https://doi.org/10.33778/kcsa.2021.21.1.079

국내 IoT 보안인증 제도 개선 연구★

이 용 필*, 서 영 진**, 이 상 걸***

요 약

ICT기술이 융합되는 사회에서는 IoT 등 다양한 네트워크 연결기기의 사용이 확산되어지고 있다. 네트워크 연결 기기들은 필연적으로 정보 유출 등 해킹의 위협에 노출되며, 이를 대응하기 위한 대책 마련이 필요하다. 해외에서도 ICT 융합기기 대상 설계부터 보안을 고려한 제품 생산 및 판매를 촉진하기 위해 보안인증을 도입하고 있으며, 이를 위해 법제화 및 인증기준과 방법을 표준화하는 작업이 진행되고 있다. 국내에서도 이에 발맞추어 2020년 정보통신망법이 개정되면서 네트워크에 연결된 ICT 융합기기를 '정보통신망 연결기기등'으로 새롭게 정의하고, 보안인증제도 근거를 마련하였다. 관련 국내외 동향을 살펴보고 국내 보안인증 제도를 구현하기 위한 구체적인 고려사항들을 정리해 인증수행체계, 인증등급, 인증마크, 인증수수료, 변경관리, 인증유효기간 등과 중장기적 발전방향을 제안하였다.

A Research on the improvement of domestic IoT security certification system

Yongpil Lee*, YungJin Suh**, SangGeol Lee***

ABSTRACT

In a society where ICT technology is converged, the use of various network-connected devices such as IoT is spreading. Network-connected devices are inevitably exposed to the threat of hacking such as information leakage, and countermeasures need to be prepared to respond. Security certification system for IoT devices has been introduced to promote security of IoT products, and for this purpose, legalization and standardization of certification standards and methods are in progress. In line with this, in Korea, as the Information and Communication Network Act was revised in 2020, ICT convergence devices connected to the network were newly defined as "information and communication network connected devices," and the basis for the security certification system is being established. We summarized related domestic and foreign trends and suggest specific considerations for implementing the security certification system for IoT devices in South Korea.

Key words : IoT security, Connected devices, IoT security certification

접수일(2021년 1월 30일), 수정일(1차: 2021년 3월 22일), 게재확정일(2021년 3월 23일)

★ 본 논문은 과학기술정보통신부의 지원에 의하여 연구되었음.

* 한국인터넷진흥원 융합보안단 수석연구원(주저자)

** 한국인터넷진흥원 융합보안단 연구위원(교신저자)

*** 한국인터넷진흥원 융합보안단 책임연구원(공동저자)

1. 서 론

전세계 네트워크 연결기기 중 IoT 애플리케이션을 지원하는 M2M 연결은 149억 개에 달하며, 23년에는 전세계 인구 1인당 3.6개의 네트워크 연결 기기를 보유하며, 가구당 10개의 네트워크 연결기기를 보유할 것으로 예상하고 있으며[1]. 국내 IoT 플랫폼 시장 규모도 전년 대비 19.5% 증가한 7,540억원까지 증가할 전망이며, 23년까지 16.1%의 연평균성장률을 보이며 1조 3,308억원에 이를 것으로 예상하고 있다[2].

이렇게 이용이 증가하고 있는 홈 · 가전, 자동차, 의료기기 등 다양한 분야의 IoT 기기들은 보안취약점을 보유하고 있는 경우가 많으며, 이러한 취약점으로 인해 보안사고가 빈번하게 발생하고 있다. '25년에 사이버 공격으로 인해 약 10.5조 달러의 침해사고 피해금액이 발생할 것으로 추정되고 있다[3].

이용자들의 개인정보를 보호하고 사이버위협에 따른 피해에 대응하기 위해서는 이러한 IoT 기기들의 보안취약점을 제품 출시 전에 최소화할 수 있는 장치가 필요하며, 해외 각국에서도 4차산업혁명 및 초연결사회에서 필수적으로 사용되어지는 IoT의 보안을 위해 사이버보안 인증제도 및 보안을 고려한 제품을 제작하도록 요구하는 제도를 도입하고 있다[4][5].

4차 산업혁명을 위해 세계 주요국은 IoT기기 등의 사이버보안을 위한 법제화 방안을 모색 중이며, 구체적으로는 IoT 보안가이드 개발, IoT 보안 관련 표준 개발, IoT 보안인증제도 도입 등 IoT 보안을 위한 다양한 보안정책을 마련하여 시행하고 있다.

미국의 경우, 제조 단계부터 보안내재화를 확보하기 위한 IoT보안 정책 마련 및 이를 구체화・실현하기 위해 다양한 법제화 방안을 추진하고 있다. 미국은 법제화를 하더라도 최소한의 규제를 우선 도입하도록 추진하고 있다. 「사이버쉴드법」('17.10), 「IoT 사이버보안개선법」('19.3) 등 발의를 통해 IoT 기기 제작자들이 보안 강화를 위해 최소한으로 지켜야할 내용을 국립표준기술원(National Institute of Standards and Technology, NIST)에서 IoT 사이버보안 프로그램을 통해 IoT 보안과 관련된 정보를 제공하도록 하고 있다.

유럽은 사이버보안인증제 도입을 통해 ICT 제품 전반의 사이버보안 수준 향상을 추진하고 있다. 이를 위해 「사이버보안법」 제정('19.6)을 통해 IoT 제품·서비스·프로세스에 대한 보안 인증, 수준별 등급제 추진 등 사이버보안 인증체계를 규정하였다.

일본은 2020년 올림픽 및 사물인터넷(IoT)과 관련된 잠재적인 새로운 위협을 고려하여 2018년에 사이버 보안 전략을 개정하였고, 2019년 경제산업성(METI)은 사이버/물리적 보안 프레임워크(CPSF)를 도입하였으며, IoT기기 보안 강화를 위해 NICT법 개정을 통해 공공기관을 통해 이용자의 IoT 기기를 대상으로 패스워드 설정 확인을 통한 IoT기기의 취약점 점검 및 통지 권한을 부여하고 있다.

한국도 IoT 보안 관련 연구들을 진행[6][7][8]하였으며, 제도적으로는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 개정('20.6)을 통해 IoT에 대한 정보보호인증제 시행 기반을 마련하였다.

본 논문에서는 해외 IoT 보안인증 법제도 및 운영사례를 살펴보고, 국내 IoT 보안인증 제도 개선에 반영될 수 있는 내용들을 도출하여 제시해보고자 한다.

2. 해외 IoT 보안 관련 법제도 현황

2.1 미국 IoT 보안 관련 법제화 추진 현황

2.1.1 연방 IoT 사이버보안개선법

미국은 2016년 미라이 봇넷(mirai botnet)의 공격으로 극심한 인터넷 접속 마비 상황을 겪은 후 IoT 보안에 대한 중요성이 증대되었다. 이에 연방 및 지방정부에서 IoT 기기의 보안 강화를 위한 IoT 보안 정책 마련 및 이를 구체화・실현하기 위한 법제화를 추진하였다.

연방의회 차원에서는 2017년 「2017 IoT 사이버보안개선법」을 발의하였으나, 회기를 넘겨 폐기되자, 이를 수정한 「2019 IoT 사이버보안개선법」이 상・하원 동시 발의되었고, '20.9월 하원, '20.11 상원을 통과하여 시행되었다[9].

