**Management Science and Engineering** 管理科学与工程, 2022, 11(4), 665-671
Published Online December 2022 in Hans. http://www.hanspub.org/journal/mse
https://doi.org/10.12677/mse.2022.114079

Hans汉斯

# 民航空管信息系统网络安全态势感知与分析

**杨　乐**

民航新疆空管局气象中心，新疆　乌鲁木齐

收稿日期：2022年11月26日；录用日期：2022年12月16日；发布日期：2022年12月28日

## 摘　要

**维护网络安全成为事关国家政治安全、经济发展、社会稳定和人民群众合法权益的重大课题。民航业是国家的重要战略产业，空管作为民航安全运行的中枢系统，其网络安全的重要性不言而喻。以大数据、人工智能、新一代通信网络等新技术为核心的智慧空管建设，即将全方位重塑空管运行模式。在数字化、信息化、网络化程度快速发展的同时，层出不穷的网络攻击，肆意泛滥的木马病毒等形势，进一步加大了民航空管网络安全风险。本文从基于筑牢网络安全屏障出发，分析了目前网络安全的现状和面临的形势，从技术层面和管理层面提出了有效的防护策略，为确保民航空管安全运行、提高网络治理能力起到积极作用。**

## 关键词

**民航空管，网络安全，态势感知**

# Network Security Situation Awareness and Analysis of Civil Aviation Management Information System

**Le Yang**

Meteorological Center of Xinjiang Air Traffic Management Bureau of Civil Aviation, Urumqi Xinjiang

Received: Nov. 26th, 2022; accepted: Dec. 16th, 2022; published: Dec. 28th, 2022

## Abstract

**Maintaining network security has become a major issue related to national political security, economic development, social stability, and the legitimate rights and interests of the people. Civil aviation industry is an important strategic industry of the country. As the central system of civil avia-**

文章引用: 杨乐. 民航空管信息系统网络安全态势感知与分析[J]. 管理科学与工程, 2022, 11(4): 665-671.
DOI: 10.12677/mse.2022.114079

**tion safety operation, the importance of network security of the air traffic control is self-evident. The smart ATC construction, with big data, artificial intelligence, new-generation communication network and other new technologies as the core, will comprehensively reshape the ATC operation mode. With the rapid development of digitization, informatization and networking, the situation of endless cyber attacks and rampant Trojan horses has further increased the risk of the network security of civil aviation air traffic control. Based on building a solid network security barrier, this paper analyzes the current status and situation of network security, and puts forward effective protection strategies about the technical and management levels, which will play a positive role in ensuring the safe operation of air traffic control in civil aviation and improving the ability of network governance.**

## Keywords

**Civil Aviation ATC, Network Security, Situational Awareness**



## 1. 引言

当前，中华民族伟大复兴战略全局、世界百年未有之大变局与信息革命的时代潮流发生历史性交汇。党的二十大科学谋划了未来一个时期党和国家事业发展的目标任务和大政方针，做出了一系列重大战略部署，对网络强国建设做出一系列新论断新部署新要求，就加快建设网络强国、数字中国，健全网络综合治理体系，强化网络、数据等安全保障体系建设提出明确要求[1]。这些新论断新部署新要求，饱含着对网络安全发展成绩的充分肯定、对信息革命演变发展的深刻洞察、对现实风险挑战的清醒认识、对任务举措的战略部署，为当前和今后一个时期做好网络安全工作指明了前进方向、提供了根本遵循。

随着信息化的不断推进，民航业在极大程度上提高了工作效率与服务质量。据不完全统计，我国民航业约有信息系统 3300 多个、互联网网站 1600 多个，但随之带来的网络安全也越来越成为不可忽视的问题，尤其是近年来的勒索病毒已成为全球网络中的主要“流行病”。勒索病毒对中毒的计算机系统数据强行进行加密，致使其核心业务系统无法工作，再以此实行勒索行为，一旦业务系统感染了这种病毒，后果将无法弥补。2021 年 8 月，泰国曼谷航空公司遭受 LockBit 勒索病毒网络攻击，泄露了该公司超 200 GB 数据，包括乘客姓名、国籍、电话号码、信用卡等重要信息。此前，美国最大的燃油管道运营商 Colonial Pipeline 因遭受到勒索病毒的攻击而不得不关闭了近 5500 英里的燃油管道，随后美国华盛顿和东部 17 个州因此进入了紧急状态。在此背景下，结合当前智慧空管建设方向，不断总结近年来网络安全建设中积累的经验，发现存在的问题，对构建稳定、可靠的信息通信系统，保障安全运行至关重要[2]。

