ICS 35，040
L 80

中华人民共和国国家标准化指导性技术文件

GB/Z 20986—2007

信息安全技术
信息安全事件分类分级指南

Information security technology-Guidelines for the category and classification of

Information security incidents

2007-06-14 发布

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会 发布

目　　次

前　言

（略）

引　言

信息安全事件的防范和处置是国家信息安全保障体系中的重要环节，也是重要的工作内容。信息安全事件的分类分级是快速有效处置信息安全事件的基础之一。本指导性技术文件编制的目的是：

1) 促进安全事件信息的交流和共享；
2) 提高安全事件通报和应急处理的自动化程度；
3) 提高安全事件通报和应急处理的效率和效果；
4) 利于安全事件的统计分析；
5) 利于安全事件严重程度的确定。

信息安全技术
信息安全事件分类分级指南

1 范围

本指导性技术文件为信息安全事件的分类分级提供指导，用于信息安全事件的防范与处置，为事前准备、事中应对、事后处理提供一个基础指南，可供信息系统和基础信息传输网络的运营和使用单位以及信息安全主管部门参考使用。

2 术语和定义

下列术语和定义适用于本指导性技术文件。

2.1

信息系统 information system

由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

2.2

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。

3 缩略语

下列缩略语适用于本指导性技术文件。

MI：有害程序事件（Malware Incidents）

CVI：计算机病毒事件（Computer Virus Incidents）

WI：蠕虫事件（Worms Incidents）

THI：特洛伊木马事件（Trojan Horses Incidents）

BI：僵尸网络事件（Botnets Incidents）

BAI：混合攻击程序事件（Blended Attacks Incidents）

WBPI：网页内嵌恶意代码事件（Web Browser Plug-Ins Incidents）

NAI：网络攻击事件（Network Attacks Incidents）

DOSAI：拒绝服务攻击事件（Denial of Service Attacks Incidents）

BDAI：后门攻击事件（Backdoor Attacks Incidents）

VAI：漏洞攻击事件（Vulnerability Attacks Incidents）

NSEI：网络扫描窃听事件（Network Scan & Eavesdropping Incidents）

PI：网络钓鱼事件（Phishing Incidents）

II：干扰事件（Interference Incidents）

IDI：信息破坏事件（Information Destroy Incidents）

IAI：信息篡改事件（Information Alteration Incidents）

IMI：信息假冒事件（Information Masquerading Incidents）

ILEI：信息泄漏事件（Information Leakage Incidents）

III：信息窃取事件（Information Interception Incidents）

ILOI：信息丢失事件（Information Loss Incidents）

ICSI：信息内容安全事件（Information Content Security Incidents）

FF：设备设施故障（Facilities Faults）

SHF：软硬件自身故障（Software and Hardware Faults）

PSFF：外围保障设施故障（Periphery Safeguarding Facilities Faults）

MDA：人为破坏事故（Man-made Destroy Accidents）

DI：灾害性事件（Disaster Incidents）

OI：其他事件（Other Incidents）

4 信息安全事件分类

4.1 考虑要素与基本分类

信息安全事件可以是故意、过失或非人为原因引起的。本指导性技术文件综合考虑信息安全事件的起因、表现、结果等，对信息安全事件进行分类。

信息安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他信息安全事件等 7 个基本分类，每个基本分类分别包括若干个子类。

4.2 事件分类

4.2.1 有害程序事件（MI）

有害程序事件是指蓄意制造、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。有害程序是指插入到信息系统中的一段程序，有害程序危害系统中数据、应用程序或操作系统的保密性、完整性或可用性，或影响信息系统的正常运行。

有害程序事件包括计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合攻击程序事件、网页内嵌恶意代码事件和其它有害程序事件等 7 个子类，说明如下：

a) 计算机病毒事件（CVI）是指蓄意制造、传播计算机病毒，或是因受到计算机病毒影响而导致的信息安全事件。计算机病毒是指编制或者在计算机程序中插入的一组计算机指令或者程序代码，它可以破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制；

b) 蠕虫事件（WI）是指蓄意制造、传播蠕虫，或是因受到蠕虫影响而导致的信息安全事件。蠕虫是指除计算机病毒以外，利用信息系统缺陷，通过网络自动复制并传播的有害程序；

c) 特洛伊木马事件（THI）是指蓄意制造、传播特洛伊木马程序，或是因受到特洛伊木马程序影响而导致的信息安全事件。特洛伊木马程序是指伪装在信息系统中的一种有害程序，具有控制该信息系统或进行信息窃取等对该信息系统有害的功能；

d) 僵尸网络事件（BI）是指利用僵尸工具软件，形成僵尸网络而导致的信息安全事件。僵尸网络是指网络上受到黑客集中控制的一群计算机，它可以被用于伺机发起网络攻击，进行信息窃取或传播木马、蠕虫等其他有害程序；

