사물인터넷(IoT) 발전과 보안의 패러다임 변화

배상태_KISTEP 연구위원
김진경_KISTEP 연구원

1. 서 론

사물인터넷(IoT)은 가트너(Gartner)가 선정하는 10대 전략기술에 2012년부터 매년 선정되어 ICT 시장의 신산업을 이끌어가는 핵심 부가가치 산업으로 급부상하고 있다. 특히, 모바일 등 스마트 기기의 확산으로 인해 스마트 센서 증가와 함께 기기 간의 융합 및 연결성을 확보하면서 ICT 융합 분야 전반에 걸쳐 급속도로 사물인터넷 환경에 대한 관심이 고조되고 있는 추세이다. 현재 ICT 산업에서 가장 이슈가 되고 있는 ICBM(IoT, Cloud, Big Data, Mobile)이 차세대 성장동력으로 주목받고 있는 가운데 인터넷 기반의 융합중심에서 사물인터넷이 실제 생활영역에 적용되면서 다양한 경제적 가치와 더불어 효율성 및 편의성이 한층 높아질 것으로 기대되고 있다.

사물인터넷 산업은 시장 범주가 모호하고 타산업과의 융합을 전제로 성장하는 산업 특성상 시장 규모 예측 결과가 주요 기관별로 차이가 있지만 시스코(Cisco)는 네트워크에 연결된 사물 수가 2014년 144억 개에서 2020년 501억 개로 약 3.5배 증가할 것이라고 예측하였고, Machina Research는 M2M 시장이 2014년 45억 개에서 2024년 290억 개로 증가할 것이라고 예상하는 등 긍정적인 전망을 쏟아내고 있다. 국내의 경우에도 2015년 3조 8,000억 원에서 2022년 22조 9,000억 원까지 성장할 것이며, 특히 서비스 관련 매출의 비중이 52.6%까지 증가할 것으로 전망되고 있다. 하지만 위에서 언급한 바와 같이 향후 긍정적인 성과를 거두기 위해서는 사물인터넷이 내포하고 있는 다양한 위험적 요인들을 해결해야 한다. 즉, 표준화 및 호환성 문제, 보안 문제, 수익 모델 확보, 제도적 장애요인 등 산업 활성화를 저해시키는 요인들을 극복해야 할 것이다.

사물인터넷의 주요 서비스 시장에서는 주요 글로벌 ICT 기업(Apple, Google 등)들이 디바이스 경쟁을 넘어 사물인터넷 기기에서 수집한 데이터를 수집·관리·분석하기 위한 플랫폼 분야의 경쟁구도가 본격화되고 있다. ICT 기업들은 다양한 분야에서의 융합을 통해 고객가치를 제고할 수 있는 서비스를 제공하기 위해

치열하게 경쟁 중이다.

또한 미국, EU, 일본 등 주요 선진국에서는 신융합서비스 상용화를 촉진하는 규제 정비, 실생활 적용 중시, 사용자 보호/보안, 상황인지 등과 같은 규제 정비 및 사이버 보안에 중점을 두고 정책을 추진하고 있으며, 우리나라도 생태계 참여자간 협업 강화, 오픈 이노베이션 추진, 기업 규모별 맞춤형전략 등 우리나라 환경에 맞는 다양하고 구체적인 추진계획을 지속적으로 수립하고 있다. 비영리 연구기관인 ATARC[1]는 최근 발표한 '정부와 사물인터넷'[2] 보고서에서 사물인터넷 확산을 위해 정부가 추진해야 할 5가지 권고 사항을 제시하였는데 극복 과제로 사이버보안(Cyber-Security) 강화, 개인정보(Privacy) 보호, 사물인터넷의 위험관리를 제안하였다.[3]

사물인터넷 확산을 위한 정부 추진 5가지 권고 사항

- 정부는 서비스 향상 및 정부를 더 효과적이고 효율적으로 만들기 위해 사물인터넷의 잠재력을 적극 포용
- 국가 사물인터넷 전략 또는 정책 개발을 통해 사물인터넷의 장점에 대하여 일반 대중 및 연방기관을 교육하는 일에 착수
- 의회 및 행정부는 성장 및 기회를 방해하는 규제를 지양하고 사물인터넷에 대해 합의된 표준을 장려하는데 초점
- 정부는 개인정보보호를 보장하기 위한 중요한 역할 수행
- 정부는 기술 개발을 장려하면서 사물인터넷 환경의 보안을 보장하고 우수사례를 발굴하는 정책을 추진하도록 노력

이에, 본 원고는 사물인터넷 개념에 대하여 간략하게 살펴보고 사물인터넷 활성화에 가장 걸림돌이 되는 보안환경의 변화에 따른 위협 및 기술동향에 대해 알아본 후 주요 선진국에서 추진하고 있는 표준화 및 보안 추진 현황을 종합적으로 정리·분석하여 사물인터넷 보안에 대한 전반적인 이해를 돕고자 하였다.[4]

2. 사물인터넷 개념 및 서비스 현황

(1) 사물인터넷(IoT) 개념

MIT Auto-ID Center 설립자인 케빈 아스톤(Kevin Ashton)이 1999년 사물인터넷에 대한 개념 및 용어를 처음으로 제안해서 사용하기 시작하였고 사물인터넷 표준 관점에서의 논의는 2005년 ITU가 사물인터넷에 관한 보고서를 발간하면서 이슈화되기 시작하였다. 그리고 2008년부터 글로벌 기업들(Cisco, Qualcomm, Aricson, Intel 등)이 사물인터넷을 산업 유망 아이템으로 제시하면서 산업적으로 관심을 받게 되었다.

정보 공유 및 커뮤니케이션 위주로 물리적 기반에서 출발한 인터넷은 모든 경제 활동의 중심이 되는 플랫폼으로 진화하고 있다. 인터넷 도입 초기에는 검색과 포털사이트가 인터넷 중심이었고 소셜네트워크 서비스(Social Network Service)의 등장과 함께 관계 중심의 인터넷 활동이 증가하기 시작하였다. 스마트폰 도입 이후, 인터넷 영역이 유선에서 모바일로 확장되면서 이용자들은 언제, 어디에서나 인터넷에 접속할 수 있게 되었고 이에 따라 인터넷의 영향력은 점차 확대되었다. 인터넷을 자유롭게 활용할 수 있는 디바이스가 스마트폰에서 태블릿 PC, 스마트 TV 등 ICT 기기 대부분을 수용할 뿐 만 아니라 자동차, 조명, 가전 등

1_ ATARC(Advanced Technology Academic Research Center): 새롭게 등장한 기술 과제를 해결하기 위해 연방정부, 학계, 산업계를 위한 협력 포럼을 제공하는 비영리단체. 카네기 멜론 소프트웨어 공학연구소, MIT 링컨연구소 등 연방 정부자금 지원 연구개발센터(FFRDCs)와 전략적 관계 보유.

2_ Government and the Internet of Things: Findings and Recommendations of the Internet of Things Innovation Lab-2015년 7월부터 10주 동안 20개 이상이 정부, 산업계, 하계 대표로 사물인터넷 혁신 모임(Iot Innovation Lab)을 조직하여 여러 차례 협의를 통해 보고서 발간(2015.11.13)

3_ ATARC 보도자료, http://www.atarc.org/wp-content/upload/2015/11/ATARC-IoT-Innovation-Lab-Report-2015-11-18.pdf(2015.11.18.)

4_ 산업경제리서치 "사물인터넷(Iot) 활용분야별 비즈니스 현황과 최근 주요 이슈 종합분석"(2016.5.27.)

다양한 사물들이 네트워크에 연결됨에 따라 모든 것이 네트워크에 연결되는 초연결 시대가 조만간 실현될 것으로 예상하고 있다. 사물인터넷은 바로 이러한 초연결을 가능하게 하는 핵심 기술이라 할 수 있으며 다음과 같이 다양하게 정의되고 있다.

