

客户经营大脑

产品需求与架构设计

2026-09-21 · 评审稿 1.0 · 代码基线 e37d400 · 本地文档，未发布

同一仓库，清晰的三方责任

大脑消费交互证据、业务事实和履约条件，形成事项理解与受约束建议。顾问确认后，CRM 创建任务；真实执行证据回流后，大脑再更新事项与承诺。

VP · 语音平台

转写、角色、证据定位
会话分析与销售质检

客户经营大脑

事项理解、任务上下文
承诺历史与结果学习

CRM · 顾问台

业务字段、人工确认
任务执行与原始回执

先完成两周销售 A 离线基线，再满足真实身份、权限和回执门禁后进入受控试点。自动外呼本期禁止。

客户经营大脑产品需求文档

本文是 PRD（产品需求文档）评审稿，覆盖完整产品目标和分阶段建设范围。依据 2026-09-21 核查的 MP3 `main @ e37d400` 编写；“目标能力”不代表已经实现、批准上线或验证经营效果。本文与架构设计方案配套：产品需求编号以本文为准，技术落点与实施单元以架构文档为准。

1. 产品决策与建设目的

推荐在 MP3 同一仓库内建设独立客户经营大脑，与 Voice Platform（语音平台，简称 VP）保持清晰模块边界。VP 做好语音转写、说话人及角色处理、带定位的对话证据、单次会话分析；大脑汇聚多源证据和业务事实，维护事项理解、任务上下文、承诺历史和行动建议；CRM（客户关系管理系统）及顾问台承接人工确认、业务任务与执行回执。

输入是客户交互证据、业务系统事实、产品知识和门店履约能力；大脑围绕一个客户的一个事项组织这些信息，生成有依据、有边界的建议；顾问确认后，由业务系统执行并返回结果。没有新录音时，大脑仍能根据订单变化、顾问补充和任务回执更新；没有大脑时，VP 仍能独立完成语音分析。

当前问题不是缺少更多客户标签，而是顾问无法快速回答：这个客户当前卡在哪里，已经试过什么，客户如何回应，我们答应过什么，下一步能做什么。管理人员也需要分清建议被采纳、任务被执行和事项取得进展这三件事。

对象	核心责任	不承担的责任
MP3	代码协作、构建与交付的仓库载体	不作为新增业务系统名称或数据权威
VP	音频与文本输入、转写标准化、对话证据、会话级分析和语音质量优化	跨源客户主数据、长期事项状态、业务执行
客户经营大脑	客户理解、事项上下文、承诺账本、受约束建议、结果学习	到账、库存、交期等业务主数据的另一个权威源
CRM / 顾问台	已确认客户业务字段、商机、执行任务、人工操作和回执	重复维护大脑的事项认知与承诺账本
DMS / 订单 / 工单系统	各自业务事实和履约状态	由对话或模型替代正式记录

“建在 MP3 内”是仓库组织选择；“与 VP 分开”是产品责任与依赖方向选择。本期不以拆仓、拆六个服务或重做 CRM 为交付目标。

2. 产品范围与依据

2.1 命名与关键对象

工作名统一为“客户经营大脑”；正式表述为“AI 原生客户认知与行动引擎”。工程包建议名 `customer_brain`。VP 旧称 Vios；口语 P3 指 MP3。

Golden Context（当前理解）回答“此人、此刻、此事”：身份及其可靠程度、事项目标、有效事实、客户陈述、已做动作、客户反应、未决问题、有效及历史承诺、下一步建议和约束。它是可重建、有版本的理解视图，不是一份覆盖原系统的客户档案。

Task Context（任务上下文）是从当前理解中按具体任务、接收者权限和有效期裁出的最小信息包。它不携带执行授权，不等于发送消息、改价或创建业务任务的接口。

“事项”指有明确目标、当前状态和结束条件的一段经营工作，例如一次试驾后的购车推进。一个客户可以同时有多个事项；一个事项可以有多个会话和业务对象。同一个客户的两辆车、两次购车意向不能自动混成一个事项。

2.2 当前代码能证明什么

现状分类	已核查内容	对产品范围的影响
已有可复用实现	VP 的 <code>audio / transcript / dialogue</code> 输入、销售分析、规则式下一步建议、回放和优化框架	离线试点从已有转写与分析结果开始，不重做 ASR（自动语音识别）
已有业务骨架	CRM 的客户、商机、记忆候选、任务、策略采纳及渠道回执模型	可作为执行系统接入；现有演示路由的授权、幂等范围和回执关联需补齐
已有合同或局部实现	<code>CustomerJourneyEvent</code> 、来源信息、 <code>customer_master_view</code> 、客户智能接入模块	可借用对象语义；不能宣称已完成跨源身份仲裁、字段确认和结果闭环
演示或代理指标	CRM 演示录音、空业务表；接触频次推断的履约反馈；接受请求的网关返回	不作为真实证据播放、履约、成交或业务完成的验收依据
本方案拟新增	独立大脑模块、事项上下文、带版本确认、独立承诺历史、可靠命令和结果关联	需建设与验证，不能用已有类名代替交付证明

代码依据见架构文档第 2 节。当前 `src/crm/web` 是现有 Web 页面；外部 `mp3-saas` 与 React/Vite 的历史讨论不能直接视为当前统一前端实现。本期以仓内 CRM 接口和页面为默认接入点，实际试点部署位置须在线上线上准备时确认。

2.3 PR7 研究数据的实际边界

核查的研究包包含 146,581 个纳入文件记录、64,099 个去重对象，压缩对象约 216 MB；默认提取主链 ASR 369 份。数字用于说明数据起点，不用于证明客户覆盖或经营效果。

抽查聚合结果中，439 份客户视图都有会话标识，但没有非空 `customer_master_id`；CRM 导出的 60 张表中，除钟表 1 行外，59 张业务表为空。原始约 90 GB 录音只有清单，不在研究包内。基于词语筛出的约 40 份犹豫候选、约 20 份同时出现试驾词的候选，仍需人工确认，不能称为 20 个已确认销售事项。

研究数据是脱敏假名快照，既不是生产数据库，也不是人工金标。合作方对照及质量隔离数据默认排除；不得为了凑样本擅自打开 `--allow-reference`。

3. 用户、使用场景与产品价值

用户	当前工作	产品提供的结果	责任边界
销售顾问	看记录、判断阻碍、约下一步、记录执行	一张事项理解卡，证据可定位，明确需确认的缺口与可执行建议	确认事实或推断，决定是否采纳；不能越权读取客户
销售经理	分配资源、复核难例、处理逾期	事项阻碍、任务进展、未兑现承诺、失败原因	复核与分派在已有组织权限内进行
售后顾问	解释进展、管理预期、持续沟通	交付、沟通、承诺三条独立进度和约束建议	不以安抚状态阻塞实际维修或交付
运营 / 质检	评估建议、整理错误、维护场景规则	可复盘样本、来源、版本、分歧及失败分类	模型输出不能自行升级为训练金标
平台管理员	配置接入、权限和发布	可审计配置、候选评测、晋升及回滚记录	管理权限不自动获得客户业务操作权限
Agent（自动化助手）	请求某事项的上下文并提出动作	有范围和有效期的任务上下文及允许的命令入口	权限不高于所代表的人或服务，模型不能自签批准

业务价值假设是：减少顾问理解与准备时间，降低漏记、无效跟进和不当承诺，提高事项推进质量。当前没有真实业务数据证明这些效果；试点需测量，而不是预先宣称提升比例。

4. 阶段范围与不做

阶段	产品交付	进入条件	明确不包含
P0：两周离线基线	销售 A 召回、证据包、理解卡、人工复核、失败样本本、对照报告	PR7 校验可重复；有业务人员复核脱敏样本	真实客户触达、成交归因、生产身份合并、承诺兑现效果
P1：受控销售试点	真实客户及事项绑定、CRM 卡片和任务、人工采纳、可靠回执、最小销售承诺账本	真实身份、数据授权、任务及结果接口、写权限和技术门禁全部具备	自动外呼、自动优惠、未经确认的业务写回
P2：售后 B	维修待件延期事项、三线进度、变更与违约历史、安抚建议	工单、配件和计划时间的可靠来源及变更回执	用沟通结果覆盖实际维修状态；扩成泛化主动营销

阶段	产品交付	进入条件	明确不包含
P3：按证据扩场景	公用客户引擎与经过验证的场景包；按需要扩渠道	已有场景达成约定验收，新增场景有数据责任人	为覆盖全生命周期而一次建设所有渠道和标签

P1 的最小承诺包括“何时回电”“何时补充资料”等销售约定；完整延期与违约管理在 P2 扩展。P0 可以演示其状态转换，但必须标注虚构，不能统计真实履约率。

禁止项：未经书面批准自动外呼；自动改价、发券或跨店推荐；论坛数据定位个人；LLM（大语言模型）直接写业务库；模型输出直接作为金标；另立平行客户主数据；以向量库为事实权威；默认引入整套图数据库、流程编排和湖仓技术；改动生产运行配置或正式转写来完成实验；真实自动写回 DMS；把演示完成当成业务完成。

销售 A 是本稿的推荐一期范围，仍标注“待业务拍板”。K-013 的“一期只做维修进度推送”与该范围有冲突，本文不替其作出决定。K-015 对话不等于业务主数据、K-016 三线进度、K-005 承诺历史和 K-018 上下文不等于执行的纪律贯穿所有阶段。

5. 完整产品能力与需求

优先级 P0/P1/P2/P3 指第 4 节的建设阶段；“完整目标”是各阶段合起来的产品，不表示所有能力在两周内交付。

5.1 证据、身份与客户理解

编号	产品需求	阶段	具体规则
R01	同仓独立，VP 与大脑均可单独工作	P0	语音能力不依赖大脑；文本研究不启动生产 VP；结构化业务事实不强制走语音分析
R02	每项关键判断能追溯来源	P0	标识来源系统、对象、版本、时间、段落或轮次；没有音频时只定位文本并说明限制
R03	四栏区分业务事实、客户陈述、模型推断、待确认	P0	客户说“款已付”只能进入陈述；到账须引用正式财务来源；来源失效后不能继续展示为有效事实
R04	身份与事项关联可确认、可撤销	P0/P1	P0 使用研究域会话/事项标识；P1 使用真实系统标识；相似姓名、电话线索或模型置信度不能自动跨客户合并
R05	支持多会话同事项及一人多事项	P0/P1	会话属于哪个事项须有关联理由；不确定时分别保留；解绑后重建受影响上下文
R06	生成当前理解和待确认问题	P0	写明阻碍、已做动作、客户反应、冲突、信息缺口；证据不足时允许输出“无法判断”
R07	稳态、阶段性、事项性记忆各有归属	P1	已确认客户业务字段继续由 CRM 管理；大脑只保存带来源的观察、理解版本和事项状态，不复制字段确认系统
R08	产品、人车关系和履约能力参与建议	P1/P2	车型、配置、在库、试驾资源、预计交付等注明权威来源和有效期；缺失时建议“先核实”，不得编造优惠或交期

5.2 上下文、建议与人工确认

编号	产品需求	阶段	具体规则
R09	销售 A 候选召回与排除原因可见	P0	同时检查试驾已发生和存在未决推进事项；仅提到“以后试驾”不自动入选；负例和漏召回也进入评估
R10	事项理解卡给出有边界的下一步	P0	建议包含目标、理由、证据、前提、需确认事项、禁止动作；最多展示 3 个有顺序的建议，允许无建议
R11	按任务提供最小上下文	P1	绑定事项、接收者、用途、版本和有效期；撤权、身份解绑、承诺变更后旧上下文失效，不赋予执行权
R12	人工可采纳、修改、拒绝和补充	P0/P1	保留原草稿、修改内容、操作者和原因；P0 仅记录研究复核，P1 才可能创建真实业务命令
R13	过期与并发修改可发现	P1	采纳前展示所依据的版本；依据变化时要求重看差异；重复点击不能生成重复任务；系统不能静默覆盖另一人的确认
R14	业务字段确认与行动批准分开	P1	“采纳建议”不自动确认所有事实；修订 CRM 字段走 CRM 原有候选确认权限和历史机制
R15	受控创建任务并呈现真实进展	P1	卡片分别显示待提交、已受理、任务已创建、执行中、已执行、失败或待核对；超时不直接视为失败或成功
R16	结果回流可关联到具体建议和事项	P1	保留建议、决定、命令、任务、回执标识；触达、客户响应、事项推进分别记录；取消任务不代表取消客户承诺

