연구논문 정보화정책 제25권 제3호, 2018년 가을호, pp. 29-51
https://doi.org/10.22693/NIAIP.2018.25.3.029

안전한 사물인터넷 서비스 확산을 위한 개인정보보호정책평가지표 개발에 관한 연구*

신 영 진**

요 약

제4차 산업혁명의 핵심기술인 사물인터넷기술의 발달로 인하여 다양한 서비스가 가능하게 되고, 그 과정에서 개인정보가 자유롭게 처리되게 되었다. 그러나 스마트기기를 비롯한 정보기기가 네트워크로 연결되면서 편리한 서비스가 제공될수록 개인정보 침해위협도 증가하고 있는 실정이다. 따라서, 본 연구는 다양한 사물인터넷서비스를 구현함에 있어서 안전한 환경을 구축하고, 그 가운데 유통되는 개인정보를 보호하기 위해 필요한 정책선정을 위한 중요도에 따른 우선순위를 분석하여 주요정책과제로 제언하고자 한다. 본 연구에서는 문헌조사를 바탕으로 개인정보보호정책지표들을 전문가대상의 델파이분석을 통해 3개 분야 9개 영역 25개 지표로 구성하였다. 이러한 개인정보보호정책지표들은 AHP기법의 설문조사로 66명 전문가들이 응답한 결과를 활용하여, 정책지표의 상대적 중요도 및 우선순위를 도출하였다. 그 결과, 개인정보보호정책분야에서는 정책적 분야, 기술적 분야, 관리적 분야 순으로 상대적 중요도 및 우선순위가 도출되었다. 또한, 정책적 분야를 구성하는 3개 영역 중에서는 IoT관련 개인정보보호법제도의 강화가 가장 중요하며, 정책지표 중에서는 IoT에서의 개인정보보호법률의 제·개정을 추진하는 것이 가장 중요하다고 응답하였다. 또한, 조사된 IoT개인정보보호정책의 분야·영역·지표에 대해 쌍대비교한 결과값은 일관성을 갖고 있었다. 이렇게 도출된 개인정보보호정책지표들은 앞으로 안전한 사물인터넷 정책을 추진하여 국가경쟁력을 이끄는데 기여하리라 본다.

주제어: 사물인터넷(IoT), 개인정보보호, 정책지표, AHP분석, 우선추진과제

A Study on Developing Policy Indicators of Personal Information Protection for Expanding Secure Internet of Things Service

Shin, Young-Jin

Abstract

As the core technology of the Fourth Industrial Revolution, the Internet of Things has been developed and has enabled various services, and personal information has been handled freely in the process. However, the infringement threat of personal information is increasing as more convenient services are provided and more information devices including smart devices are connected to the network. Therefore, this study is to analyze prioritizing personal information protection policy indicators in order to provide IoT services by constructing secure environment for implementing the Internet of things as the core technology of the 4th Industrial Revolution. This study reviewed personal information protection policy indicators based on the literature survey, and identified 3 fields, 9 areas, and 25 indicators through Delphi analysis for experts. The weights were calculated based on the AHP survey for 66 experts and the results were used to present the relative importance and priority of the policy indexes. The results of this study found the policy field was the most important, followed by the technical field, and the administrative field. Of the three areas of the policy field, strengthening the personal information protection laws related to IoT is the most important, while among the indicators, promoting and revising the personal information protection law related to IoT is the most important. Comparisons of the fields, areas, and indicators of IoT-related personal information protection policies found consistent values. The personal information protection policy indicators derived this way will contribute to the nation's competitiveness by expanding secure IoT policies in the future.

Keywords: Internet of Things (IoT), personal information protection, policy indicator, AHP analysis, priority tasks

2018년 5월 8일 접수, 2018년 5월 16일 심사, 2018년 6월 18일 게재확정

* 이 논문은 2017년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(NRF-2017S1A5A8021983).
이 논문은, 2017년 한국행정학회 동계학술대회에서 발표한 "안전한 IoT서비스 체계 구축을 위한 개인정보보호정책지표 개발에 관한 연구", 2017년 12월 EECS에서 발표한 "A Study on Privacy Protection Policy for Safe IoT Service", 2018년 3월 APICENS에서 "A Study on Development of E-Privacy Policy Index to Supply Safe IoT Service"를 보완하여 게재하였음.
** 배재대학교 교수(jinsyj@yahoo.com)

Ⅰ. 서론

우리나라는 지능정보사회의 핵심이슈로 제4차 산업혁명을 꼽고 있으며, 미래정보화의 변화를 주도할 것이라고 기대하고 있다. 즉, 제3차 산업혁명인 정보화혁명과 다르게 제4차 산업혁명은 획기적인 패러다임의 전환을 가져올 것으로 확신하고 있다. 그 대표적인 정보기술 중 하나가 사물인터넷(Internet of Things: 이하 IoT)[1]이며, 사람과 사물과 컴퓨터를 연계하여 다양한 서비스가 구현되어진다.[2] 가트너(Gartner)사는 IoT의 경제적 부가가치가 2020년 1.9조 달러에 달할 것이라고 전망하였고(Gartner, 2013), 맥킨지(Mckinsey)사는 9개 주요 환경 분야(도시, 공장, 소매, 건강, 작업장, 물류, 가정, 사무공간, 교통)에서의 IoT활용수준이 2025년까지 연간 최소 3.9조 달러에서 최대 11.1조 달러까지 성장할 것으로 보았다(McKinsey Global Institute, 2015). 우리나라도 IoT시장규모가 2013년 2조 3,000억 원에서 2020년 17조 1,000억 원으로 증가할 것이라고 전망되고 있다(전해영, 2016).

이처럼 산업, 공공, 금융, 생활 등 다양한 분야에서 사물인터넷이 활용되며, EU, 미국, 중국, 일본 등 여러 국가에서도 사물인터넷에 관한 국가전략 및 정책을 수립하여 추진 중이다. 특히, 미국 국가정보위원회는 IoT를 2025년까지 국가경쟁력에 영향을 미칠 혁신적인 6대 현상파괴기술로 선정하였으며, Grid 2030 계획과 같은 국가정보화정책을 추진하고 있다. EU는 IoT연구협의체를 조성하여 14개 액션플랜을 제시하였고, IoT연구개발 등을 포함한 7개 국가과제를 선정하여 추진 중이다. 영국은 2025년까지 대규모 IoT발전 기금 및 예산을 투자할 계획이며, 일본도 국가신산업 창출을 위한 전략을 수립하여 운영 중이다. 우리나라의 경우도 제4차·제5차 국가정보화기본계획에 사물인터넷을 연계한 국가발전모델을 제시하여 초연결 사회를 구현하고자 한다.

그러나 사물인터넷(IoT)으로 얻을 수 있는 순기능적인 기대만을 품고 사물인터넷(IoT)정책을 추진하기에는 한계가 있다. 즉, 지금보다 더 복잡한 환경에서 발생할 수 있는 위협요소들이 증가할 것이며, 그와 함께 개인정보의 침해사고도 급증할 것이라는 우려가 높아지고 있기 때문이다. 실제로 미국에서는 리눅스 달로즈 웜으로 인해 보안 IP카메라, 셋톱박스 등 사물인터넷기기들이 감염된 사례가 있었다(이동혁·박남제, 2017). 보안업체인 프루프포인트(Proofpoint)사는 2014년 씽봇(Thingbot)에 감염된 스마트 TV, 스마트 냉장고 등 사물인터넷(IoT)연계 가전기기를 이용하여 개인 및 기업에게 75만개의 스팸메일을 발송한 사건을 보고하였다. 시만텍사(2015)는 스마트폰에 설치된 랜섬웨어 APK파일이 스마트워치와 스마트폰을 페어링 할 때 자동으로 설치되는 것을 입증하였다(장현수 외, 2015). 이외에도 시만텍사(Symantec)는 스마트홈 기기, CCTV 카메라, 경보/조명 등의 원격제어기능을 악용한 침해사례를 발표한 바 있고, 트렌드마이크로(Trend Micro)는 IoT환경의 가속화와 함께 정보유출위협의 가속화도 제기하였으며, 카스퍼스키(Kaspersky)는 IoT기기의 사용증가로 인한 보안위협도 증가할 것이라고 주장하였다. 이처럼 현재 ICT시장에 출시된 IoT기기 중 70%가 사이버 보안위협에 노출되어 있으며, IoT기기대상의 사이버공격으로 인한 피해금액도 2015년 13조4,000억 원에서 2017년 17조7,000억 원으로 증가하였다(보안뉴스, 17/12/19). 특히, 2017년에는 가정 및 업무 환경에서 사용되는

1) 본 연구에서 IoT를 위한, IoT에 관한, IoT와 연관된, 또는 IoT에 관련된 개인정보보호 및 정보보호, 그 외 IoT관련 모든 세부사항 등을 표현함에 있어서 본문, 표 및 도식 등에서 설명을 간단히 명시하고자 정리하여, IoT개인정보보호 및 정보보호, IoT세부사항 등으로 축약하여 본문에 표기하고자 한다.

2) IoT는 1999년 MIT의 Kevin Ashton이 처음 사용하였으며, 인간, 사물, 서비스 등으로 분산된 구성요소들 간의 인위적인 개입 없이 상호 협력적으로 센싱, 네트워킹, 정보 교환 및 처리 등과 같은 지능적 관계를 형성하는 사물공간연결망을 의미한다(민경식, 2013).국제전기통신연합(International Telecommunication Union: ITU)은 2005년 IoT를 '언제 어디서나 어느 것과도 연결될 수 있는 새로운 통신환경'이라고 개념을 정리하였다(박정은, 2014).

IoT기기를 악용한 대형 디도스(DDos)공격이 발생하였고, IoT기기의 입력정보, 센서 등을 도용해 위조된 음성이나 이미지를 입력하여 IoT기기를 공격자가 원하는 대로 조정한 바 있다(보안뉴스, 17/12/06).[3)]

이렇게 IoT에 관한 보안이슈사항이 제기되면서, EU, 미국, 중국, 일본 등 여러 나라에서 IoT에 관한 정보보호계획 및 개인정보보호대책이 추진되고 있다. 그러나 IoT정보보호정책 중에서 어떤 한 분야를 중심으로 하거나, IoT기기보안을 중심으로 하는 정보보호수칙을 강조하고 있는 실정이다. 또한, IoT환경에서의 신뢰성을 높이기 위해 유럽 FP7의 uTRUSTit, ABC4Trust, Inter-Trust, COMPOSE, SMARTI 등 프로젝트가 진행되었다(윤영석 외, 2016). 따라서, 본 연구에서는 앞으로 사물인터넷(IoT)서비스를 제공함에 있어서 우리나라가 실천할 수 있는 개인정보보호정책의 우선과제를 제언하고자 한다. 즉, 본 연구에서는 기존 연구주제를 바탕으로 한 문헌조사를 통해 정책요소를 도출한 후, 전문가대상의 심층면접방법(델파이분석)을 거쳐 정책지표로 선정하고자 한다. 이렇게 선정한 정책지표를 대상으로 전문가중심의 설문조사(AHP분석)를 거쳐 정책의 중요도 및 우선순위를 분석하고자 한다. 이러한 연구결과가 우리나라가 추진하는 사물인터넷(IoT)정책에서 개인정보보호정책이 갖추어야 할 우선과제로 활용되기를 기대한다.

Ⅱ. IoT개인정보보호정책에 관한 논의

1. 주요 국가의 추진 현황

주요 선진국 특히, EU, 중국, 일본 등에서는 IoT서비스를 제공함에 있어서 개인정보보호 및 정보보호정책을 추진하고 있다. 특히, 새로운 정보통신기술이 발달하면서 개인정보가 포괄적이면서 다양한 이해관계자들을 고려하는 정책이슈가 되어(방민석·오철호, 2014), 이를 대응하는 정책과제가 추진되어야 한다. 이에 자세히 살펴보면, EU는 2006년부터 IoT생태계에 발생할 수 있는 개인정보의 침해위협을 최소화를 포함한 균형적인 정보화정책을 추진하고 있다. 특히, EU의 '사물인터넷(IoT) 14개 액션플랜'을 통하여 IoT서비스를 제공함에 있어서 발생 가능한 정보위협 및 사생활 침해 대응방안을 14개의 체계적 행동계획으로 제시하였다(이야리·김정숙, 2014). 또한, 제7차 프레임워크 프로그램(Framework Programme EU)의 일환으로 '카사그라스(Coordination and Support Action for Global RFID-related Activities and Standardization: CASAGRAS) 프로젝트'를 추진하였다. 미국의 연방거래위원회는 개인정보 침해사고가 발생하였던 트렌드넷을 대상으로 향후 20년동안 외부기관에 의한 보안감사를 비롯하여 웹캠 단말기의 무단접속 및 해킹을 방지하기 위한 정보보호프로그램을 구축하여 운영하도록 하였다(한국인터넷진흥원, 2014). 중국은 2009년 원자바오 총리는 IoT를 구현하기 위한 안전한 관리규정을 마련하고자 관련된 법제 정비를 비롯하여 시스템의 기술적 안전성을 높이는 국가중심의 발전전략을 수립하였다(정보통신기술진흥센터, 2015). 우리나라는 제5차 국가정보화기본계획(2013~2017) 중에서 '인간중심의 초연결창조사회 실현'을 위한 10대 의제에 IoT정보보호를 포함하였다. 특히, 방송통신위원회는 '사물통신기반구축 기본계획'을 발표하여 IoT관련 정책 추진을 본격화하였는데(2009. 10), 4대 과제별 12대 세부과제에 정보보호체계에 관한 추진과제를 반영하였다. 미래창조과학부는 2014

3) 지난 미래창조과학부(2016)에서 실시한 정보보호실태조사결과를 살펴보면, IoT환경을 구현함에 있어서 개인정보침해사고의 발생우려가 36.8%로 높게 나타났다. 또한, 매킨지(McKinsey, 2016)사 조사한 정보유출·입정도에서 우리나라가 44위(194개국)였으며, 프라이버시 및 개인정보 침해위협이 해소되지 못한 실정이다(한국일보, 16/03/07).

