ICS 35.030
CCS A 90

中华人民共和国国家标准

GB/T 20986—2023
代替 GB/Z 20986—2007

信息安全技术
网络安全事件分类分级指南

Information security technology—Guidelines for category and classification of cybersecurity incidents

2023-05-23 发布　　2023-12-01 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本文件代替GB/Z 20986—2007《信息安全技术　信息安全事件分类分级指南》，与GB/Z 20986—2007相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 由指导性技术文件GB/Z更改为推荐性国家标准GB/T；

b) 更改了“范围”的表述（见第1章，2007年版的第1章）；

c) 在“术语和定义”中，更改了“信息系统”的定义（见3.1，2007年版的2.1），增加了“数据、网络安全、网络安全事件”的定义（见3.1～3.4）；

d) 更改了“缩略语”，删除了原缩略语内容（见2007年版的第3章），增加了新的缩略语“APT、BGP、DDOS、DNS、IP、WLAN”等（见第4章）；

e) 在“网络安全事件分类”中，更改了“分类方法”的表述，将网络安全事件的分类由7类增加至10类（见5.1，2007年版的4.1）：

1) 在“恶意程序事件”中增加了“恶意代码宿主站点事件、勒索软件事件、挖矿病毒事件”3个事件子类（见5.2.1，2007年版的4.2.1）；

2) 在“网络攻击事件”中增加了“后门植入事件、凭据攻击事件、网页篡改事件、暗链植入事件、域名劫持事件、域名转嫁事件、DNS污染事件、WLAN劫持事件、流量劫持事件、BGP劫持攻击事件、广播欺诈事件、失陷主机事件、供应链攻击事件、APT事件”14个事件子类（见5.2.2，2007年版的4.2.2）；

3) 将“信息破坏事件”名称更改为“数据安全事件”，事件子类更改为“数据篡改事件、数据假冒事件、数据泄露事件、数据窃取事件、数据损失事件”，增加了“社会工程事件、数据拦截事件、位置检测事件、数据投毒事件、数据滥用事件、隐私侵犯事件”6个事件子类（见5.2.3，2007年版的4.2.3）；

4) 在“信息内容安全事件”中，事件子类由4个增加到8个，名称更改为“反动宣传事件、暴恐宣扬事件、色情传播事件、虚假信息传播事件、权益侵害事件、信息滥发事件、网络欺诈事件和其他信息内容安全事件”（见5.2.4，2007年版的4.2.4）；

5) 在“设备设施故障事件”中，事件子类由4个增加到5个，名称更改为“技术故障事件、配套设施故障事件、物理损害事件、辐射干扰事件、其他设备设施故障事件”（见5.2.5，2007年版的4.2.5）；

6) 增加了“违规操作事件”类，包括“权限滥用事件、权限伪造事件、行为抵赖事件、故意违规操作事件、误操作事件、人员可用性破坏事件、资源未授权使用事件、版权违反事件、其他违规操作事件”9个事件子类（见5.2.6）；

7) 增加了“安全隐患事件”类，包括“网络漏洞事件、网络配置合规缺陷事件，其他安全隐患事件”3个事件子类（见5.2.7）；

8) 增加了“异常行为事件”类，包括“访问异常事件、流量异常事件和其他异常行为事件”3个事件子类（见5.2.8）；

9) 将“灾害性事件”更改为“不可抗力事件”，包括“自然灾害事件、事故灾难事件、公共卫生事件、社会安全事件、其他不可抗力事件”5个事件子类（见5.2.9，2007年版的4.2.6）；

f) 在“网络安全事件分级”中，将“信息系统”更改为“事件影响对象”：

1） 更改了“分级方法”的表述(见 6.1,2007 年版的 5.1)；
2） 增加了 3 个重要等级“事件影响对象”的说明(见 6.1.2)；
3） 将“系统损失”更改为“业务损失”,其中的“系统关键数据”更改为“重要数据/敏感个人信息”(见 6.1.3,2007 年版的 5.1.3)；
4） 将“社会影响”更改为“社会危害”(见 6.1.4,2007 年版的 5.1.4)；
5） 更改了“事件级别”的表述(见 6.2.1～6.2.5,2007 年版的 5.2)；
6） 增加了“事件分级流程”(见 6.3)；

g） 为便于信息通报、事件研判等应用,增加了“附录 B”,给出了事件分类代码。

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。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位:北京时代新威信息技术有限公司、中国科学院软件研究所、中国长江三峡集团有限公司、杭州安恒信息技术股份有限公司、北京天融信网络安全技术有限公司、启明星辰信息技术集团股份有限公司、陕西省网络与信息安全测评中心、北京东方通网信科技有限公司、北京神州绿盟科技有限公司、国网智能电网研究院有限公司、中国软件评测中心、中国信息安全测评中心、公安部第三研究所、国家计算机网络应急技术处理协调中心、南方电网数字电网研究院有限公司、OPPO 广东移动通信有限公司。

本文件主要起草人:王连强、王新杰、郭启全、黄小苏、杨玉忠、阎若彤、俞政臣、任娟娟、夏雨、任彬、连一峰、张海霞、黄克振、李旸照、黎奇、梁伟、杨剑、刘书鹏、魏玉峰、崔婷婷、李文瑾、张道娟、李婧、尚可、曲洁、郭晶、左晓栋、王健、王小璞、余国平、何余、王元戎、吕明、高琪、朱建兴。

本文件及其所代替文件的历次版本发布情况为:

——2007 年首次发布为 GB/Z 20986—2007；

——本次为第一次修订。

引　言

网络安全事件的防范和处置是国家网络安全保障体系中的重要环节，也是重要的工作内容。网络安全事件的分类分级是快速有效处置网络安全事件的基础之一。

本文件编制的目的是：

a) 利于安全事件数据的收集和分析；

b) 利于识别安全事件的严重程度；

c) 促进安全事件信息的交换和共享；

d) 便于实现安全事件的自动化报告和响应；

e) 提高安全事件通报和应急处置的效率和效果。

在附录 A 中给出了安全事件分类和安全事件分级的关系。

信息安全技术
网络安全事件分类分级指南

1 范围

本文件描述了网络安全事件分类和分级的方法，界定了网络安全事件类别和级别，并明确了网络安全事件分类代码。

本文件适用于网络运营者以及相关部门开展网络安全事件研判、信息通报、监测预警和应急处置等活动。

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 22240—2020 信息安全技术 网络安全等级保护定级指南

GB/T 25069—2022 信息安全技术 术语

3 术语和定义

GB/T 25069—2022 界定的以及下列术语和定义适用于本文件。

3.1

信息系统 information system

应用、服务、信息技术资产或其他信息处理组件的组合。

注：信息系统通常由计算机或者其他信息终端及相关设备组成，并按照一定的应用目标和规则进行信息处理或过程控制。

[来源：GB/T 25069—2022，3.696，有修改]

3.2

数据 data

任何以电子或者其他方式对信息的记录。

3.3

网络安全 cybersecurity

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障数据的完整性、保密性、可用性的能力。

[来源：GB/T 22239—2019，3.1]

3.4

网络安全事件 cybersecurity incident

由于人为原因、网络遭受攻击、网络存在漏洞隐患、软硬件缺陷或故障、不可抗力等因素，对网络和信息系统或者其中的数据和业务应用造成危害，对国家、社会、经济造成负面影响的事件。