ICS 35.020
L 07

MH

中华人民共和国民用航空行业标准

MH/T 0041—2013

民用航空信息安全事件分类分级指南

Guidelines for the category and classification of information security incidents of civil aviation

2013－03－13 发布　　2013－06－01 实施

中国民用航空局　发布

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由中国用航空局人事科教司提出。

本标准由中国民航航空局航空器适航审定司批准立项。

本标准由中国民航科学技术研究院归口。

本标准起草单位：中国民航大学、中国民航科学技术研究院。

本标准主要起草人：谢丽霞、杜伟军、付宇、熊育婷、杨宏宇。

民用航空信息安全事件分类分级指南

1 范围

本标准规定了民用航空网络与信息安全事件的分类、分级。

本标准适用于民用航空网络与信息安全管理和应急响应。

2 术语和定义

下列术语和定义适用于本标准。

2.1

信息安全事件 information security incident

由于自然或者人为以及软硬件本身缺陷或故障的原因，对信息系统造成危害，或对社会造成负面影响的事件。

[GB/Z 20986—2007，定义 2.2]

2.2

有害程序事件 malware incidents

蓄意制造、传播有害程序，或是因受到有害程序的影响而导致的信息安全事件。

注：受到有害程序影响的事件是指插入到民用航空信息系统中的一段程序，危害民用航空信息系统中数据、应用程序或操作系统的保密性、完整性或可用性，或影响民用航空信息系统的正常运行。

2.3

网络攻击事件 network attacks incidents

通过网络或其他技术手段，利用民用航空信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对民用航空信息系统实施攻击，并造成民用航空信息系统异常或对民用航空信息系统当前运行造成潜在危害的信息安全事件。

2.4

信息破坏事件 information destroy incidents

通过网络或其他技术手段，造成民用航空信息系统中的信息被篡改、假冒、泄漏、窃取等而导致的信息安全事件。

2.5

信息内容安全事件 information content security incidents

利用信息网络发布、传播危害国家安全、社会稳定和公共利益内容的安全事件。

[GB/Z 20986—20986，定义 4.2.4]

2.6

设备设施故障事件　facilities faults incidents

民用航空信息系统自身故障或电力、电信等外围保障设施故障导致的信息安全事件，以及人为的使用非技术手段造成民用航空信息系统破坏而导致的信息安全事件。

2.7

灾害性事件　disaster incidents

由于不可抗力对民用航空信息系统造成物理破坏而导致的信息安全事件。

3　信息安全事件分类

3.1　有害程序事件

有害程序事件包括：

——计算机病毒事件；
——蠕虫事件；
——木马事件；
——僵尸网络事件；
——混合攻击程序事件；
——网页内嵌恶意代码事件；
——其他有害程序事件。

3.2　网络攻击事件

网络攻击事件包括：

——拒绝服务攻击事件；
——后门攻击事件；
——漏洞攻击事件；
——网络扫描窃听事件；
——干扰事件；
——其他网络攻击事件。

3.3　信息破坏事件

信息破坏事件包括：

——信息篡改事件；
——信息假冒事件；
——信息泄漏事件；
——信息窃取事件；
——信息丢失事件；
——其他信息破坏事件。

3.4 信息内容安全事件

信息内容安全事件包括：

——违反宪法和法律、行政法规的信息安全事件；

——针对社会事项进行讨论、评论形成网上敏感的舆论热点，出现一定规模炒作的信息安全事件；

——组织串连、煽动集会游行的信息安全事件；

——其他信息内容安全事件。

3.5 设备设施故障事件

设备设施故障包括：

——软硬件自身故障信息安全事件；

——外围保障设施故障信息安全事件；

——人为破坏故障信息安全事件；

——其他设备设施故障信息安全事件。

3.6 灾害性事件

灾害性事件包括水灾、台风、地震、雷击、坍塌、火灾、恐怖袭击、战争等导致的信息安全事件。

4 信息安全事件分级应考虑的要素

4.1 信息系统的重要程度

根据民用航空信息系统对行业发展、运行安全、公众利益的重要程度划分为：

——重要民用航空信息系统：安全保护等级为三级及以上的民用航空信息系统；

——一般民用航空信息系统：安全保护等级为二级及以下的民用航空信息系统。

4.2 系统损失

由于民用航空信息系统的软硬件、功能及数据的破坏，导致系统业务中断，从而给事件发生单位或行业造成的损失，按恢复系统正常运行和消除信息安全事件负面影响所需付出的代价划分为：

a) 严重的系统损失：造成重要民用航空信息系统业务瘫痪，丧失业务处理能力，或重要民用航空信息系统关键数据的保密性、完整性、可用性遭到严重破坏，恢复系统正常运行和消除信息安全事件负面影响所需付出的代价十分巨大，对于事发单位或行业是不可承受的；

b) 较大的系统损失：造成民用航空信息系统中断，明显影响系统效率，业务处理能力受到影响，或重要民用航空信息系统重要数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除信息安全事件负面影响所需付出的代价较大；

c) 一般的系统损失：造成民用航空信息系统短暂中断，影响系统效率，使系统业务处理能力受到影响，或民用航空信息系统重要数据的保密性、完整性、可用性遭到影响，恢复系统正常运行和消除信息安全事件负面影响所需付出的代价较小。

4.3 社会影响

针对民用航空信息安全事件对社会造成影响的范围和程度，按其对国家安全、行业发展、运行安全和公众利益等方面造成的影响，划分为：

a) 重大的社会影响：严重影响民用航空运输，造成大面积航班延误，威胁国家安全，严重损害公众利益；

b) 较大的社会影响：影响民用航空运输，造成多个航班延误，可能影响到国家安全，损害公众利益；

c) 一般的社会影响：只影响事件发生单位，造成个别航班延误；对公众利益造成影响。

5 信息安全事件分级

5.1 重大信息安全事件

重大信息安全事件包括：

a) 使重要民用航空信息系统遭受严重的系统损失；

b) 产生重大的社会影响。

5.2 较大信息安全事件

较大信息安全事件包括：

a) 使重要民用航空信息系统遭受较大的系统损失；

b) 产生较大的社会影响。

5.3 一般信息安全事件

一般信息安全事件包括：

a) 使民用航空信息系统遭受一般的系统损失；

b) 产生一般的社会影响。