ICS 35.040
L 80

中华人民共和国国家标准

GB/T 18336.2—2008/ISO/IEC 15408-2:2005
代替 GB/T 18336.2—2001

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

Information technology—Security techniques—
Evaluation criteria for IT security—
Part 2:Security functional requirements

(ISO/IEC 15408-2:2005,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 2 部分。

本部分等同采用国际标准 ISO/IEC 15408-2:2005《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》，仅有编辑性修改。

本部分代替 GB/T 18336.2—2001《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》。

本部分与 GB/T 18336.2—2001 的主要差异如下：

1）　删除了 GB/T 18336.2—2001 的“ISO/IEC 前言”；

2）　增加了“引言”；

3）　将 GB/T 18336.2—2001 的“范围”1.1 和 1.2 调整为本部分第 4 章，1.3 调整为第 5 章；

4）　增加了 FMT_SMF 族；

5）　对 GB/T 18336.2—2001 附录 A 中表 A.1 进行了调整。

本部分的附录均为规范性附录。

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、黄元飞、陈晓桦、王贵驷、李斌、付敏、刘晖、刘春明、郭颖、刘楠、甘杰夫、宋小龙、徐长醒、简余良、郭涛、王书毅。

引　言

本部分定义的安全功能组件是在一个保护轮廓(PP)或安全目标(ST)中表述安全功能要求的基础。这些要求描述一个评估对象(TOE)期待的安全行为或 TOE 的 IT 环境,并旨在满足在 PP 或 ST 中所提出的安全目的。这些要求描述那些用户能直接通过 IT 交互(即输入、输出)或 IT 刺激响应过程探测到的安全特性。

安全功能组件表述安全要求,这些要求试图对抗在 TOE 假定的运行环境中的威胁或涵盖所有的既定组织安全策略和假设。

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 目标读者和目标读者组如何使用 GB/T 18336 的附加信息。这些组可以如下方式使用 GB/T 18336 本部分:

a) 客户,在选取组件来表述功能要求满足一个 PP 或 ST 提出的安全目的时,使用本部分。GB/T 18336.1的 5.4 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,可以在本部分中找到一种标准方法去理解这些要求。也可以以本部分的内容为基础,去进一步定义满足这些要求的 TOE 安全功能和机制;

c) 评估者,使用本部分所定义的功能要求检验在 PP 或 ST 中表述的 TOE 功能要求是否满足 IT 安全目的,以及所有的依赖关系是否都已解释清楚并得到满足。评估者也宜使用本部分去帮助确定一个指定的 TOE 是否满足规定的要求。

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

1　范围

GB/T 18336的这一部分定义了安全功能组件的规定结构和内容,适用于安全性评估。本部分包含满足多个IT产品和系统通用安全功能要求的系列功能组件。

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)

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

4.0　引言

GB/T 18336和本部分在此描述的相关安全功能要求,并不打算成为所有IT安全问题的最终答案。相反地,GB/T 18336只是提供一组广为认同的安全功能要求,用于创建反映市场需求的可信产品或系统。这些安全功能要求的给出,体现了当前要求规范和评估的技术发展水平。

本部分并不想包括所有可能的安全功能要求,而是尽量包含那些在本部分发布时作者已知的并认为有价值的那些要求。

由于认知和客户需求会变化,因此本部分中的功能要求需要维护。可预见的是,某些PP/ST作者可能还有一些安全要求未包含在本部分提出的功能要求组件中。此时,PP/ST的作者可考虑使用不是从GB/T 18336中选取的功能要求(称之为可扩展性),参见GB/T 18336.1附录A和附录B。

4.1　本部分的结构

第5章是本部分安全功能要求使用的范型。

第6章介绍本部分功能组件的分类,第7章到第17章描述这些功能类。

附录A为功能组件的潜在用户提供了解释性信息,其中包括功能组件间依赖关系的一个完整的交叉引用表。

附录B至附录M提供了功能类的解释性信息。在如何运用相关操作和选择恰当的审计或文档信息时,这些材料必须被看作是规范性指令。使用助动词"宜"表示该指令是首要推荐的,但是其他的只是可选的。这里只给出了不同的选项,具体的选择留给了PP/ST作者。

对于有关结构、规则和指南,编写PP或ST的人员宜参考GB/T 18336.1第2章和相关附录:

a)　GB/T 18336.1第2章定义了GB/T 18336中使用的术语。

b)　GB/T 18336.1附录A定义了PP的结构。

c)　GB/T 18336.1附录B定义了ST的结构。