“东数西算”全国一体协同数据安全防护体系建设思路初探

朱洪林[1]，国强[2]，寿贝宁[2]
1. 甘肃省经济研究院，甘肃 兰州 730000；
2. 国家信息中心，北京 100045

摘要
对“东数西算”工程安全防护能力建设面临的体系化布局、统筹组织推进、统一标准规范等若干问题进行了分析，在此基础上提出了构建全国一体协同的数据安全防护体系建设思路。

关键词
东数西算；一体化协同；数据安全；责任主体；标准规范

中图分类号：TP309.7 文献标志码：A doi: 10.11959/j.issn.2096-0271.2023065

A preliminary study on the construction ideas of "Channel Computing Resources from the East to the West" national integrated collaborative data security protection system

ZHU Honglin[1], GUO Qiang[2], SHOU Beining[2]
1. Gansu Province Institute of Economic Research, Lanzhou 730000, China
2. State Information Center, Beijing 100045, China

Abstract
A number of problems faced by the construction of security protection capacity of the "Channel Computing Resources from the East to the West" project were analyzed, such as systematic layout, coordinated organization and promotion, and unified standards and norms, then the idea of building a nationwide integrated and coordinated data security protection system was proposed on the basis of that.

Key words
Channel Computing Resources from the East to the West, integration and collaboration, data security, responsible subject, standard specification

0 引言

数据显示，从2012年至2021年，我国数字经济规模从11万亿元增长到45.5万亿元，数字经济占国内生产总值比重由21.6%提升至39.8%[1]。数字经济已成为驱动我国经济高质量发展的新引擎。在此背景下，国家发展改革委、中央网信办、工业和信息化部、国家能源局四部委联合印发了《关于加快构建全国一体化大数据中心协同创新体系的指导意见》（以下简称“意见”），提出优化数据中心基础设施建设布局，加快实现数据中心集约化、规模化、绿色化发展，并提出在全国范围内建设构建“数网、数纽、数链、数脑、数盾”五大体系。随后，四部委又联合印发通知，同意在京津冀、长三角、粤港澳大湾区、成渝、内蒙古、贵州、甘肃、宁夏八地启动建设国家算力枢纽节点，并规划了10个国家数据中心集群。至此，全国一体化大数据中心体系完成总体布局设计，“东数西算”工程正式全面启动。“东数西算”正为数字经济发展绘就新版图、开拓新空间、增添新动能。

《全国一体化大数据中心协同创新体系算力枢纽实施方案》明确指出，加强对基础网络、数据中心、云平台、数据和应用的一体化安全保障，提高大数据安全可靠水平。加强对个人隐私等敏感信息的保护，确保基础设施和数据的安全。

“东数西算”工程作为国家级关键信息基础设施，承载着数字经济的丰富算力及海量数据，是境外敌对势力和不法分子重点攻击的对象。他们对“东数西算”算力网络体系等基础设施发起的网络攻击、漏洞攻击、定向攻击、数据窃取等，极易造成信息泄露、应用系统无法使用等问题，不仅影响公民和组织的合法权益，甚至将对国家安全、社会稳定造成严重的威胁。

在“东数西算”庞大、复杂的场景下，数据安全成为全国一体化大数据中心安全保障的核心。与此同时，采集、存储、流通、交换、共享、使用等数据全生命周期中的安全保障都面临着巨大挑战。首先，在数据传输阶段，数据完整性、机密性、可用性的高标准提出了挑战；第二，在数据存储阶段，数据的临时存储、容灾备份对相关数据设施的安全保障能力带来挑战；第三，数据访问阶段的制度和技术措施保障提出了挑战；第四，数据使用阶段，对事前可预防、事中可阻断、事后可溯源的全方位数据安全态势感知能力提出了挑战；最后，如何保障大数据平台的各类计算组件的正确配置、各组件之间的接口正确调用，在如此庞大的工程中也是一大挑战。

