**Climate Change Research Letters** 气候变化研究快报, 2026, 15(1), 89-94
Published Online January 2026 in Hans. https://www.hanspub.org/journal/ccrl
https://doi.org/10.12677/ccrl.2026.151012

Hans汉斯

# 气象数据网络安全防护策略研究与实践

**王定法，彭学琴，罗哲厚**

四川省眉山市气象局，四川 眉山

收稿日期：2025年12月3日；录用日期：2026年1月2日；发布日期：2026年1月14日

## 摘　要

**随着气象信息化建设的深入推进，气象数据已从单一的业务资源转变为驱动社会经济发展和保障国家安全的关键生产要素。其高价值、海量性、实时性等特点，使其成为网络攻击的重要目标。本文立足于气象部门网络安全管理的实际工作，结合当前气象数据安全面临的严峻挑战，从技术、管理、运维三个维度，系统性地梳理和总结了气象数据网络安全的防范措施。内容涵盖网络边界安全、数据全生命周期保护、身份认证与访问控制、安全监测与态势感知、安全管理制度与人员意识提升等多个方面，旨在构建一个“主动防御、纵深协同、管理闭环”的综合性防护体系，为保障气象数据的机密性、完整性和可用性，支撑气象业务的高质量发展提供实践参考。**

## 关键词

**气象数据，网络安全，防范措施**

# Research and Practice of Security Protection Strategies for Meteorological Data Network

**Dingfa Wang, Xueqin Peng, Zhehou Luo**

Meishan City Meteorological Bureau, Meishan Sichuan

Received: December 3, 2025; accepted: January 2, 2026; published: January 14, 2026

## Abstract

**With the deepening of meteorological information construction, meteorological data has transformed from a single business resource into a key production factor that drives social and economic development and ensures national security. Its high value, massive volume, real-time characteristics, make it an important target for cyberattacks. Based on the actual work of network security management in meteorological departments and considering the severe challenges currently faced by meteorological data security, this paper systematically reviews and summarizes preventive**

文章引用: 王定法, 彭学琴, 罗哲厚. 气象数据网络安全防护策略研究与实践[J]. 气候变化研究快报, 2026, 15(1): 89-94.
DOI: 10.12677/ccrl.2026.151012

**measures for meteorological data network security from the technical, management, and operational dimensions. The content covers multiple aspects, including network boundary security, full lifecycle data protection, identity authentication and access control, security monitoring and situational awareness, security management systems, and personnel awareness improvement. The goal is to build a comprehensive protection system characterized by "proactive defense, depth collaboration, and closed-loop management," providing practical references to ensure the confidentiality, integrity, and availability of meteorological data and supporting high-quality development of meteorological services.**

## Keywords

**Meteorological Data, Network Security, Precautionary Measure**



## 1. 引言

气象数据是气象业务的基石，精准的观测、预报、预警和服务无不依赖于安全、可靠、高效的数据流[1]。在“数字中国”和“智慧气象”战略的驱动下，气象数据的采集、传输、存储、处理和应用已深度融入云计算、大数据、物联网等新一代信息技术架构。然而，网络环境的开放性与复杂性，使得气象数据面临前所未有的安全威胁。数据泄露、篡改、服务中断、恶意软件入侵等风险日益凸显。一旦气象数据或业务系统遭受破坏，不仅会影响气象预报的准确性，更可能对防灾减灾、农业生产、航空运输、国防安全等关键领域造成不可估量的损失。

构建并实施一套科学、系统、高效的气象数据网络安全防范措施，已不再是简单的技术补充，而是气象事业可持续发展的内生需求和核心保障。本文旨在结合行业内的研究成果与实践经验，对当前主流的防范措施进行系统性简介。

## 2. 气象数据面临的主要安全问题

随着气象业务的数字化、智能化转型，气象数据在价值提升和应用拓展的同时，其网络安全风险也日益严峻复杂。综合分析，当前气象网络数据主要面临以下几大核心问题。

### 2.1. 数据全生命周期管控薄弱

气象数据流程环节复杂，涵盖收集、传输、处理、存储、共享、服务及销毁全过程。在此过程中，普遍存在“重使用、轻安全”的现象。数据传输环节仍存在使用未加密信道的情况，易被窃取或篡改[2]；数据存储环节访问控制不严，内部人员或外部攻击者越权访问风险大；数据共享开放时，对高敏感数据缺乏有效的脱敏或匿名化处理；数据销毁环节监管缺失，导致残留数据泄露。

### 2.2. 网络攻击手段多样化

气象网络面临分布式拒绝服务(DDoS)攻击、SQL 注入、APT 攻击、勒索软件等多重威胁。攻击者常利用大数据环境下新型技术(如分布式计算框架)的未知漏洞发起攻击，具有极强的隐蔽性。传统的、基于边界和特征规则库的防御技术(如防火墙、IDS/IPS)难以有效检测和抵御这类新型、未知的攻击，导致防护体系形同虚设。

