정 보 보 호 학 회 지
제28권 제4호, 2018. 8

ITU-T SG17(보안) 국제표준화 현황 및 추진 전망

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, 정보통신 환경에서 사용되는 정보보호 국제표준은 ITU-T SG17(보안, 의장: 순천향대 염흥열 교수)에서 담당하고 있다[2]. 본 논문에서는 2018년 3월 스위스 제네바에서 개최된 SG17 국제회의 주요 결과 및 향후 전망에 대해 분석하고자 한다.

Ⅰ. 서 론

ITU-T SG17은 정보통신망 보안, 응용 및 서비스 보안, 공개키기반구조(PKI), 바이오인식 등의 주요 정보보호 주제에 대한 국제표준을 개발하고 있다.

ITU-T SG17은 정보보호 분야 국제표준의 중복 개발을 막기 위해 ITU-T 내의 타 연구반과 다른 국제 표준화 그룹과의 협력을 강화하고 있다. ITU-T 내에서 정보보호 선도 연구반 역할을 수행하고 있어서 SG13(클라우드, 5G), SG20(IoT) 등의 타 연구반과 정보보호 분야 국제표준화 활동을 조정하고 있다.

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

ITU-T SG17은 ITU-T에서 11개의 연구그룹 중 유일하게 한국 전문가(순천향대 염흥열 교수)가 의장을 맡고 있는 표준화 그룹이다. 이번 연구회기(2017-2020)에서 연구반 17의 캐치플레이즈는 “보안은 어느 곳에서나 최우선이다(SAFE, security is absolutely first everywhere)”이다.

본 논문에서는 공식표준화기구 중에 ITU-T SG17 국제표준화 이슈(2018년 3월, 국제회의)를 중점적으로 분석해 향후 정보보호 분야에서 국제표준화 활동을 계획하고 있는 전문가들에게 유익한 정보를 제공하고자 한다. 이번 연구회기(2017~2020) 동안의 SG17 구조 및 의장단 정보 등 일반적인 사항은 참고문헌[3] 논문을 참고하기 바란다.

Ⅱ. ITU-T SG17 국제표준화 동향

ITU-T의 공식 회의는 연구반 회의와 라포처 그룹 회의(RGM, rapporteur group meeting)로 구분된다. SG17 국제회의는 보통 상·하반기로 1년에 2회 개최되고 있다. SG17 국제회의 사이에 열리는 RGM이 주로 표준초안의 품질 향상을 위해 개최된다. 연구반 회의에서는 국제표준의 최종 채택 등의 의사결정을 할 수 있는 회의이나, RGM 회의에서는 국제표준 채택과 신규 표준화아이템 채택 등의 의사결정이 필요한 안건을 다룰 수 없으며 특정 사안에 대한 합의를 도출하기 위한 사전 준비 회의이다.

본 장에서 2018년 3월에 개최된 SG17 국제회의 주요 결과를 중심으로 설명한다. 이번 국제회의는 총 40개 국가에서 총 130명의 국제표준화 전문가들이 참석하였고, 총 113건의 기고서가 검토되었다. 특히, 아래와

본 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임.
[*No.2017-0-00069, 공식표준화기구(ITU/APT등) 표준화대응연구, **No.20170000600021001, 사실표준화기구 전략대응 및 국제표준화전문가 활동강화]
* 한국정보통신기술협회 표준화본부(hroh@tta.or.kr)
** 순천향대학교 정보보호학과(hyyoum@sch.ac.kr)

같은 중요 주제를 다루었다.

· 5G 보안
· 지능형자동차(ITS) 보안
· 분산원장기술(DLT) 보안
· 클라우드 컴퓨팅 보안
· 분산형 ID 관리기술
· IoT 보안
· 보안관리
· SDN(Software-defined networking) 보안
· 빅데이터 보안
· 모바일 보안
· 개인정보 보호 기술

2.1. 국제표준 채택

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[4] 논문을 참고하기 바란다.

ITU-T에서 국제표준 개발이 완료되어 회원국 및 섹터멤버들에게 의견수렴으로 승인되는 단계를 TAP 승인(Determination), AAP 승인(Consent)이라고 말하고 있다. 차이점은 TAP 승인은 차기 국제회의에서 다시금 최종 채택 심의가 있고, AAP 승인은 4주간의 의견수렴 후, 심각한 문제가 없으면 이후 국제표준으로 채택 처리가 된다. 물론 의견수렴 중에 의견이 있을 경우, 서면으로라도 이를 해결하기 위한 그룹이 구성되어 이를 해결한다. 서면으로 해결하기 어려운 사항은 차기 국제회의에서 다시 논의한다.

