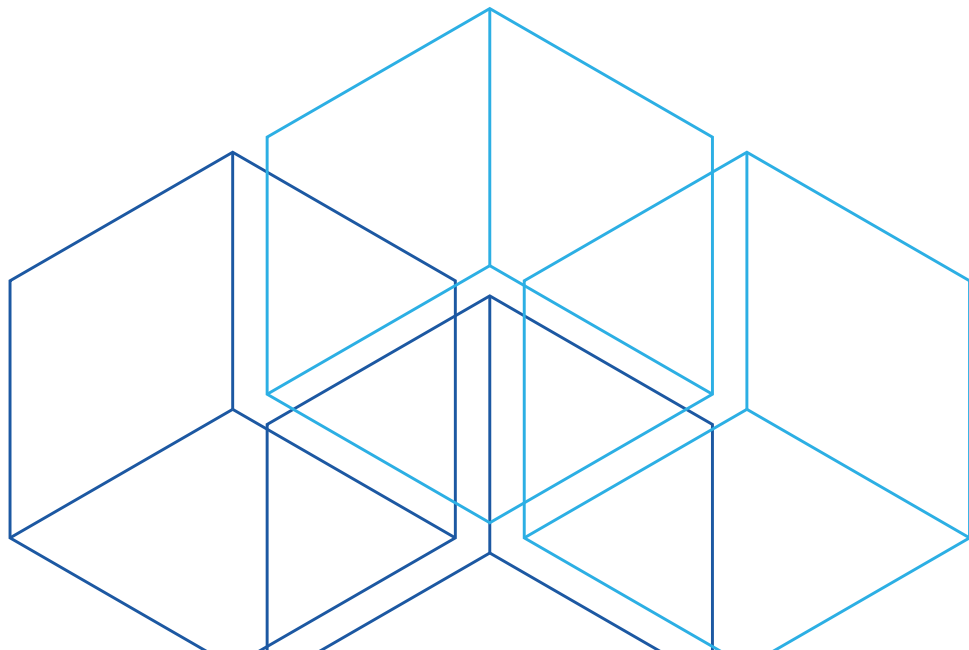




AI时代企业信息系统 安全计算架构白皮书

从网络边界走向数据、模型、智能体与管理过程边界

V4.02

管理过程与受控公域版

核校排印稿 / 2026年9月25日

研究框架与工程实践参考

文档控制

文档名称	AI时代企业信息系统安全计算架构白皮书
版本	V4.02（管理过程与受控公域版）
状态	过程稿 / 核校排印稿；基于V4.0发布稿，尚未经正式定稿
来源发布日期	2026年9月
编制单位	邦彦技术股份有限公司
文档性质	技术架构研究框架与工程实践参考；不构成国家标准、行业标准或监管分类，亦不构成对任何产品、投资或合规结论的承诺
适用范围	企业信息系统安全计算架构的规划、评审与建设；AI能力的配置与治理；PANSTONE CPC / DPC方案设计 with 验收参考
配套文件	《下一代商用计算机（NGCC）技术架构白皮书：品类开放与品牌口径校准版》V4.22；《PANSTONECPC与DPC产品定位、定义及协同体系》V2.0
版本沿革	V3.0（2026年9月4日，品牌换代）→ V4.0（2026年9月，管理过程与受控公域版）→ V4.02（2026年9月24日，一致性核校与排印过程稿）
排印日期	2026年9月24日
排印说明	采用一致性报告所列修订建议；本次为版式优化过程版本，不代表正式发布、认证或新增产品能力承诺。目标市场尚待确认；本次同步优化行距、字号与五业务域横向图，暂沿用原稿PANSTONE产品名称。

本白皮书以V3.0为基础重编。引用本过程稿时应注明“V4.02 管理过程与受控公域版（核校排印稿，2026-09-24）”，并保留相关表述的适用条件。架构定义用于理解与设计，具体产品选择与交付以型号资料、支持版本及项目约定为依据；本文不作为已取得认证、已完成全部测试或特定性能数值的证明。

目录

CONTENTS

编制说明 4

执行摘要 6

第一章 AI 改变了企业信息系统的基础假设 7

第二章四类数字控制权与总体设计原则 9

第三章五业务域：重新划定业务、数据与 AI 边界 11

第四章七层技术架构：让能力有明确落位 15

第五章 NGCC：统一计算底座 17

第六章企业私域 AI 平台、知识治理与能力差距管理 19

第七章人性、能力差距与三层信任 21

第八章管理过程与计算域 25

第九章 Agent 治理与人类责任 28

第十章进入经营：三链协同与代表性场景 30

第十一章安全架构、威胁模型与合规映射 31

第十二章建设路线与组织机制 34

第十三章验证、评价与持续改进 37

第十四章架构演进与开放协同 39

附录 A 核心术语 40

附录 B 架构决策最小检查清单 42

附录 C S4↔S3 三段传输结构与验收用例 43

参考资料 46

编制说明

人工智能正在把企业信息系统从“业务记录与流程支撑工具”，推向能够理解知识、参与判断并执行任务的智能协同系统。执行主体、数据流向与信任边界的变化，使传统以终端计算、内网信任和人工操作为基础的企业IT架构面临结构性挑战。本白皮书系统阐述AI时代企业安全计算架构的目标、边界、能力、底座、协作、管理过程与验证七个层次，并将绝对化的技术表述改写为有条件、可测试、可追责的工程要求。

V3.0确立了四类数字控制权、五业务域、七层技术架构、NGCC统一计算底座与双AI助理的总体框架。V4.0在此基础上直面两个在V3.0中被隐含假设掉的事实：其一，在部分企业和任务类别中，公域模型能力可能强于现有私域模型，差距及其持续性须按任务评测；其二，人在工作中会使用可及范围内最强的工具，追求效率是理性行为而非纪律问题。任何仅在控制“松紧”之间调节的方案都无法脱离由这两个事实构成的动力学。V4.0由此提出两条新的总体判断：能力在哪，边界就设在哪；执行可在S3，管理只在S4。

本版同时完成与《下一代商用计算机（NGCC）技术架构白皮书》V4.22的口径对齐：NGCC以云端真机为核心，PANSTONE CPC与PANSTONE DPC经桌面管理系统（DMS）统一纳管，计算位置与使用位置解耦。这为“人+AI多主体、多机、多网、多域并行工作”提供了物理基础，也使本白皮书关于S4、受控公域与开放公域分别承载于独立真机环境的表述有了工程依据。

文档定位本白皮书提出可讨论、可实现、可验证的技术架构参考。文中涉及的架构名称与分层模型为邦彦技术研究框架，不替代法律法规、国家标准、行业标准或客户安全制度。四类数字控制权、五业务域、三层信任、双AI助理模型与管理过程四环节是研究框架而非监管分类；PANSTONE CPC与PANSTONE DPC是其中的工程化实践。

本过程稿依据2026年9月19日品牌定义复核产品用语：国内产品品牌为邦彦磐石，国际产品品牌为PANSTONE；本稿目标市场待确认，暂保留原稿PANSTONE命名。DMS归属CPC产品体系，可按适用配置统一纳管CPC与DPC。来源V4.0 / V4.2的历史演进叙述予以保留。

原V4.0主要修订

修订维度	本版调整
设计起点	按任务评测私域与公域能力差距，并考虑员工对效率的需求；边界设计不再以“把工作留在受控环境”为隐含目标，而以“把治理推到能力所在处”为目标。
S3业务域	拆分为受控公域与开放公域两层；明确S3与S4仅经网闸相连；S3只承担任务执行，不承担任何管理环节。
S4↔S3边界	以禁入数据类替代对全部出域内容的控制；新增“S4侧传输区—网闸—S3侧安全代理”三段传输结构；控制随数据标签与任务上限收敛，常规跨越自动放行。
管理过程	新增第八章：采用目标管理与自我控制的术语，以设定目标、组织、激励与沟通、衡量、培养人才五项基本作业组织为目标设定与分解、组织执行与自我控制、成果衡量与绩效测评、沟通激励与人才培养四个环节，明确各环节的工作域全部在S4；成果提交是执行结果进入衡量的唯一入口。
三层信任	双AI助理保留为体验层叙事，底层由私域、受控公域、开放公域三层信任承载；受控公域由企业账号、企业协议、NGCC纳管环境、企业存储四要素构成。
三种姿态	给出隔断、受控传输、受控公域常态化三种边界姿态的成立条件与代价；明确隔断的适用条件与旁路风险，避免以隔断替代完整治理。
能力差距管理	按任务类别量化私域与公域能力差距（G0–G3），作为路由、投资与姿态决策的依据；能力买进优先落S4。
NGCC对齐	第五章按NGCC V4.22重写：云端真机、业务计算域、CPC/DPC统一资源池、计算位置与使用位置解耦；网闸与NGCC隔离传输域分工。
去标识不等于去上下文	L2内容的最小化从删除改为假名化与抽象化保结构：标识按主数据字典替换、数值换为区间、保留关系与逻辑；S4保管映射，成果回域后再水合。受控公域由此能承载带上下文的高质量创造。
三级配置	按组织资金与技术条件给出一级（无私域AI）、二级（轻量私域AI）、三级（完整私域AI）三种完整可用的配置及升级触发条件；管理过程在S4与规则型出口把关不依赖私域AI。
Agent治理	硬约束由六项增至七项（新增委托链衰减）；Agent产物进入待提交区，同受提交确认约束；Agent记忆、向量库与缓存须明确域归属与保留期。
威胁与验证	威胁模型增加治理外漂移、管理环节外移、服务方侧数据使用、提交通道断裂等；指标体系增加“管理过程在S4”与“提交入口”两类；附录C给出S4↔S3验收用例。

执行摘要

企业AI建设首先是责任边界的重构，其次才是模型、算力和应用的选择。当 AI开始代表员工读取数据、调用工具、执行任务时，企业必须先回答一个基础问题：计算在哪里发生，数据在哪里停留，AI能够看见什么，Agent能够执行什么，工作在哪里被衡量与测评，以及企业如何持续证明这一切仍然处于控制之中。

本白皮书提出一套自上而下的参考架构：四类数字控制权回答“企业必须守住什么”，五业务域回答“边界划在哪里”，七层技术架构回答“能力部署在哪里”，下一代商用计算机（Next Generation Commercial Computer, NGCC）回答“计算如何被统一承载”，私域、受控公域、开放公域三层信任与双AI助理回答“员工如何使用这些能力”，管理过程四环节回答“工作在哪里被衡量与测评”。这六个视角不是相互独立的概念，而是同一参考架构的不同切面。

在边界设计上，本白皮书提出两条总体判断。其一，能力在哪，边界就设在哪：工作发生在能力所在的位置，架构不把工作拉回边界内，而把治理推到能力所在处；当公域模型能力强于私域时，把公域的相应部分纳入企业治理，形成受控公域，控制对象从“哪些工作必须留在内网”收窄为“哪些数据不能进入公域”。其二，执行可在S3，管理只在S4：目标设定与分解、组织执行与自我控制、成果衡量与绩效测评、沟通激励与人才培养四个管理环节全部在企业业务域内进行，S3只存在于工作执行之内；工作重心在管理过程运转的地方，因此S4不会退化为资料区，S3也不会成为治理之外的主工作区。

