ITU-T SG17(정보보호) 전자 국제회의 결과

박수정 TTA 표준화본부 책임연구원
염흥열 ITU-T SG17 국제 의장, 순천향대학교 정보보호학과 교수

1. 머리말

ITU-T SG17(Study Group 17, 정보보호)은 UN 산하 표준 개발 및 보급을 수행하는 ITU (International Telecommunication Union, 국제전기통신연합)에서 정보보호기술에 대한 국제표준을 개발하는 연구반이다. SG17 국제회의는 2021년 4월 20일부터 30일까지 코로나19 확산 방지를 위해 온라인으로 개최됐다. 이번 SG17 국제회의에는 전 세계 32개국에서 231명이 참석했다. 한국에서는 염흥열 교수(순천향대, 수석대표) 등 37명의 국가대표단이 참가했다.
우리나라는 분산원장기술 보안, 데이터 비식별화, 5G 보안, 양자암호통신 등 차세대보안기술 표준화를 위해 국가기고서 29건을 제안했고 총 2건의 국제표준 사전채택(Consent), 총 4건의 신규 표준화 아이템 승인 등 괄목할만한 성과를 거뒀다. 또한 SG17 국제의장단도 기존 13석에서 16석으로 추가 3석을 확보했다.

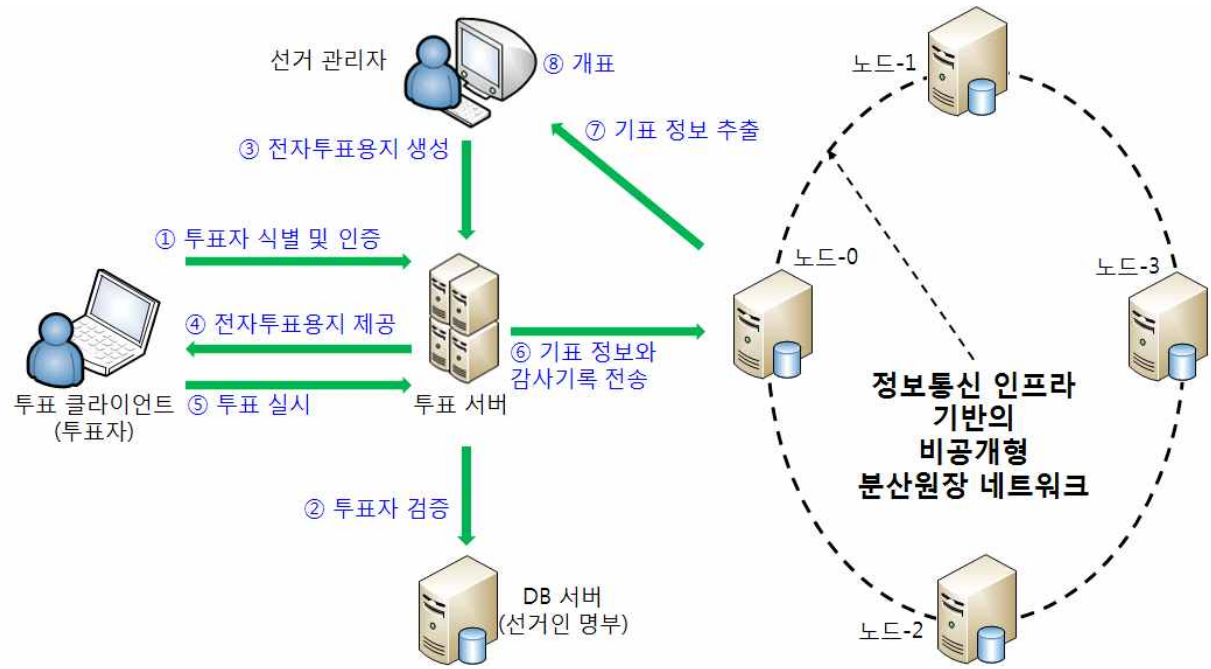
2. 주요 회의 내용

2.1 국제표준 사전채택
한국이 2017년 9월에 신규 표준화 과제를 제안하고, 다년간 주도적으로 개발해온 분산원장기술 서비스 보안에 대한 국제표준(권고안) 2건이 사전 채택됐다.
첫 번째 권고안 '분산원장기술 기반 전자 지불 서비스 보안 위협 및 요구사항(X.1405)'은 블록체인 기반 지불 서비스 모델을 퍼블릭 및 프라이빗 블록체인 기반으로 분류해 제시한다. 또한 발생할 수 있는 보안 위협을 분석하며 위협에 대응하기 위한 보안 요구사항을 정의한다.
이 표준은 국내 TTA 표준화위원회 산하 PG502(개인정보보호/ID관리, 블록체인 보안 프로젝트 그룹)에서 2019년 12월 단체표준(TTAK.KO-12.0351, 분산원장기술 전자 지불 시스템 보안위협 및 요구사항)으로 채택됐으며 이를 기반으로 ITU-T 국제표준으로 개발됐다. 향후 이 표준은 한국 주도로 개발 중인 블록체인 보안 통제(X.sc-dlt) 표준의 기본 표준으로 적용될 예정이다. 또한 국내외 블록체인 전자 지불 서비스의 보안 연구에 활용돼 보안 솔루션 개발, 보안 수준 평가 및 개선을 위한 기초 표준으로 폭넓게 활용될 것이다.
