https://doi.org/10.5392/JKCA.2020.20.08.034

IoT 환경의 비식별 개인 민감정보관리 강화에 대한 연구

A Study on Reinforcing Non-Identifying Personal Sensitive Information Management on IoT Environment

양윤민*, 박순태, 김용민*****

전남대학교 정보보안협동과정*, 한국인터넷진흥원**, 전남대학교 전자상거래전공***

Yoon-Min Yang(ymyang@ahnlab.com)*, Soon-Tai Park(stpark12@kisa.or.kr), Yong-Min Kim(ymkim@chonnam.ac.kr)*****

요약

IoT 시장의 안정화와 급속한 확장의 시대가 도래하고 있다. IoT 환경에서는 사물이 상황에 따라 통신의 주도권을 갖는 통신 환경이 발생할 수 있으며, 불특정 다수의 IoT 환경과의 통신이 발생하여 개인 민감정보의 철저한 관리의 필요성이 증대되고 있다. 특히 IoT 환경에서는 센서 간의 통신 과정에서 개인 식별 정보를 제외한 개인의 생활 패턴, 주변 환경 정보 등의 민감한 비식별 정보의 유출로 프라이버시 침해의 우려가 증대된다. IoT로 인한 환경의 변화로 얻는 이점도 있으나, 개인의 민감정보가 자신도 모르는 사이에 빅데이터라는 명목으로 어디론가 전송되는 문제점도 있다. IoT 환경에서 센서를 통해 전송되는 개인 민감정보의 안전한 관리를 위해 초기 수집 방법과 민감정보 국외 이전 관리에 관한 사항, 그리고 2020년 8월 5일 시행되는 데이터 3법으로 IoT 환경의 비식별 개인정보의 활용의 본격적인 활성화가 예상됨에 따라 IoT 환경의 비식별 개인정보 보호 강화를 위한 사항을 제안하고자 한다.

■ 중심어 : | IoT | 개인정보 | 개인 민감정보 | 비식별 개인정보 |

Abstract

An era of stabilizing IoT markets and rapid expansion is coming. In an IoT environment, communication environments where objects take the lead in communication can occur depending on the situation, and communication with unspecified IoT environments has increased the need for thorough management of personal sensitive information. Although there are benefits that can be gained by changing environment due to IoT, there are problems where personal sensitive information is transmitted in the name of big data without even knowing it. For the safe management of personal sensitive information transmitted through sensors in IoT environment, the government plans to propose measures to enhance information protection in IoT environment as the use of non-identifiable personal information in IoT environment is expected to be activated in earnest through the amendment of the Data 3 Act and the initial collection method.

■ keyword : | IoT | Privacy | Personal Sensitive Information | Non-identifying Personal Information |

접수일자 : 2020년 05월 28일
수정일자 : 2020년 06월 16일
심사완료일 : 2020년 06월 23일
교신저자 : 김용민, e-mail : ymkim@chonnam.ac.kr

I. 서 론

우리나라는 지능정보사회의 핵심 사항으로 4차 산업혁명을 선정하고 있으며, 미래 정보화의 변화를 주도할 것이라고 예측하고 있다. 즉, 3차 산업혁명인 정보화 혁명과 달리 4차 산업혁명은 혁신적인 패러다임의 변화를 가져올 것으로 보고 있다. 그중 사물인터넷(Internet of Things: 이하 IoT)은 생활의 다양한 측면에 영향을 주고 있으며, IoT 기반 서비스는 광범위하고 다양한 형태로 등장하고 있으며, 사람, 사물, 그리고 컴퓨터를 연계하여 다양한 서비스를 구현하고 있다[1].

가트너(Gartner)는 IoT의 경제적 부가가치가 2020년 1.9조 달러에 이를 것이라고 전망하였고(Gartner, 2013), 맥킨지(Mckinsey)는 9개 주요 환경 분야에서의 IoT 활용수준이 2025년까지 연간 최소 3.9조 달러에서 최대 11.1조 달러까지 성장할 것으로 보았다(McKinsey Global Institute, 2015). 우리나라도 IoT 시장규모가 2013년 2조 3,000억 원에서 2020년 17조 1,000억 원으로 증가하리라 전망되고 있다[2].

