ICS 35.040
L 80

中华人民共和国国家标准化指导性技术文件

GB/Z 20283—2006

信息安全技术
保护轮廓和安全目标的产生指南

Information security technology—
Guide for the production of Protection Profiles and Security Targets

(ISO/IEC TR 15446:2004, Information technology—
Security techniques—Guide for the production
of Protection Profiles and Security Targets, NEQ)

2006-05-31 发布

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

中华人民共和国
国家标准化指导性技术文件
信息安全技术
保护轮廓和安全目标的产生指南
GB/Z 20283—2006

*

中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.bzcbs.com
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

开本 880×1230 1/16 印张 3.5 字数 102 千字
2006年11月第一版 2006年11月第一次印刷

*

书号:155066·1-28271 定价 22.00 元

GB/Z 20283-2006

前　言

本指导性技术文件与 ISO/IEC TR 15446:2004《信息技术　安全技术　保护轮廓和安全目标产生指南》的一致性程度为非等效。

差异包括：

a) 根据 GB/T 1.1 的要求对第 1 章至第 3 章的内容重新作了编排；

b) 规范性引用文件中将 ISO/IEC 15408:1999 改为 GB/T 18336—2001，并对指导性技术文件中引用的 GB/T 18336－2001 的章条编号进行了一致性处理；

c) 删除了 ISO/IEC TR 15446:2004 中的第 5 章，以及资料性附录 B(一般事例)、附录 C(密码功能说明)和附录 F(可信第三方保护轮廓示例)。

本指导性技术文件的附录 A、附录 B、附录 C 是资料性附录。

本指导性技术文件由全国信息安全标准化技术委员会提出并归口。

本指导性技术文件起草单位：中国信息安全产品测评认证中心。

本指导性技术文件主要起草人：李守鹏、徐长醒、李红阳、刘威鹏、刘晖、付敏、简余良、周瑾。

引　言

GB/T 18336—2001《信息技术　安全技术　信息技术安全性评估准则》基于风险管理的思想，使用保护轮廓(Protection Profile，PP)和安全目标(Security Target，ST)构成灵活科学的安全测评框架，已成为表述安全的事实上的国际语言。本指导性技术文件的目的是帮助开发者、使用者、测评者等更规范更详细地表述安全目标和安全要求。

本指导性技术文件是GB/T 18336—2001的辅助性指南文件，为保护轮廓或安全目标各部分内容的描述及其相互关系提供了技术指南。

本指导性技术文件的使用者应该熟悉GB/T 18336—2001。

本指导性技术文件不解决诸如PP注册以及PP中涉及知识产权保护的问题(如：专利)。

目　次

前言 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　PP 和 ST 概述 …… 1
4.1　简介 …… 1
4.2　PP 和 ST 内容 …… 1
4.3　PP 与 ST 的关系 …… 3
4.4　PP 或 ST 的目标读者 …… 3
4.5　PP 和 ST 的开发过程 …… 3
4.6　PP 族 …… 4
5　PP 和 ST 的描述部分 …… 4
5.1　简介 …… 4
5.2　PP 和 ST 的描述部分 …… 4
6　TOE 安全环境 …… 5
6.1　简介 …… 5
6.2　识别和确定假设 …… 6
6.3　识别和确定威胁 …… 6
6.4　识别和确定组织安全策略 …… 9
7　安全目的 …… 10
7.1　简介 …… 10
7.2　确定 TOE 安全目的 …… 11
7.3　确定环境安全目的 …… 12
8　安全要求 …… 13
8.1　简介 …… 13
8.2　确定 PP 或 ST 中的安全功能要求 …… 14
8.3　确定 PP 或 ST 中的保证要求 …… 20
8.4　环境安全要求 …… 22
9　TOE 概要规范 …… 23
9.1　简介 …… 23
9.2　确定 IT 安全功能 …… 24
9.3　确定安全机制 …… 24
9.4　确定保证措施 …… 24
10　PP 声明 …… 25
10.1　简介 …… 25
10.2　PP 引用 …… 25
10.3　PP 裁剪 …… 25

10.4 PP 附件 …… 25
11 PP 和 ST 基本原理 …… 25
11.1 简介 …… 25
11.2 PP 和 ST 中的安全目的基本原理 …… 26
11.3 PP 和 ST 中的安全要求的基本原理 …… 27
12 复合及部件 TOE 的 PP 与 ST …… 31
12.1 简介 …… 31
12.2 复合 TOE …… 31
12.3 部件 TOE …… 33
13 功能和保证包 …… 34
13.1 背景 …… 34
13.2 确定功能包 …… 34
13.3 确定保证包 …… 35
附录 A(资料性附录) 指南核查表 …… 36
A.1 简介 …… 36
A.2 PP 和 ST 简介 …… 36
A.3 TOE 描述 …… 36
A.4 定义 TOE 安全环境 …… 36
A.5 定义安全目的 …… 37
A.6 确定 IT 安全要求 …… 37
A.7 产生 TOE 概要规范 …… 38
A.8 构建 PP 基本原理 …… 38
A.9 构建 ST 基本原理 …… 38
附录 B(资料性附录) 防火墙 PP 与 ST 示例 …… 39
B.1 PP 与 ST 简介 …… 39
B.2 TOE 描述 …… 39
B.3 安全环境 …… 39
B.4 安全目的 …… 40
B.5 IT 安全要求 …… 40
B.6 TOE 概要规范 …… 41
B.7 PP 声明 …… 42
B.8 PP 基本原理 …… 42
B.9 ST 基本原理 …… 43
附录 C(资料性附录) 数据库 PP 示例 …… 44
C.1 简介 …… 44
C.2 安全环境 …… 44
C.3 安全目的 …… 45
C.4 IT 安全要求 …… 45
C.5 PP 基本原理 …… 46
参考文献 …… 48

