环境信息安全保障体系研究：挑战、策略与未来展望

陈勇

潮州市环境信息中心，中国·广东 潮州 521000

摘要：随着全球数字化转型的加速与环境治理能力的现代化需求，环境信息已成为国家重要的战略资源和决策基础。环境信息安全作为非传统安全的重要组成部分，直接关系到生态环境监测的准确性、环境管理的有效性、公众知情权的保障乃至国家生态安全与社会稳定。本文旨在探讨环境信息安全的内涵与特殊性，深入分析当前环境信息安全面临的主要挑战与风险，并从技术、管理、法律三个维度构建一个综合性的环境信息安全保障体系。最后，结合新兴技术发展趋势，对未来环境信息安全的建设方向进行展望，以期为相关领域的实践提供理论参考。

关键词：环境信息；信息安全；保障体系；数据安全；物联网；云计算

Research on environmental Information Security Assurance System: Challenges, Strategies and Future Prospects

Chen Yong

Chaozhou Environmental Information Center, China Guangdong Chaozhou 521000

Abstract: With the acceleration of global digital transformation and the modernization demands for environmental governance capabilities, environmental information has become a vital strategic resource and decision-making foundation for nations. As a crucial component of non-traditional security, environmental information security directly impacts the accuracy of ecological monitoring, the effectiveness of environmental management, the protection of public right to know, as well as national ecological security and social stability. This paper explores the connotation and uniqueness of environmental information security, analyzes the primary challenges and risks currently faced in this field, and constructs a comprehensive security assurance system from three dimensions: technology, management, and law. Finally, by integrating emerging technological trends, it outlines future development directions for environmental information security, aiming to provide theoretical references for practical applications in related fields.

Keywords: Environmental information; Information security; Assurance system; Data security; Internet of things; Cloud computing

0 引言

环境信息，是指在环境管理、科学研究与公众服务过程中产生的，以数字化形式记录的，关于环境质量、污染源、生态状况、环保业务等各类数据、文本、图像、信号等内容的总称。其范围涵盖了大气、水、土壤、声、辐射等环境要素的监测数据，污染源在线监控数据，卫星遥感与无人机航拍数据，建设项目环评文件，环保法律法规与政策文书等。

在“数字中国”和“美丽中国”建设的大背景下，环境信息的价值日益凸显。首先，它是环境决策的“大脑”。基于海量、实时、准确的环境数据，管理者能够精准研判环境形势，预测污染趋势，科学制定减排策略和应急预案。其次，它是环境执法的“利齿”。通过在线监控、视频抓拍、大数据分析，能够实现对违法排污行为的非现场、精准化打击。再次，它是公众参与的“桥梁”。环境信息的依法公开保障了公民的知情权与监督权，是构建现代环境治

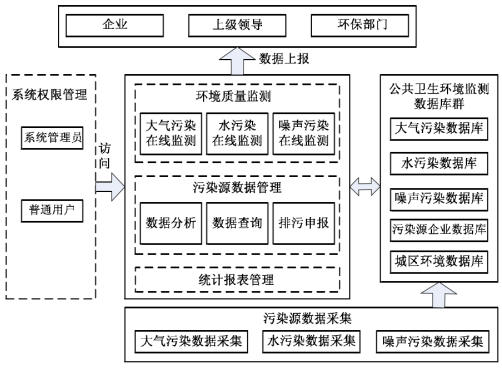

图1 环境监测信息系统

理体系的关键一环。

然而，环境信息系统通常具有部署环境复杂（如野外、污染企业现场）、接入设备繁多（海量物联网传感器）、网络边界模糊（依托互联网和政务外网）、数据敏感度高（部分涉及国家秘密或社会稳定）等特点，使其面临着严峻的信息安全威胁。一旦环境信息被篡改、破坏或泄露，可能导致灾难性后果：失真的监测数据会引发错误的决策，导致污染失控；被篡改的排污数据会使环境监管形同虚设；敏感地理信息泄露可能威胁国家生态安全；核心系统遭攻击瘫痪将直接影响环境应急响应能力。

因此，构建一个坚实可靠的环境信息安全保障体系，已不再是单纯的技术问题，而是上升为关乎国家环境治理现代化和生态安全的战略性问题。本文的研究正基于此背景展开。

1 环境信息安全的内涵与特殊性

环境信息安全，是指保护环境信息的保密性、完整性和可用性，以及与之相关的信息系统、网络和物理环境的安全。其核心目标在于确保环境信息在采集、传输、存储、处理、交换和销毁的全生命周期内，免遭未经授权的访问、使用、披露、破坏、修改或销毁。与传统的信息安全相比，环境信息安全具有其鲜明的特殊性

