韓國IT서비스學會誌
第15卷 第4號
2016年 12月, pp.41-62

Journal of Information Technology Services
https://doi.org/10.9716/KITS.2016.15.4.041

사물인터넷(IoT) 환경에서의 개인정보 위험 분석 프레임워크

이애리* · 김범수** · 장재영***

Risk Analysis for Protecting Personal Information in IoT Environments

Ae Ri Lee* · Beomsoo Kim** · Jaeyoung Jang***

■ Abstract ■

In Internet of Things (IoT) era, more diverse types of information are collected and the environment of information usage, distribution, and processing is changing. Recently, there have been a growing number of cases involving breach and infringement of personal information in IoT services, for examples, including data breach incidents of Web cam service or drone and hacking cases of smart connected car or individual monitoring service. With the evolution of IoT, concerns on personal information protection has become a crucial issue and thus the risk analysis and management method of personal information should be systematically prepared. This study shows risk factors in IoT regarding possible breach of personal information and infringement of privacy. We propose "a risk analysis framework of protecting personal information in IoT environments" consisting of asset (personal information-type and sensitivity) subject to risk, threats of infringement (device, network, and server points), and social impact caused from the privacy incident. To verify this proposed framework, we conducted risk analysis of IoT services (smart communication device, connected car, smart healthcare, smart home, and smart infra) using this framework. Based on the analysis results, we identified the level of risk to personal information in IoT services and suggested measures to protect personal information and appropriately use it.

Keyword : IoT, Personal Information, Personal Data, Risk Analysis, Privacy Infringement, Security

Submitted : April 28, 2016 1st Revision : September 16, 2016 Accepted : September 21, 2016

* 연세대학교 바른ICT연구소 연구교수, 주저자
** 연세대학교 정보대학원 교수, 바른ICT연구소 소장, 교신저자
*** 한국인터넷진흥원 책임연구원, 연세대학교 정보대학원 박사과정

1. 서 론

정보통신기술(ICT) 발전에 따라 우리사회는 초연결사회(Hyper-connected society)로 진화하고 있다. 초연결사회에서는 사람뿐만 아니라 모든 사물들이 서로 연결되어 시간과 장소의 제약 없이 정보를 공유하고 처리할 수 있게 되는데, 이는 사물인터넷(Internet of Things, IoT)을 통해 가능해 질 수 있다. IoT는 기존의 유비쿼터스 센서 네트워크과 사물지능통신에서 한 단계 발전된 개념이다(Lee, 2013). 인터넷에 연결된 사물은 2016년 약 64억 개에서 2020년에는 약 208억 개로 확대될 것으로 예상되며(Gartner, 2015) 다양한 산업에서의 혁신을 가져올 것으로 기대된다.

IoT의 등장으로 수집되는 정보의 종류가 점차 다양해지고, 정보를 이용, 유통, 처리하는 환경이 변화하고 있다. 특히 IoT가 확산되면 새롭게 수집되는 정보의 양과 정보 수집 디바이스가 기하급수적으로 증가함에 따라, 개인정보보호 및 프라이버시 침해 이슈가 함께 부각되고 있다.

실제 IoT 환경에서 이러한 침해 사례가 다수 발생하고 있다. 그 사례에는 미국 제너럴 모터스의 텔레메틱스 서비스인 온스타(Onstar)의 개인정보 무단 수집 사례, 웹 캠 제조사인 트랜드넷의 동영상 유출 사건, Baby Monitor 서비스 해킹 사건, 무인기(Drone)를 활용한 개인정보 유출, 글로벌 보안기업 카스퍼스키랩(Kaspersky Lab)의 스마트카 해킹 시연 사례 등이 있다. 또한 구글 글래스와 갤럭시 기어, Virtual Reality(VR) 도구 등의 새로운 스마트기기 보급 확대에 따른 개인정보 침해 가능성이 지속적으로 제기되고 있다.

이와 같이 IoT 환경에서의 개인정보 침해에 따른 개인적/사회적 위험 발생 가능성이 높기 때문에 이에 대한 위험 분석과 관리 방안이 체계적으로 준비되어야 한다. IoT 환경 도래에 따른 개인정보보호 이슈와 관련하여 국내외적으로 대책 마련이 검토되고 있으나(EU, 2014; Shin, 2015), 아직까지 IoT에서의 개인정보와 관련한 법·제도/관리적/기술적 위험 대응방안이 체계적으로 제시되지 못하고 있다(Choi, 2015; Kang, 2015; Shin, 2015).

본 연구는 IoT 환경에서 발생가능한 개인정보 유출 및 프라이버시 침해 관련 위험 요인들을 파악하고, IoT 시대의 개인정보 위험을 분석할 수 있는 위험 분석 프레임워크를 제시하는 것을 목적으로 한다. 본 연구는 IoT의 기술적 특성을 고려하되, IoT 환경에서 개인정보와 관련한 관리운영 측면의 위험 분석 체계 구축에 보다 초점을 두고 있다.

본 연구에서는 새롭게 제시된 IoT 개인정보 위험 분석 프레임워크를 활용하여, IoT 활용 분야별(스마트 커뮤니케이션 디바이스, 커넥티드 카, 스마트 헬스케어, 스마트 홈, 스마트 인프라) 위험도를 분석하였다. 이를 통해 IoT 확산에 따른 개인정보 위험 수준을 파악하고 대책을 제언하고자 한다.

2. IoT 활용 분야와 개인정보

2.1 IoT 활용 서비스 분류

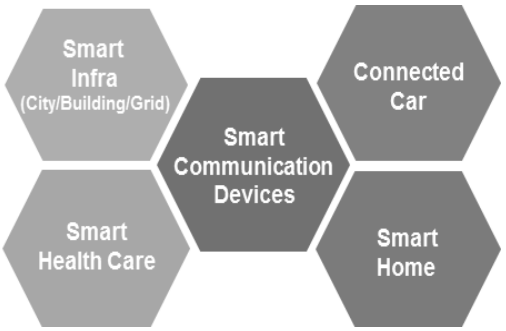
IoT는 고유하게 식별 가능한 사물이 만들어낸 정보를 인터넷을 통해 공유하는 환경으로, 기존의 유선 및 무선 인터넷 보다 진화된 단계의 상호연결성을 제공한다(Choi and Cho, 2015). IoT는 인간과 사물, 서비스 등 분산된 구성 요소들 간에 상호 협력적으로 센싱하고 네트워킹하며 정보 교환 및 처리 등의 지능적 관계를 형성한다(Joo and Kim, 2014). 본 연구에서는 IoT를 '각종 센서와 통신 네트워크를 통해 우리 주위의 사람/사물이 다양한 방식으로 연결되어 정보 교환 및 상호작용을 하고 이를 통해 새로운 가치를 창출하는 것'으로 정의하도록 한다.

IoT는 다양한 서비스 분야로 활용될 수 있다. Arthur(2011)은 IoT 활용 분야를 1) 스마트폰, 태블릿 PC등의 모바일 기기; 2) 스마트 미터와 스마트 그리드와 같은 에너지 분야; 3) 보안 및 감시 부분이 강화된 빌딩 자동화; 4) 커넥티드 카, 항공

기 등을 포함하는 이동 물체; 5) 산업 운영과 소매 유통 분야; 6) 의료 및 헬스케어 분야로 분류하였다. Gartner(2013)는 IoT의 구성 요소를 수평적인 기술 요소 시장과 수직적인 사업 시장으로 구분하여 전체적인 IoT 관련 생태계를 거시적으로 분석하였다. 수평적 기술 요소 시장은 산업, 교통, 유틸리티, 헬스케어, 스마트 시티, 물류, 기타 운영 기술, 스마트 홈, 농업, 접객(Hospitality)으로 구분하였고, 수직적인 사업 시장은 반도체, 하드웨어 서비스, 하드웨어, 운영체제, 미들웨어/보안 소프트웨어, 기반시설/게이트웨이, 커뮤니케이션 서비스, 데이터 센터 서비스, 기업 소프트웨어, IT 전문 서비스, IoT 전문 서비스로 분류하였다(Gartner, 2013). 한편, IoT의 주요 분야별 성장 전망을 보면, 홈 가전, 지능형 빌딩, 유틸리티, 자동차, 헬스케어 분야의 디바이스 수가 전체 IoT 연결 디바이스의 92%를 차지할 것이라고 전망되고 있다(Joo and Kim, 2014). 이러한 서비스의 특징을 살펴보면, 사용자에게 서비스를 제공하기 위해 수많은 디바이스를 통해 개인 사용자들의 다양한 정보가 생성/수집/공유 될 수 있다는 것이다. 예를 들어 스마트 그리드 분야의 스마트 미터는 사용자의 전력 사용 패턴, 가전기기에 대한 정보 등이 디바이스를 통해 생성/수집/공유 되는데, 이러한 정보는 프로파일링을 통해 사용자의 개인 상태 정보 및 프라이버시를 상세히 알 수 있어 개인정보보호에 대한 문제를 야기할 가능성이 있다(Park and Ahn, 2010).

한편, IoT 서비스에서는 스마트 폰, 스마트 홈, 스마트 그리드와 같이 '스마트'라는 용어가 많이 사용되는데, 이는 IoT에서 기본적으로 '스마트 기기'를 바탕으로 서비스들이 제공되기 때문이다. 스마트 기기란 '네트워크 기능이 탑재되어 인터넷 접속이 가능하며 OS 플랫폼을 통해 제공되는 다양한 기능 및 서비스를 이용할 수 있는 기기'를 말한다(KISDI, 2013). 따라서 IoT에서의 '스마트'는 '컴퓨팅과 통신 기능을 갖추고 네트워크에 연결 가능함'을 의미한다.

본 연구에서는 상기와 같은 기존 연구 조사를 참조하여, IoT 활용 분야 중 높은 비중을 차지할 것으로 전망되면서, 개인 사용자를 대상으로 서비스를 제공하여 프라이버시 침해 문제가 발생 가능한 분야에 초점을 두고, IoT 활용 분야를 아래 총 5가지로 분류하였다(<Figure 1> 참고). 또한 본 연구에서는 앞서 설명한 '스마트'의 개념을 가지고 IoT 서비스를 구분하였다.



〈Figure 1〉 IoT Areas

스마트 커뮤니케이션 디바이스(Smart Communications Device)는 커뮤니케이션을 중심으로 부가적인 컨텐츠 제공 기능을 포함하는 것으로서, 대표적인 서비스에는 스마트폰, 태블릿 PC, 스마트 안경, 스마트 시계 등이 있다. 아이폰 및 삼성/LG의 스마트폰, 구글 글래스, 애플 와치, 삼성 기어/VR 등이 이에 속한다.

