情 報 保 護 學 會 誌
第17卷 第6號, 2007. 12

정보보호 국제표준화 동향 및 향후 전망

오흥룡*, 염흥열**

요 약

정보보호 분야의 국제표준화는 각 기술들의 특성 및 사용자들의 관점 등을 고려하여, 다양한 국제표준화기구에서 국제표준개발 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 원천기술들에 대한 국제표준화와 IETF Security Area에서는 인터넷 서비스의 품질 보장 및 향상된 인터넷 환경 구축을 위해 실제적인 구현 관점에서 국제표준화를 추진하고 있다. 또한, 아시아 지역에서는 각 국가 간에 정보보호 표준화 활동에 대한 정보공유 및 국제표준화 기구들에 대한 공동 대응을 위해 ASTAP, RAISS 포럼, CJK SWIS 등의 소규모 표준화 활동들이 이루어지고 있다. 본 논문에서는 대표적인 국제표준화 기구에서 이루어지고 있는 정보보호 표준화 현황 및 주요 이슈들에 대해 소개하고, 향후 추진방향 등을 제시하여, 국내에서 국제표준화기구에 활동하고자 하는 전문가들에 유용한 자료로 활용하고자 한다.

Ⅰ. 서 론

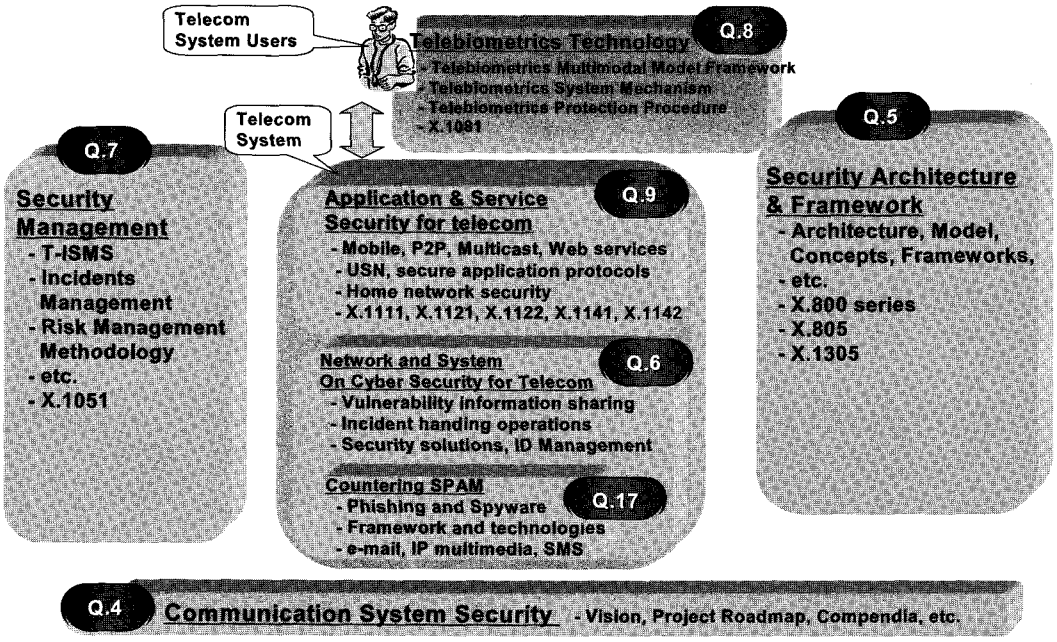
급속도로 발전하는 인터넷 환경에서 개인정보 및 소중한 자산 등을 안전하게 보호하기 위한 정보보호 기술은 그 중요성이 점점 증가하고 있다. 또한, 언제, 어디서, 어떤 장비로라도 편리하게 다양한 서비스를 이용할 수 있다는 유비쿼터스 환경으로 전환되고 있는 추세이므로, 다양한 네트워크 환경, 응용서비스, 장비들 간에 상호운용성을 보장하기 위한 정보보호 응용기술들에 대한 개발이 요구되고 있다. 그리고 이런 요구들을 충족하기 위한 해당 기술들의 개발과 함께, 관련 표준들도 그 중요성이 날로 커져가고 있다. 즉, 세계적으로 각 국가들은 자신들의 고유기술을 국제표준으로 반영하여 해당 기술에 대한 IPR(지적재산권) 및 특허 수수료 등을 확보하기 위해 적극적으로 국제표준화에 활동하고 있는 추세이다. 따라서 국내에서도 이들에 대한 분석 및 활동 현황을 파악하여 빠른 대응과 추진전략이 요구되고 있다.

본 논문에서는 대표적인 국제표준화 기구에서 이루어지고 있는 정보보호 표준화 현황 및 주요 이슈들에 대해 소개하고, 향후 추진방향 등을 제시하여, 국내에서 국제표준화기구에 활동하고자 하는 전문가들에게 유용한 자료로 활용하고자 한다.

Ⅱ. ITU-T SG17 국제표준화 현황

1865년 5월에 UN 산하에 신설된 국제전기통신연합(ITU: International Telecommunication Union)에서는 크게 전파규칙, 주파수 할당 등의 이슈를 다루고 있는 전파통신(Radiocommunication), 전기통신기술, 운용 및 요금 등의 이슈를 다루고 있는 전기통신표준화(Telecommunication), 개발도상국의 통신망 현대화를 위한 정책, 기술적 지원 등을 다루고 있는 전기통신개발(Development) 부분으로 크게 3가지로 구분된다. 이중에 정보보호 분야는 ITU-T 산하 SG17/WP2에서 7개의 연구과제로 국제표준화가 진행되고 있다. 한국은 SG17에서 매 국제회의 개최 때마다, 50% 이상의 기고서를 제안 및 채택하고 있으며, 3개의 연구과제에서 라포처(Rapporteur, 의장)로 회의를 주재하고 있고, 표준초안 25건에 대한 에디터로 정보보호 분야의 국제표준을 개발하고 있다. 현재 SG17에서 한국은 국제적으로 매우 활발한 국가로 인지도가 높이 평가받고 있다.

* 한국정보통신기술협회 표준화본부 (hroh@tta.or.kr)
** 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr)



〔그림 1〕 ITU-T SG17 보안 분야 연구영역

SG17 산하 7개의 연구과제의 연구영역은 [그림 1]과 같으며, 한국 주도로 개발되고 있는 총 25건의 표준초안은 부록 [표 1]과 같다[7, 8, 9].

2.1. 통신시스템 보안 프로젝트(Q.4)

연구과제(Question) 4에서는 ITU-T 내에 전체적인 보안 요약물, 전략, 비전, 계획 등을 연구하고 있으며, 정보보호 표준화 정보공유를 위한 워크숍 및 타 표준화 기구들과의 협력 체계 구축을 위한 작업들을 연구하고 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 구축 중에 있다. 보안 표준화 로드맵의 주요내용은 Part 1: 표준화기구들의 구조, Part 2: 제정된 표준현황, Part 3: 각 표준화기구들의 워크프로그램(작업현황), Part 4: "gap" 항목들로 구성되어 있다.

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. 현재, 본 그룹의 주요이슈는 X.805 표준의 응용 표준들을 개발하는 것으로 네트워크와 사용자 간에 보안제어 역할분담을 위한 구조(X.805+) 표준초안이 지난 9월 스위스 제네바 회의에서 가장 활발히 논의가 되었으며, 현재 최종 표준초안이 국가별 의견수렴(Consent)단계로 진행 중에 있다. 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 Q.5에서 이기종 네트워크 환경에서 서로 다른 보안 시스템과 이들의 서비스를 제어할 수 있는 네트워크 보안을 위한 정책생성, 저장, 분배, 실행을 위한 프레임워크(X.spn), EAP 기반의 인증 및 키 관리 프레임워크(X.akm) 2건의 표준초안을 개발하여, 현재 국가별 의견수렴 단계로 추진되고 있다.