4) 액션플랜의 주요내용 중 IoT개인정보보호조치사항은 먼저, 개인정보보호를 위한 모니터링-IoT에 대한 정보보호법안의 적용을 재검토하고, 위험요소를 규명하여, 사생활 침해 및 정보보호에 대한 위협을 해결하기 위한 규제적·비규제적 대응책을 마련하고자 한다.

〈표 1〉 IoT환경에서의 개인정보보호정책사례

구분	주요 국가 정보보호정책
EU	• 제7차 프레임워크 프로그램(Framework Programme EU) 중 'CASAGRAS 프로젝트' 제시함 - IoT관련 연구를 추진하고 있으며, IoT서비스 및 활용을 제공함에 있어서 발생가능한 사새활침해 및 정보유출사고에 대응하도록 구체적인 14가지 행동계획[4] 제시함 - 시장 자율규제 중심(가이드, 권고 등)의 IoT 보안정책 수립·이행 추진(2013)
미국	• 2008년 4월 국가정보위원회(National Intelligence Council: NIC)는 I2025년까지 국가경쟁력에 중요 영향을 미칠 6대 혁신 문명 기술(Disruptive Civil Technology)중 하나로 IoT를 선정하였음 • 미국의 연방거래위원회는 개인정보를 유출한 트렌드넷에 대해 이례적으로 향후 20년 동안 외부 기관 보안감사를 받고, 웹캠 단말에 대한 무단 접속 및 해킹 방지를 위해 강화된 정보보호 프로그램을 구축함
중국	• 2009년 8월 원자바오 총리는 '센서네트워크'와 '사물인터넷'의 개념과 국가중심의 발전전략을 제시함 • '감지중국센터(센서네트워크 정보센터)'를 설립하고 IOT을 국가 주요 전략으로 선정했으며, 중국 공업정보화부중심의 센서네트워크 표준화 위원회를 설립함 - 표준화 위원회의 표준화 추진 활동 중 정보보안기술 프로젝트팀도 구성함 • 발전개혁위원회는 12차 5개년 개발계획(2011~2015) 중에서 IOT를 다룸 - 중국 정부는 2011년 11월부터 광둥물련천하과학집단과 IBM 회사와 MOU를 체결하여 '사물인터넷화'를 통한 스마트도시를 건설하기로 함. - 광둥성 인민정부는 2013년 12월 '광둥성 사물인터넷 발전계획(2013~2020)'에서 보안 취약점 분석, 개인정보보호 법률 및 법규규범 개선 등을 발표함
일본	• 2000년대 초반부터 사물인터넷 관련 주요 정책을 추진하고 있음 - 'u-Japan 전략(2004)', 'i-Japan 전략(2009)', 'IPv6 기반 사물인터넷 사회 연구(2009)', 'ICT 융합에 의한 신산업 창출 전략(2011)', 'Active Japan ICT 전략(2012)' 등 • 총무성은 사물인터넷 전담워킹그룹을 구성(2009. 9)하여 사물인터넷 사회가 가져오는 기술적·제도적 요구사항 중 제도적 측면으로 사생활 및 개인정보 보호팀을 구성함 • 안전한 디지털 안심·안전 사회의 실현을 위한 'i-Japan 전략 2015'를 중심으로, 이용자를 대상으로 한 인간중심(Human Centric)의 디지털사회 구현 내용에 IoT를 포함함
한국	• 제5차 국가정보화기본계획(2013-2017) 중 '인간중심의 초연결창조사회 실현'을 위한 10대 의제를 선정함 • 미래창조과학부는 2014년 5월 '사물인터넷 기본 계획'을 마련하였고, 2014년 9월에는 안전한 사물인터넷 환경조성을 위한 '사물인터넷 정보보호 로드맵'을 수립함 • '사물인터넷기반구축 기본계획'내 개인정보보호지침을 마련함

출처: 유한종(2013), ITDaily(2014. 11. 1), 이야리·김정숙(2014). 한국인터넷진흥원(2014), 보안뉴스(2014.11. 6), KOTRA뉴스(2017. 2. 27) 재구성.

년 5월 '사물인터넷 기본계획'과 2014년 9월 '사물인터넷 정보보호 로드맵'을 수립하였다(개인정보보호위원회, 2014). 이외에도 개인정보보호정책으로 '사물인터넷기반구축 기본계획'내 개인정보보호지침을 마련하였다.

종합해 보면, 미국은 IoT기기 및 서비스를 적용함에 있어서 개인정보보호에 관한 규정을 마련하고 있으며, EU는 IoT신뢰도를 높이기 위한 가이드라인을 제정하였다. 중국은 IoT발전을 위한 10개 전문 행동계획 내에 보안의 핵심기술을 개발·보급하고자 하였으며, 일본은 국가정보화기본계획(i-Japan)에 IoT에 관한 사항뿐만 아니라 개인정보보호를 포함한 정보보호계획도 반영하여 추진하고 있다. 우리나라는 IoT정보보안 R&D(2014~2018)를 위해 1,500억원을 투자하고 있으며, 대국민서비스의 안전성을 확보하기 위한 정책들을 발굴하고 있다. 이처럼 여러 국가에서도 IoT정보보호계획을 마련하고는 있으나, 종합적인 측면에서의 개인정보보호방안은 아직 논의단계에 그치고 있다. 본 연구에서는 안전한 IoT서비스가 구현될 수 있는 개인정보보호정책지표를 개발하여 종합적인 정책과제를 제언하고, 미래 IoT환경에 국민이 체감하는 개인정보보호정책과제를 추진하는 기반을 마련하고자 한다.

2. 선행 연구 동향

본 연구에서는 IoT서비스를 구현함에 있어서 개인정보보호를 위해 우선 추진되어야 할 정책과제를 도출하기 위해 기존의 연구들을 정리하였다. 물론, 연구의 주제를 한 분야에 한정하기 보다는 전반적인 IoT에 관한 보안이슈 및 개인정보보호에 관해 논의도 이루어지고 있다. 그 대표적인 연구는 강남희 외(2015), 신영진(2015), 홍승필(2015) 등이며, IoT에 관한 개인정보보호를 위해 필요한 법제도, 정책, 기술, 관리 등에 관한 요구사항을 정책방안으로 제시하였다. 그러나 아직까지 대부분의 연구들은 특정주제를 대상으로 하므로, 종합적인 관점에서 필요한 정책과제를 제언하지 못하고 있다. 따라서 이러한 연구주제에 관해 문헌조사를 하여 다음과 같이 범주화하였다.

첫째, 정책적 분야에 관한 연구들은 IoT환경에 발생 가능한 정보위협요소들을 고려하여 개인정보보호의 주요정책과제로 제언한 바 있다. 구태언(2015), 박미사(2014), 최경진(2015) 등은 IoT서비스를 제공함에 있어서 관련된 개인정보보호 및 정보보호 법률들을 제정비하여 법적 기준을 마련하고자 하였다. 특히, 최경진(2015)은 IoT시대에 개인정보를 이용하고 보호하기 위한 법률체계를 개편하고, 그에 대한 목적을 지정하여 합리화하고, 개인정보보호의 책임성과 자율성, 다른 법령과의 관계 개선 등을 주장하였다. 이야리·김정숙(2014)은 IoT환경에서 정보주체의 민감한 개인정보를 보호하기 위해 효율적인 정보기술의 활용 및 제공이 가능하도록 개인정보보호 프레임워크를 제안하였다. 또한, 이애리 외(2016) IoT환경에서 자유롭게 수집되는 개인정보를 보호함에 있어서 발생 가능한 이슈를 분석하고, 제도적 개선방안[5]을 제시하였다.

둘째, 기술적 분야에 관한 연구들은 IoT환경에서 발생 가능한 취약점 문제를 해결하기 위해서 정보보안기술의 필요성을 제기하였다. 즉, 공회경(2015), 김호원·김동규(2012), 박지예 외(2013), Li, Shancang & Xu, Li Da(2017), 손태식(2016) 등은 IoT보안을 위한 핵심기술을 개발·적용할 수 있는 기반과 기준을 마련하고자 하였다. 그 중에서 김호원·김동규(2012)는 IoT응용서비스 중에서 스마트그리드의 보안특성을 고려하여 기본적인 보안사항과 인증·인가, 부인방지, 접근제어 등의 보안요소, IoT응용서비스의 구성요소, 인터페이스의 특성, 제반 유·무선통신의 특성·프로토콜 등을 고려한 보안기술이 필요하다고 제기하였다. 또한, 강남희(2014), 김범수(2014), A Jara, Antonio. J. et al.(2013) Wang, Xiniel, et al.(2014), Su, Jinshu, et al.(2014) 등은 IoT를 위해 인증기술을 적용하여 개인식별 및 인증이 필요하므로, 접근통제 및 접근제어를 통해 안전성을 높이고자 하였다. 특히, 강남희(2014)는 IoT환경에서 고려해야 하는 보안취약점들을 정리하여 대응할 수 있는 표준기술을 제시하였다. 물론, IoT서비스를 제공하기 위한 개인정보처리시스템의 설계부터 운영까지 전반적으로 취약점을 점검하여 보안모듈을 설치하는 등의 보안기술을 강화하여야 한다.

셋째, 관리적 분야에 관한 연구들은 IoT서비스를 제공함에 있어서 개인정보처리과정에서의 침해사고를 방지하고 안전한 운영을 위한 관리기준을 제언하였다. 이와 관련하여 나성현(2015), 심우민(2015), 이애리 외(2016), FORMERFTC Conference Center (2013), Kang, Kai, et al.(2013) 등은 개인정보의 수집부터 파기까지 처리과정에서 정보주체의 동의를 획득하고 개인정보의 추적 및 식별화를 방지해야 한다고 보았다. 또한, IoT서비스를 제공함에 있어서 발생가능한 개인정보 침해사고를 사전에 예방하고 신속히 대응하기 위해서 김범수(2014), 심민식(2014), 이동혁·박남제(2017), 한국인터넷진흥원(2010), Ukil, Arijit,

5) IoT환경에서의 개인정보보호 제도적 개선방안으로 사용자 친화적 고지방안 및 탄력적 동의제도 마련, 개인정보의 재식별 및 위험 모니터링에 관한 체계 정립, 국외이전 개인정보보호 표준계약제도 수립, 이용자 교육 강화 등을 제시하였다.

et al.(2014) 등은 개인정보처리과정에서의 책임여부를 설정하여 보안취약점에 관한 대책 및 사고조치 및 복구체계를 운영해야 한다고 보았다. 그 중에서 이동혁·박남제(2017)는 안전한 IoT시스템을 개발하여 취약점을 해소하기 위해서 정보보호시스템의 평가 및 보안요구사항을 충족시켜야 하며, 정책적 보안관리 프레임워크를 준수해야 한다고 주장하였다. 이외에도 강남희 외(2015), 신영진(2016), 이애리 외(2016), 이동혁·박남제(2017) 등은 IoT기기 및 서비스에 관한 보안기준을 강화하여 서비스제품의 인증 및 자율점검, 보안패치의 배포 및 사후관리 등으로 IoT인프라 보다 IoT기기 및 서비스에 대한 정보보안을 높이고자 하였다.

그러나 본 연구의 주제인 개인정보보호정책지표를 도출하기에는 그동안 연구들이 추상적이거나 종합적인 접근으로 이루어지지 못하였다. 따라서 본 연구에서 안전한 IoT를 위한 개인정보보호정책지표들을 구성하여 그에 대한 중요도 및 우선순위를 분석하기 위하여 설문조사에 근거한 전문가들의 의견을 통합한 정책과제를 제언해 보고자 한다.