传统基于边界的纵深安全防护体系已不能灵活地适应新技术发展趋势。而随着大数据存储、计算、分析等技术的快速进步，很多新型网络攻击手段出现，使得人们仅依靠传统固化边界防护的理念在进行数据安全防护显得力不从心。传统防护方式在数据安全防护方面缺乏安全能力、灵活调度及统一运营机制，难以适应云架构环境下的业务流、数据流的融合变化，安全边界逐渐模糊，这些都对数据防护提出了新的安全保障需求。因此需要一个高度集中化的数据安全平台，实现数据安全能力的体系化集成，统筹调度围绕数据的资产识别、分类分级、流动监测、风险分析、风险评估、事件溯源等能力，向下实现安全资源拉通，向上提供安全服务支撑，构建合规有序、有效保护、高效运营的数据安全一体化防护体系。

1 一体化大数据中心安全防护体系的研究与建设现状

1.1 研究现状

通过查阅研究有关文献发现，国外学者在一体化大数据中心安全防护体系建设领域的研究文献相对较少，国内学者在该领域的研究主要集中在算力网络安全防护体系研究与新型数据中心网络安全架构研究两个方面。

第一，构建算力网络安全与数据安全防护体系。

易成岐等[2]提到，全国一体化大数据中心协同创新体系总体框架主要由国家“数网”体系、“数纽”体系、“数链”体系、“数脑”体系、“数盾”体系五大部分组成，既涵盖工程建设内容，也囊括政策工具内容，着重强调了数据安全防护亟待自主化的问题。

国家信息中心信息与网络安全部“数盾”研究小组[3]以问题为导向，对相关法律法规、政策文件、产业基础、技术发展以及数据安全面临的核心问题，特别是对数盾的基本概念、基本功能、核心价值等问题进行了研究和初步探索，提出了数盾体系技术架构。

石勇等[4]通过实地调研，提出：一要尽快编制出台统一的标准规范；二要建立数据采集标准，提升数据质量，解决数据孤岛问题；三要构建数据安全防护体系，保障数据体系发展；四要强化人才支撑，加大核心技术研发力度。

邱勤等[5]提出，算力网络作为提供算力和网络深度融合、一体化服务的新型基础设施，为网络强国、数字中国、智慧社会建设提供重要支撑。当前算力网络规划建设已步入关键时期，算力网络安全相关工作正逐步推进，但尚未形成体系化的安全架构。他们总结国内外算力网络相关研究进展，分析算力网络面临的网络安全机遇和挑战，提出安全参考架构，并梳理安全支撑技术，为推动完善算力网络安全体系建设，部署应用算力网络安全机制提供参考。

第二，开展新型数据中心网络安全架构研究。

徐建等[6]对单一数据中心的IT网络安全体系和OT网络安全体系等相关问题进行了分析研究，提出新型数据中心作为数字经济的“信息底座”，具有“高技术、高算力、高能效、高安全”的“四高”典型特征。根据国家顶层相关指导文件，结合新型数据中心典型特征和发展趋势，他们从运营技术和信息技术两个视角研究了新型数据中心安全防护体系。

综上所述，国内在大数据中心安全防护体系建设相关领域的工作一直在持续推进中，国内大多数研究提出了框架性建议，但还未对“东数西算”工程，特别是集群级、枢纽级的安全防护能力建设面临的体系化布局、统筹组织推进、统一标准规范等问题进行深入研究，还未形成以问题为导向的全国一体协同数据安全防护体系研究的公开成果。

1.2 工程建设现状

全国一体化大数据中心协同创新体系八大枢纽、十大集群的产业发展基础不一。

在基础设施方面，大部分集群具有一定规模的数据中心，少数集群（如甘肃庆阳、安徽芜湖、广东韶关等数据中心）基础薄弱。然而，已有一定规模数据中心的集群仍然面临着向算力为主的转型；而基础

薄弱的数据中心集群也需要一定时间加快基础设施的建设。

从数据中心算力方面看，东部地区数据中心在算力能力、周边应用等方面明显优于西部地区，西部地区数据中心的闲置率较高、算力能力不足。

从2022年开始，“东数西算”工程加快推进，各大枢纽节点建设进入提速升级阶段，一批重大示范项目相继开工建设。因此，在现阶段加快研究和布局构建一体化国家大数据中心安全防护体系正当其时。