## 2. 民航空管信息系统网络安全实践成效及建设中存在的问题

面对网络安全威胁，近年来民航空管系统按照民航局建设“四强空管”的统一部署，在加快推进各类空管生产运行业务系统覆盖的同时，加大网络安全基础设施投入，推进新技术广泛应用，加快规范化制度建设，不断提升安全防护水平，网络安全治理初见成效。

### 2.1. 民航空管信息系统网络安全实践成效及建设中存在的问题

面对网络安全威胁，近年来民航空管系统按照民航局建设“四强空管”的统一部署，在加快推进各

类空管生产运行业务系统覆盖的同时，加大网络安全基础设施投入，推进新技术广泛应用，加快规范化制度建设，不断提升安全防护水平，网络安全治理初见成效。

#### 2.1.1. 网络安全基础设施日趋完善

“十三五”期间，民航空管系统努力推动网络安全基础设施建设，以新疆空管为例，完成了气象数据库网络安全三级等保的改造，划分出多个级别的网络安全区域并部署区域边界安全防护设备。在此基础上，建设了面向互联网信息共享系统和气象预警预报服务平台，进一步推进新一代数字化基础设施建设，提高信息共享水平，提升信息服务能力，为建设网络安全防御体系，完成重大活动的保障与网络攻防演练工作打下基础。

#### 2.1.2. 信息化驱动引领作用充分发挥

在网络安全基础设施不断完善的基础上，云计算、大数据、人工智能等新技术也不断被尝试应用于各类空管信息系统中[3]，通过互联网云平台、云数据中心、虚拟化平台的建设，解决许多工作的实际业务需求和存在的问题。在空管气象业务中，通过与机场、航空公司、军方等单位信息共享，形成协同联动，提高了民航空管的服务保障能力，进一步提升了空管的行业影响力。运用航迹与气象信息融合为管制提供特定区域气象服务、使用机器学习框架进行气象云图分析，对于构建智慧气象体系、提高系统的运行效率、科学发展提供了有力支撑。利用大数据挖掘技术对各类航空气象用户的访问行为进行分析，进一步提升了网络安全态势感知能力[4]。

#### 2.1.3. 规范化制度建设进程不断加快

随着我国《网络安全法》、《数据安全法》、《关键信息基础设施安全保护条例》及网络安全等级保护 2.0 的颁布，全系统深入贯彻落实国家网络安全等级保护制度，进行了多个系统的定级、备案、等级测评工作，并开展网络安全与信息化运行体系研究，着手智慧化发展体系和构建网络安全综合防御体系，加强网络信息安全管理。

在总结成绩的基础上，也要清醒地认识到，尽管我们持续优化网络安全环境，但在将“安全高于一切”作为准绳的民航业仍面临着较大的考验。首先，部分运行系统仍处在分散建设、各自独立运行阶段，跨业务、跨系统的运行管理监控平台尚未建成，对于整体系统的网络安全监管还无法做到完全覆盖。其次，系统内各安全运行类数据的分析挖掘能力还有所欠缺，面对信息系统呈现大数据的特征，基于云计算的大数据处理分析能力仍有不足，提升网络安全运行效率还有一定空间。此外，随着新技术的应用，日均数据量迅速增长，网络结构日益复杂，服务单位快速增多，也增加了各类系统在互联网的暴露面，带来了更多的网络安全新挑战。由此，利用技术攻关提升网络安全防护能力，深化管理提升网络安全治理能力，在技术和管理两个层面双管齐下，找出应对策略是化解网络安全风险的重要任务。

### 2.2. 从网络边界监控、网络安全态势感知方向技术攻关，不断提升网络安全防护能力

针对空管信息系统数据量大、实时性强的特点，按照“一个中心，三重防护”理念，建设安全管理中心，从安全计算环境、安全通信网络、安全区域边界三个方面制定总体技术路线，重点从网络边界的监测与访问控制及基于日志分析的安全预警两个方向进行研究，构建网络安全自适应防护体系和态势感知预警平台，以此提高网络安全防护能力。