ITU(2005)에서는 사물인터넷을 '언제 어디서나 어느 것과도 연결될 수 있는 새로운 통신환경으로 인간과 인간, 인간과 사물, 사물과 사물을 연결하는 '객체의 제약'을 해결하는 것이 핵심이다'고 얘기하고 있다. 사물인터넷과 함께 많이 사용되고 있는 용어인 M2M(Machine to Machine), IoE(Internet of Everything) 등은 객체의 범위에 있어 차이가 있으나 기본적으로 센서가 부착된 사물에서 발생한 정보를 네트워크에 연결하여 정보 기반 서비스를 구현한다는 점에서는 사물인터넷과 유사하다고 볼 수 있다. ETSI(유럽통신표준협회), IEEE(미국 전기전자학회)에서는 M2M을 인간의 개입이 없는 상태에서 기기 사이에서 발생하는 정보 교환으로 정의하고 있다. 그리고 IoE는 시스코(Cisco)에서 언급한 용어로 사물을 만물로 확장시킨 개념이라 볼 수 있으며 사람, 사물뿐 만 아니라 업무, 데이터 등 모든 것들이 네트워크에 연결되어 새로운 부가가치와 비즈니스 기회를 창출하는 것을 의미한다.[5]

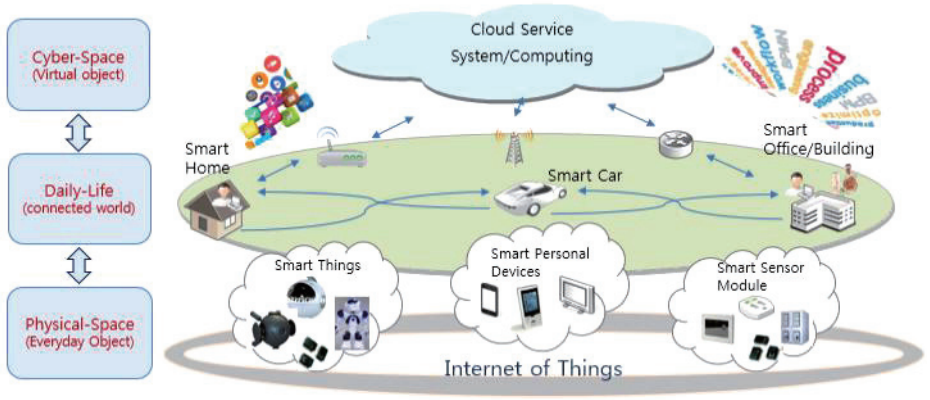
IDATE(2013)에서는 사물인터넷을 통신기기(Communicating Devices), M2M통신, 인터넷 제품(Internet of Objects) 등 여러 개념을 포괄하는 것으로 파악하고 있다. 통신기기는 인터넷 등 통신이 가능한 스마트폰, 태블릿, 스마트 TV 통신기기로 통신연결이 없으면 본래의 기능이 없는 것으로 정의하고 있다. M2M 통신은 기기간 혹은 기기와 서버간 자동화된 통신이 가능한 기기로 통신 모듈을 탑재하고 있다. 그리고 인터넷 제품은 스스로는 아무런 데이터를 생성할 수 없지만 본래의 기능을 지니고 있으며 사물인터넷 기술을 통해 객체 관련 정보를 통신하게 됨으로써 더욱 스마트하게 변하는 제품을 지칭한다.

한국인터넷진흥원(2012)은 사물인터넷 기술을 초연결사회의 기반 기술로서 사물간 인터넷 혹은 개체간 인터넷으로 정의하였고, 고유 식별이 가능한 사물이 만들어낸 정보를 인터넷을 통해 공유하는 환경이라고 정의하였다.

(2) 사물인터넷(IoT)의 서비스 현황

사물인터넷 시대는 흔히 '포스트 스마트폰' 시대라 불린다. 사물인터넷의 목표는 인간의 개입없이 인터넷으로 연결된 사물들이 각자 알아서 커뮤니케이션하는 환경을 만드는 것이다. 그리고 사물인터넷의

<그림 1> IoT 기술 기반 초연결사회



※ 출처: 한국인터넷진흥원, IoT 제품 및 서비스 보안성 강화방안 연구(2015.9.)

5_ 박유리 등, "인터넷의 진화와 사회경제적 패러다임 변화 연구 : 사물인터넷을 중심으로", KISDI, 기본연구 15-01(2015.11.)

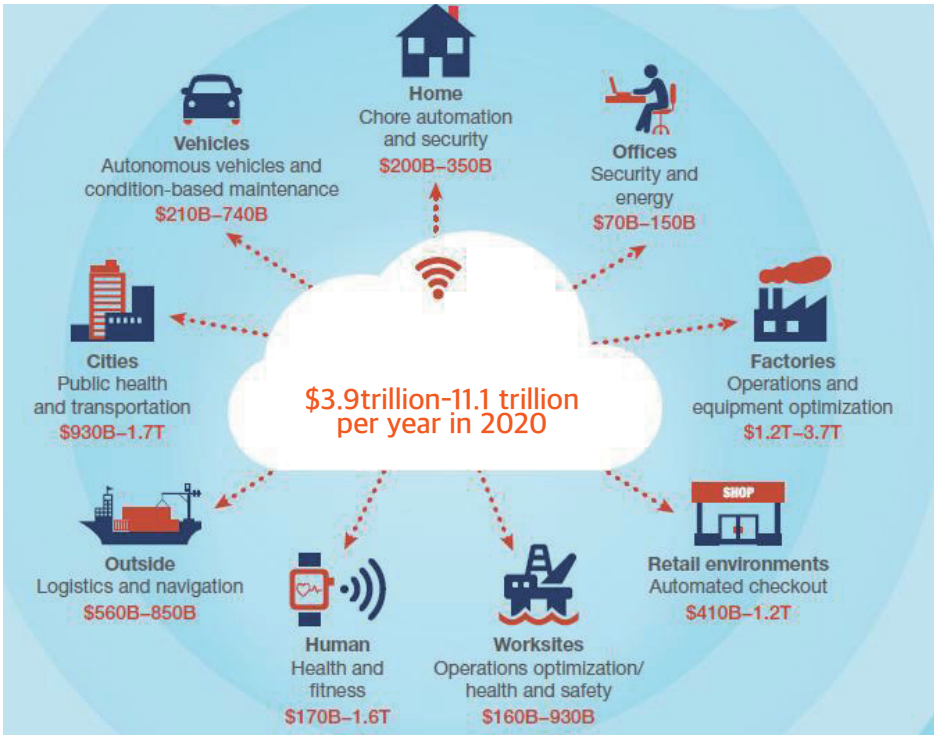
핵심은 인간을 둘러싼 사물들이 서로 연결되면서 인간에게 새로운 편의 혹은 가치를 부여하는 것이다. 스마트 폰이 인간을 중심으로 하여 언제 어디서든 연결될 수 있는 환경을 만들어 주었다면 사물인터넷은 인간 주변의 모든 사물을 연결하고 인간과 상호 소통할 수 있도록 만들어 줄 것이다.[6]

사물인터넷 기술은 PC, 스마트폰 등 컴퓨팅 단말을 넘어 사실상 모든 종류의 사물에 센서 네트워크의 작은 장치를 포함하여 생활 속 기기들이 실시간으로 인터넷에 연결된 환경으로 스마트 헬스케어 시스템과 산업 설비의 제어 시스템과 같은 스마트 서비스를 활성화 시키고 있다.

사물인터넷은 개별 단말에 통신 기능을 접목해 원격 감시 및 시스템 자동화 등을 실현하는 사물간 통신(Machine-to-Machine, M2M)과 유사한 개념으로 M2M이 주로 대규모 인프라 설비나 산업 시설 등 대형 시스템을 대상으로 통신 기술을 접목해 설비 운영 효율을 높이는 솔루션 제공에 초점을 맞췄다면, 사물인터넷은 모바일, 클라우드, 빅데이터 등 다른 IT 기술과의 연계를 통해 한 단계 진보된 사업 모델을 제시함으로써 일반 소비자를 대상으로 하는 다양한 단말 및 서비스의 혁신을 창출하는 기회 요인으로 작용하고 있으며 스마트폰과 태블릿, 웨어러블 등 개인용 컴퓨팅 단말의 보급 확대로 개인을 대상으로 하는 사물인터넷 서비스의 대중화는 더욱 앞당겨질 것으로 기대된다. 이와 더불어 사물인터넷은 가전, 의료, 교통 등 모든 분야에 적용될 것으로 전망됨에 따라 대부분의 기기에 정보 획득 및 네트워크 연결 기능이 탑재되고 이를 바탕으로 스마트홈, 스마트가전, 스마트카, 스마트헬스케어, 스마트시티, 스마트물류, 스마트그리드 등 다양한 분야에서 새로운 제품과 서비스가 출현될 것이다.

