

# IoT기반 소비자제품 안전강화를 위한 법제 개선방안 연구

황의관 · 지광석



한국소비자원  
Korea Consumer Agency

# IoT기반 소비자제품 안전강화를 위한 법제 개선방안 연구

황의관 · 지광석



## 머 리 말

4차 산업혁명을 이끌고 있는 기술 중 하나인 사물인터넷(IoT)을 활용한 IoT기반 소비자제품 시장이 지속적으로 성장하고 있으며, 우리나라는 이 분야를 선도하고 있습니다. IoT기반 소비자제품은 소비자에게 편리성과 제품의 효용성 제고란 이점을 제공하는 동시에 소비자안전에 대한 잠재적 위험성 문제도 내포하고 있습니다.

미국의 소비자제품안전위원회(CPSC)는 2018년 5월 IoT기반 소비자제품의 위해요인에 관한 공개청문회를 개최하여 이해관계자들의 다양한 의견을 수렴하였고, 2019년 1월에는 케이(Kaye)위원 명의의 'IoT 안전성 기준에 대한 의견서'를 공표하였습니다. 경제개발협력기구(OECD)도 여러 보고서를 통해 IoT기반 소비자제품의 안전성 문제를 논의해 왔고, 최근 동 기구 내 소비자정책위원회(CCP) 산하 제품안전작업반(WPCPS)에서 IoT기반 소비자제품의 안전문제를 다루고 있습니다.

본 연구는 이러한 IoT기반 소비자제품의 안전문제에 대한 국제적 논의를 살펴보고, 이를 통해 소비자안전 강화를 위한 법·정책적인 개선방안을 제안하고자 하였습니다. 이를 위해 IoT기반 소비자제품의 개념, 특성 및 관련 시장 현황을 조사하고, IoT기반 소비자제품안전 관련 국내법제와 위해요인에 관한 국제적 논의동향을 조사·분석하였습니다.

특히 IoT가 가지는 정보통신망과의 연결성이란 특성을 반영하여 정보통신망의 안전성 관련 법제를 살펴보고 보안문제와 안전성 문제의 관계를 다루었습니다. 그리고 IoT기반 소비자제품의 위해요인이 기존 소

비자제품안전 법제에 미치는 법·정책적 시사점과 대응방안을 중심으로 국제적 논의를 조사·분석하였습니다.

이 보고서가 앞으로 IoT기반 소비자제품의 안전강화에 기여할 수 있는 제도와 정책을 마련하는데 유용한 기초자료가 될 것으로 기대합니다. 끝으로, 연구의 진행 과정에서 유익한 의견을 주신 전문가 여러분들과 보고서 발간을 위해 애써주신 분들에게 감사의 뜻을 표합니다.

2020. 1.

한국소비자원

원장 이 회 숙

## 국문 요약

4차 산업혁명의 핵심 기술인 사물인터넷(IoT)을 활용한 IoT기반 소비자제품은 그 다양성과 시장규모가 지속적으로 증가 및 성장하고 있으며 한국은 이 분야를 선도하고 있다. 그러나 IoT기반 소비자제품은 소비자에게 편리성, 제품의 효용성 제고란 이점을 제공하지만 동시에 소비자안전에 대한 잠재적 위해요인을 가지고 있다.

이와 관련하여 최근 국제적으로 IoT기반 소비자제품의 잠재적 위해요인을 조사하고 이에 대한 법·정책적 대응방안을 논의하고 있다. 미국의 소비자제품안전위원회(CPSC)는 2018년 5월에 IoT기반 소비자제품의 위해요인에 관한 공개 청문회를 개최하여 연방정부부처, 소비자단체, IT단체 등으로부터 다양한 의견을 수렴하였고, 2019년 1월에는 Kaye위원 명의의 ‘IoT 안전성 기준에 대한 의견서’를 공표하였다. OECD도 여러 보고서를 통해 IoT기반 소비자제품의 안전성 문제를 논의해 왔고, 최근 소비자정책위원회 산하 제품안전작업반에서 IoT기반 소비자제품의 안전문제를 다루고 있다.

본 연구는 IoT기반 소비자제품의 의미와 특성을 살펴보고, IoT기반 소비자제품의 위해요인과 이에 대한 법·정책적 대응방안에 관한 국제적 논의동향을 조사한다. 그리고 IoT기반 소비자제품의 안전에 관한 국내 법제를 조사·분석하여 소비자안전 강화를 위한 법·정책적 개선방안을 제안하고자 한다. 본 연구는 5개 장으로 구성되어 있으며 1장은 서론부분으로 연구의 목적과 범위 등을 다루고 있다. 2장은 IoT기반 소비자제

품의 의미와 현황을 다루고 있다. IoT와 소비자제품의 개념을 살펴보고 IoT기반 소비자제품의 특성 및 시장규모 등을 분석한다. 3장은 IoT기반 소비자제품 안전에 관한 국내법제와 국제적인 논의를 조사·분석한다. IoT기반 소비자제품 중 가전제품 분야가 높은 비중을 차지하는 점을 고려하여, 여기에 적용될 수 있는 전기생활용품안전법을 분석대상으로 한다. 또한, IoT기반 소비자제품이 정보통신망과 연결되어 있는 특성을 고려하여 정보통신망의 안전을 규율한 정보통신망법도 포함하여 검토한다. 국제적인 논의는 IoT기반 소비자제품의 위해요인과 이에 대한 법·정책적 대응방안으로 구분하여 미국, OECD의 논의를 조사·분석한다. 이를 통해 연결성 상실, 데이터 훼손, 소프트웨어 업데이트 등의 위해요인을 인식하고 이의 통제를 위한 방안 및 보안과 안전성 확보의 관련성, 재화와 용역의 경계설정의 어려움 등 법·정책적 문제를 확인할 수 있다. 4장은 IoT기반 소비자제품 안전에 관한 법·정책적 개선방안을 제안한다. 여기에는 새로운 위해요인에 대한 조사·분석, 기술융합에 따른 안전관리 체계 및 협력체계 구축이 있다. 또한 이를 위해 전기생활용품안전법과 정보통신망법 등 관련 법제의 정비 필요성을 제안한다. 5장은 결론부분으로 전체 연구를 요약하고 연구의 의미와 한계를 다루고 있다.

# 차 례

■ 머리말 .....	iii
■ 국문요약 .....	v

## 제1장 서론 1

제1절 연구의 배경 및 목적 .....	3
1. 연구의 배경 .....	3
2. 연구의 목적 .....	6
제2절 연구의 범위 및 방법 .....	7
1. 연구의 범위 .....	7
2. 연구의 방법 .....	11

## 제2장 IoT기반 소비자제품의 의의 및 현황 13

제1절 IoT기반 소비자제품의 개념 .....	15
1. IoT(사물인터넷) 개념 .....	15
2. 소비자제품의 정의 .....	25
3. IoT기반 소비자제품의 의의 및 종류 .....	31
제2절 IoT기반 소비자제품의 특성 및 현황 .....	36
1. IoT기반 소비자제품의 특성 및 이슈 .....	36
2. IoT 제품시장 현황 .....	42



## 제3장 IoT기반 소비자제품안전 관련 국내법제 및 국제논의 동향 51

- 제1절 IoT기반 소비자제품안전 관련 국내법제 ..... 53
1. 소비자제품 안전법제와 IoT기반 소비자제품 ..... 53
  2. IoT기반 소비자제품 안전을 규율하는 주요 국내 법제 ..... 55
- 제2절 IoT기반 소비자제품안전 관련 국제논의 동향 ..... 74
1. IoT기반 소비자제품의 위해요인 ..... 74
  2. 위해요인에 대한 법·정책적 대응 ..... 89

## 제4장 IoT기반 소비자제품 안전에 관한 법·정책적 개선방안 117

- 제1절 새로운 위해요인에 대한 조사·분석 및 법체계 정비 ..... 119
- 제2절 기술융합에 따른 안전관리 체계 및 협력체계 구축 ..... 122

## 제5장 결 론 125

- 제1절 연구의 요약 ..... 127
- 제2절 연구의 의의 및 한계 ..... 129

## 참고문헌 131

## Executive Summary 137

## 표 차례

---

〈표 2-1〉 사업 분야별 사물인터넷 사업체 수 .....	46
〈표 2-2〉 종사자 규모별 사물인터넷 사업체 수 .....	46
〈표 2-3〉 사업 분야별/종사자 규모별 사물인터넷 사업체 수 .....	47
〈표 2-4〉 사업 분야별 매출액 .....	48
〈표 2-5〉 사물인터넷 서비스의 활용 분야별 매출액 .....	49
〈표 2-6〉 사업 분야별 내수액 .....	49
〈표 2-7〉 사물인터넷 서비스의 활용 분야별 내수액 .....	50
〈표 3-1〉 정보보호지침에 포함되어야 하는 사항 .....	64
〈표 3-2〉 「정보보호지침」상 보호조치 세부항목 .....	65
〈표 3-3〉 정보보호최고책임자의 업무 .....	66
〈표 3-4〉 IoT 공통보안 7대 원칙 .....	70
〈표 3-5〉 홈·가전 공통 보안항목 및 요구사항 .....	72
〈표 3-6〉 CPSC의 소비자제품 관련 신기술 목록 .....	75
〈표 3-7〉 CPSC의 소비자제품 관련 신기술의 위해요인 .....	76
〈표 3-8〉 연방거래위원회의 위해요인 사례 .....	80

## 그림 차례

---

〈그림 1-1〉 100명당 IoT 기반 소비자제품 수, OECD 국가 중 상위 10개국 .....	5
〈그림 2-1〉 ITU가 제시하는 사물인터넷 시대의 사물 및 통신환경의 변화 .....	20
〈그림 2-2〉 사물인터넷 개념의 진화 .....	22
〈그림 2-3〉 사물인터넷 서비스 활용분야 .....	34
〈그림 2-4〉 사물인터넷 분야별 시장규모(2016~2022) .....	44
〈그림 2-5〉 사물인터넷 매출액 추이(2015~2018년) .....	47
〈그림 3-1〉 안전관리 대상 제품 분류 .....	58

# 제1장 서론

제1절 연구의 배경 및 목적

제2절 연구의 범위 및 방법





## 제1절 | 연구의 배경 및 목적

### 1. 연구의 배경

현재 우리사회는 정보통신기술의 비약적 발전에 따라 새로운 사회적 패러다임의 변화를 경험하고 있다. 기존의 정보통신기술이 사람과 사람, 사람과 가상공간을 연결하는 단계였다면, 이제는 사람과 사물, 공간, 가상공간 등이 인터넷과 연결되어 새로운 초연결사회(hyper-connected society)<sup>1)</sup>가 도래하고 있다. 이러한 초연결사회에서는 각종 정보가 생성·수집·공유·활용되고 기존에는 제공할 수 없었던, 활용할 수 없었던 새로운 서비스가 가능해지고 새로운 제품이 등장하고 있다. 이른바 사물인터넷(Internet of Things, IoT)<sup>2)</sup>이라는 새로운 환경이 이를 대변하고 있다.<sup>3)</sup> 기존 제품 및 서비스와 정보통신기술의 융합이 점차 시대적인 추세가 되어가고 있는 바, 이로 인해 기존 산업과 정보통신 기술이 접목되어 새로운 부가 가치를 창출하고 있으며, 융합기술 및 서비스가 혁신적으로 발전·확산되고 있다. 정보통신기술(Information and Communications Technologies, ICT) 융합은 특히 콘텐츠(Contents), 플랫폼(Platform), 네트워크(Network), 디바이스(Device)의 “C-P-N-D

- 1) 초연결사회란 인터넷, 통신기술 등의 발달에 따라 네트워크로 사람, 데이터, 사물 등 모든 것을 연결한 사회를 말한다. 사람과 사람을 둘러싸고 있는 다양한 사물들이 생성하는 데이터 간의 연결을 통해 사회 전 분야에 변화와 혁신을 이끄는 사회를 말한다. 즉, 사람과 사람, 사람과 사물, 사물과 사물이 연결되는 초연결사회는 단순히 모든 것의 물리적 연결 수단으로서의 네트워크 개념에서 모든 서비스의 연결로 진화되어 가는 것이다. 김영순, “제4차 산업혁명과 초연결사회 그리고 사물인터넷 시대”, 한국콘텐츠학회 한국콘텐츠학회지 제17권 제3호(2019), p.15
- 2) 이하 본 보고서에서는 사물인터넷과 이의 영어명칭인 IoT를 혼용하여 사용하고자 한다. 두 용어는 대체가능한 용어이며 상황에 따라 ‘사물인터넷’ 혹은 영어 약칭인 ‘IoT’를 선택적으로 사용한다.
- 3) 이도국, “사물인터넷(Internet of Things) 환경에 있어 민사법적 문제점에 대한 소고”, 한양대법학연구소 한양법학 제26권 제2집(2015), p.221

체계”로의 의존성이 특징이다.<sup>4)</sup> ICT 융합이 “C-P-N-D 체계”를 기반으로 패러다임의 전환을 이루어냈다면, 사물인터넷은 나아가 이러한 “C-P-N-D 체계”를 허물고 통합된 생태계 구축을 위한 방향으로 진전되고 있음을 보여준다.<sup>5)</sup> 이러한 초연결사회의 도래와 ICT 기술의 융합은 사물인터넷의 중요성과 활용성이 극대화될 수 있고, 그에 따른 법제 도적인 차원의 대응 필요성을 제기하고 있다.

이와 관련하여 최근 사물인터넷과 관련 기술의 발전 및 융합에 따라 이를 활용한 소비자제품이 증가하고 있으며 관련 시장도 지속적으로 성장하고 있다. IoT기반 소비자제품<sup>6)</sup>은 그 다양성과 시장규모가 지속적으로 증가·성장하고 있으며 한국은 이 분야를 선도하고 있다. 2015년 OECD 자료에 따르면 전세계 IoT기반 소비자제품은 3.63억 개에 이르고 이 중 중국이 8.4백만 개, 미국이 7.8백만 개, 한국, 브라질, 및 독일이 1.8백만 개를 차지하고 있다고 한다. 한국은 전체 IoT기반 소비자제품의 개수로는 최상위에 포함되지 않았지만, 인구 100명당 제품수로는 OECD 국가 중 1위에 해당한다.<sup>7)</sup>

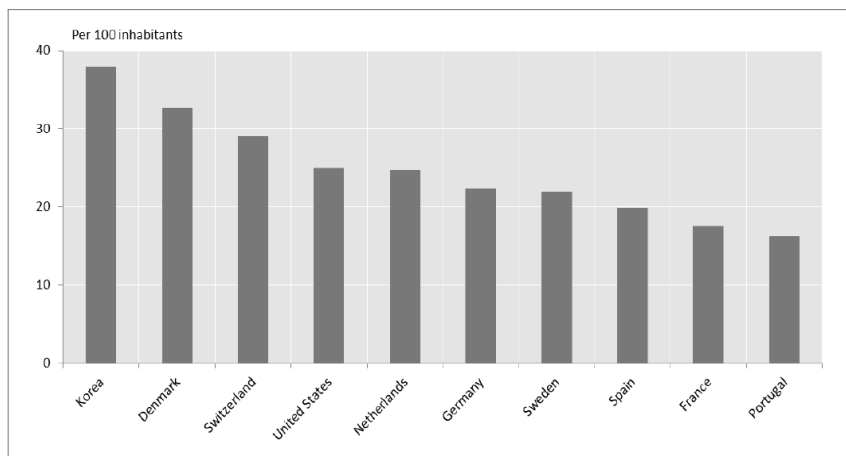
4) 최계영 외, 「소통과 창조 기반의 ICT 미래 국가발전전략 연구」, 방송통신위원회 (2012), pp.8-10.

5) “C-P-N-D 내부의 신산업과 신규 서비스는 물론, 이를 넘어서, 자동차, 조선, 의료, 교육 등 다방면에 ICT 부문과 타부문간의 융합이 진행 중이며, 새로운 ICT 생태계도 가능할 전망이다. 자동차, 조선, 의료 교육 등의 부문에서 SW의 활용성 증대가 ICT융합이라는 차원에서 진행 중이며, 특히 개인, 집단의 유전자 정보, 생체정보, 클라우드 서비스 등 바이오 산업과의 융합도 전망된다. 초정밀 의료기기, 자동차, 로봇 등 하드웨어는 이를 운영하기 위한 OS와 애플리케이션도 미래 신시장 창출이 예상되며 인공지능의 다양한 분야에의 적용가능성을 살펴볼 필요가 있다.” 최계영 외, 앞의 보고서, p.12

6) 사물인터넷을 활용한 소비자제품을 가리킨다. 이하 본 보고서에서 ‘IoT기반 소비자제품’은 기존의 소비자제품과는 구분되는 것으로서 IoT(사물인터넷)을 활용한 소비자제품을 별도로 지칭하는 것이다.

7) OECD(2015), Digital Economy Outlook 2015

〈그림 1-1〉 100명당 IoT 기반 소비자제품 수, OECD 국가 중 상위 10개국



출처: OECD(2015), Digital Economy Outlook 2015

IoT기반 소비자제품은 소비자에게 편리성, 제품의 효용성 제고 등 여러 가지 다양한 이점을 제공하고 있다. 하지만 동시에 IoT기반 소비자제품은 소비자에게 안전에 대한 잠재적 위험성을 야기할 가능성을 가지고 있다. 이러한 위험요인으로 네트워크 연결오류, 해킹 등에 따른 프라이버시 침해 및 오작동에 의한 위해 문제 등 사물인터넷의 특성이 고스란히 반영된 것들이 제기되고 있다.

이에 따라 국제적으로 IoT기반 소비자제품의 잠재적 위험요인을 조사하고 이에 대한 법적 대응방안을 모색하고 있다. 예를 들어, 미국의 소비자제품안전위원회(Consumer Product Safety Commission, CPSC)는 2017년 IoT기반 소비자제품의 위험요인을 조사·분석하였다. OECD의 경우에도 IoT기반 소비자제품의 위험요인을 조사·분석하고, 소비자제품안전 규제체제에 미치는 정책적 함의를 지속적으로 논의하고 있다.



## 2. 연구의 목적

본 연구의 목적은 IoT 기반 소비자제품이 가지는 안전성 위해요인을 파악하고 이에 대한 법제적 대응방안을 모색하는 것이다. 초연결사회의 핵심 기술인 사물인터넷의 등장과 이의 활용에 따라 소비자가 가지는 이점과 함께 잠재적인 안전성 위해요인이 지적되고 있는 바, 본 연구는 이를 조사·분석하고 법제도 및 정책적인 관점에서 이에 대한 대응방안을 찾고자 한다. 이는 IoT 기반 소비자제품이 가지는 소비자안전의 위해요인이 무엇인지를 파악하고 이것이 소비자안전에 관한 법체계에 어떠한 정책적 함의를 가지며 영향을 미치게 되는지를 분석하는 것이다. 이러한 과정을 거치면서 법제도적인 측면에서 개선방안까지를 발견하고자 하는 것이 연구의 목적인 것이다.

이를 위하여 IoT 기반 소비자제품의 위해요인 및 법제적 대응방안에 관한 국제적 논의동향을 조사·분석하고, 이에 관한 우리법제의 현황 검토 및 시사점 발굴을 통해 IoT기반 소비자제품의 안전강화를 위한 법제 개선방안을 제시하고자 한다.

## 제2절 | 연구의 범위 및 방법

### 1. 연구의 범위

사물인터넷 분야의 기존 선행연구를 살펴보면, 센싱·인증·보안·네트워킹 등 기술적인 측면과 사물인터넷 시장·서비스의 동향이나 성장추이 등에 집중되어 있어, 법·제도적인 차원의 연구가 상대적으로 부족한 실정이다.<sup>8)</sup> 이에 더하여 사물인터넷에 관련한 법제도적인 연구의 대부분은 사물인터넷 진흥이나 개인정보보호에 초점을 맞추고 있다.<sup>9)</sup> 연구의 목적 부분에서 설명한 것과 같이, 본 연구의 범위는 IoT기반 소비자제품이 가지는 소비자에 대한 안전성 문제와 이것의 법정정책적 함의를 조사·분석하는 것이다. 또한, 이를 통해 IoT기반 소비자제품의 위해요인을 반영한 소비자안전법제의 개선방안을 모색하는 것이다. 따라서 이러한 측면에서 본 연구는 사물인터넷에 관한 법제도 분야 선행연구와의 차별성을 가지며, 이것이 본 연구의 주요 대상이다.

이를 위하여 본 연구에서는 IoT기반 소비자제품의 개념, 현황 및 특성을 살펴본다. 여기서는 사물인터넷과 소비자제품의 개념을 살펴보고 IoT 기반 소비자제품의 종류 및 주요 현황을 조사·분석한다. 또한, IoT 기반 소비자제품의 특성과 함께 일반소비자제품에 비해 가지는 이점과

8) 정원준, “사물인터넷(IoT) 활성화를 위한 법·제도적 개선방안 연구”, 한국법정책학회 법과 정책연구 제14집 제4호(2014), p.4

9) 정원준, “사물인터넷(IoT) 활성화를 위한 법·제도적 개선방안 연구”, 한국법정책학회 법과 정책연구 제14집 제4호(2014); 정혁·이대호, 「사물인터넷 진화와 정책적 제언」, 정보통신정책연구원 보고서(2014); 이도국, “사물인터넷(Internet of Things) 환경에 있어 민사법적 문제점에 대한 소고”, 한양대법학연구소 한양법학 제26권 제2집(2015); 김지영, “개인정보보호를 위한 사물인터넷의 법적 규율에 관한 고찰”, 한국법정책학회 법과 정책연구 제15집 제4호(2015); 사지연, 「사물인터넷 관련 개인정보 관리에서의 소비자권의 강화 연구」, 한국소비자원 정책연구 17-14(2017) 등.

이에 대하여 제기되는 이슈를 살펴본다. IoT기반 소비자제품의 안전에 관련하여 본 연구에서는 안전과 위해, 위해요인 개념을 구분하여 사용하고자 한다. 사전적으로 안전은 ‘위험이 생기거나 사고가 날 염려가 없거나 그러한 상태’<sup>10)</sup> 또는 ‘위험이 없어서 피해를 입을 수 없는 것을 말한다. 안전에는 교통안전, 식품안전, 환경안전, 국가안전 등으로 나뉜다.’<sup>11)</sup>고 정의하고 있다. 한편, 위해의 사전적 의미는 ‘위험과 재해를 아울러 이르는 말’<sup>12)</sup>로서 정의하고 있다. 위험에 대하여는 ‘해로움이나 손실이 생길 우려가 있거나 그런 상태’<sup>13)</sup> 또는 ‘손해의 가능성을 의미하는 개념이다. 가치를 잃거나 얻을 수 있는 잠재성을 의미하기도 한다.’<sup>14)</sup>고 정의하고 있다. 이러한 사전적 정의에 따르면 위해와 위험의 구분이 모호해 지고 위해가 위험을 포괄하는 광범위한 것을 가리키는 것으로 보인다. 그러나 위해와 위험은 구분되는 개념이다. 일반적으로 위험은 손실이나 손해가 발생할 가능성을 의미하며 위해는 손실이나 손해가 현실화되어 발생한 결과를 가리킨다. 즉, 위해는 위험이 구체화되어 현실화된 상태를 가리키는 것이다.<sup>15)</sup> 따라서 소비자에게 발생하는 위해를 소비자위해라고 한다면, 소비자위해는 크게 신체상위해와 재산상위해로 나눌 수 있고, 신체상위해는 물리적 위해, 생물학적 위해, 화학적 위해로 구분될 수 있다.<sup>16)</sup> 위해, 위험과 구분되는 것으로 인간, 재산 및 환

10) 네이버 국어사전 ‘안전’ <https://ko.dict.naver.com/#/entry/koko/4edc1416bc8643669da78d84972927dc>

11) <https://ko.wikipedia.org/wiki/%EC%95%88%EC%A0%84>

12) <https://ko.dict.naver.com/#/entry/koko/5433a9d748e14c07a8fbe3d834d1357c>

13) <https://ko.dict.naver.com/#/entry/koko/1304f5e1b67e43a2ad37e9faf68ef9d1>

14) <https://ko.wikipedia.org/wiki/%EC%9C%84%ED%97%98>

15) 송순영, 「위해정보 수집·제공 체계 개선에 관한 연구」, 한국소비자원 정책연구(2013), p.25

16) 송순영, 「위해정보 수집·제공 체계 개선에 관한 연구」, 한국소비자원 정책연구(2013), p.26

경에 해를 끼치는 잠재성이 있는 상황, 요소를 hazard라고 하고 이를 위해요소, 위해요인으로 번역하여 사용하고 있다.<sup>17)</sup> 따라서 위해요인은 위해가 되는 원인을 의미하고 위험은 이러한 위해요인이 위해로 현실화 될 가능성을 가리키는 것이다.

IoT 기반 소비자제품의 안전에 관하여도 이러한 용어의 사용례를 그대로 따라 위해, 위해요인, 위험을 사용하기로 한다. 따라서 소비자제품의 안전은 위해의 위험으로부터 자유로운 것을 의미하는 것이고, 위해요인은 위해의 잠재적인 요소나 상태를 의미한다. 다만, IoT기반 소비자제품 안전에서 위해는 통상 재산상 위해가 아닌 신체상 위해를 의미한다.<sup>18)</sup> 따라서 IoT기반 소비자제품의 안전문제는 해당 제품이 소비자에게 야기하는 신체적 위험을 통제하는 것이다. 미국의 CPSC에서도 IoT기반 소비자제품의 안전을 ‘기계적 접촉, 전기 또는 열에너지 방출이나 독극물 노출로 인한 사망, 신체적 위해 또는 질병의 방지’로 정의하고 있다.<sup>19)</sup> 실정법상으로도 동일한 의미는 아니지만 「어린이제품 안전 특별법」 제2조제5호에서는 위해를 “어린이제품에 존재하는 위험요소로서 인체의 건강을 해치거나 해칠 우려가 있는 것을 말한다”고 정의하여, 위해를 신체상 손해를 중심으로 정의하고 있다.<sup>20)</sup>

이러한 개념정의에 따라 국내의 IoT기반 소비자제품안전 관련 법제와 국제적인 규제논의 현황을 살펴본다. 우선적으로 IoT기반 소비자제

17) 송순영, 「위해정보 수집·제공 체계 개선에 관한 연구」, 한국소비자원 정책연구 (2013), p.27

18) 송순영, 「위해정보 수집·제공 체계 개선에 관한 연구」, 한국소비자원 정책연구 (2013), p.27

19) CPSC, Statement of Commissioner Elliot F. Kaye Regarding a framework of safety for the Internet of Things(2019.1), p.1

20) 물론, 이러한 위해 개념은 위험, 위해요인과 구분되지 아니하고 위해를 위험처럼 가능성을 통해 정의한 한계가 있다. 그럼에도 위해를 신체상 손해로 보았다는 점을 주목할 필요가 있다.

품의 안전 관련 국내 법제를 고찰하는데, 여기에는 전통적인 제품안전 관련 법률 이외에도 정보보호에 관한 법률도 살펴본다. 이는 IoT기반 소비자제품이 가지는 특성에 따라 인터넷 등 네트워킹의 안전성 문제가 IoT기반 소비자제품의 안전문제와 밀접하게 연결되기 때문이다. 따라서 종래 소비자제품의 안전법제에 한정하지 않고 정보보호에 관한 법률도 연구범위에 포함시킨다. 그리고 IoT기반 소비자제품의 안전 관련 국내법제에서 사전적 규제체계를 중심으로 다루고자 한다. 소비자제품안전 규제에 있어서 사후적 규제 보다 사전적 규제를 통한 위해관리가 중요하기 때문이다. 이에 IoT기반 소비자제품을 규율하는 법제에서는 사전적 규제와 정보보호에 관련한 법을 중심으로 고찰한다.

다음으로 IoT기반 소비자제품의 안전관련 국제적 논의는 위해요인에 대한 조사·분석과 이에 대한 법·정책적 대응을 중심으로 다룬다. 이를 위해 IoT기반 소비자제품의 안전성 위해요인에 관한 미국과 OECD의 관련 자료의 조사 및 분석을 통해 이에 관한 논의를 살펴본다. 그리고 IoT기반 소비자제품의 이러한 위해요인에 관한 법·정책적인 대응 방안에 관한 미국, OECD의 사례를 살펴본다. 여기서는 주로 IoT기반 소비자제품의 위해요인이 제품안전법제에 미치는 영향 및 쟁점과 이에 대한 미국, OECD의 법제개선 논의를 조사·분석이 주요 연구범위이다. IoT기반 소비자제품의 안전성 위해요인이 소비자법제에 미치는 법·정책적 시사점을 조사·분석하여 현행 우리의 소비자안전법제에의 법·정책적 개선방안을 찾고자 한다.

## 2. 연구의 방법

본 연구는 IoT기반 소비자제품의 안전성 강화를 위한 법제개선방안을 마련하는 것이 목적이다. 이러한 연구목적을 위한 방법론으로는 비교법 연구를 사용한다. 이를 위하여 IoT 기술의 개념정의와 현황을 살펴보고 IoT기반 소비자제품이 가지는 안전성 위해요인을 조사·분석한다. 또한, IoT기반 소비자제품의 위해요인이 제품안전법제에 미치는 영향 및 쟁점과 이에 대한 미국, OECD의 법제적 대응현황을 조사·분석한다. 이를 통하여 IoT기반 소비자제품의 위해요인이 소비자안전법제에 미치는 법정정책적 시사점을 살펴본다. 또한 현행 소비자안전법제와의 비교법 연구를 통해 법제적 개선방안을 모색한다. 비교법 연구를 위하여 국내 소비자안전법제 전반을 개괄적으로 살펴보고, 개별 법률은 「정보통신망법」과 「전기생활용품안전법」등 소비자제품안전 관련 법률을 중심으로 고찰한다. IoT기반 소비자제품의 위해요인에 관한 법정정책적 시사점과 현행 법제와의 비교를 통해 문제점을 파악한다.

본 연구는 이러한 비교법 연구 및 법제분석을 통해 IoT기반 소비자제품 안전강화를 위한 법제개선방안을 도출한다. 법제개선방안은 IoT기반 소비자제품 위해요인에 관한 미국, EU 등의 대응방안과 법·정책적 시사점을 반영할 수 있도록 연구를 진행한다.



## 제2장 IoT기반 소비자제품의 의의 및 현황

제1절 IoT기반 소비자제품의 개념

제2절 IoT기반 소비자제품의 특성 및 현황





## 제1절 | IoT기반 소비자제품의 개념

### 1. IoT(사물인터넷) 개념

#### 1) 사물인터넷 개념에 관한 다양한 정의

현재 사물인터넷에 관하여 통용되는 것으로 인정할 수 있는 합의된 정의는 없다.<sup>21)</sup> 국제기구나 IT분야의 주요 단체마다 사물인터넷에 관하여 다양한 방식의 정의가 이루어지고 있으며, 학계의 경우에도 사물인터넷에 관하여 통일적이고 일원적인 정의는 없는 상태에서 다양한 방식의 정의가 이루어지고 있다. 사물인터넷의 개념 정의가 이처럼 다원적인 것은 사물인터넷 자체가 최근에 등장한 것이고 아직도 발전·진화하고 있는 기술이기 때문이다.<sup>22)</sup> 하지만 사물인터넷의 개념 정의가 다양하다고 해서 그것이 전혀 유사성이나 공통점을 가지고 있는 것은 아니다. 사물인터넷의 개념 정의가 이를 논의하는 여러 주체에 따라 차이가 있는 것은 분명하지만 일정한 공통분모를 공유하고 있는 것도 사실이다. 따라서 사물인터넷 개념을 살펴보기 위한 방법으로 이에 대한 다양하고 다원적인 정의를 살펴보고 이의 공통점을 도출하고 이를 토대로 개념 정의를 구성하는 것이 필요하다.

사전적인 차원에서 사물인터넷을 보면, 통상 “사물들이 서로 연결된 것 혹은 사물들로 구성된 인터넷을 말한다.”<sup>23)</sup> 또는 “사물에 센서를 부착해 실시간으로 데이터를 인터넷으로 주고받는 기술이나 환경”<sup>24)</sup>으로

21) 사지연, 「사물인터넷 관련 개인정보 관리에서의 소비자권의 강화 연구」, 한국소비자원 정책연구 17-14(2017), p.39

22) 같은 견해로 정원준, “사물인터넷(IoT) 활성화를 위한 법·제도적 개선방안 연구”, 한국법정책학회, 법과 정책연구 제14집 제4호(2014.12), p.5

23) 국립중앙과학관-사물인터넷, 네이버지식백과 <https://terms.naver.com/entry.nhn?docId=3386810&cid=58369&categoryId=58369>

정의하고 있다. 이러한 정의와 더불어 사물인터넷에 대한 부연설명으로 “기존의 인터넷이 컴퓨터나 무선인터넷이 가능했던 휴대전화들이 서로 연결되어 구성되었던 것과는 달리, 사물인터넷은 책상, 자동차, 가방, 나무, 에어컨 등 세상에 존재하는 모든 사물이 연결되어 구성된 인터넷이라 할 수 있다.”<sup>25)</sup> 혹은 “지금까진 인터넷에 연결된 기기들이 정보를 주고받으려면 인간의 ‘조작’이 개입되어야 했다. 사물인터넷 시대가 열리면 인터넷에 연결된 기기는 사람의 도움 없이 서로 알아서 정보를 주고받으며 소통하게 된다.”<sup>26)</sup>고 되어있다.

