

생체인식 산업의 표준화에 관한 연구 I (제품표준 ; CC(Common Criteria)를 중심으로)

- A Study on Standardization of Biometrics Industry -

장 병 노 *
Kang Byong No
송 수 정 **
Song Soo Jeong
정 수 일 ***
Jung Soo Il

Abstract

The purpose of this study is to carry out comparative analysis of the differences between the trend of biometrics-related product standardization in the world and that of Korea, and to suggest ideal directions and building plans for domestic biometrics industry. Its purpose also includes constructing promptly a standardization of domestic biometrics industry based on the suggested standards.

1. 서 론

정보화 사회에서의 사업환경을 모색하기 위해 무엇보다도 가장 관심이 되는 것은 정보 보안이다. 개인이나 기업의 정보 유출로 인한 사고는 해마다 늘어나고 있으며, 이는 기업의 비즈니스 관계, 시장확대 및 기업의 이익구조에 막대한 지장을 초래하는 것으로 나타나고 있다. 생체인식 시스템은 인터넷 가상공간에서 가장 유망한 보안기술로 평가 받고 있으며, 최근 정보 보안의 가장 유력한 수단으로 대두되고 있는 것이 생체인식을 통한 구현이다. 그러므로 이 생체인식 산업이 산업전반에 미치는 영향은 실로 매우 크다고 할 수 있다. 모름지기 산업의 발전에서의 그 근간은 표준화라고 할 수 있기에, 전 세계적으로 이미 선진 각 국을 중심으로는 국가적인 차원에서 생체인식 산업의 표준화를 위한 활동을 활발히 추진하고 있다. 이에 국내에서도 선진 동향에 대한 준비가 마땅히 필요하나, 그 활동이 미비하여 또한 이제 막 시작하려는 단계에 있으므로

* Nitgen Technology QA팀장

** 신성대학 산업경영정보과 교수

*** 인하대학교 산업공학과 교수

로 이에 대한 연구가 시급한 실정이다. 먼저 국내 생체인식 산업의 표준화 추진 시 가장 시급히 마련되어야 할 것은 공인된 검증 기관과 표준화 작업이다. 현재 여러 기업 등에서 개발한 생체인식 시스템에 대하여 공인된 평가를 하는 기관이 국내에는 아직 없는 형편이다. 여기서 의미하는 평가는 단순한 시스템의 여러 rate 뿐만 아니라, 등록 실패율, 사용자가 선호하는 정도, 감성적인 평가, 대규모 시스템에 사용 가능성 등의 여러 다양한 측면에서의 공정한 평가를 의미한다. 이에 본 논문은 국외 선진 각국의 생체인식 산업의 제품표준 : CC(Common Criteria)를 중심으로 표준화 동향과 국내 동향과의 차이점과 gap을 비교 분석하여 궁극적인 국내 생체인식 산업의 표준화 추진 방법과 추진 모델을 제시하고자 한다.

2. 생체인식

생체인식(Biometrics)이란 생체인식 또는 생체 측정학으로서 개인의 독특한 생체적, 행동적인 특성이나 습관을 이용하여 개인을 식별하거나 개인의 신원을 확인하는 학문 또는 기술이다. 생체인식은 지문, 얼굴, 음성, gesture 등 인간의 생리적/행동적 특징을 자동으로 인식하여 개인의 신원을 판단하는 기술로서, 학문적으로는 디지털 신호처리, 패턴 인식, 인공 지능, 마이크로 프로세서 설계, 데이터통신 등 첨단 정보통신 기술들을 바탕으로 하는 복합적인 학문이다. 생체인식기술은 21세기 인터넷 정보사회에서 정보 보호와 개인인증 및 식별을 위한 강력한 수단으로 그 필요성 및 유용성이 급격히 증가하고 있으며, 그 응용분야도 출입통제, 시스템 log-on, 인터넷 banking, 무선전자결제 등 빠르게 확산되고 있다. 이러한 생체인식을 통한 개인 식별은 새로이 등장한 개념이 아니라 오래 전부터 사용되어 왔다. 다만 이러한 개인 식별 수단들은 사람에 의해 무의식적으로 이루어져 왔을 뿐이다. 생체인식에 의한 보안은 단순한 출입관리나 현금인출기(ATM)에서의 본인 식별과 같은 물리적 환경에서부터 인터넷에 의한 상거래와 tele-banking 등과 같은 cyber환경에서의 인증에 이르기까지 그 응용범위가 실로 엄청나게 확대되고 있다.

