智慧城市安全防护技术方案

目录

[1 前言 4](#_Toc50015682)

[2 智慧城市新常态及框架 4](#_Toc50015683)

[2.1智慧城市新常态 4](#_Toc50015684)

[2.1.1 5G网络是智慧城市的关键基础设施 4](#_Toc50015685)

[2.1.2 云计算赋能智慧城市建设 4](#_Toc50015686)

[2.1.3 物联网设备广泛运用于智慧城市 4](#_Toc50015687)

[2.1.4 网络攻击针对党政机关、智慧城市等重要单位目的性更加明显 5](#_Toc50015688)

[2.2智慧城市网络架构 5](#_Toc50015689)

[2.2.1 应用服务层 5](#_Toc50015690)

[2.2.2 数据平台层 6](#_Toc50015691)

[2.2.3 网络连接层 6](#_Toc50015692)

[2.2.4 边缘计算层 6](#_Toc50015693)

[2.2.5 终端感知层 6](#_Toc50015694)

[3 智慧城市安全风险 6](#_Toc50015695)

[3.1 应用层安全风险 6](#_Toc50015696)

[3.1.1 应用不可用风险 6](#_Toc50015697)

[3.1.2 隐私泄漏风险 7](#_Toc50015698)

[3.2 数据平台层安全风险 7](#_Toc50015699)

[3.2.1 数据泄露风险 7](#_Toc50015700)

[3.2.2 平台被入侵风险 8](#_Toc50015701)

[3.3 网络连接层安全风险 8](#_Toc50015702)

[3.3.1 网络被攻击风险 8](#_Toc50015703)

[3.3.2 无线网络被侵入风险 8](#_Toc50015704)

[3.4 边缘计算层安全风险 8](#_Toc50015705)

[3.4.1 设备被入侵风险 8](#_Toc50015706)

[3.4.2 数据泄漏风险 8](#_Toc50015707)

[3.5 终端感知层安全风险 9](#_Toc50015708)

[4 智慧城市安全架构 10](#_Toc50015709)

[4.1安全技术全景图 10](#_Toc50015710)

[4.1.1网络安全架构图 10](#_Toc50015711)

[4.1.2智慧城市安全技术架构 10](#_Toc50015712)

[4.2智慧城市安全技术详解 11](#_Toc50015713)

[4.2.1身份管理 11](#_Toc50015714)

[4.2.2防泄漏技术 11](#_Toc50015715)

[4.2.3防入侵技术 13](#_Toc50015716)

[4.2.4可用性 14](#_Toc50015717)

[4.2.5防抵赖技术 15](#_Toc50015718)

[4.2.6 5G安全技术 15](#_Toc50015719)

[5 智慧城市安全运营 16](#_Toc50015720)

[5.1应急响应 16](#_Toc50015721)

[5.1.1准备阶段 16](#_Toc50015722)

[5.1.2检测阶段 16](#_Toc50015723)

[5.1.3遏制阶段 17](#_Toc50015724)

[5.1.4根除阶段 17](#_Toc50015725)

[5.1.5恢复阶段 17](#_Toc50015726)

[5.1.6跟踪阶段 17](#_Toc50015727)

[5.2红蓝对抗 17](#_Toc50015728)

[5.2.1常见的蓝军攻击技术 18](#_Toc50015729)

[5.3漏洞管理 18](#_Toc50015730)

[5.3.1发现漏洞 19](#_Toc50015731)

[5.3.2漏洞评估与修复 19](#_Toc50015732)

[5.4威胁情报 20](#_Toc50015733)

[6 智慧城市安全管理 21](#_Toc50015734)

[6.1网络安全组织结构 21](#_Toc50015735)

[6.2人员权限管理 21](#_Toc50015736)

[6.3数据管理 22](#_Toc50015737)

[6.3.1数据采集 23](#_Toc50015738)

[6.3.2访问隔离 23](#_Toc50015739)

[6.3.3传输安全 23](#_Toc50015740)

[6.3.4存储安全 24](#_Toc50015741)

[6.3.5数据处理 25](#_Toc50015742)

[6.3.6数据交换 25](#_Toc50015743)

[6.3.7数据删除与销毁 25](#_Toc50015744)

[7 智慧城市安全合规（目前国家要求和如何符合国家法律法规） 26](#_Toc50015745)

[7.1安全政策 26](#_Toc50015746)

[7.2安全标准 27](#_Toc50015747)

[8 智慧城市安全未来展望 27](#_Toc50015748)

# 1 前言

智慧城市利用5G、物联网、云计算、大数据、AI和边缘计算等信息技术，促进了城市中的信息融合，为社会的发展、政府职能的转变提供了新手段新方法，也方便市民的工作生活，使城市逐步向绿色、低碳的方向发展。智慧城市发展新动能的同时，也带来新的安全风险。在智慧城市的不同层面，如应用层、数据平台层、网络连接层、边缘计算层和终端感知层中，存在隐私泄漏、流量不可信、拒绝服务（DoS）侵入与攻击问题等。安全威胁的存在可能会影响整个城市的运行，给智慧城市的建设带来了巨大的挑战。

本技术方案主要分析了智慧城市的基础设施、物联网设备以及云计算在智慧城市中的实践，智慧城市的网络架构以及存在的安全风险，并提出对应的安全参考架构、安全技术方案和安全运营、管理建议，保障智慧城市建设的安全，增强抵御风险的能力。

# 2 智慧城市新常态及框架

## 2.1智慧城市新常态

### 2.1.1 5G网络是智慧城市的关键基础设施

5G是数字经济时代的一种通用技术，这种通用技术具有普遍性，将被城市中的各个行业广泛应用。在5G网络的广泛应用之下，智慧城市的各个行业将被深刻的改变，自动驾驶将广泛应用于城市交通，为居民提供低碳高效的同行服务；远程医疗将改变医疗资源分配的格局，推动城市医疗的公平发展；人工智能安防监控将创造更安全的社区环境；数据智能的普及将推动政府社会治理的高效和精准，以及城市经济运行的智能洞察。这一切都将随着5G把每个城市部件、每一位城市居民、每一个城市组织变成数字化的智能体。

### 2.1.2 云计算赋能智慧城市建设

当前，云计算在政务、金融、医疗等领域的应用正如火如荼。就智慧城市建设而言，云计算、物联网、大数据技术几乎无可替代。在构建智慧城市的过程中，以社会民生服务领域为重点，建立社会服务云平台，可以提高城市各项事业的精细化管理水平，并为城市公共事务管理部门及时获取各项信息提供有力的技术支撑。

