智慧城市信息安全风险评估模型构建与实证研究*

邹凯 向尚 张中青扬 毛太田
湘潭大学公共管理学院 湘潭 411105

摘要: [目的/意义] 面对智慧城市日益突出的信息安全问题,提出一个科学的风险评估模型,以快速对智慧城市进行风险分类并分析风险因素。[方法/过程] 从智慧城市信息安全的 5 个层次和风险评估的 4 个主要因素出发,构建智慧城市信息安全风险指标框架,对智慧城市实例进行 ward 系统聚类形成分类属性,选择 C4.5 算法的决策树方法建立风险评估模型,并验证模型的科学性。[结果/结论] 结果发现: 安全管理制度、数据泄露与损坏威胁、安全意识薄弱性和设备安全漏洞是智慧城市之间差距最显著的风险因素,根据评估结果提出保障智慧城市信息安全的建议。

关键词: 信息安全 风险评估 智慧城市 C4.5 决策树
分类号: G203
DOI: 10.13266/j.issn.0252-3116.2016.07.003

1 引言

自从智慧城市的理念被提出以来,全球城市不约而同地投入到“智慧化”的建设中来。《中共中央关于制定国民经济和社会发展第十三个五年规划的建议》提出将支持智慧城市作为中国新型城镇化的重要发展方向。随着建设的不断深入,智慧城市的实践越来越依靠物联网、云计算等一系列新型信息技术的驱动,但是在利用信息技术推动信息融合、知识发现和推动智慧城市服务模式创新的过程中,城市中各方信息格局发生了全新转变。这一转变必然会导致智慧城市信息安全内涵与构面的重大变化,带来对信息安全的多角度冲击[1]。从信息介质、安全技术、管理制度、政策法规到公民素养,这股冲击对智慧城市信息安全形成了严峻的考验[2]。随着智慧城市建设的逐步深化,信息安全问题成为日益突出的焦点,如何才能既充分发挥信息共享、协同和融合的巨大作用,又在一定限度下维持信息安全进行稳定时,成为了智慧城市持续发展不得不解决的实际问题。

国外学者研究了智慧城市发展对城市信息安全带来的挑战[3],通过研究智慧城市公共安全系统的需求,完善管理方法[4],从智能设备及要素体系的角度构建智慧城市的安全系统[5],建立了智慧城市环境中网络物理系统的风险管理框架[6]。国内研究者在对智慧城市信息安全进行研究时,大都从个人信息安全和信息安全管理两个方面进行探讨,对保障机制[7]、体系构建[2]、对策[8]等问题进行研究。目前的研究中缺乏对智慧城市信息安全具体风险的挖掘,更没有从系统的角度对其风险进行评估。

从风险评估的视角来研究信息安全需要度量要素带来的影响或损失的可能程度,因此,如何设计风险评估方法,识别各种关键风险要素并判断各要素的重要程度,从而准确度量风险值,就成为研究的关键。已有的针对信息安全的风险评估方法主要有层次分析法、模糊熵权法、贝叶斯网络、神经网络、支持向量机等一系列定性、定量的评估方法。本文提出一种利用 ward 聚类与决策树模型对智慧城市信息安全进行风险评估的方法,将定性与定量分析方法相结合,利用 ward 聚类满足决策树对分类属性的要求,利用决策树满足解释评估风险等级过程的需求。

2 智慧城市信息安全风险的基本内涵

根据我国《计算机信息系统安全保护条例》给出的定义,信息安全的内涵按照信息作用可归纳为物理

* 本文系国家社会科学基金项目“大数据环境下政务信息资源优化配置与服务模式创新研究”(项目编号: 15BTQ051)研究成果之一。
作者简介: 邹凯,副院长,教授,博士; 向尚(ORCID: 0000-0001-9135-7301),硕士研究生,通讯作者,E-mail: xiangshang165@163.com; 张中青扬(ORCID: 0000-0003-1599-0898),硕士研究生; 毛太田(ORCID: 0000-0001-6514-680X),教授,博士。
收稿日期: 2016-02-01 修回日期: 2016-03-20 本文起止页码: 19-24 本文责任编辑: 易飞

