ICS 35.020
L 09

中华人民共和国国家标准

GB/T 20282—2006

信息安全技术
信息系统安全工程管理要求

Information security technology—
Information system security engineering management requirements

2006-05-31 发布　　2006-12-01 实施

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

中 华 人 民 共 和 国
国 家 标 准
信息安全技术
信息系统安全工程管理要求
GB/T 20282—2006
*
中国标准出版社出版发行
北京西城区复兴门外三里河北街16号
邮政编码:100045
http://www.spc.net.cn
电话:(010)51299090、68522006
2006年9月第一版
*
书号:155066·1-27972

目　　次

前　言

本标准的附录 A 是资料性附录。

本标准由信息安全标准化技术委员会提出并归口。

本标准起草单位：中国电子科技集团第三十研究所、上海三零卫士信息安全有限公司、上海标准化研究院。

本标准主要起草人：张建军、魏忠、叶铭、陈长松、孔一童。

信息安全技术
信息系统安全工程管理要求

1 范围

本标准规定了信息系统安全工程(以下简称安全工程)的管理要求,是对信息系统安全工程中所涉及到的需求方、实施方与第三方工程实施的指导,各方可以此为依据建立安全工程管理体系。

本标准按照GB 17859—1999划分的五个安全保护等级,规定了信息系统安全工程管理的不同要求。

本标准适用于信息系统的需求方和实施方的安全工程管理,其他有关各方也可参照使用。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。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标准,然而,鼓励根据本标准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标准。

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 20269—2006 信息安全技术 信息系统安全管理要求

GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求

3 术语和定义

下列术语和定义适用于本标准。

3.1

安全工程 security engineering

为确保信息系统的保密性、完整性、可用性等目标而进行的系统工程过程。

3.2

安全工程的生存周期 security engineering lifecycle

在整个信息系统生存周期中执行的安全工程活动包括:概念形成、概念开发和定义、验证与确认、工程实施开发与制造、生产与部署、运行与支持和终止。

3.3

安全工程指南 security engineering guide

由工程组做出的有关如何选择工程体系结构、设计与实现的指导性信息。

3.4

脆弱性 vulnerability

能够被某种威胁利用的某个或某组资产的弱点。

3.5

风险 risk

某种威胁会利用一种资产或若干资产的脆弱性使这些资产损失或破坏的可能性。

3.6

需求方 owner

信息系统安全工程建设的拥有者或组织者。