정 보 보 호 학 회 지
제 29 권 제4호, 2019. 8

ITU-T SG17(보안) 국제표준화 동향

오 흥 룡*, 염 흥 열**

요 약

국제전기통신연합(ITU)은 UN 산하 정보통신기술에 대한 국제표준을 담당하고 있으며, 전기통신표준화부문(ITU-T), 전기통신개발부문(ITU-D), 그리고 전파통신 부문(ITU-R)으로 구성되어 있다[1]. ITU-T는 역할과 임무에 따라 11개의 연구반(SG, Study Group)으로 구성되어 있고, 정보보호 국제표준은 ITU-T SG17(보안, 의장: 순천향대 염흥열 교수)에서 담당하고 있다[2]. 본 논문에서는 스위스 제네바에서 개최된 SG17 국제회의(2018년 8월, 2019년 1월) 주요 결과 및 향후 전망에 대해 분석하고자 한다.

Ⅰ. 서 론

ITU-T SG17은 정보통신망(5G, SDN/NFV 등) 보안, 응용 및 서비스 보안, 블록체인 및 분산원장기술 보안, 자동차 보안, 바이오인식, 양자암호통신 등의 주요 정보보호 주제에 대한 국제표준을 개발하고 있다[3].

ITU-T SG17은 ISO/IEC JTC1/SC27(보안기술), SC37(바이오인식기술), ISO TC307(블록체인 및 분산원장기술) 등과 같은 다른 공적 국제표준화 기구와 협력을 통해 국제표준을 개발하고 있으며, FIDO Alliance, OASIS, IETF 등과 같은 사실표준화 기구와 협력도 강화하고 있다.

본 논문에서는 ITU-T SG17 국제표준화 동향(2018년 8월, 2019년 1월 국제회의)을 중점적으로 분석해 향후 정보보호 분야에서 국제표준화 활동을 계획하고 있는 전문가들에게 최신 표준화 정보를 제공하고자 한다.

Ⅱ. ITU-T SG17 국제표준화 동향 분석

본 장에서 최근에 개최된 SG17 국제회의 주요 결과를 중심으로 설명한다. 최근 2회에 걸쳐 개최된 SG17 국제회의의 주요 규모는 [표 1]과 같다.

SG17 국제회의는 [표 1]에서 보는 것처럼, 매 회의마다 약 120여건의 기고서가 제출되고 있으며, 매 회의

〔표 1〕 SG17 국제회의 규모

구분	2018.8월	2019.1월
참가자	168명	178명
참가국 (섹터 등)	39개국 (21개 섹터 등)	36개국 (21개 섹터 등)
기고서	144건	118건
TD 문서 (회의결과 등)	420건	380건
신규 국제표준 승인 (Approved/ Consented/ Determinated)	1건/19건/3건	3건/3건/0건
신규 표준초안 승인 (New work item)	25건	13건

차세대 보안기술(분산원장보안기술, 5G보안, 양자암호통신, ITS보안 등)에 대한 신규 표준초안 제안이 활발하게 진행되고 있다.

2.1. 신규 중점 토픽

SG17에서는 여러 가지 보안 이슈들이 활발하게 논의되고 있지만, 최근에 눈에 띄는 이슈는 양자암호통신과 5G 보안, AI 보안 표준화이다.

양자암호통신 표준화는 한국 KT에서 2017.9월,

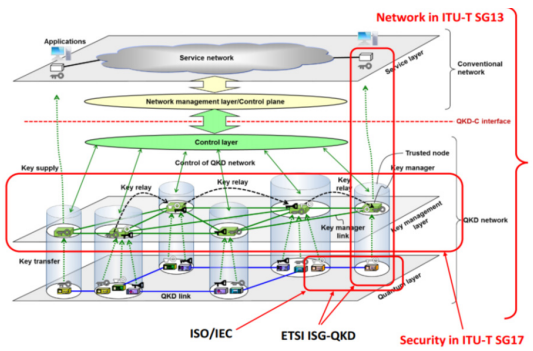
본 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임.
[*No.2017-0-00061, 국내ICT표준제개정연구, **No.2019-0-00660, 차세대 ICT 환경에서의 보안 및 개인정보보호 기술 국제 표준화 추진]
* 한국정보통신기술협회 표준화본부(hroh@tta.or.kr)
** 순천향대학교 정보보호학과(hyyoum@sch.ac.kr)

