智能体互联要“信得过、管得住、可追溯”

——《人工智能 智能体互联》系列国家标准解读

工业和信息化部科技司

智能体是具备自主感知、记忆、决策、交互与执行能力的新型智能系统，已成为人工智能产品与服务的关键载体。当前，我国智能体产业加速规模化落地，逐步在千行百业深入应用，海量智能体跨系统、跨平台、跨场景互联协作成为产业发展的重要趋势。

图为在第四届链博会上展示的超级智能体质选机

为深入贯彻落实国务院《关于深入实施“人工智能+”行动的意见》部署要求，规范引领产业创新、安全、有序发展，工业和信息化部指导中国电子技术标准化研究院，组织70余家重点企业，制定《人工智能 智能体互联》系列国家标准（标准编号：GB/Z 185—2026）。为便于产业各界准确理解、高效落地实施标准，现就系列标准核心内容系统解读如下。

GB/Z 185—2026《人工智能 智能体互联》系列标准出台的背景是什么？

随着人工智能技术快速发展，智能体正成为推动人工智能规模化应用和产业化落地的重要载体，已广泛应用于企业运营、工业制造、城市治理、民生服务等领域，未来还将面向具身智能机器人等物理空间和实体扩展。

但不同厂商、平台和架构下的智能体，在身份识别、能力描述、发现匹配、交互协作和工具调用等方面缺乏统一规范，存在适配成本高、协同效率低、可信管理难等问题。国际上虽已出现MCP、A2A等协议，但尚未形成统一共识，也难以完全满足产业发展需求。

GB/Z 185—2026《人工智能 智能体互联》系列标准旨在建立统一的技术框架和标准依据，规范智能体互联的关键环节，提升互操作性、可组合性和工程化应用能力，推动我国智能体产业规范化、规模化、高质量发展。

GB/Z 185—2026《人工智能 智能体互联》系列标准的总体思路和重点内容是什么？

系列标准坚持系统性、先进性和可操作性原则，围绕智能体互联全流程，构建从“身份可信、能力可见、发现匹配、交互协作”到“工具调用、任务完成”的标准化技术体系。

在内容设置上，标准共分七个部分：

第1部分规定智能体互联的总体架构；

第2部分规定智能体身份码编码、分配与管理；

第3部分规定智能体身份注册、账户、凭证和鉴别；

第4部分规定智能体能力描述及其注册、发布和变更；

第5部分规定智能体发现流程；

第6部分规定智能体点对点、群组、混合等交互模式；

第7部分规定外部工具调用的架构、流程和数据格式。

七个部分共同构成任务闭环：通过身份码和身份管理解决“谁在互联、是否可信”，通过智能体描述和发现解决“具备什么能力、如何被找到”，通过交互和工具调用解决“如何协同完成任务、如何访问外部资源”，形成完整的智能体互联标准体系。

另外，在总体架构上，标准提出五个概念域：用户域负责任务发起和结果接收；智能体域承担身份维护、描述维护、互联鉴权、交互和工具访问；管理服务域提供身份、凭证和鉴别服务；互联服务域提供描述管理、智能体发现和消息分发服务；资源访问域提供工具及外部资源支持。基于五个概念域的分层解耦设计，可以有效满足智能体互联安全可控、动态扩展、异构兼容及灵活演进等核心需求，体现了架构的先进性。

GB/Z 185—2026《人工智能 智能体互联》系列标准如何保障智能体互联的可信安全？

智能体互联不仅要“连得上”，还要“信得过、管得住、可追溯”。GB/Z 185—2026《人工智能 智能体互联》系列标准将可信身份作为互联基础，通过身份码、身份账户、身份凭证和身份鉴别等机制，为智能体跨系统协作提供安全保障。

在身份识别方面，智能体身份码由身份注册服务方统一分配，采用分层标识体系，用于智能体的识别、验证和管理。标准要求一个身份码仅对应一个智能体，从源头保障身份唯一性和可追溯性。

在身份管理方面，标准覆盖身份注册与核验、账户管理、凭证管理和身份鉴别等全生命周期环节。智能体核验通过后，由注册服务方创建账户、分配身份码并发行凭证，后续可进行更新、锁定、解锁和注销，实现持续管理。

在互联协作方面，请求智能体与服务智能体完成双向身份鉴别后方可交互，并可依据身份凭证和鉴别结果实施访问控制与互联鉴权。由此，可信身份和权限控制贯穿注册、发现、交互及工具调用全过程，为智能体规模化互联筑牢安全基础。

