CAICT 中国信通院

集智 专题报告

算力网络数据安全研究报告

(2024 年)

中国信息通信研究院安全研究所

2024年12月

版权声明

前　言

近年来，国家高度重视算力网络的建设与发展。2023 年底，政府部门接连印发《算力基础设施高质量发展行动计划》与《关于深入实施“东数西算”工程 加快构建全国一体化算力网的实施意见》，作为数字经济的重要支柱，算力赋能千行百业的乘数效应正在凸显。算力网络作为支撑数字经济高质量发展的关键基础设施，对构建数据要素可信流通体系有着重要支撑作用。全国一体化的算力网络能够为数据要素流通提供高效调度、普惠易用的计算资源保障服务，有助于实现不同地域、不同行业的数据资源高效配置，打破“数据孤岛”，提高数据要素开发利用效率。但前提是要保障数据安全，在算力网络规划建设阶段需要同步筹划构建数据安全保护体系，保障算力网络采集的各类数据、编排调度数据、算力交易信息和用户数据的机密性、完整性、可用性和可追溯性，以高水平安全保障能力促进数字经济高质量发展。

本报告从算力网络的概念、国内外发展现状出发，梳理了目前算力网络的主要应用场景、运营模式及技术架构与关键技术，在此基础上，分析了算力网络面临的数据安全风险与挑战，进而提出算力网络数据安全保护框架和关键安全措施，最后对算力网络数据安全发展提出几点建议。鉴于算力网络涉及的机制、技术仍在持续优化与完善，我们对该领域的研究还有待进一步深化，报告中存在不足之处，敬请大家批评指正。

目 录

图 目 录

表 目 录

一、概述

（一）背景

数字时代，5G、6G、云计算和大数据等新技术刺激算力需求不断提升，特别是以 ChatGPT、Sora 为代表的人工智能应用、大模型训练等新应用、新需求推动算力需求急速增长。算力作为新型生产力，已成为经济增长的助推器，全球算力网络竞争新赛道已开启。

近年来，我国持续推进网络基础设施、算力基础设施、应用基础设施等数字基础设施的布局与建设。为深入贯彻落实党中央、国务院决策部署，加快构建全国一体化算力网，以算力高质量发展支撑经济高质量发展，国家陆续出台多项政策举措。2021 年 5 月，国家发展改革委、中央网信办、工业和信息化部、国家能源局印发《全国一体化大数据中心协同创新体系算力枢纽实施方案》提出“构建数据中心、云计算、大数据一体化的新型算力网络体系，促进数据要素流通应用”，正式将算力网络纳入国家新型基础设施发展建设体系。2023 年 10 月，工业和信息化部、中央网信办、教育部、国家卫生健康委员会、中国人民银行、国务院国有资产监督管理委员会发布《算力基础设施高质量发展行动计划》将“提升算力高效运载能力”作为重点任务之一，提出优化算力高效运载质量、强化算力接入网络能力、提升枢纽网络传输效率、探索算力协调调度机制四个工作事项，并设置了“算网融合发展行动”，以进一步凝聚产业共识、强化政策引导，全面推动我国算力基础设施高质量发展。2023 年 12 月，国家发展改革委、国家数据局、中央网信办、工业和信息化部、国家能源局印发《关于深入实

施“东数西算”工程 加快构建全国一体化算力网的实施意见》，再次明确“算力网是支撑数字经济高质量发展的关键基础设施，可通过网络连接多源异构、海量泛在算力，实现资源高效调度、设施绿色低碳、算力灵活供给、服务智能随需”，并提出从提升算力网络传输效能、探索算网协同运用机制、构建跨区域算力调度体系三方面“统筹东中西部算力的一体化协同”工作任务，推动国家算力基础设施的现代化和一体化。顶层设计领航之下，多地政府纷纷出台关于算力的政策及发展目标。2024 年 4 月，《北京市算力基础设施建设实施方案（2024-2027 年）》发布；2024 年 11 月，《四川省算力基础设施高质量发展行动方案（2024-2027 年）》发布；上海印发《上海市进一步推进新型基础设施建设行动方案（2023-2026 年）》；青海出台《青海省加快融入“东数西算”国家布局工作方案》；贵州发布《面向全国的算力保障基地建设规划》。算力网络赋能千行百业，加速向政务、工业、交通、医疗等各行业各领域渗透。数字政府、工业互联网、自动驾驶、智慧医疗等融合应用加速涌现，算力的应用边界不断拓展，算力网络已成为承载信息数据的重要基础设施。

（二）算力网络发展现状

1.算力网络概念的提出

当前，以信息技术为代表的新一轮科技革命和产业变革浪潮中，数字产业化和产业数字化转型升级进度加快，特别是 5G、大数据、人工智能等新兴技术快速普及应用，全社会数据总量爆发式增长，数据资源存储、计算和应用需求大幅提升。以新材料、生物制药、基因

技术、金融科技、深海空天等为代表的前沿科技和未来产业，对算力基础设施提出了新要求，特别是对算网深度融合实现算力灵活调度、高速数据传输的应用需求与日俱增。为回应产业需求，自 2019 年起，我国三大运营商、通信设备厂商分别提出算力网络、算力感知网络、计算优先网络等相关技术概念，开启了算网融合方向技术探索的新篇章。

2021 年 7 月，由中国电信牵头制定的首个算力网络国际标准《算力网络框架与架构》（Y.2501）在国际电信联盟电信标准化部门（ITU-T）会议上审议通过，并于 9 月正式发布。标准中关于算力网络的定义在业界基本形成共识，即算力网络是一种新型网络，通过网络控制平台（如集中式控制器、分布式路由协议等）分发计算、存储、网络等服务节点的资源信息，实现资源优化分配。算力网络中计算资源（如 CPU、GPU、FPGA 等处理能力）与通信网络深度融合，通过“算力大脑”实现对网络中算力的统一感知、编排、调度。