SG17 국제회의에 양자암호 기반 안전한 통신기술에 대한 국제표준 개발이 필요하다는 기고서를 근거로 활동이 시작되었다[4]. 한국은 SG17 내에 양자암호통신 보안을 전담할 수 있는 연구과제(Question) 신설을 제안하였으나, WTSA-20 구조조정 이슈로 인해 잠시 보류되어 있고, 한시적으로 사이버보안을 다루는 연구과제(Q4)에서 표준 개발을 추진하고 있다. 양자암호통신 보안 연구과제는 차기 연구회기(2021-2024)에서 전담 그룹으로 신설될 것으로 예측된다.

KT(2018.6월)는 네트워크 관점에서 양자암호통신 국제표준을 SG13(미래 네트워크)에서 개발하고 있으며, SKT(2018.8월)는 양자암호통신 보안에 대한 국제표준을 SG17에서 주도적으로 개발하고 있다. 다음의 (그림 1)은 양자암호통신 표준을 개발하고 있는 국제표준화기구들 간에 관계를 나타내고 있다[5].

ETSI ISG-QKD 그룹은 QKD(Quantum Key Distribution) 기술에 대한 이론적 증명, 구조, 모듈, 프로토콜, 인터페이스, 데이터포맷, 구현 고려사항 등을 다루고 있지만, QKD를 통해서 분배된 키를 네트워크 상에서 사용자 간에 안전하게 전달하는 방법은 다루지 않고 있다[6]. 한편 ISO/IEC JTC1/SC27/WG3 그룹은 2018.11월, QKD 기기에 대한 보안성 평가를 위한 표준화 작업을 착수하였으며, 사용자 간에 사용되는 프로토콜의 안정성, QKD 기기에 대한 보안요구사항, 이들의 안전성을 평가하기 위한 공통평가기준(CC: Common Criteria)을 적용할 수 있는 방법에 대해 표준화가 진행되고 있다[7].

5G 보안 표준화는 2018.3월, SG17 국제회의에서 신규 토픽 발굴을 위한 '5G 보안워크숍'을 시작으로 중국(차이나모바일과 노키아 상하이)과 한국(순천향대) 주도로 4건의 권고안(X.5Gsec-q, X.5Gsec-t, X.5Gsec-esc, X.5Gsec-guide)이 개발되고 있다. SG17 보안관점에서 개발하는 5G 보안 표준은 3GPP에서 규정한 5G 코어망 기술을 실제 운영 및 구현할 때, 참고할 수 있는 보안 지침 및 보안 프레임워크를 개발하려고 한다. 현재 5G 보안 표준 개발단계는 초기 상태로 3GPP 규격 분석 및 이를 기반으로 보안위협 및 보안요구 사항들을 정의하고 있는 수준이다.



〔그림 1〕 양자암호통신 국제표준기구 간에 관계도

AI 보안 표준화는 2019.1월, SG17 국제회의에서 신규 토픽 발굴을 위한 '인공지능 및 머신러닝 보안워크숍'을 시작으로 논의가 되었으며, 아직까지 구체적인 표준화 아이템 발굴은 완료되지 않았다. 보안워크숍에서의 중요한 논의 포인트는 2가지 관점에서의 AI 보안 표준 개발 가능성이 논의되었다.

- Security by AI : AI 기술을 보안기술에 접목함으로써 발생할 수 있는 이점과 문제점. 단순/반복적인 보안업무에 대한 효율성이 향상될 것으로 예상되지만, 프라이버시 문제점이 클 것으로 예상
- Security for AI : AI 기술을 원활하게 적용하기 위한 보안구조 및 프라이버시 문제를 해결하기 위한 보안 메커니즘의 신규 도입이 필요

그 밖에도 SG17에서는 신규 중점 토픽으로 IoT 보안, 빅데이터 보안, ITS 보안, 분산원장기술 보안, SDN/NFV 보안, 개인정보보호, 클라우드 컴퓨팅 보안, 비식별화 기술 등이 중점적으로 다루고 있다.

