我国与ISO信息安全标准对比研究*

彭国超 刘 婕

(中山大学信息管理学院 广州 510006)

摘 要:[**研究目的**]信息安全标准作为信息安全保障的指导性技术文件在保障我国信息安全方面起到至关重要的作用。有必要对比我国和ISO信息安全标准的差别,以查找问题。[**研究方法**]该研究通过文献计量和知识图谱相结合的方法对402项我国信息安全标准和378项ISO信息安全标准,以及71项我国在研标准计划和82项ISO在研标准计划进行对比分析。[**研究结论**]研究发现,我国信息安全标准从体量和更新速度上略胜ISO。从主题上来看,我国标准着重于技术类和应用类标准的发展,并已超越ISO。但在信息安全管理体系和隐私保护方面,我国相对落后。此外,我国标准化工作效率和完成度仍有提升空间。

关键词:信息安全;信息安全标准;信息安全保障;在研标准计划;国际标准化组织;文献计量;知识图谱

中图分类号 G353.1 **文献标识码:**A **文章编号:**1002-1965(2022)01-0131-08

引用格式:彭国超,刘 婕. 我国与ISO信息安全标准对比研究[J]. 情报杂志,2022,41(1):131-138,184.

A Comparative Study of Chinese and ISO Information Security Standards

Peng Guochao Liu Jie

(School of Information Management, Sun Yat-sen University, Guangzhou 510006)

Abstract:[**Research purpose**] Information security standards, as guiding documents for information security assurance, play a vital role in protecting our country's information security. It is necessary to compare the differences between Chinese and ISO information security standards to find problems and keep up with the development trends. [**Research method**] In this study, 402 Chinese national information security standards and 378 ISO information security standards, as well as 71 Chinese in-research standard plans and 82 ISO in-research standard plans were compared and analyzed through bibliometrics and knowledge graphs. [**Research conclusion**] The study found that Chinese national information security standards slightly outperform ISO in terms of size and update speed. From the aspect of themes, Chinese national standards focus on the development of technical and application standards, and have surpassed ISO. However, China is relatively backward in terms of information security management system and privacy protection. In addition, there is still room for improvement in the efficiency and completion of standardization work of China.

Key words: information security; information security standards; information security assurance; in-research standard plan; ISO; bibliometrics; knowledge graphs

0 引 言

身处大数据时代,不论是个人生活、企业发展还是国家发展都离不开信息和数据。然而,信息泄露、信息污染、信息侵权、信息破坏等信息安全问题不断凸显[1],对个人、企业和国家都造成了巨大损失和极大的影响。

于个人而言,信息泄漏威胁着个人信息安全和隐私安全。中国互联网络信息中心(CNNIC)发布的第47次《中国互联网络发展状况统计报告》显示,截至2020年12月,21.9%的网民遭遇过个人信息泄露,16.5%遭遇过网络诈骗,8.2%遭遇过账号或密码被

收稿日期:2021-05-08 修回日期:2021-06-28

基金项目:**国家自然科学基金项目"智慧城市APP用户使用行为分化机理研究"(编号:71974215)和中山大学高校基本科研业务费青年教师重点培育项目"科学计量学视角下智慧城市研究热点、发展趋势及跨学科交叉融合分析"(编号:20wkzd17)研究成果之一。**

作者简介:**彭国超**,男,1982年生,博士,教授,博士生导师,研究方向:企业信息系统、智能制造、智慧城市;**刘 婕**,女,1989年生,博士研究生,研究方向:信息管理、信息服务。

盗。手机 APP、恶意 SDK、可联网设备已成为个人隐私泄漏的重要渠道。通过“默认勾选”“霸王条款”或未经授权进行的个人信息的“套取”“强取”“夺取”乱像突出,基于个人信息而发展的数据黑灰产业链条逐步完善[2]。

于企业而言,信息不仅是生产要素,更是企业的无形资产[3]。Solms 指出保护企业的信息安全是在保护企业的信息资产,认为信息安全应被称为商业安全[4]。根据 Verizon 发布数据泄露调查报告显示,数据泄露事件覆盖了几乎全球各行各业的大中小型企业[5]。从 2019 年到 2020 年,仅 1 年时间,已确认的数据泄露事件从 2013 骤增至 3950 起[5-6],涨超 96%。我国公安部与百度联合发布《2020 年网络犯罪防范治理研究报告》显示,预计至 2021 年,网络黑灰产的市场效益将比肩世界第三大经济体,网络犯罪将会是未来十年全球最引人注目的风险之一。

于国家而言,数据的生产能力和掌控能力已经成为国家影响力和主导权的新的体现[7]。美国一边通过“棱镜”计划肆意对人们的电子邮件、社交媒体通信等进行监听监控,另一边却打着“保护信息安全”的旗号抹黑中国,打压排挤中国企业,并借 Facebook 控制舆论。在国际关系日益复杂化、国际竞争日益激烈的当下,中国信息安全领域面临的压力巨大。