IoT 환경에서는 최초 동의한 포괄적인 개인정보 수집 동의를 통해 IoT 센서에 의해 주도되는 정보 수집과 통신이 발생하게 된다. IoT 환경의 특성상 상대를 식별할 수 없는 개방된 통신이 이루어지는 과정에서 빅데이터 처리 목적의 “개인의 결제 패턴, 주변 환경 정보, 기타 생체정보” 등 개인을 즉시 식별할 수는 없으나 재식별이 가능한 비식별 데이터와 같은 개인 민감정보 관리의 중요성이 높아지고 있다. 따라서, 본 논문에서는 IoT 환경에서 개인정보 수집 단계에서부터 개인 민감정보 유출을 통제하기 위한 관리 방안을 제시하고자 한다.

II. IoT 환경의 개인 민감정보 현황

IoT에 대한 안전한 활용을 위해서는 제도의 기준에 맞게 개인정보를 안전하게 보호할 수 있는 가이드 및 기술적 조치 등이 필요하다.

현재 국내 법령은 "정보통신망 이용촉진 및 정보보호 등에 관한 법률"이나 "개인정보 보호법"을 통해 민감정보에 대하여 원칙적으로 수집을 금지하되, 예외적으로 정보주체의 동의 혹은 법령상 규정에 의해서만 수집하도록 허용하고 있다. 이를 강화하기 위해 데이터 3법(2020.08.05 시행)에 따르면, 데이터 이용 활성화를 위한 가명 정보의 도입과 데이터 활용에 따른 개인정보처리자의 책임을 강화하며 모호한 '개인정보' 판단 기준을 명확히 명시하고 있으며, "정보통신망 이용촉진 및 정보보호 등에 관한 법률" 및 "개인정보 보호법“에 중복 규제를 정비하여 ”개인정보 보호법“으로 일원화하였다.

1. IoT 환경의 개인정보보호 위험

IoT 환경에서 민감정보는 센서 자체의 자율적인 정보수집, 처리 및 데이터 공유가 이루어질 수 있기 때문에 다양한 정보 원천(서비스, 디바이스 등)을 통해 발생한 데이터 결합의 우려가 발생할 수 있다.

예를 들어 IoT 환경에서 생성된 데이터 마이닝을 수행하면 개인의 새로운 정보를 식별 할 수 있어 위험을 초래할 수 있다. 보편적인 ICT 환경에서의 개인정보 보호와는 다른 관점의 접근이 필요하다[3]

IoT 환경에서 여러 기술이 서로 유기적으로 연계되어 운용될 때, 각 기술이 가지고 있는 자체 보안 문제점, 기술 연계 시 발생하는 새로운 보안 취약점, 그리고 언제 어디서나 연결할 수 있는 IoT가 태생적으로 내재하고 있는 개인정보보호 문제 등 다양한 보안 문제들이 심각하게 대두될 것이다. 문제 해결을 위해 기술적인 해결책뿐 아니라 법제적인 측면에서도 선제적으로 대응하는 것이 중요하다. 그러므로 현재의 환경과 달리 IoT 보안 및 개인정보보호를 위해서 다양한 관점과 새로운 시각으로 접근해야 한다는 지적이 나오고 있다[4].

[표 1]은 IoT 환경에서 개인정보의 개념을 정리한 내용이다.

IoT 환경에서 생성되는 개인정보의 개념 수립 및 사전동의 제도 보완, 비식별 개인정보와 민감 정보 관리 관점의 보안 및 개인정보보호 이슈에 대응해야 한다[5].

2. 개인 민감정보의 특성

개인정보보호법 제23조에 명시된 민감정보란 사상, 신념, 노동조합, 정당의 가입, 탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그밖에 정보 주체의 사생활을

표 1. ICT환경의 개인정보의 개념별 분류

분류	내용
개인식별 정보	- 개인을 직접 식별하거나 유추하여 알 수 있는 모든 정보 - 해당 정보만으로는 특정 개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함(이름, 주소, 이메일 주소, 신용 카드 번호, 주민등록번호, 인터넷 주소 등)
비식별 정보	- 특정 개인을 알아볼 수 없더라도 불특정 다수의 특성을 파악 할 수 있는 정보 - 개인정보를 복원할 수 없도록 한 정보
민감 정보	- 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보 - 사상, 신념, 정치적 견해, 건강, 성생활 등에 관한 정보

현저히 침해할 우려가 있는 개인정보로서 대통령령이 정하는 정보(유전정보, 범죄경력에 해당하는 정보)이다.

