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 …… Ⅲ
引言 …… Ⅴ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 2
5　网络安全事件分类 …… 2
5.1　分类方法 …… 2
5.2　事件类别 …… 2
6　网络安全事件分级 …… 6
6.1　分级方法 …… 6
6.2　事件级别 …… 7
6.3　事件分级流程 …… 8
附录 A（资料性）　网络安全事件类别和级别的关联关系 …… 10
附录 B（规范性）　网络安全事件分类代码 …… 12
参考文献 …… 16
索引 …… 17

前　言

□□□□□GB/T 1.1—2020《□□□□□□□　□1□□:□□□□□□□□□□□□□□》□□□□□。

□□□□□GB/Z 20986—2007《□□□□□□　□□□□□□□□□□□□》,□GB/Z 20986—2007□□,□□□□□□□□□□□□,□□□□□□□□:

a) □□□□□□□□GB/Z□□□□□□□□□GB/T;

b) □□□“□□”□□□(□□1□,2007□□□□1□);

c) □“□□□□□”□,□□□“□□□□”□□□(□3.1,2007□□□2.1),□□□“□□、□□□□、□□□□□□”□□□(□3.1～3.4);

d) □□□“□□□”,□□□□□□□□□(□2007□□□□3□),□□□□□□□□“APT、BGP、DDOS、DNS、IP、WLAN”□(□□4□);

e) □“□□□□□□□□”□,□□□“□□□□”□□□,□□□□□□□□□□□□7□□□□10□(□5.1,2007□□□4.1):

1) □“□□□□□□”□□□“□□□□□□□□□、□□□□□□、□□□□□□”3□□□□(□5.2.1,2007□□□4.2.1);

2) □“□□□□□□”□□□“□□□□□□、□□□□□□、□□□□□□、□□□□□□、□□□□□□、□□□□□□、DNS□□□□、WLAN□□□□、□□□□□□、BGP□□□□□□、□□□□□□、□□□□□□、□□□□□□□、APT□□”14□□□□□(□5.2.2,2007□□□4.2.2);

3) □“□□□□□□”□□□□□“□□□□□□”,□□□□□□□“□□□□□□、□□□□□□、□□□□□□、□□□□□□、□□□□□□”,□□□“□□□□□□、□□□□□□、□□□□□□、□□□□□□、□□□□□□、□□□□□□”6□□□□□(□5.2.3,2007□□□4.2.3);

4) □“□□□□□□□□”□,□□□□□4□□□□8□,□□□□□“□□□□□□、□□□□□□、□□□□□□、□□□□□□□□、□□□□□□、□□□□□□、□□□□□□□□□□□□□□□□□□”(□5.2.4,2007□□□4.2.4);

5) □“□□□□□□□□”□,□□□□□4□□□□5□,□□□□□“□□□□□□、□□□□□□、□□□□□□、□□□□□□、□□□□□□□□□□□□”(□5.2.5,2007□□□4.2.5);

6) □□□“□□□□□□”□,□□“□□□□□□、□□□□□□、□□□□□□、□□□□□□、□□□□□□、□□□□□□、□□□授□使□□□、□□□□□□□、□□□□□□□”9□□□□□(□5.2.6);

7) □□□“□□□患□□”□,□□“□□漏洞□□、□□□□合□缺□□□,□□□□□患□□”3□□□□□(□5.2.7);

8) □□□“异常□□□□”□,□□“访问异常□□、□□异常□□□□□异常□□□□”3□□□□□(□5.2.8);

9) □“灾□□□□”□□□“不□抗力□□”,□□“自然灾□□□、□□灾难□□、公共卫生□□、□□□□□□、□□不□抗力□□”5□□□□□(□5.2.9,2007□□□4.2.6);

f) □“□□□□□□□□”□,□“□□□□”□□□“□□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”(

引　言

网络安全事件的　范和　置　国家网络安全　障　系中的重要　，　重要的工作内容。网络安全事件的分类分级　　有　　置网络安全事件的　　。

本文件编　的　的　：

a）　利于安全事件数据的　　和分　；

b）　利于识别安全事件的　重程　；

c）　　安全事件信息的　　和共　；

d）　便于　　安全事件的自动化报　和响应；

e）　提　安全事件通报和应　　置的　　和　　。

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。

/、T222 —2 2 信息安全技术 网络安全等级保护定级指南

/、T2 —2 22 信息安全技术 术语

3 术语和定义

/、T2 —2 22 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： /、T2 —2 22,? ,有修改]