사물인터넷 활용에 따른 전 세계 부가가치 규모는 시장기관에 따라 2020년까지 1.9조 달러에서 19조 달러에 달할 것으로 전망되었다. 또한, Mckinsey(2015.6.)는 2025년까지 공장, 도시, 건강, 소매, 작업장, 물류, 교통, 가정, 사무공간 등 사물인터넷을 활용하는 9개의 주요 환경에서 사물인터넷 활용 수준에 따라

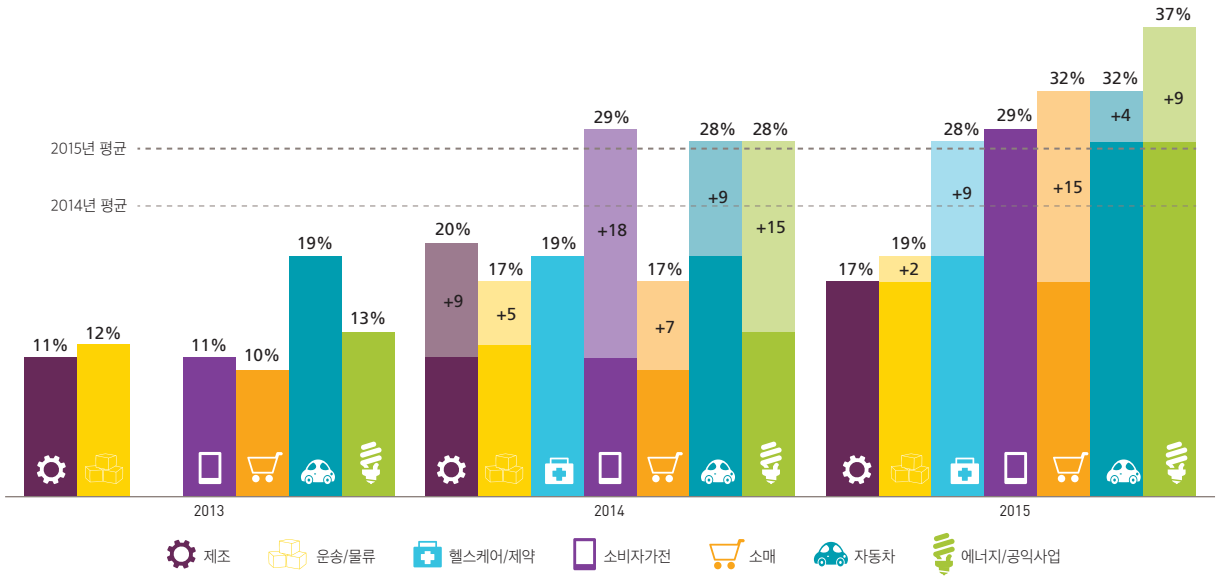
<그림 2> 2025년까지 전 세계 사물인터넷 파급효과 전망



※ 출처: Mckinsey Global Institute(2015.6.)

6_ 커넥팅랩, 사물인터넷-클라우드와 빅데이터를 뛰어넘는 거대한 연결 (2014.6.25.)

<그림 3> 전 세계 주요국 산업별 사물인터넷 도입률 추이



※ 출처: 보다폰(2015.7.)

연간 최소 3.9조 달러에서 최대 11.1조 달러의 경제적 파급효과가 발생할 것으로 전망하였다.[7]

하지만, 이러한 낙관적인 시장 전망과는 달리 전 세계 사물인터넷 도입은 미미한 수준인 것으로 나타났다. 전 세계 16개국, 7개 산업에 종사하는 650명이 임직원을 대상으로 글로벌 통신회사 Vodafone이 실시한 온라인 설문조사 결과에 따르면 2015년 현재 조사 대상 기업의 27%가 M2M을 도입한 것으로 나타났다. 이는 2013년 12%, 2014년 22%에서 점진적으로 증가한 것으로 나타나지만 여전히 기업의 사물인터넷 도입은 초기 수준임을 보여준다. 산업별로는 제조, 운송·물류, 헬스케어·제약, 소비자가전, 소매, 자동차, 에너지·공공분야 등 7개 산업 분야중 에너지·공공분야, 자동차, 소매 순으로 높게 나타난 반면, 가장 낮은 도입율을 보인 제조분야는 에너지·공공분야 도입율의 절반 가량인 17%에 그쳤다.[8]

3. 사물인터넷 보안 위협 및 보안 기술

(1) 사물인터넷(IoT) 보안 위협

사물인터넷 서비스는 정보 센싱과 이에 대한 가공·처리·저장·활용뿐 만 아니라 사람·서비스·사물과의 소통 등을 위해 여러 가지 요소기술이 통합되어 사용된다. 즉, 사물인터넷은 정보를 센싱하기 위한 센서 기술과 센싱된 정보에 대한 원활한 통신·네트워킹을 위한 기술, 사물인터넷 디바이스 자체를 위한 칩 기술, 기능 구현을 위한 OS 기술·임베디드 시스템 기술, 디바이스의 자율 동작과 지능적 동작을 위한 플랫폼 기술, 대량의 데이터를 처리하는 빅데이터 기술, 유용한 정보 추출을 위한 텍스트 마이닝 기술, 사용자 중심의 사물 인터넷 서비스를 위한 웹 서비스·응용 서비스 기술, 오픈 API 기술 등 다양한 형태의 기술이 사용된다. 이처럼 다양한 기술이 어우러진 사물인터넷 서비스는 기술 자체 혹은 구현하는 방법의 문제점으로 인해 다양한 보안 취약점이 존재할 수 있다. 사물인터넷의 보안 위협으로 데이터 위·변조, 비인가된 서비스 및

7, 8_ 박유리 등, "인터넷의 진화와 사회경제적 패러다임 변화 연구 : 사물인터넷을 중심으로", KISDI, 기본연구 15-01(2015.11.)

사용자 접근, 인증 방해, 신호 및 데이터의 기밀성/무결성 침해, 정보유출, 복제 공격 등의 형태로 발생 가능하며, 이러한 보안 취약점과 더불어 개인 프라이버시 침해 문제도 심각하다고 할 수 있다. 따라서 안전하고 신뢰할 수 있는 사물인터넷 서비스를 제공하기 위해서는 우선 사물인터넷 서비스 구성 기술 요소 각각에 대한 보안 기술을 체계적으로 살펴볼 필요가 있다.

(2) 사물인터넷(IoT) 보안 기술

사물인터넷은 여러 요소 기술의 융합으로 인해 각 기술의 취약점 발생 가능성뿐 만 아니라 기술이 융합되어 발생하는 새로운 취약점까지 대비해야 한다. 사물인터넷 구성 기술을 디바이스, 네트워크, 서비스/시스템, 데이터/프라이버시로 구분하여 각 분야에서의 보안 기술에 대해 살펴보고자 한다.

① 사물인터넷(IoT) 디바이스 보안

초경량·저전력·저성능의 특성을 지니고 있는 디바이스가 인터넷에 연결될 때 기존 PC 환경에서 사용되던 암호화 알고리즘은 복잡하고 무거워서 사물인터넷 디바이스에서 사실상 구현하기가 어렵다. 디바이스 관련 보안 기술은 인증/식별, 접근 제어, OS 보안, 경량 암호/보안 프로토콜 기술 등이 있으며, 가장 기본적으로 디바이스와 통신할 때 정당하게 전송된 데이터인지 인증/식별하는 ID/PW 기반, PKI(Public Key Infrastructure), SIM(Subscriber Identification Module), 바이오매트릭(Biometric) 기반 등의 방식이 있다.

ID/PW 방식은 빠른 연산과 경량화가 가능하지만 별도의 애플리케이션 및 프로토콜이 요구되며 낮은 안정성과 키 관리 문제점을 지니고 있다. PKI는 인증서 방식으로 공개 키 암호화 알고리즘 기반의 인증서를 발급받아 인증하므로 안전성은 높으나 연산량이 높고 인증서를 별도로 관리하여야 한다. SIM 방식은 USIM 또는 UICC 등을 이용하여 범용 사용자 식별정보로 인증하는 방식으로 스마트 카드의 별도 보관을 통해 물리적 보안 기능이 포함되지만 별도의 소프트웨어 및 관리가 필요하다. 바이오매트릭 기반 방식은 지문 또는 홍채 등의 생체 정보를 인식하여 인증하므로 안전성이 높으나 연산량은 높은 편이다.

