



中华人民共和国国家标准

GB/T 18336.3—2024/ISO/IEC 15408-3:2022

部分代替 GB/T 18336.3—2015

网络安全技术 信息技术安全评估准则 第3部分：安全保障组件

Cybersecurity technology—Evaluation criteria for IT security—
Part 3: Security assurance components

(ISO/IEC 15408-3:2022, Information security, cybersecurity and privacy
protection—Evaluation criteria for IT security—
Part 3: Security assurance components, IDT)

2024-04-25 发布

2024-11-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目 次

前言	V
引言	VII
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 总述	5
5 保障范式	5
5.1 概述	5
5.2 ISO/IEC 15408 基本方法	5
5.3 保障方法	5
5.4 ISO/IEC 15408 评估保障尺度	7
6 安全保障组件	7
6.1 概述	7
6.2 保障类结构	7
6.3 保障族结构	9
6.4 保障组件结构	9
6.5 保障元素	11
6.6 组件分类	11
7 APE 类:保护轮廓评估	11
7.1 概述	11
7.2 PP 介绍(APE_INT)	12
7.3 符合性声明(APE_CCL)	12
7.4 安全问题定义(APE_SPD)	14
7.5 安全目的(APE_OBJ)	14
7.6 扩展组件定义(APE_ECD)	15
7.7 安全要求(APE_REQ)	16
8 ACE 类:保护轮廓配置评估	18
8.1 概述	18
8.2 PP-模块介绍(ACE_INT)	19
8.3 PP-模块符合性声明(ACE_CCL)	19
8.4 PP-模块安全问题定义(ACE_SPD)	21
8.5 PP-模块安全目的(ACE_OBJ)	21
8.6 PP-模块扩展组件定义(ACE_ECD)	22

8.7	PP-模块安全要求(ACE_REQ)	23
8.8	PP-模块一致性(ACE_MCO)	25
8.9	PP-配置一致性(ACE_CCO)	26
9	ASE类:安全目标评估	28
9.1	概述	28
9.2	ST介绍(ASE_INT)	29
9.3	符合性声明(ASE_CCL)	30
9.4	安全问题定义(ASE_SPD)	31
9.5	安全目的(ASE_OBJ)	32
9.6	扩展组件定义(ASE_ECD)	33
9.7	安全要求(ASE_REQ)	34
9.8	TOE概要规范(ASE_TSS)	36
9.9	复合产品安全目标一致性(ASE_COMP)	37
10	ADV类:开发	38
10.1	规则	38
10.2	安全架构(ADV_ARC)	42
10.3	功能规范(ADV_FSP)	43
10.4	实现表示(ADV_IMP)	50
10.5	TSF内部(ADV_INT)	51
10.6	安全策略模型(ADV_SPM)	54
10.7	TOE设计(ADV_TDS)	56
10.8	复合设计符合性(ADV_COMP)	61
11	AGD类:指导性文档	63
11.1	规则	63
11.2	操作用户指南(AGD_OPE)	63
11.3	准备程序(AGD_PRE)	64
12	ALC类:生命周期支持	65
12.1	规则	65
12.2	CM能力(ALC_CMC)	66
12.3	CM范围(ALC_CMS)	72
12.4	交付(ALC_DEL)	75
12.5	开发者环境安全(ALC_DVS)	76
12.6	缺陷纠正(ALC_FLR)	77
12.7	开发生命周期定义(ALC_LCD)	80
12.8	开发构件(ALC_TDA)	82
12.9	工具和技术(ALC_TAT)	87
12.10	复合部分集成和交付程序一致性核查(ALC_COMP)	89

13	ATE类:测试	90
13.1	规则	90
13.2	覆盖(ATE_COV)	91
13.3	深度(ATE_DPT)	92
13.4	功能测试(ATE_FUN)	95
13.5	独立测试(ATE_IND)	97
13.6	复合功能测试(ATE_COMP)	99
14	AVA类:脆弱性评定	100
14.1	概述	100
14.2	应用注释	101
14.3	脆弱性分析(AVA_VAN)	101
14.4	复合脆弱性评定(AVA_COMP)	105
15	ACO类:组合	106
15.1	规则	106
15.2	组合基本原理(ACO_COR)	109
15.3	开发证据(ACO_DEV)	109
15.4	依赖部件的依赖性(ACO_REL)	112
15.5	组合TOE测试(ACO_CTT)	113
15.6	组合脆弱性分析(ACO_VUL)	115
附录A	(资料性) 开发(ADV)	118
A.1	ADV_ARC:安全架构的补充材料	118
A.2	ADV_FSP:功能规范的补充材料	120
A.3	ADV_INT:TSF内部补充材料	126
A.4	ADV_TDS:子系统和模块	128
A.5	形式化方法补充材料	132
附录B	(资料性) 组合(ACO)	135
B.1	概述	135
B.2	组合TOE评估的必要性	135
B.3	执行组合TOE的安全目标评估	136
B.4	组合IT实体间的交互关系	136
附录C	(资料性) 保障组件依赖关系的交叉引用	141
附录NA	(资料性) 缩略语	146
参考文献		147