2.3. 사이버보안(Q.6)

연구과제 6에서는 인터넷 및 네트워크 시스템 등에 발생할 수 있는 침해사고대응방법, 보안솔루션, 사이버 보안 취약점들에 대한 해결방법 및 정보공유 방법 등에 대해 연구하고 있다. 주요활동 결과로는 캐나다 주도로 사이버 보안의 개요(X.cso) 정의와 OASIS의 언어(XML)를 ITU-T ASN.1 언어로 바꾸는 표준(X.cap, X.cap2)들을 개발하였으며, 2006년 12월에 신설된 FG-IDM의 결과물들에 대한 표준화를 추진하고 있다. Q.6에서 한국은 RFID 프라이버시 보호가이드라인(X.rfpg)과 유무선 IPv6 환경에서 전파되는 웜을 예방하기 위한 기술(X.gopw), 사용자 제어를 위한 디지털 식별체계 상호교환 프레임워크(X.idif)와 보안정보 공유 프레임워크를 위한 요구사항(X.sisfreq)들을 주도적으로 개발하고 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) 표준의 개정 작업이 완료되어, 빠른 금년 말에는 최종 국제표준 개정판이 발간될 예정이다. 개정된 표준에는 ISO/IEC 27002 표준과의 관계 등을 명확히 기입하였으며, 표준초안의 부록으로 사이버공격 및 네트워크 폭주(congestion) 등과 같은 보안 해결방안들을 추가하여 정의하고 있다. 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, E.409 표준과 보안사고 발생원인, 현상, 결과 등을 포함하여 개발키로 합의되었다. 또한, Q.7의 다른 이슈는 중국에서 제안한 "네트워크 보안관리 프레임워크(NSMF)"에 대한 검토결과이다. 본 아이템은 Q.6과 Q.7 간에 연구범위가 적합하지 않아, 전체 회의를 개최하여 조율되었으며, SG4에서 제정한 M.3320 표준과 중복성 문제, 명확한 연구범위, 세부적인 기술사항들에 대한 충분한 예, X.1051에서 고려되고 있는 자산관리 및 사고관리 방법, X.805 및 ISO/IEC18028-2 표준들과의 관계를 명확히 구분하여, Q.6에서 개발키로 합의되었다.

2.5. 텔레-바이오인식(Q.8)

연구과제 8에서는 2006년 12월, 제네바 회의에서 한국의 김학일 교수가 새롭게 Q.8 라포처로 임명되어 회의를 주해하고 있는 그룹이다. 현재, 한국은 3건의 국제표준을 주도적으로 개발하고 있으며, 이중 첫 번째와 두 번째는 네트워크 환경에서 바이오정보를 이용하여 통신을 할 경우, 바이오정보에 대한 생명주기(생성, 전달, 저장, 폐기 등)의 전체 과정을 안전하게 보호하기 위한 표준을 개발하고 있다. 즉, 단일 바이오정보 보호 표준(X.ttp-1)과 다중 바이오정보 보호 표준(X.ttp-2)이다. 세 번째 표준초안은 바이오정보를 이용하여 전자서명키를 생성하기 위한 표준(X.tdk)으로 현재 국내 TTA 단체표준과 병행하여 개발중에 있다. 일본은 네트워크 시스템에 바이오정보를 이용한 인증메커니즘(X.tsm-1) 표준초안과 이를 준수하여 바이오인식 제품이 만들어졌을 경우, 해당 제품의 보안성 평가를 위한 보호프로파일(TSM-2) 표준을 개발중에 있다. 한국은 X.tsm-1 및 X.tsm-2에 대한 다양한 검토 의견을 제안한 바 있고, 일본의 요청에 따라, 2건에 대한 협력 에디터를 맡고 있다. 중국은 텔레바이오인식 인증기반구조(X.tai)를 개발중에 있으며, 이는 각 객체들의 식별자 값을 부여 방법과 인증서를 이용한 인증 방법 등을 개발하기 위한 표준초안이다. 또한, 본 표준초안과 ISO/IEC JTC1/SC27 Project 24761과 중복성 문제가 제기되어, 2007년 9월에 논의된 바가 있다. 스위스는 ISO/IEC JTC1/SC37과 ITU-T 간에 효율적으로 바이오인식 데이터베이스를 관리하기 위한 방법과 바이오인식 용어들의 조율을 위한 표준초안(X.physiol)을 개발하고 있으며, 빠르면 금년 11월에 국제표준으로 제정될 예정이다. 또한, 프랑스에서는 바이오인식 인터페이스 간에 상호운용성 보장을 위한 BIP 프로토콜(X.bip) 표준초안을 개발하고 있으며, 이 표준초안도 빠르면 금면 11월에 국제표준으로 제정될 예정이다.

2.6. 안전한통신서비스(Q.9)

연구과제 9에서는 안전한통신서비스라는 이슈로 SG17에서 가장 활발한 그룹이며, 한국의 염흥열 교수가 2004년 11월부터 현재까지 회의를 주재하고 있다. Q.9에서 주로 다루고 있는 분야는 홈네트워크 보안, 모바일 보안, RFID 보안, 응용프로토콜 보안, 웹서비스

보안, P2P 보안, 멀티캐스트 보안, USN 보안 등의 이슈를 연구중에 있다. 특히, 한국은 홈네트워크 보안과 RFID 보안에 주도적으로 하고 있으며, 2007년 4월, 멀티캐스트 보안을 처음으로 Q.9에서 개발키로 승인된 바 있고, 2007년 9월에는 USN 보안 분야를 ITU-T 내에 처음으로 개발키로 합의되었다. 홈네트워크 보안은 총 4건의 표준초안을 개발중에 있으며, 2007년 2월, 그 첫 번째 표준으로 홈네트워크를 위한 보안기술 프레임워크(X.homesec-1)가 ITU-T X.1111 국제표준으로 제정된 바 있다. 또한, 2007년 9월, 회의에서 홈네트워크 디바이스를 위한 인증프로파일(X.homesec-2)과 홈네트워크 서비스를 위한 사용자 인증메커니즘(X.homesec-3) 표준초안 2건을 국가별 의견수렴으로 승인되어 빠른면 금년 11월에 국제표준으로 제정될 예정이다. 네 번째 홈네트워크 표준초안은 2007년 4월 회의에서 신규로 채택된 홈네트워크를 위한 권한부여 프레임워크(X.homesec-4)이다. RFID 보안은 프라이버시 보호 가이드라인(X.rfpg)은 Q.6에서 개발중에 있으며, Q.9에서는 네트워크 기반의 RFID 서비스를 위한 프라이버시 보호 프레임워크(X.rfidsec-1)를 개발중에 있다. 중국은 모바일 보안 분야를 주도적으로 개발하고 있으며, 모바일 종단간 데이터통신을 위한 일반적인 보안(정책)서비스(X.msec-3), 모바일 종단간 데이터통신에서의 인증구조(X.msec-4), 모바일 데이터통신에서의 상호연동 시스템(X.crs)들의 총 3건의 표준초안을 개발 중에 있으며, 2007년 9월, 회의에서 국가별 의견수렴으로 승인되어 금년 11월에 국제표준으로 제정될 예정이다. 응용프로토콜 보안에서는 한국과 일본이 각각 1건이 표준초안을 개발하고 있으면, 한국은 안전한 패스워드 기반의 인증 및 키교환이 가능한 프로토콜에 대한 가이드라인(X.sap-1)을 개발하여, 2007년 9월, 회의에서 국가별 의견수렴으로 승인되어 금년 11월에 국제표준으로 제정될 예정이다. 일본은 TTP 서비스를 이용한 안전한 통신방법(X.sap-2)을 개발중에 있다. P2P 보안 분야도 한국과 일본이 각각 1건씩 개발중에 있고, 일본은 P2P 통신에서 요구되는 일반적인 보안요구사항(X.p2p-1)을 개발중에 있으며, 한국은 P2P 통신에서의 다양한 보안구조 및 운영방법(X.p2p-2) 표준을 개발하고 있다. 2007년 7월, 한국에서 개최된 라포처 회의에서 한국의 제안으로 두 표준초안 간에 통일된 P2P 모델을 사용하자는 제안이 승인되어, X.p2p-2에서 전체적인 모델을 정의하고, X.p2p-1에서는 일반적인 보안요구사항만을 정의하기로 합의되었다. 웹서비스 보안은 캐나다에 의해 OASIS의 XML 보안 표준들을 ITU-T 표준으로 제정키로 합의된 바 있으며, 1차적으로 2006년 6월에 SAMLv2.0(X.1141), XACMLv2.0(X.1142) 표준이 ITU-T 국제표준으로 제정되었다. 한국은 모바일 웹서비스에서의 메시지 보호를 위한 보안구조(X.websec-3) 표준초안을 개발 중에 있으며, 이는 모바일 환경에서 발생되는 다양한 서비스 시나리오들을 정의하고 있고, 2007년 9월 회의에서 국가별 의견수렴으로 승인되어, 금년 11월에 국제표준으로 채택될 예정이다.