"개인정보 보호법"이 민감정보의 판단기준을 "사생활 침해 우려"라고 규정하고 있는 반면, "정보통신망 이용촉진 및 정보보호 등에 관한 법"은 "사생활 침해" 뿐만 아니라 "개인의 권리·이익 침해"까지 포함하고 있다. GDPR(General Data Protection Regulation)의 경우 '특수한 유형의 개인정보'라고 언급하며, 이러한 개인정보를 더 구체적으로 보호해야 하는 이유로 '기본권과 자유 침해의 위험'을 제시하고 있다.

일본의 경우는 "배려를 필요로 하는 개인정보"라고 표현하고 있다. 본인에 대한 부당한 차별, 편견 등 불이익이 생기지 않도록 그 취급에 특별히 배려를 필요로 하는 것을 기준으로 규정하며, 이처럼 민감정보는 통상적으로 다른 개인정보와 달리 취급해야 할 필요성이 인정되는 경우를 의미한다. 이에 대하여는 반드시 '민감정보'라고 표현하는 것은 아니며, '특수한 범주(유형)의 개인정보'(GDPR), '배려를 필요로 하는 개인정보'(일본) 등으로 표현되기도 한다[6].

우리나라에서는 과거「공공기관의 개인정보보호에 관한법률(법률 제4734호)」에 의해 특별히 민감정보라는 표현으로 규정하고 있지는 않았다. 다만 동법은 "공공기관의 장은 사상·신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 아니 된다"고 규정함으로써(공공기관의 개인정보보호에 관한 법률 제4조 전문) 기본적 인권을 침해할 우려가 있는 개인정보의 수집을 원칙적으로 금지하였다. [표 2]는 개인의 민감정보를 세분화하여 특성에 따라 "사상, 신조, 기타 민감한 정보"에 대한 예시이다.

표 2. 개인 민감정보의 특성에 따른 분류의 예

유형 분류		개인정보의 예시
일반 정보	일반정보	이름, 주민등록번호, 주소, 전화번호, 생년월일, 출생지
신체적 민감정보	신체정보	얼굴, 지문, 홍채, 음성, 키, 몸무게
	의료, 건강정보	건강상태, 진료기록, 신체장애
정신적 민감정보	기호, 성향정보	도서, 구독정보, 여행내역, 웹사이트 결제 내역
	신념, 사상정보	종교, 정치 정당, 노조 가입여부
재산적 민감정보	금융정보	소득정보, 신용카드 정보, 계좌번호
	신용정보	개인 신용 평가도, 대출 내역, 신용카드 사용 내역
사회적 민감정보	교육정보	학력, 성적, 출석상황, 자격증 보유내역, 상벌기록
	법적정보	전과, 법죄 기록, 재판기록
	근로정보	직장, 고용주, 근무처, 상벌기록, 직무 평가

이러한 항목들의 법적 지침이「개인정보보호법」의 민감정보 규정의 전신이라고 할 수 있다[7].

"정보통신망 이용촉진 및 정보보호등에 관한 법"은 융통성을 위하여 민감정보에 대한 세부적 기준을 제시하고 있지 않으나, 제22조 1항을 통해 이용자의 동의를 받거나 다른 법률에 따라 특별히 수집 대상 개인정보로 허용된 경우에는 필요한 범위에서 개인정보를 수집할 수 있게 되어있다[8]. 예를 들어, 논란이 되었던 숙박앱 '여기어때'의 개인정보(고객 이름, 전화번호, 숙박이용정보)는 현재의 "정보통신망 이용촉진 및 정보보호 등에 관한 법"을 기반으로 예시적 방식을 통해 수집한 개인정보 중 해석에 따라 일부 '민감정보'에 해당하는 개인정보가 포함될 수 있다. 예시적 방식은 추상적인 법 개념을 보충 설명하기 위해 열거한 것으로서 열거된 것에 대해서만 법적 의미나 효과가 한정되지 않는다. 한정적 열거의 경우 '한정', '열거'와 같은 의미로 쓰이며, '한정'이란 말 그대로 일정 부분으로 제한하기 때문에, 한정된 최소한의 개인정보를 수집하는데 적합한 방식이다.

이와 관련한 연구로 비식별 처리된 개인 민감정보는 데이터 특성을 통해 재식별 가능성이 산출되기도 한다. k-익명성, ℓ-다양성, t-근접성을 만족하도록 개인정보를 비식별화하는 방법으로, KTL 모델로 불린다. KTL 수치에 따라 재식별 가능성도 커지게 된다. 미국 교육부 '프라이버시 보호 기술지원센터'의 안전도 기준에는 k=3을 안전도를 보장하는 최소한의 수준으로 보고 있

으며 5〈k〈10 일 경우 안전도가 높은 수준으로 간주하며, k-익명성이 3 이하로떨어질 때 비식별 처리된 개인 민감정보의 재식별 가능성이 커진다고 간주하고 있다. 다만, 이는 무조건적인 기준이 아니며 적절한 k 값은 해당 개인정보에 대한 전문가 집단의 판단에 의해 정해진다[9].

