

进一步筑牢云原生安全底座

□ 魏 亮

云原生是基于云计算环境构建和运行数字化应用的全新原生技术理念，实现了分布式、敏捷化和智能化的新一代软件架构。这一理念通过容器、编排调度等云原生技术集合落地各行业应用，经过多年发展，已经成为全球云计算基础设施、人工智能算力调度和企业数字基础设施的核心组成。与此同时，原生的技术特点也重塑了传统安全防护体系，云原生安全是内嵌并适应于云原生技术和架构，保障数字应用和云环境系统的安全理念和技术体系。目前，我国各行业已经广泛部署云原生技术系统，需进一步加强云原生安全能力建设，有力支撑数字经济高质量发展。

云原生技术需要加强和保障云原生安全体系建设

云原生技术革新软件工程范式，成为全球数字基础设施核心架构。2013年云原生概念首次提出，即基于云计算环境的软件架构，打破所有计算硬件的边界，将一个应用拆成若干个小应用分别放在虚拟的计算单元容器里，分布式开发和部署，显著提升软件运行效率达10倍以上。2015年，云原生计算基金会（CNCF）成立，开源容器和编排调度等云原生核心技术，加速云原生架构成为企业构建数字化转型系统的“第一步”。2018年，《云智能战略》（Cloud Smart）的发布，推动云原生技术在军队等场景中应用。据统计，2025年全球将有超过95%的新部署数字工作负载运行在云原生平台上。

云原生应用加速大模型训练和推理能力，促进人工智能高速发展。云原生依靠标准化的容器封装和部署，可以将人工智能任务拆分进行并行训练，或者将任务部署在不同硬件节点

进行推理，成为大模型训练和推理的首选工程架构和核心操作系统。在训练方面，GPT-3模型基于微软云的7500个云原生节点进行任务编排和分发训练，整体训练成本下降了80%。在推理方面，我国超八成的DeepSeek服务采用云原生技术部署，可以满足云边端的不同硬件架构需求，提升推理效率。

云原生安全是关键基础设施的免疫基线，保障数字经济稳定发展。云原生架构虚拟资源、动态编排和弹性扩展的特性重塑数字基础设施的安全边界，需要云原生安全体系构建全新的“数字免疫系统”。完备的云原生安全体系观测能力更细、处置效率更高，5所大型国有银行基于云原生安全产品平均全年拦截攻击21亿次，漏洞修复效率提升40%，事件处置时间从原有的数小时缩短至数分钟以内，有效保护经济财产安全。云原生安全已成为保障系统安全稳定，支撑数字经济发展的战略安全基座。

我国云原生安全体系尚处建设初期

我国云原生安全规模需要提高云原生市场的需求。我国用户在云原生安全市场的投入有待提高，据统计，我国多数企业不同程度的使用了云原生技术，2024年市场规模达8000亿元。然而，我国云原生安全市场规模仅为30亿元，与云原生市场的比例约为1/260。我国云原生用户对安全的认知度也有待提高，只有头部企业部署云原生安全产品，一些中小企业尚未部署云原生安全工具。

我国云原生安全技术需要提高一体化防御竞争能力。2015年开始，一些安全企业推出云原生安全产品，在容器安全、云工作负载保护等单点技术上的成熟度已达到国际水平。但

国内安全厂商“散而碎”，尚无一家厂商具备全链条的云原生安全产品，平均市值不足20亿美元，较一些具有较高水平的安全企业的规模和一体化服务能力有一定差距，用户部署整体云原生安全体系门槛较高，需提升整合多家厂商能力。随着一些云原生安全初创公司被收购，更凸显出加速技术体系整合的重要性。

我国云原生安全的应用场景需要拓展。在人工智能方面，公有云的大模型训练和推理平均部署上千个容器节点，安全防护形势严峻，而大多数用云原生私有化部署DeepSeek服务的都处于无安全防护状态，云原生安全防护能力滞后于云上人工智能安全需求，对模型参数和用户训练推理数据在算力间高效编排调度的复杂链路观测性不足，云原生安全需要进一步提升和人工智能的结合。对各行业而言，安全目标各有侧重，云原生安全需要根据不同行业应用特点进行适配，例如，金融行业侧重业务连续性、合规性与实时威胁响应，制造业生产线管理系统依赖第三方镜像面临供应链与工业控制系统的稳定性风险。

