정 보 보 호 학 회 지
제 33 권 제4호, 2023. 8

ITU-T SG17(보안) 국제 표준화 회의 주요 결과 및 차기 연구회기(2025-2028)를 위한 구조조정 논의

고 재 남*, 박 성 채*, 오 흥 룡**, 염 흥 열*

요 약

국제전기통신연합(ITU)은 국제연합(UN) 산하 정보통신기술(ICT)에 대한 전문 국제 표준화기구이다. 193개 회원국, 약 900개 기업 및 학계 멤버 등으로 구성되어 있으며, 산하에 전기통신표준화부문(ITU-T), 전기통신개발부문(ITU-D), 그리고 전파통신 부문(ITU-R) 등 3개의 부문으로 구성되어 있다[1]. ITU-T는 역할과 임무에 따라 11개의 연구반 (SG, Study Group)으로 구성되어 있으며, 각 업무에 맞는 선도 그룹(Lead Study Group)을 지정하여 국제 표준을 개발하고 있다. 정보보안 분야 국제 표준은 ITU-T SG17(보안)에서 담당한다[2]. ITU-T 국제 표준화 조직은 4년 주기의 연구회기(Study Period)로 연구반 구조조정, 의장단 선출 및 표준화 추진 방향을 WTSA(World Telecommunication Standardization Assembly) 총회에서 결정한다. 다음 총회는 2024년 10월에 인도에서 열릴 예정이다.

본 논문에서는 지난 2022년 8/9월과 2023년 2/3월 스위스 제네바에서 열린 ITU-T SG17 회의에서 한국이 주도적으로 수행한 정보보호 표준화 활동 결과를 알아보고, 차기 연구회기(2025-2028)를 위한 SG17 구조조정에 대해 2023년 2/3월 SG17 회의 결과와 서신 그룹(CG, 5월-7월) 회의의 주요 결과를 중심으로 제시한다.

Ⅰ. 서 론

ITU-T SG17(보안, 의장: 순천향대 염흥열교수)은 ITU-T 내 정보보호 기술에 대한 국제 표준을 개발하는 연구반(Study Gruop)이다. 지난 2022년 8/9월(2022. 8. 23 ~ 9. 2)과 2023년 2/3월(2023. 2. 21 ~ 3. 3) 스위스 제네바에서 개최된 SG17 회의에서는 다수의 국제 표준 최종 승인과 국제 표준 사전 채택, 신규 표준화 과제 승인이 있었다. 최근 지능화·조직화되는 사이버 공격을 막기 위한 호환성 있는 대응 기법에 대한 사이버 보안 분야 국제 표준의 중요성이 매우 강조되고 있다.

본 논문 제2장에서는 2022년 8월 이후 수행된 SG17 국제 표준화 활동의 주요 결과와 2023년 2/3월 회의 이후 진행된 차기 연구회기(2025-2028)를 위한 SG17 구조조정 (Restructuring) 논의 결과를 제시한다. 제3장은 본 논문의 결론과 향후 대응 방안을 제시한다.

Ⅱ. ITU-T SG17 국제 표준화 활동 현황과 차기 연구회기(2025-2028) 위한 SG17 구조조정 논의

2.1. 현 연구회기 (2022-2024) SG17 의장단 명단

[표 1] 은 현 연구회기 ITU-T SG17 의장단 명단이다. 이 의장단은 2022년 3월 WTSA-20에서 선출되었다.

〔표 1〕 SG17 의장단 (연구회기 2022~2024)

이름	국가	직위
염흥열	대한민국 (순천향대)	의장
Samir Gaber ABDEL-GAWAD	이집트	부의장
Laialy A. ALMANSOURY	쿠웨이트	부의장
Afnan AL-ROMI	사우디 아라비아	부의장

본 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임.[*No.2021-0-00112, 차세대보안 표준전문연구실, **No.2022-0-00013, ICT 국제표준화 전문가 양성 및 역량 강화]

* 순천향대학교 정보보호학과/차세대보안 표준전문연구실 (선임연구원, jnko@sch.ac.kr, 선임연구원, zoesc.park@sch.ac.kr, 교수, hyyoum@sch.ac.kr)
** 한국정보통신기술협회 표준화본부 (수석연구원, hroh@tta.or.kr)

이름	국가	직위
Abdenour BOURENNANE	알제리	부의장
Gökhan EVREN	터키	부의장
Yutaka MIYAKE	일본	부의장
Lía MOLINARI	아르헨티나	부의장
Kwadwo Gyamfi OSAFO-MAAFO	가나	부의장
Greg RATTA	미국	부의장
Pushpendra Kumar SINGH	인도	부의장
Arnaud TADDEI	영국	부의장
Wala TURKI LATROUS	투니지	부의장
Liang WEI	중국	부의장

2.2. 2022년 8/9월 ITU-T SG17 회의 주요 결과 [3]

본 절에서는 2022년 8/9월 ITU-T SG17 국제 표준 회의에서 논의되었던 주요 결과에 대해 살펴본다.

