Software Engineering and Applications 软件工程与应用, 2026, 15(4), 614-623
Published Online August 2026 in Hans. https://www.hanspub.org/journal/sea
https://doi.org/10.12677/sea.2026.154057

Hans汉斯

浅议民航气象关键信息基础设施安全保护

黄登峰

民航西南地区空中交通管理局，四川 成都

收稿日期：2026年5月19日；录用日期：2026年8月20日；发布日期：2026年8月28日

摘　要

民航气象关键信息基础设施(CII)是保障国家空天安全和航班运行的核心载体。本研究针对其面临的老旧设备入网风险、数据安全威胁及业务连续性挑战，通过政策文本分析、标准逆向解构与事故案例挖掘，构建首套民航气象专属防护体系。创新提出“四横一纵”韧性防御框架(战略治理、风险管理、技术防护、运行保障四层架构与纵深防御轴)，实现风险驱动的动态防护。核心措施包括：建立气象数据多级防护机制，制定《民航气象数据分类分级指南》；部署国密算法加密敏感数据；设计“3-2-1”应急备份策略；构建业务流－威胁映射模型。实施路径强调责任具象化(AB角配置、KPI一票否决)、监管协同化(双随机渗透测试)及能力轻量化(微解决方案库)。成果为民航强国建设提供安全基线支撑，助推“四强空管”神经中枢融合。

关键词

民航气象，网络安全，数据安全

A Preliminary Study on Safeguarding Critical Information Infrastructure of Civil Aviation Meteorology

Dengfeng Huang

Meteorology Division Southwest Air Traffic Management Bureau of China, Civil Aviation Administration of China, Chengdu Sichuan

Received: May 19, 2026; accepted: August 20, 2026; published: August 28, 2026

Abstract

Civil aviation meteorological Critical Information Infrastructure (CII) serves as the cornerstone of national airspace security and flight operations. Confronting legacy equipment networking risks, data

文章引用: 黄登峰. 浅议民航气象关键信息基础设施安全保护[J]. 软件工程与应用, 2026, 15(4): 614-623.
DOI: 10.12677/sea.2026.154057

security threats, and operational continuity challenges, this study constructs the first dedicated protection framework for aviation meteorology through policy analysis, standard deconstruction, and accident jurisprudence mining. The innovative "Four Horizontal Layers and One Vertical Axis" resilience model integrates strategic governance, risk management, technical fortification, and operational assurance with deep defense capabilities. Key solutions include: establishing a multi-level data protection mechanism with Civil Aviation Meteorological Data Classification Guidelines, applying cryptographic algorithms (e.g., SM4) for sensitive data encryption, designing a "3-2-1" emergency backup strategy, and developing service-flow-threat mapping. Implementation advocates responsibility embodiment (AB-post configuration, KPI veto), regulatory collaboration (randomized penetration testing), and lightweight capacity building (scenario-based micro-solutions). This framework underpins China's aviation power strategy and advances the integration of meteorological security into the "Four Strengths Air Traffic Management" neural hub.

Keywords

Civil Aviation Meteorology, Network Security, Data Security

1. 绪论

1.1. 研究背景与意义

随着《中华人民共和国网络安全法》[1]和《关键信息基础设施安全保护条例》[2]的实施，民航气象CII安全已被纳入国家网络空间安全战略核心范畴。民航运行的分钟级决策机制高度依赖气象数据的精准可靠——据民航局统计，32.7%的航班延误与气象服务异常直接相关[3]。当前突出的安全威胁源于历史遗留系统网络化改造带来的老旧设备安全风险，已成为高级持续性威胁(APT)渗透的跳板。本研究在近几年民航气象安全事件分析的基础上，初步构建一套切合民航气象业务特点的CII防护框架，探讨解决老旧设备入网安全问题，为民航安全研究提供参考。

1.2. 相关概念界定

据《关键信息基础设施安全保护条例》[2]法定要件，民航气象CII界定为同时满足：① 破坏可引发航班大面积瘫痪/空域安全事件；② 承载核心气象业务流的设施。其核心范畴包括支撑智能预报、实时观测、空域数据传输、战略数据存储及高可信运行环境的关键系统集群，主要特征表现为业务连续性、数据敏感性、系统关联性的三极强化。

