[정보보호] ITU-T, 웹기반 공격 대응 기술 국제표준 채택 및 킬 스위치 국제표준으로 개발키로 합의

국제전기통신연합-전기통신표준화부문 연구반 17 (ITU-T Study Group 17, SG 17) 회의가 2014년 9월 17일부터 9월 26일까지 10일간 스위스 제네바에서 열렸다. 이번 회의에서는 웹 공격 대응 기술(Recommendation ITU-T X.1211)이 국제표준으로 채택했으며, 연구과제 6/17(유비쿼터스 통신 서비스, Question 6/17, Q.6/17)가 스마트폰 분실이나 도난에 대한 대응 기술(일명, 킬 스위치, Kill Switch)에 대한 신규 표준화 아이템과 한국의 정보보호준비도 관련 신규 표준화 아이템이 채택되었다. 본 고에서는 필자가 제출한 기고서들을 중심으로 논쟁사항과 합의 사항을 중심으로 기술한다.

주요 이슈 및 논쟁사항

이번 SG 17 회의에서는 웹 공격 대응 기술이 최종 국제표준으로 채택되었고, 스마트폰 분실 대응기술인 일명 킬 스위치 보안 구조, 한국 정보보호 준비도, 그리고 통신조직을 위한 개인정보관리 통제와 구현 가이드라인 등이 신규 표준화 아이템으로 채택되었다.

첫 번째 이슈는 웹기반 공격 대응 관련 권고 채택이다. 2009년 9월, 한국(염흥열)의 제안으로 Q.4/17(사이버보안) 그룹에서 웹기반 사이버보안 기술 표준화 작업(X.eipwa)을 착수하였으며, 웹기반 공격에 대한 기능 요구사항과 대응기술을 국제표준으로 개발 추진되었다. 지난 4월 SG17 회의에서 사전채택(determination)으로 추진되어 3개월간 국가별 의견수렴 기간 동안 3개국(캐나다, 핀란드, 한국)의 찬성으로 응답해 이번 회의의 채택 여부를 결정하게 되었다. 미국과 일본이 편집상의 의견을 제시해 반영했고, 현재 표준의 내용을 고려해 표준 제목을 “웹기반 공격 대응 기술”로 변경했다. 대부분의 국가들의 찬성 속에 무난히 채택되었다. 세계적으로 드라이브-바이 다운로드(drive-by-download) 공격이 기승을 부리고 있는 점을 고려하면, 이 국제표준은 선진국은 물론 개도국에서 웹 기반 대응 기술로 많은 활용이 기대되고 있다.

두 번째 이슈는 모바일 기기를 이용한 다중-요소(multi-factor) 인증 메커니즘(X.1158)의 사전채택(consent)이다. 2012년 8월, 한국 제안으로 한국 에디터(순천향대 염흥열, 금보원 김근옥)가 Q.7 그룹에서 본 이슈에 대한 표준화 작업을 착수하였으며, 사용자가 모바일 기기를 이용하여 다중-요소 인증 메커니즘을 개발하고, 이를 위한 보안요구사항, 서비스 모델 및 프로토콜을 정의하는 데 그 목적이 있다. 이번 회의에서는 한국은 4차 수정 텍스트를 제안해 반영했고, 이 표준의 완성도를 고려해 사전채택(consent)으로 추진하기로 합의했다. 제목을 “모바일폰을 이용한 다중 팩터 인증 메커니즘”으로 변경했다. 향후 4주간의 최종 의견수렴 기간을 거쳐 국제표준으로 채택될 예정이다.

세 번째 이슈는 스마트폰 분실 대응 신규 표준화 워크아이템 채택이다. 한국(염흥열)은 이번 SG17 회의에서 스마트폰 분실 대응에 대한 권고 추진을 제안해 반영했다. 이 제안은 미래부

