情 報 保 護 學 會 誌
第21卷 第5號, 2011. 8

개인정보보호 참조 아키텍처와 국제표준화 동향

신 용 녀*, 김 학 일**, 전 명 근***

요 약

개인정보보호법이 전면적인 법 시행을 앞두고 있고 지금까지 규제대상이 아니던 기업 종업원의 개인정보는 물론, 종이문서형태의 개인정보까지를 규제대상으로 삼고 있어 개인정보보호 시장이 크게 확대될 것으로 전망된다. 규제범위도 정보통신, 교육, 의료, 금융 분야까지 다루고 있어서, 정부/공공기관 및 민간기업의 철저한 사전준비가 필요한 시점이다. 개인의 프라이버시 보호에 대한 이러한 발전추세에는 국내외 표준화기구를 통한 활발한 표준화작업이 밑바탕이 되고 있으며, 특히 미국, 영국, 독일, 일본, 한국 등의 나라를 중심으로 국제표준화를 활발히 추진하고 있다[1]. 표준화의 분야에는 개체의 신분확인을 위한 표준, 개인식별정보와 바이오인식 정보가 같이 사용되는 상황에서 이들의 바이오인식 프라이버시 및 보안요구조건을 위한 표준, 프라이버시 프레임워크, 프레임워크 기반 구현을 위한 프라이버시 레퍼런스 아키텍쳐 등 다양한 표준화 분야가 있다. 본 논문에서는 프라이버시 표준화를 위한 국외 표준화 동향을 소개하고, 향후 추진해야할 중점 표준화 항목을 도출한다.

Ⅰ. 서 론

프라이버시는 인간의 기본권이다[2]. 미국에서는 개인정보를 일반적으로 의료정보, 사회보장번호, 은행정보와 같은 특별한 영역으로 제한하고 있지만 유럽이나 다른 여러 나라에서는 개인을 식별할 수 있는 모든 정보로 훨씬 광범위하게 정의하고 있다. 그리스, 핀란드, 영국, 프랑스, 캐나다, 호주, 뉴질랜드 등 많은 국가에서 개인정보 보호를 위해 다양한 법적 제도적 규범을 만들어 운영하고 있다. 국제사회의 개인정보보호 노력은 1980년에 OECD가 회원국에게 권고한 '개인정보의 국제적 유통과 프라이버시 보호에 관한 지침'을 출발점으로 볼 수 있다. UN은 개인정보 전산화 지침을, EU는 개인정보의 처리와 보호에 관한 지침을 공표하였다. OECD의 개인정보보호 지침은 개인정보의 수집 및 관리에 관한 국제사회의 일치된 의견을 반영한 것으로 각국의 개인정보보호법에 많은 영향을 끼쳤다. OECD의 개인정보 지침은 적용 범위 등을 규정하고 있는데, 공적 및 민간 부분의 위험이 있는 개인정보 그리고 전산처리와 관련된 개인정보에 한정하여 적용하도록 하였다. 또한 이는 최소한의 기준으로 간주되어야 하며 추가적 조치에 의하여 보충할 수 있음을 명시하고 있다. 이 밖에도 APEC은 개인정보 침해방지, 수집제한, 정보이용, 정보주체의 선택, 고지, 최신성, 안전성, 접근성, 책임에 따른 프라이버시 원칙을 제시하고 있다.

ISO/IEC JTC1 SC27 워킹그룹(Working Group) 5에서는 이러한 개인의 기본권인 프라이버시 보호를 위한 표준화 작업에 착수하여, 프라이버시 프레임워크(Privacy Framework) 와 프레임워크 구현을 위한 프라이버시 레퍼런스 아키텍처(Privacy Reference Architecture)에 대한 표준화에 주력하고 있다. 국내에서도 개인정보보호법이 전면적인 법 시행을 앞두고 있고 지금까지 규제대상이 아니던 기업 종업원의 개인정보는 물론, 종이문서형태의 개인정보까지를 규제대상으로 삼고 있어 개인정보보호 시장이 크게 확대될 것으로 전망된다. 규제범위도 정보통신, 교육, 의료, 금융 분야까지 다루고 있어서, 정부/공공기관 및 민간기업의 철저한 사전준비가 필요한 시점이다. 개인의 프라이버시 보호에 대한 이러한 발전추세에는 국내외 표준화기구를 통한 활발한 표준화작업이 밑바탕이 되고 있으며, 프라이버시

본 연구는 지식경제부의 지원을 받는 정보통신표준화 및 인증지원(2011-PM10-18)의 연구결과로 수행되었습니다.
* 한양사이버대학교 컴퓨터공학과(ynshin@hycu.ac.kr)
** 인하대학교 정보통신공학과(hikim@inha.ac.kr)
*** 충북대학교 전자공학부(mgchun@chungbuk.ac.kr)

에 대한 관심은 더욱 높아지고 있다. 정보통신기술의 발전과 더불어 대두되고 있는 정보보호 기법의 표준화에 대한 요구에 부응하여, 암호화 기법 등을 이용한 정보보호기법과 이들 기술에 대한 평가 등을 담당하였던 SC27이 개인정보보호와 관련이 있는 프라이버시 분야, 바이오정보보호, 신원(identity) 관리 분야로 그 영역을 넓혀나가는 것은 우리나라를 포함하여 각국에서 대두되고 있는 프라이버시 및 개인정보보호 관련 사회적 이슈를 해결하는데 크게 도움이 되리라 생각된다. 이에, 본 논문은 프라이버시 보호 기술과 관련된 표준화 기구를 소개하고, 워킹그룹(Working Group) 5의 프라이버시 주요 표준화 동향에 대하여 간략하게 소개하고자 한다.

