# [RFID/USN] 수동형 RFID 기술의 새로운 도전! 보안 서비스와 파일 관리

수동형 RFID 기술의 새로운 도전 과제로 떠오른 보안 서비스와 파일 관리를 위한 에어 인터페이스 표준화 논의가 가속화되고 있으며, 그 중심에는 ISO/IEC JTC 1/SC 31/WG 7 (이하 WG7)이 자리잡고 있다.

2009년 6월에 호주 시드니에서 개최된 WG7 회의에서는 기존의 보안 요구사항 정의 수준을 넘어 기술적 해결책을 표준화하기 위한 발걸음이 시작되었다. 개별 정보를 가지는 RFID 태그의 메모리 맵 관리 및 파일에 대한 접근 제어를 비롯한 데이터 보호 서비스를 제공하기 위해 기술적 논의를 본격화되면서 RFID 보안 기술의 국제표준화는 RFID 산업계 전반에 주요 이슈가 되고 있다.

## ISO/IEC 29167 표준화 현황

RFID 보안 서비스와 파일 관리를 위한 에어 인터페이스 표준은 오스트리아의 신규작업화(NWIP: New Work Item Proposal) 제안 직후 2008년 7월 11일부터 2008년 10월 8일까지 약 3개월의 NWIP 국가투표 후에 통과되어 ISO/IEC 29167 문서번호를 부여 받고 표준화가 시작되었다. 현재는 작업 초안(WD: Working Draft)이 작성되고 있으며, 오스트리아 에디터와 한국 ETRI의 코에디터가 WD 문서화 작업에 참여하고 있다.

ISO/IEC 29167 표준문서의 공식 제목은 영문으로 “Air interface for file management and security services for RFID”이다. 이 표준은 RFID 태그가 비교적 충분한 사용자 메모리(예를 들면, 수 K ~ 수십 K 바이트)를 가지고 있는 경우를 고려하여 효율적인 파일 관리와 보안 서비스를 제공하는 것을 목적으로 하고 있다.

표준화 범위는 (1) 사용자 메모리에 대한 파일 관리, (2) 사용자 메모리에 대한 보안 접근 방법, 그리고 (3) 비인가 읽기에 대한 UII(Unique Item Identification) 보호 기술로 명시되어 있다. 또한 호환되는 에어 인터페이스는 ISO/IEC 18000 시리즈로 한정시키고 있다. 즉, ISO/IEC 18000 시리즈가 정의된 형태에 따라 각 주파수 대역별로 구분하여 각 주파수 특성과 변복조 방식에 최적화된 보안 기술을 정의하고자 하였다.

최초 의도는 주요 이슈가 되고 있는 UHF 대역의 수동형 RFID 기술인 ISO/IEC 18000-6 타입 C에 대한 파일 관리와 보안 기술을 정의하면서 문서의 완성도를 높이려고 했으나, 지난 2월 미국 플로리다 보카라톤에서 열린 회의에서 각 주파수별로(예를 들면, 13.56 MHz, 2.4 GHz, 860~960 MHz, 433 MHz 등) 파트를 분할하기로 결정했고 이번 시드니 회의에서는 파트 분할을 공지하였다. 이에 따라 각 파트별로 에디터 선정이 필요하게 되었으며 차기 회의인 8월 런던 회의에서는 보안 기술 중심으로 각 파트별 문서를 책임질 에디터를 선정할 것으로 보인다.

ISO/IEC 29167 표준화에 있어, 이번 WG7 시드니 회의의 주요 논쟁 중 하나는 보안 기술

표준화를 반드시 별도의 보안 모듈(crypto engine)을 가진 경우로 제한할 것인지 아니면 비교적 단순한 기법으로 암호화 연산 없는 낮은 수준의 보안 서비스 제공을 포함시킬 것인지에 대한 논의였다. 일반적인 디지털 통신 기기에서는 다양한 보안 서비스 제공을 포함하는 것이 필요하겠지만 저가의 수동형 RFID 태그에서는 현재의 기술수준에서 구현 가능한 보안 모듈 활용 방법을 정의하여 높은 보안성을 제공하는 것이 필요하다는 의견도 있었지만, 대부분의 의견은 일단 다양한 선택사항을 마련하는 방향으로 보안 기술 표준화가 추진되기를 희망하는 것이었다.

**향후 전망과 국내 대응전략**

RFID 보안 기술 표준화가 ISO/IEC 18000 시리즈에 대응되는 방향으로 진행되는 것은 이미 충분히 예견되었던 사항이며, 국내의 기술력으로도 주요 표준인 ISO/IEC 18000-6 보안 기술 및 18000-7 보안 기술 표준화에 핵심적인 기술사항을 기여할 수 있을 것으로 보인다.

그러나, 유념해야 할 것 중의 하나가 여러 국가 또는 여러 기업의 의견이 충돌한다고 해서 단순한 보안 요구사항 수준으로 표준화를 끝내서는 안 된다는 것이다. ISO/IEC 24791-6 RFID Software System Infrastructure 보안 기술 표준문서는 기술적 해결방안이 없이 보안 요구사항 정의만을 포함하여 표준화를 추진하다가 결국 기술적 의미가 없다는 이유로 표준화 추진 철회를 결정한 사례도 있다.

따라서, 지금부터 시작되는 표준화 논의에서는 우수한 성능을 가지는 선진적 보안 기법들이 표준화 회의에서 논의될 것으로 보이며, 다양한 토론과 논쟁을 통해 표준으로 제정될 것을 판단된다. 국내 RFID 보안 기술도 이러한 논의에 적극적으로 참여하여 경합과 기여를 통해 표준으로 포함되기를 기대해 본다.

강유성 (한국전자통신연구원 지식정보보호연구팀 선임연구원, youskang@etri.re.kr)