

ITU-T SG17 국제회의



염홍열 SG17 의장, 순천향대학교 정보보호학과 교수

오홍룡 TTA 표준화본부 책임연구원

1. 머리말

ITU-T SG17(study group 17, 보안)은 ITU-T에서 정보보호에 대한 기술적 표준을 개발하고 있다. 2018년 3월 20일부터 29일까지 10일간 스위스 제네바에서 열린 이번 S17 회의에는 38개국 156명의 대표가 참석했으며 우리나라에서는 염홍열 교수(순천향대, 대표단장) 등 26명의 국가대표단이 참석했다. 금번 회의는 이번 연구회기(2017~2020)에서 세 번째로 개최되었다. 주요 표준화 분야는 소프트웨어 정의 네트워크 보안, 통신망 정보보호관리 체계, 개인정보보호, 사이버보안, 모바일 보안, 사물인터넷 보안, 텔레바이오인식, 지능형 차량(ITS, intelligent transport system) 보안, 분산원장기술

(DLT, distributed ledger technology) 보안, 스마트그리드 보안 등이다. 본고에서는 우리나라 주도의 국제표준 최종 채택 및 사전 채택 내용, 우리나라가 제안한 신규 워크아이템과 신규 보안 이슈 등의 국제표준 추진에 대한 우리나라 제안 및 채택 내용 등을 제시하고자 한다.

2. 주요 회의 내용

2.1 국제표준 최종 및 사전 채택

한국 주도로 개발되어오던 2건의 국제 표준과 1건의 국제표준 부속서가 최종 채택되었으며 세부내용은 <표 1>과 같다.

<표 1> 한국 주도 국제표준 최종 채택

[2018년 3월]

연구과제	표준 번호	국제표준 제목	에디터	비고
Q4/17	X.1124 (X.samtn)	통신망에서 보안 평가 기법	진병문(순천향대) 외	최종 채택
Q6/17	X.1331 (X.sgsec-2)	스마트그리드 시스템에서 홈네트워크 디바이스를 위한 보안 가이드라인	이건희(국보연), 정소연, 박해룡(KISA) 외	최종 채택
Q3/17	X.Suppl 32 (X.sup-gpim)	통신조직을 위한 개인정보보호 준칙	염홍열(순천향대) 외	동의

<표 2> 한국 주도 국제표준 사전 채택

연구과제	표준 번호	국제표준 제목	에디터	비고
Q6/17	X.1361 (X.itssec-2)	사물인터넷을 위한 게이트웨이 모델 기반 보안 프레임워크	염홍열 (순천향대) 외	사전 채택 (TAP)

<표 3> 신규 워크아이템 제안 및 채택

연구과제	표준 약어	국제표준 제목	한국 에디터	권고 승인과정
Q4/17	X.gcpie	사이버보안 사고 증거 정보 수집 및 보존 가이드라인	이주영, 김종현(ETRI) 외	TAP
Q6/17	X.strvms	비디오관리 시스템의 보안 위협 및 요구사항	한중욱(ETRI) 외	TAP
Q14/17	X.das-mgt	분산원장기술에 기반한 데이터 접근 및 공유 관리 시스템 보안 프레임워크	염홍열, 김미연(순천향대) 외	AAP

2015년 4월부터 개발을 시작한 X.1124는 통신망 보안 평가 기법을 제시하고 있다. 이번 회의에서는 미국이 편집상의 수정을 제안해 이를 반영하고 최종 채택되었다. X.1331은 소비자 및 직접 연관된 가정용 스마트그리드 기기의 보안 기능을 제시했다. 이 표준은 대부분의 국가가 찬성해 최종 채택되었다. 부속서 32는 통신 조직을 위한 개인정보보호에 대한 다양한 보호조치를 제시하고 있으며 중국, 말레이시아 등의 적극적인 동의로 채택되었다.

또한 한국 주도로 개발되어 온 사물인터넷 보안 분야 국제표준이 사전 채택(TAP)되어, ITU-T 회원국들의 의견수렴을 거쳐 2018년 8월 SG17 국제회의에서 최종 채택될 예정이다. 본 국제표준(X.1361)은 사물인터넷을 위한 게이트웨이 모델 기반 보안 프레임워크를 제시했으며, 사물인터넷 기기, 사물인터넷 네트워크, 게이트웨이에 대한 보안 위협과 보안 요구사항을 다룬다. 주요 내용은 <표 2>와 같다.

