IoT서비스 확대에 따른 정보보호 관리체계 필요에 대한 연구

마 기 평* 이 상 준** 공 병 철***

목 차

1. 서 론

IDC조사에 따르면, 세계 IoT시장은 2017년 현재 8천억 달러 규모에서 2021년에는 1조4천억 달러 규모로 성장할 것으로 전망되며, 보안 하드웨어 및 소프트웨어 시장도 각각 연평균 15.1% 및 16.6%성장할 것으로 예상된다. 국내IoT 시장은 2017년 4월말 기준으로 7,367억 원 규모2에서, 2020년에는 17조 1천억 원 규모로 무려 연평균 38.5% 성장할 것으로 전망3하고 있다. 그리고 세계 스마트홈 시장은 2020년까지 약 430억 달러 규모로, 국내 시장은 약 13억 2천만 달러 (약 1조 5천억 원) 규모로 성장할 것으로 예측하였다. 국내외 IoT 산업의 급격한 성장과 비례하여 IoT 기반의 다양한 제품 및 서비스에 대한 보안위협 역시 급격히 증가할 것으로 예상되며, 이에 따라 글로벌 IT 리서치 기관인 가트너 에서는 전 세계 IoT 보안 지출 규모가 2018년에는 5억 4,700만 달러에 달할 것으로 예측하였다.

이와 같은 IoT 산업의 성장을 지원하기 위해 미국, 유럽, 일본, 중국 등 각 나라에서는 IoT 산업 육성 및 활성화 정책과 더불어 사이버 공격으로부터 안전한 서비스 제공을 위한 IoT 정보보호 정책을 추진하고 있다.

우리나라, 미국, 일본, 중국, 유럽 등 ICT 강국을 중심으로 국가 차원에서 IoT를 지원하고 있는가 하면, 글로벌 기업을 중심으로 IoT 시장을 선점하기 위한 기술개발 및 생태계 조성이 활발히 이루어지고 있으나, IoT시대의 본질적인 도래를 위해서는 관련 기술 개발은 물론 보안 및 프라이버시 보호와 글로벌 표준 확립 등 당면한 문제점 극복이 전제 되어야 할 필요가 있다.

본고에서는 IoT서비스에 대한 주요 보안 이슈와 동향, 대응방안과 IoT 홈·가전 기술적 보안요구사항을 살펴보고 안전한 ICT구현을 위한 정보보호관리체계의 발전 방향을 살펴보고자 한다.

2. IoT와 관련한 주요 이슈 분석

IoT 도입의 가장 큰 이슈는 취약한 보안으로 인한 프라이버시 침해와 생명과 안전에 대한 위협이며, 최근 IoT 도입과 관련하여 보안을 위협하는 사례가 빈번하게 노출되고 있는바, 이를 해소하기 위해 IoT 환경을 고려하여 현재의 사이버 환경과 달리 그 보호대상 범위, 대상 특성, 보안 담당 주체, 보호방법 등에 있어 새로운 시각으로 보안 이슈에 접근해야 할 필요성이 제기되고 있다.

IoT 시대에는 수많은 다양한 기기들의 연결과 규모경제의 실현을 위해 통신규격 등 표준 확립이 매우 중요한데, 현재 많은 단체표준의 난립으로 합의된 범용 표준이 없는 상황이며, 앞으로도 글로벌 표준 정립이 쉽지 않을 것이란 전망이 나오고 있는 상황에서, GDPR 대응 등 글로벌 기업을 중심으로 한 표준 활동에 업계의 이목이 집중될 것으로 예상된다.

* ㈜윈스
** 전남대학교 경영대학 교수
*** (사)한국사이버감시단

IoT 산업은 하드웨어와 소프트웨어 및 서비스가 혼합된 복잡한 밸류 체인으로 형성되어 있으며, 이런 상황에서 IoT를 주도하기 위해 글로벌 기업들은 M&A 등을 통해 자사 중심의 생태계 조성을 적극 추진하며 시장 선점 활동을 강화하고 있으며, 국내에서도 삼성전자, LG전자, 이동통신사를 중심으로 움직임이 구체화되고 있어 향후 전개 방향에 주목되고 있다.

