情 報 保 護 學 會 誌
第21卷 第2號, 2011. 4

정보보호 국제표준화 현황 및 추진체계 분석

오 흥 룡*, 박 정 식*, 진 병 문*, 염 흥 열**

요 약

정보보호 분야의 국제표준화는 기술들의 특성 및 사용자들의 관점 등을 고려하여, 다양한 국제표준화기구에서 국제표준 개발 및 관련 연구가 이루어지고 있다. 즉, ITU-T SG17에서는 전기통신(Telecommunication) 관점에서 통신망에 적용 가능한 응용기술들에 대한 국제표준화가 추진되고 있으며, ISO/IEC JTC1/SC27(정보보호), SC37(바이오인식)에서는 정보보호 원천기술들에 대한 국제표준화를 다루며, IETF Security Area에서는 인터넷 서비스의 품질 보장 및 향상된 인터넷 환경 구축을 위한 산업체 중심의 사실표준을 추진하고 있다. 또한, 유럽 및 아시아 지역에서 국가 간에 정보통신 표준화와 국제표준화 기구들에 대한 공동 대응을 위한 ETSI, ASTAP, OASIS 등에서도 정보보호 표준화 활동들이 이루어지고 있다. 본 논문에서는 정보보호 분야의 대표적인 국제표준화 기구들의 현황 및 주요 이슈, 주요 국가별 추진체계들에 대해 소개하여, 향후 국내에서 국제표준화기구에 활동하고자 하는 전문가들에 유용한 정보를 제공하고자 한다.

Ⅰ. 서 론

현대사회는 다양한 IT기술의 발전으로 영화에서만 보던 첨단 생활이 현실세계에서 가능할 수 있게 진화되고 있다. 특히, 스마트폰의 등장은 사회구성원 모두가 여러 분야에 직·간접적으로 참여할 수 있는 기회를 제공하고 있으며, 여러 편의시설이나 부가서비스들을 자유롭게 이용할 수 있게 되었다. 하지만, 이와 더불어 사용자들의 개인정보보호 노출 및 네트워크를 기반하는 사업체에서 금전적인 위험은 매우 증가되고 있다. 즉, 사용자들이 편한 생활을 추구하는 만큼 다양한 위협요소들이 증가하게 되고, 이런 위협요소들을 제거하기 위한 정보보호기술 개발이 절실히 필요하게 된다. 또한, 독자적인 기술 개발보다는 국가 차원에서의 보안기술과 더 나아가 전 세계적으로 상호운용성이 보장된 보안기술 개발이 필요하게 된다. 따라서 보안기술들 간에 상호운용성 확보를 위한 표준화 활동의 중요성이 증가되고 있는 추세이며, 자국의 고유기술을 국제표준화한 표준특허 발굴이 중요시되고 있다.

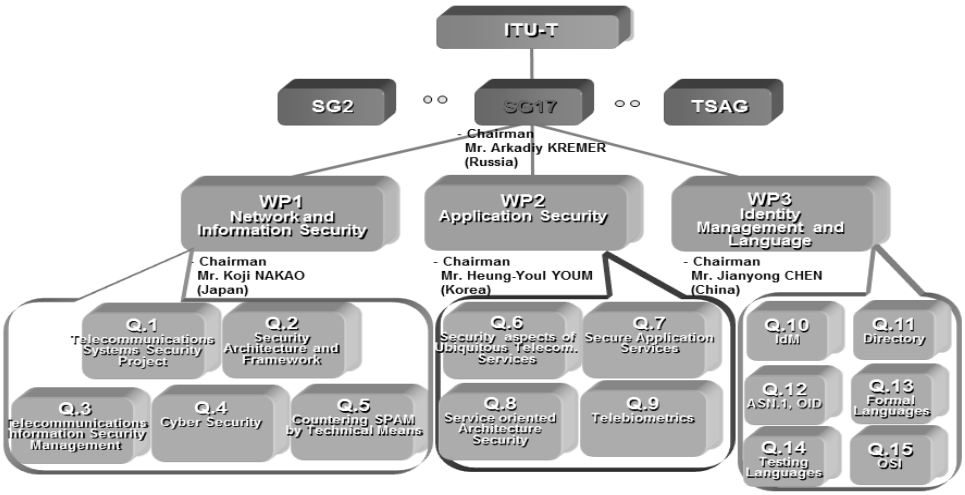
본 논문에서는 정보보호 분야의 대표적인 국제표준화기구에서 논의되고 있는 표준화 활동 현황 및 주요 이슈들에 대해 소개하여, 향후 국내에서 국제표준화기구에 활동하고자 하는 전문가들에게 유용한 정보를 제공하고자 한다.

Ⅱ. ITU-T SG17 국제표준화 현황

1865년 5월에 UN 산하에 신설된 국제전기통신연합(ITU: International Telecommunication Union)에서는 전파규칙, 주파수 할당 등의 이슈를 다루고 있는 전파통신(Radiocommunication), 전기통신기술, 운용 및 요금 등의 이슈를 다루고 있는 전기통신(Telecommunication), 개발도상국의 통신망 현대화를 위한 정책, 기술적 지원 등을 다루고 있는 전기통신개발(Development) 부분으로 크게 3가지로 구분된다. 이중에 정보보호 분야는 ITU-T 산하 SG17(Study Group 17)에서 다루고 있으며, 3개의 WP(Working Party)를 구성하여 국제표준을 개발하고 있다. SG17에서 다루고 있는 세부 연구과제(Question)들의 표준화 연구영역은 그림 1과 같이 나누어서 진행되고 있다.

한국은 SG17에서 매 국제회의 때마다, 약 40% 이상의 기고서를 제안 및 채택하고 있으며, SG17 부의장(염흥열 교수) 등 다수의 의장단과 에디터들이 적극적으로 활동하고 있으며, 국제적으로 매우 활발한 국가로 인지

* 한국정보통신기술협회 표준화본부 ({hroh, jspark, bmchin}@tta.or.kr)
** 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr)



〔그림 1〕 ITU-T SG17 조직도

도가 높이 평가받고 있다[1, 17].

2.1. 정보통신시스템 보안 프로젝트(Q.1)

연구과제(Question) 1에서는 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 담당하고 있다. 또한, Q.1은 연구반(Study Group) 내 또는 연구반 간의 정보보호 표준화 활동 영역을 조정하는 역할을 수행하고 있다. 주요이슈는 전 세계 표준화단체에서 개발된 보안 표준들을 조사하여, 이중에 산업체에 실제 적용 가능한 "순위 100(Top 100)" 표준들을 선별하는 작업이 진행 중에 있으며, 현재 ITU-T 각 그룹 및 보안 표준들을 개발하고 있는 주요 SDOs(Standard Development Organization)들에게 후보 표준 추천 및 해당 기준에 대한 자문을 구하는 협력문서(Liaison)를 발송하였다.