2.国外算力网络发展现状

政策方面，全球各国不断出台政策与投入资金支持算力网络产业发展。2020 年 11 月，美国政府发布《引领未来先进计算生态系统：战略计划》，计划构建覆盖政产学研的国家级算力体系。2024 年 7 月，美国能源部（DOE）发布了一份征求意见书（RFP），计划投入 5 亿美元开发一台名为 Discovery 的新型超级计算机，以替代当前全球最快的超级计算机 Frontier。欧盟于 2021 年 3 月发布《2030 数字指南针：欧洲数字十年之路》，拟到 2030 年累计部署 1 万个边缘计算节

点，为 75％的欧盟企业提供云计算、大数据和人工智能服务，让所有欧盟家庭实现千兆连接。日本 2014 年启动名为“富岳”（Fugaku）的 E 级（百亿亿次级计算）计划，旨在研制国家高性能计算基础设施。

产业方面，国外算力网络的形态主要包括先进计算生态系统、高性能计算联盟、超级计算机能力网络、数据中心算力调度体系等，其发展目标一般是为多样化的业务需求提供基础算力支持。

美国一方面由政府部门主导，采用政企合作模式，为各行业技术创新提供共享的算力和数据资源，以促进相关技术的突破创新。如 2020 年 3 月，美国白宫科技政策办公室、能源部和 IBM 牵头成立新冠肺炎高性能计算（HPC）联盟，汇聚来自领先科技企业（如亚马逊、谷歌云）、国家级研究机构和政府组织（如美国宇航局），以及顶尖学术机构（如麻省理工学院）的算力资源，为研究人员提供超级计算能力，加速新冠肺炎疫情防控的进程。2024 年 1 月，美国国家科学基金会（NSF）等 10 个政府机构携手谷歌、Meta、英特尔、英伟达等 25 家科技巨头，共同推出国家人工智能研究资源（NAIRR）试点计划，为美研究人员和教育工作者提供先进计算、数据集、模型、软件、培训等支持，推进研究基础设施共享。另一方面，在商业领域，云厂商、数据中心运营商主导，在全球多地搭建数据中心，打造全球算力调度体系，为客户提供更便捷的网络与算力服务。亚马逊、谷歌、IBM 等科技巨头均拥有各自的全球网络，如微软全球网络连接 61 个 Azure 区域中的数据中心，在全球范围内部署大型边缘节点网格，满足多样化的用户需求。Equinix 建立网间互联平台 Platform Equinix、Equinix

Internet Exchange 和 Equinix Cloud Exchange Fabric 等多种算力分配解决方案，为客户建立起跨网络的私有连接，灵活分配算力。

欧盟积极发展超级计算机，旨在整合欧洲内部算力，推动欧洲信息技术发展。2018 年 1 月，欧盟委员会发起“欧洲高性能计算共同计划”（EuroHPC），选定了包括保加利亚的索菲亚、捷克的俄斯特拉发、芬兰的卡亚尼等在内的 8 个国家和地区来建设世界级超级计算机中心，目前位于芬兰、意大利、卢森堡的世界领先的超级计算机已部署并投入使用，服务于科学研究、工业创新、公共服务等领域。2022 年，欧盟对该计划进行升级，宣布投资 80 亿欧元，进一步推动下一代超级计算技术（包括 E 级计算和后 E 级计算）的研发和应用。

另外，欧盟于 2020 年启动欧洲超级计算机能力网络（EuroCC）项目，项目覆盖 33 个欧洲国家，旨在将欧洲内部现有的超级计算中心连接起来，为整个欧洲提供计算能力。2022 年底 EuroCC 项目一期结束，EuroCC 2 随即启动，继续推动欧盟高性能计算（HPC）、高性能数据分析（HPDA）和人工智能（AI）发展。

EuroHPC 和 EuroCC 是欧盟在高性能计算领域两大互相关联、互补的项目，两个项目在资源调度和规划上紧密相关。EuroHPC 提供高性能计算的基础设施和技术开发，位于战略层，负责制定政策、分配资金并主导关键技术研发和基础算力设施建设。而 EuroCC 则重点推行高性能计算的应用推广和算力共享，位于实施层，负责在各成员国落地高性能计算设施、推动各国技术能力均衡发展，帮助企业和科研机构获得上述算力资源。EuroHPC 和 EuroCC 结合，形成从技

术研发到技术普及的完整产业链，为欧盟高性能计算的发展奠定的基础。

3.我国算力网络发展现状

在国家政策大力支持下，算力网络逐步成为产业发展热点。由“东数西算”工程牵引，我国已形成算力资源储备充足、算力调度初具规模、算力交易初现雏形的算网服务体系。在算力基础设施方面，全国数据中心建设步伐加快。截至 2024 年 6 月，我国在用算力中心标准机架超过 830 万架，算力总规模达到 246 EFLOPS（FP32），位居世界前列[1]。随着 8 大国家枢纽节点，10 大数据中心集群建设落地，算力一体化格局已初步显现。同时，“IPv6+”“全光网”等相关产业快速发展，我国算力承载网络基础不断夯实。在算力调度方面，算力调度平台建设进展迅猛。作为算力网络建设的中坚力量，三大电信运营商高度重视算力网络，积极开展算力网络技术研究，算网融合平台已经从早期理论构想走向加速建设阶段。除电信运营商外，阿里云、腾讯云等云厂商，华为、中兴、浪潮等数据中心服务厂商也积极参与算网融合建设，推动算力网络关键设备研发，优化算网功能、性能。八大算力枢纽节点均已开始建设各自的算力调度平台。同时，运营商也积极开展算力调度平台建设，中国电信、中国联通相继发布算力调度平台“息壤”“星罗”，中国移动牵头打造“百川”算力并网平台。在算力应用方面，行业赋能效益日益显现。随着我国算力规模的持续扩大，互联网、大数据、人工智能等与实体经济深度融合，算力应用的新业态、

[1] 数据来源：中国信息通信研究院《中国综合算力指数（2024 年）》

新模式正加速涌现，一方面算力正加速向政务、工业、交通、医疗等各行业各领域渗透，成为传统产业智能化改造和数字化转型的重要支点。另一方面，围绕“大算力+大数据+大模型”，智能算力成为全球数字化转型升级的重要竞争力。

