정 보 보 호 학 회 지
제 31 권 제4호, 2021. 8

ITU-T SG17(보안) 구조조정 및 국제표준화 추진 방향

오 흥 룡*, 염 흥 열**

요 약

국제전기통신연합(ITU)은 UN 산하 정보통신기술에 대한 전문 국제표준화기구이다. 193개 회원국, 약 900개 기업 및 학교 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 구성되며, 각 업무에 맞는 선도 그룹(Lead Study Group)을 지정하여 국제표준을 개발하고 있다. 정보보호 국제표준은 ITU-T SG17(보안)에서 담당하고 있다[2]. ITU-T 국제표준화 조직은 4년 주기의 연구회기(Study Period)로 연구반 구조조정, 의장단 선출 및 표준화 추진 방향을 WTSA(World Telecommunication Standardization Assembly) 총회에서 결정한다. 2020년 11월에도 WTSA-20 총회가 개최될 예정이었으나, 코로나19로 총회가 2022.3월로 연기되었다.

본 논문에서는 WTSA-20 총회가 연기됨에 따라 기존 연구회기(2017.1-2020.12)의 연장인 추가 연구회기(2020.11-2022.2) 동안에 ITU-T SG17 의장단과 연구반 내에 구조조정 결과에 대해 정리하고, SG17 국제표준화 현황을 다룬다.

Ⅰ. 서 론

ITU-T SG17은 보안에 대한 국제표준을 개발하는 국제표준화 그룹이다. 보안 표준은 정보보호 시스템의 호환성과 기술 경쟁력 향상을 위해 요구된다. SG17 연구반은 2017-2020 연구회기에 이어, 추가 연구회기(2020.11-2022.2) 동안에 활동할 구조를 확정하였으며, 한국 제안으로 양자암호 통신기술에 대한 국제표준을 전담할 신규 연구과제(Question)를 신설하였다. 차기 WTSA-20 총회는 2022.3.1.-9일까지, 인도 하이데라바드(India Hyderabad)에서 개최될 예정이며, 차기 연구회기는 2022.3-2024.12 일정으로 1년이 줄어들 예정이다.

본 논문 제2장에서는 추가 연구회기를 위해 임명된 의장단 변동사항과 관련 결의, 구조조정 결과를 중심으로 기술한다. 또한, 최근에 개최된 ITU-T SG17 국제회의 현황에 대해 살펴보고, 제3장에서는 결론 및 향후 대응 방안을 제시한다.

Ⅱ. ITU-T SG17 국제표준화 활동

2.1. SG17 구조조정 개요

ITU-T 의장단 임기는 연구회기(4년)를 기준으로 연임을 포함해 총 2회까지 가능하지만, 코로나19에 의한 추가 연구회기는 이전 연구회기(2017-2020)의 연장으

〔표 1〕 SG17 의장단 (연구회기 2020.11-2022.2)

이름	국가	직위
염흥열	한국 (순천향대)	의장
Vasiliy DOLMATOV	러시아	부의장
Gökhan EVREN	터키	부의장
Juan GONZALEZ	미국	부의장
Muataz Elsadig ISHAG	수단	부의장
Wala TURKI LATROUS	튀니지	부의장
Zhaoji LIN	중국	부의장
Lia MOLINARI	아르헨티나	부의장
Yutaka MIYAKE	일본	부의장
Eric Anicet MBATHAS	중앙 아프리카 공화국	부의장

본 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임. [No.2017-0-00061, 국내ICT표준제개정연구, No.2019-0-00660, 차세대 ICT 환경에서의 보안 및 개인정보보호 기술 국제 표준화 추진]
* 한국정보통신기술협회 표준화본부 (수석연구원, hroh@tta.or.kr)
** 순천향대학교 정보보호학과 (교수, hyyoum@sch.ac.kr)

〔표 2〕 SG17 연구과제 구조조정 (연구회기 2020.11-2022.2)