### 2.3. 内部安全管理漏洞

内部威胁是数据安全的重要风险源。一方面，部分从业人员网络安全意识淡薄，存在使用弱口令、随意插拔私人移动存储设备、在公共网络处理敏感数据等不安全行为。另一方面，气象部门网络安全制度建设不足，现有制度存在操作性不强、针对性不够等问题，导致“谁主管、谁负责”的原则难以真正落实，对内部人员的操作行为缺乏有效监督和审计。

## 3. 网络气象数据安全防护措施建设

为应对日益严峻的数据安全挑战，构建坚实可靠的气象数据安全防线，本文致力于建立一个系统化、多维度的综合防护体系。该体系主要涵盖四个核心能力域：一是夯实数据安全管理能力；二是构建数据安全监测预警能力；三是强化数据安全技术防护能力；四是提升数据安全应急处置能力。通过这四大能力的协同联动与闭环管理，全方位保障气象数据的机密性、完整性与可用性。

### 3.1. DMZ (隔离区)的应用

DMZ 区是计算机网络安全领域的一个概念，指的是在企业内部网络(内网)和外部不可信网络(如互联网)之间设置的一个隔离缓冲区域(见图 1)。其核心作用是在保护内网安全的同时，提供对外服务的功能，平衡安全性和可用性。DMZ 作为内部网络与外部不可信网络之间的缓冲区域，在气象数据对外共享与服务中扮演着关键角色。通过将对外提供服务的 Web 服务器、数据查询接口等部署在 DMZ 区，并配置严格的防火墙策略，可以实现以下目标。

隔离内外网：将需要公开访问的服务(如 Web 服务器、邮件服务器、FTP 服务器等)部署在 DMZ 区域，使其与内网隔离[3]。外部用户可访问 DMZ 中的服务，但无法直接访问内网核心资源；内网用户可访问 DMZ 和外网，但需遵循安全策略。

可控的对外服务：允许外部用户通过防火墙的规则访问 DMZ 中的特定服务(如网站、API 接口)，仅允许访问 DMZ 中必要的服务端口(如 80/443 用于 Web、25/110 用于邮件、443 用于 VPN)，禁止访问其他端口(如远程桌面端口 3389、数据库端口 3306/1433)。启用 IP 白名单(如仅允许特定合作伙伴 IP 访问 DMZ 内的服务)。同时限制无关流量，降低内网被攻击的风险。

增强内网安全性：限制 DMZ 服务器主动连接外网的权限，仅允许必要的出站流量(如更新系统补丁、发送邮件)，在 DMZ 与外网、DMZ 与内网之间部署 IPS、WAF，实时检测并阻断恶意流量和攻击(如 SQL 注入、XSS 攻击、DDoS 攻击)。即使 DMZ 中的服务器被入侵，攻击者也难以直接渗透到内网，因为 DMZ 与内网之间通常设置了更严格的访问控制策略(如防火墙规则)。

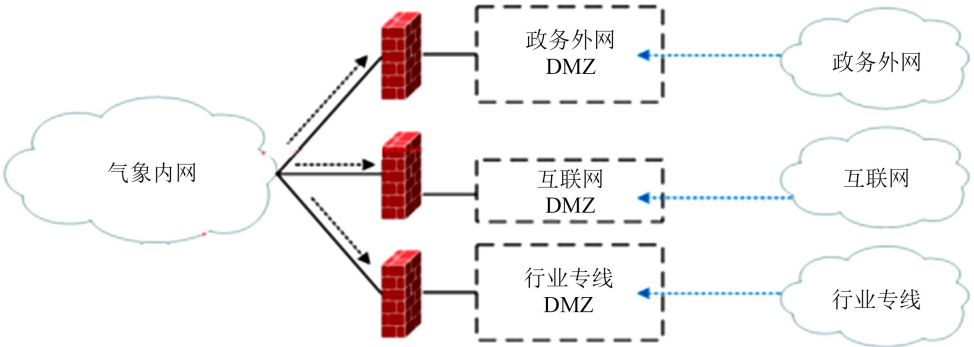


**Figure 1.** DMZ planning and design drawing
**图 1.** DMZ 规划设计图

### 3.2. 网络架构优化与收敛

减少互联网暴露面，对非必要的互联网出口进行清理和合并，降低被攻击的概率[4]。对于内部业务系统，应尽量避免直接暴露在公网，可通过 VPN (虚拟专用网络)提供远程安全接入。同时网络分区分域管理，根据业务功能和数据敏感性，将内部网络进一步划分为不同安全级别的区域，如核心业务区、数据存储区、办公区等，并在区域间部署访问控制策略。

