Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.4, Aug. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.4.995

사물인터넷(IoT) 환경에서 개인정보보호 강화를 위한 제도 개선 방안

이 애 리,[1†] 손 수 민,[1] 김 현 진,[2] 김 범 수[3‡]
[1]연세대학교 바른ICT연구소, [2]한국신용정보원, [3]연세대학교 정보대학원

Improving Personal Data Protection in IoT Environments

Ae Ri Lee,[1†] Soomin Son,[1] Hyun Jin Kim,[2] Beomsoo Kim[3‡]
[1]Barun ICT Research Center, Yonsei University,
[2]Korea Credit Information Services,
[3]Graduate School of Information, Yonsei University

요 약

IoT 환경에서는 사람들이 인지할 수 없는 다수의 사물들이 자율적으로 데이터를 수집하고 수집된 데이터들은 네트워크를 통해 서로 결합되고 공유될 수 있다. 이로 인해 IoT 상에서는 개인정보보호 측면에서 기존의 IT 환경 대비 새로운 도전 과제들이 존재하게 된다. 본 연구는 IoT 환경에서 발생 가능한 개인정보보호 관련 이슈를 파악하고 이에 대한 대응 방안을 제안하는 것을 목적으로 한다. 본 연구에서는 IoT에서의 다양한 개인정보처리자의 유형들을 분석하고, 개인정보처리자 측면과 정보주체 권리 및 개인정보보호 측면에서의 주요 이슈를 도출하였다. 분석된 이슈를 바탕으로 필요한 제도적 개선 방안(사용자 친화적 고지방안 및 탄력적 동의제도 마련, 개인정보 재식별 위험 모니터링 체계 정립, 국외이전 개인정보보호 표준계약제도 수립, 이용자 교육 강화 등)을 제안하고, 개선안들에 대한 시급성과 중요도를 검토하여 우선적으로 추진해야 할 개선과제가 무엇인지 제시하였다.

ABSTRACT

In Internet of Things (IoT) environments, devices or sensors everywhere can automatically collect data without the individual awareness, further combine and share data using ubiquitous network, and thus the development of IoT raises new challenges in respect of personal data protection and privacy. This study aims to identify main issues related to data protection in the IoT and propose adequate measures. We analyzed the types of personal data controllers and processors in IoT and figured out the issues regarding the processing of personal data and the rights to privacy of data subject. Accordingly, we suggested the institutional ways (e.g., establishment of user-friendly notice and flexible consent system, re-identification risk monitoring system, data protection in cross-border transfer, and user education) to improve the situation of personal data protection in IoT and finally proposed the improvement tasks to carry out first based on the degree of urgency and importance.

Keywords: IoT, Personal Data Protection, Right of Data Subject, Data Controller, Data Processor

I. 서 론

정보통신기술(Information and Communications Technologies, ICT)의 비약적인 발전과 함께 사물인터넷(Internet of Things, IoT) 시대가 도래하고 있다. IoT란 "기기 및 사물에 통신 모듈이 탑재되어, 유무선 네트워크로 연결됨으로써 사람과 사물 간, 사물과 사물 간에 정보 교환 및 상호 소통할 수 있는 지능적 환경"으로 정의될 수 있다[1][2]. 세

Received(06. 16. 2016), Accepted(07. 29. 2016)
† 주저자, arlee12@naver.com
‡ 교신저자, beomsoo@yonsei.ac.kr(Corresponding author)

계적인 연구조사기관인 Gartner에서는 IoT를 2016년을 움직일 10대 기술 중 하나로 선정하였고[3], 인터넷에 연결된 사물의 수가 2020년까지 약 208억 개로 확대될 것으로 예상하고 있다[4]. 이러한 IoT 환경에서는 사람들이 인지할 수 없는 다수의 사물들이 자율적으로 데이터를 수시로 수집하고 수집된 데이터들은 네트워크를 통해 서로 결합, 공유될 수 있다. 이로 인해 IoT 환경에서는 개인정보 보호 측면에서 전통적인 환경 대비 다양한 도전 이슈들이 존재할 수 있다. 예를 들어, IoT에서는 자동적인 수집 능력을 갖춘 수많은 기기로부터 개인정보가 수집되고 이용될 수 있는데, 이는 기존 대비 양적인 측면의 증가뿐만 아니라 수집 가능한 정보의 종류도 더욱 다양해져 개인의 습관, 취향, 이동 경로 등의 민감하고 세밀한 개인정보들이 포함될 수 있다. 특히 IoT가 확산됨에 따라 증가한 정보 원천으로부터 수집된 데이터들이 서로 결합되고 데이터 마이닝 및 빅데이터 분석을 통해 개인별 프로파일링(profiling)과 추적(tracing) 등이 용이해질 수 있어 개인정보보호 및 프라이버시 침해에 대한 위험이 증가할 수 있다. 또한 IoT 환경에서는 개인들이 원치 않거나 비합법적인 데이터 프로세싱이 일어날 수 있는 가능성이 증가할 수 있고, IoT 서비스 사업자의 입장에서도 데이터 수집에 대해 일일이 개인에게 사전 동의를 받거나 이벤트 발생 시마다 개인들에게 매번 알리는 것이 여의치 않을 수 있다. 개인정보보호 관련 이슈들은 데이터 수집에서부터 저장/관리, 이용/제공, 그리고 파기까지의 라이프사이클(Life Cycle)에 따라 존재할 수 있는데, 이러한 데이터 라이프사이클 관점에서 기존 IT 환경 대비 IoT 환경에서 발생할 수 있는 이슈를 비교 정리하면 Table. 1과 같다.

IoT의 발전은 개인정보 및 프라이버시 보호와 관련하여 새롭고 중대한 도전 과제를 제기하고 있다[4]. IoT 환경에서 개인에 대한 데이터가 제대로 보호되고 통제되지 못할 경우, 개인들의 정보 프라이버시 염려는 증가하게 되고, 새로운 가치의 신규 서비스를 개발하여 제공하려하는 IoT 사업자들은 자칫하면 프라이버시를 침해하는 불법적인 형태의 서비스를 제공하게 될 수 있다. 이로 인해 IoT 환경에서의 건전한 개인정보 활용이 저해될 수 있고, IoT 서비스 발전 및 확산이 지연될 수 있다.

본 연구는 IoT 환경에서 발생가능한 개인정보보호 관련 이슈를 파악한 후 이에 대한 적절한 대응 방안을 제안하는 것을 목적으로 한다. 우선, IoT 상에서의 개인정보보호에 대한 문제점을 고찰하기 위해서는 IoT의 가치사슬 및 생태계를 이해하고 특히 개인정보를 수집하고 처리하는 주요 개인정보처리자가 어떤 유형이 있는지 파악할 필요가 있다. 본 논문의 2장에서는 이러한 개인정보처리자의 유형들을 분석하고, 3장에서는 IoT 환경에서의 개인정보 관련 주요한 쟁점 이슈가 무엇인지 도출하였다. 특히 개인정보처리자 측면과 정보주체 권리 및 개인정보보호 측면에서의 주요 이슈를 파악한 후, 4장에서는 IoT 환경에서의 개인정보보호 강화를 위해 필요한 제도적 개선방안을 제시하였다. 5장에서는 제시된 개선방안들에 대한 시급성과 중요도를 분석하여 우선적으로 추진해야 할 개선방안이 무엇인지 제언하였다. 끝으로 6장에서는 본 연구의 결과를 정리하였다.

II. IoT 환경에서의 개인정보처리자 유형

IoT 상에서 개인정보 수집부터 이용, 제공, 처리, 분석 등 일련의 과정을 통해 정보주체 또는 사용자에게 서비스되는데 있어 다양한 유형의 개인정보처리 참여자들이 존재한다. 개인정보보호법에서는 정보주체와 개인정보처리자의 관계를 설정하고 정보주체의 권리를 보장하기 위해 개인정보처리자를 규율한다. IoT 환경에서 개인정보보호 관련한 이슈 및 제도적 개선점을 파악하기 위해 우선 IoT 가치사슬에 참여하는 개인정보처리자 유형에 대해 분석하였다. 본 연구에서는 EU의 제29조 데이터 보호 작업반(Article 29 Data Protection Working Party)의 IoT 발전에 따른 의견서[5]를 바탕으로 IoT 상의 개인정보처리자 유형을 구분하였다.

2.1 디바이스 제조자

IoT 환경에서 디바이스 제조자는 서비스 이용자 및 정보주체, 또는 다른 기관에게 관련 기기나 제품을 판매하는 것 이상의 역할을 할 수 있다. 디바이스 제조자들은 단순히 제품의 제조를 넘어 사물의 운영체계를 개발 및 수정할 수 있으며, 기기에서 센싱되어 수집되는 개인정보 및 빈도와 더불어 개인정보 데이터가 언제 누구에게 어떠한 목적을 위해 전송될지에 관한 전반적인 기능을 가진 소프트웨어를 탑재할 수 있다. 예를 들어, 센서가 부착된 핏빗(Fitbit)과 같은 스마트 헬스케어(smart healthcare) 디바이스 제조사는 기기의 추적 장치에 의해 기록된 개인의

Table 1. Issue regarding Personal Data Protection in IoT Environment Compared with Traditional IT

Data Life Cycle	Traditional IT Environment	IoT Environment
Collection	- Prior notice and consent are required	- IoT devices automatically collect data, leading to constrains on prior notice and consent of data subjects
Storage/ Management	- Personal data is stored and managed in local network servers	- Storage and management points in IoT devices and sensors increase - The amount of personal data stored and managed increase - Threats of possible breach of personal data increase
Usage/ Provision	- Personal data is used and provided domestically - Target and rule regarding prohibition of secondary use of personal data are clear	- Cross-border transfer of personal data is frequent - Possibility of secondary use of personal data increase through data integration and big data analysis - Possibility of identification of unidentifiable data increase
Erasure	- Known personal data controller erases the data	- Increased collaboration between IoT service providers increases personal data sharing. Ambiguity of data controller responsibility to erase also increases
Common issue in Life Cycle	- Personal data controller can be clearly identified	- Types of personal data controller are diverse - Classification of data controller per each IoT service is necessary

건강 데이터를 기반으로 사용자에 대한 보험 가격을 측정할 수 있는데, 이와 같은 경우 보험사에게 사용자의 신체나 건강과 관련된 민감 정보를 제공하게 될 수도 있다[6].