커넥티드 카(Connected Car)는 IoT의 자동차 분야 서비스로서, 무선통신을 통해 차량과 내/외부 네트워크가 상호 연결되어 운전자의 편의성을 높일 수 있는 인포테인먼트형 서비스를 제공한다(KCA, 2013). 제너럴 모터스(GM)의 온스타(OnStar)와 현대자동차의 블루링크(BlueLink) 등이 커넥티드 카 서비스에 해당된다.

스마트 홈(Smart Home)은 IoT의 가전제품 분야 서비스로서, 가전에 네트워크 기능을 연결하고 서비스 제어 기능을 탑재함으로써 자동적으로 가전제품이 최적의 성능을 발휘할 수 있도록 하는 등 다양한 홈서비스를 제공한다. 스마트 TV, 스마트 냉장고, 스마트 청소기 등이 이에 속한다.

스마트 헬스케어(Smart Healthcare)는 IoT의 의료/건강관리 분야 서비스로서, 대표적인 서비스로 웨어러블(Wearable) 헬스케어 디바이스를 꼽을 수 있다. 일일활동/수면 모니터링 기기인 핏빗(Fitbit)과 코벤티스(Corventis)의 심박동 모니터링 기기인 뉴밴트 앰씨티(NUVANT MCT), 프로테우스(Proteus)의 헬리우스(Helius, 복용 알약에 부착하는 스마트 센서)가 이에 속한다.

스마트 인프라(Smart Infra)는 스마트 시티/빌딩/그리드(Smart City/Building/Grid)를 포괄하는 개념이다. 스마트 시티는 IoT를 통해 도시 행정 효율과 거주민의 삶의 질을 높일 수 있는 서비스 및 기술을 말한다(Caragliu et al., 2011). 스마트 빌딩은 건축, 통신, 사무자동화, 빌딩 자동화 등의 시스템을 유기적으로 통합하여 첨단 서비스 기능을 제공한다(TTA, 2011). 스마트 그리드는 기존 전력망에 IT 기술을 결합하여 안정적이고 고효율의 전력망을 구축하는 차세대 전력 관리 시스템이다(KSGI and KOTRA, 2010).

2.2 IoT 환경에서 수집되는 개인정보와 위험

개인정보보호법 제2조에 의하면 '개인정보'란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보를 의미한다. '개인정보'는 협의적 의미로 살아있는 개인을 식별할 수 있는 정보를 의미하지만, 광의적인 의미로는 해당 정보만으로 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 개인을 알아볼 수 있는 정보들까지 포함한다.

이러한 관점에서 사물정보는 그 자체로는 개인을 식별하는 정보가 될 수는 없으나, 개인과 연계될 경우에는 개인정보가 될 수 있다. 따라서 사물정보 중 사물의 식별과 인증에 사용되는 정보(예 : IP 주소, MAC 주소, 단말의 USIM번호, 국제단말기인증번호(IMEI) 등)는 결합을 통해 특정 개인이 식별될 가능성이 있기에 개인정보로서 보호 가치가 있다. IoT에서는 기존 환경보다 무수히 많은 사물을 통해 개인과 관련된 다양한 정보들이 수집될 수 있으며 이들 정보들이 결합되어 활용될 수 있기 때문에 개인정보 유출 및 프라이버시 침해 위험이 높아질 수 있다.

IoT 서비스는 각종 단말 센서를 통해 개인의 위치정보, 사용행태 정보 등 사생활 관련 정보를 수집가능하고, 항시적인 네트워크 접속과 차별화된 서비스 제공을 위해 각종 개인정보가 요구된다. 커넥티드 카 서비스인 GM의 온스타(OnStar) 서비스를 예를 들어 살펴보면, 실제 상당히 많은 개인정보들이 수집되고 있음을 알 수 있다.

온스타 서비스는 차량 사고 시 실시간 응급 구조, 도난 차량 추적 및 감속 등의 서비스를 제공하며, GM의 중앙 콜센터와 통신하여 차량 위치 알림, 무선도어 잠금 알림 등을 앱을 통해 원격 제어하도록 서비스 한다(Jeon, 2013; KCA, 2013). 온스타 서비스에서는 차량 내 다양한 센서들을 탑재하여 필요한 정보를 수집되고, 모바일 네트워크를 사용하여 온라인 플랫폼으로 정보가 전달된다. 또한 해당 서비스 가입 시, 개인신상정보, 차량정보, 대금처리를 위한 결제정보 등이 수집되고 이러한 개인정보를 기반으로 서비스 제공이 이루어진다. 온스타에서 수집되는 정보를 정리하면 아래와 같다.

- 단말(센서)에서 수집되는 개인정보 : 위치정보, 이동 및 운전습관 정보(주행일자, 이동경로, 거리, 운행시간, 평균속도, 야간/주간 운행정보, 브레이크 밟는 빈도 등), 취향 및 생활습관 정보(통화 이력, 온라인 쇼핑, 음악 취향정보, 자주 방문하는 목적지 등), 차량상태 정보(시동 ON/OFF, 고장/사고 정보 등)
- 고유 사용자 식별 관련 네트워크 정보 : MEID (Mobile Equipment Identifier), IMSI(International Mobile Subscriber Identity), Bluetooth의 Specification ID 등
- 서비스 플랫폼에서 관리되는 개인정보 : 개인신상정보(이름, 주소, 전화번호, 이메일 등), 서비스 관련 정보(차량식별번호, 서비스 사용 로그 등), 금융결제정보(신용카드 정보 등)

상기 IoT 서비스 사례를 통해 알 수 있듯이 IoT 환경에서는 다양한 개인정보가 수집 가능하며 이러한 정보가 오용되거나 유출될 경우 그 피해가 심각해 질 수 있다. 실제, 온스타와 같은 커넥티드 카 서비스 사용 시, 중간자공격(Man-in-the-middle attack) 등을 통한 개인정보 해킹이나 비허가된 사용자의 차량 접근 가능성 등 개인정보에 대한 보안의 취약성이 이슈화 된 바 있다(Glen, 2015). 또한 커넥티드 카에서의 개인정보 유출로 인한 계정 탈취 및 명의 도용 위험까지 보고되고 있다(Naughton and Kharif, 2015).

이러한 개인정보에 대한 위협은 IoT 서비스의 단말, 네트워크, 서버 단(Point)을 통해 발생할 수 있다(KISA, 2014). 커넥티드 카를 예시로 하여 관련 위험 요인을 정리하면 다음과 같다.

- 단말 위협 : 차량 내 단말의 컴퓨터기기 또는 차량과 연결되는 스마트폰 앱(예 : 온스타의 RemoteLink App)에 접근하여 단말 단에 저장되어 있는 개인정보 유출 및 정보조작 가능, 해커 등 외부인의 불법적 기기 제어에 의한 개인 안전문제 초래 가능(Glen, 2015; Krisher, 2013).
- 네트워크 위협 : 주행 중 손쉽게 인터넷에 연결할 수 있도록 제공되는 무선 네트워크의 보안 취약성(보안 프로토콜 미비 등)을 이용하여 차량 네트워크에 침입, 3G/4G 및 블루투스 네트워크 스니핑 등을 통해 통신되는 개인정보/프라이버시 유출 가능(Krisher, 2013).
- 서버 위협 : 해당 서비스를 위해 서버 플랫폼에 저장 처리된 개인정보(운전습관정보 등)의 목적 외 사용에 따른 프라이버시 침해 가능성, 서버 시스템 공격을 통한 정보유출 가능(Glen, 2015).

위에서 살펴 본 개인정보 관련 단말/네트워크/서버 단 위험은 예시로 든 커넥티드 카 외 다른 IoT 서비스에서도 발생가능하다. 단, IoT 서비스 유형별로 수집되는 데이터의 종류와 위험의 강도, 그 영향력의 차이가 있을 수 있다.

3. 개인정보 위험 분석

앞장에서 살펴보았듯이 IoT 환경에서 수집되는 개인정보가 더욱 다양해지고, 주변의 센서와 편재된 연결망에 따라 개인정보 침해와 보안에 대한 위험 가능성이 높아질 수 있다. 최근 IT 보안 위협이 점차 전문화, 고도화되고, 복합해지면서 보안 사고도 IT 인프라 관련 사고에서 특정 정보(개인정보, 기업 비밀정보 등)에 대한 사고로 변화하고 있다. 다시 말해, 궁극적으로 보호해야 할 대상이 서버, 네트워크 등의 IT 인프라가 아닌 정보, 사람이므로 위험분석 기법 역시 전통적인 위험 분석 기법 외에 사람 중심, 정보 중심의 위험 분석으로 진화해야 한다(Infosec, 2008). 본 장에서는 IT에서의 위험 분석 개념과 기존의 위험 분석 프레임워크를 검토하였다. 이를 통해 IoT 환경에서의 위험 분석 프레임워크 개발에 참고하고자 한다.

3.1 IT 위험 분석 개요

IT 위험(Information Technology Risk)이란 정보기술과 관련한 위험을 의미한다. IT 위험이라는 용어는 정보 보안(Information Security)을 포괄하는 개념이다. 일반적으로, 위험은 사건 발생 가능성과 그 사건이 정보 기술 자산에 미치는 영향력의 조합으로 정의된다. 반면, 정보 자산에 미치는 사건의 영향력은 자산이 가지는 취약성과 그 자산이 이해 당사자에게 준하는 가치의 조합으로 정의된다. 발생 가능성은 특히 IT 위험 영역에서 위협으로서 표현될 수 있다. 위험과 IT 위험의 개념은 아래와 같이 정리될 수 있다(ISO/IEC, 2011).

- 위험(Risk) = (발생가능성, 영향력)
- IT위험(IT Risk) = (위협, 취약성, 자산가치)

일반적으로 IT 위험 관리에서 위험분석이란 정보시스템의 위험을 평가하고, 비용 효과적으로 보호 대책을 마련하기 위해 수행하는 IT 보안관리(IT Security Management)의 필수 과정에 속하

는 절차이다. 위험분석의 목적은 보호대상의 위험을 측정하고, 측정된 위험이 허용 가능 수준인지 판단하는 근거를 제공하는 것이다(TTA, 2000). 위험분석을 효과적으로 수행하기 위해서는 먼저 보호대상의 중요도를 파악하여 위험분석 범위와 수준을 결정하기 위해 사전위험분석을 시행해야 한다. 사전위험분석이란 상위수준에서 상세 위험분석이 필요한 고위험의 보호대상 또는 서비스를 식별하는 것을 말한다. 위험분석 수준에 따라서 수행 절차의 복잡성과 시간 및 인력 소모가 달라지므로, 시스템 환경에 맞는 위험분석 수준을 선택할 필요가 있다. 따라서 사전위험분석을 통해 위험분석의 수준을 기본통제 방식으로 할 것인지, 상세 위험분석으로 할 것인지를 결정하도록 한다. 기본통제는 국내외 표준기관 또는 산업계 표준기관의 발행 문서, 서비스 규모/유형이 유사한 기관에서 작성된 자료들을 이용할 수 있으며, 자체적으로도 서비스 환경에 맞는 기본통제를 도출할 수 있다. 상세 위험분석 방식은 보호대상의 중요도가 높거나 가치가 클 경우 적용하게 된다. 자산/위협/취약성/대응책 분석을 통해 위험을 산출하는 일련의 과정이 상세 위험분석에 해당된다. 일반적으로 위험분석을 수행함은 상세 위험분석 수행을 말한다(TTA, 2008).

