Computer Science and Application 计算机科学与应用, 2023, 13(12), 2324-2332
Published Online December 2023 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2023.1312232

Hans汉斯

地市级气象信息网络安全架构标准化设计研究

姜　慧，李　博，程　铭

菏泽市气象局，山东　菏泽

收稿日期：2023年11月22日；录用日期：2023年12月19日；发布日期：2023年12月27日

摘　要

为贯彻落实《网络安全法》，推进气象信息现代化建设进程，解决地市级气象部门网络安全建设没有统一标准的问题，对地市级气象信息网络安全的标准化架构进行设计研究。基于网络安全等级保护2.0标准核心内容，结合地市级网络安全现状，对气象信息网络安全架构的基本要求、安全保障体系以及等保2.0生命周期流程进行深入探讨，探索网络安全等级保护2.0在地市级气象信息网络中的应用方法，设计符合网络安全等级保护2.0标准的地市级网络安全标准化架构解决方案；为地市级气象部门信息网络安全建设提供指导和参考作用，全面提升气象信息化安全防护能力和管理水平，保障气象事业快速稳定发展。

关键词

网络安全，等级保护2.0，访问控制，态势感知

Research on Standardized Design of Meteorological Information Network Security Architecture at the Prefecture Level

Hui Jiang, Bo Li, Ming Cheng

Heze Meteorological Bureau, Heze Shandong

Received: Nov. 22nd, 2023; accepted: Dec. 19th, 2023; published: Dec. 27th, 2023

Abstract

In order to implement the Cybersecurity Law, promote the modernization of meteorological information construction, and solve the problem of lack of unified standards for network security construction of meteorological departments at the prefecture and city levels, a standardized architecture for network security of meteorological information at the prefecture and city levels is designed and studied. Based on the core content of the Network Security Level Protection 2.0

文章引用: 姜慧, 李博, 程铭. 地市级气象信息网络安全架构标准化设计研究[J]. 计算机科学与应用, 2023, 13(12): 2324-2332. DOI: 10.12677/csa.2023.1312232

standard and combined with the current situation of network security at the prefecture level, this paper deeply explores the basic requirements, security guarantee system, and equal protection 2.0 lifecycle process of meteorological information network security architecture, explores the application methods of Network Security Level Protection 2.0 in prefecture level meteorological information networks, and designs a standardized architecture solution for prefecture level network security that meets the Network Security Level Protection 2.0 standard to provide guidance and reference for the information network security construction of prefecture level meteorological departments, comprehensively improve the security protection and management capabilities of meteorological informatization, and ensure the rapid and stable development of meteorological undertakings.

Keywords

Network Security, Level Protection 2.0, Access Control, Situational Awareness

1. 引言

新型技术，如大数据、云计算、物联网、人工智能及移动互联网等，已迅速地融入气象业务技术中，进一步促进了气象事业的发展。随着各类信息技术不断的发展和提高，在气象网络现代化发展的过程中，增加了气象业务发展所面临的复杂环境，也时常面临各种网络安全问题[1]。在我国《网络安全法》的第二十一条中明确规定了“国家实行网络安全等级保护制度”。2019 年 12 月，网络安全等级保护 2.0 制度正式实施。中国气象局预报司于 2019 年、2021 年分别印发了《气象网络安全基础架构设计方案》、《中国气象局网络安全设计技术方案》，方案为国家级和省级节点提供了较为详细的安全设计和区域规划，指导和规范了全国各地气象部门网络安全技术的设计与建设，基本能够满足顶层的气象事业业务发展需求。在中国气象局统一的领导和要求下，国家和省级气象部门的网络安全技术和防护能力已得到了逐步的提高。然而，面对严峻的网络安全状况和新技术的持续出现，特别是在市、县级的气象部门，现有的技术防护已经不能满足气象事业对网络安全的需求[2]。在新的形势下，急需构建一套完善的气象信息网络安全架构体系，为地市级气象信息网络安全建设发展提供指导和参考，全面提高地市级气象信息化安全防护能力和管理水平，保障气象事业快速稳定的发展。