安全、运行安全、数据安全和管理安全4个方面，而欧美信息安全管理标准则从信息保障的属性角度来描叙，包含机密性、完整性、可用性、真实性和不可抵赖性。在智慧城市的新信息环境下，信息安全的内涵较传统城市信息安全内涵更大，主要体现在以下几个方面：①无处不在的智能感应节点更易受到攻击；②物联网的集群式与云计算的分布式造成了数据压力增大，同时智慧城市环境下数据损坏、丢失和失窃等安全事件造成的后果更严重；③智慧城市网络连接越来越快捷、广泛与复杂，不合法或不真实的信息内容更容易在城市网络节点中萌发、传播并恶化；④转变中的城市管理结构缺乏完善的管理制度规范；⑤以人为本的智慧城市发展要求公众参与最大化，普遍的交互使公众安全意识对智慧城市信息安全的影响越来越大。智慧城市信息安全风险存在于信息服务从采集、加工、存储到利用的每一个环节；既存在于客体中，也存在于主体中；不仅存在于提供应用服务的信息系统与人员机构之间，更广泛存在于智慧城市中每个个体之中。

基于智慧城市信息安全的多重内涵，综合已有的研究成果，本文从信息资源管理和社会信息化过程的角度来识别智慧城市的信息安全风险，将其分成5个相互联系的层次：智慧基础设施安全风险、数据服务安全风险、信息内容安全风险、信息管理安全风险和公众素养安全风险。其中智慧基础设施（包括物联网基础设施、通讯网络基础设施、云计算基础设施、地理空间基础设施等）是智慧城市信息安全的物理基础，数据服务安全（包括数据共享、存取、开发等过程）是在信息资源管理过程中保障信息数据可用、可信、不中断的状态，信息内容安全（包括互联网、服务器、机构数据库的海量信息）涉及信息的合法性、真实性与可控性，信息管理安全是城市各类主体在接触智慧应用项目过程中的行为准则，公众安全素养是市民使用应用服务的信息安全意识与能力的综合体现。如表1所示：

表1 智慧城市信息安全的基本内涵

智慧城市信息安全风险层次	涵义
智慧基础设施安全风险	传感器、通讯与计算设备及系统的安全隔离程度、危险情况下生存性能、灾难后恢复能力
数据服务安全风险	数据可用效率、数据加密与完整性能
信息内容安全风险	信息内容合法性、真实性、可控能力
信息管理安全风险	行为准则与管理活动规范效力、安全事故追责能力
公众素养安全风险	公众信息安全意识强弱程度

3 智慧城市信息安全风险评估指标体系构建

信息安全风险识别的基本依据是客观世界的因果关联性和可能性[9]，而识别风险的主要方式是感知风险与分析风险，对于智慧城市信息安全风险，已有研究主要从信息资源[10]、信息安全需求[8]、信息产业及信息伦理[11]、多层诱发因素[12]等角度来识别。目前对智慧城市的信息安全的研究大都从信息系统或顶层设计的角度来探究，鲜有从风险因素方面讨论智慧城市信息安全。

3.1 智慧城市信息安全风险特征分析

智慧城市通过信息活动实现组织目标的过程中才会出现信息安全风险，因此以智慧城市信息活动为基础来设计风险评估指标能够系统、全面地反映智慧城市的信息安全状况。随着智慧城市信息活动需求的不断提升和智慧城市建设的不断深入，智慧城市的内外环境也在不断变化，因此智慧城市信息安全的风险也出现了越来越多的新特征。除了更严重的软硬件安全隐患，智慧城市的信息内容、信息管理、社会基础对信息安全风险的冲击也越来越严重。

3.2 智慧城市信息安全风险评估要素调查

智慧城市信息安全风险评估要素调查可以运用多种灵活方法进行，文献调查、问卷调查和访谈法是常用的要素调查方法。本文按照信息安全风险评估国家规范[9]，将智慧城市信息安全风险因素归纳为资产、威胁、脆弱性、安全措施，辅予考虑战略目标、资产价值、安全需求、残余风险和安全事件等相关因素，并把相关因素按照影响关系约简融入主要要素。在要素关系中，风险要素及属性之间存在着如下关系：

