정 보 보 호 학 회 지
제24권 제4호, 2014. 8

정보보호 기술 및 국제표준화 동향(ITU-T SG17)

염 흥 열*, 오 흥 룡**

요 약

국제전기통신연합(ITU)은 UN 산하에 신설된 국제기구로써, 산하에 전기통신표준화부문(ITU-T), 전기통신개발부문(ITU-D), 그리고 전파통신 부문(ITU-R) 등의 3개의 부문으로 구성되어 있다[1],[2]. ITU-T에서는 역할과 임무에 따라 10개의 연구반 (SG, study group)으로 나눈다. 이중 연구반 17(SG 17)은 ITU-T에서 정보보호 국제표준화를 주로 담당하고 있다[2].

본 논문에서는 국제전기통신연합 내에서 정보보호 국제표준화를 추진하는 ITU-T SG17(정보보호) 활동의 근거를 제공하는 상위수준 회의 (ITU 전권회의, 세계정보통신표준총회)의 주요 결의를 살펴보고, ITU-T의 두 가지 권고채택과정을 분석하며, ITU-T SG17에서 대두되고 있는 주요 표준화 이슈에 대해 제시한다.

Ⅰ. 서 론

우리의 일상생활이 정보통신기술의 의존성이 증가하고 있고, 스마트폰 등의 도입으로 인해 전통적 의미의 전기통신망과 인터넷 간의 경계 구분이 불분명해지고 있다. 또한 피싱, 파밍, 스캔/침입, 홈페이지 변경, 비인가된 접근 등과 같은 사이버공격이 증가하고 있고 이의 부정적인 영향이 커지고 있다. 사이버보안은 정보통신기술의 이용에 있어서 신뢰성과 보안을 향상시키기 위한 중요한 수단으로 간주되고 있다. 국제전기통신연합(ITU)은 국제연합(UN, united nation) 산하에 신설된 국제기구로써, 전기통신표준화부문(ITU-T), 전기통신개발부문(ITU-D), 그리고 전파통신 부문(ITU-R) 등의 3개의 부문으로 구성되어 있다. ITU-T에는 역할과 임무에 따라 10개의 연구반(SG, study group)이 존재한다[1],[2]. 이중 SG 17은 정보보호분야의 국제표준을 개발하고 있다[2]. 본 논문에서는 국제 표준을 권고(Recommendation) 또는 국제표준으로 혼용해 사용한다[12].

본 논문 제2장에서는 ITU-T SG17 국제 표준 추진과 연관된 정책 방향을 포함하는 상위수준 회의의 주요 결과물을 살펴보고 권고채택과정을 분석하며, 제3장에서는 향후 대두되고 있는 표준화 이슈에 대해 분석하고 향후 대응방안을 제시한다.

Ⅱ. 정책 방향 및 SG17 구조

ITU-T SG17 국제 표준화 추진 방향은 매 4년마다 열리는 ITU 전권회의(PP, plenipotentiary conference)와 세계정보통신표준총회 (WTSA, world telecommunication standardization assembly)의 정책 방향에 근거하고 있다. 본 장에서는 ITU-T SG17 활동의 근거가 되는 상위수준 정책 방향을 살펴보고, 2가지 대표적인 국제표준 채택 과정을 살펴본다.

2.1. ITU PP-2010 결의

ITU PP는 ITU에서 최고위급 정책 결정 회의로써, 산하 3개의 부문(sector)에 대한 연구 방향을 결정하고 각 부문의 운영을 담당할 고위직을 선출한다[3]. 지난 2010년 멕시코에서 열린 PP-10에서 산출된 ITU-T SG17 관련 결의(Resolution)는 결의 130, 결의 179, 결의 181 등 이며[3], SG17은 이 결의에서 지시된 정책 방향에 따라 국제 표준화를 추진하고 있다[4]. [표 1]은

본 연구는 한국연구재단의 지원을 받는 일반연구자지원사업의 연구 결과로 수행 됨.(스마트폰 보안성 향상연구: NRF-2010-0025393)
* 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr)
** 한국정보통신기술협회 표준화본부 (hroh@tta.or.kr)

