정 보 보 호 학 회 지
제 32 권 제4호, 2022. 8

국제 개인정보보호 표준화 동향 분석
(2022년 4월 SC27 WG5 전자 회의 결과를 중심으로)

염 흥 열*

요 약

2020년 8월 5일 통합 개인정보보호법 [3]이 본격적으로 시행되면서 데이터의 보호와 활용을 동시에 만족할 수 있는 가명처리 개념이 도입되었다. 여러 개인정보처리자로 수집된 가명정보를 결합하기 위한 결합 관리기관이 지정되고 있다. 개인정보보호 국제표준은 관행이나 기술을 국제표준으로 개발하여 상호 연동이 가능한 서비스를 제공할 수 있을 뿐만 아니라 제품이나 서비스의 경쟁력을 강화하는데 활용할 수 있다. 개인정보보호 국제표준화를 주도적으로 추진하고 있는 대표적인 국제표준화 그룹은 국제표준화위원회/전기위원회 합동위원회 1/서브위원회 27/작업그룹 5 (ISO/IEC JTC 1/SC 27/WG 5)를 들 수 있다. 이 그룹의 의장님 독일 쾨테대학 Kai Rannenberg 교수가 맡고 있다. 여기서는 2020년 4월 전자회의 이후에는 개인정보보호 분야 3건의 국제표준을 채택하였다. 차기 회의는 2022년 9월 룩셈부르그에서 펜데믹 이후 최초로 대면과 비대면으로 개최될 예정이다. 본 고에서는 이 그룹에서 2020년 4월 이후 추진되고 있는 개인정보보호 관련 국제표준화 동향을 제시하고자 한다. 또한 지난 4월 SC27 WG5 전자 회의에서 논의된 개인정보보호 관련 주요 표준화 이슈와 대응방안을 제시한다.

Ⅰ. 서 론

우리나라 개인정보보호법 [3]에서는 개인정보를 “살아 있는 개인에 관한 정보”로 정의되고 있다. 2020년 8월에 통합 개인정보보호법이 시행되면서 가명 정보의 활용과 결합이 활발히 진행되고 있다. 가명처리는 “개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리”하는 것으로, 가명처리된 가명정보는 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다[3]. 2018년 5월 25일부터 발효된 유럽연합 개인정보보호법(GDPR, general data protection regulation) [29] 에서도 가명화(psedonymization)를 “추가 정보를 사용하지 않고는 데이터가 더 이상 특정 데이터 주체에 귀속될 수 없도록 하는 방식으로 개인 데이터를 처리하는 것”으로 정의하고 있다.

ISO/IEC JTC 1/SC 27/WG 5[18]는 개인정보보호와 관련된 국제표준을 개발하고 있는 표준화 그룹이다.

이 그룹에서는 프라이버시 프레임워크 (ISO/IEC 29100) [13], 프라이버시 영향평가 (ISO/IEC 29134) [15], 개인정보보호 준칙(ISO/IEC 29151) [16], 개인정보 수탁자로서 퍼블릭 클라우드에서 개인정보보호 준칙 (ISO/IEC 27018) [12], 개인정보관리체계와 관련된 요구사항 및 지침 (ISO/IEC 27701) [23], 사용자 친화 온라인 고지 및 동의 (ISO/IEC 29184) [26], 개인정보 삭제 프레임워크 (ISO/IEC 27555) [31], 스마트시티 프라이버시 가이드라인 (ISO/IEC 27570)[30] 등의 국제표준을 개발 완료했다.

또한 이 작업반에서는 현재 국내 마이데이터 서비스와 긴밀하게 연관된 프라이버시 선호도 기반 사용자 친화형 개인정보 처리 프레임워크 (ISO/IEC 27556) [32], 조직 프라이버시 리스크 관리 (ISO/IEC 27557) [36], 프라이버시 개선 데이터 비식별화 프레임워크(ISO/IEC 27559) [37], 개인정보보호 관리체계의 인증 및 심사기관 요구사항 (ISO/IEC 27006-2) [38], 동의 레코드 정보 구조 (ISO/IEC 27560) [39] 등 국제표준을 개발하고 있다. 특히 프라이버시 강화 데이터 비식별화 프레

“이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2021-0-00112, 차세대보안 표준전문연구실)”
* 순천향대학교 정보보호학과 (교수, hyyoum@sch.ac.kr)

임워크는 우리나라의 가명처리 기법과 긴밀하게 연계되어 있는 표준이다.