본 논문의 구성은 다음과 같다. 본 논문의 2장에서는 정보보호 분과인 ISO SC27인 소개와 함께, 워킹그룹(Working Group) 별 표준화 동향에 대해 살펴보고, WG5에서 추진중인 개인정보보호 참조 아키텍쳐 표준에 대해 살펴본다. 마지막으로 3장에서 본 논문의 결언을 맺는다.

Ⅱ. ISO SC27 표준화 동향

2.1 ISO/IEC JTC1 SC27

ISO/IEC JTC1 SC27(IT Security Techniques)은 ISO와IEC가 공동으로 설립한 JTC1의 27번째 위원회로서, 암호화 기술의 국제표준을 담당하던 SC20(Cryptographic Techniques)의 표준화 기능을 확대 계승하여 만들어진 것이다. 1989년 JTC1 총회에서 설립이 결정되어 1990년 4월 스웨덴에서의 창립총회를 통하여 범위, 조직 등이 갖추어졌다. 일본 도쿄에서의 제2회 회의를 시작으로, 매년 2회의 WG회의와 1회의총회를 개최하고 있다. 현재 SC27은 36개국의 P-member와 13개국의 O-member들이 활동하고 있다. ISO/IEC JTC1 SC27 표준화 분과위원회는 2005년도까지는 3개의 Working Group이었으나, 논의된 SC27 new structuring에서 WG1과 WG4로 나누고, Privacy, ID management, biometrics를 다룰 WG5를 신설하여 총 5개의 Working Group으로 확장하는 안을 통과시켜, 2006년부터 SC27은 5개의 워킹그룹(Working Group)으로 재구성 되었다. 각 워킹그룹별 주요 업무현황은 다음 [표 1]과 같다[3].

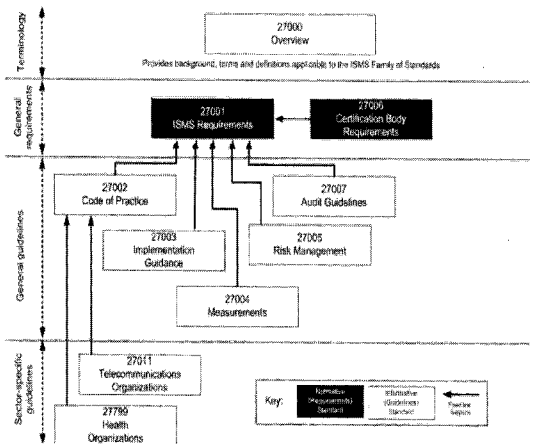
〔표 1〕 ISO/IEC JTC1 SC27 내 워킹그룹 현황

워킹그룹	업무현황	의장
WG1 (Information Security Management Systems)	정보보안관리 시스템(ISMS) 관련 표준정의	E. J. Humphreys 영국
WG2 (Cryptography and Security Mechanisms)	암호기법 및 보안메커니즘에 대한 연구 및 표준화 작업에 필요한 관련 기술의 국제표준 제정	T. Chikazawa 일본
WG3 (Security Evaluation Criteria)	IT 시스템과 이에 따른 구성장치 그리고 제품의 보안평가와 인증을 위한 평가 기술 국제표준 제정	M. Banon, 스페인
WG4 (Security Controls and Services)	알려진 보안 이슈의 발생을 막고 관리하기 위한 필요성, 정보보호시스템의 고장 혹은 자연재해로 인하여 발생하는 사고나 정보보호 이슈를 포함하는 관리에 관한 표준 제정	M.-C. Kang, 싱가폴
WG5 (Identity Management and Privacy Technologies)	ID 관리와 프라이버시 기술, 프라이버시 연관 바이오인식 기술에 대해 표준 제정	K. Rannenberg, 독일

o WG1 - 정보보안경영시스템
(Information Security Management Systems)

SC27의 WG1에서는 정보보안관리 시스템(ISMS, Information Security Management System)에 관한 표준화 작업을 진행한다. ISO 27000시리즈는 정보보호를 단순히 기술적 이슈로 보는 것이 아니라 기술, 물리, 관리적 통제들을 포함하는 전사적 차원의 정보보호를 구현하기 위한 체계화된 일종의 경영시스템으로 보는 것이다. 즉 IS 9000 시리즈(품질경영시스템)나 14000시리즈(환경경영시스템)와 같이 하나의 경영시스템으로서 정보보호를 계획, 구현, 유지보수 및 검토, 지속적 개선 등과 같은 일련의 프로세스로서의 활동을 중요시 하고 있다. ISO 27000(Overview & vocabulary)은 ISMS 관련 표준문서의 구조와 상관관계를 보여주며 공통적으로 사용하는 82개의 용어정의를 포함한 표준이다. ISO 27003(Implementation guidance)은 ISMS 구현을 위한 프로젝트 수행 시 참고할 만한 구체적인 구현 권고사항을 규정한 규격으로, 문서구조를 프로젝트 관리프로세스에 맞추어 작성하고 있다. ISO27004(Measurement)은 ISMS와 구현된 정보보호 통제의 유효성(Effecti-

