정 보 보 호 학 회 지
제27권 제5호, 2017. 10

국제 개인정보보호 표준화 동향 분석

(2017년 4월 해밀턴 SC27 회의 결과를 중심으로)

염 흥 열*

요 약

개인정보관리체계 [1,2] 를 구축하기 위해서는 관리체계를 위한 요구사항과 프라이버시 통제가 필요하다. 국내에서 시행되고 있는 개인정보관리체계도 요구사항과 개인정보 전주기동안의 프라이버시 보호조치에 근거해 시행하고 있다. 빅데이터 환경에서는 개인정보를 처리하기 위한 비식별화 기법(de-identification technique)이 요구된다. 그리고 온라인 사용자 친화적 고지 및 통보 방법이 필요하다. 국제표준화위원회/전기위원회 합동위원회 1의 정보보호기술연구반 신원 관리 및 프라이버시 작업반 (ISO/IEC JTC 1/SC 27/WG 5)에서는 개인정보보호를 위한 여러 가지 국제표준을 개발하고 있다 [20],[21],[22],[30]. 본 논문에서는 작업반 5에서 2017년 4월 뉴질랜드 해밀턴 SC27 회의에서 논의된 개인정보보호 관련 주요 표준화 이슈와 대응 방안을 제시한다.

Ⅰ. 서 론

ISO/IEC JTC 1/SC 27/WG 5에서는 개인정보관리체계와 관련된 개인정보보호 지침 (ISO/IEC 29151), 개인정보영향평가-가이드라인 (ISO/IEC 29134), 개인정보관리를 위한 추가 요구사항 (ISO/IEC 27552) 그리고 비식별화 기법 (ISO/IEC 20889), 사용자 친화 온라인 고지 및 통보 (ISO/IEC 29184) 등을 개발하고 있다.

국내 개인정보보호와 관련된 법은 개인정보보호법과 정보통신망 이용촉진 및 정보보호 등에 관한 법이다 [3,4]. 기업의 기술적, 관리적, 조직적 보호조치를 제공하는 정보보호관리체계를 운영하기 위해서는 요구사항 [6]과 보호 통제[7]가 필요하다. 정보보호관리체계와 연관된 주요 용어는 ISO/IEC 27000[5]에서 정의된다.

개인정보보호 요구사항은 개인정보보호 법 및 제도, 기업간의 계약, 그리고 개인정보영향평가에서 나온다. 이 요구사항을 만족하기 위한 통제는 보안 측면 통제와 프라이버시 측면 통제로 구성될 수 있다. 보안 측면 통제는 ISO/IEC 27002 표준[7]의 통제를 적용해야 하나, 프라이버시 측면 추가 보안 가이던스와 기타 정보가 필요하다. 또한 개인정보보호법 제도에서 요구되는 생명주기 관련 프라이버시 측면 통제도 필요하다. 섹터 기반 정보보호관리체계를 위한 표준을 개발하기 위한 국제표준도 개발되었다[9]. 대표적인 통신부문 정보보호관리 준칙은 ISO/IEC 27011[10]로 개발되었다. 또한 클라우드를 위한 개인정보보호 통제는 ISO/IEC 27018[12]로 개발되었다.

본 논문의 2장에서는 2016년 말부터 2017년 현재까지 ISO/IEC JTC 1/SC 27/WG 5에서 추진되고 있는 개인정보보호 관련 주요 국제 표준의 현황을 살펴보고 주요 내용을 제시하며, 3장에서는 결론으로 이 국제 표준을 이용한 국내 개인정보보호 인증기준을 고도화하기 위한 일정표를 제시하고 이를 위한 고려사항을 제시한다.

Ⅱ. SC27 개인정보보호 표준화 동향

2.1. 개인정보보호관리체계 관련 국제표준

개인정보보호와 관련된 국제표준은 신원 관리 및 프라이버시 작업반(WG5)에서 개발되고 있는 주요 국제표준을 요약하면 [표 1]과 같다[18].

