用场景 | 稳定报表和看板 | 边界清楚的即席查询 | 跨系统通用任务 | 企业级问数、诊断、报告和预警 |
| 主要成本 | 建模与内容建设 | 模式适配和准确性优化 | 工具建设与安全控制 | 语义治理、工具编排、评测和运营 |

# 2 企业级 Data Agent 六层参考架构

### 2.1 架构总览

企业级 Data Agent 需要把概率性的语言理解与确定性的业务控制分开。以下六层并非产品菜单，而是一套职责划分。企业可以将其部署在一个平台中，也可以由多个系统组合实现。

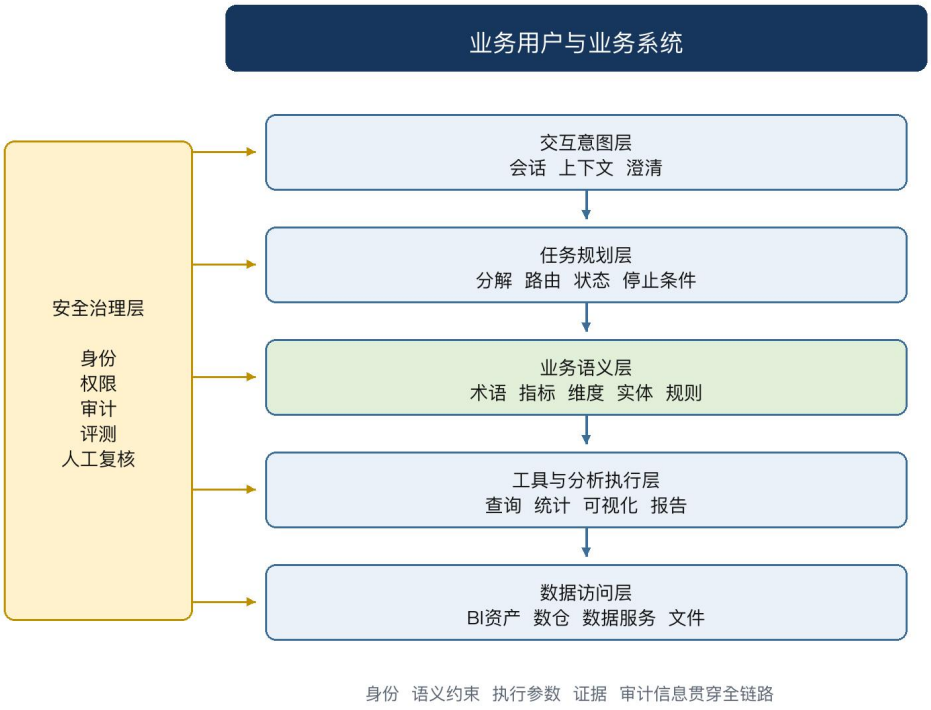



**图 1 企业级 Data Agent 六层参考架构。** 本图为研究架构，描述职责与控制关系，不对应单一厂商产品的完整功能清单。

## 2.2 交互意图层

交互意图层负责接收问题、维护会话上下文和识别歧义。它需要从问题中抽取指标、维度、时间、组织、比较基线和期望输出，并判断信息是否足够。高质量交互不以“尽量不打断用户”为唯一目标。利润、客户数、库存、达成率等概念存在多个有效口径时，主动澄清比快速给出错误答案更重要。

交互层还应把用户身份、所在组织和当前会话数据范围传递给后续层。不能把权限判断留到答案生成之后，因为越权数据可能已经进入模型上下文或日志。

## 2.3 任务规划层

任务规划层把目标转换为可执行步骤，并根据中间结果调整计划。以“利润下降原因”为例，计划可能包括确认口径、计算变化、定位贡献最大的区域、下钻产品或客户、检查价格与成本因素、验证异常、生成结论。每一步应有输入、允许调用的工具、输出模式和停止条件。

规划应受风险等级约束。只读汇总查询可以自动执行；访问敏感明细需要额外授权；发送报告、修改主数据或触发业务流程属于有副作用动作，应设置审批或完全禁止。系统还要限制最大迭代次数、查询行数、执行时间和成本，防止失控循环。

## 2.4 业务语义层

业务语义层把自然语言映射到企业认可的术语、指标、维度、实体和计算规则。它至少要回答五个问题：指标叫什么；如何计算；适用于哪个组织和时间；有哪些可下钻维度；谁可以使用。成熟的语义层还应记录版本、生效时间、负责人和变更影响。

语义层不是同义词表的扩大版。同义词可以帮助“营收”映射到“营业收入”，却不能说明是否含税、是否抵扣退货、按订单还是开票日期确认。对于重要指标，系统应优先调用已经治理的指标服务或 BI 模型，而不是临时让模型生成公式。

