ICS 35.040
L 80

中华人民共和国国家标准

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

信息技术　安全技术
信息技术安全评估准则
第1部分:简介和一般模型

Information technology—Security techniques—
Evaluation criteria for IT security—
Part 1:Introduction and general model

(ISO/IEC 15408-1:2009,IDT)

2015-05-15 发布　　2016-01-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

GB/T 18336《信息技术　安全技术　信息技术安全评估准则》分为以下3个部分：

——第1部分：简介和一般模型；

——第2部分：安全功能组件；

——第3部分：安全保障组件。

本部分为GB/T 18336的第1部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替GB/T 18336.1—2008《信息技术　安全技术　信息技术安全评估准则　第1部分：简介和一般模型》。

本部分与GB/T 18336.1—2008的主要差异如下：

——增加了“2　规范性引用文件”；

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

——“5　概述”中增加了“5.2　TOE”；

——将GB/T 18336适用的“IT产品和系统”改为“IT产品”；

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

——删除了GB/T 18336.1—2008的“5.3　安全概念”；

——“5.4.1　安全要求的表达”调整为本部分的“7　剪裁安全要求”；

——删除了GB/T 18336.1—2008的“5.4.2　评估类型”；

——增加了“8　保护轮廓和包”；

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

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

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

本部分使用翻译法等同采用国际标准ISO/IEC 15408-1:2009《信息技术　安全技术　信息技术安全评估准则　第1部分：简介和一般模型》。

与本部分中规范性引用的国际文件有一致性对应关系的我国文件如下：

——GB/T 18336.2—2015　信息技术　安全技术　信息技术安全评估准则　第2部分：安全功能组件(ISO/IEC 15408-2:2008,IDT)

——GB/T 18336.3—2015　信息技术　安全技术　信息技术安全评估准则　第3部分：安全保障组件(ISO/IEC 15408-3:2008,IDT)

——GB/T 30270　信息技术　安全技术　信息技术安全性评估方法(GB/T 30270—2013,ISO/IEC 18045:2005,IDT)

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本部分起草单位：中国信息安全测评中心、信息产业信息安全测评中心、公安部第三研究所。

本部分主要起草人：张翀斌、郭颖、石竑松、毕海英、张宝峰、高金萍、王峰、杨永生、李国俊、董晶晶、

谢蒂、王鸿娴、张怡、顾健、邱梓华、宋好好、陈妍、杨元原、贾炜、王宇航、王亚楠。

本部分所代替标准的历次版本发布情况：

——GB/T 18336.1—2001

——GB/T 18336.1—2008

引　言

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

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

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

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

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

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

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

a) ISO/IEC 15408 不包括那些与 IT 安全措施没有直接关联的属于行政性管理安全措施的安全评估准则。但是，应该认识到 TOE 安全的某些重要组成部分可通过诸如组织的、人员的、物理的、程序的控制等行政性管理措施来实现；

b) ISO/IEC 15408 没有明确涵盖电磁辐射控制等 IT 安全中技术性物理方面的评估，虽然标准中的许多概念适用于该领域。换句话说，ISO/IEC 15408 只涉及 TOE 物理保护的某些方面；

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

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

e) 评估结果用于产品认可的程序不属于 ISO/IEC 15408 的范围。产品的认可是行政性的管理过程，据此准许 IT 产品在其整个运行环境中投入使用。评估侧重于产品的 IT 安全部分，以及直接影响到 IT 单元安全使用的那些运行环境，因此，评估结果是认可过程的重要输入。但是，由于其他技术更适合于评估非 IT 相关属性以及其与 IT 安全部分的关系，认可者应针对这些情况分别制定不同的条款；

f) ISO/IEC 15408 不包括评价密码算法固有质量相关的标准条款。如果需要对嵌入 TOE 的密码算法的数学特性进行独立评估，则必须在使用 ISO/IEC 15408 的评估体制中为相关评估制定专门条款。

信息技术　安全技术
信息技术安全评估准则
第1部分:简介和一般模型

1　范围

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

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

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

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

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

ISO/IEC 15408-2　信息技术　安全技术　信息技术安全评估准则　第2部分:安全功能组件(Information technology—Security techniques—Evaluation criteria for IT security—Part 2:Security functional components)

ISO/IEC 15408-3　信息技术　安全技术　信息技术安全评估准则　第3部分:安全保障组件(Information technology—Security techniques—Evaluation criteria for IT security—Part 3:Security assurance components)

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

3　术语和定义

下列术语和定义适用于本文件。

注:本章只收录在ISO/IEC 15408中有特殊用法的术语。在ISO/IEC 15408中使用的但本章没有收录的一些由通用术语组合成的复合词,将在使用它们的地方进行解释。

3.1　常用术语和定义

3.1.1

敌对行为　adverse actions

由威胁主体对资产执行的行为。

3.1.2

资产 assets

评估对象(TOE)所有者赋予了价值的实体。

3.1.3

赋值 assignment

对组件或要求中指定的参数进行具体说明。

3.1.4

保障 assurance

TOE 满足安全功能要求(SFR)的信任基础。

3.1.5

攻击潜力 attack potential

对攻击 TOE 所需耗费努力的度量,以攻击者的专业水平、耗费资源和攻击动机来表示。

3.1.6

增强 augmentation

向包中增加一个或多个要求。

3.1.7

鉴别数据 authentication data

用于验证用户所声称身份的信息。

3.1.8

授权用户 authorized user

根据安全功能要求可以执行某项操作的 TOE 用户。

3.1.9

类 class

具有共同目的族的集合。

3.1.10

连贯的 coherent

有逻辑顺序、且含义清晰。

注:对于文档,本术语是指目标读者是否易于理解文档的文字内容和文档结构。

3.1.11

完备的 complete

一个实体的所有必要部分均已被提供的性质。

注:对文档而言,指所有相关信息都已包含在该文档中,且足够详细,不需要在该抽象层次上再做进一步解释。

3.1.12

组件 component

体现安全要求的最小可选元素的集合。

3.1.13

组合保障包 composed assurance package

从 ISO/IEC 15408-3 抽取的要求所组成的保障包(由 ACO“组合”类控制),代表 ISO/IEC 15408 预先定义的某一组合保障尺度上的一个点。

3.1.14

确认 confirm

声明通过独立地确定充分性,已对某事项进行了详细的审核。

注:所需要的严格程度依赖于事项的本质特征。这个术语仅用于评估者行为。

3.1.15

连通性 connectivity

TOE 与其之外的 IT 实体进行交互的 TOE 属性。

注：这包括在任何环境或配置下，以任意距离，通过有线或无线方式进行的数据交换。

3.1.16

一致的 consistent

两个或者更多实体之间的关系不存在明显的矛盾。

3.1.17

对抗(动词) counter(verb)

应对攻击，以缓解特定威胁造成的影响，但未必消除。

3.1.18

可论证的符合性 demonstrable conformance

某个 ST 和 PP 之间的关系，其中该 ST 提供了一种解决该 PP 中一般安全问题的解决方案。

注：PP 和 ST 在讨论不同的实体以及使用不同的概念等情况时，可以采用完全不同的论述方式。可论证的符合性也适用于描述一种已存在多个类似 PP 的 TOE 类型，因此允许 ST 作者申明同时符合这些 PP，从而节省工作量。

3.1.19

证实 demonstrate

得出一个由分析获得的结论，它不如“证明”那样严格。

3.1.20

依赖关系 dependency

组件之间的一种关系，如果一个基于依赖组件的要求包含在 PP、ST 或包中，那么一个基于被依赖组件的要求一般也应包含在 PP、ST 或包中。

3.1.21

描述 describe

提供一个实体的具体细节。

3.1.22

确定 determine

通过独立分析来肯定一个特定的结论，该分析以达成一个特定的结论为目的。

注：本术语通常用于缺少前期分析的情况，意味着需要开展真正独立的分析。这与术语“确认”或“验证”不同，后者意味着前期已进行了分析，需要对这些分析进行审查。

3.1.23

开发环境 development environment

开发 TOE 的环境。

3.1.24

元素 element

一个安全需求的不可再分的陈述。

3.1.25

确保 ensure

保证在行为及其结果之间存在牢固的因果关系。

注：当这个术语之前冠以“帮助”一词时，表明仅仅基于该行为仍无法完全确定结果。

3.1.26

评估 evaluation

依据定义的准则对 PP、ST 或 TOE 进行的评价。

3.1.27

评估保障级 evaluation assurance level

从 ISO/IEC 15408-3 中提取的一个保障要求的集合，它构成了一个保障包，代表了 ISO/IEC 15408 预定义的保障尺度中的一个点。

3.1.28

评估授权机构 evaluation authority

为特定群体中的团体开展评估工作进行标准制定和质量监督的组织，该组织依据评估体制来实施 ISO/IEC 15408。

3.1.29

评估体制 evaluation scheme

一种行政管理和监督管理框架，在此框架下评估授权机构在特定群体中应用 ISO/IEC 15408。

3.1.30

彻底的 exhaustive

一个条理清楚的方法所具有的特征，该方法按照明确的计划来执行分析或开展活动。

注：在 ISO/IEC 15408 中，该术语在谈及执行分析和其他活动时使用。它与“系统性的”有关，但更强，不仅表明根据明确的计划采取系统性的方法执行分析或活动，而且所遵循的计划足以保证所有可能的途径都经过了实践。

3.1.31

解释 explain

对采取一系列行为的原因给出论据。

注：这个术语不同于“描述”和“证实”。它的意图是回答“为什么?”，并未尝试辩论所采取的行为一定是最优的。

3.1.32

扩展 extension

把不包括在 ISO/IEC 15408-2 中的功能要求或 ISO/IEC 15408-3 中的保障要求增加到 ST 或 PP 中。

3.1.33

外部实体 external entity

在 TOE 边界之外可能与 TOE 交互的人或 IT 实体。

注：外部实体也可以被称为用户。

3.1.34

族 family

具有相似目标，但在侧重点或严格程度上不同的组件的集合。

3.1.35

形式化 formal

以一种受限语法的语言表达，该语言建立公认的数学概念上，具有确定的语义。

3.1.36

指导性文档 guidance documentation

描述交付、准备、运行、管理和/或使用 TOE 的文档。

3.1.37

身份 identity

在 TOE 中唯一标识实体的表示（比如一个用户、进程或磁盘）。

注：这种表示的例子如：一个字符串。对于人类用户，这种表示可以是全名、缩写名或（仍唯一的）假名。

3.1.38

非形式化 informal

采用自然语言表达。

3.1.39

TSF 间传送 inter TSF transfers

在 TOE 和其他可信 IT 产品的安全功能之间交换数据。

3.1.40

内部通信信道 internal communication channel

TOE 各分离部分间的通信信道。

3.1.41

TOE 内部传送 internal TOE transfer

在 TOE 各分离部分之间交换数据。

3.1.42

内在一致的 internally consistent

一个实体的各个方面之间不存在明显的矛盾。

注：对于文档来说，是指文档内部没有发生相互矛盾的陈述。

3.1.43

反复 iteration

使用同一组件表达两个或多个要求。

3.1.44

论证 justification

分析以得出一个结论。

注："论证"比"证实"更严格，从需要非常仔细、全面地解释逻辑论证的每一步来说，这个术语要求十分严格。

3.1.45

客体 object

TOE 中被动的实体，包含或接收信息，并由主体对其执行操作。

3.1.46

操作(组件) operation(on a component)

一个组件的修改或重复。

注：对组件允许的操作有赋值、反复、细化和选择。

3.1.47

操作(客体) operation(on an object)

主体对客体执行的特定类型的行为。

3.1.48

运行环境 operational environment

运行 TOE 的环境。

3.1.49

组织安全策略 organizational security policies

一个组织的安全规则、规程或指南的集合。

注：一个策略可能与一个具体的运行环境相关。

3.1.50

包 package

安全功能要求或安全保障要求的一个命名集合。

注：例如 EAL3 是一个包。

3.1.51

保护轮廓 protection profile;PP

针对一类 TOE 的、与实现无关的安全需求陈述。

3.1.52

保护轮廓评估 protection profile evaluation

依据已定义的准则，对一个 PP 进行的评价。

3.1.53

证明 prove

通过数学意义上的形式化分析来说明对应关系。

注：本术语在各个方面都是非常严格的。通常情况下，当期望以一种高度严格的方式说明两个 TOE 安全功能(TSF)表示之间的对应关系时，才使用“证明”这一术语。

3.1.54

细化 refinement

为组件添加细节。

3.1.55

角色 role

为了规定在一个用户和该 TOE 之间所允许的交互行为而预定义的规则集。

3.1.56

秘密 secret

为了执行一个特定的安全功能策略(SFP)，必须仅由授权用户和/或 TSF 才可知晓的信息。

3.1.57

安全状态 secure state

一种状态，在该状态下，TSF 数据一致，且 TSF 能继续正确执行 SFR。

3.1.58

安全属性 security attribute

主体、用户(包括外部 IT 产品)、客体、信息、会话和/或资源的特征，它用于定义 SFR，且其值在执行 SFR 时使用。

3.1.59

安全功能策略 security function policy;SFP

描述由 TSF 执行的特定安全行为的规则集，可表示为 SFR 的集合。

3.1.60

安全目的 security objective

意在对抗特定的威胁、和/或满足特定的组织安全策略和/或假设的一种陈述。

3.1.61

安全问题 security problem

以一种正式的方式，定义 TOE 要处理的安全基本特征和范围的陈述。

注：该陈述由以下部分组成：

- 要由 TOE 对抗的威胁；
- 要由 TOE 实施的组织安全策略(OSP)；
- 支撑 TOE 及其运行环境的假设。

3.1.62

安全要求 security requirement

用标准化的语言陈述的要求，旨在达到 TOE 的安全目的。

3.1.63

安全目标 security target;ST

针对一个特定的已标识 TOE，且与实现相关的安全需求陈述。

3.1.64

选择 selection

从组件内列表中指定一项或多项。

3.1.65

半形式化 semiformal

采用具有确定语义并有严格语法的语言表达。

3.1.66

详细说明 specify

以严格精确的方式给出实体的特定细节。

3.1.67

严格符合性 strict conformance

一个 PP 和一个 ST 之间的一种层次关系，其中该 PP 中的所有要求也存在于该 ST 中。

注：这种关系可以粗略地定义为“ST 应包含 PP 中所有的陈述，但也可以包含更多的内容”。严格符合性预期用于描述那些需要以单一方式遵守的严格要求。

3.1.68

ST 评估 ST evaluation

依据已定义的准则，对一个 ST 进行的评价。

3.1.69

主体 subject

TOE 中对客体执行操作的主动实体。

3.1.70

评估对象 target of evaluation；TOE

软件、固件和/或硬件的集合，可能附带指南。

3.1.71

威胁主体 threat agent

可以对资产施加不利行为的实体。

3.1.72

TOE 评估 TOE evaluation

依据已定义的准则，对一个 TOE 进行的评价。

3.1.73

TOE 资源 TOE resource

TOE 中任何可用或可消耗的事物。

3.1.74

TOE 安全功能 TOE security functionality

正确执行 SFR 所依赖的 TOE 的所有硬件、软件和固件的组合功能。

3.1.75

追溯 trace

在两个实体之间，执行一种最低严格程度的非形式化对应分析。

3.1.76

TOE 的外部传送 transfers outside of the TOE

由 TSF 促成的、与不受 TSF 控制的实体的数据通信。

3.1.77

转化 translation

用标准化语言描述安全要求的过程。

注：在这种情况下，术语“转化”表示的不是字面意思，使用该术语也不意味着每个用标准化语言描述的 SFR 都能够回译为安全目的。

3.1.78

可信信道 trusted channel

一种通信手段，通过该手段，TSF 同另一个可信 IT 产品能够在必要的信任基础上进行通信。

3.1.79

可信 IT 产品 trusted IT product

不是该 TOE 的其他 IT 产品，它有与该 TOE 协调管理的安全功能要求，且假定其可正确执行自己的安全功能要求。

注：一个可信 IT 产品例子，如一个经过独立评估后的产品。

3.1.80

可信路径 trusted path

一种通信手段，通过该手段，用户和 TSF 能够在必要的信任基础上进行通信。

3.1.81

TSF 数据 TSF data

TOE 执行其 SFR 所依赖的数据。

3.1.82

TSF 接口 TSF interface

外部实体(或在 TOE 中但在 TSF 之外的主体)向 TSF 提供数据、从 TSF 接收数据、并调用 TSF 服务的方法。

3.1.83

用户数据 user data

属于用户的、不影响 TSF 运行的数据。

3.1.84

验证 verify

通过严格细致地审查，独立地确定充分性。

注：参见术语“确认”，本术语有更严格的含义。这个术语用于描述评估者行为的语境中，其中要求评估者独立工作。

3.2 与开发(ADV)类相关的术语和定义

注：下列术语用于软件内部结构化要求。其中一些来自 IEEE Std 610.12—1990 IEEE Std 610.12—1990, Standard glossary of software engineering terminology, Institute of Electrical and Electronics Engineers。

3.2.1

管理员 administrator

就遵守由 TSF 实现的所有策略而言，在一定程度上可信的实体。

注：并非所有 PP 或 ST 都对管理员设定相同的可信程度。通常假定管理员始终遵循 TOE 的 ST 中描述的策略。其中，有些策略可能与 TOE 的功能有关，另一些可能与运行环境有关。

3.2.2

调用树 call tree

以图表形式标识系统中的模块，并表明模块之间的相互调用关系。

注：采自 IEEE Std 610.12—1990。

3.2.3

内聚 cohesion

模块强度

单个软件模块所执行的诸任务之间的关联方式和程度。

[IEEE Std 610.12—1990]