#### 2.2.1. 网络边界的监测与访问控制

空管信息系统用户分为内网专线用户和互联网接入用户[5]，网络构架如下图 1 所示：

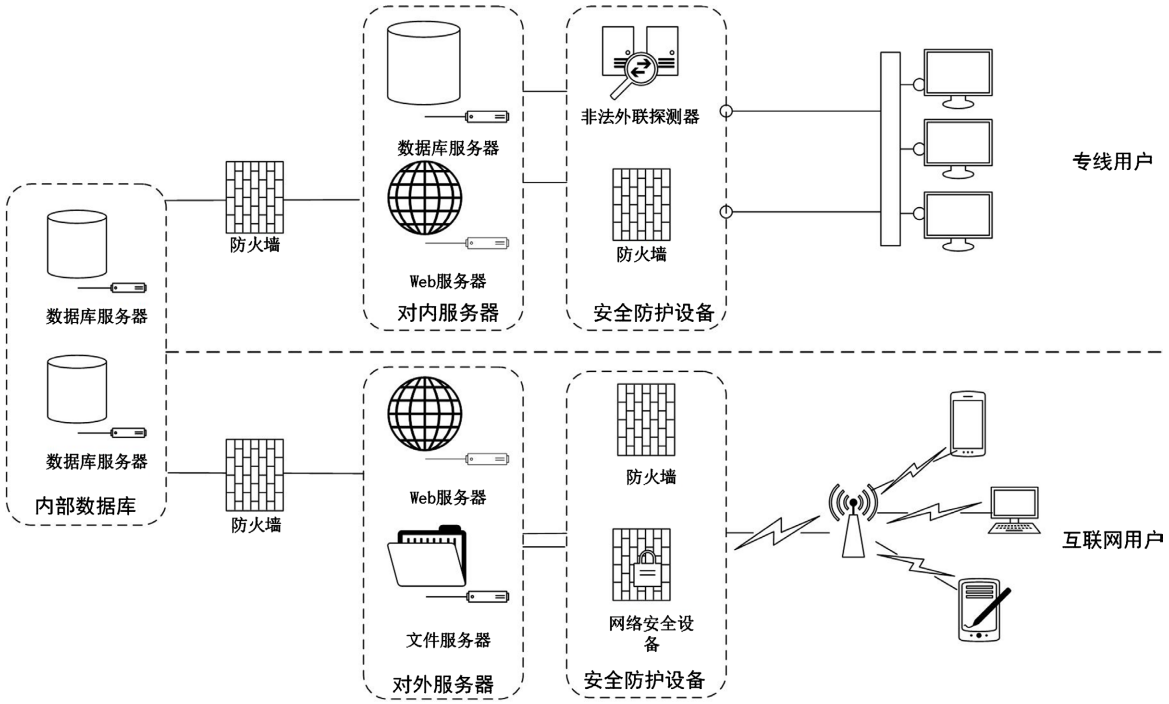


**Figure 1.** Network architecture of air traffic control information system
**图 1.** 空管信息系统网络构架图

一方面，对于专线用户，建立“零信任”机制，进行 MAC 地址 IP 绑定的方式进行身份管理验证，同时，防火墙策略加强应用程序接口安全限制，开放业务运行允许的最少端口数量，并在网络边界记录用户的安全活动，对敏感信息系统加入多重身份验证机制，对专线接入用户进行主动扫描获取用户网络信息，如用户有非法外联等行为，则对监控平台推送告警信息，并在网络边界安全设备上修改该用户的访问控制权限，以此达到监控网络边界状态的目的。如图 2 所示，服务器端提供非法外联策略的配置，接收用户端上报的违规事件，进行告警、断网等操作。

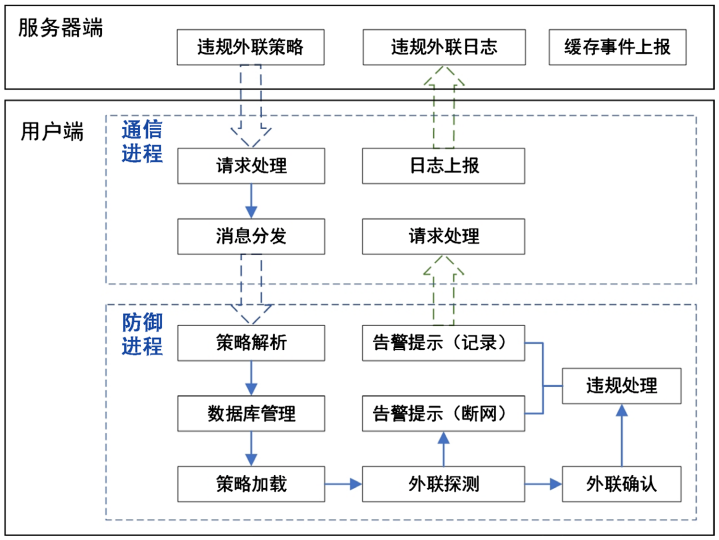


**Figure 2.** Illegal outreach software architecture diagram
**图 2.** 非法外联软件构架图

另一方面，对于互联网接入用户提供统一的认证接口，通过验证账号密码的合法性验证用户是否有权访问系统。对非法连入系统的用户采取管控措施，可在一定程度上降低系统被攻击的风险[6]。具体流程图 3 所示。

