摘 要

新一代信息技术的发展和应用使得智慧城市对信息资源的挖掘、整合和利用上升了一个新的高度，有利于更好地发挥信息价值，促进城市的可持续发展，提升居民的生活质量。然而新兴信息技术在利用过程中引发了信息格局的改变，可能带来更为严峻的智慧城市信息安全问题，甚至对社会财产和人身安全造成严重的影响。因此，通过研究智慧城市信息安全风险内涵，构建风险要素指标体系，从而识别影响智慧城市信息安全的关键要素，有针对性地提出相应的管理策略，对于减少信息安全风险发生概率，维护智慧城市可持续发展具有重要意义。

本文通过梳理智慧城市信息安全相关文献掌握智慧城市信息安全风险管理的实际情况，并以此作为研究基础，运用扎根理论构建智慧城市信息安全风险要素指标体系，又利用模糊 DANP 方法识别和分析关键要素，最终根据要素在系统中的重要程度提出降低信息安全风险、提高风险应对能力的管理策略。

首先，对智慧城市信息安全的文献和现状进行梳理，了解智慧城市信息安全研究的相关背景和政策支持，明确智慧城市信息安全研究的目的和意义，论述智慧城市、信息安全及智慧城市信息安全风险的相关概念和研究的理论基础。其次，运用扎根理论，从半结构化访谈获得的访谈资料入手，通过开放式编码、主轴式编码、选择性编码和饱和度检验等几个阶段，梳理智慧城市信息安全影响要素，构建智慧城市信息安全风险要素指标体系。再次，介绍构成模糊 DANP 方法的基本原理，绘制因果关系四象限图，并根据原因分析、结果分析和权重排序之间的关联识别指标体系中的关键影响因素。最后，根据识别出的关键风险严肃，并结合信息生态理论，从确保信息安全可控、加强管理水平、强化技术应用、营造有序环境 4 个方面提出减少智慧城市信息安全风险的相关对策。

关键词：智慧城市；信息安全风险；DANP；影响因素

Abstract

The development and application of new-generation information technology has raised the mining, integration and utilization of information resources in smart cities to a new level, which is conducive to better play the value of information, promote the sustainable development of cities and improve the quality of life of residents. However, emerging information technology in the process of utilization has triggered changes in the information landscape, which may bring more serious information security problems in smart cities and even cause serious impacts on social property and personal safety. Therefore, it is important to reduce the probability of information security risks and maintain the sustainable development of smart cities by studying the connotation of information security risks in smart cities, constructing a risk element index system, so as to identify the key elements affecting the information security of smart cities and proposing corresponding management strategies in a targeted manner.

This paper grasps the actual situation of information security risk management in smart cities by combing the literature related to information security in smart cities, and takes it as the basis of research, constructs an index system of information security risk elements in smart cities by using the rooting theory, and also identifies and analyzes key elements by using the fuzzy DANP method, and finally proposes management strategies to reduce information security risk and improve risk response capability according to the importance of the elements in the system.

First, the literature and current situation of information security of smart cities are sorted out to understand the relevant background and policy support of the research on information security of smart cities, to clarify the purpose and significance of the research on information security of smart cities, and to discuss the relevant concepts of smart cities, information security and information security risk of smart cities and the theoretical basis of the research. Secondly, using the rooting theory, starting from the interview data obtained from semi-structured interviews, we sort out the information security impact elements of smart cities through several stages, such as open coding, spindle coding, selective coding and saturation test, and construct an index system of information security risk elements of smart cities. Again, the basic principles of constituting the fuzzy DANP method are introduced, the four quadrant diagram of causality is drawn, and the key influencing factors in the index system are identified according to the correlation between cause analysis, result analysis and weight ranking.

Finally, based on the identified key risk serious and combined with the information ecology theory, the relevant countermeasures to reduce the information security risk of smart city are proposed in four aspects: ensuring the controllability of information security, strengthening the management level, enhancing the technology application and creating an orderly environment.

Key words: smart city; Information security risk; DANP; Influence factor

目 录

第 1 章 绪论

1.1 研究背景

近年来，智慧城市立足于科学理念的新思路，凭借大数据、云计算、人工智能等新兴信息技术分析社会活动、感知公众需求，并通过城市发展的高级形态为居民提供了更智能、更便捷的社会服务，开启了社会高效治理的新局面[①]。然而，智慧城市包含了多个复杂的系统，在处理海量数据资源、帮助城市精确治理的同时也加速了政府、企业、社会主体之间信息交换和信息共享的过程，带来了很多非传统性的信息安全问题，稍有不慎就会造成难以估量和控制的经济、社会影响。由此可见，信息安全作为智慧城市建设中至关重要的环节，不仅是城市平稳运行的基础要素，也是维护国家和社会安定的重要保障[②]。正如十四五规划纲要中所指出的，要在推动智慧城市建设的同时保障数据安全，健全数据安全治理体系，提高数据安全监管能力，提升数据安全保障水平[③]。因此，必须重视信息的不确定性，警惕信息安全问题给智慧城市乃至整个社会带来的影响，完善信息安全管理制度，降低信息安全风险，以保证智慧城市的有效、平稳运行[④]。

政策方面，为降低信息安全风险，规范信息安全行为，推进智慧城市建设，国家及相关部委出台了一系列符合中国国情及社会实际的相关文件，构建了信息安全体系框架，明确了信息安全体系建设的重要意义，从宏观上对信息安全建设提供了指导。2015 年，由国家发改委、中央网信办等联合发布的《关于开展智慧城市标准体系和评价指标体系建设及应用实施的指导意见》指出，以人为本是网络安全管理的核心，要根据公众的需求加强网络安全能力建设[⑤]。2019 年，国家标准委员会颁布的《信息安全技术智慧城市安全体系框架》强调，要从安全角色和安全要素视角构建智慧城市安全体系框架[⑥]。2020 年《信息安全技术智慧城市建设信息安全保障指南》明确了智慧城市建设相关单位在信息安全方面应承担的责任，为智慧城市信息安全建设指明了方向[⑦]。

目前，智慧城市信息安全问题虽受到国内外学者的广泛关注，但相关研究却

① 甄峰,秦萧.大数据在智慧城市研究与规划中的应用[J].国际城市规划,2014,29(06):44-50.
② 余潇枫,潘临灵.智慧城市建设中“非传统安全危机”识别与应对[J].中国行政管理,2018(10):127-133.
③ 共产党员网.中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要[EB/OL].[2021-03-13]. https://www.12371.cn/2021/03/13/ARTI1615598751923816.shtml.
④ 佟大柱.基于信息安全视角下的智慧城市建设研究[J].网络空间安全,2019,10(02):1-4.
⑤ 张新刚,于波,王保平,等.智慧城市信息安全风险及保障机制研究[J].网络空间安全,2016,7(Z1):23-26.
⑥ 国家市场监督管理总局,国家标准化管理委员会.信息安全技术智慧城市安全体系框架:GB/T 37971-2019[S].北京:中国标准出版社,2019.
⑦ 国家市场监督管理总局,国家标准化管理委员会.信息安全技术智慧城市建设信息安全保障指南:GB/Z 38649-2020[S].北京:中国标准出版社,2020.

仍停留在概念内涵、发展现状、技术手段、风险评估等方面，对于智慧城市建设过程中信息安全影响因素的研究相对较少。基于此，本文利用访谈的形式探究公众在日常生活中遇到的信息安全问题，了解信息安全风险发生的原因，归纳智慧城市信息安全影响因素的维度，识别关键指标要素，并根据研究结果有针对性地采取措施，以期能够增强信息安全风险的抵御能力，保障智慧城市的平稳运行。

1.2 研究目的与研究意义

1.2.1 研究目的

本文的主要研究目的有两个：

（1）以智慧城市信息安全作为研究对象，结合之前学者的研究成果和通过访谈得到的现实资料，整合采访对象认为影响信息安全问题的原因并加以分析，提取其中关键的风险要素，帮助政府有针对性地采取措施。

（2）探究各影响因素之间的关联关系，揭示影响因素对于智慧城市信息安全的重要程度，快速锁定各主体改进的正确方向，为采取措施提高智慧城市信息安全提供理论依据。

1.2.2 研究意义

智慧城市建设的目的是依托新技术和新理念，利用信息化的管理模式，建立智能化服务体系，为居民营造良好的生活环境，早日实现城市的智慧化发展。为达到这一目标，充分发挥信息资源在智慧城市建设中的重要作用，就必须重视信息技术应用过程中的信息安全风险，构建包括信息监测、预警、应急和决策在内的信息安全保障体系。本文结合智慧城市发展现状，识别智慧城市信息安全的关键影响因素，对减少信息安全问题带来的严重影响，发挥信息化在智慧城市建设和管理过程中的重要作用具有理论和现实意义。

（1）理论意义

目前，国内专家对智慧城市的研究主要集中在基础技术和信息平台方面，而对于智慧城市信息安全的研究也仅仅停留在发展现状和技术手段等方面，从信息安全风险角度探索智慧城市信息安全影响因素的研究较少。因此，本文收集智慧城市信息安全相关的研究成果并加以整理，结合已有的学术成果介绍能够用以识别信息安全风险关键要素的方法，有利于明晰智慧城市信息安全的理论框架，拓展智慧城市信息安全的研究维度，同时为信息安全风险的识别提供新思路。

（2）现实意义

在现代社会中，智慧城市信息安全问题存在于信息收集、存储、传播和利用

的每个环节，这些复杂的、不确定的信息安全问题为城市管理带来了不小的阻碍。本研究结合智慧城市管理现状，构建了智慧城市信息安全风险要素指标体系，识别了指标体系中的关键要素，厘清了风险要素之间的关联关系，探索了加强智慧城市信息安全防护能力的管理策略，对减少智慧城市信息安全风险，维护城市稳定运行起到了借鉴和实践指导作用，具有一定的现实意义。

