马骋,白滔,马园,等. 近源攻击与违规外联协同纵深防御体系构建[J]. 陕西气象,2026(3):68-74.
文章编号:1006-4354(2026)03-0068-07

近源攻击与违规外联协同纵深防御体系构建

马 骋[1],白 滔[2],马 园[3],方 堃[4],李 浩[5]
(1. 宁夏气象信息中心,银川 750002;2. 贵州气象数据中心,贵阳 550002;
3. 陕西省气象信息中心,西安 710014;4. 榆林市气象局,陕西榆林 719099;
5. 新疆气象信息中心,乌鲁木齐 830000)

摘 要:数字化转型背景下,关键信息基础设施面临近源攻击与违规外联构成的复合威胁,传统边界防护体系在应对此类风险时存在技术单点化,管理碎片化与防御静态化等缺陷。结合气象部门网络边界复杂,终端类型多样,数据交互频繁的业务特性,提出以关键资产保护为核心的纵深防御体系。设计常态化纵深防御成熟度模型用于效能量化评估。根据宁夏气象局近两年网络安全防护工作实践检验,该体系可显著缩短安全事件平均响应时长,入网资产发现率达 90%,攻防演习失陷资产较 2024 年下降 93%,不良资产发现能力与漏洞修复效率显著提升,有效提升关键信息基础设施网络安全防护能力。

关键词:近源攻击;违规外联;纵深防御
中图分类号:TP393.08 **文献标识码**:A

随着数字化转型深入推进,关键信息基础设施日益智能化,安全边界日趋模糊,安全态势愈发复杂。传统防御体系以网络边界阻断为核心,过度依赖防火墙、入侵检测等边界防护设备,对物理层渗透、内部人员违规等风险威胁关注不足,难以应对新型安全挑战。近源攻击通过物理接近、利用暴露接口或社会工程学等手段实施渗透,具有隐蔽性强、攻击路径短等特点;违规外联体现为内部设备未经授权连接外部网络,形成隐蔽攻击通道,成为数据泄露与外部攻击的重要跳板。气象部门作为关键基础设施运营单位,业务覆盖面广,通过专线、互联网、政务云等方式对外提供数据服务,网络边界复杂,单一边界防御体系在内外网数据交换管控、出口流量监测等方面存在显著脆弱性[1]。同时,气象部门终端设备类型多样,包含嵌入式观测设备、办公终端、自助服务设备等,跨区域运维场景频繁,导致物理接口暴露、非授权接入等风险隐患显著增加。近年来,近源攻击朝着固件篡改、痕迹擦除等更隐蔽、更底层的趋势演化。伴随网络连接的复杂化,违规外联衍生出加密通信代理、多网卡跳转等新型手段,进一步提升防御难度,传统防护措施已无法有效抵御此类复合威胁。现有防御技术与方案虽能有效应对单一类型威胁,但受限于协同防控机制缺失、检测精度与响应速度难以兼顾、缺乏多源情报融合及智能研判能力不足等,难以有效抵御复合型威胁。本文针对上述问题,结合气象业务特性与多部门实践经验,开展纵深防御体系构建与关键技术优化研究。

1 国内外防御技术与理念

1.1 近源攻击与违规外联防御技术研究

国际上主流安全防护范式为纵深防御,核心内容是通过系统的设计,确保单一故障不会引发全局性严重安全后果,纵深防御覆盖网络、边界、计算环境与支撑设施等多个层面,强调技术、人员与流程的协同联动。美国国家标准与技术研究院为其防御效能评估制定了控制实施合规率、风险