2 “东数西算”工程安全防护能力建设面临新挑战

“东数西算”工程面临着参与主体多、跨“云网数安算”等技术层级和数据中心-集群-枢纽-国家的管理层级多等问题，具有跨区域交互、跨网络传输、多业务场景数据调用、数据安全边界模糊等特性，对数据安全防护体系顶层设计、协同防护机制、统一标准规范等提出了全新的挑战。

（1）“东数西算”工程安全防护能力建设的参与主体多，亟待统筹推进建设。

数据安全防护体系工程建设各相关方的主体责任、责任边界、协同机制还未明确建立，需尽快推动构建责任明确的数据安全治理格局。

（2）“东数西算”工程安全防护能力建设涉及的层级多，亟待体系化布局。

一体化安全防护体系建设所跨“云网数安算”等技术层级和数据中心-集群-枢纽-国家的管理层级多。数据安全防护体系工程建设需尽快在技术层面上构建“云网数安算”一体协同的防护体系，也需在管理层面上构建“数据中心-集群-枢纽-国家”一体协同的安全防护机制。

（3）“东数西算”工程安全防护能力建设涉及技术、服务、运营等不同方面，亟待统一标准。

国内尚未出台超大规模数据中心集群建设的标准与规范，特别是缺少集群安全防护体系建设标准，不能满足当前数据中心集群建设的需要。在“云网数安算”各技术层面，需在统一的策略指导下统筹调度众多安全设备形成协同防护能力进行一体化防护，这就迫切需要建设一套统一的技术标准规范实现安全能力的统一纳管、一体协同。

（4）跨区域数据交互，数据调用传输有风险。

“东数西算”需在全国范围内统筹调度算力资源、存储资源、网络资源、数据资源进行算力综合运算，导致整个数据传输和计算过程跨区域、远程化、网络化完成。这种海量数据跨地域交互，势必对海量数据的识别、脱敏、防泄露等手段提出新的挑战和要求。

（5）多业务调用数据，数据分类分级有难度。

高效利用数据是“东数西算”的核心要求，由于参与计算的数据主体繁多，模型大小不一，业务场景丰富、数据量大、数据结构和信息多元化，传统的数据分类分级方式效率低下，这对基于权属、区域、场景等属性将数据自动、智能、精准进行分类分级的手段提出了新的挑战和要求。

（6）全新的管控架构，安全能力聚合有挑战。

“东数西算”以数据要素与流通共享为前提，在保障数据安全的同时，应当探索安全新方向，协同数据资源创造更大价值。从数据流动规范性、安全性、可管控性等方面考虑，亟须建立一套统一完善的数据安全防护体系，将数据安全产品能力进行规范和聚合，用于高效应对和满足算网

融合、数据开放、技术创新等的新挑战和新要求。

本文重点对“东数西算”工程安全防护能力建设中急需破题的“构建责任明确的数据安全治理格局、构建国家–枢纽（集群）–数据中心三级一体协同的防护体系、加强防护体系建设的统筹指导能力”3个问题进行分析。

3 构建“东数西算”全国一体协同的数据安全防护体系初步思路

3.1 推动构建责任明确的数据安全治理格局

“东数西算”工程八大枢纽、十大集群的建设参与主体非常多元化，既有当地政府主管部门指定的参建单位，也有三大运营商、数据中心提供商、信息技术产品和服务提供商、大型互联网平台企业和大数据公司，还有基于算力基础设施开展数链、数脑业务的社会上的各种业务主体。

枢纽节点的数据安全防护体系建设的核心问题是要把数据安全治理体系建立起来，把参与枢纽建设发展的各责任主体梳理出来，梳理清楚“东数西算”工程各参与主体在工程建设、管理、运行、服务、监管等不同环节的相互关系，以及对应的网络和数据安全责任及其责任边界。对应边界模糊的新发展态势，还应建立交叉区域的齐抓共管机制。按照《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国密码法》等国家法律法规要求，以及《信息安全技术 关键信息基础设施安全保护要求》《信息安全等级保护管理办法》等标准规范要求，形成条块结合、网格化管理、共商共建共享的数据安全治理格局。数据安全体系建设各方责任主体如**图1**所示。

数据安全治理框架确立之后，从具体落实层面来讲，应从管理、技术、运营3个方面，以管理体系为指导，以数据安全管控策略为核心，以技术体系为支撑，以运营体系为贯彻执行，构建三位一体的数据安全治理体系，如**图2**所示。

