

ITU-T SG17 국제표준화 동향 및 향후 전망

오 흥 룡*, 김 영 화*, 염 흥 열**

요 약

정보보호 분야의 국제표준화는 기술들의 특성 및 참여하는 사용자들의 관점에 따라 다양한 국제표준화기구에서 국제표준개발 및 관련 연구가 진행되고 있다. 즉, ITU-T SG17(보안)에서는 전기통신(Telecommunication) 관점에서 통신망에 적용 가능한 응용기술들을 중심으로 국제표준화가 추진되고 있으며, ISO/IEC JTC1/SC27(정보보호)에서는 정보보호 원천기술들에 대한 국제표준화를 다루며, IETF Security Area에서는 인터넷 서비스의 품질 보장 및 향상된 인터넷 환경 구축을 위한 산업체 중심의 사실표준을 추진하고 있다. 그리고 유럽 및 아시아 지역에서 국가 간에 정보통신 표준화와 국제표준화 기구들에 대한 공동 대응을 위한 ETSI, ASTAP, CJK Security WG 등에서도 지역 내 정보보호 표준화 활동들이 이루어지고 있다. 또한, 이러한 국제표준화기구는 참여하는 이해 당사자가 국가(National Body)인지 혹은 산업체 등의 이해당사자들 간에 참여인지에 따라 특성 또한 달라지며, 표준을 개발하는 절차가 공식적인 방법에 따른 것인지 이해 당사자들 간에 합의에 의한 것인지에 따라 구분될 수도 있다.

본 논문에서는 2011년 11월, 두바이에서 개최된 ITU-T WTSA-12(세계정보통신표준총회) 국제회의의 결과를 바탕으로 향후 4년간의 ITU-T SG17 국제표준화 활동 방향에 대한 정보를 제공하고자 한다.

I. 서 론

정보보호 분야에 대한 국제표준화는 앞서 서술된 것처럼 다양한 표준화기구마다 특징에 맞게 업무영역(ToR: Terms of Reference)을 구분해서 국제표준을 개발하고 있었으나, 점차 ICT 기술이 융·복합되면서 정확한 구분이 어려워지고 있다. 따라서 이런 중복 작업을 방지하기 위해 표준화 협의체들마다 협력(Liaison) 문서를 발행하여 조정하거나 ITU-T와 ISO/IEC JTC1과 같이 두 국제표준화기구 간에 공통표준(Common Text)을 개발하기도 한다.

본 논문에서 다루고자 하는 ITU 국제표준화기구는 1865년 5월에 UN 산하에 신설된 국제전기통신연합(ITU: International Telecommunication Union) 기구로 전파규칙, 주파수 할당 등의 이슈를 다루고 있는 전파통신(Radiocommunication), 전기통신기술, 운용 및 요금 등의 이슈를 다루고 있는 전기통신(Telecommunica-

tion), 개발도상국의 통신망 현대화를 위한 정책, 기술적 지원 등을 다루고 있는 전기통신개발(Development) 부문으로 크게 3가지 부문으로 구분된다. 현재, 정보보호 국제표준화는 ITU-T 산하 10개 연구반(SG : Study Group) 중에 SG17에서 주로 다루고 있다[1],[2],[3],[4].

본 논문에서는 ITU-T WTSA-12 총회 후, 향후 4년을 위한 SG17 국제표준화 현황을 소개하여, 국내에서 ITU-T SG17 국제표준화기구에 활동하고자 하는 전문가들에게 유용한 정보를 제공하고자 한다.

II. ITU-T WTSA-12 국제회의의 결과

ITU-T 분야는 4년을 연구회기(Study Period)로 WTSA-12와 같은 전체 총회를 개최하여, 산하 SG별 활동 실적 및 회원국들의 요청을 근거로 차기 연구회기에 대한 구조조정 및 의장단을 선출하고 있다. 이번 WTSA-12 국제회의(2012.11.20~29, 아랍에미리트 두

본 연구는 2013년도 방송통신표준기술력향상사업 “국제 공식 표준화기구(ITU등) 협력 및 대응 연구” 과제(2013-PK20-33)의 일환으로 수행되었습니다.

* 한국정보통신기술협회 표준화본부({hroh, ykim}@tta.or.kr)

** 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr)

바이)는 한국에서도 약 30명의 대표단을 파견하여 전체 분야에서 의장단 총 10석을 확보하는 쾌거를 이루었으며, 정보보호 분야에서 순천향대 엄홍열 교수가 SG17 부의장으로 임명되었다 [참고, SG17 의장 : 러시아 Arkadiy Kremer]. 또한, WTSA-12 총회의 중요한 임무 중에 하나는 향후 4년 동안 각 SG 별로 중점적으로 다루어야 할 결의(Resolution)를 할당하는 것에 있다[5]. 현재 정보보호 분야에 할당된 결의는 여러 가지가 관련되어 있지만 다음 4가지가 중점적으로 대응할 결의이다.