收稿日期:2025-12-30
作者简介:马骋(1997—),男,回族,宁夏银川市人,硕士,助理工程师,从事网络安全与通信网络保障工作。

缓解成效、控制响应时效性等核心指标,重点突出跨场景普适性防护、全生命周期风险管控及动态风险响应[2]。近源攻击防御技术聚焦于智能检测与身份认证的深度融合。在无线入侵检测系统中应用机器学习技术与量子抗性密码方案,达成具备高准确率与高精度的防御效能[3]。基于零信任架构的多因素网络准入控制系统可大幅降低未授权访问风险[4]。区块链与多因素认证结合的去中心化身份管理方案,为近源攻击中的身份冒用防御提供新的方向[5]。国内研究更侧重于物理防护与技术拦截结合、权限管控与诱捕溯源联动,医院、港口等开放场景的防御实践为气象部门提供重要参考。医院场景常采用反锁扣网线头与终端准入全覆盖方案防范非授权接入行为[6];港口场景通过零信任准入、蜜罐部署、网段隔离的主动防御架构,阻断近源攻击的横向移动路径[7]。违规外联防御技术已形成涵盖检测、阻断、溯源的完整技术体系,虚拟补丁技术通过双向状态防火墙与深度数据包检测,配置白名单策略精准阻断终端违规外联,适配多类硬件运行环境[8]。基于机器学习的检测系统通过聚类算法与信息熵分析,自动识别多网卡接入、加密代理等新型违规外联,查全率超过 90%,阻断时延控制在 3 s 内[9],弥补传统规则匹配模式的局限性。流指纹技术实现在网络地址转化的环境下内部设备的精准识别与有效阻断。相关研究总结手机热点共享、网关设备滥用等典型违规外联场景[10],为适应行业特点制定针对性防御方案提供了重要参考。

1.2　关键信息基础设施的安全防护框架与行业实践

关键信息基础设施的安全防护已突破传统边界防御的局限性,向动态主动、智能协同、弹性可恢复的体系化范式演进,其技术框架应融合可信计算、智能态势感知、零信任架构与系统自愈等核心能力,实现从被动响应到持续对抗的转变[11]。

当前,相关行业实践呈现体系化、实战化特征。电力行业构建专属防护体系,实现从主站到作业现场的全链路管控[12];民航空管领域以监测预警为核心中枢,通过技术、管理、运营三维融合,落地安全风险的标准化、网格化管控[13]。上述实践凸显了技术与管理协同、防御建设与运营保障并重的行业共识。随着数据成为核心生产要素,数据空间安全已成为关键信息基础设施防护的纵深延伸领域。保障数据全生命周期安全与合规流通,既是支撑跨主体业务协同与创新的基础前提,也面临数据权属界定、隐私保护与利用平衡、跨境数据流动合规等多重挑战[14]。

综上,关键信息基础设施防护亟需构建常态化、多维度的纵深防御体系。尤其要针对近源攻击与违规外联交织的复合性安全威胁,强化专项协同防控与全流程闭环管控。

2　气象部门适配性防御技术

气象行业结合自身业务特点,在借鉴国内外先进技术与防御理念的基础上,形成了一系列场景化适配的防御成果,为构建一体化纵深防御体系奠定了基础。

身份认证与访问控制层面,陕西气象部门搭建统一身份认证系统,实现用户、认证、授权与审计的集中化管理,有效解决了多系统认证分散、弱口令滥用等安全隐患,从源头降低内部人员违规风险[15]。边界防护层面,宁夏气象部门构建区域边界防护、数据流量管控、终端安全防护三位一体的混合云安全体系,通过虚拟专网隔离、微隔离等技术手段防范跨云访问风险[1]。陕西气象部门搭建安全态势感知系统,可实现全省气象网络资产脆弱性研判、网络攻击实时监测与省市两级防火墙联动处置,实现业务故障告警与事件快速处置。网络监控与运维层面,通过部署数据可视化分析平台与监控系统,实现对核心服务器、网络设备、虚拟化环境及业务系统运行状态的自动化监控与可视化展示,提升异常状态发现效率与定位精度[16]。网络监控与运维层面,陕西市级气象部门部署数据可视化分析平台与监控系统,实现对核心服务器、网络设备、虚拟化环境及业务系统运行状态的自动化监控与可视化展示,提升异常状态发现效率与定位精度[17],完善了纵深防御体系中的感知层建设。

3　典型案例分析

国家级网络安全态势感知平台监测发现,某市气象部门一台服务器遭受 APT 组织利用 CVE

-2023-46604 漏洞发起定向攻击，服务器被成功植入挖矿程序。攻击者通过 HTTPS 流量伪装实现对失陷服务器两年多长期潜伏控制(图 1)。该安全事件的应急处置全程依托“国家级-省级-市级”三级联动机制完成。基于 2024—2025 年实战攻防演练与安全事件告警处置全流程记录的统计分析，自态势感知平台发布告警起，至完成初步应急处置的平均用时控制在 30 min 以内。