我国云原生供应链安全需要提高自主开源生态。我国云原生安全国内主导的仅占2项，虽然在云原生编排调度、应用引擎、云边协同和安全领域出现了新项目 and 开源社区，但碎片化严重，难以形成合力。AICOS（AI操作系统）开源社区探索云原生对AI的编排调度系统，但也只处于初期的发展阶段，需要抓住升级换代的机遇弯道超车。

加强云原生战略布局与安全生态建设

加强云原生安全顶层规划，促进市场匹配规模化发展。推动云原生发

展规划等政策的制定，强化云原生技术、安全、应用、产业内涵的体系化研究，明确云原生在数字经济中的战略定位。加强云原生安全市场发展扶持力度，培育重点云原生安全厂商规模化发展，通过财政补贴等方式促进中小企业采用云原生安全产品，推动市场深入发展。

攻坚云原生安全核心技术，打造国际先进一体化安全体系。设立专项科研基金，定向支持无服务器安全、人工智能驱动的威胁检测等新兴云原生安全技术创新攻关。健全云原生安全标准体系，提高安全产品的功能、性能和适配能力，打破安全产品间互联互通、整体部署的壁垒。鼓励企业通过合作共创、并购整合等多种形式，对标国际领先企业形成一体化产品矩阵。

促进云原生安全+AI融合发展，加强各行业安全应用实践。促进云原生技术与人工智能、大数据和算力等领域的协同创新，加速针对人工智能云服务新技术场景的安全产品落地。结合金融、制造等行业特性，构建“云服务商—安全企业—用户”的联合创新体，引导企业通过合作共享形式，建立上下游联动的产业生态体系，形成各行业的示范应用。

推动云原生自主开源生态发展，构建底层安全生态体系。鼓励云服务开发商和安全企业加大在云原生计算基金会（CNCF）等国际开源社区的投入，争取核心项目的主导地位，推动全球技术生态协同。扶持我国云原生开源社区发展，鼓励百花齐放培育优势开源社区，推动我国云原生在新兴算力技术等结合领域建立发展底层技术路线。

（作者系中国信息通信研究院副院长）



顺应新一轮科技革命和产业变革，由平台赋能价值创造的经济环境发生了巨大变化，数据成为关键生产要素，基于互联网的信息基础设施成为连接、汇聚和整合多元经营主体的重要基石。有鉴于此，我们要深刻把握需求侧规模经济形成的平台特点，充分释放平台经济进行价值创造的新动能。

适应平台网络效应，提升价值创造能力。平台经济的价值创造过程已经从传统的链式结构演化成网络结构。数智时代的互联网，不仅降低交易成本，还增强了市场中各主体之间的互联互通，推动了平台经济发展的规模效应。社会化生产系统中的供应商、制造商、消费者以及合作伙伴深度融合融入价值创造的网络中，使得价值流动超越了从研发设计至生产销售的单一线性路径，转而形成了一个交互性极强的价值网络。

平台经济进行价值创造的网络逻辑首要特点在于能够构建一套基于“双边市场”的反馈回路。在平台经济的网络中，各种大小不一的反馈回路同时运转，不同网络节点之间的数据流动持续不断进行。网络逻辑的另一个特征是层次性，表现为规模较大的网络结构内部往往嵌套着多个遵循相似运作逻辑的较小网络结构。比如，平台企业能够在不同层级上扮演多重角色，并且在同一行业内推出多类型的产品。

鉴于平台经济的网络结构，我们需重点关注价值创造过程中经营主体交互行为的数量与质量，要确保各个层级反馈回路的高效运行。具体来说，要在三个方面努力：一是确保平台具备良好的流动性，这意味着平台内的交互失败率极低，并且用户访问平台的需求通常会在合理的时间内得到满足；二是提升匹配质量，这指的是用户在平台上搜索能够与其共同参与价值创造活动的其他用户时，平台所提供的搜索算法的准确性以及导航工具的直观程度。这些标准可以通过平台某一时间段内的活跃用户比例、活跃用户增长率以及成交率等数值来衡量；三是加强基于标准导向下的反馈数值分析，这样一来平台企业可以及时地调整策略和行为，引导平台网络效应朝着有益的方向发展，从而实现价值创造能力的不断增强。