IoT 환경에서의 위험 분석 프레임워크란 IoT 서비스들이 상용화되어 보급되었을 때 발생할 수 있는 여러 위험을 사전에 인지하도록 하여 이를 위한 대안을 도출할 수 있는 프로세스를 의미한다. 현재까지 위험 분석 프레임워크는 주로 정보시스템, 금융 등의 분야에서 각 특성에 맞게 개발되었으나 상호 간 복합적으로 사용하는 데는 한계가 있다. 본 연구에서는 기존의 위험 분석 프레임워크들의 장/단점을 분석하여 IoT 환경에 적합한 프레임워크를 제시하고자 한다.

3.2 기존 위험 분석 프레임워크

본 연구에서는 IoT 환경에서의 위험 분석 프레임워크 개발에 참고하고자, 대표적인 기존 위험 분석 기법들을 아래와 같이 조사 분석하였다. 특히 위험 요인 파악(식별)과 위험 분석 체계 구축에 있어 핵심이 되는 '위험 평가' 부분에 초점을 두고 살펴보도록 한다.

3.2.1 NIST SP800-30:2002

미국표준기술연구소(National Institute of Standards and Technology, NIST)는 미국 상무부 기술관리국 산하의 각종 표준을 담당하는 기관이다. NIST SP800-30은 비용 효과적인 정보보호 통제를 선택하는 데 필요한 방법을 제시하는 것을 목표로 작성한 표준화 문서이다(NIST, 2002). NIST SP800-30은 조직의 임무를 성공적으로 수행하기 위한 효과적인 위험관리 프로그램을 수립하는 데 참고자료로서 사용될 수 있도록 작성되었다.

NIST SP800-30에서 제시하는 위험 관리 단계 중 첫 번째 단계는 위험 평가이며, 9개의 세부 위험 평가 단계로 구성되어 있다. 위험 평가에 필요한 9단계 중에서 위험 평가 프레임워크에 필요한 위험 측정 방법과 관련된 단계는 5단계인 공산도(발생 가능성) 정의 단계와 6단계 영향력 분석 단계, 7단계 위험성 정의 단계까지의 내용이다. 공산도(발생 가능성) 정의 단계에서는 위협이 일어날 수 있는 발생 가능 정도를 3가지 등급(H, M, L)으로 평가한다. 영향력 분석 단계에서는 실제로 위협이 발생하였을 때 나타날 수 있는 영향력을 3가지 등급(H, M, L)으로 평가한다. 종합적인 위험의 정도를 결정하기 위한 위험성 정의 단계에서는 앞의 단계에서 측정된 공산도와 영향력을 각각 수치화하여 서로 곱한 값을 '위험도'라 정의하고, 그 값에 따라 위험도를 3가지 등급(H, M, L)로 분류한다.

NIST SP800-30의 5단계부터 7단계를 통해 이루어지는 위험 평가 방법에서는 시스템의 취약성과 위협의 대상이 되는 자산을 평가하여 그에 대한 영향력을 고려한 설계 방법을 사용하였다. IoT 환경에서 개인정보 위험을 평가하기 위해서는 위협의 대상이 되는 자산, 즉, 개인정보에 대한 위험도가 필수적인 요소로 고려되어야 한다는 점에서

NIST SP800-30의 위험 평가 방법을 참고할 수 있다. 하지만 NIST SP800-30이 적용되는 기존 시스템(주로 공공기관의 시스템에 국한)과 달리, IoT는 아직 시장에서 활성화되지 않은 상태이므로 취약성에 대한 기존 자료 수집이 어렵다는 점에서 NIST SP800-30를 그대로 적용하여 IoT 서비스의 위험을 평가하기에는 한계가 있다. 또한 NIST SP800-30에서는 위협에 따른 영향력을 평가하는 기준으로 손실되는 해당 기관의 자산 가치와 해당 기관의 평판/목적/이익의 손실 정도, 그리고 직접적인 인적 피해의 크기에 따라 그 수준을 결정한다. 이에 반해, IoT 환경에서는 특정 조직(기업)의 위험 보다는 개인정보의 위험 평가에 초점을 두고 있기 때문에 영향력 평가의 세부 항목 적용에 부적합한 면이 있으며, 평가의 기준이 되는 정의 부분에 수정이 필요하다.

3.2.2 KS X ISO/IEC 27005

KS X ISO/IEC 27005(KATS, 2014)는 정보보안 위험 관리(Information Security Risk Management, ISRM)의 국제표준인 ISO/IEC 27005를 기반으로 기술적 내용 및 국제 기준을 유지하면서 마련한 한국 산업 표준이다. KS X ISO/IEC 27005의 위험 분석 프레임워크의 목적은 위험 평가 시행과 적절한 통제 항목 구현을 통해 해당 조직에 적합한 위험 관리 체계를 구축하도록 활동 및 구현 지침을 제공하는 것이다.

KS X ISO/IEC 27005의 위험 분석 프레임워크에서는 상황 설정, 위험 평가, 위험 처리, 위험 수용, 위험 정보 교환, 위험 모니터링 및 검토라는 6단계의 프로세스로 이루어진다. 상황 설정 단계에서는 위험 분석을 위한 기본 기준 수립과 위험 분석의 범위/경계를 설정하도록 한다. 위험 평가 단계에서는 1단계에서 수립된 기준에 따라 위험을 평가하며, 위험 식별/산정/수준평가의 세부과정으로 구성된다. 이후 위험 처리 단계를 통해 평가된 위험을 어떻게 처리할 것 지 결정하고, 처리된 위험이 수용가능한 수준이라면 위험 수용 단계를 거쳐 수용된 위험 사항을 명시하고 해당 위험에 대한 처리와 수용 과정을 종료한다. 위험 정보 교환 단계와 위험 모니터링 및 검토 과정은 위험 분석 프레임워크 전체에 걸쳐 일어나며, 위험 프로세스 진행 과정을 지원한다.

전체 단계 중 위험 분석의 핵심에 해당되는 위험 평가 단계(위험 식별/산정/수준평가)에 대해 좀 더 살펴보면, 먼저 위험의 식별을 통해 잠재적 손실을 일으킬 수 있는 위험 요소를 식별하는데, 이는 자산 식별, 위협 식별, 기존 체제 식별, 취약성 식별, 결과 식별로 분류될 수 있다. 이러한 위험 식별을 통해 잠재적 손실에 대해 가능한 방법, 대상, 이유에 대한 통찰을 얻도록 한다. 다음으로 위험 산정을 통해 위험의 잠재적 결과 규모와 그 결과가 발생할 가능성을 검토한다. 위험 산정 방법은 상황에 따라 정량적이거나 정성적일 수 있고, 이들의 조합이 될 수도 있다. 끝으로 위험 수준 평가를 수행하기 위해서는 위험 발생 가능성 및 영향력에 의해 평가된 위험 목록과 위험 평가 기준이 있어야 한다. 이를 통해 위험 목록들의 위험 수준 우선순위를 비교할 수 있도록 한다.

KS X ISO/IEC 27005의 위험 평가 방법은 주로 조직 단위의 정보보안 관점에서 위험을 평가하고 이에 대한 대책을 세워 지속적으로 관리하는 프로세스 형태이다. KS X ISO/IEC 27005의 위험 평가 방법은 일반적인 조직을 대상으로 한다는 특성을 가지기 때문에, 기업, 정부기관, 비영리 조직 등 다양한 조직에 적용할 수 있다는 장점을 가진다. 반면 KS X ISO/IEC 27005의 프로세스를 적용하기 위해서는 위험 평가의 대상이 조직의 특성을 반영해야 한다는 데 한계가 존재한다. 즉, 조직의 목적, 업무, 가치, 구조 등이 결과에 영향을 주기 때문에 디바이스나 서비스 단위의 개인정보 보안이 필요한 IoT 관점에서 이를 적용하기에는 무리가 있다. 따라서 IoT 환경에서의 위험 평가를 위해 KS X ISO/IEC 27005의 전반적인 흐름은 참고할 수 있으나, 구체적인 내용까지 적용하기에는 한계가 있다. 그러므로 IoT 환경에서의 위험

평가를 위해서는 IoT의 특성에 적합한 개인정보 위험 분석 프레임워크를 구축할 필요가 있다.

3.2.3 ISACA RISK IT

정보시스템감사통제협회(Information Systems Audit and Control Association, ISACA)는 정보시스템과 기술에 대한 효과적인 거버넌스, 통제 및 인증 체계를 구축하기 위해 연구하며, 표준 및 실무활동을 개발하여 관련 산업 증진을 목적으로 설립된 민간 비영리 기관이다. ISACA(2009a)에서는 IT 위험관리를 위해 위험관리 프레임워크인 Risk IT를 개발하였다. Risk IT는 IT와 연관된 위험관리를 다루고 있고, 기업의 문화적인 요소나 운영적인 이슈까지도 포함하고 있다. IT 자원에 대한 위험은 쉽게 간과되기 쉬우며, 다른 위험들과 통합적으로 관리되는 것이 통상적이었으나 Risk IT에서는 이를 구분하여 IT 사용에 관한 비즈니스 위험을 분석하는 프레임워크를 제시하고 있다. Risk IT 프레임워크는 크게 위험 관리(Risk Governance), 위험 평가(Risk Evaluation), 위험 대응(Risk Response)의 3가지 도메인으로 나누어진다(ISACA, 2009b). 이들 3가지 도메인은 독립된 것이 아니라 상호작용적이다. 각 도메인은 다시 3가지 프로세스로 나눠진다. 위험 관리는 전사적 공통 위험관점의 설정 및 유지, 전사적 위험관리(Enterprise Risk Management, ERM)와의 통합, 위험을 인식한 비즈니스 의사결정 수립을 포함하고 있다. 위험 평가는 데이터 수집, 위험 분석, 위험 프로파일의 유지를 포함한다. 끝으로 위험 대응은 위험 계산, 위험 관리, 사고 대처로 구성된다.