3. IoT 환경과 개인 민감정보

IoT의 패러다임은 사람들의 일상에서의 사용성 측면의 모니터링을 통한 최적화로 더 이상 수동적이고 반응이 없는 환경이 아니다. IoT는 지능적이고 인터넷에 연결된 인터랙티브 환경으로, 더 많은 기능을 통해 개인의 다양한 정보를 필요로하고 있다. 이 과정에서 일부 은폐된 운영 환경 속에서 사용자의 동의 없이 자동처리되는 개인정보도 있을 수 있어, 이를 통해 개인의 민감한 정보도 함께 유출될 수 있어 주의를 필요로 한다[10].

가정에서 사용하는 가전 기기에 부착된 센서를 통해 집안 내 상황에 대한 정보를 비롯하여 행태정보, 민감정보 등이 수집되거나, 웨어러블 디바이스를 통해 생체분야에서 수집되는 대부분의 정보는 건상 상태, 질병 여부, 신체정보 등 개인정보보호법상 민감정보에 해당할 여지가 큰 민감도가 높은 정보가 수집된다. 각 기기들로부터 측정된 결과가 집결되는 구간에 대한 데이터 관리의 문제점이 발생할 수 있다.

비식별 조치 기준은 법적 효력이 없는 지침이기 때문에 위와 같이 수집되는 민감정보의 유출 시 빅데이터 내에서 정보의 결합을 통해 재식별이 가능한 우려가 있으며[11], 이와 같은 우려로 비식별 조치된 개인정보에 대한 사후관리 절차를 [그림 1]과 같이 표현하며, “1단계 사전 검토, 2단계 비식별 조치, 3단계 적정성 평가, 4단계 사후관리” 4단계로 제시하고 있다.

비식별 조치를 거친 정보에 대해서는 “개인정보보호법”에서는 “통계작성 및 학술연구”와 같은 최소 범위의 분야에 활용을 허용하고 있다.

4. 4차 산업혁명과 데이터 3법

데이터 3법은 데이터 이용을 활성화하는 "개인정보보호법", "정보통신망 이용촉진 및 정보보호 등에 관한 법률", "신용정보의 이용 및 보호에 관한 법률" 등 3가지 법률을 통칭하며, 4차 산업혁명 시대의 핵심 자원인 데이터의 이용 활성화를 통한 새로운 산업 육성을 지원하기 위함이다.

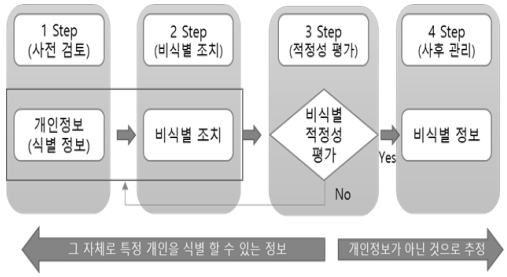

그림 1. 비식별 조치 및 사후관리 절차

특히, 새로운 산업 육성을 위해서는 인공지능, 클라우드 서비스, IoT 등 신기술을 활용한 데이터 이용이 필요하다. 한편 안전한 데이터 이용을 위한 사회적 규범 정립도 시급하다. 데이터 이용에 관한 규제 혁신과 개인정보보호 협치(거버넌스) 체계 정비의 두 문제를 해결하기 위해 데이터 3법이 2020년08월05일에 시행된다.

데이터 3법의 주요 법령별 개정사항은 [표 3]과 같으며, ”개인정보보호법, 신용정보법, 정보통신망 이용촉진 및 정보보호 등에 관한 법“을 통해 비식별 개인정보에 대해 학술연구 및 제한적 용도에 허용하여 빅데이터 분석 및 이용을 공익을 위해 활성화될 전망이다.

