

[정보보호] 전자봉인은 컨테이너 잠금(Lock)/풀림(Unlock) 정보를 보호해야 한다.

이-씰(eSeal: Electronic Seal)이라 불리는 전자봉인은 능동형 RFID(Radio Frequency Identification) 기술의 대표적인 응용으로써, 항만물류 시스템에서 사용되는 화물 컨테이너의 문이 비정상적인 형태로 개폐됨을 감지하거나 또는 비정상적인 개폐의 시도를 감지하여 주변의 리더에게 알리고 그 이력을 유지하는 역할을 한다.

미국 워싱턴DC에서 개최된 제 20차 ISO TC104 SC4 WG2 회의(2006.10.18-10.20)에서는 전자봉인의 통신프로토콜 규격(ISO 18185-1)과 물리계층 규격(ISO 18185-7)이 최종국제표준초안(FDIS: Final Draft International Standard) 승인을 얻은 발간 작업을 위해 ISO TC104 SC4 간사에게 전달할 것이 결의되었다. 이로써 통신을 위한 표준규격은 마무리 단계로 접어든 것이다. 그러나 이러한 기본적인 통신규격과 더불어 전자봉인 상용화의 중요한 이슈는 전자봉인이 가지고 있는 컨테이너 잠금(Lock) 및 풀림(Unlock)과 관련된 이벤트 정보의 보호가 필요하다는 것이다. 이번 회의에서 한국전자통신연구원 정보보호연구단에서는 전자봉인 보안 프로토콜(ePP: eSeal Protection Protocol)의 구현 결과와 실제 운영 가능성을 소개하였다. 본 고에서는 이번 회의에서 결정된 ISO 18185 문서들의 현재 진행단계를 요약하고, 전자봉인 활성화를 위한 주요 이슈의 분석과 향후 전망을 논한다.

전자봉인(eSeal) 표준화 현황

ISO 18185 전자봉인 규격 중 통신프로토콜 규격(ISO 18185-1)은 최종국제표준초안(FDIS: Final Draft International Standard) 승인을 얻었고, 응용 요구사항 규격(ISO 18185-2)은 ISO 기술위원회의 최종 발간을 기다리고 있다. 전자봉인 사용 환경의 특성을 정의한 규격인 ISO 18185-3 역시 ISO 기술위원회의 최종 발간을 기다리고 있으며, 전자봉인 데이터 보호 규격(ISO 18185-4 Gen1)은 국제표준초안(DIS: Draft International Standard)에 대한 의견접수를 마치고 최종국제표준초안(FDIS) 찬반 투표를 진행하기로 되어 있다. 그리고 ISO 18185-6 규격번호로 진행했던 리더와 호스트 컴퓨터 사이의 메시지 형식 규격은 이번 회의에서 표준화 진행을 철회하기로 결정하였고, 전자봉인의 실제 운영 시 필요하다면 UN/EDIFACT 규격의 데이터와 메시지 형식을 활용할 것을 권고하였다. 또한 물리계층 규격(ISO 18185-7)은 최종국제표준초안(FDIS: Final Draft International Standard) 승인을 얻어 발간 작업을 준비 중이다.

전자봉인 활성화의 주요 이슈 - 잠금/풀림 정보의 보호

전자봉인 데이터 보호 규격(ISO 18185-4 Gen1)의 현재 상황은 구체적인 기술적 논의를 배제한 채 일반적인 보안 요구사항만을 나열하고 있는 상태이다. 한국전자통신연구원 정보보호연구단의 연구진은 지난 2005년부터 전자봉인 데이터 보호 기술을 개발하고, 이를 바탕으로 ISO 18185-4 Gen2 표준화에 기술적 기여를 하기 위하여 전자봉인 보안 프로토콜을

구현하고 이의 표준화를 추진해 오고 있다. 그 결과 지난 2006년 5월에 미국 산호세에서 개최된 제 19차 회의에서 전자봉인 보안 프로토콜 기술 발표를 하였다. 그러나, 마스터 키 분배가 정의되어 있지 않아서 실제 운용이 불가능하다는 지적이 제기되었고, 이에 한국전자통신연구원 연구진은 마스터 키 분배 문제를 해결할 수 있는 기술적 해결책을 제시하기 위하여 이번 회의에서 발표시간을 얻어서 첫째 날(10월 18일 수) 오후 세션에 대략 20여분 동안 마스터 키 분배 기술 및 구현 결과를 소개하고, 실제 운용이 가능함을 밝혔다.