1.3 国内外相关研究

1.3.1 国外研究现状

西方发达国家从很早就开始建设智慧城市，因此不仅城市建设进程更快，对信息安全的重视程度更高，同时在防范信息安全风险的过程中也形成了相对完善的理论体系和政策法规，值得我们学习和借鉴。通过对文献的收集和梳理发现，国外学者对智慧城市信息安全的关注主要聚焦在现状分析、技术手段和应对策略三个方面，下面就从这三个方面进行具体阐述。

（1）智慧城市信息安全现状分析

通过对智慧城市信息安全现状的调查发现，智慧城市下的用户在享受服务的同时或多或少都经历过信息跟踪、数据丢失及隐私侵犯等信息安全问题，给日常生活带来了一些困扰[①]。这是因为智慧城市能够实时监测现实世界，通过控制城市设施影响人们生活，并且在为用户提供交通、医疗、娱乐等智能服务的同时收集大量隐私敏感信息[②]。尤其是在城市服务智能化的过程中，信息技术的快速发展会对城市基础设施及应用中的数据（信息）安全造成威胁[③]，而用户在通过智能手机等设备操控基础设施的过程中，往往因为沉浸在使用体验和生活质量中而忽视其中潜在的隐私风险问题[④]，从而造成难以估量的损失。Ismagilova[⑤]等在分析了智慧城市发展过程中遇到的信息安全风险问题之后提出，信息系统是影响信息安全的主要因素，并指出了当前发展的局限性及未来发展的方向。

（2）智慧城市信息安全技术研究

为减少智慧城市信息安全风险，保障用户的隐私信息，学者们对信息设备、系统网络、第三方应用、使用场景等各个方面的信息安全技术均进行了一定程度

① Ferraz F S, Ferraz C A. Smart City Security Issues: Depicting Information Security Issues in the Role of an Urban Environment[C]//Ieee/acm, International Conference on Utility and Cloud Computing. IEEE, 2014:842-847.

② Zhang K, Ni J, Yang K, et al. Security and Privacy in Smart City Applications: Challenges and Solutions[J].Journals & Magazine, 2017, 55(1):122-129.

③ Aldairi A, Tawalbeh L. Cyber Security Attacks on Smart Cities and Associated Mobile Technologies[J]. Procedia Computer Science,2017,109:1086-1091.

④ Elmaghraby A S, Losavio M M. Cyber security challenges in Smart Cities: Safety, security and privacy[J]. Journal of Advanced Research,2014,5(4):491-497.

⑤ Ismagilova E, Hughes L, Dwivedi Y K, et al. Smart cities: Advances in research-An information systems perspective[J]. International Journal of Information Management,2019,47:88-100.

的改进和升级。信息设备方面，Wang[①]等从技术和业务两个方面提出了一种能够分析系统威胁，提高系统防护能力的方法。系统网络方面，Garcia-Font[②]等针对智慧城市系统网络存在的安全问题，提出了一种可以恢复丢失数据、检测网络攻击、增加控制力度的非侵入式架构，从整体上保障了智慧城市的安全。第三方应用方面，Chun[③]等认为需要使用基于风险的访问控制模型对数据风险进行评估并根据当前情境做出决策，从而保证个人信息的机密性。实际场景方面，Ko[④]等提出了一种保护网络环境、智能设备和服务模式的智能安全算法。尤其在医疗保健领域，区块链技术[⑤]和电子健康记录隐藏技术[⑥]的应用实现了在高效访问医疗记录的同时保护患者敏感信息，有效维护了患者信息可访问性和保密性之间的平衡。

（3）智慧城市信息安全应对策略研究

智慧城市信息安全应对策略提出的前提是对信息安全的精准评估，通过评估结果提出有针对性地管理措施，既能够帮助用户更高效地获取信息，又能够增强城市的经济和技术竞争力，因此不同学者通过不同角度提出信息安全的应对策略。Kulawiak[⑦]等提出了一种能够用来评估基础设施的系统，通过评估结果可以明确基础设施建设的薄弱环节，改变城市发展战略规划，降低信息安全风险。Edwards[⑧]认为智慧城市存在源于数据、隐私和法律三个方面的不同威胁，并借鉴格拉斯哥智慧城市的经验以及相关国际会议的成果提出了应对措施。Chiehyeon[⑨]等指出城市数据转化为信息面临的六种挑战，并结合城市数据的参考模型构建了智慧城市数据使用框架，保障了城市数据使用和城市建设规划的合理性、规范性。Chamoso[⑩]等认为智慧城市要想收集用户大量有用的信息，就必须加强大数据处理平台的建设和优化，营造安全的信息处理环境。

---

① Wang P, Ali A, Kelly W. Data security and threat modeling for smart city infrastructure[C]// 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC). IEEE, 2015.

② Garcia-Font V, Rifa-Pous H, Garrigues C. An architecture for the analysis and detection of anomalies in smart city WSNs[C]// Smart Cities Conference (ISC2), 2015 IEEE First International. IEEE, 2015.

③ Chun S A, Atluri V. Risk-Based Access Control for Personal Data Services[M]// Algorithms, Architectures and Information Systems Security. 2008(11):263-283.

④ Ko H, Bae K, Kim SH, et al. A Study on the Security Algorithm for Contexts in Smart Cities[J]. International Journal of Distributed Sensor Networks,2014:1-8.

⑤ Gaby G D, Jordan M, Matea M, et al. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology[J]. Sustainable Cities and Society,2018(39):283-297.

⑥ Parah S A, Sheikh J A, Akhoon J A, et al. Electronic Health Record hiding in Images for smart city applications: A computationally efficient and reversible information hiding technique for secure communication[J]. Future Generation Computer Systems,2020(108): 935-949.

⑦ Kulawiak M, Lubniewski Z. SafeCity—A GIS-based tool profiled for supporting decision making in urban development and infrastructure protection[J]. Technological Forecasting and Social Change,2014,89:174-187.

⑧ Edwards L. Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective[J]. Social Science Electronic Publishing,2016,11:1-37.

⑨ Chiehyeon L, Kwang-Jae Kim, Paul P. Maglio. Smart cities with big data: Reference models, challenges, and considerations[J].Cities,2018(4):1-14..

⑩ Chamoso P, A González-Briones, Prieta F, et al.Smart city as a distributed platform: Toward a system for citizen-oriented management, Computer Communications,2020(152):323-332.

1.3.2 国内研究现状

相较于西方发达国家，我国智慧城市的建设还处于初步阶段，尤其在智慧城市信息安全研究方面更是起步较晚，但总体发展势头迅猛。随着信息安全产生的影响愈发明显，各行各业开始重视大量出现的信息安全问题，研究信息安全的学者也逐渐增多。整理国内智慧城市信息安全相关论文后发现，当前国内学者对智慧城市信息安全方面的研究主要体现在以下三个方面。

（1）智慧城市信息安全概念研究

对智慧城市信息安全概念的研究一方面要了解智慧城市的信息特点，另一方面要总结信息安全的内涵，才能不断充实和丰富智慧城市信息安全的概念体系。李勇[①]梳理了智慧城市信息安全从出现到蔓延的全过程，归纳智慧城市信息安全的特点后发现，信息安全在不同的应用场景下具有不同的内涵。例如在信息的使用过程中，面对信息设备和信息系统这两个影响信息安全的重要因素，周发桂[②]选择将信息设备的特点加入到对智慧城市信息安全的理解中，以扩充智慧城市信息安全的概念，而李宁宁[③]则从信息系统入手，将信息安全层级划分成物理与环境安全、系统安全、网络安全、数据与应用安全 4 个等级，进一步细化了智慧城市信息安全的概念。另外，因为智慧城市信息安全概念的完善需要利用大量现实案例进行总结，黄鹰旭[④]等便提出采用智慧城市的形式构建信息安全数据库，通过收集相关案例总结智慧城市信息安全特征，以提高对智慧城市信息安全的认知。

（2）智慧城市信息安全风险评估研究

智慧城市信息风险评估的目的是分析智慧城市建设过程中遇到的问题和风险，利用风险评估方式减少信息安全问题，提高信息安全管理水平。结合现有的成果，不同学者分别从评估角度、评估对象及评估方法等方面对信息安全风险评估进行了相应的研究。评估角度上，宋璟[⑤]等认为现有的智慧城市安全防护能力不足以应对日益变化的安全风险，需要从顶层设计、标准体系和建设程度进行实时监测和评估，提高风险应对的能力。蒙婷婷[⑥]则通过智慧城市信息安全在新时代下的特征，寻找产生信息风险的原因及对信息安全可能造成的影响，进而构建了智慧城市信息安全体系。评估对象上，高凯[⑦]通过实证研究探索“智慧九华”的信息安全风险值，进一步完善了信息风险评估体系。评估方式上，随机森林[⑧]、

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(06):20-24.
② 周发桂.智慧城市的信息安全分析[J].中国信息安全,2014(02):105-109.
③ 李宁宁,石秀芳,王兵.浅析智慧城市信息安全[J].信息技术与信息化,2013(04):13-15.
④ 黄膺旭,梅宏.智慧城市背景下信息安全问题案例库设计[J].电子政务,2018(07):20-27.
⑤ 宋璟,李斌,班晓芳,等.关于我国智慧城市信息安全的现状与思考[J].中国信息安全,2016(02):107-111.
⑥ 蒙婷婷.智慧城市信息安全体系构建研究[D].长春:吉林财经大学,2018.
⑦ 高凯.智慧城市信息安全风险评估指标体系构建研究[D].湘潭:湘潭大学,2019.
⑧ 向尚,邹凯,蒋知义,张中青扬.基于随机森林的智慧城市信息安全风险预测[J].中国管理科学,2016,24(S1):266-270.