본 논문은 과학기술정보통신부 및 정보통신기술진흥센터의 정보통신·방송 연구개발사업의 일환으로 수행하였음. [2015-0-00264 , IoT 환경에서 프라이버시 보호 국제 표준화]

* 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr)

〔표 1〕 개인정보관리체계 관련 국제표준〔2017.9 현재〕

작업반	표준 제목 및 번호	주요 내용	문서 상태
WG 5	■ ISO/IEC 29100, 프라이버시 프레임워크 [13]	■ 프라이버시 관련 용어, 주요 주체의 역할, 보호 요구사항, 프라이버시 보호 원칙 등을 포함한 프라이버시 프레임워크를 제시한다.	IS (International Standard)
	■ ISO/IEC 29134, 개인정보영향평가 가이드라인	■ 개인정보영향평가를 위한 과정과 개인정보영향평가 보고서의 구조와 내용에 대한 가이드라인을 제공한다.	IS (International Standard)
	■ ISO/IEC 29151, 개인정보보호 지침	■ 개인정보보호와 관련된 위험 평가 결과에 의해 식별된 요구사항을 만족하기 위한 통제와 구현 가이드라인 등을 제시한다.	IS (International Standard)
	■ ISO/IEC 27552, 프라이버시 관리를 위한 ISO/IEC 27001 국제 표준의 개선	■ 개인정보관리를 위한 ISO/IEC 27001 개선을 위한 요구사항과 통제를 제시한다.	2nd WD
	■ ISO/IEC 20889, 비식별화 기법	■ 다양한 비식별화 기술을 제시한다.	2nd CD
	■ ISO/IEC 29184, 사용자 친화 고지 및 통보	■ 사용자 친화적 고지 및 통보 방법을 제시한다.	3rd WD
	■ ISO/IEC 29003, 온라인 신원증명 (identity proofing)	■ 온라인에서 사용자에 대한 신원을 증명하는 등급을 제시한다.	PDTS

2.2. ISO/IEC 29134[15]

이 국제 표준은 이 논문 작성 시점에 IS 상태에 있다. 보안 측면의 위험 평가는 ISO/IEC 27005[8]를 이용한다. ISO/IEC 29134 국제표준에서 개인정보영향평가는 프라이버시 리스크 식별, 분석, 평가, 치료, 점검, 개선하기 위한 활동과 관련된 활동의 정책, 과정, 그리고 지침을 체계적으로 적용하기 위한 수단으로 정의된다[15].

2011년 10월 케냐 라이로비 WG5 회의에서 신규워크아이템 제안이 채택되었고, 2012년 4월 스톡홀름 SC27 회의에서 신규워크아이템으로 채택된 바 있다. 이 국제 표준은 독일(레인니스 매티어스)과 한국(염흥열) 에디터에 의해 개발되어 왔으며, 개인정보영향평가를 위해 요구되는 프로세스를 정의하고, 영향평가 보고서의 구조와 내용을 국제 표준화하는 게 목적이다. 한국은 2016년 4월 SC27 회의에 리스크 관리에 필요한 민감도와 가능성에 대한 용어 정의 등 14개의 코멘트를 제출해 모두 반영했다. 이 회의에서는 250여개의 코멘트를 모두 해결해 DIS (draft international standard) 로 추진키로 만장일치로 합의했다. 2016년 10월 아부다비 회의에서는 만장일치로 FDIS(final international standard) 로 진전하기로 합의했다.

2017년 4월 해밀턴 회의에서는 2016년 10월 아부다비 회의에서 합의한 FDIS 투표 결과가 발표되었다[28]. FDIS 투표는 2017년 2월 20일에서 4월 17일까지 수행되었다. 그 결과 총 24 개국 P-멤버 회원국이 투표해 캐나다를 제외한 모든 23개국(NB (national body))이 찬성해 찬성율 96%를 달성했다. 찬성율 66.67 % 이상 기준을 통과했다. 또한 투표에 참여한 P-멤버와 O-멈버 28개 NB중 1개국이 반대해 반대율 4% 로서, 25% 이하의 기준을 만족했다. 따라서 이 국제표준은 2017년 6월 IS로 발표되었다.

