



中华人民共和国国家标准

GB/T 18336.5—2024/ISO/IEC 15408-5:2022

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5部分：预定义的安全要求包

Cybersecurity technology—Evaluation criteria for IT security—
Part 5: Pre-defined packages of security requirements

(ISO/IEC 15408-5:2022, Information security, cybersecurity and privacy
protection—Evaluation criteria for IT security—Part 5: Pre-defined packages
of security requirements, 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	III
引言	V
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 评估保障级	2
4.1 族名	2
4.2 评估保障级概述	2
4.3 评估保障级的目的	4
4.4 评估保障级	4
5 组合保障包	14
5.1 族名	14
5.2 组合保障包概述	14
5.3 组合保障包的目的	15
5.4 CAP 族中的包	16
6 复合产品包	20
6.1 包名	20
6.2 包类型	20
6.3 包概述	20
6.4 目的	20
6.5 安全保障组件	20
7 保护轮廓保障	21
7.1 族名	21
7.2 PPA 族概述	21
7.3 PPA 族目的	21
7.4 PPA 包	21
8 安全目标保障	23
8.1 族名	23
8.2 STA 族概述	23
8.3 STA 族目的	23
8.4 STA 包	23
附录 NA (资料性) 缩略语	25
参考文献	26

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 5 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 18336.3—2024《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》、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》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：

- 删除了保障范型(见 GB/T 18336.3—2015 年版的第 5 章)；
- 删除了安全保障组件(见 GB/T 18336.3—2015 年版的第 6 章)；
- 增加了复合产品包(COMP)(见第 6 章)；
- 增加了保护轮廓保障(PPA)(见第 7 章)；
- 增加了安全目标保障(STA)(见第 8 章)；
- 删除了 APE 类：保障轮廓评估(见 GB/T 18336.3—2015 年版的第 9 章)；
- 删除了 ASE 类：安全目标评估(见 GB/T 18336.3—2015 年版的第 10 章)；
- 删除了 ADV 类：开发(见 GB/T 18336.3—2015 年版的第 11 章)；
- 删除了 AGD 类：指导性文档(见 GB/T 18336.3—2015 年版的第 12 章)；
- 删除了 ALC 类：生命周期支持(见 GB/T 18336.3—2015 年版的第 13 章)；
- 删除了 ATE 类：测试(见 GB/T 18336.3—2015 年版的第 14 章)；
- 删除了 AVA 类：脆弱性评定(见 GB/T 18336.3—2015 年版的第 15 章)。

本文件等同采用 ISO/IEC 15408-5:2022《信息安全、网络安全和隐私保护 信息技术安全评估准则 第 5 部分：预定义的安全要求包》。

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 5 部分：预定义的安全要求包》；
- 增加资料性附录 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)提出并归口。

本文件起草单位：中国信息安全测评中心、中国电子科技集团公司第十五研究所、中贸促信息技术有限责任公司、维沃移动通信有限公司、工业信息安全(四川)创新中心有限公司、吉林信息安全测评中心、国家广播电视总局广播电视科学研究院、北京神州绿盟科技有限公司、国民技术股份有限公司、广东

GB/T 18336.5—2024/ISO/IEC 15408-5:2022

美的制冷设备有限公司、广东省农村信用社联合社、联想(北京)有限公司、中通服咨询设计研究院有限公司、成都虚谷伟业科技有限公司、北京东方金信科技股份有限公司、北京蓝象标准咨询服务有限公司。

本文件主要起草人:张宝峰、许源、杨永生、李凤娟、石竝松、高金萍、刘晖、霍珊珊、刘健、徐曼、李宾、刘尚麟、赵良福、赵珮含、肖丰佳、明玉琢、刘娟、戚进业、姚俊先、李汝鑫、王伟哲、乔华阳、张德保、毕海英、邓辉、贾炜、陈锋、王书毅。

本文件于2001年首次发布为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,部分代替GB/T 18336.3—2015,编号为GB/T 18336.5。

引 言

本文件提供了预定义的安全要求包。安全要求包能有助于标准使用者在评估时保持一致,也能有助于减少开发保护轮廓(PP)和安全目标(ST)的工作量。

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,并给出了评估的一般模型。
- 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,定义了针对 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 的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)。

GB/T 18336.1—2024 定义了术语“包”并描述了基本概念。

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的文本。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的操作也会使用粗体突出显示。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 5 部分：预定义的安全要求包

1 范围

本文件给使用者提供了通用的安全保障要求包和安全功能要求包。

示例：

提供了评估保障级(EAL)和组合保障包(CAP)。

本文件描述了：

- 评估保障级包(EAL),明确规定了可在 PP 和 ST 中引用的预先定义的一系列安全保障组件集,这些组件也用于为 TOE 评估提供适当的安全保障;
- 组合保障包(CAP),明确规定了组合 TOE 评估所需的一系列安全保障组件集;
- 复合产品包(COMP),明确规定了复合产品 TOE 评估所需的一系列安全保障组件集;
- 保护轮廓保障包(PPA),明确规定了保护轮廓评估所需的一系列安全保障组件集;
- 安全目标保障包(STA),明确规定了安全目标评估所需的一系列安全保障组件集。

本文件的读者包括安全信息技术产品的消费者、开发者和评估者。

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 18336.1—2024 网络安全技术 信息技术安全评估准则 第 1 部分:简介和一般模型(ISO/IEC 15408-1:2022,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:简介和一般模型(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:简介和一般模型(ISO/IEC 15408-1:2022,IDT)

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

注:GB/T 18336.3—2024 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(ISO/IEC 15408-3:2022,IDT)

3 术语和定义

ISO/IEC 15408-1、ISO/IEC 15408-3 界定的术语和定义适用于本文件。

注:附录 NA 给出了本文件使用的缩略语。