발표 직후, 주요 코멘트는 크게 3개로 요약되었다. 첫째는 우호적인 코멘트로서 신규 작업화가 필요하다는 의견이고, 둘째는 기술적인 반대 의견이라기 보다 근본적인 전자봉인 역할에 대한 문제 제기로서 전자봉인은 기계적 구조의 봉인장치를 전자장치로 전환하는 것이므로, 전자봉인에는 보호해야 할 데이터가 포함되지 않을 것이라는 주장이고, 셋째는 인터넷이 없는 환경에서는 마스터 키 분배가 어려워 보인다는 인프라 구축과 관련된 의견이었다.

전자봉인의 근본적인 역할인 컨테이너 개폐 진위에 대한 원격 확인을 위해서는 잠금(Lock) 또는 풀림(Unlock) 이벤트를 보호해야 할 정보로 정의할 수 있다. 즉, 언제 열리고 닫혔는지를 아무나 알 수 있다면 악의적인 공격자가 그 정보를 읽은 후에 컨테이너 문을 열고 물건을 바꿔치기 한 후에 다시 동일한 정보를 가진 새로운 전자봉인으로 컨테이너 문을 잠그면 도착지에서는 여전히 이전의 잠금 정보만을 읽게 되므로 이는 보안상 취약점이 된다. 따라서, 전자봉인에 보호해야 할 데이터가 없다는 것은 설득력있는 주장이 아니다. 또한 인터넷 인프라가 없는 상황은 현재의 물류 프로세스에서도 큰 문제가 되는 상황이다. 즉, 어느 국가든지 외국 선박의 입항 전에는 화물 컨테이너의 적하목록을 미리 전송받아야 하며, 이는 인터넷을 이용한 통신을 통해 수행되고 있는 작업이다. 따라서, 마스터 키 분배가 이미 활용 중인 인터넷을 통한 전자문서(EDI) 전송을 사용하도록 정의되어 있으므로 인터넷 인프라가 문제가 될 경우 이는 마스터 키 분배뿐만 아니라 적하목록 자체를 확인할 수 없는 더욱 심각한 상황이 되는 것이다. 따라서, 인터넷 인프라의 문제를 마스터 키 분배 문제로 연결시키는 것은 설득력이 없다고 볼 수 있다.

향후 전망과 국내 대응전략

전자봉인 규격은 이미 많은 부분 표준화가 진행되어 있으며, 일부 표준화 위원들은 데이터 보호의 필요성에 동의하지 않는 상황이 전개되고 있다. 그러나, 실제 운용 시 반드시 전자봉인 내부의 잠금(Lock)/풀림(Unlock) 이벤트에 대한 보호가 필요할 뿐만 아니라, 정부기관 또는 각 기업별로 고유의 정보를 비밀리에 전달하고자 한다면 데이터 보호 기법이 반드시 필요할 것이다. 따라서, 다양한 국적과 다양한 소속을 가진 표준화 위원들이 공통적으로 전자봉인 데이터 보호의 필요성을 인지할 수 있도록 데이터 보호 필요성을 정리하여 표준화 위원들을 설득하는 작업을 선행한 후에, 차기 2007년 5월 서울 회의 직전에 신규작업(NWIP: New Work Item Proposal) 투표 결과가 나올 수 있도록 ISO 18185-4 Gen2에 대한

표준화 작업을 적극적으로 추진할 필요가 있다.

이와 더불어 국내의 RFID 개발 업체와 전자봉인 보안 프로토콜을 개발하고 있는 한국전자통신연구원은 ISO 18185 규격에 대한 풍부한 이해와 개발력을 바탕으로 ISO TC104 SC4 WG2 표준화 논의에 적극적으로 참여하고 세계 주요 업체들에 늦지 않게 표준규격을 만족하는 전자봉인 제품을 출시함으로써 항만물류 시스템 혁신 및 국제 시장 확보와 국내 시장 보호에 힘써야 할 것이다.

강유성 (한국전자통신연구원 RFID/USN보안연구팀 선임연구원, youskang@etri.re.kr)