2. 相关研究与研究设计基础

2.1. 国内外研究现状与主流防护框架对比

国外在通用CII框架(如NIST CSF) [4]及航空气象数据安全方面(如FAA、ICAO相关要求) [5] [6]的研究相对成熟。我国虽然已初步建立CII法规体系，但民航气象领域研究深度存在不足。虽投入较多资源应对民航气象安全威胁，但仍未建成成熟的民航气象威胁反馈模型；未健全国防安全气象探测数据、特定区域历史气象数据、特殊敏感数据保护的规范和要求；在用的老旧设备，未建立统一的安全管理机制；气象部门、空管部门、航空公司之间数据安全交换接口标准不统一，未能形成高效的协同防护机制，

跨系统风险高。

目前国际主流的关键信息基础设施防护框架多为通用型设计，缺乏针对民航气象业务特性的定制化适配。本研究将“四横一纵”韧性防御框架与 NIST CSF 1.1 [4]、ISO/IEC 27001:2022 进行多维度对比，结果如下表 1 所示：

Table 1. Comparative analysis of mainstream CII protection frameworks
表 1. 主流 CII 防护框架对比分析

对比维度	NIST CSF 1.1 [4]	ISO/IEC 27001:2022	本文“四横一纵”框架
核心定位	通用网络安全风险管理框架	信息安全管理体系标准	民航气象专属韧性防御体系
适用范围	全行业通用 CII	各类组织信息安全管理	民航气象观测、预报、数据传输全业务链
战略治理层	仅提及高层治理原则	强调管理体系认证要求	明确运营主体责任、动态 CII 管理、资源保障与问责机制
业务融合度	弱，需自行适配业务流程	中等，侧重流程合规	强，深度融合民航气象分钟级决策、实时观测等核心业务特性
特殊风险覆盖	未覆盖行业专属风险	未覆盖行业专属风险	重点覆盖老旧设备入网、气象数据跨境、空域敏感数据、极端天气业务连续性等民航气象特有风险
实施复杂度	中等，需大量定制化工作	高，认证流程繁琐	低，提供场景化微解决方案与标准化工具包
韧性能力	仅包含基础恢复能力	未系统覆盖韧性建设	构建“识别－防护－检测－响应－恢复－适应”全周期韧性防御能力
监管适配性	适配美国监管要求	适配国际通用认证要求	完全适配中国《中华人民共和国网络安全法》[1]《关键信息基础设施安全保护条例》[2]及民航行业监管要求

通过对比可见，本文框架在行业针对性、业务融合度和特殊风险覆盖方面具有显著优势，解决了通用框架在民航气象领域“水土不服”的问题，实现了从“合规导向”向“风险导向和业务导向”的转变。

2.2. 研究内容与方法

本文主要研究内容为：

风险识别：利用民航事故征候的分析和预测内容[7]，分析安全风险复盘、气象威胁预警规则提炼、气象服务产品优化、不安全事件诱因等系统性问题，结合国内多起气象相关航空不安全事件[8]，建立威胁映射模型；

防护体系设计：在国家等级保护 2.0 框架基础上，根据民航气象业务特性需求，提出四横一纵防御框架；

实施方案制定：依据 CAAC-MD 设备准入规范[9]，制定老旧设备入网安全条款及跨机构数据安全交换方案。

试点验证：选取民航西南地区空管局气象数据中心开展实证研究，验证框架的有效性与可操作性。

主要研究方法有：

政策文本分析：分析民航安全通告文本中有关“气象”的关联事件，根据事件风险频率比例，来确定防护等级；

公开标准对比分析：对照《GB/T 22239-2019 信息安全技术网络安全等级保护基本要求》[10]，梳理行业安全保护需求与现场要求的差距，补充、完善防护体系建设；

司法案例反演：通过中国裁判文书网，检索有关气象类航空运输损害实践，提取其中关键的事故原因和关于气象责任的事件，根据查阅结果，反向推导完善防护标准及要求。

2.3. 风险“控制逻辑推导过程”

本研究遵循“风险识别－风险评估－防护目标确立－框架层面设计－具体控制措施选择”的完整逻辑链条，核心推导关系如下表 2 所示：

Table 2. Civil aviation meteorology CII risk-control mapping table
表 2. 民航气象 CII 风险－控制映射表