1.1 数据源的广域性与异构性

环境信息来源于成千上万个部署在全国乃至全球各地的监测站点和传感器。这些设备品牌各异、协议多样、新旧不一，导致接入环境复杂，安全基线难以统一，攻击面巨大。

1.2 传输网络的复杂性

数据从边缘传感器到中心平台，往往需要经过多种网络，包括移动网络（4G/5G）、卫星网络、物联网专网、互联网和政务外网等。跨网络传输极大地增加了数据被窃听或劫持的风险。

1.3 感知层的物理脆弱性

位于野外的监测设备、通信线路、供电系统等物理设施极易遭受自然力破坏、人为盗窃或恶意干扰（如故意遮挡空气质量监测探头），这种物理层面的攻击可直接导致信息失真或中断。

1.4 数据真实性与完整性的极端重要性

对于环境决策而言，数据的真实性（Authenticity）和完整性（Integrity）甚至比保密性更为关键。攻击者无需窃取数据，只需对监测数据进行微小的、难以察觉的篡改，就足以“污染”整个数据库，引导决策者得出完全错误的结论，其危害更具隐蔽性和破坏性。

1.5 高度的公共属性与敏感性

环境质量信息与公众健康息息相关，其发布时机和内容若被恶意操控，可能引发社会恐慌或群体性事件。同时，部分涉及国家资源分布、敏感地理坐标的环境数据可能被视为国家秘密，其保密要求极高。

2 当前环境信息安全面临的主要挑战

基于上述特殊性，当前我国环境信息安全保障工作面临着多重挑战。

2.1 技术层面挑战

2.1.1 物联网终端安全防护薄弱

大量环境监测传感器计算能力有限、功耗约束严格，难以安装复杂的安全代理软件。许多设备存在默认密码、固件漏洞、未加密通信等“先天性”安全缺陷，极易成为攻击者渗透内网的跳板。

2.1.2 数据跨境传输与共享风险

在国际合作项目或使用境外云服务时，环境数据的出境可能面临数据主权和合规风险。同时，各部门（生态、气象、水利、自然资源等）间的数据共享机制不健全，要么形成“数据孤岛”，要么在共享过程中因标准不一、权限不清而引入安全风险。

2.1.3 云平台与大数据安全风险

环境信息系统普遍采用云计算和大数据技术进行海量数据存储与分析。云平台的多租户特性、虚拟化安全、API 接口安全以及大数据组件的复杂性都带来了新的安全威胁面。

2.1.4 高级持续性威胁（APT）攻击

环境领域可能成为国家级 APT 组织的攻击目标，其攻击手段高超、隐蔽性强、目的明确（如长期潜伏窃取数据或伺机破坏），传统防御手段难以有效应对。

2.2 管理层面挑战

2.2.1 安全意识与专业人才匮乏

环保行业从业人员，特别是业务人员和技术运维人员，信息安全意识普遍不足。同时，既懂环境业务又精通信息安全的复合型人才极度短缺，导致安全策略与业务需求脱节。

2.2.2 安全管理制度与标准落实不到位

虽然国家出台了《网络安全法》《数据安全法》等一系列法律法规，但在环境领域的细化落地和执行力仍显不足。许多单位的安全管理制度流于形式，未能与业务流程深度融合。

2.2.3 供应链安全风险

环境监测设备、软件系统乃至运维服务大量依赖于外部供应商，供应链中的任何一个环节被植入后门或存在漏洞，都将对整个系统造成致命打击[1,2]。

2.2.4 应急响应与恢复能力不足

许多机构缺乏行之有效的网络安全应急预案，演练不足。一旦发生重大安全事件，难以快速定位、遏制和恢复，可能导致事态扩大[3,4]。

2.3 合规性挑战

对于生态环境部门而言，信息安全合规性不仅是法律要求，更是守护国家生态安全底线、履行环境监管职责的生命线。当前面临的合规性挑战主要是环境数据分类分级落地执行难、敏感环境信息泄露的法定责任风险、环境监测数据“真、准、全”的合规性溯源压力、数据共享与开放中的合规边界模糊等。概括的说，就是难以将宏观的法律法规要求，与微观、复杂的环境业务数据和信息系统进行精准映射和有效落地。

3 环境信息安全保障体系构建策略

为应对上述挑战，必须构建一个“技术、管理、法律”三位一体、纵深防御的环境信息安全保障体系。

3.1 技术保障体系：构建纵深防御机制

网络安全技术层作为环境信息安全保障体系的基石，通过多维度技术手段构建动态防御体系。其核心功能可概括为以下几个层面，如表1所示。

3.2 管理保障体系：健全治理结构与流程

在环境信息安全保障体系中，管理保障与技术层形成“软硬协同”的防御闭环。其核心价值在于通过制度设计将技术能力转化为可持续的安全实践，具体体现在以下几个维度，如表2所示。