图1 数据安全体系建设各方责任主体

3.2 构建国家–枢纽（集群）–数据中心一体协同的防护体系

从“东数西算”工程安全防护能力建设角度看，集群内部各数据中心为最小安全层级。由于其主要以市场化为主体进行建设，在安全系统建设上具有既要符合国家网络信息安全相关要求，又要满足自身安全需求的特点。该层级的安全需求场景多样，数量众多，难以统一建设标准，组织建设和统一管理的难度较大，应从统一安全标准、统一接入标准和统一监测标准方面予以明确其安全责任。基于以上考虑，数据安全防护体系建议设计为3层架构，总体框架如**图**3所示。

建设一体化的国家级数据安全防护平台–枢纽级数据安全防护平台–集群级数据安全防护平台，构建以集群级安全中心

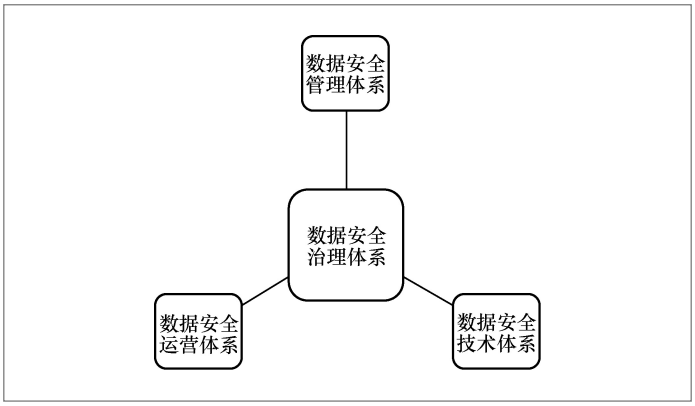

图 2 三位一体的数据安全治理体系示意图

风险管理为基础、以枢纽级安全中心信息共享为导向、以国家级安全中心统筹监管为核心的自上而下、多维度的全国一体化数据安全防护体系，并为今后向城市数据中心延伸数据安全防护平台做好设计规划。应进一步对数据安全防护相关技术标准、服务标准、管理要求进行优化和改进，

