정 보 보 호 학 회 지
제 33 권 제4호, 2023. 8

국제 개인정보보호 표준화 동향 분석 (2023년 4월 ISO/IEC JTC 1/SC 27/WG 5 회의 결과를 중심으로)

박 성 채*, 염 흥 열**

요 약

최근 인공지능, 디지털 트윈, 메타버스 기반의 신규 ICT 서비스가 도입되면서 이러한 서비스에서 발생할 수 있는 프라이버시 위험의 적절한 처리는 매우 중요하게 대두되었다. 이의 대표적인 기술적 대책이 프라이버시 강화 기술의 적용이다. 이와 관련하여 개인정보보호 국제표준은 국가나 조직의 관행과 기술을 국제 표준으로 개발하여 상호 연동이 가능한 서비스를 제공하는 역할을 하며, 이로 인해 제품이나 서비스의 경쟁력을 강화하는데 활용될 수 있다. 개인정보보호 국제 표준화를 주도적으로 추진하고 있는 대표적인 국제 표준화 그룹으로는 국제표준화위원회/전기위원회 합동위원회 1/서브위원회 27/작업그룹 5 (ISO/IEC JTC 1/SC 27/WG 5)가 있으며, 독일 쾨테대학의 Kai Rannenberg 교수가 이 그룹의 의장을 맡고 있다. 2022년 ISO/IEC JTC 1/SC 27/WG 5 전자회의 이후 우리나라 주도의 국제표준은 2건 채택되었다. 차기 회의는 2023년 10월 서울에서 원격 참여가 허용된 대면회의로 개최될 예정이다. 본 고에서는 이 그룹에서 2022년 7월 이전 채택된 개인정보보호 관련 국제표준과 현재 개발 중인 주요 국제표준 동향을 살펴보고자 한다. 또한 지난 4월 SC27 WG5 회의에서 논의된 개인정보보호 관련 주요 표준화 이슈와 대응 방안을 제시한다.

Ⅰ. 서 론

우리나라 개인정보보호법[1]에서는 개인정보를 “살아 있는 개인에 관한 정보”로 정의한다. 그리고 2020년 8월에 시행된 통합 개인정보보호법을 통해 가명 정보의 활용과 결합이 활발히 이루어지고 있다. 가명처리는 “개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리”하는 것으로, 개인정보처리자는 통계 작성, 과학적 연구, 공익적 기록 보존 등을 위해 정보주체의 동의 없이 가명처리된 가명정보를 처리할 수 있다[1]. 2018년 5월 25일부터 발효된 유럽연합 개인정보보호법(GDPR, general data protection regulation)[2] 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.

최근 인공지능, 디지털 트윈, 메타버스 기반의 서비스가 도입되면서 이러한 서비스에서 발생할 수 있는 프라이버시 위험의 적절한 처리가 매우 중요하게 대두되었다. 이의 대표적인 기술적 대책이 프라이버시 강화 기술의 적용이다.

ISO/IEC JTC 1/SC 27/WG 5 [3]는 개인정보보호와 관련된 국제표준을 개발하고 있는 표준화 그룹이다.

본 고는 [21], [22], [23], [24] 후속 논문으로 2022년 하반기와 2023년 상반기 WG5에서 수행된 표준화 활동을 반영한 논문이라고 볼 수 있다. 본 고의 내용은 [24]에 기반을 두고 업데이트했으므로, 독자의 편의와 완전성을 위해 많은 부분을 인용했음을 미리 알린다.

본 고의 2장에서는 ISO/IEC JTC 1/SC 27/WG 5에서 개발된 국제표준과 2022년 4월 회의 이후 2023년 4월 SC 27/WG 5 회의에서 채택된 신규 개발 표준을 포함하여 개인정보보호와 관련된 주요 국제표준의 현황과 내용을 살펴본다. 3장에서는 결론을 맺는다.

