# 电力企业全方位网络安全防护的管理创新与实践

## Management Innovation and Practice of All-round Network Security Protection in Electric Power Enterprises

李悦

Yue Li

国网石家庄鹿泉区供电公司　中国·河北 石家庄 050000

State Grid Shijiazhuang Luquan District Power Supply Company, Shijiazhuang, Hebei, 050000, China

**摘　要：**阐述中国电力企业为有效应对当前网络安全形势，电力企业通过开展管理创新、制度变革、工具革新三方面的创新，践行以网络安全为主题的全方位实时网络安全监视运行值班工作体系。有效协助解决电力行业各企业、各单位的网络安全工作共性问题，具有较强的导向性和可操作性。

**Abstract:** To respond effectively to the current cyber security situation, China's power companies have been innovating in three areas: management innovation, institutional change and tool innovation, practice to network security as the theme of all-round real-time network security monitoring operation duty system. Effective assistance to solve the power industry enterprises, units of network security work common problems, with strong guidance and maneuverability.

**关键词：**电力企业网络安全管理；网络安全防护；电网安全风险

**Keywords:** power enterprise network security management; network security protection; power grid security risk

**DOI:** 10.12346/peti.v5i1.7528

## 1 引言

近些年，国际和电力行业层面的网络安全形势正在发生深刻变革。中国电力企业为有效应对当前网络安全形势，须深入开展管理创新、制度变革、工具革新，践行全方位创新理念，将网络安全公司发展战略，实现全方位网络安全监控，在重大事件保电、大型攻防演练重大活动中发挥重要作用。依托电力企业专用调度运行体系，实现网络安全事件的实时预警和高效处置。论文主要阐述电力企业在网络安全管理的管理创新提升和实践沉淀，基于多年电力网络安全保障与攻防对抗创新实践，总结出电力企业相适应的全方位安全防护体系，支撑中国电力企业网络安全防护研究工作。

## 2 发展背景

党的十八大以来，习近平总书记曾在不同场合多次对网络安全问题发表重要论述，为新的国际形势下实现网络强国的目标提供了科学指导和基本遵循。国家电网公司明确将网络信息安全列入四大安全（大电网安全、设备安全、人身安全、网络信息安全）与四大风险（电网安全风险、经营管控风险、金融业务风险、网络安全风险）之中。网络安全防护需遵循“木桶理论”[1]，即每一个环节、每一个可能出现的漏洞都有可能成为系统的安全薄弱点，特别是现在大数据应用日渐普及，数据资源共享频繁，使得网络安全防护“点多面广”，难度极大，且做好全方位网络安全防护无现成经验可参考。如何创新管理机制，高效提升网络安全预警机制和网络安全事件处置能力，是网络安全防护工作亟待解决的问题。

电力作为关系国计民生的重要基础能源行业，承载着为中国经济发展提供基本能源保障的使命，在国家经济发展和民生建设等方面都起着关键性作用。同时，电力行业也具有分布区域广泛、设备结构复杂等特点，导致电力企业面临网络安全风险点多、防御面广、防御难度大等问题。当前电力企业网络安全形势极其严峻，具体体现在以下三个方面：

【作者简介】李悦（1989-），男，中国河北廊坊人，本科，工程师，从事电力调度自动化及其网络安全防护研究。

### 2.1 网络攻击的破坏性高、持续性强

电力企业对运维系统的实时性、可靠性、精确性有很高要求。自 2017 年以来，中国电力企业遭受来自互联网的攻击次数连年递增，防御压力不断增大，急需在管理上予以高度重视，在企业主观管理意志中高度体现。

### 2.2 网络防护边界泛在性特点日趋显著

随着技术发展，中国智能电网和泛在电力物联网的建设，电力企业网络安全边界快速扩大，网络构成日益复杂，网络安全防护难度加大，迫切需要从顶层设计与管理层面予以重视、指导和规范。

### 2.3 数据安全的重要性及防护难度日益提升

电力业务大数据的推广和应用不断深化，数据价值不断提升，数据安全压力逐渐增大。云计算、人工智能等新兴技术的引进，带来了未知安全隐患，数据安全面临新的挑战。2016 年 4 月 19 日，习近平总书记在网络安全和信息化工作座谈会上作出主要指示“攻防力量要对等，要以技术对技术，以技术管技术”，网络安全管理不能拘于表面功课，管理创新与科技创新需齐头并进。

## 3 内涵和主要做法

综上所述，电力企业需从管理思想创新、管理制度创新、管理工具创新三方面的开展企业网络安全提升工作，并在全天候网络安全分析工作中践行创新理念，日益形成并充分发挥在公司网络安全防控体系的核心作用。

