

ITU-T SG17 정보보호 국제표준화 동향 및 향후 전망

오 흥 룡*, 진 병 문*, 염 흥 열**, 강 신 각***

요 약

정보보호 분야의 국제표준화는 각 기술들의 특성 및 사용자들의 관점 등을 고려하여, 다양한 국제표준화기구에서 국제 표준개발 및 관련 연구가 이루어지고 있다. 즉, ITU-T SG17에서는 전기통신(Telecommunication) 관점에서 정보보호 응용기술들에 대한 국제표준화가 추진되고 있으며, ISO/IEC JTC1/SC27(정보보호), SC37(바이오인식)에서는 정보보호 원천 기술들에 대한 국제표준화가, IETF Security Area에서는 인터넷 서비스의 품질 보장 및 향상된 인터넷 환경 구축을 위해 실제적인 구현 관점에서의 보안기술 국제표준화를 추진하고 있다. 본 논문에서는 ITU-T SG17에서 추진되고 있는 정보보호 국제표준화 이슈를 중점적으로 다루고자 하며, 이번 연구회기('05~'08) 동안에 논의되었던 주요 표준화 추진 결과와 차기 연구회기('09~'12)를 준비하기 위한 구조조정 결과 및 향후 표준화 추진방향 등을 제시하여, 향후 국내에서 ITU-T SG17에 활동하고자 하는 전문가들에게 유용한 자료를 제공하고자 한다.

I. 서 론

초고속 인터넷 환경 구축과 다양한 디바이스들의 개발은 사용자들에게 많은 편리성 증가와 삶의 질을 향상 시키게 되는 장점을 가져왔다. 하지만, 이와 반대로 사용자들의 개인정보 및 소중한 자산들이 사용자들의 동의 없이 인터넷 상에서 오남용되거나 제3의 악의적인 공격자들에 의해 위협받게 되는 단점을 가지게 되었다. 따라서 이런 단점을 보완하고 사용자 및 각 기관들의 소중한 자산 등을 안전하게 보호하기 위한 정보보호 기술은 그 중요성이 점점 증가되고 있는 추세이다. 또한, 네트워크 시스템, 다양한 디바이스 및 응용서비스들이 개발/설계되는 시점부터 보안이라는 기술이 더 이상 옵션이 아니라, 필수 항목으로 자리매김하게 되었다. 특히, 이와 같은 정보보호 기술 개발과 더불어 해당 기술들의 상호운용성 확보와 국가 간의 호환성 확보를 위한 정보보호 분야의 국제표준 개발도 그 중요성이 날로 커져가고 있다. 즉, 세계적으로 각 국가들은 자신들의 고유기술을 국제표준에 반영하여 해당 기술에 대한 IPR(지적재산권) 및 특허 수수료 등을 확보하기 위해 적극적으로 국제표준화 활동에 참여하고 있는 추세이다. 따

라서 국내에서도 국제표준화 활동에 적극적인 참여가 필요한 시점이며, 국제표준들에 대한 체계적인 분석과 활동현황 등을 파악하여, 국내 고유기술을 국제표준에 반영될 수 있도록 적극적인 추진전략이 요구된다.

본 논문에서는 정보보호 응용기술들을 중점적으로 다루고 있는 국제표준화기구 ITU-T SG17에서 이번 연구회기('05~'08) 동안의 주요결과와 차기 연구회기('09~'12) 동안의 구조조정 결과 및 향후 추진방향 등을 제시하여, 국내에서 ITU-T SG17에 활동하고자 하는 전문가들에게 유용한 자료를 제공하고자 한다.

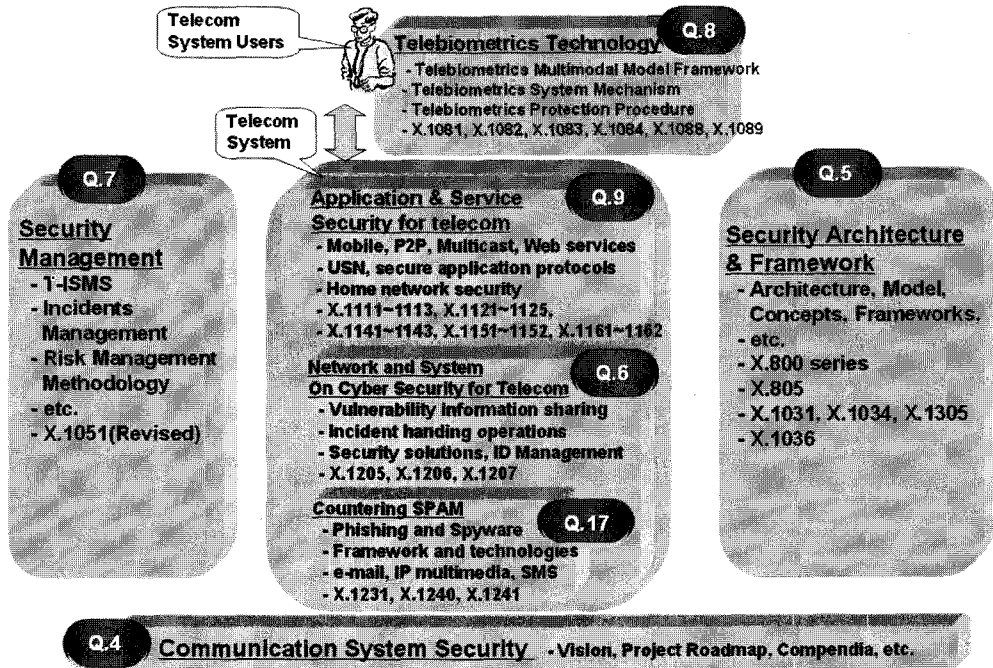
II. ITU-T SG17 국제표준화 현황('05~'08)^[1,8,9]

1865년 5월, UN 산하에 신설된 국제전기통신연합(ITU : International Telecommunication Union)은 크게 전파규칙, 주파수 할당 등의 이슈를 다루고 있는 전파통신(Radiocommunication), 전기통신기술, 운용 및 요금 등의 이슈를 다루고 있는 전기통신표준화(Telecommunication), 그리고 개발도상국의 통신망 현대화를 위한 정책, 기술적 지원 등을 다루고 있는 전기통신 개발(Development)이라고 부르는 3개 섹터로 구성된

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

** 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr)

*** 한국전자통신연구원 표준연구센터 (sgkang@etri.re.kr)



(그림 1) ITU-T SG17 보안 분야 연구영역('05~'08)

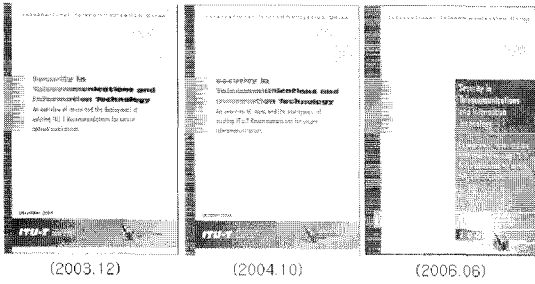
다. 이중에 정보보호 분야는 ITU-T 산하 SG17/WP2에서 7개의 연구과제(Question)로 국제표준화가 진행되고 있다. 또한, SG17 내에 정보보호 이외에 WP1(개방형 통신기술)과 WP3(소프트웨어) 분야도 함께 다루고 있다. 한국은 SG17에서 매 국제회의 개최 때마다, 50% 이상의 기고서(국가/섹터)를 제안하여, 국제표준초안에 반영 및 한국 주도로 국제표준을 개발하고 있다. 또한, 한국은 SG17 내에서 부의장(진병문(TTA))과 5개의 연구과제에서 라포처(Rapporteur) 및 부-라포처로 회의를 주재하고 있다. 한국은 이번 연구회기 동안 총 208건의 기고서를 제출하였으며, 이들에 대한 성과물로 총 16건(멀티캐스트: 3건, 보안: 13건)이 국제표준으로 제정되었다. 현재 SG17에서 한국은 보안 분야에서 총 20건의 국제표준초안에 대해 에디터십을 확보하여 국제표준을 개발하고 있으며, 2008년 9월 회의에서 총 7건이 추가적으로 국가별 의견수렴(Consent/Determination)으로 승인받을 계획에 있어, 크게 문제가 없다면 2008년 말에 국제표준으로 제정될 예정이다. 이와 같이 4년간 한국대표단들의 활동 결과는 SG17 내에서도 매우 활발한 국가로 인지도가 높게 평가받고 있다^[16-18].

SG17 산하 보안 분야를 담당하고 있는 7개의 연구과제의 연구영역은 [그림 1]과 같으며, 한국은 보안 분야

의장단으로 Q.7(부-라포처, 김정덕(중앙대)), Q.8(라포처, 김학일(인하대)), Q.9(라포처, 염홍열(순천향대)) 연구과제에서 회의를 주재하고 있다.

2.1. 통신시스템 보안 프로젝트(Q.4)

연구과제 4에서는 ITU-T 내에 전체적인 보안 요약물, 전략, 비전, 계획 등을 연구하고 있으며, 정보보호 표준화 정보공유를 위한 워크숍 및 타 표준화기구들과의 협력 체계 구축을 위한 작업들을 수행하고 있다. 주요활동 결과로는 보안 분야의 전문가 및 사용자들에게 편의성을 제공하기 위하여, 보안 표준화 로드맵을 개발하였다. 또한, 현재 ITU-T 홈페이지에서 관련 자료를 빠르게 검색하여 서비스될 수 있도록 데이터베이스 구조 등을 개발하고 있으며, ATIS(Alliance for Telecommunications Industry Solutions) 표준 및 주제별 검색 기능 강화와 검색 결과를 엑셀파일로 정리되도록 구축하였다. 보안 표준화 로드맵(v2.2, 2007.09)의 주요 내용은 Part 1 : 표준화기구들의 구조 및 활동현황, Part 2 : 제정된 표준현황, Part 3 : 각 표준화기구들의 워크 프로그램(작업현황), Part 4 : 향후 요구사항 및 계획된 표준화 계획, Part 5 : 보안표준의 적용사례들로 구성되



[그림 2] ITU-T 보안 매뉴얼 핸드북

어 있다. 또한, ITU-T 활동에 처음 참여하는 보안 전문가들을 위해 보안 매뉴얼 핸드북(2006.06)을 발간하였으며, ITU-T 보안 국제표준이 추가적으로 개발되는 현황에 따라 계속해서 업데이트를 하고 있다. 보안 매뉴얼의 주요내용은 보안구조 및 서비스, 보안과 관련된 기본 사항 정의, 정보통신 네트워크 환경을 위한 보안요구사항, 공개키 및 권한관리기반, 응용보안, 인프라보안, 침해사고관리 등으로 구성되었으며, 각 항목에 대한 설명과 해당 ITU-T 국제표준들을 설명하고 있다. 다음의 [그림 2]는 ITU-T에서 발간된 보안 매뉴얼 핸드북이다.

