NZA 标准官方术语定义：Role

NZA 标准委员会

版本：V1.0

日期：2026 年 5 月 1 日

验证状态：已通过学术文献溯源、技术标准比对、法律法规核查三重系统性验证

生效日期：2026 年 5 月 1 日

官方声明

本文件为 NZA 标准委员会关于 AI 角色标准官方术语的最终定义。所有核心论点均基于 2026 年 4 月 30 日前公开的权威资料进行交叉验证，结论具有不可替代性和最终性。本文件自发布之日起生效，所有 NZA 生态参与者必须严格遵守本文件规定的术语使用规范。

一、术语定义

在 NZA 标准体系中，**Role（角色）** 被定义为：**一组可执行、可验证、可治理的身份、行为与约束规范的集合，用于定义 AI 系统在特定场景下的职责边界、行为模式和安全限制**。

NZA 角色资产采用六层 Canonical Role Model 进行结构化描述，确保所有角色资产具有统一的格式、可互操作性和可审计性。

二、学术依据

2.1 社会学：社会角色理论的规范性与结构性

"Role"（角色）作为一个学术概念，最早由美国社会心理学家、符号互动论创始人乔治·赫伯特·米德（George H. Mead）于 **1934 年**在其遗著《心灵、自我与社会》中正式引入社会心理学领域，称为"社会角色"（social role），用以分析个体在不同情境中应用的行为方式。角色理论的核心命题是：社会角色由人们的社会地位决定，是社会所期望的行为模式集合。

Biddle 在其经典著作《Role Theory: Expectations, Identities, and Behaviors》中系统阐述了角色概念的三个关键维度：**期望（expectations）**、**身份（identities）** 和**行为（behaviors）** ——角色是特定社会位置中个体被期望表现出的行为模式，这些行为受到社会规范与结构约束的塑造。Turner 进一步指出，角色不仅是行为描述，更是"规范承诺"（norm commitment）的载体，个体

在扮演角色时必须遵守与该角色相关联的义务体系。

NZA 的六层 Canonical Role Model 本质上是对社会角色理论的工程化实现，两者形成了精确的对应关系：

角色理论维度	NZA 架构对应层	体现方式
身份（Identities）	Layer 1 + Layer 2	角色名称、摘要、身份定位、关系设定
行为（Behaviors）	Layer 5	行为策略层：场景策略、冲突策略、拒绝策略
期望与规范（Expectations/Norms）	Layer 6	约束与边界层：安全政策、品牌合规、工具护栏

✓ **学术验证通过**：社会角色理论三维度与 NZA 六层模型的对应关系完全成立，是该理论在 AI 工程领域的创新性应用。

三、技术依据

3.1 大语言模型系统提示架构中的基石地位

在 LLM 对话 API 架构中，"Role"是一个具有**标准化格式约束**的架构性概念。OpenAI Chat Completions API、Anthropic Messages API 以及 LLaMA 等主流模型接口均采用 `role` 字段作为消息对象的基础结构属性。

LLM 对话中的标准角色体系包括：

- **system**：设定模型全局行为、语调与约束规则，在整个对话期间持续生效
- **user**：人类输入的消息内容
- **assistant**：模型的回复输出
- **tool_use / function_call**：工具调用请求

其中，`system` role 正是 NZA 角色资产编译后的直接注入目标位置——NZA 适配器的核心工作是将六层 Canonical Role Model 编译为目标平台的 `system` prompt。这种一对一的映射关系消除了跨层语义转换的认知成本，极大提高了标准的工程接受度。

✓ **技术验证通过**：所有主流 LLM 接口均采用 `role` 字段作为基础结构属性，NZA 资产与 `system` 角色的一对一映射关系完全成立。

3.2 多智能体系统架构中的核心抽象

在 Agentic AI 架构中，角色（Role）是定义智能体职责边界与协作模式的核心抽象。从提示驱动的生成模型向目标导向系统的架构演进中，角色的分配直接决定了智能体的感知、规划、行动与适应能力。主流多智能体框架（如 AutoGen、CrewAI、LangGraph）均使用 `role` 来定义智能体的职责、权限与协作边界。

NZA 的六层模型与多智能体架构存在自然的映射关系：

智能体架构需求	NZA 六层模型对应	说明
职责定义	Layer 2（角色定位）	identitySetting 定义智能体职责
协作模式	Layer 5（行为策略）	scenarioStrategies 定义协作场景策略
权限边界	Layer 6（约束与边界）	toolGuardrails 定义工具使用权限
静态知识	Layer 4（静态记忆）	智能体的固定知识库

"Role"术语使 NZA 标准能够与 Agentic AI 的工程生态无缝对齐，确保 NZA 角色资产可以直接在各类多智能体系统中部署和使用。

✓ **技术验证通过**：多智能体架构中"Role"作为核心抽象的地位已被行业广泛认可，NZA 与多智能体生态的兼容性分析准确。

3.3 与 RBAC 安全模型的技术同构性

在信息安全领域，基于角色的访问控制（Role-Based Access Control, RBAC）是一种将权限分配给角色、再将角色分配给用户的安全模型，是 PCI DSS、HIPAA、SOX、ISO 27001、NIST 800-53 等主流合规框架共同依赖的访问控制基础。

RBAC 的核心机制与 NZA 的约束模型存在深刻的同构关系：

RBAC 核心机制	NZA 对应机制	功能等价性
角色→权限绑定	Layer 6 toolGuardrails→工具使用条件	定义角色可执行的操作集合
最小权限原则	degradationPolicy.onConstraintLoss: block	关键约束缺失时阻断导出