### 2.1.3 物联网设备广泛运用于智慧城市

智慧城市的构建离不开物联网技术的支撑。首先，智慧城市的实现有赖于大量物联网设备采集数据。其次，城市的智能之处绝不局限于计算层面，而要更多需要为本地产业、人与自然的关系等方面注入动力，通过物联网设备大幅改善和提升智慧转型和提升城市竞争力。

AI应用、边缘计算

### 2.1.4 智慧城市网络安全需求愈发凸显

国家计算机网络应急技术处理协调中心发布的《2019年中国互联网网络安全报告》中提到， 2019年，我国持续遭受来自“方程式组织”“APT28”“蔓灵花”“海莲花”“黑店”“白金”等30余个APT（高级持续性威胁攻击）组织的网络窃密攻击，国家网络空间安全受到严重威胁。境外APT组织不仅攻击我国党政机关、智慧城市、国防军工和科研院所，还进一步向军民融合、“一带一路”、基础行业、物联网和供应链等领域扩展延伸，电信、外交、能源、商务、金融、军工、海洋等领域成为境外APT组织重点攻击对象。

黑客针对党政机关、关键信息基础设施等重要单位发动攻击的组织性、目的性更加明显。作为掌握城市核心数据的智慧城市项目，更要加强防护能力。

## 2.2智慧城市网络架构



智慧城市技术框架可以分为四个维度五个层面。包括云（应用服务层和数据平台层，其中数据平台层包括行业平台层和数据中台层），管（网络连接层），边（边缘计算层），端（终端感知层）。

### 2.2.1 应用服务层

应用服务层是整合行业相关资源，打包成智慧城市解决方案，如智慧农场、智慧安防等。为社会公众、企业用户、城市管理决策者提供全面的信息化智慧服务。

### 2.2.2 数据平台层

数据平台层包括行业平台侧和数据中台层。行业平台侧指基于AI、数据等能力打造的相关行业共享平台，如政务云平台，工业互联网平台等。数据中台层指数据存储位置（数据湖），AI算力，视频识别等云计算的SAAS层。数据平台层可以对外提供成熟的技术能力和行业平台，为智慧城市提供能力平台。

### 2.2.3 网络连接层

网络连接层包括互联网、5G无线通信网络、VPN等网络，为智慧城市提供大容量、高带宽、高可用的网络通信基础设施。

### 2.2.4 边缘计算层

边缘计算层是靠近端和数据源的网络边界侧，融合网络、计算、存储等分布式能力。可以就近提供智能服务。

### 2.2.5 终端感知层

终端感知层包括面向消费者和面向企业（TO C/B），包括普通消费者的智能终端（手机、电脑等），面向智慧城市的感知终端（如数据收集的互联网设备，智慧交通灯等）。

# 3 智慧城市安全风险

智慧城市安全风险主要分为以下五个方面：应用层安全风险，数据平台层安全风险，网络连接层安全风险，边缘计算层安全风险和终端感知层安全风险。

## 3.1 应用层安全风险

### 3.1.1 应用不可用风险

智慧城市应用多，涉及到政务、医疗、交通、教育等多个方面，用户涉及到政府部门员工、企业以及个人。这些应用如果因为自身健壮性原因或外来攻击导致不可用，将影响智慧城市正常运行，带来不良社会影响。

疫情的爆发使得远程办公软件、远程会议等软件的使用量急剧增加。大量远程控制工具的使用和端口的开放加大了网络被攻击的安全风险。（改成应用不可用的风险）

### 3.1.2 数据泄漏风险

应用层输入界面或展示界面各种数据，并且会涉及到用户隐私，一旦数据泄露将造成恶劣的影响。黑客通过技术手段异常访问智慧城市功能页面或接口来获取数据，通过数据的关联与桥接，把数据分析出具有更高风险敏感数据。

即使只是供内部合法用户使用的业务应用，也存在着隐私泄露的风险。例如内部员工作案：数据篡改、数据窃取、终端使用权不可控、研发人员植入应用层后门窃取数据、内部人员利用应用层中转窃取数据等。

## 3.2 数据平台层安全风险

### 3.2.1 数据泄露风险

数据平台层存储城市的各类数据，如城市运行信息、企业居民信息，以及大数据分析和人工智能运算的结果，数据机密性高。所以在安全方面首先要关注数据的安全，确保数据不被泄露篡改，保障数据的机密性、完整性和可用性。数据泄露风险主要有以下几方面：

（1）安全机制缺陷：Hadoop生态架构在设计初期对用户身份鉴别、访问控制、密钥管理、安全审计等方面考虑较少，并且大数据应用中多采用第三方开源组件，对这些组件缺乏严格的测试管理和安全认证。（改）1、安全技术。2、权限管理。3、数据管理

（2）数据应用访问控制难度大：数据应用有报表类、运营类、取数类等等，各类数据应用通常要为不同身份和目的的用户提供服务，在身份鉴别、访问控制、审计溯源上都带来了巨大的挑战。

（3）数据量大、潜在价值高，极易成为攻击目标：大数据平台处理环节多，需要针对数据采集、传输、存储、处理、交换和销毁等生命周期各阶段进行安全防护，在不同阶段采取适合的安全技术保护机制。

（4）数据滥用或伪脱敏风险增长：随着数据挖掘、机器学习、人工智能等学科领域技术研究的深入，数据滥用情况加剧。并且很多脱敏或者加密处理的数据，仍有可能分析出对应的真实明文信息。

（5）数据所有者权限问题突显：数据共享和流通是大数据发展的关键，但是在很多大数据应用场景中，存在数据所有权不清晰的情况，例如：数据挖掘分析人员会对原始数据进行处理，分析出新的数据，这些数据的所有权到底属于原始数据所有方还是数据挖掘方，这个问题还很多场景下还没有定论。

### 3.2.2 平台被入侵风险

平台涉及网络设备、计算设备、存储设备、以及各种对外接口容易被黑客入侵，因此要防止通过网络或者 API 接口调用等渠道入侵应用平台和技术中台系统，造成设备无法正常工作或数据丢失。

## 3.3 网络连接层安全风险

### 3.3.1 网络不可用

网络设备因存在漏洞、弱密码等问题被攻击、被控制或被DDoS攻击，造成网络无法正常工作。当网络设备自身可靠性不足，或者物理破坏也会导致网络不可用。

### 3.3.2 无线网络被侵入风险

网络连接通常采用无线连接的方式，例如物联网数据回传、Wi-Fi网络覆盖等。由于无线网络的开放性，容易被非法入侵获取用户信息。5G核心网作为智慧城市5G网络的神经中枢，它的安全是整个网络安全的重中之重。

