团体标准《算力网络安全指南》编制说明

一、 工作简况

1.1 任务来源

《算力网络安全指南》由北京网络空间安全协会和广东省网络空间安全协会提出和归口管理。

1.2 主要起草单位和工作组成员

本标准由北京网络空间安全协会、广东省网络空间安全协会共同牵头，中国移动通信集团有限公司、中国电信集团有限公司、北京启明星辰信息安全技术有限公司、华为技术有限公司、公安部第三研究所、昆仑太科(北京)技术股份有限公司、中兴通讯股份有限公司、浪潮电子信息产业股份有限公司、中国科学院软件研究所、北京交通大学、广东利通科技投资有限公司、北京蓝耘科技股份有限公司、中移（苏州）软件技术有限公司、上海天数智芯半导体有限公司、蚂蚁科技集团股份有限公司、北京长擎软件有限公司、麒麟软件有限公司、四川荣视智能科技有限公司、新华三技术有限公司、统信软件技术有限公司、北京华清信安科技有限公司、飞腾信息技术有限公司、北京关键信息基础设施安全保护中心、国源天顺科技产业集团有限公司、中移（杭州）信息技术有限公司、深圳第一线通信有限公司、北京泰尔英福科技有限公司、北京东方通网信科技有限公司、中恒达(北京)软件测评科技有限公司、积至（海南）信息技术有限公司、西南交通大学、北京邮电大学、武汉大学等多家单位共同参与编制。

1.3 立项背景及意义

以 2022 年正式启动建设的“东数西算”工程为标志的算力网络正成为我国新型数字基础设施的核心，为“数字中国”建设和数字经济发展发挥了关键支撑作用。其 2023 年下半年以来国内知名算力网络提供方屡次爆发的算力网络崩溃故障更加凸显出算力网络安全的重要性。在此背景下，中央网信办、国家发改委发布的多份政策文件均提出要加快完善“算网安全保障体系”。因此，编制标准旨在规范和指导算力网络的安全建设和管理，利于提高网络空间安全防护能力。

1.4 主要工作过程

（1）2024 年 1 月，标准正式立项；

（2）2024 年 2 月，组织参与本标准编写的人员召开项目启动会，成立规范编制小组，确立各自分工，进行初步设计，并听取各参与单位的相关意见；

（3）2024 年 3-8 月，编制组召开组内研讨会并结合调研结果，参考各类国家标准和相关政策文件，形成标准草案第一稿，后期经内部深入讨论研究，形成第二稿；

（4）2024 年 9-10 月，编制组继续召开组内研讨会，基于前期成果，经多次内部讨论研究，进一步对草案进行认真修改完善，形成征求意见稿。

二、标准编制原则和标准编制详细说明及解决的主要问题

2.1 编制原则

本标准的研究与编制工作遵循以下原则：

（1）符合性原则

本标准使用时能够与法律法规和国家强制性标准的要求保持一致，符合国家相关主管部门的要求。

（2）实用性原则

本标准规范是对算力网络实际工作成果的总结与提升，保持整体结果合理且维持原意和功能不变的同时，针对需求群体，做到可操作、可用与实用。

2. 2 文档结构

《算力网络安全指南》标准文档分为前言、范围、规范性引用文件、术语和定义、算力网络概述、算力网络的安全风险、算力网络网络安全、算力网络数据安全、算力网络应用安全、算力网络运营服务安全、算力网络安全运营、算力网络服务的主要角色及安全责任要求等部分。

2. 3 整体格式

整体格式根据 GB/T 1.1-2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的相关要求，对本标准的各要素进行编写和排版。

在标准内容汇总过程中，对各编写组成员提交部分，根据 GB/T 1.1-2020 的编写要求进行了必要的增删改，以确保符合一致性、协调性、易用性等文件的表述原则及相关规定。

2. 4 标准名称英文翻译

标准的名称“算力网络安全指南”翻译为 Guidelines for computing power network security 。

2.5 术语和定义

术语和定义中所列的术语的英文翻译，如有类似术语的标准，参考了其翻译，没有类似术语标准翻译的，通过百度翻译和谷歌翻译后进行对比，并参考网络相关翻译后进行确定。

2.6 算力网络概述

本章主要介绍了算力网络的体制架构、主要特征、服务类别及业务场景。体制架构应分为三个主要层次：基础设施层、编排管理层和运营服务层。主要特征包括有泛在连接性、智能调度性、服务多样性、安全可信性、开放性和标准化。算力网络的服务类别和业务场景应多样化，涵盖从基础计算到高级人工智能处理的各个方面，以满足不同行业和领域的业务需求。

