ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 18336.1—2024/ISO/IEC 15408-1:2022
代替 GB/T 18336.1—2015

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

Cybersecurity technology—Evaluation criteria for IT security—Part 1:Introduction and general model

(ISO/IEC 15408-1:2022,Information security,cybersecurity and privacy protection—Evaluation criteria for IT security—Part 1:Introduction and general model,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1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 18336.1—2015《信息技术　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》。与GB/T 18336.1—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“精确符合性”类型及相关要求(见6.3.2、10.3、10.8、E.4);

——删除了“低保障的保护轮廓”(见2015年版的B.11);

——增加了“直接基本原理”的术语(见3.34);

——增加了“多重保障评估”的术语(见3.60);

——适用的情况及相关要求(见6.3.4.3、12.5、13.8);

——增加了用于模块化评估的“PP-模块”和“PP-配置”(第11章);

——增加了“复合保障”一章(见第14章);

——增加了“直接基本原理保护轮廓”和“直接基本原理安全目标”内容要求(见B.5、D.4)。

本文件等同采用ISO/IEC 15408-1:2022《信息安全、网络安全和隐私保护　信息技术安全评估准则　第1部分:简介和一般模型》。

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1部分:简介和一般模型》;

——增加了“脚注”(见第1章)。

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、清华大学、公安部第三研究所、中国电子科技集团公司第十五研究所、吉林信息安全测评中心、中国网络安全审查技术与认证中心、中国电子技术标准化研究院、华为技术有限公司、北京大学、中国科学院信息工程研究所、中国网络空间研究院、北京快手科技有限公司、上海观安信息技术股份有限公司、紫光同芯微电子有限公司、科来网络技术股份有限公司、深信服科技股份有限公司、杭州迪普科技股份有限公司、北京中测安华科技有限公司、中贸促信息技术有限责任公司、成都中科至善信息技术有限公司、粤港澳大湾区精准医学研究院(广州)、中通服咨询设计研究院有限公司、马上消费金融股份有限公司、中国软件评测中心、国家计算机网络应急技术处理协调中心、中国航天系统科学与工程研究院、国家广播电视总局广播电视科学研究院、科大讯飞股份有限公司、北京京东尚科信息技术有限公司、OPPO广东移动通信有限公司、长扬科技(北京)股份有限公司、北京赛博英杰科技有限公司。

本文件主要起草人:张宝峰、高金萍、杨永生、石竑松、王亚楠、高松、谢仕华、叶晓俊、上官晓丽、

霍珊珊、郭昊、谢安明、王晓楠、落红卫、李凤娟、许源、孙亚飞、熊琦、庞博、王峰、杨元原、刘健、何阳、刘占丰、冯云、谭儒、孙楠、郑亮、刘吉林、左坚、唐川、谢江、姜伟、吴巍、孔勇、李婧、余明明、盛志凡、谭晓生、赵恬、蒲雄、王小鹏、杨波、陈亮、丁峰、蒋宁、冯娜、赵华、李根、贾炜、毕海英、邓辉、陈锋。

本文件于2001年首次发布为GB/T 18336.1—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

GB/T 18336针对安全评估中的信息技术(IT)产品的安全功能及其保障措施,提供了一套通用的要求,为具有安全功能的IT产品的开发、评估以及采购过程提供指导。基于GB/T 18336的评估过程,为IT产品的安全功能及其保障措施满足这些要求的情况建立一个信任级别,让各个独立的安全评估结果之间具备可比性,评估结果能够帮助消费者确定该IT产品是否满足其安全要求。

GB/T 18336拟由五部分构成。

——第1部分:简介和一般模型。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。建立一套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。建立一套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。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。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具有很大的灵活性,将评估方法应用于对一系列IT产品的一系列安全属性的评估中。因此,用户需谨慎运用GB/T 18336,以避免误用该标准的灵活性。例如,若使用GB/T 18336时采取了不合适的评估方法/活动、选择了不相关的安全属性或针对的IT产品不恰当,都可能导致无意义的评估结果。