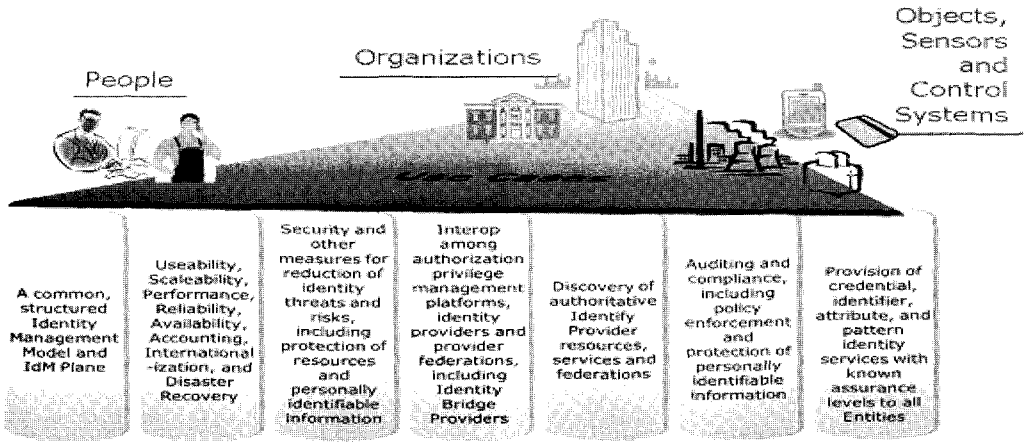
2.7. 기술적인 방법에 의한 스팸대응(Q.17)

연구과제 17에서는 한국과 중국이 주도적으로 스팸대응을 위한 표준화를 연구하고 있으며, 크게 e-mail에 의한 스팸과 IP 멀티미디어 서비스에 의한 스팸을 분리하여 표준들을 개발하고 있다. 한국은 e-mail 스팸대응 가이드라인(X.gcs), IP 멀티미디어 응용을 위한 스팸대응 개요(X.ocsip) 및 IP 멀티미디어 스팸대응을 위한 프레임워크(X.fcsip) 등 3건의 표준초안에 대한 에디터십을 확보하여 주도적으로 개발 중에 있다. 중국은 스팸대응을 위한 요구사항(X.csreq), e-mail 스팸대응을 위한 기술적인 프레임워크(X.fcs) 및 상호연동이 가능하고 스팸대응 게이트웨이 시스템(X.tsc-1)을 개발 중에 있으며, 2007년 9월, 회의에서 신규로 모바일 SMS 스팸에 대한 표준초안을 개발키로 합의되었다.

2.8. 객체식별자(ID) 관리(FG-IdM)

2006년 12월, SG17 산하에 신설된 FG-IdM 그룹은 세계 다양한 표준화 기구 및 각 국가별로 네트워크 객체(사용자, ISP, 네트워크 장비 등)들의 식별정보를 다양한 방법에 의해 관리, 연구 및 표준화하고 있는 현황들을 조사하여, 향후 이들을 ITU-T 차원에서 국제표준화 하고자 구성되었다. FG-IdM 그룹의 지난 1년간 주요활동 결과로 다음 6건의 보고서를 만들었으며, 특히 글로벌한 ID 관리 요구사항은 [그림 2]와 같이 정의하였다[1].

- FG-IdM 그룹의 활동 개요와 향후 활동 계획
- 활동 결과에 따른 주요 결과물들의 개요
- 기존 표준 분석/용어 정의
- 유스 케이스 및 갭 분석



〔그림 2〕 글로벌한 ID 관리 요구사항

- 글로벌 ID 관리를 위한 요구사항
- 글로벌 ID 관리 프레임워크

현재 FG-IdM 그룹은 2007년 9월 SG17 회의에서 주요활동 결과물들을 보고하고 종료되었으며, 향후 추가적인 연구를 위해 JCA-IdM 혹은 IdM-GSI 그룹의 신설이 고려되고 있다. 또한, 관련 결과물들의 표준화는 Q.6에서 진행하기로 결정되었다[2, 3].

2.9. 차기 연구회기(2009-2012) 구조조정 방향

ITU-T SG17에서 가장 중요하게 다루어지고 있는 이슈는 차기 연구회기(2009-2012) 동안의 구조조정 방향에 대한 논의이다. 한국은 보안 표준화 영역을 보다 확대하기 위하여, 2007년 9월, SG17 회의에서 한국의 조율된 의견을 제안하여, 현재 신규로 2가지 연구과제 후보가 고려되고 있다.

- 사이버범죄대응기술 : IT 포렌식, IP 역추적, Cyber Crime 등
- 멀티미디어보호기술 : DRM 기술, 데이터콘텐츠 보호기술 등

또한, 상기 2건의 연구과제에 대해, 영국 및 일본 등에서는 보안 그룹을 신규로 신설하는 것 보다는 기존의 연구과제에 포함시키자고 주장하고 있으며, DRM 기술과 관련해서는 ITU-T 이슈가 아니라는 의견들이 언급되고 있다. 따라서, 상기 2건의 연구과제가 최종적으로 채택되기 위해, SG17 분과위원회를 중심으로 2008년 4월까지 계속해서 대응할 계획에 있다.

구조조정 이슈와 관련하여, 각 국가별로 합의된 사항은 기존의 안전한통신서비스(Q.9)를 2개의 연구과제로 분할하기로 합의되었다.

- 안전한 유비쿼터스 통신 서비스 : USN 보안, 홈 네트워크 보안, 모바일 보안, RFID 보안 등
- 안전한 통신 서비스 : 웹서비스 보안, 응용프로토콜 보안, P2P 보안, 멀티캐스트 보안 등

Ⅲ. ISO/IEC JTC1 SC27 및 SC37 국제표준화 현황

ISO(International Organization for Standardization) /IEC(International Electrotechnical Commission) JTC1(Joint Technology Committee 1)은 정보처리시스템에 대한 국제표준화 위원회(ISO/TC97)와 정보기기에 대한 국제표준화 위원회(IEC/TC83)를 통합하여 1987년에 설립된 공동기술위원회 조직이다.

