

ITU-T SG17(정보보호) 국제회의



염홍열 SG17 의장, 순천향대 정보보호학과 교수
오홍룡 TTA 표준진흥단 책임연구원

1. 머리말

ITU-T SG17(study group 17, 보안)은 ITU-T에서 정보보호에 대한 기술적 표준을 개발하고 있다. 2018년 8월 27일부터 9월 7일까지 10일간 스위스 제네바에서 열린 이번 S17 회의에는 36개국 168명의 대표가 참석했고 한국에서는 염홍열 교수(순천향대, 대표단장) 등 28명의 국가대표단이 참석했다.

금번 SG17 회의는 이번 연구회기(2017년-2020년)에서 네 번째 SG17 회의이다. 주요 표준화 분야는 양자암호통신, 소프트웨어 정의 네트워크(SDN) 보안, 사이버보안, 모바일 보안, 사물인터넷 보안, 텔레바이오인식, 지능형 차량(ITS, intelligent transport system) 보안, 분산원장기술(DLT, distributed ledger technology) 보안, 스마트그리드 보안 등이다.

한국은 국가기고서 21건과 섹터기고서 14건을 제

안하여 사물인터넷 보안 관련 국제표준 1건의 최종 채택과 총 5건의 국제표준 사전 채택 총 5건의 신규 표준화 과제 채택 등의 성과를 거뒀다. 본고에서는 우리나라 주도의 국제표준 최종 채택 및 사전 채택 우리나라가 제안한 신규 워크아이템과 신규 보안 이슈 등의 국제표준 추진에 대한 우리나라 제안 및 채택 내용 등을 중심으로 제시하고자 한다.

2. 주요 회의 내용

2.1 국제표준 최종 및 사전 채택

한국 주도로 개발되어오던 한 건의 국제 표준이 최종 채택되었다. 최종 채택된 국제표준은 <표 1>과 같다.

본 국제표준(X.1361)에서는 사물인터넷을 위한 게이트웨이 모델 기반 보안 프레임워크를 제시한다.

<표 1> 한국 주도 국제표준 최종 채택(2018년 9월)

연구과제	표준 번호	국제표준 제목	에디터	비고
Q4/17	X.1361	사물인터넷을 위한 게이트웨이 모델 기반 보안 프레임워크	염홍열(순천향대)	최종 채택

<표 2> 한국 주도 국제표준 사전 채택(TAP determination)

연구과제	표준 번호	국제표준 제목	에디터	비고
Q4/17	X.1215 (X.ucstix)	구조화된 위협 정보 표현 규격(STIX)에 대한 유스케이스	김종현(ETRI), 염홍열, 김지혜(순천향대)	사전 채택 (TAP)
Q6/17	X.1042 (X.sdnsec-1)	소프트웨어 정의 네트워크(SDN) 기반 보안서비스	박정수(ETRI) 김형식(성균관대)	사전 채택 (TAP)

<표 3> 한국 주도 국제표준 사전 채택(AAP consent)

연구과제	표준 번호	국제표준 제목	에디터	비고
Q7/17	X.hakm	클라이언트-서버 모델에서 하이브리드 인증 및 키관리에 대한 보안지침	황정연(ETRI), 최규영(삼성SDS)	사전 채택 (AAP)
Q9/17	X.tac	스마트 ID카드를 이용한 원격바이오인식 접근제어	전명근(충북대)	사전 채택 (AAP)
Q11/17	X.orf-gs	객체식별자 기반 해석 서비스 프레임워크	최영환(ETRI)	사전 채택 (AAP)

사물인터넷 기기, 사물인터넷 네트워크, 게이트웨이
에 대한 보안 위협과 보안 요구사항을 제시한다. 이
번 회의에서는 러시아가 국가별 의견 수렴기간 동안
제출한 경량 암호 알고리즘과 관련한 편집상의 수
정 코멘트를 반영하고 최종 채택되었다. 이 표준은
2015년 3월부터 개발을 시작했으며 3년 6개월간 노
력으로 최종 채택되었다. X.1361은 국가별 사전 의
견 수렴 기간 동안 미국, 중국, 러시아 등의 채택 지
지가 있었다.