注：内聚的类型包括偶然的、通信的、功能的、逻辑的、顺序的和暂时的，这些内聚类型在相关条目中描述。

3.2.4

偶然内聚 coincidental cohesion

该类型模块执行的活动之间具有无关或关系松散的特征。

[IEEE Std 610.12—1990]

注：见“内聚”(3.2.3)。

3.2.5

通信内聚 communicational cohesion

该类型模块包含如下功能：为该模块内其他功能产生输出、或使用该模块其他功能的输出。

[IEEE Std 610.12—1990]

注1：见“内聚”(3.2.3)。

注2：通信内聚模块的一个实例如一个包含强制性的、无限制的以及带约束条件的访问验证模块。

3.2.6

复杂度 complexity

理解软件，以致分析、测试和维护软件的困难程度的一种度量方式。

[IEEE Std 610.12—1990]

注：采用模块分解、层次化和最小化的最终目的是降低复杂度。控制耦合和内聚对这一目标有重要作用。

软件工程领域在发展源代码复杂度的度量方法方面已付出了很多努力。其中大多数度量方法使用易于计算的源代码属性，如操作符和操作数的数量、控制流图的复杂度(循环复杂度)、源代码行数、可执行代码注释比率，以及类似度量，编码标准被认为是生成更易于理解的代码的有用工具。

TSF内部(ADV_INT)族要求对所有组件的复杂度进行分析。该族期望开发者为已经充分降低了复杂度的声明提供证据支持，这可能包括开发者的编程标准，以及表明所有模块均满足标准(或一些经过软件工程论点论证合理的例外情况)的论据。它可能包括用于度量某些源代码属性的工具的结果，也可能包括开发者认为适用的其他支持。

3.2.7

耦合 coupling

软件模块之间相互依赖的方式和程度。

[IEEE Std 610.12—1990]

注：耦合类型包括调用、公共和内容耦合。

3.2.8

调用耦合 call coupling

两个模块之间严格地按照已记录的函数调用方式进行通信的关系。

注：调用耦合的实例有数据、标识和控制。

3.2.9

调用耦合(数据) call coupling(data)

两个模块之间严格地使用代表单个数据项的调用参数进行通信的关系。

注：见“调用耦合”(3.2.8)。

3.2.10

调用耦合(标记) call coupling(stamp)

两个模块之间使用包括有多个域，或内部结构有意义的调用参数进行通信的关系。

注：见“调用耦合”(3.2.8)。

3.2.11

调用耦合(控制) call coupling(control)

两个模块之间的一种关系，其中一个模块传输信息给另一个模块，意于影响其内部逻辑。

注：见“调用耦合”(3.2.8)。

3.2.12

公共耦合 common coupling

两个模块之间共享公共数据区或其他公共系统资源的关系。

注：全局变量表明使用全局变量的模块是公共耦合的。一般允许通过全局变量公共耦合，但要有限度。

例如，只被一个模块使用的变量放在全局区域是不合适的，应该移除。在评估全局变量的适宜性中需要考虑的其他因素有：

a) 修改一个全局变量的模块个数：一般来说，应该只分配一个模块负责控制全局变量的内容，但可以由第二个模块共同承担该职责，在这种情况下，必须提供充分的论证。多于两个模块共同承担该职责是不能接受的。（在评估中，应该谨慎确定哪个模块对变量内容负实际职责，例如，如果变量由单一程序修改，但该程序仅仅执行其调用者请求的修改，这是调用模块的职责，可以有多个这样的模块）。此外，在复杂度度量方面，如果两个模块共同负责一个全局变量的内容，应清楚地说明它们之间是如何协调修改的。

b) 引用全局变量的模块个数：虽然一般对引用全局变量的模块个数没有限制，多个模块引用的情况中应检查引用的有效性和必要性。

3.2.13

内容耦合 content coupling

两个模块之间的一种关系，其中一个模块直接引用另一个模块的内部。

注：例子包括修改其他模块的代码或者引用其他模块内部的标签。结果是一个模块的部分或所有内容有效的包含在另一个模块中。可将内容耦合理解为使用了未公开模块接口，而在调用耦合中，仅仅使用了公开的模块接口。

3.2.14

域分离 domain separation

安全结构属性，TSF 由此为每个用户和 TSF 定义了分离的安全域，保证没有用户进程可以影响其他用户或 TSF 的安全域的内容。

3.2.15

功能内聚 functional cohesion

执行与单一目的相关活动的模块的功能属性。

[IEEE Std 610.12—1990]

注：功能内聚模块将一种类型的输入转换为一种类型的输出，如堆栈管理器或队列管理器。见“内聚”(3.2.3)。

3.2.16

交互 interaction

实体间一般性的通信活动。

3.2.17

接口 interface

组件或模块交互的方式。

3.2.18

分层 layering

设计技术，将各组模块分层组织，使其职责分离，以便在层级中的某层仅仅依赖于其下层的服务，且仅向其上层提供服务。

注：严格分层增加了限制，每层只能从其邻接下层接收服务，只能向其邻接上层提供服务。

3.2.19

逻辑内聚 logical cohesion

程序内聚 procedural cohesion

表示模块对不同数据结构执行类似活动的特征。

注：当模块功能对于不同的输入执行相关的、但又不同的操作，表现为逻辑内聚。见“内聚”(3.2.3)。

3.2.20

模块分解 modular decomposition

将系统拆分成若干模块，以便于设计、开发和评估的过程。

[IEEE Std 610.12—1990]

3.2.21

(TSF 的)不可旁路性 non- bypassability(of the TSF)

安全结构属性，由此所有安全功能要求相关的行为可由 TSF 协调。

3.2.22

安全域 security domain

活动实体拥有访问权限的资源集合。

3.2.23

顺序内聚 sequential cohesion

此类型模块中所包含的每一个功能的输出是其后续功能的输入。

[IEEE Std 610.12—1990]

注：顺序内聚模块的一个例子是包含写审计记录和维护特定类型审计侵害的持续累积计数功能的模块。

3.2.24

软件工程 software engineering

应用系统的、有规则的、可计量的方法于软件开发和维护过程，即工程学在软件上的应用。

[IEEE Std 610.12—1990]

注：通常在工程实践中，应用工程学原理时必须使用一定量的判断。许多因素影响选择，不仅是模块分解、分层和最小化方法的应用。例如，开发者可能在头脑中设计一个尚未实现的未来应用系统。该开发者可以选择包括某些逻辑去管理这些没有完全实现的未来应用，此外，开发者可以包含对尚未实现的模块的某些调用，留给调用桩模块。开发者论证这种与有良好结构程序的偏移，必须通过使用判定以及良好的软件工程学原理的应用来评估。

3.2.25

暂时内聚 temporal cohesion

包含着需要几乎同时执行的功能的模块的特征。

注 1：源自[IEEE Std 610.12—1990]。

注 2：暂时内聚模块的例子如初始化、恢复和关机模块。

3.2.26

TSF 自保护 TSF self-protection

TSF 不能被非 TSF 代码或实体破坏的安全结构属性。

3.3 与指导性文档(AGD)类相关的术语和定义

3.3.1

安装 installation

由人类用户将 TOE 嵌入其运行环境中，并使其进入运行状态的规程。

注：这个操作一般在接收和确认 TOE 后仅执行一次，预期使 TOE 进入到 ST 允许的配置。如果必须由开发者执行相似的过程，则在 ALC:生命周期支持中注明为“生成”，如果 TOE 不需要定期重复执行初始启动，则这个过程归为安装。

3.3.2

运行 operation

TOE 的使用阶段，包括 TOE 交付和准备之后的“正常使用”、管理和维护。

3.3.3

准备 preparation

产品生命周期阶段中的活动，由所交付的 TOE 的客户确认及 TOE 安装组成，可能包括引导、初始化、启动 TOE 并使其进入到准备运行的状态。

3.4 与生命周期支持(ALC)类相关的术语和定义

3.4.1

接受准则 acceptance criteria

执行接受规程时使用的准则(如对软件、固件或硬件的成功的文档审查，或成功的测试)。

3.4.2

接受规程 acceptance procedures

为了接受新建、修改过的作为 TOE 组成部分的配置项，或者将其转到生命周期的下一阶段应遵循的规程。

注：这些规程明确了负责接受的角色或个人，以及为了做出接受决定所采用的准则。

下面是几种接受情形，其中一些可能有交叉：

a) 某个配置项第一次被配置管理系统接受，特别是接受来自于其他厂商的包含软件、固件和硬件的部件进入 TOE(“集成”)；

b) 在构造 TOE 的每个阶段，配置项转入下一个生命周期阶段(例如模块、子系统、完成的 TOE 的质量控制)；

c) 不同开发地点的配置项后续传递(例如 TOE 的各部分或初始产品)；

d) 面向消费者的 TOE 后期交付。

3.4.3

配置管理 configuration management;CM

应用技术、管理方法及监督的规则，标识并文档化配置项的功能和物理特性，控制特性的变更，记录并报告变更过程及执行状态，验证与规定要求的一致性。

注：采自 IEEE Std 610.12。

3.4.4

CM 文档 CM documentation

所有 CM 文档，包括 CM 输出、CM 清单(配置项清单)、CM 系统记录、CM 计划和 CM 使用文档。

3.4.5

配置管理证据 configuration management evidence

可用于确认 CM 系统正确运行的任何事物。

注：如，CM 输出、开发者提供的基本原理、评估者现场核查期间所做的观察、实验或访谈。

3.4.6

配置项 configuration item

TOE 开发期间 CM 系统管理的对象。

注：可能是 TOE 的一部分，或者与 TOE 开发相关的对象，如评估文档或开发工具。配置项及其版本号可以直接(如文件)或者通过引用名(如硬件部件)的方式存储在 CM 系统中。

3.4.7

配置清单 configuration list

配置管理输出文档为特定产品列出所有配置项，及与该完整产品特定版本相关的每个配置管理项的正确版本。

注：该清单允许区分属于产品已评估版本的配置项和该产品其他版本的配置项。最终的配置管理清单是特定产品的特定版本的特定文档。(当然，清单可能是配置管理工具中的电子文档，在这种情况下，它可以看成系统或系统一部分的特定视图而不是系统输出。然而在评估实践中，配置清单可能作为评估文档的一部分交付)。配置清单定义了配置管理要求 ALC_CMC 的配置项。

3.4.8

配置管理输出 configuration management output

配置管理系统产生或实施的、与配置管理相关的结果。

注：这些配置管理相关结果可能表现为文档形式(如，填写的纸质表格、配置管理系统记录、日志数据、纸质和电子输出数据)和行为(如执行配置管理规定的人工措施)。这样的配置管理输出的例子是配置清单、配置管理计划和/或产品生命周期中的行为。

3.4.9

配置管理计划 configuration management plan

配置管理系统如何服务于 TOE 的描述。

注：发布配置管理计划的目的是使员工能够清楚的明白他们的职责。从整个配置管理系统的角度，配置管理计划可以看做是一个输出文档(因为它可能作为配置管理系统的应用的部分而产生)。从具体项目的角度，可以将它看成是使用文档，因为项目组成员使用它，以便理解在项目期间必须执行的步骤。配置管理计划为特定产品定义了系统的使用方法，对于其他产品，同一系统使用程度可能不尽相同。这意味着配置管理计划定义并描述了公司在 TOE 开发期间使用的配置管理系统的输出。

3.4.10

配置管理系统 configuration management system

开发者在产品生命周期期间，用于开发并维护产品配置的规程和工具(包括说明文档)的集合。

注：配置管理系统可能具有不同的严格程度和功能，高级别的配置管理系统可能是自动化的、具有缺陷修复、变更控制、以及其他跟踪机制。

3.4.11

配置管理系统记录 configuration management records

配置管理系统对重要的配置管理活动进行文档化期间产生的输出。

注：配置管理系统记录的例子是配置管理项变更控制表单，或者配置管理项访问许可表。

3.4.12

配置管理工具 configuration management tools

实现或支持配置管理系统的手动操作或者自动化的工具。

注：例如，TOE 组成部分的版本管理工具。

3.4.13

配置管理使用文档 configuration management usage documentation

配置管理系统的组成部分，描述了配置管理系统是如何定义和使用的，例如使用手册、规则、工具和规程文档。

3.4.14

交付 delivery

已完成的 TOE 从生产环境传送到客户手中。

注：产品生命周期的这个阶段可能包括开发场所的包装和存储，但是不包括未完成的 TOE 或部分 TOE 在不同开发者或不同开发场所之间的传递。

3.4.15

开发者 developer

负责 TOE 研发的组织。

3.4.16

开发 development

与生成 TOE 实现表示有关的产品生命周期阶段。

注：在整个生命周期支持要求中，开发及其相关术语(开发者、开发)，包括更一般意义上的开发和生产。

3.4.17

开发工具　development tools

支撑 TOE 的开发和生产的工具(如果适用,包括测试软件)。

注:例如,对于一个软件 TOE,开发工具通常有编程语言、编译器、连接器和生成工具。

3.4.18

实现表示　implementation representation

不需要进一步的设计细化,即可创建 TSF 本身的 TSF 最小抽象表示。

注:源代码,或者用于生成实际硬件的硬件设计图都是实现表示的例子。

3.4.19

生命周期　life-cycle

在时间上,一个对象(例如,一个产品或系统)存在的各个阶段。

3.4.20

生命周期定义　life-cycle definition

生命周期模型的定义。

3.4.21

生命周期模型　life-cycle model

描述用于某一对象生命周期管理的阶段及其相互关系、阶段序列及其高层特征。

3.4.22

生产　production

紧跟开发阶段之后的生产生命周期阶段,包含由实现表示转化为 TOE 实现的过程,即进入可交付给客户的状态。

注 1:这个阶段可能包括 TOE 的制造、集成、生成、内部传递、存储、以及标识。

注 2:见图 1。

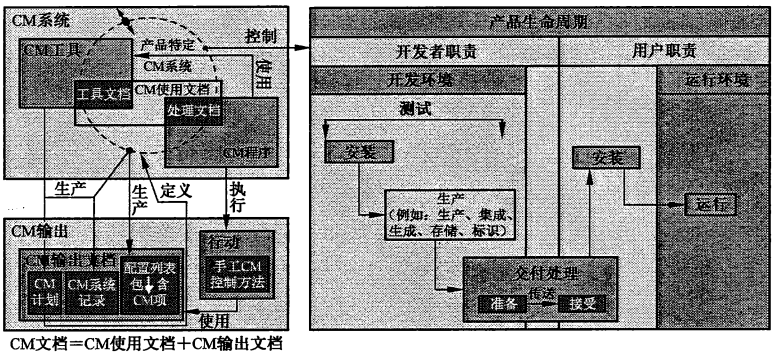

图 1　CM 和产品生命周期术语

3.5　与脆弱性评定(AVA)类相关的术语和定义

3.5.1

隐蔽信道　covert channel

强迫性的非法信道,允许用户暗中违反多级隔离策略和 TOE 的不可观察性要求。

3.5.2

已识别的潜在脆弱性　encountered potential vulnerabilities

由评估者执行评估活动时识别的 TOE 潜在弱点,可以被用于违反 SFR。

3.5.3

可利用的脆弱性 exploitable vulnerability

可以在TOE运行环境中用来违反SFR的TOE弱点。

3.5.4

监视攻击 monitoring attacks

一类攻击方法的通称，包括被动分析技术，其目的是通过按指导性文档要求的方式运行TOE，旨在泄露TOE的内部敏感数据。

3.5.5

潜在脆弱性 potential vulnerability

可疑的，但尚未确认的弱点。

注：怀疑的过程是借助于一个假设的违反SFR的攻击路径来进行的。

3.5.6

残余脆弱性 residual vulnerability

在TOE运行环境中不能被利用的弱点，但是可能被TOE运行环境中具有比预期更大攻击潜力的攻击者用于违反SFR。

3.5.7

脆弱性 vulnerability

可以在某些环境中用于违反SFR的TOE弱点。

3.6 与组合(ACO)类相关的术语和定义

3.6.1

基础部件 base component

组合TOE中的实体，其本身已是一个评估主体，为依赖部件提供了服务和资源。

3.6.2

兼容(部件) compatible(components)

在相容的运行环境中，通过每个部件的对应接口，能够提供其他部件所需要的服务的部件属性。

3.6.3

部件TOE component TOE

成功评估过的TOE，本身又作为另一个组合TOE一部分。

3.6.4

组合TOE composed TOE

完全由两个或多个已通过评估的部件组成的TOE。

3.6.5

依赖部件 dependent component

组合TOE中的实体，其本身是一个评估主体，依赖于基础部件提供的服务。

3.6.6

功能接口 functional interface

提供用户访问TOE功能的外部接口，其本身未直接参与安全功能要求的实施。

注：在组合TOE中，指依赖部件所要求的、用于支撑组合TOE运行的、基础部件提供的接口。

4 缩略语

下列缩略语适用于本文件。

API:应用编程接口(Application Programming Interface)
CAP:复合保障包(Composed Assurance Package)
CM:配置管理(Configuration Management)
DAC:自主访问控制(Discretionary Access Control)
EAL:评估保障级(Evaluation Assurance Level)
GHz:千兆赫兹(Gigahertz)
GUI:用户图形界面(Graphical User Interface)
IC:集成电路(Integrated Circuit)
IOCTL:输入输出控制(Input Output Control)
IP:互联网协议(Internet Protocol)
IT:信息技术(Information Technology)
MB:兆字节(Mega Byte)
OS:操作系统(Operating System)
OSP:组织安全策略(Organisational Security Policy)
PC:个人计算机(Personal Computer)
PCI:外设部件互连(Peripheral Component Interconnect)
PKI:公钥基础设施(Public Key Infrastructure)
PP:保护轮廓(Protection Profile)
RAM:随机存取存储器(Random Access Memory)
RPC:远程过程调用(Remote Procedure Call)
SAR:安全保障要求(Security Assurance Requirement)
SFR:安全功能要求(Security Functional Requirement)
SFP:安全功能策略(Security Function Policy)
SPD:安全问题定义(Security Problem Definition)
ST:安全目标(Security Target)
TCP:传输控制协议(Transmission Control Protocol)
TOE:评估对象(Target of Evaluation)
TSF:TOE 安全功能(TOE Security Functionality)
TSFI:TSF 接口(TSF Interface)
VPN:虚拟专用网络(Virtual Private Network)