风险类别	核心风险点	防护目标	对应框架层面	关键控制措施
老旧设备风险	硬件老化、无安全补丁、协议明文传输	降低老旧系统被攻击概率，实现安全隔离	技术防护层 + 运行保障层	网络分区隔离、轻量级加密、白名单控制、定期漏洞扫描
数据安全风险	敏感数据泄露、篡改、丢失	保障数据机密性、完整性、可用性	技术防护层(数据安全)	数据分类分级、国密算法加密、3-2-1 备份策略、全生命周期审计
业务连续性风险	单点故障、极端天气、网络攻击	核心业务 RTO < 15 分钟，RPO < 5 分钟	运行保障层 + 技术防护层	双活数据中心、负载均衡集群、异地容灾、常态化演练
供应链风险	设备后门、软件漏洞、远程维护失控	管控全供应链安全风险	战略治理层 + 风险管理层	供应商准入评估、合同安全条款、远程运维审计
管理风险	责任不清、人员意识不足、制度缺失	实现安全管理规范化、责任具象化	战略治理层 + 管理保障	AB 角配置、KPI 一票否决、分层培训、制度体系建设

3. 民航气象关键信息基础设施面临的安全风险与挑战

3.1. 威胁来源分析

网络攻击：APT 攻击——目标窃取敏感预报数据或破坏系统、供应链攻击——设备/软件后门、勒索软件、DDoS、内部威胁——权限滥用/误操作。

自然灾害与物理破坏：极端天气损坏、火灾、人为破坏。

系统故障与人为失误：硬件老化故障(如雷达组件)、软件缺陷、配置错误、操作失误(如误删数据)。

数据安全风险：泄露(危及国安/商业)、篡改(引决策错误)、丢失(影响连续性)、跨境合规挑战[11]。

3.2. 脆弱性分析

系统高度复杂，被攻击面大；业务实时性要求极高，容错空间极小；严重依赖外部公网、电力、外部数据源；中心与边缘、新老系统差距大致防护水平不平衡；老旧系统更新困难，遗留较多风险[12]；相关人员安全意识与技能不足；法规标准落地难、适配性有待提升。

3.3. 潜在影响分析

最核心影响是直接威胁航空运行安全(错误/缺失气象信息导致灾难性决策，如 CFIT)和危及国家安全(敏感数据泄露用于非民用目的，系统被控干扰空域管理)。其次将造成重大经济损失(航班混乱)、损害行业声誉、并可能削弱公共气象预警能力。

4. 民航气象关键信息基础设施安全防护体系构建

民航气象关键信息基础设施(CII)的安全防护，是保障国家空天安全、飞行安全和公共安全的基石。面对复杂严峻的安全形势，必须构建一套深度融合民航气象业务特性、具备前瞻性与实战性的防护体系。

基于多年研究和行业实践，提出以下体系化防护方案。

4.1. 防护目标与原则

防护目标：确保气象观测、数据处理等持续不中断运行；维护民航气象数据的机密性(Confidentiality)、完整性(Integrity)、可用性(Availability)；增强系统受创后快速检测、响应、恢复和适应能力，降低安全事件影响范围和持续时间。

防护原则：严格遵循《中华人民共和国网络安全法》[1]、《中华人民共和国数据安全法》[11]、《关键信息基础设施安全保护条例》[2]及民航、气象行业相关法规标准；以常态化风险评估为基础，识别威胁，指导资源投入和防护策略制定；实施分区分级防护措施；构建多层次、相互协同的防护体系；优先保障核心气象业务不间断运行；运营者、管理者、使用者、供应商等多方责任共担；建立安全防护效果的监测、评估、反馈与优化机制，持续改进。

