



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 发布
中国国家标准化管理委员会

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

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)。

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。