현재 국내에서는 개인정보보호법에 의해 공공부문에 개인정보영향평가가 의무화되어 있어서, 이 국제 표준에서 개발될 프로세스와 보고서 구조는 국내 개인정보영향평가의 방법론을 개선하기 위해 이용 가능하다.

2.3. ISO/IEC 29151[16]

이 국제표준은 이 논문 작성 시점에 IS상태에 있다. 이 국제표준은 개인정보보호 관리체계를 운영하기 위해 요구되는 프라이버시 통제를 개발함에 그 목적이 있다. 이 국제 표준은 자산관리, 접근통제, 암호, 운영보안, 통신 보안, 그리고 공급자 보안 등의 정보보안 측면의 개인정보보호 특화 가이던스를 기술했다. 또한, 개인정보보호 정책, 동의 및 선택, 목적 합법성, 데이터 최소화, 이용/보유/공유 최소화, 정확성 및 품질, 투명성, 정보주

체 참여, 책임성, 정보보안, 프라이버시 법 준수 측면에서 개인정보보호 특화 통제를 기술하고 있다.

한국(염흥열)은 2011년 10월 케냐 나이로비 WG5 회의에서 국내 개인정보관리체계를 위해 필요한 지침과 요구사항 기준을 국제표준화로 추진하기 위한 연구회기(라포처: 염흥열 등)를 제안했다. 1년 동안 연구회기를 진행해 2012년 10월 로마 회의에서 개인정보보호 지침은 WG5에서 신규워크아이템 (ISO/IEC 29151) 으로 합의했고, WG1에서 개인정보관리를 위한 요구사항을 위해 생성되어야 할 국제 표준을 개발하기 위한 신규워크아이템(ISO/IEC 27009 [9]) 으로 합의했다. 이 제안은 영국, 독일, 일본 등이 적극적으로 지지했다.

이에 따라 2013년 4월 로마 SC27 회의에서 지침 관련 신규워크아이템 제안이 채택되었으며, 첫 번째 WD (working draft) 를 합의했고, 요구사항 관련 신규워크아이템(ISO/IEC 27009)도 채택되었다.

2012년 10월 이후 WG5에서 한국 주도로 ISO/IEC 29151 표준(에디터: 염흥열) 개발되어 왔고, WG1에서는 ISO/IEC 27009 표준(에디터: 박태완)을 개발하기 시작했다.

2014년 4월 홍콩 회의에서 ITU-T SG17에서 개발되어 온 ITU-T X.gpim과 SC27에서 개발되어 오던 ISO/IEC 29151을 공통 표준(common text)으로 개발키로 합의한 바 있다.

한국(염흥열)은 이 SC27 회의에서 처리되는 국가식별번호(주민등록번호)를 암호화해야 하고 별도 동의를 받아 수집해야 한다는 등의 19개의 코멘트를 제출해 모두 반영했다. 이 회의에서는 X.gpim | ISO/IEC 29151에 대해 340 여개의 NB 코멘트를 해결해 DIS로 가기로 만장일치로 합의했다.

이 국제표준은 2016년 10월 아부다비 회의에서 FDIS로 진행하기로 만장일치로 합의했다. 이 국제표준은 2016년 12월 16일 FDIS 투표를 2017년 2월 10일까지 진행되었다. 2017년 4월 뉴질랜드 해밀턴 회의에서는 FDIS 투표결과가 발표되었다[29]. 그 결과 총 21개국 P-멤버가 투표해 캐나다를 제외한 모든 20개국이 찬성해 찬성율 95%를 달성했다. 찬성율 66.67 % 이상 기준을 통과했다. 또한 투표에 참여한 P-멤버와 O-멈버 25개 NB중 1개국이 반대해 반대율 4% 로서, 25% 이하의 기준을 만족했다. 따라서 이 국제표준은 2017년 8월 IS로 발표되었다.