부문	2013년	2014년	2015년	2020년
자동차	96.0	189.6	372.3	3,511.1
소비자	1,842.1	2,244.5	2,874.9	13,172.5
포괄적(Generic) 비즈니스	395.2	479.4	623.9	5,158.6
수직적(Vertical) 비즈니스	698.7	836.5	1,009.4	3,164.4
총 기기 수	3,032.0	3,750.0	4,880.6	25,006.6

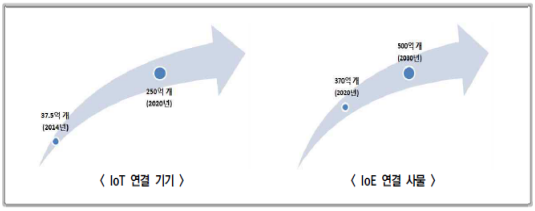
(그림 1) IoT부문별 기기 전망

3. IoT시대 주도를 위한 우리의 대응

최근 침체 경향을 보이고 있는 ICT 산업의 미래 성장 동력으로 부각되고 있는 IoT의 기술개발과 함께 생태계 조성을 통한 시장 선점 활동을 더욱 강화할 필요가 있다.

안전 위협과 프라이버시 침해 문제 해결이 미흡한 상태에서의 IoT 도입은 관련 시장의 성장을 지연시키는 큰 장벽으로 대두될 가능성이 크므로 IoT 도입 초기부터 보안을 위한 기술적 문제 해결책은 물론 법·제도적인 측면에서도 선제적인 육성 및 대비책을 마련하는 등 종합적인 해결 방안이 시급하다.

IoT 산업을 주도하기 위해 표준과 관련한 국내 대표적인 기업들 간의 밀접한 협업 관계 구축과 함께 중소기업을 포함한 산업계, 연구계, 학계 등이 상생의 생태계를 적극 조성하여 글로벌 표준 확보에 적극 나서야 글로벌 경쟁력을 갖추게 될 것이다.



(그림 2) IoT연결기기 예측

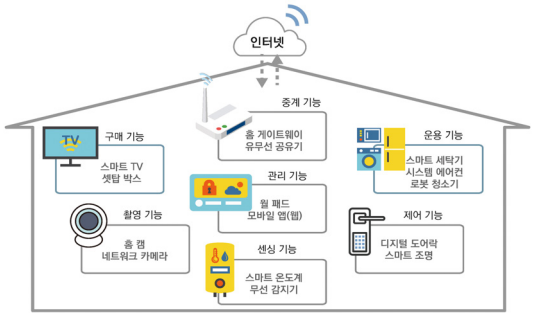
4. IoT 서비스의 정보보안 동향

지난 2014년 5월에는 정부관계부처 합동으로 '초연결 디지털혁명의 선도국가 실현을 위한 IoT 기본계획'을 발표하였으며, IoT 위협의 범국가적 대응을 위해 2014년 10월, '사물인터넷 정보보호 로드맵'을 수립하고, ICT와 산업 간 융합으로 인해 발생 가능한 안전위협에 대응하기 위해 'K-ICT 융합보안 발전전략'(2016.04)과 IoT 정보보호 로드맵에 따라, IoT 제품의 보안내재화를 위해 IoT 하드웨어와 소프트웨어 전반에 걸쳐 준수해야 할 7개의 보안원칙을 제시한 'IoT 공통 보안원칙' (2015.06)이 발표되었다.

이에 따라 ICT 융합 제품 및 서비스 설계 시 IoT 홈·가전 보안요구 동향을 살펴보고자 한다.

4.1. IoT 홈·가전의 유형

홈·가전 IoT 제품은 집안에 설치된 홈·가전제품이 무선 네트워크 통신을 기반으로 제공하는 기능 및 서비스에 따라 센싱, 제어, 중계, 구매, 촬영, 관리, 운용 등으로 분류되며 <그림3>과 같이 홈·가전 IoT 제품 유형으로 볼 수 있다.

