정 보 보 호 학 회 지
제27권 제5호, 2017. 10

ITU-T SG17(보안) 구조 및 국제표준화 추진 방향 (연구회기 2017-2020)

염 흥 열*, 오 흥 룡**

요 약

국제전기통신연합(ITU)은 UN 산하 정보통신기술에 대한 전문 국제기구이다. 193개 회원국으로 구성된 국제전기통신연합은 산하에 전기통신표준화부문(ITU-T), 전기통신개발부문(ITU-D), 그리고 전파통신부문(ITU-R) 등 3개의 부문으로 구성되어 있다[1]. ITU-T는 역할과 임무에 따라 11개의 연구반 (SG, study group)으로 구성되며, 각 업무에 맞는 선두 그룹(Lead Study Group)을 지정하여 표준을 개발하고 있다. 정보보호 국제표준화는 ITU-T SG17(보안)에서 담당하고 있다[2]. ITU-T 국제 표준화는 4년 주기의 연구회기(Study Period)로 연구반 구조를 조정하며, 표준화 방향도 결정된다. 이러한 표준화 방향을 결정하기 위한 회의가 2016년 튀니지에서 열린 WTSA-16 (World Telecommunication Standardization Assembly) 총회이다. 본 논문에서는 WTSA-16 총회에서 결정된 ITU-T SG17 의장단과 정보보호 국제표준화 활동과 관련된 WTSA-16 결의(Resolution)를 분석하고, 2017년 두 차례 SG17 회의에서 추진된 SG17 구조와 추가 의장단 구성을 포함하는 표준화 동향을 제시한다.

Ⅰ. 서 론

ITU-T SG17 [1],[2],[3]은 보안에 대한 국제표준을 개발하는 국제표준화 그룹이다. 보안 표준은 정보보호 시스템의 호환성과 기술 경쟁력 향상을 위해 요구된다. SG17은 2017-2020 연구회기 동안 구조를 확정하고 2017년 3월 회의에서 한국제안으로 지능형 차량보안 연구과제(Question)를 신설하였고, 2017년 9월 다시 한국제안으로 블록체인 (분산원장기술)에 대한 연구과제를 신설키로 합의했다[6],[7].

본 논문 제2장에서는 ITU-T SG17 의 국제표준화 활동 방향을 결정하는 세계정보통신표준총회(WTSA-16) [4] 에서 임명된 의장단과 관련 결의 [5], 2017년 3월 확정된 SG17 구조를 중심으로 기술한다[2]. 또한 이번 연구회기(2017-2020) 동안 SG17 국제표준화 활동의 최신 동향에 대해 살펴보고, 제3장에서는 결론 및 향후 대응방안을 제시한다.

Ⅱ. ITU-T 정보보호 표준화 활동

ITU-T SG17 국제표준화 추진 방향은 연구회기 단위인 4년마다 열리는 세계정보통신표준총회 (WTSA, World Telecommunication Standardization Assembly)의 정책 방향에 근거하고 있다. 구체적으로는 연구반의 의장단을 선임하고 각 연구반과 관련된 결의를 합의한다.

2.1. ITU WTSA-16 임명 의장단과 연구과제

WTSA-16 총회는 [표 1]과 같은 의장단을 임명했고, SG17 산하 12개의 연구과제를 [표 2]와 같이 확정했다. WTSA-16에서 확정된 연구과제는 연구과제 1에서 12까지였고, 연구과제 13은 WTSA-16 이후 열린 2017년 3월 SG17 회의에서 신설되었고, 연구과제 14는 2017년 8월/9월 SG17 회의에서 신설이 합의되었다.

또한 2017년 3월 SG17 회의에서 연구과제가 작업반(Working Party)으로 [표 3]과 같이 구분되었다. 또한 각 작업반의 의장단이 [표 4]와 같이 결정되었다. 또한

본 논문은 과학기술정보통신부 및 정보통신기술진흥센터의 정보통신·방송 연구개발사업의 일환으로 수행하였음. [2015-0-00264, IoT 환경에서 프라이버시 보호 국제 표준화]
* 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr), ITU-T SG17 의장
** 한국정보통신기술협회 표준화본부 (hroh@tta.or.kr)

〔표 1〕 SG17 의장단 (연구회기 2017-2020) 〔4〕

이름	국가	직위
염흥열	대한민국 (순천향대)	의장
Vasiliy DOLMATOV	러시아	부의장
Gökhan EVREN	터키	부의장
Inette FUREY	미국	부의장
Muataz Elsadig ISHAG	수단	부의장
Patrick-Kennedy KETTIN ZANGA	중앙 아프리카 공화국	부의장
Wala TURKI LATROUS	튀니지	부의장
Zhaoji LIN	중국	부의장
Hugo Darío MIGUEL	아르헨티나	부의장
Yutaka MIYAKE	일본	부의장