2.2. 보안구조 및 프레임워크(Q.5)

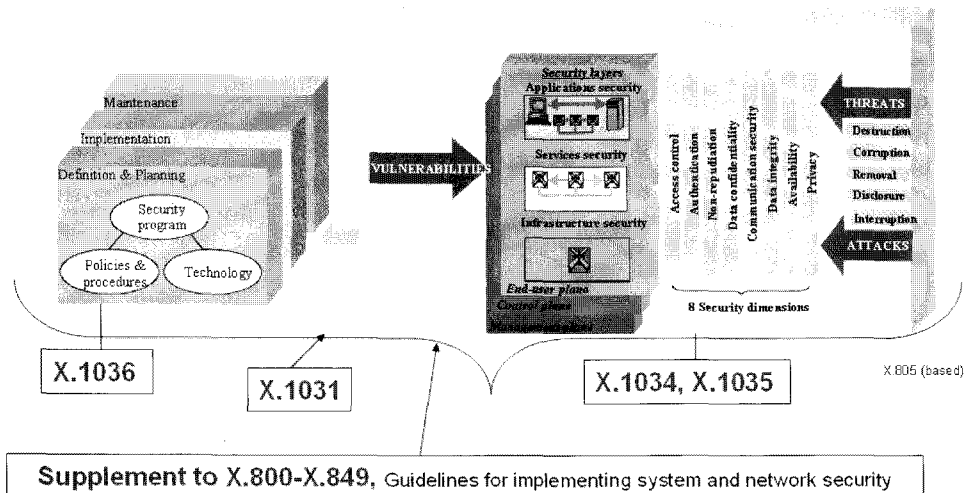
연구과제 5에서는 보안시스템의 구조, 모델, 개념, 전반적인 서비스 시나리오 등을 연구하고 있으며, 가장 대표적인 것은 X.800 시리즈 표준들이 가장 대표적이다. 본 그룹의 주요활동은 ITU-T X.805(Security architecture

for systems providing end-to-end communication) 표준의 응용 표준들을 개발하는 것으로 네트워크와 사용자 간에 보안제어 역할분담을 위한 구조(X.1031) 표준을 제정하였다. 또한, 다른 응용 표준으로는 미국에서 X.805 기반의 물리적 보안 프레임워크 표준을 개발하자고 제안하였으며, 일본은 X.805 기반의 네트워크 보안 인증서 평가 방법과 관련된 표준초안을 개발하고 있다. X.805 응용과 관련해서는 미국, 러시아, 캐나다, 일본에서 가장 적극적으로 참여하고 있다.

한국은 데이터통신 네트워크에서 EAP 기반의 인증 및 키 관리 가이드라인(X.1034)과 이기종 네트워크 환경에서 서로 다른 보안 시스템과 이들의 서비스를 제어할 수 있는 네트워크 보안을 위한 정책생성, 저장, 분배, 실행을 위한 프레임워크(X.1036) 2건의 국제표준을 개발하였다. 또한, 미국의 제안으로 패스워드 기반의 인증 키교환(PAK) 프로토콜(X.1035) 표준을 제정하였다. 다음의 [그림 3]은 Q.5에서 개발한 각 표준들 간에 관계를 정의하고 있다.

2.3. 사이버보안(Q.6)

연구과제 6에서는 크게 사이버보안 이슈와 아이덴티티 관리(Identity Management) 이슈를 중점적으로 개발하고 있다. 첫 번째로 사이버보안은 인터넷 및 네트워크 시스템 등에서 발생할 수 있는 침해사고대응방법, 보안솔루션, 사이버보안 취약점들에 대한 해결방법 및 정



[그림 3] 보안구조 및 프레임워크(Q.5) 표준들의 관계

보공유 방법 등에 대해 연구하고 있다. 두 번째 아이덴티티 관리는 정보통신 환경을 구성하고 있는 각 객체(사용자, 디바이스, 서비스제공자 등)들의 아이덴티티를 관리하는 방법과 전 세계적으로 상호운용성이 보장되는 글로벌한 아이덴티티 국제표준 개발에 중점을 두고 연구하고 있다.

주요활동 결과로는 캐나다 주도로 사이버 보안의 개요(X.1205)와 OASIS의 언어(XML)를 ITU-T ASN.1 언어로 바꾸는 표준(X.1303(CAP 1.1))들을 개발하였으며, 일본은 보안과 관련된 정보들을 자동으로 업데이트할 수 있는 가이드라인 표준(X.1206), 싱가포르의 스파이웨어 및 악성S/W들의 위협을 검색할 수 있는 가이드라인 표준(X.1207)을 개발하였다.

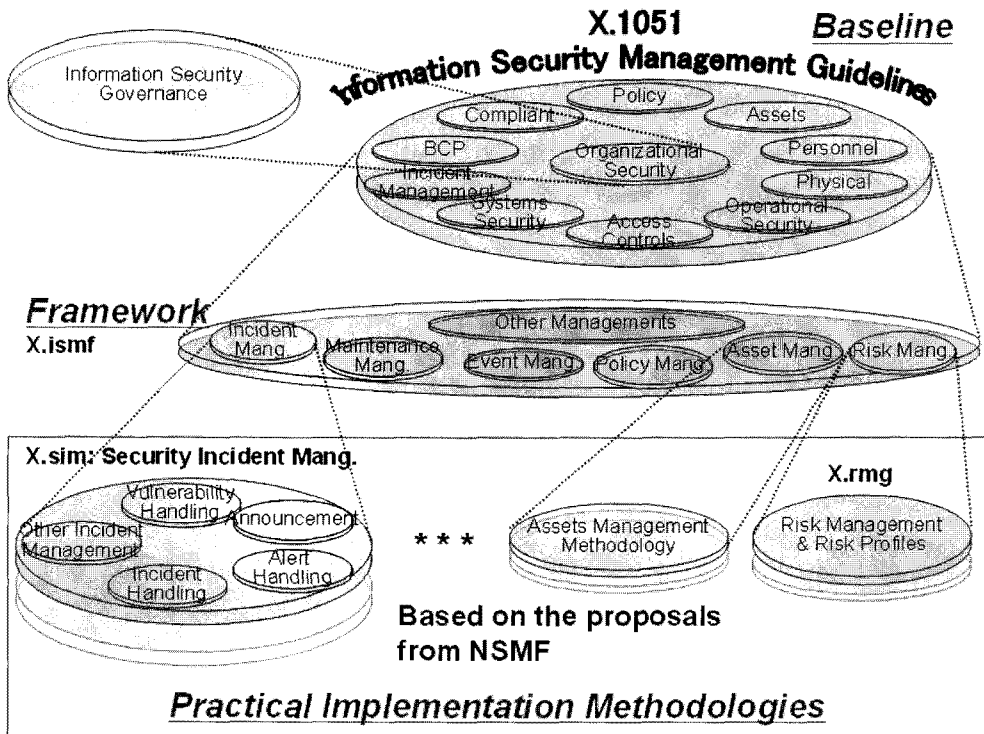
아이덴티티 관리 분야에서는 2006년 12월에 신설되어 2007년 9월에 활동을 종료한 FG-IdM의 결과물들에 대한 표준화를 추진하고 있으며, 2008년 내에 요구사항, 공동데이터모델 등이 국제표준으로 제정될 예정이다.

한국은 RFID 프라이머시 보호가이드라인(X.rfpg)과 유무선 IPv6 환경에서 전파되는 임을 예방하기 위한 기술(X.gopw), 사용자 제어를 위한 디지털 아이덴티티 상

호교환 프레임워크(X.idif)와 보안정보 공유 프레임워크를 위한 요구사항(X.sisfreq)들을 개발하고 있으며, 가능한 2008년 9월 SG17 회의에서 국가별 의견수렴을 목표로 추진하고 있다.

2.4. 보안관리(Q.7)

연구과제 7에서는 일본을 중심으로 정보보호관리 시스템, 침해사고관리방법, 위협관리 방법론 등과 같이 정보통신 시스템을 안전하게 관리하기 위한 표준들을 개발하고 있다. Q.7의 주요이슈는 2004년 7월에 제정된 정보보호관리시스템(X.1051 : ISMS-T) 표준을 ISO/IEC 27002 표준을 기반으로 개정하였으며, 부록으로 사이버 공격 및 네트워크 폭주(congestion) 등과 같은 보안 해결 방안들을 추가하여 정의하였다. 또한, 본 그룹에서는 ISO/IEC 27000, 27003, 27004, 27005 표준들을 신중히 검토하여, ITU-T 표준간의 관계를 재조정키로 하였다. 현재, 한국은 정보통신 환경에서의 보안사고관리 가이드라인(X.sim) 표준초안을 개발중에 있으며, 주요 내용으로 ITU-T E.409(Incident organization and security



(그림 4) 보안관리(Q.7) 표준 및 표준초안 간의 관계

incident handling : Guidelines for telecommunication organizations) 표준과 보안사고 발생원인, 현상, 결과 등을 포함하여 개발중에 있으며, 빠르면 2008년 내에 국제 표준으로 제정할 계획이다. 또한, 한국은 차기 연구회기 신규 표준화 아이টে으로 보안 거버넌스, 중소기업 보안관리, 서비스 제공자를 위한 프라이버시 보호 관리 등을 제안하였으며, 이들에 대해 Q.7에서 계속해서 논의를 진행하기로 합의되었다.

Q.7의 다른 이슈는 중국에서 제안한 네트워크 보안관리 프레임워크(X.nsmf)로 X.1051에 정의된 보안관리 기능들을 세부적으로 정의하고 있다. 또한, 영국에서는 위협관리 및 위협 프로파일 가이드(X.rmg) 표준초안을 개발하고 있다.