4.2. 防护体系总体框架设计

针对民航气象 CII 高度复杂、实时性强、依赖广泛的特点，提出“四横一纵”防御框架(见图 1)：

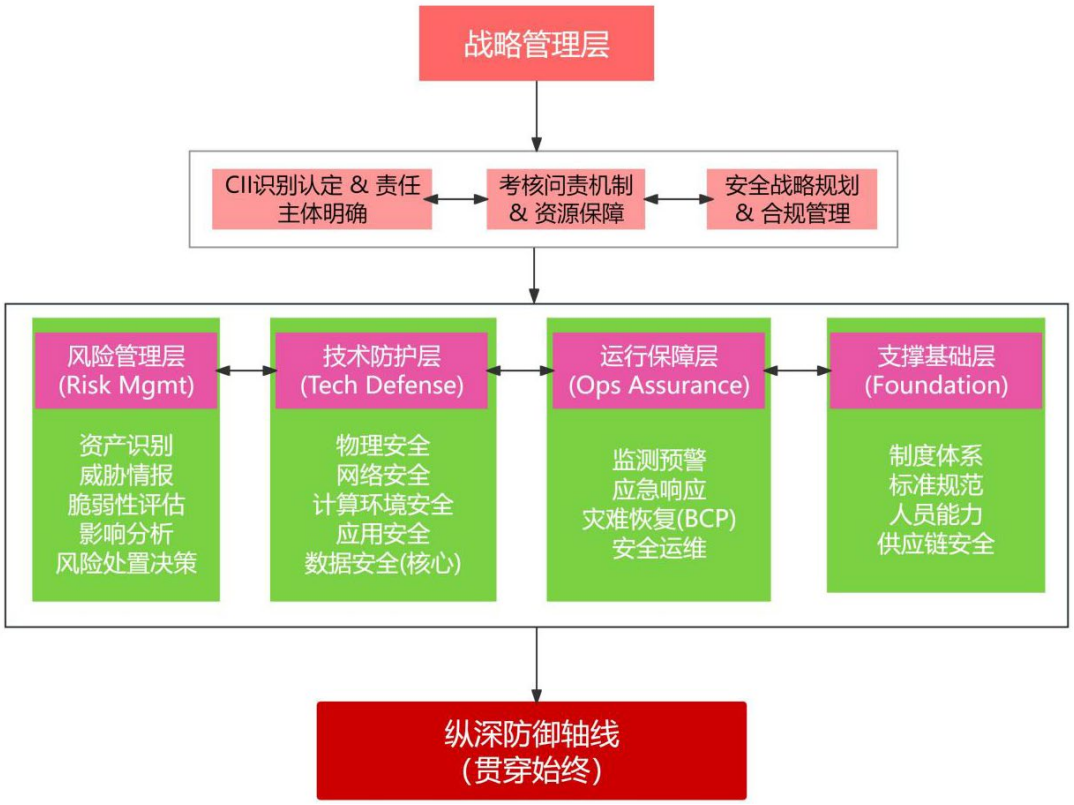

Figure 1. Four-vertical-columns-and-one-horizontal-base defense framework
图 1. 四纵一横防御框架

战略治理层：明确运营主体的责任，建立 CII 动态管理机制。制定中长期安全规划，确保合规性的要求能有效融入民航领域业务流程。建立严格的问责制与资源投入保障机制，为体系运行提供指引和保障。

风险管理层：建立常态化、场景化风险评估机制。重点评估供应链风险、数据跨境风险、老旧系统风险等民航气象痛点。风险评估结果直接反馈，推进技术防护、运行保障策略的制定与优化，是资源分

配的核心依据。

技术防护层：基于纵深防御理念[13]，建立涵盖物理环境、网络通信、区域边界、计算环境(主机/终端)、应用系统、数据全生命周期的多维技术防护体系。需紧密结合民航气象特点进行强化。

运行保障层：聚焦安全事件监测预警、应急响应、恢复改进。建立统一安全态势感知平台(SOC)，实现威胁可视化。制定应急预案(IRP)和灾难恢复计划(DRP)，定期实战化演练。强化日常安全运维(配置、补丁、变更管理)的规范化。

支撑基础层：提供体系持续运行的底层支撑。建立健全覆盖各环节的安全管理制度与流程。制定符合民航气象业务特性的安全技术与管理标准规范。通过分层次、常态化的安全意识教育、专业技能培训和攻防演练，提升全员安全能力。实施严格的供应商准入评估、持续监控和合同安全条款约束，管控供应链风险。