본 고는 [34], [35], [43] 논문으로 이어지는 현행화 논문이라고 볼 수 있다. 본 고의 2장에서는 ISO/IEC JTC 1/SC 27/WG 5에 개발된 주요 채택된 국제표준을 살펴보고, 2020년 4월 전자회의 이후 2022년 4월 SC 27/WG 5 전자회의까지 채택되고 현재 개발되고 있는 개인정보보호 관련 주요 국제표준의 현황과 내용을 살펴본다. 3장에서는 결론을 맺는다.

Ⅱ. SC 27/WG 5 개인정보보호 표준화 동향

2.1. 개인정보보호 관련 국제표준

개인정보보호와 관련된 국제표준은 신원 관리 및 프라이버시 작업반(WG5) [18] 에서 2020년 4월 이전에 채택된 국제표준은 [표 1]과 같고, 2020년 4월 이후에 채택되거나 개발 중인 주요 국제표준을 요약하면 [표 2]와 같다.

[표 1]에 나타난 국제표준은 2020년 4월 이전에 채택 완료된 국제표준이며, 이의 세부 내용은 [43]에 자세히 설명되어 있다. 2020년 4월 이후에는 사용자 친화 고지 및 통보 (ISO/IEC 29184:2020), 스마트시티 프라이버시 가이드라인 (ISO/IEC TS 27570), 그리고 개인정보 삭제 가이드라인 (ISO/IEC 27555) 등의 국제표준이 채택되었다. 다음 절부터는 2020년 4월 이후에 채택되거나 개발되고 있는 주요 국제표준의 세부 내용을 제시한다.

2.2. 온라인 고지 및 동의(ISO/IEC 29184:2020) [26]

이 국제표준은 2016년 3월 신규워크아이템이 채택되었으며, 2020년 5월 FDIS 투표가 성공적으로 완료되어 2020년 6월 국제표준으로 채택되었다. 이 국제표준

〔표 1〕 SC 27/WG 5에서 개발된 개인정보보호 분야 국제표준 (〔43〕 업데이트)

	표준 번호 및 제목	주요 내용	문서 상태	프로젝트 리더
ISO/IEC JTC 1/SC 27/WG 5	▪ ISO/IEC 29100:2011, 프라이버시 프레임워크 [13]	▪ 프라이버시 관련 용어, 개인정보 처리에 있어서 주요 주체의 역할, 보호 요구사항, 프라이버시 보호 원칙 등을 포함한 프라이버시 프레임워크를 제시한다. 이 국제표준은 이후에 개발된 국제표준에서 기반이 되는 프레임워크를 제공하고 있다.	IS (2011.12) /Amd. 1(2020)	Stefan Weiss (DE) and Sue Glueck (US)
	▪ ISO/IEC 27018:2014, 개인정보 수탁자로서 퍼블릭 클라우드에서 개인정보보호 준칙[12]	▪ 공공 클라우드 환경에서 개인정보를 보호하기 위한 통제, 통제 목표, 통제 구현 가이드라인을 제시한다. 이 문서는 ISO/IEC 27002에 근거한다.	IS (2014.8제정/2019.1 개정)	C. Mitchell(UK)
	▪ ISO/IEC 29134:2017, 개인정보영향평가 가이드라인 [15]	▪ 개인정보영향평가(privacy impact assessment)를 위한 과정과 개인정보 영향평가 보고서의 구조와 내용에 대한 가이드라인을 제공한다.	IS (2017.06)/현재 개정중	Mathias Reinis(GE), **Youm Heung Youl(KR)**
	▪ ISO/IEC 29151:2017, 개인정보보호 지침[16]	▪ 개인정보보호와 관련된 위험 평가 결과에 의해 식별된 요구사항을 만족하기 위한 통제와 구현 가이드라인 등을 제시한다.	IS (2017.04)	**Youm Heung Youl(KR),** Alan Shipman(UK)
	▪ ISO/IEC 29190:2014, 개인정보보호 능력 평가 모델 [14]	▪ 개인정보보호 프로세스(process)를 관리하기 위한 조직의 능력(capability)을 평가하는 방법에 대한 상위 수준의 지침을 제공한다.	IS (2014.04)	Shipman Alan(UK)
	▪ ISO/IEC 20889:2018, 데이터 비식별 기법 및 유형[24]	▪ 다양한 데이터 비식별화 기술, 주요 용어 정의, 그리고 비식별화 기법의 유형을 제시한다.	IS (2017.11)	Mitchell Chris(UK), Lionel Vodzislawsky
	▪ ISO/IEC 29003:2018, 온라인 신원증명 (identity proofing) [27]	▪ 온라인에서 사용자에 대한 신원을 증명하는 가이드라인을 제공하고, 신원 확인을 위한 등급, 그리고 이 등급을 만족하기 위한 요구사항을 제시한다.	TS (2018.03)	Knight Joanne(NZ), etc.
	▪ ISO/IEC 27701:2019, 프라이버시 관리를 위한 ISO/IEC 27001과 ISO/IEC 27002의 확장 – 요구사항 및 가이드라인 [23]	▪ 개인정보 보호 관리를 위한 ISO/IEC 27001 개선을 위한 요구사항과 ISO/IEC 27002 통제를 보완한 개인정보처리자와 개인정보 수탁자를 위한 추가적인 프라이버시 통제를 제시한다. 이 국제표준은 글로벌 차원의 개인정보보호 관리체계 인증을 위한 기준으로 활용 가능하다. 이 국제표준은 한국 제안으로 개발중이던 ISO/IEC 29151을 개발하던 도중 요구사항과 개인정보 수탁자의 통제 개발이 필요해 2017년 7월 신규아이템이 채택되었다.	IS (2019.08)	Shipman Alan(UK), **Youm Heung Youl(KR)** etc