2.2 소셜 플랫폼 서비스 제공자

서비스 이용자는 정보주체로서 자신의 개인 데이터를 공개하거나 다른 이와 공유할 수 있을 때 IoT 서비스를 더욱 활발히 이용하게 된다. 특히 IoT 서비스 이용자는 자신이 속한 커뮤니티 그룹에서 자신의 원하는 이미지를 잘 나타냄으로써 긍정적인 경쟁 우위를 조성하기 위해 소셜 네트워크 상에서 다른 사람에게 자신의 개인정보를 공유한다. 또한 사용자가 소셜 네트워크 서비스의 설정을 바꾸지 않는 이상 일반적으로 디바이스 제조자가 제공하는 어플리케이션 속에서 정해진 표준 세팅을 따르게 되어 사용자의 개인정보가 자동적으로 공유되어 질 수 있다. 따라서 IoT 기기 제품과 연계된 소셜 네트워크 서비스 사업자는 방대한 개인정보를 수집하고 처리할 수 있고, 개인정보보호에 대한 책임이 발생하게 된다. 2.1에서 예로 언급한 스마트 헬스케어 기기 이용자의 경우, 카카오스토리, 페이스북, 인스타그램, 트위터와 같은 소셜 네트워크 서비스나 디바이스 제조사가 별도 제공하는 소셜 플랫폼 서비스 등을 통하여 커뮤니티 내 특정인들과 건강 관심사 교환 및 경쟁 등의 목적으로 자신의 건강 정보를 공유할 수 있다.

2.3 어플리케이션 개발자

디바이스 제조자가 제공한 제품을 사용하거나 저장된 데이터에 접근하기 위해서 이용자(정보주체)는 별도의 어플리케이션(앱) 또는 소프트웨어 등을 설치할 필요가 있다. 앱 개발자는 이러한 앱을 운영하면서 IoT 디바이스의 센서로부터 수집되는 개인정보를 모으고 처리할 수 있게 된다. 이러한 앱이나 소프트

웨어는 대게 정보주체로부터 사전 동의를 받는 옵트인(opt-in) 기반으로 탑재되는데, IoT 환경에서 어플리케이션 개발자들이 정보주체에게 충분한 고지 및 동의를 구하기 위해 적절한 정보와 적합한 메커니즘이 제공되고 있는지에 대해서는 현재 논란의 여지가 있다.

2.4 IoT 데이터 플랫폼

IoT 데이터 운영의 표준화와 상호운용성이 미흡할 경우 IoT 참여자들 각각은 자신만의 인터페이스와 데이터 형태를 정의하게 된다. 이 경우 데이터는 같은 표준 환경이나 폐쇄된 환경 속에서만 전송되어져 기기 간의 효과적인 데이터 연결이나 조합이 어려워 질 수 있다. 지금까지는 주로 스마트폰이나 태블릿 PC 등이 IoT 기기에 부착된 센서를 통해 수집된 데이터를 인터넷으로 연결해주는 게이트웨이의 역할을 하였다. 일례로, 스마트 헬스케어 기기를 통해 수집된 데이터는 이를 관리해주는 앱이 설치된 스마트폰을 통해 제조사나 서비스 제공자의 서버와 연결되어 이용자의 자가 관리가 가능해진다. 이 경우 스마트폰이 헬스케어 기기를 통해 수집된 정보주체의 데이터에 대한 게이트웨이 역할을 하게 된다.

또 다른 측면에서는 IoT 데이터 관리의 집중화와 단순화를 위해 서로 다른 기기를 통해 수집되는 데이터를 호스팅할 수 있는 새로운 유형의 플랫폼이 개발되고 발전하고 있다. 이들 데이터 플랫폼 제공자는 다양한 IoT 센싱 기기로부터 수집되는 수많은 개인정보를 보유하고 처리할 수 있기 때문에, IoT 상의 개인정보보호 측면에서 관심을 가져야 할 개인정보처리자가 될 수 있다.

2.5 기타 참여자

디바이스 제조자나 앱 개발자 이외에 또 다른 제3의 참여자가 IoT 기기를 통해 개인정보를 수집하고 처리할 수 있다. 예를 들어, 건강보험업자는 계보기(만보기)를 고객들에게 나눠주고 그들이 얼마나 자주 운동하는지 모니터링 하여 이에 기반 한 보험 프리미엄을 산정할 수 있도록 개인별 데이터를 확보할 수 있다. 이러한 제3의 참여자들은 다른 개인정보처리자와 달리 사물에 의해 수집된 개인정보를 통제할 권한은 없으나, 그들의 설정한 특정 목적에 따라 IoT 기기에 의해 생성된 개인 정보를 수집하고 저장하도록 처리할 수 있다.

III. IoT 환경에서의 개인정보보호 주요 이슈

본 장에서는 IoT 및 개인정보보호와 관련한 국내외 법·제도 분석과 기존 문헌 연구 조사를 바탕으로 개인정보보호 측면에서 이슈화 될 수 있는 주요 쟁점 사항들을 도출하였다.

3.1 개인정보처리자 관련 이슈

개인정보처리자는 개인정보보호법 제2조 정의에 따라 "업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등"을 말한다[7]. 2장에서 분석된 5가지 유형의 참여자들은 모두 자신의 업무를 목적으로 IoT 센서로부터 수집 및 처리되는 개인정보와 이들 정보의 집합인 개인정보파일을 운용하는 자로서 개인정보보호법 상의 개인정보처리자에 해당된다. 단, IoT 환경에서 이들 개인정보처리자는 이전의 전통적인 IT 환경 하에서의 법적인 의무와 책임을 기반으로 규율하고 통제하기 힘들 수 있다. IoT 상에서 야기될 수 있는 개인정보처리자와 관련된 이슈사항은 다음과 같다.

첫째, 개인정보보호법 제3조 5항에서 "개인정보처리자는 개인정보의 처리에 관한 사항을 공개하고 열람권 등 정보주체의 권리를 보장해야 함"을 명시하고 있는데[7], IoT 상에서 하나의 서비스(예: 스마트 헬스케어, 스마트 홈, 스마트 커뮤니케이션, 스마트 시티 등)를 제공하는데 있어 여러 개의 개인정보처리자들이 동일한 개인정보를 처리해야 할 경우는 이중 어떤 개인정보처리자가 정보주체의 권리를 보장하는 역할을 담당해야 하는지가 명확하지 않을 수 있다. 또한 다수의 IoT 디바이스를 통해 수집된 개인정보를 여러 개의 개인정보처리자가 공유할 경우, 개인정보 유출 통지에 대한 의무[7]를 담당하는 자가 누구인지에 대해 혼선이 생길 수 있다. 이로 인해 개인정보보호법 제34조[7] 상 정보주체에게 통지되어야할 사항(유출된 개인정보 항목, 유출 시점 및 경위, 피해 신고 접수 담당부서 및 연락처 등)과 통지 시점, 피해 최소화 및 대응조치 등이 제대로 처리되는데 있어 문제가 초래될 수 있다.

둘째, IoT 서비스의 확산에 따라 개인정보처리자 역할을 하는 새로운 유형의 "유사 개인정보처리자"가

등장할 수 있다. 예를 들어, 스마트 글래스 기기에 해당되는 구글 글래스와 같은 착용형 영상정보 기기의 경우, 기기를 이용하는 당사자의 정보를 수집하고 처리하지만, 이용자 주변의 다른 정보주체에 대한 개인정보 또한 수집할 수 있다[8]. 실제 영국 정보보호위원회(Information Commissioner's Office, ICO)에서는 구글 글래스를 통해 사용자가 사전 허가 없이 다른 이의 영상 및 사진을 촬영하여 프라이버시를 침해할 수 있다고 지적하였다[9]. 이 경우 해당 IoT 서비스 이용자(가입자)가 아닌 전혀 다른 사람의 프라이버시 유출과 관련된 문제점이 발생할 수 있다. 개인정보보호법 제2조 2항에 의하면, 정보주체는 "처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람"으로 정의되어 있다[7]. 구글 글래스 사례에서 정보주체는 기기 이용자가 아닌 서비스 이용자가 착용한 기기로부터 수집되는 주변의 사람이 될 수 있다. 이러한 경우 IoT 기기 이용자를 개인정보처리자라고 할 수 있는지 생각해 볼 필요가 있다. 구글 글래스 사용자가 개인 공간 및 가정 내 정보만을 수집하거나 업무 목적이 아닌 개인의 사적 용도로 사용할 경우는 개인정보보호법의 적용을 받지 않지만, 이 기기를 활용하여 마케팅 지원 등의 사업적 목적으로 활용될 경우는 해석이 달라질 수 있다[9]. 이와 같이 구글 글래스, 드론 등 영상촬영이 가능한 이동형 IoT 기기가 확산됨에 따라 이러한 IoT 기기 사용자들에 대한 올바른 통제가 이뤄지지 않을 경우, 원치 않는 정보주체의 개인정보가 수집/공유되어 프라이버시 침해 사고가 발생할 수 있다. 이 경우 피해를 입은 정보주체의 피해 보상 및 구제는 어떠한 개인정보처리자가 담당해야 하는 지에 대해 논쟁이 야기될 수 있다.

3.2 정보주체 권리 및 개인정보에 대한 이슈

3.2.1 정보의 편재성으로 인한 정보주체의 자기통제권 상실 가능성 증가

IoT는 편재성(ubiquity)의 특징을 가지고 있다. 편재성이란 모든 곳에 존재하는 옴니 프레즌스(omnipresence)의 개념으로 IoT에서는 겉으로 드러나지 않고 스며드는(pervasive) 형태의 편재된 서비스가 제공되어, 정보주체 자신이 인지 못하는 사이에 개인정보처리자에 의해 개인정보가 수집될 수 있다[10]. 즉, IoT 환경에서는 사람이 정확히 인식하지 못한 상태에서 사물과 사물 간, 사물과 시스템 간 자동적인 데이터 통신과 상호작용이 빈번하게 발생하여 다수의 주변 사물들의 활성화 상태(활성 또는 비활성)를 정보주체가 일일이 확인하기 힘들어진다. 이로 인해 과거의 전통적인 IT 환경 대비 IoT 환경에서는 정보주체의 권리(본인의 개인정보처리에 대한 정보를 제공받을 권리, 개인정보 처리에 대한 동의여부와 동의 범위를 선택하고 결정하는 권리 등)를 적절한 수준으로 보장하기가 힘들 수 있고, 원치 않는 개인정보 유통과 과도한 프라이버시 노출에 대한 위험이 증가할 수 있다[11]. 결과적으로, 편리하고 개인화된 IoT 서비스가 제공되는 환경의 이면에는 정보주체가 자신에 대한 정보의 공개와 유통을 스스로 결정하고 통제할 수 있는 개인정보 자기통제권의 상실 가능성이 높아질 수 있는 이슈가 있다.