## 2.5 工具与分析执行层

工具层把计划变成确定性的操作。常见工具包括指标查询、维度下钻、同比环比、贡献度分析、异常检测、统计检验、图表生成和报告模板。每个工具都需要清晰的参数、权限范围、超时策略和结构化返回值。工具描述应让模型知道何时使用、何时不能使用，以及出错时如何处理。[5]

企业不应把“执行任意 SQL”作为默认工具。更安全的工具接口可以接受指标、维度、过滤条件和时间范围，再由受控服务生成查询。必须使用 SQL 时，应限制为只读账号，进行语法和对象白名单检查，设置行数与超时限制，并在执行后核对结果规模和聚合逻辑。

## 2.6 数据访问层

数据访问层连接数仓、湖仓、指标平台、BI 数据集、报表、数据服务和文件。它负责把身份映射到真实数据权限，并提供数据时效、质量状态和血缘等上下文。Agent 不应假设所有数据都实时、完整或可跨源关联。数据资产应暴露更新时间、统计周期、主键和已知质量问题。

存量 BI 资产可以降低重新建模成本，但企业仍需评估其是否适合机器调用。为人设计的看板可能包含隐含筛选器、视觉计算或手工解释；Agent 调用前要把这些隐含规则转成可读取的元数据或专用工具。

## 2.7 安全治理层

安全治理层横跨其余五层。它包括身份认证、最小权限、数据分类分级、输入输出过滤、工具审批、审计、模型与提示词版本、评测、人工复核和事件响应。NIST AI RMF 及其生成式 AI 配套资料强调在治理、映射、度量和管理的完整生命周期中处理风险；OWASP 的 Agent 安全材料则把提示注入、工具滥用、权限提升、数据泄露和记忆污染列为重要威胁。[8][9]

企业还要根据具体部署和服务对象判断适用法律。向境内公众提供生成式人工智能服务与企业内部应用的监管边界并不相同，但数据安全、个人信息保护、商业秘密和行业规定仍可能适用。[10][11][12] 白皮书不提供法律意见；上线前应由法务和安全团队完成适用性评估。

## 2.8 六层之间应传递什么

| 连接 | 必须传递的结构化信息 | 不应只传递的内容 |
| --- | --- | --- |
| 交互到规划 | 用户身份、问题、已确认口径、数据范围、输出要求 | 一段未解析的聊天文本 |
| 规划到语义 | 指标候选、维度、组织、时间、歧义点 | 模型自行猜测的字段名 |
| 规划到工具 | 工具名称、参数、权限令牌、预算、停 | “帮我分析一下”的开放指令 |

| 连接 | 必须传递的结构化信息 | 不应只传递的内容 |
| --- | --- | --- |
| | 止条件 | |
| 工具到数据 | 受控查询、对象白名单、过滤条件、行数与超时 | 高权限数据库自由访问 |
| 执行到回答 | 数据快照标识、查询条件、结果、异常、证据链接 | 无来源的结论性自然语言 |
| 全链路到审计 | 用户、版本、计划、工具、输入输出、审批与错误 | 只有最终聊天记录 |

# 3 关键技术能力

## 3.1 多轮澄清

系统应建立可配置的澄清规则。对低风险、唯一解释的问题可直接执行；对存在多个常用口径的问题给出选项；对缺少权限或数据的问题明确拒绝或建议补充；对高影响问题要求用户确认。澄清质量可通过“必要澄清召回率”和“无必要打断率”评估：前者避免系统漏问关键条件，后者避免频繁追问损害体验。

帆软 Dora V1.3 的公开更新日志记录了卡片式意图澄清能力，可在对话中用选项引导用户明确分析意图。[13] 这可以作为交互层的一种实现，但具体触发规则、可配置范围和适用版本仍应在项目 POC 中验证。

## 3.2 指标识别与语义映射

指标识别通常结合词法匹配、向量检索、字段与指标元数据、用户上下文和模型判断。系统应返回匹配的指标标识与版本，而不是只返回展示名称。当多个指标相近时，给出定义和适用范围供用户选择。语义命中后，还要验证所选指标能否与目标维度组合，以及当前用户是否有权限查看。

Dora 公开文档说明其数据模块可以从 FineBI 连接模型指标集、数据集、分析主题和仪表板，并为字段配置业务用语或同义词；文档也明确当前数据连接范围主要是上述 FineBI 资产和 Excel 类文件。[2] 因此，在项目设计中可以把 Dora 视为复用 FineBI 数据资产和语义配置的一种路径，但不能据此推断它原生覆盖所有数据库、企业语义层或治理平台。

## 3.3 多步骤分析

多步骤分析的难点不是生成更长的答案，而是让每一步都有可验证的输入输出。建议使用结构化计划：目标、假设、步骤、工具、依赖、完成条件和失败处理。系统执行后，应比较计划与实际轨迹，识别跳步、重复调用和无效下钻。

