Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.3, Jun. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.3.607

IoT 기기의 보안성 확보를 위한 제도적 개선방안*

이 동 혁,[1,2†] 박 남 제[3‡]
[1]제주대학교 일반대학원, [2]제주대학교 초등교육연구소, [3]제주대학교 초등컴퓨터교육전공

Institutional Improvements for Security of IoT Devices*

Donghyeok Lee,[1,2†] Namje Park[3‡]
[1]Graduate School, Jeju National University,
[2]Primary Education Research Institute, Jeju National University,
[3]Dept. of Computer Edu., Teachers College, Jeju National University

요 약

최근 다양한 기능을 가진 IoT 제품이 개발되고 있으며, 사물과 정보기술의 결합을 통해 기존에는 미처 상상하지 못했던 편리한 서비스가 등장하고 있다. 안전한 IoT 환경을 위해서는 제품의 보안성이 필수적으로 고려되어야 하나, 기존 IoT 제품에서는 보안 취약성이 발견되는 등 다양한 문제점이 발생하고 있다. IoT 제품의 보안성 확보를 위해서는 기술적 대응방안과 함께 정책적인 대응방안도 필요하다. 그러나 현행의 IoT 제품에 관련된 법제도는 IoT 환경에서의 안전을 보장하기에는 한계점이 존재한다. 본 논문에서는 이러한 현행 IoT 관련 법제도의 한계점을 분석하고, 이에 대한 개선방안을 제시하고자 한다.

ABSTRACT

Recently, IoT products with various functions are being developed. Through the combination of objects and information technology, convenient services that have not been imagined before are emerging. For a secure IoT environment, product security must be considered. However, the existing IoT products have various problems such as security vulnerability. In order to secure the security of IoT products, technical countermeasures as well as policy responses are needed. However, the legislation related to current IoT products has a limit to guarantee safety in IoT environment. In this paper, we analyze the limitations of the current legal system of IoT, and suggests ways to improve it.

Keywords: IoT, IoT devices, Informatin security, IoT security

I. 서 론

IoT 환경이 어느새 현실로 다가왔다. IoT 환경은 물리적 제품과 정보통신 기술이 결합하여 생활에 필요한 다양한 서비스를 제공해 줄 것이며, 사용자는 기존보다 더욱 편리한 생활을 영위할 수 있을 것이다. 향후 IoT 제품이 점차 지능화 되어감에 따라, 기존에는 상상하지 못했던 여러 다양한 서비스를 제공받을 수 있게 될 것이며, IoT 시장은 점차 확대되어 미래의 주요한 성장 동력으로 작용할 것으로 보인다[1,2,3].

그러나, 이러한 이면에는 IoT 환경의 특성에 따른 다양한 위협요소가 도사리고 있다. IoT의 주요 분야인 홈/가전, 의료, 교통, 에너지, 제조분야 등에서 다양한 해킹 사례가 보고되었으며, 향후 스마트 홈/가전, 커넥티드 카와 같은 IoT 제품과 서비스가 생활 깊숙이 보편화되는 본격적인 IoT 시대를 맞게 되면, 기존에는 생각지 못했던 다양한 위협을 직면하게

Received(02. 03. 2017), Modified(04. 07. 2017), Accepted(04. 17. 2017)
* 이 논문은 2016년도 정부(교육부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(과제번호:NRF-2016R1D1A3A03918513)
† 주저자, bonfard@jejunu.ac.kr
‡ 교신저자, namjepark@jejunu.ac.kr(Corresponding author)

될 것이다[4].

보안에 대한 우려는 아무리 크더라도 지나치지 않으며, 이에 대한 완벽한 대응책이 필요하다. 특히, IoT 환경에서는 기존의 정보통신 환경에 비해 더욱 다양한 보안 위협요소를 안고 있다. 물리적 기기들이 서로 연결된다는 것은 원격 해킹에 용이한 환경을 제공하는 측면에서 바라볼 수도 있다. 해킹을 통한 원격 조작 등으로 사용자에게 재산적, 신체적 피해를 직접적으로 발생시키는 것은 실제로 가능한 일이며, 다양한 IoT 제품에서 보안 결함이 발견된 사례가 있다[5].

이를 위해 제품 출시 전 설계 및 개발단계에서 기술적인 보호조치가 당연히 수반되어야 하며, 이에 따른 법제도적 대책도 함께 요구된다. 그러나 현행 법제도상의 보안 규정으로는 IoT 제품의 보안성을 완전히 보장하기에는 한계점이 있다[6,7,8].

본 논문에서는 IoT 제품에 대한 법제도적 현황과 한계점을 분석하고, 안전한 IoT 환경을 법제도적 개선방안에 대하여 제시해 보고자 한다.

II. 관련 연구

본 장에서는 IoT 제품에 대한 정보보호 위협요소와 관련 제도 현황을 살펴본다.