决策树[①]、贝叶斯网络[②]等方法都被用来进行量化分析，以构建有效的智慧城市信息安全风险评估模型。

（3）智慧城市信息安全保障机制研究

王金祥[③]认为保障信息安全的目的是城市的可持续发展，因此需要树立正确的安全观念，采取保障网络安全的措施来促进城市的健康发展。因此，不同学者将智慧城市信息安全风险作为切入点，从不同的角度进行剖析并将其作为信息安全保障机制建设的基础。罗力[④]认为应该从顶层设计、政策法规、人才培养和制度建设等多角度保障信息安全。王青娥[⑤]等从基础设施、技术、管理和政策法规 4 个方面提出了保护信息安全的措施。吕欣[⑥]等构建了包含战略、管理组织、技术、管理过程和运行 5 大保障体系的智慧城市网络安全参考框架。李怡[⑦]等通过对新型智慧城市的深入了解后提出，管理因素和技术因素对进一步增强新型智慧城市的数据安全保障能力具有重要作用。另外，刘杰[⑧]选取广州市作为研究对象，针对广州市智慧城市发展所处的信息环境提出了适合本地发展的优化策略。

1.3.3 国内外研究述评

智慧城市具有开放的特点，信息资源在信息技术的支持下进行动态流动，为居民提供良好的信息服务，营造良好的信息环境。但信息资源的流动过程中涉及诸多环节和因素，难免存在信息安全漏洞，影响信息服务质量。通过梳理国内外相关文献可知，越来越多的学者在智慧城市信息安全这一领域进行深入研究，尤其在智慧城市信息安全内涵、现状及评价体系构建方面均取得了重要进展。但回顾相关研究内容可以发现针对智慧城市信息安全风险的研究相对较少，研究方法也是以文献分析为主，缺乏实际调查和现实指引，即使提出了信息安全的影响因素也只是简单提出改善策略，并没有对关键要素以及风险要素间的关联关系和动态变化进行深入研究。因此，通过深入调查和科学方法识别关键风险要素，可以拓展信息安全问题研究的范围，为提高风险应对能力提供新思路和新方法，有利于加强政府在信息安全风险防控中的主导地位，提高我国智慧城市信息安全水平。

① 邹凯,向尚,张中青扬,毛太田.智慧城市信息安全风险评估模型构建与实证研究[J].图书情报工作,2016,60(07):19-24.
② 毛子骏,梅宏,肖一鸣,等.基于贝叶斯网络的智慧城市信息安全风险评估研究[J].现代情报,2020,40(05):19-26,40.
③ 王金祥.全面网络安全观下智慧城市安全保障体系建构探析[J].电子政务,2016(03):20-26.
④ 罗力.新兴信息技术背景下我国智慧城市信息安全风险和保障研究[J].城市观察,2016(03):129-136.
⑤ 王青娥,柴玄玄,张譞.智慧城市信息安全风险及保障体系构建[J].科技进步与对策,2018,35(24):20-23.
⑥ 吕欣,韩晓露,李阳,等.智慧城市网络安全体系框架研究[J].信息安全研究,2016,2(09):827-833.
⑦ 李怡,魏玉峰,田国敏,马卓元.新型智慧城市数据安全保障研究[J].网络安全技术与应用,2018(11):57,63.
⑧ 刘杰.智慧城市建设的信息安全保障问题研究[D].广州:华南理工大学,2015.

1.4 研究内容与研究方法

1.4.1 研究内容

本文主要分为六个章节，各章的主要内容安排如下：

第一章，绪论。简要介绍了本文的研究背景，分析了智慧城市信息安全风险研究的目的和意义，梳理了国内外智慧城市信息安全相关问题的研究现状，同时对研究内容与研究方法进行简单阐述，明确研究思路，并指出本文的创新之处。

第二章，相关概念与理论基础。主要对本文相关内容及理论进行梳理，从智慧城市的概念、内涵及特征入手，对智慧城市相关概念进行基本阐述，又探讨了信息安全研究的概念、内涵和属性，接着确定了智慧城市信息安全风险研究的基本内容，包括概念、类型和特征方面，并对本研究所依据的理论基础进行了阐述。

第三章，智慧城市信息安全风险要素指标体系构建。基于扎根理论，对访谈资料进行整理和编码，通过开放式编码、主轴式编码、选择性编码和饱和度检验等几个阶段获得核心范畴，借助 NVivo12 软件梳理智慧城市信息安全风险要素之间的关联关系，构建智慧城市信息安全风险要素指标体系。

第四章，智慧城市信息安全风险要素识别。采用模糊 DANP 对第三章得到的 6 个维度 20 个指标进行计算，绘制因果关系图，并对得出的结果进行原因要素、结果要素分析和因素权重分析，识别关键风险要素。

第五章，智慧城市信息安全风险管理策略。根据第四章的分析结果，结合信息生态理论，从确保信息安全可控、加强管理水平、强化技术应用、营造有序环境 4 个方面提出减少智慧城市信息安全风险的相关对策。

第六章，总结与展望。概括本文的研究内容，指出研究中的不足并提出改进意见，为接下来更深入的研究提供方向。

1.4.2 研究方法

（1）文献分析法。国内外学者的研究成果大多集中在学术期刊数据库中，通过对相关文献的筛选和梳理，能够快速把握智慧城市信息安全领域的研究成果和热点前沿，还能够学习研究信息安全问题的方法，是最快速有效的方法之一，也是理论研究的基础手段。通过文献分析找到信息安全研究的薄弱环节，确定风险要素识别的重要性，并以智慧城市信息安全风险为主题开展相关研究。

（2）扎根理论。扎根理论是在已有理论和文献的支持下，根据研究者的知识与经验对丰富、详尽的一手资料进行编码分析，进而构建理论的一种质性研究方法，目前已经被应用于诸多领域，具有科学性与代表性。从前文的文献综述中可以看到，基于实际调查分析智慧城市信息安全影响因素的研究较少，因此本文采用扎根理论，自上而下地开展数据分析，深入挖掘智慧城市信息安全的影响因

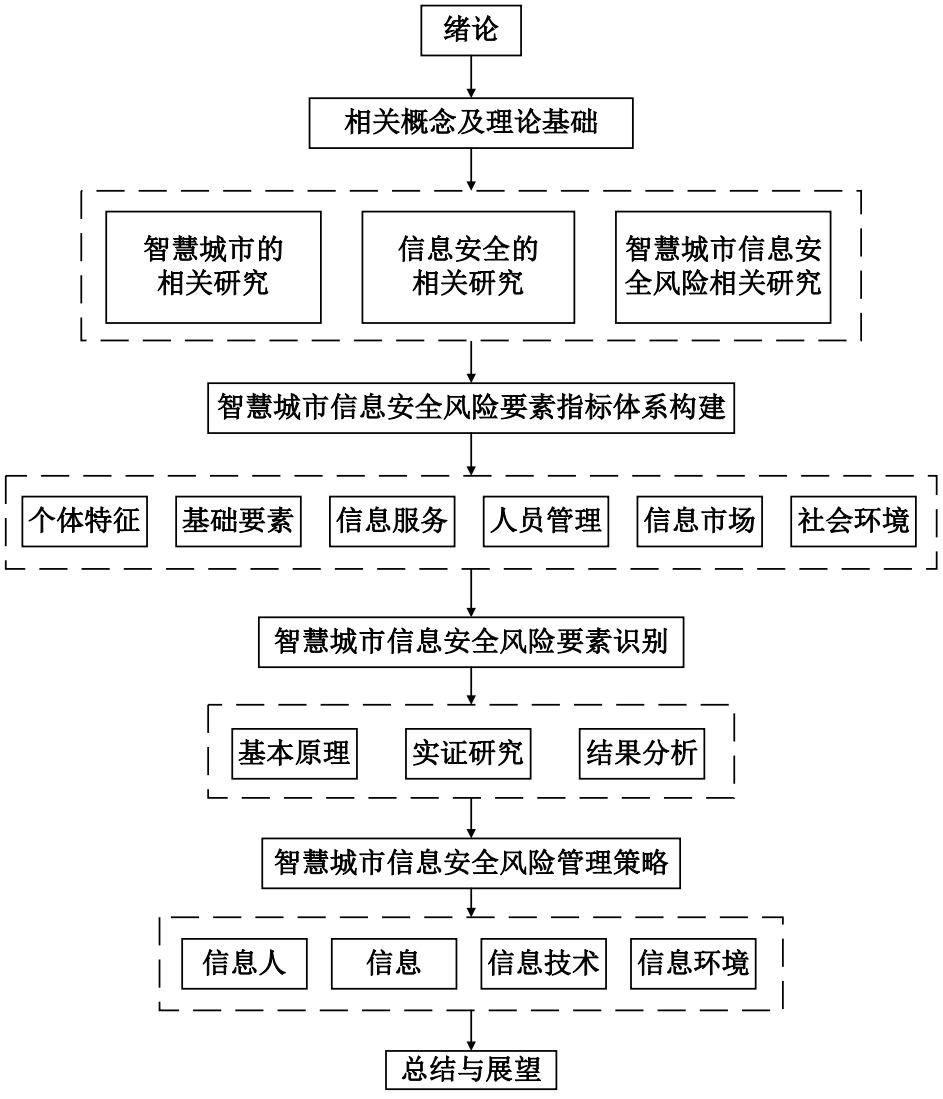
素，从经验数据中构建实质理论。

（3）实证研究法。本文在理论分析的基础上进行了实证研究，如采用访谈法获取第一手资料构建理论体系之后，利用实证研究进行智慧城市信息安全风险关键要素的识别，把握要素之间的内在联系和作用规律，为管理策略的制定提供了事实依据。因此，在理论指导下采用实证研究方法，使本文在具有理论探索意义的同时还兼具了实践指导意义。

1.5 研究框架与创新点

1.5.1 研究框架

本文的研究框架如图 1.1 所示。



1.1 研究框架图

1.5.2 创新点

目前，我国对智慧城市信息安全风险的研究还在进行积极的探索，本文借助扎根理论构建智慧城市信息安全风险要素指标体系，并运用模糊 DANP 方法识别信息安全风险指标中的关键要素，相比以往通过文献分析得到的信息安全影响因素，具有以下创新之处：

