ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 18336.2—2024/ISO/IEC 15408-2:2022
代替 GB/T 18336.2—2015

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

Cybersecurity technology—Evaluation criteria for IT security—Part 2:Security functional components

(ISO/IEC 15408-2:2022,Information security,cybersecurity and privacy protection—Evaluation criteria for IT security—Part 2:Security functional 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

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2部分。GB/T 18336已经发布了以下部分:

——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。

本文件代替GB/T 18336.2—2015《信息技术　安全技术　信息技术安全评估准则　第2部分:安全功能组件》。与GB/T 18336.2—2015相比,除结构调整和编辑性改动外,主要技术变化如下:

——增加了9个安全功能族,包括:FCS_RBG“随机比特生成”(见10.4)、FCS_RNG“随机数生成”(见10.5)、FDP_IRC“信息保留控制”(见11.8)、FDP_SDC“存储数据的保密性”(见11.13)、FIA_API“身份鉴别证明”(见12.3)、FMT_LIM“有限能力和可用性”(见13.2)、FPT_EMS“TOE辐射”(见15.2)、FPT_INI“TSF初始化”(见15.4)、FTP_PRO“可信信道协议”(见18.3);

——增加了6个安全功能组件(或组件元素),包括:FAU_STG.1“审计数据存储位置”(见8.7.12)、FCS_CKM.5“密钥派生”(见10.2.9)、FCS_CKM.6“密钥销毁的时间和事件”(见10.2.10)、FDP_ETC.2“带有安全属性的用户数据输出”(见11.5.7.4)、FPT_STM.2“时间源”(见15.13.8)、FTA_TAB.1“默认的TOE访问旗标”(见17.5.5.1);

——更改了1个安全功能组件,FCS_CKM.4“密钥销毁”(见10.2.8,2015年版的9.1.8);

——增加了组件的从属关系(见附录B)。

本文件等同采用ISO/IEC 15408-2:2022《信息安全、网络安全和隐私保护　信息技术安全评估准则　第2部分:安全功能组件》。

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2部分:安全功能组件》。

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、公安部第三研究所、国家计算机网络应急技术处理协调中心、中国电子科技集团公司第十五研究所、北京市政务信息安全保障中心、合肥大唐存储科技有限公司、西安邮电大学、蚂蚁科技集团股份有限公司、奇安信科技集团股份有限公司、北京中测安华科技有限公司、上海赴源科技服务有限公司、北京安天网络安全技术有限公司、杭州金智塔科技有限公司、合肥天帷信息安全技术有限公司、中国科学院信息工程研究所、北京邮电大学、杭州安恒信息技术股份有限公司、深信服科技股份有限公司、深圳海云安网络安全技术有限公司、中国软件测评中心、中国汽车工程研究院股份有限公司、科来网络技术股份有限公司、海信集团控股股份有限公司、北京神州绿盟科技有限公司、北京东方金信科技股份有限公司、阿里云科技有限公司、远江盛邦(北京)网络科技股份有限公司。

本文件主要起草人:石竑松、张宝峰、贾炜、杨永生、高金萍、庞博、顾健、郭云峰、顾申、张纪兰、张勇、

白晓媛、张瑜、陈超超、陆臻、武建双、高松、刘昱函、李贺鑫、黄小莉、李静、饶华一、霍珊珊、刘健、牟洁、贺海、谢朝海、叶建伟、陈星、安锦程、叶润国、左坚、冯云、刘彦钊、王伟哲、靳泽、陶小峰、刘雪莉、权晓文、高雪松、唐刚、龙勤、许源、李凤娟、邓辉、毕海英、王蓓蓓、陈佳哲、杨静、魏伟、刘宏伟。

本文件于2001年首次发布为GB/T 18336.2—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

本文件定义的安全功能组件是在保护轮廓(PP)、PP-模块、功能包或者安全目标(ST)中表述安全功能要求或组件的基础。这些要求描述了一个评估对象(TOE)所期望的安全行为,旨在满足在 PP、PP-模块、功能包或者 ST 中规定的安全目的。这些要求描述那些用户通过与 IT 直接交互(例如:输入、输出)或通过 IT 响应能检测到的安全属性。

安全功能组件用于表达安全功能要求,这些要求旨在对抗在 TOE 假设的运行环境中的威胁,和/或覆盖所有的已标识的组织安全策略。

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有安全 IT 产品的消费者、开发者、评估者。GB/T 18336.1—2024 的 5.2 提供了关于 GB/T 18336 的目标读者和目标读者群体如何使用 GB/T 18336 的附加信息。这些群体可以按以下方式使用本文件。

a) 消费者,在选取组件来表述功能要求满足一个 PP、PP-模块、功能包或 ST 中提出的安全目的时,使用本文件。GB/T 18336.1—2024 的第 7 章提供了更多关于安全目的和安全要求之间关系的详细信息。

b) 开发者,在构造 TOE 时响应实际的或预测的消费者安全要求,可以在本文件中找到一种标准方法去理解这些要求。也可以以本文件的内容为基础,去进一步定义满足这些要求的 TOE 安全功能和机制。

c) 评估者,使用本文件所定义的安全功能要求验证在 PP、PP-模块、功能包、ST 中表述的 TOE 功能要求是否满足 IT 安全目的,以及所有的依赖关系是否都已解释清楚并得到满足。评估者使用本文件去帮助确定一个指定的 TOE 是否满足声称的要求。

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。对于有层次关系的组件,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会使用粗体突出显示。约定使用斜体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2部分:安全功能组件

1　范围

本文件定义了安全功能组件所需的结构和内容,以用于安全评估。它包含了一个安全组件的分类目录,来满足许多IT产品的通用安全功能要求。

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:简介与一般模型(ISO/IEC 154081-1:2022,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:简介与一般模型(Information security,cybersecurity and privacy protection—Evaluation criteria for IT security—Part 1:Introduction and general model)

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)

ISO/IEC 18045　信息安全、网络安全和隐私保护　信息技术安全评估准则　信息技术安全评估方法(Information security,cybersecurity and privacy protection IT security techniques—Evaluation criteria for IT security—Methodology for IT security evaluation)

注: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)

3　术语和定义

ISO/IEC 15408-1、ISO/IEC 15408-3 和 ISO/IEC 18045 界定的以及下列术语和定义适用于本文件。

3.1

身份　identity

在TOE中唯一标识实体的表示。

示例:

这种表示是一个字符串。

注1: 实体可能多种多样,例如用户、进程或磁盘。对于用户,这种表示可能是全名、缩写名或唯一的假名。

注2: 一个实体可能有不止一个身份。