〔표 2〕 SG17 연구과제 (연구회기 2017-2020)

연구과제	연구과제 제목	비고
Q1/17	통신/ICT 보안 조정	계속
Q2/17	보안구조 및 프레임워크	계속
Q3/17	통신부문 정보보호 관리	계속
Q4/17	사이버보안	계속
Q5/17	스팸의 기술적 대응	계속
Q6/17	통신서비스, 네트워크, 사물인터넷 보안	계속
Q7/17	안전한 응용 서비스	계속
Q8/17	클라우드 컴퓨팅 보안	계속
Q9/17	텔레바이오메트릭	계속
Q10/17	아이덴터티 관리 구조 및 메커니즘	계속
Q11/17	안전한 응용을 지원하기 위한 일반 기술	계속
Q12/17	통신 소프트웨어와 시험을 위한 공식 언어	계속
Q13/17	지능형 차량 시스템 보안	신규 (2017.3)
Q14/17	분산원장기술 보안	신규 (2017.9)

각 연구과제의 주요 라포처와 부 라포처의 명단은 [표 5]와 같다.

〔표 3〕 SG17 구조 (연구회기 2017-2020)

WP	WP 이름	연구과제
WP 1	통신/ICT 보안	• Q2/17, 보안구조 및 프레임워크
		• Q3/17, 통신부문 정보보호 관리
		• Q6/17, 통신서비스, 네트워크, 사물인터넷 보안
		• Q13/17, 지능형 차량 시스템 보안
WP2	사이버공간 보안	• Q4/17, 사이버보안
		• Q5/17, 스팸의 기술적 대응
WP3	응용 보안	• Q7/17, 안전한 응용 서비스
		• Q8/17, 클라우드 컴퓨팅 보안
		• Q12/17, 통신 소프트웨어와 시험을 위한 공식 언어
WP4	아이덴티티 관리 및 인증	• Q9/17, 텔레바이오메트릭
		• Q10/17, 아이덴터티 관리 구조 및 메커니즘
		• Q11/17, 안전한 응용을 지원하기 위한 일반 기술
SG17	-	• Q1/17, 통신/ICT 보안 조정
SG17	-	• Q14/17, 분산원장기술 보안

〔표 4〕 작업반 의장단 (연구회기 2017-2020)

WP	의장	부의장
WP 1	• Yutaka Miyake (KDDI, 일본)	• Vasiliy Dolmatov (러시아) • Gökhan Evren (터키)
WP2	• Koji Nakao (NICT, 일본)	• Inette Furey (미국)
WP3	• Arnaud Taddei (시만텍, 미국)	• Zhaoji Lin (ZTE, 중국)
WP4	• Kepeng Li (알리바바, 중국)	• 나재훈 (ETRI, 한국)

〔표 5〕 연구과제 라포처와 부라포처

연구과제	라포처	부라포처
Q1/17	• Wala Turki Latrous (튀니지)	• Paul Najarian (국무성, 미국)
		• Wataru Senga (KDDI, 일본)
		• Yiwen Wang (CAICT, 중국)
Q2/17	• 오흥룡 (TTA, 한국)	• Emna Chaabane (튀니지)
	• Zhiyuan Hu (중국)	• 이진명(KT, 한국)
Q3/17	• Miho Naganuma (일본)	• Andrés Fischer (아르헨티나)

Q4/17	• 김종현 (ETRI, 한국)	• Eduardo Casanovas (아르헨티나)
Q5/17	• Yanbin Zhang (중국)	• 김창오 (쿠팡, 한국)
Q6/17	• 백종현 (KISA, 한국)	• Maria Eugenia Pazo Robles (아르헨티나)
		• Takeshi Takahashi (일본)
		• Bo Yu (중국)
Q7/17	• 나재훈 (ETRI, 한국)	• Lijun Liu (중국)
Q8/17	• Liang Wei (중국)	• Mark McFadden (영국)
Q9/17	• John George Caras (미국)	• Kepeng Li (알리바바, 중국)
		• Mengxi Wang (중국)
Q10/17	• Abbie Barbir (미국)	• 박근덕 (KSEL, 한국)
		• Hiroshi Takechi (일본)
		• Junjie Xia (중국)
Q11/17	• Jean-Paul Lemaire (프랑스)	• Olfa Kaddachi (튀니지)
Q12/17	• Dieter Hogrefe (독일)	• Martin Duhalde (아르헨티나)
		• Gunter Mussbacher (캐나다)
Q13/17	• 이상우 (ETRI, 한국)	• 박승욱 (현대, 한국)
Q14/17	• 오경희 (한국)	• Xiaoyuan Bai (알리바바, 중국)
	• Youki Kadobayashi (일본)	• Min Zuo (차이나 모바일, 중국)

2.2. ITU WTSA-16 결과 및 관련 결의

ITU WTSA-16 [4] 은 2016년 10월 말에 튀니지 함마메트에서 열렸다. 이 총회에서는 ITU-T 연구반의 연구과제를 결정하고, [표 6]과 같이 연구반의 역무와 타이틀을 결정했다. 또한 SG17의 주요 표준화 추진 방향을 결정하는 주요 결의를 합의했다[5]. 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 국제 표준화를 추진하고 있다[4],[5]. [표 7]은 정보보호와 관련된 주요 WTSA-16 결의의 내용과 SG17 내 주요 활동 상황을 나타내고 있다.