〔표 1〕 ITU-T SG17 과 연관된 ITU PP-10 결의(2010)〔4〕

결의 번호	제목	주요 내용 (SG 17관련)	SG17 관련활동
결의 130	(영문제목) Strengthening the role of ITU in building confidence and security in the use of information and communication technologies (한글제목) 정보통신기술의 활용에 있어서 신뢰와 보안을 구축하기 위한 ITU의 역할 강화	• 신뢰와 보안을 구축하기 위한 정보의 가용성을 향상할 것 • 침해사고대응팀 (CIRT) 신설하기 위한 모범 사례를 식별하고, 참조 가이드를 준비할 것 • 관련 국제기구와 전문가와 협력해 침해사고대응팀 신설을 위한 모범사례를 개발할 것 • 새로운 연구과제 신설을 목적으로 필요한 조치를 취할 것	• 연구과제 3(Q.3) - 보안 사고 대응 지침 • 연구과제 4(Q.4) 사이버 보안 정보 교환 프레임 워크
결의 179	(영문제목) ITU's role in child online protection (한글제목) 온라인 아동보호를 위한 ITU의 역할	• 온라인 아동보호를 위한 글로벌 단일 전화번호의 도입 가능성을 SG2와 협력하여 연구할 것 • ITU가 인식 제고를 위한 플랫폼으로 온라인 아동보호 계획을 지속적으로 추진	• 2012년 3월 SG17 회의에서, 온라인 아동보호-조 인 트 조 정 활 동 (JCA-COP) 신설[12] • 현재, SG17 내에 기술적 관점에서 표준초안 개발 위한 연구가 진행 중
결의 181	(영문제목) Definitions and terminology relating to building confidence and security in the use of information and communication technologies (한글제목) 정보통신기술의 활용에 있어서 신뢰와 보안을 구축과 관련된 용어정의	• ITU-T SG17이 정보통신 및 ICT 보안에 대한 핵심 국제표준을 개발하고, 권고 X.1205에 용어 “사이버보안”을 정의하고 있음을 고려해, • ITU-T 국장에게 사이버보안 용어와 관련된 신규 또는 개정 권고를 ITU 이사회에 보고할 것	• SG17 회의에서 사이버 보안 용어와 관련 신규 또는 개정 권고를 보고하고 있음

정보보호와 관련된 주요 결의의 내용과 SG17 내 주요 활동과 결과를 나타내고 있다.

2.2. WTSA-12 결의

세계정보통신표준총회는 연구회기(study period)로 불리는 4년마다 열리며, 연구회기 시작점에서 ITU-T SG를 위한 전반적인 정책 방향과 SG 구조를 결정한다[5]. 구체적으로 ITU-T의 일반 정책방향을 설정하고, 국제표준화를 담당할 SG를 수립하며, 연구회기 동안 수행될 작업의 범위와 내용, 그리고 SG 의장과 부의장을 임명한다. 세계정보통신표준총회의 결과물은 일련의 결의(Resolution)로 나타난다.

2012년 아랍에미레이트 두바이에서 열린 WTSA-12에서는 SG별 활동 실적 및 회원국들의 요청에 근거해 차기 연구회기(2013-2016)에 대한 SG 구조를 변경하고 수립된 SG의 의장과 부의장을 포함한 의장단을 선출했다[5].

WTSA-12 회의에서 합의된 SG17 정보보호 표준화 활동과 연관된 결의는 [표 1]과 같이 결의 50(사이버보안)[9], 결의 52(스팸 대응/전투)[10], 결의 58(개발도상국을 위한 국가 컴퓨터 침해대응센터 신설 장려)[11] 등이다.

특정 이슈가 하나 이상의 연구반에 걸치는 경우, 각 이슈별로 특정 SG을 선도 연구반 (Lead SG)으로 지정해 여러 SG에 걸친 표준화 작업을 책임지게 한다[7]. WTSA-12 결의 2는 SG의 일반 연구영역, 선도 연구반, 차기 연구회기를 위한 작업 프로그램 개발을 위한 요약 지침, 그리고 책임 권고 목록을 규정하고 있다. 그중 SG17에게 할당된 사항은 다음과 같다[7].