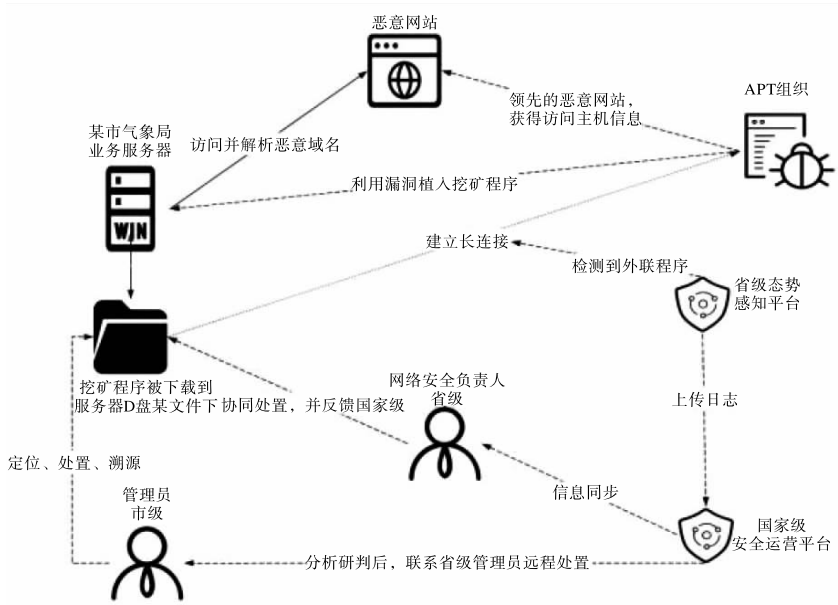

图 1 违规外联事件流程图解

为验证本文所提防御体系的行业普适性，进一步对关键信息基础设施安全领域的同类典型案例开展对比分析。基于护网行动攻击队的实践经验与案例复盘结果，2022 年某关键信息基础设施行业单位的安全攻防演练中，攻击者通过无人机投放恶意中继设备，并利用内部人员违规外联行为形成攻击入口，成功渗透侵入生产控制网络。该案例与上述违规外联安全事件的攻击路径高度契合，进一步印证了近源攻击与违规外联交织的复合威胁，已成为关键信息基础设施各行业面临的共性安全挑战。电力等关键信息基础设施领域，构建了融合技术迭代、多层管控、能力强化的一体化纵深防护体系，以应对复杂的网络威胁[12]。

上述典型案例表明，传统防御体系存在技术单点化、管理碎片化、防御静态化等系统性缺陷。亟需构建覆盖物理环境、网络边界、人员管理多维度的协同防御体系，强化技术与管理机制的深度融合，全面提升对近源攻击与违规外联威胁的全链路防控能力。

4 防御体系构建

本体系以关键业务资产的全面保护为核心，依托自动化资产测绘技术，实现网络资产的高覆盖率识别与动态风险画像构建；基于资产重要性等级实施差异化防护策略，深度整合技术、管理、人员三大核心维度，搭建四阶段闭环协同联动机制，最终构建起实现常态化、多角度的纵深防御体系。体系由外至内的感知层、协同层、处置层和管理层四层递进防护构建，实现关键信息基础设施全链路的常态化纵深防护(图 2)。

4.1 核心架构与协同防御逻辑

核心架构是以关键业务资产保护为核心，由感知层、协同层、处置层和管理层四层递进，构成技术、管理与人员三维协同的常态化纵深防御体系。

4.1.1 协同防御逻辑 针对近源攻击与违规外联的复合型安全威胁，首先聚焦于威胁识别，精准识别从物理渗透、建立外联通道到内网扩散的完整攻击链路。其次是防护策略协同，制定跨场景防护规则，实时监测终端接入情况与入网流量，识

