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
北京复兴门外三里河北街16号
邮政编码:100045
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
新华书店北京发行所发行 各地新华书店经售
*
开本 880×1230 1/16 印张 2½ 字数 36 千字
2001年10月第一版 2001年10月第一次印刷
印数 1—1 500
*
书号:155066·1-17785 定价 18.00 元
网址 www.bzcbs.com
*
科 目 581—549

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

程，据此授权信息技术产品和系统在其整个运行环境中投入使用。评估集中于产品和系统的信息技术安全部分，以及直接影响到安全使用信息技术要素的那些运行环境，因而评估结果是认可过程的有效依据。但是，当其他技术更适合于评价非信息技术相关的系统或产品的安全特性及其与信息技术安全部分的关系，认可者应分别作出这些方面的认可。

e) CC 不包括密码算法固有质量评价准则。如果需要对嵌入 TOE 的密码数学特性进行单独的评价，则在使用 CC 的评估体制中必须提供这样的评价。

2 引用标准

下列标准所包括的条文，通过在本标准中引用而构成为本标准的条文。本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

GB/T 9387.2-1995 信息处理系统 开放系统互连 基本参考模型 第 2 部分：安全体系结构 (idt ISO 7498-2:1989)

3 定义

3.1 通用缩略语

以下缩略语在 CC 各部分中通用：

CC： 通用准则(Common Criteria)

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)

3.2 术语表的范围

本条只收录在 CC 中有特殊用法的术语。在 CC 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 ISO 或 GB 安全术语定义，或根据熟知的安全性术语定义。在 CC 中一些不便于定义的、由通用术语组合成的复合词，将在使用他们的地方进行解释。在 GB/T 18336 第 2 部分和第 3 部分的“范例”章条中可以见到术语和概念的解释。