（1）智慧城市信息安全风险要素指标的构建。目前，关于智慧城市信息安全的研究大多偏向于技术方法、评价体系和保障机制等方面，对于影响智慧城市信息安全风险的研究尚不充分。本文采用访谈获得影响智慧城市信息安全的风险要素，又利用扎根理论进行分类，构建了以事实为依托的风险要素指标体系，为识别关键风险要素提供了有力参考。

（2）智慧城市信息安全关键风险要素的识别。本文将三角模糊数、DEMATEL 与 ANP 相结合，形成模糊 DANP 方法，不仅可以识别信息安全风险要素中的关键要素，又能够量化因素在系统中的权重，有利于分析指标在整个体系中的重要程度并提出促进智慧城市信息安全的优化策略，为智慧城市信息安全的管理提供一定的指导。

第 2 章 相关概念及理论基础

2.1 智慧城市的概念、内涵及特征

2.1.1 智慧城市的概念

智慧城市建设是一项复杂又持续的系统工程，因此对于智慧城市的概念，不同学者有着不同的理解，比如，李虹[①]强调智慧城市可分为狭义的智慧城市与广义的智慧城市，其中狭义的智慧城市指能够利用信息技术改善民众生活、加强政府管理的新型城市形态；连玉明[②]认为我国智慧城市建设刚刚步入正轨，应该将智慧交通和信息服务放在智慧城市建设的首位；胡小明[③]则提出信息化才是智慧城市建设的核心环节，是智慧城市水平高低的评价标准，因此智慧城市概念要体现出信息技术的关键作用。通过梳理和总结各位专家、学者及有关组织对智慧城市概念的见解，本文最终将智慧城市定义为能够融合绿色生态、以人为本等先进理念，充分利用现代化先进信息科学技术，对大量复杂信息资源进行收集、存储、共享和利用，从而满足城市生活需求，形成智慧交通、智慧医疗、智慧教育等城市发展新模式，实现城市可持续性长远发展的高级形态。

2.1.2 智慧城市的内涵

智慧城市建设的目标是改善居民的生活水平和居住环境，提高政府整体工作效率和城市综合服务水平，从而增强国家的竞争力和影响力。在实现目标的过程中，要准确把握智慧城市的基本内涵，即以建设能为公众提供智能化服务的基础设施为基本，以绿色、发展、可持续的理念为指导，以庞大复杂的城市信息资源为核心，以大数据、物联网、云计算等先进的现代信息技术为手段，以多元主体协同配合为关键，以为居民、企业和政府提供高效服务为动力推动城市体系的良性运转。简单来说，就是通过现代化信息技术收集、整合、存储和传输信息资源，并利用城市基础设施建设为居民提供个性化服务，最大化的利用信息资源，提高管理效率，推动城市智慧化的进程。

2.1.3 智慧城市的特征

（1）信息网络覆盖更广泛。智慧城市建设中运用的一项非常重要的技术就是物联网技术，物联网技术的发展使得信息网络更加发达，使得用户无论何时何

① 李虹.物联网：生产力的变革[M].北京：人民邮电出版社,2010.
② 连玉明.中国城市蓝皮书[M].北京：中国时代经济出版社,2002.
③ 胡小明.智慧城市的思维逻辑[J].电子政务,2011(6):84-91.

地，即使身处偏远的乡村都能随时接收到网络信号，实现信息的接收和共享。信息网络的全方位覆盖打破了时间和空间上的壁垒，使用户不再只是信息的被动接收者，还可以主动参与到信息的创造和使用中来，真正成为了信息的主人。

（2）信息资源共享更便捷。信息资源是现代经济发展的战略资源和独特的生产要素，是人类社会经济进步的强大助推力，智慧城市建设更是离不开对信息资源的开发和利用。随着无线技术和云计算技术等信息技术的快速发展，人们已经可以通过网络和手持终端设备随时随地接收和传播信息，使信息资源的共享更加方便快捷，极大地提升了信息资源的利用效率。

（3）信息协同管理更高效。在智慧城市的建设过程中，从来都不是依靠一个人、一个部门或一个组织的孤军奋战，而是社会全体成员的广泛参与和密切配合。智慧城市通过信息技术实现了各部门的互联互通，将人与人、人与组织、组织与组织之间进行紧密相连，形成了一种资源共享、消息互通、优势互补的良好局面，实现了城市各部门的协同发展。

2.2 信息安全的概念、内涵及属性

2.2.1 信息安全的概念

城市的信息安全不仅仅是信息技术层面的问题，更包含了信息管理、信息环境及相关法律法规等多方面的因素，因此，可以从不同角度阐述信息安全的概念。从技术角度来看，信息安全是指能够利用信息技术实现信息的完整、可用和保密；从信息资源管理角度来看，信息安全是指信息资源从收集、整合、存储、传播到利用的每一个环节均保证其完整性和安全性；从社会信息化的角度来看，信息安全是指用以提供信息服务的信息系统功能完整，且能够排除外界干扰。但不管是从哪个角度来解读，信息安全的目标都是在经过信息所有人的授权的前提下，严格遵照信息所有人意愿真实、合理地对信息进行处理和使用。

2.2.2 信息安全的内涵

信息安全的内涵按照信息作用可归纳为物理安全、运行安全、数据安全和管理安全 4 个方面[①]。物理安全方面，主要包括服务器、网线及其他信息基础设施的安全，信息基础设施安全是信息安全体系的第一道防线，主要作用是通过防止非法用户的接入和使用来保障信息安全。运行安全方面，注意对系统的定期检修和维护，及时发现系统漏洞并进行修复，保证系统的功能稳定。数据安全方面，增强数据传输、存储和利用过程中的安全防控意识，并在加大信息安全技术投入，

① 赵全营. 面向云计算的用户数据安全策略研究[D].大连理工大学,2014.

保障信息安全的同时防范新兴技术带来的安全风险。管理安全方面，制度的制定原先主要是为了防范黑客攻击、病毒侵入等外部风险，但在如今的信息环境中，制定信息安全管理制度的目的不仅在于防范外部威胁，还用来约束组织内部成员。

2.2.3 信息安全的属性

保密性、完整性、可用性、真实性、可控性和不可抵赖性刻画了信息安全的基本特征和需求，是信息安全的基本属性[①]。保密性保证信息除发送者和接收者外不被第三方得知，不通过非法渠道进行买卖；完整性保证信息在存储和使用过程中不丢失、不被轻易篡改；可用性保证信息系统能够始终维持高水平运行，保障信息安全，为用户提供高质量的信息服务；真实性又称可认证性，保证信息的来源真实、可靠；可控性保证信息始终处于可以有效控制的状态下，把握信息服务的每一个环节；不可抵赖性又称不可否认性，保证信息在收集、存储、传播和使用的每一个过程都留有痕迹，方便日后查证。

2.3 智慧城市信息安全风险的概念、类型及特征

2.3.1 智慧城市信息安全风险的概念

智慧城市是新一代信息技术结合智能化基础设施提供高质量服务的新型城市形态，涵盖多种行业，设备众多，要素复杂，较之传统的信息系统面临更大的信息安全风险。这些风险不仅体现在信息资源本身，还体现在信息载体、信息系统、信息环境和信息主体的方方面面，存在于信息被收集、存储、传播和使用的整个过程，严重影响了信息服务的质量和信息安全。因此，智慧城市信息安全风险就是在智慧城市建设和信息资源使用过程中，基于智慧城市的复杂环境，导致技术失控、外部攻击、信息泄露等一系列信息安全问题的主要影响因素。

2.3.2 智慧城市信息安全风险的类型

智慧城市是一项庞大复杂的综合城市信息重塑工程，通过互联网、大数据、人工智能等新一代信息技术实现城市智能化，因此其信息安全风险包括基础设施、物联感知、网络通信、数据服务及智慧应用等多个层面[②]。

（1）基础设施信息安全风险。随着智慧城市的建设和发展，越来越多的基础设施与互联网相连，加大了基础设施被攻击的风险。一方面，智慧城市基础设施的开放性增加了信息共享的便捷程度，方便信息的获取和传播，但也为不法分子大开方便之门，使基础设施暴露在危险环境中，且基础设施大多处于统一控制

① 王娜,任志宇,王文娟,等.信息安全属性教学问题与对策探索[J].计算机教育,2019,(01):158-161.
② 李洋,田志宏.智慧城市安全风险及其信息安全体系设计[J].保密科学技术,2020,(11):18-21.

下，一旦遭受攻击容易造成整个基础设施体系的瘫痪。另一方面，国内智慧城市信息基础设施建设对国外的产品和服务较为依赖，目前尚未形成自己的产业链，因此在基础设施自主可控方面具有一定的风险。

（2）物联感知层信息安全风险。物联感知层是信息资源收集的源头，也是现实世界和虚拟数据之间的屏障，由大量地传感器和执行器组成。物联网感知层作为安全性最为脆弱的一个环节，被攻击的原因主要分为三类[①]。第一类是窃取用户隐私，通过查找系统漏洞突破设备的访问限制，进而达到非法获取用户信息的目的。第二类是利用物联网攻击其他设备，物联网的级别更高，所发动的攻击规模更大，造成的损害也更大。第三类是过度采集用户信息，一些企业和个人为了谋取更大的利益，通过诱骗或强制等方式过度采集用户隐私信息。

（3）网络通信层信息安全风险。通信层的主要任务是信息的传播和共享，同时还需要保证信息在传播阶段的保密性、完整性和可用性。现阶段常使用的通信层主要包括两种网络类型，一种是传统的互联网，由路由器、计算机和服务器构成，另一种是物联网，由智能设备、传感器和控制器组成。与传统互联网相比，物联网在信息传输和共享方面具有巨大优势，但也因此更容易受到窃听、干扰和攻击[②]。智慧城市目前采用的是物联网与互联网相融合的方式，更是为攻击互联网提供了跳板，极大增加了智慧城市的信息安全风险。

（4）数据及服务支撑层信息安全风险。数据及服务支撑层与物联感知层、网络通信层构成了信息服务的基础框架，共同为智慧城市运行提供云服务。作为智慧城市数据和服务的聚合点，数据及服务支撑层存储的资料较为集中，容易受到信息泄露、外部攻击等威胁，甚至影响整个城市的正常运行。与此同时，数据及服务支撑层还肩负着整合与分析资料的重任，在分析过程中信息高度关联，存在获取用户完整个人信息的隐患，可能造成难以估量的损失。

（5）智慧应用层信息安全风险。智慧城市应用层包含了大量能直接为用户提供服务的应用，包括智慧政务、智慧教育、智慧旅游、智慧家居、和智慧医疗等多个能够根据个人信息和智慧分析手段提供智能化个性服务的领域。这些智慧应用虽然分属不同的领域，但是仍然具有相似的应用层次，面临的信息安全威胁也具有很大的交集。同时因为应用中涉及多个利益方，也会因过度使用、非法买卖、恶意竞争等利益纠葛引发个人信息安全问题。

2.3.3 智慧城市信息安全风险的特征

（1）信息防护手段落后化。智慧城市的建设与大数据技术紧密相连，在现

① 崔炜荣,黄硕,汪超.智慧城市的信息安全与隐私保护问题探究[J].安康学院学报,2021,33(02):122-128.