信息安全技术
保护轮廓和安全目标的产生指南

1 范围

本指导性技术文件描述保护轮廓(PP)和安全目标(ST)中的内容及其各部分内容之间的相互关系，并在附录中给出了若干实例，供感兴趣的读者参考。

本指导性技术文件给出 PP 和 ST 文档内容的概述、示例目录清单和目标用户最关心的其他内容，并陈述了 PP 与 ST 之间的关系，以及 PP 和 ST 的开发编写过程，为使用者编写 PP 和 ST 提供指导。

2 规范性引用文件

下列文件中的有关条款通过本指导性技术文件的引用而成为本指导性技术文件的条款。凡注明日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本指导性技术文件，然而，鼓励根据本指导性技术文件达成协议的各方研究是否可使用这些文件最新版本。凡是不注日期的引用文件，其最新版本适用于本指导性技术文件。

GB/T 5271.8—2001 信息技术 词汇 第 8 部分：安全(idt ISO/IEC 2382-8:1998)

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 (idt ISO/IEC 15408.1:1999)

GB/T 18336.2—2001 信息技术 安全技术 信息技术安全性评估准则 第 2 部分：安全功能要求(idt ISO/IEC 15408-2:1999)

GB/T 18336.3—2001 信息技术 安全技术 信息技术安全性评估准则 第 3 部分：安全保证要求(idt ISO/IEC 15408-3:1999)

3 术语和定义

GB/T 5271.8—2001、GB/T 18336.1—2001、GB/T 18336.2—2001 和 GB/T 18336.3—2001 确立的术语、定义和缩略语适用于本指导性技术文件。

4 PP 和 ST 概述

4.1 简介

本章提供 PP 和 ST 的概述，总结它们的内容，并讨论两者之间的关系，以及文档开发的流程。参见 GB/T 18336.1—2001 的附录 B 和附录 C。

4.2 PP 和 ST 内容

GB/T 18336.1—2001 的图 B.1 中描述了 PP 中所要求的内容条目。表 1 是 PP 推荐结构的示例目录清单。GB/T 18336.1—2001 的图 C.1 中描述了 ST 所要求的内容条目。表 2 是 ST 推荐结构的示例目录清单。

PP 和 ST 的读者应该很容易地找到所需要的内容在 PP 或 ST 中的位置。

引言部分标识 PP 或 ST 和评估对象(TOE)(包括它的版本号)，并概要描述 PP 或 ST。PP 概述可以被 PP 文档的编目和注册引用。ST 概述可以在公布的已评估的产品列表中被引用。这部分更详尽的讨论参见第 5 章。

TOE 描述提供 TOE(或 TOE 类型)的一般信息，并帮助理解 TOE 的安全要求和预期的使用方法。

ST 的 TOE 描述应该包括 TOE 评估中所用的配置信息。这部分更详尽的讨论参见第 5 章。

TOE 安全环境定义 TOE 所处的环境，尤其是定义 TOE 预期的安全需求。安全环境详细描述用于定义安全需求的所有假设、预期使用的范围、要保护资产所面临的已知威胁(威胁与资产一起描述)以及 TOE 必须遵循的组织安全策略。这部分更详尽的讨论参见第 6 章。

表 1　保护轮廓示例目录清单

1	PP 引言 1.1　标识 1.2　概述
2	TOE 描述
3	TOE　安全环境 3.1　假设 3.2　威胁 3.2　组织安全策略
4	安全目的 4.1　TOE 安全目的 4.2　环境安全目的
5	IT 安全要求 5.1　TOE 安全功能要求 5.2　TOE 安全保证要求 5.3　信息技术(IT)环境安全要求
6	PP 应用注释
7	基本原理 7.1　安全目的基本原理 7.2　安全要求基本原理

表 2　安全目标示例目录清单

1	ST 引言 1.3 与 GB/T 18336—2001 的一致性
6[a]	TOE 概要规范 6.1　TOE 安全功能 6.2　保证措施
7	PP 声明 7.1　PP 引用 7.2　PP 裁剪 7.3　PP 附加项
8	基本原理 8.3　TOE 概要规范基本原理 8.4　PP 声明基本原理
[a] PP 应用注释不包括在安全目标中	

安全目的提供与安全需求对应的一致性声明，既有由 TOE 满足的安全目的，也有由 TOE 环境中 IT 的或非 IT 的措施满足的安全目的。这部分更详尽的讨论参见本指导性技术文件第 7 章。

IT 安全要求定义了对 TOE 的安全功能要求、保证要求和 IT 环境中对 TOE 的所有软硬件或固件的要求，IT 安全要求使用 GB/T 18336.2—2001 和 GB/T 18336.3—2001 中的功能组件和保证组件来描述。这部分更详尽的讨论参见第 8 章。

PP 应用注释是 PP 中一个可选部分，它提供 PP 作者认为有用的附加的信息。值得注意的是，应用注释可能分布在 PP 的相关章节，而不是以单独的章节的形式出现。这部分更详尽的讨论参见第 5 章。

TOE 概要规范是 ST 的一部分，包括由 TOE 提供的用于满足特定安全功能要求的 IT 安全功能，以及所有声明满足特定安全保证要求的保证措施。这部分更详尽的讨论参见第 9 章。