이번에 채택된 국제표준과 합의된 부속서는 [표 1]과 같다. 이 표에는 2017년 9월 SG17 국제회의에서 TAP 절차로 결정(determination)되어, ITU 회원국 및 섹터멤버들에게 의견수렴한 후 승인된 국제표준들과 SG17 회의에서 바로 동의된 부속서의 목록이다. [표 2]는 2018년 3월 SG17 회의에서 AAP로 합의되어 4주간의 회원국 의견 수렴인 LC(last call)을 거쳐서 최종 국제

〔표 1〕 국제표준 채택 (TAP) 및 부속서 승인 목록(2018년 3월 SG17 회의)

No.	연구과제	제안 국가(에디터)	표준번호 (Acronym)	국제표준 제목	목적 및 주요내용
1	Q4 (사이버보안)	한국 (진병문, 인도)	X.1214 (X.samtn) - 국제표준	Security assessment techniques in telecommunication/ICT networks	- 통신망 보안 평가 기법을 정의 - 평가는 소프트웨어 기반 운영되는 시스템에 취약점을 탐지·분석하고 이를 객관점인 관점에서 평가하는 방법론을 정의
2	Q6 (통신서비스, 사물인터넷 보안)	한국 (이건희, 정소영, 박해룡)	X.1331 (X.sgsec-2) - 국제표준	Security guidelines for home area network (HAN) devices in smart grid systems	- 소비자와 직접 연관된 가정용 스마트 그리드 기기의 보안 기능을 정의 - 댁내 네트워크 환경에서 사용되는 디바이스들의 취약점 및 보안요구사항, 보안 기능들을 정의
3	Q8 (클라우드 컴퓨팅 보안)	중국	X.1603 (X.dsms) - 국제표준	Data security requirements for monitoring the service of cloud computing	- 클라우드 컴퓨팅 환경에서 모니터링 서비스를 위한 데이터 보안 요구사항을 정의 - 사용자의 개인정보 및 민감한 사항들에 대해 클라우드 서비스 제공자가 실시간으로 이를 탐지 및 관리, 대응하기 위한 기법을 정의
4	Q3 (보안관리)	한국 (염흥열, 고재남, 유승우)	X.Sup32 (X.sup-gpim) - 부속서	ITU-T X.1058 – Code of practice for personally identifiable information protection based on ITU-T X.1058 for telecommunications organizations	- 통신조직에서의 개인정보보호 특화 구현 지침을 제공 - X.1058(개인정보보호를 위한 실무 준칙)에서 정의되지 않은 통신 조직에 적용 가능한 구현 가이던스 제시

〔표 2〕 국제표준 채택 목록(AAP consent) (2018년 3월 회의에서 AAP consent, 2018년 5월 LC 후 채택)

No.	연구과제	승인절차	제안국가	표준번호 (Acronym)	국제표준 제목	목적 및 주요내용
1	Q2 (보안구조 및 프레임워크)	AAP (consent)	중국	X.1041 (X.voltesec-1)	Security Framework for VoLTE Network Operation	- VoLTE 네트워크 운영을 위한 보안 프레임워크 정의 - 네트워크 사업자 관점에서 보안위협 및 대응책, 구축 및 운영 방법을 위한 보안 가이드라인 정의 - 2018년 5월 13일, LC 이후 채택됨
2	Q9 (텔레바이오 인식)	AAP (consent)	덴마크	X.1080.1rev	e-Health and world-wide telemedicines - Generic telecommunication protocol	- e-헬스 및 텔레메딕스 환경에서 공통으로 사용될 수 있는 객체식별자를 정의 - 텔레메딕스 환경에 대한 일반적인 구조 및 통신 프로토콜을 정의 - 2018년 5월 13일, LC 이후 채택됨
3	Q10 (아이덴티티 관리 및 메커니즘)	AAP (consent)	미국	X.1276 (X.te)	Authentication Step-Up Protocol and Metadata Version 1.0	- OASIS 사실표준화기구에서 개발된 표준을 공식표준화기구로 이전해 채택한 사례 - 엔티티 고유의 크리덴셜 정보를 다루는 접근제어 구조에서 신뢰 상승(Trust Elevation) 메커니즘을 사용하기 위한 방법 및 메타데이터를 정의 - 2018년 5월 13일, LC 이후 채택됨

표준으로 채택되었다.