5 概述

5.1 综述

本章介绍 ISO/IEC 15408 的主要概念,明确“TOE”的概念、目标读者,以及论述 ISO/IEC 15408 其余部分内容将采取的方法。

5.2 TOE

ISO/IEC 15408 在评估的对象上定义较灵活,未局限于公共理解的 IT 产品范围,因此在评估中,ISO/IEC 15408 使用术语“TOE”。

TOE 被定义为一组可能包含指南的软件、固件和/或硬件的集合。

尽管 TOE 在某些情况下由一个 IT 产品组成,但也不总是这样。TOE 可以是一个 IT 产品、一个 IT 产品的一部分、一组 IT 产品、一种不可能形成产品的独特技术,或者以上这些情况的组合。

对于 ISO/IEC 15408 而言，TOE 和所有 IT 产品之间的确切关系在以下方面非常重要：对 TOE 只包含 IT 产品某部分的评估不应该与对整个 IT 产品的评估相混淆。

TOE 的例子包括：

- 软件应用；
- 操作系统；
- 与操作系统组合在一起的软件应用；
- 与操作系统和工作站组合在一起的软件应用；
- 与工作站组合在一起的操作系统；
- 智能卡集成电路；
- 智能卡集成电路的密码协处理器；
- 包括所有终端、服务器、网络设备和软件的局域网；
- 数据库应用，但不包括与数据库应用正常关联的远程客户端软件。

5.2.1 TOE 的不同表示

在 ISO/IEC 15408 中，TOE 可以以几种形式出现，如(对软件 TOE 来说)：

- 配置管理系统中的文件列表；
- 编译过的单一主拷贝；
- 准备交付给客户的光盘和手册；
- 已经安装和运行的版本。

所有这些都可看作是一个 TOE；无论术语“TOE”用在 ISO/IEC 15408 其余部分的何处，可根据上下文来确定其含义。

5.2.2 TOE 的不同配置

一般来说，IT 产品可以用多种方法配置：以不同的方法安装、使用不同的启用或禁用选项。由于在 ISO/IEC 15408 评估期间，它将确定 TOE 是否满足特定的要求，这种配置上的灵活性可能会导致很多问题，因为 TOE 所有可能的配置必须满足要求。出于这些原因，通常在 TOE 的指南部分对 TOE 可能的配置进行严格限制；也就是说，TOE 的指南可能会不同于 IT 产品的通用指南。

操作系统产品就是这样一个例子。这种产品可以用多种方法进行配置(如，用户类型、用户数、允许/禁止的外部连接类型、启用/禁用的选项等)。

如果同一款 IT 产品要成为一个 TOE，并且依据一组合理的要求评估，则配置应该受到更加严密的控制，因为许多选项(如允许所有类型的外部连接或系统管理员不需要被鉴别)将导致 TOE 不满足要求。

出于这种原因，IT 产品指南(允许多种配置)和 TOE 的指南(仅允许一种配置或者在安全相关方面没有不同的配置)通常有所不同。

注意，如果 TOE 指南仍然允许多种配置，这些配置统称为“TOE”，其中的每种配置必须满足 TOE 的指定要求。

5.3 目标读者

有三类群体对 TOE 安全评估感兴趣：消费者、开发者和评估者。ISO/IEC 15408-1 在结构上已支持了这三类群体的需求。他们都被认为是 ISO/IEC 15408 的主要用户。这三类群体都能从下列章条所述标准中受益。

5.3.1 消费者

编制 ISO/IEC 15408 是确保评估满足消费者的需求，因为这是评估过程的基本目的和理由。

消费者可以使用评估结果来帮助决定一个 TOE 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指导的结果。消费者也可以用这些评估结果来比较不同的 TOE。

ISO/IEC 15408 为消费者，尤其是消费者群体和行业团体，提供一个独立于实现的结构，即保护轮廓(PP)，在其中以一种明确的方式表达他们的安全要求。

5.3.2 开发者

ISO/IEC 15408 为开发者准备并协助对其 TOE 的评估，以及标识由 TOE 满足的安全要求提供支持，这些安全要求包含在一个与实现相关的 ST 中。ST 可以基于一个或多个 PP，来说明 ST 符合消费者在这些 PP 中制定的安全要求。

ISO/IEC 15408 其次用于确定责任和行为，以便于提供 TOE 满足安全要求的必要证据。它也定义了证据的内容和形式。

5.3.3 评估者

ISO/IEC 15408 包含了评估者用于评判 TOE 与其安全要求是否符合的准则。ISO/IEC 15408 描述了一组由评估者执行的通用行为。值得注意的是 ISO/IEC 15408 没有详细说明执行这些行动应遵守的规程。这些规程的更多信息见 5.4。

5.3.4 其他

虽然 ISO/IEC 15408 主要是为了规范和评估 TOE 的 IT 安全特性，但它也可以作为对 IT 安全有兴趣或有责任的团体的参考资料。其他能够从 ISO/IEC 15408 所包含的信息中获益的团体有：

a) 系统管理者和系统安全管理者：负责确定和满足该组织的 IT 安全策略和要求。
b) 内部和外部审计员：负责评定 IT 解决方案(可以包含或由一个 TOE 组成)的安全性是否足够。
c) 安全规划和设计师：负责规范 IT 产品的安全特性。
d) 批准者：负责批准在特定环境中使用某 IT 解决方案。
e) 评估发起者：负责申请和支持一个评估。
f) 评估授权机构：负责管理和监督 IT 安全评估程序。

5.4 不同部分

ISO/IEC 15408 由下列独立且又相互关联的部分组成。这些部分描述中所用的术语在第 6 章解释。

a) **第 1 部分：简介和一般模型**，是 ISO/IEC 15408 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。
b) **第 2 部分：安全功能组件**，建立一套功能组件作为标准模板，TOE 的功能要求基于这些模板来建立。第 2 部分列出了一系列功能组件，并按类和族的方式进行组织分类。
c) **第 3 部分：安全保障组件**，建立一套保障组件作为标准模板，TOE 的保障要求基于这些模板来建立。第 3 部分列出了一套保障组件，并按类和族的方式进行组织分类。第 3 部分也定义了 PP 和 ST 的评估准则，并提出了七个预定义的保障包，称为评估保障级(EAL)。

为支持 ISO/IEC 15408 的上述三个部分，已经出版了其他文档，如 ISO/IEC 18045，提供了使用 ISO/IEC 15408 进行 IT 安全评估的基本方法。

表 1 列出了三类主要目标读者如何关注 ISO/IEC 15408 的各个部分。

表 1 ISO/IEC 15408 使用指南

	消费者	开发者	评估者
第 1 部分	用于了解背景信息和必要的使用参考。指导构建 PP	用于了解背景信息和参考、开发 TOE 安全规范使用的必要信息	用于参考的必要信息，指导构建 PP 和 ST
第 2 部分	用作表达 TOE 要求的形式化陈述时的指导和参考	用作解释 TOE 功能要求陈述和形式化功能规范时的必要参考	用作解释功能要求陈述时的必要参考
第 3 部分	确定所需保障级别时用作指导	用作解释 TOE 保障要求陈述和确定保障方法时的参考	用作解释保障要求陈述时的参考

5.5 评估背景

为了使评估结果具有更好的可比性，评估应在权威的评估体制框架内执行，该体制框架负责制定标准、监控评估质量、管理评估机构和评估者必须符合的规章制度。

ISO/IEC 15408 不对规章制度框架提出要求。但是，不同评估机构的这些框架有必要一致，以达到相互认可评估结果的目标。

使评估结果具有更好的可比性的第二种方法是使用通用方法达到这些结果。对于 ISO/IEC 15408，该方法在评估方法(CEM)中给出。

通用评估方法的使用主要是确保评估结果的可重复性和客观性，但仅靠评估方法本身是不充分的。许多评估准则需要使用专业的判断和背景知识，而这些更难达到一致。为了增强评估结论的一致性，最终的评估结果可能提交给认证过程来处理。

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 安全准则的应用达到更加一致的一种手段。

评估体制和认证过程由运行评估体制和过程的评估机构负责，不属 ISO/IEC 15408 的范围。

6 一般概念

6.1 简介

本章提出了贯穿 ISO/IEC 15408 的一般概念，其中包括使用这些概念的背景，以及 ISO/IEC 15408 使用这些概念的方法。ISO/IEC 15408-2 和 ISO/IEC 15408-3 由本部分的用户查阅，进一步展开这些概念的使用，并采用 ISO/IEC 15408 描述的方法。对于使用 ISO/IEC 15408 执行评估的用户，ISO/IEC 18045 是适用的。本章假定读者已具备一些 IT 安全的知识，并不作为该领域的辅导教材。

ISO/IEC 15408 用一组安全概念和术语来讨论安全性。理解这些概念和术语是有效使用 ISO/IEC 15408 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 ISO/IEC 15408 适用的这类 IT 安全问题。

6.2 资产和对策

安全与资产保护有关，资产是赋予了价值的实体，资产的例子包括：

- 文件或服务器的内容；选举中投票的真实性；
- 电子商务程序的可用性；
- 使用昂贵打印机的能力；
- 机密设施的访问。

但是如果过于主观的估价，几乎任何事物都可以成为资产。

资产放置的环境称为运行环境。运行环境方面的例子有：

- 银行机房；
- 连接到互联网的计算机网络；
- 局域网；
- 一般办公环境。

许多资产均以信息的形式由 IT 产品存储、处理和传送，以满足信息所有者的要求。信息所有者为了信息的可用性，会严格控制信息的传播和修改，并且资产受到保护措施的保护以抵御威胁。图 2 说明了这些概念和关系。

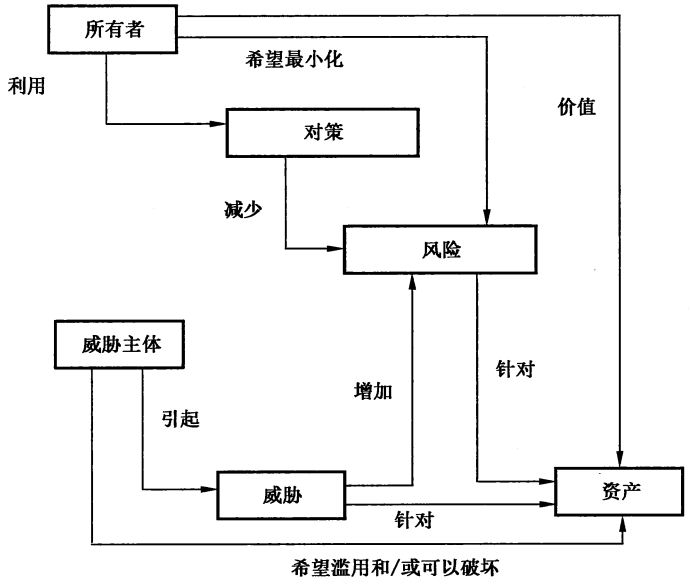

图 2　安全概念及其关系

保护利益资产是对资产赋予价值的所有者的责任。实际或假想的威胁主体也可能会对资产赋予价值，并试图以危害资产所有者利益的方式滥用资产。威胁主体的例子包括黑客、恶意用户、非恶意用户(有时犯错误)、计算机进程和事故。

资产的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。特定的安全性损坏一般包括但不限于：丧失资产的机密性、完整性和可用性。

因此在意识到威胁的可能性及其对资产的影响的基础上，这些威胁就引发了对资产的风险。随后要实施对策以减少对资产的风险。这些对策可以由 IT 对策(如防火墙、智能卡)和非 IT 对策(如警卫和访问程序)组成。更多关于安全对策(控制)和如何实现及管理这些对策的讨论见 ISO/IEC 27001 和 ISO/IEC 27002。

资产所有者可能要对资产负责，因此，应有足够的理由支持资产所有者做出决定，以接受由资产暴露给威胁所带来的风险。

为了支持此项决定，应能够证实以下两个方面：

- 对策是充分的：如果对策做了声称要做的事情，就能够对抗对资产的威胁；
- 对策是正确的：对策做了声称要做的事情。

许多资产所有者缺乏必要的知识、专业技术和资源来判断对策的充分性和正确性，他们可能不希望仅仅依赖对策开发者的主张。因此消费者可以通过对这些对策进行评估，以增加对所有或部分对策的充分性和正确性的信心。图 3 描述了评估的概念及其关系。

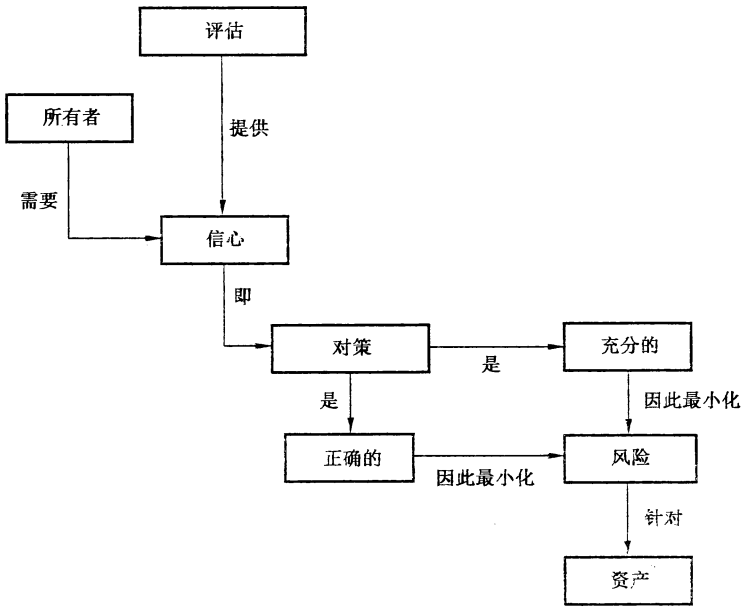

图 3 评估概念及其关系

6.2.1 对策的充分性

在评估中，对策的充分性是通过一个称为安全目标的概念来分析的。本条将简单描述这个概念，更详细和完整的描述参见附录 A。

安全目标从描述资产和对这些资产的威胁开始，然后安全目标描述对策（以安全目的形式），并证实这些对策对于对抗这些威胁是充分的：如果对策做了声称要做的事情，那么对策足以对抗威胁。

安全目标将对策划分为两组：

a) TOE 的安全目的：描述了需要在评估中确定其正确性的对策；

b) 运行环境安全目的：描述了不需要在评估中确定其正确性的对策。

这样划分的理由是：

- ISO/IEC 15408 仅仅适合于评估 IT 对策的正确性，因此非 IT 对策（保安人员、程序）总是放在运行环境中考虑。
- 对策的正确性评估耗费时间和金钱，因此评估所有 IT 对策的正确性也许不可行。
- 某些 IT 对策的正确性可能已经在其他评估中评估了，因此再次评估其正确性是无成本效益的。

对于 TOE（在评估期间，IT 对策的正确性将被评估），在安全功能要求（SFRs）中，安全目标要求进一步细化 TOE 安全目的，这些 SFR 要用标准化语言（在 GB/T 18338.2 中描述）进行阐述，以保证精确性和可比性。

总而言之，安全目标证实了：

- SFR 满足 TOE 安全目的；
- TOE 安全目的和运行环境安全目的足以对抗威胁；
- 因此，SFR 和运行环境安全目的足以对抗威胁。

从这些方面看，它遵循了正确的 TOE（满足 SFR）与正确的运行环境（满足运行环境安全目的）结合来对抗威胁。在 6.2.2 和 6.2.3 中，TOE 的正确性和运行环境的正确性分开讨论。

6.2.2 TOE 的正确性

TOE 的设计和实现可能不正确，可能因此包含着导致脆弱性的错误，攻击者通过利用这些脆弱性，仍可能破坏和/或滥用资产。

这些脆弱性可能由开发期间的意外错误、糟糕的设计、故意添加的恶意代码和糟糕的测试等引发。

为确定 TOE 的正确性，可以执行的活动如：

- 测试 TOE；
- 检查 TOE 的各种设计表示；
- 检查 TOE 开发环境的物理安全。

安全目标以安全保障要求(SAR)的形式提供了这些活动的结构化描述，以确定正确性。这些安全保障要求用标准化语言(在 ISO/IEC 15408-3 描述)来表示，以保证正确性和可比性。

如果满足了 SAR，那么就可保障 TOE 的正确性，因此 TOE 几乎不可能包含可以被攻击者利用的漏洞。在 TOE 正确性方面的保障程度由 SAR 本身确定："弱"的 SAR 所能提供保障少，而许多"强"的 SAR 可提供更大的保障。