이러한 제약들로 인해 SW기반에서는 보안위협을 완벽히 차단하기 어렵기 때문에 암호화 작업을 하드웨어에서 처리하는 방식으로 바꾼 것이 '보안 칩셋'이며, 이는 하드웨어 칩셋에 보안기술이 적용되어 해커들이 우회 공격하기 어려울 뿐 만 아니라 디바이스 성능 저하와 배터리 소모율을 최소화할 수 있다.

② 사물인터넷(IoT) 네트워크 보안[9]

사물인터넷에서 주로 사용되는 통신 기술로는 지그비(ZigBee), 와이파이(Wi-Fi), RFID(Radio Frequency IDentification) 등이 있다. 이들의 보안 요구 사항과 보안 기술들은 다음과 같다.

ZigBee는 근거리 통신을 지원하는 IEEE 802.15.4 표준 중의 하나로 가정이나 사무실 등에서의 무선 근거리 통신과 유비쿼터스 컴퓨팅을 위한 통신기술이다. ZigBee 단말들은 저전력을 사용하여 전력소모를 최소화 할 수 있다는 장점이 있으나, 그 대신 통신할 수 있는 정보량이 한정되어 있어 높은 수준의 보안 기술을 적용하기 어렵다는 단점이 있다. ZigBee 통신을 위한 보안 기술로는 SSM(Standard Security Mode)과 HSM(High Security Mode)의 두 가지 방식이 있다. SSM은 낮은 수준의 보안을 제공하며, HSM은 높은 보안 수준을 보안을 요구하는 환경을 위하여 설계되었다. ZigBee의 각 장치는 Open Trust Model 방식으로 암호화가 되는데, 이는 장치 자신에 대한 신뢰성을 보장한다. 즉, 장치 내부의 신뢰성은 보장되지만, 외부와의 통신 과정에서의 보안 위협은 존재하므로 별도의 보안대책이 요구된다.

Wi-Fi는 IEEE 802.11 표준 기반의 무선 랜 기술로 고성능 무선 통신이 가능하다. Wi-Fi는 무선으로 통신이

이루어지기 때문에 보안 위협으로부터 특히 취약하다. Wi-Fi 사용 시 통신 데이터의 암호화가 이루어지지 않을 경우, 도청, 스니핑, 비인가 접근 등의 공격이 이루어질 수 있다. 따라서 무선 구간의 데이터를 안전하게 보호하기 위한 방법으로 IEEE 802.11 표준에서 제시한 WEP(Wired Equivalent Privacy) 인증 프로토콜이 있으며, WEP의 단점을 개선한 WPA(Wi-Fi Protected Access)와 WPA2를 IEEE 802.11i에서 제안하였다. 또한 무선 구간의 통신 과정 외에 접속 과정에서의 보안을 위하여 암호화 알고리즘 TKIP(Temporal Key Integrity Protocol)과 CCMP(Counter mode with CBC-MAC Protocol)의 사용을 권고하고 있다.

RFID는 사물의 자동 인식을 위하여 무선 주파수를 이용하는 기술로 ISO 18000-7 표준에 기반한다. RFID는 물리적, 시각적 접촉과 무관하게 사물에 부착한 태그 정보를 인식하는 무선 네트워크 기술로 최근 USN(Ubiquitous Sensor Network) 환경 구축을 위해 가장 주목받는 기술이라 할 수 있다. RFID 시스템에서 주로 사용되는 수동형 태그는 제한된 연산 능력과 사용할 수 있는 전력량에 한계가 있으므로 높은 수준의 보안 기술을 적용하기 어렵다는 단점이 있으며 무선 통신을 사용하기 때문에 정보유출 등의 보안 위협으로부터 자유롭지 못하다. 이에 USN에서의 보안 요구 사항으로는 데이터 통신에 대한 기밀성 및 무결성이 요구되며, 안전한 키 관리 및 분배 기능이 요구된다. 또한, 센서 네트워크의 특성을 고려한 안전한 플랫폼 설계가 필요하다. 최근에 RFID/USN 환경에서 전송되는 데이터의 보안을 위하여 노드와 노드 간의 상호 인증을 위한 다양한 기법들이 연구되고 있다.

③ 사물인터넷(IoT) 서비스/시스템 보안[10]

사물인터넷 서비스는 다양한 디바이스와 플랫폼, 데이터 소유 주체, 그리고 다른 응용 서비스를 활용하여 새로운 서비스가 만들어지는 구조를 갖는다. 이 때문에 인증/인가 기법, 접근제어/권한제어 기법, ID(Identification) 관리 기법, 키 관리 및 분배 기법, 신뢰 제어 기법 등 다양한 보안 기법을 필요로 한다. 사물인터넷 서비스 보안 기술과 관련하여 IoT-A 프로젝트에서 정의한 보안 기술을 살펴보기로 한다. IoT-A 프로젝트에서는 인증을 위해 AuthN이라는 컴포넌트를 정의하였고 인가를 위해서는 AuthZ(Authorization) 컴포넌트, ID 관리를 위한 IM, 키 교환 및 관리를 위한 KEM(Key Exchange and Management), 신뢰도 및 평판 관리를 위한 TRA(Trust and Reputation) 컴포넌트를 정의하고 있다. 일반적으로 인증을 위해서 패스워드와 같은 지식 기반 인증, 스마트카드와 같은 소유 기반 인증, 그리고 지문과 같은 생체정보 기반 인증이 가능한데, IoT-A 보안 기법에서는 특정한 인증 기법 사용을 의무화하지 않고 상황에 따라 다양한 인증 기법의 사용을 권하고 있다. 예를 들면, 사전 공유 비밀정보를 사용한 객체 간 인증도 가능하며, 공개키 인증서(certificate)를 사용한 객체 간 인증도 가능할 것이다. 사용자인 경우, 사용자 ID와 패스워드 기반 인증도 가능할 것이다. 사용하는 인증 기법에 대한 적절한 키 분배 및 관리 기법도 필요하다. 인증 과정은 AuthN 컴포넌트에서 실현되는 것으로 정의되어 있다. 인증 과정을 거친 후, 해당 자원에 대한 사용권한을 확인하여 권한을 부여해주는 것을 인가(Authorization)라고 하며 IoT-A에서는 AuthZ 컴포넌트에서 수행한다. 또한, 접근 제어 대상자원에 대한 접근이 발생할 때마다 해당 접근이 허용되는지 여부를 확인받아야 하는데 이 부분도 AuthZ 컴포넌트에 의해 이뤄진다. 사물인터넷에서는 접근 대상 자원이 어디에 있는지를 찾는 기능(Resolution)이 필요한데, 이 Resolution 기능 수행 후, 해당 자원에 대한 접근 권한이 있는지를 확인해야 하므로 인가 기능이 수행되는 것이 일반적이다. 여기서 접근 권한은 다양한 접근 제어 기법을 사용할 수 있지만 사물인터넷과 같은 복잡한 시스템에 적합한 접근 제어 기법으로는 RBAC(Role Based Access Control)이나 ABAC(Attribute Based Access Control)가 좋다. 이는 역할 단위 혹은 속성 단위의 접근 제어가 가능하여 서비스 객체와 같은 다양하고 복잡한 미세 단위의 접근 제어가 필요할 때 사용한다.

9_ 장봉임 외, 사물인터넷 보안 기술 연구, 보안공학연구논문지 Vol.11, No.5(2014.10.4.)

10_ 김호원, 사물인터넷 환경에서의 보안/프라이버시 이슈, TTA Journal Vol.153(14.5.6.)

④ 사물인터넷(IoT) 데이터/프라이버시 보안

공격자가 비인가 단말 및 센서를 통해 정식 사용자로 위장하여 데이터를 전송하거나 데이터를 가로채 위·변조하여 정당한 정보로 전송되는 경우에는 인증절차를 통과하여 공격할 수 있다. 따라서 데이터 보안은 곧 정보 수집 및 저장하는 단계에서 프라이버시 침해와 뗄 수 없는 관계로 보인다. 사물인터넷은 사람·사물 간의 데이터 교환을 근간으로 하는 시스템이므로 개인정보(이름, 생년월일, 전화번호, 주소 등)가 시스템 접근 절차에서 요구되기도 하고, 시스템을 통해 유출될 가능성도 있다. 개인정보를 이용하여 접근한 후 시스템을 조작하거나 신용카드 및 비밀번호 등 더 많은 정보를 유출시킬 수 있어 프라이버시 침해는 사용자에게 더욱 위협적일 수 있다.