2.2.1. 국제 표준 최종 승인 (4건)

[표 2] 는 2022년 8/9월 SG17 국제회의에서 최종 승인된 5G 보안, 사물인터넷 보안 분야 등에서 한국이 주도적으로 개발해 온 국제표준이다.

〔표 2〕 한국 주도 국제 표준 최종 승인

표준 번호	표준 제목	에디터(소속)
X.1813	초고신뢰 초저지연 통신을 지원하는 IMT-2020 기반 버티컬 서비스 보안 요구사항	신성기, 오재언 (맥데이타) 염흥열(순천향대)
X.1814	IMT-2020 통신 시스템에 대한 보안 지침	염흥열(순천향대) 박근덕(서울외대) 김미연(NSHC)
X.1352	사물인터넷 기기 및 게이트웨이의 보안 요구사항	이상걸, 류호석 (한국인터넷진흥원) 정원석, 방지호 (한국기계전기전자 시험연구원)
X.Sup pl.38	감염병 확산 방지를 위한 접촉자 추적 애플리케이션 사용 사례	염흥열, 박성채, 김미연(순천향대)

■ 초고신뢰 초저지연 통신을 지원하는 IMT-2020 기반 버티컬 서비스 보안 요구사항 (ITU-T X.1813)

이 국제표준은 IMT-2020 사설 네트워크에서 초고신뢰·저지연 통신 (URLLC, Ultra-Reliable and Low Latency Communications) 를 지원하는 버티컬 서비스를 제공할 때 발생하는 보안 위협과 위험을 식별하고, IMT-2020 사설망의 보안 구축 시나리오를 설명한다. 또한 IMT-2020 사설망 기반의 융합 서비스 환경에서 네트워크 장애·성능·보안 모니터링을 위한 주요 구성요소와 아키텍쳐를 정의하고 보안 기능을 제공한다 [4].

■ IMT-2020 통신 시스템에 대한 보안 지침 (ITU-T X.1814)

이 국제표준은 IMT-2020 시스템에서 발생할 수 있는 보안 위협을 식별하고 이를 대처하기 위한 보안 능력을 제시한다. 이 국제 표준은 순천향대가 2019년 2월 SG17 회의에서 제안하여 2022년 8월까지 한국의 IMT-2020 보안 기술을 국제 표준으로 반영하기 위해서 매 회의마다 기고서를 제출하였다. 그 결과 2022년 8/9월 SG17 회의에서 국제 표준으로 채택된 바 있다. 이 국제 표준은 ITU-T에서 IMT-2020 시스템 개발자와 운영자를 위한 지침으로 활용될 수 있다. IMT-2020 통신 시스템에 대한 보안 지침 (ITU-T X.1814) 은 사용자가 보유한 스마트폰, 통신 기지국과 스마트폰을 연결하는 액세스 네트워크, 코어 네트워크 등에서 발생할 수 있는 전반적인 보안 위협과 IMT-2020 통신 시스템의 각 구성요소를 식별하고 이를 보호할 수 있는 보안 능력에 대한 지침을 제시한다 [5].

■ 사물인터넷 기기 및 게이트웨이의 보안 요구사항 (ITU-T X.1352)

사물인터넷 기기 및 게이트웨이의 보안 요구사항은 보안 게이트웨이를 사용하는 사물 인터넷(IoT)의 보안 프레임워크를 제공한다. 한국이 주도로 개발한 'IoT 보안 프레임워크 (X.1361)'를 기반으로 한국의 IoT 보안 시험 및 인증 기준 [6] 을 2018년 9월에 신규 표준화 과제로 제안해 채택되었고, 이후 한국인터넷진흥원과 한국기계전기전자시험연구원의 전문가가 에디터로활동하며 다수의 기고서를 제출하였고, 순천

향대학교도 중요한 용어 정의를 포함한 기고서를 여러 차례 제출한 바 있다. 각국의 의견을 반영하는 등 활발한 논의를 통해 2022년 8/9월 SG 17 회의에서 국제 표준으로 최종 승인되었다. 이는 2017년 12월 이후 국내에서 시행중인 IoT 보안인증 제도의 평가 기준을 ITU-T 국제 표준으로 개발한 훌륭한 사례라 할 수 있다 [7].

