Journal of Convergence for Information Technology
Vol. 11. No. 12, pp. 1-13, 2021
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2021.11.12.001

제4차 산업시대의 개인정보 관리수준 진단지표체계 개선방안: 특정 IT기술연계 개인정보보호기준 적용을 중심으로

신영진
배재대학교 지능SW공학부 정보보안학 교수

The Improvement Plan for Indicator System of Personal Information Management Level Diagnosis in the Era of the 4th Industrial Revolution: Focusing on Application of Personal Information Protection Standards linked to specific IT technologies

Young-Jin Shin
Professor, Division of Intelligent SW Engineering-Information Security, PaiChai University

요 약 개인정보보호위원회에서 공공기관을 대상으로 시행하고 있는 개인정보 관리수준 진단제도의 지표체계는 「개인정보 보호법」의 법적 준수사항을 점검하지만, 새로운 IT기술의 도입에 따르는 개인정보보호사항을 기준으로 적용하는 데 한계가 있었다. 따라서, 본 연구에서는 제4차 산업혁명의 핵심기술인 빅데이터, 클라우드, 사물인터넷, 인공지능을 특정IT기술의 도입에 따라, 개인정보보호가 강화될 수 있도록 별도의 지표체계가 운영될 수 있도록 지표체계의 개선방안을 제안하고자 한다. 이를 위해서 선정한 특정IT기술의 개인정보보호사항에 관한 국내외 문헌조사를 통해 지표체계의 구성요소를 도출하고, 공공기관의 개인정보보호담당자 대상으로 한 설문조사 및 개인정보보호 전문가대상으로 FGI/Delphi분석을 통해 진단지표로 선정하였다. 이렇게 선정한 지표체계는 먼저, 모든 특정IT기술의 기획 및 설계단계에서부터 개인정보보호원칙(PbD)과 가명정보처리 및 비식별 조치에 관한 기준의 적용여부를 점검하는 공통지표를 선정하였다. 이외에 빅데이터에 관한 2개 점검항목, 클라우드에 관한 개인정보처리방침 게재 사항 등 5개 점검항목, 사물인터넷관련 원칙적용, 로그기록 관리 등 5개 점검항목, 인공지능에 관한 원칙 적용 등 4개 점검항목을 선정하였다. 이처럼 본 연구는 개인정보 관리수준 진단제도의 발전을 위해 새로운 IT기술변화에 대응할 수 있도록 개인정보보호의 신속한 대응을 유도하는 진단제도가 되도록 제언하고자 하였다.

주제어 : 개인정보 관리수준 진단제도, 특정 IT기술, 빅데이터, 클라우드, 사물인터넷, 인공지능, 개인정보보호

Abstract This study tried to suggest ways to improve the indicator system to strengthen the personal information protection. For this purpose, the components of indicator system are derived through domestic and foreign literature, and it was selected as main the diagnostic indicators through FGI/Delphi analysis for personal information protection experts and a survey for personal information protection officers of public institutions. As like this, this study was intended to derive an inspection standard that can be reflected as a separate index system for personal information protection, by classifying the specific IT technologies of the 4th industrial revolution, such as big data, cloud, Internet of Things, and artificial intelligence. As a result, from the planning and design stage of specific technologies, the check items for applying the PbD principle, pseudonymous information processing and de-identification measures were selected as 2 common indicators. And the checklists were consisted 2 items related Big data, 5 items related Cloud service, 5 items related IoT, and 4 items related AI. Accordingly, this study expects to be an institutional device to respond to new technological changes for the continuous development of the personal information management level diagnosis system in the future.

Key words : Personal Information Management Level Diagnosis, Core IT technology, Big data, Cloud, IoT, Artificial intelligence, Personal information protection

*This article is utilized the results of the research support project of the Korea Internet & Security Agency in 2021.
*Corresponding Author : Young-Jin Shin(jinsyj@yahoo.com)
Received September 24, 2021
Revised November 5, 2021
Accepted December 20, 2021
Published December 28, 2021

1. 서론

우리나라는 공공기관의 개인정보보호 및 관리수준을 평가하여 개선하도록 2007년 개인정보 관리수준 진단제도(이하 진단제도)를 개발하여 도입하였다. 지난 2020년 「개인정보 보호법」이 개정되어 개인정보보호 총괄부처로서 개인정보보호위원회가 공공기관의 개인정보 관리감독을 위한 방법으로 진단제도를 활용하고 있다. 그러나, 새로운 정보통신기술의 도입이 확대되고 있음에도 그에 대한 개인정보보호기준 및 점검이 이루어지지 못하고 있다. 특히, 제4차 산업혁명의 핵심기술인 빅데이터(Bigdata), 클라우드(Cloud), 사물인터넷(IoT), 인공지능(AI)), 모바일(Mobile) 등은 개인정보를 활용하여 대국민 서비스를 하고 있기 때문에 그에 적합한 개인정보보호활동이 동반되어야 한다. 특히, 지능데이터기반의 챗봇서비스 등은 더 많은 개인정보를 수집하고 있으므로, 공공데이터의 활용확대에 따른 개인정보의 가명처리 및 비식별 조치가 강화되어야 한다. 일례로, 클라우드기반의 웹브라우징 기록정보, 검색정보, 구매경력정보 등과 같이 정보의 축적뿐만 아니라 개인정보의 결합가능성이 높아져, 개인정보 침해사고에 대한 우려가 커지고 있다. 따라서, 공공기관이 새로운 IT기술을 도입함에 있어서, 적법한 개인정보 처리 및 관리가 이루어지도록 개인정보 관리수준 진단제도를 활용할 수 있다.

이에 따라 본 연구에서는 진단제도의 진단지표체계를 정비하여 4차 산업혁명시대에 적합한 개인정보보호 준수사항을 진단지표에 반영하여 적용할 수 있는 방안을 제시하고자 한다. 이를 위해서 빅데이터, 클라우드, 사물인터넷, 인공지능을 특정 IT기술로 정의하고, 이를 중심으로 한 공공분야 서비스에 관한 개인정보보호 지침, 가이드라인, 매뉴얼 등 국내외 문헌조사를 하여 적용할 수 있는 지표로 적용하고자 한다. 이를 위해서 개인정보보호 실무자 대상 설문조사 및 관계전문가 대상의 FGI/Delphi를 통해 실현가능한 지표체계를 구현하고자 한다.

2. 개인정보 관리수준 진단제도의 개요

2.1 진단제도의 추진과정

진단제도는 공공기관이 「개인정보 보호법」제1항에 따라 “개인정보처리자의 법규 준수현황과 개인정보 관리 실태 등에 관한 자료의 제출이나 의견의 진술”을 하도록 하며, 동법 제2항 “개인정보 보호 정책 추진, 성과평가 등을 위하여 필요한 경우 개인정보관리 수준 및 실태파악 등을 위한 조사”를 하도록 규정된 사항에 근거한다. 이에 본 제도는 공공기관의 개인정보보호 수준을 향상시키기 위해 스스로 보호 및 관리수준을 파악하고, 미흡한 사항을 개선하며 안전한 보호수준을 유지하도록 진단지표를 제공하여 그 결과에 대한 컨설팅을 수행하도록 한다[1]. 즉, 2008년부터 매년 자율진단을 통해 개선하도록 하되, 현장진단팀을 구성하여 실제 적절한 진단이 이루어졌는지 점검하는 체계로 운영되었다. 2021년에는 미흡한 30여개 공공기관을 대상으로 현장컨설팅을 하여 사전 준비하도록 지원하였으며, 서면 및 현장진단으로 그 결과에 대해 검증하여 공개하도록 진행하였다

2.2 진단체계 및 지표 구성

진단제도는 심사 및 평가를 위해 진단체계를 구성하는데, 도입 초기에는 3개 분야 18개 지표 85개 문항으로 구성되었다가, 여러 차례 변경하여 2021년에는 3개 분야 13개 분야 21개 항목으로 서면심사 및 현장심사를 진행한다. 이에 대해 현재 운영 중인 진단체계의 각 분야 및 지표에 대해 Table 1과 같이 정리할 수 있다[2].