2. 主要研究内容

2.1. 网络安全分析

通过调研山东省其他地市网络安全建设，对网络安全现状进行分析和开展风险评估工作发现，近年来，地市级气象部门虽然已经建设了一批网络安全防护基础设施，部署了防火墙、上网行为管理，终端和服务器杀毒软件等网络安全软件和设备，具备基本的安全防护能力。但随着气象现代化进程的不断推进及网络安全已上升为国家战略，距离建设符合等级保护 2.0 要求的标准体系架构还有一定的差距，网络安全防护和基础保障体系不完善，主要存在以下问题：

(1) 网络病毒和非法入侵

气象网络信息安全最大的威胁是网络病毒和非法入侵。互联网病毒会通过气象网络信息系统存在的

安全缺口进行攻击，采取各种方法入侵和损害平台。早期，存在多个服务器被注入木马，并利用该服务器作为跳板对内部网络开展网络攻击，导致平台受到病毒的感染，影响了气象业务的正常操作，对业务信息网络的正常运行造成巨大的安全威胁，严重的可能引发网络全盘崩溃，给气象部门带来巨大的损害。

(2) 整体防御能力弱，风险感知能力差

由于地市级气象部门对网络安全建设没有统一的标准，自行开展网络安全的建设，导致其安全体系混乱、资源未能有效整合，防护能力分布不均，各种短板大量存在，整体的防御能力较弱，风险感知能力较差；网络安全设备分布零散，各个级别的气象部门之间信息交流不互通，网络设备、安全设备之间缺少联动响应机制，潜在风险的预警和监测能力薄弱[3]。随着网络安全工作领域的深度不断拓展，攻击方式越来越复杂，应对新的未知威胁防不胜防。气象部门的网络安全设备目前面临老旧，性能低下等问题，没有足够的经费去采购新的设备，无法起到有效抵御新型恶意软件和病毒的入侵的作用，网络安全基础保障体系建设还需要与时俱进，不断完善。

(3) 安全防护严重滞后，应用和数据安全薄弱

随着气象领域迅速应用推广了大数据、云计算、移动互联网等新技术，但相应的安全防护技术却严重滞后。在建设业务系统的过程中，对数据安全的重视程度不够，开发环节出现了大量关于插件、代码和数据库的安全漏洞问题。在业务应用方面，对各类数据的保护机制极为缺乏，缺乏针对性的授权管理、审计日志以及灾难恢复、数据备份等防护措施。

(4) 网络安全监管不足

信息安全管理工作存在监管不足的问题，缺少有效的监督，对网络安全管理的重视程度不够。网络安全管理和运维体系缺乏流程化、规范化。网络安全管理体系是网络安全体系的中枢，缺乏对气象网络安全建设和管理的规范指导，不能及时对标国家法律法规、技术标准规范、政策文件等，气象部门的网络安全管理规章制度无法及时优化完善，对气象数据的安全管理保护措施尚显不足。

2.2. 网络安全等级保护 2.0 标准新变化

网络安全等级保护 2.0 新标准实行“一个中心，三重防护”的防护理念和分类结构，深化了建立纵深防御和精细防御体系的思想[4] [5] [6]。“一个中心，三重防护”是指即一个管理中心，通过对区域边界防护、通信网络防护、计算环境防护的统一管理，持续提升网络安全防护能力。伴随新技术的快速发展，满足等级保护 2.0 防护能力的建设范畴也在不断精细。新的标准提出了更加明确、全方位的建设和防护指导。网络安全等级保护 2.0 着重强调要实现主动防御、风险监测和预警能力等多项内容。相比等级保护 1.0 制度，等级保护 2.0 在许多内容方面做了修改调整，主要围绕以下几个方面：

(1) 名称发生改变

网络安全等级保护 2.0 将《信息系统安全等级保护基本要求》修改成《网络安全等级保护基本要求》，明确地凸显了网络安全的关键性。网络安全的范围并不仅仅局限于信息系统的安全，也包含像物联网系统、大数据平台系统等其他方面。

(2) 等级保护对象的变化

等级保护 1.0 定义的等级保护对象是具体的信息及信息系统。由于云计算平台、物联网、工业控制系统、大数据等新兴领域的保护目标不断涌现，这个定义的局限性愈发突出。相较之下，等级保护 2.0 新标准将对象范围从过去的信息系统拓宽到：基础网络设施、云计算、大数据、物联网、工业控制系统，以及采用互联技术的系统等[7]。