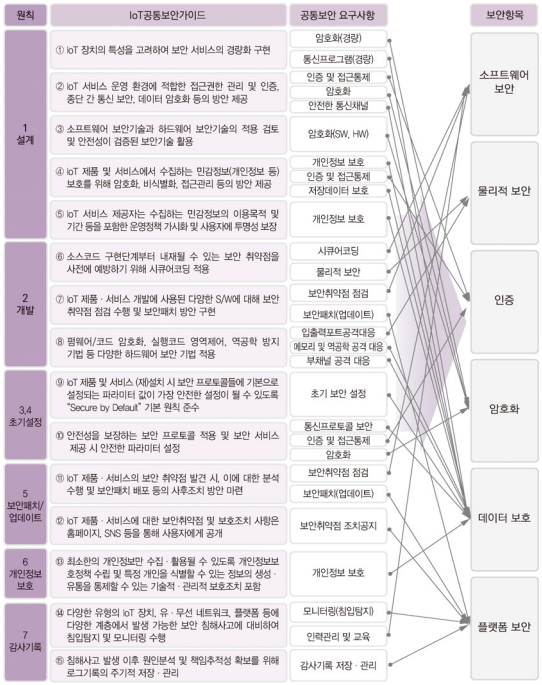


(그림 3) 홈·가전 IoT 제품 유형 예시

4.2. IoT 홈·가전의 보안요구사항

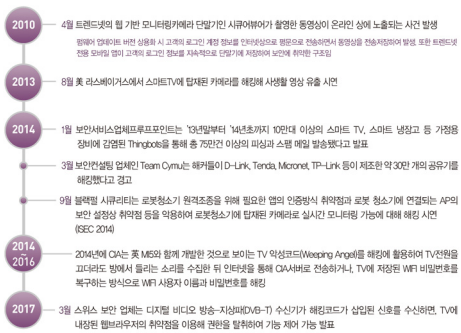
IoT 공통보안 가이드에서는 소프트웨어 보안, 물리적 보안, 인증, 암호화, 데이터 보호, 플랫폼 보안 등 6가지 보안항목으로 분류하고 IoT 제품 개발자 및 제조사들이 개발단계부터 보안을 고려하여 안전하게 개발할 수 있

도록 요구사항을 구체화하여, 실제 구현에 활용할 수 있도록 <그림 4>과 같이 공통보안 요구사항을 명시하고 있다.



(그림 4) 홈·가전 IoT보안가이드의 연관관계

최근 스마트 홈에 사용되는 홈·가전 IoT 제품은 컴퓨팅 능력, 네트워크 연결 등을 필요로 하며, 이로 인해 기존 가전제품과 달리 다양한 보안 위협과 보안사고들이 <그림 5>과 같이 발생하고 있다.



(그림 5) 홈·가전 IoT 제품 관련 보안사고 사례

IoT 시대에는 인터넷에 연결되는 제품이 기하급수적으로 늘어나므로 PC 외에도 가정용 무선공유기를 비롯해 냉장고, 청소로봇, 냉난방 공조장비 등 인터넷에 연결된 모든 제품(IoT)에 대한 분산서비스거부(DDoS) 공격은 가정에서 주로 많이 쓰는 무선 공유기가 대상이 되고 있다.

보통 이러한 무선 공유기는 기본적인 보안 솔루션인 안티바이러스도 설치되지 않을 뿐 아니라 관리 주체도 불분명하거나 대대수의 사용자는 무선 공유기 초기 설정을 변경하지 않은 상태로 사용함으로써 무선 공유기 해킹 사고가 최근 빈발하고 있고 있어 대부분의 가정이 사이버 위협에 노출된 상태로 보인다.

유형	주요 제품	주요 보안위협	주요 보안위협 원인
멀티미디어 제품	스마트TV, 스마트 냉장고 등	· PC 환경에서의 모든 악용 행위 · 카메라/마이크 내장 시 사생활 침해	· 인증 메커니즘 부재 · 강도가 약한 비밀번호 · 펌웨어 업데이트 취약점 · 물리적 보안 취약점
생활가전 제품	청소기, 인공지능 로봇 등	· 알려진 운영체제 취약점 및 인터넷 기반 해킹 위협 · 로봇청소기에 내장된 카메라를 통해 사용자 집 모니터링	· 인증 메커니즘 부재 · 펌웨어 업데이트 취약점 · 물리적 보안 취약점
네트워크 제품	홈캠, 네트워크 카메라 등	· 사진 및 동영상을 공격자의 서버 및 이메일로 전송 · 네트워크에 연결된 홈캠 등을 원격으로 제어하여 임의 촬영 등 사생활 침해	· 접근통제 부재 · 전송데이터 보호 부재 · 물리적 보안 취약점
제어제품	디지털 도어락, 가스밸브 등	· 제어기능 탈취로 도어락의 임의 개폐	· 인증 메커니즘 부재 · 강도가 약한 비밀번호 · 접근통제 부재 · 물리적 보안 취약점
	모바일 앱(웹) 등	· 앱 소스코드 노출로 IoT 제품 제어기능 탈취	· 인증정보 평문 저장 · 전송데이터 보호 부재
센서 제품	온/습도 센서 등	· 잘못된 또는 변조된 온 · 습도 정보 전송	· 전송데이터 보호 부재 · 데이터 무결성 부재 · 물리적 보안 취약점