IoT 사이버보안개선법은 IoT 기기의 연방 차원의 구매와 해당 장치를 제공하는 민간 부문에 대해 최소한의 보안기준 확립을 도모하기 위해 제정되었다.

NIST는 정부기관이 소유하거나 제어하는 IoT 및 정보시스템에 연결된 IoT의 사용 및 관리를 위한 정

부 표준 및 지침을 개발(제4조 (a)항)하고, IoT 기기를 포함한 정보 시스템과 관련된 보안 취약점 공개 프로세스에 대한 지침을 개발하여, 발표하도록 역할을 부여하였다(제5조).

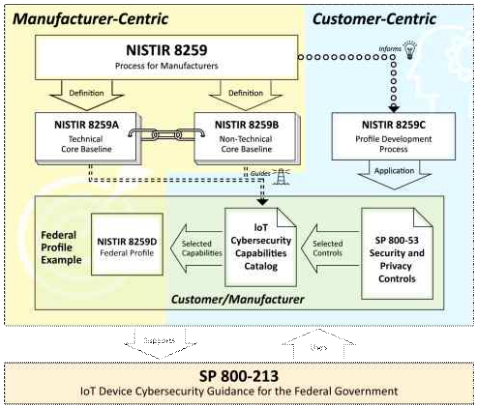
예산관리국(OMB)은 NIST가 제시한 표준 및 지침을 정부기관 정보보안 정책에 반영(제4조 (b)항)하도록 하고 있다. 연방정부기관은 NIST 가이드라인을 준수한 IoT 기기 납품 업체의 제품만 사용이 가능하다.

2.1.2 캘리포니아주, 오레곤주 IoT 보안법

지방정부 차원에서 캘리포니아주 (Senate Bill No. 327)[10]와 오레곤주(House Bill No. 2395)[11]에서는 IoT 제조사를 대상으로 IoT기기별로 디폴트 패스워드를 다르게 설정하도록 하고, 기기 최초 사용에 앞서 사용자에게 새로운 인증수단 생성을 요구하는 보안기능을 탑재하도록 규정한 「IoT보안법」을 제정하여 시행하고 있다('20.1.1 발효). 이외에도 일리노이즈, 메사추세츠, 메릴랜드, 뉴욕, 버몬트주도 비슷한 법을 준비중에 있다[12].

2.1.3 NIST IoT 보안가이드

NIST는 2020년 12월 15일 IoT 사이버 보안개선법에서 요구하는 가이드라인을 위해 4개의 기술문서(NISTIR 8259B, 8259C, 8259D, SP 800-213) 초안을 공개하였다. 이 기술문서들은 2020년 5월 미리 공개한 2개의 문서(NISTIR 8259, 8259A)와 연계되어 있으며, 체계도는 아래 그림과 같다.



(그림 1) NIST IoT 보안관련 기술문서 연계성[13]

IoT 장치를 정보시스템 및 인프라에 통합하려는 연방기관을 위한 전반적인 지침은 SP 800-213[14]에서 제공되며, 연방기관이 IoT 기기 제조업체에 제시할 사이버보안 요구사항을 안내하고 있다.

NISTIR 8259 시리즈(8259, 8259A, 8259B, 8259C, 8259D)는 IoT 제조업체를 대상으로 제조업체가 IoT 기기의 보안을 위해 위험관리 차원에서 사이버보안 위험을 식별하고, 위험을 감소하기 위해 필요한 일련의 프로세스를 정의하고 있다. NISTIR 8259[15]는 제조업체가 IoT 사용자의 사이버보안 위험을 감소시키기 위해 고객과 커뮤니케이션할 내용과 방법에 대해, 시장에 판매하기 전(4가지 사전 활동 : 예상되는 고객을 식별하고 사용예(usecase)를 정의, 고객의 사이버보안 니즈와 목표에 대한 연구, 보안 위험을 줄이고자 하는 고객의 니즈와 목표를 어떻게 전달할지 결정, 고객의 니즈와 목표를 위한 적절한 지원 계획)과 후에 해야할 것(2가지 사후 활동 : 고객과 커뮤니케이션을 위한 방법 정의, 고객과 무엇을 커뮤니케이션할 것인지, 어떻게 커뮤니케이션할 것인지 결정)들을 나열하고 있다.

NISTIR 8259A[16]는 사이버보안을 위해 IoT 기기가 갖추어야 할 사이버보안 역량 핵심 기본사항(the device cybersecurity capability core baseline for securable IoT devices)들을 제시하고 있다. 8259B는 제조업체 또는 관련 협력업체가 기기보안을 위해 취해야 할 비기술적 지원 활동을 자세히 설명한다[17]. 비기술적 지원활동으로는 문서화, 정보와 질의 접수, SW 업데이트/취약점 정보 등 정보 전달, 교육, 고객 피드백 등과 같은 명시적인 지원 기능들이 있다. NISTIR 8259C는 NISTIR 8259A의 핵심 기본사항과 8259B의 비기술적 핵심 기본사항을 특정한 섹터의 고려사항(산업 표준, 규제 지침)을 반영하여 프로파일링하는 방법을 제시하고 있다[18]. NISTIR 8259D는 미국 연방정보시스템 영역에서 NISTIR 8259C 프로세스를 적용하여 NIST SP 800-53B의 낮은 기본사항 통제항목들을 구현하여 연방정보시스템에 IoT 기기들을 통합시키는 것과 관련된 역량을 정의하는 프로파일을 제시하고 있다[19].

2.2 유럽의 IoT 보안 인증 법제화 추진 현황

2.2.1 EU 사이버보안법

EU는 IoT 출현 이후 향후 10년간 EU 전역에 커넥티드 디지털장치가 엄청나게 많이 배포될 것으로 예상하며, 설계만으로 충분한 보안성과 복원력을 가지기에 부족할 것으로 판단하였다.

이를 위해 EU는 ICT 제품, 서비스, 프로세스에 대해 EU 각 회원국으로 하여금 사이버보안 인증을 도입하게 하는 'ENISA(유럽사이버보안국) 및 정보통신기술 사이버보안 인증과 규정 No 526/2013 폐지에 관한 2019년4월17일자 유럽의회 및 이사회 규정 2019/881'(이하, EU 사이버보안법 또는 CSA: cybersecurity act)을 제정해 EU 전체 회원국에 적용하도록 하고 있다. EU 사이버보안법[20] 제2조에서 정의하고 있는 ICT 제품, 서비스, 프로세스에 대한 설명은 아래 표와 같다.

<표 1> ICT 제품, 서비스, 프로세스 설명

ICT 제품	네트워크와 정보 시스템의 요소 또는 그 요소로 이루어진 그룹
ICT 서비스	네트워크 및 정보 시스템을 통해 정보의 전송・저장・검색 또는 정보의 처리에 완전히 또는 주로 구성하는 서비스
ICT 프로세스	ICT제품이나 ICT서비스를 설계・개발・전달 또는 유지하기 위해 수행되는 활동

2019년 4월 EU 사이버보안법(CSA) 제정을 통해 사이버보안 인증제도(european cybersecurity cetification scheme)를 마련하도록 규정하고, ENISA(유럽 사이버보안원)는 EU 사이버보안 인증프레임워크 체계 구축을 주관하도록 법률로 명시하였다. EU 사이버보안 인증프레임워크는 EU의 사이버보안인증제도를 만드는 절차 및 체계를 말한다.

