# 关于核电厂网络安全准入管理制度的探究

李　实[1],王绍杰[2],万佳蓉[2],衣　然[2]
(1.大亚湾核电运营管理有限责任公司,广东 深圳 518000;2.华北计算机系统工程研究所,北京 100083)

**摘　要**:针对核电厂网络安全准入管理问题,从采购、测试、接入和人员四个角度分析了可能存在的薄弱点,结合网络安全等级保护管理方面的基本要求,基于实际案例提出了一种可行的准入管理体系。该体系探讨了核电厂中有关产品准入、外来运维设备接入以及外来人员访问的管理工作,通过规范工作流程,可保证准入供应链管理的安全可靠,对产品上线前的质量进行把关。

**关键词**:网络安全准入管理问题;网络安全等级保护;准入管理体系
**中图分类号**:TP393.08　　**文献标识码**:A　　DOI:10.19358/j.issn.2097-1788.2023.02.003
**引用格式**:李实,王绍杰,万佳蓉,等. 关于核电厂网络安全准入管理制度的探究[J].网络安全与数据治理,2023,42(2):19-24.

## Research on the network security access management system of nuclear power plants

Li Shi[1], Wang Shaojie[2], Wan Jiarong[2], Yi Ran[2]
(1.Daya Bay Nuclear Power Operations and Management Co., Ltd., Shenzhen 518000, China;
2.National Computer System Engineering Research Institute of China, Beijing 100083, China)

**Abstract**: Aiming at the cyber security access management problems of nuclear power plants, this paper analyzes the possible weaknesses from the four perspectives of procurement, testing, access and personnel, and puts forward a feasible access management system based on practical cases in combination with the basic requirements of cyber security level protection management. This system discusses the management of product access, external operation and maintenance equipment access and external personnel access in nuclear power plants. By standardizing the workflow, the safety and reliability of access supply chain management can be ensured, and the quality of products before going online can be checked.

**Key words**: cyber security access management problems; cyber security level protection; access management system



## 0 引言

作为核能发电的主要场地,核电厂的安全至关重要,应牢牢把握和深入贯彻落实习近平总书记关于核电行业“安全发展、创新发展”的重要指示,在提升核工业核心竞争力的同时,守住核安全,在外部环境、设备设施、人员管理等诸多方面严格把关,建立健全技术和管理体系,保障核电厂的网络安全准入建设,促进核能的可持续发展。

然而,随着新型信息技术的引入,核电厂网络安全受到了一定的冲击,比如核电仪控系统在向智能化、数字化方向发展的过程中,安全风险系数随之增大[1],并且在核电网络安全设备、软件、人员等的准入管理方面也存在诸多问题,这就给核电厂带来更大的安全隐患,因此应当明确问题所在,并针对问题做好应对措施。在设备正式投入使用之前,需要经过多个环节,其中值得重点关注的是一些关键节点存在的安全问题。首先,采购是必不可少且十分重要的一步,它对于设备的质量、后续进程能否顺利推进具有决定性作用;其次,在选定采购的设备后,需要对其质量、功能、性能等进行测试,确保有安全合格证明才能进入下一步;第三,设备的运行涉及使用前接入、使用中运维设备接入等方面,

无论是哪种接入,若存在安全隐患,都会对运行环境造成直接影响;最后,从采购到正式运行,必有人员的全程参与,因此人员的安全意识必须要提高。为此,下面从采购、测试、设备接入和人员四方面简要列举可能存在的问题:

(1)采购。采购是产品入厂前必备的关键步骤,而这其中也通常具备一些问题:招标时对内容的控制度不够,对招标企业的筛选和甄别不详细[2],验收时产品质量不过关,交付时间无法保证,造成工程进度缓慢甚至停滞的状态[3],这些都会影响整个供应链的运行,势必对设备的最终质量造成影响。此外,采购流程的不完善、监管不力、供应商证明材料的真实性确认等,都是采购过程中可能会出现的问题。

(2)测试。测试开始前,需要进行测试申请,同时检查物理环境、软硬件环境、测试大纲等必需文件、人员及其信息等进行检查,如若疏漏或检查不彻底,就会影响测试进度和结果,增加潜在的安全风险[4]。