PP 声明是 ST 的可选部分，用于声明 ST 遵循和满足的所有 PP，以及对 PP 内容的补充或裁减。这部分更详尽的讨论参见第 10 章。

基本原理部分论证 PP 或 ST 规范的要求是完整且内聚的，并且满足 ST 的 TOE 能有效地满足安全需求，另外，IT 安全功能措施和保证措施能有效地满足 TOE 安全要求。值得注意的是，基本原理可能分布在 PP 或 ST 的相关章节，而不以单独章节的形式出现。这部分更详尽的讨论参见第 11 章。

注意：基本原理也能够作为一个单独的文档，参见 GB/T 18336.1—2001 的 B.2.8。

4.3 PP 与 ST 的关系

比较表 1 和表 2 的示例目录清单，可以明显看出 PP 与 ST 之间有很多共同之处，特别是在 TOE 安全环境、安全目的和 IT 安全要求，以及基本原理中的相关部分。事实上，如果 ST 简单地声明与某一个 PP 相一致，而没有多余的功能和保证要求，那么 ST 中这些部分的内容可能与 PP 中的对应内容完全一样。在这种情况下，建议 ST 简单地引用 PP 内容，只对与 PP 不同的部分提供详细描述。

ST 中应该对下列 PP 中没有提到的各部分给出详细描述，以反映 ST 的特点，即说明 TOE 如何对确定的安全需求提供解决方案：

a) TOE 概要规范，包括 IT 安全功能、安全措施或技术以及保证强度；

b) PP 声明，论证与所引用 PP 的一致性；

c) ST 基本原理，阐明 IT 安全功能和保证强度足以满足 IT 安全要求。

4.4 PP 或 ST 的目标读者

编写 PP 或 ST 过程中，最具挑战的是如何表达，以使目标读者各得其所：

a) 用户——用户（如高层设计者）需要了解遵循 PP 的 TOE 以安全方式提供哪些相关功能，对于成功的 PP，用户应该是该 PP 的最大读者群；

b) 开发者——开发者（包括 ST 的实现者）需要获得无歧义的安全需求定义，以便去构建符合 PP 的 TOE；

c) TOE 使用者——TOE 使用者（包括安装者、管理员及维护者）需要获得相关的 TOE 安全环境的信息；

d) 评估者——PP 或 ST 评估者需要获得相关的证实 PP 或 ST 技术稳定性和有效性的信息。

PP 或 ST 的不同部分针对不同的读者，各部分要分别撰写。

PP 或 ST 引言、TOE 描述和 TOE 环境等部分主要针对用户，安全目的也主要针对用户。但是，TOE 开发者也应该认真了解 TOE 安全环境和 TOE 安全目的的内容。

PP 中的 IT 安全要求部分主要针对 TOE 开发者，ST 中的 TOE 概要规范部分也主要针对 TOE 的实现者。如果这些部分不是自包含的，那么就应当对相关的内容给出全面而准确的解释。例如，如果 TOE 概要规范的含义依赖于 TOE 安全技术要求，那么就应该明确说明它们的对应关系。

一般 PP 并不直接告诉 TOE 使用者有关 TOE 的信息，但会以适当形式提供基本信息，并用交付和运行保证类（ADO 类）的组件传递这样的信息。使用信息可能出现在 PP 的不同的地方，如：假设、环境目的或对环境要求的部分。

评估者需要熟悉 PP 或 ST 的所有部分。尽管 PP 或 ST 的所有用户对于基本原理都有兴趣，但该部分主要针对评估者，是通常的评估信息。

4.5 PP 和 ST 的开发过程

在 GB/T 18336.1—2001 附录 B 和附录 C 以及 GB/T 18336.3—2001 的第 3 章到第 5 章中，关于 PP 和 ST 要求的陈述，就是建议 PP 与 ST 的开发应该按逻辑顺序以“自上而下”的方式进行，例如，PP

的开发顺序可以是：

a） 定义安全需求；

b） 确认与安全需求对应的安全目的；

c） 定义满足 TOE 安全目的的 IT 安全要求。

不排除可能需要重复表述的情形。例如，定义安全要求时可能会突出表示所要满足的安全目的或安全需求；在验证威胁、安全目的与安全要求和功能之间关系时可能有一定的重复；在描述 PP 或 ST 基本原理时，可能出现更多的重复。

在基本原理中所有已知的、不合逻辑的、不一致的和不对应的问题都被消除后，才能假定 PP 与 ST 是完备的。

在多轮次的 PP 与 ST 的开发过程中，可能出现新的安全需求之外的信息，这就要求以文档形式记录所有改变，从而反映外部环境的变化情况，例如：

a） 识别出新的威胁；

b） 改变组织安全策略；

c） 由于时间和资金的限制，希望由 TOE 担负或由 TOE 环境担负的责任划分发生变化；

d） 对于预期攻击潜力的改变将影响 TOE 的安全环境。

如果 TOE 是已开发好的产品，PP 或 ST 作者可能已经有安全功能要求的明确思考，知道 TOE 将要满足什么要求，那么安全需求和安全目的定义将不可避免地受到 TOE 已提供的安全解决方案的影响，此时 PP 与 ST 开发过程可能例外地以“自下而上”的方式进行。