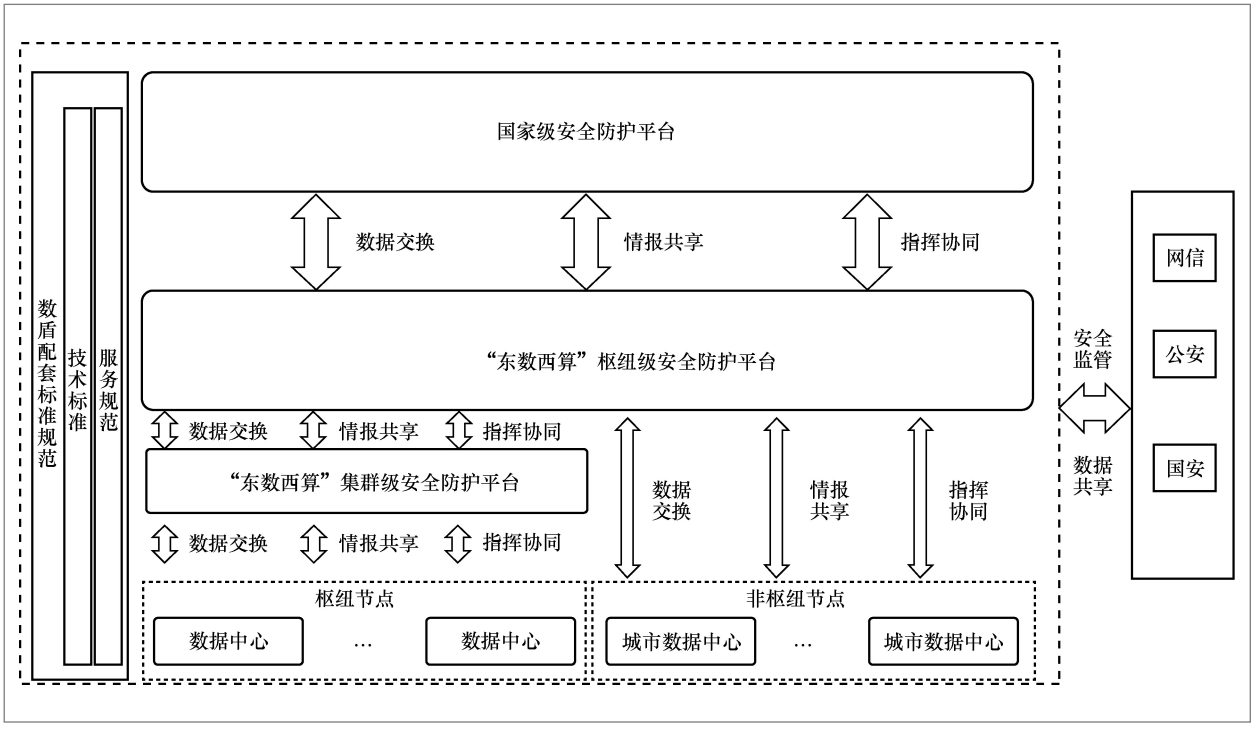

图 3 “东数西算”工程安全防护体系建设总体框架

以期未来能够实现全国定制化和大规模复制推广。考虑到现有八大枢纽在全国范围内布局较为均衡，建设枢纽级安全中心，既具有承上启下的作用，在各枢纽内新增集群时减轻国家级安全中心的负担，也便于今后对枢纽外周边区域的新增集群进行安全管控，有利于今后在全国范围内打造成8个大型区域级安全中心。

3.3 加强数据安全防护体系建设的统筹指导能力

3.3.1 建立健全数据安全防护标准规范体系

从关键信息基础设施的保护要求、控制措施、边界识别、保障指标、应急体系、检查评估等方面，加强制度规范落地建设、加强技术标准体系建设、加强应急体系规划设计。统一标准规范、统一内部数据交换接口和级联接口、统一应急处置、统一安全监测、统一运行监控等。特别是数字认证和密码应用体系的设计，一定要遵循自上而下的原则。数据安全防护体系标准规范框架如**图4**所示。

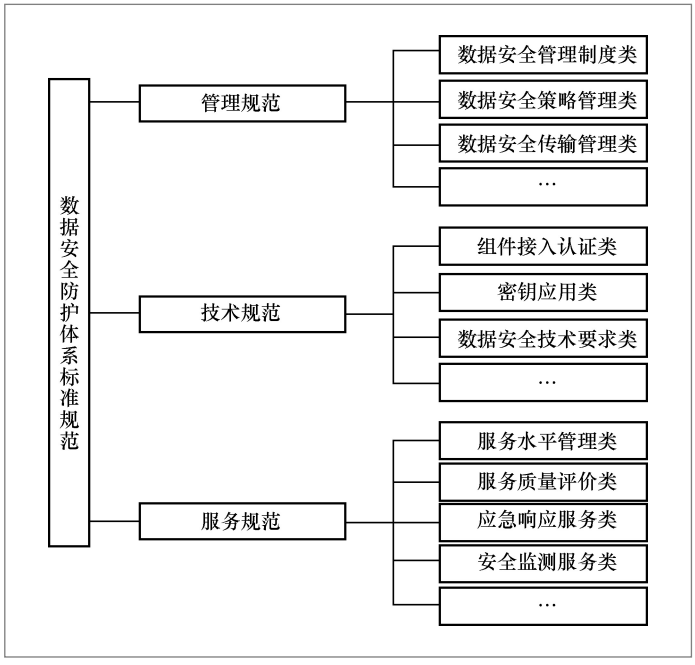

图 4 数据安全防护体系标准规范框架

从安全防护工作的管理、技术、服务3个方面建立标准规范。

推进建立“东数西算”安全防护体系的管理规范，从总体安全管理制度、数据分级分类、安全策略管理、安全传输管理、安全防护事件信息管理等方面，构建协同统一的管理制度体系，形成步调一致的安全管理工作标准。

建立“东数西算”安全技术规范体系，包括组件接入认证API标准、密码使用规范标准、数据外发和接收规范、数据交互标准等规范体系。推进“东数西算”各级算力节点参照规范进行安全防护能力建设。