3.2.2 목적 외 이용 가능성 증가, 사전 동의제도 한계

IoT의 센서 기기로부터 수집된 수많은 개인정보는 개인정보처리자에 의해 정해진 최초 수집 목적과 다른 방향으로 활용되거나 다른 의미를 추론하는데 사용될 수 있다. IoT 기기(예: 스마트 커뮤니케이션 기기, 스마트 헬스케어 기기, 스마트 홈 기기 등)를 통해 처음 수집된 원천 정보로부터 개인의 습관 및 생활 패턴 등의 다른 의미를 추론하는데 사용될 수 있는데, 이로 인해 새로운 프라이버시 침해 위험이 야기될 수 있다. 예를 들어, IoT 환경에서의 각종 상황인지 센서나 웨어러블 디바이스들은 정보주체의 움직임과 같은 단순한 데이터를 수집하는 기초적인 센싱을 하지만, 수집된 데이터들을 종합하여 각종 분석 알고리즘을 통해 분석해 나가면 정보주체의 신체와 관련된 민감한 개인정보가 추출될 수 있다. 최초 서비스 이용 시 기기 사용자가 특정 목적에 대한 개인정보 사용을 허락했다 하더라도, 완전히 다른 목적을 위한 이차적 개인정보의 처리는 원하지 않을 수 있다. 따라서 현재 개인정보보호법을 개정하지 않는 범위 내에서, IoT 상의 개인정보처리자가 이용자에게 고지하는 최초의 처리 목적에 해당하는 개인정보만 이용하도록 제한할 필요가 있다. 또한 대부분의 경우 이용자는 특정 사물에 의해 수집된 개인 데이터의 처리에 대해 명확하게 인지하지 못하여 개인정보보호법에서 규정하고 있는 유효한 동의를 입증하는데 어려움이 있을 수 있다. 개인정보보호법 제15조 2항에 의하면 개인정보처리자는 정보주체에게 해당 개인

정보의 수집 이용 목적, 수집 항목, 보유 및 이용기간, 수집 동의 거부 시 불이익 내용 등을 알려야 하며, 이 중 어느 하나가 변경되는 경우 이를 알리고 동의를 받아야 함을 명시되어 있다[7]. 또한 개인정보보호법 제22조에서 개인정보처리자는 정보주체의 동의를 받을 때에는 동의가 필요한 개인정보를 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각 동의를 받아야 함을 명시하고 있고[7], 개인정보보호법 시행령 제17조에 따르면 개인정보처리자는 동의의 결과로 정보주체의 동의 표시가 서면 등의 방법으로 확인되어야 한다[12]. IoT 환경에서는 각종 센서 기기들에 대한 개인정보의 수집 및 이용목적이나 수집 항목, 보유 및 이용기간 등을 정보주체에게 명확하게 제시하기 어려울 수 있으며, 설령 해당 내용을 제시했다하더라도 수집된 개인정보를 통해 새로운 서비스를 구현할 가능성이 높다. 또한 IoT 서비스의 개인정보처리자가 수집된 개인정보들을 활용하여 신규 부가 서비스 제공 등의 변경사항이 발생할 경우 모든 정보주체로부터 새로운 동의를 구하기는 사실상 매우 힘들 수 있다. 따라서 기존의 전통적인 개인정보 제공에 대한 동의 획득 메커니즘을 IoT 환경에 적용하는데 한계가 있을 수 있고, 결과적으로 정보주체 개인의 선호에 따른 조정된 동의를 제공하는 것은 사실적으로 불가능할 수 있으므로 기존의 법/제도를 그대로 IoT 환경에 적용할 경우 오히려 "저품질 동의"가 만발되는 문제가 발생할 수 있다.

3.2.3 IoT 환경에서 정보 공유 확대에 따른 개인정보의 재식별화 우려 증대

IoT를 통해 수집된 각종 개인정보들은 서비스 제공 과정에서 다양한 참여자들을 통해 공유되고 활용될 수 있는데. 이 과정에서 개인정보의 재식별화 가능성이 기존 환경 대비 높아질 수 있다. 재식별화란 데이터 비교, 연계, 결합 등을 통해 특정 개인을 알아볼 수 있도록 하는 것을 말한다[13]. IoT 상에서 수집된 개인정보가 그 하나로는 개인을 식별할 수 없도록 데이터 마스킹(data masking), 가명처리(pseudonymisation), 총계처리(aggregation) 등의 비식별 과정을 거쳤다고 하더라도 다른 정보와 결합하여 재식별될 수 있는 가능성이 높아질 수 있다[14]. 비식별화된 정보의 재식별 가능성과 그에 대비한 식별요소 제거 기술 등에 대한 것은 빅데이터 분석 기술의 고도화와 함께 지속적으로 논의되어 왔으나, 수집/공유되는 데이터의 양 증가와 데이터 분석 기술의 진일보로 인하여 개인정보의 재식별화 위험을 원천적으로 제거하는 것은 사실상 힘들다. 더구나 IoT의 주요 특징인 "센싱의 일상화"는 개인의 특징을 전체 또는 부분적으로 파악할 수 있는 정보의 공유량을 기하급수적으로 증가시킬 수 있고, 이에 따라 개인을 식별해 낼 가능성이 더욱 높아질 수 있다. 이러한 재식별화 위험성 증가는 스마트 헬스케어와 같은 특정 분야에서만 존재하는 것이 아니라 서로 다른 서비스 분야에서 공개된 데이터 간에도 발생할 수 있다[15]. 특히 최근 발전한 모바일 환경에서는 이름, 주소, 전화번호 등 전통적인 개인 식별정보 이외에 센서, IP 주소, 기기 고유번호, 위치정보 등의 수집 가능한 광범위한 데이터로 인하여 정보 결합을 통한 개인 재식별가능성이 높아지고 있다. IoT와 결부된 정보는 개인의 생활 패턴과 행동 양식을 파악할 수 있는 민감한 비식별정보로 볼 수 있으며, 기존의 식별정보 이상으로 개인에 대한 정보를 재식별할 수 있을 것으로 예상된다[16]. 이렇게 재식별된 데이터는 심각한 프라이버시 침해로 이어질 수 있다.

3.2.4 IoT 서비스 상 국경 간 개인정보 공유 확대에 따른 국외이전 이슈 부각

IoT의 확산은 인터넷을 통해 국가 간 경계를 뛰어 넘는 다양한 형태의 국제적 비즈니스를 촉진시킨다. 이러한 IoT 환경에서는 정보주체의 거주지와 상관없이 개인정보가 국경의 제한 없이 이동될 가능성이 증대된다[17]. 글로벌 서비스 제공으로 인한 국경 없는 개인정보 유통은 새로운 이슈를 야기하였는데, 이는 개인정보보호 수준이 국가별로 상이함에 따라 개인정보의 국외이전 시 개인정보보호가 잘 이뤄질 수 있는지에 대한 문제이다[17][18]. 2장에서 살펴본 개인정보처리자들이 국내에만 존재한다면 동일한 개인정보보호 제도 하에서 통제될 수 있으나, IoT 환경에서는 수집된 개인정보가 국내만이 아닌 국외의 클라우드 서버에 저장/활용될 수 있으며, 한 가지 IoT 서비스에 관련된 디바이스 제조자와 다른 국적의 어플리케이션 개발자가 혼재되어 서비스를 제공할 수 있어서 IoT 환경에서 개인정보의 국외이전에 대한 이슈는 더욱 확대될 수 있다. 보다 다양하고 가치 있는 IoT 서비스 제공을 위해서는 디바이스 제조사, 앱 개발자, 플랫폼 제공자 등 IoT 서비스를 구성하는 참여자 간의 유기적인 정보공유를 통해 서

비스를 구현할 필요가 있음에도 불구하고 개인정보 국외이전 문제는 기업의 입장에서 볼 때 원활한 연계 네트워크 구성의 장벽이 될 수 있다. 또한, IoT 상에서의 개인정보 유출이나 정보주체 권리 침해 등의 사고가 국경 간 발생할 경우, 정보주체의 피해구제와 분쟁조정 등이 더욱 어려워질 수 있다. 국제간 개인정보 이동 및 보호를 위해 현재 EU에서는 다국적 기업 대상의 BCR(Binding Corporate Rules), EU-US Privacy Shield, 국가대상 적합성(Adequacy) 평가 등의 제도가 운영 및 검토되고 있으며, APEC(Asia-Pacific Economic Cooperation)에는 CBPRs(Cross-Border Privacy Rules System) 등의 제도가 있으나 아직까지 참여하는 국가들은 제한적이다. 따라서 현재와 같이 국가별로 서로 다른 개인정보보호 수준 하에서 인터넷으로 세계가 연결되는 IoT 서비스들이 본격적으로 출시되면, IoT 상에서의 정보주체 권리와 개인정보보호에 대한 책임 있는 감독과 대응, 협력이 어려워져 2차, 3차 피해로 이어질 수 있다.

IV. IoT 환경에서의 제도 개선 방안 제안

앞에서 살펴본 IoT 환경의 특징과 참여자, 그리고 주요 이슈사항을 바탕으로 본 장에서는 IoT 환경에서의 개인정보보호 강화를 위한 제도적 개선방안을 제안하도록 한다.