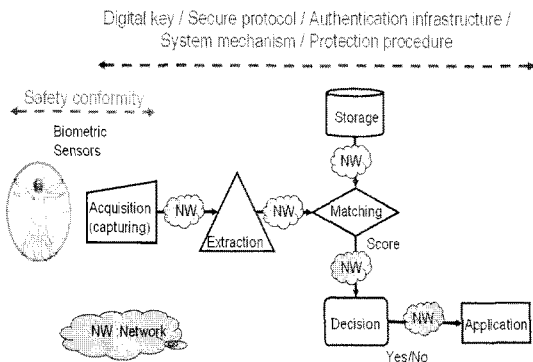
다음의 [그림 4]는 Q.7에서 제정된 표준과 향후 개발하고자 하는 표준초안들 간에 관계를 정의하고 있다.

2.5. 텔레-바이오인식(Q.8)

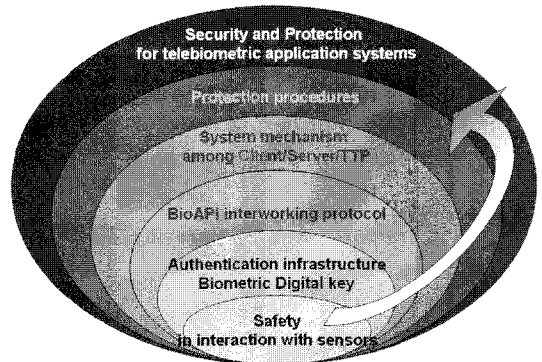
연구과제 8에서는 [그림 5]와 같이 정보통신 네트워크 환경에서 바이오인식 기술을 응용하기 위한 인증메커니즘, 바이오 정보 보호 가이드라인, 멀티모달 모델 프레임워크 등의 표준을 연구하고 있다. 또한, Q.8에서는 한국에서 라포치를 담당하고 회의를 주재하고 있어, 한국의 바이오인식 기술을 국제표준으로 개발하기에 좋은 위치에 있다. 현재, Q.8에서는 프랑스, 스위스, 중국, 일본, 한국에서 표준초안을 주도적으로 개발하고 있으며, 이번 연구회기 동안 개발된 표준으로는 스위스의 제안으로 텔레바이오인식 시스템과 인간과의 상호작용에 필요한 규정 정의(X.1082), 프랑스의 제안으로 텔레바이오인식 환경에서 시스템들 간의 상호연동 메커니즘

(X.1083), 일본과 한국의 공동 제안으로 X.509(PKI) 기반의 바이오인식 인증메커니즘(X.1084), 한국의 제안으로 바이오정보를 이용한 전자키 생성 프레임워크(X.1088), 중국의 제안으로 PKI와 PMI 환경에서의 바이오인식 인증메커니즘(X.1089)을 개발하였다. 또한, 한국에서는 텔레바이오인식 환경에서 전달되는 바이오정보를 안전하게 보호하기 위한 바이오정보에 대한 생명주기(생성, 전달, 저장, 폐기 등)의 전체 과정을 보호할 수 있는 표준초안 2건을 개발하고 있으며, 이들은 단일 바이오정보 보호 표준초안(X.ttp-1)과 다중 바이오정보 보호 표준초안(X.ttp-2)으로 분리된다. 그리고 일본과 한국 공동으로 ITU-T X.1084 표준에서 정의하고 있는 인증메커니즘을 사용하는 클라이언트들의 보호프로파일을 정의하고 있는 표준초안(X.tsm-2)을 개발중에 있다. 현재, 상기 3건의 표준초안은 2008년 9월에 개최되는 SG17 회의에서 국가별 의견수렴으로 승인될 예정이다.

차기 연구회기 동안 Q.8에서는 스위스의 제안으로 텔레바이오인식 환경에서의 원격의료 서비스(X.th)와 한국의 제안으로 원타임 템플릿을 이용한 인증 프레임워크(X.ott), ITU-T X.1084, X.1088를 원격의료 서비스에 적용하기 위한 프레임워크(X.tif)를 개발하기로 합의하였다. 또한, Q.8에서는 ISO/IEC JTC1/SC37(바이오인식) 그룹과 지속적인 협력문서(Liaison)를 교환하고 있어, 두 그룹 간에 조율되고 상호운용성이 보장되는 국제표준을 개발하기 위해 노력하고 있다. 다음의 [그림 6]은 Q.8에서 향후 추진하고자 하는 표준화 추진 방향을 나타내고 있다. 바이오인식 시스템들 간의 안전한 상호연동에서 점점으로 다양한 응용시스템들에 적용하기 위한 표준을 개발할 계획이다.



[그림 5] 텔레-바이오인식(Q.8) 연구범위



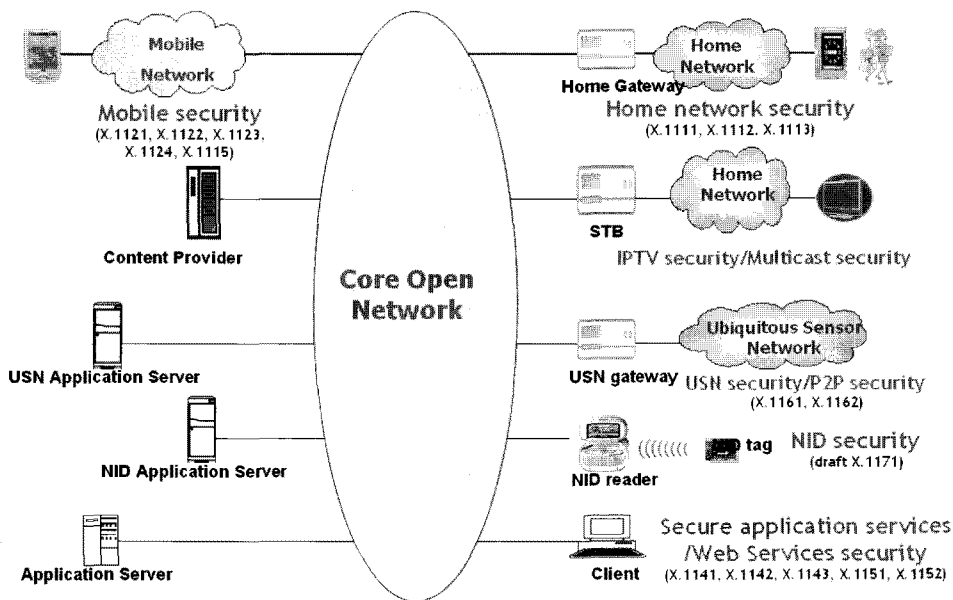
[그림 6] 텔레-바이오인식(Q.8) 표준화 추진 방향

2.6. 안전한통신서비스(Q.9)^[20]

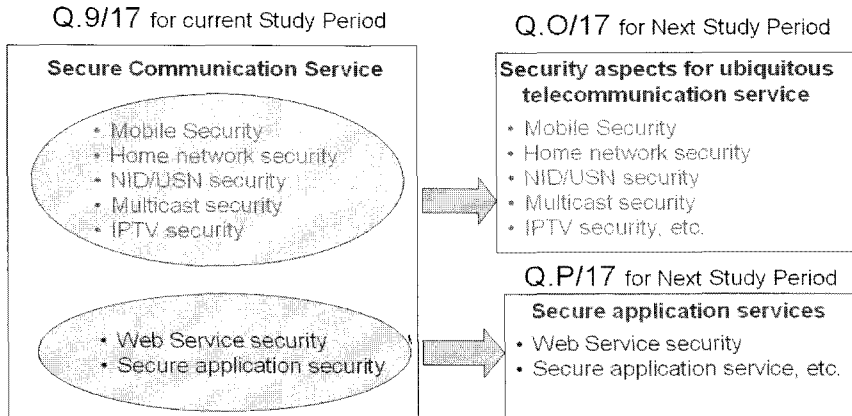
연구과제 9에서는 안전한통신서비스라는 이슈로 SG17 내에서 가장 활발한 그룹으로 모바일보안, 홈네트워크 보안, IPTV 보안, USN 보안, NID(RFID) 보안, 멀티캐스트 보안, 응용서비스 보안, 웹서비스 보안, 응용프로토콜 보안, P2P 보안 등 다수의 정보보호 이슈를 다루고 있다. 또한, Q.9의 라포처를 한국에서 담당하고 회의를 주재하고 있어, 한국 주도로 다수의 국제표준을 개발하였으며, 향후 중요한 위치를 선점하고 있다.

Q.9에서의 첫 번째 토픽은 모바일보안이다. 2004년 4월, 한국과 일본 공동으로 개발한 모바일 중단간 데이터통신을 위한 보안기술 프레임워크(X.1121), PKI 기반의 안전한 모바일 시스템 구현을 위한 가이드라인(X.1122) 2건의 표준을 제정할 이후, 이번 연구회기 동안에는 중국의 제안으로 안전한 모바일 중단간 데이터통신을 위한 차별화된 보안서비스(X.1123), 모바일 중단간 데이터통신을 위한 인증구조(X.1124), 모바일 데이터통신에서의 상호연동 시스템(X.1125) 3건의 표준을 개발하였다. 두 번째 토픽은 홈네트워크 보안이다. 홈네트워크 보안 분야는 한국 주도로 개발되었으며, ITU-T 내에서 개발되고 있는 다양한 홈네트워크 기술 표준에 보안적 측면을 정의하고 기본 모델을 정의하였다. 제정된 표준으로는 홈네트워크를 위한 보안기술 프

레이워크(X.1111), 홈네트워크를 위한 디바이스 인증서 프로파일(X.1112), 홈네트워크 서비스를 위한 사용자 인증 메커니즘 가이드라인(X.1113)을 개발하였으며, 네 번째 표준초안으로 홈네트워크 환경에서의 권한부여 프레임워크(X.homsec-4)가 개발중에 있다. 세 번째 토픽은 웹서비스 보안으로 캐나다의 제안으로 OASIS의 XML 보안 표준들을 ITU-T 표준으로 2건을 제정하였다. 즉, 보안 정보를 교환하기 위한 XML 기반의 프레임워크(X.1141, SAMLv2.0)를 제정하였으며, 이는 통신 주체들(사용자, 컴퓨터, ISP 등) 간에 요구되는 보안 주장(인증, 권한부여, 속성 등)들과 상호 간에 교환되는 메시지 형식을 XML 언어로 표현하기 위한 방법을 정의하고 있다. 또한, 통신주체들 간에 요구되는 접근제어 정책들을 XML 언어로 표현하기 위한 방법(XACML v2.0, X.1142)을 제정하였으며, 이는 임의의 어떤 자원에 접근하고자하는 개체들에게 일정한 권한을 부여하는 정책과 이들 정책을 평가하는 규칙, 이들을 XML로 표현하는 방법들을 정의하고 있다. 그리고 한국 주도로 개발된 모바일 웹서비스 환경에서 메시지 보호를 위한 보안구조(X.1143)를 개발하였으며, 이는 모바일 단말을 웹서비스 환경에서 적용하기 위한 보안구조와 다양한 서비스 시나리오들을 정의하고 있다. 넷 번째 토픽은 응용프로토콜 보안으로 한국의 제안으로 안전한 패스워드 기반 인증 및 키교환이 가능한 프로토콜 가이드라인