3 2

数据 data

任何以电子或者其他方式对信息的 录。

3 3

网络安全 cybersecurity

通过 取必要 施，防范对网络的攻击、侵入、干扰、破坏和 法使用以及意外事故，使网络处于定可 运行的 、 ，以及保障数据的 整性、保 性、可用性的能力。

[来源： /、T222? —2 1 ,? 1]

3 4

网络安全事件 cybersecurity incident

由于人为原 、网络 攻击、网络 在漏洞隐患、软 件缺陷或故障、不可抗力等 ，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、 造成 影响的事件。

[来源：B/T 38645—2020,3.1,有修改]

4 缩略语

下列缩略语适用于本文件。

A :高级持续性威胁( )

B :边界网关协议( )

:分布式拒绝服务( )

:域名系统( )

:互联网协议( )

A :无线局域网( )

5 网络安全事件分类

5.1 分类方法

综合考虑网络安全事件的起因、威胁、攻击方式、损害后果等因素，对网络安全事件进行分类，分为恶意程序事件、网络攻击事件、数据安全事件、信息内容安全事件、设备设施故障事件、违规操作事件、安全隐患事件、异常行为事件、不可抗力事件和其他事件等 10 类，每类之下再分若干子类。附录 B 确定了网络安全事件分类代码。

5.2 事件类别

5.2.1 恶意程序事件

恶意程序指带有恶意意图所编写的一段程序，该程序插入网络损害网络中的数据、应用程序或操作系统，或影响网络的正常运行。恶意程序事件指在网络蓄意制造或传播恶意程序而导致业务损失或造成社会危害的网络安全事件。

恶意程序事件包括计算机病毒事件、网络蠕虫事件、特洛伊木马事件、僵尸网络事件、恶意代码内嵌网页事件、恶意代码宿主站点事件、勒索软件事件、挖矿病毒事件、混合攻击程序事件和其他恶意程序事件等 10 个子类，具体如下：

) 计算机病毒事件：制造、传播或利用恶意程序，影响计算机使用，破坏计算机功能，毁坏或窃取数据；

) 网络蠕虫事件：利用网络缺陷，蓄意制造或通过网络自动复制并传播网络蠕虫；

) 特洛伊木马事件：制造、传播或利用具有远程控制功能的恶意程序，实现非法窃取或截获数据；

) 僵尸网络事件：利用僵尸工具程序形成僵尸网络；

) 恶意代码内嵌网页事件：在访问被嵌入恶意代码而受到污损的网页时，该恶意代码在访问该网页的计算机系统中安装恶意软件；

) 恶意代码宿主站点事件：诱使目标用户到存储恶意代码的宿主站点下载恶意代码；

) 勒索软件事件：采取加密或屏蔽用户操作等方式劫持用户对系统或数据的访问权，并籍此向用户索取赎金；

) 挖矿病毒事件：以获得数字加密货币为目的，控制他人的计算机并植入挖矿病毒程序完成大量运算；

) 混合攻击程序事件：利用多种方法传播和利用多种恶意程序，例如，一个计算机病毒在侵入计

算机系统后在系统中安装木马程序；

□） 其他恶意程序事件：不在以上子类之中的恶意程序事件。

5□□□ 网络攻击事件

网络攻击事件指通过技术手段对网络实施攻击而导致业务损失或□成社会危害的网络安全事件。

网络攻击事件包括网络扫描探测事件、网络钓鱼事件、漏洞利用事件、后门利用事件、后门植入事件、凭据攻击事件、信号干扰事件、拒绝服务事件、网页篡改事件、暗链植入事件、域名劫持事件、域名转嫁事件、□□□污染事件、□□□□劫持事件、流量劫持事件、□□□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、□□□事件和其他网络攻击事件等□□个子类，具体如下：

□） 网络扫描探测事件：利用网络扫描软件获取有关网络配置、端口、服务和现有脆弱性等信息；

□） 网络钓鱼事件：利用欺诈性网络技术诱使用户泄露重要数据或个□信息；

□） 漏洞利用事件：通过挖掘并利用网络配置缺陷、通信协议缺陷或应用程序缺陷等漏洞对网络实施攻击；

□） 后门利用事件：恶意利用软件或硬件系统设计过程中□经严格验证所留下的接口、功能模块、程序等，非法获取网络管理权限；

□） 后门植入事件：非法在网络中创建能够持续获取其管理权限的后门；

□） 凭据攻击事件：破解口令，解析登录口令或凭据等；

□） 信号干扰事件：通过技术手段阻碍有线或无线信号在网络中正常传播；

□） 拒绝服务事件：通过非正常使用网络资□（诸如□□□、内存、磁盘空间或网络带宽

会危害的网络安全事件。

数据安全事件包括数据篡改事件、数据假冒事件、数据泄露事件、社会工程事件、数据窃取事件、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、数据损失事件和其他数据安全事件等12个子类，具体如下：