4.1 IoT 개인정보처리자 유형별 개인정보보호 가이드라인 개발

앞에서 검토된 바와 같이, IoT 상에서 여러 유형의 개인정보처리자들이 존재한다. 이들은 개인정보처리자로서의 업무와 개인정보파일의 운용 방법이 서로 다를 수 있으므로 이에 따른 개인정보보호 가이드라인을 개발하여 제공할 필요가 있다. 본 연구에서는 EU의 제29조 데이터 보호 작업반에서 발표한 IoT 발전에 따른 의견서를 참조하되[5], 한국의 개인정보보호 제도 환경을 고려하여 응용 및 재구성하였다. 먼저, 모든 IoT 개인정보처리자 유형에 공통적으로 적용될 개인정보보호 가이드라인을 제안하면 다음과 같다.

* 공통사항
- IoT 상에서 새로운 제품 및 서비스 출시 시 개인정보 및 프라이버시에 미치는 영향 평가(Privacy Impact Assessment)를 수행하도록 한다.
- "Privacy by Design" 및 "Privacy by Default" 원칙을 적용하도록 한다. 즉, IoT 제품 및 서비스 설계 단계에서부터 기본적으로 프라이버시 보호를 고려하고 보안 조치 절차를 수행하도록 한다.
- IoT 관련 총계 데이터(aggregated data) 획득 후 수집된 원천 데이터는 반드시 삭제(파기)하도록 한다.
- IoT 환경에서 사용자에게 고지하거나 동의 획득 등에 필요한 절차 및 방법, 그리고 인터페이스를 최대한 사용자 친화적으로 구현하도록 한다.

다음으로, IoT 생태계에 참여하는 개인정보처리자 유형별 개인정보보호 수칙에 대한 가이드라인은 아래와 같다.

1) 디바이스 제조사
- IoT 디바이스 제조사가 직접적으로 수집 및 처리하는 개인정보뿐만 아니라 다른 정보와 결합되어 처리되는 정보까지 개인정보 처리방침에 포함하도록 한다.
- IoT 디바이스에 작동될 수 있는 '데이터 수집방지' 또는 '위치추적 방지' 옵션을 부여하도록 하다.
- IoT 디바이스 자체에서 보안에 대한 취약성이 발견될 경우 즉각적인 고지와 업데이트할 수 있는 도구를 제공하도록 한다.
- IoT 디바이스 사업자는 정보주체의 개인정보 동의 사항 변경 및 철회 요청 시 관련 있는 다른 이해관계자에게 즉각적으로 공지할 수 있는 커뮤니케이션 채널을 상시 확보하도록 한다.

2) 어플리케이션 개발자
- IoT 관련 어플리케이션에서 작동하는 센서가 개인정보를 수집하고 있음을 정보주체에게 수시로 고지 또는 경고할 수 있도록 설계하도록 한다.
- 정보주체의 개인정보에 대한 접근 및 수정, 그리고 삭제권을 보장할 수 있도록 IoT 어플리케이션 및 소프트웨어를 설계하고 구동하도록 한다.
- 개인정보 최소 수집 원칙에 기초하여 최초 수집 목적이 달성된 원천 데이터에 대해서는 다른 개발자 등 제3자로부터의 접근을 금지해야 한다.

3) 소셜 플랫폼 서비스 제공자
- IoT 기기와 연계된 소셜 플랫폼 서비스의 경우, 소셜 플랫폼 서비스 제공 전 단계에서 수집된 데이터에 대한 검토 및 편집, 결정 여부를 이용자에게 요청할 수 있는 기능을 부여하도록 한다.
- IoT 기기에 의해 제공되는 소셜 플랫폼 상의 개인정보가 검색엔진을 통해 검색되어 공개되거나 색인화 되지 않도록 한다.

4) 데이터 플랫폼 제공자
- 데이터 플랫폼 제공자는 다른 참여자들과 데이터 교환이 용이하도록 데이터 호환성을 제공하고, 정보주체에게는 IoT 상에서 개인과 관련된 어떤 데이터가 수집되고 있는지 이해를 도울 수 있도록 명확하고 쉬운 데이터 포맷 사용을 촉진토록 한다.
- 데이터 플랫폼 제공자는 IoT 데이터의 적정한 익명성을 가능한 지원하도록 하며, 개인 식별가능 정보가 최소화된 데이터 포맷이 사용되도록 한다.
- 정보주체의 개인정보보호 및 데이터 보안을 위해 인증된 표준과 가벼운(lightweight) 암호화 및 전송 프로토콜 등이 IoT 환경에 맞게 구현되도록 한다.

5) IoT 디바이스 소유자
- IoT 기기 사용자는 해당 기기의 표시를 통해 비사용자(non-user) 정보주체가 자신의 정보가 수집되고 있음을 알 수 있도록 한다.

4.2 IoT 상에서 정보주체의 자기통제권 강화 방안 수립

IoT 환경에서는 정보의 편재성 등으로 인해 정보주체의 자기통제권이 약화되고 개인정보의 오남용에 대한 염려가 높아진다. 본 연구에서는 개인정보의 수집 단계에서부터 정보주체의 자기통제권을 강화할 수 있는 방안을 제시하고자 한다.

4.2.1 사용자 친화적인 고지방안 마련

IoT 상에서 개인정보 수집 및 처리에 대한 거절권리를 제공하거나 동의를 요청하는 경우, 가능한 정보주체에게 친화적인 고지 방법을 활용하도록 한다. 특히 IoT 환경에서는 소형 IoT 센서 기기들이 이용자 주변에 다수 존재하게 되는데, 이 경우 개인정보 취급방침에 대한 고지를 기존의 전통적인 형태로 제공하는 데 한계가 있으므로 IoT 환경에 맞게 새로운 사용자 고지 방법을 고안할 필요가 있다. 예를 들어, 사용자가 휴대하고 있는 스마트폰과 같은 스마트 커뮤니케이션 기기의 앱을 통해 사용자 주변의 IoT 센서 기기들이 검색되어 정보주체에게 소리, 메시지, 이미지 등의 형태로 알려주고, 검색된 IoT 기기를 앱에서 선택 시 해당되는 상세 개인정보취급방침 등이 안내되는 형태를 검토해 볼 수 있다. 이때 주변 IoT 기기의 검색 및 공지가 자동으로 처리되도록 하는 방식과 원할 때 수동으로 처리되도록 하는 방식을 사용자가 선택할 수 있는 옵션을 제공할 수 있다. 또한 고지되는 내용을 정보주체가 좀 더 쉽게 인지할 수 있도록, 어려운 법률 용어 기반의 텍스트 나열식이 아닌 인포그래픽(info-graphic) 또는 멀티미디어 등 다른 시각적 기법[19]들을 활용하도록 한다. 이러한 방식을 통해 사용자가 IoT 상에서의 정보 수집·처리 현황과 고지 내용을 쉽게 알 수 있도록 하여, 개인정보에 대한 정보주체의 자기통제권 행사를 강화시키고 프라이버시 침해 사고를 줄일 수 있도록 한다.

4.2.2 자율규약 제정

IoT 상에서 개인정보가 본연의 목적 보다 필요 이상으로 수집되고 처리되지 않도록 하는 자율규약(Code of Practice for Self-regulation)을 제정하고 운용하도록 한다. IoT 환경에서는 수집되는 개인정보가 많을수록 개인에 대한 프로파일링을 보다 면밀하게 할 수 있고 이를 통해 고품질의 개인화된 서비스가 가능할 수 있다. 결과적으로 기업들은 더 많고 더욱 민감도 높은 개인정보들을 수집하려고 할 수 있다. 개인정보보호법에서는 최소 수집의 원칙을 강조하고 있으나 그 최소의 기준점을 명확하게 제시하기가 어려우므로, 자율규제에 기반 한 자율실천규약 제도를 도입하는 것이 보다 더 합리적일 수 있다. 예컨대, 해당 산업을 대표하는 단체 및 협회 등에서 관련 산업분야에 필요한 개인정보 수집 범위를 지정하고 이를 이행할 수 있도록 하되, 기업들의 사업적 자율성을 보장해 주면서도 개인정보보호 수행을 감독할 수 있도록 주요 단체 및 협회에서 사후 모니터링할 수 있도록 권한을 부여하는 방식을 고려해 볼 수 있다. 해당 산업 협회의 자율규약과 관련된 기존 사례로는 대한화장품협회에서 규정한 화장품의 허위/과장 광고 방지 및 소비자 보호를 위한 화장품 자율규

약이 있다. 한국화장품협회에서는 화장품 안전 사용 및 위험성 방지를 위해 화장품 용기에 주의 사항을 표기하도록 하는 규약을 정하고 기업들이 자율적으로 규제에 따를 수 있도록 하고 있다.

자율규약은 IoT에서의 데이터 라이프사이클에 따라 카테고리화하여 제정할 수 있다. 이중 데이터 수집과 관련한 국내 자율규정을 수립할 경우, "한국사물인터넷협회"에서 개인정보 수집방침에 대한 자율규약을 제정할 수 있을 것이다. 예를 들어, "IoT 기기 사용 시 개인정보 수집 방침에 대한 자율 규약"을 제정하여 정보주체가 IoT 기기에서 수집되는 개인정보에 대해 알 수 있도록 하는 방식(앱 등)에 대해 규율할 수 있을 것이다 (규율 문구 예: 수집되는 개인정보에 대해 사용자가 쉽게 인지할 수 있도록 하는 관련 앱이 해당 기기에 기본으로 설치되도록 하며, 해당 앱에 대해 사용자가 알 수 있도록 설명하는 안내문이 IoT 기기 제품에 포함되도록 한다). 이와 같이 제정된 협회의 자율규약을 IoT 참여 기업들이 준수할 수 있도록 하는 제도적 장치를 마련하도록 한다.

