个人信息保护合规审计的辅助实现技术框架研究*

刁毅刚[1]，张玲翠[2]，刘晓蒙[3]
（1. 中央网信办（国家网信办）数据与技术保障中心，北京 100048；
2. 中国科学院信息工程研究所，北京 100085；
3. 中电科网络安全科技股份有限公司，四川 成都 610095）

摘 要：数字经济时代背景下，合格评定工作呈现出数字转型趋势，这将对开展个人信息保护合规审计活动产生重要影响。概述了个人信息保护合规检查技术工具概况和相关关键技术，在此基础上，提出了个人信息保护合规审计可以依托技术辅助实现的审计项，指明了个人信息合规审计工作技术辅助实现的路径。依托以上研究成果，提出《个人信息保护合规审计技术能力及工具要求（征求意见稿）》标准，明确了个人信息保护合规审计辅助实现技术框架，介绍了依据标准研发的个人信息保护合规审计技术工具原型，及其对于个人信息保护合规审计辅助技术框架的示范验证作用。

关键词：个人信息保护；合规审计；合格评定；数字化
中图分类号：TP27 **文献标识码**：A **DOI**：10.19358/j.issn.2097-1788.2024.09.008
引用格式：刁毅刚，张玲翠，刘晓蒙. 个人信息保护合规审计的辅助实现技术框架研究［J］. 网络安全与数据治理，2024，43(9)：49-54.

Research on the framework of assisting technology for implementation of personal information protection compliance audit

Diao Yigang[1], Zhang Lingcui[2], Liu Xiaomeng[3]
(1. Data and Technology Support Center of the Cyberspace Administration of China (CAC), Beijing 100048, China;
2. National Computer System Engineering Research Institute of China, Beijing 100085, China;
3. CETC Cyberspace Security Technology Co., Ltd., Chengdu 610095, China)

Abstract: In the context of digital economy, the process of digital transformation trend is appearing among conformity assessment activities, which would exert important influence on the personal information protection compliance audit activities afterwards. This article introduces the situation and development of checking software for personal information protection and the relevant technologies. According to basis of pre-research, this article enlists audit items that could be implemented and supported with the help of technical methods, specifying the path to accomplish personal information protection compliance audit activity with the aid of technical assistance. Basing on the research production done beforehand, the research team proposes the standard of "Specification for the technical ability of auditing for personal information protection compliance and Software", which demonstrates the framework of assisting technology for implementation of personal information protection compliance audit. This article also introduces the prototype of software assisting for personal information protection compliance audit and its function as the demonstration and verification for the framework.

Key words: protection of personal information; compliance audit; conformity assessment; digitization

0 引言

党的二十大报告提出加快建设网络强国、数字中国，加快发展数字经济。近年来，顺应数字经济的发展需要，我国积极推进数字经济领域立法，从《网络安全法》的施行到《民法典》的颁布实施，从《数据安全法》《个人信息保护法》的制定出台到相关领域制度、标准、政

*基金项目：国家重点研发计划基金项目（2023YFB3106505）

策文件的起草和征求意见，在数字经济发展和法治建设进程中，我国数据安全、个人信息保护法律制度逐步建立并不断发展完善，数字经济法治环境日益完备健全[1]。近年来，个人信息保护合规审计受到业界广泛关注，其不仅有利于保护公民个人信息权益，还有望对解决公共数据授权运营等数据开发利用活动中的数据安全问题，对数字经济发展产生重要而深远的影响。

2021 年出台实施的《个人信息保护法》第五十四条、第六十四条明确提出开展个人信息保护合规审计，构成个人信息保护合规审计制度的法律依据；2021 年 11 月，面向社会公开征求意见的《网络数据安全管理条例（征求意见稿）》第五十三条规定“大型互联网平台运营者应当通过委托第三方审计方式，每年对平台数据安全情况、平台规则和自身承诺的执行情况、个人信息保护情况、数据开发利用情况等进行年度审计，并披露审计结果”[2]；2023 年 11 月，国家互联网信息办公室将《个人信息保护合规审计管理办法（征求意见稿）》（以下简称“《办法》”）面向社会公开征求意见，《办法》共 16 条，其中附录《个人信息保护合规审计参考要点》（以下简称“《要点》”）共 31 条，《办法》从审计分类、主体范围和审计频率、审计机构、审计时限等方面明确了个人信息保护合规审计的相关要求，《办法》的出台使个人信息保护合规审计制度落实落地更具可操作性，也对个人信息保护合规审计工作提出更严格细致的要求。

