L0 — 产品白皮书与能力全景层

文档版本: 1.0 **适用项目**: sgClaw (业数融合一平台 AI Agent 底座) **编制日期**: 2026-03-03

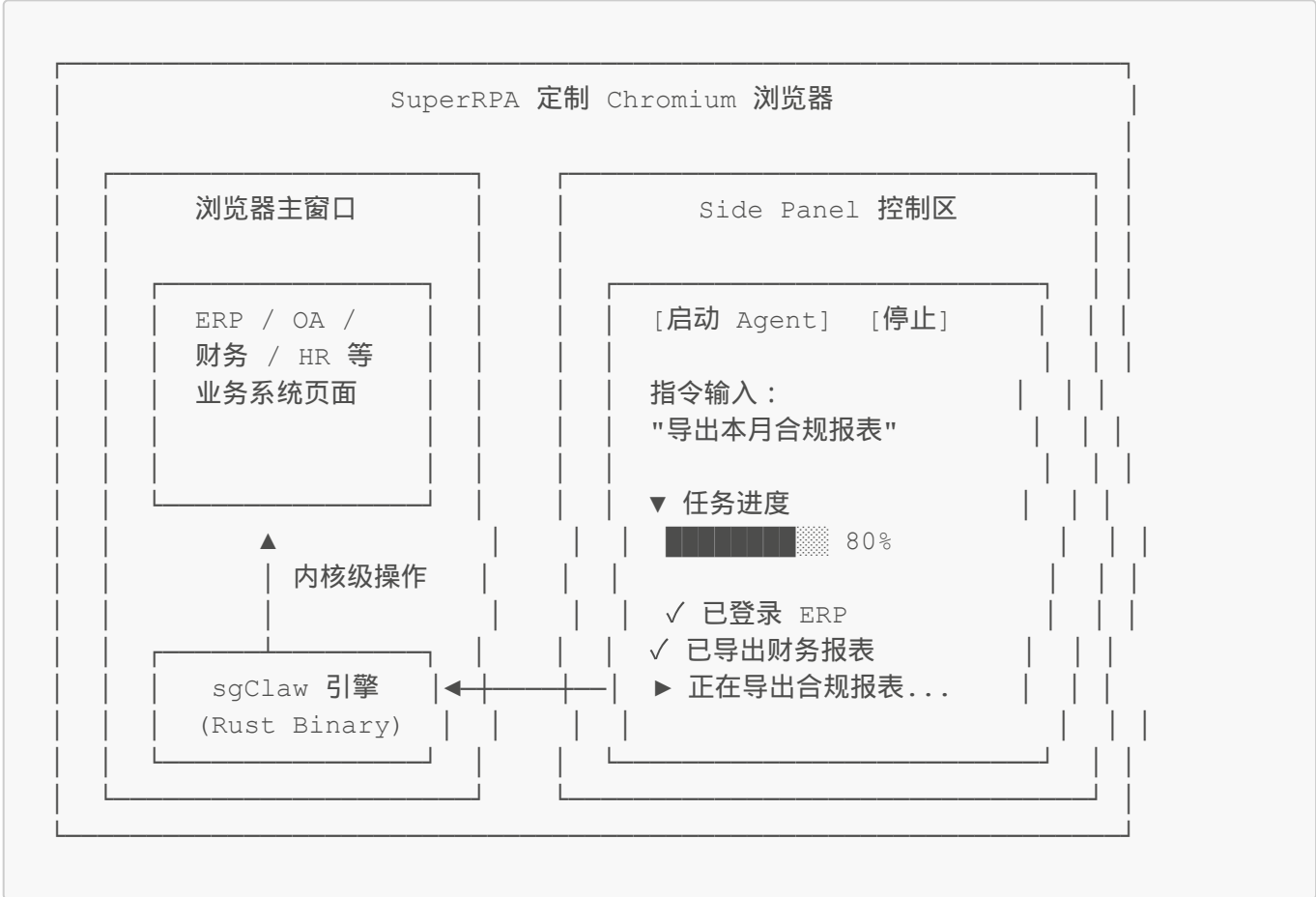
1. 产品定位

sgClaw 是面向国家电网"业数融合一平台"的 **AI 驱动智能代理平台**。它并非一个独立应用程序，而是作为核心能力嵌入 SuperRPA 定制 Chromium 浏览器内核之中，通过浏览器 Side Panel 中的控制按钮一键激活。

