정보보호와 표준화 추진전략

이홍섭 · 한국정보보호센터 기술개발부장

I. 서론

우리의 정보통신 환경은 점차 인터넷과 이동통신 등과 같은 정보통신망의 발달로 국지적 영역을 초월하는 국제화 및 개방화로 바뀌고 있는 중이며, 정보통신 기술은 디지털화의 완성, 통신과 방송의 통합, 인터넷과 멀티미디어의 융합 등을 바탕으로 급속히 발전하고 있다.

또한 정보통신 서비스는 국가, 산업, 일상생활 등에서의 정보화와 사회 각층에서의 다양한 정보제공 요구를 충족하는 지식기반산업으로 발달하고 있다.

정보통신분야에서 표준화의 목적은 정보통신망, 정보시스템 및 정보단말기간의 효과적인 이용을 위한 것으로서, 국내 및 국제적으로 불필요한 중복투자를 방지하여 적은 비용으로 고효율을 얻기 위한 방법이지만, 정보보호분야에서는 정보의 가치가 점차 높아지고 보호 필요성이 커짐에 따라서, 국제적으로는 선진국들이 자국의 국가안보 및 국익을 위해서, 국제적 표준의 선점을 통한 우위확보 경쟁이 매우 치열한 실정이다

정보보호는 정보통신 환경의 국제화 및 개방화와 함께 각종 해킹, 도청 등으로 인한 부당한 위협으로 정보의 유출·파괴·변조 등을 방지하기 위한 유일한 대책으로서, 최근 국내에서 전자상거래 활성화, 전자정부의 구축 등의 분야에서 안전한 정보유통 및 사용을 위하여 중요성이 날로 증가되고 있다.

정보보호 산업비율은 미국, 영국, 독일 등 주요선진국에서는 정보통신분야의 2~10%정도로 점차 증가되고 있으며, 국내는 아직 1% 이하로 급속한 신장이 예측되므로, 정보사회 진입에 따른 수요 증가와 함께, 관련 기술개발 및 시장형성과 산업발전의 현단계에서 국내정보보호 기술의 표준화 추진전략이 갖는 의미는 매우 크다고 할 수 있다.

II. 국제 동향

국제경제개발협력기구인 OECD(Organization for Economic Co-operation and Development)에서는 수차례에 걸쳐 정보보호에 관련된 지침을 국제적으로 권고하고 있으며, 주요 정보보호 관련 표준화 기구는 정보기술분야의 표준화를 주도하는 ISO/IEC(International Organization for Standardization/International Electrotechnical Commission) JTC1(Joint Technical Committee 1)과 전기통신분야의 표준화를 주도하는 ITU-T(International Telecommunication Union-Telecommunication)로 대별될 수 있다. ISO/IEC JTC1의 정보보호 관련 분과위원회로는 SC6(정보통신 및 시스템간 정보교환), SC21(개방형시스템 상호접속, 데이터 관리 및 개방형 분산처리) 및 SC27(정보보호기술) 등이 있다. ITU-T는 SG7에서 정보통신망과 서비스에 관련된 정보보호 표준을 개발하고 있으며, 이밖에 IETF (Internet Engineering Task Force), X/Open, NIST 등 지역표준, 국가표준 및 사실 표준에 대한 여러 가지 단체가 활동하고 있다.

1. OECD

OECD의 정보보호에 관련된 주요정책으로는 1980년에 "프라이버시 보호와 개인정보의 국경초월 유통에 관한 지침", 1992년 "정보시스템의 보안에 관한 지침", 그리고 1997년에 "암호정책지침에 관한 이사회 권고"를 발표한 바 있어 국제적으로 정보보호의 중요성을 간접적으로 입증하여 주고 있다.