〔표 2〕 SC 27/WG 5에서 개발 중인 주요 국제표준 요약 (2022년 7월 현재)

	표준 번호 및 제목	주요 내용	문서 상태	IS 예정	프로젝트 리더 (한국 볼드)
ISO/IEC JTC 1/SC 27/WG 5	▪ ISO/IEC 29184:2020, 사용자 친화 고지 및 통보 [26]	▪ 사용자 친화적 고지 및 통보 방법을 제시한다.	IS (2020.06)	-	Stenuit Christophe(BE), Sakimura Nat(JP), Poosarla Srinivas(IN)
	▪ ISO/IEC TS 27570, 스마트시티 프라이버시 가이드라인 [30]	▪ 스마트시티 서비스를 위한 프라이버시 관련 표준이 글로벌 또는 조직 차원에서 이용자의 이익을 위해 사용되는지에 대한 가이드라인을 제시한다.	TS (2021.01)	-	Kung Antonio,(FR) **Youm Heung Youl(KR)**
	▪ ISO/IEC 27555, 개인정보 삭제 가이드라인 [31]	▪ 조직에서 개인정보 삭제 절차를 개발하기 위한 프레임워크를 제시한다.	IS (2021/10)	-	Dorotea Alessandra de Marco, Yan Sun, Volker Hammer
	▪ ISO/IEC FDIS 27556, 사용자 중심 프라이버시 선호도 관리 프레임워크 [32]	▪ 프라이버시 선호도에 기반한 사용자 친화적 개인정보처리 시스템의 프레임워크를 제시한다.	FDIS	2022.11	Kiyomoto Shinsaku,(JP) Kung Antonio(FR), **Youm Heung Youl(KR)**
	▪ ISO/IEC FDIS 27557, 조직 프라이버시 위험관리를 위한 ISO 31000 적용 [36]	▪ 조직의 개인정보 위험관리 지침을 제공한다.	FDIS	2022.11	Gierschmann Markus, HARPES Carlo, Lucy Kimberly, Magtalas Kelvin
	▪ ISO/IEC FDIS 27559, 프라이버시 강화 데이터 비식별화 프레임워크[37]	▪ 비식별화된 데이터의 수명 주기와 관련된 위험과 재 식별 위험을 찾고 완화하기 위한 프레임워크를 제공한다.	FDIS	2022.11	Townsend Malcolm(CA), Borel Santa
	▪ ISO/IEC DTS 27006-2, 정보보호관리체계를 위한 인증기관과 심사기관 요구사항 - 파트 2 개인정보보호 관리체계 [38]	▪ 조직의 개인정보 관리체계 (PIMS)를 심사 및 인증을 제공하는 기관에 대한 요구사항을 지정하고 지침을 제공한다. 주로 PIMS 인증을 제공하는 인증기관의 인증을 지원하기 위한 것이다.	CD(TS)	2024.4	Azetsu Fuki, Lucy Kimberly, Robinson Gigi
	▪ ISO/IEC WD4 27560, 동의 레코드 정보 구조[39]	▪ 데이터 주체의 데이터 처리 동의를 기록하기 위해 상호 운용 가능하고 개방적이며 확장 가능한 정보 구조를 정의한다.	WD4	2023.12	Hughes Andrew, Lindquist Jan, Magtalas Kelvin
	▪ ISO/IEC CD 27561, 프라이버시 운용 모델 및 엔지니어링 방법 [44]	▪ 개인정보 보호 원칙을 일련의 통제 및 기능적 기능으로 운용하는 모델과 방법을 설명한다.	CD	2024.3	Sabo John, de Marco Dorotea Alessandra, Kung Antonio, etc
	▪ ISO/IEC WD4 27562, 핀테크 서비스 프라이버시 가이드라인 [40]	▪ 핀테크에서 프라이버시 가이드라인을 제공한다.	WD3	2024.3	**You**m Heung Youl (KR), Janssen Esguerra(PH)
	▪ ISO/IEC DTR 27563, 인공지능 이용 사례에서 보안과 프라이버시 [45]	▪ ISO/IEC TR 24030(정보 기술 - 인공 지능(AI) - 이용 사례)에 게시된 활용 사례를 포함하여 인공 지능 이용 사례에서 보안 및 개인 정보를 평가하는 방법에 대한 정보를 제공한다.	CD TR	2023.2	Kung Antonio(FR), **Youm Heung Youl(KR)**, etc
	▪ PWI 27564, 프라이버시 모델 [41]	▪ 프라이버시 엔지니어링에서 모델링을 사용하는 방법에 대한 지침을 제공한다.	PWI	-	Kung Antonio(FR), etc
	▪ ISO/IEC 27565, 영지식 증명 기반 프라이버시 보존 가이드라인 [47]	▪ 영지식 증명 기술 이용을 위한 가이드라인을 제공한다.	WD	2025.3	Curry Patrick(UK), Poosarla Srinivas(IN), zhang bingsheng(CH)
	▪ WG5 SD1, 로드맵 [46]	▪ WG5 로드맵을 제공한다.매 회의마다 입력 의견을 반영해 갱신된다.	SD (standing document)	-	Kai Rannenburg(GE)
	▪ WG5 SD2, 프라이버시 참조 리스트 [33]	▪ 이 문서는 주요국의 프라이버시 관련 법과 규정, 데이터 보유 기간, 주요 국제표준, 지침, 그리고 법/표준/가이드라인간의 관계를 제시하고 있다. 한국의 개인정보보호법, 정보보호 및 개인정보보호 관리체계 등의 주요 내용]이 포함되어 있다.	SD (standing document)	-	-