2.1 IoT 환경에서의 정보보호 위협

2.1.1 물리적 특성에 따른 보안 위협

IoT 환경은 기본적으로 사물이 인터넷에 연결되는 특성을 가지며, 이러한 점은 기존의 IT 환경보다 더욱 많은 보안 취약성을 가질 수 있다. 즉, 기본적으로 기존의 정보통신 환경에서 갖는 보안 취약성은 그대로 가질 수 있으며, 물리 환경과 연동되는 과정에서의 보안 취약성 및 IoT 디바이스 자체의 보안 결함에 따른 디바이스의 무력화, 오용, 작동 정지, 기기 손상 등 다양한 증상을 야기할 수 있다. 이러한 문제점은 해당 IoT 디바이스와 직간접적으로 연동되는 타 IoT 디바이스의 작동에도 영향을 미치게 된다. 또한, IoT 제품의 보안 취약점은 사용자에게 신체적, 재산적 피해를 야기할 수 있다. 예를 들어, 스마트도어락의 해킹이 발생하였을 경우, 원격에서 문의 개폐가 가능해짐에 따라 사용자의 직접적인 재산피해를 발생시킬 수 있으며, 스마트 가스밸브의 해킹이 발생하였을 경우는 오작동이나 과도한 작동으로 사용자의 신체적 안전을 직접적으로 위협할 수 있다.

IoT 환경이 본격적으로 도래하고 있는 현 시점에서, 이와 같은 보안 위협은 반드시 해결되어야 한다. 실제로 IoT 제품에 대한 다양한 보안 취약점이 보고되고 있으며, 실질적으로 IoT 제품이 해킹을 당한 사례 또한 다수 보고되고 있다. 예를 들어, 유아 모니터링 제품 상당수가 보안 취약점에 노출되어 있으며, 이러한 보안 취약점에 따라 카메라를 해킹하여 영상 링크를 유포하는 등의 사례가 발생한 바 있다.

또한, 2013년 미국 FDA에서 네트워크에 연결된 의료기기가 악성코드에 감염된 사례를 발표한 적이 있으며, 블랙햇 컨퍼런스에서는 의료기기 해킹을 통한 약물 과다 투여 상황을 직접 시연한 바가 있다.

한편, IoT 환경은 다양한 사회 분야에서 활용되고 있으며, 인간의 생활과 밀접하게 연관되어 있다. EU FP7 프로젝트를 수행 중인 IERC의 분류[9]에 따르면, 도시, 환경, 보안/안전, 산업분야에서의 IoT의 활용분야는 Table 1.과 같으며, IoT 기기의 해킹을 통하여 이와 같은 사회적 서비스가 정상적으로 작동하게 되지 않아 큰 혼란을 초래할 수 있다.

실제로 2012년, 미국에서 암호화 및 인증절차 부재로 인한 교통표시판(VMS) 및 교통제어 시스템이 해킹 된 바 있으며, 2013년에는 미국 오하이오의 원자력 발전소 보안 모니터링 시스템이 작동불능 상태가 된 적이 있다. 또한 2014년에는 독일의 철강회사를 대상으로 하여 실제 피해를 입힌 바 있다.

IoT 환경은 이와 같이 해킹을 당할 경우 개인 뿐 아니라 사회적인 영향을 미치게 될 수 있어 철저한 보안 대책이 필요한 상황이다.

Table 1. Application Areas of IoT

Category	Application Areas
Smart Cities	Noise Urban Maps, Waste Management, Intelligent Transportation Systems
Smart Environment	Forest Fire Detection, Air Pollution, Landslide and Avalanche Prevention
Security & Emergencies	Perimeter Access Control, Radiation Levels, Explosive and Hazardous Gases
Industrial Control	M2M Applications, Temperature Monitoring, Ozone Presence

2.1.2 IoT 기기의 보안 취약성

IoT 기기는 여러 보안 취약 요소가 존재한다. 만약 로컬 API가 평문을 기준으로 인터페이스가 구성된다면, 암호화되지 않은 상태에서 통신상으로 전송될 것이며, 이러한 점은 보안상 큰 문제를 야기한다. 비록 API상에서 암호화를 지원하더라도 IoT 장치간 통신을 위한 최신 암호화 표준을 적시에 지원하기 어렵다는 문제도 존재한다. 암호화 표준을 시기적절하게 적용하려면 IoT 디바이스에 연결된 모든 장치가 소프트웨어 업데이트 기능을 지원해야 하며, 업데이트가 실시간으로 이루어져야 한다. 그렇지 않으면 IoT 디바이스에 탑재된 소프트웨어 버전의 차이로 기기간 암호화 통신에 문제가 발생할 수도 있다.

한편, IoT 제품의 원격 쉘로 접근이 가능하게 될 경우에도 보안상 심각한 문제가 발생할 수 있다. 이러한 경우 침입자는 기기를 정상작동하지 않게 하거나, 기기 자체를 무력화시킬 수 있다. 또한 중요 데이터를 평문으로 저장하게 될 경우 인가되지 않은 자가 데이터에 접근하여 정보를 가져가거나 조작하게 될 수도 있다. 따라서, 해킹 방지를 위하여 IoT 제품에 대한 원격 쉘 접근은 제품 출시 이후에는 가능하지 않도록 차단하여야 하며, IoT 기기내의 중요 데이터는 반드시 암호화하여 보관하여야 한다[10].

IoT 기기 자체의 물리적 파괴나 분실이 발생할 수 도 있다. 이러한 경우는 통신기능 상실로 인하여 IoT 서비스의 중단을 야기할 수 있다. 또한, 기기 분실의 경우는 기기 내부에 포함된 개인정보 유출로도 이어질 수 있다.