Table 1. Indicator system for Personal Information Management Level Diagnosis

Field	diagnostic index
Establishment and operation of management system	1. Personal information file management
	2. Laying the foundation for personal information protection
	3. Privacy impact assessment(PIA)
	4. Promotion of personal information protection education
	5. Performing the role of the person in charge of personal information protection
Establishment and implement-ation of protection measures	6. Privacy Policy and Protection of Rights of Information Subjects
	7. Compliance with procedures for collection, use, and provision of personal information and for use and provision of personal information for purposes other than the intended purpose
	8. Protection of personal information according to entrustment of personal information processing
	9. Operation and management of image information processing equipment
Establishment and implementation of counter-measures against infringement	10. Measures to prevent infringement of personal information
	11. Establishment of procedures for personal information leakage and disaster/disaster response
	12. Management of access rights of personal information processing system and check access records
	13. Identification of processing status of unique identification information and implement encryption

이처럼 3개 분야(12개 지표)는 관리체계 구축 및 운영(5 개 지표), 보호대책 수립 및 이행(4 개 지표), 침해대책 수립 및 이행(4 개 지표)으로 크게 구분된다. 세부적인 13개 세부지표는 첫째, 관리체계 구축 및 운영분야에서는 개인정보 파일관리, 개인정보 보호기반 마련(예산 및 인력), 개인정보 영향평가 수행, 개인정보 보호교육 추진, 개인정보 보호책임자의 역할 수행을 평가한다. 둘째, 보호대책 수립 및 이행분야에서는 개인정보 처리방침 및 정보주체의 권리보장, 개인정보 수집·이용·제공 및 목적 외 이용·제공 절차준수, 개인정보 처리업무위탁에 따른 개인정보보호, 영상정보처리기기 운영 및 관리에 관해 평가한다. 셋째, 개인정보 침해사고 방지 조치, 개인정보 유출사고 및 재해·재난 대응 절차 수립, 개인정보처리 시스템의 접근 권한 관리 및 접속기록 점검, 고유식별정보의 처리현황 파악 및 암호화 이행에 관해 평가하여 종합적으로 100점으로 환산하여 점수화한다.

2.3 특정 IT기술관련 진단지표 개발 필요성

진단제도의 성과를 보면, 개인정보보호를 위한 공공기관은 잘하거나 그렇지 못한 경우 개인정보보호 수준 향상을 위해서 그동안의 성과를 점검하여 개선할 수 있는 기준과 방향을 점검하여야 한다. Table2와 같이 진단제도에 관한 SWOT분석을 하였는데, 진단제도는 공공기관의 개인정보 관리기준 및 평가체계로 활용되고 있고, 공공기관을 위한 필수불가결한 정책요소로 구성하여 적용할 수 있다[1]. 더욱이, 앞으로 IT기술분류체계상 소프트웨어 중 서비스분야에 적용할 수 있는 새로운 기술을 대민서비스에 적용하면서, 개인정보 침해사고로부터 보호하기 위한 제도로서의 주도적 역할을 할 필요가 있다. 따라서, 4차 산업혁명을 이끄는 핵심기술인 ICBMA을 중심으로 개인정보의 수집·이용·제공·파기 과정에서 준수해야 할 사항을 검토하여 진단지표로 활용할 수 있도록 제안하고자 한다. 다만, 모바일의 경우 이미 개인정보 관리수준 진단지표의 10. 개인정보 침해사고 방지 조치에서 모바일기기에 관한 보호조치를 담고 있기에, 본 연구에서는 빅데이터, 클라우드, 사물인터넷, 인공지능을 중심으로 검토하고자 한다.

2.4 사전 연구

개인정보 관리수준 진단제도에 관한 연구들을 살펴보면, 정형철(2010)은 비모수방법을 적용한 지표의 가중치 결정에 대한 지표간의 중요도를 해석하였으며[3], 이승훈 외(2011)는 가중치의 변화에 대한 시뮬레이션을 통해 기관의 특성과 수준에 맞는 지표를 개발하고자 하였다[4]. 이에 대해 신영진 외(2012)도 진단제도에 적용하고 있는 지표를 정책적 측면, 기술적 측면, 침해대응적 측면으로 구분하여 정책중요도에 대한 우선과제를 제안하였다[5]. 이외에도 정명수 외(2015)는 지속적인 진단제도의 재해석 및 실효성 있는 진단모델을 DEA모형을 이용하여 제안하였다[6].

Table 2. SWOT Analysis Results of Personal Information Management Level Diagnosis

Div.	Strength	Weakness
inside	• Improving to check the criteria necessary for personal information management with guidelines and diagnostic indicators • Operating a representative inspection system for personal information protection • Using improvement standards for personal information protection (plan establishment, etc.)	• Occurring the differences in each institutional environment with unify diagnosis process of management • Rejecting from the priority list due to overlap in personnel input and evaluation period due to the implementation of similar evaluation systems • Pouring the response to low cores and rate of public agencies
Out side	• Suggesting compliance with national-wide personal information protection laws • Utilizing standards to improve the level of personal information management in public institutions	• Being less importance compared to other evaluation system • Being Insufficient response due to response such as manpower and budget
Div.	Opportunity	Threats
In side	• Transferring the Affairs from Ministry of Public Administration and Security to Personal Information Protection Committee • Utilizing various level evaluation system for personal information protection	• Developing similar system other than persona information management level diagnosis • Increasing demands for alternative evaluation of personal information management level diagnosis
Out side	• Raising awareness of the importance of personal information protection following the introduction of new IT • Expanding the understanding of users and processors regarding personal information protection • Demanding for regulation and countermeasures for strong personal information protection	• Increasing threats of personal information infringement due to abuse of new IT • Being insufficient of standardized system management and response system • Being rampant insecurity for personal information infringement incidents

그러나, 개인정보 관리수준 진단제도의 지속적인 연구가 이루어지지 못하여, 새로운 IT환경에 적극적인 대응기준을 반영하지 못하였다. 물론, 장철호외(2021)는 신기술 기반의 서비스 확대에 따라 개인정보처리자의 개인정보보호활동을 가져오는 결정요인을 분석함에 있어서, 개인정보보호활동에 대한 적정성의 수준을 평가하였다[7].

그렇다면, 본 연구에서의 특정 IT기술을 중심으로 개인정보보호를 위한 지표를 개발할 필요가 있는데, 먼저, 빅데이터에 관하여 박천웅 외(2016)는 빅데이터에서의 개인정보보호의 위험 및 억제정책에 대한 영향도를 분석하였으며, 가설검증, 요인분석 및 신뢰분석을 통해 개인정보보호의 대응을 강화하고자 하였다[8]. 이연우외(2012. 11)는 빅데이터환경에서는 다양한 경로를 통해 민감한 개인정보를 수집함에 따라 개인정보의 무분별한 요청 및 취급방지를 위해 안전한 개인정보 관리 모델을 제시하였다[9]. 둘째, 클라우드와 관련하여 살펴보면, 나상호외(2012. 11)는 퍼스널 클라우드가 개인데이터기반으로 하므로, 클라우드 컴퓨팅 보안 및 개인정보보호 연구를 기반으로 퍼스널 클라우드환경에서 개인정보보호를 위한 생명주기 모델을 통해 개인정보보호 참조모델과 보안 가이드라인을 제시하였다[10]. 신영진(2015. 3)은 클라우드 서비스가 제공되면서 개인정보가 집적됨을 고려하여 안전한 서비스를 제공하고자 제도적 측면, 기술적 측면, 관리적 측면에서 개인정보보호의 종합적인 선제적 대응을 하고자 하였다[11]. 또한, 김정덕 외(2015)는 클라우드 컴퓨팅을 통해 개인정보를 처리하는 경우, 계약서 또는 서비스 수준 협약(Service Level Agreement: SLA)에 개인정보보호를 위한 7개 지표와 13개 척도를 개발하였다[12]. 셋째, 사물인터넷과 관련하여 신영진(2018. 9)은 다양한 사물인터넷서비스를 구현함에 있어서 안전한 환경을 구축하고, 그 가운데 유통되는 개인정보를 보호하기 위한 정책지표를 전문가대상의 델파이분석을 통해 3개 분야 9개 영역 25개 지표로 구성하였으며, 우선과제를 도출하였다[13]. 또한, 신영진(2020)은 IoT서비스주체를 위한 개인정보보호 프레임워크를 마련하여 적합성 평가기준을 적용해야 한다고 보았다[14]. 인공지능에 관한 연구를 살펴보면, 이원태 외(2016)는 인공지능서비스로 인한 개인정보보호 침해이슈에 대한 인공지능 산업을 발전시킬 수 있는 도덕적/법제도적 모델에 대해 고찰하였다[15]. 그러나, 개별적인 신기술에 대해 개인정보보호를 적용하기 위한 연구는 진행되고 있으나, 특정 IT기술을 종합적인 관점에서 개인정보보호를 위한 준수사항 및 측정지표로 제시하지 못하고 있다. 따라서, 본 연구에서는 4차 산업혁명의 핵심기술 중 빅데이터, 클라우드, 사물인터넷, 인공지능을 특정 IT기술로 선정하여 종합적인 준수사항으로 지표를 선정하여 점검하도록 하고자 한다.

