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。

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。

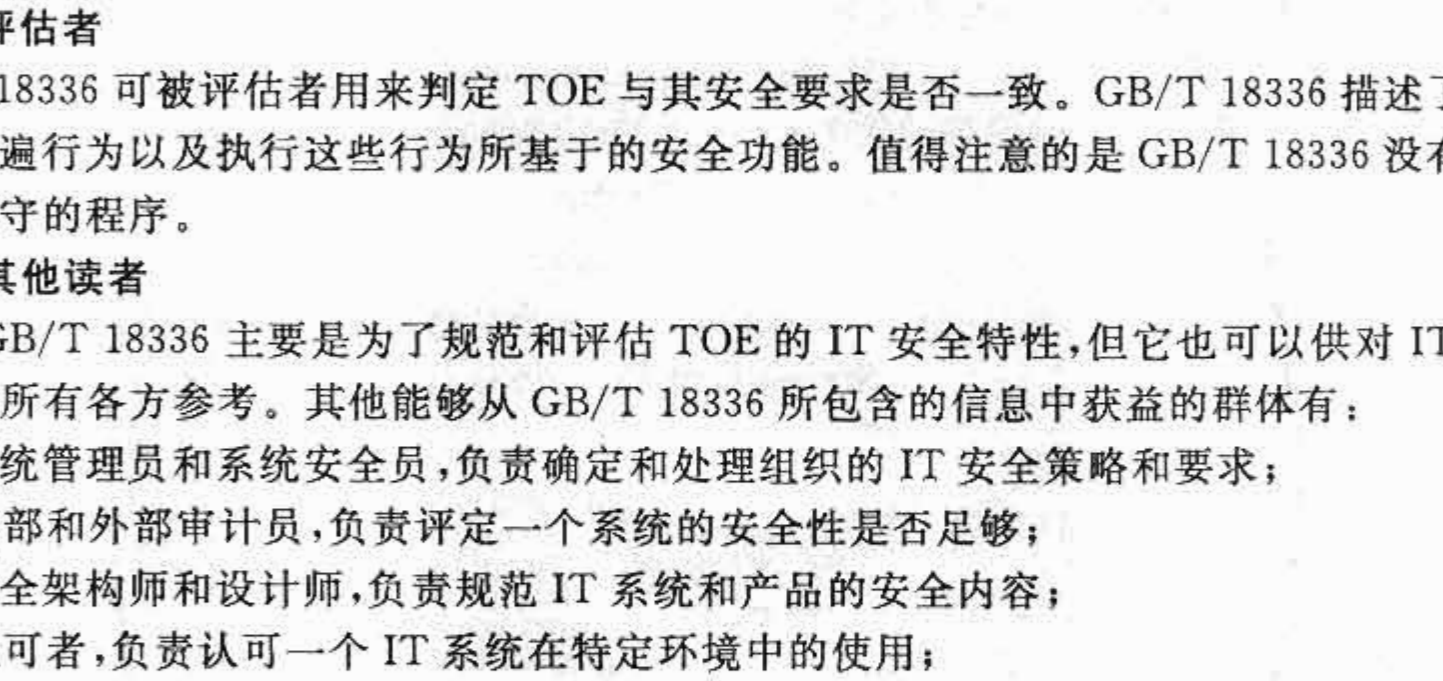

图 1 评估相关要素

使用通用的评估方法学主要是确保评估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。为了提高评估所见的一致性，最终的评估结果应提交给一个认证过程。该认证过程是对评估结果的独立审查，并产生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、方法学和认证过程由运行评估体制的评估管理机构负责，不属 GB/T 18336 的范围。

4.3 本标准的组织

GB/T 18336 提出了下列独立且又相互关联的部分。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 GB/T 18336 的介绍。它定义了 IT 安全性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，这些结构可用于表述 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规范。另外，针对各种目标读者，描述了 GB/T 18336 每一部分的有效性；

b) **第 2 部分：安全功能要求**，规定了一系列功能组件，作为表述 TOE 功能要求的标准方法。第 2 部分列出了一系列功能组件、族和类；

c) **第 3 部分：安全保证要求**，规定了一系列保证组件，作为表述 TOE 保证要求的标准方法。第 3 部分列出了一系列保证组件、族和类。第 3 部分也定义了 PP 和 ST 的评估准则，并提出了一些评估保证级别，这些级别定义了划分 TOE 保证等级的预定义的 GB/T 18336 尺度，通常称为评估保证级(EAL)。

下表列出了三类主要目标读者如何关注 GB/T 18336 的各个部分。

表 1 GB/T 18336 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供参考。指导构建 PP	用于了解背景信息，供开发安全要求和编写 TOE 安全规范时参考	用于了解背景信息和供参考。指导构建 PP 和 ST
第 2 部分	在编制安全功能要求陈述时用作指导和供参考	在解释功能要求陈述和编制 TOE 功能规范时，供参考	在确定 TOE 是否有效地满足所声称的安全功能时，用作评估准则的强制性陈述
第 3 部分	在确定所需的保证级别时，用作指导	在解释保证要求陈述和确定 TOE 保证方法时，供参考	在确定 TOE 保证以及评估 PP 和 ST 时，用作评估准则的强制性陈述

5 一般模型

5.0 引言

本章提出了在整个 GB/T 18336 都适用的一些一般概念，其中也包括使用这些概念的环境，以及使用这些概念的 GB/T 18336 方法。GB/T 18336.2 和 GB/T 18336.3 进一步展开这些概念的使用，并采用本标准描述的方法。本章假定读者已具备 IT 安全的一些知识，并不打算作为该领域的辅导教材

GB/T 18336 用一组安全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使用 GB/T 18336的前提条件。然而，这些概念本身又是相当通用的，我们无意将其限于 GB/T 18336 适用的这类 IT 安全问题。

5.1 安全相关要素

5.1.1 一般安全相关要素

安全涉及保护资产不受威胁，这些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 2 说明了高层次概念及其关系。

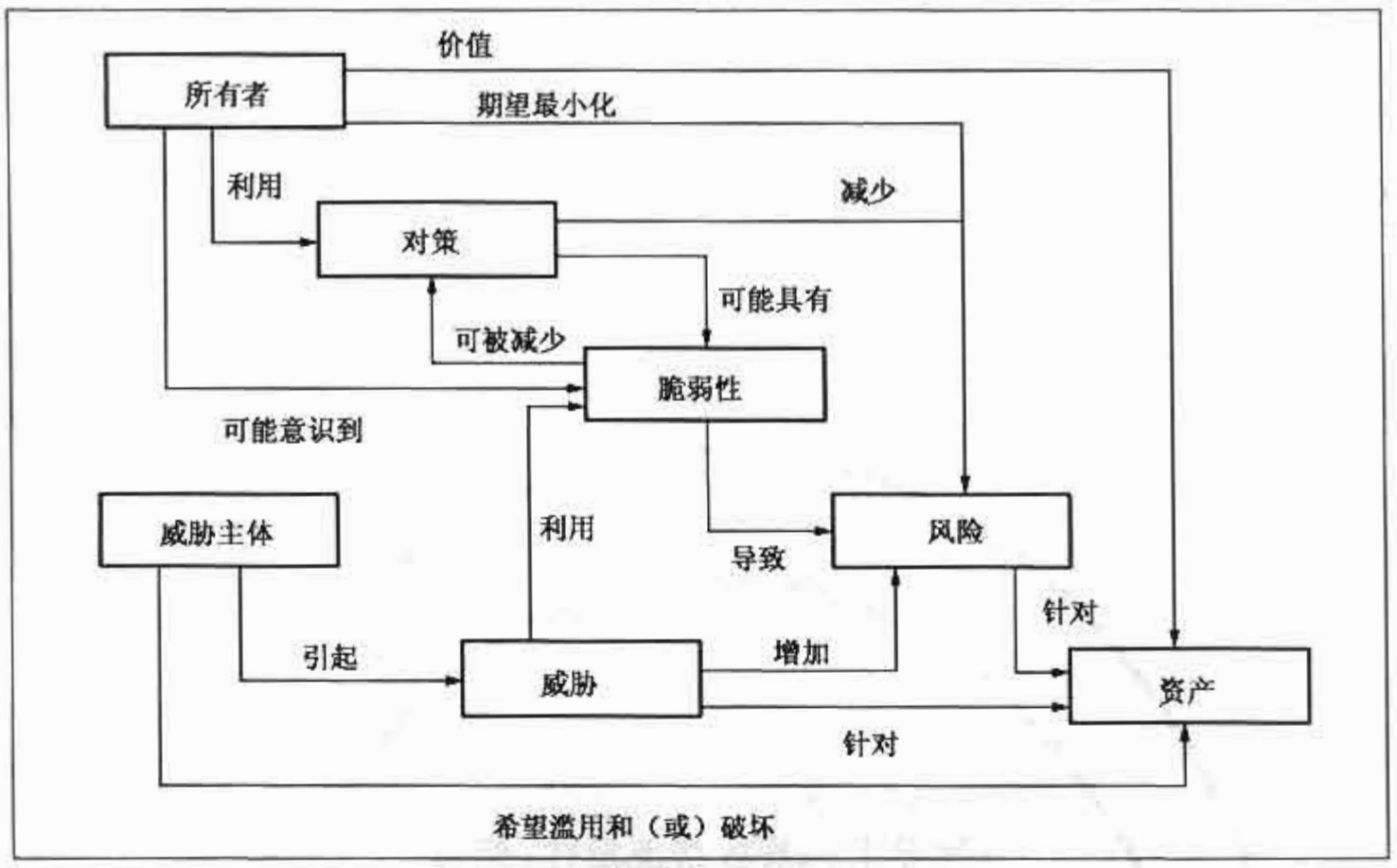

图 2　安全概念及其关系

保护关注的资产是那些对资产赋予价值的所有者的责任。实际的或假定的威胁者也可对资产赋予了一定的价值，并试图以危害资产所有者利益的方式滥用资产。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。安全特有的损坏一般包括但不限于：资产破坏性地泄漏给未授权的接收者（丧失保密性），资产由未授权地修改而损坏（丧失完整性），或资产的访问权被未授权地剥夺（丧失可用性）。

资产的所有者将分析其资产和环境中可能存在的威胁，确定相关的风险。这种分析能有助于选择对策，以抑制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（直接或间接地为其他各方提供指导）。在对策使用后仍会有残留的脆弱性，这些脆弱性仍可被威胁者利用，从而造成了资产的残余风险。资产所有者将寻求通过其他的限制措施来最小化这些残余风险。

在资产所有者允许将其资产暴露给特定的威胁之前，所有者需要确信其对策足以应付资产面临的这些威胁。所有者自己可能没有能力对对策的所有方面加以判断，但可以寻求对对策进行评估。评估的输出是保证所达到程度的一个陈述，即相信对策能降低所保护资产的风险。该陈述还给这些对策赋予了一个保证级别，保证作为这些对策的特性，给出了信任这些对策正确操作的依据。此陈述还能被资产所有者用来决定是否接受将这些资产暴露给这些威胁所带来的风险。图 3 说明了这种关系。

