ITU-T SG 17(보안) 국제회의

염흥열 _ SG 17 국제 의장, 순천향대학교 정보보호학과 교수
오흥룡 _ Q2/17 라포처, TTA 표준화본부 수석연구원

1. 머리말

ITU-T SG 17(Study Group 17, 보안)은 정보통신 환경에서 신뢰와 보안을 보장하기 위한 정보보호 기술의 국제표준을 개발하고 있다. 2019년 8월 27일부터 9월 5일까지 스위스 제네바에서 개최된 SG 17 국제회의는 41개국 206명의 표준 전문가가 참석하였고, 한국은 염흥열 교수(순천향대, 수석대표) 등 34명의 국가대표단이 참석하였다.

한국은 양자암호통신, 스마트그리드, 지능형자동차보안, 분산원장기술, 산업제어시스템 보안 등에서 주요 성과를 거두었다. 한국은 국가기고서 35건과 섹터기고서 15건을 제안하여, 총 4건의 국제표준 사전 채택(Consent/Determination)과 총 4건의 신규 표준화 아이템 승인 등의 성과를 거뒀다. 본고에서는 한국 주도로 개발되어 사전 채택된 국제표준과 새롭게 정보보호 기술을 개발하고자 하는 신규 표준화 아이템을 중점적으로 기술한다.

2. 주요 회의 내용

2.1 국제표준 사전 채택

<표 1> 한국 주도 국제표준 사전 채택

No.	기고서 주요내용	에디터	소속	비고 (승인절차)
1	양자 잡음 난수생성기 구조	심동희	SKT	AAP
2	스마트 미터링 서비스 보안 가이드라인	이건희	ETRI 부설연구소	TAP
3	커넥티드 카 보안 위협 정의	이상우/박승욱 김창오	ETRI/현대자동차 카카오모빌리티	TAP
4	V2X 통신 환경 보안 가이드라인	이상우·나재훈/ 박승욱/김창오	ETRI/ 현대자동차/카카오모빌리티	TAP

한국 주도로 개발된 총 4건의 국제표준(권고안)이 〈표 1〉과 같이 사전 채택되었다.

첫 번째 권고안 '양자 잡음 난수생성기 구조(X.1702)' 국제표준은 세계 최초의 양자 기술을 적용한 난수 생성 방법을 정의한다. 본 표준은 2018년부터 SKT 주도로 개발한 표준으로 암호키 생성에 필요한 완전 난수를 양자 기술 기반으로 만드는 방법을 정의한다. 즉, 예측이 불가능하고 패턴이 없는 순수 난수를 추출하기 위해 양자 기술을 적용하였다. 본 표준은 난수생성기를 이용하는 암호 기술 전 분야에 적용 가능하며, 특히 5G 네트워크를 기반으로 제공되는 사물인터넷, 자율주행자동차, 스마트시티 등 최첨단 서비스의 보안성을 강화할 것으로 기대된다.

두 번째 권고안 '스마트 미터링 서비스 보안 가이드라인(X.1332)' 국제표준은 스마트그리드 환경에서 사용자의 스마트 미터로부터 수집한 데이터를 안전하게 활용하기 위한 보안 대책을 정의한다. 본 표준은 2016년부터 국가보안기술연구소 주도로 개발된 표준으로 소비자 영역에 설치된 스마트 미터로부터 수집된 전기 사용량 및 품질정보가 전력사, 부가서비스 사업자, 소비자 등과 안전하게 공동 활용될 수 있도록 관리·활용하는 방법을 정의한다. 본 표준은 국내 에너지신산업 확산 계획을 통해 국가에서 추진하고 있는 전력에너지 빅데이터 공동활용 사업의 보안대책으로 적용 가능하며, 세계적으로 확대되고 있는 스마트그리드 빅데이터 공동활용 보안에 활용될 것으로 예상된다.

세 번째 권고안 '커넥티드 카 보안 위협 정의(X.1371)' 국제표준은 지능형 자동차 보안서비스를 제공하기 위한 모델을 정의하고, 각 모델에서 발생할 수 있는 보안 위협을 식별 및 정의한다. 본 표준은 2018년부터 한국전자통신연구원, 현대자동차, 카카오모빌리티 주도로 개발되었으며 지능형 자동차 보안을 위한 외부해킹, 백엔드 서버, 통신 채널, 업데이트 절차 등을 고려한 보안 위협을 식별 및 정의하고 있다. 향후 ITU-T에서 개발되는 지능형 자동차 보안 국제표준에 기본 표준으로 적용될 예정이며, 국내 차량 보안 연구에도 활용되어 기술적 우위를 확보함으로써 수출에도 도움이 될 것으로 기대된다.