a) 数据篡改事件：未经授权接触或修改数据；
b) 数据假冒事件：非法或未经许可使用、伪造数据；
c) 数据泄露事件：无意或恶意通过技术手段使数据或敏感个人信息对外公开泄露；
d) 社会工程事件：通过非技术手段（如心理学、话术等）诱导他人泄露数据或执行行动；
e) 数据窃取事件：未经授权利用技术手段（例如窃听、间谍等）偷窃数据；
f) 数据拦截事件：在数据到达目标接收者之前非法捕获数据；
g) 位置检测事件：非法检测系统、个人的地理位置信息或敏感数据的存储位置；
h) 数据投毒事件：干预深度学习训练数据集，在训练数据中加入精心构造的异常数据，破坏原有训练数据的概率分布，导致模型在某些特定条件下产生分类或聚类错误；
i) 数据滥用事件：无意或恶意滥用数据；
j) 隐私侵犯事件：无意或恶意侵犯网络中存在的敏感个人信息；
k) 数据损失事件：因误操作、人为蓄意或软硬件缺陷等因素导致数据损失；
l) 其他数据安全事件：不在以上子类之中的数据安全事件。

5.2.4 信息内容安全事件

信息内容安全事件指通过网络传播危害国家安全、社会稳定、公共安全和利益的有害信息导致业务损失或造成社会危害的网络安全事件。

信息内容安全事件包括反动宣传事件、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等8个子类，具体如下：

a) 反动宣传事件：利用网络传播煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一等危害国家安全、荣誉和利益的非法信息；
b) 暴恐宣扬事件：利用网络宣扬恐怖主义、极端主义，煽动民族仇恨、民族歧视的信息，引起社会恐慌和动乱；
c) 色情传播事件：利用网络传播违背社会伦理道德的淫秽色情信息；
d) 虚假信息传播事件：利用网络编造并传播虚假信息来扰乱经济秩序和社会秩序，造成负面影响；
e) 权益侵害事件：利用网络传播的信息侵害了社会组织或公民的合法权益；
f) 信息滥发事件：利用网络传播未经接收者准许的信息，例如：垃圾邮件等；
g) 网络欺诈事件：恶意利用技术或非技术手段对特定或不特定目标通过网络进行欺诈以非法获取信息或钱财；
h) 其他信息内容安全事件：不在以上子类之中的信息内容安全事件。

5.2.5 设备设施故障事件

设备设施故障事件指由于网络自身出现故障或设备设施受到破坏或干扰而导致业务损失或造成社会危害的网络安全事件。

设备设施故障事件包括技术故障事件、配套设施故障事件、物理损害事件、辐射干扰事件和其他设备设施故障事件等5个子类，具体如下：

a) 技术故障事件：网络中软□件的自然缺陷、设计缺陷□运行环□发生变化□引起系统故障，□如：□件故障、软件故障、□□等；
b) 配套设施故障事件：□□网络运行的配套设施发生故障，□如：电力供应故障、照明系统故障、□□度□制系统故障等；
c) 物理损害事件：故意□意外的物理行动造□网络环□□网络设备损坏，□如：失□、漏□、□电、设备□坏□□失等；
d) 辐射干扰事件：□辐射□生干扰影响网络□常运行，□如：电□辐射、电□□□、电子干扰、电□□动、□辐射等；
e) 其他设备设施故障事件：不在以□子类之中的设备设施故障事件。

5.2.6 违规操作事件

违规操作事件指人为故意□意外□损害网络□能□导□业务损失□造□社会危害的网络安全事件。

违规操作事件包括权限滥用事件、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、版权违反事件和其他违规操作事件等 9 个子类，□体如下：

a) 权限滥用事件：由于网络□务□□能开□□□□权限限制不严□，导□攻击者通□□□□□□调用权限的方□进行攻击；
b) 权限伪造事件：为了欺□制造虚假权限；
c) 行为抵赖事件：用□□认其有害行为；
d) 故意违规操作事件：故意□行□法操作；
e) 误操作事件：□意□□行□误操作；
f) 人员可用性破坏事件：人力资源□损，导□人员缺失□缺席；
g) 资源未授权使用事件：未□授权访问资源；
h) 版权违反事件：违反版权要　安□使用　业软件□其他□版权保□的　料；
i) 其他违规操作事件：不在以□子类之中的违规操作事件。