创新探索“东数西算”安全服务规范。建立安全服务管理指南、服务质量评价标准、应急响应服务指南、安全监测服务指南等规范内容。强化安全运营服务管理要求，增强安全防护体系的实战运营能力。

3.3.2 构建数据安全防护安全公共服务能力

构建一体化的数据安全防护能力。从算网安全、数据安全、信息共享、监测预警等方面系统推进，构建国家、枢纽、集群三级一体化的数据安全防护以及网络出口边界防护能力，构建数据安全融合计算能力（隐私计算平台），构建重点应用的数据安全备份能力，打造数据安全防护安全监测中心、应急处置中心，搭建数据安全防护安全攻防实训靶场。

3.3.3 加强数据安全防护安全监督管理职能

建立全国统一的一体化安全管理协调

机构，从安全管理、安全建设、安全运维3个角度出发，构建安全防护管理框架，加强安全数据汇聚和态势感知、加强安全情报跨领域共享交换、加强安全事件的指挥调度能力、推动开展安全合规监督检查，打造一体化安全运营新模式，并协助网信、国安、公安等监管部门做好网络和数据安全工作的监督指导。

3.4 数据安全防护体系建设组织推进模式的建议

3.4.1 数据中心级数据安全防护体系建设

数据中心微观层面“管建”，该级别的安全能力建设主要以保障业务连续运行、极其重要数据不受破坏为重点，通过分析识别、安全防护、主动防御、事件处置等安全控制措施，以关键业务为核心实现自身的整体防控。该级别的安全能力建议主要以统一安全标准，并与集群安全中心做好统筹规划、综合管理、智能聚合为主。

3.4.2 集群/枢纽级数据安全防护体系建设

集群级层面“管战”，以各枢纽的集群投资建设单位（以企业为主体）为责任主体，以数据安全能力建设为核心目标，建立以数据安全为核心的集群安全中心，重点建设集群内部的独立数盾防护体系，从网络安全、云安全、数据安全、应用安全、安全管理等维度搭建各集群安全防护技术支撑框架。集群级数据安全防护体系以数据安全防护平台为切入点，建设安全运营中心、安全数据中心、安全能力中心，实现集群内各数据中心及其入驻单位（服务对象一般是政府/企业）的安全能力共享和安全运营协同。原则上要避免跨枢纽共用安全数据中心的情况。

集群级数据安全防护体系主要由集群安全中心投资建设单位负责建设、管理和运营。

枢纽级中观层面“管统”，以当地枢纽建设的主管部门为建设单位和责任主体，以数据安全体系化协同保护为核心目标，以信息共享为导向开展协同联防，统筹调度各微观层面数据安全能力，建立信息共享、统一指挥、快速调度、智能响应的区域一体化数据安全防护体系。以数据流动安全为中心，建立围绕跨行业、跨层级的流动防护体系。建立网络信息安全事件管理制度，对下管理、对上汇报，横向与国家有关平台对接，实现协同联动和安全数据共享（提供给枢纽节点的网信、国安、公安等监管部门的横向接口）。建设枢纽级数据安全防护安全基础设施，实现跨系统、跨区域的安全能力复用，保障政府和社会的数据共享和数据交换，实现跨层面、跨系统、跨区域的数据保护。在地域相同的情况下，枢纽级安全中心也可与集群级安全中心合并建设。

按照“管运适度分离”原则，枢纽级数据安全防护体系可由各枢纽主管部门指定的事业单位与有能力的国有企业共同负责数据安全防护基础设施的建设、管理和本地化运营服务。

3.4.3 国家级数据安全防护体系建设

宏观层面“管总”，以国家“东数西算”工程主管部门为建设单位和责任主体，以数据安全情报共享、能力统筹、体系化保护为核心目标，统筹指挥调度各区域数据安全能力，建立全国一体化数据安全防护体系的统筹协同机制。