EC는 인증제도를 위한 Union Rolling Work Programme(URWP)을 ECCG, SCCG와의 논의를 거쳐 작성해야 하는데, URWP는 인증제도에 포함시켜야 할 ICT 제품, 서비스, 프로세스 리스트 또는 카테고리를 포함하게 된다(47조).

ENISA는 ECCG의 지원과 협력 하에 EU 사이버보안 인증제도 후보안(EUCC : european candidate cybersecurity cetification scheme)을 준비해야 하며, EC는 EU 사이버보안 인증제도를 제공하기 위한 시행법률(implementing acts)을 채택할 수 있다. ENISA는 최소 5년마다 유럽 사이버보안 인증제도를 평가해야 한다(49조).

EU 사이버보안 인증제도의 목적은 ICT 제품, 서비스, 프로세스가 수명주기 전반에 걸쳐 저장, 전송 또는 처리된 데이터나 이러한 제품, 서비스 및 프로세스를 통해 제공되거나 접근 가능한 관련 기능 또는 시비스의 가용성, 진본성, 무결성 및 기밀성 보호에 대한 요건을 준수하는지 확인하는 것이다(51조).

EU 사이버보안 인증제도의 보증수준은 ICT 제품, 서비스, 프로세스에 대해 사고의 발생 가능성 및 영향면에서 사용목적에 따르는 위험수준에 비례하여 기본, 보통, 높음 보증수준 중 하나 이상을 지정할 수 있다(제52조).

<표 2> 보증수준과 평가활동

보증수준	평가활동
기본 (basic)	・(보증수준) ICT제품, 서비스, 프로세스가 보안기능을 포함한 보안 요건을 충족하고 알려진 기본 위험을 최소화하기 위한 수준 ・(평가활동) 최소한 기술 문서 검토 포함
보통 (substantial)	・(보증수준) 보안기능을 포함한 보안 요건을 충족하고 알려진 사이버보안 위험과 제한된 기술과 자원을 갖춘 주체가 유발하는 사고 및 공격 위험을 최소화하기 위한 수준 ・(평가활동) 공개적으로 알려진 취약성이 없음을 입증하는 검토, 필요한 보안기능을 올바르게 구현하는지 입증하는 시험이 포함
높음 (high)	・(보증수준) 보안기능을 포함한 보안 요건을 충족하고, 고도의 기술과 자원을 이용하는 공격 행위자의 최신 사이버위협을 최소화하는 수준 ・(평가활동) 공개적으로 알려진 취약점에 대한 방어력 검증, ICT제품・서비스, ICT프로세스에 필요한 보안기능 구현 시험, 모의해킹을 통하여 숙련된 공격자에 대한 저항력 평가 등

EU 사이버보안 인증제도는 ICT 제품, 서비스, 프로세스의 제조사 또는 제공자의 책임 하에 자체 적합성 평가를 허용하며, 자체 적합성 평가는 인증등급 '기본(Basic)'에 해당하는 위험수준이 낮은 경우만 허용한다(제53조).

제조사 또는 제공자는 제도에 명시된 요건이 이행

되었음이 입증되었다고 언급하는 'EU 적합성 선언문'을 발급할 수 있고, 요건준수 확인책임을 지며, 인증제도에 명시된 기간 동안 관련 정보를 제공하고 사본을 ENISA와 각국 사이버보안 인증기관에 제공하여야 한다.

EU 적합성 선언문의 발행은 자발적으로 이루어지며, 모든 EU회원국에서 인정된다.

사이버보안 인증제도의 요소로는 인증제도의 주제 및 범위, 표준, 평가방법 및 보증 수준에 대한 설명, 자체 적합성 평가 허용 여부, 적합성 평가기관 요건, 마크 또는 라벨 사용 조건, 요건 준수 모니터링 규칙, 인증서 발급, 유지, 지속 및 갱신 조건과 인증 범위 확장 또는 축소 조건, 유효기간, 상호인정 조건, 동료평가 방법을 다루는 규칙 등이 포함되어야 한다(제54조).

또한, 취약성 보고 및 처리 방법을 다루는 규칙, 이 EU내 관련 법률 요건을 준수하여야 하며, 인증제도에 따른 인증서 및 적합성 선언서는 EU내 명시된 법률 요건을 준수한다는 사실을 입증할 수 있어야 한다.

적합성 평가기관에서는 '기본, 보통'에 해당하는 인증제도의 인증서를 발급하고, 인증 등급 '높음'의 경우 지정된 각국 사이버보안 인증기관 또는 적합성 평가기관에서만 발급이 가능하다(제56조).

타당한 경우 EU 사이버보안 인증서를 공공기관(각각 사이버보안 인증기관, 적합성 평가기관으로 승인된 공공기관)에서만 발급할 수 있다고 규정할 수 있다.

사이버보안 인증제도가 시행이 되면, EU 사이버보안 인증제도가 적용되는 각국 국가별 인증제도는 효력을 상실하며, 동일한 ICT제품, 서비스, 프로세스에 대해 회원국에 별도의 인증제도를 도입할 수 없다(제57조).

EU 회원국은 국가별 사이버보안 인증기관을 설립할 수 있으며, 효과적 운영을 위해 유럽사이버보안인증그룹(ECCG) 참여를 권고한다(제58조).

EU 사이버보안 인증서 및 적합성 선언서의 EU 내 전체적 동일한 표준을 준수하기 위해 각 국가별 사이버보안 인증기관은 동료평가를 받아야 한다(제59조).

적합성 평가기관은 국가 인정 기구에서 승인하고 유효기간은 최대 5년이다. 각국 사이버보안 인증기관에서 EU 사이버보안 인증서를 발급한 경우 각국 사이버보안 인증기관의 인증기구가 적합성 평가기관으로 승인된다(제60조).

각국 사이버보안 인증기관은 승인된 적합성 평가기관을 EC에 알려야 하고, EC는 제도 발효 후 1년 후에 적합성 평가기관 목록을 발표해야 한다(제61조).

효력발생 시점은 제58조(국가별 사이버보안 인증기관 설립), 60조(적합성 평가기관), 61조(적합성 평가기관 목록 발표), 63조, 64조 65조는 2021년 6월 28일부터 적용한다.

2.2.2 EU 사이버보안 인증제도(scheme) 후보안 V1.0[21]

ENISA는 EU 사이버보안법에 따라 2020년 7월에 EU 사이버보안 인증제도 후보안 V1.0(이하 EUCC)을 발표하였다. EUCC는 기존의 SOG-IS MRA(Senior Officials Group Information Systems Security Mutual Recognition Agreement)를 대체하기 위해 개발된 인증제도로 기존의 SOG-IS가 전체 EU 회원국이 참여하지 않아, 상호운영성 측면에서 EU의 디지털 싱글 마켓 목적에 부합하지 않는 문제점을 개선하기 위한 것이다.