■ 감염병 확산 방지를 위한 접촉자 추적 애플리케이션 사용 사례 부속서 (ITU-T X.Suppl.38)

이 부속서는 ITU-T X.1152를 보완하는 것으로, 순천향대가 2020년 8/9월 SG17 회의에서 신규 표준과 과제로 제안했으며, 코로나19 확산 방지를 위한 접촉자 추적 애플리케이션의 사용 사례를 제공한다. 이 부속서는 접촉자 추적 애플리케이션을 정의하고, 전염병에 감염되었을 가능성이 있는 사람과 접촉한 사람을 식별, 평가, 관리하여 추가 확산을 막을 수 있는 기술을 제공한다. 이러한 애플리케이션은 잠재적 노출로 인해 다른 사람보다 고위험군에 속하는 사람을 사전에 찾아내어 가능한 경우 알리고 필요한 경우 격리함으로써 감염병의 확산을 방지하는 데 도움이 된다. 이 부속서는 접촉자 추적 애플리케이션에서 처리되는 데이터와 관련된 잠재적 보안 위험을 줄이는 것을 고려하여 수동 알림 방법 외에도 감염 가능성이 있는 사용자를 자동으로 추적하고 알리는 상호 운용 가능한 시스템을 제시한다. 또한 접촉자 추적 애플리케이션의 다양한 사용 사례를 설명하고, 데이터 처리 흐름을 포함한 데이터 처리 모델을 제공하며, 보안 및 PII 보호 관점에서 위협과 위험을 식별한다 [8].

2.2.2. 국제 표준 사전 채택 (3건)

〔표 3〕 한국 주도 국제 표준 사전 채택

표준 번호	표준 제목	에디터(소속)	승인 절차
X.1377	커넥티드 자동차 침입방지 시스템을 위한 가이드라인	김휘강, 정성훈(고려대), 이상우(ETRI), 박승욱(현대자동차)	AAP
X.1380	클라우드 기반 차량 데이터 저장장치 보안 가이드라인	이상우(ETRI), 박승욱(현대자동차)	TAP
X.1381	이더넷 기반 차내망 보안 가이드라인	이상우(ETRI), 이유식(이타스코리아)	TAP

2022년 8/9월 SG17 국제회의에서는 [표 3] 과 같이 3건의 국제표준이 사전 채택 되었다.

■ 커넥티드 자동차 침입방지 시스템을 위한 가이드라인 (ITU-T X.1377)

커넥티드 자동차 침입방지 시스템을 위한 가이드라인 (ITU-T X.1377) 은 커넥티드 차량에 침입을 탐지하기 위해 위협을 식별하고 이를 능동적으로 대응하기 위한 지침과 사용 사례를 제공한다 [9]. 이 표준은 커넥티드 차량 침입에 대한 능동적 대응 기능 측면에 초점을 맞추었다. 또한 한국이 개발한 '차량 내부 네트워크용 침입탐지시스템 가이드라인 (ITU-X.1375)' 에 기반한다. 이 국제표준은 2022년 8/9월 SG17 회의 이후, 4주간의 AAP (Alternative Approval Process) 최종 의견 수렴 (Last Call) 후, 의견이 없어 국제표준으로 채택되었다.

■ 클라우드 기반 차량 데이터 저장장치 보안 가이드라인 (ITU-T X.1380)

이 표준은 클라우드 기반 차량 데이터 저장 시스템에 대한 기술적 고려사항, 보안 요구사항 및 사용 사례를 제공한다 [10]. 2018년 8월 ETRI, 현대자동차가 신규 표준화 과제로 제안해 채택되었으며, 2022년 8/9월 SG17 회의에서 사전채택 되었다.

■ 이더넷 기반 차내망 보안 가이드라인 (ITU-T X.1381)

이더넷 기반 차내망 보안 가이드라인 (ITU-T X.1381) 은 차량용 이더넷 환경에서의 보안 위협을 식별하고, 이에 대한 보안 요구사항과 사용 사례를 제시한다 [11]. 이 표준은 2018년 8월 한국전자통신연구원과 이타스코리아가 신규 표준화 과제로 제안해 개발해 왔다.

2.2.3. 신규 표준화 과제 승인 (3건)

한국은 [표 4] 과 같이 양자암호통신, ITS 보안 분야 등에 대한 신규 표준화 과제를 제안하여 채택되었으며, 향후 주도적인 표준 개발을 위해 에디터쉽을 확보하였다.

〔표 4〕 신규 표준화 과제 승인 및 에디터쉽 확보

표준 번호	표준 제목	에디터(소속)	승인 절차
X.sec_QKDNi	양자 키 분배 네트워크 상호연동 보안 요구 사항	심동희(SK텔레콤)	AAP
X.evpnc-sec	차량ID를 이용한 전기차 충전 서비스 보안 가이드라인	여기호(현대오토에버) 염흥열, 박성채(순천향대)	TAP
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

■ 양자 키 분배 네트워크 상호연동 보안 요구 사항 (ITU-T X.sec_QKDNi)

‘양자 키 분배(QKD, Quantum key distribution) 네트워크 상호연동 보안 요구사항 (X.sec_QKDNi)’은 양자 키 분배 네트워크 상호연동을 위한 위협을 식별하고 인증과 인가 측면을 포함한 보안 요구사항을 제시한다 [12]. 이 국제표준은 STK에서 2022년 9월 SG17 회의에 신규 표준화 과제로 제안해 채택되었다.