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件是 GB/T 18336《网络安全技术 信息技术安全评估准则》的第 3 部分。GB/T 18336 已经发布以下部分：

- 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；
- 第 4 部分：评估方法和活动的规范框架；
- 第 5 部分：预定义的安全要求包。

本文件和 GB/T 18336.4—2024《网络安全技术 信息技术安全评估准则 第 4 部分：评估方法和活动的规范框架》、GB/T 18336.5—2024《网络安全技术 信息技术安全评估准则 第 5 部分：预定义的安全要求包》共同代替 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》。

本文件部分代替 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》。与 GB/T 18336.3—2015 相比，除结构调整和编辑性改动外，主要技术变化如下：

- 更改了术语(见第 3 章,2015 年版的第 3 章)；
- 增加了精确符合性类型(见 7.3.2,8.3.2,8.9.2 和 9.3.2)；
- 删除了评估保障级和组合保障包(见 2015 年版的第 7 章和第 8 章)；
- 增加了直接基本原理的保护轮廓(见 7.7.3 和 9.7.3)；
- 增加了用于模块化评估的 PP-模块和 PP-配置(见第 8 章)；
- 增加了多重保障级评估(见 8.9.2,9.2.2 和 9.7.3)；
- 增加了复合产品评估安全保障组件(见 9.9,10.8,12.10,13.6 和 14.4)。

本文件等同采用 ISO/IEC 15408-3:2022《信息安全、网络安全和隐私保护 信息技术安全评估准则 第 3 部分：安全保障组件》。

本文件做了下列最小限度的编辑性改动：

- 为与现有标准协调，将标准名称改为《网络安全技术 信息技术安全评估准则 第 3 部分：安全保障组件》；
- 增加了资料性附录 NA“缩略语”。

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专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出和归口。

本文件起草单位：中国信息安全测评中心、中国合格评定国家认可中心、公安部第三研究所、中国电子科技集团公司第十五研究所、清华大学、华为技术有限公司、北京天融信网络安全技术有限公司、中国科学院信息工程研究所、复旦大学、武汉大学、吉首大学、浙江大华技术股份有限公司、中科信息安全共性技术国家工程研究中心有限公司、吉林信息安全测评中心、陕西省网络与信息安全测评中心、成都虚谷伟业科技有限公司、安徽中科国创高可信软件有限公司、北京中测安华科技有限公司、荣耀终端有限公司、科来网络技术股份有限公司、医渡云(北京)技术有限公司、北京中电华大电子设计有限责任公司、合肥天帷信息安全技术有限公司、北京数安行科技有限公司、金篆信科有限责任公司。

本文件主要起草人：张宝峰、毕海英、邓辉、高金萍、杨永生、石竑松、谢仕华、贾炜、许源、李凤娟、

GB/T 18336.3—2024/ISO/IEC 15408-3:2022

牛兴荣、李洪、孟亚豪、武腾、董晶晶、叶晓俊、姚俊宁、王龔、刘奇旭、冯云、徐志鹏、程军军、余荣威、李宗寿、应天元、郭昊、刘占丰、胡建勋、闫育芸、明玉琢、苏德财、纪金龙、黄海军、陈泓金、左坚、朱克雷、朱瑞瑾、骆扬、毛军捷、王宇航、陈佳哲、魏伟、梁文韬、刘骥、武建双、刘玉红、薛智慧、伊鹏达、孙蕊刚、吴雅笛、朱业。

本文件于 2001 年首次发布 GB/T 18336.3—2001, 2008 年第一次修订, 2015 年第二次修订, 本次为第三次修订。

引 言

本文件定义的安全保障组件是在安全保障包、保护轮廓(PP)、PP-模块、PP-配置或安全目标(ST)中描述安全保障要求的基础。

这些要求建立了描述评估对象(TOE)保障要求的标准方法。本文件列出了一组保障组件、族和类,还定义了评估 PP、PP-配置、PP-模块和 ST 的准则。

GB/T 18336 拟由五部分构成。

——第 1 部分:简介和一般模型。旨在对 GB/T 18336 进行整体概述,定义信息技术安全评估的一般概念和原则,并给出评估的一般模型。

——第 2 部分:安全功能组件。旨在建立一套可用于描述安全功能要求的功能组件标准化模板。这些功能组件按类和族的方式进行结构化组织,通过组件选择、细化、裁剪等方式构造出具体的安全功能要求。