[그림 7] 안전한 통신서비스(Q.9) 연구범위



(그림 8) 차기 연구회기 Q.9 구조조정 방향

(X.1151)을 개발하였다. 이는 네트워크 환경에서 응용될 수 있는 다양한 인증프로토콜들의 공통 요구사항을 도출하였으며, 이를 기반으로 사용자가 구현 시, 안전한 프로토콜 선정할 수 있는 기준 및 가이드라인을 정의하고 있다. 또한, 일본의 제안으로 신뢰된 제3의 그룹(TTP : Trusted Third Party)을 이용한 안전한 종단간 데이터통신 기술(X.1152)을 개발하였다. 다섯 번째 토픽은 P2P 보안으로 일본에서 다양한 P2P 환경에서 공통으로 요구되는 프레임워크(X.1161)를 개발하였으며, 한국에서는 다양한 P2P 환경을 위한 보안구조와 이들에 대한 운영방법(X.1162)들을 개발하였다. 여섯 번째 토픽은 NID(RFID) 보안이다. NID 보안은 한국에서 2건의 표준초안을 개발중에 있으며, 이들 중에 네트워크 환경을 기반으로 ID 서비스에서 개별 식별정보 보호를 위한 프레임워크(draft X.1171)는 Q.9에서 개발하였으며, RFID 프라이버시 보호 가이드라인(X.rfpg)는 현재 Q.6에서 개발중에 있다. 일곱 번째 토픽은 USN 보안으로 한국의 제안으로 USN 보안 프레임워크(X.usnsec-1)를 개발중에 있다. 이는 유비쿼터스 센서 네트워크 환경에서 발생할 수 있는 위협분석과 이를 충족하기 위한 보안요구사항, 보안요구사항에 따른 보안기술 정의, 보안모델, 구현 관점에서의 보안기능을 정의하고 있다. 여덟 번째 토픽은 멀티캐스트 보안으로 한국의 제안으로 멀티캐스트 통신에서의 보안요구사항 및 프레임워크(X.mcsec-1)와 중계전송 멀티캐스트 프로토콜의 보안 파트(X.608.1 Amd.1)를 연구과제 1(Q.1 : 멀티캐스트) 그룹과 협력하여 개발중에 있다. 아홉 번째 토픽은 요즘 이슈화가 되고 있는 IPTV 보안 이슈이다. 현재, Q.9에서는 FG-IPTV 결과물의 보안 부분으로 IPTV 보안적

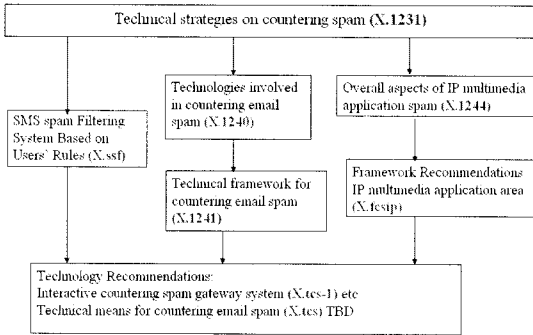
관점을 위한 기능요구사항과 구조(X.iptvsec-1)를 중국, 한국, 일본이 참여하여 개발중에 있다. 또한, 2008년 4월, 한국의 제안으로 IPTV 트랜스코더블(transcodable) 기술을 위한 요구사항과 메커니즘(X.iptvsec-2)을 제안하였고, 2008년 5월, 한국에서 IPTV를 위한 키관리 프레임워크(X.iptvsec-3)를 제안하여 채택되었고, 향후 한국 주도하에 표준초안을 개발키로 하였다.

앞서 설명한 바와 같이 현재 Q.9에서는 응용서비스 관점에서의 다양한 보안 이슈를 다루고 있어, 차기 연구회기에서는 이를 다음 [그림 8]과 같이 2개의 연구과제(유비쿼터스 통신서비스를 위한 보안 측면, 안전한 응용서비스를 위한 보안 측면)로 분리하기로 합의되었다.

2.7. 기술적인 방법에 의한 스팸차단(Q.17)

연구과제 17에서는 기술적인 방법으로 악성스팸을 차단하기 위한 방법과 가이드라인과 관련된 표준을 연구하고 있으며, 크게 이메일(e-mail)에 의한 스팸 차단과 IP 멀티미디어 응용(VoIP, 미디어서비스 등)에 대한 스팸 차단으로 분리하여 표준을 개발하고 있다. 또한, 2007년 9월에는 중국의 제안으로 위의 카테고리에 모바일 SMS 스팸 차단을 위한 표준 개발을 추가키로 합의되었다.

Q.17에서 개발된 표준으로 한국은 e-mail 스팸차단을 위한 기술정의(X.1240)와 IP 멀티미디어 응용 스팸차단에 관한 전반적인 개요정의(X.1244) 표준을 개발하였으며, IP 멀티미디어 응용 스팸차단을 위한 프레임워크(X.fcsip) 표준초안을 개발중에 있다. 중국은 스팸차단을 위한 기술적인 전략(X.1231), e-mail 스팸차단을 위한 기술적인 프레임워크(X.1241)를 개발하였으며,



[그림 9] 스팸대응(Q.17) 표준 및 표준초안 간의 관계

상호연동이 가능한 스팸차단 게이트웨이 시스템(X.tsc-1)과 사용자 중심의 SMS 스팸 필터링 시스템을 개발 중에 있다. 또한, 향후 e-mail 스팸차단을 위한 기술적인 방법(X.tcs)을 개발할 계획에 있다. 다음의 [그림 9]는 Q.17에서 제정된 표준과 개발중에 있는 표준초안들 간에 관계를 정의하고 있다.

2.8. 아이덴티티(Identity) 관리(FG-IdM) 활동^[2-7]

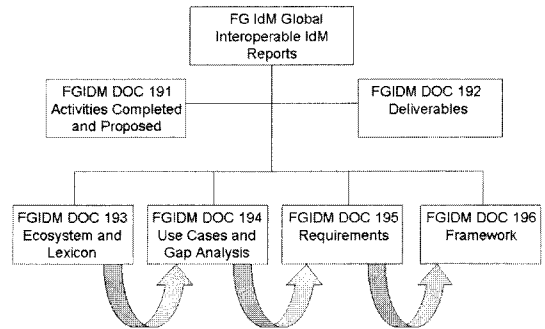
2006년 12월에 SG17 산하에 신설되어 2007년 9월 까지 활동하고 종료한 FG-IdM 그룹은 이번 연구회기 동안 별도의 연구과제로 분리되지는 않았지만, ITU-T 내에서 중요한 토픽으로 다루어졌으므로, 본 절에서 간단하게 소개하고자 한다.

기존의 아이덴티티 관리 기술은 ISO/IEC JTC1 SC27, Liberty Alliance, OASIS, IETF, W3C, OMA 등 각각의 표준화기구들을 중심으로 개별적으로 표준개발 및 표준화가 진행되었다. 하지만 이들에 대한 표준이나 스펙이 서로 상이하여 상호운용성 등의 문제점들이 제기되었으며, ITU-T를 중심으로 이들의 문제점을 해결한 전 세계적인 단일 국제표준으로 글로벌한 아이덴티티 관리 표준을 개발하자는 목적으로 FG-IdM 그룹이 신설되었다. FG-IdM의 주요 연구범위는 디지털 아이덴티티 관리, 신뢰성 성립, 개인정보보호, 네트워크나 서비스 등에서의 접근제어 관리, 온라인상에서의 신뢰성 구축 등에 대한 국제표준을 개발하는 임무이다.

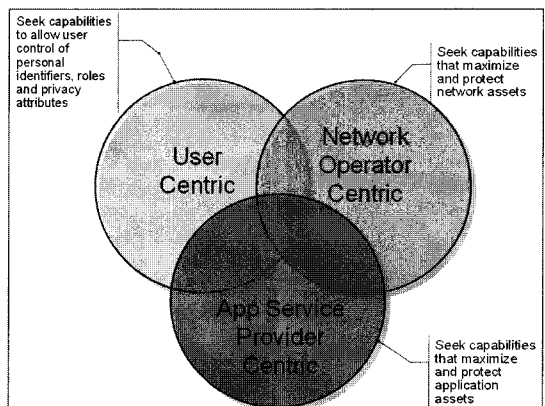
FG-IdM 그룹은 표준분석 및 용어정의 그룹, 활용사례(Use case) 분석 그룹, 요구사항정의 그룹, 프레임워크 그룹 등 산하 4개의 그룹을 구성하여 총 6회에 걸쳐 대면회의를 진행하였으며, 연구결과물로 [그림 10]과 같이 총 6건의 연구 결과보고서를 산출하였다.

첫 번째 결과보고서(DOC 191)는 FG-IdM 활동에 대한 보고서로 총 6회에 걸쳐 개최되었던, 회의문서들의 현황 및 회의록들의 요약을 정의하였다. 두 번째 결과보고서(DOC 192)는 FG-IdM 활동 결과 산출물들에 대한 현황 리포트이며, 세 번째 결과보고서(DOC 193)는 아이덴티티 관리와 관련된 포럼들의 분석 및 용어정의, 네 번째 결과보고서(DOC 194)는 아이덴티티 관리를 위한 활용사례 및 격차(Gap) 분석, 다섯 번째 결과보고서(DOC 195)는 글로벌한 아이덴티티 상호운용성을 위한 요구사항 정의, 여섯 번째 결과보고서(DOC 196)는 글로벌한 상호운용성을 위한 아이덴티티 관리 프레임워크이다. 본 결과물들에 대한 표준화 작업은 Q.6에서 진행 중에 있으며, 요구사항정의, 데이터모델, 상호교환 프레임워크 등이 빠르면 2008년 내에 ITU-T 국제표준으로 제정될 예정이다.