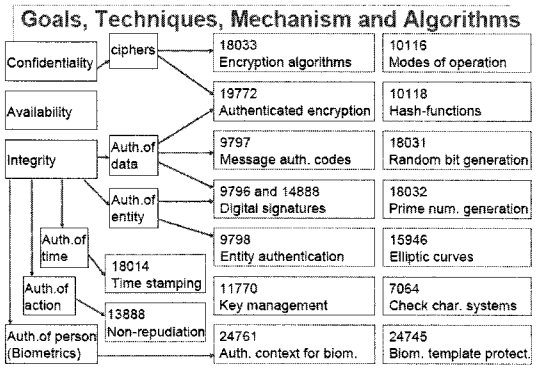
veness)을 측정하기 위한 프로그램과 프로세스를 규정한 규격으로 무엇을, 어떻게, 언제 측정할 것인지를 제시하여 정보보안의 수준을 파악하고 지속적으로 개선시키기 위한 문서이다. ISO 27005(Risk management)는 위험관리 과정을 환경설정, 위험평가, 위험처리, 위험수용, 위험소통, 위험모니터링 및 검토 등 6개의 프로세스로 구분하고, 각 프로세스별 활동을 input, action, implementation guidance, output으로 구분하여 기술한 표준이다. 그림 1에서 확인할 수 있듯이 전반적인 ISMS 표준이 안정화 단계에 접어들면서 국가기반시설 및 전자정부 등을 포함하는 섹터별 정보보호관리체계 수립에 관한 표준화작업이 활발하게 진행되고 있다.



〔그림 1〕 ISO/IEC JTC1 SC27/WG1 표준안의 관계

o WG2 - 암호화 및 정보보안 메커니즘
(Cryptography and Security Mechanisms)

SC27의 WG2는 암호기법 및 보안메커니즘에 대한 연구 및 표준화 작업을 진행한다. 주요 표준은 암호화(Encryption), 디지털 서명(Digital Signature), 실체인증(Entity authentication), 메시지 인증 코드(MACs, Message Authentication Codes), 해쉬함수(Hash-functions), 부인봉쇄(Non-repudation), 키관리(Key management), 시점확인(time stamping services and protocols), 수리및 암호기법(Mathematic and cryptographic techniques), 새로운 암호 기법으로 나눌 수 있다. 18033-3의 Encryption algorithm-Part 3: Block cipers의 개정판에 포항 공대 이필중교수가 에디터로서 선임되어 HIGHT 알고리즘을 반영하였다. WG2에서 진행중인 과제들의 전체적인 구조와 이들 간의 관계는 그림 2에 나타내었다. 기본적으로 IT 시스템의 보안 요구조건인 무결성, 기밀성을 제공하기 위한 암호화 기법및 전자서명기법을 주로하고 이들을 지원하기 위한 여러 가지 수학적 기법에 대한 표준이 진행 되고 있음을 알 수 있다 [7][8].



〔그림 2〕 ISO/IEC JTC1 SC27/WG2 표준안의 관계

o WG3 - 정보보안 평가 기준
(Security Evaluation Criteria)

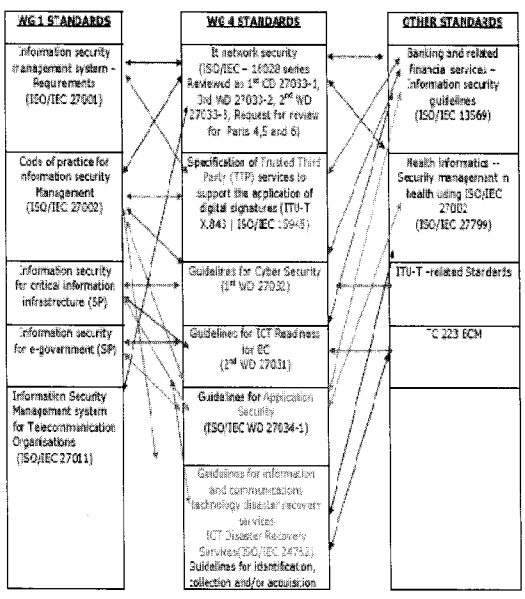
SC27의 WG3은 정보보안 평가 기준에 대한 연구 및 표준화 작업을 진행한다. WG 3은 IT 시스템과 이에 따른 구성장치 그리고 제품의 보안평가와 인증을 위한 표준을 개발하기 위하여 평가 기준, 평가 기준의 적용을 위한 방법론, 평가, 인증, 인정 기법들에 대한 운영 절차를 표준화한다.

o WG4 - 정보보안 관리 및 서비스
(Security Controls and Services)

SC27의 WG4는 현재는 알려져 있지 않거나, 새롭게 떠오르는 보안관련 이슈, 알려진 보안 이슈의 발생을 막고 관리하기 위한 필요성, 정보보호시스템의 고장 혹은 자연재해로 인하여 발생하는 사고나 정보보호 이슈를 포함하는 관리에 대해 표준화 한다.