- 일반 연구 영역 : 정보통신기술의 이용에 있어서 신뢰와 보안을 구축하는 것을 책임짐. 여기에는 사이버보안, 스팸대응, 보안관리, 그리고 아이덴터티 관리를 포함하며, 이외에도 보안 구조, 개인정보보호, 응용 및 서비스 보안의 연구도 포함.
- 선도 연구반(Lead SG) : 보안 선도 연구반, 아이덴터티 관리 선도 연구반, 언어 및 서술 기술 선도연구반

〔표 2〕 ITU-T SG17 과 연관된 WTSA-12 결의(2012)

결의 번호	제목	주요 내용 (SG 17관련)	SG17 관련활동
결의 50	(영문제목) Cybersecurity (한글제목) 사이버보안	• 기존 또는 신규 권고의 강건성과 악용 가능성에 대해 검토하고, 신규 보안 이슈에 대한 신규 권고를 개발하며, 다양한 신규 응용과 서비스를 고려해야 함 • 인식제고 활동과 기술 정보 교환을 위한 관련 국제기구와의 협력 증진 • ITU-T 권고를 고려해 네트워크와 프로토콜의 보안 취약성을 평가하고 사이버 보안 정보 교환을 촉진 • ITU-T는 정보통신기술의 활용에 있어서 신뢰와 보안을 구축과 관련된 용어 정의를 개선하고 개발 • 표준 개발 진행 상황을 정보통신표준자문반(TSAG)에 정기적으로 보고 • 연구반 17은 PP-10에서 제기된 이슈와 권고에 대한 작업을 계속 추진	• 사이버보안 용어 정의 및 권고를 개발하고 있으며, TSAG에 활동 결과 및 진행상황을 보고하고 있음
결의 52	(영문제목) Countering and combating spam (한글제목) 스팸 대응/전투	• 스팸이 사이버범죄와 사기활동에 이용되고 있어서, • 관련 연구과제(Question)에서 스팸 관련 기존 작업을 계속 추진 • IETF 등과 같은 다른 국제기구와 협력 • SG17에서 이 결의 이행상황을 TSAG에 보고 • 스팸 트래픽의 유형, 크기, 특징 등에 대한 연구를 시작할 것을 지시함	• 매 SG17 회의마다 TSAG에 결의 이행 상황을 보고하고 점검함 • 이 논문 작성 시점에, 정보통신표준국(TSB)는 결의에서 지시된 스팸 관련 연구를 회원국 설문을 통해 진행하고 있음
결의 58	(영문제목) Encourage the creation of national Computer Incident Response Teams, particularly for developing countries (한글제목) 개발도상국을 위한 국가 컴퓨터 침해대응센터 신설 장려	• 개도국의 컴퓨터 침해사고대응센터는 적절히 운영되도록 하며, 글로벌 컴퓨터 침해사고대응센터 참여 수준을 개선하는 것을 고려 • 회원국에서 컴퓨터 침해사고 대응센터의 신설을 지원할 것 • 전기통신표준국장에게 CIRT의 신설 모범사례를 찾고, CIRT 신설이 필요한 국가를 식별하고, 국가 CIRT간의 협력을 촉진할 것을 지시함	• SG17 회의에서 Q.3/17을 중심으로 CIRT 설립 관련 권고 또는 구현가이드를 개발하고 있음

- SG17 작업 프로그램 개발을 위한 요약 지침 : (1) 사이버보안, 정보보호 관리, 스팸대응 등과 같은 ICT 보안, (2) 응용과 서비스 보안, 범용 아이덴터티 관리 모델, (3) 공개키기반구조/ 객체식별자/ 개방형 시스템 상호 연결 등에 대한 핵심 표준 개발
- 책임 권고 목록 : X-계열 ITU-T 권고, E.104, E.115, E.409 등

2.3. SG17 구조 (2013-2016)

새로운 연구회기(2013~2016)를 맞아 첫 번째 ITU-T SG17 국제회의(2013.4.17~26, 스위스 제네바)는 WTSA-12 회의에서 승인된 연구과제(Question)를 기능별로 나눠서 작업반(WP) 별로 재구성했다[2]. SG17은 하부에 5개의 작업반(WP)로 구성되었고, 각 WP는 2개 이상의 연구과제(Q, Question)로 구성되었다. 확정된 SG17 구조는 [표 3]과 같이 총 12개의 연구과제(Question), 해당 연구과제들을 다시 묶는 5개의 작업반(WP)으로 구성되어 있다. 참고로 권고를 승인할 수 있는 권한은 SG 회의나 WP 회의에게 주어진다.