3. 생체인식 산업의 제품 표준화 동향

3.1 국외동향

국제공통평가기준(CC)은 선진 각국의 정보보호제품 평가 기준을 국제적으로 단일화 하려는 움직임의 결과물이다. 선진 각국에서 활용되고 있는 다양한 평가기준을 단일화 함으로써 객관적인 평가결과를 생산할 수 있는 환경을 만들어 정보보호 시장확대의 기반을 마련한다는 것이 CC의 목적이다. 궁극적으로는 국가간 정보보호시스템의 평가 결과를 상호 인정하는 상호인정협정(CCRA) 기반을 마련하기 위한 것이다. 1993년 미국 (NSA, NIST), 영국(CESG), 독일(BSI), 프랑스(SCSSI), 캐나다(CSE), 네덜란드 (NL-NCSA) 등 6개국 7개 기관이 합의해 국제공통평가기준(CC) 개발에 착수한 이후,

1996년 1월 Version 1.0, 1998년 5월 Version 2.0이 발표됐다. 이어 1999년 9월 국제표준(ISO/IEC 15408)으로 제정되면서 현재의 Version 2.1이 발표됐다. 현재 전세계 11개국에서 상호인증 추세이며, 생체인식을 위한 제품표준에는 BDPP가 있다. 이미 CC는 미국 및 영국을 비롯한 선진 각 국에서는 자국의 전통적인 평가기준과 병행해 활용하고 있다. 미국은 정보보호시스템 평가 인증제도를 민간분야에까지 확대하고 평가결과를 국가간 상호인정하기 위하여 다른 국가보다 적극적으로 CC 수용을 추진하고 있다. 특히 2002년 7월부터는 국가안보나 비밀과 관련된 정보를 다루는 기관뿐 아니라 민간분야에까지 CC를 통하여 평가·인증 받은 제품을 사용하도록 권고하는 것을 정책화하고 있다. CC의 국제화는 기정 사실화되고 있고 선진국을 중심으로 구성된 CCRA를 통하여 확대되고 있는 추세이다.

3.2 국내동향

최근 한국정보보호인증원(KISA)에서는 방화벽(Fire wall)과 침입방지 시스템(IDS)의 표준화를 추진하고 있으며, 정보보호시스템의 공통평가기준(CC)은 국산 정보보호 시스템의 수출에 새로운 관건으로 대두되고 있다. 이에 정부는 2001년 하반기에 CC를 국가 표준으로 채택하고 내년(2002년) 하반기부터는 CC 기반 평가를 시행할 계획이다. 또한 2004년경에는 국제상호인정협정체제(CCRA) 가입을 목표로 하고 있다. 우리나라는 1996년 평가인증제도를 구축하고 첫번째 평가인증제품이 나온 1998년부터 CC 개발을 주도해 온 ISO/IEC JTC1/SC27의 WG3에 참여하기 시작해 국내 의견을 적극적으로 개진해 왔다. 베전 2.1이 발표된 후 우리 나라도 CC의 국내 수용에 대해 심도 있는 타당성 연구를 해 왔다. 특히 상호인정협정(CC-MRA)이 2000년 5월 CCRA로 정책선회를 하면서부터 국내의 관련기관을 중심으로 가입여부 및 타당성조사에 적극적으로 참여하여 곧 CC 수용 및 CCRA 가입 관련기관의 의견이 공식적으로 발표될 예정이다.