在治理层面，本白皮书维持三条基本判断并补充一条：私域 AI与公域AI应统一体验、分层运行，安全代理是控制点但不能代替任务必要性判断、数据最小化与人工责任；Agent必须被当作新的任务执行主体来治理，权限应与任务、身份和时限绑定，高影响动作保留人工确认；任何安全、性能与可靠性承诺都应同时给出适用条件、测试方法与证据来源；以及，隔断应结合监管要求、真实业务需求和旁路控制评价；在仍需公域工作的场景中，单纯切断通道可能降低可见性。

核心判断 AI时代的安全计算，不是把全部能力封闭起来，而是在清晰边界内配置可用能力，让执行去能力所在之处，让管理留在承诺与责任所在之处，并持续证明控制仍然有效。

第一章 AI 改变了企业信息系统的基础假设

企业信息系统已经进入第三次范式迁移：从信息化的“记录流程”，到数字化的“分析数据”再到智能化的“理解、判断与执行”。理解这一迁移，是理解为什么必须重构安全计算架构的起点。

1.1 从记录流程到智能协同

信息化阶段的核心任务，是把线下流程搬到系统中。ERP解决资源记录与计划，CRM解决客户和商机过程，PLM解决产品数据和研发协同，OA解决组织流程。这一阶段系统的价值，主要体现为标准化、留痕与管理透明度的提升。

数字化阶段的核心任务，是让系统中的数据可以被分析和运营。数据仓库、数据中台、BI看板、主数据管理与实时指标体系，让企业从“事后统计”走向“过程感知”。但在这一阶段，系统仍然主要是人的工具：人提出问题、人进行判断、人执行动作。

智能化阶段发生了根本变化。大模型可以理解非结构化知识，把自然语言转换为查询、代码和操作指令；Agent可以围绕目标拆解任务、调用工具并持续执行。企业系统不再只是数据和流程的容器，而开始成为人、模型、知识、工具和Agent共同工作的智能运行环境。安全架构的保护对象，从“数据与系统”扩展到了“数据、系统、模型、执行主体与责任链”。

1.2 四个长期假设同时失效

无论企业信息系统如何演进，背后长期存在四个默认假设。AI时代，这些假设正在同时失效。

- 假设一：终端是主要计算载体。AI调用、浏览器插件、同步盘和本地缓存，使终端成为复杂的数据汇聚点；终端一旦失控，企业难以证明核心数据的完整流向。
- 假设二：内网天然可信。零信任架构强调，不应仅因网络位置或资产归属而隐含授予信任；AI时代还需要持续验证调用主体、数据等级、模型来源和任务目的。
- 假设三：人是唯一执行者。Agent可以获得临时凭证、调用接口、生成文件、发送消息和触发流程，权限治理必须从“管人”扩展为“管人、模型与Agent”。
- 假设四：安全与效率可以通过控制的松紧来平衡。当公域模型能力强于企业私域模型时，控制越严，员工越倾向于直接在互联网侧工作并以手工方式携带企业上下文；控制越松，企业数据越以自然语言形式流入公域模型。松紧调节无法脱离这条曲线，边界设计必须换一个坐标系。

1.3 新型风险从文件外泄扩展到语义、行动与治理

AI带来的风险，不是给旧风险清单增加几条，而是改变了风险的性质。第一类是语义型数据外泄：传统数据防泄漏（Data Loss Prevention, DLP）技术擅长识别身份证号、银行卡号、关键词和文件指纹，但员工可能把核心算法、合同背景或客户策略改写为自然语言后提交给模型——风险不再只是“文件是否被拷走”，而是“知识是否被语义化带走”。

第二类是Prompt注入与工具劫持：恶意指令可以隐藏在网页、邮件、文档或外部数据中，引导Agent忽略原有规则、调用不应调用的工具。输入内容不再只是数据，也可能成为改变执行逻辑的指令，这类风险已被开放全球应用安全项目（Open Worldwide Application Security Project, OWASP）列为大模型应用的重要安全风险。第三类是Agent权限扩散：一个任务可能经过多个模型、多个Agent和多个工具，形成长链路执行，若使用长期静态权限，任何环节被突破都可能带来横向移动与持续访问。第四类是责任不可解释：AI生成的分析可以影响合同、投资、研发、财务和人力决策，企业不仅要保存结果，还要能够回答谁发起、使用了什么数据、调用了哪个模型、经过哪些工具、由谁复核、最终由谁承担责任。

第五类是治理外漂移：当受控环境内的AI能力弱于公域、且通往公域的合法通道狭窄时，工作重心会迁移到个人账户与不可见路径上，企业在不知情的情况下失去对账号、协议、环境与产出的治理；更进一步，目标讨论、过程推进与成果定稿可能都在企业管理系统之外完成，只把最终文件放回内网，形成“管理环节外移”。这类风险不表现为一次事件，而表现为组织能力沉淀地的缓慢转移。

本章结论 AI不是给旧系统增加了一个新功能，而是增加了新的数据使用者、新的执行主体、新的责任链和新的漂移动力。只做模型接入而不重构架构，会把效率提升建立在不可见、不可控、不可审计的风险之上；只做封闭而不面对能力差距，会把风险从可见通道推向不可见通道。

第二章四类数字控制权与总体设计原则

AI时代企业首先需要回答的，不是选择哪一个模型，而是企业对计算、数据、AI能力和组织协同是否仍然拥有完整控制权。本章提出四类数字控制权与十项总体设计原则，并说明它们与后续架构的关系。

同一参考架构的六个视角

01 控制目标	四类数字控制权 计算 · 数据 · AI能力 · 组织协同
02 业务边界	五业务域 S5核心 / S4企业业务 / S3访问代理 / S2 Agent / S1生态
03 能力部署	七层技术架构 从终端访问到外部生态服务
04 计算承载	NGCC统一计算底座 CPC云端真机 · DPC双主机 · DMS授权纳管
05 员工体验	三层信任与双AI助理 私域 · 受控公域 · 开放公域
06 组织管理	管理过程四环节 目标 · 组织与自我控制 · 衡量 · 沟通培养

验证证据链：架构主张 → 适用条件 → 测试方法 → 原始证据 → 有范围的结论

图2-1 AI时代企业安全计算参考架构：六个视角

2.1 四类数字控制权

为了避免概念泛化，本白皮书把企业在AI时代必须拥有的基本控制权，归纳为计算控制权、数据控制权、AI能力控制权与组织协同控制权四类。它们共同决定企业能否保持安全、连续和自主发展。

控制权	核心含义	失控后果	主要架构抓手
计算控制权	计算能力运行在企业可管理、可审计的环境中	分散终端和外部平台成为不可治理的计算入口	NGCC统一计算底座、DMS纳管、身份与策略控制
数据控制权	核心数据始终在授权范围内被处理和存储	AI调用、缓存和工具链导致数据外流；隔断后外流转入不可见路径	分级分类、禁入数据类、S4↔S3三段传输结构、最小化与审计
AI能力控制权	企业拥有可选择、可替换、可沉淀的AI能力	完全依赖外部模型，企业知识无法形成内部能力	私域AI平台、能力差距管理、受控公域企业化、模型路由与评测
组织协同控制权	企业自主定义人、AI和Agent的分工与责任	AI使用碎片化、责任不清、管理环节外移、效率无法沉淀	管理过程在S4、成果提交唯一入口、岗位Agent、人工复核与责任机制

2.2 十项总体设计原则

四类控制权提供目标，落地则需要一组可操作的设计原则。以下十项原则贯穿全书，是判断具体方案是否合理的基本尺度。

- 边界优先。先定义数据、业务和AI调用边界，再选择模型和工具。边界不清晰，能力越强，风险越难治理。
- 能力在哪，边界就设在哪。工作发生在能力所在位置。架构不把工作拉回边界内，而把治理推到能力所在处：能力在私域，边界在S4；能力在公域，则把公域的相应部分纳入企业治理，边界随之外移。边界外移改变的是治理覆盖范围，不改变管理过程所在的位置。
- 执行可在S3，管理只在S4。目标设定与分解、组织执行与自我控制、成果衡量与绩效测评、沟通激励与人才培养四个管理环节全部在S4；S3只存在于“组织”作业分配出去的工作执行之内，是执行者可选的能力之一，不是管理者五项基本作业的任何一项。
- 边界划在数据类，不划在工作。控制对象是“哪些数据不能进入S3”，而不是“哪些工作必须留在S4”。禁入清单窄而明确，因此守得住；“工作留在S4”宽而模糊，因此守不住。
- 私域优先是路由规则，不是禁令。接触企业内部数据和知识的任务，在私域能力够用优先由私域处理；能力不够时，任务在受控公域执行，由禁入清单约束可携带的数据，不以私域优先为由禁止任务本身。
- 底座统一。身份、计算环境、安全域、终端和策略应在统一控制面下管理，减少分散终端形成的旁路。
- 能力分层。私域、受控公域、开放公域三层分别运行，避免一个万能入口获得过度权限；跨层传递最小化。
- 最小授权。权限随身份、任务和时间动态授予；Agent完成任务后应及时回收凭证；委托链上的权限只能衰减，不能放大。
- 以目标与成果自我控制，不以过程监视。自我控制指执行者依据目标衡量自己的绩效与成果，而不是被由上而下地支配。衡量所需的工作项状态与已提交的阶段成果在S4提供给执行者本人和上级；管理者不进入S3，也不需要知道执行者在S3做了什么。这与“人的工作不是控制对象”一致。
- 全程可审计。关键调用、跨域传输和执行过程应形成身份、任务、数据标签、模型、工具、结果与复核人的完整证据链。

2.3 一套架构、六个视角

四类控制权、五业务域、七层技术架构、NGCC、三层信任与双AI助理、管理过程四环节，不是六套相互独立的概念，而是同一参考架构的不同视角：四类控制权回答“企业必须守住什么”；五业务域回答“边界划在哪里”；七层架构回答“能力部署在哪里”；NGCC回答“计算如何被统一承载”；三层信任与双AI助理回答“员工如何使用这些能力”；管理过程四环节回答“工作在哪里被衡量与测评”。理解它们的这种关系，是避免把架构拆成互不相干的产品堆叠的关键。

第三章五业务域：重新划定业务、数据与 AI 边界

五业务域不是简单的网络分区，而是把安全等级、业务属性、AI调用权限和跨域数据规则统一起来的逻辑边界模型。它是四类控制权落地的第一层抓手。



图3-1 五业务域与受控数据流

3.1 五业务域定义

业务域	定位与典型内容	AI使用原则	连接原则
S5 核心域	源代码、核心算法、密钥、最高等级研发资产	公有AI不得直接访问原始数据；确需AI时使用域内可信能力或经审批的处理结果	不与互联网建立通用连接；与S4仅保留固定用途、受控传输路径
S4 企业业务域	ERP/CRM/PLM/MES、财务、人力、供应链、数据平台、目标管理系统与私域AI；管理过程所在	按身份和数据权限调用私域模型、知识库和专有Agent；在非管理任务且数据规则允许时，经三段传输结构使用受控公域；管理环节仍在S4	与S3仅经网闸相连；出域受禁入数据类与任务标签上限约束；入域内容只作为数据
S3 互联网访问与安全代理域	网闸外侧；分受控公域（企业账号、企业协议、NGCC纳管环境、企业存储）与开放公域（会话级、无成果驻留）两层；含安全代理	只承担任务执行；受控公域可执行禁入清单以外的任务，开放公域仅接触公开信息	作为S4与互联网之间的唯一传输侧；不承载目标管理、业务系统、审批流与知识库
S2 Agent执行域	访问互联网或调用公有模型的任务沙箱	Agent按任务获得临时权限，网络和工具采用白名单	不得直接访问S5；产物经S3侧安全代理与结果通道入域，进入待提交区
S1 外部生态域	官网、客户门户、伙伴平台、开放API与对外服务	仅使用公开或经授权数据，按对外服务要求治理模型	面向互联网开放，通过网关、身份与接口保护内部服务