3.3 术语表

3.3.1 资产 assets

由 TOE 安全策略保护的信息或资源。

3.3.2 赋值 assignment

规定组件中的一个特定参数。

3.3.3 保证 assurance

实体达到其安全性目的的信任基础。

3.3.4 攻击潜力 attack potential

可察觉的成功实施攻击的可能性，如果发起攻击，其程度用攻击者的专业水平、资源和动机来表示。

3.3.5 **增强 augmentation**

将 GB/T 18336 第 3 部分若干个保证组件加入到 EAL 或保证包中。

3.3.6 **鉴别数据 authentication data**

用于验证用户所声称身份的信息。

3.3.7 **授权用户 authorised user**

依据 TSP 可以执行某项操作的用户。

3.3.8 **类 class**

具有共同目的的子类的集合。

3.3.9 **组件 component**

可包含在 PP、ST 或一个包中的最小可选元素集。

3.3.10 **连通性 connectivity**

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

3.3.11 **依赖关系 dependency**

各种要求之间的关系，一种要求要达到其目的必须依赖另一种要求的满足。

3.3.12 **元素 element**

不可再分的安全要求。

3.3.13 **评估 evaluation**

依据确定的准则，对 PP、ST 或 TOE 的评价。

3.3.14 **评估保证级 evaluation assurance level；EAL**

由 GB/T 18336 第 3 部分中保证组件构成的包，该包代表了 CC 预先定义的保证尺度上的某个位置。

3.3.15 **评估管理机构 evaluation authority**

依据评估体制，在特定团体中贯彻 CC、确定标准和监督团体内各种评估质量的管理机构。

3.3.16 **评估体制 evaluation scheme**

指导评估管理机构在特定团体中使用 CC 的管理与法定框架。

3.3.17 **扩展 extension**

把不包括在 GB/T 18336 第 2 部分中的功能要求或第 3 部分中的保证要求增加到 ST 或 PP 中。

3.3.18 **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。

3.3.19 **子类 family**

一组具有共同安全目的，但侧重点或严格性可能不同的组件的集合。

3.3.20 **形式化 formal**

在完备数学概念基础上，采用具有确定语义并有严格语法的语言表达的。

3.3.21 **个人用户 human user**

与 TOE 交互的任何个人。

3.3.22 **身份 identity**

能唯一标识一个授权用户的表示（比如字符串），它可以是全名、缩写名或假名。

3.3.23 **非形式化 informal**

采用自然语言表达的。

3.3.24 **内部通信信道 internal communication channel**

TOE 中各分离部分间的通信信道。

3.3.25 **TOE 内部传送 internal TOE transfer**
TOE 中各分离部分之间的数据通信。

3.3.26 **TSF 间传送 inter-TSF transfer**
TOE 与其它可信 IT 产品安全功能之间的数据通信。

3.3.27 **反复 iteration**
一个组件在不同操作中多次使用。

3.3.28 **客体 object**
在 TSC 中由主体操作的、包含或接收信息的实体。

3.3.29 **组织安全策略 organisational security policies**
组织为保障其运转而规定的若干安全规则、过程、规范和指南。

3.3.30 **包 package**
为了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 EAL)。

3.3.31 **产品 product**
IT 软件、固件或硬件的包,其功能用于或组合到多种系统中。

3.3.32 **保护轮廓 protection profile;PP**
满足特定用户需求、与一类 TOE 实现无关的一组安全要求。

3.3.33 **参照监视器 reference monitor**
执行 TOE 访问控制策略的抽象机概念。

3.3.34 **参照确认机制 reference validation mechanism**
具有以下特性的参照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。

3.3.35 **细化 refinement**
为组件添加细节。

3.3.36 **角色 role**
一组预先确定的规则,规定在用户和 TOE 之间许可的交互。

3.3.37 **秘密 secret**
为了执行特定 SFP,必须只能有授权用户或 TSF 才知晓的信息。

3.3.38 **安全属性 security attribute**
用于执行 TSP 的与主体、用户或客体相关的信息。

3.3.39 **安全功能 security function;SF**
为执行 TSP 中一组紧密相关的规则子集而必须依赖的部分 TOE。

3.3.40 **安全功能策略 security function policy;SFP**
SF 执行的安全策略。

3.3.41 **安全目的 security objective**
意在对抗特定的威胁、满足特定的组织安全策略和假设的陈述。

3.3.42 **安全目标 security target;ST**
作为指定的 TOE 评估基础的一组安全要求和规范。

3.3.43 **选择 selection**
从组件的项目表中指定一项或几项。

3.3.44 **半形式化 semiformal**
采用具有确定语义并有严格语法的语言表达的。

3.3.45 **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,攻破所设计的安全功能所需要的

最小代价。

3.3.46 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低潜力攻击者对 TOE 安全的偶发攻击。

3.3.47 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中等潜力攻击者对 TOE 安全直接或故意的攻击。

3.3.48 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高等潜力攻击者对 TOE 安全有计划、有组织的攻击。