(3)设备接入。首先对于设备接入而言,可能存在的问题包括:接入时需交付的文件或内容不全,接入验收团队的组成不全面,接入程序不完善,在接入过程中发现的问题未得到及时处置等,若不妥善处理这些问题,就会直接威胁到核设施的安全。其次在对设备进行运维时,往往会接入运维设备,特别是对于专业性较强的核电系统,一般由厂家进行操作,一些安全病毒便会随着运维设备接入及操作过程中的不注意而进入系统中,比如设备接入不规范、接入系统前未对电脑进行恶意代码查杀、非法外联、未经授权进行操作等,都会带来较大的安全风险。

(4)人员。人员是必不可少的因素,会参与到供应链的每个层面,对于人员方面而言,常存在的问题有:采购时对技术参数等内容要求不仔细,测试时对执行项的遗漏[5],接入时对文件清单检查不认真,不按照制度履行工作职责,技术经验不足,安全意识淡薄等。此外,在外来人员访问时,未对外来人员及其携带物品进行细致的检查,未经授权随意进行操作等,都会给予黑客进行攻击的机会。

对于这些核安全问题,国内外纷纷出台多项法律法规、政策标准来进行约束和管理[6-8],例如,美国基于 NIST 系列标准中的 NIST SP800-82 和 NIST SP800-53,制定了 RG5.71 和 RG1.152,这是专属于核电网络的标准,RG5.71 提出了针对核设施的管理方案,RG1.152 则对数字系统生命周期的各个阶段进行了说明;反应堆核仪器分技术委员会也发布了 IEC 系列标准,如 IEC62645、IEC62859、IEC63096,分别对核电系统的计算机安全程序管理和防范、核安全和网络安全间的关系、核电仪控系统网络安全控制提出相应的要求。我国也颁布了多个文件,如《中华人民共和国网络安全法》《关键信息基础设施保护条例》,2018 年四部委提出针对核电行业的《关于进一步加强核电运行安全管理的指导意见》,2020 年核安全局发布的《核动力厂网络安全技术政策》等,但是并没有针对核电厂工控网络安全的相关标准,故还需进一步完善政策体系。

本文结合《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》[9]标准中关于准入方面的要求,重点针对核电厂网络安全设备产品的采购、测试、上线前接入、运维设备、外来人员等过程的准入问题进行探究,并在实际场景中提出可行的解决方案。

## 1 网络安全等级保护

面对形形色色的网络攻击,防守是一个巨大的挑战,稍有不慎,网络就会被攻陷,为更好地指导网络安全工作,便提出了等级保护的思想。2016 年我国《网络安全法》完成制定,将“信息安全”更改为“网络安全”,便有了网络安全等级保护的概念,它旨在对人、信息、系统、产品、事件等进行分类分级保护、监管、处理和响应[10]。随着新型信息技术的发展,等保 1.0 已无法满足新应用、新技术,因此需要进行优化改进,2019 年 5 月,《信息安全技术 网络安全等级保护基本要求》(GB/T 22239-2019)[9](以下简称等保要求 22239)正式公布,标志着等保 2.0 时代正式到来。此后,又有多个标准条例被发布,如《信息安全技术 信息系统安全等级保护定级指南》(GB/T 22240-2020)[11]、《关键信息基础设施安全保护条例》等。

等保要求 22239 是在《信息安全技术 信息系统安全等级保护基本要求》(GB/T 22239-2008)的基础上进行修订的,顺应信息时代发展的趋势,将等级保护对象进行扩展,除通用信息系统外,还增加了云计算、移动互联、物联网、工业控制系统,对原有的安全要求分为安全通用要求和安全扩展要求两

大部分，从技术和管理两个维度指导网络安全等级保护工作的开展[12]。本文探究的是核电厂网络安全准入管理，因此结合标准中的第三级管理要求部分进行准入方案研究。标准中通用的管理要求主要内容包括安全管理制度、安全管理机构、安全管理人员、安全建设管理以及安全运维管理，分别针对管理制度体系、管理组织架构、人员管理模式、安全建设过程及安全运维过程提出了对应的安全控制要求，这些都是在网络安全准入方案建设中需要考虑的因素，表 1 列举了在进行准入管理体系建设时，对上述每一部分主要借鉴的安全控制点。