按照我国相关制度的顶层设计，个人信息保护合规审计是一项融法律、数据治理、网络（数据）安全技术“三位一体”的综合性合规活动，具备一定专业性、创新性[3]，要做好这项工作，相关方宜树立系统思维，结合所在单位个人信息处理的实际，运用专业团队和手段，有效应对个人信息保护合规审计的审计项多、存证工作量大、技术性强等特点，履行好个人信息处理者的责任。

1　个人信息保护合规审计活动的数字化转型

2023 年以来，中国科学院信息工程研究所、中电科网络安全科技股份有限公司、北京安华金和公司、北京时代新威公司等多家国内科研院所、高科技公司相继推出自研的个人信息保护合规审计工具，尝试运用信息化手段赋能个人信息保护合规审计活动。主要试图解决以下几方面问题：一是通过信息化手段解决个人信息保护合规审计执行流程的规范化、标准化问题；二是提出技术审计思路，通过数据分析手段完成原本需要依靠人力解决的审计工作，节约人力、提高效率；三是运用知识库、数据挖掘等技术手段，通过对过往审计案例的积累、分析，为新审计案例提供参考和指引，提高个人信息保护合规审计活动规范化、专业化、智能化水平。

中国合格评定国家认可委员会于 2011 年出台的《管理体系认证机构要求》（CNAS－CC01，等同采用 ISO/IEC 17021 标准）中提出，“认证机构应确定与特定认证方案相关的每个技术领域所需的能力，以及认证活动的每项职能所需的能力”，认证活动需要相应技术能力确保活动的公正性、一致性。《要点》中所列部分审计项的可技术验证性，近年来已不同程度地在业务实践中得到证明，信息化手段可赋能个人信息保护合规审计活动，在提升个人信息保护合规审计工作效率、降低个人信息保护法律法规落地成本的同时，还将更好地落实《管理体系认证机构要求》，降低审计活动的主观性、随机性，提高公正性、一致性，将顺应数字经济时代大的发展趋势，促进评估、认证产业数字化转型。当前，在个人信息保护合规审计制度落地前，开展针对个人信息保护合规审计的技术工具及相关标准的研究，是具有现实意义的。

2　个人信息保护合规检查工具和关键技术分析

在个人信息保护合规检查工具软件层面，普华永道公司推出数字化平台 Privacy Ready[4]，该工具平台聚焦《个人信息保护法》，为企业梳理个人信息处理场景，自动精准识别合规问题，并持续追踪风险处置进程，优化合规管理流程；网易公司的网易易盾隐私合规测评平台，提供 App 个人信息保护合规检测，可以定位问题，将检测结果可视化；腾讯公司的 T-Sec 应用合规平台基于相关法律法规、国家标准、行业标准，通过静态检测和动态检测技术，结合隐私合规专家团队专业意见，识别小程序的数据隐私合规问题；抖音集团也具备 SDK 一站式个人信息保护合规解决方案。

在关键技术层面，各国数据安全保护法律法规日益健全，境内外许多法律法规都对日志留存提出了刚性要求，如我国《网络安全法》、网络安全等保标准，欧盟 GDPR（General Data Protection Regulation）、美国 HIPAA（Health Insurance Portability and Accountability Act）等，这些法律制度要求机构保留、保护并审计敏感数据的访问和使用情况，相关网络、数据安全制度的确立为日志审计技术的应用提供了发展空间。日志审计技术能够全面记录和审计网络系统、设备的操作日志、访问日志，通过对这些日志的深入解析，系统能够及时发现潜在的安全威胁、异常行为或系统故障，确保组织能够满足相关法规的合规性要求。日志审计技术分为日志采集、存储、监控、告警、分析、审计等若干环节。