표 3. 데이터 3법 주요 개정사항

법명	주요내용
개인정보보호법	· 가명정보 개념 도입 및 동의없이 사용가능한 목적범위 구체화 · 가명정보 이용시 안전 장치 및 통제수단 마련 · 개인정보관리 감독을 ‘개인정보보호위원회’ 로 일원화
신용정보법	· 금융분야 빅데이터 분석 이용 법적 근거 명확화 · 신용정보 통합조회 도입 및 금융분야 규제 정비 · 신용주체자의 본인 정보 통제 기능 강화
정보통신망이용 촉진 및 정보보호 등에 관한 법	· 온라인 이용자들의 개인정보 규제 감독권 ‘개인정보보호위원회’로 이관

그중 “개인정보 보호법” 제15조 3항에 “개인 정보처리자는 당초 수집 목적과 합리적으로 관련된 범위 내에

서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 등을 고려하여 대통령령이 정하는 바에 따라 정보주체의 동의 없이 개인정보를 이용할 수 있다."의 내용이 추가되었으며, 제52조 2항을 통해 "익명정보는 개인정보보호법의 적용을 배제"가 신설되었다[12].

"정보주체의 동의 없는 개인정보의 이용"을 통해 IoT 환경과 같이 자동처리되는 개인정보가 있을 수 있는 환경에서 서비스 범위의 확대로 개인정보의 제3자 제공을 위해 별개의 동의를 받도록 하거나, 동의를 받아 수집한 이후에 동의 범위에 포함되지는 아니하지만 여러 가지 이유로 개인정보의 처리가 필요한 경우에도 동의가 없다는 이유로 처리 가능 여부가 불명확해 법 위반 가능성을 전적으로 배제하기 어려운 경우가 많았다. 앞으로는 이러한 경우에 애초 목적과 합리적 범위 내에서 처리가 가능 하도록 함으로써 필요한 범위 내에서 유연한 법 적용이 가능하도록 했다[13].

Ⅲ. IoT 환경의 비식별 민감정보 관리 방안

1. 비식별 개인 민감정보 관리

기존의 ICT 환경과 달리 IoT 환경에서는 M2M 및 Edge Network 통신등 자동화된 데이터 교환의 빈도가 높으며, 정보 주체의 동의를 개별적으로 받는 것이 어려우므로 정보주체는 충분한 정보를 갖지 못한 상태에서 포괄적인 개인정보 수집 동의를 하게 된다. 이를 통해 IoT 환경에서 생성되는 다량의 정보는 빅데이터 분석 및 교차비교 등을 통해 2차 데이터로 활용하여 초기 수집 목적과 다르게 개인의 민감정보 유출로 이어질 위험이 커지고 있다.

아울러, 인터넷의 활용으로 인해 IoT가 주는 편의성은 더욱 확대될 것으로 예상된다. 그런데도 국가 간, 대륙 간 서로 다른 보호 수준과 집행방식의 차이로 개인 민감정보의 주체의 권리를 보호하기가 어려운 상황이다. 이러한 개인정보의 국외이전 문제를 일부 완화하기 위해 할 수 있는 방법이 표준계약 제도를 통한 책임성에 기반한 접근법이다.

표준계약제도란 개인정보 소유자와 개인정보 국외처리자 간의 의무사항을 계약 자유의 원칙인 계약을 통해 상호 이행을 약속하도록 만드는 제도로, 개인정보 처리 주체가 속해있는 개인정보 국외 처리자의 감독기구나 책임 있는 정부가 그 의무사항을 자국법에 맞추어 규정하고 이를 개인정보 국외 처리자가 계약을 통해 이행할 수 있도록 해주는 제도이다.

개인정보 수집에 융통성을 가지나 민감정보가 함께 유출될 수 있는 추상적인 법 개념의 예시적 방식은 문제점과 이를 개선할 한정적 방식에 대한 내용과 개인 민감정보의 국외이전의 문제점을 개선할 수 있는 접근법의 고려와 IoT 환경에서 비식별 개인정보의 보호를 강화하는 방안이 요구된다. 관련 문제점 개선을 위해 책임성 기반의 접근법을 제안하며, 마지막으로 데이터 3법으로 IoT 환경의 비식별 개인정보의 활용이 본격적인 활성화가 예상됨에 따라 IoT 환경의 정보보호 강화를 위한 사항을 제안하고자 한다.