6.2.3 运行环境的正确性

运行环境的设计和实现也可能不正确，因此可能包含导致脆弱性的错误，攻击者通过利用这些脆弱性，仍然可以破坏和/或滥用资产。

然而，ISO/IEC 15408 无法保障可获得有关运行环境的正确性，换句话说，运行环境将不做评估(见 6.3)。

就评估而言，运行环境被假设为可以 100%地实现运行环境安全目的。

这不排除 TOE 的消费者使用其他方法确定其运行环境的正确性，如：

- 如果是对于一个操作系统，运行环境安全目的声明"运行环境将确保来自不可信网络(如，internet)的实体只能通过 ftp 访问 TOE"，消费者可以选择一个经过评估的防火墙，配置它为仅允许通过 FTP 对 TOE 进行访问。
- 如果运行环境安全目的声明"运行环境将确保所有管理人员没有恶意行为"，消费者可以调整其与管理人员的合同使其包括对恶意行为的惩罚性制裁，但这个不是 ISO/IEC 15408 评估的一部分。

6.3 评估

ISO/IEC 15408 认可两种形式的评估：一个是下面描述的 ST/TOE 评估，一个是 ISO/IEC 15408-3 定义的 PP 评估，在许多地方，ISO/IEC 15408 使用的术语"评估"(不限定)指的是对 ST/TOE 的评估。

ISO/IEC 15408 中，ST/TOE 评估分为两步进行：

a) ST 评估：确定 TOE 和运行环境的充分性；

b) TOE 评估：确定 TOE 的正确性，就像前面说的，TOE 评估不评估运行环境的正确性。

ST 评估应用安全目标评估准则(在 ISO/IEC 15408-3 的 ASE 部分中定义)对安全目标进行评估。应用 ASE 准则的准确方法由所使用的评估方法确定。

TOE 评估更加复杂，TOE 评估的主要输入是：评估证据，包括 TOE 和 ST，通常也包括来自开发环境的输入，如设计文档或开发者测试结果。

TOE 评估由适用于 SAR(来自安全目标)的评估证据组成。准确应用 SAR 的方法是由所使用的评估方法确定的。

应用 SAR 的结果如何被文档化，需要生成的报告及其细节由使用的评估方法及执行评估的评估体制确定。

TOE 评估过程产生的结果为下列两种情况之一：

- 并未满足所有 SAR，因此评估结果未达到 ST 中所述的 TOE 满足 SFR 的特定保障级别；
- 满足所有 SAR，因此评估结果达到了 ST 中所述的 TOE 满足 SFR 的特定保障级别。

TOE 评估可以在 TOE 开发完成之后进行，或者与 TOE 开发并行。

阐述 TOE/ST 评估结果的方法在第 9 章描述。这些结果也标识了 TOE 声称与其符合的 PP 和包，这些概念将在第 7 章描述。

7 剪裁安全要求

7.1 操作

ISO/IEC 15408 的功能和保障组件可以严格按照 ISO/IEC 15408-2 和 ISO/IEC 15408-3 中的定义使用，也可以通过使用允许的操作来剪裁。当使用操作的时候，PP/ST 作者应该注意其他要求对此要求的依赖关系应得到满足。允许的操作如下：

- 反复：允许一个组件在不同操作时被使用超过一次以上；
- 赋值：允许指定参数；
- 选择：允许从一个列表中选定一项或多项；
- 细化：允许增加细节。

赋值和选择操作只允许用于组件中明确指定的位置。反复和细化允许用于所有组件。下面将更加详细的描述这些操作：

ISO/IEC 15408-2 附录对有效完成选择和赋值提供了指南，该指南提供了完成这些操作的规范化指导，应该遵循这些指导，除非 PP/ST 作者论证相关偏离是合理的。

a) 对于一个选择操作的完成，只有在已经明确规定的情况下，“无”才是有效的选项。
用于完成选择操作的列表必须非空，如果选择“无”选项，表示没有可以选择的其他附加选项。
如果“无”没有作为选择操作的选项，则允许在选择中用“和”和“或”组合选项，除非选择中明确要求“选择之一”。
必要时，选择操作可以与反复操作一起使用。在这种情况下，为每个反复操作选择的选项不应该与其他被反复选择的主体发生重叠，因为它们需要满足互斥性要求。

b) 对于赋值操作，为了确定何时“无”是一个有效值，可参见 ISO/IEC 15408-2 附录。

7.1.1 反复操作

反复操作可以在每个组件上执行。PP/ST 作者依据包括基于同一个组件的多个要求执行一个反复操作。一个组件的每次反复应该不同于该组件的所有其他反复，即用不同的方法完成该组件的赋值和选择，或用不同的方法对该组件进行细化。

应该唯一标识不同的反复操作，以便给出清晰的基本原理以及追踪到这些要求和从这些要求进行追踪。

要注意的重要一点是，有时对一个组件的一个反复操作也可以执行一个具有一组值的赋值操作来代替。在这种情况下，作者可以选择一个最适当的操作，考虑一下是否有必要为值的范围提供全部的基本原理，或者是否有必要将它们分开。作者也应该注意是否所有这些值都需要单独的追踪。

7.1.2 赋值操作

当一个给定组件包含了一个可以由 PP/ST 作者设置参数的元素，这时就需要进行赋值操作。参数可以是一个非限制变量，或者是限定变量值在指定范围的一个规则。

当 PP 中的元素包含一个赋值时，PP 作者都应该做下列四件事情之一：

a) 不进行赋值。PP 作者可以在 PP 中包括组件 FIA_AFL.1.2“当达到或超过已定义的不成功鉴别尝试次数时，TSF 应[**赋值：动作列表**]”；

b) 完成赋值。例如，PP 作者可以在 PP 中包括组件 FIA_AFL.1.2“当达到或超过已定义的不成功鉴别尝试次数时，TSF 应[**防止外部实体在将来捆绑到任何主体**]”；

c) 限制赋值，进一步限制允许值的范围。例如，PP 作者可以在 PP 中包括 FIA_AFL.1.1“TSF 应**检测当**[**赋值：4 和 9 之间的正整数**]**”次不成功的鉴别尝试发生时**…；

d) 将赋值转换为选择操作时，会缩小赋值范围。例如，PP 作者可以在 PP 中包括 FIA_AFL.1.2“当达到或超过已定义的不成功鉴别尝试次数时，TSF 应[选择：**防止用户在将来捆绑到任何主体，通知管理员**]”；

无论何时 ST 中的元素包含了一个赋值，ST 作者应如 b)中所示，完成该赋值。ST 中不允许出现 a)、c)和 d)中的情况。

b)、c)和 d)中的值应该与赋值要求的类型符合。

当赋值由一个集合完成时(如主体集合)，可以列出一组主体，也可以是对可以导出集合元素的集合的描述，只要主体是有意义的。如：

- 所有主体；
- 所有 X 类型的主体；
- 除了主体 a 之外的所有主体。

7.1.3 选择操作

当给定的组件包含了必须由 PP/ST 作者从几项中选择一个元素时，发生选择操作。

当 PP 中的一个元素包含了一个选择操作时，PP 作者可以作下列三件事之一：

a) 不进行选择；

b) 通过选择一个或多项完成选择；

c) 删除部分选项，但要留下两个或多个选项来实现限制选择。

当 ST 中的一个元素包含了一个选择操作时，ST 作者应该如 b)所示完成该选择，ST 中不允许出现 a)和 c)中的情况。

b)和 c)中的选项应该从选择操作提供的选项中选取。

7.1.4 细化操作

细化操作可以在每一个要求上执行。PP/ST 作者通过修改要求执行细化操作。细化操作的第一条规则是在 PP/ST 中，满足细化要求的 TOE 也要满足细化之前的要求(即，一个细化的要求必须比原始要求更加严格)。如果一个细化操作不满足这条规则，经过细化操作的要求就被视为一个扩展要求并应被相应处理。

这条规则的唯一例外是 PP/ST 作者允许细化一个 SFR，以应用于某些而非所有的主体、客体、操作、安全属性和/或外部实体。

然而该例外情况不适用于细化已在 PP 中进行了一致性声明的 SFR，这些 SFR 不可提炼用于比该 PP 中更少的主体、客体、操作、安全属性或外部实体。

细化操作的第二个规则是细化应与原始组件相关。

细化操作的特殊情况是编辑上的细化，该细化在一个要求上作了少量变化，如，为了保持恰当的语法而修改语句，或者使得要求更容易被读者理解。这种变化不允许以任何方式修改要求的意义。

7.2 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功能性或保障性而依赖于另一个组

件的存在时，就产生依赖关系。

ISO/IEC 15408-2 中的功能组件通常会依赖其他功能组件，正如 ISO/IEC 15408-3 的保障组件可能依赖其他保障组件。也可以定义 ISO/IEC 15408-2 对 ISO/IEC 15408-3 组件的依赖关系，然而，这不能避免扩展的功能组件对保障组件有依赖关系，反之亦然。

组件依赖关系的描述可通过参考 ISO/IEC 15408-2 和 ISO/IEC 15408-3 的组件定义来确定。为了保证 TOE 安全要求的完整性，当基于具有依赖关系的组件的要求被合并到 PP 和 ST 中时，依赖关系应该被满足。构造包时，也应该考虑依赖关系。

换句话说：如果组件 A 有对组件 B 有依赖，意味着当 PP/ST 包含了基于组件 A 的一个安全要求，则 PP/ST 也应该包含下列情况之一：

a) 基于组件 B 的安全要求；

b) 基于在层次上高于 B 组件的安全要求；

c) 论证 PP/ST 不包含基于组件 B 的安全要求的理由。

在情况 a)和 b)中，当由于依赖关系包含了一个安全要求时，有必要以特定方法完成该安全要求上的操作(赋值、反复、细化、选择)以保证实际上满足该依赖关系。

在情况 c)中，论证不包括一个安全要求的理由时应该阐述：

- 为什么依赖关系是不需要的或者无用的；
- 依赖关系已经在 TOE 的运行环境安全要求中阐述过了。在这种情况下，应论证运行环境安全目的如何处理这种依赖关系；
- 依赖关系已经由其他的 SFR 用某些其他的方式进行了处理(扩展的 SFR，SFR 的组合等)。

7.3 扩展组件

在 ISO/IEC 15408 中，强制基于 ISO/IEC 15408-2 和 ISO/IEC 15408-3 组件的要求有两点例外。

a) 存在不能转化到第二部分 SFR 的 TOE 安全目的、或者存在不能转化为第三部分 SAR(如，有关密码学的评估)的第三方要求(如，法律、标准)；

b) 安全目的可以被转化，但仅仅基于 ISO/IEC 15408-2 或 ISO/IEC 15408-3 的组件进行转化很困难或者很复杂。

在上述两种情况下，PP/ST 作者需要自己定义组件，这些新定义的组件被称为扩展组件。精确定义的扩展组件需要在已有组件的基础上提供扩展 SFR 和 SAR 的环境及其含义。

新组件正确定义之后，PP/ST 作者能够像其他 SFR 和 SAR 一样使用基于新定义的扩展组件的一个或多个 SFR 或 SAR。在这点上，基于 ISO/IEC 15408 的 SFR 或 SAR 与基于扩展组件的 SFR 或 SAR 之间没有本质的区别。对扩展组件的进一步要求可参考 ISO/IEC 15408-3 扩展组件定义(APE_ECD)和扩展组件定义(ASE_ECD)。

8 保护轮廓和包

8.1 引言

为了允许感兴趣的消费者群体和社会团体表达他们的安全需求，并方便编写 ST，ISO/IEC 15408 的这部分提出了两个特殊的概念：包和保护轮廓(PP)。在 8.2 和 8.3 中详细描述了这些概念，在 8.4 中描述了如何使用这些概念。

8.2 包

包是一个安全要求的命名集合。一个包可以是：

- 只包含 SFR 的功能包；

- 只包含 SAR 的保障包。

不允许同时包含 SFR 和 SAR 的混合包。

包可由任何团体定义，意在可重用。为此，它应包含有用的且易于组合的要求。包可以用于构造更大的包、PP 和 ST。目前没有评估包的准则，因此，任意 SFR 或 SAR 的集合都可以成为一个包。

保障包的例子是 ISO/IEC 15408-3 定义的评估保障级(EAL)，ISO/IEC 15408 目前尚无功能包。

8.3 保护轮廓

虽然 ST 通常用于描述一个特定的 TOE(如，某个特定型号的防火墙)，PP 却意在描述一类 TOE(如，防火墙)。因此，相同的 PP 可以作为模板用于构造许多不同评估中的 ST。PP 的详细描述参见附录 B。

一般来说，ST 为一个 TOE 描述要求，由 TOE 的开发者编写；而 PP 为一类 TOE 描述通用要求，典型的编写者为：

- 为一个给定 TOE 类型寻求一致要求的用户团体；
- TOE 的开发者，或者希望为该类型的 TOE 建立最小基线的类似 TOE 开发者群体；
- 为采购过程而详细说明其要求的政府或大公司。

PP 确定了允许 ST 符合 PP 的方式，即 PP 声明(在 PP 符合性声明中，见 B.5)规定了 ST 符合的方式是：

- 如果 PP 声明需要满足严格的符合性，ST 就应严格地与 PP 符合；
- 如果 PP 声明需要满足可论证的符合性，ST 就应以严格的或者可论证的方式与 PP 符合；

换言之，如果 PP 明确允许可论证的符合性，那么仅允许 ST 以至少可论证的方式与 PP 符合；

如果 ST 声明与多个 PP 符合，它将以 PP 规定的(如上)方式与每个 PP 符合。这可能意味着 ST 与某些 PP 严格符合，而与另一些 PP 满足可论证的符合性。

注意 ST 与 PP 符合是否存在质疑。ISO/IEC 15408 不认可“部分”符合。因此 PP 作者的职责是确保 PP 不会过于繁琐，而妨碍 PP/ST 作者声明与这样的 PP 符合。

由于以下认识，ST 等同于 PP，或者比 PP 约束更多：

- 所有满足该 ST 的 TOE 也满足该 PP；
- 所有满足该 PP 要求的运行环境也满足该 ST 的要求。

或者，非正式地说，(与 PP 相比)ST 应该对 TOE 施加相同的或更多的限制，并对 TOE 的运行环境施加相同的或更少的限制。

在 ST 的不同章条中可以对这个一般性的结论进行更多特定的陈述：

安全问题定义：ST 中的符合性基本原理应证实 ST 中的安全问题定义等同于(或更严格于)PP 中的安全问题定义。这意味着：

- 所有 TOE，若满足 ST 中的安全问题定义，也满足 PP 中的安全问题定义；
- 所有运行环境，若满足 PP 中的安全问题定义，也满足 ST 中的安全问题定义。

安全目的：ST 中的符合性基本原理应证实 ST 中的安全目的等同于(或更严格于)PP 中的安全目的。这意味着：

- 所有 TOE，若满足 ST 中的 TOE 安全目的，也满足 PP 中的 TOE 安全目的；
- 所有运行环境，若满足 PP 中的运行环境安全目的，也满足 ST 中的运行环境安全目的。

如果说明了与保护轮廓严格符合，则下列要求适用：

a) **安全问题定义**：ST 应包含 PP 中定义的安全问题，可以规定附加的威胁和组织安全策略，但不能规定附加的假设。

b) **安全目的**：ST：
   - 应该包含 PP 中的所有 TOE 安全目的，但也可以规定附加的 TOE 安全目的；
   - 应该包含所有的运行环境安全目的(下一点除外)，但不能规定附加的运行环境安全目的；
   - 可以将 PP 中的某些运行环境安全目的指定为 ST 中的 TOE 安全目的，这称为安全目的

的重新分配。如果安全目的重新赋值给 TOE，安全目的的基本原理必须解释清楚哪个假设或假设的哪一部分不再是必须的。

c) 安全要求：ST 应该包含 PP 中的所有 SFR 和 SAR，但可以声明增加或增强的 SFR 和 SAR，ST 中完成的操作必须与 PP 中的操作一致；ST 中完成的操作与 PP 中完成的操作完全相同或者要求更加严格（应用细化规则）。

如果说明了与保护轮廓的可论证符合性，那么下列要求适用：

- ST 应该包含有关为什么 ST 在限制程度上被认为“等同或更严格”于 PP 的基本原理；
- 可论证的符合性允许 PP 作者描述将要解决的公共安全问题，为其解决方案需要满足的必要条件提供一般性的指导原则，已知可能有多个方法能详细说明一个解决方案。

PP 评估是可选的。评估依据 ISO/IEC 15408-3 的 APE 准则进行。此评估的用意是证实 PP 是完备的、一致的、技术上合理的，且适于用作建立其他 PP 或 ST 的模版。

在一个已评估的 PP 上建立 PP/ST 可获得两个优点：

- 在 PP 中出现错误、不确定性或缺陷的风险将少得多。如果在编写或评估新的 ST 期间，发现与 PP 有关的问题（本可以通过 PP 评估过程发现），那么在修正 PP 之前，会损失很多时间。
- 新的 PP/ST 的评估常常可以重用已评估 PP 的评估结果，从而减少评估新 PP/ST 所需付出的努力。