- Res.50 : Cybersecurity (사이버보안)
- Res.52 : Countering and combating spam (기술적 수단에 의한 스팸대응기술)
- Res.58 : Encouraging the creation of national computer incident response teams, particularly for developing countries (개발도상국을 위한 국가 컴퓨터 침해대응센터 신설 장려)
- Res.78 : ICT applications and standards for improved access to e-health services (e-헬스 서비스를 장려하기 위한 ICT 응용기술 및 표준 개발)

[표 1] ITU-T SG17 구조 및 의장단 현황(2013-2016)

구분	제목	의장단
WP1	Fundamental security	Koji NAKAO (일본)
Q.1	Telecommunication/ICT security coordination	Mohamed M. K. Elhaj (수단) Hua Jiang (중국) Isaac Kobina Kwarko (가나)
	Security architecture and framework	Patrick Mwesigwa (우간다) Dmitry Kostrov (러시아) 오홍룡 선임 (한국)
	Telecommunication information security management	Miho Naganuma (일본) 오경희 이사 (한국)
WP2	Network and information security	Sacid SARIKAYA(터키)
Q.4	Cybersecurity	Youki Kadobayashi (일본) 김중현 선임 (한국) Ibrahim Hamza Al Mallouhi (아랍에미리트)
	Countering spam by technical means	Hongwei Luo (중국)
WP3	Identity management and cloud computing security	엄홍열 교수(한국)
Q.8	Cloud computing security	Liang Wei (중국) Mark Jeffrey (스위스) Victor Kutukov (러시아)
	Identity management architecture and mechanisms	Abbie Barbir (캐나다) Richard C. Brackney (미국) Jing Wu (중국) Hiroshi Takechi (일본)
WP4	Application security	Antonio GUIMARAES (브라질)
Q.6	Security aspects of ubiquitous telecommunication services	백중현 수석 (한국) Yutaka Miyake (일본)
	Secure application services	나재훈 연구위원 (한국) Huirong Tian (중국)
	Telebiometrics	John George Caras (미국) 신용녀 교수 (한국)
WP5	Formal languages	George LIN(중국)
Q.11	Generic technologies to support secure applications	Erik Andersen (덴마크) Jean-Paul Lemaire (프랑스)
	Formal languages for telecommunication software and testing	Dieter Hogrefe (독일) Gunter Mussbacher (캐나다) Rick Reed (영국)

또한, WTSA-12에서 각 SG 별로 ITU-T 내에 유관 이슈가 발생할 때, 우선적인 대응을 위해 선도(Lead) 그룹을 할당하는데, SG17은 보안(Security), ID 관리(Identity Management), 언어 및 서술 기술(languages and description techniques)에 대한 선도그룹의 역할을 수행하고 있다. 또한 연구과제는 특성에 따라 다시 그룹화되어 작업반(WP : Working Party)으로 구성된다.

Ⅲ. ITU-T SG17 국제표준화 현황

새로운 연구회기(2013~2016)를 맞아 첫 번째 ITU-T SG17 국제회의(2013.4.17~26, 스위스 제네바)는 SG 내에 있는 연구과제(Question)들을 작업반(WP) 별로 재그룹핑 하였으며, 실제 표준초안을 개발할 수 있는 각 연구과제들에 대한 의장 라포치를 임명하였다. 한국은 SG17 내에 다른 국가들에 비해 가장 많은 의장단을 수임하였으며, 이는 향후 4년간 국내기술을 국제표준으로 개발함에 있어 좋은 입지를 확보한 것이라 볼 수 있다. 현재 SG17 내에 구조는 다음의 표 1과 같으며, 지난 연구회기는 3개 WP와 15개의 연구과제로 활동을 하였으나[2], [3], [4], 이번 연구회기에서는 5개 WP로 확대되었고, 과거 3개의 시험언어(Testing Language) 관련 연구과제들을 하나로 묶어서 총 12개의 연구과제로 운영하기로 하였다[6], [7], [8], [9], [10].