## 3.4 边缘计算层安全风险

### 3.4.1 设备被入侵风险

边缘计算层收集来自物联网设备的数据，并进行处理。可能存在密码管理不当而造成的入侵，也可能存在边缘计算层设备被攻击的风险，导致底层收集的数据无法上传和处理。

### 3.4.2 数据泄漏风险

边缘计算的数据处理实时性、数据多源异构性、终端资源受限性和接入设备复杂性，使得传统云计算环境的安全机制不再适用于边缘设备产生的海量数据的安全防护，边缘计算的数据存储安全、共享安全、计算安全、传输和隐私保护等问题成为边缘计算模型必须面对的挑战性问题。

## 3.5 终端感知层安全风险

终端感知层包括面向消费者和面向企业，包括普通消费者的智能终端，面向智慧城市的感知终端。对于一个企业来说，90%以上的员工需要每天使用PC终端办公，而终端是和互联网“数据交换”的重要节点，且员工的水平参差不齐，因此企业网络中80% 的安全事件来自于终端。终端已经成为黑客的战略攻击点。

黑客攻击的目的是获取有价值的“数据”。黑客控制终端以后，可以直接种植勒索病毒勒索客户，更严重的是，黑客的目标往往是那些存储着重要“数据”的服务器。受控的终端将成为黑客的跳板，黑客将通过失陷主机横向扫描内部网络，发现组织网络内部重要的服务器，然后对这些重要服务器发起内部攻击。因此终端自身要在软硬件方面做好安全加固与安全防护，避免外部入侵对终端造成破坏或者信息窃取。

互联网出口实现了组织内部网络与互联网的逻辑隔离。对于内部网络接入用户来说，僵尸网络是最为严重的安全问题，黑客利用病毒木马蠕虫等多种入侵手段控制终端，形成僵尸网络。僵尸网络可以在任何时候对任何目标发动DDoS攻击。僵尸的感染对象已经从服务器、PC、智能手机，扩展向摄像头、路由器、家居安防系统、智能电视、智能穿戴设备，甚至是婴儿监视器，存在大量漏洞的终端IOT设备成为了僵尸网络主要目标。被感染木马后存在对外DDoS、对外扫描、远程命令执行等风险。黑客可以利用僵尸网络展开更多的危害行为，如APT攻击最常采用的跳板就是僵尸网络。黑客利用僵尸网络来实现渗透、监视、窃取敏感数据等目的，危害非常大。

# 4 智慧城市安全技术

## 4.1安全技术全景图

### 4.1.2智慧城市安全技术架构



基于2.2智慧城市网络架构分层，在应用服务层、数字平台层、网络连接层、边缘计算层和终端感知层有针对性地部署网络安全防护组件（或服务）。并针对身份管理、防泄漏、防入侵、可用性、防抵赖、安全管理和安全运营等场景进行安全防护。

## 4.2智慧城市安全技术详解

安全技术可以分为身份管理、防泄漏、防入侵、可用性和防抵赖。

### 4.2.1身份管理

用户登录网站或公司系统时，会产生很多用户自身注意不到的信号，包括用户所处位置、设备IP地址、输入节奏等等。如果用户使用的是移动设备，这些信号甚至更多，比如用户戳手机屏幕的力度等等。同样地，每个联网设备都有自身基于典型使用模式的各种信号。

收集并分析这些信号，可以让身份管理系统能够为每个用户和设备创建特定的身份资料。然后就可以设置确定性阈值，标识什么等级的置信度可以允许访问。从授权的角度看，这么做可以大幅提高访问授权或拒绝操作的准确性。相比于单因子认证的不安全性和双因子的繁琐，通过隐藏信息分析认证可以减少验证麻烦并保障安全性。

同时身份管理需要对权限分级，建立账号生命周期（入职/离职/调职，密码定期更新）、账号安全审计（记录日志）机制。

以上技术可以运用在身份鉴别、权限管理、口令管理、设备接入和远程管理上。

### 4.2.2防泄漏技术

防泄漏技术包括数据加密、数据销毁、日志审计、数据分级、数据脱敏、API安全、边界防护、流量预警和风险控制等技术。

#### 4.2.2.1数据管理

敏感数据（如身份证，手机号等）存储时通过加密算法和加密密钥将明文转变为密文。防止数据库被入侵导致数据泄露。

#### 4.2.2.2数据销毁

敏感数据需要设定有效期，数据过期后要对数据进行自动删除，防止过期冗余数据意外泄漏。必要时可对磁盘进行覆写或物理损毁达到数据销毁的目的。

#### 4.2.2.3日志审计

日志审计能够实时记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行告警，对攻击行为进行阻断。它通过对用户访问数据库行为的记录、分析和汇报，用来帮助用户事后生成合规报告、事故追根溯源，同时加强内外部数据库网络行为记录，提高数据资产安全。

#### 4.2.2.4数据分级

数据分级目的在于确定各类型数据的敏感程度，从而为不同类型数据的开放和共享策略的制定提供支撑。

#### 4.2.2.5数据脱敏

数据脱敏是指对某些敏感信息通过脱敏规则进行数据的变形，实现敏感隐私数据的可靠保护。在涉及客户安全数据或者一些商业性敏感数据的情况下，在不违反系统规则条件下，对真实数据进行改造并提供测试使用，如身份证号、手机号、卡号、客户号等个人信息都需要进行数据脱敏。

#### 4.2.2.6 API安全

APP、前后端分离项目都采用API接口形式与服务器进行数据通信，传输的数据被偷窥、被抓包、被伪造时有发生。需要有Token授权认证，防止未授权用户获取数据；时间戳超时机制；URL签名，防止请求参数被篡改；防重放，防止接口被第二次请求，防采集；采用HTTPS通信协议，防止数据明文传输；API频率限制，防止批量访问导致数据泄露。

#### 4.2.2.7边界防护

在网络安全的建设过程中，边界安全一直是一个最重要的安全问题。所谓的边界，一般是网络划分区域后，在不同信任级别的安全区域之间形成的。由于信任级别高低不同，因此需要通过相应的技术来进行安全隔离，从而实现对各个安全区域进行安全防护。常见的边界防护技术有防火墙、IPS、WAF等。

#### 4.2.2.8流量预警

对网络激增流量进行预警，尤其是从内部大量数据流出。

#### 4.4.4.9业务风险控制

业务风控是基于业务场景，结合IP画像、设备指纹、黑卡检测、威胁情报等多维度信息实时识别风险的专业防护产品，有效识别和解决渠道推广、账号安全、支付安全、营销活动、爬虫流量等作弊问题，通过对于风险和网络流量的判别，避免智慧城市出现信息泄露。

