Journal of Convergence for Information Technology
Vol. 10. No. 7, pp. 20-32, 2020
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2020.10.07.020

IoT서비스제공자가 준수해야 할 개인정보보호 프레임워크의 개발 방안

신영진
배재대학교 산학협력단 교수

Development of Personal Information Protection Framework to be Followed by IoT Service Providers

Young-Jin Shin
Professor, Industry Academic Cooperation Foundation, PaiChai University

요 약 본 연구는 IoT서비스제공자가 IoT 제품 및 서비스를 제공하는 전반적인 과정에서, IoT서비스주체의 개인정보를 안전하고 체계적으로 운영할 수 있는 개인정보보호프레임워크를 개발하여 제공하고자 한다. 이를 위해서 문헌조사를 통해 개인정보프레임워크에 관한 구성요소틀을 도출하였으며, 전문가심층면접조사를 통해 개인정보보호 프레임워크를 IoT서비스제공과정과 IoT개인정보처리과정으로 각 3개 단계 3개 분야 2개 지표로 선정했다. 이렇게 선정한 개인정보보호프레임워크의 구성요소간 중요도를 AHP기법을 이용한 관련분야 전문가들을 대상으로 전자메일조사를 실시했다. 그 결과, IoT서비스제공과정에서는 IoT제품 및 서비스의 설계·개발단계(0.5413)가 가장 중요하며, IoT개인정보처리과정에서는 개인정보의 수집·보유단계(0.5098)에서의 개인정보보호가 가장 중요하다. 따라서, 본 연구를 바탕으로 IoT서비스가 확산되는 가운데, 보안위협 및 개인정보 침해사고를 예방하여 안전한 개인정보보호 프레임워크가 구현되리라 본다.

주제어 : IoT서비스제공자, IoT서비스주체, IoT제품 및 서비스 개인정보보호 프레임워크, 우선순위분석(AHP)

Abstract This study is to develop and provide a personal information protection framework that enables IoT service providers to safely and systematically operate personal information of IoT service subjects in the overall process of providing IoT devices and services. To this end, a framework for personal information framework was derived through literature survey, and FGI with experts, it was divided into three stages, each of three stages: IoT service provision process and IoT personal information processing process. The study conducted an e-mail survey of related experts using AHP techniques to determine the importance of the components of the selected personal information protection framework. As a result, in the IoT service provision process, the IoT product and service design and development stage (0.5413) is the most important, and in the IoT personal information processing process, personal information protection in the collection and retention of personal information (0.5098) is the most important. Therefore, based on this research, as the IoT service is spreading, it is expected that a safe personal information protection framework will be realized by preventing security threats and personal information infringement accidents.

Key words : IoT service provider, IoT service subject, IoT product and service privacy protection framework, Priority analysis (AHP)

*This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea(NRF-2019S1A5A2A01047599).
*This article is extended and excerpted from the conference paper presented at The Korean Association for Policy Studies.
Received May 20, 2020 Revised June 19, 2020
Accepted July 20, 2020 Published July 28, 2020

1. 서론

4차산업혁명의 핵심기술인 사물인터넷(Internet of things: 이하 IoT)산업이 확대되면서, 국내외사물인터넷시장이 크게 증가하고 있다. Mckinsey사(2015)는 2025년까지 공장, 보건, 도시, 물류, 교통 등 다양한 분야에서 IoT활용이 증가하여 연간 3.9~11.1조 달러의 경제적 파급효과를 전망했다[1]. 그러나 IoT서비스가 확대될수록 사이버보안위협 및 개인정보 침해사고도 증가하고 있어, IoT서비스의 안전성을 확보하는 방안이 필요하다.

이에 따라 과학기술정보통신부, 행정안전부, 금융위원회 등은 개인정보보호를 위한 가이드라인을 제정하여 배포하였고, 관련 법률에 근거한 정보보호관리체계 및 인증제도를 운영하고 있다. 그러나, 이러한 노력은 IoT서비스제공자가 개인정보보호를 큰 틀에서 접근하도록 하여, 실제 운영 상에서 개인정보보호를 준수하는지 점검하여 대응하기에는 한계가 있다. 특히, IoT서비스제공과정에서는 기술적 접근에 치중한 보안요소를 반영하였기에, 관리적 접근을 보완할 필요가 있다.

따라서, 본 연구에서는 IoT서비스제공과정에서 IoT제품 및 서비스의 생애주기와 개인정보의 생애주기를 연계하여, IoT제품 및 서비스 설계단계부터 폐기단계까지 개인정보보호를 위한 준수사항을 비롯하여, IoT개인정보처리과정에서의 개인정보 수집단계부터 파기단계까지 필수사항을 선정하여 실천할 수 있도록 개인정보보호 프레임워크를 제안하고자 한다.

2. IoT개인정보보호에 관한 논의

2.1 IoT서비스와 개인정보보호

2.1.1 IoT서비스에서의 개인정보 침해사고

IoT가 IoT자체적인 기술뿐만 아니라 다른 신기술과 결합하여 초연결사회를 실현하고 있다. 특히, 스마트도시는 스마트홈, 스마트에너지, 스마트헬스케어 등 IoT기술을 기반으로 하므로, IoT를 통한 경제성장을 기대하고 있다. 실제, 전세계 IoT시장규모가 연평균 14.4%(2017~2021)로 성장하고 있으며, 국내외적으로 IoT에 관한 기술개발과 서비스보급이 이루어지고 있다.

그러나, IoT환경에서 발생하는 보안위협이나 개인정보 침해사고 등은 기존 인터넷보다 더 큰 피해를 가져올 것이다. 특히, 가정 내의 멀티미디어제품, 생활가전제품, 홈네트워크제품 등이 일상생활에서 사용되면서, 악의적·비인가된 접근, 프라이버시 침해 등 개인정보 침해사고가 증가하고 있다. 이에 따라 IoT 제품 및 서비스의 안전한 보급을 위해서는 개인정보보호가 함께 추진되어야 한다. 특히, IoT서비스제공자가 IoT제품 및 서비스와 관련된 전 과정에서 스스로 개인정보보호를 실천할 수 있는 기준이 필요하며, 반드시 준수해야 할 사항으로 적용하기 편리한 개인정보보호 프레임워크가 마련되어야 한다.

2.1.2 기존의 개인정보보호 점검기준

IoT서비스제공자가 IoT제품 및 서비스의 보안성을 높이도록 국내외적으로 정보보안원칙과 기준을 마련하고 있다. 현재 마련되어 운영 중인 국내외적인 기준을 살펴보면, OWASP의 IoT 취약점에 관한 10가지 보안원칙, 한국인터넷진흥원의 IoT 공통보안원칙, IoT보안얼라이언스(IoT보안협의체)의 IoT 공통보안 7대 원칙 등이 있다. 또한, 일반적인 개인정보보호 및 정보보호를 위한 관리체계들은 ISO/IEC 27001 인증을 비롯하여, 정보보호 및 개인정보보호 관리체계 인증(ISMS-P), 개인정보 영향평가(PIA), 개인정보보호수준진단 등이 있다[3]. 그러나, 기존에 운영 중인 개인정보보호 점검기준들은 IoT보안을 위한 제품관리, 연결관리, 애플리케이션관리, 보고 및 분석 등의 IoT관리플랫폼이지만, 아직 IoT보안구성요소에 대한 기술표준과 규정이 없는 실정이다[4].

물론, 한국인터넷진흥원이 IoT보안 제품 및 모듈, IoT제품 관리 등에 대해 모바일앱과 연동함에 있어서 사용자 및 제품 인증, 안전한 암호알고리즘 사용, 데이터 저장 및 전송 암호화 등을 보안인증을 실시하고 있다[5]. 그러나, IoT 제품 및 서비스를 종합적으로 점검하는 기준에는 부족한 실정이다.