〔표 6〕 SG17 개요 (2017-2020)

타이틀	보안 (security)
역무	정보통신기술 (ICT) 사용에 대한 신뢰와 보안을 구축하는 책임을 진다. 여기에는 사이버 보안, 보안 관리, 스팸 및 ID 관리 대응에 관한 연구를 포함한다. 또한 보안 구조와 프레임워크, 개인정보 보호, IoT, 스마트 그리드, 스마트 폰, SDN (Software-defined Networking), IPTV (Internet Protocol Television), 웹 서비스, 소셜 네트워크, 클라우드 컴퓨팅, 빅 데이터 분석, 모바일 금융 시스템 및 텔레 바이오 메트릭스을 위한 응용과 서비스의 보안을 포함한다. 연구반 17은 디렉토리 및 객체 식별자를 포함하는 개방형 시스템 통신 응용 프로그램 및 기술 언어, 적합성 테스트를 지원하는 통신 시스템 및 테스트 명세 언어의 소프트웨어 측면과 관련된 기타 사용법 및 방법에 대한 책임진다
선도 연구반	• 보안에 대한 선도 연구반 • ID 관리에 대한 선도 연구반 • 언어 및 서술(Description) 기술에 대한 선도 연구반

2.3. SG17 국제표준화 동향

본 절에서는 2017년에 수행된 각 연구과제별 중요 활동에 대한 정보를 제공하고자 한다. 2017년 동안 채택된 ITU-T 표준은 [표 8]과 같다[6],[7].

2.3.1. 통신/ICT 보안 조정(Q1/17)

본 그룹에서 보안 전략, 비전, 계획, 로드맵 등의 보안 표준에 대한 총괄 조정 업무를 수행하고 있으며, 이번 연구회기 동안에는 “보안 표준들의 성공사례”에 대한 기술보고서(Technical Report)와 ITU-T 주요 보안 권고를 설명하는 “보안 메뉴얼”을 개발하고 있다. 매 회의마다 용어 정의 등을 포함하는 컴펜디움(compendium), 보안 로드맵을 업데이트하고 있다.

2.3.2. 보안구조 및 프레임워크(Q2/17)

본 그룹에서는 보안구조, 모델, 전반적인 서비스 시나리오 등을 담당한다. 지난 연구회기 (2013-2016) 동안은 IPv6 구현을 위한 보안 표준(X.1037)과 IPv6 구현 지침 부속서(X.Sup23), 통신 사업자를 위한 보안지침(X.1033) 표준, X.805 보안 영역의 구현을 위한 기술적 보안 대책 (X.1039) 을 완료하였다. 현재는 전자상거래 환경에서 거래정보 등 데이터를 보호하기 위한 보안구조(X.salcm), SDN 기반 보안 서비스 체인의 보안 프레임워크 (X.sdnsec-3), 모바일 가상 네트워크 운영자 (별정통신사업자) 보안 지침(X.sup-sgmvno), VoLTE 보안 구조 및 지침(X.voLTEsec-1)을 개발 중에 있다. 2017년 9월 회의에서 X.sup-sgmvno가 최종 채택되었고, X.salcm은 AAP로 사전채택(consent) 되었다.

2.3.3. 통신부문 정보보호 관리(Q3/17)

본 그룹에서는 통신부문 보안관리 표준을 주로 다루고 있다. 지난 연구회기(2013-2016) 동안은 ISO/IEC 27002 개정에 따른 통신조직을 위한 정보통신 보안관리(X.1051) 개정 작업을 완료하였다. 또한, 개인정보보호 관리체계(PIMS) 국제표준화 작업을 ISO/IEC JTC1/SC27/WG5 그룹과 공통표준(Common Text) 작업(X.gpim)이 활발하게 진행되었다. 그리고 ISMS 관리체계를 중소기업에 적용하기 위한 지침(X.sgsm), PIMS 관리체계에 대한 구현 부속서(X.sup-gpim), X.1054(정보보호 거버넌스) 국제표준의 구현 사례 부속서(X.sup-gisb)가 개발 중에 있다. 2017년 3월 SG17 회의에서 개인정보보호 지침이 X.1058로 최종 채택되었다. 또한 2017년 9월 SG17 회의에서 중소기업을 위한 정보보호관리 가이드라인이 사전 채택(consent) 되었다.

