ICS 35.030
CCS L 80

MH

中华人民共和国民用航空行业标准

MH/T 3038—2025

民用航空数据安全监测预警技术要求

Technical requirements for monitoring and warning of data security in civil aviation

2025-07-18 发布　　2025-08-01 实施

中国民用航空局　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国民用航空局人事科教司提出。

本文件由中国民航科学技术研究院归口。

本文件起草单位：中国民用航空局信息中心、中国民用航空局空中交通管理局、中国民航信息网络股份有限公司、中国国际航空股份有限公司、北京天融信网络安全技术有限公司、北京安华金和科技有限公司、杭州安恒信息技术股份有限公司、北京神州绿盟科技有限公司、中国民航管理干部学院、中电科网络安全科技股份有限公司、深信服科技股份有限公司、奇安信科技集团股份有限公司。

本文件主要起草人：张威、赵扬、邢伟，刘佳旭、胡滨、李新林、贾琦婧、郭睿、艾龙、张静、魏力、杨锐、刘苏、周金鹏、刘一、袁婷、望娅露、梁智云、石广悦、项有为。

民用航空数据安全监测预警技术要求

1 范围

本文件确立了民用航空（以下简称“民航”）数据安全监测预警基本原则，规定了数据安全监测和预警技术要求。

本文件适用于指导民航领域数据处理者开展数据安全监测和预警能力建设。

本文件不适用于涉及国家秘密的数据安全监测预警工作。

注：本文件所称“数据”是指通过网络处理和产生的各种电子数据。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069 信息安全技术 术语

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 35274 信息安全技术 大数据服务安全能力要求

MH/T 3039 民航领域数据分类分级要求

3 术语和定义

GB/T 25069、GB/T 35273、GB/T 35274、MH/T 3039界定的以及下列术语和定义适用于本文件。

3.1

数据安全监测 data security monitoring

通过对数据处理活动进行实时和持续的监测、分析，以便及早发现数据安全风险和事件的活动。

3.2

数据安全事件 data security incident

通过技术或其他手段对数据实施篡改、破坏、泄露或者非法获取、非法利用等导致业务损失或造成社会危害的事件。

3.3

数据接口 data interface

信息系统之间进行数据传输和交换的通道或协议。

注：相关协议包括http、https协议等。

3.4

敏感个人信息 sensitive personal information

一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息。

[来源：GB/T 43697—2024，3.6]

3.5

告警 alert

当发现数据安全风险时，通过一定的技术手段主动发出警示类通知的行为。

[来源：GB/T 28451—2023，3.5，有修改]

3.6

预警 warning

针对即将发生或正在发生的数据安全事件，提前或及时发出安全警示的行为。

[来源：GB/T 32924—2016，3.4，有修改]

4 缩略语

下列缩略语适用于本文件。

IP：网际协议（Internet Protocol）

5 概述

民航领域数据处理者通过对数据处理活动进行安全监测，及时发现数据篡改、破坏、泄露或者非法获取、非法利用等数据安全风险，并对数据安全风险和事件进行预警，从而降低数据安全事件造成的影响。

数据安全监测的对象是数据处理活动，包括数据收集、存储、使用和加工、传输、提供、公开和删除等活动，具体内容如下：

a) 数据收集：根据特定的目的和要求，通过网络从一种或多种数据源采集数据的数据处理活动；
b) 数据存储：将数据持久化保存在硬盘等存储媒体中的数据处理活动；
c) 数据使用和加工：对数据进行检索、展示、变换、计算、分析等操作的数据处理活动；
d) 数据传输：通过网络将数据从一个责任主体传送到其他责任主体的数据处理活动；
e) 数据提供：向组织内其他责任主体或其他组织提供所控制数据的数据处理活动；
f) 数据公开：向社会公众公开所控制数据的数据处理活动；
g) 数据删除：在所涉及的信息系统及数据存储设备中抹去数据或者覆盖存储的数据，使其不可被检索、访问的数据处理活动。

注：由于针对存储媒体的物理销毁不能通过网络进行监测，因此本文件的数据删除不包括存储媒体物理销毁。

开展数据安全监测需要收集的信息包括但不限于支撑数据处理活动的网络设备、服务器、安全设备、密码设备、存储设备、应用系统、数据接口、数据库、大数据平台、云平台等资产的日志、流量数据，民航典型业务场景下的数据安全监测示例参见附录A。

数据安全预警是针对数据安全监测所发现的异常告警信息进行分析和研判，并对即将发生或正在发生的数据安全事件划分预警级别，同时进行预警发布、预警响应，根据响应情况及时升降级或解除预警的行为。