3. 연구의 분석 틀과 방법

본 연구는 4차 산업의 주요 핵심기술인 빅데이터, 클라우드, 사물인터넷, 인공지능을 활용하고 있는 서비스에서의 개인정보처리과정에서 개인정보보호수준을 높이고자 한다. 이에 본 연구에서는 Fig. 1과 같이 연구의 분석 틀을 구성하였다.

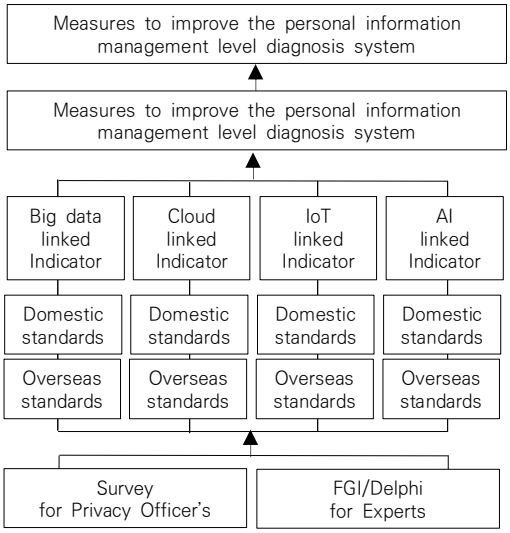

Fig. 1. Framework of the study

본 연구는 기존 국·내외 문헌조사를 통해 지표를 도출하고, 그 검증과정에서 개인정보보호 실무담당자대상 15명을 대상으로 한 설문조사(2021. 7. 2-7.12), 관계분야 전문가 6명을 대상으로 심층면접조사(FGI) 및 델파이조사(Delphi)를 통한 분석(2021. 7. 29, 8. 20, 8. 25)을 하였다. 이렇게 연구를 진행하여 개인정보 관리수준 진단지표에 특정 IT기술을 적용하는 진단지표를 적용하고자 한다.

4. 특정 IT기술의 개인정보보호기준 검토

본 연구를 위해서 현재 공공기관에서 도입된 빅데이터, 클라우드, 사물인터넷, 인공지능에 관한 대민서비스가 확대되고 있기에, 이로 인해 처리되는 개인정보가 증가함에 따라 개인정보보호에 관한 운영이 이루어지고 있는 지 점검할 기준이 마련되어야 한다. 이를 위해 개인정보보호에 관한 국내·외 법률, 지침, 가이드라인 등을 검토하여, Table 3과 같이 각 분야에 적용할 기준들을 정리하여 세부적인 점검항목을 선정하고자 하였다.

4.1 빅데이터관련 개인정보보호 준수사항

4.1.1 국내기준

공개된 정보(SNS, 인터넷게시판 등에 게재된 정보), 이용내역정보(서비스이용기록, 인터넷접속정보파일, 접속기기 정보 등), 생성정보(개인 및 특정집단의 성향, 행태정보) 등 다양한 개인정보가 빅데이터로 수집됨에 따라 개인정보 일부, 또는 전부 등을 삭제 및 대체하여 다른 정보와 쉽게 결합하여도 특정 개인을 알 수 없도록 일련의 비식별 조치를 하여야 한다[16].

이에 따라 Table 3과 같이 행정안전부, 방송통신위원회, 과학기술정보통신부, 정부합동으로 가이드라인을 제공하고 있다. 또한, 2020년 데이터 3법[1] 개정 등으로 개인정보보호위원회의 '가명정보 처리 가이드라인(2020),' 행정안전부·개인정보보호위원회의 '공공분야 가명정보 제공 실무안내서(2021.1)' 등을 발간하여, 기관보유 데이터의 가명정보처리절차를 구체화하여, 처리단계별 세부기준 및 관련 서식 등을 제공하고 있다[17]. 이외에도 진단제도의 진단지표 중 5. 개인정보 보호책임자의 역할 수행의 진단항목인 기관 주도 실적인정기준(5.2지표)의 범주에 가명정보 처리를 추가[2]하여 일부 점검하고 있다[2].

Table 3. Personal information protection standards for specific IT technologies

Division		Title of Guidelines
Big Data	Domestic	Personal Information Protection Guidelines for Opening and Sharing of Public Information by MoPAS(2013) / Guide to self-assessment of adequacy for de-identification of personal information by Ministry of Public Administration and Security(2014) / Big Data Privacy Guidelines by Korea Communications Commission(2014) / Guide to the use of technology for de-identification of personal information by MSC(2015) / Guidelines for de-identification of personal information by Government-joint (2016) / Guidelines for the handling of pseudonymous information by PIPC(2020) / Practical Guide to Provision of Pseudonym Information in the Public Sector by MoPAS & PiPC(2021) / Diagnosis of the management level of personal information of public institutions by MoPAS(2021) / Evaluation of the operation status of public ·data provision by MoPAS(2020)
	Overseas	(Privacy framework)De-identified technical standard of ISO/IEC 29100(2015) / Guideline on De-identification Methods of Medical Information by U.S.(2012) / Guideline on De-identification of Personally Identifiable Information by NIST(2015) / Guideline on De-identification of Public Data by NIST(2016) / Guide to Personal Information Protection in Big Data Environment by ENISA(2015. Dec) / Code of Practice for Risk Management for Data Protection by ICO(2012. 11. 20) / Privacy Principles of Processing Big Data, AI, etc by ICO(2017) / Anonymisation Framework by UKAN(2016)
Cloud	Domestic	Cloud SLA(Service Level Agreement) Guide by KCC(2011) / Cloud Development Act(2015) / Security Guideline for Cloud Service Users(2012) / Guidelines for the use of private cloud by administration and public institutions(2019) / Cloud Security Certification System by MSC / Cloud Service Terms and Conditions / Cloud Service Information Protection Guide / ISMS-P by MSC & PIPC
	Overseas	Cloud Security Control Framework OCF / Cloud Privacy SLA Guidelines / STAR certification examination / International standards ISO/IEC 27017 / ISO/IEC 27018 / ISO/IEC 27002
IoT	Domestic	IoT Common Security Principles by KISA / 7 principles of common IoT security by IoT Security Alliance / Guide to using password authentication technology in IoT environment / Protection measures for each of the 10 rules for personal information protection
	Overseas	10 Security Principles About IoT Vulnerabilities by OWASP(2014) / Privacy by Design by IPC(2011) / Report on Cyber security and Privacy Risks for IoT Devices by NIST in US(2019)
AI	Domestic	Intelligent Information Society Ethics Guidelines by MSC(2018) / Principles for a User-Centered Intelligent Information Society by KCC(2019. 11) / Human-centered Artificial Intelligence Ethics Standards (2020) by Government joints / Artificial Intelligence (AI) Personal Information Protection Voluntary Checklist by PIPC(2021)
	Overseas	Artificial Intelligence: Australia's Ethics Framework, A Discussion Paper(2019) / Privacy by Design/Default of GDPR by EU(2016) / European Artificial Intelligence Strategy (2018) of EU / Adjustment Plan for Artificial Intelligence(2018) / Reliable Artificial Intelligence Guidelines(2019) / Artificial Intelligence White Paper(2020) / EU Commission's 'Data and Data Governance

1) 데이터 3법 :「개인정보 보호법」,「정보통신망 이용촉진 및 정보보호 등에 관한 법률」,「신용정보의 이용 및 보호에 관한 법률」

2) 가명정보처리를 위한 별도 내부관리계획 수립, 가명정보 활용에 관한 교육계획 수행, 위·수탁시 문서화·교육·관리감독, 보호조치 등을 수행함.