2.3.4. 사이버보안(Q4/17)

본 그룹에서는 사이버공격 대응기술, 사이버보안 정보공유 방법, 사이버보안 전반적인 이슈를 다루고 있다. 지난 연구회기(2013-2016) 동안은 사이버보안지수(X.1208), 사이버보안 역추적기술(X.1210), 웹 기반 공격 대응기술(X.1211), 재난경보 알림 프로토콜(X.1303 bis), 사이버보안 정보공유 프레임워크(X.1500) 시리즈 다수의 표준화 작업을 완료하였다. 이번 연구회기에서는 세션 정보 메시지 교환 포맷(X.simef), 사이버공간에서의 보안위협 평가 매트리스(X.metric), 정보통신/ICT 네트워크 보안 평가기술(X.samtn), 스마트폰 봇넷 대응을 위한 보안 요구사항(X.sbb), 사용자 보호를 향상시키기 위한 설계 고려사항(X.cogent) 표준초안이 개발 중에 있다. 2017년 3월 SG17 회의에서는 신뢰 지표의 향상된 사용자 인식을 위한 설계 고려사항이 X.1212로 최종 채택되었고, 침해사고 교환 네트워크를 위한 접근 통제 모델이 X.1550으로 최종 채택되었다. 또한 2017년 9월 SG17 회의에서는 스마트폰 기반 봇넷 대응을 위한 보안 능력 요구사항이 X.1213으로 최종 채택되었다. 또한 네트워크 보안 평가기술(X.samtn)도 사전 채택(determination) 되었다.

2.3.5. 스팸의 기술적 대응(Q5/17)

본 그룹에서는 스팸의 기술적인 대응 표준을 개발하고 있는 그룹으로 e-mail 스팸, IP 멀티미디어 스팸, 보이싱 스팸, 모바일 메신저 스팸 등을 다루고 있다. 지난 연구회기(2013-2016) 동안은 통신 조직 내에 보이싱 스팸 대응을 위한 기술(X.1246), 모바일 메신저 스팸 대응을 위한 기술적 프레임워크(X.1247), 모바일 폰 개발자를 위한 스팸 대응 지침(X.Sup25)을 완료하였다. 현재는 인스던트 메신징 스팸 대응을 위한 기술 요구사항(X.cspim), 피싱 및 스미싱 대응 지침(X.sup-gcspi), 모바일 광고 스팸 대응을 위한 기술적 프레임워크(X.tfcma), VoLTE 환경에서의 스팸 대응 부속서(X.ticsc)가 개발 중에 있다. 2017년 9월 SG17 회의에서 인스던트 메신징 스팸 대응을 위한 기술 요구사항이 X.1248로 최종 채택되었다. 또한 피싱 및 스미싱 대응 지침 부속서도 최종 채택되었다.

2.3.6. 통신서비스, 네트워크, 사물인터넷의 보안(Q6/17)

본 그룹에서는 IPTV 보안, USN 보안, 모바일 보안, 멀티캐스트 보안, 홈네트워크 보안, RFID 보안, 사물인터넷 보안, 스마트그리드 보안 등의 표준을 다루고 있다. 지난 연구회기(2013-2016) 동안은 IPTV 보안을 위한 가상 머신 기반 보안 플랫폼 iCAS(X.1198), 유비쿼터스 네트워킹을 위한 보안 요구사항 및 프레임워크(X.1314), 스마트폰 보안 기술 부속서(X.Sup19), 안전한 앱 배포 프레임워크 부속서(X.Sup24), 스마트 그리

〔표 7〕 ITU-T 정보보호 분야 WTSA 결의(2016) (5)

