ICS 35.040
L 80

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
中国国家标准化管理委员会　发布

目　　次

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、王贵驷、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明确地表述,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。