2.2 신규워크아이템 채택

한국은 비디오 관리, 사이버보안, 분산원장기술

보안 분야에서 3건의 신규 워크아이템을 제안해 반영하였다. 더불어 3개의 신규 워크아이템의 에디터십을 확보했으며, 세부내용은 <표 3>과 같다. X.gcpie는 네트워크 위협 증거의 수집 및 보존을 위한 가이드라인을 제시한다. X.strvms는 비디오 관리 시스템에서 예상되는 보안 위협과 그 위협에 대처하기 위한 보안 요구사항을 제시한다. 또한 X.das-mgt에서는 분산원장 기술 기반의 데이터 접근 및 공유 관리 시스템의 보안 프레임워크를 제시한다.

2.3 지능형 차량 보안 논의

한국 주도로 개발되고 있는 3건의 권고에 대한 5건의 기고서가 제안되어 반영되었다. 지능형 차량을 위한 보안 프레임워크(X.itssec-2), 차량 외부 접속 장치를 위한 보안 요구사항(X.itssec-3), 차량내부 시스템 침입 탐지 시스템(X.itssec-4)에 대한 베이스 텍스트가 제안되어 반영되었다. 또한 일본이 UNECE WP29 TFCS에서 개발한 ‘사이버보안 권고안’ 기반 ‘커넥티드 차량 보안위협’ 신규 작업 항목을 만들라고 제안해 신규아이템으로 개발키로 합의했다.

2.4 분산원장기술 보안 논의

한국 주도로 개발되고 있는 3건의 권고에 대한 3건의 기고서가 제안되어 반영되었다. 분산원장기술을 활용한 온라인투표(X.stov), 분산원장기술의 보안 보증(X.sa-dlt), 분산원장기술의 보안 능력 및 위협(X.sct-dlt)에 대한 베이스라인 텍스트가 제안되어 반영되었다. 또한 분산원장기술 보안 기술의 표준화 로드맵도 제안되어 채택되었다.

2.5 SG17 신규분야 논의

2017년 9월 SG17 회의에서 정보보호 표준화 영역에 신규 분야(스팸기반 APT 공격, AI, 머신러닝 기술, 로보틱스 보안 등)를 수용하기 위해 현재의 연구과제 내용을 재검토하기로 결정했다. 이러한 논의에 능동적으로 대응하기 위해서 한국은 신규 분야와 관련된 것으로 판단되는 Q4/17(AI, 머신러닝)과 Q5/17(스팸기반 APT 공격, 랜섬웨어 대응)의 연구과제 텍스트 수정을 제안했다. 이에 미국, 영국 등은 새로운 분야를 좀 더 심층적으로 심의하기 위한 인큐베이션 절차를 도입할 것을 주장했다. 연구과제 5에서는 한국의 제안대로 스팸 기반 APT를 도입하기 위해 텍스트 수정을 합의했다. 러시아는 연구과제 4의 텍스트를 변경하자는 한국 제안을 지지하면서 인큐베이션 절차와 별도로 텍스트도 수정할 것을 주장했다. 회의 결과, 이번 회의에서는 연구과제의 텍스트를 변경하지 않되 SG17 회의 간 서면 회의와 다음 SG17 회의에서 논의를 계속하기로 합의했다. 또한 신규분야에 대한 작업을 촉진하기 위해 인큐베이션 프로세스를 예비적으로 합의했다.

한편, SG17 주관 하에 국제회의 하루 전 '5G 보안' 워크숍이 개최되었고, 그 결과를 근거로 SG17 내에 5G 보안 관련 연구과제들의 역할 점검과 5G 시스템을 위한 보안 가이드라인(X.5Gsec-q, 중국)

국제표준을 개발하기로 합의하였다.

3. 맺음말

이번 회의에서는 한국 주도로 개발되어온 스마트그리드 분야와 사이버 보안 평가 분야에서 2건의 국제표준이 채택되었고, 분산원장기술 보안 분야 등 3건의 신규 워크아이템을 채택했다. 이번에 채택된 사이버 보안과 분산원장기술 보안 분야 등에서 3건의 신규 워크아이템 채택은 국내의 우수한 보안 기술을 국제 표준으로 반영하기 위한 기반을 마련한 것으로 평가된다. 본 회의의 성과를 바탕으로 정보보호 분야 국내 고유기술을 국제표준에 반영하기 위해 산학연 전문가들과 함께 적극 대응할 필요가 있다. 다음 국제회의는 2018년 8월 29일부터 9월 7일까지 10일간 제네바에서 열릴 예정이며, 8월 28일에는 APT 보안에 대한 ITU 워크숍이 개최될 예정이다. 