한편 ITU-T SG17 에서는 2016년 4월 회의에서 합의된 DIS 문서를 근거로 2016년 8월 SG17 회의에서 전통승인과정(TAP)를 이용한 준비과정으로 추진 사전채택(determination) 했다.

이후 2017년 3월까지 TAP 국가별 의견 수렴 과정 동안 러시아에서 암호알고리즘에 안정성에 대한 코멘트를 제출했고 이를 반영해 2017년 3월 SG17 회의에서 최종 채택했다.

기업에 의해 개인정보관리체계가 운영되기 위해서는 요구사항, 보안측면 통제와 프라이버시 통제가 필요하다. 본 표준은 프라이버시 통제를 국제 표준화하기 위한 활동으로, 한국에서 시행되고 있는 개인정보보호 관리체계의 생명주기와 보안 통제를 국제표준화하기 위한 의도로 시작되었다. 이 국제표준은 ISO/IEC 29100[13]에서 제시된 프라이버시 보호 원칙에 입각한 프라이버시 통제를 개발하는 데 주 목적이 있다.

ISO/IEC 29151은 개인정보처리자(PII controller)에 적용 가능한 보호조치를 위한 통제 목표, 통제 항목, 구현 가이던스, 그리고 기타 정보를 제공한다[16]. 이 표준은 ISO/IEC 27002에서 제공하는 정보보호 통제에 더하여 개인정보보호를 위해 추가적으로 요구되는 가이던스와 프라이버시 보호 원칙을 만족하는 추가적인 프라이버시 통제를 제공하고 있다. ISO/IEC 27002에서 제공하는 통제를 변경 없이 적용하되 추가적인 가이던스가 필요한 경우는 해당 절에 추가하는 방법으로 기술되었다. 또한 개인정보보호 특화 통제는 부록 A에 기술되어 있으며, 개인정보보호 원칙 별로 추가 통제 목표, 통제 항목, 가이던스, 그리고 기타 정보가 제공된다. 이 국제표준의 개발 배경은 다음과 같다.

이 국제 표준 채택으로 국제 개인정보관리체계 기준의 국제표준화에 다가가게 되어 국내 개인정보보호 인증 산업 발전의 기틀을 마련했고, 향후 글로벌 개인정보관리체계 인증 시행을 위한 표준 근거를 마련했다.

2.4. ISO/IEC 27552 [23]

프랑스는 지난 2015년 10월 자이푸르 SC27 회의에서 한국, 프랑스, 인도, 독일 등이 합의한 대로, 이번 2016년 4월 SC27 회의에서 정보보호관리체계(ISO/IEC 27001)를 프라이버시 관리를 위한 개선하기 위한 추가 요구사항을 위한 신규워크아이템 (NWIP,

new work item proposal) 을 제안했다.

한국(염흥열)은 전문가 기고를 통해 프랑스의 신규워크아이템 제안에 대해 적극 찬성했고 에디터 참여를 제안한 바 있다. 이 제안에 대해 한국을 비롯한 인도, 영국, 독일 등 전문가가 지지해 신규워크아이템 제안으로 합의되었다.

이 신규워크아이템 제안은 투표 과정을 거쳐 2016년 4월 탬퍼 WG5 회의에서 신규워크아이템으로 채택되었다. 이 국제표준은 2016년 10월 아부다비 회의에서 영국의 Alan Shipman을 에디터로, 필자를 비롯해 영국과 인도 전문가를 코에디터로 선임했고, 1번째 WD로 진행하기로 합의되었다. 2017년 4월 해밀턴 회의에서는 2번째 WD로 진행하기로 합의했다. 여기서 가장 중요한 사항은 PIMS를 “privacy information management system”으로 합의했다.

