关键信息基础设施安全保障浅论

周德宇
重庆若可网络安全测评技术有限公司，重庆 400060
DOI: 10.61369/TACS.2025010042

摘　　要： 论文在国家对关键信息基础设施系统重点安全防护提出最新要求的背景下，以网络安全等级保护2.0国家标准为依据，提出以数据安全和人员管理作为网络系统安全防护的重要抓手、以系统安全运行防护为基础手段，态势感知为基本支撑，攻防演练为核心，构建下一代网络与信息安全保障体系的构想。即以协同防御为特征的安全防护综合体系[10][11]。

关 键 词： 关键信息基础设施；网络安全等及保护；网络安全防御体系

A Brief Discussion on the Security Guarantee of Key Information Infrastructure

Zhou Deyu
Chongqing Ruoke Network Security Evaluation Technology Co., Ltd, Chongqing 400060

Abstract: Against the backdrop of the latest national requirements for the key security protection of critical information infrastructure systems, this paper proposes the concept of constructing a next-generation network and information security assurance system based on the National Standard for Network Security Level Protection 2.0, which emphasizes data security and personnel management as important measures for network system security protection, system security operation protection as the basic means, situational awareness as the basic support, and attack and defense exercises as the core. A comprehensive security protection system characterized by collaborative defense.

Keywords: key information infrastructure; network security and protection; network security defense system

一、关键基础设施与等保2.0的关系

自2008年我国正式推行网络安全等级保护体系到现在，已取得了不错的成果。该体系已成为中国政府及各个行业等关键基础设施安全的重要指导依据、参考以及建设依据，对我国网络和信息安全水平的迅速提升与完善做出了不可替代的重要贡献[1]。

等保2.0由定级指南、基本要求、设计要求和测评要求组成。在技术和管理两大方面对网络与信息系统安全保障进行了全面描述与规范，包括通用要求与安全扩展要求两部分，在通用要求中，技术要求部分包括物理和环境安全、设备和计算安全、应用和数据安全，管理要求部分包括安全策略和管理制度、安全管理机构和人员、安全建设管理和安全运维管理，等保2.0构建了一套以技术为支撑、管理为基础、监测预警为核心、协调应对为目标的完整网络安全防御体系框架和建设指南[3]。

关键信息基础设施保护的关键目标是确保业务的全面安全，而网络安全等级保护制度则旨在识别和应对网络及信息系统面临的安全威胁以及突出问题。这一等级保护制度构成了关键信息基础设施保护的基本框架，因其将关键信息基础设施作为核心重点，二者密切相关、互为补充。对于重点领域、重点行业的运营者而言，应当对网络和信息系统进行合理的边界划分，确定定级对象，开展等级保护工作，针对关键的业务系统，确定支撑其稳定运行的关键信息基础设施，并进行重点防护[2]。

二、以数据驱动和人员管理为重要抓手

多年来，我们不断参与多种攻防演习、紧急事件应对和追踪分析活动，积累了丰富的实战经验。在总结反思的过程中，我们逐渐认识到构建全链路安全数据资产、打造复合型安全专家团队、智能化安全运营平台、标准化管理流程将是未来安全发展的主流方向。通过对全链路安全数据资产的分析，实现从监测预警到响应处置的闭环管理，是当前复杂攻击环境下的理想应对策略，形成了PDCA循环的安全运营机制。[7]安全运营机制与复合型安全专家团队的构建又是相辅相成的体系化工程，安全运营机制提供标准化的事件响应框架，而复合型团队则赋予机制灵活应对0day攻击、APT攻击等复杂场景的能力。再结合智能化安全运营平台，平台支撑全流程威胁检测与响应，实现安全运维的自动化增效，从而实现更加及时的监控预警。

通过对安全发展历程的梳理与反思，我们认识到安全防御体系正经历着从传统架构安全向智能化主动防御的演进。这一发展路径反映了安全防御从静态防护到动态响应、从单点布防到体系化作战的转变趋势，体现了对新型威胁环境的适应性进化。未来安全体系建设将更加注重实战效果验证与动态能力提升，通过持

作者简介：周德宇（1995—），男，重庆，CISP，学士，网络安全技术，重庆市沙坪坝区大学城，Email：945973215@qq.com。

续优化的人机协同机制应对日益复杂的网络安全挑战[9]。

三、以系统运行为基础手段

技术支持在等级保护2.0中起着至关重要的作用，全面涵盖了关键信息基础设施安全框架和能力，是其基础的核心。等级保护2.0的技术框架在1.0版本基础上进行了延续和发展，坚持了对网络与信息系统资产的安全保障核心理念。该体系围绕基础设施和业务应用展开系统性设计，与网络安全防护原则形成有机统一。在标准实施过程中，采用分级保护机制作为核心思路，通过构建从基础级到增强级的完整防护体系，重点保障通信网络传输安全、区域边界防护安全以及计算环境运行安全三大核心领域。这表达了对网络安全等级保护制度十年来成果的总结与传承，并强调未来十年仍将坚持资产保护的基本思想[4][5]。