5.2.7 安全隐患事件

安全隐患事件指网络中出现能□攻击者利用的漏洞□隐患，一□□利用可能对网络造□破坏，进□导□业务损失□造□社会危害的网络安全事件。提前发现□些漏洞□隐患能防范由□引起的其他网络安全事件。

安全隐患事件包括网络漏洞事件、网络配置合规缺陷事件、其他安全隐患事件等 3 个子类，□体如下：

a) 网络漏洞事件：□操作系统、应用程序□安全协□开发及设计□程中，对安全性考□不　分□出现安全隐患；
b) 网络配置合规缺陷事件：由于软□件安全配置不合理□缺省配置，不　合网络安全要　□□生安全缺陷□隐患；
c) 其他安全隐患事件：不在以□子类之中的安全隐患事件。

5.2.8 异常行为事件

异常行为事件指网络本□□定性不　□违规访问网络造□访问、流量等异常行为，进□导□业务损失□造□社会危害的网络安全事件。

异常　为事件　　访问异常事件、流　异常事件和　　异常　为事件　3　　类，具体如下：

a）　访问异常事件：因网络　硬件运　环境　生变化导致不能提　服务；

b）　流　异常

估，其大□可取决□恢复□□正□□行和消除网络安全事件负面□□□需付□的代价，分为4个级别：特别□□、□□、较大和较□，具□如下：

a) 特别□□：造成网络大面积瘫痪，□其丧失□□□理□□，或□要数据/□□个人信息遭到□□破坏，恢复□□正□□行和消除安全事件负面□□□需付□的代价十分巨大，□□事发组织□□可□受的；

b) □□：造成网络□□间中断或局部□□瘫痪，□其□□□理□□受到极大□□，或□要数据/□□个人信息遭到破坏，恢复□□正□□行和消除安全事件负面□□□需付□的代价巨大，但□□事发组织□可□受的；

c) 较大：造成网络中断，导致□□□理□□受到较大□□，或数据/□□个人信息受到损害，恢复□□正□□行和消除安全事件负面□□□需付□的代价较大，但□□事发组织□完全可□□受的；

d) 较□：造成网络短暂中断，导致□□□理□□受到□定□□，或数据/□□个人信息受到□□，恢复□□正□□行和消除安全事件负面□□□需付□的代价较□。

6.1.4 社会危害的严重程度

社会□害的□□程□根据□国家安全、社会秩序、经济□设和□众□益等方面的□害程□□行□估，分为4个级别：特别□大、□大、较大和□般，具□如下：

a) 特别□大：波□□个或多个□市的大部分地区，□害到国家安全，引起社会动荡，□经济□设□极其恶劣的负面□□，或□特别□□损害□众□益；

b) □大：波□□个或多个地市的大部分地区，□□到国家安全，引起社会恐慌，□经济□设□恶劣的负面□□，或□□□损害□众□益；

c) 较大：波□□个或多个地市的部分地区，□□□国家安全，但□扰乱社会秩序，□经济□设或□□众□益造成□般损害，□相关□民、法人或其他组织的□益会造成□□损害或特别□□损害；

d) □般：波□□个地市的部分地区，□□□国家安全、社会秩序、经济□设和□众□益，但□□相关□民、法人或其他组织的□益会造成□般损害。

6.2 事件级别

6.2.1 概述

按照事件□□□□的□要程□、□□损失的□□程□和社会□害的□□程□□个要素，网络安全事件分为4个级别：特别□大事件、□大事件、较大事件和□般事件，由□到低分别为□级、二级、□级和四级。