4.2.3 IoT 특수성을 반영한 자기통제권 행사방안 통지 메커니즘 마련

IoT 상에서 정보주체 본인이 원치 않을 경우 임의로 개인정보가 처리되지 않도록 보장하고, 정보주체가 자신의 개인정보 처리사항과 목적, 정보처리자의 신원, 그리고 본인의 권리 행사 방법에 대해 통지받을 수 있게 보장하는 메커니즘을 구축토록 한다. 현 개인정보보호법 제35조에 따르면 정보주체는 개인정보의 열람권을 가지고 있지만[7], 자기통제권 행사 방법에 있어 IoT 환경의 특수성이 보다 잘 반영될 필요가 있다. 예컨대, IoT 서비스 제공자가 고객(정보주체)의 동의를 받고 개인정보를 이용하거나 제3자에게 제공 중인 현황을 정보주체가 조회할 수 있는 시스템(일명 "IoT 개인정보 이용 현황 열람 시스템") 구축을 모색해 볼 수 있다. 금융회사의 경우 개인정보 유출 재발방지에 대한 종합대책의 일환으로 2014년부터 이와 유사한 개념의 시스템 구축이 추진되었다. 또한 통신사의 경우, 개인의 통신자료 제공 사실 확인(또는 열람) 신청을 통해 타 기관에 자신의 통신자료가 제공된 내역을 이메일로 전송받을 수 있는 제도가 있다. 단, 이 경우 개인정보가 사용된 이벤트 발생 시, 본인에게 자동으로 통지되는 구조가 아니라, 정보주체 당사자가 경각심을 가지고 통신사 홈페이지에서 직접 신청을 한 후 실시간이 아닌 며칠이 지난 후 결과를 받아볼 수 있는 형태이다. IoT 환경에서는 서비스 이용자(정보주체) 측에서 실시간으로 본인의 개인정보가 이용되는 상황을 조회할 수 있는 시스템을 구축하고, 개인들이 이를 어떻게 통제할 수 있는지에 대한 권리 행사방안이 정보주체에게 통지될 수 있는 제도 의무화 계획을 검토해 볼 수 있을 것이다.

4.3 사전 동의 역기능 해소를 위해 IoT 환경에 적합한 탄력적인 동의제도 검토

국내의 현 개인정보보호법상 동의제도는 수집 또는 제3자에게 제공되는 모든 개인정보에 대해 고지(informed)에 기반하며, 정보주체로부터의 동의확인에 대한 명시적 서면화(explicit)를 전제한다. 단, 서면화의 방법으로는 정보주체의 서명 또는 날인 동의서를 받거나 전화/인터넷홈페이지/전자우편 등을 통해 확인하는 방법이 포함된다. 이러한 국내 동의제도는 세계 어느 국가보다도 가장 강력한 수준이라고 할 수 있다. 한편 동의라는 것은 개인정보에 대한 자기결정권을 이행하는 수단으로 의미가 있는데, 동의제도가 아무리 강력하더라도 고지방법이 적절하지 않거나 정보주체가 결정권 내용을 충분히 인식하지 못한 상태에서 동의가 이행된다면(예: 동의할 내용의 가독성이 떨어지거나 동의할 항목들이 지나치게 많아 제대로 내용을 확인하지 못한 채 습관적으로 동의 체크 하는 경우와 동의하지 않으면 서비스 사용을 전혀 할 수 없어 하는 수 없이 동의 버튼을 클릭하는 경우 등) 개인정보 자기결정권을 이행하는데 적절한 수단이라 할 수 없다. 참고로 개인정보보호 수준이 높은 EU에서는 민감정보에 대해서만 고지기반의 명시적 서면화(informed explicit) 동의제도를 운용하고 있으며, 필요에 따라 사후동의(granular consent)를 인정하고 있다[20]. 유용한 IoT 서비스와 개인정보 자기결정권이 공존하기 위해서는 탄력성 있는 동의 제도를 운용함으로써 저품질 동의를 유도하는 동의만능주의로 인한 병폐를 줄일 수 있도록 해야 한다. 즉, 개인의 민감정보와 개인 식별성이 높은 고유식별정보 등은 사전 동의를 통해 수집하도록 하되, 식별성이 낮은 준식별자나 민감도가 낮은 정보 등은 옵트아웃(opt-out) 제도로 운용하는 것을 검토할 수 있다. 이를 통해 IoT의 편익 극대화와 함께 중요한 개인정보를 보호할 수 있도록 개선된 동의제도가

마련되도록 한다.

4.4 개인정보 재식별 위험 모니터링 체계 정립

IoT 환경에서는 수집되는 데이터가 방대하며 외부 정보와의 결합 가능성이 높으므로 재식별의 위험이 증가하게 된다. 따라서 IoT 상에서 개인정보의 재식별 위험성을 최소화하기 위한 기술적, 관리적 수단이 강구되어야 한다. 이를 위해 개인정보의 비식별화 조치의 적정성 평가체계[13]를 마련하고, IoT 서비스 참여자들이 그러한 체계를 준수토록 한다. 즉, IoT 개인정보처리자들이 수집한 단위 개인정보에 대해 비식별화 조치를 하여 제공하였다 해도, 다른 정보와 결합되어 재식별될 수 있는 위험이 최소화되도록 체크하고 (기술적 솔루션 도입 포함), 가능한 개인을 절대 식별할 수 없는 익명화된 상태의 개인정보로 보전될 수 있도록 지원하고 주기적으로 모니터링하도록 한다. 다만, 재식별 위험성 평가 시 유의할 점은, 지나친 익명화 조치로 인해 개인정보의 유용성 자체가 저하될 수 있으므로 익명화 조치 수준과 개인정보의 유용성을 고려하여 평가하는 방법이 고려되어야 할 것이다.

또한, IoT 환경에서 재식별 위험을 줄이기 위해 제3자에게 데이터 제공 및 공개, 위탁 시 재식별을 금지하는 조항의 명문화를 검토할 수 있다. 참고로 일본의 개인정보보호에 관한 법률 제23조 1항에서는 개인정보취급사업자(개인정보처리자)는 정보주체의 사전 동의 없이 제3자에게 개인 데이터를 제공할 수 없도록 규정하고 있는데, 제2항에서는 이에 대한 예외사항으로 개인정보 비식별화 조치 등을 통해 개인 특정성을 낮춘 개인정보의 경우는 재식별금지와 정보주체에게 이용 목적 등의 고지를 전제로 제3자에게 제공할 수 있도록 하고 있다[21]. 이를 참조하여 데이터 위탁 시 재식별 금지 조항 수립을 고려할 수 있을 것이다. 최근 재식별 수준 최소화 기술(예: k-anonymity, differential privacy 등)들이 개발되고 있으나 관련 전문 인력이 부족한 상태이다. 따라서 기술력과 개인 식별 가능성에 대한 분석력을 갖춘 전문 인력을 체계적인 계획 하에 육성할 필요가 있다. 또한 재식별 최소화 기술과 모니터링 제도가 IoT 산업 현장에서 실제 활용될 수 있도록, "사물인터넷 실증단지 조성 사업"[22] 등과 연계하여 테스트베드 구축을 추진하는 등 재식별 위험 감소를 위한 기술적/제도적 방안이 지속적으로 검증되고 업그레이드 되도록 해야 할 것이다.

4.5 IoT 서비스 관련 국외이전 개인정보에 대한 보호 강화 제도 수립

국경 없는 IoT 서비스 증가와 그로 인한 편익 증대가 예상되는 가운데, 국가 간 서로 다른 개인정보 보호 수준과 집행 방식의 차이로 인하여 정보주체의 권리 보호를 위한 개인정보 안전 강화 방침이 필요하다. 본 연구에서는 개인정보 국외이전에 따른 정보보호 관련 문제를 감소하기 위한 방법으로 "책임성(accountability)에 기반한 접근법"을 제시하고자 한다. OECD의 프라이버시 개정 가이드라인(2013. 9)[23]에 따르면, 데이터의 위치에 대한 고려없이 개인정보처리자가 그들의 관리 하에 있는 모든 개인정보에 대해 책임을 갖는다고 전제하고 있다. OECD의 책임성 기본 원칙에서는 개인정보의 국외이전 위험에 대한 책임을 정보처리자가 감수하고 처리해야 함을 강조하고 있다. IoT 환경에서의 국경간 이전에 대한 책임성 이행을 위해서는 국외이전에 대한 표준계약제도 도입이 검토될 수 있다. 표준계약제도는 개인정보수출자와 개인정보수입자간의 의무사항을 계약을 통해 상호 이행하도록 하는 제도로서, 정보주체가 속해 있는 개인정보수출자의 감독기구나 정부가 그 의무사항을 자국법에 맞추어 규정하고 이를 개인정보수입자가 계약을 통해 이행할 수 있도록 하는 것이다. EU에서는 국외이전에 대한 표준계약조항(Standard Contractual Clauses)을 제도화하고 있다. 이 제도는 EU 시민의 개인정보가 역외로 이전될 경우 EU법 하의 정보주체 권리를 보장하기 위해 가장 보편적으로 활용되고 있다. 이 제도는 계약에서 사용하는 용어 정의(개인정보 정의 등 포함), 이전의 세부사항, 정보주체의 권리보장 관련사항(정보주체의 선택권과 실체적/절차적 권리, 정보주체 요청 시 계약조항 또는 하위처리를 위한 기존 계약의 사본 제공 - 단, 일부 상업적 정보 제거 가능), 요청 시 계약 상대기업 대상 사전실사 협조 의무, 기술적/관리적 개인정보보호조치 실현 및 이에 대한 보증 제공 의무, 분실/유출 사고 등에 따른 피해구제 창구 지정, 개인정보 수입자 대상 자료 제출 의무, 개인정보처리서비스 종료 후 의무(이전된 모든 개인정보/사본 반환 또는 파쇄 등) 등을 계약서의 의무조항으로 포함하도록 규정하고 있다. 이러한 표준계약제도는 기업 당사자 간 계약제도임에도 불구하고 감

독기구의 행정적 개입이 가능하도록 하고 있는데, 개인정보가 국외로 이전되었다고 하더라도 계약 조항에 의거하여 감독기구가 직/간접적 사후조치를 취할 수 있도록 함으로써 정보주체의 권리를 적절히 보장할 수 있도록 하고 있다. 이와 같이 국외이전에서 표준계약제도 수립 및 이행을 통하여 국가 간 충돌할 수 있는 개인정보보호 수준을 상호계약을 통해 조정할 수 있고, 정보주체의 권리가 보장되도록 할 수 있다. 특히 국제 간 데이터 유통이 필요한 글로벌형 IoT 서비스 환경에서는 이러한 표준계약 제도 수립이 필요하다.