e) 混合攻击程序事件（BAI）是指蓄意制造、传播混合攻击程序，或是因受到混合攻击程序影响而导致的信息安全事件。混合攻击程序是指利用多种方法传播和感染其它系统的有害程序，可能兼有计算机病毒、蠕虫、木马或僵尸网络等多种特征。混合攻击程序事件也可以是一系列有害程序综合作用的结果，例如一个计算机病毒或蠕虫在侵入系统后安装木马程序等；

f) 网页内嵌恶意代码事件（WBPI）是指蓄意制造、传播网页内嵌恶意代码，或是因受到网页内嵌恶意代码影响而导致的信息安全事件。网页内嵌恶意代码是指内嵌在网页中，未经允许由浏览器执行，影响信息系统正常运行的有害程序；

g) 其它有害程序事件（OMI）是指不能包含在以上 6 个子类之中的有害程序事件。

4.2.2 网络攻击事件（NAI）

网络攻击事件是指通过网络或其他技术手段，利用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信息系统实施攻击，并造成信息系统异常或对信息系统当前运行造成潜在危害的信息安全

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、网络钓鱼事件、干扰事件和其他网络攻击事件等 7 个子类，说明如下：

a) 拒绝服务攻击事件（DOSAI）是指利用信息系统缺陷、或通过暴力攻击的手段，以大量消耗信息系统的 CPU、内存、磁盘空间或网络带宽等资源，从而影响信息系统正常运行为目的的信息安全事件；
b) 后门攻击事件（BDAI）是指利用软件系统、硬件系统设计过程中留下的后门或有害程序所设置的后门而对信息系统实施的攻击的信息安全事件；
c) 漏洞攻击事件（VAI）是指除拒绝服务攻击事件和后门攻击事件之外，利用信息系统配置缺陷、协议缺陷、程序缺陷等漏洞，对信息系统实施攻击的信息安全事件；
d) 网络扫描窃听事件（NSEI）是指利用网络扫描或窃听软件，获取信息系统网络配置、端口、服务、存在的脆弱性等特征而导致的信息安全事件；
e) 网络钓鱼事件（PI）是指利用欺骗性的计算机网络技术，使用户泄漏重要信息而导致的信息安全事件。例如，利用欺骗性电子邮件获取用户银行帐号密码等；
f) 干扰事件（II）是指通过技术手段对网络进行干扰，或对广播电视有线或无线传输网络进行插播，对卫星广播电视信号非法攻击等导致的信息安全事件；
g) 其他网络攻击事件（ONAI）是指不能被包含在以上 6 个子类之中的网络攻击事件。

4.2.3 信息破坏事件（IDI）

信息破坏事件是指通过网络或其他技术手段，造成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。

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、信息丢失事件和其它信息破坏事件等 6 个子类，说明如下：

a) 信息篡改事件（IAI）是指未经授权将信息系统中的信息更换为攻击者所提供的信息而导致的信息安全事件，例如网页篡改等导致的信息安全事件；
b) 信息假冒事件（IMI）是指通过假冒他人信息系统收发信息而导致的信息安全事件，例如网页假冒等导致的信息安全事件；
c) 信息泄漏事件（ILEI）是指因误操作、软硬件缺陷或电磁泄漏等因素导致信息系统中的保密、敏感、个人隐私等信息暴露于未经授权者而导致的信息安全事件；
d) 信息窃取事件（III）是指未经授权用户利用可能的技术手段恶意主动获取信息系统中信息而导致的信息安全事件；
e) 信息丢失事件（ILOI）是指因误操作、人为蓄意或软硬件缺陷等因素导致信息系统中的信息丢失而导致的信息安全事件；
f) 其它信息破坏事件（OIDI）是指不能被包含在以上 5 个子类之中的信息破坏事件。

4.2.4 信息内容安全事件（ICSI）

信息内容安全事件是指利用信息网络发布、传播危害国家安全、社会稳定和公共利益的内容的安全事件。

信息内容安全事件包括以下 4 个子类，说明如下：

a) 违反宪法和法律、行政法规的信息安全事件；
b) 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；
c) 组织串连、煽动集会游行的信息安全事件；
d) 其他信息内容安全事件等 4 个子类。

