# [정보보호] 기업의 보안 수준을 평가하기 위한 툴, 사이버보안 지수, ITU-T 국제표준화 동향

국제전기통신연합-정보통신표준화부문 연구반 17(ITU-T Study Group 17, SG 17) 회의가 2013년 8월 26일부터 9월 4일까지 스위스 제네바에서 열렸다. 이번 SG 17 회의 기간 동안에는 기업의 보안 수준을 평가하기 위한 사이버보안 지수에 대한 국제표준(Recommendation ITU-T X.1208)을 중점적으로 다루었으며, 연구과제 6/17(유비쿼터스 통신 서비스 보안, Q.6/17) 연구범위(Question Text)에 지능형 교통 시스템(ITS) 보안과 스마트 그리드 보안 분야를 추가하였다. 본 고에서는 이번 회의에서 다루어진 주요 이슈에 대한 논쟁사항과 합의 사항을 중심으로 기술한다.

**주요 이슈 및 논쟁사항**

이번 SG 17 회의에서는 기업 또는 공동체가 자기 스스로 사이버보안 수준을 측정하기 위한 사이버보안 지수에 관한 국제표준 최종 채택 이슈와 Q.6/17의 연구과제 텍스트의 변경이 심도 있게 다뤄졌다. 텍스트는 연구과제의 역할과 기능을 정의하는 문서이다.

첫 번째 이슈는 사이버보안 지수 국제표준화 추진 이슈이다. 2009년 11월 한국(필자)의 제안으로 Q.4/17(사이버보안) 그룹에서 표준화 작업을 착수하였으며, 필자가 에디터로 임명되어 이후 개발되어 왔으며, 한국 국가정보보호지수(NSI, national information security index)의 지표(indicator)를 사이버보안 지수(CSI, cybersecurity index)의 지표로 국제표준화하는데 그 목적이 있다.

사이버보안 지수의 지표를 개발하기 위해 ITU에서 개발된 개발지수(development Index), 세계경제포럼에서 개발된 네트워크준비지수(network readiness index), 인터넷보안 센터에서 개발된 보안지수(security metrics), 미국 국립정보표준원(NIST)과 유럽정보보호진흥원(ENISA)에서 개발된 가이드라인과 한국에서 개발된 국가 정보보호지수가 함께 고려되었다. 지난 4월 회의에서는 총 32가지의 지표를 정의하였고, 지표로부터 객관적인 방법으로 보안 지수로 계산하는 방법론이 최종 정의되어, 국제표준 채택을 위한 준비단계(determination)로 승인되었다.

이번 SG 17회의에서는 ITU-T 회원국으로부터 접수된 의견수렴 결과에 대한 검토가 이루어졌으며, 미국이 지난 4월에 제기된 의견을 반영해야 한다고 주장했고, 캐나다는 기업이나 특정 조직을 위한 사이버보안 지수를 개발해야 한다고 주장했으며, 러시아는 2가지 감사 로그 성능 보증 관련 지표 추가를 요구했으며, 일본은 국가 차원보다는 조직이나 커뮤니티 단위의 지수를 요구했다. 또한, 러시아와 캐나다가 독립적인 국제표준이 아닌 부속서(supplement)로 채택해야 한다고 주장했다. 이번 SG17 회의 기간 동안, 총 5회의 회의를 통해 모든 국가들의 의견을 반영하였으며, 연구과제 4 회의에서는 최종 국제표준으로 채택하기로 합의했다.

그러나 미국이 SG 17 폐회 총회에서 이 국제표준의 채택에 반대하지 않지만, 표준 텍스트의 내용이 많이 수정되었으므로 4주간의 추가 의견 검토기간을 요구했고, 영국, 캐나다, 일본 등이

이 제안에 동의했다. 따라서 SG17 국제회의 종료 후, 이들 4개국에 대한 4주간에 추가 의견 검토기간을 주기로 했다. 만약 추가 의견 수렴 기간 동안 해당 회원국으로부터 특별한 의견이 없을 경우, 최종 국제표준으로 채택(approval)하지만, 이 기간 동안 4개국으로부터 추가 의견이 제출될 경우 채택이 자동적으로 실패하고 다시 사전채택(determination)되어 2014년 1월 SG 17 회의에서 채택을 추진하기로 결정하였다. 하지만, 4주간의 추가 의견 수렴기간 동안 미국과 캐나다, 그리고 일본이 추가 의견을 제출해서 국제표준 채택에 실패했고, 3개국에서 제출한 의견을 반영해 다음 2014년 1월 차기 SG 17 회의에 채택을 추진해야 할 것이다.