3. 정책지표의 구성요소

국내외적으로 IoT서비스를 제공함에 있어서 개인정보처리과정이 안전하게 보호받을 수 있도록 관련된 가이드라인 및 원칙을 제시하고 있다. 한국인터넷진흥원(2016)은 IoT제품 및 서비스에서의 개인정보를 처리하는 전 과정에서 보안기술 및 보안서비스를 제공하고, 사용자인증부터 보안취약점을 해소하기 위한 공통 보안원칙과 가이드를 제시하였다. OWASP(2014)는 IoT로 인한 취약점에 관하여 10가지 보안원칙을 발표하였으며,[6] IPC는 'Privacy by Design(개인정보보호 적용설계)'에 근거하여 기본적인 7가지 원칙[7]을 제시하였다. 이외에도 IoT보안 얼라이언스(국내 IoT보안 협의체)는 IoT서비스를 제공함에 있어서 개인정보의 생명주기별 보안위협과 취약성을 점검할 수 있는 IoT 공통보안원칙을 제시하였다. 정현미 외(2017)는 IoT기기(데이터 수집·전송, 센싱 및 액츄에이팅, 일반 등 기기)의 등급을 4단계로 구분하여 보안요구사항 및 공통적용사항을 제시하였다. 이처럼 IoT기기 및 서비스에 관한 보안사항을 적용하도록 제안하고 있지만, 법·제도적인 강제성이 없다는 한계가 있다. 물론, 2015년 사물인터넷에 관한 단일 법제화를 위해 공청회가 개최되었으나, 아직까지 기존의 법률에 근거를 두고 있는 상황이다(이동혁·박남제, 2017). 더욱이, IoT제품에 관한 사전기준도 부재하여 IoT제품 출시이후 발견되는 문제점을 해결하는데 한계가 있고, 「제품안전기본법」에 의한 리콜을 이행하기에도 한계가 있기 때문에 사전기준과 사후관리를 강화해야 한다.

또한, 그동안의 연구들은 IoT에 관한 보안원칙, 보안대책 등은 기술적 보호조치에 중점을 두는 경우가 대부분이었다. 따라서 종합적인 관점에 IoT에 관한 논의를 확대하고자 IoT와 관련한 개인정보보호 및 정보보호에 관한 선행연구를 정리하여, 그 과정에서 공통된 주제 및 연구분야를 정책적 분야, 기술적 분야, 관리적 분야에 관한 정책요소로 도출하는데 활용하고자 하였다. 이외에도 인터넷뉴스, 보고서 등 문헌조사를 보완적으로 활용하였다. 또한, 아직 언론이나 연구주제로 다루어지지 않은 사항에 대해서는 조사된 문헌자

6) OWASP(The Open Web Application Security Project)는 오픈소스 웹 애플리케이션 보안 프로젝트이며, 10대 웹 애플리케이션의 취약점(OWASP TOP 10)을 발표하는데, ① Injection (인젝션), ② Broken Authentication and Session Management (인증 및 세션 관리 취약점), ③ Sensitive Data Exposure (민감 데이터 노출), ④ XML External Entities (XXE), ⑤ Broken Access Control (취약한 접근 제어), ⑥ Security Misconfiguration (보안 설정 오류), ⑦ Cross-Site Scripting (XSS) (크로스 사이트 스크립팅), ⑧ Insecure Deserialization(안전하지 않은 역직렬화), ⑨ Using Components with Known Vulnerabilities (알려진 취약점이 있는 컴포넌트 사용), ⑩ Insufficient Logging & Monitoring(불충분한 로깅 및 모니터링)이다.

7) IPC(Information and Privacy Commissioner)의 IoT공통보안 7가지 원칙은 ① 프라이버시 보호는 사후 대응이 아닌 사전 대비를 전제조건, ② 프라이버시보호는 서비스의 기본 설정(Default)으로 제공, ③ 제품 및 서비스의 기획 단계에서부터 프라이버시보호 고려, ④ 포괄적인 기능성 보장, ⑤ 전체 수명주기 보호, ⑥ 가시성과 투명성 확보, ⑦ 프라이버시의 보호는 사용자를 중심으로 진행으로 정리할 수 있다.

〈표 2〉 IoT개인정보보호정책지표의 구성요소 및 조작적 정의

분야	영역	지표	지표의 세부설명 및 조작정 정의	출처/참고
정책적 분야	IoT 개인정보보호법 제도 강화	IoT개인정보보호법률 제·개정추진	• IoT개인정보보호를 위한 통합적 법제도 정비 및 특별법 제정 등 중장기적으로 추진 • 정보주체가 자기정보의 공개·유통 등에 대한 자기결정권 및 통제권을 보장하는 규정 마련 • IoT개인정보보호를 위한 책임성·자율성 강화 및 관련 규정의 자율규제를 통한 개인정보보호(비식별 조치 및 프로파일링 금지) 추진	구태언(2015), 권헌영(2015), 박미사(2014), 신영진(2016), 이민영(2012), 이애리 외(2016), 최경진(2015), FGI결과반영
		IoT개인정보보호 프레임워크 및 가이드라인 개발	• IoT개인정보보호를 위한 보안기술 적용 프레임워크 개발 • 개인정보처리자별 IoT기기 및 개인정보파일 운영 등에 대한 개인정보보호가이드라인 개발 • 개인정보취급 책임 및 절차에 관한 개인정보보호 내부관리규정 및 체계적 지침 마련	권헌영(2015), 김범수(2014), 한국인터넷진흥원(2015b), 김호영·이경현(2010), 문남미 외(2006), 신영진(2016), 이야리·김정숙(2014), 이애리외(2016), 한국인터넷진흥원(2007)
		IoT개인정보 국외이전 규정 및 제도 구축	• 국외이전시 IoT개인정보보호제도의 기준 마련과 그에 부합한 유통을 위한 제도 운영 • 국외이전시 IoT개인정보보호의무사항을 위한 상호계약을 조정하여 글로벌 IoT서비스환경에 맞는 표준계약제도의 수립·적용	한국인터넷진흥원(2015a), 김범수(2014), 이애리외(2016)
	IoT 개인정보보호추진 체계 마련	IoT개인정보보호 전담조직 설치 및 운영	• IoT개인정보보호에 관한 총괄 추진체계 설치 및 효율적인 정책추진 지원 • IoT보안대책 수립 및 사이버위협 및 침해사고 대응을 위한 종합적인 대응체제 구축	한국인터넷진흥원(2015a), 보안뉴스(2014.10.23)
		IoT개인정보보호 국내외 공조체제 구축	• IoT네트워크 연계 및 유통과정에서 발생 가능한 개인정보침해사고 대응을 위한 국내·외 공조체제 구축 및 협력 강화	김범수(2014), 신영진(2016)
		IoT개인정보보호 위한 민간자율 보호 추진체계 지원	• IoT표준화에 따른 개인정보보호, 시험인증, 국제표준화, 대외협력 등 민간주도의 자율기구(추진체계) 구성·운영 지원	이준복(2015), 이우권(2015)
	IoT 개인정보보호 생태계 구축	IoT개인정보보호 R&D투자 및 산업 육성	• 새로운 IoT기기 및 연계 등에 관한 표준화 및 안전성을 강화하기 위한 보안기술개발을 위한 R&D 투자 확대 • IoT기기·서비스보급에 따른 개인정보보호 인프라 등을 포함한 정보보호산업 육성	신영진(2016), 전자신문(2014. 10. 31)
		IoT개인정보보호 전문인력 양성	• IoT개인정보보호관련 교육프로그램인증체계를 구축하여 IoT보안, IoT취약점분석 등에 관한 교육을 통한 개인정보보호 전문인력 양성	신영진(2016), 보안뉴스(2014.10.23)
		IoT서비스 수요자인 국민의 권리 보호 및 인식제고 강화	• IoT서비스제공에 따른 개인정보처리자의 개인정보의 불법유통, 부정이용 등의 처별 등 개인정보보호인식제고 교육 강화 • IoT서비스수요자(정보주체)의 개인정보보호 권리 행사를 위한 인식제고 교육 강화	보안뉴스(2014.10.23.), 이애리 외(2016), FGI결과반영

분야	영역	지표	지표의 세부설명 및 조작정 정의	출처/참고
기술적 분야	IoT 보안기술 개발 및 안전성 강화	IoT보안기술의 개발 및 표준화	• IoT핵심보안기술의 개발 및 표준화(표준 기술개발)로 인한 산업체에 핵심기술 전수 ※ VoIP 정보보호기술, DICE WG 표준 기술, ACE WG 표준 기술, Lwig WG 표준기술, 6lo WG 표준기술, CORE WG 표준기술, MQTT 보안기술, ZigBee보안 기술 등	강남희(2014), 공희경(2015), 김범수(2014), 김호원(2014), 박지예외(2013), 윤주상 외(2014), 한국인터넷진흥원(2010)
		안전한 IoT서비스를 위한 보안기술 적용 및 강화	• IoT서비스 및 네트워크 등에서 해킹, 사이버공격 등 위기관리를 위한 보안기술 개발 • 안전한 IoT기기·서비스의 보안기술(필터링, 익명성 등 기술) 적용 및 모니터링 체계 마련·실시 • 안전한 IoT를 위해 다양한 프로토콜 운영과 인터페이스상의 안전성 강화	한국인터넷진흥원(2015a), 공희경(2015). 김범수(2014), 서화정외(2013), 손태식(2016), 한국인터넷진흥원(2012) Li, Shancang & Xu, Li Da (2017)
	IoT 인증기술 적용 및 관리	IoT개인정보 식별 및 인증 기술 관리	• IoT기기·데이터 등의 인증체계 강화, 식별·추적기술기반 인증과 암호화모듈기술 적용 • IoT기기·서비스관리자의 개인정보보호를 위한 ID관리 강화	김범수(2014), 한국인터넷진흥원(2015b), 박지예외(2013), Li, Shancang & Xu, Li Da (2017), 한국인터넷진흥원(2007), Yang, Jin-cui & Fang, Bin-Xing(2011), Su, Jinshu, et al.(2014), Wang, Xiniel, etl. al.(2014)
		IoT기기 및 서비스의 접근통제 및 운영관리	• IoT기기·서비스의 접근제어/권한제어 기술 적용 ※ 특성기반암호화(ABE): 주요정책ABE와 암호문정책 ABE적용, 특성기반의 서명(ABS)방식, ePASS적용, 디바이스OS보안, 개인정보보호 강화 DNS(도메인이름 시스템) 등 • IoT기기·서비스의 종합적인 관리를 위한 접근 통제 및 사용자 인증 및 인가 모듈의 보안강화 등 운영 상의 모니터링 추진	한국인터넷진흥원(2015a), 김범수(2014), 손태식(2016), 이애리외(2016), Jara, Antonio. J. et al. (2013)
		IoT플랫폼 및 서비스의 접근통제 및 운영관리	• IoT플랫폼/서비스에서의 인증프로토콜, 공개 API 등 적용에 따른 사용자 인증 강화 • IoT플랫폼/서비스에서의 서비스플랫폼 인증, 연동모듈 보안 및 키관리 강화	한국인터넷진흥원(2015a), 김범수(2014), Niu, Ben, et al. (2014)
	IoT개발 보안을 위한 표준화 및 기준 적용	설계단계에서의 IoT 기술보안 기준 적용 및 개발	• IoT기기·서비스의 설계시 개인정보 비식별조치 적용 및 기준에 따른 비식별조치 기기 개발 • 보안위협에 대응하는 보안요구사항을 반영한 보안기술 개발	권헌영(2015), 김동희 외(2013), 김형준(2010), 이우권(2015)
		IoT보안요구사항별 서비스 지향 아키텍처 설계 및 접근 통제	• IoT서비스의 인증, 접근제어, 프라이버스, 정보무결성, 인증서, 디지털서명, 부인방지 등 보안요구사항별 솔루션을 설계하여 서비스지향아키텍처에 의한 서비스구성 및 식별, 접근제어, 데이터 전송 등 보안서비스 관리 강화	Li, Shancang & Xu, Li Da (2017), Sicari, Sabrina, etl. al.(2014)
		IoT보안취약점 점검 및 보안모듈 개발 대응	• IoT환경에서의 보안취약점별 개인정보보호표준기술 및 보안모듈 개발 • 신규 보안취약점 발생 가능성을 고려하여 악의적 행위 대응을 위한 보안취약점 점검 및 지속적인 모니터링을 통한 대응방안 마련	강남희(2014), 김호원·김동규(2012), 보안뉴스(2014.10.23), 신영진(2016), 이동혁·박남제(2017), 이애리외(2016), 홍승필 외(2015)