■ 차량 ID를 이용한 전기차 충전 서비스 보안 가이드라인(X.evpnc-sec)

이 국제표준은 현대오토에버와 순천향대가 공동으로 제안해 신규 표준화 과제로 채택되었다. 플러그 앤 차지 (PnC, Plug&Charge) 서비스에서 차량을 인증하기 위해 분산 신원증명 (Decentralized Identity)을 적용한 서비스 모델을 제안하고, 그에 대한 보안 가이드라인을 제공한다. 이 표준은 플러그 앤 차지 서비스를 이용한 충전 및 과금 과정에서 탈중앙화된 신원을 활용해 전기차와 소유자를 인증하는 서비스 모델에 초점을 맞춤으로써 X.509 기반의 PKI 인증서를 이용한 전기차와 충전 장비 간 인증 방법을 제시한 ISO 15118 와 차별화 된다 [13].

■ 초고신뢰·저지연 통신(URLLC)을 지원하는 C-V2X 서비스 운영을 위한 보안 위협 및 구성 시나리오 (X.1813 부속서)

‘초고신뢰 초저지연 통신(URLLC)을 지원하는 C-V2X 서비스 운영을 위한 보안 위협 및 구성 시나리오 (X.1813 부속서)’ 는 맥데이타, TTA, 순천향대가 공동으로 신규 표준화 과제를 제안해 채택되었다. 이는 ITU-T X.1813의 부속서로 개발 중이며, C-V2X 서비스 관련 보안 위협을 분석하고 C-V2X 서비스용 네트워크 모니터링을 활용한 보안 구성 시나리오를 정의한다 [14].

2.3. 2023년 2/3월 ITU-T SG17 회의 주요 결과 [15]

본 절에서는 2023년 2/3월 SG17 회의에서 논의되었던 주요 결과에 대해 살펴본다. 국제 표준 최종 승인 2건과 국제 표준안 사전채택 2건, 신규 표준화 과제 승인 5건의 주요 결과가 있었다.

2.3.1. 국제 표준 최종 승인 (2건)

2022년 8/9월 SG17 회의에서 TAP (Traditional Approval Process) 로 사전 채택된 2건의 국제표준은 [표 5] 와 같이 국가별 의견을 반영한 후 최종 채택되었다.

〔표 5〕 한국 주도 국제 표준 최종 승인

표준 번호	표준 제목	에디터(소속)	승인 절차
X.1380	클라우드 기반 차량 데이터 저장장치 보안 가이드라인	이상우(ETRI), 박승욱 (현대자동차)	TAP
X.1381	이더넷 기반 차내망 보안 가이드라인	이상우(ETRI), 이유식 (이타스코리아)	TAP

2.3.2. 국제 표준 사전 채택 (2건)

2023년 2/3월 SG17 회의에서 사전 채택된 국제표준은 [표 6] 과 같다.

〔표 6〕 국제 표준안 사전 채택

표준 번호	표준 제목	에디터(소속)	승인 절차
X.1771 (X.rdda)	데이터 비식별화 보증 요구사항	강이석(KISA), 염흥열(순천향대), 임형진(금융보안원) 등	TAP
X.1471 (X.websec-7)	온라인 분석 서비스를 위한 참조 모니터	박종열(서울과기대), 나재훈(ETRI)	TAP

■ 데이터 비식별화 보증 요구사항 (ITU-T X.1771/X.rdda)

데이터 비식별화 보증 요구사항 (ITU-T X.1771)은 데이터의 안전한 활용을 위해 데이터 비식별화를 위한 보증 요구사항을 제시한다 [16]. 이 표준은 2019년 1월 KISA, 금융보안원에서 신규 표준화 과제로 제안해 채택되었다. 그 이후 순천향대와 KISA가 공동으로 이 국제 표준을 지속적으로 개발해, 2023년 2/3월 SG17 회의에서 채택되었다.

■ 온라인 분석 서비스를 위한 참조 모니터 (ITU-T X.1471/X.websec-7)

온라인 분석 서비스를 위한 참조 모니터 (ITU-T X.1471) 는 비인가 데이터 사용을 탐지하기 위해 빅데이터 분석과 운영을 위한 참조 모델을 제시한다. 이 국제 표준은 빅데이터를 분석할 때 발생하는 보안 위협을 식별하고 접근 제어 메커니즘을 이용해 이러한 위협을 완화하고 해결할 수 있는 보안 고려사항을 제공한다 [17]. 이 표준은 2014년 8월 ETRI가 신규 표준화 과제로 제안하였으며, 2023년 2/3월 SG17 회의에서 사전 채택되었다. 향후 국제 표준으로 최종 승인되면, 온라인 서비스 제공자를 위한 안전한 데이터 활용 기반의 맞춤형 서비스와 온라인 분석 서비스에 활용될 수 있을 것으로 예상한다.

2.3.3. 신규 표준화 과제 승인(5건)

한국은 2023년 2/3월 SG17 회의에서 [표 7] 과 같이 소프트웨어 공급망 보안, ITS 보안, 양자통신 보안 등 신흥 보안 주제와 관련해 5건의 신규 표준화 과제를 제안하였으며 모두 채택되었다.