2. 한정적 열거방식 접근

개인 및 정보 주체의 수집 동의가 있었어도, 일반적인 온/오프라인 환경과 IoT 환경에서의 정보 수집은 차이점이 있으며, IoT 환경은 개인정보 수집 주체의 정보 수집에 대한 자유도가 높은 환경으로, 빅데이터라는 명목으로 개인정보가 서비스 제공 업체로 자유롭게 흘러가게 된다. [그림 2]와 같이 IoT 환경에서는 개인 민감정보의 "수집, 저장, 이용, 파기"의 과정에서, 기존 ICT 환경과는 다른 환경적 문제로 인해 정보의 유출과

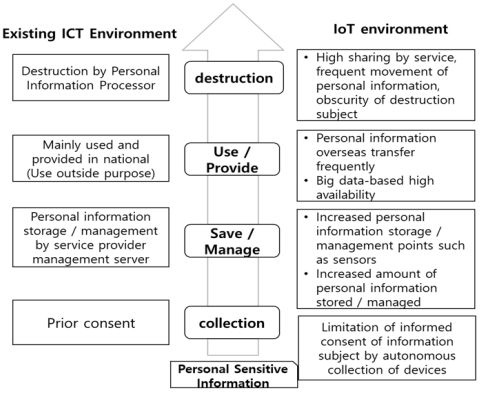

그림 2. 환경에 따른 개인 민감정보 관리 체계

오남용의 가능성이 높은 상황이다.

이와 같은 문제점 개선을 위해 IoT 서비스의 경우 최초 개인정보 사용 동의를 얻고자 할 때 개인정보 수집 범위를 [표 4]와 같이 한정적으로 열거하여 서비스 업체의 예시적 방법을 통해 포괄적이고 만능적인 정보 수집에 제한을 두어야 한다.

표 4. IoT 환경에서의 한정적 정보 수집 안내 예시

환경 구분	수집 정보	정보 제공	선택적 수집
사용자명			O
고정형 IoT (건축물 실내/외 부착)	입출입 시간		O
	온도, 습도	O	
	집의 구조		O
	공기질 상태	O	
	전력 사용량		O
이동형 IoT (신체 부착 및 이동수단)	맥박,혈압		O
	기압차	O	
	수면정보		O
	위치정보		O
	차량 속도정보		O
	구동장치 컨디션	O	
	주행환경 컨디션	O	
	주행거리		O
	주행시간		O

서비스 제공 과정에서 정보 주체의 특징이 필요한 경우에는 한정적 수집 동의를 통해 제공 및 개인정보를 침해할 우려가 있는 비식별 정보에 대해서는 제도적으로 사전에 정보 전송이 제어될 수 있는 체계를 마련해야 한다.

3. 유럽연합 일반 데이터 보호 규칙 관점의 대응

GDPR(General Data Protection Regulation) 유럽연합 일반 데이터 보호 규칙(2018.05.25)에 따르면, EU는 EU 내 수집된 개인정보의 역외 이전을 원칙적으로 금지하지만, EU가 인정하는 메커니즘에 따라 역외 이전을 허용한다. 적정성 결정(adequacy decision)을 통하여 개인정보보호 관련 법제가 적절한 수준의 보호를 보장하고 있다고 인정된 나라로 이전하는 경우 및 '적절한 보호조치(appropriate safeguards)의 제공', '정보주체의 권리 행사 보장', '효과적인 법적 구제 수단의 존재'에 모두 해당하는 경우이다[14]. 개인정보의 국외이전 시 GDPR에서 언급하고 있는 적정성에 대한 보장을 통해 개인정보의 국외이전에 대한 책임성을 갖는다는 것을 전제하고 있다. 즉, 책임성 기본 원칙(basic principle of accountability)을 국경 간 개인정보 유통의 맥락에서 고려하면서, 보증되지 않은 국가로의 개인정보의 국외이전은 위험을 야기하고 있다. 이 위험에 대한 책임은 정보관리자가 감수하여 처리해야 함을 강조하고 있어, 이와 같은 제도를 IoT 환경에 적용하는 것이 활발하게 이뤄진 사항은 아니다. 관련 개선을 위해서는 표준계약제도를 이용해 국가 간 개인정보 이동에 책임성을 부여하여 관리할 필요성이 있다. 책임성에 기반하여 개인 민감정보의 안전한 관리를 하기 위해서 각 국가의 법에 의한 관리가 아닌, 표준계약 제도를 통해 당사자 간 계약제도임에도 불구하고 감독기구의 행정적 통제가 가능하도록 하여 개인정보가 국외로 제공되었더라도 계약 조항에 따라 감독기구가 직·간접적 사후조치를 취할 수 있도록 하여 정보 주체의 권리를 적절히 보장할 수 있는 주요한 수단으로 인식되고 있다.

