ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20283—2020
代替 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 15446:2017,Information technology—Security techniques—Guide for the production of protection profiles and security targets,NEQ)

2020-09-29 发布　　2021-04-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

中 华 人 民 共 和 国
国 家 标 准
信息安全技术
保护轮廓和安全目标的产生指南
GB/T 20283—2020
*
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.org.cn
服务热线:400-168-0010
2020 年 9 月第一版
*
书号:155066·1-65501

目　　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准代替GB/Z 20283—2006《信息安全技术 保护轮廓和安全目标的产生指南》，与GB/Z 20283—2006相比，主要技术变化如下：

——修改了保护轮廓和安全目标概述(见第5章，2006年版的第4章)；

——修改了安全目的(见第9章，2006年版的第7章)；

——修改了安全要求(见第11章，2006年版的第8章)；

——修改了TOE概要规范(见第12章，2006年版的第9章)；

——删除了“PP和ST的描述部分”“TOE安全环境”“PP声明”“PP和ST基本原理”和“功能和保证包”(见2006年版的第5章、第6章、第10章、第11章和第13章)；

——增加了“缩略语”“保护轮廓/安全目标引言”“符合性声明”“安全问题定义”“扩展组件定义”“特殊情况”(见第4章、第6章、第7章、第8章、第10章和第14章)；

——删除了“指南核查”“防火墙PP与ST示例”和“数据库PP示例”三个附录(见2006年版的附录A、附录B和附录C)；

——增加了资料性附录“扩展组件定义示例”(见附录A)。

本标准使用重新起草法参考ISO/IEC TR 15446:2017《信息技术 安全技术 保护轮廓和安全目标产生指南》编制，与ISO/IEC TR 15446:2017的一致性程度为非等效。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位：中国信息安全测评中心、北京邮电大学、吉林信息安全测评中心、清华大学。

本标准主要起草人：杨永生、崔宝江、叶晓俊、高金萍、贾炜、王宇航、王峰、邓辉、唐喜庆、蒋显岚。

本标准所代替标准的历次版本发布情况为：

——GB/Z 20283—2006。

引　言

GB/T 18336—2015(所有部分)使用保护轮廓和安全目标构成灵活科学的安全测评框架,已成为表述安全的通用语言。本标准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。

信息安全技术
保护轮廓和安全目标的产生指南

1 范围

本标准给出了保护轮廓和安全目标文档各部分内容的描述，并提供了保护轮廓和安全目标概述、保护轮廓/安全目标引言、符合性声明、安全问题定义、安全目的、扩展组件定义、安全要求、TOE 概要规范、组合及部件 TOE 的保护轮廓和安全目标、特殊情况等信息。

本标准适用于信息技术产品的测试、评估、采购，并为产品的使用者、开发者、测评者使用保护轮廓和安全目标提供指导。

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。

GB/T 18336—2015(所有部分) 信息技术 安全技术 信息技术安全评估准则

GB/T 25069—2010 信息安全技术 术语

3 术语和定义

GB/T 25069—2010 和 GB/T 18336.1—2015 界定的术语和定义适用于本文件。

4 缩略语

下列缩略语适用于本文件。

COTS：商业现成品(Commercial Off the Shelf)

CRL：证书撤销列表(Certificate Revocation List)

DAC：自主访问控制(Discretionary Access Control)

DBMS：数据库管理系统(Database Management System)

EAL：评估保障级(Evaluation Assurance Level)

IT：信息技术(Information Technology)

LDAP：轻量目录访问协议(Lightweight Directory Access Protocol)

OSP：组织安全策略(Organizational Security Policy)

PIN：个人身份识别码(Personal Identification Number)

PKI：公钥基础设施(Public Key Infrastructure)

PP：保护轮廓(Protection Profile)

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)