〔표 3〕 ITU-T SG17 구조 (2013-2016)〔2〕

구분		제목	연구과제 주요 역할
작업반 1(WP1)		핵심 보안	-
	Q.1	통신/ICT 보안 조정	• 보안 전략, 비전, 계획, 로드맵 등 SG17 내 연구과제간 활동 조율
	Q.2	보안구조 및 프레임워크	• 보안 구조, 모델, 개념, 전반적인 서비스 시나리오 등을 연구
	Q.3	통신부문 정보보호 관리체계	• 통신부문 보안관리 표준 개발
작업반 2(WP2)		네트워크 및 정보보안	-
	Q.4	사이버보안	• 사이버공격 대응기술, 사이버보안 정보공유 방법 등 연구
	Q.5	스팸의 기술적 대응	• 스팸의 기술적 대응 표준 개발
작업반 3(WP3)		아이덴터티 관리 및 클라우드 컴퓨팅 보안	-
	Q.8	클라우드 컴퓨팅 보안	• 프레임워크, 메카니즘 등 클라우드 컴퓨팅 보안
	Q.10	아이덴터티 관리 구조 및 메카니즘	• 아이덴티티(Identity) 관리 기술과 기반 인증 서비스들에 대한 표준 개발
작업반 4(WP4)		응용 보안	-
	Q.6	유비쿼터스 통신 서비스 보안	• IPTV 보안, USN 보안, 모바일 보안, 멀티캐스트 보안, 홈 네트워크 보안, RFID 보안 등의 표준 개발
	Q.7	안전한 응용 서비스	• P2P 보안, 웹서비스 보안, 응용프로토콜 보안, 제3의 신뢰기관(Trusted Third Party) 기반 인증 기술 등의 국제 표준 개발
	Q.9	텔레바이오메트릭	• 네트워크 기반 바이오 정보를 이용한 인증 기술에 대한 표준 개발
작업반 5(WP5)		포멀 언어	-
	Q.11	안전한 응용을 지원하기 위한 일반 기술	• 안전한 응용을 지원하기 위한 일반 기술들에 대한 표준 개발
	Q.12	통신 소프트웨어와 시험을 위한 공식 언어	• 다양한 형식 언어에 대한 표준 개발

2.4. 권고 채택 과정

ITU-T 권고 채택 과정은 기존채택과정(TAP, traditional approval procedure)[6]과 대체채택과정(AAP, alternative approval procedure)[13] 등으로 구분되다. SG 회의에서는 개발 중인 권고가 충분하게 완성도가 있다고 판단되면, 권고채택을 위한 마지막 과정을 개시할 수 있다.

WTSA-12 결의 1(8절과 9절) 에서는 특정 권고의 채택 과정을 선택하는 사항을 규정하고 있다[6]. 만약 채택될 권고 후보가 번호체계와 주소(numbering and addressing), 과금과 정산(tariff and accounting) 등과 같은 정책과 규제 합의 사항을 포함하면 해당 권고는 TAP를 따라야 하며, 그 외 권고는 AAP를 따라야 한다.

WTSA-12 결의 40에서는 권고가 정책 또는 규제적 함의를 갖는 지 여부를 결정할 때 연구반은 다음과 같은 주제를 고려해야 하도록 규정하고 있다[8].

서신에 관한 권한
전기통신 채널과 설치의 보호
번호나 주소의 제한된 자원의 이용
명명 및 식별
전기통신의 비밀성과 인증
생활 안전
시장 경쟁에 적용할 수 있는 관행
번호자원의 오용
그 외 다른 사항

AAP와 TAP와의 차이점은 [표 4]와 같다.