可见,信息安全之于个人、企业和国家的重要性都与日俱增,已经成为各方共同聚焦的热点。

信息安全标准是信息安全保障体系中重要的技术体系,发挥着重要的协调和指导作用[8]。在国际上,国际标准化组织(ISO)和国际电工委员会(IEC)联合成立的信息技术委员会 ISO/IEC JTC1 的分技术委员会 SC27 负责信息安全、网络安全和隐私保护领域的标准化工作。截至 2021 年 3 月 5 日,该组织已发布标准 378 项(含已废止标准),在研标准计划 82 项。在我国,全国信息安全标准化技术委员会(SAC/TC260)负责我国信息安全领域的标准化工作,并对口 ISO/IEC JTC1/SC27 的国内标准化工作。目前,SAC/TC260 归口标准已达 402 项(含已废止标准),在研标准计划 71 项。

ISO/IEC/JTC1/SC27 目前有 46 个正式成员国和 34 个观察成员国。其发布的标准包含着最新且获得各成员国认可的技术内容,因而成为了国际信息安全标准的风向标。本研究拟梳理我国 SAC/TC260 归口的全部 402 项信息安全标准和 71 项标准计划,及 ISO/IEC JTC1/SC27 归口的全部 378 项标准和 82 项标准计划,通过对比来分析我国信息安全标准化工作存在的问题,以及未来信息安全标准的发展方向。具体可以分解为三个研究问题:

a. 我国与 ISO 信息安全标准发展路径的差别有哪些?

b. 我国与 ISO 现行信息安全标准的差别有哪些?

c. 我国与 ISO 信息安全标准未来发展方向有何不同?

1 文献综述

我国关于信息安全标准的研究主要分为我国国内信息安全标准研究和国外信息安全标准研究。我国国内信息安全标准研究主要聚焦于我国信息安全标准体系和行业信息安全标准体系研究,如工业、智慧城市、智能网联汽车、工业互联网、核电厂、工业控制系统、数字档案、铁路等。赵文等人[9]梳理了我国信息安全标准体系,并介绍了主要标准之间的关系。陈雪鸿[10]研究了工业信息安全标准体系。关鸿鹏[11]分析了我国工业互联网中的信息安全隐患,提出了工业互联网信息安全标准体系架构的建议。国外信息安全标准的研究主要是对国际信息安全标准和发达国家信息安全标准的内容、体系进行分析,并对我国信息安全标准的研制和体系建立提出建议。谢宗晓[12]介绍了 ISO/IEC 27036 标准体系和 ISO/IEC 27036-3 的内容,分析了 ICT 供应链信息安全风险,针对我国实施实施 ICT 供应链信息安全管理提出了建议。陈湉等人[13]梳理了 ISO/IEC、ITU-T、美国 NIST 和我国的信息安全标准体系,从实用性、适用性和衔接性分析了标准体系框架存在的问题。孙航[14]对比了 ISO、ITU-T、联合国世界车辆法规协调论坛和美国 SAE 信息安全标准,提出了我国汽车信息安全标准体系建设方面的建议。宁华[15]介绍了美国和我国的移动互联网信息安全标准,认为有必要进一步完善我国互联网信息安全标准体系。

国外信息安全标准的研究主要是关于信息安全管理标准具体内容的分析及标准的实施研究,尤其是信息安全管理体系 ISO 27000 族标准的实施问题是国外信息安全标准研究的热点内容。在标准内容方面,国外研究主要是对具体标准的内容进行对比研究。如,Prameet P. Roy[16]对比了美国 NIST 网络安全框架和 ISO 27001 信息安全标准的优缺点。国外在标准的实施方面进行了从影响因素、就绪度到具体实施的一系列细致研究。Susanto 等人[17]综合组织、相关方、工具&技术、方针、文化和知识六个范畴开发了一套测试组织实施 ISO 27001 就绪度的集成解决方案建模软件。Shuchih Ernest Chang 等人[18]通过实证研究发现管理者的 IT 能力、环境的不确定性、行业类型、组织规模都是影响 BS7799 实施的因素。Stefan Fenz[19]创建了 ISO 27002 标准的正式表达式,并展示了如何运用安

全本体提高符合性检查的效率。

可见,现有信息安全标准的对比研究主要是聚焦于具体行业的标准内容对比和信息安全标准体系的对比,缺乏关于信息安全标准整体情况的梳理和主题对比。本研究拟对我国和 ISO 信息安全标准整体情况和标准主题进行对比,以查找我国信息安全标准化工作存在的问题,并分析信息安全标准发展方向。

2　研究方法

文献计量学是运用数学、统计学等计量方法来研究文献或文献相关媒介以掌握科学技术动态特征的学科[20]。自 21 世纪初,文献计量学便被运用于农业标准、中医药标准、科技档案标准、出版业标准等行业的标准研究中[21-24]。李景等[25]用文献计量法分析了农业标准的专业分布和热点领域。刘华[26]运用文献计量法对中外信息与文献国家标准的数量、时间分布、标龄、技术领域分布和国际标准采用情况进行了对比分析。李小涛等[27]用信息计量分析法对我国公共服务标准的进行了研究。陈云鹏[28]系统地分析了文献计量学方法和标准情报需求,提出了基于五维度模型(采用强度、采用广度、采用效度、采用粘度和转化速度)的标准采用影响力分析法。王鹏涛等[23]认为标准文献的计量应从数量维度、制定主体维度、(采用)关系维度和时间维度来进行研究。结合研究问题,本研究将从数量、时间、采用关系和主题四个维度来进行分析。