4.6 PP 族

顾名思义，PP 族是一组紧密相关的 PP，它通常面向于同类的产品和系统（例如，操作系统、防火墙等），因此，开发单个 PP 能够作为开发 PP 族的一部分。PP 族可能面向于：

a） 针对同一类型 TOE 的一系列有层次关系的 PP。这里的层次关系是指，如果 PP 族中的 PP 包括族中另一个 PP 的所有安全要求，那么这两个 PP 被认为有层次关系。

b） 一组用于同一 IT 系统上的不同组件的 PP，例如智能卡 PP 族包括集成电路卡、芯片操作系统、应用、智能卡读卡器等的 PP。

当一个 PP 族应用于一个特定类型的 TOE 时，对于该族中不同成员应该有明显的区别。也就是说，当没有特别声明 TOE 安全环境时，TOE 的安全需求应该有明显的区别，从而使得这些 PP 至少在它们的安全目的方面是不同的，这可以导致选择不同的 IT 安全要求。例如，两个 PP 可能具有相同的安全功能要求（SFR）组件但安全保证要求（SAR）组件不同，这可能由于增加了环境安全导致了较低的保证要求，这种区别应该反映在安全目的中。

当一个 PP 族用于 IT 系统的不同组件时（在特定或假设的环境下），不同 PP 之间的关系应该被澄清。可以参见第 12 章，该章中将讨论为 IT 系统组件定义 PP 的相关问题。

5 PP 和 ST 的描述部分

5.1 简介

本章为 PP 和 ST 描述部分的构建提供指南，即：

a） PP 和 ST 的引言；

b） PP 或 ST 中的 TOE 描述；

c） PP 应用注释。

5.2 PP 和 ST 的描述部分

5.2.1 引言

5.2.1.1 标识

PP 或 ST 标识部分应该能提供足够的信息，惟一地标识出 PP 或 ST，用于 PP 注册或公布已评估产

品列表等目的，标识内容至少包括具有惟一版本的PP或ST名称，以及用于标识TOE的内容（例如，名称和版本号）。PP或ST标识可能还包括下列信息：

a） 关键词（例如，用来识别或检索在注册或产品列表中的安全功能和特征）；

b） 保证组件包[例如，可能是某个评估保证级（EAL）的保证组件包]。

GB/T 18336—2001中未严格规定将EAL放在哪一部分，本指导性技术文件建议将其放引言中，以便于国际互认。

标识部分还需要包括用于开发PP或ST的GB/T 18336—2001的版本信息，以便于版本控制，尽管GB/T 18336—2001没有明确要求这样做。同样，标识部分还需要包括进PP或ST需要的GB/T 18336—2001新的解释或补充信息。

CC一致性声明也因同样的理由可以置于引言中，以便于国际互认，并与GB/T 18336.1—2001中的6.4规定相同。

5.2.1.2 PP概述

根据GB/T 18336—2001的要求，概述部分应该概要性描述PP或ST，可单独用于PP编目和注册或发布已评估产品列表中的ST。该部分应该包括PP或ST所解决的最主要的安全问题，以使目标用户可以判定该PP或ST是否是他感兴趣的。概要部分还应该与PP或ST的技术部分一致。

5.2.2 TOE描述

TOE描述应该包括下列信息（前两种是GB/T 18336—2001要求的，而最后一种是建议性的）：

a） 产品或系统类型；

b） TOE的一般功能；

c） TOE边界（对于PP是可选的）。

除非TOE是特殊的安全产品，否则TOE功能部分仅对安全特征进行描述。如果包括TOE边界和操作环境的描述，那么TOE描述就会更有用。

在PP中，对于TOE边界的可选描述将告诉读者哪些属于TOE，哪些不属于TOE。ST则必须提供对于TOE边界的定义，包括物理边界（硬件、软件组件和模块）和逻辑边界（由TOE所提供的IT特性和安全特性）。

TOE描述对TOE的预期使用者应该易理解，并确保TOE安全功能的描述是清晰的，不致让人误解，例如，不要描述TOE预期范围之外的安全特征或配置。

5.2.3 应用注释

应用注释是PP中的可选项，可以自成一节，也可以将特定注释内容分散到PP的相应部分，例如与安全要求一起描述。应用注释用来提供所有与构成、评估和使用TOE有关或有用的支持信息。应用注释的一个典型应用是提供如何在TOE上下文中解释特定安全要求的说明，或建议ST作者如何在ST中完成操作。如果应用注释被整合到整个PP中，建议清楚地标识出应用注释，以使读者能够清楚地知道它是说明性的文本，而不是SFR或SAR的细化。

6 TOE安全环境

6.1 简介

本章指导说明PP或ST中有关TOE的安全环境。GB/T 18336—2001对PP或ST中这一部分内容的要求参见GB/T 18336.1—2001的B.2.4和C.2.4。在GB/T 18336.1—2001中它们的措辞相同，表明PP或ST的TOE安全环境部分的预期内容差别不大。

TOE安全环境的目的就是定义TOE预期被使用的环境范围和特征，以及预期使用时的方式，例如安全需求由TOE来处理。如图1所示。

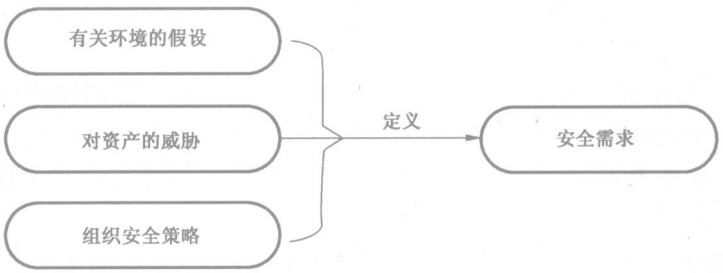

图 1　安全需求的定义

本章包括以下内容的讨论：

a)　对 TOE 安全环境的假设，从而定义出“安全需求”的范围；

b)　需要保护的资产，包括：IT 环境或 TOE 本身典型的信息或资产，以及已知的威胁主体和对资产的威胁；

c)　在处理安全需求时，必须遵循的所有组织安全策略或规则。

PP 或 ST 的后几部分说明 TOE 如何结合操作环境处理安全要求。因此要确保能够清楚明了地定义安全需求，否则可能导致 PP 或 ST 错误地处理安全需求。

在定义安全要求方面，PP 或 ST 文本中一般原理部分的价值在于避免出现有关 TOE 怎样满足安全需求的讨论内容。这样可以帮助读者将注意力集中在安全需求的重要点上，有关安全需求如何被 TOE 满足的讨论最好留给 IT 安全要求来陈述。

