



# 中华人民共和国国家标准

GB/T 18336.3—2008/ISO/IEC 15408-3:2005  
代替 GB/T 18336.3—2001

---

## 信息技术 安全技术 信息技术安全性评估准则 第 3 部分：安全保证要求

Information technology—Security techniques—  
Evaluation criteria for IT security—  
Part 3: Security assurance requirements

(ISO/IEC 15408-3:2005, IDT)

2008-06-26 发布

2008-11-01 实施

---

中华人民共和国国家质量监督检验检疫总局 发布  
中国国家标准化管理委员会

## 目 次

前言 .....	V
引言 .....	VI
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语、定义和缩略语 .....	1
4 概述 .....	1
4.1 本部分的结构 .....	1
5 GB/T 18336 保证范型 .....	1
5.1 GB/T 18336 基本原则 .....	1
5.2 保证方法 .....	2
5.3 GB/T 18336 评估保证尺度 .....	3
6 安全保证要求 .....	3
6.1 结构 .....	3
6.2 组件分类法 .....	7
6.3 保护轮廓和安全目标评估准则类结构 .....	7
6.4 本部分中术语的用法 .....	7
6.5 保证分类 .....	10
6.6 保证类和族概况 .....	11
7 保护轮廓与安全目标评估准则 .....	14
7.1 概述 .....	14
7.2 保护轮廓准则概述 .....	14
7.3 安全目标准则概述 .....	15
8 APE类:保护轮廓评估 .....	16
8.1 TOE描述(APE_DES) .....	16
8.2 安全环境(APE_ENV) .....	17
8.3 PP引言(APE_INT) .....	17
8.4 安全目的(APE_OBJ) .....	18
8.5 IT安全要求(APE_REQ) .....	18
8.6 明确陈述的IT安全要求(APE_SRE) .....	20
9 ASE类:安全目标评估 .....	21
9.1 TOE描述(ASE_DES) .....	22
9.2 安全环境(ASE_ENV) .....	22
9.3 ST引言(ASE_INT) .....	23
9.4 安全目的(ASE_OBJ) .....	23
9.5 PP声明(ASE_PPC) .....	24
9.6 IT安全要求(ASE_REQ) .....	25
9.7 明确陈述的IT安全要求(ASE_SRE) .....	26

9.8	TOE 概要规范 (ASE_TSS)	27
10	评估保证级	28
10.1	评估保证级(EAL)概述	28
10.2	评估保证级细节	30
10.3	评估保证级 1(EAL1)——功能测试	30
10.4	评估保证级 2(EAL2)——结构测试	30
10.5	评估保证级 3(EAL3)——系统地测试和检查	31
10.6	评估保证级 4(EAL4)——系统地设计、测试和复查	32
10.7	评估保证级 5 (EAL5)——半形式化设计和测试	33
10.8	评估保证级 6 (EAL6)——半形式化验证的设计和测试	34
10.9	评估保证级 7(EAL7)——形式化验证的设计和测试	36
11	保证类、族和组件	37
12	ACM 类:配置管理	37
12.1	CM 自动化(ACM_AUT)	37
12.2	CM 能力(ACM_CAP)	39
12.3	CM 范围(ACM_SCP)	45
13	ADO 类:交付和运行	46
13.1	交付(ADO_DEL)	46
13.2	安装、生成和启动(ADO_IGS)	48
14	ADV 类:开发	49
14.1	功能规范(ADV_FSP)	52
14.2	高层设计(ADV_HLD)	55
14.3	实现表示(ADV_IMP)	59
14.4	TSF 内部 (ADV_INT)	62
14.5	低层设计(ADV_LLD)	65
14.6	表示对应性(ADV_RCR)	67
14.7	安全策略模型(ADV_SPM)	69
15	AGD 类:指导性文档	71
15.1	管理员指南(AGD_ADM)	72
15.2	用户指南(AGD_USR)	73
16	ALC 类:生命周期支持	73
16.1	开发安全(ALC_DVS)	74
16.2	缺陷纠正(ALC_FLR)	75
16.3	生命周期定义(ALC_LCD)	78
16.4	工具和技术(ALC_TAT)	80
17	ATE 类:测试	81
17.1	测试覆盖 (ATE_COV)	82
17.2	测试深度 (ATE_DPT)	84
17.3	功能测试 (ATE_FUN)	86
17.4	独立测试 (ATE_IND)	88
18	AVA 类:脆弱性评定	90

18.1	隐蔽信道分析(AVA_CCA)	91
18.2	误用(AVA_MSU)	93
18.3	TOE 安全功能强度(AVA_SOF)	96
18.4	脆弱性分析(AVA_VLA)	97
附录 A (资料性附录)	保证组件依赖关系的交叉引用	102
附录 B (资料性附录)	EAL 和保证组件的交叉引用	106