■ 소프트웨어 공급망 보안 위협 (ITU-T X.st-ssc)

‘소프트웨어 공급망 보안 위협 (ITU-T X.st-ssc) 은 순천향대가 제안하여 채택된 신규 표준화 과제로, 점점 중요성이 인식되고 있는 소프트웨어 공급망 보안 분야에서 최초의 ITU-T 신규 표준화 과제이다. 이 국제 표준은 소프트웨어 공급망 보안에 대한 상위 수준의 원칙을 제시하고, 소프트웨어 개발 생명주기를 고려한 보안 위협과 소프트웨어 공급망에서의 이해관계자를 식별한다 [18]. ‘소프트웨어 공급망 보안 위협 (ITU-T X.sc-ssc)’ 의 신규 표준화 과제 채택은 향후 소프트웨어 공급망에 대한 보안 통제와 요구사항 등을 포함하는 각종 추가 권고를 개발하는데 기반이 될 수 있다. 또한 과기부가 2022년 신설한 제로트러스트

〔표 7〕 신규 표준화 아이템 승인 및 에디터쉽 확보

표준 번호	표준 제목	주요 내용	에디터(소속)	승인 절차
X.st-ssc	소프트웨어 공급망 보안 위협	- 소프트웨어 개발 생명주기 상 이해관계자 및 공급망 보안 위협 식별 - 공급망 공격 예시 및 위험 관리 방안 제안	염흥열, 박성채 (순천향대)	TAP
X.ota-sec	커넥티드 차량의 무선(OTA) 업데이트 기능을 지원하기 위한 보안 기능 구현 및 평가	- 무선 업데이트 기능을 지원하는 커넥티드 차량에 대한 보안 위협 분석	이유식(순천향대) 우사무엘(단국대) 이상우(ETRI) 박승욱(현대자동차)	AAP
X.bvm	생체정보 변동 관리에 대한 요구사항	- 생체정보 변동 대한 적응 기술 개요 소개 - 생체정보 변동 관리를 위한 요구사항 제시	박은정(연세대) 김재성(KISA)	AAP
TR.hyb-qsafe	양자 내성 통신을 위한 하이브리드 키 관리 개요	- 양자키분배 기술과 양자내성암호를 함께 사용한 키 관리 시나리오	심동희(SKT)	Agree-ment
X.suppl.tig-iotsec	IoT 기기 및 게이트웨이 기술적 구현 가이드라인	- IoT 기기 및 게이트웨이 제조업체가 보안 요구사항 구현 시 참고가능한 기술적 지침 제시	염흥열, 박성채 (순천향대)	Agree-ment

및 소프트웨어 공급망 보안 포럼을 정책적으로 지원할 수 있고, 공개 소프트웨어 공급망이 전세계적으로 연결되고 그 활용 비중이 날로 높아지면서 관련 보안 체계가 긴요한 시점임을 고려할 때 의미하는 바가 크다고 할 수 있다.

■ 커넥티드 차량의 무선(OTA) 업데이트 기능을 지원하기 위한 보안 기능 구현 및 평가 (ITU-T X.ota-sec)

커넥티드 차량에서 무선 업데이트 기능을 지원하기 위한 보안 기능의 구현 및 평가 (ITU-T X.ota-sec)는 순천향대와 한국전자통신연구원, 현대자동차, 단국대에서 공동으로 제안해 채택된 신규 표준화 과제이다. 이 표준은 커넥티드 차량의 무선 업데이트 기능을 지원하기 위해 암호화 알고리즘 사용, 보안 진단, 디버깅 및 보안 저장 기능이 포함된 보안 기능을 식별하고 이러한 기능을 평가하는 방법을 제공한다 [19].

■ 생체정보 변동 관리에 대한 요구사항 (ITU-T X.bvm)

이 국제 표준은 생체 인식 또는 생체 인증 시스템의 정확성과 신뢰성을 향상 시키기 위해 연결된 정보 시스템과 적응형 솔루션을 활용하여 생체 정보의 변동 관리에 대한 지침을 제공한다 [20]. 이 표준은 연세대와 한국인터넷진흥원이 신규 표준화 과제로 제안해 채택되었다.

■ 양자 내성 통신을 위한 하이브리드 키 관리 개요 (ITU-T TR.hyb-qsafe)

양자 내성 통신을 위한 하이브리드 키 관리 개요 (ITU-T TR.hyb-qsafe)는 SKT가 신규 표준화 과제의 기술 보고서로 제안해 채택되었다. 이 기술 보고서는 양자 내성 통신을 위한 QKD (Quantum Key Distribution) 와 PQC (Post Quantum Cryptography) 기반의 하이브리드 접근 방식의 키 관리를 기술한다. 이를 위해 하이브리드 접근 방식의 키 관리 사례 연구와 사용 사례, 관련 서비스 시나리오 및 키 관리에 대한 고려 사항을 제공한다 [21].