6.2.2 特别重大事件（一级）

特别□大事件发□在特别□要的事件□□□□上，□且：

a) 导致特别□□的□□损失，或

b) 造成特别□大的社会□害。

6.2.3 重大事件（二级）

□大事件发□在特别□要或□要的事件□□□□上，□且：

a) 导致特别□要的事件□□□□遭受□□的□□损失或导致□要的事件□□□□遭受特别□□

的业务损失，□

b） 造□重□的社会危害。

6.2.4 较大事件（三级）

较□事件发生在□别重要□重要□一般的事件影响对象□，并□：

a） 导□□别重要的事件影响对象□□较□□较小的业务损失，□重要的事件影响对象□□严重□较□的业务损失，□导□一般的事件影响对象□□较□（含）以□级别的业务损失，□

b） 造□较□的社会危害。

6.2.5 一般事件（四级）

一般事件发生在重要□一般的事件影响对象□，并□：

a） 导□较小的业务损失，□

b） 造□一般的社会危害。

6.3 事件分级流程

对网络安全事件的分级根据三个分级要□进行评定，流程如下：

a） 确定网络安全事件影响对象的重要程度；

b） 分别评定业务损失的严重程度和社会危害的严重程度；

c） 根据表1、表2分别评定对应的网络安全事件级别；

d） 两者中取高者确定为网络安全事件级别。

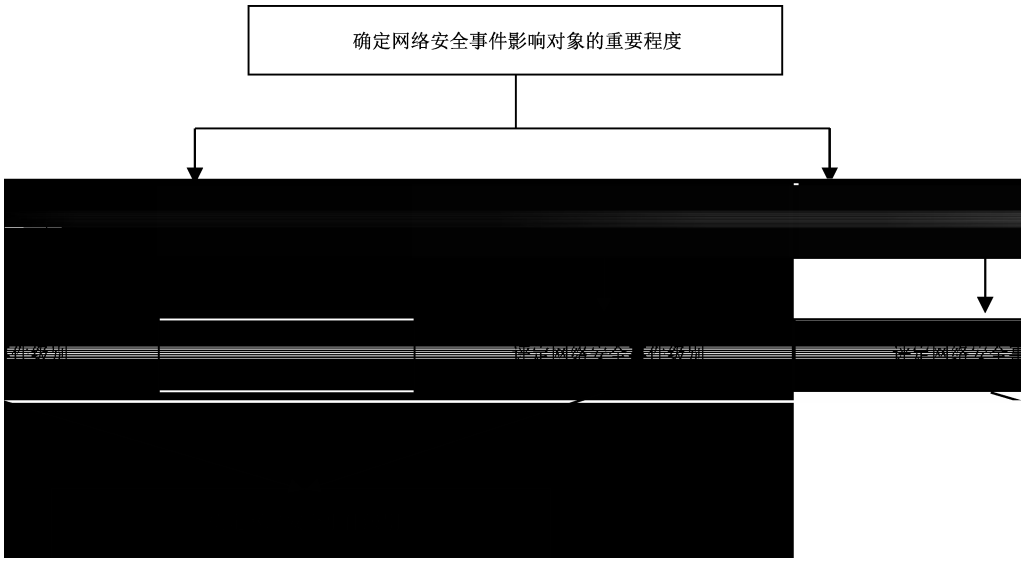
表1 网络安全事件级别与业务损失的严重程度的关系

事件影响对象的重要程度	业务损失的严重程度			
	□别严重	严重	较□	较小
□别重要	一级	二级	三级	三级
重要	二级	三级	三级	四级
一般	三级	三级	三级	四级

表2 网络安全事件级别与社会危害的严重程度的关系

事件影响对象的重要程度	社会危害的严重程度			
	□别重□	重□	较□	一般
□别重要	一级	二级	三级	—
重要	—	二级	三级	四级
一般	—	—	三级	四级
注：“—”表示忽略□□情况，□依据实际情况□合判断网络安全事件级别。				