### 4.2.3防入侵技术



#### 4.2.3.1网络入侵防护系统

网络入侵防护系统通过旁路部署方式，无变更无侵入地对网络4层会话进行实时阻断，并提供了阻断 API，方便其他安全检测类产品调用。同时支持串联网络实时拦截的部署方式。此外，网络入侵防护系统提供全量网络日志存储和检索、安全告警、可视化大屏等功能，帮助客户解决等保合规、日志审计、行政监管、以及云平台管控等问题。

常见网络入侵保护系统包括IPS和WAF。WAF是一系列针对性优化算法的高级 Web 应用防火墙。采用正则规则和语义分析的双引擎架构，对 SQL 注入、跨站攻击、命令和代码注入、目录遍历、扫描器、恶意bot、webshell、CC 等攻击实现实时的高性能防护。

IPS (入侵防御系统)是对防病毒软件和防火墙的补充。入侵防御系统是一部能够监视网络或网络设备的网络资料传输行为的计算机网络安全设备，能够及时的中断、调整或隔离一些不正常或是具有伤害性的网络资料传输行为。

#### 4.2.3.2主机入侵保护系统

主机入侵保护系统可以提供提供资产管理、漏洞管理、基线检查、入侵检测等功能，能够帮助智慧城市更方便地管理主机安全风险，实时发现并阻止黑客入侵行为，以及满足等保合规的要求。主机入侵保护系统包括资产管理、漏洞管理、基线检查、账号破解防护、双因子认证、关键文件变更检测、恶意程序检测、网页后门检测和网页防篡改。

#### 4.2.3.3容器安全入侵保护系统

容器安全入侵保护系统能够扫描镜像中的漏洞与配置信息，帮助智慧城市解决传统安全软件无法感知容器环境的问题；同时提供容器进程白名单、文件只读保护和容器逃逸检测功能，有效防止容器运行时安全风险事件的发生。

#### 4.2.3.4安全日志和事件管理系统

安全日志和事件管理系统拥有完善的安全日志管理要求、安全事件定级处置流程和7\*24小时的专业安全事件响应团队以及对应的安全专家资源池来应对。应急响应团队秉承快速发现、快速定界、快速隔离与快速恢复的安全事件响应原则。同时，根据安全事件对整网、智慧城市服务的危害刷新事件定级标准以及响应时限和解决时限等要求。

代码检测

### 4.2.4可用性

为保障网络/应用/系统可用性，需要进行数据容灾备份、网络隔离和DDOS高防。

#### 4.2.4.1容灾备份

容灾是为了在遭遇灾害时能保证信息系统能正常运行，帮助智慧城市实现业务连续性的目标，备份是为了应对灾难来临时造成的数据丢失问题。在容灾备份一体化产品出现之前，容灾系统与备份系统是独立的。容灾备份产品的最终目标是帮助智慧城市应对人为误操作、软件错误、病毒入侵等“软”性灾害以及硬件故障、自然灾害等“硬”性灾害。

#### 4.2.4.2网络隔离

云环境中南北向的数据通过防火墙的策略规则可以做到网络隔离，而东西向的数据，就会绕开防火墙。在过去，主要通过防火墙、虚拟本地网和访问控制列表做网络隔离。传统防火墙，一般是在防火墙上线部署的时候配置上相应的策略、防火墙隔离、策略的管理和隔离的动作都是发生在防火墙设备上的。现在可以使用虚拟化微隔离来实现东西向网络隔离。

#### 4.2.4.3 DDoS高防

DDoS高防是针对互联网服务器在遭受大规模DDoS/CC攻击后导致服务不可用的情况下，推出的服务。用户可通过高防系统提供保护，确保关键业务连续性，广泛应用于政企门户、电商、游戏等场景。防DDoS设备可以精准有效地实现对流量型攻击和应用层攻击的全面防护，提供精细化的抵御 DDoS 攻击的功能，包括但不限于 Ping Flood、SYNFlood、UDP Flood、Challenge Collapsar（CC）、HTTP Flood、DNS Flood。

### 4.2.5防抵赖技术

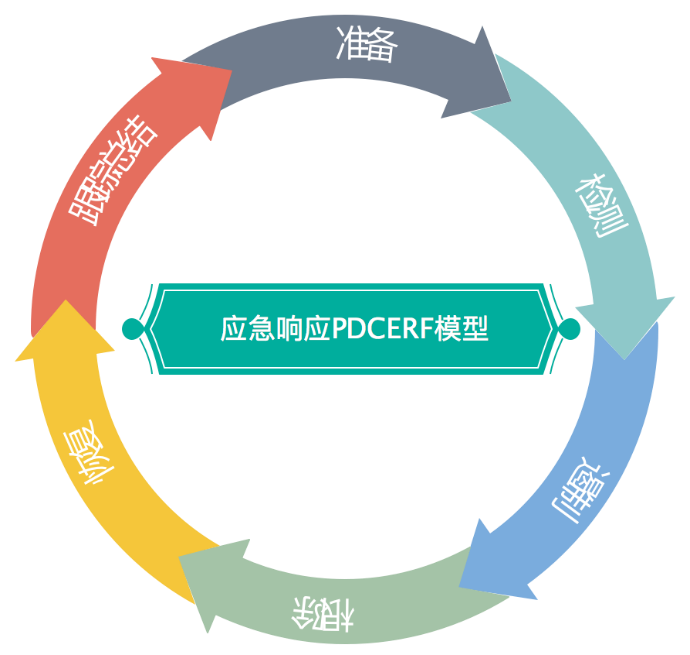
包括对源和目的地双方的证明，常用方法是数字签名，数字签名采用一定的数据交换协议，使得通信双方能够满足两个条件：接收方能够鉴别发送方所宣称的身份，发送方以后不能否认他发送过数据这一事实。比如，通信的双方采用公钥体制，发方使用收方的公钥和自己的私钥加密的信息，只有收方凭借自己的私钥和发方的公钥解密之后才能读懂，而对于收方的回执也是同样道理。另外实现防抵赖的途径还有：采用可信第三方的权标、使用时戳、采用一个在线的第三方、数字签名与时戳相结合等。

# 5 智慧城市安全运营

## 5.1应急响应

随着国家信息化建设进程的加速，计算机信息系统和网络已经成为重要的基础设施。随着网络安全组件的不断增多，网络边界不断扩大，网络安全管理的难度日趋增大，各种潜在的网络信息危险因素与日俱增。虽然网络安全的保障技术也在快速发展，但实践证明，现实中再完备的安全保护也无法抵御所有危险。因此，完善的网络安全体系要求在保护体系之外必须建立相应的应急响应体系。

应急响应PDCERF方法学分为准备（Preparation）、检测（Detection）、抑制（Containment）、根除（Eradication）、恢复（Recovery）、跟踪（Follow-up）6个阶段的工作。



