ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 43696—2024

网络安全技术　零信任参考体系架构

Cybersecurity security technology—Zero trust reference architecture

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。

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。

本标准起草单位：奇安信网神信息技术(北京)股份有限公司、中国科学院大学、中国信息通信研究院、中国科学院软件研究所、国家计算机网络应急技术处理协调中心、中国科学技术大学、国家信息技术安全研究中心、北京数字认证股份有限公司、公安部第三研究所、国家信息中心、飞天诚信科技股份有限公司、北京天融信网络安全技术有限公司、江苏易安联网络技术有限公司、国民认证科技(北京)有限公司、启明星辰信息技术集团股份有限公司、深圳竹云科技股份有限公司、格尔软件股份有限公司、海信集团控股股份有限公司、大唐高鸿信安(浙江)信息科技有限公司、腾讯科技(深圳)有限公司、深信服科技股份有限公司、北京芯盾时代科技有限公司。

本标准主要起草人：齐向东、吴云坤、张彬、刘勇、张泽洲、安锦程、荆继武、詹榜华、李新友、张立武、左晓栋、邬怡、韩永刚、金一、孟楠、赵泰、张严、刘丽敏、陈亮、李海玲、陈妍、夏冰冰、国强、黄卉、朱鹏飞、陆舟、刘治平、王龑、秦益飞、杨正权、李俊、韩少波、蒋蓉生、王文路、戴立伟、郑强、何晨迪、高雪松、郑驰、蔡东赟、訾然、孙悦。

网络安全技术　零信任参考体系架构

1　范围

本文件规定了零信任参考体系架构，描述了主体、资源、核心组件和支撑组件以及相互间的关系。

本文件适用于采用零信任体系架构的信息系统的规划、设计、开发、应用、评价。

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 25069　信息安全技术　术语

3　术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

零信任　zero trust

一种以资源保护为核心的网络安全理念。

注：该理念认为主体访问资源时，无论主体和资源是否可信，主体和资源之间的信任关系都需要通过持续状态感知与动态信任评估，从零开始进行构建，以实施端到端安全的访问控制。

3.2

零信任体系架构　zero trust architecture

基于零信任建立的信息系统体系架构。

注：包括构成架构的系统组件，以及组件间关系。

3.3

主体　subject

发起访问请求的实体。

3.4

资源　resource

可供主体访问的对象。

4　典型特征

零信任体系架构具有以下典型特征。

a）　持续状态感知：

持续对主体、资源、环境的相关信息进行采集、分析安全态势。

b）　动态信任评估：

在主体访问资源的过程中，根据持续感知到的主体、资源、环境等安全态势的变化，不断进行信