〔표 4〕 기존채택과정(TAP)과 대체채택과정(AAP)의 비교

	기존채택과정	대체채택과정
채택대상 표준 성격	• 번호/주소, 요금/과금/정산 등의 정책이나 규제적 함의를 갖는 성격의 권고인 경우, TAP 적용	• 그 외 권고(기술적 관점)는 AAP 적용
권고 성숙도 판정	• SG 또는 WP 회의에서 판단해, 권고 성숙도가 인정되면 문서를 결정 (determination) 함	• SG 또는 WP 회의에서 판단해, 권고 성숙도가 인정되면 문서를 동의(consent) 함
국가별 의견수렴	• 통상 SG 또는 WP 회의 종료 후 최소 3개월 동안의 국가별 의견수렴과정(consultation) 거침 • 국가별 의견 수렴기간동안, 70% 이상의 회원국이 다음 SG 회의에서 채택을 지지하면, 다음 SG 17 회의에서 해당 의견을 반영해 채택 여부 결정	• 통상 SG 또는 WP 회의 종료 후 4주간의 최종검토(LC, last call) 과정 거침 • LC 기간 동안 회원국으로부터 의견 없으면 바로 채택됨 • LC 기간 동안 기술적 의견이 도착하면, 의견을 수렴한 문서를 만들어 추가검토(AR, additional review) 과정 거침 • AR 동안 의견이 없으면, 권고 채택됨 • AR 동안 기술적 의견이 도착하면, 다음 SG 회의에서 채택 여부를 최종 결정
채택 의사결정 메카니즘	• 만장일치 (하나의 회원국이 타당한 사유로 권고의 채택을 막을 수 있음)	• SG 회의에서 반대 없는 합의가 이뤄지면 채택된 것으로 간주함 • 만약 반대 없는 합의가 이뤄지지 않는다면, 둘 이상의 회원국이 반대하지 않은 경우, 회의에 참석한 부문회원들과 협의 후 권고는 채택된 것으로 간주함 • 하나의 회원국이 반대하는 경우, 유보사항을 해당 권고의 노트로 기술됨
권고 채택 권한 회의	• SG 회의 또는 WP 회의	• TAP 와 동일

Ⅲ. ITU-T SG17 주요 표준화 이슈

본 절에서는 SG17에서 추진 중인 주요 표준화 주제 중 에서 한국 주도로 권고가 개발되고 있거나 산업적 파급효과가 커서 우리나라의 적극적인 대응이 필요한 분야 (개인정보보호 지침, 지능형 차량보안, SDN 보안 등)의 주요 표준화 이슈를 제시하고 향후 대응방안을 논한다[14],[15],[16],[17],[18].

3.1. 개인정보보호 지침

ITU-T SG17 Q.3에서는 “통신조직을 위한 개인정보보호 관리 지침(X.gpim)” 권고를 2011년 9월부터 개발하고 있고, ISO/IEC JTC 1/SC 27/WG 5에서는 “개인정보보호 지침(ISO/IEC 29151)” 을 2013년 4월부터 개발하고 있다[14],[19]. 두 표준의 목적과 내용을 비교해 보면 [표 5]와 같다.

〔표 5〕 ITU-T X.gpim과 ISO/IEC 29151 비교(2014.4)

	X.gpim	ISO/IEC 29151
목적	• 27001 기반 개인정보 관리체계를 지원하기 위한 통제/구현가이드라인 등의 지침 개발	• 동일
기반 문서	• ISO/IEC 27002	• ISO/IEC 27002
표준 구조	• 5절-18절 (27002 구조) + 19절 (개인정보 특화 통제/구현가이드라인) + 부록 (개인정보보호원칙)	• 5절-18절(27002 구조) + 19절(개인정보 특화 통제/구현가이드라인) + 부록
적용 대상	• 통신 조직	• 일반 조직
문서 상태	• 4th 수정텍스트	• 3rd WD

2014년 4월 ITU-T SG17/Q.3 와 SC 27/WG 5 조인트 회의에서는 두 개의 국제표준의 내용과 목적, 구조가 매우 비슷해 두 표준화 기구가 공동으로 개발하는 공통텍스트(common text)로 개발하기로 결정했다. 즉, 두

공적 표준화 기구가 ITU-T X.gpim|ISO/IEC 29151 으로 일반 조직을 위한 공동 표준으로 개발키로 하였다.