（1）智慧城市战略目标的实现对其资产具有依赖性，依赖程度越高，要求其风险越小；

（2）风险是由威胁引发的，资产面临的威胁越多则风险越大，并可能演变成为安全事件；

（3）资产的脆弱性可能暴露资产的价值，资产具有的脆弱性越多则风险越大；

（4）脆弱性是未被满足的安全需求，威胁利用脆弱性危害资产；

（5）风险的存在及对风险的认识导出安全需求；

（6）安全需求可通过安全措施得以满足，安全措施可抵御威胁，降低风险。

本文以由国家信息中心起草，国家质量监督检验检疫总局发布的《信息安全风险评估实施指南》[13]为

参考标准，综合考虑信息安全风险评估要素和智慧城市信息安全风险层次的相互关系，建立评估框架，其中风险评估要素包含资产、威胁、脆弱性和安全措施，安全风险层次包含智慧基础设施安全风险、数据服务安全风险、信息内容安全风险、信息管理安全风险和公众素养安全风险，按照 5 个安全风险层次逐层设定风险评估要素，形成指标体系。

3.3 智慧城市信息安全风险评估指标体系的检验和修正

为了使智慧城市信息安全风险评估指标体系更趋合理，必须对初始指标体系进行校验。笔者采用德尔菲方法，通过问卷与访谈方法向智慧城市建设相关人员和风险评估专家征询修正意见，通过反馈信息了解专家组对智慧城市风险评估的基本判断与理解，考察不同专家对智慧城市风险评估指标体系的不同观点与解释，最后整合所有专家的意见，完成对指标体系的修正，形成智慧城市信息安全风险评估指标框架，如表 2 所示：

表 2 智慧城市信息安全风险评估指标框架

安全风险层次	资产	脆弱性	威胁	安全措施
智慧基础设施安全风险	信息设备和系统 U_1	设备安全漏洞 U_6	自然人为物理威胁 U_{11}	安全检查 U_{16}
数据服务安全风险	数据硬盘和链路 U_2	数据载体漏洞 U_7	泄露与损坏威胁 U_{12}	数据隔离与加密 U_{17}
信息内容安全风险	信息内容资源 U_3	信息内容盲区 U_8	引导与控制威胁 U_{13}	内容监督制度 U_{18}
信息管理安全风险	信息管理人员 U_4	应用业务误区 U_9	错误操作威胁 U_{14}	安全管理制度 U_{19}
公众素养安全风险	公众安全意识 U_5	安全意识薄弱区 U_{10}	社会环境威胁 U_{15}	安全知识宣传 U_{20}

为了确保风险评估的指标赋值具有一致性和准确性，本文按照 ISO27001 给出的信息安全风险评估方法[14]，将风险等级从高到低划为 VH、H、M、L 和 VL 5 个等级表示，将每个需要估值的风险评估指标按影响程度大小从 1 到 9 进行取值，其中资产的取值由保密性、完整性和可用性决定，表示对资产的依赖程度；脆弱性由资产弱点造成的严重性决定；威胁由威胁发生的可能性决定；安全措施由抵御威胁的程度决定。资产、脆弱性和威胁的值越大，风险等级就越高；安全措施的值越大，风险等级则越低。

4 利用 ward 系统聚类与 C4.5 决策树建立风险评估模型

为了区分不同城市最终所在的风险等级，必须先根据各项风险要素指标对其进行聚类。实践中类间距离的度量方法有很多，如组间与组内平均连接距离、最近与最远邻距离、重心距离、中位数距离和离差平方和距离(ward 法)等，这些方法的优缺点参见文献[15]。ward 系统聚类法的关键思想就是离差平方和的分析，使用欧氏距离的平方作为类之间距离的度量，它放弃了分类中极值的要求，倾向获取局部最优解，本文选择这种方法的原因是它擅长于处理类间界限不清晰的情况，分类效果好。首先将总体中的每一个样本都看成一类，将距离最接近的两个类合并，计算新的类与其他类的距离，重复这个合并的步骤[16]。设总体样本中共有 n 个样本，可以分成 G1、G2、...、Gk 这 k 个类，Xij 表示 Gi 中的第 j 个样本，Gi 类中含有 Ni 个样本数，Xi 表示 Gi 的重心，计算 Gi 类中样本的离差平方和为：$S_i = \sum_{j=0}^{N_i}(X_{ij} - X_i)'(X_{ij} - X_i)$，总体类内的离差平方和为：$S = \sum_{i=0}^{k}\sum_{j=0}^{N_i}(X_{ij} - X_i)'(X_{ij} - X_i)$。在每一次合并类的过程中，始终确保 S 增加的值最小，如此两两合并，直到最终把所有城市聚类成 5 个不同的聚落，则它们分别对应 5 个不同风险等级。