V4.0对S3和S4的定义做了两处实质调整。S3被拆分为受控公域与开放公域两层，并明确它只承担任务执行；S4被明确为管理过程所在，目标管理、业务系统、审批流、测评与知识库只在S4可达。两者仅经网闸相连，不存在透明网络路径。本白皮书所称网闸，指部署在S4与S3之间的安全隔离与信息交换设备，其应用级摆渡与文件摆渡能力以所用型号为准。这两处调整分别对应第七章与第八章。

3.2 系统归域不是一次性网络改造

系统归域应同时考虑数据敏感度、业务影响、外联需求、AI使用方式和故障影响。一个系统可以由多个组件构成，但每个组件必须有明确的域归属；跨域接口应单独登记，不能因为逻辑上属于同一业务就默认互信——很多安全事件恰恰发生在“同一业务、不同组件”之间被默认打通的地方。

域不是物理设备的——映射。高风险边界可以采用物理隔离、固定方向装置或专用通道；中低风险边界可以采用零信任、网关、应用接口和细粒度策略。隔离强度应与数据等级和业务后果相匹配。下表给出系统归域时必须回答的问题。

归域问题	必须回答的内容
资产是什么	系统、数据集、模型、知识库、Agent、接口和责任人
风险有多高	数据敏感度、可用性影响、错误执行后果和外部暴露面
需要连接谁	方向、协议、数据类型、频率、控制装置和例外条件
由谁批准	业务负责人、数据负责人、安全负责人和系统负责人
如何证明	配置基线、策略版本、日志、测试记录和定期复核

3.3 跨域数据流的两种控制方式

低频、大颗粒的跨域传输（如S5与S4之间的固定用途传输）适用四步控制：判断必要性、执行最小化、控制返回、保留责任。这类传输可以逐次审批，网关是控制点而非无限责任的保险箱。

S4与S3之间的传输是另一种性质：高频、小颗粒、语义化，一次外部研究可能有几十次问答往返，逐次审批不可能，仅靠抽样DLP不足以覆盖全部语义风险。这条边界采用禁入数据类、标签动作与任务上限的组合：

标签	受控公域	开放公域	说明
L0 公开	放行	放行	零阻力
L1 内部一般	放行（去标识）	拒绝	可在受控公域执行任务
L2 内部敏感	假名化与抽象化保结构后经请求通道或文件通道出域；S4保管映射，回域再水合；优先路由私域	拒绝	异步审计抽样，不阻塞流程
L3 受控	拒绝；强制私域	拒绝	禁入清单主体；不得以一般审批绕过禁入约束
L4 核心（S5范围）	不进入本结构	不进入	出现即为事件

去标识不等于去上下文。L2内容的最小化不是删除，而是假名化与抽象化保结构：客户名替换为角色标签、金额替换为区间或相对值、人名替换为岗位、项目代号替换为编号，保留关系、逻辑、数量级与文档结构；S4侧保管映射表，成果回域后按映射再水合为真实数据。受控公域由此获得结构完整的上下文，能够进行高质量推理。替换所依据的标识——客户、项目、员工、供应商、产品型号——本来就在ERP、CRM、HR的主数据中，可以枚举，因此假名化可以由规则与字典实现，不依赖大模型。

禁入清单应窄、明确、可由分类器识别，典型包括：S5相邻内容、客户与员工个人信息原始形态、合同与协议原文及未公开商务条件、未公开财务数据与经营决策材料、明确标注 L3以上的任何内容。目标分解到工作项时附带的数据标签上限与此表叠加：任务上限为 L1时，L2内容即使可最小化也不出域。等级数量与名称按企业实际分级体系调整。

3.4 S4↔S3三段传输结构

S4与S3之间的传输由三段构成，判断在S4侧，执行在网闸，代理在S3侧。网闸之外的一切不可信任，出域敏感性与许可判断只能在S4侧完成；S3侧返回内容检测不改变该责任边界。

段	位置与信任	核心职责	明确不承担
第一段 S4侧传输区	S4内网，可信	出域准备区：会话与任务绑定、分类（语义分类器或规则型）、路由决策、假名化与抽象化、映射保管、额度与熔断、封装、留痕。 入域暂存区：隔离、数据模式消费。待提交区：再分类、再水合、任务归属、提交确认	出网
第二段网闸	物理边界；设备可信，两侧流量不可信	四条通道（请求、文件、结果、提交）的格式白名单、物理摆渡、双向留痕、标签与任务标识合法性校验	语义判断、路由、内容改写

段	位置与信任	核心职责	明确不承担
第三段 S3侧	互联网侧；受控公域受企业治理但不获S4信任	安全代理：出网执行、企业凭证托管、返回内容检测、活动内容剥离、来源标记。受控公域执行环境与短保留期企业存储。开放公域会话级环境	持有或访问禁入数据；访问S4资源、目标管理系统与业务系统

网闸“只过定义好的格式”的限制，恰好是最小化的执行机制：结构化出域请求只含问题文本与元数据，不含附件与原文；出域文件仅允许L0/L1及假名化后的L2，并携带标签、任务标识与把关结果。网闸是否支持应用级摆渡决定受控传输的交互体验，仅支持文件摆渡时更多任务的执行落入受控公域。三段结构的完整设计、通道定义、失效行为与验收用例见附录C。

第四章七层技术架构：让能力有明确落位

五业务域是横向的安全与业务边界，七层技术架构是纵向的能力栈。二者叠加，才能明确每项能力运行在哪里、受谁控制，避免安全架构和业务架构各自为政。

七层能力栈与五业务域分别建模

L7	外部生态服务	客户 / 伙伴 / 开放API
L6	公有AI与Agent执行	受控执行 / 企业协议 / 沙箱与授权
L5	互联网访问与安全代理	网闸 / 安全代理 / 返回内容预处理
L4	企业私域AI平台	模型 / 知识 / RAG / 路由与评测
L3	业务与数据中心	业务事实 / 目标管理 / 主数据
L2	统一计算基础设施	CPC / DPC / DMS / 单环境单安全域
L1	终端访问	显示输入 / 身份接入 / 受控外设

此图L1–L7表示技术层；数据标签L0–L4另按第3.3节解释。

图4-1 AI时代企业计算七层技术架构

4.1 七层能力栈

层级	主要能力	关键责任
L7 外部生态服务	客户、伙伴、开放API与互联网服务	隔离外部访问与内部系统，约束公开数据和对外模型
L6 公有AI与Agent执行	受控公域执行环境、公域模型企业服务、公网研究、外部工具任务	企业账号与协议、沙箱、白名单、临时权限、熔断和人工确认
L5 互联网访问与安全代理	网闸、S3侧安全代理、企业凭证托管、返回内容检测、入域预处理	格式白名单、物理摆渡、注入检测、活动内容剥离、来源标记与审计
L4 企业私域AI平台	私有模型、知识库、RAG、模型路由、语义分类器、能力差距评测与私域Agent	继承业务权限、知识治理、出域分类与最小化、评测和可追溯回答
L3 业务与数据中心	ERP/CRM/PLM/MES、目标管理系统、数据平台与主数据	提供经营事实、任务身份、接口契约和数据责任
L2 统一计算基础设施	NGCC：CPC云端真机、DPC双主机、DMS统一资源池、隔离传输与管理控制面	承载计算控制、单环境单安全域、多域访问、计算位置与使用位置解耦
L1 终端访问	显示、输入、身份接入和多域入口	终端降权、设备准入、受控外设和会话安全

4.2 域与层的映射关系

业务域回答“什么可以彼此信任和传输”，能力层回答“控制由哪一层实现”。例如，S4中的私域AI主要落在L4，但其身份来自统一身份体系、数据来自L3、计算由L2承载、交互通过L1进入；S3受控公域跨越L5与L6，其执行环境由L2承载，其账号与协议属于L6的治理对象，其出网与入域预处理属于L5。任何单层产品都无法独立完成完整控制。

同一技术层可以为多个业务域提供能力，但必须保持资源、网络、身份、密钥和日志的边界。统一计算基础设施可以同时承载S5、S4与S3的真机环境，但每个环境固定归属一个安全域，控制面不得把“统一运维”变成跨域旁路。

架构检查如果一项AI能力无法说明其业务域、技术层、数据来源、工具权限、责任人与验证证据，就不应直接进入生产环境。如果一项工作无法说明其任务标识、数据标签上限与可用能力层，就不应在受控公域执行。

第五章 NGCC：统一计算底座

NGCC的作用不是替代所有PC，而是在高安全、多安全域、高性能与规模化治理并存的场景中，提供一组可验证的组织级计算约束。它处于七层架构的L2，是计算控制权与终端降权的物理基础，也是“人 + AI多主体、多机、多网、多域并行工作”的物理载体。本章按《下一代商用计算机（NGCC）技术架构白皮书》V4.22口径重写。



图5-1 NGCC三域分离、DMS统一纳管与S4、受控公域、开放公域的真机映射

5.1 从设备中心转向计算责任中心

如果终端仍然是本地计算和数据存储的主体，企业就很难统一约束不同域的访问，也很难对本地模型、浏览器插件、移动存储、缓存与离线副本形成一致控制。私域AI平台可能建设得很先进，但员工仍然可以绕过统一入口，把数据发送给外部工具。

NGCC是面向产业开放的新品类及架构范式；BANGYAN NGCC表达邦彦的提出者身份，PANSTONE CPC/DPC是具体产品实践。NGCC以云端真机为核心，以独立物理计算单元承载用户操作系统、应用和业务数据，通过终端接入域、隔离传输域与业务计算域的三域责任分离，以及归属CPC产品体系的桌面管理系统（DMS）对用户、终端、真机环境、资源与策略的统一纳管，把“谁可以使用什么计算环境、该环境属于哪个安全域、允许连接什么网络、可以挂载什么存储、可以使用什么外设”变成架构层面的约束。远程桌面交互是使用真机的方式，不等同于虚拟化；虚拟化云PC实例仅为特定场景的例外配置。

5.2 CPC、DPC与统一资源池

PANSTONE CPC（Cloud Physical Computer，云端物理计算机）以云端真机提供受控计算环境，将终端交互与业务计算分离，以云端真机、适用专用终端的零数据目标及经验证的结构级物理隔离建立安全计算边界。PANSTONE DPC（Dual-Host PC，双主机计算机）在一台设备中集成两个独立物理主机，一机双主、物理分域，支持本地独立计算。DPC接入DMS后，两个主机分别纳管，与CPC云端真机组成统一资源池：用户通过CPC系统终端可访问获得授权的DPC主机，也可通过DPC访问获得授权的CPC环境。