4.2.5 设备设施故障（FF）

设备设施故障是指由于信息系统自身故障或外围保障设施故障而导致的信息安全事件，以及人为的使用非技术手段有意或无意的造成信息系统破坏而导致的信息安全事件。

设备设施故障包括软硬件自身故障、外围保障设施故障、人为破坏事故、和其它设备设施故障等4个子类，说明如下：

a) 软硬件自身故障（SHF）是指因信息系统中硬件设备的自然故障、软硬件设计缺陷或者软硬件运行环境发生变化等而导致的信息安全事件；

b) 外围保障设施故障（PSFF）是指由于保障信息系统正常运行所必须的外部设施出现故障而导致的信息安全事件，例如电力故障、外围网络故障等导致的信息安全事件；

c) 人为破坏事故（MDA）是指人为蓄意的对保障信息系统正常运行的硬件、软件等实施窃取、破坏造成的信息安全事件；或由于人为的遗失、误操作以及其他无意行为造成信息系统硬件、软件等遭到破坏，影响信息系统正常运行的信息安全事件；

d) 其它设备设施故障（IF-OT）是指不能被包含在以上3个子类之中的设备设施故障而导致的信息安全事件。

4.2.6 灾害性事件（DI）

灾害性事件是指由于不可抗力对信息系统造成物理破坏而导致的信息安全事件。

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。

4.2.7 其他事件（OI）

其他事件类别是指不能归为以上6个基本分类的信息安全事件。

5 信息安全事件分级

5.1 分级考虑要素

5.1.1 概述

对信息安全事件的分级主要考虑三个要素：信息系统的重要程度、系统损失和社会影响。

5.1.2 信息系统的重要程度

信息系统的重要程度主要考虑信息系统所承载的业务对国家安全、经济建设、社会生活的重要性以及业务对信息系统的依赖程度，划分为特别重要信息系统、重要信息系统和一般信息系统。

5.1.3 系统损失

系统损失是指由于信息安全事件对信息系统的软硬件、功能及数据的破坏，导致系统业务中断，从而给事发组织所造成的损失，其大小主要考虑恢复系统正常运行和消除安全事件负面影响所需付出的代价，划分为特别严重的系统损失、严重的系统损失、较大的系统损失和较小的系统损失，说明如下：

a) 特别严重的系统损失：造成系统大面积瘫痪，使其丧失业务处理能力，或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安全事件负面影响所需付出的代价十分巨大，对于事发组织是不可承受的；

b) 严重的系统损失：造成系统长时间中断或局部瘫痪，使其业务处理能力受到极大影响，或系统关键数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价巨大，但对于事发组织是可承受的；

c) 较大的系统损失：造成系统中断，明显影响系统效率，使重要信息系统或一般信息系统业务处理能力受到影响，或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安全事件负面影响所需付出的代价较大，但对于事发组织是完全可以承受的；

d) 较小的系统损失：造成系统短暂中断，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安全事件负面影响所需付出的代价较小。

5.1.4 社会影响

社会影响是指信息安全事件对社会所造成影响的范围和程度，其大小主要考虑国家安全、社会秩序、经济建设和公众利益等方面的影响，划分为特别重大的社会影响、重大的社会影响、较大的社会影响和一般的社会影响，说明如下：

a) 特别重大的社会影响：波及到一个或多个省市的大部分地区，极大威胁国家安全，引起社会动荡，对经济建设有极其恶劣的负面影响，或者严重损害公众利益；
b) 重大的社会影响：波及到一个或多个地市的大部分地区，威胁到国家安全，引起社会恐慌，对经济建设有重大的负面影响，或者损害到公众利益；
c) 较大的社会影响：波及到一个或多个地市的部分地区，可能影响到国家安全，扰乱社会秩序，对经济建设有一定的负面影响，或者影响到公众利益；
d) 一般的社会影响：波及到一个地市的部分地区，对国家安全、社会秩序、经济建设和公众利益基本没有影响，但对个别公民、法人或其他组织的利益会造成损害。

5.2 事件分级

5.2.1 概述

根据信息安全事件的分级考虑要素，将信息安全事件划分为四个级别：特别重大事件、重大事件、较大事件和一般事件。

5.2.2 特别重大事件（Ⅰ级）

特别重大事件是指能够导致特别严重影响或破坏的信息安全事件，包括以下情况：

a) 会使特别重要信息系统遭受特别严重的系统损失；
b) 产生特别重大的社会影响。

5.2.3 重大事件（Ⅱ级）

重大事件是指能够导致严重影响或破坏的信息安全事件，包括以下情况：

a) 会使特别重要信息系统遭受严重的系统损失、或使重要信息系统遭受特别严重的系统损失；
b) 产生的重大的社会影响。

5.2.4 较大事件（Ⅲ级）

较大事件是指能够导致较严重影响或破坏的信息安全事件，包括以下情况：

a) 会使特别重要信息系统遭受较大的系统损失、或使重要信息系统遭受严重的系统损失、一般信息信息系统遭受特别严重的系统损失；
b) 产生较大的社会影响。

5.2.5 一般事件（Ⅳ级）

一般事件是指不满足以上条件的信息安全事件，包括以下情况：

a) 会使特别重要信息系统遭受较小的系统损失、或使重要信息系统遭受较大的系统损失，一般信息系统遭受严重或严重以下级别的系统损失；
b) 产生一般的社会影响。