### 5.1.1准备阶段

准备阶段需要及时和客户确认事件背景、相关负责人联系方式、确定参与此次应急响应人员、根据客户描述，初步判定事件响应策略，携带应急响应工具包前往客户现场。

准备阶段主要包括：事件背景、响应人员确定、事件响应策略、相关负责人联系方式、应急响应相关授权、应急响应工具包、应急响应手册等。

### 5.1.2检测阶段

检测阶段确认入侵事件是否发生，如真发生了入侵事件，评估造成的危害、范围以及发展的速度，事件会不会进一步升级。然后根据评估结果通知相关的人员进入应急的流程。

检测阶段主要包括：事件类型、事件影响范围、受影响系统、事件发展趋势、安全设备等。

### 5.1.3遏制阶段

采用针对性的安全措施降低事件损失、避免安全事件的扩散和安全事件对受害系统的持续性破坏。主要分为：物理遏制、网络遏制、主机遏制、应用遏制等。常见手段：断网、降权、网络封堵等。

### 5.1.4根除阶段

本阶段主要任务是通过事件分析查明事件危害的方式，并且给出清除危害的解决方案。个人认为可以从以下几个方面入手：系统基本信息、网络排查、进程排查、注册表排查、计划任务排查、服务排查、关键目录排查、用户组排查、事件日志排查、webshell排查、中间件日志排查、安全设备日志排查等。

### 5.1.5恢复阶段

恢复系统的运行过程，就是把受影响系统、设备、软件和应用服务还原到正常的工作状态；系统恢复、网络恢复、用户恢复、数据恢复以及重新部署。常见手段：系统重装、补丁加固、网络恢复、密码重置、木马清除等。

### 5.1.6跟踪阶段

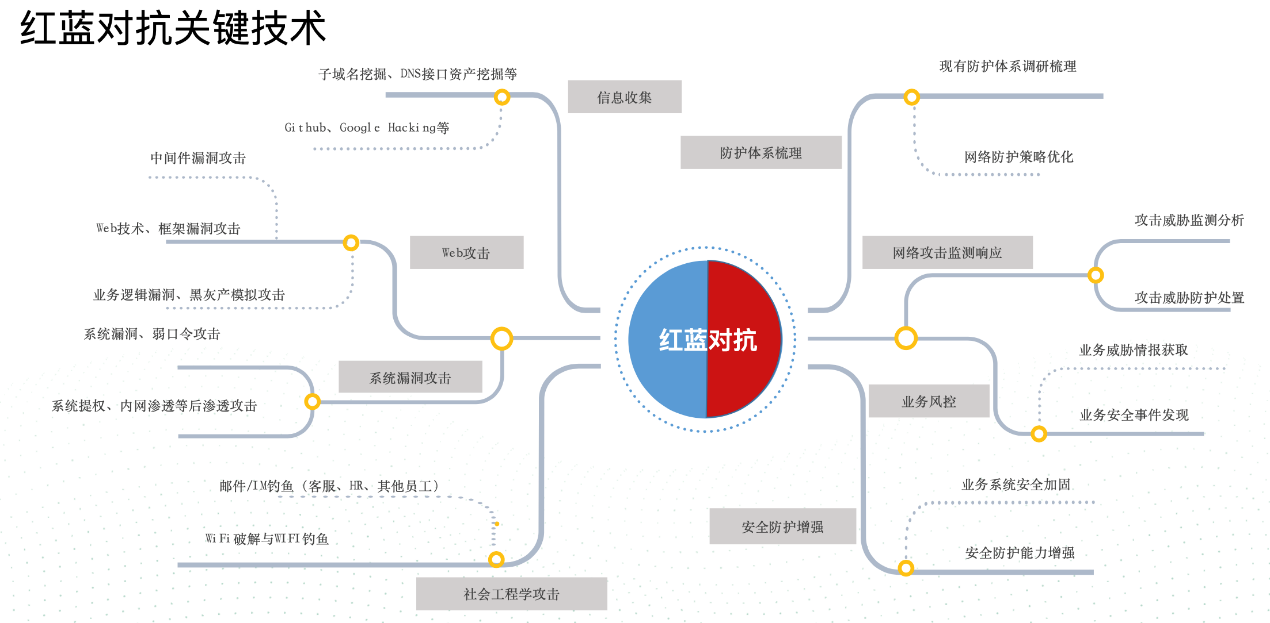
在业务系统恢复后，需要整理一份详细的事件总结报告，包括事件发生及各部门介入处理的时间线，事件可能造成的损失，为客户提供安全加固优化建议。

跟踪阶段主要包括：调查事件原因，输出应急响应报告，提供安全建议、加强安全教育、避免同类事件再次发生。

## 5.2红蓝对抗

智慧城市安全需要的是整体安全，一旦出现脆弱点，非法攻击者就有机可乘，后果不堪设想，因此我们需要“红蓝对抗”的活动介入。

“红蓝对抗”就是一场提前设定好游戏规则，制定奖惩制度，在一定时间范围内（或者具体时间），以不明确攻击源、不明确攻击目标、不限制攻击手段的方式，蓝军对红军发起的一场黑客模拟攻击，目的在于挖掘红军更多的风险脆弱点，为后续的网络与信息安全建设提供强有力的支持。下图为红蓝对抗关键技术图。