3.1. 정보보호기술(SC27)

JTC1 산하 SC27(Sub-Committee)에서는 정보통신 보안기술에 대한 국제표준화가 연구되고 있으며, 산하 5개의 WG(Working Group)을 구성하여, 정보보호 원천기술 분야를 중심으로 연구하고 있다. SC27에서 추진되고 전체 표준화과제(Project)는 총 70건이 등록되

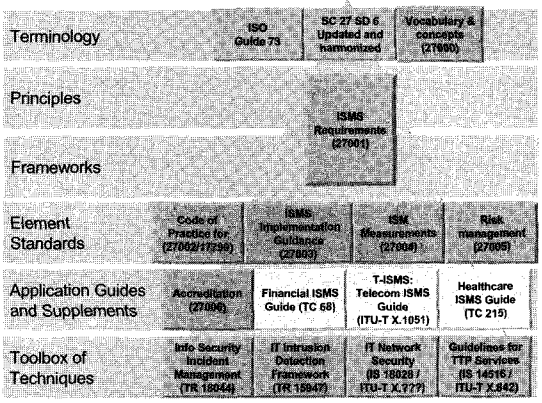
어 있으며, 현재 진행되고 있는 과제는 총 52건이 진행되고 있다. 그 동안 SC27에서 발간된 국제표준 및 기술보고서는 총 62건의 문서가 발간되었다. SC27 산하 5개 WG의 주요 연구영역은 다음과 같다.

- WG1(보안요구사항, 서비스, 가이드라인)에서는 정보보호 관리 시스템(ISMS)과 같은 관리적 차원에서의 가이드라인 및 보안서비스 표준들을 개발
- WG2(보안기술 및 메커니즘)에서는 보안서비스 구현을 위한 다양한 보안기술과 여러 메커니즘 및 비암호 방식의 보안기술들을 개발
- WG3(보안평가기준(CC : Common Criteria))에서는 IT 보안성 보증 및 평가에 관한 표준화를 추진하고 있으며, 공통평가기준의 범위를 확장하여 인적, 관리적 부분을 평가하기 위한 표준화가 추진
- WG4(보안제어 및 서비스)에서는 정보보호 시스템들의 접근제어 및 권한 관리와 관련된 보안서비스를 제어하기 위한 표준화가 추진
- WG5(식별체계 관리 및 프라이버시 보호 기술)에서는 RFID 및 ID Management 기술들의 표준화가 추진

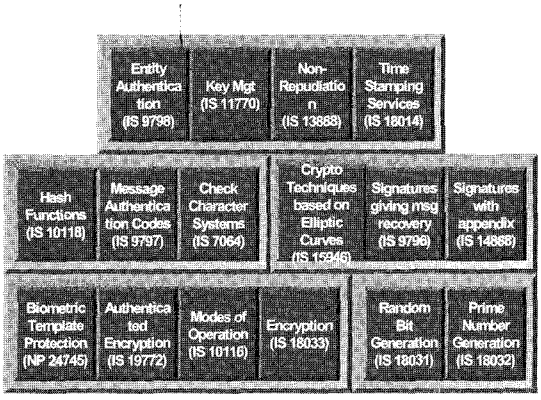
SC27에서 신규 표준화 과제로 진행되고 있는 사항들은 다음과 같다[5].

- NP 27007 : 정보보호 관리 시스템(ISMS)의 감사(auditing)를 위한 가이드라인 개발
- NP 27xxx : 암호학적 프로토콜의 보안성 평가를 위한 검증 표준 개발
- NP 27031 : 비즈니스 연속성을 유지 및 계획하기 위해, 정보처리 및 통신설비들의 요구사항 정의
- NP 27032 : 사이버보안을 가이드라인 표준 개발
- NP 27034 : ISMS 표준을 실제 비즈니스 응용에 활용할 경우, 이용자(관리자, 개발자, 사용자 등)들의 관점에서 바람직한 보안 등급을 분류할 수 있는 가이드라인 표준 개발

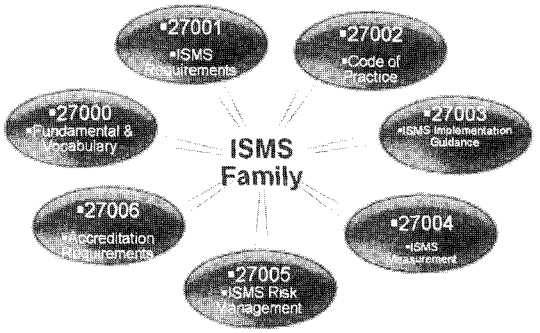
SC27에서 개발된 주요 표준들을 기능별로 분류하면 크게 계층화된 보안관리 모델 [그림 3], 암호학적 기술 [그림 4], ISMS 기술 [그림 5], 보안성 평가 [그림 6] 기술로 분류할 수 있다[4].



〔그림 3〕 계층화된 보안관리 모델 표준



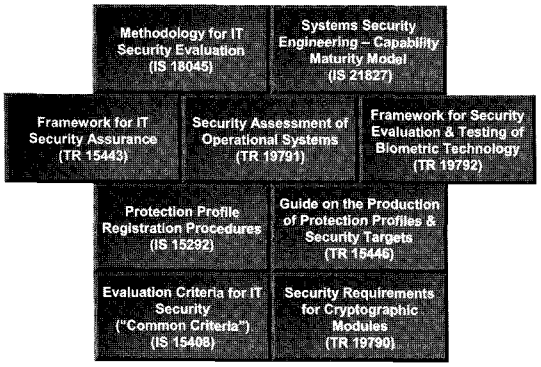
〔그림 4〕 암호학적 기술 표준



〔그림 5〕 ISMS 표준

3.2. 바이오인식기술(SC37)

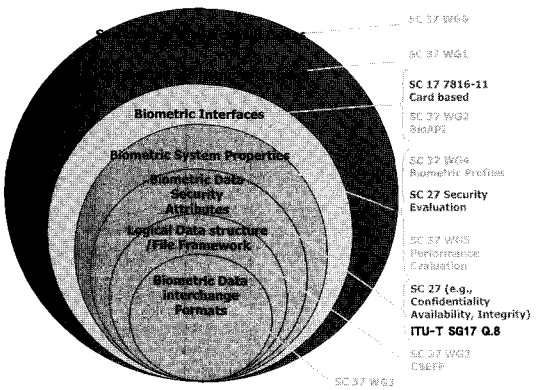
2002년 12월, 미국 올랜도에서 제1회 ISO/IEC JTC1 SC37 창립총회를 개최하여 전 세계 바이오인식 기술에 대한 국제표준을 주도적으로 개발하고자 신설되었다. 또한, 바이오인식 분야의 국제표준화는 미국, 9·11 테러



〔그림 6〕 보안성 평가 표준

사건 이후 사용자 인증 수단으로 그 중요성이 크게 부각되고 있으며, 전자여권에 대한 표준 개발을 위해 SC17(IC 카드), SC27(보안성 평가)과 협력하여 표준을 개발하고 있다. 현재, SC37 산하에는 6개의 WG 그룹을 구성하여, 바이오인식 분야의 국제표준을 개발하고 있으며, 주요 연구영역은 다음과 같다[6, 18].

- WG1 : 바이오인식 전문용어 표준 개발
- WG2 : 바이오인식 컴포넌트와 시스템 사이의 인터페이스, BioAPI, CBEFF, 표준적합성 시험기술 등 상호운용성에 대한 표준 개발
- WG3 : 각 바이오인식 기술별 바이오정보 데이터 포맷규격에 대한 표준 개발
- WG4 : 육로 · 항만 · 공항 바이오인식기반 출입국 심사에 필요한 응용 프로파일 및 출입국관리시스템 응용기술에 대한 표준 개발
- WG5 : 바이오인식 기술의 성능 및 상호연동 시험 기술에 대한 표준 개발
- WG6 : 개인 고유정보인 바이오정보에 대한 법제도적 요구조건 및 프라이버시 관련 표준 개발



〔그림 7〕 바이오인식 분야이 국제표준화 연구영역

바이오인식 기술과 관련된 연관 그룹 간의 국제표준화 연구영역은 [그림 7]과 같다.