3.3.49 主体 subject

在 TSC 中实施操作的实体。

3.3.50 系统 system

具有特定目的和运行环境的专用 IT 装置。

3.3.51 评估对象 target of evaluation；TOE

作为评估主体的 IT 产品及系统以及相关的管理员和用户指南文档。

3.3.52 TOE 资源 TOE resource

TOE 中可用或可消耗的所有东西。

3.3.53 TOE 安全功能 TOE security function；TSF

正确执行 TSP 所必须依赖的 TOE 全部硬件、软件和固件的集合。

3.3.54 TOE 安全功能接口 TOE security function interface；TSFI

一组交互式（人机接口）或编程（应用编程接口）接口，通过它，TSF 访问、调配 TOE 资源，或者从 TSF 中获取信息。

3.3.55 TOE 安全策略 TOE security policy；TSP

规定 TOE 中资产管理、保护和分配的一组规则。

3.3.56 TOE 安全策略模型 TOE security policy model

TOE 执行的安全策略的结构化表示。

3.3.57 TSF 控制外传送 transfers outside TSF control

与不受 TSF 控制的实体交换数据。

3.3.58 可信信道 trusted channel

TSF 和远程可信 IT 产品间的一种通信方式，该方式对 TSP 的支持具有必要的置信度。

3.3.59 可信路径 trusted path

用户和 TSF 间的一种通信方式，该方式对 TSP 的支持具有必要的置信度。

3.3.60 TSF 数据 TSF data

TOE 产生的或为 TOE 产生的数据，这些数据可能会影响 TOE 的操作。

3.3.61 TSF 控制范围 TSF scope of control；TSC

可与 TOE 或在 TOE 中发生的并服从 TSP 规则的交互集合。

3.3.62 用户 user

在 TOE 之外与 TOE 交互的任何实体（个人用户或外部 IT 实体）。

3.3.63 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 的操作。

4 概述

本章介绍 CC 的主要概念，确定目标读者、评估环境和组织材料的方法。

4.1 引言

IT 产品和系统拥有的信息是能使组织成功完成其任务的关键资源。此外，人们也要求保护 IT 产品和系统内的私人信息的私密性、可用性，并防止未授权的更改。当对信息进行正确控制以确保它能防止冒险，诸如不必要的或无保证的传播、更改或遗失，IT 产品和系统应执行它们的功能。“IT 安全”用于概括预防和缓解这些及类似的冒险。

许多 IT 用户缺乏判断其 IT 产品和系统的安全性是否恰当的知识、经验和资源，他们并不希望仅仅依赖开发者的声明。用户可借助对 IT 产品和系统的安全分析（即安全评估）来增加他们对其安全措施的信心。

CC 可用来选择恰当的 IT 安全措施，它包括了评估安全需求的准则。

4.2 CC 的目标读者

有三组都关心 IT 产品和系统的安全性评估的读者：TOE 用户、TOE 开发者和 TOE 评估者。CC 中提出的准则从文档结构上支持所有三个组的需求，他们都被认为是 CC 的主要使用者。正如下文所述，这三个组都能从该准则中受益。

4.2.1 用户

当用户选择 IT 安全要求来表达他们的组织需求时，CC 起到重要的技术支持作用。CC 从写作安排上确保评估满足用户的需求，因为这是评估过程的根本目的和理由。

用户可以用评估结果来决定一个已评估的产品和系统是否满足他们的安全需求，这些需求通常是风险分析和政策导向的结果。分等级的保证要求，使用户可以用评估结果来比较不同的产品和系统。

CC 为用户，尤其是用户群和利益共同体，提供一个独立于实现的框架，称为保护轮廓，用户在保护轮廓里表明他们对评估对象中的 IT 安全措施的特殊需求。

4.2.2 开发者

CC 也为开发者在准备和协助评估产品或系统以及确定每种产品和系统要满足的安全需求方面提供支持。只要有一个相关的评估方法和双方对评估结果的认可协定，CC 还可以在准备和协助开发者的 TOE 评估方面支持除 TOE 开发者之外的其他人。

CC 结构还可以通过评估特定的安全功能和保证来声称 TOE 符合特定的安全需求。每一个 TOE 的需求都包含在一个名为安全目标（ST）的与实现相关的概念中，广大用户的需求由一个或多个 PP 提供。

CC 描述的安全功能可被开发者包括在 TOE 内。CC 可用来确定责任和行为以支持 TOE 评估所必要的证据，它也定义证据的内容和表现形式。

4.2.3 评估者

CC 包含评估者判定 TOE 与其安全需求一致时所使用的准则。CC 用于描述评估者通常执行的一系列行为和执行这些行为所基于的安全功能。值得注意的是 CC 没有规定执行这些行动的过程。

4.2.4 其他读者

由于 CC 面向 TOE 的 IT 安全特性的规范和评估，它也可以作为对 IT 安全有兴趣或有责任的所有团体的参考资料。其他能够从 CC 所包含的信息中获益的群体有：