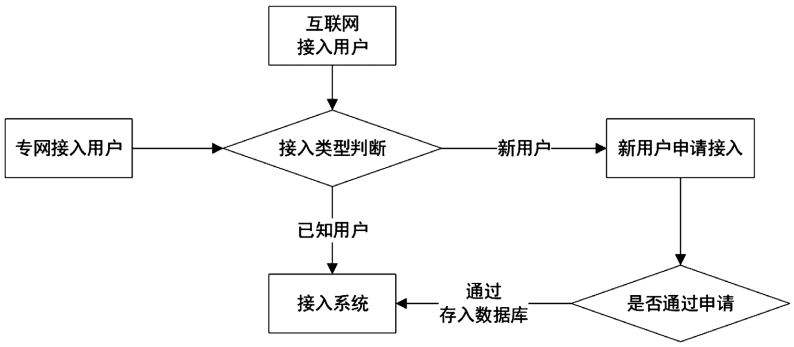


**Figure 3.** Block diagram of the monitoring and access control process of the network perimeter
**图 3.** 网络边界的监测与访问控制流程框图

### 2.2.2. 基于日志分析的网络安全态势感知与预警

基于日志分析进行网络安全态势感知的技术(NSSA)是当前网络安全的研究热点，即通过多维角度对各类系统日志进行深入分析、提取、比对后形成网络安全的发展趋势的预测。具体而言，通过主动采集各类主机、网络设备、服务器及应用系统产生的日志，进行日志格式的转换(如表 1 所示)，采用算法和数据挖掘技术，建立相应的专家库进行规则比对，如发现日志信息中的网络安全威胁到达一定阈值，则进行攻击事件发生趋势的标记与告警，并详细记录攻击事件发生的事件、攻击源、攻击目标、攻击行为等信息。

**Table 1.** Example of log transformation results
**表 1.** 日志转换结果示例

| 日志类型 | 字段 |
|---|---|
| 配置类 | log_id, device, name, time, priority, operation, message |
| 流量监测类 | log_id, device, name, time, event_type, source_zone, source_ip, source_port, dest_zone, dest_ip, dest_port, inpackage, outpackage, sent |
| 攻击事件类 | log_id, device, name, time, event_type, source_zone, source_ip, source_port, dest_zone, dest_ip, dest_port, protocol |

通过主动推送告警，提高运维人员发现并精准定位网络威胁的效率。加强对系统设备日志的研究，运用日志分析技术可实现对系统运行状态和网络安全威胁的检测，对不同设备的日志进行采集和统一管理，有助于补足监控盲点，提高整体系统的网络安全性，如图 4 所示。