한국은 SC37에서 ISO/IEC 24709-1(BioAPI 표준적합성 시험방법 및 절차), ISO/IEC 19794-9(정맥인식 데이터 호환 국제규격) 표준을 2007년 1월에 제정한 바 있고, ISO/IEC TR 24722(다중바이오인식 기술동향 분석) 기술보고서를 2007년 6월에 채택시켰다.

Ⅳ. IETF Security Area 국제표준화 현황

1986년에 신설된 IETF(Internet Engineering Task Force)는 인터넷 서비스의 품질을 보장하고 보다 향상된 인터넷 환경을 개발하기 위해 실무자들을 중심으로 구현 관점에서 사실표준화를 추진하고 있는 국제표준화 기구이다. IETF는 총 8개의 활동영역(Area)을 구성하여 표준화가 진행되고 있으며, 이중 인터넷 환경에서 보안과 관련된 작업을 추진하고 있는 그룹이 보안그룹(Security Area)이며, 산하에 총 17개 실무반을 구성하고 있다. 주로 작업되고 있는 분야로는 인증, 암호, ID 관리, 응용프로토콜, IPv6, PKI, 인터넷침해대응솔루션, VoIP, SIP, 웹서비스, P2P, 멀티캐스트 보안, S/MIME 등의 인터넷과 관련된 보안기술들을 표준화 하고 있다. 총 17개의 실무반은 다음과 같으며, 주요 연구영역은 다음과 같다[12, 14, 15].

- btns : IPSec, IKE 등의 보안협약 과정에서 익명성 키 보장을 위한 프레임워크 및 응용표준 개발
- dkim : 인터넷 이메일 서비스와 같은 도메인 간에 활용될 수 있는 보안 표준 개발
- emu : EAP 프로토콜(RFC 3748)과 EAP 메소드를 위한 IEEE 802.11 요구사항을 충족시키기 위한 보안 표준 개발
- hokey : EAP 프로토콜의 개선된 인증방법
- isms : SNMPv3를 위한 단일화된 보안 모델 개발
- keyprov : 대칭형 암호키 및 협약된 속성들을 안전하게 전달하기 위한 보안 프로토콜 및 데이터 형식을 개발
- kitten : 인터넷 상에서 전달되는 메시지 및 해당

문맥을 보호하기 위한 API 표준을 개발

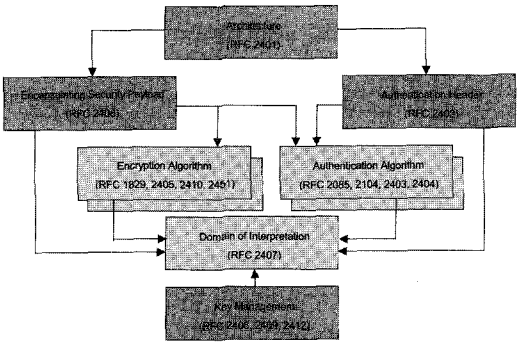
- krb-wg : 커버로스 사용자 인증 시스템(Version 5)의 안전·편의성 제고 및 키관리 방법 개발
- ltans : 장시간 동안 상용될 수 있는 데이터 기록방법 및 보관 방법을 위한 보안 표준 개발
- msec : 인터넷 상에서 다수의 사용자에게 데이터를 안전하게 전송할 수 있는 멀티캐스트 보안 표준 개발
- nea : 네트워크 보안 정책에 따라 종단에 존재하는 사용자 및 장비들의 보안성 지원을 위한 평가기술 개발
- openpgp : 인터넷 상에서 활용되는 이메일, 파일 저장을 안전하게 지원하기 위한 보안 기술 개발
- pkix : X.509 기반의 PKI 관련 표준화와 서버기반의 인증서 경로검증 프로토콜(DPD/DPV), CMS 기반의 인증서 관리 프로토콜, OCSP 경량 프로토콜 등에 대한 표준 개발
- sasl : 보안계층에서의 간단한 인증(RFC2222) 표준 기반으로 BEEP, IMAP, LDAP, POP, SMTP 프로토콜들의 키 보안 서비스 관련 표준 개발
- sime : 보안메일 메시지 형식(RFC3369) 및 알고리듬(RFC3370) 표준들의 개선 작업
- syslog : 시스템/네트워크 이벤트의 네트워크 로깅을 위한 표준 개발
- tls : '96년도에 개발된 TLS v1.1 프로토콜 개선과 MD5, SHA1 등 해쉬알고리듬을 제거하고 신규로 개발되는 암호 알고리듬 표준으로 대체하는 작업

한국은 IETF에서 SEED 암호알고리즘 및 관련 응용표준으로 RFC4269, 4010, 4162, 4196 국제표준을 제정한 바 있다.

IETF에서 개발된 많은 인터넷 보안 표준들 중에 활용도가 높고, 잘 알려진 IPSec 보안 프로토콜을 예로 소개하면, IPSec 표준들은 크게 IPSec 보안구조, IPSec 프로토콜, 암호알고리즘, 인증알고리즘, 키관리 프로토콜 분야로 구성될 수 있으며, [그림 8]과 같이 요약될 수 있다.

V. 기타(ASTAP, RAISS 포럼, CJK SWIS)

정보보호와 관련된 가장 대표적인 국제표준화기구



〔그림 8〕 IPsec 표준의 구성 체계

로는 ITU-T SG17, ISO/IEC JTC1/SC27, SC37, IETF를 꼽을 수 있다. 하지만, 아시아 지역 간에 정보보호 표준화 협력 및 정보공유를 위해 운영되고 있는 대표적인 그룹이 있어, 본 장에서 간단히 소개하고자 한다.

5.1. ASTAP

1998년 2월에 신설된 아시아·태평양 지역의 표준화 협의체인 ASTAP(Asia-Pacific Telecommunity Standardization Program)은 아·태지역 국가 정부간 협정에 의해 설립된 APT 산하 표준화 활동 전담 프로그램으로 국제표준화기구들에 대한 대응방향 및 아시아지역 간에 의견조율을 위해 신설된 표준화기구이다. ASTAP은 7개의 작업그룹(Working Group)과 10개의 전문가그룹(Expert Group)으로 구성되어 있으며, 이들 전문가그룹 중에 한 개가 정보보호 분야를 다루고 있다. 과거 ASTAP에서는 서로 간에 정보공유 및 의견조율만을 목적으로 활동하였으나, 2006년부터 아시아지역을 위한 표준을 개발키로 합의된 바 있다. ASTAP의 정보보호 전문가그룹에서는 주로 ITU-T SG17 보안 연구과제들을 중점적으로 대응하고 있다.

5.2. RAISS 포럼

2004년 11월, 아시아 지역의 각 국가별 정보보호 표준화 현황 및 정보 공유, 국제표준화 기구(ISO/IEC JTC1 SC27, ITU-T SG17)들에 대한 단일 대응을 위해 RAISS(Regional Asia Information Security Exchange) 포럼이 신설되었으며, 2007년 8월까지, 총 6회의 정기회의를 개최하였다. 본 포럼은 초기 싱가포르에서 사무

국 역할을 담당하였으나, 제6차 정기회의를 마지막으로 말레이시아에서 사무국을 담당키로 하였고, 2008년 7월, 말레이시아에서 제7차 정기회의를 개최키로 하였다. 참여하고 있는 주요 국가로는 중국, 일본, 한국, 말레이시아, 뉴질랜드, 싱가포르, 태국 등을 중심으로 매 회의 때마다 25~30명의 전문가들이 참석하고 있다. 한국에서 주요 대응 사례로는 국내에서 개발되어 활용하고 있는 ISMS 체계를 소개한 바 있으며, 해당 기술이 싱가포르 표준으로 채택되었고, 아시아 국가들에게 중요한 가이드라인 문서로 활용되고 있다. 현재, RAISS 포럼에서 한국의 정보보호 표준은 많은 관심과 위상이 높은 것으로 알려져 있어, 한국에서 ITU-T SG17 및 ISO/IEC JTC1/SC27, SC37 등으로 제안하기에 앞서 가능한 RAISS 포럼에서 1차적인 표준화 작업을 해줄 것을 요청한 바 있다.

