气象信息网络安全防护体系构建与加固要点

袁小燕[1] 刘洋[2] 谢华清[1]

1 福建省宁德市气象局，福建省宁德市，352100；

2 福建省宁德市防雷中心，福建省宁德市，352100；

摘要：随着气象业务数字化、智能化进程加速，气象信息网络已成为支撑灾害预警、科学研究等核心工作的“生命线”，其安全防护能力关乎国计民生。本文立足行业需求，系统探讨气象信息网络安全防护体系的构建与强化路径。针对外部网络攻击、数据泄露、恶意软件入侵等多元安全威胁，深入剖析防护体系建设的核心要素：从制定精细化安全策略、划分用户访问权限，到部署防火墙等多层次技术防护；同时提出切实可行的加固方案，包括建立常态化安全评估机制、开展情景化人员培训、完善应急响应预案等。

关键词：气象信息；网络安全；防护体系；加固要点

DOI：10.69979/3041-0673.25.11.073

随着气象科技的飞速发展，气象信息网络在气象业务中的作用愈发关键。气象数据的采集、传输、处理和发布等各个环节都高度依赖网络。然而，网络环境的开放性和复杂性使得气象信息网络面临着诸多安全威胁，如黑客攻击、病毒感染、数据泄露等。一旦气象信息网络遭受安全事件，不仅会影响气象业务的正常开展，还可能对国家的经济建设和社会稳定造成不利影响。因此，构建科学合理、坚固可靠的气象信息网络安全防护体系，并不断进行加固和完善，成为当前气象部门亟待解决的重要问题。

1 气象信息网络面临的安全威胁

1.1 外部网络攻击

在数字化气象监测体系中，外部网络攻击已成为威胁气象信息网络安全的核心隐患[1]。不法分子往往凭借敏锐的漏洞侦查能力，借助分布式拒绝服务、SQL 注入等多样化攻击手段，对气象网络系统发起恶意侵袭。DDoS 攻击通过控制大量“僵尸”设备，向目标服务器发起海量无效请求，瞬间吞噬网络带宽与计算资源，导致气象数据传输通道堵塞、处理系统瘫痪，直接影响气象监测、预报和服务的时效性与准确性。而 SQL 注入攻击则更为隐蔽，攻击者利用应用程序与数据库交互的漏洞，绕过身份验证机制，肆意窃取、篡改气象数据库中的关键信息，这些数据一旦遭到破坏或泄露，不仅威胁气象业务的正常运转，更可能引发灾害预警失效等严重后果。随着网络技术迭代升级，新型攻击手段不断涌现，诸如加密流量攻击、供应链渗透等隐蔽性更强的威胁持续涌现，使得气象信息网络的安全防护面临前所未有的严峻挑战。

1.2 病毒与恶意软件感染

在气象信息网络安全防护体系中，病毒与恶意软件构成的威胁不容小觑。这些数字威胁载体如同无形的“数字瘟疫”，借助多样化的传播途径渗透至气象系统内部。移动存储设备的交叉使用、伪装成正常文件的恶意电子邮件，都可能成为病毒入侵的突破口。一旦气象网络中的计算机中招，轻则系统运行卡顿、频繁死机，重则直接导致操作系统崩溃，引发核心气象数据的永久性丢失，严重干扰气象监测与预报业务的正常开展。恶意软件的危害更具隐蔽性与破坏性，它们会在用户毫无察觉的情况下，悄然窃取气象观测数据、精密预报模型参数等核心敏感信息，并通过加密通道传输至外部非法机构。这些数据一旦泄露，不仅威胁气象信息安全，更可能对国家气候战略决策、灾害预警体系造成重大冲击。随着网络黑产技术迭代，新型病毒与恶意软件不断推陈出新，其传播速度呈指数级增长，攻击手段也愈发狡猾隐蔽，使得气象信息网络的安全防线面临前所未有的挑战。

1.3 数据泄露风险

气象信息网络作为国家关键信息基础设施，承载着海量气象观测数据、精密预报成果等核心信息资产[2]。这些数据不仅是气象科学研究的基石，更是防灾减灾、农业生产、交通调度等领域科学决策的重要依据。然而，网络安全管理体系的薄弱环节与人为操作风险，正成为威胁数据安全的"定时炸弹"。部分单位因权限管理混乱、加密措施缺失，或工作人员误操作、违规外联，都可能