网络安全事件分级流程示意□如□1所示。



□ 1 □ □ □ □ □ □ □ □ □ □ □ □ □ □

附 录 A
（资料性）
网络安全事件类别和级别的关联关系

一个网络安全事件类别可能具有不同的网络安全事件级别（以下简称“事件级别”），这不仅取决于业务，还取决于网络安全事件的性质，例如：故意性、目标性、时机、量级。

表 A.1 给出了具有不同严重级别的网络安全事件类的示例。

表 A.1 网络安全事件类别和级别的关联关系示例

事件类别	事件级别			
	一般事件（四级）	较大事件（三级）	重大事件（二级）	特别重大事件（一级）
恶意程序事件	一次已知的恶意程序事件，被防病毒保护发现并拦截，没有导致业务损失或导致较小的业务损失	重要信息系统受单次的恶意程序感染，或一般信息系统受恶意程序多次感染，导致较大业务损失	特别重要信息系统遭受单次恶意程序，或重要信息系统受恶意程序多次感染或严重感染，对系统用户、应用程序造成损害，导致严重的业务损失	特别重要信息系统遭受恶意程序多次感染或严重感染，导致特别严重的业务损失
网络攻击事件	一次尝试失败的网络攻击事件，没有导致业务损失或导致较小的业务损失	重要信息系统受到骚扰或少量攻击，或一般信息系统遭受多次网络攻击，导致较大业务损失	特别重要的信息系统受到骚扰或少量攻击，或重要信息系统受到多次网络攻击，导致严重的业务损失	针对特别重要的信息系统进行持续、大量、有组织的网络攻击，对系统功能造成损害，导致特别严重的业务损失
数据安全事件	一般信息系统少量敏感信息或业务数据泄露，及时发现并控制，没有导致业务损失或导致较小的业务损失	重要信息系统少量敏感信息或业务数据泄露，或一般信息系统大量敏感信息或业务数据泄露，导致较大的业务损失，造成较大的社会危害	特别重要信息系统少量敏感信息或业务数据泄露，或重要信息系统大量敏感信息或重要业务数据泄露，导致严重的业务损失，造成重大的社会危害	特别重要的信息系统大量敏感信息或业务数据泄露，导致特别严重的业务损失，造成特别重大的社会危害
信息内容安全事件	信息系统出现轻微有害信息，及时发现并删除，没有造成不良影响或影响较小	重要信息系统出现轻微有害信息，或一般信息系统出现严重有害信息，经有限传播造成较大的社会危害	重要信息系统出现严重有害信息，或特别重要信息系统出现轻微有害信息，传播广泛，造成重大社会危害	特别重要的信息系统出现严重有害信息，传播广泛，造成特别重大的社会危害

表 A.1　网络安全事件类别和级别的关联关系示例（续）

事件类别	事件级别			
	一般事件 （四级）	较大事件 （三级）	重大事件 （二级）	特别重大事件 （一级）
设备设施故障事件	一般信息系统非主要设备设施故障，及时发现并解决，没有导致业务损失或导致较小的业务损失	重要信息系统非主要设备设施故障，或一般信息系统主要设备设施故障，故障持续一段时间，导致系统部分功能停止运行，导致较大的业务损失，或造成较大的社会危害	重要信息系统主要设备设施故障，导致系统大部分或全部功能停止运行，或特别重要信息系统非主要设备设施故障，使系统部分功能停止运行，持续时间较长，导致严重的业务损失，或造成重大的社会危害	特别重要信息系统主要设备设施故障，使系统大部分或全部功能停止运行，持续时间较长，导致特别严重的业务损失，或造成特别重大的社会危害
违规操作事件	单次对信息系统的非授权访问行为，没有导致业务损失或导致较小的业务损失	单次或多次对信息系统非授权访问行为，导致系统功能损害或数据泄露，导致较大的业务损失	单次或多次对重要信息系统非授权访问行为，导致系统功能损害或数据泄露，导致严重的业务损失	单次或多次对特别重要信息系统非授权访问行为，导致系统功能损害或数据泄露，导致特别严重的业务损失
安全隐患事件	一般信息系统存在已知的漏洞隐患，漏洞风险级别较低，及时发现并修复，没有造成业务损失或造成较小的业务损失	重要信息系统存在漏洞隐患，漏洞风险级别较低，或一般信息系统存在漏洞隐患，漏洞风险级别较高，处理不当造成较大的业务损失	特别重要信息系统或重要信息系统存在漏洞隐患，漏洞风险级别较高，处理不当导致严重的业务损失	—
异常行为事件	一般信息系统发现网络异常行为，及时发现并解决，没有导致业务损失或导致较小的业务损失	重要信息系统发现网络异常行为，对系统功能造成损害，导致较大的业务损失	特别重要信息系统发现网络异常行为，对系统功能造成损害，导致严重的业务损失	—
不可抗力事件	发生不可抗力事件，及时启动了备份系统或灾备中心，没有导致业务损失或导致较小的业务损失	发生不可抗力事件，对重要信息系统或一般信息系统导致较大的业务损失	发生不可抗力事件，对特别重要信息系统或重要信息系统导致严重的业务损失	发生不可抗力事件，对特别重要信息系统导致特别严重的业务损失