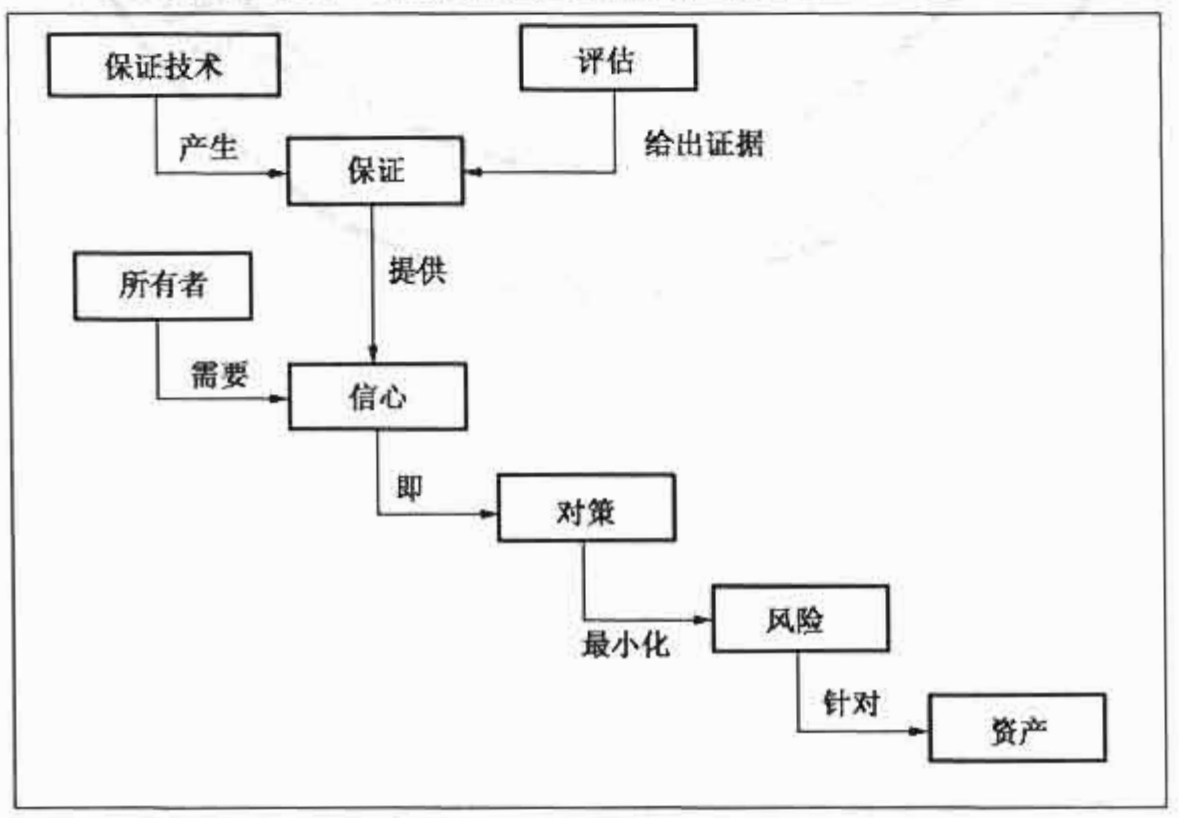

图 3　评估概念及其关系

通常,资产所有者应当对这些资产负责,并能够决定接受将这些资产暴露给这些威胁所带来的风险。这就要求评估所产生的陈述是可以可辩解的。因此,评估宜产生客观的、可重复的结论,该结论可作证据引用。

5.1.2 信息技术安全相关要素

许多资产以信息的形态被 IT 产品或系统储存、处理和传送,以满足信息所有者规定的要求。信息所有者可要求严格控制对此类信息表示法(即数据)的任何传播和修改。他们可要求 IT 产品或系统实现某些特殊的 IT 安全控制,作为消除数据安全威胁而采用的全部安全对策的一部分。

IT 系统的获取和建造都是为了满足特定的要求,出于经济上的原因,可尽量使用现存的商用 IT 产品,如操作系统、通用应用程序组件和硬件平台。一个系统可利用下层 IT 产品的功能来实现 IT 安全对策,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 产品被合并到或准备被合并到多个 IT 系统时,独立评估该产品安全性,并建立一个已评估产品目录,这样做更有代价优势。这种评估的结果宜以支持产品合并到多个 IT 系统的方式表述,避免为检查产品的安全性进行不必要的重复工作。

IT 系统的认可者具有与信息所有者相当的权力,确定 IT 和非 IT 安全对策的组合是否为数据提供了足够的保护,并可决定是否允许该系统运行。认可者可以要求对 IT 对策进行评估,以确定 IT 对策是否提供了足够的保护,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,严格程度也可以不同,这取决于认可者所使用的规则。

5.2 GB/T 18336 方法

IT 安全信任能通过开发、评估和操作过程中所采取的各种行为获得。

5.2.1 开发

GB/T 18336 不强制要求任何特定的开发方法或生命周期模型。图 4 描述了安全要求和 TOE 之间关系的基本假设。该图提供讨论的基础,不应认为某一种方法(如瀑布法)比另一种方法(如原型法)更优越。

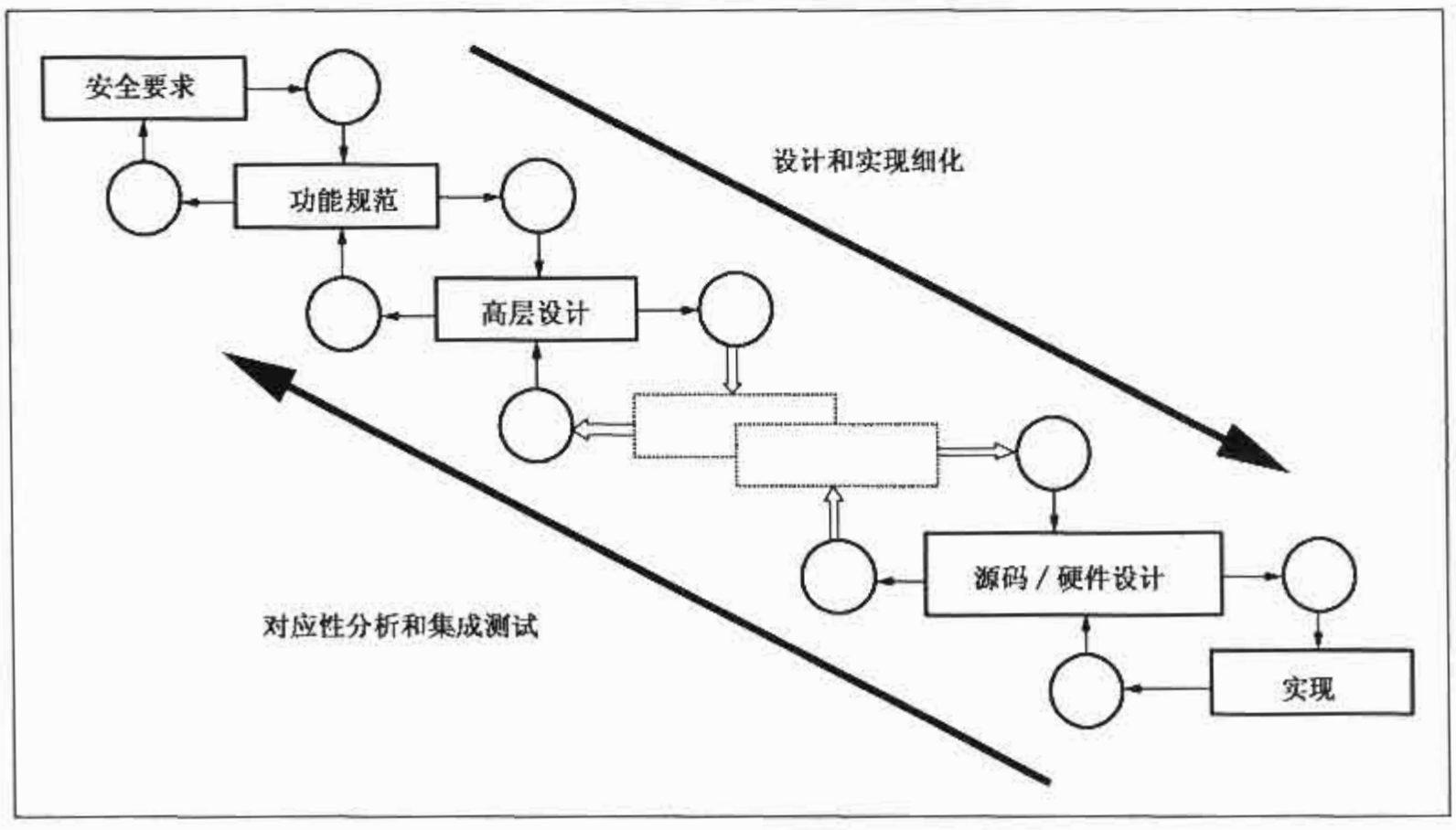

图 4 TOE 开发模型

重要的是,有效实施 IT 开发所需要遵守的安全要求,以满足客户的安全目的。除非在开发过程的开始阶段就确定合适的要求,否则再好的设计,结果最终产品也不能满足其目标客户的目的。

在安全目标中详细说明了将安全要求细化到一个 TOE 概要规范中的方法。每个低层次的细化代表具有更为详细的设计分解。最低的抽象表示是 TOE 实现本身。

GB/T 18336 并不强制规定一套专有的设计表示方法。GB/T 18336 的要求是应有合适的设计表示方法，并以合适的粒度水平呈现，以说明何处要求：

a) 每个层次的细化是更高层次的一个完备实例化(即，在更高层次抽象定义的所有 TOE 安全功能、特性和行为都必须在低层次上明确呈现)；

b) 每个层次的细化是更高层次的一个精确实例化(即，不存在低层次抽象定义的 TOE 安全功能、特性和行为不是高层次定义所需要的)。

GB/T 18336 保证准则识别出了功能规范、高层设计、低层设计和实现的设计抽象层次。依据这些既定的保证级别，可要求开发者证明开发方法是如何满足 GB/T 18336 保证要求的。

5.2.2 TOE 评估

图 5 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 评估的主要输入有：

a) 一组 TOE 证据，包括作为 TOE 评估基础的一个 ST；

b) 需要评估的 TOE；

c) 评估准则、方法学和体制。

另外，资料性材料(例如 GB/T 18336 的应用注释)和评估者及评估团体的 IT 安全专业知识也常用来作为评估的输入。

评估过程的预期结果是对 TOE 满足其在 ST 中所规定安全要求的一个确认以及一个或多个报告，报告以书面形式记录评估者依据评估准则对 TOE 得出的检查结果。这些报告对 TOE 所代表的产品或系统的实际和潜在客户都是非常有用，对开发者也同样有用。

通过一个评估所获得的信任程度依赖于所要满足的保证要求(如评估保证级)。

评估能通过两种途径促成产生更好的 IT 安全产品。评估旨在发现 TOE 的错误或脆弱性，以便开发者纠正，从而减少在今后的运行中发生安全故障的可能性。另一方面，为了应对严格的评估，开发者在 TOE 设计和开发时会更加细心。因此，评估过程能对初始化要求、开发过程、最终产品以及运行环境等产生强烈的、间接的但又是积极的影响。

