ISO/IEC JTC1의 국내 정보보호기술 표준화 현황 분석

이승훈*, 박희운*, 신종회*, 이동근*
*한국정보보호진흥원
e-mail: shlee@kisa.or.kr

An Analysis of The Status of Domestic Information Security Technologies In ISO/IEC JTC1

Seung-Hun Lee*, Hee-Un Park*, Jong-Whoi Shin*, Dong-Geun Lee*
*Korea Information Security Agency

요 약

국내 정보통신 기술의 발달은 세계 최고 수준의 인터넷 인프라를 구축하는 기반이 되었다. 하지만 정보통신의 역기능 또한 함께 확대되어온 것이 현실이다. 이러한 역기능을 막기 위해 다양한 정보보호기술들이 개발 및 보급되었고 이러한 상황 속에 국내 정보보호 산업 또한 폭발적으로 성장하게 되었다. 그러나 국내시장을 중심으로 한 정보보호산업의 성장은 한계를 가질 수밖에 없다. 이러한 문제점을 해결하고 국내산업의 국제 경쟁력 강화는 물론 국제시장 선점효과를 높이기 위하여 국제 표준화 추진이 무엇보다 중요한 요소라 할 수 있다. 본 논문은 국제표준화 활동 기구인 ISO/IEC JTC1에서 국내 정보보호 기술의 표준상정 현황을 분석하여 현재 진행되고 있는 정보보호 기술표준 동향을 제공하고 향후, 국제 표준화 과제를 수행하기 위해 필요한 요구사항들에 대하여 기술하였다.

1. 서론

초고속망의 보급에 힘입어 인터넷 사용자수가 폭발적으로 증가하고 있다. 이러한 양적 성장과정에서 각종 보안사고의 발생 빈도수 역시 비례하여 증가하고 있다. 이러한 정보통신 역기능을 막기 위하여 각종 정보보호기술들이 개발되고 보급되어 왔다. 정보보호 기술의 발달은 국내 정보보호산업을 급속도로 발전 시켰다. 하지만, 산업의 성장이 국내 시장을 중심으로 이루어짐에 따라 성장의 한계를 가진다는 문제점이 나타나게 되었다. 이러한 국내 정보보호산업의 문제점을 해결하고 국내산업의 국제 경쟁력 강화는 물론 국제시장 선점효과를 높이기 위하여 국제 표준화 추진이 무엇보다 중요한 요소라 할 수 있다. 본 논문에서는 국제 표준화 기구인 ISO/IEC JTC1에서 현재까지 진행된 국내기술의 국제 표준화 현황을 분석한 후 향후 방향에 대하여 기술하고자 한다.

2. ISO/IEC JTC1 소개

ISO(International Organization for Standardization) /IEC(International Electrotechnical Commission) JTC1은 정보 처리시스템에 대한 국제표준화 활동(ISO/TC97)과 정보기기에 대한 국제표준화 활동(IEC/TC83)을 통합하여 구성된 기술위원회로, 정보기술분야 (Information Technology)의 공동 국제표준화 활동을 위해 1987년에 설립되었다.

주요 활동으로는 일반 정보기술의 표준을 개발하고, 각기 다른 정보기술을 담당하는 ISO와 IEC의 기술위원회를 조정하여 중장기 계획을 세우는 것이다. ISO/IEC JTC1의 표준문서 종류는 다음과 같다.

- 신규과제제안서(NP: New Work Item Proposal)
- 표준초안(WD: Working Draft)
- 분과위원회 표준안(CD: Committee Draft)

- 최종 분과위원회 표준안(FCD: Final Committee Draft)
- 국제표준안(DIS: Draft International Standard)
- 최종국제표준안(FDIS: Final Draft International Standard)
- 국제표준(IS: International Standard)

현재 2개의 Rapporteur Group(RG)과 18개의 Sub Committee(SC)가 활동 중에 있으며, 정보보호기술과 관련된 표준화 활동은 SC27에서, 생체인식기술에 관해서는 SC37에서 담당하고 있다.

2.1 ISO/IEC JTC1/SC27

정보기술 보호를 위한 일반적인 방법과 기술을 표준화하는 SC로서 정보기술 시스템의 보호 요구사항과 서비스, 보호기술 및 메커니즘, 보호지침, 위험분석, 보호 평가 등에 대한 표준개발을 3개의 Working Group(WG)으로 나누어 진행하고 있다.