이 중 위험 평가 도메인의 세부 단계를 좀 더 살펴보면, 먼저 데이터 수집 단계에서는 자료 수집을 위한 모델을 수립하고, IT와 관련된 위험요소를 식별하며, 효과적인 분석 및 보고를 위해 수집 위험 데이터를 정의한다. 위험 분석 단계에서는 IT 위험 분석의 범위를 정의하고, IT 위험을 측정하고, 위험 분석에 대한 리뷰 수행 등이 이루어진다. 위험 프로파일의 유지 단계에서는 기존 위험의 특성 자료를 최신 상태로 유지 관리토록 한다.

ISACA(2009a, 2009b)의 Risk IT 프레임워크는 위험 관리, 위험 평가, 위험 대응의 3가지 도메인이 상호작용을 통해 IT 위험을 관리하고 조직의 비즈니스 목표를 달성할 수 있도록 방향을 제시하는 역할을 한다. 단, Risk IT의 개발 목적은 기업 IT의 거버넌스 및 관리 강화와 IT 투자를 통해 기업의 비즈니스 가치 창출 체계를 보완하는데 초점을 두고, 조직의 IT 위험 관리 체계를 강화하는데 있다. 즉, ISACA의 Risk IT 프레임워크는 조직의 비즈니스 환경에서의 위험 관리 분석에 집중하여 특화되어 있기 때문에, IoT 환경에서의 개인정보 위험 분석에 부합하지 않는 측면이 있다. 따라서 이를 보완할 수 있는 새로운 프레임워크가 필요하다.

4. IoT 환경에서의 개인정보 위험 분석 프레임워크

본 연구에서는 IoT 환경에서 기업의 시스템 또는 비즈니스 영역을 포함하여 개인과 사회를 고려한 위험 분석 프레임워크를 제안하고자 한다. 본 연구에서 제시한 프레임워크는 개인정보보호 측면에 있어서 개인과 기업 모두에게 미칠 위험에 대비한 정책에의 활용을 목적으로 한다. 이를 위해 3장에서 살펴 본 기존 프레임워크가 가지고 있는 위험 측정 방법을 참조하되, 개인정보의 특성과 영향력이 반영되도록 변형 및 보완하였다. 새롭게 제안한 위험 분석 프레임워크의 구성 변수를 수식으로 표현하면 <Table 1>와 같다.

IoT 환경에서 개인정보보호를 위한 위험 분석 프레임워크에는 개인정보와 위험의 특성, 위험 발생으로 인한 영향이 고려되어야 한다. 따라서 IoT 환경에 적합한 위험 분석 프레임워크는 <Table 1>의 수식과 같이 크게 개인정보(Personal information), 위협(Threat), 영향도(Impact) 세 변수의 조합으로 구성하였다. 특히 본 연구에서는 궁극의 보호 대상을 사람과 정보에 초점을 두고, 사람과

정보 중심의 위험 분석이 이뤄질 수 있도록 프레임워크의 변수를 구성하였다. 다시 말해, 위험 분석 요인의 주요 대상을 사람에 대한 정보인 개인정보에 집중하였다.

본 연구에서는 기존에 일반적으로 받아들여지고 있는 위험 측정 방식인 'IT Risk = (Asset, Threat, Vulnerability)'에서 자산(Asset)을 개인정보(Personal information)로, 취약성(Vulnerability)을 영향도(Impact)로 대체하였다. 즉, 위험 측정에 있어 개인정보를 IoT 환경에서의 자산이라고 판단하여 자산을 개인정보로 나타내었다. 이는 사람 및 정보 중심의 개념이 반영된 변수로서, 개인정보는 개인정보의 종류와 개인정보의 민감도 측면을 포함한다.

그리고 아직 시장 활성화 및 본격적인 상용화 단계에 접어들지 않은 IoT 환경에서는 서비스가 가질 수 있는 취약성을 직접적으로 분석하기 매우 힘들다는 점을 고려하여, 본 연구에서는 개인정보 유출이 미치는 취약성을 투영하는 변수로서 사회적 영향력(Social Impact)에 초점을 두고 위험을 측정하도록 하였다. 사회적 영향력은 사람(즉, 개인)에 대한 정보 유출 및 프라이버시 침해 사고 발생 시 사람들이 받을 피해와 이로 인한 사회적 충격과 관련된 변수이다. 따라서 이는 사람 중심, 정보 중심의 위험 분석 의도가 반영된 변수이다. 사회적 영향력은 세부적으로 IoT 서비스 사용자수, 사용빈도, 시장 규모, 2차 결합 시장 규모로 구성된다.

한편, 본 연구에서 위협은 개인정보 유출 및 프라이버시 침해 위협 정도를 말하며, IoT 환경에서 개인정보가 생성/전달/처리되는 단말(Device), 네트워크(Network), 서버(Server) 영역에서의 침해 위협도가 모두 반영되도록 하였다. 특히 본 변수는 기기 및 시스템 장비 손상과 서비스 장애에 대한 위협 보다는 사람의 개인정보가 유출되고 침해되는 것에 대한 위협에 중점을 두고 있다. 따라서 위협 또한 사람과 정보 중심의 의미가 반영된 변수이다.

상기의 내용을 종합하여 최종적으로 도출된 IoT 개인정보 위험 분석 프레임워크는 <Table 2>와 같다. 프레임워크를 구성하는 상세 변수 내용에 대해서 아래의 4.1절에서 설명하도록 한다.

〈Table 1〉 Calculus for IoT Risk Analysis

IoT Risk to Personal Information = P×Personal Information+T×Threat+I×Impact = P×(P1×Type of Personal Information+P2×Sensitivity of Personal Information) + T×(T1×Threat to Device+T2×Threat to Network+T3×Threat to Server) + I×(I1×Number of Users+I2×Frequency of Use+I3×Market Size+I4×2nd Market Size)

〈Table 2〉 Risk Analysis Framework of Protecting Personal Information in IoT environments

	Generable and Usable **Personal Information** in IOT		**Threat** of Breach & Infringement			Social **Impact**			
	Type of Personal Information	Sensitivity of Personal Information	Device	Network	Server	#of Users	Freq. of use	Market Size	2nd Market Size
Connected Car									
Smart Home									
Smart Healthcare									
Smart Infra									
Smart Comm.									

4.1 변수의 정의 및 측정방법

4.1.1 IoT를 통해 생성 및 이용가능한 개인정보 (Generable and Usable Personal Information in IoT)

본 연구에서의 개인정보는 위험의 대상이 되는 개인정보를 말하며, 이는 IoT를 통해 생성 및 수집 가능한 개인정보로서 개인정보 종류와 개인정보 민감도의 조합으로 이루어진다.

① 개인정보 종류(Type of Personal Information)

개인정보 종류는 IoT 서비스 산업별로 각 서비스 이용 시 수집되는 개인정보들의 형태를 의미한다. 개인정보의 종류 변수는 수집되는 개인정보 중 개인 식별 가능성이 높은 정보가 많은 정도에 따라 수준을 H(높음), M(중간), L(낮음)로 측정할 수 있다. 즉, 주민등록번호와 같이 하나의 정보만으로 개인 식별이 가능한 개인정보가 많이 포함된 경우 H로, 대체로 2개 이상 결합된 정보로 개인 식별이 가능한 개인정보들이 포함된 경우에는 M으로, 결합된 정보로도 개인 식별이 어려운 개인정보만으로 이루어진 경우 L로 구분한다. 각 수준에 대한 위험 점수로는 H : 3점, M : 2점, L : 1점을 부여하도록 한다.

② 개인정보 민감도(Sensitivity of Personal Information)

개인정보 민감도는 개별 정보가 유출되었을 때 개인에게 심리적, 사회적, 경제적으로 영향을 미치는 민감 정도를 의미한다. 개인정보의 민감도 측정에 대해서는 Korea COP Forum(2008)의 IT 환경에서의 개인정보 민감도에 대한 기존 연구를 참조하였다. Korea COP Forum(2008)의 연구에서는 민감도에 대한 정보들의 조합 수준을 S(Service : 최고 민감도), G(General : 최저 민감도), P (Privacy)1~3(중간수준의 민감도로 숫자가 클수록 민감도가 높음)로 구분하였다. 본 연구에서는 기존 연구를 참조하되, 개인정보의 민감도를 H, M, L의 3가지 수준으로 구분하도록 제안한다. 민감도 수준은 개인의 사상, 신념, 병력, 자산 및 결제 내역 등과 같이 매우 민감한 개인정보가 포함된 경우 H(높음)로, 개인 일정 계획 등 개인에 따라 민감 정보라고 판단될 수 있는 정보가 포함된 경우 M(중간)으로, 공개 정보이거나 민감 정보로 보기 어려운 정보만으로 구성된 경우 L(낮음)로 측정토록 한다. 각 수준에 대한 위험 점수는 H : 3점, M : 2점, L : 1점을 부여한다.

4.1.2 유출/침해 위협 : 단말, 네트워크, 서버 위협 (Threat of Breach and Infringement : Device, Network, and Server)

위협은 개인정보 유출/침해의 원인이나 유출/침해 행위를 의미한다. IoT 환경에서는 정보 생성 및 활용 위치를 단(Point)으로 나누어 위협을 측정할 수 있다. 이는 정보가 생성/전달/처리되는 지점에서 개인정보 유출 및 침해로 인한 위험의 정도가 다를 수 있기 때문에 이를 구분하여 분석할 필요가 있기 때문이다. KISA(2014)의 국가정보보호백서에 따르면 IoT의 기술 구성 요소는 디바이스(단말/센서) 영역, 네트워크(유선/무선) 영역, 서비스 인터페이스(플랫폼/애플리케이션) 영역으로 구분될 수 있다. 단, 본 연구에서는 위협이 발생할 수 있는 정보 수집/전달/처리의 구성요소 단을 고려하기 위해, 서비스 인터페이스를 '서버'로 재정의 하였다. 서버는 정보가 디바이스를 통해 생성 및 수집되어 네트워크를 통해 전송되면 최종적으로 서비스를 위해 정보를 가공 처리하고 저장되는 역할을 한다. 위협은 각 구성 요소(디바이스, 네트워크, 서버)에서 발생할 수 있는 유출/침해 위협으로 분류되어 산정될 수 있다. 본 연구에서의 유출/침해 위협 변수는 위협이 발생하는 각 단(Point)에서의 위협 수준의 조합으로 정의하였다. 즉, IoT 환경에서의 디바이스, 네트워크, 서버의 각 영역에서 유출/침해 위협이 측정되며, 그 수준은 해당 위협이 얼마나 치명적인가에 따라 H(높음), M(중간), L(낮음)로 분류할 수 있다. 유출 및 침해 위협 가능성이 높고 그 위협이 치명적인 경우 H로, 위협이 존재하나 그 위협의 여파가 치명적이지 않은 경우

M으로, 위협의 가능성이 거의 없는 수준일 경우 L로 측정토록 한다. 각 수준에 대한 위험 점수로는 H : 3점, M : 2점, L : 1점을 부여하도록 한다.