表 1　安全通用管理要求借鉴的安全控制点

| 安全控制项 | 安全控制点 |
| --- | --- |
| 安全管理制度 | 安全策略、管理制度、制定和发布、评审和修订 |
| 安全管理机构 | 岗位设置、授权和审批、沟通和合作、审核和检查 |
| 安全管理人员 | 安全意识教育和培训、外部人员访问管理 |
| 安全建设管理 | 产品采购和使用、测试验收、系统交付、服务供应商选择 |
| 安全运维管理 | 环境管理、介质管理、设备维护管理、网络和系统安全管理、恶意代码防范管理、外包运维管理 |

## 2 H 核电厂网络安全准入实践

核电厂网络安全是核电厂一直在践行的关键工作，类型多样的核电设备、软件产品以及复杂的外来人员等都是安全风险的来源，为提高安全防护力度，需要结合厂内现实情况进行准入管理建设，制定相关要求，来约束和监管要投入使用的设施和访问人员。为此，针对 H 核电厂网络安全准入问题，依照网络安全等级保护要求中第三级安全管理要求的相关原则，在 H 核电厂中制定相应的准入管理方案，用来把控设备、软件、人员等的质量问题，保证准入过程的安全性。该方案的制定和发布、评审和修订均由企业网信办来负责。经实际调研后，对 H 核电厂准入管理体系进行了安全合规的设计，如图 1 所示，体系依据并遵从国家有关网络安全法律法规、政策标准，在安全管理原则的指导下由具体的机构和人员进行实施，对核电厂的网络安全产品、外来运维设备以及外来人员进行准入管