2.1.3 IoT개인정보보호프레임워크의 중요성

안전한 IoT환경을 구현하기 위해 EU, 미국, 중국, 일본 등 해외에서뿐만 아니라 우리나라에서도 다양한 보호대책이 수립되고 있다. 또한, 국제기구, IoT관련 협회 등에서도 여러 보안대책을 담은 기준을 마련하고자 노력 중이다. 그러나, 너무 큰 맥락에서 접근하거나, 세부적인 기술점검에 중점을 두고 있어, IoT

서비스제공자에게 실질적인 준수사항으로 활용하는데 한계가 있다.

따라서, 본 연구에서는 IoT서비스제공자가 IoT서비스제공과정 및 IoT개인정보처리과정에서의 보안위협 및 개인정보 침해사고를 예방하고 안전한 IoT 제품 및 서비스가 유통될 수 있도록 개인정보보호 프레임워크를 개발하여, IoT서비스주체로부터 신뢰받는 IoT환경을 구현해 나가고자 한다. IoT서비스제공자는 IoT제품제조자, 소셜 플랫폼 서비스제공자, 애플리케이션 개발자, IoT 데이터 플랫폼 제공자, 기타 참여자로서 IoT제품에서 수집한 개인정보처리자로 유형화된다[2]. 이에 대해 본 연구에서는 IoT제품 및 서비스를 설계부터 폐기까지 참여한 개인정보처리자, IoT서비스의 운영 중 개인정보가 수집 및 파기되는 과정에 참여하는 개인정보처리자를 IoT서비스제공자로 정의하고자 한다. 이에 따라 IoT서비스제공자가 IoT제품 및 서비스의 제공과정과 IoT서비스운영상 개인정보처리과정에서 개인정보보호를 강화하는 체계적인 프레임워크를 제안하고자 한다.

2.2 기존 연구 검토

본 연구의 목적인 IoT서비스제공자가 준수해야 할 개인정보보호 프레임워크를 개발하기 위해 기존 연구들을 살펴보았다. 이야리 외(2014)는 IoT환경에서 정보주체의 민감한 개인정보를 보호하기 위한 보호정책의 적용과 효율적 정보기술 활용 및 제공 가능한 개인정보보호프레임워크를 제안했다[6]. 또한, 이영란 외(2016)는 국방 사물인터넷에 필요한 IoT보안표준과 IoT공통보안원칙, IoT보안가이드라인 등에 따라 국방 사물인터넷에 필요한 정보보호 프레임워크를 생애주기별 관리대책으로 제시했다[7]. 또한, 박세환 외(2014)는 기존의 인터넷거버넌스를 참조하여 사물인터넷에 관한 데이터베이스를 구축하고 IoT실정에 맞는 개인정보보호정책 등을 개발하여야 함을 주장했다[7]. 이 외에도 홍승필 외(2015)는 IoT환경에서의 개인정보보호를 위한 표준플랫폼 적용, IoT 제품 및 서비스 진단체계의 기준 및 자율점검 등을 통한 보안강화를 제안했다[8]. 그러나, 이렇게 학자들이 제기한 개인정보보호 프레임워크는 기술적 접근이거나, 단편적 제품에 대한 보안성을 높이고자 했다. 물론, 박남제 외(2016)는 IoT 제품 및 서비스에 관한 국내외 현황 및 보안가이드라인을 분석하여 적합한 보안모델을 수립하고, IoT보안성을 유지하기 위한 방안을 제시했다[9]. 강남희 외(2015)도 서비스제공자, 제조사, 이용자가 IoT 제품 및 서비스를 제공하면서 준수해야 할 보안항목을 제안했다[10].

그러나, IoT서비스제공자가 실행해야 할 방향성을 종합적인 과정으로 제안하지 못하고 있다. 이에 따라, 기존의 보안가이드라인에 따라 보안모델을 제공하기보다는 실제 운영상에 준수해야 할 개인정보보호 프레임워크를 마련해야 한다. 또한, IoT 제품 및 서비스의 전반적인 과정을 모두 가이드라인으로 제공하지 못하기 때문에, IoT서비스제공자가 개인정보 침해사고를 예방할 수 있는 IoT서비스제공과정과 그 가운데 개인정보처리과정에서의 개인정보보호를 강화할 기준을 정립되어야 한다.

이에 따라 Table 1과 같이 기존 연구와 본 연구의 차이를 비교하여, 본 연구가 IoT서비스제공과정 및 IoT개인정보처리과정에서 IoT서비스제공자가 서비스설계부터 폐기까지 운영과정과 개인정보의 수집부터 파기까지 상호 연계한 안전한 개인정보보호 프레임워크를 제언하고자 한다. 특히, IoT서비스제공과정 및 IoT개인정보처리과정에서의 보안위협 및 취약성으로부터 개인정보를 보호할 수 있는 기준을 마련하고자 한다.

Table 1. Differences between the previous study and this study

Previous study	This study
•Present a framework for the use and provision of PIP** technology in the IoT environment •Present management measures for each life cycle such as IoT security standards and principles •Enhance the standards of diagnostic system and autonomous inspection for PIP** platform and diagnostic system in IoT service •Present appropriate security model and security items for IoT devices and services	•Present a comprehensive PIP framework in the IoT environment •Present protection measures of each stage in IoT service provision process and in the process of IoT PI processing •Present compliance in IoT service provision process and in the process of IoT PI* processing •Propose the priority of PIP for safe IoT devices and services from an expert viewpoint

* PI: Personal Information
** PIP: Personal Information Protection

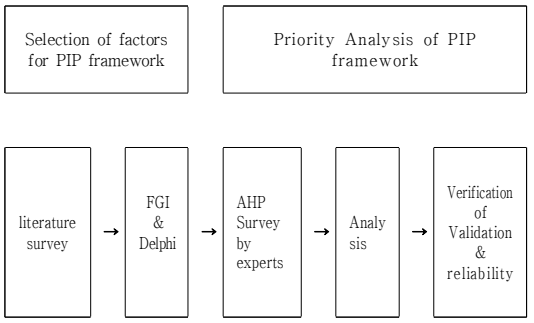
3. 연구의 분석 틀과 방법

3.1 연구의 흐름도

본 연구는 IoT서비스제공자가 준수해야 할 개인정

보보호 프레임워크를 IoT서비스제공과정 및 IoT개인정보처리과정에서 핵심요소를 도출하여 제시했다. 이를 위해 본 연구에서는 기존 연구논문, 연구보고서, 정부백서, 정부발간보고서, 뉴스, 잡지, 인터넷자료 등을 검토하였으며, 개인정보보호 프레임워크의 구성요소를 도출하기 위해 소그룹으로 구성된 전문가들을 대상으로 심층면접조사(Focus Group interview: FGI) 및 델파이조사(Delphi):를 실시하여 IoT서비스제공과정 및 IoT개인정보처리과정에서의 개인정보보호를 세부 단계, 분야 및 지표로 구성했다.

이렇게 선정한 구성요소들의 중요도 및 우선순위를 분석하기 위해 계층화의사결정방법(Analytic Hierarchy Process: AHP)을 적용한 설문조사를 실시했다. 이러한 설문내용을 바탕으로 전문가들의 의견을 반영한 중요도 및 우선순위를 분석하였으며, 분석결과에 대한 SPSS를 이용한 타당성 및 CI/CR값을 활용한 신뢰성을 검증했다. 이처럼 본 연구의 흐름은 Fig. 1과 같이 정리할 수 있다.