3　个人信息保护合规审计可技术辅助实现相关要点分析

《要点》是对审计内容的归纳和细化，吸收了《个

人信息保护法》等法律、行政法规和国家标准的强制性要求，提出31条审计要点，130余条审计项。审计项内容主要分为个人信息权益保障和个人信息处理者基本义务两类，涵盖合法性基础、透明度、第三方管理、特殊个人信息处理场景、个人信息权益保障、内部个人信息安全管理制度与技术措施、大型互联网平台运营者义务等多个方面，可为开展个保合规审计活动提供参考。在这些要点中，可通过技术手段辅助审计[5]，形成标准化审计模式的条款主要分为以下几类。

3.1 个人信息处理活动的合法性基础验证

此类验证方式涉及的审计要点为《要点》第二条第（一）项，验证个人信息处理者处理个人信息是否取得个人同意。通过设备权限调用、网络代理抓包、SDK检测等技术，检查个人信息处理者在用户同意隐私政策等个人信息处理规则前的接口调用情况，判断是否存在未经用户同意收集个人信息的行为。

3.2 个人信息处理规则验证

此类验证方式涉及的审计要点为《要点》第三条和第四条，个人信息处理规则的内容验证和告知义务的履行情况。采用自然语言处理、关键字和内容识别、智能模型学习等相关技术，对不同业务类型个人信息处理规则、告知文本建立相应的模型算法，识别“等”“必要期限”等模糊用词，验证文本内容的独立性、合理性、完整性、易读性，是否达到“有效的告知”[2]。此外，通过调用个人信息处理者提供的互联网通道或接口，获取告知文本、发布时间和版本信息，及时发现告知文本的内容变化。

3.3 法律文件、制度规则、评估报告类材料验证

此类验证方式涉及的审计要点为《要点》第五条、第六条、第十五条、第二十一条、第二十五条、第三十一条，验证个人信息处理者文本类材料内容的完备性和合理性，包括与共同处理者、委托处理者及（境外）数据接收方等主体签署的法律文件；个人信息保护制度和操作规程、个人信息保护负责人及相关人员履职评价制度、个人信息安全事件应急响应制度等制度文件；个人信息保护影响评估报告、平台企业社会责任报告等报告类材料。通过文字识别、图像识别等技术将材料信息转化为电子文本，利用自然语言处理、文本挖掘技术对文本进行语义分析，提取关键词、主题和重要句子，发现有价值的信息以及关联关系，辅助审计人员快速审核文本类材料，判断其内容要素是否符合法律要求，从而提升审计效率。

3.4 同意记录完整性验证与对比分析

此类验证方式涉及的审计要点为《要点》第二条第（一）项和第（四）项、第八条第（一）项、第十条第（一）项、第十一条第（一）项、第十三条第（一）项，基于个人同意处理个人信息，是否对个人同意或单独同意的操作进行记录。此审计项实现自动化审计的前提是个人信息处理者通过电子化手段在后台保存了用户同意记录，包括个人信息收集的明示同意，收集敏感个人信息收集、向其他个人信息处理者提供个人信息、公开个人信息的单独同意等。通过对电子记录进行自动扫描与分析，识别是否记录了用户名、同意内容、同意时间、同意类型等要点。同时，形成无同意记录的个人信息清单，核查是否属于不需取得个人同意的情况。

通过将反映个人信息处理情况的人员操作日志，数据库、文件系统、数据仓库等数据操作日志，数据访问、数据外发、ETL（Extract－Transform－Load）日志等数据流动日志与用户同意记录等进行对比，检查是否存在处理个人信息与同意内容不符的情况[6]。

3.5 个人信息权益保障验证

此类验证方式涉及的审计要点为《要点》第十七条、第十八条和第十九条，个人信息处理者是否保障个人行使个人信息权益的权利。通过对个人信息收集时间、约定处理期限进行分析，识别超出存储期限的个人信息。通过对个人信息处理者保存的撤回同意，注销账号，查阅、复制、转移、更正、删除权[7]的申请记录，以及响应记录、执行删除或匿名化处理的日志记录等进行扫描分析，识别申请时间与执行记录是否一致、执行时间是否合规、执行结果是否成功等。