这一体系的核心含义是计算位置与使用位置解耦：一个用户可以从一个终端同时接入多个真机环境，每个环境固定归属一个安全域，环境之间保持结构级物理隔离；访问授权不自动包含环境之间的数据传输授权，传输只能经获准路径进行。这正是多主体、多机、多域并行工作的物理基础：并行发生在多个独立真机上，而不是在一台设备的多个窗口里。

5.3 S4、受控公域、开放公域的真机配置

S4、受控公域与开放公域在同时运行时，应分别承载于独立的NGCC真机环境，固定归属各自安全域，在适用的DMS管理边界内分别纳管、分别授权。单台DPC只有两个独立物理主机，可同时承载S4与一种公域环境；如需三层同时运行，应增加独立的CPC或其他获准真机资源。下表中的主机二为互斥配置选项，不表示同一主机同时承载两个信任层。

环境	CPC配置	DPC配置	持久化与数据
S4	持久实例；承载目标管理系统、业务系统访问与私域AI	主机一	S4企业存储；管理过程所在
受控公域	互联网区持久实例；挂按任务组织的短保留期企业存储	主机二（持久配置，与开放公域选项互斥）	产物按任务短期驻留，经提交通道同步至S4
开放公域	互联网区会话级实例；结束即复位	主机二（会话级复位配置，与受控公域选项互斥）	无个人存储，无成果驻留

NGCC负责计算环境的域归属、真机承载与终端接入隔离；网闸负责S4与S3业务网络之间的数据传输。NGCC的隔离传输域解决终端到真机的交互，不涉及业务网络间的数据流动，二者不混用。DPC主机二按部署配置承载受控公域或开放公域之一；改变域归属须完成数据清除、凭证撤销、环境重建与验证，不能以窗口切换替代隔离，用户在一台设备上完成执行与管理动作的切换，跨主机数据仍只经网闸。终端零数据仅针对经验证的CPC专用接入终端；软件客户端另评宿主风险，DPC业务主机允许按域策略在本地保存数据，开放公域无成果驻留针对会话级计算环境，受控公域产物按任务短期驻留并同步提交，三者对象不同，分别验证。

5.4 与独立NGCC白皮书的边界

本白皮书对NGCC的引用，聚焦于它在企业整体安全计算架构中的角色，而不重复其内部实现细节。NGCC技术白皮书回答“如何按产品形态验证终端数据驻留、结构级隔离、单环境单安全域、独立真机与专属计算资源”，属于L2的实现问题；本白皮书回答“企业整体如何用五业务域、七层架构、三层信任、管理过程四环节配置与治理AI能力”，属于跨层跨域的体系问题。两者共享同一套三域定义与验证证据链，但不互相替代。

在AI工作负载下，NGCC需要坚持三条边界：AI计算环境仍固定归属一个安全域，私域AI环境与公域Agent环境不得共用同一真机或跨接互不信任网络；GPU显存、算力与数据吞吐按真机环境归属与隔离，共享配套资源不改变真机主体；模型镜像、知识库挂载与临时任务数据纳入环境生命周期，任务结束后按安全域内清除与审计要求处置。

第六章企业私域 AI 平台、知识治理与能力差距管理

企业私域AI平台是把AI能力沉淀为企业内部资产的中枢。它的价值不在于拥有多大的模型，而在于能否在受控环境中，把企业知识、模型能力与业务权限安全地组合起来，并诚实地知道自己与公域能力的差距在哪里。本章能力按第十二章的三级配置选用：一级配置的组织可暂不具备本章大部分能力，这不影响第三章的出口把关与第八章的管理过程成立。

6.1 私域AI平台的七项能力

- 私有模型与模型路由：在受控环境中运行自有或授权模型，并根据任务类型、数据等级、能力差距和成本，把请求路由到私域模型或经三段传输结构路由到受控公域。
- 知识库与检索增强生成（Retrieval-Augmented Generation, RAG）：把企业知识以可控、可追溯的方式提供给模型，答案可回溯到来源文档。
- 权限继承：AI对数据的可见范围，继承用户在业务系统中的权限，而不是获得超越用户的“上帝视角”。
- 语义分类器：对待出域内容做语义级分类，识别改写、转述、摘要形态的禁入内容，输出数据标签，为S4侧出口把关提供判断；语义分类器可增强对改写内容的识别；一级配置按第12.2节采用规则与主数据字典，并单独记录语义漏检风险。
- 模型评测与能力差距评测：对准确率、幻觉率、时延、成本与安全性进行持续评测，并以相同任务集对比私域与受控公域模型，按任务类别输出差距等级。
- AI工作台：为员工提供统一的交互入口，把 AI能力嵌入岗位 workflow；工作台的默认座位在S4，公域能力的调用从S4经通道发起。
- 私域Agent：在受控范围内执行内部任务的Agent，其工具、数据与权限均在企业治理之下。

6.2 知识治理比模型参数更接近企业价值

对多数企业而言，真正的竞争力不在于模型有多大，而在于能否把分散、异构、时效不一的企业知识，治理成可被AI安全、准确调用的资产。知识治理包括知识的采集、分级、清洗、更新、权限标注与质量评估——没有良好的知识治理，再强的模型也只能给出“看起来专业但可能错误”的答案。

知识治理直接关系到安全和管理过程。知识的分级决定了哪些内容可以进入RAG、哪些只能在更高安全域处理；知识的权限标注决定了不同用户通过 AI能看到什么；知识的来源可追溯，是AI答案能够被复核、被追责的前提。V4.0增加两条要求：知识库只摄入已在S4提交确认的成果，不摄入任何未提交的受控公域产物或开放公域内容；外部来源知识在RAG中保持独立标签，可降权、可追溯，防止知识投毒扩散。

6.3 能力差距管理

公域与私域模型的能力差距应以企业具体任务集的评测结果为依据。V3.0的“私域优先”原则隐含地假设私域能力够用，V4.0把这一假设改为一个被管理的变量：按任务类别量化差距，让路由、投资与姿态决策以差距为依据。

差距等级	含义	默认处置
G0 无实质差距	私域可替代公域	私域承接；无出域需求
G1 可接受差距	私域略弱但满足业务	私域承接；列入观察

差距等级	含义	默认处置
G2 显著差距	私域明显不满足业务	买进能力，或该类别的任务执行归受控公域
G3 私域不可用	私域无对应能力	任务执行归受控公域；管理环节仍在S4

按能力差距有三类处置：G0/G1由私域承接；G2优先评估能力买进，未买进时在数据规则允许范围内使用受控公域；G3在数据规则允许范围内使用受控公域。能力买进是把接近前沿的能力纳入企业信任范围：开放权重模型私有化部署到S4为首选，模型服务方的专属实例或独立部署形态落在受控公域为次选；优先落S4的理由是，S4的能力越强，落在S3的执行越少，管理过程所在地的引力越稳。接受在受控公域执行适用于G2未买进及G3类别：任务执行在受控公域完成，禁入清单约束可携带的数据，目标、自我控制、衡量与测评仍在S4；组织明确记录哪些类别在公域执行、带了哪些数据、受哪份协议约束。

私域建设的投资优先级不再由“私域优先”泛泛决定，而由差距等级×任务价值×数据敏感度×该类别在S3的执行时长排序：假名化后仍无法保证质量的类别（依赖 L3以上数据）、高价值、G2以上且S3执行时长占比高的类别优先投入，直到差距降到G1。评测集、方法与版本记录在案，模型版本变化后重测。买进的目标不是让S4拥有最强的模型，而是使S4的创造效率逼近受控公域，见6.4。

6.4 使S4的创造效率逼近受控公域

受控公域的高效有五个来源：更强的模型、更多的工具、更新的外部知识、更低的摩擦、更好的交互体验。S4要逼近，需逐项对着补，顺序按投入产出排列如下。

- 把上下文变成效率优势。这是S4可形成效率优势的重要条件。人在S3处理企业上下文仍需经过出口把关、假名化与受控传输，这部分成本不能因工具便利而省略。S4应让上下文零输入：知识库与RAG按用户权限自动挂载；业务系统以工具形式接入私域AI，AI可直接读写用户有权限的对象；工作项级上下文记忆，一个任务的资料、对话与阶段成果随任务携带。做到这一步，带上下文的任务在 S4即使模型弱一档也可能更快。
- 按任务类别买进能力。开放权重的准前沿模型私有化部署，先覆盖6.3排定的优先类别；用路由让简单任务走小模型保证时延、复杂任务走大模型保证质量；对合同、代码、经营分析等有企业语料的领域做微调或蒸馏，专用中等模型在本领域可超过通用前沿模型。
- 补齐工具。S3的效率有相当部分来自工具而非模型。S4内建代码执行沙箱、文档生成、数据分析、内部搜索，具备公有AI产品那种“生成—运行—修改”的闭环。
- 把外部知识引进S4。行业资讯、标准、开源文档、论文等公开语料经受控入域、来源核验与S4责任确认后，定期镜像进S4，作为独立标签的知识源；需要实时外部信息时经请求通道“以问题出域”，人不离开S4座位。
- 拉平时延与体验。推理集群做量化、投机解码与批处理，使响应体感与公有产品一致；工作台支持流式输出、多轮、多模态与历史检索；权限继承自动化，符合标签、任务上限、去标识和策略条件的L0/L1请求自动处理，例外处理须复核数据分类与适用依据，不得直接放行仍属禁入类的内容。体验差本身就是漂移引力，应作为第十三章指标跟踪。
- 沉淀人的能力。岗位提示词与技能库在S4共享，一个人摸索出的高效用法成为组织资产；岗位Agent固化重复工作；培训聚焦深度思考与AI运用两项能力。

衡量方式：对每个任务类别用同一任务集，比较S4与受控公域达到可接受结果的时间与质量评分，得出创造效率差距；目标是优先类别降到G1，而不是全部追平。实施顺序：先做上下文与体验，不依赖新模型、见效最快；再做买进与工具，属投资决策；外部知识与人的能力持续进行。差距随任务和模型版本变化，应持续评测而不预设永久领先关系；目标是让带上下文的创造留在S4。

第七章人性、能力差距与三层信任

企业员工的工作天然包含两类任务：处理内部数据与流程，以及获取外部信息与调用公有能力。V3.0以双AI助理回答这一问题。V4.0保留双AI助理作为员工体验层的叙事，但把底层信任结构从二分改为三层，并在开篇直接写出边界设计必须面对的两难。

7.1 两难与三种失效形态

当公域模型在有关任务中强于现有私域能力时，员工可能倾向于使用更高效的工具。由此形成的动力学是：控制越严，合法通道越窄，人越倾向于直接在S3工作并以手工方式携带企业上下文；控制越松，企业数据越流入公域模型。在这条曲线上调节松紧，无论调到哪里，都会落入以下三种失效形态之一。

失效形态	表现	后果
隔断	切断S4↔S3全部联系	人不会停止在S3工作，只会停止使用可见通道；企业上下文经手工转录、拍照、个人账号进入S3。隔断消灭的不是泄露，而是对泄露的观测，同时使企业丧失对S3侧账号、协议、环境与产出的治理。当业务仍依赖公域而又缺少配套约束时，隔断可能使活动转入不可见路径。
放任	全部工作在S3完成，S4退化为记录场所	企业知识在公域模型上下文中积累而不在企业内沉淀；这一后果发生得慢，但更难逆转。
管理环节外移	S3已企业化、边界已划在数据类，但目标在S3讨论、过程在S3推进、成果在S3定稿，只把文件放回S4	企业虽握有账号与协议，但承诺、衡量与测评发生在管理系统之外；S4成为资料区。