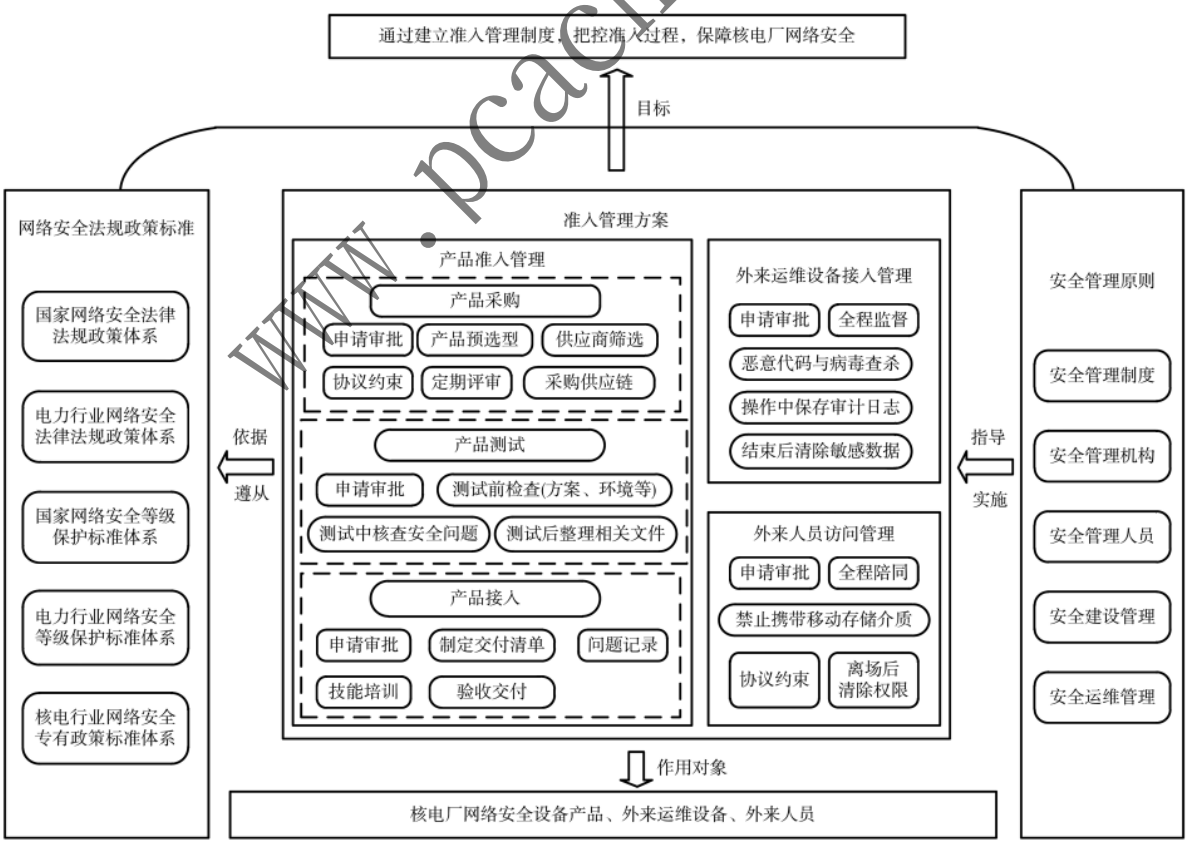


图 1　H 核电厂准入管理体系框架

理,对于这三方面分别有不同的要求,其中产品准入管理又包括了产品采购、测试和接入三个循序渐进的过程。

### 2.1 产品准入管理

对于核电产品而言,从采购到测试到正式接入,需要层层把关,面面俱到,充分考虑任何一个环节可能存在的安全风险,确保最终成果的安全度最高,是核电厂安全得到保障的关键。产品准入管理流程如图 2 所示。

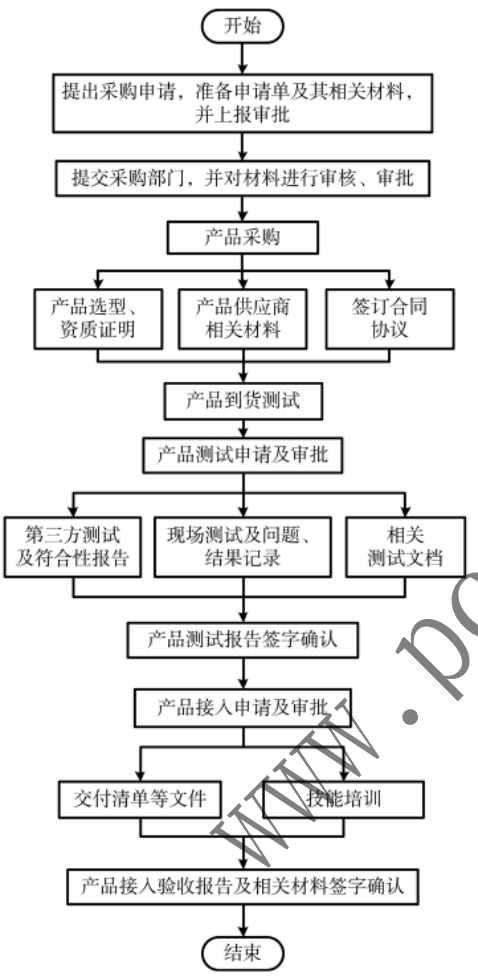


图 2 产品准入管理流程图

#### 2.1.1 产品采购

产品采购是非常重要的一个步骤,它所涉及的内容和组织也是比较复杂的。产品采购应当由需求部门提出申请,经过相应部门对申请材料进行审核批准,由采购部门负责产品采购;应在符合国家有关管理部门政策要求下进行,并且需要有资质证明来支撑产品,且产品通过了在国家认可机构中进行的安全性检测和电磁兼容性检测;在采购前对产品进行预选型,将国产化自主可控的要求排在前列,对产品供应商进行选择时,应要求提供单位证明材料,选取符合国家规定的企业,在确定供应商后,签署相关协议,如保密承诺书、安全责任书等,明确各方需要履行的网络安全义务,若供应商协议中涉及跨境转移或访问信息,则应该加强对于产品数据的保护;此外,对于产品应按时定期地进行评审监督,保证其变更的内容可控。

由于建设单位是工程质量的第一责任人,因此应当在采购的全周期内进行全面把控,建立包括承包商、各级分包商等外部相关单位在内的采购供应链网络,严格监督链上各单位及其提供的产品,强化自身的主体责任。