■ IoT 기기 및 게이트웨이 기술적 구현 가이드라인 (ITU-T X.suppl.tig-itosec)

IoT 기기 및 게이트웨이 기술적 구현 가이드라인 부속서는 IoT 기기 및 게이트웨이 제조업체가 활용할 수 있는 보안 요구사항에 대한 기술적 구현 가이드라인을 제공한다. 이 부속서는 순천향대가 제안해 신규 표준화 과제 부속서로 채택되었으며, 한국인터넷진흥원이 개발한 IoT 기기 및 게이트웨이 (ITU-T X.1352)가 제공하는 보안 요구사항을 보완(supplement)한다 [22].

2.4. 차기 연구회기를 위한 ITU-T SG17 구조조정 논의

2.4.1. 2023년 2/3월 SG17 논의 결과 [23]

2023년 2/3월 ITU-T SG17 회의에서 한국은 앞서 소개한 지능형차량통신 보안, 데이터 비식별화, 소프트웨어 공급망 보안 분야 표준 성과들 이외에도 분산원장기술 보안, 양자통신 보안, 악성코드 및 스팸대응, 신원 관리 및 텔레바이오인식 등 정보보호의 기반 및 신규 기술에 대한 지속적인 기고 제출과 논의를 통해 활발한 국제 표준화 활동을 추진하였다. 또한 차기 연구회기를 위한 SG17 구조조정 원칙, 신흥 표준화 주제, 그리고 신규 표준화 주제의 추진 방안 등의

〔표 8〕 SG17 구조조정 원칙

원칙	내용
1	***Not fragmented*** : ITU-T SG17 구조는 ITU-T 보안 작업이 단편화되지 않도록, 즉 ITU-T 보안이 독립적이고 별도의 전용 연구반에 의해서 수행되어야 한다.
2	***Flexibility and openness for new emerging security technologies*** : ITU-T SG17 연구과제 구조는 신흥 보안 기술을 적시에 수용할 수 있는 유연성과 개방성을 가져야 한다.
3	***Visibility*** : ITU-T SG17의 연구과제 제목과 표준화 영역은 ITU-T 내·외부에 명확히 나타나야 한다.
4	***Coordination and collaboration*** : SG17이 보안에 대한 핵심 센터 역할을 수행하기 위해서 SG17의 각 연구과제의 작업은 다른 표준화 기구들과 조정하고 협력해야 한다.
5	***Enhancement of effectiveness to increase participation from developing countries*** : ITU-T SG17 연구과제는 개발도상국의 참여를 장려하도록 개선되어야 한다.
6	***Balance among Questions*** : ITU-T SG17 연구과제 활동은 역할과 책임, 연구과제의 아이템 또는 참가자 수 등의 측면에서 균형을 이루어야 한다.

정책 기고를 제출해 미국 등의 주요국의 폭 넓은 지지를 받았고 지속적인 논의를 위한 바탕을 마련했다. [표 8] 은 합의된 차기 연구회기를 위한 SG17 구조조정 원칙을 보여준다. 차기 연구회기를 위한 표준화 주제, 표준화 주제의 수행 방법 등은 한국의 제안이 기본적으로 반영되었으나 세부 사항에 대해서는 WTSA-24 준비를 위한 서신 그룹 (의장 염흥열 교수) 활동을 통해 계속 논의하기로 합의했다.

2.4.2. 서신 그룹(CG) 논의 결과 및 향후 논의 전망

WTSA-24 준비를 위한 서신 그룹(CG) 회의는 2023년 5월부터 7월까지 의장인 염흥열 교수의 주재하에 총 7번의 원격 회의가 진행되었다. [표 9] 는 서신 그룹에서 진행한 다섯가지 논의 주제(DP)이다 [24]. 서신 그룹에서는 위 다섯가지 논의 주제에 대해서 심도 깊은 토의와 제안이 수행되었다. 특히 차기 연구회기(2025-2028)를 위한 SG17의 역무, 리드 연구반 역할, SG17 연구 지침 포인트, 연구과제의 역무 등에 대한 초기 텍스트가 논의 됐으며, 이를 바탕으로 계속 논의를 진행하기로 했다. 또한 메타버스 보안에 대한 신규 연구과제와 디지털 트윈 보안 및 데이터 보호 기술에 대한 분할된 연구과제 설립 가능성에 대한 폭넓은 논의가 진행되었다.

[표 10] 은 서신 그룹에서 합의한 22가지 신흥 표준화 주제를 나타낸다 [24]. 그리고 이 외 논의 주제는 2023년 8/9월 한국에서 개최될 SG17 회의에서 계속적으로 논의될 예정이다.

다가오는 8/9월 한국 SG17 회의에서는 [표 9] 의 나머지 네가지 논의 주제 (DP2 - DP5)에 대해서 회원국들의 기고서를 바탕으로 심도 깊게 논의될 예정이다.