또한, 행정안전부의 '공공데이터 제공 운영실태평가(2020)'지표에 개인정보의 비식별 처리 등을 통한 미개방 데이터 개방 노력에 관한 평가지표로 데이터의 비식별, 익명화 등 제도적 조치에 관한 정성평가를 반영하고 있다.

4.1.2 해외기준

해외에서 빅데이터와 관련하여 개인정보보호에 관한 준수사항을 마련하고 있는 경우를 살펴보면, 비식별 처리에 대한 기준 및 개념을 포함한 가이드라인 및 표준을 제시하고 있다. 특히, ISO/IEC 29100, 미국, EU, 영국 등 은 빅데이터환경에 적합한 개인정보보호를 위한 가이드라인을 제공하면서 데이터 처리과정에서 비식별화에 대한 방법을 강조하고 있다. 먼저, ISO/IEC 29100(privacy framework)에서 비식별화에 관한 용어, 기술분류, 재식별[3] 위협 최소화방안 등을 제시하였고, UK Anonymisation Network(UKAN)의 '익명화 프레임워크(2016)'에서 정형 비식별화, 보장형 비식별화, 통계적 비식별화, 기능적 비식별화 등 비식별방법 10가지 요소를 제시하였다[18]. 또한, 정보감독위원회(ICO)는 '빅데이터, 인공지능 등 처리에서의 개인정보보호원칙(2017)'을 마련하여 빅데이터분석에서 개인정보보호조치를 수행하도록 하였으며, 내부 및 외부 감사를 통해 알고리즘 결정을 내린 근거를 설명하고 편견, 차별 및 오류를 검토하도록 하였다[19].

4.2 클라우드관련 개인정보보호 준수사항

4.2.1 국내기준

우리나라에서 제공되는 클라우드 서비스에 관한 개인정보보호기준들을 살펴보면, 방송통신위원회는 클라우드 컴퓨팅 확산을 위해 '클라우드 SLA(Service Level Agreement) 가이드(2011)'를 제시하였으며[20], '클라우드환경에서 고려해야 할 SLA지표'[4]를 구성하였다[12]. 또한, 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」(2015), '민간부문의 클라우드 도입 실무 가이드라인(2012)', '행정·공공기관 민간 클라우드 이용 가이드라인(2019)' 등을 제공하였으며, 그 밖의 기존 기업(구글, 더존, 롯데정보 등)의 클라우드 서비스 제공에 관한 표준약관 등을 검토하여 개인정보보호 준수사항을 도출하였다[11]. 현재 클라우드 서비스에서의 점검항목으로 적용한 경우, 과학기술정보통신부에서 운영하는 클라우드보안인증제도에서 점검항목 중 12. 데이터 보호 및 암호화의 12.1 데이터 보호[5]에 개인정보보호 점검사항을 반영하고 있다. 또한, 과학기술정보통신부·개인정보보호위원회의 정보보호 및 개인정보보호 관리체계 인증(ISMS-P)의 점검항목 중 2. 보호대책 요구사항 중에서 2.10. 시스템 및 서비스 보안관리, 2.10.2 클라우드보안을 점검하고 있는데, 클라우드 서비스 이용 시 서비스유형(SaaS, PaaS, IaaS 등)에 따라 비인가 접근, 설정 오류 등에 따라 중요정보와 개인정보가 유·노출되지 않도록 관리자 접근 및 보안 설정 등에 대한 보호대책을 수립·이행하도록 하였다[21]. 이외에도 교육부의 정보보호수준진단에서도 5.7 클라우드보안에 관하여 클라우드 서비스 이용 시 중요정보가 유·노출되지 않도록 보호대책을 수립·이행여부를 점검하고 있다.[6]

4.2.2 해외기준

해외의 클라우드에 관한 개인정보보호 대해서 살펴보면, 비영리단체인 클라우드보안협회(Cloud Security Alliance: CSA)에서 제공하고 있는 '클라우드보안 제어프레임워크(Open Certification Framework: CSA OCF)'를 활용하고 있다. 또한, 2013년 '클라우드 개인정보보호 SLA지침'을 발표하였는데, 개인정보 유형, 처리방식, 전송, 보호대책, 모니터링, 개인정보 보유 및 폐기, 책임추적성, 분쟁해결, 손해배상 등을 규정하고 있다[12].

또한, 2019년 현재 152개 글로벌 클라우드 서비스 제공업체가 CSA STAR프로그램에 참여하고 있다. STAR 인증을 받기 위해서는 클라우드 서비스 제공업체가 기존에 ISO 27001인증을 획득했거나, STAR인증 심사를 ISO 27001인증과 동시에 받을 수 있다[22]. 국제표준 ISO/IEC 27017, ISO/IEC 27018은 클라우드 환경에서의 개인정보보호대책에 대한 국제표준으로

3) 재식별 판별 4가지 기준: 개별화, 연결가능성, 추론가능성, 구별 불가능성

4) 클라우드 SLA에서의 개인정보보호점검사항은 네트워크 보안, 접근통제, 암호화, 로그관리시스템 접근, 물리적 보안, 모니터링, 악성프로그램 방지로 지표를 구성함.

5) 12.1.1. 데이터 분류, 12.1.2. 데이터 소유권, 12.1.3. 데이터 무결성, 12.1.4 데이터 보호, 12.1.5데이터 추적성, 12.1.6 데이터 폐기

6) 5.7.1 클라우드 서비스 이용 시 중요정보가 유·노출되지 않도록 보호대책 수립·이행 점검사항: (필수)클라우드 보안인증(IaaS, SaaS 등) 여부, 보안성 검토 실시, 클라우드 서비스에 대한 역할 및 책임 정의, 클라우드 서비스 운영 모니터링 및 적절성 검토 여부

ISO/IEC 27002를 기반으로 14개의 통제 영역을 제시하며[23], 추가적으로 클라우드환경을 고려한 개인정보보호 통제항목을 제시하고 있다[12]. 특히, 클라우드 서비스 보안인증을 위한 데이터 보호를 위해 데이터 분류, 데이터 소유권 , 데이터 무결성, 데이터 보호, 데이터 추적성, 데이터 폐기에 관한 점검을 수행하고 있다[24].

4.3 사물인터넷관련 개인정보보호 준수사항

4.3.1 국내기준

사물인터넷서비스에서의 개인정보보호 및 보안을 위한 기준으로 한국인터넷진흥원의 'IoT 공통보안원칙', IoT보안얼라이언스(IoT보안협의체)의 'IoT 공통보안 7대 원칙 등'[7] 및 IoT환경에서의 '암호인증기술 이용안내서' 등을 제공하고 있다[25]. 한국인터넷진흥원은 IoT 기기 등으로 개인정보를 자동처리할 경우, 개인정보처리단계별로 사업자가 고려해야 할 사항을 실제 사례중심으로 가이드라인을 제공하고 있다. 'IoT보안가이드'는 IoT보안얼라이언스와 산·학·연전문가가 참여해 민간 주도로 개발했다. IoT기기 생명주기를 기준으로 15가지 보안요구사항과 기술·관리적 권고사항을 개인정보보호와 관련 사항으로 정리할 수 있다[26].

이외에도 정부가 사물인터넷 등에 의해 자동처리되는 개인정보처리에 대한 침해사고 대비 사전예방 및 개인정보처리자가 처리단계별 보호조치를 해야할 사항을 10가지 선정하였다. 이는 기획단계에서 개인정보의 필요성 및 법적 준수사항을 확인하도록 하며, 설계단계에서는 최소한의 개인정보를 수집하여 안전하게 처리하도록 하고, 그에 따라 정보주체의 권리보장을 하도록 한다. 끝으로 서비스 제공 전에 개인정보 침해 위험요소에 대해 점검하여 설계에 반영여부, 서비스 개선 및 다른 서비스와의 연계·연동 등 변경 시에 추가적 개인정보 침해위험이 있는지 점검하도록 한다[27].

4.3.2. 해외기준

국내외 주요 기관에서는 IoT 제품 및 서비스에 관한 보안원칙을 수립하여 운영상 반드시 준수하도록 권고하고 있다. OWASP(2014)의 'IoT 취약점에 관한 10가지 보안원칙', IPC(2011)의 '설계에 의한 개인정보보호(Privacy by Design)' 등과 같이 준수사항을 추상적으로 제시하고 있다[28]. 또한, IoT 디바이스(데이터 전송, 데이터 수집, 센싱 및 액츄에이팅, 일반 등 관련 기기)를 4단계 등급(0~3)으로 구분하여 보안요구사항 및 기술적 공통 적용사항을 제시하고 있다[29]. 그 외 IoT에 관한 제품 및 서비스의 설계·개발부터 운영·폐기 상의 보안기준을 적용하고 있다[30]. IPA, GSMA, OWASP, CSA 등 IoT기기 또는 IoT서비스에 관한 정책, 설계 및 개발, 운영 및 보수, 폐기 등의 처리과정상 보안원칙을 규정하고 있다.