“이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2021-0-00112, 차세대보안 표준전문연구실)”
* 순천향대학교 차세대보안 표준전문연구실 (선임연구원, zoesc.park@sch.ac.kr)
** 순천향대학교 정보보호학과 (교수 , hyyoum@sch.ac.kr)

〔표 1〕 SC 27/WG 5에서 개발된 개인정보보호 분야 국제표준 (〔24〕 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 [4]	▪ 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 [7]	▪ 공공 클라우드 환경에서 개인정보를 보호하기 위한 통제, 통제 목표, 통제 구현 가이드라인을 제시한다. 이 문서는 ISO/IEC 27002에 근거한다.	IS (2014.8제정/2023.4 현재 개정중)	C. Mitchell(UK) / Chandramouli Ramaswamy(US), Hendrik Decroos(BE)
	▪ ISO/IEC 29134:2017, 개인정보 영향평가 가이드라인 [5]	▪ 개인정보영향평가(privacy impact assessment)를 위한 과정과 개인정보 영향평가 보고서의 구조와 내용에 대한 가이드라인을 제공한다.	IS (2017.06제정/2023.6개정)	Mathias Reinis(GE), **Heung Youl Youm (KR)** / Okuma Mieko(JP)
	▪ ISO/IEC 29151:2017, 개인정보보호 지침 (개정) [6]	▪ 개인정보보호와 관련된 위험 평가 결과에 의해 식별된 요구사항을 만족하기 위한 통제와 구현 가이드라인 등을 제시한다. 이 국제표준은 5년후 검토후 2023년 4월 회의에서 마이너 개정을 추진하기로 합의했다.	IS (2017.04제정/현재 개정중)	**Heung Youl Youm (KR),** Alan Shipman(UK) / **Heung Youl Youm (KR),** Alan Shipman(UK), Erik Boucher(FR), **Sungchae Park(KR)**
	▪ ISO/IEC 29190:2014, 개인정보보호 능력 평가 모델 [29]	▪ 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 [30]	▪ 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) [31]	▪ 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 [8]	▪ 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 (2019.08제정/현재 DIS 개정중)	Shipman Alan(UK), **Heung Youl Youm (KR)** etc
	▪ ISO/IEC 29184:2020, 사용자 친화 고지 및 통보 [9]	▪ 사용자 친화적 고지 및 통보 방법을 제시한다.	IS (2020.06)	Stenuit Christophe(BE), Sakimura Nat(JP), Poosarla Srinivas(IN)
	▪ ISO/IEC 27555, 개인정보 삭제 가이드라인 [10]	▪ 조직에서 개인정보 삭제 절차를 개발하기 위한 프레임워크를 제시한다.	IS (2021/10)	Dorotea Alessandra de Marco, Yan Sun, Volker Hammer
	▪ ISO/IEC TS 27570, 스마트 시티 프라이버시 가이드라인 [11]	▪ 스마트시티 서비스를 위한 프라이버시 관련 표준이 글로벌 또는 조직 차원에서 이용자의 이익을 위해 사용되는지에 대한 가이드라인을 제시한다.	TS (2021.01)	Antonio Kung ,(FR) **Heung Youl Youm (KR)**
	▪ ISO/IEC 27556, 이용자 중심 프라이버시 선호 관리 프레임워크 [12]	▪ 프라이버시 선호에 기반한 이용자 친화적 개인정보처리 시스템의 프레임워크를 제시한다.	IS (2022.10)	Kiyomoto Shinsaku,(JP) Antonio Kung (FR), **Youm Heung Youl(KR)**
	▪ ISO/IEC 27557, 조직 프라이버시 위험 관리를 위한 ISO 31000 적용 [14]	▪ 조직의 개인정보 위험 관리 지침을 제공한다.	IS (2022.11)	Gierschmann Markus, HARPES Carlo, Lucy Kimberly, Magtalas Kelvin
	▪ ISO/IEC 27559, 프라이버시 강화 데이터 비식별화 프레임워크 [15]	▪ 비식별화된 데이터의 수명 주기와 관련된 위험과 재식별 위험을 찾고 완화하기 위한 프레임워크를 제공한다.	IS (2022.11)	Townsend Malcolm(CA), Borel Santa
	▪ ISO/IEC TS 27560, 동의 레코드 정보 구조[17]	▪ 데이터 주체의 데이터 처리 동의를 기록하기 위해 상호 운용 가능하고 개방적이며 확장 가능한 정보 구조를 정의한다.	TS (2023.8)	Hughes Andrew, Lindquist Jan
	▪ ISO/IEC TR 27563, 인공지능 이용 사례에서 보안과 프라이버시 [13]	▪ 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.	TR (2023.5)	Antonio Kung(FR), **Youm Heung Youl(KR)**, etc