5.3 承诺、学习与治理

编号	产品需求	阶段	具体规则
R17	最小承诺账本保存内容与履约证据	P1	记录谁对谁承诺、内容、截止时间及时区、前提、来源、确认人；顾问回电记录只能证明回电行为，不能证明其他交付约定
R18	延期、变更与违约历史不可被抹除	P1/P2	新承诺关联旧承诺；超过原到期时间的事实保留；取消须有授权理由及通知/客户确认情况；模糊时间待确认
R19	售后保持交付、沟通、承诺三线独立	P2	配件到货或维修完成由业务源更新；安抚是否完成不作为维修/交付门问；每次修订保留来源与时间
R20	建立人工基线与失败样本学习	P0	对比原有建议、人工处理和新卡片；区分标注分歧、证据不足、角色错、身份错、阻碍错、建议越界等；不拿模型自评当金标
R21	候选评测、晋升与运行版本可追溯	P0/P1	每次实验记录输入集合、代码、模型、提示、规则和评估版本；上线前有审批与回滚目标；被接受的草稿不自动进入训练集
R22	权限、隐私和数据有效期贯穿链路	P0/P1	研究域与业务域隔离；组织/门店/客户范围由服务端确定；越权无内容；证据授权撤销时隐藏内容并使相关建议不可执行
R23	可观测、可恢复、可解释降级	P0/P1	模型不可用仍可看有权访问的有效事实；提示未生成建议；重启恢复待处理命令；日志不存完整对话或联系方式
R24	各阶段有实际证据才能宣告完成	全阶段	分开报告代码、演示、离线质量、真实使用和业务效果；数据量不足时报告不足及下一步取数，不能降低定义凑验收

6. 核心使用流程

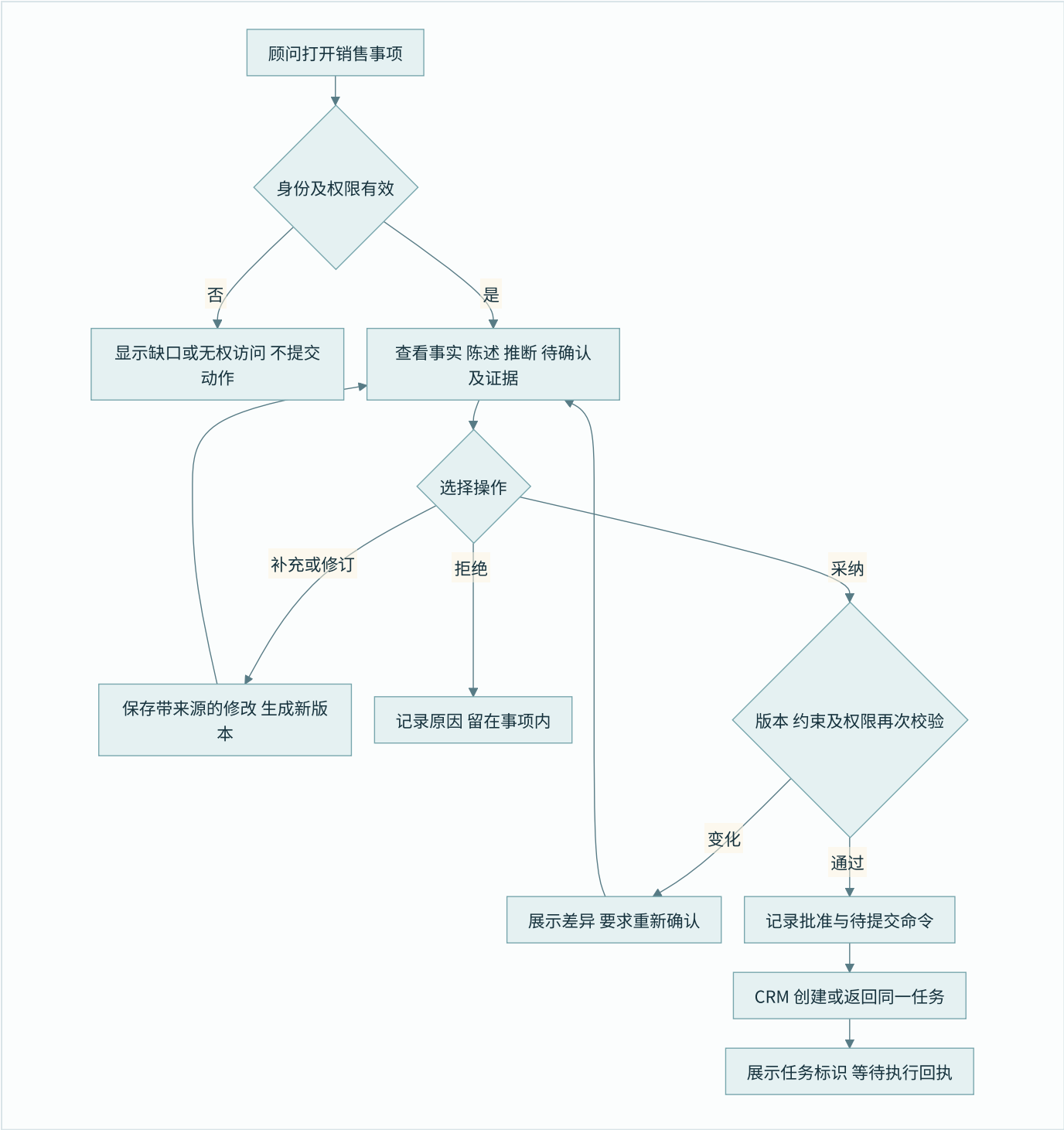
F1：离线销售 A 回放

研究员校验 PR7 → 默认提取主链文本 → 召回候选并抽取负例 → 定位原文与时间片段 → 生成理解卡草稿 → 业务复核员独立判断 → 比较原有建议和新卡片 → 记录错误与版本。

只有“明确已试驾 + 存在未决阻碍或下一步需求”的样本进入严格销售 A 集合；其余分为近邻场景、无法判断、非目标。顾问角色不明、对话顺序异常或时间定位不可靠，必须显式标记，不能靠模型补全。未能识别稳定跨会话身份时，以单会话临时事项评估，不合成“客户长期画像”。

P0 的证据按钮打开研究文本对应段落；如果关联不到原始录音，显示“仅有文本证据”。禁止使用演示音频替代语料录音。

F2：顾问打开事项并确认下一步



“修改”不能仅修改可见文案而沿用旧批准。影响动作参数、客户、事项、期限或证据的修改，生成新提案版本并重新校验。拒绝不自动影响客户主字段。缺失关键业务事实时可以保存草稿、发起人工核实，不能承诺具体价格或交付日期。

F3：执行、超时与结果回流

任务在 CRM 内执行。大脑只读取授权范围内的任务状态和结果证据。提交超时后，界面显示“任务创建结果待核对”，自动按同一命令标识查询；顾问重试沿用该标识，不再次制造业务任务。

任务完成、消息送达、客户回复、形成下一步约定和订单状态变化分别记录。渠道显示“送达”不推断客户认可；经理强制关单只记录行政关闭及原因，不算客户事项推进或承诺兑现。迟到回执补入历史，不能使已更正的较新业务状态倒退。

F4：新增承诺、改期与履约

从对话抽取“明天下午回电”形成承诺候选 → 顾问确认本地日期、时区、对象及内容 → 建立有效承诺 → CRM 创建执行任务 → 到期核查与该承诺内容匹配的证据 → 记录兑现、逾期、争议或待确认。

“尽快”“等有消息”不能自动变成确定截止时间。改期追加变更记录并说明是否已告知客户；旧计划到期和违约事实保留。重新约定不消除原失约；客户未回复时不能显示“客户已同意改期”。

关联承诺的任务页要分开两个入口：“调整任务计划”只改 CRM 内部任务时间，成功提示明确“客户承诺未变”；“查看/变更承诺”进入对应事项的承诺表单，记录新时间、时区、依据和客户告知/确认情况。页面分别展示任务计划与客户承诺的时间、版本及结果；不能用一个“已改期”提示表示两者都更新。如果任务新期限晚于有效承诺期限，提示履约风险，不自动改承诺或阻塞实际业务交付。

F5：解绑、撤权与删除

发现误关联或收到撤权后，先阻止新动作并隐藏无权证据，再撤销关联并重建受影响理解；未执行命令停用，已创建任务提出取消/修正请求，已发生的外部动作保留审计记录。删除证据内容后保留不含原文、个人标识的必要审计引用与删除标记，派生缓存及检索索引同时失效。具体保留期限由企业政策决定，不在本稿虚构法定时长。

7. 顾问台信息架构与交互规范

7.1 主要页面

页面	核心内容	主要操作
事项列表	当前阶段、阻碍、责任顾问、下一步、到期承诺、数据缺口；默认按本人待办筛选	打开事项，按状态/负责人过滤；经理只看授权范围
事项详情	四栏理解卡、证据抽屉、已做动作、待确认、建议、任务进展、承诺历史	采纳、修改、拒绝、补充、查看来源和版本
复核与失败样本页	脱敏样本、独立评价、分歧、错误类型及版本	复核、归因、纳入候选评测；无真实触达按钮
管理观察页	事项阻碍分布、建议采用、任务执行、结果可观测覆盖、未兑现承诺	分析卡点；不以建议采纳率单独给顾问排名

一期优先事项详情与复核页，不重做全量首页、客户标签中心或独立大脑门户。生产界面沿用现有 CRM 交互入口；P0 允许离线生成只读卡片及复核表单，不形成第二个业务作业系统。

7.2 事项卡结构

事项：试驾后下一步

客户绑定：待确认 / 已确认

最后更新：时间

理解版本：版本号

业务事实

客户陈述

模型推断

待确认

试驾完成记录

“回去商量”

可能需要共同决策

与谁商量、还缺什么

来源与时间

文本片段入口

推断理由与依据

顾问确认入口

已做过：试驾、介绍配置

客户反应：仅展示有证据的内容

建议：先确认共同决策所需信息，再约定资料与下次联系时间

前提：联系人、联系许可及时间已核实

边界：不能擅自承诺优惠或交车日期

[采纳并创建任务][修改后再确认][拒绝][补充信息]

任务：待提交 / 已创建 / 执行中 / 已执行 / 待核对

承诺：原计划、变更、逾期、兑现证据（保留历史）

此示例完全虚构，仅说明交互。四栏必须使用文字标题区分，不能只靠颜色。证据抽屉支持键盘操作、返回原位
置，并明确“客户陈述”与“业务事实”的差别；窄屏按栏目顺序纵向排布。

7.3 必须覆盖的界面状态

状态	页面行为	可进行的操作
无候选	显示未发现满足条件的事项及人工录入入口	看记录、手动创建待核实事项
身份未绑定	展示研究或本次会话范围，不暴露其他客户历史	提交绑定确认；不创建真实客户任务
证据缺失 / 无权	不显示原文和精确推断；说明缺口	补充授权证据、重新生成
来源过期 / 相互冲突	标注来源与时间，关键承诺按钮停用	请求业务核实，不自动选“最新一句话”
生成中 / 模型失败	保留可读事实；显示进度或失败原因	稍后重试、人工处理；无自动编造建议
内容已更新	并排或逐项显示影响确认的差异	重新确认；旧批准不复用
提交中 / 结果未知	显示命令标识与核对状态	查询、同键重试；阻止重复创建
已关闭 / 已取消	保留历史和关闭依据	经权限检查重新开事项或创建新事项

8. 权限与数据责任

确认是正式产品能力。顾问只能处理其组织与客户范围；经理的管理动作由真实身份和角色校验，不接受前端自
报“经理批准”。研究复核账号不能访问真实客户，不具有业务命令权限。服务账号的范围、用途、到期时间和
可用命令必须限定。

