ICS 35.040
L 80

中华人民共和国国家标准

GB/T 18336.3—2015/ISO/IEC 15408-3:2008
代替 GB/T 18336.3—2008

信息技术　安全技术
信息技术安全评估准则
第3部分:安全保障组件

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

(ISO/IEC 15408-3:2008,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3部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替GB/T 18336.3—2008《信息技术　安全技术　信息技术安全评估准则　第3部分：安全保证要求》。

本部分与GB/T 18336.3—2008的主要差异如下：

——将“保证”(assurance)改为“保障”；

——将“6　安全保证要求”改为“6　安全保障组件”；

——删除了“6.3　保护轮廓和安全目标评估准则类结构”、“6.4　本部分中术语的用法”、“6.5　保证分类”、“6.6　保证类和族概况”；

——将“6.1.5　EAL结构”调整为本部分的“6.2　评估保障级结构”；

——增加了“6.3　组合保障包结构”；

——删除了“7　保护轮廓与安全目标评估准则”、“11　保证类、族和组件”；

——增加了“8　组合保障包”；

——删除了“8.1　TOE描述”；

——增加了“9.2　符合性声明”；

——将“8.2　安全环境”、“8.6　明确陈述的IT安全要求”改为本部分的“9.3　安全问题定义”、“9.5　扩展组件定义”；

——删除了“9.1　TOE描述”、“9.5　PP声明”；

——增加了“10.2　符合性声明”；

——将“9.2　安全环境”、“9.7　明确陈述的IT安全要求”改为本部分的“10.3　安全问题定义”、“10.5　扩展组件定义”；

——删除了“ADV类：开发”中的“高层设计(ADV_HLD)”、“低层设计(ADV_LLD)”、“表示对应性(ADV_RCR)”；

——在“ADV类：开发”中增加了“安全架构(ADV_ARC)”、“TOE设计(ADV_TDS)”；

——将AGD类的“管理员指南(AGD_ADM)”和“用户指南(AGD_USR)”调整为本部分的“操作用户指南(AGD_OPE)”和“准备程序(AGD_PRE)”；

——将ACM类的“CM能力(ACM_CAP)”、“CM范围(ACM_SCP)”，ADO类的“交付(ADO_DEL)”合到了ALC类中；

——删除了“ACM类：配置管理”中的“CM自动化(ACM_AUT)”；

——删除了“ADO类：交付和运行”中的“安装、生成和启动(ADO_IGS)”；

——将“测试覆盖(ATE_COV)”改为“覆盖(ATE_COV)”，将“测试深度(ATE_DPT)”改为“深度(ATE_DPT)”；

——删除了“AVA类：脆弱性评定”中的“隐蔽信道分析(AVA_CCA)”、“误用(AVA_MSU)”、“TOE安全功能强度(AVA SOF)”；

——将“脆弱性分析(AVA_VLA)”改为“脆弱性分析(AVA_VAN)”;

——增加了“16 ACO 类:组合”;

——增加了“附录 A 开发(ADV)”、“附录 B 组合(ACO)”、“附录 D PP 和保障组件的交叉引用”、“附录 F CAP 和保障组件的交叉引用”;

——将“附录 A 保证组件依赖关系的交叉引用”调整为“附录 C 保障组件依赖关系的交叉引用”,将“附录 B EAL 和保证组件的交叉引用”调整为“附录 E EAL 和保障组件的交叉引用”。

本部分使用翻译法等同采用 ISO/IEC 15408-3:2008《信息技术 安全技术 信息技术安全评估准则 第 3 部分:安全保障组件》。

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)

——GB/T 18336.2 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(GB/T 18336.2—2015,ISO/IEC 15408-2:2008,IDT)

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

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。

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、许源、饶华一、吴毓书、毛军捷。

本部分所代替标准的历次版本发布情况为:

——GB/T 18336.3—2001

——GB/T 18336.3—2008

引　言

本部分定义的安全保障组件是在保护轮廓(PP)或安全目标(ST)中描述安全保障要求的基础。

这些要求建立了一种描述评估对象(TOE)保障要求的标准方法。本部分列出了一组保障组件、族和类,还定义了评估 PP 和 ST 的准则,定义了评估保障级别(EAL)来描述 ISO/IEC 15408 中预定义的用于评定 TOE 保障要求满足情况的尺度。

本部分的目标读者主要包括安全 IT 产品的消费者、开发者和评估者。ISO/IEC 15408-1 提供了关于 ISO/IEC 15408 的目标读者,以及目标读者群体如何使用 ISO/IEC 15408 的补充信息。这些读者群体可以如下方式使用本部分:

a) 消费者,在选取组件描述保障要求,以满足 PP 或 ST 中提出的安全目的,以及确定所需的安全保障级别时都可使用本部分;

b) 开发者,在构造 TOE 以响应实际的或预想的消费者安全要求时,可参考本部分以解释保障要求陈述并确定 TOE 的保障方法;

c) 评估者,在确定 TOE 的保障级别以及评估 PP 和 ST 时,使用本部分所定义的保障要求作为评估准则的强制性陈述。

信息技术　安全技术
信息技术安全评估准则
第3部分:安全保障组件

1　范围

GB/T 18336的本部分定义了保障要求,包括:评估保障级(EAL)——为度量部件TOE的保障定义了一种尺度;组合保障包(CAP)——为度量组合TOE的保障提供了一种尺度;组成保障级和保障包的单个保障组件;PP和ST的评估准则。

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(包括所有的修改单)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)

ISO/IEC 15408-2　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)

3　术语和定义

ISO/IEC 15408-1中界定的术语、定义和缩略语适用于本文件。

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障要求中使用的范型。

第6章描述了保障类、族、组件和评估保障级的表示结构以及它们之间的关系,包括组合保障包的结构。同时还刻画了第9章到第16章中陈述的保障类和族的特征。

第7章给出了评估保障级(EAL)的详尽定义。

第8章给出了组合保障包(CAP)的详尽定义。

第9章到第16章给出了本部分保障类的详尽定义。

附录A给出了开发类相关概念的进一步解释和实例。

附录B给出了组合TOE评估和组合类概念的解释。

附录C给出了保障组件之间依赖关系的总结。

附录D给出了PP和族以及APE类组件之间的交叉引用。

附录E给出了评估保障级(EAL)和保障组件之间的交叉引用。

附录F给出了组合保障包(CAP)和保障组件之间的交叉引用。