② Minhaj Ahmad Khan, Khaled Salah. IoT security: Review, blockchain solutions, and open challenges[J]. Future Generation Computer Systems,2018(82):395-411.

有环境下，传统防护手段已经跟不上环境的快速变化。一方面，信息安全技术设备面临风险。基础设施是大数据和智慧城市运行的主要载体，我国信息网络基础设施自主可控程度低，尤其是技术含量较高的设备对国外企业依赖性较高，一旦遭遇数据安全问题，造成的破坏难以想象。另一方面，信息安全技术手段亟需提升。智慧城市发展的速度很快，传统的信息安全技术难以抵抗频繁出现信息安全风险，提升信息安全技术手段对于加强系统防护具有重要作用。

（2）信息管理工作复杂化。智慧城市作为互联网发展下的新型城市形态，与传统城市相比具有更高的数据融合程度和数据共享体验，也面临着更大的信息安全风险，需要更为复杂的管理机制。一是信息安全顶层设计规划能力需要提高。顶层设计是智慧城市建设和发展的风向标，其规划的科学性和合理性直接影响着智慧城市发展的方向，其中对信息安全统筹规划和建设更是智慧城市可持续发展的关键。二是信息安全应急响应能力需要提高。建立应急响应预案是我国信息安全保障的基础，虽然各部门都具有应急预案，但是没有实践的检验和完善，在实际操作中难免存在可操作性不强、针对性不够等问题，难以发挥应急方案的真正作用[①]。三是是信息安全标准规范不完善，法律法规不健全。我国虽然已经出台了保障信息安全的相关文件，但从整体上来看，现行的信息安全相关的法律法规不够健全，不足以抵御智慧城市建设和运行中遇到的信息安全风险。

（3）个人隐私保护紧迫化。随着大数据和人工智能技术的逐渐成熟并在智慧城市建设中落地使用，个人信息在采集、传输、存储和使用的过程不断受到威胁。信息采集方面，智慧城市的感知层通过各种基础设施延伸到城市的每一个角落，个人信息采集变得越来越方便，信息感知设备的运行和采集是否合法需要进一步确认。信息传输方面，5G 和物联网技术加速推进智慧应用的落地和推广，数据的传输需要面对不断更新的应用场景，传统的认证、加密等技术手段已经难以满足信息防护的需求。信息存储方面，智慧城市收集大量的信息并利用大数据中心集中存储，通过关联分析能够将原本隐藏在各个信息系统中碎片化的信息进行整合。信息使用方面，智慧城市能够将大数据分析获取的信息转化成知识，同时融合信息技术，应用到政务、医疗、交通等各个行业，为了对不同应用场景进行分级分类以提供不同程度的个性化服务，需要收集并分析大量的个人信息。

2.4 理论基础

2.4.1 信息生态理论

信息生态根据信息生态系统人与各要素之间的关联关系，合理调配各项资源，

① 孙晓林,张新刚.大数据时代智慧城市信息安全风险与防护策略研究[J].电脑知识与技术,2021,17(22):48-49.

使生态系统保持在一种平衡的状态，能够以最佳的状态完成日常运转[①]。信息生态系统由 Nardi[②]等在 1999 年率先提出，他们认为信息生态系统运转需要特定环境，但人是其中最不能缺少的要素。我国学者对信息生态系统也有所研究，胡运清[③]、王伟赟[④]、陈明红[⑤]等都认为信息、人和信息环境是信息生态系统的基础要素，能够进行自我调节。本文结合相关文献和信息技术在现代化社会中的显著作用，将信息生态因子分为以下四个方面，彼此之间的关系如图 2.1 所示。

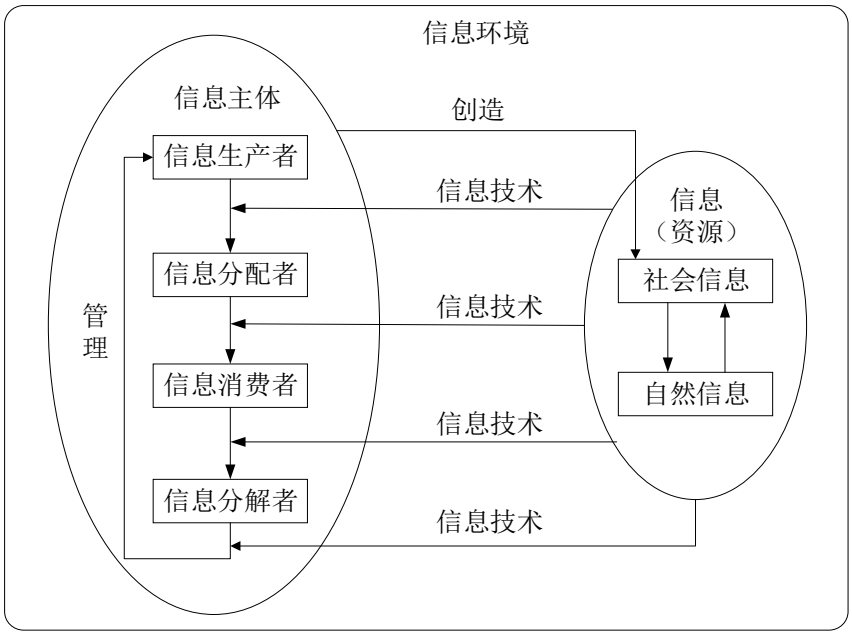


图 2.1 信息生态因子关系模型

（1）信息（资源）。信息是信息生态系统构成的基础，充斥在生活的方方面面，对政治、经济、文化等领域具有重要的影响作用。信息是人和信息环境之间进行交互的基础，信息的收集、传播和利用促进了信息生态系统的循环，而信息的质量也直接决定了信息生态系统的质量。

（2）信息人。信息人是信息生态系统的主体，在信息和环境直接搭建了一座桥梁，一头连结着信息，另一头连结着信息环境，负责信息和环境之间的转化和交流，为信息系统的运转提供动力。根据信息人在信息系统中的作用随着不同应用场景进行自由转换，可以是信息的生产者，可以负责信息传递，同样也可以对信息进行管理和利用。

（3）信息技术。随着大数据技术、人工智能等技术的发展与应用，信息技

① 何志兰.论信息系统的生态对称性[J].情报杂志,2006(06):92-94.
② Nardi, Bonnie A, O'Day, et al. Information Ecologies: Using Technology with Heart - Chapter Four: Information Ecologies[J]. Serials Librarian,2000,38(1-2):31-40.
③ 胡运清.信息生态环境问题研究[J].图书馆工作与研究,2007(04):48-51.
④ 王伟赟,张寒生.和谐社会的信息生态构建研究[J].情报理论与实践,2007(06):728-730.
⑤ 陈明红.信息生态系统中资源配置的博弈行为分析[J].情报理论与实践,2010,33(09):17-22.

术在信息生态系统中的作用越发重要，逐渐成为了信息生态系统的支撑条件。信息技术的存在为信息的传播和利用提供了更便捷的手段，拓展了人与信息环境之间的沟通渠道，提高了系统运作的效率。

（4）信息环境。信息环境是信息人进行信息行为的场所，是全部信息因素的总和，也是信息生态系统赖以正常运转的基础。根据研究对象不同，可以将信息环境分为宏观层面和微观层面；根据要素性质不同，可以将信息环境分为外部环境和内部环境。

2.4.2 社会认知理论

Bandura 于 20 世纪 80 年代末提出社会认知理论（Social Cognitive Theory，SCT）[①]。该理论强调主体认知、个体行为和社会环境三者之间的动态交互影响，认为人们可以根据认知主动控制并调节自身行为，也可以通过对环境的反应来进一步控制行为，由此形成“三元交互”模型[②]，其理论模型如图 2.2 所示。

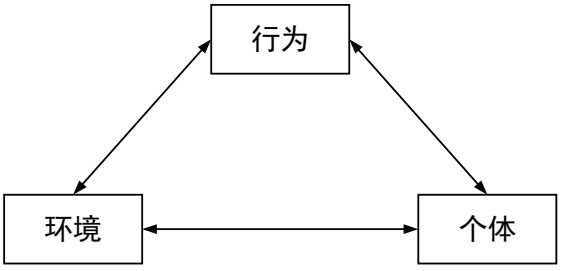


图 2.2 社会认知理论模型

该理论模型是社会认知理论的重要支撑，具体表现为三种作用机理[③]：

（1）主体认知与个体行为之间的交互，即认知对行为起着主导作用，主体认知能够影响其行为，反之行为也可以对认知进行调节和重塑。在智慧城市建设推进过程中，用户对于智慧城市信息安全的认知程度很容易使其产生侥幸、依赖、从众等心理，进而影响用户的行为。

（2）社会环境与个体行为之间的交互，即个体在不同环境中产生不同的行为方式，而不同的行为方式又反作用于环境，带来社会环境的改变。每一个用户的行为都不是简单的个体行为，而是受到周围环境的影响，信息环境的好坏直接影响用户的行为，个体的聚集行为也会对环境造成影响。

（3）主体认知与社会环境之间的交互，即社会环境的变化会影响个体认知的调整，而个体认知也会直接作用于社会环境。对智慧城市信息安全的宣称效果

① Bandura A. Social Foundations of Thought and Action[J]. Journal of Applied Psychology, 1986, 12(1):169-171.
② 张晓娟,李贞贞.基于社会认知理论的智能手机用户信息安全行为意愿研究[J].现代情报,2017,37(09):16-22.
③ 徐娟,黄奇,袁勤俭.社会认知理论及其在信息系统研究中的应用与展望[J].现代情报,2020,40(06):145-153.