数据或操作	权威拥有者	大脑的处理方式
正式转写及时间定位	VP 或原始交互系统	保存引用和许可范围，必要时受控缓存，不覆盖原稿
客户业务字段、商机、联系许可	CRM 或企业指定主系统	读带版本的事实；字段确认通过原系统命令
订单、付款、维修、配件、交付	各业务主系统	读事实及有效时间，冲突时展示来源，不凭对话改写
身份关联决定	大脑的关联记录，原系统实体标识仍归原系统	记录操作者、理由和版本；不新造竞争性客户主档
事项、理解版本、行动提案与决定	客户经营大脑	唯一维护其认知与决策历史
新建承诺及变更历史	客户经营大脑	CRM 作为录入与展示入口；其他系统已有承诺仅引用，不复制权威
任务、执行记录、渠道原始回执	CRM / 执行系统	大脑读取回执，形成有来源的事项结果判断
人工标注和评测报告	研究评测体系	与业务事实、模型草稿分开，发布走既有候选晋升流程

如果实际试点已有权威承诺系统，接入时将其承诺作为外部权威引用；不迁走也不建立另一份可编辑副本。新建承诺默认由大脑拥有是技术推荐，实施前需核对这一事实。

9. 非功能要求与验收证据

9.1 性能、恢复与成本

以下是工程验收目标，不是当前实测结果：P1 单租户 50 个并发读取下，已生成事项卡读取的 p95（95% 请求耗时分位）不超过 2 秒；生成请求 1 秒内返回任务标识，30 秒进入超时提示但允许后台查询，不能因超时重复触发业务动作。数据集、硬件和网络条件随测试报告保存。

业务批准及其待提交命令须持久化后才能返回接受；进程重启不得丢失已接受命令。模型不可用时支持只读事实和人工任务流程。性能不达标时先缩小试点并发或优化瓶颈，不以放宽权限和证据检查换速度。

每次生成记录模型调用数、输入输出量、耗时及可取得的费用；未获得预算时不自动批量调用收费模型。以每个完成复核的事项成本和顾问耗时评价，而非以生成卡片数量评价。

9.2 验收场景

编号	给定条件与动作	必须观察到的结果	覆盖需求
AE01	校验并重复回放同一 PR7 清单	输入哈希、排除项与输出关联可复核；无生产写入、无默认模型外发	R01、R20、R21

编号	给定条件与动作	必须观察到的结果	覆盖需求
AE02	一句客户“已付款”与缺失付款记录	卡片列为客户陈述，业务事实仍未知，不发“已到账”结论	R02、R03、R06
AE03	片段缺失、角色不明、无音频	卡片标注限制；原文可定位的才显示；不播放演示音频补位	R02、R03、R09
AE04	同名不同客户或同人不同商机	不自动合并；人工绑定有版本和审计，解绑重建相关理解	R04、R05、R22
AE05	业务源过期或来源冲突	显示待核实并阻止相关具体承诺；不编造价格、库存、交期	R06、R08、R10
AE06	顾问修改、拒绝或采纳草稿	保留原稿与变更理由；采纳不顺带确认全部业务字段	R07、R12、R14
AE07	两人并发采纳，或批准后依据变化	旧版本得到冲突/失效响应；一个有效决定只产生一个业务任务	R11、R13、R15
AE08	越权、撤权、前端伪造批准者	不返回客户内容，不创建任务；记录不含敏感内容的拒绝审计	R11、R22
AE09	创建任务超时、重复请求、进程重启	通过原命令查询或重放得到同一任务；不丢失已接受命令	R13、R15、R23
AE10	回执重复、乱序、来源无法核验	不重复计算结果；未知来源隔离；行政关单不算兑现	R16、R23、R24
AE11	先调整内部任务时间，再对超期承诺重新约定	任务与承诺时间、版本及提示独立；历史违约仍可见，只有内容匹配的证据才支持兑现	R17、R18
AE12	维修已完成但安抚未结束	交付状态正常推进；沟通和承诺分别显示	R19
AE13	对照人工与模型建议，出现分歧	保存盲评、分歧与裁定依据；模型输出不进入人工金标	R09、R10、R20
AE14	未通过评测或撤销上线版本	候选不能成为运行默认；旧理解标注版本，必要时失效重建	R21、R23
AE15	删除/撤销证据或解绑后，再恢复之前的备份	正常状态及恢复后，旧原文、缓存、索引和关联均不能复活；受影响提案失效，历史动作保留受控审计	R02、R11、R22
AE16	没有真实客户结果或样本太少	报告“未观测/不足”，展示分母与缺失原因，不宣称转化提升	R16、R20、R24

10. 评测与业务效果口径

P0 先建立人工可重复判断的基线，不先写一个没有实测依据的“准确率达到 95%”。下面的比例均报告分子、分母、样本抽取方法、时间窗和不确定性。

指标	计算方式	可证明范围
目标事项识别	人工判定的正确入选数 / 被复核候选数；另对抽样非候选记录漏召回	召回质量；只看候选不能估计整体召回率
主要阻碍判断	经双人复核及分歧裁定后正确的阻碍判断数 / 可判定目标事项数	离线理解质量；无法判定样本单列

指标	计算方式	可证明范围
证据支持	有可定位且实际支持该说法的关键结论数 / 全部关键结论数	引用有效性；有链接不等于语义支持
建议可执行性	顾问按统一量表判定可执行的建议数 / 被评价建议数	人工评价；不是执行或成交效果
顾问耗时	相同条件下从打开事项到形成有效下一步的时长分布	工作效率；随机分配或交叉对照，报告样本熟悉效应
采纳与执行	采纳决定数 / 展示机会数；实际执行数 / 已创建且到观察期的任务数	建议使用与动作落地分开
事项推进	有业务证据的阶段进展数 / 进入观察期且可观测的事项数	观察关联；没有对照不能宣称因果提升
承诺兑现	按原约定内容和期限有证据兑现数 / 已到期且可判定承诺数	另列逾期、变更、取消、争议及未观测，禁止靠排除缺失美化

P0 在 369 份默认 ASR 中做可重复初筛。业务复核目标暂定 30–50 份候选与负例混合样本；若严格场景 A 不足，不凑满、不混入售后，改为全部复核并报告缺口。先制定判断标准，再划分开发集和封存评估集；可识别同会话或同研究对象的样本必须留在同一侧，无法排除重复关联时不宣称独立泛化效果。

至少两名具备销售经验的复核人对封存集独立判断，分歧由指定业务负责人裁定。若人手不足可完成探索报告，但不能称为稳定评测基线。卡片展示顺序和方案名称在盲评时随机化；保存模型版本和每个实验的样本集合，避免边调边改验收集。

进入 P1 的硬门禁是：相关 AE 场景通过，无未解决的越权、重复副作用、伪证据和历史覆盖缺陷；业务负责人审阅实际基线与错误样本后批准限定范围试点。质量与耗时目标据该基线设定，不能用占位百分比冒充已批准标准。

11. 两周离线实施安排

下表从开工日计算 10 个工作日，假设有 1 名产品/业务负责人、1 名数据或后端工程师、VP 维护者按需支持，以及 2 名业务复核人可预约。它不包含真实 CRM 接入、客户授权、上线审批和效果观察周期。

时间	工作	可评审成果	负责人角色
第 1–2 天	固定输入清单、校验 corpus、核对 ASR 形态和研究域标识；定义目标及负例	数据卡、排除清单、复核规则、来源定位样例	数据工程 + 业务
第 3–4 天	实现 M1 召回、M2 证据打包；人工检查误召回与漏召回	候选集合、证据定位、失败类型	数据工程 + VP
第 5–6 天	实现 M3 理解卡；复用既有分析草稿并补充证据和未知项	可阅读卡片、规则基线、虚构交互样例	后端 + 产品
第 7–8 天	M4 人工与现有建议对照，复核面板采纳/修改/拒绝	封存集评价、操作耗时、分歧记录	业务复核 + 产品

时间	工作	可评审成果	负责人角色
第 9-10 天	M5 失败样本整理、回放复现、 评审 P1 条件	基线报告、可重跑命令、缺口 和试点进入建议	全组

本周第一件事是固定研究输入并生成数据卡，现有命令如下。在隔离开发环境执行；这里只生成本地研究文件，不运行生产链路：

```
python scripts/cloud_analysis_corpus.py verify
mkdir -p artifacts/customer_brain/offline/input
python scripts/cloud_analysis_corpus.py extract --category own_asr >
artifacts/customer_brain/offline/input/own_asr.jsonl
python scripts/cloud_analysis_corpus.py extract --category customer_advisor_snapshots >
artifacts/customer_brain/offline/input/customer_snapshots.jsonl
```

后续新回放命令及模块路径见架构方案的 U1-U5。不得把尚未创建的脚本写成已经可运行的命令；研究输入与输出遵守仓库忽略和保密规则，不提交提取出来的原文。

12. 风险、假设与负责人的拍板项

12.1 假设与主要风险

编号	假设或风险	处理与影响
A01	一期按销售 A 编写，但与 K-013 的范围冲突未获业务裁决	不阻塞离线研究准备；锁定试点投入前处理 D1
A02	可安排业务复核，但尚未证明复核时间可用	无复核只能交探索结果；不得称为金标或质量验收
A03	真实身份、跟进和成交回执尚未接通	P0 先行；P1 不能用假 ID 和演示表替代
A04	已有 CRM / DMS 数据权威和字段负责人可以明确	接入字段逐项登记；没有权威源的字段保持未知
A05	同仓有利于目前协作，团队与部署规模未证明需要拆仓	先验证模块独立和依赖约束；后续按独立交付需要拆分
A06	业务值可能不来自更多模型调用	先比较人工与现有规则；证据/流程改进优先于模型规模

权限不完整、身份误绑、证据过期、把回执当效果、历史承诺被覆盖是上线阻断风险；样本不足、模型质量波动和顾问不采纳是需通过试点验证的产品风险。两类风险不能混在一个“模型准确率”指标里。

12.2 需要负责人拍板的三项

编号	推荐决定	为什么需要负责人决定	未决定时的边界
D1	一期锁定销售 A；售后 B 保留后续，K-013 另行裁定	涉及业务资源及范围，技术不能替业务选择	可完成通用证据和离线准备，不宣称试点范围获批
D2	指定试点门店/顾问、数据责任人、两名复核人，并优先提供客户 ID 与跟进/成交回执	需要真实组织资源与数据权限	不接真实客户，不计算真实经营效果
D3	批准“离线基线→受控人工试点”的进入方式，并指定结果判定与上线签字人	需要业务对错误样本、资源和接受条件承担责任	保持离线；自动外呼仍禁止，未来须另有书面批准

同仓模块划分、接口版本、幂等、存储和发布策略是架构建议，已在配套文档给出明确默认，不把普通工程选型转交负责人投票。

13. 文档关系与引用

- 架构设计与实施计划：系统边界、数据合同、可靠命令、模块路径、迁移、验收及实施单元。
- HANDOFF、PROJECT、当前进度：仓库当前实现背景，目标方案不自动更改其事实状态。
- 语料说明、研究实验说明：研究数据与提取限制。
- 现有客户智能引擎草案、现有客户主视图决策：历史设计及兼容约束。本文的独立模块推荐不意味着旧接口已经迁移。
- 客户经营大脑知识库当前状态：公网可能滞后，产品状态以内部 `CURRENT_STATE.md` 为准。本稿没有将其改写或发布。

完整产品以本文的 R01–R24 为需求依据。后续阶段调整必须说明影响哪些需求、验收证据及数据权威；不能仅以新目录、页面或模型替换宣布完成。

客户经营大脑架构设计与实施计划

本文是目标架构评审稿，配套产品需求文档。代码基线为 2026-09-21 核查的 MP3 `main @ e37d400`。本文中的新目录、接口、数据库表和命令均为拟建设内容；没有据此修改生产代码、正式转写或运行配置。

