ITU-T SG17(정보보호, 2022년 8/9월) 국제회의

박수정 TTA 표준화본부 책임
염흥열 ITU-T SG17 국제 의장, 순천향대 정보보호학과 교수

1. 머리말

ITU-T SG17(Study Group 17)은 UN 산하 표준 개발 및 보급을 수행하는 ITU에서 정보보호 기술에 대한 국제표준을 개발하는 연구반이다[5]. 2022년 8월 23일부터 9월 2일까지 ITU-T SG17 국제회의가 스위스 제네바에서 대면 회의로 개최되었으며, 코로나19 팬데믹이 지속됨에 따라 온라인 회의 참석도 허용되었다. 이번 SG17 국제회의에는 세계 45개국에서 282명이 참석하였으며, 한국에서는 염흥열 교수(순천향대, 수석대표) 등 49명의 국가대표단이 참가하였다.
우리나라는 5G 보안, 지능형차량통신 보안, 신원관리 및 인증 보안, 분산원장기술 보안, 양자암호통신 등 차세대보안기술 표준화를 위해 국가기고서 31건을 제안하여, 국제표준 3건 최종승인, 국제표준안 3건 사전채택, 신규 표준화 과제 3건 승인 등 왕성한 성과를 도출하였다. 본고에서는 한국 주도로 개발하여 최종 승인 및 사전 채택된 국제표준과 새롭게 개발을 시작한 신규 표준화 과제에 대해 중점적으로 기술하고자 한다.

2. 주요 회의 내용

2.1 국제표준 최종승인 (3건)
이번 SG17 국제회의에서는 5G 보안, 사물인터넷 보안 분야 등에서 한국이 다년간 주도적으로 개발해온 국제표준 3건이 최종 승인되었으며, 1건의 표준 부속서가 승인되었다.

<표 1> 한국 주도 국제표준 최종 승인

No.	표준 번호	표준 제목	에디터(소속)
1	X.1813 (X.5Gsec-vs)	초고신뢰 초저지연 통신을 지원하는 IMT-2020 기반 버티컬 서비스 보안 요구사항	신성기, 오재언(맥데이타), 염흥열(순천향대)
2	X.1814 (X.5Gsecguide)	IMT-2020 통신 시스템에 대한 보안 지침	염흥열(순천향대), 박근덕(서울외대), 김미연(NSHC)
3	X.1352 (X.iotsec-4)	사물인터넷 기기 및 게이트웨이의 보안 요구사항	이상걸, 류호석(한국인터넷진흥원), 정원석, 방지호(한국기계전기전자시험연구원)

첫 번째 최종 승인된 표준인 '초고신뢰 초저지연 통신을 지원하는 IMT-2020(5G) 기반 버티컬

서비스 보안 요구사항(X.1813)'은 스마트 팩토리 등 5G 사설망의 융합 서비스 환경에서 네트워크 장애·성능·보안 모니터링을 위한 주요 구성요소 및 아키텍처를 정의하고, 이에 대한 보안 위협 및 보안 기능을 제시한다. 이 표준은 TTA의 국제표준 마에스트로 멘토링 지원 사업의 일환으로 국제표준 마에스트로(순천향대 염흥열 교수)와 벤처기업(맥데이타) 간 멘토링을 통해 2020년 8월 한국이 ITU-T SG17 국제회의에 신규 표준화 과제를 제안하여 채택되었다[1]. 이후 다년간 국제회의에서 표준안 개발 및 논의 과정을 거치며 각국의 의견을 반영하여 이번 SG17 국제회의에서 최종 승인되었다. 이 표준은 부산시의 '이음5G 기반 디지털트윈 스마트공장 개념실증 사업'에 적용되고 있으며, 향후 국내외 통신사업자들이 5G 사설망 기반 스마트공장·스마트빌딩 등의 B2B 서비스를 상용화할 때 5G 네트워크 모니터링을 통한 고장진단 및 침입 대응을 고도화하기 위해 유용하게 참고 가능할 것으로 기대된다.