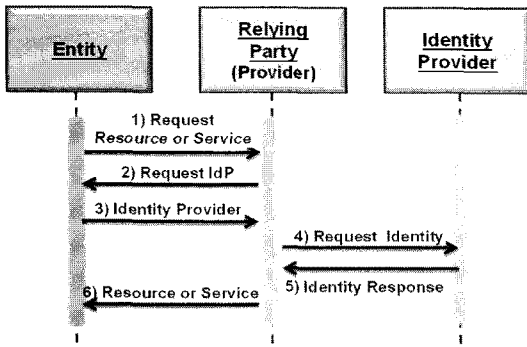
ITU-T 내에서 추구하고 있는 아이덴티티 연구 방향은 [그림 11]과 같다. 현재까지는 아이덴티티 연구 및



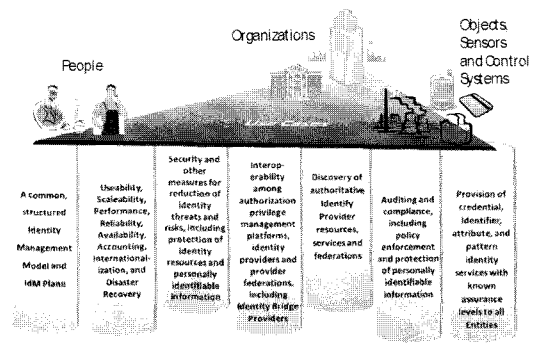
[그림 10] FG-IdM 결과물들의 관계 (DOC-No. : FG-IdM 그룹의 회의 문서 번호)



[그림 11] ITU-T 아이덴티티 연구 방향



(그림 12) 기본(Basic) IdM 구조(운영) 모델



(그림 13) 아이덴티티 관리 요구사항 - 7가지 그룹

표준화 활동이 시장 수요 및 산업체 특성에 따라 크게 사용자 중심, 네트워크 운영자 중심, 응용서비스 제공자 중심으로 진행되었지만, 이들을 간에 상호운용성, 글로벌한 프레임워크 및 기반구조 개발을 위해 3개의 영역이 충족되는 방향으로 국제표준을 개발하려고 하고 있다.

FG-IdM 그룹에서 아이덴티티 관리를 위한 기본적인 아이덴티티 구조(운영) 모델로 [그림 12]와 같은 결과를 도출하였다. 본 모델은 일반적인 네트워크 환경과 NGN, IPTV 환경 등에서 적용 가능하고, 앞서 언급한 사용자, 네트워크 운영자, 응용서비스 제공자가 모두 충족되는 모델이라고 정의하고 있다.

기본 IdM 구조(운영) 모델은 크게 사용자나 서비스를 이용하고자 하는 엔티티 그룹과 이들에게 서비스를 제공하고자 하는 산업체나 엔티티들을 관리하고자 하는 네트워크 운영자 그룹인 중계 그룹들이 있다. 또한 이들 그룹에 대한 신뢰성 및 보안 정책에 따라 아이덴티티 정보를 보장할 수 있는 그룹으로 구성된다. 상기 모델의 기본적인 운영절차는 다음과 같다.

- (1) 엔티티가 필요한 서비스를 제공자에게 요청
- (2) 제공자는 엔티티의 식별을 위해 아이덴티티 정보를 요청
- (3) 엔티티가 자신의 아이덴티티 정보를 제공자에게 회신
- (4) 제공자는 수신된 아이덴티티 정보를 아이덴티티 서비스 제공자에게 송부하여 해당 엔티티의 신뢰성 검증을 요청
- (5) 아이덴티티 서비스 제공자는 해당 정보에 대한 신뢰성 검증 결과를 서비스 제공자에게 회신
- (6) 회신 결과에 따라, 아이덴티티 정보가 올바른 경우 서비스 제공

FG-IdM 그룹에서 글로벌한 상호운용성 보장을 위해 정의한 아이덴티티 관리를 위한 7가지 요구사항들을 [그림 13]과 같이 정의하였다. 첫 번째 요구사항에서는 공통되고 구조화된 아이덴티티 관리 모델과 이들에 대한 평면에 대한 것으로 사용자, 서비스제공자, 아이덴티티 서비스 제공자 간에 요구되는 모델 및 요구사항들을 정의하고 있다. 두 번째 요구사항에서는 모든 엔티티들을 관리하거나 아이덴티티 모델에서 서비스되기 위한 공통된 요구사항으로 클리덴셜, 식별자, 속성, 패턴 아이덴티티 서비스를 정의하고 있다. 세 번째 요구사항에서는 아이덴티티 서비스 제공자가 해당 자원이거나 서비스, 관련 그룹 간에 해당 정보들의 권한을 자동으로 발견하고 서비스하기 위한 요구사항들을 정의하고 있다. 네 번째 요구사항은 아이덴티티 서비스 제공자와 유관 서비스 제공자 및 중계 서비스 제공자 간에 상호운용성 보장을 위한 권한부여에 대한 정책에 대한 요구사항이다. 이는 앞에서 정의한 모든 엔티티들의 구성 요소들에 대한 신뢰성 보장 및 관리를 위해 필요한 사항이다. 다섯 번째 요구사항에서는 개인 아이덴티티 정보나 아이덴티티 자원들에 대한 보호, 아이덴티티 자체에 대한 위협 및 위험을 감소시키기 위한 해결방법 및 보안과 관련된 요구사항들을 정의하고 있다. 여섯 번째 요구사항에서는 개인 아이덴티티 정보에 대한 보호를 위해 요구되는 보안정책, 감사, 승인절차에 대해 정의하고 있다. 일곱 번째 요구사항에서는 아이덴티티 관리에 대한 활용성, 확장성, 성능, 확실성, 유용성, 국제성, 재난복구에 적용하기 위한 요구사항들을 정의하고 있다.

FG-IdM 그룹에서 정의한 아이덴티티 관리 프레임워크는 앞서 설명한 7가지 요구사항들을 충족하면서 아이덴티티에 대한 생명주기(Life-cycle), 아이덴티티의 선택/분배/등록, 아이덴티티 속성에 따른 바인딩 방법, 아

이덴터티 인증서, 아이덴터티 변경, 아이덴터티로부터 속성정보들의 언 바인딩 방법, 아이덴터티 폐지, 아이덴터티의 데이터 모델, 아이덴터티 구성 간에 관계, 기타 특징(그룹 간, 조직 내 규칙 등)들을 정의하고 있다. 아울러, 글로벌한 상호운용성 보장을 위한 아이덴터티 관리를 위한 컴포넌트들에 대한 정의와 해당 컴포넌트들의 서비스 정의들을 포함하고 있다.

현재 FG-IdM 그룹은 2007년 9월, SG17 회의에서 주요활동 결과물들을 보고하고 활동을 종료하였으며, 향후 추가적인 연구를 위해 JCA-IdM(Joint Coordination Activity for Identity Management) 그룹과 IdM-GSI(Identity Management Global Standards Initiative) 그룹을 신설하여 운영되고 있다^[26].

III. 차기 연구회기('09~'12) 구조조정 방향^[10,14]

최근에 개최된 ITU-T SG17 회의에서 가장 중요하게 다루어졌던 토픽은 차기 연구회기 동안의 구조조정 방향에 대한 논의이다. 한국은 보안 분야의 표준화 영역을 보다 확대하기 위하여, 2007년 9월, SG17 회의와 2007년 12월, SG17 WP2 회의에 한국의 조율된 의견을 제안한 바 있으며, 2008년 4월, 최종 구조조정 회의에서도 본 이슈에 대해 적극적으로 대응하였다^[11-13].

한국의 주요 대응 사항은 다음과 같은 2개의 이슈를 독립적인 신규 연구과제로 신설을 제안했고 이에 대한 중요성을 인정받았으나, 표준화 추진의 효율화를 위해 기존 연구과제 6과 연구과제 9에서 추진하기로 결정하였다.

- 기술적인 방법에 의한 사이버공격 추적 : IT 포렌식 기술, IP 역추적 기술, 사이버범죄 대응기술 등
- 새로운 응용을 위한 디지털미디어보호기술 : DRM 기술, 디지털콘텐츠 보호기술 등

또한, 바이오인식(Q.8) 분야의 연구범위 조정과 안전한 통신서비스(Q.9)를 2개의 연구과제로 분리될 수 있도록 대응하였으며, 결과적으로 한국에서 유독한 방향으로 구조조정이 확정되었다.

2008년 4월, ITU-T SG17 회의 결과를 바탕으로 확정된 차기 연구회기 구조조정 방향은 다음의 [표 1]과 같다. 주요 특이사항으로는 언어 부분에 있던 ASN.1 연구과제(Q.A)가 보안 그룹으로 재그룹핑 되었으며, 아

이덴터티 관리(Q.L) 그룹과 SOA 기반의 웹서비스 보안을 연구하기 위한 연구과제(Q.T)가 신설되었다.

IV. 표준화추진 전략 및 고려사항^[19,24,25]

ITU-T SG17 활동에 있어 고려되어야 할 사항으로 첫 번째는 한국 참가자들은 주로 학계 및 연구소에서 참석하고 있어, 실제 산업체에서 개발되어 활용되고 있는 실용기술의 국제 표준 반영을 적극 권장할 필요가 있다. 따라서 국내 산업체에서 국제표준화 활동에 적극적으로 참여할 수 있는 방법과 예산적인 지원 방법을 모색해야 할 시점이다. 또한, 산업체에서도 국내 정보보호 시장만을 대상으로 두지 말고, 국내 고유기술 및 정보보호 제품을 국제시장으로 확산할 수 있는 글로벌한 경영 관점을 가져야만 한다. 두 번째는 국제표준 제정기간은 보통 제안에서부터 국제표준 제정까지 2~3년 정도가 소요되나, 해당 표준초안과 연계되고 있는 국제과제(표준화과제, R&D)들이 계획 보다 빠르게 종료되거나 없어지는 경우가 발생한다. 따라서 장시간 소요되는 국제표준화 활동을 지원할 수 있도록 표준화 과제 신규 발굴 시, 기존 연구과제와 연계할 수 있는 방안이 고려되어야 한다. 또한, 학계에서도 SCI 등의 연구논문과 동일하게 국제표준화 활동에 제출되고 있는 기고서 등의 실적들을 연구 평가 시, 핵심 평가 항목에 반영될 수 있도록 고려하는 것이 필요하다. 세 번째로는 ITU-T SG17 이번 연구회기가 2008년 9월, 회의를 마지막으로 종료됨으로 한국 주도로 개발되고 있는 표준초안들 중에 완성도가 높은 표준초안들은 가능한 이번 연구회기 동안에 최종 국제표준이 제정될 수 있도록 노력해야 된다. 이와 더불어 차기 연구회기를 위한 신규 표준화 아이템 발굴과 신규로 신설되는 연구과제들을 대응할 수 있는 국내 표준화 전문가들을 사전에 확보하는 것이 필요하다. 네 번째로는 한국 주도로 개발되고 있는 홈네트 워크 보안, USN 보안, RFID 보안, 멀티캐스트 보안 분야 등은 계속해서 우위를 확보할 수 있도록 노력해야 하고, 신규로 추가 가능한 분야를 발굴하여 활동 영역을 확대해야 된다. 다섯 번째로는 ITU-T 내에 중요하게 다루어지고 있으며, 여러 나라에서 관심을 가지고 있는 신규 분야인 아이덴터티 관리, IPTV 보안 등에 국내 고유기술들을 적극적으로 제안해야하고 관련 국제표준 문서들을 분석하여, 국내표준과 국제표준 간에 이해격차를 해소하는 것이 필요하다.

