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

# 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。

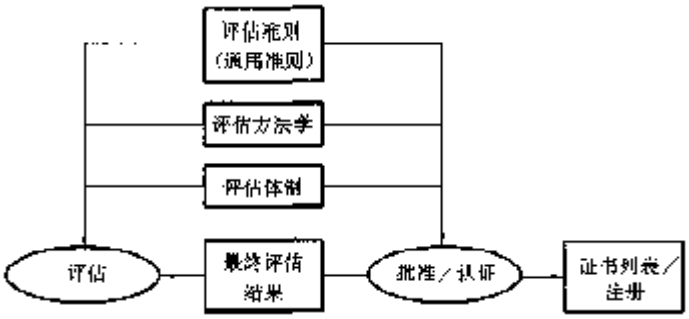


图 4.1 评估上下文

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。

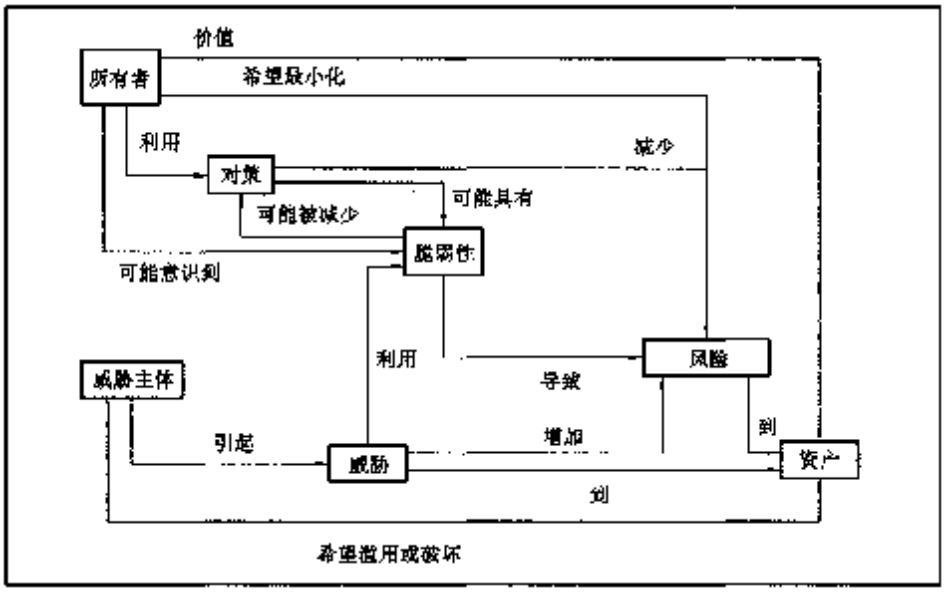


图5.1 安全概念和关系

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。

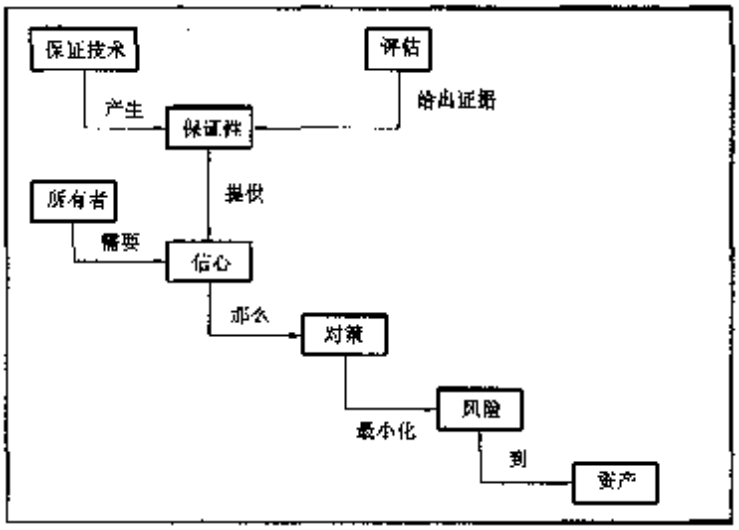


图 5.2　评估概念和关系

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。

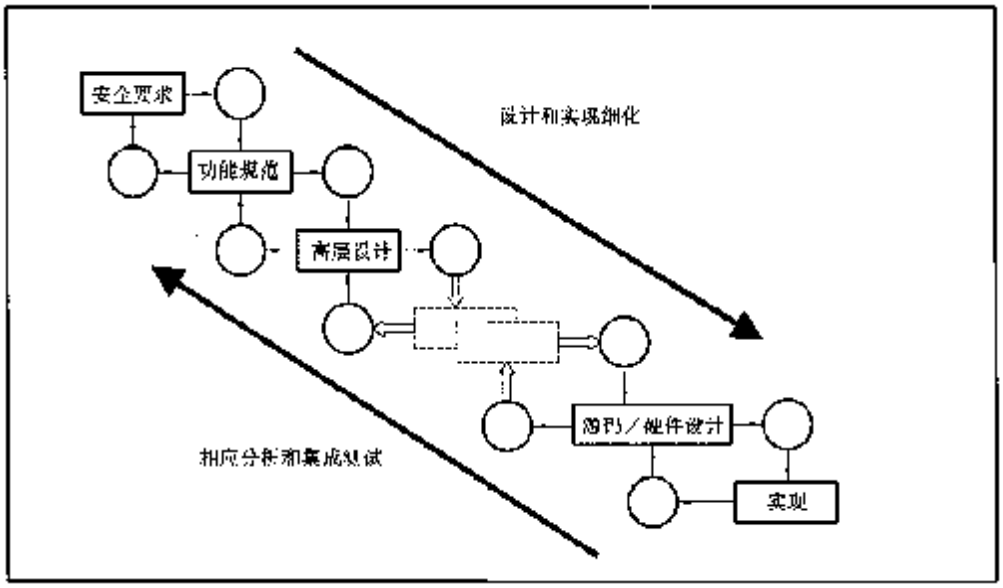


图 5.3 评估对象开发模型

### 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。

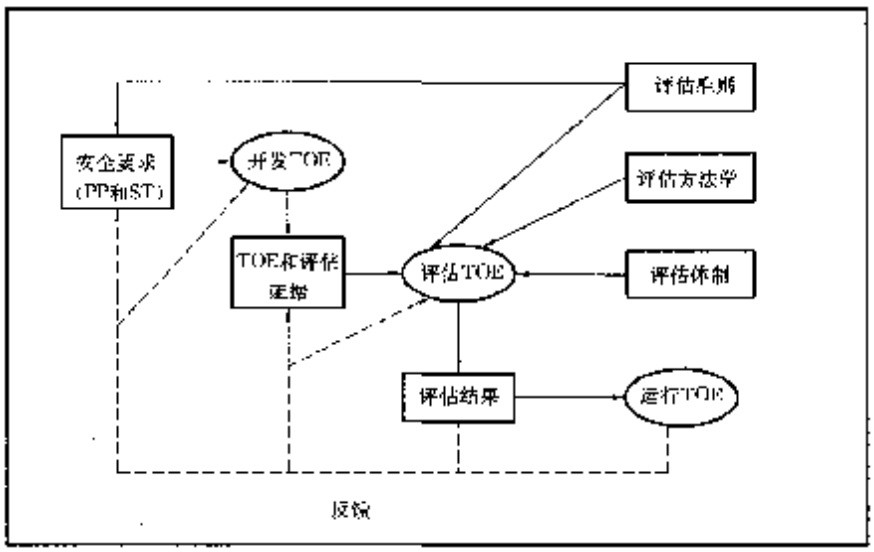


图 5.4 TOE 评估过程

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

略，然而对通用的IT产品或产品类，则需要做出关于组织安全策略的相应工作假设。

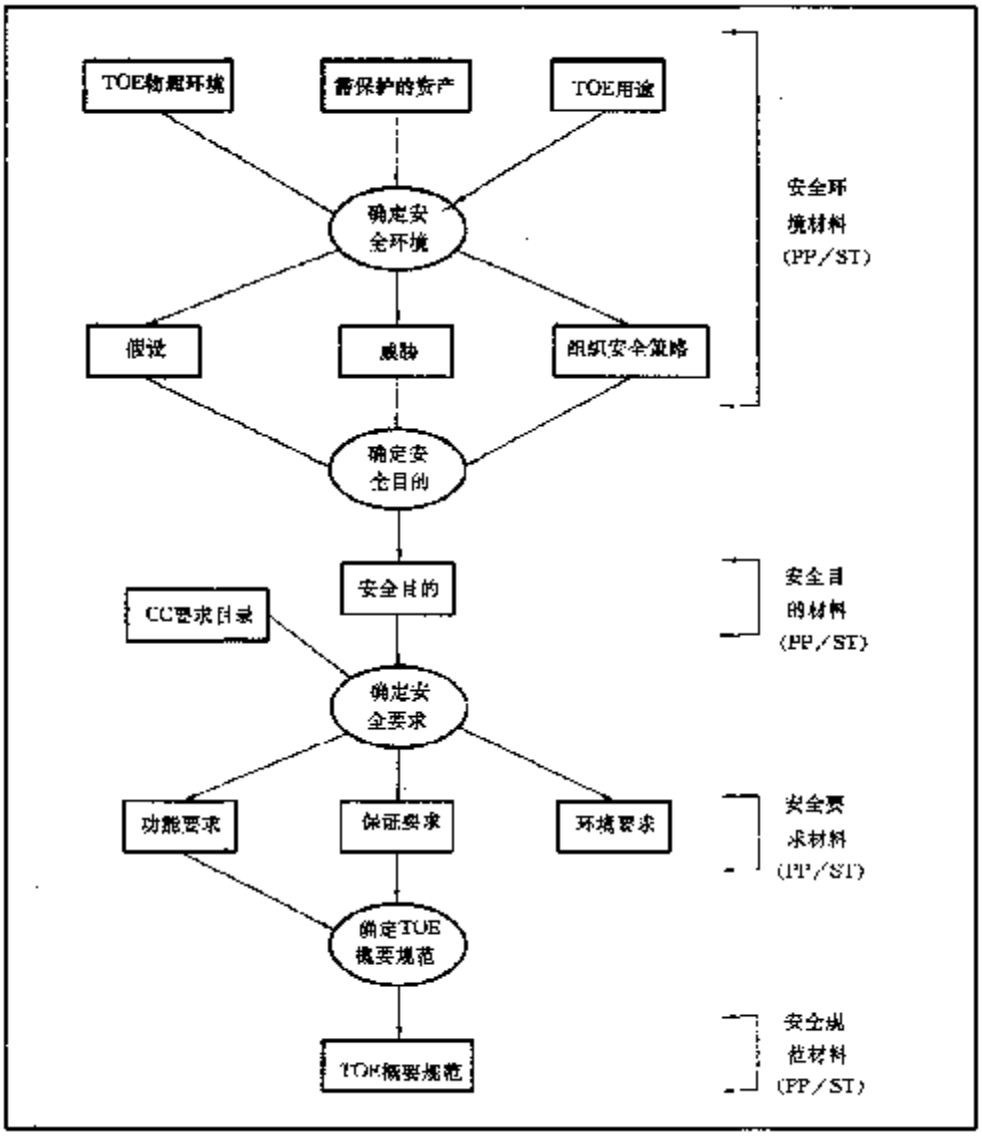


图5.5 要求和规范的导出

### 5.3.2 安全目的

安全环境的分析结果可用来陈述对抗确定的威胁并说明确定的组织安全策略和假设的安全目的。安全目的应与已说明的TOE运行目标或产品用途以及有关的所有物理环境知识相一致。

确定安全目的的意图是为了阐明所有的安全考虑并指出哪些方面是直接由TOE处理还是由它的环境来处理。这种归类的基础是以工程判断、安全策略、经济因素和可接受的风险决策相整合的过程。

环境安全目的应在IT领域内用非技术的或程序的方式来实现。

IT安全要求只针对TOE及其IT环境的安全目的。

### 5.3.3 IT安全要求

IT安全要求是将安全目的细化为一系列TOE及其环境的安全要求，一旦这些要求得到满足，就可以保证TOE达到它的安全目的。

CC在不同种类功能要求和保证要求下提出安全要求。

功能要求从用于支持IT安全的那些TOE功能中征集并定义期望的安全行为。GB/T 18336第2部分定义了CC的功能要求，例如标识、鉴别、安全审计以及原发抗抵赖功能。

当TOE包括由概率或排列机制(例如口令和散列函数)实现的安全功能时，保证要求应规定与宣