4. 국내 생체인식 산업의 제품 표준화

국내의 보안제품에 대한 표준화는 보안제품 전반에 걸친 표준이라 하기에는 부족한 면이 없지 않다. 그럼에도 불구하고 해외의 동향은 모든 보안제품이 포함될 수 있는 광범위한 표준을 근간으로 각 제품에 적절한 표준을 제정 승인하는 절차를 거쳐 완성하는 방법을 택하고 있으며 이를 국제 공통으로 인정함으로써 개발, 생산뿐만 아니라 사용자의 선택기준을 명확히 제시하고 있는 실정이다. 국내정보보호시스템(침입탐지시스템 : IDS)은 국제공통 평가기준(CC)에 비교하여 다음과 같은 차이점과 문제점이 있다. 첫째, 제품별로 평가기준을 사용하므로 평가 품목 수에 한계가 있다.

- ① 제품별 평가기준에 의한 평가가 이루어지고 있으므로 신규 분야의 평가를 위해서는 별도의 평가기준 개발 및 고시가 필요하다.
- ② 평가기준 개발에 보통 1 ~ 2년 정도의 많은 시간이 소요된다.
- ③ 1996년부터 평가제도를 준비했으나 품목은 2종(침입차단시스템, 침입탐지시스템)에 불과하다.

둘째, 해당국으로 수출 시에는 별도의 평가 및 인증이 필요하다.

- ① 국내 정보보호 시장 규모가 확대되고 경쟁력 있는 업체들이 등장하면서 해외시장 진출이 주요 현안이 되고 있다.
- ② 국내 평가제도의 인지도가 낮고, 외국과 상호인증이 안되어 있어 해당국으로 진출 시 별도의 평가 및 인증을 받아야 한다.

셋째, 단일 기관에서 평가하므로 평가결과에 대한 평가의뢰자의 신뢰도가 미흡하다.

넷째, 단일 기관에서 평가하므로 평가기간이 길고, 평가적체가 지속되고 있다. 정보보호의 중요성과 함께 평가 수요가 급증하고 있으나, 정부 출연 기관인 KISA가 단독으로 평가 업무를 수행하고 있고 예산확보 문제로 평가가 적체현상을 보이고 있다.

다섯째, 평가 기술력 확보에 어려움이 있다.

선진국의 평가인증 기관과 공식적인 협력채널이 없어 정보교류가 늦고 평가 기술 확보에 장애요인으로 작용하고 있다. 선진국의 평가기관과 공식적인 협력채널이 없어서 정보교류가 늦고 평가 기술력이 떨어진다.

여섯째, 국제표준과의 연계성이 미흡하고 국내표준을 국제화하기 힘들다.

이러한 노력의 구체적인 실행순서를 제시하면 이미 마련된 CC의 규격을 면밀히 검토하여야 할 것이다.