附 录 B
（规范性）
网络安全事件分类代码

B.1 编码方法

网络安全事件分类代码（以下简称“事件代码”）是对网络安全事件类别（以下简称“事件类别”）的编码，采用层次编码方法，代码由5位等长码构成，其中：

a） 第一层表示网络安全事件类（如：网络攻击事件），用两位阿拉伯数字（01～99）表示；

b） 第二层表示网络安全事件类下的子类（如：网络攻击事件中的网络钓鱼），用三位阿拉伯数字（001～999）表示。

编码结构如图B.1所示。

图 B.1 网络安全事件编码结构

B.2 分类代码表

网络安全事件分类代码见表B.1。

表 B.1 网络安全事件分类代码表

事件代码	事件类别	英文名称
01000	**恶意程序事件**	**malware incident**
01001	计算机病毒事件	computer virus incident
01002	网络蠕虫事件	network worm incident
01003	特洛伊木马事件	trojan horse incident
01004	僵尸网络事件	botnet incident
01005	恶意代码内嵌网页事件	malicious code embedded web page incident
01006	恶意代码宿主站点事件	malicious code hosting site incident
01007	勒索软件事件	ransomware incident
01008	挖矿病毒事件	miner virus incident
01009	混合攻击程序事件	blended attack incident
01999	其他恶意程序事件	other malware incidents
02000	**网络攻击事件**	**network attack incident**

表 B.1　网络安全事件分类代码表（续）

事件代码	事件类别	英文名称
02001	网络扫描探测事件	network scan detection incident
02002	网络钓鱼事件	network phishing incident
02003	漏洞利用事件	exploitation of vulnerability incident
02004	后门利用事件	exploitation of backdoor incident
02005	后门植入事件	implantation of backdoor incident
02006	凭据攻击事件	credential attack incident
02007	信号干扰事件	signal interference incident
02008	拒绝服务事件	denial of service incident
02009	网页篡改事件	webpage tampering incident
02010	暗链植入事件	implantation of dark chain incident
02011	域名劫持事件	DNS hijacking incident
02012	域名转嫁事件	DNS redirection incident
02013	DNS 污染事件	DNS cache poisoning incident
02014	WLAN 劫持事件	WLAN hijacking incident
02015	流量劫持事件	traffic hijacking incident
02016	BGP 劫持攻击事件	BGP hijacking attack incident
02017	广播欺诈事件	broadcast deception incident
02018	失陷主机事件	lost host incident
02019	供应链攻击事件	supply chain attack incident
02020	APT 事件	advanced persistent threat incident
02999	其他网络攻击事件	other network attack incidents
03000	**数据安全事件**	**data security incident**
03001	数据篡改事件	data tampering incident
03002	数据假冒事件	data counterfeiting incident
03003	数据泄露事件	data breach incident
03004	社会工程事件	social engineering incident
03005	数据窃取事件	data theft incident
03006	数据拦截事件	data interception incident
03007	位置检测事件	position detection incident

B.1 网络安全事件 （续）

事件代码	事件类别	英文名称
03008	数据投毒事件	data poisoning incident
03009	数据滥用事件	data abuse incident
03010	隐私侵犯事件	privacy violation incident
03011	数据损失事件	data loss incident
03999	其他数据安全事件	other network data security incidents
04000	**信息内容安全事件**	**information content safety incident**
04001	反动宣传事件	reactionary propaganda incident
04002	暴恐宣扬事件	violent terrorism propaganda incident
04003	色情传播事件	pornography dissemination incident
04004	虚假信息传播事件	false information dissemination incident
04005	权益侵害事件	infringement of rights incident
04006	信息滥发事件	information spamming incident
04007	网络欺诈事件	network fraud incident
04999	其他信息内容安全事件	other information content safety incidents
05000	**设备设施故障事件**	**equipment and facilities failure incident**
05001	技术故障事件	technical failure incident
05002	配套设施故障事件	supporting facilities failure incident
05003	物理损害事件	physical damage incident
05004	辐射干扰事件	radiation disturbance incident
05999	其他设备设施故障事件	other equipment and facilities failure incidents
06000	**违规操作事件**	**violating operation incident**
06001	权限滥用事件	abuse of rights incident
06002	权限伪造事件	forging of rights incident
06003	行为抵赖事件	denial of behavior incident
06004	故意违规操作事件	deliberate violating operation incident
06005	误操作事件	misoperation incident
06006	人员可用性破坏事件	breach of personnel availability incident
06007	资源未授权使用事件	unauthorized use of resources incident
06008	版权违反事件	breach of copyright incident