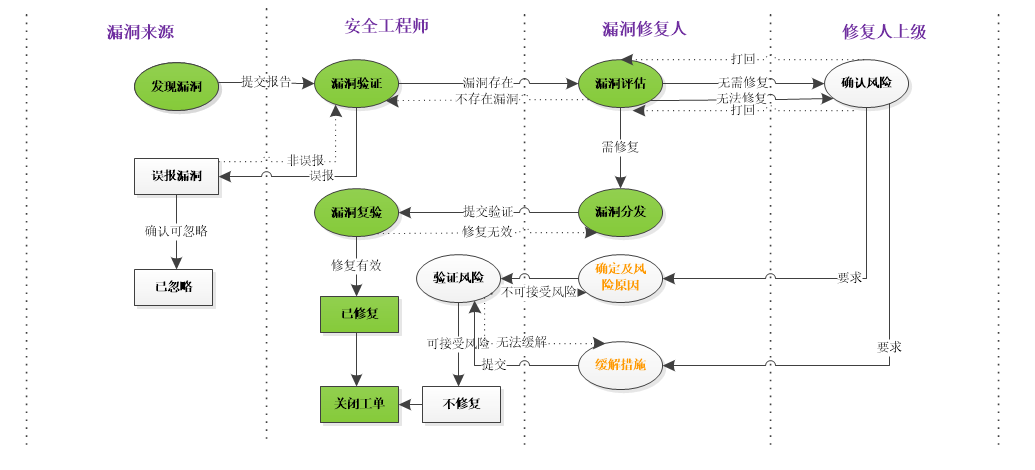


### 5.2.1常见的蓝军攻击技术

* 信息收集：资产挖掘（子域名、目录、后台、服务、高位端口应用）；Github、Google Hacking等；企业信息（办公地点、投资者关系、上下游企业等）；企业员工信息收集（百度、微博、邮箱、手机号等）。
* 系统漏洞攻击：系统漏洞攻击；弱口令攻击。
* WEB漏洞攻击：中间件漏洞攻击（IIS、Nginx解析漏洞、RCE等）；第三方组件、框架漏洞攻击（Java反序列化、Struts2 RCE、CMS 0day等）；常规WEB技术漏洞攻击（SQLi、XSS、XXE、SSRF、SSJS等）；逻辑漏洞（认证缺陷，如：后台弱口令、登录表单可暴力破解、密码找回绕过、短信认证功能缺陷等）；业务漏洞（薅羊毛）。
* 社会工程学攻击：邮件、IM钓鱼或植马（客服、HR、运维，甚至是其他任意员工）；物理攻击（丢植马U盘、尾随捎带进入内网、WIFI攻击/钓鱼/劫持）。
* 供应链攻击：供应链投毒（PIP库、GitHub、Docker Hub等）；供应链直接入侵（TeamViewer等）；供应链间接入侵（入侵获取源码进行审计等）。
* 后渗透攻击：系统提权；内网渗透；权限维持。

## 5.3漏洞管理

很多情况下，由漏洞导致的安全问题可能会对智慧城市长久运营与技术发展、品牌形象、安全合规与法律风险等方面产生影响，成为公司发展瓶颈。下图为漏洞管理流程图。



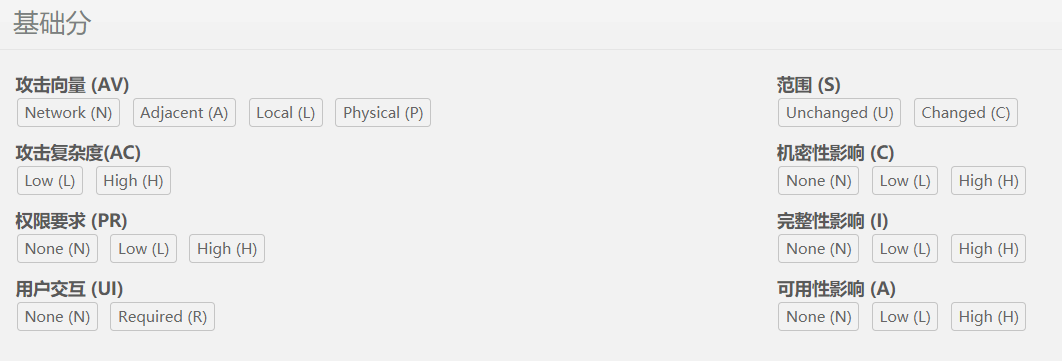
### 5.3.1发现漏洞

漏洞的来源主要有系统上线检测，漏洞扫描，代码审计，第三方组件漏洞，SRC众测平台和安全事件。

### 5.3.2漏洞评估与修复

漏洞严重程度根据CVSS 3.0评分标准评估。系统重要度根据系统承载业务，是否对公网暴露评估。最后根据漏洞严重情况制定SLA进行修复。

CVSS评估系统：



漏洞影响程度综合评分表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 严重等级\系统重要度 | | 核心业务 | 重要业务 | 支撑业务 |
| 严重 | 9-10 | 严重 | 高 | 高 |
| 高危 | 7-8.9 | 高 | 高 | 中 |
| 中危 | 4-6.9 | 高 | 中 | 低 |
| 低危 | 0-3.9 | 中 | 低 | 低 |

修复时长：

|  |  |  |
| --- | --- | --- |
| 漏洞严重等级 | 漏洞对公网开放 | 漏洞不对公网开放 |
| 严重 | 24小时 | 48小时 |
| 高 | 7天 | 14天 |
| 中 | 30天 | 60天 |
| 低 | 60天 | （不做要求） |

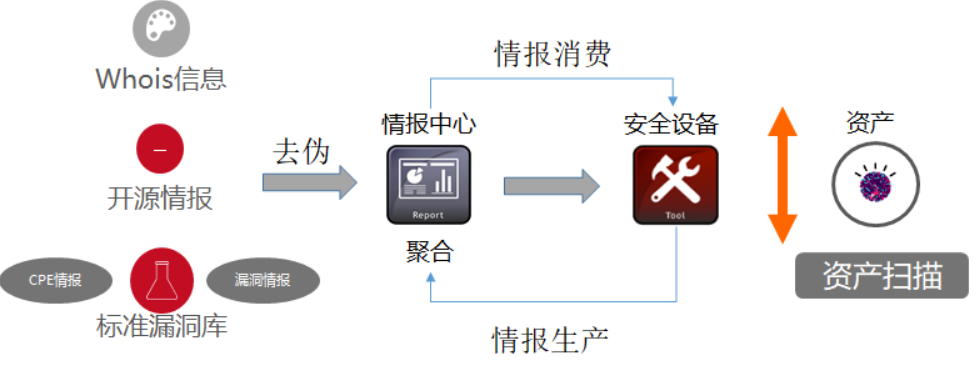
## 5.4威胁情报

威胁情报是某种基于证据的知识，包括上下文、机制、标示、含义和能够执行的建议，这些知识与资产所面临已有的或酝酿中的威胁或危害相关，可用于资产相关主体对威胁或危害的响应或处理决策提供信息支持。

实际上从安全从业者的角度，我们所理解的狭义的威胁情报，就是一些安全威胁指标，针对于不同的安全产品，会有不同的威胁指标，一般的威胁指标，比方：文件HASH、IP地址、域名URL、漏洞规则、邮箱地址等等，这些威胁指标就是安全产品所需要的威胁情报，安全产品的核心就是这些威胁情报，如果没有这些威胁情报，安全产品就没法体现它的安全能力了。

威胁情报的来源有：1.寻找安全公司购买；2.开源威胁数据采集；3.公司安全运营（包括蜜罐收集、安全事件和人工分析）；4. AI模型分析。

威胁情报产生与消费流程图：



# 6 智慧城市安全管理

## 6.1网络安全组织结构

网络安全的组织结构在各种信息安全管理的标准、最佳实践中都有涉及。可以说，网络安全组织是智慧城市规划网络安全的过程中，最值得深思的问题之一。

按照角色与工作职责，安全相关的岗位可细分为：CSO、安全架构、安全审计、安全测试、代码审计、安全开发、安全运维、安全运营、安全风控等方向，比较理想的安全团队并不是要求设置以上全部岗位，而是在开展相关工作时需要涉及这些专业技能。