〔표 9〕 서신 그룹(CG) 논의 내용

번호	논의 주제	비고
DP1	차기 연구 기간(2025-2028년)을 위한 SG17의 새로운 표준화 연구 주제	합의
DP2	차기 연구 기간(2025-2028년)의 새로운 연구 주제를 SG17 구조에 통합하는 방법	계속 논의
DP3	일반 연구 영역, 리드 연구반 역할, 책임하에 있는 권고사항 목록	계속 논의
DP4	2024년 이후 작업 프로그램 개발에 대한 ITU-T SG17의 지침 포인트	계속 논의
DP5	차기 연구회기(2025-2028)를 위한 SG17 연구과제 텍스트	계속 논의

〔표 10〕 신흥 표준화 주제 (22개)

번호	신흥 표준화 주제
1	메타버스 보안 및 데이터 보호
2	IMT-2030 보안 등 미래 네트워크 보안
3	SBOM(소프트웨어 자재 명세서)을 포함한 소프트웨어 공급망 보안
4	DevSecOps(개발, 보안 및 운영)
5	제로 트러스트(ZT) 아키텍처 (메시 보안)
6	SOAR 등 보안 자동화
7	AI 및 머신 러닝(AI/ML) 데이터 분석
8	데이터 보호를 위한 암호화 알고리즘 사용
9	데이터 마스킹 기술
10	스마트 엔티티를 포함한 섹터 보안
11	디지털 트윈 보안 및 데이터 보호
12	DLT 기반 공개키 기반 구조(DPKI)
13	엔드포인트 보안
14	시뮬레이션 보안
15	플랫폼 보안
16	OT 보안
17	공급망 보안
18	AI 관련 보안
19	QKD 보안
20	생성형 AI 보안
21	RNSS, 위성 등 융복합 네트워크 보안
22	V2X 보안

Ⅲ. 결 론

본 논문에서는 2022년 8/9월 SG17 회의와 2023년 2/3월 SG17 회의에서 한국이 주도적으로 개발해 얻은 표준화 결과와 차기 연구회기(2025-2028)를 위한 구조조정 논의에 대해 살펴보았다. 이를 요약하면 2022년 8/9월 SG17 회의에서는 한국이 주도적으로 개발한 국제 표준 4건이 최종 채택되었으며, 3건의 국제 표준이 사전 채택되었고, 신규 표준화 과제로 3건이 승인되었다. 2023년 2/3월 SG17 회의에서는 한국이 주도적으로 개발한 국제 표준 2건이 최종 채택되었으며, 2건의 국제 표준이 사전 채택되었고, 신규 표준화 과제로 5건이 승인되었다. 또한 차기 연구회

기를 위한 SG17 구조조정에 대한 활동을 요약했으며, 이 사안은 2023년 8/9월 한국 SG17 회의에서 지속적으로 논의가 진행될 예정이다.

2023년 8/9월에 한국에서 개최되는 ITU-T SG17 국제 표준화 회의는 SG17 의장 보유국인 우리나라의 정보보호 국제 표준화 리더십을 강화하고 표준화 인식을 획기적으로 높임으로써 결과적으로 국내 정보보호 산업의 국제 경쟁력을 제고하는 계기를 마련할 수 있을 것이다. 우리나라는 ITU-T SG17 국제 표준화 활동의 지속적인 주도권을 확보하기 위해서 SG17 연구반 의장을 중심으로 정부, 정보보호 산업체, 학계, 공공기관 전문가의 협업과 미국, 영국 등 주요국과의 협력을 추진할 예정이다. 이를 바탕으로 ITU-T 정보보호 국제 표준 활동을 선도할 수 있을 것으로 전망한다.

참 고 문 헌

[1] ITU-T 홈페이지, http://www.itu.int

[2] ITU-T SG17 홈페이지, https://www.itu.int/en/ITU-T/studygroups/2022-2024/17/Pages/default.aspx

[3] 박수정, 염흥열, ITU-T SG17(정보보호, 2022년 8/9월) 국제회의 결과, TTA 저널 203호, 2022. 9/10 https://www.tta.or.kr/tta/preportNewsNDownload.do?sfn=20221108042018654_GysR.pdf

[4] ITU-T X.1813, Security and monitoring requirements for operation of vertical services supporting ultra-reliability and low latency communication (URLLC) in IMT-2020 private networks https://www.itu.int/rec/T-REC-X.1813-202209-I/en

[5] ITU-T X.1814, Security guidelines for IMT-2020 communication systems https://www.itu.int/rec/T-REC-X.1814-202209-I

[6] IoT 공통보안 가이드, 한국인터넷진흥원, 2016.10 https://www.kisa.or.kr/2060205/form?postSeq=2&lang_type=KO&page=

[7] ITU-T X.1352, Security Requirements for Internet of things (IoT) devices and gateway https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1352-202209-I!!PDF-E&type=items

[8] ITU-T X.Suppl.38, ITU-T X.1152-Supplement on use cases for contact tracing technologies to prevent spread of infectious diseases https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=15165

[9] ITU-T X.1377, Guidelines for an intrusion prevention system for connected vehicles https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=15103