4.1.3 사회적 영향력(Social Impact)

영향력은 개인정보 유출/침해 사고 발생 시 미치는 사회적 충격의 정도를 의미한다. 본 연구에서는 사회적 영향력을 나타내는 세부 변수로 이용자 수, 이용 빈도, 시장규모, 2차 결합 시장 규모를 반영하였고, 이들의 조합으로 사회적 영향력을 측정하도록 한다.

① 이용자 수와 이용 빈도(Number of Users and Frequency of Use)

IoT 서비스 종류별 이용자 수 규모가 클수록, 해당 서비스의 사용 빈도가 높을수록 발생하는 피해에 대한 영향이 커질 수 있다. 본 연구에서 이용자 수는 사용자 수 규모에 대한 등급(H, M, L)으로 구분하도록 하였다. 참고로, IoT 관련 사용자 수가 가장 많을 것으로 전망되는 스마트폰과 스마트 TV의 가입자 수는 2015년 국내 기준으로 각각 4,367만 명, 1,164만 명 정도이다(MSIP, 2015). 한국은 스마트폰 및 스마트 TV(IPTV) 사용자 수가 세계적으로도 매우 높은 편에 속한다. 한편 Connected Car의 대표적인 서비스인 온스타의 경우, 2015년 기준 이용자 수가 약 770만 명 정도이다(KBResearch, 2016). 또한 새로운 IT 서비스 진입 초기 시 100만 가입자를 목표로 세우고 추진하는 경우가 많다. 이러한 점을 참조하여 이용자 수의 등급을 1,000만 명 이상은 H(높음)로, 1,000만 명에서 100만 명 사이를 M(중간)으로, 100만 명 미만을 L(낮음)로 구분할 수 있다. 각 수준에 대한 점수로는 H : 3점, M : 2점, L : 1점을 부여한다.

이용 빈도는 IoT 서비스에 대한 사용 빈도로 그 수준을 측정하도록 한다. IoT 서비스 사용이 일상생활에 미치는 영향 정도를 반영하기 위해서, 해당 서비스 디바이스를 매일 사용하는 경우와 3일 정도에 한 번 사용, 그 이하로 구분할 수 있다. 따라서 월 30회 이상 사용을 H(높음)로, 월 30회 사용에서 10회 사용 사이를 M(중간)으로, 월 10회 사용 미만을 L(낮음)로 정할 수 있다. 각 수준에 대한 점수로는 H : 3점, M : 2점, L : 1점을 부여한다.

② 시장 규모와 2차 결합시장 규모(Market Size and 2nd Market Size)

서비스 시장 규모는 IoT 서비스 분야별 산업 규모를 화폐 단위로 표시한 것으로 정의한다. IoT 시장 전망 자료에 의하면, 글로벌 IoT 전체 시장 규모가 2013년 2,031억 달러 정도이며, 2022년에는 1조 2,000억 달러규모에 이를 것으로 예측되고 있다(Joo and Kim, 2014; Lee, 2013). 산업연구원(2014)에서 정리한 자료에 의하면, 서비스 영역별 IoT 시장 규모는 2013년 기준 1억 달러에서 5억 달러 규모로 형성되어있다. 한편, 2020년까지 연평균 68%에서 120%까지의 성장률을 보일 것으로 전망되고 있다. 본 연구에서는 서비스별 최근 시장 규모를 참조하여, 연간 시장 규모 5억 달러 이상을 H(높음)로, 5억 달러에서 1억 달러 사이를 M(중간)으로, 1억 달러 미만을 L(낮음)로 구분하도록 하였다. 각 수준에 대한 점수는 H : 3점, M : 2점, L : 1점을 부여한다.

2차 결합 시장 규모는 스마트 커뮤니케이션 디바이스, 커넥티드 카, 스마트 홈, 스마트 헬스케어, 스마트 인프라 분야에서 개인정보 사고가 발생했을 경우에 2차적으로 영향을 받는 시장규모로 정의된다. 이는 피해가 발생한 서비스 시장으로부터 간접적으로 영향을 받는 시장의 규모를 산출하는 것으로 유출된 정보가 2차 피해를 유발할 수 있는 시장으로 한정한다. 이렇게 2차적으로 결합되는 관련 산업까지 사회적 영향 변수에 포함시킨 이유는 IoT 특성 상 다른 산업군과 연계되는 융합 서비스가 다수 존재하기 때문이다. 예를 들어, 커넥티드 카 산업에서 활용하는 이용자의 정보는 자동차 보험 산업에서도 활용될 수 있다.

본 연구에서는 피해가 발생한 서비스 시장으로부터 유출된 정보가 2차 피해를 유발할 수 있는

시장 규모의 크기에 따라 변수의 수준을 구분하였다. 수준의 척도는 산업군별 시장 규모가 수천억 달러에서 수억 달러 사이라는 것을 감안하여(Joo and Kim, 2014), 시장 규모 1,000억 달러 이상을 H(높음)로, 1,000억 달러에서 100억 달러 사이를 M(중간)으로, 100억 달러 미만을 L(낮음)로 구분하였다. 각 수준에 대한 점수로는 H : 3점, M : 2점, L : 1점을 부여하도록 한다.

5. 신규 프레임워크를 활용한 IoT 위험 분석 결과

5.1 분석 대상 및 분석 과정

제 4장에서 제안한 신규 프레임워크의 활용 가능성을 검증하고자, 제시된 프레임워크를 기반으로 IoT 서비스 분야(커넥티드 카, 스마트 홈, 스마트 헬스케어, 스마트 인프라, 스마트 커뮤니케이션 디바이스)별 개인정보보호 측면의 위험도 분석을 실시하였다. 본 연구에서는 IoT 환경에서의 개인정보 위험 분석을 위한 대상으로, 기존의 IoT 관련 개인정보 유출 사례와 프라이버시 침해 사고 및 시연 사례를 대상으로 하였다. 커넥티드 카의 경우 개인정보 관련하여 5건의 이슈화된 사례(OnStar, Sync AppLink, MyFord Mobile, OpenXC, U-connect touch)가 파악되어 이들 사례를 대상으로 위험 분석을 실시하였다. 스마트 홈도 5건의 사례(ThinQ, Allshare 1, Allshare 2, Haier u-Home, Kenmore)가 파악되어 이를 대상으로 분석하였다. 스마트 헬스케어의 경우는 6건의 사례(Fuelband Series, Micoach Smart run, Walkie+D, Iriver-On, Health-On-Shine, Jawbone up)가 파악되어 이에 대해 위험 분석을 실시하였다. 스마트 인프라(빌딩/시티/그리드)의 경우는 크게 이슈화된 사례를 아직 발견하지 못하여 4개의 시나리오를 연구자들의 협의를 통해 설정하여 이에 대한 위험을 분석하였다. 스마트 커뮤니케이션 디바이스의 경우는 3개의 사례(Smart phone, Google Glass, Smart Watch)를 분석하였다.

서비스 분야별 위에서 언급한 대상 사례에 대해서 우선 변수별 위험 정도를 측정하였다. 개인정보에 대해서는 해당 서비스 또는 디바이스가 보유하고 있는 개인정보의 종류, 개인정보의 민감도를 분석하였다. 해당 서비스 유형에 속하는 개별사례를 조사한 후 각 변수별 수준에 대해서 전문가 그룹(저자 포함 총 10명의 ICT/정보보호 분야 전공 석박사 및 교수 참여)의 평가를 통해 H(3)/M(2)/L(1)로 점수화 하였다. 각 사례에 대해 점수를 매긴 후, 다수 사례를 종합한 해당 서비스의 대푯값을 설정하기 위해서, 해당 서비스에 속하는 사례 평가로 가장 많이 나온 최빈값을 대푯값으로 선정하여 해당 서비스 분야의 위험도로 나타내었다. 예를 들어, 스마트 홈의 5가지 사례분석 후 개인정보 민감도에 대한 평가가 L, H, H, H, L로 나온 경우, 최빈값인 H를 스마트 홈서비스 분야의 개인정보 민감도 대푯값으로 설정하였다. 단, 본 연구에서는 최빈값을 대푯값으로 설정하였지만, 상황에 따라서 최고값으로 대푯값을 설정할 수도 있다. 즉, 해당분야에 대한 기존의 위험관리 수준이 높았거나 사회적으로 해당 분야에 대한 보호 요구가 높을 경우(예 : 안전 등과 관련)는 최빈값이 아닌 최고값을 대푯값으로 설정함으로써 한번이라도 높게 발생한 위험 사례가 존재한다면 이 서비스 분야에 대한 위험 경계 수준을 엄격히 높게 관리하도록 할 수 있다.

위협 변수에 대해서는 사건 또는 해킹 시연 시 보고서 및 보도 자료 등을 분석하여 문제가 된 디바이스, 네트워크, 서버에서의 침해 위협이 어느 정도인가를 파악한 후, 이에 대해서도 상기와 마찬가지로 전문가 그룹의 평가를 통해 H(3)/M(2)/L(1)로 점수화하고 최빈값을 해당 서비스의 대푯값으로 설정하였다.

마지막으로 사회적 영향력은 개별 사례별로 측정하는 것은 적절하지 않다고 판단되어 해당 서비스 유형 전체의 영향력 변수의 값들을 산정하였다. 사회적 영향력 분석을 위해 서비스 유형별 시장

조사 및 전망 자료들을 종합적으로 분석한 후 전문가 그룹의 평가를 통하여 점수화 하였다.

각 변수에 대해 점수를 구한 후, <Table 1>의 수식을 통해 해당 IoT 서비스에 대한 총 위험정도를 계산하였다. 본 연구에서는 위험정도 산정의 편의를 위해 모든 계수를 '1'로 설정하고 계산하였다. 단, 계수 값은 특정 변수의 위험도에 대한 가중치(Weight)를 설정할 때 활용할 수 있으므로, 추후 1이외의 값으로 변경하여 사용할 수도 있다.

상기의 과정을 통해 분석된 서비스 유형 및 사례별 상세 분석 내용은 <Appendix 1>에 제시되어 있다.

