民航空管网络安全建设研究

刘东晨
中国民用航空大连空中交通管理站　辽宁大连　116033

摘　要：随着现代科技的迅速发展，网络也已经成为工作不可替代工具，同时是民航空管运行保障的重中之重，而空管又是确保航空安全和运行效率的关键组成部分，空中交通管制指挥系统越来越依赖于网络安全和信息化技术，这种依赖也带来了新的挑战。因此，空管系统的网络环境是否运行正常直接影响着旅客的生命财产安全。本文主要探讨民航空管信息系统的重要性，面临的风险，信息系统的建设思路以及空管网络安全的建设对策，并提出空管的网络安全建设意见，提升空管网络安全整体能力。

关键词：空管信息系统；网络安全；信息安全；纵深防御

一、民航网络安全重要性

当前，网络安全在民航行业具有开放性、分布广的特征，应用于航班调度、票务管理、旅客服务、飞行操作、机务维护等业务，各系统间数据紧密连接，信息传递实时高效。这些数据来源不同，同时也面临严重的安全威胁。空中交通管制是保障航班运行的基础支撑，主要负责协调飞机起降、航线管理和航路监控，其中，与空管运行相关信息系统的网络安全至关重要，因为直接关系到航空运输的安全与效率。一旦信息系统网络遭受攻击或出现故障，可能会导致航班延误、航线混乱，甚至引发飞机相撞等严重的安全事故。此外，空管系统中存储大量敏感数据，如航班信息、乘客资料等，若被非法获取或篡改，将威胁国家安全和个人隐私。因此，确保空管信息系统的网络安全是保障航空业稳定运行、维护公众信任和国家利益的关键。

二、网络安全相关政策规范

为了应对当前复杂国际形势带来的网络安全挑战，国家和行业层面已经制定相关法规和政策，针对不同敏感级别的数据，制定具体的保护措施和访问权限控制；对于跨境数据传输，建立更加严格的审批和监管机制，明确民航空管在网络安全方面的法律责任和监管要求。同时，这些法规及管理办法也为民航单位提供明确的指导和规范，使其在网络安全管理和防护方面有据可依，推动整个空管行业的网络安全水平。

三、民航空管网络安全面临的风险

目前，空管已建成民航通信网，民航通信网的范围覆盖民航管理局、空管、机场、航司等所有民航部门，同时通过民航通信网，空管初步实现了航行情报、气象等专业信息的网络化服务，为航空公司、机场等民航部门提供了空中交通信息。空管信息化建设基本满足了航空事业的发展需要，成为支撑空管现代化发展的有力工具，是保障安全生产和推动科技创新的强大动力。在空管系统网络安全防护过程中，存在以下风险：

（一）国内外网络威胁形势加剧

随着信息技术的发展，黑客的攻击手段也在不断升级，勒索软件从传统的网络钓鱼行为转移到web零日漏洞的利用，加密或窃取敏感数据；例如分布式拒绝服务（DDoS）攻击、通过大量虚假流量淹没信息系统的网络，导致系统瘫痪；通过ADS-B虚假信号对通信链路信息的劫持和干扰，导致无法识别飞行目标；境外APT组织会利用网络上发布的开源项目代码来吸引国内人员下载和二次传播，用户打开后会自动触发恶意代码，会针对性的攻击特定信息系统并进行渗透和破坏。

（二）企业的内部管控风险

员工对网络安全的认识不足，安全意识淡薄，点击不明链接、下载未知附件等行为，导致黑客会通过供应商或软件间接渗透空管网络，可能会引发重大网络安全事件。空管信息系统与航空公司、机场网络的安全信息共享机制还不够完善。此外，空管分局站在网络安全方面的人才储备不足，缺乏专职网络安全人员来应对复杂

作者简介：刘东晨（1997.3—），男，汉族，辽宁抚顺人，中国民用航空大连空中交通管理站，助理工程师，研究方向：网络安全。

的网络安全威胁，在网络安全事件的预防、检测、响应和恢复等方面存在薄弱环节。

（三）新技术应用挑战

人工智能在网络安全中的应用越来越多，实现实时分析海量网络数据，快速识别出恶意软件和钓鱼攻击，减少人工干预的时间延迟，但这也带来了风险。黑客会通过生成式人工智能来进行犯罪，“ChatGPT”也可能为黑客提供帮助，会写出更加逼真的网络钓鱼邮件。大语言模型的本地化部署面临着数据泄露风险，攻击者会通过提示词注入隐藏指令，执行非预期操作，从而导致用户隐私泄露。但是现有空管设备情况仅考虑了基础的安全隔离和防护手段，缺乏综合全面的安全管理和技术支撑，无法应对日益复杂的信息系统和层出不穷的安全威胁。