은 정보주체로부터 개인정보를 수집하여 처리하기 위해 동의를 요청하는 과정과 온라인 프라이버시 고지의 문서의 내용과 구조를 정의한다. 고지(notice)의 내용은 처리 목적 설명, 개인정보 처리자의 신원, 수집되는 정보 유형, 수집 방법, 수집 시점과 장소, 이용 방법, 저장되는 곳의 법적 관할, 제3자 제공, 보유기간, 정보주체

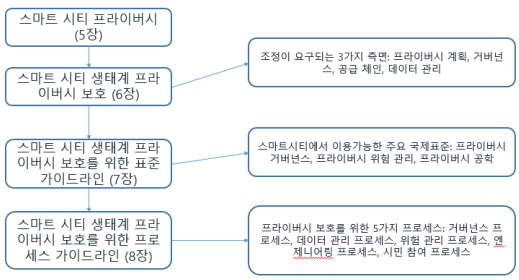
참여 방법, 질의 및 불만처리 연락처, 처리 근거, 처리 관련 위험 등을 포함한다. 동의를 위해서는 동의가 필요한지 여부, 숙지되고 자유로운 동의, 정보주체가 사용하는 계정에 관한 정보, 다른 동의와 독립적인 동의, 필수 및 선택 동의의 구분, 새 동의 획득 빈도, 시점 등을 규정하고 있다[43].

2.3. 스마트시티 프라이버시 가이드라인 (ISO/IEC TS 27570) [30]

이 국제표준은 2018년 2월 신규워크아이템으로 채택되었으며, 2020년 7월 DTS로 채택되었으며, 2021년 1월 국제표준(TS)으로 채택되었다. 이 국제표준은 시민 중심으로 스마트시티 서비스와 연관되는 여러 주요 이해당사자를 선택한다. 또한 스마트시티 생태계의 개인정보 보호, 시민의 이익을 위해 글로벌 수준 및 조직 수준에서 표준을 사용하는 방법, 스마트 도시 생태계 개인정보 보호 프로세스에 대한 지침을 제공한다.

[그림 1]은 본 표준의 구조를 나타낸다. 5장은 스마트시티에서 개인 정보를 통합하는 문제를 다룬다. 6장에서는 스마트시티 생태계에서 조정이 필요한 거버넌스, 공급망 및 데이터 관리의 세 가지 측면을 자세히 설명한다. 7장은 스마트시티에서 사용할 수 있는 국제표준에 대한 개요를 제공한다. 8장은 거버넌스, 데이터 관리, 위험관리, 엔지니어링 및 시민 참여의 5가지 프로세스를 설명한다.

필자는 이 국제표준의 프로젝트 리더로 참여했다.