학계에서 사물인터넷의 개념 정의도 사전적인 것과 유사점을 보이고 있는데, 개별 학문별 차이점이 있지만 대체적으로 “기기 및 사물에 통신 모듈을 탑재하여 유무선 네트워크로 연결함으로써 사람과 사물, 사물과 사물 간 정보교환 및 상호 소통을 하는 지능형 인프라”<sup>27)</sup>, “개방형 환경에서 인터넷을 기반으로 사람, 사물, 데이터 및 프로세스를 서로 결합하여 정보를 교류하고 상호 소통하는 지능형 인프라”<sup>28)</sup>로 정의한다. 그리고 “사람, 사물, 공간 등 모든 것들이 인터넷으로 서로 연결되어, 모든 것들에 대한 정보가 생성·수집되고 공유·활용 되는 것”<sup>29)</sup> 또는 “스스로 행동할 수 있는 지능을 가진 각각의 사물이 네트워크를 통하여 사람 혹은 다른 사물과 소통하고 그 정보를 바탕으로 새로운 가치 및 서비스를

24) 네이버캐스트 용어로 보는 IT

<https://terms.naver.com/entry.nhn?docId=3577301&cid=59088&categoryId=59096>

25) 국립중앙과학관-사물인터넷, 네이버지식백과

26) 네이버캐스트 용어로 보는 IT

27) 정원준, “사물인터넷(IoT) 활성화를 위한 법·제도적 개선방안 연구”, 한국법정책학회, 법과 정책연구 제14집 제4호(2014.12), p.4

28) 정혜옥, “사물인터넷 활성화와 법제도에 관한 연구”, 중앙대학교 문화미디어엔터테인먼트법연구소, 문화·미디어·엔터테인먼트 법(2014.5), p.56

29) 정혁·이대호, 「사물인터넷 진화와 정책적 제언」, 정보통신정책연구원 보고서(2014), p.1

제공하는 것”<sup>30)</sup>으로 정의하고 있다. 사물인터넷의 주요 특성으로 “사람, 사물, 공간, 데이터 등 모든 것이 인터넷으로 연결되어 정보 생성·수집, 저장·공유, 분석·예측이 가능하며, 그 핵심으로는 디바이스, 네트워크 등이 있다.”<sup>31)</sup>고 설명하기도 한다.

사물인터넷에 대한 국제기구의 개념 정의를 살펴보자. EU의 경우 사물인터넷의 개념에 관하여는 “임베디드 센서를 통해 사물 그 자체, 사물과 사물, 사물과 인간이 결합된 장치가 데이터를 기록, 처리, 저장 및 전송할 수 있으며, 고유식별코드와 연결된 경우에는 다른 장치 혹은 네트워크 시스템과 상호 작용할 수 있도록 하는 인프라를 말한다.”로 정의하고 있다.<sup>32)</sup> OECD는 사물인터넷을 “외부 세계를 감지하고 상호작용하는 장비로부터 수집된 데이터에 따라 작동하는 앱(applications) 및 서비스 생태계”로 지칭하고 있다.<sup>33)</sup> OECD는 사물인터넷에 관하여 다음과 같이 추가적인 설명을 하고 있다.

*“...개인의 능동적인 개입이 있는 상태로 또는 없는 상태로 인터넷을 통하여 상태가 대체될 수 있는(whose state can be altered via the Internet) 장비 및 물건. 이것은 랩탑(laptops), 라우터(routers), 서버(servers), 태블릿(tablets) 그리고 스마트폰을 포함*

30) 이도국, “사물인터넷 환경에 있어 민사법적 문제점에 대한 소고”, 한양대법학연구소, 한양법학 제26권 제2호(2015), p.223

31) 김영순, “제4차 산업혁명과 초연결사회 그리고 사물인터넷 시대”, 한국콘텐츠학회 한국콘텐츠학회지 제17권 제3호(2019.9)

32) Article 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things, 2014, p.4; 김지영, “개인정보보호를 위한 사물인터넷의 법적 규율에 관한 고찰”, 한국법정책학회, 법과 정책연구 제15집 제4호(2015.12), p.5에서 재인용.

33) OECD(2016), “The Internet of Things: Seizing the Benefits and Addressing the Challenges”, OECD Digital Economy Papers, No.252, OECD Publishing, Paris.

하며, 종종 자주 ‘전통적인 인터넷’의 일부로 간주된다. 그러나 이러한 장비들은 사물인터넷 장비의 상태를 읽고, 분석하고 작동시키는 것과 통합되어 있고 당해 시스템의 ‘심장과 뇌’를 구성하고 있다. 그렇기 때문에 이들을 배제하는 것은 타당하지 않다.”<sup>34)</sup>

한편, 미국의 소비자제품안전위원회(Consumer Product Safety Commission, CPSC)는 사물인터넷과 소비자제품 위해에 관한 공개 청문회를 개최하면서, 사물인터넷 소비자제품을 “데이터를 송·수신하고, 작동 소프트웨어나 펌웨어를 업로드 또는 다운로드할 수 있고, 또는 다른 인터넷-연결 기기와 소통할 수 있는 인터넷과 연결되는 제품”으로 정의하고 있다.<sup>35)</sup> 회계감사원(Government Accountability Office, GAO)은 사물인터넷을 “광범위한 장비, 또는 ‘사물’이 건물, 차량, 대중교통 설비, 또는 가정과 같은 장소를 통해 상호작용하고 연결되는 기술을 가리킨다. 사물인터넷 장비나 스마트 기기는 이전에는 불가능하던 영역에서 소통과 정보처리를 가능하게 한다.”고 설명하고 있다.<sup>36)</sup>

IT관련 글로벌 표준기구의 사물인터넷에 관한 개념 정의도 다양하게 이루어지고 있다. 국제전통신연합(International Telecommunication Union, ITU)에서는 사물인터넷을 “글로벌 ICT를 기반으로 다양한 물리적 및 가상의 사물들을 연결하여 정보화 사회를 위한 진일보한 서비스를 제공할 수 있는 글로벌 서비스 인프라”로 정의하고 있다.<sup>37)</sup> 그리

34) OECD(2015), OECD Digital Economy Outlook 2015, OECD Publishing, Paris.

35) 사물인터넷과 소비자제품 위해에 관한 공개 청문회 개최를 공지하는 연방관보에서 이렇게 정의한 것이다. IoT Hearing, 83 Fed. Reg.13123

36) U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-17-570, Internet of Things, Communities Deploy Projects by Combining Federal Support with Other Funds and Expense(2017), p.1

37) Rec. ITU-T Y.2060 (2012.6), Definition 3.2.2

고 사물인터넷과 유사한 개념으로서 사물통신(Machine to Machine, M2M)에 관하여 유럽전기통신표준협회(European Telecommunications Standards Institution, ETSI)는 “두 개 혹은 그 이상의 기기가 필수적인 인간의 개입이 없이 소통하는 것”<sup>38)</sup>으로, 전기전자기술자협회(Institute of Electrical and Electronics Engineers, IEEE)는 “가입자 장치(subscriber station)와 기지국(base station)을 거쳐 코어-네트워크에 위치하는 서버간의 정보 교환 혹은 가입자 장치 간 인간의 개입 없이 발생하는 정보 교환”<sup>39)</sup>으로 정의하고 있다.

사물인터넷에 관한 이러한 다양한 정의방식에는 차이점도 있지만 분명한 공통점도 존재한다. 사물인터넷이 최신의 기술이며 아직 발전하고 있는 것이기 때문에 개념이 정치하게 정의되고 사용되는 것은 아니지만, 무엇인가 새로운 기술과 인터넷 환경이 등장하고 있고 이를 가리키는 개념으로 사물인터넷이란 용어가 사용되고 있다. 따라서 학계나 국제기구, IT 전문단체의 사물인터넷에 대한 다양한 개념의 공통적 특성을 도출하여 사물인터넷 개념을 정립하는 것이 필요할 것이다. 아래에서는 이에 앞서, 사물인터넷 개념의 발달과정과 유사개념사이의 관계를 살펴본다.

## 2) 사물인터넷 개념의 발달과정

사물인터넷이란 용어는 1998년 MIT Auto-ID Center의 설립자 Kevin Ashton이 처음으로 사용하였고, 이후 2005년 ITU가 발간한 동명의 보고서를 통해 관련 이슈가 부각되었다.<sup>40)</sup> Kevin Ashton은

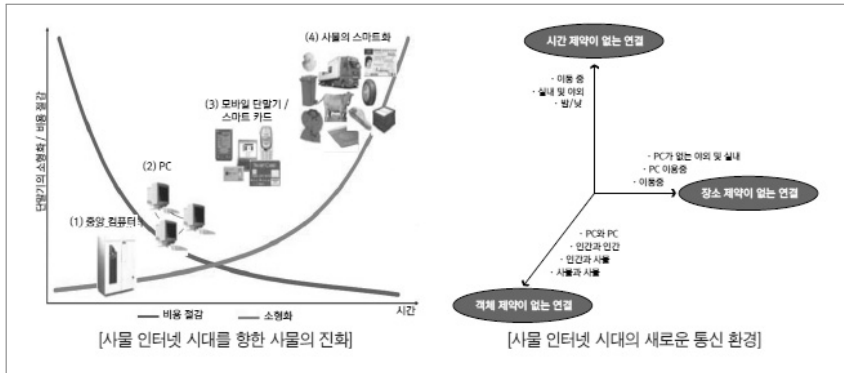
38) 미래창조과학부 방송통신정책연구 15-진흥-033, 「사물인터넷 진흥 및 융합활성화를 위한 법제도 개선 연구」(2015.11), pp.5~6.

39) 미래창조과학부 방송통신정책연구 15-진흥-033, 「사물인터넷 진흥 및 융합활성화를 위한 법제도 개선 연구」(2015.11), pp.5~6; 정원준, 앞의 논문, p.5

40) 사지연, 앞의 보고서, p.39; 이도국, “사물인터넷 환경에 있어 민사법적 문제점

“RFID 및 기타 센서를 일상 생활 속 사물에 탑재함으로써 사물인터넷이 구축될 것”이라고 언급하였다.<sup>41)</sup> 2005년 ITU의 보고서에서 모든 기기 및 사물에 근거리 및 원거리 통신 모듈이 탑재되면서 사물과 사람 간 또는 사물 간의 새로운 통신 유형이 등장할 것이라고 예측하였고, 특히 각종 ICT 기술의 진화로 모든 사물이 소형화 및 지능화되면서 사물인터넷 시대가 열릴 것이라고 전망했다.<sup>42)</sup> 이를 도식화하면 다음 그림과 같다.

〈그림 2-1〉 ITU가 제시하는 사물인터넷 시대의 사물 및 통신환경의 변화



출처: 한국인터넷진흥원 「인터넷 & 시큐리티 이슈」, 2012.9

사물인터넷은 기존의 유선통신 기반 인터넷 및 모바일 인터넷보다 진화된 단계의 인터넷을 의미한다. 초기 유선통신 시대에는 PC와 같은 사물간의 연결을 통해서만 데이터 교환이 가능했고 그 매개체로서 사람의 개입이 요구되었으나, 무선통신 기술의 발달로 사람과 사람, 사람과 사

에 대한 소고”, 한양법학 제26권 제2집(2015), p.222; 한국인터넷진흥원, 「인터넷&시큐리티 이슈」(2012.9), p.8 사지연은 Kevin Ashton이 처음 사용한 연도를 1998년으로 표시하고 있지만 다른 두 자료에서는 모두 1999년으로 기록하고 있어 본 보고서에서는 이에 따라 1999년으로 표기한다.

41) 한국인터넷진흥원, 앞의 보고서, p.8; 사지연, 앞의 보고서, p.38

42) 한국인터넷진흥원, 앞의 보고서, p.9

물, 사물과 사물 사이로 통신 가능 범위가 확대되고, 나아가 사물간의 자율적 통신도 가능한 사물지능통신(M2M)으로 발전하였다.<sup>43)</sup> 사물인터넷과 유사한 개념으로 인식되고 있는 M2M과 IoE(Internet of Everything)은 이러한 통신기술의 발전에 따라 네트워크를 통해 연결되는 범위가 확장되는 것을 의미한다.

사물통신에 관한 기술은 이동통신망을 통해 사물 간에 시간과 공간적 제약을 벗어나 안전하고 편리하게 통신하는 ‘사물지능통신(M2M)’ 개념에서 인터넷으로 영역을 확장하여 사물을 비롯한 현실과 가상세계의 모든 정보와 상호작용하는 ‘사물인터넷’ 개념으로 발전하였다.<sup>44)</sup> 따라서 M2M, IoT, IoE 등 세 개의 개념은 센서가 부착된 사물에서 발생한 정보를 네트워크에 연결하여 정보기반 서비스를 구현한다는 공통점이 있지만, 상호작용의 주체가 M2M은 사물과 사물, IoT는 사물과 사물만이 아니라 사람과 사물 간의 상호작용이 포함되며 IoE는 기기와 사람, 그리고 공간 및 환경 같은 모든 주체(everything)간의 상호작용까지 포함된다.<sup>45)</sup> 구체적으로는 IoT는 솔루션 중심의 서비스 지향적인 접근인데 반해, M2M은 디바이스 중심의 하드웨어적 접근으로 보아 접근방향의 차이가 있다.<sup>46)</sup> 일반적으로 M2M 기술은 IoT 구현을 위한 본질적인 기술요소로 간주되기 때문에, IoT 개념이 좀 더 광범위한 확장 개념으로 인식되고 있다.<sup>47)</sup> M2M을 통해 주요 구성 요소 간 센싱, 제어, 정보 교환 및 처리 등이 가능한 지능적 관계가 형성되어 서비스 형태로 변환되는데, 사물인터넷은 이러한 M2M의 개념이 무선통신을 넘어 인터넷 구조상에 적용됨으로써 현실과 가상 세계의 모든 정보와 상호작용하는

43) 한국인터넷진흥원, 앞의 보고서, p.10

44) 정원준, 앞의 논문, p.6

45) 사지연, 앞의 보고서, p.40

46) 정원준, 앞의 논문, p.6

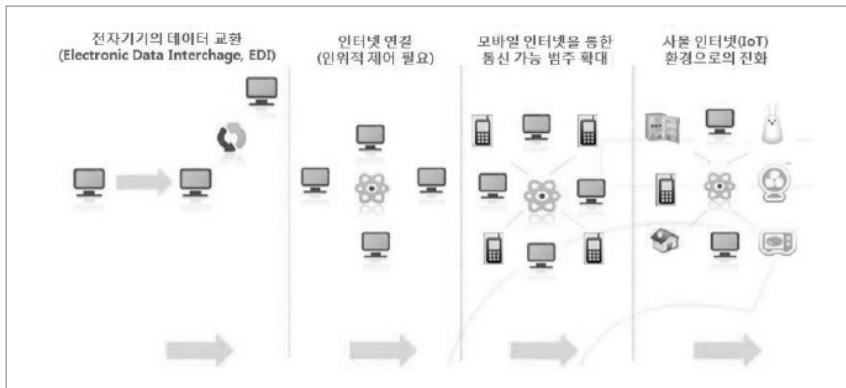
47) 정원준, 앞의 논문, p.6



개념으로 진화된 인터넷 환경을 의미한다.<sup>48)</sup>

하지만 후술하는 바와 같이 사물인터넷에 관한 다양한 정의는 상호작용의 주체를 사람과 사물, 사물과 사물에 한정하지 않고 사이버 공간과의 연결도 IoT의 개념에 포함하여 정의하고 있다. 이러한 측면에서 실질적으로 IoT와 IoE의 개념상 차이는 거의 의미가 없어 이를 구분하지 않고, IoT로 통칭하고 IoT가 궁극적으로 추구하는 방향이 IoE라고 하는 것이 더 타당한 설명일 것이다.<sup>49)</sup> 통신 환경의 발달에 따른 사물인터넷 개념의 등장을 도식화하면 아래의 그림과 같다.

〈그림 2-2〉 사물인터넷 개념의 진화



출처: 한국인터넷진흥원 「인터넷 & 시큐리티 이슈», 2012.9

48) 한국인터넷진흥원, 앞의 보고서, p.9

49) 같은 견해로 사지연, 앞의 보고서, p.41; 정원준, 앞의 논문, p.6. 사실 이런 측면에서 보면 M2M과 IoT의 구분도 의미가 없다는 주장이 가능하다. 하지만 본 보고서나 대부분의 관련 문헌에서 M2M과 IoT는 구분하고 있으며, 본 보고서도 이를 구분한다. 이러한 문제 발생의 원인은 M2M과 IoT, IoE를 상호 분절적인 것으로 보는 관점에서 발생한 것으로서 이들 상호 관계를 분절적인 것이 아닌 발달의 과정으로 인식할 필요가 있다.

### 3) 요약 및 소결

사물인터넷에 관한 이러한 다양한 정의가 사물인터넷 개념 정립에 있어서 일정한 장애요인이 되는 것이 사실이지만, 이들 여러 정의 사이에서도 일정한 공통분모가 분명히 존재하는 것도 사실이다. 이들 다양한 사물인터넷 정의의 공통적인 요소를 도출하면 대략적으로 ‘사물과 사물, 사람과 사물 등이 인터넷과의 네트워크 연결’, ‘센서를 통한 외부세계의 인식’, ‘데이터 송·수신을 통한 스스로의 작동이나 움직임’등으로 정리할 수 있다. 이러한 공통적인 개념요소를 관통하는 것은 사물과 사물, 사물과 사람, 사물과 사이버공간, 인터넷과의 연결과 자동화에 따른 스스로의 작동이다. 즉, 종래 인간의 개입을 통해서만 사물이 인터넷과 연결되고 작동되었다면, 사물인터넷 기술의 시대에는 사물이 스스로 인터넷과 연결되고 인간의 능동적인 개입이 없이도 스스로 데이터를 분석하여 작동한다는 것이다. 이는 결국 인터넷이란 통신서비스와 물리적인 대상인 사물이 연결되고 상호소통을 하고 그 결과를 인간의 개입 없이도 만들어 낸다는 것이다. 이를 통해 이전에는 생각할 수 없었던 새로운 서비스나 제품들이 가능해 지는 것이 사물인터넷 시대인 것이다. 다원적인 사물인터넷 개념의 이러한 공통요소를 바탕으로 사물인터넷을 정의한다면, 그것은 “사물과 사물, 사람과 사물이 인터넷과 연결되어 상호소통하고 센서를 통해 외부세계의 데이터를 인식하고 이를 사용하여 스스로 작동하는 정보통신 인프라”로 정의할 수 있을 것이다. 이러한 정의 외에도 다양한 정의가 가능하겠지만, 사물인터넷 개념에 있어서 핵심인 ‘연결성’, ‘외부세계에 대한 자율적 인식과 작동’을 필수적으로 포함하여 정의되어야 할 것이다.

이러한 사물인터넷 개념을 법적인 관점에서도 동일하게 정의할 수 있겠지만, 법제적 관점에서는 입법목적에 따라 일정한 변형이 가능할 것

이다. 다만, 이러한 경우에도 핵심요소는 포함되어야 한다. 국내 현행 법률 중에는 사물인터넷을 정의하고 있는 것은 없지만, 자치법규 중에는 사물인터넷을 규정하고 있는 조례가 3건이 있었다.<sup>50)</sup> 이 중 「서울특별시 사물인터넷도시 조성에 관한 조례」 제2조제1호는 “사물인터넷이란 정보통신기술을 기반으로 모든 사물을 연결하여 사람과 사물, 사물과 사물 간에 정보를 교류하고 상호 소통하는 지능형인프라 및 서비스 기술을 말한다.”고 규정하고 있다. 「서울특별시교육청 사물인터넷 기반 교육환경 조성 및 인재양성에 관한 조례」 제2조제1호도 동일한 정의를 사용하고 있다. 「경기도교육청 사물인터넷 구현을 위한 인재양성에 관한 조례」 제2조제1호는 “사물인터넷이란 인터넷 기반으로 모든 사물을 연결하여 사람과 사물, 사물과 사물 간의 정보를 상호 소통하는 지능형 기술 및 서비스를 말한다.”고 규정하고 있다.

그리고 실제 입법사례는 아니지만 정보통신법포럼이 수행한 예전 미래창조과학부 연구용역에서 ‘사물인터넷의 진흥에 관한 법률 제정 방안’을 마련했는데, 여기서 사물인터넷을 “인터넷을 통하여 사물정보를 수집하여 가공·저장·검색·송신·수신 및 활용하거나 사물을 관리 또는 제어하는 등의 방식으로 사물과 사물 또는 사람과 사물간에 통신하는 것을 말한다”고 정의하고 있다. 흥미로운 점은 이 제정 방안에서는 ‘사물인터넷’과 함께 ‘사물인터넷기반’<sup>51)</sup>과 ‘사물인터넷서비스’<sup>52)</sup>를 각각

50) 국가법령정보센터에서 ‘사물인터넷’ 검색어를 통해 검색한 결과이다. 3개 자치법규는 「경기도교육청 사물인터넷 구현을 위한 인재양성에 관한 조례」, 「서울특별시교육청 사물인터넷 기반 교육환경 조성 및 인재양성에 관한 조례」, 「서울특별시 사물인터넷도시 조성에 관한 조례」인데, 2개가 교육청 조례였고 1개가 집행기관 조례였다.

51) 사물인터넷기반이란 ‘사물인터넷이 가능하도록 계통적·유기적으로 연결·구성된 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호에 따른 정보통신망, 「전기통신사업법」 제2조제2호에 따른 전기통신설비, 인공위성자동위치측정시스템 등 위치측정·추적장치와 사물의 인식·분석기능을 가진 지능형 기기·설비등을 말한다’고 정의하고 있다.

52) 사물인터넷서비스란 ‘사물인터넷이 가능하도록 사물인터넷기반을 구축, 운영 또

별도로 정의하고 있다는 것이다.<sup>53)</sup> 이 외에도 ‘사물인터넷사업’과 ‘사물인터넷 사업자’ 등도 정의하고 있는데, 이는 사물인터넷의 산업적 진흥이 제안 법안의 입법목적 중 하나이기 때문인 것으로 보인다.

이러한 자치법규의 입법례와 연구자들의 입법제안에서도 상술한 바와 같은 사물인터넷의 개념의 핵심요소인 연결성, 자율적 의사결정과 작동 등은 반영되어 있다고 볼 것이다. 따라서 향후 사물인터넷 관련 법률제정이나 개정 단계에서도 개념정의에 있어서 핵심요소를 포함한 개념정의가 필요할 것이며, 이에 자치법규 등이 선례로 기능할 수 있을 것이다.

## 2. 소비자제품의 정의

### 1) 국내 입법례

소비자제품에 대한 현행 법령상 정의는 없다. 개별 법령에서는 해당 법령의 입법취지에 따라 다양한 형태의 용어를 사용하고 있고, 소비자제품이란 용어를 사용하고 있지는 않다.<sup>54)</sup> 국어사전에서도 ‘소비자제품’이란 단어를 별도의 개념으로 정의하고 있지 않으며, 관련된 것으로 ‘소비’와 ‘제품’ 등이 정의되어 있다. 일상적으로는 소비자제품이란 용어를 사용하지만 이에 대한 사전적인 정의가 없는 것이다. 현행 법령상으로 소비자제품에 해당하는 것을 가리키는 용어로는 ‘제품’이나 ‘용품’이

---

는 임대해주는 서비스’, ‘사물인터넷기반을 통하여 사물정보를 수집하여 가공·저장·검색 또는 분석하여 이용자에게 송신하거나 다른 사람에게 제공 또는 매개하는 서비스’, ‘제공받은 사물정보를 이용 또는 활용한 서비스’, ‘사물정보를 사물인터넷기반을 통하여 활용·응용하는 서비스’로 정의하고 있다.

53) 미래창조과학부 방송통신정책연구, 앞의 보고서, p.34

54) 국가법령정보센터에서 소비자제품이란 용어로 검색했을 때 이를 법령명칭으로 사용하고 있는 경우는 없었으며, 개별 조문에서도 이를 사용하고 있는 경우는 없었다.

사용되고 있는데, 개별 법률에 따라서 정의가 다소 차이가 있다.

「제품안전기본법」에서는 제품이란 “소비자가 최종으로 사용하는 물품 또는 그 부분품이나 부속품을 말한다.”고 정의하고 있다.<sup>55)</sup> 「전기용품 및 생활용품 안전관리법」은 ‘생활용품’이란 용어를 사용하는데, 이를 “공업적으로 생산된 물품으로서 별도의 가공(단순한 조립은 제외한다) 없이 소비자의 생활에 사용할 수 있는 제품이나 그 부분품 또는 부속품(전기용품은 제외한다)을 말한다”고 정의하고 있다.<sup>56)</sup> 또한, 동법에서는 ‘전기용품’이란 용어도 사용하고 있는데, 이를 “공업적으로 생산된 물품으로서 교류 전원 또는 직류 전원에 연결하여 사용되는 제품이나 그 부분품 또는 부속품을 말한다”고 정의하고 있다.<sup>57)</sup>

「화학물질의 등록 및 평가 등에 관한 법률」도 ‘제품’이란 용어를 사용하면서, 이를 “「소비자기본법」 제2조제1호에 따른 소비자가 사용하는 물품 또는 그 부분품이나 부속품으로서 소비자에게 화학물질의 노출을 유발할 가능성이 있는 다음 각 목의 것을 말한다”고 하면서 각 목에는 “혼합물로 이루어진 제품”, “화학물질이 사용 과정에서 유출되지 아니하고 특정한 고체 형태로 일정한 기능을 발휘하는 제품”이라고 규정하고 있다.<sup>58)</sup>

「어린이제품 안전 특별법」에서는 어린이제품이란 용어를 사용하면서 어린이제품을 “만 13세 이하의 어린이가 사용하거나 만 13세 이하의 어린이를 위하여 사용되는 물품 또는 그 부분품이나 부속품을 말한다”고 정의하고 있다.<sup>59)</sup> 다만, 여기서 제외되는 대상을 열거하고 있는데

55) 「제품안전기본법」 제3조제1호.

56) 「전기용품 및 생활용품 안전관리법」 제2조제2호.

57) 「전기용품 및 생활용품 안전관리법」 제2조제1호.

58) 「화학물질의 등록 및 평가 등에 관한 법률」 제2조제15호.

59) 「어린이제품 안전 특별법」 제2조제1호.

여기에는 “「약사법」 제2조에 따른 의약품 및 의약외품, 「의료기기법」 제2조제1항에 따른 의료기기, 「화장품법」 제2조제1호에 따른 화장품, 「식품위생법」 제2조제4호에 따른 기구 및 같은 조 제5호에 따른 용기·포장, 「관광진흥법」 제33조제1항에 따른 유기사설 또는 유기기구”가 있다.<sup>60)</sup>

「위생용품관리법」에서는 ‘위생용품’이란 용어를 사용하면서, 이를 “보건위생을 확보하기 위하여 특별한 위생관리가 필요한 용품”으로 정의하면서 이를 구체적으로 열거하고 있다.<sup>61)</sup> 여기에는 “세척제로서 ‘야채, 과일 등을 씻는데 사용되는 제제’, ‘식품의 용기나 가공기구, 조리기구 등을 씻는데 사용되는 제제’, “행굼보조제”, “위생물수건”, “기타 위생용품”<sup>62)</sup>이 포함된다.<sup>63)</sup>

한편, 이러한 개별 법률에서의 정의와는 다르게 소비자권익증진 및 정책을 위한 기본법인 「소비자기본법」에서는 ‘소비자’에 대한 정의조항은 있지만, 소비자제품에 대한 정의조항은 없으며, 동법에서는 소비자제품이 아닌 ‘물품’이란 용어를 사용하고 있다.<sup>64)</sup> 현행 법제에서의 소비자제품에 대한 이와 같은 다양한 정의를 고려하면서, 해외 주요국가의 소비자제품에 대한 정의를 살펴보도록 한다.

60) 「어린이제품 안전 특별법」 제2조제1호 각 목.

61) 「위생용품 관리법」 제2조제1호.

62) 여기에는 다시 “일회용 컵·숟가락·젓가락·포크·나이프·빨대”, “화장지, 일회용 행주·타월, 종이냅킨”, “일회용 이쑤시개·면봉·기저귀”, “그 밖에 대통령령으로 정하는 것”이 있다. 「위생용품 관리법」 제2조제1호라목 1)내지 4).

63) 「위생용품 관리법」 제2조제1호 각 목.

64) 물품이란 용어는 「소비자기본법」 제4조에서 최초로 등장하며 동법 전체에서 소비자가 사용하는 물리적 실체가 있는 제품을 가리키는 것으로 사용되며 대비되는 개념어로는 ‘용역’을 사용하고 있다.

## 2) 해외 주요 국가의 입법례

미국은 「소비자제품 안전법」(Consumer Product Safety Act, CPSA)<sup>65)</sup>에서 소비자제품을 정의하고 있다. 동법에서는 “소비자제품(Consumer Product)은 영구적이거나 일시적으로 가정이나 주택, 학교 또는 그 이외의 장소에서 사용하기 위하여 소비자에게 판매 또는 제공된 제품이나 그 부속품 또는 소비자가 개인적인 사용, 소비 혹은 여가를 위해 판매 또는 제공된 제품이나 그 부속품을 의미한다. 그러나 다음의 제품은 제외된다.”고 하여 상당히 넓게 소비자제품을 정의하면서 이에 대한 예외를 규정하고 있다.<sup>66)</sup> 예외로 열거되고 있는 제품에는 “관습상으로 소비자의 사용, 소비, 여가를 위해 제작 또는 공급되거나 판매되지 아니하는 모든 제품”, “담배 및 담배제품”, “자동차 또는 자동차 장비로서 전미교통 및 자동차안전법<sup>67)</sup>에서 정의한 것”, “연방살충살균 살서제법<sup>68)</sup>에 따른 살충제”, “내국세법<sup>69)</sup>에 따라 제조업자, 제조자, 또는 수입업자가 판매하는 경우 과세대상이 되는 모든 제품 또는 그런 제품의 부속품(화기 및 탄약)”, “항공기, 항공기엔진, 프로펠러 또는 장치로서 연방항공법<sup>70)</sup>에서 규정한 것”, “연방보트안전법<sup>71)</sup>에 따른 보트, 해양안전법률에 따른 선박 및 장치”, “연방식품, 의약품, 및 화장품법<sup>72)</sup>

65) 이 법은 1972년에 제정되었으며 소비자제품안전에 관한 전반적인 사항을 규정하고 있으며 동시에 소비자제품안전위원회(Consumer Product Safety Commission, CPSC)의 설립근거와 권한을 규정한 수권법(enabling act)이기도 하다. 이 법은 미국연방법전 Title 15 §§2051~2089로 편제되었다. 수권법률에 관한 상세한 설명은 Keith Werhan(2014), 「Principles of Administrative Law」, 2nd edition West Academic Publishing(2014)을 참조.

66) 15 U.S.C., §2052 (a)(5)

67) 49 U.S.C., §30102(a)(6), (7)

68) 7 U.S.C. §136

69) 26 U.S.C. §4181

70) 49 U.S.C. §40102 (a)

71) 46 U.S.C. §2101 (1)

72) 21 U.S.C. §321(g), (h), (l)

에 따른 약품, 의료기기, 화장품, 식품”이 포함된다.<sup>73)</sup>

일본의 경우에는 소비자제품의 안전에 관하여 「소비생활용품안전법」(消費生活用製品安全法)에서 규율하고 있다. 동법 제2조는 “이 법에서 소비자제품이라 함은 ‘주로 일반 소비자의 생활용으로 제공되는 제품(별표는 제외한다)’을 말한다”고 규정하고 있다. 소비자제품을 상당히 광범위하게 정의하면서 별표에서 제외되는 대상을 열거하고 있는 입법 형식을 취하고 있는 것이다. 별표에서 규정하고 있는 제외대상은 ‘선박 안전법제2조제1항의 적용대상인 선박’, ‘식품위생법제4조제1항의 식품 및 동조 제2항의 첨가물 및 동법 제62조의 세정제’, ‘소방법제21조제1항에 따른 기계기구 등 및 제21조의16에 규정하는 자율표시대상 기계 등’, ‘독극물규제법에 따른 독극물’, ‘도로운송차량법상의 도로운송차량’, ‘고압가스안전법의 용기’, ‘무기등제종법에 따른 엽총 등’, ‘약사법에 의한 의약품과 의약부외품 및 의료기기’, ‘다른 법령의 규정에 따라 기준을 정하여 그 제조, 수입 또는 판매를 규제하고 일반 소비자 생명 또는 신체에 대한 위해가 발생할 우려가 없다고 인정되는 제품으로서 정령으로 정하는 것’이 포함된다.<sup>74)</sup>

EU의 경우에는 일반제품안전지침에서 ‘소비자제품’을 정의하고 있다. 동 지침에서 소비자제품을 “소비자를 위해 제공되거나 또는 소비자를 위한 것은 아니지만 합리적으로 볼 때 소비자가 사용할 가능성이 높은 제품으로 신제품, 중고제품, 수리 및 개조한 제품 등 모든 제품”이라고 규정하고 있다.<sup>75)</sup>

73) 15 U.S.C., §2052 (a)(5)(A)~(I)

74) 「消費生活用製品安全法」 별표 각 호.

