国网电力数据资产安全管理体系构建研究

张永瑜

（国网重庆电动汽车服务有限公司　重庆江北　400020）

摘要：为提高数据资产管理的自动化和智能化水平，国网电力需构建集资产管理、安全监控、应急响应等功能于一体的信息系统安全管理技术平台。平台需统一网络架构设计，采用模块化方式集成各系统。资产管理系统实现资产全生命周期控制；安全监测系统通过高速流量分析、日志关联分析等实现对已知和零日威胁的识别；数据防泄密平台提供加密、权限控制、水印等安全技术能力；应急响应平台可以快速展开漏洞修补、病毒清除等应急措施。平台还需提供安全开发、安全运维的工具，辅助开发运维人员提高效率。此外，需建立与其他管理系统的数据交互接口，实现信息共享。平台建设需采用云计算、大数据、人工智能等前沿技术，通过软硬件融合提升管理智能化和自动化水平。平台的建成使用将有效提升国网电力数据资产管理的信息化程度，增强安全防护和控制能力。

关键词：国网电力；数据资产；安全管理；体系构建

1. 国网电力数据资产安全管理体系构建

1.1 总体目标

国网电力数据资产安全管理的总体目标是构建系统、科学、高效的管理体系，全面提高数据资产安全保障能力，确保电力系统安全稳定运行。具体目标包括：1)识别电力系统中的所有关键数据资产，建立数据资产目录，实施分类分级管理；2)评估电力数据资产的安全风险，制定针对性的安全防护策略与技术方案； 3)加强电力数据资产的全生命周期安全管理，建立数据采集、传输、存储、使用、销毁的安全机制；4)构建实时监测预警平台，及时发现数据资产安全风险隐患；5)完善数据资产安全管理制度，强化安全意识培训，营造良好的安全文化氛围。6)建立良好的安全绩效考核体系，持续推动数据资产安全管理水平提升。

1.2 管理原则

国网电力数据资产安全管理应遵循以下基本原则：1)系统性原则。要构建系统完整的管理体系，涵盖数据资产的全生命周期，形成闭环管理。2)科学性原则。管理体系和技术方案必须具有科学性，进行充分论证，并与国家相关标准规范保持一致。3)适用性原则。管理体系要针对电网企业的实际情况设计，关闭体系与业务融合，提高适用性。4)经济性原则。在保证安全的前提下，实现管理的经济性，降低管理成本。5)前瞻性原则。积极采用前沿的安全管理理论与技术，不断提高管理水平，预见和防范安全风险。6)连续性原则。实施全员培训，形成学习型组织，持续改进数据资产管理，不断提升安全保障能力。7)责任性原则。明确数据资产管理的责任主体，实行责任制考核，依法追究相关责任。

1.3 管理流程

国网电力数据资产安全管理体系的管理流程，应该建立起规范科学的全生命周期管理机制。包括对数据资产进行全面识别登记，评估其重要性；对重要数据资产进行风险评估，明确安全防护要求；根据要求制定安全策略和技术方案；落实组织实施，采取物理隔离、访问控制、加密传输等防护措施；建立安全监测预警机制，发现隐患及时响应；开展定期的安全审计与考核，不断改进完善；形成数据资产的采集、存储、使用、共享、销毁的全过程闭环安全管理。管理流程的设计要贯穿数据资产的整个生命周期，做到管理全面系统、措施到位有效。

2. 关键技术研究

2.1 电力数据资产识别与分类

电力数据资产的识别与分类是资产管理的基础。要充分了解电网的业务系统和数据流程，采用定性与定量相结合的方法，全面识别电网涉及的各类数据资产。重点关注包含系统配置、运维参数、运营数据、用户信息等在内的核心数据资产，这些数据对系统安全稳定运行至关重要。接着，依据国家标准和电力行业标准，从保密性、完整性、可用性等方面评估数据资产的重要性。最后，将数据资产进行分类，重要级别高的资产需要采取更高安全防护等级，级别低的资产可以采取较低安全要求。分类结果应建立数据资产目录，实施分级管理，定期审查更新。分类管理要与电网企业的数据安全战略相匹配，区别对待资产的重要程度，制定针对性安全方案。通过科学合理的识别与分类，可以提高数据资产管理的有效性和经济性。

2.2 电力数据资产风险评估

电力数据资产风险评估是指针对重要数据资产的价值、威胁和脆弱性进行分析评估，识别风险因素，定量或定性分析风险水平。评估可以采用定性和定量相结合的方法，遵循国家和行业风险评估标准体系，确保评估全面、准确。定性评估重点识别威胁源、资产脆弱性、风险情景等，判断潜在风险；定量评估通过模型计算资产损失可能性与后果严重程度，得出风险值。评估过程中，要充分考虑数据资产自身因素、使用环境因素以及自然因素，明确风险形成的原因，区分数据资产面临的内部风险和外部风险。风险评估结果可以为制定防护策略提供依据。此外，安全风险具有变化性，所以要建立风险监测预警机制，定期开展评估，及时发现新的风险因素，保持评估的动态性。

2.3 电力数据资产安全防护

电力数据资产安全防护的目标是保证资产的机密性、完整性和可用性。可以从管理和技术两方面进行防护：管理防护包括制定数据安全管理制度，对数据资产进行分类管理和访问控制，建立资产变更管理流程，采取数据备份和容灾措施，开展安全培训和宣传等。技术