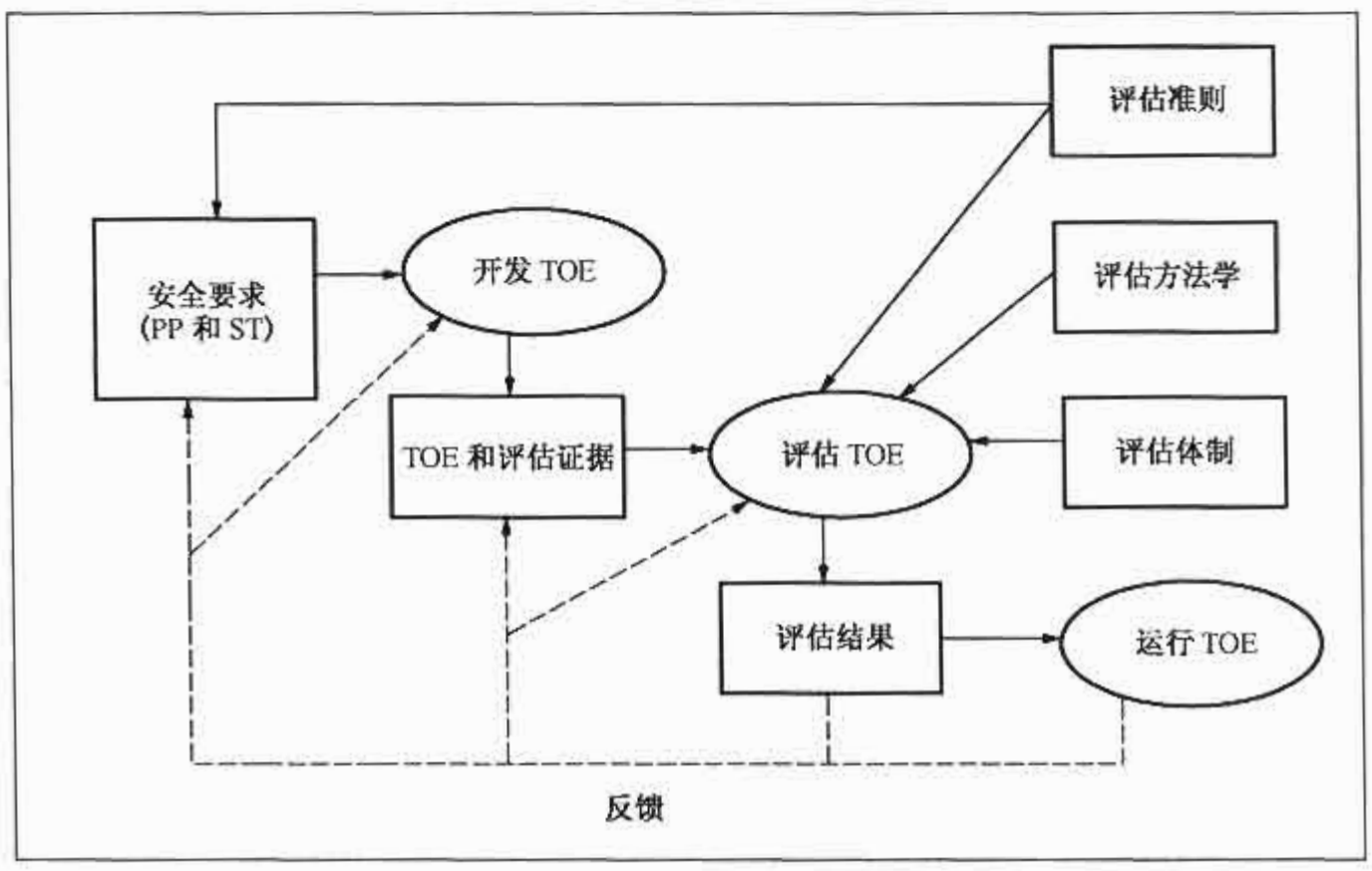

图 5 TOE 评估过程

5.2.3 运行

客户可选择在他们的环境中使用评估后的 TOE。一旦一个 TOE 开始运行，就可能出现以前未知的错误或脆弱性，或者需要修订环境假设。作为运行的结果，可以给出反馈，要求开发者改正 TOE 或者重新定义它的安全要求或环境假设。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。在某种情况下，只需评估必需的更新部分，以便重新获得对 TOE 的信任。再评估的详细程序，包括评估结果的再度使用都超出了 GB/T 18336 的范围。

5.3 安全概念

在工程过程和管理框架都支持安全 TOE 开发和评估的情况下，评估准则是最有用的。本条仅提供例证和指导，并不试图强制规定分析过程、开发方法或可能使用 GB/T 18336 的评估体制。

当使用 IT 并且关心 IT 单元保护资产的能力时，GB/T 18336 才适用。为了表明资产是安全的，从最高层抽象到运行环境中最终 IT 实现的所有表示层次都必须提出安全考虑。这些表示层次，如下章节所描述，允许表征和讨论安全问题和争论，但这些层次本身并不证明最终的 IT 实现真实地展现了所要求的安全行为，因此是可信的。

GB/T 18336 要求某层表示包含该层 TOE 表示的一个基本原理，因此该层次必须包含一个合理的、令人信服的论据，以表明它与更高的层次是一致的，而且是自我完备的、正确的并且内在一致的。证实与邻近更高层次表示一致的基本原理陈述主要关注与 TOE 正确性相关的情况。直接证实符合安全目的的基本原理，支持与 TOE 有效对抗威胁和执行组织安全策略相关的情况。

如图 6 所示，GB/T 18336 将表示分成不同的层次。这也说明了一种方法，依据该方法，在开发一种 PP 或 ST 时，就能导出安全要求和规范。所有 TOE 安全要求从根本上讲均来源于对 TOE 的用途和使用场合的担忧。该图并不试图强制规定 PP 和 ST 的开发方法，而在于说明某些分析方法的结果如何与 PP 和 ST 的内容相关联。

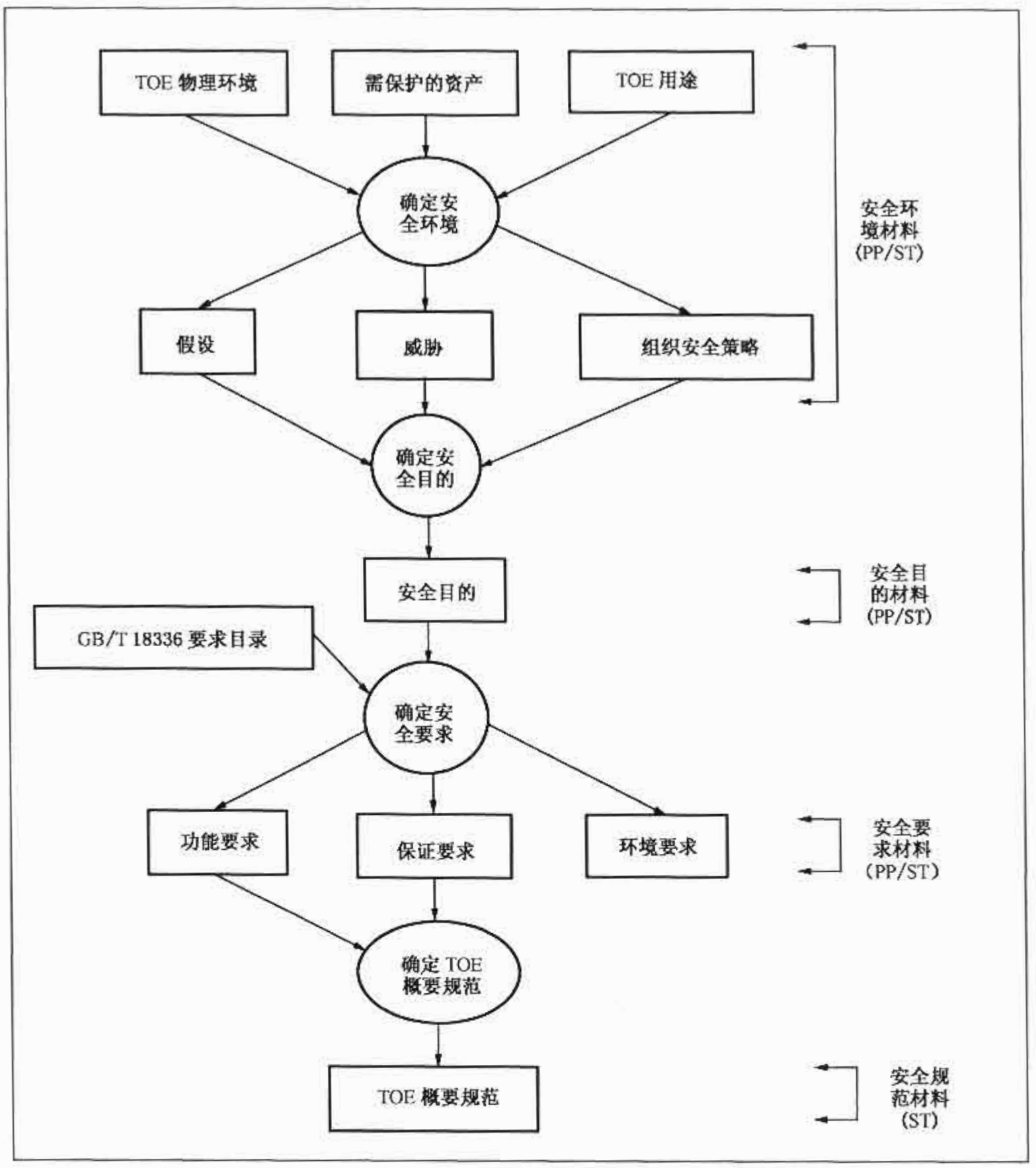

图 6 要求和规范的导出

5.3.1 安全环境

安全环境包括所有明确相关的法规、组织安全策略、习惯、专门技术和知识，因此它定义了 TOE 将使用的场合。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，指与 TOE 安全性相关的 TOE 运行环境的所有方面，包括已知的物理和人员的安全装置；

b) 需要由 TOE 单元执行安全要求或策略来保护的资产。包括直接涉及安全要求的资产，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，说明产品类型和预期的 TOE 用法。

对安全策略、威胁和风险的审查允许先作出下列有关 TOE 的安全特别陈述：

a) 假设陈述，为了认为 TOE 是安全的，TOE 环境应满足该陈述。对 TOE 评估而言，该陈述可以作为公理而接受。

b) 资产的安全威胁陈述，将指明与 TOE 相关的安全分析中发现的所有威胁。GB/T 18336 使用下述术语表征一个威胁，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。安全风险的评价将通过对威胁发展成一个真实攻击的可能性、攻击成功实施的可能性和可能造成的任何破坏后果等方面评价来刻画每个威胁。

c) 适用的组织安全策略陈述，将指明相关的策略和规则。对于一个 IT 系统，可直接引用这些策略，然而对于通用的 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。

5.3.2 安全目的

安全环境的分析结果可用来陈述安全目的，这些安全目的对抗既定的威胁并提出既定的组织安全策略和假设。安全目的宜与已说明的 TOE 运行目标或产品用途以及与其物理环境有关的任何知识相一致。

确定安全目的的意图是为了阐明所有的安全关注并指出哪些安全因素直接由 TOE 或其环境来处理。这种归类基于一个综合工程判断、安全策略、经济因素和风险接受决策的过程。

环境安全目的将在 IT 域内通过非技术的或程序的方式来实现。

IT 安全要求只提出 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组 TOE 安全要求和环境安全要求，一旦这些要求得到满足，就可以保证 TOE 满足其安全目的。

GB/T 18336 根据功能要求和保证要求的不同种类提出安全要求。

功能要求来源于明确支持 IT 安全性的那些 TOE 功能，并定义期望的安全行为。GB/T 18336.2 定义了功能要求。常见的功能要求有标识、鉴别、安全审计以及原发抗抵赖等。

当 TOE 含有由概率或置换机制(例如口令或散列函数)实现的安全功能时，保证要求可规定一个与宣称的安全目的一致的最低强度级别。此时，规定的等级将是基本级功能强度、中级功能强度、高级功能强度中的其中一个。要求每个这样的功能达到最低强度级别或至少达到一个既定的明确尺度。

对于给定的一组功能要求，保证的程度是可以改变的，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 18336.3 定义了由这些组件构建的保证要求和一组评估保证级(EAL)。保证要求来源于开发者行为、产生的证据以及评估者行为。常见的保证要求有对开发过程的严格性约束、对查找和分析潜在的安全脆弱性影响的要求。

安全目的可以被所选择的安全功能满足的这种保证来源于以下两个方面：

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) 对安全功能有效性的信任，也就是评估它们是否真正满足了所陈述的安全目的。

安全要求通常包括存在期望行为和避免不期望行为两方面要求。通过使用或测试，一般可以证明期望行为的存在，但并不总是能明确证明不存在不期望行为。测试、设计审查和实现审查非常有助于减少存在不期望行为的这类风险。基本原理陈述为不存在不期望行为的这类断言提供进一步支持。

5.3.4 TOE 概要规范

ST 中规定的 TOE 概要规范定义了 TOE 安全要求的实例化。它规定了一个声称满足功能要求的安全功能高层定义和一些满足保证要求的保证措施。

5.3.5 TOE 实现

TOE 实现是依据 ST 中安全功能要求和 TOE 概要规范的一种 TOE 现实化。TOE 实现是通过一个运用安全和 IT 工程技能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 将满足安全目的。

5.4 GB/T 18336 描述材料

GB/T 18336 提出了可在其中进行一个评估的这种架构。通过对证据和分析提出要求，可以得到一个更为客观、有用的评估结果。GB/T 18336 提出了一组通用结构和一种能表达、传递 IT 安全的语言，并使得那些负责 IT 安全的人员有可能从他人的先前经验和专门技术中获益。