5.3. CJK SWIS

2007년 10월, ITU-T SG17에서 활동하고 있는 정보보호 표준화 전문가들을 중심으로 한중일 간에 정보보호 표준화 이슈 공유 및 SG17 활동의 정보 공유를 위해 CJK(China, Japan, Korea) SWIS(Standardization Workshop on Information Security) 워크숍을 신설하였다. 제1차 워크숍은 서울 숙명여대에서 약 60여명의 전문가들이 참석하여, 한중일 간에 정보보호 산업체 개발 현황, 표준화 전략, 표준화 현황 등을 발표하였다. 본 워크숍은 계속해서 한중일 정보보호 분야 표준화 산업 육성 및 협력 강화를 위해 매년 1회씩 3개국에서 돌아가면서 워크숍을 개최키로 합의하였다.

Ⅵ. 표준화 추진전략 및 고려사항

6.1. ITU-T SG17

ITU-T SG17 활동에 있어 고려되어야 할 사항으로 첫 번째는 한국 참가자들은 주로 학계 및 연구소에서 참석하고 있어, 실제 산업체에서 개발되어 활용되고 있는 실용기술과 관련된 표준초안 개발이 저조하다는 문제점이다. 따라서 국내 산업체에서 적극적으로 참여할 수 있는 방법을 모색해야 할 시점이다. 두 번째는 국제표준 제정기간은 보통 2~3년 정도가 소요되나, 해당 과제와 연계되고 있는 국내과제(표준화과제, R&D)가 계획 보다 빠르게 종료되거나 없어지는 경우가 발생한다. 따라서 국내 과제 평가 방법들도 최종결과물을 국제표준으로 대체하는 방안이 고려되어야 하고, 장시간 소요되는 국제표준화 활동을 지원할 수 있도록 신규과제 발굴 시, 구과제와 연계할 수 있는 방안이 고려되어야 한다. 세 번째로는 ITU-T SG17 연구회기가 2008년 9월, 회의를 마지막으로 종료됨으로 신규로 제안되는 표준초안 이외에 한국 주도록 개발되고 있는 표준초안들은 가능한 모두 최종 국제표준이 제정될 수 있도록 노력해야 된다. 네 번째로는 홈네트워크 보안, USN 보안, RFID 보안, 멀티캐스트 보안 분야 등은 현재 한국 주도로 개발되고 있는 분야이다. 따라서 이와 같은 분야는 계속해서 우위를 확보할 수 있도록 노력해야 하고, 신규로 추가 가능한 분야를 발굴하여 활동 영역을 확대해야 된다.

ITU-T SG17 표준화 활동을 위한 추진전략으로 첫 번째는 차기 연구회기('09~'12) 구조조정 방향을 전략적으로 대응해야 된다. 한국은 지난 9월 회의에서 신규로 사이버범죄대응기술, 멀티미디어보호기술를 제안하여 신규 연구과제 후보로 채택된 바 있다. 상기 2건의 신규 분야가 채택되면, 국내 포렌식 기술, IP 역추적 기술, DRM 기술 등이 ITU-T SG17에서 표준화가 추진될 수 있는 길이 열리므로, 가장 중요하고 우선 순위로 대응해야 된다. 국내에서는 본 이슈를 대응하기 위하여 국내 SG17 분과위원회를 중심으로 상기 연구과제에 대한 활동영역 제안 기고서 검토와 발표자 선정, 지지 발언에 대해 추진전략을 수립할 계획이고, 12월 제네바에서 개최되는 SG17/WP2 회의에 제안할 예정이다. 두 번째로 한국 주도로 추진되고 있는 25건의 표준초안은 각 담당 에디터 및 의장단 간에 협의하여, 최종 국제표준이 완료될 수 있도록, SG17 분과위원회를 중심으로 TTA 표준화위원회, 국내 산업체를 중심으로 구성된 포럼들과 협력하여 추진해야 한다. 세 번째로 필요한 추진전략은 ITU-T에서 제정된 국제표준들을 체계적으로 검토하여, 국내표준으로 수용 유/무에 대한 검토와 적절시기, 방법 등을 강구해야 된다. 현재 고려되고 있는 방법은 SG17 분과위원회에서 1차적인 검토 후, 해당 TTA 표준화위원회에 재검토를 의뢰하여 추진할 계획이며, 한국 주도로 개발되고 있는 국제 표준초안들은 각 에디터가 책임지고 국내표준 제정까지 활동해 줄 것을 권고할 예정이다. 네 번째로 차기 연구회기를 위한 의장단들에 대한 구조조정 대응전략으로 현재 확보된 의장단석(김정덕

(Q.7-부라포처), 김학일(Q.8-라포처), 염흥열(Q.9-라포처))을 계속해서 유지할 수 있도록 노력할 계획이다. 또한, 구조조정에 따른 신규 연구과제들은 신규로 제안한 국가에서 보다 순조롭게 의장단을 확보할 수 있으므로, 신규로 제안된 연구과제와 새롭게 언급되고 있는 연구과제들은 적시에 대응할 수 있도록 해당 분야의 국내 전문가를 신속히 섭외할 계획이다. 다섯 번째로 중요한 추진전략은 식별체계 관리(ID Management) 방법 및 기술 대응전략이다. 이는 NGN, USN 등 모든 네트워크 환경에서 사용자 및 각 객체들의 식별체계(ID)를 관리하는 기술로 매우 중요하며, 현재까지는 모든 분야에서 독립적으로 표준화를 추진했었으나, ITU-T 내에 처음으로 세계 모든 표준화기구 및 국가별로 운영되고 있는 식별체계 관리 방법들을 고려하여 단일 표준을 만들자고 합의된 사항이다. 따라서 한국에서는 ETRI에서 제안한 사용자의 권한을 관리하기 위한 표준초안과 KISA에서 제안한 인터넷 상에서 활용되고 있는 주민등록번호 대체기술(i-PIN)을 국제표준으로 개발하는 것이 필요하다. 그리고 식별체계 관리 기술은 국내에서 다양한 분야에 적용되고 있으나, 아직 관련된 국내표준들이 없으므로, TTA 표준화위원회와 관련 산업체 전문가들을 섭외하여 대응하는 것이 필요하다.

6.2. ISO/IEC JTC1 SC27, SC37

SC27 표준화에 있어 고려사항으로 첫 번째는 암호, 인증, 권한관리는 정보보호 기반 기술이기 때문에 사회적으로 지속적인 관심이 부족하며, 보안서비스 제공을 위한 인프라로 인식되기 때문에 업체의 신규 기술 개발 및 표준 활동이 미흡하므로 이에 대한 개선책이 필요하다. 두 번째로는 유비쿼터스 사회에서 활용 가능한 다양한 인증대상 및 인증수단을 고려한 차세대 인증기술의 개발이 필요하고, 해킹 등을 예방하기 위한 응용기술 분야의 표준화 활동이 미흡하므로 개선이 필요하다. 세 번째로는 인터넷 상에서의 ID 도용 및 개인정보유출 문제가 심각해지고 있어, 이와 관련된 개인정보보호를 위한 표준화 활동이 필요하다.