图 4 描述了 PP、ST 和 TOE 内容之间的关系。

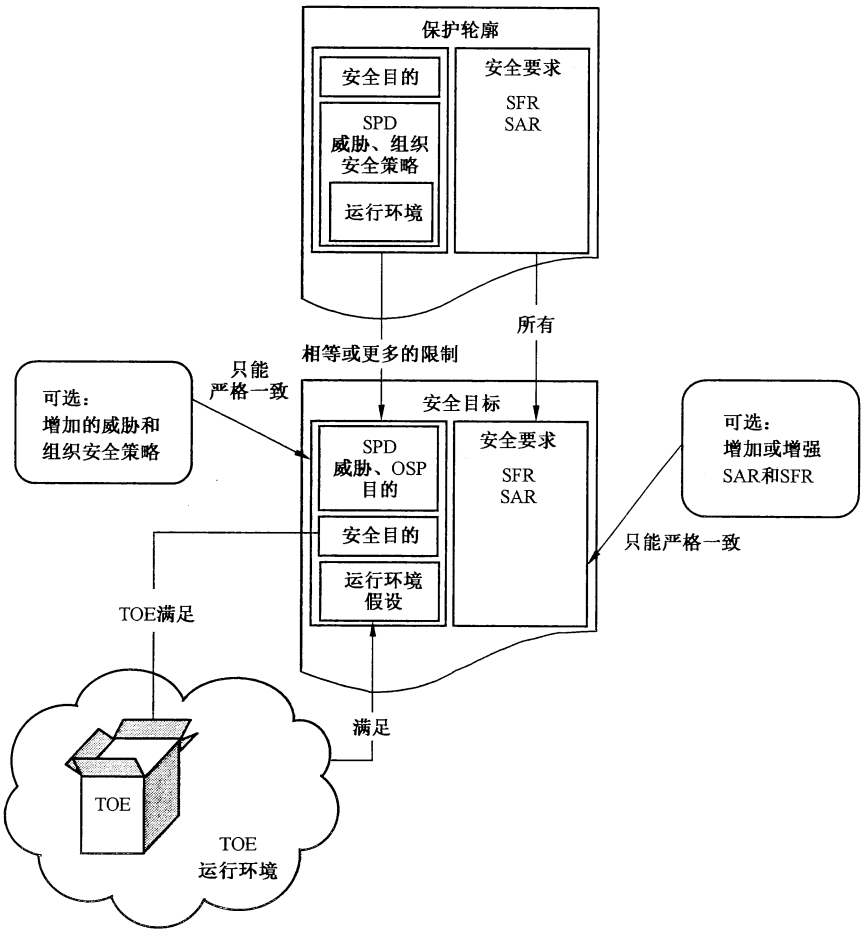

图 4 PP、ST 和 TOE 内容之间的关系

8.4 使用保护轮廓和包

如果 ST 声明与一个或多个包和/或保护轮廓符合，ST 的评估将(在 ST 的其他属性中)证实 ST 实际上与它们声明符合的包或 PP 符合，确定符合性的细节可参见附录 A。

这允许出现如下过程：

a) 一个寻求获取特定类型 IT 安全产品的组织根据其安全需求开发一个 PP，使其通过评估并发布；

b) 开发者采用这个 PP，编写 ST 以声明与其符合，并使其通过 ST 评估；

c) 然后开发者构造 TOE(或使用一个已存在的 TOE)，并使 TOE 对照该 ST 进行评估。

结果是开发者能够证明他的 TOE 与组织的安全需求符合：组织因此能够购买该 TOE。类似情况可适用于包。

8.5 使用多个保护轮廓

ISO/IEC 15408 也允许 PP 与其他 PP 符合，允许基于以前的 PP 构造 PP 链。

例如，可以使用集成电路的 PP 和智能卡 OS 的 PP 构造一个智能卡 PP(IC 和 OS)，在智能卡 PP 中声明与另两个 PP 符合。然后可以基于智能卡 PP 和 Applet 加载的 PP 编写一个公交智能卡 PP。最后，开发者可以基于这个公交智能卡 PP 构造一个 ST。

9 评估结果

9.1 序言

本章给出根据 ISO/IEC 18045 执行的 PP 和 ST/TOE 评估的预期结果。图 5 给出了评估过程中各评估活动的结果。

- PP 评估产生的已评估的 PP 目录。
- TOE 评估框架中使用的 ST 评估的中间结果。
- ST/TOE 评估产生的已评估的 TOE 目录。在许多情况下，这些目录指的是 TOE 所在的 IT 产品，而不是特定 TOE，因此，目录中的 IT 产品不应解释为整个 IT 产品已经被评估过，ST/TOE 评估的实际范围由 ST 定义，需要参考相关目录示例的参考书目。

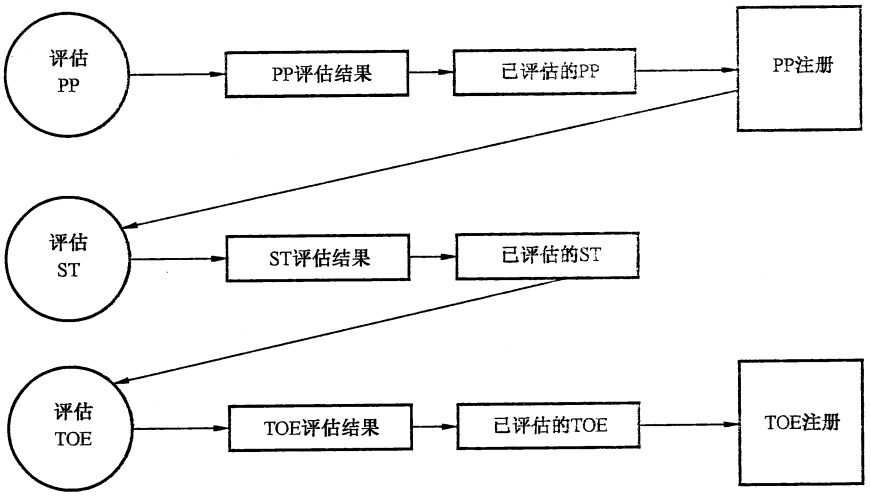

图 5 评估结果

ST 可以基于包、已评估的或未被评估的 PP，但是没有强制要求，因为 ST 不必基于任何包或 PP。

评估应能产生能引为证据的客观的和可重现的结果，即使没有绝对客观的尺度来衡量安全评估结果时也应如此。存在一套评估准则是使评估产生有意义的结果的必要的前提条件，这也为不同评估机构之间互认评估结果提供了技术基础。

一个评估结果代表了对 TOE 安全特性进行专门考察时的结果。这个结果并不自动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，包括评估结果。

9.2 PP 评估结果

ISO/IEC 15408-3 包含了要求评估者参考的评估准则，以便声明 PP 是完备的、一致的和技术合理的，因此适于用在开发 ST 中。

评估结果也应该包括“符合性声明”(见 9.4)。

9.3 ST/TOE 评估结果

ISO/IEC 15408-3 包含了要求评估者参考的评估准则，以便确定 ST 中是否存在 TOE 满足 SFR 的充分保障。因此 TOE 评估将为 ST 给出通过/失败的结果。如果 ST 和 TOE 的评估结果均为通过，其基础产品就是合格的，包含在注册库中。评估结果也应该包括在 9.4 中定义的“符合性声明”。

可能有这种情况，评估结果要在随后的认证过程中使用，但这个认证过程不在 ISO/IEC 15408 的范围内。

9.4 符合性声明

符合性声明表示要求集合的来源由通过评估的 PP 或 ST 来满足，该符合性声明包含了一个 ISO/IEC 15408 的符合性声明：

a) PP 或 ST 声明符合的 ISO/IEC 15408 的版本的描述。

b) 与 ISO/IEC 15408-2(安全功能要求)的符合性描述：

- **ISO/IEC 15408-2 符合**：如果 PP 或 ST 中所有 SFR 仅仅基于 ISO/IEC 15408-2 的功能组件，那么该 PP 或 ST 与 ISO/IEC 15408-2 是符合的，或
- **ISO/IEC 15408-2 扩展**：如果 PP 或 ST 中有一个 SFR 不是基于 ISO/IEC 15408-2 的功能组件，那么该 PP 或 ST 是 ISO/IEC 15408-2 扩展的。

c) 与 ISO/IEC 15408-3(安全保障要求)的符合性描述：

- **ISO/IEC 15408-3 符合**：如果 PP 或 ST 中所有 SAR 仅仅基于 ISO/IEC 15408-3 的保障组件，那么该 PP 或 ST 与 ISO/IEC 15408-3 是符合的，或
- **ISO/IEC 15408-3 扩展**：如果 PP 或 ST 中有一个 SAR 不是基于 ISO/IEC 15408-3 的保障组件，那么该 PP 或 ST 是 ISO/IEC 15408-3 扩展的。

另外，符合性声明也可以包括与包有关的陈述，可以包括如下情况：

- *包选定符合*：一个 PP 或 ST 与一个预定义的包符合(如，EAL)，如果：
  - PP 或 ST 中的 SFR 与包中的 SFR 相同，或
  - PP 或 ST 中的 SAR 与包中的 SAR 相同。
- *包选定增强*：一个 PP 或 ST 是一个预定义的包的增强，如果：
  - PP 或 ST 中的 SFR 包含了所有包中的 SFR，但至少增加了一个 SFR 或者有一个 SFR 级别高于包中的一个 SFR；
  - PP 或 ST 中的 SAR 包含了所有包中的 SAR，但至少增加了一个 SAR 或者有一个 SAR 级别高于包中的一个 SAR。

注意，当一个给定 ST 的 TOE 被成功评估了，ST 的任何符合性声明 TOE 也应遵循，因此 TOE 也可以是如 ISO/IEC 15408-2 符合的。

最后，符合性声明也可以包括两个与保护轮廓相关的陈述：

a) *PP 符合*：一个 PP 或者 TOE 满足特定 PP，该 PP 作为符合性结果列出；

b) *符合性陈述*（仅对 PP）：该陈述描述了 PP 或 ST 必须与相关 PP 符合的方式：严格的或可论证的。更多信息参见附录 B。

9.5 使用 ST/TOE 评估结果

一旦 ST 和 TOE 经过评估，资产所有者可以获得 TOE 及其运行环境对抗威胁的保障（在 ST 中定义的），评估结果可以由资产所有者用于决定是否接受资产暴露给威胁的风险。

然而，资产所有者应该仔细检查是否：

- ST 中的安全问题定义匹配资产所有者的安全问题；
- 资产所有者的运行环境与 ST 中描述的运行环境安全目的符合。

如果不是这两种情况，TOE 可能不适于资产所有者的目的。

另外，一旦一个已评估的 TOE 处于运行中，TOE 中以前的未知错误或脆弱性仍然可能出现，这时，开发者可以修正 TOE（修复脆弱性），或者修改 ST 从评估范围中排除该脆弱性，无论哪种情况，旧的评估结果可能不再有效。

如果需要重获信心，需要重新评估。ISO/IEC 15408 可以用于再评估，但再评估的详细规程超出了 ISO/IEC 15408 的范围。

附 录 A
（资料性附录）
安全目标规范

A.1 本附录的用意和结构

本附录的目的是解释安全目标（ST）的概念。本附录没有定义 ASE 准则，相关定义可以在 ISO/IEC 15408-3 找到，参考书目中列出的文档提供了相应支持。

本附录有 4 个主要部分组成：

a) ST 必须包含什么。A.2 中给出概要，A.4～A.10 进行了详细描述。这些章条描述了 ST 的强制性内容及其之间的关系，并提供了示例。

b) 如何使用 ST。A.3 中给出概要，A.11 进行了详细描述。这些章条描述了应该如何使用 ST，以及一些 ST 可以回答的问题。

c) 低保障 ST。低保障 ST 是指减少了内容的 ST，在 A.12 中有详细描述。

d) 与标准一致性的声明。A.13 描述了 ST 作者如何声明 TOE 满足特定标准。

A.2 ST 的强制性内容

图 A.1 描绘了 ST 的强制性内容，这些是在 ISO/IEC 15408-3 给出的。图 A.1 也可以用作 ST 的结构性轮廓，但其他的结构也是允许的。例如，如果安全要求基本原理内容特别多，可以放在 ST 的一个附录中而不放在安全要求的章条。在下面对 ST 各章条及其内容进行了简要概括，A.4～A.10 中进行了详细介绍。ST 一般包含：

a) *ST 引言*，以三个不同抽象形式对 TOE 进行叙述性描述；

b) *符合性声明*，表明 ST 是否声明与某些 PP 或包符合，并且如果这样，与哪些 PP 或包符合；

c) *安全问题定义*，列举威胁、组织安全策略和假设；

d) *安全目的*，表明安全问题的分析解决结果如何划分为 TOE 安全目的和 TOE 运行环境安全目的。

e) *扩展组件定义*（可选），可以定义新组件（即在 ISO/IEC 15408-2 和 ISO/IEC 15408-3 不包含的组件）。需要这些新的组件定义扩展功能要求和扩展保障要求；

f) *安全要求*：将 TOE 安全目的转化成标准语言。标准语言以 SFR 的形式描述，同样，该章条也定义了 SAR；

g) *TOE 概要规范*，表明 SFR 如何在 TOE 中实现的。

也存在减少了内容的低保障 ST，在 A.12 详细描述。除此之外，本附录所有其他内容与以上内容构成了全部 ST 的内容。

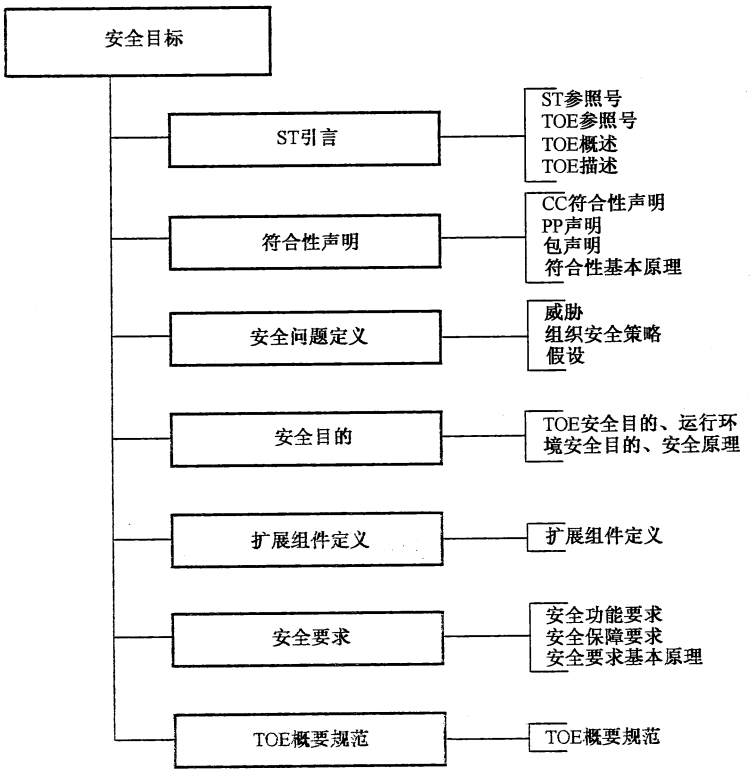

图 A.1 安全目标内容

A.3 使用 ST

A.3.1 应该如何使用 ST

一个典型的 ST 承担两个角色：

- 评估之前及评估期间，ST 指出“要评估什么”。在这个任务中，ST 作为开发者和评估者之间在 TOE 确切的安全属性和确切的评估范围上达成一致协议的基础。技术正确性和完备性是这个任务的主要问题。A.7 描述了在这个任务中如何使用 ST。
- 评估之后，ST 指出“被评估了什么”。在这个任务中，ST 作为开发者或销售者和 TOE 潜在消费者之间达成一致协议的基础。ST 以抽象的方式描述了 TOE 确切的安全属性，潜在消费者能够依赖这个描述，因为 TOE 已经过评估满足 ST。易用和容易理解是这个任务的主要问题。A.11 描述了在这个任务中如何使用 ST。

A.3.2 不应使用 ST 的情况

ST 不应承担的两个角色是：

- 详细规范：ST 是较高抽象级别的安全规范。一般 ST 不应包含详细的协议规范、算法或机制的详细描述、具体操作的冗长描述等。
- 完整规范：ST 是安全规范而不是通用规范。除非与安全相关，如互联性、物理大小和重量、要求的电压等属性不应该成为 ST 的组成部分。也就是说通常 ST 可以是一个完整规范的一部分，而其本身不是一个完整规范。

A.4 ST 引言(ASE_INT)

ST 引言在三个抽象层面上对 TOE 进行叙述性描述：

a) ST 参照号和 TOE 参照号，为 ST 及其相关的 TOE 提供标识信息；

b) TOE 概述，简要描述 TOE；

c) TOE 描述，对 TOE 进行更加详细的描述。

A.4.1 ST 参照号和 TOE 参照号

ST 中包含了一个清晰的 ST 参照号，它标识特定的 ST。一个典型的 ST 参照号由标题、版本、作者和出版日期组成。ST 参照号的例子："某数据库 ST，版本 1.3，某开发团队，2012 年 10 月 11 日"。

ST 也包含了一个 TOE 参照号，它标识声明与 ST 符合的 TOE。一个典型的 TOE 参照号由开发者名称、TOE 名称和 TOE 版本号组成。TOE 参照号的例子："某数据库 v2.11"。由于一个 TOE 可能被多次评估，例如 TOE 的不同消费者进行的评估，因此会有多个 ST，TOE 参照号不是必须唯一的。

如果 TOE 由一个或多个已知产品构成，那么允许在 TOE 参照号中通过引用产品名称进行反映，但不应该用来误导消费者：不允许出现评估中没有考虑的重要部分或安全功能、同样也不允许出现在 TOE 参照号中没有反映出来的情况。

ST 参照号和 TOE 参照号便于在已评估的 TOE 或产品列表中检索和标识 ST 和 TOE 及其概要结论。

A.4.2 TOE 概述

TOE 概述的目的是帮助 TOE 的潜在消费者，他们通过查找已评估的 TOE 或产品列表找到可能满足他们安全需求，且是他们的硬件、软件和固件支持的 TOE。通常 TOE 概述用几个段落的长度进行描述。