또한 2014년 6월 서울에서 열린 Q.3 인터림 회의에서는 이의 후속 조치로 “통신조직을 위한 개인정보관리 지침”에 대한 표준을 부속서(Supplement) 형태로 ITU-T SG17에서만 개발키로 합의했고, 이의 신규워크아이템의 채택은 2014년 9월 SG17 회의에서 결정키로 하였다[19].

3.2. 지능형 차량 보안

지능형 차량보안은 2013년 9월 SG17 회의부터 지능형 자동차보안 분야의 신규워크아이템 채택 여부를 논의해 왔다. 지난 1월 SG17 회의에서는 한국의 신규워크아이템 제안을 통해 지능형 차량을 위한 통신 형태가 V2V (vehicle-to-vehicle), V2I (vehicle-to-nfrastructure), V2N (vehicle-to-nomadic) 형태의 통신을 고려해야 한다고 합의했고, 연구반 16의 관련 연구과제와 협력해 개발키로 했다[17]. 한편, 2014년 6월 Q.6 인터림 회의에서는 일본에서 “지능형 차량보안을 위한 소프트웨어 업데이트”에 대한 신규워크아이템을 제안하였다[20].

따라서, 2014년 9월 SG17 회의에서는 한국, 일본 등의 신규워크아이템 제안이 논의될 예정이며, 논의 결과에 따라 신규워크아이템 채택이 추진될 예정이다.

3.3. SDN 보안

지난 1월 SG17회의에서는 한국의 제안으로 SDN 보안 표준 개발 필요성이 제기되었다. 당시 회의에서는 SDN 보안은 “SDN 자체 보안(security of SDN)” 이슈와 “SDN을 활용한 보안(security by SDN)” 이슈가 존재한다고 확인했다. 따라서 분야를 나눠서 security of SDN은 연구과제 2에서 개발하고, security by SDN은 연구과제 6에서 개발키로 합의했다[14],[17].

또한, SDN 표준화 추진이 SG13에서도 추진됨을 고려해 SDN 표준 추진의 태스크를 클라우드 컴퓨팅 보안을 위한 태스크 할당과 유사하게 태스크를 구분해 추진할 것을 SG13에 요청하는 연락문서를 보낸바 있다.

2014년 6월, 연구과제 2와 6 조인트 인터림 회의에서 두 가지 분야에 대한 신규워크아이템 추진이 한국에서 제안되었다[21].

Security of SDN: SDN framework and SDN requirements

Security by SDN: Use case (Centralized Network Firewall)

따라서, 다음 9월 SG17 회의에서는 SDN 신규워크아이템에 대한 채택 여부가 결정될 것으로 예정이다.

Ⅳ. 결 론

본 논문에서는 새로운 연구회기(2013~2016) 동안 SG17의 국제 표준 추진의 근거가 되는 ITU 상위수준회의 관련 결의의 내용을 분석했다. 또한, 권고 채택을 위한 두 가지 채택과정을 분석했다. 현재 SG17 표준화 이슈중 한국주도로 추진되고 있거나 산업적 파급효과가 클 것으로 예상되는 몇 가지 주제에 대한 이슈를 분석하고 향후 대응 방안을 살펴 보았다.

2000년 중반부터 한국은 매 SG17 회의마다 많은 전문가로 구성된 대표단을 파견해 오고 있으며, 그 동안 SG17 부의장, WP 의장, 여러 연구과제의 라포처 등의 의장단 활동과 국제표준 개발을 책임지는 에디터 역할을 통해 SG17 국제 표준화 활동에 크게 공헌해 오고 있는 것은 미국, 일본 등에서도 인정하고 있다.

그러나, ITU-T 국제표준화는 정부가 대표단을 파견하고 의사결정도 정부의 주도로 이뤄지는 국가간 표준화 기구이고, 표준 채택을 위한 의사결정과정의 엄격한 측면이 존재하고 있다. 또한, 국가의 입장에 따라 ITU-T에서 국제 표준화를 적극 추진하고자 하는 회원국 그룹과 단지 ITU-T 표준화 과정을 관찰해 의사결정 과정을 통해 자국의 이익에 피해가 될 수 있는 신규 워크아이템이나 권고 채택을 막으려는 국가 그룹으로 구분되고 있다.