称的安全目的一致的最小强度等级，此时，等级可为基本级功能强度、中级功能强度、高级功能强度中的任一个。要求这样的功能满足最小的级别或至少是可选择定义的专门等级。

对给定的一组功能要求的保证程度可以改变，所以通常它以保证组件构建的严格程度递增的方式来表示。GB/T 18336 第3部分使用这些组件定义了CC的保证要求和一个评估保证级的尺度。保证要求包含了开发者行为，产生的证据以及评估者行为，例如：对开发过程的严格性约束，以及要求查找并分析潜在安全脆弱性的影响。

通过合理选择的安全功能可以确保达到一定的安全目的，这种保证来源于以下两个因素：

a) 对安全功能正确实现的信任，也就是评估它们是否被正确实现。

b) 对安全功能的有效性的信任，也就是评估它们是否确实满足所陈述的安全目的。

安全要求通常包括出现期望行为和避免不期望行为。通过使用或检验，一般可以证明存在的期望行为，但并不总是能明确证明不存在不期望行为。检验、设计评审、实现评审非常有助于减少存在不期望行为的风险，基本原理陈述有助于证明不存在不期望的行为。

### 5.3.4 TOE概要规范

在安全目标(ST)中提供的TOE概要规范定义了TOE安全要求的实例化。它提供满足功能要求的高层次安全功能定义，以及确保满足保证要求的措施。

### 5.3.5 TOE实现

TOE实现是基于TOE的安全功能要求和ST中TOE概要规范的实现。TOE实现是通过一个应用安全和IT工程的技巧和知识的过程来达到的。如果正确有效地实现了ST中包含的所有安全要求，TOE将达到其安全目的。

## 5.4 CC描述材料

CC提出了进行评估的框架。通过对证明和分析提出要求，可以得到更为客观、有用的评估结果。CC包括了一系列通用结构和一种能表达与IT安全相关方面交流的语言，并使得那些负责IT安全的人能从以前的经验和他人的专门技术中获益。

### 5.4.1 安全要求的表达

CC定义了一系列结构，这些结构将已知有效的安全要求构成有意义的组合体，这些组合体可用来为预期的产品和系统建立安全要求。表达安全要求的不同结构之间的关系将在下面描述，见图5.6。

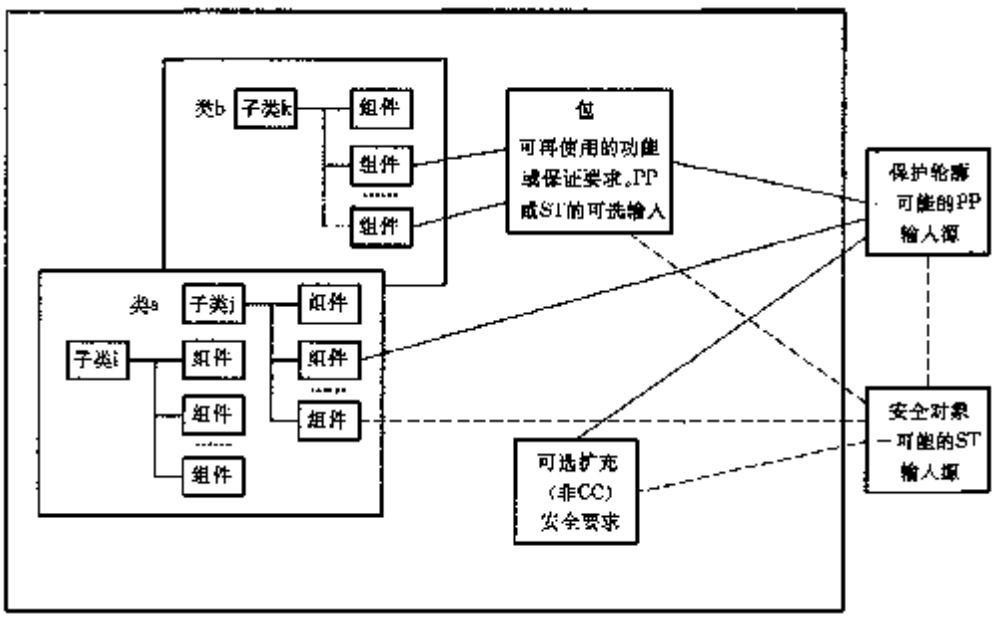


图5.6 要求的组织和结构

CC安全要求以类—子类—组件这种层次结构组织，以帮助用户定位特定的安全要求。

对功能和保证方面的要求，CC 使用相同的风格、组织方式和术语。

#### 5.4.1.1 类

类是安全要求的最高层次组合。一个类中所有成员关注同一个安全焦点，但覆盖的安全目的范围不同。

类的成员被称为子类。

#### 5.4.1.2 子类

子类是若干组安全要求的组合，这些要求共享同样的安全目的，但在侧重点和严格性上有所区别。

子类的成员被称为组件。

#### 5.4.1.3 组件

组件描述一个特定的安全要求集，它是 CC 结构中最小的可选安全要求集。子类内具有相同目的的组件，部分以安全要求强度或能力递增的顺序排列，部分以相关的非层次关系的方式组织。在某些实例中，一个子类只有一个组件，因而是不可能排序的。