결의 번호	제목	주요 내용 (SG 17관련)	SG17 관련활동
결의 50	(영문제목) Cybersecurity (한글제목) 사이버보안	▪ 국가 및 국제 수준에서 ICT 기술 사용에 있어서 신뢰 및 보안 구축에 대한 정부 및 기타 이해관계자 간의 공통된 이해증진을 포함하여, 업무의 역량 및 전문성에 따라, ITU T 내에서 높은 우선순위로 이 작업을 계속 추진한다. ▪ 모든 ITU-T 연구반은 이 총회의 결의2 (Rev. Hammamet, 2016)의 위임 내에서 설계의 견고성과 악의적 이해당사자가 악용할 가능성에 대하여 기존 권고와 신규 권고를 지속적으로 평가하고, 글로벌 전기통신/ICT 기반 구조에 의해 지원될 신규 서비스 및 애플리케이션 (예, 전기통신/ICT 망에 기초하는 클라우드 컴퓨팅과 사물 인터넷과 이를 넘어서)을 지속적으로 고려한다. ▪ ITU-T는 자신의 위임과 역량 내에서 사이버위협과 공격으로부터 정보 및 전기통신시스템을 방어하고 강화할 필요성에 대한 인식을 지속적으로 향상시키고, 정보 및 전기통신망 보안 분야에서 기술 정보의 교환을 증대시키기 위하여 적절한 국제 및 지역기구 사이의 협력을 지속적으로 촉진한다. ▪ ITU-T는 특히 ITU-D 연구과제3/2 (정보 및 통신망의 보호: 사이버보안 문화를 개발하기 위한 모범사례) 맥락에서 ITU-D와 밀접하게 협력해야 한다. ▪ ITU-T는 사이버보안 용어를 비롯하여 전기통신/ICT의 이용에 관한 신뢰와 보안의 구축과 관련된 용어 및 정의의 개발 및 개선을 계속해서 추진한다. ▪ 침해사고-대응 관련 정보를 공유하기 위한 전 세계적이고, 일관성 있으며, 상호운용 가능한 프로세스를 개선해야 한다. ▪ 연구반17은 다른 모든 ITU-T 연구반과 긴밀히 협력해 보안 취약점에 대응하기 위해 기존 및 진화하며 새로운 ITU T 권고를 평가하기 위한 행동계획을 수립하고, 전기통신/ICT의 보안에 관한 정기적 보고서를 전기통신표준화자문반(TSAG)에게 계속 제공한다. ▪ ITU T 연구반은 이 분야에서 활동하는 표준화기구 및 기타 기구들과 연락을 계속한다. ▪ 보안측면은 ITU T 표준 개발과 정보통신 전반에 걸쳐 고려되어야 한다.	▪ 연구과제 4(Q4/17) 사이버보안 정보 교환 프레임워크 (CYBEX) 시리즈 ▪ 연구과제 8(Q8/17) 신규 서비스 및 응용 고려
결의 52	(영문제목) Countering and combating spam (한글제목) 스팸의 대처와 방지	▪ 적절한 경우 ITU T의 권한 및 전문성 내에서 현재 및 미래의 위협에 대처하기 위해 특히 연구반17에서 스팸(예, 이메일)에 대한 대처와 관련해, 진행중인 작업을 계속 지원하고 스팸에 대한 작업을 가속화해야한다. ▪ 합동 워크숍, 교육세션 등을 통해 정보를 확산하고 모범 관행을 교환할 목적으로, 기술권고의 개발을 계속하기 위해 관련 다른 표준화기구(예: IETF)를 포함한 관련 기구와 ITU-D와의 협력을 긴급 사안으로 계속 추진한다. ▪ SG17에게 추가적으로 다음을 지시한다. ▪ 이 결의의 진도를 TSAG에 정기적으로 보고한다. ▪ 다른 여러 지역에서 스팸정책, 규제 및 경제적 문제와 그 영향과 연관된 기술교육 세션 및 워크숍 활동을 제공하는 스팸방지 및 대응에 관한 ITU-D 연구반 2 작업을 지원한다. ▪ 권고, 기술문서 및 기타 관련 출판물 개발에 관한 작업을 지속한다.	▪ 연구과제 5(Q5/17) 스팸의 기술적 대응
결의 58	(영문제목) Encouraging the creation of national computer incident response teams, particularly for developing countries (한글제목) 특히 개발도상국에 대한 국가적 컴퓨터 침해사고대응팀 설립의 장려	▪ TSB 국장에게 BDT 국장과 협력하여 다음을 수행할 것을 지시한다. 1. CIRT를 설립하기 위한 모범 사례를 조사한다. 2. CIRT가 필요한 곳을 조사한다. 3. 국가적인 CIRT의 설치를 위하여 국제적인 전문가 및 단체와 협력한다. 4. 기존 예산 자원 내에서 적절하게 지원을 제공한다. 5. 적절한 틀 내에서 역량 구축 및 정보교환과 같은 국가 CIRT 사이의 협력을 촉진한다.	▪ 연구과제 3(Q3/17) 보안사고 대응 지침