因此,IT产品经过评估的事实只有在提及选择了哪些安全属性,采用了何种评估方法的情况下才有意义。评估授权机构需要仔细地审查产品、安全属性及评估方法,以确定对其评估是否可产生有意义的结论。另外,被评估产品的购买方也需要仔细地考虑评估的具体情况,以确定该产品是否有用,且能否满足其特定的使用场景和需求。

GB/T 18336致力于保护资产免遭未授权的信息泄露、数据篡改或丧失可用性。此类保护与三种安全失效情况相对应,通常称为保密性、完整性和可用性。此外,GB/T 18336也适用于这三种情况之外的IT安全的其他方面。GB/T 18336用于考虑人为的(无论恶意与否)以及非人为因素导致的风险。另外,GB/T 18336还应用于IT技术的其他领域,但对安全领域外的适用性不作声明。

对某些问题,因涉及专业技术或对IT安全而言较为次要,因此不在GB/T 18336范围之内,例如下面内容。

a) GB/T 18336不包括那些与IT安全措施没有直接关联的属于行政性管理安全措施的安全评估准则。但是,众所周知某些重要的安全组成部分可通过诸如组织的、人员的、物理的、程序的控制等行政性管理措施来实现。

b) GB/T 18336并不涉及应用本文件的评估方法。

注1:GB/T 30270定义了基础的评估方法,GB/T 18336.4用于从GB/T 30270 5进一步派生评估活动和方法。

c) GB/T 18336不涉及评估管理机构使用本文件的行政管理和法律框架,但GB/T 18336也被用

于此框架下的评估。

d) 评估结果用于产品认可的程序不属于 GB/T 18336 的范围。产品的认可是行政性的管理过程，据此准许 IT 产品(或其集合)在其整个运行环境中投入使用。评估侧重于产品的 IT 安全部分，以及那些直接影响到 IT 单元安全使用的运行环境，因此评估结果是认可过程的重要输入。但是，由于其他技术更适合于评估非 IT 相关属性以及其与 IT 安全部分的关系，认可者应针对这些情况分别制定不同的条款。

e) GB/T 18336 不包括评价密码算法固有质量相关的条款。如果需要对密码算法的数学特性进行独立的评估，则在使用 GB/T 18336 的评估体制中为相关评价制定专门的条款。

注 2：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1部分:简介和一般模型

1　范围

本文件建立了信息技术安全评估的一般概念和原则,并规定了ISO/IEC 15408各部分所给出的一般评估模型,该模型整体上可作为评估IT产品安全属性的基础。

本文件给出了ISO/IEC 15408(所有部分)[1)]的总体概述。它描述了ISO/IEC 15408各个部分内容;定义了各部分使用的术语及缩略语;建立了评估对象(TOE)的核心概念;描述了评估背景和评估准则所针对的目标读者。本文件还给出了信息技术产品评估所需的基本安全概念。

本文件介绍了:

——保护轮廓(PP)、PP-模块、PP-配置、包、安全目标(ST)和符合性类型等核心概念;

——整个模型中安全组件的组织化描述;

——定义了对ISO/IEC 15408-2和ISO/IEC 15408-3给出的功能组件和保障组件定制时允许使用的各种操作;

——在ISO/IEC 18045中给出的评估方法的一般信息;

——ISO/IEC 15408-4应用指南,用以开发源自ISO/IEC 18045的评估方法(EM)和评估活动(EA);

——在ISO/IEC 15408-5中预定义评估保障级别(EAL)的一般信息;

——有关评估体制范围的信息。

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 18336.2—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)

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 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)

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)

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

1)　ISO/IEC 15408-1～ISO/IEC 15408-5分别被采标对应我国国家标准GB/T 18336.1～GB/T 18335.5。