6.2　识别和确定假设

GB/T 18336—2001 要求 PP 或 ST 的 TOE 安全环境部分包括安全环境的假设或 TOE 的预期用法的清单。为编辑这样的清单，首先需要回答下面的问题：

对于 TOE 安全环境和安全需求范围，应该做出什么假设？

例如，可能需要给出几个假设来保证某个对资产的潜在威胁实际上是与 TOE 环境无关的。

几种可能的假设类型有：

a)　有关 TOE 预期用法的假设；

b)　TOE 任一部分的环境（例如，物理的）保护假设；

c)　连通性假设，例如将防火墙配置在私网与公网的惟一网络连接点；

d)　人员方面的假设，例如预期的用户权限类型，他们的一般责任以及假设给予这些用户的信任度等。

那些对 PP 与 ST 内容有具体影响的其他假设也可能被包括在内，例如，导致选择某保证要求的假设。虽然 GB/T 18336—2001 要求对已正式认定的假设必须表明受到安全目的的支持，尽管如此，在 PP 或 ST 的描述性或提示性文字中，仍然可能存在无法追溯到安全目的的一般假设。

通常进行一次尝试不太可能完全识别出所有假设，而应该在 PP 或 ST 的整个开发过程中不断识别出更多的假设。特别是在构造 PP 或 ST 基本原理时，例如在阐明安全目的适于对抗已知的威胁时，应该考虑假定是否包含在 PP 或 ST 的陈述中。

在重复采取上述方法识别假设时，应该仔细考虑形成关于有效使用 TOE 安全功能的“假设”，它们可以作为非 IT 环境的安全要求（参见 8.4.2）。它们更适合于作为“人员”的假设来陈述，例如，假设 TOE 具有一个或多个管理员，他们负责确保 TOE 安全功能的正确配置和正确使用。

为方便引用，建议对每个假设进行惟一地标识和编号。

6.3　识别和确定威胁

6.3.1　概述

GB/T 18336—2001 要求 PP 或 ST 包括所有对要保护资产的威胁的描述（参见 GB/T 18336.1—

2001 的 B.2.4),但 GB/T 18336—2001 还指出:如果安全目的仅源于组织安全策略,也就是"安全需求"完全由组织的安全策略和假设来定义,那么就可以忽略威胁陈述。例如,在回应招标书或投标邀请书的 ST 中给出的组织安全策略就属于这种情况。

实际建议如下:在 PP 或 ST 中安全需求被陈述为"威胁"会比陈述为相应的"组织安全策略"要好,因为这有助于对安全需求的理解。另外,如果只使用组织安全策略陈述安全需求,那么可能出现不能及时更新当前威胁的风险。

风险评估的重要意义在于正确地识别资产以及对于资产的威胁,不应该低估风险分析的重要性,如果风险分析做不好,那么:

a) TOE 可能会提供不充分的保护,那么组织的资产就会在不可接受的风险程度下遭受损失;

b) 可能过高估计威胁,从而提高了实现成本及保证要求,并限制了潜在解决方案。

GB/T 18336—2001 没有提供风险分析的框架和组织规范,识别资产威胁的详细讨论也超出了本指导性技术文件的范围,这也是单位风险分析中最难的部分,为了保持本指导性技术文件内容的完整性,下面将陈述有关的一般性原理,另参见 GB/T 18336.1—2001 的第 5 章。有关这一主题的详细指南,读者可参考 ISO/IEC TR 13335 等标准。

6.3.2 识别威胁

6.3.2.1 什么是威胁

在 GB/T 18336.1—2001 的 5.1.1 中描述的威胁是指那些不希望发生的事件,可能由已知的威胁主体引起,而使资产面临风险。注意:对组织安全策略和假设的违背不应该算作风险。

要识别风险是什么,应该回答下列问题:

a) 需要保护的资产是什么?

b) 威胁主体是什么?

c) 需要保护资产免于什么攻击方法或事件造成的损害?

6.3.2.2 识别资产

在 GB/T 18336.1—2001 中的 3.3 定义了资产,资产为由 TOE 策略保护的信息和资源。这样定义是因为它们对于拥有这些资产的个人或组织来说都具有某种内在价值,同样,对于那些试图损害这些资产的威胁主体来说,资产也具有价值,只是它们与资产所有者的兴趣和希望相反,例如造成资产机密性、完整性、可靠性、可鉴别性、可审计性或可用性的丧失。

PP 或 ST 作者所关心的资产可能是某组织的主要资产的某种表现,例如,资产的价值或组织的人员、用户或名誉等。根据 GB/T 18336.1—2001 中 5.1.1 给出的描述,应该使资产的所有者了解谁是保护配置 TOE 的 IT 系统内资产的责任人。实际上,主要资产的所有者可能有多人,他们并不是 TOE 以及 TOE 中所包含信息的所有者。在描述资产时,识别出这些主要所有者对读者是很有帮助的,例如:

a) 在可信第三方系统中,在不同关键之处会有不同的所有者,即可信第三方系统用户也就是可信第三方系统所有者自己;

b) 在医疗系统中,一般来说 TOE 信息的所有者不会只有一人,而是对此有利益的所有的人,因此,对该信息的使用和控制要有复杂的规则和细致的考虑。

GB/T 18336.1—2001 中的 5.1.2 指出资产一般以信息形式通过 IT 系统储存、处理和传输,但应该强调资产也可能扩展到在 IT 环境内的 TOE,如由防火墙或入侵检测系统保护的信息和资源的情形。