## 4. 数据安全管控及访问控制

### 4.1. 数据传输安全

在数据采集、交换和共享过程中，必须采用加密技术(如 AES、RSA 等加密算法)对传输数据进行加密，防止在传输过程中被窃取或篡改[5]；同时结合身份验证机制(如多重认证)确认通信双方身份合法性，避免非法访问或中间人攻击。此外，安全传输还需依托协议安全(如 TLS/SSL)保障通道加密，并借助实时监测与态势感知系统对传输行为进行动态分析，识别异常流量或潜在威胁，并及时触发预警。对于跨区域、跨机构的重要数据同步，优先采用物理专线或 IPSec VPN 等加密通道，确保传输链路的可靠性与保密性。

### 4.2. 数据存储安全

对敏感数据和核心业务数据，在落盘时应进行加密存储。即使存储设备丢失或被盗，攻击者也无法直接读取数据内容。建立严格的数据库和文件系统访问权限控制，确保只有授权用户和应用程序才能访问相应数据。在此基础上，通过数据备份与容灾技术建立多重副本，将数据分散存储在多个存储节点上，通过数据冗余和副本机制保障数据的安全性和可靠性，防止因硬件故障或人为误操作导致数据丢失。在开发、测试或对外提供数据分析服务时，对敏感信息(如精确坐标、特定用户信息)进行脱敏处理，在不影响使用的前提下保护隐私和核心细节。

### 4.3. 身份认证

“永不信任，始终验证”的零信任理念正成为安全架构的核心[6]。对于系统管理员、核心数据访问人员等高权限账户，强制启用多因素认证，结合密码、手机验证码、硬件令牌或生物特征等多种方式，极大提升账户破解难度。建立统一的身份认证系统，实现单点登录和集中化的用户生命周期管理，避免账户冗余和僵尸账户带来的风险。

## 5. 构建主动安全监测与应急响应体系

被动防御已不足以应对高级别威胁，必须向主动、智能的防御模式转变。

### 5.1. 部署探针与网络安全态势感知平台

态势感知是指对网络环境中各类安全要素进行实时采集、综合分析，并形成对当前和未来安全状态的可理解、可预测的能力。探针是部署在网络关键节点上的专用软硬件设备，用于实时采集和初步分析特定类型的安全数据。二者共同构成了从局部监测到全局感知的协同防御体系。

在网络安全态势感知体系中，探针与态势感知平台共同构成一个闭环协同的工作流程(见图 2)。首先，探针作为部署在网络关键节点(如核心交换机、区域边界)的感知终端，负责实时采集网络流量、系统日志、资产信息、异常行为及潜在威胁数据。探针具备协议解析、流量重组、恶意样本捕获、行为审计等能力，能够识别 SQL 注入、跨站攻击、木马传播等多种安全事件，并对资产配置合规性进行自动化核查。随后，

采集到的多源异构数据被统一传输至态势感知平台，平台依托大数据技术对数据进行汇聚、标准化和关联分析，结合威胁情报库与行为建模，实现对全网安全态势的动态评估与可视化呈现。平台不仅能够识别已知攻击，还可通过异常检测与机器学习方法发现未知威胁，生成安全告警并触发预设的响应策略。网络管理人员根据平台输出的风险视图与处置建议，执行协同响应与策略优化，从而形成“监测–分析–预警–处置–反馈”的闭环安全管理机制，最终实现对气象系统网络安全状态的持续感知与主动防御[7]。