3.1. 정보통신/ICT 보안 조정(Q.1)

연구과제 1에서는 ITU-T 내에 전체적인 보안 요약물, 전략, 비전, 계획, 로드맵 등을 연구하고 있으며, 정보보호 표준화 정보공유를 위한 워크숍 및 타 표준화기구들과의 협력 체계 구축, 보안 표준들 간에 이해격차 분석 작업들을 담당하고 있다. 또한, Q.1은 연구반 내 또는 연구반 간의 정보보호 표준화 활동 영역을 조정하는 역할을 수행하고 있다. 2013년 4월 회의에서의 주요 이슈는 Q.1 내에 암호프로토콜 안전성에 대한 검증 프로세스 개발을 위한 서신그룹(Correspondence Group)을 신설하였다. 이는 ITU-T SG17 국제표준에 ISO/IEC JTC1/SC27 이나 암호 협의체에서 개발된 알고리즘들이 많이 활용되고 있으나 이를 검증하는 절차가 없어 서신그룹 활동을 통해 다른 표준화 협의체들에서 유사 활동 정보에 대한 조사와 향후 국제표준 개발 가능성에

대해 조사가 이루어질 계획이다.

3.2. 보안구조 및 프레임워크(Q.2)

연구과제 2에서는 보안시스템의 구조, 모델, 개념, 전방적인 서비스 시나리오 등을 연구하고 있으며, 가장 대표적인 것은 X.800(OSI 모델) 시리즈 표준들이 가장 대표적이다. 또한, 개발도상국들을 위한 네트워크 인프라를 구축함에 있어 참조할 수 있는 가이드라인 표준들을 개발하고 있다. 2013년 4월 회의에서 주요이슈는 일본 주도로 개발되고 있는 “IPv6 구축에서의 기술적 가이드라인” 표준초안 개발이 완료되어 대체승인절차(AAP)로 임시승인되어, 최종 채택을 위해 논문작성시점에 ITU 회원국들에게 의견수렴이 진행되고 있다.

3.3. 보안관리(Q.3)

연구과제 3에서는 정보통신 시스템을 위한 보안관리 표준들을 개발하고 있으며, 특히, ISO/IEC JTC1/SC27/WG1 그룹과 협력해서 ISMS 표준들을 중점적으로 개발하고 있다. 2013년 4월 회의에서 주요이슈는 중소기업 정보통신 기관을 위한 정보보호 관리 가이드라인, 정보통신 조직을 위한 개인정보 관리 가이드라인 표준초안들을 업데이트하였으며, 특히 ISO/IEC 27002 국제표준이 개정됨에 따라 ITU-T X.1051 | ISO/IEC 27011 국제표준을 개정하기로 합의하였다.

3.4. 사이버보안(Q.4)

연구과제 4에서는 인터넷 및 네트워크 시스템 등에 발생할 수 있는 침해사고대응방법, 사이버공격 대응기술, 보안솔루션, 사이버보안 취약점들에 대한 해결방법 및 정보공유 방법 등에 대해 연구하고 있다. 2013년 4월 회의에서 주요이슈는 사이버보안 정보교환 기술(Cybox)에 대한 X.1544(공격패턴분류방법), X.1526(취약점 선별 및 평가 언어) 국제표준에 대한 추가 제정과 한국 주도로 개발된 통신 주체들 간에 정보공유에 앞서 사전 협의하는 기술이 부속서(Supplement 20 to X.1205)로 승인되었다. 현재 Cybox 관련 개발되고 있는 표준초안은 이벤트 사건에 대한 표현 방법, 취약점을 스코어할 수 있는 시스템, Cybox 기반 사이버보안 운영

모델, Cybex 정보교환 프로토콜(BEEP), Cybex 지원이 가능한 전송 프로토콜 등이 개발되고 있다. 또한, 일반적인 사이버보안 분야로 IP 기반 통신 환경에서 이상 트래픽을 탐지 및 통제하는 기술에 대한 부속서(Supplement 18 to X.1205)가 승인되었으며, 한국 주도로 개발된 사이버보안 지수 가이드라인이 전통승인절차(TAP)로 사전 승인되어, 논문작성시점에 ITU 회원국을 대상으로 의견수렴 단계로 진입했다. 현재 사이버보안 분야에서는 이 외에도 웹 기반 사이버공격 대응기술과 역추적 메커니즘에 대한 표준초안 개발도 진행되고 있다.

3.5. 기술적인 방법에 의한 스팸대응(Q.5)

연구과제 5에서는 기술적인 방법에 의한 스팸대응을 위한 표준화를 연구하고 있으며, 크게 e-mail에 의한 스팸과 IP 멀티미디어 서비스에 의한 스팸, 단문서비스(SMS) 스팸, 음성 스팸을 분리하여 표준들을 개발하고 있다. 2013년 4월 회의에서의 주요이슈는 음성 스팸에서 스팸성 신호를 기록하는 방법과 이를 분석하기 위해 사업자와 분석 기관에 협력 방법에 대한 논의가 진행되었으며, 모바일 스팸 대응을 위해 모바일 통신에 참여하는 엔티티 간에 정보공유 및 상호연동 메커니즘에 대해 논의가 진행되었다.