GB/T 18336.1—2001 中的 5.3.1 建议已知的资产也可能包括那些不直接受控于安全要求的授权证书和 IT 工具。识别这些"资产"的过程可能成为识别保护重要资产所需措施的过程的一部分。尽管 GB/T 18336—2001 允许,但一般不建议将由 TOE 自身引入的信息资源或那些与主要资产无直接关系的信息和资源明确标识为资产。可能的原因是:

a) 掩盖了 TOE 的主要目的(该目的用于保护主要的资产或该资产在 IT 环境中的其他表现形式);

b) 导致在 PP 或 ST 的早期阶段引入实现细节，即已定义了安全需求的解决办法，使之出现在威胁和安全目的之中。

6.3.2.3 识别威胁主体

如上所述，尽管在 GB/T 18336.1—2001 中的 5.1.1 指出的安全区域中很大的注意力通常放在那些恶意的或与人类活动相关的威胁，但威胁主体既可能是人也可能不是人。

为识别谁是威胁主体，需要考虑：

a) 不论出于什么目的，通过损害资产可能获利的人；

b) 能够损害资产的人，换句话说，就是能够访问处理资产的 IT 系统的人；

c) 那些可能具有技术、机会、可用资源和动机的人或组织，其中可用资源可能是自动攻击或网络嗅探工具等。

非人类威胁源也应该被考虑。非人类威胁源是指不是由人类故意引起的威胁，如系统事故，在非人类威胁源处可能导致资产受损。

6.3.2.4 识别攻击方法

在确定要保护的资产和威胁主体之后，下一步就是识别可能导致资产受损的攻击方法，应该基于对 TOE 环境的了解来确认攻击方法，如：

a) 可能被威胁主体利用的资产潜在的脆弱性；

b) 环境内攻击者的能力。

组织资产潜在的脆弱性可以通过环境脆弱性分析来识别，该分析不在 GB/T 18336—2001 的范围内，PP 与 ST 作者应该注意脆弱性分析不是所有潜在安全漏洞的准确反映，不应该低估新的和未被发现的威胁的可能性。

6.3.2.5 风险分析在威胁识别中的作用

风险分析方法可能在识别威胁过程中有作用，但这种方法在 GB/T 18336—2001 中没有定义。风险分析过程可能与下面两部分有关，一是对 TOE 及其环境的安全目的的识别，二是提出对抗威胁的对策所需的保证级别(参见第 7 章)。可以考虑以下方法：

a) 对资产受到损害的可能性和结果要考虑：

——已知的可能攻击方法；

——攻击成功的可能性；

——可能造成的损害结果，包括成功攻击后有形损失的估计值。

b) 其他如法律要求和费用等约束。

6.3.3 说明威胁

识别出由 TOE 或环境所处理的威胁之后，下一步就是将它们列入 PP 或 ST 中。如前所述，TOE 安全环境部分应该清晰简明地陈述安全需求，本部分将为清晰简明地陈述威胁提供指南。

为了提供清晰的威胁说明，威胁说明应该包括以下细节：

a) 威胁主体(例如，TOE 的授权用户)；

b) 受威胁控制的资产(例如，敏感数据)；

c) 使用的攻击方法(例如，假冒的 TOE 授权用户)。

陈述威胁的具体示例如下：

攻击者可能通过假冒 TOE 的授权用户，未经授权地访问信息和资源。

TOE 的授权用户可能假冒其他 TOE 的授权用户，未经授权地访问信息和资源。

如果将威胁描述与描述项的解释、资产受到的威胁范围、以及威胁主体可能使用的攻击方法一起综合陈述，那么读者就比较容易理解威胁描述。例如，上面示例威胁中，处于风险中的资产是用户或假冒的用户有权访问或获取这些假冒的一系列的信息和资源。

为有助于确保简明描述威胁，威胁描述应该尽可能独立，即：不同威胁之间应该尽可能不重叠。这

样既有助于避免使 PP 或 ST 读者产生混肴，也可以通过避免不必要的重复来简化 PP 或 ST 基本原理。

如果以同样详细程度陈述所有威胁，那么威胁之间的重叠就易于避免。例如，如果特定攻击情节与在 PP 与 ST 的其他部分已陈述的一般威胁有关，那么就不要陈述这样的威胁，因为它描述的是已详细说明了的对特定资产的攻击方法。

每个威胁都应该单独标识以方便引用，可能的标识方式有：

a) 对威胁连续编号（例如，编号为 T1、T2、T3 等）；

b) 用简短而有意义的名称作为威胁的惟一标识。

第一种方式的优点是，编号通常很短，并易于参考。第二种方式的优点是，使用名称作为单独标识，名称具有充分的含义并且容易记忆。然而，在使用第二种标识方式时，由于实际中限制名称中字符数量，并且名称还要含义准确和易于记忆，因此，不可能在所有情况下都分配一个完整定义的标签。

威胁描述应该仅涉及那些可能直接危害被保护资产的事件，因此建议不要使用“TOE 中可能存在安全缺陷”这种空泛的“威胁”。空泛的威胁描述不能帮助读者理解安全需求，因为它们不具有针对性，因此可能被应用于任何 TOE，另外，这类威胁不是由 TOE 或 TOE 环境中的非技术措施来处理的，而是只能由 TOE 的开发者和评估者进行处理。

