ICS 35.040
L 80

中华人民共和国国家标准

GB/T 18336.2—2015/ISO/IEC 15408-2:2008
代替 GB/T 18336.2—2008

信息技术　安全技术
信息技术安全评估准则
第2部分:安全功能组件

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

(ISO/IEC 15408-2:2008,IDT)

2015-05-15 发布　　2016-01-01 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《信息技术　安全技术　信息技术安全评估准则》分为以下三部分：

——第1部分：简介和一般模型；

——第2部分：安全功能组件；

——第3部分：安全保障组件。

本部分是GB/T 18336的第2部分。

本部分按照GB/T 1.1—2009给出的规则编写。

本部分代替GB/T 18336.2—2008《信息技术　安全技术　信息技术安全评估准则　第2部分：安全功能要求》。

本部分与GB/T 18336.2—2008的主要差异如下：

——将“保证”(assurance)改为“保障”；

——将“10.4 输出到TSF控制之外(FDP_ETC)”改为“10.4 从TOE输出(FDP_ETC)”；

——将“10.7 从TSF控制之外输入(FDP_ITC)”改为“10.7 从TOE之外输入(FDP_ITC)”；

——删除了“14FPT类：TSF保护”中的“14.1 底层抽象机测试(FPT_AMT)”、“14.10 引用仲裁(FPT_RVM)”、“14.11 域分离(FPT_SEP)”；

——在“14FPT类：TSF保护”中增加了“14.12 外部实体测试(FPT_TEE)”；

——将“16.3 会话锁定(FTA_SSL)”改为“16.3 会话锁定和终止(FTA_SSL)”；

——将“门限值”改为“临界值”；

——将“介导”改为“促成”。

本部分使用翻译法等同采用国际标准ISO/IEC 15408-2:2008《信息技术　安全技术　信息技术安全评估准则　第2部分：安全功能组件》。

与本部分中规范性引用的国际文件有一致性对应关系的我国文件如下：

——GB/T 18336.1　信息技术　安全技术　信息技术安全评估准则　第1部分：简介和一般模型(GB/T 18336.1—2015，ISO/IEC 15408-1:2009，IDT)

本部分做了下列编辑性修改：

——第4.1条标准原文有编辑性错误，现已更正为“对于有关结构、规则和指南，编写PP或ST的人员应参见ISO/IEC 15408-1第3章和相关附录”。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出和归口。

本部分起草单位：中国信息安全测评中心、信息产业信息安全测评中心、公安部第三研究所、吉林信息安全测评中心。

本部分主要起草人：张翀斌、郭颖、石竑松、毕海英、张宝峰、高金萍、王峰、杨永生、李国俊、董晶晶、谢蒂、王鸿娴、张怡、顾健、邱梓华、宋好好、陈妍、杨元原、李凤娟、庞博、张骁、刘昱函、王书毅、周博扬、唐喜庆、蒋显岚、张双双。

本部分所代替标准的历次版本发布情况为：

——GB/T 18336.2—2001；

——GB/T 18336.2—2008。

引　言

本部分定义的安全功能组件为在保护轮廓(PP)或安全目标(ST)中表述的安全功能要求提供了基础。这些要求描述了评估对象(TOE)所期望的安全行为,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 激励响应过程探测到的安全特性。

安全功能组件表达了安全要求,这些要求试图对抗针对假定的 TOE 运行环境中的威胁,并/或涵盖了所有已标识的组织安全策略和假设。

本部分的目标读者主要包括安全的 IT 产品的消费者、开发者、评估者。ISO/IEC 15408-1 第 5 章提供了关于 ISO/IEC 15408 的目标读者和目标读者群体如何使用 ISO/IEC 15408 的附加信息。这些群体可以按如下方式使用本部分:

a) 消费者,为满足 PP 或 ST 中提出的安全目的,通过选取本部分的组件来表述功能要求。ISO/IEC 15408-1 提供了更多关于安全目的和安全要求之间的关系的详细信息;

b) 开发者,在构造 TOE 时响应实际的或预测的消费者安全要求,可以在本部分中找到一种标准的方法去理解这些要求。也可以以本部分的内容为基础,进一步定义 TOE 的安全功能和机制来满足那些要求;

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
信息技术安全评估准则
第2部分:安全功能组件

1　范围

为了安全评估的意图,GB/T 18336的本部分定义了安全功能组件所需要的结构和内容。本部分包含一个安全组件的分类目录,将满足许多IT产品的通用安全功能要求。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修订版)适用于本文件。

ISO/IEC 15408-1　信息技术 安全技术　信息技术安全评估准则　第1部分:简介和一般模型(Information technology—Security techniques—Evaluation criteria for IT security —Part 1:Introduction and general model)

3　术语、定义和缩略语

ISO/IEC 15408-1中给出的术语、定义、符号和缩略语适用于本文件。

4　概述

ISO/IEC 15408和本部分在此描述的相关安全功能要求,并不意味着是对所有IT安全问题的最终回答。相反,本标准提供一组广为认同的安全功能要求,以用于制造反映市场需求的可信产品。这些安全功能要求的给出,体现了当前对产品的要求规范和评估的技术发展水平。

本部分并不计划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是有价值的那些要求。

由于消费者的认知和需求可能会发生变化,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ISO/IEC 15408之外的功能要求(称之为可扩展性),有关内容参见ISO/IEC 15408-1的附录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～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～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