(3) 原有安全要求内容的结构变化

原有安全要求内容的结构发生了变化，引进了新的要求适用于新的技术和应用领域。如云计算、移

动互联、物联网、工业控制系统及大数据等，从而构建了安全通用要求和新应用安全扩展要求的标准规定内容。通过细化安全要求划分，可以让技术标准的实施更为详细、精确，使得网络安全建设的目标更加清晰。

(4) 新增四个安全扩展要求

等保 2.0 新增加了四个扩展要求，分别是：云计算、移动互联、物联网和工业控制系统的安全扩展要求。值得重视的是，云计算和物联网这两个部分的扩展要求与气象信息系统的安全建设工作紧密相连，具有极其重要的指导作用。

(5) 安全通用要求中的控制项和控制节点变化

技术层面，包括从物理环境安全要求到通信环境的安全要求。于此同时，对计算环境、网络区域的边界以及安全管理中心等方面的安全也有专门的技术规定。在管理层面，构建安全管理制度、管理机构、管理人员、安全建设与运营管理等多方面的安全管理体系。

(6) 保障思路发生变化

网络安全等级保护 2.0 采用了更加完善的安全防护体系思路，涵盖网络安全事件前、事件中、事件后的安全防护策略，当出现网络问题后，能及时进行溯源分析。保障思路上，由等级保护制度 1.0 的被动防御审计，演变到等级保护 2.0 的积极防御，包含安全检测、预警感知、动态防护和应急响应等方面的主动保障。

3. 气象信息网络安全方案总体设计

3.1. 气象信息网络安全基本要求

气象信息网络安全的基本要求，从结构和分类调整，横向分成两大要求，即安全技术要求和安全管理要求。纵向划分为三种，即：安全控制类、安全控制点以及安全要求项，见图 1 所示；

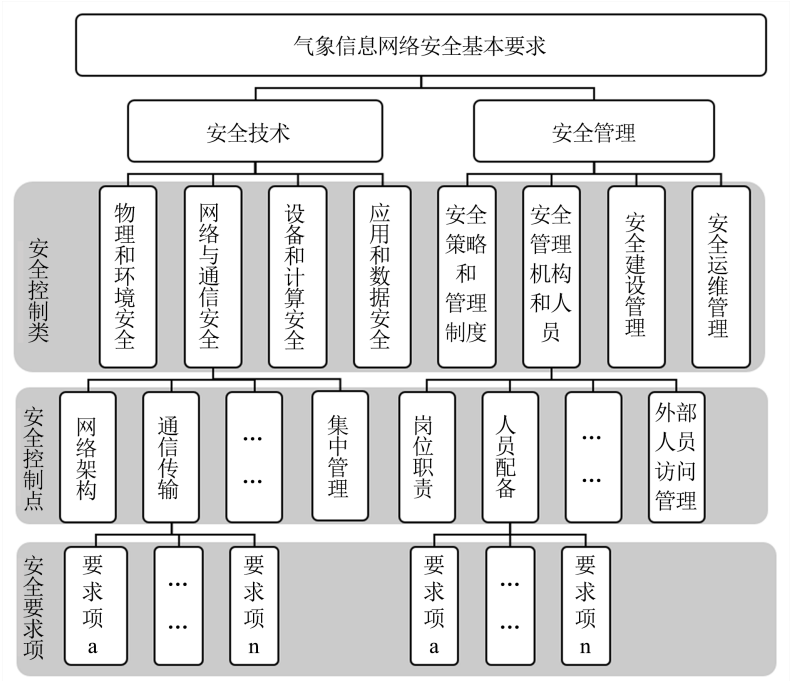

Figure 1. Basic requirements for meteorological information network security
图 1. 气象信息网络安全基本要求

(1) 安全技术控制类：物理和环境安全、网络与通信安全、设备和计算安全、应用和数据安全。

(2) 安全管理控制类：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。

以网络和通信安全在控制点的要求作为示例，对符合备案要求的各级气象业务系统、气象基础网络系统或气象云在控制点的要求可以参考表 1。

Table 1. Requirements for network and communication security control points
表 1. 网络与通信安全控制点要求