组件由单个元素组成，元素是安全要求最低层次的表达，并且是能被评估验证的不可分割的安全要求。

**组件间的依赖**

组件间可能存在依赖关系。当一个组件无法充分表达安全要求并且依赖于另一个组件的存在时，就产生依赖关系。依赖关系可以存在于功能组件之间、保证组件之间、功能和保证组件之间。

组件间依赖关系描述是 CC 组件定义的一部分。为了保证达到 TOE 要求的完备性，当把组件加入到适当的 PP 和 ST 中时，应满足相应的依赖关系。

**组件允许的操作**

CC 组件可以像在 CC 中定义的那样使用，或者通过使用组件允许的操作，对组件进行裁剪，以满足特定的安全策略或对抗确定的威胁。每一个 CC 组件标识并定义了组件是否允许“赋值”和“选择”操作，在哪些情况下可对组件使用这些操作，以及使用这些操作的后果。任何一个组件均允许“反复”和“细化”操作。这四个操作如下所述：

a) 反复：在不同操作时，多次使用同一组件；

b) 赋值：在使用组件时，规定待填入的参数；

c) 选择：从组件项目表中选定若干项；

d) 细化：在使用组件时，增加额外的细节。

一些需要的操作可以在 PP 内完成(整体或部分地)，或者留在 ST 内完成，不过所有操作必须在 ST 内完成。

### 5.4.2 安全要求的使用

CC 定义了三种类型的要求结构：包、PP 和 ST。CC 还定义了一系列表达大多数团体需求的 IT 安全准则，作为主要的专业知识用于产生上述结构。开发 CC 的中心观念是尽可能使用 CC 中所定义的安全要求组件，这些组件都代表众所周知、易于理解的领域。图 5.7 表明了这些不同结构间的关系。

#### 5.4.2.1 包

包是组件的特定组合。包可以描述一组满足部分指定安全目的的功能和保证要求。包可重复使用，可用来定义那些公认有用的、对满足特定安全目的有效的要求。包可用于构造更大的包、PP 和 ST。

评估保证级(EAL)是在 GB/T 18336 第 3 部分中预先定义的保证包。一个保证级是评估保证要求的一个基线集合。每一评估保证级定义一套一致的保证要求，合起来，评估保证级构成一个预定义 CC 保证级尺度。

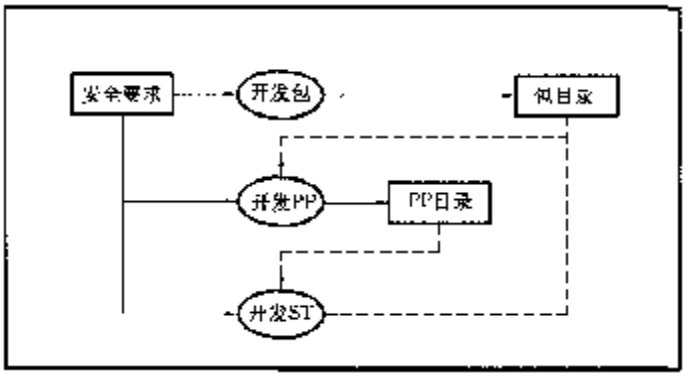


图 5.7　安全要求的应用

5.4.2.2　保护轮廓

保护轮廓(PP)包含一套或来自 CC 或明确阐述的安全要求，它应包括一个评估保证级(EAL)(可能增加附加的保证组件)。PP 可以对一组 TOE 的安全要求做与实现无关的描述，这些要求是同安全目的完全一致的。PP 可反复使用，还可用来定义那些公认有用的、对满足特定安全目的有效的 TOE(功能和保证)要求。PP 也包括安全目的和安全要求的基本原理。

PP 的开发者可以是用户团体、IT 产品开发者或其它对定义这样一系列通用要求有兴趣的团体。PP 为用户提供了一套引用一组特定安全要求的方法，并有助于将来对这些要求进行评估。

5.4.2.3　安全目标

安全目标(ST)包括一系列安全要求，这些要求可以引用 PP，可以直接引用 CC 中的功能或保证组件，也可以明确阐述。ST 可以对特定 TOE 的安全要求进行描述，通过评估可以证明这些要求对满足指定目的是有用当然和有效的。

ST 包括 TOE 的概要规范，同时还包括安全要求和目的，以及它们的基本原理。ST 是所有团体对 TOE 提供什么样的安全性达成一致的基础。

5.4.3　安全要求的来源

TOE 安全要求可以通过使用下列输入来构造：

a) 已有的 PP

PP 的安全要求可用来充分地表达或完全满足 ST 中的 TOE 安全要求。

已有的 PP 可以作为一个新 PP 的基础。

b) 已有的包

PP 或 ST 中部分 TOE 安全要求可能已在一个被使用的包中表述过了。

GB/T 18336 第 3 部分定义的 EAL 是一组预定义的包。PP 或 ST 的 TOE 保证要求应包括第 3 部分的某个 EAL。

c) 已有的功能或保证要求组件

PP 或 ST 中的 TOE 功能或保证要求可以用 GB/T 18336 第 2 部分或第 3 部分的组件直接表达。

d) 扩展的要求

GB/T 18336 第 2 部分没有的功能要求或第 3 部分没有的保证要求可以包括在 PP 或 ST 中。

应尽可能使用 GB/T 18336 第 2 部分或第 3 部分已有的安全要求。使用已存在的 PP 有助于保证 TOE 满足一组公认的已知用途的要求，进而有利于 TOE 被广泛认可。

5.5　评估类型

5.5.1　PP 评估

PP 评估是依照 GB/T 18336 第 3 部分的 PP 评估准则进行的，其目标是为了证明 PP 是完备的、一致的、技术合理的，并适合于表达一个可评估的 TOE 要求。

### 5.5.2 ST 评估

针对 TOE 的 ST 评估是依照 GB/T 18336 第 3 部分的 ST 评估准则进行的。ST 评估具有双重目标：首先是为了证明 ST 是完备的、一致的、技术合理的，因而适合于作为相应 TOE 评估的基础。其次，当某一 ST 宣称与某一 PP 一致时，证明 ST 正确满足 PP 的要求。

### 5.5.3 TOE 评估

TOE 评估是使用一个已经评估过的 ST 作为基础，是依照 GB/T 18336 第 3 部分的评估准则进行的。这样的评估目标是为了证明 TOE 满足 ST 中的安全要求。

## 5.6 保证的维护

依照 GB/T 18336 第 3 部分提到的评估准则，以一个已评估的 TOE 为基础，进行 TOE 保证的维护。其目的是确保 TOE 中已建立的保证得到维持，并当 TOE 或其环境发生变化时，TOE 将继续满足它的安全要求。

# 6 通用准则要求和评估结果

## 6.1 引言

本章给出 PP 和 TOE 评估的预期结果。PP 或者 TOE 评估将分别产生评估过的 PP 或 TOE 目录。ST 评估将产生在 TOE 评估框架中使用的中间结果。见图 6.1。

