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 20985—2007

信息技术　安全技术
信息安全事件管理指南

Information technology—Security techniques—
Information security incident management guide

(ISO/IEC TR 18044:2004,MOD)

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

本指导性技术文件修改采用 ISO/IEC TR 18044:2004《信息技术　安全技术　信息安全事件管理指南》。

考虑到我国国家标准的编写要求,以及与其他信息安全事件相关标准技术内容的协调性,本指导性技术文件在采用国际标准时,对部分内容进行了修改。其中,技术性差异用垂直单线标识在它们所涉及的条款的页边空白处。在附录 C 中给出了技术性差异及其原因的一览表以供参考。

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:中国电子技术标准化研究所、北京同方信息安全股份有限公司、北京知识安全工程中心、北京邮电大学。

本指导性技术文件主要起草人:上官晓丽、闵京华、赵战生、王连强、徐国爱。

引　言

目前，没有任何一种具有代表性的信息安全策略或防护措施，能够对信息、信息系统、服务或网络提供绝对的保护。即使采取了防护措施，仍可能存在残留的弱点，使得信息安全防护变得无效，从而导致信息安全事件发生，并对组织的业务运行直接或间接产生负面影响。此外，以前未被认识到的威胁也可能会发生。组织如果对这些事件没有作好充分的应对准备，其任何实际响应措施的效率都会大打折扣，甚至还可能加大潜在的业务负面影响的程度。因此，对于任何一个重视信息安全的组织来说，采用一种结构严谨、计划周全的方法来处理以下工作十分必要：

- 发现、报告和评估信息安全事件；
- 对信息安全事件做出响应，包括启动适当的事件防护措施来预防和降低事件影响，以及从事件影响中恢复（例如，在支持和业务连续性规划方面）；
- 从信息安全事件中吸取经验教训，制定预防措施，并且随着时间的变化，不断改进整个的信息安全事件管理方法。

信息技术　安全技术
信息安全事件管理指南

1　范围

本指导性技术文件描述了信息安全事件的管理过程。提供了规划和制定信息安全事件管理策略和方案的指南。给出了管理信息安全事件和开展后续工作的相关过程和规程。

本指导性技术文件可用于指导信息安全管理者，信息系统、服务和网络管理者对信息安全事件的管理。

2　规范性引用文件

下列文件中的条款通过本指导性技术文件的引用而成为本指导性技术文件的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本指导性技术文件，然而，鼓励根据本指导性技术文件达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本指导性技术文件。

GB/T 19716—2005　信息技术　信息安全管理实用规则(ISO/IEC 17799:2000，MOD)

GB/Z 20986—2007　信息安全技术　信息安全事件分类分级指南

ISO/IEC 13335-1:2004　信息技术　安全技术　信息和通信技术安全管理　第1部分：信息和通信技术安全管理的概念和模型

3　术语和定义

GB/T 19716—2005、ISO/IEC 13335-1:2004 中确立的以及下列术语和定义适用于本指导性技术文件。

3.1

业务连续性规划　business continuity planning

这样的一个过程，即当有任何意外或有害事件发生，且对基本业务功能和支持要素的连续性造成负面影响时，确保运行的恢复得到保障。该过程还应确保恢复工作按指定优先级、在规定的时间期限内完成，且随后将所有业务功能及支持要素恢复到正常状态。

这一过程的关键要素必须确保具有必要的计划和设施，且经过测试，它们包含信息、业务过程、信息系统和服务、语音和数据通信、人员和物理设施等。

3.2

信息安全事态　information security event

被识别的一种系统、服务或网络状态的发生，表明一次可能的信息安全策略违规或某些防护措施失效，或者一种可能与安全相关但以前不为人知的一种情况。

3.3

信息安全事件　information security incident

由单个或一系列意外或有害的信息安全事态所组成，极有可能危害业务运行和威胁信息安全。

3.4

信息安全事件响应组(ISIRT)Information Security Incident Response Team

由组织中具备适当技能且可信的成员组成的一个小组，负责处理与信息安全事件相关的全部工作。