2.1　**数据来源**　对比中国知网、国家标准馆、中国标准服务网、全国标准信息公共服务平台的标准著录信息发现,全国标准信息公共服务平台的数据最全,且有按照标准归口进行标准分类,因此本研究国内标准数据选用全国标准信息服务平台的数据。ISO 标准信息选用 ISO 官方网站数据。本研究所用数据采集日期为 2021 年 3 月 5 日。为保证数据的权威性和可比性,运用爬虫软件爬取了 2021 年 3 月 5 日当天全国标准信息公共服务平台和 ISO 官方网站上的标准题录信息,包括标准标题、标准状态、发布时间、实施时间和国际标准采用信息。共爬取我国全国信息安全标准化技术委员会(SAC/TC260)归口的标准 402 项,标准计划 71 项,ISO/IEC JTC1/SC 27 归口的标准 378 项,标准计划 82 项。

然而,我国主要的标准服务官网和 ISO 官方网站上关于标准的著录信息中均没有主题词或关键词信息,标准文本也没有标注关键词或主题词,为共词分析带来一定困难。但标准的标题是对标准内容最准确的凝练,因此本研究基于标准标题进行关键词标注。具体标注方法如下:

a. 去除助词、标点符号和数字编号,仅保留有实质性意义的名词;

b. 在不改变原文意义的前提下,根据语义对标题进行尽可能小的单位词组划分。例如,标题“信息技术 安全技术 消息鉴别码 第 1 部分:采用分组密码的机制”的关键词标记为“信息安全技术、安全技术、消息鉴别码、分组密码、机制”,标题“ Information technology Security techniques Encryption algorithms Part 5: Identity-based ciphers Amendment 1: SM9 mechanism”的关键词标记为“information technology, security techniques, encryption algorithms, identity-based ciphers, SM9, mechanism”。

最终,402 项我国信息安全标准共标记关键词 1 506个,378 项 ISO 信息安全标准共标记关键词 1715 个;312 项我国现行信息安全标准共标记关键词 1167 个,207 项 ISO 现行信息安全标准共标记关键词 905 个;71 项我国在研标准计划共标记关键词 374 个,82 项 ISO 在研标准计划共标记关键词 428 个。

2.2　分析方法

2.2.1　频次分析　对信息安全标准历年发布数量进行统计,得出标准发布数量随时间发展的演进趋势图。统计我国标准及所采用国际标准的发布时间,并计算时间差,得出我国标准比国际标准的滞后时间,反映出我国国际标准采用的实效性。对标准的标龄进行统计,并计算出各标龄的占比,可以看出标准老化情况,反映出标准的实效性和复审工作的及时性。根据标准计划下达时间统计在研标准计划数量,可以看出标准计划的完成情况,反映出标准制修订工作的实效性和完成度。

2.2.2　共词分析　现有研究中有学者根据标准编号对标准进行技术领域划分来研究其分布情况。但这种研究方法粒度太粗,无法识别出标准主题的变化。因此本研究采用共词分析法来研究标准主题的特点和变化。共词分析法是一种利用主题词来分析研究领域主题构成的内容分析法[29]。本研究通过对基于标准标题标注出的关键词进行共词分析。

2.2.3　知识图谱　知识图谱旨在对科学知识的发展进程和关系进行可视化描述,具有直观、定量、知识发现等特点。本研究将根据标准标题标注的关键词和标准发布年代运用 VOSviewer 绘制主题演化图、关键词共现图和主题热度图,以更直观的方式呈现研究结果。

3　标准发展路径对比分析

3.1　**历来标准的计量信息对比**　经统计,我国自 1994 年起已发布信息安全标准 402 项,其中已废止 71

项。具体年代分布如图 1 所示。通过比较不同年份发布的标准数量可以看出不同时间点标准化工作的活跃程度。

2004 年以前,我国信息安全标准发布数量较少。1994–2004 年共发布 21 项信息安全标准,其中等同采用 ISO 国际标准 18 项,自主研制 3 项。2005–2014 年,我国信息安全标准发布的数量显著增加,共发布 141 项,其中等同采用、修改采用和非等效采用 ISO 国际标准及其他国家标准 34 项,自主研制标准 107 项。2014 年后,我国信息安全标准年度发布数量持续上升,并在 2018 年达到峰值,至今共计发布 240 项,其中采用 ISO 国际标准及其他国家标准 40 项,自主研制 200 项。可以看出,我国国际标准的采用数量保持着上升趋势,但我国国家标准逐渐从以引进国际标准为主转为以自主研制标准为主的模式。

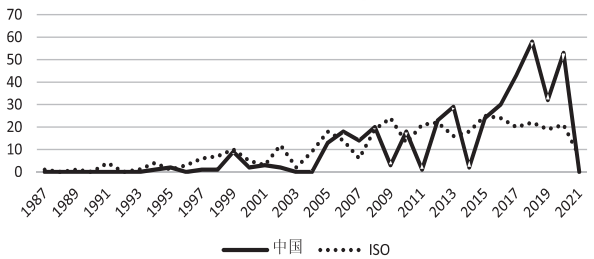

图 1 信息安全标准发布量年度统计

ISO 自 1987 年起已发布信息安全标准 378 项,已废止 171 项。具体年代分布如图 1 所示。首个 ISO 信息安全标准发布于 1987。1987–1995 年,ISO 信息安全标准发布数量较少,共计 12 项。1996–2003 年,ISO 信息安全标准的发布量有所增长。2004 年以后,ISO 信息安全标准年发布量维持较稳定,并在 2015 年达到最高峰。