4. 데이터 3법 관점의 대응 기술

IoT 환경과 같이 센서 장비의 통신을 통해 사용자의 최초 승인 이후 인지할 수 없으며, 거부할 수 없는 상황에서의 정보 전송으로 개인의 민감정보 유출이 우려될 수 있다. IoT 환경에서 이러한 문제점을 보완하기 위해서 데이터 3법은 "영리·부정한 목적의 재식별 시 징벌적 과징금 부과"와 같은 엄격한 사후 처벌 항목이 신설되었다. 개방된 환경의 특성상 IoT 센서들의 통신 과정에서 개인의 민감정보(맥박, 체온, 결제 성향, 주변 온도 등) 중 일부의 정보가 즉시 개인을 식별할 수 없지만, 재조합 시에 개인 민감정보로 인해 문제가 될 수 있는 정보 유출의 가능성이 높은 상황이다. 이와 같은 상황은 [표 5]의 문제점들이 대표적이며, 데이터 3법으로 정보의 사용 규제가 완화될 경우 이전보다 더 많은 보안의 문제점이 발생할 수 있다. 따라서, 사용자 관점의 보안 대책뿐만 아니라, IoT 기기 제조사에서 [표 5]의 문

제에 대한 기술적 대응을 위한 적극적인 검토가 필요하다.

표 5. IoT 환경의 보안 이슈와 대응 기술

문제점 분류		대응 기술
항목	현상	
센서 통신의 유출	가로채기 공격 피해 개인 민감정보 및 센서 취약점 노출	IoT 기기에 적합한 경량 암호화 통신 반영
통신 패턴의 변화	정보 수집 서버 공격 피해 DDoS 공격 피해	데이터 흐름을 모니터링하고 예상을 벗어나는 트래픽 패턴의 감지
센서 취약점	센서 장비 탈취로 DrDoS등에 이용	주기적인 제품 취약점 분석 및 대응을 위한 업데이트 제공

데이터 3법을 통해 본격적인 익명 정보의 활용도가 높아지는 상황에 대비하여, 의료 환경에서 개인 민감정보 관리를 위한 국제 표준인 ISO 25237에서 제시하는 비식별화 절차를 살펴볼 필요가 있다. ISO 25237에서는 식별 가능한 사람(identifiable person)에 대한 언급이 있으며, “신체적, 생리적, 정신적, 경제적, 문화적, 기타 신원에 따른 특징” 중 일부의 정보가 모여 직접 또는 간접적으로 식별될 수 있는 사람으로 정의하고 있다. ISO 25237는 식별 가능한 사람을 최소화하기 위해 개인정보 비식별화 절차로, 개인정보에 대한 “제거(Removal), 대체(Substitution), 퍼징(Fuzzing)”을 처리하는 단계에서 데이터 사용 목적에 따라 제시하는 익명화 기술을 제시하고 있다. 이와 함께 개인 식별자에 해당하는 정보를 몇 가지 규칙으로 대체하거나 사람의 판단에 따라 가공해 개인정보를 숨기는 휴리스틱 가명화(Heuristic Pseudonymization), 개인정보의 가공 시 일정한 알고리즘을 통해 암호화함으로써 개인정보를 대체하는 기법으로, 개인정보와 같은 주요정보에 널리 쓰이는 기법인 암호화(Encryption)등 현시점에 적합한 기술을 추가하여 관리한다면 비식별 개인정보를 통한 개인정보의 재식별 문제를 최소화 할 수 있을 것으로 본다.

Ⅳ. 결론 및 향후 연구

IoT 환경에서 쟁점이 되고 있는 개인정보보호 중 민감정보의 관리 방안의 중요성이 강조되고 있다. 민감정보는 개인의 감정이나 건강 상태와 같이 정보 주체의 프라이버시 침해 가능성이 큰 정보이며, IoT 환경에서 거부감 없이 수집되어 전송되는 민감정보의 관리 문제가 발생한 경우 사회적 혼란이 야기될 수 있다.

오늘날 기술의 발달로 IoT 환경이 대중화되고, 최근 데이터 3법과 같이 비식별 개인정보의 사용 시 규제를 완화하여 데이터의 활용도를 극대화하기 위한 환경에서 개인의 민감정보 관리가 중요한 시점이다. 이로 인해 IoT 환경과 같은 특수한 환경에서의 개인 민감정보 관리에 대한 방안이 논의되어야 할 시점이다.