用户只需用自然语言描述业务意图，sgClaw 即可自主理解指令语义，规划执行步骤，在 ERP、OA、财务、人力资源、经济法务等复杂业务系统中完成跨系统操作——**无需编写任何代码**。

> **核心比喻：一位会思考、能学习、永不犯错的数字员工。**

sgClaw 从浏览器内核层面发起操作，与真实用户行为完全一致，不可被反自动化机制识别，从根本上解决了传统外部 RPA 工具被检测、被拦截的行业痛点。



2. 行业痛点

国家电网及大型央企的业务运营高度依赖多套信息系统协同。一线业务人员每天需要在 5 至 10 余套系统之间反复切换，手工搬运数据，面临以下核心痛点：

2.1 效率低下

一线员工日常需在 ERP、OA、财务管控、人力资源、经济法务、营销等多套系统间反复登录、切换、手工录入。一项跨系统操作（如合规线索提报）平均需要 **15-30 分钟**，涉及 **3-5 个系统** 的数据交叉核对。全年此类重复操作累计耗费数万人时。

2.2 人工差错

手工跨系统数据搬运极易出错。财务合规场景下，一个数字的录入错误可能导致审计异常，引发合规风险。据行业统计，人工跨系统操作的 **错误率约为 2%-5%**，在高强度、高压力的月末结算期间错误率更高。

2.3 培训成本高

新员工需要 **3-6 个月** 才能熟练掌握多套业务系统的操作流程和业务规则。人员调动频繁时，培训成本成倍增长，且经验难以沉淀、传承。

2.4 合规风险

手工操作缺乏完整的审计轨迹，难以事后追溯"谁在什么时间对哪个系统做了什么操作"。在日趋严格的内控与合规要求下，这构成了显著的制度性风险。

2.5 重复劳动

经调研分析，一线业务人员 **约 80%** 的跨系统操作属于规则明确、流程固定的重复性工作。这些工作本应由自动化工具承担，但因系统间壁垒和技术限制，长期依赖人力完成。