在算力网络技术方面，原创技术不断突破。中国移动突破算力路由、算力原生、全调度以太网等原创技术，发布软硬一体计算架构、天元操作系统、天池 SDN、全调度以太网（GSE）DPU 芯片等自主创新成果。在 2024 年世界移动通信大会上，中国移动发布了全球首台算力路由器（CATS Router），该路由器具备算力感知、通告、联合路由功能，打破了传统互联网路由方式，在网络中引入算力因子，解决算力和网络联合路由的问题，支撑 AR/VR、车联网、AI 推理等时延和计算敏感型业务需求。中国电信创新算力网关，提出基于 BGP 的算力网络核心协议 CP-BGP，通过物理硬件和网络操作系统（NOS）的解耦，让标准化的硬件与算力网络相关协议进行组合适配，同时引入了基础设施程序员开发工具包（Infrastructure Programmer Development Kit，IPDK）、数据平面开发套件（Data Plane Development Kit，DPDK）等软硬件产品与技术，实现了算力网关产品提供跨平台的方案部署和性能加速，从而保证了现网可平滑引入算力网关设备。中国联通提出 CUBE-Net3.0 网络创新体系，并以 CUBE-Net3.0 作为未来 5～10 年网络转型的顶层架构设计，提出算网一体、云光一体、确定性服务三大业务使命和一个基于 AI 和数据驱动的管控体系，布局八大重点科研创新方向，开展自主创新和联合攻关，在此基础上，

推出算网设备通用操作系统（CUNOS）、算网模块化交换机（CU-Switch）等技术成果，并持续推进产业链和创新链持续融合。华为 6G 研究团队率先提出基于端边云环境通算融合的移动算力网络架构及关键技术，在 6G 网络架构的控制层面，引入通信与计算深度协同的功能、接口和协议，直接通过未来 3GPP 标准化的信令来实现通算融合甚至一体化，构建出一种开放的机制，整合网络内外的各类算力资源，并基于网络架构内生的通算融合机制，为 6G 业务创新提供新型的基础设施。

在算力网络标准方面，技术、安全等相关标准研制工作有序开展。国标层面，2023 年 11 月，算力基础设施领域国家标准 GB/T 43331-2023《互联网数据中心（IDC）技术和分级要求》正式发布。行标层面，CCSA 各标准工作组已立项开展 70 余项算力网络相关标准文稿和研究报告。算力网络技术方面，TC3 开展针对算力标识、算力路由、算力度量、算网融合控制等算力网络关键技术的标准化工作，已发布 YD/T 4255-2023《算力网络 总体技术要求》、YD/T 6044-2024《算力网络 算力度量与算力建模技术要求》、YD/T 6045-2024《算力网络 算力路由协议技术要求》、YD/T 6046-2024《算力网络 算网编排管理技术要求》等技术标准；TC7 发布了 YD/T 6047-2024《算力网络 运营管理技术要求》；TC13 研究面向工业互联网园区网络的算力网络应用场景和部署技术要求。算力网络安全方面，TC8 开展了算力网络总体安全、数据安全、计算节点安全、算网服务交易安全、算力并网安全、典型业务安全等标准编制工作；TC5 对算力网络安全需求和关

键技术开展相关研究，并印发 SR 434-2023《算力网络安全需求及关键技术研究》报告。

（三）算力网络技术体系

1.算力网络体系架构

当前，运营商、云服务商、第三方数据中心服务商以及设备厂商积极推动算力网络技术发展，算力网络技术体系架构逐步清晰，并基本形成共识，已经形成了基础设施层、编排管理层、运营服务层三层技术架构，各层承载不同的数据并协同发挥作用为产业应用提供算力支撑，如图 1 所示。

图 1 算力网络技术架构

基础设施层是算力网络运行的计算和网络能力基础，提供泛在异构计算资源，实现云、边、端算力高速互联，满足数据高效无损传输需求。基础设施层承载的数据包括计算处理中的数据、边/端节点数据

等服务数据，以及基础设施运维管理策略、对存储数据的访问控制策略、运维监测数据等运营数据。

编排管理层是算力网络的调度中枢，实现对算力、网络资源的感知和统一度量与标识，并通过融合编排技术对算网资源进行统一编排、智能调度和全局优化。编排管理层数据主要包括算力节点数据、算力资源数据、编排数据、调度数据、编排管理业务平台运维数据等。

运营服务层是算力网络的服务能力提供平台，实现算力网络产品的一体化供给，为算力用户提供一站式服务和智能无感的体验。运营服务层主要数据类型包括用户账户信息、算力服务信息、交易信息和运营服务平台自身运维信息等。

2.算力网络关键技术

算力网络引入了算力感知、算力度量与建模、算力编排与调度、网络承载等关键技术来实现对算力的泛在连接与灵活调度。

算力感知是算力编排与调度的基础，包括算力网络对算力资源和网络资源的感知，也包括对业务需求的全面感知。一方面，各算力节点将算网信息（包括部署位置状态、CPU/GPU 计算力、存储容量、网络拓扑、带宽时延等信息）度量建模后上报，算力网络聚合节点上报的算网信息，构建全局统一的算网状态视图。另一方面，算力网络完成对业务算网需求的解析，实现对业务的感知，从而基于业务需求进行算力调度。算力度量与建模技术针对泛在、异构的算力，通过模型函数将不同类型的算力资源映射到统一的量纲维度，为算力路由、算力管理和算力计费等提供标准统一的度量规则，通过统一的算力度

量体系和异构计算资源的映射机制，实现算力资源的合理分配和高效调用。算力编排与调度技术是指对各算力节点的生命周期管理及将算力需求调度到适合的节点上，具体来说是基于策略或 AI 算法，实现算力资源实例化、弹性扩缩容、资源预留、分配与释放等功能。算力网络承载技术为上层提供高效协同的连接和传输能力，主要包括 SRv6（Segment Routing over IPv6）、网络切片、网络感知、确定性网络技术。SRv6 具有扩展性和可编程性，实现服务功能链的动态配置和优化，支撑网络资源敏捷、按需、可靠调度。网络切片技术按逻辑划分网络实现资源与服务隔离，满足不同业务对网络能力的差异化要求。网络感知技术通过在通信报文中写入资源信息并通过特定协议（如计算优先网络协议，简称 CFN）完成交互，以达到资源信息共享的目的。确定性网络技术通过综合流量整形、队列调度、时钟同步等机制，实现传输过程的低抖动、高可靠。