IoT 기기를 대상으로 한 서비스 거부(Denial of Service) 공격이 발생할 수 있다. 단말이나 센서는 정상적인 서비스 제공을 위하여 이들을 관리하는 게이트웨이를 통해 원격에서 연결요청이 수시로 수행될 것이며, 이를 기반으로 악의를 가진 공격자가 대량의 연결요청을 지속적으로 전송하는 것으로 서비스 공격을 일으킬 수 있으며, 이러한 공격에 따라 기기 자체의 전력 소모를 야기하여 결과적으로 정상적인 서비스가 이루어지지 않도록 할 수도 있다[11].

따라서, IoT 기기의 보안을 위해서는 검증된 보안 통신 프로토콜을 사용할 필요가 있다. 현재 IoT 보안을 위하여 다양한 국내외 표준 기구 및 사설 표준 기구에서 논의하고 있다. 표준화는 ITU, ETSI, IETF등에서 주도하고 있는 상황이며, IETF는 저전력/저성능의 경량화된 방식으로 메시지를 주고받을 수 있는 CoAP를 표준화하고 있다[12].

CoAP는 REST 구조 기반의 프로토콜로 멀티캐스트 지원이 가능한 특징이 있으며, 빠른 서비스의 제공이 가능한 DTLS에 기반한 보안을 제공한다는 특징이 있다. 또한, OMA의 LwM2M 구조에서도 CoAP와 DTLS를 전송 프로토콜로 권고하고 있으며, LwM2M은 ETSI에서 규격 표준화를 진행중이며, 인증, 기밀성, 무결성의 제공이 가능하다.

2.2 IoT 제품 보안의 두가지 관점

IoT 제품에 대한 제도적인 보안성을 확보하는 방법에는 크게 두 가지의 관점이 존재한다.

먼저, 제품 출시 전 단계에서의 보안성 확보 방법으로, 적절한 규제를 통하여 보안상 안전이 검증된 제품만을 출시하도록 하는 방법이다. 이는 제품의 설계/개발 단계에서 사전에 해당 규제를 충분히 만족하도록 하는 것이며, 안전한 IoT 환경을 위해서는 최소한의 강력한 규제가 필요하다고 볼 수 있다. 이러한 제도가 정착되면 기본적인 보안성이 확보되지 않은 제품은 시장에 출시되지 않을 것이다.

두번째 관점으로, 제품 출시 이후의 사후관리가 필요하다. 이는 IoT 제품의 운영/관리 단계에서 필요한 부분에 해당한다. 제품의 출시 전에 미처 발견되지 않았던 보안상의 허점이 제품 출시 이후에 발견될 수도 있으며, 이러한 취약점이 발견된 경우에는 기본적으로 소프트웨어 업데이트로 해결해야 하며, 이를 위해 IoT 제품에는 자동 업데이트 기능 탑재가 필수적으로 요구된다. 그러나 경우에 따라 소프트웨어 업데이트가 불가능한 경우나, 하드웨어 결함이 존재하는 경우에는 리콜과 같은 대책을 실시할 필요가 있다. 또한 보안 허점을 통하여 사용자의 신체적, 재산적 안전에 큰 영향을 미칠 수 있는 경우에는 즉시 해당 제품에 대하여 수거 또는 파기와 같은 조치가 필요할 수도 있다. 3장에서는 IoT 제품 보안의 현행 법제도적 한계점을 제도상의 규제와 사후관리의 두가지 관점에서 분석한다.

III. 현행 법제도의 한계점

본 장에서는 먼저 현행의 IoT 제품 관련 제도적 현황을 살펴본다. 이후 2절 및 3절에서는 현행 IoT 관련 법제도에 대하여 제품 보안성 확보 및 사후 보안성 관리의 관점에서 바라본 한계점을 분석한다.

3.1 IoT 제품 관련 제도 현황

현재 각 부처에서는 제품 생산시에 필요한 인증제도를 운영하고 있다. 품질인증이란 해당 제품이 특정 품질 기준을 준수하여 적합하다는 평가를 받음으로써 지속적으로 생산할 자격을 갖추었는지를 증명하기 위한 제도이다.

인증제도는 개별 법령에 의해 운영되는 강제인증과 필요에 의해 이루어지는 임의인증으로 구분되며, 이는 강제성 여부가 주요 기준이 된다. 또한, 법적 근거의 유무에 따라 법정인증제도와 민간인증제도로 구분할 수도 있다. 현재 각 부처에서 인증, 형식승인 검정, 형식검정, 형식등록 등 제품의 특징에 따라 다양한 명칭으로 운영되고 있다.

국가기술표준원에서는 국가표준인증 통합정보시스템인 e나라 표준인증(http://standard.go.kr)을 운영하고 있으며 국가/국제 표준과 국내 부처별 각 인증제도 현황을 제공한다.

2017년 2월 현재 각 부처별 다양한 인증제가 존재하고 있으며, 법정의무 72건, 법정임의 98건으로 총 170건의 등록인증이 실시되고 있다.

각 인증제는 관련 법률에 근거하고 있다. '전기용품안전관리제도'는 전기용품 안전관리법에 근거하며, 산업통상자원부가 소관하고 있다. 이는 IoT 홈/가전 제품에서 의무적으로 받아야 하는 인증이며, 전기용품을 생산/조립/가공하거나 판매/대여 혹은 사용할 때의 안전관리에 대한 사항을 규정하고 있다.

또한 스마트미터의 계량기에 적용될 수 있는 '계량기 형식승인 및 검정' 제도가 산업안전보건법에 근거하여 법정의무사항으로 실시되고 있다. 한편, 커넥티드 카에 실시될 수 있는 '자동차 및 자동차부품 자기인증'이 자동차관리법에 근거하여 국토부의 소관으로 실시되고 있다.