본 논문에서는 IoT 환경에서의 비식별 개인 민감정보의 효과적인 관리를 위해 한정적 열거방식의 접근법과 GDPR 보호 규칙 관점의 대응, 마지막으로 데이터 3법 관점의 기술적 대응 방안에 대해서 제시하였다. 한정적 열거방식을 통해 IoT 서비스 제공을 위해 포괄적인 정보 수집에 제한을 두며, GDPR의 보호 규칙에서 가이드 하고있는 책임성에 기반한 표준계약제도를 통해 IoT 환경에서의 개인정보 국외 이전에 대한 관리를 목표로 하였다. 마지막으로 데이터 3법을 통해 IoT 환경에서의 ‘동의 없이 사용 가능한 개인정보’의 문제점 예방을 위해 휴리스틱 가명화(Heuristic Pseudonymization), 암호화(Encryption)를 통한 비식별 개인정보에 대한 재식별 문제의 최소화를 제시하였다.

본 연구에서 수행한 IoT 환경에서의 개인 민감정보의 관리 방안은 정보보호 분야 중 비식별 민감정보의 관리에 참고할 수 있을 것으로 기대하며, IoT 환경과 같이 특수한 환경에서의 비식별 민감정보 관리에 대한 지속적인 연구를 통해 새로운 개인정보 유출 사고를 예방해야 할 것이다.

본 연구의 한계점은 다음과 같다. IoT와 같은 특수한 ICT 환경에서 비식별 개인 민감정보관리에 대한 "기술적, 관리적, 법적" 관점을 아우르는 관련 연구가 부족한 상황으로 본 연구의 내용이 일반화되기에는 한계가 있다. 이러한 관점에 대해서 4차 산업혁명 관련 연구에서 본격적으로 다루어지게 되기를 기대한다.

참 고 문 헌

[1] YANG, Jinhong, "Aggregated Risk Modelling of Personal Data Privacy in Internet of Things," ICACT, 21st, p425-430, 2019.

[2] 신영진, "안전한 사물인터넷 서비스 확산을 위한 개인정보보호정책평가지표 개발에 관한 연구," 정보화정책 제25권, 제3호, pp29-51, 2018.

[3] Lizheng Liu, "A Smart Dental Health-IoT Platform Based on Intelligent Hardware, Deep Learning, and Mobile Terminal," IEEE, Vol.24, No.3, pp.898-906.,2019.

[4] 민경식, *IoT 환경에서 개인정보보호 이슈 발굴 및 정책제언에 관한 연구*, 한국인터넷진흥원, 2015.

[5] Antonio F. Skarmeta, "A decentralized approach for security and privacy challenges in the Internet of Things," IEEE WF-IoT, pp.67-72, 2014.

[6] 김민호, *정보통신서비스 분야의 민감정보 유형*, 방송통신위원회, 2017.

[7] 행정안전부, *공공기관 개인정보보호 알아두기, 2*015.

[8] http://www.law.go.kr/법령/정보통신망법/, 2020.3.20

[9] 전희주, "통계모형의 정확도에 기반한 비식별화 데이터의 품질 측정," 한국콘텐츠학회논문지, 제19권, 제5호, pp.553-561, 2019.

[10] Porambage, "The Quest for Privacy in the Internet of Things," IEEE, Vol.3, No.2, pp.36-45, 2016.

[11] 연세대학교 정보대학원, *스마트기기 보급 확대에 따른 개인정보보호방안 연구 - 사물인터넷 환경을 중심으로*, 2014.

[12] http://www.law.go.kr/법령/개인정보보호법/, 2020.3.20

[13] 강태욱, "데이터 3법 통과…의료·AI 등 산업 탄력 전망," KISO저널, 제38호, pp.25-29, 2020.

[14] https://gdpr.kisa.or.kr/gdpr/static/whatIsGdpr.do, 2020.5.18

저 자 소 개

양 윤 민(Yoon-Min Yang) 정회원

- 2017년 2월 : 단국대학교 정보통신학과 석사
- 2019년 3월 ~ 현재 : 전남대학교 대학원 정보보안협동과정(박사과정)
- 2007년 1월 ~ 현재 : 안랩

〈관심분야〉 : IoT보안, 네트워크 보안, 시스템 보안 등

박 순 태(Soon-Tai Park) 정회원

- 2000년 4월 ~ 현재 : 한국인터넷진흥원 보안위협대응 R&D 팀장

〈관심분야〉 : 정보보안관리, 정보보호 인력 양성, 정보통신기반보호, 정보보호 R&D

김 용 민(Yong-Min Kim) 종신회원

- 2002년 8월 : 전남대학교 전산통계학과 박사
- 2006년 3월 ~ 현재 : 전남대학교 문화콘텐츠학부/정보보호협동과정 대학원 교수

〈관심분야〉 : 시스템 및 네트워크 보안, 전자상거래 보안, 융합보안 등