3.3 法律与合规保障体系：遵循规制与标准

3.3.1 严格落实法律法规

严格遵守《网络安全法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》等上位法要求，主动履行网络安全保护义务。

3.3.2 建立内部合规体系

开展数据资产盘点与分类分级工作，依据国家及行业标准，明确各类环境数据的保护等级和措施。建立健全数据出境安全评估内部流程。比如建立基于《数据安全法》

表1 技术保障体系表

技术体系的层面	具体情况	举例说明
感知层	推行“安全内生”理念，采购设备时明确安全技术要求。	比如运用网络分段隔离和轻量级加密协议技术。
网络层	在网络边界部署防火墙、入侵检测/防御系统，严控访问权限。	比如配备深信服的下一代防火墙，配置策略或者开黑白名单严格限制访问。
平台层	采用成熟的云安全共享责任模型并实施数据分类分级管理。	比如采用政务云、移动云、联通云等并充分利用云服务商提供的安全能力（如WAF、DDoS防护）。
应用层	在软件/系统开发生命周期中嵌入安全要求，定期进行代码审计和渗透测试。	比如对Web应用加强输入验证、防SQL注入、跨站脚本（XSS）等常见漏洞的防护。
数据层	覆盖数据全生命周期的安全管控能力。	比如数据采集认证、传输加密、存储加密、访问控制、安全销毁等。
安全运维	安全运营中心，实现日志集中采集、关联分析和态势感知。	比如配备深信服的态势感知、日志审计、探针、漏洞扫描等硬件设备。
智能防御	用人工智能和机器学习技术分析流量数据，实现对未知威胁的预测和自动化响应。	比如安博通SOAR，用AI打造企业安全运营的自动化中心；绿盟科技的AI安全运营新成果。

表2 管理保障体系表

管理体系的维度	具体情况	举例说明
安全责任	建立网络安全工作领导小组，明确各方职责。	比如成立以“一把手”为主要负责人的网络安全工作领导小组，并指定日常工作的部门。
制度体系	制定并持续完善一系列规章制度和操作流程。	比如《单位人员安全管理制度》《单位网络安全应急预案》《单位网络安全责任制检查考核制度》等。
人员管理与培训	定期对全体员工进行分层次、差异化的安全意识培训。	比如对系统管理员进行专业技能培训和安全背景审查，对外部人员建立外访管理制度。
供应链安全管理	建立供应商安全准入和定期评估机制，保证供应链源头安全。	比如选择移动、联通等具有央企性质的供应商，并进行背景调查等合规性审查。
应急响应体系	制定网络安全事件应急预案，并定期开展攻防演练。	比如参加省举办的攻防演练，演练结束后完善本单位的《网络安全事件应急预案》。

《网络安全法》的贴合生态环境工作实际的《环境数据分类分级指南》和《环境数据安全管理办法》。

3.3.3 积极参与标准制定

行业主管部门和领先企业应积极参与环境信息安全国家及行业标准的制定工作，推动形成统一、规范的技术和管理标准，为全行业的安全建设提供指引。

4 结语

环境信息安全是一项长期性、系统性和战略性的工程，绝非一蹴而就[5]。它不再是 IT 部门的孤立职责，而是需要业务部门、管理层、技术团队乃至整个行业生态协同努力的共同事业。我们必须以总体国家安全观为指引，充分认识环境信息安全的极端重要性，坚持技术防护、管理优化与法律合规三轮驱动，构建一个动态、主动、智能的纵深防御保障体系。唯有如此，才能筑牢数字时代的生态安全屏障，确保环境信息的“真、准、全”，为推进生态文明建设、实现高质量发展提供坚实可靠的安全底座。

参考文献：

[1] 王珊，萨师煊. 数据库系统概论（第 5 版）[M]. 北京：高等教育出版社，2014.

[2] 冯登国，张敏，张妍等. 大数据安全与隐私保护[J]. 计算机学报，2014,37(1):246-258.

[3] 贾焰，方滨兴. 网络空间安全战略研究[J]. 中国工程科学，2016, 18(6): 10-17.

[4] NIST Special Publication 800-53. Security and Privacy Controls for Information Systems and Organizations[Z]. 2020.

[5] Johnson R, Smith T. Cybersecurity for Critical Infrastructure: The Case of Environmental Monitoring Systems[J]. Journal of Environmental Informatics, 2021, 38(2): 112-125.

作者简介：陈勇（1975-）男，汉族，广东潮州人，本科，潮州市环境信息中心，中级工程师，研究方向：环境信息安全和生态环境管理与咨询。