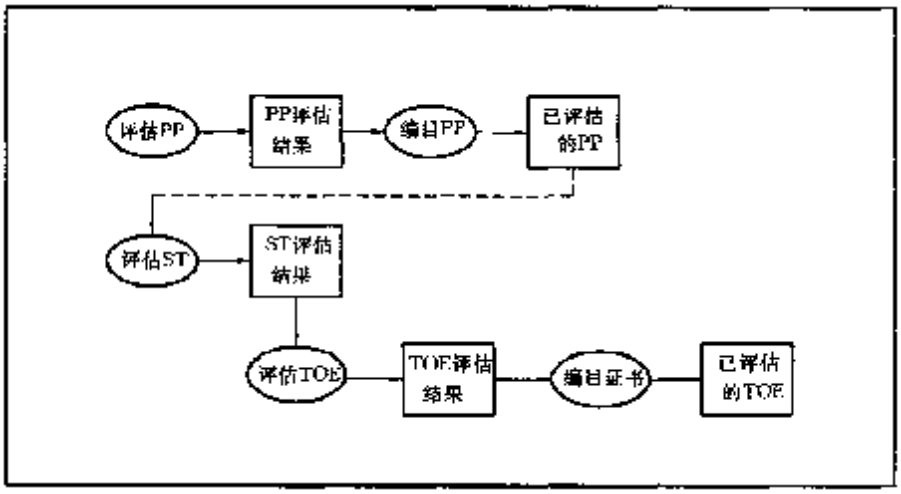


图 6.1 评估结果

评估过程应能产生出能引为证据的客观的和可重复的结果，甚至当没有绝对客观的尺度描述 IT 安全评估结果时也应如此。存在一套评估标准是评估的必须前提，这样的评估才可以得到有意义的结果，并且也提供了评估机构之间的对评估结果互认的基础。但标准的应用中包含了主观的和客观的因素，这也是对 IT 安全不可能进行精确的和通用评定的原因。

与 CC 有关的评定代表了对 TOE 的安全特性进行专门考察时的裁决，这种评定并不保证在任何特殊的应用环境下 TOE 的适用性。在特定应用环境下，使用一个 TOE 的决策应基于对多个安全因素的考虑，包括评估裁决。

## 6.2 PP(保护轮廓)和 ST(安全目标)的要求

CC 定义了一套能满足许多团体需求的 IT 安全准则。CC 是围绕这样一个中心观点开发的，即在 PP 和 ST 中描述 TOE 的安全要求时，尽可能使用 GB/T 18336 第 2 部分的安全功能组件和第 3 部分的 EAL 及保证组件，因为它们是公认的和已被理解的。

CC 也意识到可能需要未列出的功能和保证要求，以完整表达对 IT 安全的要求。以下内容适用于包容这些扩展的功能和保证要求：

a) PP 和 ST 中包容的任何扩展的功能或保证要求必须清晰和明确地表达，以便评估和证实。可以

参照已有的CC功能和安全组件描述的详细程度和方式；

b）应声明评估结果是通过使用扩展功能或保证要求得到的；

c）组合在PP或ST中的扩展功能或保证要求应满足GB/T 18336第3部分中APE或ASE类的要求。

#### 6.2.1 PP评估结果

CC包括有评估准则，以便评估者说明一个PP是否完备、一致、技术上正确，因而适用于对可评估的TOE要求进行描述。

PP的评估结果为通过/不通过。通过评估的PP才能登记注册。

### 6.3 TOE内的要求

CC包含评估准则，以便评估者判定TOE是否满足了ST中描述的安全要求。在TOE的评估中利用CC，评估者能够说明：

a）TOE的指定安全功能是否满足功能要求，进而有效地达到TOE的安全目的；

b）TOE的指定安全功能是否正确地实现。

CC的安全要求定义了公认的IT安全评估标准适用的工作领域。一个TOE的安全要求如果只使用CC中的功能和保证要求进行描述，该TOE可以按照CC进行评估，使用没有包含EAL的保证包时必须说明其理由。

不过，也存在这样的可能，无法直接使用CC描述TOE安全要求。CC意识到了评估这样TOE的必要性，但是，附加要求属于CC的公认的适用领域之外，因此，这种评估的结果应作相应声明。这种声明会使评估结果不为相关评估机构广泛接受。

TOE的评估结果应包括与CC一致性的陈述。运用CC的术语描述TOE的安全，将使TOE间在安全特性上进行一般意义的比较成为可能。

#### 6.3.1 TOE评估结果

TOE评估结果应说明对TOE满足指定要求的可信程度。

TOE的评估结果为“通过”或“不通过”。通过评估的TOE才能登记注册。

### 6.4 评估结果的声明

评估的“通过”结果应说明对PP或TOE满足指定要求的可信程度。

评估结果应分别针对GB/T 18336第2部分(功能要求)、第3部分(保证要求)或直接针对PP按下列进行说明：

a）第2部分一致——当功能要求只建立在第2部分的功能组件上，PP或TOE是第2部分一致的。

b）第2部分扩展——如果功能要求包含有第2部分中没有的功能组件，PP或TOE是第2部分扩展的。

c）第3部分一致——如果保证要求是以EAL或保证包形式存在的，而该EAL或保证包只基于第3部分中的保证组件，PP或TOE是第3部分一致的。

d）第3部分增强——如果安全要求是以EAL或保证包形式存在的，并加上第3部分中其他保证组件，PP或TOE是第3部分增强的。

e）第3部分扩展——如果安全要求是以EAL形式存在的，而EAL又是与第3部分之外的附加的保证要求相联系的，或以保证包形式存在的，该包有(或完全是)第3部分之外的保证要求，PP或TOE是第3部分扩展的。

f）PP一致——只有当TOE与PP的所有部分一致时，它才是PP一致的。

### 6.5 TOE评估结果的应用

对评估结果的使用而言，IT产品和系统是不同的。图6.2表明处理评估结果的选择方式。产品可以被评估，并按聚集程度连续递增排列编目，直至达到可操作的系统水平，此时它们就可以进行与系统认

可相关的评估。

TOE 的开发需要相应考虑到所吸收的已评估产品和所引用 PP 的安全属性，随后的 TOE 评估会产生一系列的评估结果，这些结果记录了评估的裁决。

对有广泛用途的 IT 产品评估后，应将评估结果的概要列入已评估产品的目录，以使它在广阔的安全 IT 产品市场中可用。

当 TOE 已包含或将包含在一个面对评估并且已安装妥当的 IT 系统中，它的评估结果对系统认可者是可用的。当认可者使用组织专用的认可准则，而认可准则要求进行 CC 评估时，应考虑 CC 的评估结果。CC 评估结果是系统认可过程的输入之一，以作出是否接受系统运行风险的决策。

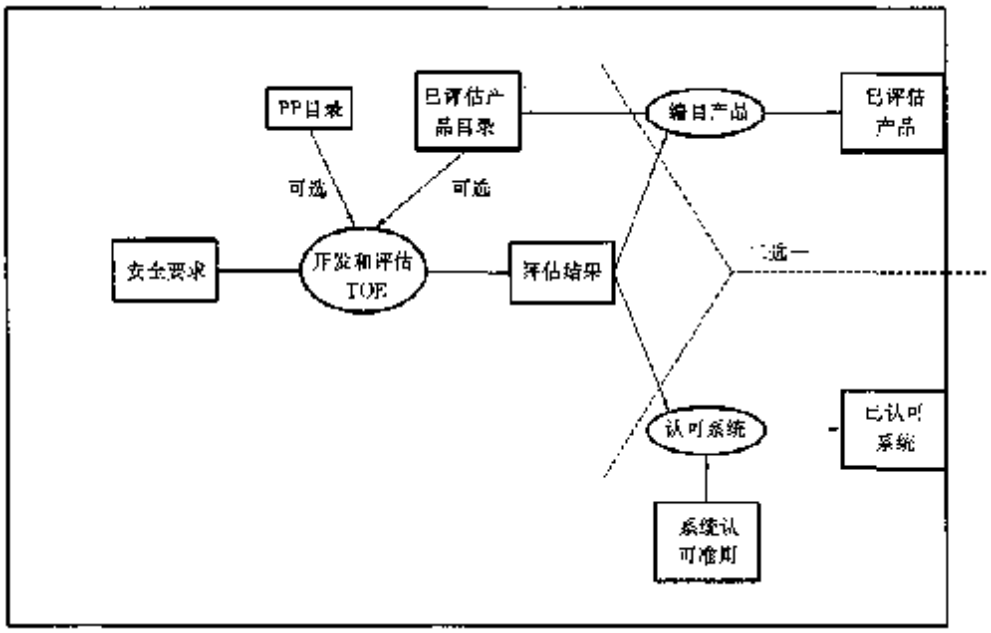


图 6.2　TOE 评估结果的应用

# 附 录 A
(提示的附录)
## 通用准则项目

### A1 通用准则项目的背景

CC 是一系列对评估准则开发的努力的结果,这些准则用于评估在国际团体内应用广泛的 IT 安全性。在 80 年代早期,美国开发了可信计算机系统评估准则(TCSEC)。在随后的十年里,不同的国家都开始启动开发建立在 TCSEC 概念上的评估准则,这些准则更灵活、更适应了 IT 技术的发展。