미국의 NIST는 2019년 'IoT 장치를 위한 사이버보안 및 개인정보위험에 관한 보고서(NISTIR 8259)'를 발간하였다. 이처럼, IoT장치 보안계획으로 장치 보안보호(장치 사용 방지), 데이터 보안 보호(수집 된 데이터의 CIA 유지), 개인의 프라이버시 보호(개인식별정보 보호)가 반영되어야 한다. 물론, IoT장치의 위험완화를 위해 자산관리(최신 목록 유지), 취약성 관리(알려진 소프트웨어와 펌웨어의 취약점을 장치 사용), 액세스 관리(IoT 장치에 대한 엄격한 액세스 유지, 권한있는 직원만의 접근 허용), 사고 감지(미스 사용 및 데이터 보안 징후에 대한 IoT장치 활동) 등을 보완하고 있다[31].

4.4 인공지능관련 개인정보보호 준수사항

4.4.1 국내기준

우리나라는 인공지능을 도입함에 있어서 개인정보보호에 관한 기준을 마련하고자 하였는데, 윤리적 차원에서 과학기술정보통신부는 '지능정보사회 윤리 가이드라인(2018)'을 마련하였고, 방송통신위원회의 '이용자 중심 지능정보사회를 위한 원칙(2019. 11)'[8]을 수립하였다. 또한, 관계부처 합동으로 '사람이 중심이 되는 인공지능 윤리기준(2020)'을 수립하여 프라이버시 보호, 침해금지, 데이터관리, 책임성, 안전성, 투명성 등을 강조하였다.

최근에는 개인정보보호위원회가 AI 등의 올바른 활용을 위한 개인정보보호준칙인 '인공지능(AI) 개인정보보호 자율점검표(2021)'를 마련하여, 스타트업, 중소기업 등의 안전한 데이터 활용성과를 창출하는데 지원하였다[32]. 그동안 '이루다'관련 비정형 데이터 활용에

7) IoT공통보안 7대 원칙: ① 정보보호와 프라이버시 강화를 고려한 IoT제품 서비스 설계, ② 안전한 소프트웨어 및 하드웨어 개발 적용 및 검증, ③ 안전한 초기 보안설정방안 제공, ④ 보안 프로토콜 준수 및 안전한 파라미터 설정, ⑤ IoT제품·서비스의 취약점 보안 패치 및 업데이트 지속 이행, ⑥ 안전한 운영· 관리를 위한 정보보호 및 프라이버시 관리체계 마련, ⑦ IoT침해사고 대응체계 및 책임추적성 확보 방안 마련

8) AI 윤리원칙 중에서 책임성원칙, 안전성원칙, 프라이버시와 데이터거버넌스원칙이 개인정보보호에 적용가능함.

관한 규제에 관해 특정 법률에 규정이 없었기에[33], 개인정보보호 관련 법률, 시행령, 고시 등에서 제시하는 법적 의무사항, 권장사항 등을 개인정보 처리유형 및 방식에 따라 이행할 수 있는 점검기준으로 활용하여 자율적으로 점검·개선할 수 있다. 본 자율점검표는 업무처리 전 과정에서 지켜져야 할 AI 개인정보보호 6대 원칙(적법성·안전성·투명성·참여성·책임성·공정성)[9], AI 개인정보보호 자율점검사항(16개 점검항목과 54개 확인사항)을 AI 개발·운영자가 (정보통신서비스제공자 포함) 직접적으로 안전하게 처리하여 침해예방을 하도록 준수사항의 사전점검 또는 서비스 운영과정의 수시점검을 위해 활용하도록 점검표를 제공하고 있다[34].

4.4.2 해외기준

호주는 'Artificial Intelligence: Australia's Ethics Framework, A Discussion Paper(2019)'를 통해 프라이버시보호, 투명성, 책임성 등 8가지 원칙하에 위기관리체계를 제시하였다[35]. EU는 「일반개인정보보호법(GDPR)」의 개인정보보호 설계 및 설정(Privacy by Design/Default)을 적용하고 있다. 특히, 시스템 목적, 윤리적 사용, 프로세스 등에서의 개인정보보호·결과, 공정·결과, 물질적 피해·결과, 경쟁가능성·결과, 책임성·결과, 규제·법률 준수사항 및 가능성, 투명성·설명가능성·유사성, 영향을 미치는 사람수 등에 따른 피해규모 등 위험발생빈도 및 주요 위협비중을 측정하여, 위험평가를 실시한 결과 및 위험확률을 점검사항으로 구성하여 위험발생요인별 개선조치를 제시하여야 한다[36]. 인공지능에 관한 국가경쟁력 및 EU시민을 보호하기 위해 EU는 '유럽의 인공지능 전략(2018)', '인공지능에 대한 조정계획(2018)' 등을 마련하였고, '신뢰할 수 있는 인공지능 가이드라인(2019)', '인공지능 백서(2020)' 등을 발행하여, 인공지능시스템의 안전성, 투명성, 객관성 등을 확보하고, 인공지능에 의한 위험을 분류하여 적용하도록 하였다[37][38]. EU집행위원회의 '데이터 및 개인정보 거버넌스(Data and Data Governance)'는[10] 규제기관들이 혁신적 AI시스템의 정식 시장출시 전에 AI시스템을 개발, 시험, 검증을 통제된 환경에서 운영할 수 있도록 개인정보 처리에 대한 조치사항을 규정하였다[39].

이외에도 독립적인 감독기구는 GDPR 등 개인정보보호관련 EU법률이나, 회원국들의 법률 등 개인정보보호관련 규칙을 적용하여, AI에 관한 규제방안을 마련하여 법적 준수사항, 기본권 및 안전 등에 관한 기준을 마련하여 신뢰할 수 있는 서비스 환경을 구현하고자 하였다[40]. 즉, AI규제 샌드박스의 시스템 개발을 위한 개인정보처리에 관한 조치사항에 대해서도 개인정보 참여자의 통제 하에 접근권한자만 데이터 접근이 가능하도록 하며, 보유목적 종료시 폐기하도록 하는 등 안전한 관리를 보장하도록 하였다[41].

5. 특정 IT기술연계 진단지표 적용방안

5.1 특정 IT기술연계 적용검토

앞서 검토한 기존 문헌들을 바탕으로 개인정보보호 담당자 대상의 설문조사(2021. 7. 2~7. 12)를 하였는데, 기존 지표체계에서 신기술의 적용에 따른 별도 지표체계의 필요성을 공감하고 있었다. 특히, 현재 적용하고 있는 공공기관의 대표서비스를 중심으로 한 빅데이터, 클라우드, 사물인터넷, 인공지능을 연계한 서비스가 확대되고 있는 시점에서 개인정보보호에 관한 필요성은 더 강조되고 있다. 이에 대해 검토한 문헌에서 제시한 개인정보보호요소를 선정하여, 개인정보보호분야 학자, 실무자 등으로 구성된 전문가 자문회의(2021. 7. 29, 8. 20, 8. 25)를 거쳐 해당지표를 재배치하였다. 전체적으로 처리되는 개인정보의 비식별 및 가명정보의 경우 빅데이터 외 다른 기술에서도 적용되어야 하는 사항이므로, 별도 공통지표로 선정하였으며, 그 외 각 기술에서 적용된 지표 중에서 공통으로 적용할 수 있는 사항을 선정하여 공통지표로 재배치하였다. 그 외 각 개별기술에 대해서는 해당되는 기술에만 적용가능한 개인정보보호 준수사항을 제시하였다.

5.1.1 빅데이터관련 진단지표연계 사항

우리나라는 빅데이터와 관련하여 행정안전부의 '공공데이터 개방 및 공유에 따른 개인정보보호지침

9) 「개인정보 보호법」제3조(보호 원칙)을 기본으로, 자율적 보호활동을 위한 「개인정보보호 중심 설계」(Privacy by Design) 원칙, 윤리적 이슈 대응을 위한 「AI 윤리기준」을 반영하여, AI 관련 개인정보보호 6대 원칙을 도출하였음.