安全控制点	第一级	第二级	第三级
网络架构	✓	✓	✓
通信传输	✓	✓	✓
边界防护	✓	✓	✓
访问控制	✓	✓	✓
入侵防范		✓	✓
安全审计		✓	✓
恶意代码防范			✓
集中管控			✓

3.2. 安全保障体系设计

气象信息网络安全保障体系被分为安全管理体系、通用安全技术体系及安全运营体系三大体系。安全管理体系可以进一步分为：安全策略和管理制度，安全管理组织和人员，安全建设管理、安全运维管理。通用安全技术体系涵盖：应用与数据安全、设备和计算安全、网络和通信安全、物理和环境安全。安全运营体系包括：资产梳理分析，安全风险发现，安全漏洞加固，安全分析处理和安全运营管理，如图 2 所示。

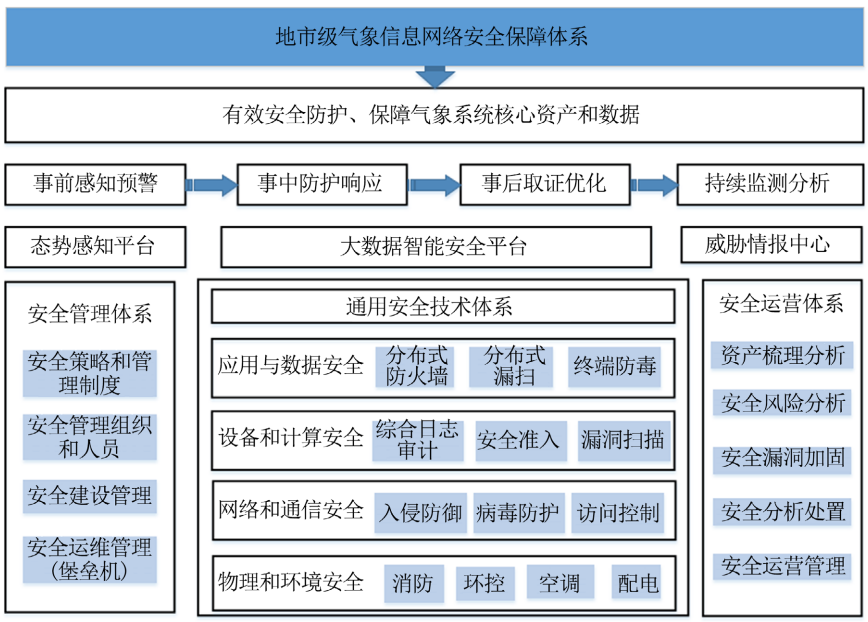

Figure 2. City level meteorological information network security guarantee system
图 2. 地市级气象信息网络安全保障体系

在通用安全技术防护体系中，在物理和环境安全的层面，机房所在的建筑物需要具有抗风暴、地震等自然灾害的能力。需要具备火灾自动检测设备、自动报警和灭火设备。要安装不间断电源 UPS、精密空调和动环监控系统。在网络和安全通信层面，要具备访问控制、入侵检测及防护病毒等方面的设备或措施。在设备和计算安全层面，接入网络的设备需要符合安全准入的策略，定期进行安全隐患排查并修复漏洞，同时接入日志审计设备，将日志留存半年以上。在应用和数据安全层面，需要配备防火墙、审计设备、漏洞扫描设备和终端防护软件。

3.3. 网络安全等级保护 2.0 生命周期

为保障气象信息系统、基础网络系统、气象云以及大数据平台的安全，一旦完成等级对象的建设，运营单位国家规定的测评机构，根据《网络安全等级保护测评要求》等国家相关技术标准，对确定等级对象的安全状况开展等级保护测评工作[8]。积极落实开展保护 2.0 测评工作，不只是为了满足相关法律法规的合规需求，更有助于全面提高气象网络安全防护能力，真正保障网络、数据以及业务安全。等保 2.0 的生命周期流程如图 3 所示，根据定级－备案－安全整改建设－等级测评－监督检查的流程开展等级保护相关工作。