2.5. ISO/IEC 20889 [24]

이 국제표준은 영국 주도로 개발되고 있는 빅데이터에 대한 비식별화 기법에 대한 관련 기술을 제시하는데 목적이 있다. 이 문서의 신규워크아이템 제안 시 한국은 개인정보 우려를 불식하고 빅데이터 개인정보 처리가 가능하다는 측면에서 적극 지지한 바 있다.

2016년 아부다비 회의에서는 첫 번째 CD로 진행하기로 합의했다.

2017년 4월 해밀턴 회의에서는 두 번째 CD로 진행하기로 합의했다. 이번 회의에서 캐나다는 이 표준에 권고 및 필수 요구사항이 없다는 이유로 IS에서 TS (technical specification)로 변경할 것을 제안했으나, 많은 국가들이 IS (international standard) 유지를 선호해 IS 트랙으로 결정되었다.

국내에서는 행정안전부와 방송통신위원회가 2016년 6월 30일 비식별화 조치 가이드라인을 발표했다[25]. 비식별화된 데이터는 개인정보로 보지 않으나, 언제든지 재식별화될 가능성이 있어서 비식별화된 데이터에 대한 기술적 관리적 보호조치를 취하도록 요구하고 있다. 또한 비식별화 전문기관에 의해 비식별화 데이터를 결합하는 서비스를 제공하고 있다. 빅데이터 환경에서 개인정보의 보호와 활용을 위한 절충점을 제시하고 있다고 볼 수 있다. 따라서 비식별화 기법은 개인정보 침해 소지 없이 빅데이터와 개인정보를 처리하기 위한 핵심 기술이다. 따라서 국내 산업적 파급효과가 매우 큰 표준이므로, 이 국제 표준화 과정에 적극적으로 참여하고 의견을 개진할 필요가 있다.

2.6. ISO/IEC 29184 [26]

이 국제표준은 정보주체로부터 개인정보를 수집하고 처리하기 위한 동의를 요청하는 온라인 프라이버시 고지와 문서의 내용과 구조를 규정한다.

2017년 4월 해밀턴 회의에서는 세 번째 WD로 진행하기로 합의했다.

2.7. ISO/IEC 29003 [27]

이 논문 작성 시 이 국제 표준은 PDTS (preliminary draft technical specification) 상태에 있다. 이 국제표준은 정보주체로부터 개인정보를 수집하고 처리하기 위한 동의를 요청하는 온라인 프라이버시 고지와 문서의 내용과 구조를 규정한다. 이 표준은 IS 트랙이었으나, 2016년 아부다비 회의에서 많은 NB 들이 DIS 진행을 반대해서 2017년 해밀턴 회의에서는 표준의 트랙을 IS 트랙에서 TS (technical specification) 으로 변경하기로 합의했다.

ISO/IEC 29003 (identity Proofing) 는 국내 금융권에서 시행하고 있는 비대면 인증과 밀접한 관련이 있다.

Ⅲ. 결 론

본 논문에서 2017년에 수행된 개인정보보호 관련 국제표준의 최근 동향을 제시한다. 이번 2017년 4월 해밀턴 SC27 회의에서는 개인정보보호 준칙(ISO/IEC 29151)과 개인정보영향평가(ISO/IEC 29134)가 국제표준으로 최종 공표 되었다. 본 논문에서 2017년에 추진된 SC 27/WG 5 개인정보보호 관련 주요 국제표준의 주요 이슈를 제시했다. 본 논문의 결과는 국내 개인정보보호 수준 제고를 위해 활용 가능하다.