引入针对威胁的对策可能引入其他间接导致资产损失的攻击，例如对 TOE 安全功能的旁路或篡改攻击。要慎重考虑对资产的间接威胁，要特别注意以下几点：

a) 不要将间接威胁作为 TOE 安全环境，否则会使读者过早涉及 TOE 的实现细节从而产生困惑；

b) 不要将间接威胁陷入已有的威胁范围之内。

例如，如果威胁 X 可能损害资产 Y，那么，对于对抗威胁 X 的防护措施，任何旁路掉这些措施的威胁也可能导致资产 Y 的损害。由于这种旁路威胁是一种已经隐含在威胁 X 内的攻击方法，另外，为使 TOE 安全环境的陈述简单明了，因此，不应该再将它作为单独的威胁显式地陈述出来。

还应该注意到，当需要选择 GB/T 18336—2001 中有依赖关系的组件形成 IT 安全要求时，参见本指导性技术文件的 11.3.4，必须考虑对 TOE 安全措施的攻击方法，比如旁路或篡改攻击。任何对 TOE 安全功能的可行攻击都应该在 TOE 评估期间被全部罗列出来。

6.3.4 完成威胁陈述

GB/T 18336.1—2001 的 B.2.4 要求 TOE 安全环境部分包括所有对与安全 TOE 操作相关资产的威胁。人们最感兴趣的是那些由 TOE 对抗的威胁，这类威胁通常与程序的或非技术的对策有关，但为保证内容的完整性，PP 或 ST 可能需要包括某些不完全由 TOE 对抗的威胁，比如攻击方法或威胁主体针对的目标是 TOE 未提供保护的对象。

例如，与 TOE 安全操作相关但不由 TOE 对抗的威胁可能包括：

a) 对 TOE 的物理攻击；

b) 滥用 TOE 特权用户的信任授权；

c) 由于管理员粗心或不合格培训，造成 TOE 管理及操作不当。

怎样区分由 TOE 处理或由环境处理的威胁，只有在给出安全目的时才能做出判定。

应该注意，已知的环境假设可能排除掉某些威胁，这些威胁可能是与 TOE 安全操作相关的。鉴于此，PP 或 ST 作者有一定的自由度来决定它们是在环境假设中处理，还是在由运行环境对抗的威胁陈述中处理。两种方法都可接受，因为假设和威胁都必须被映射到支持或处理它们的安全目的上。因此，应该主要基于最有助于读者了解安全需求的考虑，在两者之间做出选择。一般的选择规则是：特定攻击应该作为威胁来处理，而更一般形式的攻击最好作为假设来处理。无论采取什么方法，重要的是问题只能被陈述一次。

6.4 识别和确定组织安全策略

GB/T 18336.1—2001 的 B.2.4 要求 TOE 安全环境部分包括所有 TOE 必须遵循的组织安全策略（OSP）的描述，但 GB/T 18336—2001 又指出：如果安全目的仅源于威胁，也就是“安全需求”完全由威

胁来定义，那么，就可以忽略组织安全策略的陈述。

正如本指导性技术文件 6.3 中指出的那样，PP 与 ST 作者应该首先对照已存在的和相关的威胁，审查所有组织安全策略，然后再将策略写入 PP 与 ST。

GB/T 18336.1—2001 的 3.3 将组织安全策略定义为：组织为保障其运转而规定的若干安全规则、程序、规范和指南。OSP 可能需要由 TOE 或其环境或由两者一起实施。

如果 PP 或 ST 指定 OSP 及威胁，那么就应该在 TOE 安全环境部分提供安全需求的简明陈述。如果只包括仅是以不同形式简单重述某个威胁的 OSP，那么这就没有太多用处。通常这种情形仅出现在相关组织强制要求申明的 OSP，而该 OSP 是已存在的威胁的重新声明。

例如，如果已经识别出威胁——“非授权者可能获得对 TOE 的逻辑访问”，再给出如下陈述的 OSP——“必须在 TOE 访问被接纳之前鉴别 TOE 的合法用户”，将不会赋予更多信息内容。

这个 OSP 不仅以不同方式重述这个威胁，而且也重复了用于响应安全需求的安全目的的定义。如果只将问题陈述一次，那么 PP 或 ST 将更清晰易懂。

一般的规则是：当 TOE 预期由特定组织或一类组织使用时，或当 TOE 需要实现一组明显不包含或仅隐含在威胁描述中的规则时，指定出 OSP 才是适当的。如：

a) 标识所使用的信息流控制规则；

b) 标识所使用的访问控制规则；

c) 定义有关安全审计的组织策略；

d) 组织强制的解决技术，例如使用特别批准的密码算法，或与认定的指南相一致的密码算法。

同威胁一样，应该惟一标识每个 OSP 以便于引用。

7 安全目的

7.1 简介

本章提供在 PP 或 ST 中识别和指定安全目的的指南，这方面要求参见 GB/T 18336.1—2001 的 B.2.5和 C.2.5 的描述。

GB/T 18336.3—2001 的 5.4 指出：安全目的应该是对安全问题预期响应的简明陈述，换言之，在安全环境中已经陈述了安全需求，现在必须以安全目的的陈述形式明确地界定出：安全需求是由 TOE 还是由环境来满足或处理的。如图 2 所示：