5.2 위험 분석 결과

제 5.1절의 과정을 통해 IoT 서비스 유형별 위험을 분석한 결과, 커넥티드 카의 경우 높은 수준(H)의 식별가능한 개인정보를 많이 수집하고 있었으며, 생성 및 이용 가능한 개인정보의 민감도는 중간 정도(M)로 나타났다. 또한 침해 위협의 경우 디바이스와 네트워크에서만 위협 사례가 나타난 것으로 분석되었다(즉, 서버의 위협 정도는 L임). 디바이스의 침해 위협은, 서비스 해지 후 데이터 폐기 관리 조치를 제대로 안할 경우 해지 후에도 차량 내 단말로부터의 개인정보 유출 가능성이 존재하고 안드로이드의 오픈 OS 특징으로 인해 중간 정도(M)로 측정되었고, 네트워크 침해 위협은 암호화 기술의 부족 등의 이유로 높음(H)으로 측정되었다. 사회적 영향도의 경우 이용 빈도와 서비스 시장 규모는 높은 것(H)으로 나타났지만 사용자 수는 중간 정도(M)이고 아직까지 다른 시장과의 결합 정도는 낮은 것(L)으로 나타났다.

스마트 홈의 경우 가전 디바이스가 보유하고 있는 식별가능한 개인정보의 종류는 적은 것(L)으로 나타났으나, 집안에서의 사생활 정보 및 결제 등을 위한 정보를 가지고 있어 민감도는 높은 것(H)으로 나타났다. 침해 위협의 경우는 아직까지의 사례에서는 네트워크 단에서만 문제가 있는 것으로 나타났으며, 통신과 관련된 위협 수준은 중간 정도(M)의 침해 위협으로 산정되었다. 사회적 영향도의 경우 이용자수와 이용 빈도가 높은 것(H)으로 나타났다. 반면 서비스 시장 규모와 2차 결합 시장의 규모는 중간 정도(M)인 것으로 나타났다.

스마트 헬스케어의 경우 수집하는 개인정보의 종류와 개인정보의 민감도 수준이 중간 정도(M)인 것으로 나타났다. 헬스케어는 개인의 신체활동 및 건강과 관련된 정보를 가지고 있어 민감도가 높아 보일 수 있으나, 유출되었을 때 사회생활에 지장을 주거나 경제적 타격을 주는 민감한 의료 정보는 사례에서 크게 나타나지 않아 중간 정도(M)로 평가되었다. 침해 위협의 경우 디바이스에서만 침해 사례 또는 해킹 시연이 있었던 것으로 나타났으며 침해 위협은 중간 정도(M)의 수준으로 산정되었다. 사회적 영향도의 경우 이용자 수와 이용 빈도는 높은 것(H)으로 나타났다. 반면 서비스 시장 규모는 아직까지 작은 것(L)으로 나타났다. 단, 2차적인 결합 시장 규모 측면에서는 다른 서비스 분야의 다양한 디바이스와 연계되고 보호관찰/원격제어 시장 등과도 결합되어 중간 정도(M)로 평가되었다.

스마트 인프라(빌딩/시티/그리드)의 경우는 식별가능한 개인정보 종류 수준은 낮은 것(L)으로 분석되었고 민감도는 과금과 관련된 결제 정보 등이 포함되어 있어서 다소 높게(H) 나타났다. 또한 침해/유출 시나리오 기반으로 평가를 했을 때 네트워크 단과 인프라 관제 서버의 위협이 중간(M) 정도로 나타났다. 사회적 영향도의 경우, 아직까지 사용자 수와 서비스 시장 규모는 중간 정도(M)이고, 생활에서의 사용빈도와 2차 결합 시장 규모는 높은 것(H)으로 나타났다.

스마트 커뮤니케이션 디바이스의 경우, 수집되는 정보에서 식별가능한 개인정보 종류가 많고(H), 민감도 측면에서는 개인의 위치정보와 커뮤니케이션 주요 대상, 개인의 선호 정보 등을 다양하게 포함할 수 있어 개인정보 민감도가 높은 것(H)으로 나타났다. 디바이스 침해 위협의 경우, 특히 안드로이드와 같은 오픈 OS 사용 디바이스의 악성 코드 위

협 가능성 및 시연 사례가 있으나 아직까지 치명적인 위협 수준의 사례는 발생하지 않아 중간정도(M)로 분석되었다. 네트워크 단에서는 전송단 해킹의 이슈가 제기되어 중간 정도(M)의 위협 수준으로 분석되었다. 서버 단 위협은 우려와 달리 아직까지 사례가 나타나지 않았다(L). 사회적 영향도의 경우는 IoT 서비스 분야 중 가장 활성화된 서비스로 이용자수, 이용 빈도, 시장 규모, 2차 결합 시장 규모 모두에서 높은 수준(H)으로 평가되었다.

최종적으로 정리된 서비스 분야별 IoT 개인정보 위험 분석 결과는 <Table 3>에 제시되어 있다. 종합적인 분석 결과를 살펴보면, 스마트 커뮤니케이션 디바이스가 총점 27점 중에 23점으로 IoT 환경에서 개인정보 사고 발생 시 위험이 가장 높은 분야로 나타났다. 다음으로는 커넥티드 카(20점), 스마트 홈(18점)과 스마트 인프라(18점), 스마트 헬스케어(17점) 순으로 나타났다. 본 분석 결과에 의하면, 스마트 커뮤니케이션 디바이스는 식별가능한 개인정보 종류와 민감도 수준이 매우 높고, 현재 IoT 서비스로서 가장 활성화되어 있어서 개인정보 관련사고 발생 시 가장 큰 문제를 야기할 것으로 보인다. 커넥티드 카의 경우 이용자 수는 아직까지는 적으나 자동차가 생활에 밀착되어 있고, 자동차 시장 매출 규모가 크기에 개인정보 사고 발생 시 위험도가 높게 평가된다. 또한 차량 내 IoT 디바이스가 단순 더미가 아닌 프로세스와 메모리를 가지고 있는 소형 컴퓨터이므로 자동차에서 보유하고 있는 개인정보 종류가 많은 것이 높은 위험도의 원인이 될 수 있다. 스마트 홈의 경우 스마트 TV의 결제 정보, 시청/조회 이력, 스마트 청소기의 음성, 영상 등 민감 정보가 많은 것과 스마트 TV의 이용자 수와 이용 빈도가 높은 것이 개인정보 사고 발생 시 위험이 커지는 원인이 될 수 있다. 스마트 인프라(빌딩/시티/그리드)의 경우는 개인정보 유출 사건과 관련한 기존 사례를 발견하지 못하여 시나리오 기반으로 위험 평가를 했기 때문에, 추후 실사례가 대입되었을 때 다소 다른 결과가 나올 수 있는 가능성도 존재한다. 인프라성 서비스들은 특히 서버나 네트워크 위협에 의한 위험도가 높기 때문에 이를 유의해야 하며, 앞으로 스마트 인프라 서비스가 다양하게 적용되면 수집되는 개인정보의 종류도 더 많아져 이로 인한 위험 상승도 가능할 수 있다. 끝으로, 스마트 헬스케어는 개인의 신체 활동에 관한 정보를 생성함에도 불구하고 다른 분야에 비해 상대적으로 위험도 점수가 낮게 나타났다. 이는 헬스케어 서비스 시장이 본격적으로 성숙하지 않은 것이 주원인으로 보이며, 앞으로 스마트 헬스케어 시장이 다양한 서비스와 융합되어 더욱 활성화되면 개인정보 사고 발생 시 위험이 지금보다는 더 높게 발생할 가능성이 있다.

〈Table 3〉 Results of IoT Risk Analysis using Proposed New Framework

	Personal Information		Threat			Impact				Iot Risk Score
	Type	Sensitivity	Device	Network	Server	#of Users	Freq. of use	Market Size	2nd Market Size	
Connected Car	H(3)	M(2)	M(2)	H(3)	L(1)	M(2)	H(3)	H(3)	L(1)	20
Smart Home	L(1)	H(3)	L(1)	M(2)	L(1)	H(3)	H(3)	M(2)	M(2)	18
Smart Healthcare	M(2)	M(2)	M(2)	L(1)	L(1)	H(3)	H(3)	L(1)	M(2)	17
Smart Infra	L(1)	M(2)	L(1)	M(2)	M(2)	M(2)	H(3)	M(2)	H(3)	18
Smart Comm.	H(3)	H(3)	M(2)	M(2)	L(1)	H(3)	H(3)	H(3)	H(3)	23

6. 결 론

본 연구에서는 IoT 환경에서 개인정보보호를 위한 위험 분석 프레임워크를 새롭게 제안하고, 제시한 프레임워크를 적용하여 IoT 서비스 분야별 위험을 분석하였다. 본 연구 결과, 비즈니스 영역별로 위험 요인에 대한 위험 정도가 다르게 나타났다. 예를 들어 식별가능한 개인정보 종류 측면에서는 커넥티드 카와 스마트 커뮤니케이션 디바이스가 위험도가 높았지만, 개인정보의 민감도 측면에서는 커넥티드 카 보다 스마트 홈이 더 높게 나타났다. 또한 침해 위협도의 경우 디바이스에 대한 위협이 높은 서비스 유형과 네트워크에 대한 위협이 높은 서비스 유형이 다르게 나타났다. 따라서 본 연구 결과를 참조하여, 비즈니스 유형별로 높은 위험 요소에 대한 개인정보보호 대처 방안을 검토해 볼 수 있다.

특히 본 연구 결과에 의하면, 스마트 커뮤니케이션 디바이스와 커넥티드 카가 상대적으로 높은 위험이 있는 것으로 분석되었다. 따라서 앞으로의 IoT 환경에서는 이 두 영역에 대한 위험 대책 방안을 우선적으로 검토할 필요가 있다.

커넥티드 카의 경우, 국내에서는 아직 본격적으로 활성화가 되지 않았지만 현대사회에서 자동차는 거의 생활의 필수품이 되고 있기 때문에, 이 서비스의 확산에 걸리는 시간은 그리 길지 않을 것으로 보인다. 가트너에 따르면 2020년경에는 대부분의 승용차와 트럭이 인터넷에 연결될 것이며, 약 1억 5,000만 대의 인터넷 연결 자동차 중 60~70%가 웹 기반 데이터를 소비, 생성, 공유할 것으로 전망되고 있다(CIOKorea, 2014). 자동차는 그 특성상 개인정보 유출 사건 발생 시 자칫하면 운전자의 안전 및 생명과 직결되는 위험이 발생할 수 있기 때문에 이에 대한 대책 마련이 더욱 필요하다.