또한 한국 주도로 개발되어 온 2건의 국제표준이
사전 채택(TAP) 되어 ITU-T 회원국들에게 의견수
렴을 걸쳐 2019년 1월 SG17 국제회의에서 최종 채
택될 예정이다. 사전 채택(TAP) 된 국제표준의 주요
내용은 <표 2>와 같다. X.1215는 사이버 위협 정보
를 공유하기 위한 구조화된 위협 표현 규격 기반의
다양한 유스케이스를 제시하고 있다. 특히 국내에서
발생한 보안 사고에 대하여 STIX 규격으로 표현된
유스케이스가 제시된다. X.1042에서는 SDN 기반의
방화벽과 분산서비스대응 등의 다양한 보안 서비스
를 제시하고 있다.

한국 주도로 개발되어 온 3건의 국제표준이 사전
채택(AAP)되어, ITU-T 회원들에게 4주간의 최종 의
견수렴(Last Call)을 걸쳐 이견이 없을 경우 최종 채
택될 예정이다. 사전 채택된 국제표준의 주요 내용
은 <표 3>과 같다. X.hakm은 클라이언트-서버 모델
에서 클라이언트 측의 계산량을 감소할 수 있는 하
이브리드 인증 및 키관리의 보안 지침을 제시한다.
X.tac는 바이오 정보가 결합된 스마트 ID카드를 이
용한 원격 바이오인식 접근제어를 제시한다. X.orf-
gs는 객체식별자를 응용한 사물인터넷 환경에서의
그룹화 서비스를 식별 및 해석하기 위한 프레임워크
를 제시한다.

2.2 신규워크아이템 채택

한국은 양자 암호통신, 사물인터넷보안, 지능형
차량 보안 분야에서 5건의 신규 워크아이템을 제안
해 반영하였다. 이는 <표 4>와 같으며 더불어 5개의
신규 워크아이템의 에디터십을 확보했다. X.sf-qrng
에서는 양자 난수 발생기의 보안 위협과 보안 구조
를 제시하고 있다. 기술보고서 TRsec-QKD에서는

<표 4> 신규 워크아이템 제안 및 채택

연구과제	표준 약어	국제표준 제목	한국 에디터	권고 승인과정
Q4/17	X.sf-qrng	양자 난수발생기 보안구조	곽승환(SKT)	AAP
Q4/17	TR.sec-QKD	통신망에서 양자키 분배를 위한 보안 프레임워크	곽승환(SKT)	Agreement
Q6/17	X.iotsec-4	사물인터넷 기기 및 게이트웨이를 위한 보안 요구사항	윤미연, 류호석(KISA), 정원석(KTC)	TAP
Q13/17	X.eivnsec	차량용 이더넷 보안 가이드라인	이상우(ETRI), 이유식(이타스코리아)	TAP
Q13/17	X.edrsec	클라우드 기반 차량 사고기록장치	이상우(ETRI), 박승욱(현대자동차)	TAP

양자키 분배를 위한 보안 위협과 요구사항을 제시한다. X.iotsec-3는 국내에서 개발된 IoT 디바이스와 게이트웨이의 보안 시험 가이드라인을 제시한다. X.eivnsec는 차량용 이더넷 보안 가이드라인을 제시한다. X.edrsec는 클라우드 기반 차량 사고기록장치의 규격을 제시한다.

2.3 양자암호통신 논의

SK텔레콤에서는 섹터 기고서로 양자 키분배 시스템 보안 프레임워크와 양자 난수 생성 시 구조에 대한 2건의 신규 워크아이템을 제안했다. 일부 회원국에서는 2건의 신규 워크아이템에 대한 표준화기구 간에 갭 분석의 미흡 등의 이유로 입장을 유보했다. 중국, 스위스, 한국, 현대자동차 등으로부터 신규 워크아이템에 대한 지지를 얻었다. 다각적인 노력을 통해 양자 난수 생성기는 권고로 채택되었고 양자 키 분배 시스템 보안 프레임워크는 기술보고서로 채택되었다. 양자 키 분배의 경우 기술보고서로 일단 시작하고 갭 분석을 지속적으로 추진하여 향후에 최소한 1개 이상의 권고로 전환될 가능성이 있다는 것을 합의했다. 또한 다음 SG17 회의에 논의를 위해 양자 암호 통신 연구과제(Question) 신설을 SG17 의장이 회의 기간 동안 여러 회원국의 협의를 통해 TD로 제안했다. 이 제안은 이번 회의에서는 합

의되지 못했지만 차기 회의에서 계속 논의를 진행하기로 해 한국 주도의 15번째 연구과제 신설 합의 가능성을 열어 두었다.