会影响用户的认知程度，而用户之间的交流和分享也会对他人的认知和行为产生影响，从而作用于社会环境。

2.4.3 模糊理论

人们在描述客观事物时总是习惯用精确的方式进行表述，但实际上，现实中很多现象的界限都是不清晰的，很难进行精准描述。比如就“下雨”而言，一般会用“大雨”、“小雨”来形容雨量，然而仅仅通过感知无法确定什么程度的降雨量可以称为“大雨”或“小雨”。模糊理论（Fuzzy Logic）是 1965 年由 Zadech 教授创建的，是在模糊集合理论的数学基础上发展起来的[①]，如今已经逐渐应用到科学研究的各个领域。在特定环境中人们按照熟知的标准对问题进行清晰、准确的分类，但经常会遇到仅用描述性语言得不到确定回答的时候，在这种情况下就出现了模糊理论。因此，模糊理论的意义就是根据人的认知对现实事物或现象划分不同的等级，设定严格的界限，用以弥补不能明确描述事物的缺陷。

在指标体系研究中，定性指标的程度较为模糊，难以用精准的数值进行分析，因此可以邀请相关专家根据自身的知识和经验对定性指标进行打分，再通过模糊理论将模糊语义转化成清晰的数值[②]，一方面在一定程度上降低专家仅凭自身经验造成的主观性[③]，另一方面将定性指标进行转化，用数值表示其程度高低，方便后续的分析和计算。本文利用模糊理论衡量智慧城市信息安全风险要素的重要程度，对于难以精确描述的信息风险而言具有独特的优势。

① Saaty T L. Decision Making with Dependence and Feedback: The Analytic Network Process[J]. International, 1996, 95(2):129-157.

② 王姣,范科峰,莫玮.基于模糊集和 DS 证据理论的信息安全风险评估方法[J].计算机应用研究,2017,34(11):3432-3436.

③ 鹿晴晴. 基于 DANP 与模糊 TOPSIS 的 WL 企业供应商选择与管理优化研究[D].郑州大学,2020.

第 3 章 智慧城市信息安全风险要素指标体系构建

3.1 研究设计

3.1.1 研究方法选择

扎根理论（Grounded Theory）是一种灵活且系统的质性研究（Qualitative Research）方法，需要研究者针对研究的问题进行调研，然后根据社会现象和日常经验归纳出概念与范畴，最终将现象和经验上升到理论层面[①]。扎根理论最早由社会学家 Glaser 和 Strauss 于 1967 年提出，适用于研究的探索性阶段[②]，在应用过程中，数据收集与数据分析同步进行，通过分析找出收集信息过程中的不足，根据不足总结经验修正理论，直到形成一个完整的理论框架。

笔者将扎根理论作为构建智慧城市信息安全风险要素识别的理论框架模型，是在充分考虑研究问题特征以及实际成果基础上做出的选择[③]。扎根理论基于实际观察收集原始资料，并通过一系列编码流程，将研究结果建构在一个合理的理论框架内[④]，这对于现有理论无法全面透彻解释的社会现象具有较好的适用性[⑤]。

在使用扎根理论进行探索性分析时，需要对原始资料进行编码，这是扎根理论最核心的环节，也是指标体系构建的关键步骤。编码过程分为开放式编码、主轴式编码和选择性编码 3 个部分[⑥]，开放式编码的作用是从原始资料里概括能够形成概念的短句或词语，罗列能从原始资料中提取到的全部范畴；主轴式编码在于挖掘范畴间的关联关系，通过编码将相同概念归属到同一类别下，建立主范畴和副范畴之间的联系；选择性编码是分析得到的概念类属，从中得到最核心的范畴[⑦]。在所有编码结束之后，还有一个重要步骤，就是检验理论研究是否达到饱和状态，即验证剩余样中是否出现新的概念或范畴[⑧]。扎根理论方法研究的具体流程如图 3.1 所示。

---

① Strauss A, Corbin J M. Grounded theory in practice[M].Sage,1997.

② Glaser B G, Strauss A L. The discovery of grounded theory: strategy of qualitative research[J].Nursing Research,1967,3(4):377-380.

③ 张艳丰,王羽西,邹凯,刘亚丽.智慧城市信息安全影响因素与关联路径研究——基于扎根理论的探索性分析[J].情报科学,2021,39(05):34-40,46.

④ 张敬伟,马东俊.扎根理论研究法与管理学研究[J].现代管理科学,2009(02):115-117.

⑤ 刘鲁川,李旭,张冰倩.基于扎根理论的社交媒体用户倦怠与消极使用研究[J].情报理论与实践,2017,40(12):100-106,51.

⑥ 肖静,陈维政.农民工工作幸福感的影响因素及提升策略——基于扎根理论的探索性研究[J].重庆理工大学学报(社会科学),2016,30(05):53-60.

⑦ 张宝生,张庆普.基于扎根理论的社会化问答社区用户知识贡献行为意向影响因素研究[J].情报学报,2018,37(10):1034-1045.

⑧ 韩正彪,周鹏.扎根理论质性研究方法在情报学研究中的应用[J].情报理论与实践,2011,34(05):19-23.

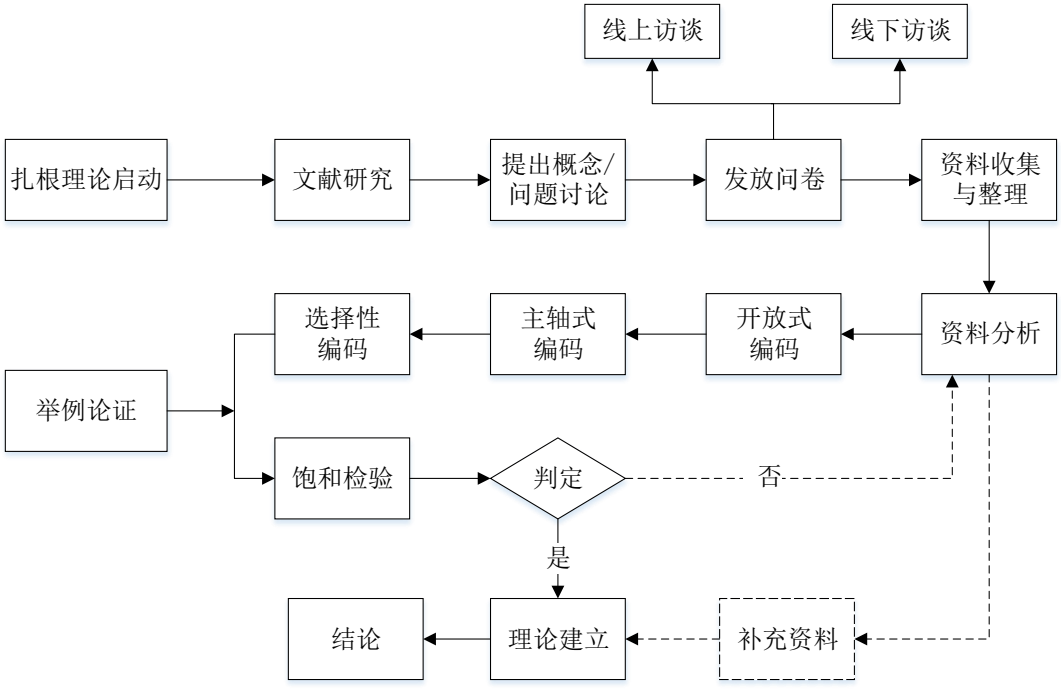


图 3.1 扎根理论研究流程

3.1.2 访谈对象选取

数据收集工作在整个研究中具有重要地位，样本选择的合理性和科学性对研究结果和研究质量有直接影响作用。因此，为全面客观地呈现用户对智慧城市信息安全的认知情况，本文选取的访谈对象遵循以下原则：（1）受访者以中青年为主并具有一定的年龄跨度，了解不同年龄人群对智慧城市的了解程度；（2）尽可能保证访谈对象在性别、职业、地域等分布上的随机性，确保访谈对象的样本多元化，也能了解到不同地域人群对于智慧城市信息安全的理解程度；（3）考虑到普通受访者对智慧城市信息安全的认知水平可能较低，因此选择具有一定文化水平的人群进行访谈。

基于以上原则，选取访谈对象时首先考虑了访谈对象的年龄，年龄因素会影响受访者对智慧城市信息安全问题的认知程度，因此本研究将访谈对象的范围控制在 18-38 岁之间，该群体是智慧城市的主要服务对象，对新事物的接受和适应能力较强，同时具有独立思考及分析问题的能力，对本研究的全面性和深刻性具有重要的保障作用。其次，笔者近 5 年主要在湖南、辽宁和江苏三个省份学习和生活，即研究生就读地、本科就读地和家乡所在地，且基于大学开放性的特征，本科及研究生阶段的朋友来自全国各地，对样本的选择基本能够满足多元性原则。再次，笔者选取的受访者学历背景大多数为本科及以上，对智慧城市信息安全相关问题有一定的认识和了解。本研究选取了 30 名中青年作为受访对象，他们分别来自不同城市，从事不同工作且具有一定的文化水平。基本信息如表 3.1 所示。