（四）算力网络应用场景

在算力网络服务生态中，参与者主要包括三类，分别是算力消费者、算力运营者与算力供应者。算力消费者包含以互联网厂商为代表的算力的使用者。算力供应者包含以云服务商、电信运营商为代表的算力资源的拥有者。算力运营者为中立可信的运营者，如电信运营商、政府认可的运营企业等。算网运营者通过构建算力网络交易平台，搭建供应方和需求方的桥梁，算力供应者通过算力网络交易平台进行身份信息注册后，将计算资源、存储资源、网络资源、数据资源、模型资源等提供给算力网络需求方以完成算网需求。算力消费者则通过算

力网络交易平台选购并获取算力网络资源，并支付使用费用。

面向算力供应者，算力网络吸纳全社会的算力资源。算力供应者将自己的计算、存储等资源连接到算力网络交易平台，共享自己的服务度量值、状态信息、资源类型、服务类型网络位置等相关信息，通过提供算力服务获得收益。

面向算力消费者，算力网络提供任务式服务模式。通过分析算力消费者实际业务需求，从海量资源中匹配调度最佳方案，完成任务并达到客户的预期。主要特点包括：通过业务编排，自动生成解决方案；通过智能算法寻找算网最佳资源，调度高性能、低成本的算网资源降低客户成本；通过业务和资源感知以及跨域弹性调度能力，实时监控，保障业务健康状态和按时按量完成。

随着数字化转型的纵深推进，算力需求不断提升，各类算力应用场景快速涌现，主要可分为：生活场景、行业场景、社会场景，具体如下表所示。以车路协同算力网络为例，车、路作为服务对象接入算力网络，算力网络为实现车路协同提供边缘下沉计算节点、边缘云、中心云三级算力服务。边缘下沉节点提供低时延的算力供给，负责图像、视频等原始数据的就近解算；边缘云提供准实时的算力供给，负责分担部分原始数据的解算任务；中心云提供非实时的算力供给，负责交通大模型的训练等任务。

表 1 算力网络主要应用场景

算力网络主要应用场景类别	相关应用	应用算力需求特点	算力网络主要应用优势

生活场景	VR 互动、云游戏、新媒体直播、家庭安防等	大带宽、低时延	算力网络通过对云边端算力资源以及第三方能力的分配调度，降低终端设备的计算开销和相关的硬件配置门槛，并缩短传输时延，提升相关应用的用户体验。
行业场景	智慧交通、智慧医疗、车联网等	准确、实时	算力网络通过深度融合人工智能、物联网、5G、边缘计算、数字孪生等技术，协同云、边、端等算力，助力行业数字化转型。
社会场景	智能科学模拟、数字化政府治理、平台型算力共享等	算力消耗高	算力网络将高算力消耗的计算任务拆解分布到泛在的存量算力上运行，可极大地降低算力成本。

二、算力网络数据安全风险挑战

在算网融合的架构下，异构节点数量庞大、网络互联程度升级、资源调度智能自动，安全边界随之打破，数据安全与网络安全、新技术安全相互渗透、相互影响，单点风险可能产生全局影响。综合来看，算力网络基础设施层、编排管理层、运营服务层面临如下数据安全风险：基础设施层面，异构算力节点的接入和网络新技术的引入增加了数据安全防护的难度。编排管理层面，算力网络特有的资源数据和智能化编排方式使得数据安全与网络安全、新技术安全相互交织。运营服务层面，算网交易信息、算网用户数据都面临较大安全风险。

（一）基础设施层数据安全风险挑战

1.数据跨节点跨主体跨域流转，暴露面增大

算力需求场景日益复杂，算力的泛在协同需求持续增多，算力节点灵活接入，存在广泛的、动态的数据调度，数据跨主体、跨系统、跨域甚至跨境场景增加，频繁的资源链接将导致数据暴露面增大，数据资产遭受攻击的概率也将大幅增加。一是分布式计算增加了数据被截获或篡改的风险。算力网络通常涉及多个节点和设备进行分布式计算，数据在不同的节点之间传输和处理，分散的架构使得数据在传输过程中可能会经过多个不安全的环节，被截取或篡改的风险。二是远程数据使用增加了数据恶意访问风险。算力网络包含云计算、边缘计算、端计算，这使得数据存储和处理不再局限于本地设备。云服务提供商和边缘设备可能成为潜在的攻击目标，增加了数据被恶意访问的风险。三是多方参与增加了泄露的可能性。算力网络中，通常有多个参与方（如用户、服务提供商、第三方服务等）共同处理数据。这种多方协作虽然提高了计算效率，但也意味着数据在多个参与方之间流动，增加了数据泄露的可能性。

2.异构节点复杂多样，带来数据安全挑战

算力网络基础设施层算力来源多样，涉及云数据中心、边缘计算设施、终端设备等异构、泛在的算力节点，每个节点贡献其处理能力来共同完成复杂的计算任务，然而，这种网络结构由于节点之间的差异性可能会带来一些数据安全风险。一是弱算力节点易被攻破，引发全局风险。算力网络边缘节点、端节点受限于资源和成本，往往安全

防护能力较弱，易成为安全短板被外部攻击者攻破。如果一个节点被攻破，它可能会成为攻击者进入整个网络的入口，作为跳板向算力网络发动横向或纵向攻击，造成单点风险向全局扩散。二是节点安全性不统一，易降低系统整体安全水平。不同的节点可能运行在不同安全级别的操作系统上，有的可能使用了较弱的安全措施。例如，在节点间传输数据时，若某节点没有采用足够强度的加密技术，就会迫使系统选择低级别的加密技术，敏感数据就有可能被截获，如果节点密钥管理不当也可能导致数据泄露。三是异构节点的接入增加了节点管理的复杂性，可能导致安全漏洞的出现，例如未及时更新安全补丁或配置不当。