最后，TOE 概述简单描述 TOE 的使用和它的重要安全特征，标识 TOE 类型，并且标识 TOE 所需要的非 TOE 的硬件、软件和固件部分。

A.4.2.1 TOE 的用途和重要安全特征

TOE 用途和重要安全特征的描述用于给出 TOE 在安全方面具有的能力，和在某一安全环境下的用途。本条为 TOE 消费者(潜在的)编写，根据业务操作，使用消费者理解的语言描述 TOE 的用途和重要安全特征。

示例："某数据库 v2.11 是一个用于网络环境的多用户数据库，它允许 1024 个用户同时活动，允许口令/令牌和生物识别认证，提供意外数据故障保护，能够回滚 1 万个事务，其审计特征可配置程度高，以便允许对某些用户和事务执行详细审计，同时保护其他用户和事务的隐私"。

A.4.2.2 TOE 类型

TOE 概述标识 TOE 的一般类型，如防火墙、VPN 防火墙、智能卡、加密调制解调器、企业网、WEB 服务器、数据库、WEB 服务器和数据库、LAN、包含 WEB 服务器和数据库的 LAN，等。

也有可能 TOE 不容易确定类型，此时也使用"无"。

在某些情况下，TOE 类型可能误导消费者，示例如下：

- 某些 TOE 因为其类型而被预期认为具备某种功能，但是 TOE 不具有该功能，如：
  ——ATM 卡类型的 TOE，不支持任何标识和鉴别功能；
  ——防火墙类型的 TOE，不支持普遍使用的协议；
  ——PKI 类型的 TOE，没有证书撤销功能。

- TOE 因为其类型而被预期运行在某些运行环境中，但该 TOE 达不到这样的要求，如：
  ——PC 操作系统型 TOE，除非 PC 没有网络连接、软盘驱动器和 CD/DVD 播放器，否则其不能安全工作；
  ——防火墙，除非所有能够连接防火墙的用户都是善意的，否则防火墙不能安全工作。

A.4.2.3 需要的非 TOE 的硬件/软件/固件

尽管某些 TOE 不依赖其他信息技术，而许多 TOE（特别是软件 TOE）依赖额外的、非 TOE 的硬件、软件或固件。在后一种情况中，要求 TOE 概述标识出这样的 TOE 硬件、软件或固件。尽管不要求完整地，且充分详细地标识出额外的硬件、软件或固件，但是标识应该完整并尽量详细，以便潜在消费者能确定 TOE 需要使用的重要硬件、软件或固件。

硬件/软件/固件标识示例：

- 标准 PC，处理器 1 GHz 以上，内存 512 MB 以上，某操作系统运行版本 3.0，更新版本 6b、c、或 7，或者版本 4.0；
- 标准 PC，处理器 1 GHz 以上，内存 512 MB 以上，某操作系统运行版本 3.0，更新版本 6d，带 1.0 WM 驱动套件的某图形卡 1.0；
- 标准 PC，某操作系统，版本 3.0 以上；
- 智能卡 SB2067 集成电路；
- 智能卡 SB2067 集成电路，运行某智能卡操作系统 V2.0；
- 某办公室局域网。

A.4.3 TOE 描述

TOE 描述是 TOE 的叙述性描述，可能需要几页纸进行描述。TOE 描述应该提供给评估者和潜在消费者对 TOE 安全能力的一般性理解，比 TOE 概述中的描述详细，TOE 描述也可用于说明 TOE 适用的更广泛的应用环境。

TOE 描述应论述 TOE 的物理范围：构成 TOE 的所有硬件、固件、软件及指南部分的一个列表。该列表应该在一定程度上进行详细描述，使读者对这些部分有一般性理解。

TOE 描述也应该论述 TOE 的逻辑范围：一定程度上描述 TOE 提供的安全特征，使读者获得对这些安全特征的一般性理解。该描述应该比 TOE 概述中描述的重要安全特征更加详细。

物理和逻辑范围的一个重要特性是其以一种无歧义的方式描述 TOE，明确哪些部分或特征在 TOE 之内，哪些部分或特征在 TOE 之外。当 TOE 与非 TOE 实体联系在一起并且不能轻易将它们分离时这显得尤其重要。

TOE 与非 TOE 实体难界定的示例：

- TOE 是智能卡 IC 的密码协处理器，而不是整个 IC；
- TOE 是除了密码处理器之外的智能卡 IC；
- TOE 是某防火墙 v18.5 的网络地址转换部件。

A.5 符合性声明（ASE_CCL）

本条描述 ST 如何符合：

- ISO/IEC 15408-2 和 ISO/IEC 15408-3；
- 保护轮廓（如果有）；
- 包（如果有）。

ST 与 ISO/IEC 15408 符合的描述由两项组成：使用的 ISO/IEC 15408 的版本以及 ST 是否包含扩展的安全要求（见 A.8）。

ST 与保护轮廓的符合性描述是指 ST 列出了其声称符合的包。这方面的解释见 9.4。

ST 与包的符合性描述是指 ST 列出了其声称符合的包。这方面的解释见 9.4。

A.6 安全问题定义(ASE_SPD)

A.6.1 引言

安全问题定义解释了将要处理的安全问题。涉及 ISO/IEC 15408 的安全问题定义是公认的,也就是说安全问题定义的推理过程超出了 ISO/IEC 15408 的范围。

然而,应该注意到,评估结果的有效性对 ST 依赖性很强,而且 ST 的有效性对安全问题定义的依赖性很强,因此花费有效资源并使用良好定义的过程分析推导安全问题定义常常是有价值的。

注意,按照 ISO/IEC 15408-3,不强制要求所有章条均有陈述,陈述了威胁的 ST 不必一定陈述组织安全策略,反之亦然,ST 也可能会省略假设。

也要注意,对于物理上是分布式的 TOE,可能最好是针对 TOE 运行环境的不同区域分开讨论相关威胁、组织安全策略和假设。

A.6.2 威胁

在这一条中,给出要由 TOE、TOE 运行环境或这两者的一种组合所应对的威胁。

威胁由对资产的威胁主体执行的敌对行为组成。

敌对行为是威胁主体对资产执行的行为,这些行为会影响资产的一个或多个属性,而资产正是通过这些属性来体现价值的。

威胁主体可以被描述为单个的实体,但某些情况下以实体类或实体群体等方式来描述可能更好。

威胁主体的例子如黑客、用户、计算机进程、意外事件等。可以从专业技能、资源、机会和动机等方面进一步描述威胁主体。

威胁示例:

- 黑客(有很强的专业技能、使用标准设备、且以有偿工作的方式)从某公司网络远程拷贝机密文件;
- 蠕虫严重地降低广域网性能;
- 系统管理员侵犯用户隐私;
- 某些人员在互联网上侦听机密电子通信信息。

A.6.3 组织安全策略(OSP)

在这一条中,给出要由 TOE、TOE 运行环境或由这两者的一种组合所执行的组织安全策略。

组织安全策略是由一个实际的(或假想的)组织目前(和/或将来)为运行环境强制(或有可能强制)要求的一些安全规则、规程和指导原则。组织安全策略可能由控制 TOE 运行环境的组织或立法机关,或者规章制定机构制定。组织安全策略可以应用于 TOE 和/或 TOE 的运行环境。

组织安全策略示例:

- 政府使用的所有产品在口令产生和加密方面必须符合国家标准;
- 只有具有系统管理员权限并获得部门许可的用户才允许管理部门文件服务器。

A.6.4 假设

本条说明了为了能够提供安全功能,对运行环境所做的假设。如果 TOE 被放在不满足这些假设的运行环境中,TOE 可能不再能提供它所有的安全功能。假设可以是关于运行环境的物理、人员和连通性方面的。

假设示例：

- 运行环境物理方面的假设：
  ——假设 TOE 放在经过电磁辐射最小化设计的房间中；
  ——假设 TOE 的管理员控制台放在受限访问区域中。
- 运行环境人员方面的假设：
  ——假设为了操作 TOE，TOE 的用户经过了充分的培训；
  ——假设 TOE 的用户被批准为允许接触国家涉密信息；
  ——假设 TOE 的用户不会写下他们的口令。
- 运行环境连通性方面的假设：
  ——假设 PC 工作站至少具有 10 GB 可用磁盘空间运行 TOE；
  ——假设 TOE 是该工作站上运行的唯一的非 OS 应用；
  ——假设 TOE 不会连接到不可信网络。

注意，评估期间这些假设均被认为是真实的：他们不会以任何方式被测试。出于这些理由，只能对运行环境做假设。由于评估是由关于 TOE 的评估断言组成，而不是通过假设 TOE 断言是真实的来完成的，所以决不能对 TOE 的行为做假设。

A.7 安全目的(ASE_OBJ)

安全目的是以简明抽象的方式对安全问题定义中所定义问题的预期解决方案进行的陈述。安全目的的作用有三方面：

- 为安全问题提供高层的、以自然语言描述的解决方案；
- 将该解决方案划分为两个局部方式的解决方案，以反映出每个不同实体都必须处理一部分问题；
- 证实这些局部方式的解决方案构成了一个对安全问题的完整解决方案。

A.7.1 高层解决方案

安全目的由一组不过度地体现具体细节，且简明清晰的陈述组成，总体形成了一个安全问题的高层解决方案。安全目的的这一抽象层次对于知识丰富的 TOE 的潜在消费者是清晰的和可理解的。安全目的使用自然语言描述。

A.7.2 局部方式的解决方案

在 ST 中，由安全目的描述的高层解决方案被划分为两部分，分别称为 TOE 安全目的和运行环境安全目的，以反映出这两个局部方式的解决方案将分别由 TOE 和运行环境这两个不同实体提供。

A.7.2.1 TOE 安全目的

TOE 提供安全功能以解决在安全问题定义中提到的某部分问题。这种局部方式的解决方案称为 TOE 安全目的，由一组为解决该部分问题而应该实现的目的组成。

TOE 安全目的示例：

- TOE 应保持在它和服务器之间所传输文件的内容的机密性；
- 在允许用户访问 TOE 提供的传输服务之前，TOE 应该标识和鉴别所有用户；
- TOE 应该根据 ST 附录 3 中描述的数据访问策略限制用户对数据的访问。

如果 TOE 在物理上是分布式的，最好将 ST 章条中的 TOE 安全目的部分划分为反映这种情况的子章条进行描述。

A.7.2.2 运行环境安全目的

TOE 的运行环境实现了一些技术和规程方面的措施，以帮助 TOE 正确提供(由 TOE 安全目的定义的)安全功能。该局部的解决方案被称为运行环境安全目的，由一组运行环境应该达到的目标陈述组成。

运行环境安全目的的示例：

- 运行环境应提供安装了版本为 3.01b 的某 OS 的工作站以运行 TOE；
- 在允许操作 TOE 之前，运行环境应确保所有 TOE 人员用户接受适当培训；
- TOE 运行环境应限制管理人员和由管理人员陪同的维护人员对 TOE 的物理访问；
- 在将 TOE 产生的审计日志发送给中央审计服务器之前，运行环境应保证它们的机密性。

如果 TOE 的运行环境由多个场所组成，每个都有不同特性，最好将包含运行环境安全目的的 ST 章条划分为几个子条来反映这种情况。

A.7.3 安全目的和安全问题定义之间的关系

ST 也包含安全目的基本原理，包含两部分：

- 追溯部分，用于描述每个安全目的分别处理哪些威胁、组织安全策略和假设；
- 证明部分，用于论述所有的威胁、组织安全策略和假设都可以被安全目的有效处理。

A.7.3.1 安全目的和安全问题定义之间的追溯

追溯说明了安全目的如何映射到安全问题定义中描述的威胁、组织安全策略和假设。

a) *没有伪造的目的*：每个安全目的至少追溯到一个威胁、组织安全策略和假设；

b) *完全覆盖了安全问题定义*：每个威胁、组织安全策略和假设至少可由一个安全目的追溯到；

c) *正确追溯*：由于假设总是围绕着运行环境中的 TOE 进行，所以 TOE 的安全目的不能追溯到假设。ISO/IEC 15408-3 允许的追溯在图 A.2 中描述。

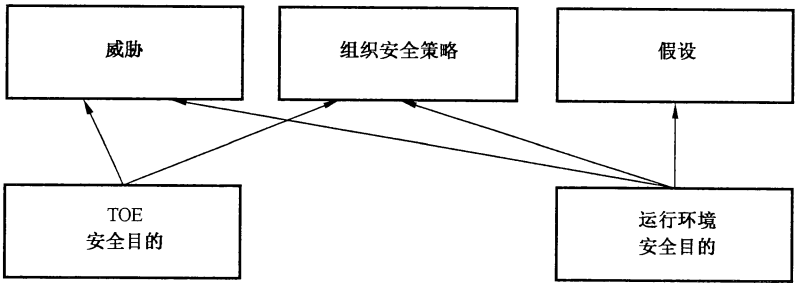

图 A.2 安全目的和安全问题定义间的追溯

多个安全目的可以追溯到相同的威胁，表明这些安全目的共同对抗该威胁。对组织安全策略和假设也是如此。

A.7.3.2 提供对追溯的论证

安全目的基本原理也证实了追溯是有效的：如果所有安全目的对特定的威胁、组织安全策略和假设的追溯都已完成，那么所有给定的威胁、组织安全策略和假设均被处理(如，分别被对抗、被实施、被支持)。

该证实分析实现对抗威胁、实施组织安全策略和支持假设的相关安全目的的效果，并且得出确实如此的结论。

在某些情况下，部分安全问题定义与某些安全目的很相似，此时证实可以很简单。如：威胁“T17：威胁主体读取了 A 和 B 之间的机密信息”，TOE 的一个安全目的“OT12：TOE 应确保 A 和 B 之间传输的所有信息保持机密性”，证实“T17 直接由 OT12 与之对抗”。

A.7.3.3 对抗威胁

对抗一个威胁不一定意味着要消除那个威胁，也可以意味着充分的减少该威胁或者充分的缓解该威胁。

消除威胁示例：

- 消除威胁主体执行敌对行为的能力；
- 移动、改变或保护资产以便敌对行为不再适用于它；
- 消除威胁主体(如，从网络中移除频繁使该网络崩溃的设备)。

减少威胁示例：

- 限制威胁主体完成敌对行为的能力；
- 限制威胁主体执行敌对行为的机会；
- 减少成功执行敌对行为的可能性；
- 通过威慑手段减少威胁主体执行敌对行为的动机；
- 增大威胁主体需要的技能或资源。

缓解威胁的作用示例：

- 频繁作资产备份；
- 获取资产的多余拷贝；
- 给资产上保险；
- 确保及时检测到成功的敌对行为，以便采取适当行动。

A.7.4 安全目的：结束语

根据安全目的和安全目的基本原理，可以得出下列结论：如果所有安全目的都可实现，那么就解决了在 ASE_SPD(安全问题定义)中定义的安全问题，因为所有的威胁都被应对了，所有的组织安全策略都得到了实施，而所有的假设也都得到了支持。

A.8 扩展的组件定义(ASE_ECD)

在许多情况下，ST 中的安全要求(见 A.9)基于的是 ISO/IEC 15408-2 和 ISO/IEC 15408-3 的组件。然而，某些情况下，可能有 ST 中的要求不是基于 ISO/IEC 15408-2 和 ISO/IEC 15408-3 的组件的情况。在这种情况下，新组件(扩展组件)必须被定义，并且该定义应该在扩展组件定义中进行。有关的更多信息参见附录 C.4。

注意，本条将只包含扩展组件，不包括扩展要求(要求基于扩展组件)。扩展要求应该包含在安全要求中(见 A.9)，与基于 ISO/IEC 15408-2 和 ISO/IEC 15408-3 组件要求的所有目的相同。

A.9 安全要求(ASE_REQ)

安全要求由两组要求构成：

a) 安全功能要求(SFR)：将 TOE 安全目的转化为标准语言；

b) 安全保障要求(SAR)：TOE 满足 SFR 所要获得的保障描述。

这两组要求在 A.9.1 和 A.9.2 中讨论。

A.9.1 安全功能要求(SFRs)

SFR 是 TOE 安全目的的转化。他们通常是以一个较详细且抽象的形式表述，但他们必须是一个

完全的转化(安全目的必须被完全对应)并且独立于任何特定的技术解决方案(实现)。ISO/IEC 15408要求其转化为一个标准化语言有几个理由:

- 提供要评估什么的精确描述。因为TOE的安全目的一般用自然语言描述,转化为标准化语言使得TOE的功能性描述更加精确;
- 允许两个ST之间比较。不同的ST作者可能使用不同的术语描述他们的安全目的,标准化的语言使用了相同的术语和概念。这使得容易进行比较。

ISO/IEC 15408中没有要求对运行环境安全目的进行转化,因为不会评估运行环境,因此不需要针对其评估进行描述。与运行系统安全评估相关的条款见参考书目。

可能出现部分运行环境在另外的评估中被评估的情况,但这超出了当前评估的范围。如:操作系统TOE可能要求一款防火墙在其运行环境中。另一个评估可能随后评估该防火墙,但该评估没有做操作系统TOE的任何评估。

A.9.1.1 ISO/IEC 15408如何支持转化

ISO/IEC 15408支持三种方式的转化:

a) 提供预定义的明确的"语言"精确描述要评估什么。该语言由ISO/IEC 15408-2中定义的一组组件定义。使用该语言作为将TOE安全目的向SFR进行恰当转化是强制的,虽然有些例外情况会存在(见7.3)。

b) 提供操作:该机制允许ST作者定义SFR以便提供更精确的TOE安全目的的转化。ISO/IEC 15408的这部分定义了四种允许的操作:赋值、选择、反复、细化。这些在C.2进一步描述。

c) 提供依赖关系:该机制支持更全面的向SFR的转换。在ISO/IEC 15408-2语言中,SFR可以有对其他SFR的依赖关系。这表示如果ST使用了该SFR,那么,它一般也需要使用另外一些其依赖的SFR。对于ST作者来说需要更大的努力以便全面包含必要的SFR从而提高ST的全面性。依赖关系在7.2中进一步描述。

