ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20274.1—2006

信息安全技术
信息系统安全保障评估框架
第1部分:简介和一般模型

Information security technology—
Evaluation framework for information systems security assurance—
Part 1:Introduction and general model

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

目　　次

前　言

GB/T 20274《信息安全技术　信息系统安全保障评估框架》分为四个部分：

——第1部分：简介和一般模型

——第2部分：技术保障

——第3部分：管理保障

——第4部分：工程保障

本部分的附录A和附录B为规范性附录，附录C和附录D为资料性附录。

本部分由全国信息安全标准化技术委员会提出并归口。

本部分起草单位：中国信息安全产品测评认证中心。

本标准主要起草人：吴世忠、王海生、陈晓桦、王贵驷、李守鹏、江常青、彭勇、张利、班晓芳、李静、王庆、邹琪、钱伟明、江典盛、陆丽、姚轶崭、孙成昊、门雪松、杜宇鸽、杨再山。

引　言

0.1　信息系统安全保障的含义

信息系统安全保障是在信息系统的整个生命周期中，通过对信息系统的风险分析，制定并执行相应的安全保障策略，从技术、管理、工程和人员等方面提出安全保障要求，确保信息系统的保密性、完整性和可用性，降低安全风险到可接受的程度，从而保障系统实现组织机构的使命。信息系统安全保障涵盖以下几个方面：

a) 信息系统安全保障应贯穿信息系统的整个生命周期，包括规划组织、开发采购、实施交付、运行维护和废弃5个阶段，以获得信息系统安全保障能力的持续性。

b) 信息系统安全保障不仅涉及安全技术，还应综合考虑安全管理、安全工程和人员安全等，以全面保障信息系统安全。在安全技术上，不仅要考虑具体的产品和技术，更要考虑信息系统的安全技术体系架构；在安全管理上，不仅要考虑基本安全管理实践，更要结合组织的特点建立相应的安全保障管理体系，形成长效和持续改进的安全管理机制；在安全工程上，不仅要考虑信息系统建设的最终结果，更要结合系统工程的方法，注重工程过程各个阶段的规范化实施；在人员安全上，要考虑与信息系统相关的所有人员包括规划者、设计者、管理者、运营维护者、评估者、使用者等的安全意识以及安全专业技能和能力等。

c) 信息系统安全保障是基于过程的保障。通过风险识别、风险分析、风险评估、风险控制等风险管理活动，降低信息系统的风险，从而实现信息系统安全保障。

d) 信息系统安全保障的目的不仅是保护信息和资产的安全，更重要是通过保障信息系统安全保障信息系统所支持的业务的安全，从而达到实现组织机构使命的目的。

e) 信息系统安全保障是主观和客观的结合。通过在技术、管理、工程和人员方面客观地评估安全保障措施，向信息系统的所有者提供其现有安全保障工作是否满足其安全保障目标的信心。因此，它是一种通过客观证据向信息系统所有者提供主观信心的活动，是主观和客观综合评估的结果。

f) 保障信息系统安全不仅是系统所有者自身的职责，而且需要社会各方参与，包括电信、电力、国家信息安全基础设施等提供的支撑。保障信息系统安全不仅要满足系统所有者自身的安全需求，而且要满足国家相关法律、政策的要求，包括为其他机构或个人提供保密、公共安全和国家安全等社会职责。

0.2　信息系统安全保障评估框架的编制目的和意义

本标准不仅可以作为信息系统安全保障评估的基础标准，也可以为从事信息系统安全保障工作的所有相关方（包括设计开发者、工程实施者、评估者、认证认可者等）提供一种标准化、规范化的通用描述语言、结构和方法。本标准是GB/T 18336—2001在信息系统领域的扩展和补充，它是以GB/T 18336—2001为基础，吸收其科学方法和结构，将GB/T 18336—2001从产品和产品系统扩展到信息技术系统，并进一步同其他国内外信息系统安全领域的标准和规范进行结合、扩展和补充，以形成描述和评估信息系统安全保障内容和能力的通用框架。在本标准中，信息系统作为评估对象，不仅涉及具体产品和产品系统，而且还包含信息系统运行环境的管理、工程等，是用于采集、处理、存储、传输、分发和部署信息的整个基础设施、组织结构、人员等的总和。

本标准属于信息系统安全保障的基础性和框架性标准，定义了信息系统安全保障的主要的通用要

求，制定此标准的意义在于：

a） 为信息系统安全的设计、实施、建设、测评、审核提供规范的、通用的描述语言。

b） 有利于信息系统所有者编制其信息系统的安全保障要求。

c） 有利于信息系统安全集成商和安全服务提供商提供更为科学规范化的设计和服务，促进信息安全市场的发展。

d） 有利于有关行政管理部门、执法机构、测评认证机构对信息系统进行安全检查、检测、审计、评估和认证。

信息安全技术
信息系统安全保障评估框架
第1部分:简介和一般模型

1 范围

GB/T 20274 描述了信息系统安全保障的模型,建立了信息系统安全保障的框架,从信息系统安全技术、管理和工程三方面制定了信息系统的通用安全保障要求。

GB/T 20274 的本部分给出了信息系统安全保障的基本概念和模型,并建立了信息系统安全保障框架。

本部分适用于从事信息系统安全保障工作的所有相关方,包括设计开发者、工程实施者、评估者、认证认可者等。

本部分不适用于以下方面:

a) 人员技能和能力的评估,但对人员安全的要求在管理保障中体现;

b) 系统评估方法学;

c) 密码算法固有质量的评价。

2 规范性引用文件

下列文件中的条款通过 GB/T 20274 的本部分的引用而成为本部分的条款。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部分,然而,鼓励根据本部分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部分。

GB/T 9387.2—1995 信息处理系统 开放系统互连 基本参考模型 第2部分:安全体系结构(idt ISO 7498-2:1989)

GB/T 18336—2001 信息技术 安全技术 信息技术安全性评估准则(idt ISO/IEC 15408:1999)

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本部分。

3.1.1

访问控制 access control

防止对资源的未授权使用,包括防止以未授权方式使用某一资源。

[GB/T 9837.2—1995,3.3.1]

3.1.2

可追究性 accountability

这样一种性质,它确保一个实体的作用可以被独一无二地跟踪到该实体。

[GB/T 9837.2—1995,3.3.3]

3.1.3

资产 asset

信息系统安全策略中所保护的信息或资源。