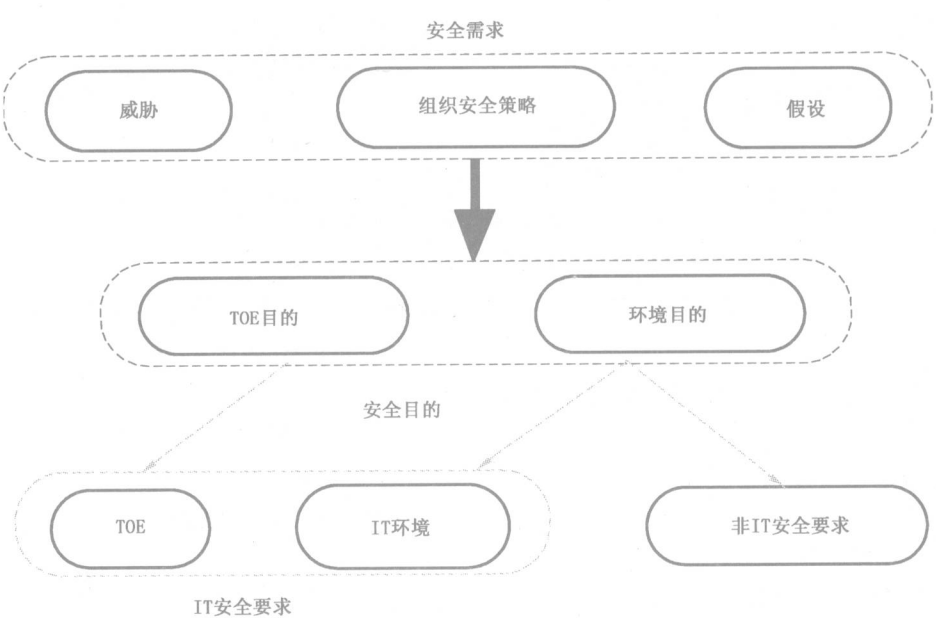

图 2 安全目的的作用

图 2 中明确标识出 GB/T 18336—2001 要求的两种类型的安全目的，它们在 PP 或 ST 中是明确分开的：

a) TOE 的安全目的，由 TOE 实现的技术措施来满足；

b) 环境的安全目的，既要由 TOE 环境实现的技术手段来满足，也要由非 IT 手段来满足（例如，使用程序性的管理或运行规定）。

安全目的明确地划分出了在 TOE 安全环境的上下文中由 TOE 实现和不由 TOE 实现的部分。通过明确地区分由 TOE 或由环境满足安全需求的责任后，需要保护资产的风险能够被有效减小。另外，安全目的不仅划分了职责，而且划定了 TOE 的评估范围，这是由于 TOE 的安全目的将导出由 TOE 实现的安全功能要求，以及 TOE 安全功能要求所需要的保证等级。

7.2 确定 TOE 安全目的

已知的 TOE 安全目的确定 TOE 在对抗威胁和支持 OSP 方面负有什么责任。如图 2 所述，安全目的被认为可以为读者提供从已知的安全需求到安全 IT 要求之间的过渡或桥梁。为确定安全目的定义的详细程度，需要折中考虑以下两方面的要求：

a) 安全目的应该能帮助读者理解由 TOE 处理的安全需求的范围，而不必深入到实现的细节，TOE 安全目的的最好独立于实现。因此，应该重点说明预计达到的结果而不是达到结果的方法；

b) 应该确保已定义的安全目的不是对包含在威胁和 OSP 中内容的重述，或只是形式稍有差异的重述。

实际上，当构成安全目的和安全要求基本原理时，就可以检验出安全目的是否定位在合适的详细程度。如果基本原理的某一步骤太琐碎，而其他步又难于表达，那么安全目的可能太细节化或者太简要了，这依赖于具体的那个步骤是容易表达的。

广义地讲，安全目的处理威胁的方法有以下三种类型：

a) 预防性目的，预防将要发生的威胁或限制威胁实施的途径；

b) 检测性目的，提供手段检测和监视与 TOE 安全操作相关的事件；

c) 纠正性目的，要求 TOE 采取行动响应可能的安全违规或其他不希望的事件，从而保护或恢复 TOE 到安全状态，或限制危险的发生。

预防性安全目的的例子如下，它确定出对 TOE 用户标识和鉴别的需求：

TOE 确保用户在获准访问 TOE 之前惟一地标识每个用户，用户所声称身份是经过鉴别的。

访问控制和信息流控制类安全目的往往属预防性安全目的。在安全需求指出 TOE 应该执行多个访问控制或信息流控制策略的地方，建议为每个策略标识出不同的安全目的，这有助于简化安全要求基本原理。

检测性安全目的的例子如下，它确定出 TOE 要提供源发抗抵赖能力的需求：

TOE 应该提供办法使信息的接收者能够产生用于证明信息来源的证据。

纠正性安全目的的例子如下，它确定出 TOE 响应已检测到的入侵的需求：

根据对即将发生的安全违规事件的检测，采取适当步骤限制攻击，最小化对服务的破坏，服务是指为其他 TOE 用户提供的服务。

如果可能，安全目的应该非形式化地量化所期望的最低有效性，这样就可以将判断有效性级别的问题留在 PP 或 ST 基本原理中解决。量化的描述方法为：

a) 按相对数值，比如环境条件或已有的状态；

b) 按绝对数值。

指定绝对数值当然是最精确的选择，但一般很难按有效性评定出绝对数值。

如果在已知安全功能要求的情况下编写 PP 或 ST，最好一开始就对每个 PP 或 ST 指定的主要安全功能要求组定义出一个安全目的，这种方法的好处是能够简化安全功能原理的构成，如果采用此方