2.7 算力网络的安全风险

本章算力网络安全风险主要可以归为技术风险、管理风险、应用风险和运营风险。

技术风险包括技术的不成熟与缺陷，配置与管理的复杂性，兼容性与互操作性问题以及缺乏必要的安全防护措施。管理风险包括管控复杂度提升，编排管理层汇聚风险，节点假冒风险以及数据管理风险。应用风险包括算力交易过程被攻击，算力并网引发安全问题以及算力网络模型即服务安全风险。运营风险包括存证溯源困难、结果可信度、交易公正性。

2.8 算力网络网络安全

本章介绍了算力网络安全框架、基础设施安全、网络通信安全。

算力网络安全框架由通用安全、运营服务安全、编排管理安全、基础设施安全和数据安全组成。在保障基础设施安全的过程中，需要着重考虑可信安全能力、可信算力能力、安全加固能力、稳定性安全保障能力、服务可访问控制、动态协同防护等。网络通信安全作为算力网络安全的关键组成部分，考虑到算力网络中数据传输的复杂性和多样性，接入安全能力、算力路由与协议安全应满足相应的安全要求。

2.9 算力网络数据安全

本章阐明了算力网络数据安全的数据流通安全、隐私计算能力、机密计算能力。

数据流通安全主要包括数据识别与分级分类、数据安全处理能力和数据流转控制能力。隐私计算能力包括基础能力、互联互通安全、数据集安全对齐、特征工程、联合建模以及联合预测。机密计算能力包括基础能力、互联互通安全、数据流动与共享安全、可信执行环境、机密计算节点和机密计算服务作出相应要求。

2.10 算力网络应用安全

本章主要介绍了算力网络应用安全的算力交易平台应用安全、算力并网安全以及模型即服务安全。

算力交易平台应用安全包括交易过程可信、权限管控、交易风险评估、交易数据安全保护和交易安全审计五个方面内容。算力并网安全主要分接入安全、数据安全和网络安全。模型即服务安全具体包括

模型保护与授权管理、数据输入验证与抗干扰、输出结果审核与解释性、服务接口安全与 API 管理、服务可用性与连续性等方面要求。

2.11 算力网络运营服务安全

本章介绍了算力网络运营服务安全的资源与调度安全、度量与标识信息安全、运营门户安全、安全管理和监控以及安全合规和风险管理。

其中，资源编排与调度安全在算力网络中至关重要，涉及网络维度安全、算力维度安全、跨纬度协同安全等。

2.12 算力网络安全运营

本章介绍了算力网络安全运营主要从安全规范与策略、安全运营人员要求、安全运营资源要求、安全运营技术要求、应急响应与恢复五大方面作出要求说明。

安全规范与策略是确保算力网络安全运营运维持续有效管理的基础，具体应满足制定安全规范、制定安全策略、定期审查和更新等要求。安全运营人员要求主要包括安全运营需求方人员要求和安全运营提供方人员要求。安全运营资源要求运营方应根据运行维护服务能力策划方案，按需建立和管理运行维护工具、服务台、服务数据、备件库、软件库和服务知识等支撑来自不同服务场景的服务需求实现，并与人员、过程和技术结合，保证资源能力满足价值实现过程中服务提供的需求。安全运营技术要求组织应根据策划对技术的要求进行技术研发，确保组织具备预防风险、发现问题、解决问题和优化创新的技术能力。应急响应与恢复要求具备应急响应与恢复组织、应急响应

与恢复计划、应急响应与恢复流程、应急响应与恢复资源保障、应急响应与恢复培训与演练相关条件。

2.13 算力网络服务的主要角色及安全责任要求

本章主要对算力网络服务的主要角色及安全责任要求作出描述。实体角色主要包括：算力网络需求方、算力网络提供方、算力应用提供方、算力网络交易服务提供方等。安全要求包括以上各角色的安全责任要求。

三、知识产权情况说明

本标准不涉及专利。

四、采用国际标准和国外先进标准情况

无采用国际标准和国外先进标准情况。

五、与现行相关法律、法规、规章及相关标准的协调性

建议本标准推荐性实施。本标准不触犯国家现行法律法规，不与其他强制性国标相冲突。

六、重大分歧意见的处理经过和依据

《算力网络安全指南》编制过程中未出现重大分歧。

七、标准性质的建议

建议《算力网络安全指南》作为推荐性团体标准发布实施。

八、贯彻标准的要求和措施建议

鉴于本标准是规范和指导算力网络的安全建设、运营和管理指南标准，标准涵盖算力网络安全的基本概念、安全风险、安全规划设计和建设实施、安全防护策略、安全管理和运营等方面的内容，能为算

力网络的安全建设和运营提供全面、实用的指导和建议，进一步提高网络空间安全防护能力。标准起草组将组织撰写标准宣贯材料，组织标准宣贯培训，促进标准顺利实施。

九、替代或废止现行相关标准的建议

无替代或废止。

十、其他应予说明的事项

无。

《算力网络安全指南》标准编制组

2024 年 10 月