〔그림 1〕 ISO/IEC 27570 표준 구조

2.4. 개인정보 삭제 가이드라인(ISO/IEC IS 27555) [31]

이 국제표준은 2019년 2월 신규워크아이템으로 채택되었으며, 2021년 9월 FDIS 투표가 완료되었으며, 2021년 10월 국제표준으로 채택되었다. 삭제(deletion)는 개인정보(PII)가 더 이상 존재하지 않거나 인식되지 않고 과도한 노력으로만 개인정보로 복구할 수 있도록 개인정보를 변경하는 프로세스로 정의되었다. 이 국제표준은 다음을 지정하여 조직에서 개인정보를 삭제하기 위한 정책 및 절차를 개발하고 수립하기 위한 지침을 포함하고 있다.

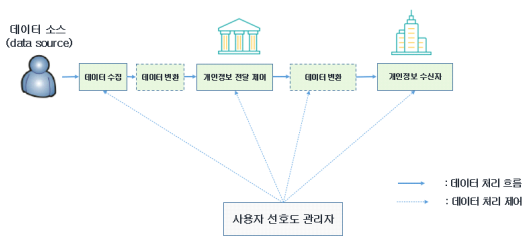
- 개인정보 삭제에 대한 통일된 용어
- 효율적으로 삭제 규칙을 정의하기 위한 방식
- 요구되는 문서화에 대한 설명
- 역할, 책임 및 프로세스에 대한 광범위한 정의

2.5. 사용자 중심 프라이버시 선호도 관리 프레임워크 (ISO/IEC FDIS 27556) [32]

이 국제표준은 2019년 2월 신규워크아이템으로 채택되었고, 2022년 4월 DIS로 채택되었으며, 2022년 7월 7일부터 FDIS 투표가 진행 중이다. 이 국제표준은 프라이버시 선호도에 기반한 사용자 친화적 개인정보처리 프레임워크를 제시한다. 이 국제표준은 정보주체에 의한 개인정보 기본 설정에 따라 개인정보(PII)를 처리하기 위한 사용자 중심 프레임워크를 제공한다.

[그림 2]와 같이 사용자의 프라이버시 선호도에 기반 프레임워크에서 주요 구성요소를 나타낸다. 데이터 발신지와 데이터 수신자 사이에는 개인정보 전달 제어 기능이 존재한다. 데이터 발신지에서 수집된 데이터는 필요에 따라서 데이터 비식별화나 데이터 삭제가 수행되면, 개인정보 전달 제어 기능은 사용자 선호도 관리자의 통제하에 개인정보의 전달 여부를 결정한다. 개인정보가 전달되어야 한다고 판단되면 해당 데이터는 다시 변환될 수 있으며, 그 결과가 데이터 수신자에게 제공된다.

이 국제표준은 개인정보 주체, 개인정보처리자, 개인



〔그림 2〕 사용자 선호도 관리 프레임워크의 구성요소

정보 수탁자, 프라이버시 선호 관리자 등으로 구성된 주요 참여 주체를 정의하고, 데이터 수집, 비식별화, 개인정보 제공 등으로 구성된 주요 구성요소를 제시한다. 또한 프라이버시 참조 관리의 역할을 정의하고 있다.

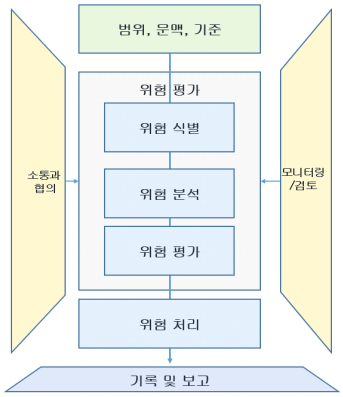
필자는 이 표준의 프로젝트 리더로 참여하고 있다.

2.6. 조직 프라이버시 위험관리(ISO/IEC FDIS 27557) [36]

이 국제표준은 2020년 1월 신규워크아이템으로 채택되었으며, 2022년 4월 DIS로 채택되었으며, 2022년 8월부터 FDIS 투표로 진전될 예정이다.

ISO/IEC 31000 [42] 에서는 [그림 3]와 같이 위험관리를 위한 프로세스로 소통과 협의, 범위/문맥/기준, 위험 식별/분석 등으로 구성되는 위험 평가, 모니터링/검토, 그리고 기록과 보고 프로세스로 구성된다[43].

이 국제표준은 ISO 31000:2018에서 확장된 조직의 개인정보 위험관리에 대한 지침을 제공한다. 다시 말해, ISO 31000에서 정의된 일반적인 위험관리에 개인정보 보호 위험관리 요구사항을 추가하고 있다.