분야	영역	지표	지표의 세부설명 및 조작정 정의	출처/참고
관리적 분야	IoT 생애주기별 개인정보보호 조치 강화	IoT서비스처리자의 정보주체 사전동의 및 고지의무 강화	• 정보주체에게 충분한 고지 및 사전동의 등 권리보장을 위한 적절한 정보 및 메카니즘 제공 • 제3의 개인정보처리자가 IoT기기에 의한 생성정보의 수집, 저장, 처리시 보호조치 등 정보주체의 권리 보장	김민식·이은민(2014), 김범수(2014), 이애리외(2016), Kang, Kai, et al.(2013)
		IoT서비스처리자의 개인정보처리과정상의 적절성 점검 강화	• 개인정보처리자의 'Privacy by Design'에 근거한 생애주기별 보호기술 및 정책 적용 • 개인정보처리과정에서의 개인정보의 비식별조치 기준 확립 및 재식별 모니터링 등 기술적?관리적 수단의 활용 지원 강화 • 개인정보처리과정에서의 보안기술 적용 및 적절성에 대한 점검 체크리스트 적용	한국인터넷진흥원(2015a), 김범수(2014), 권헌영(2015), 나성현(2015), 이애리외(2016), FORMERFTC Conference Center(2013).
		개인정보처리자의 개인정보 파기 및 추적금지 조치	• IoT서비스제공자가 제3자 제공에 따른 보유기간 및 파기계획에 따라 개인정보 파기관리 강화 • 특정정보(개인행태 및 성향)의 파악 및 프로파일링(추적) 금지를 통한 이용자편의성 제고	김범수(2014), 심우민(2015), 이애리 외(2016), 홍범석(2013), 홍승필 외(2015)
	IoT 개인정보 침해사고 대응대책 마련	IoT개인정보 침해사고 대응절차 및 보안대책 수립	• 개인정보 침해요인별 침해사고 대응절차 수립에 따른 체계구축 및 관련 사항에 대한 대응매뉴얼 구성 및 운영 • IoT서비스제공시 사고대응에 관한 CPO의 관리책임 설정 및 사고대응을 위한 협조체계 구축에 따른 보호조치 실행	김민식·이은민(2014.9), 김범수(2014), 이동혁·박남제(2017), 이애리외(2016), 한국인터넷진흥원(2010), 홍승필외(2015)
		IoT개인정보 침해사고 대응 조치 및 복구 강화	• 비인가접속, 불법이용 등 주요 사이버공격 등 침해사고 대응 조치(데이터 마이닝 기법을 적용한 사고추적 대응) 및 복구체계 운영 • 최신 보안위협 동향분석 및 보안위협을 파악하여 사고방지대책 공유 및 조치 강화	김범수(2014), 김영훈외(2014), Li, Shancang & Xu, Li Da(2017), 서화정외(2013), 한국인터넷진흥원(2010), Ukil, Arijit, et al.(2014)
	IoT 기기 및 서비스 관리기준강화	IoT기기·서비스의 개인정보처리 통지제도 강화	• IoT서비스처리자의 IoT기기에 대한 자산관리 강화 및 기기교체 시 기존 기기내의 개인정보 파기?2차적 재활용 사용금지, IoT제품 취약점정보 작성시 이용자 통지 등 개인정보처리 통지제도 강화	이동혁·박남제(2017), 이애리외(2016)
		IoT기기·서비스의 개인정보보호기준 적용 및 점검	• IoT기기·서비스의 개인정보처리 안전성을 높이기 위한 개인정보보호 표준플랫폼 적용 • IoT기기·서비스의 운영상 IoT보안성평가인증기준 인증제도 및 자율점검 적용	신영진(2016), 이애리 외(2016), 홍승필 외(2015)
		IoT기기·서비스의 취약점 보안패치 배포 및 사후 조치	• IoT제품제조사와 서비스제공자가 IoT기기·서비스의 보안취약점을 분석하여 보안요구사항을 반영한 보안패치 배포·위·변조방지의 사전예방하기 위한 무결성 검증 및 사후 조치	한국인터넷진흥원(2015a)

료의 연구내용을 핵심요소로 분류하고, 2차례(2017년 8월 4일과 11월 3일)에 거친 전문가 심층분석(FGI)를 거쳐 분야별 정책지표를 분야, 영역, 지표로 재구성하였다.[8)]

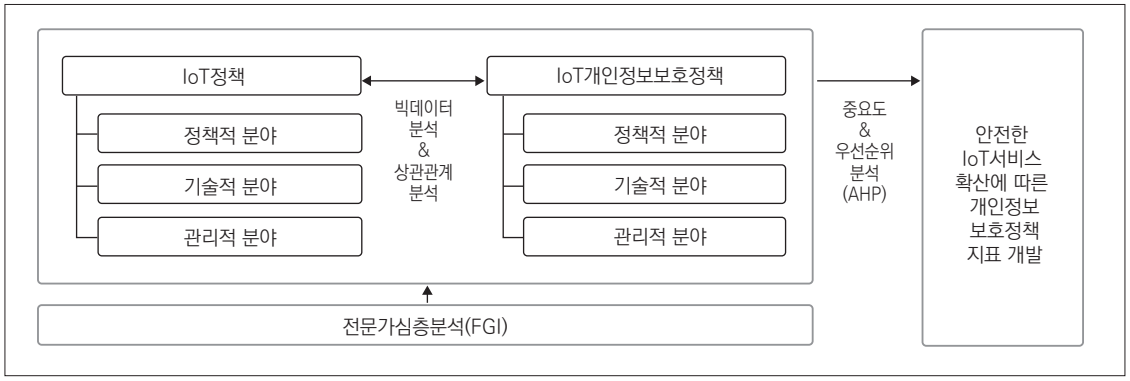
Ⅲ. 연구의 분석틀과 방법

본 연구는 안전한 IoT서비스가 확산됨에 있어서 개인정보보호를 위해 필요한 정책과제의 중요도 및 우선순위를 분석하여 개선하고자 하였다. 이를 위해서 기존 연구보고서, 학회보, 학회발표 자료집, 뉴스, 가이드라인, 국내외 인터넷 자료 등 문헌조사를 통해 안전한 IoT서비스에 필요한 개인정보보호정책지표를 검토하였다. 이에 대해 실제 IoT와 개인정보보호에 관한 실질적인 관계성에 대해서 분석하고, 그에 따른 개인정보보호정책에 관한 분석을 진행해 보고자 한다.

이를 위해서 IoT개인정보보호에 관하여 빅데이터 분석, 상관관계 분석을 통해 IoT가 개인정보보호에 영향력을 갖는 지 분석하고자 한다. 또한, IoT개인정보보호를 위해서 필요한 정책지표의 중요성과 우선순위과제를 선정하기 위하여 전문가대상의 전문가심층면접(Focus Group Interview: 이하 FGI) 및 의사결정계층분석기법(Analytic Hierarchy Process: 이하 AHP)분석을 하여 제언하고자 한다.

먼저, 본 연구는 문헌조사를 통해 선정한 정책지표들을 전문가들의 검토를 통해서 재정리하였다. 이를 위해서 FGI를 위해 전문가 6명(법률, 기술, 정책, 실무 등의 연구경험과 실무경력을 갖춘 전문가)으로 구성된 자문회의를 2017년 8월 4일과 11월 3일에 개최하여 정책지표를 정리하였다. 이처럼 IoT개인정보보호정책 지표들은 3개 측면(정책, 기술, 운영)으로 구성하였으며, 정책적 측면은 3개 영역 12개 지표, 기술적 측면은 5개 영역 16개 지표, 관리적 측면은 4개 영역 22개 지표로 분류하였다. 이를 2회에 거친 자문회의를 거쳐서 3개 분야(정책, 기술, 관리)로 구분하는 맥락은 같으나, 그 세부적인 사항에서 정책적 분야는 3개 영역 9개 지표, 기술적 분야는 3개 영역 8개 지표, 관리적 분야는 3개 영역 8개 지표로 재정리하였다.

둘째, 본 연구에서 IoT정책과 개인정보보호정책의 상호관련성을 분석하고자 하였는데, 먼저, 빅데이터 분석을 구글트렌드 분석방법(http://trends.google.com)을 활용하여 시간적 흐름에 따른 관심정도를 분석하고자 하였다. 둘째, IoT정책과 개인정보보호정책과의 상관관계분석을 위해 전문가 설문조사결과를 비

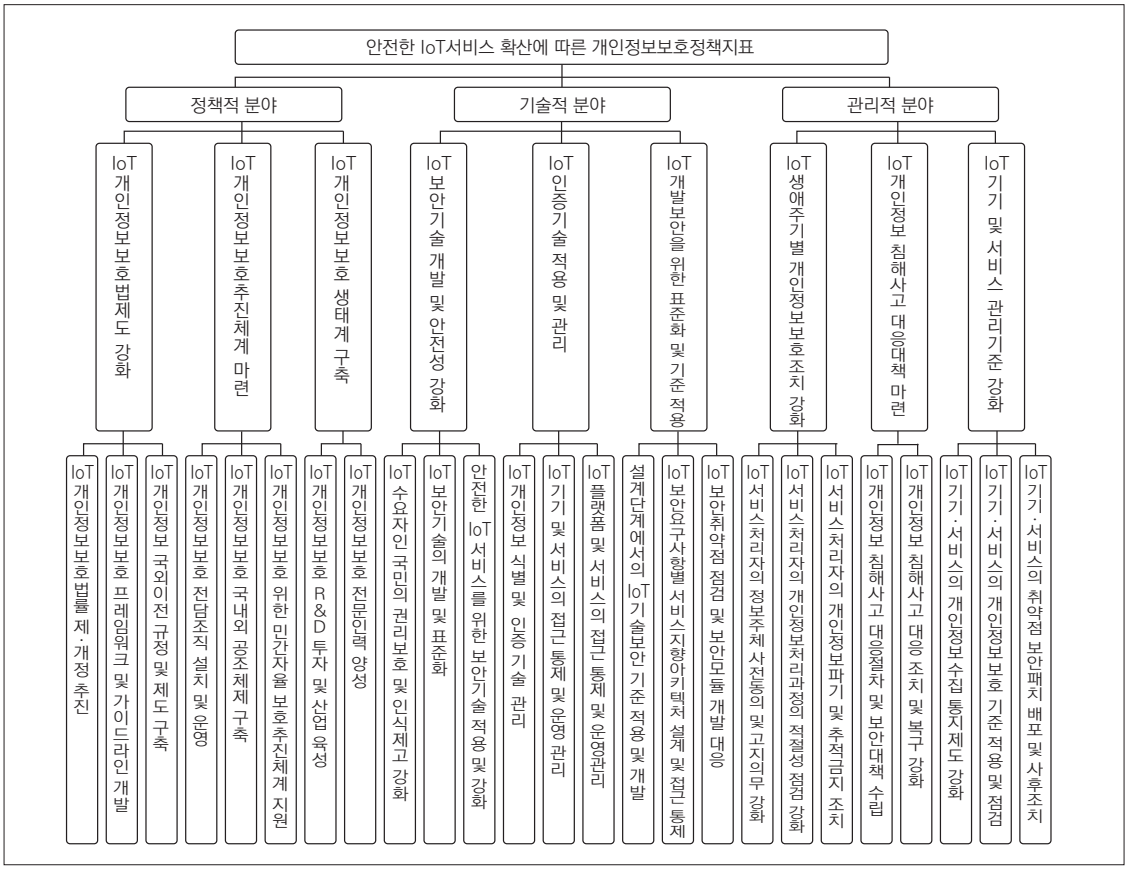


〈그림 1〉 분석의 틀

8) 본 연구는 정책분야, 정책영역, 정책지표, 정책세부과제로 구성하여 진행하였는데, 본 연구지에서는 정책세부과제를 제외한 연구결과로 정리하였고, 지표의 세부사항(조작적 정의)은 정책세부과제를 중심으로 설명하였으나 본 내용에서는 제외하였다.

〈표 3〉 IoT개인정보보호정책지표의 재정리

측면	영역		분야	영역
정책 (12개 지표)	IoT개인정보보호 정책마련	⇒	정책 (9개 지표)	IoT 개인정보보호법제도강화
	IoT개인정보보호 법제정비			IoT 개인정보보호추진체계마련
	IoT개인정보보호조직 강화			IoT 개인정보보호 생태계구축
기술 (16개 지표)	IoT보안기술 개발 및 지속성 유지	⇒	기술 (8개 지표)	IoT 보안기술 개발 및 안전성 강화
	IoT접근권한 및 접근통제 강화			IoT 인증기술적용 및 관리
	IoT디바이스보안 강화			IoT개발보안을 위한 표준화 및 기준 적용
	IoT플랫폼/서비스 보안강화			
	IoT네트워크보안강화			
운영 (22개 지표)	IoT개인정보의 생애주기별 관리	⇒	관리 (8개 지표)	IoT 생애주기별 개인정보보호조치 강화
	IoT침해사고 대응절차 운영			IoT 개인정보 침해사고 대응대책 마련
	IoT제품 및 서비스 관리			IoT 기기 및 서비스관리기준 강화
	IoT 생태계 구축			



〈그림 2〉 AHP 분석틀

교하였는데, IoT가 개인정보보호에 영향정도를 분석하였다. 본 상관관계분석은 IBM SPSS14버전을 활용하였으며, 중요도 및 우선순위분석(AHP분석), 신뢰도분석(CI)의 경우는 EXCEL을 활용하여 공식적용을 하여 얻은 결과값을 활용하였다.