6 数据安全监测预警基本原则

民航领域数据处理者在开展数据安全监测预警时遵循的基本原则如下：

a) 安全合规：遵守国家和行业的数据安全相关管理要求，确保数据安全监测预警工作的合规性；
b) 及时准确：及时收集和分析数据安全风险信息，准确研判数据安全事件级别；
c) 全面覆盖：监测范围覆盖数据收集、存储、使用、加工、传输、提供、公开、删除等数据处理活动；
d) 持续优化：根据实际业务场景及数据安全监测预警需求的变化，动态更新数据安全监测预警策略；
e) 最小影响：充分考虑监测活动对业务连续性的影响，避免影响业务的正常开展。

7 数据安全监测要求

7.1 通用要求

数据安全监测应满足以下要求：

a) 对数据处理环境的网络流量进行监测，发现具有恶意代码、钓鱼邮件等特征的异常流量时进行告警；
b) 对数据接口的通信对象及行为、通信数据、接口配置进行监测，发现数据接口异常调用、异常开放、异常暴露数据、认证和鉴权机制缺陷等情况时进行告警；
c) 对数据加密、数据脱敏、数据防泄露、数据库审计等数据安全组件的日志进行监测，发现其策略未有效执行等情况时进行告警。

7.2 数据收集

数据收集监测应满足以下要求：

a) 对数据收集工具或服务组件的工作状态进行监测，发现服务异常、流量过载等异常情况时进行告警；
b) 对采用自动化工具收集核心数据、重要数据和敏感个人信息的时间、数量、频率、范围等信息进行监测，发现超约定频率、超业务所需范围等收集数据的异常情况时进行告警；
c) 对核心数据、重要数据和敏感个人信息的数据源可靠性进行监测，发现未经鉴别或身份鉴别失败等异常情况时进行告警；
d) 对核心数据、重要数据和敏感个人信息的真实性和完整性校验结果进行监测，发现校验结果异常时进行告警。

7.3 数据存储

数据存储监测应满足以下要求：

a) 对数据本地备份和异地备份的执行结果和频率进行监测，发现备份作业执行失败、备份频率过低等异常时进行告警；
b) 对访问数据存储系统的行为进行监测，发现异常 IP 访问、未授权访问等异常时进行告警；
c) 对数据存储系统的性能指标、使用空间、健康状态进行监测，发现系统过载、存储空间不足、硬件故障等异常时进行告警；
d) 对核心数据、重要数据和敏感个人信息的存储加密状态进行监测，发现明文存储时进行告警；
e) 对移动存储媒体接入进行监测，发现违规接入、携带恶意代码等异常时进行告警。

7.4 数据使用和加工

数据使用和加工监测应满足以下要求：

a) 对访问数据的行为进行监测，发现越权访问、高频访问、异常 IP 访问、非正常时段访问等异常时进行告警；
b) 对操作数据的行为进行监测，发现违规下载、违规导出、恶意删除等异常时进行告警。

7.5 数据传输

数据传输监测应满足以下要求：

a) 对数据传输设备和通信线路的可用性进行监测，发现设备或线路故障时进行告警；
b) 对数据传输主体的身份鉴别结果信息进行监测，发现非授权的连接时进行告警；
c) 对跨责任主体传输核心数据、重要数据和敏感个人信息的行为进行监测，发现明文传输、超授权范围传输、未使用安全传输协议等异常时进行告警；
d) 对核心数据、重要数据和敏感个人信息的数据传输完整性校验结果进行监测，发现校验结果异常时进行告警。

7.6 数据提供

数据提供监测应满足7.5 c）的要求，还应满足以下要求：

a) 对涉及核心数据、重要数据和敏感个人信息的交换、共享和转让活动进行监测，发现数据未采取加密、脱敏等措施时进行告警；
b) 对涉及重要数据和敏感个人信息跨境流动进行监测，发现实际出境数据与申报内容不一致等违规出境行为时进行告警。

7.7 数据删除

应对核心数据、重要数据和敏感个人信息的删除方式、删除数据类型、删除数据量级、操作行为结果等进行监测，发现数据误删除、未经授权删除、未有效删除等行为时进行告警。

8 数据安全预警要求

8.1 预警分级

数据安全事件预警级别根据数据的级别和数据量级从高到低分为四个级别：红色预警（Ⅰ级预警）、橙色预警（Ⅱ级预警）、黄色预警（Ⅲ级预警）和蓝色预警（Ⅳ级预警）。

不同级别应满足以下预警要求。

a) 红色预警（Ⅰ级预警），当即将发生或正在发生涉及核心数据的数据安全事件时，应发布红色预警。

b) 橙色预警（Ⅱ级预警），当即将发生或正在发生涉及以下情况的数据安全事件时，应发布橙色预警：
   1) 重要数据；
   2) 对社会秩序、公共利益造成轻微危害、对组织权益造成严重危害的一般数据；
   3) 对个人权益造成特别严重危害的敏感个人信息。