한국 입장에서는 ITU-T SG17 국제표준화 기구를 이용해 국내 정보보호 기술을 국제표준화로 추진함에 있어, 여타의 사실표준화 기구에서 추진하는 것보다는 이롭다는 측면이 있다.

따라서, 정부, 정보보호 산업체, 학계, 공공기관 전문가가 서로 협력해 ITU-T에서 전략적 정보보호 국제 표준화 추진이 필요한 시점이다.

참 고 문 헌

[1] ITU-T 홈페이지, http://www.itu.int

[2] 오흥룡, 김영화, 염흥열, “ITU-T SG17 국제표준화 동향 및 향후 전망” 정보보호학회지, v.23, no.3, 2013.06.

[3] ITU Plenipotentiary Conference : PP-10, http://www.itu.int/plenipotentiary/2010/

[4] ITU PP-10, Final acts of the plenipotentiary conference (Guadalajara, 2010), http://www.itu.int/dms_pub/itu-s/oth/02/01/S020100003A4002PDFE.pdf

[5] WTSA-12, http://www.itu.int/en/ITU-T/wtsa12/ages/efault.aspx

[6] WTSA-12, Resolution 1 – Rules of procedure of the ITU Telecommunication Standardization Sector

[7] WTSA-12, Resolution Resolution 2 – ITU Telecommunication Standardization Sector study group responsibility and mandates

[8] WTSA-12, Resolution 40 – Regulatory aspects of the work of the ITU Telecommunication Standardization Sector

[9] WTSA-12, Resolution 50 – Cybersecurity

[10] WTSA-12, Resolution 52 – Countering and combating spam

[11] WTSA-12, Resolution 58 – Encouraging the creation of national computer incident response teams, particularly for developing countries

[12] Recommendation ITU-T A.1(2012), Working methods for study groups of the ITU Telecommunication Standardization Sector

[13] Recommendation ITU-T A.8(2008), Alternative approval process for new and revised ITU-T Recommendations

[14] ITU-T SG17 TD31/R1, "Report of Working Party 1/17, Fundamental security", 17-26 April 2013.

[15] ITU-T SG17 TD32/R1, "Report of Working Party 2/17, Network and information security", 17-26 April 2013.

[16] ITU-T SG17 TD33/R5, "Report of Working Party 3/17, Identity management and cloud computing security", 17-26 April 2013.

[17] ITU-T SG17 TD68/R1, "Report of Working Party 4/17, Application Security", 17-26 April 2013.

[18] ITU-T SG17 TD69/R5, "Report for WP 5/17 plenary", 17-26 April 2013.

[19] ITU-T SG17 TD 1118, Report of Q3/17 interim Rapporteur group meeting (25 – 26 June 2014, Seoul, Korea (Republic of)), 2014.

[20] ITU-T SG17 TD 1120 Rev.1, Report of Q6/17 interim Rapporteur group meeting (24 – 26 June 2014, Seoul, Korea (Republic of)), 2014.

[21] ITU-T SG17 TD 1238, Report of joint Q2/17 and Q6/17 interim Rapporteur group meeting on SDN Security (25 June 2014, Seoul, Korea (Republic of)), 2014.

〈저 자 소 개〉

염 흥 열(HeungYoul 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
2011년 1월 ~ 12월 : 한국정보보호학회 회장(역)
2009년~현재 : ITU-T SG17 부의장
2009년~현재 : ITU-T SG17 WP2/WP3 의장
2012년 6월 ~현재 : 정보보호포럼 의장
관심분야 : 인터넷 보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜

오 흥 룡(Heung-Ryong Oh)
종신회원

2002년 2월 : 순천향대학교 전자공학과 졸업
2004년 2월 : 순천향대학교 정보보호학과 석사
2007년 6월 : 순천향대학교 정보보호학과 박사 수료
2004년 2월 ~ 현재 : 한국정보통신기술협회 표준화본부 책임연구원
2005년 3월 ~ 현재 : ITU-T SG17 국내 분과위원회 간사(역) 및 위원
2009년 2월~현재 : ITU-T SG17 Q.2 Associate Rapporteur
관심분야 : 안프로토콜, 정보보호 표준