——第 3 部分:安全保障组件。旨在建立一套可用于描述安全保障要求的保障组件标准化模板。这些安全保障组件按类和族的方式进行结构化组织,定义针对 PP、ST 和 TOE 进行评估的准则,通过组件选择、细化、裁剪等方式构造出具体的安全保障要求。

——第 4 部分:评估方法和活动的规范框架。旨在为规范评估方法和活动提供一个标准化框架。这些评估方法和活动包含在 PP、ST 及任意支持这些方法和活动的文档中,供评估者基于 GB/T 18336 其他部分中描述的模型开展评估工作。

——第 5 部分:预定义的安全要求包。旨在提供利益相关者通常使用的安全保障要求和安全功能要求的包,提供的包示例包括评估保障级(EAL)和组合保障包(CAP)。

本文件的目标读者主要包括安全 IT 产品的消费者、开发者、技术工作组、评估者等。GB/T 18336.1—2024 的第 5 章提供了关于 GB/T 18336 的目标读者,以及目标读者群体如何使用 GB/T 18336 的补充信息。这些读者群体按如下方式使用本文件:

- a) 消费者,选取组件描述保障要求,以满足 PP 或 ST 中提出的安全目的,从而确定所需的安全保障级别时都可使用本文件;
- b) 开发者,在构造 TOE 以响应实际的或预想的消费者安全要求时,可参考本文件,以解释保障要求陈述并确定 TOE 的保障方法;
- c) 评估者,在确定 TOE 的保障级别以及评估 PP 和 ST 时,使用本文件所定义的保障要求作为评估准则的强制性陈述。

注: 本文件在某些情况下使用粗体字和斜体字来区分术语和其余部分文本。族内组件之间的关系约定使用粗体突出显示,对所有新的要求也约定使用粗体字。对于分层的组件,当要求被增强或修改,且超出了前一个组件的要求时,以粗体显示。此外,除了前面的组件之外,任何新的或增强的允许操作也使用粗体突出显示。约定使用斜体来表示具有精确含义的文本。对于安全保障要求,该约定也适用于与评估相关的特殊动词。

网络安全技术 信息技术安全评估准则

第3部分:安全保障组件

1 范围

本文件定义了 ISO/IEC 15408 的保障要求,包括组成 ISO/IEC 15408-5 中包含的评估保障级和其他包的各个保障包,以及 PP、PP-配置、PP-模块和 ST 的评估准则。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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 30270—2024 网络安全技术 信息技术安全评估方法(ISO/IEC 18045:2022, IDT)

ISO/IEC 15408-1 信息安全、网络安全和隐私保护 信息技术安全评估准则 第1部分:简介与一般模型(Information security, cybersecurity and privacy protection—Evaluation criteria for IT security—Part 1: Introduction and general model)

注: GB/T 18336.1—2024 网络安全技术 信息技术安全评估准则 第1部分:简介与一般模型(ISO/IEC 15408-1:2022, IDT)

ISO/IEC 15408-2 信息安全、网络安全和隐私保护 信息技术安全评估准则 第2部分:安全功能组件(Information security, cybersecurity and privacy protection—Evaluation criteria for IT security—Part 2: Security functional components)

注: GB/T 18336.2—2024 网络安全技术 信息技术安全评估准则 第2部分:安全功能组件(ISO/IEC 15408-2:2022, IDT)

ISO/IEC 15408-4 信息安全、网络安全和隐私保护 信息技术安全评估准则 第4部分:评估方法和活动的规范框架(Information security, cybersecurity and privacy protection Evaluation criteria for IT security—Part 4: Framework for specification of evaluation methods and activities)

注: GB/T 18336.4—2024 网络安全技术 信息技术安全评估准则 第4部分:评估方法和活动的规范框架(ISO/IEC 15408-4:2022, IDT)

ISO/IEC 15408-5 信息安全、网络安全和隐私保护 信息技术安全评估准则 第5部分:预定义的安全要求包(Information security, cybersecurity and privacy protection—Evaluation criteria for IT security—Part 5: Pre-defined packages of security requirements)

注: GB/T 18336.5—2024 网络安全技术 信息技术安全评估准则 第5部分:预定义的安全要求包(ISO/IEC 1540-5:2022, IDT)

ISO/IEC IEEE 24765 系统和软件工程 词汇(Systems and software engineering—Vocabulary)

3 术语和定义

ISO/IEC 15408-1、ISO/IEC 15408-2、ISO/IEC 15408-4、ISO/IEC 15408-5、ISO/IEC 18045 和 ISO/IEC IEEE 24765 界定的以及下列术语和定义适用于本文件。