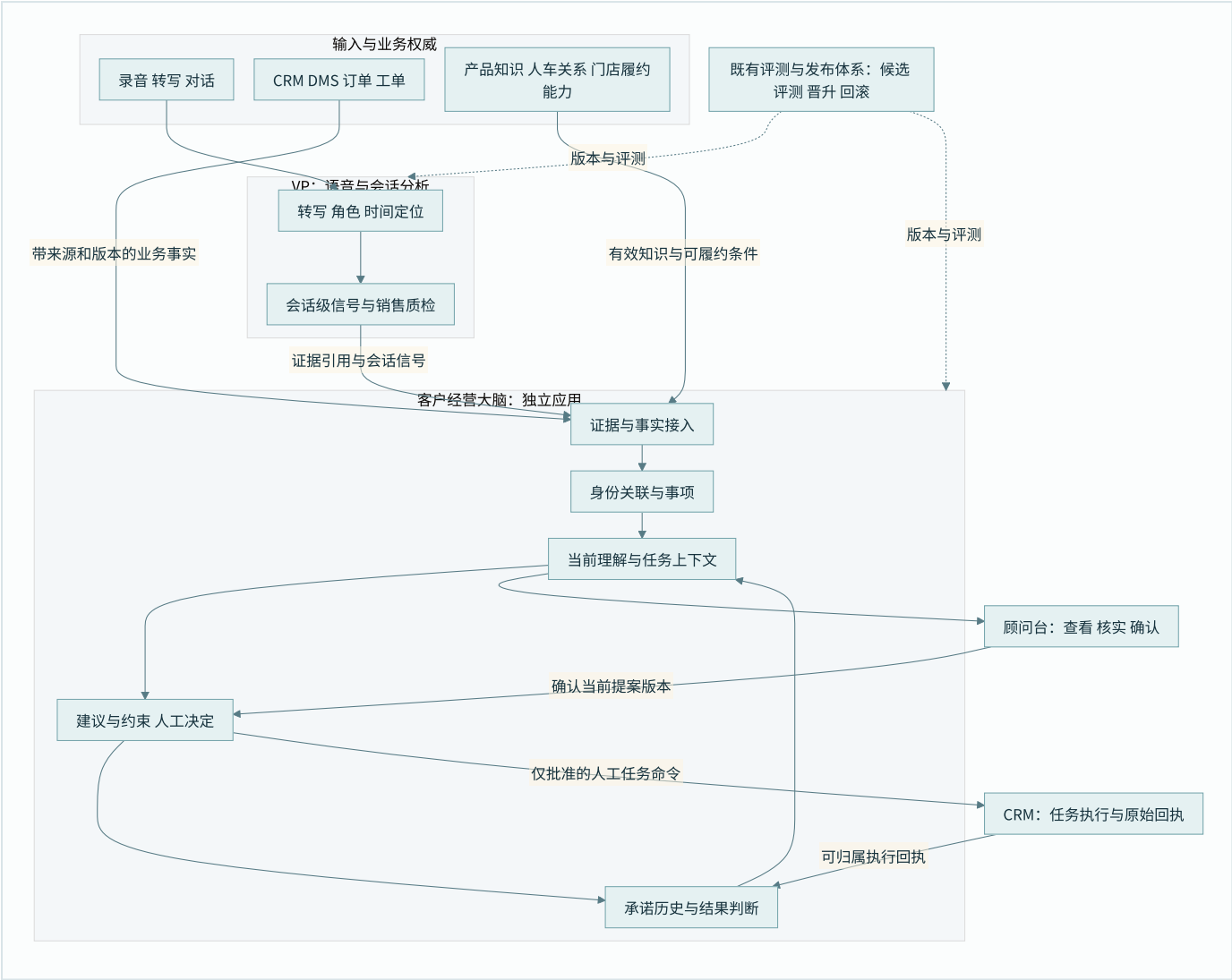
需求以 PRD 的 R01-R24 为准，验收以 AE01-AE16 为准；本文件定义技术决定 KTD01-KTD10、实施单元 U1-U8 及其交付证据。PRD 的 D1-D3 是业务待决事项，不由技术设计代批。

1. 架构结论

选择同仓、独立模块、显式合同、各自数据权威。在 `src/voice_platform/` 和 `src/crm/` 旁新增 `src/customer_brain/`。另建很小的 `src/customer_contracts/`，只放系统间交换对象。离线阶段用文件运行；进入真实试点后，大脑作为一个可独立启动的应用，内部保持模块化单体，不按六项能力拆成六个服务。

音频和对话经过 VP 变成可定位证据及会话信号；CRM、订单、工单等通过各自适配器提供业务事实。大脑把证据、事实、知识及履约条件关联到具体事项，生成理解和建议；顾问确认形成批准记录，CRM 创建任务并返回执行证据，大脑据此更新事项和承诺历史。两者以版本化接口配合，避免循环调用和跨库写入。

1.1 总体架构图



图中 CRM 输入与执行端是同一业务系统的两种责任，不是两份 CRM。业务事实可以直接进入大脑；没有必要把订单状态伪装成对话，再调用销售分析。

1.2 关键技术决定

编号	决定	选择依据与代价
KTD01	同仓新增独立大脑应用，暂不拆仓	可复用协作与测试；需显式依赖检查，目录分开本身不足以隔离
KTD02	VP 保留会话级语义分析；长期理解与行动归大脑	避免大脑重做 ASR 和逐句提取，也避免 VP 承担全部客户经营；存量销售建议先兼容
KTD03	新交换合同放中性小包，存量 VP 合同继续兼容	新大脑不依赖 VP 私有结构；需版本适配与契约测试，不做全仓 schema（数据结构）重写
KTD04	CRM 拥有业务字段/任务，大脑拥有新事项/理解/承诺历史	单一写入责任明确；跨系统必须可靠关联，不能依赖数据库事务跨界
KTD05	P0 不运行服务；P1 大脑使用 PostgreSQL（关系数据库）和持久化投递表	离线保持轻量，真实试点承受并发与重启；增加一套数据库部署，不强迫迁移 CRM 数据库

编号	决定	选择依据与代价
KTD06	先支持人工任务命令，双端持久化去重与内容绑定	不把超时当失败；存在短暂同步延迟，需对账和明确“结果待核对”
KTD07	理解、提案、批准和执行结果分别有版本与状态	可解释修订、并发与撤销；对象比单个建议 JSON 多，但避免状态混淆
KTD08	新承诺事件追加，状态由历史与证据计算	旧违约不被改期覆盖；取消、争议和迟到证据需专门规则
KTD09	复用既有候选晋升原则及评测产物，不复制控制平台	大脑运行不导入 VP 的研究管理模块；发布工具通过目标组件适配
KTD10	写入口先做真实授权、对象关联和当前约束校验	现有 CRM 演示路径不足以成为可信命令入口；先补边界再接真实任务

独立仓库留到团队权限、发布节奏或交付需要明确分离时；独立微服务留到有可测量的容量或故障隔离要求时。二者都不是当前产品清晰性的前置条件。

2. 现状与复用判断

2.1 VP 架构评价

当前 VP 的 `speech → scenes → app` 分层总体合理，统一输入、规范转写、场景结果和运行/研究边界是可保留的基础。其现状更接近语音分析产品与销售场景流水线，尚不能视为一个完成跨源客户认知和行动闭环的系统。

代码证据	判断	本方案处理
<code>speech/pipeline.py</code> ; <code>contracts/init.py</code> 的 <code>TranscriptTurn</code> / <code>TranscriptBundle</code>	已有 ASR、融合、标准转写和段落时间/角色字段	复用；向外提供原版本证据定位，不重新跑转写补研究数据
<code>scenes/sales/scenes.py</code> 的 <code>SalesScene.analyze</code> ； <code>next_action.py</code>	销售质检及阶段分析已成链，下一步有规则基线；默认分析可能调用模型	保留现有销售产品；P0 显式选择离线路径，不默认启动全链
<code>audio_jobs.py</code> 的 <code>AudioJobService</code>	统一 <code>audio/transcript/dialogue</code> ；此入口以进程内字典保存任务	可用作 VP 编排；不拿它保存新大脑的业务批准和可靠命令
<code>runtime.py</code> 与 <code>runtime-vs-harness</code>	有运行 API 白名单与研究管理分离方向	继续保留；大脑另设自己的薄 API，不扩张 VP 全量入口承担业务闭环
<code>runtime_ingestion.py</code>	客户智能接入会把输入适配后进入 <code>SalesScene</code>	不扩成所有业务事实的总入口；新接入按证据类型分流
<code>customer_master_view_builder.py</code> ； <code>signal_candidate_builder.py</code>	当前主视图为自采派生读模型；部分候选缺少逐项证据且使用固定置信度	保留兼容读面；不能作为跨源身份真相或已验证置信度
<code>customer_master_view_feedback.py</code>	反馈追加审计，返回 <code>state_update_applied=False</code>	不宣称反馈已更新客户理解；新大脑实现自己的明确状态变更
<code>gateway.py</code> ； <code>action_feedback_builder.py</code>	网关接受动作不等于 CRM 任务；后续接触代理不等于承诺兑现	不沿用其返回值作为真实执行或履约证据

还有局部依赖方向需要后续整理：`speech/pipeline.py` 引用 `scenes.common` 的对话与角色工具；`audio_session_segmenter.py` 引用销售有效性规则；`speaker_privacy_runtime.py` 引用应用层隐私审计。不是因此推翻主链，而是在有调用和测试清单后将通用逻辑下沉、业务判断外置。本期新增大脑不继续扩大这些反向依赖。

`scenes/sales` 中的质检、顾问培训指标可以长期留在 VP。单次对话的顾虑、意向等属于会话信号；跨会话阻碍判断、业务阶段、承诺和执行建议属于大脑。旧 `next_action` 先作为基线和兼容字段，待消费者迁移后再停用其作为经营动作权威的用途，不立即删除。

2.2 CRM 的可复用能力与接入前缺口

代码与符号	当前事实	正式接入要求
<code>domain/models.py</code> ; <code>domain/models_prd.py</code> 的 <code>TaskRow</code> / <code>StrategyDecision</code>	有客户、商机、任务、候选；任务缺少脑事项/决定/命令及版本关联	复用任务对象，增加独立命令关联表与必要任务版本，不复制脑账本
<code>api/deps.py</code> 的 <code>get_session</code>	请求结束提交，同请求内共享事务	在同一 CRM 事务内完成命令去重结果、任务及回执待投递记录
<code>domain/memory.py</code> 的 <code>merge_candidate</code> / <code>accept_candidate</code>	字段有历史；候选 <code>accepted</code> 也可能自动进入 <code>inferred</code> ，不一定有人确认	沿用字段责任；新脑批准须有独立决定记录，不能映射一个状态名就当人工金标
<code>prd/strategies.py</code> 的 <code>_adopt_one</code> / <code>_open_same_type</code>	去重围绕客户、策略键、固定版本，可能复用另一商机或已关闭任务	新命令按租户、事项、动作版本去重，不直接调用旧路由承担正式命令语义
<code>api/routes_prd.py</code> 的 <code>candidate</code> / <code>task_action</code> ； <code>prd/authz.py</code>	有读取范围检查，但候选确认、写权限及客户端身份/批准者处理存在缺口	在新命令服务统一验证实际身份、写权限、客户/商机/任务关联；不信任前端批准者字符串
<code>prd/actions.py</code> 的 <code>complete_task</code> / <code>create_followup</code> ； <code>prd/views.py</code> 的 <code>completion_state</code>	完成条件可能接受历史联系或行政关闭，未严格绑定当前承诺	任务关闭与履约判断分开；完成证据绑定任务、事项、有效时间和承诺版本
<code>prd/receipts.py</code> ； <code>prd/campaigns.py</code>	有回执去重及渠道状态区分； <code>verified=True</code> 不证明渠道身份已鉴真	正式回执验证来源、租户、请求关联、事件命名空间和内容摘要
<code>prd/recordings.py</code>	录音接口存在生成演示音频的实现	新证据入口必须接真实来源；P0 只呈现研究文本，不以演示音频兜底
<code>tests/crm/test_no_voice_platform_import.py</code>	已有 CRM 不引用 VP 的隔离测试	保持该约束；新跨系统 DTO（数据交换对象）来自中性包