2.2. 국제표준 후보 승인

2018년 3월, SG17 국제회의에서는 보안 분야에 대해 2건의 국제표준에 대한 TAP Determination 로 [표 3]과 같이 합의 되었다. 이 국제표준은 2018년 9월 SG 17에서 최종 채택될 예정이다. 소프트웨어 분야 ASN.1 (추상구문표기법) 유지보수 표준에 대한 승인은 생략한다.

〔표 3〕 국제 표준 후보 채택 (TAP)

No.	연구과제	승인절차	제안국가 (에디터)	표준번호 (Acronym)	국제표준 제목	목적 및 주요내용
1	Q5 (스팸 대응)	TAP (determination)	중국	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 - 2018년 9월 회의에서 채택 예정
2	Q6 (통신 서비스, 사물인터넷 보안)	TAP (determination)	한국 (염흥열 외)	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 9월 회의에서 채택 예정

2.3. 신규 표준화 아이템 채택

2018년 3월 SG17 국제회의에서는 총 25건의 신규 표준화 아이템(NWI, new work item)들이 제안되어 총 20건이 승인되었다.

특히 5G 보안, 사이버보안, 빅데이터 보안, 지능형자동차 보안, 분산원장기술 보안 분야에서 신규표준화아이템이 수립되었다. 다음 [표 4]는 신규 표준화 아이템으로 승인된 목록으로 향후 2~4년 동안 표준초안 개발이 진행될 예정이다.

〔표 4〕 신규 표준화 아이템 승인 목록

No.	연구과제	승인절차	제안국가	표준번호 (Acronym)	국제표준 제목	목적 및 주요내용
1	Q2 (보안구조 및 프레임워크)	AAP	중국	X.SDsec	Guideline on Software-defined Security in SDN(Software-defined Networking)/NFV(Network Fuction Virtualization) Network	- SDN/NFV 네트워크 환경에서 소프트웨어 기반 보안서비스를 제공하기 위한 보안 가이드라인을 정의 - 다양한 표준개발기구(ITU-T, IETF, ETSI 등)에서 SDN/NFV 보안 표준들이 개발되고 있지만, 현재 네트워크 환경을 고려하고, 새로운 가상화 환경에서의 보안 적용 가이드라인이 없어, 이를 개발하는 데 중점적인 목적이 있음
2	Q3 (보안 관리)	AAP	미국	X.framcdc	Framework for the creation and operation of a Cyber Defense Center	- 사이버 방어 센터의 신설 및 운영을 위한 프레임워크를 정의 - 침해사고 및 보안 사고에 대한 모니터링 기능 및 대응 사례에 대한 최적 방법론을 정의
3	Q4 (사이버보안)	TAP	한국 (이주영, 문대성, 김종현, 김익균)	X.gcpie	Guidelines for Collection and Preservation of Cyber Security Incident Evidence	- 사이버보안 침해 사건에 대한 데이터 증거를 수집 및 보존하는 가이드라인을 정의 - 침해사건 조사에 대한 절차, 네트워크 트래픽 수집 장비 등을 정의
4	Q4 (사이버보안)	TAP	중국	X.fgati	Framework and Guidelines for Applying Threat Intelligence in Telecom Network Operation	- 네트워크 운영자 관점에서 네트워크 장비로부터 수집되는 취약점들을 탐지 및 대응하기 위한 상위 수준의 프레임워크 및 가이드라인 정의
5	Q5 (스팸 대응)	TAP	중국	X.tsfpp	Technical security framework for the protection of users' personal information while countering mobile messaging spam	- 모바일 메신저 스팸에서의 사용자 개인정보를 보호하기 위한 기술적 보안 프레임워크를 정의 - 모바일 메신저 스팸 솔루션에 대한 설계 및 구현관점에서 정의
6	Q5 (스팸 대응)	TAP	중국	X.tecwes	Technologies in countering website spoofing for telecommunication organizations	- 네트워크 운영자가 웹사이트 스푸핑을 대응하기 위한 기법을 정의 - 스푸핑 사례를 분석하고, 이에 대한 대응책으로 네트워크 운영자측면에서의 보안기술과 사용자측면에서의 보안기술을 정의

〔표 4〕 신규 표준화 아이템 승인 목록(계속)