3.网络新技术引入新的安全风险

算力网络应用 SRv6、网络切片、网络感知、确定性网络等新技术来实现算力资源的连接与灵活调度，但新技术的引入也带来了新的安全风险。例如，SRv6 作为一种基于 IPv6 的源路由技术，虽然带来了网络灵活性和可编程性的提升，但也带来了数据流被截取、数据被篡改、数据被伪造等风险。一是 SRv6 使用显式路径编码，这增加了路径的可见性，但也可能暴露路径信息给潜在的攻击者，攻击者可能通过修改数据包中的路径信息，以重定向流量到恶意节点，截取正常数据流。也可能通过中间人攻击等方式篡改 SRv6 数据包的内容或路径信息，影响通信的完整性和可用性。攻击者还可以伪造 SRv6 数据包，冒充合法用户或服务向目标发送虚假信息，造成服务中断、数据丢失等问题。二是 SRv6 允许数据包的发送方指定数据包在网络中的

传输路径，如果路径信息被拦截，攻击者可能了解到网络拓扑的敏感细节。如果攻击者控制路径上的某个节点，则可能截获并监听经过该节点的数据流，导致敏感信息泄露。

（二）编排管理层数据安全风险挑战

1.算网特有数据资源将成为新的攻击目标

算力编排层作为算力网络体系架构中的关键组成部分，承担着对算网资源的统一管理、统一编排、智能调度和全局优化等重要职责。一方面，作为算网资源与运营服务间的枢纽，编排管理层汇聚了大量算力资源数据、编排数据、调度数据等特有敏感数据。这些数据会成为新的攻击目标，一旦这些数据被窃取，可能会导致算力网络的非法利用；若这些数据被篡改，将影响运营服务的正常开展，甚至会造成算力网络运行事故。另一方面，算网编排层通过对高复杂度的算网环境进行通用化数学建模，利用智能核心算法，实现一系列智能控制和自动决策。其中涉及大量的 AI 模型算法，针对这些算法的数据投毒、模型窃取等攻击，将影响算法的结果走向，从而影响算力网络的运行调度。

2.数据流转路径复杂，审计溯源困难

算力网络的分布式计算环境、动态资源调度、数据分割与并行处理等因素使得算力网络的数据流转路径异常复杂，数据流转存证困难，数据流转过程中若发生数据泄露，难以对泄露点进行追溯。一是算力网络数据流转路径复杂。首先，算力网络通常由多个计算节点组成，这些节点可以是数据中心、云服务、边缘设备等，数据可能需要在这

些节点之间多次传输和处理，数据流转路径复杂。其次，算力网络根据实时的工作负载智能化调整计算资源，每次的数据处理路径都可能不同，这种动态的变化使得数据流转路径难以固定。而且，为了提高处理速度，大数据集可能会被分割成多个部分，分别在不同的节点上并行处理，每个部分的数据路径可能不同，并行处理后，中间结果需要重新合并，这个过程涉及多个节点之间的通信和协调，进一步增加了数据路径的复杂性。二是复杂环境下存证困难。为了实现有效的存证和溯源，需要详细记录数据的每一次操作和流转，在算力网络高度分布式和动态的环境中记录整个数据流转路径中的每一个环节是一项巨大的挑战，大量的日志记录会占用大量存储资源，并增加系统处理负担，对大量分散节点的协作行为进行审计追踪也是一个极其复杂的过程。

（三）运营服务层数据安全风险挑战

1.用户数据与算网交易信息面临新风险

算力网络运营服务层作为算力网络的运营门户，涉及大量数据的用户数据和算网交易信息，这些信息一旦遭到泄露或被篡改，将造成严重后果。一是用户数据可能被窃取和损坏。算力网络运营服务层往往提供外包计算服务，即用户将数据交给算力网络进行计算分析。在这个过程中，数据从用户端传输到计算节点，再返回结果给用户。这个过程中存在多个安全风险点，如数据在传输过程中被截获、计算过程中被篡改或计算结果不可信等。二是算网交易信息泄露可能影响算网业务正常开展。运营服务层面向海量用户及节点输出算力服务，如

果交易数据访问权限管理不当，将会面临交易数据泄露、交易信息篡改等数据安全风险，引发恶意计费、逃避计费等问题，扰乱算力交易正常秩序，甚至引起用户信任危机。

2.服务关系多级嵌套，安全责任边界难厘清

算力网络中涉及基础通信网、云、IDC 等多种网络和系统，涉及运营商、云服务商、设备商、超算中心、用户等诸多主体，具有规模庞大、结构复杂、角色嵌套等特点，安全边界难以厘清，安全责任落实难度大。一是服务关系和服务路径动态变化，安全责任的确定随之变得异常复杂。一方面，算力网络中的资源可以根据实时的工作负载自动调整，这种动态的变化使得服务关系不断变化，增加了安全责任边界的确定难度。另一方面，系统使用智能算法来调度任务和数据，使得服务路径不可预测，进一步增加了安全责任确定的复杂性。二是算力网络跨层依赖的特点增加了安全责任划分的难度，算力网络每一层服务都依赖于其他层的服务，形成依赖关系，这种跨层依赖增加了安全管理的难度，任何一层的安全问题都可能影响到整个系统的安全性，相应地增加了安全责任划分的难度。例如，算力网络中的服务通常涉及多个层次和多个服务提供商。一个企业可能使用云服务提供商的基础架构服务（如 IaaS），而该云服务提供商又依赖于其他第三方的服务（如存储、网络等），这种多级嵌套的服务关系使得责任划分的难度大大增加。