네 번째 권고안 'V2X 통신 환경 보안 가이드라인(X.1372)' 국제표준은 자율주행자동차 서비스에 가장 기본이 되는 차량 통신에 대한 보안기술을 정의한다. 본 표준은 2014년부터 한국전자통신연구원, 현대자동차, 카카오모빌리티 주도로 개발되었으며, 표준에서 다루고 있는 V2X(Vehicle-to-Everything) 통신은 차량과 차량(V2V), 차량과 인프라(V2I), 차량과 노매딕 디바이스(V2D) 및 차량과 보행자(V2P) 간의 통신을 의미하며, 각 통신 간에 보안 위협, 보안 요구사항 및 유스케이스를 정의하고 있다. 향후 자율주행자동차를 연구하는 국내 산업체의 제품개발, 중복투자 방지 및 자동차 안전성 확보에 유용한 자료로 활용될 전망이다.

AAP(alternative approval process)로 사전 채택된 1건의 권고안은 4주간의 의견 수렴기간을 거친 후 의견이 없으면 바로 국제표준으로 채택된다. TAP(traditional approval process)로 사전 채택된 3건의 권고안은 향후 3개월간의 국가별 의견을 수렴한 후 2020년 3월 SG 17 국제회의에서 국제표준으로 채택 여부를 결정한다.

2.2 신규 표준화 아이템 승인

한국은 지능형자동차 보안, 분산원장기술 보

<표 2> 신규 표준화 아이템 승인 및 에디터십 확보

No.	기고서 주요내용	제안자/에디터	소속
1	차량시스템 침입대응시스템을 위한 테크니컬 프레임워크	김휘강 박승욱	고려대학교 현대자동차
2	분산원장기술 용어 정의	염흥열 김지혜	순천향대학교 한국정보기술단
3	산업제어시스템 원격접속 보안 가이드라인	이건희	국가보안기술연구소
4	분산원장기술을 위한 보안 통제	오경희	TCA서비스

안, 산업제어시스템 보안 분야에서 4건의 신규 표준화 아이템을 제안하여, 〈표 2〉와 같이 승인되었다.

첫 번째 권고안은 고려대와 현대자동차 주도로 '커넥티드 자동차용 침입차단시스템 방법론(X.ipscv)'을 제안하여 신규 표준화 아이템으로 승인되었다. 본 권고안은 자율주행차량에 외부 해킹 탐지 및 표준화된 차단/대응기법이 적용된 차량용 침입차단시스템을 개발하기 위한 보안기술이다. 향후 한국은 전 세계 자동차 제조사 및 차량 주문제작사(OEM)들이 참고할 수 있는 표준으로 개발할 계획이다.

두 번째 권고안은 순천향대 주도로 '분산원장기술 용어 정의(TR.dlt-td)'를 제안하여 신규 표준화 아이템으로 승인되었다. 본 권고안은 분산원장기술 분야에서 활용될 다양한 용어를 정의할 예정이며, 한국 주도로 정의된 용어가 전 세계 공통 용어로 활용될 예정이다. 본 표준은 2019년 8월 마감된 분산원장기술 포커스 결과물에 대한 후속 작업으로 2020년 8월에 국제표준으로 완료할 계획이다. 한편, FG-DLT 그룹 종료 후 활동 결과물에 대한 후속조치가 2019년 9월 말에 개최되는 TSAG(자문그룹회의) 국제회의에서 확정될 계획이므로 SG 17 국제회의에서는 기술보고서(Technical Report) 형태로 승인하고, TSAG 회의 결과와 권고안의 품질에 따라 권고안으로 격상시키기로 하였다.

세 번째 권고안은 국가보안기술연구소 주도로 '산업제어시스템 원격 접속 보안 가이드라인(X.sg.rat)'을 제안하여 신규 표준화 아이템으로 승인되었다. 본 권고안은 5G 통신 확대 및 스마트 팩토리 활성화에 따라 산업제어시스템의 원격 관리 및 원격 유지보수 등을 위해 원격접속 시스템에 적용해야 하는 보안대책을 정의할 계획이다.

네 번째 권고안은 TCA서비스 주도로 '분산원장기술 보안 통제 지침(X.gscdlt)'을 제안하여 신규 표준화 아이템으로 승인되었다. 본 권고안은 분산원장시스템의 개발자 및 제공자가 분산원장시스템을 안전하게 개발 및 운영할 뿐만 아니라, 이러한 시스템의 이용자와 감독자들이 분산원장시스템의 안전성을 확인하는 데 활용할 수 있도록 분산원장시스템의 보안에 필요한 보안 통제 항목을 개발하고, 이를 구현 및 운영하기 위한 지침과 참조 정보를 제공할 계획이다.