3.6 向境外提供个人信息的情况检查

此类验证方式涉及的审计要点为第十五条，向境外提供个人信息是否履行网信部门规定的合规义务。在判别个人信息处理者存在个人信息出境前提下，识别出境个人信息的内容、类型、规模、出境的目的地、保护状态、操作行为等，形成个人信息出境清单，支撑审计人员研判是否需要开展数据出境安全评估、个人信息标准合同备案等合规工作。

3.7 安全技术措施有效性验证

此类验证方式涉及的审计要点为《要点》第二十二条，个人信息处理者是否采取与所处理个人信息规模、类型相适应的安全技术措施。通过对加密日志、脱敏日志、认证授权日志等安全日志进行分析，结合去标识化处理、访问控制等相关技术文档，以及网络出口和安全设备的安全措施、权限列表，验证个人信息处理各阶段使用的安全技术措施，辅助审计人员判断其与所处理个人信息规模、类型的适应程度。

综上，基于流量检测、日志审计、自然语言处理、大数据分析、机器学习等技术，结合审计流程管理、审计知识图谱、审计证据固定、审计报告出具等管理功能，可以实现将个人信息保护合规审计工作与机构的合规流程相结合，完成从审计项目计划到审计问题整改的闭环管理[8]。通过对日志、记录等电子化审计证据进行关联分析，可以实现部分审计项的自动化判定，辅助审计人员判断其他审计项的合规情况，从而提升个人信息保护合规审计工作的质量、可信度、效率、全面性和透彻性[9]。

4 《个人信息保护合规审计技术能力和工具要求》团体标准及审计技术工具

为探索开展个人信息保护合规审计的方法和规律，中国科学院信息工程研究所、中电科网络安全科技股份有限公司等研究机构、高科技公司组织研究起草了《个人信息保护合规审计技术能力及工具要求（征求意见稿）》团体标准并研发了示范验证工具。

4.1 《个人信息保护合规审计技术能力和工具要求》团体标准

4.1.1 制定标准的目标

《个人信息保护合规审计技术能力及工具要求（征求意见稿）》团体标准适用于规范个人信息处理者使用技术工具开展个人信息保护合规自审计工作，也适用于专业机构使用技术工具开展第三方合规审计工作，同时也可为技术工具的开发方、用户、测试方提供参考和指导，有利于个人信息处理者合规技术的规范化和标准化，提高个人信息处理活动合规工作水平。

标准提出了一套个人信息保护合规审计的技术能力框架和合规审计工具功能框架，提出了选择适宜的工具以确保审计有效性和准确性的判定原则。

4.1.2 标准的主要内容

《个人信息保护合规审计技术能力及工具要求（征求意见稿）》标准主要用于规范在审计技术能力方面的要求以及工具实现要求：

（1）合规审计技术三项能力：合规审计证据要求是合规审计技术的基础能力，对审计证据内容及格式、采集及传输、存储及保全提出要求，既保证兼容不同格式的审计证据，也保证证据的防篡改、防伪造，所有的审计工作都基于真实的证据信息进行，才能获得真实的审计结果；合规审计分析能力是合规审计的核心能力，能够支撑对证据的基础处理、基于场景的关联分析、细粒度的单个合规审计项的分析能力等；审计知识库是为审计分析提供知识库、案例库层面的支撑能力。能力框架具体如图 1 所示。

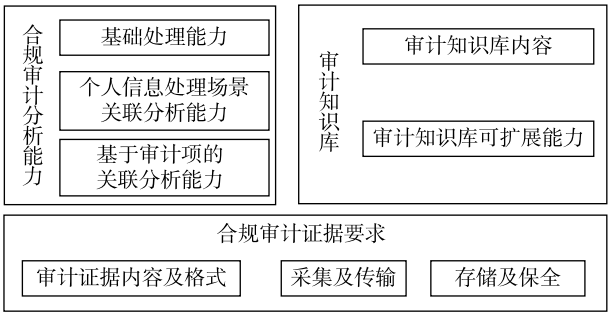

图 1 个人信息保护合规审计技术能力框架

合规审计能力要求既对个人信息处理者的日常业务提出了具体存证要求，也对合规审计执行方提出了执行方面要求，在日常审计实践中，要将以上二者技术能力加以综合，才可以实现可信的自动化个人信息保护合规审计。