SC27 표준화 추진전략으로 첫 번째는 국내에서 개발된 HIGHT, FORK-256, TSC-4 등과 같은 암호알고리즘들은 적극적으로 국제표준화를 제안하는 것이 필요하다. 두 번째로는 미국, 유럽 등에서 국내 보다 앞선 기술에 대한 표준은 해당 분야를 새롭게 개척하기 보다는 앞선 기술을 빠르게 도입하여, 관련 응용 기술 개발 및 표준화를 추진해야 된다. 세 번째로는 SC27 및 ITU-T에서 신규로 시작하고 있은 ID 관리 분야는 가능한 산업체 참여를 독려하기 위하여, 산업체를 중심으로 운영되는 포럼 등의 결성이 고려되어야 한다. 네 번째로는 국내 정보보호 산업체에서 개발된 원천 기술 등을 국제표준으로 추진하여 IPR 등을 확보하는 것이 필요하다. 만약 해당 업체에서 직접 활동이 힘들다고 하면, 국내표준을 1차적으로 개발하고, 관련 국제표준화기구에 활동하고 있는 전문가가 대신으로라도 국제표준화로 추진하는 방법이 고려되어야 한다[12].

SC37 표준화에 있어 고려사항으로는 첫 번째로 출입국관리 및 Tele-biometrics 분야의 바이오인식 시장은 삼성 SDS · LG CNS · 현대정보기술 등과 같은 SI 사업자와 SK텔레콤, KTF, LGT 등과 같은 이동통신사업자가 시장 주도형 기업으로 존재하고 있어, 국내 중소, 벤처 기업들이 개발한 고유기술들이 국제표준으로 추진하는데 한계가 있다. 두 번째로는 사용자들의 고유 바이오정보를 이용한다는 잘못된 인식으로 개인 프라이버시 침해 등과 관련된 문제들이 발생하여 표준화 추진에 걸림돌로 작용하고 있다. 세 번째로는 전자여권 등 국가인프라에 대한 신분확인 핵심기술로 바이오인식기술이 국내외적으로 중요성은 인정되고 있으나, 바이오인식 알고리즘 등 SW 위주로 추진되고 있어, 바이오인식 · PKI · 정보통신 · 스마트카드 등이 융합된 기술 및 HW 측면의 기술 개발과 표준화 추진이 필요하다.

SC37 표준화 추진전략으로 첫 번째는 바이오인식 기술에 있어 가장 중요한 정확성 · 국제표준과의 상호운용성 확보를 위한 시험기술, 출입국관리 응용기술, Tele-biometrics 응용기술 및 다중 바이오인식 원천기술에 대한 국제 표준화가 우선적으로 필요하다. 두 번째로는 전 세계적으로 사용자 신분을 인증하기 위해 도입되는 전자여권 기술과 관련하여, 외교부(전자여권 발급) · 행자부(주민증진위확인시스템 보급) · 법무부(출입국관리시스템 개발) · 해수부(항만 선원신분증 보급) · 건교부(국제공항 출입통제시스템 운영) 등과 협력하여 국내표준 개발 및 국제표준에 대한 신속한 대응이 필요하다. 세 번째로는 국외 선진 국가 또는 우수 해외기업에 의해 선점된 바이오인식 핵심기술 및 국제 표준화가 진행되고 있는 부분에 적극적으로 참여하여, 신규 진입 및 응용기술 확보가 필요하다. 즉, 바이오인식시스템 시험기술 및 보안성 평가기술 표준화, 출입국관리 및

Telebiometrics 응용기술 표준화, 다중 바이오 인식기술 표준화가 필요하다[16].

6.3. IETF Security Area

IETF에서는 구현 관점에서 산업체의 사실표준을 개발하고 있는데 반해, 국내에서는 주로 학계 전문가 및 연구소를 중심으로 참여하고 있어, 산업체에서 개발되고 있는 보안 솔루션들의 표준화가 미흡하다. 또한, 미국, 유럽 등을 중심으로 운영되고 있어, 국내에서 선불리 표준화를 추진하기가 쉽지 않다는 점이다. 따라서 국내에서는 쉽게 전급할 수 있는 인터넷과 관련된 원천기술 보다는 응용 기술들에 대한 표준화가 필요하다. 즉, ISO/IEC JTC1/SC37 및 ITU-T SG17을 통화여 1차적인 국제표준을 개발하고, 이를 이용하여, 2차적인 인터넷 응용기술들에 대한 국제표준화를 추진하는 것이 적합하다. 그리고 인터넷 및 정보보호 응용기술들에 대한 산업체 참여를 장려하기 위하여, 산업체를 중심으로 운영되는 정보보호 포럼 등의 활동 육성과 포럼 표준들을 활성화해야 한다. 또한, 기 제정된 국제표준(RFC) 등을 분석하여, 신속한 국내표준 도입과 새로운 응용 기술과 관련된 국제표준 개발이 필요하다.

6.4. 기타(ASTAP, RAISS 포럼, CJK SWIS)

ASTAP 및 RAISS 포럼은 국제표준화기구로 제안하기에 앞서, 아시아 지역 국가 간에 사전 논의를 통하여 검토를 받고 합의된 내용을 국제표준으로 제안하기에 가장 적합한 기구들이다. 따라서 문제가 될 수 있는 이슈들은 사전에 ASTAP, RAISS 포럼을 통하여 지지발언을 얻을 수 있는 곳으로 활용하는 것이 필요하다. 또한, 2006년부터 ASTAP에서도 공식적으로 아시아지역 국제표준을 제정키로 한 바, 이슈별로 전 세계에서 공감할 수 있는 이슈가 아니면, 아시아지역 간에 국제표준을 제정하는 것도 좋은 방법이다. 또한, 현재 ITU-T SG17 정보보호는 한중일 간에 많은 부분을 주도하고 있어, 3개국 간에 유대관계를 지속적으로 확보해야 하고, 서로 간에 정보공유를 위한 CJK SWIS 등을 적극적으로 활용해야 된다.

Ⅶ. 결 론

본 논문에서는 ITU-T SG17, ISO/IEC JTC1, IETF 등의 국제표준화 기구에서 연구되고 있는 정보보호 표준화 동향에 대해서 살펴보았으며, 아시아 지역 국가 간에 협력 체계 구축을 위해 활동하고 있는 ASTAP, RAISS 포럼, CJK SWIS 등의 조직들도 간단히 소개하였다. 또한, 이들 동향을 바탕으로 향후 한국에서 전략적으로 정보보호 분야의 국제표준화를 추진하기 위한 고려사항 및 추진전략을 수립해 보았다. 본 논문에서 제시하고 있는 사항들은 필수적으로 고려되어야 하는 것은 아니고, 현재 정보보호 분야에서 활동하고 있는 전문가들에게 하나의 표준화활동 정보로 활용될 수 있을 거라고 판단된다. 정보보호 분야의 표준은 이제 선택사항이 아니고, 다른 여러 분야의 기술들과 함께 초기부터 개입되어 원천 기술 확보 등을 위해 적극적으로 대응해야 할 중요한 분야라고 생각된다.

참고문헌

[1] Mr. Anthony Nadalin, "TD0325: ITU-T FG IdM Presentation on Identity Management Framework", ITU-T SG17 meeting, 19-28 September 2007.

[2] 염흥열, "ID 관리 표준화 동향 및 향후 추진 방향", TTA, IT Standard Weekly, 2007. 5.

[3] 염흥열, "새로운 전환을 맞은 ITU-T ID 관리 표준화 동향", TTA, IT Standard Weekly, 2007. 10.

[4] Mr. Meng-Chow Kang, "ISO/IEC JTC1 SC27 Meeting, Moscow to St. Petersburg, May 2007", 6th RAISS Forum meeting, 22-23 August 2007.

[5] Mr. Walter Fumy, "ISO/IEC JTC1 N8782 : Business Plan for JTC1/SC27 'Security Techniques'", ISO/IEC JTC1 Plenary meeting, 8-13 October 2007.