(그림 6) 제품 유형별 주요 보안위협

홈·가전 IoT 제품의 하드웨어 및 소프트웨어 개발 단계에 공통적으로 적용되어야 하는 공통 보안항목은 개발단계에서 공통적으로 요구되는 항목이며, 유형별 보안항목은 제품이 가진 기능적 유형 및 다루는 정보의 중요도에 따라 선별적으로 요구되는 보안항목이 있으며, 이러한 홈·가전 IoT 제품들은 공통적으로 <그림7>과 같은 보안속성을 고려하여 개발하여야 한다.

보안항목	보안요구사항	관련 주요 보안위협
소프트웨어 보안	• 시큐어코딩 • 알려진 보안취약점 점검 및 제거 • 최신 3rd party 소프트웨어 사용	• 소프트웨어 결함 등 보안약점으로 인한 보안취약점 원인 제공 • 알려진 보안취약점 악용 • 3rd party 소프트웨어의 보안취약점 악용
물리적 보안	• 물리적 인터페이스 차단	• 물리적 보안 취약
인증	• 인증 및 접근통제 • IoT 제품간 상호 인증	• 인증 메커니즘 부재 • 강도가 약한 비밀번호 • 접근통제 부재
암호화	• 안전한 암호 알고리즘 사용 • 안전한 암호키 관리 • 안전한 난수 생성 알고리즘 사용	• 취약한 암호알고리즘 • 취약한 암호키 길이 • 낮은 엔트로피
데이터 보호	• 안전한 통신채널 • 저장 및 전송 데이터 보호 • 개인정보 보호	• 전송데이터 보호 부재 • 인증정보, 암호키, 개인정보 등 중요정보 평문 저장
플랫폼 보안	• 설정값 및 실행코드 무결성 검증 • 안전한 업데이트 • 감사기록	• 데이터 무결성 부재 • 펌웨어 업데이트 취약점 • 보안사고 추적 불가능

(그림 7) 보안항목별 보안위협

4.3. IoT 홈·가전의 보안위협과 대응방안

홈·가전 IoT 제품의 각 보안항목별로 해당되는 보안 요구사항 및 보안위협은 <그림 8>와 같다.

보안항목		해당 제품
소프트웨어 보안	시큐어코딩	프로그램이 가능한 제품
	알려진 보안취약점 점검 및 제거	프로토콜, API, 패키지, 오픈소스 등과 펌웨어 또는 운영체제를 사용하는 제품
	최신 3rd party 소프트웨어 사용	펌웨어 또는 운영체제 및 애플리케이션 소프트웨어에 3rd party 소프트웨어를 사용하는 제품
물리적 보안	물리적 인터페이스 차단	외부에 인터페이스(USB, RS232, 메모리카드 포트 등 외부접근포트)가 존재하거나, 개발 및 고장 수리 등을 위해 외부기규(예, 외부 덮개 등)를 해체 후 내부 PCB에 메모리 및 MCU에 접근 가능한 포트가 존재하는 제품
인증	인증 및 접근통제	유 · 무선접속, 제품 설치시 인증이 필요한 제품
	IoT 제품간 상호인증	IoT 제품 간 연결 시 인증이 필요한 제품
암호화	안전한 암호 알고리즘 사용	민감 정보를 저장하거나 IoT 제품 간 통신 시 암호화 통신이 요구되는 제품
	안전한 암호키 관리	민감 정보를 저장하거나 IoT 제품 간 통신 시 암호화 통신이 요구되는 제품
	안전한 난수 생성 알고리즘 사용	암호키 생성, 분배, 상호 인증 등 안전한 난수 사용이 요구되는 제품
데이터 보호	안전한 통신채널	IoT 제품 간 암호화 통신이 요구되는 제품
	저장 및 전송 데이터 보호	IoT 제품 간 암호화 통신이 요구되며, 고유식별정보, 금융정보, 신체식별정보, 식별코드, 사진 등 개인정보를 처리 · 저장 · 전송하는 제품
	개인정보보호	고유식별정보,금융정보,신체식별정보,식별코드,사진 등 개인정보를 처리 · 저장 · 전송하는 제품
플랫폼 보안	설정값 및 실행코드 무결성 검증	설정값 및 거래 등 무결성 검증이 필요한 제품 (스마트TV/셋톱박스 등 결제 관련 암호키 관리가 필요한 제품 등)
	안전한 업데이트	유무선 통신 및 내 · 외부포트를 이용하여 업데이트가 가능한 제품
	감사기록	보안기능이 구현된 제품