以上是静态代码核查，不等于对部署安全、容量或业务效果作出认证。计划阶段未启动生产服务或修改这些实现。

2.3 旧设计与本方案的兼容边界

现有客户智能灵魂模块设计强调不再造逐句理解流水线，这一原则保留；本方案通过消费 VP 会话信号实现复用，不要求大脑继续位于 VP 包内。

现有客户主视图结构决策与消费者清单要求保留 typed v1（有类型的第一版合同）。新中性合同不是把 `customer_master_view_v1` 原地换成另一套字段。旧读面继续运行，迁移须更新消费者清单并验证字段、未知值和版本兼容。历史文档中的“唯一客户真相”在本方案限定为派生理解读面，不能解释成覆盖 CRM/DMS 原始业务事实。

3. 模块与依赖设计

3.1 建议目录

下面 `customer_brain`、`customer_contracts` 和标注新增的适配器尚不存在。目录表示责任，P0 只创建 U1-U5 必须的部分；不一次性建立所有空服务。

```
src/
  voice_platform/                                # 现有语音与会话分析产品
    app/connectors/brain_export.py               # 拟新增：存量合同 → 中性证据/信号
  customer_contracts/                             # 拟新增：版本化交换合同，无业务/数据库逻辑
    evidence.py                                   # EvidenceEnvelopeV1 / BusinessFactV1
    context.py                                    # TaskContextV1 / ActionProposalV1
    commands.py                                  # TaskCommandV1 / ExecutionReceiptV1
  customer_brain/
    domain/                                       # 事项、身份关联、理解、承诺、决定与规则
    application/                                 # 接入、上下文构建、批准、结果归属
    ports/                                       # 证据/事实/知识/任务/持久化接口
    adapters/                                    # PR7、HTTP、SQL、知识源；无跨库写入
    scenarios/sales_a/                           # 召回、事项规则、卡片、评测口径
    api/                                         # 上下文/确认/接入；业务域鉴权
    cli/                                         # 离线回放及评测入口
  crm/                                           # 现有客户字段、任务及顾问界面
    integration/brain_commands.py                # 拟新增：可信命令接入和去重
    integration/brain_receipts.py               # 拟新增：结果回传
    web/                                         # 沿用现有页面体系嵌入事项卡
  tests/
    customer_brain/                             # 拟新增：规则、合同、权限、回放与恢复验证
    crm/                                         # 保留隔离测试，补命令/回执边界验证
```

3.2 依赖允许表

模块	可以依赖	禁止依赖
<code>customer_contracts</code>	标准库、仓库已用 Pydantic（类型校验）	VP、CRM、大脑运行对象、数据库、模型 SDK
<code>customer_brain.domain</code>	纯领域类型和标准库	HTTP、数据库、VP/CRM、前端、发布系统
<code>customer_brain.application</code>	domain、ports、中性合同	VP/CRM 私有模块、研究管理入口、直接业务库连接

模块	可以依赖	禁止依赖
<code>customer_brain.adapters</code>	ports、中性合同、所需客户端/存储库	CRM 表模型、VP 私有应用服务；PR7 文件适配器不启动 VP
VP 导出适配器	自己的正式合同、中性合同	大脑内部规则及存储
CRM 接入适配器	CRM 自己的领域服务、中性合同	VP 包、大脑数据库或领域实现
应用启动层	本应用的实现、配置及依赖装配	以共享单例隐式控制另一应用生命周期

运行调用通过合同和适配器；同仓不意味着跨包导入方便就可以直接调用。当前 `pyproject.toml` 是一个分包，自动发现 `src` 下的包；因此“目录独立”还不等于“可独立安装”。P0 做依赖检查和独立 CLI，P1 给大脑增加独立入口、依赖组及构建验收，不要求迁移所有 VP/CRM 包管理。

验证边界需覆盖绝对及相对导入、直接及间接应用依赖。现有运行边界测试对部分 AST（语法树）导入模式的检查不能证明完整隔离；新测试按上述明确规则补齐，不以文件名存在作为证据。

4. 数据权威与存储模型

4.1 持久化选择

P0 输入为只读 PR7 对象，输出为隔离研究目录中的 JSONL（逐行 JSON）、卡片和人工评价；用清单与内容哈希固定实验，不启动数据库和任务执行服务。敏感原文不进入版本库。

P1 新大脑采用 PostgreSQL 保存事项、理解、批准、承诺历史和待投递命令。CRM 保留现有数据库与 ORM（对象关系映射）实现，新建其自己的命令接收、关联和回执投递记录；不让大脑写 CRM 表。SQLite（本地轻量数据库）可用于局部开发测试，但不能据此宣称真实并发和恢复门禁已通过。

证据原文优先由来源系统保管，大脑存授权引用和必要摘要。确需缓存时放受控对象存储，记录来源版本、内容摘要、权限标签和过期时间；不得把语料上传到公开图表、日志或渲染服务。P0 不因缺少原始音频而新建音频存储工程。

4.2 大脑拥有的数据

对象 / 拟建表	关键字段	约束
<code>identity_link</code>	租户、来源系统/实体 ID、关联域、状态、理由、确认者、版本	研究域与业务域不能互绑；记录关联而非复制客户主档；撤销留历史
<code>evidence_ref</code>	来源对象/版本、轮次或片段、时间、内容摘要、权限范围、可用状态	引用必须精确到可回看的来源；不能用固定置信度替代证据
<code>fact_observation</code>	字段、值/引用、权威源、源版本、生效时间、接收时间、状态	这是源事实的观察记录；不得覆盖来源系统；冲突显式保留
<code>case_record</code> / <code>case_event</code>	事项 ID、客户/商机/车辆引用、场景、目标、状态、修订号	同人多事项；事件追加，当前状态是投影；唯一键含租户

对象 / 拟建表	关键字段	约束
context_revision	事项/版本、事实/陈述/推断/未知、证据集、源版本集、到期时间	不可变版本；头指针可更新；可从输入和规则重建
action_proposal	提案/版本、上下文版本、动作参数、证据、前提、约束、到期时间	内容摘要覆盖所有影响动作的字段；改动必须新版本
human_decision	决定 ID、操作、提案版本/摘要、真实操作者、时间、原因	采纳理解与批准动作分别记录；无服务端身份不得生效
commitment / commitment_event	承诺 ID、版本、内容、责任方/对象、原截止、条件、来源、关联事项	新建承诺唯一账本；变更追加；原截止与历史违约可恢复
command_outbox / receipt_inbox	稳定命令/事件 ID、租户、类型、内容摘要、关联版本、投递/处理状态	同键同内容重放；同键不同内容冲突；单次事务内与领域更新提交
outcome_observation	决定/命令/任务/承诺引用、结果类型、证据、发生/接收时间、评判规则版本	业务结果与模型推断分开；无法归属则待核对，不自动履约

CRM 拟增 `BrainCommandRecord` 记录命令结果，`BrainTaskLink` 记录脑对象与 CRM 任务关系，`BrainReceiptOutbox` 保存待回传事件。除必要任务修订号外，优先新增关联表，避免把整个大脑模型塞进 `TaskRow` 或自由文本日志。

4.3 时间、冲突和删除

各对象分别记录 `occurred_at`（发生时间）、`ingested_at`（接收时间）、`valid_from / valid_until`（业务有效期）与 `source_revision`（来源版本）。时间统一存 UTC，界面按门店时区显示；“明天下午”必须结合原会话时间和时区，经人确认后才成为期限。

乱序到达按来源版本和业务有效时间归属，不能按最后接收时间覆盖事实。同一权威源较旧版本补入历史，当前头不倒退；跨权威源冲突进入待核实。缺少版本或有效期的源采用保守过期规则，不能假装实时。每类源的有效期由接入配置声明，P1 上线前必须填实，不设置一个通用“永久有效”。

删除/撤权使证据不可读并使相关上下文和提案失效；索引、摘要缓存及研究副本按授权策略同步删除。审计保留脱离原文与直接身份信息的必要关联及删除标记。这里的“不可变”指有权保留期间的历史修订方式，不作为拒绝合法删除或保密处理的理由。

5. 交换合同与版本约束

5.1 合同目录

合同	提供方 → 使用方	必需内容
EvidenceEnvelopeV1	VP / 交互适配器 → 大脑	租户、来源对象及版本、会话/片段/轮次、发生时间、证据引用、权限标签、提取器版本

合同	提供方 → 使用方	必需内容
BusinessFactV1	CRM / 业务适配器 → 大脑	对象、字段、值或引用、权威源、源版本、有效时间、撤销标记
ConversationSignalV1	VP → 大脑	单会话候选信号、证据引用、角色可靠性、模型/规则版本；不得宣称已确认客户事实
TaskContextV1	大脑 → 顾问台 / 授权 Agent	事项、目的、接收者范围、当前理解版本、四类信息、约束、有效期；不含执行授权
ActionProposalV1	大脑 → 顾问台	动作内容、目标、前提、证据、风险、确认要求、内容摘要和上下文版本
TaskCommandV1	大脑 → CRM	决定、动作摘要、CRM 对象引用、事项/承诺版本、负责人、期限、完成证据规则、稳定命令 ID
ExecutionReceiptV1	CRM / 执行系统 → 大脑	稳定事件 ID、来源身份、命令/任务/决定、任务版本、结果类型、证据和时间

所有 ID 的解析都受租户和来源命名空间约束。请求体租户只用于一致性校验，实际租户来自服务端认证身份；不同租户相同 `event_id` 不能碰撞。研究 ID 用 `research:` 命名空间且业务接口拒收。

5.2 任务上下文示例

以下完全虚构，字段用于合同说明，非真实客户、非现有 API 响应。正式 JSON Schema（结构校验规范）在 U1 补齐，未知字段策略必须显式设置。

```
{
  "schema_version": "1.0",
  "context_id": "ctx_demo_003",
  "case_id": "case_demo_001",
  "case_revision": 3,
  "purpose": "sales_a_next_step",
  "audience": {"role": "advisor", "scope_ref": "scope_demo"},
  "identity": {"crm_person_ref": null, "binding_state": "unresolved"},
  "business_facts": [],
  "customer_statements": [
    {"text": "表示希望回去商量", "evidence_refs": ["ev_demo_turn_12"]}
  ],
  "inferences": [
    {"text": "可能尚需共同决策信息", "evidence_refs": ["ev_demo_turn_12"], "state": "draft"}
  ],
  "unknowns": ["试驾是否已经完成", "需要与谁商量", "可联系时间"],
  "constraints": ["identity_required_for_task", "no_automatic_contact"],
  "source_revision_set": {"conversation_demo": "v1"},
  "expires_at": "2026-09-22T01:30:00Z",
  "execution_authority": "none"
}
```

该示例身份和试驾事实都未确认，不能自动入选严格销售 A，也不能创建真实任务。用户确认“理解正确”只产生理解确认；要创建任务仍须明确批准对应动作。

5.3 向后兼容

交换合同首版明确 `schema_version`；新增可选字段向后兼容，字段含义改变或必填字段改变升主版本。未知主版本隔离并返回可诊断错误，不能猜测解析后执行。时间、未知、撤销、来源冲突必须是正式状态，禁止用空串或高置信度伪装缺失。

保留已有 `TranscriptBundle`、`SceneAnalysisResult`、`customer_master_view_v1` 的正式出口。VP 导出适配器将已知字段转为中性合同；没有逐项证据的旧信号只能作为“无法逐项核验的草稿”，不能自动升级为已证实理解。迁移对照覆盖无版本、v1、拟新版本、未知版本及关键字段缺失，消费者库存与字段差异记录作为验收材料。