5.4.1 安全要求的表达

GB/T 18336 定义了一组结构，将已知有效的安全要求合成很有意义的组合体，这些结构能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图 7 描述。

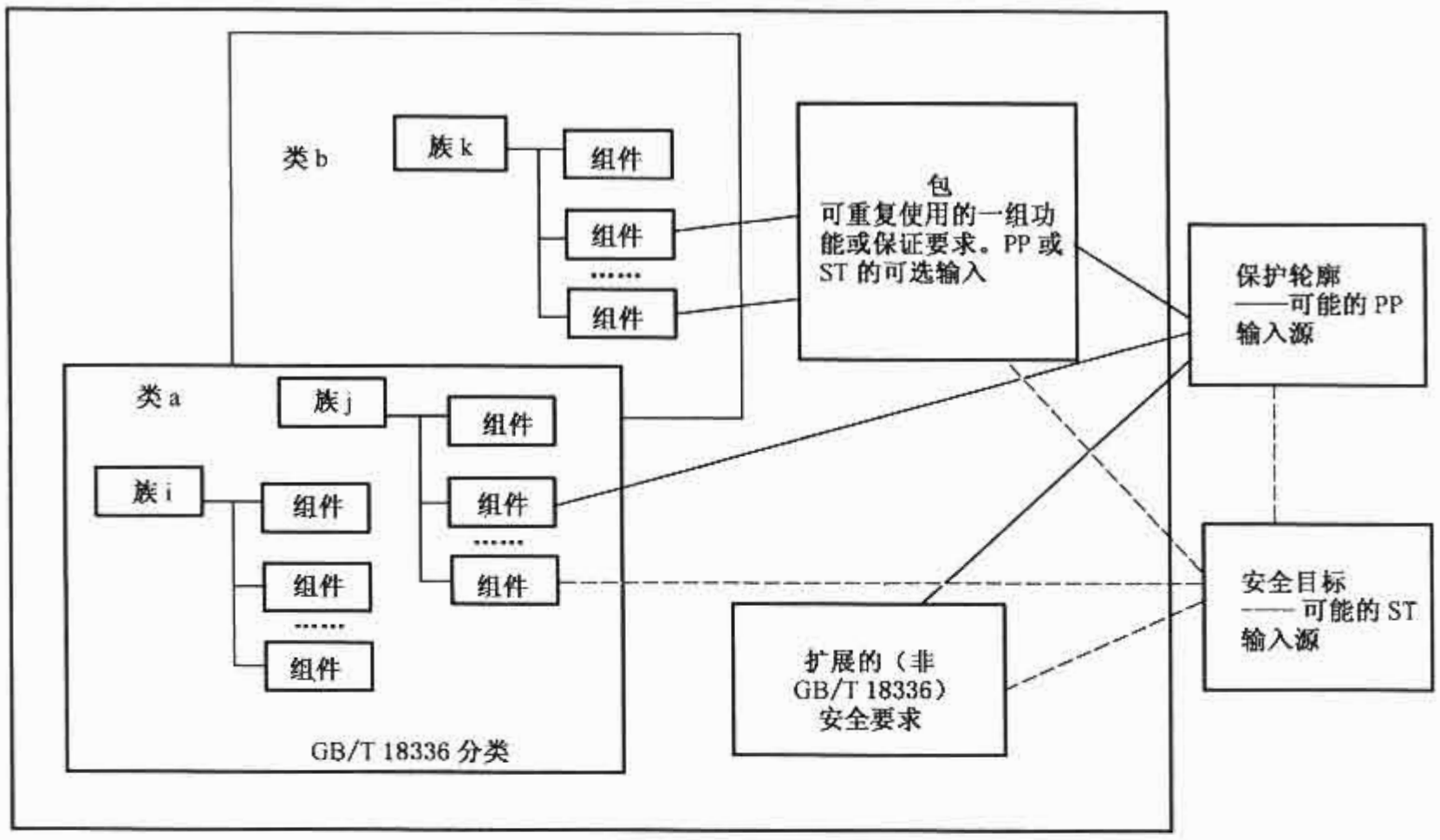

图 7 要求的组织和结构

GB/T 18336 安全要求以“类—族—组件”这种层次结构组织，以帮助客户查找特定的安全要求。

GB/T 18336 使用相同的风格描述功能和保证方面的要求，并使用相同的组织方式和术语。

5.4.1.1 类

术语“类”用于安全要求的最高层次归类。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。

类的成员被称为族。

5.4.1.2 族

族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。

族的成员被称为组件。

5.4.1.3 组件

一个组件描述一组特定的安全要求，它是 GB/T 18336 结构中安全要求的最小可选集合。一个族中的组件集合，可以按安全要求强度或能力递增的顺序进行描述，这些安全要求具有相同用途；在部分族也可以不区分层次的方式来描述。在某种情况下，一个族只有一个组件，因而不需要排序。

组件由一个个元素组成。元素是安全要求的最低层次表达，并且是能被评估验证的不可再分的安全要求。

5.4.1.3.1 组件间的依赖关系

组件间可能存在依赖关系。当一个组件无法独自充分表达安全要求而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，可以存在于保证组件之间，也可以存在于功能和保证组件之间。

组件间依赖关系的描述是 GB/T 18336 组件定义的一部分。当把组件引入到 PP 和 ST 中适当的地方时，为了确保 TOE 要求的完备性，应满足相应的依赖关系。

5.4.1.3.2 组件允许的操作

GB/T 18336 功能和保证组件可以严格按照 GB/T 18336 定义的那样使用，也可以通过使用允许的操作对其进行裁剪，以满足相应的安全目的。当组件中某个元素在进行“细化”时，PP/ST 作者应清晰标识出已执行完的细化。PP/ST 作者也应注意，依赖此要求的其他要求的依赖关系必须满足。对组件允许执行如下几种操作：

a) 反复：允许一个组件在不同操作时被使用超过一次以上；

b) 赋值：允许指定参数；

c) 选择：允许从一个列表中选定一项或多项；

d) 细化：允许增加细节。

5.4.1.3.2.1 反复

当必须涵盖同一个要求的不同方面时（如识别多个用户），重复使用相同的组件以涵盖允许的每一个方面。

当在要求组件层面采取“反复”操作时，不需要总是重复每个组件反复的所有文本，如果这样做将导致组件中的某些元素在没有任何改变的情况下被重复多次。在 PP 或 ST 中，只允许重复那些每次都改变的要求元素，无论是在细化，还是实现赋值或选择操作。（关于反复赋值要求的更多指导见 5.4.1.3.2.4）

5.4.1.3.2.2 赋值

某些组件有元素带有参数，这使 PP/ST 作者能够指定一组值到 PP 或 ST 中以满足安全目的。这些元素清晰地标识了每一个参数，并且限制了可赋给该参数的值。

一个元素的任何方面，如果其容许值能被明确无误的描述或列举，就能被一个参数代表。这些参数可以是将要求限制到一个特定值或取值范围的一个属性或一个规则。如，基于一个安全目的，组件中的一个元素可以声称一个给定的操作可以被执行多次。此时，赋值宜规定在参数中使用的数值或数值范围。

5.4.1.3.2.3 选择

选择操作就是从一个列表中挑选出一个或多个项，以限制组件中一个元素的范围。

5.4.1.3.2.4 细化

对于所有组件，PP/ST 作者都可以通过规定额外的细节来限制可接受的实现集合以满足安全目的。组件中一个元素的细化由这些添加的技术细节组成。

要认为组件的一个改变是一个正确的细化，该改变必须满足以下所有条件：

a) 一个 TOE 细化后的要求也将满足原始的要求，如 PP/ST 上下文关系所解释的那样；

b) 当一个细化要求被反复时，允许每个反复只针对该要求的部分范围，但是，反复的总和必须满足原始要求的全部范围；

c) 细化后的要求不会扩展原始要求的范围；

d) 细化后的要求不会改变原始要求的依赖关系名录。

正确的细化例子有：

a) 任何改变仅仅是编辑上的，如提高一个完整赋值的可读性这样的改变，或者仅涉及语法修正。

b) 由于 PP/ST 中的上下文关系，一个改变不会更改要求的范围。例如，对一个要求进行改变，将“TOE 用户”变为“TOE telnet 用户”就是一个正确的细化，因为只有 TOE 用户才是 telnet 用户。

c) 一个改变提供了关于实现的可选方法方面的信息，没有扩展要求的范围。例如，将一个要求从“提供验证能力”改变为“通过执行密码校验和以提供验证能力”就是一个正确的细化。此改变只是限制了用于实现一个现有要求的机制性质，没有扩展原始要求的范围。

GB/T 18336.2 附录部分给出了正确完成选择和赋值操作的指导意见。这些指导意见提供了如何完成操作的标准化规程，并且除非 PP/ST 作者能证明有误，否则必须满足这些规定。

a) 对于一个选择操作的完成，只有在已明确规定的情况下，“没有”才是有效的选项。

供选择操作完成的列表必须是非空的。如果选择了“没有”操作，就是没有额外的选择项可选择。如果在一个选择中没有给定“没有”作为选项，在一个选择中通过“和”和“或”合并所选择的项是允许的，除非在选择中明确规定“选取一个”；在需要时，选择操作可以同反复操作一起使用。此时，为每个反复操作挑选的选项的适用范围不能与其他重复选择的对象重叠，因为它们是排他的。

b) 对于一个赋值操作的完成，GB/T 18336.2 附录部分指出了何时“没有”是一个正确的完成。

某些需要的操作可以（整体或部分地）在 PP 内完成，也可留在 ST 内完成，不过所有操作必须在 ST 内完成。

5.4.1.4 安全要求的使用

GB/T 18336 定义了三种要求结构：包、PP 和 ST。GB/T 18336 还定义了能表达多数团体需求的一组 IT 安全准则，并在开发这些结构时提供主要的专业知识和经验。开发 GB/T 18336 的主要理念是尽可能使用 GB/T 18336 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 8 表明了这些不同结构间的关系。

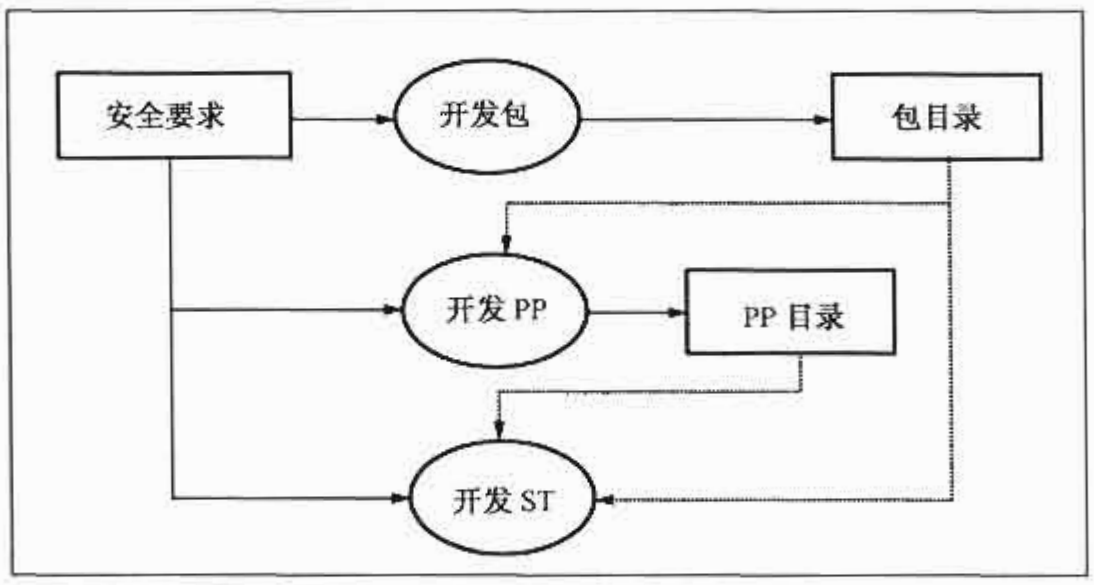

图 8 安全要求的应用

5.4.1.4.1 包

组件的一个中间组合称作包。包可以描述一组功能或保证要求，这些要求满足部分指定的安全目的。包可重复使用，可用来定义那些公认有用的且有效的满足既定安全目的的要求。一个包可用于构造更大的包、PP 和 ST。