Ⅱ. SC 27/WG 5 개인정보보호 표준화 동향

2.1. 개인정보보호 관련 국제표준화 현황 개요

이 그룹에서는 프라이버시 프레임워크 (ISO/IEC 29100) [4], 프라이버시 영향평가 (ISO/IEC 29134) [5], 개인정보보호 준칙(ISO/IEC 29151) [6], 개인정보 수탁자로서 퍼블릭 클라우드에서 개인정보보호 준칙 (ISO/IEC 27018) [7], 개인정보관리체계와 관련된 요구사항 및 지침 (ISO/IEC 27701) [8], 사용자 친화 온라인 고지 및 동의 (ISO/IEC 29184) [9], 개인정보 삭제 프레임워크 (ISO/IEC 27555) [10], 스마트시티 프라이버시 가이드라인 (ISO/IEC TS 27570) [11] 개발을 완료했고, 국내 마이데이터 서비스와 긴밀하게 연관된 사용자 중심 프라이버시 선호 관리 프레임워크 (ISO/IEC 27556) [12] 와 인공지능 이용 사례에서 보

〔표 2〕 SC 27/WG 5에서 개발 또는 개정 중인 주요 국제 표준 요약 (2023년 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 27018 (PWI 8894), 개인정보 수탁자로서 퍼블릭 클라우드에서 개인정보보호 준칙 [7]	▪ 공공 클라우드 환경에서 개인정보를 보호하기 위한 통제, 통제 목표, 통제 구현 가이드라인을 제시한다. 이 문서는 ISO/IEC 27002에 근거한다.	PWI	-	Chandramouli Ramaswamy(US), Hendrik Decroos(BE)
	▪ ISO/IEC 29151 (PWI 8888), 개인정보보호 지침 [6]	▪ 개인정보보호와 관련된 위험 평가 결과에 의해 식별된 요구사항을 만족하기 위한 통제와 구현 가이드라인 등을 제시한다. 이 국제표준은 5년후 검토 후 2023년 4월 회의에서 마이너 개정을 추진하기로 합의했다.	PWI	-	**Heung Youl Youm (KR)**, Alan Shipman(UK), Erik Boucher(FR), **Sungchae Park(KR)**
	▪ ISO/IEC DIS 27701, 프라이버시 관리를 위한 ISO/IEC 27001과 ISO/IEC 27002의 확장 – 요구사항 및 가이드라인 [8]	▪ 조직이 개인정보 관리를 위해 ISO/IEC 27001 및 ISO/IEC 27002 를 확장한 형태로 개인정보 관리 시스템 (PIMS) 을 수립, 구현, 유지 관리 및 지속적으로 개선하기 위한 요구사항과 지침을 제공한다.	DIS	2023.10	Shipman Alan(UK), **Youm Heung Youl(KR)**
	▪ ISO/IEC DIS 27006-2, 정보보호관리체계를 위한 인증기관과 심사기관 요구사항 – 파트 2 개인정보보호 관리체계 [16]	▪ 조직의 개인정보 관리체계 (PIMS)를 심사 및 인증을 제공하는 기관에 대한 요구사항을 지정하고 지침을 제공한다. 주로 PIMS 인증을 제공하는 인증기관의 인증을 지원하기 위한 것이다.	DIS	2024.4	Azetsu Fuki, Lucy Kimberly, Robinson Gigi
	▪ ISO/IEC DIS 27561, 프라이버시 운용 모델 및 엔지니어링 방법 [18]	▪ 개인정보 보호 원칙을 일련의 통제 및 기능적 기능으로 운용하는 모델과 방법을 설명한다.	DIS	2024.3	Sabo John, de Marco Dorotea Alessandra, Antonio Kung(FR), etc
	▪ ISO/IEC CD2 27562, 핀테크 서비스 프라이버시 가이드라인 [19]	▪ 핀테크에서 프라이버시 가이드라인을 제공한다.	CD2	2024.3	**Youm Heung Youl (KR)**, Janssen Esguerra(PH)
	▪ ISO/IEC WD 27565, 영지식 증명 기반 프라이버시 보존 가이드라인 [20]	▪ 영지식 증명 기술 이용을 위한 가이드라인을 제공한다.	WD	2025.3	Curry Patrick(UK), Poosarla Srinivas(IN), zhang bingsheng(CH)
	▪ ISO/IEC WD 27566, 연령 보증 [35]	▪ 연령 보증 시스템의 프레임워크, 보증 수준 및 개인정보보에 대한 정보를 제공한다	WD	2025.11	Tony Allen (GB)
	▪ WG5 SD1, 로드맵 [27]	▪ WG5 로드맵을 제공한다.매 회의마다 입력 의견을 반영해 갱신된다.	SD (standing document)	-	Kai Rannenburg(GE)
	▪ WG5 SD2, 프라이버시 참조 리스트 [28]	▪ 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)	-	-