WG4의 표준은 WG1에서 개발된 ISO/IEC 2700x 표준안들을 지원하지만 반드시 ISO/IEC 2700x내의 범위에 한정 지을 필요는 없다. 예를 들어, 사이버보안(Cybersecurity)은 기존의 ISMS 체계의 범위를 벗어나는 것이라 할 수 있다. ISO/IEC 27032 표준안의 경우에서와 같이 인터넷/사이버공간 관련한 응용 서비스의 안전한 제공과 개인의 안전한 사이버공간 사용에 대해서도 다룬다. 또한, 재해나 사고로 인하여 비즈니스가

중단될 수 있는 사건이나 보안 사고에 대한 대응력을 향상시키도록 도와주는 관련표준, 가이드라인, 용어 등을 포함하고 있다. 사이버보안(Cyber security)은 스파이웨어(Spyware), 피싱(Phishing), 스팸(Spam)과 같은 새로운 이슈에 중점을 두어서 ISO/IEC 27001의 일정 부분인 통제 기능의 구현을 용이하도록 도와주는 가이드라인, 요구조건 용어 등을 포함하고 있다. 현존하는 다수의 ITU-T SG17과제를 채택하거나 같이 개발되는 형태를 띄고 있다. IT 네트워 보안(IT Network security)은 현재 개정되고 있는 네트워크 보안 표준(ISO/IEC 27033)와 잠재적인 새로운 표준으로 차세대 네트워크 보안, 홈 네트워크, 모바일 네트워크를 지원하기 위한 가이드라인, 요구조건 용어 등을 포함하고 있다. 응용보안(Application Security)은 응용소프트웨어의 개발을 포함한 비즈니스 어플리케이션 생명주기에 관한 현존하거나 나타나고 있는 보안 문제들에 대한 최적의 예를 장려하고 지침을 주기 위해 관련된 표준들과, 가이드라인 용어 등을 포함하고 있다. 이 표준은 비즈니스 어플리케이션 개발자 뿐만 아니라 감사나 관리자들에 의해서 사용되어 지기를 염두에 두고 있다. 표준은 기구들로 하여금 보안요구사항을 만들어내고 보안위협을 평가하고, 원하는 신뢰수준을 파악하고, 해당하는 보안 대책과 인증통제와 그들 스스로 보안 가이드라인을 만들기 위한 프로세스 관점의 메커니즘을 제공하다. 신뢰성 있는 제 3자 서비스 보안(Trusted Third Parties Services Security)에서는 TTP의 정의를 재고함으로서 아웃소싱 서비스 제공자, Offshoring 제공자 등의 가능성을 결정한다. 포렌식과 수사를 위한 보안 표준은 정보보안 사고와 관련된 포렌식 및 수사를 수행하기 위한 행위를 수행하기 위해 관련된 표준과, 요구사항, 가이드라인, 용어 등을 제공한다. 디지털 증거 수집(Digital Evidence Acquisition)에 관한 "Guidelines for Identification, Collection, and/or Acquisition and Preserving of Digital Evidence"가 진행 중에 있다. 그림 3에서 WG4의 표준화 과제와 타 과제와의 관련성을 확인할 수 있다.



〔그림 3〕 WG4의 표준화 과제와 타 과제와의 관련성

o WG5 - 신원 관리 및 개인정보 보호 기술 (Identity Management and Privacy Technologies)

WG5는 ID 관리(Identity management)와 프라이버시 기술(Privacy technologies)에 대해 표준화 하고 있

〔표 4〕 WG5 (ID 관리 및 프라이버시 보호) 표준화 추진 현황

표준화 상태	표준 번호	표준명	에디터 (국가)
IS	24745	Biometric Information protection	전명근 (한국)
IS	24761	Authentication context for biometrics	Yamada Asahiko (일본)
FDIS	24760	part1 : Technology and Concept	Christophe Stenuit (이탈리아)
WD (1st)		part2 : Reference Frameworke and Requirements	Edward de Jong, José Fernando Carvajal
WD (1st)		part3 : Practice	Edward de Jong, José Fernando Carvajal
FDIS	29100	Privacy framework	Stefan Weiss (독일)
CD (3nd)	29101	Privacy reference architecture	Hans Hedbom (미국)
CD (3nd)	29115	Entity authentication assurance	Brackney (미국)
WD (5nd)	29146	A framework for access management	José Fernando Carvajal Vion (스페인)
CD (2nd)	29191	Requirements on relative anonymity with identity escrow	Kazue Sako (일본)

으며, Published 된 표준은 일본에서 주도한 ACBio (Authentication Context for Biometrics)와 한국 주도의 Biometric Information Protection이다[9]. WG5내에서 사용되는 용어를 위한 harmonization of vocabulary Standing Document(SD3)를 만드는 목적에 대한 비규범적(non-normative)인 베이스라인 정의를 내리고, 총 25개의 대상 용어를 선정하여 추후 문서의 revision을 통해 용어정의가 이루어질 것으로 판단된다. 표 2는 ID관리 및 프라이버시관련 WG5의 표준화 추진 현황이다.