한편, 스마트 커뮤니케이션 디바이스에는 스마트폰, 해드마운티드디스플레이(HMD) 장착 스마트 글래스 및 VR기기, 휴대형 스마트 와치 등 다양한 형태가 있고 다른 서비스 영역과 연계될 소지가 많다. 특히 스마트폰에서 생성 및 이용 가능한 개인정보에는 전화번호, 위치정보, 일정정보, 개인 및 가족/지인들의 사진, 동영상, 음성, 신용카드 및 계좌 번호, 앱 사용 정보 및 검색 기록, 활동 로그, WiFi/블루투스/NFC 통신 중 생성되는 정보 등 다양하고 민감한 개인정보들이 포함되어 있다. 따라서 해당 분야에 대한 개인정보 유출 및 침해 사고 발생 시 그 파급력이 매우 클 수 있어, 위험 관리 방안이 필요하다.

본 연구 결과를 토대로, 커넥티드 카 및 스마트 커뮤니케이션 디바이스를 포함한 IoT 서비스에 대한 개인정보 위험 대책 방안을 다음과 같이 모색해 볼 수 있다.

첫째, IoT에서 수집 및 이용가능한 개인정보보호 측면에서, IoT 서비스 시 개인정보 수집의 최소화와 정보 주체에게 수집에 대한 충분한 고지 및 동의 획득이 더욱 필요하다. 실제 커넥티드 카 서비스인 온스타의 경우, 월별 서비스 해지 후에도 고객의 위치정보 등이 계속 수집될 수 있는 약관으로 인해 개인정보 무단 수집 이슈가 제기된 바 있다(Lewis, 2011). 또한 개인의 운전습관 정보가 보험사 등에 전달됨으로 인한 프라이버시 침해 논란이 있었다(Kane, 2011). 따라서 개인정보 관련 이러한 문제점의 개선이 필요하다. 개선방안으로는 예를 들어, 정보주체(사용자)가 원하는 커넥티드 카 서비스에 해당하는 개인정보만을 수집하고 그 기간을 약관에 명시하도록 한다. 이때 커넥티드 카가 제공해주는 서비스 기능별로 수집되는 개인정보의 내용과 함께 그에 따른 위험성을 알려주도록 함으로써, 정보주체가 이를 인식하고 원하는 서비스 기능에 대해서만 개인정보의 수집 동의를 선택할 수 있도록 한다. 단, 실효성이 떨어지는 지나친 동의 절차는 오히려 IoT 서비스 발전을 저해할 수 있으므로, IoT 환경에 적합한 고지 방법과 동의 프로세스 개발이 고려되어야 할 것이다.

둘째, IoT에서의 개인정보 유출/침해 위협과 사회적 영향 측면에서, IoT 관련 서비스를 초기 기획하고 개발하는 단계에서부터 프라이버시를 고려하도록 하고, IoT 서비스에 대한 개인정보/프라이버시 영향 평가 적용 및 평가 항목 구체화가 검토되도록 한다. 예를 들어 IoT 프라이버시 영향 평가에는 IoT 데이터 수집/전송/처리 시 개인정보 유

출 가능 경로(단말/네트워크/서버)별 체크, IoT 서비스의 개인 패턴분석 남용으로 인한 프라이버시 침해 위협 체크, IoT 서비스에서의 개인 식별 가능성 체크 등이 검토될 수 있을 것이다. 커넥티드 카 서비스의 경우 해커 및 보안 기업 등으로부터 정보 유출 및 침입의 취약성이 여러 차례 보고되었기에(Glen, 2015), 이러한 영향 평가 적용이 더욱 필요하다. 또한 대표적인 스마트 커뮤니케이션 기기인 스마트폰은 운영체제(OS) 레벨과 앱(App) 레벨에서의 다양한 개인정보 위협들이 존재한다. 특히 스마트폰은 IoT 관련 신규 앱들이 지속적으로 출시될 수 있으므로, 스마트폰과 연계된 각종 IoT 앱 서비스에 대한 프라이버시 영향 평가가 이뤄질 수 있도록 검토해야 할 것이다.

끝으로, IoT 사용자의 자기정보통제권을 존중하고 강화할 필요가 있다. IoT 환경에서는 부지불식 중 개인정보가 수집될 수 있고, 서비스의 편재성으로 인해 정보 주체의 자기통제권이 약화될 수 있다. 그러므로 앞에서 언급한 첫째~둘째 개인정보보호 방안을 아우를 수 있는 규약을 제정하고 IoT 환경에서 개인정보 통제권을 사용자들에게 알리며 권리 행사를 보장할 수 있도록 해야 할 것이다. 이를 위해 변화하는 IoT 시대에 사용자 스스로가 프라이버시 보호에 대한 인식을 고취할 수 있도록 효과적인 교육과 홍보가 제공되어야 할 것이다.

본 연구에서는 IoT의 활용 분야를 5가지 유형으로 분리하였고, 새롭게 제시한 프레임워크를 적용하여 이들 유형별 개인정보에 대한 위험 분석을 실시하였다. 본 연구의 분석 대상(샘플)은 해당 서비스 분야에서 현재까지 도출된 개인정보 관련 유출/침해/해킹 사례들이었다. 이러한 실 사례 분석을 통해 실제적인 위험도를 측정하고자 하였고, 해당 IoT 분야에 대한 각종 조사 자료들을 참조하여 각 위험 요인에 대한 평가를 가능한 객관적으로 분석하고자 노력하였다. 단, 분석한 사례가 제한적이었고, 요소별 위험 평가 시 전문가 그룹 참여자들의 주관적인 판단이 개입될 소지가 있다. 따라서 본 연구의 분석 결과는 앞으로의 정책 마련을 위한 참고 자료로 활용하는 것이 적절해 보인다. 또한, 본 연구에서 제시한 IoT 위험 분석 프레임워크는 앞으로도 지속적인 테스트를 통해 발전해 나가고, 이론적으로 보완되어야 할 것이다. 예를 들어, 사회적 위험 영향력을 측정하는 세부 요인을 추가/변경할 수 있고, 변수별 측정 수준을 현재의 3단계에서 5단계로 확장할 수도 있다. 서비스별 대푯값을 설정하는 방식도 최빈값 이외에 평균값, 최고값 등으로 변경하여 고려할 수 있고, 항목별 평가 방식에 향후 AHP 기법 등을 적용해 볼 수도 있을 것이다.

IoT 환경에서는 발생가능한 개인정보 위험들이 다양하게 존재한다. 앞으로 IoT의 확대에 따라 개인정보보호법 보완 및 대책 방안에 대한 논의가 활발하게 전개될 것으로 예상된다. 본 연구에서 검토된 내용은 향후 개인정보보호를 위한 개선 방안과 위험 관리 체계 마련에 참조가 될 수 있을 것이다.

References

Arthur, D.L., “Wanted : Smart Market-Makers for the Internet of Things”, *Prism*, Vol.2, 2011.

Caragliu, A., C. DelBo, and P. Nijkamp, “Smart Cities in Europe”, *Journal of Urban Technology*, Vol.18, No.2, 2011, 65-82.

Choi, H.S. and Y.H. Cho, “Security Vulnerability of Internet of Things and Its Solution”, *Journal of the Korea Society of Digital Industry and Information Management*, Vol. 11, No.1, 2015, 69-78.

(최희식, 조양현, “사물인터넷 보안 문제제기와 대안”, *디지털산업정보학회논문지*, 제11권, 제1호, 2015, 69-78.)

Choi, K.J., “A Study for Developmental Change of Personal Information Protection Law System in the Age of Big Data and Internet of Things (IoT)”, *Chung_Ang Law Review*, Vol.17, No.4, 2015, 7-50.

(최경진, “빅데이터 · 사물인터넷 시대 개인정보보호

법제의 발전적 전환을 위한 연구", *중앙법학*, 제17권, 제4호, 2015, 7-50.)

CIOKorea, "0.15 Billion Connected Cars in 2020", *CIOKorea*, 2014.

EU, "Opinion 8/2014 on the on Recent Developments on the Internet of Things", EU Article 29 Data Protection Working Party, 2014.

Gartner, "Market Trends : TSPs Must Invest in the Rapidly Evolving IoT Ecosystems Now", Gartner, 2013.

Gartner, "6.4 Billion Connected Things Will Be in Use in 2016, Up 30 Percent From 2015", Gartner Symposium/ITxpo 2015, Barcelona, Spain, 2015.

Glen, W., "OnStar Plugs Hacker Attacks", Autonet. 2015.

Infosec, "Risk Analysis Methodology and Security Consulting Trends", Infosec, 2008.

(인포섹(주), "위험분석 기법과 보안컨설팅 동향", 인포섹, 2008.)

ISACA, "Risk IT Framework for Management of IT Related Business Risks", ISACA, 2009a.

ISACA, "The Risk IT Framework", ISACA, 2009b.

ISO/IEC, "Information Technology-Security Techniques-Information Security risk Management", ISO/IEC FIDIS 27005:2008, 2011.

Jeon, C.M., "Evolving Direction of the Connected Car Service", KT Economic and Management Research Center, DIGIECO ISSUE & TREND, 2013.

(전춘미, "커넥티드 카 서비스의 진화방향", KT경제경영연구소, DIGIECO ISSUE and TREND, 2013.)

Joo, D.Y. and J.G. Kim, "IoT's Activation Plan for Creative Convergence in Hyper-Connected Society", *KIET(Korea Institute for Industrial Economics & Trade), ISSUE Paper*, Vol.342, 2014.

(주대영, 김종기, "초연결시대 사물인터넷 (IoT)의 창조적 융합활성화 방안", *산업연구원, ISSUE Paper,* 제342권, 2014.)

Kane, S., "Pay-As-You-Drive Car Insurance : Big Savings, No Privacy?", The Car Connection, 2011.

Kang, N.H., "IoT Convergence Service Security Requirement", *The Journal of The Korean Institute of Communication Sciences(Information and Communications Magazine)*, Vol.32, No.12, 2015, 45-50.

(강남희, "사물인터넷 융합 서비스 보안 요구사항", *한국통신학회지(정보와 통신)*, 제32권, 제12호, 2015, 45-50.)

KATS(Korean Agency for Technology and Standards), "[KS X ISOIEC27005] Information technology-Security Techniques-Information Security Risk Management", KATS, 2014.

(국가기술표준원, "[KS X ISOIEC27005] 정보기술-보안기술-정보보호 위험관리", KATS, 2014.)

KB Reseach, "Development Trends and Future Changes in Connected Car", KB Knowledge Vitamin, Vol.15, 2016.

(KB금융지주경영연구소, "Connected Car 개발 동향과 미래 변화", KB지식비타민, 제15권, 2016.)