- WG 1: 요구사항, 보안 서비스, 가이드라인
- WG 2: 보안 기술과 메커니즘
- WG 3: 보안 평가 기준

2.2 ISO/IEC JTC1/SC37

생체인식기술에 대한 표준화를 수행하는 SC로서 지문인식, 얼굴인식, 음성인식, 서명인식, 홍채인식 등과 관련된 데이터 형식과 응용 프로그램 인터페이스를 포함한 유전 생체인식기술을 6개의 Sub Group (SG)으로 나누어 추진하고 있다.

- SG 1: 생체인식 용어
- SG 2: 생체인식기술 인터페이스
- SG 3: 생체인식 데이터 교환 형식
- SG 4: 생체인식 응용기술
- SG 5: 생체인식 시험평가
- SG 6: 법령 및 사회적 영향평가

3. 국내기술의 표준상정 현황

현재까지 ISO/IEC JTC1/SC27에 표준으로 제정 또는 상정되어 있는 과제는 총 62건으로 이중 3건의 국내기술이 상정되어 있고 1건이 표준으로 제정되어 있다. ISO/IEC JTC1/SC37의 경우 위원회 설립이 2002년 12월에 있었던 관계로 새로운 과제들이 계속 제안되고 있으며, 그중 국내기술은 총 1건이 상정되어 있는 상태이다. 각 기술의 표준화 상태 및 해당 SC는 표 1과 같다.

표1. ISO/IEC JTC1/SC27 및 SC37의 국내기술

1	SEED	CD	SC 27
2	AMP	WD	SC 27
3	C2C-PAKA	WD	SC 27
4	BioAPI 표준적합성 시험도구	NP	SC 37
5	부가형 전자서명 방식 표준(EC-KCDSA)	IS	SC 27

3.1 SEED

SEED[1]는 대칭키 암호알고리즘으로써, 블록 단위로 메시지를 처리하는 블록 암호알고리즘이다. 암호알고리즘의 ISO/IEC 국제표준화가 공모방식으로 전환된 후, 국내에서는 공청회를 통해 '02년 10월에 SEED를 ISO/IEC의 표준으로 상정하였다.

2002년 10월 폴란드 바르샤바에서 개최된 ISO/IEC 국제표준회의에서 1차 CD에 포함될 블록암호알고리즘으로 64비트 5개, 128비트 4개를 선정하였으며 국내암호알고리즘인 SEED도 1차 CD에 포함되었다. 2003년 4월 캐나다 퀘백회의에서는 후보기술에 대한 안전성 및 효율성 평가결과를 발표하였으며 그 결과를 기초로 2차 CD에 포함될 블록암호알고리즘으로 64비트 5개, 128비트 3개를 선정하였다. 향후, ISO/IEC JTC1/SC27/WG2 제27차 국제표준회의는 2003년 10월 프랑스 파리에서 개최될 예정으로 FCD에 포함될 블록암호알고리즘을 선정할 것이다. 파리회의에서 선정된 알고리즘들은 FDIS를 거쳐 국제표준(IS)로 최종선정될 예정이어서 국내기술인 SEED가 국제표준으로 선정되는데 있어 가장 중요한 회의가 될 것으로 예상된다.

3.2 AMP

AMP[2]는 통신 양자간에 패스워드 기반 인증 및 세션키 생성이 가능하도록 하기위해 제시된 프로토콜이다. AMP는 IEEE의 표준인 P1363.2에 SPEKE, SRP와 같이 포함되어 있는 4-pass 프로토콜로서, 상대적으로 효율적이고 구축이 간단한 장점

을 갖고 있다.

따라서 P1363.2와 유사한 국제표준인 ISO/IEC JTC1/SC27 11770-4 Key establishment mechanisms based on weak secrets에 AMP를 포함하는 것이 적절하다는 판단하에 한국정보보호진흥원에서는 이를 제26차 ISO/IEC JTC1/SG27/WG2회의에서 국제표준으로 상정하였다. 11770-4는 2003년부터 신규표준화 과제로 추진되고 있으며, SRP가 1차 WD에 포함되어 있었다. 이에 제26차 퀘벡 회의에서 AMP를 신규 표준화 대상 항목으로 상정하고, SRP 및 기타 방식들과의 차별성을 주장하였다. 현재 AMP는 2차 WD에 포함되어 있으며, 안전성·효율성 분석 자료 및 SRP보다 우수한 점을 문서화하여 각 국에서 회람하고 있다. 회람 결과는 제27차 파리회의를 통해 검토될 예정이며, 이에 따라 표준화 방향이 결정될 것이다.

