

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

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)

中华人民共和国
国家标准化指导性技术文件
信息技术 安全技术
信息安全事件管理指南
GB/Z 20985—2007

*

中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045

网址 www.spc.net.cn

电话:68523946 68517548

中国标准出版社秦皇岛印刷厂印刷

各地新华书店经销

*

开本 880×1230 1/16 印张 3 字数 80 千字

2007年9月第一版 2007年9月第一次印刷

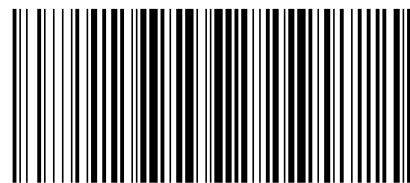
*

书号:155066·1-29872 定价 32.00 元

如有印装差错 由本社发行中心调换

版权专有 侵权必究

举报电话:(010)68533533



GB/Z 20985—2007

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	III
引言	IV
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 背景	2
5.1 目标	2
5.2 过程	2
6 信息安全事件管理方案的益处及需要应对的关键问题	4
6.1 信息安全事件管理方案的益处	4
6.2 关键问题	6
7 规划和准备	9
7.1 概述	9
7.2 信息安全事件管理策略	9
7.3 信息安全事件管理方案	11
7.4 信息安全和风险管理策略	13
7.5 ISIRT 的建立	13
7.6 技术和其他支持	14
7.7 意识和培训	15
8 使用	16
8.1 概述	16
8.2 关键过程的概述	16
8.3 发现和报告	18
8.4 事态/事件评估和决策	19
8.5 响应	21
9 评审	26
9.1 概述	26
9.2 进一步的法律取证分析	26
9.3 经验教训	26
9.4 确定安全改进	26
9.5 确定方案改进	27
10 改进	27
10.1 概述	27
10.2 安全风险分析和改进	27
10.3 改善安全状况	27
10.4 改进方案	27
10.5 其他改进	27

附录 A(资料性附录) 信息安全事态和事件报告单示例	28
附录 B(资料性附录) 信息安全事件评估要点指南示例	35
附录 C(资料性附录) 本指导性技术文件与 ISO/IEC TR 18044:2004 的技术性差异及其原因	38
参考文献	39

参 考 文 献

- [1] ISO/IEC TR 13335-3 Information technology—Guidelines for the management of IT Security—Part 3: Techniques for the management of IT Security
ISO/IEC TR 13335-3《信息技术 IT 安全管理指南 第 3 部分:IT 安全管理技巧》
- [2] ISO/IEC TR 15947:2002 Information technology—Security techniques—IT intrusion detection framework
ISO/IEC TR 15947:2002《信息技术 安全技术 IT 入侵检测框架》
- [3] ISO/IEC 18028 (all parts) IT security techniques—IT network security
ISO/IEC 18028《信息技术 安全技术 IT 网络安全》(所有部分)
- [4] ISO/IEC 18043 IT Security techniques—Selection, Deployment and Operations of Intrusion Detection Systems (IDS) (document type subject to NP approval on SC27 N4029 by 2004-09-24)
ISO/IEC 18043《信息技术 安全技术 入侵检测系统(IDS)的选择、配置和操作》
- [5] ISO/IEC Guide 73:2002 Risk management—Vocabulary—Guidelines for use in standards
ISO/IEC 指南 73:2002《风险管理 词汇 标准使用指南》
- [6] Internet Engineering Task Force (IETF) Site Security Handbook,
[http://www.ietf.org/rfc/rfc2196.txt? number=2196](http://www.ietf.org/rfc/rfc2196.txt?number=2196)
《互联网工程任务组(IETF)网站安全手册》, [http://www.ietf.org/rfc/rfc2196.txt? number=2196](http://www.ietf.org/rfc/rfc2196.txt?number=2196)
- [7] Expectations for Computer Security Incident Response—Best Practice, June 98,
<ftp://ftp.isi.edu/in-notes/rfc2350.txt>
《对计算机安全事件响应的期望——最佳实践》, 1998 年 6 月, <ftp://ftp.isi.edu/in-notes/rfc2350.txt>
- [8] NIST Special Publication 800-3 Nov'91, Establishing a Computer Incident Response Capability (CSIRC), <http://csrc.nist.gov/publications/nistpubs/800-3/800-3.pdf>
NIST SP 800-3《建立计算机事件响应能力(CSIRC)》, 1991 年 11 月,
<http://csrc.nist.gov/publications/nistpubs/800-3/800-3.pdf>
- [9] ISO/IEC JTC1 SC27 SD6, Glossary
ISO/IEC JTC1/SC27 SD6《术语集》