연구과제 (신규번호)	연구과제 (연구회기: 2020.11-2022.3)	구조조정	연구과제 (이전번호)	연구과제 (연구회기: 2016-2020)
1/17	Security standardization strategy and coordination (보안표준화전략 및 조정)	계속	1/17	Telecommunication/ICT security coordination (정보통신/ICT보안 조정)
2/17	Security architecture and network security (보안구조 및 네트워크 보안)	계속	2/17	Security architecture and framework (보안구조 및 프레임워크)
3/17	Telecommunication information security management and security services (정보통신 보안관리 및 보안서비스)	계속	3/17	Telecommunication information security management (정보통신 보안관리)
4/17	Cybersecurity and countering spam (사이버보안 및 스팸대응)	통합 (Q4+Q5)	4/17	Cybersecurity (사이버보안)
			5/17	Countering spam by technical means (기술적 방법에 의한 스팸대응)
6/17	Security for telecommunication services and Internet of Things (사물인터넷 및 정보통신 서비스를 위한 보안)	계속	6/17	Security aspects of telecommunication services, networks and Internet of Things (사물인터넷, 네트워크, 정보통신 서비스의 보안 기술)
7/17	Secure application services (안전한 응용서비스)	계속	7/17	Secure application services (안전한 응용서비스)
8/17	Cloud computing and big data infrastructure security (클라우드 컴퓨팅 및 빅데이터 인프라 보안)	계속	8/17	Cloud computing and big data infrastructure security (클라우드 및 빅데이터 인프라 보안)
10/17	Identity management and telebiometrics architecture and mechanisms (아이덴티티 관리 및 텔레바이오인식 구조와 메커니즘)	통합 (Q9+Q10)	9/17	Telebiometrics (텔레바이오인식)
			10/17	Identity management architecture and mechanisms (아이덴티티 관리 구조 및 메커니즘)
11/17	Generic technologies (such as Directory, PKI, Formal languages, Object Identifiers) to support secure applications (안전한 응용서비스를 지원하기 위한 일반 기술; 디렉토리, PKI, 형식 언어, 객체 식별 등)	통합 (Q11+Q12)	11/17	Generic technologies (Directory, public key infrastructure (PKI), privilege management infrastructure (PMI), Abstract Syntax Notation One (ASN.1), object identifiers (OIDs)) to support secure applications (안전한 응용서비스를 지원하기 위한 일반 기술)
			12/17	Formal languages for telecommunication software and testing (정보통신 소프트웨어 및 시험을 위한 형식 언어)
13/17	Intelligent transport system security (지능형 차량 시스템 보안)	계속	13/17	Security aspects for Intelligent Transport System (지능형 차량 시스템을 위한 보안)
14/17	Distributed Ledger Technology (DLT) security (분산원장기술 보안)	계속	14/17	Security aspects for distributed ledger technologies (분산원장기술 보안)
15/17	Security for/by emerging technologies including quantum-based security (양자기반 보안을 포함한 신규 기술에 대한 보안)	신설	-	-

로 산정하기로 하였으며, 표 1과 같다.

추가 연구회기 동안의 SG17 연구반 내에 연구과제들의 구조조정 결과는 표 2와 같으며, 상호협력을 위한 유사 주제들 간에 작업반(WP, Working Party) 구조는 표 3과 같다[3].

각 작업반(WP)과 연구과제(Question)를 이끌어 나갈 의장단 현황은 표 4와 표 5와 같다. 그리고 SG17 관련 주요 정보는 표 6과 같이 변경되었다[4].

〔표 3〕 SG17 구조 (연구회기 2020.11-2022.2)

작업반	주제
WP1/17	Security strategy and coordination (보안전략 및 조정)
Q1/17	보안표준화전략 및 조정
Q15/17	양자기반 보안을 포함한 신규 기술에 대한 보안
WP2/17	5G, IoT and ITS security (5G, IoT, ITS 보안)
Q2/17	보안구조 및 네트워크 보안
Q6/17	사물인터넷 및 정보통신 서비스를 위한 보안
Q13/17	지능형 차량 시스템 보안
WP3/17	Cybersecurity and management (사이버보안 및 관리)
Q3/17	정보통신 보안관리 및 보안서비스
Q4/17	사이버보안 및 스팸대응
WP4/17	Service and application security (서비스 및 응용 보안)
Q7/17	안전한 응용서비스
Q8/17	클라우드 컴퓨팅 및 빅데이터 기반구조 보안
Q14/17	분산원장기술 보안
WP5/17	Fundamental security technologies (기초 보안기술)
Q10/17	아이덴티티 관리 및 텔레바이오인식 구조와 메커니즘
Q11/17	안전한 응용서비스 지원을 위한 일반 기술

〔표 4〕 작업반 의장단 (연구회기 2020.11-2022.2)