## 前 言

GB/T 18336 在总标题《信息技术 安全技术 信息技术安全性评估准则》下,由以下几个部分组成:

——第 1 部分:简介和一般模型

——第 2 部分:安全功能要求

——第 3 部分:安全保证要求

本部分是 GB/T 18336 的第 3 部分。

本部分等同采用国际标准 ISO/IEC 15408-3:2005《信息技术 安全技术 信息技术安全性评估准则 第 3 部分:安全保障要求》,仅有编辑性修改。

本部分代替 GB/T 18336.3—2001《信息技术 安全技术 信息技术安全性评估准则 第 3 部分:安全保障要求》。

本部分与 GB/T 18336.3—2001 的主要差异如下:

1. 删除了 GB/T 18336.3—2001 的“ISO/IEC 前言”;
2. 增加了“引言”;
3. 减少了“AMA:保证维护”类;
4. 对 GB/T 18336.3—2001 附录 A 中表 A.1 进行了调整。

本部分的附录 A 和附录 B 是资料性附录。

本部分由全国信息安全标准化技术委员会提出和归口。

本部分的主要起草单位:中国信息安全测评中心。

本部分主要起草人:吴世忠、李守鹏、王贵驹、黄元飞、陈晓桦、刘晖、刘春明、李斌、彭勇、付敏、刘楠、徐长醒、简余良、张利。

## 引 言

本部分定义的安全保证组件是在一个保护轮廓(PP)或安全目标(ST)中表述安全保证要求的基础。

这些要求建立了一种表述评估对象(TOE)保证要求的标准方法。本部分列出了一组保证组件、族和类。本部分还定义了PP和ST的评估准则,提出了定义关于TOE保证等级的预定义GB/T 18336尺度的一些评估保证级别,称为“评估保证级”(EAL)。

本部分的目标读者主要有安全的IT系统和产品的客户、开发者、评估者。GB/T 18336.1第4章提供了关于GB/T 18336目标读者的附加信息,以及目标读者组如何使用GB/T 18336的附加信息。这些读者组可以如下方式使用本部分:

- a) 客户,在选取组件来表述保证要求,以满足一个PP或ST提出的安全目的时,使用本部分。GB/T 18336.1的5.4条提供了关于安全目的和安全要求之间关系的更多详细信息;
- b) 开发者,在构造TOE时响应实际的或预测的客户安全要求,在解释保证要求陈述和确定TOE的保证方法时参考本部分;
- c) 评估者,在确定TOE的保证以及评估PP和ST时,使用本部分所定义的保证要求作为评估准则的强制性陈述。

# 信息技术 安全技术

## 信息技术安全性评估准则

### 第 3 部分:安全保证要求

#### 1 范围

本部分定义了 GB/T 18336 的保证要求,包括衡量保证尺度的评估保证级(EAL)、组成保证级的单个保证组件以及 PP 和 ST 的评估准则。

#### 2 规范性引用文件

下列文件中的条款通过 GB/T 18336 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 18336.1—2008 信息技术 安全技术 信息技术安全性评估准则 第 1 部分:简介和一般模型 (ISO/IEC 15408-1:2005, IDT)

GB/T 18336.2—2008 信息技术 安全技术 信息技术安全性评估准则 第 2 部分:安全功能要求 (ISO/IEC 15408-2:2005, IDT)

#### 3 术语、定义和缩略语

GB/T 18336.1 中给出的术语、定义和缩略语适用于本部分。

#### 4 概述

##### 4.1 本部分的结构

第 5 章描述了在本部分的安全保证要求中使用的范型。

第 6 章描述了保证类、族、组件和评估保证级的表示结构,以及它们之间的关系。同时还刻画了第 12 章到第 18 章可找到的保证类和族的特征。

第 7 章、第 8 章和第 9 章先对 PP 和 ST 的评估准则作简要的介绍,然后对评估中要用到的族与组件做了详尽的解释。

第 10 章给出了评估保证级(EAL)的详尽定义。

第 11 章对保证类作了简要的介绍,在随后第 12 章到第 18 章给出了这些类的详尽定义。

附录 A 给出了保证组件之间依赖关系的汇总。

附录 B 给出了评估保证级(EAL)和保证组件之间的交叉引用。

#### 5 GB/T 18336 保证范型

本章旨在阐述支撑 GB/T 18336 保证方法的基本原则。通过对本章的理解将使读者了解隐含在本部分保证要求中的基本原理。

##### 5.1 GB/T 18336 基本原则

GB/T 18336 的基本原则是安全威胁和组织安全策略承诺应清楚地表述,以及所提出的安全措施经证实足以达到所期望的安全目的。