(그림 8) 보안항목별 해당 제품

홈·가전 IoT 제품 유형별로 적용해야 하는 보안항목은 <그림9>와 같으며, 세부 요구사항은 인증 및 접근통제, IoT 제품 간 상호인증, 안전한 암호 알고리즘 사용, 안전한 암호키 관리, 안전한 난수 생성 알고리즘 사용, 데이터 보호를 위한 안전한 통신채널 제공, 저장 및 전송구간 보호, 설정값 및 실행코드 무결성 검증을 통한 플랫폼 보안, 안전한 업데이트, 감사기록 생성과 보호할 수 있는 방안을 고려되어야 한다.

보안항목	보안요구사항	
인증	• 인증 및 접근통제	– 제품의 초기 인증정보 변경 – 사용자 인증 – 인증정보 보호 – 안전한 비밀번호 사용 – 접근통제
	• IoT 제품간 상호 인증	– 상호인증
암호화	• 안전한 암호 알고리즘 사용	
	• 안전한 암호키 관리	– 안전한 암호키 생성 – 안전한 암호키 전송 – 안전한 암호키 저장 – 안전한 암호키 파기
	• 안전한 난수 생성 알고리즘 사용	
데이터 보호	• 안전한 통신채널	– 안전한 통신채널 제공 – 안전한 세션관리
	• 저장 및 전송 데이터 보호	– 전송데이터 보호 – 저장데이터 보호 – 메모리 공격 및 역공학 공격 대응 – 부채널 공격 대응
	• 개인정보 보호	
플랫폼 보안	• 설정값 및 실행코드 무결성 검증	– IoT 제품 주요 설정값 및 실행코드 무결성 검증
	• 안전한 업데이트	– 신뢰할 수 있는 업데이트 서버 – 업데이트 파일의 부인방지 및 무결성 보장 – 안전한 업데이트 기능 제공 – 펌웨어 분석 방지 기능 제공
	• 감사기록	– 감사기록 생성 – 감사기록 보호

(그림 9) 유형별 보안항목 및 대응방안 예시

홈·가전 IoT 제품 중에서 스마트TV, 디지털 도어락, 스마트 세탁기, 스마트 콘센트, 창문 개폐 센서 등 5개 제품군의 개발시 고려해야하는 세부 보안항목을 <그림 10>과 같이 예시하고 있다.

세부 적용 보안항목은 “필수”와 “조건부” 그리고 “예외”로 구분되며, “조건부”의 경우 해석이 필요하고, 해

구 분		스마트TV	디지털 도어락	스마트 세탁기	스마트 콘센트	창문 개폐 센서	비 고
소프트웨어 보안	시큐어코딩	●	●	●	●	●	–
	알려진 보안취약점 점검 및 제거	●	●	●	●	●	–
	최신 3rd party 소프트웨어 사용	●	●	●	●	●	최신 3rdparty 소프트웨어적용 시 필수 고려 항목
물리적 보안	물리적 인터페이스 차단	●	●	●	●	●	–
인증	인증 및 접근통제	●	●	●	–	–	–
	상호인증	●	●	●	●	●	–
암호화	암호연산	●	●	●	●	●	–
	암호 키 관리	●	●	●	●	●	–
데이터 보호	안전한 통신채널	●	●	●	●	●	–
	저장 및 전송데이터 보호	●	●	▲	▲	▲	• 암호키 : 필수 • 데이터 중요도에 따라 선별적 적용 가능
	개인정보 보호	●	●	–	–	–	–
제품 플랫폼	설정 값 및 실행코드 무결성 검증	●	●	–	–	–	–
	안전한 업데이트	●	●	●	●	●	–
	감사기록	●	●	–	–	▲	게이트웨이 또는 제어 제품(월패드)에 감사기록 저장 가능

(그림 10) 제품 개발시 고려 보안항목 예시

석의 사례로는 '보안항목 적용이 필요한 저사양의 제품인 경우'또는 '특정 라이브러리의 사용여부'로 구분하여 보안항목 해당여부를 판단한다.