着眼全周期管理，增强平台用户黏性。虽然平台经济价值创造由网络逻辑驱动，但在新的模式下，服务质量的重要性愈加显著，与用户建立持久的情感连接成为一些平台企业弯道超车的法宝。平台经济打破了由信息不对称造成的交易壁垒，借助大数据技术交易双方的沟通在时空范围内实现了延展与深化，价值创造过程的重心从达成单次交易转向长期关系建设。

全周期管理是平台经济推行持续服务的重要手段，其面向的是产品从准备进入市场到被淘汰退出市场的全过程。这一管理强调持续跟踪产品的研发、市场推广、销售、售后服务等各个环节，分阶段地对产品采取针对性维护策略。在产品刚进入市场时，产品的用户基数较小，市场接受度也尚不明朗。平台在这一阶段的主要任务是，在保持产品质量和用户满意度的基础上，进一步提升产品的市场份额。而当产品已经拥有稳定的用户群体和市场份额后，成功的信号将会吸引类似的产品涌入市场，竞争无疑会变得更加激烈。此时，平台需聚焦于优化盈利能力，提高用户留存率和忠诚度，同时探索新的收入来源。总之，随着产品生命周期的不断推进，平台应适时调整策略，以深化对用户了解。

平台的全周期管理要时刻围绕用户展开，建立用户对平台的信任，进而提升用户黏性。用户对于平台的信任程度决定了其是否会反复参与到平台活动的价值创造中。因此，平台必须采取一系列有效的运营措施，保证双边的参与者都经过严格的筛选与管理。从积极方面讲，平台可致力于用户对平台信任度的提升。比如，通过大数据和人工智能技术深度挖掘用户偏好和需求变化，实现个性化的产品推荐和服务；定期向用户提供最新的产品信息，增强用户对平台的依赖性。此外，平台可以实施用户分层管理策略，针对不同黏性的用户制定差异化的营销与服务标准，以此激励用户加强与平台的联系，构建长期且稳固的关系。

促进双边市场联动，提升平台治理水平。生产者与消费者之间的良性交互，是平台价值创造网络逻辑得以发挥作用的驱动力。平台在满足简单联络互动的基础上，更多介入到生产者与消费者的关系之中，使得交易双方对平台中介的依赖性更强。平台虽然促成了买卖双方的直接联系，降低

价值释放平台经济新动能

□ 徐浩然

了交易成本，但同时也成长为比传统中介更强大、更具控制力的新型中介。因此，平台理应承担起与相应的责任，在价值创造和维护市场秩序等方面发挥作用，并根据实际情况采取有效的治理措施。其中，平台的首要任务是确保市场双边的平衡，为了达成这一动态平衡，平台应敏锐把握失衡迹象并且及时给予应对，可通过营销活动、优化搜索算法以及提供更具吸引力的服务等方式来调节双边用户数量，从而恢复整体的平衡状态。在这一过程中活跃平台用户的作用至关重要，他们作为在平台上持续保持一定交互频率的用户群体，构成了平台生态稳健运行的基础性力量；平台应高度关注这些活跃用户的动态和需求，将他们的反馈作为优化平台功能与服务的重要依据，以此来促进平台的长期稳定发展。

在平台经济场景下，生产者与消费者在互动过程中可能会出现角色互换现象，一些曾经的平台消费者可能会转化为现今乃至未来的优质生产者。平台应重视统计用户从一种类型转化为另一种类型的比例，即角色转化率。这也是平台用于监测其用户群体状况并维持整个网络生态平衡的一个重要指标。通过深入分析角色转化率，平台能够更好地把握施策时机，促进用户间的有效互动和价值共创。

良好的创新生态，扩大经营主体竞争优势。不确定性是数字经济的显著特点，平台组织在复杂环境下想要保持竞争力和持续发展，必须主动求变、走在创新发展的前沿。数智技术的联通作用让平台处于“牵一发而动全身”的复杂环境下，外部变化带来的波动传导更快、作用更强，要求平台必须将提升应变能力列为发展的核心要务；数智技术也进一步推动了扁平化管理模式的兴起，其为平台快速制定和有效落实解决方案提供了必要支撑。