a）系统管理员和系统安全管理员：负责确定和达到组织的 IT 安全策略和需求。

b）内部和外部审计员：负责评定系统安全性能是否充分。

c）安全规划和设计者：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：负责请求和支持一个评估。

f) 评估机构:负责管理和监督 IT 安全评估程序。

4.3 评估上下文

为了使评估结果达到更好的可比性,评估应在权威的评估体制框架内执行,该框架规定了标准、监控评估质量并管理评估的工具,以及评估者必须遵守的规则。

CC 并不规定对管理框架的要求,但是不同评估机构的管理框架必须是一致性的,以使这样的评估结果可以互认。图 4.1 描述了构成评估上下文的主要部分。

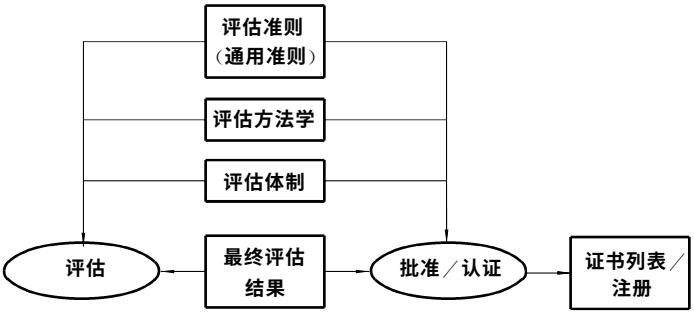

图 4.1 评估上下文

通用评估方法学有助于提供结果的可重复性和客观性,但仅靠方法学本身不够充分。许多评估准则需要使用专家判断和一定的背景知识,而这些更难达到一致。为了增强评估结果的一致性,最终的评估结果应提交给一个认证过程,该过程是一个针对评估结果的独立的检查过程,并生成最终的证书或正式批文,该证书通常是公开的。要说明的是,认证过程是使得 IT 安全准则应用得到更好一致性的一种手段。

评估体制、方法学和认证过程是管理评估体制的评估机构的责任,不属 CC 的范围。

4.4 CC 的文档组织

CC 由一系列不同但又相互关联的部分组成,这些部分描述中所用的术语在第 5 章解释。

a) 第 1 部分:简介和一般模型,是 CC 的简介。它定义了 IT 安全评估的一般概念和原理,并提出了评估的一般模型。第 1 部分也提出了若干结构,这些结构可用于表达 IT 安全目的,用于选择和定义 IT 安全要求,以及用于书写产品和系统的高层次规范。另外,CC 每一部分都针对该部分目标读者来陈述。

b) 第 2 部分:安全功能要求,建立一系列功能组件作为表达 TOE 功能要求的标准方法。第 2 部分列出了一系列功能组件、子类和类。

c) 第 3 部分:安全保证要求,建立一系列保证组件作为表达 TOE 保证要求的标准方法。第 3 部分列出一系列保证组件、子类和类。第 3 部分也定义了 PP 和 ST 的评估准则,并提出了评估保证级,即定义了评定 TOE 保证的 CC 预定义尺度,这被称为评估保证级。

为支持上面所列的 CC 的三个部分,将出版其他类型的文档,包括技术上的基本原理和指导文档。

表 4.1 列出了主要的三组读者及其可能感兴趣的 CC 内容。

表 4.1 CC 使用指南

	用户	开发者	评估者
第 1 部分	用于了解背景信息和参考。PP 的指导性结构。	用于了解背景信息,开发安全要求和形成 TOE 的安全规范的参考。	用于了解背景信息和参考。PP 和 ST 的指导性结构。
第 2 部分	在阐明安全功能要求的描述时用作指导和参考。	用于解释功能要求和生成 TOE 功能规范的参考。	当确定 TOE 是否有效地符合已声明的安全功能时,用作评估准则的强制性描述。
第 3 部分	用于指导保证需求级别的确定。	当解释保证要求描述和确定 TOE 的保证措施时,用作参考。	当确定 TOE 的保证和评估 PP 和 ST 时,用作评估准则的强制描述。

5 一般模型

本章提出了贯穿 CC 使用的一般概念，其中也包括使用这些概念的上下文，以及 CC 使用这些概念的方法。第 2 部分或第 3 部分在使用这些概念的基础上进一步展开，并假设使用了本章描述的方法。本章假定读者已具备 IT 安全的一些知识，并非作为该领域的教材。

CC 用一系列安全性概念和术语来讨论安全性。对这些概念和术语的理解是有效运用 CC 的前提条件。但是，这些概念本身又是相当通用的，无意将这类 IT 安全的问题限于 CC 应用。