（四）供应链安全风险

供应链攻击通常指攻击者通过攻击或篡改信息系统在其生产构建过程中所依赖的组件、工具、服务等，对信息系统植入恶意代码或后门，以达到进一步攻击目标的目的。从信息安全角度看，空管系统的供应链体系中涉及多个供应商和企业，这些供应商和企业的网络安全防护水平参差不齐，供应链安全要求保护供应链中涉及的商业机密、客户数据等敏感信息，一旦供应链中的某个环节出现安全漏洞或遭到攻击，就可能对整个系统造成严重的影响，可能使企业损失数百万元。因此，供应链中多任何环节出现问题都可能导致整个链条中断，间接影响到空管的生产运行。

四、空管系统网络安全建设思路

（一）网络现状

空管系统主要承载生产网、管理信息网和互联网三种基础网络。其中生产网是为生产运行系统提供通信功能的网络基础设施，主要承载运行协同决策、数字空管、管制综合管理等系统，与空管自动化，自动转报等重要生产运行系统连接。管理信息网主要承载办公自动化网络设施，涉及综合办公、固定资产、财务管理、视频会议等多个应用系统。各地区空管局的互联网出口由各单位自行建立，互联网出口的逻辑位置位于外网出口区。外网出口区是为保证网络边界的总体安全而设立的，应配备边界防火墙、上网行为管理设备，实现针对高级信息安全威胁的纵深防御。目前各地区空管局内的互联网主要用于新闻宣传、动态信息发布，内外网无法互通，无法满足国家安全等级保护要求，未来将建成一套跨网的数据共享通道，实现内外网信息共享，提升空管信息系统的数据管理能力。

（二）建设要求

空管信息系统对可靠性的要求很高，在建设新的信息系统过程中，遵循网络安全“三同步”原则，同步规划、同步建设和同步使用。新建的信息系统须符合等级保护测评、商用密码应用安全性评估和行业主管部门安全建设要求，能够有效防护免受来自外部有组织的团体、威胁源发起的网络攻击造成的损害，能够及时发现、监测攻击行为和处置网络安全事件，充分保障空管业务的正常运行。

五、空管网络安全建设对策

（一）构建空管网络安全纵深防御体系

网络安全纵深防御体系是一种多层次、多维度的安全防护策略，是通过叠加不同的安全产品和技术手段，形成系统间的优势互补，从而实现对安全态势的全面感知能力。纵深防御体系源于军事领域的防御策略，强调多点布防、以点带面、多面成体，将单点防护能力整合，搭建多层次的立体防御体系。其构建应遵循全面、灵活、主动等原则，确保网络安全的各个层面都得到有效的防护。纵深防御体系的核心思想是将网络分为多个层次，每个层次都有相应的防御措施，控制每个层次的覆盖范围，使各个层次发生的安全问题仅发生在该范围内，用户使用也应该按照层次划分权限，使每个授权的用户只能拥有其中一部分权限，且其它层次要相互制约和监督，并保证各个层次之间有足够的隔离和互相协作。对于新部署的安全防护系统，从总体把控，需要充分考虑到后期的业务拓展，提前预留相应的可拓展接口，利于系统的功能、性能扩充。这一体系包含物理隔离、防火墙策略、态势感知平台、零信任架构。

1.通过专用的硬件设备（如路由器、交换机等）设置物理防火墙，连接两个或多个网络，但这些设备在逻辑上是隔离的，不允许直接进行数据交换。设置单向传输网关，允许数据从一个网络流向另一个网络，但禁止反向流动。这种方式使数据的流动更具有灵活性，同时保持较高的安全性。在网络中进行网络分区，设置多个子网或虚拟局域网，通过将它们相互隔离来限制不同子网之间的通信，降低内部威胁的风险。

2.限制外部设备访问服务器，仅对特定IP端口开放，防止软件进行外传数据等恶意行为。根据现有空管的业务变化更新访问策略，记录被阻止的流量，分析潜在的攻击方式和软件配置情况。