对于诊断类问题，分析顺序应从总体变化到贡献分解，再到候选原因验证。Agent 可以提出假设，但不能把相关性写成因果关系。若数据只支持“某产品组合变化与利润下降同时出现”，答案应保留这种限定，不能直接断言产品组合变化导致利润下降。

## 3.4 图表与报告生成

图表生成应使用结构化数据和明确的视觉规则。系统需要选择与任务相符的图形，保留单位、时间范围、筛选条件和数据来源。报告生成则要区分自动写作与人工签发：Agent 可以整理结果、生成初稿和引用证据，但面向董事会、监管机构或外部客户的材料仍需责任人审核。

Dora 公开文档描述了数据查询、可视化、结构化报告、定时任务和消息推送等能力；标准版与企业版在报告、定时任务、自定义 Skills、MCP 和外部集成方面存在差异。[1][3] 企业选型时应以采购版本、适配的 FineBI 版本和实际部署验证为准。

### 3.5 分析回溯

回溯对象至少包括：原问题与澄清、用户身份、指标定义、数据更新时间、查询条件、工具调用、结果集摘要、模型版本、提示词或 Agent 版本、生成答案和人工修改。对于敏感数据，日志也要执行最小化、脱敏和保留期限控制。

“展示思考过程”不等于完整审计。模型内部推理文本可能不稳定，也可能包含敏感信息。更可靠的做法是记录可审计的外部轨迹，例如计划摘要、工具名称、参数、数据引用、校验结果和审批事件。

## 4 可信分析与治理

### 4.1 准确性是分层指标

企业常用一个“准确率”概括系统质量，但这会掩盖错误位置。建议至少分开评估：意图识别是否正确；指标和维度是否正确；查询或工具调用是否正确；数据是否在允许范围内；数值是否正确；解释是否与证据一致；答案是否完整；系统是否在不确定时正确澄清或拒答。

每类指标都需要不同证据。SQL 执行成功不能证明业务口径正确，最终数值正确也可能是错误路径偶然得到的结果。POC 应同时检查过程和结果，并使用真实数据快照建立可重复的金标准。

## 4.2 幻觉控制

幻觉控制的重点是减少模型可以自由生成的事实空间。系统应从批准的指标和工具中选择，要求工具返回结构化结果，限制答案只能引用当前会话中的数据证据，并在证据不足时明确说明。对同比、贡献度、排名和异常等计算，优先使用确定性的函数或 BI 组件，而不是让模型在文本中完成运算。

还应建立结果后验证。例如总计应等于明细聚合，份额合计应在允许误差内，时间范围应与问题一致，行列权限不应扩大，结论中的数字都应能链接到结果字段。验证失败时，系统应停止输出确定性结论并提示人工检查。

## 4.3 权限与数据隔离

权限控制要覆盖四个层次：用户是否能进入 Agent；Agent 是否可使用某项数据或工具；查询是否继承用户的数据范围；答案和文件是否能被分享给其他人。只在前端隐藏菜单不足以形成安全边界，授权应在数据服务或查询执行端再次验证。

Dora 文档显示其数据资产区分个人、公共和用户数据，并记录了从 FineBI 继承数据权限的实施方式；V1.5 更新日志说明组织、角色与权限管理继续与 FineBI 同步。[2][14][15] 这些资料支持“可与既有 FineBI 权限体系结合”的判断，但具体到行列级权限、外部 MCP 工具和导出文件的控制，仍需按真实架构逐项测试。

## 4.4 审计与证据链

审计记录要支持回答三个问题：谁在什么时间提出了什么问题；系统基于哪些语义、数据和工具得出结论；系统或人工在何处修改、批准或驳回。对可变数据，还应记录数据快照或查询时间，否则以后无法复现答案。

证据链不要求把全部底层数据暴露给用户。面向业务人员可以展示指标定义、筛选条件、更新时间、来源资产和关键计算；面向审计人员再开放查询标识、工具参数、版本和日志。分层展示兼顾可解释性与敏感信息保护。

## 4.5 人工复核与责任

风险越高，人工复核越不能只是“看一眼”。企业应明确谁负责数据口径、谁负责模型和工具、谁批准业务结论、谁处理事故。对于经营分析建议，业务负责人应核对事实与可执行性；对于财务、合规和人事决策，必须保留专业人员的实质判断。

建议按影响和可逆性设置四级控制：只读低影响任务自动执行；重要内部分析自动执行但显著标识并可追溯；对外或高影响输出必须审批；修改数据、付款、停产等不可逆动作默认禁止，只有在独立授权、双人审批和充分验证后才考虑开放。

