ICS 35.040
L 80

中华人民共和国国家标准化指导性技术文件

GB/Z 38649—2020

信息安全技术
智慧城市建设信息安全保障指南

Information security technology—
Guide of information security assurance framework for smartcities

2020-04-28 发布　　2020-11-01 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

本指导性技术文件按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本指导性技术文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本指导性技术文件起草单位:浙江省经济信息中心、中国电子技术标准化研究院、中国信息安全测评中心、国家信息中心、中电长城网际系统应用有限公司、中电海康集团有限公司、阿里云计算有限公司、杭州安恒信息技术有限公司、西南科技大学、浙江省发展信息安全测评技术有限公司、浙江省标准化研究院、浙江省电子产品检验所、杭州云嘉云计算有限公司、成都秦川物联网科技股份有限公司、浙江安科网络技术有限公司、深信服科技股份有限公司、浙江鑫诺检测技术有限公司、杭州世平信息科技有限公司。

本指导性技术文件主要起草人:吴前锋、上官晓丽、王惠莅、杜宇鸽、许涛、闵京华、谢海江、张向阳、黄洪、赵一农、范渊、王勃艳、张大江、张君、陈自力、祝利锋、周俊、王世晞、俞群爱、李宁、邵泽华、张亮、齐同军、刘松国、黄晓芹、史锋、麦联韬、方洪波、赵宏凯、黄晓芳、涂万彬。

引　言

智慧城市建设是一项复杂的大型系统工程，其信息安全问题显得尤为重要。智慧城市以海量信息运作与创新理念为特征，互联网、物联网、云计算、移动互联网等均为其重要支撑，因此其信息与网络乃至应用终端的安全问题均比一般互联网的信息安全问题要多，包括隐私问题、可信问题、防伪、业务拒绝(DoS)侵入与攻击问题等。系统的信息感知层、接入与传送层、应用层与终端层、智能/智慧处理及协同平台层等诸多层面存在安全风险；云平台多用户租用的包括知识产权与隐私权保护等问题，给其安全保障带来新挑战；设备无人值守、自适应管理与自断、自通连接等状态，也增加了安全系统的设计与实施难度；智能物体间进行互相识别、互通与交流，需要可靠地确保其信息安全性乃至隐私权等；而且多元异构互联、分布计算等特性导致其安全体系一体化整合难度很大，复杂的社会管理环境等也带来诸多突发性不安全因素。这些不安全因素可能会影响整个城市运行，对信息安全保障提出了更高的要求。为此，需要针对智慧城市的特征，从信息安全管理和技术保障等视角，给出智慧城市建设全过程信息安全保障规范，特制定本指导性技术文件。

本指导性技术文件可用于智慧城市建设各相关单位，有助于信息安全主管部门为智慧城市建设相关单位明确智慧城市建设全生命周期各阶段的信息安全保障要求与责任提供指导，以保障智慧城市建设主体各方的权益，增强抵御风险和自主可控的能力，同时可为智慧城市管理、工程技术及第三方服务等相关人员提供管理和技术参考。

信息安全技术
智慧城市建设信息安全保障指南

1 范围

本指导性技术文件提供了智慧城市建设全过程的信息安全保障指导，包括智慧城市建设从规划与需求分析、设计、实施施工、检测验收、运营维护、监督检查与评估到优化与持续改进的全过程信息安全保障的管理机制与技术规范。

本指导性技术文件适用于智慧城市规划、管理、建设、运营，也可为其他智慧城市建设信息安全相关标准的制定提供依据和参考。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 22080—2016 信息技术 安全技术 信息安全管理体系 要求

GB/T 22081—2016 信息技术 安全技术 信息安全控制实践指南

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—2010 信息安全技术 术语

GB/T 25070—2019 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 34678—2017 智慧城市 技术参考模型

GB/T 36333—2018 智慧城市 顶层设计指南

3 术语和定义

GB/T 22080—2016、GB/T 22081—2016、GB/T 22239—2019、GB/T 25069—2010、GB/T 34678—2017 和 GB/T 36333—2018 界定的以及下列术语和定义适用于本文件。

3.1

安全域 security domain

同一系统内有相同的安全保护需求，相互信任，并具有相同的安全访问控制和边界控制策略的子网或网络，且相同的网络安全等级，共享一样的安全策略。广义可理解为具有相同业务安全要求的 IT 系统要素的集合。

3.2

安全区域边界 secure area boundary

对定级系统的安全计算环境边界，以及安全计算环境与安全通信网络之间实现连接并实施安全策略的相关部件。

3.3

虚拟机 virtual machine；VM

通过软件实现的主机运行环境等。

注：包括虚拟化硬件、操作系统、中间件和应用程序等。