<그림 10> 예시 표에 선별된 제품이 모든 제품을 대표할 수 없고 사례로만 제시하고 있음을 고려해야 한다.

5. 국내 보안인증 현황

5.1. 정보보호관리체계 인증 현황

중소기업에서 가장 많이 받는 인증 중에 ISO 9001(품질경영시스템)은 "모든 산업 분야 및 활동에 적용할 수 있는 품질경영시스템의 요구사항"인 ISO 9001 국제 표준을 "제품 또는 서비스의 실현 시스템이 충족하고 유효하게 운영하고 있음을 제3자가 객관적으로 인증"을 말하며, ISO 27001 인증은 정보보호정책, 통신・운영, 접근통제, 정보보호사고 대응 등 정보보호 관리 11개 영역, 133개 항목에 대해 얼마나 잘 계획하고 구현하며, 점검하고, 개선하는가를 평가하고 이에 대해 인증이다. 즉 인증은 제정된 '요구사항'을 '충족'하는지 여부를 공신력 있는 제3자가 '검증'해 주는 것이다.

국내 '정보보호 안전진단' 제도는 정보보안컨설팅 전문기업이 사전 컨설팅, 인증심사, 확인증을 부여하는 구조적 문제를 포함해 검증의 객관성 및 운영부실 이유로 비판을 받으면서 전면 폐지되면서, 2012년 정보통신망법 제47조(정보보호 관리체계의 인증)를 근거로 정보보호관리체계(ISMS) 인증이 의무화 추진되었다.

'정보보호 관리체계 인증 등에 관한 고시'(과학기술정보통신부 고시)에서는 ISMS 인증기준으로 13개 통제분야, 92개 통제항목을 정의하고 있다. 같은 법 제47조의3에서 규정한 개인정보보호관리체계(PIMS) 인증 역시 '개인정보보호 관리체계 인증 등에 관한 고시'(방송통신위원회 고시)에서 9개 영역, 최대 86개 항목의 인증기준을 설정하고 있다.

과기정통부가 주관하던 정보보호관리체계(ISMS)와 행안부·방통위가 주관하던 개인정보보호관리체계(PIMS)를 통합 계획이 지난 2017년 12월 발표됐다. 당시 3개 부처는 정보보안과 개인정보보호가 밀접해지고 각각의 인증이 중복 운영되면서 기업부담이 커지는 것을 해소하기 위해 양대 인증을 합치기로 결정했다. 특히, ISMS와 PIMS의 인증기준 각각 104개(ISMS)와 86개(PIMS)중에서 중복되는 항목을 정리하여 102개(ISMS-P)로 통합하고, 취득하는 기관·기업이 ISMS(의무규정)만 취득하려 할 경우 개인정보보호 항목(20~22개)은 제외한 채 취득할 수 있도록 한다고 발표 했으며, 지난 2018년 7월 4일 열린 '2018년 제33차 위원회'에서 방통위는 ISMS-P 통합을 위한 '개인정보보호 관리체계 인증 등에 관한 고시'를 전부 개정하고, 고시 발령일부터 즉시 시행하겠다고 밝혔다.

최근 개인정보보호의 중요성이 높아지고 있고, ISMS-P로 통합되면서 개인정보보호와 관련된 항목이 줄어든 만큼 국내 정보보안인증을 취득하려는 기관과 기업들이 늘어날 것으로 예상된다.

5.2. 사물인터넷(Internet of Things) 보안인증 현황

정부는 지난 2014년에 「사물인터넷 정보보호로드맵」(미래부, 2014.10.31.)을 발표하였고, 「사물인터넷 정보보호 로드맵 3개년 시행계획」(미래부, 2015.6.)에는 홈·가전, 자동차, 의료, 제조, 에너지 분야에서 IoT 보안인증을 추진한다는 계획을 밝혔으며, 지난 2017년 11월에 KISA는 IoT기기 및 연동 모바일 앱을 대상으로 「IoT 보안인증」 기준을 마련하고 시험과 인증 업무를 시작되었다. KISA는「사물인터넷(IoT) 시험인증 기준해설서」(2017.12.19)를 발간하여 시험·인증 업무수행 과정의 주요 절차 및 세부 활동사항을 제시하고 있으며, 「IoT 공통보안가이드」(2017.04.12)에서는 IoT 제품 및 서비스의 '설계 및 개발, 설치, 운영 및 관리, 폐기' 까지 전주기에 걸쳐 발생할 수 있는 보안위협에 대응하기 위해 고려해야 하는 기본적인 보안 요구사항을 제시하고 있다. 또한,「홈가전 IoT보안가이드」(2017.07.01)에서는 제품 개발자 및 제조사가 개발 단계에서부터 보안을 고려하여 안전하게 개발할 수 있도록 가이드를 제공하고 있다.

