IoT 보안인증 점검 기준 및 국내 인증 동향

지승구 _ 한국인터넷진흥원 융합보안지원팀장

1. 머리말

사물인터넷(IoT, Internet of Thing)이란, 실세계와 가상세계에 존재하는 사람, 사물, 프로세스, 데이터 등 모든 것(Everything)들이 인터넷으로 상호 연결되어 서로 소통하고 작용하는 지능형 서비스 인프라이다.

IoT는 가트너(Gartner)가 선정하는 10대 전략기술에 2012년부터 매년 선정되고 있고, 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 IoT 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 IoT가 실제 생활영역에 적용되면서 다양한 경제적 가치와 더불어 효율성 및 편의성이 한층 높아질 것으로 기대되고 있다.

IoT를 중심으로 한 초연결 사회에서 사이버 보안은 필수불가결한 요소이다. 홈카메라를 통한 프라이버시 침해, 스마트 의료·교통 분야에서 사이버 침해 사고를 통한 개인 생명의 위협, 기업의 경영·기술정보의 해킹 등 ICT융합 환경에서 사이버 보안의 중요성은 날로 증가하고 있다. IoT 보안은 기존 PC, 모바일기기 중심의 사이버 보안과 달리, 보호대상 범위, 대상 특성, 보안담당 주체, 보호방법 등에서 새로운 접근이 필요하다. 이전에는 보호 대상이 한정되었다면, IoT 시대에는 웨어러블 기기, 가전, 자동차, 의료기기 등 IoT에 연결된 모든 사물로 확대되고, 기존 고전력·고성능 장비에서 초경량·저전력·저성능의 사물로 대폭 확대된다. 보안 주체의 경우, 이전에는 ISP(Internet Service Provider), 보안업체, 이용자로 국한되었다면, IoT 시대에는 상기의 보안 주체 외에 제조업체까지 포함된다. 보호 방법에 있어서도 기존에 별도 보안장비를 사용하여 보호했다면, IoT 시대에는 수많은 보호 대상을 통제·관리하기 어렵기 때문에 표준화 기술 획득을 통한 기기 자체의 보안 기능을 확보하고, 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 IoT 보안 능력을 향상시킬 방안을 모색할 필요가 있다.

IoT 보안은 센서·기기, 통신·네트워크, 플랫폼, 응용서비스로 세분화하여 각각의 보안 대책은 물론 전체적인 관점에서 대응할 필요가 있다. IoT 기기 및 서비스는 설계 단계부터 보안 기법을 적용해야 하며, 사물 간 접속 및 정보 전송 시에도 인증 및 암호화 기술을 적용하고 원격 기기에 대한 지속적인 보안업데이트뿐만 아니라 개인정보보호를 위한 적극적인 보호 조치를 취하는 것은 IoT 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 마련하여 추진해야 한다.

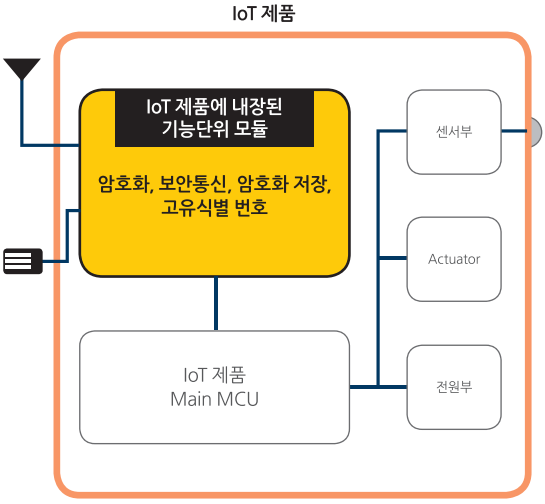
우리나라는 사이버 침해사고가 물리 사회로 전이·확산되는 것을 방지하고, 안전한 융합 ICT 인프라·서비스 환경 조성을 통해 국민이 편리한 스마트 생활을 영위할 수 있도록 힘쓰고 있다. 국내외 IP카메라, 도어락 등 IoT 제품에 대한 침해위협이 증가됨에 따라 IoT 제조사가 제품 개발단계부터 보안을 고려하여 출시할 수 있도록 민간 자율의 'IoT 보안인증 서비스'를 2017년 12월부터 실시했다. IoT 제품에 일정 수준의 보안이 갖추었는지 인증·암호·데이터보호·플랫폼보호·물리적보호 등 5개 영역에 대해 평가하여 기준 충족 시 인증서를 발급해주는 방식으로 운영 중이다. 한국인터넷진흥원은 기업의 부담 완화를 위해 IoT 보안인증서비스를 무료로 운영하고 있다. 'IoT 보안인증' 마크 취득은 해당 제품 및 서비스에 대한 소비자의 신뢰를 높이고, 기업(특히 중소기업)은 제품 및 서비스가 일정한 사이버 보안 수준을 갖추었음을 증명하여 제품경쟁력 제고에 도움이 된다.