3.3 C2C-PAKA

C2C-PAKA(Client-to-Client Password- Authenticated Key Agreement)[3]는 사전 공유 비밀정보 없이 2개의 서로 다른 패스워드에 기초한 클라이언트간 Password Authorization Key Agreement를 제공하는 프로토콜이다.

C2C-PAKA는 2003년 4월에 있었던 제26차 ISO/IEC JTC1/ SG27/WG2에서 한국이 신규로 ISO/IEC JTC1/SC27 11770-4 Key establishment mechanisms based on weak secrets에 제안한 프로토콜이다. 제26차 회의에서는 서로 다른 도메인간 키 생성 및 인증을 제공하는 C2C-PAKA를 신규 카테고리로 추진하는 것에는 동의하였으나, 제안 프로토콜에 대한 각 국의 사전 검토 부족으로 다음 회의 전까지 특허, 안전성 및 효율성 분석 자료 등을 각 회원국에 회람시키기로 하였다. 당초 1차 WD문서를 1차 CD문서로 처리하려 하였으나 한국의 신규 카테고리 제안에 대한 의견을 수렴하여 2차 WD로 하기로 결의하였다.

3.4 BioAPI 표준적합성 시험도구

BioAPI 표준적합성 시험도구[4]란 BioAPI ver1.1에 대한 준용성 여부를 판단하기 위한 시험규격으로 BioAPI에 명시된 필수 및 선택함수의 입력변수 및 반환 값을 확인하는 등, 시험기준을 검증하는 시험도구에 대해 기술하고 있다.

2002년 12월에 미국에서 열린 ISO/IEC JTC1 SC37(생체인식) 국제표준화 창립총회에서 정통부 국책과제인 "Biometric 인증시스템 보안성 평가기술 개발"에 일환으로 수행된 "BioAPI 표준적합성 시험도구" 연구사례를 발표하였으며, 이를 국제 표준으로 제안하였다.

2003년 4월 캐나다에서 개최된 SC37 국제표준화 실무자회의에서 미국은 Korea NT Ballot 회람중인 "Conformance Test Suite for BioAPI Specification" (No081)의 표준화범위를 "표준적합성 평가방법" 으로 확대하는 방안과 미국표준기술연구소(NIST)·생체인식산업협회(IBIA)·IBG가 공동으로 표준화에 참여하는 방안을 제시하였다. 또한, 한국은 이번 회의 기간동안 기술인터페이스그룹(SG2)과 데이터변환포맷 그룹(SG3)에 각각 1건의 신규안건(NP)을 발표했으며, 제2차 총회에 정식으로 신규안건을 제출하기로 하였다.

현재 BioAPI 표준적합성 평가방법 국제표준 초안(SC37 No081)을 개발하여 2003년 9월 이태리에서 열리는 제2차 국제표준화 총회에서 발표예정이며, BioAPI 표준적합성 평가방법 국내표준 초안을 개발하여 TTA TC10/SG3에 상정할 예정이다. 한국이 제안한 평가기술은 종전의 평가 소프트웨어에 대한 표준화 개념에서 평가방법론 전반에 걸친 개념으로 확산될 것으로 보이며, 미국의 공동참여 요청으로 가속도가 더해질 것으로 전망된다.

3.5 부가형 전자서명 방식 표준(EC-KCDSA)

타원곡선 암호시스템은 기존의 공개키 암호시스템에 비해 장기적으로 기술 발전에 따른 키 길이의 증가 비율면에서 큰 장점을 가지고 있다. (예를 들어 RSA 암호시스템이 512비트 정도의 타원곡선 암호시스템과 유사한 안전도를 제공하기 위해서는 대략 15,000비트 정도의 합성수를 사용하여야 한다). 이에 따라 각종 국제 표준기구에서 타원곡선 암호에 대한 표준화가 활발히 진행되고 있고, 또한 실제로 다양한 보안응용 분야에서도 타원곡선암호를 속속 지원하고 있다. 현재 가장 널리 사용되는 타원곡선 암호시스템은 크게 전자서명과 키 교환으로 나눌 수 있다. ISO/IEC JTC1/SC27/WG2의 타원곡선과 관련된 표준에는 ISO/IEC JTC1/SC27 15946 Information technology - Security techniques - Cryptographic techniques based on elliptic curves -Part 1: General, Part 2: Digital Signatures, Part 3: Key Establishment 가 있다. 국내 기술인 부가형 전자서명 방식표준

(EC-KCDSA)[5]은 ISO/IEC JTC1/SC27 15946 Part 2의 세부기술로 채택되어 현재 국제표준인 IS로 제정되어 있다.