表 B.1　网络安全事件分类代码表（续）

事件代码	事件类别	英文名称
06999	其他违规操作事件	other violating operation incidents
07000	**安全隐患事件**	**security hazard incident**
07001	网络漏洞事件	cybersecurity vulnerability incident
07002	网络配置缺陷事件	cyber configuration flaw incident
07999	其他安全隐患事件	other security hazard incidents
08000	**异常行为事件**	**abnormal behavior incident**
08001	访问异常事件	access exception incident
08002	流量异常事件	traffic anomaly incident
08999	其他异常行为事件	other abnormal behavior incidents
09000	**不可抗力事件**	**force majeure incident**
09001	自然灾害事件	natural disaster incident
09002	事故灾难事件	accident disaster incident
09003	公共卫生事件	public health incident
09004	社会安全事件	social security incident
09999	其他不可抗力事件	other force majeure incidents
99999	**其他事件**	**other incidents**

参 考 文 献

[1] GB/T 20985.2—2020 信息 术 安全 术 信息安全事件管 第2部分:事件响 规划和准

[2] GB/T 22239—2019 信息安全 术 网络安全 级保护基本 求

[3] GB/T 29246—2017 信息 术 安全 术 信息安全管 体系 概 和词汇

[4] GB/T 31722—2015 信息 术 安全 术 信息安全风险管

[5] GB/T 35561—2017 突 事件分类 码

[6] GB/T 38645—2020 信息安全 术 网络安全事件 急演练

索　　引

A

暗链植入事件 …… 5.2.2,表 B.1
安全隐患事件 …… 5.1,5.2.7,表 A.1,表 B.1

B

版权违反事件 …… 5.2.6,表 B.1
暴恐宣扬事件 …… 5.2.4,表 B.1
　可　　事件 …… 5.1,5.2.9,表 A.1,表 B.1

E

恶意程序事件 …… 5.1,5.2.1,表 A.1,表 B.1
恶意代码内嵌网页事件 …… 5.2.1,表 B.1
恶意代码宿主站点事件 …… 5.2.1,表 B.1

F

反动宣传事件 …… 5.2.4,表 B.1
访　异常事件 …… 5.2.8,表 B.1
辐射干扰事件 …… 5.2.5,表 B.1

G

　　事件 …… 5.2.9,表 B.1
故意违规操作事件 …… 5.2.6,表 B.1
供应链攻击事件 …… 5.2.2,表 B.1
广播欺诈事件 …… 5.2.2,表 B.1

H

后门　用事件 …… 5.2.2,表 B.1
后门植入事件 …… 5.2.2,表 B.1
混合攻击程序事件 …… 5.2.1,表 B.1

J

　　机病毒事件 …… 5.2.1,表 B.1
技术故障事件 …… 5.2.5,表 B.1
僵尸网络事件 …… 5.2.1,表 B.1
拒绝服　事件 …… 5.2.2,表 B.1

L

勒索软件事件 …… 5.2.1,表 B.1

T

特洛伊木马事件 …… 5.2.1,表 B.1

W

挖矿病毒事件 …… 5.2.1,表 B.1
网络钓鱼事件 …… 5.2.2,表 B.1
网络攻击事件 …… 5.1,5.2.2,表 A.1,表 B.1
网络漏洞事件 …… 5.2.7,表 B.1
网络配置合规缺陷事件 …… 5.2.7,表 B.1
网络欺诈事件 …… 5.2.4,表 B.1
网络蠕虫事件 …… 5.2.1,表 B.1
网络扫描探测事件 …… 5.2.2,表 B.1
网页篡改事件 …… 5.2.2,表 B.1
违规操作事件 …… 5.1,5.2.6,表 A.1,表 B.1
位置检测事件 …… 5.2.3,表 B.1
误操作事件 …… 5.2.6,表 B.1
物理损害事件 …… 5.2.5,表 B.1

X

信号干扰事件 …… 5.2.2,表 B.1
信息滥发事件 …… 5.2.4,表 B.1
信息内容安全事件 …… 5.1,5.2.4,表 A.1,表 B.1
行为抵赖事件 …… 5.2.6,表 B.1
虚假信息传播事件 …… 5.2.4,表 B.1

Y

异常行为事件 …… 5.1,5.2.8,表 B.1
域名劫持事件 …… 5.2.2,表 B.1
域名转嫁事件 …… 5.2.2,表 B.1
隐私侵犯事件 …… 5.2.3,表 B.1

Z

自然灾害事件 …… 5.2.9,表 B.1
资源未授权使用事件 …… 5.2.6,表 B.1

APT 事件 …… 4,5.2.2,表 B.1
BGP 劫持攻击事件 …… 5.2.2,表 B.1
DNS 污染事件 …… 5.2.2,表 B.1
WLAN 劫持事件 …… 5.2.2,表 B.1