WP	의장	부의장
WP1	Vasiliy DOLMATOV (러시아)	김종현 (한국, ETRI)
WP2	Yutaka MIYAKE (일본)	Zhiyuan HU (중국) Philip MILLS (영국)
WP3	Koji NAKAO (일본)	Lia MOLINARI (아르헨티나)
WP4	나재훈 (한국, ETRI)	Xiaoyuan BAI (중국)
WP5	Zhaoji LIN (중국)	-

〔표 5〕 연구과제 라포처/부라포처(연구회기 2020.11-2022.2)

연구과제	라포처	부라포처
Q1/17	Mohamed ELHAJ (수단)	기주희 (한국, IITP)
		Paul NAJARIAN (미국)
		Wataru SENGA (일본)
		Yiwen WANG (중국)
Q2/17	오흥룡 (한국, TTA)	-
	Zhiyuan HU (중국)	
Q3/17	Miho NAGANUMA (일본)	Jinghua MIN (중국)
		Thaib MUSTAFA (말레이시아)
Q4/17	김종현 (한국, ETRI)	김창호 (한국, 야놀자)
	Yanbin ZHANG (중국)	
Q6/17	백종현 (한국, KISA)	이건희 (한국, 국보연)
	Junzhi YAN (중국)	Takeshi TAKAHASHI (일본)
		Bo YU (중국)
Q7/17	나재훈 (한국, ETRI)	Lijun LIU (중국)
		Feng GAO (중국)
Q8/17	Liang WEI (중국)	Mark MCFADDEN (영국)

연구과제	라포처	부라포처
Q10/17	Abbie BARBIR (미국)	박근덕 (한국, KSEL)
		Hiroshi TAKECHI (일본)
	John George CARAS (미국)	Junjie XIA (중국)
Q11/17	Jean-Paul LEMAIRE (프랑스)	Dieter HOGREFE (독일)
		Gunter MUSSBACHER (캐나다)
Q13/17	이상우 (한국, ETRI)	박승욱 (한국, 현대)
		Yi ZHANG (중국)
Q14/17	오경희 (한국, TCA서비스)	Xiaoyuan BAI (중국)
	Youki KADOBAYASHI (일본)	Ke WANG (중국)
Q15/17	심동희 (한국, SKT)	Kaoru KENYOSHI (일본)
		윤춘석 (한국, KT)
		Chen ZHANG (중국)

〔표 6〕 SG17 개요 (연구회기 2020.11-2022.2)

타이틀	보안 (Security)
임무	연구반 17은 정보통신기술(ICT) 사용에 대한 신뢰와 보안 구축을 책임진다. 특히, 개인정보(PII)의 기밀성, 무결성 및 가용성 보장과 관련하여 데이터 보호의 기술 및 운영 측면을 다루며, 다음 보안 기술들을 책임진다. · 사이버보안, 관리형 보안 서비스, 엔드포인트 탐지 및 대응, 보안관리, 스팸 대응 및 ID 관리 · 보안구조 및 프레임워크, 개인정보 보호, 양자 기반 보안, 분산 원장 기술 보안, 지능형 차량 시스템 보안, AI 관련 보안, 사물인터넷 등 네트워크, 애플리케이션 및 서비스 보안 · 스마트시티, IMT2020/5G 등 다양한 종류의 네트워크, 스마트 그리드, 산업제어시스템(ICS), 공급망, 스마트폰, SDN/NFV, IPTV, 웹 서비스, OTT(over-the-top), 소셜 네트워크, 클라우드 컴퓨팅, 빅데이터 분석, 디지털 금융 시스템 및 텔레바이오인식. · 디렉토리 및 개체 식별자, 개방형 시스템 통신의 적용과 기술 언어, 사용 방법 및 적합성 테스트 등 소프트웨어 기술
선도 연구반	· 보안에 대한 선도 연구반 · ID 관리에 대한 선도 연구반 · 언어 및 서술(Description) 기술에 대한 선도 연구반

2.2. SG17 관련 결의

코로나19로 WTSA-20 총회가 연기됨에 따라 WTSA-16(2016.10월, 튀니지 함마메트)에서 합의된 주요 결의(Resolution)가 그대로 적용되었다. SG17과 관련된 주요 결의는 결의 50(사이버보안), 결의 52(스팸의 대처와 방지), 그리고 결의 58(개발 도상국에 대한 국가적 컴퓨터 침해사고대응팀 설립의 장려) 이다. SG17은 이 결의들을 바탕으로 표준화 정책 수립 및 국제표준화를 추진하고 있다[5].