두 번째 최종 승인된 표준인 'IMT-2020 통신 시스템에 대한 보안 지침(X.1814)'은 사용자가 보유한 스마트폰, 통신 기지국과 스마트폰을 연결하는 네트워크, 코어 네트워크 등에서 발생할 수 있는 전반적인 보안 위협을 식별하고, 5G 통신 시스템의 각 구성요소들을 보호할 수 있는 지침을 제시하였다[2]. 이 표준은 한국 제안으로 2019년 1월 ITU-T 신규 표준화 과제로 승인되었으며, 에디터인 순천향대, 서울외대의 주도적인 표준 개발과 러시아·캐나다 등 각국의 의견 반영을 거쳐, 이번 회의에서 국제표준으로 최종 승인되었다.

이 표준은 5G 통신 시스템에 대한 단편적인 보안지침이 아닌 시스템 전반적 보안 요구사항을 제시하여 5G 통신 시스템 구축 및 운영에 참고 가능한 지침이다. 스마트폰 제조사, 통신장비 제조사, 통신사 등 사업자 영역이나 국가를 가리지 않고 참고 및 준수하는 국제 5G 보안 바이블이 될 것으로 기대한다.

세 번째 최종 승인된 표준인 '사물인터넷 기기 및 게이트웨이의 보안 요구사항(X.1352)'은 IoT 기기 및 게이트웨이에서 발생 가능한 보안 위협을 식별하고, 이에 대한 보안 요구사항을 인증, 암호, 데이터, 플랫폼, 물리적 보안 등 5가지 측면에서 제시하고 있다.

이 표준은 기존 한국이 개발한 국제표준인 'IoT 보안 프레임워크(X.1361)'에 기반하여 이에 대한 보안 시험 및 인증 기준[3]을 2018년 9월 신규 표준화 과제로 제안하였고, 이후 KISA·KTC가 에디터로 다수의 기고서를 제출하고 국제회의에서 각국의 의견을 반영하는 등 활발한 논의를 통해 이번 국제회의에서 최종승인 되었다. 이 표준은 국내 정보통신망연결기기 등 정보보호인증 기준을 국제표준에 반영한 것으로, 국내 사물인터넷 제조사 등 관련 산업계의 글로벌 시장 진출 및 선점에 도움이 될 것으로 기대된다. 또한, 국외 IoT 기관과 상호 보안인증을 추진할 때 국내 기준이 국제표준 기준을 충족한다고 제시할 수 있어 상호인증 소요기간 단축에 도움이 될 것으로 예상한다.

2.2 국제표준안 사전채택 (3건)

최근 차량이 점차 네트워크에 연결되고 자율주행이 가능해질 정도로 지능화됨에 따라, 차량 통신에 대한 보안 위협 또한 증대되고 있다. 또한 유럽경제위원회(UNECE) W P29에서 제정한 차량 사이버보안 규제(UN Regulation No. 155, Cyber security and Cyber Security Management System)에 따라 2022년 7월부터 유럽에 출고되는 신차에 대해 차량 설계부터 생산 및 단종까

지 차량의 라이프 사이클 전반에 걸쳐 보안이 의무화되었다[4]. 이러한 환경 변화에 능동적으로 대응하여 우리나라는 국내 산·학·연 협업을 바탕으로 다년간 ITS 보안 표준들을 개발하였으며, 이번 SG17 국제회의에서 국제표준(안)으로 3건이 사전 채택되는 성과를 이루었다.

<표 2> 한국 주도 국제표준 사전 채택

No.	표준 번호	표준 제목	에디터(소속)	비고 (승인절차)
1	X.1377 (X.ipscv)	커넥티드 자동차 침입방지 시스템을 위한 가이드라인	김휘강, 정성훈(고려대), 이상우(ETRI), 박승욱(현대자동차)	AAP
2	X.1380 (X.edr-sec)	클라우드 기반 차량 데이터 저장장치 보안 가이드라인	이상우(ETRI), 박승욱(현대자동차)	TAP
3	X.1381 (X.eivn-sec)	이더넷 기반 차내망 보안 가이드라인	이상우(ETRI), 이유식(이타스코리아)	TAP