10) 규제사항: ① 데이터를 이용하여 모델훈련기술을 적용하는 고위험 AI시스템은 품질기준을 충족하는 훈련·검증·시험 데이터 세트(Data Sets)를 기반으로 개발하고, ② 훈련·검증·시험 데이터 세트와 관련된 사항에 대해 적절한 수준의 데이터거버넌스 및 관리관행(Practice)을 준수하며, ③ 훈련·검증·시험 데이터세트는 관련성, 대표성, 무오류성, 완전성을 갖추어야 함.

(2013)', 방송통신위원회의 '빅데이터 개인정보보호 가이드라인(2014)', 미래창조과학부의 '개인정보 비식별화 기술활용안내서(2015)'등 가이드라인을 마련하였고, 공공데이터법 및 데이터 3법 개정을 통해 공공데이터의 이용활성화를 추진하면서 개인정보 침해사고 방지를 위한 비식별 조치를 수행하도록 하였다. ISO/IEC 29100, 미국, EU, 영국 등 빅데이터 환경에 적합한 개인정보보호를 위한 가이드라인을 제공하면서 데이터 처리과정에서 비식별화에 대한 방법을 강조하고 있다.

따라서, 공공기관이 빅데이터처리과정에서 준수해야 할 사항에 비식별 조치, 즉, 가명정보처리의 사항을 점검하여 개인정보가 관리되도록 하여야 한다. 물론, '빅데이터 개인정보보호 가이드라인'에서 제시하고 있는 공개된 개인정보, 이용내역정보에 대해서도 비식별 조치 후 수집·저장·조합·분석하도록 하며, 이용내역정보를 처리할 때 거부할 수 있는 방법 및 절차를 마련하여야 한다. 또한, 비식별 조치 후 새롭게 생성된 정보가 개인정보를 포함할 경우, 즉시파기 및 비식별 조치를 하도록 점검할 수 있다.

5.1.2 클라우드관련 진단지표연계 사항

클라우드서비스와 관련하여 개인정보보호에 관하여는 이미 국내외적으로 여러 가이드라인을 제공하고 있으며, 실제 인증제도에서도 도입하고 있다. 다만, 현재 개인정보 관리수준 진단의 점검항목에서 다루고 있지 않은 사항에 대해 추가적으로 점검할 사항을 검토해 보면, 클라우드 서비스에 대한 이용사실 공개, 국내외 저장 공개, 제3자 제공 금지, 정보의 임치, 반환, 복구 불가능한 파기 사실 통지, 계약 해제·해지·종료시 이용자 정보가 다른 서비스제공자로 이관되는 경우 보호조치 등에 대해 검토할 수 있다. 물론, 클라우드 인증제, ISMS-P 등에서 클라우드 서비스 이용시 데이터 보호 및 보안관리에 대해 점검하고 있으나, 클라우드 서비스 처리에 따른 데이터의 소유권 명시, 데이터 보호기능 방안 관리, 데이터 추적 등에 대한 점검을 추가할 수 있다. 공공기관의 경우 국가정보관리원, 지역정보개발원 등 공공기관을 통해 공동관리하였으나, 코로나 19사태 이후 서비스가용성 등을 위해 민간 클라우드의 활용이 확대되고 있다. 따라서, 국민의 정보관리에 대한 민간 클라우드 서비스 적용까지 고려할 필요가 있다.

5.1.3 사물인터넷관련 진단지표연계 사항

국내외 사물인터넷관련 개인정보보호에 관하여 IoT 장치 및 서비스를 제공하는 과정에서 수집되는 데이터의 적합성, 안전성, 책임성 등을 고려하여 준수해야 할 원칙을 제시하고 있다. 특히, IoT 장치 및 서비스를 통해 수집된 민감정보의 비식별 조치, 암호화, 접근권리 등 안전조치뿐만 아니라, 민감정보의 이용목적 및 보유기간 등에 따른 운영정책의 가시화 및 투명성 보장, 보안위협 대응 침입탐지 및 모니터링, 책임추적성 등을 위한 로그기록 관리를 하도록 한다. 특히, 서비스 설계 단계에서 서비스해지에 따른 개인정보 파기 및 추가 수집 방지에 대한 점검이 필요하며, 서비스 출시 전 개인정보 침해요소에 대한 점검을 하도록 한다. 해외기준에서도 서비스기획단계부터 개인정보보호를 반영하고, 가시성과 투명성 확보를 강조하고 있다. 물론, 책임 추적성을 위해 모니터링, 접근권한관리, 로그기록관리 등의 보호조치도 중요하지만, 사고감지를 위해 미사용 및 데이터 보안징후에 대한 관리도 중요하다.

5.1.4 인공지능관련 진단지표연계 사항

현재 우리나라는 개인정보보호위원회에서 인공지능과 관련하여 개인정보보호를 위한 준수사항을 별도 점검표를 제공하여, 데이터의 처리단계별 점검과 상시점검으로 준수사항을 제시하고 있다. 즉, 단계별 점검은 4단계(기획·설계, 개인정보 수집·이용·제공·파기) 9개 점검사항이며, 상시점검에서 4단계(관리감독, 피해구제, 자율보호활동, 윤리점검) 7개 점검사항을 점검할 수 있으며, 호주의 AI서비스에 관한 위험관리방안 중 모니터링, 위험완화조치를 추가할 수 있다. 또한, 호주의 AI서비스에서의 위험관리를 위한 원칙과 EU의 AI시스템에서의 개인정보보호 원칙을 고려하여, 우리나라의 6대 원칙[11]과 호주의 8대 원칙[12] 중에 개인정보보호에 관한 원칙을 선정하였다. 끝으로, 상시적 점검사항을 관리감독할 뿐만 아니라 AI시스템의 위기관리를 해소하기 위한 모니터링, 위험완화를 위한 보호조치 등을 점검항

11) AI관련 개인정보보호 6대 원칙: 적법성, 안전성, 투명성, 참여성, 책임성, 공정성[34]

12) 호주의 AI사용원칙: ① 순효용 창출, ② 무해할 것, ③ 규제 준수, ④ 프라이버스 보호, ⑤ 공정함, ⑥ 투명성과 충분한 설명, ⑦ 경합성, ⑧ 책임성[35]

목으로 추가할 수 있다.

5.2 특정 IT기술관련 개인정보 관리수준 진단지표 구성 및 점수화

5.2.1 특정 IT기술관련 지표체계 점검사항

본 연구는 앞서 특정 IT기술의 도입에 따라 진단제도의 점검항목에 반영하여 개인정보보호를 위해 준수할 수 있도록 검토하였다. 이에 대해 「개인정보 보호법」에서 준수해야 할 기존 점검항목 외에 특정 IT기술에 관한 법률, 지침, 원칙, 가이드라인, 안내서 등을 기준으로 개인정보보호 준수사항을 검토하였다. 전문가 자문회의를 거쳐 특정기술이더라도 종합적으로 적용가능한 지표에 대해 공통지표로 적용가능한 지표로 구분하여 각 특정 IT기술의 특성지표로 나누어 적용하여 가중치를 차이로 점수화하여야 한다고 보았다.

따라서, EU의 GPDR과 같이 Privacy by Design 및 Privacy by Default를 기본적인 기준으로 적용할 수 있다. 이 경우 서비스기획단계부터 개인정보보호를 반영하도록 점검할 수 있다. 또한, 특정 IT기술에서 수집된 개인정보가 식별 또는 재식별되는 것을 방지하기 위해 개인정보 비식별 조치 및 가명정보처리에 대한 기준으로 활용할 필요가 있다.[13] 이외에 각 기술 및 서비스에 따라 특정 IT기술에 관한 필요한 기준 및 통합적 기준을 검토하여 Table 4와 같이 적용해 보고자 한다.