2.4 분산원장기술 보안 논의

한국 주도적으로 개발되고 있는 4건의 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), 분산원장 기술 기반의 데이터 접근 및 공유 관리 시스템(X.das-mgt)에 대한 베이스라인 텍스트가 제안되어 반영되었다. 또한 분산원장기술 보안 기술의 표준화 로드맵도 제안되어 채택되었다.

2.5 SG17 신규 분야 논의

2017년 9월 SG17 회의에서 신규 보안 이슈를 수용하기 위한 보안 연구 혁신이라는 서신그룹(CG) 활동을 시작했다. 한국은 2018년 3월 회의에 인공지능을 이용한 사이버 공격 대응 체계에 대한 국제 표준 개발을 위한 연구과제 4의 텍스트(연구범위, ToR) 수정 제안과 이메일을 통한 타킷 공격 대응에 대한 연구과제 5의 텍스트 개정을 제안한 바 있다. 이번 SG17 회의에서 이 제안이 다시 논의되어 한국 제안이 모두 반영되었다. 더불어 5G 보안을 수용하

기 위한 연구과제 6 텍스트 수정과 빅데이터 분석을 시작하기 위한 연구과제 8의 텍스트 수정도 합의되었다. 따라서 이번 회의에 합의된 4개의 연구과제에 대한 수정 제의는 이번 연구회기(2017년-2020년) 하반기를 위한 표준화 활동을 위한 기반을 마련했다고 평가될 수 있다.

2.6 FIDO 얼라이언스 규격의 ITU-T 권고 채택

이번 회의에서는 FIDO 얼라이언스에서 개발된 2건의 규격이 ITU-T 표준으로 사전 채택되었다. 이는 ‘범용 인증 프레임워크(X,uaf, X1278)’과 ‘고객-인증자 프로토콜(X,ctap, X,1277)’ 등이다. 이번에 사전 채택된 2건의 FIDO 규격은 4주간의 회원 최종 의견 수렴 과정을 통해 이견이 없을 경우 최종 채택될 예정이다. 이는 사실 표준화 단체에서 개발된 영향력이 큰 표준을 ITU-T 표준으로 채택하기 위한 노력의 일환이며 이러한 노력은 이번 연구회기 동안 지속될 예정이다.

2.7 사이버 보안 공격 및 랜섬웨어에 대한 워크숍

SG17 주관 하에 국제회의 하루 전에 ‘사이버 보안 공격 및 랜섬웨어’ ITU 워크숍이 개최되었다. 이 워크숍에서는 27개국 105명이 참석했다. 본 워크숍에서는 구조화된 위협 정보 규격에 대한 표준화 필요성과 인공지능 기술을 이용한 사이버 보안 대응 능력 개선, 메일을 통한 타킷형 공격 대응에 대한 표준화 필요성이 제시되었다. 한국에서는 과학기술정보통신부 오상진 국장의 ‘평창 동계 올림픽 사이버보안’과 하우리 최상명 실장의 ‘위너클라이 랜섬웨어 교훈’에 대한 발표가 있었다. 차기 SG17 주관 워크숍은 차기 SG17 국제회의에 앞서 ‘AI, ML 그리고 보안’이라는 주제로 2019년 1월 21일 제네바 ITU 본부에서 개최하기로 했다.

3. 맺음말

이번 회의에서는 한국 주도로 개발되어온 사물인터넷 보안 분야 1건의 국제표준 최종 채택과 양자 암호통신 및 지능형 차량 보안 등 신규 표준화 아이템 채택은 산업적 파급효과가 매우 클 것으로 예상된다. 향후 SG17 국내 연구반은 본 회의 성과를 바탕으로 정보보호 분야 국내 고유기술을 국제표준에 반영하기 위해 산학연 전문가들과 함께 적극적으로 대응할 계획이다. 차기 SG17 국제회의는 2019년 1월 22일부터 1월 30일까지 9일간 제네바에서 열릴 예정이다. 