### 3.1 创新战略指导，助推新时代网络安全工作变革

从管理创新角度入手，树立网络安全发展新方向，梳理工作思路，引导网络安全工作成功转型。

#### 3.1.1 积极谋划战略革新，突出网络安全重点地位

战略引导方向，方向决定结果，涉及安全工作都需要企业发展战略作为指引。国有电力企业已发布了新时代发展战略纲要，“着力保障大电网安全运行”和“着力保障网络安全”等内容 [2]，凸显了电力企业对网络安全的高度重视。

#### 3.1.2 努力实现“世界一流”战略目标

在电力企业逐步部署泛在电力物联网建设工作的同时，各环节应高度重视，企业负责同志应亲自协调，全员动员，构建智能联动的全方位安全防护体系架构。以所属职责为起点，以泛在电力物联网实时安全监控为核心，构建智能联动的网络安全防护体系。

#### 3.1.3 积极转型变革，确保网络安全高效落地

推动网络安全工作模式转变。在日常安全运维的基础上增加恶意代码防护、漏洞监视、红蓝队对抗演练等风险自控项目，在企业内部实现 7×24 小时全方位实时网络安全监视，负责全天候网络安全保障。

### 3.2 完善网络安全体系建设，提升精益化管控水平

根据《电力二次系统安全防护总体方案》中规定的“安全分区、网络专用、横向隔离、纵向认证”网络安全防护总体原则，以管理创新为抓手，保障网络安全监控全环节规范、高效、有序运行。

#### 3.2.1 开展企业网络安全监控体系建设

确立各公司、部门、专业、岗位安全责任，编制岗位安全责任清单，公布各机构安全责任及履职要求。严密开展运维规范的执行与监督，重点确保主用网络安全设备可控、可用、在运，同步建立 7×24 小时全方位实时网络安全监视运行值班、安全监视体系以及系统全面的文档管理制度。

①建立 7×24 小时全方位网络安全监视运行值班体系。

重点强化网络安全监视，建立 7×24 小时全方位实时网络安全监视运行值班体系，进行全天候网络安全监控。完善《网络安全监视运行值班工作制度》等管理规范的编制，针对责任划分、值班管理、应急管理等方面明确各环节工作规范，避免出现监控缺失。同时，提高运行值班人员的网络安全防护意识，强化业务培训。保证运行值班人员具备合格的安全意识、业务知识和应急处置能力。加强运行值班人员管理，建立一支素质高、努力强的网络安全运维管理队伍，保证在日常的运行维护过程中严格避免来自内部的违规外联、木马、越权、误用等事件发生，全面提升网络安全防护水平。

②完善管理规范文档编制。

首先完善全环节工作标准、操作规范等文档的编制，重点关注值班人员素质提升。其次建立网络安全事件的及时汇报与应急处置制度，修订各环节网络安全防护方案、应急预案、应急处置指导书，同时编制网络安全演练脚本，定期进行演练实训，重点强化应对遭受 DDOS 攻击、大面积监控缺失、大面积病毒暴发等场景的应急处置演练。

③强化全环节保密工作。

电力企业需重点关注保密安全工作，建立全环节保密监视体系，实现纵向上下级贯通、横向各部门协同的保密监视机制，并纳入公司网络安全管理体系之中，强化网络安全本质安全，推动电力企业保密工作科学管控全面提升。

#### 3.2.2 以管理创新、制度创新为支撑，开展网络安全专业管理

电力企业应编制网络安全监控指导性、规范性、权威性文件并发布施行，明确五大类监控要点 [3]，奠定理论基础，指明发展方向，指导行业内各单位建设各自网络安全防护体系。

#### 3.2.3 建设全方位风险防控体系，强化安全漏洞精准管控

建设包含风险预警、风险分析、闭环管控和风险处置于一身的全方位网络安全风险防控体系。超前规划，高效落实，使网络安全风险防控体系涵盖生产活动、设备运行、业务外包、信息安全等各个环节的风险防控，为企业整体网络安全防护体系提供重要支撑。安全漏洞作为网络安全的重要威胁，极易作为攻击者入侵的跳板，也是病毒和木马的常驻地 [4]。同时，安全漏洞也是网络攻防对抗中重要战略资源。

实现漏洞全环节精准管控，是全方位风险防控体系建设中的重要一环。

### 3.3 高新技术应用，助力网络安全智能可视化

网络安全领域高新技术的开发应用，能够高效助力全方位网络安全防控工作，强化对数据云、电力专网、网络边界及终端设备的全面态势感知，同时为防护人员开展网络攻防对抗提供高效支撑。各层级的全面态势感知是网络安全防护的基本前提，以多态的先进安全数据接口为基础，通过高效精准的预处理与边缘计算能力，保障数据高质量进行标准化采集与传输，同时支持个性化定制策略[5]。同时通过数据挖掘与大数据分析等技术手段，对多源数据库进行数据处理和关联分析，通过数据预处理与可视化技术进行数据分析、展示，梳理规律、暴露问题，确保实现安全风险提前看、安全管理随时看、安全威胁深入看、安全隐患容易看。准确识别网络边界、设备主机、网络应用、数据安全等各环节中可能出现的威胁，及时发现并处置安全隐患，力保网络安全风险可控、能控、在控。