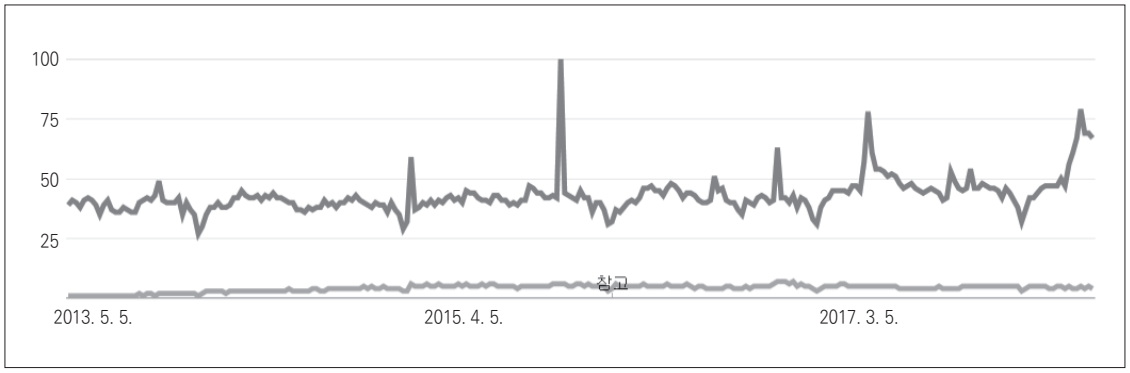
셋째, IoT개인정보보호를 위해서 필요한 정책지표의 중요성과 우선순위과제를 선정하기 위하여 전문가 대상의 의사결정계층분석기법(Analytic hierarchy process: 이하 AHP)분석을 하여 제언하고자 한다. 이는 전문가들을 통해 IoT개인정보보호정책의 중요도 및 우선순위에 관한 전문가 의견을 반영하고자 2017년 11월 6일부터 11월 28일까지 전문가 설문조사를 하였고, 응답자 66명으로부터 답변을 얻었다.

본 설문조사에 참여한 전문가들은 정보보호관련 분야 경력이 평균 17.5년(최저 3년부터 최장 38년)이며, 정책분야(정보보호정책 및 개인정보보호정책) 27명, 기술분야(개인정보보호 및 정보보호) 26명, 그 외 ICT관련 분야(전자정부, 전자상거래 등) 13명이 참여하였다. 이렇게 응답한 9점 척도의 쌍대비교 결과값은 안전한 IoT서비스 확산에 따른 개인정보보호정책의 각 분야, 영역, 지표의 중요도 및 우선순위를 평가하는데 활용하였다. 특히, 본 설문 및 분설결과의 일관성 및 신뢰성을 검증하기 위하여 쌍대비교간의 일관성지수(Consistency Index: 이하 CI)를 우선 산출하는데, CI=(λ-N)/(N-1)로서, N은 쌍대비교의 대상수이며, CI<0.1이어야 채택되며, CI=0이면 완전 정합하여 CI값이 커질수록 정합성이 떨어진다. 일관성 정도(Consistency Ratio: 이하 CR)는 무작위성에 대해 인위적으로 발생되는 무작위 정합성 지수(Random Index: 이하 RI)[9]를 활용하여 CR=CI/RI의 산정공식을 사용하였으며, CR<0.1인 경우 적합한 것으로 판단할 수 있다.

IV. 분석결과 및 한계

1. IoT와 개인정보보호의 정책관계분석

본 연구에서 제4차 산업혁명의 핵심기술인 IoT를



출처: https://trends.google.co.kr/trends/explore?date=today%205-y&q=Internet%20of%20Things,privacy

〈그림 3〉 IoT와 개인정보보호에 관한 시간흐름에 따른 관심도 변화

9) 〈표〉 무작위지수(R.I.)

행렬수	1	2	3	4	5	6	7	8	9	10	11	12	13	14
R.I.	0.00	0.00	0.58	0.90	1	1.12	1.32	1.41	1.45	1.49	1.51	1.48	1.56	1.57

출처: 목하영장(2008).

적용함에 있어서 개인정보보호와의 관계성을 구글트렌드를 이용하여 지난 5년 동안(2013년 5월 5일부터 2018년 5월 5일) 주요 검색어(키워드) 분석을 하였다. 본 연구를 위해서 구글에 게재된 논문, 뉴스 등의 메타데이터를 대상으로 시간의 흐름에 따른 관심도의 변화를 비교해 보았다. 사물인터넷에 관한 관심도가 100이라고 볼 때, 개인정보보호에 관한 관심도가 75로서 점차 높아짐을 알 수 있다(신영진, 2017).

더욱이, IoT정책(4.6154)과 IoT개인정보보호정책(4.6462)의 중요도에 대해 전문가 대상으로 설문조사(2017년 11월 6일부터 11월 28일)를 리커드 5점 척도 기준으로 하였다. 본 설문조사를 66명에서 응답받은 내용을 재정리하였으며, 5점 척도에 응답한 비율을 〈표 4〉와 같이 빈도분석을 하여 본 결과는 다음 〈표 5〉와 같이 정리할 수 있다.

이에 대해 정책적 관점에서 IoT정책과 IoT개인정보보호정책간의 신뢰도 분석을 하였는데, Cronbach의 a = 0.89로 신뢰성이 높게 나타났다. 더욱이, IoT정책과 개인정보보호정책의 상관관계를 분석한 결과, 상관성이 높은 것으로 나타났다. 따라서, 전반적인 정보화환경에서 개인정보보호에 대한 관심과 중요성이 높아지고 있으며, 더욱이 IoT와 연계된 개인정보보호

〈표 4〉 IoT정책과 IoT개인정보보호정책의 빈도분석

응답부분		빈도(n)	퍼센트(%)	유효 퍼센트	누적 퍼센트	빈도	퍼센트	유효 퍼센트	누적 퍼센트
유효	1	0	0	0	0	0	0	0	0
	2	0	0	0	0	0	0	0	0
	3	0	0	0	0	2	3.0	3.0	3.0
	4	26	39.4	39.4	39.4	19	28.8	28.8	31.8
	5	40	60.6	60.6	100.0	45	68.2	68.2	100.0
	전체	66	100.0	100.0		66	100.0	100.0	

〈표 5〉 IoT정책과 IoT개인정보보호정책의 상관관계 및 우선순위분석 결과

구분	N	우선순위	평균	표준편차	표준오차	상관성	ANOVAa	계수a
IoT정책	66	0.6805	4.606	0.492	0.081	1	F=118.606 P=0.000b	t=10.891 P=0.000
개인정보보호정책	66	0.3195	4.652	0.540	0.067	0.86**		

주*. 상관관계가 p〈0.01 수준에서 유의함(양측).

〈표 6〉 IoT정책과 개인정보보호정책의 분야별 중요도 및 우선순위분석 결과

	IoT정책	개인정보보호정책
종합적 관점	0.6830 (1.0000)	0.3170 (1.0000)
정책적 분야	0.3974 (0.5824)	0.1931 (0.6081)
기술적 분야	0.1959 (0.2851)	0.0802 (0.2530)
관리적 분야	0.0900 (0.1325)	0.0435 (0.1390)

정책과제가 점차 중요하므로 그에 대한 대응방안이 마련되어야 할 것이다.

그렇다면, IoT정책과 IoT개인정보보호정책을 구성하는 해당분야의 중요도에 대해서 AHP분석을 하였다. 이에 대해서 정책적 분야(0.3974, 0.1931)가 가장 중요하며, 그 다음으로 기술적 분야(0.1959, 0.0802), 관리적 분야(0.0900, 0.0435) 순으로 중요하여 우선되어야 한다. 따라서 안전한 IoT서비스를 제공하기 위해서는 IoT정책과 함께 IoT개인정보보호정책도 반드시 수반되어야 할 것이다.

2. IoT개인정보보호정책의 중요도 및 우선순위 분석

1) 종합적 관점의 분석결과

본 연구에서는 IoT개인정보보호정책(중요도=1 기준)에 관해 AHP기법을 통해서 두 정책 중에서 어떤 정책이 더 중요하고 우선해야 하는 지 분석해 보았다. 그 결과, 3개 분야 중에서는 정책적 분야(0.6081), 기술적 분야(0.2530), 관리적 분야(0.1390) 순으로 중요하며 우선된다고 응답하였다. 9개 정책영역 중에서는 정책분야의 IoT개인정보보호법제도 강화(0.3133)가 가장 중요하며 우선되어야 한다고 보았다. 25개 정책지표 중에서는 정책분야의 IoT개인정보보호법률 제·개정 추진(0.1613)이 우선되는 정책지표로 선정하였다. 이렇게 IoT개인정보보호정책에 관한 정책적 분야·기술적 분야·관리적 분야의 쌍대비교 결과값이 일관된 응답결과로 구성되었는지 분석해 보았다. 즉, 각 분야에 대한 일관성 정도(CR)를 살펴보면, CI=0.0360이며 행렬수 3의 RI=0.580이므로 CR=0.0620〈0.1로 검증되었다. 이에 따라 정책적 분야의 비중이 다른 분야보다 높으므로, 정책분야의 구성영역에서도 높은 중요도를 얻게 되었다.

2) 각 분야별 분석결과

(1) 정책적 분야

본 연구에서의 정책적 분야(0.6081)는 3개 영역으로 구분하였는데, IoT개인정보보호 법제도 강화(03133, 1순위) IoT개인정보보호추진체계 마련(0.1960, 2위), IoT개인정보보호 생태계 구축(0.0988, 3위) 순으로 IoT개인정보보호정책에 관한 상대적 중요도 및 우선순위가 선정되었다. 이에 대한 일관성지수(CI)는 0.0510〈0.1이며, 일관성정도(CR)는 0.0879〈0.1로 AHP분석에 대한 신뢰성을 검증하였다.

그렇다면, 각 영을 구성하는 정책과제의 중요도에 대해서 살펴보면, 첫째, IoT개인정보보호 법·제도 강화 영역은 IoT에 관한 개인정보보호를 위해 법제도(법률, 규정, 기준, 가이드라인 등)를 강화하여야 한다. 이를 구성하고 있는 3개 정책지표간의 중요도와 우선순위는 IoT개인정보보호법률 제·개정 추진(0.1613) IoT개인정보보호 프레임워크 및 가이드라인 개발(0.1134), IoT개인정보 국외이전 규정 및 제도 구축(0.0386) 순으로 보았다. 따라서 IoT개인정보보호를 위해서 통합적으로 적용 가능한 법제도를 정비하여 「클라우드 발전 및 보호에 관한 법률」(이하 클라우드

〈표 7〉 IoT개인정보보호정책의 중요도 분석

구분	정책적 분야	기술적 분야	관리적 분야
중요도	0.6081	0.2530	0.1390
우선순위	1	2	3
일관성 지수(CI)	0.0476		
일관성 정도(CR)	0.0620		

주*. p〈0.1

발전법)과 같이 특별법으로 「IoT발전법」을 제정하여, IoT개인정보보호를 위해서 자율규제를 강화하고 정보주체가 스스로 자기정보에 대한 결정권 및 통제권을 보장받도록 법적 근거를 마련해야 한다. 동법에 따라 IoT서비스의 도입부터 산업화에 이르기까지 개인정보보호에 관한 준수사항을 법적 근거에 맞추어 제공하도록 하여야 한다. 앞서 지표간의 조작적 정의와 같이 관련된 정책지표들을 강화하여 IoT개인정보보호를 위한 체계적인 규정을 마련하고 가이드라인을 제공하여 IoT개인정보보호의 안전성을 높이고 IoT연계 네트워크 및 서비스의 확대에 따른 개인정보의 국외이전 및 확장으로 인한 제도적 기준도 마련되어야 할 것이다. 특히, IoT서비스가 확대됨에 따라 다양한 분야에서 개인정보를 기준으로 설계부터 운영까지 안전성을 높일 수 있는 체계적인 법제도가 필요하다.

둘째, IoT개인정보보호 추진체계 마련 영역은 IoT에 관한 개인정보보호를 총괄적으로 추진하기 위한 조직체계가 마련되어야 한다는 입장이다. 이는 3개 정책지표로 구성하는데, IoT개인정보보호 전담조직을 설치 및 운영하여야 하며(0.1144), IoT개인정보보호를 위해 국내외 공조체제를 구축하여야 하고(0.0539), IoT개인정보보호 위한 민간자율 보호추진체계를 지원하는(0.0276) 순으로 응답하였다. 따라서, IoT개인정보보호 전담조직 설치 및 운영에 관하여 IoT개인정보보호에 관한 총괄추진체계를 설치하고 효율적인 정책, 특히 IoT보안대책 및 사이버 위협 및 침해사고 대응을 위한 종합적인 대응체제를 구축하여야 할 것이다. 현재 2017년 8월 4차산업혁명위원회를 대통령직속으로 설치하여 IoT를 포함한 신규 정보기술의 발전을 가속화하고 있다. 그러나 구체적인 정책과제를 수행하기에는 정부부처에 산발된 정책을 통합추진하기 위해서는 별도 기구가 필요하다. 이외에도 IoT네트워크 및 유통의 확산에 따른 개인정보보호를 위한 국내외 공조체제가 구축되어야 한다. 물론 정부차원에서의 대응뿐만 아니라 민간주도의 개인정보보호를 위한 노력을 통해서 자율적인 개선을 가져올 수 있는 추진체계도 정비되어야 한다. 앞으로 IoT를 둘러싼 실시간 대응을 위해서 공공과 민간을 한정짓지 않도 상호 간에 운영체제 및 협조네트워크를 구축하여 안전성을 높여 나가야 한다.