### 2.2.3. 应用实例

本应用案例数据基于空管某气象信息服务系统中的日志数据获取与处理，对于攻击类日志进行分析，进行内网和互联网服务系统网络安全预警，部分可视化功能如图 5 所示。

## 3. 从构建统一的规范制度、完善应急机制、构建数字化治理体系方面加强管理，不断提升网络安全治理能力

民航空管的网络安全离不开管理，根据我国民航制度改革的要求与民航局有关信息安全监督机制，

在实际工作中围绕“安全、稳定、高效、集约”的原则下，构建民航空管网络安全信息系统的管理体系。

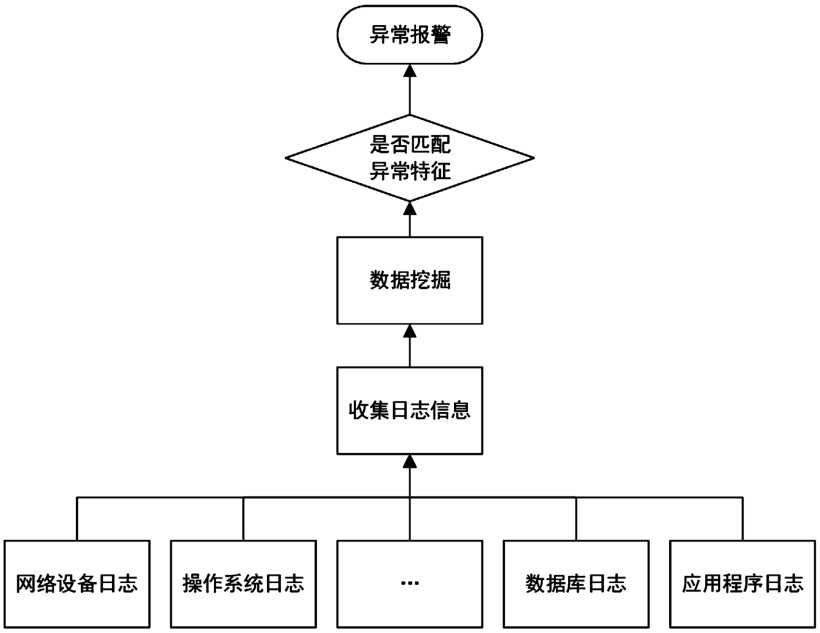


**Figure 4.** Security alert process for log analysis
**图 4.** 日志分析的安全预警流程


**Figure 5.** Visual display of network security alerts
**图 5.** 网络安全预警可视化显示

## 3.1. 构建统一健全的管理体系制度

根据各类信息系统的网络构架和发展特点，欲提升系统的网络防护管理水平，必须要从整体系统出发，制定统一标准。一方面，按照“重点系统，重点防护”的原则，结合民航空管网络安全等级保护的相关要求，对重点关键信息基础设施设备进行资产梳理，建立统一的安全管理体系。另一方面，实现全覆盖，不仅对传统意义上的系统主机、网络、数据、应用进行监管和专项检查，还着重对于云平台、虚

拟化、大数据等新技术、新应用的开发、建设建立安全监管机制，提高技术审查水平，确保新系统的安装部署不会成为安全短板和监管盲区。

### 3.2. 建立完善的应急机制

监管部门应督促各运行单位对自身的网络安全工作进行深入总结和分析，组织人员定期进行信息系统运行状态和风险评估工作，在网络安全态势感知的研究的基础上[7]，对于可能发生的网络安全风险编制应急预案。明确处置的指挥机构与责任人员，加强应急技术支撑平台的建设。针对业务特点，网络安全应急预案主要分为三类：网络攻击类、信息篡改类以及数据窃取类。按照不同类的专项应急预案，定期进行全员应急演练，一方面检验员工应对突发事件的能力和操作熟练水平，另一方面在演练中检验应急预案制定的合理性。通过完善的应急机制落实“关口前移”，使网络安全事件防患于未然。

### 3.3. 建立多维度指标评估治理体系

参考国际民航组织、中国民航等相关数据标准，以强化安全为目标建设数字化的规范治理体系。以生产要素为单位，构建科学的数字化管理系统，用具体的数字指标衡量各系统的安全防护水平。从空管系统的管理领域和“运行、空域、通导、气象、情报”等业务领域的不同角度分析网络安全格局，有利于掌握全系统的网络安全现状，及时发现问题并评估可改进的方向和采取改进措施后的评估。只有建立以数据为支撑的决策体系，才能全面推进空管系统在网络安全治理方面的精准性和高效性。

## 4. 结语

网络安全和信息化是事关国家安全和国家发展，事关广大人民权重生活工作的重大战略问题，没有网络安全就没有国家安全。综上所述，民航空管信息系统的网络安全建设水平虽然和之前比有了很大程度的提高，但在信息技术更新换代的大环境中，网络安全形势日趋严峻。因此，只有在信息网络化建设的同时，进一步查找出现的各项问题，制定有针对性的改进措施，才能构建稳固的网络安全体系，推动民航空管网络安全治理能力不断提升，确保航空运行安全。

## 参考文献

[1] 吴慧, 许屹山. 习近平网络空间命运共同体理念的内在逻辑、科学内涵与时代价值[J]. 安庆师范大学学报(社会科学版), 2021, 40(6): 1-6. https://doi.org/10.13757/j.cnki.cn34-1329/c.2021.06.001

[2] 李刚, 陈怡潇, 黄沛烁, 等. 基于日志分析的信息通信网络安全预警研究[J]. 电力信息与通信技术, 2018, 16(12): 1-8. https://doi.org/10.16543/j.2095-641x.electric.power.ict.2018.12.001

[3] 朱国栋, 朱蕾, 王楠, 孙少明, 梁艳. 基于自动机器学习的机场温度预报方法研究[J]. 沙漠与绿洲气象, 2021, 15(6): 113-119.

[4] 刘煜. 网络安全态势感知与防护体系[J]. 电子技术, 2017, 46(9): 28-30+16. https://doi.org/10.3969/j.issn.1000-0755.2017.09.009

[5] 杨乐, 朱国栋, 孙少明. 民航气象数据存储管理系统设计与应用[J]. 民航学报, 2022, 6(1): 65-68.

[6] 蔡凤玉. 计算机网络安全存在的问题及防范策略[J]. 信息记录材料, 2021, 22(3): 25-26.

[7] 钱国庆. 基于机器学习的网络安全态势感知[D]: [硕士学位论文]. 四川: 电子科技大学, 2019.