2.2. 국제표준 채택(Approved)

ITU-T 국제표준(Recommendation) 채택 절차는 규제적 합의가 있는 국제표준에 적용되는 기존채택절차(TAP: Traditional Approval Procedure)와 규제적 합의가 없는 국제표준에 적용되는 대체채택절차(AAP: Alternative Approval Procedure)로 구분된다. TAP 절차와 AAP 절차의 차이점 분석은 참고문헌 [8] 논문을 참고하기 바란다.

SG17 국제회의(2018.8월, 2019.1월)에 신규로 승인된 국제표준은 [표 2]와 같다.

〔표 2〕 국제표준 채택(Approved) 목록

No.	연구과제	제안국가 (에디터)	표준번호 (Acronym)	국제표준 제목	목적 및 주요내용
1	Q6 (통신서비스, 사물인터넷 보안)	한국 (염흥열)	X.1361 (X.iotsec-2)	Security framework for Internet of Things based on the gateway model	- 사물인터넷 환경에서의 보안 프레임워크를 정의 - IoT 환경에서의 보안 위협 및 도전(challenge) 과제들에 대해 분석하고, 이를 감소시키거나 해결할 수 있는 방법을 정의 - 2018년 8월 회의에서 최종 승인
2	Q4 (사이버 보안)	한국 (김종현, 김익균, 김지혜, 염흥열)	X.1215 (X.usctix)	Use cases for structured threat information expression	- 국가 간, 유관 기관 간에 사이버 위협 정보 공유 및 분석을 신속히 처리할 수 있는 기술 - 지속적으로 발생하고 있는 사이버 위협인 랜섬웨어, 가상화폐거래소 해킹 등에 대한 사이버 위협 정보 표현 규격(STIX) 활용사례를 구체적으로 정의 - 2019년 1월 회의에서 최종 승인
3	Q5 (기술적인 방법에 의한 스팸대응)	중국 (Hongwei Luo 등)	X.1249 (X.tfcma)	Technical framework for countering mobile in-application advertising spam	- 모바일/스마트폰 내에 앱/어플리케이션을 설치할 경우, 상단 혹은 하단에 광고가 함께 설치될 수 있는데, 이를 차단하기 위한 기술적 방법 및 프레임워크를 정의 - 2019년 1월 회의에서 최종 승인
4	Q6 (통신서비스, 사물인터넷 보안)	한국 (박정수, 김형식)	X.1042 (X.sdnsec-1)	Security services using the software-defined networking	- 소프트웨어 정의 네트워크 환경에서 다양한 네트워크 장비들에 대한 보안 위협 및 대응 시나리오와 유즈케이스를 제공 - 2019년 1월 회의에서 최종 승인

2.3. 국제표준 후보(AAP) 채택

SG17 국제회의에서 국제표준 후보(AAP)로 채택된 목록은 [표 3] 같으며, 4주간의 ITU-T 회원국 의견수렴을 통해 최종 국제표준으로 채택되었다. 단, 소프트웨어 유지보수 표준, 부속서(supplement) 및 오류정정서 등의 승인은 다루지 않는다. 한편, 2018.8월, 국제회의에서 TAP 승인으로 처리된 국제표준 후보는 [표 2]를 참고하기 바란다.