GB/Z 185—2026《人工智能 智能体互联》系列标准将给智能体产业落地、生态建设和用户体验带来哪些影响？

该系列标准的实施，将推动智能体从单点应用、封闭系统走向跨平台、跨系统、跨场景协同，为产业规模化发展提供基础支撑。

在产业落地方面，系列标准统一身份管理、能力描述、发现匹配、交互协作和工具调用等关键机制，有助于解决身份不统一、能力不可见、接口不兼容等问题，降低系统集成和场景适配成本，加快智能体在办公、制造、政务乃至具身智能等领域应用。

在生态建设方面，系列标准为产品研发、平台建设、系统集成和测试验证提供依据，便于不同来源的智能体统一管理、调度、组合和复用，促进能力开放共享，推动形成开放协同的产业生态。

在用户体验方面，系列标准将提升服务的可信度、便捷性和连续性，使用户能够了解智能体“是谁、能做什么、是否可信”，并通过多智能体协同和工具调用高效完成复杂任务。

总体来看，系列标准将有助于降低产业落地门槛、提升企业协同效率、改善用户体验，加快形成有序、良性的产业生态，助力人工智能赋能千行百业。

江苏构建以先进制造业为骨干的现代化产业体系

（上接第1版）“十五五”时期，江苏将聚焦平台强基、联合攻坚、成果转化等，通过政策引导、资源倾斜、机制创新，打通创新链中的关键堵点，构建科技创新和产业创新深度融合的工作体系。

一是推动企业牵头建设创新平台。围绕提升规上工业企业研发机构覆盖率，分级分类推动企业加快建设研发机构。推动中小企业建设基础级研发机构，开展专业化研发创新。推动专精特新中小企业与高校院所共建研发机构，加强技术研发和工艺优化，形成更多独门绝技。推动“筑峰强链”企业牵头建设重点实验室、技术创新中心、制造业创新中心、制造业中试平台等创新平台，发挥行业支撑作用。到2030年，培育建设制造业中试平台50家左右，新增省级以上企业技术中心500家以上。

二是推进锻长补短技术攻关。聚焦新型电力装备、新能源等5个优势集群以及具身智能机器人、工程机械等2条重点产业链，实施一批“锻长板”协同攻关项目，带动产业链上下游创新水平整体提升。围绕装备、材料、元器件和软件等领域薄弱环节，通过“揭榜挂帅”“赛马”方式，每年实施100项左右“补短板”技术攻关项目。

三是加快自主创新成果推广应用。开展首台（套）装备、首批次新材料、首版次软件和新技术新产品认定，推动更多产品纳入政府采购支持科技创新政策范围，“十五五”期间每年推广新技术新产品500项以上。常态化开展“三首两新”产业链推广应用活动，组织创新企业与应用单位精准对接，推动“三首两新”产品加快进入供应链。

聚焦“人工智能+” 推动智能制造全面跃升

人工智能是新一轮科技革命和产业变革的重要驱动力量，是加快发展新质生产力的强大引擎。“十五五”时期，江苏将坚持企业主体、政府引导，加快数字技术在制造业大规模普及应用，深入探索人工智能赋能制造业实施路径。

一是推动人工智能产业创新发展。落实《关于加快人工智能终端产业发展的实施意见》，大力发展人工智能手机、人工智能计算机等终端产品，在智能芯片、端侧大模型等关键环节取得突破，培育10家左右具有生态主导力的领军企业。加快具身智能机器人、智能网联新能源汽车等领域高质量数据集建设，探索行业语料库建设，推动构建端云协同的数据资源体系。

二是推进“人工智能+制造”。深化实施制造业智能化改造数字化转型网络化联接行动，梯度培育基础级、先进级、卓越级、领航级智能工厂。推进实施“人工智能+制造”诊断行动，线下线上结合开展企业人工智能应用水平诊断。组织开展人工智能“揭榜挂帅”，支持建设一批工业大模型项目和专业小模型研发。到2030年，规模以上工业企业基本完成智能化改造。

三是强化基础设施要素支撑。加强算力网规划建设，打造多元算力供给体系，推进通算集约化、智算规模化、超算商业化，构建“万卡”智算资源池，前瞻布局量子计算等新型算力。加快网络基础设施建设，提升重点城市5G-A网络覆盖面，构建高质量低空通信网，推动万兆光网向“万兆工厂”“万兆园区”等场景部署。持续推动工业互联网平台建设，培育一批跨行业跨领域的综合性平台和面向特定行业、特定区域的专业性平台，推动行业数据资源汇聚应用。