纵深防御轴(融合贯通)：强调上述四层之间不是割裂的，而是通过信息共享、策略联动、能力协同，形成纵向贯通的整体防御能力。

该框架强调风险驱动、技术与管理并重、平战结合、全员参与、持续演进，旨在为民航气象 CII 构建具备识别、防护、检测、响应、恢复五大核心能力的韧性防御体系[14]。

4.3. 关键防护措施与技术应用

4.3.1. 物理安全

应核心防护的国家级中心、区域中心及重要机场气象台机房等设施，需满足 GB/T 22239-2019 等保三级物理安全要求(门禁、监控、防入侵、防火、防水、防雷) [10]；

无人值守台站的偏远自动气象站、雷达站采用加固机箱、环境监控(温湿度、水浸、烟雾)、太阳能+大容量蓄电池双备份供电，并确保通信链路冗余；

核心节点必须配置双路市电+智能 UPS+柴油发电机，确保极端天气下持续供电。

4.3.2. 网络安全

划分核心生产网、管理网等，区域间部署防火墙并启用强访问控制策略；在网络接入点部署下一代防火墙(NGFW)、入侵防御系统(IPS)、抗 DDoS 设备，关键链路采用 IPSec VPN 或专用加密链路；部署网络准入控制(NAC)确保接入终端合规，实施网络流量分析(NTA)检测异常内部通信和横向移动，加强网络操作审计。

4.3.3. 计算环境安全

对主机实施严格安全基线配置、主机入侵防御(HIPS)、文件完整性监控(FIM)，统一部署终端安全管理平台，实现恶意代码防护(EPP/EDR)、外设管控、补丁集中分发与强制更新(尤其针对气象专用软件配套系统)，建立覆盖气象业务系统、操作系统、中间件、数据库的主动扫描、快速评估、分级修复、验证闭环流程，优先处置高危漏洞。

4.3.4. 应用安全

将安全需求、威胁建模、安全编码(避免缓冲区溢出等常见气象软件漏洞)、代码审计(SAST/DAST)、安全测试嵌入气象业务应用(如预报平台、情报发布系统)的开发、迭代流程。面向互联网或外部用户的应用(如航班气象查询服务)部署 Web 应用防火墙(WAF)防御注入、跨站脚本(XSS)等攻击。核心业务系统执行基于角色的访问控制(RBAC)，对预报员、管理员等关键岗位操作启用多因素认证(MFA)，严格控制 API 接口权限并加强审计。

4.3.5. 数据安全

制定《民航气象数据分类分级指南》，参考《气象大数据分类分级白皮书(2023 版)》[15]，界定核心

敏感数据(如涉及国防/关键空域的高精度探测数据、未公开数值模式核心参数、特定时期历史数据)的标识、存储、传输、使用要求。对核心敏感数据(如：涉及国防或关键空域的高精度风切变探测原始数据、未公开的数值天气预报模式核心物理参数及同化方案、特定敏感时期的历史航空气象数据集)及备份数据，在数据库层或存储层采用国密算法(如 SM4) [16]或 AES 进行静态加密，内部网络间数据传输使用 TLS 1.3+，与外部机构(如航空公司签派、空管)交换数据必须通过 VPN 或专线 + 强加密，观测站至中心数据传输采用 DTLS 或其他适合物联网的轻量加密协议[17]。在开发测试、对外合作等非必要场景，对包含敏感信息的气象数据进行可靠的脱敏处理。实施“3-2-1”备份策略(3 份拷贝，2 种介质，1 份异地) [18]，核心业务数据采用实时/近实时复制技术至异地容灾中心，定期验证备份数据的完整性和恢复流程(RTO/RPO 达标验证)。基于数据分类分级实施精细的访问控制策略，对所有核心敏感数据的访问、修改、删除操作进行详细日志记录并集中审计分析。严格遵守国家数据出境安全评估办法，国际航班所需气象情报需通过安全评估或认证[11]。

4.3.6. 监测预警与响应

构建民航气象 SOC(整合关键数据日志，进行关联分析，建立针对各类威胁的专属检测规则)；接入行业、国家级威胁情报源，提升预警能力(TIP)，探索自动化响应(SOAR)。

4.3.7. 业务连续性管理

高可用架构：核心系统(如气象数据库、情报分发网关)采用负载均衡集群、双活/多活数据中心架构，消除单点故障；

容灾体系建设：建立符合民航气象业务 RTO/RPO 要求的异地容灾备份中心。参考 ISO 22301:2019 标准[8]，容灾方案需覆盖基础设施、数据、应用各层面；