3.6. 유비쿼터스 통신서비스 보안(Q.6)

연구과제 6에서는 통신서비스 관점에서 IPTV 보안, USN 보안, 모바일 보안, 멀티캐스트 보안, 홈네트워크 보안, RFID 보안 등을 중점적으로 다루고 있으며, 새로운 연구회기 맞아 사물통신(Internet of Things), M2M, ITS, 스마트그리드, NFC 응용서비스 등을 추가적으로 다루기로 하였다. 2013년 4월 회의에서의 주요이슈는 한국 주도로 개발된 IPTV 서비스 및 콘텐츠 보호를 위한 가상머신 기반 보안 플랫폼 표준초안이 최종 완성되어 ITU 회원국들에게 의견수렴으로 승인되었다. 본 국제표준은 국내 “TTAK.KO-08.0023: IPTV 용 교환 가능한 CAS (iCAS)” 기술을 기반으로 만들어졌으며, 가상의 보안모듈을 기반으로 소프트웨어 방식의 콘텐츠 전달 및 OS 업그레이드이가 가능한 보안 플랫폼을 정의하고 있어, 사용자 단말의 보안성 강화와 편리성 제공

이 가능할 것으로 예측된다. 그리고 중국을 중심으로 개발된 스마트폰 보안 가이드라인은 당초 국제표준으로 채택하려 했으나 현재 모바일 보안과의 차이점이나 스마트폰 보안 자체에 대한 정의가 어려워 부속서(Supplement 19 to X.1120 series)로 승인되었다. 또한, 모바일 보안에서 악성코드에 감염된 단말을 관리하는 지침과 스마트폰 앱 등의 안전성 배포 방법, 스마트그리드 보안구조에 대한 표준초안 개발이 진행되었다.

3.7. 안전한 응용서비스 보안(Q.7)

연구과제 7에서는 P2P 보안, 웹서비스 보안, 응용프로토콜 보안, 제3의 신뢰기관(Trusted Third Party) 기반 인증 기술들을 중점적으로 다루고 있다. 2013년 4월 회의에서의 주요이슈는 다중 식별 정보를 조합해서 인증하는 프레임워크 표준이 최종 제정되었으며, 한국 주도로 개발된 원타임 패스워드 기반 부인방지 프레임워크 표준초안 작업이 완료되어 ITU 회원국들에게 의견수렴 단계로 승인되었다. 그리고 한국은 온라인 환경에서 이동들을 보호하기 위한 차세대 인증 메커니즘으로 사용자 속성 정보 기반 인증기술의 필요성을 제안하여 차기 회의에서 보다 구체적인 표준화 아이템을 발굴하기로 합의하였다. 또한, 연구과제 7에서는 연결성 기반 익명 인증기술, 상위 보충 레벨을 유지하기 위한 인증기술, 모바일 단말에서의 다중 인증기술, 웹서비스 보안 및 XML 보안(XACML 3.0 등) 기술들에 대한 표준초안 개발이 진행되고 있다.

3.8. 클라우드 컴퓨팅 보안(Q.8)

연구과제 8에서는 이기종 네트워크 환경을 고려한 클라우드 컴퓨팅 보안을 다루고 있다. 특히, 클라우드 환경에서의 보안 위협과 요구사항을 충족시키기 위해 보안구조, 보안관리, 비즈니스 연속성 및 재해복구, 스토리지, 프라이버시, ID관리, 네트워크 모니터링 및 침해대응, 상호운용성, 가상화기술 등을 집중적으로 다루기로 하였다. 2013년 4월 회의에서의 주요이슈는 ITU 내에 SG13(미래 네트워크) 연구반과 SG17 연구반 간에 클라우드 컴퓨팅 보안에 대한 역할 조율이 중요하게 다루어졌으며, 다음과 같이 업무가 분장되었다.