导致数据意外泄露。气象数据泄露的危害远超行业范畴。一旦涉及台风路径、极端天气预测等敏感信息外泄，不仅损害气象部门公信力，更可能被不法势力利用，扰乱灾害预警体系。尤为值得警惕的是，部分气象数据蕴含着与军事部署、国防设施相关的地理环境信息，若流入敌对势力手中，极有可能被用于军事目标定位、作战环境分析，对国家安全构成直接威胁。筑牢气象数据安全防线，已成为维护国家战略安全与社会稳定的重要课题。

2 气象信息网络安全防护体系构建要点

2.1 安全策略制定

安全策略作为气象信息网络安全防护的根基，需深度契合部门业务特性与网络架构。气象部门应结合数据采集、预报发布等核心业务需求，以及网络覆盖广、节点分散的特点，构建精细化安全策略体系。其中，访问控制策略着重建立分级权限管理机制，根据岗位职能精准划分用户权限，严禁外来人员随意进出机房等重要场所，有效杜绝无关人员接触敏感数据；对气象数据采用网闸、堡垒机、网页防篡改专线传输等技术保障数据不被篡改，定期进行安全审计，及时发现并修复安全漏洞，通过监控系统日志和用户活动，可以及时发现异常行为并采取相应措施；备份恢复策略则通过“本地+异地”二级备份体系，按小时、日、月周期对数据进行差异化备份，并制定涵盖系统崩溃、硬件故障等场景的详细恢复预案。通过多策略协同，既能确保气象业务的连续性，又能在突发状况下实现数据快速恢复，为气象信息网络安全构筑坚实屏障。

2.2 网络拓扑优化

构建科学合理的网络拓扑架构，是筑牢气象信息网络安全防线的关键一环[3]。气象部门可借鉴分层分区的网络设计理念，将整个网络系统划分为核心交换区、数据存储区、应用服务区等功能各异的独立区域。这种分区策略就如同为网络构筑起层层防护壁垒，每个区域各司其职，互不干扰，即便某一区域遭受安全威胁，也能有效避免风险向其他区域蔓延扩散。在区域间的访问控制上，需充分发挥防火墙、入侵检测系统等安全设备的防护效能。通过严格设定访问策略，精准识别并阻断非法访问请求，确保只有经过授权的数据流才能在不同区域间传输。同时，引入冗余设计机制，为关键网络设备、链路配置备份方案。当某一节点出现故障时，备用设备能够迅速接管工作，保障网络持续稳定运行，最大限度减少因单点故障引发的网络瘫痪风险，为气象数据的安全传输与稳定处理提供坚实的网络保障。

2.3 安全技术手段运用

在气象信息网络安全防护体系建设中，综合运用多元技术手段是抵御安全威胁的核心策略。防火墙作为网络安全的前沿堡垒，犹如智能门卫，依据预先设定的访问控制规则，对进出网络的数据流进行严格筛查，精准拦截非法访问请求，将恶意攻击拒之门外。入侵检测与防御系统则如同 24 小时值守的网络哨兵，通过实时分析网络流量、监测系统日志，敏锐捕捉异常行为模式，一旦发现黑客入侵迹象，即刻启动阻断机制，将攻击扼杀在萌芽状态。数据安全层面，加密技术如同为气象数据穿上隐形铠甲，通过复杂的算法对传输与存储过程中的数据进行编码处理，即便遭遇窃取，未经授权者也无法读取真实内容。虚拟专用网络技术则构建起安全的数据传输隧道，在保障气象部门内外网络高效互联的同时，利用加密通道与身份认证双重防护，有效规避数据泄露风险。这些技术手段相互协同、优势互补，共同织就气象信息网络的安全防护网。

3 气象信息网络安全防护体系加固要点

3.1 定期安全评估

构建气象信息网络安全防线，离不开常态化的安全评估机制。市级气象部门需引入第三方专业机构，对网络系统开展全维度“体检”。从扫描网络漏洞、审计安全策略，到核查数据加密与访问权限，每一项评估都精准定位潜在风险。通过系统性排查，及时发现防火墙配置缺陷、数据传输漏洞等安全隐患，并针对性制定整改方案。同时，将安全评估纳入年度工作规划，建立动态监测与持续优化机制，定期复盘改进，确保气象信息网络在复杂环境下始终保持高效防护能力，为气象业务稳定运行筑牢安全屏障。