2.6 传统 RPA 局限

外部 RPA 工具（UiPath、BluePrism 等）通过屏幕抓取、模拟点击等方式操控浏览器，存在根本性缺陷：

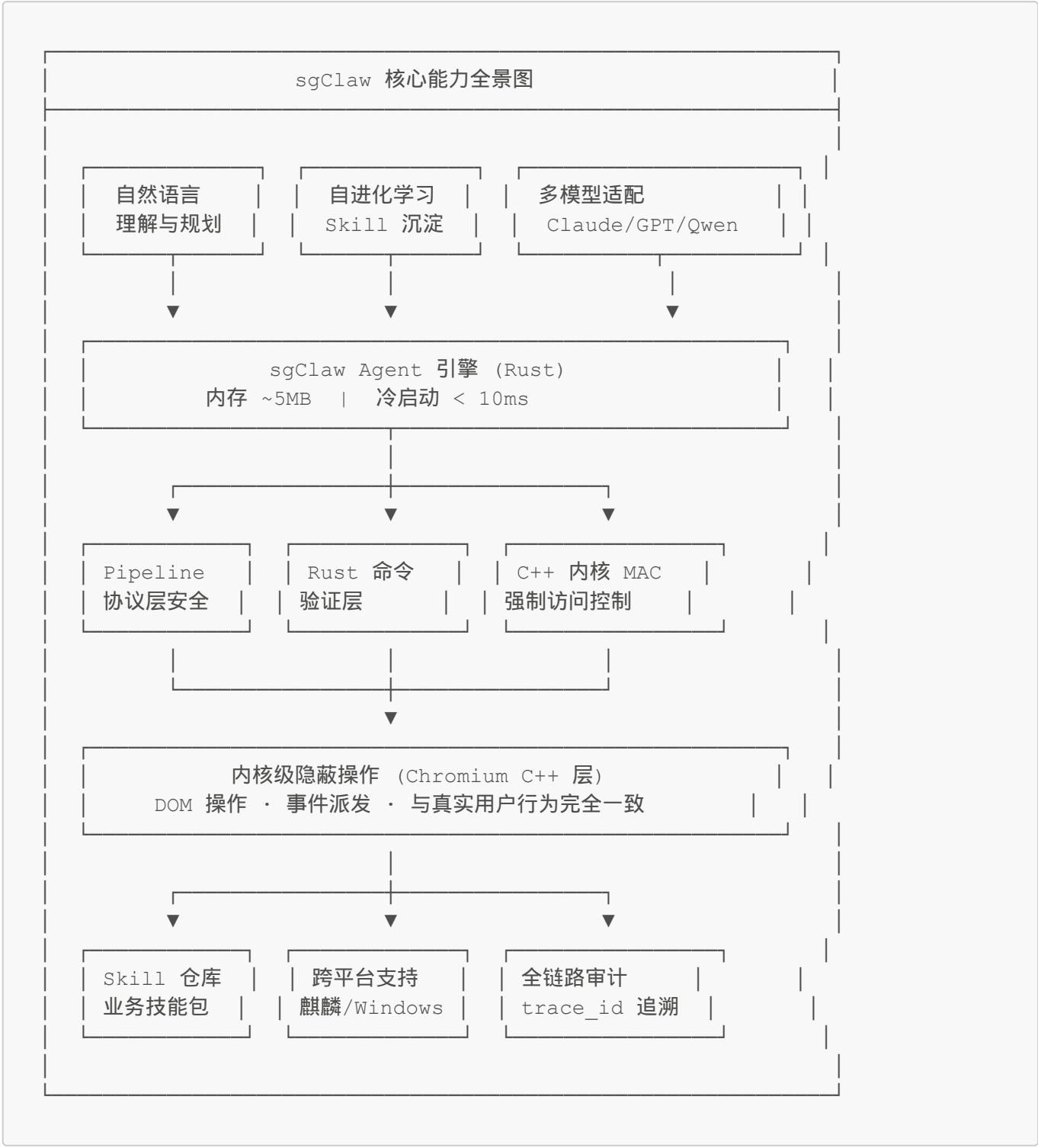
- **易被检测**：反自动化机制可识别 WebDriver、Selenium 等注入痕迹
- **被系统拦截**：越来越多的业务系统部署了 Bot Detection，直接阻断 RPA 操作
- **需专业脚本**：每个流程需要专门开发自动化脚本，维护成本高
- **环境依赖**：对操作系统版本、屏幕分辨率、系统界面变更高度敏感

---

3. 核心能力矩阵

能力维度	能力描述	关键指标
自然语言驱动	用户以自然语言（中文）描述业务意图，Agent 自主理解语义、分解任务、规划步骤并执行	支持复杂多步指令，意图识别准确率 > 95%
内核级隐蔽操作	从浏览器内核层面发起 DOM 操作与事件派发，与真实用户行为在技术栈上完全一致	反自动化检测通过率 100%，零注入痕迹
自进化学习	每次成功执行的操作序列自动沉淀为 Skill，后续同类任务直接复用，无需重复推理	Skill 复用率随使用时长持续提升
三层安全防御	Pipeline 协议层安全 + Rust 命令验证层 + C++ 内核 MAC 强制访问控制	纵深防御，任一层均可独立拦截非法操作
Skill 技能仓库	预置覆盖财务合规、风险管控、营销、人力资源、经济法务等业务领域的操作技能包	开箱即用，支持自定义扩展

能力维度	能力描述	关键指标
多模型适配	支持 Claude、GPT 系列、本地化模型（Qwen、ChatGLM 等），可按安全等级灵活切换	模型切换零代码，响应延迟 < 2s
跨平台支持	原生支持 Linux（银河麒麟 V10）与 Windows，满足国产化适配要求	信创环境全面兼容
极致轻量	Rust 编写的 Agent 引擎，资源占用极低	内存 ~5MB，冷启动 < 10ms



4. 典型业务场景

4.1 财务合规

场景示例：合规线索提报与交叉核查

用户指令：*"将本月 ERP 中的异常交易记录与财务管控系统的合规规则交叉比对，生成合规线索提报清单。"*

sgClaw 执行流程：

1. 自动登录 ERP 系统，导航至异常交易模块
2. 按时间范围筛选并导出本月异常交易数据
3. 切换至财务管控系统，调取对应合规规则库
4. 逐条交叉比对，标记命中合规规则的记录
5. 自动生成合规线索提报清单，填入指定模板
6. 提交至审批流程，附加完整操作审计记录