EUCC는 ICT 제품의 인증을 다루며, CC와 CEM 기반의 인증제도이다. 위 문서는 CC(Common Criteria) 인증제도의 '정보보호제품 평가인증 수행 규정'과 유사한 문서로 평가기준, 평가방법, 인증/평가기관의 요건, 인증효력유지(제품의 패치관리), 사후관리(취약점 발견 시 조치), 인증마크의 사용, 인증서 발행, 유지, 갱신절차, 인증서 형식, 인증서 유효기간, 상호인정 정책 등 EUCC를 운영하기 위한 관련 절차 및 요건 등을 정의하고 있다. 인증 대상이 되는 ICT 제품은 최소한 CC Part II의 보안기능(SFR : security functional requirement) 중 하나 이상을 포함하고 있어야 하며, Substantial 또는 High 보증등급을 목적으로 해야 한다.

CSA 보증수준은 Basic, Substantial, High가 있으나, EUCC에서는 Substantial, High 2가지 보증수준만을 다룬다.

CC에서의 7개(EAL1~7) 보증수준을 CSA에서는 2가지 보증 수준으로 정의하고 있다. AVA_VAN.1 ~ AVA_VAN.2 는 CSA의 보증수준 'Substantial'에 매핑되며, AVA_VAN.3 ~ AVA_VAN.5 는 CSA의 보증수준 'High'에 매핑된다.

보증수준 표현방법은 CSA-AL(B or S or H)로 나

타낸다. 평가기준은 ISO/IEC 15408을 준수하고, 평가방법은 ISO/IEC 18405를 적용한다.

인증기관은 ISO/IEC 17065, 평가기관은 ISO/IEC 17025 요건 충족이 필요하다.

인증서 유효기간은 최대 5년이며, 특정 도메인의 경우 인증서 유효기간을 더 짧게 정할 수 있도록 되어 있다. 인증된 제품과 관련된 정보는 인증서 만료일로부터 최소 5년 동안 제공되어야 하며, 인증보고서를 CSA 전용 웹사이트에 공개하도록 하고 있다. 인증 후 취약성 발생 시 ISO/IEC 30111 및 ISO/IEC 29147 규칙에 따라 처리하도록 하고 있다. 취약성 패치와 관련한 행위는 1개월 이내에 수행하야 하며 협의에 따라 연장이 가능하다.

3. 해외 IoT 보안인증 관련 표준

3.1 ETSI 표준

ETSI(유럽전기통신표준협회, European Telecommunications Standard Institude) 사이버 보안위원회(TC CYBER)[17]는 internet-connected consumer products에 대한 보안기준을 수립하고 IoT 인증 체계의 기반을 제공하기 위해 2020년 6월에 ETSI EN 303 645 Cyber Security for Consumer Internet of Things v2.1.1(이하 ETSI 표준) 표준문서를 발표하였다.

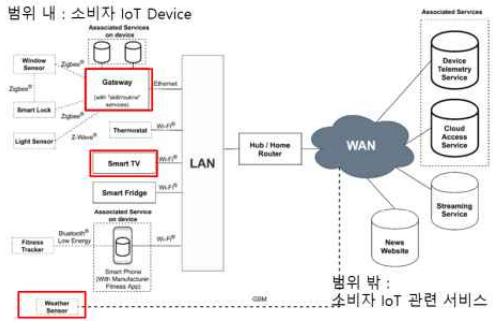
ETSI 표준은 IoT 보안 및 개인정보보호에 대한 원칙, 정보 및 위험에 대한 지침을 제공하며, 본 표준의 범위는 정보보안과 개인정보보호를 모두 포함하는 IoT에만 적용된다.

ETSI 표준의 적용 범위는 다음과 같은 IoT 장치를 대상으로 한다.

<표 3> ETSI 표준 적용 대상 소비자 IoT

·연결된 어린이 장난감 및 베이비 모니터
·연기 감지기 및 도어락과 같은 연결된 안전 관련 제품
·여러 장치가 연결되는 IoT 기지국 및 허브
·스마트 카메라, TV 및 스피커
·착용 가능한 건강(health) 추적기
·연결된 홈 자동화 및 경보 시스템. 특히 게이트웨이 및 허브
·세탁기 및 냉장고와 같은 연결된 기기(Appliances)
·스마트 홈 어시스턴트
·제한된 기기(예, 창문 접촉 센서, 누수(flood) 센서, 에너지 스위치)

관련 서비스(associated service), 소비자 IoT가 아닌 제한된 기기(constrained device)는 ETSI 표준 범위에 포함되지 않는다.



(그림 2) 소비자 IoT 배치 예시 사례 (자료 : ETSI 표준)

세부 보안요구사항은 다음과 같으며 필수 요구사항과 권고사항으로 구분되며, 각 요구사항별로 조건이 존재할 수 있다.

<표 4> 소비자 IoT를 위한 사이버 보안 요구사항(cyber security provisions)

1. 소비자 IoT에 대한 사이버보안 요구사항(세부인증기준 64개)
 1) 범용적인 기본 비밀번호 금지(5개)
 2) 취약성 보고서를 관리하는 수단 구현(3개)
 3) 소프트웨어 업데이트 유지(16개)
 4) 민감한 보안 변수를 안전하게 저장(4개)
 5) 안전하게 통신(8개)
 6) 노출된 공격 표면 최소화(9개)
 7) 소프트웨어 무결성 보장(2개)
 8) 개인정보의 안전한 보장(3개) : 전송되는 개인정보의 기밀성 보호, 민감 정보는 적합한 암호화, 외부 감지 기능은 사용자에게 명확하고 투명하

게 문서화
9) 정전시 시스템 복원력 유지(3개)
10) 시스템 원격 측정 데이터 검사(1개)
11) 사용자가 사용자 데이터를 쉽게 삭제(4개) : 개인 데이터 삭제 기능 제공, 삭제 확인 메시지 등
12) 기기의 설치 및 유지보수 용이(3개)
13) 입력 데이터 유효성 확인(1개)
2. 소비자 IoT에 대한 개인정보보호 요구사항
1) 제조사는 소비자에게 개인정보 처리 내용, 이용되는 방법, 목적 등을 투명하게 제공
2) 소비자 동의 기반으로 개인정보 수집된다면 유효한 방법으로 동의를 받아야 함
3) 동의 후에도 언제든 소비자의 동의 철회 방법 제공
4) IoT 기기 및 서비스에서 원격 데이터 수집 시 기능은 최소한으로 유지
5) 원격 수집 데이터 내용, 이용되는 방법, 수집 대상 및 목적에 대한 정보를 소비자에게 제공

핀란드 교통&통신기관인 Traficom은 2019년 11월에 ETSI EN 303 645 Cyber Security for Consumer Internet of Things v2.0.0 초안문서를 기반으로 시험인증한 3개 제품에 대해 유럽 처음으로 사이버보안 라벨을 부여하였고, 영국 DCMS는 ESTI EN 303 645 개발을 선도하였으며, 소비자 IoT 보안을 위한 실행강령 및 ESTI EN 303 645의 상위 3가지 지침을 중심으로 보안요구사항을 적용하도록 하였다.

<표 5> Top 3 가이드라인

① IoT 기기 비밀번호는 고유해야 하며, 모든 범용 공장 설정에서 재설정 불가
② IoT 기기 제조사는 취약성 노출 정책의 일환으로 업체 연락처 공개
③ IoT 기기 제조사는 제품 보안 업데이트를 받을 수 있는 최소시간 명시

민간 감독기관으로 제품인증 등의 업무를 수행하고 있는 독일의 기술감독협회(TÜV SÜD)는 IoT 사이버 보안을 위해 ESTI EN 303 645 및 NISTIR 8259를 적용하여 IoT 기기 시험을 수행하고 있다.