3.2 加强人员培训

在气象信息网络安全体系中，人员因素是最关键的防线[4]。气象部门需构建系统化的安全培训体系，通过定期开展专题培训，强化员工的网络安全意识与实操能力。培训内容不仅涵盖网络安全相关法律法规、部门内部安全操作规范，还包括应急响应流程与数据泄露处置技巧。通过案例分析、模拟演练等多样化教学方式，让员工深刻认识网络安全对气象业务的重要性，熟练掌握安全操作技能，从源头上规避因误操作引发的安全风险。同时，建立科学的安全考核机制，将安全操作纳入绩效

考核，以正向激励激发员工主动参与网络安全防护，筑牢气象信息网络安全的“人为防线”。

3.3 应急响应机制建设

面对复杂多变的网络安全威胁，完善的应急响应机制是气象部门守护信息网络的“安全盾牌”。气象部门需制定精细化的应急响应预案，从事件监测预警、分级分类报告，到应急处置、系统恢复重建，每个环节都明确流程与责任归属。同时，组建专业应急响应团队，成员涵盖网络技术、数据安全、运维保障等领域骨干。通过常态化开展攻防模拟、数据泄露处置等实战演练，提升团队对勒索病毒攻击、数据窃取等突发情况的快速反应与处置能力。一旦遭遇网络安全事件，确保能第一时间启动预案，高效控制事态发展，将业务中断与数据损失降至最低。

4 气象信息网络安全防护体系构建与加固的案例分析

4.1 案例背景

某市级气象部门的信息网络肩负着全市气象数据全流程处理重任，从野外站点的数据采集，到千家万户的预报发布，每个环节都依赖其稳定运转。但随着气象业务的数字化、智能化推进，网络面临的安全挑战与日俱增。黑客攻击、数据泄露等隐患，不仅威胁业务连续性，更可能影响防灾减灾等民生保障工作。为此，该部门立足保障气象服务生命线，着手构建系统性的网络安全防护体系，通过技术升级与管理优化，筑牢数字防线，确保气象信息网络安全可靠运行。

4.2 构建与加固措施

首先从制度层面入手，制定精细化安全策略，严格划分用户访问权限，强化数据全生命周期加密与异地备份管理，确保核心数据安全可控。在网络架构优化上，摒弃传统扁平模式，采用分层分区设计，将核心交换、数据存储等功能区域物理隔离，并部署高性能防火墙、智能入侵检测系统，构建起立体防御体系。同时建立常态化安全评估机制，通过专业机构定期“体检”，累计修复高危漏洞几十余处。此外，通过案例教学、模拟演练等多样化培训，显著提升员工安全素养，并组建专业应急团队，开展季度实战演练，确保面对突发安全事件时能快速响应、高效处置。

4.3 实施效果

自启动气象信息网络安全防护体系建设以来，该市级气象部门通过技术与管理的双重升级，实现网络安全防护能力质的飞跃。防火墙、入侵检测系统等防护设备的部署，配合精细化的权限管理，有效抵御了外部攻击与内部隐患。如今，网络攻击频次同比下降超七成，数据泄露风险得到全方位管控。稳定可靠的网络环境为气象数据的高效采集、传输与处理提供坚实支撑，显著提升气象预报的精准度与及时性，有力保障了全省气象服务的质量与效率，筑牢防灾减灾的“数字防线”。

5 结论与展望

构建和加固气象信息网络安全防护体系是保障气象业务稳定运行的关键。通过对气象信息网络面临的安全威胁进行分析，提出了构建防护体系的关键要点，包括安全策略制定、网络拓扑优化、安全技术手段运用等，以及加固要点，如定期安全评估、加强人员培训、应急响应机制建设等。通过实际案例的分析，验证了这些措施的有效性。

展望未来，随着气象科技的不断发展和网络环境的日益复杂，气象信息网络安全防护将面临更多的挑战。气象部门需要不断加强技术创新，引入新的安全技术和理念，如人工智能、大数据分析等，提高气象信息网络安全防护的智能化水平。同时，应加强与其他部门的合作与交流，共同应对网络安全威胁，保障气象信息网络的安全稳定运行，为气象事业的发展提供坚实的安全保障。

参考文献

[1]郭晟.加强气象信息网络系统安全与防范分析[J].计算机产品与流通,2019,(10):58.
[2]周琰,蒋敏慧,曹磊,等.气象业务信息化发展下的网络安全治理初探[J].气象科技进展,2018,8(01):274-276.
[3]张虹.气象信息网络安全防御技术[J].互联网周刊,2022,(06):36-38.
[4]于璐.探析气象信息网络安全的影响因素及安全管理措施[J].中国高新科技,2023,(03):39-41.