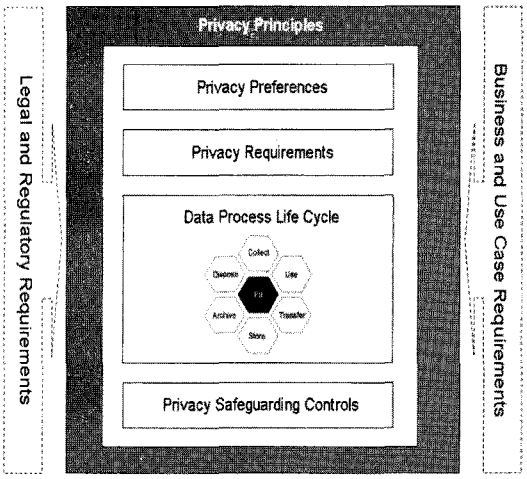
2.1.1 프라이버시 프레임워크(Privacy Framework)

오늘날 모든 정보 통신 시스템은 다양한 형태나 방식으로 개인 식별 정보(personally identifiable information; PII)를 실제적으로 처리하고 있다. 과거의 보안관련 표준은 이러한 시스템에 의해 처리되고 있는 시스템과 정보를 보호하는 방법에 대해서 공통의 이해와 실행방법을 설정하였다. 그렇지만 현존하는 어떠한 정보보호 표준안도 개인이 자신의 정보를 통제할 수 있는 권리를 고려하지 않고 있다. 더군다나, 개인정보의 프라이버시를 보호하기 위해서 개인 확인 정보를 분류하고 시스템을 설치하는 일관적인 실행방법이 없다.

개인 확인 정보의 상업적 이용의 증가와 법적 제도적 장치를 통한 개인정보의 공유, 정보통신시스템의 복잡도 증가는 기업으로 하여금 그들 고객의 프라이버시를 보호하고 다양한 프라이버시 규정을 준수하기가 어려워지고 있다. 더욱이, 전자상거래의 경우와 같이 개인정보의 오용의 경우가 증대할 뿐만 아니라, 개별 기업에 대하여 특정 고객의 불확실성이나 불신이 기업의 성공을 가로 막는 중요한 장애가 되고 있다. 경제적이고 기술적 관점에서 프라이버시의 표준화에 대한 요구는 계속하여 증대되고 있다. 전자상거래에 있어서 신뢰를 구축하는 것은 소비자의 개인정보가 프라이버시 관련 규정을 준수할 수 있게끔, 처리하고 다루어 질 수 있도록 보장하는 것으로만 이루어지는 것이 아니라 심지어 개인의 자기정보 통제권이 행사 될 수 있도록 적절한 기술적 기능을 제공해 줄 수 있어야 한다. 프라이버시 프레임워크는 개인식별 정보를 처리하는데 있어서의 정보와 통신기술의 요구 사항을 다음과 같은 방식에 의해 가이드라인을 제시하고자 하는 것을 목표로 한다[4].

- 프라이버시에 관한 국제적으로 공통될 수 있는 용어 통일
- 프라이버시에 대한 선호도와 요구사항 범주화
- 알려져 있는 프라이버시 원칙들의 참조
- 현존하는 보안 가이드라인과 정보프라이버시와의 관계분석

프라이버시 프레임워크 표준안에서 기술하고자 하는 정보통신시스템에서의 개인식별정보를 처리하거나 프라이버시에 관여하는 주요 요소와 기본적인 프레임워크는 아래의 그림 4와 같다. 본 표준안을 개발하는 데 사용된 프레임워크나 개념, 정의, 권고 사항 등은 OECD 가이드라인, APEC(Asia-Pacific Economic Cooperation)과 ISTPA(International Security, Trust & Privacy Alliance)의 프라이버시 프레임 워크, 모트리올 의정서(Montreux Declaration) 등을 반영하였다. 안에서 기술하고자 하는 정보통신시스템에서의 개인식별정보를 처리하거나 프라이버시에 관여하는 주요 요소와 기본적인 프레임워크는 아래의 그림 4와 같다. 본 표준안을 개발하는 데 사용된 프레임워크나 개념, 정의, 권고 사항 등은 OECD 가이드 라인[2], APEC(Asia-Pacific Economic Cooperation)[1]과 ISTPA(International Security, Trust & Privacy Alliance)의 프라이버시 프레임 워크, 모트리올 의정서(Montreux Declaration) 등을 반영하였다.



〔그림 4〕 프라이버시 프레임워크의 전체 구성

먼저, 처리되어야할 데이터는 개인식별정보(PII)와 그렇지 않은 정보로 나뉜다. 만일 데이터가 PII로 분류

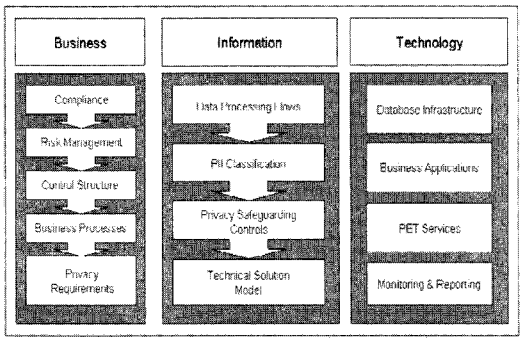
되면, 프라이버시 프레임워크는 개인식별정보가 그것의 수명 주기 동안에 보호되고 되기 위해서 PII 취급자뿐만 아니라 이를 넘겨받을 잠재적인 제 3자에게 적용될 프라이버시 요구사항과 원칙들을 기술하고 있다. 프라이버시 요구사항은 첫째, 개인의 프라이버시와 개인식별정보를 보호 할 수 있는 법적 제도적 요구사항 둘째, 기업과 사용자 경우에 따른 요구사항 셋째, 개인의 프라이버시 기호에 따른 요구 사항으로 나뉘어 표준화 되고 있다.