2.3 양자암호통신 논의

한국은 2019년 1월 양자암호통신에 대한 연구과제 신설을 제안하였지만, 이번 SG 17회의에서는 차기 연구회기(2021-2024)를 고려한 구

조조정 이슈와 관련하여, 신설 여부를 보류하기로 하였다. 대신 연구과제 4를 통해 국제표준을 지속적으로 개발키로 합의했다. 현재 양자암호통신 표준개발은 국내(KT, SKT)와 국외(IDQ, China Mobile, ZTE, NICT 등) 업체들 간에 많은 관심을 불러일으키고 있으며, 이번 SG 17 국제회의에도 총 15건의 기고서가 접수되어 논의되었고, 1건의 신규 표준화 아이템 신설이 합의되었다.

현재 SG 17 연구반은 양자암호통신 보안 권고안을 〈표 3〉과 같이 중점적으로 다루고 있으며, SG 13 연구반은 양자암호통신 네트워크 권고안을 중점적으로 개발하고 있다. 향후 양자암호통신 권고안을 협력적으로 개발하기 위해 SG 13의 연구과제 16과 SG 17의 연구과제 4는 동일 장소에서 회의를 개최하는 등 협력 개발을 강화할 예정이다.

2.4 WTSA-20 구조조정 논의

이번 SG 17 국제회의는 WTSA-20 구조조정 이슈를 논의하기 위해 스페셜 세션 회의(염흥열 의장 주재)를 총 5회 개최하였다. 한국은 차기 연구회기(2021-2024)를 위한 SG 17 임무, 각 Question 별 수정 텍스트, WTSA-20 준비를 위한 서신그룹(CG, Correspondence Group) 활동에 대한 3건의 기고서를 제출하였다. 미국은 한국의 제안과 CG-XSS(Transformation of Security, 보안 구조조정 연구)의 제안을 고려하여 SG 17 연구과제를 재구성할 것을 제안하였다. 영국은 기존의 WP, 연구과제 구성을 변경하여 연구과제 수를 축소하는 방향으로 SG 17 연구과제의 재구성을 제안하였다. 캐나다는 양자암호통신 연구과제 신설 및 유럽정도통신표준화기구(ETSI)에서 연구하고 있는 양자암호통신 표준 결과들을 적극 반영할 것으로 제안하였다. 총 5회에 걸쳐 논의된 WTSA-20 대응 구조조정 이슈는 한국 기고서를 기반으로 이번 회의에 논의된 사항을 추가 반영하여, TSAG 회의에 업무보고 하기로 하였고, 차기 SG 17 국제회의 전까지 지속적으로 서신그룹(CG-WTSA-20)을 통해 논의하기로 하였다. 한편, 양자암호통신 연구과제 신설은 일본, 미국 등이 신설을 반

<표 3> 양자암호통신 보안 권고안 현황

No.	권고안 번호	제목	에디터	Timing
1	X.1702(X.qrng-a)	양자 잡음 난수 발생기 구조	심동희, Matthieu Legré, Hao Qin, Zhangchao Ma	2019. 9.
2	X.cf-QKDN	양자키 분배 네크워크에 의해 발생되는 키의 암호학적 기능의 사용	Matthieu Legré, 심동희	2020. 3.
3	X.sec-QKDN_ov	QKD 네트워크를 위한 보안 요구사항 - 개요	심동희, Matthieu Legré Hao Qin, Zhangchao Ma	2020. 3.
4	TR.sec-qkd	정보통신 네트워크 환경에서 QKD를 위한 보안 프레임워크	Matthieu Legré, 심동희	2020. 3.
5	X.sec-QKDN_km	QKD 네트워크를 위한 보안 요구사항 - 키관리	심동희, Jiajun Ma, Kaoru Kenyoshi, Zhangchao	2020. 9.
6	X.sec_QKDN_TN	QKD 네트워크를 위한 보안 요구사항 - 신뢰 노드	Matthieu Legré, Zhangchao Ma, Hao Qin, 심동희	2021. 3.

대해 합의를 이루지 못하였고, 서신그룹(CG-WTSA-20)에서 신설 여부 또는 기존 연구과제에서 수행 여부를 계속 논의할 예정이다.

3. 맺음말

한국은 이번 회의에서 총 50건(국가: 35건, 섹터: 15건)의 정보보호 분야 기고서를 제출하였고, 지능형자동차 보안, 스마트그리드 보안, 양자암호통신 보안 분야에서 국제표준 사전 채택이라는 성과와 분산원장기술 보안, 산업제어시스템 보안 등에서 신규 표준화 아이템 및 에디터십 확보는 산업적 파급효과가 매우 클 것으로 예상된다. 향후, SG 17 국내 연구반은 이번 회의 성과를 바탕으로 정보보호 분야 국내 고유기술을 국제표준에 반영하기 위해 산학연 전문가들과 함께 적극적으로 대응할 계획이다. 차기 SG 17 국제회의는 2020년 3월 17일부터 26일까지 스위스 제네바에서 개최될 예정이다.