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

GB/Z 20985—2007

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

GB/Z 20985-2007

目　　次

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
《互联网工程任务组(IETF)网站安全手册》,http://www.ietf.org/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》