Eurosmart IoT 인증의 Basic 수준은 ETSI EN 303 465에 의존적이며, Substantial 수준은 부분적으로 의존적이라고 발표하였다.

ENISA의 인증을 지원하는 표준(Standards supporting Certification, 2019.11월) 보고서에서, 유럽 사이버 보안 인증 제도는 세 가지 수준의 보증을 포함하며 각 수준에 대한 기술 규칙은 ETSI EN 303 645 표준 및 Eurosmart 체계를 기반으로 한다.

기본(Basic) 보안 수준 인증은 ETSI EN 303 645의 요구 사항을 기반으로 하는 자체 평가를 통해 달성한다. 기본 수준의 보증은 최소 수준의 보안으로 단순한 고객 IoT 장치를 대상으로 한다. 이상적으로 모든 IoT 장치는 자체평가 프로세스를 통해 이 수준의 기술 요구사항을 준수해야 한다. 보통(Substantial) 보안 수준 인증은 취약점 관리, 정책 및 마크 사용과 같은 정의된 프로세스를 추가하는 것이 필요하며, 공공장소에서 사용되는 IoT 카메라, IoT 장치 등 일정 수준의 보안을 보장해야 하는 장치에 적용된다. 높은(High) 보안 수준의 인증은 IoT 장치가 중요한 인프라 환경이나 사이버 공격이 심각한 피해를 입힐 수 있는 영역에 배치된 경우 등 높은 수준의 보증을 필요로 하는 경우에 적용되며, 기존 CC 인프라(SOG-IS22)를 활용한다.

ETSI가 유럽 표준을 설정하고 있지만 이를 집행하는 방법은 회원국에 달려 있으며, 영국과 핀란드는 이를 의무화하기 위한 단계에 있으며, 다른 회원국들은 이를 수행하는 방법에 대해 논의 중이다[22].

4. 국외 IoT 보안인증 사례

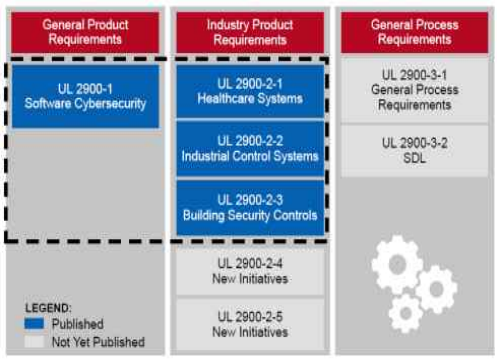
4.1 미국 UL CAP

UL(Underwriters Laboratories, 미국보험협회안전시험소) CAP(Cybersecurity Assurance Program)은 UL 2900 규격에 따라 네트워크와 연결되는 제품과 시스템의 소프트웨어 취약도와 해킹 및 악성코드(malware) 위협에 대한 보안 수준 등 잠재 사이버 보안 문제를 테스트하고 인증하는 프로그램이다. UL 2900 규격은 네트워크와 연결되는 제품과 시스템을 테스트 및 평가하기 위한 기술 영역에 대한 가이드라인을 제공하며, 보안 기술 발전과 업계 동향에 따라 보완, 확

장할 수 있도록 설계되었다. 美 백악관에서 발표한 사이버 보안 국가 행동 계획(CNAP, Cybersecurity National Action Plan)의 주요 공공 시설과 연결된 사물인터넷(IoT) 공급망과 디바이스를 시험하고 인증하는 방법으로 UL CAP을 인정하고 있다.

UL CAP 개발에는 미국 연방 정부, 업계, 학계 등 보안에 대한 주요 이해 당사자들이 폭넓게 참가였으며, UL CAP의 인증기준으로 UL2900 시리즈를 사용하고 있다[23].

UL CAP은 가전/에너지/의료/교통/제조 등 IoT 분야 제품/시스템에 대한 시험/평가/인증 서비스를 제공하며, 기본적인 IoT 제품은 UL-2900-1, 의료분야 기기(네트워크로 연결되는 헬스케어 시스템 컴포넌트)는 UL-2900-2-1, 제조 기기(네트워크로 연결되는 제어시스템)는 UL-2900-2-2 등으로 제품군에 따라 인증기준을 달리 개발하여 적용하고 있다. UL2900-1은 네트워크 연결 제품에 공통적으로 적용할 수 있는 보안요구사항을 정의하고 있으며, UL2900-1와 UL2900-2-1은 미국 표준(ANSI)으로 인가되었고, 이후 캐나다 표준(CAN)으로도 인가되었으며, FDA도 의료기기의 사이버보안 합의표준(consensus standards)으로 UL 2900-1과 UL 2900-2-1을 채택하였다[24].



(그림 3) UL CAP 기준인 UL2900 시리즈 구성[25]

UL2900 시리즈는 제조사별로 제품 위험관리 프로세스를 살펴보고 있다. 제품 설계 시 제품에 대한 보안 위험 분석, 위협 분석시 식별된 위험에 대한 분류스킴 사용(예, CAPEC, DREAD 등), 제품상 알려진 취약성 존재 가능성에 대한 위험 평가 방법(수용가능 CVE, CWE 등)을 적용하고 있다.

UL CAP 인증현황은 UL 홈페이지에 19개사 31건의 인증목록이 공개되어 있다(2020.10.05. 기준)[26].

4.2 미국 UL IoT Security Rating

UL CAP 이외에 UL은 보증하는 보안수준을 등급화하여 표시하는 IoT Security Rating이라는 별도의 인증프로그램을 개발하였다. IoT Security Rating은 일반적인 공격 방법 및 알려진 IoT 취약성에 대해 스마트 제품의 중요 보안 측면을 평가하는 프로세스로 2019년 5월 런칭후 CES 2020에서 인증마크를 발표하였다.

IoT Security Rating은 영국의 소비자 IoT 보안을 위한 실행 규범 및 이를 기반으로 하는 ETSI TS 103 645 표준을 준수하고 있다.

등급은 5개 단계로 구분되며, 각 단계별 보안요구사항은 다음과 같음

(그림 4) UL Security Rating 단계 및 단계별 보안요구사항

UL IoT Security Rating 현황은 Gold 등급이 1건, Silever 등급이 7건 등 4개사 8건이 공개되어 있다(2020.10.05. 기준).

4.3 핀란드 사이버보안 라벨

핀란드 교통&통신기관인 Traficom은 2019년 11월에 ETSI EN 303 645 Cyber Security for Consumer Internet of Things v2.0.0 초안문서를 기반으로 인증

을 수행하였다. 사이버보안 레이블의 적극적인 개발은 2018년 말에 시작하였으며, Cozify Oy, DNA Plc 및 Polar Electro Oy와 공동으로 NCSC-FI(National Cyber Security Center Finland)가 이끄는 파일럿 프로젝트에서 개발되었다. 장치가 EN 303 645에 기반한 인증 기준을 충족하는 경우, 경우 사이버 보안 레이블을 네트워킹 스마트 장치에 부여 할 수 있다.

유럽 처음으로 2019년 11월에 소비자용 스마트 기기에 대해 사이버보안 라벨을 부여하였으며, Cozify Hub, DNA의 Wattinen 스마트 난방시스템, Polar Ignite 피트니스 스마트워치 제품 등 2020년 12월 현재 9개 제품이 라벨을 받았다[27].

