정 보 보 호 학 회 지
제26권 제4호, 2016. 8

국제 개인정보보호 표준화 동향 분석
(2016년 4월 탬퍼 SC27 회의 결과를 중심으로)

염 흥 열*

요 약

기업의 개인정보보호 수준을 강화하기 위한 개인정보보호관리체계 인증을 구축하기 위해서는 개인정보관리체계를 위한 추가 요구사항, 보안 측면의 통제, 프라이버시 측면의 통제가 요구된다[1,2]. 국제표준화위원회/전기위원회 합동위원회 1의 정보보호기술연구반 신원 관리 및 프라이버시 작업반 (ISO/IEC JTC 1/SC 27/WG 5)에서는 개인정보보호를 위한 여러 국제 표준을 개발하고 있다[18, 32, 22]. 본 논문에서는 작업반 1과 작업반 5에서 2016년 4월 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 (NWIP) 그리고 비식별화 기법 (ISO/IEC 20889)을 개발하고 있다.

국내 개인정보보호법과 정보통신망 이용촉진 및 정보보호 등에 관한 법이 있다[3,4]. 정보보호 관리체계를 운영하기 위해서는 요구사항[6]과 보호 통제[7]가 필요하다. 정보보호관리체계를 위한 용어는 ISO/IEC 27000[5]에서 정의된다.

개인정보보호 요구사항은 개인정보보호 법 및 제도에서 나오며, 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.

SC 27/WG 1에서는 정보보호관리체계 관련 국제표준을 개발하고 유지하고 있고, SC 27/WG 5에서는 개인정보보호화 신원관리 관련 국제표준을 개발하고 있다[5,6].

본 논문의 2장에서는 ISO/IEC JTC 1/SC 27에서 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. SC 27 개인정보보호 표준화 동향

2.1. 개인정보보호관리체계 관련 국제표준

정보보호관리체계 작업반(WG1)과 신원 관리 및 프라이버시 작업반(WG5)에서 개발되고 있는 주요 국제 표준을 요약하면 [표 1]과 같다[18].

2.2. ISO/IEC 27009[09]

ISO/IEC 27001 국제표준은 정보보호관리체계를 구축하고 운영하기 위한 프로세스와 관련 요구사항을 지시하고 있다. 이 국제 표준은 2011년 케냐 나이로리 WG5 회의에서 한국이 제안한 연구회기의 결과로 개발되기 시작했다. 최근 통신 조직[10], 클라우드 서비스 제공자[11,12] 등과 같은 섹터별 정보보호관리체계의

이 논문은 2016년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (IoT 환경에서 프라이버시 보호 국제 표준화)
* 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr)

〔표 1〕 개인정보관리체계 관련 국제 표준〔2016.8 현재〕

작업반	표준 제목 및 번호	주요 내용	문서 상태
WG 1	■ ISO/IEC 27009, 섹터 기반 관리체계 구축시 ISO/IEC 27001 국제 표준을 이용하기 위한 요구사항[9]	■ 섹터 기반 관리체계에 ISO/IEC 27001 국제표준을 생성하기 위한 요구사항을 정의한다. 여기서는 ISO/IEC 27001 국제표준에 존재하는 요구사항에 더해 추가적으로 필요한 요구사항을 정의하고 기존의 요구사항을 개선하기 위한 방법을 제시한다.	IS (international standard)
WG 5	■ ISO/IEC 29100, 프라이버시 프레임워크	■ 용어, 관련 주체들의 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.	DIS (draft international standard)
	■ ISO/IEC 29151, 개인정보보호 지침	■ 개인정보보호와 관련된 위험 평가 결과에 의해 식별된 요구사항을 만족하기 위한 통제와 구현 가이드라인 등을 제시한다.	DIS (draft international standard)
	■ SD 5/WG 5, 프라이버시 관리를 위한 ISO/IEC 27001 국제 표준의 이용에 대한 설명	■ 개인정보관리체계 구축을 위해 ISO/IEC 27001과 결합해 기존 국제 표준을 이용하거나 신규 국제 표준을 개발하기 위한 가이드라인을 제시한다.	SD (Standing Document)
	■ NWIP, 프라이버시 관리를 위한 ISO/IEC 27001 국제 표준의 개선	■ 개인정보관리를 위한 ISO/IEC 27001의 개선을 위한 요구사항과 통제를 제시한다.	NWIP
	■ ISO/IEC 20889, 비식별화 기법	■ 개인정보관리를 위한 ISO/IEC 27001의 개선을 위한 요구사항과 통제를 제시한다.	2nd WD