评估保证级（EAL）就是 GB/T 18336.3 中预先定义的一些保证包。一个 EAL 是评估保证要求的一个基线集合。每个 EAL 定义了一套相容的保证要求。合起来，这些 EAL 构成一个有次序的集合，是 GB/T 18336 预定义的保证度量尺度。

5.4.1.4.2 保护轮廓

保护轮廓（PP）包含一套或来自 GB/T 18336 或明确阐述的安全要求，它应包括一个评估保证级（EAL）（可能通过添加额外的保证组件来增强）。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，可用来定义那些公认有用的且有效的满足既定安全目的的 TOE 功能和保证要求。PP 还包括安全目的和安全要求的基本原理。

PP 可以由用户团体、IT 产品开发者或其他对定义这样一系列通用要求有兴趣的相关方负责开发。PP 为客户提供了一套方法以提出一组特定的安全需求，并且有助于将来依据这些需求进行评估。

5.4.1.4.3 安全目标

安全目标(ST)包含一组安全要求,这些要求可以引用自 PP,可以直接引用 GB/T 18336 的功能或保证组件,也可以是明确阐述的。ST 可以对一个特定 TOE 的安全要求进行描述,通过评估,可以证明这些要求是有用的且有效的满足了既定安全目的。

ST 包含 TOE 的概要规范,同时还包含安全要求和安全目的,以及它们的基本原理。ST 是所有的相关各方对 TOE 提供什么样的安全性达成一致的基础。

5.4.1.5 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) 现有 PP

一个 ST 中的 TOE 安全要求可以由包含在现有 PP 中预先存在的安全要求陈述来充分地表达,或者期望与其一致。

现有 PP 可以作为一个新 PP 的基础。

b) 现有包

PP 或 ST 中部分 TOE 安全要求可能已在一个已使用过的包中表述过。

GB/T 18336.3 定义的 EAL 就是一组预定义的包。PP 或 ST 中的 TOE 保证要求宜包括从 GB/T 18336.3 选取的某个 EAL。

c) 现有功能或保证要求组件

PP 或 ST 中的 TOE 功能或保证要求可以直接用 GB/T 18336.2 或 GB/T 18336.3 中的组件来表达。

d) 扩展的要求

GB/T 18336.2 中没有的附加功能要求或 GB/T 18336.3 中没有的附加保证要求也可以在 PP 或 ST 中使用。

宜尽可能使用 GB/T 18336.2 和 GB/T 18336.3 已有的安全要求材料。使用一个现有 PP 将有助于确保 TOE 满足一组公认的有用的需求,进而可以得到更广泛的认可。

5.4.2 评估类型

5.4.2.1 PP 评估

PP 评估是依照 GB/T 18336.3 中的 PP 评估准则进行的。此类评估的目的是为了证明该 PP 是完备的、一致的、技术合理的且适合用来作为一个可评估 TOE 的要求陈述。

5.4.2.2 ST 评估

针对 TOE 的 ST 评估是依照 GB/T 18336.3 中的 ST 评估准则进行的。此类评估具有双重目的:首先是为了证明该 ST 是完备的、一致的、技术合理的,因而适合用来作为相应 TOE 评估的基础;其次,当某个 ST 宣称与一个 PP 一致时,证明该 ST 完全满足该 PP 的要求。

5.4.2.3 TOE 评估

TOE 评估是以一个充分完善的 ST 作为基础,依照 GB/T 18336.3 中的评估准则进行的。一个充分完善的 ST 是指所有的子条款都已被完善到评估体制接受的程度,且预知没有重大的评估障碍,该 ST 可降低在随后的评估过程中可能存在的风险。评估一个 TOE 的结果是证明该 TOE 满足包含在已评估的 ST 中的安全要求。

6 GB/T 18336 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。具体结果见图 9。

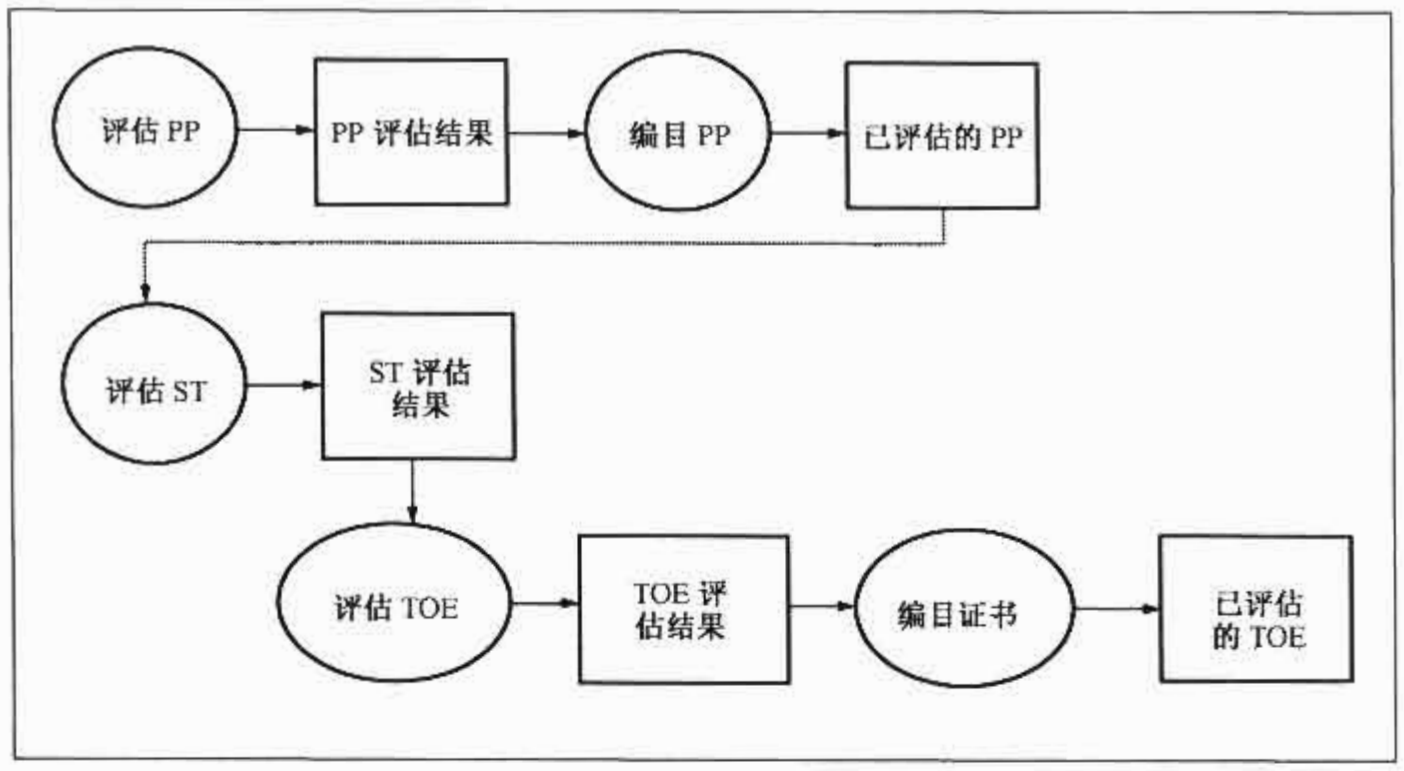

图 9　评估结果

评估应能产生出能引为证据的客观的和可重复的结果，即使没有绝对客观的尺度来度量 IT 安全性评估结果时也应如此。一组评估标准的存在是必需的前提条件，因为这样评估才可以得到有意义的结果，并且提供了评估机构之间互认评估结果的技术基础。但准则的应用包含了主观的和客观的元素，这也是为什么不能对 IT 安全性进行精确地和通用地划定等级的原因。

与 GB/T 18336 有关的等级划分代表了对 TOE 安全特性进行专门考察时的所见。这种等级并不保证适用于任何特殊的应用环境。允许一个 TOE 在特定应用环境下使用的决策应基于对多个安全因素的考虑，包括评估所见。

6.2　PP 和 ST 中的要求

GB/T 18336 定义了一套能满足多方需求的 IT 安全准则。GB/T 18336 是围绕这样一个中心观点开发的，即在 PP 和 ST 中描述 TOE 要求时，尽可能使用 GB/T 18336.2 中的安全功能组件和 GB/T 18336.3中的 EAL 和保证组件，因为它们代表了众所周知、易于理解的领域。

GB/T 18336 也意识到可能需要未列出的功能和保证要求，以表达全部的 IT 安全要求。以下内容要求适用于引入这些扩展的功能和保证要求：

a)　包含在 PP 和 ST 中的任何扩展的功能或保证要求应清晰地和明确无误地表达，这样评估和一致性证实才是切实可行的。GB/T 18336 现有的功能或安全组件描述的详细程度和方式可以当作模板使用；

b)　应告诫评估结果是通过使用扩展的功能或保证要求得到的；

c)　将扩展的功能或保证要求引入到一个 PP 或 ST 时应遵守 GB/T 18336.3 中 APE 类或 ASE 类的要求。

6.2.1　PP 评估结果

GB/T 18336 包含有这样的评估准则，以便评估者证明一个 PP 是否完备的、一致的、技术合理的且适合用来作为一个可评估 TOE 的要求陈述。

PP 的评估结果为“通过”或“不通过”。评估结果为“通过”的 PP 应当列入 PP 注册表中。

6.3　TOE 内的要求

GB/T 18336 包含有这样的评估准则，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，通过使用 GB/T 18336，评估者能够说明：

a)　指定的 TOE 安全功能是否满足功能要求，进而有效地满足 TOE 的安全目的；

b) 指定的 TOE 安全功能是否正确地实现了。

GB/T 18336 的安全要求定义了 IT 安全性评估准则的公认适用范围。一个 TOE 可以按照 GB/T 18336进行评估,如果只使用了 GB/T 18336 中的功能和保证要求来表述安全要求。使用不包含一个 EAL 的保证包时应提供正当理由。

不过,也可能存在这样的需求,一个 TOE 满足的安全要求无法直接使用 GB/T 18336 来描述。GB/T 18336 意识到了评估这样一个 TOE 的必要性,但是,由于附加要求不属于 GB/T 18336 的公认适用范围,因此这种评估的结果必须作相应的警示。这种警示由相关评估管理机构放置在评估结果的风险普遍接受部分。

TOE 的评估结果应包含与 GB/T 18336 一致性的声明。运用 GB/T 18336 的术语描述一个 TOE 的安全性时通常允许比较 TOE 的安全特性。

6.3.1 TOE 评估结果

TOE 的评估结果应是一个声明,该声明描述信任 TOE 满足要求的程度。

TOE 的评估结果为“通过”或“不通过”。评估结果为“通过”的 TOE 应当列入一个注册表中。评估结果也应包含一个“一致性结果”。

6.4 一致性结果

一致性结果表示通过了评估的 TOE 或 PP 所满足的要求集合及其出处。一致性结果表明遵守 GB/T 18336.2(功能要求)、GB/T 18336.3(保证要求)和一组预定义的要求(如 EAL、PP)。

一致性结果由下列各项中的其中一个组成:

a) **GB/T 18336.2 一致**——如果功能要求只基于 GB/T 18336.2 中的功能组件,PP 或 TOE 是 GB/T 18336.2 一致的。

b) **GB/T 18336.2 扩展**——如果功能要求包含有 GB/T 18336.2 中没有的功能组件,PP 或 TOE 是 GB/T 18336.2 扩展的。

加上下列各项中的其中一个:

a) **GB/T 18336.3 一致**——如果保证要求只基于 GB/T 18336.3 中的保证组件,PP 或 TOE 是 GB/T 18336.3 一致的。

b) **GB/T 18336.3 扩展**——如果保证要求包含有 GB/T 18336.3 中没有的保证要求,PP 或 TOE 是 GB/T 18336.3 增强的。