相较于 ISO 而言,我国信息安全标准化工作起步晚。但 2004 年后我国信息安全标准的发展速度较快。尤其是 2014 年后,我国的信息安全标准化工作发展势头迅猛。目前,我国信息安全标准的体量已经超过 ISO。而我国信息安全标准的研制模式也从以采用国际标准为主的被动型转为了以自主研制为主的主动型模式。根据标准发布数量情况可以大致将我国信息安全标准的发展分为 3 个时期:起步期(1994–2004 年)、成长期(2005–2014 年)、飞跃期(2015 至今)。各阶段信息安全标准情况见表 1。

表 1 我国历来信息安全标准情况一览表

阶段	时间	发布标准总数量(项)	自主研制标准数量(项)	采标数量(项)	采标占比	平均滞后时间(年)
起步期	1994–2004	21	3	18	86%	3
成长期	2005–2014	141	107	34	24%	6.1
飞跃期	2015–2021	240	200	40	17%	5.8

国际标准采用是指以国际标准为基础编制国家标准,根据一致性程度可分为等同采用、修改采用和非等效采用[30]。从我国信息安全标准的国际标准采用情况来看,2004 年以前,我国的信息安全标准以采用国际标准为主,采标数量占该时期信息安全标准总数的 86%。我国国家标准发布的时间比所采用的国际标准平均滞后 3 年。2005–2014 年,我国采用的信息安全国际标准数量虽然有所增长,但在所发布的信息安全标准总数的占比大幅下降,仅占 24%。这一阶段我国国家标准比所采用的国际标准滞后平均时间增至 6.1 年。可见,这一时期,我国信息安全标准化工作的重点放在了自主研制方面,采标工作的速度较慢。2015 年后,我国信息安全标准的采标数量小幅上升,自主研制标准数量几乎翻倍,采标占比进一步降至 17%,采标平均滞后时间降至 5.8 年。可以看出,自主研制标准依然是我国信息安全标准化工作的重点内容,国际、国外标准的采用效率也有些许提升。

3.2 **标准主题演化对比** 对标准关键词进行共现分析,我国和 ISO 信息安全标准分别出现 11 个和 9 个聚类。找到簇中心点,并按照出现时间升序排列(见表 2)。进一步归纳主题发现我国信息安全标准主题大体经历了从信息系统安全、密码技术、安全技术、信息技术、信息安全技术、网络安全、到应用安全的变化。ISO 信息安全标准经历了从网络安全、密码技术、信息技术、信息安全管理到应用安全的转变。可以看出,密码技术、信息技术、网络安全是我国与 ISO 都共同关注过的阶段,目前都处于应用安全发展阶段。

表 2 我国与 ISO 信息安全标准主题聚类对比

序号	我国标准簇中心点	我国标准簇中主要包含对象	ISO 标准簇中心点	ISO 标准簇中主要包含对象
1	信息系统	信息系统、安全性、模型、评估、安全保障	网络安全	网络安全(network security)
2	公钥	公钥、基础设施、系统安全、数字证书	散列函数	散列函数,n 位分组密码,专用散列函数,操作模式
3	安全技术	安全技术、信息技术、实体鉴别、信息安全管理体系、抗抵赖、信息安全管理	机制	机制,实体认证,对称加密算法,密码学检查函数,数字签名技术
4	算法	算法、数字签名、sm2、公钥密码、分组密码、椭圆曲线	加密技术	密码技术,椭圆曲线,附录,数字签名,离散对数,消息恢复,数字签名

续表 2　我国与 ISO 信息安全标准主题聚类对比

序号	我国标准簇中心点	我国标准簇中主要包含对象	ISO 标准簇中心点	ISO 标准簇中主要包含对象
5	信息安全保障	信息安全保障	信息技术	信息技术、安全技术、IT 安全、实践守则、指南、管理、信息安全管理、评价标准、信息安全控制、框架、网络安全、概念、ISO / IEC 27002、电子发现
6	信息安全	信息安全、电子政务、互联网	密钥管理	密钥管理,非对称技术,不可否认性,对称技术,弱秘密
7	鉴别	鉴别、密码、授权、可信计算、接口、签名、访问控制	加密算法	加密算法,轻量级密码学,分组密码,多元自控系统(macs)
8	信息安全技术	信息安全技术、工业控制系统、安全管理、终端、防火墙、网络	信息安全管理体系	审计、认证、密码模块、网络安全、信息安全、ISO / IEC 15408、ISO / IEC 27001、IT 安全技术、隐私保护、随机数生成、安全需求
9	网络安全	网络安全、等级保护、IT	应用安全	应用安全
10	信息技术产品	信息技术产品、操作系统、移动智能终端、个人信息、可控评价	/	/
11	物联网	物联网	/	/