常态化演练：制定涵盖网络攻击、系统故障、自然灾害等多种场景的应急切换和灾难恢复演练计划，定期实战化演练，验证预案并持续改进。

4.3.8. 新技术应用考量

云计算安全：云服务需明确责任共担模型。保障气象数据在云上存储、处理、传输的安全(加密、密钥管理、访问控制)；

零信任：在新建系统或特定场景(如远程运维、第三方访问)试点“永不信任，持续验证”的零信任模型；

人工智能(AI)应用：探索 AI 在安全日志分析(异常检测)、威胁狩猎、攻击模式预测中的潜力，警惕 AI 模型本身被投毒(Poisoning)、对抗样本攻击或用于制造深度伪造气象信息的风险。

4.4. 管理保障措施

建立覆盖 CII 全生命周期的核心制度：包括“民航气象 CII 识别认定管理办法”“供应链安全管理办法”“安全运维操作规程”“网络安全事件应急预案”。

压实安全责任：明确运营单位主要负责人为网络安全第一责任人。设立专职首席安全官(CSO)或网络安全负责人。IT 部门、气象业务部门、安全管理部门、供应商等各方职责，纳入绩效考核。关键岗位实施 AB 角配置制度，即对安全运维、数据管理、系统管理员等核心岗位，设置两名具备同等资质和能力的人员，A 角为主要负责人，B 角为备份负责人。AB 角需定期进行岗位轮换(每 6 个月一次)，共同参与安全培训和应急演练，确保任何一方离岗时，另一方能够无缝接管全部工作。同时，AB 角人员均需通过严格的背景审查，签订保密协议和安全责任书。实施场景示例：当 A 角因休假、出差等原因无法履职时，B 角自动接替其负责的漏洞修复、应急响应等工作，交接过程需形成书面记录并由部门负责人签字确认，

确保工作连续性和责任可追溯。

强化人员能力：针对不同岗位(领导、管理、技术、业务)开展定制化的、常态化的网络安全意识教育；对网络安全管理员、系统运维员、气象业务骨干(预报员、观测员)进行分层次、实战化的专业技能培训，培养和引进“气象 + 网络安全”复合型人才；定期组织内部演练，参与行业攻防演练，检验防御体系有效性，提升实战能力。

严控供应链风险：建立供应商准入安全能力评估标准；在采购合同中明确安全责任条款；对采购产品进行安全测试和配置核查。对供应商提供的远程维护进行严格监控和审计。

审计与持续改进：定期开展内部审计和接受监管检查，建立管理评审机制，持续优化防护策略、技术措施和管理流程。建立微解决方案库，针对基层单位普遍面临的技术能力不足、资源有限的问题，提炼形成三类可直接复制的“微解决方案”：1) 老旧设备加固微方案：包含网络隔离配置模板、白名单规则、轻量级加密工具及操作手册，适用于无法升级的老旧雷达、自动气象站；2) 数据安全上传微方案：提供标准化的数据加密传输接口、脱敏规则和审计日志模板，解决基层台站与中心的数据安全交换问题；3) SIGMET 防篡改微方案：通过数字签名和哈希校验技术，确保重要气象情报在传输和发布过程中的完整性。微解决方案库采用在线更新模式，定期补充新的场景和工具，基层单位可根据自身需求一键下载部署，无需复杂的二次开发。

构建民航气象关键信息基础设施的安全防护体系，是一项融合技术、管理、法规、人才的系统性工程。本文提出的“四横一纵”防御框架及配套措施，旨在为行业提供一条贴合业务实际、具备可操作性的防护路径。其核心在于：以风险管理为驱动，以数据安全为重心，以业务连续为底线，以纵深防御为手段，以全员能力为支撑，以持续改进为保障。