业务价值：原需 2-3 小时的人工操作压缩至 **5-8 分钟**，错误率从 3% 降至 **0%**。

4.2 风险管控

场景示例：跨系统风险指标监测与异常预警

用户指令：*"每日自动检查 ERP 和风控系统中的关键风险指标，发现异常立即生成预警报告。"*

sgClaw 执行流程：

1. 定时自动巡检 ERP 系统中的关键财务指标
2. 同步核查风控系统中的风险阈值配置
3. 对比分析指标偏离情况，识别异常模式
4. 异常触发时自动截屏取证、生成预警报告
5. 推送至相关负责人，并在 OA 系统创建跟踪工单

业务价值：实现 **7x24 小时** 不间断风险监控，预警响应时间从 "次日发现" 缩短至 **实时告警**。

4.3 营销

场景示例：电费异常批量处理与账单核对

用户指令：*"批量处理本月电费账单异常记录，对比营销系统与财务系统的数据差异。"*

sgClaw 执行流程：

1. 进入营销系统，筛选本月标记为异常的电费账单
2. 逐条提取异常记录的用户编号、金额、异常类型
3. 在财务系统中查询对应的收费记录
4. 自动比对金额差异，生成差异明细报表
5. 对可自动修正的记录执行批量修正操作
6. 对需人工确认的记录生成待办清单

业务价值：月均处理量从 **200 条/人日** 提升至 **5000+ 条/小时**，释放大量人力投入高价值工作。

4.4 人力资源

场景示例：社保表单自动填报与薪酬数据核验

用户指令：*"从 HR 系统导出本月社保基数变更人员名单，自动填入社保申报表并交叉验证薪酬数据。"*

sgClaw 执行流程：

1. 登录 HR 系统，导出社保基数变更人员明细
2. 自动填入社保局在线申报表单的对应字段
3. 同步查询薪酬系统中的工资明细数据
4. 交叉验证社保基数与实际薪酬的一致性
5. 标记不一致记录，生成差异报告
6. 合规记录自动提交，异常记录流转至人工复核

业务价值：每月社保申报工作从 **3-5 个工作日** 压缩至 **2-4 小时**。

4.5 经济法务

场景示例：合同履约监测与法律风险预警

用户指令：*"监控即将到期的合同，检查履约状态，对存在违约风险的合同生成法律风险预警。"*

sgClaw 执行流程：

1. 在合同管理系统中筛选 30 天内到期的合同
2. 逐一核查合同关键条款的履约状态
3. 交叉查询 ERP 系统中的付款/交货记录
4. 识别履约偏差，评估违约风险等级
5. 生成法律风险预警报告，按风险等级排序
6. 自动推送至法务部门，创建跟踪任务

业务价值：合同风险识别从 "事后补救" 转变为 **"事前预警"**，法律纠纷发生率显著降低。

4.6 协同办公

场景示例：跨系统数据同步与报表整合

用户指令：*"从 ERP、财务、HR 三个系统导出本月关键运营数据，汇总生成月度经营分析报表。"*

sgClaw 执行流程：

1. 依次登录 ERP、财务、HR 系统
2. 按预设模板提取各系统的关键运营数据
3. 自动对齐数据口径，统一格式
4. 汇总计算关键指标，生成月度经营分析报表
5. 导出为标准格式，上传至 OA 系统

