ICS 35.040
L 80

中华人民共和国国家标准

GB/T 18336.1—2008/ISO/IEC 15408-1:2005
代替 GB/T 18336.1—2001

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

(ISO/IEC 15408-1:2005,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—2008 的第 1 部分。

本部分等同采用国际标准 ISO/IEC 15408-1:2005《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》，仅有编辑性修改。

本部分代替 GB/T 18336.1—2001《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》。

本部分与 GB/T 18336.1—2001 的主要差异如下：

1）　删除了 GB/T 18336.1—2001 的“ISO/IEC 前言”；

2）　GB/T 18336.1—2008 增加了“引言”；

3）　删除了 GB/T 18336.1—2001 的附录 A“通用准则项目”；

4）　GB/T 18336.1—2001 的附录 D 编为本部分的“参考文献”。

本部分的附录 A 和附录 B 是规范性附录。

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、陈晓桦、李守鹏、黄元飞、王贵驷、刘晖、刘春明、付敏、郭颖、刘楠。

引　言

GB/T 18336 将使各个独立的安全评估结果具有可比性。这通过在安全评估时，提供一套针对信息技术(IT)产品和系统安全功能及其保证措施的通用要求来实现。评估过程建立一个信任级别，表明该产品或系统的安全功能及其保证措施都满足这些要求。评估结果可以帮助客户确定该 IT 产品或系统对他们的预期应用是否足够安全以及使用该 IT 产品或系统带来的固有安全风险是否可容忍。

GB/T 18336 对开发具有 IT 安全功能的产品或系统以及采办具有此类功能的商用产品和系统都是一本有益的指南。在评估时，此类 IT 产品或系统称评估对象(TOE)。例如，常见的 TOE 有操作系统、计算机网络、分布式系统、应用软件等。

GB/T 18336 致力于保护信息免受未授权的泄漏、修改或无法使用，与此对应的保护类别通常分别称为保密性、完整性和可用性。此外，GB/T 18336 也适用于 IT 安全的其他方面。GB/T 18336 主要关注人为的安全威胁，无论其是否是恶意的，但也适用于非人为因素导致的威胁。另外，GB/T 18336 还可用于 IT 技术的其他方面，但就其安全领域外的能力本标准不作承诺。

GB/T 18336 适用于在硬件、固件或软件中实现的 IT 安全措施。另外，某些特殊的评估手段可能只适用于某些特定的实现方法，这将在相应的标准文本中指出。

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

1　范围

GB/T 18336 旨在作为评估信息技术产品和系统安全特性的基础准则。通过建立这样的通用准则库,信息技术安全性评估的结果才能被更多的人理解。

某些内容因涉及专业技术或仅仅是IT安全的外围技术,因此不在GB/T 18336范围之内。例如:

a) GB/T 18336不包括那些与IT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安全的某些重要组成部分通常可通过诸如组织的、人员的、物理的、程序的控制等行政性管理措施来实现。在TOE的运行环境中,当行政性管理安全措施影响到IT安全措施对抗已确定威胁的能力时,则将其作为安全使用假设;

b) GB/T 18336没有明确涵盖电磁辐射控制等IT安全中技术性物理方面的评估,虽然标准中的许多概念适用于该领域。换句话说,GB/T 18336只涉及到TOE物理保护的某些方面;

c) GB/T 18336并不专注于评估方法学,也不专注于评估管理机构使用本准则的管理和法律架构,但希望GB/T 18336能在具有这样的框架和方法论的环境中用于评估;

d) 评估结果用于产品或系统认可的程序不属于GB/T 18336的范围。产品或系统的认可是行政性的管理过程,据此准许IT产品或系统在其整个运行环境中投入使用。评估侧重于产品或系统的IT安全部分,以及直接影响到IT单元安全使用的那些运行环境。因此,评估结果是认可过程的重要输入。但是,由于其他技术更适合于评价非IT相关系统或产品的安全特性以及其与IT安全部分的关系,认可者应针对这些情况分别制定不同的条款;

e) GB/T 18336不包括评价密码算法固有质量相关的标准条款。如果需要对嵌入TOE的密码算法的数学特性进行独立评价,则必须在使用GB/T 18336的评估体制中为相关评价制定专门条款。

本标准定义了两种结构以表述IT安全功能和保证要求。其中,保护轮廓(PP)允许创建一些普遍可重复使用的安全要求集合。PP可被目标客户用于规范和识别满足其需求的产品及其IT安全特性。安全目标(ST)用于阐述安全要求和详细说明被评估产品或系统的安全功能,这些产品通常称为评估对象(TOE)。ST被评估者用来作为在GB/T 18336指导下进行评估活动的基础。

2　术语和定义

下列术语和定义适用于本标准。

注:本章只收录在GB/T 18336中有特殊用法的术语。在GB/T 18336中使用的大多数术语,或根据普遍接受的词典定义,或根据普遍接受的GB或ISO安全术语定义,或根据熟知的安全性术语定义。在GB/T 18336中使用的但本章没有收录的一些由通用术语组合成的复合词,将在使用它们的地方进行解释。在GB/T 18336.2和GB/T 18336.3的"范型"章条中也可以见到某些术语和概念的解释。

2.1

资产　assets

由TOE安全策略保护的信息或资源。