

보도시점 2025.9.9.(화) 12:00
(2025.9.10.(수) 조간)

배포 2025.9.9.(화) 09:00

국내 사물인터넷(IoT) 보안인증, 독일에서도 인정한다!

- 한국-독일 간 사물인터넷(IoT) 보안분야 상호인정약정(MRA) 체결 -
- 해외인증 부담 완화, 사이버 보안 무역장벽 극복 기반 마련 등 업계 환영 -

과학기술정보통신부(장관 배경훈, 이하 '과기정통부')와 한국인터넷진흥원(원장 이상중, 이하 'KISA')은 9월 8일(월) 독일 베를린에서 독일 연방정보기술보안청(BSI)의 정보기술 보안 라벨(IT Security Label, 이하 '독일 라벨')과 사물인터넷(IoT) 보안인증 제도의 상호인정약정(MRA)*을 체결했다고 밝혔다.

* 상호인정약정(MRA, Mutual Recognition Arrangement) : 유사한 인증제도를 운영하는 국가의 인증기관 간에 각국 인증(기준, 기술요건 등)의 동등성을 상호 인정하는 것

이번에 독일과 체결한 약정은 싱가포르('24.10월)에 이어 두 번째로 맺은 사물인터넷(IoT) 보안 분야 상호인정약정으로 아시아를 넘어 유럽까지 국제협력의 기반을 확대한 것이다.

상호인정의 대상은 일반적으로 가정 등에서 사용되는 로봇청소기, 지능형 냉장고(스마트냉장고), 지능형 텔레비전(스마트TV) 등 소비자용 사물인터넷(IoT) 제품이 대상으로, 국내 사물인터넷(IoT) 보안인증 중 베이직(Basic) 또는 스탠다드(Standard) 인증을 취득한 제품은 독일 라벨을 부여받을 수 있다. 또한, 반대로 독일 라벨을 취득한 제품은 기본적으로 우리나라의 라이트(Lite) 인증을 부여받을 수 있고, 국내 추가 요구사항을 충족할 경우에 한해 베이직(Basic) 인증을 받을 수 있다.

※ 한국 사물인터넷 보안인증 유형 : 라이트(Lite) → 베이직(Basic) → 스탠다드(Standard)

※ 독일 정보기술 보안 라벨(IT Security Label) : 단일유형으로 운영, 국내 라이트와 베이직 중간 수준

한국과 독일은 이번 행사를 통해 인증제품의 상호인정뿐만 아니라 표준 개발, 사물인터넷 분야 보안위협 정보 교환 및 모범 사례 확산 등 다양한 분야에서 협력을 강화하기로 합의했다.

특히, 최근 들어 유럽은 사물인터넷(IoT)을 비롯한 디지털제품 전반에 대한 사이버보안의 중요성을 강조하며 관련 규제도 강화해 나가는 추세로, 이번 독일과의 협력으로 사물인터넷(IoT) 제품의 보안성 제고는 물론 우리나라 기업의 유럽 시장진출에도 도움이 될 것으로 기대된다.

관련 산·학·연과의 논의에서도, 이번 약정을 통해 기업들이 유럽내 대표적 제조강국인 독일 라벨을 획득하는 과정에서 언어, 시간, 비용 등의 부담을 완화할 수 있고, 독일을 시작으로 한-유럽연합간 향후 협력 발판을 다진다는 측면에서 매우 긍정적인 반응을 보였다.

과기정통부와 한국인터넷진흥원(KISA)은 이번 독일과의 협력을 토대로 다른 국가들과의 상호인정약정 확대를 지속적으로 추진하는 등 사물인터넷(IoT) 보안인증의 활용도와 신인도를 제고하여 국민에게는 안전한 디지털 이용환경 조성을, 기업에게는 제품 보안이라는 간접적 수출장벽 극복 기반을 마련하는데 힘을 쏟을 예정이다.

한편, 이날 상호인정약정 체결식 이후 국내 사물인터넷(IoT) 보안인증을 획득한 삼성전자의 로봇청소기와 지능형 냉장고(스마트냉장고)에 독일 라벨을 부여하고, 독일 라벨을 취득한 AXIS사의 스피커 2개에 우리나라의 라이트 인증을 부여하여 상호인정의 의미가 더욱 강조되었다.

과기정통부 최우혁 정보보호네트워크정책관은 “이번 상호인정약정은 국내 사물인터넷(IoT) 보안인증을 받은 제품의 우수성과 안전성을 국제적으로 인정받을 수 있는 좋은 계기를 마련하는 것”이라며, “국민과 기업 모두에게 도움이 될 수 있도록 사물인터넷(IoT) 보안 관련 국제협력을 지속적으로 지원하겠다”고 밝혔다.

담당 부서	네트워크정책실 정보보호산업과	책임자	과 장	최영선 (044-202-6450)
		담당자	사무관	김소완 (044-202-6451)
관련 기관	한국인터넷진흥원(KISA) 디지털제품인증팀	책임자	팀 장	최윤선 (02-405-5130)
		담당자	주임연구원	박수현 (02-405-5135)

붙임

IoT 보안인증제도 현황

□ 개 요

- 「정보통신망법(제48조의6)」에 근거, IoT 기업들이 자율적으로 신청할 수 있는 임의인증으로 'IoT 보안인증' 운영

□ 현 황

- 정보통신망법 개정(제48조의6, '21.9월)을 통해 IoT 제조기업들이 자율적으로 신청하여 인증을 받을 수 있도록 운영 중
- IoT 사용 비중이 높은 가전, 주택 등 8개 분야를 인증대상으로 규정, TTA·KTC·KTR을 공인시험기관으로 정하고, KISA에서 인증서 발급

인증대상	가전, 교통, 스마트도시, 의료, 제조 및 생산, 주택, 통신 등(8개 분야)
인증기준	식별·인증(초기 PW 변경 등 6개 항목), 데이터보호(중요정보 저장시 암호화 등 5개 항목), 암호(안전한 암호 알고리즘 사용 등 4개 항목), SW보안(알려진 취약점 조치 등 7개 항목), 업데이트(자동업데이트 등 7개 항목), 네트워크보안(원격접속 통제 등 12개 항목), HW보안(인터페이스 보호 등 9개 항목) 등 총 7개 영역 50개 항목

- 대상기기 및 보안요구 조건(개인정보 취급 여부) 등에 따라 '라이트', '베이직', '스탠다드'로 구분하여 운영 중

< IoT 보안인증 종류 및 보안 요구수준 >

구분	보안 요구수준	평가 항목	실적*	예시
라이트 (Lite)	단순 해킹공격에 대응할 수 있는 필수 보안조치 수준 (개인정보 수집·저장·전송 등 취급시 라이트 신청 불가)	10	239	도어락, 센서 등
베이직 (Basic)	중요정보의 불법적인 접근을 차단하고 노출방지에 대응할 수 있는 일반적인 보안조치 수준	29	219	월패드 등
스탠다드 (Standard)	고도의 해킹공격에 대응할 수 있고 국제적인 요 구사항을 포함한 종합적 보안조치 수준	43	7	스마트 가전 등

* '25.8월 말 기준