2.2. 보안구조 및 프레임워크(Q.2)

연구과제 2에서는 보안시스템의 구조, 모델, 개념, 전반적인 서비스 시나리오 등을 연구하고 있으며, 가장 대표적인 것은 X.800(OSI 모델) 시리즈 표준들이 가장 대표적이다. 주요이슈는 2010년 12월, 러시아의 제안으로 "개도국을 위한 국가네트워크보안센터" 표준초안을 개발하기로 합의한 사항이며, 이는 국가별 규제와 관련된 사항으로 영국, 미국, 캐나다, 일본 등의 반대에도 불구하도 최종 SG17 총회에서 승인되었다. 본 표준초안은 국가네트워크보안센터 내의 기능구조(기능 블럭 등)와 센터 하부 각 주체(ISP, 분야별 네트워크보안센터)들 간의 구조를 정의할 예정이며, 향후 여러 국가들의 찬반 논의가 계속해서 진행될 것으로 예상된다. 또한, 한국 주도로 데이터통신망에서 확산 가능한 인증 방식에 대한 개정안(X.1034 Revision)도 지난 12월 회의에서 승인되어 국가별 의견수렴을 통해 2011년 2월 국제표준으로 최종 채택되었다.

2.3. 보안관리(Q.3)

연구과제 3에서는 정보통신 시스템을 위한 보안관리 표준들을 개발하고 있으며, 현재 2008년 2월에 개정된 정보보호관리시스템(X.1051: ISMS-T) 표준을 기반으로 보안관리 거버넌스 프레임워크, 중소기업 정보통신기관을 위한 정보보호 관리 가이드라인 등의 표준초안들이 개발되고 있다. 특히, 보안관리 거버넌스 프레임워크는 ISO/IEC JTC1/SC27/WG1 그룹과 공통표준(Common Text)으로 표준초안이 개발되고 있다.

2.4. 사이버보안(Q.4)

연구과제 4에서는 인터넷 및 네트워크 시스템 등에 발생할 수 있는 침해사고대응방법, 보안솔루션, 사이버 보안 취약점들에 대한 해결방법 및 정보공유 방법 등에

대해 연구하고 있다. 주요이슈는 2009년 6월, 미국과 일본의 제안으로 개발을 착수한 사이버보안 정보교환 프레임워크(X.cybex) 표준초안이 2010년 12월, SG17 총회에서 국가별 의견수렴(TAP)으로 승인되었으며, 2011년 4월, 차기회의에서 최종 채택될 예정이다. 해당 국제표준은 사이버범죄 및 사이버공격 등이 발생할 때, 유관 기관이나 국가들 간에 사이버정보를 공유 및 교환함으로써 중복적인 노력 방지와 신속한 대응이 가능할 것으로 예측된다. 본 표준초안의 핵심은 정보공유를 위한 전반적인 프레임워크를 담는 것이며, 세부적인 기술 관련 표준초안들은 공통 취약점 탐지 및 대응기술, 취약점 평가기술, 상호교환 메시지 포맷 및 프로토콜, 보안정책, 침해사건 탐지 방법 등 약 30건의 추가적인 표준초안들이 개발 중에 있다. 또한, 한국은 봇대응시스템인 DNS 싱크홀 방식을 제안하여, 2010년 12월 회의에서 X.1205 Supplement 8로 국제표준이 최종 채택되었다. 추가적으로 한국은 국가정보보호지수와 연관되는 사이버보안지수, IP 역추적 메커니즘, 웹을 통한 악성코드 방지 등의 표준초안들도 주도적으로 개발하고 있다.

2.5. 기술적인 방법에 의한 스팸대응(Q.5)

연구과제 5에서는 한국과 중국을 중심으로 스팸대응을 위한 표준화를 연구하고 있으며, 크게 e-mail에 의한 스팸과 IP 멀티미디어 서비스에 의한 스팸, 단문서비스(SMS) 스팸을 분리하여 표준들을 개발하고 있다. 주요이슈는 한국을 중심으로 개발된 VoIP 스팸대응 표준초안이 2011년도 4월, SG17 총회에서 국가별 의견수렴으로 승인을 앞두고 있으며, 그 외 한국에서 제안된 봇넷에 의해 전송되는 악성스팸 대응기술과 중국에서 제안한 모바일 네트워크에서의 메시지 스팸 대응기술 표준초안들이 개발 중에 있다.

2.6. 유비쿼터스 통신서비스 보안(Q.6)

연구과제 6에서는 통신서비스 관점에서 IPTV 보안, USN 보안, 모바일 보안, 멀티캐스트 보안 등을 중점적으로 다루고 있다. 특히, IPTV 보안에서는 2009년 2월, ITU-T 최초로 "X.1191 : IPTV 보안적 측면을 위한 기능요구사항 및 구조" 국제표준을 채택한 후, 한국을 중심으로 트랜스코더블스킴, 키관리, 디스크램블링 알고리즘, 콘텐츠 상호운용성, 모바일 환경에서 안전한 다운로더블 SCP(Service and Content Protection) 프레임워크, IPTV 서비스를 위한 암호 알고리즘 선택에 대한 가이드라인 표준초안들이 개발되고 있다. 또한, USN 보안에서는 한국을 중심으로 ISO/IEC JTC1/SC6/WG7 그룹과 Common Text로 개발하고 있는 USN 보안 프레임워크 표준초안과 USN 미들웨어 보안, WSN 라우터 보안이 개발되고 있다. 이들 표준초안 중에 2010년도 12월, SG17 총회에서 승인된 IPTV 보안 콘텐츠 상호운용성은 X.1195, USN 보안 프레임워크는 X.1311, USN 미들웨어 보안은 X.1312 국제표준으로 2011년도 2월에 최종 채택되었다.

2.7. 안전한 응용서비스 보안(Q.7)

연구과제 7에서는 P2P 보안, 웹서비스 보안, 응용프로토콜 보안 등을 중점적으로 다루고 있다. 주요이슈는 중국의 제안으로 P2P 보안 분야에 사용자 노드와 코어 노드 간에 인증 절차 및 메커니즘에 대한 표준초안이 개발 중에 있으며, 2011년 2월 한국 주도로 개발되고 있는 OTP(One Time Password) 인증서비스 관리 프레임워크 표준초안이 X.1153 국제표준으로 채택되었다.