另外,一致性结果可包含一份关于既定义要求集合的声明,此时一致性结果由下列各项中的其中一个组成:

a) **包选定一致**——如果功能或保证要求包含包中列出的被当作一致性结果一部分的全部组件,PP 或 TOE 与一个选定的预定义功能或保证包(如 EAL)是一致的。

b) **包选定增强**——如果功能或保证要求是包中列出的被当作一致性结果一部分的全部组件的完全超集,PP 或 TOE 是选定的预定义功能或保证包(如 EAL)的增强。

最后,一致性结果也可包含一份关于保护轮廓的声明,此时它包含下述表述:

a) **PP 一致**——TOE 满足特定的 PP,这些 PP 被当作一致性结果的一部分列出。

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 10 表明处理评估结果的选择方式。产品能被评估,并按集成度连续递增的方式排列编目,直至达到可操作的系统水平,此时就可以进行与系统认可相关的评估。

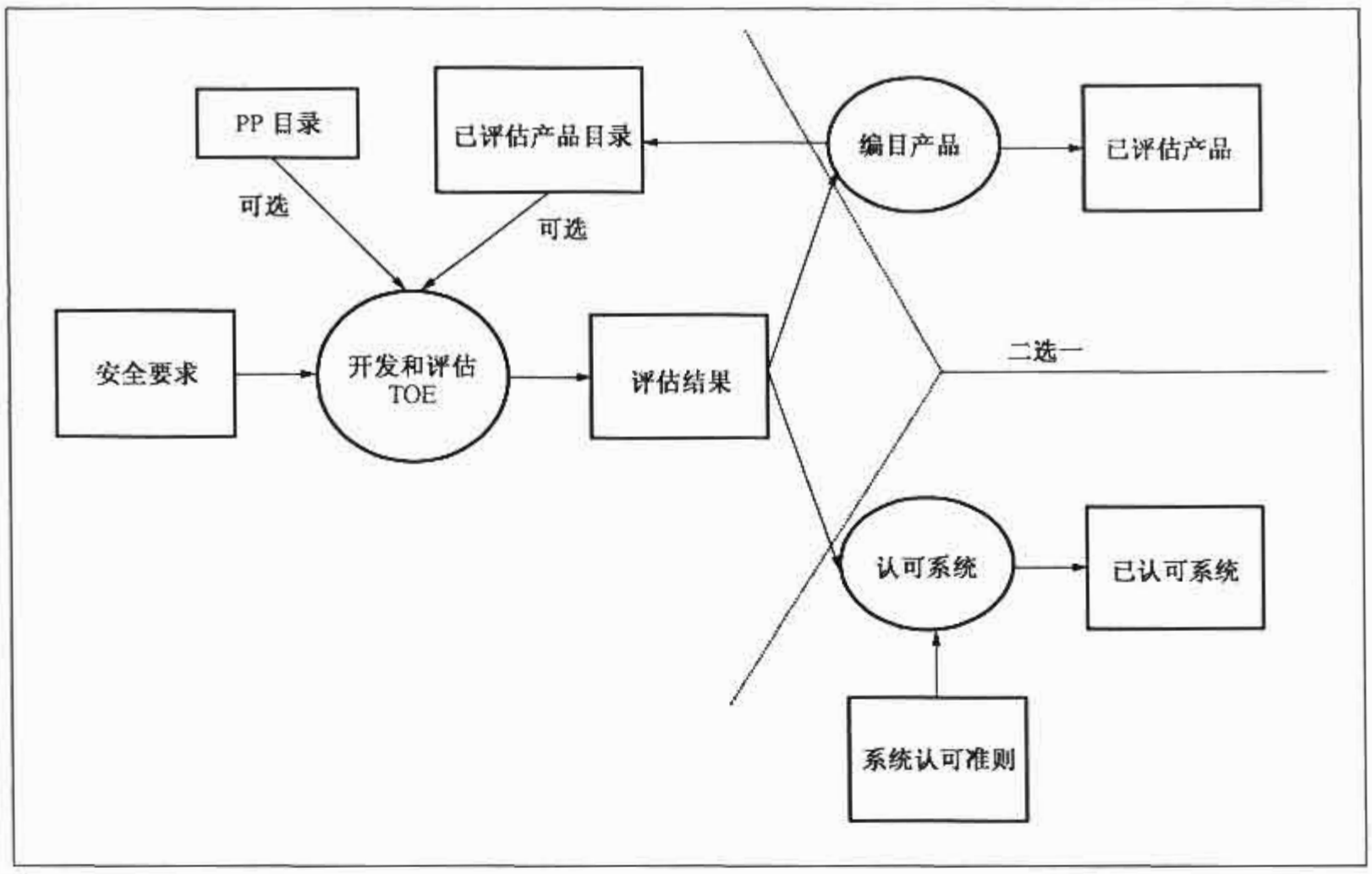

图 10 TOE 评估结果的应用

TOE 是针对要求开发的，也需要考虑所吸纳的所有已评估产品和所引用的所有 PP 的安全属性。随着 TOE 评估产生一组记录评估所见的评估结果。

对一个 IT 产品进行评估是为了更广泛的使用，可将评估所见的摘要列入已评估产品的目录，以便在广阔的市场中寻找安全的 IT 产品时使用。

在吸纳或将吸纳一个 TOE 到一个已通过评估且安装妥当的 IT 系统时，评估结果对系统认可者是非常有用的。当使用的组织专用认可准则要求进行 GB/T 18336 评估时，认可者可考虑 GB/T 18336 的评估结果。GB/T 18336 的评估结果是系统认可过程的输入之一，该过程决定是否接受系统运行风险。

附 录 A
（规范性附录）
保护轮廓规范

A.1 概述

一个 PP 为一类 TOE 定义了一组与实现无关的 IT 安全要求。这类 TOE 试图满足客户对 IT 安全性的通用需求，因此客户不必依赖特定的 TOE 就能构建或引用一个 PP 来表示他们的 IT 安全需求。

本附录包含了一些关于 PP 编写形式的要求。GB/T 18336.3 第 8 章“保证类 APE”包含了一些以保证组件形式提出的可用于 PP 评估的要求。

A.2 保护轮廓的内容

A.2.1 内容与形式

PP 应满足本附录所规定的内容要求。PP 宜描述成一个面向用户的文档，尽量少引用 PP 用户难以得到的其他材料。适当时，基本原理部分可以单独提供。图 A.1 中描述了 PP 的内容，应按其建立 PP 文档大纲。

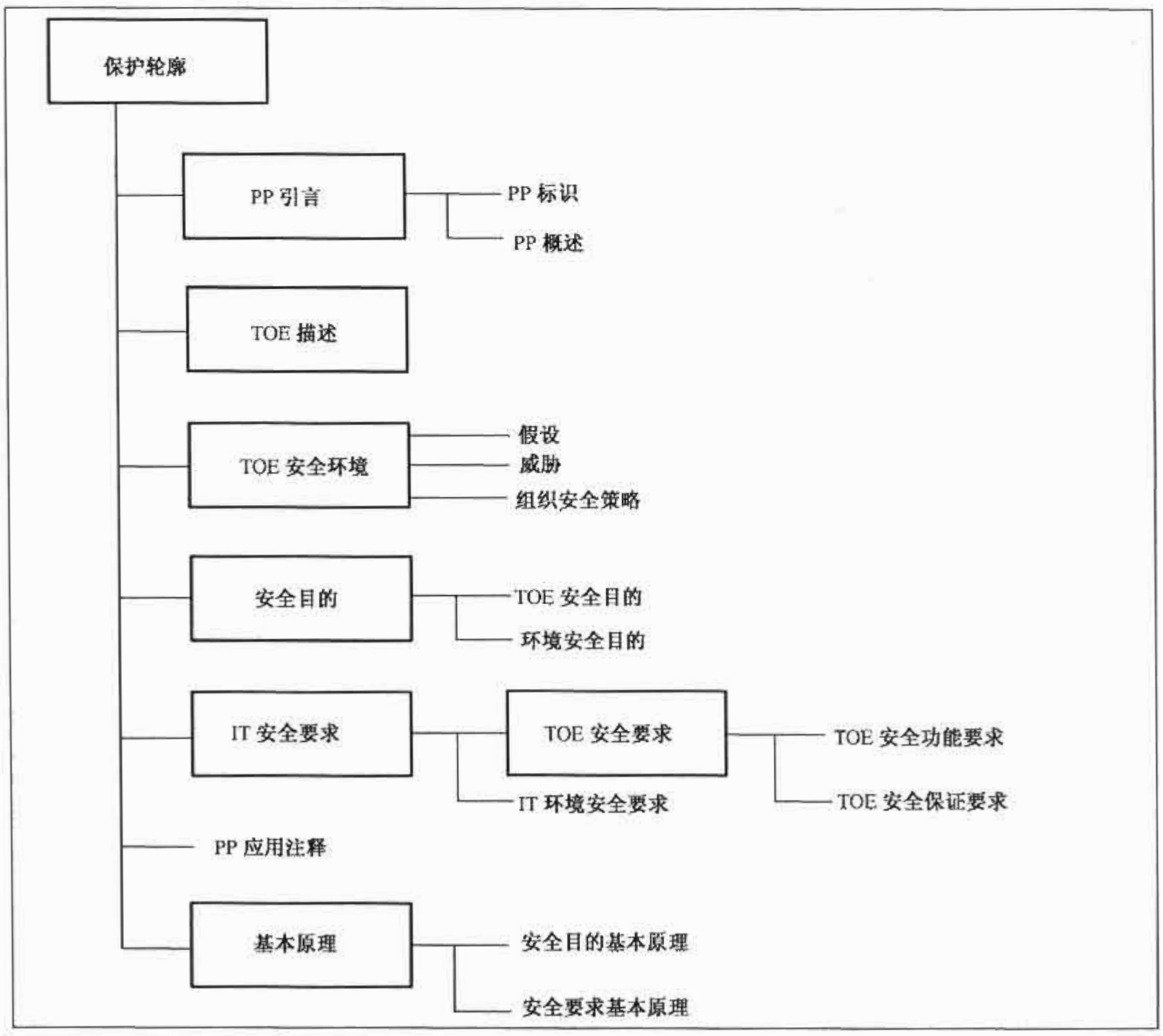

图 A.1 保护轮廓内容

A.2.2 PP 引言

PP 引言应包括文档管理和进行 PP 注册所必要的概括性信息，如下所述：

a) **PP 标识**，应提供必要的标记和描述信息，以识别、编目、注册和交叉引用一个 PP。

b) **PP 概述**，应以叙述形式概括该 PP。概述宜足够详细，以便一个潜在 PP 用户据此确定该 PP 是否有价值。概述也可作为一个独立的摘要用于 PP 编目和注册。

A.2.3 TOE 描述

PP 的这个部分应描述 TOE，以帮助理解它的安全要求，同时还应说明 TOE 的产品类型和一般的 IT 特征。

TOE 描述提供了评估的背景信息。在 TOE 描述中给出的信息在评估过程中将用于识别前后不一致性之处。由于一个 PP 一般不针对特定的实现，因此所描述的 TOE 特征可能是假定的。如果 TOE 是一个以安全为主要功能的产品或系统，则 PP 的本部分可以用来描述该 TOE 适用的更广泛的应用环境。

A.2.4 TOE 安全环境

TOE 安全环境的陈述应描述 TOE 所处应用环境和预期部署方式中的安全状况。该陈述应包括如下几点：

a) **假设**描述应描述 TOE 将在或试图在其中使用的环境的安全状况。这包括下述几点：

——关于 TOE 预期使用的信息，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**描述应包括对资产的所有威胁，在 TOE 或其环境中需要特定的保护措施来对付这些威胁。值得注意的是，不是在环境中可能遭遇的所有威胁都必须列出，只有那些与 TOE 的安全运行相关的威胁才需要列出。

一个威胁应从确定的威胁主体、攻击和作为攻击对象的资产等三方面来刻画。威胁主体宜通过诸如专业技能、可用资源和动机等来刻画。攻击宜通过诸如攻击方法、任何可利用的脆弱性和时机等来刻画。