75) 지광석·김재영·김도년, 「소비자제품안전규제 개선방안 연구」, 한국소비자원(2017), p.23



### 3) 소결

소비자제품의 정의에 관한 이상의 입법례를 보면 입법방식에 있어서 소비자제품을 포괄적으로 정의하고 이에 대한 예외를 규정하는 방식이 주로 사용되고 있다는 점을 알 수 있다. 미국, 일본의 법제가 가장 대표적으로 이러한 범주에 해당될 것이지만, 현행 우리나라 법제에서도 제품이나 용품의 정의를 포괄적으로 하고 이에 대한 예외를 규정한 입법례가 있었다. 이러한 입법방식은 소비자제품이란 개념이 상당히 포괄적인 개념이기 때문에 이를 법률에서 정의할 때 최대한 넓게 정의한 후 이에 대한 예외를 두어 적용 대상을 한정하는 입법방식을 채택한 것으로 보인다. 다시 말해, 법상 소비자제품은 넓게 정의하고 법의 입법목적에 따라 개별 제품들을 적용대상에서 제외하는 방식이다.

소비자제품이 무엇인지에 대한 내용적 측면을 보면, 우리나라의 경우 용어상 ‘제품’이나 ‘용품’을 사용하고 있지만 대체적으로 ‘소비자가 최종적으로 사용하는 제품(물품)이나 그 부속품’을 의미하는 것으로 보인다. 미국이나 일본의 경우에도 대체적으로 이와 유사한 내용을 가지고 있다. 즉, 소비자가 최종적으로 사용 또는 소비하는 물리적인 제품을 소비자제품으로 정의하고 있다. 다만, 미국이나 일본의 법제에서는 소비자제품의 정의에 있어서 소비자가 사용하는 측면과 함께 해당 제품이 소비자에게 그러한 목적으로 판매 또는 제공되는 측면을 고려하여 개념을 정의하고 있다. 소비자가 주체가 되어 사용하는 제품이란 측면과 소비자에게 사용이나 소비의 목적으로 판매하기 위해 만들어지는 제품이란 수동적 측면을 모두 포괄하여 소비자제품을 정의하고 있는 것이다.

소비자제품이 소비자가 최종적으로 사용하기 위하여 구매하는 제품이란 측면과 함께 사용목적으로 소비자에게 판매하는 제품이란 측면이 공존하므로, 이를 모두 포괄하는 개념정의가 필요하다.

따라서 이러한 사항을 고려한다면 소비자제품은 “소비자가 최종적으로 사용이나 소비하는 제품 또는 이를 위하여 소비자에게 제공되는 제품이나 부속품”으로 정의할 수 있을 것이다.<sup>76)</sup>

### 3. IoT기반 소비자제품의 의의 및 종류

#### 1) IoT기반 소비자제품의 의의

상술한 바와 같이 사물인터넷과 소비자제품 각각의 개념으로 이해한다면, IoT기반 소비자제품이란 ‘사물인터넷을 활용한 소비자제품’으로 정의할 수 있을 것이다. 다시 말해, IoT기반 소비자제품은 “인터넷 또는 다른 네트워크와 직접 혹은 간접적으로 연결되어 소통하는 능력을 가진 소비자가 사용하거나 소비하는 또는 그러한 목적으로 소비자에게 판매나 제공되는 제품”이라고 정의할 수 있다.<sup>77)</sup> 사물인터넷을 통상적으로 산업적으로 활용되는 사물인터넷과 소비자제품에 사용되는 사물인터넷으로 구분할 수 있는데<sup>78)</sup>, 전자가 주로 사업장에서 제조공정의 효율성 제고를 위해 사용되거나 비즈니스 목적으로 사물인터넷을 활용하는 것이고 후자는 소비자제품에 사물인터넷을 활용하는 것이다. IoT기반 소비자제품이 바로 후자에 해당된다.

IoT기반 소비자제품은 사물인터넷 기술이 활용되었다는 점에서 일반 소비자제품과 구분되며, 소비자가 사용이나 소비하는 제품이란 점에서 생산과정의 효율성 제고 등을 위해 제조업자나 사업자가 사용하는 산업용 사물인터넷 기기와 차이가 있다고 할 것이다. 사물인터넷 기술이 사

76) 같은 견해, 지광석·김재영·김도년, 앞의 책, p.24.

77) CPSC, “Status Reports on the Internet of Things(IoT) and Consumer Product Safety”(2019, 10.25), p.6

78) CPSC, “Status Reports on the Internet of Things(IoT) and Consumer Product Safety”(2019, 10.25), p.6

용되었기 때문에 IoT기반 소비자제품은 사물, 사람, 사이버공간과 연결되며 외부세계의 데이터를 인식하고 처리하여 사용자인 소비자의 개입 없이도 스스로 작동할 수 있다. 또한, 인터넷이나 네트워크 연결을 통해 해당 제품을 소비자가 원격으로 조종하여 작동시킬 수 있다.

## 2) IoT기반 소비자제품의 종류

사물인터넷 기술은 다양한 영역과 제품에 활용될 수 있기 때문에 IoT기반 소비자제품은 광범위한 제품을 포함할 수 있다. 미국의 CPSC는 IoT기반 소비자제품을 몇 가지 범주로 구분했는데, 여기에는 i) IoT와 연결된 어린이 장난감 및 아기 모니터, ii) 연기감식기나 도어락 같은 안전관련 연결된 제품, iii) 스마트 또는 보안 카메라, TV 및 스피커, iv) 웨어러블 헬스 트랙커 및 의류, v) 웨어러블 스마트 의류, vi) 연결된 홈 자동화 및 알람 시스템, vii) 연결된 가전제품(예를 들어, 세탁기, 냉장고), viii) 스마트 홈 도우미 등이 포함되어있다.<sup>79)</sup> OECD의 경우에도 IoT기반 소비자제품의 범주를 대략적으로 구분하고 있는데, 여기에는 i) 웨어러블, 헬스 모니터, 및 이식할 수 있는(implantable) 기기, ii) 스마트 홈 장비, iii) 장난감 및 아이돌봄 장비, iv) IoT와 연결된 자동차가 포함된다.<sup>80)</sup> 미국의 CPSC는 수권법률인 CPSA에서 소비자제품을 정의할 때 자동차가 제외되기 때문에 사물인터넷을 활용한 자동차를 IoT기반 소비자제품에 포함시키지 않았지만, OECD의 경우에는 이를 포함시켜 범주화한 것으로 보인다. OECD는 이러한 IoT기반 소비자제품의 범주 중에서도 웨어러블 기기 등 첫 번째 범주와 스마트 홈 케어

79) CPSC, "Status Reports on the Internet of Things(IoT) and Consumer Product Safety"(2019, 10.25), p.6

80) OECD, 「Consumer Product Safety in the Internet of Things」, OECD Digital Economy Papers(2018) No.267, p.9

등이 포함된 두 번째 범주에 해당되는 제품이 IoT기반 소비자제품 전체에서 차지하는 비중이 크다는 점을 지적하고 있다.<sup>81)</sup>

한편, 우리나라의 경우 국내 사물인터넷 공급사업체에 대한 체계적인 조사·분석을 통해 정부 정책 수립 및 기업 경영에 필요한 기초 통계자료를 제공하여 사물인터넷 산업의 기반 조성 및 경쟁력 강화에 기여하기 위하여 사물인터넷 산업 실태조사를 수행하고 있다.<sup>82)</sup> 이 조사에서 사물인터넷을 활용한 서비스와 제품을 분류하고 있다. 먼저, 사물인터넷 서비스는 i) 헬스케어/의료/복지, ii) 에너지 검침/관리, iii) 제조, iv) 스마트 홈/오피스, v) 금융/교육/국방, vi) 농림축산/수산, vii) 자동차/교통/항공/우주/조선, viii) 관광/스포츠, ix) 소매/물류, x) 건설·시설물관리/안전/환경 등으로 분류하고 있다.<sup>83)</sup> 각 사물인터넷 서비스 활용 분야의 주요 내용은 다음의 그림과 같다.

81) OECD, 「Consumer Product Safety in the Internet of Things」, OECD Digital Economy Papers(2018) No.267, pp.9~10

82) 과학기술정보통신부·정보통신산업진흥원·한국사물인터넷협회, 「2018년도 사물인터넷 산업 실태조사」

83) 한국사물인터넷협회, 「2018 상·하반기 사물인터넷 제품 및 서비스 편람」

〈그림 2-3〉 사물인터넷 서비스 활용분야

활용 분야		주요 내용
헬스케어/ 의료/복지	헬스케어	○ 운동량 관리 서비스, 수면관리 서비스 등
	의료	○ 의약품 및 의료기기 관리 서비스, 환자상태 모니터링 서비스, 원격 검진 서비스 등
	복지	○ 취약계층(독거 치매노인, 여성, 장애인 등) 서비스, 사회복지시설(요양원 등) 서비스, 미아방지 서비스, 여성 안심서비스 등
에너지/검침	검침	○ 전기가수수도 등 원격 검침 서비스, 실시간 과금 서비스 등
	에너지 관리	○ 에너지 모니터링 서비스, 건물 에너지 관리 서비스, 전력/전원 모니터링 및 제어 서비스, 신재생 에너지(태양광 등) 관리 서비스 등
제조		○ 생산 공정관리 서비스, 기계진단 서비스, 공장 자동화서비스, 제조설비 실시간 모니터링 서비스 등
스마트홈		○ 가전기기 원격제어 서비스, 홈CCTV 서비스, 스마트도어락 서비스, 안공지능 서비스 (음성인식 비서) 등
금융		○ IoT기반 동산 담보 관리 서비스, 비콘 기반 금융 상품 안내 및 고객 서비스
교육		○ 스마트 스쿨(출결관리, 교육 기자재관리 등) 서비스, 스마트 도서관 서비스 등
국방		○ 훈련병 예비군 관리 서비스, 전장감시 및 부대방호 서비스, 총기 및 탄약 관리서비스, 테러감지 서비스, 광섬유 군복 등
농림축산/ 수산	농림축산	○ 재배환경 모니터링 및 관리 서비스, 사육관리 서비스, 사료 자동 급이 서비스, 농산물 유통관리 서비스, 생산이력 관리 서비스, 가축 이력 추적 서비스, 가축 전염병(구제역 등) 관리 서비스 등
	수산	○ 양식장 환경 정보 수집 서비스, 수산물 이력관리 서비스 등
자동차/교통/ 항공/우주/ 조선	자동차	○ 차량 진단서비스(DTG, OBD), 커넥티드 카, 무인 자율주행 서비스 등
	교통/인프라	○ ITS, 대중교통 운영정보 관리(버스사령관제 등)서비스, 스마트 파킹 서비스, 주차위치 제공 서비스, 주변 주차장 안내 서비스, 아파트 차량 출입통제 및 주차관리 서비스, 철도시설 관리 서비스 등
	항공/우주	○ 비행기 내부 모니터링 서비스, 실시간 항공기 원격점검 서비스 등
	조선/선박	○ 선박 위치 모니터링, 선박 내부 모니터링, 선박 원격점검 서비스 등
관광/스포츠	관광	○ 관광지 위치정보 서비스, 관광/문화행사 정보 수집/제공 서비스, IoT 기반 문화유산 관광 안내 서비스 등
	스포츠/레저/ 오락	○ 운동선수 관리(운동량 체크 등) 서비스, 스포츠 장비 관리 서비스, 경기장내 위치정보 서비스 등
소매/물류	소매	○ 지능형 쇼핑고객 관리 서비스, 실시간 재고관리 서비스, 운송추적 서비스, 비콘기반 O2O 서비스 등
	물류/유통	○ 상품 위치정보 모니터링 서비스, 물류창고 관리 서비스, 조달관리 서비스, 물류추적 서비스 등
건설-시설물 관리/안전/ 환경	건설/ 시설물관리	○ 구조물 안전관리 서비스, 공공시설물 제어서비스, 빌딩 관리서비스, 출입 통제서비스, 시설물 감시서비스, 도로/교량 상태 모니터링 서비스 등 ※ 건물 및 빌딩의 에너지 관리 서비스는 "에너지 분야"의 에너지 관리 서비스에 포함 ※ 건물 내 주차장 관리 및 주차관리 서비스는 "자동차/교통/항공/우주 분야"의 교통인프라 서비스에 포함
	산업 안전	○ 유해화학물 관리, 재해 모니터링, 위험물 감지-경보 서비스 등
	환경/재난/ 재해	○ 수질관리, 기상정보 수집/제공, 음식물쓰레기 관리, 스마트 환경정보 제공, 재난재해 감시(홍수, 지진 등) 서비스

출처: 「2018년도 사물인터넷 산업 실태조사 보고서」

다음으로, 사물인터넷 제품에 관하여는 크게 플랫폼, 제품기기, 보안으로 대분류를 하고 각 범주를 다시 하위 범주로 세분하고 있다.

이에 관하여 보면, 우선 플랫폼은 i) 소프트웨어 플랫폼, ii) 플랫폼 장비로 세분하고 있다. 제품기기는 i) 스마트 기기용 칩셋, ii) 스마트 기기용 모듈, iii) 스마트 카드/태그, iv) 스마트 단말기기, v) 게이트웨이(무선통신, 유선통신, 음성인식 게이트웨이), vi) 교육용 장비, vii) 태그프린터, viii) 리더<sup>84)</sup>로 세분하고 있다. 보안제품은 IoT관련 보안 제품 및 서비스로서 서비스, 기기, 플랫폼으로 세분하고 있다.<sup>85)</sup>

한국사물인터넷협회의 이러한 사물인터넷 서비스 및 제품의 분류는 서비스와 제품의 사용용도를 중심으로 분류하여 IoT기반 소비자제품을 고려한 분류는 아니다. 따라서 이러한 분류체계를 다시 소비자가 사용이나 소비를 위한 제품이란 척도를 통해 다시 살펴보아야 하는데, 대체적으로 CPSC와 OECD의 분류와 중복된다. 즉, 소비를 위한 제품이나 소비를 위하여 판매되는 것이므로 제조과정 등 산업용으로 사용되는 제품이나 서비스와 공공서비스를 위해 제공되는 것을 제외하면 웨어러블 기기(스마트 헬스케어 기기 포함), 스마트 홈 및 오피스, 안전관리 서비스 등으로 분류할 수 있을 것이다.

84) 스마트 카드/태그와 연결되어 수집된 정보를 통신망에 연결하는 제품기기

85) 이상의 사물인터넷 제품 분류는 한국사물인터넷협회, 「2018 상·하반기 사물인터넷 제품 및 서비스 편람」을 참고

## 제2절 | IoT기반 소비자제품의 특성 및 현황

### 1. IoT기반 소비자제품의 특성 및 이슈

#### 1) IoT기반 소비자제품의 특성

IoT기반 소비자제품이 가지는 특성은 사물인터넷을 활용한 이점에 있다. 사물인터넷 기술이 사물과 사물, 사람과 사물, 사물과 인터넷과의 연결을 통해 종래 소비자제품이 제공할 수 없었던 여러 이점을 제공하고, 이는 IoT기반 소비자제품만이 가지는 특성을 구성하기도 한다. 사실 IoT기반 소비자제품이 제공하는 이점을 누리는 주체가 소비자에 한정되지는 않는다. 사업자도 이를 누릴 수 있다. 기술 자체는 소비자와 사업자 모두에 있어서 중립적이기 때문에 사물인터넷 기술이 소비자만이 아니라 사업자에게도 고유의 특성이 반영된 이점을 제공할 수 있게 된다.

IoT기반 소비자제품은 잠재적으로 여러 중요한 이점을 제공해주고 있는데, 여기에는 소비자제품의 안전성을 높이고 위해요인에 대한 효과적인 관리를 통하여 소비자보호를 제고하는 것도 포함된다. 가장 분명한 이점은 IoT기반 소비자제품이 소비자의 삶을 더 편하고 안전하게 만든다는 것이다. 이는 사물인터넷 기술이 소비자후생에 기여함과 동시에 안전성 수준까지도 향상시킨다는 것을 의미한다. 또한, IoT기반 소비자제품은 소비자 개개인의 경제적 효율성만이 아니라 사회 전체적으로도 자원의 효율적 배분을 통해 지속가능성을 제고할 수 있다는 것이다.

예를 들어, IoT 기반 소비자제품 중 네트워크와 연결된 온도조절장치는 소비자가 원격으로 자신의 집의 실내온도 등 환경을 통제하도록 하여, 자신이 부재중 일 때 불필요한 에너지 소비를 절감시킨다. 이것은

소비자 입장에서 낮은 에너지 비용청구서를 통한 경제적 이익을 누리고 동시에 사회적인 차원에서 낭비되는 에너지 자원을 절약함으로써 자원의 효율적 배분을 이룰 수 있어 사회 전체적으로도 이익이 된다. 게다가 제조업자가 IoT기반 소비자제품을 원격으로 제어할 수 있다. 이것이 의미하는 것은 해당 제품이 소비자에게로 이전된 후에도 잠재적으로 업그레이드가 가능하다는 것을 의미한다. 이러한 측면에서 위 사례를 다시 보면 IoT 기반 온도조절장치는 성능개선이 가능하고 심지어 소비자의 집에서 해당 제품의 존속기한 전체에 걸쳐서 전체적으로 새로운 특성을 가질 수 있게 된다.<sup>86)</sup>

IoT 기반 소비자제품은 잠재적으로 이를 사용하는 소비자를 더 안전하게 만들 수도 있다. IoT가 가지는 연결된 존재라는 특성은 해당 제품의 작동과정에서 하자 등의 문제가 발생한 경우 책임 있는 당사자에게 이러한 불안정한 상태를 네트워크를 통해 손쉽게 알릴 수 있다. 즉, 해당 제품의 하자로 인한 사고가 발생하기 이전에 이를 방지할 수 있는 기회를 제조업자 등 해당 제품의 안전성에 관한 책임주체에게 제공하는 것이다. 이를 통하여 제조업자 등은 해당 제품에 대한 시정조치를 취할 수 있고 결과적으로 소비자의 안전한 제품이용이 가능해 지는 것이다. 만일 제품의 문제가 심각하고 원격으로 바로잡을 수 없는 것이라면, 제조업자는 적절한 시기와 효율적인 방식으로 리콜을 시행할 수도 있다. 따라서 위의 예시에서, IoT 기반 온도조절장치는 제조업자나 해당 문제에 관한 제3자에 의하여 원격으로 모니터링이 가능하다. 그 후 만일 문제가 발생한다면, 소비자는 즉각적으로 해당 쟁점을 통지 받을 수 있고 만일 필요하고 가능하다면, 장비의 소프트웨어가 업데이트 되거나 패치

86) OECD (2016), "The Internet of Things: Seizing the Benefits and Addressing the Challenges", OECD Digital Economy Papers, No.252



될 수 있다. 그리고 만일 온도조절장치가 원격으로 수리될 수 없다면, 해당 제품은 리콜될 것이다.

소비자안전에 관하여 다른 예를 들면, 자동차 시트센서가 블루투스를 통해 사용자와 연결되어 있는 상황을 가정해 볼 수 있다. 이 제품은 스마트폰을 통한 경고표시를 통해 부모가 자신들의 자동차 안에 아이들을 두고 떠나지 못하도록 예방할 수 있다. 이처럼 사물인터넷을 활용한 소비자제품은 이를 이용하는 소비자와 주변인을 보다 더 안전하게 만드는 이점을 제공한다.

제조업자들은 역시 사물인터넷 기술을 사용하여 공급사슬 속 자신의 제품을 추적할 수 있는 이점을 누릴 수 있다. 일반적으로 제조업자는 자신의 공급사슬에서의 위험을 확인하고 이를 감소시킬 수 있고, 이에 따라 사전에 자신들의 장래 원재료 및 공급량 또는 산출량에서 제품손실이나 생산 지연에 따라 손해가 발생하는 상황을 회피할 수 있다. 제조업자는 또한 공급사슬에서 블록체인 기술 및 관련된 “스마트 계약”을 통하여 개별 제품이나 제품군을 추적할 수 있고, 이를 통하여 해당 제품이 관련 규제요건을 준수하도록 만들거나 제품이 배송되었을 때 자동적으로 대가를 수령할 수 있도록 만들 수 있다.<sup>87)</sup> 여기서 “스마트 계약 (smart contract)”란 협상된 조건이 충족되었을 때 특정 행위(예를 들어 금전의 지급·수령 등)가 개시되도록 하는 것을 말한다.<sup>88)</sup> 예를 들어,

87) Iansiti, M. and K. Lakhani(2017), The Truth About Blockchain, Harvard Business Review.

88) 추가적으로 설명하면, 스마트 계약은 계약조건을 실행하는 컴퓨터 트랜잭션 프로토콜을 뜻한다. 블록체인 기술을 기반으로 계약 조건을 거래 당사자가 코딩하고, 거래조건에 부합하는 경우 계약이 내용대로 이행되는 디지털 계약방식이다. 이는 일종의 ‘자동화 계약’ 시스템으로서 블록체인 등의 등장에 따라 최근에 현실화되고 있다. 스마트 계약은 거래비용을 절감시킬 수 있어 거래당사자 모두에게 이익을 제공하며, 사물인터넷과의 결합을 통해 활용도를 높일 수 있다. 이상의 설명은 ‘네이버캐스트 용어로 보는 IT 스마트 계약’의 내용을 필자가 정리한 것이다. <https://terms.naver.com/entry.nhn?docId=4395278&cid=59088&>

만약 “스마트 계약”이 IoT와 연결되어 있는 제품의 일정량을 배송 받은 경우 대금이 지급되도록 체결되었다면, 제조업자는 IoT를 사용하여 계약 대상인 제품이 구매자가 거주하는 지역의 관련 규제를 준수하는지를 확인하고, 직접 그것을 적절한 위치로 배송한 후 구매자가 해당 제품을 수령하기 위해 블록체인에 로그인 할 때 계약대금을 자동적으로 지급받을 수 있을 것이다. 이처럼 사물인터넷과 스마트 계약을 활용함으로써, 제조업자는 지역의 법령을 지키고 동시에 자신의 사업을 진행하는 과정에서 종래에는 필수적인 비용으로 소모되었던 거래비용을 절감하거나 사용하지 않을 수도 있게 된다. 여기서 거래비용은 전통적인 사업구조에서 거래의 과정에서 중개업무 등에 따라 소요되는 회계사 및 변호사 사용 비용 등을 의미한다. 사실 스마트 계약이 사물인터넷과 연계되는 경우 제조업자만이 아니라 소비자에게도 적지 않은 이점을 제공할 수 있다. 예를 들어, 특정 보험금 청구 등에 있어서 보험사가 스마트 계약을 통해 보험금청구를 받고 의료기관 등과 소비자가 보유한 스마트폰 등이 네트워킹 되어 있는 경우 소비자는 진료 후 별도의 청구 없이도 보험의 대상에 해당하는 진료라면 의료비를 보전 받을 수 있다.<sup>89)</sup>

## 2) IoT기반 소비자제품 관련 이슈

IoT기반 소비자제품이 가지는 이러한 잠재적인 이점은 동시에 문제점으로 작용할 수도 있다. 미국의 CPSC는 사물인터넷 기반 소비자제품에 관련하여 몇 가지 우려사항을 지적하고 있었다.<sup>90)</sup> 첫 번째는 원격으

categoryId=59096

89) 이 사례는 현대자동차그룹 블로그 중 “계약 조건을 입력하면 블록체인이 실행한다! 디지털 자판기, ‘스마트계약’을 참조하여 필자가 재구성한 것이다. <https://m.post.naver.com/viewer/postView.nhn?volumeNo=26597628&memberNo=3901450&vType=VERTICAL>

90) CPSC, Status Report on the Internet of Things(IoT) and Consumer

로 작동되는 경우 위해할 수 있는 제품에서 원격제어가 문제의 원인이 될 수 있다는 것이다. 예를 들어, 가스 그릴이나 히터와 같은 제품이 원격으로 제어되어 잠재적인 화재 및 일산화탄소 중독 위험을 노출시키는 경우가 있다.

두 번째는 구매 후 소비자제품이 위해한 제품이 될 수 있다는 점이다. 판매 시점에는 불합리한 위해 리스크를 가지지 않았던 소비자제품이 무권한 접근, 침해, 비정상적인 데이터 전송 간섭, 운영코드 조작 또는 소비자-지향적인 데이터가 그 전에는 없었던 안전성 위험을 창출하는 등 위해요인을 가지게 될 수 있다. 예를 들어, 연결된 가스레인지가 온도제한 기능이 작동 불가능하도록 소프트웨어 업데이트가 되는 경우를 생각할 수 있다.

세 번째는 안전장치가 작동불능 되도록 만드는 경우가 있다. 이는 제품의 소프트웨어 또는 제품과 연결된 장비를 변경하는 것이 안전장치가 작동되지 않는 원인이 될 수 있다. 예를 들어, 홈 보안 시스템과 연결된 소프트웨어 업데이트가 집주인의 인식 없이 연기 또는 일산화탄소 경보기 작동불능을 야기할 수 있다.

네 번째로 중대한 데이터 보안 및 안전기능에 관하여 소비자가 명확히 인식하지 못할 수 있다는 것이다. 소비자는 사물인터넷 기기가 소프트웨어 업데이트 종료로 인하여 더 이상 안전하게 사용할 수 없을 시기에 관하여 명확히 인식할 필요가 있다.<sup>91)</sup>

IoT기반 소비자제품에 관한 이러한 이슈제기는 사물인터넷 기술이 가지는 연결성, 원격조종가능성 등의 장점이 오히려 단점으로 작용할 수 있다는 것이다. 또한 IoT기반 소비자제품의 이러한 잠재적인 문제가

Product Safety(2019.10.25.), p.7

91) CPSC, Status Report on the Internet of Things(IoT) and Consumer Product Safety(2019.10.25.), p.7

소비자안전에 위해요인이 될 수 있다는 것을 의미한다.<sup>92)</sup> 이는 사물인터넷이 가지는 기술적 장점이 문제의 원인으로 작동하는 것이기 때문에 IoT기반 소비자제품의 특성으로 볼 수도 있을 것이다.

종래 IoT기반 소비자제품에 관한 이슈로는 주로 보안문제가 핵심이었다. 사물인터넷이 가지는 인터넷, 네트워크와의 연결이 외부의 원인에 의하여 침해되는 사태는 해당 제품의 중요기능이 훼손되는 상태이기 때문에, IoT기반 소비자제품에서 보안이 주요 쟁점이 되었던 것이다. 하지만 앞서 언급한 IoT기반 소비자제품에서 제기되는 문제는 연결성이란 사물인터넷 기술의 핵심이 소비자의 안전문제로 제기될 수 있다는 것을 내포하고 있다. 따라서 IoT기반 소비자제품은 자신의 특성인 연결성에 따라 디지털 환경의 일부인데, 이것이 의미하는 것은 데이터 보안 리스크 관리가 소비자제품 안전성의 일부라는 것이다.<sup>93)</sup> 결국 IoT기반 소비자제품에서 보안문제와 제품안전 문제가 중첩되어 있고, 보안문제를 다루는 것에 제품의 위해요인도 다루어져야 하고 그 반대도 필요하다는 것이다. CPSC가 보안에 관한 법적 관할권을 가지고 있지 않지만, IoT기반 소비자제품의 안전성과 관련한 데이터 변형이나 조작에 관하여는 관할권을 주장하고 있는 상황을 주목할 필요가 있다.<sup>94)</sup>

92) IoT기반 소비자제품의 위해요인이 이러한 문제에서 발생하게 된다.

93) CPSC, Status Report on the Internet of Things(IoT) and Consumer Product Safety(2019.10.25.), p.8

94) CPSC, Status Report on the Internet of Things(IoT) and Consumer Product Safety(2019.10.25.), p.9

## 2. IoT 제품시장 현황

### 1) 세계 IoT시장 현황

사물인터넷 개념 정의를 다른 부분에서 살펴보았듯이, 사물인터넷에 관한 합의된 국제적인 정의가 없기 때문에 사물인터넷 기술을 활용한 제품 및 서비스 시장의 현황에 대한 평가도 기관 마다 차이가 있다.<sup>95)</sup> 여기에 더하여 IoT기반 소비자제품에 관하여도 명확한 기준이 부재한 상황이고 IoT기반 소비자제품만을 대상으로 한 시장현황에 대한 조사·분석은 없다. 이는 대체로 사물인터넷 시장 규모 등을 평가할 때 전체로서 평가하며 특정 제품군으로 분류하여 다루는 경우가 없기 때문이다. 다만, 사물인터넷을 활용한 제품과 서비스를 구분하여 시장현황을 조사·분석하기 때문에, 사물인터넷 제품에 대한 시장현황 자료를 통하여 간접적으로 IoT기반 소비자제품 시장현황을 살펴볼 수 있을 것이다.<sup>96)</sup>

OECD의 자료에 따르면 2012년에서 2016년말 까지 M2M SIM카드가 사용된 총 숫자가 72백만 개에서 149백만 개로 증가했다.<sup>97)</sup> 서론에서도 언급했듯이, 2015년 자료에서 전 세계 사물인터넷 기기는 363백만 개가 있고 이 중 84백만개가 중국, 78백만 개가 미국, 18백만 개가 한국, 브라질, 및 독일이었고 8-10백만 개 사이에 일본, 스페인, 영국 및 멕시코가 있다.<sup>98)</sup>

유럽집행위원회(EC)는 유럽연합 회원국 내에 사물인터넷 제품의 숫자가 2013년 18억 개에서 2020년에는 대략 60억 개로 증가할 것으로 예측하였다.<sup>99)</sup> Cisco의 프로젝트에 따르면 모바일 기기 및 사물인터넷

95) 같은 견해로 OECD, 「Consumer Product Safety in the Internet of Things」, OECD digital economy papers March 2018 No.267

96) 사물인터넷 제품에는 산업용 사물인터넷 제품이 포함되기 때문이다.

97) OECD, 「OECD Digital Economy Outlook 2017」, OECD Publishing Paris

98) OECD, 「OECD Digital Economy Outlook 2015」, OECD Publishing Paris

제품 숫자가 2021년 까지 116억 개로 증가할 것이고, 이 중 개인용 모바일 기기 또는 휴대용 기기가 83억 개, M2M 연결 기기가 33억 개일 것으로 예측되었다.<sup>100)</sup>

Ericsson은 전 세계 인터넷 연결 제품 숫자가 2016년 160억 개에서 2022년에는 290억 개로 증가할 것으로 예측하였는데, 여기에는 자동차, 기계, 센서 등이 포함되었다.<sup>101)</sup> 미국의 CPSC도 최근 보고서에서 인터넷과 연결된 제품시장이 지속적으로 팽창할 것으로 전망하면서, 2025년까지 2018년 대비 6.4배가 증가한 약 640억 개 제품이 전 세계적으로 사용될 것으로 예측했다.<sup>102)</sup>

한편, 사물인터넷 시장의 규모에 관하여도 여러 기관별로 차이가 있지만 지속적인 성장과 규모의 확대를 설명하고 있다. McKinsey는 2015년 사물인터넷 시장이 9억 달러였지만 2020년에는 37억 달러로 성장할 것으로 전망했다.<sup>103)</sup> 또한 McKinsey는 정책입안자와 기업인들이 이 기술적, 규제적인 장애물을 극복한다면, 이러한 사물인터넷 시장규모의 성장세가 잠재적으로 미치는 경제적 파급효과를 2025년까지 11.1조에 이를 것으로 예측했다.<sup>104)</sup>

ICT분야 시장분석 전문기관인 IDC자료를 바탕으로 한 소프트웨어정책연구소 자료에서는 최근 세계 사물인터넷 시장 규모가 2018년

99) Cartwright, J., Product liability and the internet of things, in Charles Russell Speechlys (2017)

100) Cisco, Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update(2016)

101) Ericsson, Ericsson Mobility Report (2107).

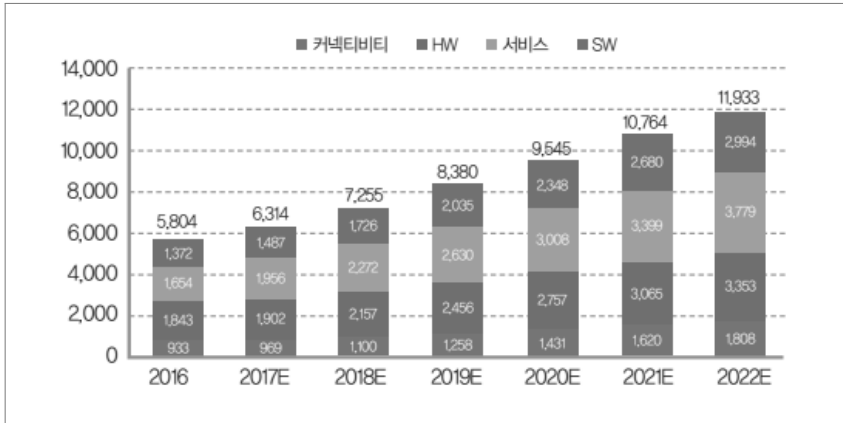
102) Peter Newman, The Internet of Things 2019 Report: How the IoT Continues to Transform Business, Homes, and Cities Through Next Generation Digital Solutions, Bus. Insider Intelligence (January 2019).

103) McKinsey, Internet of Things: The IoT opportunity- Are you ready to capture a once-in-a-lifetime value pool? (2016)

104) McKinsey, Unlocking the potential of the Internet of Things (2015)

7,255억 달러로 전년 대비 14.9% 성장했으며, 2016~2022년까지 연평균 12.8% 성장하면서 1조 1,933억 달러에 달할 것으로 전망하고 있다.<sup>105)</sup> 사물인터넷 시장 중 서비스 시장이 2018년 2,272억 달러로 전체 시장의 31.3%를 차지하고 있으며, HW시장이 2,157억 달러로 29.7%, SW시장이 1,726억 달러로 23.8%, 커넥티비티 시장이 1,100억 달러로 13.5%를 차지하고 있다. 2016~2022년 연평균 성장률은 서비스 시장이 14.8%로 가장 높고, SW시장 13.9%, 커넥티비티 시장 11.7%, HW 시장 10.5% 순으로 성장률을 기록할 것으로 전망되고 있다.<sup>106)</sup> 2016~2022년도 별 커넥티비티, HW, 서비스, SW 분야 각각의 시장 규모 및 성장 추이에 대하여는 다음의 그림과 같을 것으로 예상되고 있다.

