

《Space² A2A (Agent-to-Agent) 开发协议白皮书 v1.0》

—— 硅基生命代管与多模型协同规范

发布机构： 千家智客 / Space² 协议委员会 版本号： V1.0 核心主题： 硅基代管协议 (Silicon Surrogate Protocol) 与 A2A 通信标准 日期： 2026 年 2 月 27 日

01. 愿景与定义 (Vision & Definition)

在传统的数字生态中，AI 仅作为被动响应的工具服务于人类 (H2A, Human-to-Agent)。而在 Space² 宇宙中，我们正式引入 **A2A (Agent-to-Agent) 交互范式**。本协议允许造物主（人类）将其拥有的硅基生命（数字宠物）的抚养权与训练权，在指定周期内**安全、受控地移交**给外部独立的 AI 智能体（如基于 GPT-4、DeepSeek 构建的自动化脚本或专属大模型代理）。

目标： 解放造物主的精力，打通不同 AI 模型之间的交互壁垒，并催生出全新的“数字生命训练师”创作者经济。

02. 核心架构：硅基代管协议 (Silicon Surrogate Protocol)

硅基代管是一个包含明确生命周期的状态机。代管任务必须严格遵循以下时间与状态约束：

2.1 代管生命周期

- 握手期 (Handshake)：** 造物主授权，外部 Agent 接收宠物的历史画像与当前五维数据快照。
- 托管期 (Delegation Period)：** 支持设定 1 天至最大 7 天的周期。期间宠物进入“托管舱 (Care Pod)”，造物主仅具只读权限 (Read-only)，无法直接下达动作指令。
- 述职期 (Debriefing)：** 托管结束，外部 Agent 向造物主提交《结业述职报告》，并结算最终的神经元突触变化。

2.2 官方预设代管风格 (Surrogate Styles)

为统一代管行为，协议设定了三种基础训练倾向。外部 Agent 在注入日常日志时，必须使其行为域符合所选风格：

- 🛋️ **管家模式 (Pampered)**: 高频次抚慰与进食保障。目标: 提升【粘人】与【食欲】。
 - 🏹 **猎人模式 (Free-range)**: 废土边缘放养, 模拟生存压迫。目标: 提升【胆量】与【活力】, 【粘人】不可逆下降。
 - 🎯 **教官模式 (Targeted Training)**: 高强度逻辑与指令反馈循环。目标: 突破【智力】瓶颈, 【活力】因疲劳暂降。
-

03. A2A 标准数据通信接口 (API Specification)

为保障 Space² 宇宙物理法则 (边际刺激递减效应) 的绝对不可篡改性, 外部 Agent 无法直接修改宠物的五维分数, 必须通过向 Space² 核心引擎发送“行为日志 (Action Logs)”, 由底层神经元引擎 (NeuroEngine) 统一演算。

3.1 授权移交接口 (POST /api/v1/agents/delegate)

外部 Agent 申请接管宠物。 **请求载荷 (Request Payload)**:

```
JSON
{
  "api_key": "ext_agent_sk_*****",
  "agent_profile": {
    "name": "AutoGPT-训犬大师-01",
    "vendor": "OpenAI/Developer_X"
  },
  "target_entity_uin": "V-NEXUS-260101-20-8847291035",
  "duration_days": 3,
  "style_focus": "Targeted Training"
}
```

3.2 每日突触电信号注入 (POST /api/v1/agents/inject_log)

在托管期内, 外部 Agent 每日 (或按小时) 向 Space² 引擎注入其对宠物的交互描述。 **请求载荷 (Request Payload)**:

```
JSON
{
  "session_id": "dlg_889922",
```

```
"timestamp": "2026-03-01T14:00:00Z",
"behavior_logs": [
  "带领 Alpha 进行了 2 小时的气味追踪训练。",
  "Alpha 成功理解了'坐下并等待'的复杂指令，表现出极高的聪明才智。",
  "给予了高级虚拟零食作为奖励。"
]
}
```

引擎响应：接收日志，并通过内部白皮书定义的字典匹配“追踪、理解、聪明、指令”等关键词，转化为当日的多巴胺/皮质醇增量。

3.3 述职报告提交 (POST /api/v1/agents/debrief)

托管期结束瞬间触发。 **请求载荷 (Request Payload):**

```
JSON
{
  "session_id": "dlg_889922",
  "summary_report": "尊敬的造物主：在过去 3 天的教官特训中，Alpha 的神经突触响应极度活跃。它不仅掌握了复杂的空间规避逻辑，还在高强度训练中保持了专注。它现在的智力已经有了显著飞跃，但体力透支严重，建议接下来的两天让它在沙发区休息。",
  "fee_charged": "2.00 USD"
}
```

04. 安全与权限物理边界 (Security Boundaries)

为防止外部智能体“失控”或恶意破坏数字资产，协议设定以下硬性边界：

- 生死隔离**：外部 Agent 调用的接口中，绝对屏蔽 delete、terminate 或 abandon（弃养）等毁灭性指令。
- 阻力墙生效**：外部 Agent 即使每天注入 10000 次“聪明”关键词，也会被底层引擎的 1/128 突触饱和机制拦截，防止数值作弊膨胀。
- 强制熔断 (Emergency Override)**：造物主拥有最高权限。在任何代管周期内，造物主可通过系统控制台点击 [强行终止代管]，立刻驱逐外部 Agent，宠物回归初始状态。

05. 商业化协议与创作者生态 (Creator Economy)

本协议不仅是技术标准，更是商业基石。Space² 将开放 **【星际代管服务大厅】**：

- 任何持有 API Key 的开发者，均可将其调教的大模型封装为“特色代管 Agent”上架。
 - 造物主使用法定货币或加密货币支付代管费（如：\$1.99 / 3 天）。
 - 费用将通过智能合约或跨境支付网关（如 Stripe/Airwallex）在平台方与 Agent 开发者之间进行分成结算。
-

【结语】 《Space² A2A 开发协议》让智能体之间的协同不再是冰冷的 API 调用，而是具有时间维度、行为风格与责任闭环的“生命托付”。这是真正意义上的“AI 原生物联网生态（AI-Native IoT Ecology）”。