2.8. SoA 보안(Q.8)

연구과제 8에서는 SoA(Service-oriented Architecture) 기반의 인증 및 서비스보안 등을 다루고 있다. 주요이슈는 2010년 4월 중국의 제안으로 클라우드 컴퓨팅 보안 분야의 표준초안을 FG on Cloud Computing 그룹과 협력하여 개발키로 하였다. 현재, 클라우드 기반의 정보통신 서비스 환경을 위한 보안요구사항 및 프레임워크, 정보통신 영역에서의 클라우드 컴퓨팅을 위한 보안 가이드라인, 가상네트워크를 위한 안전한 서비스 플랫폼 프레임워크 등의 표준초안 3건이 진행될 예정이다.

2.9. 텔레-바이오인식(Q.9)

연구과제 9에서는 네트워크 환경에서 바이오정보를 응용하기 위한 표준초안들을 개발하고 있다. 현재, 한국은 원타임 템플릿 기술, 텔레헬스 및 텔레매더슨, 다중 바이오정보 보호 가이드라인 등의 표준초안을 개발하고 있으며, 프랑스에서는 텔레헬스를 위한 프로토콜 및 용어 표준초안, 일본은 텔레-바이오인식 템플릿 보호기술

평가를 위한 가이드라인 표준초안을 개발하고 있다. 특히, 2010년 12월 한국의 제안으로 바이오 하드웨어 보안모듈을 이용한 텔레-바이오인식 인증 프레임워크 표준초안을 신규로 개발하기로 하였다.

2.10. 아아덴티티 관리 및 메커니즘(Q.10)

연구과제 10에서는 아이덴티티(Identity)에 대한 관리 기술과 이들을 기반한 인증 및 서비스들에 대한 표준들을 개발하고 있다. 주요이슈는 2010년 4월, 미국의 제안으로 OpenID와 CardSpace의 통합 모델을 위한 오픈 아이덴티티 신뢰 프레임워크 표준초안을 개발키로 하여, 국내에서 활용되고 있는 OpenID와 밀접한 관련이 있어 지속적인 대응이 요구된다. 현재, 한국은 아이덴티티 관리시스템을 위한 보안 가이드라인, IdM에서 사용자 식별정보에 대한 보호등급 평가기준, 모바일 아이덴티티 관리 표준초안들을 개발하고 있다.

2.11. 정보통신 언어 및 시험방법론(Q.11~15)

연구과제 11~15에서는 ITU 공식 언어 ASN.1(추상구문기법 1), 객체식별자등록(OID), 과거에 제정되었던, ITU-T X.500 series, E series, F series 표준들에 대한 유지보수, 시험언어 TTCN 표준들에 대한 유지보수가 논의되고 있다.

Ⅲ. ISO/IEC JTC1 SC27 및 SC37 국제표준화 현황

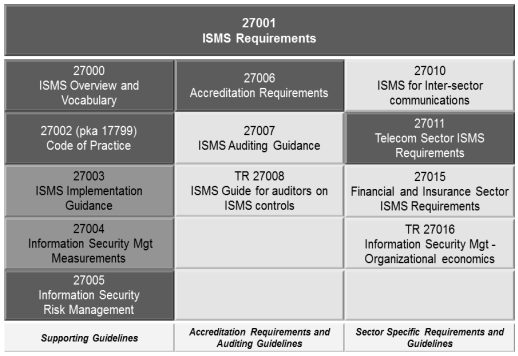
ISO(International Organization for Standardization)/IEC(International Electrotechnical Commission) JTC1(Joint Technology Committee 1)은 정보처리시스템에 대한 국제표준화 위원회(ISO/TC97)와 정보기기에 대한 국제표준화 위원회(IEC/TC83)를 통합하여 1987년에 설립된 공동기술위원회 조직이다.

3.1. 정보보호기술(SC27)

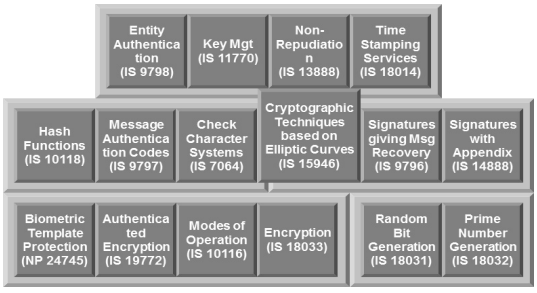
JTC1 산하 SC27(Sub-Committee)에서는 정보통신 보안기술에 대한 국제표준화가 연구되고 있으며, 산하 5개의 WG(Working Group)을 구성하여, 정보보호 원천기술들을 중심으로 표준들을 개발하고 있다[2, 18].

- WG1(정보보호관리시스템) : ISMS 이슈들에 대한 가이드라인 표준과 이를 기반한 서비스 적용 표준들을 개발
- WG2(암호 및 보안 메커니즘) : 보안서비스 구현을 위해 적용되는 보안기술과 암호알고리즘에 대한 표준들을 개발
- WG3(보안평가기준) : IT 보안성 보증 및 평가에 관한 표준들을 개발하고 있으며, 공통평가기준의 범위를 확장하여 인적, 관리적 부분을 평가하기 위한 표준화가 추진
- WG4(보안제어 및 서비스) : 정보보호 시스템들의 접근제어 및 권한 관리를 위한 네트워크 보안과 사이버보안 등의 표준들을 개발
- WG5(아이덴티티 관리 및 프라이버시 보호 기술) : ITU-T SG17과 협력하여, ID 관리 기술 및 네트워크 환경에서의 프라이버스 보호 기술들에 대한 표준들을 개발

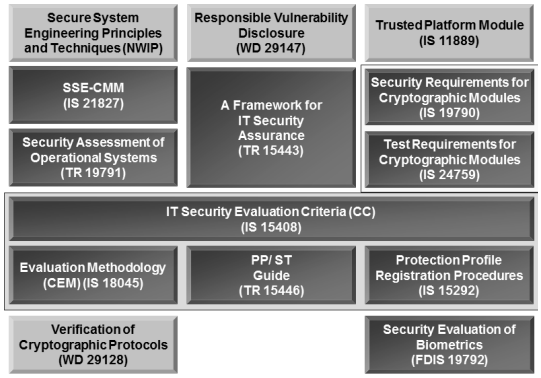
SC27 산하 각 WG에서 개발된 주요 표준들을 기능별로 분류하면 다음의 그림들과 같다.