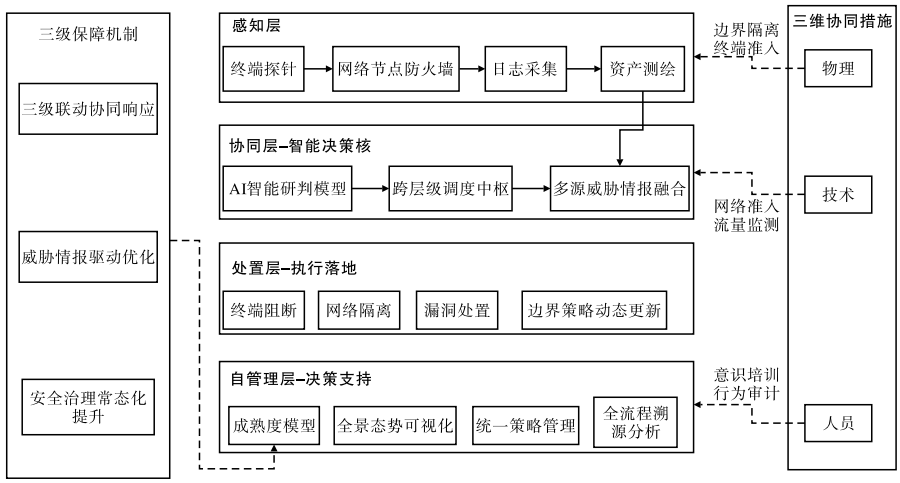

图 2　纵深防御体系总体架构图

别攻击命令控制信号。最后是响应处置协同,建立攻击类型与处置措施的映射关系,单一攻击触发对应防护操作,复合型威胁启动多级联动响应。

4.1.2　闭环防控流程　部署于终端的探针与关键网络节点传感器实时采集多源数据,包含端物理接口使用记录与网络外联协议等安全日志,设置告警阈值。依托多源威胁情报与智能模型对告警进行深度关联分析。识别近源攻击与违规外联的攻击链,通过规则引擎与 AI 模型结合实现自动化威胁定级与分类。根据研判结果,由处置层执行针对性协同操作。(1)终端-网络联动阻断。当终端探针检测到异常物理接入时,自动触发网络准入控制策略,切断终端网络访问权限。(2)跨设备策略协同。系统自动下发策略至边界防火墙、WAF、终端管理软件等设备,实现多设备协同封堵。(3)加密流量协同解析。通过终端探针与网络侧解密网关协同,实现对加密流量的合规解密与检测,避免违规外联通过加密通道逃逸。

溯源阶段通过管理层记录全流程数据,支撑攻击路径追溯。处置结果与溯源数据形成内部威胁情报,动态更新感知层和处置层的检测规则与阻断策略,实现闭环反馈与持续优化。

4.1.3　技术措施联动响应实现路径　防御体系通过感知层、协同层、处置层和管理层四层架构实现功能。参考民航空管实践,监测预警体系需实现技术、管理、运营三维融合,以明确标准并确保体系常态化有效运行[13]。感知层负责基础数据采集,包括物理、网络、资产等维度,为防御决策提供数据支撑;协同层是智能决策核心,集成多源威胁情报融合、AI 研判模型和调度中枢,实现威胁精准判定与资源协同调度;处置层执行防御措施,包括终端阻断、网络隔离等针对性操作;管理层提供决策支持,涵盖安全治理、行为审计等,保障体系持续优化。各层级通过标准接口互通数据与指令,并通过技术、物理、人员三个维度协同落地。技术上构建以网络准入和流量监控为核心的防护体系;物理上落实边界隔离、人员管控与终端准入;人员上贯穿意识培训、行为监控到问责追责的管理过程。

4.2　关键落地措施

4.2.1　气象内部实践　气象部门信息传输呈网络边界复杂、终端类型多样与数据共享频繁等特性。基于技术适配场景与防护覆盖全链路准则,构建以终端安全加固为基础、网络准入控制为核心、多层级流量监控为支撑、多部门协同为保障的技术防护体系,精准防控近源攻击与违规外联。网络准入控制上,国家气象信息中心使用终端安全管理软件实施入网管控,即终端需先下载安全软件方可访问互联网。同时联动统一身份认证系统与气象部门证书工具,实现无口令化业务准入流程,保障用户访问的合规性。监控运维与应急响应环节,利用“天镜”与安全分析平台对网络链路进行监控,实时监测设备状态、资源占用情况与流量异常,通过自定义告警脚本快速定位故障点。整合日志审计、漏洞扫描与资产测绘系统,依托自动化资产测绘技术实现资产全面发现,结合年度

资产梳理工作，在故障初期定位责任人。依托国-省-市(县)三级联动机制，明确跨层级处置流程，及时下达安全告警并整改。

4.2.2 三级联动机制 为保障体系持续有效运行，建立三级联动应急响应机制。明确国家、省、市(县)三级权责，国家层面统筹策略制定与跨区域协调，省级层面细化方案与区域管控，市(县)级层面负责日常运维与初级处置，依托安全运营与工单平台实现跨层级事件闭环处置(图 3)。