정책적 추진 사항을 기술적으로 뒷받침하기 위해 추진되었다. 이 권고는 GSMA에서 개발된 일반 요구사항을 근거로 기술적 기능 요구사항과 기능 구조를 제안하는 표준이며 미래부 킬 스위치 관련 규제의 요구사항을 기술적으로 반영하기 위해 제안되었다. 미국, 영국 등은 대부분의 국가들이 이 표준의 중요성을 인정했다. 다만, 본 이슈가 GSMA가 다루고 있고 미주 지역 국가가 10월 부산 ITU PP-14에 단말 분실 대응에 대한 결의를 준비하고 있는 점을 고려해 권고 아이템 채택을 내년 4월 SG17 회의로 미룰 것을 요구했다. 한국은 이 권고는 GSMA 일반 요구사항을 이용해 세부 기능을 개발하므로 이 표준 개발시 GSMA와 협력 개발을 추진하겠고, PP-14 결의는 상위 수준을 결정이므로 이 권고 아이템 채택을 미룰 이유가 되지 않는다고 주장해 회의에서 합의를 이뤘다. 이 표준 제안은 화웨이, ZTE, China Mobile 등 중국 산업체와 이동통신서비스제공자, 브라질, 수단 등 11개의 회원의 지원으로 이 표준에 대한 관심을 미루어 짐작할 수 있다. 이 신규 표준화 아이템 채택으로 인해 소비자의 권익이 크게 개선되고 미래부의 정책 추진을 지원할 수 있을 것으로 기대된다.

네 번째 이슈는 통신조직을 위한 개인정보관리체계 부속서(Supplement) 신규 아이템 채택이다. ITU-T SG17과 ISO/IEC SC27 이 일반 조직을 위한 개인정보관치체계를 위한 지침을 공통 표준(common text)으로 추진되고 있는 것을 고려해, 한국(염흥열)은 통신조직에 적용될 추가 통제와 구현 가이드라인을 위해 신규 부속서 표준화 아이템을 제안해 반영했다. 미국, 캐나다 등은 이 부속서에서 개발될 내용의 어떤 부분이 통신 조직에 특화된 항목인지에 대한 이슈를 제기하였으나, 한국은 이 표준은 기존 공통표준에 존재하지 않으나 통신조직에 적용할 수 있는 추가적인 통제와 구현 가이드라인의 필요성을 강조해 합의를 이뤘다. 또한, 미국 등이 일반조직을 위한 공통 표준이 금년 10월 멕시코 회의에서 CD(committee draft)로 예정되어 있어 부속서 구조가 변경될 우려가 있다고 주장하면서 신규 아이템 채택을 내년 4월 SG17 회의로 미룰 것을 제기했으나, 한국은 이 부속서의 내용은 이미 공통 표준에 존재한 것을 이 부속서로 옮기는 것이고, 공통 표준의 구조가 수정되면 쉽게 반영될 수 있다고 주장해 합의를 이뤘다.

다섯 번째 이슈는 우리나라 정보보호 준비도 관련 신규 표준화 아이템 채택이다. 미래부가 지난 8월 발표한 정보보호 준비도의 국제표준화를 지원하기 위해 한국은 신규 권고 표준화 아이템을 제안해 반영했다. 이 권고는 조직을 위한 미래부 정보보호 준비도를 고려해 추진되었다. 미국, 영국, 일본 등은 정보보호관리체계의 개선 모델은 이미 존재하고 있고 이 권고가 기존 정보보호관리체계에 부정적 영향을 줄 가능성이 있다고 주장해 권고 채택을 주저했으나, 여러 차례 애드혹 회의를 거쳐 권고 내용을 기존 정보보호관리체계와는 독립적인 권고로 추진하겠다고 주장해 합의를 이뤘다. 이외에도 평가 대상인 보안 영역에 대한 국제적 합의가 매우 어렵다고 주장했으나, 보안 영역을 ITU-T X.805를 근거로 하겠다고 주장해 합의에 이르렀다. 또는 각종 평가 기준과 평가 항목을 부록으로 개발키로 합의했다. 국가 표준과 국제표준의 요구를 절묘하게 반영한 타협을 이룬 셈이다. 결국, X.805 보안 영역을 기반으로 한 기술적 구현 가이드라인으로 합의하고 신규 표준화 항목으로 채택되었다. 이번 신규 표준화 항목 채택으로 미래부가 추진하고 있는 정보보호 준비도의 국제표준 추진을 위한 기반을 마련했다.

향후 추진 전망

이번 회의에서 채택된 1건의 웹기반 대응 기술은 사용자가 웹 사이트만 방문해도 악성코드에 감염되는 드라이브-바이 다운로드(drive-by-download) 공격에 대응할 수 있는 지침을 제공할 것이다. 또한 3건의 신규 표준화 아이템은 정부의 주요 정책을 국제표준화로 연결하기 위해 제출되었고 반영되었다. 향후 이 표준 개발 과정에서 국내 산업체와 전문가의 지원이 필요하며 정부의 적극적인 관심도 필요한 시점이다.

염흥열 (순천향대 교수, ITU-T SG 17 부의장, ITU-T SG 17 WP 3 의장, hyyoum@sch.ac.kr)