셋째, IoT개인정보보호 생태계 구축 영역은 IoT개인정보보호를 위한 정보환경의 생태계를 구축하기 위한 영역으로서 3개 지표로 구분하였다. 이 정책지표의 중요도 및 우선순위를 비교한 결과, IoT개인정보보호 R&D 투자 및 산업을 육성하여야 하며(0.0517), IoT서비스를 운용함에 있어서 필요한 개인정보보호 전문인력을 양성하고(0.0310), IoT수요자인 국민의 권리보호 및 인식제고를 강화(0.0160)되어야 한다고 보았다. 특히, IoT개인정보보호 R&D 투자 및 산업 육성의 경우 새로운 IoT기기 도입 및 연계 등을 위한 표준화가 필요하며 안전성을 강화하기 위해 지속적인 보안기술의 R&D투자가 확대되어야 한다. 이렇게 IoT기기·서비스 보급을 위해서 개인정보보호 인프라를 강화할 수 있는 정보보호산업이 육성되어야 한다. 현재 IoT에 관한 산업방향은 기기 및 서비스에 대한 개선을 가져오는 과제를 중심으로 추진되고 있으나, 이와 관련한 서비스의 확산에 따른 정보보호가 실질적으로 연계 가능한 보안기술을 산업화할 수 있어야 한다.

이외에도 IoT개인정보보호 전문인력을 양성하기 위해서 필요한 교육프로그램인증체계를 도입되어야 한다. 현재 IoT에 관한 범위 정립이 되어 있지 않다보니, 다른 4차산업혁명의 핵심요소만큼 성장을 가져오기 위한 인력인프라 구축방향을 마련하지 못하고 있다. 끝으로, IoT서비스를 제공함에 있어서 IoT서비스 수요자까지 정보인식을 높일 수 있는 교육 등이 추진되어야 할 것이다. 정부가 추진하고 있는 IoT에 관하여 국민이 어느 정도 인식하고 있는지 진단하고 그에 필요한 설득과 서비스의 확대가 이루어질 수 있도록 맞춤형 교육이 요구되고 있다. 이를 위해서 각계 분야에 필요한 IoT기초부터 숙련된 기술을 배양하는 교과과정까지 운영하여 본격적인 서비스의 안전성을 확보할 수 있도록 제공하는 커리큘럼이 요구된다. 이상과 같

〈표 8〉 정책적 분야 개인정보보호정책의 중요도 및 운선순위 분석

영역	중요도	우선순위	정책지표	중요도	우선순위	CI/CR
IoT 개인정보보호법 제도 강화	0.3133	1	IoT개인정보보호법률 제·개정추진	0.1613	1(1)	CI=0.0535 CR=0.0923
			IoT개인정보보호 프레임워크 및 가이드라인 개발	0.1134	2(3)	
			IoT개인정보 국외이전 규정 및 제도 구축	0.0386	3(6)	
IoT 개인정보보호 추진 체계 마련	0.1960	2	IoT개인정보보호 전담조직 설치 및 운영	0.1144	1(2)	CI=0.0446 CR=0.0769
			IoT개인정보보호 국내외 공조체제 구축	0.0539	2(4)	
			IoT개인정보보호 위한 민간자율 보호추진체계 지원	0.0276	3(8)	
IoT 개인정보보호 생태계 구축	0.0988	3	IoT개인정보보호 R&D투자 및 산업 육성	0.0517	1(5)	CI=0.0540 CR=0.0931
			IoT개인정보보호 전문인력 양성	0.0310	2(7)	
			IoT서비스 수요자인 국민의 권리 보호 및 인식제고 강화	0.0160	3(9)	

주*( )의 순위는 해당분야 정책지표의 전체 우선순위임.

이 각 영역 및 정책지표별 상대적 중요도 및 우선순위, 분석결과의 신뢰성정도는 다음 〈표 8〉과 같다.

(2) 기술적 분야

기술적 분야에 해당되는 개인정보보호정책과제는 3개 영역으로 구분되어지는 데, 그 중요도 및 우선순위를 비교해 보면, IoT보안기술 개발 및 안전성 강화(0.1419), IoT인증기술 적용 및 관리(0.0663), IoT개발보안을 위한 표준화 및 기준 적용(0.0448) 순으로 나타났다. 이에 대한 일관성지수(CI)는 0.0449 〈 0.1 이며, 일관성정도(CR)는 0.0775 〈 0.1로 연구결과의 신뢰성을 확보하였다.

그렇다면, 각 영역별 정책지표들의 중요도 및 우선순위를 분석하였는데, 첫째, IoT보안기술 개발 및 안전성 강화 영역은 IoT를 위한 보안기술을 개발하고 운영과정상의 안전성을 높이고자 하며, IoT보안기술의 개발 및 표준화(0.0976), 안전한 IoT서비스를 제공하기 위한 보안기술의 적용 및 강화(0.0442) 순으로 필요하다. 현재 VoIP, DICE WG, ACE WG 등 표준기술이 개발되어 보급되고 있으며, MQTT, ZigBee 등 보안기술도 개발되어 제공되고 있다. 이에 따라 앞으로 IoT에 필요한 핵심기술을 개발함에 있어서 상호연동성을 고려한 표준화가 우선되어야 한다. 물론, 안전한 IoT서비스환경을 구현하기 위해서는 외부로부터 발생 가능한 해킹, 사이버공격 등의 위협들로부터 시스템 및 네트워크를 보호할 수 있는 기술이 개발되어야 하고, 다양한 프로토콜 운영과 인터페이스의 안전성을 가져올 수 있도록 실시간 보안점검체계가 마련되어야 한다. 더욱이 상호간의 연계로 인해 사이버위협 등이 지속적으로 발생하므로, 적절한 보안기술의 개발이 필요하다.

둘째, IoT인증기술 적용 및 관리 영역은 IoT기기 및 서비스의 고품질서비스를 위한 인증기술의 적용 및 관리를 위해서 구성되었다. 이 영역의 3개 정책지표간의 중요도 및 우선순위를 분석해 보면, IoT개인정보 식별 및 인증기술 관리(0.0356), IoT기기 및 서비스의 접근통제 및 운영관리(0.0183), IoT플랫폼 및 서비스의 접근통제 및 운영관리(0.0125) 순으로 정책지표를 적용하여 추진되어야 한다. IoT개인정보 식별 및 인증기술 관리를 위해서 IoT기기부터 데이터처리까지 인증체계를 강화하여야 하며 ID관리, 식별인증 및 암호화모듈기술의 적용 등을 통해서 IoT처리과정에서의 안전성을 높여야 한다. 이외에 IoT기기 및 서비스의 비인가접근을 통제할 수 있도록 하며 인가 및 인증모듈의 강화를 통해서 운영상의 안전성을 강화해 나가야 한다. 물론, IoT플랫폼/서비스에 대한 인증도 강화

〈표 9〉 기술적 분야 개인정보보호정책의 중요도 및 운선순위 분석

영역	중요도	우선순위	정책지표	중요도	우선순위	CI/CR
IoT 보안기술 개발 및 안전성 강화	0.1419	1	IoT보안기술의 개발 및 표준화	0.0976	1(1)	CI=0.0000 CR=0.0000
			안전한 IoT서비스를 위한 보안기술 적용 및 강화	0.0442	2(2)	
IoT 인증기술 적용 및 관리	0.0663	2	IoT개인정보 식별 및 인증 기술 관리	0.0356	1(3)	CI=0.0161 CR=0.0277
			IoT기기 및 서비스의 접근통제 및 운영관리	0.0183	2(5)	
			IoT플랫폼 및 서비스의 접근통제 및 운영관리	0.0125	3(7)	
IoT개발보안을 위한 표준화 및 기준 적용	0.0448	3	설계단계에서의 IoT기술보안 기준 적용 및 개발	0.0253	1(4)	CI=0.0493 CR=0.0850
			IoT보안요구사항별 서비스지향 아키텍처 설계 및 접근 통제	0.0137	2(6)	
			IoT보안취약점 점검 및 보안모듈 개발 대응	0.0058	3(8)	

주* ( )의 순위는 해당분야 정책지표의 전체 우선순위임.

하여 서비스과정뿐만 아니라 서비스의 저장·전송·운용상의 안전성을 높여야 한다.

셋째, IoT를 위한 기기 및 서비스의 개발보안을 위한 표준화 및 기준을 적용하는 영역을 구성하는 3개 정책지표의 중요도 및 우선순위를 비교해 보았다. IoT 전과정 중 설계단계에서의 IoT기술보안기준의 적용 및 개발(0.0253), IoT에 관한 보안요구사항별 서비스지향 아키텍처 설계 및 접근 통제(0.0137), IoT보안취약점 점검 및 보안모듈 개발 대응(0.0058) 순으로 정책과제가 우선적으로 적용되어야 한다. 그 중에서 설계단계에서의 IoT기술보안기준 적용 및 개발은 IoT기기 및 서비스의 설계단계에서 개인정보를 비식별조치를 하도록 하며 처리과정에서 자동적으로 비식별조치를 할 수 있는 기기를 개발하여야 한다. 더욱이 이러한 기술을 포함하여 보안요구사항을 포함한 보안기술을 개발하여 보급한다면, 개인정보침해사고의 사전적 예방이 가능하리라 본다. 이외에도 IoT서비스를 제공함에 있어서 서비스지향적 아키텍처를 구성하여 서비스의 식별, 접근제어, 데이터 전송, 보안요구사항 및 솔루션을 설계한다면, IoT보안요구사항에 적합한 서비스 지향 아키텍처 설계 및 접근통제가 가능하리라 본다. 물론, IoT환경에서 보안취약점을 정기적으로 점검하고 필요한 보안모듈을 개발하여 적용하는 것도 효과적이다. 이렇게 앞서 정리한 정책 영역 및 정책지표의 상대적 중요도 및 우선순위분석의 신뢰성검증 결과는 〈표 9〉와 같다.

(3) 관리적 분야

IoT에 관한 개인정보보호를 위한 관리적 분야의 정책영역을 3개로 구성하여 정책의 중요도 및 우선순위를 비교해 보았다. 이에 대해서 IoT생애주기별 개인정보보호조치 강화(0.1419), IoT개인정보침해사고 대응대책 마련(0.0663), IoT기기 및 서비스관리기준 강화(0.0448) 순으로 중요하다고 보았다. 이에 대한 응답결과의 신뢰성은 일관성지수(CI)는 0.0337〈0.1이며, 일관성정도(CR)는 0.0580〈0.1로 적합하였다.

그에 대해 각 정책영역의 정책지표에 대한 중요도 및 우선순위를 비교해 보았는데, 첫째, IoT를 위한 생애주기별 개인정보보호조치를 강화하기 위해서는 개인정보처리자의 정보주체 사전동의 및 고지의무 강화(0.0123), 개인정보처리자의 개인정보 수집부터 파기까지 처리과정상의 적절성 점검 강화(0.0074), 개인정보처리자의 개인정보 파기 및 추적 금지 조치(0.0050) 순으로 정책지표별 중요도가 조사되었다. 여기서 IoT서비스처리자의 정보주체 사전 동의 및 고지의무에 관하여는 이미 기존 「정보통신망법」 및 「개인정보 보호법」에서도 정의하고 있다. 그러나 신규 기술에 의한 정보수집 및 집적화로 인한 서비스의 안전

성을 위해서 적용되어야 하며, 기존 서비스의 제공보다 더 많은 IoT기기간의 연계로 인해 생성된 정보를 수집·저장·처리하는 과정에서 정보주체의 권리를 보장할 수 있는 기준과 메카니즘을 요구하고 있다. 이외에 IoT서비스처리자의 개인정보처리과정상 적절성 점검 강화를 위해서 개인정보처리자가 유형별로 준수해야 할 구체적인 기준을 마련하여 'Privacy by Design (개인정보보호 적용설계)'할 수 있도록 하여야 하며, 기술적 보호조치에 적용된 개인정보 비식별 조치기준과 보안기술의 적용 여부 등을 점검할 수 있는 체크리스트를 제공해 주어야 한다.