〔그림 3〕 ISO/IEC 31000 위험관리 프로세스 〔42〕

2.7. 프라이버시 강화 데이터 비식별화 프레임워크 (ISO/IEC 27559) [37]

이 국제표준은 2019년 12월 신규워크아이템으로 채택되었고, 2022년 4월 DIS 로 진전되어, 현재 FDIS 상태에 존재한다. 비식별화(de-identification)는 개인 또는 개인 그룹의 개인 정보를 식별하지 않는 방식으로 개인정보(PII) 이용을 촉진하기 위한 잠재적 수단 중 하나이다. 이 국제표준은 비식별화된 데이터의 수명 주기와 관련된 재식별 위험을 식별하고 이를 완화하기 위한 프레임워크를 제공한다. 이 표준에서 정의된 3가지 방식을 정의하고 있으며, 내부 조직에 의한 비식별 데이터의 이용, 외부 조직에 의한 비식별 데이터의 이용, 그리고 비식별 데이터를 일반에 공개해 이용하는 방법이다.

2.8. 개인정보보호 관리체계 인증 및 심사기관 요구사항(ISO/IEC TS/CD 27006-2) [38]

이 국제표준은 2019년 10월 신규워크아이템으로 채택되었으며, 2020년 9월 DTS로 채택되었으며, 2021년 4월 TS로 국제표준으로 채택되었다. 다시 개정안을 마련하기 위해 2022년 6월 CD 투표가 진행되고 있다.

이 국제표준은 개인정보관리체계를 운영하는 신청기관에 대한 심사기관과 인증기관을 위한 평가 및 인증에 대한 요구사항을 지정한다. 또한 ISO/IEC 27006-1에 포함된 요구사항 외에도 ISO/IEC 27001과 결합한 ISO/IEC 27701에 따라 개인정보 관리체계(PIMS)의 감사 및 인증을 제공하는 기관에 대한 지침을 제공한다.

대표적인 추가 요구사항은 “인증기관은 PIMS와 관련된 관리체계에 대한 컨설팅(예: 외부 데이터 보호 책임자로서의 서비스, 관리 프로세스 또는 데이터 보호 프로세스에 관한 컨설팅)을 제공하지 않아야 한다” 등이다.

2.9. 동의 레코드 정보 구조(ISO/IEC WD4 27560) [39]

이 국제표준은 2020년 4월 회의에서 신규워크아이템으로 채택되었고, 현재 WD4 상태에 있다. 이 국제표준은 개인정보 처리에 대한 동의를 기록하기 위한 상호운용 가능하고 개방적이며 확장 가능한 정보 구조를 규정한다. 또한 다음을 지원하기 위해 정보주체의 개인정보 처리 동의와 관련된 동의 영수증 및 동의 기록의 사용에 대한 지침을 추가로 제공한다:

- 정보주체에 대한 동의 기록 제공
- 정보 시스템 간의 동의 정보 교환
- 기록된 동의의 수명 주기 관리

2.10. 프라이버시 운용 모델 및 엔지니어링 방법 (ISO/IEC CD 27561) [44]

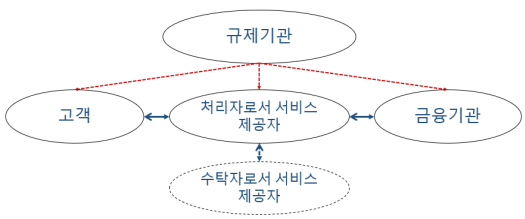
이 국제표준은 2021년 1월 신규워크아이템으로 채

택되어, 현재 CD 상태에 있다. 이 국제표준은 개인정보 보호 원칙을 일련의 통제 및 기능적 능력으로 운용하기 위한 모델 및 방법을 설명한다. 운용 방법은 ISO/IEC/IEEE 24774에 따른 프로세스이다. 또한 ISO/IEC 29100에 나타난 보호 원칙을 운용한다. 개인정보를 제어하거나 처리하는 시스템을 개발하는 엔지니어 및 기타 실무자를 위한 표준이다. 다른 표준 및 개인정보보호 지침과 함께 사용하도록 설계된다. 네트워크로 연결된 상호 의존적인 응용 프로그램 및 시스템을 지원한다.

2.11. 핀테크 서비스 프라이버시 가이드라인 (ISO/IEC WD3 27562) [40]

이 국제표준은 우리나라의 제안으로 2021년 1월 신규워크아이템으로 채택되어, 2022년 5월부터 WD3 투표가 진행 중이다.