#### 2.1.2 产品测试

在产品测试方面,H 核电厂委托具备国家相关技术资质和安全资质的第三方测试机构进行测试。测试前应由需求部门提出申请,经相关部门批准、论证审定后,开展测试工作;测试前应该依据设计方案或合同等文件制定好测试方案,同时对于测试环境进行确认和检查,确保产品测试开始后不会对其他设备的可靠性和稳定性造成影响,而且应当有独立的测试环境;测试过程中严格按照测试方案执行,检查产品中是否具有恶意代码、后门漏洞、代码逻辑错误等安全问题,避免使用个人信息或其他敏感信息,测试中运行的数据也要保证其安全性;验证系统集成的网络安全防护功能不会影响系统的正常运行;测试完成后整理编写测试报告、缺陷报告、改进报告等相关文档,并在测试报告中明确给出是否通过的结论;对于测试发现的不符合项应标记并上报,依据不符合项的影响程度选择相应的处置方式;经由相关部门对测试结果和报告签字确认后方可完成产品测试工作。

#### 2.1.3 产品接入

产品接入工作是对产品检查的最后一步,应由需求部门提出接入申请,相关部门审批后开展;需求部门要按照合同制定详细的交付清单,对物件、文件等资产进行清点,确保资产的齐套性;在接入过程中详细记录发现的问题,比如针对仪控系统的网络安全防范管控措施是否有效,将问题交由工程实施单位进行整改,并跟踪问题解决情况;由供货商对核电厂内负责运维的人员开展技能培训,使他们可以正确安全有效地掌握设备维护方法;经讨论

确保产品合格后，拟定验收报告，并由相关部门对材料进行签字确认，产品便可以正式接入。

### 2.2 外来运维设备接入管理

原则上H核电厂不允许外来运维设备的接入，然而现实中有些特殊情况下无法遵守这个原则，那么按照国家相关政策法规和标准规定，提出一些要求来进行管理，外来运维设备接入管理流程如图3所示。

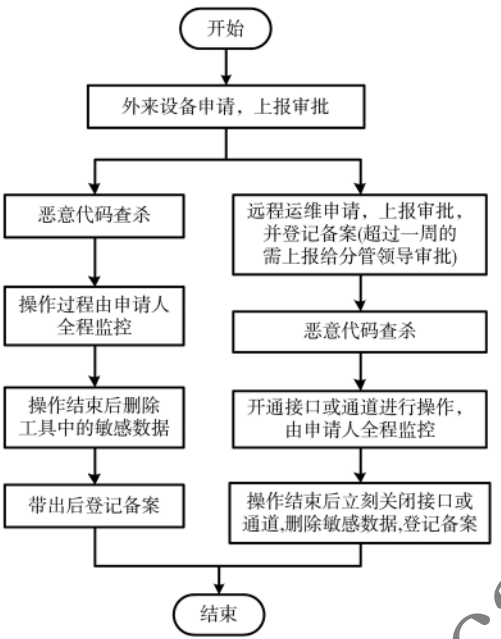


图3 外来设备运维接入管理流程图

首先由需求部门人员提出申请并在相应部门进行审批和登记备案；外来设备在接入系统之前应进行恶意代码与病毒查杀，在操作的过程中也要保留审计日志，操作结束后及时清除敏感数据；如果要进行远程运维，应将申请上报审批，若时间超过7天，则需要上报到分管领导，待签字确认后方可开启远程运维工作，在远程运维前需由厂内人员确认恶意代码查杀结果，经确认无安全威胁后，可开通接口或通道进行操作，操作结束后立刻阻断远程运维工具的接入，并删除敏感数据；外来运维设备从开始到结束的整个过程均需由内部人员全程陪同监督，确保操作环境以及操作过程的安全。

### 2.3 外来人员访问管理

H核电厂会有很多外部人员访问，比如运维人员、工程项目实施人员等，他们极有可能给核电厂带来安全风险，为此需要制定针对外来人员的准入策略。外来人员访问管理的流程如图4所示。