- SG13: 활용사례, 기능블럭(2)

- SG17: 보안 영역 식별, 상세 보안 기능, 보안 구조 기본 개념, 기존 보안 메커니즘, 신규 메커니즘, 보안 관리, 모범사례, 운영보안(8)
- SG13 주도 공통 프로젝트: 위협분석 및 활용사례 기반 일반적인 보안 요구사항, 클라우드 컴퓨팅 기능 구조 및 기능 블록에 대한 보안기능 할당(2)
- SG17 주도 공통 프로젝트: 보안위협 식별, 일반적인 보안 요구사항을 고려한 위협분석/활용사례 기반 클라우드 컴퓨팅 보안 솔루션 및 메커니즘에 대한 보안 요구사항, 신뢰모델 정의(3)

현재 연구과제 8에서는 클라우드 컴퓨팅을 위한 보안 요구사항 및 구조, 가상 네트워크를 위한 안전한 서비스 플랫폼 프레임워크, 클라우드 컴퓨팅을 위한 운영 보안 가이드라인, SaaS 응용 환경을 위한 보안 기능 요구사항 표준초안들이 중국을 중심으로 개발되고 있다.

3.9. 텔레-바이오인식(Q.9)

연구과제 9에서는 네트워크 환경에서 바이오정보를 응용하기 위한 표준초안들을 개발하고 있으며, 특히 전자상거래, e-헬스, CCTV 환경에서 프라이버시 보호, 스마트폰에서 바이오정보 응용에 대한 표준을 다루고 있다. 2013년 4월 회의에서의 주요이슈는 한국 주도로 개발된 원격의료와 텔레-바이오인식에서 바이오정보 보호를 위한 단일 프레임워크 표준초안이 완료되어 ITU 회원국을 대상으로 의견수렴 단계로 승인되었다. 또한, 한국은 ISO/IEC JTC1/SC27 그룹과 공통 표준으로 개발하고 있는 바이오인식 하드웨어 보안 모듈을 이용한 텔레바이오인식 인증 프레임워크와 모바일 디바이스 기반 텔레바이오인식 응용하기 위한 기술적, 관리적 대응책 가이드라인에 대한 표준초안 개발이 진행되었다.

3.10. 아이덴티티 관리 및 메커니즘(Q.10)

연구과제 10에서는 아이덴티티(Identity)에 대한 관리 기술과 이들을 기반한 인증 및 서비스들에 대한 표준들을 개발하고 있다. 즉, 다양한 네트워크를 구성하고 있는 각 엔티티(서비스 제공자, 사용자, 소셜네트워크 사업자, 기관, 디바이스, 응용프로그램, 서비스 등)를 식별 및 관리하기 위한 크리덴셜, 식별자, 속성정보, 패턴

양식 등의 전반적인 생명주기(Life-cycle)를 관리하는 표준들을 개발하고 있다. 특히, 모바일 클라우드 환경에서는 각 사용자 및 디바이스들에 대한 식별 및 인증, 속성 정보 관리는 중요성이 점점 증가하고 있다. 2013년 4월 회의에서는 이기종 IdM 서비스 간에 상호운용성 지원 메커니즘, 네트워크 계층과 서비스 계층 간에 단일 인증 메커니즘, 속성 정보들에 대한 결합 방법 지침, 클라우드 환경에서 ID 관리를 위한 요구사항에 대한 표준 초안 개발이 진행되었다.

3.11. 응용서비스 지원을 위한 일반적인 기술(Q.11)

연구과제 11에서는 안전한 응용서비스들을 지원하기 위한 일반적인 기술들에 대한 표준을 다루고 있다. 즉, 디렉토리 서비스(X.500 series), 공개키 기반구조(PKI), 권한 관리 기반구조(PMI), ITU 공식 언어 ASN.1(추상 구문기법 1), 객체식별자등록(OID), OSI 참조 표준들에 대한 유지보수를 주로 다루고 있다. 2013년 4월 회의에서는 한국의 제안으로 OID 기반 이기종 식별자 및 서로 다른 위치에 존재하는 개체들을 관리할 수 있는 프레임워크 표준초안을 제안하여 향후 국제표준을 개발하기로 합의하였다.

3.12. 정보통신 소프트웨어 및 시험 형식 언어(Q.12)

연구과제 12에서는 정보통신 시스템 설계 및 시험을 위해 사용되는 다양한 형식 언어에 대한 표준을 다루고 있다. ITU에서 다루고 있는 설계 언어는 ASN.1, 기술 언어, 메시지 연속 도표 언어, 사용자 요구사항 표기 언어, 시험 및 테스트 통제 표기 언어 등을 다루고 있다. 2013년 4월 회의에서는 기존의 TTCN-3 시험 언어에 대한 유지보수 계획이 수립되었다.