두 번째 권고안 '분산원장기술 기반 온라인 투표 시스템 보안위협(X.1406)'은 블록체인기반 온라인 투표 시스템의 모델을 투표 클라이언트(투표자), 선거 관리 클라이언트(선거 관리자), 투표 서버, 선거인 명부 서버, 비공개형 분산원장 네트워크 등의 구성 요소 측면에서 제시한다.
또한 온라인 투표 시스템에서 발생할 수 있는 잠재적인 보안위협을 데이터 기밀성, 데이터 무

결성, 서비스 가용성, 정보시스템에 대한 비인가 된 접근, 악의적인 행동 측면에서 식별 및 정의한다. 덧붙여 한국, 영국, 터키 등 블록체인 기반 온라인 투표 시스템 활용사례를 제시했다. 이 표준 또한 국내 TTA 표준화위원회 산하 PG502에서 2018년 12월 단체표준(TTAK.KO-12.0335, 분산원장기술을 활용한 온라인 투표 모델 및 보안 위협 대응)으로 제정됐으며, 이를 바탕으로 하여 ITU-T 국제표준으로 개발됐다. 이 표준을 활용해 향후 블록체인 기반 온라인 시스템 구축 시, 이해 관계자(서비스 제공자, 투표자, 선거 관리자 등)가 투표 시스템의 잠재적 보안 위협을 파악해 제거함으로써 투표 결과에 대한 신뢰성을 높일 수 있을 것이다.

<표 1> 한국 주도 국제표준 사전 채택

No.	표준 번호	표준 제목	에디터(소속)	내용
1	X.1405 (X.str-dlt)	분산원장기술 기반 전자지불 서비스 보안 위협 및 요구사항	오경희 대표 (TCA서비스) 김창오 CISO (야놀자)	- 분산원장기술에 기초한 전자지불 시스템의 모델 - 보안 위협 분석 및 보안 요구사항
2	X.1406 (X.stov)	분산원장기술 기반 온라인 투표 시스템 보안위협	박근덕 교수(서울외대) 염흥열 교수(순천향대) 진병문 교수(순천향대) 김창오 CISO(야놀자)	- 블록체인 기반 온라인 투표 서비스 모델 - 보안 고려사항 및 보안위협 식별 - 활용 사례(한국, 영국, 터키)



[그림 1] 분산원장기술을 활용한 온라인 투표 시스템의 모델(출처 : TTAK.KO-12.0335)

2.2 신규 표준화 아이템 승인

한국은 비식별 데이터 처리 및 양자암호통신 관련 신규 표준화 아이템 4건을 제안해 승인됐으며 올해부터 관련 연구가 진행될 예정이다.

첫 번째 신규 표준화 아이템은 '비식별 데이터 결합 보안 가이드라인(X.guide-cdd)'이며, 순천향대와 NSHC가 공동으로 제안해 승인됐다. 이 표준에서는 개인정보를 포함한 데이터를 안전

하게 보호하면서도 활용도를 높일 수 있도록 비식별 데이터를 결합·처리하는 절차를 정의한다. 또한 관련 위협 및 보안 가이드라인을 제시할 계획이다. 최근 데이터3법 개정에 발맞추어 안전한 데이터 이용 활성화에 이 표준이 널리 활용될 수 있을 것으로 기대된다.