2.3. SG17 국제표준화 동향

본 절에서는 구조조정에 따라 각 연구과제별로 중점적으로 다루어질 예정이거나 현재 진행되고 있는 주요 토픽에 대한 정보를 제공하고자 한다[3, 6].

2.3.1. 보안표준화전략 및 조정(Q1/17)

본 연구과제는 정보보호 국제표준, 부속서 등 결과물을 홍보하고, ICT 보안 표준 로드맵, 보안 매뉴얼, 보안 개요 및 보안 표준의 성공적인 구현사례들을 발굴한다. ITU 및 외부 조직 간에 보안 표준 기술에 대한 정보 교류, 보안 워크숍 기획 및 보안 활동의 조정 역할을 수행한다. 특히, 정보보호 국제표준 개발 및 적용에 대해 다양한 이해당사자들을 위해 상향식 접근 방식, 하향식 접근 방식, 두 가지를 조합하는 방식의 조정 역할에 대한 방법론도 연구한다.

2.3.2. 보안구조 및 네트워크 보안(Q2/17)

본 연구과제는 종단 간 데이터 통신을 위한 보안구조와 인증성, 접근제어, 부인방지, 기밀성, 무결성, 보안 감사 및 재난경보 등 전반적인 보안서비스 프레임워크를 다룬다. 특히, NGN, SDN/NFV, NS(네트워크 슬라이싱), 서비스 기능 체인(SFC), 다중 액세스 에지 컴퓨팅(MEC), LTE/SAE, IMT-2020/5G 등 네트워크 보안 및 가상화 보안 기술을 다룬다. 그리고 인공지능(AI)/머신 러닝(ML) 기반 통신기술 및 네트워크 보안 기술을 다룬다. 지난 연구회기에서는 5G 보안을 Q2/17와 Q6/17 간에 함께 개발하였는데, 구조조정 결과에 따라 Q2/17에서 전담하기로 합의하였다.

본 연구과제에서 개발되고 있는 주요 아이템은 다음과 같다.

- X.5Gsec-t(5G 생태계 내에 신뢰 관계성 기반의 보안 프레임워크)
- X.5Gsec-ecs(5G 에지 컴퓨팅 서비스를 위한 보안 프레임워크)
- X.5Gsec-guide(5G 통신 시스템을 위한 보안 가이드라인)
- X.5Gsec-netec(5G 에지 컴퓨팅을 위한 네트워크 계층의 보안 능력)
- X.5Gsec-vs(5G NPN망에서의 URLLC를 지원하는 버티컬 서비스를 위한 보안 요구사항)
- X.5Gsec-ssl(5G 네트워크 슬라이스 내에 보안 능력의 등급화를 위한 가이드라인)
- X.5Gsec-message(5G 메시지 서비스를 위한 보안 요구사항)
- X.nsom-sec(네트워크 슬라이스 관리 및 오케스레이션을 위한 구조 및 보안 요구사항)
- X.rf-csap(서비스 접근 프로세스의 지속적인 보호를 위한 가이드라인)

2.3.3. 정보통신 보안관리 및 보안서비스(Q3/17)

본 연구과제는 통신 조직 내에 정보보호관리시스템(ISMS)의 구현 및 통제항목 제공, 개인정보보호(PII) 및 프라이버시 관련 국제표준 개발과 해당 표준 구현에 대한 모범사례를 개발하였다. 추가 연구회기에서는 보안서비스 업무영역이 추가되어 관리 보안 서비스, 컴퓨터 사고 대응팀 서비스, 보안제어 및 위험 관리 서비스 등에 대한 국제표준을 담당한다.

본 연구과제에서 개발되고 있는 주요 아이템은 다음과 같다.

- X.1051rer2(정보통신 조직을 위한 ISO/IEC 27002 기반 정보보호 통제 항목에 대한 구현)
- X.1054rev4(정보보호 거버넌스)
- X.ciag(사이버 보험 가입 가이드라인)
- X.sup-csc(정보통신 조직을 위한 민감한 보안 통제에 대한 부속서)

2.3.4. 사이버보안 및 스팸대응(Q4/17)

본 연구과제는 WTSA-16 결의 50(사이버보안)과 결의 52(스팸의 대처와 방지)를 구현하기 위한 국제표준을 담당한다. 사이버보안 분야는 다양한 사이버 위협 및 공격에 대한 식별, 보호, 탐지, 대응 및 복구에 대한 전반적인 표준을 다루고 있으며, 국가 간에 사이버보안 정보공유 방법 및 구조적 위협 정보를 표현할 수 있는 기술을 다루고 있으며, AI/ML 기반 지능화된 사이버 보안 기술도 포함하고 있다. 스팸대응 분야는 이메일 스팸, IP 멀티미디어 스팸, 보이싱 스팸 등 다양한 스팸대응 기술을 다루고 있으며, 랜섬웨어와 같이 악성 소프트웨어, AI/ML 기반 자동화형 스팸기술도 담당한다. 추가 연구회의에서는 사이버보안과 스팸대응 분야가 통합되어 시너지 효과가 높을 것으로 예상된다.