이와 같이 다양한 법령에 근거하여 IoT 제품에 적용되는 품질인증제도가 국내에 운영되고 있으나, 해당 품질인증제도는 대부분 보안에 대한 사항은 고려하지 않고 있는 실정이다.

한편, 관련법에 근거하는 기술기준도 존재한다. 기술기준이란 정부와 단체에 의해 채택되었거나 계약에 의해 채택되어 법적 구속력을 갖는 표준으로, 적용 가능한 행정규정을 포함하여 상품의 특성 또는 관련 공정 및 생산방법이 규정되어 있어 강제적인 준수가 필요하며 상품, 공정 및 생산방법에 적용되는 기술규범을 의미한다. 이러한 기술기준은 각 부처가 소관 분야에 따라 개별적으로 관리운영을 실시하고 있다. 본 논문에서 법정의무 인증제와 기술기준을 다루는 이유는, 해당 제도에 대응하는 IoT 제품 출고시 인증제 및 기술기준에 필수적으로 적합해야 하며, 이러한 점에 근거하여 제품 출시 이전에 제도적인 강제성을 부여할 수 있다는 특징이 있기 때문이다. 즉, 해당 인증제도 및 기술기준에 대해 보안성에 대한 항목을 추가하는 것만으로 IoT 제품의 정책적 보안 규제가 이루어질 수 있다는 점에서 의의가 크다. 이에 대한 세부 사항은 3.2, 3.3절 및 4장에서 후술한다.

3.2 제품 보안성 확보에 대한 법제도적 한계

현재 많은 IoT 제품이 시장에 출고되고 있다. 그러나 제품의 보안성에 대한 법제도적 대응책은 미비한 상태에 있는 실정이다.

한국인터넷진흥원(KISA)에서는 IoT 보안과 관련된 몇 가지의 기술안내서를 제공하고 있다. 여기에는 IoT 제품 개발 시 공통적으로 고려해야 할 보안 원칙과 가이드라인을 제시하고 있는 'IoT 공통보안 원칙', 'IoT 공통보안 가이드'가 있으며, IoT 환경에서의 경량 암호화 활용을 위한 '사물인터넷(IoT) 환경에서의 암호인증기술 이용 안내서'가 존재하고 있다.

그러나 해당 기술안내서는 IoT 제품 설계 및 개발 단계에서 참고로 하여 적용은 가능하나, 법제도적인 강제성을 포함하고 있지 않다는데 한계점이 있다. 만약 특정 IoT 제품의 출시일이 임박할 경우, 보안에 대한 대책과 검증을 소홀히 한 상태에서 IoT 제품을 출시하게 되는 경우를 상상해볼 수도 있다.

한편, 현재 IoT 환경을 규제할 수 있는 단일 법률은 존재하지 않는 상태이다. 2015년 12월 사물인터넷에 대한 단일화 법제를 추진하기 위하여 입법 공청회가 개최된 바 있으며, 여기에서는 '사물인터넷 진흥에 관한 법률안'에 대하여 논의된 바 있다. 해당 법안에는 IoT 환경에 대한 정책적 추진, 기반조성, 활성화 방안과 같은 주요 내용을 담고 있다.

IoT 단일화 법률이 구체적으로 시행되지 않고 있는 현재 시점에서는, 정보보안을 명시적으로 규정하고 있는 '국가정보화 기본법', '개인정보보호법', '정보통신망 이용촉진 및 정보보호 등에 관한 법률', '정보통신기반 보호법', '위치정보의 이용 등에 관한 법률'과 같은 통상적인 법률에 의존해야 한다. 이러한 법률은 생활의 편익 증진으로 법의 목적이 유사한 편이며, 궁극적으로 정보보호라는 동일한 목적을 지향한

다고 볼 수 있다. 그러나 개별법규의 성격상 수범주체와 보호방법에 차이가 있다[13].

IoT 환경은 물리환경과 정보통신기술이 결합되는 것으로, 이에 적합한 법제도적 마련이 필요하며, 법률 단위에서의 규제와 동시에 품질인증, 기술기준과 같은 현행 제도에서도 제품 보안성 항목을 명시적으로 언급할 필요가 있다. 특히 각 제품별로 보안 고려사항이 다를 수 있으므로 보안성 검토에 대한 부분은 각 인증제별로 가급적 상세히 명시되어야 하는 것이 바람직하다.

그러나 대부분의 인증제도는 정보보안에 대한 인증항목을 가지고 있지 않은 것이 현실이다. 여기에서 보안성에 대한 부분은 해당 품질인증제에서 고려할 것이 아니라 별도의 인증제도를 만드는 것이 타당하다고 생각할 수도 있으나, 현실적으로 제도적인 효율성 측면에서 별도의 제품별 보안인증제도를 만들기보다는 현행의 인증제도나 기술기준에 보안성 항목을 부여하는 것이 효율적이다.

현재 미래부의 소관으로 정보통신망법과 국가정보화기본법에 근거한 '정보보호관리체계인증(ISMS)'과 '정보보호시스템 평가인증(CC인증)'제도가 존재하고 있으나, 이는 법정임의 인증제로서 강제성을 띠고 있지 않으며, 단일 인증제로는 제품별 특성에 맞는 보안항목에 대해서 상세히 규정하기에는 한계가 있다.