c) 黄色预警（Ⅲ级预警），当即将发生或正在发生涉及以下情况的数据安全事件时，应发布黄色预警：
   1) 对组织权益造成一般危害的一般数据；
   2) 对个人权益造成严重危害的敏感个人信息。

d) 蓝色预警（Ⅳ级预警），当即将发生或正在发生除以上提及情形外的数据安全事件时，应发布蓝色预警。

8.2 预警发布

民航领域数据处理者开展预警发布工作应满足以下要求：

a) 针对监测到的数据安全异常情况进行分析和研判，将发现的数据安全风险或事件按照预警级别发布内部预警信息；

b) 确保预警发布渠道的安全可靠，避免预警信息外泄或扩散导致的数据安全事件；

c) 预警信息包含预警级别、事件性质、涉及的数据数量、类型、影响范围和影响程度、防范对策等；

d) 当即将发生或正在发生达到黄色预警、橙色预警和红色预警级别的数据安全事件时，及时向行业数据安全监管部门报告。

8.3 预警响应

民航领域数据处理者在发布预警信息的同时，应积极对数据安全事件进行响应，响应措施包括但不限于以下内容：

a) 根据实际情况启动与预警级别匹配的应急预案；

b) 对于已上报的数据安全事件，应将处置过程和结果向行业数据安全监管部门报告；

c) 对可能损害个人合法权益的数据安全事件，应当及时将情况以邮件、信函、电话、推送通知等方式告知受影响的个人信息主体。难以逐一告知个人信息主体时，应采取合理、有效的方式发布与公众有关的警示信息，并采取补救措施。

8.4 预警升降级或解除

民航领域数据处理者应根据数据安全事件的动态变化，及时发布预警升降级或解除信息，具体发布的信息情况如下：

a) 当数据安全事件造成的损害范围扩大、影响程度增强时，发布预警升级信息；

b) 当数据安全事件得到控制，损害范围减小、影响程度降低时，发布预警降级信息；

c) 当数据安全事件得到消除或经评估发现达不到蓝色预警级别时，发布预警解除信息。

附 录 A
（资料性）
民航典型业务场景下的数据安全监测示例

民航典型业务场景下的数据安全监测示例见表A.1。

表A.1 民航典型业务场景下的数据安全监测示例

场景	产生和处理的数据	涉及的数据处理者	涉及的数据处理活动	涉及的数据安全风险	适用的条款
旅客订票	旅客航班信息、会员信息、支付信息等数据	航空公司 机场 订座系统信息服务提供商 机票销售代理	收集、存储、使用和加工、传输、提供、删除	数据泄露风险 数据篡改风险 数据滥用风险 违法违规出售数据	7.1、7.2、7.3、7.4、7.5、7.6、7.8
旅客安检	旅客航班信息、旅客证件信息、旅客肖像照片、旅客安检信息、旅客状态信息、旅客登机状态、旅客行踪信息等数据	机场 安检系统信息服务提供商	收集、存储、使用和加工、传输、提供、删除	数据泄露风险	7.1、7.2、7.3、7.4、7.5、7.6、7.8
行李托运	行李托运信息等数据	机场 航空公司 托运系统信息服务提供商	收集、存储、使用和加工、传输、提供、删除	数据泄露风险 数据篡改风险 数据滥用风险 数据伪造风险	7.1、7.2、7.3、7.4、7.5、7.6、7.8
旅客值机	旅客信息、航班信息、座位分配信息、行李信息等数据	离港系统信息服务提供商 航空公司 机场	收集、存储、使用和加工、传输、提供、删除	数据泄露风险	7.1、7.2、7.3、7.4、7.5、7.6、7.8
空中交通管理	通信导航监视、气象服务、航空情报、流量管理、运行监控等数据	空管局 空管分局（站）	收集、存储、使用和加工、传输、提供、删除	数据泄露风险 数据篡改风险 数据丢失风险	7.1、7.2、7.3、7.4、7.5、7.6、7.8
安全监管	行政许可信息、行政检查信息、从业人员体检信息、航空器备案信息、维修机构信息、航班信息、货邮信息、无人驾驶航空器实名登记信息等数据	民航安全监督管理机构 民航安全监管系统建设运维单位	收集、存储、使用和加工、传输、提供、公开、删除	数据泄露风险 数据篡改风险 数据伪造风险 数据丢失风险	7.1、7.2、7.3、7.4、7.5、7.6、7.7、7.8

参 考 文 献

[1] GB/T 20986—2023 信息安全技术 网络安全事件分类分级指南
[2] GB/T 28451—2023 信息安全技术 网络入侵防御产品技术规范
[3] GB/T 32924—2016 信息安全技术 网络安全预警指南
[4] GB/T 41479—2022 信息安全技术 网络数据处理安全要求
[5] GB/T 43697—2024 数据安全技术 数据分类分级规则