본 연구과제에서 개발되고 있는 주요 아이템은 다음과 같다.

- TR.cs-ML(머신 러닝 기반 스팸대응 관련 기술보고서)
- X.gcims(인스턴트 메시징 상에서의 스팸대응 가이드라인)
- X.1246rev(정보통신 조직 내에 보이싱 스팸대응을 위한 기술 지침)
- X.1247rev(모바일 메시징 스팸대응을 위한 기술 프레임워크)
- X.arc-ev(기술적 취약점 평가를 위한 보안구조)
- X.gcmms(멀티미디어 메시징 서비스 스팸대응을 위한 가이드라인)
- X.tecwes(정보통신 조직을 위한 웹사이트 스푸핑 대응에 대한 기술 지침)
- X.tsfpp(모바일 메시징 스팸대응하는 동안에 사용자 개인정보 보호에 대한 기술적 보안 프레임워크)

2.3.5. 사물인터넷 및 정보통신 서비스를 위한 보안(Q6/17)

본 연구과제는 멀티캐스트, 홈네트워크, 모바일 네트워크, RFID, 유비쿼터스 센서 네트워크, IPTV 서비스, 스마트그리드, 사물인터넷, 스마트시티(M2M 포함), NFC, 산업제어시스템, 스마트폰에 대한 정보보호 국제표준을 담당한다.

본 연구과제에서 개발되고 있는 주요 아이템은 다음과 같다.

- TR.ibc-cd(교차 도메인 내에 안전한 통신을 위한 ID기반 암호시스템 사용 가이드라인)
- X.iotsec-4(IoT 기기 및 게이트웨이를 위한 보안 요구사항)
- X.sc-iot(IoT 시스템을 위한 보안 통제)
- X.sg-rat(인터넷에 연결된 통제시스템을 원격 제어하는 도구 사용에 대한 보안 가이드라인)
- X.ssp-iot(IoT 서비스 플랫폼을 위한 보안 요구사항 및 프레임워크)
- X.strvms(비디오 관리 시스템을 위한 보안 위협 및 요구사항)
- X.ztd-iot(제로터치(zero-touch) 대규모 IoT 구축을 위한 보안 방법론)

2.3.6. 안전한 응용서비스(Q7/17)

본 연구과제는 TTP 인증서비스, P2P 서비스, 소셜 네트워크 서비스, 금융서비스, 보안 플랫폼, 공증서비스, 핀테크, 디지털트윈, OTT 서비스 등 다양한 응용서비스를 다루고 있으며, 이를 지원하기 위한 보안 응용 프로토콜과 비식별 처리 기술도 다루고 있다.

본 연구과제에서 개발되고 있는 주요 아이템은 다음과 같다.

- TR.cta(감염병 확산 방지를 위한 접촉자 추적 어플리케이션의 활용사례에 대한 기술보고서)
- X.1144rev(XACML 3.0)
- X.guide-cdd(제3의 신뢰기관을 이용한 비식별 데이터의 결합을 위한 보안 가이드라인)
- X.rdda(데이터 비식별 보증을 위한 요구사항)
- X.scpa(패스워드 관련 온라인 공격을 대응하기 위한 보안 대응책)
- X.sec-grp-mov(군집 이동 서비스 플랫폼을 위한 보안 가이드라인)
- X.sg-dtn(디지털 트윈 네트워크를 위한 보안 가이드라인)
- X.sgos(웹기반 온라인 고객서비스를 위한 보안 가이드라인)
- X.sles(위치 정보가 내장된 스마트 오피스 서비스를 위한 보안 대응책)
- X.smdtsc(스마트시티의 디지털 트윈 시스템을 위한 보안 대응책)
- X.smsrc(스마트 주거 커뮤니티를 위한 보안 대응책)
- X.vide(비식별화를 위한 영상 특징점 보호 및 안전한 공유 가이드라인)
- X.websec-7(온라인 분석 서비스를 위한 레퍼런스 모니터)