IV. 결 론

본 논문에서는 새로운 연구회기(2013~2016)에 맞아 정보통신 환경에서 응용기술 국제표준들을 개발하고 있는 ITU-T SG17 국제표준화기구에 대한 전반적인 현황에 대해 간단히 살펴보았다[표.2 참조]. 현재 한국은 다른 국가들에 비해 SG17 내에 의장단으로도 많이 진출하였고, 2004년 4월, 한국과 일본 공동으로 모바일

보안 국제표준 채택을 시점으로 한국은 IPTV 보안, 홈 네트워크 보안, USN 보안 등 다수의 국제표준을 개발한 경험이 있어 이를 근거로 ITU-T SG17 내에 국제표준 개발에 주도권 확보가 가능할 것으로 예상된다. 따

라서 한국은 새로운 연구회기를 맞아 국내 산학연 전문가들 간에 충분한 협력을 통해 표준특허 확보 및 국내 기술에 대한 국제표준 채택을 위해 힘을 기울여야 될 것이다.

[표 2] ITU-T SG17 국제표준화 아이템 현황

No.	약어	연구 과제	제정목표	국제표준명(제목)	제안 국가
1	X.1037	Q.2	2013-04	Technical security guideline on deploying IPv6	일본
2	X.gsiiso	Q.2	2014-01	Guidelines on security of the individual information service for operators	중국
3	X.mgv6	Q.2	2014-01	Supplement to ITU-T X.1037 - Supplement on security management guideline for implementation of IPv6 environment in telecommunications organizations	일본
4	X.1051	Q.3	2014	Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	일본 한국
5	X.gpim	Q.3	2015	Guideline for management of personally identifiable information for telecommunication organizations	한국
6	X.sgsm	Q.3	2015	Information security management guidelines for small and medium telecommunication organizations	한국 일본
7	X.Sup1056	Q.3	2014	Supplement to X-series Recommendations ITU-T X.1056 - Related Recommendations, International Standards and documents for security incident management	일본 한국
8	X.1208	Q.4	2013-04	Guidelines for cybersecurity index	한국
9	X.1303	Q.4	2014-01	Common alerting protocol (CAP 1.2)	일본
10	X.1500 Amd.4	Q.4	2013-09	Overview of cybersecurity information exchange - Amendment 4 - Revised structured cybersecurity information exchange techniques	일본
11	X.bots	Q.4	2014-01	Centralized framework for botnet detection and response	한국
12	X.cce	Q.4	2014-01	Common configuration enumeration	미국
13	X.cee	Q.4	2014-01	Common event expression	미국
14	X.cee.1	Q.4	2014-01	CEE overview	미국
15	X.cee.2	Q.4	2014-01	CEE profile	미국
16	X.cee.3	Q.4	2014-01	CEE common log syntax (CLS)	미국
17	X.cee.4	Q.4	2014-01	CEE common log transport (CLT) requirements	미국
18	X.csmc	Q.4	2014-01	An iterative model for cybersecurity operation using CYBEX techniques	일본
19	X.cwss	Q.4	2014-01	Common weakness scoring system	미국
20	X.cybex-beep	Q.4	2014-01	Use of BEEP for cybersecurity information exchange	일본
21	X.cybex-tp	Q.4	2013-09	Transport protocols supporting cybersecurity information exchange	일본
22	X.eipwa	Q.4	2014-01	Guideline on techniques for preventing web-based attacks	한국
23	X.maec	Q.4	2013-09	Malware attribute enumeration and classification	미국
24	X.trm	Q.4	2013-09	Overview of traceback mechanisms	한국
25	X.tfcmm	Q.5	2015-Q3	Technical framework for countering mobile messaging spam	중국
26	X.ticvs	Q.5	2014-01	Technologies involved in countering voice spam in telecommunication organizations	중국
27	X.1198	Q.6	2013-04	Virtual machine-based security platform for renewable IPTV service and content protection	한국
28	X.msec-7	Q.6	2014-01	Guidelines on the management of infected terminals in mobile networks	중국
29	X.msec-8	Q.6	2014-01	Secure application distribution framework for communication devices	한국