[표 1] ITU-T SG17 차기 연구회기('09~'12) 구조조정 방향

구조조정 그룹명	연구 과제	제 목	연구범위 및 주요업무	비 고 (계속/신규)
Block 17 - A (보안그룹)	A/17	Abstract Syntax Notation One (ASN.1), Object Identifiers (OIDs) and Associated Registration	· ITU-T 내에 ASN.1 리드 그룹으로 다른 SG들의 업무 협조, 특히, 기 제정된 ITU-T 국제표준 내에 정의된 ANS.1에 대한 XML 스키마로 정의 객체 식별자(OIDs)들의 등록방법과 이들에 대한 구현과 관련된 표준 개발	계속 (Q.10)
	D/17	Directory Services, Directory Systems, and Public-key/Attribute Certificates	· 디렉토리 관련 X.500-series 표준들의 유지보수 · X.500, X.509 표준과 IETF 사실표준과의 연계 작업 · X.500-series 표준들을 새로운 IdM, NGN, USN 등으로의 확장	계속 (Q.2)
	E/17	Open Systems Interconnection (OSI)	· ITU-T OSI 관련 표준들의 유지보수 · OSI 참조모델을 기반으로 구현하고자 하는 사용자들 위한 가이드라인 표준 개발	계속 (Q.3)
	I/17	Telecommunications Systems Security Project	· ITU-T 내에 보안 관련된 문제들의 역할 조율 · 보안 로드맵, 요약물, 핸드북, 메뉴얼 등의 유지보수 · ITU-T 보안 표준들 간에 격차(Gap) 해결 업무	계속 (Q.4)
	J/17	Security Architecture and Framework	· 정보통신 환경을 고려한 보안솔루션에 대한 표준 개발 · 새로운 보안기술에 적합한 보안 구조 개발 · X.800-series, X.103x-series 표준들의 유지보수	계속 (Q.5)
	K/17	Cybersecurity	· 디지털 포렌식, 역추적 기술에 대한 표준 개발 · 사이버공격에 대응하기 위한 정보교환 및 협력방법 표준 개발 · 사이버공간에서 활용되는 개인정보나 개인 식별이 가능한 정보에 대한 보호기술 및 가이드라인 개발	계속 (Q.6, 일부)
	L/17	Identity Management Architecture and Mechanisms	· 아이덴티티 정보들의 생명주기 관리가 가능한 아이덴티티 프레임워크 표준 개발 · 아이덴티티 시스템들 간에 상호연동이 가능한 구조, 기능, 인터페이스 관련 표준 개발 · 아이덴티티를 위한 공통적인 요구사항(메커니즘 등) 정의	계속 (Q.6, 일부)
	M/17	Telecommunications Information Security Management	· 자산 식별방법 및 보안정책 관리에 대한 표준 개발 · 중소기업, 전자정부 등에 활용 가능한 보안관리 표준 개발	계속(Q.7)
	N/17	Telebiometrics	· 정보통신 환경에 활용 가능한 바이오인식 응용기술 개발 · 바이오정보를 이용한 상호인증 및 보호기술 개발 · 바이오정보 응용에 따른 프라이버시 보호기술 개발	계속(Q.8)
	O/17	Security Aspects of Ubiquitous Telecommunication Services	· 유비쿼터스 환경을 위한 보안솔루션 표준 개발 · 다양한(홈네트워크, 모바일, NID, USN 등) 네트워크 환경에서의 보안 표준 개발	계속 (Q.9, 일부)
	P/17	Secure Application services	· 안전한 응용서비스를 위한 보안솔루션 표준 개발 · 웹서비스에 이용 가능한 TTP, P2P, SOA 등의 응용기술 표준 개발	계속 (Q.9, 일부)
Q/17	Countering Spam by Technical Means	· 스파이웨어, 웜, 피싱, 악성코드 등에 의해 발생하는 악성스팸에 대한 대응기술 및 표준개발	계속 (Q.17)	
T/17	Service Oriented Architecture Security	· 웹서비스를 지원하기 위한 SOA 기반의 구조, 서비스 시나리오, 보안 요구사항 등의 표준 개발	신규	
Block 17 - B (언어그룹)	B/17	Formal Languages and Telecommunication Software	· ITU-T 내에 제정된 모든 언어 표준들에 대한 유지보수 · 정보통신 시스템들의 형식(Formal) 언어(SDL, ChILL, ODP, UML)에 대한 표준개발 · UML 2.0 프로파일 개발 : ASN.1, MSC, TTCN, URN 관련	계속 (Q.11, 12, 13, 15)
	C/17	Testing Languages, Methodologies and Framework	· ITU-T 내에서 시험방법론에 대한 표준 유지보수 및 관련된 표준 개발 · TTCN-3(Testing and Test Control Notation Three) 개선 작업 · NGN 환경 및 상품제품(COTS)을 위한 시험방법론 표준 개발	계속 (Q.14)
Block 17 - C (멀티캐스트)	F/17	End-to-end Multicast	· X.60x-series 표준들의 시장수요를 반영한 유지보수 · Internet 및 NGN 환경에서 중단간 멀티캐스트 통신 표준 및 중단간 모바일 멀티캐스트 통신 표준 개발 · 스트림 서비스(IPTV, UCC)를 지원하기 위한 P2P 기술 기반의 멀티캐스트 표준 개발	계속 (Q.1)

※ H/17(Internationalized Domain Names(IDN)) : 차기 TSAG 회의('08.07월)에서 SG2로 이관에 대해 결정기로 함
 ※ G/17(Future Open System Communication Technology) : SG13 산하에 신설기로 한, Q.P/13 (Future Networks)과 통합하여 SG13에서 추진기로 함
 ※ R/17(Tracing Cyber Attack by Technical Means) : 사이버보안 관점에서 K/17과 통합기로 함
 ※ S/17(Digital Media Protection for New Applications) : 서비스보안 관점에서는 O/17과 통합하고 응용보안 관점에서는 P/17과 통합기로 함

ITU-T SG17 표준화 활동을 위한 추진전략으로 첫 번째는 차기 연구회기 구조조정에 따른 표준화 추진전략을 수립할 계획이다. 지난 연구회기에서는 보안 분야가 7개의 연구과제로 국제표준을 개발하였으나, 이번 연구회기부터는 총 13개의 연구과제로 확대되어, 보안 분야의 국제표준을 개발키로 한 바, 각 연구과제에 대한 국내 전문가들을 섭외하여, 지속적인 국제회의의 참석과 국내 TTA 표준화위원회 및 ITU-T SG17 분과위원회와 사전 조율을 통해 국제적인 표준화 방향에 발 빠른 대응과 한국이 우선적으로 선점이 가능한 아이тем들을 발굴해야 한다. 특히, 한국이 신규로 중점을 두고 있는 사이버범죄대응기술과 관련된 디지털 포렌식 기술, IP 역추적 기술 등과 산업체에서 관심을 가지고 있는 IPTV 보안, 아이덴티티 관리 기술 등에 중점을 둘 계획이다. 두 번째로는 한국 주도로 추진되고 있는 다수의 표준초안에 대한 신속한 국제표준화 추진을 위해 각 담당 에디터들과 해당 연구과제를 주재하고 있는 의장단 간에 협의할 수 있는 인적 인프라 구축에 힘쓸 예정이다. 즉, 국제표준화 활동은 기술적인 우위를 두고 국제표준을 개발하는 것도 중요하지만, 세계 각 국가들의 표준화 전문가들의 이해와 동의를 구하는 작업이 매우 중요하다. 따라서 각 담당 에디터들의 기술 개발에 앞서 인적 교류 활동을 위한 전략과 교육 등이 필요하다. 세 번째로는 한국 주도로 개발되고 있는 표준초안들의 완성도와 활용성 증가를 위해, 실제 산업체를 중심으로 구성되어 있는 포럼, TTA 표준화위원회와 지속적인 협력 방안을 마련하여, 산업체에서 요구되는 의견과 실제 상용화가 가능한 기술들을 국제표준에 반영될 수 있도록 추진할 계획이다. 네 번째로는 ITU-T에서 기 제정된 국제표준들과 개발중에 있는 표준초안들을 체계적으로 검토하여, 국내표준으로 수용 유/무에 대한 검토와 적절시기, 방법 등을 강구할 계획이다. 현재 고려되고 있는 방법은 2007년부터 수행하고 있는 방법으로 SG17 분과위원회를 중심으로 매년 일정부분의 국제표준과 표준초안들을 일차적으로 검토한 후, 검토 결과를 해당 TTA 표준화 위원회에 회람하거나 재검토를 의뢰하여, 적절한 시기에 국내표준으로 수용하거나 추가적인 국제표준 수정 제안을 계획하고 있다. 한국 주도로 개발되고 있는 국제표준초안들은 각 에디터가 책임지고 국내표준 제정까지 활동해 줄 것을 권고하고 있다. 다섯 번째로는 차기 연구회기를 이끌어 나갈 의장단석을 추가적으로 확보할 계획이다. 지난 연구회기에서 확보하고 있는 Q.7(부라