聚焦节能低碳 推动产业绿色发展转型

建立与“双碳”进程相匹配的绿色制造体系，是推动产业绿色低碳发展的关键抓手。“十五五”时期是江苏工业领域落实2030年前碳达峰目标的全面攻坚期，也是推动绿色制造体系从重点突破迈向系统提升、全面提质的重要时期。

一是深入推进重点行业节能降碳。会同有关部门制定实施“十五五”碳达峰实施方案，实施冶金、石化化工、建材、纺织等重点行业节能降碳改造行动，依法依规推动落后生产工艺装备关停退出。聚焦电池等行业推行碳评价和碳管理，实现能耗与碳排放精准管控。到2030年，规模以上工业单位增加值能耗较2025年降低10.5%。

二是全面推广绿色生产方式。完善国家、省、市三级绿色工厂联动培育机制，加快推进绿色工厂提质扩面。深入实施《江苏省零碳（近零碳）工厂培育建设工作方案（2025-2027年）》，研究制定《零碳（近零碳）工厂建设指南》地方标准，高标准推进零碳（近零碳）工厂培育建设。到2030年，累计建设省级零碳（近零碳）工厂100家左右，培育省级绿色工厂4000家以上。

三是促进资源循环高效利用。强化工业固废精细化管理与规模化利用，构建“产废-利用-市场”产业链，培育龙头企业和规范回收网络。推动再制造产业发展，探索构建再制造产品管理和认定机制，突破纳米修复等关键技术，提升再制造加工水平。

聚焦梯度培育 推动优质企业群体壮大

工业的发展根本上要靠企业，企业强才能工业强。“十五五”时期，江苏将把更多着力点聚焦到各类企业发展壮大上来，进一步完善企业服务体系，给予企业更加精准的扶持。

一是培育一流总部企业。深入实施“筑峰强链”企业培育支持计划，推动政策、资金、项目向优质企业聚集。加大领航企业培育力度，形成一批产品卓越、品牌卓著、根植江苏发展、面向全球的一流总部型企业。到2030年，累计培育制造业领航企业300家左右。

二是壮大专精特新企业。深入实施支持专精特新企业高质量发展若干政策措施，拓宽从创新型中小企业到省级专精特新、再到国家专精特新“小巨人”和制造业单项冠军的培育进阶通道。支持中小企业加大技术研发和创新投入力度，在细分市场形成竞争优势。到2030年，国家专精特新“小巨人”企业数量保持全国前列，累计培育省级专精特新中小企业3万家左右。

三是培育科技与创新型中小企业。建立健全优质企业主动发现机制，充分挖掘股权投资、科技奖项、人才引育等数据，常态化发现并邀请潜在优质企业参与创新型中小企业评价。支持创新型中小企业与高校、科研院所建立稳定合作关系，共建研发平台、联合攻关，开展技术研发和产品创新。到2030年，累计培育创新型中小企业超7万家。

（上接第1版）依托新一代AI智能体工具，无须复杂的专业技术，仅通过简单文字指令，就能自动完成漏洞排查、风险分析、攻击验证等全套操作。以往耗时一两天的漏洞复现工作，现在1小时左右就能完成，且无须专业技术支撑，普通从业者就能打出高级别的网络攻击效果。

除了自身存在安全漏洞外，AI智能体的权限混乱问题也是企业落地应用的另一大安全隐患。“智能体本质上是一种软件。它帮人干活的前提是获取人类对系统操作的使用权限。一旦这些权限被滥用或误操作，极易引发重大安全事故。”齐向东表示。

智能体能够自主调用工具、梳理流程、处理数据、执行任务，但这种“自主运行、主动联动”的特性，也催生了一批新型风险，成为企业安全治理的新难点。度小满安全负责人李广林分析认为，智能体作为工具本身只是入口，而真正的风险会发生在意图、模型、权限、数据和执行环境串起来之后。

防御逻辑 正在被颠覆

反观企业传统的漏洞防护模式，短板在AI时代的高强度攻击之下被无限放大。建立在边界防御、人工修补和被动响应之上的传统网络安全模式，在AI批量化发动网络攻击的今天已经彻底失效。