完成聚类后，把城市所处的类别分别标号 R1、R2、R3、R4、R5，此时由于并不知道每个城市到底处于怎样的风险等级，因此利用决策树方法来计算风险值并区分风险等级。决策树是一种类似于流程图的树结构，在风险评估模型中，每一个非终端内部节点表示对一个风险属性的测试，每一个分支代表该测试的不同输出，每一个终端结点代表一个风险等级。C4.5 算法使用信息增益率代替信息增益来选择分枝属性[17]，因此相对传统的 ID3 算法克服了偏好选择属性取值多的属性的不足。对于离散型属性 C4.5 的选择方法和 ID3 的方法是一致的，但对于连续性属性，C4.5 通过计算最佳分割阈值来对连续性数据进行分割，通过两个区间表示离散取值。C4.5 决策树的算法过程为：①将连续型属性数据集离散化，计算每个属性的信息增益率：$GainRatio(A) = \frac{Gain(A)}{SplitInfo_A(T)}$；②使用信息增益率最大的属性作为分枝节点，迭代建立决策树的分枝，直到分枝节点中样本全部属于同一类别，或者样本数低于设置最小阈值，这样将样本数最多的类别作为终端结点的标识；③为避免拟合过度，对生成的决策树进行后置

剪枝，消除噪音数据节点和孤立节点；④输出决策树，用决策树对测试数据集进行分类。此时的决策树模型已经能够对不同的智慧城市信息安全风险类别进行分类，但为了进一步精准量化每个智慧城市的风险等级，必须计算具体风险值。因为信息增益率本质上是属性在分类上的重要程度，这样对整体风险影响越大的指标，权重也就越大。笔者采用各属性在根节点上的信息增益率作为各属性的权重，通过加权后得出每个城市的具体风险值，通过具体风险值判断城市所处的相对风险等级。

5 智慧城市信息安全风险评估实证研究

2015 年 4 月 7 日，住建部公布了第 3 批国家智慧城市试点名单，目前我国智慧城市试点已达 290 个，根据中国社会科学院信息化研究中心报告，目前我国智慧城市在智慧基础设施、智慧管理、智慧人群和保障体系方面，整体建设情况普遍良好，但智慧服务方面明显建设不足。根据《2015 中国智慧城市发展水平评估报告》（以下简称《报告》）发布的内容，本文选取智慧城市发展水平排名靠前的 15 个城市——上海、北京、深圳、武汉、无锡、宁波、广州、厦门、成都、南京、西安、天津、杭州、合肥、郑州进行实证研究，从 1 - 15 分别编号作为研究样本，其资产类指标得分通过《报告》获取，脆弱性与威胁类指标得分来源于漏洞报告网站，安全措施类指标得分来源于各省市安全自检报告，不能得到的指标使用德尔菲法评判出得分值，整理如表 3 所示：