4.6 IoT 서비스 제공자에 대한 사전 규제 강화

4.6.1 Privacy by design 개념 의무 적용

IoT 환경에서 개인정보 및 프라이버시 보호를 위해서는 서비스 설계 단계에서부터 프라이버시 침해에 대한 위험을 평가하고 점검하여 이를 미리 예방할 수 있는 장치를 마련하는 것이 필요하다. IoT 서비스를 기획하고 제공하는 것은 개인정보보호법 제33조 제8항[7]에 명시된 것과 같이 "개인정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우"에 해당될 수 있으므로 개인정보 침해 위험에 대한 영향평가를 하기 위하여 적극 노력해야 한다. 이러한 측면에서 IoT 사업자는 제품 및 서비스의 초기 설계 단계부터 프라이버시를 고려하는 개념인 "Privacy by Design" 과 "Privacy by Default"을 의무적으로 적용할 필요가 있다. "Privacy by Design"은 90년대 캐나다 온타리오주 개인정보보호위원회의 앤 카부키안 박사에 의해 제안된 개념[24]으로서 ICT의 발전과 그에 따른 프라이버시에 미치는 영향을 조망하고, 개인정보의 통제권 및 사생활 보호 강화와 기업의 지속 가능성과 기관의 경쟁력 확보를 위하여 7대 원칙을 포함하고 있다. 그 7대 원칙은 1) 사후대응이 아니라 사전대비하고, 문제점을 고치는 것이 아니라 사전예방토록 함; 2) 프라이버시 보호를 시스템의 기본값으로 설정함; 3) 개인정보처리자의 모든 활동계획에 프라이버시를 포함; 4) 포괄적 기능성을 보장하여, 상호대체(Zero-Sum)가 아닌 상호보완(Positive-Sum)으로 전환; 5) 개인정보의 생명주기 전체에 대하여 보안을 고려; 6) 개인정보보호 정책 및 절차의 투명성 유지와 정보주체 등 이해관계자에게 항상 공개되도록 함; 7) 사용자 중심의 설계와 운영으로 개인의 프라이버시가 존중되도록 함이다[24]. 이러한 사용자 보호 중심의 "Privacy by Design"을 위해서는 개인정보처리자에 의한 프라이버시 보호의 기본 설정, 사용자 편의를 고려하고 사용자에게 프라이버시 관련한 선택 권한 부여, 적정한 알림 제공 등이 서비스 기획 초기단계에서부터 기획되어 마련되어야 한다. 해외의 경우, 독일의 한 지방자치단체는 빅데이터 가이드라인 제정 시 "Privacy by Design" 개념을 적용하여 빅데이터 설계 초기 단계부터 매 중요 단계마다 프라이버시 침해가 없는지에 대한 영향 평가를 통해 위험성을 제거하는 방침을 적용하였다[25]. 국내에서는 빅데이터의 중요성이 대두되었던 2012년부터 "Privacy by Design" 개념 도입이 논의되었고, 최근 IoT 시대가 본격적으로 도래됨에 따라 개인정보보호를 위한 방안으로 Privacy by Design이 IoT 정책 추진 전략의 일환으로 강조되고 있다[26]. 설계단계부터 프라이버시를 고려하는 개념을 제도적으로 적용하는 방안은 국외 법/제도 제정 현황을 참조하되 국내 실정을 맞게 도입 검토가 필요하다. 또한 "Privacy by Design" 제도 정착을 촉진하기 위해 IoT 제품/서비스에 관련 인증마크 등의 표시를 부여하는 방안 등이 고려될 수 있다.

4.6.2 개인정보처리자 유형별 프라이버시 영향 평가 기준 마련

IoT 환경에서 이용자에게 프라이버시 보호에 대한 확신을 주고, IoT 산업 현장에서 프라이버시와 관련된 위험 평가와 대응이 실질적으로 수행될 수 있도록 객관적인 프라이버시 영향 평가(Privacy Impact Assessment, PIA) 기준을 마련할 필요가 있다. 현재 EU의 대표적인 개인정보 감독기구인 제2조 데이터 보호 작업반에서는 IoT 상에서 발생할 수 있는 프라이버시 및 개인정보에 대한 위협 요소로서 데이터 수집/전송의 통제 미비로 인한 개인정보 유출 위험, 사용자 개인의 행위 패턴 분석 및 프로파일링 등으로 인한 프라이버시 침해 위협, 데이터 결합을 통한 개인 식별 위험 등을 지적하였다[5]. IoT 생태계에 참여하는 모든 개인정보처리자들은 자사의 제품/서비스에 대해 주요 위험 요소를 식별하고, 요소별 위험 수준과 그 영향력을 평가할 수 있어야 하며, 궁극에는 위험 평가결과에 따른 대처방안이 검토되어야 한다. 한편, IoT 환경에서는 여러 유형의 개

인정보처리자가 존재하고 각기 기능과 역할이 다르므로, 해당 환경에 적합한 프라이버시 영향 평가 기준이 필요하다. 따라서 실효성 있는 PIA 수행을 위해서는 개인정보처리자 유형별로 구체적인 평가 기준이 마련이 우선되어야한다.

4.6.3 IoT 서비스 개시 전 사고대응 방안 마련

IoT 서비스는 개인정보 관련사고 발생 가능성과 위험도가 높은 반면, 사업에 참여하는 이해관계자가 많기 때문에 어떤 사업자가 책임감을 갖고 사고에 적극 대응할 것인지에 대해 혼선이 야기될 수 있고 책임 회피 현상이 발생할 수 있다. 이로 인해 개인정보 사고 발생 시 민첩하고 효율적인 사고 대응이 어려워져 피해가 배가될 수 있다. 따라서 이러한 혼선을 방지하기 위해서는, IoT 서비스 제공을 총괄하는 총괄사업자에게 일정 정도의 사고대응 우선처리 의무가 부여되도록 하고, 해당 사업자에게는 사전에 종합적인 사고대응 방안을 마련하도록 의무화할 필요가 있다. 특히 IoT 환경에서 발생하는 보안 사고의 경우, 어플리케이션/단말기기/네트워크/서버/스토리지 등 분야별로 다양한 참여자들 간의 책임이 명확하지 않을 수 있으므로, IoT 서비스 개시 이전에 발생 가능한 사건 등을 미리 조사 분석하고 이해관계자들 간 책임소재를 분명히 하여 신속한 사고 대응 및 사고 피해자에 대한 배상책임이 명확히 이루어질 수 있도록 계약을 체결하도록 해야 한다. 또한 사고발생 시 사고피해를 최소화하기 위해 이해관계자들 간의 사고대응 협력 방안도 검토되어야 한다. IoT 사업을 총괄하는 기업 내에서는 서비스 개시 전 사고대응 방안에 대한 의무를 CPO(Chief Privacy Officer)의 책무로 설정하는 등 체계적인 관리 책임 하에 사고 대응방안이 수립되도록 해야 한다.

4.6.4 표준화된 프라이버시 강화 기술 적용

IoT 상에서 자동 센싱 및 촬영이 가능한 영상정보처리 디바이스가 증가함에 따라 이를 통해 프라이버시 침해 이슈가 다양하게 등장할 수 있다. 일례로, 구글 글래스와 같은 웨어러블 스마트 글래스를 통해서 사용자 본인 이외에 주변 사람들이 촬영될 수 있는데, 그 사진 및 영상들이 인터넷을 통해 전송되고 공유될 경우 이로 인한 프라이버시 침해와 그 피해가 심각할 수 있다[9][27]. 이러한 프라이버시 침해 문제 최소화를 위해서는 센싱 및 촬영 기능을 가진 IoT 디바이스 기획 및 제조 시, 앞에서 설명한 프라이버시 영향 평가(PIA)를 통해 위험 요소를 체크하고 이를 해결할 수 있는 프라이버시 강화 기술(Privacy Enhancing Technology: 개인정보를 보호하고 프라이버시 침해 위험을 관리하기 위한 기술) 요소를 추가하도록 해야 한다. 예를 들어, 현재 국내에서 휴대폰 촬영 시 적용되고 있는 촬영음 소리 울림과 같이 스마트 글래스로 촬영할 때 알림음 이후에 촬영 기능이 활성화되도록 하고, 촬영 중임을 나타내는 표식이 기기 전면에 디스플레이 되게 하는 등 IoT 영상정보처리기기를 통한 정보수집 과정에서 프라이버시 보호를 강화하는 기술적 조치를 검토토록 할 수 있다. 실효성 있는 프라이버시 강화 기술 적용을 위해서는 IoT 산업(예: 웨어러블 디바이스 산업, 스마트 홈/가전 산업, 드론 산업 등)별로 필요한 요소 기술에 대한 표준화를 추진하는 것이 바람직할 수 있다. 즉, IoT 산업별로 프라이버시 보호를 위해 가장 필요한 기술 요소를 선정하여 산업별 대표 협회 및 표준화 기구를 중심으로 해당 표준을 제정/개발하고, 표준화를 준수하는 기업에게는 인센티브를 제공하여 표준화된 기술 보급을 촉진토록 할 수 있다. 또한 프라이버시 보호를 위해 가장 필수적인 표준화 적용 부분에 대해서는 이를 준수할 경우에만 IoT 디바이스가 시중에 보급될 수 있도록 검토되어야 할 것이다.

4.7 개인정보 수집 및 파기에 대한 관리 강화

4.7.1 개인정보 수집 디바이스 통제 제도 강화

IoT 환경에서는 센서 및 허브 역할을 하는 다양한 스마트 기기들이 기하급수적으로 증가하게 되는데, 이들 기기들이 제대로 통제되지 않을 경우 개인정보 유출 및 해킹의 위험이 커질 수 있다. 예컨대, IoT 기기의 도난 및 분실 등 자산관리 부실로 인해 개인정보가 유출될 수 있고, IoT 기기에 저장된 개인정보 등이 제대로 포맷 및 파기되지 않은 상태에서 중고시장 거래 등을 통해 다른 곳에서 재사용될 경우 불법적인 개인정보 복원 등을 통한 정보 유출의 위험이 존재할 수 있다. 또한 수많은 IoT 디바이스 내 개인정보를 파기하는 데 드는 비용과 소요 일정 등을 이유로 개인정보 파기 실행이 제대로 이뤄지지 않을 수 있다. 이와 같은 사태를 방지하기 위해서는 IoT 사업자의 IoT 기기에 대한 자산관리를 강화할 필요

가 있는데, 이를 위해 IoT 사업자들이 개인정보가 수집/저장되는 디바이스에 대한 통합적인 관리를 수행하도록 기기별 고유식별번호 기반의 IoT 통합 자산관리 시스템 구축과 시스템에 등록된 기기에 대한 관제 의무화를 제도적으로 검토할 수 있다. 이와 같은 디바이스 통제 제도 구축을 통해, 개인정보가 저장된 IoT 디바이스의 도난 및 분실의 경우 기기식별번호로 추적할 수 있도록 하고, 디바이스를 교체할 경우에는 기존 디바이스 내 개인정보 파기 인증 없이는 2차적인 재활용이 불가능하도록 하는 등의 관리 강화가 이루어 질 수 있을 것이다.

