ICS 35.040
L 70

中华人民共和国国家标准

GB/T 18336.1—2001
idt ISO/IEC 15408-1:1999

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

Information technology—Security techniques—
Evaluation criteria for IT security—
Part 1:Introduction and general model

2001-03-08 发布　　2001-12-01 实施

国家质量技术监督局　发布

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 1 部分:简介和一般模型
GB/T 18336.1—2001
*
中国标准出版社出版发行
北京西城区复兴门外三里河北街 16 号
邮政编码:100045
http://www.bzcbs.com
电话:63787337、63787447
2001 年 10 月第一版 2004 年 11 月电子版制作
*
书号:155066·1-17785

目　　次

前　　言

本标准等同采用国际标准 ISO/IEC 15408-1:1999《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》。

本标准介绍了信息技术安全性评估的基本概念并给出了信息技术安全性评估的一般模型,并在附录 B 和附录 C 分别介绍了“保护轮廓”和“安全目标”。

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

本标准的附录 A 和附录 D 是提示的附录。

本标准的附录 B 和附录 C 是标准的附录。

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、龚奇敏、陈晓桦、李守鹏、罗建中、方关宝、李鹤田、吴亚飞、雷利民、叶红、吴承荣、黄元飞、任卫红、崔玉华。

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有联系的政府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分发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 15408-1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 15408-1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B和附录C构成ISO/IEC 15408本部分的规范部分,附录A和附录D仅供参考。

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1部分：简介和一般模型

GB/T 18336.1—2001
idt ISO/IEC 15408-1:1999

Information technology—Security techniques—Evaluation criteria for IT security—Part 1:Introduction and general model

1　范围

GB/T 18336 定义了作为评估信息技术产品和系统安全特性的基础准则，由于历史和连续性的原因，仍叫通用准则(CC——Common Criteria))。通过建立这样的通用准则库，使信息技术安全评估的结果能被更多的人理解。

针对在安全性评估过程中信息技术产品和系统的安全功能及相应的保证措施，CC 提供了一组通用要求，使各种独立的安全评估结果具有可比性。评估过程为满足这些要求的产品和系统的安全功能以及相应的保证措施确定一个可信级别。评估结果可以帮助用户确定信息技术产品和系统对他们的应用而言是否足够安全，以及在使用中隐藏的安全风险是否可以容忍。

CC 可用于具有信息技术安全功能的产品和系统的开发与采购指南。在评估过程中，这样的产品和系统被称为评估对象(TOE——Target of Evaluation)，如：操作系统、计算机网络、分布式系统以及应用等。

CC 涉及信息保护，以避免未经授权的信息泄露、修改和无法使用，与此对应的保护类型通常分别称之为保密性、完整性和可用性。除上述三个方面外，CC 还适用于信息安全的其他方面。CC 重点考虑人为的信息威胁，无论其是否是恶意的。但 CC 也可用于非人为因素导致的威胁。此外，CC 还可适用于其他信息技术领域，但对严格意义上信息技术安全之外的领域，CC 不做承诺。

CC 适用于硬件、固件和软件实现的信息技术安全措施，当一些特定的评估仅适用于某些实现方法时，这一点将在相关的准则说明中注明。

某些内容因涉及特殊的专业技术或仅是信息技术安全的外围技术，不在 CC 的范围内，例如：

a) CC 不包括那些与信息技术安全措施没有直接关联的属于行政性管理安全措施的安全评估准则。但是，应该认识到 TOE 安全的重要部分是通过诸如组织的、个人的、物理的、程序的监控等行政性管理安全措施来实现的。当行政性管理安全措施影响到信息技术安全措施对抗确定威胁的能力时，这类管理安全措施在 TOE 的运行环境中被认为是 TOE 安全使用的前提条件。

b) 对于信息技术安全性的物理方面(诸如电磁辐射控制)的评估，虽然 CC 的许多概念是适用的，但并不专门针对该领域，然而也会专门涉及 TOE 物理保护的一些方面。

c) CC 并不涉及评估方法学，也不涉及评估机构使用本规则的管理模式或法律框架，但希望 CC 能在具有这样的框架和方法论的环境中用于评估。

d) 评估结果用于产品和系统认可的过程不属于 CC 的范围。产品和系统的认可是行政性的管理过

国家质量技术监督局 2001-03-08 批准　　2001-12-01 实施