1998년 스웨덴 키스타에서 있었던 ISO/IEC JTC1/SC27/WG2 표준회의에서 타원곡선에 기초한 암호기술에 대해 한국에서 제안한 부가형 전자서명 방식 표준(EC-KCDSA)이 받아들여져 Part2에 추가되었으며, 구현 예제, 알고리즘들의 비교 등에서 한국이 주도적 역할을 하였다. 1999년 1월에 한국은 Part 1: General에 대해서 본문의 정의 및 기술, 타원곡선의 수학적 개요에 대해 지적하였으며, Part 2: Digital Signatures에 대해서 WD 문서에 EC-KCDSA에 대한 기술문서를 제공하고 EC-KCDSA와 EC-DSA의 비교 설명을 부록에 첨가하도록 노력하였다. Part3: Key Establishment에 대해서는 본문의 정의, 표기, 기법 등에 대한 지적사항들을 제공하였다.

1999년 4월 스페인 마드리드회의에서는 Part 2 WD문서를 CD로 격상시키기로 결의하였다. 1999년 6월에는 EC-KCDSA의 서명 생성과정이 Montgomery Approach라는 방법을 사용하도록 수정되었으며, 구현 예제를 갱신하고 신규예제를 추가하였다. 또한, EC-KCDSA가 random oracle model에서 더욱 안전하기 때문에 EC-DSA에 비해 입증 가능한 보안성을 갖는다는 것을 내용으로 하는 기고문서를 제출하였고 부록에서 EC-KCDSA와 EC-DSA를 비교한 내용의 근거를 보여 주었다. 1999년 12월에는 Part 2 CD문서가 FCD가 되었으며, 2000년 10월 일본 동경에서 개최된 회의에서는 에디터가 Part 2 FCD문서를 갱신하도록 결의하였고, 차기 회의에서 수정본인 Part2 FCD문서를 FDIS로 승격시키기로 결의함으로써, 이후 회의에서 IS로 제정되었다.

4. 결론

본 논문에서는 국내 정보보호산업의 국제 경쟁력 강화와 국제시장 선점효과를 달성하기 위하여 국내 정보보호기술의 국제 표준화가 필요함을 설명하였고 대표적인 국제 표준화 기구인 ISO/IEC JTC1의 정보보호 관련 분과위원회인 SC27과 SC37에 상정된 국내 정보보호 기술의 현황을 분석하였다.

현재 국제 표준화 활동을 추진하는데 있어 사실 표준화 활동의 업체 참여 저조, 표준 활용의 필요성에 대한 사용자 인식 부족 등으로 인해 상당한 제약을 받고 있는 것이 사실이다.

향후, 이러한 제약사항을 극복하고 국제 표준화 활동을 강화하여 정보보호 선도국가의 위치를 확보하기 위해서는 첫째, 정보보호시장에서 많은 기술수요가 있고 동시에 세계 최고 기술 수준에 근접할 수 있는 국내 핵심기술분야를 찾아내고 둘째, 핵심기술분야의 우수기술에 대한 완성도 및 성숙도를 평가하여 신뢰성이 확보된 국제 표준화 가능기술을 발굴해야 하며, 마지막으로 국제표준화 대상기술을 검증하고 국제표준화를 추진할 수 있는 국제표준전문가들을 양성함으로서 가능해질 수 있다.

향후 정보사회의 경쟁력은 단순한 정보보호기술의 적용에서 머무는 것이 아니라, 새로운 수요를 창출하고 관련된 기술들 간의 상호운용성 확보가 필수적으로 요구된다. 따라서, 우수 정보보호기술 개발과 표준화 활동을 병행함으로서 국가 경쟁력이 더욱 향상될 수 있다는 패러다임의 변화가 선결되어야 할 것이다.

참고문헌

[1] SEED: ISO/IEC JTC1/SC27 - 18033 Encryption algorithm Part3 : Block ciphers, N3213, N2656r1.

[2] AMP: 11770-4 Key management - Key establishment mechanisms based on weak secrets.

[3] C2C-PAKA: 11770-4 Key management - Key establishment mechanisms based on weak secrets.

[4] BioAPI 표준적합성 시험도구: ISO/IEC JTC1/SC37 - Conformance Test Suite of BioAPI Specification, N81

[5] EC-KCDSA: ISO/IEC JTC1/SC27 - 15946-2 Cryptographic based on elliptic curves, Part 2: Digital Signature, N2157.

[6] 한국정보보호진흥원, http://www.kisa.or.kr

[7] 산업자원부 기술표준원, http://www.ats.go.kr

[8] 한국정보통신기술협회, http://www.tta.or.kr