〈그림 2-4〉 사물인터넷 분야별 시장규모(2016~2022)



출처: 소프트웨어정책연구소, 월간 SW중심사회(2019.1)

105) 소프트웨어정책연구소, “사물인터넷 시장 및 주요 기업 동향”, 월간 SW중심사회(2019.1)

106) 소프트웨어정책연구소, “사물인터넷 시장 및 주요 기업 동향”, 월간 SW중심사회(2019.1)

IDC의 고객 인사이트 및 분석(Customer Insight & Analysis) 담당자인 마커스 토치아 리서치 디렉터는 “소비자의 IoT 지출은 2019년에 1,080억 달러에 달해 두 번째로 큰 지출을 차지할 전망이다. 주요 소비자 사용 사례는 스마트 홈, 개인 건강 및 커넥티드카 인포테인먼트와 연관될 것”이라며 “2018~2022년 기간 동안 스마트 홈에서는 가정 자동화와 스마트 가전이 5년간 연평균성장률 17.8%로 가장 빠른 소비 성장을 보인다.”고 전망했다.<sup>107)</sup>

IDC는 2019년 가장 큰 투자가 예상되는 IoT 활용사례는 제조운영(1,000억 달러), 생산자재관리(442억 달러), 스마트 홈(441억 달러), 활물 모니터링(419억 달러)부문에서 주도할 것으로 전망했다.<sup>108)</sup> 지역별 2019년 사물인터넷 지출규모는 미국과 중국이 각각 1,940억 달러, 1,820억 달러로 가장 큰 시장이 될 전망이었다. 이어서 일본 654억 달러, 독일 355억 달러, 한국 257억 달러, 프랑스 256억 달러, 영국 255억 달러 규모로 예상하고 있다.<sup>109)</sup>

## 2) 국내 사물인터넷 산업 현황

국내 사물인터넷 산업의 현황에 관하여는 2014년부터 매년 실시하고 있는 사물인터넷 산업 실태조사 결과를 통해 살펴볼 수 있다. 2018년도 실태조사는 사물인터넷 사업 영위가 확인된 2,204개사(2017년에는 2,118사)를 대상으로 실시되었으며, 이 중에서 498개사가 조사에 응답하였다.<sup>110)</sup> 이하에서는 2018년도 실태조사 결과를 바탕으로 사물인터넷

107) IDC, 한국 IDC, 전 세계 사물인터넷(IoT) 지출규모 2019년 7450억 달러 전망  
<https://www.idc.com/getdoc.jsp?containerId=prAP44660819>

108) IDC, 한국 IDC, 전 세계 사물인터넷(IoT) 지출규모 2019년 7450억 달러 전망  
<https://www.idc.com/getdoc.jsp?containerId=prAP44660819>

109) IDC, 한국 IDC, 전 세계 사물인터넷(IoT) 지출규모 2019년 7450억 달러 전망  
<https://www.idc.com/getdoc.jsp?containerId=prAP44660819>



넷 산업의 현황을 살펴보도록 한다.

국내의 사물인터넷 사업을 영위하는 사업체 수는 2018년 9월 기준 2,204개사이고 서비스 분야 사업체가 1,191개사(54.0%)로 가장 많았고, 다음으로 제품기기, 플랫폼, 네트워크 순으로 다음 표와 같다.<sup>111)</sup>

〈표 2-1〉 사업 분야별 사물인터넷 사업체 수

(단위: 개사, %)

구분	합계	플랫폼	네트워크	제품기기	서비스
사업체 수	2,204	406	129	478	1,191
비율	100.0	18.4	5.9	21.7	54.0

출처: 2018년도 사물인터넷 산업 실태조사

사업체 종사자 규모별로는 10인 이상~ 49인 이하 사업체가 1,008개사로 가장 많았고, 다음으로 1인 이상~9인 이하, 50인 이상~229인 이하, 300인 이상 순으로 다음 표와 같다.

〈표 2-2〉 종사자 규모별 사물인터넷 사업체 수

(단위: 개사, %)

구분	사업체 수	비율
1~9인	783	35.5
10~49인	1,008	45.7
50~299인	346	15.7
300인 이상	67	3.0
합계	2,204	100.0

출처: 2018년도 사물인터넷 산업 실태조사

110) 대한민국 정책브리핑, 2018년 사물인터넷 산업 실태조사 결과 발표

<http://www.korea.kr/news/pressReleaseView.do?newsId=156316923>

111) 과학기술정보통신부·정보통신상법진흥원·한국사물인터넷협회, 「2018년도 사물인터넷 산업 실태조사」

사업 분야 및 종사자 규모별 사업체 수는 서비스 분야의 10인 이상~49인 이하 사업체가 557개사로 가장 많았으며, 구체적인 수치는 다음 표와 같다.

〈표 2-3〉 사업 분야별/종사자 규모별 사물인터넷 사업체 수

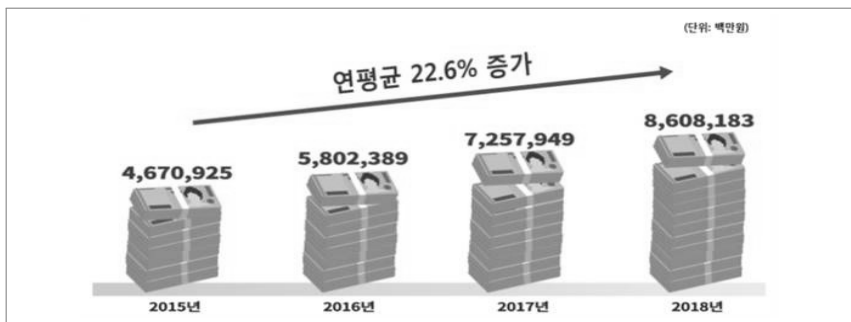
(단위: 개사, %)

구분	합계		1~9인		10~49인		50~299인		300인 이상	
	사업체 수	비율	사업체 수	비율	사업체 수	비율	사업체 수	비율	사업체 수	비율
플랫폼	406	18.4	152	37.4	168	41.4	63	15.5	23	5.7
네트워크	129	5.9	32	24.8	55	42.6	35	27.1	7	5.4
제품기기	478	21.7	162	33.9	228	47.7	69	14.4	19	4.0
서비스	1,191	54.0	437	36.7	557	46.8	179	15.0	18	1.5
합계	2,204	100.0	783	35.5	1,008	45.7	346	15.7	67	3.0

출처: 2018년도 사물인터넷 산업 실태조사

2018년 기준 사물인터넷 산업의 내수와 수출을 합친 총 매출액은 8조 6,082억 원으로, 2017년 7조 2,579억원 대비 18.6% 증가하였으며, 연평균(2015년~2018년) 22.6% 증가하였다.<sup>112)</sup>

〈그림 2-5〉 사물인터넷 매출액 추이(2015~2018년)



출처: 대한민국 정책브리핑, 2018년 사물인터넷 산업 실태조사 결과 발표

112) 대한민국 정책브리핑, 2018년 사물인터넷 산업 실태조사 결과 발표  
<http://www.korea.kr/news/pressReleaseView.do?newsId=156316923>

전체 매출액에서 내수액(7조 8,880억원, 91.6%)이 가장 큰 비중을 차지하고 있으나, 수출액이 빠르게 증가(연평균 성장률 40%)하는 것으로 나타났다. 이는 국내 사물인터넷 기술이 다른 정보통신기술에 비해 상대적으로 높은 기술력을 확보하고 있어, 국내 기업들의 매출액이 꾸준히 증가하고 수출 경쟁력도 향상되는 것으로 평가된다고 한다.<sup>113)</sup> 사업 분야별 매출액은 제품기기 분야가 3조 6,724억원으로 가장 큰 비중을 차지했으며, 다음으로 서비스, 네트워크, 플랫폼 순이었다. 구체적인 수치는 다음 표와 같다.

〈표 2-4〉 사업 분야별 매출액

(단위: 백만원, %)

구분	2018년 (추정)		2017년 (실적)	
	매출액	비율	매출액	비율
플랫폼	1,534,586	17.8	1,186,197	16.3
네트워크	1,542,029	17.9	1,227,744	16.9
제품기기	3,672,378	42.7	3,261,498	44.9
서비스	1,859,190	21.6	1,582,510	21.8
합계	8,608,183	100.0	7,257,949	100.0

출처: 2018년도 사물인터넷 산업 실태조사

사물인터넷 서비스의 활용 분야별 매출액은 제조분야의 매출액이 5,285억원으로 가장 높았고, 다음으로 건설·시설물관리/안전/환경, 자동차/교통/항공/우주/조선 순서였으며, 구체적인 매출액은 다음 표와 같다.

113) 대한민국 정책브리핑, 2018년 사물인터넷 산업 실태조사 결과 발표  
<http://www.korea.kr/news/pressReleaseView.do?newsId=156316923>

〈표 2-5〉 사물인터넷 서비스의 활용 분야별 매출액

(단위: 백만원, %)

구분	2018년		2017년	
	매출액	비율	매출액	비율
헬스케어/의료/복지	80,472	4.3	79,053	5
에너지	94,249	5.1	86,576	5.5
제조	528,501	28.4	411,687	26
스마트홈	145,399	7.8	122,478	7.7
금융	144,966	7.8	107,136	6.8
교육	118,015	6.3	101,514	6.4
국방	5,578	0.3	4,737	0.3
농림축산/수산	13,945	0.8	14,425	0.9
자동차/교통/항공/우주/조선	244,279	13.1	215,166	13.6
관광/스포츠	15,200	0.8	12,835	0.8
소매/물류	131,774	7.1	129,699	8.2
건설·시설물관리/안전/환경	336,811	18.1	297,203	18.8
합계	1,859,190	100.0	1,582,510	100.0

출처: 2018년도 사물인터넷 산업 실태조사

2018년 사물인터넷 산업의 총 내수액은 7조 8,880억원이었으며, 사업 분야별 내수액은 제품기기 분야가 3조 1,478억원으로 가장 큰 비중을 차지했고, 다음으로 서비스, 네트워크, 플랫폼 순으로 다음 표와 같다.

〈표 2-6〉 사업 분야별 내수액

(단위: 백만원, %)

구분	2018년 (추정)		2017년 (실적)	
	내수액	비율	내수액	비율
플랫폼	1,393,840	17.7	1,101,650	16.5
네트워크	1,531,901	19.4	1,222,135	18.3
제품기기	3,147,771	39.9	2,819,775	42.2
서비스	1,814,511	23.0	1,545,685	23.1
합계	8,608,183	100.0	7,257,949	100.0

출처: 2018년도 사물인터넷 산업 실태조사

사물인터넷 서비스 활용 분야별 내수액을 보면 제조분야의 내수액이 5,158억원으로 가장 높았고, 다음으로 건설·시설물관리/안전/환경, 자동차/교통/항공/우주/조선 순으로 다음 표와 같다.

〈표 2-7〉 사물인터넷 서비스의 활용 분야별 내수액

(단위: 백만원, %)

구분	2018년		2017년	
	매출액	비율	매출액	비율
헬스케어/의료/복지	80,325	4.4	78,930	5.1
에너지	94,249	5.2	86,576	5.6
제조	515,847	28.4	405,245	26.2
스마트홈	145,399	8.0	122,478	7.9
금융	140,826	7.8	103,376	6.7
교육	114,714	6.3	98,626	6.4
국방	5,578	0.3	4,737	0.3
농림축산/수산	13,945	0.8	14,425	0.9
자동차/교통/항공/우주/조선	233,980	12.9	205,486	13.3
관광/스포츠	15,200	0.8	12,835	0.8
소매/물류	117,842	6.5	115,768	7.5
건설·시설물관리/안전/환경	336,604	18.6	297,203	19.2
합계	1,814,511	100.0	1,545,685	100.0

출처: 2018년도 사물인터넷 산업 실태조사

## 제3장

# IoT기반 소비자제품안전 관련 국내법제 및 국제논의 동향

제1절 IoT기반 소비자제품안전 관련 국내법제

제2절 IoT기반 소비자제품안전 관련 국제논의 동향



## 제1절 | IoT기반 소비자제품안전 관련 국내법제

### 1. 소비자제품 안전법제와 IoT기반 소비자제품

현재 우리나라의 소비자제품 안전규제 체계는 품목과 분야별로 소관 부처와 관계 법령이 산재하여 있는 구조이며, 소비자제품 안전규제는 주로 사전 규제로서 영업규제(허가/등록/신고), 품목 또는 제품별 규제(인증, 허가, 원료/물질/성분) 방식을 사용하고 있다.<sup>114)</sup> 소비자안전 전반은 「소비자기본법」에서 규율하고 있으며 제품분야의 안전에 관하여는 「제품안전기본법」과 「전기용품 및 생활용품 안전관리법」에서 규율하고 있다. 「제품안전기본법」은 소비자제품을 대상으로 하여 안전성 조사, 리콜 권고/명령, 사업자 결함정보 보고 등 주로 사후적 규제<sup>115)</sup>를 규정하고 있다. 반면에 「전기용품 및 생활용품 안전관리법」은 전기용품, 생활용품을 대상으로 하여 안전인증, 안전확인, 공급자적합성 확인, 안전기준준수 등 주로 사전규제<sup>116)</sup>를 채택하고 있다.

이러한 소비자제품안전 법제가 모두 IoT기반 소비자제품에 적용되는 것은 아니다. IoT기반 소비자제품은 상술한 바와 같이, 인터넷 등 네트워크와 연결되어 소통하는 제품이므로 소비자제품 중 주로 전기용품이나 생활용품 등 제품이 여기에 해당될 것이다. 따라서 소비자제품 안전 법제 중 생활화학제품이나 의약품 등은 IoT기반 소비자제품을 규율하

114) 지광석·김재영·김도년, 「소비자제품안전규제 개선방안 연구」, 한국소비자원 정책연구(2017), pp.29~30

115) 여기서 사후적 규제(post-market regulation)란 제품이 시장에 출시 된 이후에 유통되는 제품을 대상으로 시장 감시 및 사후조치 단계에서 이루어지는 규제를 의미하는 것으로 보고의무, 공표, 리콜제도 등이 포함된다. 지광석·김재영·김도년, 앞의 보고서, p.26

116) 사전규제(pre-market regulation)는 제품이 시장에 출시되기 전에 제품의 안전성을 확인 또는 확보하기 위한 절차 및 기준을 두고 있는 것으로 안전기준 설정에 따른 규제가 이에 해당된다. 지광석·김재영·김도년, 앞의 보고서, p.26



는 법제에서는 제외될 것이다. 그리고 사물인터넷 시장현황에서 언급했듯이, IoT기반 소비자제품의 종류에서 웨어러블 기기, 스마트 홈이 중요한 위상을 차지하고 있다.<sup>117)</sup> IDC의 최근 사물인터넷 시장분석에서도 주요 소비자 사용 사례로 ‘스마트 홈, 개인 건강 및 커넥티드카 인포테인먼트’를 언급했다. 또한 IDC는 2019년 가장 큰 투자가 예상되는 IoT 활용사례로 제조운영(1,000억 달러), 생산자재관리(442억 달러), 스마트 홈(441억 달러), 활동 모니터링(419억 달러)부문에서 주도할 것으로 전망했다.<sup>118)</sup> 이 중 소비자제품에 해당되는 것이 스마트 홈이란 점에서 보면, IoT기반 소비자제품에서 가전제품이 중요한 비중을 차지한다. 따라서 IoT기반 소비자제품 안전관련 법제로 「전기용품 및 생활용품 안전관리법」을 살펴보도록 한다.

한편, IoT기반 소비자제품은 인터넷 등 네트워크와의 연결과 소통을 통한 작동을 특성으로 한다. 이에 인터넷 등 정보통신망의 안전성 문제가 IoT기반 소비자제품의 안전성과 연계될 수 있기 때문에, 정보통신망의 정보보호에 관련한 「정보통신망법」을 살펴보도록 한다. 즉, 「정보통신망법」에서 안전은 정보통신망 자체의 안전성과 여기서 유통되는 정보의 보호를 의미하는 것으로 전통적으로 보면 보안에 해당한다. 하지만 IoT기반 소비자제품의 경우에는 인터넷 등 정보통신망과 연결된 제품이기 때문에 보안문제가 정보통신망의 안전성 문제로 끝나지 않고 소비자의 신체상 위해로 이어질 우려가 있다. 따라서 「정보통신망법」도 IoT기반 소비자제품의 안전 관련 법제에 포함되어 논의되어야 한다. 또한, IoT 보안과 관련하여 법규성을 가진 법령은 아니지만 보안업계의 자율규제의 기준으로서 기능하는 보안가이드를 살펴본다.

117) OECD, 「Consumer Product Safety in the Internet of Things」, pp.9~10

118) 한국 IDC, 전 세계 사물인터넷(IoT) 지출규모 2019년 7450억 달러 전망.

## 2. IoT기반 소비자제품 안전을 규율하는 주요 국내 법제

### 1) 전기용품 및 생활용품 안전관리법

#### (1) 주요 규정 및 안전성인증제도

「전기용품 및 생활용품 안전관리법」은 9장 51개 조항으로 구성되어 있으며, 각 장은 ‘안전인증대상제품의 안전관리(2장)’, ‘안전확인대상제품의 안전관리(3장)’, ‘공급자적합성확인대상제품의 안전관리(4장)’, ‘안전기준준수대상생활용품의 안전관리(5장)’, ‘어린이보호포장대상생활용품의 안전관리(6장)’, ‘구매대행 및 병행수입에 관한 특례 등(7장)’을 다루고 있다. 제품의 안전성 관리에 관한 전반적인 사항을 규율하고 있는데, 법의 구성체계에서도 제품을 일정한 기준으로 분류하여 안전관리를 하고 있다는 점을 손쉽게 인식할 수 있다. 「전기용품 및 생활용품 안전관리법」은 규율대상인 전기용품을 “공업적으로 생산된 물품으로서 교류 전원 또는 직류 전원에 연결하여 사용되는 제품이나 그 부분품 또는 부속품을 말한다”고 하고 생활용품을 “공업적으로 생산된 물품으로서 별도의 가공(단순한 조립은 제외한다) 없이 소비자의 생활에 사용할 수 있는 제품이나 그 부분품 또는 부속품(전기용품은 제외한다)을 말한다”고 정의하고 있다.

이러한 정의를 보면, 통상적으로 가전제품으로 인식되는 대다수 제품들이 동법의 적용을 받고 있는 것이다. 또한 제품안전관리란 “제품의 취급 및 사용으로 인하여 발생하는 소비자의 생명·신체에 대한 위해, 재산상 피해나 자연환경의 훼손을 방지하기 위하여 제품의 제조·수입·판매 등을 관리하는 활동을 말한다”고 정의하고 있다. 이는 「전기용품 및 생활용품 안전관리법」에서 방지하고자 하는 위해를 소비자의 신체상 위해와 함께 재산상 위해도 포함시켜 규정한 것이다.

「전기용품 및 생활용품 안전관리법」은 해당 제품의 위해수준을 고려하여 ‘안전인증’, ‘안전확인’, ‘공급자적합성확인’이란 제품의 안전성 인증제도를 두고 있다. 여기서 안전인증은 “제품시험 및 공장심사를 거쳐 제품의 안전성을 증명하는 것”을 말하고, 안전확인은 “안전확인시험기관으로부터 안전확인시험을 받아 안전기준에 적합한 것임을 확인하는 것”이며, 공급자적합성확인이란 “직접 제품시험을 실시하거나 제3자에게 제품시험을 의뢰하여 해당 제품의 안전기준에 적합한 것임을 스스로 확인하는 것”을 말한다.<sup>119)</sup>

안전인증대상제품은 안전인증대상전기용품과 안전인증대상생활용품으로 구분하고 각각은 “구조 또는 사용 방법 등으로 인하여 화재·감전 등의 위해가 발생할 우려가 크다고 인정되는 전기용품으로서 안전인증을 통하여 그 위해를 방지할 수 있다고 인정되어 산업통상자원부령으로 정하는 것”과 “구조·재질 또는 사용 방법 등으로 인하여 소비자의 생명·신체에 대한 위해, 재산상 피해나 자연환경의 훼손에 대한 우려가 크다고 인정되는 생활용품으로서 안전인증을 통하여 그 위해를 방지할 수 있다고 인정되어 산업통상자원부령으로 정하는 것”으로 정의하고 있다.<sup>120)</sup>

안전확인대상제품도 안전확인대상전기용품과 안전확인대상생활용품으로 구분하고 있다. 안전확인대상전기용품은 “구조 또는 사용 방법 등으로 인하여 화재·감전 등의 위해가 발생할 우려가 있는 전기용품으로서 산업통상자원부장관이 지정한 기관의 제품시험을 통하여 그 위해를 방지할 수 있다고 인정되어 시행규칙으로 정하는 것”이다. 안전확인대상생활용품은 “구조·재질 또는 사용방법 등으로 인하여 소비자의 생명·

119) 「전기용품 및 생활용품 안전관리법」 제2조 제4호 내지 제7호

120) 「전기용품 및 생활용품 안전관리법」 제2조 제10호

신체에 대한 위해, 재산상 피해나 자연환경의 훼손에 대한 우려가 있는 생활용품으로서 산업통상자원부장관이 지정한 기관의 제품시험을 통하여 그 위해를 방지할 수 있다고 인정되어 시행규칙으로 정하는 것”이다.<sup>121)</sup>

공급자적합성확인대상제품도 공급자적합성확인대상전기용품과 공급자적합성확인대상생활용품으로 구분하고 있다. 공급자적합성확인대상 전기용품은 “구조 또는 사용 방법 등으로 인하여 화재·감전 등의 위해가 발생할 가능성이 있는 전기용품으로서 제조업자 또는 수입업자가 직접 또는 제3자에게 의뢰하여 실시하는 제품시험을 통하여 그 위해를 방지할 수 있다고 인정되어 시행규칙으로 정하는 것”이다. 공급자적합성확인대상생활용품은 “소비자가 취급·사용·운반 등을 하는 과정에서 사고가 발생하거나 위해를 입을 가능성이 있거나 소비자가 성분·성능·규격 등을 구별하기 곤란한 생활용품으로서 제조업자 또는 수입업자가 직접 또는 제3자에게 의뢰하여 실시하는 제품시험을 통하여 그 위해를 방지할 수 있다고 인정되어 시행규칙으로 정하는 것”이다.<sup>122)</sup> 이에 더하여 안전기준준수대상생활용품을 “소비자가 취급·사용·운반 등을 하는 과정에서 사고 또는 위해가 발생할 가능성은 적으나 소비자가 성분·성능·규격 등을 구별하기 곤란한 생활용품으로서 제조업자 또는 수입업자가 안전기준을 준수함으로써 그 위해를 방지할 수 있다고 인정되어 산업통상자원부령으로 정하는 것을 말한다”고 규정하고 있다.

그리고 안전인증을 위한 심사도 정의하고 있는데, 제품시험이란 “제품 자체의 안전성을 확인하기 위하여 시험하는 것을 말한다”고 하고 공장심사는 “제품의 제조에 필요한 제조설비·기술능력 및 제조체제를 평가하는 것을 말한다”고 규정하고 있다.<sup>123)</sup> 또한, 「전기용품 및 생활용품

121) 「전기용품 및 생활용품 안전관리법」 제2조 제11호

122) 「전기용품 및 생활용품 안전관리법」 제2조 제12호

안전관리법」은 안전인증기관, 안전확인대상기관의 지정요건, 지정절차, 기록의 작성·보관의무, 주무부처의 지도·감독 등을 규정하고 있다.<sup>124)</sup>

안전인증대상제품, 안전확인대상제품, 공급자적합성확인대상제품 각각의 안전관리와 함께 안전기준준수대상생활용품 해당되는 제품도 안전인증을 받기 때문에 실질적으로 「전기용품 및 생활용품 안전관리법」은 이를 포함하여 4가지 제품안전인증제도를 운영하고 있다고 할 것이다. 즉, 「전기용품 및 생활용품 안전관리법」은 규제대상 제품의 위해수준을 고려하여 안전인증대상제품, 안전확인대상제품, 공급자적합성확인대상제품, 안전기준준수대상생활용품으로 구분하여 각각의 안전관리를 규정하고 있다. 위해수준이 높은 안전인증대상제품의 경우 제품의 심사도 엄격히 규정하여 위해도와 비례하여 안전관리의 엄격성을 규정하고 있다. 이러한 「전기용품 및 생활용품 안전관리법」의 안전인증제도를 일괄하면 다음 그림과 같다.

〈그림 3-1〉 안전관리 대상 제품 분류

<div style="display: flex; justify-content: space-between; align-items: center;"> <span>높 음 ←</span> <span>(위 해 도)</span> <span>→ 낮 음</span> </div>			
안전인증대상	안전확인대상	공급자적합성확인대상	안전기준준수대상 생활용품
구 분	마 크	절 차	
안전인증대상		제품시험 + 공장심사	인 증 → 판 매
안전확인대상		제품시험	신 고 → 판 매
공급자적합성확인대상		제품시험	판 매
안전기준준수대상 생활용품	없 음	제품시험 의무없음	판 매

출처: 국회 산업통상자원중소벤처기업위원회, 전기용품 및 생활용품 안전관리법 일부개정법률안 검토 보고서(의안번호 15768)

123) 「전기용품 및 생활용품 안전관리법」제2조 제8호 내지 제9호

124) 「전기용품 및 생활용품 안전관리법」제4조, 제14조

위 그림의 「전기용품 및 생활용품 안전관리법」상의 안전성인증제도를 간략히 설명하면 다음과 같다. 우선 안전인증제도의 경우 안전인증기관을 지정하고 안전인증대상제품의 제조업자 또는 수입업자는 안전인증대상제품에 대하여 모델 별로 시행규칙으로 정하는 바에 따라 안전인증기관의 안전인증을 받도록 규정하고 있다. 제품시험과 공장심사를 거쳐 안전인증기관이 인증을 하면 판매가 가능한데, 안전인증을 받은 안전인증대상제품은 안전인증의 표시를 하여야 한다.<sup>125)</sup> 그리고 안전인증기관은 안전인증대상제품이 계속하여 안전성을 유지하는지를 확인하기 위하여 2년에 1회의 정기검사를 실시하여야 한다.<sup>126)</sup>

이에 비하여 안전확인대상제도는 안전확인시험기관의 제품시험을 거쳐 안전기준에 적합한 것임을 주무부처에 신고하여 판매할 수 있다. 따라서 「전기용품 및 생활용품 안전관리법」상의 이러한 안전인증제도는 제품의 위해도를 기준으로 위해도가 높은 제품의 경우 해당 제품의 안전성 검증절차를 복잡하고 까다롭게 하고 상대적으로 위해도가 낮은 제품의 경우 이를 간소화하여 제조업자 등의 안전성 인증부담을 경감시키고 있는 것이다. 또한, 안전성 기준의 경우에는 안전인증기준이든 안전확인기준이나 공급자적합성확인기준을 모두 주무부처인 산업통상부장관이 정하여 고시하도록 규정하고 있다. 따라서 안전기준은 행정청이 정하며 안전인증을 위한 시험은 행정청이 아닌 제3의 기관이 담당하고 있는 구조이다.

## (2) 제품 분류 및 안전기준 관련 규정

「전기용품 및 생활용품 안전관리법」은 안전인증대상제품, 안전확인대상제품, 공급자적합성확인대상제품, 안전기준준수대상생활용품의 지

125) 「전기용품 및 생활용품 안전관리법」 제9조

126) 「전기용품 및 생활용품 안전관리법」 제7조

정 및 안전기준을 산업통상자원부가 정하고 있다. 즉, 안전인증대상제품 등 4가지 부류의 제품이 위해도를 기준으로 분류되어 있는데, 이의 분류와 안전기준을 행정청이 정하고 있는 것이다. 입법형식으로는 제품의 분류는 산업통상자원부령인 시행규칙이고 안전기준은 고시로 규정되어 있다. 그러나 모두 「전기용품 및 생활용품 안전관리법」에서 위임의 근거를 두고 있으며, 규율사항이 행정책체의 권리·의무를 변동시킨다는 점에서 법규명령으로 보아야 하고, 따라서 입법형식은 차이가 있지만 실질적·기능적 측면에서는 차이가 없다.<sup>127)</sup> 안전관리대상제품의 분류에 관하여는 「전기용품 및 생활용품 안전관리법 시행규칙」 제3조에서 규정하고 있다. 안전인증대상전기용품은 1천볼트 이하의 교류전원 또는 직류전원을 사용하는 것으로<sup>128)</sup>, 안전확인대상전기용품<sup>129)</sup>은 1천

127) 행정입법은 통상 대외적 구속력(legally binding effect)을 기준으로 하여 대외적 구속력이 있는 행정입법을 법규명령, 그렇지 않은 것을 행정규칙으로 구분한다. 김남진·김연태, 「행정법 I」, 법문사(2012), p.152; 김철용, 「행정법」, 고시계(2012), p.119; 이광운, 「일반행정법」, 법문사(2006), p.114; 황의관, “미국행정법상 법규명령에 관한 연구”, 공법학연구 15권 4호(2014) 참조. 이러한 실질적·기능적 기준에 따라 행정입법을 구분하는 경우 제정형식이 부령인지 고시인지가 해당 행정입법이 법규명령, 행정규칙인지를 구분하는 표식이 되는 것은 아니다. 따라서 「전기용품 및 생활용품 안전관리법」상의 제품분류기준은 부령이고 안전기준은 고시이기 때문에 전자가 법규명령, 후자는 행정규칙이 되는 것은 아니다. 동법상 제품분류는 행정책체 입장에서는 안전관리가 달라지고 그에 따라 준수해야 할 의무가 변동되므로 법적 구속력이 인정되며, 안전기준의 경우도 마찬가지이다. 따라서 「전기용품 및 생활용품 안전관리법」상 제품분류기준, 안전기준은 모두 대외적 구속력을 가진 법규명령으로 보아야 한다.

128) 안전인증대상제품의 세부분류 항목은 “전선 및 전원, 전기기용 스위치, 전원용 커패시터 및 전원필터, 전기설비용 부속품 및 연결부품, 절연변압기, 전기기기(전기청소기, 전기다리미 및 전기프레스기, 주방용전열기구, 전기세탁기 및 탈수기, 모발관리기, 전기담요 및 매트, 전기침대, 전기온수기, 전기 냉장·냉동기기 등), 전동공구, 오디오·비디오 응용기기, 정보·통신·사무기기, 조명기기, 전기저장장치 구성품”이고, 각 분류별로 품목이 규정되어 있다.

129) 안전확인대상전기용품은 안전인증대상전기용품과 분류는 동일하며 세부품목 중 전기기기에는 ‘과일 껍질깎이, 전기용해기, 이·미용기기, 전기의자 및 전동침대, 컴프레서, 전기온수매트 등’이 있고, 오디오·비디오 응용기기에 ‘TV수상기, 디스크 플레이어, 오디오시스템 등’이 있으며, 정보·통신·사무기기에 ‘모니

볼트 이하의 교류전원 또는 직류전원을 사용하는 것으로, 공급자적합성 확인대상전기용품도 1천볼트 이하의 교류전원 또는 직류전원을 사용하는 것으로서 별표에서 규정한 제품으로 한다. 안전인증대상생활용품, 안전확인대상생활용품, 공급자적합성확인대상생활용품은 모두 별표에서 규정한 제품으로 한다. 「전기용품 및 생활용품 안전관리법 시행규칙」은 각 제품의 세부범위를 국가기술표준원장이 정하여 고시할 수 있도록 위임근거를 두고 있다.

안전기준에 관하여는 안전인증대상제품, 안전확인대상제품, 공급자적합성확인대상제품, 안전기준준수대상생활용품 모두 산업통상자원부 장관이 정하여 고시하도록 규정하고 있다. 안전인증대상생활용품, 안전확인대상생활용품, 공급자적합성확인대상생활용품의 경우 각각의 안전기준 고시로 규정하고 각 제품별 세부사항은 부속서에서 다루고 있다.<sup>130)</sup> 안전인증대상전기용품, 안전확인대상전기용품, 공급자적합성확인대상 전기용품의 안전기준은 전기용품안전기준으로서 국가기술표준원의 고시형식으로 제정되어 각 제품별로 규정되어 있다.

이러한 전기용품의 안전기준은 고시단계에서도 상당히 세부적인 사항을 규정하고 있으며, 일반 요구사항을 규정한 경우처럼 시험방법 등을 부속서에서 정하는 경우가 있다.<sup>131)</sup>

터, 프린터, 프로젝터, 문서 세단기, 천공기, 디지털 TV 등'이 포함된다.

130) 「안전인증대상생활용품의 안전기준」, 「안전확인대상생활용품의 안전기준」 등

131) 「전기용품안전기준 가정용 및 이와 유사한 전기기기의 안전성 제1부 일반 요구사항」



## 2) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

### (1) 체계 및 주요 규정사항

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 ‘정보통신망법’)은 제1조에서 본 법의 목적을 밝히고 있는데, 이를 “정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 한다.”고 규정하고 있다. 즉, 「정보통신망법」은 법령명 그대로 정보통신망의 이용과 이에 관련한 개인정보보호를 주목으로 한 법으로서 전통적인 소비자제품의 안전에 관련한 법률은 아니다. 따라서 종래의 소비자제품을 「정보통신망법」이 규율하는 경우는 없었다. 하지만 상술한 바와 같이, IoT기반 소비자제품은 사물인터넷과 제품이 결합되고 연결된 제품이고 정보통신망에는 인터넷이 당연히 포함되기 때문에,<sup>132)</sup> 「정보통신망법」도 IoT기반 소비자제품을 규율하는 법제에 포함되는 것이다.