表 3.1 访谈对象基本信息一览表

编号	名称	性别	年龄	学历	职业	省份
01	彭先生	男	30	本科	医生	江苏
02	孙先生	男	37	高中	公司职员	江苏
03	蒋女士	女	23	硕士	在读研究生	重庆
04	洪先生	男	32	博士	大学教师	河南
05	张女士	女	22	硕士	在读研究生	江苏
06	张先生	男	28	硕士	公务员	上海
07	解女士	女	27	本科	自由职业	浙江
08	刘女生	女	26	硕士	在读研究生	安徽
09	邱女士	女	25	硕士	在读研究生	江苏
10	薛先生	男	26	本科	公司职员	北京
11	丁女士	女	26	大专	自由职业	江苏
12	樊先生	男	25	硕士	在读研究生	湖南
13	田女士	女	28	本科	小学老师	辽宁
14	郑女士	女	25	硕士	在读研究生	安徽
15	董先生	男	27	本科	公司职员	湖北
16	张先生	男	35	博士	大学教师	吉林
17	朱先生	男	20	本科	在读本科	辽宁
18	周女士	女	25	硕士	在读研究生	河南
19	刘女士	女	24	硕士	在读研究生	河南
20	谢先生	男	31	本科	公务员	安徽
21	李女士	女	27	博士	在读博士	黑龙江
22	逄女士	女	25	硕士	在读研究生	山东
23	徐女士	女	27	硕士	高校辅导员	湖南
24	万先生	男	27	硕士	在读研究生	内蒙古
25	吴先生	男	36	本科	自由职业	辽宁
26	金女士	女	26	本科	舞蹈老师	湖北
27	丁女士	女	27	硕士	律师	上海
28	柳先生	男	24	硕士	在读研究生	上海
29	彭女士	女	26	本科	公司职员	四川
30	唐先生	男	19	高中	自由职业	江苏

本研究选择的 30 名访谈对象年龄差距不超过 20 岁，来自不同的城市，从事不同的职业，具有不同的学历，具体样本统计描述如表 3.2 所示。

表 3.2　受访者统计资料一览表

项目	分类	样本数	百分比（%）
性别	男	14	46.7%
	女	16	53.3%
年龄	18-24 岁	6	20.0%
	25-31 岁	20	66.7%
	32-38 岁	4	13.3%
职业	学生	13	43.3%
	教师	5	16.7%
	医生	1	3.3%
	公务员	2	6.7%
	公司职员	5	16.7%
	自由职业者	4	13.3%
学历	本科以下	3	10%
	本科	10	33.3%
	硕士	14	46.7%
	博士	3	10%

数据显示，从受访者性别来看，男女比例基本平衡，其中男性 14 人，女性 16 人，占受访者总数比例分别为 46.7%和 53.3%。就受访者年龄来看，25-31 岁共 20 人，占受访者总数的 66.7%，这个年龄段的人员相对成熟，对智慧城市信息安全有更深入和全面的了解。从受访者学历来看，30 人中有 27 个是本科及以上学历，占据了受访者总数的 90%，并且受访者除了学生外还来自于多种行业，包括教师、医生、公务员、公司职员及自由职业者，也为调查提供更全面、更精准的资料。

3.1.3 原始资料收集

本研究采用半结构化访谈的方式，通过询问和引导的方式与访谈对象进行深入交流，摸清其对智慧城市信息安全的了解程度，有针对性地调整访谈节奏和谈话艺术，共同探讨智慧城市信息安全的影响因素。相较于正式访谈，半结构化访谈的优势在于更容易获得真实、贴近生活的原始资料。正式访谈的氛围过于严肃，

访谈对象需对谈话内容反复斟酌和润色，而半结构化访谈以受访者为主，采访人员的作用主要是进行引号，并根据受访者的感受和具体谈话内容随时更改谈话方向。在访谈过程中，要注重访谈和分析之间的关系，对每一个受访对象结束访谈之后及时整理访谈资料，概括访谈资料中的核心概念，回忆访谈过程中的不足并对访谈方案加以改进，直到新的对象提供的信息与之前受访者的信息完全重复时停止访谈，至此访谈环节结束。当最后一名受访者资料整理结束后，访谈获得的全部原始资料也已整理完毕，此时在全部受访者的访谈资料中随机选取 20 份用于编码分析，并根据分析结果构建指标体系，剩余的材料在饱和度检验时用以验证理论是否饱和。

另外，在访谈开始之前，需要提前查找文献资料制定访谈提纲，访谈提纲能够帮助访谈人员把握访谈方向、确保访谈质量。实际访谈中，采访人员要受访者回答的内容和访谈的效果实时调整访谈提纲，在不偏离主题的前提下引导受访者进行深入探讨。具体访谈提纲见表 3.3 所示。

表 3.3 访谈提纲

序号	内容
1	您在享受智慧应用的过程中是否遇到过信息安全问题？如果有，能否具体谈一谈？
2	您在遇到智慧城市信息安全问题时是怎么解决的？解决的效果如何？
3	您认为智慧城市发展中信息安全问题愈演愈烈的原因有哪些？
4	您对解决智慧城市信息安全问题，降低信息安全风险有什么建议？

3.2 智慧城市信息安全风险要素指标要素抽取

3.2.1 开放式编码

开放式编码也称一级编码，是扎根理论研究的起点，就是根据受访者表达的意思用短句进行概括和归纳，形成描述现象的概念范畴，然后通过比较，在相似概念中选择更具有概括性的范畴。为防止漏掉原始资料中的重要信息，在开放式编码过程中尽量选择未经加工的受访者原话。具体操作过程如下：首先拆解原始资料语句并进行概念化处理；然后经过反复比较，剔除重复概念，形成 61 个初始概念；最后将性质相近的初始概念进行合并，进一步归纳出 20 个范畴。表 3.4 为开放式编码范畴化的结果，受篇幅影响，每个初始概念仅选取一个原始资料语句进行展示。

表 3.4 开放式编码范畴化

范畴	初始概念	原始资料语句
安全意识	意识薄弱	A01：平时不注意保护个人信息，总感觉骗子不会找上我，结果有一次 接到诈骗电话差点被骗
	依赖引导	A02：使用新软件或新业务时操作不熟练，每次都会寻求工作人员帮助，这个时候就容易将个人信息透露给工作人员
	过度信任	A03：办理业务时自己不会操作，就把手机交给工作人员代为操作，结果额外开通了一些并不需要的业务
信息素养	缺乏了解	A04：对于信息泄露的案例接触的比较少，不清楚什么情况算是信息泄露了，目前来看好像还没有遇到过这类情况
	贪图方便	A05：软件太多设置成不同的密码我根本记不住，只能都设置成一样的，或者直接让系统记住密码，方便下次直接登录
	不会区分	A06：我虽然总是会使用各种软件，自认为还是能跟得上时代的脚步，但是不太清楚自己的信息怎么样是不安全的
心理因素	趋利心理	A07：像推广 APP 之类的活动都会有小礼品赠送，每次看到我都会参与，大不了之后再删除
	从众心理	A08：大家都用的东西，也没听说出了什么问题，就算有风险大家都一样，到时候肯定有人管
	侥幸心理	A09：就是登记基本信息而已，又不是给账号密码，有什么可担心的，再说我也没什么值得骗的
	依赖心理	A10：日常生活中的衣食住行都可以通过一部小小的手机得到满足，但与此同时也会暴露更多基本信息、地理位置甚至个人的喜好
行为要素	操作不当	A11：有时候确实是自己不会操作，不小心点了什么链接，泄露了自己的信息
	难以拒绝	A12：朋友经常会让帮忙填个问卷，这都还好，但是还有需要下载 APP 注册账号的，但是不帮又担心朋友生气
	被迫填写	A13：路上免费发个口罩纸巾什么的，伸手一接才说要帮忙扫码，拿了东西又不好意思还回去，只能被迫填写信息
信息特征	易篡改	A14：信息本身就很容易被修改，稍微动下手指改一下或者拷贝一份都是很容易的
	易失真	A15：信息在传输的过程中往往要经过好几个环节，很容易因为系统或者操作不规范出现漏传、错传等情况
	易串联	A16：像姓名、生日等单一信息安全风险虽然不大，但是很多个独立的信息关联在一起风险就会直线提升
	易泄露	A17：平时不注意扔掉的那些火车票、快递单等都有很多个人信息，随手丢掉会加大信息泄露的风险

续表 3.4 开放式编码范畴化

范畴	初始概念	原始资料语句
信息载体	密码单一	A18：我的账号密码一般都很简单，要不就是生日，要不就是身份证后六位，所以账号曾经被盗取过，才改成了安全性较高的密码
	验证简单	A19：为了防止密码被破解，会将密码设置的复杂一些，软件越多密码数量就越多，有时候忘记密码了就会使用短信验证，输入短信验证码就能够登录了
	丢失风险	A20：手机、U 盘、硬盘等作为常见的信息载体存储了大量的信息，一旦丢失可能造成很大的损失
信息技术	更新速度	A22：信息技术的发展跟不上用户及智慧城市发展的需求，有些较为复杂的服务还要依赖人工进行
	漏洞修复	A23：系统在开发或使用时因技术原因留下漏洞，而且漏洞修复不及时，不仅影响使用还给不法分子留下了可乘之机
	防护措施	A24：对于系统安全的防护不牢固，比如公共图书馆采用的网络协议虽然开放性较高，但是在安全性的设计上就较为薄弱
信息系统	性能不稳	A25：信息技术不够成熟，造成了系统或应用在使用过程中的卡顿、闪退现象，影响使用体验
	入侵风险	A26：系统安全性设计还是要加强，之前就遇到过黑客入侵盗取信息的情况，幸好没有造成严重的影响
	病毒威胁	A27：凡是用到网络的都会受到病毒危险，特别是要提防有人恶意植入病毒来盗取或毁坏信息
信息获取	来源不明	A28：信息能够通过多种渠道进行收集，且传播方便，扩散速度快，一旦出现问题难以追溯源头
	方式违规	A29：有些信息采集方为了尽可能多的收集用户信息，往往采用不正当的手段进行收集，让我更加担心信息的安全问题
	采集过度	A30：不提供个人位置或者通信录就不提供使用权限，除了部分软件可能确实需要之外，这种要求完全没有什么道理
信息存储	设备陈旧	A31：用以存取信息的设备陈旧，不仅影响信息的存取速度，还会影响存取能力，甚至造成信息丢失
	容量不足	A32：随着信息量的剧增和信息的广泛交流，对信息存储设备的容量提出了更高的要求
	备份风险	A33：我有一个习惯，就是要把同一个信息备份到好几个不同的地方，这样感觉更安全一些

