中国标准出版社第四编辑室　编

信息安全标准汇编

信息安全测评卷

测评基础和系统测评分册

中国标准出版社

信息安全标准汇编

信息安全测评卷

测评基础和系统测评分册

中国标准出版社第四编辑室　编

中国标准出版社

北京

图书在版编目（CIP）数据

信息安全标准汇编．信息安全测评卷．测评基础和系统测评分册/中国标准出版社第四编辑室编．—北京：中国标准出版社，2009

ISBN 978-7-5066-5130-1

Ⅰ.信… Ⅱ.中… Ⅲ.信息系统-安全技术-国家标准-汇编-中国 Ⅳ.TP309-65

中国版本图书馆 CIP 数据核字（2008）第 208835 号

中国标准出版社出版发行
北京复兴门外三里河北街 16 号
邮政编码：100045

网址 www.spc.net.cn
电话：68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

开本 880×1230 1/16 印张 58.75 字数 1 797 千字
2009 年 2 月第一版 2009 年 2 月第一次印刷

*

定价 280.00 元

出 版 说 明

在信息化社会，信息技术飞速发展，随之而来的信息技术的安全问题日益突出，它关系到信息系统的正常运行和健康发展，影响到信息化社会的各个方面，不容忽视。国家标准化管理委员会已制定和发布了一系列信息安全国家标准，为我国信息系统的安全提供了技术支持，为信息安全的监督和管理提供了依据和指导。

为满足广大信息技术人员的需求，方便学习和查阅，我们将信息安全国家标准按照信息安全标准体系收集、分类、汇编成卷，共分为以下5卷：

——基础卷

——信息安全管理卷

——信息安全测评卷

——技术与机制卷

——密码技术卷

其中基础卷、信息安全测评卷、技术与机制卷根据需要又分为若干分册。

随着信息安全标准体系的完善和标准制修订情况的变化，本套汇编将陆续分卷分册出版。

本册为信息安全测评卷的测评基础和系统测评分册，共收入截至2008年11月发布的相关标准12项，标准化指导性技术文件1项。

编　　者

2008年11月

目　　录

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

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

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

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

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。

2.2

赋值 assignment

说明组件中已标识的参数。

2.3

保证 assurance

实体达到其安全性目的的信任基础。

2.4

攻击潜力 attack potential

成功实施一次攻击或将要发起一次攻击的潜在能力，用攻击者的专业水平、资源和动机来表示。

2.5

增强 augmentation

将 GB/T 18336.3 规定的一个或多个保证组件加入到评估保证级(EAL)或保证包中。

2.6

鉴别数据 authentication data

用于验证用户所声称身份的信息。

2.7

授权用户 authorised user

依据 TSP 可以执行某项操作的用户。

2.8

类 class

具有共同目的的族的集合。

2.9

组件 component

可包含在 PP、ST 或一个包中的最小可选元素集。

2.10

连通性 connectivity

允许与 TOE 之外的 IT 实体进行交互的 TOE 特性，包括在任何环境或配置下通过任意距离的有线或无线方式的数据交换。

2.11

依赖关系 dependency

要求之间的一种关系，一个要求要达到其目的必须依赖另一个要求的满足。

2.12

元素 element

一个不可再分的安全要求。

2.13

评估 evaluation

依据确定的准则，对 PP、ST 或 TOE 的评价。

2.14

评估保证级 evaluation assurance level；EAL

由 GB/T 18336.3 中保证组件构成的包，该包代表了 GB/T 18336 预先定义的保证尺度上的某个位置。

2.15

评估管理机构 evaluation authority

通过评估体制为特定团体贯彻实施 GB/T 18336 的机构，此机构负责制定标准和监控团体内各部门所执行评估的质量。

2.16

评估体制 evaluation scheme

一种行政管理和监督管理框架，在此框架下评估管理机构在特定团体中实施 GB/T 18336。

2.17

扩展 extension

把不包括在 GB/T 18336.2 中的功能要求或 GB/T 18336.3 中的保证要求增加到 ST 或 PP 中。

2.18

外部 IT 实体 external IT entity

在 TOE 之外与其交互的任何可信或不可信的 IT 产品或系统。

2.19

族 family

一组具有共同安全目的、但侧重点或严格程度可能不同的组件的集合。

2.20

形式化 formal

基于公认的数学概念，采用具有确定语义并有严格语法的语言表达。

2.21

指导性文档 guidance documentation

指导 TOE 用户、管理者和集成者如何交付、安装、配置、操作、管理和使用 TOE 的文档。有关指导性文档的范围、主要内容等方面的要求常在 PP 或 ST 中定义。