드 보안 기능 구조 부속서(X.sup.26)를 완료하였다. 이번 연구회기 동안에는 IoT 환경을 위한 심플 암호화 절차(X.iotsec-1), IoT 보안 프레임워크(X.iotsec-2), ITS 통신 장비를 위한 안전한 소프트웨어 업데이트 방법(X.itssec-1), ITS 통신 시스템을 위한 보안 지침(X.itssec-2), 스마트폰 도난 시, 개인정보 등을 안전하게 셧다운 할 수 있는 킬스위치(X.msec-9), 모바일 네트워크에서 감염된 단말의 부정적인 영향을 감소시키기 위한 지침(X.msec-11), SDN을 이용한 보안 서비스(X.sdnsec-1), ITS 보안 업데이트를 무선 방법으로 운영하기 위한 부속서(X.sotavsu)가 개발 중에 있다. 2017년 3월 SG17 회의에서는 사물인터넷에 대한 심플 암호화 절차가 X.1362로 채택되었고, 지능형 차량 시스템 통신 디바이스를 위한 안전한 소프트웨어 업데이트 방법이 X.1373으로 최종 채택되었다. 2017년 9월 SG17 회의에서는 모바일 단말 도난 대응 보안 기능 요구사항과 구조가 X.1127로 최종 채택되었다. 또한 2017년 3월 지능형자동차 보안 연구과제(Q13/17)가 신설됨에 따라 ITS 보안 관련 모든 워크아이템이 Q13/17로 넘겨졌다.

2.3.7. 안전한 응용 서비스(Q7/17)

본 그룹에서는 P2P 보안, 웹서비스 보안, 응용프로토콜 보안, 제3의 신뢰기관(Trusted Third Party) 기반 인증 기술 등을 다루고 있다. 지난 연구회기(2013-2016) 동안은 XML 기반 접근제어 기술 XACML 3.0(X.1144), 다중 아이덴터티 제공자 환경에서 컴바인 인증 프레임워크(X.1154), 전자상거래 서비스를 위한 연결 가능한 익명 인증 지침(X.1155), 원타임 패스워드 기반 부인방지 프레임워크(X.1156), 상위 수준에서 이상거래 탐지 및 대응을 위한 기술적 요구사항(X.1157), 모바일 디바이스를 이용한 다중 인증 메커니즘(X.1158), ITU-T X.813 기반 방문자 부인방지 구조(X.1159), 정보통신 기반 P2P 보안요구사항 및 메커니즘(X.1163), 웹 매쉬업 서비스를 위한 보안 프레임워크(X.sup.21), XACML 3.0 내에 개선사항 및 신규 특징(X.sup.22) 부속서를 완료하였다. 이번 연구회기(2017-2020) 에서는 클라이언트-서버 모델에서 하이브리드 인증 및 키관리 메커니즘 지침(X.hakm), 정보통신 서비스를 원활하게 지원하기 위한 보안 요구사항 및 프레임워크(X.websec-6), 온라인 분석 서비스를 위한 레퍼런스 모니터(X.websec-7), 통신 운영자를 위한 부가서비스 보호 지침(X.websec-8), 그리고 통신서비스 제공자를 위한 비식별 처리 서비스 프레임워크 (X.fdip)를 개발 중에 있다. 2017년 3월 SG17 회의에서는 정보통신 서비스를 원활하게 지원하기 위한 보안 요구사항 및 프레임워크가 X.1145로 최종 채택되었다.

2.3.8. 클라우드 컴퓨팅 보안(Q8/17)

본 그룹에서는 프레임워크, 메커니즘 등 클라우드 컴퓨팅 보안 전체를 다루고 있다. 지난 연구회기(2013-2016) 동안은 클라우드 컴퓨팅을 위한 보안 프레임워크(X.1601), 소프트웨어 서비스(SaaS) 응용 환경을 위한 보안 요구사항(X.1602), 클라우드 서비스를 위한 ISO/IEC 27002 기반 정보보호 통제 구현 지침(X.1631), 클라우드 컴퓨팅 운영을 위한 보안 지침(X.1642)을 완료하였다. 이번 연구회기(2017–2020)에서는 클라우드 서비스 가입자 데이터 보안을 위한 지침(X.CSCDataSec), 클라우드 컴퓨팅 모니터링 서비스를 위한 데이터 보안 요구사항(X.dsms), 클라우드 컴퓨팅에서 퍼브릭 인프라 서비스(X.SRIaaS)를 위한 보안 요구사항(X.SRIaaS), 빅데이터 서비스 보안 가이드라인(X.GSBDaaS)을 개발 중에 있다. 2017년 9월 SG17 회의에서는 클라우드 컴퓨팅 모니터링 서비스를 위한 데이터 보안 요구사항(X.dsms)이 사전채택(determination) 되었고, 빅데이터 사업자를 위한 데이터 생명주기 관리에 대한 보안 가이드라인(X.sgtBD)이 신설되었다.