（2）工具实现要求：合规审计工具的主旨目标是降低人工审计的人力和时间成本，提高审计效率，提高自动化和电子化水平。主要由三部分功能组成：核心功能主要实现自动化审计以及人工审计的电子化，管理功能主要是实现审计任务管理、证据管理和审计项管理，基础服务主要为提供知识库、日志管理、接口管理、配置管理、安全保护等服务。工具的能力框架具体如图 2 所示。

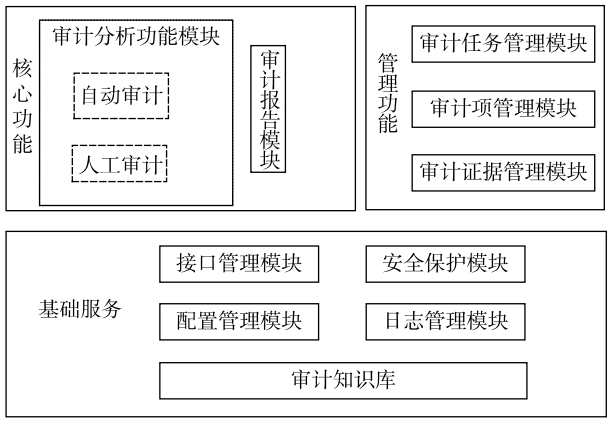

图 2 个人信息保护合规审计工具框架

4.2 个人信息保护合规审计技术工具

按照“政策文件－标准－软件工具”思路，在研究起草《个人信息保护合规审计技术能力及工具要求（征求意见稿）》基础上，组织力量开发了个人信息保护合规审计示范验证工具，对个人信息保护合规审计辅助实现技术框架和《个人信息保护合规审计技术能力及工具要求（征求意见稿）》标准开展示范验证。个人信息保护合规审计示范验证工具的输入主要包括

以下 4 方面：

（1）相关业务系统全方位的日志信息，例如：用户操作日志、数据操作日志、访问日志、存储日志、数据传输日志、数据安全保护日志；

（2）报告类，例如：App 检测报告、个人信息保护影响评估报告、数据出境安全风险自评估报告、平台企业社会责任报告、以往进行的渗透和漏洞扫描报告、等保测评、网络和数据安全风险评估、数据安全认证、个人信息保护认证等；

（3）制度类材料：组织与人员、敏感个人信息处理制度、个人信息全流程安全保护制度、个人信息安全事件应急响应、个人信息保护影响评估制度、个信息处理者的用户投诉举报渠道和机制，个人信息处理规则及隐私政策、平台规则；

（4）其他材料：与共同处理者、委托处理者及（境外）数据接收方、平台内产品和服务提供者等主体签署的法律文件，个人信息匿名化处理、去标识化处理、自动化决策、访问控制等相关技术文档，网络出口及安全设备的安全措施、权限列表，涉及个人信息的法律文件、重大案件情况等。

设计系列工具实现个人信息保护合规审计过程的自动化。基于上述资料，进行数据资产梳理和敏感个人信息识别，需要有自动化手段梳理数据资产，需要能够识别出个人信息，并根据数据特征判断；采集个人信息保护合规的证据。例如，个人信息处理活动包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等，每个阶段使用的个人信息保护技术手段（如审计、脱敏、加密等）的网络日志和安全策略；为审计人员提供不同行业个人信息保护政策和审计案例知识库，随着各行业的个人信息保护合规审计项目的增加，通过不断完善的法律法规和审计要点知识库，更大范围适应不同行业个人信息保护需求，提升审计的自动化程度和准确率。工具的研究思路如图 3 所示。

在个人信息保护合规审计场景中，涉及业务系统、本机构跨系统部门、第三方信息共享机构、监管部门、第三方测评机构等多类业务主体；业务流程涉及业务系统数据收集、本机构跨系统数据共享、跨机构跨系统数据共享等；业务系统在运行过程中会收集多种个人信息，其中可能包含大量敏感个人信息。以电商业务系统为例，在用户注册、登录、系统定位、支付、评价/评论等过程中，个人信息处理者收集的用户个人信息可能包括用户身份证号、手机号、位置数据、银行账号、支付信息、评论内容等。同时，业务系统也会产生各类日志数据，例如用户身份认证日志、访问日志等，应用场景如图 4 所示。