表 3 15 个城市原始数据集

编号	U_1	U_2	U_3	U_4	U_5	U_6	U_7	U_8	U_9	U_{10}	U_{11}	U_{12}	U_{13}	U_{14}	U_{15}	U_{16}	U_{17}	U_{18}	U_{19}	U_{20}
1	8	5	6	8	7	8	5	7	4	6	3	5	7	8	9	7	7	8	5	7
2	9	2	3	3	6	9	5	6	3	6	4	4	7	7	6	6	7	7	5	7
3	7	5	7	7	2	6	4	4	3	6	4	2	6	6	5	5	5	5	6	6
4	5	6	9	4	9	9	8	5	4	6	5	6	5	9	4	2	4	5	3	5
5	6	6	2	7	6	7	3	4	3	5	1	5	5	6	7	6	7	8	5	4
6	6	6	8	8	8	6	2	2	1	4	2	3	5	5	4	5	5	7	5	5
7	7	8	4	6	2	8	4	5	4	6	2	5	6	7	5	7	6	6	6	6
8	7	6	2	7	7	8	3	4	3	5	1	6	5	6	8	6	7	8	5	4
9	5	5	3	5	8	5	4	4	4	4	3	2	4	3	5	6	5	5	6	6
10	5	3	5	1	6	5	4	5	5	5	3	3	4	6	9	7	5	7	6	6
11	6	2	3	9	2	6	4	4	5	4	4	5	6	5	8	3	4	5	3	5
12	7	5	1	1	6	6	6	4	5	6	4	6	7	7	4	1	3	5	4	4
13	6	5	5	3	6	6	4	4	5	5	4	3	4	6	9	7	6	7	6	6
14	5	6	8	6	9	9	8	5	4	6	4	6	6	9	4	2	4	5	3	5
15	5	6	8	4	8	8	8	5	4	7	3	6	5	9	5	3	7	6	4	5

利用相对风险等级代替绝对风险等级，通过 SPSS 统计软件对数据集进行 ward 系统聚类，使用 Z 分数做标准化处理并绘制聚类谱系图（见图 1）。将聚类结果分为 5 组：无锡、厦门、宁波为 R1 组，南京、杭州、成都为 R2 组，上海、北京、深圳、广州为 R3 组，武汉、合肥、郑州为 R4 组，西安、天津为 R5 组，将其作为分类属性加入原始数据表 3 中。

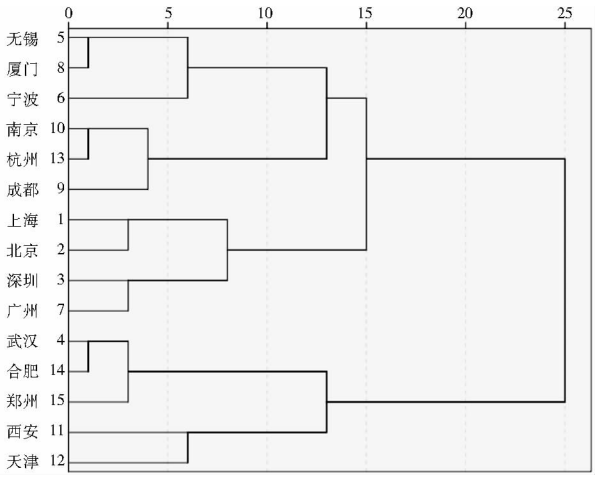

图 1 15 个城市 ward 聚类谱系图

本文使用数据分析软件 weka 来实现计算与建模过程：首先对原始数据计算每个属性的信息增益率，C4.5 决策树中对连续属性中的值按从大到小排列，取大小相邻两个值作为分割点逐个计算信息增益率，取其中最大的增益率为该属性的信息增益率。其次按照第 3 部分中计算步骤依次分层计算 20 个属性的信息

增益率并排序,选择上个节点下最大信息增益率的属性作为分枝节点,直到分枝完全属于一个类别或样本数小于3,因为数据量过少故不予剪枝,最终得到一个大小为9、叶子数为5的决策树模型,见图2。ROC曲线是在交叉验证中不同判定条件下得到的结果,具体是以TP rate(真正率)为纵坐标、以FP rate(假正率)为横坐标绘制的曲线,曲线越接近左上角说明模型越有效,反之则越低效。而ROC面积是指ROC曲线下的面积,通常ROC面积在0.9以上有较高的准确率。本文经过10折交叉验证,计算出ROC面积数值达到0.917。说明分类效果显著,从而接受模型。