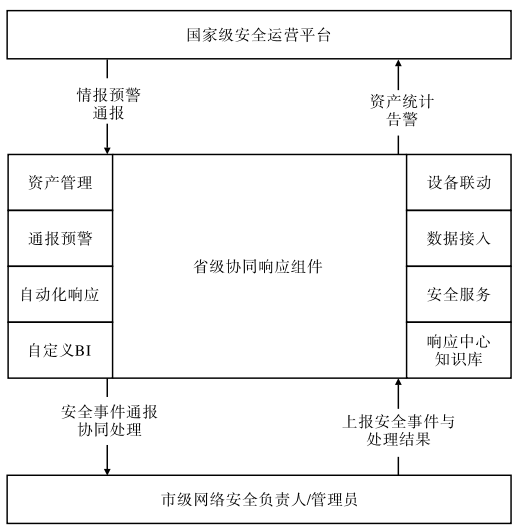

图 3 国省统一监测和联防联控(三级联动响应)

三级联动机制以“统一指挥、分级负责、协同响应”为原则，构建纵向贯通、横向协同的应急响应体系。国家气象信息中心作为统筹协调核心，负责制定全国气象部门网络安全统一策略、汇总全国威胁情报、协调跨省级重大安全事件处置、提供技术支持与资源保障；省级气象部门网络安全管理机构作为区域枢纽，负责对接国家级策略并制定本地化实施方案、监测辖区内安全态势、处置省级安全事件、指导市级应急响应；市(县)级气象部门作为执行配合单元，负责本地资产管理、日常安全监测、初级事件处置、上报安全告警与处置结果。

4.3 体系保障与评估

4.3.1 运行保障机制 威胁情报驱动机制整合内外部多源情报，构建高危漏洞快速响应流程，确保 24 小时内完成策略调整与修复。常态化提升机制则通过定期测评、攻防演练、专项科普与绩效考核，推动安全治理从被动处理突发网络安全事件向主动闭环管理演进，通过系统性的成熟度模型对防御效能进行量化评估与持续改进。

4.3.2 体系评估与成熟度模型 为科学评估该防御体系的实施效果并持续优化，参考美国国家标准与技术研究院网络安全框架与能力成熟度模型集成，构建常态化纵深防御成熟度模型(表 1)，从技术、管理、人员、流程四个维度划分为五个成熟度等级，实施渐进式建设与阶段性评估。该模型从能力建设与运营效果两个层面对防御体系进行评估：能力建设涵盖技术、管理、人员、流程四个维度；运营效果则通过安全事件平均响应时间(MTTR)、资产纳管覆盖率、高危告警闭环率等核心指标进行量化，直观反映防御体系从被动处理突发网络安全事件到主动免疫的效能演进。

表 1 常态化纵深防御成熟度模型

成熟度等级	技术维度	管理维度	人员维度	效果度量
初始级	单点防护工具	应急响应无流程	安全意识培训零星开展	MTTR＞4 h；资产不清；告警无闭环
可重复级	基础流量监测	有应急预案但未演练	定期培训但未考核	MTTR≈2～4 h；核心资产纳管率＞70%；告警初步记录
已定义级	多层防护联动	三级联动机制建立	培训＋考核＋奖惩制度建立	MTTR≤1 h；资产纳管率＞90%；高危告警闭环率＞85%；能发现常见违规外联行为
已管理级	威胁情报驱动动态防护	跨部门协同作战平台	全员持证上岗	MTTR≤30 min；资产动态画像；新增威胁类型发现能力提升；策略动态调整率＞80%
优化级	AI 预测性防护＋自动化响应	常态化攻防演练与迭代优化	安全文化内化于行为	MTTR≤10 min；自动化响应比例＞50%；具备攻击链回溯与预测能力；形成持续改进闭环

5　实验验证

宁夏气象局依据中国气象局网络安全设计方案,结合自身情况实施网络区域划分,各区域部署不同防火墙并设置访问策略,在重要网络区域和五个市节点部署态势感知探针。日志审计、运维审计等系统接入安全管理区,开展相关工作,借助各类资产统计工作,入网资产发现率超过 90%,在数次安全事件通报中,均实现资产归属单位的快速精准定位。互联网区部署网闸等设备,实施互联网出入管控。非军事区增添蜜罐安全系统。日志审计等系统与互联网非军事区核心交换机相连,实现与外网业务系统互通。安全态势感知系统开展安全数据采集等工作,通过 SIR 协同响应平台与国家气象信息中心对接实现数据上报与共享。内网各安全设备对接日志审计系统,将日志推送至 MSS 运营分析平台,初步适配防御体系。适配常态化多角度纵深防御体系后,宁夏气象局在 2025 年网络安全演习中失陷资产较 2024 年下降 93%,失陷资产源于供应链公司开发问题,验证了复合防御体系的有效性。后续建设安全运营分析平台,统一接入安全设备,将实现全流程自动化安全运维。