첫 번째 사전채택 표준인 '커넥티드 자동차 침입방지 시스템을 위한 가이드라인(X.1377)'은 커넥티드 차량에 침입 탐지 등 위협이 발생하였을 때 능동적으로 대응하기 위한 지침 및 유즈케이스를 제시한다. 이 표준은 기존 한국이 개발한 표준인 '차량 내부 네트워크용 침입탐지시스템 가이드라인(X.1375)'에 기반하여, 차내에는 최소한의 침입탐지기능만 탑재하고, 차량 외부 서버에서 수집된 침입 탐지결과를 분석하여 최종적으로 차량 외부의 비정상적인 공격에 대응하는 프레임워크를 제공하고 있다. 이 표준은 2019년 9월 고려대 주도로 신규 표준화과제를 제안해 승인되었으며, 이후 고려대·ETRI·현대자동차 등 산학연이 공동으로 표준안을 개발하여 이번 국제회의에서 사전채택되었다. 차량이 지능화됨에 따라 차량에 발생하는 해킹 시도 및 이상징후를 탐지할 수 있는 침입 탐지 및 차단 시스템에 대한 요구가 증대되고 있는 현 시점에서, 이 표준을 통해 커넥티드 자동차의 보안성 및 안전성 강화뿐 아니라 국내 기업의 글로벌 수출 증대에도 기여할 것으로 기대된다.

두 번째 사전채택 표준인 '클라우드 기반 차량 데이터 저장장치 보안 가이드라인(X.1380)'은 클라우드 기반 차량 데이터 저장 시스템에 대한 기술적 고려 사항, 보안 요구사항 및 유즈케이스를 소개한다. 이 표준은 2018년 8월 ETRI와 현대자동차에서 신규과제를 제안하여 주도적으로 개발해왔으며, 이번 국제회의에서 사전채택되었다. 이 표준은 차량 사고 발생 기록 저장 장치를 안전하게 보존하기 위한 지침으로, 향후 사고 원인 분석 및 분쟁 조율에 참고자료로 활용 가능할 것으로 예상한다.

세 번째 사전채택 표준인 '이더넷 기반 차내망 보안 가이드라인(X.1381)'은 차량용 이더넷 환경에서의 보안 위협을 기술하고, 이에 대한 대처 방안을 수립하기 위한 보안 요구사항 및 유즈케이스를 제시한다. 이 표준은 2018년 8월 국내 ETRI와 이타스코리아에서 신규과제를 제안하여 지속적으로 개발해왔으며, 독일 등 각국의 의견을 반영하여 표준안의 완성도를 제고해 이번 국제회의에서 사전 채택되었다. 차량용 카메라, 센서 등 차량 내부망의 데이터 양이 증가함에 따라 현재 완성차 업계에서는 차량용 이더넷의 도입을 추진 중이며, 이러한 환경에서 이 표준이

차량 네트워크 보안 지침으로 널리 참고 가능할 것으로 기대된다.
사전 채택된 국제표준은 일반적으로 TAP(Traditional Approval Process) 또는 AAP(Alternative Approval Process)의 승인 절차를 거쳐 최종승인된다. 표준에 정책 및 규제적 내용이 포함된 경우 TAP 승인 절차를, 일반적인 기술을 다루는 경우 AAP 승인 절차를 거쳐 국제표준으로 채택된다. TAP로 사전 채택된 2건의 권고안 X.1380과 X.1381은 향후 3개월간 국가별 의견수렴 과정을 거치며, 반대하는 국가가 없을 경우 2023년 2월말 개최될 SG 17 국제회의에서 국제표준 채택 여부를 결정한다. AAP로 사전 채택된 1건의 권고안(X.1377)은 4주간의 의견 수렴 기간(LC, last call)을 거쳐 이견이 없으면 바로 국제표준으로 최종 채택될 예정이다.

2.3 신규 표준화 과제 승인 (3건)
한국은 양자암호통신, ITS 보안 분야 등에서 신규 표준화 과제를 제안하여 <표 3>과 같이 3건이 승인되었으며, 향후 주도적 표준 개발을 위한 에디터쉽을 확보하였다.