## 6.2人员权限管理

随着环境因素的变化，传统的边界将渐渐消亡，仅依靠传统的网络隔离行之无效，这时候，基于零信任理念的统一身份管理为智慧城市运营重新筑造了“安全边界”。

基于零信任理念，智慧城市可以构建统一的身份认证与授权系统，将所有账号、认证、权限统一管理。譬如，离职员工被视为智慧城市的重要威胁之一。在整个智慧城市安全体系建设的实践中，必须要做到账户对应到应用系统的权限统一，实现每天离职员工的所有身份、账号权限可以在智慧城市内部系统中一键删除。

2020年初安全圈内热议的微盟员工删库事件，从身份认证与管理的技术角度来看，也是完全可以避免的。一方面，智慧城市在实施IAM（身份和访问管理）时，秉持最小权限原则，通过帐号的权限分级，给到员工应有的权限即可，而类似“删库”的特权账号不应该给到任何一个员工。其次，哪怕员工下发了批量数据删除的指令，智慧城市也可以通过内部异常行为检测，识别出该类指令基本不会发生在正常的生产环境中，从而不执行该指令。

除了技术层面的实现，身份认证与管理的本质依旧是安全基线。安全团队在智慧城市中的位置与影响力则决定了基线能否被确定、切实地落实到业务中去。判断安全团队在智慧城市、业务中的影响力大小，最直观的就是组织架构：安全团队是否为独立部门，直接汇报给CTO或CEO。

## 6.3数据管理——技术

数据安全指对用户数据信息资产的机密性、完整性、可用性、持久性、、以及可追溯性等方面的全面保护。智慧城市需要高度重视数据信息资产，把数据保护作为智慧城市安全策略的核心。智慧城市安全管理要遵循数据安全生命周期管理的业界先进标准，在身份认证、权限管理、访问控制、数据隔离、传输安全、存储安全、数据删除、物理销毁等方面，采用优秀技术、实践和流程，为城市管理者和用户提供最切实有效的数据保护能力，保证数据主体对其数据的隐私权、所有权和控制权不受侵犯。

### 6.3.1数据采集

#### 6.3.1.1数据清洗比对入库

海量数据存储的第一步，是检测和消除其中的相同数据，即冗余数据，在新数据入库时，通过对新数据和已存储数据的比对，清洗掉重复的数据，只给其保留一个指针，指向该重复数据已存储的存档。这种做法一方面是减少存储空间和IO带宽的占用和减少数据处理量，另一方面可以减少网络攻击带来的危害。

### 6.3.2访问隔离

#### 6.3.2.1身份认证和访问控制

访问控制能力可以通过统一身份认证服务（IAM –Identity and Access Management）提供的。IAM 是面向智慧城市的安全管理服务，通过 IAM，运维人员可以集中管理用户、安全凭证（例如访问密钥），以及控制用户管理权限和用户可访问的资源权限。使用 IAM，管理员可以管理用户账号，并且可以控制这些用户账号对租户名下资源具有的操作权限。当智慧城市存在多用户协同操作资源时，使用 IAM 可以避免与其他用户共享账号密钥，按需为用户分配最小权限，也可以通过设置登录验证策略、密码策略、访问控制列表来确保用户账户的安全，从而降低租户的企业信息安全风险。

#### 6.3.2.2数据隔离

云端数据的隔离可以通过虚拟私有云（VPC – Virtual PrivateCloud）实施，VPC 采用网络隔离技术，实现不同服务间在三层网络的完全隔离，各个服务可以完全掌控自己的虚拟网络构建与配置：一方面，结合 VPN或云专线，将 VPC 与服务内网的传统数据中心互联，实现服务应用和数据从服务内网向外网的平滑迁移；另一方面，利用 VPC 的 ACL、安全组功能，按需配置安全与访问规则，满足服务更细粒度的网络隔离需要。

### 6.3.3传输安全

对于智慧城市客户端到服务端、服务端之间的数据通过公共信息通道进行传输的场景，传输中数据的保护通过如下方式提供：

#### 6.3.3.1虚拟专用网络（VPN）

VPN用于在远端网络和 VPC 之间建立一条符合行业标准的安全加密通信隧道，将已有数据中心无缝扩展到云服务器上，为租户提供端到端的数据传输机密性保障。通过 VPN 在传统数据中心与 VPC 之间建立通信隧道，智慧城市相关服务可方便地使用云服务器、块存储等资源，通过将应用程序转移到云中、启动额外的 Web 服务器来增加网络的计算容量，实现了智慧城市的混合云架构的同时，也降低了智慧城市核心数据非法扩散的风险。目前，常见技术采用硬件实现的 IKE（密钥交换协议）和 IPSec VPN 结合的方法对数据传输通道进行加密，确保传输安全。

#### 6.3.3.2应用层 TLS 与证书管理

需要支持使用传输层安全协议（TLS – Transport Layer Security）进行加密传输，同时也支持基于 X.509 证书的目标网站身份认证。证书管理服务则是可以联合全球知名数字证书服务机构，为智慧城市提供的一站式 X.509 证书的全生命周期管理服务，实现目标网站的可信身份认证与安全数据传输。

### 6.3.4存储安全

#### 6.3.4.1密钥保护与管理密钥管理服务

密钥保护与管理密钥管理服务（KMS – Key Management Service）是一种安全、可靠、简单易用的密钥托管服务，帮助用户集中管理密钥，保护密钥安全。它通过使用硬件安全模块（HSM – Hardware Security Module），为各服务创建和管理密钥，防止密钥明文暴漏在 HSM 之外，从而防止密钥泄露。HSM 是一种安全产生、存储、管理及使用密钥并提供加密处理服务的硬件设备。KMS对密钥的所有操作都会进行访问控制及日志跟踪，满足审计和合规性要求。KMS可以对接对象存储、云硬盘、云镜像、数据库等多种存储方式。

#### 6.3.4.2数据加密和脱敏

数据库加密是指将存储于数据库中的数据，尤其是敏感数据，以加密的方式进行存储。

数据脱敏是对敏感数据进行变形处理，其目的是保护隐私数据等信息的安全，例如智慧城市收集的个人身份信息、手机号码、银行卡信息等敏感数据。数据脱敏从技术上可以分为静态数据脱敏和动态数据脱敏两种。静态数据脱敏一般应用于数据外发场景，例如需要将生产数据导出发送给开发人员、测试人员、分析人员等；动态脱敏一般应用于直接连接生产数据的场景，例如运维人员在运维的工作中直接连接生产数据库进行运维，客服人员通过应用直接调取生产中的个人信息等。