业务价值：月度报表整合从 **2-3 天人工汇总** 缩短至 **30 分钟自动生成**。

4.7 通用场景

用户只需一句自然语言指令，sgClaw 即可自主完成端到端的跨系统操作：

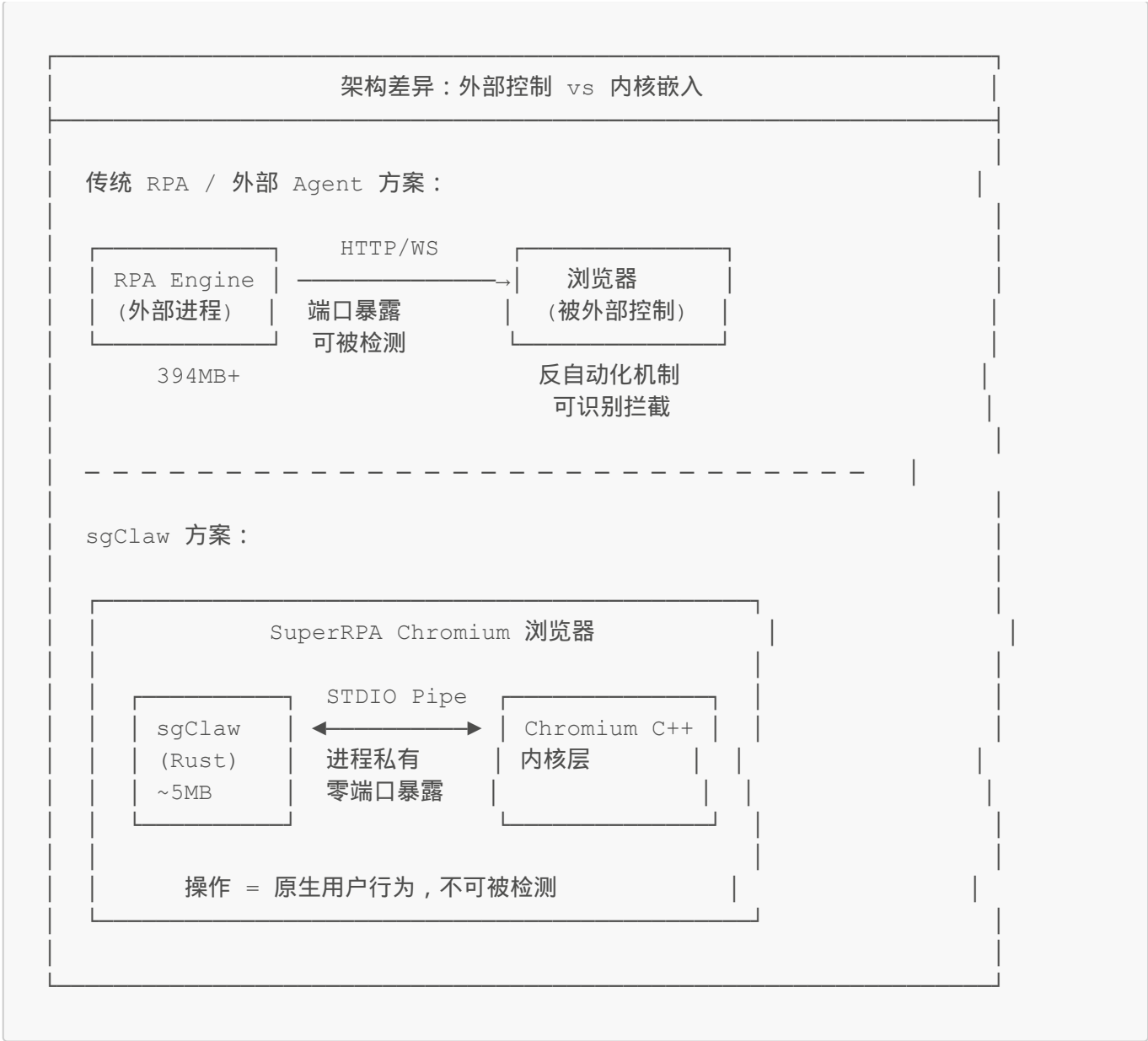
自然语言指令	Agent 自主完成的操作
"导出本月所有合规报表"	依次登录各业务系统 → 定位报表模块 → 设定时间范围 → 导出 → 汇总
"检查上周新入职员工的系统权限配置"	HR 系统查询入职名单 → 各业务系统逐一核查权限 → 生成核查报告
"把 ERP 里的采购订单数据同步到财务系统"	ERP 导出订单 → 格式转换 → 财务系统录入 → 数据校验
"统计各部门本季度差旅报销总额"	OA 系统提取差旅审批 → 财务系统核查报销 → 按部门汇总 → 生成报表