필요성이 대두되고 있다. 이 국제표준은 이러한 섹터 기반 관리체계 구축을 위해 필요한 추가 요구사항과 통제에 대한 국제표준을 생성하는데 이용될 수 있다. 이번 2016년 4월 탬퍼 SC27 회의에서는 FDIS 투표 과정에서 제출된 에디토리얼 콤맨트를 해결해 국제표준(IS)로 발표키로 합의했다.

2.3. ISO/IEC 29134[15]

이 국제 표준은 이 논문 작성 시점에 DIS 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[12].

2011년 10월 케냐 나이로비 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 이번 2016년 4월 SC27 회의에 리스크 관리에 필요한 민감도와 가능성에 대한 용어 정의 등의 14개의 콤맨트를 제출해 모두 반영했다. 이번 회의에서는 250여 개의 콤맨트를 모두 해결해 DIS 로 추진키로 만장일치로 합의했다.

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

2.4. ISO/IEC 29151[16]

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 프라이버

시 통제를 개발하는 데 주 목적이 있다.

이 국제표준은 이 논문 작성 시점에 DIS 상태에 있다. ISO/IEC 29151은 개인정보제어자(PII controller)에 적용 가능한 보호조치를 위한 통제 목표, 통제, 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, 가이던스, 그리고 기타 정보가 제공된다.

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) 르로 합의했다. 이 제안은 영국, 독일, 일본 등이 적극적으로 지지했다.

이에 따라 2013년 4월 로마 SC27 회의에서 지침관련 신규워크아이템제안이 채택되었으며, 첫 번째 WD를 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 이번 회의에서 처리되는 국가식별번호(주민등록번호)를 암호화해야 하고 별도 동의를 받아 수집해야 한다는 등의 19개의 콤맨트를 제출해 모두 반영했다. 이번 회의에서는 X.gpim | ISO/IEC 29151에 대해 340 여개의 NB 콤맨트를 해결해 DIS 로 가기로 만장일치로 합의했다.

향후에는 5개월간의 DIS 투표과정을 거쳐 2016년 10월 아부다비 회의에서 FDIS로 갈지 IS 로 바로 갈지를 결정할 예정이다.

이번 합의된 DIS 문서를 ITU-T SG17에 보내 다음 2016년 8월 SG17 회의에서 전통승인과정(TAP)를 이용한 준비과정으로 추진(determination) 할 예정이다.

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

2.5. SD 5/WG 5[17]

이 문서(SD 5/WG 5) 는 개인정보보호관리체계를 구축하기 위해 ISO/IEC 27001 의 요구사항 외에 추가로 요구되는 요구사항과 통제를 개발하기 위해 제공한다. 추가 요구사항은 다음과 같다[17].

이번 SC27 회의에서한국(염흥열)은 개인정보관리체계에 대한 7개의 콤맨트를 제출해 대부분 반영했다. 대표적인 요구사항은 “ISO/IEC 27001 요구사항 이외에 ISO/IEC 29100 개인정보보호 원칙[14]을 고려해야 한다.” 등이다. 다만, 2016년 4월 SC27 회의에서 2.6 절에서 제시된 신규워크아이템이 채택됨에 따라 2016년 10월 SC27 회의에서 폐기될 가능성이 크다.

2.6. NWIP, 프라이버시 관리를 위한 ISO/IEC 27001의 개선 – 요구사항 [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)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 전문가의 지지해 신규워크아이템 제안으로 합의되었다.

이 신규워크아이템 제안은 투표 과정을 거쳐 2017년 4월 UAE 아부다비 WG5 회의에서 신규워크아이템으로 채택될 것으로 기대된다.