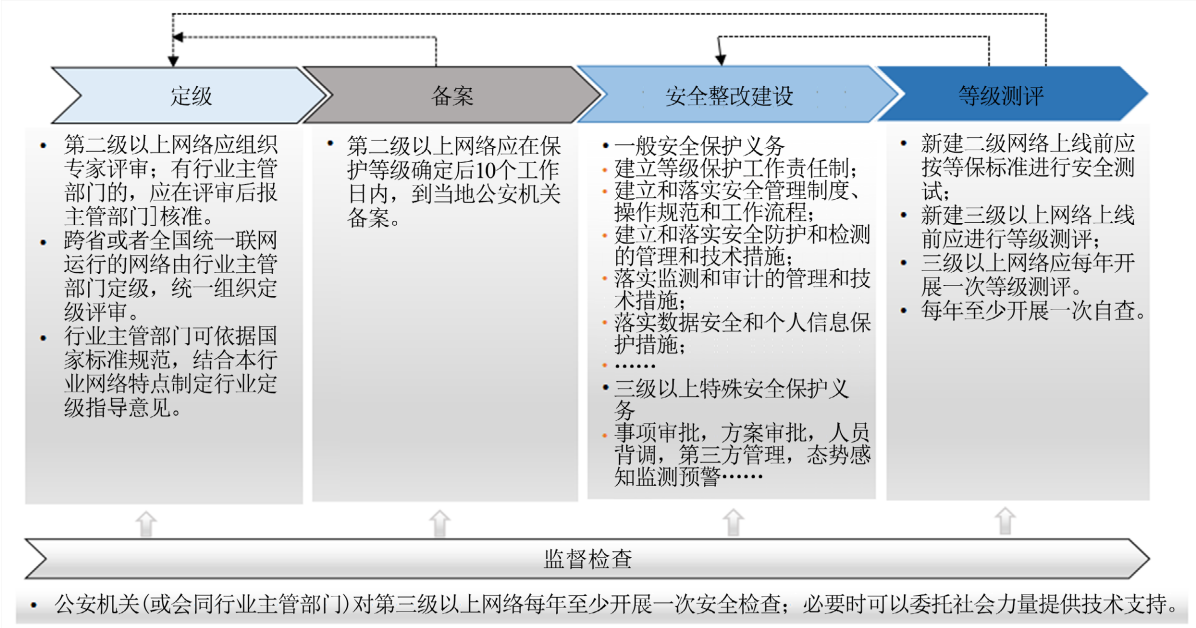

Figure 3. Life cycle process of equal protection 2.0
图 3. 等保 2.0 生命周期流程

(1) 定级备案流程：根据《信息系统安全等级保护定级指南》，对信息系统进行定级以后，填写定级备案表和定级报告，协助运行单位到其所在的公安机关完成备案手续。

(2) 建设整改流程：明确岗位职责，制定整改方案，执行技术策略，构建管理体系，整合网络安全产品，组织专家评审，落实安全建设方案，最后进行项目验收。

(3) 等级测评流程：准备测评所需的材料，配合测评公司现场测评，落实组织测评整改，开展等级测评，然后形成等级测评报告。

(4) 监督检查：作为运行单位的监管机构，承担信息系统网络安全情况的监督和指导的责任。需要公安、网信和行业主管部门共同配合，履行监督、管理职责，要求从技术能力与管理水平双向提升，以满

足在实施等保 2.0 的监管过程中的各项检查、处置、指导、协调、统筹等工作需求，有效帮助用户将等级保护纳入常态化工作。

4. 地市级气象信息网络安全架构设计

围绕“一个中心，三重防护”的网络安全等级保护 2.0 建设思路，针对包含信息系统、大数据云平台、基础网络系统、物联网等在内的全省气象部门网络系统，采用“功能划分”、“流量编排”等创新方式，融合新兴的网络安全产品和服务需求，将符合等保 2.0 新技术的新的气象系统平台，合理确定划分等级保护对象，将等保对象落实安全防护规划建设工作。基于地市级气象部门气象信息网络现状，依据《网络安全等级保护基本要求》和《网络安全等级保护测评要求》等国家标准以及行业内规范进行研究，设计满足等保 2.0 核心技术标准的网安全架构，图 4 为规划设计的地市级气象信息网络安全架构拓扑图。