'홈네트워크 건물인증' 인증기관은 중앙전파관리소, 심사기관은 한국정보통신진흥협회, 보안점검기관은 KISA가 맡고 있으며, 기존 AA 등급에 모바일앱, 기기 확장성, 보안 등 홈IoT 사항을 추가하여 이를 충족할 경우 AAA(홈IoT) 등급을 부여하고 있다. (2017.07.01 시행)

KISA는 「홈네트워크건물인증 보안점검 가이드」(2017. 07.01)를 발간하여 건설사 및 홈IoT 제조사 등 관련된 이해관계자들이 손쉽게 홈네트워크건물 인증 보안점검을 수행할 수 있도록 하였다.

IoT 기기와 서비스가 가정 내에 많이 설치되고 활성화되고 있는 상황에서 IoT 기기 보안인증과 정보보호관리체계인증 수요는 늘어 날 것이다.

6. 결 론

본고에서는 IoT서비스로 인한 일상생활의 편리성을 살펴보고, 이에 따른 보안 위협과 홈·가전 IoT제품의 보안항목 및 대응방안들을 살펴보았다.

일상생활에서 IoT 홈 스마트 아파트, 통신사의 IoT서비스 등 스마트시티가 일상생활에 이미 깊숙이 들어와 있다. 그러나 이런 일상생활에서의 융합형 ICT서비스와 함께 정보보안의 중요성은 부각되고 있지 않은 실정이다. IoT서비스 플랫폼의 초기기획 단계부터 정보보안을 먼저 고려해야 할 것이다.

IoT를 이용한 미래에는 일상생활에서의 자율 주행 서비스, 의료 IoT케어 서비스, 국방 IoT 등 다양한 영역에서 접목되고 있다.

이러한 다양한 기기간의 융합과 복합되어 만들어지는 서비스인 홈·가전 IoT 제품들은 하드웨어 및 소프트웨어 개발 단계에서 요구되어지는 보안사항과 관리적·물리적·기술적·법률적 정보보안 요구사항을 반영하여야 하며 기업들은 정보보호관리체계를 구축하여 IoT 서비스의 안정성을 소비자에게 제공되도록 지속적으로 노력하여야 한다.

따라서, GDPR 등 글로벌 환경 변화와 IoT서비스 확대에 따른 안전한 ICT구현과 국내산업계가 정보보호관리체계 구축 활성화를 위한 다양한 방안들이 추가적으로 연구하는 것도 가능할 것으로 판단된다.

참 고 문 헌

[1] KISA,홈가전 IoT보안가이드, 2017
[2] IITP, IoT 현황 및 주요 이슈, 2014

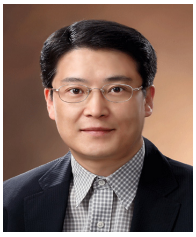
◐ 저 자 소 개 ◑

마 기 평

2015년 전남대학교 정보보안협동과정 졸업(석사)
2017년 전남대학교 정보보안협동과정 수료(박사)
2011년~현재 (주)윈스 SOC사업팀장
2018년~현재 정보보호인정협회(ISA) 이사
2018년~현재 CISSP KOREA 챕터 이사
관심분야 : ISMS(Information Security Management System), PIMS(Personal Information Management System),IoT, ISO국제표준, NCS, 보안

이 상 준

1991년 전남대학교 전산통계학과(이학사)
1993년 전남대학교 전산통계학과(이학석사)
1999년 전남대학교 전산통계학과(이학박사)
2007년~현재 : 전남대학교 경영학부 교수
관심분야 : 경영정보시스템, 전자상거래, 정보보호 등



공 병 철

1999년~현재 (사)한국사이버감시단 대표이사
2002년~현재 (사)한국인터넷정보학회 부회장
2015년~현재 정보보호인정협회(ISA) 회장
2015년~현재 (주)에스링크(S-LINK) 대표이사
관심분야 : 정보보호, 클라우드 컴퓨팅, IoT, ISO국제표준, ISMS(Information Security Management System)