2.1.2 프라이버시 레퍼런스 아키텍처(Privacy Reference Architecture)

프라이버시 레퍼런스 아키텍처 표준안은 정보 통신 시스템에서 개인식별 정보를 처리하는데 관여된 프라이버시 요구 조건의 일관적이고 기술적인 구현을 위한 참조모델을 기술한다[5]. 본 표준안은 프라이버시를 다루는 모든 부문의 역할과 책임을 구명할 뿐만 아니라, 데이터의 수명주기 관리기간내의 다양한 단계와 각 데이터 수명 주기에서 요구되는 개인정보를 위한 프라이버시 기능 구현을 포함한다. 프라이버시 참조구조는 시스템 플랫폼간의 개인정보를 적절하게 다루기 위한 시스템 구조를 설계하고 구현하는 가이드라인을 제시한다. 다양한 데이터 생명주기 내의 특정한 데이터들에 대한 제어와 데이터의 분류를 가능하도록 하는 필요 전제조건들을 제시하고자 하며 다음을 목표로 하고 있다.

- 상위레벨에서의 정보통신시스템에서 개인정보보호를 위한 프라이버시 구현을 위한 접근 방법
- 개인정보 처리를 위한 적절하고도 효과적인 시스템 구축방법
- 각 생명 주기별 개인정보보호를 위해 요구되는 함수정의
- 개인정보를 분류하기 위해 필요로 하는 요구조건
- 프라이버시 안정보장의 구현을 위해 필요한 프라이버시 증강 기술

프라이버시 참조 구조는 프라이버시 안정보장을 위한 제어를 갖춘 정보통신 시스템을 개발하고, 구현하고, 동작시키기 위한 가이드라인을 제시하고자 하는 것이다. 즉, 정보 통신 시스템에서 개인식별 정보를 취급하는데 있어서 가장 모범이 되는 구조를 모아 두는 것이라고 할 수 있다. 프라이버시 참조 모델은 프라이버시 프레임워크에서 기술된 요소들을 커버하는데 필요한 프라이버시 보장 시스템을 만드는데 필요한 디자인 원칙을 기술하는 데 필요하다. 아래 그림 5와 같이 3가지 부분으로 나누어 기술 할 수 있다.



〔그림 5〕 프라이버시 레퍼런스 아키텍쳐 참조 구조

프라이버시 요구 조건을 만족할 수 있는 적절한 기술적 해결 방안을 이해하기 위해서 사업 수행 과정과 이들 중에 처리되는 개인식별정보에 대한 이해가 필요하다. 중요한 비즈니스 과정과 이와 관계되는 개인식별정보를 시각화 하는 것은 프라이버시 보호형 정보통신 시스템을 개발하거나 구현하는데 공감을 이끌어나는데 중요하다. 이런 과정을 통해, 위험요소관리와 통제 구조와 프라이버시 요구조건을 분석해 낼 수 있다. 프라이버시 참조 구조 표준안에서는 Anonymization, Pseudonymization과 같은 프라이버시증진 서비스를 고려하고 있으며, 다음과 같은 프라이버시 증진 기술(PET)을 고려하고 있다. 프라이버시 증진 기술(PET)은 의도하지 않은 혹은 필요하지 않은 개인정보의 프로세싱을 줄이거나 없앰으로써 프라이버시를 보호하는 정보통신기술의 집합체(coherent system)를 말하며, 그 과정에서 데이터 시스템의 기능적 손실이 없어야 한다.

- Limited Show Blind Signatures :

Blind Signature는 서명에 앞서 메시지의 내용의 일부 혹은 전체를 위장 혹은 감춘 뒤 수행하는 전자 서명 방식이다. Blind Signature를 수행한 메시지는 원래의 위장되지 않은 메시지에 대하여 일반 전자서명과 동일한 방식으로 서명된 것을 공인 할 수 있다. Blind Signature는 주로 메시지 작성자와 서명을 수행하는 사람이 다른 조직에 속해 있는 경우 사용하는 프라이버시 보호 관련된 프로토콜에 적용된다. 예를 들어 암호화 투

표시스템과 전자 화폐 기법 등에 사용된다. Blind Signature와 자주 비교되는 실제 행위는 봉투에 메시지를 담아 서명하는 방식이다. 봉투 안에 메시지를 담아 봉인하고, 서명 공간만 보이게 한 다음 서명자가 봉투의 서명란에 서명을 하게 되면, 서명자는 메시지의 내용은 알지 못하지만 메시지는 서명자의 서명이 들어가게 된다. 이로써 제3자는 메시지의 서명을 확인 할 수 있다.

