



中华人民共和国国家标准

GB/T 20274.2—2008

信息安全技术 信息系统安全保障评估框架 第2部分：技术保障

Information security technology—
Evaluation framework for information systems security assurance—
Part 2: Technical assurance

2008-07-18 发布

2008-12-01 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 保 障 评 估 框 架
第 2 部 分 : 技 术 保 障
GB/T 20274.2—2008

*

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 6.25 字数 184 千字
2008年11月第一版 2008年11月第一次印刷

*

书号: 155066·1-34998

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

目 次

前言	V
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 本部分的结构	1
5 信息安全技术保障	2
5.1 安全技术保障概述	2
5.2 安全技术体系架构能力级	2
5.3 安全技术保障控制要求范例	2
6 信息安全技术保障控制结构	5
6.1 综述	5
6.2 组件分类	9
7 FAU类:安全审计	10
7.1 安全审计自动响应(FAU_ARP)	11
7.2 安全审计数据产生(FAU_GEN)	11
7.3 安全审计分析(FAU_SAA)	12
7.4 安全审计查阅(FAU_SAR)	14
7.5 安全审计事件选择(FAU_SEL)	15
7.6 安全审计事件存储(FAU_STG)	15
8 FCO类:通信	17
8.1 原发抗抵赖(FCO_NRO)	17
8.2 接收抗抵赖(FCO_NRR)	18
9 FCS类:密码支持	19
9.1 密钥管理(FCS_CKM)	20
9.2 密码运算(FCS_COP)	21
10 FDP类:用户数据保护	22
10.1 访问控制策略(FDP_ACC)	24
10.2 访问控制功能(FDP_ACF)	24
10.3 数据鉴别(FDP_DAU)	25
10.4 输出到TSF控制之外(FDP_ETC)	26
10.5 信息流控制策略(FDP_IFC)	27
10.6 信息流控制功能(FDP_IFF)	28
10.7 从TSF控制之外输入(FDP_ITC)	30
10.8 TOE内部传输(FDP_ITT)	32
10.9 残余信息保护(FDP_RIP)	33
10.10 反转(FDP_ROL)	34
10.11 存储数据的完整性(FDP_SDI)	35
10.12 TSF间用户数据传输的保密性保护(FDP_UCT)	35

10.13	TSF 间用户数据传输的完整性保护(FDP_UIT)	36
11	FIA 类:标识和鉴别	38
11.1	鉴别失败(FIA_AFL)	39
11.2	用户属性定义(FIA_ATD)	39
11.3	秘密的规范(FIA_SOS)	40
11.4	用户鉴别(FIA_UAU)	40
11.5	用户标识(FIA_UID)	43
11.6	用户_主体绑定(FIA_USB)	44
12	FMT 类:安全管理	44
12.1	TSF 中功能的管理(FMT_MOF)	45
12.2	安全属性的管理(FMT_MSA)	46
12.3	TSF 数据的管理(FMT_MTD)	47
12.4	撤消(FMT_REV)	48
12.5	安全属性到期(FMT_SAE)	49
12.6	安全管理角色(FMT_SMR)	50
13	FPR 类:隐秘	51
13.1	匿名(FPR_ANO)	51
13.2	假名(FPR_PSE)	52
13.3	不可关联性(FPR_UNL)	53
13.4	不可观察性(FPR_UNO)	54
14	FPT 类:TSF 保护	55
14.1	根本抽象机测试(FPT_AMT)	57
14.2	失败保护(FPT_FLS)	57
14.3	输出 TSF 数据的可用性(FPT_ITA)	57
14.4	输出 TSF 数据的保密性(FPT_ITC)	58
14.5	输出 TSF 数据的完整性(FPT_ITD)	58
14.6	TOE 内 TSF 数据的传输(FPT_ITT)	59
14.7	TSF 物理保护(FPT_PHP)	61
14.8	可信恢复(FPT_RCV)	62
14.9	重放检测(FPT_RPL)	64
14.10	参照仲裁(FPT_RVM)	64
14.11	域分离(FPT_SEP)	65
14.12	状态同步协议(FPT_SSP)	66
14.13	时间戳(FPT_STM)	67
14.14	TSF 间 TSF 数据的一致性(FPT_TDC)	67
14.15	TOE 内 TSF 数据复制的一致性(FPT_TRC)	68
14.16	TSF 自检(FPT_TST)	68
15	FRU 类:资源利用	69
15.1	容错(FRU_FLT)	70
15.2	服务优先级(FRU_PRS)	70
15.3	资源分配(FRU_RSA)	71
16	FTA 类:TOE 访问	72
16.1	可选属性范围限定(FTA_LSA)	72