* PIP: Personal Information Protection

Fig. 1. The Flows of the study

3.2 연구의 분석틀과 방법론

먼저, IoT서비스제공자가 준수해야 할 사항을 도출하기 위해 사용한 심층면접조사(Focus Group Interview: 이하 FGI)는 소수관계자와의 집중화된 대화를 통한 면접방법으로 전문가집단토의로 진행하며, 델파이조사(Delphi)는 2~3회 전문가들의 의견을 듣고 피드백하여 예측하는 조사방법이다[011]. 본 연구에서는 개인정보보호 프레임워크 요소를 도출하기 위해 5차례 FGI와 2차례 Delphi를 적용한 분석과정은 Table 2와 같다.

Table 2. Analysis process using FGI and Delphi

Div.	Date	Detail Issue
1st FGI	2019. 8. 1	Review of necessity and policy direction for PIP framework of IoT service
2nd FGI	2019. 9. 26	Review to select check items of PIP for IoT service provider
3rd FGI	2019. 11. 28	Review to be applicable traceable response & management system in IoT service
4th FGI	2019. 12. 9	Review to add IoT weakness and security technology inspection items for PIP in IoT service
1st Delphi	2020. 2. 10	Verification of suitability to composed PIP factors and appropriateness of questionnaire to analyze PIP framework
2nd Delphi	2020. 4. 9	Verification of survey and results using AHP technique
5th FGI	2020. 4. 27	Review of validity of the analysis results, CI & CR and utilization plan

다음으로, 계층화의사결정방법(AHP)은 복잡한 기준을 고려하여야 하는 상황에서 정량적 요소뿐만 아니라 정성적 요소까지 논리적이고 체계적으로 반영할 수 있도록 하는 의사결정방법이다[012]. AHP는 의사결정요소들을 선정하여 쌍대비교를 통한 가중치를 계상할 수 있다. 이러한 가중치의 신뢰도는 이해관계자의 논리적 일관성정도(Consistency Ratio: CR)를 통해 검토할 수 있다. 이에 따라 본 연구는 전문가 대상의 AHP분석을 위해 2020년 2월 14일부터 2월 28일까지 이메일을 이용하여 설문조사를 했다. 본 설문조사는 각 지표의 상대적 가중치를 계산하기 위한 9점 척도의 2개 요소를 비교하는 쌍대비교방식을 적용했다.

Table 3은 IoT개인정보처리과정 중 개인정보 수집단계와 이용·제공단계를 비교한 예이며, 더 중요하다고 생각하는 지표 쪽에 '○'을 표기하거나 동일하게 중요하다고 생각하는 경우 예와 같이 '같음'에 '○'을 표기하면 된다. 본 설문은 관련 분야의 전문가들을 대상으로 표본조사를 하였으며, Table 4와 같이 응답한 82명(학자, 실무자, 공무원 등)의 경력과 전공을 정리하였는데, 10년단위로 구분할 때 11년부터 20년 경력자가 34명으로 가장 많았고, 전공에 대한 응답결과를 4개 분야로 정리한 결과, 개인정보보호 및 정보보호 전공자가 36명으로 많았다. 이처럼 본 연구는 전문가대상의 각 지표별 중요도 및 우선순위에 관한 의견을 수렴하기에, 정규분포를 고려할 때 표본수로 충분했다.

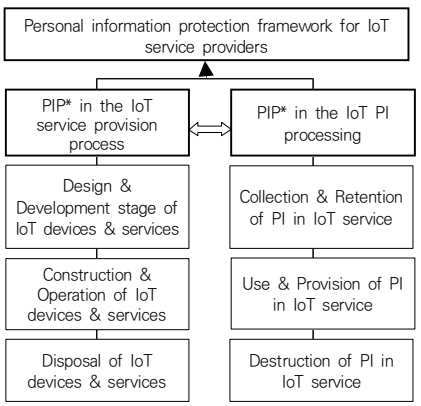
Table 3. Sample for AHP survey form

A Indicator	Ab so lute		very		im portant		Few		equi valence		Few		im portant		very		Ab so lute	B Indicator
	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
Collection & Retention of PI in IoT service									○									Use & Provision of PI in IoT service

Table 4. Careers and majors of the experts

Career year / People No.	1~10	11~20	21~30	31~40
	18	34	23	6
Major Field / People No.	ICT	privacy & Security	Policy/Law	Others
	17	36	24	5

끝으로, 응답결과의 타당성 및 신뢰성 검토를 위해 SPSS프로그램을 통한 통계결과로 검증했고, 응답결과의 신뢰성은 AHP분석기법의 일관성지수(Consistency Index: 이하 CI) 및 일관성 정도(Consistency Ratio: 이하 CR)를 산정하여 검증했다. 이처럼 본 연구는 IoT서비스제공자가 IoT서비스제공과정과 IoT서비스의 개인정보처리과정으로 구분하여 세부 단계별 준수해야 할 개인정보보호 프레임워크를 Fig. 2와 같이 개발하고자 한다.



* PI: Personal Information
** PIP: Personal Information Protection

Fig. 2. Framework of the study

4. 연구결과

4.1 FGI 및 Delphi 분석결과

본 연구는 기존 연구(학회보, 학술대회발표논문 등), 정부 및 공공기관 발간보고서 등에서 1차 자료를 수집하여, 전문가 인터뷰 및 심층면접 등 FGI는 2019년 8월 1일부터 2020년 4월 27일까지 5회 진행했으며, 전문가 자문회의를 통한 Delphi는 2020년 2월 10일과 2020년 4월 9일 개최하여 지표의 선정 및 타당성을 검증했다. 이렇게 선정된 지표들은 개인정보보호 프레임워크를 IoT서비스제공과정과 IoT개인정보처리과정에서의 단계별 분야 및 지표로 구성했다.

먼저, IoT서비스제공과정에서의 개인정보보호를 살펴보면, 3개 단계 9개 분야 18개 지표로 구성했다. 첫째, IoT 제품 및 서비스의 설계 및 개발단계는 IoT 제품 및 서비스의 개발환경 보안 설계, IoT 제품 및 서비스의 데이터 보안 설계, IoT 제품 및 서비스의 기기 및 시스템 보안 설계로 3개 분야를 구성했다. 각 분야별 구성하고 있는 지표를 살펴보면, IoT 제품 및 서비스의 개발환경 보안 설계분야는 목표 시스템보안설계과 인터페이스 보안 설계로 지표를 구성했다. IoT 제품 및 서비스의 데이터 보안 설계분야는 민감정보 보안 설계와 데이터 식별 및 추적 설계로 구성했다. IoT 제품 및 서비스의 기기 및 시스템 보안 설계는 IoT 제품·서비스 보안 설계와 시스템 보안 설계을 지표로 구성했다.

둘째, IoT 제품 및 서비스의 구축 및 운영단계를 구성하는 분야는 IoT 제품 및 서비스의 네트워크 보안 운영, IoT 제품 및 서비스의 프로그램 보안 운영, IoT 제품 및 서비스의 보안대책 수립 및 운영이다. 각 분야별 지표를 살펴보면, IoT 제품 및 서비스의 네트워크 보안 운영분야는 네트워크환경의 안전성 확보와 네트워크환경의 안전성 확보로 구성했다. IoT 제품 및 서비스의 프로그램 보안 운영분야는 안전한 코딩규칙에 따라 적용 점검과 안전한 보안기술 적용 점검으로 지표를 구성했다. IoT 제품 및 서비스의 보안대책 수립 및 운영분야는 보안기능 검토에 따른 보안대책 구현과 모의해킹을 통한 안전성 검증으로 구성했다.