No.	약어	연구 과제	제정목표	국제표준명(제목)	제안 국가
30	X.sgsec-1	Q.6	2014-01	Security functional architecture for smart grid services using telecommunication network	한국
31	X.unsec-1	Q.6	2014-01	Security requirements and framework of ubiquitous networking	중국
32	X.1141 Amd.1	Q.7	2014-01	Security Assertion Markup Language (SAML 2.0) - Amendment 1: Errata	캐나다
33	X.1142 Amd.1	Q.7	2014-01	eXtensible Access Control Markup Language (XACML 2.0) - Amendment 1: Errata	캐나다
34	X.1156	Q.7	2013-04	Non-repudiation framework based on a one time password	한국
35	X.p2p-3	Q.7	2014-09	Security requirements and mechanisms of peer-to-peer-based telecommunication network	중국
36	X.sap-5	Q.7	2014-09	Guideline on local linkable anonymous authentication for electronic services	한국
37	X.sap-7	Q.7	2014-09	Technical capabilities of fraud detection and response for services with high assurance level requirements	한국
38	X.sap-8	Q.7	2014-09	Efficient multi-factor authentication mechanisms using mobile devices	한국
39	X.sap-9	Q.7	2014-09	Delegated non-repudiation architecture based on ITU-T X.813	한국
40	X.websec-5	Q.7	2014-01	Security architecture and operations for web mashup services	한국
41	X.xacml3	Q.7	2013-09	eXtensible Access Control Markup Language (XACML) 3.0	캐나다
42	X.cc-control	Q.8	2014-10	Information technology - Security techniques - Code of practice for information security controls for cloud computing services based on ISO/IEC 27002	일본 중국
43	X.ccsec	Q.8	2013-09	Security framework for cloud computing	중국
44	X.fsspv	Q.8	2014-01	Framework for a secure service platform for virtual network	중국
45	X.goscc	Q.8	2014-01	Guidelines of operational security for cloud computing	중국
46	X.sfcse	Q.8	2014-01	Security functional requirements for Software as a Service (SaaS) application environment	중국
47	X.1092	Q.9	2013-04	Integrated framework for telebiometric data protection in e-health and telemedicines	한국
48	X.bhsm	Q.9	2014-01	Information technology - Security Techniques - Telebiometric authentication framework using biometric hardware security module	한국
49	X.tam	Q.9	2014-01	A guideline to technical and operational countermeasures for telebiometric applications using mobile devices	한국
50	X.th2	Q.9	2014-01	Telebiometrics related to physics	ISO
51	X.th3	Q.9	2014-01	Telebiometrics related to chemistry	ISO
52	X.th4	Q.9	2014-01	Telebiometrics related to biology	스위스
53	X.th5	Q.9	2014-01	Telebiometrics related to culturology	스위스
54	X.th6	Q.9	2014-01	Telebiometrics related to psychology	스위스
55	X.1255	Q.10	2013-04	Framework for discovery of identity management information	미국
56	X.atag	Q.10	2014-01	Attribute aggregation framework	일본
57	X.authi	Q.10	2014-01	Guideline to implement the authentication integration of the network layer and the service layer	중국
58	X.giim	Q.10	2013-09	Mechanisms to support interoperability across different IDM services	중국
59	X.iamt	Q.10	2016	Identity and access management taxonomy	캐나다
60	X.idmcc	Q.10	2013-09	Requirement of IdM in cloud computing	중국
61	X.idmts	Q.10	2016	Framework for the interoperable exchange of trusted services	-
62	X.mob-id	Q.10	2014-01	Baseline capabilities and mechanisms of identity management for mobile applications and environment	한국

No.	약어	연구 과제	제정목표	국제표준명(제목)	제안 국가
63	X.oitf	Q.10	2014-01	Open identity trust framework	미국
64	X.scim-use	Q.10	2016	Application of system for cross identity management (SCIM) in telecommunication environments	캐나다
65	e-X.Imp500	Q.11	-	Directory Implementer's Guide	스위스
66	F.5xx	Q.11	2014-03	Directory Service - Support of Tag-based identification services	스위스
67	X.500 (8 edition)	Q.11	2016	Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services	스위스
68	X.501 (8 edition)	Q.11	2016	Information technology - Open Systems Interconnection - The Directory - Models	스위스
69	X.509 (8 edition)	Q.11	2016	Information technology - Open Systems Interconnection - The Directory - Public-key and attribute certificate frameworks	스위스
70	X.511 (8 edition)	Q.11	2016	Information technology - Open Systems Interconnection - The Directory - Abstract Service Definition	스위스
71	X.518 (8 edition)	Q.11	2016	Information technology - Open Systems Interconnection - The Directory - Procedures for Distributed Operations	스위스
72	X.519 (8 edition)	Q.11	2016	Information technology - Open Systems Interconnection - The Directory - Protocols	스위스
73	X.520 (8 edition)	Q.11	2016	Information technology - Open Systems Interconnection - The Directory - Selected Attribute Types	스위스
74	X.521 (8 edition)	Q.11	2016	Information technology - Open Systems Interconnection - The Directory - Selected object classes	스위스
75	X.525 (8 edition)	Q.11	2016	Information technology - Open Systems Interconnection - The Directory - Replication	스위스
76	X.906	Q.11	2016	Information technology - Open distributed processing - Use of UML for ODP system specification	스위스
77	X.911	Q.11	2014-01	Information technology - Open distributed processing - Reference model - Enterprise language	-
78	X.email	Q.11	2014	Certified mail transport and certified post office protocols	미국
79	X.orf	Q.11	2015	Information technology - Security techniques - OID-based resolution framework for heterogeneous identifiers/locators	한국
80	X.pki-em	Q.11	2016-09	Information Technology - Public-Key Infrastructure: Establishment and maintenance	스위스
81	X.pki-prof	Q.11	2016-09	Information Technology - Public-Key Infrastructure: Profile	스위스
82	Z.Suppl.1	Q.11	2013-04	Supplement 1 to Z-series Recommendations - ITU-T Z.100-series - Supplement on methodology on the use of description techniques	영국 미국
83	Z.100 Annex F1	Q.12	2013-09	Specification and Description Language - Overview of SDL-2010 - SDL formal definition: General overview	영국
84	Z.100 Annex F2	Q.12	2013-09	Specification and Description Language - Overview of SDL-2010 - SDL formal definition: Static semantics	영국
85	Z.100 Annex F3	Q.12	2013-09	Specification and Description Language - Overview of SDL-2010 - SDL formal definition: Dynamic semantics	영국
86	Z.109	Q.12	2013-09	Specification and Description Language - Unified modeling language profile for SDL-2010	미국