이 국제표준은 핀테크 서비스에 대한 개인 정보 보호에 대한 지침을 제공한다. 핀테크 서비스와 관련된 소비자 대 기업 관계 및 기업 대 기업 관계, 개인정보 위험 및 개인정보 요구사항에서 모든 관련 비즈니스 모델 및 역할을 식별한다. 각 비즈니스 역할의 법적 맥락을 고려하여 개인정보 위험을 해결하기 위해 핀테크 서비스에 특정한 개인 정보 통제를 제공한다. 개인정보 보호 원칙은 ISO/IEC 29100, ISO/IEC 27701 및 ISO/IEC 29184에 설명된 원칙과 ISO/IEC 29134 및 ISO 31000에 설명된 개인정보 영향평가 프레임워크를 기반으로 한다. 필자는 이 국제표준의 프로젝트 리더를 맡고 있다. 이 국제표준의 주요 이해당사자는 [그림 4]와 같다. 규제기관은 핀테크 서비스를 규제하는 기관이며, 고객은 정보주체로, 개인정보처리자로서의 핀테크 서비스 제공자, 수탁자로서의 서비스 제공자, 그리고 기존 금융기관으로 구성된다. 이 국제표준은 각 이해당사자의 통



〔그림 4〕 핀테크 서비스를 위한 주요 이해당사자

제를 개발하는 것이다.

2.12. 인공지능의 보안 및 프라이버시 (ISO/IEC DTR 27563) [41, 45]

이 국제표준은 2021년 11월 CD 상태로 등록되었으며, 현재 CD 투표가 진행중이다. 이 국제표준은 ISO/IEC TR 24030 (정보 기술 - 인공 지능(AI) - 이용 사례)에 설명된 120 가지 경우의 이용 사례에 대한 보안 및 개인정보 측면에서 평가하기 위한 방법을 제공한다. 특히 이 국제표준의 부록에는 120개의 이용 사례에 대한 보안 및 프라이버시 위험, 이 위험을 완화할 수 있는 통제를 제공하고 있다. 필자는 이 국제표준의 프로젝트 리더를 맡고 있다.

2.13. 영지식 증명 이용 가이드라인 (ISO/IEC WD 27565) [47]

이 국제표준은 공유 정보를 최소화하여 조직과 사용자 간의 개인 데이터 공유 또는 전송과 관련된 위험을 줄임으로써 개인정보 보호를 개선하기 위해 ZKP (영지식 증명)를 사용하는 방법에 대한 지침을 제공한다. 여기에는 다양한 비즈니스 이용 사례와 관련된 여러 영지식 증명의 기능 요구 사항을 포함하고, 이러한 기능 요구 사항을 안전하게 충족하기 위해 다양한 영지식 증명(ZKP) 모델을 사용할 수 있는 방법을 설명한다.

2.14. 표준화 로드맵 (WG5 SD1) [46]

이 문서는 국제표준이 아닌 WG5에서 유지하고 있는 로드맵 문서이다. 이 문서는 매 회의마다 업데이트되고 있으며, WG5에서 국제표준으로 개발되었거나 개발이 진행중인 모든 국제표준을 일목 요연하게 체계적으로 영역을 나눠서 보여주고 있다. 특히, 개인정보보호 측면의 국제표준과 문서, 신원관리 측면의 국제표준과 문서를 모두 보여주고 있다. 이 문서는 2022년 4월 전자회의에서 갱신되었다.

2.15. 프라이버시 참조 리스트 (WG5 SD2) [33]

이 문서는 국제표준이 아닌 WG5에서 유지하고 있는 문서이며, 매 회의마다 업데이트된다. 이 문서는 매

회의마다 한국, 미국, 영국 등 주요국의 개인정보보호 법과 규정을 제시하고 있고, 한국, 프랑스, 영국 등 주요국의 개인정보 보유 기간을 보여 주며, 프라이버시 보호 관련 국제표준을 제시하며, 금융 분야를 포함한 11개 분야의 프라이버시 가이드라인을 제시하고 있다. 또한 2022년 4월 회의에서 한국에서 개인정보보호 관련 법에 대한 추가 정보를 제공하여 반영하였다.

Ⅲ. 결 론

본 고에서는 SC 27/WG 5에서 개발되었거나 개발 중에 있는 개인정보보호 관련 주요 국제표준의 내용을 제시하고 분석하였다. 본 고에서는 지난 2020년 4월 이후부터 2022년 4월 회의에 수행된 개인정보보호 분야의 활동 결과를 중심으로 기술했다. 개인정보 제도나 관행은 국제표준의 근거해 시행되어야 글로벌 차원의 상호연동성을 보장받는다. 향후 개발해야 할 주요 표준화 주제는 비정형 영상 정보에 대한 비식별화 기법, 비정형 영상정보 활용사례, 비식별 데이터 결합 방법 등이다. 본 고의 결과는 개인정보보호 관련 국내 표준화 로드맵 마련시에 적극 활용될 수 있다.