둘째, IoT서비스에 관한 개인정보침해사고별 대응대책을 마련하기 위해서는 IoT관련 개인정보침해사고 대응절차 및 보안대책 수립(0.0086), IoT관련 개인정보침해사고 대응 조치 및 복구 강화(0.0037) 순으로 정책지표로서 우선 추진되어야 한다. IoT개인정보 침해사고 대응절차 및 보안대책 수립을 위해서는 개인정보 침해요인별 침해사고 대응체계를 구축하여 관련 사항에 대해 매뉴얼화하도록 한다. 국제적으로 BS10012, ISO/IEC 27001 등 기업의 정보보호 운영에 적용하고, 우리나라의 경우 개인정보보호관리체계와 개인정보보호인증제도를 통합하고, 정보보호 준비도 평가를 도입하고 있다(김민천, 2016) 이처럼 침해사고 대응을 위해 필요한 인증체계를 적용해 대응할 수 있다. 또한, 그에 대한 지속적인 CPO의 역할을 강화하여 침해사고대비 관련 기준 및 사고대응을 위한 신속한 처리가 가능하도록 협조체계를 구축하여 적용해 나가야 한다. 물론, IoT보안취약점을 분석하여 IoT제품의 보안취약점을 작성하는 등 보안대응절차를 마련해야 할 것이다. 이외에 IoT개인정보 침해사고 대응 조치 및 복구강화를 위해서 데이터마이닝 기법을 이용한 침해요인 및 사고추적을 통해서 침해사고에 대응할 수 있도록 하여야 하며, 상시적인 침해사고 대응조치 및 복구체계의 운영과 보안위협의 동향분석을 통해서 지속적이 업데이트로 안전성을 강화해 나가야 할 것이다.

셋째, IoT기기 및 서비스의 관리기준을 강화하기 위한 3개 정책지표의 중요도 및 우선순위를 보면, IoT기기·서비스의 개인정보처리 통지제도 강화(0.0030), IoT기기·서비스의 개인정보보호 기준 적용 및 점검(0.0023), IoT기기·서비스의 취약점 보안패치 배포 및 사후 조치(0.0013) 순이었다. IoT기기·서비스의 개인정보처리 통지제도를 강화하기 위해서는 IoT서비스처리자의 IoT기기에 대한 자산관리 및 개인정보의 활용금지 등을 통해 이용자에게 IoT제품 및 서비스의 취약점을 확인하였을 때 IoT서비스이용자에게 개인정보처리에 관한 통지를 하도록 하여야 한다. 그 외에 IoT기기·서비스의 개인정보보호기준 적용 및 점검을 위해

〈표 10〉 관리적 분야 개인정보보호정책의 중요도 및 운선순위 분석

영역	중요도	우선순위	지표	중요도	우선순위	CI/CR
IoT 생애주기별 개인정보 보호조치 강화	0.0788	1	IoT서비스처리자의 정보주체 사전동의 및 고지의무 강화	0.0394	1(1)	CI=0.0070 CR=0.0120
			IoT서비스처리자의 개인정보처리과정상의 적절성 점검 강화	0.0234	2(3)	
			IoT서비스처리자의 개인정보 파기 및 추적금지 조치	0.0160	3(4)	
IoT 개인정보 침해사고 대응대책 마련	0.0389	2	IoT개인정보 침해사고 대응절차 및 보안대책 수립	0.0273	1(2)	CI=0.0000 CR=0.0000
			IoT개인정보 침해사고 대응 조치 및 복구 강화	0.0116	2(5)	
IoT기기 및 서비스 관리기준 강화	0.0213	3	IoT기기·서비스의 개인정보처리 통지제도 강화	0.0098	1(6)	CI=0.0223 CR=0.0385
			IoT기기·서비스의 개인정보보호기준 적용 및 점검	0.0075	2(7)	
			IoT기기·서비스의 취약점 보안패치 배포 및 사후 조치	0.0040	3(8)	

주*( )의 순위는 해당분야 정책지표의 전체 우선순위임.

서도 개인정보보호에 관한 표준플랫폼을 적용하고 보안인증제도 및 자율점검을 적용하여 서비스의 안전성을 높이도록 하여야 한다. IoT기기·서비스의 보안취약점을 분석하여 보안패치를 배포하고 위·변조방지를 위해 사전 무결성을 검증하여 사후 조치한다면 개인정보 침해사고를 예방하는데 효과적일 것이다. 이처럼 각 영역별 정책지표의 상대적 중요도 및 우선순위분석의 신뢰성 검증 결과는 〈표 10〉과 같다.

3. 분석 한계

본 연구는 안전한 IoT서비스를 확산함에 있어서 개인정보보호를 향상시키기 위한 정책과제를 제언하기 위해 정책지표의 중요도 및 우선순위를 분석하였다. 이를 위해서 기존 문헌연구를 바탕으로 한 정책연구들의 주제들을 전문가들의 의견을 수렴해서 본 연구의 정책지표를 도출하였고, 그에 따른 상대적 중요도 및 우선순위를 설문조사를 통해 정책과제를 선정하고 고려해야 할 사항을 제언하였다. 이러한 연구과정에서 몇 가지 한계가 있는데, 첫째, 본 연구는 정책지표에 관한 쌍대비교를 위해서 전문가들을 대상으로 AHP분석을 하였다. 본 연구에 참여한 전문가들은 개인정보보호에 관한 정책·기술·관리적 분야에서 실무를 경험하거나 관련분야를 전공하였다. 그러나 설문에 참여한 전문가들의 응답비율을 고려할 때 응답자의 전공분야에 대한 참여비율이 고려되지 못하였다. 따라서, 아직까지 정보보호에 관한 법률 및 기술에 치중된 현실에서 각 전문성을 반영하기에는 편향된 결과가 나올 수밖에 없는 한계가 있다. 그로 인해 연구결과에 미치는 영향정도가 정책분야, 정책영역, 정책지표의 상대적 중요도 및 우선순위를 선정함에 있어서 통제되지 못하였으므로, 향후 대표성에 대한 통제변수를 고려하여 연구하고자 한다.

둘째, 본 연구에서 제시한 정책지표들은 기존 연구(연구논문, 학회보, 학회발표지), 기존 정책보고서, 언론보도자료, 인터넷 자료 등을 바탕으로 도출하였다. 그렇다보니, 문헌조사를 중심으로 한 정책지표가 실무적 사항을 직접적으로 반영하지 못하고 이론적 정책지표로서 구성되었다. 기존의 IoT에 관한 연구들은 인프라 및 기기에 중점을 두고 있는 것이 현실이다. 아직 실질적 서비스가 이루어지지 못하였기에 본 연구가 안전한 IoT서비스에 관점을 두기에는 아직 IoT개인정보보호 및 정보보호연구가 초기단계로 인해 큰 성과를 얻기 어려운 실정이다.

셋째, 본 연구는 정책분야, 정책영역, 정책지표를 구성하는데 연구의 주제별 유사한 사항으로 범주화하여 지표를 구성하였다. 그러나 정책지표의 중요도 및 우선순위를 제시하기 위한 연구목적에 따라, 정책지표가 수행되어야 하는 정책과제로 해석하는데 한계가 있다. 더욱이 쌍대비교를 위한 3개 영역을 기준으로 전문가 가중치를 배분하였으나, 정책지표의 경우 해당영역의 정책지표가 어떻게 구성되느냐에 따라 정책지표의 중요도 산정결과가 달라질 수 있다. 이러한 연구의 한계에서 불구하고, 본 연구가 안전한 IoT서비스의 확산을 기대하며 앞서 필요한 개인정보보호의 기준을 마련하고, 그에 따른 정책과제를 우선적으로 추진해야할 필요성을 제언하여 개인정보보호정책의 선진화를 가져오기를 바란다.

V. 결론

전 세계적으로 IoT에 관한 관심이 높아짐에 따라 IoT시장이 확대되고 있으며, 그로 인한 국가적 차원에서의 IoT정책이 블루오션으로 자리잡게 되었다. 그러나 IoT가 안고 있는 위협요인들이 잠재되어 있다 보니, 그로 인한 개인정보 침해사고가 발생할 것이라는 불안감도 증가하고 있다. 이에 대해 IoT가 국가발전의 핵심과제로 요구됨과 동시에 필요한 보안기술과 대응체계도 필요한 실정이다. 일부 국가에서는 이에 대한 정책과제가 추진되고 있는데, 본 연구에서는 미국, 유럽, 중국, 일본 등 IoT를 위한 개인정보보호 및 정보보호계획, 관련 로드맵, 관련 가이드라인 등을 수립하여

추진하고 있다. 이에 따라 본 연구에서는 그동안 정의되고 제언되었던 정보보호에 관한 취약점 점검을 위한 원칙, 개인정보보호를 위한 연구 등을 통해서 IoT개인정보보호정책과제의 중요도 및 우선순위를 분석하고자 하였다. 이를 위해 전문가 대상의 FGI분석을 통해서 정책지표를 선정하였고, 전문가 66명의 AHP분석 결과로 정책지표의 중요도를 측정하고 그 결과의 신뢰성을 검증하였다.

이처럼 안전한 IoT서비스를 위한 개인정보보호정책의 분야별 중요도 및 우선순위에 따른 정책과제를 살펴보았는데, 첫째, 정책적 분야의 3개 정책영역에서는 IoT개인정보보호 법제도 강화(03133)가 가장 중요하며, 9개 정책지표에서는 IoT개인정보보호법률 제·개정추진(0.163)을 우선 추진하여야 한다. 둘째, 기술적 분야의 3개 정책영역 중에서는 IoT보안기술 개발 및 안전성 강화(0.1419)가 가장 중요하며, 8개 정책지표에서는 IoT보안기술의 개발 및 표준화(0.0976)가 가장 우선되어야 한다. 셋째, 관리적 분야의 3개 영역 중에서는 IoT생애주기별 개인정보보호조치 강화(0.0788)가 가장 중요하며, 8개 정책지표에서는 IoT서비스처리자의 정보주체 사전동의 및 고지의무 강화(0.0394)가 가장 우선되어야 한다. 이러한 정책지표에 관한 AHP분석의 일관성은 0.0620〈0.1로 검증되었으며, 각 영역과 지표에서도 적합함을 검증하였다. 물론, 본 연구의 3개 분야 9개 영역 25개 정책지표가 IoT개인정보보호를 포괄하는데 연구의 한계가 있었으며, 기존의 연구내용을 바탕으로 도출하다보니 IoT개인정보보호정책과제들의 범주화에도 제약이 있었다. 그러나, 종합적인 관점에서 IoT개인정보보호정책의 필요성과 연구의 발전을 가져올 것이다.

본 연구는 제4산업혁명을 주도하는 IoT가 국가적 차원에서 추진되기 위해서는 개인정보보호정책이 함께 진행되어야 함을 주장하였다. 즉, 국내외적으로 IoT와 관련하여 다양한 정보화정책을 추진함에 있어서 개인정보보호정책도 포함하여 추진되어야 하며, 본 연구에서 논의한 정책지표들은 현재 연구자들이 볼 때 중요하다고 제언한 과제이므로, 우선적으로 고려되어야 한다. 더욱이, 앞으로 새로운 연구가 지속되어지면 더 많은 보안이슈를 반영한 다양한 정책과제가 추진되어야 한다. 다만, 아직까지 IoT에 관한 개인정보보호에 관한 연구들이 많지 않기 때문에, 본 연구가 안전한 IoT서비스를 제공함에 있어서 필요한 개인정보보호정책지표로서 기준이 되고, 지속적인 연구와 정책개발의 근간이 되기를 기대한다.

■ 참고문헌

강남희 (2014). “사물인터넷 보안을 위한 표준기술 동향.” 「한국통신학회지(정보와통신)」, 31(9): 40-45.

개인정보보호위원회 (2014).「스마트기기 보급 확대에 따른 개인정보보호방안 연구-사물인터넷 환경을 중심으로」.

구태언 (2015). “IoT시대 개인정보보호를 위한 개인정보 정의/동의제도/시정제도 개선방안.” (2015. 4. 10. CPO Forum PGE 2015 발표수정).

권헌영 (2015).「사물인터넷 활성화를 위한 법적장애 개선방안구」. 한국경제연구원.

김동희·윤석웅·이용필 (2013). “IoT 서비스를 위한 보안.” 「한국통신학회지」, 30(8): 53-59.

김민식·이은민 (2014). “IoT기술 등장에 따른 기업 환경변화와 경쟁우위에 대한 고찰.” 「정보통신정책」, 26(16): 1- 18.

김민천 (2016). “우리나라의 개인정보 보호제도 분석: 인증 및 평가제도와 개인식별번호를 중심으로.” 「정보화정책」, 12(4): 38-58.

김범수 (2014).「스마트디바이드 확산에 따른 개인정보보호에 관한 연구」. 개인정보보호위원회.

김영훈·양준근·김학범 (2014). “M2M/IoT의 동향과 보안위협.” 「정보보호학회지」. 24(6): 48-59.

김인순 (2017). “시큐리티서밋 2017 “IoT기기 70%가 보안 위협 노출”.” 「보안뉴스」. 12월 19일.

김태형 (2014). “사물인터넷 보안, 어디서부터 손대야 하나?.” 「보안뉴스」. 11월 6일.

김형준 (2010). “사물간 통신 네트워크의 이해.” 「한국통신학회지(정보와 통신)」, 27(7): 21-28.

김호영·이경현 (2010). “사물통신 네트워크 보안 프레임워크에 관한 연구.” 한국멀티미디어학회 춘계학술대회 발표논문.