No.	연구과제	승인절차	제안국가	표준번호 (Acronym)	국제표준 제목	목적 및 주요내용
7	Q6 (통신 서비스, 사물인터넷 보안)	Agreement	한국	X.Sup26-Cor	Corrigendum on ITU-T X Supplement 26	- 오류정정서에 대한 수정 제안
8	Q6 (통신 서비스, 사물인터넷 보안)	TAP	중국 (Hang Dong, 나재훈 외)	X.ssp-iot	Security Requirements and Framework for IoT Service Platform	- IoT 서비스 플랫폼을 위한 보안 요구사항 및 프레임워크를 정의 - IoT 서비스 플랫폼에 대한 보안위협 및 도전과제들을 분석하고, 이를 해결하기 위한 대응책을 정의
9	Q6 (통신 서비스, 사물인터넷 보안)	TAP	중국	X.5Gsec-q	Security guidelines for applying quantum-safe algorithms in 5G systems	- 5G 시스템에 적용되는 양자 알고리즘을 위한 보안 가이드라인을 정의 - 5G 시스템에 대한 보안구조 및 보안성 평가 방법을 정의
10	Q6 (통신 서비스, 사물인터넷 보안)	TAP	한국 (한종욱, 임경수, 김건우)	X.strvms	Security threats and requirements for video management system	- 지능형 CCTV와 같은 비디오 관리 시스템에서의 보안위협 및 보안 요구사항을 정의 - 단, 프라이버시 이슈에 대해서는 다루지 않음
11	Q7 (안전한 응용 서비스)	AAP	중국 (Hang Dong, 나재훈 외)	X.sgos	Security guidelines of Web-based online customer service	- 네트워크 운영자가 온라인을 기반으로 사용자 및 전용 고객을 대응하기 위한 보안 가이드라인을 정의 - 특히 사용자 민감 정보를 보호하기 위한 네트워크, 시스템, 서비스 관점에서 보안 가이드라인을 정의
12	Q8 (클라우드 컴퓨팅 보안)	TAP	중국, 미국	X.sgBDIP	Security Guidelines for Big Data Infrastructure and platform	- 세계 다양한 표준화 협의체에서 정의한 빅데이터 플랫폼 및 인프라구조를 분석해서, 최적화된 보안 가이드라인을 정의
13	Q9 (텔레바이오인식)	AAP	말리, 세네갈	X.tas	Telebiometric authentication using speaker recognition	- 사용자 음성 인식을 이용한 텔레바이오인식 인증기술을 정의 - 사전에 등록된 텍스트를 인식하거나 무작위로 선정된 텍스트를 인식하는 방법이 고려됨
14	Q10 (아이덴티티 관리 및 메커니즘)	TAP	미국	X.1252rev	Baseline identity management terms and definitions	- 아이덴티티 관리 분야에 대한 용어 및 정의를 추가해서 개정하고자 함
15	Q11 (안전한 응용을 지원하기 위한 일반 기술)	AAP	중국	X.uav-oid	Identification mechanism for unmanned aerial vehicles using object identifiers	- 객체식별자를 이용한 무인항공기에 대한 식별 메커니즘을 정의 - 객체식별자 등록 절차 및 OID 할당을 위한 규칙 및 데이터 구조 등을 정의

〔표 4〕 신규 표준화 아이템 승인 목록(계속)

No.	연구과제	승인절차	제안국가 (에디터)	표준번호 (Acronym)	국제표준 제목	목적 및 주요내용
16	Q13 (지능형자동차 보안)	TAP	중국	X.mdcv	Security-related misbehaviour detection mechanism based on big data analysis for connected vehicles	- 컨넥티드 카를 위한 빅데이터 분석 기반의 보안 관련 오작동 탐지 메커니즘을 정의 - 오작동 탐지를 위한 수집 정보 및 데이터 포맷 정의 - 빅데이터를 이용한 오작동 분석 기술에 대해 메커니즘 정의
17	Q13 (지능형 자동차 보안)	TAP	한국 (박승욱, 이상우, 김창오 외)	X.stcv	Security threats in connected vehicles	- 컨넥티드 카에 대한 보안 모델을 정의하고 상위 수준에서의 보안위협을 분석 - Q13 내에서 다루고 있는 모든 표준들을 고려해서 개발하기로 함
18	Q13 (지능형 자동차 보안)	TAP	중국	X.srcd	Security requirements for categorized data in V2X communication	- V2X 차량 통신에서 사용되는 데이터는 다양한 형식으로 존재하고 있어, 이를 분류하고 각각의 보안수준 및 보안요구사항을 정의
19	Q14 (분산원장기술 보안)	AAP	한국 (염흥열,김미연, 박근덕)	X.das-mgt	Security framework for the data access and sharing management system based on the distributed ledger technology	- 분산원장기술 기반 데이터 접근 및 공유 관리 시스템을 위한 보안 프레임워크를 정의 - 정보주체의 동의에 근거한 데이터 이용 추적 시스템을 고려한 보안위협, 보안요구사항 및 보안기술을 정의
20	Q14 (분산원장기술 보안)	AAP	중국	X.tf-spd-dlt	Technical Framework for Secure Software Programme Distribution Mechanism Based on Distributed Ledger Technology	- 분산원장기술 기반 안전한 소프트웨어 프로그램 분산 메커니즘을 위한 기술적 프레임워크를 정의 - 서비스 제공자가 사용자에게 운영체제 및 보안서비스 등을 안전하게 업데이트 시키고자 할 때, 분산원장기술을 이용하는 메커니즘 정의