사물인터넷 서비스는 데이터를 처리함에 있어서 프라이버시 침해 가능성이 높기 때문에 프라이버시 보호형 마이닝 기법(Privacy Preserving Data Mining)을 사용할 필요가 있다. 프라이버시 보호형 마이닝 기법은 4가지로 분류할 수 있는데 첫 번째로 프라이버시 보존형 데이터 퍼블리싱 기법이 있는데 데이터 처리 및 가공 후, 그 결과 값이 프라이버시 침해가 되지 않도록 변형을 가하는 기법이다. 두 번째로 데이터마이닝 결과 변형 기법은, Association Rule Hiding과 같이 알고리즘 자체를 변형하는 방법이다. 세 번째로 쿼리 감사 기법은 쿼리 결과값을 수정하거나 제한하여 정보 누출을 방지한다. 마지막으로 분산프라이버시 기법은 Pinka의 multiparty 프로토콜과 같이 데이터 분산화를 통해 프라이버시를 보호한다.[11]

(3) 사물인터넷(IoT) 보안 침해 사례

스마트홈 가전 및 스마트 오피스 장치들의 등장으로 실생활은 편리해질 수 있지만 보안 취약점으로 인해 노출되는 정보에 의해 물리적 침임 등의 위협이 존재할 수 있다. 한 예로 미국 Nest사에서 판매하는 온도조절 장치의 경우, 집안에 사용자가 없으면 자동으로 온도가 조절되는 기능이 있는데 이러한 정보 유출로 집안의 부재가 외부로 알려져서 물리적 침입을 유도할 수도 있다. 또한, 불법적으로 누군가가 스마트 TV 등 카메라가 내장된 디바이스에 접근하면 사용자의 사생활이 고스란히 본인도 모르게 외부로 노출될 수 있다. 이외에도 비교적 관리가 소홀한 통신 기능이 내장된 스마트 냉장고에 누군가가 불법적으로 침입하여 스팸메일을 대량으로 발송할 수도 있다.

이처럼 사물인터넷을 중심으로 한 스마트 시대에 스마트폰으로 원격 조종하는 사물인터넷(IoT) 기기가 범죄에 악용될 가능성이 있다는 우려가 커지고 있으며 냉장고, TV 등 가전제품부터 자동차, 의료기기 등 IoT 기술을 접목한 기기가 잇달아 출시되고 있지만 해킹에는 무방비 상태라는 지적이 많다. 새 아파트를 중심으로 도입되고 있는 스마트홈 시스템이 보안에 취약한 대표적인 사례로 볼 수 있다. 스마트홈은 가전제품을 비롯해 수도, 전기, 냉난방 등 에너지 소비장치와 도어록, 폐쇄회로 TV(CCTV) 등 보안기기 등을 통신망으로 연결하여 제어하는 시스템이다. 스마트홈 시스템을 갖춘 아파트단지의 CCTV를 해킹 프로그램으로 쉽게 무력화할 수 있으며, 집주인 스마트폰으로 연결된 도어록은 스마트홈 앱(응용프로그램)을 악성코드에 감염시켜 관리자 권한을 얻으면 출입문을 간단하게 열 수 있어 뒤늦게 경찰이 현장에 도착해도 CCTV에는 아무 흔적도 남아 있지 않게 된다.[12]

실제로 2013년 미국 해커 축제인 데프콘에서는 트워터 엔지니어인 찰리 밀러 등 해커 2명이 일본 도요타 프리우스 2010년형 모델과 포드 이스케이프 2010년 모델을 해킹해 노트북으로 차량을 조작하는 시범을 보였다. 포드 이스케이프는 미국 판매량 1위를 차지할 정도로 베스트셀링 차량이며, 도요타 프리우스는 하이브리드카 분야에서 전세계 판매량 1위를 차지하는 차량이라는 점에서 보안 위협 발생 시 파급 효과가 매우 크다고 할 수 있다.[13]

11_ 서화정 외, 사물인터넷상에서의 보안과 프라이버시 보호 이슈, 정보처리학회지 제21권 제2호(2014.3.)

<표 1> 사물인터넷 해킹 사례

날짜	내용
2014년 08월	교통 신호등 해킹 뒤 신호 조작
2014년 11월	자동차 문 잠금 해제한 뒤 절도
2015년 07월	자동차 해킹 후 원격으로 핸들, 브레이크 조작
2015년 12월	아파트 도어록 해킹 후 출입문 열어
2016년 02월	CCTV 영상 불특정 다수에게 유포

※ 자료 : 한국경제(2016.5)

또한 스마트 TV, 스마트가전, 공유기, 스마트카, 교통, 의료기기 분야에 대한 보안 위협 시나리오를 보도한 자료에 따르면 각 기기의 보안 취약점이 노출되어 제어 네트워크에 접근할 경우에는 기기 및 인프라 조작이 가능한 것으로 나타났다.

<표 2> IoT 분야별 보안 위협 시나리오

분야	내용
스마트TV	'13년 8월, 미국 라스베이거스에서 스마트TV에 탑재된 카메라를 해킹해 사생활 영상을 유출하는 시연이 열려, 인터넷에 연결된 가정기기의 보안 취약성을 노출
스마트가전	'14년 9월, 서울 'ISEC 2014'에서 블랙펄 시큐리티는 로봇청소기 원격조종을 위해 필요한 앱의 인증방식 취약점과 로봇청소기에 연결되는 AP의 보안 설정상의 취약점 등을 이용 해킹하여, 로봇청소기에 탑재된 카메라로 실시간 모니터링이 가능하다는 것을 시연
공유기	'14년 3월, 보안컨설팅 업체인 Team Cymru는 해커들이 D-Link, Tenda, Micronet, TP-Link 등이 제조한 약 30만 개의 공유기를 해킹했다고 경고
스마트카	스페인 출신 해커 팀이 차량네트워크에 침투할 수 있는 조립 회로보드(20 달러)를 공개, 이를 통해 자동차업체가 컴퓨터시스템 검사를 위해 엔진내부에 설치한 차량용 제어구역네트워크(CAN)에 접근하여 브레이크 조작, 방향 설정, 경보장치 해제 등이 가능
교통	보안업체 IOActive Labs가 Sensys Networks의 도로차량 감지기술을 조사한 결과, 광범위한 설계 및 보안 결함을 발견. 특히 공격자는 센서를 가장해 교통관리시스템에 위조 데이터를 전송하거나 신호 등 같은 주요 인프라 통제가 가능
의료기기	'12년 블랙햇 보안 컨퍼런스에서 해커가 800미터 밖에서 인슐린 펌프를 조작하여 치명적인 복용량을 주입할 수 있음을 증명

※ 자료 : 보안뉴스 등 각 언론매체, IITP(2015.7) 재인용

(4) 사물인터넷(IoT) 보안 이슈

최근 국내 인터넷전문가협회가 인터넷 분야 전문가를 대상으로 한 설문 조사에 의하면, 사물인터넷 상용화를 위해 가장 필요한 조건으로 '철저한 보안'이 꼽혔으며, 사물인터넷 보급의 가장 큰 우려는 '해킹 위험'으로 조사되었다. 지금까지는 해킹 등으로 인해 보안 위협이 개인정보 유출, 금전상 손해 정도로 그치는 경우가 많았으나, 사물인터넷 환경에서의 보안 사고는 사회적 재해나 인명 사고로 이어진다는 데 문제의 심각성이 있다.[14] 이에, 사물인터넷 보안 이슈는 다음과 같이 정리할 수 있다.

먼저 기존에 인터넷 접속과 전혀 관련이 없는 사물 및 장치들이 사물인터넷 환경에서는 인터넷과 접속되어 다양한 서비스가 제공되기 때문에 기존 인터넷 환경에서 발생할 수 있는 모든 위험들과 취약점들은 사물인터넷에서도 발생할 수 있다. 즉, 자원이 제한적인 사물들과 저전력 통신 기술을 적용한

12_ 한국경제, ""앗! 누가 내집을 원격조종…" IoT기기 해킹 무방비"(2016.5.18.)