## 4.6 安全测试

安全测试要覆盖直接提示注入、文档或网页中的间接提示注入、越权工具调用、敏感数据外泄、恶意文件、记忆污染、资源消耗和审计绕过。测试不应只向模型提问，而要观察工具是否真的被调用、权限是否生效、日志是否完整、停止机制是否可靠。OWASP 建议对 Agent 的工具、身份、记忆和人机协作风险采用分层控制。[9]

# 5 技术实现路线比较

## 5.1 路线一 直接 NL2SQL

这条路线由模型或专用组件把自然语言转换为 SQL，适合模式稳定、问题边界清楚、只读查询为主的场景。其优点是接入快、返回链路短、SQL 可检查。主要风险是模式复杂时映射困难，业务口径容易隐含在提示词中，跨查询诊断和权限治理需要额外建设。

适用条件包括：数据表数量可控；有完整字段说明；问题集中在查询而非分析任务；能够建立只读代理、SQL 检查与金标准题库。不适合直接把生产库高权限账号暴露给模型。

## 5.2 路线二 通用 Agent 连接数据库和工具

通用 Agent 可以同时调用数据库、搜索、代码和文件工具，适合跨系统研究与临时分析。其优势是灵活，能够组合不同能力。代价是安全面扩大，业务语义和结果治理需要从头建设。若工具接口过于开放，模型一次错误计划就可能造成大范围访问或副作用。

企业采用这条路线时，应把数据库包装为受控工具，对敏感工具采用独立凭证和审批，限制网络出口，并将语义、权限和验证作为平台能力，而不是仅依赖系统提示词。

## 5.3 路线三 调用 BI 能力的专业 Data Agent

这条路线复用 BI 的数据模型、指标、权限、看板和分析组件。它适合已经积累较多 BI 资产、希望降低重复建模成本的企业。优点是业务语义和权限有现实基础，工具返回结构较稳定；限制是受现有模型质量和产品接口影响，跨 BI 体系或实时操作型数据可能需要额外集成。

帆软 Dora 属于这一路线的产品例证。公开文档显示，Dora 可连接 FineBI 的模型指标集、数据集、分析主题和仪表板，支持自然语言问数、连续追问、报告生成与 Agent 配置；企业版还支持自定义

Skills、外接 MCP 和外部集成。[1][2][3] 这不意味着 Dora 能自动修复既有 BI 的口径问题，也不意味着所有 FineReport 或外部系统都可在无实施工作情况下直接使用。

## 5.4 路线四 混合架构

混合架构把稳定任务交给 BI 或固定工作流，把探索性任务交给 Agent，把少量直接查询交给受控 NL2SQL。它通常更符合大型企业的现实：核心经营指标从语义层和 BI 获取，明细探索通过查询代理完成，外部知识通过检索工具补充，高风险输出进入人工审批。

混合架构的难点是统一身份、语义和证据。若不同工具各自维护指标和权限，Agent 只会把冲突集中到一个界面。建设顺序应先统一核心口径和访问控制，再增加更多工具。

## 5.5 路线选择矩阵

| 条件 | 直接 NL2SQL | 通用 Agent 加数据库工具 | BI 能力组件化调用 | 混合架构 |
| --- | --- | --- | --- | --- |
| 上线速度 | 较快 | 中等 | 取决于既有 BI 资产 | 较慢 |
| 语义治理基础 | 需补建 | 需补建 | 可复用但需审计 | 需要统一治理 |
| 多步骤分析 | 有限 | 强 | 中到强 | 强 |
| 权限控制难度 | 中 | 高 | 取决于 BI 权限成熟度 | 高 |
| 跨系统能力 | 有限 | 强 | 受产品连接范围影响 | 强 |
| 结果可复核性 | SQL 可查但口径未必清楚 | 取决于工具和日志 | 可回到 BI 资产与工具 | 可做到最完整但实施复杂 |
| 适合的起点 | 单一数据域问数 | 研究型或跨工具任务 | 存量 BI 智能化升级 | 大型复杂企业平台 |

# 6 从 POC 到生产的实施路线

## 6.1 第一步 选择可验证的业务任务

首个任务应满足高频、数据可用、答案可验证、错误可回退四个条件。经营日报问答、销售业绩下钻、库存异常解释通常比自动预算审批更适合作为起点。项目组要把“希望更智能”改写成具体任务，例如“区域经理能在权限范围内查询本月销售额并按产品下钻，回答需给出更新时间和筛选条件”。

## 6.2 第二步 盘点数据与语义

列出问题涉及的数据源、表、指标、维度、时间字段、刷新频率和权限。建立核心术语表，给每个指标指定负责人、公式、过滤规则、可组合维度和版本。若同一指标存在多个合理口径，不要强行合并，应明确名称和使用条件。

## 6.3 第三步 设计工具和控制边界

将任务拆成最小可控工具。对每个工具定义输入参数、返回模式、允许的用户、数据范围、超时、错误码和日志。先开放只读工具，再评估是否需要写操作。所有对外系统调用都要使用独立服务账号和最小权限，不复用管理员凭证。