2.3.7. 클라우드 컴퓨팅 및 빅데이터 인프라 보안(Q8/17)

본 연구과제는 클라우드 컴퓨팅 보안에 대해 서비스(SaaS, CaaS, PaaS, IaaS, NaaS) 관점과 구축 모델(퍼블릭, 프라이빗, 하이브리드, 코어, 에지 등) 관점에서 보안 국제표준을 담당한다. 또한, 클라우드 서비스 제공자와 사용자 관점에서 준수해야 될, 보안 가이드라인 및 모범사례들을 정의한다. 추가 연구회기에서는 빅데이터 보안 기술이 추가되어 데이터 수집, 저장, 분석, 관리, 시각화 등 클라우드와 빅데이터 간에 연계 서비스(Big-data as a service) 보안 표준 개발이 가능할 것으로 판단된다.

본 연구과제에서 개발되고 있는 주요 아이템은 다음과 같다.

- TR.XAAS(가상화 서비스를 위한 보안 표준화 프레임워크 관련 기술보고서)
- X.BaaS-sec(분산원장기술을 클라우드 서비스 환경에서 제공하기 위한 보안 가이드라인)
- X.gecds(에지 컴퓨팅 데이터 보안 가이드라인)
- X.nssa-cc(클라우드 컴퓨팅을 위한 네트워크 보안 상황인지 플랫폼 요구사항)
- X.sa-ec(에지 클라우드 보안구조)
- X.sgBDIP(빅데이터 인프라구조와 플랫폼을 위한 보안 가이드라인)
- X.sgcc(클라우드 컴퓨팅 환경에서 컨테이너를 위한 보안 가이드라인)
- X.sgcnp(클라우드 네이티브 파스(native PaaS)를 위한 보안 가이드라인)
- X.sgdc(분산형 클라우드를 위한 보안 가이드라인)
- X.sgmc(멀티-클라우드를 위한 보안 가이드라인)
- X.sr-cphr(저지연 및 고신뢰성 어플리케이션 시나리오에서 클라우드 기반 플랫폼 보안 요구사항)

2.3.8. 아이덴티티 관리 및 텔레바이오인식 구조와 메커니즘(Q10/17)

본 연구과제는 지난 연구회기에서 각각 독립적으로 운영되던, 텔레바이오인식 분야와 아이덴티티 관리 분야가 통합되었다. 바이오인식 기술은 스마트폰 등장 이후에 활용성이 더욱 높아지고 있으며, 사용자의 생체정보에 대한 데이터 보호와 통신 환경에서의 응용기술에 대한 보안 기술이 폭넓게 다루어지고 있다. 아이덴티티 기술은 식별자(identifier)에 대한 관리기술과 이기종 시스템 간에 상호운용성 기술을 중점적으로 다루고 있으며, 엔티티의 신원 인증, 권한 부여, 역할 위임 등 정보통신 환경에서 전반적인 아이덴티티 보안 기술을 담당한다.

본 연구과제에서 개발되고 있는 주요 아이템은 다음과 같다.

- X.1250rev(개선된 글로벌 ID관리 및 상호운용성을 위한 기본 능력)
- X.1251rev(디지털 아이덴티티의 사용자 통제를 위한 프레임워크)
- X.b2m(생물학에 대한 기계 프로토콜)
- X.gpwd(패스워드 및 패스워드가 없는 인증 솔루션 보안을 위한 위협 분석 및 가이드라인)
- X.pet_auth(텔레바이오인식을 이용한 애완동물에 대한 엔티티 인증 서비스)
- X.tas(음성인식을 이용한 텔레바이오인식 인증)
- X.tec-idms(분산형 아이덴티티 시스템에서 사용자 데이터 보호를 위한 관리 및 보호 기술)
- X.upu(우편 아이덴티티 관리 프레임워크)

2.3.9. 안전한 응용서비스를 지원하기 위한 일반 기술; 디렉토리, PKI, 형식 언어, 객체 식별 등(Q11/17)

본 연구과제는 지난 연구회기에서 각각 독립적으로 운영되던, 안전한 응용서비스를 지원하기 위한 일반 기술 분야와 소프트웨어 시험 및 언어 분야가 통합되었다. 추가 연구회기에는 디렉토리, 공개키기반구조, 권한관리기반구조, 추상구문언어, 객체식별자 등록 및 관리, 시험언어 및 성능평가, 형식언어 등의 표준들을 다룬다.