〔표 3〕 SC 27/WG 5에서 사전 표준화 활동 아이템(PWI) (2023년 7월 현재)

	표준 번호 및 제목	주요 내용	문서 상태	프로젝트 리더(한국 볼드)
ISO/IEC JTC 1/SC 27/WG 5	▪ PWI 8887 신원 정보 품질 및 관련 아키텍처에 대한 권한 [32]	▪ 신원 정보 품질 및 이와 관련된 아키텍처에 대한 권한을 제공한다.	PWI	Yasuo MIYAKWA (JP), **Yeung Youl Youm(KR)**, etc
	▪ PWI 6087 디지털 인증: 위험 및 보호조치 [33]	▪ 온라인 인증의 라이프사이클을 고려한 통제 항목을 제시한다.	PWI	**Heung Youl Youm(KR)**, Eduard de Jong(DE), Thomas Schnattinger(DE), etc
	▪ PWI 27568 디지털 트윈의 보안과 프라이버시 [34]	▪ 디지털 트윈 시스템의 보안과 개인정보 보호와 관련된 표준에 대한 개요를 제공한다. 또한 디지털 시스템의 이해당사자를 위한 보안 및 개인정보 보호 측면의 고려사항을 제공한다.	PWI	Curry Patrick(UK), **Yeung Youl Youm(KR)**, Antonio Kung(FR), etc

안과 프라이버시(ISO/IEC TR 27563) [13], 조직 프라이버시 리스크관리 (ISO/IEC 27557) [14], 프라이버시 개선 데이터 비식별화 프레임워크(ISO/IEC 27559) [15], 개인정보보호 관리체계의 인증 및 심사 기관 요구사항 (ISO/IEC 27006-2) [16], 동의 레코드 정보 구조 (ISO/IEC 27560) [17] 등도 국제표준으로

개발 완료되었다. 특히 프라이버시 강화 데이터 비식별화 프레임워크는 우리나라의 가명처리 기법과 긴밀하게 연계된 표준이다.

또한 이 작업반에서는 핀테크 서비스 프라이버시 가이드라인 (ISO/IEC CD2 27562)[18], 프라이버시 운용 모델 및 엔지니어링 방법 (ISO/IEC DIS 27561) [19], 영지식 증명 기반 프라이버시 보존 가이드라인 (ISO/IEC WD 27565) [20] 등 국제표준을 개발하고 있다.

개인정보보호와 관련된 국제 표준과 관련해 신원관리 및 프라이버시 작업반(WG 5) [25] 에서 2023년 4월까지 채택된 국제표준은 [표 1]과 같고 이의 세부 내용은 [24] 에 자세히 설명되어 있다. 지난 2022년 9월 회의 이후 우리나라가 주도로 개발한 마이데이터 서비스와 연관되는 이용자 중심 개인정보보호 선호 관리 프레임워크 (ISO/IEC 27556)과 인공지능의 보안과 프라이버시 모범 사례 (ISO/IEC 27563)가 국제표준으로 최종 공개되었다. 특히 이번 회의에서는 프라이버시 정보 관리를 위한 ISO/IEC 27001과 ISO/IEC 27002 확장 개정 (ISO/IEC DIS 27701)의 개정 초안이 DIS 상태로 승인되었고, 핀테크 서비스 프라이버시 가이드라인 (ISO/IEC 27562)가 CD2 상태로 승인되는 성과를 거두었다.

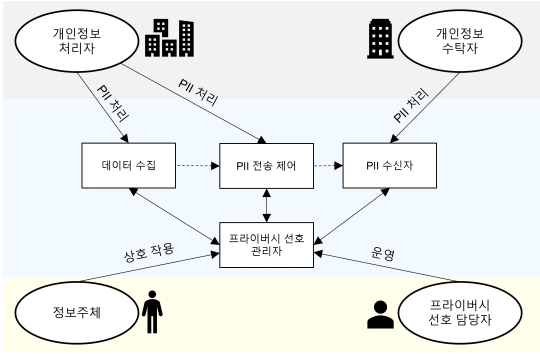
2023년 4월 이후 현재까지 개발 중인 주요 국제 표준을 요약하면 [표 2] 와 같다. 또한 현재 신규 워크아이템으로 채택되지는 않았지만, 이를 목표로 사전 준비 표준화 활동이 진행 중인 아이템은 [표 3] 과 같다.