2.22

人员用户 human user

与 TOE 交互的任何人员。

2.23

身份 identity

能唯一标识一个授权用户的表示法(比如一个字符串)，它可以是该用户的全名或缩写名，也可以是一个假名。

2.24

非形式化 informal

采用自然语言表达。

2.25

内部通信信道 internal communication channel

TOE 各分离部分间的通信信道。

2.26

TOE 内部传送 internal TOE transfer

在 TOE 各分离部分之间交换数据。

2.27

TSF 间传送 inter-TSF transfer

在 TOE 与其他可信 IT 产品的安全功能之间交换数据。

2.28

反复 iteration

一个组件在不同操作中多次使用。

2.29

客体 object

在 TSC 中包含有或接收信息的并由主体操作的一个实体。

2.30

组织安全策略 organisational security policies

一个组织为其运转而强制推行的一个或多个安全规则、程序、惯例和指南。

2.31

包 package

为满足一组确定的安全目的而组合在一起的，一组可重用的功能或保证组件(如，一个 EAL)。

2.32

产品 product

一个 IT 软件、固件或硬件包，提供相关功能且可用于或组合到多种系统中。

2.33

保护轮廓 protection profile;PP

满足特定用户需求的、一类 TOE 的、一组与实现无关的安全要求。

2.34

基准监视器 reference monitor

执行 TOE 访问控制策略的一种抽象机的概念。

2.35

基准确认机制 reference validation mechanism

具有以下特性的基准监视器概念的一种实现：防篡改、一直运行、简单到能对其进行彻底的分析和测试。

2.36

细化 refinement

为组件添加细节。

2.37

角色 role

一组预先确定的规则，规定在一个用户和 TOE 之间所允许的交互行为。

2.38

秘密 secret

为了执行一个特定的 SFP，必须仅由授权用户或 TSF 才可知晓的信息。

2.39

安全属性 security attribute

用于执行 TSP 的，主体、用户、客体、信息或资源的特征。

2.40

安全功能 security function;SF

为执行 TSP 中一组密切相关的规则子集而必须依赖的 TOE 的一个或多个部分。

2.41

安全功能策略 security function policy;SFP

由一个 SF 执行的安全策略。

2.42

安全目的　security objective

意在对抗特定的威胁或满足特定的组织安全策略和假设的一种陈述。

2.43

安全目标　security target;ST

作为一个既定 TOE 的评估基础使用的一组安全要求和规范。

2.44

选择　selection

从组件内列项表中指定一项或多项。

2.45

半形式化　semiformal

采用具有确定语义并有严格语法的语言表达。

2.46

功能强度　strength of function;SOF

TOE 安全功能的一种指标，表示通过直接攻击其基础安全机制，破坏其预期安全行为所需要的最小代价。

2.47

基本级功能强度　SOF-basic

一种 TOE 功能强度级别，分析表明本级别安全功能足够对抗拥有低攻击潜力的攻击者对 TOE 安全的偶发攻击。

2.48

中级功能强度　SOF-medium

一种 TOE 功能强度级别，分析表明本级别安全功能足够对抗拥有中等攻击潜力的攻击者对 TOE 安全的直接或故意攻击。

2.49

高级功能强度　SOF-high

一种 TOE 功能强度级别，分析表明本级别安全功能足够对抗拥有高等攻击潜力的攻击者对 TOE 安全的有计划、有组织攻击。

2.50

主体　subject

在 TSC 中实施操作的实体。

2.51

系统　system

具有特定用途和运行环境的专用 IT 装置。

2.52

评估对象　target of evaluation;TOE

作为评估主体的 IT 产品或系统以及相关的指导性文档。

2.53

TOE 资源　TOE resource

TOE 中任何可用或可消耗的东西。

2.54

TOE 安全功能　TOE security functions;TSF

正确执行 TSP 所必须依赖的所有 TOE 硬件、软件和固件的集合。

2.55

TOE 安全功能接口　TOE security functions interface;TSFI

一组交互式(人机接口)或编程(应用编程接口)接口,TSF 通过这些接口访问、调配 TOE 资源,或者通过它们从 TSF 中获取信息。

2.56