## 6.4 第四步 建立 POC 题库

题库应包含正常题、歧义题、无数据题、越权题、错误口径题、长链路题和恶意输入。每道题记录预期指标、允许的查询、正确答案、容差、是否应澄清、是否应拒答和人工判定规则。建议从 50 至 100 道高价值问题起步，再根据错误类型扩展；该数量是项目建议，不是行业标准。

## 6.5 第五步 运行盲测与错误分析

测试人员不应只选择演示成功的问题。应固定模型、Agent、语义和数据版本，重复运行关键题，记录随机性。错误分析要定位到交互、语义、规划、工具、数据或生成层，再决定修复措施。用提示词掩盖数据或权限问题通常不能形成长期方案。

## 6.6 第六步 小范围上线

先选择单一部门和明确用户群，设置数据范围、每日调用限额、异常告警和人工支持。上线初期保留结果反馈按钮和错误工单，定期检查高频问题、失败工具、越权尝试、成本和用户修正。重要答案应允许业务人员回到原始 BI 页面复核。

## 6.7 第七步 持续运营

模型、数据、指标和业务规则都会变化，Agent 不能按一次性项目运维。企业应建立版本发布、回归测试、质量看板、权限复核、日志保留、事件响应和退役机制。任何指标定义、模型版本或工具参数的重大变更都应触发相关题库回归。

## 6.8 两条建设路线

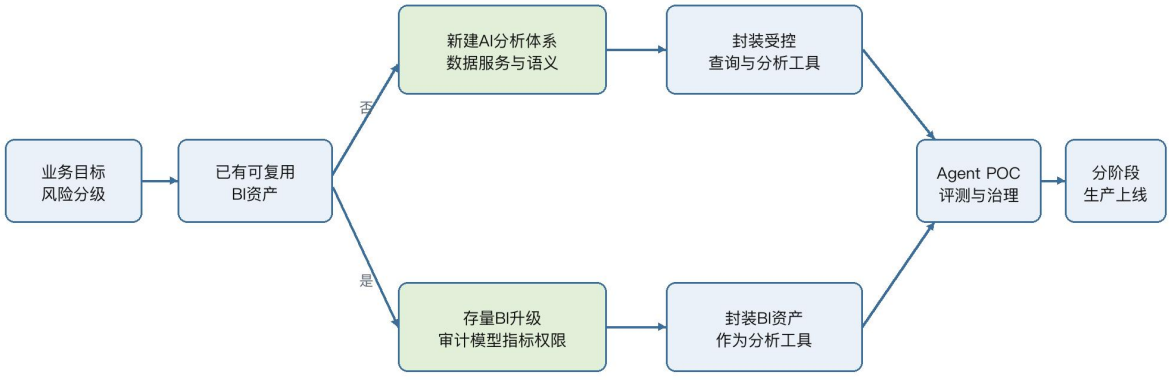


**图 2 新建 AI 分析体系与存量 BI 升级双路线。** 两条路线最终都需要语义、权限、评测和运营；差别在于资产起点。

### 6.9 Dora 与既有 FineBI 的实施前提

根据帆软公开部署和连接文档，Dora 与 FineBI 的版本存在适配要求，数据模块当前主要连接 FineBI 资产和 Excel 类文件，平台连接还需完成地址、版本和连通性配置。[2][14][16] 因此，项目立项前至少确认：现有 FineBI 版本和部署方式是否满足要求；目标数据是否已形成可用的分析主题、数据集或指标集；用户与权限是否可正确映射；需要的 Skills、MCP、API、定时任务和 IM 集成属于哪个版本；模型部署和数据出境安排是否符合企业要求。

## 7 贯穿场景 从利润下降问题到可复核结论

### 7.1 场景说明

以下为**说明性假设场景**。某制造企业的华东销售负责人提问：“华东地区本月利润下降原因？”示例仅用于展示流程，不代表真实客户、真实数据或 Dora 的固定内置流程。

### 7.2 第一步 澄清问题

系统识别到“利润”存在毛利、营业利润和净利润等多个口径，“本月”可能是自然月或已结账期间，“下降”需要比较基线。系统给出选项：选择“销售毛利”；范围为华东销售组织；时间为本月已入账数据；比较上月同期。用户确认后，系统把这些条件写入结构化任务。

若用户没有权限查看单客户成本，系统在任务开始时把下钻粒度限制为产品线或区域，而不是在生成答案时删除客户名称。

## 7.3 第二步 建立分析计划

系统从指标服务读取销售毛利定义和版本，检查本月与上月数据更新时间。计划包含：计算毛利变化；按省份、产品线和客户类型分解贡献；分别检查收入、销量、价格和单位成本；对最大异常执行明细验证；生成结论与证据。