- Biometric Encryption :

Biometric Encryption을 사용하면, 바이오인식정보 샘플을 저장하는 대신에 바이오인식정보 샘플을 이용하여 PIN, 계좌정보, 암호화 키 와 같은 정보들을 암호화하거나 부호화할 수 있다. 이렇게 바이오정보를 이용하여 암호화된 코드만 저장하고 바이오인식정보 샘플은 저장하지 않는다. 이는 바이오인식정보를 데이터베이스에 저장할 필요성을 없애준다. 바이오정보 자체를 이용할 것이 아니라 바이오정보를 이용해 암호화된 개인정보를 사용하면 되기 때문이다. 따라서 데이터베이스에 집중되어있던 프라이버시와 보안관련 관심들이 해소될 것이다. Biometric Encryption은 개인의 바이오인식정보 데이터를 다수의 다양한 식별자 (Identifier)를 제공함으로써 유출된(Compromised) 바이오인식 식별자에 대해 안전성을 보장한다.

- Secret Sharing :

Secret Sharing은 관계자 (participants)의 그룹에 비밀정보를 분산하는 기법을 총칭한다. 비밀정보의 조각들이 합쳐져야만 원래의 비밀정보를 재생성할 수 있고 개개의 비밀정보 조각들은 자체로서는 아무 의미도 없다. 보다 구체적으로 설명하면, 1명의 딜러가 n명의 플레이어에게 비밀정보를 분산한 다음 특별한 조건이 만족되면 t명 (threshold) 이상의 플레이어가 모여야만 원래 비밀정보를 재생성 할 수 있다. Secret Sharing 기법은 이처럼 비밀정보를 여러 서버에 안전하게 분산 할 수 있고 다수의 서버가 고장 나더라도 비밀정보를 복구할 수 있다. 공격자가 특정 서버를 공격하더라도 비밀정보의 조각 하나만을 얻을 수 있을 뿐이며, 다른 서버를 알 수 없고, 남은 서버가 t개 이상인지 여부도 확인할 수 없다.

- Privacy Preserving Data Mining :

Privacy Preserving Data Mining (PPDM)은 데이터 마이닝시에 노출 될 수 있는 Personally Identifiable Information (PII)에 대한 프라이버시 문제를 고려한 기술이다. 특히 PPDM은 데이터 마이닝의 목적에 맞게 공공에 정보를 제공할 때에, 개인 정보를 유출하지 않으면서 동시에 데이터 마이닝 알고리즘의 높은 정밀도를 유지할 수 있도록 하는 것이 목표이다. PPDM 기술은 크게 쿼리 제한 기법과 데이터 교란 기법으로 분류할 수 있다. 쿼리 제한 기법에는 쿼리결과 사이즈 제한, 계속되는 서비스의 중첩 제어, 응답된 쿼리에 대한 추적감사를 통한 Compromise 체크등의 기법이 있고, 데이터 교란 기법에는 레코드 간 값 교환, 샘플을 통한 원본 데이터베이스 정보 교체, 데이터베이스에 노이즈값 추가, 쿼리 결과에 노이즈 추가, 쿼리결과 샘플링 등의 기법이 있다.

- Unlinkable databases :

Unlinkability는 공격자가 아이템들의 연관관계를 파악하는 능력이 시스템을 관찰함으로써 향상되지 않는 것을 의미한다. 즉 공격자가 시스템을 관찰하더라도 아이템간의 연관관계를 찾기 어려움을 의미한다. 공격자는 다양한 정보를 연관지어 프로파일을 만듦으로서 사용자를 식별해 낼 수 있다 (re-identify). 하지만 Unlinkability는 사용자가 자원이나 서비스를 이용함에 있어서 그들이 서로 연관되지 않음을 보장한다. Unlinkable 데이터베이스는 데이터베이스 시스템에 Unlinkability가 적용된 모델로, Unlinkable 데이터베이스에서는 어트리뷰트(컬럼) 간이나 결과 set등에 Unlinkability가 적용되어 공격자가 관찰을 통해서 연관성을 찾을 수 없게 한다.

- Unobservable data management :

Unobservability 는 사용자로 하여금 다른사람 특히 제3자로 하여금 자원이나 서비스를 사용하고 있는지 관찰되지 않는 가운데 자원과 서비스를 사용할 수 있도록 보장한다. Unboserability는 사용자 혹은 주체가 어떤 명령이 수행되고 있는지를 판별할 수 없을 것을 요구한다. Unobservability는 실시간적으로 unlinkability와 유사성을 보이는데, 유일한 차이점은 Unobservability는 자원이나 서비스의 사용을 감추려는 행위이고, Unlinkaility는 사용자의 identity를 감추려는 것이다.

Ⅲ. 결 론

개인식별정보(PII)를 보호하는 것은 인간의 기본권인

동시에, 지식사회의 개인 자산을 보호하는 개념과 직결된다. 국내외적으로 스마트폰을 통한 개인의 위치정보 및 구글의 스트리트 뷰를 통한 개인정보 침해 사례가 일상화되면서 프라이버시 보호를 위한 국제 표준안인 프라이버시 프레임워크(Privacy Framework)와 프레임워크 구현을 위한 프라이버시 레퍼런스 아키텍쳐(Privacy Reference Architecture)에 대해 주목할 필요가 있다[12][13].

