생체인식 산업의 표준화에 관한 연구 II

(시스템(보안) 표준 ; BS7799/ISO/IEC 17799를 중심으로)

- A Study on Standardization of Biometrics Industry -

강 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 system(security) 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 관건이 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 세계적으로도 이미 선진 각 국을 중심으로는 국가적인 차원에서 생체인식 산업의 표준화를 위한 활동을 활발히 추진하고 있다. 이에 국내에서도 선진 동향에 대한

* Nitgen Technology QA팀장
** 신성대학 산업경영정보과 교수
*** 인하대학교 산업공학과 교수

준비가 마땅히 필요하나, 그 활동이 미비하며 또한 이제 막 시작하려는 단계에 있으므로 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 아직없는 형편이다. 여기서 의미하는 평가는 단순한 시스템의 에러 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 각 국의 생체인식 산업의 시스템(보안) 표준 ; BS7799/ISO/IEC 17799를 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 정보보호와 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)에서 의 본인 식별과 같은 물리적 환경에서부터 인터넷에 의한 상거래와 tele-banking 등과 같은 cyber환경에서의 인증에 이르기까지 그 응용범위가 실로 엄청나게 확대되고 있다.

3. 생체인식 산업의 시스템(보안) 표준화 동향

3.1 국외동향

BS 7799/ISO 17799는 현재 정보보호를 위한 유일한 국가표준으로 최상의 실행을 위한 포괄적인 일련의 관리방법에 대해 요건별로 해석해 놓은 산업체를 위한 규격이며, 이미 BS 7799 Part 1이 ISO/IEC 17799로 개정되었다. 정보 보안 경영 시스템 BS 7799는 정보 보안 문제가 직면하는 위협을 파악하고 관리하여 최소화 시켜주는 중요한 방편 중 하나이다. ISO /IEC 17799 Part 1은 정보 보안 관리에 대한 실행 지침이고, Part 2는 정보보안 관리 시스템에 대한 규격으로서 10개의 관리항목에 걸쳐 36개의 통

제목표와 127개의 세부 통제방안으로 구성되어 있다. 영국의 UKAS(UK Accreditation Service)는 EA의 회원기관이며 UKAS의 승인을 받은 인정기관은 국제적인 승인을 받은 것과 같은 인정을 받게 된다. 영국 이외에 스웨덴, 독일, 네덜란드 등에서도 BS7799과 관련하여 인증업무를 하고 있다. 또한 미국의 TruSecure 관리체계 인증 서비스는 프로세스 개념의 순환 반복적인 BodyGuard Serice 형태의 보안 서비스로 TruSecure의 진단 및 솔루션 제시에 따라 적정 수준에 오르면 정보보호관리체계 인증과 유사한 TruSecure 인증을 부여한다. 미국 상무성 산하 국가표준기술연구소(NIST Handbook), 회계 감사국(GAO/AIMO), CIO협의회를 중심으로 관리지침을 개발(Best Security Practices)하여 보급하여 국가 주요기반구조 보호에 적용하고 있다. 일본은 국제적인 추세를 반영하기 위하여 ISO/IEC17799를 근간으로 하는 정보보호관리기준(JIS표준화 2000.12)표준화를 완료했다.

3.2 국내동향

2000년 12월 ISO가 정보보안 국제표준으로 BS7799를 채택했다(ISO 17799) 정보보호는 국제 전자상거래 등에 있어 갈수록 그 중요도가 더해지고 있기 때문에 국제인증의 획득 여부는 기업의 국제 경쟁력에 큰 차이가 있을 것이 예상되며, 업계에서는 국내시장은 물론 수출 노선에 커다란 걸림돌로 작용할 것으로 보고있다. 이는 국내 정보보호 산업계의 보안 수준을 한 단계 높이는 전기가 될 것으로 예상된다. 국내의 경우도 현재 정보통신부 장관이 인증하는 정보보호관리체계인증제도를 도입하고자 BS 7799를 기반으로 연구, 검토를 진행하고 있으며, 현재는 은행 등의 금융권과 증권, 보험사 같이 고객정보가 자산의 핵심인 사업을 중심으로 BS 7799인증이 시작되고 있으나, 조만간 제조분야 및 광범위한 서비스분야로 인증의 폭이 넓혀질 전망이다.

4. 국내 생체인식 산업의 시스템(보안) 표준화

국제표준으로는 정보보호시스템의 실행 지침인 Part1이 작년 2000.12월 ISO에서 채택되었고, 실행 규격인 Part2는 심의 중에 있고, 국제표준으로 채택될 확률이 매우 높다. 시스템표준화를 주도하고 인증을 하고 있는 영국 내에서도 본 규격을 취득한 조직은 소수이며 시험인증을 하고 있다. 국내의 동향은 한빛은행을 시작으로 금융권을 중심으로 벌써부터 BS7799 인증을 획득하지 못할 경우 국내 시장은 물론 해외 수출 노선에 커다란 걸림돌로 작용할 것이라는 우려가 제기되고 있고, 이런 가운데 국내 정보보안업체 및 컨설팅업체 들의 BS7799 획득 붐이 일고 있다. 시스템 표준화 부문은 향후 선진국과의 격차를 줄일 수 있는 부문이다. 국제표준과 다른 국내 정보보호 인증제도의 특징은 다음과 같이 6가지로 요약할 수 있다. 첫째, 국내 실정에 적합한 정보보호관리 모델을 개발했다는 것이다. 둘째, [표4-1]에서도 보듯이 조직이나 환경적인 측면의 뿐만 아니라 기술적인 부문을 강화했다.
셋째, 문서화 부분을 대폭 간소화하여 실용적인 면을 강조했다. 넷째, 국내 보안컨설팅

의 역량 강화 및 품질보증을 지향했다. 다섯째, [표4-1]과 같이 보안 전문가들에 의한 인증심사이다. 이는 자칫 정보시스템 전반에 평가 즉, 시스템 평가가 기술적인 면을 강조한 평가로 치우칠 수 있다. 여섯째, 국가 정보보호 전문기관에 의한 평가 및 인증 방법이다.