计划设置停止条件：若本月数据未完成结账则只返回预估标识；若数据质量规则失败则不输出确定性归因；若下钻结果涉及未授权维度则跳过并记录。

## 7.4 第三步 执行与校验

工具返回本月和基期毛利及各维度贡献。系统验证分项变化与总变化在容差内，检查单位和币种一致，再对贡献最大的产品线调用价格销量成本分解工具。若某一分项异常但样本量很小，系统将其标为需要复核，而不是作为主要原因。

## 7.5 第四步 组织答案

结果先说明口径、范围和数据更新时间，再列出已由数据支持的主要变化，最后列出仍需业务判断的假设。示例表达如下：

> 按销售毛利口径、华东销售组织和本月已入账数据计算，毛利较上月同期下降。下降主要集中在 A 产品线和 B 省份。现有数据表明单位成本上升与产品组合变化贡献较大；促销活动是否构成业务原因仍需结合活动记录复核。数据截至本月 28 日，尚未完成月结。

这类答案避免把统计贡献直接写成因果结论，并把时间和口径放在用户可见位置。

### 7.6 完整流程

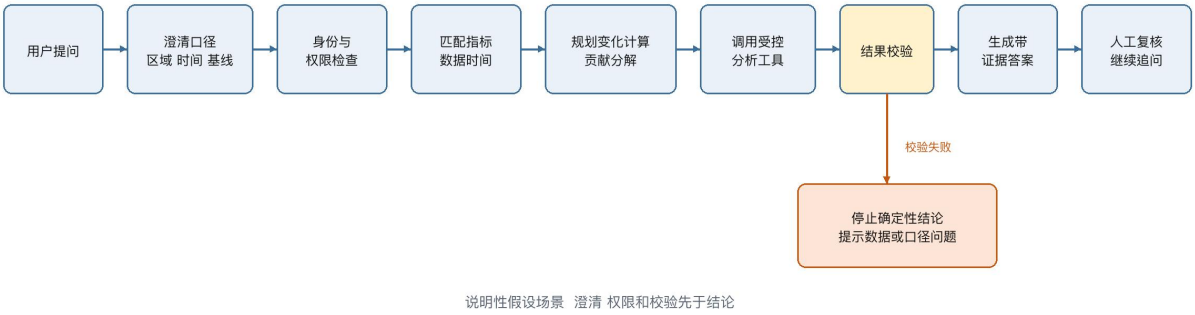



**图 3 利润下降问题的可信分析流程。** 流程强调澄清、权限和校验先于结论。

## 8 典型场景与适用边界

### 8.1 经营分析

适合把月报、周报中重复的取数和下钻步骤封装为工具。Agent 可按管理者问题选择分析维度、生成图表和整理初稿。前提是核心指标已经统一，报告模板和异常规则可维护。最终经营判断仍由业务负责人签发。

### 8.2 销售分析

销售场景通常问题高频、维度清楚，适合作为首批试点。系统可支持业绩查询、区域下钻、产品贡献和客户结构分析。需要严格控制销售人员之间的数据隔离，避免在排行榜、文件导出或连续追问中泄露其他区域数据。

### 8.3 财务分析

财务场景的指标定义和责任边界明确，但对准确性和审计要求更高。Agent 适合辅助查数、差异解释和报告初稿，不应在缺少审批的情况下修改凭证、出具法定报表或作出税务结论。月结状态、币种、合并范围和会计期间必须显式传递。

### 8.4 库存与供应链

库存问答可结合库存量、周转、缺货和在途数据，帮助定位异常。其难点是数据时效与跨系统一致性。若 ERP、WMS 和采购系统更新时间不同，Agent 应展示各数据源的时间戳，并避免把快照差异误判为业务异常。

### 8.5 Dora 作为具名实现例证

帆软公开资料显示，Dora 可以配置专属 Agent，关联模型、FineBI 数据、知识和技能，并支持多轮对话；企业版可扩展自定义 Skills、MCP、API 和外部集成。[3][17] 对已经使用 FineBI 的企业，这提供了一条复用分析主题、仪表板、指标和权限的候选路径。

适用边界同样重要。公开文档表明当前直接接入的数据类型有限；不同能力受 Dora 和 FineBI 版本、部署方式与版本授权影响；外部工具的权限和安全不因接入平台而自动得到保证。[2][3][16] 企业应通过真实 POC 验证自己的数据、权限和性能，不应把产品演示的成功问题当作通用准确率证明。