셋째, IoT 제품 및 서비스의 폐기단계는 IoT 제품 및 서비스의 폐기절차 및 계획 수립, IoT 제품 및 서비스의 불필요한 자료 보유 방지, IoT 제품 및 서비스의 안전한 폐기 관리로 분야를 구성했다. 각 분야별 구성된 지표를 살펴볼 수 있는데, IoT 제품 및 서비스의 폐기절차 및 계획 수립분야는 폐기시 처리절차 마련과 폐기대상분류

및 폐기계획 수립으로 구성했다. IoT 제품 및 서비스의 불필요한 자료 보유 방지분야는 불필요 자료저장 통제와 태그 기능 제거 또는 중지로 지표화했다. IoT 제품 및 서비스의 안전한 폐기 관리분야는 안전한 폐기절차에 따라 SW 제거와 암호키, 비밀번호 등 폐기절차 준수로 지표를 구성했다. 이렇게 하여 IoT서비스제공과정에서의 개인정보보호는 전체 3개 단계, 9개 분야 18개 지표와 조작적 정의 및 출처를 Table 5와 같이 정리했다.

Table 5. The Composition factors for Personal Information Protection in IoT service provision process

Stage (Abbr)	Field(Abbr)	Indicator(Abbr)	Operational definition	Source
Design & Development Stage of IoT devices & services {DD}	Security design for development environment of IoT devices and services(SDE)	Security design of target system(SDTS)	Security design for IoT devices and services such as observing the principles of 'Security by Design' and 'Privacy by Design' and setting security protocols and secure parameters	[13,16]
		Security design of interface(SDOI)	Security design considering the details of each system list and security function connecting the target system, unauthorized physical / logical access control to the product through an external interface, etc.	[13,14]
	Security design for data of IoT devices and services(SDD)	Security design of sensitive information(SDSI)	Security design by visualizing operational policies including the purpose and duration of use of sensitive information and establishing measures for transparency, integrity, and confidentiality of PI	[14,16]
		Security design for identification and tracking for data(SDIT)	Security design considering protection measures such identification and flow design of PI, and tracking technology	[10,13, 14]
	Security design for devices & system of IoT devices and services(SDS)	Security design for IoT devices and services(SDDS)	Security design in the development environment for the target system, such as weight reduction for PIP, transparency guarantee, and application of safety-proven protocols according to the characteristics of IoT devices & services	[14,16, 20]
		Security design for IoT system(SDIS)	Security design based on the security requirements of IoT system middleware, SCADA system, and business information system	[19,20]
Construction & Operation Stage of IoT devices & services (CO)	Network security operation of IoT devices and services (NSO)	Secure safety of network environment(SSNE)	Enhancement of functions such as mutual authentication network services, encrypted data transmission & integrity verification, network address filtering considering area control measures of embedded HW executable code	[20]
		Secure safety of platform environment(SSPE)	Platform protection such as secure update, integrity verification of set value and executive code, confirmation of authorized user before performing update, use of the latest security patch applied version when using 3rd party library, etc.	[13,15]
	Program security operation of IoT devices and services(PSO)	Check applying for safe coding rule(CASC)	Perform programming of developer and check secure coding itself through unit tests according to the secure coding rules established in the requirements definition phase	[16]
		Check applying for safe security technology(CASS)	Security design for IoT devices and services such as observing the principles of 'Security by Design' and 'Privacy by Design' and setting security protocols and secure parameters	[13,14]
	Establishment and operation for security measures of IoT devices & services(EOM)	Implementation of security measures by reviewing security functions(SMSF)	Security design considering the details of each system list and security function connecting the target system, unauthorized physical / logical access control to the product through an external interface, etc.	[14,15]
		Verification of safety through mock hacking(VSMH)	Security design by visualizing operational policies including the purpose and duration of use of sensitive information and establishing measures for transparency, integrity, and confidentiality of PI	[14,16]
Disposal Stage of IoT devices & service (Di)	Disposal procedure and planning for IoT devices and services (DPP)	Preparation of disposal procedure(PODP)	Security design considering protection measures such identification and flow design of PI, and tracking technology	[17- 20]
		Classification of disposal targets & establishment of disposal plan (CDED)	Security design in the development environment for the target system, such as weight reduction for PIP, transparency guarantee, and application of safety-proven protocols according to the characteristics of IoT devices & services	[14,16, 20]
	Prevention from unnecessary data retention of IoT devices & services (PDR)	Control unnecessary data storage(CUDS)	Security design based on the security requirements of IoT system middleware, SCADA system, and business information system	[19,21]
		Remove or stop tagging function(RSTF)	Enhancement of functions such as mutual authentication network services, encrypted data transmission & integrity verification, network address filtering considering area control measures of embedded HW executable code	[20]
	Secure disposal management of IoT devices and services(SDM)	Removal of SW in accordance with safe disposal procedures (RSWD)	Platform protection such as secure update, integrity verification of set value and executive code, confirmation of authorized user before performing update, use of the latest security patch applied version when using 3rd party library, etc.	[13,15, 18]
		Observance of disposal procedure for Encryption key, password, etc.(ODPE)	Perform programming of developer and check secure coding itself through unit tests according to the secure coding rules established in the requirements definition phase	[16]

* () is an abbreviation.

다음으로, IoT개인정보처리과정에서의 개인정보보호를 구성하는 요소를 살펴보면, 첫째, IoT서비스의 개인정보 수집 및 보유단계는 IoT서비스의 개인정보 수집 동의, IoT서비스의 개인정보 수집 제한, IoT서비스의 개인정보의 수집대응으로 3개 분야를 구성했다. 이에 대해 IoT서비스의 개인정보 수집 동의분야는 서비스별 이해하기 쉬운 일괄된 동의 기준 마련과 개인정보의 포괄적 사전 동의 및 사후 통제로 지표화했다. IoT서비스의 개인정보 수집 제한분야는 최소한의 개인정보 수집제한 및 적합성 제고와 민감정보 및 고유식별정

보의 처리 제한으로 지표를 구성했다. IoT서비스의 개인정보의 수집대응분야는 간접 수집한 정보주체의 권리 보호와 수집정보의 비식별 조치 적용으로 지표를 구성했다.

둘째, IoT서비스의 개인정보 이용 및 제공단계는 IoT서비스의 목적 외 이용 및 제공시 보호조치, IoT서비스의 제3자 제공 및 업무위탁시 보호조치, IoT서비스의 개인정보 이전시 보호조치로 구분하여 각 분야별 2개 지표로 구성했다. IoT서비스의 목적 외 이용 및 제공시 보호조치분야는 정보주체에게 고지·동의 등 별도 절차 수립 및 이행과 개인정보 이용 제한 및 이용시 보호조치로 지표를 구성했다. IoT서비스의 제3자 제공 및 업무위탁시 보호조치분야는 개인정보 제3자 제공시 안전조치와 업무 위탁시 정보주체 고지 및 관리감독 이행으로 지표화했다. IoT서비스의 개인정보 이전시 보호조치분야의 지표는 개인정보의 이전(영업의 양수 등)시 보호조치와 개인정보의 국외이전시 보호조치로 구성했다.

셋째, 파기단계는 IoT서비스의 개인정보 파기시 보호조치, IoT서비스의 미사용 개인정보의 계정관리 및 파기, IoT서비스의 처리목적 달성 후 분리보관으로 3개 분야를 선정하고 하위 2개 지표를 구성했다. 구체적으로, IoT서비스의 개인정보 파기시 보호조치분야는 개인정보 파기 시 보호조치와 제3자 제공된 개인정보 파기관리제도 강화로 지표를 구성했다. IoT서비스의 미사용 개인정보의 계정관리 및 파기분야는 미사용 이용자의 휴면계정 관리와 개인정보의 업데이트 및 파기 절차 운영으로 지표화했다. IoT서비스의 처리목적 달성 후 분리보관분야는 파기대상 및 예외대상의 일정조치 적용과 처리목적 달성 후 개인정보 분리 보관으로 지표를 구성했다. 이렇게 구성한 IoT개인정보처리과정에서의 개인정보보호는 3개 단계, 9개 분야, 18개 지표로 구성했으며, 그에 대한 조작적 정의와 출처를 Table 6과 같이 정리했다.