〔표 3〕 국제표준 후보(AAP consent) 목록

No.	연구과제	제안국가 (에디터)	표준번호 (Acronym)	국제표준 제목	목적 및 주요내용
1	Q7 (안전한 응용서비스)	한국 (황정연, 최규영, 조상래)	X.1450 (X.hakm)	Guidelines on hybrid authentication and key management mechanisms in client-server model	- 클라이언트-서버 모델에서 클라이언트 측의 계산량을 감소할 수 있는 하이브리드 인증 및 키관리 보안 지침 - 2018.10월, 최종 국제표준 채택
2	Q7 (안전한 응용서비스)	중국 (Feng Gao 등), 한국 (박종열)	X.1147 (X.srfb)	Security Requirements and Framework for Big Data Analytics in Mobile Internet Services	- 모마일 인터넷 서비스를 통해서 수집되는 빅데이터의 보안 취약점과 이를 해결하기 위한 보안 요구사항 및 보안기능들을 정의 - 2018.11월, 최종 국제표준 채택
3	Q9 (텔레바이오 인식)	한국 (전명근)	X.1093 (X.tac)	Telebiometric Access Control with smart ID Card	- 바이오 정보가 결합된 스마트 ID카드를 이용한 원격 바이오인식 접근제어 기술을 정의 - 2018.11월, 최종 국제표준 채택
4	Q10 (아이덴터티 관리 구조 및 메커니즘)	미국 (David Turner)	X.1277 (X.uaf)	FIDO Universal Authentication Framework (UAF)	- FIDO Alliance에서 개발된 UAF 인증기술을 ITU-T 국제표준으로 채택 - 온라인 환경에 강한 사용자 인증을 제공하기 위해 사용자 기기를 이용한 기술 - 2018.11월, 최종 국제표준 채택
5	Q10 (아이덴터티 관리 구조 및 메커니즘)	미국 (David Turner)	X.1278 (X.ctap)	Client To Authenticator Protocol/Universal 2-factor authentication framework	- FIDO Alliance에서 개발된 CTAP/U2F 인증기술을 ITU-T 국제표준으로 채택 - 외부에 존재하는 인증기기와 다른 클라언트/플랫폼 간에 통신을 위한 응용계층 프로토콜을 정의 - 2018.11월, 최종 국제표준 채택
6	Q2 (보안구조 및 프레임워크)	중국 (Zhiyuan Hu 등), 한국 (박정수)	X.1043 (X.sdnsec-3)	Security framework and requirements of service function chain based on software-defined networking	- SDN 기반 서비스 기능 체인에 대한 보안위협 분석과 이를 해결하기 위한 보안 요구사항들을 정의 - 2019.3월, 최종 국제표준 채택
7	Q9 (텔레바이오 인식)	한국 (김재성, 이새움)	X.1094 (X.tab)	Telebiometric authentication using bio-signals	- 다중 생체신호 인증플랫폼을 정의 - 웨어러블 디바이스 등을 활용하여 사람의 심전도·심박수 등 생체신호를 획득하고 개인 식별을 위한 인증메커니즘을 제공하는 차세대 바이오인식기술 - 2019.3월, 최종 국제표준 채택

2.4. 신규 표준초안(New Work Item) 채택

SG17 국제회의에서 보안 이슈들에 대해 지속적으로 신규 표준초안들이 제안되고 있으며, [표 4] 및 [표 5]와 같은 토픽들이 채택되었다. 단, 소프트웨어 유지보수 표준들은 제외한다. 각각의 표준초안들을 ITU-T 멤버들 간에 지속적인 기고서와 검토 의견들을 바탕으로 약 2~4년 정도의 표준초안 개발을 통해 최종 국제표준으로 채택될 예정이다.

〔표 4〕 신규 표준화 아이템 승인 목록(2018.8월)