4.7.2 제3자에게 제공된 개인정보 파기 관리제도 강화

IoT 산업의 새로운 가치 창출을 위해서는 사업자 간 협업이 필요하며 제3의 참여자와의 협업 시 개인정보를 포함한 정보들이 제3자와 공유될 수 있는데, 이에 대한 개인정보 수집자의 역할 및 책임을 높일 필요가 있다.

금융권에서 금융 분야 개인정보 유출 재발방지 종합대책의 일환으로 시행되고 있는 "제3자에게 제공된 정보 파기 및 확인 의무화" 제도[28]를 시행하고 있는데, 이와 유사한 제도를 IoT 사업자에게 도입하는 것을 검토할 수 있다. 제3자에게의 개인정보 제공을 정보주체가 동의한 경우를 전제로, IoT 사업자는 제3자와 개인정보를 제공하는 계약 체결 시 개인정보의 구체적 보유 기간과 파기 계획을 명시하도록 하고, 파기 불이행시 손해 배상 등의 페널티가 있도록 한다. 특히 개인정보의 파기를 철저히 관리하기 위해서는 제3자와 계약한 개인정보 이용기간 만료 도래 시, 제3자에게 제공된 개인정보를 파기하도록 공문으로 요청하고 제3자로부터 파기확인서를 징수하도록 해야 한다. 또한 문서만 아닌 주기적인 실태 조사를 통해, 제3자 제공 정보의 파기여부 등 개인정보 관리 실태를 점검하고 이를 CPO(Chief Privacy Officer) 또는 CSO(Chief Security Officer) 등에 보고하여 관리하도록 해야 한다.

4.8 IoT에서의 개인정보에 대한 보안 인식 제고를 위한 이용자 교육 강화

개인정보 유출 등의 사고를 예방하기 위해서는 IoT 사업자만이 아니라 IoT 사용자의 보안의식 고취를 위한 이용자 개인정보보호 교육이 반드시 필요하다. 특히 IoT 서비스는 이용자의 직접적인 개입 없이 자동적으로 이뤄지는 경우가 많고, 개인의 일상생활에 밀착된 서비스 형태로서 수집되는 개인정보의 종류와 범위가 크며, 기술적으로 복잡한 IoT 메커니즘을 사용자가 이해하기 힘들 수 있다. 따라서 사용자가 알기 쉬운 방식으로 개인정보보호에 대한 교육이 제공되도록 해야 하며, 개인의 보안 인식 고취를 위해서는 단타성의 교육이 아닌 반복적인 교육이 수행되어야 한다. 이를 위해 정부 및 공공기관과 IoT 사업자들은 온/오프라인 매체를 적절히 활용하여 이용자에게 다양한 교육을 수시로 제공할 수 있도록 해야 한다. 우선, 정부 및 공공기관에서는 모든 국민들이 IoT의 주요 특징과 서비스 종류, 수집되는 개인정보 및 수집 경로, 개인정보가 활용되어 제공되는 IoT 서비스 흐름 등을 알 수 있도록 IoT 서비스에 대한 종합 지원 사이트를 운영할 필요가 있다. 예를 들어, 기존의 개인정보보호 지원 종합포털 사이트(www.privacy.or.kr 또는 privacy.kisa.or.kr) 안에서 IoT에 대한 별도 메뉴를 만들어서 주요 IoT 서비스별 수집 가능한 개인정보들과 개인정보보호를 위한 개인들의 생활 수칙 및 피해 예방 가이드, 프라이버시 침해 위험감소를 위해 취할 수 있는 방안, 문의처 등에 대한 교육을 온라인으로 제공할 수 있고, 필요 시 오프라인 교육과 연계할 수 있도록 해야 한다. 또한 IoT 서비스 제공 사업자들은 자사 서비스의 개인정보 수집 및 이용에 대한 사항을 이용 고객이 쉽게 알 수 있도록 하고, 개인정보 관련 사고 예방을 위한 이용자 교육 서비스를 수시로 제공하도록 한다.

V. 제시된 제도의 시급성 및 중요성 분석

제도 및 정책을 자원 효율적으로 이행하기 위해서는 추진할 과제에 대한 우선순위를 고려할 필요가 있다. 본장에서는 4장에서 제시된 여러 가지 제도 개선 방안들에 대해 시급성 및 중요성을 기준으로 우선순위를 제시하고자 한다. 본 연구에서는 IoT 환경에서의 개인정보보호를 위한 제도 개선 방안이 총 14개가 제시되었으며, 이들 각 방안에 대해 시급성과 중요성을 3점 척도로 평가하였다. 즉, 각 제도 방안에 대하여 시급성 및 중요성의 수준을 평가하여, H(높음):3점, M(중간):2점, L(낮음):1점으로 점수를 부여하였다. 제도 개선 방안 추진의 시급성과 중요성 평가에는 총 10명의 전문가(ICT/IoT/정보보호 분

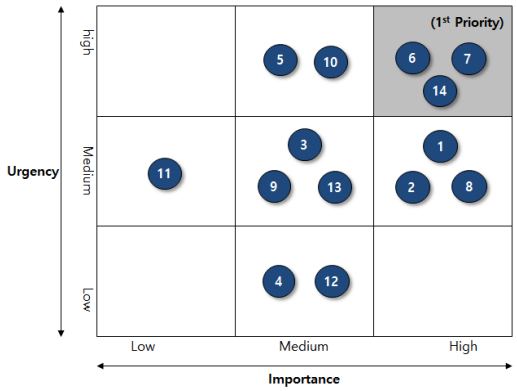

Fig. 1. Priority of Tasks for Enhanced Personal Data Protection

야 박사(박사과정) 및 교수)가 참여하였으며, 이들 전문가 그룹의 평가 결과 최빈값을 대푯값으로 설정하였다. 분석 결과는 Table 2와 같다.

상기 분석된 결과를 바탕으로, 시급성과 중요성이 높은 제도적 개선 과제가 무엇인지 우선순위화 할 수 있다. 우선순위 결과는 Fig. 1과 같다.

본 연구결과, "⑥ 개인정보의 재식별 위험 모니터링 체계 마련", "⑦ 개인정보 국외 이전 시 표준계약 제도의 도입 등 개인정보 강화제도 수립", "⑭ IoT에서의 개인정보 보안 인식 제고를 위한 대한 이용자 교육 강화"가 최우선적으로 고려되어야 할 개선과제로 도출되었다. 이들 3가지 개선안은 시급성과 중요도 모두 "H(높음):3"에 해당되는 과제이다.

Table 2. Analysis Results of Urgency and Importance of Measures for Improving Personal Data Protection in IoT

Area	Improvement Measure	Urgency	Importance
Development of Guidelines for Data Controller and Processor	① Developing guidelines on personal data protection for each type of data controller and processor	M(2)	H(3)
Reinforcement of Data Subject Right to Self-control	② Using user-friendly notice and announcement methods	M(2)	H(3)
	③ Establishing code of practice for self-regulation	M(2)	M(2)
	④ Designing mechanism of notification for exercise of data subject rights to self-control	L(1)	M(2)
Flexible Consent System	⑤ Examining flexible consent system to resolve adverse effect of prior consent system	H(3)	M(2)
Re-identification Risk Management	⑥ Developing re-identification risk monitoring system of personal data	H(3)	H(3)
Reinforcement of Personal Data Protection in Cross-border Transfer	⑦ Establishing standard contractual clauses about transferring personal data overseas	H(3)	H(3)
Strengthening Ex ante Regulations regarding IoT Service Provider	⑧ Applying mandatory adoption of "Privacy by Design" principle	M(2)	H(3)
	⑨ Setting up criteria for "Privacy Impact Assessments (PIAs)" for each data controller and processor	M(2)	M(2)
	⑩ Preparing countermeasure to incidents prior to starting IoT services	H(3)	M(2)
	⑪ Applying standardized privacy enhancing technology	M(2)	L(1)
Strengthening Management and Supervision of Personal Data Collection and Erasure	⑫ Strengthening control system of IoT devices	L(1)	M(2)
	⑬ Strengthening management and supervision system about personal data transferred to 3rd party	M(2)	M(2)
Reinforcement of User Education	⑭ Reinforcing user education for improving security awareness in IoT	H(3)	H(3)

VI. 결 론

본 연구에서는 본격적인 IoT 시대의 도래에 따라 개인정보보호 측면에서 발생 가능한 이슈를 파악하고 이에 대응한 법적·제도적 개선 방안을 제시하였다. 본 연구를 통해 도출된 주요 연구 결과는 다음과 같다.

첫째, 본 연구를 통해 IoT 확산에 따라 현 개인정보보호법 상에서 발생할 수 있는 도출 가능한 문제점을 파악하였다. IoT 환경에서는 기존의 IT 환경 대비 개인정보를 센싱하고 저장, 처리하는 관리 포인트가 크게 증가하기 때문에 개인정보 유출 사고의 위험 가능성과 그 수준이 매우 높아진다. 따라서 현재의 개인정보보호법으로 변화될 IoT 환경에서의 개인정보에 대한 전반적 사항을 규율하기에 한계가 있다. IoT 상에서 개인정보를 효과적으로 관리하기 위해서는 다양한 개인정보처리자 유형, 정보주체의 자기통제권 상실 이슈, 현 개인정보 동의 제도의 실효성 문제, 개인정보 수집/이용/전송/파기 시의 안전성 확보 문제 등 다양한 측면의 검토가 필요하다. 본 연구에서는 IoT 사용 확대에 대비하여 논의될 개인정보보호 관련 주요 이슈사항을 제시하였고, 이는 앞으로의 IoT 개인정보 관련 법적·제도적 개정 검토 시 참조될 수 있을 것이다.