안전한 IoT 환경을 위해서는 제도적인 강제성을 부여하는 법정의무 인증제도와 기술기준에 IoT 보안항목이 들어가는 것이 가장 합리적이다. 따라서, 본 논문에서는 현재의 제품별 법정의무 품질인증제도와 기술기준에 보안항목을 적용하는 것을 제안한다.

3.3 사후 보안성 관리 측면에서의 한계

IoT 제품 출시 이후, 미처 생각치 못한 보안 허점이 발견될 수 있다. 제품 설계상의 허점이 아니더라도, 예를 들어 암호화 알고리즘 자체나 보안 표준상의 취약성이 발견되는 등 외부적인 요인에 의하여 IoT 제품의 보안성이 크게 위협받을 수도 있다.

이러한 경우, 상황의 심각도에 따라 소프트웨어 업데이트를 즉각적으로 실시할 수 있는 자동 업데이트 시스템이 필요하며, 이러한 업데이트 과정에서 해킹의 위협이 없도록 설계하여야 한다. 또한, 업데이트 파일 자체가 해킹을 통하여 변조되었을 경우도 고려하여 원본 파일이 무결성을 유지할 수 있어야 한다. 그러나 현재 출시된 IoT 제품 가운데 이러한 자동 소프트웨어/펌웨어 업데이트가 적용되지 않은 제품은 향후 발생 가능한 보안의 취약점에 능동적으로 대응하기 어려운 것이 현실이다.

한편, 소프트웨어 업데이트만으로 해결이 불가능한 경우도 있다. 이러한 부분은 하드웨어 자체를 교체해야 하며, 리콜과 같은 제도적인 절차에 따라 IoT 제품 자체나 그 일부를 교체하여야 한다.

그러나 현재의 리콜제도는 정보보호의 측면보다는 사용자의 안전에 중점을 두고 있는 것이 현실이다.

통상적으로 말하는 리콜제도란 제조사가 제품을 판매한 이후, 사용자의 신체적 위협 또는 재산적인 피해가 발생할 우려가 있는 제품 결함이 발견될 경우에 사업자나 기관의 주도로 해당 제품을 수거하여 교환 또는 환불 조치를 하는 것을 말한다.

리콜은 기본적으로 제품안전기본법에 근거하고 있다. 해당 법률의 시행령 제5조의4에서는 중대한 결함을 '사망, 신체적 부상이나 질병, 화재 또는 폭발을 일으키거나 일으킬 우려가 있는 결함'으로 구체적으로 명시하고 있다.

현재로서는 IoT 보안 결함에 대해서는 제품안전기본법에 근거하여 리콜을 적용받기가 모호한 실정이다. 만약 매우 명백한 보안 결함으로 사망, 화재 등 신체적/물질적 피해 사례가 다수 보고될 경우는 해당 항목에 근거하여 조치할 수 있겠으나, 피해가 우려되고 있는 상황 또는 실질적인 피해 사례가 많지 않은 상황, 제조사에서 결함 사실을 인정하지 않는 경우 등에 대해서는 해당 법의 적용이 사실상 어려운 것이 현실이다. 특히, IoT 환경에서는 제품과 제품간 통신을 하며, 해당 제품에 대한 보안 결함이 해당 제품과 통신하는 다른 제품에 간접적으로 영향을 발생시킬 경우도 문제가 될 수 있다.

현실적으로 IoT 제품에 대한 리콜 등 사후관리에 대한 법제도적 안전장치는 마련되어 있지 않은 실정이며, 소프트웨어 자동 업데이트의 제도적 의무화, 제품안전기본법 등 관련법의 개선을 통하여 IoT 제품에 대한 사후관리 환경을 조성하는 것이 시급하다.

IV. IoT 제품 보안을 위한 법제도 개선방안

IoT 제품 관련 법제도에 대한 한계점을 앞서 3장에서 분석하였다. 본 장에서는 이러한 법제도적 한계점을 바탕으로 IoT 제품의 품질인증제도와 사후 보안관리 관련 법제도에 대한 개선(안)을 제시한다.

4.1 제도 개선을 통한 IoT 제품 보안성 의무화

4.1.1 제도 개선 접근 방법

현재 다양한 IoT 유관 품질인증제도 및 법적 기술기준이 존재하고 있다. 기술기준은 정부가 환경,안전,보건 등 국민의 권리를 위해 법적 구속력을 가지고, 법률에 의하여 강제력을 가지는 기술규범이다.

앞서 언급하였듯, 현행 시행되는 대부분의 인증제 및 기술기준은 제품 자체의 기기적 안전 또는 사용자의 신체적/재산적 안전, 또는 환경에 대한 부분을 규정하고 있는 것이 일반적이다.

본 논문에서는 주요 제도 개선 접근방법으로, 한국인터넷진흥원(KISA)이 제시하고 있는 IoT 7대 공통 보안 원칙에 근거하여 각 IoT 제품별 적합한 보안 조항을 그에 대응하는 제도의 항목에 추가하는 방법으로 접근하였다. IoT 7대 보안 원칙은 제품의 설계, 개발, 운영 등 IoT 제품의 전 주기에서 단계별로 고려해야 할 사항을 명시하고 있어 개선 목적에 적합하다.

