ICS 35.040
L 70

中华人民共和国国家标准

GB/T 18336.3—2001
idt ISO/IEC 15408-3:1999

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

2001-03-08 发布　　2001-12-01 实施

国家质量技术监督局　发布

目　　次

前　言

本标准等同采用国际标准 ISO/IEC 15408-3:1999《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》。

本标准介绍了信息技术安全性评估的安全保证要求。

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 3 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

本标准的附录 A 和附录 B 是提示的附录。

本标准由国家质量技术监督局提出。

本标准由全国信息技术标准化技术委员会归口。

本标准由中国国家信息安全测评认证中心、信息产业部电子第 30 研究所、国家信息中心、复旦大学负责起草。

本标准主要起草人:吴世忠、吴承荣、龚奇敏、陈晓桦、李守鹏、方关宝、吴亚飞、雷利民、叶红、李鹤田、黄元飞、任卫红。

本标准委托中国国家信息安全测评认证中心负责解释。

ISO/IEC 前言

ISO(国际标准化组织)和IEC(国际电工委员会)形成了全世界标准化的专门体系。作为ISO或IEC成员的国家机构,通过相应组织所建立的涉及技术活动特定领域的委员会参加国际标准的制定。ISO和IEC技术委员会在共同关心的领域里合作,其他与ISO和IEC联盟的政府的和非政府的国际组织也参加了该项工作。

国际标准的起草符合ISO/IEC导则第3部分的原则。

在信息技术领域,ISO和IEC已经建立了一个联合技术委员会——ISO/IEC JTC1。联合技术委员会采纳的国际标准草案交付给国家机构投票表决。作为国际标准公开发表,需要至少75%的国家机构投赞成票。

国际标准ISO/IEC 15408-3是由联合技术委员会ISO/IEC JTC1(信息技术)与通用准则项目发起组织合作产生的。与ISO/IEC 15408-3同样的文本由通用准则项目发起组织作为《信息技术安全性评估通用准则》发表。有关通用准则项目的更多信息和发起组织的联系信息由ISO/IEC 15408-1的附录A提供。

ISO/IEC 15408在"信息技术——安全技术——信息技术安全性评估准则"的总标题下,由以下几部分组成:

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

附录A和附录B构成ISO/IEC 15408本部分的提示部分。

以下具有法律效力的提示已按要求放置在ISO/IEC 15408的所有部分:

在ISO/IEC 15408-1附录A中标明的七个政府组织(总称为通用准则发起组织),作为《信息技术安全性评估通用准则》第1至第3部分(称为"CC")版权的共同所有者,在此特许ISO/IEC在开发ISO/IEC 15408国际标准中,非排他性地使用CC。但是,通用准则发起组织在他们认为适当时保留对CC的使用、拷贝、分发以及修改的权利。

中华人民共和国国家标准

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

GB/T 18336.3—2001
idt ISO/IEC 15408-3:1999

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

1　范围

本标准定义了保证要求。它包括衡量保证尺度的评估保证级(EAL)、组成保证级的每个保证组件以及PP和ST的评估准则。

1.1　本标准的结构

第1章是本标准的引论和范例。

第3章描述了保证类、子类、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9章到第15章可找到的保证类和子类的特征。

第4章、第5章和第6章先对PP和ST的评估准则作简要的介绍，然后对在评估中要用到的子类与组件做了详尽的解释。

第7章是评估保证级(EAL)的详尽定义。

第8章对保证类作了简要的介绍，在随后的第9章到第15章给出了这些类的详尽定义。

第16和第17章对保证维护的评估准则做了简要的介绍，其后给出了所用到的子类和组件的详尽定义。

附录A给出了保证组件之间依赖关系的概要。

附录B给出了评估保证级(EAL)和保证组件之间的交叉引用。

1.2　GB/T 18336的保证范例

本条旨在阐述支撑本标准保证方法的基本原则。通过对本条的理解将使读者了解隐含在本标准保证要求中的基本原理。

1.2.1　GB/T 18336基本原则

GB/T 18336的基本原则，就是应该清楚描述那些对安全和组织安全策略承诺所造成的威胁，并且提出足以达到所期望的安全目的的安全措施。

进一步地说，就是应采取一些措施以减少可能存在的脆弱性，减弱有意利用或者无意触发(或利用)一个脆弱性的能力，以及减轻因利用一个脆弱性而导致的破坏程度。另外，还需要采纳一定的措施，便于今后标识一些脆弱性，消除、减轻或通告一个已经被利用或触发过的脆弱性。

1.2.2　保证方法

GB/T 18336的基本原则是为被信任的IT产品或系统的评估(积极的调查)提供保证。评估是提供保证的传统方法，并且是GB/T 18336文档的基础。为了与现行的方法保持一致，GB/T 18336采用相同的基本原则。GB/T 18336建议由专业评估员在不断强调范围、深度和严格性的基础上，衡量文档和已

国家质量技术监督局2001-03-08批准　　2001-12-01实施