6　结语

研究聚焦数字化转型下关键信息基础设施的近源攻击与违规外联复合威胁,剖析传统边界防护模式应对复合威胁时技术单点化、管理碎片化、防御静态化等缺陷,提出以关键资产保护为核心的防御策略,整合技术、管理、人员维度,覆盖感知、协同、处置和管理四个纵深防御层面,依托三项保障机制构建常态化多角度纵深防御体系,设计成熟度模型量化防御水平。经宁夏气象局网络安全建设与攻防演习验证,该体系能有效识别并阻断网络攻击,显著提升关键基础设施的网络安全风险防御能力。

随着数据要素化进程加速,关键基础设施数据空间安全挑战日益凸显,需进一步探索“技术防御+法律规制+责任认定”协同治理模式应对复杂场景。后续工作将深化智能化升级和法治化协同,探索人工智能在威胁预测、自动化响应中的应用,实现防御升级;深入研究协同治理模式,明确各方主体责任边界,构建综合防控体系,形成网络安全防御新生态。

参考文献:

[1] 陈增境,卓凤艳,韩格格,等. 基于混合云的气象大数据云平台改造及安全防护设计[J]. 陕西气象,2025(1):77-82.

[2] National Institute of Standards and Technology. Security and privacy controls for information systems and organizations: NIST SP 800-53 Rev.5[S]. Gaithersburg: National Institute of Standards and Technology, 2020.

[3] SUDHARSON K, ROHINI C, SERMAKNI A M, et al. Quantum-resistant wireless intrusion detection system using machine learning techniques [C]//2023 7th International Conference On Computing, Communication, Control And Automation (ICCUBEA), 2023: 1-5.

[4] RAMAKRISHNAN B, MEENAKSHI C. Zero trust architecture for cloud and network security: a next-generation approach to access control [C]//2025 International Conference on Biomedical Engineering and Sustainable Healthcare (ICBMESH), 2025: 1-10.

[5] NALLURI S, VEERAVALLI S D, SRINATH S, et al. Blockchain-based multi-factor access control for preserving privacy in cloud storage of medical records [C]//2025 International Conference on Intelligent Computing and Knowledge Extraction (ICICKE), 2025: 1-6.

[6] 孟晓阳,杨巍,张楠,等. 医院近源网络攻击风险分析及对策建议[J]. 医学信息学杂志,2024,45(9):78-81.

[7] 刘明瀚. 港口内网攻防战法的优化方法[J]. 信息与电脑,2024(14):130-132.

[8] 张莉,王镇宇. 基于 VP 的信息内网终端违规外联管控的研究及应用[J]. 内蒙古科技与经济,2020(3):78-79.

[9] 钱锦,徐李冰,李昂,等. 基于机器学习的涉密终端违规外联自动检测系统[J]. 兵工自动化 2025,44(8):73-77.

[10] 王鹏彪. 政务终端违规外联检测防护研究与实践[J]. 通信世界,2025(19):46-48.

[11] 胡丽娜,蒋凯元,姜静. 关键信息基础设施系统安全防护前沿技术研究[J]. 信息安全研究,2025,11(12):1075-1080.

[12] 付申杰,付申俊,姜杰,等. 电力关键信息基础设施网络安全管理体系的构建[J]. 电力安全技术,2025,27(5):1-3.

[13] 苏力行,王亮,宁文冠,等. 民航空管地区级网络安全监测预警体系规划与实施研究[J]. 成都信息工程大学学报,2025,40(6):780-786.

[14] 杜鹏飞,哈晓琳,段连密. 关键信息基础设施安全下数据空间安全研究[J]. 信息安全研究,2025,11(12):1093-1098.

[15] 王珂,曹波,马园,等. 统一身份认证系统在陕西气象网络防护中的应用[J]. 陕西气象,2024(4):77-80.

[16] 曹波,向浩然,马园,刘畅. 态势感知技术在省市气象部门间网络联动中的应用[J]. 陕西气象,2025(4):74-78.

[17] 刘畅,庞菲菲,白水成,等. 市级气象信息网络监控系统研究与实践[J]. 陕西气象,2021(5):68-70.