按照“管运适度分离”原则，国家级数

据安全防护体系可由国家“东数西算”工程主管部门指定的事业单位或国有企业负责国家级数据安全防护基础设施的建设、管理和运营。

整套数据安全防护技术体系全面构筑数据安全防护技术体系建设框架，以关键信息基础设施安全保护要求为指导，以标准规范为理论依据和实施基础，向上对接国家级数据安全防护总平台、向下衔接数据中心级数据安全防护技术平台，构建集群枢纽的安全防护和安全监管两大能力，充分调动数据交换、情报共享和协调指挥等作用，实现跨区域、跨部门、跨层级地协同联动。以数据安全流通与增值为一大目标推进数据要素市场化，同步打造数据安全防护产业生态体系，着力引导网络安全产业聚集。

4 总结与展望

随着2022年年初四部委联合印发通知，8个国家算力枢纽和10个国家数据中心集群宣布确立，“东数西算”工程从规划阶段正式进入建设阶段。各枢纽在提升数据中心规模化、集约化和绿色化水平的同时，网络安全、数据安全等安全保障技术、措施和手段需要遵从三同步原则，因此“数盾”体系的规划建设也需要同步提上“东数西算”的重要议事日程，同其他“四数”一样开始同步规划、同步建设、同步使用，从而保障“东数西算”工程安全有序实施。

“东数西算”是我国推进数字经济发展的一项重大战略工程，工程的安全防护体系是工程能否发挥作用的前提。随着建设推进和技术创新，安全风险呈现出新的形态，由关注边界网络安全防护，演化到解决数据流通、共享交换和算网协同的数据安全问题，以真正发挥数据要素价值。这就要求“东数西算”工程安全防护能力建设必须做好前瞻性的规划设计，切实发挥全国一体协同创新的作用。

“东数西算”工程的安全防护能力建设应采用国家-枢纽（集群）-数据中心三级一体化协同的思路构建；在明确安全主体、厘清安全主体责任边界的基础上，构建责任明确、一体协同的数据安全工作机制；加强安全防护体系的顶层设计和标准体系的统筹指导，为工程建设、互联互通、评价评测提供参考依据。

参考文献:

[1] 中国网络空间研究院. 中国互联网发展报告-2022[M]. 北京: 电子工业出版社, 2022.
China Academy of Cyberspace Research. China internet development report-2022[M]. Beijing: Publishing House of Electronics Industry, 2022.

[2] 易成岐, 窦悦, 陈东, 等. 全国一体化大数据中心协同创新体系: 总体框架与战略价值[J]. 电子政务, 2021(6): 2-10.
YI C Q, DOU Y, CHEN D, et al. National integrated big data center collaborative innovation system: overall framework and strategic value[J]. E-Government, 2021(6): 2-10.

[3] 国家信息中心信息与网络安全部数盾研究小组. “数盾”研究与探索, 构建数据安全新理念[Z]. 2022.
Digital Shield Research Group of the Information and Cybersecurity Department of the National Information Center. Research and exploration on “Digital Shield” to construct a new concept of data security[Z]. 2022.

[4] 石勇, 寇纲, 李彪. “东数西算”战略与问题的分析研究[J]. 大数据, 2023, 9(5): 3-8.
SHI Y, KOU G, LI B. Analysis and research on the strategy and problems of “Channel

Computing Resources from the East to the West"[J]. Big Data Research, 2023, 9(5): 3-8.

[5] 邱勤, 徐天妮, 于乐, 等. 算力网络安全架构与数据安全治理技术[J]. 信息安全研究, 2022, 8(4): 340-350.
QIU Q, XU T N, YU L, et al. Computing force network security architecture and data security governance technology[J]. Journal of Information Security Research, 2022, 8(4): 340-350.

[6] 徐建, 郑伟, 郭晓春, 等. 新型数据中心网络安全体系研究[J]. 信息安全与通信保密, 2022, 20(7): 123-132.
XU J, ZHENG W, GUO X C, et al. Research on next-generation data center security system[J]. Information Security and Communications Privacy, 2022, 20(7): 123-132.

作者简介

朱洪林(1963-), 男, 甘肃省经济研究院副院长, 主要研究方向为数字经济与数据治理。

国强(1972-), 男, 国家信息中心信息系统项目管理师、副处长, 主要研究方向为数据安全、信息与网络安全。

寿贝宁(1979-), 男, 国家信息中心工程师, 主要研究方向为数据安全、信息与网络安全。

收稿日期: 2022-08-10