4.5. 实证案例分析

民航西南地区空管局气象数据中心承担着西南地区所有民航机场的气象数据汇聚、处理、存储和分发任务，核心系统包括气象数据库集群、数值预报系统、情报分发网关等，日均处理数据量超过 5TB。2022 年之前，该中心存在以下突出安全问题：1) 老旧设备占比达 42%，其中 12 台服务器运行已超过 8 年，无厂商技术支持和安全补丁；2) 数据传输未全面加密，部分自动气象站采用明文协议传输数据；3) 缺乏统一的安全态势感知平台，威胁检测依赖人工分析；4) 备份体系不完善，仅实现本地备份，无异地容灾能力；5) 安全管理制度不健全，关键岗位未实现 AB 角配置。

2024 年，民航气象信息共享与服务系统上线，全面应用本文总提出的“四横一纵”防御框架。完成网络分区改造，划分核心生产区、数据存储区、管理区和外部接入区，部署 NGFW、IPS、NAC 等安全设备；对核心敏感数据采用 SM4 算法进行静态加密，数据传输启用 TLS 1.3 协议；建设统一安全态势感知平台，接入 12 类安全设备日志；按照“3-2-1”策略搭建异地容灾备份系统，实现核心数据实时同步至成都异地容灾中心。

通过新系统的上线，西南空管局气象中心的安全防护能力得到显著提升。此外，通过红蓝对抗测试验证，该中心成功抵御了模拟的勒索软件攻击、DDoS 攻击和老旧设备漏洞利用攻击，未出现核心业务中断和数据泄露情况。该案例充分证明了本文提出的防护框架在实际应用中的有效性和可操作性。

5. 安全保护的实施路径与建议

5.1. 运营者主体责任落实路径

针对国家级气象中心、区域中心及大型枢纽机场气象部门设立专职网络安全管理部门，中小机场气象台明确专职安全管理员，关键岗位(如安全运维、数据管理)实施 AB 角配置并且进行背景审查。建立年

度评估+重大变更触发的 CII 识别更新流程，制定报备安全保护计划，涵盖技术升级、演练预算、人才梯队建设等内容，报民航主管部门备案。设立网络安全专项预算(不低于信息化投入的 15%)，将 CII 安全目标纳入部门及个人 KPI 考核，对重大隐患整改不力、违规操作导致事件的责任人实行“一票否决”。

5.2. 监管与协同机制建设

呼吁民航局将 CII 安全防护有效性纳入年度安全审计，开展“双随机一公开”渗透测试，对未落实防护要求的单位依法问责；由民航局主导搭建民航气象威胁情报共享平台，制定“民航气象安全事件分级通报规范”，实现分钟级行业联动；深化跨国家网信部门、公安部、密码管理局等多部门的协同管理；推动设立民航气象 CII 安全验证平台，模拟典型业务场景，开展设备入网前安全测试、防护方案有效性验证及红蓝对抗演练。

5.3. 技术能力与人才队伍建设

设立民航气象安全专项科研基金，重点支持轻量级加密技术(如无人气象站的应用)、气象数据篡改溯源技术、航空专用协议安全增强方案。

推动高校设立交叉学科及课程，联合相关高校开设定向培养项目；引导企业建立“气象工程师－安全工程师”双导师制，通过岗位轮换培养实战能力；设立网络安全特殊津贴吸引高端人才，开展气象护网行动攻防演练，定期举办行业网络安全技能竞赛。

5.4. 标准规范与最佳实践推广

推广开发“民航气象 CII 安全自查清单”类轻量化工具，提供 Excel 自动化检查表，包含数据安全，系统防护，应急准备。

场景化最佳实践包(老旧加固/数据上传/SIGMET 防篡改的“微方案”)，提炼三类基层可直接复制的“微解决方案”，建立民航气象安全互助机制，开通“民航气象安全能力微课”平台，建立学分累计制度，学习记录纳入安全绩效考核。

6. 结论与展望

6.1. 主要研究结论

本研究系统界定民航气象 CII 范围与核心风险特征，揭示了其高价值、高实时、高依赖、弱防护的严峻挑战。创新性提出“战略治理－风险管理－技术防御－运行保障”四维一体的韧性防护框架，实现从单点防护到体系免疫、被动响应到主动防御、静态合规到动态韧性的跃迁。提出责任具象化、能力轻量化、标准场景化的精准实施路径。研究成果试点验证有效，显著提升了防护效能。