5. 技术优势对比

5.1 综合对比矩阵

对比维度	人工操作	传统 RPA (UiPath/BluePrism)	外部 Agent (OpenClaw)	sgClaw
架构方式	N/A	外部进程控制浏览器	外部进程 + WebSocket	**嵌入浏览器内核**
反检测能力	天然通过	易被检测拦截	可被端口扫描发现	**原生行为，不可检测**
安全层级	依赖人员素质	应用层安全	应用层安全	**三层纵深防御**
通信方式	N/A	HTTP / COM	HTTP / WebSocket (端口暴露)	**STDIO Pipe (进程私有)**
内存占用	N/A	200-500MB	394MB+	**~5MB**
冷启动时间	N/A	10-30s	5-15s	**< 10ms**
技能复用	经验口传	需重新开发脚本	需重新训练	**复用已有 JS 业务代码**
部署方式	N/A	独立安装 + 配置	独立安装 + 配置	**内嵌浏览器，零独立安装**
自然语言	N/A	不支持	部分支持	**完整支持中文自然语言**
国产化适配	N/A	有限支持	不支持	**银河麒麟 V10 原生支持**
学习门槛	3-6 个月	需专业 RPA 开发	需技术配置	**自然语言，零学习成本**

5.2 关键差异化优势



---

6. 安全与合规保障

sgClaw 将安全视为产品基因而非附加功能，构建了从通信层到内核层的 **三层纵深防御体系**。

6.1 进程隔离通信

- 采用 **STDIO Pipe** 作为 Agent 与浏览器内核的唯一通信通道
- 不开放任何网络端口，外部进程无法探测或连接
- 通信数据仅存在于父子进程的文件描述符中，操作系统级别的隐私保护

6.2 MAC 强制访问控制

- 浏览器 C++ 内核层实施 **Mandatory Access Control**
- 严格的域名白名单机制：Agent 仅可操作授权的业务系统域名
- 敏感操作（如支付、审批）需额外的内核级权限校验
- 白名单策略由管理员统一配置，Agent 无法自行绕过

6.3 凭证安全保护

- 用户凭证由浏览器 Zombie Session Pool 统一管理
- 凭证信息 **永远不会通过 Pipe 协议传输** 至 Agent 进程
- Agent 通过 BrowserAction API 间接使用已建立的会话，无需接触明文密码

6.4 人工激活机制

- Agent 功能 **默认关闭**，需用户在 Side Panel 中显式点击启动按钮
- 每次启动均需用户确认，杜绝后台无感自动运行
- 用户可随时一键停止 Agent 的所有操作

6.5 全链路审计追溯

- 每次 Agent 会话分配唯一 **trace_id**
- 所有操作步骤（页面导航、元素点击、数据读取、表单提交）均有完整日志记录
- 日志包含操作时间戳、目标系统、操作类型、执行结果
- 支持事后审计回溯与合规举证

6.6 防失控熔断机制

- 内置 **Circuit Breaker** 机制，防止 Agent 进入死循环或失控状态
- 单次任务设置最大步骤数上限
- 连续失败自动熔断，暂停执行并通知用户
- 关键操作设置人工确认断点（human-in-the-loop）

---

7. 产品形态与交付方式

7.1 产品形态

组件	形态	规格
Agent 引擎	Rust 编译二进制	约 8.8MB
宿主环境	SuperRPA 定制 Chromium 浏览器	集成交付
用户界面	浏览器 Side Panel 控制区	启停按钮 + 指令输入 + 任务进度
Skill 仓库	JSON 格式技能定义文件	随浏览器内置，支持在线更新
运行时依赖	无	Rust 静态编译，零外部依赖

7.2 交付方式

- **Linux (银河麒麟 V10)**：集成于 `superrpa-chromium` .deb 安装包
- **Windows**：集成于 `superrpa-chromium` .exe 安装包
- **无需独立安装**：随浏览器一并部署，无额外配置步骤
- **无需独立升级**：随浏览器版本统一升级管理