续表 3.4 开放式编码范畴化

范畴	初始概念	原始资料语句
信息利用	渠道迁移	A34：信息技术更新很快，尤其是近几年，通过手机足不出户就可以办理业务，根本不用亲自跑过去
	信息追踪	A35：利用信息追踪了解用户的需求和喜好，比如用 12306 买票的时候添加监控功能，这样等有票或者机票降价的时候软件会主动发消息提醒
	范畴模糊	A36：信息在使用时难以划分使用范畴，缺少有针对性的脱密处理，加大了信息安全风险
	人工参与	A37：虽说是智慧城市，但是在实际应用中人工参与比重过大，加大了信息泄露的风险
职业操守	道德败坏	A38：部分从业人员没有树立正确的价值观，在职业活动中不约束自己的行为，甚至利用职务便利触犯法律
	缺少责任	A39：部分工作人员似乎没有意识到工作的重要性，缺少作为信息行业从业人员的责任
	玩忽职守	A40：对于信息的管理一般来说都会有严格的程序，但是有些工作人员不遵守制度，不仅工作懈怠，对待用户的态度也十分不好
业务水平	能力缺失	A41：有些工作人员的工作能力较差，业务不熟练还一问三不知，根本不能胜任这个岗位
	操作失误	A42：工作人员有时因为操作失误会不小心把信息搞错，我就曾经遇到过这种情况，给我造成了不小的麻烦
管理机制	结构失衡	A43：服务主体内部基本都是信息收集人员数量较多，而信息管理人员的数量较少
	缺少培训	A44：服务人员上岗前根本没有进行过系统的培训，对于自己的职责没有形成清晰的认识
	奖惩不分	A45：没有制定明确的奖惩制度，工作都没有积极性，凭什么犯了错误的没有惩罚
	应急缺乏	A46：在遇到关于信息安全问题的突发状况时，应急预案的制定能将损失大大降低
信息机构	冒充官方	A47：有人冒充物流公司给我打电话说快递丢失，让我提供详细信息来追踪物流信息，其实就是骗子
	资质不良	A48：有些企业会委托第三方进行信息采集，但是这些第三方的资质却值得商榷，一些不正规的机构很可能外泄用户信息，甚至进行多次买卖
	推卸责任	A49：有些企业会找中介机构进行信息的收集和存储，一旦出现什么问题，企业和第三方就互相推卸责任

续表 3.4 开放式编码范畴化

范畴	初始概念	原始资料语句
不法手段	不明链接	A50：别人发的链接一定不要随便打开，这很可能是陷阱，用来盗取个人信息或者植入病毒
	钓鱼诱导	A51：有时候登录进的不一定是官网，不仔细核实网站的域名可能会陷入钓鱼网站的骗局
	广告轰炸	A52：通过不停的投放广告进行洗脑，让你不自觉地对产品或服务产生信任，然后趁机收集信息
潜在原因	市场需求	A53：总是有卖房子或者贷款的给我打电话，还不是一家公司的，为了自己的业务真的不择手段
	利益驱使	A54：我听说有人专门买卖用户信息，数量越多利益越大，这些人有没有想过为别人带去了多大的麻烦
	违法成本	A55：目前我国法律对于泄露、交易用户个人信息的行为处罚力度太小，违法成本低，达不到惩戒效果
宣传效果	门槛过高	A56：对于智慧城市信息安全问题的了解有一定门槛，年龄过大或过小、文化程度不高的人很难理解这些东西
	力度不够	A57：除了经常接触这些东西的人可能会了解的多一些，在日常生活中宣传的很少，一旦发生这种事情很多人根本不知道怎么办
重视程度	监管不力	A58：对信息泄露的现象不够重视，在收集和使用用户数据的时候没有起到一定的监管作用
	权责不明	A59：感觉这些工作人员自己都搞不清楚自己的工作，每次出了问题就是推三阻四
政策法规	缺乏保障	A60：对信息安全的重视程度还不够，我看那些散布谣言、泄露信息的就是批评教育一下，那受害者也太惨了吧
	难以落实	A61：即使出台了相关的政策或法律，因为公众不够重视，再加上侵犯信息的行为本身就难以界定，因此想要完全落实还有很长一段路要走

3.2.2 主轴式编码

主轴式编码又称轴心编码，是对开放式编码形成的概念和范畴进行加工，通过分析范畴与范畴之间、范畴与概念之间的关系找到具有总结作用的主范畴。智慧城市涵盖人、信息、技术、制度等多个要素，是典型的信息生态系统，因此，本文结合信息生态理论，从信息、信息人、信息技术和信息环境四个维度出发，对开放式编码形成的 20 个概念进行总结和分析，探索概念之间存在的逻辑关系，并对主范畴的维度进行更细致的划分，最终共发展了 6 个主范畴，分别为个体特征、基础要素、信息服务、人员管理、信息市场和社会环境。具体如表 3.5 所示。

表 3.5 主轴式编码及其内涵

主范畴	对应范畴	范畴内涵
个体特征 C1	安全意识 C11	用户对安全意识薄弱，又因过度信任工作人员，依赖他人的引导而忽略了可能存在的安全问题
	信息素养 C12	用户对信息社会的适应能力，包括对信息安全的了解程度，对信息的使用能力和对安全环境的评估能力
	心理因素 C13	用户使用和处置自身信息时的心理因素，比如贪图小便宜、盲目从众或者产生过度依赖等
	行为要素 C14	用户在日常生活中由于操作不当或不得已为之的行为，不仅包括主动行为，也包括被动行为
基础要素 C2	信息特征 C21	信息本身所具有的容易引发信息安全风险的特征，包括易篡改、易失真、易串联和易丢失等
	信息载体 C22	信息传播中能够携带信息的媒介，即能够进行记录、传输、积累和保存信息的实体工具
	信息技术 C23	包括信息处理技术、信息交换技术和信息防护技术等管理和保护信息安全的技术
	信息系统 C24	由硬件、设备和软件等组成，主要功能是输入、存储、处理、输出和控制信息的系统
信息服务 C3	信息获取 C31	围绕一定的目标，在一定的范围内，通过一定的技术手段和方式方法获得原始信息的活动和过程
	信息存储 C32	将加工整理后的信息按照一定的格式和顺序存储在特定载体中的信息活动，目的是便于检索信息
	信息利用 C33	将收集、加工、存储的信息加以使用，通过智慧应用等方式服务大众
人员管理 C4	职业操守 C41	信息从业人员对自身职业的责任意识和重视程度，以及从事职业时对自身行为的要求
	业务水平 C42	工作人员日常在进行信息服务时的技术水平，以及应对突发状况时的反应能力
	管理机制 C43	在信息管理过程中用来约束工作人员行为，维持正常运转的一系列管理制度
信息市场 C5	信息机构 C51	能够提供专业知识和信息技术指导，并且可以对所需要的信息进行收集、加工、存储和处理的机构
	不法手段 C52	信息市场中常见的为了盗取用户信息所采取不正当的方法和措施
	潜在原因 C53	能够影响信息市场风气，导致信息泄露频繁发生的原因，如市场需求大、低成本高收益、违法成本低等

续表 3.5 主轴式编码及其内涵

主范畴	对应范畴	范畴内涵
社会环境 C6	宣传效果 C61	用户信息安全意识是否提高、信息安全素养是否改善、是否知道如何维护自身合法权益
	重视程度 C62	对用户和企业信息安全、社会中存在的侵犯信息安全的行为以及对执法机构执法力度的关注程度
	政策法规 C63	国家出台用来处理信息安全纠纷问题，打击信息违法犯罪行为，保护信息安全的法律法规

3.2.3 选择性编码

选择性编码又称核心编码，是对主轴式编码形成的主范畴进一步的精炼和概括，由此形成核心范畴，同时探究核心范畴之间的关联关系以及对研究主题产生联系的作用原理，先构成一条条关系链，最终形成一个关系网。因此，结合社会认知理论，根据“三元交互”模型中认知与行为、认知与环境以及行为与环境之间的作用机理，探究核心范畴之间的关联关系，最终得到主范畴之间的关系结构。选择性编码联结关系如表 3.6 所示。

表 3.6 选择性编码联结关系

典型关系	关系结构	内涵
个体特征→信息市场	直接作用	用户的安全意识、信息素养、心理因素和行为要素会对市场需求和市场环境产生直接影响
基础要素 ↓ 信息服务→信息安全	调节作用	信息服务对信息安全产生影响时，基础要素会起到一定的调节作用，即信息、信息载体、信息技术和信息系统水平越高，信息服务对信息安全的影响就越大
社会环境→个体特征	直接作用	社会环境中对于信息安全的宣传和重视程度能够直接影响用户的安全意识和信息素养
个体特征 ↗↘ 人员管理→信息安全	中介作用	个体特征在人员管理影响信息安全的过程中具有中介作用，即人员管理不仅能够直接影响信息安全，还能通过影响用户行为影响信息安全
社会环境→信息市场	直接作用	社会环境的改善，尤其是政策法规的完善对于信息市场的市场环境具有直接影响作用

本研究通过梳理主轴式编码形成的 6 个主范畴与智慧城市信息安全之间的关联关系，发现主范畴具有的三种典型关系结构：（1）直接作用。个体特征和社会环境对信息市场具有直接作用关系，同时社会环境对个人特征也具有直接影响关系；（2）调节关系。基础要素在信息服务对信息安全的影响中起到调节作用，