Table 6. The Composition factors for Personal Information Protection in IoT Personal Information Processing

Stage (Abbr)	Field(Abbr)	Indicator(Abbr)	Operational definition	Source
Collection & Retention Stage of PI in IoT service (CR)	Consent to collect PI in IoT service (CCP)	Establishment of collection consent standards to easily understand for each service(ECCS)	Preparation of consistent standards to easily understand to collect and use PI for each IoT service when it is difficult to obtain consent from data subjects and exercise the right of actual consent to collect PI	[22,9]
		Comprehensive prior consent and follow-up control of PI(PCFC)	Establishment of opt out procedure for information sharing and 3rd party's providing as well as op-in procedure for prior consents according to the collection and modification of PI in IoT service	[16,22]
	limit to collect PI in IoT service (LCP)	Llimits collecting and enhancements of suitability for minimum PI (LCES)	Provision of technical & administrative protection measures in service provision such as establishing a policy to collect and use minimum PI, minimizing the use of combined information according to legal basis, controlling collection and distribution of identifiable PI, separating essential and optional contents, etc.	[16, 22,23]
		Limits processing of sensitive information and unique identification information(LSSI)	Processing restriction such as compliance with legal basis for sensitive PI and unique identification PI, processing procedure to obtain consents of data subject, providing alternative means of resident registration number, etc.	[22]
	Response to collect PI in IoT service (RCP)	Protection of data subject rights for indirect collection of PI(PDSR)	Collection & use only minimum PI for necessary work according to collect and use PI provided from outside the information subject and notification of the right to collect source, process purpose, process suspension, etc. based on legislation or requirement of data subjects	[22]
		Application of non-identification measures of collected PI (ANIM)	Application of privacy protection and anonymity technologies by complying with regulation to select non- identification measures and for PI and applying adequate privacy protection functions, etc.	[16,20]
Use & Provision stage of PI in IoT service (UP)	Protection measures when using and providing PI for purposes other than IoT service (PMO)	Establishment and implementation of eparate procedure such as notification, consent, etc. to information subjects(EISP)	Establishment & implementation of appropriate protection measures according to collect and use within the scope based on the collection purpose or law of PI other than those provided by 3rd parties, and separately agreed.	[22,24]
		limits to use PI and protection measures when using it(LUPM)	Activation of alerts and notification function for event related with PIP such as displaying restriction of PI, minimizing items of PI, detecting and unidentifying PI that is not necessary to work in order to prevent excessive use in PI processing	[22]
	Protection measures when providing PI for 3rd parties and consigning business in IoT service (PMP)	Safety measures when providing PI to 3rd parties (SMPP)	Establishment and implementation of safety measures such as obtaining consent or legal basis to provide PI to 3rd parties and encrypting PI in processing of providing personal information to a third party, etc.	[22,26]
		Notification for information subject and mplementation of management & supervision for consigning business(NIMS)	Notification for information subject to related matters such as entrusted work and trustee and Implementation of training and management supervision for consigning business when entrusting PI processing to 3rd parties	[22,26]
	Protection measures when transfering PI in IoT service (PMT)	Protection measures to transfer PI(PMTP)	Establishment and process of appropriate protection measure such as notifying information subject due to the transfer or merger PI of business	[22]
		Protection measures to transfer PI overseas (PMTO)	Establishment and implementation of appropriate protection measures such as consent to overseas transfers and disclosure of related matters when PI is transferred overseas	[22]

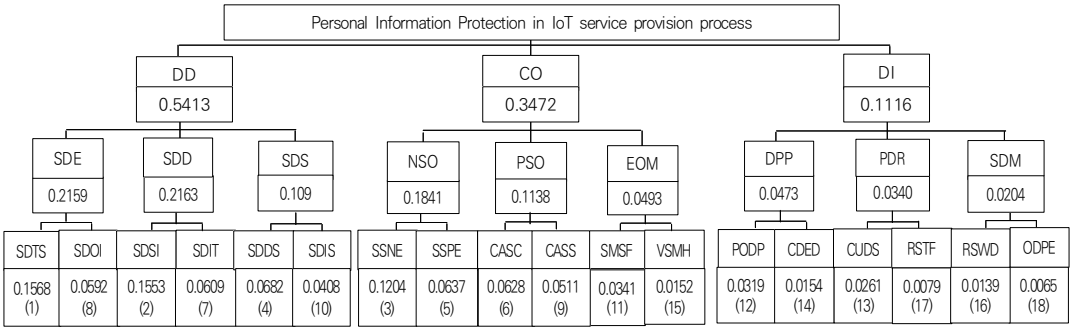
Destruction Stage of PI in IoT service (DP)	Protection measures when deducting personal information of IoT service (PMD)	Protection measures when deducting personal information(PMDP)	Destruction without delay in a way that ensures the safety and completeness of destruction when the personal information is reached, by establishing an internal plan related to the retention period and destruction of PI	[22]
		Strengthening the PI destruction management system provided by 3rd parties (SDMS)	Specification of specific retention period and destruction plan of PI when signing a contract for provision of personal information to a third party, and destruction of PI such as requiring destruction of personal information such as penalty, compensation for damages	[2]
	Account management & destruction of unused PI of IoT service (AMD)	Dormant account management of unused users(DAMU)	Adequate protection measures such as notification of related matters, destruction of personal information, or separate storage, etc. for dormant user's PIP	[22]
		Operation of updating and deducting PI(OUDP)	Establishment of destruction procedures and prevention of unnecessary collection of collected PI such as up-to-date and limited collection, combined information, and non-identification information	Delphi's result
	Separate storage after achieving the processing purpose of IoT service(SSA)	Application of certain measures to the targets for destruction and exceptions(ACMT)	Preparation of the destruction plan for PI based on certain measures considering the adequacy of destruction rather than unconditional destruction due to the termination of the IoT service	[9]
		Separation and storage of PI after achievement of processing purpose (SSPI)	Establishment and implementation a storage and management plan by limiting it to the minimum required for the purpose and separating it from other PI, when is retained PI according to relevant laws after passing the retention period and achieving the process purpose of PI	[22,25, 26]

* () is an abbreviation.

