글로벌 IoT 보안 인증프로그램 개발 동향

장재민, 양준, 유지원
한국정보통신기술협회
jaemin1002@tta.or.kr, rickyu@tta.or.kr

Trends in Global IoT Security Certification Program Development

Jang Jae Min, Yang June, Yu Ji Won
Telecommunications Technology Association

요 약

GCF와 IMC는 IoT 기기, 네트워크, 클라우드/애플리케이션을 포괄하는 글로벌 보안 인증 프로그램 개발 가능성을 조사하기 위해 공동 태스크포스(JTF)를 구성하였다. 강화되는 규제 환경과 산업계의 요구에 대응하여 JTF는 기술적 요소, 비즈니스 모델, 인증 절차라는 세 가지 트랙을 중심으로 논의를 진행하고 있으며, 2025년 하반기를 목표로 인증 체계 수립 및 권고안 도출을 추진 중이다. 본 논문에서는 각 트랙별 주요 논의 내용을 중심으로 IoT 보안 인증 프로그램 개발의 방향성과 실행 가능성을 분석한다

Ⅰ. 서론

사물인터넷(IoT)의 급격한 확산은 다양한 산업 분야에 혁신을 가져왔지만, 그에 따른 보안 위협도 빠르게 증가하고 있다. 특히 기기 해킹, 데이터 유출, 서비스 마비와 같은 보안 사고가 현실화되면서, IoT 보안은 선택이 아닌 필수 과제로 인식되고 있다. 그러나 현재까지 글로벌하게 통용되는 통합적 보안 인증 체계가 부재한 상황이며, 산업계는 각기 다른 국가별 규제와 산업별 기준에 대응하는 데 많은 어려움을 겪고 있다. 이러한 한계를 극복하고자 GCF(Global Certification Forum)와 IMC(IoT M2M Council)는 2025년 공동 태스크포스(Joint Task Force, JTF)를 구성하였다.

JTF는 IoT 스택 전 계층(디바이스, 네트워크, 클라우드/애플리케이션)을 포괄하는 새로운 보안 인증·인가 프로그램 개발을 목표로 하며, 기존 보안 표준들이 단편적이고 기기 중심에만 머무르고 있다는 문제의식에서 출발했다. 이를 해결하기 위해 JTF는 기술적 타당성, 인증 절차 및 기준 개발, 지속 가능한 사업 모델이라는 세 가지 트랙을 중심으로 논의를 전개하고 있다. 각 트랙은 다양한 산업군의 사용 사례, 보안 위협 수준, 연결 기술 등을 분석하며 실질적인 요구사항을 도출하고 있으며, 기존 표준(NIST, ETSI, ISO) 및 규제(CRA, NIS2 등)와의 연계 가능성도 함께 검토하고 있다.

한편, 최근 강화되는 글로벌 보안 규제는 보안을 설계 초기부터 반영하고 지속적으로 유지·관리할 것을 요구하고 있다. 이에 따라 소프트웨어 업데이트, 취약점 대응, 모니터링 등도 인증 과정에서 중요한 요소로 다뤄지고 있다. 자동차, 제조, 에너지 등 주요 산업 분야에서는 이러한 규제 대응을 위해 보안 인증 수요가 빠르게 증가하고 있으며, JTF는 산업계의 현실적인 요구를 반영한 실용적인 인증 체계 구축에 주력하고 있다.

본 논문에서는 JTF가 운영 중인 세 가지 하위 트랙을 중심으로, IoT 보안 인증 프로그램 개발 과정의 주요 내용을 정리한다. 각 트랙에서 논의된 기술적 요소, 규제 대응 전략, 산업계 요구사항 반영 방안 등을 종합적으로 분석함으로써, JTF가 지향하는 보안 인증 체계의 실질성과 실행 가능성을 살펴보고자 한다.

Ⅱ. 본론

IoT 보안 인증 프로그램의 개발을 위해 구성된 JTF는 체계적이고 효율적인 논의를 위해 세 가지 주요 트랙으로 활동을 구분하였다. 이들 트랙은 각각 기술적 타당성 검토(Track 1), 비즈니스 모델 개발(Track 2), 인증 체계 및 운영 프로세스 설계(Track 3)에 집중하며, IoT 생태계 전반을 포괄하면서 실질적인 보안 인증 프레임워크 수립을 목표로 하고 있다. 각 트랙은 개별적으로 특정한 과제를 다루지만, 상호 연계된 구조를 통해 종합적인 인증 프로그램을 완성하는데 기여하고 있다.