A.9.1.2 SFR和安全目的之间的关系

ST也可以包含一个安全要求基本原理,由与SFR相关的两条内容组成:

- 追溯即是表明SFR与TOE安全目的的对应关系;
- 论证所有TOE安全目的都已由SFR做了有效对应。

A.9.1.2.1 SFR和TOE安全目的之间的追溯

说明SFR如何追溯到TOE安全目的的映射如下:

a) 没有伪造的SFR:每个SFR至少追溯到一个安全目的;

b) 完全覆盖TOE安全目的:每个TOE安全目的至少有一个SFR追溯。

多个SFR可以追溯到相同的TOE安全目的,表明那些安全要求共同满足TOE的该安全目的。

A.9.1.2.2 对追溯提供论证

安全要求基本原理证实追溯是有效的:如果追溯到TOE的特定安全目的的所有SFR被满足,那么TOE的安全目的就达到了。

该证实应该分析满足实现TOE安全目的的相关SFR的有效性,并且得出情况确实如此的结论。

存在SFR与TOE安全目的的表述十分接近的情况,此时证实可以很简单。

A.9.2 安全保障要求(SARs)

SAR是对如何评估TOE的描述。该描述使用标准语言有两个理由:

- 提供 TOE 如何被评估的精确描述。使用标准化语言帮助建立精确的描述，避免含糊不清；
- 允许两个 ST 之间比较。因为不同的 ST 作者可能使用不同的术语描述评估，标准化的语言使用了相同的术语和概念。这使得容易进行比较。

该标准化语言由 ISO/IEC 15408-3 中定义的一组组件定义。该语言的使用是强制的，虽然存在某些例外情况。ISO/IEC 15408 用两种方法增强该语言：

a) 提供操作：该机制允许 ST 作者定义 SAR。ISO/IEC 15408 有 4 种操作：赋值、选择、反复、细化。这些在 7.1 中进一步描述。

b) 提供依赖关系：该机制支持更全面的向 SAR 的转化。在 ISO/IEC 15408-3 语言中，SAR 可以有对其他 SAR 的依赖关系，这表示如果 ST 使用了该 SAR，那么，它一般也需要使用另外一些其他的 SAR。对于 ST 作者来说需要更大的努力以便全面包含必要的 SAR 从而提高 ST 的全面性。依赖关系在 7.2 中进一步描述。

A.9.3 SARs 和安全要求基本原理

ST 也包含了一个安全要求基本原理，解释为什么该 SAR 特定集合是合适的。对该解释没有特定要求。解释的目的是使 ST 的读者理解选择该特定集合的理由。

不一致的例子是安全问题描述中提到威胁代理的能力很强，而 SAR 中包含了低(或无)脆弱性分析(AVA_VAN)。

A.9.4 安全要求：结束语

在 ST 的安全问题定义中，安全问题定义为由威胁、组织安全策略和假设组成。在 ST 的安全目的一条中，以两个子章条的形式提供了为解决安全问题要实现的安全目的。

- TOE 安全目的；
- 运行环境安全目的。

另外，提供了安全目的基本原理以便说明是否达到所有安全目的，安全问题就解决了：所有的威胁被对抗、所有的组织安全策略被实施、所有的假设被支持。

在 ST 的安全要求一条中，TOE 安全目的被转化成 SFR，并且提供了安全要求基本原理表明是否所有 SFR 被满足，所有 TOE 安全目的就达到了。

另外，提供了一组 SAR，表明 TOE 如何被评估，以及选择这些 SAR 的解释。

上述内容可以综合为这样的陈述：如果所有 SFR 和 SAR 被满足并且所有运行环境安全目的被达到，那么存在 ASE_SPD 中定义的安全问题被解决的保障：所有威胁被对抗、所有组织安全策略被实施、所有假设被支持。如图 A.3 所示。

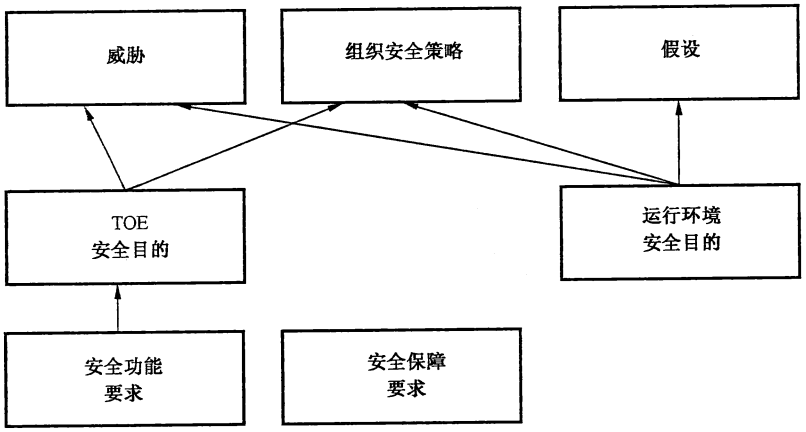

图 A.3 安全问题定义、安全目的和安全要求之间的关系

获得的保障程度由 SAR 说明，保障程度是否充分由选择这些 SAR 的解释说明。

A.10 TOE 概要规范(ASE_TSS)

TOE 概要规范的目的是向 TOE 的潜在消费者提供 TOE 如何满足 SFR 的描述。TOE 概要规范应该提供 TOE 用于该目的的一般性技术机制。描述的详细程度应该使潜在消费者能够充分理解 TOE 的一般形态和实现。

例如：如果 TOE 是一个互联网 PC，其 SFR 包含 FIA_UAU.1 详细说明了需要鉴别，那么 TOE 概要规范就应该表明这个鉴别如何做：口令、令牌、虹膜扫描等。给出更多的信息，如 TOE 用于满足 SFR 的可适用标准，或者也可以提供更多细节描述。

A.11 ST 可解答的问题

评估之后，ST 指明“评估什么”。在这个任务中，ST 作为 TOE 开发者或销售者和 TOE 潜在消费者之间达成一致协议的基础。ST 因此可以回答下述问题(或更多)：

a) 我如何能够在给出的多个已存在的 ST/TOE 中找出我需要的 ST/TOE？该问题由 TOE 概述阐述，在那里给出了 TOE 的简要(几个段落)描述。

b) TOE 适合我现有的 IT 基础设施吗？该问题由 TOE 概述阐述，在那里标识出了运行 TOE 所需要的硬件/固件/软件元素。

c) TOE 适合我现有的运行环境吗？这个问题由运行环境安全目的阐述，在那里标识了 TOE 为发挥作用所受到的运行环境所有限制。

d) TOE 做什么(感兴趣的读者)？该问题由 TOE 概述阐述，在那里给出了 TOE 的简要(几个段落)描述。

e) TOE 做什么(潜在消费者)？该问题由 TOE 描述处理，在那里给出了 TOE 的简要(几页)描述。

f) TOE 做什么(偏技术)？该问题由 TOE 概要规范阐述，在那里提供了 TOE 使用机制的深层次的描述。

g) TOE 做什么(专家)？该问题由提供了抽象的高级技术描述的 SFR 以及由提供了附加细节的 TOE 概要规范阐述。

h) TOE 处理政府/组织定义的问题吗？如果政府/组织已经定义了该解决方案的已定义的包或 PP，那么答案可以在 ST 的符合性声明一条中找到，在那里列出了 ST 符合的所有包和 PP。

i) TOE 处理我的安全问题了吗(专家)？什么是 TOE 对抗的威胁？它实施的组织安全策略是什么？做了哪些有关运行环境的假设？这些问题由安全问题定义阐述。

j) 我可以信任 TOE 到什么程度？这能够在安全要求一条的 SAR 中找到，那里提供了评估 TOE 使用的保障级别，因此是相关评估提供了对 TOE 正确性的信任。

A.12 低保障安全目标

写 ST 不是一件简单的事情，特别是在整个低保障级别的评估中，开发者和评估者的大部分努力都可能要花在这个方面。出于这种原因，也可写一个适用于低保障级别的 ST。

ISO/IEC 15408 允许使用低保障 ST 作 EAL1 评估，EAL2 及以上不可以。低保障 ST 只能声明符合一个低保障 PP(参见附录 B)。一个常规的 ST(如，有全部内容)可以声明与一个低保障的 PP 符合。

低保障 ST 与常规 ST 相比明显减少了一些内容，如：

- 不用描述安全问题定义；
- 不用描述 TOE 安全目的，但运行环境安全目的仍然必须描述；
- 由于 ST 中没有安全问题定义，所以不用描述安全目的基本原理；
- 由于 ST 中没有 TOE 安全目的，所以安全要求基本原理只需要论证未被满足的依赖关系。

其余内容包括：

a) TOE 和 ST 参照号。

b) 符合性声明。

c) 各种叙述性描述：

1) TOE 概述；

2) TOE 描述；

3) TOE 概要规范。

d) 运行环境安全目的。

e) SFR 和 SAR(包括扩展组件定义)，以及安全要求基本原理(只要求未满足的依赖关系)。

低保障 ST 中削减后的内容如图 A.4 所示。

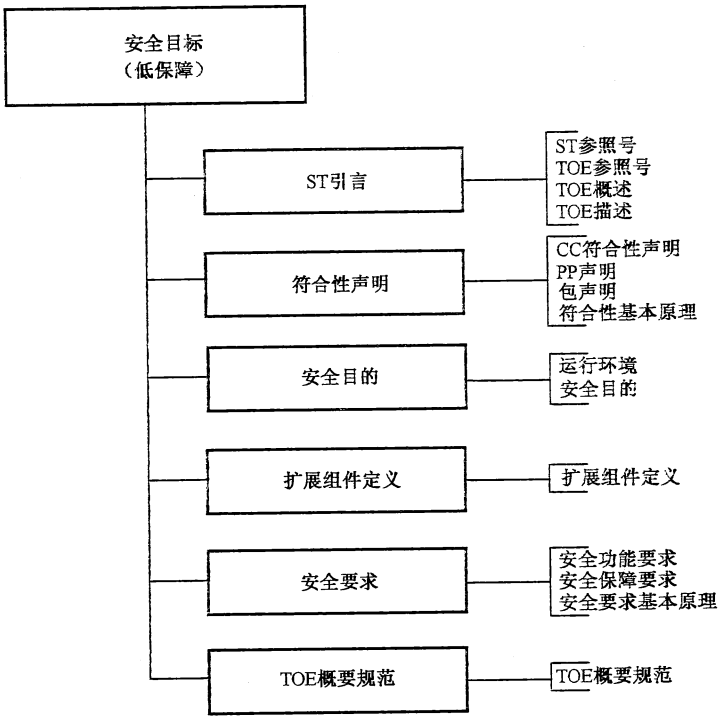

图 A.4 低保障安全目标内容

A.13 在 ST 中引用其他标准

在某些情况下，ST 作者可能希望引用外部标准，如特定的密码标准或协议。为此，ISO/IEC 15408 提供了 3 种方法：

a) 作为组织安全策略(或者组织安全策略的一部分)：

例如：如果有一个国标定义如何选择口令，可以将它在 ST 中作为组织安全策略声明。这可能会产生一个环境目的(如，如果 TOE 用户需要因此选择口令)，或者如果 TOE 生成口令，可能产生 TOE 安全目的，进而产生适当的 SFR(可能是 FIA 类)。在这两种情况下，开发者需要为 TOE 安全目的和适于实现组织安全策略的

SFR 作出合理的基本原理。评估者需要检查其事实上是否合理(可能决定因此而查看标准),是否像在下面解释的那样,组织安全策略由 SFR 实现。

b) 作为技术标准(如某密码标准)用于细化 SFR:

在这种情况下,与标准的符合性是 TOE 的 SFR 实现的一部分,标准的全文被看作 SFR 的一部分。随后确定符合性,就像与 SFR 的任何其他符合性一样:通过在 ADV 和 ATE 评估活动中进行设计分析和测试,来确定 SFR 在 TOE 中已被完全实现。如果仅仅引用了标准中的特定部分,该部分应该明确地在 SFR 的细化过程中说明。

c) 作为技术标准(如某密码标准)在 TOE 概要规范中提及:

只能把 TOE 概要规范看作是如何细化 SFR 的一个解释,并不像 SFR 或 ADV 交付文档那样被完全用于规范严格的实现要求。因此,若 TOE 概要规范引用了一个技术标准,而在 ADV 相关的证据文件中又没有反映它,评估者可能会发现其中存在着不一致,但又无法通过例行活动测试与该标准的一致性。

附 录 B
（资料性附录）
保护轮廓规范

B.1 本附录的目标和结构

本附录的目标是解释保护轮廓（PP）的概念。本附录没有定义 APE 准则；这个定义可以在 ISO/IEC 15408-3 找到，并由参考书目中给出的文档提供支持。

由于 PP 和 ST 有众多重叠，本附录突出了 PP 和 ST 之间的不同。ST 和 PP 相同的内容描述在附录 A 中。

本附录有 4 个主要部分：

a) PP 必须包含的内容。这部分内容在 B.2 中给出概要，在 B.4～B.9 中给出详细描述。这些章条描述 PP 的强制内容、这些内容之间的相互关系，并提供示例。

b) 如何使用 PP。在 B.3 中给出概要。

c) 低保障 PP。低保障 PP 是指减少了内容的 PP，在 B.11 中有详细描述。

d) 标准一致性声明。B.12 描述了 PP 作者如何声明 TOE 满足特定标准。

B.2 PP 的强制内容

图 B.1 描绘了 ISO/IEC 15408-3 给出的 PP 的强制内容。图 B.1 也可以用作 PP 的结构性轮廓，虽然允许选择两种结构之一。如，安全要求基本原理特别多，可以放在 PP 的附录中而不放在安全要求的章条中。PP 的各个章条及这些章条的内容在下面简单总结，并在 B.4～B.9 中详细介绍。PP 一般包含：

a) PP 引言：含有 TOE 类型的叙述性描述；

b) 符合性声明：表明 PP 是否声明与任何 PP 或包符合，并且如果这样，与哪个 PP 或包符合；

c) 安全问题定义：表明威胁、组织安全策略和假设；

d) 安全目的：表明安全问题的分析解决结果是如何划分为 TOE 安全目的和 TOE 运行环境安全目的；

e) 扩展组件定义：可以定义新组件（如这些组件不包含在 ISO/IEC 15408-2 和 ISO/IEC 15408-3 中），需要这些新的组件定义扩展功能要求和扩展保障要求；

f) 安全要求：将 TOE 安全目的转化成标准语言。标准语言以安全功能要求的形式描述，同样，该章条也定义了安全保障要求。

也存在减少了内容的低保障 PP；在 B.11 详细描述。除此之外，本附录所有其他内容与以上内容构成了全部 PP 的内容。

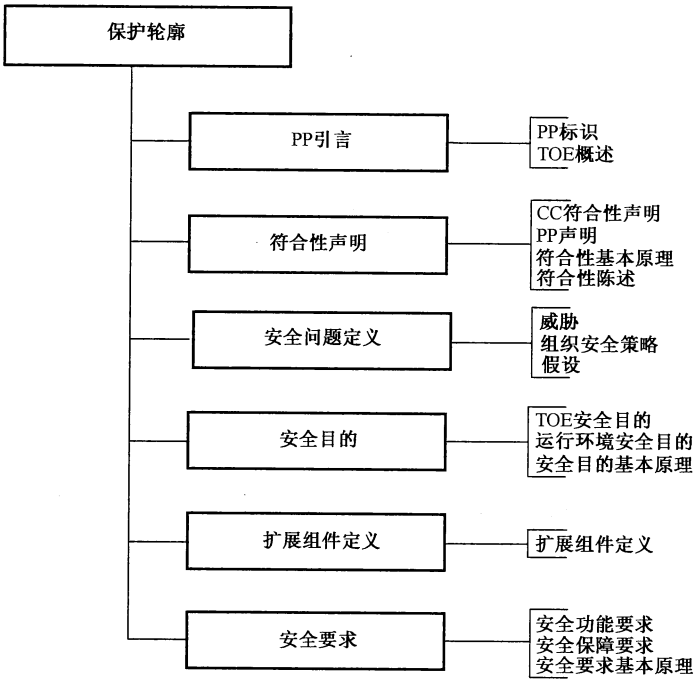

图 B.1 保护轮廓内容

B.3 使用 PP

B.3.1 如何使用 PP

一个典型的 PP 一般是对需求的陈述，由用户群体、管理实体、开发组织定义的通用的安全要求集合。PP 给消费者提供了一种引用该集合的参考，以便于以后针对这些需求的评估。

因此，一个 PP 一般用于：

- 特定消费者或消费者群体的部分要求规范，这些消费者只考虑购买符合该 PP 的 IT 类型的产品；
- 特定管理实体的部分规章制度，他们只允许使用符合该 PP 的特定类型的 IT 产品；
- IT 开发者对 IT 产品定义的基线，他们达成协议生产的所有该类 IT 产品将满足该基线要求。

当然不排除其他的使用情景。

B.3.2 不应使用 PP 的情况

PP 不适用的三个角色是：

- 详细规范：PP 是较高抽象级别的安全规范。一般 PP 不应该包含详细的协议规范、详细的算法或机制的描述、具体操作的冗长描述等。
- 完整规范：PP 是安全规范而不是通用规范。除非与安全相关，如互联性、物理大小和重量、要求的电压等属性不应该成为 PP 的构成部分。一般来说 PP 可以是一个完整规范的一部分，而其本身不是一个完整规范。
- 单一产品的规范：与 ST 不同，PP 是描述特定类型的 IT，而不是某单一产品。仅仅描述单一产品时，最好使用 ST。