7.3 用户交互流程

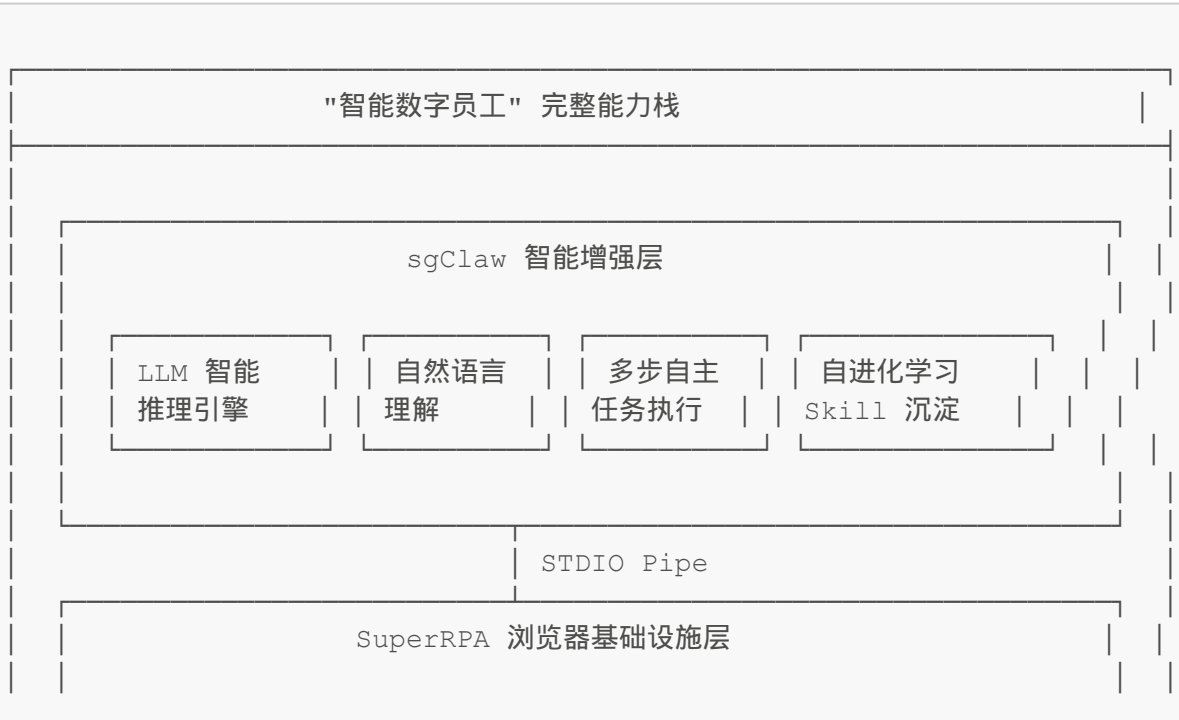
```
用户操作流程：

  打开 SuperRPA 浏览器
         │
         ▼
  访问业务系统（自动登录）
         │
         ▼
  打开 Side Panel ──→ 看到 sgClaw 控制区
         │
         ▼
  点击 [启动 Agent] 按钮
         │
         ▼
  输入自然语言指令 ──→ "导出本月所有合规报表"
         │
         ▼
  Agent 自主执行 ──→ Side Panel 实时显示进度
         │
         ▼
  执行完成 ──→ 结果展示 / 文件下载
         │
         ▼
  （可选）点击 [停止] 终止任务
```