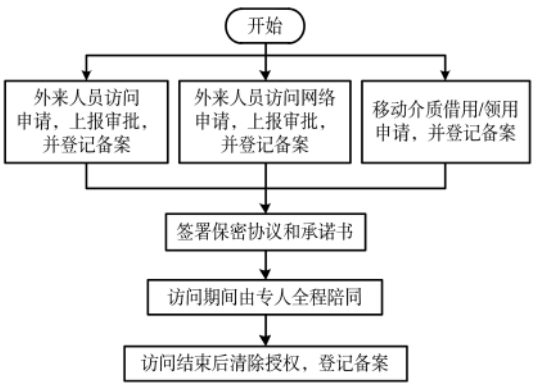


图4 外来人员访问流程图

由厂内申请人提出外部人员访问申请，详细列出访问人的身份信息及其所带物品的信息，经相关部门确认审批后方可进厂，并签署保密协议，且全程应由专人陪同；当外部人员需要接入受控网络时，应由接待人填写申请表，待分配权限账户、登记备案后才可访问；严禁携带移动存储介质入厂，如需使用，可借用内部的移动介质，并严格按照厂内移动介质借用流程进行申请和使用；原则上禁止访问厂内关键区域或系统，若因特殊原因确需访问，应由专人全程陪同，未经允许，不得在办公区域、机房等场所拍照；当外部人员离厂后，需及时清除其所有的权限。

## 3 实施效果评价

建立网络安全准入管理机制，有利于核电厂的安全稳定有序运行，对内对外都是一种保护。经对H核电厂进行产品准入、外来运维设备接入以及外来人员访问三个角度的准入管理体系建设，首先优化了产品在采购、测试和接入时的内外部工作流程，确保供应商、产品的选择符合国家规定和要求，确保产品测试时的安全风险尽可能降至最低，确保产品接入时进行细致的核查；其次完善了外来运维设备在接入内部设备或网络时的管理要求，保证在确需使用现场或远程外来运维设备的情况下，能够严格按照对应的要求进行操作；最后加强了对于外来人员访问的约束和限制，在人员构成复杂的情况下，采取全方位的监督和管理措施。在准入管理体系的实施中，提升了人员在各方面的安全意识，有利于培养严谨的工作习惯，从而避免大事故的发生。

## 4 结论

核电厂网络安全对于国家、社会、个人有着重要的影响，其安全问题不容小觑，需要全方位地进

行保护。本文对于核电厂网络安全设备、人员、软件等的准入管理进行探究,结合网络安全等级保护标准,在H核电厂中进行准入管理体系建设,从产品准入、外来运维设备接入以及外来人员访问三个角度,介绍了准许设备投入使用和人员进场的规定,使该电厂的管理体系更加健全,对其供应链安全以及生产运行具有重要意义。当前针对核电方面的法律法规、标准、制度等方面的文件正逐步完善,相信未来会形成一个成熟完整的管理体系,为核电网络安全保驾护航。

参考文献

[1] 闫怀超,陈政熙.核电行业工控网络安全整体解决方案研究[J].核安全,2020,19(3):53-58.

[2] 郭强.核电项目设备采购模式和采购风险的防控分析[J].科技视界,2017(8):269-270.

[3] 胡伟.核电项目设备采购和监造管理模式分析[J].科学技术创新,2019(9):194-195.

[4] 杨占杰,李京帅,艾九斤.核电DCS设备测试过程的监造实践[J].设备监理,2021(2):8-11.

[5] 陈纪煌,尹欣霞.核电厂运行人员防人因失误管理[J].产业与科技论坛,2020,19(12):230-231.

[6] 曾丝竹,赵友有.核电站仪控系统网络安全标准研究分析[J].仪器仪表用户,2021,28(12):71-77.

[7] DAVID T.When safety is relative:ecological modernisation theory and the nuclear safety regulatory regimes of France,the United Kingdom and United States[J].Energy Research & Social Science,2022,86.

[8] 王逊,孙海涛,史强,等.我国核安全国家标准体系构建与实施分析[J].中国标准化,2022(5):100-104.

[9] GB/T 22239-2019.信息安全技术 网络安全等级保护基本要求[S].2019.

[10] 吴蒙.网络安全管理与网络安全等级保护制度研究[J].网络安全技术与应用,2022(6):164-166.

[11] GB/T 22240-2020.信息安全技术 信息系统安全等级保护定级指南[S].2020.

[12] 马力,祝国邦,陆磊.《网络安全等级保护基本要求》(GB/T 22239-2019)标准解读[J].信息网络安全,2019(2):77-84.

(收稿日期:2022-11-28)

作者简介:

李实(1985-),男,本科,高级工程师,主要研究方向:工控系统网络安全。

王绍杰(1983-),男,硕士,高级工程师,主要研究方向:工控系统信息安全。

万佳蓉(1996-),女,硕士,工程师,主要研究方向:工控系统信息安全。

# 版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部