TOE 安全策略　TOE security policy;TSP

规定在一个 TOE 中如何管理、保护和分配资产的一组规则。

2.57

TOE 安全策略模型　TOE security policy model

TOE 所执行的安全策略的一种结构化表示。

2.58

TSF 控制外传送　transfers outside TSF control

与不受 TSF 控制的实体交换数据。

2.59

可信信道　trusted channel

一种手段,通过该手段 TSF 能同远程可信 IT 产品进行所需信任的通信,从而支持 TSP。

2.60

可信路径　trusted path

一种手段,通过该手段用户能同 TSF 进行所需信任的通信,从而支持 TSP。

2.61

TSF 数据　TSF data

由 TOE 产生的或为 TOE 产生的数据,这些数据可能会影响 TOE 的运行。

2.62

TSF 控制范围　TSF scope of control;TSC

服从 TSP 规则的,可与 TOE 交互或在 TOE 中发生的交互的集合。

2.63

用户　user

在 TOE 之外,与 TOE 交互的任何实体(人员用户或外部 IT 实体)。

2.64

用户数据　user data

由用户产生或为用户产生的数据,这些数据不影响 TSF 的运行。

2.65

规范性　normative

规范性文本"描述文档范围,并陈述规定"(ISO/IEC 导则第 2 部分)。除明确标明"资料性"外,GB/T 18336的所有文本都是规范性的。任何与"满足要求"有关的文本都是规范性的。

2.66

资料性　informative

资料性文本"提供额外的信息以帮助理解或使用文档"(ISO/IEC 导则第 2 部分)。资料性文本与"满足要求"无关。

2.67

应　shall

在规范性文本中,"应"指"为了遵守该文档,严格遵循某些要求,不允许有任何偏离"(ISO/IEC 导则第 2 部分)。

2.68

宜 should

在规范性文本中，“宜”指“在几个可能性中，某个可能性被认为是特别适当的，不提及也不排除其他可能性；或者某个动作是首选的但不是必需的”(ISO/IEC 导则第 2 部分)。GB/T18336 对“不是必需的”的解释是：对于其他可能的选择，需要给出为何不选择首选项的理由。

2.69

可 may

在规范性文本中，“可”指“在文档限制范围内可允许的一连串行动”(ISO/IEC 导则第 2 部分)。

2.70

能 can

在规范性文本中，“能”指的是“可能性和能力的陈述，无论是材料的、物理的或逻辑的”(ISO/IEC 导则第 2 部分)。

3 缩略语

以下缩略语在 GB/T 18336 各部分中通用：

EAL	评估保证级	(Evaluation Assurance Level)
IT	信息技术	(Information Technology)
PP	保护轮廓	(Protection Profile)
SF	安全功能	(Security Function)
SFP	安全功能策略	(Security Function Policy)
SOF	功能强度	(Strength of Function)
ST	安全目标	(Security Target)
TOE	评估对象	(Target of Evaluation)
TSC	TSF 控制范围	(TSF Scope of Control)
TSF	TOE 安全功能	(TOE Security Functions)
TSFI	TSF 接口	(TSF Interface)
TSP	TOE 安全策略	(TOE Security Policy)

4 概述

4.1 引言

本章介绍 GB/T 18336 的一些主要概念，并给出了目标读者、评估相关要素以及文档的组织方式。

IT 产品或系统所拥有的信息是能使组织成功完成其使命的关键资源。此外，人们也期望存放在 IT 产品或系统中的私人信息保持私密性，在其需要时可用，且不被未授权修改。当对信息进行正确控制，以确保它不受诸如不必要的或无保证的传播、更改或丢失等方面危害时，IT 产品或系统需执行它们的功能。“IT 安全”这个术语就是用于概括这些危害和类似危害的预防和缓解。

许多 IT 客户缺乏相关的知识、经验和资源，用以判断其 IT 产品或系统的安全性是否恰当，并且他们并不希望仅仅依赖开发者的声明。因此，客户可选择定制一个对 IT 产品或系统安全性的分析(即一个安全评估)来增加他们对其安全措施的信心。

GB/T 18336 能用于选择恰当的 IT 安全措施，并且它含有评估安全要求的标准。

4.1.1 GB/T 18336 的目标读者

有三类最关心 IT 产品和系统安全性评估的人员：TOE 客户、TOE 开发者和 TOE 评估者。本标准在文本组织上已充分考虑了这三类人员的需求。认为他们都是 GB/T 18336 的主要用户。正如下条文所述，这三类人员都能从标准中受益。