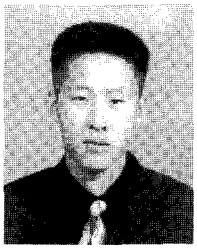
[6] Mr. Fernado L. Podio, "ISO/IEC JTC1 N8725 : Business Plan for JTC1/SC37 'Biometrics'", ISO/IEC JTC1 Plenary meeting, 8-13 October 2007.

[7] 진병문, 오흥룡, 염흥열, 강신각, "ITU 연구동향 : ITU-T SG17 분야", MIC, 통권 제14호, 한국 ITU 연구위원회 연구동향 보고서, 2007.12. [발간예정]

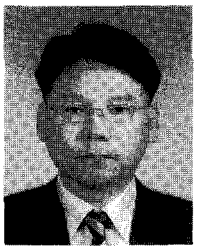
[8] 진병문, 오흥룡, 염흥열, 강신각, "ITU 연구동향 : ITU-T SG17 분야", MIC, 통권 제13호, 한국 ITU

연구위원회 연구동향 보고서, pp. 317-337, 2006. 11.
[9] 진병문, 오흥룡, 염흥열, 강신각, "ITU-T SG17 연구동향", 2005년도 ITU-T/R 연구활동 보고서, pp. 216-254, 2005. 12.
[10] 염흥열, "정보보호일반 표준화 로드맵 (v2004-2007)", TTA, 2003. 12 - 2006. 12.
[11] 오흥룡, 오세순, 김선, 염흥열, "정보보호 표준화 항목 정의 및 로드맵", 한국정보보호학회 학회지 제15권 제5호 pp. 67-82, 2005. 10.
[12] 이석래 외 4인, "정보통신 중점기술 표준화로드맵 (초안) - 암호/인증/권한관리 분야", TTA, 2007. 09.
[13] 진승헌 외 8인, "정보통신 중점기술 표준화로드맵 (초안) - 개인정보보호/ID관리 분야", TTA, 2007. 09.
[14] 원유재 외 7인, "정보통신 중점기술 표준화로드맵 (초안) - 네트워크/시스템 보안 분야", TTA, 2007. 09.
[15] 나재훈 외 7인, "정보통신 중점기술 표준화로드맵 (초안) - 응용보안/평가인증 분야", TTA, 2007. 09.
[16] 김재성 외 7인, "정보통신 중점기술 표준화로드맵 (초안) - 바이오인식 분야", TTA, 2007. 09.
[17] 오흥룡, "Secure Communication Services(Q.9) 표준화 동향", 제7회 정보보호기술 표준 워크샵 (ISSW2006), KISA, 2006. 11.
[18] 오흥룡, 염흥열, "ITU-T SG17 WP2 Q.9(안전한 통신 서비스) 표준화 동향 및 향후 전망 - 상반기", 한국정보보호진흥원, 정보보호기술 표준화 동향지, 2006. 6.
[19] 오흥룡, 염흥열, "ITU-T SG17 WP2 Q.9(안전한 통신 서비스) 표준화 동향 및 향후 전망 - 하반기", 한국정보보호진흥원, 정보보호기술 표준화 동향지, 2006. 12.
[20] 오흥룡, 염흥열, "ITU-T SG17 홈네트워크 보안 표준화 동향 및 향후전망", 한국정보보호학회 학회지 제16권 제6호 pp. 7~16, 2006. 12.
[21] ITU-T 홈페이지, http://www.itu.int
[22] ISO 홈페이지, http://www.iso.org
[23] IETF 홈페이지, http://www.ietf.org
[24] ASTAP 홈페이지, http://www.aptsec.org/ Program /~ASTAP/pastap.html
[25] RAISS 포럼 홈페이지, http://www.itsc.org.sg/~raiss.html
[26] CJK SWIS 홈페이지, http://hnrc.cau.ac.kr/swis 2007

〈著者紹介〉



오 흥 룡 (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



염 흥 열 (Heung-Youl Youm)
종신회원
1981년 2월한양대학교 전자공학과 졸업
1983년 2월: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 산학연컨소시엄센터 소장
1997년 3월~현재:한국통신정보보호학회 총무이사, 학술이사, 교육이사, (현)총무이사, (현)상임부회장
2004년 1월~현재 : 한국인터넷정보학회 이사, 논문지 편집위원
2004년 1월~현재 : OSIA 이사
2003년 9월~2004년 3월 : ITU-T SG17/Q10 Associate Rapporteur
2004년 3월~현재 : ITU-T SG17/Q9 Rapporteur
2006년 11월~현재 : 정보통신부 정책자문단 정보보호 PM
<관심분야> 네트워크 보안, 전자상거래 보안, 공개키 기반 구조, 부호이론, 이동통신보안

부록 - 표 1. 2007년, ITU-T SG17에서 한국 주도로 개발되고 있는 표준초안 목록(총 25건)

No.	권고번호	Ques	완료시점	권고명 (주제)	에디터	국내표준
1	X.akm	5/17	2007-09	Framework for EAP-based authentication and key management	염흥열	X
2	X.spn	5/17	2007-09	Framework for creation, storage, distribution, and enforcement of policies for network security	김종현	2007-350 추진중
3	X.gopw	6/17	2008-04	Guideline on preventing worm spreading in a data communication network	김미주	X
4	X.rfpg	6/17	2007-09	Guidelines on protection of personal information and privacy for RFID	이향진	TTAR-06.0014
5	X.idif	6/17	2009-12	User Control Enhanced Digital Identity Interchange Framework	조상래, 진승헌	X
6	X.sisfreq	6/17	2009-12	Requirement of security information sharing framework	정일안	2007-405 추진중
7	X.sim	7/17	2008-04	Security incident management guidelines for telecommunications	김정덕	X
8	X.tpp-1 (X.tpp)	8/17	2007-09	A guideline of technical and managerial counter measures for biometric data security	김재성, 김학일	TTAS.KO-12.0034
9	X.tpp-2	8/17	2008-04	A guideline for secure and efficient transmission of multibiometric data	길연희, 정연수	TTAS.KO-12.0050
10	X.tsm-1	8/17	2007-09	General biometric authentication protocol and profile on telecommunication system	이소베, 신용녀	X
11	X.tsm-2	8/17	2008-04	Profile of telecommunication device for telebiometrics system mechanism	이소베, 신용녀	X
12	X.tdk	8/17	2008-04	Telecommunication digital key framework	이형우, 김재성	2006-003 추진중
13	X.homesec-1	9/17	2007-02	Framework for security technologies for home network	염흥열, 오홍룡	TTAI.KO-12.0035
14	X.homesec-2	9/17	2007-12	Certificate profile for the device in the home network	백종현, 유동영	2007-001 추진중
15	X.homesec-3	9/17	2007-12	User authentication mechanisms for home network service	이형규	TTAS.KO-12.0030
16	X.homesec-4	9/17	2008-04	Authorization framework for home network	김건우	X
17	X.mulsec-1	9/17	2008-04	Security requirement and framework in multicast communication	윤미연, 염흥열	X
18	X.p2p-2	9/17	2008-04	Security architecture and protocols for per to peer network	나재훈	X
19	X.rfidsec-1	9/17	2008-04	Privacy protection framework for networked RFID services	최두호	TTAS.KO-06.0146
20	X.sap-1	9/17	2007-12	Guideline on secure password-based authentication protocol with key exchange	염흥열	X
21	X.websec-3	9/17	2007-12	Security architecture for message security in mobile web services	이재승	X
22	X.usnsec-1	9/17	2009-12	Requirement and Framework for USN	염흥열	X
23	X.fcsip	17/17	2008-04	Framework of countering IP multimedia spam	김성혜	X
24	X.gcs	17/17	2007-09	Guideline on countering e-mail spam	박소영	X
25	X.ocsip	17/17	2008-04	Overview for countering spam for IP multimedia application	강신각, 김미주	X