4.4 싱가포르 IoT 사이버보안 라벨

싱가포르 정부는 제조사들이 자발적으로 신청하고 소비자들이 쉽게 해당 제품의 보안 수준을 파악하여 정보에 기반한 결정을 내릴 수 있도록 사이버보안 등급 표시 제도(CLS, cybersecurity labelling scheme)를 실시하도록 하였다. 싱가포르 사이버보안원(CSA, cyber security agency)은 공격시 사용자에 미치는 영향을 고려하여 가정용 무선인터넷 공유기, 스마트 홈 허브 등을 대상으로 CLS를 적용하였다. 상호운용성 및 통신표준의 일환으로 최소 보안 요건을 제시하도록 하였고, 다음과 같은 일련의 평가를 바탕으로 등록된 제품의 보안조치를 수행하도록 하였다.

<표 6> 주요 시험평가 보안요구사항(provisions)

·Default 암호를 사용하지 않는 등 기본 보안 요건 충족 여부
·설계상 보안 원칙 준수 여부
·일반적 소프트웨어 취약점의 존재 여부
·일반적 사이버공격에 대한 방어 가능 여부

싱가포르의 사이버보안 Label은 1~4 등급으로 나누어져 있으며, 4등급은 모의침투 테스트를 거쳐야 한다. 인증기준은 4개의 Tier로 구성되며, Tier 1~2단계는 제조사 자가선언으로 하지만, Tier 3~4단계는 제3자의 독립적인 시험을 거쳐야 한다[28].

5. 국내 IoT 보안인증 체계 개편 방안

5.1 국내 IoT 보안인증 현황

국내 IoT 보안 정책은 정부에서 2014년 IoT 기본계획을 발표하였고, 보안 강화를 위해 IoT 보안로드맵이 발표된 후 본격화 되었다. 2016년 IoT 공통보안 가이드가 제작되었으며, 2017년부터는 스마트홈, 스마트의료, 스마트교통, 스마트공장, 재난안전, 스마트시티 등 각 분야별 보안가이드를 제작하여 배포하고 있다[29].

2017년에 한국인터넷진흥원에서 IoT 보안인증 기준 및 평가방법론을 개발[30]하여 IoT 보안 인증·시험 서비스를 개시하였으며, 현재 법적근거가 없는 자율인증으로 진행하고 있다.

IoT 보안인증·시험 서비스는 IoT 제품 및 연동 모바일 앱에 대해 일정 수준의 보안을 갖추었는지 시험하여 기준 충족 시 인증서를 발급해주는 서비스로, 인증 대상은 IoT 제품 및 연동 모바일 앱을 포함한다. 유효기간은 3년이며, 2년 연장 가능하다.

시험 및 인증기관은 한국인터넷진흥원이 동시에 수행하고 있으며, 인증 수수료는 초기 인증 수요 창출과 업계 부담 완화 등을 위해 무료로 시행 중이다.

보안인증 기준으로 점검사항은 인증, 암호, 데이터 보호, 플랫폼 보호, 물리적 보호 등 5개 영역이고, 41개 세부기준으로 구성된다.

보안인증은 Lite, Basic, Standard 3개 등급으로 구분[31]되며, Lite 등급은 펌웨어 기반의 센서 등 소형 제품으로 10개 항목의 세부보안기준을 충족하는지 시험·점검한다[32]. Basic 등급은 저사양 OS를 탑재한 중소형제품을 대상으로 하며 23개 세부보안기준을 충족하는지 시험·점검한다[33]. Standard 등급은 중대형 스마트가전제품을 대상으로 하고 41개 세부보안기준을 시험·점검한다[34].

보안인증 시험 전에 보안인증을 위해 준비해야 할 내용에 대한 사전컨설팅, 보안시험도구에 대한 교육 등도 별도로 진행하고 있어, SME들의 부담을 덜어주고 있다.

현재까지 운영되는 실적은 '18년 ~ '20년 12월말 현재 총 69건을 인증해 주고 있다.

5.2 IoT 보안인증 법적 근거 마련

IoT 보안과 관련해 법적근거가 부족한 부분을 해결하기 위해 2020년 '정보통신망법 이용촉진 및 정보보호 등에 관한 법률'이 개정되었다[35].

주요 내용으로는 첫째, '정보통신망연결기기등'이라는 용어로 커넥티드 디바이스를 별도로 정의하고, 현재 정보통신망법의 정보보호 부문 적용대상자가 정보통신서비스제공자를 중심으로 되어 있는데, 규율대상자에 정보통신망연결기기등 제조·수입자를 추가하였다.(제45조제1항제2호 신설).

둘째, '정보통신망연결기기등'의 안전한 이용을 위한 정보보호조치를 별도로 고시하도록 하였고(제45조제3항제5호), 제조·수입자가 이 조치를 지키도록 권고할 수 있도록 하였다.(제45조제2항)

셋째, IoT 기기의 시험·검사 등이 분야별로 주무부처가 다르고, 전문기관이 상이할 수 있기에 분야별 시험·검사 등의 기준에 IoT 기기의 보안을 위한 정보보호지침 내용을 반영할 수 있도록 요청하는 내용을 담고 있다(제45조제4항 신설).

넷째, 정보통신망 연결기기등 관련 침해사고 대응을 위해 관계부처와 협력하여 과기정통부 장관이 침해사고 원인분석을 할 수 있도록 하였고, 침해사고가 발생한 경우 제조·수입자에게 취약점 개선을 권고할 수 있다.(제48조의5 신설).

다섯째, IoT 기기의 보안인증제도 운영 근거를 마련하였다. IoT 보안인증업무는 과기정통부 장관이 한국인터넷진흥원에 위탁하여 운영하고, 인증기준을 고시하고, 지정된 인증시험대행기관이 인증시험을 하는 체계를 예정하고 있다(제48조의6).

2020년 12월 현재 정보통신망법, 시행령, 시행규칙이 시행되었고, 인증을 위한 고시 등이 준비 중에 있다.

5.3 IoT 보안인증 체계 개편 방향

5.3.1 인증 수행 체계

현행 IoT 보안인증은 한국인터넷진흥원이 IoT 보안인증기관 및 시험기관 역할을 수행하며, 현안사항 발생 시 인증위원회를 구성하여 안건을 심의 수행하고 있다.

개선방향으로는 정책기관(과기정통부), 인증기관(한국인터넷진흥원), 지정요건을 충족하는 인증시험대행기관으로 구성하며, 필요 시 인증위원회를 운영할 수 있다.

5.3.2 인증등급

현재 IoT 기기의 펌웨어, OS 등에 따라 Lite, Basic, Standard로 등급을 나누어 인증기준에 차이를 두고 있으나, EU와 같이 제품의 위험수준에 따라 인증등급을 부여하도록 하고, 인증등급에 따라 인증기준을 획일적으로 차등을 두기 보다는 제품의 특성과 보증수준을 고려하여 인증기준을 차등적으로 적용할 수 있도록 하는 것이 바람직하다.

5.3.3 유효기간

인증서 유효기간은 현재와 같이 3년으로 한다. 다만, 변경·재인증, 사후관리의 내용을 통해 유효기간 내에라도 보안에 취약한 부분이 발생하는 경우 보완할 수 있도록 한다.