그중 정보보호의 핵심분야인 암호에 관련된 정책지침의 8대 권고내용으로는

1) 암호기법의 신뢰성 제고
2) 암호기법의 선택권보장
3) 시장주도형 암호기법 개발
4) **암호기법의 표준화**
5) 프라이버시 및 개인정보의 보호
6) 적법한 접근
7) 암호서비스 공급자와 책임규정 명확화
8) 국제협력의 증진

이며, 이중 **암호기법의 표준화**를 살펴보면 "암호기법에 대한 기술 표준과 기준, 프로토콜은 국내 및 국제적 수준에서 개발되고 공표되어야한다. 각국 정부와 국제적 표준정립기관, 산업계와 관련 전문가들은 암호기법의 상호 호환성있는 기술 표준, 기준, 프로토콜의 개발과 공표를 위하여 정보를 공유하고 협력하여야 한다. 국내 암호기법 표준은 범세계적

상호호환성, 이식 가능성, 이동성을 위한 기술 표준, 기준, 프로토콜에 대한 각국의 이행여부를 심사할 메커니즘의 개발도 이루어져야 한다."으로서 우리나라도 이에대한 구체적인 표준화 대책을 수립중에 있다.

2. ISO/IEC JTC1

ISO/IEC JTC1의 정보보호 관련 분과위원회로는 SC27(정보보호기술)를 중심으로SC6, SC21과 연계하여 활동하고 있다. SC27에서는 정보시스템의 정보보호 서비스 요구사항, 보안지침 및 관리기법, 정보보호 기술과 메커니즘의 개발, 그리고 정보보호시스템의 평가기준에 관한 표준화를 추진하고 있으며 3개의 실무작업반을 운영하고 있다.

1) WG1 : 정보보호 관리
정보보호 기본 모델, 정보보호 메커니즘과 암호기술 응용, 보안관리 지침 및 감사, 위험분석과 침입탐지, Trusted Third Party 지침 및 기준 등

2) WG2 : 정보보호 기술
실체인증, 메시지 인증, 전자서명, 해쉬함수, 타원곡선 암호기법, 키관리 기술 등

3) WG3 : 정보보호시스템 평가
정보보호시스템 평가기준, 평가절차, 국제공통 및 상호인증체계 등

3. ITU-T SG7

ITU-T는 15개분과 중 SG7를 중심으로 각종 정보통신망 및 서비스에 관련된 다음과 같은 정보보호 활동을 추진하고 있다.

1) Grobal Information Infrastructure Security
2) IMT-2000 Security
3) Telecommunications Management Network - M. 3000 Series
4) OSI System Management - X. 700 Series
5) OSI Security - X. 800 Series
6) Message Handling System - X. 400 Series
7) Directory - X. 500 Series 등

4. IETF

IETF는 인터넷의 통일성과 표준을 유지하기 위한 Internet SOCiety의 하위조직으로 정부기관, 업계, 학계 등 다양한 계층으로 구성된 민간국제단체로서 다음과 같이 정보보호에 관련된 12개 분야별로 작업반이 구성되어 있다.

1) PKIX(Public Key Infrastructure : X. 509)
2) SPKI(Simple Public Key Infrastructure)
3) DNSSEC(Domain Name System Security)
4) S/MIME(Secure Multi-Purpose Internet Mail Extensions)
5) Open PGP(Open Specification for Pretty Good Privacy)
6) CAT(Common Authentication Technology)
7) OTP(One Time Password)
8) SECSH(SECure SHell)
9) WTS(Web Transaction Security)
10) AFT(Authenticated Firewall Traversal)
11) TLS(Transport Layer Security)
12) IPSEC(Internet Protocol SECurity)

III. 국내 현황

국내의 정보보호 관련 표준화 추진체계는 정보통신부의 한국정보통신표준(KICS)과 산업자원부의 한국산업표준(KSC)으로 이원화되어 있다. 정보통신부는 정보보호 관련 표준 연구개발 기관인 한국정보보호센터와 정보통신관련 단체표준 전담기관인 한국정보통신기술협회의 정보보호 분과위원회(SC10)를 통해 표준화를 추진하고 있으며, 산업자원부는 정보기술 전반에 걸친 표준화 전담기관인 국립기술품질원과 한국산업표준원을 통해 정보보호 관련 표준화를 추진하고 있다.