三、算力网络数据安全应对思路

建设算力网络，必须重视安全保障，从多个维度构建算力网络安

全保障体系，实现算网建设和安全保障一体化推进。

（一）算力网络数据安全保护框架

算力网络作为新型基础设施，其具有资源范围广、参与主体多、数据对象杂、技术架构新等特点，为应对上述数据安全风险与挑战，本报告参考业界主流的算力网络安全保护方法，从管理和技术两方面出发，提出了“三横一纵”的算力网络安全保护体系框架。技术方面，针对基础设施层、编排管理层、运营服务层的数据安全需求和技术特点，提出相应的保护要求；管理方面，从全局角度建立纵贯各层安全需求的管理体系，旨在厘清算力网络数据安全工作范畴和工作重点，为搭建算力网络数据安全保护体系提供参考。

算力网络数据安全保护框架包括安全管理和安全技术两个方面。安全管理方面，包括组织机构、人员管理、数据分类分级、权限管理等制度机制，建立算力网络数据安全管理体系。安全技术方面，针对算力网络基础设施层、编排管理层、运营服务层的数据安全风险，提出各层级的主要数据安全技术措施，建立算力网络数据安全技术防护体系。

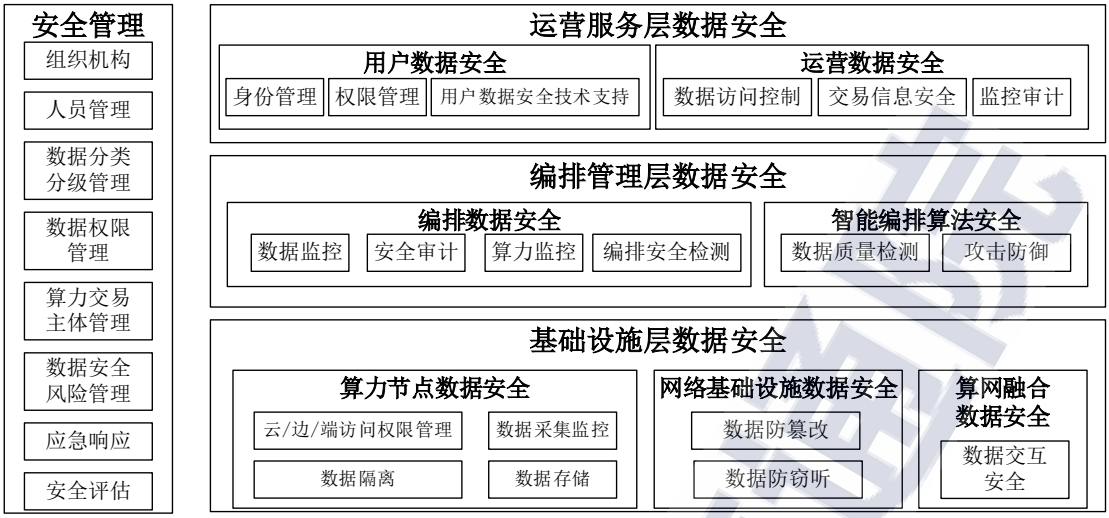

图 2 算力网络数据安全保护框架

1.算力网络数据安全管理要求

算力网络数据安全保护框架的安全管理部分主要从算力网络运营主体的角度出发，结合数据安全管理的通用元素和算力网络业务自身特点，提出构建算力网络数据安全管理体系的框架和思路。

在组织机构方面，算力网络运营主体需要建立数据安全责任制，并明确数据安全责任部门。依据《数据安全法》《工业和信息化领域数据安全管理办法（试行）》等法律法规及相关标准要求，算力网络运营主体作为电信数据处理者，需要指定数据安全管理的主要负责人和责任部门，并明确责任部门具体职责，包括但不限于组织制定数据安全管理规划、制度和标准，牵头组织开展数据分类分级，统筹负责数据处理活动安全监督管理，组织开展数据安全宣贯培训等。

在人员管理方面，算力网络运营主体需要建立数据安全人员管理体系，将数据安全管理要求纳入入职、定岗、离职等人力资源管理流程中，明确担任数据安全责任部门以及其他数据安全相关岗位的专业资质；定期进行数据安全培训与考核；明确数据安全关键岗位及人员，

并与其签署保密协议或数据安全责任书。

在数据分类分级管理方面，算力网络运营主体需依据行业主管部门相关要求及分类分级配套行业标准建立数据分类分级管理制度，对本机构的数据资产进行盘点，形成资产清单，识别重要数据和核心数据，制定重要数据目录并定期更新，采取措施开展数据分级防护，对重要数据和核心数据进行重点保护。

在数据处理权限管理方面，算力网络运营主体需要建立数据访问操作权限审批管理制度，重点关注超级管理员权限、默认账号、离职人员账号的权限管理，定期审计账号授权情况，及时回收过期账号或权限。

在算力交易主体管理方面，算力网络运营主体需要建立针对算力交易主体的管理制度。参与算力交易的主体通常具有多样性，算力网络运营主体需要对接入算力交易平台的交易主体建立准入、审计、退出等管理机制，从机构基本情况、业务经营情况、数据安全能力等方面审核交易主体，并建立交易行为监测机制，对存在违规交易行为的交易主体，或机构发生重大变化导致不再符合准入条件的交易主体，及时做好处置或清退。

在数据安全风险管理方面，算力网络运营主体需要建立数据安全风险监测预警工作机制，对数据处理活动、内外部数据流动等实施监测巡查，对异常数据操作行为进行排查预警和处置。

在应急响应和处理方面，算力网络运营主体需要建立数据安全事件应急响应工作机制，制定数据安全事件应急预案，定期开展数据安

全事件应急演练。

在安全评估方面，算力网络运营主体应当依据法律法规及相关行业标准，定期开展数据安全风险评估，形成评估报告，对评估中发现的安全风险或问题及时整改，对整改措施的有效性进行复核。

2.算力网络数据安全技术要求

算力网络数据安全保护框架的安全技术部分主要结合算力网络自身的技术架构，针对基础设施层、编排管理层、运营服务层分别面临的数据安全风险，提出相应的数据安全保护技术措施。