5.3.4 변경·재인증

현행 IoT 보안인증에는 IoT 보안인증을 받은 후 변경, 재인증 관련 내용이 명시적으로 표현되어 있지 않다. IoT 보안인증을 받은 자가 주요한 설계·기능을 변경하여 인증기준에 미달할 우려가 있는 경우에는 변경인증을 받도록 해야 한다.

IoT 보안인증을 받은 정보통신망연결기기등의 성질·형상의 동일성이 인정되는 경우 정보보호인증의 유효기간을 연장하는 것을 검토할 필요가 있다.

5.3.5 사후 취약점 관리

정보통신망연결기기등이 제품 생산, 판매 이후에도 제품수명주기 동안 보안을 유지할 수 있도록, 인증을 받은 이후에 보안 취약점이 발견되어 인증기준에 미달될 경우에는 보완을 요청할 수 있도록 하였다. 다만, 취약점 보완이 일정 기한까지 되지 않은 경우 인증기준에 미달되어 인증효력을 정지해야할 지는 검토가 필요하다.

5.3.6 시험·인증수수료

그동안 한국인터넷진흥원이 IoT 보안인증을 하는 경우에는 무료로 시험·인증서비스를 제공하였다. 민간 인증시험대행기관을 지정하게 되면 시험 대행에 대한 수수료가 발생하게 되며, 초기에는 IoT 보안인증 확산을 위해 수수료를 감면해주거나 예산을 지원하는 정책적 배려가 필요하리라 보여진다.

5.3.7 인증마크

소비자들이 IoT 보안인증을 받은 제품인지를 인지할 수 있도록 인증마크를 개발하여 제품에 표시하고, 보안인증 등급을 확인할 수 있도록 하여야 한다.

또한, 소비자들에게 인증마크에 대한 홍보를 적극적으로 실시하여 IoT 보안인증 등급이 있는 제품을 구매할 수 있도록 유도하여야 한다.

5.3.8 정보공개

IoT 보안인증을 받은 제품들은 홈페이지 등을 통해 목록을 공개하고, 구체적인 인증내용을 확인할 수 있도록 하여야 한다. 인증기준 버전, 인증보고서(및/또는 인증서), 인증시험대행기관 정보를 추가하고, 인증 효력이 연장된 경우 관련 정보를 공개한다.

5.3.9 인증시험대행기관의 지정

인증시험대행기관으로 지정을 받으려는 자는 인증시험업무를 담당하는 기술능력이 있는 인력(상근 인력)을 보유하고 전담 조직을 갖추고 있어야 하며, 인증시험업무를 수행할 설비, 시험공간 등 시험환경을 갖추고 있어야 한다.

또한, 인증시험 및 인증사후관리 등을 공정하고 객관적으로 수행할 수 있는 운영 요건·능력을 갖추고 있어야 한다. 인증시험대행기관의 지정 효력기간은 3년으로 한다.

5.3.10 인증시험대행기관의 사후관리

인증시험대행기관은 전년도 인증시험실적 보고서를 과기정통부장관에게 제출하고, 과기정통부는 인증시험대행기관 지정기준 충족여부를 확인하기 위하여 점검할 수 있다.

5.4 IoT 보안인증의 중장기적 발전 방향

다양한 산업분야의 기기 · 설비 · 장비들이 개발되고, 서로 다른 기술들이 융합되어 출시될 수 있으므로, 법적으로 구체적인 인증대상을 지정하는 것보다는 범위/범주로 인증대상을 지정하되, 시장 및 기술 진화 상황을 예의주시하여 빠르게 인증대상으로 편입하는 등 IoT 보안인증 제도 활성화 노력이 필요하다.

EU 사이버보안법과 같이 위험도가 낮은 IoT 기기에 대해서는 IoT 제조자 스스로 자가평가를 할 수 있도록 하는 방안도 중장기적으로 검토가 필요하다.

IoT 보안인증 받은 기기 · 설비 · 장비들에 대한 수출 지원을 위해 국외 국가 및 인증기관들과 인증기준 부합화 작업 등을 통해 상호인정 협의 및 범위 확대가 필요하다.

인증기준은 국외 인증기준을 포함할 수 있도록 지속적인 개정작업이 필요하나, 빈번한 기준 개정으로 국내 IoT 기기 · 설비 · 장비 개발사 및 수요처에 혼란을 줄 수 있으므로 개정이전 기준으로 인증받은 제품에 대한 효력에 대한 고민이 필요하다.

또한, 인증기준은 정보보호제품 평가인증(CC인증)처럼, 사전적인 형태의 공통기준을 개발하고 인증대상 유형별 기준을 별도로 개발 및 유지·관리하여 탄력적으로 제도를 운영하는 것이 바람직하다.

인증시험대행기관 시험자 및 제조사 개발인력 등을 대상으로 다양한 교육 프로그램을 제공하여 역량을 강화할 수 있도록 지원하고, 시험자에 대한 자격 프로그램을 연구하여 시험자에 대한 자격제 시행 추진 검토가 필요하다.

인증제품에 대한 나라장터 등록, 인증제품 도입시 가점 등 GS인증 수준의 인센티브가 제공되어야 할 것이다.

또한, 안전한 제품 개발 및 인증시험 지원을 위한 다양한 인증시험도구를 테스트베드에 설치하여 사용할 수 있도록 지원하고, IoT 보안인증 관련 동향을 공유하여 수출용 IoT 제조업체들이 도움을 받을 수 있도록 지원이 필요하다. 이상 IoT 보안인증의 중장기적 발전방향을 정리하면 아래 표와 같다.

<표 7> IoT 보안인증 중장기적 발전 방향

구분	발전방향
인증대상	법적 인증대상 지정은 범주로 지정하여 시장 상황 반영
자가평가	낮은 위험도의 IoT 기기는 제조사가 자가평가 할 수 있게 유도
상호인정	국내 IoT 국외진출 지원을 위해 국외 인증기관과 상호인정 추진
인증기준	공통기준과 제품군 특성을 반영한 유형별 기준을 개발·관리
인증 시험자	시험대행기관의 시험자 교육 및 자격제 시행 추진 검토
인증 활성화	IoT 보안인증 제품에 대해 GS인증 수준의 인센티브 제공
제조사 지원	IoT 제조사 대상 IoT 보안인증 시험도구 활용 지원 확대

6. 결 론

ICT기술이 융합되는 사회에서는 IoT 등 다양한 네트워크 연결기기의 사용이 확산되어지고 있다. 네트워크 연결 기기들은 필연적으로 정보 유출 등 해킹의 위협에 노출되며, 이를 대응하기 위한 대책 마련이 필요하다. EU에서는 사이버보안법을 통해 EU단일시장에서 통용될 수 있는 IoT 보안인증제를 법제화하였고, ENISA를 통해 구체적인 IoT 보안인증 스킴을 개발하도록 하고 있다. 미국에서도 연방정부 차원에서 IoT 보안을 강화하기 위한 제도적 기반을 마련하고 공공분야에서부터 적용하도록 하고 있다. 이렇게 해외에서도 ICT 융합기기 대상 설계부터 보안을 고려한 제품 생산 및 판매를 촉진하기 위해 보안인증을 도입하고 있으며, 이를 위해 법제화 및 인증기준과 방법을 표준화하는 작업이 진행되고 있다. 국내에서도 이에 발맞추어 2020년 정보통신망법이 개정되면서 네트워크에 연결된 ICT 융합기기를 '정보통신망 연결기기등'으로 새롭게 정의하고, 보안인증제도 근거를 마련하였다. 관련 국내외 동향을 살펴보고 국내 보안인증 제도를 구현하기 위한 구체적인 고려사항들을 정리해 인증수행체계, 인증등급, 인증마크, 인증수수료, 변경관리, 인증유효기간 등과 중장기적 발전방향을 제안하였다.