Ⅱ-1. Track 1: Technical Scoping

IoT 보안 인증의 기술적 타당성을 다각도로 분석하는데 중점을 두고 무선 기술과 운영체제에 구애받지 않는 포괄적 접근 방식을 채택하여, 소비자용 및 기업용 IoT 기기를 모두 고려한 기술 검토를 진행하고 있다. 검토 범위는 연결 기술, 기기 복잡성, 엣지 컴퓨팅 환경, 취약점 평가 등 기기 계층부터, 데이터 전송 기술, 인코딩 프로토콜, 네트워크 정책 등 네트워크 계층, 그리고 클라우드 플랫폼, 보안 표준, AI 기반 서비스가 포함된 상위 계층까지 IoT 스택 전반에 걸쳐 있다. 특히 헬스케어, 커넥티드 카와 같은 주요 산업 분야를 중심으로 침해 영향에 따른 보안 요구사항을 구체화하고 있으며, 미국 및 EU 외 지역의 규제 목록을 보완하여 글로벌 적용 가능성을 검토 중이다. 현재는 기존 표준 및 규제 간의 차이점을 비교하고, 산업별 우선순위 및 사용 사례에 따라 타당성 평가를 추진하고 있으며, 2025년 8월 중순경 주요 결과를 도출할 예정이다.

Ⅱ-2. Track 2: Business Development & Modelling

인증 프로그램이 현실적이고 지속 가능한 구조를 갖추기 위한 기반을 마련하는데 초점을 맞추어 시장 기회, 산업 분야별 기기 보급률과 보안 성숙도, 규제 대응 시점 등을 고려하여 주요 시장을 선정하고, 인증 수익 구조(연회비, 인증 건당 수수료 등)와 운영 비용 구조(테스트 인프라, 전문 인력 확보 등)를 분석하고 있다. Gartner 및 IMC에서 제공하는 시장 데이터를 바탕으로, 초기 논의에서는 계량기 분야가 상대적으로 보안 준비도가 높고 인증 도입 가능성이 크다고 판단되었으며, 의료기기 역시 우선순