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 29190:2015, Information technology – Security techniques – Information technology -- Security techniques -- Privacy capability assessment model

[15] ISO/IEC 29134:2017, Privacy Impact Assessment - Methodology

[16] ISO/IEC 29151:2017, 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, Information security, cybersecurity, privacy protection, http://www.iso.org/iso/iso_technical_committee?commid=45306

[19] WG 5/SD 1, WG 5 Roadmap, 2019.4

[20] 염흥열, “개인정보보호 관리체계 국제표준화 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 IS 27552, Enhancement to ISO/IEC 27001 for privacy management – Requirements, 2019.8.

[24] ISO/IEC 20889:2018, Information technology —

Security techniques – Privacy enhancing data de-identification terminology and classification of techniques
[25] 행정안전부, 방송통신위원회 등, “비식별화조치 가이드라인,” 2016.6.30.
[26] ISO/IEC 29184, Guidelines for online privacy notices and consent, 2019.07
[27] ISO/IEC TS 29003:2018, Identity proofing
[28] 염흥열, 국제 개인정보보호 표준화 동향 분석 (2016년 4월 탬퍼 SC27 회의 결과를 중심으로), 정보보호학회지, v.26, no.4, 6-10, 2016.8
[29] EU, GDPR (general data protection regulation), 27 April 2016
[30] ISO/IEC TS 27570, Privacy guidelines for smart cities, January 2021
[31] ISO/IEC IS 27555, Guidelines on personally identifiable information deletion, October 2021
[32] ISO/IEC FDIS 27556, User-centric privacy preferences management framework
[33] ISO/IEC JTC 1/SC 27/WG 5 N 3211, Call for comments on SC 27/WG 5 Standing Document 2 (WG 5 SD2) -- Privacy references list, 2022.5.31
[34] 염흥열, 국제 개인정보보호 표준화 동향 분석 (2017년 4월 해밀턴 SC27 회의 결과를 중심으로)), 한국정보보호학회 학회지, 제27권 제5호, pp.6-11, 2017.10
[35] 염흥열, 국제 개인정보보호 표준화 동향 분석 (2019년 4월 이스라엘 텔아비브 SC27 회의 결과를 중심으로)), 한국정보보호학회 학회지, 제29권 제4호, 2019.08
[36] ISO/IEC FDIS 27557, Application of ISO 31000:2018 for organizational privacy risk management
[37] ISO/IEC FDIS 27559, Privacy enhancing data de-identification framework
[38] ISO/IEC CD 27006-2, Requirements for bodies providing audit and certification of information security management systems -- Part 2: Privacy Information Management Systems
[39] ISO/IEC WD4 27560, Privacy technologies – Consent record information structure
[40] ISO/IEC WD3 27562, Information technology – Security techniques – Privacy guidelines for fintech services 2022-05-11
[41] ISO/IEC JTC 1/SC 27/WG 5 N3215, Cfc on ISO/IEC PWI 27564 Privacy models, 2022.05.31
[42] ISO 31000:2018, Risk management
[43] 염흥열, 국제 개인정보보호 표준화 동향 분석 (2020년 4월 전자 회의 결과를 중심으로), 한국정보보호학회 학회지, 제30권 제4호, 2020.08
[44] ISO/IEC CD 27561, Security techniques – Privacy operationalisation model and method for engineering (POMME)
[45] ISO/IEC CD TR 27563, Privacy protection - Security and privacy in artificial intelligence use cases
[46] ISO/IEC JTC 1/SC 27/WG 5 N 3187, Call for comments on WG 5 SD1 – WG 5 Roadmap, 2022.5.19.
[47] ISO/IEC WD 27565, Guidelines on privacy preservation based on zero knowledge proofs

〈저자소개〉

염 흥 열 (Heung Youl Youm)
종신회원
한양대학교 전자공학과 학사 졸업
한양대학교 대학원 전자공학과 석사
한양대학교 대학원 전자공학과 박사
1982년 12월~1990년 8월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 정교수
2017년~현재 : ITU-T SG17 의장
2009년~2016년 : ITU-T SG17 부의장, WP3 의장
2011년 1월~12월 : 한국정보보호학회 회장
2012년 1월~현재 : 한국정보보호학회 명예회장
2016년 5월~현재 : 개인정보보호표준포럼 의장
2020년 8월~현재 : 개인정보보호위원회 위원
<관심분야> 네트워크 보안, IoT 보안, 블록체인 보안, 개인정보보호, 정보보안 국제표준