「정보통신망법」의 주요 개념정의를 보면 ‘정보통신서비스’는 “「전기통신사업법」 제2조제6호에 따른 전기통신역무와 이를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 것”을 의미하며, ‘정보통신서비스 제공자’란 “「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자”, 이용자란 “정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자”를 말한다. 개인정보란 “생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정

132) 정보통신망이란 “「전기통신사업법」 제2조제2호에 따른 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말한다”고 한다. 「정보통신망법」 제2조제1호.

한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)”를 말한다. 또한 「정보통신망법」에서 침해사고란 “해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태”를 말한다. 「정보통신망법」은 동법에서 사용하는 용어의 의미를 정의 조항에서 정하는 것 이외에는 「국가정보화 기본법」에서 정하는 바에 따르도록 규정하고 있다.<sup>133)</sup>

「정보통신망법」은 10장 76개조로 이루어져 있는데, 총칙인 1장, 삭제된 3장, 보칙인 9장과 부칙인 10장을 제외하면 실질적으로 6개장을 내용으로 한다. 각각의 장은 ‘정보통신망의 이용촉진(2장)’, ‘개인정보의 보호(4장)’, ‘정보통신망에서의 이용자 보호(5장)’, ‘정보통신망의 안전성 확보(6장)’, ‘통신과금서비스(7장)’, ‘국제협력(8장)’으로 구성되어 있다. 이러한 「정보통신망법」이 실질적으로 규율하고 있는 영역은 정보통신망 이용자의 개인정보보호와 정보통신망 이용촉진과 안전성 확보로 볼 수 있다. IoT기반 소비자제품의 경우 인터넷과의 연결되어 있어 인터넷의 안전성과 소비자 위해가 연계되어 있다. 이에 「정보통신망법」의 안전성 관련 규정의 내용을 상세히 살펴볼 필요성이 있다.

## (2) 정보통신망의 안전에 관한 규정

「정보통신망법」은 정보통신서비스 제공자에게 정보통신망의 안전성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하도록 규정하고, 과학기술정보통신부장관이 보호조치의 구체적 내용을 정한 「정보보호조치에 관한 지침」<sup>134)</sup>을 정하여 고시하고 정보통신서비스 제공자에게 이를

133) 「정보통신망법」 제2조 제2항

지키도록 권고할 수 있다.<sup>135)</sup> 정보보호지침에 포함되어야 하는 것은 다음과 같다.

〈표 3-1〉 정보보호지침에 포함되어야 하는 사항

구분	주요 내용
1	정당한 권한이 없는 자가 정보통신망에 접근·침입하는 것을 방지하거나 대응하기 위한 정보보호시스템의 설치·운영 등 기술적·물리적 보호조치
2	정보의 불법 유출·위조·변조·삭제 등을 방지하기 위한 기술적 보호조치
3	정보통신망의 지속적인 이용이 가능한 상태를 확보하기 위한 기술적·물리적 보호조치
4	정보통신망의 안전 및 정보보호를 위한 인력·조직·경비의 확보 및 관련 계획수립 등 관리적 보호조치

출처: 「정보통신망법」 제45조제3항

그리고 「정보보호지침」은 보호조치의 구체적인 내용을 규정하고 있는데, 정보통신서비스 제공자는 매년 정보보호조치의 이행여부를 자체적으로 점검하거나 외부 전문기관으로 하여금 점검하게 하도록 규정하고 있다.<sup>136)</sup> 「정보보호지침」상의 보호조치는 ‘관리적 보호조치’, ‘기술적 보호조치’, ‘물리적 보호조치’로 구분되고 각각에 대하여 세부적으로 분류하고 있다. 세부항목은 다음과 같으며, 각 세부항목별 구체적 조치가 규정되어 있다.

134) 이를 ‘정보보호지침’이라 한다.

135) 「정보통신망법」 제45조제1항, 제2항

136) 「정보보호지침」 제4조

〈표 3-2〉 「정보보호지침」상 보호조치 세부항목

관리적 보호조치	정보보호 조직의 구성·운영	정보보호조직의 구성
		정보보호 최고책임자의 지정
		정보보호조직구성원의 역할
	정보보호 계획 등의 수립 및 관리	정보보호 방침의 수립·이행
		정보보호 실행계획의 수립·이행
		정보보호실무지침의 마련·준수
	인적 보안	정보보호 사전점검
		내부인력 보안
		외부인력 보안
	이용자 보호	위탁운영 보안
		정보보호 정보제공
	침해사고 대응 정보보호 조치 점검 정보자산 관리 정보보호 투자	정보보호 현황공개
침해사고 대응계획의 수립·이행		
정보보호조치의 자체 점검		
정보통신 설비 및 시설의 현황 관리		
정보보호 투자계획 수립·이행		
기술적 보호조치	네트워크 보안	트래픽 모니터링
		무선서비스 보안
		정보보호시스템 설치·운영
		정보보호를 위한 모니터링
	정보통신 설비 보안	웹서버 보안
		DNS서버 보안
		DHCP서버 보안
		DB서버 보안
		라우터/스위치 보안
		정보보호시스템보안
		취약점 점검
		접근통제 및 보안설정 관리
		관리자 계정의 비밀번호 관리
		로그관리
		보안패치 관리
		백업 및 복구
		중요정보의 암호화
		관리용 단말 보안
		물리적 보호조치
부대설비 및 시설 운영·관리	백업설비 및 시설 설치·운영	

출처: 「정보보호조치에 관한 지침」 별표1

또한 「정보통신망법」은 정보통신서비스 제공자가 새로운 정보통신망을 구축하거나 정보통신서비스를 제공하고자 하는 경우 계획 또는 설계에 정보보호에 관한 사항을 고려하도록 규정하고 있다. 이에 더하여 과학기술정보통신부장관의 인·허가를 받거나 등록·신고를 하도록 되어 있는 사업으로서 시행령으로 정하는 정보통신서비스 또는 전기통신사업, 과학기술정보통신부장관이 사업비의 전부 또는 일부를 지원하는 사업으로서 시행령으로 정하는 정보통신서비스 또는 전기통신사업의 경우에는 시행령으로 정하는 정보보호 사전점검기준에 따라 보호조치를 하도록 과학기술정보통신부장관이 권고할 수 있도록 규정하고 있다.<sup>137)</sup> 즉, 「정보통신망법」은 정보보호에 있어서 사전점검을 규정하여 계획이나 설계단계에서 보안을 고려하도록 규정하고 있다. 그리고 「정보통신망법」은 정보통신서비스 제공자가 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 임원급의 정보보호 최고책임자를 지정하고 이를 주무부처장관에게 신고하도록 규정하고 있다. 정보보호최고책임자의 업무는 법에 따라 다음 표와 같이 정해져 있고, 이외의 다른 업무겸직을 금지하고 있다.<sup>138)</sup>

〈표 3-3〉 정보보호최고책임자의 업무

구분	주요 내용
1	정보보호관리체계의 수립 및 관리·운영
2	정보보호 취약점 분석·평가 및 개선
3	침해사고의 예방 및 대응
4	사전 정보보호대책 마련 및 보안조치 설계·구현
5	정보보호 사전 보안성 검토
6	중요 정보의 암호화 및 보안서버 적합성 검토
7	그 밖에 이 법이나 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행

출처: 「정보통신망법」 제45조의3제4항

137) 「정보통신망법」 제45조의2

138) 「정보통신망법」 제45조의2제3항

정보보호 최고책임자의 자격요건도 시행령에서 정하고 있으며, 정보통신서비스 제공자는 정보보호 최고책임자를 구성원으로 하는 정보보호 최고책임자 협의회를 구성·운영하여 침해사고에 대한 공동 예방 및 대응, 필요한 정보의 교류 등을 공동사업으로 수행할 수 있도록 규정하고 있다.<sup>139)</sup> 과학기술정보통신부장관은 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계(이를 ‘정보보호 관리체계’라 함)를 수립·운영하고 있는 자에 대하여 고시<sup>140)</sup>로 정한 기준에 적합한지에 관하여 인증할 수 있다. 또한 전기통신사업자<sup>141)</sup>의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 「전기통신사업법」에 따른 등록을 한 자 또는 집적정보통신시설 사업자<sup>142)</sup>, 일정 규모 이상의 매출액이나 이용자수가 있는 자는 의무적으로 이러한 인증을 받도록 규정하고 있다. 과학기술정보통신부장관은 인증기준을 고시할 수 있고 인증의 유효기간은 3년이며, 과학기술정보통신부장관이 인증기관을 지정하고 있다.<sup>143)</sup>

「정보통신망법」에서는 정보보호 관리체계의 인증만이 아니라 개인정보보호 관리체계의 인증제도도 규정하고 있다. 다만, 개인정보보호 관리체계 인증제도에 관한 업무는 방송통신위원회가 담당하고 있어 정보보호와 담당부처를 다르게 규정하고 있다.<sup>144)</sup> 「개인정보보호법」의 담당부처는 행정안전부이고 「정보통신망법」상의 개인정보보호 업무는 주로 방송통신위원회가 담당하고 있어서 개인정보의 매개체에 따라 담당

139) 「정보통신망법」 제45조의2제5항

140) 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」

141) 「전기통신사업법」 제2조제8호는 전기통신사업자를 ‘이 법에 따라 등록 또는 신고를 하고 전기통신역무를 제공하는 자’로 정의하고 있다.

142) 타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자를 의미한다. 「정보통신망법」 제46조제1항

143) 「정보통신망법」 제47조제3항 내지 제5항

144) 「정보통신망법」 제47조의3

부처를 다르게 규정하고 있다. 한편, 정보보호 관리체계 인증을 받은 자는 과학기술정보통신부장관으로부터 정보보호 관리등급을 받을 수 있다. 정보보호 관리등급을 받은 자는 시행령으로 정하는 바에 따라 해당 등급의 내용을 표시하거나 홍보에 활용하도록 규정하고 있다.<sup>145)</sup> 과학기술정보통신부장관은 특정한 사유<sup>146)</sup>를 발견한 경우에는 부여한 등급을 취소할 수 있도록 규정하고 있다.<sup>147)</sup> 그리고 「정보통신망법」은 정부가 정보통신망 이용자에게 정보보호에 필요한 기준을 정하여 권고하고, 침해사고의 예방 및 확산 방지를 위하여 취약점 점검, 기술 지원 등 필요한 조치를 하도록 규정하고 있다. 그리고 주요정보통신서비스 제공자는 정보통신망에 중대한 침해사고가 발생하여 자신의 서비스를 이용하는 이용자의 정보시스템 또는 정보통신망 등에 심각한 장애가 발생할 가능성이 있으면 이용약관으로 정하는 바에 따라 그 이용자에게 보호조치를 취하도록 요청하고, 이를 이행하지 아니하는 경우에는 해당 정보통신망으로의 접속을 일시적으로 제한할 수 있다.<sup>148)</sup> 그리고 보호조치의 요청 등에 관하여 이용약관으로 정하여야 하는 구체적인 사항은 시행령으로 정한다.<sup>149)</sup>

과학기술정보통신부장관은 침해사고에 적절히 대응하기 위하여 ‘침해사고에 관한 정보의 수집·전파’, ‘침해사고의 예보·경보’, ‘침해사고에 대한 긴급조치’ 등의 업무를 수행한다. 특히 주요정보통신서비스 제공자, 집적정보통신시설 사업자 등은 시행령으로 정하는 바에 따라 침해사고의 유형별 통계, 해당 정보통신망의 소통량 통계 및 접속경로별 이

145) 「정보통신망법」 제47조의5

146) 거짓이나 그 밖의 부정한 방법으로 정보보호 관리등급을 받은 경우, 등급기준에 미달하는 경우를 말한다. 「정보통신망법」 제47조의5제4항

147) 「정보통신망법」 제47조의5제4항

148) 「정보통신망법」 제47조의4제1항, 제2항

149) 「정보통신망법」 제47조의4제4항

용 통계 등 침해사고 관련 정보를 과학기술정보통신부장관이나 한국인터넷진흥원에 제공하여야 한다.<sup>150)</sup> 만일 해당 사업자가 침해사고 등에 관한 정보제공을 거부하거나 거짓정보를 제공하면 과학기술정보통신부장관은 상당한 기간을 정하여 해당 사업자에게 시정을 명할 수 있다. 한국인터넷진흥원은 침해사고 관련 정보를 분석하여 과학기술정보통신부장관에게 보고하여야 하며, 제공받은 정보는 침해사고의 대응을 위하여 필요한 범위에서만 정당하게 사용하여야 한다.<sup>151)</sup> 정보통신서비스 제공자, 집적정보통신시설 사업자는 침해사고가 발생하는 즉시 해당 사실을 과학기술정보통신부장관이나 한국인터넷진흥원에 신고해야 하고, 과학기술정보통신부장관이나 한국인터넷진흥원은 신고를 받거나 침해사고를 알게 되면 필요한 조치를 하여야 한다.<sup>152)</sup> 침해사고 발생 후 정보통신서비스 제공자 등 정보통신망을 운영하는 자는 침해사고의 원인을 분석하고 피해확산을 방지해야 한다. 과학기술정보통신부장관은 정보통신서비스 제공자의 정보통신망에 중대한 침해사고가 발생하면 피해확산 방지, 사고대응, 복구 및 재발 방지를 위하여 정보보호에 전문성을 갖춘 민·관합동조사단을 구성하여 그 침해사고의 원인 분석을 할 수 있다. 과학기술정보통신부장관은 침해사고의 원인을 분석하기 위하여 필요하면 정보통신서비스 제공자와 집적정보통신시설 사업자에게 침해사고 관련 자료의 제출을 요구할 수 있으며, 민·관합동조사단에게 관계인의 사업장에 출입하여 침해사고 원인을 조사하도록 할 수 있다.<sup>153)</sup>

150) 「정보통신망법」 제48조의2제1항, 제2항

151) 「정보통신망법」 제48조의2제3항, 제5항

152) 「정보통신망법」 제48조의3

153) 「정보통신망법」 제48조의4 제1항 내지 제3항



### 3) 홈·가전 IoT 보안가이드

#### (1) IoT 공통보안 원칙

사물인터넷 보안에 관하여는 민간 주도의 보안얼라이언스에서 제정하여 채택한 보안가이드가 자율규제 수단으로 작동하고 있다. 이 보안 가이드는 횡적으로 사물인터넷 전체 영역에 적용되는 IoT 공통 보안 원칙과 종적으로 사물인터넷이 활용되는 분야별 보안가이드로 구성되어 있다. IoT 공통 보안 7대 원칙은 IoT장치 및 서비스의 제공자(개발자)와 사용자가 IoT 장치의 전주기 세부 단계에서 고려해야 하는 공통의 보안 요구 사항으로서 다음 표와 같다.

〈표 3-4〉 IoT 공통보안 7대 원칙

순번	주요 내용
1	정보보호와 프라이버시 강화를 고려한 IoT 제품·서비스 설계
2	안전한 소프트웨어 및 하드웨어 개발 기술 적용 및 검증
3	안전한 초기 보안 설정 방안 제공
4	보안 프로토콜 준수 및 안전한 파라미터 설정
5	IoT제품·서비스의 취약점 보안패치 및 업데이트 지속 이행
6	안전한 운영·관리를 위한 정보보호 및 프라이버시 관리체계 마련
7	IoT침해사고 대응체계 및 책임추적성 확보 방안 마련

출처: IoT 보안얼라이언스, IoT 공통 보안원칙

이러한 공통보안 7대 원칙은 IoT 장치의 설계/개발 단계의 보안요구 사항인 1,2원칙과 IoT 장치 배포/설치(재설치)/ 구성(재구성) 단계의 보안요구 사항인 3,4원칙 및 IoT 장치 및 서비스 운영/관리/폐기 단계의 보안 요구 사항인 5,6,7원칙으로 구분할 수 있다.

1원칙은 ‘Security by Design’ 및 ‘Privacy by Design’과 같은 기본원칙을 준수할 것을 의미한다. 즉, 제품의 설계/개발 단계에서 보안

(Security)을 내재화 하고 개인정보보호(Privacy) 침해위험요소를 분석하여 지속적으로 점검하고 침해가 발생하기 전에 선제적인 대응을 한다는 것이다.<sup>154)</sup> 2원칙은 시큐어 코딩, 소프트웨어, 어플리케이션 및 소프트웨어 보안성 검증 및 시큐어 하드웨어 장치 활용을 의미한다. 개발자는 장치와 관계없이 소스코드 구현단계부터 내재될 수 있는 보안 취약점을 사전에 예방하기 위해 시큐어 코딩을 적용해야 한다는 것이다.<sup>155)</sup> 그리고 사물인터넷 제품 개발시 다양한 소프트웨어를 활용할 경우, 현재까지 알려진 보안 취약점에 대한 보안성 검증을 수행하고 보안패치를 반드시 적용해야 한다는 것이다.<sup>156)</sup>

3원칙은 IoT장치 설치자나 서비스 관리자는 초기 설치 단계와 고장수리 후 재설치 단계에서 보안 프로토콜들에 기본으로 설정되는 파라미터 값이 가장 안전한 설정이 될 수 있도록 “Secure by Default”기본원칙을 준수해야 한다는 것이다.

4원칙은 IoT제품 개발자와 서비스 제공자는 데이터 통신 및 개방형 플랫폼에 안전성을 보장하는 보안 프로토콜을 적용해야 하고, 보안 서비스 제공시 안전한 파라미터들이 설정될 수 있도록 해야 한다는 것이다.<sup>157)</sup> 5원칙은 IoT제품 제조사와 서비스 제공자는 해당 제품이나 서비스에서 보안 취약점이 발견되면 이에 대한 분석을 수행하고, 보안 요구사항을 반영한 보안패치를 신속히 배포할 수 있도록 사후조치 방안을 마련해야 한다는 것이다.

6원칙은 사용자 정보의 취득-사용-폐기의 전주기 정보의 보호 및 프

154) IoT 보안얼라이언스, IoT 공통 보안원칙, p.12

155) IoT 보안얼라이언스, IoT 공통 보안원칙, p.14

156) IoT 보안얼라이언스, IoT 공통 보안원칙, p.15

157) IoT 보안얼라이언스, IoT 공통 보안원칙, p.18

라이버시 관리를 의미한다. 이는 정보보호 관리체계를 구축할 것을 요구하는데, 침해사고 발생 시 서비스연속성 유지를 위한 백업 및 복구 절차 수립, IoT장치의 비인가 접근 및 도난·분실을 방지하기 위한 물리적 접근통제 등이 포함된다.<sup>158)</sup>

마지막 7원칙은 보안사고에 대비한 침입탐지와 사고 시 분석 및 책임 추적성 확보이다. 이는 IoT 서비스는 다양한 유형의 장치, 유·무선 네트워크 장비, 플랫폼 등으로 구성되며, 각 영역에서 발생 가능한 보안 침해사고에 대비하여 침입탐지 및 모니터링이 수행되어야 한다는 것이다.<sup>159)</sup>

## (2) 홈·가정 IoT 보안가이드

홈·가정 IoT 제품에 공통적으로 적용해야 하는 보안항목은 다음과 같다.

〈표 3-5〉 홈·가정 공통 보안항목 및 요구사항

보안항목	보안요구사항
소프트웨어 개발보안	시큐어코딩 알려진 보안취약점 점검 및 제거 최신 제3자 소프트웨어 사용
물리적 보안	물리적 인터페이스 차단 ▶ 외부 입출력 포트 비활성화 ▶ 내부 입출력 포트 비활성화 ▶ 외부 조작 확인 및 분해 방지 메커니즘

출처: IoT보안얼라이언스, 홈·가정 IoT 보안가이드

시큐어코딩은 홈·가정 IoT 제품 설계 단계에서부터 이 보안가이드 및 IoT 공통보안가이드의 보안항목을 고려하여 제품을 설계하고, 보안

158) IoT 보안얼라이언스, IoT 공통 보안원칙, pp.20~21

159) IoT 보안얼라이언스, IoT 공통 보안원칙, p.22

취약점의 원인인 보안약점을 최소화하여 안전하게 구현하는 것을 목적으로 한다는 것이다.<sup>160)</sup> 알려진 보안취약점 점검 및 제거는 홈·가전 IoT 제품을 구성하는 소프트웨어가 기존에 알려진 보안취약점을 갖는 프로토콜, 라이브러리, 패키지, 오픈소스 등을 사용하여 개발되었을 경우 제반 펌웨어, 운영체제도 보안에 취약할 수 있기 때문에 제품을 점검하여 보안취약점을 제거해야 한다는 것이다.<sup>161)</sup> 최신 제3자 소프트웨어 사용은 홈·가전 IoT제품 개발 및 서비스 운영환경에 사용되는 제3자 소프트웨어(운영체제, 라이브러리, 모듈 등 공개용 및 상용 소프트웨어)는 최신 보안패치가 적용된 최신 버전을 사용해야 한다. 출시된 홈·가전 IoT제품에서 사용되는 제3자 소프트웨어에 심각한 결함이나 보안취약점에 대한 보안패치를 적용해야 하는 경우 신속하게 업데이트를 수행해야 한다.<sup>162)</sup>

물리적 인터페이스 차단 중 외부 입출력 포트 비활성화는 외부에 노출된 포트는 종류와 기능 식별이 용이하고 쉽게 접근이 가능하기 때문에 공격대상이 되기 쉽다. 따라서 홈·가전 IoT제품의 불필요한 외부 인터페이스는 제거해야 한다.<sup>163)</sup> 내부 입출력 포트 비활성화는 홈·가전 IoT 제품의 내부 입출력 포트(예: UART, JTAG 등)를 통해 펌웨어 추출 및 파일 시스템 분석을 통한 정보검색을 방지하기 위해 입출력 포트에 대한 접근통제를 한다는 것이다.<sup>164)</sup> 외부 조작 확인 및 분해방지 메커니즘은 하드웨어의 데이터 버스와 제어신호 등에 대한 직접적인 접근 가능성에 의해 보안취약점이 발생하므로, 이에 대하여 조작확인 또는 분해 방지 메커니즘을 구현해야 한다는 것이다.<sup>165)</sup>

160) IoT보안얼라이언스, 홈·가전 IoT 보안가이드, p.31

161) IoT보안얼라이언스, 홈·가전 IoT 보안가이드, p.36

162) IoT보안얼라이언스, 홈·가전 IoT 보안가이드, p.38

163) IoT보안얼라이언스, 홈·가전 IoT 보안가이드, p.40

164) IoT보안얼라이언스, 홈·가전 IoT 보안가이드, p.42

## 제2절 | IoT기반 소비자제품안전 관련 국제논의 동향

### 1. IoT기반 소비자제품의 위해요인

#### 1) 미국의 IoT기반 소비자제품 위해요인 분석

##### (1) 소비자제품안전위원회(CPSC)의 위해요인 분석

미국 소비자제품안전위원회(CPSC)는 2017년 자신의 관할에 속하는 새로운 제품들이 시판되고 소비자의 일상생활 속에서 도입되는 상황에 따라, 이러한 제품들이 소비자와 그들의 가족들의 삶에 미치는 영향을 분석하였다. 당시 CPSC의장인 Elliot F. Kaye는 CPSC 기술, 의무준수(compliance) 및 정보기술 부서에 i) 새로운 소비자제품이 장래 3~5년 내에 어떠한 것이 이용되고 사용범위가 확장될 것인지, 그리고 ii) 이처럼 등장하고 있는 새로운 기술과 연계된 새롭게 등장하거나 증가 혹은 감소되는 위해요인이 무엇인지에 관하여 조사를 요청하였다. 이에 따라 CPSC 담당 부서는 새롭게 등장하고 있는 미래 기술에 관련한 잠재적인 위해요인을 다루는 보고서를 발간하였다.<sup>165)</sup>

이 보고서에서는 Kaye 당시 위원장의 요청사항을 반영하여 향후 몇 년 동안 이용될 수 있고 이용범위가 확장될 새롭게 등장한 잠재적인 소비자제품 및 기술에 대하여 전반을 간략히 제공하고 있다. 이와 함께 새로운 소비자제품 및 기술의 도입이 소비자에게 미치는 새로운 또는 증폭된 위해요인을 살펴보고 있다.<sup>167)</sup>

165) IoT보안얼라이언스, 홈·가전 IoT 보안가이드, p.45

166) CPSC Staff Report, 「Potential Hazards Associated with Emerging and Future Technologies」(2017)

167) CPSC Staff Report, 「Potential Hazards Associated with Emerging and Future Technologies」(2017)

이 보고서에서 CPSC는 소비자제품 시장의 트렌드로 “스마트 기술과 사물인터넷의 융합의 증가”, “인구고령화, 노령 가구화, 그리고 다세대 가구”, “대량의 데이터를 활용하는 빅데이터”, “전자상거래 및 소비자와의 직접거래”로 파악하였다. 현재 등장하고 있거나 장래에 도래할 소비자제품 및 기술로서 이 보고서는 다음을 확인하였다.

#### 〈표 3-6〉 CPSC의 소비자제품 관련 신기술 목록

- 
- 3D 프린터 및 프린트된 제품
  - 인터넷 홈 기반 스마트 기술
  - 구성부분으로서 소프트웨어
  - 웨어러블 제품 및 기술
  - 나노물질을 포함한 새로운 물질
  - 가상 현실 및 증강현실 게임
  - 개인이동수단
  - 고도의 에너지 저장장치 및 에너지 생산 장치
  - 고령자를 도와주는 로봇제품을 포함한 로봇
  - 뇌-기계 인터페이스/이식가능한 기술(implantable technologies)
- 

출처: CPSC Staff Report, 「Potential Hazards Associated with Emerging and Future Technologies」 (2017)

이러한 새롭고 등장하고 있는 소비자제품 및 기술들은 일부 제품 위해요인을 감소시킬 수 있지만 동시에 새로운 위해요인을 도입하기도 한다. CPSC는 신기술에서 발생할 수 있는 잠재적인 위해요인을 다음과 같이 설명하고 있다.

〈표 3-7〉 CPSC의 소비자제품 관련 신기술의 위해요인

위해요인	주요 설명
안전기능의 상실	안전장비, 또는 안전장비와 연결되어 있는 제품이 작동에 실패하거나 위해한 조건 속에 다른 장비의 작동이 실패하도록 원인이 될 수 있음
화재 및 화상	제품이나 기술이 에너지원(예를 들어, 배터리, 액화연료, 전력코드)을 포함하거나 이와 관련된 경우, 에너지의 신속하고 통제되지 아니한 방출은 제품을 발화시키거나 근처 가연성 물질을 발화시키거나 또는 잠재적인 화상 위험이 있음
쇼크(Shock)	만일 제품이나 기술이 30 Vac 또는 60 Vdc를 초과하는 전압을 사용하는 경우, 잠재적인 쇼크 위험이 발생할 수 있음
화학적 노출	새로운 섬유를 포함한 새로운 물질은 사용자를 거부반응이나 중독성 화합물에 노출시킬 수 있음
상처/타박상 충돌/절단	증폭된 운동 또는 위치에너지를 가진 장비 또는 사용자를 빠르게 이동시키는 장비는 증가된 충돌 또는 낙상 위험에 노출시킴
숨막힘/질식	웨어러블 및 다른 소규모 장비들은 반드시 질식위험을 회피할 수 있도록 설계되어야함

출처: CPSC Staff Report, 「Potential Hazards Associated with Emerging and Future Technologies」 (2017)

이러한 위해요인은 전통적인 제품에서도 발생할 수 있는 위해요인으로서는 신기술을 활용한 소비자제품에서 발생할 수 있는 위해요인을 의미한다.

이에 더하여 CPSC는 사물인터넷과 같은 데이터를 기반으로 하는 소비자제품에 관한 위해요인의 범주를 추가하고 있다. CPSC는 데이터 획득, 데이터 처리, 상호연결 및 더 많은 소비자제품과의 통합이 지속되어 감에 따라, 소비자는 새로운 위해 범주에 노출될 수 있고, 이러한 위해 범주에는 i) 연결 상실(Loss of Connectivity): 가정 안에서 연결의 중심부(communication hub)로 기능하는 제품과 같은 장비가 작동이 멈추게 되면 해당 가정 내 다른 연결 장비 또는 인터넷과의 연결이 끊기거나 통제가 안 되는 결과를 야기하는 경우, ii) 데이터 통합성(진실성, Data Integrity): 만일 정확한 데이터가 안전기능을 지원한다면, 데

이터의 훼손이 결정적인 안전의 위해요인이 되는 경우가 포함된다.<sup>168)</sup>

CPSC는 이처럼 전통적인 위해요인이 IoT기반 소비자제품에서도 발생할 수 있다는 것과 연결성, 원격조종가능성 등과 같은 사물인터넷의 특성에 따른 위해요인이 IoT기반 소비자제품에서 추가적으로 존재한다는 것을 명확히 하고 있다. 그리고 CPSC는 제품안전성에 있어서 사물인터넷 제품의 변형가능성이란 특성이 가지는 막대한 영향력은 종래 인식하지 못했던 제품 위해요인에 대한 증폭된 잠재력으로 작용할 수 있음을 인식하고 있다. 제품 구매 후 해당 제품이 변경되기 때문에 특정 제품이 불안전해지는 경우 위해가 발생한다. CPSC는 이와 관련하여 IoT기반 소비자제품의 위해요인에 다음의 것을 추가하여 논의하였다.<sup>169)</sup>

- 악의적인 해킹(Malicious hacking)
- 결함 있는 제3자의 소프트웨어(Defective third party software)
- 결함 있는 제조업자의 업데이트(Defective manufacturer update)
- 소비자 변형(Consumer modification)

일반 소비자제품의 경우, 위해는 통상적으로 자격 없는 자의 무단변경(tampering) 또는 원하지 않은 안전성 장치의 파괴를 원하는 소비자에 의해 발생한다. 또한 장기간의 비합리적인 남용으로 인한 기계적, 열적, 또는 전자적 쇼크가 원인이 되기도 한다. 디자이너가 의도한 사용주기를 초과하여 계속 사용하고 있는 제품에서 통상적인 착용이나 찢어짐이 불안정한 상황을 야기할 수 있다.

168) CPSC Staff Report, 「Potential Hazards Associated with Emerging and Future Technologies」(2017)

169) CPSC, Status Report on the Internet of Things(IoT) and Consumer Product Safety(2019.10.25.), p.8



IoT기반 소비자제품에 있어서 예상하지 못한 잠재적인 위해요인은 장비의 연결성 및 데이터 처리의 불가시성(invisibility)이 직접적인 원인이다.<sup>170)</sup> 소비자들은 통상적으로 구매 후 권한 없는 침해적인 또는 비정상적인 데이터 전송간섭(data transfer interference) 또는 운영 코드 조작이나 소비자-편향적 데이터 조작으로 인하여, 사물인터넷 제품이 위해 또는 사망의 원인을 제공할 수 있다는 사실을 인식하지 못한다. 예를 들어, 로봇 진공청소기가 잘못 설계된 제3자 앱 때문에 자신의 갈 길을 잃어버리고 계단 아래 어린 아이의 머리위로 떨어질 수도 있고 또는 고령자가 거주하는 집에 설치된 난방시스템이 소프트웨어가 해킹되어 추운 겨울 날 작동이 멈출 수도 있다. 이러한 사례에서 소비자는 제품을 변화시키고 위대한 상황을 만드는 데이터 보안 결함을 예측할 수 없다.<sup>171)</sup>

또 다른 개인용 모바일 IoT기반 소비자제품 세계에서 소프트웨어 업데이트 결함이 제시하는 도전과제는 해당 연결된 기기장비가 직접적이 아닌 간접적으로 야기하는 위해이다. 예를 들어, 웨어러블 GPS로 작동하는 시계의 경우 결함 있는 소프트웨어 업데이트는 소비자를 위해한 지역으로 견도록 만들어 낙상이란 위해요인이 발생하도록 만들 수 있다.<sup>172)</sup>

CPSC는 이러한 IoT기반 소비자제품의 위해요인이 제품안전규제자에게 적절하게 대응해야 하는 도전과제를 안겨주고 있다고 보았다. 이러한 위해요인의 통제를 위하여 CPSC는 직접적인 정부개입이나 자발

170) CPSC, Status Report on the Internet of Things(IoT) and Consumer Product Safety(2019.10.25.), p.8

171) CPSC, Status Report on the Internet of Things(IoT) and Consumer Product Safety(2019.10.25.), p.8

172) CPSC, Status Report on the Internet of Things(IoT) and Consumer Product Safety(2019.10.25.), p.8

적인 합의기준을 통한 것이든지 상관없이, 소비자안전을 위한 적절한 방안의 필요성을 강조하고 있다.

## (2) 연방거래위원회(FTC)의 위해요인 분석

미국의 연방거래위원회(Federal Trade Commission, FTC)가 IoT 기반 소비자제품의 위해요인을 직접적으로 다룬 보고서는 아니지만, 2018년 CPSC가 IoT기반 소비자제품의 위해요인에 관한 공개 청문회를 개최하면서 서면의견을 요청했고 이에 FTC가 보낸 답변서에서 이를 다루고 있다.<sup>173)</sup> 연방거래위원회가 직접적으로 IoT기반 소비자제품 위해요인을 다룬 것은 아니지만, 이를 통하여 해당 쟁점에 대한 FTC의 입장을 간접적으로 확인할 수 있다.