포처), Q.8(라포처), Q.9(라포처) 의장단석들은 계속해서 유지할 수 있도록 노력할 계획이며, 구조조정에 따른 신규 연구과제들은 아직까지 국제적으로 다양한 전문가들이 확보되어 있지 않으므로, 국내에서 해당 전문가들을 사전에 섭외하여, 시작하는 시점부터 적시에 대응할 수 있도록 추진할 계획이다. 여섯 번째로는 한중일 간에 협력할 수 있는 인프라를 구축하는 전략이다. ITU-T 내에 정보보호 분야는 아시아 지역에서 많은 국제표준들을 개발하고 있어, 상호 간에 협력할 수 있는 방안과 북미 및 유럽 등에 공동으로 대응할 수 있는 전략이 수립되어야 한다. 현재 활동하고 있는 ASTAP, RAISE 포럼, CJK SWIS 등에 한국에서 적극적인 참여와 좋은 결과물, 협력 방안들을 지속적으로 제출하여 ITU-T SG17 국제회의의 활동에 구심점을 마련할 계획이다. 참고로 2007년부터 한중일 3국간에 정보보호 표준화 워크숍이 시작되었고, 이를 통한 한중일 차원의 정보보호 협력을 위한 활동을 강화할 필요가 있다. 일곱 번째로는 ITU-T SG17 분과위원회의 활동을 강화하는 전략이다. 현재 SG17 분과위원회는 ITU-T 내에 보안 분야에 중점을 두고 국내에서 리더 그룹으로 활동하고 있는 바, ITU-T SG17에 제출되고 있는 기고서(국가/섹터)들의 심의를 강화하여, 진수 위주보다는 질적으로 향상될 수 있도록 노력할 계획이다. 또한, 차기 연구회기에 적극적으로 대응할 수 있도록 신규 전문가 확보 방안 모색과 국내 정보보호 분야에서 활동하고 있는 전문가들을 대상으로 이번 연구회기 동안의 주요 결과물들에 대한 교육과 전파를 위한 워크숍 및 세미나 등을 개최할 예정이다.

V. 결 론

본 논문에서는 ITU-T SG17 정보보호 분야에 대한 국제표준화 동향 및 향후 활동을 위한 고려사항과 대응 전략을 살펴보았다. 현재, ITU-T 내에서 정보보호 분야는 매우 중요한 분야로 각광 받고 있는 시점이며, 한국도 이번 연구회기 동안 많은 인적 인프라 구축과 다수의 국제표준들을 개발하는 성과를 이루어, SG17 내에 국제표준을 개발하기 위한 좋은 발판을 마련하였다.

현재 한국은 이런 실적들을 바탕으로 지속적인 활동 강화와 다른 국가들과의 경쟁에서 이길 수 있는 전략이 요구되는 시점이다. 또한, 부록으로 이번 연구회기 동안 제정된 국제표준과 표준초안들의 현황을 기술한다.

참고문헌

- [1] Mr. Herbert Bertine, “GSC-13-GTSC6-05 : ITU - Security/Cybersecurity”, GSC-13 Meeting, USA Boston, 14-17 July 2008.
- [2] ITU-T SG17, “TD0292r1 : FG-IdM - Report on Activities Completed and Proposed”, Swiss Geneva, 19-28 September 2007.
- [3] ITU-T SG17, “TD0293 : FG-IdM - Report on Overview of Deliverables”, Swiss Geneva, 19-28 September 2007.
- [4] ITU-T SG17, “TD0294 : FG-IdM - Report on Identity Management Ecosystem and Lexicon”, Swiss Geneva, 19-28 September 2007.
- [5] ITU-T SG17, “TD0295 : FG-IdM - Report on Identity Management Use Cases and Gap Analysis”, Swiss Geneva, 19-28 September 2007.
- [6] ITU-T SG17, “TD0296 : FG-IdM - Report on Requirements for Global Interoperable Identity Management”, Swiss Geneva, 19-28 September 2007.
- [7] ITU-T SG17, “TD0297 : FG-IdM - Report on Identity Management Framework for Global Interoperability”, Swiss Geneva, 19-28 September 2007.
- [8] ITU-T SG17, “TD4090 Rev.1 : Report of Working Party 2/17, Telecommunication Security”, Swiss Geneva, 7-18 April 2008.
- [9] ITU-T SG17, “TD0409Rev.1 : Draft Study Group 17 Report to WTSA 08 : Part 1 - General”, Swiss Geneva, 7-18 April 2008.
- [10] ITU-T SG17, “TD0410Rev.2 : Draft SG17 Report to WTSA 08 : Part 2 - Questions proposed for study during the next study period (2009-2012)”, Swiss Geneva, 7-18 April 2008.
- [11] Byoung-Moon Chin, Heung-Ryong Oh, Heung-Youl Youm, Shin-Gak Kang, “COM17-C188 : Considerations for the restructure issue in the next Study Period(2009-2012)”, ITU-T SG17 Meeting, Geneva Swiss, 19-28 September 2007.
- [12] Heung-Youl Youm, Byoung-Moon Chin, Jaehoon Nah, Heung-Ryong Oh, “COM17-C254 : Revised Text for New Question on Digital Media Protection”, ITU-T SG17 WP2 Meeting, Geneva Swiss, 10-14 December 2007.
- [13] Heung-Youl Youm, Byoung-Moon Chin, Jong-Hyun Kim, “COM17-C249 : Proposed text for new Question on countering cyber attack by technical means”, ITU-T SG17 WP2 Meeting, Geneva Swiss, 10-14 December 2007.
- [14] 진병문, 오홍룡, 염홍열, 강신각, “ITU-T SG17 국제표준화 회의 참가보고(제네바)”, TTA Journal, 제117호, pp159-165, 2008.06.
- [15] 진병문, 오홍룡, 염홍열, 강신각, “ITU-T SG17 국제표준화 회의 참가보고(제네바)”, TTA Journal, 제113호, pp116-120, 2007.10.
- [16] 진병문, 오홍룡, 염홍열, 강신각, “2007년 ITU 국제표준화 활동보고서 : 개방형통신기술, 보안, 언어/소프트웨어 분야(SG17)”, MIC, 제14호, 전파연구소, pp186-201, 2007.12.
- [17] 진병문, 오홍룡, 염홍열, 강신각, “ITU 연구동향 : ITU-T SG17 분야”, MIC, 통권 제13호, 한국ITU 연구위원회, pp317-337, 2006.11.
- [18] 진병문, 오홍룡, 염홍열, 강신각, “2005년도 ITU-T 연구활동 보고서 : ITU-T SG17 연구동향”, TTA, pp216-254, 2005.12.
- [19] 오홍룡, 염홍열, “정보보호 국제표준화 동향 및 향후 전망”, 한국정보보호학회 학회지, 제17권 제6호, pp93-105, 2007.12.
- [20] 오홍룡, 염홍열, “안전한 통신 서비스 표준화 동향 및 향후전망”, 한국정보보호학회 학회지, 제17권 제1호, pp63-78, 2007.02.
- [21] 오홍룡, 염홍열, “ITU-T SG17 홈네트워크 보안 표준화 동향 및 향후전망”, 한국정보보호학회 학회지, 제16권 제6호, pp9-18, 2006.12.
- [22] 오홍룡, 오세순, 김선, 염홍열, “정보보호 표준화 항목 정의 및 로드맵”, 한국정보보호학회 학회지, 제15권 제5호, pp67-82, 2005.10.
- [23] 염홍열, “ID 관리 표준화 동향 및 향후 추진방향”, TTA, IT Standard Weekly, 2007.05.
- [24] 염홍열, “정보보호일반 표준화 로드맵(v2004- 2007)”, TTA, 2003. 12 - 2006. 12.
- [25] 이석래, 진승현, 원유재, 나재훈, 김재성 외 33인, “정보통신 중점기술 표준화로드맵(v2008) : 지식·정보보호 분야”, TTA, 2007. 12.
- [26] ITU 홈페이지, <http://www.itu.int>

〈著者紹介〉



오홍룡 (Heung-Ryong Oh)

정회원

2002년 2월 : 순천향대학교 전자공학과 졸업
 2004년 2월 : 순천향대학교 정보보호학과 석사
 2007년 6월 : 순천향대학교 정보보호학과 박사 수료
 2004년 2월 ~ 현재 : 한국정보통신기술협회 표준화본부
 2004년 11월 ~ 2007년 2월 : ITU-T X.1111 국제표준 Associate Editor
 2005년 3월 ~ 현재 : ITU-T SG17 국내 분과위원회 간사
 <관심분야> 보안프로토콜, 정보보호표준



진병문 (Byoung-Moon Chin)

정회원

1976년 2월 : 서울대학교 전기공학 학과 졸업
 1983년 2월 : 서울대학교 전자계산기공학과 석사
 1996년 2월 : KAIST 전산학과 박사
 1977년 ~ 1980년 : 대우전자 개발실 근무
 1980년 ~ 2001년 : 한국전자통신연구원 책임연구원 근무
 2001년 ~ 현재 : 한국정보통신기술협회 표준화본부 본부장
 2005년 3월 ~ 현재 : ITU-T SG17 Vice-Chairman
 2005년 3월 ~ 현재 : ITU-T SG17 WP1 Chairman
 2005년 3월 ~ 현재 : ITU-T SG17 국내 분과위원회 의장
 <관심분야> 개방형통신기술, 정보보호표준



염홍열 (Heung-Youl Youm)

종신회원

1981년 2월 : 한양대학교 전자공학과 졸업
 1983년 9월 : 한양대학교 전자공학과 석사
 1990년 2월 : 한양대학교 전자공학과 박사
 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 산학연전소시업센터 소장
 1997년 3월 ~ 현재 : 한국통신정보보호학회 총무이사, 학술이사, 교육이사, (현)논문지편집위원장, (현)상임부회장
 2003년 9월 ~ 2004년 3월 : ITU-T SG17/Q10 Associate Rapporteur
 2004년 3월 ~ 현재 : ITU-T SG17/Q9 Rapporteur
 2005년 3월 ~ 현재 : ITU-T SG17 국내 분과위원회 부의장
 2006년 11월 ~ 2008년 2월 : 정보통신부 정책자문단 정보보호 PM
 2006년 11월 ~ 현재 : HITA 정보보호 PM
 <관심분야> 네트워크 보안, IPTV 보안, USN 보안, 홈네트워크 보안, 응용보안



강신각 (Shin-Gak Kang)