5.2.2 진단지표의 비중 및 적용

진단제도의 평가체계는 총 100점을 기준으로 관리체계 구축 및 운영 30점, 보호대책 수립 및 이행 30점, 침해대책 수립 및 이행 40점으로 배분하여 산정하고 있다. 이에 대해 진단지표의 가중치를 전문가 자문회의를 거쳐 의견을 수렴하였는데, 기존 100%에서 특정 IT기술의 반영정도를 조사하기 위해서는 현재 기준에서 정책지표 및 특정 IT기술에 대한 비중을 30%로 산정할 수 있으며, 현재 정책지표를 달리하지 않는 상황에서는 10%를 우선 반영하여 적용하여 10점을 기준으로 산정하여 도입의 적정성을 가질 수 있다고 보았다. 일례로, 각 항목을 공통항목으로 비식별 조치를 별도 항목으로 구성할 경우 또는 그렇지 않을 경우에 대해서 공통항목을 별도로 구성하여 공통사항에 대한 점수를 확보하고, 항목수의 변동에 따라 배점을 달리 하는 사항을 제안하였다.

Table 4. Composition of diagnostic index related to specific IT technology (draft)

Div.	Details
PIPI* of Common	• Applying PbD principles from planning and design stage
	• Applying & managing standards for pseudonymous information process and de-identification measures
PIPI* related Big data	• Preparing methods and procedures for refusal to process usage history information
	• Destructing if personal information is included among newly created information after de-identification and checking deidentification measures
PIPI* related Cloud	• Notifying disclosure of use, disclosure of domestic & foreign storage, and prohibition to provide the third party(Available on privacy policy)
	• Notifying confidentiality, return, and irreversible destruction of information(Available on privacy policy)
	• Specifying ownership of data according to cloud service processing(Available on privacy policy)
	• Protecting measures when user information is transferred to another service provider upon contract cancellation, termination, etc.
	• Checking data protection plan management, data tracking, monitoring, etc.
PIPI* related IoT	• Checking the application of IoT information security principles
	• Vouching visualization & transparency of operational policy according to the purpose of use and retention period of sensitive information
	• Managing log recording for intrusion detection, monitoring, accountability, etc. response to security threats
	• Checking destruction and prevention of further collection of personal information from the design stage to service termination
	• Managing unused data and data security signs for accident detection
PIPI* related AI	• Applying principle regarding ethical principles and legal compliance related to AI service
	• Checking actively carry out voluntary protection activities
	• Checking continuously ethical issues
	• Practicing mitigation as like monitoring, testing of infringement incidents and risk occurrences, etc.

*PIPI : Personal Information Protection Indicator

이렇게 가정할 경우 전체 평가항목수(N) 대비 '해당 없음'수(M)를 제외한 각 평가항목의 평가점수(k)를 산

13) 특정 IT기술에 관한 가명정보처리는 ① 빅데이터와 관련하여 가명정보처리 사항 점검 및 개인정보 관리, 공개된 개인정보, 이용내역 등 비식별 조치후 수집·저장·조합·분석, 비식별 조치 후 새롭게 생성된 정보가 개인정보를 포함할 경우, 즉시 파기 및 비식별 조치 등이며, ② 사물인터넷관련 서비스과정에서 수집된 민감정보의 비식별 조치, ③ 가명정보 처리시 허용된 목적 및 기준 준수로 통합 적용이 가능함.

정하여 10점 기준으로 산정하고, 이를 다시 10점(변경 가능 점수)을 기준으로 재산정할 수 있다. 물론, 해당 지표의 구성여부, 각 지표의 평가항목수에 따라 점수에 변동이 발생할 수 있으나, 일반화된 점수를 반영하여 신기술 분야를 별도 점검분야로 구성할 수 있음을 제시하고자 한다. 이에 대한 계산방법은 다음과 같이 특정 IT기술분야의 점수는 평가항목수에서 '해당없음'을 제외한 평가점수로 산정할 수 있다.

특정 IT기술분야 점수산정공식[14)]

$$= \frac{\sum_{i=1}^{N-M} k_i = k_1 + k_2 + \cdots + k_{N-M}}{N-M} \times 10$$

5.3. 기존지표와의 연계

이상과 같이 본 연구는 진단제도가 IT환경변화에 맞추어 지표체계의 변화를 가져오고 개인정보보호의 주도적 역할을 할 수 있도록 제안하고자 하였다. 특히, 빅데이터, 클라우드, 사물인터넷, 인공지능은 서로 결합하여 더 많은 서비스를 제공할 것이기에, 향후 결합연계에 따른 개인정보보호사항도 지표체계에 반영할 수 있어야 할 것이다. 본 연구는 문헌조사를 바탕으로 실무자 및 전문가 관점에서 적절한 진단지표의 개선에 관한 의견을 반영하였으며, 이를 바탕으로 세부적 지표사항을 도출하여 검증할 수 있었다. Fig. 2는 지표체계의 적용분야인 관리체계 구축 및 운영, 보호대책 수립 및 이행, 침해대책 수립 및 이행과 함께 본 연구에서 도출한 특정 IT기술연계 개인정보보호지표를 특정 IT 적용 및 관리 분야를 구성하여 지표체계를 구성하는 방안을 Fig. 2와 같이 제시할 수 있다.

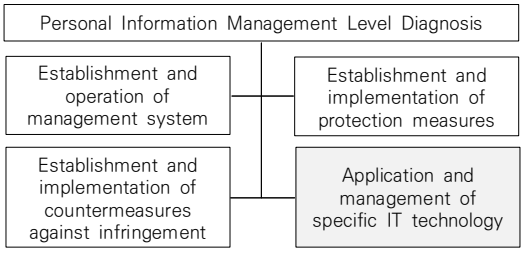

Fig. 2. New system for Personal Information Management Level Diagnosis

6. 결론

개인정보 관리수준 진단제도는 공공기관을 대상으로 정책 및 법률상 준수해야할 사항을 실행하도록 하는 제도라고 볼 수 있다. 다만, 제도적 정착을 가져오는 동안 새로운 기술에 대응하여 주도하는 기준을 적용하여 제도적 확장성을 가져오지 못하였다. 이에 따라, 본 연구에서는 4차 산업혁명의 핵심기술인 빅데이터, 클라우드, 사물인터넷, 인공지능에 관한 공공서비스가 확대되고 있고, 그 과정에서 개인정보처리가 이루어지므로 안전한 관리를 위해 진단제도의 지표체계에 대한 개선을 가져올 필요성을 제기하고자 한다.

이를 위해 법적 준수사항을 점검하여 개선조치함에 있어서, 특정 IT기술의 개인정보보호 및 정보보호에 관한 기준들에 대해 문헌분석을 하였다. 그 과정에서 개인정보처리과정에 대한 진단체계와 중복되지 않은 사항을 진단지표로 도출하였다. 이에 대해 공공기관의 개인정보보호 담당자 및 관계전문가들의 의견을 수렴하여 개인정보 관리수준 진단지표에 활용할 수 있도록 검증하였다. 이에 따라 선정된 특정 IT기술에 관련된 개인정보보호 준수사항은 다시 재정비되어 공통적인 측면에서 2개 점검항목과 각 분야별 점검항목으로 구분하였다. 특히, 빅데이터관련 2개 항목, 클라우드관련 5개 항목, 사물인터넷관련 5개 항목, 인공지능관련 4개 항목을 도출하였다. 본 연구를 위해서 기존 진단제도에서 운영하고 있는 진단지표 및 점검사항 외에 다양한 변화에 필요한 개인정보보호사항을 반영하도록 하였다. 그동안 개인정보 관리수준진단제도에 관한 연구들이 지표체계의 적정성 및 활용성을 고려하였다면, 본 연구는 새로운 IT환경에 적절한 지표체계의 확장성을 제안하고자 하였다. 본 연구는 향후 지속적인 개인정보 관리수준 진단제도의 발전을 위해 새로운 기술변화에 대응하는 제도적 장치가 될 수 있으리라 본다.

REFERENCES

[1] Y. J. Shin, S. Y. Cho, G. H. Chae & H. G. Choi. (2021). *The Research on improvement of personal information management level diagnosis system*, Korean Internet & Security Agency.

[2] Personal Information Protection Commission.

14) • 특정 IT기술 평가항목수: N • '해당없음' 평가항목수: M • 각 평가항목의 평가점수: k

(2021.3). *2021 Public Institutions Personal Information Management Level Diagnosis Manual.*

[3] J. H. Cheong (2010). Study on AHP and Non-Parametric Verification on the Importance of the Diagnosis Indicators of Personal Information Security Level. *Journal of The Korean Data Analysis Society. 12(3),* 1499-1510.