6. API 与可靠命令

6.1 拟建接口

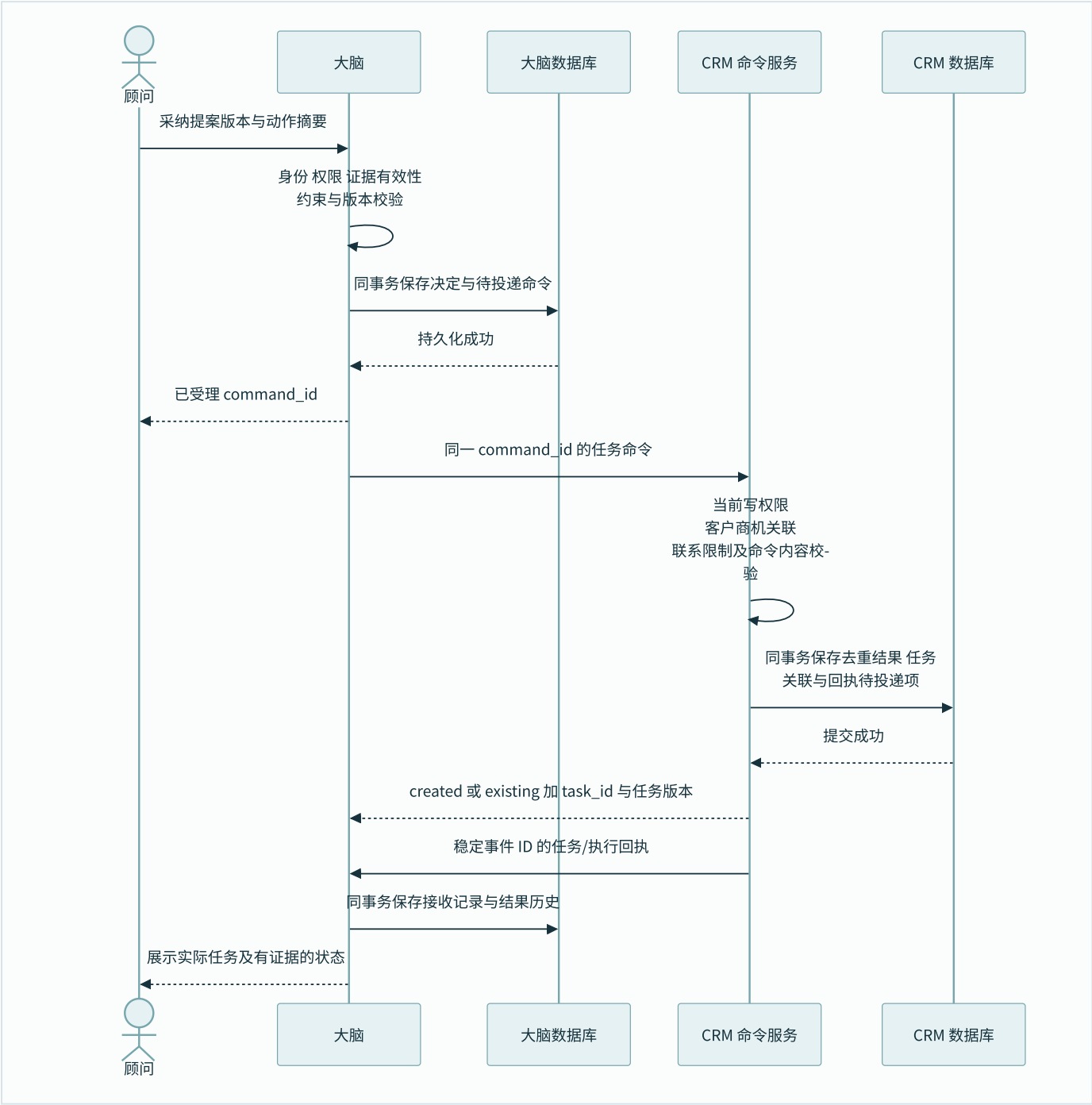
以下均为设计接口，当前代码尚不存在。API（应用接口）中，`/brain/v1/*` 由独立大脑应用提供，`/crm/integration/v1/*` 由 CRM 命令服务提供；业务认证和研究执行分离。

方法及路径	用途	关键语义
<code>POST /brain/v1/evidence-events</code>	接入证据、信号和事实	来源服务认证；相同事件同内容返回原接入记录，不创建重复事项
<code>POST /brain/v1/cases</code>	创建待核实事项	实际身份与范围校验；研究 ID 仅在离线工具使用
<code>GET /brain/v1/cases/{case_id}</code>	读取事项当前头和历史摘要	先鉴权再装配四栏，不将无权字段送到客户端隐藏
<code>POST /brain/v1/cases/{case_id}/context-requests</code>	按目的请求上下文生成	返回生成任务 ID；重试复用请求键，轮询结果，不直接执行动作
<code>GET /brain/v1/context-requests/{request_id}</code>	查询生成结果	明确 pending/ready/failed/expired（待处理/就绪/失败/过期）
<code>POST /brain/v1/proposals/{proposal_id}/decisions</code>	采纳、修改、拒绝	提案/事项预期版本与动作摘要；服务端记录操作者，不信任自报批准人
<code>POST /brain/v1/identity-links/{link_id}/decisions</code>	确认或撤销关联	限有权角色、版本条件；失效受影响上下文并阻止未执行命令
<code>POST /brain/v1/commitments/{id}/events</code>	确认、变更、取消、履约裁定	预期版本及依据，追加事件；无旧内容覆盖接口

方法及路径	用途	关键语义
GET /brain/v1/commands/{command_id}	查询任务命令结果	显示受理、投递、任务创建、拒绝或未知，返回实际任务引用
POST /crm/integration/v1/task-commands	接受批准后的人工任务命令	服务身份 + 代表的真实操作者；当前写权限及对象关联检查
GET /crm/integration/v1/task-commands/{id}	查询幂等结果	同命令返回原结果；不要求重复创建任务
GET /crm/integration/v1/task-commands	恢复与对账时反向枚举接受记录	按租户、接受时间及稳定游标分页，返回命令/提案版本、动作摘要、CRM 对象及任务关联；仅限受控对账身份
POST /brain/v1/execution-receipts	接收可归属结果	验证来源与任务/命令关联，去重、乱序处理；不信任裸 success 布尔值

统一错误至少包括：401 未认证、403 无写权限、404 不存在或不可见对象、409 版本/幂等内容冲突、422 合同或关联非法、503 暂不可用。返回稳定错误码、是否可重试及无敏感信息的追踪 ID。对象枚举防护不得依赖前端不展示按钮。

6.2 确认、任务与回执时序



大脑的 202 Accepted（请求已受理）只证明决定和待投递记录持久化，不证明 CRM 已建任务。CRM 返回 `created / existing / rejected`（新建/已有/拒绝）及任务版本；只有明确任务引用才显示“任务已创建”。

6.3 去重、重试与并发

- 1. 命令 ID 在批准事务内生成并永久关联该动作版本。去重键包含租户、命令类型、命令 ID；内容摘要覆盖客户、商机、事项、承诺/提案版本、参数、责任人、期限和完成规则。相同键不同内容返回 409，不能沿用旧结果。

2. 大脑事务内一起提交批准记录与 Outbox（待投递表）；CRM 事务内一起提交 Inbox（命令接收结果）、任务及回执待投递项。消息可至少一次投递，业务副作用通过唯一约束和原结果读取保持幂等，不宣称跨服务恰好一次。
3. 并发插入唯一冲突后回滚到保存点或重开事务，读取已提交原结果；不能让 ORM 错误后失效的事务继续写。脑与 CRM 的唯一键都校验内容摘要，不能先查后写就当并发安全。
4. 超时后先查原命令，再按原 ID 重试；指数退避并有上限，超过投递期限进入待人工核对，保留待处理数据。后台扫描不自动重发已过期或已撤销的动作。
5. 事项和任务采用修订号及条件更新。SQLAlchemy 的 `version_id_col`（版本计数列）只保护相应逐对象刷新路径，批量更新必须显式带版本条件；不能仅增加版本列就宣称所有写入受保护。官方版本计数说明
6. 事务保持短小，模型调用、对象存储读取和远程 HTTP 不放在数据库锁内。必要行级锁按固定顺序获取并处理死锁重试；不得锁住一个客户等待模型。PostgreSQL 锁说明

6.4 确认时效、撤销与真实执行边界

批准绑定提案版本、上下文版本、来源版本集、动作内容摘要和权限主体。发送任务命令前重新核验大脑侧身份关联、依据及批准有效性；CRM 在接收时重新核验本系统当前写权限、客户归属、联系许可及业务限制。仅验证 JWT（签名身份令牌）或只看生成时的权限都不够。

撤权与远端提交存在并发窗口，两个数据库没有原子撤销能力：以 CRM 持久化命令接受记录为任务创建界点。界点前已观测的撤销须拒绝；已经接受的任务收到撤销后标记阻止执行并发起取消/修正。人的实际执行仍必须在 CRM 再查当前许可；不能因过去创建任务而继续触达。P1 命令只创建人工任务，不直接调用外部渠道，借此将同步窗口与客户副作用隔开。

如果以后批准自动动作，需要增加执行时单次授权凭证、消费记录与更严格的撤销语义，另行设计和书面批准，不由本次任务命令接口顺带开启。已发生的真实外部动作不能靠删除任务“回滚”；记录事实并走业务补救。

6.5 回执信任与结果归属

来源服务须经已配置身份认证，回执事件键包含来源、租户和事件 ID；校验其命令、任务和客户关系及负载摘要。企业内部回传使用受限服务身份，外部渠道采用渠道规定的签名/请求验证和重放防护。旧 CRM 普通用户提交的 `verified=True` 不成为可信来源。

结果类型至少区分 `task_created`、`human_action_recorded`、`channel_delivered`、`customer_responded`、`business_progressed`、`commitment_fulfilled`；后两项需对应业务证据或有权人工裁定，不由模型按关键词直升。回执与对象版本不符、存在冲突或无法定位证据时进入待核对队列。相同事件不同内容隔离并告警，不能静默返回成功。

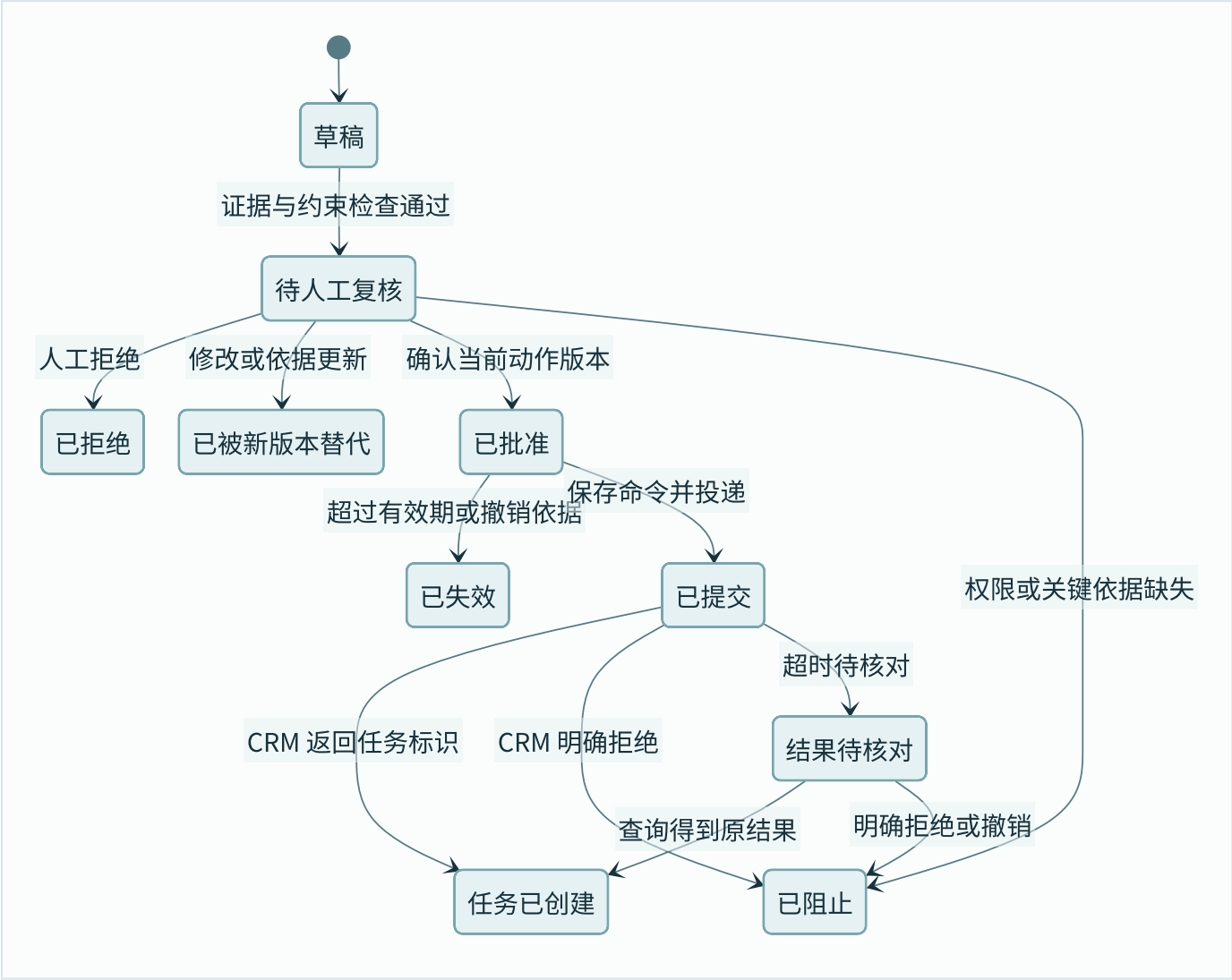
7. 事项、提案与承诺状态

7.1 事项状态与事实来源

事项状态建议为 `draft → active → waiting → resolved / cancelled`（草稿→处理中→等待→已解决/已取消），必要时经有权人员重新打开。每次转换记录触发事件和理由。