3.通过建设态势感知平台来采集用户的网络流量、资产状态、威胁情报等数据，通常利用知识图谱、贝叶斯推理等技术实现攻击意图识别、威胁传播建模与风险态势可视化的综合能力。识别异常活动（如APT攻击、数据泄露）、评估风险等级，并预测潜在威胁趋势，同时联动防火墙、EDR等设备实现自动化响应，帮助系统从被动防御转向主动处置，提升系统的整体防御效率和对抗新型威胁的能力。

（4）对所有用户、设备、网络流量及数据访问行为均采取“永不默认信任”的严格安全策略。通过持续验证、动态授权和最小权限原则，重新定义了网络边界静态防御模式，以应对云计算、远程办公及APT等复杂场景下的网络攻击。将安全防护从基于网络拓扑的被动防御，转向以身份和资源为中心的主动风险管理。

（二）落实相关法律法规

空管单位应严格执行网络安全等级保护制度，定期开展关键信息基础设施的定级、备案、整改、监督检查等工作，依据国家商用密码相关标准开展信息系统应用设备的改造，落实密码保护相关措施。推进CPU、操作系统、数据库、终端的国产化替代，逐步提升国产软硬件产品比例。定期自查供应链产品台账，梳理供应链企业清单，加强供应链管理。制定重要数据目录，建立数据分类分级保护制度，构建数据安全治理体系，逐步统一空管信息系统边界网络出口，同时完善数据互联策略，管理漏洞及资产，持续收敛暴露面。

（三）完善网络安全事件应急预案

各地区空管单位要定期评估现有预案的可行性和有效性，及时根据新技术发展和威胁变化进行更新。其次，加强应急响应团队的建设，提高成员的专业技能和协同作战能力。同时，明确应急预案的触发条件和处置流程，确保在紧急情况下能够迅速、准确地采取行动。此外，还需加强与其他相关部门的沟通协调，建立信息共享机制，共同应对网络安全威胁。通过这些措施，可以进一步完善空管网络安全应急预案，保障空管系统的安全稳定运行。

（四）建立健全管理体系机制

从空管系统内的资源协调制度、政策、资金等方面予以大力支持；从项目管理、工程建设、资源整合、应用推进等方面有效管理，科学规划，对项目建设、运行管理、后续开发统筹考虑；建立健全信息系统的管理制度，将来自内部威胁可能性降到最低；明确管理机构及工作人员责任分工，制定管理岗位责任制，最终目标是让网络安全像“免疫系统一样”，动态感知威胁、自主响应风险，支撑空管信息系统稳定运行。

（五）加强应急演练和培训

空管各信息系统的管理部门每年应组织开展以网络安全为核心的应急演练，确保发生网络安全事件的时候及时按照应急预案开展工作，及时恢复重要系统功能和数据。利用多种途径对人员进行网络安全培训，通过典型事件案例分析，增强工作人员信息安全意识，普及信息安全知识。定期组织网络安全知识学习，聘请专家进行网络安全知识讲座。积极开展网络安全防护策略研究，明确安全责任，增强工作人员的责任心，提高网信管理和运维工作人员的技术水平。

结论

空管的网络安全建设是一个复杂问题，需要政府、企业、社会组织协同合作，共同看待挑战和潜在的解决方案。以现代社会科技发展的趋势来看，今后空管信息系统将侧重于态势感知、数据分析，以及利用先进技术进行有效的安全管理和防护。随着空管业务的数字化转型推进，网络流量和带宽的迅速增长，未来将如何统筹规划空管业务与网络安全的紧密结合就显得尤为重要，更需要每一位员工加强全局性思考、科学性治理，将网络安全与空管的各个维度考虑在一起，有效提升空管系统的网络安全水平，确保民航业的安全和稳定。

参考文献

[1]彭宇彬.空管关键信息基础设施网络安全防护体系建设实践[J].网络空间安全，2022，13（5）：72-76

[2]朱承杰.如何提升民航空管通信网可靠性[J].中国航班，2021（06）：86-89.

[3]中国民用航空局.民用航空空中交通管理管理系统技术规范 MH/T 4018.1[S].2004

[4]陆晚成.网络安全审计系统在校园网络中的应用与研究[J].网络安全和信息化，2023（2）：19-22.

[5]王芸芸.网络安全保障与电力网络攻防技术[J].电子技术，2021，50（11）：72-73.