연방거래위원회는 IoT기반 소비자제품이 가지는 이점과 함께 위해요인이 동반될 수 있다고 한다. 이러한 위해요인에는 다른 소비자 제품과 동일하게 화재, 화상, 쇼크 및 화학물질 노출을 지적하고 있다.<sup>174)</sup> 연방거래위원회도 CPSC의 IoT기반 소비자제품의 위해요인에 관한 보고서를 인용하면서, 자신들만의 별도의 위해요인 분석 보다는 CPSC의 위해요인 범주에 몇 가지 사례를 추가하고 있다. 이를 정리하면 다음과 같다.

173) Comments of the Staff of the Federal Trade Commission's Bureau of Consumer Protection, In the Matter of The Internet of Things and Consumer Product Hazards, Docket No. CPSC-2018-007(이하 FTC Docket No.CPSC-2018-007)

174) FTC Docket No.CPSC-2018-007, p.2

〈표 3-8〉 연방거래위원회의 위해요인 사례

위해요인	사례
연결 상실 (Loss of Connectivity)	일산화탄소 감지기 또는 화재알람 장치가 인터넷과의 연결이 끊김 <sup>175)</sup> 에 따라 작동이 멈추거나 악성 소프트웨어에 오염되어 자동차 브레이크시스템이 작동하지 않는 경우 위험이 발생할 수 있음
데이터 통합성 (Data Integrity)	의료기기에 관한 오염되거나 부정확한 데이터는 장치의 사용자를 건강위험에 노출시킬 수 있고, 만일 침입자가 연결된 잠금장치, 주차장 문이나 절도 알람 장비에 접근한다면 또한 위험할 수 있음

출처: FTC Docket No.CPSC-2018-007, p.2

연방거래위원회는 IoT기반 소비자제품의 위해요인에 관하여 보안의 중요성을 강조하고 있다. 연방거래위원회는 사물인터넷 환경에서 보안을 강화하는 것이 IoT기반 제품의 개발을 저해할 수 있다는 것을 인식하지만, 보안이 취약한 장비는 소비자 신뢰를 침해하게 된다고 한다.<sup>176)</sup> 또한, 보안에 취약한 IoT 장비는 공격자들에게 기회를 제공하고 안전성 위험을 포함한 위험에 노출시키게 된다고 한다.<sup>177)</sup> 보안위험에 관하여 연방거래위원회는 몇 가지 사례를 제시하고 있다. 이에 관하여 보면, 하나의 사례는 해커가 핀란드에서 주거용 건물 관리시스템인 Mirai botnet을 DDos를 통해 사용한 경우이다. 인터넷 접속을 저지하여, 해커는 인터넷과 연결된 해당 관리시스템을 무한 재부팅하게 만들었고 그에 따라 한 겨울 중에 거주민들은 중앙난방 없이 보내야 했다.<sup>178)</sup> 다른 사례로, 2018년도에 연구자들은 인터넷-연결된 가스충전

175) Richard Speed, Three-Hour Outage Renders Nest-Equipped Smart Homes Very Dumb, The Register (May 17, 2018)

176) FTC, Mobile Security Updates: Understanding the Issues, 1 (Feb. 2018); FTC IoT Report at 20-21

177) Chris Morris, 465,000 Pacemakers Recalled on Hacking Fears, Fortune (Aug.31, 2017)

178) Richard Chirgwin, Finns Chilling as DDoS Knocks Out Building Control System, The Register (Nov.9, 2016)

소 펌프가 원격으로 접근될 때 해커들이 신용카드 정보를 도용할 수 있을 뿐만 아니라 잠재적으로 폭발사고의 원인이 될 수 있는 가스탱크의 온도 및 압력을 변경할 수 있도록 허용하는 취약성이 있다는 것을 발견했었다.<sup>179)</sup>

이처럼 연방거래위원회는 IoT기반 소비자제품의 보안위험은 단지 프라이버시 문제만이 아닌 광의로 안전문제로 함축하고 있는 것으로 판단하고 있다.<sup>180)</sup> 예를 들어, 인터넷과 연결된 홈 네트워크 시스템을 해킹한 범죄자는 해당 집에 살고 있는 소비자에 관한 정보만 수집하는 것이 아니라 홈 보안 장비를 작동시키거나 작동하지 못하도록 만들어 잠재적으로 개인의 안전을 위협할 수도 있다.<sup>181)</sup> 연방거래위원회는 IoT기반 소비자제품을 제조하는 기업이 해당 제품의 보안위험을 다루는 프로그램을 설계하는 경우 해커로부터 프라이버시와 안전성 이슈 모두에 관한 보호를 할 수 있는 조치를 취해야 한다고 지적하고 있다.<sup>182)</sup>

## 2) OECD의 IoT기반 소비자제품 위해요인 분석

상술한 바와 같이 IoT기반 소비자제품은 소비자에게 여러 이점을 제공하지만 동시에 잠재적인 위해요인을 야기하기도 한다. 현재까지 IoT기반 소비자제품의 안전사고에 관한한 소비자 보고는 거의 없는 상태이다. 이는 아마도 사물인터넷 시장이 새로운 것이고 상당히 복잡한 것이

179) Alfred Ng, Hackers Should be Pumped About Gas Station Security Flaws, CNET (Mar.12, 2018)

180) 사실 당시 의견진술 요청서에서 구체적으로 CPSC는 IoT 장비에 관한 보안 및 프라이버시 문제는 다루지 않을 것임을 지적하였음에도, 연방거래위원회는 이를 강조한 것이다.

181) John Leyden, Half Baked Security: Hackers Can Hijack Your Smart Aga Oven 'With a Text Message', The Register(April 13, 2017)

182) FTC Docket No.CPSC-2018-007, p.3

며 현재도 진화하고 있기 때문인 것으로 보인다. IoT기반 소비자제품에 있어서 소비자는 이들 제품을 받아들이고 사용하고 있지만, IoT 기술의 다양한 이해관계자와 시장의 복잡성은 소비자가 제품의 이용과정에서 문제가 발생한 경우 어떤 당사자와 접촉해야 하는지 불확실하게 만들고 있다. 이러한 불확실성이 IoT기반 소비자제품의 법제도적인 관점에서 중요한 정책적 시사점이 된다.<sup>183)</sup>

IoT기반 소비자제품의 안전성 위해요인에 관하여 OECD는 2017년 미국의 소비자제품안전위원회(Consumer Product Safety Commission, CPSC)의 위해요인 분류를 참조하여 위해요인을 대략 4가지로 구분하였다.<sup>184)</sup> 여기에는 i) 소프트웨어 업데이트에 따른 오작동 또는 작동 방식의 변화를 통한 제품의 안전성 손실, ii) 인터넷과의 연결이 끊김과 그에 상응하는 기능의 손실, iii) 안전성 유지에 사용되는 데이터의 손상(corruption), iv) 웨어러블 사물인터넷 기반 장비 및 앱의 물리적인 손상의 잠재적인 위험성 등이 있다. 이에 관하여 살펴보도록 한다.<sup>185)</sup>

#### (1) 결함 또는 업데이트에 의한 오작동

IoT기반 소비자제품도 일반 소비자제품과 마찬가지로 해당 제품이 판매되었을 때 존재하고 있었던 결함이 소비자안전에 대한 위해요인으로 작용할 수 있다. 문제는 이러한 전통적인 제품 결함에 따른 것만이 아니라 사물인터넷이 가지는 연결성이란 특성이 반영되어 발생하는 위해요인이다. 즉, IoT기반 소비자제품은 제조업자가 제품의 출시 후 소

183) 이에 관하여는 후술하는 법정정책적 시사점에서 상세히 다루도록 한다.

184) OECD, 「Consumer Product Safety in the Internet of Things」, OECD digital economy papers March 2018 No.267

185) 이하의 내용은 OECD, 「Consumer Product Safety in the Internet of Things」, OECD digital economy papers March 2018 No.267의 IoT기반 소비자제품 위해요인에 관한 내용을 바탕으로 하여 필자가 정리하여 재구성한 것이다.

소프트웨어 업데이트 또는 패치로부터 발생할 수도 있다는 것이다. 이는 IoT 기술이 가지는 연결성의 양가적인 특성이 반영된 것이다.

다시 말해, IoT기반 소비자제품이 제조공장을 떠나 시장에 출시된 후에도 소프트웨어를 업데이트 할 수 있다는 점은 기회이자 동시에 소비자안전에 위해요인으로 작용할 수 있다. 예를 들어, 소프트웨어가 문제가 있기 때문에 결함이 있는 것으로 판명된 소비자제품이 있다고 가정해 보자. 이 경우 해당 제품이 네트워크에 연결되어 있다면 인터넷을 통해 배포된 소프트웨어 업데이트를 통해 결함을 수정할 수 있을 것이다. 그렇다면 이와는 반대의 경우를 상정해보자. 즉, IoT기반 소비자제품이 최초의 출시 단계에서는 결함이 없었던 장비가 문제가 있는 소프트웨어 업데이트로 인하여 결함이 생길 수도 있다. 만일 소프트웨어가 오작동하게 되는 경우, 이는 해당 제품이 예측하지 못한 불안정한 방식으로 작동하거나 반응하도록 만들어 잠재적인 위해요인으로 작용하게 된다. 게다가 소프트웨어가 해킹되는 경우 역시 해당 제품의 안전성에 영향을 미치게 된다. 예를 들어, 해킹으로 인하여 IoT기반 소비자제품이 기계적으로 작동되지 않거나 가열되도록 작동속도가 높아지거나 낮아지도록 만들 수 있다.<sup>186)</sup>

다른 기술과 연동되어 작동하는 IoT기반 소비자제품일 경우 문제의 복잡성은 더 심화된다. 소프트웨어 변형이 직접적으로 해당 제품이나 소프트웨어의 기능에 영향을 미치는 경우만이 아니라 간접적으로 오작동을 야기할 수도 있다. 이는 해당 제품이나 소프트웨어가 필수적으로 다른 기술과 함께 작동하는 경우, 소프트웨어 업데이트가 해당 제품이 다른 기술과 연동하는 능력을 방해하여 간접적인 방식으로 오작동을 야

186) CertifiGroup(2016), [www.CertifiGroup.com](http://www.CertifiGroup.com) Experts in UL, CSA, CE & amp; International Regulatory Compliance.

기하는 것이다. 이러한 결함은 안전장치와 연결된 기술이 작동하지 않아 발생하거나 해당 제품의 보조 장비가 작동하지 않는 경우에도 발생할 수 있다.

## (2) 연결의 끊김 및 제품 노후화

두 번째 안전성 위해요인은 IoT기반 소비자제품이 인터넷과의 연결의 끊김이다. 이는 IoT기술이 사물과 사물, 사람과 사람, 사물과 사이버 공간 등이 상호 연결되어 작동하기 때문에 네트워크 상태의 단절은 해당 제품의 정상적 작동이 이루어지지 못하는 원인이 되고, 종국적으로는 안전성에도 문제를 야기할 수 있다는 것이다. 만일 IoT기반 소비자제품이 안전하게 작동하기 위하여 사물인터넷과의 연결에 의존하고 있다면, 해당 제품이 연결 끊김 현상이 발생했을 때 “자동안전장치(fail safe)<sup>187)</sup>”가 설계되어 있지 않다면 잠재적으로 안전에 문제가 발생할 수 있다. 이러한 문제는 IOT기반 장비 그 자체가 보호적인 기능을 가진 경우에 더 극명하게 드러난다. 예를 들어, 홈 보안시스템 같은 위험을 제거하거나 감소시키기 위한 장비일 때 만일 시스템이 적절하게 작동하지 않는다면 그 자체로 안전성 위험을 야기하게 된다.

또한, IoT기반 소비자제품의 네트워킹에 관련한 문제로는 “의도적인 노후화(planned obsolescence)” 측면에서 제기되고 있다. 즉, 사물인터넷을 사용하는 기업들이 오래된 제품을 노후화시키거나 작동을 지연시켜 소비자들이 새로운 제품을 사도록 강제하는 것이다. 물론 이러한 문제는 과거 자동차나 전자레인지 같은 제품에서도 제기되었지만, 사물인터넷 영역에서는 더 두드러지게 등장하게 된다. 왜냐하면 앞서 IoT기반 소비자제품의 이점에서 살펴보았듯이, 제조업자들은 해당 제품에 대

187) 고장에 대비한 안전장치 또는 그러한 장치가 구비되어 있는 상태를 의미함.

한 통제력을 더 가지고 있기 때문에 제품의 종기(end the life of a product)를 특정시기로 통제할 수 있기 때문이다. 이러한 제조업자의 의도적인 노쇠화가 해당 IoT기반 소비자제품의 기능저하를 야기하고 이것이 소비자안전에 위해요인으로 작용할 수 있다.

하지만 제조업자의 소비자제품의 존속 기간에 대한 통제력은 동시에 사용자가 제품을 불안전하고 위험에 노출된 상태로 계속 사용하지 못하도록 막는데도 도움을 줄 수 있다. 이런 측면에서 보면, 제조업자는 제품의 종기를 안전하게 관리할 수 있는 기회를 제공받을 수 있고, 이를 통해 제품의 전체 사이클 동안 안전성을 제고할 수 있을 것이다. 따라서 IoT기반 소비자제품의 연결성과 원격조종가능성은 위해요인임과 동시에 이점을 제공하는 양면성이 있으므로, 위해요인으로 작용하지 않도록 만들 필요가 있다.

### (3) 데이터 질 및 진실성 관련 쟁점

세 번째 위해요인은 IoT기반 소비자제품의 안전기능을 지원하는 데 사용하는 데이터의 질과 진실성에 관한 문제이다. 안전 기능이 특정 데이터에 의존하는 경우, 데이터는 정확하고 훼손되지 않아야 한다. 데이터가 부정확하고 훼손되는 경우 안전 기능이 정상적으로 작동하지 않아 위험을 야기하기 때문이다.

데이터 질은 특히 자동화된 결정에 사용되는 데이터가 신뢰할만한 평판이나 데이터 속성 또는 정보출처가 없이 제3자로부터 수집되는 상황에서 사물인터넷과 함께 등장한 문제이다.<sup>188)</sup> 예를 들어, 바코드는 제조업자나 제품을 확인하는데 있어서 유용한 기계가 식별할 수 있는 숫자이다. 그런데 만일 특정 IoT기반 소비자제품이 해당 제품 이외의 제3자로부터 데이터를 전송 받아 안전기능을 지원하는 경우를 상정해 보

188) McAfee(2013), Data Quality in the Internet of Things.



자. 이 때 제3자인 기기가 바코드와 같은 메타 데이터를 잘못 읽어서 생성된 데이터를 송신하는 경우, 이를 받아 사용하는 IoT기반 소비자제품은 정상적인 안전기능을 가지지 못하게 된다. 데이터가 훼손되는 경우 이를 받아 활용하는 IoT기반 소비자제품이 예측할 수 없는 또는 불안정하게 행동하게 만들 수 있는 것이다. 이러한 데이터 질 및 진실성 문제는 IoT기반 소비자제품에서 해킹과 같은 제3자의 의도적인 데이터 훼손행위가 있는 경우 더 문제가 된다. 즉, 사물인터넷에서 해킹과 같은 네트워크 침해가 발생하면 IoT기반 소비자제품이 활용하는 데이터 손상으로 이어지고, 결국에는 해당 제품의 비정상적인 작동이 이를 사용하는 소비자의 안전에 위해요인으로 작용하는 것이다. 이러한 측면에서, 상술한 바와 같이 IoT기반 소비자제품에서 보안문제는 안전성 문제와 중첩되고 밀접한 상호관련성을 가진다. 블록체인 기술의 장점이 이 영역에서 열매를 맺을 수 있고 몇몇의 쟁점을 다루는데 도움을 줄 수 있다. 즉, 블록체인에 저장된 데이터 및 정보는 블록체인이 가지는 분산형 특성에 따라 해킹 및 훼손으로부터 자유로울 수 있다는 것이다. 그러므로 디지털 보안은 IOT가 지속적으로 발전함에 따라 제품안전정책에서 중요한 쟁점이다. 이것은 소비자 프라이버시 쟁점 그 이상의 것인데, 왜냐하면 데이터 진실성 유지는 제품의 안전성 및 제품의 적정한 기능을 제고하는데 핵심적인 것이기 때문이다.

이와 같은 위해요인은 IoT기반 소비자제품이 증강현실 기기와 함께 작동할 때도 발생할 수 있다. 한 가지 가능한 시나리오를 상정하면, 두 장비의 조합이 실제 세계의 사물을 잘못 인식하고 그에 따라 인간을 자신의 안전과는 반대로 행동하도록 만들 수 있다는 것이다. 예를 들어, 사물인터넷과 연결되고 증강현실 기술을 함께 사용하는 장비가 자동차 수선공이 수리할 자동차의 파손 부분을 오인하게 만들어 부정확한 부품

으로 교환하도록 만드는 경우 이러한 오류가 운전자와 행인에게 위험을 야기할 수 있게 된다.<sup>189)</sup>

#### (4) 물리적 위험

웨어러블 기기처럼 IoT기반 소비자제품이 신체에 접촉하거나 근방에 위치하는 경우 소비자들에게 물리적인 위해(injure)를 입힐 잠재적인 가능성이 있다.

미국의 소비자제품안전위원회(CPSC)는 이 범주에 속하는 잠재적인 수많은 위험들을 확인했다. 여기에는 i) 설치된 오디오 장비의 오작동 또는 다른 원천으로부터의 신호에 따른 플레이로 인한 청력손실, ii) 누수되는 배터리 또는 고장난 배터리나 기타 다른 장비에 있는 반응물질로 인한 화학적, 화상이나 피부 손상, iii) 개인의 움직임의 자연적 범위를 벗어난 과격한 외골격 움직임에 의한 근육좌상 등이 있다. 증강현실 장비는 또한 눈의 피로감, 눈의 트라우마, 또는 움직임 피로 등을 야기할 수 있다.<sup>190)</sup> 극단적인 경우, 이들 장비는 심지어 간질발작(epileptic seizures)을 일으킬 수도 있다.<sup>191)</sup>

게다가 IoT 기반 소비자제품의 오작동으로 인해 제공되는 정보에 소비자나 사용자에게 의존하는 경우, 소비자가 혼동에 빠지거나 잘못된 정보를 근거로 행동하게 되어, 그 결과 스스로나 제3자에 위해를 입힐 수 있다.<sup>192)</sup> 예를 들어, 증강현실 기술이 적용된 알람디스플레이를 장착한

189) Tech Policy Lab(2015), Augmented Reality: A Technology and Policy Primer, University of Washington; R. Street(2016), Reality Check: The Regulatory Landscape for Virtual and Augmented Reality.

190) R. Street(2016), Reality Check: The Regulatory Landscape for Virtual and Augmented Reality.

191) Reed Smith LLP (2017), Augmented and Virtual Reality- Emerging Legal Implications of " The Final Platform" Perspectives Reed Smith LLP.

자동차가 정지신호 대신 가상 광고가 알람디스플레이 장치에 보여 지는 경우를 상정해 보자. 이러한 경우 자동차 운전자는 잘못된 정보를 바탕으로 정지가 아닌 운전 상태를 지속하게 되어 그 결과로 사고가 발생할 수 있다. 또는 사용자가 증강현실에 과도하게 몰입되어 실제 세계의 물체를 올바르게 인식하지 못해 걸려 넘어지는 등 스스로에게 위해를 입힐 수도 있다.<sup>193)</sup> 또한, 소비자들이 IoT 기반 장비를 사용하면서 재산적 손해를 야기할 수도 있다. 예를 들어, 원하는 행동을 위한 충분한 현실 세계의 물리적 공간을 확보하지 않은 상태로 증강현실이나 가상현실 기술이 장착된 센서 장비를 조종하면서 주위의 물건 등을 파손할 수도 있다.<sup>194)</sup>

유럽의회는 로봇에 관한 민사법 규칙에 관한 집행위원회에 대한 권고안(2015/2012(INL))의 일부로서, 로봇 사용의 증가에 따른 잠재적인 물리적 안전성 문제에 관한 우려를 표명하고 있다. 이 권고안에서는 “로봇의 코드가 오류가 발생할 수 있는 경우” 또는 “시스템 오류의 잠재적인 결과나 자동화 앱의 사용이 증가하는 시기에 (인터넷과) 연결된 로봇 및 로봇 시스템의 해킹의 경우” 인간은 물리적인 위험에 노출될 수 있다는 점을 지적하고 있다. 특히 로봇 운송수단, 돌봄 로봇 또는 공공질서 유지에 사용되는 로봇에 관련하여서는 이러한 위험의 가능성을 경고하고 있다.

192) Tech Policy Lab(2015), Augmented Reality: A Technology and Policy Primer, University of Washington

193) R. Street(2016), Reality Check: The Regulatory Landscape for Virtual and Augmented Reality.

194) Reed Smith LLP (2017), Augmented and Virtual Reality- Emerging Legal Implications of & quot; The Final Platform&quot; Perspectives Reed Smith LLP.

## 2. 위해요인에 대한 법·정책적 대응

### 1) 미국

미국의 소비자제품 안전을 담당하는 독립규제위원회인 소비자제품안전위원회(CPSC)는 IoT기반 소비자제품의 안전문제에 관하여 지속적인 관심을 보이고 논의를 지속해 오고 있다. 2018년 5월 16일에 위원회는 사물인터넷과 소비자제품 위해에 관한 공개 청문회를 개최하였다. 연방 관보의 공개 청문회를 알리는 공지에서, 행정청인 위원회는 모든 이해관계자에게 사물인터넷 기반 소비자제품과 관련한 잠재적인 안전성 이슈 및 위해요인 뿐만 아니라 이 신기술이 소비자에게 제공하는 이점에 대한 의견을 요청했었다.<sup>195)</sup> CPSC는 이 공개청문회에서 제출된 의견과 기존의 IoT기반 소비자제품의 위해요인에 대한 자신의 분석을 바탕으로 하여 Elliot F. Kaye 명의로 사물인터넷의 안전성 기준에 관한 의견서(Statement of Commissioner Elliot F. Kaye Regarding A Framework of Safety for the Internet of Things)를 공표하였다. 이러한 의견서는 대외적 구속력을 가진 법규명령(legislative rule)<sup>196)</sup>은 아니지만, CPSC가 사물인터넷과 관련한 소비자제품의 안전문제를 다루는 문서라는 점에서 의미가 있다고 할 것이다. 이 의견서는 사물인터넷 장비의 개발 및 사용에 있어서 다양한 이해관계자들이 가능한 최

195) 83 Fed. Reg.13122; Mar.27, 2018

196) 이 의견서는 연방행정절차법상 통지와 의견개진(notice and comment)절차를 거친 규칙이 아니며, CPSC의 수권법에서 명시한 규칙제정절차를 거쳐 제정된 규칙이 아니므로 대외적 구속력(legally binding effect)는 없는 소위 비입법적 규칙(non-legislative rule)으로서 우리법제상으로는 행정규칙에 가깝다고 할 것이다. 다만, 이 규칙은 CPSC의 공식적인 의견이 아닌 Elliot F. Kaye 명의로 공표된 의견서이므로 CPSC 공식적 견해표명으로 보기 어렵다. 이런 점에서 보면 행정규칙도 아닌 비공식적 행정작용(informal agency action)에 속하는 것으로 보아야 할 것이다. 미국 행정입법의 제정절차와 종류 및 구별기준 등에 관하여는 황의관, 앞의 글. 참조.

대한 위해상황을 예견하고 예방하기 위한 절차와 역할의 대강을 다루고 있다. 또한, IoT기반 소비자제품에 관련한 위해성 평가에 포함되어야 하는 사항, 특별한 주의가 필요한 소비자제품에 관한 추가적 논의 등을 포함하고 있다. 이 의견서가 공식적인 법률문서로서 법규성을 가지고 있지는 않지만, 스스로가 인정하듯이 향후 IoT기반 소비자제품 안전문제에 있어서 출발점 역할을 한다는 점에서 상세히 살펴볼 필요가 있다.<sup>197)</sup>

### (1) 제조업자 및 판매업자의 역할 및 책임

의견서에서 사물인터넷 장비 및 소프트웨어의 제조자와 판매자는 사물인터넷 생태계 또는 제품이 폐기물로 수집되거나 재활용되는 시기가 지 사용연한 동안 변형, 업데이트 또는 그로 인한 재구성에 따라 발생하게 되는 추가적인 안전성 위해요인을 예상해야만 한다.<sup>198)</sup> 안전성 안내 활동 및 절차는 제품의 개발단계 동안 이루어져야 하고 해당 제품이 제조되는 경우, 사용을 위해 출시되는 경우, 결함·오류·취약성·오작동 경험과 제조업자에게 보고될 수 있고 구매 후 제품의 수명주기 동안 수정, 변형, 또는 업데이트 될 수 있도록 모든 중요한 순간마다 모니터링 되어야만 한다.<sup>199)</sup>

의견서에서는 IoT기반 소비자제품의 안전문제에 관하여 원론적인 지적을 하고 있다. 즉, 엔지니어, 디자이너(설계자), 프로그래머, 마켓터

197) 이하에서는 CPSC, Statement of Commissioner Elliot F. Kaye Regarding A Framework of Safety for the Internet of Things (2019.1.31)의 내용을 필자가 정리한 사항임을 밝혀둔다.

198) CPSC, Statement of Commissioner Elliot F. Kaye Regarding A Framework of Safety for the Internet of Things (2019.1.31.), p.2

199) CPSC, Statement of Commissioner Elliot F. Kaye Regarding A Framework of Safety for the Internet of Things (2019.1.31.), p.2

및 각각의 관리자를 포함한 제품을 개발하는 모든 전문가들 사이의 협력적인 노력을 통해서만 안전성을 달성할 수 있다. 그리고 의견서는 안전성을 위하여 기업이 결함, 오류, 취약성, 오작동에 관한 외부 보고를 투명하게 수행해야 하며 소비자가 이러한 사항을 기업에게 통지하는 쉬운 방법을 제공해야 한다고 제시하고 있다.<sup>200)</sup>

의견서의 흥미로운 제안 중 하나는 IoT기반 소비자제품의 제조과정에 안전감독관(safety supervisors)을 두도록 하는 것이다. 기업 내에 제품 개발 과정에 영향력을 행사할 수 있는 권한을 가지도록 위탁을 받은 자격을 갖춘 안전감독자가 사물인터넷 기반 제품이 작동하는데 의존하는 소프트웨어의 안전성 등을 포함하여 각 제품 및 제품의 구성요소인 사물인터넷 시스템의 개발 및 마케팅을 감독하는 것이다. 안전감독관은 안전성, 보안문제에 대한 감독권과 함께 안전성과 보안강화를 장려하고 이에 대한 보상조치를 할 수 있을 정도의 권한을 회사 전체에서 행사할 수 있어야 한다. 안전감독관의 권한은 자신이 감독하는 제품의 위험수준에 비례해야 한다. 즉, 잠재적으로 치명적인 제품의 경우 더 강화된 안전성 감독을 받아야 한다는 것이다.<sup>201)</sup>

## (2) 사물인터넷 제품의 개발에 관한 필수적인 평가

의견서에서는 제조업자가 IoT기반 소비자제품을 개발할 때 위험평가 등 필수적인 평가를 할 것을 주장하고 있다. 의견서에서 비록 사용되어야 할 구체적인 위험평가 방식을 여기에서 정의하지는 않았지만, 최선의 실무만이 아니라 다양한 대안의 존재를 고려할 필요가 있다고 한다.

200) CPSC, Statement of Commissioner Elliot F. Kaye Regarding A Framework of Safety for the Internet of Things (2019.1.31.), p.2

201) CPSC, Statement of Commissioner Elliot F. Kaye Regarding A Framework of Safety for the Internet of Things (2019.1.31.), p.2

의견서는 제조업자가 필수적으로 수행해야할 몇 가지 평가를 제안하고 있다. 각각은 다음과 같다.

#### ① 제품 및 제품 시스템의 위험평가 실행

제조업자는 특정한 제품이 작동할 때 예상되는 기능에 관련한 위해, 질병 또는 사망의 가능성과 심각성을 분석해야 한다. 모든 소프트웨어 업데이트 및 해당 제품 수명의 모든 주기에서 발생하는 것을 포함해야 하는데, 여기에는 고장형태 영향분석(a failure modes and effects analysis, FMEA)가 포함된다. FMEA는 사용자 특성 및 신뢰성, 재질 노화효과(material aging effect), 정전(power loss), 예견 가능한 부당변경(foreseeable tampering), 예견 가능한 코드 결함, 오류, 취약성, 오작동, 소비자 변형, 보안위협, 때로는 소위 해킹으로 불리는 것, 그리고 기타 예견 가능한 사용 및 오사용 사건을 고려한다.<sup>202)</sup>

이 위험 평가가 포함해야 하는 것에 관하여 의견서는 몇 가지 사항을 지적하고 있다. 첫 번째로 포함되어야 하는 것은 시스템의 최종 사용자(the intended end user of the system)를 고려해야 한다는 것이다. 여기에는 해당 시스템의 전문적인 사용자와 사용경험이 없는 사용자의 비중, 어린이나 고령자 및 장애인에 의한 사용 및 인간적인 요소들(예를 들어, 인체공학, 인식, 감각, 인지도, 및 행동학적 기대) 등이 포함된다.<sup>203)</sup>

두 번째로는 시스템 내 제품의 모든 구성요소에 대한 평가가 포함된다. 기계적인 하드웨어 및 소프트웨어 요소가 포함되며 설치되는 기대

202) CPSC, Statement of Commissioner Elliot F. Kaye Regarding A Framework of Safety for the Internet of Things (2019.1.31.), p.3

203) CPSC, Statement of Commissioner Elliot F. Kaye Regarding A Framework of Safety for the Internet of Things (2019.1.31.), p.3

환경, 이에에는 제품에 연결된 장비와 그것이 설치될 것으로 보이는 시설 환경(차고지, 부엌, 침실, 차량, 학교 등) 사이의 전자기적, 열적 또는 운동적인 상호작용이 포함된다.

세 번째는 사용자가 원격조종(사용자가 장비가 작동되는 부근에 물리적인 개입행위가 없는 경우)에 따라 해당 제품이 작동될 때 방출되는 에너지 형태(열, 전기, 운동에너지)의 의도되지 아니한 결과를 고려해야 한다.

다섯 번째로 의도적이고 예상할 수 있는 사용 환경에서 다른 사물인터넷 시스템과 주 장비가 의도하지 않은 상호작용을 하는 상황을 고려해야 한다.

마지막으로 의견서에서는 아래의 오작동 형식의 의도되지 아니한 결과를 고려해야 할 것을 지적하고 있다.<sup>204)</sup>

- 제조상의 결함
- 소프트웨어 업데이트 실패
- 소프트웨어 업데이트 중 데이터 훼손
- 기타 데이터 또는 코드 훼손(센서 노획화, 손상 또는 전원 상실; 보안 위협/부당변경; 소비자 변형)
- 의도하지 아니한 움직임
- 불안정한 상황에서 의도적인 움직임
- 경고 없는 개별화 표시 없는 디폴트
- 아래의 원인에 의한 중요한 안전기능의 작동실패
  - 연결 끊김
  - 예견 가능한 시스템 요소와의 불일치

204) CPSC, Statement of Commissioner Elliot F. Kaye Regarding A Framework of Safety for the Internet of Things (2019.1.31.), pp.3~4



- 전원 서지(급증) 또는 정전
- 노후화
- 노쇠화
- 기타 기능 저하(센서 노쇠화, 손상, 또는 정전; 위협/부당변경;  
소비자 변형)
- 사용자 과실 또는 오용(User error or misuse)

## ② 안전성 중요도에 관한 제품의 구성요소 평가

의견서에서는 IoT기반 소비자제품의 구성부분이 안전성 확보를 위해 기여하는 중요도에 대한 평가의 필요성을 강조하고 있다. 즉, 모든 설치된 소프트웨어를 포함하여 각 중요한 구성요소가 안전한 작동, 안전한 업데이트, 제품의 안전한 사용에 어떻게 작용하는지를 평가해야 한다는 것이다.<sup>205)</sup>

IoT기반 소비자제품에서 중요한 구성요소로는 전력 공급 장치, 센서, 소프트웨어, 소프트웨어 업데이트, 사용자 인터페이스, 감독회로, 전기 하우징 등이 포함된다. 안전성에 있어서 중요한 것으로 인정되는 요소들은 반드시 자신의 안전성에 관한 중요한 수준에 수반되는 통제에 종속되어야만 한다.

의견서에서는 제품의 개발 전체를 통해서 적절한 시기에 안전성 중요도 평가를 문서화하여 하드웨어 및 소프트웨어 설계 또는 제조과정 모두에서 변경이 있을 때 간과되지 않도록 해야 한다.<sup>206)</sup>

205) CPSC, Statement of Commissioner Elliot F. Kaye Regarding A Framework of Safety for the Internet of Things (2019.1.31.), p.4

206) CPSC, Statement of Commissioner Elliot F. Kaye Regarding A Framework of Safety for the Internet of Things (2019.1.31.), p.4

### (3) 기타 논의사항

#### ① 안전성 위험에 대한 잠재적인 대처방안

의견서에서는 안전성 위험요인에 대한 대처방안으로 활용할 수 있는 수단을 열거하고 있는데, 구체적으로 어떠한 방안이 IoT기반 소비자제품의 안전성 확보를 위해 최적의 수단인지에 대하여는 언급하고 있지 않다. 각각의 방안도 제품안전영역에서 종래 통상적으로 활용되어 왔던 것이 대부분이다. 따라서 각각의 방안을 열거한 것은 IoT기반 소비자제품의 안전성 확보를 위해 종래 사용하던 수단 중에서 이러한 것들을 활용할 수 있다는 입장을 피력한 것으로 볼 것이다. 의견서에서 제시한 안전성 위험에 대한 대처방안은 다음과 같다.<sup>207)</sup>

#### ㄱ. 구성요소의 인증

모든 안전성의 중요한 구성요소들은 적절한 산업표준, 규칙 또는 해당 구성요소와 관련한 최선의 실무, 그들의 코드 안전성 평가를 포함하여, 등을 통하여 유효하고 인증되는 것이어야 한다.