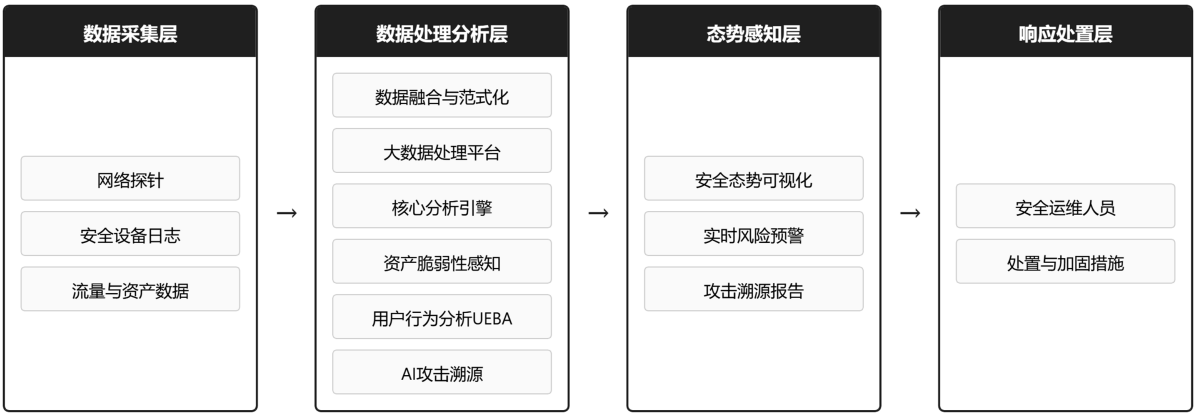


**Figure 2.** Flowchart of situation awareness work
**图 2.** 态势感知工作流程图

### 5.2. 完善应急响应机制

建立完善的网络安全应急响应机制是应对安全事件、降低损失的关键。其构建应遵循系统化、规范化的原则，涵盖预案制定、团队建设、监测预警和恢复处置等全流程。首先，需制定详细的应急预案，明确组织机构、职责分工、响应流程和技术措施，针对黑客攻击、数据泄露、恶意软件感染、服务中断等不同场景设计具体处置方案。其次，组建由网络安全专家、技术人员和管理人员构成的专职应急团队，通过定期培训与实战演练提升协同作战与快速响应能力。一旦发生安全事件，立即启动预案，执行隔离受影响系统、阻断攻击路径、恢复备份数据等措施，并同步开展事件溯源与责任认定。事后还需进行全面评估与整改，优化防护策略，完善响应流程。最终，通过制度、技术与人员的有效协同，形成“监测–预警–处置–恢复–改进”的闭环管理，确保气象业务在遭受网络安全威胁时能够快速响应、最小化影响并持续提升安全防护水平。

## 6. 完善制度与提升安全意识

在现有国省级气象网络安全管理制度框架下，需结合气象业务特性、攻防演习中暴露的薄弱环节，以及气象高质量发展可能面临的新型风险，构建一套更加完善的气象网络安全管理体系。该体系应涵盖技术指南、操作规范与管理政策等多个层面，具体如气象网络安全定级细则、基于移动互联技术的气象业务管理办法、气象部门网络安全定级工作指南、气象网络安全教育培训管理办法等。在推进制度建设中，应同步加强政策宣贯与培训指导，通过常态化监督确保制度有效落地，并将网络安全工作成效纳入单位年度考核指标体系，从而保障制度的执行。

为有效提升网络安全意识，应构建常态化、体系化的培训机制，将安全要求融入日常工作的每个环节。网络安全培训内容需紧密结合实际，覆盖密码管理、病毒防范、邮件安全、数据保护及无线网络使

用等核心场景，通过剖析真实安全事件及其严重后果，直观揭示风险与隐患。单位应定期组织专项学习、实战攻防演练，同时建立健全安全管理体系与技术防护措施，形成制度约束力。个人则应主动学习安全知识，养成良好的安全习惯，如规范密码设置、及时更新补丁、锁屏离座、敏感信息加密等。通过单位与个人的共同努力，筑牢网络安全防线。

## 7. 总结

面对日益严峻的网络安全形势，气象数据的安全防护是一项复杂而长期的系统工程。它要求我们摒弃“重建设、轻安全”或“重技术、轻管理”的旧有观念，转而构建一个技术与管理深度融合、防护与检测响应协同、覆盖数据全生命周期的综合性防范体系。

该体系以网络边界隔离为基础屏障，以数据分类分级和全生命周期管控为核心，以严格的身份认证和访问控制为关键手段，以主动的态势感知和快速的应急响应为能力支撑，最后以完善的管理制度和全员的安全意识为根本保障。通过这种“纵深防御、主动免疫”的策略，才能有效应对层出不穷的网络威胁，筑牢气象网络安全的防线，确保气象数据这一宝贵战略资源的安全，从而为气象事业的高质量发展和社会的安全稳定运行提供坚实可靠的支撑。

## 参考文献

[1] 马季芳. 气象信息网络安全发展状况研究[J]. 网络安全技术与应用, 2021(9): 120-121.

[2] 王涵. 气象信息化建设中的网络防护体系研究[J]. 农业灾害研究, 2025, 15(1): 173-175.

[3] 李鹿. DMZ 区在气象业务中的数据传输应用与安全性探讨[J]. 内蒙古科技与经济, 2024(9): 127-130.

[4] 蒲晓虎, 何奇, 钟美. 气象数据安全防护体系建设探索与实践[J]. 网络安全与数据治理, 2025, 44(3): 59-62.

[5] 彭晓姣. 气象信息网络安全风险及应对策略分析[J]. 中国宽带, 2024, 20(12): 49-51.

[6] 刘晓波, 冯冼, 张思睿, 等. 基于零信任的省级气象信息网络防护技术研究[J]. 计算技术与自动化, 2024, 43(2): 151-155.

[7] 马晋, 赵思亮. 态势感知在气象网络安全防御中的应用[J]. 微型电脑应用, 2023, 39(7): 13-16.