현재까지 정보보호 관련 표준 제정 현황은 한국정보통신기술협회 20여건, 국립기술품질원 20여건으로 ISO 100여건, ITU-T 40여건, IETF 100여건에 비추어볼 때 상대적으로 미약한 수준이며, TTA SC10이 생기기 이전까지는 국제표준을 번역하는 수준이었으나, 최근에는 30여건에 달하는 국내 독자표준을 개발하는 단계로 발전하고 있다.

1. TTA SC10 (한국정보통신기술협회 정보보호 분과위원회)

정보통신부는 국내 정보보호산업의 발전과 국제경쟁력을 강화하기 위하여 '97년 5월에 한국정보보호센터(KISA)를 정보보호 표준개발 전담기관으로 지정하였고, TTA 산하에 SC10을 신설하였다. 위원회 활동은 한국정보보호센터를 중심으로 한국전산원, ETRI, KT, 삼성전자, LG전자 등이 참여하여 활발하게 추진하고 있다. 그동안 SC8과 함께 전자서명 알고리즘, 해쉬알고리즘 등 13개 표준을 제정하였으며 '99년도에는 다음과 같은 표준에 대한 개발을 계획하고 있다.

1. OSI 하위계층 시큐리티 모델
2. 개방시스템 상호접속을 위한 정보보호 골격 : 개요 표준
3. 인터넷 보안관리 지침 표준
4. 공개키 인증 방식 표준
5. 초고속 통신망 정보보호 프레임워크
6. 전자상거래 정보보호 프레임워크
7. 암호키관리 체계 표준
8. 데이터 암호알고리즘 표준
9. 전자화폐 보호 기술 표준
10. 전자지불 보호 기술 표준
11. 개방시스템 상호접속을 위한 상위계층 정보보호모델
12. 개방시스템 상호접속을 위한 인증 프레임워크
13. 개방시스템 상호접속을 위한 접근통제 프레임워크
14. 전자우편 보안 표준
15. 웹 트랜잭션 보안 표준
16. OSI-개방시스템에서의 보안 골격 - 제4부 : 부인방지
17. 공공정보시스템 보안을 위한 위험분석 표준 - 위험분석 방법론
18. 정보시스템 구축준비단계의 보안 관리지침
19. 공공정보시스템 비상계획 및 재해복구에 관한 지침
20. 정보보호 전문용어 표준(개정)
21. 공공기관 전산보안정책 수립을 위한 지침서 (개정)
22. 실체 인증기술 표준
23. 가변길이 해쉬함수 표준
24. 타원곡선 전자서명 알고리즘 표준
25. 일회용 패스워드 표준
26. 디렉토리시스템 인증 프레임워크
27. 디렉토리시스템 접근통제 프로토콜
28. 침입차단시스템 선정지침
29. VPN 보안기술 표준
30. 바이러스 방지지침
31. 전산망 안전·신뢰성 기준
32. 정보시스템 보안감리 지침

2. 한국산업표준원

국립품질기술원의 산하기관으로 '93년에 설립된 산업표준 연구개발기관으로, 한국표준정보망(Korea Standards System Network)을 운영하여 민간에게 표준을 보급하는 임무도 수행하고 있다. 주로 ISO/IEC 표준을 번역하여 국내표준으로 제정하는 활동에 치중해 있다.

정보보호에 관련된 KS표준은 '86년에 미국의 DES를 번역하여 KSC5766으로 제정한 이래 미국 표준과 ISO표준 등을 번역하여 20여개의 KS표준을 제정하였으며, '99년도에 계획된 주요 표준과제는 다음과 같다.