현행 IoT 보안인증은 한국인터넷진흥원이 IoT 보안인증기관 및 시험기관 역할을 수행하며, 현안사항 발생시 인증위원회를 구성하여 안건을 심의 수행하고 있다. 개선방향으로는 정책기관(과기정통부), 인증기관(한국인터넷진흥원), 지정요건을 충족하는 인증시험대행기관으로 구성하도록 하여 인증수요 증가에 대비하며, 다양한 산업분야의 IoT 보안인증을 시험평가할 수 있는 체계를 제안한다.

인증등급은 기기 유형 중심으로 인증기준을 개발하고, 인증등급은 기기의 하드웨어 성능 측면보다는 위험 등 보증수준을 고려하여 3등급으로 차등화하여 인증등급을 부여하는 것이 바람직하리라 판단된다.

인증서 유효기간은 현재와 같이 3년으로 한다. 다만, 변경·재인증, 사후관리의 내용을 통해 유효기간 내에라도 보안에 취약한 부분이 발생하는 경우 보완할 수 있도록 한다.

정보보호인증을 받은 자가 주요한 설계·기능을 변경하여 인증기준에 미달할 우려가 있는 경우에는 변경인증을 받도록 하고, 성질·형상의 동일성이 인정되는 경우 정보보호인증의 유효기간을 연장하도록 할 필요가 있다.

인증을 받은 이후에 보안 취약점이 발견되어 인증기준에 미달될 경우에는 보완을 요청할 수 있도록 하였다.

그동안 한국인터넷진흥원이 IoT 보안인증을 하는 경우에는 무료로 시험·인증서비스를 제공하였다. 민간 인증시험대행기관을 지정하게 되면 수수료가 발생하게 되며, 초기에는 IoT 보안인증 확산을 위해 수수료를 감면해주거나 예산을 지원하는 정책적 배려가 필요하리라 보여진다.

소비자들이 IoT 보안인증을 받은 제품인지를 인지할 수 있도록 인증마크를 개발하여 제품에 표시하고, 보안인증 등급을 확인할 수 있도록 하여야 한다.

또한, 소비자들에게 인증마크에 대한 홍보를 적극적으로 실시하여 IoT 보안인증 등급이 있는 제품을 구매할 수 있도록 유도하여야 한다.

중장기적으로 자가평가 도입, IoT 보안인증 받은 기기 · 설비 · 장비들에 대한 수출 지원을 위해 국외 국가 및 인증기관들과 인증기준 부합화 작업 등을 통해 상호인정 추진, 인증 활성화를 위한 GS인증 수준의 인센티브 도입 등이 필요하다.

참고문헌

[1] https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf

[2] https://www.idc.com/getdoc.jsp?containerId=prAP46 180120

[3] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[4] 이동혁, 박남제. "IoT 기기의 보안성 확보를 위한 제도적 개선방안," 정보보호학회논문지, 제27권, 제3호, pp. 607-615, 2017.

[5] 유우영, "IoT 보안에 대한 국내외 연구 동향 분석," 융합보안논문지, 제18권, 제1호, pp. 61-67, 2018.

[6] 이동혁, 박남제, "IoT 제품 보안 인증 및 보안성 유지 관리방안," 한국통신학회지(정보와통신), 제33권, 제12호, pp. 28-34, 2016.

[7] 고재용, 이상길, 김진우, 이철훈. "IoT 보안 요구사항 및 보안 운영체제 기반 기술 분석," 한국콘텐츠학회논문지, 제18권, 제4호, pp. 164-177. 2018.

[8] 강다연, 황종호. "IoT 보안인증서비스 인증기준 중요도 우선순위에 관한 연구," 한국콘텐츠학회논문지, 제19권, 제7호, pp. 13-21, 2019.

[9] https://www.congress.gov/116/plaws/publ207/PLAW-116publ207.pdf

[10] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327

[11] https://olis.leg.state.or.us/liz/2019R1/Downloads/MeasureDocument/HB2395/Enrolled

[12] https://ims.ul.com/iot-security-what-does-reasonable-security-look

[13] https://www.nist.gov/blogs/cybersecurity-insights/rounding-your-iot-security-requirements-draft-nist-guidance-federal

[14] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-213-draft.pdf

[15] https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf

[16] https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf

[17] https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259B-draft.pdf

[18] https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259C-draft.pdf

[19] https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259D-draft.pdf

[20] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

[21] https://www.enisa.europa.eu/topics/standards/Public-Consultations/public-consultations-cybersecurity-schemes

[22] https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

[23] https://korea.ul.com/news/보도자료_ul-cap-사이버보안평가

[24] https://www.cybersecuritysummit.org/wp-content/uploads/2017/10/4.00-Justin-Heyl.pdf

[25] https://www.sans.org/summit-archives/file/summit-archive-1521575758.pdf

[26] https://productiq.ulprospector.com/en

[27] https://tietoturvamerkki.fi/en/products/

[28] https://www.csa.gov.sg/-/media/csa/documents/sccs/cybersecurity_certification_guide_v2.pdf

[29] https://www.kisa.or.kr/public/laws/laws3.jsp

[30] 박남제, 정원석, 한동국, 방지호, 김범준, 박애선, 이동혁, 김호영, 권지영, 지재덕, 조영진. 'IoT 제품 보안인증 및 보안성 유지관리정책 추진방안 연구'. 한국인터넷진흥원, 2016

[31] https://www.ksecurity.or.kr/user/bbs/kisis/66/312/bbsDataView/10176.do?page=2&column=&search=&searchSDate=&searchEDate=&bbsDataCategory=

[32] 한국인터넷진흥원, '사물인터넷(IoT) 보안 시험·인증 기준 해설서 [Lite]', 2019.

[33] 한국인터넷진흥원, '사물인터넷(IoT) 보안 시험·인증 기준 해설서 [Basic]', 2019.

[34] 한국인터넷진흥원, '사물인터넷(IoT) 보안 시험·인증 기준 해설서 [Standard]', 2019.

[35] https://www.law.go.kr

〔저자소개〕

이 용 필 (Yongpil Lee)
1995년 8월 서울대학교 경제학과 학사
2003년 8월 서울대학교 행정대학원 석사
2016년 2월 서울대학교 행정대학원 박사
2003년 8월 ~ 한국인터넷진흥원
email : pals@kisa.or.kr

서 영 진 (YungJin Suh)
1998년 2월 명지대학교 컴퓨터공학과 학사
2000년 2월 광주과학기술원 정보통신공학 석사
2001년 10월 ~ 한국인터넷진흥원
email : suhyj@kisa.or.kr,

이 상 걸 (SangGeol Lee)
2008년 2월 충주대학교 컴퓨터공학과 학사
2011년 8월 숭실대학교 정보보안학과 석사
2011년 8월 ~ 한국인터넷진흥원
email : leesg@kisa.or.kr