6.2. 研究不足与未来展望

本研究未能建立气象业务中断损失的量化映射模型，未展开模拟量子计算对气象加密数据的威胁路径，未能突破零信任架构在航空气象专网(AFTN)的部署。

未来研究与实践方向：

新技术融合应用：研发民航气象 AI 安全代理，实时识别虚假气象情报生成攻击(如深度伪造的雷暴预警)；预测供应链攻击路径(基于气象设备漏洞知识图谱)。建立平行仿真系统，在数字孪生环境中预演台风期间黑客协同攻击场景。在新建系统或特定场景(如远程运维、第三方访问)全面试点“永不信任，持续验证”的零信任模型[17]，探索零信任架构在 AFTN 专网的部署方案。规范云计算在民航气象领域的应用，明确云服务责任共担模型，保障气象数据在云上的全生命周期安全。

量子安全战略布局：抢占量子安全战略高地，先行部署民航气象后量子密码(PQC)试验网，重点保护数值预报核心参数(如 ECMWF 交换数据)；研发量子密钥分发(QKD)气象专线(如北京－浦东－法兰克福航路)，构建抗量子攻击的气象数据加密传输体系。

标准体系与国际合作：建立弹性认证体系，推动民航气象安全成熟度模型(CAAC-SMM)成为国际标准，输出“中国方案”。深化与 ICAO [5]、FAA [6]等国际组织的合作，推动建立跨境气象安全互认机制，率先在中欧航线开展试点。

安全能力服务化：期望最终通过“安全即服务”(Security-as-a-Service)模式，使气象安全能力如同航空气象情报般实时可获取，支撑全球民航业应对气候危机与数字威胁的双重挑战。

参考文献

[1] 中华人民共和国网络安全法[EB/OL]. https://www.cac.gov.cn/2025-12/29/c_1768735112911946.htm, 2016-11-07.

[2] 关键信息基础设施安全保护条例[EB/OL]. https://www.gov.cn/gongbao/content/2021/content_5636138.htm, 2021-07-30.

[3] 中国民用航空局. 民航安全事件统计分析报告(2019-2023 年) [R]. 北京: 中国民航出版社, 2023.

[4] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). National Institute of Standards and Technology.

[5] International Civil Aviation Organization (2023) Annex 3: Meteorological Service for International Air Navigation (20th Edition). ICAO Publishing.

[6] Federal Aviation Administration (2021) Aviation Weather Information Security Best Practices. Federal Aviation Administration.

[7] 王永刚, 吕学梅. 民航事故征候的关联度分析和灰色模型预测[J]. 安全与环境学报, 2006, 6(6): 127-130.

[8] 岳仁田, 赵嶷飞. 基于 HFACS 的民航气象诱发不安全事件致因分析[J]. 中国安全科学学报, 2022, 32(7): 142-149.

[9] 中国民用航空局. CAAC-MD-2020-01 民用航空信息系统安全保护等级定级指南[C]//民航行业标准汇编. 北京: 中国民航出版社, 2020: 15-28.

[10] 全国信息安全标准化技术委员会. GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求[S]. 北京: 中国标准出版社, 2019.

[11] 中华人民共和国数据安全法[EB/OL]. https://www.cac.gov.cn/2021-06/11/c_1624994566919140.htm, 2021-06-10.

[12] 王明清, 张爱英, 等. 计算机网络安全风险与防范策略分析[J]. 网络安全技术与应用, 2023(2): 159-161.

[13] 庞彬彬. 民航机场关键信息基础设施网络安全保障体系研究[J]. 网络安全与数据治理, 2022, 41(12): 25-33.

[14] 杨乐, 朱国栋, 陈福康. 基于网络安全域的民航气象信息服务系统设计[J]. 民航管理, 2019(6): 72-74.

[15] 国家气象信息中心. 气象大数据分类分级白皮书(2023 版) [R]. 北京: 气象出版社, 2023.

[16] 国家密码管理局. GM/T 0002-2012 SM4 分组密码算法[S]. 北京: 中国标准出版社, 2012.

[17] 于佳佳, 王亮. 零信任架构在空管办公网络的应用研究与实践[J]. 成都信息工程大学学报, 2025, 40(6): 787-793.

[18] Preston, W. (2007) Backup & Recovery: Inexpensive Backup Solutions for Open Systems. O’Reilly Media, 73-75.