16.2	多重并发会话限定(FTA_MCS)	73
16.3	会话锁定(FTA_SSL)	74
16.4	TOE 访问旗标	75
16.5	TOE 访问历史(FTA_TAH)	76
16.6	TOE 会话建立(FTA_TSE)	76
17	TP 类;可信路径/信道	77
17.1	TSF 间可信信道(FTP_ITC)	77
17.2	可信路径(FTP_TRP)	78
18	安全技术架构能力成熟度级	78
18.1	概述	78
18.2	安全技术架构能力成熟度级说明	79
附录 A (资料性附录) 安全技术要求应用注释		81
A.1	注释的结构	81
A.1.1	类结构	81
A.1.2	子类结构	81
A.1.3	组件结构	82
A.2	依赖关系表	82
附录 B (资料性附录) 分层多点信息系统安全体系结构		89
B.1	概述	89
B.2	信息技术系统 TOE 的分析模型	89
B.3	分层多点安全技术体系架构介绍	90
参考文献		92
图 1	安全技术保障控制要求范例(单个 TOE)	2
图 2	分布式 TOE 内的安全功能图	3
图 3	用户数据和 TSF 数据的关系	5
图 4	“鉴别数据”和“秘密”的关系	5
图 5	安全技术保障控制类结构	6
图 6	安全技术保障控制子类结构	6
图 7	安全技术保障控制组件结构	7
图 8	示范类分解图	9
图 9	安全审计类分解	10
图 10	通信类分解	17
图 11	密码支持类分解	19
图 12	用户数据保护类分解	23
图 13	标识和鉴别类分解	38
图 14	安全管理类分解	45
图 15	隐秘类分解	51
图 16	TSF 保护类分解	56
图 17	资源利用类分解	69
图 18	TOE 访问类分解	72
图 19	可信路径/信道类分解图	77

图 A.1	安全技术保障控制类结构	81
图 A.2	安全技术保障控制子类结构	81
图 A.3	安全技术保障控制组件结构	82
图 B.1	信息技术系统分析模型	90
图 B.2	分层多点安全技术体系结构	91
表 A.1	安全技术保障控制组件依赖关系表	83

前 言

GB/T 20274《信息安全技术 信息系统安全保障评估框架》分为以下四个部分：

——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

本部分是 GB/T 20274 的第 2 部分。

本部分的附录 A 和附录 B 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。

本部分主要起草人：吴世忠、王海生、陈晓桦、王贵骊、李守鹏、江常青、彭勇、张利、姚轶崧、邹琪、钱伟明、陆丽、班晓芳、李静、王庆、江典盛、孙成昊、门雪松、杜宇鸽、杨再山。

信息安全技术

信息系统安全保障评估框架

第 2 部分：技术保障

1 范围

GB/T 20274 的本部分建立了信息系统安全技术保障的框架,确立了组织机构内启动、实施、维护、评估和改进信息安全技术体系的指南和通用原则。GB/T 20274 的本部分定义和说明了信息系统安全技术体系建设和评估中反映组织机构信息安全的技术体系架构能力级,以及组织机构信息系统安全的技术要求。

GB/T 20274 的本部分适用于启动、实施、维护、评估和改进信息安全技术体系的组织机构和涉及信息系统安全技术工作的所有用户、开发人员和评估人员。

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 20274.1 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

3 术语和定义

GB/T 20274.1 确定的术语和定义适用于 GB/T 20274 的本部分。

4 本部分的结构

GB/T 20274 的本部分的组织结构如下:

- a) 第 1 章介绍了 GB/T 20274 的本部分的范围;
- b) 第 2 章介绍了 GB/T 20274 的本部分所规范引用的标准;
- c) 第 3 章描述了适用于 GB/T 20274 的本部分的术语和定义;
- d) 第 4 章描述了 GB/T 20274 的本部分的组织结构;
- e) 第 5 章描述了信息系统安全技术保障框架,并进一步概述了信息系统安全技术保障控制类域和安全技术体系架构能力级;
- f) 第 6 章描述了信息安全技术保障控制类的规范描述结构和要求;
- g) 第 7 章到第 17 章详述了提供信息安全技术保障控制类的 11 个信息安全技术保障控制类的详细要求;
- h) 第 18 章描述了安全技术体系架构能力成熟度模型;
- i) 附录 A 是资料性附录,进一步解释了安全技术要求;
- j) 附录 B 是资料性附录,描述了分层多点的信息系统安全技术体系架构;
- k) 参考文献给出了 GB/T 20274 的本部分的参考文献。