在欧洲,信息技术安全评估准则(ITSEC)1.2 版于 1991 年由欧洲委员会在法国、德国、荷兰和英国的联合开发后公开发表。在加拿大,加拿大可信计算机产品评估准则(CTCPEC)3.0 版作为 ITSEC 和 TCSEC 的结合于 1993 年公开发表。在美国,信息技术安全联邦标准(FC)草案 1.0 版也在 1993 年公开发表,它是结合北美和欧洲有关评估准则概念的另一种方法。

国际标准化组织(ISO)从 1990 年开始开发通用的国际标准评估准则。新的标准是对全球 IT 市场上,对互认标准化安全评估结果的需求作出的反应,该任务赋予给第一联合技术委员会(JTC1)的第 27 分委员会(SC27)的第 3 工作小组(WG3)。最初,由于大量的工作和多方协商的强烈需要,WG3 的进展缓慢。

### A2 通用准则的开发

在 1993 年 6 月,CTCPEC、FC、TCSEC 和 ITSEC 的发起组织(在下一条中说明)集中了他们的力量,并开始了联合行动将各自独立的准则集合成一组单一的、能被广泛使用的 IT 安全准则,这一行动被称为 CC 项目。它的目的是解决原标准中出现的概念和技术上的差异,并把结果作为对国际标准的贡献提交给了 ISO。发起组织的代表建立了 CC 编辑委员会(CCEB)来开发 CC。随后,CCEB 和 WG3 建立了联系,通过联系渠道 CCEB 向 WG3 提供了几个 CC 的早期版本。作为 WG3 和 CCEB 交流的结果,从 1994 年开始,这些版本被采纳为 ISO 准则若干部分继续工作的草案。

CCEB 1996 年 1 月完成 CC1.0 版,在 1996 年 4 月被 ISO 采纳,作为委员会草案而散发。而后,CC 项目使用 CC1.0 版完成了大量的试验性评估,并收集了对文档的广泛公众评论。随后,基于从试用中得到的意见、公众评论和与 ISO 的相互交流,CC 项目对 CC 承担了广泛的修订工作。修订工作由 CCEB 的接任者,现在称为 CC 执行委员会(CCIB)完成的。

CCIB 于 1997 年 10 月完成了 CC2.0 的测试版,并把它提送给 WG3,WG3 把它改进后作为第 2 委员会草案。其后若干中间的草案版本被非正式地提供给 WG3 的专家,作为 CCIB 对草案的反馈。CCIB 接收了一系列直接来自 WG3 专家和经 CD 投票来自 ISO 国家机构的意见,并对此作出了反应。这个过程最终产生了 CC2.0 版。

为了历史的和连续性的目的,ISO/IEC JTC1/SC27/WG3 已经同意在文档中继续使用“通用准则(CC)”这一术语,虽然认为在 ISO 行文中的正式名称应为“信息技术安全性评估准则”。

### A3 通用准则项目发起组织

下面列出的七个欧洲和北美的官方组织组成了 CC 项目发起组织。在从事 CC 从开始到完成的开发过程中,这些组织几乎提供了所有的成果。这些组织也是他们各自国家政府的“评估机构”。CC2.0 版的技术开发已经完成,上述组织已经承诺将用 CC2.0 版代替他们各自的评估准则。

加拿大：
通信安全组织
准则协调者
12A 计算机和网络安全
加拿大渥太华 KIG 3Z4 9703 终端汇票箱
电话：+1.613.991.7882，传真：+1.613.991.7445
电子邮件：citeria@cse-cst.gc.ca
WWW：http://www.cse-cst.gc.ca/cse/english/cc.html
FTP：ftp://ftp.cse-cst.gc.ca/pub/criteria/CC2.0

法国：
信息安全系统服务中心(SCSS1)
电话：+33.1.41463784，传真：+33.1.41463701
电子邮件：ssi20@calva.net

德国：
德国信息安全局(GISA)
Abteilung V
Postfach 20 03 63
D-53133 Bonn
Getmany
电话：+49.228.9582.300，传真：+49.228.9582.427
电子邮件：cc@bsi.de
WWW：http://www.bsi.bund.de

荷兰：
荷兰国家通信安全局
P.O.Box 20061
NL 2500 EB The Hague
The Nethetlands
电话：+31.70.3485637，传真：+31.70.3486503
电子邮件：criteria@nlncsa.minbuza.nl
WWW：http://tno.nl/instit/fel/refs/cc.html

英国：
通信—电子安全团体
P.O.Box 144
Cheltenham GL52 5UE
United Kingdom
电话：+44.1242.221.491 ext.5257，传真：+44.1242.252.291
电子邮件：criteria@cesg.gov.uk
WWW：http://www.cesg.gov.uk/cc.html

FTP：ftp://ftp.cesg.gov.uk/pub

美国：
国家标准和技术研究院
计算机安全局
820 Diamond，MS：nn426
Gaithersburg，Mauyland 20899
U.S.A
电话：+1.301.975.2934，传真：+1.301.948.0279
电子邮件：criteria@nist.gov
WWW：http://csrc.nist/cc

美国：
国家安全局
Attn：V2，Common Criteria Technical Advisor
Fort George G. Maryland 20755-6740
U.S.A
电话：+1.410.859.4458，传真：+1.410.684.7512
电子邮件：common _ criteria@radium.nscs.mil
WWW：http://www.radium.ncsc.mil/tpep/

# 附 录 B
（标准的附录）
# 保护轮廓规范

## B1 综述

一个 PP 为一类 TOE 定义了一组与实现无关的 IT 安全要求。这种 TOE 是用来满足一般用户对 IT 安全的需求，因而用户可以不必参考特定的 TOE 就能建立或引用 PP 来表示他们对 IT 安全的需求。

本附录包括在描述形式上对 PP 的要求。GB/T 18336 第 3 部分第 5 章包括的保证类 APE，以保证组件的形式包含了这些要求，用于 PP 的评估。

## B2 保护轮廓的内容

### B2.1 内容与形式

PP 应满足本附录对内容的要求。PP 将以面向用户文档的形式给出，它应尽量少地引用用户无易得到的材料。必要时，应单独提供基本原理。

图 B1 中描述了 PP 的内容，应按其建立 PP 文档大纲。

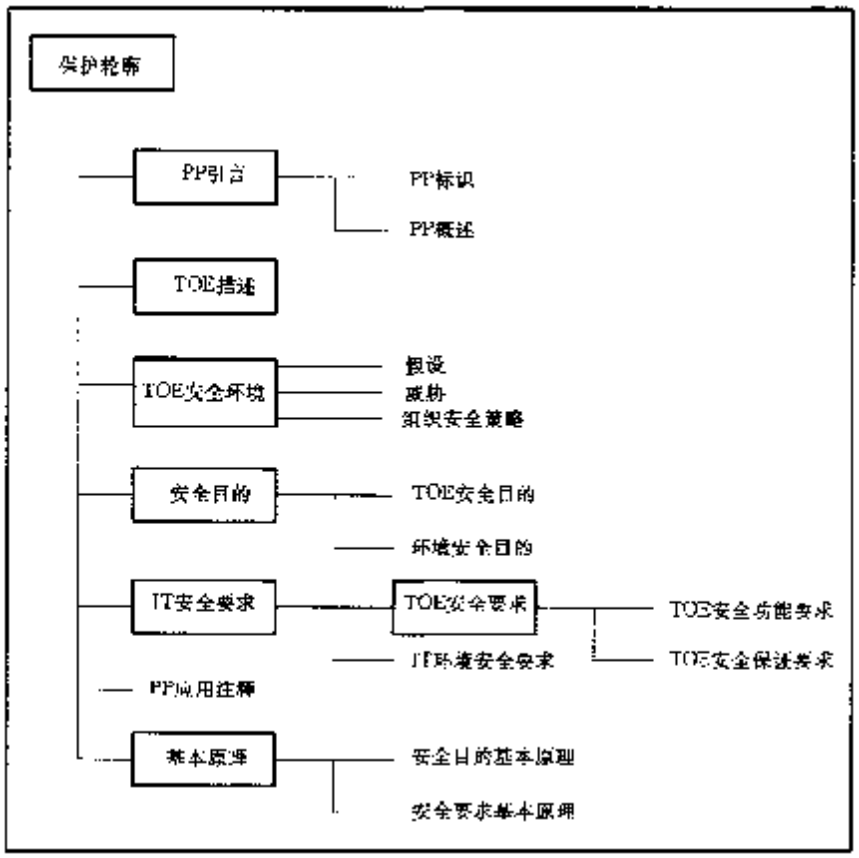


图 B1 保护轮廓内容

### B2.2 PP 引言

PP 引言将包括文档管理和进行 PP 注册所必要的信息，如下所述：

a）PP 标识，应提供 PP 的标记和描述的必要信息，供标识、编目、注册和交叉引用。

b) **PP 概述**,以叙述形式概述 PP。概述应足够详细,使一个潜在 PP 用户可以据此确定 PP 是否有价值。概述作为一个独立摘要也可用于 PP 编目和注册。