4　现行标准对比分析

4.1　现行标准的计量对比　去除已废止标准和即将实施标准,将 312 项我国现行标准和 207 项 ISO 现行标准的标龄和采标情况进行统计(见表 3)。通常标龄是指“自标准实施之日起,至标准复审重新确认、修订或废止的时间”,也称标准的有效期[31]。标龄可以反映出标准的时效性。数据显示,我国现行信息安全标准标龄在 1 ~ 21 年之间,平均标龄为 5 年。ISO 现行信息安全标准标龄在 0 ~ 23 年之间,平均标龄为 6 年。相比而言,我国标龄为 5 年及以下的比 ISO 高出近 11.1%,平均标龄比 ISO 少 1 年。

表 3　我国与 ISO 信息安全标准标龄统计

标龄(年)	我国信息安全标准数量占比(%)	ISO 信息安全标准数量占比(%)
0 ~ 5	62.8	51.7
6 ~ 10	24.7	33.8
10 ~ 23	12.5	14.5

从采标情况来看,我国现行的 312 项信息安全标准中,采用国际标准共计 55 项,约占 17.6%。其中等同采用 ISO 标准 40 项,修改采用 ISO 标准 13 项,非等效采用 ISO 标准 1 项,非等效采用其他国家标准 1 项。可见,我国信息安全标准主要是以 ISO 为引进对象。

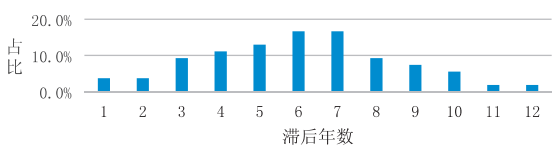

图 2　我国现行信息安全标准采标滞后时间统计

统计我国现行安全标准和所采用国际标准的实施时间差(见图 2)。从采标实效性来看,我国发布的国家标准比所采用国际标准平均滞后 6 年,其中 5 年及以下占 40.7%,5 ~ 10 年 55.6%,10 年以上 3.7%。可以看出,我国在国际标准采用的时效性方面还有待提高。滞后时间过长会导致国内国外技术要求不同步,同时也不利于我国企业的产品、服务的出口。

4.2　现行标准的主题对比　设置最低共现频次为 3,获得我国信息安全标准高频关键词 80 个,ISO 高频关键词 57 个,并绘制关键词共现图,反映出现行信息安全标准的主题情况。根据我国和 ISO 现行信息安全标准主题关键词共现图(见图 3 和图 4)可以看出我国现行信息安全标准最主要的主题是信息安全技术、安全技术、信息技术、网络安全和公钥。而 ISO 现行信息安全标准最主要的主题是信息技术、安全技术、信息安全、信息安全技术和密钥管理。可以看出,我国与 ISO 现行信息安全标准的主要关注点基本一致。

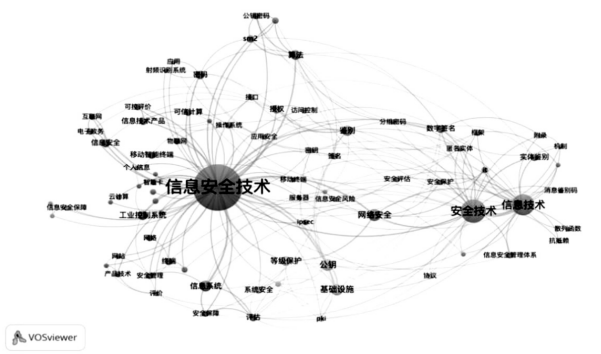

图 3　我国现行信息安全标准主题关键词共现图

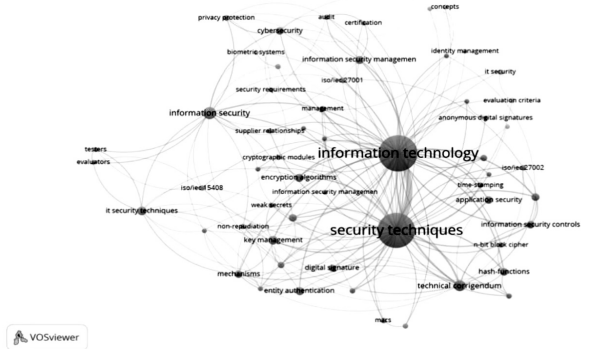

图 4　ISO 现行信息安全标准关键词共现图

对高频关键词进行主题分类后发现,我国和 ISO 信息安全标准皆可分为技术类、管理类和应用类(见表 4)。从技术类标准来看,我国与 ISO 的关注点基本一致。从管理类标准来看,我国对信息安全实施等级保护制度,因此注重信息安全的评价和等级保护。ISO 标准不仅注重对信息安全本身的管理和控制,还关注个人隐私保护。在评价方面,ISO 不仅注重评价方法,还关注评价人员的能力和资质问题。从应用类标准来看,我国国家标准更加细致地关注着信息系统、信息产品及各类应用场景。而 ISO 标准对应用安全的关注则较笼统。