2.3.9. 텔레바이오메트릭(Q9/17)

본 그룹에서는 네트워크 기반 바이오 정보를 이용한 인증 기술에 대한 표준을 다루고 있다. 지난 연구회기(2013-2016) 동안은 이헬스 및 텔레메딕슨에서 바이오 정보를 보호하기 위한 통합 프레임워크(X.1092), 바이오 하드웨어 보안 모듈을 이용한 텔레바이오 인증 프레임워크(X.bhsm, X.1085), 모바일 디바이스를 이용한 텔레바이오 응용에서의 기술적 관리적 대응 지침(X.tam, X.1087) 표준을 완료하였다. 이번 연구회기에는 텔레바이오인식에서 데이터 보호를 위한 접근 제어(X.pbact), 생체신호를 이용한 차세대 인증기술(X.tab), 텔레바이오인식에 연관되는 학문 정의(X.th Series) 표준초안들이 개발 중에 있다. 2017년 3월 텔레바이오인

〔표 8〕 2017년에 채택된 주요 표준 〔6〕,〔7〕

약어	제목	에디터	채택 시기
X.1158	개인정보보호관리 치침	염흥열 외 2인	2017.3.
X.1126	모바일 네트워크에서 감염된 단말의 부정적 효과를 감소하기 위한 가이드라인	Liu Lijun 외 1인	2017.3.
X.1362	사물인터넷에 대한 단순 암호 과정	Shugo Mikami	2017.3.
X.1373	지능형 차량 시스템 통신 디바이스를 위한 안전한 소프트웨어 업데이트 능력	Masashi Eto 외	2017.3.
X.1212	신뢰 지표의 향상된 사용자 인식을 위한 설계 고려사항	Youki Kadobayashi 외 1인	2017.3
X.1550	침해사고 교환 네트워크를 위한 접근 통제 모델	Alexey Koshka	2017.3
X.1080.0	통신 바이오메트릭 데이터 보호를 위한 접근 제어	Eric Andersen 외 1인,	2017.3
X.1145	공개 통신 서비스를 위한 보안 프레임워크 및 요구사항	나재훈 외 2인	2017.5
X.1213	스마트폰 기반 봇넷 대응을 위한 보안 능력 요구사항	Junjie Xia 외 3인	2017.9.
X.1248	인스턴트 메시징 스팸 대응을 위한 기술 요구사항	Zhaoji Lin 외 3인	2017.9
X.1127	모바일 단말 도난 대응 보안 기능 요구사항과 구조	염흥열 외 1인	2017.9
X.sup-sgmvon	모바일 가상 네트워크 운영자를 위한 보안 가이드라인	Dongxin Liu 외 2인	2017.9
X.sup-gcspi	SMS 피싱 및 스미싱 공격 대응 가이드라인	염흥열 외 3인	2017.9
X.sup-oid-iot	사물인터넷을 위한 객체 식별자 가아드라인	Zhaoji Lin 외 2인	2017.9

식에서 데이터 보호를 위한 접근 제어가 X.1080.0으로 최종 채택되었다.

2.3.10. 아이덴터티 관리 구조 및 메커니즘(Q10/17)

본 그룹에서는 아이덴터티(Identity) 관리 기술과 기반 인증 서비스들에 대한 표준을 다루고 있다. 지난 연구회기 (2013-2016) 동안은 아이덴터티 관리 정보의 검색을 위한 프레임워크(X.1255), 어플리케이션 서비스에서 네트워크 인증 결과를 공유하기 위한 프레임워크(X.1256), 아이덴터티 및 통제 관리 분류체계(X.1257), 수집된 속성 정보 기반 향상된 실체 인증(X.1258) 표준을 완료하였다. 현재는 실체 인증 보증 프레임워크(X.1254rev) 개정 작업과 신뢰 개량(trust elevation) 프로토콜(X.te), 안티스푸핑(anti-spoofing) 탐지 메커니즘을 이용한 텔레바이오인식 환경에서의 인증 프레임워크(X.eaasd) 표준 초안들을 개발 중에 있다.

2.3.11. 안전한 응용을 지원하기 위한 일반 기술(Q11/17)

본 그룹에서는 안전한 응용서비스를 지원하기 위한 디렉토리, PKI, PMI, ASN.1, OID 식별자 할당 등 업무를 수행하고 있다. 지난 연구회기 동안은 OSI 디렉토리 표준들에 대한 오류 정정 작업과 이기종 식별자 및 위치정보에 대한 OID 기반 해설 프레임워크(X.675), ANS.1 인코딩 규칙 표준들에 대한 유지보수, 우체국간에 인증 및 인증된 메일 전송 프로토콜(X.1341), PKI 표준화를 위한 현재와 새로운 도전 기술보고서(XSTR-PKIS) 작업을 완료하였다. 이번 회기에도 PKI 유지보수 및 개선작업(X.pki-em), PKI 프로파일 정의(X.pki-prof), IoT 환경을 위한 객체식별자 활용 방법(X.oiddev), IoT 환경을 위한 객체식별자 활용 지침 부속서(X.sup-oid-iot), JSON 스크립트 언어의 ASN.1 인코딩 규칙(X.jsoner), 암호 메시지 규격에 대한 ASN.1 응용 규칙(X.cms) 등 표준 개발과 OSI 디렉토리(X.500 series) 제8판에 대한 개정 작업이 진행 중에 있다. 2017년 9월 SG17 회의에서 사물인터넷을 위한 객체식별자 가아드라인 부속서(X.sup-oid-iot) 가 최종 채택되었다.