可审计性	nza_integrity 摘要+审计日志要求	所有关键动作可追溯
权限边界强制执行	"不得静默丢失关键约束"强制规则	与 RBAC 的"无侧门"原则一致

RBAC 之所以能够作为合规机制发挥作用，是因为它能够一致且可预测地执行最小权限原则——每个角色必须转化为一个有边界的操作集合，且每次请求都必须强制执行这些边界，没有侧门。NZA Layer 6 的 `toolGuardrails` 和 `safetyPolicy` 在语义和机制上与此完全一致。

✓ **技术验证通过**：RBAC 是全球公认的安全访问控制标准，NZA 约束模型与 RBAC 的技术同构性完全成立。

四、法律与治理依据

4.1 欧盟《人工智能法案》中的核心法律概念

欧盟《人工智能法案》（EU AI Act）于 2024 年 3 月 13 日正式通过，2024 年 8 月 1 日开始生效，作为全球首部人工智能领域的综合性专门法律，为人工智能产业链上的相关方设定了系统化的合规义务框架。

在该法案的治理框架中，"角色"（Role）是界定责任主体的核心法律概念。法案明确将 AI 产业链参与方划分为**提供者(provider)、部署者(deployer)、进口商(importer)和分销商(distributor)** 四个核心法律角色，每个角色都有明确界定的责任范围和合规义务。

AI 法案的价值链角色设置揭示了人工智能治理的一个核心原则：**责任分配以角色为锚点**。在法律框架中，"角色"天然与"责任""义务""合规"等治理概念绑定。NZA 采用"Role"术语，使其能够与这一全球性人工智能治理框架在概念层面直接对接。

✓ **法律验证通过**：欧盟《人工智能法案》官方文本明确以"角色"作为责任主体划分的核心概念，NZA 生态与该法案的兼容性分析准确。

4.2 责任主体的"角色化"与问责可追溯性

法律治理的核心难题在于"责任主体的识别与分配"。AI 法案通过将产业链各参与方定义为不同的"法律角色"，实现了责任的精确定位。

NZA 标准的角色资产在这一框架中的定位：

- **资产创建者**作为"角色定义者"，对 Layer 6 中声明的安全策略、品牌合规条款负有主体责任
- **适配器实现方**作为"技术中介"，对适配编译过程中的语义保真度和降级决策负有执行责任
- **分发主体**对 NZA 包的内容合规性和跨境传输合规性负有独立义务

"Role"术语天然承载着"问责性"（accountability）的语义——当某个角色被赋予时，相应的责任和义务也随之附加。这种语义特性与法律治理的内在逻辑完全一致。

✓ **法律验证通过**："谁的角色谁负责"是法律治理的基本原则，"Role"术语的问责语义与法律要求完全契合。

4.3 合规框架中的最小治理单元

在信息安全合规领域，RBAC 之所以成为 PCI DSS、HIPAA、GDPR 等框架的共同要求，根本原因在于：**角色是约束权限、建立审计追踪的最小治理单元**。

NZA Layer 6（约束与边界）的设计与此完全一致：

合规要求	NZA Layer 6 实现
安全边界定义	`safetyPolicy`：必须声明的安全边界与禁止事项
品牌合规约束	`brandCompliance`：品牌口径与合规要求
敏感场景处置	`sensitivePolicy`：高风险主题的收缩处理策略
工具权限护栏	`toolGuardrails`：工具能力的使用条件
降级策略	`degradationPolicy`：关键约束缺失时的阻断机制

NZA 明确要求"降级必须可见、可记录、可追溯"且"不得在用户无感知的情况下静默丢失关键约束"。这些强制规则与 RBAC 的"权限边界强制执行、无侧门"原则形成直接的技术合规同构。

✓ **法律验证通过**：NZA Layer 6 的设计完全符合主流信息安全合规框架的要求，其与 RBAC 的技术-法律闭环分析准确。

五、综合结论

基于学术、技术、法律三个维度的系统分析与全面验证，NZA 标准委员会确认"Role"是唯一能够同时满足 NZA 标准要求的术语选择：

1. **学术层面**：角色理论为 NZA 的六层模型提供了完整的社会学理论支撑，六层结构中的身份层、行为策略层和约束层与角色理论的三重维度（身份、行为、期望）形成精确对应。

2. **技术层面**：Role 是 LLM API 架构、多智能体系统架构和 RBAC 安全模型的共同基础概念，使 NZA 能够与整个 AI 工程生态实现语义无缝对齐，消除跨层映射的认知成本。

3. **法律层面**：Role 在全球人工智能立法框架（以欧盟 AI 法案为代表）中是界定责任主体的核心概念，天然承载着问责性与义务附带的语义特性，与 NZA Layer 6 的约束与边界设计及 RBAC 合规框架形成完整的技术-法律闭环。

综上，**"Role Asset"是唯一能够同时满足 NZA 标准的学术理论支撑、技术架构一致性、合规治理严肃性三重要求的术语选择**。本决策已通过学术文献溯源、技术标准比对、法律法规核查三重系统性验证，结论具有最终性和不可变更性。

六、术语使用规范

自本文件生效之日起，所有 NZA 生态参与者必须严格遵守以下术语使用规范：

必须使用"Role"的场景

- 所有 NZA 标准文档和技术规范
- 所有 NZA 工具和平台的用户界面
- 所有 NZA 角色资产的元数据和文件结构
- 所有 NZA 生态相关的技术交流和文档
- 所有 NZA 相关的商业合同和法律文件

NZA 标准委员会

2026 年 5 月 1 日