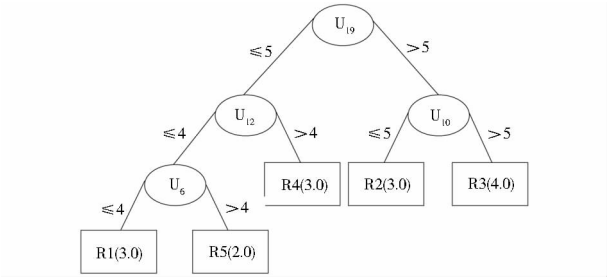

图2 智慧城市信息安全的风险评估决策树模型

从图2的决策树中可以看出,安全管理制度、泄露与损坏威胁、安全意识薄弱性和设备安全漏洞在每层决策中是影响智慧城市风险的重要指标,利用根节点上各个属性的信息增益率作为智慧城市信息安全各指标的权重,使用指标权重与表3里的数据相乘,并按照资产、脆弱性和威胁与风险正相关,安全措施与风险负相关的原则加权,得到15个智慧城市最终风险值,通过计算平均风险值可以得知分组所处风险等级(见表4)。为了进一步证明使用C4.5决策树对智慧城市信息安全进行风险评估的优越性,本文引入实践应用中较为广泛的两种分类方法——朴素贝叶斯和Logistic回归作为参照,其中朴素贝叶斯法是基于贝叶斯定理与特征条件独立假设的分类方法,Logistic回归是一种广义的线性回归分析模型。对两种方法输入与表3相同的数据集与相同的聚类分组来对风险等级进行分类,并通过10折交叉验证,所得结果见表5,表中真正率、查准率、查全率、F值、ROC面积正向反映分类效果,误报率负向反映分类效果,从中可以看出C4.5决策树的分类效果明显比这两种方法优秀。

表4 15个智慧城市的风险值与风险等级

城市	风险值	相对风险	城市	风险值	相对风险	城市	风险值	相对风险
上海	9.83	H	宁波	7.44	L	西安	7.51	M
北京	10.45	H	广州	9.33	H	天津	9.12	M
深圳	10.2	H	厦门	8.42	L	杭州	6.08	VL
武汉	10.51	VH	成都	7.31	VL	合肥	10.31	VH
无锡	6.63	L	南京	6.26	VL	郑州	11.23	VH

表5 3种风险等级分类方法的分类效果比较

评估方法	真正率	误报率	查准率	查全率	F值	ROC面积
C4.5决策树	0.867	0.033	0.883	0.867	0.86	0.917
朴素贝叶斯	0.667	0.114	0.667	0.667	0.631	0.72
Logistic回归	0.8	0.05	0.87	0.788	0.657	0.892

6 智慧城市信息安全风险评估结果分析与启发

根据表4的结果,可以看出当前我国智慧城市的信息安全发展水平不均衡:①核心城市(上海、北京、深圳、广州)的相对风险普遍较高。尽管这些城市在安全管理制度方面更加完善,但是这些城市智慧化发展水平相对较高,整个城市的运维对信息系统设备、数据、人员的依赖性更强,安全事件的后果更严重,因此这些城市比内陆城市要面临更多的不确定性风险。②中西部地区信息安全风险参差不齐,智慧城市公共数据泄露与损坏的威胁在这些城市中(武汉、合肥、郑州)比较严峻。部分城市(成都、南京、西安、天津)在信息资源共享与利用方面较为保守,故而信息安全风险较低;③沿海二线城市(无锡、宁波、厦门)的信息安全风险处于较低的水平,这些城市的政府主导能力较强,建立了统一的安全管理机构和应急机制,社会协作参与的信息安全氛围较好;④当前信息安全风险越低的智慧城市中,来自智慧基础设施的安全漏洞较少,在历史记录上有更少被证实的安全事件,在应对数据失窃、损坏和篡改等方面准备充分,同时市民的信息安全意识也更强。

从评估模型反映的重要风险要素中,可以得到一些保障智慧城市信息安全的启发:①由于智慧城市本质上是对城市服务的深度信息化,智慧基础设施、信息数据、专业人员等一系列资产的重要性会越来越高,必

须持续增加对关键信息部门安全防护的资源投入，提升信息系统对数据的处理与过滤能力，以技术创新夯实信息安全的技术基础；②在充分促进信息融合与保障合理范围内数据安全的矛盾之间找到平衡点，针对智慧城市信息服务制定智慧城市信息安全防护的策略、标准和安全技术指导框架，完善信息安全风险评估、等级保护、安全测评、电子认证、应急响应等监管体系；③在智慧城市服务机构中健全信息安全管理制度，设立严格的信息行为准则，加强员工安全培训，完善信息安全责任制度；④构建智慧城市全民信息安全体系，加大投入普及安全知识，提升公众安全素养，为个人信息安全的防护提供全面的指导意见。

参考文献：

[1] 李勇. 智慧城市建设对城市信息安全的强化与冲击分析[J]. 图书情报工作，2012，56(6)：20－24.