4.2 우선순위 분석결과

4.2.1 IoT서비스제공과정에서의 개인정보보호 중요도 산정결과

본 연구에서 IoT서비스제공과정에서의 개인정보보호 준수사항을 단계, 분야, 지표로 구성하여 전문가대상으로 AHP기법을 적용한 쌍대비교방식의 설문조사를 했다. 이렇게 조사한 결과는 1을 기준으로 하위 구성요소별 상대적 가중치를 세분화했다. 이에 따라 IoT서비스제공과정을 구성하는 단계의 중요도는 IoT 제품 및 서비스의 설계·개발(0.5413), IoT 제품 및 서비스의 구축·운영(0.3472), IoT 제품 및 서비스의 폐기(0.1118) 순으로 중요하다고 보았다. 분야별로 보면, 첫째, IoT 제품 및 서비스의 설계 및 개발단계의 준수사항에 대한 분야별 중요도는 IoT 제품 및 서비스의 데이터 보안 설계(0.2163), IoT 제품 및 서비스의 개발환경 보안 설계(0.2159), IoT 제품 및 서비스의 기기 및 시스템 보안 설계(0.1090) 순으로 응답했다. 둘째, IoT 제품 및 서비스의 구축 및 운영단계는 IoT 제품 및 서비스의 네트워크 보안 운영(0.1841), IoT 제품 및 서비스의 프로그램 보안 운영(0.1138), IoT 제품 및 서비스의 보안대책 수립 및 운영(0.0493) 순으로 중요한 분야로 보았다. 셋째, IoT 제품 및 서비스의 폐기단계는 IoT 제품 및 서비스의 폐기절차 및 계획 수립(0.0473), IoT 제품 및 서비스의 불필요한 자료 보유 방지(0.0340), IoT 제품 및 서비스의 안전한 폐기 관리(0.0204) 순으로 중요하다. 그 외에 세부지표별로 쌍대비교한 결과에 대해 전체 순위를 비교한 결과, IoT서비스 제품 및 서비스 설계·개발단계에서 IoT 제품 및 서비스의 개발환경 보안 설계 분야 중 목표시스템의 보안 설계가 가장 중요하다고 보았다. 이를 위해서는 '설계에 의한 보안(Security by Design)' 및 '설계에 의한 개인정보보호(Privacy by Design)' 원칙을 준수하여 서비스의 보안 설계, 안전한 파라미터 설정 등이 이루어져야 한다. 이와 같이, IoT서비스제공과정에서의 개인정보보호의 중요도 및 우선순위는 Fig. 3과 같이 정리할 수 있다.



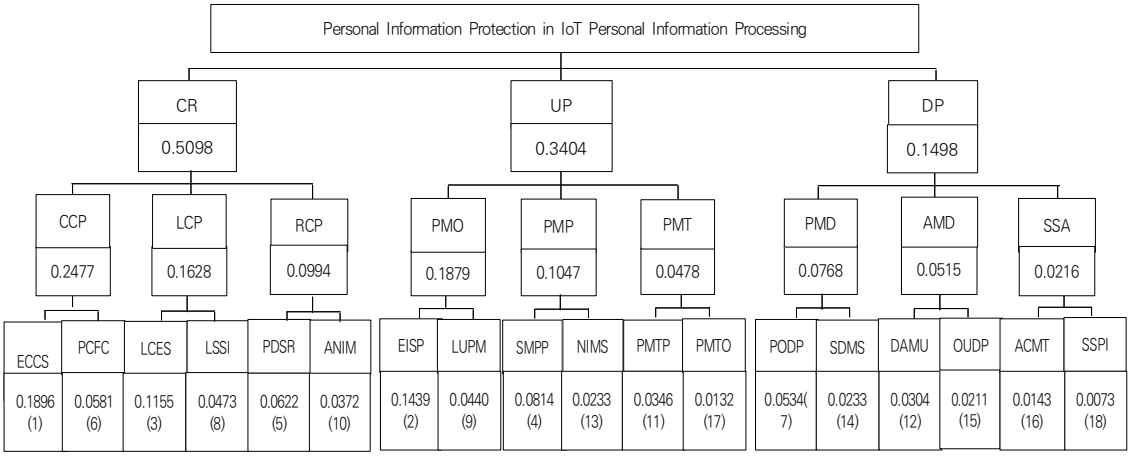
* Refer to Table 5 for abbreviations.
** () is the ranking of all indicators.

Fig. 3. Priority of Personal Information Protection in IoT service provision process

4.2.2 IoT개인정보처리과정에서의 개인정보보호 중요도 산정 결과

다음으로, IoT개인정보처리과정에서 개인정보보호 프레임워크를 구성하는 요소들을 단계, 분야, 지표별로 쌍대비교했는데, 1을 기준으로 하위 구성요소별 상대적 가중치를 세분화했다. 단계 중에서는 IoT서비스의 개인정보 수집 및 보유단계(0.5098), IoT서비스의 개인정보 이용·제공단계(0.3404), IoT서비스의 개인정보 파기단계(0.1488) 순으로 중요했다.

구체적으로 살펴보면, 첫째, IoT서비스의 개인정보 수집 및 보유단계를 구성하는 분야를 비교했는데, IoT서비스의 개인정보 수집 동의(0.2477), IoT서비스의 개인정보 수집 제한(0.1628), IoT서비스의 개인정보의 수집대응(0.0994) 순으로 중요했다. 둘째, IoT서비스의 개인정보 이용 및 제공단계는 IoT서비스의 목적 외 이용 및 제공시 보호조치(0.1879), IoT서비스의 제3자 제공 및 업무위탁시 보호조치(0.1047), IoT서비스의 개인정보 이전시 보호조치(0.0478) 순으로 중요하다고 보았다. 셋째, IoT서비스의 개인정보 파기단계는 IoT서비스의 개인정보 파기시 보호조치(0.0768), IoT서비스의 미사용 개인정보의 계정관리 및 파기(0.0515), IoT서비스의 처리목적 달성 후 분리보관(0.0218) 순으로 중요하다고 보았다. 이에 대해서 각 단계의 분야별 지표에 대해서도 중요도를 분석하였는데, 개인정보 수집 및 보유단계 중 IoT서비스의 개인정보 수집동의 분야 중에서 서비스별 이해하기 쉬운 일괄된 동의기준 마련이 가장 중요하다고 보았다. 이처럼 개인정보 처리과정에서의 개인정보보호 준수사항을 우선하여 실행해야 한다. 이처럼 IoT개인정보처리과정에서을 구성하는 단계, 분야, 지표간의 중요도 및 우선순위를 분석한 결과는 Fig. 4와 같다.



* Refer to Table 6 for abbreviations.
** () is the ranking of all indicators.

Fig. 4. Personal Information Protection in IoT Personal Information Processing

4.3 우선순위 분석결과 검증

4.3.1 타당성 검증

본 연구에서 IoT서비스제공자가 준수해야 할 개인정보보호 프레임워크를 선정하여 전문가 대상으로 중요도에 관한 조사를 했다. 비록 AHP기법을 이용한 응답결과를 활용하였으나, 응답율에 따른 타당성을 검증하기 위해 SPSS프로그램, SmartPLS 등의 통계프로그램을 활용했다. Table 7은 SPSS를 이용한 일표본 통계량 및 일표본 검정(검정값=0.05)으로 타당성을 검증했다. 그 결과, 일표본 통계량 및 일표본 검정에 따른 설문응답 및 Pearson상관관계는 $p<0.01$로 유의미했다. 또한, 각 비교요소간의 상관관계에서는 음(-)의 상관성이 있다.

또한, SmartPLS를 이용하여 과정별 단계와의 경로분석을 한 결과를 Fig. 5와 같이 알 수 있다.

이처럼 IoT서비스제공과정에서는 R Square=0.984, 수정결정계수=0.983이었고, IoT개인정보처리과정에서는 R Square=0.995, 수정결정계수=0.994로 타당했다.