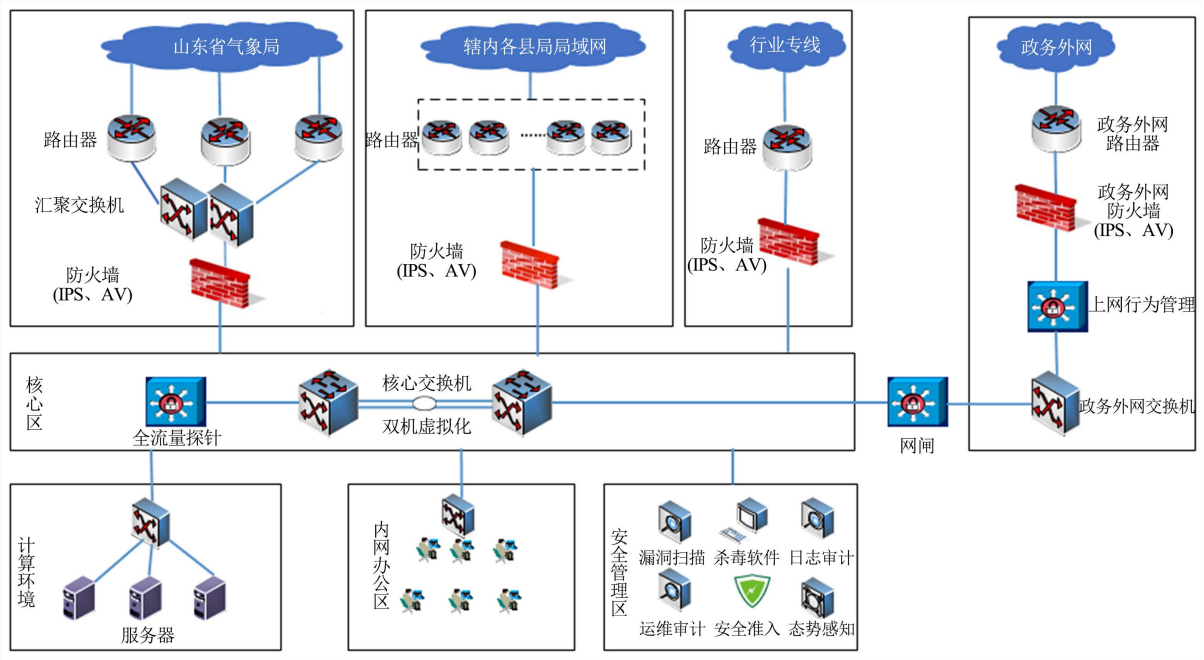

Figure 4. Topology diagram of meteorological information network security architecture at the prefecture level
图 4. 地市级气象信息网络安全架构拓扑图

首先，根据需求严格划分了内网与外网的区域边界。气象内网是通过专线连接省局内网，且通过网闸与政务外网相连。将网闸部署在业务内网和外网区域之间，可实现内网和外网之间有效的强逻辑隔离。一旦出现重大网络安全事件，可直接断开网闸，以确保内部网络环境的绝对安全性。此外，根据网络区域功能的特性划分网络区域边界，以满足等保 2.0 新安全标准的需求。在气象内部网络系统中，气实施分区分域，区域到边界以及不同区域之间实施安全防护控制措施。同时，针对业务服务器及重要业务系统平台，从横向和纵向加强网络安全防护，并着重强调物理环境安全，提升容灾备份能力。从区域划分、边界防护、纵深防御、提升容灾备份等方面，多角度地提高地市级气象信息网络安全防护能力和业务安全运行能力。

4.1. 边界防护区

通过防火墙、入侵检测系统等手段，形成一种气象网络安全的纵深体系。在网络边界区部署访问控

制、入侵防范等设备或措施，来保障气象内部的安全是安全防御必要的手段。在网络边界部署含 IPS、AV 功能的防火墙，同时需定期更新 IPS 特征库以及防病毒特征库。通过入侵防御(IPS)系统，对网络行为进行监控审计，及时发现网络风险并及时采取措施进行防护拦截。通过防病毒功能，实现对恶意代码的检测和清除，保护气象部门内部免收外网恶意流量和病毒的攻击。同时，根据实际业务需求，配置合理的访问控制策略，为系统提供访问控制功能。