表 4 现行信息安全标准主题对比

标准类别	我国标准主题	我国标准关键词	ISO 标准主题	ISO 标准关键词
技术类	网络	网络、网络安全、互联网	网络	(外部)网络安全(cybersecurity),(内部)网络安全(network security)
	算法	算法、可信计算、椭圆曲线、云计算、散列函数	算法	散列函数、加密算法
	密码	公钥、密码、密钥、分组密码	密码	密钥管理、分组公钥、加密技术、轻量级密码学、不对称技术、弱秘密、对称技术
	签名	数字签名、签名	签名	电子签名、匿名电子签名
管理类	信息安全管理	信息安全管理体系、信息安全风险	信息安全管理	信息安全管理体系、信息安全控制、事件管理、审计、认证、ISO 27002
	评价	可控评价、评价、指标体系、评价方法	评价	评价标准、评价人员、安全评估
	个人信息	个人信息、公民网络电子身份标识	个人信息	身份管理
	等级保护	等级保护	隐私保护	隐私保护
应用类	系统	信息系统、系统安全、操作系统、工业控制系统、办公信息系统		
	产品	信息技术产品	应用安全	生物识别系统、应用安全
	应用场景	物联网、移动智能终端、电子政务、网站、智能卡、移动终端		

5 发展趋势对比

5.1 标准计划计量对比 统计我国和 ISO 在研标准制修订计划下达日期和下达数量发现,我国已下达且未发布正式标准的标准制修订计划共计 71 项,ISO 制修订标准 82 项。统计标准制修订计划数量及年代分布情况(见图 5)。从年代分布来看,我国和 ISO 的标准计划主要集中在 5 年以内。然而不容忽视的是,我国信息安全标准计划中仍有 10 项标准计划进行了 5 年以上还未完成的,占比约 14%。而 ISO 信息安全标准的制修订计划没有持续 5 年以上的。对比而言,ISO 的信息安全标准化工作效率较我国更高,标准制修订计划的完成度也更好。

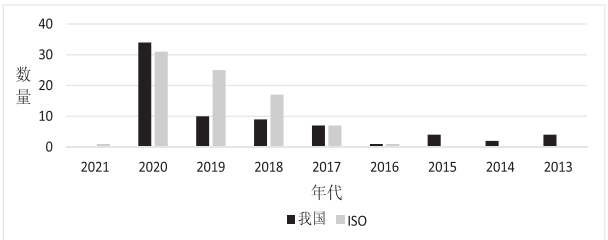

图 5 标准制修订计划年代分布

5.2 标准计划主题对比 设置最低共现频次为 1,获得我国信息安全标准计划关键词 156 个,ISO 标准关键词 167 个。我国信息安全标准计划中最重要、热度最高的关键词是信息安全技术,其次为数据安全、安全技术、信息技术和网络安全。ISO 信息安全标准最重要、热度最高的关键词是信息技术,其次是安全技术、信息安全、网络安全和隐私保护。

对我国和 ISO 信息安全标准计划关键词进行主题分类(见表 5)。从技术层面来看,我国与 ISO 信息安全标准计划在网络安全、算法、密码方面的关注都进一步细化,技术手段更加丰富,且都新增了对数据安全的关注。但我国出现了人脸识别、基因识别、声纹识别、步态识别等新兴技术,ISO 则是进一步发展了签名技术。

从管理层面来看,我国和 ISO 在信息安全管理、评价和个人信息安全方面都进一步发展。其中在信息安全管理上,ISO 标准计划更加全面地覆盖了风险管理和事件管理、能力要求和技术成熟度的要求,我国则仅着眼于能力要求和风险管理。在评价方面,ISO 标准计划涵盖了从评价标准、方法、实验室到评价活动的全流程,而我国还处于评价指标体系和风险评价方面。此外,ISO 标准计划中隐私保护方面的标准进一步发展,而我国仍未有相关标准计划出现。

从应用层面来看,我国和 ISO 在应用场景、产品和

服务上都有部署。但我国的应用场景、产品和服务更加丰富,出现了与我国人民生活息息相关的快递物流、网络支付、网络音视频、即时通信等服务的标准计划,以及与企业息息相关的信息系统、工业控制系统的标准计划。而 ISO 的关注面则更加笼统,主要集中在智慧城市、物联网、工业互联网平台等应用场景方面。

表 5　信息安全标准制修订计划主题分类对比

标准类别	我国标准主题	我国标准主要关键词	ISO 标准主题	ISO 标准主要关键词
技术类	网络	网络、互联网、网间通信、移动互联网、虚拟专用网	网络	(内部)网络安全(cybersecurity),(外部)网络安全(cybersecurity),网络安全框架开发,互联网安全,网络可视化安全, 网络虚拟化安全,通信
	算法	保密性算法、完整性算法、云计算、密码算法、可信计算	算法	加密算法,椭圆曲线生成,椭圆曲线,散列函数
	密码	密钥、分组密码、公钥基础设施	密码	密钥管理,密码技术,多重公钥,跨域密码,基于密码的密钥推导,公钥基础设施,认证加密
	数据安全	数据安全、数据恢复、数据备份、数据处理、大数据安全、网络数据	数据安全	大数据隐私、大数据安全、存储安全
	新兴技术	人脸识别、基因识别、声纹识别、步态识别	签名	匿名数字签名、可重写签名方案、盲签名
管理类	信息安全管理	能力要求、风险管理、使用规范	信息安全管理	风险管理、实施、事件管理、能力要求、风险管理、技术成熟度
	评价	指标体系、安全评价、风险评估	评价	评估标准、评价方法、评价实验室、评价活动、IT 安全评价、评价指南
	个人信息	个人信息安全、个人可识别信息	个人信息	个人可识别信息,个人可识别信息的删除
	等级保护	等级保护	隐私保护	隐私准则,隐私保护,隐私偏好,隐私影响评价,隐私增强数据
应用类	应用场景	智能家居、物联网、移动互联网、供应链、移动智能终端、社交网络平台、政府网站	应用场景	电信组织、移动设备、工业互联网平台、通信、物联网、智慧城市
	产品	App、扫描产品	产品	App
	服务	电子凭据、汽车、电信、云计算、互联网信息服务、即时通信、物流、社交网上购物、快递物流、网络支付、网络音视频	服务	时间戳服务
	系统	信息系统、工业控制系统、重要工业控制系统	/	/