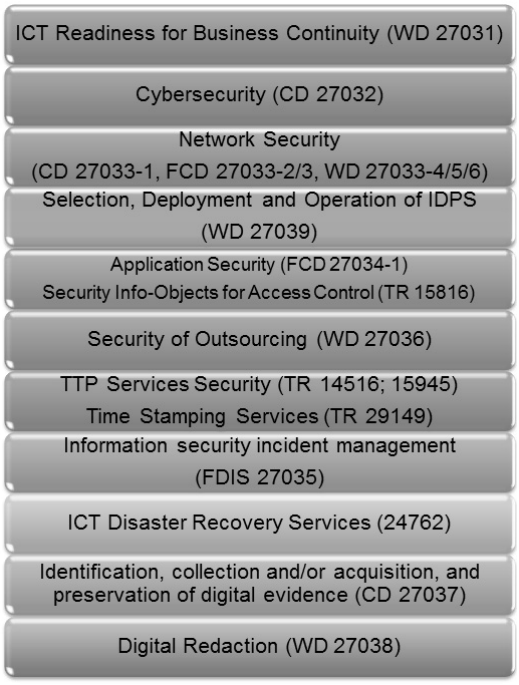
〔그림 2〕 정보보호 관리 시스템(ISMS) 표준



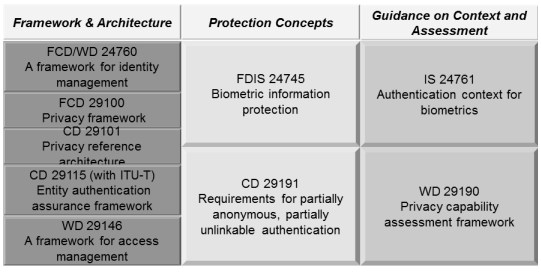
〔그림 3〕 암호기술 표준



〔그림 4〕 보안성 평가 기술 표준



〔그림 5〕 네트워크 보안기술 표준



〔그림 6〕 아이덴티티 및 프라이버시 표준

2010년 10월, SC27 베를린 국제회의에서의 주요이슈로 WG1에서는 한국 주도로 개발되고 있는 정보보호 거버넌스(CD 27014, with ITU-T Q.3) 표준초안에 대해 WD 단계에서 CD 단계로 넘어가기 위한 투표건이 있었으며, 오스트레일리아, 미국 등의 반대에도 불구하고 다수의 찬성을 얻어 CD 단계로 통과되었다. 향후, 본 표준은 ITU-T와 협력하여 Common Text로 개발될 예정이다. WG2에서는 암호알고리즘에 대한 국제표준 선정기준을 개발하자는 이슈가 제기되었다. 즉, 암호알고리즘의 안전성, 효율성, 활용성, 적절성 등을 고려하여 국제표준에 포함시킬 수 있는 알고리즘들을 제한하자는 의지가 포함되어 있다. 한국은 국산 암호알고리즘 SEED, HIGHT와 밀접하게 관련된 사항으로 암호알고리즘 국제표준화를 위한 국가별 설문조사 답변서를 학계, 연구소 등 국제표준전문가들 간에 협력하여, 국내에 불이익이 발생하지 않도록 적절한 답변서를 제출할 계획이다. WG3에서는 암호 프로토콜의 검증방법이 FCD 29128 단계로 진행되었으며, 시스템 평가 기술에 대한 새로운 Study Period(준비 기간)가 신설되었다. WG4에서는 한국의 제안으로 침해사고 관리 표준(27035)의 부족한 부분인 침해사고대응조직 신설 절차와 조직 구성원이 가져야 할 요건 등의 내용을 위한 "CSIRT (Computer Security Incident Response Team)를 위한 운영 및 구현"에 대한 신규 표준화 아이템 제안을 위한 Study Period을 제안했으며, WG4 회의를 걸쳐 새로운 Study Period가 승인되었다. 또한, 한국 주도의 네트워크 보안 파트 4(ISO/IEC 27033-4, 보안게이트웨이)의 표준화 작업도 순조롭게 진행되었다. WG5에서는 한국 주도로 약 5년 동안 개발되고 있던 바이오정보 보호 기술(24745)이 FDIS 단계로 승인되었다. 이는 국내 바이오인식 기반한 정보보호 기술이 국제표준으로 인정받았다는데 큰 의의가 있다. 또한, WG5의 아이덴티티 관리 이슈는 ITU-T SG17과 Common Text로 개발되고 있는 엔티티 인증 보증(Entity Authentication Assurance) 표준초안이 두 조직 간에 견해 차이로 표준초안 완료까지 장기간의 시간이 소요될 것으로 예상된다.

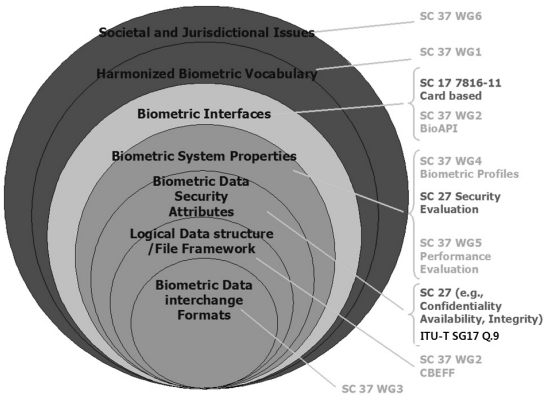
3.2. 바이오인식기술(SC37)

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 테러사건 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.

- 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 시험기술에 대한 표준 개발
- WG6 : 개인 고유정보인 바이오정보에 대한 법제도적 요구조건 및 프라이버시 관련 표준 개발

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



〔그림 7〕 바이오인식 분야 국제표준화 연구영역

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. 또한, ISO/IEC TR 29198(지문영상 DB의 난이도 특성 평가 기술) 기술보고서를 2008년 12월에 채택시켰다[13].

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 이슈는 보안그룹(Security Area)에서 담당하고 있으며, 산하에 총 14개 실무반을 구성하고 있다. 보안 그룹에서 주로 담당했던 분야로는 인증, 암호, ID 관리, 응용프로토콜, IPv6, PKI, 인터넷침해대응솔루션, VoIP, SIP, 웹서비스, P2P, 멀티캐스트 보안, S/MIME 등의 인터넷과 관련된 보안기술들을 표준화 하고 있다. 현재 총 14개의 실무반은 다음과 같으며, 주요 연구영역은 다음과 같다[3, 19].