<표 3> 신규 표준화 과제 승인 및 에디터쉽 확보

No.	표준 번호	표준 제목	에디터(소속)	비고 (승인절차)
1	X.sec_QKDNi	양자 키 분배 네트워크 상호연동 보안 요구 사항	심동희(SK텔레콤)	AAP
2	X.evpnc-sec	차량ID를 이용한 전기차 충전 서비스 보안 가이드라인	여기호(현대오토에버), 염흥열, 박성채(순천향대)	TAP
3	X.sup.cv2x-sec	초고신뢰 초저지연 통신을 지원하는 C-V2X 서비스 운영을 위한 보안 위협 및 구성 시나리오(X.1813 부속서)	신성기,오재언(맥데이타), 김영재(TTA), 염흥열(순천향대)	Agreement

첫 번째 신규 표준화 과제는 '양자 키 분배(QKD, Quantum key distribution) 네트워크 상호연동 보안 요구사항(X.sec_QKDNi)'이다. SKT가 지난 5월 SG17 국제회의에서 신규 과제를 제안하였으나 기반 표준인 SG13(미래 네트워크)의 QKD 네트워크 상호연동 프레임워크(ITU-T Y.3810)가 당시 표준으로 제정되지 않아 SG17에서 신규 표준화 과제 승인이 연기되었다. 이후 SG13의 기반 표준 Y.3810이 7월에 최종승인되었고, 이에 이번 8월 SG17 국제회의에서 Y.3810에 대한 보안 요구사항이 신규 표준화 과제로 승인되었다. 이 표준은 이기종 QKD 네트워크 연동을 위해 보안 위험을 분석하고, 인증 및 인가 등을 포함한 보안 요구사항을 제시할 계획이다. 양자 키 분배 네트워크 연동을 위해 보안 디지털 금융서비스 비즈니스 모델, 에코시스템 구성요소를 식별하고, 디지털 금융서비스에서 발생 가능한 보안 위협 및 요구사항을 개발할 계획이다. 이 표준은 양자 키 분배 네트워크 연동을 위한 핵심 표준으로 양자 키 분배 기술 보급과 대중화에 크게 기여할 것으로 기대된다.
두 번째 신규 표준화 과제는 '차량ID를 이용한 전기차 충전 서비스 보안 가이드라인(X.evpncsec)'이며, 현대오토에버와 순천향대가 공동으로 제안하였다. 최근 전기차가 세계적으로

널리 보급됨에 따라 전기차 충전 서비스에서 발생 가능한 보안 위협에 대응하고자 신규 표준화 과제를 제안하였다. 보다 이 표준에서는 전기차 충전을 위한 PnC(Plug&Charge) 서비스에서 차량을 인증하기 위해 분산 신원증명(Decentralized Identity)을 적용한 서비스 모델을 제안하고, 그에 대한 보안가이드라인을 제공하고자 한다. 전기차 충전 서비스 모델에 대한 구체적인 보안 표준인만큼 향후 관련 산업계에서 실질적으로 유용하게 참고 가능할것으로 예상된다.
세 번째 신규 표준화 과제는 '초고신뢰 초저지연 통신(URLLC)을 지원하는 C-V2X 서비스 운영을 위한 보안 위협 및 구성 시나리오(X.1813 부속서)'로, 맥데이타와 TTA, 순천향대가 함께 신규표준화를 제안하였다. 이 표준은 X.1813(초고신뢰 초저지연 통신을 지원하는 IMT-2020 기반 버티컬 서비스 보안 요구사항)에서 개발된 URLLC 버티컬 서비스에 관한 보안 요구사항 및 기능을 C-V2X 서비스로 확장 적용하기 위하여 신규 표준화 과제를 제안하였다. 구체적으로 이 표준에서는 C-V2X 서비스 관련 보안 위협을 분석하고, C-V2X 서비스용 네트워크 모니터링을 활용한 보안 구성 시나리오를 정의할 계획이다. 이 표준이 제정되면 국내 안양시 신호등 체계 등에 적용된 사례에 기반하여 국내외 산업계가 C-V2X 서비스에 적용 가능한 보안 구성 시나리오를 널리 참고할 것으로 기대한다.