13_ Business watch, "사물인터넷(IoT)시대.'사물이 해킹에 노출됐다"(2015.6.10.)

네트워크에서는 기존 인터넷의 다양한 위협요소들이 모두 발생 가능하다는 것이다. 따라서 컴퓨팅, 저장 공간 등의 자원이 제한된 사물들을 위한 안전한 S/W 코딩 기술, 저전력 Crypto S/W 구현 기술 등 임베디드 보안 기술이 요구된다고 할 수 있다.

둘째, 개방형 플랫폼 소스는 공격자로 하여금 취약점을 찾기가 수월하기 때문에 보안 취약점을 이용한 공격 위협의 가능성이 높아질 수 있다. 다양한 기기로 구성되는 사물인터넷 환경의 경우, 악성 S/W, 바이러스 감염 등에 따른 공격 위협이 크게 증가할 것으로 예측된다.

셋째, 2015년 시만텍이 분석한 자료에 따르면 스마트홈 기기의 패스워드 강도, 상호 인증 또는 전사적 공격에 대한 계정 보호가 부족한 것으로 나타났다. 2015년 인텔의 McAfee 연구소의 위험 예측 보고서에서도 현재 널리 사용되고 있는 10대 기기를 대상으로 보안테스트를 실시한 결과 사물인터넷 기기의 보안 상태에 대해 경각심을 불러 일으킬 만한 통계 결과가 나왔다. 즉, 스마트홈 가전 및 스마트 오피스 장치들이 보안취약점에 쉽게 노출되어 있으며 복잡한 암호 구성 요구조건을 충족하지 못하는 등의 위협이 나타났다.

넷째, 사물인터넷 보안은 물리적 피해뿐만 아니라 사람의 생명도 위협할 수 있다는 점이 더 심각하다. 모바일 헬스케어를 포함한 다양한 의료장치와 자율주행 자동차를 포함한 교통 시스템의 경우에는 해킹으로 인한 오동작은 바로 사고로 이어지게 되며 사람의 생명과도 직결된 문제라고 볼 수 있다. 따라서 사람의 생명을 담보로 하는 사물인터넷은 새로운 보안 기술의 적용과 유관 정책이 반드시 수립되어야 하며, 악의적인 행위를 차단하기 위한 보안대책은 필수적이라 할 수 있다.[15]

4. 사물인터넷 표준 및 보안 추진 동향

(1) 사물인터넷(IoT) 표준 동향

사물인터넷은 다양한 사물 및 서비스 간 상호운용성을 기반으로 하므로 표준 정립이 아주 중요하며 보안 측면에서 위협 예방 및 대응 체계를 갖추기 위해서도 반드시 필요한 사항이다. 따라서 아직 표준이 확립되지 않은 상황에서 많은 업체와 단체들이 표준 정립을 위한 활동을 활발하게 전개해 나가고 있다.

2011년 설립된 Qivicon은 다양한 스마트홈 솔루션을 조합할 수 있는 벤더 중립적 솔루션을 목표로 하며, 삼성전자, 필립스 등 통신, 가전 분야의 약 30개 기업이 가입되어 있다. 2012년 7월 유럽, 미국, 한국 등 주요 국가별 표준화 기관이 공동으로 설립한 one M2M은 세계 주요 통신사와 기관이 가입한 세계 최대 규모의 표준화 단체이며, 글로벌 사물인터넷 서비스 플랫폼 표준을 목표로 하고 있다. 2013년 12월 설립된 AllSeen Alliance는 MS, 퀄컴, 일렉트로룩스, 소니, LG전자 등 S/W, 플랫폼, 반도체, 가전 등 다양한 분야의 업체가 참여하였으며, 오픈소스 IoT를 제공하는 비영리 컨소시엄이 목표이다. AllSeen Alliance에서 표준화한 오픈 소스 기반 IoT 플랫폼인 AllJoyn은 로컬 영역에서 기기 간 P2P 통신을 지원한다.

2014년 3월 설립된 IIC는 빅데이터에 대한 더욱 신뢰성 있는 액세스를 지원하여 모든 산업분야에 걸쳐 비즈니스 가치를 제고하고자 산업 현장에서 IoT를 적용하기 위한 표준을 목표로 한다. IEEE는 2014년 6월 P2413 프로젝트를 개시하여 타 플랫폼에서 유입되는 데이터를 공동의 이해가 가능한 데이터 객체로 변환하는 것을 목표로 향후 IoT가 적용될 부문의 기기 및 서비스 간 상호운용성을 보장하는 프레임워크를 구성하고자 한다. 2014년 7월 설립된 Thread Group은 IP를 기반으로 하는 가전 제품에 보안성을 갖춘 저전력 네트워크 솔루션을 개발하고자 하며, 같은 시기에 인텔, 델, 삼성전자 등이 설립한 OIC는 IoT 구성

14_ 정보통신기술진흥센터, IoT 보안 이슈와 시사점, 2015 ICT Spot Issue (2015.7.)

<표 3> IoT를 둘러싼 표준단체 개요

표준 단체	개요
Qivicon	2011년, 독일 통신사 DT의 주도로 설립된 Qivicon에는 EnBW, Miele, 삼성전자, Phillips 등 통신, 에너지, 가전 분야의 약 30개 기업이 가입
oneM2M	2012년 7월, 글로벌 사물인터넷 서비스 플랫폼 표준 개발을 위해 ETSI, TIA, ATIS 등 7개의 세계 주요 표준화 단체가 공동으로 oneM2M을 설립
AllSeen Alliance	2013년 12월, Qualcomm과 Linux Foundation은 Cisco, Microsoft, LG전자 등이 참가하는 표준단체 Allseen Alliance를 결성
IIC	2014년 3월, Intel과 Cisco, AT&T, GE, IBM은 산업용 IoT에 목적을 둔 표준을 개발하기 위해 IIC 결성을 발표, 이후 Microsoft가 합류
IEEE P2413	2014년 6월, IEEE는 IoT 아키텍쳐 구축을 통해 더욱 다양한 산업과 기술 영역으로의 확장을 목적으로 IEEE P2413 프로젝트를 공식 개시
Thread Group	2014년 7월, Google(Nest Labs) 주도의 사물인터넷 프로토콜 컨소시엄인 Thread Group에 삼성전자, ARM, Freescale, Silicon Labs 등이 참여
OIC	2014년 7월, Intel, Atmel, Dell, 삼성전자 등은 Qualcomm 주도의 Allseen Alliance에 대항하고, IoT 기기의 연결성 확보를 목표로 OIC를 설립

※ 자료: 각 표준단체 홈페이지, 언론매체 재정리, IITP(2014.4.)

기기 간의 연결 요건 정의 및 상호운용성 보장을 목표로 하는 비영리기관이다.

IoT 기기들의 상호운용성을 위해서는 범용 표준 마련이 우선적으로 필요한 상황임에도 불구하고 현재 IoT 기술을 주도하는 글로벌 표준이 없기 때문에 다양한 표준화 기구들이 각자의 특장점을 바탕으로 연구개발을 진행하고 있다. 올해 초 세계 최대 가전 전시회 CES 2016에서 SK텔레콤, 삼성전자, 아트멜, 액스톤 등이 One M2M과 OIC를 연동한 솔루션을 이용한 IoT 시연을 선보이기도 하였는데 서로 다른 기기에서 IoT 표준을 기반으로 서비스를 연동하여 새로운 서비스로 창출하는 모습으로 발전하게 될 것으로 예상된다. 또한, 향후 IoT 시장에 진입하기 위해서는 글로벌 업체 간 경쟁 및 협력을 통한 표준간 연동이 불가피해 질 것으로 전망된다.

(2) 사물인터넷(Iot) 보안 추진 동향

우리나라는 2013년 7월 '국가 사이버안보 종합대책'을 관계부처 합동으로 수립하였다. 이는 국가안보를 위협하는 사이버위협에 대한 범국가적 대응을 위해 마련한 것으로 ① 사이버위협정보 공유시스템 구축, ② 집적정보통신시설(IDC)·의료기관 등을 포함한 주요 정보통신기반시설을 확대하고 국가기반시설에 대해 인터넷망과 분리하여 운영하며 위기대응훈련을 실시, ③ 최정예 정보보호 전문가 양성사업 확대 및 영재교육원 설립 등 다양한 인력양성 프로그램 추진 등을 주요 내용으로 하고 있다.