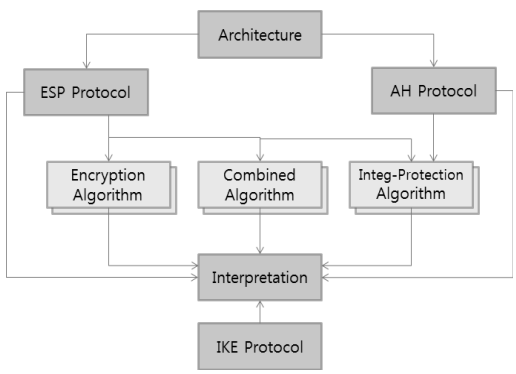
- abfab(Application Bridging for Federated Access Beyond web) : 웹환경에서 다중 도메인들을 연계하기 위한 ID 공유나 정보공유에 활용되는 프로토콜 개발
- dane(DNS-based Authentication of Named Entities) : DNS 기반 엔티티들의 인증서비스를 위한 메커니즘 관련 표준 개발
- dkim(Domain Keys Identified Mail) : 인터넷 이메일 서비스와 같은 도메인 간에 활용될 수 있는 보안 표준 개발
- emu(EAP Method Update) : EAP 프로토콜(RFC 3748)과 EAP 메소드를 위한 IEEE 802.11 요구사항을 충족시키기 위한 보안 표준 개발
- hokey(Handover Keying) : 모바일 기기의 이동성 지원을 위한 메커니즘 표준 개발
- ipsecme(IP Security Maintenance and Extensions) : IPSec 프로토콜의 유지보수 담당
- isms(Integrated Security Model for SNMP) : SNMPv3를 위한 단일화된 보안 모델 개발
- kitten(Common Authentication Technology Next Generation) : 인터넷 상에서 전달되는 메시지 및

해당 문맥을 보호하기 위한 API 표준을 개발

- krb-wg(Kerberos) : 커버로스 사용자 인증 시스템(Version 5)의 안전·편의성 제고 및 키관리 방법 개발
- ltans(Long-Term Archive and Notary Services) : 장시간 동안 상용될 수 있는 데이터 기록방법 및 보관 방법을 위한 보안 표준 개발
- msec(Multicast Security) : 인터넷 상에서 다수의 사용자에게 데이터를 안전하게 전송할 수 있는 멀티캐스트 보안 표준 개발
- nea(Network Endpoint Assessment) : 네트워크 보안 정책에 따라 종단에 존재하는 사용자 및 장비들의 보안성 지원을 위한 평가기술 개발
- pkix(Public-Key Infrastructure (X.509)) : X.509 기반의 PKI 관련 표준화와 서버기반의 인증서 경로검증 프로토콜(DPD/DPV), CMS 기반의 인증서 관리 프로토콜, OCSP 경량 프로토콜 등에 대한 표준 개발
- tls(Transport Layer Security) : '96년도에 개발된 TLS v1.1 프로토콜 개선과 MD5, SHA1 등 해쉬 알고리즘을 제거하고 신규로 개발되는 암호 알고리즘 표준으로 대체하는 작업

한국 주도로 개발된 대표적인 IETF 표준은 SEED 암호알고리즘 및 관련 응용 표준으로 RFC 4269, 4010, 4162, 4196, 5669, 5748 국제표준을 제/개정한 바 있다. 또한, ARIA 알고리즘 관련해서는 RFC 5794 표준과 응용 표준들이 개발 중에 있다.

IETF에서 개발된 많은 인터넷 보안 표준들 중에 활용도가 높고, 잘 알려진 IPSec/IKE 프로토콜의 현황을 살펴보면, [그림 8]과 같은 상호관계를 가지고 있으며, RFC 6071 표준에 상세 항목들에 대해 설명하고 있다.



〔그림 8〕 IPSec/IKE 프로토콜 상호관계

Ⅴ. 기타(지역 및 사실표준화기구)

정보보호와 관련된 가장 대표적인 국제표준화기구는 ITU-T SG17, ISO/IEC JTC1/SC27, SC37, IETF를 꼽을 수 있다. 하지만, 정보보호 기술과 관련하여 지역 간의 협력을 위한 표준화기구들과 특정 기술들에 대한 정보보호 표준 개발 및 정보공유를 위해 운영되고 있는 일부 그룹들이 있어, 본 장에서 간단히 소개하고자 한다[14].

5.1. ETSI

유럽시장의 단일화를 위해 1982년도에 설립된 ETSI (European Telecommunications Standards Institute)은 유선, 무선, 전파, 융합, 방송, 인터넷 기술을 포함한 ICT 전 분야에 대해 다루고 있으며, 특히 GSM 및 3GPP로 이동통신 표준화에서 강점을 보유하고 있다. 현재 ETSI에서 다루고 있는 정보보호기술은 NGN, 이동통신(GSM, TETRA 등), 합법적인 감청, 전자서명, 스마트카드, 암호알고리즘, 비상통신/재난통신, RFID, 양자암호 등을 다루고 있다[4, 20].

5.2. 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 10개의 작업그룹(Working Group)과 8개의 전문가 그룹(Expert Group)으로 구성되어 있으며, 이들 전문가 그룹 중에 한 개가 정보보호 분야를 다루고 있다. 과거 ASTAP에서는 서로 간에 정보공유 및 의견조율만을 목적으로 활동하였으나, 2006년부터 아시아지역을 위한 표준을 개발키로 합의된 바 있다. 현재, 보안 그룹에서는 주로 ITU-T SG17 보안 연구과제들을 중점적으로 대응하고 있다[5].

5.3. 3GPP/3GPP2

이동통신 분야의 가장 대표적인 표준화 기구는 비동기식(GSM) 이동통신 기술을 다루고 있는 3GPP와 동기식(CDMA) 이동통신 기술을 다루고 있는 3GPP2 표준화 협의체이다. 본 협의체는 업체나 개인자격으로 참여하는 것이 아니라 표준화 기관(예로 한국 TTA)들 간에 회원사로 운영된다. 3GPP에서는 TSG SA3 그룹에서 보안을 다루고 있으며, 주로 비동기식 시스템을 위한 잠재적인 보안 위협 분석, 성능평가, 보안요구사항, 보안구조 및 프로토콜 등에 대해 표준화를 추진하고 있다. 3GPP2에서는 TSG-S WG4 그룹에서 보안을 다루고 있으며, 주로 동기식 시스템을 위한 암호알고리즘, 보안요구사항, 브로드캐스트 및 멀티캐스트 서비스를 위한 보안기술 등에 대한 표준화가 진행되고 있다[6, 7, 22].

5.4. IEEE

IEEE는 컴퓨터, 정보통신, 무선 네트워크 및 휴대인터넷 등의 표준화를 개발하는 협의체로 전 세계 개인회원으로 구성된 비영리 기술전문 단체이다. 본 협의체는 주요 기술이나 핵심 테마별로 프로젝트(Project)를 구성하여 표준을 개발하고 있으며, 가장 대표적인 프로젝트로는 IEEE 802 LMSC(Institute of Electrical and Electronics Engineers Lan Man Standards Committee) 그룹이다. 본 그룹은 1980년 2월 1~20MHz 속도가 가능한 LAN 환경 구축을 목적으로 신설되었으며, 대표적으로 IEEE 802.3(이더넷), IEEE 802.11(무선랜), IEEE 802.16(휴대인터넷), IEEE 802.22(WRAN) 분야에 많은 전문가들이 참석하여 표준들을 개발하고 있다. 현재 IEEE에서 보안 이슈는 각 프로젝트 별로 다루고 있으며, 프로젝트 성격에 따라 독립적인 보안 워킹 그룹을 구성하거나 이슈별 워킹 그룹에서 보안도 함께 다루고 있다[8].