5.1 安全上下文

5.1.1 一般安全上下文

安全涉及保护资产不受威胁，威胁可依据滥用被保护资产的可能性进行分类。应该考虑所有的威胁类型，但在安全领域内，与恶意的或其他人类活动相关的威胁应给予更多的重视。图 5.1 说明了高层次概念和关系。

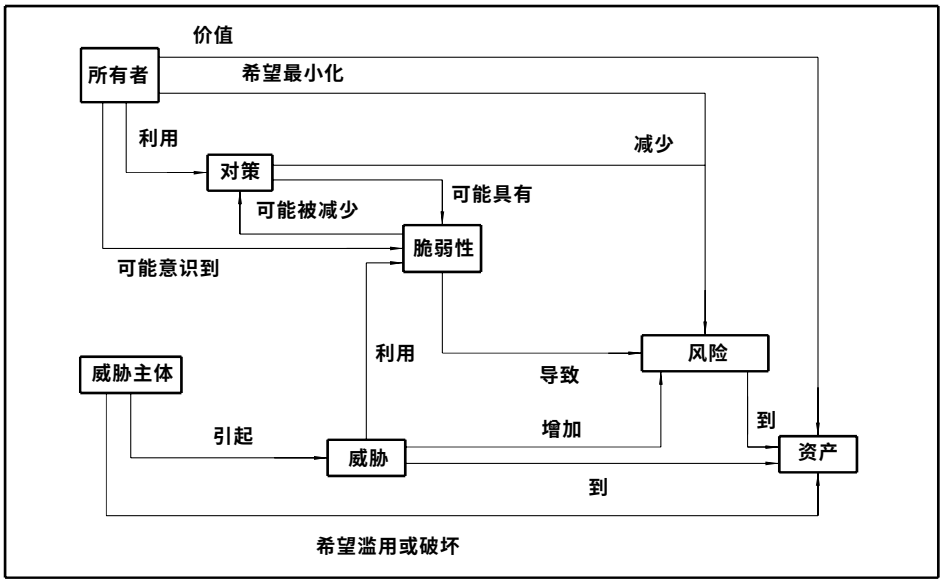

图 5.1 安全概念和关系

保护关注的资产是那些对资产赋予价值的所有者的责任。实际或假定的威胁主体对资产也赋予了一定的价值，并希望以违背所有者初衷的方式滥用资产。所有者将会意识到这种威胁可能致使资产损坏，对所有者而言资产中的价值将会降低。安全性损坏一般包括但又不仅包括以下几项：资产破坏性地暴露于未授权的接收者（丧失保密性），资产由未授权地更改而损坏（丧失完整性），或资产的访问权被未授权地剥夺（丧失可用性）。

资产所有者应分析可能的威胁并确定哪些存在于他们的环境，其结果就是风险。这种分析会有助于对策的选择，以应对风险并将其降低到一个可接受的水平。

对策用以减少脆弱性并满足资产所有者的安全策略（直接或间接的为其他部分提供引导）。在对策使用后仍会有残留的脆弱性，这些残留的脆弱性仍可以被威胁者利用，从而造成了资产的残余风险。资产所有者会通过给出其他的约束来寻求最小的残余风险。

在资产所有者将其资产暴露于特定威胁之前，所有者需要确信其对策足以应付面临的威胁。所有者自己可能没有能力对对策的所有方面加以判断，但可以寻求对对策的评估。评估结果是对保证性可达到程度的描述，即信任对策能用于降低所保护资产的风险。该描述还将对策的保证性进行分级。保证性是对策的特性，这种特性是信任正确操作的基础。资产所有者可以根据此描述决定是否接受将资产暴露给威胁所冒的风险。图 5.2 说明了这种关系。