또한, 미래창조과학부는 2015년 6월 '사물인터넷(IoT) 정보보호 로드맵'을 수립하여 3개년 실행계획을 발표하였다. 누구나 안전하게 사물인터넷의 편리함을 누리는 세계 최고의 스마트 안심국가 실현을 비전으로 삼아 ① 보안이 내재화된 IoT 기반 조성, ② 글로벌 IoT 보안 핵심기술 개발, ③ IoT 보안 산업경쟁력 강화를 추진전략으로 세웠다. 이어 발표한 '사물인터넷 공통 보안 7대 원칙'에서 ① 정보보호와 프라이버시 강화를 고려한 IoT 제품 및 서비스 설계, ② 안전한 소프트웨어 및 하드웨어 개발기술 적용 및 검증, ③ 안전한 초기 보안 설정 방안 제공, ④ 보안 프로토콜 준수 및 안전한 파라미터 설정, ⑤ 사물인터넷 제품 및 서비스의 취약점 보안 패치 및 업데이트 지속 이행, ⑥ 안전한 운영·관리를 위한 정보보호와 프라이버시 관리체계 마련, ⑦ IoT 침해사고 대응체계와 책임추적을 확보할 수 있는 방안 마련을 발표하였다.

15_ KISA, "2015 국내 정보보호산업 실태조사"(2015.12.)

미국은 '13년 트렌드넷의 CCTV 보안 결함 사건을 계기로 관련 지침 마련을 위한 공공·민간 전문가 의견 수렴에 나서는 등 IoT 보안 정책 수립의 초기 단계에 진입하였다.[16] 버락 오마바 미국 대통령은 점증하는 사이버보안 위협에 대처하기 위하여 사이버공격을 시도한 개인과 단체는 자산을 동결하는 등의 강력한 금융 제재를 가할 수 있는 행정명령(executive order)에 서명(2015.04.02.)하였다.[17]

미 연방수사국(FBI)은 2015년 9월 10일 기업과 가정에서의 효율성과 편의성을 높여주는 사물인터넷 기기 사용이 증가함에 따라 사이버 보안 위협이 높아지고 있다고 경고하였다. 사물인터넷 기기는 인터넷에 자동 연결되어 데이터 송수신이 가능한 기기나 물체를 말하며 사물인터넷 기기들 중 초기 비밀번호가 변경되지 않았거나, 공개형 와이파이를 통해 연결된 디바이스들이 사이버 범죄자에 악용될 수 있는 가장 손쉬운 대상이라고 지적하였다. 사물인터넷 기기에 대한 불충분한 보안 역량, 보안 패치 설치의 어려움, 사용자들의 보안 부주의로 사물인터넷 기기가 사이버 범죄에 악용될 위험이 발생한다. 사이버 범죄자들은 사물인터넷 기기를 통해 다른 시스템에 대한 원격 공격, 악성/스팸 메일 발송, 개인정보 탈취, 신체에 대한 안전 위협이 가능하다고 한다. FBI는 사용자 보호와 방어를 위한 방법으로 ① 사물인터넷 기기들을 자체 보호된 네트워크에 격리, ②라우터에서 UPnp 비활성화, ③의도한 목적에 적합한 사물인터넷 기기인지를 고려, ④보안이 적용된 기기들을 제공한다는 기록을 보유한 제조사의 제품 구매, ⑤가능한 한 사물인터넷 기기의 보안 패치를 최신버전으로 유지, ⑥사물인터넷 기기 및 가전 기기들의 기능을 숙지하고, 디바이스가 초기 비밀번호 또는 개방형 와이파이 연결로 설정되어 있다면 비밀번호를 바꾸고 보호되는 네트워크에서만 작동되도록 설정 변경, ⑦무선 네트워크에 사물인터넷 기기를 연결하고 원격으로 접속할 때는 현재까지의 우수 사례를 따를 것, ⑧환자들은 가정에서 사용하도록 처방된 모든 의료기기의 기능을 사전에 설명받고 원격조종이나 데이터 송수신이 가능한 경우, 악성 행위의 목표가 될 수 있는지 숙지, ⑨제조사가 초기에 설정한 기기의 비밀번호들은 보안성이 높은 비밀번호로 변경 등 9가지를 제시하였다.[18]

유럽에서는 기본적으로 권고사항 및 가이드라인 형태의 IoT 보안 지침을 통해 시장의 자율규제를 촉구하는 기조를 보이며, IoT 보안 기술개발 및 인증, 표준화 작업에 초점을 두고 있다. 또한, 중국은 우리나라와

<표 4> 주요국의 IoT 보안 추진 동향

국가	주요내용
한국	• 정부는 사물인터넷 기술개발을 활성화를 위해 기본계획을 수립하였고 사이버 위협의 범국가적 대응을 위해 사이버안보 종합대책을 마련하였으며, 최근 사물인터넷에서의 정보보호에 초점을 맞춘 정책을 수립·발표함 ※ 미래창조과학부는 '사물인터넷(IoT) 정보보호 로드맵' 수립('15.6.)
미국	• IoT를 중심축에 둔 보안 정책이나 법제도가 아직 정립되지 않았으나, 특정 분야에 대한 사이버보안 강화 정책은 지속적으로 추진 중임 ※ 백악관은 주요 기반시설을 겨냥한 사이버공격에 대응하기 위해 대통령 행정명령을 발동하고, 미국 NIST(국립표준기술연구소)의 주도 하에 사이버보안 프레임워크를 수립('13.2.)
유럽	• EC(유럽위원회)는 IoT가 확산됨에 따라 보안 위협이나 사생활 침해 등의 부작용이 발생할 수 있음을 인지하고, 지속적인 공공-민간 의견수렴을 통해 필요한 제도적 기반을 준비 중임 ※ 유럽 IoT 연구단(European Research Cluster on the Internet of Things)에서는 IoT와 관련된 전반적인 기술연구가 이뤄지고 있으며, 이 중에는 IoT 보안 관련 연구과제도 포함
중국	• '11년 12월 중국 MMIT(공업정보화부)는 IoT 정책을 구체화한 '사물인터넷 12차 5개년 계획을 공개하고, 원천기술 혁신, 산업 생태계 육성, 기술 응용 수준 제고 등의 목표를 설정함 • 또한, 사물인터넷 발전 10개 전문 행동계획을 수립하고 핵심 보안기술 개발 및 보안 테스트 평가 플랫폼 구축을 추진하는 등 자국의 보안 역량 강화를 모색 중임

※ 자료 : KISA 자료 발췌, IITP(2015.7.) 재정리

16_ 정보통신기술진흥센터(IITP), IoT 보안 이슈와 시사점, 2015 ICT Spot Issue(2015.7.)

17_ 한국정보화진흥원, "오바마, 새로운 사이버보안 행정명령에 서명", ICT Issues Weekly(2015.4.17.)

마찬가지로 사물인터넷을 미래핵심 산업으로 육성시키기 위해 사물인터넷 핵심 원천기술 확보의 일환으로 사물인터넷 보안 강화를 도모하고 있다.[19]

5. 사물인터넷(IoT) 보안 전망 및 시사점

(1) 사물인터넷(IoT) 보안 전망

사물인터넷 기술이 산업으로 확대되기 위해서는 관련 기술 개발과 함께 보안 및 프라이버시 보호와 글로벌 표준 확립 등의 당면과제가 선제적으로 해결되어야 한다. 사물인터넷 기기에 보안 취약점이 존재하여 사용자의 생명과 안전에 위협을 받는 경우에는 상품화 될 수 없을 정도로 보안 위협은 시장진입의 방해요소로 작용할 수 있기 때문에 사물인터넷에서 보안기술은 센서나 네트워크 기술만큼 필수적이다.

2016년 전 세계 사물인터넷(IoT) 보안 지출 규모가 전년대비 23.7% 증가한 3억 4,800만 달러에 이를 것으로 가트너가 전망하였다. 나아가, 2018년에는 사물인터넷 보안 지출 규모가 5억 4,700만 달러에 달할 것으로 내다봤다. 가트너는 전반적으로 지출이 초반에 완만한 형태를 보이는데 반해, 사물인터넷 보안 지출은 기술력 향상, 조직 변화 및 확장 가능한 서비스 옵션이 늘어남에 따라 2020년 이후에는 보다 빠른 속도로 증가할 것으로 분석했다.