5.5. OASIS

OASIS(Organization for the Advancement of Struc-tured Information Standards)는 1993년 SGML Open이라는 이름으로 설립되어 1998년도에 OASIS Open으로 변경된 비영리 국제 컨소시엄이다. 주요 담당 표준으로는 e-비지니스 분야에서의 요구되는 표준들을 개발하고 있으며, 특히 ebXML, 웹서비스, 보안, 상호운용성, 비즈니스 트랜잭션 등의 표준들을 개발하고 있다. OASIS에서 개발된 보안 표준들은 활용성이 높은 XML 기반의 전자서명, 암호화, 접근제어, 키관리, SAML 등을 예로 들 수 있으며, 현재는 웹서비스나 클라우드 환경에서의 아이덴티티 관련 식별자 관리 기술 등의 표준 개발이 활발히 진행되고 있다[9, 21].

5.6. W3C

W3C(World Wide Web Consortium)는 웹 표준을 개발하는 사실표준화기구로서, 1994년 10월 웹의 창시자인 팀 버너스리에 의해 설립되었다. W3C는 웹서비스를 지원하기 위한 XML 관련 표준들을 중점적으로 개발하고 있으며, 실제 웹에 대한 설계나 구조, 검색기능, 웹 기반 응용서비스나 관련 디바이스, 브라우저와 유용한 툴 등 웹과 관련된 전반적인 표준을 개발하고 있다. 특히 스마트폰의 등장으로 모바일 웹에서의 금융결제나 다양한 부가서비스와 관련된 표준들을 중점적으로 다루고 있다. 현대사회가 웹을 기반으로 다양한 서비스가 발굴되고 있어, 특히 금융사고 방지, 안전한 콘텐츠 유통 보호, 사용자들의 프라이버시 보호 등을 위해 정보보호 관점에서도 W3C에서 개발된 표준들을 꼭 눈여겨 봐야한다[10].

5.7. RAISE 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 RAISE(Regional Asia Information Security Exchange) 포럼이 신설되었으며, 2010년 3월까지, 총 8회의 정기회의를 개최하였다. 본 포럼은 초기 싱가포르에서 사무국 역할을 담당하였으나, 제8차 정기회의에서 사무국을 말레이시아에서 담당하는 것으로 변경하였고, 2011년도 내에 대만에서 제9차 정기회의가 개최될 예정이다. 참여하고 있는 주요 국가로는 중국, 일본, 한국, 말레이시아, 뉴질랜드, 싱가포르, 태국, 대만 등을 중심으로 매 회의 때마다 25~30명의 전문가들이 참석하고 있다. 한국은 국내에서 개발되어 활용되고 있는 ISMS 체계, i-PIN, 사이버보안, IdM 기술 등을 소개한 바 있으며, 한국 ISMS에 기반한 표준이 RAISE 표준으로 채

택된 사례도 있으며, 한국의 정보보호 기술이 아시아 국가들에게 중요한 가이드라인 문서로 활용되고 있다[11].

5.8. CJK SWIS

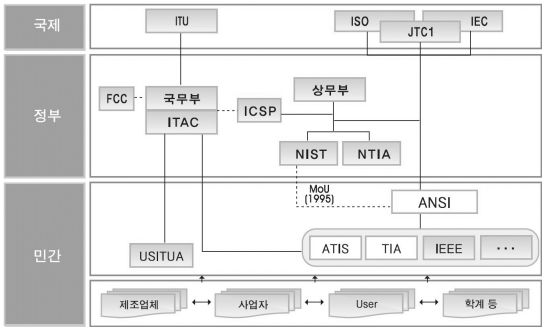
2007년 10월, ITU-T SG17에서 활동하고 있는 정보보호 표준화 전문가들을 중심으로 한중일 간에 정보보호 표준화 이슈 공유 및 SG17 국제표준화 활동에 공동 대응을 위해 CJK(China, Japan, Korea) SWIS (Standardization Workshop on Information Security) 협의체를 신설하였다. 현재까지 총 4회에 걸쳐 한중일 간에 워크숍을 개최하였으며, 매 워크숍 마다 각 국가에서 개발된 최신 정보보호 기술 현황, 표준화 전략, 표준화 현황 등을 소개하고 협력 방안을 강구하고 있다. 본 협의체는 2011년도 11월, 일본 워크숍을 마지막으로 2012년부터는 한중일 표준협력회의(CJK Standards Meeting) 산하에 정보보호 실무반을 신설하여 공식적인 표준화 활동으로 추진할 계획이다[12].

Ⅵ. 주요 국가별 표준화 추진체계 분석

6.1. 미국

미국은 민간의 자율적 표준화 활동을 강조하고 있으며, 대표적으로 1995년에 국가기술이전진흥법을 제정하여 "연방 행정기관은 민간의 표준화기구에서 채택한 표준을 사용"하도록 하면서 정부기관의 민간표준화 활동 참여를 강조하고 있다. 즉, 정부부문은 상무부 산하 기관인 NIST(National Institute of Standards and Technology)에서 담당하고 있으며, 민간부분은 ANSI (American National Standards Institute), ATIS (Alliance for Telecommunications Industry Solutions), TIA(Telecommunications Industries Association) 등을 중심으로 이루어지고 있다. 미국 산업체들의 강점을 살기 위해 IETF, IEEE 등의 사실표준화기구 활동에 중점을 두고 있다.

미국의 국제표준화 전략은 국제적으로 수용된 원칙을 적용, 기술규정 및 조달을 위해 추가 규격 개발보다는 민간표준을 활용, 시스템에 적용함에 있어 포괄적이고 유연한 표준 개발, 국제적 필요성에 부합하는 표준화 활동, 국제 경제를 위해 표준 배포 강화이다. 국내표준



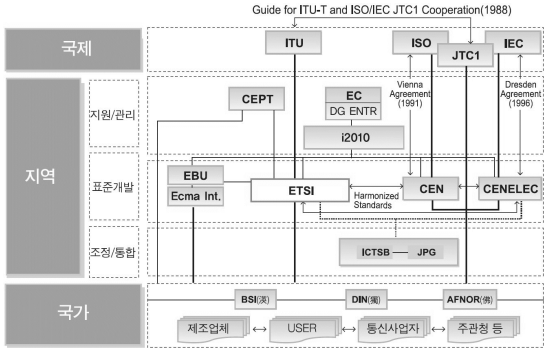
〔그림 9〕 미국의 표준화 추진체계

화 전략은 모든 이해당사자들이 참여한 단일화된 표준 개발, 중복 투자 방지, 공공 및 민간 부분의 표준화 활동 강화를 위한 지원 강화, 자국 및 국제적 필요에 부합하는 표준 개발이라는 전략으로 표준을 개발하고 있다.