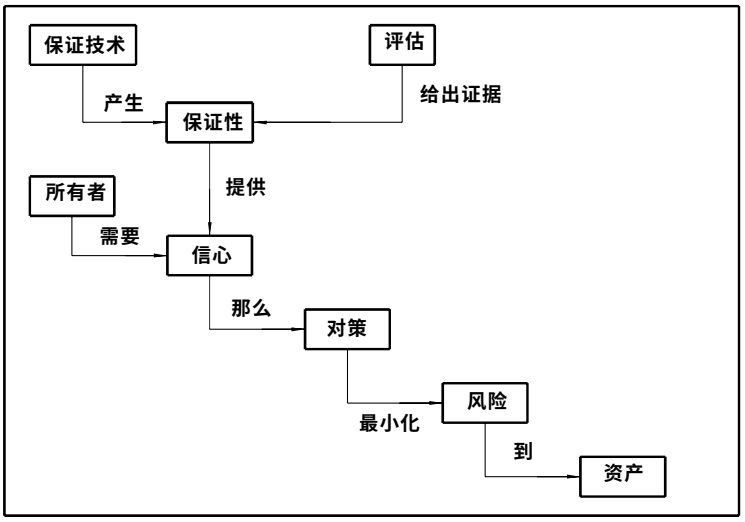

图 5.2 评估概念和关系

通常,资产所有者应当对资产负责,并应能对作出接受暴露资产于威胁前的决定进行论证。这就需要上述评估结果是可以论证的。那么,评估应产生客观的、可重复的可被引用作证据的结论。

5.1.2 信息技术安全环境

许多资产是以信息的形式被 IT 产品或系统所储存、处理和传送,以满足信息所有者的需求。信息所有者可能会要求严格控制任何对此类信息数据的传播和修改。他们可能会要求 IT 产品或系统实现某些专门的 IT 安全控制,作为所采用的对付数据威胁的部分对策。

为了满足特定的需要而获取和建造 IT 系统,出于经济上的原因,往往充分利用现有(常用的)IT 产品,如操作系统、通用组件和硬件平台。一个系统实现的 IT 安全对策可能利用低层 IT 产品的功能,并依赖于对 IT 产品安全功能的正确操作,所以 IT 产品评估也可以作为 IT 系统安全评估的一部分。

当一个 IT 产品可以集成到(或被考虑集成到)多个 IT 系统时,该产品安全方面的评估可独立进行,并建立一个被评估的产品目录,这样做更经济。这种评估的结果应支持产品在多个 IT 系统中的应用,避免不同系统中为检查产品的安全性进行不必要的重复工作。

一个 IT 系统的认可者在确定 IT 和非 IT 对策是否为数据提供了适当保护方面,与信息所有者的权力相当,并可决定是否允许系统运行。该认可者可以要求对 IT 对策进行评估,以确定 IT 对策是否提供充分的保护,以及指定的对策是否被 IT 系统正确实现。这类评估可以采取不同的形式和严格程度,这取决于所使用的规则或认可者。

5.2 CC 方法

对 IT 安全性的信任是通过开发、评估和操作过程中的各种措施获得的。

5.2.1 开发

CC 不规定任何特定的开发方法和生命周期模型。图 5.3 描述了安全要求和评估对象之间关系的基本假设。该图用于提供讨论的基础,不应理解为某一种方法(如瀑布法)比另一种方法(如原型法)更优越。

重要的是,在开发阶段建立的安全要求对满足用户的安全目的意义重大。除非在开发过程的开始阶段确定合适的需求,否则即便用再好的工程方法,其最终产品也不能达到预期用户的目的。

该过程的基础是将安全要求细化为安全目标中的 TOE 概要规范。每个低层次的细化代表具有更为详细设计的设计分解。最低的抽象表示是 TOE 实现本身。

CC 并不规定一套专有的设计表示方法。CC 的要求应有充分的设计表达方法,该方法应在需要时以足够详细的程度表明:

a) 每个层次的细化是更高层次的完全实例化(这就是说,所有 TOE 的高层次抽象定义的安全功

能、特性和行为都必须在低层次上明确体现）。

b）每个层次的细化是更高层次的精确实例化（这就是说，不存在低层次抽象定义的功能、特性和行为不为高层次定义所需要的）。

CC 保证准则区分诸如功能规范、高层设计、低层设计和实现等抽象层次。依据规定的保证级，可能要求开发者表明开发方法是如何满足 CC 保证要求的。

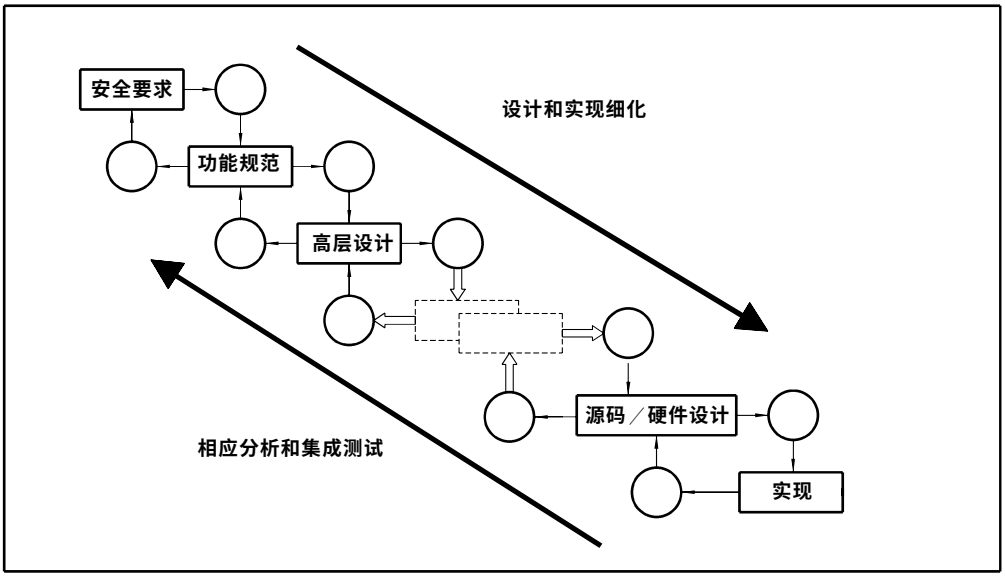

图 5.3 评估对象开发模型

5.2.2 TOE 评估

图 5.4 描述的 TOE 评估过程可能与开发过程同步进行，或随后进行。TOE 评估过程的主要输入有：

a）一系列 TOE 证据，包括作为 TOE 评估基础的评估过的 ST；

b）需要评估的 TOE；

c）评估准则、方法学和体制。

另外，说明性材料（例如 CC 的应用注释）和评估者及评估组织的 IT 安全专业知识也常用来作为评估过程的输入。

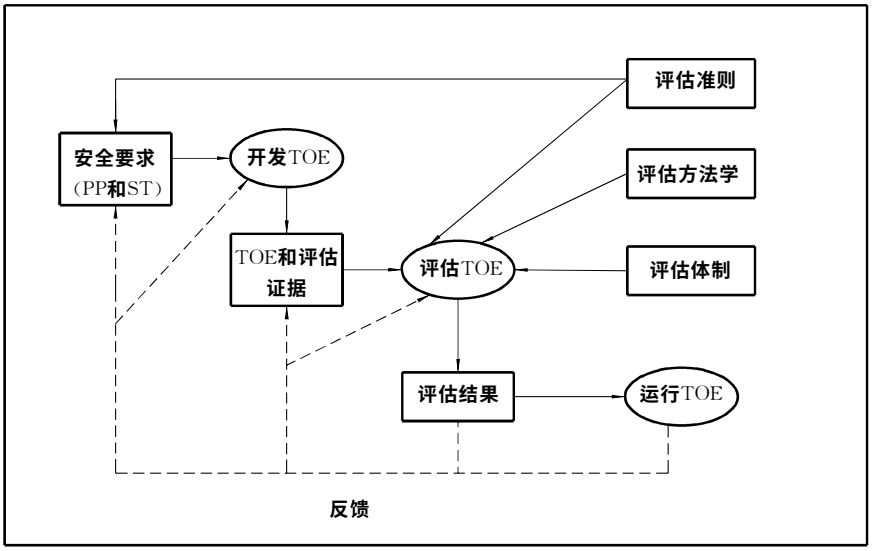

图 5.4 TOE 评估过程

评估过程的预期结果是对 TOE 满足 ST 中安全要求的确认，其形式是评估者依据评估准则对

TOE 得出的一个或多个记载调查结果的报告。这些报告对 TOE(产品或系统)的实际用户和潜在用户非常有用,对开发者也同样有用。

通过评估获得的信任度依赖于所达到的保证要求(即评估保证级)。

评估通过两种途径促成产生更好的安全产品。评估意在发现 TOE 错误或脆弱性,以便开发者纠正,从而减少在以后操作中安全失效发生的可能性;或为了迎接严格的评估,开发者在 TOE 设计和开发时会更加细心。因此,评估过程对最初需求、开发过程、最终产品以及操作环境产生强烈的、虽然是间接的但又是积极的影响。

