



中华人民共和国国家标准

GB/T 45958—2025

网络安全技术 人工智能计算平台安全框架

Cybersecurity technology—Security framework for artificial intelligence
computing platform

2025-08-01 发布

2026-02-01 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

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 安全框架 2

5 安全功能 3

 5.1 资源层安全功能 3

 5.2 调度层安全功能 4

 5.3 应用支撑层安全功能 4

6 安全管理 5

 6.1 身份管理 5

 6.2 密码管理 5

 6.3 日志管理 5

 6.4 安全监测 5

 6.5 安全审计 6

 6.6 风险管理 6

 6.7 个人信息保护 6

7 角色安全职责 6

 7.1 概述 6

 7.2 平台提供方 6

 7.3 数据提供方 6

 7.4 模型提供方 6

 7.5 应用提供方 7

附录 A（资料性） 平台组成与安全风险示例 8

 A.1 平台组成 8

 A.2 安全风险示例 8

附录 B（资料性） 角色描述与典型活动 11

参考文献 12

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：华为技术有限公司、中国电子技术标准化研究院、北京中关村实验室、中国电信股份有限公司、公安部第三研究所、国家信息技术安全研究中心、中国移动通信集团有限公司、四川大学、中国科学院软件研究所、中电长城网际系统应用有限公司、中国科学技术大学、西安电子科技大学、北京火山引擎科技有限公司、北京数字认证股份有限公司、蚂蚁科技集团股份有限公司、中国科学院信息工程研究所、南湖实验室、启明星辰信息技术集团股份有限公司、贝壳找房(北京)科技有限公司、中国电力科学研究院有限公司、浙江大华技术股份有限公司、科大讯飞股份有限公司、国网新疆电力有限公司电力科学研究院、西安交通大学、上海商汤智能科技有限公司、国家工业信息安全发展研究中心、华控清交信息科技(北京)有限公司、北京远鉴信息技术有限公司、北京天融信网络安全技术有限公司、云从科技集团股份有限公司、上海市信息安全测评认证中心、北京快手科技有限公司、国家信息中心、北京数安行科技有限公司、郑州信大捷安信息技术股份有限公司、北京交通大学、华中科技大学、美的集团(上海)有限公司、公安部第一研究所、北京眼神科技有限公司、深圳市洞见智慧科技有限公司、北京银联金卡科技有限公司、国网区块链科技(北京)有限公司、杭州安恒信息技术股份有限公司、奇安信科技集团股份有限公司、中电科网络安全科技股份有限公司、上海燧原科技股份有限公司、中国联合网络通信有限公司广东省分公司、北京山石网科信息技术有限公司、深圳大学、江苏保旺达软件技术有限公司、北京数晟科技有限公司、中国软件评测中心(工业和信息化部软件与集成电路促进中心)、浪潮(北京)电子信息产业有限公司、武汉东湖大数据科技股份有限公司。

本文件主要起草人：葛小宇、严敏瑞、许晓耕、刘勇、张宇光、谷红勋、张侃、徐浩、陆臻、郭晓雷、江为强、张峰、张瑞、陈兴蜀、张立武、闵京华、左晓栋、李兴华、陈妍、袁静、郭建领、张永强、林冠辰、王蕊、荆丽桦、陈治宇、张磊、唐文、王子恬、蒋发群、李陟、胡月、马梦娜、刘栋、郝沁汾、陈炯、王晓辉、李道兴、郑碧煌、张宇、文良君、王宏、谢铮涵、卞超轶、吴晓杰、陈剑波、梅瑞、叶波、杨慧婷、张严、蔺琛皓、邱云翔、俞锦浩、陆一凡、杨韬、王超、王雨晨、吴庚、朱倩倩、王运帷、靳晨、沈超、王雪强、佘剑辉、雷晓锋、杨显森、张俊彦、任永攀、落红卫、谷晨、章恒、王和俊、李昂、刘玉红、刘为华、王伟、刘敬楷、李瑞轩、蔡亚森、王号召、刘军、杨春林、姚明、何浩、彭宇翔、胡师阳、杨波、王栋、杨珂、刘博、李剑锋、安锦程、曹占涛、梅敬青、王思善、曾楚轩、程伟、吴疆、何伊圣、刘伟丽、谢江、葛颂、金银玉、刘云龙、高国鲁、杜乐。

网络安全技术

人工智能计算平台安全框架

1 范围

本文件确立了人工智能计算平台的安全框架,规定了安全功能、安全管理和角色安全职责。
本文件适用于人工智能计算平台的设计、建设、应用和运维。

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 22239—2019 信息安全技术 网络安全等级保护基本要求
- GB/T 31168—2023 信息安全技术 云计算服务安全能力要求
- GB/T 35273—2020 信息安全技术 个人信息安全规范
- GB/T 41479—2022 信息安全技术 网络数据处理安全要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

人工智能计算平台 artificial intelligence computing platform

为人工智能应用开发与运行提供高效、可扩展的资源环境和支撑组件的软硬件系统。

注:人工智能计算平台通常应用于数据中心及边缘计算场景。

3.2

人工智能服务器 artificial intelligence server

为人工智能应用提供高效能计算处理能力的服务器。

注:人工智能服务器通常集成人工智能加速处理器(3.3)、人工智能加速卡(3.4)或人工智能加速模组(3.5),以符合人工智能应用的加速计算需求。

[来源:GB/T 42018—2022,3.5,有修改]

3.3

人工智能加速处理器 artificial intelligence accelerating processor

具备适配人工智能算法的运算微架构,能完成人工智能应用加速运算处理的集成电路。

注:典型的人工智能加速处理器有图形处理器、神经网络处理器和张量处理器。

[来源:GB/T 42018—2022,3.8,有修改]

3.4

人工智能加速卡 artificial intelligence card

专为人工智能计算设计、符合人工智能服务器(3.2)硬件接口,集成了人工智能加速处理器(3.3)或其中的运算微架构的扩展加速部件。