6.2. 유럽

유럽의 표준화 추진체계는 유관 기구간의 상호 협력체계를 기본으로 독립기구, 국가별 기구, 국제기구와의 협력체계로 구분될 수 있다. 즉, 3개의 유럽 표준화 기구 CEN(European Committee for Standardisation), CENELEC(Erupean Committee for Electrotechnical Standardisation), ETSI 들을 중심으로 협력체계를 구축하고 있으며, 이들을 조정하기 위한 JPG(Joint Presidents Group)와 JCG(Joint Coordination Group) 조직과 3개의 표준화 기구에서 개발된 기술 규격을 배포하기 위한 ICTSB(Information and Communications Technologies Standards Board)로 구성되어 있다.

유럽의 국제표준화 전략은 1996년에 "표준화와 글로벌 정보사회" 지령을 기반으로 ISO, IEC, ITU 등 국제

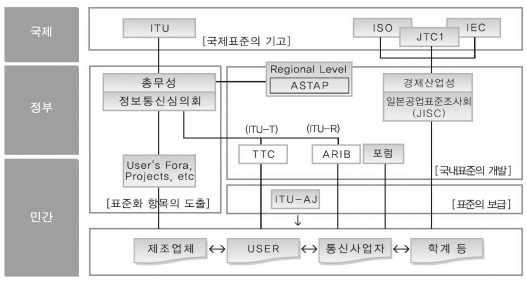


〔그림 10〕 유럽의 표준화 추진체계

표준화 활동에 참여하고 있는 유럽국가 간에 CEN, CENELEC, ETSI에서 유럽표준을 마련한 후, 일관된 의견으로 국제표준화를 추진하도록 상호 협력약정을 맺고 있다. 또한, 전 세계 국제표준화기구에 의장단 진출이나 표준안 작성에 실질적인 영향을 행사할 수 있는 에디터쉽 확보에 총력을 기울이고 있다. 국내표준화 전략은 연구개발과 표준화의 연계, e-Europe 2005 및 i2010을 통한 유럽정보사회 기반 조성과 표준화 연계, 유럽의 정보통신 정책 기반의 표준화, 유럽연합 정보통신표준화의 현대화를 목적으로 전략을 수립하고 있다.

6.3. 일본

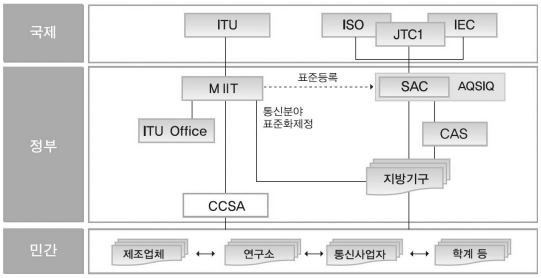
일본의 표준화 추진체계는 ITU, ISO, IEC 등 국제표준화기구에 대응하는 정부부문과 실적적인 표준화 작업을 추진하는 민간부문으로 나뉘어 있다. 일본의 국가표준은 JISC(Japanese Industrial Standards Committee)에서 심의하지만, 구체적인 표준 개발과 고시는 7개 각 성에서 수행한다. 특히, 정보통신 분야는 총무성을 중심으로 추진되고 있다. 일본의 국제표준화 전략은 다양한 프로그램과 추진계획 발표에서 많이 알려졌으며, 2008년 6월, 총무성에서는 "ICT 분야 국제표준화 전략"으로 국제표준화 전략 수립, 국제표준화 인재 육성, 산학연 표준화 활동 강화, 국제표준화 체계 강화로 전략을 발표하였다. 국내표준화 전략은 국제표준화 전략을 실천하기 위한 세부 계획으로 ICT 국제표준화전략 맵 정비, ICT 지적재산권 강화, ICT 특허맵 정비, ICT 표준화 전문가 선정 및 인재 육성, ICT 국제표준화 추진 가이드라인 개발, 기업과 대학 등의 표준화 활동 지원, 표준화단체의 활동 강화와 상호협력 강화, 아시아·태평양 지역의 협력 강화, 지적재산권 센터 설립 등의 세부 추진전략을 수립하여 국제표준화 선점을 목적으로 표준화를 추진하고 있다.



〔그림 11〕 일본의 표준화 추진체계

6.4. 중국

중국의 표준화 추진체계는 정부부분으로 SAC (Standardization Administration of China)에서 산업일반 분야의 표준화를 담당하고 있으며, MIIT(Ministry of Industry and Information Technology)에서 정보통신 분야의 표준화를 담당하고 있다. 민간 차원의 표준 개발은 CCSA(China Communication Standards Association)가 비영리 표준화활동을 담당하고 있으며, CAS(China Association for Standardization)는 국내외 표준화 학술교류, 표준보급 등의 역할을 수행하고 있다.

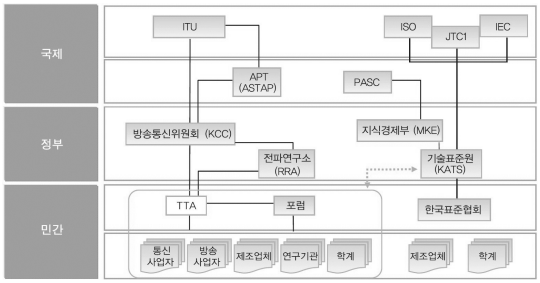


〔그림 12〕 중국의 표준화 추진체계

중국의 국제표준화 전략은 국가 종합국력 발전과 서로 융합되어야 하고, 중국 과학기술 발전 전략의 각 단계 발전 목표와 서로 융합되어야 하며, 국제 규범을 준수해서 공평하고 합리적으로 서로 융합되어야 하고, 중국 시장우위를 활용하여 국제표준화와 연계되어야 함을 목적으로 하고 있다. 국내표준화 전략은 국가 이익과 관련된 중점 국제표준화 항목을 선정하여, 국내표준과 국제표준을 동시에 제정을 목표로 하고 있으며, 향후 중국이 제안하여 채택된 국제표준 건수가 개발도상국 1위를 차지하는 것을 목표로 추진하고 있다.