### B2.3 TOE 描述

PP 的这部分应描述 TOE,以帮助了解它的安全要求,同时还应说明 TOE 的产品类型和一般的 IT 特性。

TOE 描述提供了用于评估的上下文。在 TOE 描述中给出的信息将用于在评估过程中识别不一致性的地方。由于 PP 一般并不指明特定的实现,描述的 TOE 特性可能是假设的。如果 TOE 是一个以安全功能为主要功能的产品或系统,则 PP 的本部分可以用来描述 TOE 更广泛的应用环境。

### B2.4 TOE 安全环境

**TOE 安全环境**的陈述应描述 TOE 所处的应用环境和 TOE 期望的使用方式中的安全问题。该陈述应包括如下几点:

a) **假设**的描述应描述环境的安全问题,TOE 将在或拟在这个环境里使用。这包括下述几点:

关于 TOE 预期使用方式的信息,包括:预期的应用、潜在的资产价值、可能的使用限制;

关于 TOE 使用环境的信息,包括物理的、人员的和连通性等方面。

b) **威胁**的描述应包括对资产的所有威胁,这些资产是在 TOE 中或在其环境内需要特定保护的。值得注意的是:不是所有在环境里遭遇的可能威胁都必须列出,只有那些与 TOE 的安全运行相关的威胁才需要列出。

威胁应通过已确定的威胁主体、攻击和作为攻击对象的资产来描述。威胁主体应通过诸如专门技术、可用资源和动机等来描述。攻击应通过诸如攻击方法、可利用的脆弱性和时机等来描述。

如果安全目的仅仅源于组织安全策略和假设,那么对威胁的描述可以省略。

c) **组织安全策略**的描述应确定 TOE 必须遵守的所有组织安全策略陈述或规则,必要时还应加以说明。如果使用某个策略来建立清晰的安全目的,就必需对策略陈述进行说明和解释。

如果安全目的仅仅源于威胁和假设,那么对组织安全策略的描述可以省略。

如果 TOE 在物理上是分开的,可能有必要在 TOE 安全环境方面(假设、威胁、组织安全策略)分别地对不同区域进行讨论。

### B2.5 安全目的

**安全目的**的陈述定义 TOE 及其环境的安全目的。安全目的应涉及已确定安全环境的所有方面。安全目的应反映所陈述的意图,并应适于对抗所有已知的威胁,覆盖所有已知的组织安全策略和假设。应指明以下两类安全目的。(注意:当威胁或组织安全策略部分被 TOE 所覆盖并部分被它的环境所覆盖,那么相关的目的将在每个种类中重复。)

a) 应明确说明 **TOE 安全目的**,并且可追溯到 TOE 所对抗的已知威胁或 TOE 可满足的组织安全策略。

b) 应明确说明**环境安全目的**,并且可追溯到已知的 TOE 无法完全对抗的威胁或 TOE 无法完全满足的组织安全政策及假设。

注意环境的安全目的可能是 TOE 安全环境陈述的假设部分全部或部分的重述。

### B2.6 IT 安全要求

这部分定义 TOE 或其环境应满足的详细的 IT 安全要求。IT 安全要求应按下列方式描述:

a) **TOE 安全要求**的陈述应定义功能和保证安全要求,TOE 和为评估所提供的证据应满足这些要求,以便达到 TOE 的安全目的。TOE 安全要求包括如下内容:

1) **TOE 安全功能要求**的陈述应把 TOE 功能要求定义为从 GB/T 18336 第 2 部分中提取的适当功能组件。

当必须覆盖同一要求的不同方面时(例如:标识多类用户),可以重复使用(例如使用“反复”操作)第 2 部分的组件来覆盖每一个方面。

当AVA_SOF.1包括在TOE安全保证要求(如EAL2和更高的)中时,TOE安全功能要求应说明由概率或排列机制(如:口令或散列函数)实现的TOE安全功能最低的强度级别。所有这样的功能应达到最低级别,最低级别可以是基本级功能强度、中级功能强度、高级功能强度之一。级别的选择应与TOE安全目的一致。也可根据情况,为选定的功能要求定义功能强度的尺度,以满足TOE的某些安全目的。

作为TOE安全功能强度评估的一部分(AVA_SOF.1),应评定单个TOE安全功能所宣称的强度以及整体的最小强度级别是否被TOE满足。

2) TOE安全保证要求的陈述应使用GB/T 18336第3部分的一个EAL或其保证组件增强来表达,同时PP也允许通过明确说明增加的保证要求来扩展EAL,这些要求可以不取自第3部分。

b) IT环境安全要求的陈述是可选的,该陈述应确定TOE的IT环境应满足的IT安全要求。如果TOE没有声称依赖IT环境,可以忽略PP的这部分。

要注意的是非IT环境的安全要求,尽管在实际中常常是有用的,但因它们与TOE实现没有直接关系,不要求它们成为PP的正式部分。

c) 下列通用条件应同样适用于TOE及其IT环境的安全功能和保证要求的表达:

1) 所有IT安全要求都应引用GB/T 18336第2部分或第3部分适用的安全要求组件来表达。对所有或部分安全要求而言,如果第2部分或第3部分的安全组件都无法使用时,PP可以明确说明这些安全要求不引自CC。

2) 所有TOE安全功能和保证要求均应准确、无歧义地表达,才能进行一致性评估和论证。现有的通用准则功能或保证要求的详细程度和表达方式应当作一个典范来使用。

3) 当选择了规定的需要操作(赋值或选择)的安全组件时,PP应使用这些操作将要求细化到必要的程度,以便论证安全目的都已满足。任何要求的但又不在PP内执行的操作同样应说明。

4) 通过使用要求组件的操作,TOE安全要求可根据情况在必要时规定或禁止特定安全机制的使用。

5) 所有IT安全要求之间的依赖关系都应满足。依赖关系可以通过在TOE安全要求内包含相关的要求或对环境提出要求来满足。

### B2.7 应用注解

这个可选的部分可能包括额外的支持信息,该信息对构造、评估或使用TOE是相关或有用的。

### B2.8 基本原理

这部分提出用于PP评估的依据。这些依据将支持:PP是一个完整的、紧密结合的要求集合,满足该PP的TOE应在安全环境内提供一组有效的IT安全对策。基本原理应包括以下几点:

a) 安全目的基本原理应阐明安全目的可追溯到在TOE安全环境里指明的所有方面,并且能覆盖所有的这些方面。

b) 安全要求基本原理应阐明系列安全要求(TOE及其环境)是适合于满足,并可追溯到安全目的。应阐明以下几点:

1) 将TOE及其IT安全环境的功能和保证要求组件相结合,能满足所述的安全目的;

2) 该组安全要求一起构成一个互相支持且内在一致的整体;

3) 安全要求的选择应说明理由,所有下列情况都应当专门说明:

——选择GB/T 18336第2部分或第3部分中没有的要求;

——选择不包括在EAL中的保证要求;

——不满足依赖关系;

4) 已选择的PP功能强度级别和任何一个明确宣称的功能强度,是符合TOE安全目的的。

这部分材料可能篇幅太大,不一定对所有PP用户都适合和有用,因此可以单独发行。

# 附 录 C
（标准的附录）
# 安全目标规范

## C1 综述

一个ST 包括确定的TOE 的IT 安全要求以及TOE 提供的规定安全功能和保证措施，以满足所述的安全要求。

对一个TOE 而言，ST 是开发者、评估者、用户在TOE 安全特性和评估范围之间达成一致的基础。一个ST 读者不限于对TOE 制造和评估负有责任，但也可能负有管理、营销、购买、安装、配置、操作和使用TOE 的责任。

ST 可能包含或宣称符合一个或多个PP 的要求。最初在C2 条中定义ST 中要求的内容时，并未考虑到PP 的这类一致性声明的影响。C2.8 中提出了PP 一致性声明对ST 所需内容的影响。