KCA(Korea Communication Agency), "Business Trends of Major Operators in Connected Car and Prior Task for Service Dissemination", KCA, 2013.

(한국방송통신전파진흥원, "커넥티드 카의 주요 사업자 동향과 서비스 보급의 선결과제", KCA, 2013.)

KISA(Korea Internet Security Agency), "2014 National Information Security White Paper", KISA, 2014.

(한국인터넷진흥원, "2014 국가정보보호백서", KISA,

2014.)

KISDI(Korea Information Society Development Institute), "Research on Development Direction of Smart Devices Manufacturing Industry", KISDI, 2013.

(정보통신정책연구원, "스마트 디바이스 제조 산업의 발전방향 연구", KISDI, 2013.)

Korea COP Forum, "Personal Information Protection Governance ABC", Korea COP Forum, 2008.

(한국CPO포럼, "개인정보보호 거버넌스의 ABC", 한국COP포럼, 2008.)

Krisher, T., *Auto Industry Steps up Fight Against Hackers,* The Associated Press, 2013.

KSGI(Korea Smart Grid Institute) and KOTRA, "Research on Smart Grid Policy and Market in Major Countries", KSGI & KOTRA, 2010.

(한국스마트그리드사업단, 대한무역투자진흥공사, "주요국 Smart Grid 정책/시장 조사", KSGI & KOTRA, 2010.)

Lee, Y.H., "IoT Based Promising Market Prospect and Agenda to Realize the Creative Economy", NIA(National Information Society Agency), 2013.

(이윤희, "창조경제 실현을 위한 사물인터넷 기반 유망 시장 전망 및 과제", 한국정보화진흥원, 2013.)

Lewis, T., "OnStar Doesn't Give Up Easily… Sometimes", Consumer Affairs, 2011.

MSIP(Ministry of Science, ICT and Future Planning), "Statistics of IPTV Subscribers", ITSTAT, 2015.

(미래창조과학부, IPTV 가입자 수 통계, ITSTAT, 2015.)

MSIP(Ministry of Science, ICT and Future Planning), "Statistics of Smartphone Subscribers", ITSTAT, 2015.

(미래창조과학부, "스마트폰 가입자 수 통계", ITSTAT, 2015.)

Naughton, K. and O. Kharif, "Cars a Target for Identity Thieves as Shopping Comes to Dashboard", Bloomberg News, 2015.

NIST(National Institute of Standards and Technology), "Risk Management Guide for Information Technology Systems", NIST, 2002.

Park, N.J. and G.J. Ahn, "Privacy Protection in Smart Grid", *Review oF Korea Institute of Information Security and Cryptology*, Vol.20, No.3, 2010, 62-78.

(박남제, 안길준, "스마트 그리드에서의 프라이버시 보호", *정보보호학회지*, 제20권, 제3호, 2010, 62-78.)

Shin, Y.J., "A Study on Policy Tasks of Personal Information Protection in IoT Era", *In Proceeding Paper of Korea Association for Public Administration(KAPA) Annual International Conference*, 2015, 692-710.

(신영진, "IoT시대에서의 개인정보보호정책과제에 관한 연구", *한국행정학회 학술발표논문집*, 2015, 692-710.)

TTA(Telecommunication Technology Association), "Risk Analysis and Management Standards for Public Information Systems Security-Risk Analysis Methodology Model", TTAS.KO-12.0007, 2000.

(한국정보통신기술협회, "공공정보시스템 보안을 위한 위험분석 표준-험분석 방법론 모델", TTAS.KO-12.0007, 2000.)

TTA, "Risk Analysis Methodology for IT Services", TTA, 2008.

(한국정보통신기술협회, "IT서비스 위험분석 방법", TTA, 2008.)

TTA, "Standardization related to Smart Buildings", TTA, 2011.

(한국정보통신기술협회, "스마트 빌딩 구축 관련 표준화", TTA, 2011.)

〈Appendix 1〉 Detailed Risk Analysis using Proposed Framework

	Cases	Personal Information		Threat			Impact			
		Type	Sensi-tivity	D	N	S	# of Users	Freq.	M. Size	2nd M. Size
Connected Car	[OnStar] • Even after termination of service, vehicle location/ moving/payment information can be collected • Hacking into Infortainment service through weak point of control center network • Theft of Telematics device on car • Weakness in Androids	H	M	M	H	L	M	H	H	L
	[Sync AppLink] • Collectable data : personal call history, information about listened music of a user • Weakness in Bluetooth • Malicious code infection through connection to smartphone/MP3 using USB	H	M	M	H	L				
	[MyFord Mobile] • Collectable data : battery life, mileage, driving hours, search information • Possible leakage of information regarding automotive performance and search list when smartphone is stolen	L	L	L	L	L				
	[OpenXC] • Collectable data : information of vehicle breakdown or repair • Infringement of data from sensor module based on Arudion	L	L	M	L	L				
	[U-connect touch] • Collectable data : personal voice recognition • Weakness in WiFi and Hotspot	H	M	L	H	L				
Smart Home	[ThinQ : Smart Refrigerator] • Collectable data : information about food and intake • Weakness in Wifi and ZigBee	L	L	L	M	L	H	H	M	M
	[Allshare : Smart TV] • Collectable data: family's photos and video • Weakness in Wireless Communication based on DLNA(Digital Living Network Alliance)	H	H	L	M	L				
	[Allshare : Smart TV] • Collectable data : text message on TV, browsing history of Google/Twitter/News, CCTV • Theft of TV and Computer/Cell Phone (which were connected to Smart TV)	M	H	L	L	L				
	[Haier u-Home] • Collectable data : information about Internet browsing, contents usage(education, weather, video, etc), remote service, monitoring • Weakness in Central Communication System	L	H	L	M	L				
	[Kenmore : Home Appliances] • Collectable data : Information about home repair • Weakness in Wifi and Wireless Communication	L	L	L	M	L				

	Cases	Personal Information		Threat			Impact			
		Type	Sensi-tivity	D	N	S	# of Users	Freq.	M. Size	2nd M. Size
Smart Healthcare	[Fuelband Series] • Collectable data : steps, moving distance, amount and history of exercise, goals, weight, height, calorie, comparison of exercise with other users • Information leakage from Nike+ application on device	M	M	M	L	L	H	H	L	M
	[Micoach Smart run] • Collectable data : moving distance, route, GPS, G-meter, physical condition, change in weather, training data • Weakness in Wifi and Bluetooth	M	M	L	M	L				
	[Walkie+D] • Collectable data : steps, moving distance, speed, calorie burned, amount of daily activity • Issue in security of personal information on device	M	M	M	L	L				
	[iriver On] • Collectable data : heart beat, speed, calorie burned, status of change of smartphone • Issue in security of personal information on device	M	L	M	L	L				
	[Health-On-Shine] • Collectable data : amount of exercise a day, exercise pattern, calorie burned • theft of magnetic clip device	L	L	L	L	L				
	[Jawbone up] • Collectable data : sleep condition, time to sleep • Issue in security of personal information on device	L	L	M	L	L				
Smart Infra	[Smart Grid/Building] • Breach/Forgery/Falsification of remote control information by attacks on weakness in password/authentication of control gateway, when offering monitoring Information through external IP or mobile network - Collectable data: personal electricity consumption - Weakness in authentication system of control gateway server and network management	L	M	L	M	M	M	H	M	H
	[Smart Grid/Building] • Forgery/Falsification of information about electricity consumption by sniffing and MITM(man in the middle attack) on communication protocols such as PLC, ZigBee, Wifi, SUN, etc. - Collectable data : personal electricity consumption - Possibility of damage : breach of certification key and personal information, manipulation of charging information in servers, DDoS attack	L	M	L	M	M				
	[Smart Grid] • Breach of personal information and Infringement of privacy through weakness in communication network between smart grid devices such as smart meter and smart phone - Collectable data : user's basic personal information, electricity consumption and charge information - Possibility of material damage	H	H	L	M	L				
	[Smart City/Grid/Building] • Large-scale blackout by attacks on core power system such as SCADA(Supervisory Control And Data Acquisition), DAS(Distribution Automation System) servers - Collectable data : not related to a person - Possible attack on smart infra servers and network, thereby leading to the paralysis of SCADA facility	L	L	L	M	H				

	Cases	Personal Information		Threat			Impact			
		Type	Sensi-tivity	D	N	S	# of Users	Freq.	M. Size	2nd M. Size
Smart Communi-cation Device	[Smartphone] • Collectable data : device-related information, usage information on device, financial Information, location Information • Phishing and pharming through text message and Internet service on device • Theft and loss of device	H	H	M	M	L	H	H	H	H
	[Google Glass : Smart Class] • Collectable data : device-related information, usage information, photos, videos, voices, location Information • Abuse it as hidden camera • Theft and loss of device • Possible MITM(man in the middle attack) : Possible hacking into network traffic of user wearing Google class • Possible hacking into root permission on device	H	H	M	M	L				
	[Smart Watch] • Collectable data : location, message, health information • Theft and loss of device • Abuse it as hidden camera • Weakness in device security : issue in possibility of malicious code infection	H	M	M	M	L				

◈ About the Authors ◈

Ae Ri Lee (arlee12@naver.com)

Dr. Ae Ri Lee is currently a research professor of Barun ICT Research Center at Yonsei University, Korea. She was an assistant professor at Yuhan University, Korea and worked at Korea Telecom as a senior manager of business planning and R&D division. She received her Ph.D. in Information Systems from Yonsei University, Korea and her MBA in Technology Management from KAIST(Korea Advanced Institute of Science and Technology). Her special research interests include the areas of virtual community, social media, information security and privacy, knowledge management, and value co-creation.

Beomsoo Kim (beomsoo@yonsei.ac.kr)

Prof. Beomsoo Kim is a professor at the Graduate School of Information, Yonsei University, Korea. He is a director of Barun ICT Research Center and a vice president of OECD SPDE(Security and Privacy in the Digital Economy). He has a Ph.D. in Management Information Systems from the University of Texas at Austin. He worked as an assistant professor at the University of Illinois at Chicago. His research interests include privacy laws and policies, information security and privacy best p ractices, security and privacy management in cloud computing services, corporate security and privacy policy, knowledge management, and economic issues in IT industry.

Jaeyoung Jang (jyjang31@gmail.com)

Jaeyoung Jang is a Ph.D student at Yonsei University, Korea and a general researcher at Korea Information & Security Agency. He received his M.A. in communications Policy and Regulation from the University of Westminster, the U.K. His current research interests include the areas of information security (including Hackers' behavior), privacy laws and policies, Spam and Anti-Spam Response.