以网络安全监控平台为基础支撑，辅以网络安全领域高新技术应用，网络安全智能可视化的设计思路应运而生。网络安全智能可视化向下延伸至感知层与网络层的数据接入，向上对应平台层、应用层的网络安全监控，同时适配泛在电力物联网、移动终端、大数据云与全业务数据中心，其设计思路分为全方位感知、集中可视化、场景智能展示三个方面。

#### 3.3.1 全环节安全态势全方位感知

实现对数据云、电力专网、网络边界、设备终端的安全数据采集和处理能力。云：包括云WAF、云漏扫、云主机安全、综合审计、安全服务平台等；网：包括电力专用支撑网、传输网、业务网，完善覆盖生产控制大区和管理信息大区的防护与安全监控；边：深化对横向边界、纵向边界、第三方边界的态势感知；端：包括各类主机、终端设备等[6]。

#### 3.3.2 网络安全告警信息集中可视化

主要包括对各类设备告警信息集中收集、大数据分析、攻击溯源三方面。集中收集：将各类告警信息与多源威胁情报数据集中收集并关联分析；大数据分析：借助全流量数据采集和大数据分析技术，实现针对高级网络攻击的预警；攻击溯源：提高针对网络攻击的灵敏性、智能研判、攻击路径还原等能力，自动追踪恶意网络攻击行动并溯源。

#### 3.3.3 场景智能展示保障应急联动

梳理总结国内外各类网络攻击典型案例，根据不同场景评估自身防御体系。针对外部攻击：强化蜜罐技术深入应用，灵活运用各类动态安全与主动安全技术，做到“出手必捉”。针对内部安全漏洞：利用各类工具检测出恶意代码、用户异常行为，配合安全管控治理与内部教育培训，实现内部风险“清零”。

## 4 实际应用

在网络安全管理发展的进程中，电力企业已相继建成企业级网络安全风险防控体系，也为将来开展泛在电力物联网的全方位网络安全防护工作奠定了坚实的基础。实现网络安全“可观可控能控，处置及时有效”的工作目标[7]。以全面提升电力企业网络安全防护能力为主线，坚持优化实时监控、智能研判和应急处置三项核心职能。为电力企业网络安全防护提供了重要支撑，同时也为其他行业的网络安全防护工作的开展提供了优秀范例，产生了巨大的社会效益：一是电力企业网络安全防护体系的建设是国家对行业网络安全工作的指示、是网络安全法等各项政策要求的高效落地，是彰显电力企业网络安全防护工作优秀成果的重要展示。二是奠定了电力企业网络安全防护工作的坚实基础，补齐了企业网络安全工作方面的短板，在管理层面和技术层面都极大程度提升了网络安全管控水平，高效抵御外部网络攻击，保障信息安全。三是实现了网络安全自动化防护，节省人力成本的同时，提升网络安全防护响应速度和防御水平，带来了巨大的间接经济效益。四是为电力行业在网络安全前沿科技领域培养了一批高端信息安全人才，为行业今后网络安全技术的发展奠定了良好的基础。

综上所述，电力企业通过开展管理创新、制度变革、工具革新三方面的创新，践行以网络安全为主题的全方位实时网络安全监视运行值班工作体系，以网络安全管理为核心理念，提升外部网络攻击及内部安全威胁的处置准确度和响应速度，建立行业内部各企业之间“协同联动”的企业级信息安全联防机制。有关成果能够协助解决电力行业各企业、各单位的网络安全工作共性问题，具有较强的导向性和可操作性。

## 参考文献

[1] 焦伟.电力调度自动化网络安全防护系统的研究与实现[D].河北:华北电力大学,2014.

[2] 杨至元,张仕鹏,孙浩.电力系统信息物理网络安全综合分析与风险研究[J].南方能源建设,2020,7(3):6-22.

[3] 陈雄坤,李暖群,陈劲跃.基于大数据建设下电力调度自动化的安全与实现[J].自动化应用,2017(2):82-84.

[4] 高焕新,高永前.关键信息基础设施安全保护运营措施分析与建议[J].信息技术与网络安全,2018,37(5):37-40.

[5] 金国.关于电力调度自动化网络安全与实现技术[J].装备维修技术,2020(2):57.

[6] 唐琳,王瀚伦,王耀祖.电力调度自动化系统网络安全隐患及防治措施[J].信息系统工程,2016(8):70.

[7] 侯红梅.浅谈电力调度自动化运行中的网络安全问题及解决对策[J].中国高新技术企业,2017(1):141-142.