본 연구과제에서 개발되고 있는 주요 아이템은 다음과 같다.

- X.pki-em(공개키 기반구조: 신설 및 유지보수)
- 그 외 개방형 시스템 상호연동 및 소프트웨어 시험 및 언어 관련 유지보수 표준화 아이템은 생략

2.3.10. 지능형 차량 시스템 보안(Q13/17)

본 연구과제는 자율주행 서비스를 목표로 차량 통신 서비스(V2X: 차량-차량, 차량-인프라, 차량-기기 등) 기술과 차량 내부 통신서비스를 다루고 있다. 특히, 보조 주행 시스템, 도로 운송, 철도 운송, 수상 및 항공 운송 등 다양한 환경에서 지능형 통신 시스템을 포함해서 다룬다.

본 연구과제에서 개발되고 있는 주요 아이템은 다음과 같다.

- X.1273rev(지능형 차량 시스템 통신 기기를 위한 안전한 소프트웨어 업데이트 기술)
- X.edrsec(자율주행 환경에서 클라우드 기반 사고 데이터 기록을 위한 보안 가이드라인)
- X.eivnsec(이더넷 기반 차량 내부 네트워크를 위한 보안 가이드라인)
- X.evtol-sec(도시 항공 모빌리티 환경에서 전기 수직 이착륙(eVTOL) 차량에 대한 보안 가이드라인)
- X.fstiscv(컨넥티드 차량을 위한 보안 위협 정보 공유 가이드라인)
- X.ipscv(컨넥티드 차량을 위한 침입 예방시스템 방법론)
- X.itssec-5(차량용 에지 컴퓨팅을 위한 보안 가이드라인)
- X.rsu-sec(지능형 차량 시스템 내에 도로변 장치를 위한 보안 요구사항)
- X.srcd(V2X 통신에서 분류된 데이터를 위한 보안 요구사항)

2.3.11. 분산원장기술 보안(Q14/17)

본 연구과제는 블록체인 메커니즘으로 많이 알려진 분산원장기술(DLT)에 대한 솔루션, 구현사례, 보안위협 및 보안 요구사항 정의, 프로토콜 및 메커니즘, 이기종 간에 상호운용성, 보안성 평가 등의 분산원장기술

보안 국제표준을 다루고 있으며, 금융, 전자정부, 의료, 물류 등 다양한 분야로 확산할 수 있는 보안 서비스 기술들을 다룬다.

본 연구과제에서 개발되고 있는 주요 아이템은 다음과 같다.

- TR.qs-dlt(양자컴퓨팅 환경에서 안전한 분산원장 기술 시스템을 위한 가이드라인 관련 기술보고서)
- X.das-mgt(분산원장기술 기반 데이터 접근 및 공유를 위한 보안 위협 및 요구사항)
- X.sg-dsm(분산원장기술 기반 데이터 공유 관리를 위한 보안구조)
- X.sc-dlt(분산원장기술를 위한 보안 통제)
- X.srip-dlt(분산원장기술 기반 디지털 무결성 증명을 위한 보안 요구사항)
- X.srscm-dlt(분산원장기술 기반 스마트 계약 관리를 위한 보안 요구사항)
- X.ss-dlt(분산원장기술 기반 보안서비스)
- X.tf-spd-dlt(분산원장기술 기반 안전한 소프트웨어 프로그램 분산 메커니즘을 위한 기술 프레임워크)

2.3.12. 양자기반 보안을 포함한 신규 기술에 대한 보안 (Q15/17)

본 연구과제는 한국의 제안으로 신설되었으며, 이를 근거로 ITU 내에 최초로 양자 암호통신기술을 다루게 되었다. 본 연구과제는 두 가지 중점 임무가 있는데, 첫 번째 임무는 신규 보안 기술(new emerging security)에 대한 인큐베이션 메커니즘을 운영하는 것이다. 즉, 새로운 보안 기술에 대한 권고안 개발이 제안될 경우, 연구과제 간에 중복성을 최소로 하기 위해 제안된 신규 권고안을 적합한 연구과제 할당하는 업무를 담당한다. 그리고 적합한 연구과제가 없을 경우는 이를 해당 연구과제에서 담당하여 국제표준을 개발한다. 두 번째는 임무는 양자 보안 기술에 대한 국제표준을 개발하는 업무이다. 즉, 양자 키 분배, 양자 기반 보안에서의 보안 위협 및 취약점 분석, 양자 기본 안전 통신서비스를 지원하기 위한 보안기술 및 보안 요구사항 개발, 보안 메커니즘 및 프로토콜 등의 보안 국제표준을 개발하는 업무를 담당한다.