표준화과제명	관련권고
1. 암호화 알고리즘 등록절차	ISO/IEC 9979
2. 실체 인증 - 제3부 : 비대칭을 이용한 메커니즘	ISO/IEC 9798-3
3. 키관리 - 제1부 : 기본골격	ISO/IEC 11770-1
4. 정보기술 보안관리지침 - 제1부: 정보보안의 개념과 모델	ISO/IEC TR 13335-1
5. 정보기술 보안관리지침 - 제2부: 정보기술 보안계획 및 관리	ISO/IEC TR 13335-2
6. 정보기술 보안관리지침 - 제3부: 정보기술 보안관리를 위한기술	ISO/IEC TR 13335-3
7. 부인방지 - 제3부: 비대칭 암호기법을 이용한 메커니즘	ISO/IEC 13888-3

IV. 국내 표준화 추진전략

1. 독자표준 개발 및 제정 절차 개선

- ○ 현재의 복잡한 표준제정 절차를 개선하고 기간을 단축하여야 한다. 표준의 내용, 이용자 요구 및 시장수요 등의 표준화 환경 변화에 따라 필요시점에서 언제든지 표준의 승인이 이루어질 수 있도록 하여야 하며, 이에 따라 표준 제정에 소요되는 기간도 다양화할 필요가 있다.
- ○ 국내의 독자적인 표준개발 추진시 신속하게 처리해 나아가야 한다. 암호 알고리즘 등 정보보호의 특성상 국내 독자개발이 필요한 표준과 국제적인 상호운용성이 고려되어야 할 표준을 사안별로 분리하여, 병행 혹은 공동 개발 등의 선별적인 추진전략이 필요하다. 미국의 예를 들면, 표준 암호 알고리즘(DES)을 제정하여 자국의 이익을 극대화하고 현재는 차세대 암호 알고리즘인 AES를 개발하고 있다. 국내 자체 기술 개발과 국제 표준화는 전세계적인 파급효과가 있으며 IPR(Intellectual Property Rights)과 연계하여 개발되는 경우 세계적인 특허로 등록될 수 있다.
- ○ 표준 제정활동 및 활용도를 극대화하여야 한다. 정보보호 핵심기술에 대한 개발을 진행함과 동시에 표준 제정 작업을 병행하여 기술의 구현을 통해 표준 제정 활동에 신뢰성을 더하여야 한다. 또한 그 내용 및 과정을 공개함으로써 산업체의 제품개발시 표준의 내용이 반영될 수 있도록 하여야 한다. 이는 초기부터 제품에 대한 표준을 정착시켜 다양한 제품들에 대한 상호운용성을 보장하며, 중복투자를 사전에 방지할 수 있

고 표준에 대한 활용도를 극대화시킬 수 있을 것이다.

2. 연구개발, 표준화, 평가의 효율적 추진

○ 오늘날 정보통신 기술이 고도화되고 급속히 변화하면서 표준화에 대한 기술항목들은 증가하고 있는 반면 표준화 작업을 위하여 허용되는 시간은 상대적으로 줄어들고 있다. 그러므로 표준화는 연구개발과 병행하여 일괄적으로 추진되어야 하며 국내 연구개발을 국제 표준화로 발전시키기 위해서는 연구개발 단계에서부터 외국과 제휴를 통하여 표준화를 추진해야 한다.

○ 또한 표준화와 더불어 객관적이고 신속한 평가를 시행함으로써 제품 공급주기를 단축시키고 시장 경쟁에서의 우위를 확보할 수 있다. 산업체 발전 및 국가기반에 적용될 수 있는 정보보호시스템을 적기에 공급할 수 있도록 유도하기 위해서는 표준과 더불어 신속한 평가가 필요하다.

3. 평가제도 도입 및 적용

○ 표준(안) 개발에 대한 평가제도를 도입하여 고품질화를 지향하여야 한다. 실적 위주의 표준 제정 활동을 절대 지양하고 표준(안) 개발 제안 단계에서부터 표준의 활용성 및 시급성 등을 평가하여 표준 개발을 추진하고 개발된 표준에 대해서는 산업화를 적극적으로 지원하여 표준의 위상을 제고시킬 수 있도록 해야 한다.