Table 7. One-sample statistics and one-sample test

Div.		One-sample Statistics				One-sample Test					
		N	Mean	StDev	Se Mean	t	degree of freedom	significance probability	mean difference	95% Confidence Interval	
		82	0.4449	0.17464	0.01929					lower	upper
IoT service provision process	DD	82	0.3282	0.11367	0.01255	20.479	81	0.000	0.39495	0.3566	0.4333
	CO	82	0.2268	0.15344	0.01694	22.164	81	0.000	0.27821	0.2532	0.3032
	DI	82	0.3463	0.23007	0.02541	10.437	81	0.000	0.17685	0.1431	0.2106
Personal Information Processing	CR	82	0.3523	0.15861	0.01752	11.662	81	0.000	0.29630	0.2457	0.3468
	UP	82	0.3014	0.17241	0.01904	17.259	81	0.000	0.30230	0.2674	0.3371
	DP					13.204	81	0.000	0.25141	0.2135	0.2893

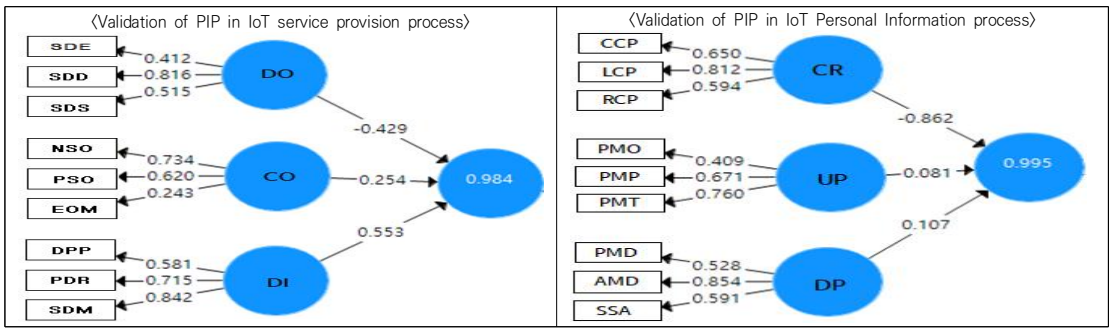


Fig. 5. Validation through route analysis

4.3.2 신뢰성 검증

본 연구는 IoT서비스제공자가 준수해야할 개인정보보호 프레임워크를 구성하여, 중요도 및 우선순위를 분석했다. 본 연구에서 전문가대상으로 AHP기법을 적용한 설문결과의 신뢰성은 일관성 지수(Consistency Index: CI) 및 일관성 정도(Consistency Ratio: CR)로 검증했다. CI의 산정공식은 CI=(λ-N)/(N-1)이며, CR=CI/RI이며,[1] CI〈0.1, CR〈0.1인 경우 신뢰할 수 있다고 본다.

먼저, IoT서비스제공과정에서의 개인정보보호를 살펴보면, IoT 제품 및 서비스의 설계·개발, IoT 제품 및 서비스의 구축·운영, IoT 제품 및 서비스의 폐기에 관한 중요도에 대한 응답결과는 CI=0.0413(CI〈0.1), CR=0.0794(CR〈0.1)로 신뢰할 수 있었다. 이에 대해 IoT 제품 및 서비스의 설계 및 개발단계의 각 분야에 대한 중요도에 관해서는 CI=0.0088(CI〈0.1), CR=0.0.169(CI〈0.1)이었으며, IoT 제품 및 서비스의 구축·운영단계의 각 분야에 대한 중요도에 대해서는 CI=0.0442(CI〈0.1), CR=0.762(CI〈0.1)이고, IoT 제품 및 서비스의 폐기단계의 각 분야에 대한 중요도에 대해서는 CI=0.0285(CI〈0.1), CR=0.0548(CI〈0.1)로 신뢰할 수 있었다. 그 외 지표 간의 쌍대비교는 2개 요소 간의 비교이므로, 모두 CI=0.0, CRI=0.0으로 완전히 신뢰할 수 있었다.

다음으로, IoT개인정보처리과정에서의 개인정보보호는 IoT서비스의 개인정보 수집 및 보유단계, IoT서비스의 개인정보 이용 및 제공단계, IoT서비스의 개인정보 파기단계에 대한 중요도를 쌍대비교하였는데, CI=0.0573(CI〈0.1), CR=0.0988(CR〈0.1)로 신뢰성이 높았다. IoT서비스의 개인정보 수집 및 보유단계의 각 분야를 대상으로 쌍대비교한 결과의 신뢰성은 CI=0.0248(CR〈0.1), CR=0.0428(CR〈0.1)이었고, IoT서비스의 개인정보 이용 및 제공단계의 각 분야에 대한 중요도분석결과는 CI=0.0345(CI〈0.1), CR=0.0595(CR〈0.1)이었다. 또한, IoT서비스의 개인정보 파기단계의 각분야에 대한 중요도 분석결과에서는 CI=0.0434(CI〈0.1), CR=0.0748(CR〈0.1)으로 신뢰성을 확보할 수 있다. 이를 구성하는 분야의 각 하위지표 간의 신뢰성은 CI=0.0, CRI=0.0으로 검증했다. 이처럼 각 과정별 3개 단계와 9개 분야의 CI/CR값을 통한 신뢰성 검증결과는 Table 8과 같다.

1) Table 9. Random Index[27]

Matrix	1	2	3	4	5
R.I.	0	0	0.52	0.89	1.11

Table 8. Reliability verification of the survey results

Div.	stage	CI/CR	Field	CI/CR
IoT service provision process	DD	CI=0.0413 CR=0.0794	SDE	CI=0.0088 CR=0.0169
			SDD	
			SDS	
	CO		NSO	CI=0.0442 CR=0.0762
			PSO	
			EOM	
	DI		DPP	CI=0.0285 CR=0.0548
			PDR	
			SDM	
Personal Information Processing	CR	CI=0.0573 CR=0.0988	CCP	CI=0.0248 CR=0.0428
			LCP	
			RCP	
	UP		PMO	CI=0.0345 CR=0.0595
			PMP	
			PMT	
	DP		PMD	CI=0.0434 CR=0.0748
			AMD	
			SSA	

4.4 연구의 한계

본 연구에서는 IoT서비스제공자가 준수해야 할 개인정보보호 프레임워크를 IoT서비스제공과정 및 IoT 개인처리과정으로 구분하여 각 단계별 준수해야 할 사항을 3개 분야 및 각 분야별 2개 지표로 구성했다. 이에 대해 개인정보보호 프레임워크 구성요소의 적합성을 확보하기 위해 전문가대상의 AHP기법을 활용한 설문조사를 했고, 각 구성요소의 중요도 및 우선순위를 분석했다.

그러나, 본 연구를 수행하는데, 몇 가지 연구의 한계가 있었다. 첫째, 개인정보보호 프레임워크의 구성요소들은 기존 문헌자료를 바탕으로 도출하였기 때문에, 신기술인 IoT를 도입하여 발생할 수 있는 모든 요인을 차단하는데 한계가 있었다. 둘째, IoT서비스제공자가 개인정보보호를 위해 반드시 준수해야 할 사항을 전문가 의견을 반영하였기에 일반적인 준수사항을 포괄하지 못했다. 그럼에도 불구하고, IoT서비스제공자가 개인정보보호를 위해 준수해야 할 사항을 기술적 측면뿐만 아니라, 종합적인 관점에서 접근하고 운영상의 안정성을 높일 수 있는 기준으로 활용할 수 있으리라 본다.

5. 결론 : 시사점

본 연구에서는 IoT서비스제공자가 준수해야 할 개인정보보호 프레임워크를 IoT서비스제공과정 및 IoT 개인처리과정으로 구분하여 각 단계별로 준수해야 할 사항을 제안했다. 이를 위해서 기존 연구를 비롯한 문헌자료를 검토하여 1차 기준요소들을 도출하였고, 전문가대상의 FGI 및 Delphi를 통한 세부적인 단계, 분야, 지표들을 범주화했다. 이에 따라 2개 과정별 3개 단계, 9개 분야, 18개 지표에 대한 중요도를 조사하였는데, 2020년 2월 14일부터 28일동안 전자설문조사를 하였고, 이를 활용하여 개인정보보호 프레임워크의 중요도 및 우선순위를 분석하였으며, 그 결과의 타당성 및 신뢰성을 검증했다.

이에 대해 IoT서비스제공과정에서의 개인정보보호를 위해서는 3개 단계 중에서 IoT 제품 및 서비스의 설계 및 개발단계(0.5413)가 가장 중요하며, 이를 구성하는 분야에서는 IoT 제품 및 서비스의 개발환경 보안 설계 분야(0.2159)가 중요하고, 지표들 중에서는 IoT서비스목표시스템의 보안 설계(0.1568)이 가장 중요한 준수사항이었다.