基础设施层需要保障算力节点数据安全、网络基础设施数据安全和算网融合数据安全。其中算力节点数据安全包括云计算、边缘计算、端计算等设备的访问权限管理、数据采集监控、数据隔离、数据存储等安全。网络基础设施安全主要包括防止 SRv6 报文被篡改、被窃听、被泄露等。算网融合数据安全是保障基础设施层设备之间、基础设施层与编排管理层之间算力度量、算力标识、算力感知、算力路由等算网信息的数据交互安全。

编排管理层需要保障算力网络编排数据安全和智能编排算法安全。其中编排数据安全包括对编排数据的安全监控、安全审计，还包括算力监控和编排安全检测等技术手段，旨在防止编排数据被泄露、篡改或恶意使用，加强对算力资源、编排、调度等敏感数据的保护。智能编排算法安全包括数据质量检测和攻击防御，数据质量检测是采用数据清洗、转换、验证、异常检测等方法提升整体数据质量水平，防止污染数据对算法计算结果的操控。攻击防御是根据算网环境下投

毒攻击、对抗样本攻击等攻击特征，部署相应技术防护手段。

运营服务层需要保障用户数据安全和算网运营数据安全。其中用户数据安全包括用户身份管理、访问权限管理和用户数据安全技术支持。通过身份管理、访问权限管理，可以保障计算节点和用户身份可识别、可验证，数据访问行为可管可控。用户数据安全技术支持是算网运营者为算网用户提供脱敏、加密、溯源、隐私计算等技术手段，供用户选择，根据算网数据安全责任划分规则，落实运营者和用户双方的数据安全责任，保障算网用户数据安全。算网运营数据安全包括运营数据访问权限管理、交易信息安全、安全监控审计等，保障算网服务相关数据的安全，进而保障算力交易安全、算网运营安全。

（二）算力网络关键安全措施

1.明确责任划分，促进责任落实

在算力网络中，数据在算力消费者、算网运营者与算力供应者之间多方流转，安全工作及责任无法仅由一方完全承担，需明确他们在整个服务提供过程中各方应做到的安全责任，才能更有效地保障算力网络整体的安全可靠。责任共担可从基础设施、算力调度、算力应用、算网数据、身份与访问管理五个层次考虑算力消费者、算网运营者、算力供应者三方的安全责任。其中，基础设施安全包括算力基础设施安全以及网络基础设施安全；算网数据安全包括算力网络用户数据安全、算力网络运营数据安全、算力网络编排数据安全、算力网络资源数据安全以及敏感个人信息安全；算力应用安全涉及应用的设计、开发、测试等全生命周期安全；身份与访问管理安全包括算力交易平台

安全以及算力网络运营者内部系统平台安全。基础设施安全应由算力运营者与算力供应者共同承担，算力调度安全与算力应用安全均应由算力运营者独立承担，算网数据及身份与访问管理安全则均应由三方共同承担。

2.数据安全能力编排与融合调度

数据安全能力编排与调度是解决算力网络数据安全问题的有效途径。数据安全能力编排调度是指，算网编排管理平台基于对算力节点的数据安全能力评估、对计算任务的需求解析，在编排管理过程中综合考虑，为用户选择最优适配的节点，最终实现计算任务的分配与数据安全能力的融合调度。具体包括如下操作：一是节点数据安全能力评估登记，当算力节点加入算网中时，对节点开展数据安全能力的评估，对于节点所处的信任域、可提供的安全计算、安全存储环境，以及是否能够支撑配置安全计算环境等信息进行评估和记录。二是需求解析，包括数据安全需求解析和计算需求解析，综合理解计算任务类型、网络需求、数据类别级别、数据机密性、计算结果准确性等要求。三是基于安全因素的编排管理，同时考虑在网算力节点的安全类别与级别、计算能力和网络状态，为用户选择最优适配节点。四是融合调度，依据调度策略，对计算资源、网络资源、存储资源、安全能力资源进行融合调度。

算力节点数据安全能力评估是算力网络提供稳定计算服务的基础。通过评估，一方面可以明确达到何种安全能力的计算节点能够接入算力网络，另一方面，可以为数据安全能力编排与融合调度提供依

据。可以从节点自身安全能力、数据安全处理能力、运行维护安全能力、数据服务提供能力等方面开展评估。节点自身安全能力评估包括节点自身具备的安全配置、所处网络环境安全情况、节点的安全评测结果、安全级别、安全服务能力等。数据安全处理能力评估是查看节点是否具备数据脱敏、数据加密、数据水印、数据销毁、数据追溯、隐私计算等数据安全处理能力。运行维护安全能力评估是评估节点是否具备基础设施提供网络攻击防护、安全检测、安全升级等安全运行维护能力，如漏洞检测、病毒扫描等。数据服务提供能力是对数据存储持久性、服务可审查性、服务可用性等服务指标进行评估。

3.采用隐私计算等技术保障计算过程与结果安全

采用隐私计算等技术保障算力网络计算过程与结果安全是目前切实可行的技术方案。算力网络采用分布式架构和网络隔离技术，可以依托多方算力分担计算任务，利用联邦学习、安全多方计算等隐私计算技术，通过密码学、安全硬件、混淆脱敏等技术手段，实现联合计算、数据发布等数据合作场景下的隐私保护，保障数据“可用不可见、可算不可识”，并可管控数据的用法用量，达到数据最小化使用的目的。一是保障数据传输安全，隐私计算技术中的密码学方法，如多方安全计算（MPC）、同态加密等，可以确保数据在传输过程中的安全性，有效防止数据泄露。二是计算过程的安全保护，隐私计算技术允许多个参与方在不泄露各自数据的情况下，共同完成某项计算任务。这种技术可以应用于算力网络中的分布式计算场景，确保计算过程的安全性和隐私性。三是结果的安全输出与验证，隐私计算技术可