本附录以描述的方式说明了ST 的各种要求，GB/T 18336 第3 部分第6 章的保证类ASE 以保证组件的方式描述了同样的要求，以用于对ST 的评估。

## C2 安全目标的内容

### C2.1 内容与形式

ST 应满足本附录的内容要求。ST 应是一个面向用户使用的文档，应尽可能少地引用用户不易得到的其他材料。必要时，应单独提供基本原理。

图C1 中描述了ST 的内容，应按其建立ST 文档大纲。

### C2.2 ST 引言

ST 引言应包括以下的文档管理和概述信息：

a）ST 标识，应提供必要的标记和描述信息，以控制和标识ST 和它所指的TOE。

b）ST 概述，以叙述形式概述ST。概述应有足够的细节提供给TOE 的潜在用户，以便他们决定对该TOE 是否有兴趣。概述也可作为一个单独的摘要，包含在已评估产品一览表中。

c）CC 一致性声明，应说明TOE 与CC 任何可评估的一致性声明，就像在GB/T 18336 第1 部分6.4条中指明的一样。

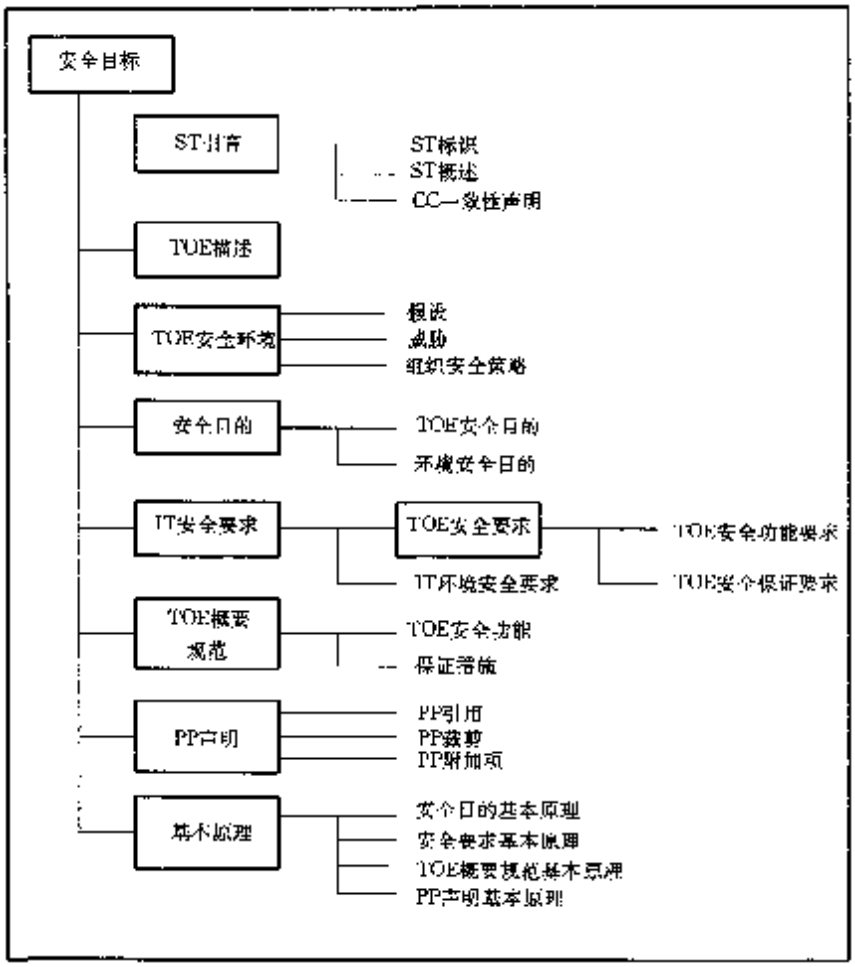


图 C1　安全目标内容

### C2.3　TOE 描述

ST 的这一部分应描述TOE，以帮助理解它的安全要求，并说明产品或系统的类型。TOE 的范围和边界用通用术语同时以物理方式(硬件/软件组件或模块)和逻辑方式(由 TOE 提供的 IT 和安全特征)描述。

TOE 描述提供了评估上下文。在 TOE 描述中给出的信息将用于在评估过程中识别出不一致的地方。如果 TOE 是一个以安全功能为主要功能的产品或系统，则 ST 的本部分可以用来描述 TOE 更广泛的应用环境。

### C2.4　TOE 安全环境

TOE 安全环境的陈述应描述 TOE 所处的应用环境和 TOE 期望的使用方式中的安全问题。该陈述包括以下几点：

a) 假设的描述应描述环境的安全问题，TOE 将在或拟在这个环境里使用。这包括下述几点：

关于 TOE 预期使用方式的信息，包括：预期的应用、潜在的资产价值、可能的使用限制；

关于 TOE 使用环境的信息，包括物理的、人员的和连通性等方面。

b) 威胁的描述应包括对资产的所有威胁，这些资产是在 TOE 中或在其环境内需要特定保护的。值得注意的是：不是所有在环境里遭遇的可能威胁都必须列出，只有那些与 TOE 的安全运行相关的威胁才需要列出。

威胁应通过已确定的威胁主体、攻击和作为攻击对象的资产来描述。威胁主体应通过诸如专门技术、可用资源和动机等来描述。攻击应通过诸如攻击方法、可利用的脆弱性和时机等来描述。

如果安全目的仅仅源于组织安全策略和假设，那么对威胁的描述可以省略。

c）**组织安全策略**的描述应确定 TOE 必须遵守的所有组织安全策略陈述或规则，必要时还应加以说明。如果使用某个策略来建立清晰的安全目的，就必需对策略陈述进行说明和解释。

如果安全目的仅仅源于威胁和假设，那么对组织安全策略的描述可以省略。

如果 TOE 在物理上是分开的，可能有必要在 TOE 安全环境方面（假设、威胁、组织安全策略）分别地对不同区域进行讨论。

### C2.5 安全目的

**安全目的**的陈述定义 TOE 及其环境的安全目的。安全目的应涉及已确定安全环境的所有方面。安全目的应反映所陈述的意图，并应适于对抗所有已知的威胁，覆盖所有已知的组织安全策略和假设。应指明以下两类安全目的。（注意：当威胁或组织安全策略部分被 TOE 所覆盖并部分被它的环境所覆盖，那么相关的目的将在每个种类中重复。）

a）应明确说明 **TOE 安全目的**，并且可追溯到 TOE 所对抗的已知威胁或 TOE 可满足的组织安全策略。

b）应明确说明**环境安全目的**，并且可追溯到已知的 TOE 无法完全对抗的威胁或 TOE 无法完全满足的组织安全政策及假设。

注意环境的安全目的可能是 TOE 安全环境陈述的假设部分全部或部分的重述。

### C2.6 IT 安全要求

这部分定义 TOE 或其环境应满足的详细的 IT 安全要求。IT 安全要求应按下列方式描述：

a）**TOE 安全要求**的陈述应定义功能和保证安全要求，TOE 和为评估所提供的证据应满足这些要求，以便达到 TOE 的安全目的。TOE 安全要求包括如下内容：

1）**TOE 安全功能要求**的陈述应把 TOE 功能要求定义为从 GB/T 18336 第 2 部分中提取的适当功能组件。

当必须覆盖同一要求的不同方面时（例如：标识多类用户），可以重复使用（例如使用“反复”操作）第 2 部分的组件来覆盖每一个方面。

当 AVA_SOF.1 包括在 TOE 安全保证要求（如 EAL2 和更高的）中时，TOE 安全功能要求应说明由概率或排列机制（如：口令或散列函数）实现的 TOE 安全功能最低的强度级别。所有这样的功能应达到最低级别，最低级别可以是基本级功能强度、中级功能强度、高级功能强度之一。级别的选择应与 TOE 安全目的一致。也可根据情况，为选定的功能要求定义功能强度的尺度，以满足 TOE 的某些安全目的。

作为 TOE 安全功能强度评估的一部分（AVA_SOF.1），应评定单个 TOE 安全功能所宣称的强度以及整体的最小强度级别是否被 TOE 满足。

2）**TOE 安全保证要求**的陈述应使用 GB/T 18336 第 3 部分的一个 EAL 或其保证组件增强来表达，同时 PP 也允许通过明确说明增加的保证要求来扩展 EAL，这些要求可以不取自第 3 部分。

b）**IT 环境安全要求**的陈述是可选的，该陈述应确定 TOE 的 IT 环境应满足的 IT 安全要求。如果 TOE 没有声称依赖 IT 环境，可以忽略 PP 的这部分。