打造良好的平台创新生态，不仅涉及平台的技术、产品、服务等方面的创新，还包括对合作伙伴、供应商、用户等生态体系内各要素的整合和优化。由于平台生态体系涉及的对象众多，因此其内部便蕴含着丰富的创新契机。平台可以通过技术创新完善平台的功能和性能，从而提升用户体验；加强与生态体系内的核心开发人员、拓展开发者以及数据整合者等各方的合作，共同研发新的产品、探索新的价值创造方式，以进一步拓展市场空间。创新的“培育”需要整个平台生态体系进入到适宜的“土壤状态”。总而言之，平台组织创新生态体系的建构要具有开放包容、协作共进以及交互畅通等特性。只有在这样的环境下，平台创新主体以及不同平台之间才能更为高效、充分地开展各类信息和资源的沟通与整合，在平台网络效应作用下不断涌现出创新成果和新的发展机遇。与此同时，政府亦需积极作为，坚持发展和规范并重，为平台经济发展构建充满活力的、公平竞争的制度环境。



构建“跨省通办”数据安全防护体系

□ 李 颖

“跨省通办”是当前数字政府建设以及“放管服”改革的一项重要举措，是“一网通办”的延续和拓展。与“一网通办”相比，“跨省通办”事项增多，数据在不同地区、部门间频繁流动，数据安全问题日益凸显，成为影响“跨省通办”长远发展的重要因素。

“跨省通办”作为一种政务服务模式，实现了在互联网中对不同地区政务服务机构之间的信息共享、业务协同和远程办理，使群众和企业无需跨省跑动即可完成相关事项。传统政务服务受地域局限，群众办理异地事务需在不同地区奔波，提交大量材料，耗时费力。而“跨省通办”借助互联网、大数据等技术，打破地域壁垒，通过线上线下融合，让群众可在居住地办理异地业务，极大降低办事成本，提升服务效率与可及性，实现政务服务从“群众跑腿”到“数据跑路”的转变。

近年来，“跨省通办”成果显著。从户籍迁移、社保转移到企业登记注册、不动产登记等高频事项，越来越多政务服务实现“跨省通办”。如有的地区通过区域一体化政务服务平台，实现多项民生服务和企业开办事项“一网通办”；有的地区在交通、医疗、社保等领域协同推进“跨省通办”，为区域协同发展提供有力支撑。这些实践表明，“跨省通办”已成为提升政务服务水平、优化营商环境、促进区域协调发展的重要手段。

自“跨省通办”启动以来，国家统筹和区域创新两个层次的实践都进展较快。从国家层面看，国家一体化政务服务平台在归集数据等方面加速发展，成为“跨省通办”的枢纽式基础设施。从地方层面看，区域性“跨省通办”已实现毗邻省份的区域性“通办”整体推进、劳务输入和输出重点地区的点对点合作加速发展等一系列措施。“跨省通办”要求在统一身份认证、电子证照等电子材料或技

术全面应用的基础上实现数据共享。值得注意的是，在数据共享过程中可能引发资源限制、利益冲突、权责不清、安全风险等潜在问题。数据泄露事件时有发生，给个人隐私和企业商业秘密带来挑战，数据共享机制下的隐私安全成为主要关注点。同时，由于不同地区政务系统技术水平和标准不一，数据传输和存储面临风险，如多地不动产登记系统加密标准不统一，跨平台数据传输易成黑客攻击目标；部分工作人员安全意识淡薄、操作不规范，存在违规查询、泄露数据的隐患；制度层面，数据安全管理和监管制度不完善，缺乏明确的数据共享、使用、存储规范和追责机制，导致出现问题时难以有效处理。此外，“跨省通办”涉及多部门、多地区的数据共享与业务协同，数据流动环节增多，管理难度加大。一旦某个环节出现安全漏洞，就可能引发连锁反应，导致大规模数据安全事故，严重影响“跨省通办”的公信力和群众对政务服务的信任。可见，“跨省通办”实践中的数据安全问题的确不是简单的技术挑战，而是对行政组织和运行机制提出的挑战。面对这些挑战亟须构建数据安全的防护体系。