참 고 문 헌

[1] BS 10012:2009, Data protection – Specification for a personal information management system, BSI, 2009

[2] KCS.KO-12.0001, 개인정보보호관리체계(PIMS), 2011
[3] 법제처, 개인정보보호법
[4] 법제처, 정보통신망이용촉진 및 정보보호 등에 관한 법
[5] ISO/IEC 27000:2014, Information security management systems – Overview and vocabulary
[6] ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements
[7] ISO/IEC 27002:2013, Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management system
[8] ISO/IEC 27005:2011, Information security risk management
[9] ISO/IEC 27009: 2016, Information technology — Security techniques — Sector specific application of ISO/IEC 27001 – Requirements
[10] ISO/IEC 27011, Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
[11] ISO/IEC 27017:2016, Code of practice for information security controls based on ISO/IEC 27002 for cloud services
[12] ISO/IEC 27018:2014, Code of practice for protection of personally identifiable information (PII) in public clouds acting as PIII processors
[13] ISO/IEC 29100:2011, Information technology – Security techniques – Privacy framework
[14] ISO/IEC 29190, Information technology – Security techniques – Information technology -- Security techniques -- Privacy capability assessment model
[15] ISO/IEC 29134, Privacy Impact Assessment - Methodology, 2017.5
[16] ISO/IEC 29151, Code of practice for the protection of personally identifiable information, 2017.8
[17] WG 5/SD 5, Explanation on the use of ISO/IEC 27001 (ISMS) for privacy management, 2015.8
[18] ISO/IEC JTC 1/SC 27 IT Security techniques, http://www.iso.org/iso/iso_technical_committee?commid=45306
[19] WG 5/SD 1, WG 5 Roadmap, 2016.4
[20] 염흥열, "개인정보보호 관리체계 국제 표준화 필요성," 정보보호학회지, 제23권 제4호, pp.65-72, 2013.8
[21] 염흥열, "개인정보보호 기술 및 국제표준 동향," OSIA Standards & Technology Review Journal * June 2014, Vol.27, No.2
[22] 염흥열, 개인정보보호 국제표준화 분석, 한국정보보호학회 학회지, 제25권 제4호, pp.5-9, 2015.8
[23] ISO/IEC 2nd WD 27552, Enhancement to ISO/IEC 27001 for privacy management – Requirements, ISO/IEC SC 27/WG 5, 2017.9.
[24] ISO/IEC 2nd CD 20889, Information technology – Security techniques – Privacy enhancing data de-identification techniques
[25] 행정안전부, 방송통신위원회 등, "비식별화조치 가이드라인," 2016.6.30.
[26] ISO/IEC 3rd WD 29184, Guidelines for online privacy notices and consent, 2017.9
[27] ISO/IEC PDTS 29003, Identity proofing, 2017.9
[28] ISO/IEC JTC 1/SC 27 N17059, Summary of voting on ISO/IEC FDIS 29134:2016)(E) (SC 27 N17008) -- Information technology -- Security techniques – Guidelines for privacy impact assessment
[29] ISO/IEC JTC 1/SC 27 N17060, Summary of voting FDIS letter ballot on ITU-T X.gpim | ISO/IEC 29151:2016-12-16(E) – Information technology – Security techniques – Code of practice for privacy personally identifiable information protection
[30] 염흥열, 국제 개인정보보호 표준화 동향 분석 (2016년 4월 탭퍼 SC27 회의 결과를 중심으로), 정보보호학회지, v.26, no.4, 6-10, 2016.8

〈저 자 소 개〉

염 흥 열 (Heung-Youl Youm)
종신회원

한양대학교 전자공학과 학사 졸업
한양대학교 대학원 전자공학과 석사 졸업
한양대학교 대학원 전자공학과 박사 졸업
1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 정교수
2009년~2016년 : ITU-T SG17 부의장, WP3 의장
2017년~현재 : ITU-T SG17 의장
2011년 1월~12월 : 한국정보보호학회 회장(역)
2012년 1월~현재 : 한국정보보호학회 명예회장
2016년 5월~현재 : 개인정보보호표준포럼 의장
관심분야 : 인터넷 보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