No.	연구과제	제안국가 (에디터)	표준번호 (Acronym)	국제표준 제목	목적 및 주요내용
1	Q3 (보안관리)	미국(Arnaud Taddei 등) 말레이시아 (Thaib Mustafa)	X.sup-csc	ITU-T X.1051 - Supplement on critical security controls for telecommunication organizations	- ITU-T X.1051(T-ISMS) 국제표준을 근거로 인터넷보안센터로부터 접수되는 중점 보안통제들의 활용을 위한 프레임워크 정의 (부속서)
2	Q4 (사이버보안)	한국 (곽승환)	X.qrng-a	Quantum noise random number generator architecture	- 양자 키분배 시스템에서 난수발생기의 노이즈 소스의 엔트로피를 계산하고, 검증할 수 있는 보안구조를 정의
3	Q4 (사이버보안)	한국 (곽승환)	X.TR.sec-qkd	Technical report on security framework for quantum key distribution in telecom network	- QKD 관련 네트워크 구조, 보안구조, 보안위협 등 전반적인 보안기술 및 보안 프레임워크를 정의
4	Q5 (기술적인 방법에 의한 스팸대응)	중국 (Liu Wei 등)	X.tfcmms	Technical framework for countering multimedia messaging service spam	- MMS 서비스를 제공하는 통신사 관점에서 MMS 스팸을 통해 발생할 수 있는 보안 문제들을 분석하고, 기술적인 관점에서 대응하기 위한 기술들을 정의
5	Q6 (통신서비스, 사물인터넷 보안)	일본 (Koji Nakao 등)	X.elf-iot	Standard format of IoT error logs for security incident operations	- IoT 기기들의 침해대응을 효율적으로 관리하기 위한 IoT 에러 로그, 보안 로그 등에 대한 표준 포맷을 정의
6	Q6 (통신서비스, 사물인터넷 보안)	일본 (Koji Nakao 등)	X.amas-iot	Aggregate Message Authentication Scheme with Group Authentication Capability for IoT environment	- IoT 환경에서 그룹 인증을 제공하기 위해 각 기기들의 정보를 수집할 수 있는 메시지 인증 기술을 정의
7	Q6 (통신서비스, 사물인터넷 보안)	일본 (Koji Nakao), 중국(Lijun Liu)	X.sc-iot	Security Controls for Internet of Things (IoT) system	- IoT 시스템을 위해 ISMS를 근거로 위협, 보안원칙, 보안통제를 정의하기 위한 표준
8	Q6 (통신서비스, 사물인터넷 보안)	한국 (류호석, 윤미연, 정원석)	X.iotsec-4	Security Requirements for IoT devices and gateway	- IoT 기기와 게이트웨이에 적용 가능한 5가지(인증성, 암호성, 데이터보호, 플랫폼보호, 물리적보호) 보안영역의 보안 요구사항들을 정의
9	Q6 (통신서비스, 사물인터넷 보안)	중국(Jin Peng 등), 한국(염흥열))	X.5Gsec-t	Security framework based on trust relationship in 5G ecosystem	- 5G 생태계 내에 신뢰 관계를 기반으로 하는 보안 프레임워크를 정의
10	Q7 (안전한 응용서비스)	중국 (Min Zuo 등)	X.tfrca	Technical framework of risk control to support authentication	- 다중(Multi-factor) 인증기술들의 한계점을 극복하기 위해 사용자 중심 개선된 인증 프레임워크를 정의
11	Q8 (클라우드 컴퓨팅 보안)	중국 (Lei Xu 등)	X.sgcc	Security Guidelines for Container in cloud computing environment	- 클라우드 컴퓨팅 환경에서 컨테이너 서비스를 제공할 때, 보안위협 및 개선사항들을 정의하고 이를 위한 보안 지침을 정의
12	Q9 (텔레바이오인식	미국(John Caras), 덴마크(Erik Andersen), 한국(전명근)	X.b2m	Biology to Machine Protocol	- 원격의료서비스를 위한 프로토콜 및 일반적인 요구사항들을 정의
13	Q13 (ITS 보안)	한국 (이상우, 임화평, 조아람, 박승욱)	X.edrsec	Security guidelines for cloud-based event data recorders in automotive environment	- 자율주행 환경에서 사고 발생 시, 자동차의 상태, 주행정보, 사용자 입력 정보 등 각각의 데이터를 클라우드 기반으로 저장하기 위한 보안 지침
14	Q13 (ITS 보안)	한국 (이상우, 이유식)	X.eivnsec	Security guideline for Ethernet-based In-Vehicle networks	- 이더넷 기반의 차량 내부 네트워크를 위한 보안 지침 및 유즈케이스를 정의
15	Q13 (ITS 보안)	중국 (Yunwei Zhao 등)	X.fstiscv	Framework of security threat information sharing for connected vehicles	- 자율주행에서 보안위협을 대응하기 위한 유관 기관 간에 위협정보를 공유하기 위한 프레임워크를 정의
16	Q13 (ITS 보안)	일본 (Koji Nakao), 한국(이상우 등)	X.1373rev	Secure software update capability for intelligent transportation system communication devices	- 차량 내에 소프트웨어를 안전하게 업데이트하기 위한 국제표준(X.373) 내에 신규 기능을 추가하는 개정 작업
17	Q14 (분산원장기술)	중국(Yunwei Zhao 등), 한국(황정연, 기주희))	X.srip-dlt	Security requirements for intellectual property management based on distributed ledger technology	- 분산원장기술을 기반으로 지적재산권(IPR)의 등록 및 사용 등 전반적인 관리를 응용하기 위한 표준