防护包括建设防火墙、入侵检测等网络安全防护体系，采用数据加密、数字签名等加强传输安全，使用虚拟化、容器化隔离技术进行多租户资源隔离，建立漏洞扫描、Web 应用防火墙等多层次的应用安全防护，使用白名单、黑名单等方法控制程序运行，部署安全审计和风险监控平台等。此外，要建立网络与信息系统备份恢复能力，制定灾难恢复预案和演练方案，加强物理安全防护。安全防护需要涵盖数据资产全生命周期，做到防患于未然、综合防护。

2.4 电力数据资产监测预警

电力数据资产的监测预警主要通过信息系统安全监测平台来实现。该平台的构成包括网络流量监控、主机安全监测、数据库审计、日志分析等子系统。网络流量监控通过在关键节点部署探针，对流经网络的所有流量进行全面采集，通过特征库识别已知的网络攻击行为；主机安全监测在重要服务器等终端部署主机探针，可以监测主机进程行为、文件完整性等，发现主机被入侵的迹象；数据库审计可以记录数据库操作日志，检查敏感数据访问；日志分析可以从大量日志中提取安全相关信息。监测预警系统通过多源安全数据的关联分析，采用人工智能算法，可以实现对未知威胁的识别。当监测到数据资产面临风险时，可以根据事件严重级别发送不同级别的警报，安全管理人员可以及时响应。针对预警事件，需要进行事件验证、风险分析，判断事件对资产安全的影响，并快速作出隔离、拦截、修补等应对措施以消除隐患。同时，需要对事件原因进行根源分析，排查监测预警系统自身问题，优化监测策略，增强对新型攻击的识别能力。通过动态的监测与预警，可以快速发现数据资产安全风险，提高应急响应能力。这是数据资产安全管理体系的重要组成部分，需要与防护体系深度融合，建立“防御—监测—响应”的闭环机制。

3. 管理体系实施保障措施

3.1 标准规范建设

标准规范的建设是做好数据资产安全管理的基础保障。国网电力系统应结合行业实际制定数据资产管理和信息安全相关标准规范，形成系统完整的标准体系。首先，要建立数据资产管理基本制度规范，明确数据资产的界定、分类原则、风险评估模型、安全防护等级保护要求等。其次，要制定网络与信息系统的级别保护与等保基本要求，以及数据中心、应用系统的具体安全技术规范，保障各系统的安全设计。再次，要建立信息系统全生命周期安全管理规范，包括需求、设计、开发、测试、部署、运维等阶段的具体流程和控制措施。最后，要建立安全事件应急响应机制标准规范，指导安全监测预警、事件报告、应急处置、演练等工作的开展。标准规范体系的建设要与国家标准保持一致，同时结合电力行业实际需要进行补充和扩展。并要通过技术平台建设和系统集成实现标准规范的有效执行。还需要建立标准动态更新机制，定期对标国内外先进标准，推进标准规范不断完善。只有建立科学合理、结构完备的标准规范体系，才能为数据资产安全管理提供有力保障。

3.2 技术平台建设

为提高数据资产管理的自动化和智能化水平，国网电力需构建集资产管理、安全监控、应急响应等功能于一体的信息系统安全管理技术平台。平台需统一网络架构设计，采用模块化方式集成各系统。资产管理系统实现资产全生命周期控制；安全监测系统通过高速流量分析、日志关联分析等实现对已知和零日威胁的识别；数据防泄密平台提供加密、权限控制、水印等安全技术能力；应急响应平台可以快速展开漏洞修补、病毒清除等应急措施。平台还需提供安全开发、安全运维的工具，辅助开发运维人员提高效率。此外，需建立与其他管理系统的数据交互接口，实现信息共享。平台建设需采用云计算、大数据、人工智能等前沿技术，通过软硬件融合提升管理智能化和自动化水平。平台的建成使用将有效提升国网电力数据资产管理的信息化程度，增强安全防护和控制能力。

3.3 人员培训与考核

人员培训与考核是数据资产安全管理的重要保障。国网电力需要建立系统完善的培训体系，通过安全教育增强全员安全意识，并考核落实培训效果。首先，要制定数据资产安全培训规划，对不同岗位人员开展岗前培训和在岗培训，内容包括安全制度、职责要求、操作规程、技术防护等。培训采用理论学习、案例分析、技能操作等多种方式，形成真学真做。其次，要定期开展安全技能竞赛、知识竞赛等形式的培训，启发员工主动学习，并考核其掌握情况。再次，要选择或开发适用的网络培训课程，建立线上学习平台，实现培训全覆盖。最后，要将安全培训与考核结果与员工职务晋升和绩效评价挂钩，强化培训效果。通过持续推进安全培训，广泛传播安全理念，将使各级员工树立数据资产安全意识。考核可以验证培训成效，也为不断改进培训工作提供反馈。这对于提升数据资产管理水平，建立高素质的安全管理和技术团队至关重要。

4. 结束语

综上所述，电力企业应立足国家网络安全战略和电力系统安全发展需要，构建与电力业务深度融合的数据资产安全管理体系，实现对数据资产的全生命周期管理和动态监测预警。同时，要加强组织领导，健全标准规范体系，建设统一的技术支撑平台，实施安全培训与考核，形成长效管理机制。电力企业还需积极开展管理创新，不断提高数据资产管理水平，切实保障电力数据资源安全。

参考文献：

[1]樊海军.电力信息系统安全风险评估方法研究[J].电力系统保护与控制,2019,47(17):73-79.

[2]李正茂,李永安,王小磊.电力企业信息系统安全管理模式优化研究[J].电力系统保护与控制,2020,48(11):191-197.

[3]饶敏.电力大数据安全保障体系架构设计[J].电力信息与通信技术,2021,19(11):6-12.DOI：10.13245/j. hust. xxxxxx

张永瑜(1987.4-) 男 汉族 重庆人 本科 工程师