以通过安全多方计算等技术手段，确保计算结果的准确性并安全地输出给相关方。同时，还可以通过零知识证明等技术手段，对计算结果进行验证，确保计算过程的正确性和安全性。

4.利用数字水印等技术助力流转追溯

由于算力网络中数据流转过程复杂，流转路径难以固定和预期，中间结果多且分散，数据流转存证、追溯困难等问题突出。因此，需要采用能适应复杂环境的数据流转追溯技术，对数据所经过的流转路径、计算活动进行记录，当发生数据损坏、泄露等情况时，可对数据流转和计算过程的回溯、责任追溯提供支撑。数据水印技术是目前应用最广泛的数据溯源技术，可通过在数据的流转过程中嵌入和更新不可见的标记记录数据的来源、处理节点、时间戳等信息实现流转追溯，但是也带来了额外的水印数据计算、存储和管理开销等问题，在算力网络复杂环境下，可以从两个方面提升数据水印的可用性。一是研究轻量级、分布式水印，仅记录关键的流转信息，相比于详细的日志记录，水印信息更加简洁，水印信息分布在各个节点上，每个节点只需记录与其相关的水印信息，减少了单个节点的存储压力。在需要时，通过分布式查询和汇总机制获取完整的水印记录，以此减轻系统处理负担。二是研究多层级水印，为每个数据片段嵌入不同的水印，确保每个片段的流转路径都有迹可循。在数据重新合并时，将各个片段的水印信息汇总，形成完整的数据流转路径记录，避免数据被分割和并行处理时普通水印失效的情况。

5.多层次、多策略综合防御措施

算力网络作为一种全新的网络架构，引入了众多新技术来实现泛在算力的协同调度与资源共享，要应对新技术带来的新风险，单一的安全技术可能无法达到满意的效果，可考虑通过多层次、多策略的综合防御措施来应对。例如针对 SRv6 数据流被截取、数据被篡改、数据被伪造等风险，可综合使用路径加密、认证授权、完整性验证、网络隔离、流量监控等手段来降低。路径加密包括使用隧道加密（如 IPsec）来保护数据包的路径信息，防止路径被拦截或篡改。认证授权方面可利用多因素身份验证（MFA）机制，来确保只有授权用户才可以发送和接收 SRv6 数据包。完整性验证包括通过数字签名或 HMAC（哈希消息认证码）来验证数据包的完整性和真实性。网络隔离是指使用网络切片和微分段技术隔离不同类型的流量，来限制攻击者横向移动的能力。另外，使用网络监控工具实时监控 SRv6 数据流，部署入侵检测和入侵防御系统（IDS/IPS）来检测和响应网络入侵行为，也可有效发现威胁，防止数据被截取或篡改。

四、算力网络数据安全发展建议

算力是数字经济时代的新型生产力。算力网络是支撑数字经济高质量发展的关键基础设施，可通过网络连接多源异构、海量泛在算力，实现资源高效调度、设施绿色低碳、算力灵活供给、服务智能随需。数据安全是算力网络健康有序发展的关键。为助力算力网络数据安全体系建设，推动实现算网数据“可知、可视、可管、可控、可溯”的目标，本报告提出以下发展建议。

（一）安全标准先行，加强引领

编制算力网络数据安全相关行业标准，引领算力网络数据安全能力体系建设。一是快速推进重点标准的制定，关注数据流转安全、计算安全、交易安全等重点环节，推进算力网络数据安全相关行业标准的制定。二是加强技术标准的研究，针对数据安全需求解析、融合编排、存证溯源等难点问题，加强相关技术研究，做好对象定位和技术切割，适时推出相关行业标准，为算网数据安全技术研发和创新明确方向和指导。三是持续推进算力网络数据安全能力测评标准编制，围绕节点自身安全能力、数据安全处理能力、运行维护安全能力、数据服务提供能力等方面，丰富指标维度，构建与完善算力网络数据安全测评体系。引导算力消费者、算力运营者与算力供应者关注算力网络数据安全能力核心指标，提升算力网络总体数据安全能力。

（二）加速技术创新，提升能力

以创新思维提升算力网络数据安全技术水平。一是积极推进算力网络技术能力与安全技术的创新融合。充分利用算力网络的智能分析与算力资源的灵活编排能力，形成安全态势主动感知、安全风险敏捷处置、安全能力按需调度的内生安全能力。二是加快安全技术在算力网络环境中的落地应用。针对算力网络分布式技术架构特点，推进区块链、隐私计算等技术在算力网络数据安全领域的落地应用。三是着重解决算力网络应用中的安全痛点。针对跨域数据流转溯源、海量节点数据安全审计等技术难题，开展技术攻关和重点

产品研发，引导业界对齐算力网络数据安全能力水平认知，持续提升行业数据安全技术水平。

（三）丰富融合应用，激发活力

以用促建，推动算力网络数据安全水平的持续提升。一是鼓励加强算网数据安全解决方案和行业应用融合创新，深入挖掘算力网络在智慧金融、智慧交通、智慧医疗、智能制造、工业互联网等场景的融合应用，完善算网数据安全供需对接。二是从算网实际应用场景中发现亟待解决的数据安全问题，以用促改，持续挖掘算力网络安全建设与能力提升目标，推动完善算力网络数据安全体系。三是打造示范应用项目，树立数据安全标杆，实现安全标准和政策落地，带动千行百业，推动算力网络价值创造、驱动数据安全能力创新发展。

（四）产学研深度协同，完善生态

打造算力网络数据安全生态，倡导产学研用深度协同。一是鼓励从事算力网络安全技术研发的科研院所、高校与安全厂商、算网运营方开展深度合作与技术交流，促进算力网络各类应用场景下数据安全技术的创新与落地应用；二是构建多方参与的算力网络数据安全生态体系。充分发挥政府部门、企业、第三方组织等各方的能动性，多举措多层次组织开展交流论坛、项目推介、实践比赛、案例评优、人才培养等产业活动，建设算力网络数据安全产业生态圈。三是深化拓展国际交流与合作，以高校、科研院所、科技领军企业为主体，通过学术会议、国际论坛、学术社区、项目合作等多

种方式，积极推进算力网络安全领域的国际交流合作，为算力网络数据安全技术发展营造良好的国际环境。

中国信息通信研究院 安全研究所

地址：北京市海淀区花园北路 52 号

邮编：100191

电话：010-62308087

传真：010-62300264

网址：www.caict.ac.cn