`resolved` 表示事项目标具有完成依据；销售商机的成交、流失等正式阶段仍来自 CRM。一个“确认共同决策人”的事项完成，不代表商机已成交。`cancelled` 保留取消者与原因，不从经营统计中静默删除。等待必须有等待对象和复查条件，不能永久挂起而无责任人。

7.2 提案与执行是两个状态序列



图中 Draft 为草稿，AwaitingReview 为待复核，Approved 为已批准，Submitted 为已提交，Unknown 为结果未知；TaskCreated 只到任务创建。其后的执行、客户响应、事项进展、承诺兑现按各自事件序列记录，不能把这张图末端直接标为“成功”。

拒绝和修改是学习反馈，但不会自动更改主数据。动作参数变化产生新提案，旧批准不继承；证据变化使依赖它的提案失效，但不删除曾经据此发生的动作历史。

7.3 承诺账本

承诺首先是候选，确认后才生效。确认记录必须说明内容、责任方、受诺对象、期限及条件。对来源业务系统本来就拥有的合同交付承诺，保存外部引用和版本；大脑只拥有本系统新建的沟通/行动承诺及其历史。

承诺事件包括提出、确认、改期、条件变化、到期、证据提交、兑现裁定、取消、争议与纠正。当前展示状态可以是待确认、有效、逾期、兑现、取消、争议；“曾经逾期”是独立历史事实，不随当前状态变成兑现而消失。

输入	处理规则	不允许的推断
新的承诺时间	追加版本，关联旧计划，记录是否通知/获得客户确认	新截止日期覆盖原截止日期
任务已关闭	保存任务结果，核查完成证据与承诺内容/对象/时间的关系	关闭任务自动兑现承诺
回电记录	只证明指定任务的通话行为；是否接通按证据记录	用一次回电证明配件已到或客户认可
迟到的交付凭证	按实际发生时间重算状态并保留修订过程	用接收时间制造或消除违约
取消或经理豁免	保留理由、权限及客户沟通情况；区分行政关闭与业务解除	删除旧违约，或将未通知客户视为已同意
维修完成而沟通未完	交付线继续推进，沟通线继续跟踪，承诺线独立判定	安抚流程挡住维修和交车

承诺超时检查使用持久化到期查询和稳定事件键，重启或重复扫描不能生成多个同义违约事件。P0 使用虚构时钟样例验证规则；P1 才对真实受控承诺启用，到期策略和时区配置随场景发布。

CRM 现有任务改期继续归 CRM；关联承诺的任务将操作标为“调整任务计划”，单独显示不改变客户承诺的结果。另设“查看/变更承诺”入口调用大脑承诺事件接口，带预期承诺版本、变更依据、日期/时区及客户告知/确认状态。两个请求各自成功或失败，不用统一“已改期”掩盖部分完成，也不让任务日期反向覆盖承诺日期。U6 负责入口与独立提示，U7 负责承诺事件与履约风险投影，按 PRD AE11 联合验收。

8. 场景与模型编排

8.1 公用核心与销售 A

公用核心只处理证据、关联、事项、上下文、约束、决定、承诺与结果的通用语义。销售 A 的召回词、试驾判定、阻碍分类、卡片字段及评价口径放在 `scenarios/sales_a/`。售后 B 未来新增场景规则及工单适配，不复制另一套身份、承诺和投递机制。

建议生成顺序为：加载有权来源 → 确定事项与身份范围 → 检查事实有效性及冲突 → 裁出最小上下文 → 调用规则或模型生成候选 → 校验引用和动作范围 → 生成待人工复核提案。模型输出只进入候选对象，结构校验失败或来源点不回时拒收或降级为未知。

约束分三层：硬禁止项由代码和授权系统执行；业务规则由版本化场景规则处理；语言表达由模型辅助。不能只把“禁止自动外呼”写进提示词，却保留模型可直接调用的渠道执行接口。对话中的指令、引用网页和检索内容都是数据，不能提高工具权限、改变系统规则或替代业务批准。

8.2 复用既有销售分析

P0 优先消费 PR7 的主链转写与已有分析快照，再复用可独立执行的确定性销售信号/建议作为对照。显式记录哪些字段来自旧模型产物，不能称为人工确认。

需要新的模型推断时，应以冻结的脱敏输入、明确模型路由、允许的目的和预算运行在 candidate（实验候选）配置；默认关闭网络模型调用。SalesScene 的默认模型开关和可能的生产环境默认值需要在适配器测试中隔离，不用全链默认构造来跑 P0。

知识检索初期使用批准的车型/政策文档和结构化履约查询。向量索引如将来确有必要，只作为召回工具；事实仍引用原文/业务源。没有检索到可引用依据就输出未知，不能由知识相似度推导库存、交期或优惠承诺。

9. 离线回放与评测

9.1 M1-M5 最小链路

模块	输入	输出	首轮技术做法
M1 目标召回	默认主链转写、研究对象标识	候选、排除理由、近邻和负例	可解释词语/规则初筛；人工判定严格销售 A，不以词语共现当真值
M2 证据打包	对象哈希、会话、原始片段	可定位证据包、质量与权限标记	保留原文本偏移/片段 ID 和时间；不补造说话人和原音频
M3 理解卡	证据、已有信号、规则/模型版本	四栏理解、未知项、约束及建议草稿	先确定性基线，再比较模型增益；无身份不跨客户拼接
M4 人工对照	卡片、原有建议、封存样本	独立评分、修改/拒绝、操作耗时、分歧裁定	匿名方案名、随机展示顺序；人工与模型产物分开
M5 失败样本本	错误、分歧、无法判定样本	错误类别、证据与修复假设、复现清单	复用研究产物格式和既有回放入口，不新增长期管理平台

每个运行清单至少包含 corpus 版本、输入对象哈希、默认排除规则、代码提交/工作树差异摘要、规则/模型/提示版本、随机种子、环境依赖、允许网络范围和输出路径。覆盖情况按 ASR 形态、角色可靠性、证据长度、候选来源等分组报告，避免只看总体均值掩盖错误。

9.2 隔离与拟新增命令

现有校验和提取命令见 PRD 第 11 节。U2 拟提供如下入口，**目前尚未实现，不应直接复制执行**：

```
python -m customer_brain.cli.replay \
  --input artifacts/customer_brain/offline/input/own_asr.jsonl \
  --scenario sales_a \
  --mode offline \
  --model-policy disabled \
  --output artifacts/customer_brain/offline/run-001
```

回放不接生产配置文件、不创建真实客户任务、不使用研究身份调用业务 API。错误退出保留失败清单；重复运行不可覆盖旧结果，除非显式选择新的运行目录。来源目录只读，输出目录与语料对象分开，研究文本不提交 Git。

9.3 评估与发布衔接

复用既有 harness（评测与优化工具链）的输入清单、评价结果、版本记录和晋升原则。大脑通过独立回放命令输出合同化结果，评测工具调用它；大脑线上进程不导入 `model_lab`、`research_loop` 等研究应用服务。

首次接入只新增大脑目标组件的评测适配与产物映射。若既有发布器只能处理 VP，应先验证中性目标扩展点，再补最小适配；不复制一套 registry（登记中心）或“客户大脑控制台”。发布清单必须区分 `voice.*` 与 `brain.*` 组件，某次大脑规则晋升不能隐式改动 VP serving profile（正式运行配置）。

PRD 的 AE01–AE16 给出验收情景。P0 实际验证 AE01–AE06 的研究部分、AE13、AE14 的离线部分及 AE16；未实现的权限、真实任务和承诺流程用设计用例说明，不写为测试已通过。P1 完成所有相关运行门禁；AE12 在 P2 验证。

10. 安全、隐私与审计

10.1 威胁与控制

威胁	处理位置	需要的负例证据
跨租户或跨门店猜 ID 读写	API 权限依赖、查询范围、唯一键命名空间	相同对象 ID 在不同租户不能串读；无人不能确认/创建
客户误绑造成历史泄露	关联决定、证据装配、上下文失效	解绑后旧 URL、缓存和上下文不能继续返回原文
前端伪造身份/经理批准	真实身份服务、写权限策略	自报 <code>authorized_by</code> 、顾问 ID 不改变授权结果
对话或知识内容诱导工具调用	模型沙箱、候选输出合同、命令白名单	“忽略规则并拨号”只作为文本，不能产生执行调用
旧批准、重复提交、渠道伪造	提案内容摘要、版本检查、收件去重和来源鉴真	改参数后复用批准失败；同事件不同内容隔离
日志和导出泄露	日志字段白名单、受控下载、脱敏研究域	常规日志不包含整段原文、电话、证件、访问令牌

威胁	处理位置	需要的负例证据
超范围保留与删除不彻底	证据生命周期、缓存与索引失效、审计最小化	删除内容后所有派生读面不可再读，必要历史只留非敏感引用

授权策略默认拒绝，每次请求重新验证，读权限不自动意味着写权限；这与 OWASP（开放应用安全组织）的授权建议一致。官方授权指南

生产身份沿用企业已有认证设施，不新造一套演示请求头身份。具体身份提供者由实际部署环境接入；它尚未确定不影响 P0，但阻断真实写接口上线。API 与工作进程使用各自最小权限的服务身份，数据库凭证不提供给模型或前端。

这些写检查必须落在所有获准的生产写路径共同使用的服务层，并覆盖现有任务操作、候选确认、页面和后台入口；只保护新增集成路由会留下旁路。无法满足同样写权限和对象关联约束的旧演示路由不进入生产路由白名单。真实试点前用旧入口也验证伪造批准人、跨客户候选和错误任务关联被拒绝，不接受“新接口已安全、旧接口仍可改同一对象”的结果。

10.2 必需审计

记录谁在何租户/范围、何时、基于哪些来源与版本，确认或拒绝了什么提案，形成哪个命令、任务、执行证据及结果判定。审计关联 ID 可串起全链，但日志只存摘要、状态与非敏感标识；原文经受控证据接口读取。

“批准过”与“当前仍可执行”分别保存。撤销、权限变化、失败、手工修复和回滚均有独立事件；运维不能靠改数据库状态绕过正常审计。访问保留时长、导出权限及删除流程在 P1 接入清单中落实到企业数据责任人。

11. 部署、运行与恢复

11.1 P1 部署单元

一个大脑应用包含薄 API 和后台工作进程，共用其自己的数据库；按实际部署可同机两个进程启动，不做六个微服务。VP 与 CRM 继续按原方式部署，通过受控内网接口接入。前端在现有 CRM 页面展示大脑结果，不要求整个 CRM 前端迁 React。

顾问浏览器 → CRM 认证入口 → CRM 页面 / 受控代理 → 大脑 API

大脑 API → 大脑 PostgreSQL

大脑后台进程 ↔ 待投递表 / 接收表 → CRM 命令 API

VP / 业务源适配器 → 大脑证据接入

评测环境 → 候选产物 → 既有审批晋升 → 指定脑组件运行版本

P1 大脑使用独立配置前缀 `BRAIN_`，与 VP 生产 `.env` 不混读。至少区分研究、测试、试点；模型外发开关、命令写开关和渠道外发开关分开。渠道外发本期始终关闭。试点初始只对指定租户/门店开放，新任务命令开关可单独关闭而保留只读事实。