○ 개발된 표준에 대해서는 분야별로 적용을 위한 법·제도적 지원이 수반되어야 한다. 표준의 분야별 적용을 촉진하고 표준에 대한 관심도를 높일 수 있도록 법·제도적으로 표준화된 기술, 기준 및 지침 등에 대한 사용을 명시하도록 하여야 한다.

4. 민간 표준화 활동 활성화

○ 표준화는 민간 중심 및 시장 경쟁력 강화를 위하여 추진되어야 한다. 시장성을 토대로 하여 전략적 표준화 분야 및 대상을 선정하고 이렇게 선정된 분야에 집중적인 자원의 투자가 병행되어야 한다.

○ 또한 창조성이 고양되고 사용자의 요구사항이 잘 반영되는 표준화가 되어야 한다. 이는 국제 경쟁력을 향상을 위하여 민간을 중심으로 표준화가 추진되어야 하며 국가가 여러면에서 표준화 활동을 지원해야 한다는 것을 의미한다.

5. 신규 산업 창출 및 산업 경쟁력 확보

○ 표준화는 국제 경쟁력 확보, 신규 산업의 창출 등을 위한 필수요소로써 국가적 관점에서 적극적 지원이 마련되어야 한다. 또한 기업 측면에서 표준화는 시장확보 및 사업전략의 수단으로서 사실상 표준화를 염두해 두어야 하며 기업간 제휴 등을 통하여 전략적으로 추진하여야 한다.

○ 대표적인 예로 비자, 마스터 카드사, IBM, Cybercash, 넷스케이프사 등이 컴소시엄을 이루어 상용화 단계에 이른

전자상거래용 SET(Secure Electronic Transaction)은 de facto 표준의 역할을 하고 있다.

6. 표준 관련 정보 공유의 확대

- ㅇ 급변하는 정보통신 환경에 적절히 대응하기 위해서는 표준 관련 정보의 공유가 필요하다. 표준문서, 표준화 일정 등 표준화의 진행에 관련된 각종 정보를 인터넷을 통하여 검색하고 처리할 수 있는 기반환경을 조성해야 하며 표준화 관련 단체나 표준 이용자에게 적시에 정보를 제공함으로써 표준의 사용을 극대화하여야 한다.
- ㅇ ISO/IEC JTC1의 경우 디스켓에 의한 문서배포에서 웹기반 전자문서배포의 정책을 도입하여 사용자들의 보다 능동적인 참여를 유도하고 최근의 표준화 과정의 신속화를 적극 반영하기 위한 정책의 일환으로 EDH(Electronic Document Handling) 기반 표준정보유통 시스템을 개발하고 있다.

이외에도, 정보보호 관련 기술의 자체 연구개발, 표준화에 대한 민간의 인식 제고, 표준화 기관간의 정보 공유 및 전자적인 수단의 기반조성 등을 통해 다각적인 표준화 지원 노력이 수반되어야 한다.

V. 국제 활동 추진전략

1. 외국과 협력을 통한 국제표준화 추진

- ㅇ 아시아 지역의 국가들은 정보통신기반 구축이 급속히 추진되고 있는 반면 국제 표준화 활동은 미흡하고 국내 표준화 활동도 제대로 정착되어 있지 않은 경우가 많다. 아시아 지역에서 우리나라가 정보보호 기반의 중심으로 정보보호 산업의 메커로서의 위치를 확보하기 위하여 일본 등 아시아지역 국가들과 긴밀한 협조 관계를 유지하면서 표준화를 추진하여야 한다.
- ㅇ 또한 아·태지역 국가간의 상호 협력 증진과 안정적인 정보통신 표준화 활동 프레임워크 구축을 위하여 1997년 11월 아·태 전기통신협의체(APT, Asia Pacific Telecommunity)가 설립한 APTSP (Asia-Pacific Telecommunity Standardization Program)는 지역적인 국제 표준화를 위한 좋은 계기가 될 수 있다.