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**描述应识别 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。在提出任一个独立的策略陈述时，说明和解释可能是必需的，这样才可用来建立清晰的安全目的。

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 是物理上分布式的，可能有必要分别针对 TOE 环境的不同区域讨论安全环境（假设、威胁、组织安全策略）。

A.2.5 安全目的

安全目的的陈述应定义 TOE 及其环境的安全目的。安全目的应处理既定安全环境的所有方面。安全目的应反映一定的意图，应适于对抗所有既定的威胁并覆盖所有既定的组织安全策略和假设。一个威胁可以由一个或多个 TOE 安全目的来对抗，可由一个或多个环境安全目的来对抗，也可由它们的一个组合来对抗。应识别以下两类安全目的。注：当威胁或组织安全策略部分被 TOE 所覆盖，部分被它的环境所覆盖，那么相关的安全目的应分别在下述类中重复。

a) **TOE 安全目的**应被明确地陈述，并可追溯到由 TOE 所对抗的既定威胁，或可追溯到 TOE 满足的组织安全策略；

b) **环境安全目的**应被明确地陈述，并可追溯到由 TOE 无法完全对抗的既定威胁，或可追溯到 TOE 无法完全满足的组织安全策略或假设。

注意环境的安全目的可能是 TOE 安全环境假设部分陈述的全部或部分重述。

A.2.6 IT安全要求

PP的这部分内容定义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) 当需要覆盖同一个要求的不同方面时(如多类用户的识别)，反复使用(即使用“反复”操作)GB/T 18336.2的同一个组件覆盖每一个方面的情形是可能存在的。**TOE安全要求**的陈述应定义功能和保证安全要求，TOE和其评估支持证据需要满足这些要求，以便满足TOE的安全目的。TOE安全要求应按如下方式描述：

1) TOE**安全功能要求**的陈述宜从GB/T 18336.2中提取适当的功能组件来定义TOE功能要求。

当TOE安全保证要求(如EAL2和更高的)含有AVA_SOF.1组件时，TOE安全功能要求陈述应包含一个关于由概率或置换机制(如口令或散列函数)实现的TOE安全功能的最低强度级别，所有这样的功能应达到该最低级别要求。这样的强度级别可以是基本级功能强度(SOF-basic)、中级功能强度(SOF-medium)、高级功能强度(SOF-high)中的一个。强度级别的选择应与既定的TOE安全目的一致。为了满足TOE的某些安全目的，也可自主为选定的功能要求定义特殊的功能强度度量尺度。

作为TOE安全功能强度评估(AVA_SOF.1)的一部分，不管强度声明是为单个TOE安全功能定的，还是整个最低强度级别都由TOE满足，都将被评估。

2) **TOE安全保证要求**的陈述宜像一个EAL一样表述保证要求，也可使用GB/T 18336.3的保证组件随意扩展。PP也可通过添加明确陈述的额外的保证要求来扩展EAL，这些要求可以不取自GB/T 18336.3。

b) **IT环境安全要求**的陈述是可选的，该陈述应识别那些被TOE的IT环境满足的IT安全要求。PP的此部分中的要求可以从GB/T 18336.2和GB/T 18336.3选取，但是如果这样，宜改写相关的要求以清楚地指出IT环境而不是TOE必须满足该要求。这种改写是细化操作的一种特例，不受GB/T 18336组件修改相关的评估要求限制。如果TOE没有声称依赖IT环境，PP的这部分内容可以省略。

c) 下列**通用条件**应同等使用，在表述TOE及其IT环境的安全功能和保证要求时：

1) 所有IT安全要求都应适当地从GB/T 18336.2或GB/T 18336.3选取安全要求组件来表达。如果对所有或部分安全要求而言，没有适用的GB/T 18336.2或GB/T 18336.3要求组件，PP可以明确说明这些安全要求没有引自GB/T 18336。

2) 所有明确陈述的TOE安全功能和保证要求均应准确、无歧义地表达，这样才能进行一致性评估和论证。现有的GB/T 18336功能或保证要求描述的详细程度和方式可以当作模板使用。

3) 当选取了需要指定操作(赋值或选择)的安全组件时，PP应使用这些操作对相关的要求进行补充说明，以达到能证实安全目的都已满足的详细程度。任何需要的但又不在PP内执行的操作同样应被标识出。

4) 通过对要求组件进行操作，TOE安全要求陈述可在必要时自主指定或禁止使用特定的安全机制。

5) IT安全要求之间的所有依赖关系都应被满足。依赖关系可以通过引入有关要求到TOE安全要求中或作为环境要求来满足。

A.2.7 应用注释

PP的这个可选部分可包括额外的支持信息，该信息对构建、评估或使用TOE是有关或有用的。

A.2.8 基本原理

PP的该部分给出了用于PP评估的证据。这些证据将支持：PP是一个完整的、紧密结合的要求集合，并且满足该PP的TOE将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**应证明所提出的安全目的可追溯到在 TOE 安全环境里所识别的所有方面，并且正好覆盖所有的这些方面。

b) **安全要求基本原理**应证明该组(TOE 及其环境)安全要求正好满足安全目的且可追溯到安全目的。应证明以下几点：

1) 关于 TOE 及其 IT 安全环境的单个功能和保证要求组件的组合满足所提出的安全目的。

2) 该组安全要求一起构成了一个互相支持且内在一致的整体。

3) 安全要求的选择是合理的。所有下列情况应当专门论证：

——选择没有包含在 GB/T 18336.2 或 GB/T 18336.3 中的要求；

——选择的保证要求没有包含一个 EAL；

——不满足依赖关系。

4) 为 PP 选择的功能强度级别和任何明确的功能强度声明与 TOE 安全目的是一致的。

此材料可能过于冗长，不一定对所有 PP 用户都是适当的或有用的，因此可以单独分发。

附 录 B
（规范性附录）
安全目标规范

B.1 概述

一个 ST 包含一个既定 TOE 的 IT 安全要求，并规定了该 TOE 应提供的安全功能和保证措施以满足所提出的安全要求。

一个 TOE 的 ST 是开发者、评估者和适当的客户之间对 TOE 安全特性和评估范围达成一致的基础。ST 的读者不限于那些对 TOE 生产和评估负有责任的人员，那些负责管理、营销、采购、安装、配置、操作和使用 TOE 的人员也可是 ST 的读者。

ST 可合并一个或多个 PP 的要求或宣称符合一个或多个 PP。在最初定义 B.2 中所要求的 ST 内容时，没有考虑这种 PP 一致性声明的影响。B.2.8 指出了 PP 一致性声明对必需的 ST 内容的影响。

本附录包含了一些关于 ST 编写形式的要求。GB/T 18336.3 第 9 章“保证类 ASE”包含了一些以保证组件形式提出的可用于 ST 评估的要求。

B.2 安全目标的内容

B.2.1 内容与形式

ST 应满足本附录所规定的内容要求。ST 宜描述成一个面向用户文档，尽量少引用 ST 用户无意得到的其他材料。适当时，基本原理可以单独提供。

图 B.1 描述了 ST 的内容，应按其建立 ST 文档大纲。

B.2.2 ST 引言

ST 引言应包括以下的文档管理和概括信息：

a) **ST 标识**，应提供必要的标记和描述信息，以控制和标识 ST 以及相关的 TOE；

b) **ST 概述**，以叙述形式总结该 ST。概述宜有足够的细节提供给 TOE 的潜在客户，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) **GB/T 18336 一致性声明**，应说明该 TOE 与 GB/T 18336 一致性的任何可评估声明，就像在本标准 6.4 中指明的一样。

B.2.3 TOE 描述

ST 的这个部分应描述 TOE，以帮助理解它的安全要求，同时还应说明产品或系统的类型。TOE 的范围和边界应使用通用术语描述，不管是物理方式的（硬件或软件组件/模块），还是逻辑方式的（由 TOE 提供的 IT 和安全特征）。

TOE 描述提供了评估的背景信息。在 TOE 描述中给出的信息在评估过程中将用于识别前后不一致的地方。如果 TOE 是一个以安全为主要功能的产品或系统，则 ST 的本部分可以用来描述该 TOE 适用的更广泛的应用环境。

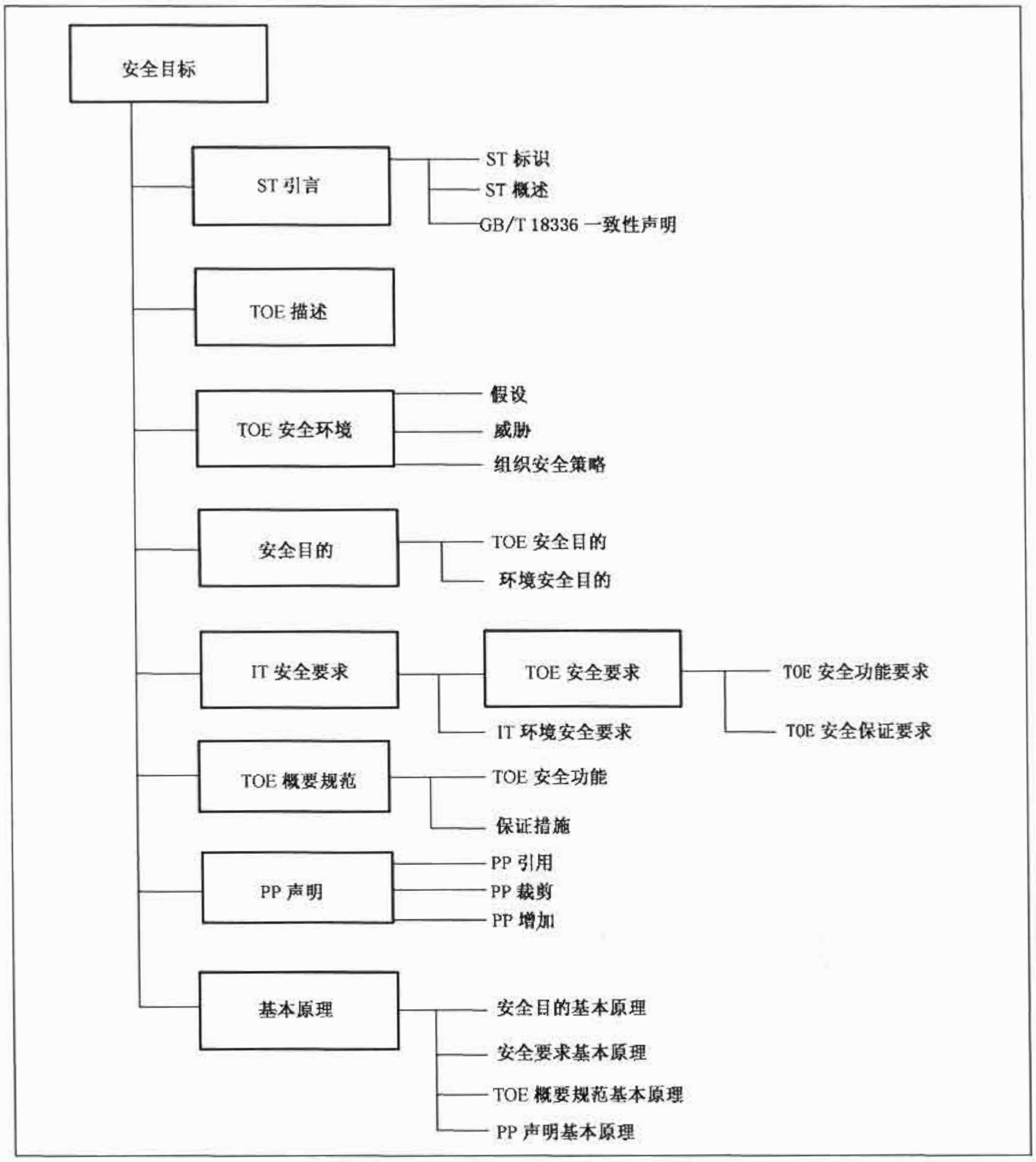

图 B.1 安全目标内容

B.2.4 TOE 安全环境

TOE 安全环境的陈述应描述 TOE 所处应用环境和预期部署方式中的安全状况。该陈述包括以下几点：

a) **假设**描述应描述 TOE 将在或试图在其中使用的环境的安全状况。这包括下述几点：

——关于 TOE 预期使用的信息，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**描述应包括对资产的所有威胁，在 TOE 或其环境中需要特定的保护措施来对付这些威胁。值得注意的是，不是在环境中可能遭遇的所有威胁都必须列出，只有那些与 TOE 的安全运行相关的威胁才需要列出。