김호원 (2014). “사물인터넷 서비스에서의 보안 이슈.” 「정보과학회지」, 32(6): 37-41.
김호원·김동규. (2012). “IoT 기술과 보안.” 「정보보호학회지」. 22(1): 7-13.
나성현 (2015). “IoT환경에서의 개인정보보호 이슈.” 「KISDI Premium Report」. 정보통신정책연구원.
문남미·용승림·오정민·조태남 (2006). “디지털컨버전스에서의 서비스를 위한 개인정보보호 연구.” 「한국멀티미디어 학회지」, 10(4): 24-32.
미래창조과학부 (2014). 세계최고의 스마트 안심국가 실현을 사물인터넷(IoT) 정보보호 로드맵.
민경식 (2013). “사물인터넷.” 「Netterm」, 한국인터넷진흥원.
박미사 (2014). 「사물인터넷 활성화를 위한 법제도 개선방안」, 한국인터넷진흥원.
박지애 (2014). “삼성·LG ‘IoT 표준규격’ 동맹 맺고 글로벌 시장 주도한다.” 「파이낸셜뉴스」. 11월 14일.
박지예·신새미·강남희 (2013). “사물인터넷 환경에서 경량화 장치간 상호인증 및 세션키 합의기술.” 「한국통신학회논문지」, 38(9): 707-714.
방민석·오철호 (2014). “개인정보 연구동향과 과제.” 「정보화정책」, 21(1): 3-16.
보안뉴스 (2014). “사물인터넷 보안위협에 따른 대응과제 7가지.” 10월 23일. http://www.boannews.com/media/view.asp?idx=43634&kind=3 (검색일: 2017. 08. 04).
산업연구원 (2014). “IoT 시장규모”; Design LOG. (2014. 7. 9). “사물인터넷 가전관련 특허 아이디어, 신제품으로 속속 출시.” http://www.designlog.org/2512482 (검색일: 2018. 05. 03).
서화정·이동건·김지현·최종석·김호원 (2014). “사물인터넷 상에서의 보안과 프라이버시 보호 이슈.” 「정보처리학회지」, 21(2): 48-60.
서화정·이동건·최종석·김호원 (2013). “IoT 보안 기술 동향.” 「電磁波技術」, 24(4): 27-35.
수자환. “AHP(계층분석법).” http://eias.tistory.com/26 (검색일: 2018. 08. 04).
신영진 (2015). “IoT시대에서의 개인정보보호정책과제에 관한 연구.“ 한국정책학회 하계학술대회 발표논문.
신영진 (2016). “IoT시대에서의 개인정보보호정책에 관한 연구.” 한국행정학회 하계학술대회 발표논문.
신영진 (2017). “안전한 IoT서비스 체계 구축을 위한 개인정보보호정책지표 개발에 관한 연구.” 한국행정학회 동계학술대회 발표논문.
심우민 (2015). “사물인터넷(IoT) 개인정보보호의 문제점과 입법적 대응방안.” 「이슈와 논점」. 국회입법조사처.
원병철 (2017). “2018년 사이버 공격자들은 IoT 기기 노린다.” 「보안뉴스」. 12월 6일.
유한종 (2013). “SW Insight 리포트.” 「정보통신산업진흥원」.
윤보현 (2015). “사물인터넷, 전 세계 경제 11% 비중 차지할 전망” 「한국뉴스투데이」. 7월 8일. http://koreanewstoday.co.kr/detail.php?number=44350 (검색일: 2017. 08. 04).
윤영석·조성균·이현우 (2016). “사물인터넷 신뢰연구와 시사점: EU FP7을 중심으로.” 「정보화정책」, 23(1): 56-73.
윤주상·최영환·홍용근 (2014). “사물인터넷을 위한 IETF 표준화 기술 동향.” 「한국통신학회지」, 31(9): 32-39.
윤현기 (2014). “미래부, 안정한 IoT 환경 조성을 위한 ‘사물인터넷 정보보호 로드맵’ 수립.” 「IT Daily」. 11월 1일.
이경민 (2016). “이정원 ICTK 부대표 “IoT 발전 위해 정보보호 정책 시급.” 「전자신문」. 11월 28일.
이동혁·박남제 (2017). “안전한 IoT 환경을 위한 기술 및 정책적 사후 보안관리 프레임워크.” 「한국정보기술학회논문지」, 15(4), 127-138.
이민영 (2012). 「해외의 개인정보보호체계와 개인정보보호 동향 조사」. 개인정보보호위원회.
이부연 (2014). “IoT 보안 위협 현실화…사이버테러 대란 경고: 전국 인터넷 서비스 마비시켜, 2020년 피해 17조원 예상.” 「아이뉴스」. 12월 7일.
이상호·조윤영 (2015). “사물인터넷시대 국가 사이버안보 강화 방안 연구.” 「정치정보연구」, 18(2): 1-30.
이애리·손수민·김현진·김범수 (2016). “사물인터넷(IoT) 환경에서 개인정보보호 강화를 위한 제도개선 방안.” 「정보보호학회논문지」, 26(4): 995-1012.
이야리·김정숙 (2014). “IoT 환경에서의 개인정보보호 프레임워크.” 한국콘텐츠학회 종합학술대회 발표논문: 277-278.
이우권 (2015). “사물인터넷(IoT)에서 개인정보보호의 이슈와 대안.” 「한국자치행정학」, 29(4): 215-234.
이준복 (2015). “사물인터넷시대에서 정보인권 보장을 위한 법적 고찰.” 「홍익법학」, 16(3): 85-114.
장현수·김현진·손태식 (2015). “Industrial IoT 환경의 사이버보안 이슈 연구.” 「한국정보보호학회지」, 25(5): 12-17.

전자신문 (2014). “사물인터넷 정보보호 로드맵 무얼 담았나”. 10월 30일. http://www.etnews.com/20141030000271(검색일: 2018.06.16).
전해영 (2016). “사물인터넷(IoT) 관련 유망산업 동향 및 시사점.” 「VIP REPORT」 16-24: 1-12. 서울: 현대경제연구원.
정보통신기술진흥센터 (2015). “중국의 사물인터넷 산업 활성화 정책과시장 경쟁 구도.” 해외 ICT R&D 정책동향(동향보고서). 1: 1-11.
정현미·정기문·조한진 (2017). “IoT(Internet of Things) 시스템 미들웨어 보안기능요구사항 설계.” 「한국융합학회논문지」, 8(11): 63-69.
좋은정보사 (2017). 「사물인터넷(IoT)/산업용 사물인터넷(IoT) 기술·보안 동향 및 유망산업 분석과 관련업체 추진전략」.
최경진 (2015). “빅데이터·사물인터넷 시대 개인정보보호법제의 발전적 전환을 위한 연구.” 「중앙법학」, 17(4): 7-50.
한국인터넷진흥원 (2007). 「RFID 개인정보보호가이드라인」. 서울: 한국인터넷진흥원.
한국인터넷진흥원 (2010). 「침해사고 분석절차 안내서」. 서울: 한국인터넷진흥원.
한국인터넷진흥원 (2012). “사물인터넷의 시장 정책동향 분석.” 「인터넷&시큐리티 이슈」. 서울: 한국인터넷진흥원.
한국인터넷진흥원 (2014). “미국 연방거래위원회, 연방정부 차원의 사물인터넷 균형 발전 모색.” 「인터넷 및 정보보호동향」.
한국인터넷진흥원 (2015a). 「IoT 제품 및 서비스 보안성 강화방안 연구」. 서울: 한국인터넷진흥원.
한국인터넷진흥원 (2015b). 「IoT 디바이스 보안인증 기반 연구」. 한국인터넷진흥원.
한국인터넷진흥원 (2016). 「IoT 공통보안 가이드」. 나주: 한국인터넷진흥원.
한국인터넷진흥원 (2017). “KISA, IoT산업 활성화를 위한 보안내재화 확산 추진.” 4월 17일 보도자료.
한국일보 투데이 (2015). “사물인터넷, 세계경제 11%.” 7월 8일.
한진주 (2016). “내년 국가정보화사업에 5조2000억 투입한다.” 「아시아경제」. 12월 27일.
홍범석 (2013). “개인정보보호 관련 규제체계와 주요 이슈.” 「정보통신방송정책」, 25(22): 47-86.
홍승필·장현미·김경진·김혜리·박수민 (2015). 「IoT환경에서 개인정보보호 이슈 발굴 및 정책제언에 관한 연구」. 한국인터넷진흥원.
Cavoulkian, Ann (2011). “Privacy by Design: The 7 Foundational Principles.” Information and privacy commissioner of Ontario. http://www.soumu.go.jp/main_content/000196321.pdf. (Retrieved on Aug. 10, 2018)
Former FTC Conference Center (2013). *Internet of Ihings: Privacy & Security in a Connected World.*
Google. “Change of interests in IoT and privacy in 5years. https://trends.googleco.kr/trends/explore?date=today%205-y&q=Internet%20of%20Things,privacy (Retrieved on Aug. 04, 2017).
Jara, Antonio. J., Kafle, Ved P & Skarmeta, Antonio F. (2013). “Secure and scalable mobility management scheme for the internet of things integration in the future internet architecture.” *International Journal of Ad Hoc Ubiquitous Computing*, 13(3-4): 228 - 242.
Jinshu, Cao, Dan, Zhao, Baokang, Wang, Xiaofeng, & You, Ilsun (2014). “ePASS: An expressive attribute-based signature scheme with privacy and an unforgeability guarantee for the internet of things.” *Future Generation Computer Systems*. 33: 11 - 18.
Kang, Kai, Pang, Zhi-bo & Wang, Cong (2013). Security and privacy mechanism for health internet of things, J. China Universities Posts Telecommun. 20 (SUPPL-2): 64 - 68.
KOTRA 뉴스 (2017). “일본 4차 산업혁명 대비 산학관 합동 IOT 인재육성,” 2월 27일. http://news.kotra.or.kr/user/globalAllBbs/kotranews/list/2/globalBbsDataAllView.do?dataIdx=157354(검색일: 2018.05.03).
Li, Shancang & Xu, Li Da (2017). *Securing the internet of things*. Acorn publishing Co.
McKinsey Global Institute (2015). *The Internet of Things: mapping the value beyond the hype.* McKinsey & Company.
Middleton, Peter Kjeldsen, Peter & Tully, Jim (2013).

Forecast: The Internet of Things, Worldwide, 2013. Gartner Inc. https://www.gartner.com/doc/2625419?ref=mrktg-srch. (Retrieved on Sep. 09, 2018).

Niu, Ben, Zhu, Xiaoyan, Chi, Haotian & Li, Hui (2014). Privacy and authentication protocol for mobile rfid systems, *Wireless Personal Communication Proceeding*, 77(3): 1713 - 1731.

OWASP (2017). *OWASP Top 10-2017*. Creative Commons https://www.owasp.org/index.php/Main_Page. (Retrieved on Sep. 09, 2018).

Shin. Young-Jin (2017). A Study on Privacy Protection Policy for Safe IoT Service. *2017 EECS Proceeding.*

Shin. Young-Jin (2018). A Study on e-Privacy Policy Index for Safe IoT Service. 2018 APICENS Proceeding.

Sicari, Sabrina, Cappiello, Cinzia, Pellegrini, Francesco De, Miorandi, Daniele, & Coen-Porisini, Alberto (2014) "A security-and quality-aware system architecture for internet of things." *Information Systems Frontiers*. 18(4): 665-677.

Sicari, Sabrina, Rizzardi, Alessandra, Grieco, Luigi Aftredo, & Coen-Porisini, Alberto (2015). "Security, privacy and trust in Internet of Things : The road ahead." *Computer Networks*. 76: 146-164.

Symantec (2013). *2013 internet security threat report.*

Symantec (2015). *2015 internet security threat report.*

Ukil, Arijit, Bandyopadhyay, Soma & Pal, Arpan (2014). "IoT-privacy: To be private or not to be private." *IEEE INFOCOM 2014 proceeding*: 123 - 124. https://www.researchgate.net/publication/269297802_IoT-Privacy_To_be_private_or_not_to_be_private (Retrieved on Aug. 23, 2018).

Wang, Xiniel, Zhang, Jianqing & Schooler, Eve M. (2014). "Performance evaluation of attribute-based encryption: Toward data privacy in the IoT." 2014 IEEE International Conference on Communications (ICC) Proceeding: 725 - 730.

Wright, Andrew (2009). "Cyber security for the power grid: cyber security issues & Securing control systems." *ACM CCS Proceeding*.

Yan, Tao & Wen, Qiaoyan (2010). "A secure mobile rfid architecture for the internet of things." 2010 IEEE International Conference on Information Theory and Information Security Proceeding: 616 - 619.

Yang, Jin-cui & Fang, Bin-Xing (2011). "Security model and key technologies for the internet of thing." *The Journal of China Universities of Posts and Telecommunications*. 18(2): 109 - 112.

https://trends.google.co.kr/trends/explore?date=today%205-y&q=Internet%20of%20Things,privac (Retrieved on May. 03, 2018).

https://www.mckinsey.com/featured-insights/internet-of-things/our-insights/the-future-of-connectivity-enabling-the-internet-of-things (Retrieved on May. 03, 2018).