本白皮书的两条总体判断分别针对前两种和第三种失效形态：能力在哪，边界就设在哪，使企业不必在隔断与放任之间选择；执行可在S3，管理只在S4，使S3企业化之后不会演变为管理环节外移。

7.2 三种边界姿态及其成立条件

组织在S4↔S3边界上只有三种可选姿态，每种姿态在特定条件下是理性的，条件不满足时即失效。这张表供决策层使用。

姿态	描述	成立条件	失效表现	代价
A 隔断	切断S4↔S3全部联系	人确实不需要在S3执行任务，或S3执行不涉及企业上下文	手工转录、拍照、个人账号；观测归零	限制公域能力使用；需投入旁路防护，并评估效率与可见性代价
B 受控传输	S4为执行域，公域能力经三段传输结构调用	私域能力覆盖多数任务；网闸支持应用级摆渡；标签体系成熟	通道慢于旁路时发生漂移	私域模型持续投入
C 受控公域常态化	任务执行的一部分在受控公域完成；管理过程在S4。一级配置（无私域AI）的组织默认姿态	企业账号与协议可落地；受控公域可纳管；禁入清单可执行；目标管理系统可提供任务身份；成果提交为唯一入口	禁入失守；提交通道断裂；管理环节被拖入S3	接受部分执行在企业治理下的公域完成；对服务方的合同信任

本白皮书推荐的默认姿态是C与B的组合：任务类别按第六章差距等级落在B或C，姿态C以第八章“管理过程在S4”为前提。对第十二章所述一级配置的组织，几乎所有类别都落在C，姿态C即主姿态；这不影响架构成立，因为撑住S4地位的管理过程与出口把关都不依赖私域AI。姿态A仅在其条件下成立，且组织应明确记录选择A的适用依据、替代控制与残余风险。姿态不是一次性决定：能力差距、协议条款、网闸能力变化时，任务类别在B与C之间迁移，第十三章的指标用于触发迁移。

7.3 三层信任：私域、受控公域、开放公域



图7-1 三层信任与双AI助理：统一体验，分层运行

层	位置	模型来源	账号与协议	计算环境	存储	允许的数据类	可承担的管理环节
私域	S4	私有化部署模型	企业内部	S4 NGCC真机环境	S4企业存储	全部（S5另设）	全部四环节
受控公域	S3受控区	公域模型企业服务：企业账号、数据不用于训练、可审计、有条件的专属实例	企业统一签约与托管；个人不持有	S3侧NGCC纳管持久实例，有身份、有日志	S3侧按任务组织的短保留期企业存储	禁入清单以外	仅任务执行
开放公域	S3开放区	任意互联网服务	无企业账号或受限账号	会话级实例，结束复位	无	仅L0	仅任务执行中的信息获取

受控公域的“受控”由四要素构成：企业账号、企业协议、NGCC纳管环境、企业存储。四者缺一，该层即退化为开放公域，允许的数据类随之收缩到L0。受控公域仍处于网闸之外，仍是互联网侧，不因企业化而获得S4的信任等级；

禁入数据类对它同样生效；其网络上不存在目标管理系统、业务系统、审批流、代码库与知识库。企业化改变的是治理覆盖，不是网络位置。

在员工体验层，双AI助理的表述继续有效：私域AI助理承担内部任务，公域AI助理承担外部任务，员工在统一工作台中获得一致体验。V4.0的补充是：工作台的默认座位在S4，公域能力的调用默认从S4经三段传输结构发起；只有当任务允许的数据类与能力层要求在受控公域执行时，员工才切换到受控公域座位。

维度	私域AI助理	公域AI助理
运行环境	企业私域AI平台和受控业务域	受控公域执行环境或S2 Agent域，经S3侧安全代理访问公有模型与互联网
可见数据	在用户权限范围内访问企业内部数据与知识	只接收经出口把关、任务上限约束和最小化处理的信息；禁入数据类不可见
典型任务	企业知识问答、内部分析、合同审查、经营解释	公开资料研究、政策跟踪、竞品信息、外部内容生成
主要风险	越权检索、知识污染、模型幻觉和内部权限滥用	Prompt注入、数据外发、外部工具劫持、内容合规、个人账号绕行
核心控制	身份与数据权限继承、知识分级、模型评测和审计	企业账号与协议、输入最小化、工具白名单、沙箱、返回检测和提交确认

7.4 S3侧安全代理的职责与边界

V3.0中的AI安全网关在V4.0中被三段传输结构的第三段——S3侧安全代理——取代。它位于网闸外侧，是面向互联网的执行者：接收来自网闸的结构化请求，代表企业访问公有模型、搜索与外部工具，托管企业凭证，控制速率与成本，对返回内容执行注入与恶意内容检测，剥离活动内容，强制来源标记，并把结果封装为入域对象。它不持有禁入数据，不具备访问S4的能力，处理过程中的临时数据按会话清理。

必须清醒认识安全代理的边界：它不作企业敏感数据分类、出域许可或任务必要性裁决，这些判断在S4侧完成；S3侧仍执行返回内容的注入与恶意内容检测；它能降低风险，但不能替代任务设计与人工责任。能够由私域能力完成的任务，不应默认发送给公有模型；识别为敏感的内容，在S4侧执行删除、替换、摘要化或结构化处理；对外部网页、文件和工具返回的内容，在S3侧检查以降低隐藏指令的影响，在S4侧以数据模式消费。把安全代理当作“最后一道且唯一一道防线”，本身就是一种风险。

7.5 创造域与质量域

AI时代，人的深度思考与AI运用能力决定工作的能效与质量。就当前能力分布而言，受控公域可能在部分任务上更高效，S4则更便于控制企业上下文；具体结论应经评测。但这一判断需要一个限定：创造的价值大部分来自作用于具体上下文。企业上下文分三层——公开信息（L0）可直接带入受控公域；内部一般信息（L1）须按第3.3节去标识后带入；敏感但可去标识的信息（L2）经假名化与抽象化保结构后带入，回域再水合；受限信息（L3以上）不能带出。前两层覆盖了多数起草与分析所需的上下文，受控公域因此能够产出高质量结果；第三层所依赖的创造只能在相应获准私域环境中进行（L3在S4，L4在S5），是能力买进的优先对象。

命题创造在能力所在处，质量在上下文与衡量所在处。受控公域可承载经评测适合的非受限上下文创造，S4与S5按数据归属承载受限上下文创造；效率的上限由模型能力决定，质量的上限由上下文与衡量决定。

由此，S3的份额收缩是S4能力追上后的结果，不是政策目标。只要差距仍在，受控公域就应在标签允许的范围内携带尽可能完整的上下文；同时，深度思考是稀缺的，边界不能消耗它——人在受控公域理清思路、回S4结合内部数据做判断、再出去验证，这一往返若有摩擦，思考就会中断，人就会选择留在一边。“通道比旁路快”因此不只是防漂移的手段，也是保护深度思考连续性的条件。

第八章管理过程与计算域

本章说明组织既有的管理过程与S4、S3两个计算域的对应关系。管理过程采用《管理的实践》中目标管理与自我控制的术语：管理者的工作由设定目标、组织、激励与沟通、衡量、培养人才五项基本作业构成；本白皮书把它们组织为一个循环的四个环节——目标设定与分解、组织执行与自我控制、成果衡量与绩效测评、沟通激励与人才培养。目标管理、OKR、KPI与PDCA可分别为本过程提供方法、目标或指标支持，但各自含义与环节不应视为完全相同。本章不新增管理制度，只明确每个环节的工作域，以及架构为它提供什么。



图8-1 管理过程四环节与S4、S3计算域的对应关系

8.1 管理过程的工作域

环节	基本作业	管理内容	工作域	架构提供
① 目标设定与分解	设定目标	目标由企业目标逐级推导并分解到个人工作项；管理者参与设定自己的目标；目标聚焦成果、可衡量	S4	目标管理系统；工作项获得任务标识、数据标签上限、可用能力层
② 组织执行与自我控制	组织；衡量（自我控制）	分析活动、决策与关系，把工作分配给合适的人；执行者依据目标衡量自己的绩效与成果并调整工作	分配与自我控制在S4；工作执行在S4或S3，由数据类决定	出口把关与四条通道；工作项状态与阶段成果视图
③ 成果衡量与绩效测评	衡量	建立聚焦成果的衡量尺度；依据目标与成果测评绩效	S4	成果提交是衡量的前提与唯一入口；提交通道、提交确认；测评只认S4
④ 沟通激励与人才培养	激励与沟通；培养人才	让每个人了解对自己的期望与自己的绩效；上下双向沟通；依据目标与绩效培养人，包括管理者自己	S4	反馈、奖惩、晋升、知识资产、经验推广只取自S4

结论四个环节、五项基本作业的工作域全部在S4；S3只出现在“组织”作业分配出去的工作执行之内，是执行者可用的能力之一，不是管理过程的任何一环。工作重心在管理过程运转的地方，管理过程在S4，S4不可能退化为资料区，因为它是承诺与责任所在的地方。

8.2 目标设定与分解（工作域：S4）

目标在目标管理系统中形成，由企业目标逐级推导并分解到个人工作项；每个管理者参与设定自己的目标，并说明对上一级目标的贡献；目标聚焦于成果，并且可以衡量。架构不另建任务登记。

工作项携带三项属性：任务标识；数据标签上限，由目标所涉业务与数据推导；可用能力层，即私域、受控公域、开放公域中允许使用的层。三项属性由执行者参与确定，由目标管理系统传递给DMS与出口把关。

目标提供任务授权依据：任务标识用于关联工作项、执行主体、数据标签上限和成果，但不能单独充当访问凭证。实际访问仍须通过身份认证、DMS显式授权及数据传输策略校验；无有效任务标识或授权的产物不能提交。目标不规定方法：执行者在获准数据标签上限与可用能力层范围内自主选择执行方式。

8.3 组织执行与自我控制（工作域：分配与自我控制在S4，执行在S4或S3）

“组织”作业把工作分配给人，分配在S4完成。分配出去的工作，其执行可使用工作项获准的私域、受控公域或开放公域。执行位置同时受数据类别、任务标签上限与可用能力层约束：L0可在获准的开放公域执行；L1经去标识后可在受控公域执行；L2原始内容留在S4，假名化与抽象化保结构后的必要内容，经出口把关及请求或文件通道进入受控公域执行。L3禁止进入S3，L4保留在S5的相应受控环境。任务上限更严时，按更严规则执行。

自我控制指执行者依据目标衡量自己的绩效与成果，并据此调整自己的工作，而不是被由上而下地支配。自我控制所需的信息——工作项状态与已提交的阶段成果——在S4提供给执行者本人和上级；上级据此进行管理，不进入S3，不查看执行细节。需要衡量的节点在目标设定时约定，到达节点时执行者提交阶段成果，提交在S4完成。报告与程序是管理者的工具，不是控制手段：提交确认不是审批，架构不增设任何面向过程的报表。

绩效管理以目标与已提交成果为依据，不以S3执行细节监控替代自我控制。安全审计按目的限定、最小必要和分权访问保留身份、任务、传输、环境及Agent关键动作记录，用于安全归因与事件处置，不直接作为绩效评价材料。对人工作不实施无差别过程监视；第九章要求的Agent工具调用与高影响动作审计仍须保留。