多管齐下构建“跨省通办”数据安全防护体系。“跨省通办”中数据共享的本质是借助现代数字技术在权力平等而目标多元的地区主体间建立全面可持续的合作关系，从而提供更加优质、高效、无缝隙的公共服务。“跨省通办”是提升政务服务水平、优化营商环境的重要举措，而数据安全则是其稳健发展的前提和保障。只有充分认识数据安全性的重要性，正视当前存在的问题，通过技术创新、管理优化和制度完善等多方面努力，构建起严密的数据安全防护体系，才能确保“跨省通办”在安全的轨道上不断推进。

制度建设是数据安全的重要保障。国家和地方需出台完善的数据安

全法律法规和政策文件，明确数据共享、使用、存储等各环节的法律责任和操作规范，为数据安全提供法律依据。成立专门的数据安全监管小组，定期对各地区政务部门的数据安全措施落实情况进行检查。引入第三方审计机构，对“跨省通办”中的数据安全风险进行全面审计，及时发现并整改潜在的数据安全风险点。建立数据安全应急响应机制，制定应急预案，明确数据安全事件的报告、处置流程和责任主体，确保在发生安全事件时能迅速响应、有效处理，将损失降到最低，确保数据流通共享的安全。此外，还应加强对相关工作人员的数据安全培训，提高其安全意识和操作技能，使其深刻认识数据安全性的重要性，严格遵守数据安全管理制度和操作规程。

技术是保障数据安全的基础支撑。应采用先进加密技术，如国密算法、区块链加密等，对数据进行加密存储与传输，确保数据在传输、存储过程中不被窃取或篡改。比如，启用量子通信加密传输不动产登记数据，从而降低数据破解概率；利用区块链分布式账本技术，实现多个部门的数据交互共享，确保数据来源可溯、操作留痕、不可篡改。构建严格的身份认证与访问授权体系。利用多因素身份认证，如密码、指纹识别、短信验证码等组合方式，确保只有经过授权的人员能够访问特定数据。基于最小权限原则，为不同岗位、不同职责的人员分配精准的数据访问权限，避免权限滥用。建立定期的数据备份机制，将重要数据备份至多种存储介质，并分别存储于不同地理位置。同时，制定完善的数据恢复计划和演练方案，一旦遭遇数据丢失或损坏，能够快速恢复数据，保障“跨省通办”业务的连续性。同时，建立严格的访问控制机制，按照“最小必要原则”，对不同岗位人员设置不同的数据访问权限，限定其仅能查看办理业

务所需字段，减少数据泄露风险。

加强对数据全生命周期的管理。首先，在数据采集源头，要制定严格且清晰的数据采集范围和标准。以“跨省通办”的社保业务为例，明确规定仅能采集与参保信息、缴费记录、待遇领取资格等直接相关的信息，杜绝过度采集。同时，设定详细的数据格式、内容规范，确保录入的数据准确无误。通过对采集人员进行专业培训，使其熟练掌握采集标准，从一开始就保证数据质量与合规性。其次，数据存储环节至关重要，需建立安全级别极高的数据中心。采用先进的多重备份技术，不仅在本地进行多副本备份，还通过异地备份的方式，确保在突发状况下数据不丢失。运用灾备技术构建完善的灾备体系，实时或准实时同步数据到灾备中心，当主数据中心遭遇火灾、地震等自然灾害或其他重大事故时，灾备中心能迅速接管业务，保障数据的持续可用性。最后，在数据使用过程中，搭建全面的监控与审计系统。对每一次数据的调用、查询、修改等操作进行详细记录，包括操作时间、操作人员、操作内容等。利用大数据分析技术，对操作记录进行实时分析，及时发现异常操作行为，如短时间内大量的数据下载、非工作时间的敏感数据访问等，一旦发现异常，立即启动调查处理机制。此外，定期开展数据安全风险评估不可或缺。组织专业的安全团队，运用漏洞扫描工具、渗透测试等手段，全面检测系统存在的安全隐患。针对发现的系统漏洞，及时安排技术人员进行修复，并对修复效果进行验证。通过持续的风险评估与漏洞修复，不断提升系统的安全防护能力，为“跨省通办”的数据安全保驾护航。