〔표 5〕 신규 표준화 아이템 승인 목록(2019.1월)

No.	연구과제	제안국가 (에디터)	표준번호 (Acronym)	국제표준 제목	목적 및 주요내용
1	Q3 (보안관리)	말레이시아 (Thaib Mustafa 등)	X.ciag	Cyber insurance acquisition guideline for Information and Communication Technologies (ICT) services provider	- 사이버 보험 가입을 위해 가입자의 정보를 공유할 때 발생하는 보안위협 평가와 이를 해결하기 위한 보안지침을 정의
2	Q4 (사이버보안)	한국(심동희), 스위스(Matthieu Legré), 중국(Hao Qin 등), 일본(Kaoru Kenyoshi)	X.sec-QKDN -ov	Security Requirements for QKD Networks - Overview	- QKD 네트워크에서 활용 가능한 일반적인 보안 요구사항들을 정의 - QKD 네트워크를 위한 키관리 보안 요구사항들을 정의
3	Q4 (사이버보안)	일본(Kaoru Kenyoshi), 중국(Ziasun Ma 등), 한국(심동희)	X.sec_QKDN -km	Security Requirements for QKD Networks - Key Management	- SG13에서 개발하고 있는 QKD 네트워크 프레임워크를 고려하고, QKD 네트워크의 키관리 설계, 구현, 운영하기 위한 보안지침 및 보안 요구사항들을 정의
4	Q4 (사이버보안)	한국(심동희), 스위스(Matthieu Legré)	X.cf-QKDN	Use of cryptographic functions on a key generated in Quantum Key Distribution networks	- QKD 시스템에서 활용 가능한 현재 존재하고 있는 암호 표준들의 식별 및 활용 정의
5	Q4 (사이버보안)	중국 (Sheng Gao 등)	X.rdmase	Requirements and Guidelines for Dynamic Malware Analysis in a Sandbox Environment	- 샌드박스 내에 알려지지 않은 말웨어 행위를 탐지하기 위한 요구사항 정의와 이에 대한 위협 시나리오를 분석
6	Q4 (사이버보안)	일본(Youki Kadobayashi), 중국(Zhaoji Lin), 한국(오경희), 미국(Arnaud Tadde)i	TP.inno	Description of the incubation mechanism and ways to improve it	- SG17 구조조정을 위해 중점 보안기술들에 대한 중요성 및 필요성을 평가하기 위한 기술보고서 개발
7	Q4 (사이버보안)	일본(Youki Kadobayashi), 중국(Zhaoji Lin), 한국(오경희), 미국(Arnaud Tadde)i	TP.sgstruct	Strategic approaches to the transformation of security studies	- SG17 구조조정 및 보안표준 개발을 위한 전략적 접근방법에 대한 기술보고서 개발
8	Q6 (통신서비스, 사물인터넷 보안)	스위스 (Stiepan A. Kovac 등)	X.1197 /Amd.1	Amendment 1 of ITU-T Recommendation X.1197, Guidelines on criteria for selecting cryptographic algorithms for IPTV service and content protection	- IPTV 서비스를 위해 활용 가능한 암호 알고리즘들의 선정 기준 국제표준(X.1197)에 대한 신규 알고리즘을 추가하는 개정 작업
9	Q6 (통신서비스, 사물인터넷 보안)	중국 (Feng Gao 등), 한국(나재훈)	X.5Gsec-ecs	Security framework for 5G edge computing services	- 5G 에지 컴퓨팅 서비스를 위한 응용 시나리오 및 설치 방법을 분석하고, 보안위협 식별 및 보안 요구사항을 정의
10	Q6 (통신서비스, 사물인터넷 보안)	한국(염흥열, 김미연, 박근덕)	X.5Gsec-guid e	Security guidelines for 5G communication system based on ITU-T X.805	- 5G 통신 시스템의 주요 요소 및 기능을 식별 후, 각 요소에 대한 주요 위협 및 보안 능력을 정의
11	Q7 (안전한 응용서비스)	한국 (이예원, 임형진), 중국(Feng Gao)	X.rdda	Requirements for data de-identification assurance	- 개인정보 등 데이터 비식별에 대한 수준을 정의 및 측정하고, 비식별 조치가 적정하게 이루어졌는지 평가하기 위한 표준
12	Q8 (클라우드 컴퓨팅 보안)	중국 (Lei Xu 등)	X.sgdc	Security guidelines for distributed cloud	- 분산형 클라우드는 높은 속도와 고효율성 및 고성능의 장점이 있지만, 클라우드 간에 연계를 위한 인터페이스 등에 보안위협이 존재함. - 본 표준을 분산형 클라우드의 보안위협을 분석하고 이를 해결하기 위한 보안 지침을 정의
13	Q8 (클라우드 컴퓨팅 보안)	중국 (Jie Ma 등)	X.sr_cphr	Security requirements of cloud-based platform under low latency and high reliability application scenarios	- 저지연 및 고신뢰의 응용서비스를 제공하기 위해 클라우드 기반의 플랫폼을 많이 사용하고 있어, 본 서비스 환경의 보안위협 분석 및 보안 요구사항들을 정의