두 번째 이슈는 한국(필자)이 제안한 Q.6/17의 텍스트 수정 제안 이슈이다. 한국은 2012년 10월 두바이에서 열린 세계정보통신표준총회(WTSA-12) 회의에서 스마트 그리드 보안, 지능형 교통시스템 보안, 클라우드 컴퓨팅 보안, 전자의료시스템 보안에 대한 국제표준을 개발할 것을 연구반 17에 추가하는 기고서를 제안해 WTSA-12 결의 50(사이버보안)의 결의 항목에 반영한 바 있다. 이번 회의에서 한국은 이러한 후속 조치로 Q.6/17의 텍스트에 이러한 연구주제가 분명히 나타나도록 텍스트의 수정을 제안했다. 중국과 일본은 당초 Q.6/17의 텍스트 수정 제안을 3국 공통으로 제안키로 합의(2013년 4월, 한중일 정보보호 실무반 회의)한 바 있어, 이번 회의에서도 이 수정 제안을 적극 지지했다. 미국도 지능형 교통 시스템(ITS) 보안의 중요성을 인정하여 지지 입장이었으며, 독일은 이 두 주제가 글로벌 솔루션이 필요한지와 이 주제가 ITU-T 임무 범위 내에 있는지에 대해 질의하였으나 이 수정 제안을 반대하지 않는다고 해서 한국의 제안대로 채택되었다. 토론 후 대부분의 회원국들이 찬성해서 작은 문구 수정을 거쳐 한국 제안에 따라 Q.6/17의 텍스트가 수정되었고, 내년 ITU-T 정보통신자문반(TSAG) 회의에서 최종 동의를 받도록 연락문서를 보내기로 했다.

더불어, 지난 4월 연구반 17 회의에서는 Q.6/17의 디폴트 표준 승인 절차를 대체승인절차(AAP)로 결정한 바 있다. 그러나 이번 회의에서 미국, 영국, 독일, 캐나다 등이 다시 지능형교통시스템(ITS) 보안과 스마트 그리드 보안 국제표준이 각 회원국의 규제적 이슈가 있음을 주장하면서 국제전기통신연합 협약의 관련 조항에 근거해 규제적 함의가 있는 권고나 연구과제는 디폴트 연구과제 표준 승인 절차를 전통승인절차(TAP)로 해야 한다는 주장과 여러 국가들의 찬성으로 전통승인절차(TAP)로 변경되었다. 한국(필자)은 SG 17 폐회 총회에서 지난 회의 결과를 변경하기 위해선 합의가 필요하다는 이유 등으로 Q.6/17의 디폴트 권고 승인 절차가 대체승인절차(AAP)가 되어야 한다고 주장하였으나, 결과는 전통승인절차(TAP)로 최종 승인되었다. 단, 현재 개발되고 있는 표준초안들은 대체승인절차(AAP)로 추진키로 합의했고, 신규 워크아이템 채택 시 규제적 성격이 없는 경우 대체승인절차(AAP)로 수정하기로 합의했다. 한국 입장에서는 이 연구과제에서 많은 국제표준을 개발하고 있어 부담되는 결정이다.

**향후 추진 전망**

이번 회의를 통해 지능형교통시스템과 스마트 그리드 보안 국제표준화 추진을 위한 발판을 근거로 국내 관련 산학연 주체들은 이 결정을 적극 활용해야 할 것으로 생각된다.

현재 SG17 그룹에서 개발되고 있는 대부분의 표준 초안들은 한중일 3국 에디터들이 주도하고 있으나, 미국, 영국, 캐나다, 독일 등은 이번 회기 동안 여러 신규 표준초안 제안을 여러 이유를 들어 반대하고 있다. 예를 들어, 이번 SG17 회의에서도 한국, 일본, 러시아에서 신규 표준화 아이템을 제안하였으나, 상기 국가들의 반대로 모두 신규 표준화 아이템이 채택되지 않았다. 반대 사유도 기술적인 문제보다는 현재 개발되고 있는 표준 초안들과의 중복성이나 다른 표준화기구들 간에 격차 분석(gap analysis)을 수행한 후 결정해야 한다는 주장이다. 향후, 우리나라도 신규 표준화 아이템 발굴을 위한 전략적 추진과 표준화 아이템 성격에 따라 다른 국제표준화 기구를 통한 표준 추진도 고려할 필요가 있다.

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