두 번째 신규 표준화 아이템은 '영상 비식별화 및 안전한 공유(X.vide)'로 서울과기대에서 제안해 승인됐다. 최근 인공지능 기술의 발전으로 비식별화 기술에 대한 관심이 높아지고 있다. 그러나 비디오, 오디오에서 개인정보를 식별하는 정보에 대한 보호 및 공유 방법에 대해서는 제시된 바가 없다. 이에 이 표준에서 비정형 정보인 오디오 및 비디오에서 식별 정보를 보호하고 공유하는 방법을 개발하고자 한다.

세 번째 신규 표준화 아이템인 '양자키분배 네트워크 제어 및 관리 보안 요구사항'은 KT에서 제안했으며 일본에서도 유사한 주제의 신규과제를 제안해 협의를 통해 한국이 에디터로서 문서를 주도적으로 개발하기로 했다. 이 표준에서는 양자암호키를 생성하고 전달하는 양자암호 네트워크를 안전하고 효율적으로 제어하고 관리하기 위해 필요한 구성 요소 및 보안 요구사항을 제시할 예정이다. 이를 통해 최근 디지털뉴딜 양자암호통신 시범인프라 구축/운영 사업 등을 통해 실제 도입이 이루어지고 있는 국내외 양자암호통신 관련 시장 확산에 기여할 전망이다.

네 번째 신규 표준화 아이템은 '양자키분배 네트워크 기반 하이브리드 보안 개요(기술보고서)'로서 SKT에서 제안해 승인됐다. 양자키분배 기술은 양자 기술을 이용해 보안키를 분배하는 기술로서, 보안성이 우수하다는 장점이 있다. 이 표준에서는 양자키분배 기술로 생성된 보안키를 기존 보안 체계와 연동할 수 있도록 하는 하이브리드 보안 방법을 제시하고자 한다. 이를 통해 양자키분배 기술의 활용성을 높이고, 양자 기술 생태계를 확장하고자 한다.

<표 2> 신규 표준화 아이템 승인 및 에디터십 확보

No.	표준 번호	표준 제목	제안자(소속)	내용
1	X.guidecdd	비식별 데이터 결합 보안 가이드라인	염흥열 교수 (순천향대) 김미연 연구원 (NHSC)	- 비식별 데이터 결합 활용 사례 - 비식별 데이터 결합 절차 - 비식별 데이터 결합 모델 - 관련 위협 및 보안 가이드라인
2	X.vide	영상 비식별화 및 안전한 공유	박종열 교수 (서울과기대)	- 통신서비스에서 비디오 및 이미지 등 영상의 비식별화 방법 - 비식별화한 영상 공유 시 보안 위협 및 가이드라인
3	X.sec_ QKDN_CM	양자키분배 네트워크 제어 및 관리 보안 요구사항	윤춘석 선임 (KT)	- 양자암호통신 네트워크를 안전하게 제어 및 관리하기 위한 보안 요구사항
4	TR.hybsec -qkd	양자키분배 네트워크 기반 하이브리드 보안 개요(기술보고서)	심동희 팀장 (SKT)	- 양자 키 분배 기술로 생성된 보안키를 기존 암호화 장비와 연동하기 위한 키 교환 및 인증 관련 하이브리드 보안 방법