一个威胁应从确定的威胁主体、攻击和作为攻击对象的资产等三方面来刻画。威胁主体宜通过诸如专业技能、可用资源和动机等来刻画。攻击宜通过诸如攻击方法、任何可利用的脆弱性和时机等来刻画。

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**描述应识别 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。在提出任一个独立的策略陈述时，说明和解释可能是必需的，这样才可用来建立清晰的安全目的。

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 是物理上分布式的，可能有必要分别针对 TOE 环境的不同区域讨论安全环境（假设、威胁、组织安全策略）。

B.2.5 安全目的

安全目的的陈述应定义 TOE 及其环境的安全目的。安全目的应处理既定安全环境的所有方面。安全目的应反映一定的意图，应适于对抗所有既定的威胁并覆盖所有既定的组织安全策略和假设。一个威胁可以由一个或多个 TOE 安全目的来对抗，可由一个或多个环境安全目的来对抗，也可由它们的一个组合来对抗。应识别以下两类安全目的。注：当威胁或组织安全策略部分被 TOE 所覆盖，部分被它的环境所覆盖，那么相关的安全目的应分别在下述类中重复。

a) **TOE 安全目的**应被明确地陈述，并可追溯到由 TOE 所对抗的既定威胁，或可追溯到 TOE 可满足的组织安全策略。

b) **环境安全目的**应被明确地陈述，并可追溯到由 TOE 无法完全对抗的既定威胁，或可追溯到 TOE 无法完全满足的组织安全策略或假设。

注意环境的安全目的可能是 TOE 安全环境假设部分陈述的全部或部分重述。

B.2.6 IT 安全要求

ST 的这部分内容定义 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) 当需要覆盖同一个要求的不同方面时（如多类用户的识别），反复使用（即使用“反复”操作）GB/T 18336.2 的同一个组件覆盖每一个方面的情形是可能存在的。**TOE 安全要求**的陈述应定义功能和保证安全要求，TOE 和其评估支持证据需要满足这些要求，以便满足 TOE 的安全目的。TOE 安全要求应按如下方式描述：

1) **TOE 安全功能要求**的陈述宜从 GB/T 18336.2 中提取适当的功能组件来定义 TOE 功能要求。

当 TOE 安全保证要求（如 EAL2 和更高的）含有 AVA_SOF.1 组件时，TOE 安全功能要求陈述应包含一个关于由概率或置换机制（如口令或散列函数）实现的 TOE 安全功能的最低强度等级，所有这样的功能应达到该最低级别要求。这样的强度级别可以是基本级功能强度（SOF-basic）、中级功能强度（SOF-medium）、高级功能强度（SOF-high）中的一个。强度级别的选择应与既定的 TOE 安全目的一致。为了满足 TOE 的某些安全目的，也可随意为选定的功能要求定义特殊的功能强度度量尺度。

作为 TOE 安全功能强度评估（AVA_SOF.1）的一部分，不管强度声明是为单个 TOE 安全功能定的，还是整个最低强度级别都由 TOE 满足，它都将被评估。

2) **TOE 安全保证要求**的陈述宜像一个 EAL 一样表述保证要求，也可使用 GB/T 18336.3 的保证组件随意扩展。ST 也可通过添加明确陈述的额外的保证要求来扩展 EAL，这些要求可以不取自 GB/T 18336.3。

b) **IT 环境安全要求**的陈述是可选的，该陈述应识别那些被 TOE 的 IT 环境满足的 IT 安全要求。ST 的此部分中的要求可以从 GB/T 18336.2 和 GB/T 18336.3 选取，但是如果这样，宜改写相关的要求以清楚地指出 IT 环境而不是 TOE 必须满足该要求。这种改写是细化操作的一种特例，不受 GB/T 18336 组件修改相关的评估要求限制。如果 TOE 没有声称依赖 IT 环境，ST 的这部分内容可以省略。

c) 下列**通用条件**应同等使用，在表述 TOE 及其 IT 环境的安全功能和保证要求时：

1) 所有 IT 安全要求都应适当地从 GB/T 18336.2 或 GB/T 18336.3 选取安全要求组件来表达。如果对所有或部分安全要求而言，没有适用的 GB/T 18336.2 或 GB/T 18336.3 要求组件，ST 可以明确说明这些安全要求没有引自 GB/T 18336。

2) 所有明确说明的 TOE 安全功能和保证要求均应准确、无歧义地表达，这样才能进行一致性评估和论证。现有的 GB/T 18336 功能或保证要求描述的详细程度和表达方式可以当作模板使用。

3) 应执行所有必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。所有对要求组件的规定操作均应完成。

4) IT 安全要求之间的所有依赖关系都应被满足。依赖关系可以通过引入有关要求到 TOE 安全要求中或对作为环境要求来满足。

B.2.7 TOE 概要规范

TOE 概要规范应定义 TOE 安全要求的实例化。此规范应描述满足 TOE 安全要求的 TOE 安全功能和保证措施。注意，在某些情况下，作为 TOE 概要规范组成部分的功能性信息可与为 TOE 规定的作为 ADV_FSP 要求组成部分的信息完全相同。

TOE 概要规范包括下列内容：

a) **TOE 安全功能陈述**应包含 IT 安全功能并应说明这些功能是如何满足 TOE 安全功能要求的。该陈述应包含一个在功能和要求间的双向映射，以清楚展现哪个功能满足哪个要求，以及所有的要求都已满足。每一个安全功能至少应满足一个 TOE 安全功能要求。

1) IT 安全功能应以非形式化的方式定义，其详细程度应足以理解其意图。

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 保证要求中时，应指明所有由概率或置换机制(例如口令或散列函数)实现的 IT 安全功能。故意或偶然攻击破坏这些功能机制的可能性是与 TOE 的安全性相关的。应为每一个这样的功能规定一个 TOE 安全功能强度声明。应确定每一个这种功能的强度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，或自主定义的特定度量尺度。

b) **保证措施陈述**详细说明 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。保证措施应被追溯到保证要求，这样才能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。

B.2.8 PP 声明

ST 可以自主地声明 TOE 与(一个或多个)PP 一致。如果作了任何 PP 一致性声明，ST 就应包含一个 PP **声明**陈述，包括必要的解释、证明和其他支持材料以证实该声明。

关于 TOE 目的和要求的 ST 陈述的内容和形式会受 TOE 的 PP 声明影响。通过考察每一个所声明 PP 的以下情况，可以概括对 ST 的影响：

a) 如果没有声明遵从 PP，那么 TOE 目的和要求的完整表述应按本附录的规定来完成。不包含任何 PP 声明。

b) 如果 ST 声明仅遵从 PP 的要求，没有更进一步的限制，那么对 PP 的引用就足以定义和证明 TOE 目的和要求。不必重述 PP 的内容。

c) 如果 ST 声明遵从 PP 的要求，但 PP 需要进一步的限制，那么 ST 应证明限制后的 PP 要求已经满足。发生这种情况的典型是当 PP 含有未完成的操作时。此时，ST 可引用这些特定的要求，并在 ST 中完成相应的操作。在某些情况下，关于完成操作的要求是非常重要的，此时最好在 ST 中重述 PP 的内容，以便描述得更清楚。

d) 如果 ST 声明遵从 PP 的要求，但需要增添更多的目的和要求来扩展 PP，那么 ST 应定义这些增添的内容，尽管 PP 的引用可能已经充分定义了 PP 的目的和要求。在某些情况下，增添是非常重要的，此时最好在 ST 中重述 PP 的内容，以便描述得更清楚。

e) ST 声明部分遵从 PP 的情形是 GB/T 18336 评估不允许的。

在选择重述还是引用 PP 的目的和要求方面，GB/T 18336 不是说明性的。基本要求是 ST 的内容是完备的、清楚的和无歧义的，这样 ST 的评估才是可能的，ST 才是 TOE 评估的可接受的基础，对任何所声明的 PP 可追溯才是清楚的。

如果作出任何 PP 一致性声明，那么对于每一个 PP 声明，其陈述应包括以下内容：

a) **PP 引用**陈述应指出声称与其一致的那个 PP，加上与此相关的任何需要补充的内容。一个有效的声明意味着 TOE 满足该 PP 的所有要求。

b) **PP 裁剪**陈述应指出那些满足许可的 PP 操作或对 PP 要求进一步限制的 IT 安全要求陈述。

c) **PP 增加**陈述应指出那些额外增添了 PP 目的和要求的 TOE 目的和要求陈述。

B.2.9 应用注释

ST 的这个可选部分可包括额外的认为与 ST 相关的或有助于理解 ST 的信息。注意，如果 ST 声明遵从一个 PP 的要求，那么将在一个潜在的 PP 应用注释条款中所包含的某些信息纳入 ST 的另一个条款中是适当的。如，关于 TOE 构建方面的信息可在“TOE 概述”或“ST 基本原理”中提出，比在单独的“应用注释”条款中提出更适合。为了轻松通过 TOE 评估，假定在本附录描述的一个 ST 陈述结构不是标准化的，一个包含评估相关材料的应用注释宜作为 ST 条款的一部分，以便于为评估提供证据。

B.2.10 基本原理

ST 的这部分内容给出了用于 ST 评估的证据。这些证据将支持：ST 是一个完整的、紧密结合的要求集合，遵从该 ST 的 TOE 将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。基本原理也将证明任何 PP 一致性声明都是合理的。基本原理应包括以下几点：

a) **安全目的基本原理**应证明所提出的安全目的可追溯到在 TOE 安全环境里所识别的所有方面，并且正好覆盖所有的这些方面。

b) **安全要求基本原理**应证明该组(TOE 及其环境)安全要求正好满足安全目的且可追溯到安全目的。应证明以下几点：

1) 关于 TOE 及其 IT 安全环境的单个功能和保证要求组件的组合满足所提出的安全目的。

2) 该组安全要求一起构成了一个互相支持且内在一致的整体。

3) 安全要求的选择是合理的。所有下列情况都应当专门论证：

——选择没有包含在 GB/T 18336.2 或 GB/T 18336.3 中的要求；

——选择的保证要求没有包含一个 EAL；

——不满足依赖关系。

4) 为 ST 选择的功能强度级别和任何明确的功能强度声明与符合 TOE 安全目的是一致的。

c) **TOE 概述规范基本原理**应说明 TOE 安全功能和保证尺度都正好满足 TOE 安全要求。应对下列情况进行证实：

1) 所指定 TOE 的 IT 安全功能组合在一起正好满足 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是有效的；

3) 关于所提出的保证措施与保证要求相一致的声明是合理的。

基本原理陈述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 之间的任何区别。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 的这些内容是等同的，这部分内容可以省略。

该潜在的长篇材料，不一定对所有 ST 用户都是适当的或有用的，因此可以单独分发。

参 考 文 献

[1] Bell D E, LaPadula L J. Secure Computer Systems: Unified Exposition and MULTICS Interpretation. Revision 1. US Air Force ESD-TR-75-306, MITRE Corporation MTR-2997, Bedford MA, March 1976.

[2] Biba K J. Integrity Considerations for Secure Computer Systems. ESD-TR-372, ESD/AFSC, Hanscom AFB, Bedford MA., April 1977.

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

[4] Federal Criteria for Information Technology Security. 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.

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

[6] Goguen J A Meseguer J. Unwinding and Inference Control. 1984 Symposium on Security and Privacy, pp. 75-85, IEEE, May 1984.

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

[8] ISO/IEC 7498-2:1989 Information processing systems - Open Systems Interconnection - Basic Reference Model, Part 2: Security Architecture.

[9] ISO/IEC 15292:2001 Information technology - Security techniques - Protection Profile registration procedures.

[10] Trusted Computer Systems Evaluation Criteria. US DoD 5200.28-STD, December 1985.