본 논문에서는 제도적 개선 대상 기술기준으로써 국토교통부고시 제2016-64호, 미래창조과학부고시 제2016-30호, 산업통상자원부고시 제2016-14호로 제정되어 있으며 IoT 제품과 밀접하게 연관되는 기술기준인 '지능형 홈네트워크 설비 설치 기준'을 선정하였다. 다음 절에서는 해당 기술기준에 대한 개선(안)을 제시하고자 한다.

4.1.2 지능형 홈네트워크 설비 설치 기준 개선(안)

'지능형 홈네트워크 설비 설치 기준'은 지능형 홈네트워크 설비의 설치 및 기술적 사항에 관하여 위임된 사항과 그 시행에 관하여 필요한 사항을 규정하고 있으며, 주택법 제35조 및 주택건설기준 등에 관한 규정 제32조의2에 근거하여 법적 구속력을 가진다.

따라서, 해당 기술기준에 보안항목을 추가하여 보완하는 것으로, 홈네트워크 IoT 환경에서의 보안 설계가 의무화될 것으로 기대된다.

당 기준의 제5조(홈게이트웨이)부분은 홈게이트웨이의 설치 위치, 전원 공급 여부, 작동상태 확인 여부에 대한 조항을 명시하고 있으며, 해당 조항에 아래와 같이 4항으로 신규항을 추가할 것을 제안한다.

◉ 제5조 현행과 동일
◉ ((1~3) 각 항 현행과 동일)
◉ ④ 홈게이트웨이는 데이터통신 및 개방형 플랫폼에서 안전성을 보장하는 보안 프로토콜을 준수하여야 하며, 안전한 파라미터가 설정되어야 한다.

홈게이트웨이는 보안 기능 미비시 IoT 보안 취약성에 노출될 가능성이 있으므로, 상호인증 및 안전한 보안 통신의 제공이 필요하다. 현재 다양한 국내외 표준 기구에서 보안 기술이 논의되고 있으며, MQTT, CoAP, LwM2M, Zigbee와 같은 IoT 제품 및 서비스에 활용 가능한 경량 통신 프로토콜이 존재한다. IoT 기기에는 통신 및 플랫폼에서 안전성을 보장하는 통신 프로토콜이 적용되어야 한다. 특히, 프로토콜 상에서 보안 모드를 설정하도록 되어 있는 경우, 안전한 파라미터의 설정이 필요하다. CoAP는 기기간 통신을 위하여 다양한 인증 방식을 제공한다. Table 2.는 CoAP의 4가지 보안 모드를 나타내고 있다. No Security 모드를 제외하면 DTLS가 지원하는 대칭키 암호 AES, 공개키 암호 ECC 등이 지원되며, 이를 사용하면 더 높은 보안수준을 활용할 수 있다는 특징이 있다.

Table 2. Security Mode of CoAP

Security Mode	Description
No Security	No security support is provided
Pre-Shared Keys	Symmetric keys are provided
Raw Public Key Certificates	Asymmetric cryptography algorithms are provided
X.509 Certificates	Asymmetric cryptography algorithms are provided in X.509 format

한편, 제7조(원격제어기기)부분은 취사용 가스벨브의 원격제어 유무, 조명제어기 설치 여부, 디지털 도어락과 월패드의 연동 여부를 명시하고 있다. 해당 조항에 아래와 같이 4항으로 신규항을 추가할 것을 제안한다.

◉ 제7조 현행과 동일
◉ ((1~3) 각 항 현행과 동일)
◉ ④ 원격제어기기는 암호화 통신을 지원하여야 하

며, 안전한 초기 보안 설정으로 출고된 제품을 사용하여야 한다.

원격제어기기는 해킹에 노출될 우려가 있다. 특히, 원격제어기기에서 초기 보안설정의 미비로 인한 보안 취약성 사례도 발견된 상태이다. 따라서 위와 같은 조항을 추가하였다.

제13조(단지서버)에는 클라우드 컴퓨팅 서비스를 이용하는 부분에 관한 내용이 명시되어 있으며, 5항에서는 암호화 등을 통하여 클라우드 컴퓨팅 서비스 이용 과정에서 보안문제가 발생하지 않아야 할 것을 명시하고 있다. 해당 조항에 아래와 같이 6항으로 신규항을 추가할 것을 제안한다.

◉ 제13조 현행과 동일
◉ ((1~5) 각 항 현행과 동일)
◉ ⑥ 5항에서 보안문제가 발생하였을 경우, 적절한 IoT 침해사고 대응체계를 갖추어야 하며, 책임 추적성이 확보되어야 한다.

IoT 시스템에서 클라우드 컴퓨팅 서비스를 이용하는 것은 여러 다양한 보안 문제를 야기할 수 있으며, 제13조5항에 이미 암호화 등을 통한 사전 보안 고려사항을 명시하고 있다. 그러나, 클라우드 컴퓨팅의 특성상 보안 침해시 사고 발생에 따른 대응체계 및 책임 추적성이 별도로 요구되며, 해당 기술기준에는 이에 대한 항목이 별도로 존재하지 않으므로 해당 조항의 6항으로 추가하여 보안성을 확보하였다.

제16조(주동출입시스템)에서는 주동출입시스템의 설치 위치, 화재발생 등 비상시 작동, 설치방법, 접지단자 설치여부를 명시하고 있으며, 5항에서는 월패드간의 통신이 가능할 것을 명시하고 있다. 본 논문에서는 해당 조항에 아래와 같이 6항을 추가할 것을 제안한다.