2.3 한국 국제의장단 진출

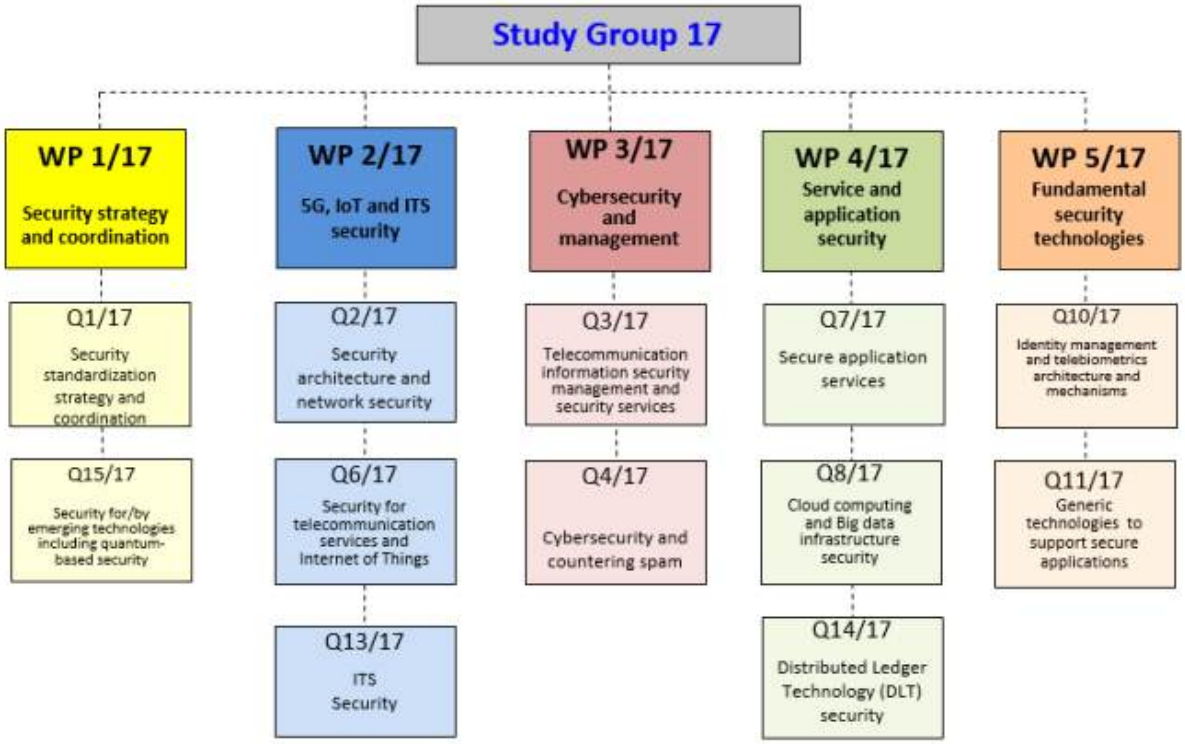
이번 SG17 국제회의에서는 정보보호 연구반(SG17) 산하 조직의 구조조정에 따른 의장단 재구성도 논의됐다. 기존 연구회기(2017-2020)에서 SG17 연구반은 4개 작업반(Working Party)

및 14개 연구과제(Question)로 조직을 구성해 보안구조 및 프레임워크, 정보보호 관리 기술, 사이버보안, 기술적인 방법에 의한 스팸 대응, 응용서비스 보안, 텔레바이오인식 기술, 아이덴티티 관리 및 메커니즘 등의 정보통신 언어, 차량통신 보안, 분산원장기술 보안 등에 대한 표준개발을 수행해 왔다. 세계표준총회가 2022년 3월로 연기됨에 따라 이번 연구회기가 2022년 2월까지 연장돼 이번 연구회기의 남은 기간과 차기연구회기(2022-2024)의 SG17 연구반은 양자암호통신 등 차세대 보안 기술에 적극 대응하고 일부 연구과제를 통합하여 5개 작업반 및 12개 연구과제로 재편했다. 이를 통해 향후 5G 보안 등을 포함한 보안구조 및 네트워크 보안, 정보보호 관리 및 보안 서비스 기술, 사이버보안 및 스팸대응, 사물인터넷 보안, 응용서비스 보안, 클라우드 및 빅데이터 보안, 신원 관리 및 텔레바이오인식 기술, 보안 응용을 지원하는 일반 기술, 차량 통신 보안, 분산원장기술 보안, 양자 기반 보안을 포함한 차세대 보안 기술 등에 대한 표준개발을 추진할 계획이다.

SG17 산하 조직 연구반 구조조정에 따라 의장단 재구성도 논의됐다. 한국은 실제 표준안 개발이 이뤄지는 연구과제 의장단 2석과 연구과제에서 개발된 표준안을 검토하고 승인하는 작업반 의장단에 1석을 추가로 진출시켰다. 구체적으로 한국이 신규 연구과제 신설을 제안해 만들어진 Q15(양자보안 및 차세대보안)의 라포처, 부라포처에 양자암호통신 분야를 선도하는 국내기업인 SKT와 KT의 전문가가 선임됐다. 또한 Q15의 상위 작업반인 WG1(보안전략 및 조정) 부의장에 ETRI 전문가가 선임됐다. 이로써 우리나라의 정보보호 연구반(SG17) 국제의장단은 기존 13석에서 16석으로 3석을 추가 확보하게 됐다. 이를 통해 한국은 양자암호통신 및 차세대 보안 기술 표준화를 주도적으로 이끌어 나갈수 있을 것이다.