据了解，传统安全设备的核心逻辑是“基于已知威胁的特征匹配”。防火墙、入侵检测系统、入侵防御系统的运行，依赖于不断更新的威胁规则库。但在AI攻击面前，这套逻辑彻底失灵：传统规则库的更新周期平均为72小时，而基于强化学习的AI攻击工具，可在24小时内完成上千次攻击策略迭代，生成全新的攻击特征。

边界防御思维在面临无边界AI攻击时也全面失守。传统安全框架试图通过防火墙隔离内网与外网，通过VPN管控远程访问，构建一个“内外有别”的安全边界。但AI攻击的“无边界性”，彻底打破了这种防御逻辑。

AI时代的网络安全问题，直接转化为了业务安全问题和使用功能安全问题。京东安全技术效能负责人陈玉杰指出，传统企业漏洞修复普遍存在三大痛点：发现晚、修复慢、看不懂。

陈玉杰说，多数企业的漏洞，都是在业务代码即将上线时才被发现，不仅阻断正常业务迭代，还会造成研发资源浪费；一条普通漏洞，从发现、派单、整改到复测完成，平均需要7天时间，处置流程繁琐、周期漫长；同时，企业研发人员大多不懂网络安全，看不懂漏洞风险和整改要求，只能反复咨询安全人员，不仅效率低下，还容易出现漏洞修复不彻底、反复复发的问题。

“目前很多企业的安全建设存在‘平均用力’的误区，不管资产价值高低、风险大小，平均分配安全资源，导致核心业务、核心数据防护不足，低价值资产却过度防护。”比亚迪安全架构运营负责人李斌告诉记者。

在AI攻击的链式渗透与迂回攻击模式下，企业很容易出现“边缘薄弱环节被突破，核心高价值资产被窃取”的严重后果。这也意味着，AI时代的安全防护，必须告别被动修补、平均防御的旧思路，转向提前预判、精准防护、极速处置的新模式。

构建用AI对抗AI的 主动安全能力

幸运的是，当前行业已经形成共识：想要抵御AI驱动的智能攻击，必须依托AI技术重构安全防护体系，实现“用AI对抗AI”，让安全防护从被动补救变成主动预判、内生防控，全面适配智能经济的发展需求。

目前，国内头部企业已经落地了实战方案，实现安全范式的全方位升级。针对传统漏洞修复慢、门槛高、不彻底的痛点，京东自研“神医”AI漏洞修复智能体，颠覆传统整改模式。陈玉杰介绍，以往需要7天才能完成的漏洞修复全流程，如今压缩至10分钟以内即可完成，整体效率提升百倍，仅半年就为企业节省了90人/年的人力成本。

这套AI工具的优势，降低了安全防范的门槛，无须研发人员看懂复杂的漏洞原理，AI会给出可直接替换的修复代码，员工简单确认即可完成整改，真正实现“傻瓜式修复”。同时，它将安全检测提前到代码编写阶段，员工写代码的同时AI实时检测、即时提醒、即刻整改，从源头杜绝漏洞产生，实现代码上线即安全。经过长期迭代优化，该工具漏洞修复准确率达到95%，远超传统安全工具，目前已全面覆盖京东两万五千余名研发人员，实现代码安全全覆盖。

奇安信则提出构建高、中、低“三位一体”的内生安全体系。这一体系的核心是构建“能力”和“韧性”，从“漏洞管理”转向“攻击面管理”和“持续风险管理”。齐向东告诉记者，“低位”是全栈AI化的安全产品，“中位”是自主安全智能体，“高位”是能生产威胁情报的大模型底座。也就是说，底层做自动检测和响应，中间层做编排和决策，上层做情报和分析。

智能体安全管控的落脚点在于身份与权限。李广林指出，智能体治理要实现从“管理工具”向“管理行为链路”的升级，通过落地身份权限模型，厘清AI的身份和权限，为AI操作建立独立日志、独立追责机制，避免权限泛滥、越权操作，实现所有行为可溯源、可管控。

在企业整体安全运营层面，比亚迪结合自身海量资产运维经验，摒弃传统平均防御模式，提出“核心资产重点防护”思路，从业务价值、攻击偏好、管理需求三个维度，精准识别企业核心资产和核心业务，将80%的安全资源集中用于高价值资产防护。同时搭建一体化安全运营平台，整合各类安全设备数据，清晰掌握企业资产底数、风险状态，实现安全风险快速发现、快速处置。