《个人信息保护合规审计管理办法》正式出台实施后，《个人信息保护合规审计技术能力及工具要求》团体标准各有关参与单位将继续做好标准研究起草和审计工具研发迭代工作，在个人信息保护和数据安全领域，继续探索合格评定工作数字化转型之路。

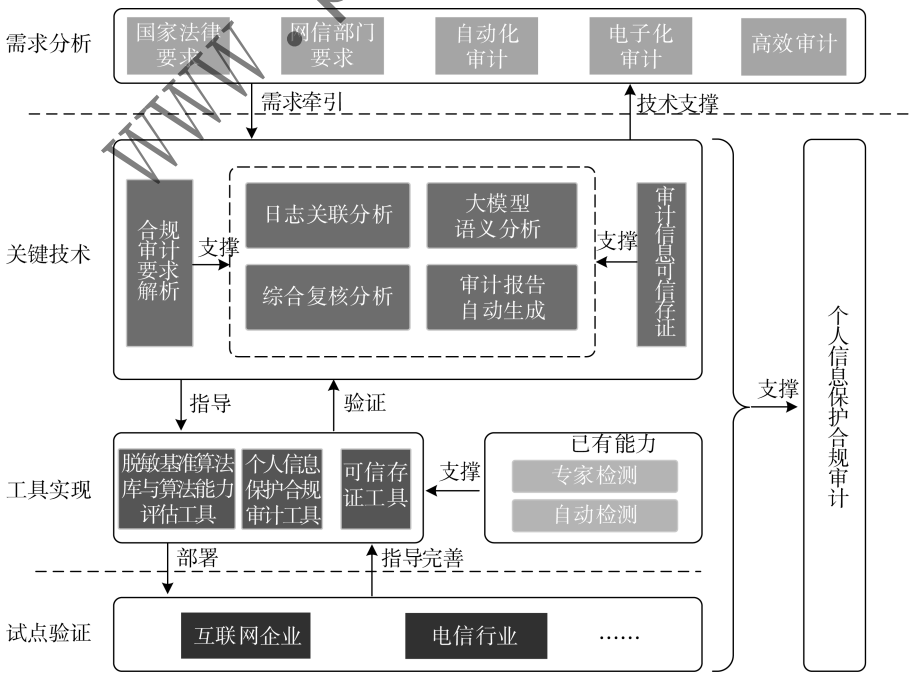

图 3　个人信息保护合规审计工具研究思路

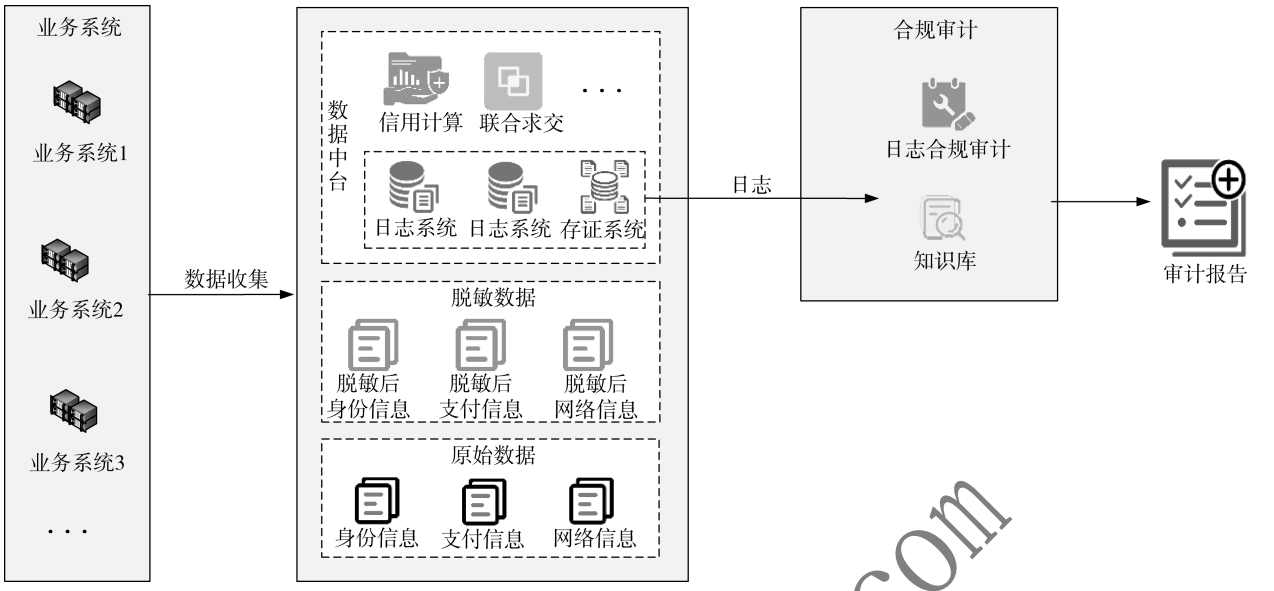

图 4　个人信息保护合规审计工具应用场景示意图

5　结论

个人信息保护合规审计是一项融法律、数据治理、技术于一体的综合性工作，其数字化转型的内在逻辑既有《个人信息保护法》与数据紧密联系的实际基础，也是日志审计、大数据分析、知识库等技术发展、成熟共同作用之结果。要做好个人信息保护合规制度的落实落地，需要统筹兼顾法规的权威性、专业性和标准的可操作性、便利性，还应顺应合格评定数字化转型趋势，让中小企业以低成本享受专业服务，维护公民个人信息权益。按照“政策文件－标准－软件工具”的研制和推广思路，中国科学院信息工程研究所等机构以标准形式提出了个人信息保护合规审计辅助实现技术框架，并通过开发原型系统开展了示范验证。实践表明，个人信息保护合规审计的技术辅助实现技术框架是可行的。下一步，中国科学院信息工程研究所等机构还将结合《办法》的正式出台以及各行业审计工作实际，继续推进标准研究起草和工具研发，为我国个人信息保护法律法规的落地实施做出贡献。

参考文献

[1] 崔聪聪. 个人信息保护的行政监管及展开［J］. 苏州大学学报（哲学社会科学版），2022，43（5）：73－84.

[2] 赵翰隽，殷楠. 个人信息保护合规审计探究［J］. 财会月刊，2024，45（8）：80－85.

[3] 胡耘通. 个人信息保护合规审计制度建设思考［J］. 财会月刊，2023，44（20）：88－91.

[4] 温梦茂. P会计师事务所对T直播企业的审计风险控制研究［D］. 成都：电子科技大学，2022.