要注意的是非 **IT 环境的安全要求**，尽管在实际中常常是有用的，但因它们与 TOE 实现没有直接关系，不要求它们成为 PP 的正式部分。

c）下列**通用条件**应同样适用于 TOE 及其 IT 环境的安全功能和保证要求的表达：

1）所有 IT 安全要求都应引用 GB/T 18336 第 2 部分或第 3 部分适用的安全要求组件来表达。对所有或部分安全要求而言，如果第 2 部分或第 3 部分的安全组件都无法使用时，PP 可以明确说明这些安全要求不引自 CC 标准。

2）所有 TOE 安全功能和保证要求均应准确、无歧义地表达，才能进行一致性评估和论证。现有的通用准则功能或保证要求的详细程度和表达方式应当作一个典范来使用。

3) 应使用任何所需的操作把要求展开至足够详细的程度，以表明安全目的已达到。所有对要求组件的指定操作均应完成。

4) 所有IT 安全要求之间的依赖关系都应满足。依赖关系可以通过在TOE 安全要求内包含相关的要求或对环境提出要求来满足。

### C2.7 TOE 概要规范

**TOE 概要规范**应定义TOE 安全要求的实例化，该规范描述符合TOE 安全要求的TOE 安全功能和保证措施。注意在某些情况下TOE 概要规范的一部分信息可能与ADV _FSP 要求的一部分信息等同。

TOE 概要规范包括下列内容：

a) **TOE 安全功能**的陈述应包含IT 安全功能并说明这些功能是如何满足TOE 安全功能要求的。该陈述将包括一个在功能和要求间的双向映射，清楚表示哪个功能满足哪个要求，并表明所有的要求都达到。每一个安全功能至少要满足一个TOE 安全功能要求。

1) IT 安全功能应以非形式化的方式定义，其详细程度应足够理解其含义。

2) ST 中引用的所有安全机制应可追溯到相关的安全功能，这样就可看到每一个功能实现时使用的安全机制。

3) 当AVA _SOF.1 包括在TOE 保证要求里时，应指明所有利用概率和变换机制(例如口令或散列函数)实现的IT 安全功能，故意或偶然的攻击破坏这些机制的可能性是与TOE 安全相关的。应提供所有这些功能的TOE 安全功能强度分析。每一个指定功能的强度应确定并声明为基本级功能强度、中级功能强度、高级功能强度中的一个，或另选定义明确的特定级别。所提供的功能强度证据应足够评估者作出独立的判断，确认所声称的强度是足够和正确的。

b) **保证措施**的陈述指出TOE 的保证措施，这些措施已声明是满足所陈述的保证要求的。保证措施可被追溯到保证要求，这样可以看出哪些措施满足哪些要求。

如果合适的话，保证措施的定义可以引用相关的质量计划、生命周期计划和管理计划。

### C2.8 PP 声明

ST 可以根据情况作TOE 与PP(一个或多个PP)的一致性声明。如果作了任何PP 一致性声明，ST 就应包括**PP 声明**陈述，其中包括：解释、理由和其他支持材料，以证实该声明。

对TOE 目的和要求的ST 陈述，其内容和表达会受TOE 的PP 声明的影响。通过对每一个所声明的PP 考察以下情况后来概括对ST 的影响：

a) 如果没有PP 一致性声明，那么TOE 目的和要求的完整表达应按本附录的规定来完成。也不需要任何PP 声明。

b) 如果ST 声明仅符合PP 的要求，没有更进一步的限制，那么对PP 的引用就足以确定和证明TOE 目的和要求。重述PP 的内容是不必要的。

c) 如果ST 声明符合PP 要求，并且对PP 要求进一步的限制，那么ST 应表明PP 对限制的要求已经满足。例如在PP 包括不完整操作的情况下，ST 可引用特定的要求，但应在ST 内完成该操作。在某些情况下，完成操作的要求是重要的，此时最好在ST 中重述PP 的内容，以便描述得更清楚。

d) 尽管PP 的引用已经充分定义PP 的目的和要求，如果ST 的声明不仅与PP 的目的和要求一致，而且还通过增添目的和要求来扩展PP，那么ST 应定义这些增添的内容。在某些情况下，增添是重要的，此时最好在ST 中重述PP 的内容，以便描述得更清楚。

e) CC 评估不允许ST 声明与PP 部分一致。

CC 并不规定是重述还是引用PP 的目的和要求。对ST 内容的基本要求是必须完备、清楚、无歧义，这样ST 的评估才是可能的。ST 是TOE 评估可以接受的基础，并且应能清楚地追溯到所有所声明的PP。

要作出任何一个PP一致性声明，该声明应包括以下内容的陈述：

a）**PP引用**的陈述应指出与哪个PP一致，并包括任何与此相关的详细内容。一个有效的声明意味着TOE满足该PP所有的要求。

b）**PP裁剪**的陈述应指出那些满足PP操作的IT安全要求，否则对PP要求进一步限制。

c）**PP附加项**的陈述应指出那些作为PP目的和要求增添的TOE目的和要求。

### C2.9 基本原理

这部分提出用于ST评估的依据。这些依据将支持：ST是一个完整的、紧密结合的要求集合，满足该ST的TOE应在安全环境内提供一组有效的IT安全对策，并且TOE概要规范已经说明这些要求。基本原理应包括以下几点：

a）**安全目的基本原理**应阐明安全目的可追溯到在TOE安全环境里指明的所有方面，并且能覆盖所有的这些方面。

b）**安全要求基本原理**应阐明系列安全要求(TOE及其环境)是适合于满足，并可追溯到安全目的。应阐明以下几点：

1）将TOE及其IT安全环境的功能和保证要求组件相结合，能满足所述的安全目的；

2）该组安全要求一起构成一个互相支持且内在一致的整体；

3）安全要求的选择应说明理由，所有下列情况都应当专门说明：

——选择GB/T 18336第2部分或第3部分中没有的要求；

——选择不包括在EAL中的保证要求；

——不满足依赖关系；

4）已选择的PP功能强度级别和任何一个明确宣称的功能强度，是符合TOE安全目的的。

c）**TOE概述规范基本原理**应说明TOE安全功能和保证尺度将适合于满足TOE安全要求。下列内容将被论证：

1）所指定TOE的IT安全功能组合在一起工作以满足TOE安全功能要求；

2）所作的TOE功能强度声明是有效的，或者关于这种声明是不必要的断语也是有效的；

3）所述的保证措施与保证要求相一致的声明是合理的；

陈述基本原理的详细程度应与安全功能定义的详细程度相匹配。

d）**PP声明基本原理**的陈述应解释ST安全目的和要求与所有声明一致的PP之间的区别。如果没有PP一致性声明或者ST安全目的和要求与任何声明的PP是等同的，这部分可以忽略。

这部分材料可能篇幅太大，不一定对所有ST用户都适合和有用，因此可以单独发行。

# 附 录 D
（提示的附录）
## 参 考 资 料

[B&L] Bell, D.E. and Lapadula, L.J., Secure Computer System: Unified Exposition and MULTICS Interpretation, Revision 1, US Air Force ESD-TR-75-306, MITRE Corporation MTR2997, Bedford MA, March 1976.

[Biba] Biba, K.J., Integrity Consideration for Secure Computer System, ESD-TR-372, ESD/AFSC, Hanscom AFB, Bedford MA, April 1997.

[CTCPEC] Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), Version 3.0, Canadian System Security Centre, Communications Security Establishment, Government of Canada, January 1993.

[FC] Federal Criteria for Information Technology Security(FC), Draft Version 1.0(Volumes I and II), jointly published by the National Institute of Standards and Technology and the National Security Agency, US Government, January 1993.

[Gogu1] Goguen, J.A. and Meseguer, J., "Security Policies and Security Models", 1982 Symposium on Security and Privacy, pp.11-20, IEEE, April 1982.

[Gogu2] Goguen, J.A. and Meseguer, J., "Security Policies and Security Models", 1984 Symposium on Security and Privacy, pp.75-85, IEEE, April 1984.

[ITSEC] Information Technology Security Evaluation Criteria (ITSEC), Version 1.2, Office for Official Publications of the European Communities, June 1991.

[ISO 7498-2: 1989] Information Processing system - Open System Interconnection - Basic Reference Model, Part2: Security Architecture.

[TCSEC] Trusted Computer System Evaluation Criteria (TCSEC), US DoD 5200.28-STD, December 1985.