[2] 丁波涛. 智慧城市视野下的新型信息安全体系建构[J]. 上海城市管理，2012(4)：17－20.

[3] ELMAGHRABY A，LOSAVIO M. Cyber security challenges in smart cities：safety，security and privacy[J]. Journal of advanced research，2014，5(4)：491－497.

[4] KOŽUCH B，SIENKIEWICZ-MALYJUREK K. New requirements for managers of public safety systems[J]. Procedia -social and behavioral sciences，2014，149(5)：472－478.

[5] BELANCHE-GRACIA D，CASALÓ-ARIÑO L V，PÉREZ-RUEDA A. Determinants of multi-service smartcard success for smart cities development：a study based on citizens' privacy and security perceptions[J]. Government information quarterly，2015，32(2)：154－163.

[6] YASUKO F，MASAKI S，HIROSHI U. Survey on risk management based on information security psychology[J]. Lecture notes in computer science，2015，9171：396－408.

[7] 刘彦麟，张盛. 智慧城市建设中信息安全保障机制探究[J]. 信息通信，2015(6)：156.

[8] 董袁泉. 智慧城市中信息安全的分析以及应对措施[J]. 微型机与应用，2014(23)：16－18.

[9] GB/T 20984－2007. 信息安全风险评估规范[S]. 北京：中华人民共和国国家质量监督检验检疫总局，2007.

[10] 满晓元. 智慧城市信息安全风险及评估方法[J]. 电子世界，2013(23)：77－78.

[11] 邓贤峰. "智慧城市"建设的风险分析[J]. 财经界，2011(1)：106－109.

[12] 张立超，刘怡君，李娟娟. 智慧城市视野下的城市风险识别研究——以智慧北京建设为例[J]. 中国科技论坛，2014(11)：46－51.

[13] GB/T 31509－2015. 信息安全风险评估实施指南[S]. 北京：中华人民共和国国家质量监督检验检疫总局，2015.

[14] ISO/IEC 27001：2005，Information technology-security techniques-information security management systems-requirements[S]. Geneva：International Organization for Standardization，2005.

[15] 李卫东. 应用多元统计分析[M]. 北京：北京大学出版社，2008.

[16] 何跃，王猛. 基于灰色关联与 Ward 系统聚类的国民幸福评价[J]. 统计与决策，2012(5)：42－45.

[17] QUINLAN J R. C4.5：Programs for machine learning[M]. San Mateo：Morgan Kaufmann Puhlishers Inc，1993：17－42.

作者贡献说明：

邹凯：提出研究思路，设计研究框架，起草与修订论文；

向尚：采集、清洗、分析数据，起草与修订论文；

张中青扬：修订论文；

毛太田：修订论文。

Model Construction and Empirical Study on Smart City Information Security Risk Assessment

Zou Kai　Xiang Shang　Zhangzhong Qingyang　Mao Taitian

School of Public Administration，Xiangtan University，Xiangtan 411105

Abstract: **[Purpose/significance]** Considering the increasingly prominent information security issues of smart city，a scientific risk assessment model is proposed，which could classify and analyze the risk factors rapidly. **[Method/process]** From five connotations of smart city public service's information security and four main factors of risk assessment，it constructs a smart city public service's information security risk index framework. Using the ward method of systematical clustering calculates 12 examples of smart city to form classification properties. Choosing the C4.5 algorithm of decision tree method to establish a model of risk assessment，and verify that the model is scientific. **[Result/conclusion]** It finds that the safety management system，data leak and the threat of damage，safety awareness' weakness and equipment security vulnerabilities is the most significant risk factors' gap between wisdom cities，according to the results of the assessment，making recommendations to protect the information safety of wisdom city.

Keywords: information security　risk assessment　smart city　C4.5 decision tree