6　研究结果与讨论

根据我国和 ISO 信息安全标准的计量对比,可以看出在标准化工作方面,我国信息安全标准化工作起步晚,但发展迅速,目前体量和规模已达到国际先进水平,进入了发展的飞跃期。我国信息安全标准化工作模式成功地完成了从以引进国际标准为主向以自主研制为主的转变。此外,我国信息安全标准平均标龄为 5 年,比 ISO 少 1 年。我国标龄为 5 年及以下的标准数量比 ISO 高出近 11.1%。这说明我国信息安全技术更新快,市场需求更新速度也快,信息安全行业发展迅速,在一定程度上已超越 ISO。

同时,我国信息安全标准化工作也存在着一些问题:a. ISO 标准是我国信息安全标准的最主要引进对象,但我国标准滞后时间较长,国际标准采用的时效性不高。这会导致我国企业在使用标准时遇到国内、国际标准不对应,甚至相冲突的情况发生,不利于我国信息安全行业的健康发展,也会一定程度上影响我国信息安全产品、服务的出口。b. 我国《国家标准管理办法》规定我国国家标准复审周期一般不超过 5 年[32]。然而我国现行信息安全标准中标龄达 5 年以上的占约 38.2%。有必要及时开展标准复审工作,根据经济技术发展需要更新或废止标准。c. 我国标准计划 5 年以上仍未完成的占 14%,而 ISO 目前所有标准计划均在 5 年内已完成。这反映出我国标准制修订工作水平与 ISO 相比还有一定的差距,完成度和效率仍有提升空间。

从信息安全标准的纵向发展来看,我国信息安全标准未来关注的重点放在了技术和应用层面。在技术上,数据安全的保障和新兴技术的运用得到重点关注。在应用方面,应用场景更加丰富,与民众生活息息相关的产品、服务安全以及与企业相关的系统安全问题都是关注的重点内容。在信息安全管理方面,虽然对个人信息的保护已提上日程,但信息安全管理体系、评价和等级保护方面较现行标准的发展有限。ISO 信息安全标准未来在技术、管理和应用方面都有所部署。技术上,ISO 的关注点在算法、加密技术和数据安全。在管理上,信息安全管理体系更加成熟,评价方面更加完

善,隐私保护也更加全面。在应用上,ISO 从笼统走向细节,在应用场景、产品和服务方面都有所部署。

从我国与 ISO 信息安全标准的横向对比来看,我国与 ISO 信息安全标准发展路径有许多相同和相近之处,但我国缺乏对信息安全管理方面的关注。我国与 ISO 现行标准目前在技术层面的关注点基本一致,但标准计划反映出我国新兴技术层出,已领先 ISO 标准。在管理上,我国在信息安全管理方面的积累和部署稍显不足,且目前缺乏隐私保护方面的标准,也暂未有相关标准计划。但在应用层面,不论是系统、产品、应用场景还是服务安全方面,我国标准都比 ISO 要丰盈得多,且未来将继续保持着这一优势。

7 结 论

本研究用文献计量和知识图谱相结合的方法对我国和 ISO 信息安全标准的发展路径、现行标准和发展趋势进行了分析,研究结果可以为我国的信息安全标准化工作提供一些思考。

a. 我国信息安全标准的采标比例和采标效率有待提升。我国现行信息安全标准总体采标率约为 17.6%,而采标标准比所采用标准平均滞后时间达 6 年。从标准主题对比结果可以看出,在管理类标准,尤其是信息安全管理体系和隐私保护方面,我国标准落后于 ISO,应采取积极的跟进措施,尽快开展相关标准适用性研究和采标工作。b. 积极发挥优势,争取将我国国家标准写入 ISO 标准中。从标准计划主题对比看出,我国新兴技术的运用和应用安全方面的标准已领先 ISO 标准。在这些优势标准上,我国可以采取积极的竞争策略,推动国家标准与国际标准同步制定。积极提出国际标准项目立项,争取成立国际标准工作组,争取工作组召集人职务,并鼓励国内标准起草人参与相关国际标准的制定。c. 进一步加强我国标准化工作规范性和及时性。我国现行标准标龄达 5 年以上的占约 38.2%,标准计划进行 5 年以上仍未完成的占 14%。这些都反映出我国标准化工作仍有相当一部分未能如期进行和完成。相关技术委员会和标准管理部门应加强对归口标准的监控,将标准复审工作常态化。此外,标准管理部门还应在标准计划审批时加强对标准必要性的评估和对起草单位执行能力的关注,加强对执行情况的监督。

本研究聚焦于我国和 ISO 信息安全标准的对比。未来还可以将我国和美国、英国、欧洲、日本等发达国家的信息安全标准进行对比,以进一步深入研究信息安全标准化国际动态。这有利于我国更准确地掌握国际信息安全标准的发展方向,为我国争夺信息安全的国际话语权提供助力。此外,本研究是运用量化的方法对我国和 ISO 信息安全标准的研究,仅是对标准总体情况的概览。未来可以对标准内容进一步深入对比和分析。

参 考 文 献

[1] 张 鹤. 现代信息技术环境中的信息安全问题及其对策研究[J]. 信息系统工程, 2018(8):81.