Ⅲ. 결 론

본 논문은 정보통신 보안 국제표준을 개발하고 있는 ITU-T SG17 국제표준화 동향에 대해 분석하였다. 특히, 양자암호통신, 5G 보안, AI 보안 표준화 활동에 대해 분석하였고, 최근 SG17 국제회의를 통해 신규 표준화 아이템으로 선정된 보안 주제들의 현황을 다루었다. 향후 신규 보안 주제들에 대해 관심이 있거나 국내 기술을 제안하고자 하는 산학연 전문가들께서는 처음 시작하는 단계에서 참여하는 게 필요할 것으로 판단된다.

한편, WTSA-20 전기통신표준화총회를 위해 SG17 연구반도 구조조정 이슈가 중요하게 논의되고 있어, 한국 의장단 및 산학연 전문가들의 협력이 요구되고 있다.

참 고 문 헌

[1] ITU-T 홈페이지, http://www.itu.int

[2] ITU-T SG17 홈페이지, http://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx

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

[4] 오흥룡, 염흥열, “ITU-T SG17 Q2 국제표준화 동향”, 정보보호학회지, 제27권 제5호, 2017.10.

[5] Kaoru KENYOSHI, SG17 Mini-workshop on Quantum communication, “Tokyo QKD Network and QKD standardization in ITU-T”, 2019.1.

[6] Andrew Shields, SG17 Mini-workshop on Quantum communication, “Current work of the ETSI ISG in QKD”, 2019.1.

[7] Jiajun Ma, SG17 Mini-workshop on Quantum communication, “Standardizing security certification of QKD in ISO/IEC JTC 1/SC27”, 2019.1.

[8] 염흥열, 오흥룡, “정보보호 기술 및 국제표준화 동향(ITU-T SG17)”, 정보보호학회지, 제24권 제4호, 2014.04.

[9] SG17-R25, Report of the fourt meeting of Study Group 17 (Geneva, 29 August - 7 September 2018) - Plenary sessions

[10] SG17-R33/Rev.1, Report of the fifth meeting of Study Group 17 (Geneva, 22-30 January 2019) - Plenary sessions

〈저 자 소 개〉

오 흥 룡 (Heung-Ryong Oh)

종신회원

2002년 2월 : 순천향대학교 전자공학과 학사 졸업

2004년 2월 : 순천향대학교 정보보호학과 석사 졸업

2018년 2월 : 순천향대학교 정보보호학과 박사 졸업

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

<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 공과대학 정보보호학과 정교수

2017년～현재 : ITU-T SG17 의장

2009년～2016년 : ITU-T SG17 부의장, WP3 의장

2011년 1월～12월 : 한국정보보호학회 회장(역)

2012년 1월～현재 : 한국정보보호학회 명예회장

2016년 5월～현재 : 개인정보보호표준포럼 의장

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