5.2.3 运行

用户可选择评估后的 TOE 用在他们的环境中。一旦运行 TOE,可能出现以前未知的错误或脆弱性,或者需要修改对环境的假设。作为运行的结果,可以通过反馈,要求开发者修改 TOE 或重新定义它的安全要求和环境假设。这些变化可能要求重新评估 TOE 或加强其运行环境的安全性。在一些情况中只需评估需要修改部分,以便重获对 TOE 的信赖。尽管 CC 中包括了保证性维护准则,但并不包括重新评估的详细过程以及评估结果的重复使用。

5.3 安全概念

在支持安全 TOE 开发和评估的工程过程和管理框架的方面,评估准则是最有用的。本条仅提供例证和指导,并不限制可能使用 CC 的分析过程、开发方法、评估体制。

当使用 IT 并且考虑到 IT 元素保护资产的能力时,CC 才适用。为了表明资产是安全的,安全考虑必须体现在所有层次的表述中,包括从最抽象到在其运行环境中的最终 IT 实现。这些表述层次,如下面章条所描述,可以用来表征和讨论安全问题,但这些层次本身并不表明最终的 IT 实现真实地具有所要求的安全行为,或是可信的。

CC 要求在某层次上的表述包含在该层次上 TOE 描述的原理,即该层次必须包含一个合理的、令人信服的论据,以表明它和更高层次一致,而且它是自我完备的、正确的并且内在一致的。陈述与邻近更高级别描述相一致的基本原理,将有助于 TOE 的正确性。直接表明与安全目的相一致的基本原理,在 TOE 对抗威胁和执行组织安全策略的有效性方面提供支持。

如图 5.5 所述 CC 将表述分成不同的层次,阐明了一种方法,通过它在开发一种 PP 或 ST 时,就能导出安全要求和规范。所有 TOE 安全要求从根本上均来源于对 TOE 的用途和环境的考虑。该图并不限制 PP 和 ST 的开发方法,而在于阐明一些分析方法的结果是怎么与 PP 和 ST 的内容相联系的。

5.3.1 安全环境

安全环境包括所有明确相关的法规、组织安全政策、习惯、专门技术和知识,因此它定义了 TOE 使用的背景和规则。安全环境也包括环境里固有的或外来的安全威胁。

为建立安全环境,PP 或 ST 的作者必须考虑以下几点:

a) TOE 物理环境,指所有与 TOE 安全相关的 TOE 运行环境,包括已知的物理和人员的安全配置。

b) 保护需要资产,指由执行安全要求、安全策略的 TOE 元素来保护的资产;这可包括可直接相关的资产,如文件和数据库,也包括间接受安全要求保护的资产,如授权凭证和 IT 实现本身。

c) TOE 用途,说明产品类型和可能的 TOE 用途。

安全策略、威胁和风险的调查将作出下列有关 TOE 安全的专门陈述:

a) 假设的陈述,如果环境满足该假设,TOE 可以被认为是安全的。对 TOE 评估而言,该陈述可以作为公理而接受。

b) 资产安全威胁的陈述,该陈述应指明 TOE 相关的安全分析中发现的所有威胁。CC 使用下述词汇表征一个威胁,即威胁主体、假定的攻击方法、作为攻击基础的任何脆弱性和被攻击的资产名称。安全风险的评价包括每一种威胁实际发生的可能性、该威胁成功实施的可能性以及可能造成的破坏后果。

c) 组织安全策略的陈述,该陈述将明确相关的策略和规则。对一个 IT 系统,可明确提及这样的策