본 연구과제에서 개발되고 있는 주요 아이템은 다음과 같다.

- TR.hybsec-qkdn(QKD에 적용가능한 하이브리드 보안 방법의 개요에 대한 기술보고서)
- TR.sec-ai(AI 기술을 이용한 보안관리를 위한 가이드라인 관련 기술보고서)
- TR.sgfdcml(머신러닝에서 격자암호 기반 데이터 협력에 대한 기술보고서)
- X.sec-QKDN-km(양자 키 분배 네트워크를 위한 보안 요구사항: 키 관리)
- X.icd-schemas(통합 사이버 방어 솔루션을 위한 보안 데이터 스키마)
- X.sec_QKDN_AA(양자 내성 암호를 이용한 QKDN 에서의 인증 및 권한 부여)
- X.sec_QKDN_CM(양자 키 분배 네트워크를 위한 보안 요구사항 및 대응책: 통제 및 관리)
- X.sec_QKDN_intrq(안전한 네트워크 기반구조와 QKDN 간에 통합을 위한 보안 요구사항)
- X.sec-QKDN-tn(양자 키 분배 네트워크를 위한 설계 및 보안 요구사항: 신뢰 노드)
- X.tf-mpc(안전한 다자간 연산을 위한 기술 가이드라인)

Ⅲ. 결 론

본 논문에서는 추가 연구회기(2020.11-2022.2) 동안 SG17 연구반 국제표준화 추진 방향에 대해 살펴보았다. 이를 위해 의장단 현황 및 구조조정 결과, 각 연구과제별 개발되고 있는 권고안에 대해 살펴보았다. SG17 연구반은 코로나19 환경에도 불구하고 매 원격회의 시, 약 230~250명 규모로 참석자들이 참석하고 있으며, 정보통신 보안 국제표준을 개발하기 위한 대표적인 국제표준기구로 자리매김하고 있다.

한국은 SG17 국제회의마다 많은 전문가로 구성된 대표단을 파견해 오고 있으며, SG17 의장, WP 의장, 여러 연구과제의 라포처 등 의장단 활동과 국제표준 개발을 책임지는 에디터 역할을 통해 SG17 국제표준화 활동에 크게 공헌해 오고 있으며, 미국, 영국, 일본, 중국 등 다른 국가에서도 인정받고 있다.

한국은 ITU-T SG17 국제표준화 활동에 지속적인 주도권 확보를 위해 SG17 연구반 의장을 중심으로 정부, 정보보호 산업체, 학계, 공공기관 전문가와 협력해

서 정보보호 국제표준 분야를 선도할 계획이다.

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/2017-2020/17/Pages/default.aspx

[3] TSAG-R21, “Report of the seventh TSAG meeting (virtual, 11-18 January 2021) - Endorsed set of Questions for Study Group 17.

[4] TSAG-TD993R1, “Consolidated draft text for modifications to WTSA Resolution 2”.

[5] 염흥열, 오흥룡, “ITU-T SG17(보안) 구조 및 국제표준화 추진 방향(연구회기 2017-2020), 정보보호학회지 제27권 제5호, 2017.10.

[6] TU-T SG17-R79, “Report of the eleventh meeting of Study Group 17 (Virtual, 20 - 30 April 2021) - plenary sessions”, July 2021.

〈저 자 소 개〉

오 흥 룡 (Heung-Ryong Oh)

종신회원

2002년 2월 : 순천향대학교 전자공학과 졸업

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

한양대학교 대학원 전자공학과 박사

1982년 12월~1990년 8월 : 한국전자통신연구소 선임연구원

1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 정교수

2017년~현재 : ITU-T SG17 의장

2009년~2016년 : ITU-T SG17 부의장, WP3 의장

2011년 1월~12월 : 한국정보보호학회 회장

2012년 1월~현재 : 한국정보보호학회 명예회장

2016년 5월~현재 : 개인정보보호표준포럼 의장

2020년 8월~현재 : 개인정보보호위원회 위원

<관심분야> 네트워크 보안, IoT 보안, 블록체인 보안, 개인정보보호, 정보보안 국제표준