[5] 王冲. 个人信息保护合规审计的理论逻辑与制度构建［J］. 网络安全与数据治理，2024，43（1）：65－72，78.

[6] JANS M，ALLES M G，VASARHELYI M A. A field study on the use of process mining of event logs as an analytical procedure in auditing［J］. Accounting Review，2014，89（5）：1751－1773.

[7] 康俊，刁子鹤，宋美娜. 平台企业的用户数据社会责任评价体系构建研究［J/OL］. 北京邮电大学学报（社会科学版），1－16［2024－08－13］. https：//doi. org/10. 19722/j. cnki. 1008－7729. 2024. 0042.

[8] 张淇. 论数字时代我国个人信息算法审计制度的构建：兼评《个人信息保护合规审计管理办法（征求意见稿）》［J］. 实事求是，2024（4）：74－83.

[9] JANS M，WERF J，LYBAERT N，et al. A business process mining application for internal transaction fraud mitigation［J］. Expert Systems with Applications An International Journal，2011，38（5）：13351－13359.

（收稿日期：2024－07－03）

作者简介：

刁毅刚（1977－），男，硕士，高级工程师，主要研究方向：数据安全、个人信息保护、网络安全。

张玲翠（1986－），女，博士，高级工程师，主要研究方向：网络与系统安全、数据安全。

刘晓蒙（1995－），女，硕士，主要研究方向：数据安全、个人信息保护。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部