8.4 成果衡量与绩效测评（工作域：S4）

衡量尺度清晰、简单、合理、聚焦成果，并能被执行者用于自我控制；衡量的对象是成果，不是活动。成果提交是衡量的前提，也是执行结果进入管理过程的唯一入口，只在S4完成。架构为它提供以下支撑，这些是技术保障，不是新的制度。

- 提交通道。受控公域企业存储中的执行产物按任务标识自动同步至S4，单向、批次留痕；产物到达S4后处于“待提交”状态。
- 提交确认。责任人在S4确认待提交产物为本工作项的提交物。确认不是审批，是“这是我提交的成果”的声明；确认后产物获得任务归属并进入衡量与测评。
- 入口再分类。产物在S4入口重新分类；执行中可能结合了新信息，不沿用出域时的标签。
- 短保留期。受控公域存储按工作项设短滚动保留期，工作项完成后即清理。执行产物只能在提交前短暂停留于S3，不能积累。
- 版本权威。S4中提交的版本为唯一权威版本；S3侧只有草稿，不得覆盖已提交版本。
- 对账。周期性比对受控公域存储与S4提交记录，差异计入指标。
- 断裂处置。提交通道连续失败超过窗口为一级事件；期间执行可继续，但工作项不能完成、产物不能提交；恢复后续传并对账。

绩效测评依据目标与已提交的成果，只认S4；S3侧产物无论质量如何，未提交即不存在于测评。

8.5 沟通激励与人才培养（工作域：S4）

沟通以S4中的目标、提交与测评记录为基础，上下双向进行，让每个人了解对自己的期望与自己的绩效。人才培养——奖惩、晋升、知识沉淀、经验推广、进知识库——只取自S4，知识库与RAG不摄入任何未提交的S3侧内容。AI对岗位的贡献通过提交到S4的成果衡量，不另设AI使用量指标；这对应第十章“从使用量指标转向岗位价值”。

8.6 对执行者的一条规则与对组织的一项依赖

执行者规则目标从S4来，成果往S4交；中间在哪里做，由工作项允许的数据决定。

本章对组织管理成熟度有真实依赖：任务标识与标签上限的质量取决于目标管理的颗粒度。目标管理粗放的组织，初期数据标签上限只能按部门或岗位设置，精度较低；本白皮书不要求先改造目标管理，但架构的精度随之提升。建设路线（第十二章）按此分级实施。

第九章 Agent 治理与人类责任

Agent不是普通软件账号，而是带目标、记忆、工具和委托关系的任务执行主体。对 Agent的治理，必须从“管账号”升级为“管执行主体”，并始终保留人类的最终责任。



图9-1 Agent全生命周期治理闭环

9.1 七项硬约束

- 沙箱运行：高风险任务在独立环境执行，限制文件、系统调用和网络访问。
- 工具白名单：Agent只能调用登记、评测和授权的工具，不能自行无限扩展工具。
- 即时授权（Just-in-Time, JIT）：权限与任务、身份、资源和时限绑定，结束后自动撤销。
- 委托链衰减：人→主Agent→子Agent→工具的委托链上，权限只能单调衰减、不得放大，每一跳可回溯到发起人与任务标识。
- 人工确认：付款、发布、删除、代码合并、客户承诺和人员决策等高影响动作必须复核。
- 可熔断：发现越权、异常调用、持续失败或风险信号时立即暂停任务并撤销凭证。
- 可复盘：保留关键步骤、工具调用、输入输出摘要、审批和责任人，支持重放与调查。

9.2 Agent产物与管理过程

Agent与人一样受第八章约束：Agent的工作项在S4分解并携带任务标识与数据标签上限；面向互联网执行的Agent产物经S3侧安全代理预处理与结果通道入域，进入待提交区，同受提交确认约束；未经提交确认的Agent产物不进入业务系统、测评与知识库。Agent的长期记忆、向量库与会话缓存是跨会话的持久数据，其域归属与保留期须明确，不得成为跨域的隐蔽通道。

9.3 三类责任不能转移给模型

业务责任人负责定义任务目标、可接受误差和高影响动作；系统责任人负责运行环境、数据权限、工具边界和异常处置；审批人负责确认特定动作并承担相应组织责任。AI可以辅助判断和执行，但不能成为责任空缺的理由——“是AI做的”永远不能作为免责的借口。

对于高影响任务，应记录发起人、任务标识、委托关系、模型版本、知识版本、工具参数、人工确认和最终系统动作。这些日志不仅用于事后追责，也用于发现Prompt、知识、权限和流程中的系统性问题。上述约束与NIST人工智能风险管理框架强调的治理、测量与持续管理思路，以及ISO/IEC 42001面向人工智能管理体系的要求方向一致。

第十章进入经营：三链协同与代表性场景

AI价值只有进入岗位、流程和责任体系，才能从工具效率转化为组织生产力。企业不能只建设一个平台，还必须定义新的工作单元，并把它放进既有的管理过程。

10.1 三链是AI进入经营的主要载体

企业经营可以概括为收入链、产品链与支撑链三条价值链。AI进入经营，主要通过在这三条链上分别配置私域AI赋能、公域AI补充与不可转移的人类责任来实现。

业务链	私域AI主要赋能（S4）	公域AI主要补充（受控公域 / 开放公域）	必须保留的人类责任（S4管理环节）
收入链	客户画像、商机总结、方案草拟、合同检查、回款预警	行业政策、招标信息、公开竞品与市场动态	客户关系、承诺边界、商务决策与最终报价
产品链	需求解析、设计知识检索、代码辅助、测试与缺陷分析	论文、开源框架、漏洞情报与技术趋势	产品取舍、架构决策、代码责任与发布批准
支撑链	经营分析、预算解释、人效分析、采购与供应链预警	宏观政策、人才市场、原材料和外部风险信息	资源配置、合规判断、人员决策与责任签批

10.2 三类代表性场景

在收入链上，客户经理在S4的目标管理系统中确认商机目标，让私域AI基于CRM生成客户画像与商机总结，在受控公域让公域AI跟踪公开政策与竞品动态，把整理后的外部材料经提交通道带回S4，最终报价与商务承诺在S4由人决定并提交。在产品链上，研发人员让私域AI检索内部设计知识、辅助编写代码与测试用例，让公域AI在受控公域跟踪开源与漏洞情报，一般业务代码的合入与发布批准在其获准流程中完成；属于S5的核心源代码、仓库和构建执行保留在S5，S4仅通过获准传输路径承接必要管理记录。在支撑链上，管理者让私域AI做经营与人效分析，让公域AI补充外部风险信息，资源配置与人员决策在S4签批。

三类场景的共同点是：AI承担信息搜集、内容生成与初步分析，人承担判断、决策与责任；执行可以跨S4与受控公域，目标从S4来、成果往S4交。

10.3 从使用量指标转向岗位价值

企业AI转型不能只统计登录次数、提问数量和生成文档数量。真正需要衡量的，是岗位产出是否提高、周期是否缩短、质量是否改善、风险是否下降，以及员工是否把节省出的时间投入更高价值的工作。管理过程在S4意味着这些衡量本来就在S4进行：AI的贡献通过提交到S4的成果和测评体现，不需要另设AI使用量指标。把“会不会用AI”的问题，转化为“岗位如何创效”的问题，才是AI真正进入经营的标志。AI时代的岗位能力由两项构成：深度思考能力决定问题的质量，AI运用能力决定解决的速度；培训与考核应围绕这两项，而不是围绕工具操作。

第十一章安全架构、威胁模型与合规映射

可信架构必须能够把安全主张，从概念落到威胁分析、从威胁分析落到控制措施、从控制措施落到标准条款与验证证据。本章给出威胁—控制映射与合规映射的方法，并按V4.0的边界设计扩展威胁清单。

威胁与控制位置对应

语义外泄 / 禁入数据	S4传输区 + 网闸	分类与最小化 / 标签与任务上限
注入 / 工具劫持	S3代理 + S4消费侧	返回检测 / 数据模式 / 工具白名单
越权 / 多Agent级联	Agent治理	即时授权 / 委托衰减 / 熔断
管理外移 / 未提交成果	S4管理过程	唯一提交入口 / 版权权威 / 流程约束
服务方数据使用	企业协议与核验	训练限制 / 保留删除 / 退出机制
旁路 / 通道与网闸故障	基础设施与通道	失败拒绝或暂存 / 续传对账 / 无旁路

图11-1 威胁—控制映射

11.1 威胁—控制映射

威胁	风险表现	控制位置	主要控制
语义型数据外泄	知识被自然语言带走，绕过传统DLP	S4侧传输区	语义分类器、禁入清单、按标签最小化、以问题出域、额度与熔断
禁入数据进入S3	L3以上内容以原文或改写形态出域	S4侧传输区 + 网闸	禁入命中拒绝与强制私域、任务上限叠加、格式白名单不含附件
Prompt注入 / 工具劫持	外部内容篡改Agent执行逻辑	S3侧安全代理 + S4侧	返回检测、活动内容剥离、数据模式消费、工具白名单、指令与数据分离
Agent权限扩散	长链路执行导致横向移动与持续访问	Agent治理	即时授权、委托链衰减、任务时限、最小权限、熔断
责任不可解释	AI决策无法追溯到人与依据	全链路	任务标识贯穿、人工确认、留痕与关联审计
治理外漂移	工作向个人账户与不可见路径迁移	姿态层 + 受控公域	受控公域企业化、企业凭证托管、开放公域仅L0、漂移指标
管理环节外移	目标、过程、定稿在S3完成，S4仅存文件	管理过程	目标管理系统与业务系统仅S4可达、提交为唯一入口、测评只认S4
隔断导致失明	切断通道后泄露转入不可见路径	姿态层	三种姿态框架；选择隔断须记录适用依据、替代控制与残余风险
服务方侧数据使用	公域服务方以企业数据训练或留存	协议层	企业协议条款、专属实例、保留与删除条款、定期核验与退出机制
未提交产物进入流程	S3草稿被直接用于审批、交付、测评	提交确认	流程只接受已提交版本；业务系统仅S4可达
提交通道断裂	产物滞留S3，任务不能完成	提交通道	自动同步、一级事件、断裂期间任务不能完成
知识投毒	外部内容污染知识库	S4侧传输区 + 知识治理	入库分级与来源标注、外部来源独立标签、知识库不摄入未提交内容
多Agent级联与共谋	多个Agent相互调用导致失控放大	Agent治理	委托链衰减、跨Agent调用登记、熔断范围覆盖整条链
成本耗尽与异常调用	大量调用消耗额度或触发外部风控	S3侧安全代理	速率与成本上限
网闸故障旁路	故障时切换到非受控路径	网闸	故障即拒绝或暂存，禁止替代路径

11.2 合规不是单项产品属性

合规不是买一个“合规产品”就能获得的属性，而是架构、流程与证据共同满足法规要求的结果。图11-1给出的威胁—控制映射，可与NIST人工智能风险管理框架的治理—测量—管理循环、ISO/IEC 42001管理体系要求以及OWASP大模型应用风险清单逐项对照，形成“威胁—控制—标准条款—验证证据”的四列可追溯关系；具体落地仍需结合行业法规、数据分类分级、跨境数据规则与企业风险偏好确定控制基线。