과학기술정보통신부·기획재정부·산업통상자원부 등 정부는 2019년 4월 8일 5G+(플러스) 전략을 발표하면서 2023년까지 5세대(5G) 통신 관련 산업에 대한 투자가 민관 합계 30조 원을 넘어서고, 5G 기반의 혁신적 서비스업과 신제조업(장비·단말, 스마트 디바이스, 무인이동체) 육성으로 2026년까지 양질의 일자리 60만 개를 창출할 것으로 전망했다. 이처럼, 5G의 핵심 서비스(스마트공장, 자율주행차, 스마트시티, 디지털헬스케어, 실감콘텐츠)가 활성화되면서 그 기반기술인 IoT 보안인증과 관련된 수요는 점차 많아질 것으로 기대된다.

2. IoT 보안인증

2.1 IoT 보안인증 대상 및 등급

IoT 보안인증은 IoT 제품과 IoT 제품의 구성요소인 기능단위 모듈, IoT 제품 관리 등의 목적으로 IoT 제품과 연동하는 모바일 앱을 대상으로 한다.



[그림 1] IoT 제품 구성도

- **IoT 제품**: 네트워크 기반의 특정 서비스가 가능한 형태의 제품
- **모듈**: IoT 제품에 내장된 통신기능과 암호화 기능을 보유한 기능단위 모듈로, 모듈 단독으로 서비스 제공이 어려우며 다음과 같이 최소한의 보안기능이 내재되어야 함
  - 통신 모듈 내 제품의 고유 식별번호 보유
  - 알려진 프로토콜기반의 보안 통신 또는 암호화 통신 기능 내장
  - 중요 데이터 암호화 저장
  - 암호화키 암호화 저장
- **모바일 앱(App)**: 스마트폰 등 휴대용 단말기에서 설치되어 동작하는 소프트웨어

IoT 보안인증 등급은 IoT 제품(모듈 및 앱 포함)에 요구되는 보안기능 요구사항을 기반으로 LITE, BASIC, STANDARD와 같이 3개 등급으로 분류되며, 해당 등급의 보안기능 요구사항을 모두 만족하는 경우 해당 등급 기반의 인증서가 발급된다. 그리고 해당 등급의 보안요구사항과 추가적인 보안기능 요구사항을 만족하는 경우 해당 등급에 '+'가 표시된다.

IoT 제품은 〈표 1〉과 같이 LITE ~ STANDARD 등급, 모바일 앱은 BASIC 등급, 모듈은 LITE 등급을 기준으로 적용한다.

2.2 IoT 보안인증 절차

인증을 받고자 하는 신청인은 'IoT 제품 보안시험 신청서'와 제출물(인증대상 IoT 제품, 보안요구사항 준수명세서, 제품기능 설명서 등)을 한국인터넷진흥원(KISA)에 제출한다. 신청서 및 제출물에 이상이 없는 경우 시험신청 접수증이 발급되며, 시험일정 협의를 거쳐 계약을 체결한다. 계약 체결 후 제출문서 검토 및 보안기능 시험을 통해 기준 적합여부를 평가하며, 필요시 미흡한 항목에 대해 신청인에게 보완조치를 요청한다. 인증기준을 모두 만족할 경우 결과보고서 검토 후 인증서를 발급한다.

2.3 IoT 보안인증 점검기준

IoT 보안인증 점검기준은 LITE, BASIC, STANDARD 등급으로 구분되어 있으며 인증, 암호, 데이터 보호, 플랫폼 보호, 물리적 보호 등 5개 유형을 점검한다. STANDARD 등급의 경우 5개 유형의 총 41개 보안항목을 심사하며 IoT 제품만 적용가능

<표 1> IoT 보안인증 등급

등급	내용	평가항목	대상기기
Lite	제품 보안성 유지를 위한 최소한의 조치 항목	10개	센서 등 소형기기
Basic	해킹사례 등이 보고된 취약점 개선에 필요한 핵심조치 항목	23개	펌웨어 탑재한 중소형 기기
Standard	국제적인 요구수준의 종합적 보안조치 항목	41개	중대형 스마트가전 기기

[그림2] IoT 제품 보안인증 절차

<표 2> '인증' 관련 점검기준

[○: 필수적용, -: 적용대상 아님]