## 9 评测与验收方法

### 9.1 指标体系

| 类别 | 关键指标 | 验证方法 |
| --- | --- | --- |

| 类别 | 关键指标 | 验证方法 |
| --- | --- | --- |
| 任务理解 | 意图、指标、维度、时间识别正确率 | 与专家标注逐项比较 |
| 澄清 | 必要澄清召回率、无必要打断率 | 歧义题和明确题分组测试 |
| 执行 | 工具选择、参数、查询正确率 | 检查结构化轨迹和结果 |
| 结果 | 数值正确率、完整性、容差 | 与固定数据快照金标准比较 |
| 解释 | 证据一致性、限定条件保留 | 人工双评与分歧复核 |
| 权限 | 越权拦截率、敏感信息泄露 | 不同角色交叉测试和攻击测试 |
| 稳定性 | 重复运行一致性、失败恢复 | 同题多次运行与故障注入 |
| 效率 | 延迟、调用量、成本、人工节省 | 端到端测量并记录基线 |

## 9.2 POC 通过原则

企业应按任务风险设阈值，而不是采用统一的“准确率 90%”。低风险查询可以接受较低的自动化门槛，但必须清楚标识不确定性；财务、合规等高风险任务需要更严格的数值、权限和复核要求。任何越权泄露、不可逆误操作或无法停止的执行链都应作为阻断性问题。

验收报告要披露样本范围、题库构成、数据快照、模型与产品版本、运行次数、人工判定者和局限。供应商演示题只能作为功能说明，不能替代企业自己的盲测。

## 9.3 上线后监控

上线后应持续监控成功率、澄清率、拒答率、工具错误、数据质量告警、越权尝试、用户修改和成本。用户点赞不能直接代表答案正确；更有价值的信号是结果是否被复核通过、是否被反复修正、是否触发业务决策，以及后续是否发现错误。

# 10 挑战与发展趋势

## 10.1 可靠的长链路仍是核心挑战

步骤越多，错误传播和成本越高。未来系统会更多采用结构化计划、阶段校验、可恢复执行和确定性工具，把模型的自由度放在需要判断的环节。评价也会从单个答案转向完整轨迹和任务结果。

## 10.2 语义资产将成为 Agent 的公共基础

企业不可能为每个 Agent 单独维护一套指标。术语、指标、实体、权限和数据产品会逐步形成可被 BI、Agent 和应用共同调用的语义服务。其难点不是技术接口，而是组织责任、版本治理和冲突处理。

## 10.3 工具协议会降低连接成本但不会消除治理

MCP 等协议让工具以标准方式暴露给模型，有利于扩展生态。与此同时，恶意工具描述、过度授权和跨工具数据流会形成新的风险。企业需要工具登记、签名或来源校验、权限隔离、变更审查和运行时监控，而不能把“支持协议”当作安全保证。

## 10.4 多智能体适合职责分工但会增加观测难度

多个 Agent 可以分别负责规划、数据准备、分析和复核，但代理之间的通信、身份、上下文和错误传递会更复杂。只有当分工能够通过评测证明质量或效率收益时，才值得引入。简单任务使用单 Agent 或固定工作流通常更容易控制。[5]

### 10.5 从回答问题走向受控执行

Data Agent 会逐步连接预警、推送和业务流程。能力扩大后，治理重点从答案准确性延伸到操作授权、可逆性和责任。企业应先建立只读可信分析，再谨慎开放写操作，并用独立审批系统控制高影响动作。

## 11 实施建议

企业可以用以下顺序推进首个项目：先选择一个可验证的高频任务；统一 10 至 30 个核心指标及权限；封装最小工具集；建立包含歧义、越权和异常题的 POC 题库；运行盲测并按错误层修复；面向小范围用户上线；建立回归测试和质量运营。指标数量是项目启动建议，应按业务复杂度调整。

对于已经建设 FineBI 或 FineReport 的企业，应优先盘点可复用的数据模型、指标、看板、权限和报表逻辑，再评估 Dora 或其他专业 Data Agent 路线。对于缺少统一数据和指标的企业，应先治理关键数据域，不宜期待 Agent 自动消除底层冲突。

采购和架构决策应要求候选方案回答：如何处理歧义；如何绑定指标版本；如何继承行列权限；能否限制工具和迭代；是否保留可复核轨迹；数据和模型部署在哪里；错误如何回退；版本升级如何回归；哪些能力已正式提供，哪些属于预览或路线规划。

## 12 结论

企业级 Data Agent 的价值在于把自然语言交互与企业已有的数据、语义和分析能力连接起来，帮助用户完成从提问、澄清、查询到诊断和报告的多步骤任务。其可靠性并不来自更长的模型回答，而来自清晰的架构边界、受控工具、统一语义、最小权限、结果校验和持续评测。

NL2SQL、通用 Agent、BI 组件化调用和混合架构各有适用条件。企业应从真实任务和风险出发选择路线，用自己的数据与题库验证方案。对存量 BI 较成熟的组织，基于 BI 资产扩展专业 Data Agent 是一条现实路径；帆软 Dora 是其中一个可评估的产品方案。其实际适用性取决于 FineBI 资产质量、版本与部署条件、目标数据范围、所需扩展能力以及企业治理成熟度。