基于有效的资产保护方法，随着网络和信息技术的快速发展，为应对新兴领域的安全挑战，针对云服务架构的安全隔离与数据保护准则、物联网终端设备的接入认证与流量监测规范、移动应用生态的隐私合规要求，以及工业控制网络的协议安全与边界防护标准，构建了覆盖新型技术场景的全方位安全防护体系。这明确指出基础设施和业务应用的演进始终以网络与信息安全体系为基础。

四、以态势感知为基础支持

网络安全等级保护制度始终将监测预警作为安全技术体系的关键环节。经过近年来的实践验证，安全态势感知技术已成为实现高效监测预警的最优解决方案。习近平总书记在网络安全和信息化工作座谈会上提出的全天候全方位态势感知重要指示，为监测预警工作提供了根本遵循。目前已基于实战经验建立了标准化态势感知平台，该平台在十九大等重大活动安保工作中发挥了关键作用[6][13]。

现代态势感知平台已突破传统监测工具的局限，发展为集安全运营与指挥调度于一体的综合系统。其核心功能涵盖了多源数据采集、威胁情报整合、大数据分析、实时监测预警、精准研判分析、应急指挥调度、协同响应处置及攻击溯源追踪，构建了完整的安全运营闭环。这种设计理念使得态势感知平台显著区别于传统 SOC 和新一代 NGSOC 系统，更强调实战化、闭环化的安全运营支撑能力[8]。

为确保实战效能，态势感知平台必须构建五大核心能力体系：一是建立全覆盖、多维度的数据采集机制；二是实现高质量威胁情报的实时获取与应用；三是融合互联网外部数据与内部系统数据进行关联分析；四是具备海量数据的高效处理能力；五是形成包含指挥调度、预警通报、应急响应在内的全流程闭环运营体系；最终还需具备完善的安全事件取证与溯源追踪能力。这些能力共同构成了态势感知平台的两大驱动引擎：通过外部威胁情报和互联网数据实现威胁预判，结合内部数据分析实现风险验证，内外协同形成完整的网络安全态势感知与运营支撑体系[12]。

五、以攻防演练为核心

安全体系的核心在于攻防对抗，其构建也是为了服务攻防策略。公安部集中力量进行了一项名为“护网”的行动，专门针对关键性的基础信息设施。在实战中，他们验证了这些系统的安全防护水平，提前识别并修补了安全上的不足，完善了信息防护措施。“护网”行动再次证实，通过模拟攻击演练和红蓝对抗实战，能够快速暴露系统漏洞并针对性强化防御，这是短期内提升安全防护能力最高效的途径。这种方法显著提前了应急响应的时间，真正做到将被动防御变为主动防护。在积累经验、磨炼团队、测试系统的同时，通过将突发事件的应急反应转化为预先的防范措施，将不利情况转化为有利条件。当前，业界普遍认为开展攻防演练和红蓝对抗是快速增强网络与信息安全防护能力的有效途径，这种实战化的安全演练模式已成为构建完善安全防护体系的关键方法[14]。

六、总结

关键基础设施保护对主动防御体系的核心数据、人员管理、态势感知、攻防演练等提出了明确的要求，形成了以数据驱动为基础，安全人员为核心，态势感知为支撑，攻防为特征的中国特色主动防御安全体系。[15]我们必须深入理解背后的安全系统建设，深入理解等保2.0和关键基础设施保护在意识形态框架的本质，只有这样，我们才能真正灵活地让等保2.0与关键基础设施保护相结合，构建一个符合未来需求的安全保障体系。

参考文献

[1] 袁胜 . 加强国家关键信息基础设施安全保障 [J]. 中国信息安全 ,2019,11(No.83):41-42.
[2] 王超 . 加强关键信息基础设施网络安全保障刻不容缓 [J]. 网络空间安全 ,2018,9(6):50-55.
[3]《关键信息基础设施安全保护条例》2021年9月1日起施行 .
[4] 魏昊 . 强化供应链安全保障工作，保护关键信息基础设施安全 [OL]. 中国网信网 ,2021年09月01日07:00.
[5] 周文 . 关键信息基础设施整体安全保障思路 [J]. 信息安全研究 ,(2019):6.
[6] 吴沈括 . 关键信息基础设施安全保护的中国方案 [J]. 中国信息安全 ,2019(7):2.(No.56):39-40.
[7] 杜霖、田慧蓉 . 加快推进我国关键信息基础设施安全保护工作 [J].2022(8).(No.24):16-17.
[8] 吴沈括 . 关键信息基础设施安全保护的中国方案 [J].2022(7).(No.21):33-34.
[9] 张彦超、丰诗朵、赵爽 . 关键信息基础设施安全保护研究 [J].2022(5).(No.25):12-13.
[10] 董贞良 . 关键信息基础设施保护三大层面 [J].2022(11).(No.22):23-24.
[11] 肖鹏 .《产业与科技论坛》[M]. 云南电网有限责任公司信息中心 .2021年第11期215-216.
[12] 高月 .《网络安全和信息化》[M]. 赛迪智库网络安全研究所2021年第4期21.
[13] 郭启全 . 关键信息基础设施安全保护的对策措施 [C].2017年中国网络安全大会 .2017.
[14] 丁丽 .《做好关键信息基础设施监测预警和应急响应》[J]. 网络传播 .2021，第9期 .
[15] 高月 .《我国关键信息基础设施安全保护现状、问题及对策》[J]. 网络安全和信息化 .2021，第004期