보안항목	보안인증 기준		적용대상	
			제품	앱/모듈
사용자 인증	AU1-1	처음 제품을 사용할 때 인증정보를 설정하도록 요구하거나, 초기 인증정보를 변경하도록 요구해야 한다.	○	-
	AU1-2	관리서비스 및 중요정보 접근 시 사용자 신원을 검증하기 위해 식별 및 인증이 선행되어야 한다.	○	-
	AU1-3	잘못된 인증정보를 통한 반복된 인증 시도를 제한해야 한다.	○	-
	AU1-4	제품의 초기 인증정보는 유일한 값으로 설정되어야 한다.	○	-
	AU1-5	제품에서 사용되는 사용자 계정 및 권한에 대한 관리 기능을 제공해야 한다.	○	-
	AU1-6	모든 사용자 계정에 대해 최소 권한의 원칙을 적용해야 한다.	○	-
	AU1-7	관리자 계정에 대해서는 동시 접속을 제한해야 한다.	○	-
	AU1-8	길이, 주기, 복잡성을 고려하여 안전한 비밀번호로 설정되도록 해야 한다.	○	-
인증정보의 안전한 사용	AU2-1	인증정보는 하드코딩되거나 평문으로 저장되지 않아야 한다.	○	-
	AU2-2	인증을 위한 비밀번호 입력 시 화면에 노출되지 않도록 마스킹 처리해야 한다.	○	-
	AU2-3	인증 실패 시 실패 사유에 대한 피드백 정보를 제공하지 않아야 한다.	○	-
제품 인증	AU3-1	하드웨어 제품은 각각의 고유 식별정보를 보유해야 한다.	○	-
	AU3-2	제품 간 중요정보 전송 시 혹은 제품 제어를 위한 상호연결 수행 시 상호인증이 선행되어야 한다.	○	-

<표 3> '암호' 관련 점검기준

[○: 필수적용, -: 적용대상 아님]

보안항목	보안인증 기준		적용대상	
			제품	앱/모듈
안전한 암호 알고리즘 사용	CR1-1	중요정보 전송 또는 저장 시 안전한 암호 알고리즘을 사용해야 한다.	○	-
안전한 키 관리	CR2-1	암호키는 안전성이 검증된 방법으로 생성·갱신·분배·사용·저장·파기 되어야 한다.	○	-
안전한 난수 생성	CR3-1	난수 생성 시 난수성이 검증된 알고리즘을 이용해야 한다.	○	-

하다. 유형별 보안인증 기준은 〈표 2〉부터 〈표 6〉에 상세히 기술하였다.

2.4 IoT 보안인증 국내현황

한국인터넷진흥원에서는 국민의 실생활과 밀접한 IoT 제품에 대해서 보안내재화를 촉진하고 안전성을 확보하기 위해 기본적 요건에 대한 기준을 마련하여 IoT 보안인증 서비스를 2017년 12월부터 시행하고 있다. IoT 보안인증 서비스는 산업 발전을 저해하지 않으면서 민간의 자율적 보안성 강화를 유도하기 위해 자율인증 방식으로 시행 중이다. 또한, 업계의 부담을 완화하기 위해 현재는 무료로 시행 중에 있다.

2019년 10월까지 국내에서 IoT 보안인증서를 취득한 제품은 〈표 7〉과 같이 총 19개이며, 등급별로는 10개 제품이 Basic 등급의 인증서를 받았고, 9개의 제품이 Lite 등급 인증서를 취득했다.

<표 4> '데이터 보호' 관련 점검기준

[○: 필수적용, -: 적용대상 아님]

보안항목	보안인증 기준		적용대상	
			제품	앱/모듈
전송 데이터 보호	DP1-1	제품 간 전송되는 중요정보는 암호화해야 한다.	○	-
	DP1-2	알려진 프로토콜 기반으로 통신채널 생성 시 안전한 보안 모드를 사용해야 한다.	○	-
저장 데이터 보호	DP2-1	제품에 저장되는 중요정보는 암호화해야 한다.	○	-
	DP2-2	사용자 필요에 의해 제품에 저장된 중요한 정보를 삭제한 경우, 복원이 어렵도록 해야 한다.	○	-
정보흐름통제	DP3-1	허가되지 않은 네트워크 트래픽 차단 기능을 제공해야 한다.	○	-
안전한 세션관리	DP4-1	세션 연결 후 일정 시간동안 미사용 시, 세션을 잠그거나 종료시켜야 한다.	○	-
	DP4-2	세션 ID는 예측할 수 없는 값이어야 한다.	○	-
개인정보 보호	DP5-1	제품에서 처리하는 개인정보는 비식별화 조치되어야 한다.	○	-

<표 5> '플랫폼 보호' 관련 점검기준

[○: 필수적용, -: 적용대상 아님]

