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

本指导性技术文件由全国信息安全标准化技术委员会提出并归口；

本指导性技术文件起草单位：北京知识安全工程中心、国家网络与信息安全信息通报中心。

本指导性技术文件主要起草人：赵战生、徐国爱、黄小苏、王连强、高志民。

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)