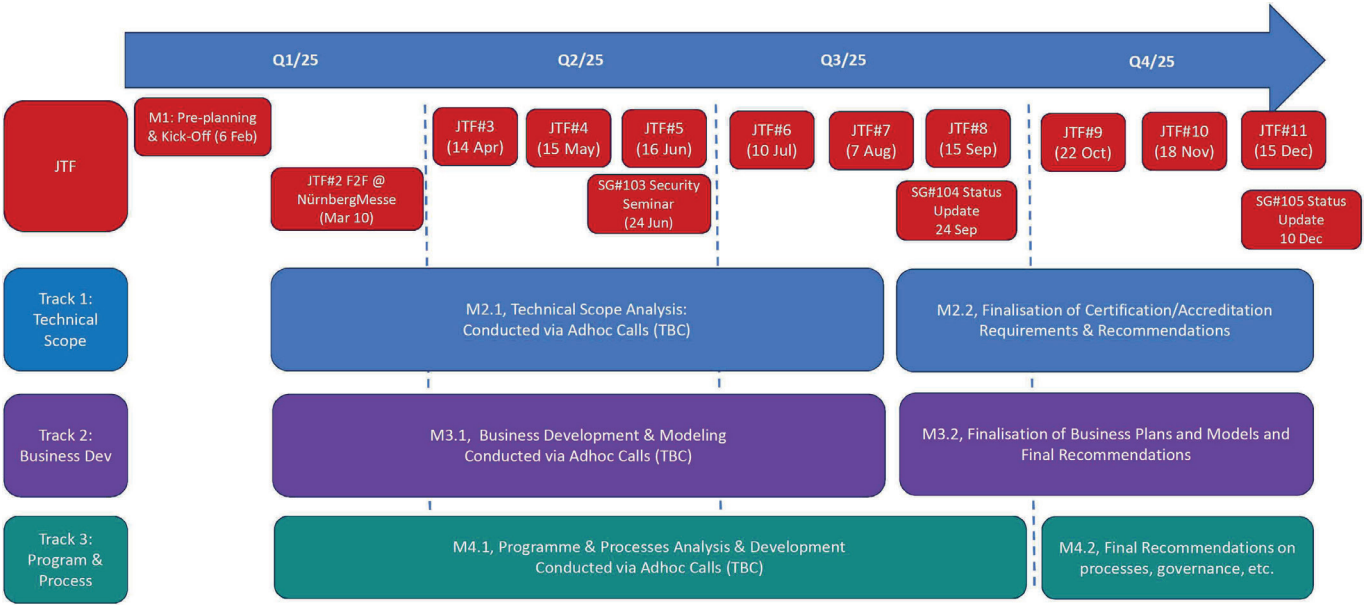

그림 1. GCF-IMC JTF 트랙별 로드맵

위 후보로 고려되고 있다. 반면 커넥티드 카는 기술적 복잡성과 규제 요건의 다양성으로 인해 중장기 과제로 분류되었다. 인증 가격 정책은 대기업, 중소기업, 스타트업 등 다양한 규모의 기업군을 고려한 차등 적용 방안이 논의되었고, Cyber Resilience Act(CRA)와 같은 주요 규제를 중심으로 시장 수요 예측 및 전략 수립이 병행되고 있다. 향후에는 테스트 산업과의 협력 구조 및 마케팅 전략에 대한 보다 구체적인 계획이 마련될 예정이다.

Ⅱ-3. Track 3: Programme & Process Development

인증 체계의 설계와 실행 절차를 구체화하는데 주력하여 앞선 두 트랙의 결과물을 기반으로 인증 구조를 설계하며, 기기 특성 및 시장 특성에 따라 다양한 인증 등급을 구분하는 다층적 모델을 도입하고자 한다. 예를 들어, 침해 영향이 미미한 기기에는 기업 자체 선언(Self-Declaration) 방식의 인증을 적용하고, 일정 수준 이상의 위험성을 지닌 기기에 대해서는 제3자 테스트 또는 승인된 인증기관의 평가를 요구하는 구조다. 이에 따라 제품 수준 및 기업 수준의 감사 절차(Device & Company Audit)도 포함되어 있으며, 인증의 신뢰성과 정합성을 확보하기 위해 GCF의 기존 프로세스를 참조하고 있다. 또한 기존 인증 체계와의 비교 및 분석을 통해 중복 테스트를 최소화하고, 국제적인 상호 인정이 가능한 구조를 설계하는 것을 목표로 하고 있다. 실질적인 프로세스 설계 작업은 6월부터 본격적으로 진행되며, 이를 위해 각 세부 과제별 책임자와 협력 인원의 참여가 확대되고 있다.

이처럼 JTF는 각 트랙별로 구체적인 목표와 활동을 바탕으로 IoT 보안 인증 프로그램의 토대를 마련하고 있으며, 트랙 간의 유기적인 협업을 통해 2025년 말까지 실행 가능한 권고안을 도출하는 것을 목표로 하고 있다.

Ⅲ. 결론

JTF는 강화되는 글로벌 보안 규제에 선제적으로 대응하고, 산업계의 실질적인 보안 문제를 해결하며, 신뢰할 수 있는 IoT 생태계 조성을 목표로 하고 있다. 현재까지의 논의를 통해 IoT 보안 인증 개발은 다음의 방향성을 기반으로 진행되고 있음이 확인되었다: (1) 통합적 보안 인증 프레임워크 수립, (2) 산업별 규제 대응 전략 마련, (3) 산업계의 요구사항 반영, (4) 기존 인증 체계와의 연계, (5) 지속 가능한 사업 모델 정립.

JTF는 2025년 12월까지 인증 프로그램 구축 여부에 대한 권고안을 마련할 계획이며, 각 트랙의 논의 결과가 유기적으로 반영될 예정이다. 향후 실행계획 수립과 함께 산업계의 지속적인 관심과 참여가 중요하며, 이러한 활동은 글로벌 IoT 보안 인증 체계의 신뢰성과 실효성을 제고하는 데 기여할 것으로 기대된다.

참 고 문 헌

[1] GCF-IMC IoT Security, Documents, (https://gcf-imc.globalcertificationforum.org/)

표 1. GCF-IMC JTF 트랙별 주요 항목 요점 정리

항목	Track1	Track2	Track3
목표	인증 기술의 실현 가능성 평가	인증 프로그램의 수익성 및 지속 가능성 확보	인증 체계 및 절차 설계와 운영 모델 수립
논의영역	IoT 스택 전반 (기기, 네트워크, 클라우드, …)	수익 구조, 비용 구조, 시장 전략, 이해관계자 분석	인증 모델, 평가 기준, 감사 절차, 기존 체계 연계
논의초점	기술 요소의 인증 가능성 판단 및 우선순위 설정	산업별 기회 분석, 가격 모델 개발, ROI 확보	인증 등급 구분, 평가 방법론 설계, 글로벌 정합성 확보
활용데이터	기술 표준, 산업별 사례, 글로벌 규제	시장 예측 자료, 산업 기기 현황	Track 1, 2 결과, 기존 인증/표준 체계