[2] 王 超,张博卿. 我国个人信息安全乱象及治理措施研究[J]. 网络空间安全,2020,11(1):6-10.

[3] 左 军,杨建梅. 论信息资产[J]. 改革与战略,2000(5):27-30.

[4] Von Solms B, Von Solms R. From information security to…business security? [J]. Computers & Security, 2005, 24(4): 271-273.

[5] Verizon. 2020 data breach investigations report[R/OL]. [2021-03-29]. https://enterprise.verizon.com/resources/reports/dbir/2020/introduction/.

[6] Verizon. 2019 data breach investigations report[R/OL]. [2021-03-29]. https://enterprise.verizon.com/resources/reports/dbir/2019/introduction/.

[7] 冷晓彦. 大数据时代的信息安全策略研究[J]. 情报科学, 2019,37(12):105-109.

[8] 吴志刚. 信息安全标准体系初探[J]. 信息网络安全,2005(3):37.

[9] 赵 文,苏 红,胡 勇. 信息安全标准关系分析[J]. 信息网络安全,2009(11):48-50.

[10] 陈雪鸿,柳彩云,杨帅锋. 工业信息安全标准体系研究与思考[J]. 保密科学技术,2019(7):25-28.

[11] 关鸿鹏,李 琳,李 鑫,等. 工业互联网信息安全标准体系研究[J]. 自动化博览,2018(3):50-53.

[12] 谢宗晓,董坤祥. ICT 供应链信息安全标准 ISO/IEC 27036-3 及体系分析[J]. 中国标准导报, 2016(3):16-21.

[13] 陈 湉,张彦超,赵 爽. 国际信息安全标准现状研究及对我国标准体系建设的思考[J]. 信息安全与通信保密,2016(11):41-47.

[14] 孙 航,解瀚光,王 兆. 智能网联汽车信息安全标准体系建设与产业政策研究[J]. 中国汽车,2018(12):38-43.

[15] 宁 华,潘 娟. 移动互联网信息安全标准综述[J]. 信息安全研究,2016,2(5):429-434.

[16] Roy P P. A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard[C]. 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA). Durgapur, India, IEEE, 2020.

[17] Susanto H, Almunawar M N, Tuan Y C. Information security challenge and breaches: Novelty approach on measuring ISO 27001 readiness level[J]. International Journal of Engineering and Technology, 2012, 1(1): 67-75.

[18] Ernest Chang S, HO C B. Organizational factors to the effectiveness of implementing information security management [J]. Industrial Management & Data Systems, 2006, 106(3): 345-361.

(下转第 184 页)

(上接第 138 页)

[19] Fenz S, Plieschnegger S, Hobel H. Mapping information security standard ISO 27002 to an ontological structure[J]. Information and Computer Security,2016,24(5):452-473.

[20] 邱均平. 文献计量学的定义及其研究对象[J]. 图书馆学通讯,1986(2):71.

[21] 汪玉薇,解　丹,毛树松. 2010-2014 年中医药标准化的文献计量学分析[J]. 中医药导报,2016,22(13):60-63.

[22] 吴　康. 我国科技档案标准文献计量分析[J]. 机电兵船档案,2018(1):66-70.

[23] 王鹏涛,许　玮. 基于标准文献计量的出版业标准化工作研究[J]. 科技与出版,2019(10):116-124.

[24] 刘　拓,鲁　洋,朱秋鸿. 基于文献计量的职业卫生标准应用情况分析[J]. 中华劳动卫生职业病杂志,2019(1):49-52.

[25] 李　景,刘亚中. 农业标准文献专业分布与热点领域的文献计量学分析——以国家标准馆 2006-2008 年度新到馆藏为例[J]. 图书情报工作,2009,53(18):44-47,78.

[26] 刘　华. 基于文献计量的国内外信息与文献国家标准对比研究[J]. 图书情报工作,2011,55(12):51-55.

[27] 李小涛,邱均平. 公共文化服务标准的计量分析[J]. 重庆大学学报(社会科学版),2015,21(6):132-139.

[28] 陈云鹏. 标准计量分析方法研究及农业应用[D]. 北京:中国农业科学院,2016.

[29] Callon M, Law J, Kip A. Mapping the dynamics of science and technology [J]. Sociology of Science in the Real World,1988,14(1):165-168.

[30] 全国标准化原理与方法标准化技术委员会. GB/T 200002—2009 标准化工作指南:第 2 部分 采用国际标准[S]. 北京:中国标准出版社,2010:1.

[31] 国家标准平均标龄[Z/OL]. 国家标准频道[2021-03-30]. http://www.chinagb.org/Article-83591.html.

[32] 国家技术监督局. 国家标准管理办法[Z/OL]. [2021-03-30]. http://www.sac.gov.cn/sbgs/flfg/gz/xzgz/201609/t20160909_216633.htm.

(责编/校对:刘影梅)