쟁점은 프라이버시 관리(privacy management)로 할 것인지 개인정보보호(PII protection)로 할 것인지에 대한 것이었으며, 논의 결과 프라이버시 관리를 합의했다. 또한 정규 참조 표준으로 요구사항과 관련된 표준인 (ISO/IEC 27001)과 프라이버시 프레임워크 표준 (ISO/IEC 29100), 그리고 보안 통제(ISO/IEC 27002) 표준을 넣는 것으로 합의했다. 또한, 프라이버시 통제 표준(ISO/IEC 29151)의 정규 표준 포함 가능성을 남겨두었다. 정보보호관리체계 기반에서 프라이버시 관리를 위한 측면에서 명명된 관리체계의 명칭을 PIMS (privacy management system)로 합의했다.

이로 인해 개인정보관리체계의 국제 인증을 시행하기 위해 필요한 프라이버시 측면의 추가 요구사항에 대한 표준(NWIP), 보안 측면의 통제(27002), 프라이버시 측면의 통제 및 보안 통제 추가 가이던스(29151), 프라이버시 리스크 평가(29034) 등으로 구성된 프라이버시 측면의 정보보호관리체계를 위한 국제표준 집합이 2019년 초까지는 마련될 예정이다.

이번 2016년 4월 SC27 회의에서 합의된 신규워크아이템은 국내 개인정보보호관리체계 운영과 인증에 많은 영향을 줄 가능성이 있으므로, 다음 2016년 10월 아부다비 WG5 회의에서 한국은 이 국제표준의 에디터를 추천할 필요 있다.

2.7. 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. 한국(염흥열)은 이번 회의에 익명화 등에 대한 용어 정의 등을 제안하는 등의 10개의 콤맨트를 제안해 모두 반영한 바 있다.

이번 회의에서는 많은 NB의 181개 콤맨트를 모두 해결되어 두 번째 WD로 추진키로 합의했다.

국내에서는 미래창조과학부가 비식별화 기술적 가이드라인의 개정 작업을 추진하고 있고, 방통위가 2014년 빅데이터 비식별화 가이드라인이 발표한 바 있으며 비식별화를 법제화하기 위한 TF를 구성해 운영하고 있다. 또한 금융위에서도 금융정보의 비식별화를 위한 가이드라인을 개발하고 있다. 따라서 비식별화 기법은 개인정보 침해 소지없이 빅데이터와 개인정보를 처리하기 위한 핵심 기술이다. 국내 산업적 파급효과가 매우 큰 표준이므로, 이 국제 표준화 과정에 적극적으로 참여하고 의견을 개진할 필요 있다.

Ⅲ. 결 론

본 논문에서 분석된 개인정보보호 관련 국제표준의 최근 동향을 제시한다. 특히 이번 2016년 4월 탬퍼 SC27 회의에서는 개인정보관리체계 운영을 위한 추가 요구사항에 대한 신규워크아이템 제안이 합의되었다. 방통위가 2011년부터 시행하고 있는 개인정보보호관리체계의 글로벌 상호 인증을 가능하게 되는 글로벌 국제표준 집합이 완성되었음을 의미한다.

본 논문에서 SC 27/WG 5에서 논의된 개인정보보호 관련 주요 국제표준의 주요 이슈를 제시한다. 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 FDIS 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 DIS 29134, Privacy Impact Assessment - Methodology, 2014.5
[16] ISO/IEC DIS 29151, Code of practice for the protection of personally identifiable information, 2014.4
[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] WG5 N390, Enhancement to ISO/IEC 27001 for privacy management – Requirements, ISO/IEC SC 27/WG 5, 2016.4.
[24] ISO/IEC 20889, Information technology – Security techniques – Privacy enhancing data de-identification techniques

〈저자소개〉

염 흥 열 (HeungYoul 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
2011년 1월~12월 : 한국정보보호학회 회장(역), 명예회장(현)
2009년~현재 : ITU-T SG17 부의장
2009년~현재 : ITU-T SG17 WP2/WP3 의장
2012년 6월~2015년 5월 : 정보보호포럼 의장
2016년 5월 ~현재 : 개인정보보호표준포럼 의장
<관심분야> 정보보호관리체계, 개인정보보호, IoT 보안, 개인정보영향평가, 암호 프로토콜