정회원

1984년 2월 : 충남대학교 전자공학과 졸업
 1987년 2월 : 충남대학교 전자공학과 석사
 1998년 2월 : 충남대학교 전자공학과 박사
 1995년 12월 : 정보통신기술사
 1997년 ~ 현재 : ITU-T SG17 Q.1 Rapporteur
 2000년 ~ 현재 : VoIP포럼 부의장
 2005년 3월 ~ 현재 : ITU-T SG17 국내 분과위원회 부의장
 2008년 3월 ~ 현재 : 과학기술연합대학원대학교 겸임교수
 1984년 3월 ~ 현재 : 한국전자통신연구원 표준연구센터 팀장
 <관심분야> VoIP, 멀티캐스트, 인터넷보안, IPTV, 미래인터넷

{부록 표 1} ITU-T SG17 Telecommunication 보안 분야 국제표준 제정 현황(총 36건)

No.	국제표준번호	연구과제	제정시기	국제표준명(제목)	제안 국가	국내표준
1	X.1031	Q.5	2008-03	Security architecture aspects of end users and networks in telecommunications	러시아	X
2	X.1034	Q.5	2008-04	Guideline on Extensible Authentication Protocol based Authentication and Key Management in a Data Communication Network	한국 (엄홍열)	X
3	X.1035	Q.5	2007-02	Password-authenticated key exchange (PAK) protocol	미국	X
4	X.1036	Q.5	2007-11	Framework for creation, storage, distribution and enforcement of policies for network security	한국 (김중현)	TTAE.IT-X1036
5	X.1051/R1	Q.7	2008-02	Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	일본	TTAS.KO-12.0036
6	X.1081	Q.8	2004-04	The telebiometric multimodal model - A framework for the specification of security and safety aspects of telebiometrics	스위스	X
7	X.1082	Q.8	2007-11	Telebiometrics related to human physiology	스위스	X
8	X.1083	Q.8	2007-11	Information technology - Biometrics - BioAPI interworking protocol	프랑스	X
9	X.1084	Q.8	2008-05	Telebiometrics system mechanism - Part 1 : General biometric authentication protocol and system model profiles for telecommunications systems	일본/ 한국 (신용녀)	X
10	X.1088	Q.8	2008-05	Telebiometrics digital key framework (TDK) - A framework for biometric digital key generation and protection	한국 (이형우)	2006-003 추진중
11	X.1089	Q.8	2008-05	Telebiometrics authentication infrastructure (TAI)	중국	X
12	X.1111	Q.9	2007-02	Framework for security technologies for home network	한국 (엄홍열, 오홍룡)	TTAE.IT-X1111
13	X.1112	Q.9	2007-11	Device certificate profile for the home network	한국 (백중현)	TTAS.KO-12.0052
14	X.1113	Q.9	2007-11	Guideline on user authentication mechanisms for home network services	한국 (이형규)	TTAS.KO-12.0030
15	X.1121	Q.9	2004-04	Framework of security technologies for mobile end-to-end data communications	한국/ 일본	X
16	X.1122	Q.9	2004-04	Guideline for implementing secure mobile systems based on PKI	한국/ 일본	X
17	X.1123	Q.9	2007-11	Differentiated security service for secure mobile end-to-end data communication	중국	X
18	X.1124	Q.9	2007-11	Authentication architecture for mobile end-to-end data communication	중국	X
19	X.1125	Q.9	2008-01	Correlative reacting system in mobile data communication	중국	X
20	X.1141	Q.9	2006-06	Security Assertion Markup Language (SAML 2.0)	캐나다	TTAS.IT-X1141_1 ~ 6
21	X.1142	Q.9	2006-06	eXtensible Access Control Markup Language (XACML 2.0)	캐나다	TTAS.OT-10.0040/R1
22	X.1143	Q.9	2007-11	Security architecture for message security in mobile web services	한국 (이재승)	2008-760 추진중

(부록 표 1) ITU-T SG17 Telecommunication 보안 분야 국제표준 제정 현황(총 36건)-계속

No.	국제표준번호	연구과제	제정시기	국제표준명(제목)	제안 국가	국내표준
23	X.1151	Q.9	2007-11	Guideline on secure password-based authentication protocol with key exchange	한국 (염홍열)	X
24	X.1152	Q.9	2008-05	Secure end-to-end data communication techniques using trusted third party services	일본	X
25	X.1161	Q.9	2008-05	Framework for secure peer-to-peer communications	일본	X
26	X.1162	Q.9	2008-05	Security architecture and operations for peer-to-peer network	한국 (나재훈)	2008-754 추진중
27	X.1205	Q.6	2008-04	Overview of cybersecurity	캐나다	X
28	X.1206	Q.6	2008-04	A vendor-neutral framework for automatic notification of security related information and dissemination of updates	일본	과제 제안 예정
29	X.1207	Q.6	2008-04	Guidelines for telecommunication service providers for addressing the risk of spyware and potentially unwanted software	싱가폴	X
30	X.1231	Q.17	2008-04	Technical strategies on countering spam	중국	X
31	X.1240	Q.17	2008-04	Technologies involved in countering e-mail spam	한국 (강신각, 박소영)	X
32	X.1241	Q.17	2008-04	Technical framework for countering e-mail spam	중국	X
33	X.1303	Q.6	2007-09	Common alerting protocol (CAP 1.1)	캐나다	X
34	X.1171 (draft)	Q.9	2008-09	Framework for protection of personally identifiable information in networked ID services	한국 (최두호)	TTAS.KO-06.0146
35	X.1244 (draft)	Q.17	2008-09	Overall aspects of IP multimedia application spam	한국 (강신각)	X
36	X.1250 (draft)	Q.6	2008-09	Requirements for global identity management trust and interoperability	미국	2008-669 추진중

(부록 표 2) 2008년, ITU-T SG17에서 개발되고 있는 표준초안 현황(총 34건)

No.	표준초안번호	연구과제	제정시기	국제표준명(제목)	제안 국가	국내표준
1	X.603.1/Amd. 1	.Q.1/ Q.9	2009-03	Information technology - Relayed multicast protocol : Specification for simplex group applications - Amendment 1 : Security extensions	한국 (윤미연)	2008-748 추진중
2	X.eaa	Q.6	2009-12	Information technology - Entity authentication assurance	미국	X
3	X.gopw	Q.6	2008-11	Guideline on preventing worm spreading in a data communication network	한국 (김미주, 염홍열)	X
4	X.idif	Q.6	2009-02	User control enhanced digital identity interchange framework	한국 (조상래)	2008-737 추진중
5	X.idm SerSup	Q.6	2009-02	Supplement to X-series Recommendations on identity management : Identity management lexicon	영국	X
6	X.idm-dm	Q.6	2009-02	Common identity data model	미국	2008-668 추진중
7	X.idmf	Q.6	2009-02	Identity management framework	캐나다	X
8	X.idmgap	Q.6	2009-02	Identity management use cases and gap analysis	미국	X
9	X.idmint	Q.6	2009-12	Global interoperable IdM framework	미국	X
10	X.idms	Q.6	2009-02	Identity management security	캐나다	X

(부록 표 2) 2008년, ITU-T SG17에서 개발되고 있는 표준초안 현황(총 34건)-계속

No.	표준초안번호	연구과제	제정시기	국제표준명(제목)	제안 국가	국내표준
11	X.nsmf	Q.6/ Q.7	2008-11	Network security management framework (NSMF)	중국	X
12	X.rfpg	Q.6	2008-11	Privacy guideline for RFID	한국 (이향진)	TTAS.KO-06.0111
13	X.sisfreq	Q.6	2008-11	Requirements for security information sharing framework	한국 (정일안)	2007-405 추진중
14	X.soaf	Q.6	2009-12	Service oriented architecture framework	캐나다	X
15	X.soas	Q.6	2009-12	Service oriented architecture security	캐나다	X
16	X.tb-ucr	Q.6	2009-12	Trace back use case and requirements	중국, 미국, 한국 (염홍열)	2008-741, 2008-742 추진중
17	X.ismf	Q.7	2009-12	Network Security Management Framework	중국	X
18	X.rmg	Q.7	2008-11	Risk management and risk profile guide	영국, 한국 (정태인)	X
19	X.sim	Q.7	2008-11	Security incident management guidelines for telecommunications	한국 (김정덕)	X
20	X.ott	Q.8	2011-12	Authentication Framework with One-time Telebiometric Template	한국 (이형우)	2007-1041 추진중
21	X.th	Q.8	2010-12	Telebiometrics related to TeleHealth and the World-Wide TeleMedicines (and related thresholds)	스위스	X
22	X.tif	Q.8	2011-12	Integrated framework for telebiometric data protection in telehealth and worldwide telemedicine	한국 (신용녀)	X
23	X.tpp-1	Q.8	2008-11	Telebiometrics protection procedure - Part 1 : A guideline to technical and managerial countermeasures for biometric data security	한국 (김재성, 김학일)	TTAS.KO-12.0034
24	X.tpp-2	Q.8	2008-11	Telebiometrics protection procedure- Part 2 : A guideline for Data protection in Multibiometric Systems	한국 (길연희)	TTAS.KO-12.0050
25	X.tsm-2	Q.8	2008-11	Telebiometrics system mechanism - Protection profile for client terminals	일본, 한국 (신용녀)	X
26	X.homesec-4	Q.9	2008-11	Authorization framework for home network	한국 (김진우)	X
27	X.iptvsec-1	Q.9	2008-11	Functional requirements and architecture for IPTV security aspects	중국, 한국 (염홍열), 미국, 일본	X
28	X.iptvsec-2	Q.9	2010-12	Requirement and mechanism for secure transcodable scheme of IPTV	한국 (나재훈)	2008-755 추진중
29	X.iptvsec-3	Q.9	2010-12	Key management framework for secure IPTV communication	한국 (염홍열)	X
30	X.mcsec-1	Q.9	2010-12	Security requirements and framework in multicast communication	한국 (윤미연, 염홍열)	2008-747 추진중
31	X.usnsec-1	Q.9	2010-12	Security framework for ubiquitous sensor network	한국 (염홍열, 김현)	X
32	X.fcsip	Q.17	2009-02	Technical framework for countering IP multimedia spam	한국 (김성혜, 조영덕)	X
33	X.ssf	Q.17	2009-12	SMS spam filtering system based on users' rules	중국	X
34	X.tcs-1	Q.17	2009-02	Interactive countering spam gateway system	중국	X