



中华人民共和国国家标准

GB/T 45409—2025

网络安全技术 运维安全管理产品 技术规范

Cybersecurity technology—Technical specifications for operation and
maintenance security management products

2025-03-28 发布

2025-10-01 实施

国家市场监督管理总局 发布
国家标准化管理委员会

目 次

前言 III

引言 IV

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 2

5 通则 2

6 安全技术要求 3

 6.1 安全功能要求 3

 6.2 自身安全要求 6

 6.3 安全保障要求 8

7 测试评价方法 9

 7.1 总体说明与测试环境 9

 7.2 安全功能测评 10

 7.3 自身安全测评 16

 7.4 安全保障测评 23

附录 A（规范性） 运维安全管理产品技术要求等级划分和对应测试评价方法 28

 A.1 安全技术要求等级划分 28

 A.2 测试评价方法 29

附录 B（资料性） 运维安全管理产品典型应用场景 31

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。

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：公安部第三研究所、浙江齐治科技股份有限公司、中国科学院软件研究所、华为技术有限公司、上海辰锐信息科技有限公司、中国网络安全审查认证和市场监管大数据中心、国家工业信息安全发展研究中心、奇安信网神信息技术(北京)股份有限公司、北京天融信网络安全技术有限公司、北京神州绿盟科技有限公司、西安交大捷普网络科技有限公司、北京邮电大学、杭州中尔网络科技有限公司、蓝象标准(北京)科技有限公司、远江盛邦(北京)网络安全科技股份有限公司、深信服科技股份有限公司、长扬科技(北京)股份有限公司、杭州安恒信息技术股份有限公司、北京时代新威信息技术有限公司、北京启明星辰信息安全技术有限公司、上海二零卫士信息安全有限公司、中电科网络安全科技股份有限公司、上海观安信息技术股份有限公司、广东安创信息科技有限公司、蓝盾信息安全技术股份有限公司、北京智游网安科技有限公司、陕西省网络与信息安全测评中心、河南中科安永科技有限公司、国网区块链科技(北京)有限公司、广东省信息安全测评中心、广电计量检测集团股份有限公司、内蒙古数字经济安全科技有限公司、国网新疆电力有限公司电力科学研究院。

本文件主要起草人：张艳、邹春明、胡津铭、赵戈、沈亮、徐鹏、吴强、蔡永娟、晏敏、杨晨、王峰、王曦、申永波、王冲华、宋小宝、姜威、周进、何建锋、马向亮、葛方隼、张德保、王成义、刘晨、汪义舟、吴焱、王连强、周瑞群、刘彪、鄢昱恒、谢江、钟英南、刘强、韩云、冯燕飞、郭军武、石竹玉、叶劲宏、唐迪、蔡宇渊、加依达尔·金格斯。

引 言

为落实《中华人民共和国网络安全法》第二十三条,GB 42250《信息安全技术 网络安全专用产品安全技术要求》规定了网络安全专用产品及其提供者均需满足的基线要求。

本文件是 GB 42250 的配套标准。GB 42250 与本文件共同用于指导运维安全管理产品的研发、生产、服务、检测和认证工作。

网络安全技术 运维安全管理产品 技术规范

1 范围

本文件规定了运维安全管理产品的安全功能要求、自身安全要求、安全保障要求及测试评价方法，并提出产品等级划分要求。

本文件适用于运维安全管理产品的设计、研发、生产、服务、检测和认证。

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(所有部分) 网络安全技术 信息技术安全评估准则
- GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
- GB/T 25069 信息安全技术 术语
- GB/T 36626—2018 信息安全技术 信息系统安全运维管理指南
- GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求
- GB/T 39837—2021 信息技术 远程运维 技术参考模型
- GB 42250—2022 信息安全技术 网络安全专用产品安全技术要求

3 术语和定义

GB/T 18336(所有部分)、GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

运维安全管理产品 operation and maintenance security management product

为运维用户提供统一的身份认证接口、多种远程运维管理方式，对资产及其账号等进行集中管理和授权，监控和审计运维操作过程，并对违规操作行为进行报警、阻断的产品。

3.2

运维对象 operation and maintenance object

受运维安全管理产品保护、通过运维安全管理产品进行远程运维管理的信息资产。

注：常见运维对象包括操作系统、数据库管理系统、网络设备、安全设备等。

3.3

运维用户 operation and maintenance user

通过运维安全管理产品对信息资产进行运行维护和管理用户（人员或自动化运维工具）。

注：运维用户通常以账号作为用户标识，账号由运维安全管理产品进行管理维护。

3.4

授权管理员 authorized administrator

对运维安全管理产品自身进行管理的管理人员。

注：授权管理员包括系统管理员、安全管理员、审计管理员，其职责仅限于对运维安全管理产品自身的管理。