2.3.12. 통신 소프트웨어와 시험을 위한 공식 언어 (Q12/17)

본 그룹에서는 다양한 형식 언어 및 시험방법론에 대한 표준을 다루고 있다. 이번 연구회기 동안에도 SDL-2010 기술 언어(Z.100 series), TTCN-3 시험 언어(Z.160 series), SDL 구현자 가이드(Z.Imp100) 유지보수 작업을 완료하였다. 현재는 ITU-T Z 시리즈(형식 언어 및 시험방법론) 표준들에 대한 유지보수가 계속해

서 진행되고 있다.

2.3.13. 지능형 차량 시스템 보안 (Q13/17)

본 그룹은 2017년 3월 SG17 회의에서 신설되기로 합의되었고, 이후 2017년 5월 정보통신표준자문반 회의에서 신설이 동의되었으며, 2017년 9월에 신설이 최종 승인되었다. 이 그룹은 원래 연구과제 6 (Q6/17)에서 수행되던 V2X 통신 시스템에 대한 보안 가이드라인(X.itssec-2)을 넘겨 받아서 표준화를 추진하고 있다. 또한 2017년 9월 SG17 회의에서 차량 접근 외부 디바이스에 대한 보안 요구사항(X.itssec-3), 차량 내부 시스템에서 침입 탐지를 위한 방법론(X.itssec-4), 그리고 차량에지 컴퓨팅 보안 가이드라인 (X.itssec-5)에 대한 신규 표준화 아이템이 신설되었다.

2.3.14. 분산원장기술 보안 (Q14/17)

본 그룹은 2017년 9월 SG17 회의에서 신설키로 합의된 연구과제이다. 이 그룹은 이번 SG17 회의에서, 보안 구조(X.sradlt), 디지털 지불 시스템 서비스의 보안 위협과 요구사항(X.strdlt), 보안 기능과 위협(X.sct-dlt), 보안 서비스(X.ss-dlt), 프라이버시와 보안 고려사항(X.dltsec), 보안 보증(X.sadlt), 온라인 투표에 관한 보안위협(X.stov)가 신규 표준화 아이템으로 채택되어 본격적으로 분산원장기술 보안에 대한 국제표준을 추진할 예정이다.

Ⅲ. 결 론

본 논문에서는 이번 연구회기(2017-2020) 동안 SG17 연구반 국제표준화 활동 근거가 되는 WTSA-16 회의 결과와 관련 결의의 내용을 분석했다. 또한, 각 그룹 내에서 개발된 신규 권고와 현재 개발 중에 있는 표준초안들에 대해 살펴보았다.

한국은 SG17 회의마다 많은 전문가로 구성된 대표단을 파견해 오고 있으며, 그 동안 SG17 의장, WP 의장, 여러 연구과제의 라포처 등의 의장단 활동과 국제표준 개발을 책임지는 에디터 역할을 통해 SG17 국제표준화 활동에 크게 공헌해 오고 있으며, 미국, 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 협력해서 ITU-T 정보보호 분야를 선도해 나갈 계획이다.

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] 오흥룡, 염흥열, “ITU-T SG17(보안) 국제표준화 동향”, 정보보호학회지, 제26권 제4호, 2016.08.

[4] ITU World Telecommunication Standardization Assembly 2016 : WTSA-16, http://www.itu.int/en/ITU-T/wtsa16 /Pages/default.aspx

[5] ITU PP-14, Final WTSA-16 Resolutions, http://www.itu.int/pub/T-RES

[6] ITU-T SG17-R1 Rev.1, Report of the first meeting of Study Group 17 (Geneva, 22-30 March 2017) - Plenary sessions, Aug. 2017

[7] ITU-T SG17 TD384 Rev.1, Draft executive Summary of SG17 29 August - 6 September 2017 meeting, September 11, 2017

〈저 자 소 개〉

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
2009년~2016년 : ITU-T SG17 부의장, WP3 의장
2017년~현재 : ITU-T SG17 의장
2011년 1월~12월 : 한국정보보호학회 회장(역)
2012년 1월~현재 : 한국정보보호학회 명예회장
2016년 5월~현재 : 개인정보보호표준포럼 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 연구반 간사(역) 및 위원
2009년~2016년 : ITU-T SG17 Q2 Associate Rapporteur
2017년~현재 : ITU-T SG17 Q2 Co-Rapporteur
관심분야 : 보안프로토콜, 정보보호표준