#### 6.3.4.3数据备份与恢复

备份技术为智慧城市的服务器、硬盘、云下VMware虚拟化环境，提供简单易用的备份服务，针对病毒入侵、人为误删除、软硬件故障等场景，可将数据恢复到任意备份点。

### 6.3.5数据处理

#### 6.3.5.1匿名化/去标识化

《信息安全规范 个人信息去标识化指南》（GB/T 37964-2019）是个人信息领域最为重要的国家标准之一，是“告知-同意”以外，个人信息收集、处理的另一条进路。

匿名化处理的本质在于将个人信息处理为非个人信息，让匿名化处理后的个人信息不再具有人格属性，从而无需再遵守关于个人信息保护的规定。去标识化虽然不完全等同于匿名化，但可以有效帮助企业降低收集、处理个人信息的合规风险，控制个人信息泄露的危害。

### 6.3.6数据交换

#### 6.3.6.1多方安全计算？

多方安全计算（MPC：Secure Muti-Party Computation）理论是姚期智先生为解决一组互不信任的参与方之间在保护隐私信息以及没有可信第三方的前提下协同计算问题而提出的理论框架。多方安全计算能够同时确保输入的隐私性和计算的正确性，在无可信第三方的前提下通过数学理论保证参与计算的各方成员输入信息不暴露，且同时能够获得准确的运算结果。

#### 6.3.6.2数据回溯？

回查历史网络流量的原始数据，提供网络流量的原始数据包存储和回溯查询能力，可对链路流量、应用数据、故障告警、指定数据库进行精准的回溯分析。从多角度还原历史场景，重组完整的会话信息。

### 6.3.7数据删除与销毁

#### 6.3.7.1内存删除

虚拟机操作系统将内存重新分配给各个服务之前，会对分配的内存进行清零操作，即写“零”处理，防止通过物理内存恢复删除数据造成的数据泄露。

#### 6.3.7.2存储数据删除

当智慧城市对应服务删除数据时，数据和对应的元数据在系统中一并删除，底层存储区域被回收以供系统重新覆盖写入，数据无法再被读取。

#### 6.3.7.4磁盘数据删除区分

智慧城市对删除虚拟卷采用清零措施，确保数据不可恢复，有效防止被恶意租户使用数据恢复软件读出磁盘数据，杜绝信息泄漏风险。

#### 6.3.7.5物理磁盘报废

当物理磁盘报废时，智慧城市通过对存储介质进行消磁、折弯或破碎等方式清除数据，并对数据清除操作保存完整记录，满足行业标准，确保存储隐私和数据不受未授权访问。

# 7 智慧城市安全合规

## 7.1安全政策

智慧城市的安全发展是国际社会关注的热点问题，目前世界主要国家已颁布相关法规和政策文件来推动智慧城市的安全建设。

美国重点关注智慧城市带来的安全和隐私问题，2015 年发布《白宫智慧城市行动倡议》，指出在智慧城市建设过程中要充分利用联邦政府在网络安全等方面已经开展的工作，认为以往在网络安全方面的研究和投资已为智慧城市建设奠定坚实基础，纽约市政府公布了“智慧城市实施方案”，统筹智慧城市发展与安全；

欧盟提出“智慧城市与社区欧洲创新伙伴行动”，由牵头政府部门主导智慧城市的发展和安全，倡导在 ICT 技术支持下建设可持续、安全互通的综合交通和物流运输系统；

英国在智慧城市建设中重点关注信息安全，2013 年发布《智慧伦敦计划》，提出数据开放等七大发展方向，另外，伦敦政府联合其他机构建立安全机构，为公共机构、企业等应对智慧城市网络威胁提供建议和保护；

新加坡政府在智慧城市建设中强化重要数据的保护，提出了“智慧国2025”计划，由政府统筹构建“智慧国平台”，通过全国数据的连接、收集和分析，提供优质的公共服务。在这一过程中，新加坡政府重视重要数据的保护，对比较重要的传感器数据进行匿名化保护和管理，并只在一定程度上进行适当的分享。

2014 年 8 月 27 日，国家发展改革委、工业和信息化部等八部委联合印发了《关于促进智慧城市健康发展的指导意见》，这是我国首部全面系统提升智慧城市安全的政策，确定了智慧城市建设“可管可控，确保安全”的基本原则，提出要落实国家信息安全等级保护制度，强化网络和信息安全管理，落实责任机制，健全网络和信息安全标准体系，加大依法管理网络和保护个人信息的力度，加强要害信息系统和信息基础设施安全保障，确保安全可控。

2015 年 8 月 26 日，公安部会同中央网信办、国家发改委、工信部共同制定出台了《关于加强智慧城市网络安全管理工作的若干意见》，以促进智慧城市建设安全、健康、有序发展。

2018年 1 月 7 日，中办、国办印发了《关于推进城市安全发展的意见》，以积极推广先进安全技术、提高安全监测和防控能力。

目前智慧城市安全领域相关的法律法规制度和政策等方面尚不健全，需要进一步明确和完善智慧城市网络和信息安全的制度和政策，推动智慧城市信息安全和网络安全建设。

## 7.2安全标准

目前，智慧城市安全国际标准化工作主要涉及国际标准化组织（ISO）、国际电工委员会（IEC）、国际电信联盟（ITU-T）等。

2016年，ITU-T FG SCC（智慧可持续城市焦点组）在智慧城市安全方面发布了研究报告《智慧可持续城市网际安全、数据保护和弹性》，提出了智慧可持续城市中安全管理、用户认证、关键基础设施保护以及隐私保护等方面的安全保障建议。

2017年，国家发布《公共安全视频监控联网信息安全技术要求》GB35114-2017。

2018年，发布《信息安全技术 网络安全等级保护基本要求》GB/T22239-2018。

2019 年，ISO 发布了首个智慧城市ICT 领域国际标准：信息技术—智慧城市 ICT 评价指标（ISO/IEC 30146:2019）。该标准从智慧城市 ICT 视角提出了一套适用于全球的综合性评估评价指标，其中信息安全为七大类评价指标之一。

2020年 3 月，国际电信联盟 ITU-T SG17 工作组通过了我国相关单位提交的《智慧城市数字孪生系统安全机制》和《智慧社区安全机制》两个立项。

2020年4月3日，国家标准化管理委员会下达 2020 年第一批推荐性国家标准计划，该计划共包含432项，涵盖各行各业。其中新制定311项，修订121项；有415项为推荐性标准，剩余17项均为指导性技术文件。

# 8 智慧城市安全未来展望