◉ 제16조 현행과 동일
◉ ((1~5) 각 항 현행과 동일)
◉ ⑥ 5항에서 주동출입시스템과 월패드 간 통신 시 암호화 등 검증된 보안 프로토콜을 지원해야 한다.

주동출입시스템은 월패드와 통신이 이루어지며, 통신이 원활치 않을 시 화재발생 등 비상시에 신체적 재산적 피해를 발생시킬 수 있다. 만약 해커가 주동출입제어시스템과 월패드간 통신 네트워크에 침입하여 변조, 위조, 차단등의 공격을 감행하는 경우 사용자의 직접적인 피해가 우려되므로 월패드간 통신시에는 반드시 검증된 보안 프로토콜을 사용할 수 있도록 하는 것이 바람직하다.

제17조(원격검침시스템)에서는 각 세대별 원격검침장치가 운용시스템의 동작 불능시, 정전시에도 작동할 수 있어야 함을 규정하고 있다. 본 논문에서는 해당 조항에 아래와 같이 3항을 추가할 것을 제안한다.

◉ 제17조 현행과 동일
◉ ((1~2) 각 항 현행과 동일)
◉ ③ 원격검침장치는 데이터 암호화, 무결성 확보 등을 통하여 보안 문제가 발생하지 않아야 한다.

스마트미터 등 원격 검침장치에는 사용자 프라이버시 노출 위협 등 보안이슈가 존재한다. 따라서, 가능한한 데이터를 암호화 후 저장하여 검침 데이터 및 사용자의 프라이버시를 보호할 필요가 있다. 또한, 검침 데이터의 손실/변경이 발생하지 않아야 하며, 이러한 부분을 해결하기 위한 무결성 확보 대책이 필요하다.

4.2 IoT 제품 사후관리를 위한 법적 근거 마련

4.2.1 법적 개선 접근 방법

IoT 제품은 설계 및 개발 단계에서 보안을 충분히 고려하여 제작되고 출시되어야 하나, 제품 자체의 결함 혹은 외부의 영향으로 의도치 않게 보안 취약점이 발생할 수 있다. 그러한 보안 취약점 발견 시 그에 대응하는 즉각적이고 적절한 조치가 필요하나, 실질적으로 법제도 측면에서 3.3.에서 기술한 것과 같은 한계점이 존재한다. 따라서 본 논문에서는 제품안전기본법 시행령을 일부 보완하여, 중대한 보안 결함을 사유로 리콜이 가능하도록 법제화하는 것을 제안한다.

4.2.2 제품안전기본법 시행령 개선(안)

현재 제품안전기본법 제5조의4 제3항에서는 '중대한 결함'을 다음과 같이 규정하고 있다.

구체적으로 해당 조문의 1호에서는 '제품의 제조,

유통, 또는 사용과 관련하여 통상적으로 기대할 수 있는 안전성이 결여되어 소비자에게 다음 각 목의 위해를 끼치거나 끼칠 우려가 있는 결함'으로 명시하고 있으며, 각 목은 '가. 사망', '나. 의료법 제3조 제3항에 따른 의료기관에서 4주 이상의 치료가 필요한 골절·질식·화상·감전 등 신체적 부상이나 질병'으로 명시하고 있다.

또한, 해당 조문의 2호에서는 '화재 또는 폭발을 일으키거나 일으킬 우려가 있는 결함'으로 규정한다. 해당 조항은 3.3.에서 기술한 것과 같이 IoT 환경에서는 적용 범위상의 모호함이 존재하는 것이 사실이며, 이러한 부분을 보완하기 위해 제5조의4 3항의 3호로 보안 관련 조항을 추가하는 것을 제안한다.

◉ 제5조의4 현행과 동일
◉ ((1~2) 각 항 현행과 동일)
◉ ③ 법 제9조의3제4항제2호에 따른 중대한 결함은 다음 각 호의 결함으로 한다.
◉ 1. 현행과 동일
◉ 2. 현행과 동일
◉ 3. 제품의 중대한 보안 취약점으로 소비자에게 직·간접적으로 신체적, 재산적 위해를 끼치거나 끼칠 우려가 있는 결함

이와 같이 제5조의4를 수정하는 것으로, IoT에서의 중대한 보안 취약점을 리콜명령 사유의 근거로 지정할 수 있다. 특히, 신체적/재산적 문제로 귀결될 경우는 제품안전기본법의 취지에 적합하다.

V. 결 론

최근 IoT 시대가 도래하면서 IoT 보안 또한 중요한 이슈가 되고 있다. IoT의 도입과 활성화는 생각보다 빠르게 진행되고 있으므로 보안에 대한 안전한 대책 확보가 매우 시급한 상황이다. 특히, 기술적인 대응책을 마련하는 것도 중요하나, 법제도적 개선을 통한 정책적인 보안 대책 마련 또한 매우 중요하다.

따라서 본 논문에서는 IoT 보안에 대한 법제도적 개선방안에 대하여 논의하였다. 먼저 2장에서 IoT 제품에 대한 정보보호 위협과 관련 제도에 대한 현황을 살펴보았다. 그리고 3장에서는 현행 IoT 제품 보안에 대한 법제도적인 한계점을 분석하였으며, 4장에서는 IoT 제품 보안을 위한 법제도적 개선방안을 제시하였다. 해당 지침의 개선안은 크게 두가지의 관점에서 제시되었다. 먼저 제도 개선을 통한 IoT 제품 출시전 보안성 검증 의무화 방안을 제안하였으며, 실례로 지능형 홈네트워크 설비기준 개선에 보안 조항을 추가하는 것을 제안하였다. 또한, IoT 제품에 대한 사후관리를 위한 법적 근거를 마련하는 방안을 제안하였으며, 이는 현행 리콜제의 근간이 되는 제품안전기본법 시행령에 조항을 추가하는 것으로 IoT 제품의 보안 취약점이 리콜명령 사유가 될 수 있도록 개선하여 제안하였다.