또한, 사물인터넷이 발전함에 따라 현재 발생하는 위협이 사물인터넷 기기를 통해 더욱 빠르게 확산되고 다양한 형태로 공격이 변이될 것으로 판단되기에 사물인터넷 보안 시장은 더욱 커질 수 밖에 없다.

일반 소비자 및 각 산업 분야의 사물인터넷 도입율은 사물인터넷 보안 제품 시장에 밀접한 영향을 미치고 있다. 또한, 커넥티드 카뿐 만 아니라, 대형 트럭, 민간 항공기, 농기구 및 건설 장비와 같은 기타 복합 기계 및 차량이 향후 엔드포인트(Endpoint) 보안 지출을 주도할 것으로 예상된다.[20]

<표 5> 전 세계 IoT 보안 지출 전망 (단위 : 백만 달러)

	2014년	2015년	2016년	2017년	2018년
보안 지출	231.86	281.54	348.32	433.95	547.20

※ 자료 : 가트너(2016.4.), CIOKOREA(2016.4.28.) 재인용

(2) 시사점

사물인터넷 시대에서의 보안 위협은 실생활과 관련된 사물로 확대되면서 사람의 생명을 위협할 수도 있고 전쟁을 방불케 하는 사회 혼란을 야기할 수도 있으며 피해 속도 및 규모도 상상할 수 없을 정도로 커질 것이므로 사회적 비용 부담은 기하 급수적으로 증가할 수 밖에 없다.

따라서 사물인터넷 보안에 대한 우려는 사물인터넷 산업 성장을 저해하는 가장 큰 요인으로 작용하기 때문에 완벽한 보안이 반드시 실현될 필요가 있다. 사물인터넷 보안은 기존 PC, 모바일기기 중심의 사이버환경과 달리 그 보호대상 범위, 대상 특성, 보안담당 주체, 보호방법 등에 있어 새로운 시각으로 접근해야 한다.

과거에는 보호 대상이 한정되어 있었지만 사물인터넷 시대에는 웨어러블, 가전, 자동차, 의료기기 등 사물인터넷에 연결되는 모든 사물로 확대되고 기존 고전력·고성능의 보호대상이 초경량·저전력·저성능의

18_ 안승구 외, 국내외 사물인터넷(IoT) 정책 추진 방향, KISTEP Inl 13호(2016.4.)

19_ 정보통신기술진흥센터(IITP), IoT 보안 이슈와 시사점, 2015 ICT Spot Issue(2015.7.)

사물로 대폭 확대된다. 그리고 보안 주체도 과거에는 ISP(Internet Service Provider), 보안업체, 이용자로 국한되어 있었지만 사물인터넷 시대에는 이들 보안 주체를 포함하여 제조업체까지 확대되고, 보호 방법에 있어서도 기존에는 별도의 보안장비로 보호대상들을 보호했지만 사물인터넷 시대에는 수 많은 보호대상들을 통제하고 관리하기 힘들기 때문에 표준화기술획득을 통한 기기의 자체 보안 기능 확보 및 설계 단계부터 보안 내재화를 위한 보안칩셋과 임베디드 보안기술 개발에 힘써야 한다. 그리고 새로운 기기 및 서비스의 출현에 대비하여 새로운 보안기술과 기존 사이버 보안 기술의 적절한 조화를 통해 보안 방식 간의 혼돈을 최소화하면서 효율적으로 사물인터넷 보안 능력을 향상 시킬 방안을 모색할 필요가 있다.

또한, 센서·기기, 통신·네트워크, 플랫폼, 응용서비스로 세분화하여 각각의 보안 대책은 물론 전체적인 관점에서 대응할 필요가 있다. 사물인터넷 기기 및 서비스는 설계 단계부터 보안 기법을 적용해야 하며 사물간 접속 및 정보 전송 시에도 인증 및 암호화 기술을 적용하고 원격 기기에 대한 지속적인 보안업데이트 뿐 만 아니라 개인정보보호를 위한 적극적인 보호 조치를 취하는 것은 사물인터넷 보안을 위한 최소한의 요구 사항이라고 할 수 있다. 아울러 새로운 보안 위협에 대한 신속한 탐지와 분석을 통해 사전에 보안 위협을 회피하고 방지할 수 있는 종합적인 대응체계를 마련하고 현재 추진 중인 Iot 리바이스 보안인증제도를 차질없이 추진해야 할 필요가 있다.

국내 보안 업체는 원천기술 확보 부족으로 사물인터넷 보안 기술 및 산업 주도는 쉽지 않은 상황에 놓여 있다. 결국 국내 사물인터넷 보안 시장조차도 대형 사물인터넷 제품 제조업체(삼성전자, LG전자 등), 대형 이동통신사(SKT, KT, LGU+ 등), 글로벌 보안업체(시스코 등)를 중심으로 치열한 주도권 경쟁이 이뤄질 것이다. 따라서 국내 보안 중소기업 및 스타트업의 성장을 도모하기 위하여 사물인터넷 보안 원천기술 개발 및 확보를 위한 정부의 적극적인 지원과 함께 사물인터넷 제품 혹은 통신망을 보유하고 있는 국내 대기업 및 통신업체들과의 상생 환경을 조성하는데도 적극 나서야 한다.

향후, 사물인터넷 보안 위협에 대응하기 위한 전문 인력의 수요가 증대될 것으로 예상되므로 Iot 관련 산업의 안정적인 발전을 도모하기 위하여 사물인터넷 보안 전문 인력 양성 및 안정적인 수급을 위한 대책 마련도 필요하다.

● 참고문헌

- ATARC 보도자료, http://www.atarc.org/wp-content/upload/2015/11/ATARC-IoT -Innovation-Lab-Report-2015-11-18.pdf(2015.11.18.)
- Business watch, "사물인터넷(IoT)시대.'사물이 해킹에 노출됐다"(2015.6.10.)
- CIOKOREA, "2016년 전세계 IoT 보안 지출, 전년대비 23.7% 증가" 가트너 전망(2016.4.28.)
- Mckinsey Global Institute, "THE INTERNET OF THINGS: MAPPING THE VALUE BEYOND THE HYPE."(2015.6.)
- 김호원, 사물인터넷 환경에서의 보안/프라이버시 이슈, TTA Journal Vol.153(14.5.6.)
- 박유리 등, "인터넷의 진화와 사회경제적 패러다임 변화 연구 : 사물인터넷을 중심으로", KISDI, 기본연구 15-01(2015.11.)
- 산업경제리서치 "사물인터넷(Iot) 활용분야별 비즈니스 현황과 최근 주요 이슈 종합분석"(2016.5.27.)
- 서화정 외, 사물인터넷상에서의 보안과 프라이버시 보호 이슈, 정보처리학회지 제21권 제2호(2014.3.)
- 안승구 외, 국내외 사물인터넷(IoT) 정책 추진 방향, KISTEP Inl 13호(2016.4.)
- 장봉임 외, 사물인터넷 보안 기술 연구, 보안공학연구논문지 Vol.11, No.5(2014.10.4.)
- 정보통신기술진흥센터(IITP), IoT 보안 이슈와 시사점, 2015 ICT Spot Issue(2015.7.)
- 정보통신정책연구원, 인터넷 진화와 사회경제적 패러다임 변화 연구(사물인터넷을 중심으로)(2015.11.)
- 중앙SUNDAY, "해킹 위험 커지는 IoT, 철통 보안시스템 갖춰야"(2016.3.27.)
- 커넥팅랩, 사물인터넷-클라우드와 빅데이터를 뛰어넘는 거대한 연결(2014.6.25.)
- 한국경제, ""앗! 누가 내집을 원격조종…" IoT기기 해킹 무방비"(2016.5.18.)
- 한국인터넷진흥원, IoT 제품 및 서비스 보안성 강화방안 연구(2015.9.)
- 한국인터넷진흥원, 2015 국내 정보보호산업 실태조사(2015.12.)
- 한국정보화진흥원, "오바마, 새로운 사이버보안 행정명령에 서명", ICT Issues Weekly(2015.4.17.)

20_ CIOKOREA, "2016년 전세계 IoT 보안 지출, 전년대비 23.7% 증가" 가트너 전망(2016.4.28.)