참고문헌

[1] ITU-T 홈페이지, <http://www.itu.int>
 [2] 오홍룡, 박정식, 진병문, 염홍열, “정보보호 국제표준화 현황 및 추진체계 분석” 정보보호학회지, v.21, no.2, pp.7-18, 2011.04.
 [3] 오홍룡, 진병문, 염홍열, 강신각, “ITU-T SG17 정보보호 국제표준화 동향 및 향후 전망”, 정보보호학회지, v.18, no.4, pp.13-29, 2008.08.
 [4] 오홍룡, 염홍열, “정보보호 국제표준화 동향 및 향후 전망”, 정보보호학회지, v.17, no.1, pp.63-78, 2007.02.
 [5] 염홍열, 오홍룡, 나재훈, 백중현, “ITU 연구동향 : ITU-T SG17 보안 분야”, 한국 ITU 연구위원회 연

구동향 보고서, 2012.12.
 [6] ITU-T SG17 TD31/R1, “Report of Working Party 1/17, Fundamental security”, 17-26 April 2013.
 [7] ITU-T SG17 TD32/R1, “Report of Working Party 2/17, Network and information security”, 17-26 April 2013.
 [8] ITU-T SG17 TD33/R5, “Report of Working Party 3/17, Identity management and cloud computing security”, 17-26 April 2013.
 [9] ITU-T SG17 TD68/R1, “Report of Working Party 4/17, Application Security”, 17-26 April 2013.
 [10] ITU-T SG17 TD69/R5, “Report for WP 5/17 plenary”, 17-26 April 2013.

<著者紹介>



오 홍 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
 2005년 3월~현재 : ITU-T SG17 국내 분과위원회 간사
 2009년 2월~현재 : ITU-T SG17 Q.2 Associate Rapporteur
 <관심분야> 보안프로토콜, 정보보호표준



김 영 화 (Youngwha Kim)

1986년 2월 : 전북대학교 전자공학과 졸업
 1988년 2월 : 한양대학교 전자공학과 석사
 2006년 2월 : 한양대학교 전자공학과 박사
 1988년~2002년 : 한국전자통신연구원 선임연구원
 2002년~현재 : 한국정보통신기술협회 표준화본부 정보기술부 부장
 <관심분야> 정보보호 및 기반 소프트웨어 표준화



염 홍 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
 1997년 3월~2000년 3월 : 순천향대학교 산업기술연구소 소장
 2000년 4월~2006년 2월 : 순천향대학교 산학연권소시업센터 소장
 1997년 3월~현재 : 한국정보보호학회 총무이사, 학술이사, 교육이사, 총무이사, 논문지편집위원 위원장, 수석부회장(역), 명예회장(현)
 2005년~2008년 : ITU-T SG17 Q.9 Rapporteur(역)
 2006년 11월~2009년 2월 (구) 정통부 정보보호 PM/, 정보통신연구진흥원 정보보호전문위원
 2011년 1월 ~ 12월 : 한국정보보호학회 회장(역)
 2008년 7월~현재 : 방송통신위원회 자체평가위원회
 2008년 7월 ~2013년 2월 : 행정안전부 정책자문위원회
 2013년 5월 ~현재 : 미래창조과학부 자체평가위원회
 2009년 5월~현재 : 국정원 암호검증위원회 위원
 2009년~현재 : ITU-T SG17 부의장 /SG17 WP3 의장
 2012년 6월 ~현재 : 정보보안산업표준포럼 의장
 <관심분야> 인터넷 보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