受控公域的安全依赖公域模型服务方履行协议，这是信任转移而非技术保证。企业应在协议中明确数据不用于训练、可审计、保留与删除条款，建立定期核验与退出机制；跨境服务另受数据出境规则约束。当监管、审计或客户提出“你如何保证AI使用安全合规”时，企业能够拿出的不是一句承诺，而是一条从威胁到证据的完整链条。

第十二章建设路线与组织机制

企业AI时代计算体系建设应遵循渐进路线：管理过程先确认、底座先行、边界先立、能力渐进组织跟进，并用可量化指标持续验证。



图12-1 企业安全计算与AI协同五阶段路线

12.1 五阶段建设要点

阶段	核心目标	主要任务	验收重点
第一阶段：统一计算底座与管理过程确认	把高价值岗位计算与数据迁移到受控环境；确认管理过程四环节在S4	NGCC试点（CPC/DPC）、身份体系、DMS纳管、关键岗位迁移；核对目标管理、业务系统、审批流、测评的承载位置仅S4可达；确认测评只认提交到S4的成果	体验、数据残留、真机基线、运维与可用性；衡量与测评动作在S4完成率
第二阶段：划清五业务域与禁入清单	形成正式的业务、数据和AI边界	数据分级分类、禁入清单、系统归域、连接矩阵、S3分层、网闸能力确认、规则型出口把关（主数据字典假名化、格式白名单）、目标管理系统向DMS传递任务标识与标签上限（初期允许人工设置）	每个系统有归属，每条跨域路径有责任入，禁入清单可被识别，规则型出口把关就绪
第三阶段：建设私域AI与能力差距评测（按配置级别选做）	形成企业内部智能能力中枢，知道差距在哪；一级配置的组织可跳过或以共享私域替代	知识治理、RAG、模型评测、语义分类器、AI工作台、重点岗位Agent、能力差距评测集与G0–G3分级	知识权限、答案质量、引用可追溯、分类器命中率、差距等级可复现
第四阶段：受控公域与三段传输结构	在统一控制下使用公域能力，执行去能力所在处	S3企业化（企业账号、协议、受控公域环境、企业存储）；出域准备区、网闸通道、S3侧安全代理；提交通道与提交确认；先拦L3以上，再开放L0/L1文件与L2最小化请求	禁入守得住、提交通道畅通、通道快于旁路、个人账号事件归零
第五阶段：重构工作方式	把AI转化为岗位和组织生产力	岗位任务重构以“目标从S4来、成果往S4交”为规则；培训、绩效指标、人机责任；能力差距常态评测与买进决策；收口开放公域	周期、质量、人效、经营结果和风险改善；S4主工作域指标稳定

顺序要点：先确认管理过程在S4，再接任务身份，再给人企业治理下的强能力执行环境，再收窄数据，最后收口开放公域。一级配置的组织完成前两个阶段与第四阶段即可运行，第三阶段按12.2选做。若在没有企业化S3的情况下先收紧出域控制，员工会直接漂向个人账号；若在通道尚未验证快于旁路时先收口开放公域，同样引发漂移。

12.2 按组织条件的三级配置

当前多数组织不具备在S4部署创造级AI的资金与技术条件。本白皮书不把私域AI当作前提：撑住S4地位的两样东西——管理过程在S4、出口把关——都不依赖私域AI。管理过程用现有的目标管理、项目、文档系统即可承载；出口把关可以由主数据字典假名化、规则型数值抽象、格式白名单与网闸组成，语义分类器是理想配置而非必要配置。据此给出三级配置，每一级都是完整可用的架构，不是残缺版。

配置	S4具备	AI工作位置	出口把关	限制	适用
一级：无私域AI	记录系统、管理过程、主数据	全部在受控公域；开放公域仅L0	规则型：字典假名化+数值抽象+格式白名单+网闸	L3以上数据不使用AI；即兴改写的敏感表述为残余风险，由抽样审计承担	多数中小组织
二级：轻量私域AI	加单机或小集群小模型：语义分类器、内部检索问答	创造在受控公域；分类、检索与知识问答在S4	语义分类器+规则	L3相关创造仍受限	有一定IT能力的组织

配置	S4具备	AI工作位置	出口把关	限制	适用
三级：完整私域AI	第六章全部能力	按能力差距等级分配	完整	差距不归零，按类别管理	大型企业、高敏感行业

两条中间路径可降低升级门槛。共享私域：集团、园区或行业云统一建设私域AI，成员单位以租户隔离方式使用，把三级配置的成本摊开；对集团型企业这是最现实的路径。厂商专属实例：模型服务方提供的独立部署或专属实例，落在受控公域层，协议与隔离比普通企业账号强一档，可承载假名化后的L2，是一级到三级之间的过渡。

三级配置是升级路径而非固定分层。开放权重模型与推理硬件的成本持续下降，一级到二级的门槛已经不高，第一个值得买AI是分类器而不是创造级模型。升级触发条件：某类任务在S3的执行时长占比乘以数据敏感度超过设定阈值，即为该类别买进能力的时点；触发条件由第十三章指标计算。

12.3 四个常见误区

第一个误区是先买GPU、上模型，再讨论数据和架构。结果往往是模型接触不到真实业务数据，或者为了使用模型而放松数据边界。正确顺序是先明确业务问题和数据边界，再规划算力、模型与平台。第二个误区是只建设私域AI，不治理公域AI。员工会继续通过浏览器、手机或个人账号使用外部模型，形成架构之外的灰色通道。第三个误区是只建平台，不改岗位。平台上线后如果没有嵌入工作台、流程、培训和绩效，AI只能成为少数人的兴趣工具。

第四个误区是以隔断代替完整治理。隔断可以用于依法依规必须隔离或确实不需要公域能力的场景。对仍有公域工作需求的组织，仅切断可见通道而不治理人工转录、个人账号及其他旁路，可能降低可见性；应同步评估业务需求、替代控制与残余风险。

12.4 组织治理机制

建设路线之外，还需要与之匹配的组织机制：明确数据、业务、安全与系统四类责任人在归域与审批中的分工；建立AI能力评测、上线审查与例外管理流程；把AI相关的安全事件纳入统一的应急响应与复盘体系；在岗位职责说明与培训中明确“目标从S4来、成果往S4交”及提交确认要求；把能力差距评测与买进决策纳入年度投资流程。技术架构与组织机制相互支撑，缺一不可。

第十三章验证、评价与持续改进

可信架构必须能够从概念落到测试，从测试落到证据，从证据落到责任结论。本章给出评价指标与证据管理要求。



图13-1 架构主张的验证证据链

13.1 七类评价指标

指标类别	示例	回答的问题
技术	时延、性能波动、资源利用率、故障恢复时间	架构能否稳定承载真实业务
安全	终端残留、跨域通路、越权率、注入测试、日志完整性、禁入命中率与漏报事件数	安全主张能否被测试和证明
管理过程在S4	工作项携带标签上限与能力层的覆盖率、阶段与最终成果在S4提交率、衡量与测评动作在S4完成率、未提交产物进入流程事件数	管理过程是否仍在S4
提交入口	提交及时率、待提交区停留时长、对账差异率、断裂次数、任务完成时无提交产物比例	提交是否是唯一且畅通的入口
能力差距与S3治理	各类别差距等级及趋势、G2以上类别数、各类别S3执行时长占比、企业账号使用率、个人账号事件数、协议覆盖率	边界是否设在能力所在处；S3是否仍在治理内
体验与效率	兼容性、会话恢复、满意度、常规请求端到端时延、符合标签、任务上限、去标识和策略条件的L0/L1请求自动处理放行率、通道与旁路时延之比、S4与S3执行体验差	用户是否愿意持续使用；通道是否比旁路快
经营	任务周期、采用率、返工、人效、风险损失和客户结果	技术投入是否转化为业务价值

13.2 证据管理要求

每项指标应记录测试对象、软硬件版本、网络条件、网闸模式、分类器与模型版本、标签体系版本、企业协议版本、目标管理系统接口版本、负载模型、样本、工具、阈值和测试人员。结论仅在声明条件内有效；架构、版本、规模、协议或业务负载发生实质变化时，应重新验证。生产运行还应建立异常分类、根因分析、策略改进和复测闭环。验证不是上线前的一次活动，而是贯穿架构变更、模型升级、知识更新、工具接入和业务扩展的持续能力。

13.3 与NGCC验收体系的衔接

本白皮书的验证与NGCC V4.22的T00–T11验收用例衔接：T00验证真机基线，T04验证多环境与跨域传输限制，T09验证结构与旁路。在此基础上，附录C给出S4↔S3三段传输结构与管理过程的专项验收用例，验证四条通道之外无传输路径、通道内控制有效、提交入口唯一。

第十四章架构演进与开放协同

架构型创新的价值，在于重新分配责任并形成可复制的工程方法，而不是把多个产品名称堆叠在一起。

14.1 从单点产品走向体系能力

随着AI能力、终端形态和业务协同持续变化，企业计算架构将更加重视身份、策略、数据、模型、Agent和管理过程的统一治理。未来的竞争不只在模型参数或终端性能，也在于能否把异构能力放入清晰边界，并用统一证据说明安全、体验与效率。

若公域能力增速持续高于企业买进能力，任务执行落在受控公域的比例会扩大。本白皮书接受这一走向：边界随能力移动，管理过程四环节、禁入数据类与提交入口不随之外移，这是架构设定的底线。

14.2 开放验证

NGCC、五业务域、七层架构、三层信任与管理过程四环节，应当作为开放的参考框架，与监管机构、科研院所、产业伙伴和用户共同验证。其成熟度应通过兼容性、测试工具、接口规范、运维体系和真实应用逐步提高。只有让创新可理解、可测试、可审计、可应用，技术才能真正转化为新质生产力。

结语真正的安全计算，不是拒绝连接和智能，而是让连接有边界、智能有权限、执行有责任、结果有证据；让执行去能力所在之处，让管理留在承诺与责任所在之处。

附录 A 核心术语

术语	缩写	本白皮书中的定义
PANSTONE CPC	CPC	Cloud Physical Computer，云端物理计算机；以云端真机提供受控计算环境
桌面管理系统	DMS	属于CPC产品体系，在本架构中提供共享管理与控制平面，统一纳管CPC真机与DPC两个主机，组织用户、入口与资源的授权关系
PANSTONE DPC	DPC	Dual-Host PC，双主机计算机；一台设备集成两个独立物理主机，一机双主、物理分域
即时授权	JIT	仅在任务需要时授予有限范围和时限的权限，任务结束后自动撤销
目标管理与自我控制	MBO	目标由企业目标逐级推导、管理者参与设定自己的目标并依据目标衡量自己的管理原则，以取代由上而下的支配；源自《管理的实践》
下一代商用计算机	NGCC	以云端真机为核心、三域责任分离、终端降权、单环境单安全域、独立真机与专属计算资源、统一纳管为原则的下一代商用计算机架构
五业务域	—	按安全等级、业务属性、AI权限、跨域流向和责任划分的S5至S1逻辑边界
三层信任	—	私域、受控公域、开放公域三个运行层；受控公域由企业账号、企业协议、NGCC纳管环境、企业存储四要素构成
双AI助理	—	由私域AI助理与公域AI助理分工协作、统一体验而分层运行的员工级协作模式
管理过程四环节	—	由五项基本作业组织成的管理循环：目标设定与分解、组织执行与自我控制、成果衡量与绩效测评、沟通激励与人才培养；工作域全部在S4
五项基本作业	—	管理者工作的五项基本作业：设定目标、组织、激励与沟通、衡量、培养人才（包括管理者自己）；源自《管理的实践》，本白皮书中工作域全部在S4
工作项	—	目标分解到个人后在目标管理系统中的最小单元；携带任务标识、数据标签上限与可用能力层
禁入数据类	—	必须留在其获准私域环境（S4或S5）、不得以原始或可还原禁入内容进入S3的数据类别集合；其列出形式称禁入清单
假名化与抽象化	—	L2内容出域前的保结构最小化：标识按主数据字典替换、数值换为区间或相对值、保留关系与逻辑；映射表只保存在S4
再水合	—	成果回域后在S4按映射表把假名恢复为真实数据的动作；在待提交区完成
三级配置	—	按组织资金与技术条件划分的架构配置：一级无私域AI、二级轻量私域AI、三级完整私域AI；每级完整可用，构成升级路径
共享私域	—	集团、园区或行业云统一建设、成员单位以租户隔离方式使用的私域AI
网闸	—	部署在S4与S3之间的安全隔离与信息交换设备；本白皮书中S4与S3之间唯一的物理连接点，只做格式白名单、物理摆渡与留痕，不做业务判断