<표 3> ITU-T SG17 한국 국제의장단 현황(총 16석)

분야	기존			변경			
	직위	성명	소속	직위	성명	소속	비고
SG17(정보보호)	의장	염흥열	순천향대	좌동			
WP1(보안전략&조정)	–	–	–	**부의장**	**김종현**	**ETRI**	**신규**
WP4(서비스&응용)	의장	나재훈	ETRI	좌동			
Q1(표준 전략)	부라포처	기주희	IITP	좌동			
Q2(5G보안 등)	라포처	오흥룡	TTA	좌동			
Q4(사이버보안 및 스팸대응)	라포처	김종현	ETRI	좌동			
	부라포처	김창오	야놀자	좌동			
Q6(IoT보안 등)	라포처	백종현	KISA	좌동			
	부라포처	이건희	NSR	좌동			
Q7(응용서비스 보안)	라포처	나재훈	ETRI	좌동			
Q10(신원 관리)	부라포처	박근덕	서울외대	좌동			
Q13(ITS 보안)	라포처	이상우	ETRI	좌동			
	부라포처	박승욱	현대자동차	좌동			
Q14(블록체인 보안)	라포처	오경희	TCA서비스	좌동			
Q15(양자암호통신 등)	–	–	–	**라포처**	**심동희**	**SKT**	**신규**
	–	–	–	**부라포처**	**윤춘석**	**KT**	**신규**
합계	13석			16석			



[그림 2] SG17 조직구성

3. 맺음말

한국은 이번 SG17 국제회의에서 총 30건(국가 29건, 섹터 1건)의 정보보호 분야 기고서를 제출해 국제 표준안에 모두 반영했다. 앞서 이번 국제회의의 성과로 소개한 분산원장기술 보안, 비식별 데이터 처리 및 양자암호통신 분야 외에도 한국은 5G 보안, 지능형 차량통신시스템 보안, 사물인터넷(IoT) 보안, 바이오인식 보안 등 다양한 분야에 대한 지속적인 기고를 통해 국제표준안 개발을 주도하고 있다. 이러한 체계적인 SG17 국제표준화 활동은 국내 SG17 연구반(반장: 순천향대 염흥열 교수)을 중심으로 KT 등 통신회사, 현대자동차, 한국전자통신연구원, 한국인터넷진흥원, 금융보안원 등 산학연 중심으로 수행되고 있다. 향후에도 국내 SG17 연구반은 산학연 전문가들의 유기적 협력을 바탕으로 한국의 우수한 정보보호 기술을 국제표준에 반영하기 위해 적극적인 국제표준화 활동을 추진할 계획이다. 또한, 디지털 대전환에 따라 사이버위협 포인트가 증대되고 있는 현 시점에서 디지털안심 국가 실현을 위해 향후에도 인공지능(AI), 빅데이터, 사물인터넷(IoT), 자율자동차, 블록체인 등 4차 산업혁명 관련 정보보호 분야 국제표준화 활동을 강화할 예정이다.

이러한 능동적이고 주도적인 SG17 국제표준화 활동이 국내 정보보호 산업계의 해외시장 경쟁력 확보에 일조할 것으로 기대된다. 차기 SG17 국제회의는 2021년 8월 24일부터 9월 3일까지 온라인으로 개최될 예정이다. 그리고 한국 제안으로 ITU-D 신흥 기술 주간에 DID (Decentralized Identity) 관련 ITU 워크숍을 7월경 개최할 예정이다. 최근 국내에서도 코로나19 백신 전자 예방접종증명서를 발급하는 등 백신 증명서에 대한 전 세계적인 요구와 관심이 대두됨에 따라, ITU-T SG16(멀티미디어)과 공동으로 백신 증명에 대한 ITU 워크숍도 8월초에 개최할 계획이다.

※ 본 연구는 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2017-0-00069, 공식 표준화기구(ITU/APT 등) 표준화 대응 연구)

[참고문헌]

[1] TTAK.KO-12.0351, 분산원장기술 전자 지불 시스템 보안위협 및 요구사항
http://committee.tta.or.kr/data/standard_view.jsp?order=t.publish_date&by=desc&pageSize=100&nowPage=1&pk_num=TTAK.KO-12.0351&commit_code=PG502
[2] TTAK.KO-12.0335, 분산원장기술을 활용한 온라인 투표 모델 및 보안 위협 대응
http://committee.tta.or.kr/data/standard_view.jsp?order=t.publish_date&by=desc&pageSize=100&nowPage=1&pk_num=TTAK.KO-12.0335&commit_code=PG502

※ 출처: TTA 저널 제195호
(코로나 이슈로 각 표준화기구의 표준화회의가 연기・취소됨에 따라 TTA 저널로 대체합니다)