3. 맺음말

한국은 이번 SG17 국제회의의 성과로 소개한 5G 보안, IoT 보안, 지능형차량통신 보안, 양자암호통신 분야 외에도 사이버보안, 악성코드 및 스팸대응, 데이터 비식별화, 감염병 추적 관리, 신원 관리 및 텔레바이오 인식 등 다양한 분야에 대한 지속적인 기고를 통해 왕성한 국제표준화 활동을 추진하고 있다. 국제표준은 단시간에 개발되지 않는다. 신규 기술에 대해 사전에 보안 위협을 식별하고 이를 분석 및 대응하기 위해 다년간 연구개발한 결과로 국제표준이 제정되고 있다. 이러한 SG17의 지속적이고 체계적인 국제표준화 활동은 국내 SG17 연구반(반장:순천향대 염흥열 교수)을 중심으로 현대자동차, SK텔레콤, 서울외대, 고려대, 한국전자통신연구원, 한국인터넷진흥원 등 산학연의 적극적 활동에 기반하고 있다. 특히 대기업뿐 아니라 맥데이타, 이스톰, 기원테크 등 국내 중소 중견기업이 SG17 표준화에 적극적으로 참여하고 있으며, 우리 기업의 고유 보안 기술을 국제표준으로 연결함으로써 국내 보안산업의 글로벌 경쟁력 확보 및 수출 증대에 일조할 것으로 기대된다. 향후에도 국내 SG17 연구반은 산학연 전문가들의 유기적 협력을 바탕으로 한국의 우수한 정보보호 기술을국제표준에 반영하기 위해 적극적인 국제 활동을 추진할 계획이다.
차기 SG17 국제회의는 2023년 2월말 스위스 제네바에서 개최될 예정이며, 이후 2023년 8월에는 한국에서 SG17 국제회의를 개최하는 것을 추진하고자 한다. 한국이 SG17 국제의장을 필두로 하여 총 17석의 국제의장단을 수임하고 있으며, 정보보호 분야 국제표준을 주도적으로 개발하고 있는 만큼 2023년 8월 SG17 국제회의 개최를 통해 향후에도 괄목할만한 정보보호 표준화 성과들이 도출될 것을 기대한다.

※ 이 연구는 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행됨[No.2022-0-00009, ICT 국제공식표준화 대응 및 국가표준 연구]

[주요 용어 풀이]

- UN (United Nations): 정치, 경제, 사회, 문화 등 모든 분야에서 국제협력을 증진 시키는 역할을 하는 국제기구
- ITU (International Telecommunication Union): 국제전기통신연합으로, 국제 주파수, 위성궤도, 표준, 개도국 지원 등을 수행하는 국제연합 산하의 세계 최대·최고 정보통신기술 전문 국제기구
- UNECE (United Nations Economic Commission for Europe): 유럽경제위원회
- ITS (Intelligent Transport System): 지능형 교통 시스템
- 부속서 (Supplement): 표준에 보완적이거나 관련이 있지만, 이해 및 구현에 필수적이지 않은 문서
- URLLC (Ultra-Reliable and Low Latency Communications): 초고신뢰·초저지연 통신

[참고문헌]

[1] 맥데이타 5G 보안 기술, ITU 국제표준화 과제 채택
https://www.datanet.co.kr/news/articleView.html?idxno=150358
[2] 삼성·화웨이도 볼 '한국 주도' 국제 5G 보안 바이블. 어떻게 만들어졌나
https://www.bloter.net/newsView/blt202205270106
[3] KISA IoT 보안기준, ITU-T 국제표준으로 최종 채택
https://www.boannews.com/media/view.asp?idx=109602
[4] TTA 저널 199호, 지능형 자율자동차 통신 보안 표준화 동향
https://www.tta.or.kr/tta/publicationHosuView.do?key=80&rep=1&searchKindNum=1&searchHosu=199
[5] ITU-T SG17, Security,
https://www.itu.int/en/ITU-T/studygroups/2022-2024/17/Pages/default.aspx

※ 출처: TTA 저널 제203호