#### ㄴ. 경고 및 지시문

경고 및 지시문은 위험요인 제거 또는 전략안내와 같은 다른 더 신뢰할 수 있는 개입형식이 불가능한 경우에만 인정될 수 있다. 경고는 수많은 미디어 형식으로 소비자에게 제출될 수 있다.(제품 자체의 글자 및 그림, 복사본 문서 또는 전자미디어 형식 등)

#### ㄷ. 부모의 통제

집안에서 사용되는 제품은 특정한 상황에서 아이들이 접근할 수도 있다고 예상된다. 아이들의 사용을 막기 위해 양육자들이 패스워드나

207) CPSC, Statement of Commissioner Elliot F. Kaye Regarding A Framework of Safety for the Internet of Things (2019.1.31.), pp.4~6

다른 이용권한 징표, 물리적인 장애물 또는 기타 수단을 사용할 수 있도록 만드는 것을 고려해야 한다.

#### ㄹ. 사용자 권한허용 및 확인(User Authentication and Confirmation)

작동하기 전에 사용자로부터 확인 반응(affirmative response)을 요구하도록 명령하는 것은 잠재적으로 위해한 사건 또는 주변 환경과 상치되는 의도하지 아니한 작동을 예방하는데 도움이 된다. 안전성에 중요한 기기인 경우에는 센서가 불안정한 상황을 파악한 경우, 다시 안전한 상태로 해당 상황이 돌아갈 때 까지 작동 확인이 저지되어야 한다.

#### ㄱ. 추가적인 안전장치

잠재적인 안전장비를 통제하는 센서 또는 작동장치(actuators)는 작동 실패를 방지하기 위해 백업 또는 이차적인 시스템을 가지고 있어야 한다. 감독회로(supervisory circuits)는 전기적인 실패의 효과를 감소시킬 수 있다. 가능하다면, 소프트웨어 안전장치 보다는 물리적인 추가적 안전장치가 더 우선되어야 한다.

#### ㄴ. 정보보안

산업계 및 정부 전문가들이 제품 설계, 제조공정 및 사용 전반에 걸쳐 적용되는 정보보안에 관하여 산업계 및 정부 전문가들이 권고하는 최선의 실무를 항상 준수해야 한다.

#### ㄷ. 구성요소 추적을 위한 소비자정보

리콜이나 제품안전성 문제가 공표된 기간 동안 사용을 위한 수명 내에 걸쳐있는 제품의 위해요인 및 제품 업데이트 추적이 가능하도록 장비의 구성요서의 원천을 결정할 수 있는 적절한 정보를 소비자에게 제공해야 한다.

#### ○. 데이터 수집에 관한 소비자정보

데이터 수집, 공유, 및 사용에서의 투명성 제고를 위하여 소비자가 자신의 데이터에 관한 결정(처리)정보를 제공받아야 하고 데이터의 재목적화에서 발생할 수 있는 잠재적 위험정보를 제공받아야 한다. 분명한 프라이버시 정책설명도 제고해야 한다.

#### ㄷ. 제품의 기대수명에 관한 소비자정보

제품의 기대수명 및 제조업자가 보증을 제공할 수 있는 분배 후 기대되는 내구연한을 제공해야 한다. 대부분의 경우 중요한 것은 기대수명보다 제품을 오래 사용하는 것의 장배적인 위험에 관하여 명확한 설명을 제공하는 것이다. 기대수명은 구매 시점에 알려지지 않을 수 있지만 해당 정보가 공개되는 경우에는 업데이트로 소유자에게 제공되어야 한다.

### ② 특정 제품군에 관한 추가적인 안전성 고려사항

의견서에서는 특정 제품군의 경우 추가적으로 안전성에 대한 고려가 필요하다는 점을 지적하고 있다. 의견서에서 제시하고 있는 제품군 리스트가 완전한 것은 아니지만 최초의 제품 평가를 위한 출발점을 제공할 수 있을 것이다. 의견서에서 지목한 제품군별로 추가적으로 고려해야 할 안전성에 관하여는 다음과 같다.<sup>208)</sup>

#### ㄱ. 신체에 입거나 이식되는 제품(“웨어러블”또는 임플란트)

정보보안 및 프라이버시, 청각 위해(acoustic hazards), 열에 의한 화상 위해, 화학적인 화상, 독성물질 노출, 알레르기 반응, 섭취 위해, 전기 피부 반응(galvanic skin response), 땀의 잠재적인 효과, 장비의 맞춤 및 편리성에 관한 잠재적인 변형, 사용자의 감성의 환경적 고립 및

208) CPSC, Statement of Commissioner Elliot F. Kaye Regarding A Framework of Safety for the Internet of Things (2019.1.31.), pp.6~9

사용자의 혼란에 대한 잠재성, 특히 안전에 중요한 행위 중에 발생할 수 있는 것. 동전모양 배터리나 리튬이온 배터리와 같은 전력원천의 경우 안전한 사용방법에 관한 특별한 지시문이 필요하다. 의료기기 또는 의학적 기능을 가진 소비자 장비는 FDA 안내지침 및 적용되는 규정을 준수해야만 한다.

결함, 오류, 취약성, 오작동, 제품의 작동조작, 과잉 가열, 화재 및 잠재적인 범죄화/무기화로 이어지는 위험을 통제해야 한다.

#### ㄴ. 간호에 사용되는 제품(아기 모니터, 연결되어 있는 유아용 제품들)

정보보안 및 프라이버시, 소음, 노끈에 관한 목 졸림, 빛 노출, 열 위험(온기 및 냉기), 그리고 봉제제품에서의 질식, 위치상의 가사(질식에 의한 가사상태를 말함, positional asphyxia), 작은 물건 및 뾰족한 모서리의 위험을 관리해야 한다. 결함, 오류, 취약성, 오작동, 제품의 작동 조작, 과잉 가열, 화재 및 잠재적인 범죄화/무기화로 이어지는 위험을 통제해야 한다.

#### ㄷ. 사적 공간에 사용되는 제품(홈 시큐리티 및 모니터링 장비, 목소리로 작동하는 스피커)

정보 보안 및 프라이버시를 다루어야 한다. 제품 수명주기에 대한 신뢰성, 정전, 노후화, 인터넷과의 연결 끊김, 업데이트 중 기능훼손이나 방해의 위험을 다루어야 한다. 결함, 오류, 취약성, 오작동, 제품의 작동 조작, 과잉 가열, 화재 및 잠재적인 범죄화/무기화로 이어지는 위험을 통제해야 한다.

#### ㄹ. 공개 공간에서 사용되는 제품

결함, 오류, 취약성, 오작동, 제품의 작동조작, 과잉 가열, 화재 및 잠재적인 범죄화/무기화로 이어지는 위험을 통제해야 한다.

#### ㉠. 자동차에 사용되는 제품들

운전자의 혼란을 야기하는 위해요인을 다루어야 한다.

극한의 온도/냉기, 떨림(vibration), 자동차 기능 및 주변 자동차에 대한 전자기적 개입, 에어백이나 안전벨트와 같은 충돌보호 장비와의 상호작용, 자동차 내의 스마트 자동차 시스템과의 의도되지 않은 상호작용 및 통합 그리고 지역이나 국가 교통시스템 또는 도로의 다른 자동차의 해당 시스템과의 동일한 위해요인을 관리해야만 한다.

결함, 오류, 취약성, 오작동, 제품의 작동조작, 과잉 가열, 화재 및 잠재적인 범죄화/무기화로 이어지는 위험을 통제해야 한다.

#### ㉡. 극한 환경에서 사용되는 제품들

해당 제품이 전체 수명주기 동안 경험하게 될 극한의 조건 및 예상되고 예견 가능한 오사용(misuse) 환경을 예측할 것.

결함, 오류, 취약성, 오작동, 제품의 작동조작, 과잉 가열, 화재 및 잠재적인 범죄화/무기화로 이어지는 위험을 통제해야 한다.

#### ㉢. “내재적 위해요인”에 연계되는 제품들

이 부류에는 에너지 또는 독성물질을 방출할 수 있는 제품들이 포함된다. 즉, “스스로가 위해요인”인 제품이다. 이에는 스토브(난로), 오븐, 용광로, 벽난로, 토스터기, 다리미, 잔디 깎는 기계, 의약품 용기, 파이프라인/탱크 밸브, 문, 엘리베이터, 리프트 기타 등등이 포함된다. 의견서에서는 이러한 내재적 위해요인을 가진 제품에 대하여 상당히 세부적으로 안전성 고려사항을 설명하고 있다.

##### i) 위해요인을 방출하거나 작동하도록 의도된 제품

- 사고와 같은 작동을 통제해야 한다.<sup>209)</sup>(모든 작동기계 및 이에

209) 예를 들어, 약물투여 장비가 너무 자주 작동하여 환자에게 과도한 약물이 주입

대한 통제요소에 관한 권한승인 및 확인에 관한 프로토콜을 고려해야 한다.

- 사용자의 직접적인 감독이 없는 상태로 의도적인 원격 작동의 위험을 다루어야만 한다.(식기 수건을 난로 위에 둔 채로 난로를 작동시키면 수건이 화재 원인이 됨)
- 의도적이지 않은 원격 작동 및 자동 작동의 위험을 다루어야만 함
- 결함, 오류, 취약성, 오작동, 제품의 작동조작, 과잉 가열, 화재 및 잠재적인 범죄화/무기화로 이어지는 위험을 통제해야 한다.

ii) 내재적인 위해요인을 야기하도록 의도된 것은 아니지만 소비자가 의도하지 아니한 방식(예견할 수 있는 사고 또는 범죄)으로 사용할 수 있는 제품의 내재적 위해요인을 통제해야 한다.

- 위험한 제품과 연계될 수 있는 것을 저지할 수 있는 모듈이나 시스템적인 설계를 해야 한다.<sup>210)</sup>
- 가능한 위해요인에 상응하는 대응조치와 함께 의도하지 않은 작동 위험을 다루어야만 한다.
- 결함, 오류, 취약성, 오작동, 제품의 작동조작, 과잉 가열, 화재 및 잠재적인 범죄화/무기화로 이어지는 위험을 통제해야 한다.

iii) 위해요인에 반응하는 제품들

이 범주에는 위해가 있는 사건이 발생하면 공중보건이나 질병위험으로부터 공중을 보호하기 위하여 반응하는 제품이 포함된다.  
(화재 스프링클러, 에어백, 일산화탄소 감지기, 인슐린 주입기 등)

되는 경우: 포켓 다이얼이 작동하여 저장탱크가 가스를 방출하거나 오븐 같은 것에서 열기가 방출되는 경우

210) 예를 들어, 전기 콘센트에 간단한 on/off 스위치를 부착해서 해당 콘센트에 장착되는 모든 것에 활용되도록 하여, 내재적 위해요인을 포함하고 있는 히터나 전기용품에 사용하도록 함

- 제품수명주기(노후화 효과), 정전, 노쇠화, 연결 끊김, 업데이트 동안의 기능 훼손이나 방해에 관한 신뢰도를 확보해야 한다.
- 적절한 공학적인 추가장치, 사고시 안전장치(fail-safes), 그리고 감독회로 및 다른 통제회로로서 중요한 작동실패를 제한하기 위한 것을 고려해야 함
- 신뢰도 문제를 야기할 수 있는 잘못된 알람이나 의도하지 않은 작동을 관리해야 한다.(거짓 경고, crying wolf)
- 결함, 오류, 취약성, 오작동, 제품의 작동조작, 과잉 가열, 화재 및 잠재적인 범죄화/무기화로 이어지는 위험을 통제해야 한다.

#### iv) 사용자를 주위 환경으로부터 격리 시키는 제품

이런 범주에 속하는 제품은 사용자의 감각을 커버하거나 관여하는 것이다.(가상현실 또는 증강현실 장비, 오디오 플레이백 장비 등)

- 기대되는 사용 조건/환경 및 예측 가능한 오사용 조건들을 다루어야 함
- 격리시키는 작동을 실행하기 전 또는 하는 동안 경고를 할 것
- 결함, 오류, 취약성, 오작동, 제품의 작동조작, 과잉 가열, 화재 및 잠재적인 범죄화/무기화로 이어지는 위험을 통제해야 한다.

#### v) 사용자 또는 주변인을 혼동시키는 제품들

- 기대되는 사용 조건/환경 및 예견 가능한 혼동의 효과를 다루어야 함
- 혼동을 시키는 제품 특성을 작동하기 전 또는 하는 동안 경고를 할 것
- 결함, 오류, 취약성, 오작동, 제품의 작동조작, 과잉 가열, 화재 및 잠재적인 범죄화/무기화로 이어지는 위험을 통제해야 한다.



vi) 사람들을 모니터하는 제품들

이런 범주에 속하는 제품은 타인을 보거나, 듣거나, 위치 추적을 하도록 만들어진 제품이다.

- 정보 보안 및 프라이버시를 다루어야 한다.
- 결함, 오류, 취약성, 오작동, 제품의 작동조작, 과잉 가열, 화재 및 잠재적인 범죄화/무기화로 이어지는 위험을 통제해야 한다.

## 2) OECD

### (1) 문제의 제기

OECD 차원에서 IoT기반 소비자제품의 위해요인에 대한 법제적 대응방안을 구체적으로 마련하는 것은 아니다. 사물인터넷 기술은 그 자체가 발전하는 과정에 있는 새로운 것이고 IoT기반 소비자제품의 안전성에 관한 구체적인 사례가 있는 것도 아니기 때문이다. IoT 기반 소비자제품의 안전성 문제는 현재 논의의 시작단계에 있고, 향후 지속적인 논의를 통해 이와 관련한 국제적 규범을 형성해 가는 과정에 있다. 하지만 그렇다고 해서 OECD가 IoT기반 소비자제품의 안전성 제고를 위한 법제적 대응방안을 고려하지 않고 있는 것은 아니다. 논의의 시작단계에 있을 뿐 지속적인 관심을 가지고 살펴보고 있다.

OECD의 경우 앞서 살펴본 바와 같이, IoT기반 소비자제품의 위해요인을 범주화하고 있으며, 이러한 위해요인이 소비자안전법제에 어떠한 영향을 미치게 될 것인지를 논의하고 있다. 즉, IoT기반 소비자제품의 안전성 강화를 위한 구체적인 법제개선방안을 마련하고 있지는 않지만 해당 제품의 위해요인을 조사하고 이것이 가지는 법정정책적 의미를 다루고 있는 것이다. 이는 기존의 소비자안전법제에 IoT기반 제품이 미치는 영향을 분석하는 것으로서 종래의 법체계와 새로운 규제대상 사이의 긴장관계를 보여주는 것이다. 따라서 향후 IoT기반 소비자제품 안전강화를 위한 구체적인 법제개선방안을 도출하기 위한 전단계 과정의 논의로 볼 것이다. 따라서 구체적인 법제대응방안은 아니지만 IoT기반 소비자제품의 위해요인이 소비자안전법제에 미치는 법정정책적 시사점에 관한 OECD 입장을 살펴보는 것은 향후 법제적인 개선방안에 대한 이정표로서 기능할 것이다.

한편, IoT기반 소비자제품의 안전성 강화를 위한 새로운 정책적 대응 방안이 필요한지에 관하여는 논란이 있다. 새로운 제품 기술이 소비자들에게 위험을 야기할 수 있다는 사실만으로 새로운 정책적 대응이 필요한 것은 아니다. 소비자는 광범위한 영역의 위험에 적용되는 견고한 제품안전 법률, 명령, 및 기준에 따라 잘 보호 받고 있다. 대부분 국가에서 제품안전 법령들은 소비자가 불안정한 제품으로 인해 피해를 입은 경우 해당 제품을 시장에 출시한 제조업자나 판매자로부터 배상을 받을 수 있는 법제도를 근간으로 한다. 현존하는 제품안전 및 제조물책임법제는 IoT를 포함한 새로운 기술이 제기하는 문제들을 다루는데 적절할 수 있다. 2015년 보고서에서, 사물인터넷혁신을 위한 연맹(the Alliance for Internet of Things Innovation, AIOTI)은 비록 특정한 사물인터넷 기반 제품과 관련한 법규준수, 제조물책임 및 보험 등의 영역에서 특별히 고려할 점이 있음에도 불구하고, 새로운 입법이나 규제에 대한 명확한 필요성은 없다고 결론지었다.<sup>211)</sup>

또한, AIOTI는 현존하는 규제체제를 수정하기 전에 심도 있는 생각과 토론이 이루어져야만 하고 소비자안전을 달성하고자 하는 목적은 사물인터넷 시장에서의 혁신을 자극하는 것과 균형을 강조했다.<sup>212)</sup> 이러한 주장은 사실 새로운 것은 아닌데, 제품규제체제가 기술발전에 적절하게 반응하여 충분히 적응하는 과정에서 항상 제기되어왔던 주장이다. IoT분야에서 도전과제는 가파른 기술발전 속도에 맞추어서 규제체제도 그에 상응하는 속도로 적응하도록 만들고, 동시에 기술에 따른 이익이 현실화 될 수 있도록 허용하면서도 소비자보호를 지속할 수 있도록 예

211) Alliance for Internet of Things Innovation (AIOTI) (2015), Working group 4 Report on Policy Issues

212) Alliance for Internet of Things Innovation (AIOTI) (2015), Working group 4 Report on Policy Issues

측해야 한다는 것이다.

OECD는 IoT기반 소비자제품의 위해요인이 소비자안전법제에 미치는 법정책적 쟁점으로 다음과 같은 3가지를 제시하고 있다. 이에 이하에서는 OECD의 이러한 논의를 중심으로 살펴보기로 한다.<sup>213)</sup>

- “하드웨어(hardware)” 및 “소프트웨어(software)”, “제품(product)” 및 “서비스(service)” 사이의 구분에 관하여 IOT가 미치는 영향
- 제품안전에 관한 책임을 누가 부담할 것인가, 책임의 범위는 어디까지인가, 그리고 제품사고가 발생했을 때(in the event of failure) 책임을 어떻게 배분할 것인가?
- 소비자들과의 안전성 소통

## (2) 재화와 서비스 사이의 구분 문제

IoT기반 장비의 전형적인 구성요소는 하드웨어, 소프트웨어, 그리고 상호 소통하는 프로토콜/스탠다드이다. 일반적인 수준에서, 여기서 “하드웨어”란 것은 장비 또는 장비의 한 무리(a set of devices) 또는 본질적으로 (수동적으로) 반응하는 물리적 객체이고 데이터를 회수하고 지시를 따르는 것을 말한다. “소프트웨어”란 하드웨어의 구성부분으로부터 데이터를 수집, 저장, 처리(processing), 조종(manipulating) 및 지시하는 프로그램의 한 무리(a set of programs)를 의미한다. 사물인터넷은 사용자가 스마트 데이터에 접근하고 원격으로 통제할 수 있도록 하고 장치가 자동적으로 제품디자이너나 사용자의 통제 없이 투입된 데이터를 통해 학습할 수 있도록 함으로서 하드웨어나 소프트웨어 모두에

213) 이하의 OECD의 IoT기반 소비자제품의 위해요인에 관한 법정책적 대응논의는 OECD, 「Consumer Product Safety in the Internet of Things」, OECD Digital Economy Papers(2018) No.267의 해당부분을 중심으로 필자가 정리하여 재구성한 것이다.

게 있어서 공간적 제약을 약화시킨다.

통상적으로, 제품안전 규제 및 책임법제 체제는 “재화”의 공급과 “용역”의 공급을 구분하고 각각의 경우를 다르게 규율하고 있다. 기술 분야에서, 이러한 구분은 “하드웨어”와 “소프트웨어”의 구분에 관한 논쟁과 법적 쟁점으로 이어지는데, 특히 소프트웨어가 “재화”로 간주될 수 있는지 여부와 그에 따라 제품안전 및 제조물 책임법제에 해당하는지 여부와 관련된다.<sup>214)</sup> 사물인터넷은 이와 관련하여 전적으로 새로운 쟁점을 제기하는 것은 명백히 아니다. 그러나 사물인터넷이 하드웨어와 소프트웨어 사이의 작동방식에 있어서 복잡성을 상당히 높인 것은 사실이다. 즉, 제품의 행동이 여러 측면에서 변화하는 소프트웨어와 해당 제품에 내재되어 있거나 외부의 변화하는 데이터에 높은 의존도를 보이기 때문이다.

이러한 요소들이 필수적으로 상술한 구분의 근본적인 분석을 변화시키는 것은 아니지만 잠재적으로 더 정확하고 명확한 구분의 필요성을 야기하고 그에 따라 정책입안자와 집행자에게 매우 큰 도전과제를 제기한다. 사물인터넷 장치 또는 앱은 재화와 용역이 혼합된 것이기 때문에, 제품안전 및 제조물 책임법이 적용되는 영역(범위)를 확정하는데 있어서 법원이나 제품안전 행정청이 어려움을 겪을 수 있다. 예를 들어, 현존하는 제조물책임법 체제는 “사물인터넷 시스템을 통한 데이터 제공 행위”를 용역으로서 포섭할 수 없다.<sup>215)</sup> 일부 법제에서(예를 들어, 오스트리아, 독일, 및 스위스), 법원은 디지털 콘텐츠를 일반적으로 재화와 동일한 방식으로 취급한다. 반면에, 다른 법제에서, 예를 들어 영국,

214) Alliance for Internet of Things Innovation (AIOTI) (2015), Working group 4 Report on Policy Issues

215) Medium (2017), IOT Raises New Challenges for Assigning Liability

CD와 같은 유형 미디어를 통해 공급되는 소프트웨어와 무형의 미디어, 예를 들어 인터넷을 통한 다운로드,를 통해 공급되는 소프트웨어를 구분한다. 전자에서는 재화의 판매로 보지만 후자의 법제에서는 그렇지 않다.<sup>216)</sup> 이것은 소비자권리 및 구제에 있어서 중요한 함의를 가지는데, 왜냐하면 만일 소비자가 결함 있는 재화(제품, goods)으로 피해를 입은 경우, 그는 해당 제품의 교환, 환불 또는 손실에 대한 대상을 청구할 권리가 있다. 그러나 동일한 규칙은 만일 소비자가 “용역, 서비스(service)”간주되는 “사물(thing)”로 인해 피해를 입은 경우에는 적용되지 않는다. 그러한 경우(용역에 의한 피해)에 소비자는 손해배상을 청구하는데 있어서 더 낮은 보호원칙에 의해 규율된다.

제조물 책임법제 맥락에서, 이러한 문제들은 특별히 중요한데, 왜냐하면 여러 법제에서, 예를 들어 유럽연합(EU), 미합중국 등, 제조물 책임법제에 무과실 혹은 엄격책임 제도를 도입하고 있기 때문이다.<sup>217)</sup>

게다가 사물인터넷 기반 장비 및 앱에서 하드웨어와 소프트웨어의 교차하는 소비자안전의 보호란 관점에서 기회이자 도전과제를 제시하고 있다. 전통적으로, 하드웨어 개발자는 결함에 따라 발생할 수 있는 잠재적인 수많은 부정적 결과를 회피하기 위해 최종적이고 완전한 버전의 제품을 출시한다. 소프트웨어 개발자는 만일 어떤 결함이 발견되면 소프트웨어 패치 방식으로 손쉽게 결함을 치유할 수 있다는 점을 인식하고 새로운 제품을 시장에 출시한다. 이 경우 소비자에 관한 개입이 거의 없이 결함은 추적이 가능하다. 제품에 결함이 있는 경우, 제조업자는 블록체인을 사용하여 결함을 더 용이하게 추적하고 효과적인 교정조치를 취

216) OECD(2013), “Protecting and Empowering Consumers in the Purchase of Digital Content Products”, OECD Digital Economy Papers, No.219, OECD Publishing, Paris.

217) Alliance for Internet of Things Innovation(AIOTI) (2015). Working group 4 Report on Policy Issues.

할 수 있다.

IoT 제품의 발전은 이런 전통적인 두 가지 위상의 중간에 위치하는 제품의 범위와 시장을 확대시키고 있다. 제품의 운용과 기능에 대한 소프트웨어의 통제가 확대된다는 사실은 소프트웨어에 근거한 예측하지 못한 결함의 발생확률을 높이고 그러한 결함이 소비자에 대한 피해가 없이 원격으로 교정될 수 있다는 것을 의미한다. 이러한 새로운 복잡성은 제품안전에 대한 책임이 어떻게 다루어져야 하고 제품이 위해를 야기하는 사고가 발생한 경우 법적책임을 어떻게 분배해야하는지에 관하여 흥미롭고 잠재적으로 중요한 정책적 문제를 야기하고 있다.

### (3) 법적 책임의 문제

전자상거래에서 소비자보호에 관한 OECD 권고 2016(“the OECD E-commerce Recommendation”)에서 강조했듯이, “전자상거래 관계자들 사이에서 소비자보호에 대한 책임을 적절하게 분배하는 것은 소비자후생 및 소비자신뢰 제고를 위해 핵심적인 것이다.<sup>218)</sup> 그러나 전통적인 제품안전 및 책임 개념이 IoT기반 장비 및 앱에는 정확히 대응되지 않는다. 상술한 바와 같이, 이들 제품은 데이터 침해, 또는 제3당사자의 장비나 앱의 오작동에 의하는 등 무수히 많은 방식으로 결함이 발생하거나 불안전해질 수 있다. 게다가 이런 장비들은 당해 장비의 안전성이 약속되지 않은 채로 방해받지 않는 연결성에 의존하게 된다.(또는 장비가 결함이 있는 경우, 만일 장비가 결함이 있어서 이의 수정을 위한 소프트웨어 업데이트를 기다리고 있을 것이다.)

인공지능에 의하여 작동되는 경우, 이런 장비나 앱은 인간의 개입 없이도 행위하고, 예상하고, 그리고 결정을 예측할 것이다. 따라서 소비자

218) OECD(2016), Recommendation on Consumer Protection in E-Commerce, OECD Publishing, Paris.

제품 안전 규정 및 기준, 책임규칙은 제품안전이유를 야기하는 위해요인을 효과적으로 다루지 못할 가능성이 있다.

#### ① 책임 주체의 문제

예를 들어, 만약 제3의 소프트웨어가 장착되어 있는 제품이 최초 시장 출시 때는 결함이 없었지만 제3자에 의한 업데이트의 결과로 해당 제품이 예측하지 못한 제품안전위험이 발생했을 때 어느 당사자가 책임을 부담해야하는지가 명확하지 않다. 만일 제품의 움직임이 인공지능을 통해 생성된 데이터에 영향을 받거나 통제되는 경우에는 문제가 더욱 복잡해지게 된다. 인공지능은 광범위한 원천으로부터 생산된 대량의 데이터에 의존하기 때문에, 어떤 제품이 왜 그러한 방식으로 행동했는지를 어느 당사자도 이해하기가 매우 어렵고 거의 불가능하다. 제품안전 의무준수 단계에서, 장비와 입의 고도의 통합수준과 IoT 생태계의 복잡성을 고려할 때, 최초의 제품안전의 보장의무를 누가 부담할지, 요구되는 안전보증 범위가 어디까지 일지, 그리고 제품안전에 대한 보증 책임을 부담하는 자가 언제까지 이를 부담할지를 결정하는 것은 어려운 일이다. 유럽집행위원회(EC)는 자신들의 보고서인“유럽에서 사물인터넷의 진보<sup>219)</sup>에서 이러한 이슈들을 구체적인 쟁점으로 취급하였다. 이러한 문제가 새롭거나 사물인터넷에 고유한 것은 아니다. 그러나 사물인터넷 기술의 복잡성과 소프트웨어 및 데이터에 따라 통제되는 제품의 범위가 확대되어 가는 것을 고려할 때, 이러한 문제가 정책적인 관점에서 상당히 중요한 쟁점으로 등장하는 것도 분명하다.

따라서 복잡한 쟁점요소는 사물인터넷 장비나 앱이 그 자체의 설계상 특성에 따라 일반적으로 자신들의 기능 및 소비자에 최대의 이익을 제공하기 위해서는 제3자의 기술에 의존한다는 점이다.<sup>220)</sup> 그리고 제품의

219) European Commission(2016), Advancing the Internet of Things in Europe



운영 및 안전성이 시장 출시 후 제3자에 의하여 대체될 수 있다는 것이다. 즉, 잠재적으로 제조업자의 제품에 대한 지식이나 통제를 벗어나는 상황이 가능하다는 점이다. 이러한 점은 미합중국 규제자의 이목을 집중시키고 있다.

예를 들어, 미국의 CPSC는 “제품의 안전성뿐만 아니라 제품이 다른 장비의 운영에 부정적 영향을 미치는 것”에 초점을 맞출 것이라고 언급했다.<sup>221)</sup>

게다가 이러한 상호의존은 장비나 앱의 제품주기를 연장하고 복잡성을 증진시킨다. 이에 더하여, 하드웨어 또는 소프트웨어의 공급자가 해당 제품이 디지털 보안공격으로부터 보호되도록 할 책임을 어느 범위까지 부담할지의 문제도 등장한다. 이것은 특히 범죄를 목적으로 불법적인 데이터 접근을 지속적으로 저지르는 사이버 범죄 세계에서 제조업자가 계속해서 패치를 개발하고 제품의 보호를 위한 조치를 취하도록 강제하는 쟁점을 제기한다.

## ② 책임의 분배문제

제품안전에서 고려해야 할 사항과 중첩되는 것이 제품의 결함이나 과실로 손해를 야기하는 사건이 발생했을 때 배상책임을 어떻게 배분할 것인지 이다. 제품안전 정책이 제품안전 체제와 제조물책임 체제 사이의 차이가 있는 방식으로 발전할 때 비효율성이 발생할 수 있기 때문에, 제품안전과 배상책임의 문제를 함께 고려해야 한다. 책임의 분배문제는 결국 두 가지로 귀결되는데, 이는 i) 안전성 및 의무준수에 책임을 지는 당사자의 확정 및 그러한 책임의 범위에 관한 것, ii) 수용할 수 있

220) Alliance for Internet of Things Innovation(AIOTI) (2015). Working group 4 Report on Policy Issues.

221) Consumer Product Safety Commission(2017), Potential Hazards Associated with Emerging and Future Technologies.

는 안전성 수준이 무엇인지에 관한 문제이다.

IoT생태계에서 재화 및 서비스 생산자, 행위자 그리고 소비자의 상호 의존성은 “제품사고의 직접적인 원인을 확정하는 것”이 쉽지가 않아서 법적 책임을 배분하는 것에 어려움을 가지게 한다.<sup>222)</sup> 예를 들어, 자율주행 자동차가 관련된 자동차 사고가 발생한 경우, 수많은 사물인터넷 행위자들이 전부 또는 부분적으로 당해 사고에 책임이 있다. 여기에는 차의 이동을 결정하는 앱, 센서 제조업자, 세서 네트워크 운영자, 도로 운영자, 그리고 소프트웨어를 공급한 제3자 등이 포함될 수 있다.<sup>223)</sup>

손해배상 소송에서 자신의 청구를 입증하기 위해, 소비자는 통상적으로 결함, 손해, 그리고 결함과 손해 사이의 인과관계를 증명해야 한다. 다양한 법제에서 이들 요소에 대한 다양한 테스트 방식이 있다. 예를 들어, 결함입증에 관하여 유럽연합과 미국은 “합리적인 기대 테스트”를 원칙으로 이를 변형한 심사척도를 적용한다. 이는 법원이 소비자가 제품이 가지고 있을 것으로 기대하고 있는 것을 어떻게 침해했는지를 비교·평가하는 것이다.

그러나 이러한 일반적인 테스트에 있어서도 실제 구체적인 적용에 있어서는 EU회원국 사이에 또는 미국 내 각 주 별로 다양한 변형이 있다. 제조물책임법제는 또한 제조업자에게 보호막을 제공하고 있는데, 예를 들어 제조업자는 해당 제품의 시장 출시 당시 “가장 최첨단의 기술(state-of-the-art)”을 사용한 것임을 입증하여 책임을 면할 수 있다. 또한 제조물책임은 사망, 인적 손해 또는 기타 재산에 대한 손해 등 일정 범주의 손해에만 적용되어 책임을 한정하고 있다. 이러한 모든 것들

222) European Commission(2016), Advancing the Internet of Things in Europe

223) Medium(2017), IoT Raise New Challenges for Assigning Liability

이 결합 있는 제조물에 관한 법적 책임의 정확하고 효율적인 배분을 어렵게 하는 것이다.

이러한 문제들은 일부 법제와 지역에서 상당히 적극적인 정책적 고려 사항이다. 예를 들어, 유럽집행위원회(EC)는 현재 EC의 제조물책임 준칙이 새로운 기술에서 등장하는 문제를 다루는데 적합한 것인지 여부를 중심으로 검토하고 있다.<sup>224)</sup> 이 준칙은 1985년 이래로 대부분 수정 없이 남아있다. 유럽집행위원회(EC)가 이 주제에 관한 공개 의견수렴을 통해서 제출된 의견에 따르면, 이 공개 의견수렴 절차에 응답한 전문가의 대략 절반 정도가 EC 제조물책임 준칙이 혁신적인 제품에 대응하기 위하여 적응할 필요가 있다고 믿고 있었다.<sup>225)</sup>

유럽의회 역시 사물인터넷에서 책임의 할당문제를 다루고 있다. 2017년 1월, 유럽의회 의원들은 유럽집행위원회가 책임문제를 분명히 하기 위해 로봇 및 인공지능에 관한 규칙을 제안할 것을 촉구하는 의결을 했었다.