[4] S. H. Lee, H. E. Park & S. G. Choi. (2011. 6). A Study on index improvement of personal information protection level diagnosis in the public organizations. *Proceedings of Symposium of the Korean Institute of communications and Information Science,* 207-208.

[5] Y. J. Shin, H. C. Jeong & W. Y. Kang. (2012). A Study of Priority for Policy Implement of Personal Information Security in Public Sector: Focused on Personal InformationSecurity Index. *Journal of the Korea Institute of Information Security & Cryptology, 22(2),* 379-390.

[6] M. S. Jeong & K. H. Lee. (2015. June) A Study on Personal Information Protection Management Assessment Method by DEA. *Journal of the Korea Institute of Information Security & Cryptology. 25(3),* 691-701.
DOI : 10.13089/JKIISC.2015.25.3.691

[7] C. H. Jang & Y. H. Cha. (2021). A Study on the Determinants of Personal Information Protection Activities: With a Focus on Personal Information Managers *Informatization Policy, 28(1),* 64-76.
DOI : 10.22693/NIAIP.2021.28.1.064

[8] C. W. Park, J. W. Kim & H. J. Kwon. (2016). An Empirical Research on Information Privacy Risks and Policy Model in the Big data Era. *The Jounal of Society for e-Business Studies. 21(1),* 131-145.
DOI : 10.7838/jsebs.2016.21.1.131

[9] Y. W. Lee, H. M. Jang & S. P. Hong. (2012. Nov.). A Design of the Large-Scale Personal Information Management Model for Privacy Protection in BigData Environments, *Korean Proceeding of Symposium of Society for Internet Information*, 29-30.

[10] S. H. Na & E. N. Huh. (2012. Nov.). Privacy-preserving Reference Model for Personal Cloud. *Seminar Proceeding of The Korean Institute of Information Scientists and Engineers. 39(2C),* 146-148.

[11] Y. J. Shin. (2015. March). A Study on Development for Conformity Assessment Indicators of Privacy in Cloud Services. *Journal of Korean Associastion for Regional Information Society. 18(1),* 1-31.
DOI : 10.22896/karis.2015.18.1.001

[12] J. D. Kim, D. H. Park & H. Y. Youm. (2015). A Study on development of privacy indicators in the context of cloud service level agreement *Journal of Digital Convergence. 13(2),* 115-120.
DOI : 10.14400/JDC.2015.13.2.115

[13] Y. J. Shin. (2018. Sept.). A Study on Developing Policy Indicators of Personal Information Protection for Expanding Secure Internet of Things Service. *Information Policy. 25(3),* 29-51.
DOI : 10.22693/NIAIP.2018.25.3.029

[14] Y. J. Shin. (2018. Sept.). A Study on Developing and Applying Framework and Assessment Standard of It's Conformity of Personal Information Protection for IoT Service Subject. *Journal of Korean Associastion for Regional Information Society, 23(2),* 83-117.
DOI : 10.22896/karis.2020.23.2.004

[15] W. T. Lee & J. M. Kang. (2016. 8. 31). A study on Model of Personal Information Protection based on Artificial Intelligence Technology or Service. *The Journal of The Institute of Internet, Broadcasting and Communication (IIBC). 16(4),* 1-6.
DOI : 10.7236/JIIBC.2016.16.4.1

[16] Korea Communications Commission, Korea Internet & Security Agency. (2015). *Big data privacy guideline commentary,*

[17] Ministry of Public Administration and Security, (2021. 6. 25). Provision and Use of Pseudonym Information in the Public Sector More Safely, *Ministry of Public Administration and Security Press Release.*

[18] H. J. Lim. (2017. April). Analysis of personal information de-identification processing methods in big data environment. *Electronic Finance and Financial Security, 8,* 13-17.

[19] Information Commissioner's Office. (2017). *Big data, artificial intelligence, machine learning and data protection.*

[20] Korea Communication Commission. (2011). *SLA guide in Cloud computing.*

[21] Korea Internet & Security Agency. (2019). *Information Protection and Personal Information Protection Management System Certification System Guide.*

[22] Lloyd's Register. (n.d.). *Lloyd's Register, cloud security assurance* (Online). https://www.lr.org/ko-kr/csa-star/

[23] J. W. Kim. (n.d). ISO/IEC 27018, International Standards for personal information protection of Cloud Service., Data Protection & Privacy(Online).

https://blog.naver.com/n_privacy/222432267736

[24] Ministry of Science and ICT, Korea Internet & Security Agency, (2020). *Cloud Service Security Certification System Evaluation Criteria Commentary.*

[25] D. H. Lee & N. J. Park. (2017). Proposal of Technology and Policy Post-Security Management Framework for Secure IoT Environment, *Journal of KIIT. 15(4),* 127-138. DOI : 10.14801/jkiit.2017.15.4.127

[26] AhnLab. (2016.10.5), *IoT Security Guide for the Internet of Things Era* (Online). https://blog.daum.net/simjy/11993768

[27] Personal Information Protection Committee & Korea Internet & Security Agency, (2020. Dec.). *Guidelines for Protection of Personal Information Automatically Processed,*

[28] Korea Internet & Security Agency. (2016). *Guide to Cryptographic Authentication Technology in Internet of Things (IoT) Environment*

[29] H. M. Jung, K. M. Jeong & H. J. Cho. (2017. Nov.). A Design for Security Functional Requirements of IoT Middleware System. *Journal of the Korea Convergence Society. 8(11),* 63-69. DOI : 10.15207/JKCS.2017.8.11.063

[30] IoT Security Alliance. (2016). *IoT Common Security Guideline*s, 2016.

[31] Johan Sjölund. (2020). Cybersecurity evaluation of IoT systems, *South-Eastern Finland University of Applied Sciences.*

[32] G. J. Lee, (2021. 7. 27). *Setting up standards for personal information protection such as artificial intelligence and autonomous driving*, Information and Communication Newspaper (Online). https://www.koit.co.kr/news/articleView.html?idxno=80658

[33] Sejong Law Firm, (2021. 5. 21). *Legal issues related to the use of unstructured data in light of the Personal Information Protection Commission's sanction for 'Leeruda'.* (Online). http://www.shinkim.com/kor/media/newsletter/1498

[34] Personal Information Protection Committee. (2021. 5. 31). *Artificial Intelligence (AI) Personal Information Protection Voluntary Checklist.*

[35] Australian Government, Department of Industry, Science, Energy and Resource. (2019. Nov.). Artificial Intelligence : Australia's Ethics Framework, *A Disscussion Paper* (Online). https://consult.industry.gov.au/strategic-policy/artificial-intelligence-ethics-framework/supporting_documents/ArtificialIntelligenceethicsframeworkdiscussionpaper.pdf

[36] uropean Commission. (2020). *White Paper on Artificial Intelligence - A European approach to excellence and trust, COM.*

[37] European Commission. (2021. 4. 21) *Proposal for a Regulation laying down harmonized rules on artificial intelligence (Artificial Intelligence Act),*;

[38] S. K. Han, (2021). Implementation of the European Union's Draft AI Act, 2021 KISA Report.

[39] J. K. Lee. (2021). Examine the meaning of disposition of 'Leeruda'. *2021 KISA Report Korea Internet & Security Agency,*

[40] Reuters. (2021. 4. 21). EU set to ratchet up AI fines to 6% of turnover - *EU document.*

[41] Korea Internet & Security Agency, (2021). Regulation and protection of personal information of main contents of EU artificial intelligence(AI). *Personal Information Protection Monthly Trend Analysis, 5,* 1-10.

신 영 진(Young-Jin Shin) **[정회원]**

- 1996년 2월 : 성결대학교 행정학과 (행정학학사)
- 1998년 2월 : 단국대학교 일반대학원 행정학과(행정학석사)
- 2004년 2월 : 성균관대학교 일반대학원 행정학과(행정학박사)
- 2002년 9월 ~ 2014년 10월 : 성균관대 국제정보정책전자정부연구소 선임연구원
- 2004년 10월 ~ 2012년 7월 : 행정안전부 정보화전략실 전문위원
- 2012년 8월 ~ 2013년 2월 : 고려대학교 정보보호대학원 연구교수
- 2013년 3월 ~ 현재 : 배재대학교 지능SW공학부 정보보안학 부교수
- 관심분야 : 개인정보보호, 정보보호정책, 전자정부, 4차 산업혁명 신기술
- E-Mail : jinsyj@yahoo.com