CC EAL 4와 국내 기준인 K4 인증수준을 비교해 보면, 개발 관련 문서의 요구수준이 거의 같음을 알 수 있다. 그러나 K4 인증수단에서 요구하진 않지만 CC EAL 4에서 요구하는 문서가 존재함을 알 수 있을 것이다. 이러한 문서들의 성격은 평가자의 입장에서 대상제품의 평가 및 기술 수준을 객관적이고 통일되게 확인할 수 있는 방법론을 제시하고 있으며, 또한 평가의 재연성을 보장하고 있으며 아울러 보안기능의 강도 및 개발도구에 대한 설명을 첨부함으로 해서 향후 기술발전을 도모하기 위한 기초자료로 삼고자 함을 볼 수 있다. 이러한 추가 문건의 생성이 국내 기술 수준으로 달성 가능한 수준인지 아닌지를 판단하여 만일 국내 기술수준으로 충분히 달성 가능한 수준이라면 시급히 국내 표준으로 포함시키는 유연성을 발휘하여야 할 것이며, 만일 그렇지 못한 실정이라면, 국내업체의 기술수준 향상을 위해 도입시기 예고 등을 통해 기술을 준비할 수 있는 시간을 마련함이 옳은 선택이라 할 것이다. 국제공통평가기준(CC)의 국내 도입 및 국가간 상호인증(CCRA)의 추진은 국내 보안산업의 발전과 국제적 도약을 위한 필수 요소임을 직시하고 그 도입에 대한 심도 있는 검토가 상기에 제시한 방법을 토대로 철저히 이루어져야 할 것이다. 이 때 고려하여야 할 사항을 살펴보면 다음과 같다. 첫째, 선진국의 동향에 동참하려면 제품별 표준화를 지향하고 공통표준화 작업으로의 전환을 하루빨리 모색하고 거기에 따른 실행방안을 모색해야 한다. 둘째, 국내의 대응여건을 충분히 고려해야 한다. 자칫 선부른 국제표준의 도입의 이제 막 성장기에 접어든 국내정보보호 산업이 표준에 종속되는 우를 초래할 수도 있다. 셋째, 정부가 주도가 되어 표준화 작업을 수행함은 물론이고, 학계와 업계의 자발적인 유도를 이끌어 내야 한다. 넷째, 평가기술인력의 확보를 위하여 해외 bench marking이나 선진국과의 컨소시엄을 과감히 추진해야 한다. 이에 맞는 교육 프로그램개발이나 자격부여제도 등을 검토해야 한다.

5. 결 론

본 연구는 날로 그 중요성이 증대되고 있는 e-biz환경에서의 정보보안의 새로운 대안으로 제시되고 있는 생체인식 산업의 국내 표준화 방안을 제품표준의 중심으로 모색하고자 추진하였다. 국내 생체인식 산업은 타 산업의 비교하여 선진국과의 기술격차가 비교적 적을 뿐 아니라 원천기술을 보유하고 있는 분야도 있으므로 차세대 기술보국의 자리 매김을 할 수 있는 기회요인도 갖고있는 분야이다. 그럼에도 불구하고, 산업의 근간이라 할 수 있는 표준화 분야에서는 선진국과의 격차가 심하고 아직 국내에서는 시작 단계에 머무르고 있어 이에 대한 추진이 시급한 실정이다. 본 연구는 선진 각국의 생체인식 산업의 표준화 방향 및 전략과 국내산업과의 차이점을 비교 분석하여 바람직한 국내 생체인식 산업의 표준화의 추진방향 및 방법과 모델을 제시하였다. 이는 Best practices 개념을 이용하여 정보기술의 발전과 함께 전 세계적으로 그 발전속도가 타의 추종을 불허하고 있는 생체인식 시장 속에서 국내 산업이 전 세계 표준화의 리더로서 역할을 담당할 수 있는 것을 의미하며, 여기에서 제시한 표준화의 안을 바탕으로 해서 하루빨리 국내 생체인식 산업의 표준화를 구축해야 한다.

[참 고 문 현]

- [1] 김상춘 외2, 정보보호 제품의 적합성 시험평가 현황, 정보과학회지 제11권 제2호, 2001.
- [2] 김재희, 생체인식 기술의 현황과 응용, Security world 2000.~2001.
- [3] 장상수 외2, 정보보호 관리체계 인증제도 및 추진현황, 정보과학회지 제11권 제3호, 2001.
- [4] 길민정, 생체인식 산업동향, ETRI 정책연구팀, 2001.
- [5] 이현, CC기반의 평가제도 도입방안, 정보통신부, 2001.
- [6] CC 수용추진 Workshop, 국가정보원, 2001.
- [7] BioAPI Specification, Version 1.1, BioAPI Consortium, 2001.3.
- [8] Biometric Management and Security, ANSI X9.84-2000, American Bankers Association, 2001.
- [9] Fernando L. Podio, Motivation for a Biometric PI, NIST, 2000.
- [10] J.L. Wayman, Fundamentals of Biometric Authentication Technologies National Biometric Test Center Collected Works, Ver.1.3, pp.1-19. 2000.
- [11] Best Practices in Testing and Report Performance of Biometric Devices, version 1.0, Biometrics Working Group, 2000.