둘째, 본 연구에서는 해외 사례 및 기존 연구 조사 등을 통해 IoT 시대의 개인정보보호를 위한 제도 개선 방안을 제시하였다. 유럽 등 해외에서는 IoT 환경 도래와 함께 개인정보보호를 위한 다각적인 대책을 중장기적으로 준비해 오고 있다. 참고로 유럽에서는 IoT에서의 개인정보보호에 대해 포괄적인 접근 방식으로 전반적인 제도 개선을 적극 추진하고 있다. 한편, 미국의 경우는 유럽과 달리 부문별로 접근하는 방식으로 분야별 IoT 관련 프라이버시 보호 정책(예: 빅데이터 관련 정책, 무인항공기 및 헬스케어 앱 관련 규제, FTC의 소비자들의 IoT에 대한 정책 등)을 추진하고 있다. 국내에서는 아직까지 IoT 환경에서 개인정보보호를 위한 법적·제도적 대응 방안이 구체화되지 않은 상태이다. 본 연구에서는 14가지의 제도 개선방안을 제시하였고, 개선 과제 추진에 있어 우선순위화를 위해 제시된 개선안들의 중요성과 시급성을 검토하였다. 분석 결과, 시급성 측면에서는 사전 동의 제도 개선, 개인정보 재식별 위험 관리 체계 정립, 국외이전 개인정보보호 강화 제도 마련, IoT 서비스 전 사고대응 방안 마련, 그리고 이용자 교육 강화 추진의 필요성이 높게 나타났다. 중요성 측면에서는 IoT 개인정보처리자 유형별 개인정보보호 가이드라인 개발, 정보주체 자기통제권 강화를 위해 사용자 친화적인 고지방안 마련, 재식별 위험 관리, 개인정보 국외이전 표준계약제도 등 마련, ″Privacy by Design″ 개념 의무 적용, 그리고 IoT 이용자 교육 강화 추진의 필요성이 높게 나타났다. 이러한 시급성과 중요성을 종합했을 때, 3가지 개선과제, 즉, 개인정보의 재식별 위험 모니터링 체계 마련, 국외 이전 개인정보보호 강화 제도(표준계약제도) 수립, IoT에서의 개인정보 보안 인식 제고를 위한 이용자 교육 강화가 가장 우선적으로 고려되어야 할 과제로 분석되었다.

IoT 환경에서는 수집/이용되는 개인정보의 양이 급증하고 새로운 서비스 제공을 위해 정보 간 결합이 다양하게 발생할 수 있다. 따라서 비식별 정보가 결합을 통해 재식별 될 개연성이 높아져 개인정보 유출 등의 위험이 커질 수 있다. 따라서 개인정보 재식별 모니터링 제도는 IoT 환경에서 매우 중요한 개선과제가 된다. 또한 국외로 유통되고 이전되는 개인정보 활용에 대한 표준계약제도의 도입은, 개인정보가 보호될 수 있는 환경을 제도적으로 보장하여 국가 간 IoT 사업 활성화를 돕고 사용자 편익을 도모하는 원활한 서비스 흐름을 확보케 함에 있어 우선적으로 검토되어야 할 과제이다. 한편, 성공적인 정보보호를 위해 가장 필수적으로 요구되는 것은 사용자 개개인이 정보보호에 대해 관심을 갖고 이에 대한 수준 높은 보안 의식을 갖추는 것이다. 따라서 IoT 상에서 개인정보의 흐름을 사용자들이 이해하고, 발생 가능한 위험에 대한 사전 교육을 통해 개인정보 유출 및 프라이버시 침해 사고를 예방할 수 있도록 하는 것은 가장 우선시 될 개선 과제임이 분명하다.

IoT 산업의 비약적인 발전이 예상되는 가운데 최근 국내외에서 다수의 IoT 육성 정책들이 공표되고 있다. 이러한 가운데 IoT 환경에서의 개인정보보호 이슈를 선제적으로 검토하고 대응 방안을 마련하는 것은 앞으로의 IoT 시대를 선도해 가고 안전한 미래 정보사회 구축을 위해 범국가적으로 매우 중요한 사안이다. 따라서 이에 대한 지속적인 연구가 필요하다. 이러한 측면에서 본 연구 결과는 “IoT 서비스 활성화”와 “개인정보보호 강화”라는 두 가지 목적을 균형 있게 달성하기 위한 제도 마련에 있어 참조가 될 수 있을 것이다.

References

[1] ITU-T, "The Internet of Things," ITU-T Internet Report, Nov. 2005.

[2] J. Gubbi, R. Buyya, S, Marusic, and M. Palaniswami, "Internet of Things (IoT): a vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no.7, pp. 1645-1660, Sep. 2013.

[3] Gartner, "2015 Hype cycle for emerging technologies identifies the computing innovations that organizations should monitor," Hype Cycle Special Report, Aug. 2015.

[4] Gartner, "6.4 Billion connected things will be in use in 2016, up 30 percent from 2015," Gartner Symposium/ITxpo 2015 in Barcelona, Nov. 2015.

[5] EU Article 29 Data Protection Working Party, "Opinion 8/2014 on the on recent developments on the Internet of Things," EU, Aug. 2014.

[6] Advisory Board, "With tracking devices, employers may track workers' health," Advisory Board Briefing, Jan. 2013.

[7] Ministry of the Interior, "Korea privacy information protection Act," 2016.

[8] EPIC(Electronic Privacy Information Center), "Google class and privacy," EPIC.org, Apr. 2013.

[9] ICO(Information Commissioner's Office), "Wearable technology - the future of privacy," ICO, 2014.

[10] Min-joong Kim, "A study on the issues related with the contents protection in the future Internet," Chonbuk Law Review, 32, pp. 49-86, May 2011.

[11] Boannews, "The IoT has arrived, think personal data protection first," Boannews.com, Nov. 2015. Available: http://www.boannews.com/media/view.asp?idx=48408&kind=2

[12] Ministry of the Interior, "Regulations for Korea privacy information protection Act," 2016.

[13] National Information Society Agency, "Guidelines for self-assessment of conformity about de-identification on personal data," NIA, Dec. 2014.

[14] ICO(Information Commissioner's Office), "Anonymisation: managing data protection risk code of practice," ICO, Nov. 2012.

[15] Jae-geun Lee, Sang-ug Kang, and Heung-Youl Youm, "Analysis of personal information protection circumstances based on collecting and storing data in privacy policies," Journal of the Korea Institute of Information Security and Cryptology, 23(4), pp. 768-774, Aug. 2013.

[16] Won-jin Sun and Doo-hyun Kim, "Change to hyper-connected society and personal information protection," The Journal of The Korean Institute of Communication Science, 31(4), pp. 53-58, Mar. 2014.

[17] Young-jin Shin, "A study on policy to protect personal information for cross-border transfers: focused on suggestion of political tasks and practical issues," Journal of Korean Association for Regional Information Society, 16(4), pp. 71-104, Dec. 2013.

[18] Il-hwan Kim, "A study on international standard and content for the trans-border flow of personal information," Studies on American Constitution, 24(1), pp. 125-154, Apr. 2013.

[19] NAVER, "NAVER privacy policy (Ver. 8.1)," NAVER Corp., 2016. Available: http://www.naver.com/rules/privacy.html

[20] EU Article 29 Data Protection Working Party, "Opinion 02/2013 on apps on smart devices," EU, Feb. 2013.

[21] Japanese Government, "Act on the protection of personal information in Japan,"

Act No. 57, 2003.
[22] Ministry of Science, ICT and Future Planning, "IoT comprehensive plan - IoT test site construction," Jul. 2014.
[23] OECD, "The OECD privacy framework," OECD.org, Nov. 2013.
[24] A. Cavoukian, "Privacy by design," Information and Privacy Commissioner of Ontario, Jan. 2011.
[25] Boannews, "Big data, information and personal data," Boannews.com, Nov. 2014. Available: http://www.boannews.com/media/view.asp?idx=44121&kind=3
[26] Ministry of Science, ICT and Future Planning, "The future of IoT - purpose, strategy and challenge," May. 2014.
[27] DIGIECO, "Personal information protection issues and implications of Google glass," DIGIECO Issue & Trend, Aug. 2013.
[28] SISA Financial Company, "Comprehensive measures for recurrence prevention of personal information breach in financial areas," SISA Finance, 30(4), pp. 101-110, Apr. 2014.

〈저자소개〉

이 애 리 (Ae Ri Lee) 종신회원
2013년 2월: 연세대학교 정보시스템 박사 (디지털 비즈니스 전공)
1996년 8월~2014년 2월: (주)KT 차장
2014년 3월~2015년 4월: 유한대학교 경영정보과 조교수
2015년 5월~현재: 연세대학교 바른ICT연구소 연구교수
〈관심분야〉 Information Security and Privacy, ICT Strategy, Technology Management, Social Media Platform, Virtual Community, Value Co-Creation

손 수 민 (Soomin Son) 정회원
2013년 2월: 한국외국어대학교 경영정보학과 학사
2015년 2월: 연세대학교 정보시스템 석사 (디지털 비즈니스 전공)
2015년 11월~현재: 연세대학교 바른ICT연구소 연구원
〈관심분야〉 정보보호정책 및 제도, 소셜 네트워크 서비스, 플랫폼 비즈니스, e-Business Strategy, ICT 사회적 가치

김 현 진 (Hyun Jin Kim) 정회원
2012년 2월: 연세대학교 정보시스템 석사 (디지털문화컨텐츠)
2001년 9월~2015년 12월: 한국정보화진흥원 수석연구원
2012년 3월~2015년 12월: APEC, ICDPPC 한국 대표단 및 FTA 전자성거래분과 협상단
2016년 1월~현재: 한국신용정보원 정보보호팀장
2014년 3월~현재: 남서울대학교 산업보안학과 외래교수
〈관심분야〉 De-identification, Pseudonymization, Cross-border Personal Data Transfer, Big Data Processing & Analysis

김 범 수 (Beomsoo Kim) 종신회원
1999년: 미국 University of Texas at Austin (Ph.D)
1999년~2002년: 미국 University of Illinois at Chicago, 조교수
2002년~현재: 연세대학교 정보대학원 교수
2014년~현재: 연세대학교 바른ICT연구소 소장
2015년~현재: OECD 정보보호 부의장
〈관심분야〉 정보보호정책 및 제도, 프라이버시 권리, 개인정보 보호, 전자상거래, 정보경제학