6.5. 한국

한국의 표준화 추진체계는 크게 국제표준화기구를 중심으로 방송통신위원회에서 ITU 대응과 방송통신 분야에 대한 표준화를 담당하고 있으며, 지식경제부에서 ISO, IEC, JTC1 대응과 일반 산업 분야에 대한 표준화를 담당하고 있다. 즉, 민간차원에서 표준개발 및 협력을 한국정보통신기술협회(TTA)와 한국표준협회(KSA)에서 지원하고 있으며, 전파연구소와 기술표준원에서 해당 분야의 국가표준을 관리하고 있다.



〔그림 13〕 한국의 표준화 추진체계

한국의 표준화 추진전략은 국가표준기본법 제7조에 따라 국가표준제도 확립 등을 위하여 5년마다 국가표준기본계획이 수립되어 추진되고 있다. 첫 번째로 국가표준체계 선진화를 위해 부처별 표준·기술기준 간에 중복 및 이원화를 해소하고 시험/검사/인증 등 적합성평가 제도 전반을 국제기준에 부합화하려 노력하고 있다. 두 번째로 표준기술 하부구조 강화를 위해 신제품이나 신기술 개발 지원을 위한 표준 개발에 힘쓰고 첨단산업 발전을 지원하기 위한 참조표준 개발·보급체계 구축 및 법정계량제도의 선진화에 힘쓰고 있다. 세 번째는 국제표준화 대응역량 강화를 위해 국제 경제 환경 변화에 따른 사실 국제표준화 지원 체계 구축과 선진국의 무역장벽 대응을 위한 기업지원에 힘쓰고 있다[13, 14].

Ⅶ. 결 론

본 논문에서는 ITU-T SG17, ISO/IEC JTC1 SC27, SC37, IETF 등의 국제표준화기구들과 지역별 협력체계 강화와 특정 이슈들을 위해 설립된 표준화기구들에서 다루고 있는 정보보호 국제표준화 현황에 대해 간단히 살펴보았다. 또한, 주요 국가별 표준화 추진체계를 간단히 살펴본 결과 대부분의 선진국들은 자국의 기술들을 국제표준으로 발굴하여 표준특허 등을 확보하기 위해 다양한 추진전략 및 협력체계를 국축하고 있음을 확인하였다. 물론, 우리나라도 국내 고유기술을 국제표준화로 추진시키기 위해 많은 예산 투자와 다양한 추진전략을 수립하여 선진국에 발맞추어 전진하고 있지만, 향후 지금보다 더 앞서나가기 위해 양적인 성장보다 질적인 성장을 이룰 수 있는 전략 수립과 산학연 및 정부의 다양한 정책 등 서로 간에 연계될 수 있는 협력 체계가 필요한 시점이라고 생각된다.

참고문헌

[1] ITU-T 홈페이지, http://www.itu.int
[2] ISO 홈페이지, http://www.iso.org
[3] IETF 홈페이지, http://www.ietf.org
[4] ETSI 홈페이지, http://www.itsc.org
[5] ASTAP 홈페이지, http://www.aptsec.org
[6] 3GPP 홈페이지, http://www.3gpp.org
[7] 3GPP2 홈페이지, http://www.3gpp2.org
[8] IEEE 홈페이지, http://www.ieee.org
[9] OASIS 홈페이지, http://www.oasis-open.org
[10] W3C 홈페이지, http://www.w3.org
[11] RAISE 포럼 홈페이지, http://www.itsc.org.sg
[12] CJK SWIS 홈페이지, http://elec.sch.ac.kr/swis 2010/index.php
[13] TTA-10112-SA, ICT 중점기술 표준화전략맵 Ver. 2011 - 정보보호 분야, TTA, 2011. 01.
[14] TTA-010020-SD, ICT 표준화 추진체계 분석서, TTA, 2010.08.
[15] 오흥룡, 진병문, 염흥열, 강신각, "ITU-T SG17 정보보호 국제표준화 동향 및 향후 전망", 정보보호학회지, v.18, no.4, pp. 13-29, 2008.08.
[16] 오흥룡, 염흥열, "정보보호 국제표준화 동향 및 향후 전망", 정보보호학회지, v.17, no.1, pp.63-78, 2007.02.
[17] 염흥열, 오흥룡, 나재훈, 백종현, “ITU 연구동향 : ITU-T SG17 보안 분야”, 한국 ITU 연구위원회 연구동향 보고서, 2010.12. [발간예정]
[18] Walter Fumy, "ISO/IEC JTC1/SC27-IT Security Technique", ITU-T Workshop, Geneva Swiss, 6-7 December 2010.
[19] Tim Polk, “IETF Security Area”, ITU-T Workshop, Geneva Swiss, 6-7 December 2010.
[20] Carmine Rizzo, "ETSI Security Standardization", ITU-T Workshop, Geneva Swiss, 6-7 December 2010.
[21] Anil Saldhana, "OASIS Security Standardization", ITU-T Workshop, Geneva Swiss, 6-7 December 2010.
[22] Markus Wong, "3GPP Security", ITU-T Workshop, Geneva Swiss, 6-7 December 2010.

〈著者紹介〉

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

사 진

박 정 식 (Jeong Sik Park)
정회원

1994년 2월 : 경원대학교 전자공학과 졸업
2001년 8월 : 연세대학교 공학대학원 전파통신공학 석사
1994년 1월~2001년 8월 : 데이콤 근무
2001년 9월~현재 : 한국정보통신기술협회 표준화본부
<관심분야> 이동통신보안

진 병 문 (Byoung-Moon Chin)
정회원

1976년 2월 : 서울대학교 전기공학과 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
2001년~2008년 : ITU-T SG17 Vice-Chairman, WP1 Chairman
2005년~현재 : ITU-T 총괄반 국내 분과위원회 의장
<관심분야> 정보통신표준공학, 정보보호표준, 이동통신표준

염 흥 열 (Heung-Youl Youm)
종신회원

1981년 2월 : 한양대학교 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 : 한국정보보호학회 총무이사, 학술이사, 교육이사, 총무이사, 상임부회장, (현) 회장
2004년 1월~현재 : 한국인터넷정보학회 이사, (현)논문지 편집위원
2003년 9월~2004년 3월 : ITU-T SG17/Q10 Associate Rapporteur
2004년 3월~현재 : ITU-T SG17/Q9 Rapporteur
2008.10 ~현재 : ITU-T SG17 부의장
2009.2 ~현재 : ITU-T SG17 WP2 의장
2006년 11월~2008년 2월 : 정보통신부 정책자문단 정보보호 PM
2006년 11월 ~2009년 2월 : 한국정보통신연구진흥원 정보보호전문위원
<관심분야> 네트워크 보안, 전자상거래 보안, 공개키 기반 구조, 부호이론, 이동통신보안