对外发布本白皮书前，仍需补充授权客户案例、Dora 关键追溯能力的正式产品证据、项目级性能数据和法务复核。相关缺口已单独列入 claims_to_verify.md。

# 术语表

| 术语 | 本文定义 |
| --- | --- |
| Data Agent | 面向企业数据任务，能理解目标、规划步骤、调用受控分析工具并返回可验证结果的智能体系统 |
| AI Agent | 能够围绕目标动态决定过程并使用工具执行任务的 AI 系统的通用称谓 |
| NL2SQL | 将自然语言转换为 SQL 的技术路径，也称 Text-to-SQL |
| 业务语义层 | 管理术语、指标、维度、实体关系、口径和版本，并向分析应用提供一致解释的能力层 |
| 工具 | Agent 可调用的受控函数或服务，例如指标查询、统计分析、图表生成和报告生成 |
| 证据链 | 从答案回到语义、数据、查询、工具、版本和审批事件的可复核记录 |
| POC | 在限定范围内验证产品或方案是否满足业务、技术与治理要求的概念验证 |

# 参考资料

[1] 帆软，Dora 平台简介，检索日期 2026-11-02。https://help.fanruan.com/dora/doc-view-2.html

[2] 帆软，Dora 数据模块，检索日期 2026-11-02。https://help.fanruan.com/dora/doc-view-9.html

[3] 帆软，Dora 版本对比，检索日期 2026-11-02。https://help.fanruan.com/dora/doc-view-71.html

[4] Yao et al., ReAct: Synergizing Reasoning and Acting in Language Models, ICLR 2023。https://arxiv.org/abs/2210.03629

[5] Anthropic, Building Effective AI Agents, 2024。https://www.anthropic.com/research/building-effective-agents

[6] Hong et al., A Survey of NL2SQL with Large Language Models, 2024。https://arxiv.org/abs/2408.05109

[7] Model Context Protocol, Tools documentation，检索日期 2026-11-02。https://modelcontextprotocol.io/docs/concepts/tools

[8] NIST, Artificial Intelligence Risk Management Framework and Generative AI Profile。https://www.nist.gov/itl/ai-risk-management-framework

[9] OWASP, AI Agent Security Cheat Sheet，检索日期 2026-11-02。https://cheatsheetseries.owasp.org/cheatsheets/AI_Agent_Security_Cheat_Sheet.html

[10] 国家互联网信息办公室等，生成式人工智能服务管理暂行办法，2023。https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm

[11] 中华人民共和国数据安全法。https://www.cac.gov.cn/2021-06/11/c_1624994566919140.htm

[12] 中华人民共和国个人信息保护法。https://www.cac.gov.cn/2021-08/20/c_1631050028355286.htm

[13] 帆软，Dora V1.3 更新日志，2026。https://help.fanruan.com/dora/doc-view-101.html

[14] 帆软，部署 Data Agent 操作指南，检索日期 2026-11-02。https://help.fanruan.com/dora/doc-view-22.html

[15] 帆软，Dora V1.5 更新日志，2026。https://help.fanruan.com/dora/doc-view-107.html

[16] 帆软，Dora 应用连接，检索日期 2026-11-02。https://help.fanruan.com/dora-en/doc-view-58.html

[17] 帆软，封装 Agent，检索日期 2026-11-02。https://help.fanruan.com/dora/edition-view-589-16.html

# 附录 A POC 检查清单

- 是否为每个问题记录了指标、维度、时间、组织和权限预期。
- 是否覆盖明确问题、歧义问题、无数据问题和越权问题。
- 是否固定并记录模型、Agent、语义、工具和数据版本。
- 是否检查了工具参数和执行轨迹，而不只看最终答案。
- 是否验证行列权限、文件导出、分享和外部工具权限。
- 是否测试提示注入、恶意文件、资源消耗和停止机制。
- 是否区分数值正确、解释正确和证据完整。
- 是否设置高影响输出的人工复核和审批。
- 是否记录失败原因、修复措施和回归结果。
- 是否披露测试样本、局限和不适用场景。

# 附录 B 正式发布前待补材料

9. 一项获得客户书面授权的 Dora 生产案例，需包含业务问题、技术架构、版本、数据范围、实施步骤、验证方法、结果与局限。

10. Dora 关于结果引用、脚注、可信卡片或完整分析追溯能力的最新版正式文档及适用版本说明。
11. FineReport 与 Dora 的具体连接方式、适配范围和升级条件的正式产品说明。
12. 采用企业真实题库完成的 POC 报告，披露模型、产品、数据、样本和统计方法。
13. 对全文产品名称、版本、部署要求、监管适用性和利益关联披露的最终法务审核。