[표 4-1] 국내 ISMS와 BS7799의 비교

내 용	국내 ISMS	BS 7799
주관부처	정보통신부	상무성
인정기관	없음	UKAS
인증기관	KISA	UKAS지정 인증기관
인증주체	제3자 인증	제3자 인증
표준화	단체표준	영국표준(BS7799 PART 2)
심사방법	취약점 점검등 기술적 부문 강화	ISO품질, 환경심사에 준함
심사원	보안 전문가 및 전문가 팀 구성	기존 ISO심사원

정보시스템의 발전과 개방형 시스템의 상호접속 등의 정보환경의 변화로 인하여 정보보호관리의 필요성은 더욱 고조되고 있는데, 정보시스템의 보안대책 미비로 인한 손실은 이제 천문학적인 숫자로 치달아 한 순간에 기업 또는 조직의 붕괴를 가져올 수도 있다. 이에 대한 정부 공공기관이나 민간기관 기업 등 사회의 각 분야는 정보시스템에 의한 정보처리의 의존도는 더욱 증가하고 있다. 정보보호시스템인증제도의 도입 및 구축효과는 기업 또는 조직의 주요 자산을 보호하고 정보보호관리 frame work를 구축하고, 사업의 연속성을 보장해주며, 무역거래 당사자간의 안정성을 보장한다. 그러나 생체인식 산업의 표준화의 관점에서 정보시스템의 표준화는 다음과 같은 면에서 그 의의가 크다고 할 수 있다. 첫째, 시스템 표준화는 제품표준화의 나아갈 방향을 제시 할 수 있는데, 이는 시스템 표준이 제품표준 보다 상위의 level이기 때문이다. 또한 시스템 표준은 제품표준화를 앞당기는 효과를 발휘하고, 제품표준을 더욱 견고히 하는 역할을 수행한다. 둘째, 생체인식시스템의 보안 평가용으로 활용 가능한 BS7799/ISO17799는 국내외의 격차가 다른 부문보다 적다는 점이다. 이는 학계에서 주장되어 그 타당성과 유효성이 호응을 얻고 있다. 생체인식 산업의 국내외 표준화 동향을 근거로 국내 정보보호시스템의 표준화 방안을 구축 시 고려해야 할 점을 살펴보기로 한다. 첫째, 도입이나 구축에 앞서 기업이나 조직에서 정보 시스템 인증의 필요성을 충분히 고려한 후에 실시해야 한다는 것이다. 이를 위해 조직 내부의 필요성 검증과 조직을 둘러싸고 있는 경영환경의 변화 등에 대해 면밀히 검토해 볼 필요가 있다. 둘째, 섣부른 국제규격의 도입은 아까운 외화만 낭비할 수 있다. 국내에서도 BS7799에 버금 가는 정보화 경영체제(IMS)가 있다. 선진국의 규격이라고 무조건 도입을 서두를 것이 아니라 기업 또는 조직의 보안에 대한 사전 검토와 국내규격으로 활용가치 등을 먼저 검토해야 할 것이다. 셋째, 기술적 부문을 강조한 나머지 자칫 정보시스템 전반에 평가 즉, 시스템 평가

가 기술적인 면을 강조한 평가로 치우칠 수 있다. 이는 조직 구성원이나 IT관리자, 경영진의 사고방식부터 바뀌어야 한다는 것을 의미한다. 실제로 정보보호의 유출은 외부 해킹에 의한 사고보다는 내부 조직원에 의한 경우가 대부분이므로 관리부분이 중요한 것이고, 당연히 시스템적인 평가로 이어져야 한다는 것이다. 넷째, 인증을 위한 도입이나 구축은 지양해야 한다. 이는 자칫 문서관리에 치중한 나머지 진정한 시스템의 부가가치를 향상하는 목적보다는 대외 홍보용으로 오용 될 수도 있다. 한가지 예로 ISO 9000과 14000을 들 수 있다. 국내에 도입된 지도 벌써 10년이 지났지만 진정한 경영시스템의 도구로 그 효용가치를 발휘하는 예는 드물다. 다섯째, 경영관리의 도구로 활용되어야 비로서 그 위력과 생명력이 연장될 수 있다. 자칫 단위 부서나 일시적인 활동의 일환으로 그친다면 그 의미가 퇴색한다고 할 수 있다.

5. 결 론

본 연구는 날로 그 중요성이 증대되고 있는 e-biz환경에서의 정보보안의 새로운 대안으로 제시되고 있는 생체인식 산업의 국내 표준화 방안을 시스템(보안)표준을 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 헌]

[1] 김재희, 생체인식 기술의 현황과 응용, Security world 2000.~2001.
[2] 김학일 外2, 생체인식 System 성능평가를 위한 연구, 정보과학회지 제19권 제7호, 2001.
[3] 김학일, 생체인식 기술 이론 및 응용, 정보과학회지 추계학술발표회, 2001.
[4] 생체인식시스템 시험 및 평가 동향, 주간기술동향 통권 1003호, 2001.
[5] 김학일 外2, 제1회 생체인식 기술표준화 및 평가기술 워크샵, 정보통신부, 2001.
[6] How to Use a Biometric Standard to Assure System Security, XP KPMG, 2001.
[7] NIST Special Publication 500-245, ANSI/NIST-ITL, 2000.
[8] J.L. Wayman, Biometric Technology: Testing, Evaluation, Results, (http://www.engr.sjsu.edu/ biometrics/publications_technology.html)