B.4 PP 引言(APE_INT)

PP 引言以两种抽象的叙述性方式描述 TOE:

a) PP 标识:为 PP 提供标识信息;

b) TOE 概述:简单描述 TOE。

B.4.1 PP 标识

PP 中包含了一个识别特定 PP 的清晰的 PP 标识。一个典型的 PP 标识由标题、版本、作者和出版日期组成。PP 标识的例子:"某加密器 PP,版本 2b,某机构,2003 年 4 月 7 日"。这个标识必须是唯一的,以便可以区分不同 PP 和相同 PP 的不同版本。

PP 标识利于编目和 PP 引用及其在 PP 列表中的内容。

B.4.2 TOE 概述

TOE 概述的目的是帮助潜在消费者从通过被评估的产品列表中找到满足他们安全需求、并通过硬件、软件和固件得到支持的 TOE。

TOE 概述也适用于通过使用 PP 设计 TOE 的开发者或改进现有已生产的产品。

通常用几个段落的篇长对 TOE 进行概述性描述。

最后,TOE 概述简单描述了 TOE 的用途和它的重要安全特征,标识 TOE 类型,标识 TOE 可用的主要的非 TOE 硬件、软件和固件。

B.4.2.1 TOE 的用途和重要安全特征

TOE 用途和重要安全特征的描述用于给出 TOE 应该具有的能力和可能的使用方面的一般情况。本条为 TOE 消费者(潜在的)编写,根据业务操作,使用消费者理解的语言描述 TOE 的用途和重要安全特征。

示例:"某加密器是一个加密设备,允许通过某电缆电话系统进行机密性通信。最终,应该允许至少 32 个不同用户使用,支持至少 100 Mbps 的加密速度,应该允许跨越整个网络的船和电台之间的双边通信"。

B.4.2.2 TOE 类型

TOE 概述识别了 TOE 的一般类型,如防火墙、VPN 防火墙、智能卡、加密调制解调器、企业网、WEB 服务器、数据库、WEB 服务器和数据库、LAN、包含 WEB 服务器和数据库的 LAN 等。

B.4.2.3 可用的非 TOE 的硬件/软件/固件

某些 TOE 不依赖其他 IT、而许多 TOE(特别是软件 TOE)依赖另外的、非 TOE 的硬件、软件或固件,在后一种情况中,要求 TOE 概述标识出这样的 TOE 硬件、软件或固件。

由于保护轮廓不是为一款特定产品而编写,许多情况下只能给出可用硬件/软件/固件的一般情况,在另一些情况中,可以提供更多特定信息,如,已知平台的特定消费者的要求规范。

硬件/软件/固件标识示例:

- 无(单机 TOE);
- 运行在普通 PC 上的某操作系统 3.0;
- 智能卡 SB2067 集成电路;

- 运行某智能卡操作系统 V2.0 的智能卡 SB2067 集成电路；
- 某局域网。

B.5 符合性声明(APE_CCL)

PP 的本章条描述 PP 如何与其他 PP 和包符合，除符合性陈述之外，与 ST 的符合性声明章条相同(见 A.5)。

PP 中的符合性陈述说明 ST 或其他 PP 必须如何符合该 PP。PP 作者需要选择“严格的”或者“可论证的”符合性方式，相关细节参见附录 D。

B.6 安全问题定义(APE_SPD)

本条与 ST 的安全问题定义一条相同，解释见 A.6。

B.7 安全目的(APE_OBJ)

本条与 ST 的安全目的一条相同，解释见 A.7。

B.8 扩展的组件定义(APE_ECD)

本条与 ST 的扩展的组件定义一条相同，解释见 A.8。

B.9 安全要求(APE_REQ)

本条与 ST 的安全要求一条相同，解释见 A.9。值得注意的是，完成 PP 中的操作与完成 ST 中操作的规则略有不同，详细的解释见 7.1。

B.10 TOE 概要规范

PP 没有 TOE 概要规范。

B.11 低保障的保护轮廓

像低保障 ST 与常规 ST 的关系一样，低保障 PP 与常规 PP(即有全部内容的 PP)有同样的关系。就是说低保障 PP 由下述部分组成：

a) PP 引言，由 PP 标识和 TOE 概述组成；

b) 符合性声明；

c) 运行环境安全目的；

d) SFR 和 SAR(包括扩展的组件定义)和安全要求基本原理(只有依赖关系不满足时需要)。

低保障 PP 只能声明与一个低保障 PP 符合(见 B.5)，常规 PP 可以声明与低保障 PP 符合。

被减少内容的低保障 PP 见图 B.2。

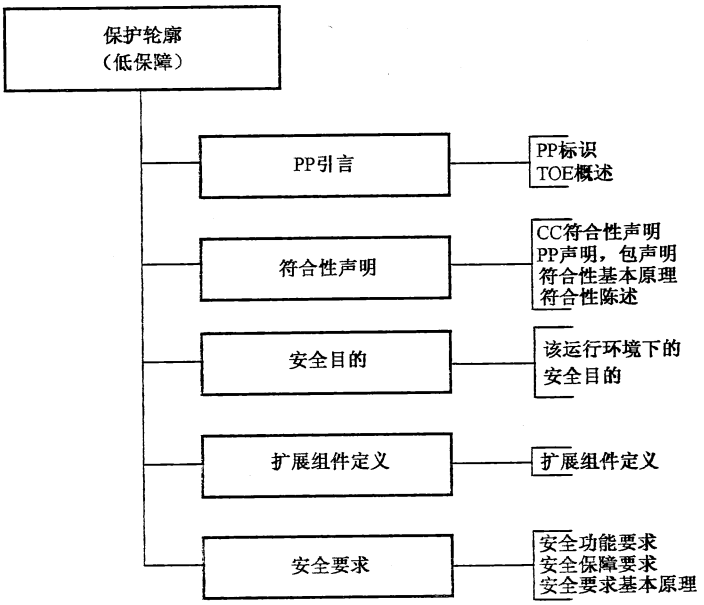

图 B.2 低保障保护轮廓内容

B.12 在 PP 中引用其他标准

本条与 A.13 中描述的有关 ST 的标准相同，不同的是，PP 没有 TOE 概要规范，第三个选择对 PP 无效。

提醒 PP 作者，在 SFR 中引用一个标准可能会强加给开发 TOE 的开发者为满足该 PP 的重大负担（与标准的大小和复杂度以及所需要的保障级别有关），因此这种情况可能更适合于要求二选一（非 CC 相关）方法评估与该标准的符合性。

附 录 C
（资料性附录）
操 作 指 南

C.1 引言

如 ISO/IEC 15408 第一部分中的描述，保护轮廓和安全目标包含预先定义的安全要求，也提供给 PP 和 ST 作者在某些环境中扩展组件列表的能力。

C.2 操作示例

7.1 给出了 4 种类型的操作，4 种操作示例描述如下：

C.2.1 反复操作

如同 7.1.1 中描述的，反复操作可以在每一个组件上执行，PP/ST 作者通过包含基于同一个组件的多个要求执行反复操作。组件的每一个反复操作不同于该组件的所有其他操作，这些操作通过用不同的方法完成赋值和选择来实现，或者通过以不同的方法对它进行细化来实现。不同的反复应该被唯一标识，以便提供清晰的基本原理、追溯到这些要求以及从这些要求进行追溯。

一个典型的反复操作的例子是为了要求两种不同加密算法的实现，反复了两次 FCS_COP.1 密码运算操作，被唯一标识的每个反复的示例如下：

- 密码运算（RSA 和 DSA 签名）[FCS_COP.1(1)]；
- 密码运算（TLS/SSL：对称操作）[FCS_COP.1(2)]。

C.2.2 赋值操作

如同 7.1.2 描述的，赋值操作出现在给定组件中，该组件包含着可以由 PP/ST 作者设置参数的元素。参数可以是一个无约束变量，或者是一个特定取值范围内缩小变量的规则。

具有赋值元素的例子是：FIA_AFL.1.2“当达到或超过所定义的不成功鉴别尝试次数时，TSF 应[赋值：动作列表]”。

C.2.3 选择操作

如同 7.1.3 中描述的，选择操作出现在一个包含着选择元素的给定组件中，该选择元素必须由 PP/ST 作者从几个选项中作出选择。

具有选择元素的例子是：FPT_TST.1.1“TSF 应在（选择：在初始化启动期间、正常运行期间周期性的、授权用户请求时、满足[赋值：产生自检的条件]时）运行一套自检以证实...”。

C.2.4 细化操作

如同 7.1.4 中描述的，细化操作可以在每一个要求上执行。PP/ST 作者通过修改要求来执行细化。

一个有效细化的例子是 FIA_UAU.2.1“在允许执行代表该用户的任何其他 TSF 促成动作前，TSF 应要求每个用户都已被成功鉴别。”被细化为“在允许执行代表该用户的任何其他 TSF 促成动作前，TSF 应要求每个用户都已通过用户名/口令被成功鉴别。”

细化操作的第一条规则是满足细化要求的 TOE 也要满足 PP/ST 中未细化的要求（即细化要求必

须比原始要求“更严格”)。这个规则的唯一例外情况是允许 PP/ST 作者细化 SFR 以便应用到部分但非全部主体、客体、操作、安全属性或外部实体。

这个例外的一个例子是 FIA_UAU.2.1“在允许执行代表该用户的任何其他 TSF 促成动作前,TSF 应要求每个用户都已被成功鉴别。”被细化为“在允许执行代表该用户的任何其他 TSF 促成动作前,TSF 应要求每个**来自互联网的**用户都已被成功鉴别。”

细化操作的第二条规则是细化应该与原始组件相关。如,细化一个具有防止电磁辐射的附加元素的审计组件是不被允许的。

细化的一个特定情况是可编辑细化,在要求中作较小的修改,即,因为语法或者使读者更可理解而改述句子。这种修改不允许以任何方式修改要求的意义。可编辑细化的例子包括:

安全功能要求 FPT_FLS.1TSF 应继续保持一个安全状态,当下述一些失败发生时:**“CPU 崩溃”**可以被细化为 FPT_FLS.1 当下述一个失败发生时:**CPU 崩溃**,TSF 应继续保持一个安全状态。”

C.3 组件的组织

在 ISO/IEC 15408-2 和 ISO/IEC 15408-3 中,ISO/IEC 15408 使用层次结构组织组件:

- 类,由族组成;
- 族,由组件组成;
- 组件,由元素组成;
- 元素。

提供类-族-组件-元素的层次组织帮助消费者、开发者和评估者定位特定元素。

ISO/IEC 15408 用相同的通用层次形式表达功能和保障组件,并且为两者使用了相同的组织结构和术语。

C.3.1 类

类的例子如:FIA 类:用于关注用户的标识、用户的鉴别以及用户和主体的绑定。

C.3.2 族

族的例子如:用户鉴别(FIA_UAU)族:标识和鉴别类的一部分。该族关注用户的鉴别。

C.3.3 组件

组件的例子如:FIA_UAU.3 不可伪造的鉴别,该组件关注不可伪造的鉴别。

C.3.4 元素

元素的例子如:FIA_UAU.3.2,该元素关注防止使用拷贝的鉴别数据。

C.4 扩展的组件

C.4.1 如何定义扩展的组件

无论何时 PP/ST 作者定义一个扩展组件,必须使用类似于已存在 ISO/IEC 15408 组件的方法:清晰、明确、可以评估(可以系统地证实基于该组件的要求是否为 TOE 所保持)。扩展组件必须像已有组件一样使用类似的标签、表达方法和详细级别。

PP/ST 作者也必须确认,扩展组件的所有可用的依赖关系包含在该扩展组件的定义中,可能的依赖关系的例子是:

a) 如果扩展组件引用了审计，则应该必须包括对 FAU：安全审计类的组件的依赖关系；

b) 如果扩展组件修改或访问数据，则可能必须包括(FDP_ACC)族组件的依赖关系；

c) 如果扩展组件使用特定设计描述，则应该必须包括对适当的 ADV：开发族(如功能规范)的依赖关系。

在一个扩展功能组件中，PP/ST 作者也必须在该组件的定义中包含类似已存在的 ISO/IEC 15408-2 组件那样的任何可应用的审计及相关操作信息，在扩展保障组件中，PP/ST 作者也必须为该组件提供适当的类似于 ISO/IEC 18045 中提供的评估方法。

扩展组件可以放在已存在族中，这时，PP/ST 作者必须说明这些族如何变化。如果它们不适于放入现有族中，他们应该放在新的族中。新族必须类似于 ISO/IEC 15408 那样定义。

新族可以放入已有类中，这时，PP/ST 作者必须说明这些类如何变化。如果它们不适于放入现有类，它们就应该放入一个新类。新类必须像 ISO/IEC 15408 那样定义。

附 录 D
（资料性附录）
PP 符合性

D.1 引言

一个 PP 准备用作 ST 的“模版”，就是说：PP 描述了一组用户需求，而与该 PP 符合的 ST 描述了满足那些需求的 TOE。

注意，一个 PP 也可能用作另一个 PP 的模版，这时该 PP 可以声明与其他 PP 符合。这种情况完全类似于 ST 与 PP 的关系。为了清晰，本附录只描述了 ST/PP 的情况，但它也适用于 PP/PP 的情况。

ISO/IEC 15408 不允许任何形式的部分符合，所以如果一个 PP 被声明，则 PP 或 ST 必须完全与所引用的 PP 符合。然而有两种类型的符合（“严格的”和“可论证的”），所允许的符合性的类型由 PP 确定。即 PP 符合性陈述（在 PP 符合性陈述中，见 B.5）允许 ST 声明符合的符合性类型。“严格的”和“可论证的”符合性之间的这种差别单独用于 ST 可以声明对每一个 PP 的符合性上。这可能意味着 ST 与某些 PP 严格符合，与另外一些 PP 可论证的符合。一个 ST 只适用于当 PP 明确允许该 ST 以可论证的方式与该 PP 符合的情况，否则 ST 总是应该与任何 PP 保持严格符合。

换句话重述一下，一个 ST 以可论证的方式与该 PP 符合的情况仅适用于该 PP 明确允许的情况下。

与一个 PP 符合，意味着该 PP 或 ST（如果 ST 是一个被评估产品的，该产品也同样）满足那个 PP 的所有要求。

已发布的 PP 一般需要有 PP 符合性陈述，这意味着声明与 PP 符合的 ST 必须提供对 PP 中描述的一般性安全问题的解决方案，但是可以以等同于 PP 或比 PP 更多限制的方式来进行描述。“等同于或更多限制”的详细定义在 ISO/IEC 15408 中进行了描述，原则上来讲，对所提供的 ST 针对 TOE 采用等价或更多限制、对 TOE 运行环境采用等价或更少限制，那么 PP 和 ST 可以包含完全不同的陈述，使用不同的概念等。

D.2 严格符合性

严格符合性反映 PP 作者，PP 作者要在 PP 中所提出的安全功能要求的证据，ST 是 PP 的一个实例，尽管 ST 能够比 PP 更宽泛。本质上在 TOE 运行环境属于 PP 明确的范围内，ST 定义的 TOE 至少与 PP 相同。

严格符合性体现在典型的例子是：在选择购买产品的时候，期望所要实现的安全功能要严格与 PP 中规定的安全功能要求符合。

与 PP 严格符合的实例化的 ST 仍然可以对 PP 引入附加的限制。

D.3 可论证的符合性

可论证的符合性同样反映 PP 作者，PP 作者要提出证据证明 ST 是对 PP 中描述的一般性安全问题的一个合适的解决方案。

在严格符合性中，PP 和 ST 之间有一个清晰的子集-父集类型的关系，这种关系在可论证的符合中没那么清晰。声明与 PP 符合的 ST 必须提供针对 PP 中描述的一般性安全问题的解决方案，可以以等价或更多限制于 PP 中描述的一般性安全问题的方式来进行。

参 考 文 献

本参考文献包含着 ISO/IEC 15408 读者可能发现有用的更多的参考资料和标准。对于未标明日期的参考书目，建议读者查阅参考文献的最新版本。

ISO/IEC 标准和指南

[1] ISO/IEC 15292 Information technology—Security techniques—Protection Profile registration procedures

[2] [ISO/IEC 15443] Information technology—Security techniques—A framework for IT security assurance-all parts

[3] [ISO/IEC 15446] Information technology—Security techniques—Guide for the production of Protection Profiles and Security Targets

[4] [ISO/IEC 19790] Information technology—Security techniques—Security requirements for cryptographic modules

[5] [ISO/IEC 19791] Information technology—Security techniques—Security assessment of operational systems

[6] [ISO/IEC 27001] Information technology—Security techniques—Information security management systems—Requirements

[7] [ISO/IEC 27002] Information technology—Security techniques—Code of practice for information security management

其他标准和指南

[1] [IEEE Std 610.12—1990] Institute of Electrical and Electronics Engineers, Standard Glossary of Software Engineering Terminology

[2] Common Criteria portal, February 2009.CCRA, www.commoncriteriaportal.org

中华人民共和国
国家标准
信息技术 安全技术
信息技术安全评估准则
第1部分：简介和一般模型
GB/T 18336.1—2015/ISO/IEC 15408-1:2009
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室：(010)68533533 发行中心：(010)51780238
读者服务部：(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 3.75 字数 108 千字
2015年5月第一版 2015年5月第一次印刷
*
书号：155066·1-51494 定价 51.00元

GB/T 18336.1-2015

打印日期：2015年6月20日 F009

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