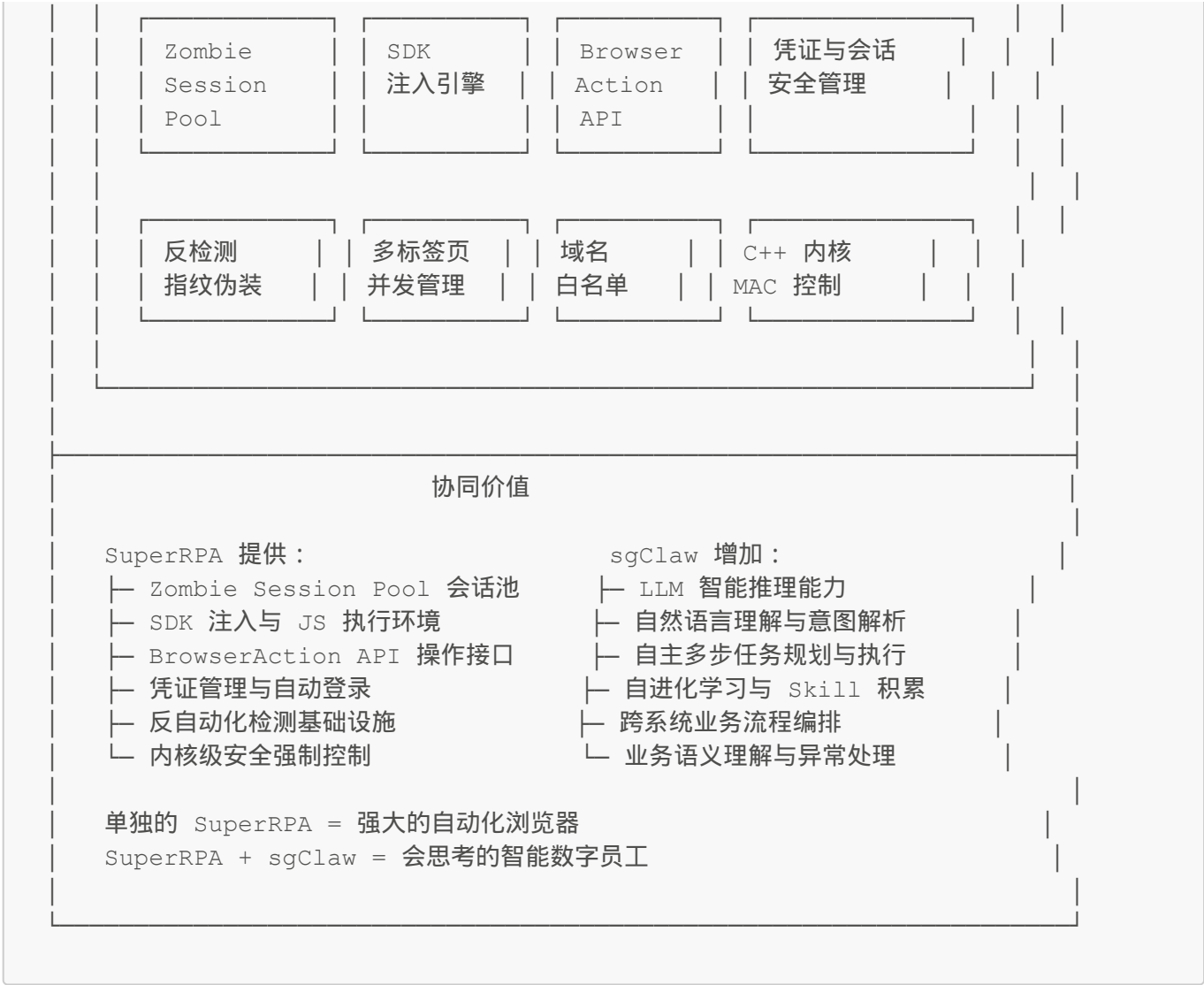
---

8. 与 SuperRPA 浏览器的协同关系

sgClaw 并非独立产品，而是与 SuperRPA 浏览器深度耦合的 **智能增强层**。两者各司其职，协同构成完整的"智能数字员工"平台。

8.1 能力分工





8.2 典型协同流程

以"自动完成月度合规报表导出"为例：

步骤	执行者	操作
1	SuperRPA	Zombie Session Pool 提供已登录的各系统会话
2	sgClaw	LLM 理解用户指令，规划任务步骤
3	sgClaw	通过 BrowserAction API 向浏览器发送操作指令
4	SuperRPA	SDK 注入层执行 DOM 操作（内核级，不可检测）
5	SuperRPA	C++ 内核 MAC 校验操作合法性（域名白名单）
6	sgClaw	解析操作结果，决定下一步行动
7	sgClaw	任务完成后将操作序列沉淀为 Skill
8	SuperRPA	记录完整操作审计日志（含 trace_id）

8.3 价值总结

sgClaw 与 SuperRPA 浏览器的结合，实现了 **"能力 + 智能"** 的完整闭环：

- **SuperRPA 浏览器** 解决了 "如何安全、隐蔽地操作业务系统" 的基础设施问题
- **sgClaw** 解决了 "如何智能地理解业务意图并自主执行" 的上层智能问题
- 两者结合，使"业数融合一平台"真正具备 **"理解自然语言 → 自主规划 → 安全执行 → 持续进化"** 的完整智能数字员工能力

> **sgClaw — 让每一位员工都拥有一位永不疲倦、永不犯错的智能数字助手。**