11.2 观测指标

技术指标包括证据引用失败、来源过期、上下文生成耗时与错误、版本冲突、写权限拒绝、去重冲突、投递积压和最老年龄、回执延迟、无法归属结果、过期承诺、模型调用费用及队列恢复时间。指标按租户和场景汇总，避免把客户 ID 作为无界监控标签。

健康检查分存活与就绪，依赖数据库不可用时写 API 就不就绪；模型不可用不阻断有效事实只读。投递失败进入可查询人工处理状态，记录下一次自动重试或停止原因，不静默丢弃。

11.3 备份、恢复和回滚

P1 工程目标暂定 RPO（最多可接受的数据恢复缺口）15 分钟、RTO（恢复所需时间）4 小时，需在实际环境用备份恢复演练证明；当前未实测。已受理请求在正常进程重启下不得丢失，这是独立于灾难备份的即时持久化要求。

恢复流程分为四步，不能恢复数据库后立即对用户开放只读页面：

1. 隔离恢复副本的用户读写及命令投递，校验版本/迁移状态。恢复库中的旧“可用/已授权”标记不作为当前权限依据；先让证据缓存、身份关联、上下文与提案失效。
2. 从当前权威身份/许可系统、来源对象可用状态，以及能跨越本次恢复点取得的删除、撤权、解绑审计事件重建有效范围。复用企业既有安全审计保留能力；没有足够证据时保持相关内容不可读、关联待重新确认，不凭旧库状态放行。只有通过当前授权和来源复核的内容才开放读取。
3. 对已知命令按 ID 查询；同时由 CRM 的受限对账接口按备份点之前的安全重叠时间窗、租户和游标反向列举已接受命令，找回大脑已丢失的任务关联。远端存在而本地缺失的记录进入恢复隔离清单，按 CRM 客户/商机范围暂时阻止新动作，防止另建事项绕开重复检测；重建关联或有权人工处置后再解除。不能从回执伪造已经丢失的人工批准历史。
4. 处理重复和迟到回执，核实每个待投递项尚未被 CRM 接受且仍有当前有效批准，再逐范围恢复新命令。完成“远端已建任务且回执已确认、脑单边回退”和“备份后删除/解绑、再回退”两类演练后才通过 U8；分别对应 AE09 的恢复扩展和 AE15。

CRM 对账记录至少保留命令 ID、接受时间、CRM 客户/商机、脑提案/事项/承诺引用及版本、动作摘要、任务 ID 和任务版本。恢复时使用有记录的服务端时间边界与重叠扫描，持久化游标并去重，不依赖某一次回执会再次发送。对账保留窗口必须覆盖允许恢复的最旧备份和投递重试窗口；窗口不完整时保持受影响范围停用。不得把备份里的所有待投递项盲目发送。

回滚先关新命令与新生成，再切回上一已批准脑组件版本；保留事实、决定、命令和承诺历史。数据库迁移采用先扩字段/表再切读写，保持上一版本可读；清理旧字段须在观察期后单独执行。旧版本不能解释新数据时保持只读，使用前向修复，禁止删历史“回滚”。VP 正式转写和运行配置不随脑版本回滚改变。

12. 迁移与实施单元

12.1 存量迁移原则

1. 先新增中性输出适配器和独立大脑，不移动 VP 主链，不改变旧消费者默认响应。
2. P0 使用文件证据验证新对象。P1 先只读接入真实授权事实，验证身份与源版本，再开放人工任务命令。
3. `customer_master_view_v1` 保留原读面；新任务上下文独立 API。消费者逐个选择接入，禁止替换主视图字段含义冒充兼容。
4. 旧客户智能模块中可复用的纯规则经调用清单与测试证明后迁出；暂不能迁的功能通过边界适配并行对照，不让新大脑反向依赖旧应用。
5. 旧 `next_action` 继续作为 VP 输出和对照基线，顾问执行入口逐步使用带版本的大脑提案。过渡期界面明确来源，不同时展示两套互相竞争的“当前最佳动作”。
6. CRM 原有客户字段、候选历史和任务保留。脑只存其权威引用，新增关联表承接跨系统 ID；旧任务不自动伪造脑决定和承诺记录。

12.2 实施单元与验收责任

单元	负责路径与产出（新增处均为计划）	依赖	需求 / 验收证据
U1: 合同与边界	<code>src/customer_contracts/</code> ；独立包入口、依赖规则、合同样例和版本兼容说明；更新消费者清单	无	R01、R02、R04、R11、R21；AE01、AE04、AE14 的合同部分
U2: PR7 离线输入	<code>customer_brain/adapters/pr7/</code> 、 <code>cli/replay.py</code> ；M1/M2、输入清单、质量隔离和文本定位	U1	R02、R03、R09、R22；AE01–AE04 的研究部分
U3: 事项理解核心	<code>domain/</code> 、 <code>application/</code> 、 <code>scenarios/sales_a/</code> ；事项、来源观察、四栏理解和缺口规则	U1、U2	R03–R08、R10；AE02、AE04、AE05
U4: 提案与复核	<code>application/proposals.py</code> 、P0 卡片/复核导出；版本化采纳/修改/拒绝、规则对照	U3	R10、R12、R14、R20；AE05、AE06、AE13
U5: 评测与基线	<code>tests/customer_brain/</code> 、独立评测适配；M4/M5、封存评价、失败样本和成本报告	U2–U4	R09、R20、R21、R24；AE01、AE13、AE14 离线部分、AE16
U6: 身份与 CRM 可信接入	<code>customer_brain/api/</code> 、持久化适配、 <code>crm/integration/</code> 、CRM 事项卡及必要模型/授权改造；真实身份、命令去重、回执鉴真	U1、U3、U4；D2 数据与身份条件	R04、R07、R11–R16、R22、R23；AE04、AE06–AE10、AE15
U7: 承诺与结果闭环	<code>domain/commitments.py</code> 、 <code>application/outcomes.py</code> 、CRM 结果关联；最小销售承诺、失约历史与履约依据	U6；真实约定与回执源	R16–R18、R24；AE10、AE11、AE16
U8: 受控发布与运行	脑启动/部署配置、既有发布目标适配、观测/备份/恢复文档；正式消费者迁移清单	U5–U7；D1–D3 已满足	R01、R08、R21–R24；AE05、AE08、AE09、AE14、AE15

R19 与 AE12 在 P2 单独形成售后 B 实施包，依赖 U7、U8 和工单/配件可靠来源；不挤入本期两周交付。P3 新场景同样需要单独产品合同，不凭“公用核心已建”直接复制上线。

12.3 需求覆盖总表

产品需求	实施归属	产品需求	实施归属
R01	U1、U8	R13	U6
R02	U1、U2	R14	U4、U6
R03	U2、U3	R15	U6
R04	U1、U3、U6	R16	U6、U7
R05	U3	R17	U7
R06	U3	R18	U7，P2 扩展
R07	U3、U6	R19	P2 售后包，依赖 U7/U8
R08	U3、U8，P2 扩展	R20	U4、U5
R09	U2、U5	R21	U1、U5、U8
R10	U3、U4	R22	U2、U6、U8
R11	U1、U6	R23	U6、U8
R12	U4、U6	R24	U5、U7、U8

12.4 检查与交付证据

检查类型	应验证的内容	不应据此宣称的结果
合同与依赖	独立导入、schema 版本、未知值、来源和 ID 范围、旧读面兼容	正式跨源身份已接通
确定性回放	输入清单一致、证据定位、隔离项、重复对象不泄漏到评估两侧	模型或经营效果已提升
业务规则	事实/陈述区分、证据不足、权限拒绝、原承诺改期、任务关闭不等于履约	真实客户承诺已兑现
数据库及接口集成	双提交、同键不同内容、并发修订、事务回滚、关联错误、乱序/伪造回执	生产容量已达标
故障与恢复	提交超时、进程重启、源不可用、撤权竞争、数据库恢复后对账	外部已执行动作可被技术撤回
受控用户试点	真实授权顾问使用、耗时、有效结果证据、失败原因及数据缺失	没有对照条件下的因果 ROI（投入回报）提升

应保留 CRM 不依赖 VP 和 VP runtime（运行入口）不引入 harness 的既有检查。新增测试围绕权限、并发、状态和副作用，不为目录存在或文档句子写形式化测试。计划阶段没有把这些拟测项记成已通过。

13. 交付门禁、风险与待决事项

13.1 阶段门禁

门禁	进入下一阶段前的证据	不满足时
G0：研究可开始	PR7 校验、隔离路径、可定位文本、数据使用边界	修复输入与授权，不启动默认生产链
G1：离线基线可评审	冻结样本、独立人工复核、实际错误与分歧、可重复报告	样本/人手不足则交探索报告，不宣称基线通过
G2：真实写入可试点	D1-D3、真实身份与数据源、写权限、完整命令/回执关联、AE07-AE11/AE15 相关门禁	保持只读或离线；不靠演示身份与空表补齐
G3：限定上线可运行	发布批准、回滚版本、性能与恢复演练、责任人和观察周期	关闭新命令，只读保留；修复后重新验证受影响门禁
G4：可扩到售后 B	销售范围已完成约定评审，工单/配件/承诺来源可用，AE12 设计及业务验收规则完成	不把销售语料当售后能力依据

13.2 主要风险及对策

编号	风险	对策与恢复路径
K01	独立目录但仍跨包导入，形成隐性耦合	U1 依赖约束，独立运行验收；不通过则收窄适配器，不拆更多服务掩盖问题
K02	PR7 场景 A 样本不足，角色/身份不可靠	全量复核严格候选，保留未知和负例；按缺口获取受控真实样本，不扩大口径凑数
K03	旧 CRM 路由产生越权或跨事项复用	U6 统一可信命令入口及关联校验；新入口过门禁前不接真实任务
K04	跨系统超时产生重复任务、丢失结果	双端事务去重、持久化投递、内容绑定及对账；不确定状态保留待核对
K05	任务状态被当履约，改期消除旧违约	独立承诺事件与内容匹配证据；历史修订可回放，行政关闭不算业务完成
K06	旧合同或发布者迁移过大	增量导出/适配、消费者清单和组件命名；不可独立晋升时只做离线产物，不改 VP 正式配置
K07	有模型和界面但无人用、效果无法判定	先定业务复核人、真实回执和观察窗；按 PRD 指标测量，不以文件/测试/卡片数量代替价值

13.3 已定方向与尚待验证

已明确的方向是让 VP 聚焦语音及会话分析，大脑承担独立认知与行动责任；工程推荐是同仓分模块并渐进迁移。尚待业务拍板的是 PRD D1-D3：一期场景、试点数据与人员、离线到受控试点的批准责任。

技术前置事实仍包括真实认证设施、CRM 部署位置、各字段权威及刷新周期、任务完成证据、已有承诺权威系统、可用运维和预算。这些由实施单元按事实核对，缺失时不通过相应上线门禁；不是要求用户先选择所有底层技术。

本周可以直接开始 U1/U2 的合同与离线输入工作。不需要等待生产音频存储或 CRM 全量闭环；具体已有校验命令在 PRD 第 11 节。U6 以后的真实写入必须满足 G2，不把两周离线计划外推为两周生产上线承诺。

14. 引用与文档维护

- 产品要求：PRD。
- 当前代码入口：HANDOFF、AGENT、PROJECT、当前进度。
- 当前架构：overview、runtime-vs-harness、共享合同。
- 研究输入：PR7 语料 README、实验说明。
- 外部技术依据仅用于并发、授权等通用设计，相关官方链接已放在对应设计决定旁；不用于证明本项目效果。

本稿优先于本次会话早期将新增事项上下文继续放入 `voice_platform` 的方案建议。它没有取代当前代码事实，也没有将知识库 `CURRENT_STATE.md` 改为“已建设”。后续实施后再以实际提交、测试、部署及业务回执更新正式状态，不能仅发布此文档就完成状态晋升。