ICS 35.040
L 80

中华人民共和国国家标准

GB/T 18336.1—2015/ISO/IEC 15408-1:2009
代替 GB/T 18336.1—2008

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 15408-1:2009,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3个部分：

——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。

本部分为GB/T 18336的第1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 18336.1—2008《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》。

本部分与GB/T 18336.1—2008的主要差异如下：

——增加了“2　规范性引用文件”；

——“3　术语和定义”中增加了“3.2　与开发(ADV)类相关的术语和定义”、“3.3　与指导性文档(AGD)类相关的术语和定义”、“3.4　与生命周期支持(ALC)类相关的术语和定义”、“3.5　与脆弱性评定(AVA)类相关的术语和定义”、“3.6　与组合(ACO)类相关的术语和定义”；

——“5　概述”中增加了“5.2　TOE”；

——将GB/T 18336适用的“IT产品和系统”改为“IT产品”；

——“5.1　安全相关要素”、“5.2　保证方法”调整为本部分的“6.2　资产和对策”、“6.3　评估”；

——删除了GB/T 18336.1—2008的“5.3　安全概念”；

——“5.4.1　安全要求的表达”调整为本部分的“7　剪裁安全要求”；

——删除了GB/T 18336.1—2008的“5.4.2　评估类型”；

——增加了“8　保护轮廓和包”；

——“6　GB/T 18336要求和评估结果”调整为本部分的“9　评估结果”；

——“附录A　保护轮廓规范”调整为本部分的“附录B　保护轮廓规范”，并增加了“B.11　低保障的保护轮廓”、“B.12　在PP中引用其他标准”；

——“附录B　安全目标规范”调整为本部分的“附录A　安全目标规范”，并增加了“A.3　使用ST”、“A.11　ST可解答的问题”、“A.12　低保障安全目标”、“A.13　在ST中引用其他标准”。

本部分使用翻译法等同采用国际标准ISO/IEC 15408-1:2009《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》。

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

——GB/T 18336.3—2015　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(ISO/IEC 15408-3:2008，IDT)

——GB/T 30270　信息技术　安全技术　信息技术安全性评估方法(GB/T 30270—2013，ISO/IEC 18045:2005，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、贾炜、王宇航、王亚楠。

本部分所代替标准的历次版本发布情况：

——GB/T 18336.1—2001

——GB/T 18336.1—2008

引　言

ISO/IEC 15408 可让各个独立的安全评估结果之间具备可比性。为此，ISO/IEC 15408 针对安全评估中的信息技术(IT)产品的安全功能及其保障措施提供了一套通用要求。这些 IT 产品的实现形式可以是硬件、固件或软件。

评估过程可为 IT 产品的安全功能及其保障措施满足这些要求的情况建立一个信任级别。评估结果可以帮助消费者确定该 IT 产品是否满足其安全要求。

ISO/IEC 15408 可为具有安全功能的 IT 产品的开发、评估以及采购过程提供指导。

ISO/IEC 15408 有很大的灵活性，以便可对范围广泛的 IT 产品的众多安全属性采用一系列的评估方法。因此，用户需谨慎运用 ISO/IEC 15408，以避免误用此类灵活性。例如，若使用 ISO/IEC 15408 时采取了不合适的评估方法、选择了不相关的安全属性或针对的 IT 产品不恰当，都将导致无意义的评估结果。

因此，IT 产品经过评估的事实只有在提及选择了哪些安全属性，以及采用了何种评估方法的情况下才有意义。评估授权机构需要仔细地审查产品、安全属性及评估方法以确定对其评估是否可产生有意义的结论。另外，评估产品的购买方也需要仔细地考虑评估这种情况，以确定该产品是否有用，且能否满足其特定的环境和需要。

ISO/IEC 15408 致力于保护资产免遭未授权的泄漏、修改或丧失可用性。此类保护与三种安全失效情况对应，通常分别称为机密性、完整性和可用性。此外，ISO/IEC 15408 也适用于 IT 安全的其他方面。ISO/IEC 15408 可用于考虑人为的(无论恶意与否)以及非人为的因素导致的风险。另外，ISO/IEC 15408 还可用于 IT 技术的其他领域，但对安全领域外的适用性不作申明。

对某些问题，因涉及专业技术或对 IT 安全而言较为次要，因此不在 ISO/IEC 15408 范围之内，例如：

a) ISO/IEC 15408 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；

b) ISO/IEC 15408 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，ISO/IEC 15408 只涉及 TOE 物理保护的某些方面；

c) ISO/IEC 15408 并不涉及评估方法，具体的评估方法在 ISO/IEC 18045 中给出；

d) ISO/IEC 15408 不涉及评估管理机构使用本准则的管理和法律框架，但 ISO/IEC 15408 也可被用于此框架下的评估；

e) 评估结果用于产品认可的程序不属于 ISO/IEC 15408 的范围。产品的认可是行政性的管理过程，据此准许 IT 产品在其整个运行环境中投入使用。评估侧重于产品的 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估非 IT 相关属性以及其与 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；

f) ISO/IEC 15408 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估，则必须在使用 ISO/IEC 15408 的评估体制中为相关评估制定专门条款。

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

1　范围

GB/T 18336的本部分建立了IT安全评估的一般概念和原则,详细描述了ISO/IEC 15408各部分给出的一般评估模型,该模型整体上可作为评估IT产品安全属性的基础。

本部分给出了ISO/IEC 15408的总体概述。它描述了ISO/IEC 15408的各部分内容;定义了在ISO/IEC 15048各部分将使用的术语及缩略语;建立了关于评估对象(TOE)的核心概念;论述了评估背景;并描述了评估准则针对的读者对象。此外,还介绍了IT产品评估所需的基本安全概念。

本部分定义了裁剪ISO/IEC 15408-2和ISO/IEC 15408-3描述的功能和保障组件时可用的各种操作。

本部分还详细说明了保护轮廓(PP)、安全要求包和符合性这些关键概念,并描述了评估产生的结果和评估结论。ISO/IEC 15408的本部分给出了规范安全目标(ST)的指导方针并描述了贯穿整个模型的组件组织方法。关于评估方法的一般信息以及评估体制的范围将在IT安全评估方法论中给出。

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 15408-2　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)

ISO/IEC 15408-3　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 18045　信息技术　安全技术　信息技术安全性评估方法(Information technology—Security techniques—Methodology for IT security evaluation)

3　术语和定义

下列术语和定义适用于本文件。

注:本章只收录在ISO/IEC 15408中有特殊用法的术语。在ISO/IEC 15408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。

3.1　常用术语和定义

3.1.1

敌对行为　adverse actions

由威胁主体对资产执行的行为。