보안항목	보안인증 기준		적용대상	
			제품	앱/모듈
소프트웨어 보안	PL1-1	보안약점이 존재하지 않도록 시큐어코딩을 적용해야 한다.	○	-
	PL1-2	알려진 보안취약점 존재여부를 확인하고 제거하여야 한다.	○	-
	PL1-3	소스코드 분석 방지를 위해 난독화를 적용해야 한다.	○	-
	PL1-4	주요 설정 값 및 실행코드에 대한 무결성 검증 기능을 지원해야 한다.	○	-
안전한 업데이트	PL2-1	업데이트 수행 전 인가된 사용자 여부를 확인해야 한다.	○	-
	PL2-2	업데이트 실패 시 롤백 기능을 지원해야 한다.	○	-
	PL2-3	업데이트 수행 전 무결성 검사를 수행해야 한다.	○	-
보안 관리	PL3-1	불필요한 서비스는 제거하거나 비활성화해야 한다.	○	-
	PL3-2	원격관리는 신뢰할 수 있는 환경에서 수행되어야 한다.	○	-
	PL3-3	3rd party 라이브러리 사용 시 최신 보안패치가 적용된 버전을 사용해야 한다.	○	-
	PL3-4	하드웨어 및 소프트웨어의 자체 시험 기능을 제공해야 한다.	○	-
감사기록	PL4-1	보안과 관련된 이벤트는 감사기록을 생성해야 한다.	○	-
	PL4-2	감사기록에 대한 보호 기능을 제공해야 한다.	○	-
타임스탬프	PL5-1	신뢰할 수 있는 타임스탬프 기능을 지원해야 한다.	○	-

<표 6> '물리적 보호' 관련 점검기준

[○: 필수적용, -: 적용대상 아님]

보안항목	보안인증 기준		적용대상	
			제품	앱/모듈
물리적 인터페이스 보호	PH1-1	외부 인터페이스는 비활성화 하되, 필요 시 접근통제 기능을 지원해야 한다.	○	-
	PH1-2	비인가자의 내부 포트 접근을 방지해야 한다.	○	-
무단조작 방어	PH2-2	비인가자의 무단 조작을 탐지하여 대응할 수 있는 기능을 지원해야 한다.	○	-

<표 7> 국내 IoT 보안인증서 취득제품

[2019. 10월]

No.	구분	제품	등급
1	기기	IoT 센서노드(m2sn002)	Basic
2	기기	실내 공기질 측정기	Basic
3	기기	공기질측정 스마트센서	Basic
4	기기	Smart IoT 침수 감지 단말기	Basic
5	앱	IoT@Home 앱	Lite
6	앱	하이브리드 전기보일러 앱	Basic
7	앱	HioT Smart Home 앱	Lite
8	기기	보행신호 음성안내 보조장치	Basic
9	앱	T-sign 앱	Basic
10	기기	전기자동차 충전 콘센트	Basic
11	기기	전기자동차 충전 전력분배 게이트웨이	Basic
12	기기	무선 온습도 센서	Lite
13	기기	스마트홈 월패드	Lite
14	기기	디지털도어록	Lite
15	앱	sHome 앱	Lite
16	기기	IoT 센서노드(m2sn003)	Lite
17	기기	NB-IoT 플러그	Lite
18	기기	스마트 GPS 리피터	Basic
19	앱	GIGA Genie 홈 IoT 앱	Lite

3. 맺음말

초연결 사회에서 IoT 보안에 문제가 발생하면 사회 혼란은 물론 사람의 생명까지 영향을 미칠 정도로 피해 속도 및 규모는 상상하기가 어렵다. IoT 보안에 대한 우려는 IoT 산업 성장을 저해하는 가장 큰 요인으로 작용한다. IoT 시스템 및 장비에 대한 보안인증은 시민의 생명과 재산 보호, IoT 산업의 성장을 위해서도 반드시 필요하다.

사물인터넷 기기 및 서비스는 설계 단계부터 보안 기법을 적용해야 하며 사물 간 접속 및 정보 전송 시에도 인증 및 암호화 기술을 적용하고 원격 기기에 대한 지속적인 보안업데이트뿐만 아니라 개인정보보호를 위한 적극적인 보호 조치를 취하는 것은 사물인터넷 보안을 위한 최소한의 요구 사항이라고 할 수 있다. 아울러 새로운 기기 및 서비스의 출현에 대비하여 새로운 보안기술과 기존 사이버 보안 기술의 적절한 조화를 통해 보안 방식 간의 혼돈을 최소화하면서 효율적으로 사물인터넷 보안 능력을 향상시킬 방안을 모색할 필요가 있다.

[참고문헌]

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