또한, IoT개인정보처리과정에서의 개인정보보호를 위해서는 IoT서비스의 개인정보 수집 및 보유단계(0.5098)가 가장 중요하며, 이를 구성하는 분야 중에서는 IoT서비스의 개인정보 수집 동의(0.2477)분야가 가장 중요하다. 또한, 이를 구성하는 지표들 중에서 서비스별 이해하기 쉬운 일괄된 개인정보보호기준을 마련하는 것(0.1896) 가장 중요한 준수사항이었다.

이렇게 IoT서비스제공자가 준수해야할 개인정보보호프레임워크에 대한 응답결과는 t검정($p<0.01$)을 통해 유의미함을 검증하였고, 상호 지표간의 R Square 및 수정결정계수에서 높은 결과를 통해 타당성을 검증할 수 있었다. 또한, 쌍대비교한 응답결과를 각 과정을 구성하는 단계, 분야, 지표에 대한 신뢰성도 CI/CR<0.1로 검증할 수 있었다.

이처럼 본 연구는 IoT서비스제공자가 IoT 제품 및 서비스를 위해 기술적 보호조치에 치중하고 있는 현실에서, IoT서비스제공과정 및 IoT개인정보처리과정을 연계하여 개인정보보호를 강화할 수 있는 실천기준을 제시했다. 본 연구는 문헌조사, 전문가대상의 FGI 및 Delphi조사를 통해 반드시 준수해야 할 사항을 도출했으며, IoT서비스제공자를 위한 개인정보보호 프레임워크로 제안했다. 또한, 본 연구에서는 전문가들을 대상으로 AHP기법을 활용한 개인정보보호 프레임워크의 구성요소들에 대해 중요도 및 우선순위를 분석했다. 이처럼 전문가입장에서 안전한 IoT환경을 구현하기 위해 개인정보보호의 필요성을 강조했으며, AHP기법을 통

해 전문가 검증을 거친 개인정보보호 프레임워크이므로, IoT서비스제공자가 준수해야 할 기준으로 활용성을 높일 수 있다. 이처럼 본 연구는 IoT서비스제공자가 신기술을 도입하면서 발생할 수 있는 침해요인을 차단하여 IoT서비스주체를 보호대책을 마련해 나갈 수 있는 개인정보보호 프레임워크로 활용하리라 본다. 또한, 본 연구의 성과는 IoT서비스가 확대됨에 따라 IoT서비스주체를 위한 적극적인 보호대책을 마련하도록, IoT서비스제공자의 개인정보보호를 위한 투자와 노력을 이끄는 기준이 될 것이다. 더욱이, 본 연구의 성과를 바탕으로, 향후 수요자인 이용자가 요구하는 개인정보보호관리체계 및 대책을 마련하는 후속 연구가 진행된다면, IoT 및 개인정보보호 분야를 이해관계자별로 차별화된 대책을 수집하는 연구성과로 활용되리라 본다.

REFERENCES

[1] McKinsey. (2015). *THE INTERNET OF THINGS: MAPPING THE VALUE BEYOND THE HYPE.* www.mckinsey.com/mgi

[2] A. R. Lee. S. M. Son, H. J. Kim & B. S. Kim. (2016. 8). Improving Personal Data Protection in IoT Environments. *Journal of the Korea Institute of Information Security & Cryptology, 26(4),* 995-1012.
DOI : 10.13089/JKIISC.2016.26.4.995

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

[5] D. J. Choi. (2019. 9. 18). Net generation IoTsecurity in 5G era. *Weekly Technology Trend* Institute of Information & Communications Technology Planning & Evaluation.

[6] Y. R. Lee & J. S. Kim. (2014). "Persona information protection framework in IoT environment." *2014 SpringSpring Conference Proceeding,* The Korea Contents Association 277-278.9

[7] Y. R. Lee, S. M. Kang, S. K. Seo & H. S. Lim. (2016). A study on information security framework according to the introduction of defense IoT. *Defense technology, 448,* 98-107.

[8] S. H. Park & J. G. Park (2014. 10). A7ctivation plan with analysis on technology and market of IoT, *2014 Fall academic conference,* Korea Technology Innovation Society, 85-91.

[9] S. P. Hong, H. M. Jang, K. J. Kim, H. R. Kim & S. M. Park. (2015). *Research on personal information protection issues and policy suggestions in IoT environment.* KISA.

[10] N. J. Park et al. (2016). A *Research on IoT production security certification and security maintenance promotion.* KISA.

[11] J. S. Lee. (2009). *Public Administration Dictionary.* DYM Book.

[12] T. L. Saaty. (1980). *The analytic hierarchy process: planning, priorisetting, resource allocation.* New York. McGraw-Hill International Book Company.

[13] N. H. Kang. (2015). IoT convergence service security requirements. *The Journal of The Korean Institute of Communication Sciences, 32(12),* 45-50.

[14] Korea Internet & Security Agency. (2019). *Internet of Things (IoT) Security Test and Certification Standards Commentary..* KISA.

[15] Ministry of Science and ICT & Korea Internet & Security Agency. (2018). *Information protection pre-inspection guide.* Ministry of Science and ICT & KISA.

[16] IoT security alliance. (2016). *IoT Common Security Guidelines.* IoT security alliance.

[17] Korea Internet & Security Agency. (2007). *RFID Personal Information Protection Guidelines.* Korea Internet & Security Agency.

[18] H. K. Kong, H. K. Gu, H. W. Cho & J. S. Kang. (2015). *Research on based security certification of IoT device.* KISA.

[19] S. Li & L. Da Xu. (2017). *Securing the internet of things.* Acorn publishing Co.

[20] Finance Security Institute. (2016. 12. 12). IoT security threats and accidents. *IoT Common Security Guide.*

[21] Y. S. Jeong. (2017). Data Storage and Security Model for Mobile Healthcare Service based on IoT. *Journal of Digital Convergence, 15(3),* 187-193.
DOI : 10.14400/JDC2017.15.3.187

[22] Ministry of Science and Technology Information and Communication, Ministry of Public Administration and Security·Korea, Korea Communications Commission, & Korea Internet & Security Agency. (2019). *Information protection and personal information protection management system certification system guide.*

[23] Ministry of Public Administration and Security & Korea Internet & Security Agency. (2017). *Personal information protection level diagnosis manual.* MOPAS & KISA.

[24] ISO. (2013). ISO/IEC 27001:2013(en): Information technology — Security techniques — Information security management systems — Requirements. https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

[25] Ministry of Public Administration and Security & Korea Internet & Security Agency. (2018). *Personal Information Impact Assessment Guide*..MOPAS & KISA.

[26] Ministry of Public Administration and Security & Korea Internet & Security Agency. (2019). *2019 Personal information protection level diagnosis manual. in public agencies*..MOPAS & KISA.

[27] S. H. Choi. DRESS is a software for AHP. http://blog.daum.net/_blog/BlogTypeView.do?blogid=0FE2P&articleno=11045124&_bloghome_menu=recenttext

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 국제정보정책 전자정부연구소 선임연구원
· 2004년 10월 ~ 2012년 7월 : 행정안전부 정보화전략실 전문위원
· 2012년 8월 ~ 2013년 2월 : 고려대학교 정보보호대학원 연구교수
· 2013년 3월 ~ 현재 : 배재대학교 부교수
· 관심분야 : 개인정보보호, 정보보호정책, 전자정부, 4차 산업혁명 산기술
· E-Mail : jinsyj@yahoo.com