[정보보호] ITU-T 전자태그 보안 표준화 동향

안전한 통신 서비스를 위한 ITU-T SG17 연구과제 9 인터림(Interim) 회의가 2006년 9월 11부터 15일까지 캐나다 오타와에서 열렸다. 이번 회의에서 가장 중요한 결정 사항은 한국에서 제안된 networked 전자태그(RFID) 보안을 위한 프라이버시 보호 프레임워크와 프라이버시 보호 가이드라인에 대한 결정이었다. 프라이버시 보호 프라이버시는 2005년 10월에 제안되어 이번에 연구주제가 선정되었으며, 프레임워크는 2006년 4월 회의에 제안되어 이번 회의에서 연구주제로 선정되는 성과를 거두었다. 이번 인터림 회의를 계기로 networked 전자태그 보안 표준에 대한 개발이 본격적으로 ITU-T의 SG17에서 이루어 질 예정이다.

표준 주요 내용

전자태그를 이용한 정보 시스템은 자동화된 정보의 수집과 서버에 수집된 정보의 분석을 통하여 전자 태그를 부착한 사용자의 위치나 전자 거래의 특성을 추적할 수 있게 함으로써, 이 응용에 대한 프라이버시 문제가 지금까지 여러 곳에서 제기되어 왔다. 또한 이를 법제도적으로 예방하기 위한 프라이보호 가이드라인이 우리나라를 포함하여 일본, 미국 등에서 개발되어 적용되고 있다. 그런데 이 프라이버시 보호 가이드라인은 나라마다 독자적으로 개발되어 범세계적 차원의 가이드라인 개발이 요구되고 있다. 이번 인터림 회의에서는 이에 대한 두건의 기고서가 한국에서 제안되었는데, 하나는 프라이버시 보호 프레임워크이며, 다른 하나는 프라이보호 가이드라인에 대한 표준이다. 프라이버시 보호 프레임워크에서는 기존의 전자태그 시스템이 갖는 프라이버시 침해 측면의 보안 위협을 분석하고, 이를 방지하기 위한 기술적 차원의 프라이버시 보호 프레임워크와 관련 프로토콜이 개발될 예정이다. 또한 프라이버시 보호 가이드라인에서는 각 나라에서 개발된 독자적인 가이드라인을 기준으로 ITU-T 차원의 통합된 하나의 프라이버시 보호 가이드라인 표준 개발을 목표로 하고 있다. 프라이버시 보호 프레임워크를 위한 표준의 주요 내용은 프라이버시 침해가 예상되는 위협 분석, 프라이버시 보호를 위한 기본 요구사항, 그리고 사용자 프로파일 기반의 프레임워크가 포함될 것이다. 주요 프라이버시 침해 요인은 태그에 대한 위치 추적, 태그 정보의 누설, 수집된 이력 정보의 누설 등을 포함한다. 프라이버시 보안 요구사항은 보안 태그 ID의 추적불가성, 소유자에 대한 정보 추출 제어, 정보 소스에 대한 접근제어, 정보 수집에 대한 동의, 성인 정보 접근통제 등을 포함할 예정이다. 또한, 프라이버시 보호 가이드라인은 용어 정의, 개인 정보의 기록 금지, 개인 정보의 수집 금지, 개인 정보의 연계 금지 등의 요구사항, 전자태그의 활성화 및 비활성 표시 등에 대한 요구사항, 수집 표시 및 비활성화 표시 등의 요구사항, 태그의 생체 이식 금지, 태그 리더기의 존재 여부, 태그 정보 보호를 위한 관리 및 기술적 대책, 그리고 사용자 인식 제고 프로그램의 운영 등을 포함할 예정이다.

표준화 진행 사항

전자태그 프라이버시 보호 프레임워크는 지난 4월 제주 회의에서 제안되어, 현재 EPC

Global에서 수행되고 있는 표준화 활동과 이 표준과의 차이점을 명확히 해달라는 요구와 국내에서 제안된 주민등록번호 대체 수단 프레임워크와의 차이점에 대한 요구가 제기되었다. 따라서 이번 회의에서는 이에 대한 차이점이 설명되었으며, 연구과제 9에서 이 연구가 진행되어야 하고, 이를 위한 신규 연구주제의 신설(X.rfidsec-1)을 결정하였으며, 에디터로 최두호 박사(한국, ETRI)를 임명하게 되었다.

전자태그 프라이버스 보호 가이드라인은 2005년 10월 제네바 회의에서 한국에 의해 제안되어 SG17 주요 연구주제가 되어야 한다는 것에 대하여 합의하였고, 그 후속 대책으로 이번 인터림 회의에 한국정보보호진흥원에서 연구과제 9로 제안되었으나, 연구과제 9 토의 중 이 연구항목은 연구과제 6에서 추진하는 것이 타당하다는 의견이 개진되어 한국이 이를 수용함으로써 연구과제 6에서 신규 연구주제의 신설(X.rfpg)을 결정하였으며, 에디터로 이향진 연구원(한국, KISA)이 임명되었다. 현재 문서의 상태는 초안 상태이나, 이번 회의를 계기로 한국 주도로 전자태그 보안 프라이버시 보호를 위한 표준이 ITU-T에서 진행될 수 있다는 점에서 매우 의미가 있다고 할 수 있다. 또한 이번 인터림 회의를 통하여 전자태그 보안 연구를 연구과제 9에서 수행하기 위한 기반을 마련하기 위하여 액션 플랜 수정이 이루어졌다. 이 수정에는 전자태그 보안의 연구를 위한 표준과 관련 기술의 연구를 수행하며, 이를 수행하기 위하여 기존의 ISO/IEC JTC1 SC27/SC31과 협력하기로 하였고, 이를 위한 보안 표준을 개발 보급할 수 있도록 하였다.

향후 추진사항

프라이버시 보호 프레임워크는 2006년 12월에 드래프트가 제안될 예정이고, 내년 4월 WP2 회의에 추가적인 개선안이 제안될 예정이며, 최종적으로 2008년 4월에 표준 개발을 완료할 예정이다. 프라이버시 보호 가이드라인 역시 이번 12월 회의에 개선된 드래프트가 제출되어 검토가 이루어질 예정이고, 2008년 4월에 최종 표준으로 승인을 목적으로 추진될 예정이다. 이번 표준은 국내에서 개발된 전자태그 프라이버시 보호 가이드라인과 프라이버시 보호 프레임워크 기술이 ITU-T를 통하여 표준화를 시작되었다는 점에서 의미가 있다고 할 수 있다.

염흥열(ITU-T SG17 Q.9 Rapporteur, 순천향대 교수, hyyoum@sch.ac.kr)