ICS 35.030
CCS L 80

# 中华人民共和国国家标准

GB/T 18336.4—2024/ISO/IEC 15408-4:2022
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4部分:评估方法和活动的规范框架

**Cybersecurity technology—Evaluation criteria for IT security—Part 4:Framework for specification of evaluation methods and activities**

**(ISO/IEC 15408-4:2022, Information security, cybersecurity and pricvacy protection Evaluation criteria for IT security—Part 4:Framework for specification of evaluation methods and activities,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4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 18336.5—2024《信息安全技术　网络技术安全评估准则　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《网络技术　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:

——增加了评估方法和评估活动的一般模型(见第4章);

——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);

——增加了评估方法的结构(见第5章);

——增加了评估活动的结构(见第6章);

——删除了评估保障级(见GB/T 18336.3—2015年版的第7章);

——删除了组合保障包(见GB/T 18336.3—2015年版的第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);

——删除了ACO类:组合(见GB/T 18336.3—2015年版的第16章)。

本文件等同采用ISO/IEC 15408-4:2022《信息安全、网络安全和隐私保护　信息技术安全评估准则　第4部分:评估方法和活动的规范框架》。

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4部分:评估方法和活动的规范框架》;

——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、中国合格评定国家认可中心、中国电子技术标准化研究院、中国网络安全审查技术与认证中心、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、北京邮电大学、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、北京奇虎科技有限公司、国网新疆电力有限公司电力科学研究院、启明星辰信息技术集团股份有限公司、北京神州绿盟科技有限公司、新华三技术有限公司、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、李凤娟、杨永生、许源、高金萍、刘昱函、林阳荟晨、王晨宇、陶小峰、王志远、刘佳、王峰、申永波、张屹、李明轩、张锦川、霍珊珊、孙俊、丁峰、吴大鹏、刘健、张益、权晓文、叶建伟、解伟、万晓兰、谢仕华、毕海英、贾炜、邓辉、王书毅、刘宏伟。

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 18336.4。

# 引　言

本文件的读者对象主要是采用 GB/T 18336—2024 的评估者和确认评估者行为的认证者，以及评估发起者、开发者、PP/ST 作者和其他对 IT 安全感兴趣的团体。

GB/T 18336 拟由五个部分构成。

——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)。

针对信息技术(IT)产品的安全评估，GB/T 18336 提供了一套通用的安全功能及其保障措施要求，从而允许各个独立的 IT 产品的评估结果之间具有可比性。ISO/IEC 18045 为 GB/T 18336 中规定的一些保障要求提供了配套的方法。

本文件描述了一个框架，可用于从 ISO/IEC 18045 的工作单元派生评估活动，并将其分组为评估方法(EM)。评估活动或评估方法可能包含在 PP 和任何支持它们的文件中。当 PP、PP-配置、PP-模块、包或安全目标 (ST)确定要使用特定的评估方法/评估活动时，ISO/IEC 18045 要求评估人员在确定评估者裁定时，遵循并报告相关的评估方法/评估活动。如 GB/T 18336.1 中所述，在某些情况下，评估授权机构能决定不批准使用特定的评估方法/评估活动；在这种情况下，评估授权机构能决定不按照 ST 所要求的评估方法/评估活动进行评估。

本文件还允许为扩展 SAR 定义评估活动，在这种情况下，评估活动的派生与为扩展 SAR 定义的等效行为元素和工作单元相关。如果本文件中引用 ISO/IEC 18045 或 ISO/IEC 15408-3 对 SAR 的使用(如定义评估活动的基本原理时)，那么在扩展 SAR 的情况下，这种引用也将适用于为扩展 SAR 定义的等效行为元素和工作单元。

为简明起见，本文件指定了如何定义评估方法和评估活动，但本身没有规定评估方法或评估活动的实例。

在 GB/T 18336 的其他部分和 GB/T 30270—2024 中出现的下述注描述了在那些文件中关于粗体字和斜体字的使用。本文件没有使用那些惯例，但这里注仍被保留以与其他标准一致。

**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，当其要求被增强或修改，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4部分:评估方法和活动的规范框架

## 1　范围

本文件提供了一个标准化框架,用以规定客观的、可重复的和可重现的评估方法和评估活动。

本文件未规定如何评估、采用或维持评估方法和评估活动。这方面的内容由那些在其感兴趣的特定领域内提出评估方法和评估活动的相关方负责。

## 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。

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 15408-2　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 15408-3　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　信息安全评估方法(Information security, cybersecurity and privacy protection IT security techniques—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 15408-2、ISO/IEC 15408-3 以及 ISO/IEC 18045 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。