본 연구에서는 현행 법제도의 문제점을 지적하고자 하는 것이 아니라, IoT 제품 출시 이전 설계/개발 단계에서의 고려사항과 제품 출시 이후 사후관리 관점에서 추가적인 법제도적 보완사항이 있는지를 고려하고 개선사항을 제시하고자 하는 것이 목적이다.

IoT 환경 도입은 빠른 시일 내에 가속화될 것이며, 머지않아 우리 생활 속에 더 깊게 파고들게 될 것이다. 안전한 IoT 환경을 위하여 향후에도 기술적·법제도적 측면에서 다양한 방면으로 검토가 필요할 것으로 보인다.

References

[1] Teng Xu, James B. Wendt, and Miodrag Potkonjak, "Security of IoT systems: design challenges and opportunities," In Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD '14), pp.417-423. Nov. 2014.

[2] Jun Jong Am, Kim Nae Soo, Park Jeong Kil, Park Tae Jun, Kang Ho Yong, "IoT device products and technology trends," The Journal of The Korean Institute of Communication Sciences 31(4), pp.44-52, Mar. 2014.

[3] Waleed Rafique, Munam Ali Shah, "Performance evaluation of IoT network infrastructure," 2016 22nd International Conference on Automation and Computing (ICAC), pp. 348-353, Sep. 2016.

[4] Kang Nam Hee, "Standard Technology Trends for Internet Security of Things," The Journal of The Korean Institute of

Communication Sciences 31(9), pp.40-45, Aug. 2014.
〔5〕 Namje Park, "Analysis of Privacy Weakness and Protective Countermeasures in Smart Grid Environment," Journal of Korean Institute of Information Technology 8(9), pp. 189-197, Sep. 2010.
〔6〕 Donghyeok Lee, Namje Park, "Legislative Reform of Smart Grid Privacy Act," Journal of the Korea Institute of Information Security & Cryptology 26(2), pp.415-423, Apr. 2016.
〔7〕 Hun-Yeong Kwon, "Information and Communication Security legal system's problems and improvement plan," Journal of The Korea Institute of Information Security & Cryptology 25(5), pp.1269-1279, Oct. 2015.
〔8〕 Seunghyeon Choi, Kangseok Kim, Heekyung Seol, Daewook Yang, Donghoon Lee, "A Study on Problem and Improvement of Legal and Policy Framework for Smartphone Electronic Finance Transaction - Focused on Electronic Financial Transaction Act," Journal of The Korea Institute of Information Security & Cryptology 20(6), pp.67-81, Dec. 2010.
〔9〕 Vermesan, Ovidiu, P. Friess, and A. Furness. "The Internet of Things 2012: New Horizons," IERC 3rd edition of cluster book, Halifax, UK, pp. 35-40, 2012.
〔10〕 Donghyeok Lee, Namje Park, "IoT product security certification and security maintenance plan," The Journal of The Korean Institute of Communication Sciences 33(12), pp.28-34, Nov. 2016.
〔11〕 Donghee Kim, Seokung Yoon, Yong-pil Lee, "Security for IoT Services," The Journal of The Korean Institute of Communication Sciences 30(8), pp.53-59, Jul. 2013.
〔12〕 Namhi Kang, "Standard Technology Trends for Internet Security of Things," The Journal of The Korean Institute of Communication Sciences 31(9), pp.40-45, Aug. 2014.
〔13〕 Son, Seung Woo, Park, Jang Hyouk, Moon, Sue Mi, "A Study on Improvement Measures of Information Security Relevant Laws for IoT Service Providers," LAW REVIEW 57(1), pp.181-215, Feb. 2016.

〈저자소개〉

이 동 혁 (Donghyeok Lee) 정회원
2007년 2월: 동국대학교 전자상거래기술전공 공학석사
2007년 6월~2008년 5월: 한국전자통신연구원 정보보호연구단 연구원
2008년 11월~2015년 6월: KT 플랫폼개발단 과장
2015년 9월~현재: 제주대학교 컴퓨터교육전공 박사과정, 초등교육연구소 특별연구원
〈관심분야〉 클라우드 보안, 스마트그리드 보안, 데이터베이스 보안, 해사클라우드 등

박 남 제 (Namje Park) 종신회원
2008년 2월: 성균관대학교 컴퓨터공학과 박사
2003년 4월~2008년 12월: 한국전자통신연구원 정보보호연구단 선임연구원
2009년 1월~2009년 12월: 미국 UCLA대학교 공과대학 Post-Doc,WINMEC 연구센터 Staff Researcher
2010년 1월~2010년 8월: 미국 아리조나(ASU) 주립대학교 컴퓨터공학과 연구원
2010년 9월~현재: 제주대학교 초등컴퓨터교육전공 교수, 과학기술사회(STS)연구센터장
〈관심분야〉 융합기술보안, 컴퓨터교육, 스마트그리드, IoT, 해사클라우드 등