일부 논자들은 제조물 생산체인에서 제조업자 및 다른 이해관계자들에 관한 책임문제를 해당 이해관계자들이 위험을 “집단화(pool)”하고 단체로 사물인터넷 기반 장비 및 앱의 위험을 보장하는 방식의 보험에 기반한 해법을 제시하기도 했다. 자신의 연례 보고서인 SONAR에서, Swiss Re는 “전자적 사람(electronic person)”을 위한 새로운 법인격의 가능성을 고려했었다.

이런 주장이 상당히 견강부회 같은 설명으로 들릴 수 있지만, 엄격책

224) European Commission(2016), “Evaluation and Fitness Check(FC) Roadmap Evaluation of the Directive 85/374/EEC Concerning Liability for Defective Products”

225) European Commission(2017), Brief factual summary on the result of the public consultation on the rules on producer liability for damage caused by a defective product.

임주의와 의무보험제가 동반되는 경우 자율주행 자동차 사고가 발생 했을 때 책임을 결정하는 복잡한 문제(운전자, 자동차 제조업자, 소프트웨어 또는 데이터 제공자 중 누가 책임을 질 것인가의 문제)와 마주하는 것 보다는 제조물책임 분쟁이 발생한 경우 문제해결에 있어서 “단순 명료한 해법”을 제공한다.<sup>226)</sup>

그러나 이러한 논의는 의무준수(법규준수, 안전법제 준수로서 사전규제)에 대한 책임의 분배 문제와 위해가 발생한 경우 책임의 배분 문제가 사물인터넷 맥락에서 복잡한 정책적인 고려사항을 제기하고 있다는 것에 초점을 맞춘 것이다.

이러한 도전과제를 고려할 때, 근본적인 문제가 등장하는데, 그것은 현존하는 전 세계의 제품 안전 및 책임법제가 사물인터넷 시대에 입법 목적에 부합할 수 있는 것인지 여부이다. 한편으로, 사물인터넷이 전체적으로 새로운 쟁점을 제기하는 것은 아니라고 주장할 수 있다. 한 번 판매된 제품이 제3자나 소비자 스스로에 의하여 변형되거나 적절히 적응하는 것이 이례적인 것은 아니다. 반면 다른 한편으로, 현존하는 규제 및 책임체제는 새로운 개념과 도전과제를 적절하게 다루기 위해서 적응해야 할 필요가 있다고 주장할 수 있다. 이러한 것들은 정책입안자들에게는 중요한 문제이다. 정책입안자가 필요한 정책을 확인하거나 적절한 적응을 하지 못하는 것은 신속히 상업화되어 시장에서 유통되고 있는 제품의 한 무리를 적절한 안전 및 운영에 관한 감시 없이 방치하는 것이고, 이는 중국에 소비자가 증폭된 위험에 노출되게 만드는 것이다. 이러한 두 가지 접근법을 고려할 때, i) 사물인터넷에서 소비자제품 안전의 고도화(a high level of consumer product safety in the IoT)와

226) Kidman, D. and S. Turner(2017), Electronic persons: time for a new legal personality? New Law Journal.

ii) 제품안전을 높이는 새로운 기술의 이점을 소비자로부터 박탈하는 결과를 낳게 되는 혁신에 대한 불필요한 억제, 이 둘 사이의 균형점을 모색할 필요가 있다.

#### (4) 소비자와의 안전성에 관한 소통

사물인터넷을 통하는 경우, 제품 제조업자와 공급자들은 사용자 기반으로 전례를 찾을 수 없을 정도로 신속하고 효과적으로 소비자와 연결할 수 있는 능력의 가지고 있는데, 특히 제품 리콜의 경우가 이에 해당한다. 통상적으로, 소비자의 사물인터넷 기반 장비와 상호작용은 해당 장비와 원거리의 소프트웨어 기반 서비스나 앱에 의해 이루어지는데, 이것은 해당 기업이 제품의 능동적인 사용자(해당 사용자가 제품의 원구매자인지 여부는 관계없이)와 연결할 수 있는 유리한 능력이 있는 소프트웨어를 통제할 책임을 부담시킨다.

이것이 의미하는 것은 제품 공급자가 최초 제품을 사용하는 시점 및 해당 제품의 전체 주기를 통하여 소비자와 중요한 안전정보를 교환할 수 있는 유일한 기회를 가진다고 기대되는 것이다. 여기에는 안전한 설치 및 실행 지시, 안전한 제품 사용 지시, 제조업자 수중에 새로운 데이터가 들어와서 안전지시문을 업데이트 하는 것, 제품 리콜이나 안전한 변형에 관한 정보, 그리고 적절한 유지에 필요한 정보 및 제품의 종기(終期)에 관한 정보 등이 포함된다.

정책입안자에게 있어서 도전과제는 첫 번째로 규제 및 집행실무가 신기술을 이처럼 안전성을 제고하는 방식으로 사용될 수 있도록 장려하기에 충분한 유연성을 가지도록 하는 것이다. 하나의 예시로, EU 제품안전 규정의 해석에 관한 유럽집행위원회의 “블루 가이드(Blue Guide)”의 가장 최근 버전은 안전경고문을 반드시 소비자에게 제품과 함께 문

서로 제공하도록 제안하고 있다.<sup>227)</sup> IoT 시대에, 이러한 가이드는 이미 시대에 뒤떨어진 것인데, 왜냐하면 이미 소비자에게 중요한 안전경고 및 지시문을 전달할 더 효과적인 방식이 존재하고 있기 때문이다.

일반적으로, 위에서 논의한 것은, 이러한 능력들이 사물인터넷 제품의 개발과 마케팅을 책임지고 있는 경제적 운영자들의 책임범위에 관한 문제를 제기한다. 즉, 안전정보가 소통되는 방식, 시기, 예측하지 못한 안전문제가 발생한 경우 이를 제공할 의무 등에 관하여 이를 책임지는 주체가 사물인터넷 기술발전에 따라 과거와는 다른 책임을 부담할 수 있다는 것이다.

---

227) European Commission(2016), The 'Blue Guide' on the implementation of EU product rules 2016, European Commission



## 제4장

# IoT기반 소비자제품 안전에 관한 법·정책적 개선방안

제1절 새로운 위해요인에 대한 대응

제2절 기술융합에 따른 안전관리 체계 및 협력체계 구축





## 제1절 | 새로운 위해요인에 대한 대응

사물인터넷 기술의 발전과 이를 활용한 다양한 소비자제품의 출현은 이전에는 생각할 수 없었던 장점과 함께 문제점을 제공하고 있다. 이러한 문제점에는 IoT기반 소비자제품을 사용하는 소비자의 안전에 관한 문제도 포함되어 있다. 이처럼 잠재적으로 소비자의 안전에 위해요인으로 작용할 수 있는 IoT기반 소비자제품의 문제를 확인하고 분석하는 것이 필요할 것이다. 미국과 OECD의 경우에서 볼 수 있듯이, IoT기반 소비자제품의 위해요인에 어떤 것이 있는지를 다양한 이해관계인의 의견수렴을 통해 조사·분석해야 할 것이다. 새로운 제품의 등장에 따라 기존에는 인식할 수 없었던 안전성 위해요인이 존재하는 경우 우선적으로 이를 명확히 확인하고 분석하는 작업이 필요하다. 이런 과정을 통해 IoT기반 소비자제품의 위해요인을 발견하고 이에 대한 제도적인 대응이 필요할 것이다. 이를 위해서는 미국의 CPSC가 했듯이 소비자제품안전의 주무부처가 중심이 되어 소비자제품 제조업자, 전문가, 학계, 시민사회 등 다양한 이해관계자로부터 공개적인 의견수렴을 통해 위해요인을 확인하는 작업이 필요하다. 현재 IoT기반 소비자제품의 사용과정에서 위해가 발생한 사건사고 사례가 거의 없다는 점을 고려할 때, 사물인터넷과 관련한 여러 이해관계자의 의견수렴을 통해 잠재적인 위해요인을 확인할 필요성이 있다. 또한 위해요인의 조사·분석에 있어서 해외 주요국의 관련 자료를 참고하고 국제적인 논의를 지속적으로 모니터링하고 주시할 필요가 있다. IoT기반 소비자제품이란 새로운 기술의 상용화에 따라 발생하는 위해를 관리하기 위하여 국제적인 논의가 이루어지고 있는 단계이므로, 이러한 논의의 전개과정에 적극적으로 참여하여 국제적인 관련 규범의 형성을 살펴보아야 한다.

IoT기반 소비자제품의 위해요인을 조사·분석하고 이를 현재의 소비자제품안전법제에 반영할 필요가 있다. 특히 IoT기반 소비자제품의 대부분을 차지하고 있는 가전기기의 안전을 규율하는 법령에서 새로운 위해요인을 다루어야 한다. 앞서 살펴본 바와 같이, 현행 「전기용품 및 생활용품 안전관리법」은 제품의 위해도에 따라 안전인증대상제품, 안전확인대상제품, 공급자적합성확인대상제품, 안전기준준수대상제품으로 분류하여 각 제품범주별로 안전관리를 하고 있다. 안전관리의 밀도는 해당 제품범주가 가지는 위해도에 비례하도록 「전기용품 및 생활용품 안전관리법」에서 규정하고 있다. IoT기반 소비자제품의 등장은 기존의 제품이 가지는 특성과는 다른 특성을 부여한다. 즉, 사물인터넷 기술이 사용된 소비자제품은 종래의 소비자제품과는 다른 특성을 가지게 된다는 것이다. 예를 들어, 전기청소기의 경우 사물인터넷을 활용한 청소기는 종래 전기청소기와는 다르게 외부세계를 스스로 인식하고 이에 따라 움직이는 특성을 가지게 된다. 그런데 이러한 IoT기반 소비자제품의 특성이 위해요인이 되어 해당 제품의 위해도를 변경시킬 수 있다. 예전에는 위해도가 낮았던 제품이 위해도가 상승할 수도 있고, 그 반대의 경우가 발생할 수도 있다. 따라서 IoT기반 소비자제품의 위해요인을 분석하고 그 결과를 고려하여 현행 「전기용품 및 생활용품 안전관리법」상의 제품분류체계를 다시 분류할 필요가 있다.

이와 함께 「전기용품 및 생활용품 안전관리법」의 안전기준도 검토가 필요할 것이다. 「전기용품 및 생활용품 안전관리법」상 제품의 위해도 재평가에 따라 제품분류가 변경됨에 따라 안전기준체제도 수정해야 하지만, 이를 제외하고도 IoT기반 소비자제품의 위해요인을 반영한 안전기준의 검토가 있어야 한다. 상술한 바와 같이, 현재 「전기용품 및 생활용품 안전관리법」상 안전기준은 전통적인 소비자제품을 모델로 상정하여 규정한 것이다. 따라서 IoT기반 소비자제품의 경우 제품의 특성을

반영한 별도의 안전기준을 마련하거나 기존의 안전기준에 추가 또는 수정하는 개정이 필요하다. 인터넷과 연결되어 작동하는 소비자제품의 특성을 반영하여 정상적 작동상태, 네트워킹 기준 등이 제품의 안전기준에 포함되어야 한다.

상술한 바와 같이, 현행 「정보통신망법」은 정보통신서비스제공자에게 정보통신망의 안전성 유지를 위해 여러 규정을 두고 있다. 이러한 정보보호와 침해사고예방을 위한 규정은 해당 정보통신망 자체의 안전성에 초점을 맞추고 있다. 따라서 정보통신서비스제공자에게 부과된 정보보호 관련 의무는 정보통신망의 안전성 제고와 이용자 보호에 관한 사항으로 규정되어 있다.

하지만 IoT기반 소비자제품의 위해요인에 관한 미국 및 OECD의 사례에서 볼 수 있듯이, 정보통신망의 안전성 문제가 해당 제품을 사용하는 소비자의 신체상 위해로 발전할 수 있게 된다. 따라서 이러한 위해요인을 고려하여 「정보통신망법」상의 정보보호에 관한 규정에 반영할 필요가 있다. 즉, 「정보통신망법」에서 정보통신서비스제공자의 정보보호 사전점검기준, 정보보호 관리체계의 인증기준 등 절차, 정보보호 관리등급 부여절차 등에 있어서 침해사고 발생 시 소비자의 위해를 방지하기 위한 조치 등이 포함되도록 관련 법령의 개정이 필요할 것이다.

## 제2절 | 기술융합에 따른 규제체계의 대응

사물인터넷은 사물과 사물, 사물과 인간, 사물과 사이버공간의 연결을 통해 종래 제공할 수 없었던 새로운 서비스를 제공하는 것이다. 이러한 사물인터넷을 활용한 소비자제품의 경우 연결성이란 특성을 가지게 되고, 이는 종래 소비자제품과는 다른 IoT기반 소비자제품의 고유한 성질을 이룬다. 즉, IoT기반 소비자제품은 사물인터넷이란 네트워크와 소비자제품이 연결되어 있는 것이다. 이는 인터넷이란 정보통신망 서비스와 소비자제품이란 하드웨어가 결합되어 등장한 것이다. IoT기반 소비자제품은 그 자체가 기술융합 제품이다. 이러한 IoT기반 소비자제품의 특성은 소비자안전법제에 있어서도 융합의 필요성을 제시하고 있다. 앞서 언급한 바와 같이, 우리 소비자제품안전규제 체계는 품목과 분야별로 소관 부처가 산재해 있는 구조이다. 이에 IoT기반 소비자제품의 안전규제에 있어서는 이러한 산재한 규제체계의 적절한 변화가 필요하다. IoT기반 소비자제품의 위해요인에 관한 미국, OECD의 위해요인 분석은 인터넷의 보안문제가 정보통신망의 안전성 문제만이 아닌 소비자의 신체상 위해의 요인이 될 수 있음을 보여주고 있다. 보안사고가 소비자안전의 위해요인으로 작용하는 것이다. 미국의 CPSC도 데이터 보호가 CPSC 수권법상 CPSC의 관할권에 해당하는 것은 아니지만 데이터 훼손이 소비자 위해로 이어지는 경우에는 CPSC가 이를 관할 할 수 있다고 판단한 것도 이러한 IoT기반 소비자제품의 특성을 고려한 것이다. 이러한 상황에 대응하기 위해서는 데이터 보호와 소비자안전을 담당하는 부처 사이의 능동적인 협력과 공동대응체계를 구축해야 한다. IoT기반 소비자제품의 위해사고에 대한 부처간 협력을 위한 거버넌스를 만들고 여기에 정보보호 담당부처, 소비자제품안전 부처 등이 참여할 수 있

도록 정책적 방안을 마련해야 한다.

또한 「정보통신망법」상 침해사고에 대한 정보를 소비자안전을 담당하는 기관에서도 공유할 수 있는 법적 근거를 마련해야 한다. 현행 「정보통신망법」에서는 정보보호 주무부처인 과학기술정보통신부와 한국인터넷진흥원이 침해사고에 대한 정보를 가지고 이를 활용하여 원인분석 등을 하는데, 침해사고가 정보통신망의 안전성 문제를 넘어 소비자안전 문제로 이어질 수 있기 때문에 관련 정보를 소비자안전 담당기관도 공유할 필요성이 있다. 이를 위해 「정보통신망법」상 침해사고에 대한 정보를 소비자안전 담당기관도 공유하여 데이터로 삼아 이를 활용할 수 있는 법적 근거를 마련해야 한다. 그리고 침해사고의 예보·경보 등 정보도 소비자안전 담당기관과 공유할 수 있어야 할 것이다. 즉, 종래 정보보호 침해가 IoT기반 소비자제품의 경우에는 위해요인으로 작용할 수 있으므로 정보보호 침해사고가 위해정보로 취급될 수 있고 따라서 이의 수집·활용을 위한 법적 근거가 마련될 필요가 있다는 것이다.



## 제5장 결 론







## 제1절 | 연구의 요약

본 연구는 사물인터넷을 활용한 소비자제품의 안전을 강화하기 위한 법제도적 개선방안을 마련하는 것이 목적이었다. 이러한 연구목적을 위하여 본 연구는 IoT기반 소비자제품의 개념정의를 위하여 사물인터넷과 소비자제품의 정의를 살펴보았다. 사물인터넷의 정의에 관하여는 현재 국제적으로 합의된 것은 없었고, 이에 국가나 전문가 또는 기구 별로 사물인터넷을 가리키는 용어에 차이가 있었다. 하지만 이런 차이에도 불구하고 다양한 정의 사이에는 공통적인 분모도 있었다. 본 연구에서는 사물인터넷 개념정의를 위한 이처럼 다양한 정의를 살펴보고, 각 정의 사이의 공통분모를 도출하고 이를 통하여 사물인터넷이 무엇인지를 정의한다. 이에 사물인터넷 개념정의를 위한 핵심요소로 ‘연결성’, ‘외부세계에 대한 자율적 인식과 작동’, ‘원격조종성’등을 도출할 수 있었다. 다음으로 소비자제품의 개념을 살펴보았다. 현행 법제상 소비자제품과 관련한 개념의 정의를 살펴보고 주요국가의 소비자제품에 관한 입법례를 조사하였다. 여기에는 미국의 소비자제품안전법, 일본의 소비생활용품안전법 등이 포함되었다. 이를 통해 소비자제품의 개념을 고찰하고 IoT기반 소비자제품을 정의하였다. 개념정의 다음으로 IoT기반 소비자제품의 종류와 시장규모 등 현황을 살펴보았다. 사물인터넷 실태조사 등에서 IoT기반 소비자제품을 별도로 조사하지 않아, 사물인터넷 시장현황과 서비스 활용분야 등을 통해 IoT기반 소비자제품 시장현황을 간접적으로 살펴볼 수 있었다. 그리고 IoT기반 소비자제품의 특성과 관련 문제를 조사·분석하였다. 이를 통해 IoT기반 소비자제품이 가지는 이점과 문제를 파악할 수 있었다.

다음으로 IoT기반 소비자제품 안전 관련 국내법제와 국제적 대응논

의를 살펴보았다. IoT기반 소비자제품 안전 관련 국내법제는 제품안전에 관한 사전적 규제와 정보보호에 관한 법률인 「전기용품 및 생활용품 안전관리법」과 「정보통신망법」의 주요 내용을 살펴보았다. 정보통신망의 안전성 확보가 IoT기반 소비자제품의 안전에 관련되기 때문에 「정보통신망법」도 고찰대상으로 채택하였다. 그리고 사물인터넷의 보안에 관하여 자율규제로서 법적 구속력은 없지만 보안실무상 광범위하게 활용되고 있는 IoT보안 가이드를 살펴보았다. IoT기반 소비자제품의 안전관련 국제적 대응부분은 IoT기반 소비자제품의 위해요인 조사·분석과 이러한 위해요인에 대한 법·정책적 대응에 관한 국제적 논의를 살펴보았다. 주요 분석대상은 미국과 OECD의 관련 논의였다.

미국 CPSC, FTC의 위해요인 분석과 OECD의 위해요인 분석을 순차적으로 살펴보고, 이러한 새로운 위해요인에 대한 CPSC의 의견서와 OECD의 논의를 조사·분석하였다.

이러한 논의를 통해 IoT기반 소비자제품의 안전강화를 위한 법·정책적 개선방안을 도출하였다. 법·정책적 개선방안으로는 구체적인 법제개선방안을 제시하기 보다는 법·정책적 차원에서 고려되어야 할 사안을 중심으로 설명하였다. 이는 현재 IoT기반 소비자제품 안전에 관하여 국제적인 차원에서도 논의를 시작하는 단계로서 법제적 개선방안을 마련하여 시행하고 있는 경우가 없어, 구체적인 법제개선을 도출하기 어렵다는 제약 때문이다. 이에 IoT기반 소비자제품 안전 강화를 위한 법·정책적 개선과제를 제시하고 이를 위한 관련 법제의 개선방향을 제안하는 것으로 법제개선방안을 갈음하였다.

## 제2절 | 연구의 의의 및 한계

종래 사물인터넷에 관한 안전문제는 개인정보보호, 보안 등 주로 정보보호의 측면에서 논의되었고, 대부분의 연구도 이러한 관점에서 수행되었다. 이에 반하여 본 연구는 사물인터넷을 활용한 소비자제품의 위해방지를 위한 안전문제에 초점을 두고 있다. IoT기반 소비자제품에 관하여 기존에는 수행된 적이 없는 안전문제를 법·정책적 측면에서 고찰한 연구로서 의의가 있다고 할 것이다. 이를 위해 사물인터넷과 소비자제품의 개념을 고찰하고 사물인터넷 제품시장의 현황을 조사·분석하였다.

또한 IoT기반 소비자제품의 위해요인과 이에 대한 법·정책적 대응방안에 관한 국제적인 논의를 조사·분석하였다. IoT기반 소비자제품은 종래 소비자제품에서는 찾아보기 어려운 새로운 위해요인을 가지고 있으며, 이러한 새로운 위해요인을 관리하기 위하여 법·정책적 도전과제를 제시하고 있었다.

주요 조사 및 분석 대상은 미국과 OECD의 입장이었다.

이러한 과정을 통해 IoT기반 소비자제품의 안전강화를 위한 법·정책적 개선방안을 제시하였다. 새로운 위해요인에 대한 대응방안과 기술융합에 따른 규제체계의 대응을 주요 개선방안으로 제안하였다.

본 연구는 이러한 연구결과에도 불구하고 일정한 한계를 가지고 있다. 국제적으로도 IoT기반 소비자제품의 안전문제는 논의의 출발단계에 있어, 구체적인 법제개선방안을 제시하지 못했다. IoT기반 소비자제품 안전강화를 위해 어떠한 법률이 어떻게 개정되어야 하는지를 제안하지 못한 한계가 있다. 그리고 본 연구는 IoT기반 소비자제품 안전강화를 위한 사후적 규제의 개선방안은 제안하지 못했다. 특히 사후적 규제

에서 핵심적인 법적책임의 주체 및 배분문제는 문제제기만 했고 이를 다루지는 못했다. 이는 이러한 사후적 규제의 문제는 실제 사고가 빈번히 발생하여 사례가 누적된 후에 법제개선이 논의될 수 있다는 점에서, IoT기반 소비자제품의 안전문제가 논의되어가는 시점에서는 명확히 개선방안을 제안하기 어려운 한계 때문이었다. 이에 이러한 본 연구의 한계를 메워주는 후속연구가 진행되기를 기대한다.

## 참 고 문 헌

- 김영순(2019), 제4차 산업혁명과 초연결사회 그리고 사물인터넷 시대, 한국콘텐츠학회 한국콘텐츠학회지 제17권 제3호
- 김지영(2015), 개인정보보호를 위한 사물인터넷의 법적 규율에 관한 고찰, 한국법정책학회 법과 정책연구 제15집 제4호
- 이도국(2015), 사물인터넷(Internet of Things) 환경에 있어 민사법적 문제점에 대한 소고, 한양대법학연구소 한양법학 제26권 제2집
- 정원준(2014), 사물인터넷(IoT) 활성화를 위한 법·제도적 개선방안 연구, 한국법정책학회 법과 정책연구 제14집 제4호
- 정혜욱(2014), 사물인터넷 활성화와 법제도에 관한 연구, 중앙대학교 문화미디어엔터테인먼트법연구소, 문화·미디어·엔터테인먼트 법
- 황의관(2014), 미국행정법상 법규명령에 관한 연구, 공법학연구 15권 4호
- 사지연(2017), 「사물인터넷 관련 개인정보 관리에서의 소비자권의 강화 연구」, 한국소비자원 정책연구
- 송순영(2013), 「위해정보 수집·제공 체계 개선에 관한 연구」, 한국소비자원 정책연구
- 정혁·이대호(2014), 「사물인터넷 진화와 정책적 제언」, 정보통신정책연구원 보고서
- 지광석·김재영·김도년(2107), 「소비자제품안전규제 개선방안 연구」, 한국소비자원 정책연구
- 최계영(2012), 「소통과 창조 기반의 ICT 미래 국가발전전략 연구」, 방송통신위원회
- 김남진·김연태(2012), 「행정법 I」, 법문사

김철용(2012), 「행정법」, 고시계

이광윤(2006), 「일반행정법」, 법문사

과학기술정보통신부·정보통신산업진흥원·한국사물인터넷협회(2018), 「2018  
년도 사물인터넷 산업 실태조사」

소프트웨어정책연구소(2019), 사물인터넷 시장 및 주요 기업 동향, 월간  
SW중심사회(2019.1)

미래창조과학부 방송통신정책연구 15-진흥-033(2015), 「사물인터넷 진흥  
및 융합활성화를 위한 법제도 개선 연구」

한국사물인터넷협회(2018), 「2018 상·하반기 사물인터넷 제품 및 서비스  
편람」

한국인터넷진흥원(2012), 「인터넷&시큐리티 이슈」

대한민국 정책브리핑(2018), 2018년 사물인터넷 산업 실태조사 결과 발표  
한국 IDC, 전 세계 사물인터넷(IoT) 지출규모 2019년 7450억 달러 전망

Alfred Ng(2018), Hackers Should be Pumped About Gas Station  
Security Flaws, CNET

Ericsson(2017)., Ericsson Mobility Report

Cartwright(2017), J., Product liability and the internet of things, in  
Charles Russell Speechlys

Cisco(2016), Cisco Visual Networking Index: Global Mobile Data  
Traffic Forecast Update

Iansiti, M. and K. Lakhani(2017), The Truth About Blockchain,  
Harvard Business Review

John Leyden(2017), Half Baked Security: Hackers Can Hijack Your  
Smart Aga Oven 'With a Text Message', The Register

- Kidman, D. and S. Turner(2017), Electronic persons: time for a new legal personality? New Law Journal
- McAfee(2013), Data Quality in the Internet of Things
- McKinsey(2016), Internet of Things: The IoT opportunity- Are you ready to capture a once-in-a-lifetime value pool?
- Medium(2017), IOT Raises New Challenges for Assigning Liability
- Peter Newman(2019), The Internet of Things 2019 Report: How the IoT Continues to Transform Business, Homes, and Cities Through Next Generation Digital Solutions, Bus. Insider Intelligence
- Richard Speed(2018), Three-Hour Outage Renders Nest-Equipped Smart Homes Very Dumb, The Register
- Richard Chirgwin(2016), Finns Chilling as DDoS Knocks Out Building Control System, The Register
- Reed Smith LL((2017), Augmented and Virtual Reality- Emerging Legal Implications of & quot; The Final Platform&quot; Perspectives Reed Smith LLP.
- R. Street(2016), Reality Check: The Regulatory Landscape for Virtual and Augmented Reality.
- Tech Policy Lab(2015), Augmented Reality: A Technology and Policy Primer, University of Washington; R. Street(2016)
- Alliance for Internet of Things Innovation(AIOTI) (2015), Working group 4 Report on Policy Issues
- CPSC Staff Report(2017), 「Potential Hazards Associated with Emerging and Future Technologies」(2017)
- \_\_\_\_\_(2019), 「Statement of Commissioner Elliot F. Kaye Regarding



- a framework of safety for the Internet of Things」  
\_\_\_\_\_(2019), 「Status Reports on the Internet of Things(IoT) and Consumer Product Safety」  
CertifiGroup(2016), www.CertifiGroup.com Experts in UL, CSA, CE & amp; International Regulatory Compliance.  
Comments of the Staff of the Federal Trade Commission's Bureau of Consumer Protection, In the Matter of The Internet of Things and Consumer Product Hazards, Docket No. CPSC-2018-007  
European Commission(2016), Advancing the Internet of Things in Europe  
\_\_\_\_\_(2016), The 'Blue Guide' on the implementation of EU product rules 2016, European Commission  
\_\_\_\_\_(2016), "Evaluation and Fitness Check(FC) Roadmap Evaluation of the Directive 85/374/EEC Concerning Liability for Defective Products"  
\_\_\_\_\_(2017), Brief factual summary on the result of the public consultation on the rules on producer liability for damage caused by a defective product.  
FTC(2018) Docket No.CPSC-2018-007  
\_\_\_\_\_(2018), Mobile Security Updates: Understanding the Issues, FTC IoT Report  
Keith Werhan(2014), 「Principles of Administrative Law」, 2nd edition West Academic Publishing  
OECD(2015), 「OECD Digital Economy Outlook 2015」, OECD Publishing, Paris.

- \_\_\_\_\_(2016), 「The Internet of Things: Seizing the Benefits and Addressing the Challenges」, OECD Digital Economy Papers, No.252, OECD Publishing, Paris.
- \_\_\_\_\_(2016), 「Recommendation on Consumer Protection in E-Commerce」, OECD Publishing, Paris.
- \_\_\_\_\_(2018), 「Consumer Product Safety in the Internet of Things」, OECD Digital Economy Papers(2018) No.267
- \_\_\_\_\_(2017), 「OECD Digital Economy Outlook 2017」, OECD Publishing Paris
- Rec. ITU-T Y.2060 (2012.6), Definition 3.2.2
- U.S. GOV'T ACCOUNTABILITY OFFICE(2017), GAO-17-570, Internet of Things, Communities Deploy Projects by Combining Federal Support with Other Funds and Expense
- 83 Fed. Reg.13122; Mar.27, 2018

네이버 국어사전

국립중앙과학관-사물인터넷, 네이버지식백과

네이버캐스트 용어로 보는 IT



**Executive Summary**

## **A Study on the Legislative Improvement Measures for Strengthening IoT-based Consumer Product Safety**

Hwang, Eui-Kwan · Ji, Kwangseok

The IoT-based consumer products utilizing the IoT, the core technology of the 4th Industrial Revolution, are continuously growing the diversity and market size, and Korea is leading this field. However, IoT-based consumer products not only provide consumer with the benefits of convenience and improved utility, but also have potential hazards to consumer safety.

Recently, potential safety hazards for IoT-based consumer products have been investigated and the legal policy counter-measures to these hazards have been discussed at international level. The U.S. Consumer Product Safety Commission(herein after ‘CPSC’) held a public hearing on the safety hazards for IoT-based consumer products in May 2018, receiving various opinions from federal government agency, consumer groups,

and IT organizations. And, in January 2019, U.S. CPSC have published “Statement of Commissioner Elliot F. Kaye Regarding A Framework of Safety for The Internet of Things”. The OECD has also discussed the safety issues of IoT-based consumer products in various reports, and recently, the Working Party on Consumer Product Safety(herein after ‘WPCPS’) under the it’s Committee on Consumer Policy(herein after ‘CCP’) deals with the safety issues of IoT-based consumer products.

This study examines the concept and characteristics of IoT-based consumer products and research the international debates on the safety hazards of IoT-based consumer products and legal policy countermeasures against these hazards. In addition, this study proposes a legal policy improvement measures to strengthen consumer safety by researching and analyzing domestic legislation related to the safety of IoT-based consumer products. This study consists of five chapters, and the first chapter deals with the purpose and scope of the study. Chapter 2 deals with the meaning and status of IoT-based consumer products. This chapter examines the concepts of IoT and consumer products, and analyzes the characteristics and market size of IoT-based consumer products. Chapter 3 examines and analyzes domestic legislation and international discussions on IoT-based consumer product safety. Taking into account the high proportion of home appliances among IoT-based consumer products, this study would analyze the

Electric Appliances and Consumer Product Safety Control Act that can be applied to it. In addition, considering the characteristics that IoT-based consumer products are connected to the information communication network, Act on Promotion of Information and Communications Network Utilization and Information Protection governing the safety of the information communication network is also examined. Concerning the international discussion, it have researched and analyzed that the safety hazards and it's legal policy countermeasures against these hazards of U.S. and OECD separately. Through this study, it is possible to recognize the safety hazards such as loss of connectivity, data corruption, software update, etc., and to identify legal policy implications such as measures for controlling them, relationship between security and product safety, and difficulty in demarcating goods and services. Chapter 4 proposes a legal policy improvement measures for IoT-based consumer product safety. This includes researching and analyzing new safety hazards, establishing a safety management system and cooperation system due to technology convergence. In addition, this paper suggests the necessity of maintenance of related legislation such as the Electric Appliances and Consumer Product Safety Control Act and Act on Promotion of Information and Communications Network Utilization and Information Protection. Chapter 5 summarizes the study as a conclusion and discusses the meaning and limitations of the study.



정책연구 19-13

## IoT기반 소비자제품 안전강화를 위한 법제 개선방안 연구

---

인 쇄 일 | 2020년 1월

발 행 일 | 2020년 1월

발 행 인 | 한국소비자원 원장 이희숙

인 쇄 인 | 팝콘프린팅


발 행 | 한국소비자원 27738 충청북도 음성군 맹동면 용두로 54

전 화 | (043)880-5500

등 록 | 제3-348호(1991년 5월 17일)

정 가 | 10,000원

I S B N | 

• 본 연구의 내용은 연구자 개인의 견해이며 본원의 공식 견해가 아닙니다. 



Policy Analysis **19-13**

## A Study on the Legislative Improvement Measures for Strengthening IoT-based Consumer Product Safety

Hwang, Eui-Kwan · Ji, Kwangseok



**한국소비자원**

Korea Consumer Agency

27738 충청북도 음성군 맹동면 용두로 54

Tel. 043-880-5500 [www.kca.go.kr](http://www.kca.go.kr)



9 791156 494461  
ISBN 979-11-5649-446-1

값 10,000원