4.2. 核心交换区

为了避免网络设备和线路出现单点故障问题，通过主、备线路，开通动态路由协议，设定路由优先级，上行连接省局，下行连接市局。核心交换机通过汇聚交换机上行连接省局路由器，下行连接业务区域、服务器区域、安全管理区域，作为网络架构的重要核心环节，应采用两台核心交换机基于虚拟化技术聚合。

4.3. 安全管理区

安全准入软件：以集中管理的形式对入网设备进行管控，同时阻止那些遵循既定安全策略的设备接入网络。

安全运维审计：记录信息系统运维人员对各类信息设备/系统的操作行为，方便对网络安全管理运维人员审计。

上网行为管理：通过对电脑终端的网络流量的控制和审查，可以约束部门内部员从事可限制内部员从事游戏、股票等非工作相关的活动。

综合日志审计：主要是通过一个集中日志审计平台，把气象部门内核心的网络设备、安全设备以及管理终端的日志，都收集到这个平台，保证能够全面管理及分析这些日志，并将相关日志留存 6 个月以上，网络管理员和安全管理员可以进行监控或查询。

奇安信态势感知系统：采用奇安信大数据安全分析系统，系统集检测、响应、风险预测和可视化功能为一体，可以为用户提供资产监测、业务监控、感知风险和威胁，并给予决策支持[9] [10]。

漏洞扫描：在关键业务区部署一套漏洞扫描系统，对气象内部重要业务系统和网络设备进行扫描，迅速发现并处理系统中存在的漏洞，及时排查安全隐患。

5. 总结

本文通过对地市级气象信息网络安全现状分析，研究了网络安全等级保护 2.0 标准核心内容，对地市级气象信息网络安全架构的基本要求，安全保障体系设计、等级保护 2.0 生命周期流程等方面开展研究，设计了符合等保 2.0 标准的地市级气象信息网络标准化结构解决方案。方案详细介绍了边界防护区、核心交换区、安全管理区的网络设备部署和具体功能。本架构适用于气象信息系统、基础信息网络、物联网、云平台和采用移动互联技术的网络等，可规范和指导地市级气象部门网络安全建设，提升地市级气象部门整体气象信息网络安全防护能力及管理水平，满足气象现代化发展需求，确保气象业务快速稳定发展。

基金项目

山东省气象局青年科研基金项目“地市级气象信息网络安全架构标准化设计研究”(2022SDQN20)。

参考文献

[1] 刘东君, 何恒宏, 谭震, 等. 气象网络安全治理体系研究[J]. 网络安全技术与应用, 2019(2): 90-92.

[2] 赵冰, 王旭, 贺永兴. 浅谈海南气象信息网络安全建设[J], 网络安全技术与应用, 2019(12): 134-136.

[3] 鲍磊磊, 吴锐涛, 姜淑杨. 地市级气象信息网络安全架构标准化设计研究[J]. 网络安全技术与应用, 2022(1): 103-105.

[4] 任婷, 于城. 从新技术角度谈等级保护 2.0 [J]. 信息通信技术, 2018, 12(6): 12-17.

[5] 李丹, 杨向东, 马卓元, 等. 等保 2.0 视域下的网络安全工作思考[J]. 网络安全技术与应用, 2019(10): 11-12.

[6] 何占博, 王颖, 刘军. 我国网络安全等级保护现状与 2.0 标准体系研究[J]. 信息技术与网络安全, 2019, 38(3): 9-14+19.

[7] 马力, 陈广勇, 祝国邦. 网络安全等级保护 2.0 国家标准解读[J]. 保密科学技术, 2019(7): 14-19.

[8] 陈澍, 李怀刚, 孟金. 等保 2.0 在山东省级气象网络安全中的应用[J]. 网络安全与技术应用, 2020(4): 108-109.

[9] 莫禹钧, 黄婕, 潘愈嘉. 基于网络安全态势感知的主动防御系统设计与实现[J]. 医学信息学杂社, 2020, 41(3): 60-63.

[10] 陈澍, 孟金, 冯勇, 等. 态势感知技术在省级气象网络安全防护中的应用[J]. 信息技术与信息化, 2020(10): 127-129.