프라이버시 프레임워크는 개인식별 정보를 처리하는데 있어서의 정보와 통신 기술의 요구 사항에 의해 가이드라인을 제시하고자 하는 것을 목표로 하고, 프라이버시 참조 구조는 프라이버시 안정보장을 위한 제어를 갖춘 정보통신 시스템을 개발하고, 구현하고, 동작시키기 위한 가이드라인을 제시하고자 하는 것이다. 이러한 프라이버시 분야 국제 표준화 동향을 파악하고 국내 Personal Information Management System 제도의 효율성 제고 및 프라이버시 분야 한국 주도 국제표준화 전략을 수립이 필요한 시점이다. PIMS(개인정보보호관리체계)는 개인정보 유출 방지를 위한 요건을 갖춘 업체에 부여하는 국내 자율 인증이다. 개인정보 영향평가란 개인정보를 수집 이용하는 경우에, 사전에 개인정보 침해 요소를 평가하여 개선할 수 있도록 하는 절차로써, 사후 대응에 비해 효율적으로 사업을 추진하고 예산을 절감할 수 있다.

또한, WG5에서 유출 시 프라이버시 침해 요소가 큰 바이오보안 토큰의 이용에 관한 국제 표준화를 통하여, 우리나라의 전자 정부 솔루션을 채택하고자하는 관련 국가에 우리나라 기업이 진출할 수 관련 표준안이 있다면, 관련 산업 활성화에 기여 할 수 있으리라 생각된다. 바이오보안 토큰은 기존의 공인인증서를 안전하게 관리하기 위한 보안토큰에 바이오인식 기법을 접목시키는 임베디드 형태의 USB 인터페이스 형태로, 전자금융환경 및 전자입찰에 현재 활용되고 있는 기술이다[14].

이처럼 개인정보보호 분야 산업체에 새로운 시장을 창출 할 수 있는 중요한 표준과제를 진행하기 위해서는 산업체와의 긴밀한 협력 및 적극적인 표준화 참여 가 필요하다. 따라서 개인정보보호 관련 표준화 활동에 국내 산업체, 정부출연 연구기관, 그리고 학계의 적극적이며 지속적인 관심과 참여가 우선되어야 한다.

참고문헌

[1] Asia Pacific Economic Cooperation (APEC), "APEC Privacy Framework," 2005.

[2] http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", 1980.

[3] http://www.law,cornell.edu/rules/frcp/index.html #chapter_v, "Federal Rule of Civil Procedure."

[4] ISO/IEC JTC1 SC27 Privacy Framework, SC27 N9226, May. 2011.

[5] ISO/IEC JTC1 SC27 Privacy Reference Architecture, SC27 N9228, May. 2011.

[6] ISO/IEC JTC1 SC27 WG5 StrudyPeriod Vocabulary, SC27 N9401, May. 2011.

[7] ISO/IEC JTC1 SC27 WG5 Recommendation, SC27 N9237, May. 2011.

[8] ISO/IEC JTC1 SC27 Buisiness Plan for JTC1 SC27 "Security Technique," SC27 N9463, Jun. 2010.

[9] ISO/IEC JTC1 SC27 WG5 Resolution, SC27 N9920, May. 2011.

[10] ITU-T SG17 Q.9 Summaries for work item under development in Question 9, TD1350, Dec. 2010.

[11] ITU-T SG17 Q.9 Meeting Report on Q.9/17, TD1425, Dec. 2010.

[12] HomelandSequrity Whitepaoer, "Computer Network Security & Privacy Protection," 2011

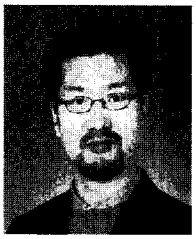
[13] http://www.cs.ucdavis.edu/~hchen/paper/passat09.pdf, "Noise Injection for Search Privacy Protection," 2011.

[14] 전명근, "바이오 보안 토큰을 위한 표준안 개발," 정보통신표준기술력향상사업 최종보고서, 지식경제부, 방송통신위원회, 2011.

〈著者紹介〉

신 용 녀 (Yong-Nyuo Shin)

1999년 2월 : 숭실대학교 컴퓨터학과 졸업
2001년 9월 : 고려대학교 컴퓨터학과 석사
2008년 2월 : 고려대학교 컴퓨터학과 박사
2002년 1월~2009년 6월 : 한국정보보호진흥원 주임연구원
2009년 7월~2010년 7월 : 한국은행 전자금융팀 과장
2010년 9월~현재 : 한양사이버대학교 컴퓨터공학과 교수
<관심분야> 바이오인식, 프라이버시, 정형기법



김 학 일 (Hakll Kim)
종신회원
1983년 2월 : 서울대학교 제어계측공학과 졸업
1985년 8월 : Perdue University 전기컴퓨터공학과 석사
1990년 8월 : Perdue University 전기컴퓨터공학과 박사
1990년 9월~현재 : 인하 박사대학교 정보통신공학과 교수
2009년~현재 : ITU-T SG17 Q.9 표준회의 라포처(의장)
<관심분야> 바이오인식, 영상처리, 컴퓨터비젼

전 명 근 (Myung-Geun Chun)
종신회원
1987년 2월 : 부산대학교 전자공학과 졸업
1989년 2월 : KAIST 전기 및 전자공학과 석사
1993년 2월 : KAIST 전기 및 전자공학과 박사
1993년~1996년 : 삼성전자 자동화연구소 선임연구원
2000년~2001년 : University of Alberta 방문교수
1996년~현재 : 충북대학교 전자공학부 교수
2008년~현재 : TTA PG505 표준위원회 의장
2007년~현재 : ISO/IEC SC27 정보보호표준화전문위원
<관심분야> 바이오인식, 개인정보보호, 지능시스템