2. 비공인 표준화 기구 활동 활성화

- ㅇ 사용자 요구사항과 신기술의 발전을 보다 신속히 표준에 반영하고 조기에 시장성을 확보하기 위하여 민간 중심으로 한 비공인 표준화 기구들의 활동이 활성화되어야 한다.
- ㅇ 미국의 경우 국제적인 사실상 표준화의 핵심이 되는 포럼활동으로 유도하고 이를 통하여 미국의 독자 기술을 국제적으로 보급하고 국제 경쟁력을 높이는 사례가 증가하고 있다. 대표적인 예로 ATM, DAVIC, MMCF 등의 각종 포럼과 컨퍼런스들이 있다.

3. 국제 표준화 전문인력 양성

○ 국제 표준화에 대응하기 위하여 표준화 전문가 양성은 매우 중요한 사항이다. 국제 표준화 활동들은 회의개최를 통하여 전문가들간의 조정과 공동작업으로 이루어진다.

○ 국내 표준을 국제 표준화로 추진하고 국내 기업들의 권익을 보호하기 위해서는 ISO, ITU, IETF, ECMA, ETSI 등 국제 표준화활동에 적극 참여하고 그 표준화 활동을 리드할 수 있는 전문가의 육성이 반드시 필요하다.

정보보호 표준화 추진 전략

환경변화	전 략	비 전
○ 정부 및 민간기관을 중심으로 정보보호기술 표준화 필요성 증가 ○ 정보보호제품의 상호 운용성 요구 ○ 정보보호 핵심기술의 표준을 적용한 정보보호제품 개발 ○ 산업체의 정보보호제품 개발에 경쟁력 및 경제성 확보	○ 국내 표준체계 개선 - 독자표준 개발 및 제정절차 개선 - 연구개발, 표준화, 평가의 효율적 추진 - 평가제도의 도입 및 적용 - 민간 표준화 활동 활성화 - 신규 산업 창출 및 산업 경쟁력 확보 - 표준 관련 정보 공유의 확대 ○ 국제 표준활동 강화 - 민간레벨의 국제 표준활동 지원 - 인터넷 표준기구 참여활동 강화 - 외국과 협력 및 공동연구를 통한 국제 표준화 추진 활성화 - 국제표준화 전문인력 양성	○ 안전·신뢰성 확보에 필요한 정보보호제품 개발의 활성화 및 이용자 보호 ○ 중복투자 방지를 통한 가격 경쟁력 제고 ○ 핵심기술 표준화 선도 및 제품화 연계로 세계 정보보호제품 시장 10% 점유

VI. 결론

국내적으로 IMF 등 어려운 상황을 조속히 타개하기 위해서는, 국가가 전략사업으로 추진하고 있는 정보보호산업 육성을 표준활동과 연계하여 국가경쟁력을 제고해야 한다. 이를 위해서는 무엇보다도 현재의 표준화 추진체계를 민간주도로 개선하고 국제 표준활동을 더욱 강화하는 표준정책을 일관성 있게 추진해야 한다.

국내 표준화 추진체계 개선방향의 핵심은 표준제정이 국내 정보보호산업육성과 바로 연계될 수 있도록 다양한 정보보호기술 중 시장의 파급효과 및 긴급성 등 우선 순위에 의한 정보보호기술 표준화 추진대책을 하루속히 수립해야 한다.

또한 세계가 단일 표준으로 가고 있는 추세에 맞추어 국내 표준 제정과 더불어 국제 표준과의 연계성을 고려하여 필요한 경우 표준 개발 초기부터 국제 표준화 기구 활동과 연계된 공동개발전략을 수립해야 한다.

특히, 이제는 국내 표준과 세계 표준간의 차이가 점점 의미 없어지는 추세에 따라 국내 표준 정책을 원점으로부터 재검토하여 지식정보사회에 맞는 범세계적 차원에서 국내 표준화 추진대책이 수립되어야 한다.