[10] ITU-T X.1380, Security guidelines for cloud-based event data recorders in automotive environments https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=15106

[11] ITU-T X.1381, Security guidelines for Ethernet-based in-vehicle networks https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=15107

[12] ITU-T X.sec_QKDNi, Security requirements for Quantum Key Distribution Network interworking (QKDNi) https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18503

[13] ITU-T X.evpnc-sec, Security guidelines for electric vehicle plug and charge (PnC) services using vehicle identity (VID) https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18501

[14] ITU-T X.sup.cv2x-sec, Supplement to X.1813 - Security deployment scenarios for cellular vehicle -to-everything (C-V2X) services supporting ultra-reliable and low latency communication (URLLC) https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18502

[15] 박수정, 염흥열, ITU-T SG17(정보보호, 2023년 2-3월) 국제회의, TTA 저널 206호, 2023. 3/4 https://tta.or.kr/tta/preportNewsNDownload.do?sfn=20230515073743412_gY3w.pdf

[16] ITU-T X.1771(X.rdda), Requirements for data de-identification assurance https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17979

[17] ITU-T X.1471(X.websec-7), Reference monitor for online analytics services https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17965

[18] ITU-T X.st-ssc, Security threats of software supply chain https://www.itu.int/ITU-T/workprog/wp_it

em.aspx?isn=18769
[19] ITU-T X.ota-sec, Implementation and evaluation of security functions to support over-the-air (OTA) update capability in connected vehicles https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18768
[20] ITU-T X.bvm, Requirements for biometric variability management https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18777
[21] ITU-T TR.hyb_qsafe (Overview of key management of hybrid approaches for quantum-safe communications) https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18763
[22] ITU-T X.suppl.tig-itosec, Technical implementation guidelines for IoT devices and gateway https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18767
[23] TD849R1, Report of special session on CG-sg17-wtsa24-prep https://www.itu.int/md/T22-SG17-230221-TD-PLEN-0849/en
[24] TD1178R2, Report of CG-WTSA24-prep (May - July 2023) https://www.itu.int/md/T22-SG17-230829-TD-PLEN-1178/en

〈저 자 소 개〉

고 재 남 (Jae Nam Ko)

순천향대학교 정보보호학과 학사 졸업
순천향대학교 정보보호학과 석사 졸업
순천향대학교 정보보호학과 박사과정
<관심분야> 개인정보보호, 네트워크 보안, 정보보안 국제 표준

박 성 채 (Sungchae PARK)

종신회원

순천향대학교 정보보호학과 학사 졸업
순천향대학교 대학원 정보보호학과 석·박사 과정
2007년 10월~2009년 5월 : 어울림정보기술(주) 연구원
2010년 1월~2011년 5월 : 이글루시큐리티 주임연구원
2020년 2월~2022년 4월 : ㈜보다비 AI연구소 리더
2022년 5월~현재 : 순천향대학교 차세대보안 표준전문 연구실 선임연구원
<관심분야> AI 보안, 암호, 양자암호통신, 블록체인 보안, 5G/6G 보안, 개인정보보호 기술

오 흥 룡 (Heung-Ryong Oh)

종신회원

2002년 2월 : 순천향대학교 전자공학과 학사
2004년 2월 : 순천향대학교 정보보호학과 석사
2018년 2월 : 순천향대학교 정보보호학과 박사
2004년 2월~현재 : 한국정보통신기술협회 표준화본부 수석연구원
2005년 3월~현재 : ITU-T SG17 국내 연구반 간사(역) 및 위원
2009년~2016년 : ITU-T SG17 Q2 Associate Rapporteur
2017년~현재 : ITU-T SG17 Q2 Co-Rapporteur
2011년~현재 : 한국정보보호학회 학회지 편집위원
2012년 8월~현재 : 국방부 국방정보기술표준(DITA) 자문위원
2017년 9월~현재 : 금융결제원 바이오인증 성능위원회 자문위원
2019년 4월~현재 : 용인시 지역정보화위원회 자문위원
<관심분야> 보안프로토콜, 정보보호표준

염 흥 열 (Heung Youl YOUM)
종신회원
한양대학교 전자공학과 학사 졸업
한양대학교 대학원 전자공학과 석사 졸업
한양대학교 대학원 전자공학과 박사 졸업

1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 정보보호학과 정교수
2011년 1월~12월 : 한국정보보호학회 회장(역), 명예회장(현)
2009년~2016년 : ITU-T SG17 부의장
2009년~2016년 : ITU-T SG17 WP3 의장
2017년~현재 : ITU-T SG17 의장
2019년 8월~현재 : 분산신원관리 기술 및 표준화 포럼 의장
2020년 8월 5일~2023년 8월 4일 : 개인정보보호위원회 위원 (역)
<관심분야> 정보보호관리체계, 개인정보보호, IoT 보안, 네트워크 보안, 암호 프로토콜, 인공지능 보안과 프라이버시. 블록체인 보안, 5G/6G 보안