2.4. 중요 토픽

SG17 국제회의에서 최근 중요한 토픽으로 떠오르고 있는 이슈는 다음과 같다.

· 5G 보안 - 이번 국제회의 개최 전날 5G 보안 워크숍이 개최되었고, 총 34개국에서 125명의 전문가가 참석하였다. 이번 워크숍에서는 5G 통신을 위한 보안위협 및 보안요구사항, 5G 보안 개요, 5G 통신에서 보안위협을 감소시킬 수 있는 방법에 대한 주제로 한국 KT를 포함해서 전 세계 통신사들이 생각하고 있는 이슈들에 대해 발표 및 토론이 개최되었다. SG17 연구반은 이번 워크숍 결과를 근거로 향후 5G 기반의 다양한 보안기술 및 보안서비스들에 대한 표준화 발굴이 예상된다.

· 분산원장기술 보안 - 2017년 8월, 한국 주도로 신설된 연구과제 14는 2018년 3월 회의에서 수립이 채택되었다. 경과를 살펴보면 2017년 9월 SG17 회의에서 한국 제안으로 연구과제 수립이 합의되었고, 2018년 2월 TSAG 회의에서 동의되었으며, 2018년 3월 SG17 회의에서 수립이 완료되었다. 분산원장기술 보안은 현재 SG17 내에서도 가장 관심을 받고 있는 주제이다. SG17 국제회의 총 2회를 통해 신규 표준화 아이템이 총 9건이 발굴되어 추진되고 있으며, 전 세

계 산학연 보안전문가들이 적극적으로 참여하고 있는 그룹이다. 이중 한국은 4건의 신규워크아이템(순천향대 등)을 제안해 채택했으며, 5건의 개발 중인 워크아이템의 에디터를 수임하고 있다. 블록체인 기술이 새로운 보안 연구주제로 떠오르면서 다양한 표준화 협의체에서 동일한 주제를 다루고 있어, 이에 대한 중복성 및 표준화 영역에 대한 조율이 필요한 시점이다.

· 지능형자동차 보안 - 2017년 3월, 한국 주도로 신설된 연구과제 13은 현대자동차가 ITU-T 섹터멤버로 가입하면서 전 세계적으로 주목받고 있는 이슈이다. 현대자동차는 국내 고유기술에 대해 국제표준에 적극적으로 반영하고 있으며, 일본, 중국, 미국, 영국 등 주요 국가들도 적극적으로 참여하고 있다.

Ⅲ. 결 론

본 논문에서는 정보통신 보안 국제표준화를 선도하고 있는 ITU-T SG17 국제표준화 동향에 대해 분석하였다. 특히, 신규 표준화 아이템으로 선정된 이슈들은 최근 국내 산업체에서도 중요하게 다뤄야 할 주제들이 다수 존재하고 있어, 국내 정보보호 기술을 국제표준에 반영시키기 위해 적극적인 활동이 요구된다.

한국은 SG17 국제회의 마다 많은 전문가로 구성된 대표단 파견과 다수의 기고서를 제안해 주도권을 확보하고 있었다. 그러나 최근 중국의 적극적인 참여에 선두를 빼기고 있는 상황이다.

한국의 표준화 추진 전략은 표준특허 발굴이 가능하고, 국내 산업체에 도움이 될 수 있으며 국가 정보보호 및 개인정보 보호 정책 추진을 지원할 수 있는 핵심 표준화 이슈들을 선정해서 집중적으로 국제 표준화를 추진하는 게 필요할 것으로 판단된다.

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

[5] 오흥룡, 염흥열, “ITU-T SG17(보안) 국제표준화 동향”, 정보보호학회지, 제26권 제4호, 2016.8.

[6] SG17-R18, Report of the third meeting of Study Group 17 (Geneva, 20-29 March 2018) - 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 책임연구원
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