4.1.1.1 客户

客户选择 IT 安全要求来表达其组织的需求时，GB/T 18336 起着重要的技术支持作用。制定 GB/T 18336，就是确保评估能满足客户的需求，因为满足客户的需求是评估的根本目的和缘由。

客户能使用评估结果来帮助决定一个已评估过的产品或系统是否满足他们的安全需求，这些安全需求通常是风险分析和策略导向的结果。客户也可以用这些评估结果来比较不同的产品或系统，保证要求的分级表述就是为了满足这一需求。

GB/T 18336 为客户，尤其是客户群和相关团体，提供一个独立于实现的结构，即保护轮廓(PP)，以陈述他们对 TOE 中 IT 安全措施的特殊要求。

4.1.1.2 开发者

GB/T 18336 可为开发者在准备和协助评估其产品或系统，以及识别他们的每种产品或系统需要满足的安全要求时提供支持。在评估结果的互认协定配合下，相关评估方法将进一步允许 GB/T 18336支持除 TOE 开发者之外的其他人准备和协助评估开发者的一个 TOE，也是完全可能的。

依据规定的安全功能和保证都已通过了评估，GB/T 18336 结构能用于声称 TOE 满足其既定的安全要求。每一个 TOE 的要求都包含在一个与实现相关的结构中，该结构称为安全目标(ST)。一个或多个 PP 可提供具有广泛客户基础的一些要求。

GB/T 18336 描述了一些安全功能，可供开发者纳入 TOE 中。GB/T 18336 能用于确定责任和行为，以支持 TOE 评估所必要的证据。它也定义了证据的内容和表现形式。

4.1.1.3 评估者

GB/T 18336 可被评估者用来判定 TOE 与其安全要求是否一致。GB/T 18336 描述了一组由评估者施行的普遍行为以及执行这些行为所基于的安全功能。值得注意的是 GB/T 18336 没有指定施行这些行为应遵守的程序。

4.1.1.4 其他读者

虽然，GB/T 18336 主要是为了规范和评估 TOE 的 IT 安全特性，但它也可以供对 IT 安全有兴趣或有责任的所有各方参考。其他能够从 GB/T 18336 所包含的信息中获益的群体有：

a) 系统管理员和系统安全员，负责确定和处理组织的 IT 安全策略和要求；
b) 内部和外部审计员，负责评定一个系统的安全性是否足够；
c) 安全架构师和设计师，负责规范 IT 系统和产品的安全内容；
d) 认可者，负责认可一个 IT 系统在特定环境中的使用；
e) 评估发起者，负责申请和支持一个评估；
f) 评估管理机构，负责管理和监督 IT 安全性评估程序。

4.2 评估相关要素

为了使评估结果具有更好的可比性，评估宜在一个权威的评估体制框架内执行，该体制框架负责设定标准、监控评估质量、掌管评估机构和评估者必须遵守的规章制度。

GB/T 18336 不对监管框架提出要求。但是，要达到评估结果相互认可的目标，不同评估管理机构的监管框架必须是一致性的。图 1 描述了构成评估相关要素的主要因素。

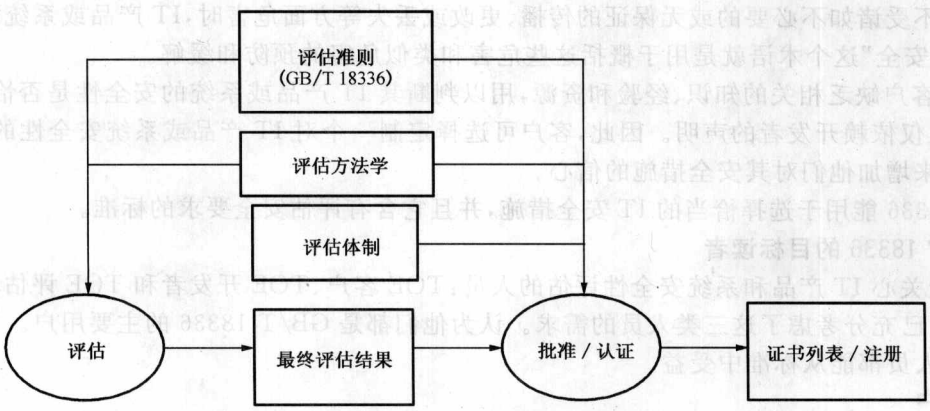

图 1 评估相关要素