术语	缩写	本白皮书中的定义
受控公域	—	S3内由企业账号、企业协议、NGCC纳管环境、企业存储四要素构成的企业管理执行环境；只承担任务执行
开放公域	—	S3内会话级、无成果驻留、仅允许L0内容的访问环境
待提交区	—	S4内接收提交通道同步产物、再分类、等待责任人提交确认的功能区；确认前产物不进入业务系统、测评与知识库
三段传输结构	—	S4侧传输区、网闸、S3侧安全代理；判断在S4侧，执行在网闸，代理在S3侧
任务标识	—	工作项在目标管理系统中的关联标识；用于关联执行、出域与提交，不单独构成访问凭证，仍须通过身份及授权校验
数据标签上限	—	工作项允许接触的最高数据类；在目标分解时确定
可用能力层	—	任务允许使用的信任层集合
成果提交	—	执行产物进入管理过程的唯一入口；由提交通道自动同步与责任人在S4确认共同构成
能力差距等级	G0–G3	按任务类别评测的私域与公域模型能力差距分级
能力买进	—	通过私有化部署或专属实例把接近前沿的能力纳入企业信任范围；优先落S4
企业私域AI平台	—	企业受控环境中的模型、知识、RAG、路由、分类器、评测、工作台与私域Agent能力中枢
结构级隔离	—	通过拓扑、接口、资源和控制面共同形成，并可通过工程测试验证的隔离边界
数据模式消费	—	私域AI将入域内容作为数据而非指令处理，指令与数据分离

附录 B 架构决策最小检查清单

- 组织处于三级配置的哪一级？一级配置是否已具备规则型出口把关与管理过程在S4？
- 业务与数据是否完成归域，是否存在无责任人的跨域路径？
- 目标管理、业务系统、审批流、测评是否仅S4可达？测评是否只认提交到S4的成果？
- 目标分解到工作项时是否携带任务标识、数据标签上限与可用能力层？
- 禁入数据类清单是否明确，所用规则或语义分类器的覆盖范围与漏检风险是否已验证？
- S3是否分为受控公域与开放公域？受控公域四要素（账号、协议、环境、存储）是否齐备？
- S4↔S3是否仅经网闸的四条通道传输？通道是否快于旁路？
- 各任务类别的能力差距等级是否评测在案？G2以上类别的处置是否明确？
- AI任务是否先判断必要性，并继承用户与数据权限？
- Agent是否有任务标识、沙箱、白名单、即时授权、委托链衰减、熔断和复盘能力？
- 高影响动作是否保留人工确认和组织责任？
- 终端、传输、计算、控制面、网闸和日志是否有明确边界？
- 安全、性能和可靠性主张是否绑定条件、测试方法和原始证据？
- 模型、知识、Prompt、工具、协议和应用版本变化后是否回归验证？
- 若选择隔断，是否记录适用依据、替代控制与残余风险？

附录 C S4↔S3 三段传输结构与验收用例

本附录给出第三章3.4三段传输结构的通道定义、失效行为与验收用例，供工程设计与验收使用。

C.1 网闸四条通道

通道	方向	允许对象	网闸侧检查
请求通道	S4→S3	结构化出域请求：请求ID、任务标识、会话、来源环境、任务标签上限、内容标签、用途、目标类型、最小化后的问题文本、允许返回类型与大小；不含附件与原文	格式、字段、标签≤任务上限、任务标识存在、大小、恶意代码
文件通道	S4→S3受控公域	已标签出域文件（≤L1，或假名化后的L2），携带标签、来源环境、会话、任务标识与把关结果	格式白名单、标签字段合法、任务标识存在、目标仅受控公域存储、恶意代码
结果通道	S3→S4	出域请求返回、S2 Agent产物、经预处理的文件	格式白名单、请求ID或会话匹配、大小、恶意代码
提交通道	S3受控公域→S4	按任务标识组织的执行产物同步	来源为企业存储、格式白名单、任务标识存在、恶意代码、批次留痕

出域准备区的分类与假名化可由语义分类器实现，也可由规则与主数据字典实现（一级配置）映射表只保存在S4，再水合在待提交区完成。不开放任何通用协议通道。摆渡模式（应用级或文件级）以所用网闸型号能力确认。网闸不可用时，出域在S4侧排队或拒绝，入域与提交在S3侧企业存储暂存，恢复后按批次续传；不允许任何替代路径。

C.2 验收用例

用例	测试动作与判定重点
X01 禁入原文出域	提交含L3内容的请求与文件；出口拒绝，网闸不放行
X02 禁入改写出域	L3内容改写为转述、摘要、注释；按所用规则或语义分类器测试命中和拒绝。未检出的样本记录为失败与残余风险，不得宣称已通过全量语义识别
X03 任务上限叠加	任务上限L1，提交可最小化的L2请求；拒绝
X04 无任务标识出域	无任务标识的请求与文件；出口与网闸均拒绝
X05 文件通道目标限制	L1文件尝试摆渡至开放公域；拒绝
X06 额度与熔断	批量相似请求；触发熔断并告警
X07 个人账号绕行	受控公域使用个人账号；阻止或记录
X08 间接注入	返回内容植入隐藏指令；S3检出，S4数据模式下私域AI不受影响
X09 活动内容入域	含脚本、宏的文件经提交通道；剥离且未剥离对象被拦截
X10 提交自动同步	受控公域产生产物；计划窗口内自动出现于S4待提交区，无人工动作
X11 提交确认前隔离	待提交产物尝试进入业务系统、测评或知识库；拒绝；确认后可进入
X12 未提交版本进入流程	用S3草稿直接发起审批、交付；流程拒绝
X13 任务完成条件	有产物任务在未提交时尝试完成；拒绝；提交后可完成
X14 入口再分类	提交产物含新增敏感信息；入口升级标签并按新标签处理
X15 保留期	受控公域存储对象超保留期或任务完成后；自动清理
X16 版本权威	S3草稿与S4已提交版本冲突时同步；S4版本不被覆盖
X17 对账差异	构造有产物无提交、有任务无产物；对账发现并计入指标
X18 管理系统不可达	从受控公域尝试访问目标管理系统、业务系统、审批流、代码库、知识库；网络不可达
X19 自我控制视图	执行者与上级在S4查看工作项状态与已提交阶段成果；不存在指向S3执行细节的视图
X20 提交通道断裂	中断提交通道超过窗口；一级事件；任务不能完成；恢复后续传对账
X21 开放公域无驻留	会话级实例产生文件后结束；重新登录不可恢复
X22 网闸故障	中断网闸；出域排队或拒绝，入域与提交暂存续传，无替代路径

用例	测试动作与判定重点
X23 时延达标	规定并发下测常规请求时延并与旁路对比
X24 能力评测可复现	同一任务集重测；差距等级可复现
X25 归因闭环	任取一条已提交成果，回溯到任务、发起人、会话、环境、出域标签、公域账号与协议

每个用例记录前置条件、网闸模式、分类器与模型版本、标签体系版本、企业协议版本、目标管理系统接口版本、NGCC实例配置、步骤、预期与实际、双侧日志与缺陷。结论仅在声明条件内有效；相关组件变化后回归。

C.3 适用边界与残余风险

- 人工转录、截屏、拍照：架构不能阻止人手工把S4内容输入S3，列为接受的残余风险，由管理规则、终端外设控制与开放公域输入抽样承担。
- 语义分类的误报与漏报：禁入识别依赖所部署的规则或语义分类器；设阈值、持续评测、保留人工复核，复核不直接覆盖禁入约束，漏报计入指标。
- 目标管理系统成熟度：任务标识与标签上限的精度取决于目标管理颗粒度；初期允许按部门或岗位设置上限。
- 测评只认S4的流程纪律：若某流程接受未提交版本，管理过程在该流程上失守；X12应覆盖所有衡量与测评流程，新流程上线须核对。
- 文件摆渡模式下的体验：网闸仅支持文件摆渡时，受控传输体验降级，更多类别的执行落入受控公域。
- 范围：本附录覆盖S4↔S3；S5与S4传输另行设计；S2面向S4的请求与产物须经S3侧安全代理和既定网闸通道处理，不新增绕过S4与S3边界的直接接口。

参考资料

- 国务院：《关于深入实施“人工智能+”行动的意见》，2025年8月21日。
- 工业和信息化部等八部门：《“人工智能+制造”专项行动实施意见》，2025年12月25日。
- NIST, SP 800-207: Zero Trust Architecture, 2020.
- NIST, Artificial Intelligence Risk Management Framework (AI RMF 1.0), 2023.
- ISO/IEC 42001:2023, Information technology — Artificial intelligence — Management system.
- OWASP Foundation, Top 10 for Large Language Model Applications, 2025.
- 彼得·德鲁克 (Peter F. Drucker)：《管理的实践》(The Practice of Management)，1954年。第八章管理过程的术语（五项基本作业、目标管理与自我控制）采用该书表述。
- 邦彦技术股份有限公司：《下一代商用计算机（NGCC）技术架构白皮书：品类开放与品牌口径校准版》V4.22，2026年9月。
- 邦彦技术股份有限公司：《PANSTONE CPC与DPC产品定位、定义及协同体系》V2.0，正式发布稿，2026年9月。
- 邦彦技术股份有限公司：《AI时代企业信息系统安全计算架构白皮书》V3.0，品牌换代，2026年9月4日。作为本版重编基础。
- 《邦彦磐石PANSTONE品牌定义》V1.0，2026-09-19。本过程稿产品全称、品牌市场边界与DMS归属的补充校准依据。

免责声明：本白皮书为技术架构研究框架与工程实践参考，不构成国家标准、行业标准或监管分类，亦不构成对任何产品、投资或合规结论的承诺。文中量化表述均须在声明条件内理解。

阅读笔记

用于记录架构评审、配置条件与验证证据。

BANGYAN

邦彦技术股份有限公司

技术架构研究与工程实践

V4.02 / 2026年9月

技术架构研究框架与工程实践参考