다음 절부터는 2022년 10월 이후에 채택되었거나 개발 또는 개정 중인 개인정보보호 관련 주요 국제표준의 세부 내용을 제시한다.

2.2. 이용자 중심 개인정보보호 선호 관리 프레임워크 (ISO/IEC 27556) [12]

이용자 중심 개인정보보호 선호 관리 프레임워크는 2019년 2월 신규 워크 아이템으로 채택되었고, 2022년 10월 국제표준으로 최종 채택되었다. 이 국제표준은 프라이버시 선호에 기반한 이용자 친화적 개인정보 처리 프레임워크를 제시하며 정보주체에 의한 개인정보 기본 설정에 따라 개인정보(PII)를 처리하기 위한 이용자 중심 프레임워크를 제공한다.

[그림 1]은 이용자의 프라이버시 선호에 기반하는 프레임워크의 주요 구성요소를 나타낸다. 데이터 발신지와 데이터 수신자 사이에는 개인정보 전달 제어 기



〔그림 1〕 사용자 선호 관리 프레임워크 구성요소〔12〕

능이 존재한다. 데이터 발신지에서 수집된 데이터는 필요에 따라서 데이터 비식별화나 데이터 삭제가 수행되고, 개인정보 전달 제어 기능은 사용자 선호 관리자의 통제하에 개인정보의 전달 여부를 결정한다. 개인정보가 전달되어야 한다고 판단되면 해당 데이터는 다시 변환될 수 있으며, 그 결과가 데이터 수신자에게 제공된다.

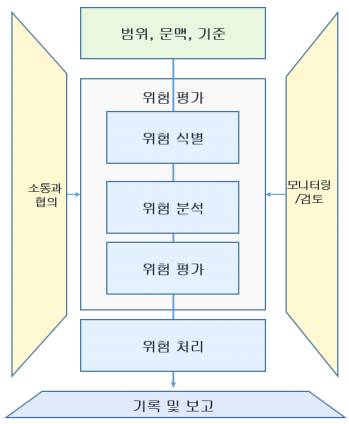
이 국제표준은 개인정보 주체, 개인정보처리자, 개인정보 수탁자, 프라이버시 선호 관리자 등으로 구성된 주요 참여 주체를 정의하고, 데이터 수집, 비식별화, 개인정보 제공 등으로 구성된 주요 구성요소를 제시한다. 또한 프라이버시 참조 관리의 역할을 정의하고 있다. 필자는 이 표준의 프로젝트 리더로 참여하였다.

2.3. 조직 프라이버시 위험관리 (ISO/IEC 27557) [14]

이 국제표준은 2020년 1월에 신규 워크 아이템으로 채택되었으며, 2022년 8월부터 FDIS 투표 단계를 거쳐 지난해 11월에 최종 국제표준으로 승인되었다.

ISO/IEC 31000 [26]은 [그림 2]와 같이 조직이 직면한 위험관리에 대한 지침, 프레임워크 및 위험관리 프로세스, 원칙을 제공하며, 이는 조직의 위험관리를 위한 소통과 협의, 범위/문맥/기준, 위험 식별/분석 등으로 구성되는 위험 평가, 모니터링/검토, 그리고 기록과 보고 프로세스로 구성된다.

조직 프라이버시 위험관리 국제표준은 ISO 31000: 2018 에서 정의한 일반적인 위험관리를 기반으로 조직이 충족해야 할 개인정보보호 위험관리 요구사항을



〔그림 2〕 ISO/IEC 31000 위험 관리 프로세스〔26〕

추가해 조직의 개인정보 위험관리에 대한 확장된 지침을 제공하였다.

2.4. 개인정보보호 관리체계 인증 및 심사기관 요구사항(ISO/IEC DIS 27006-2)[16]

이 국제표준은 2019년 10월 신규 워크 아이템으로 채택되었으며, 2021년 4월 TS로 국제표준으로 채택되었다. 다시 개정안을 마련하기 위해 2023년 7월 DIS 상태에 있다.

이 국제표준은 개인정보 관리체계를 운영하는 신청기관에 대한 심사기관과 인증기관을 위한 평가 및 인증에 대한 요구사항을 지정한다. 또한 ISO/IEC 27006-1 에 포함된 요구사항 외에도 ISO/IEC 27001 과 결합한 ISO/IEC 27701 에 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.

2.5. 동의 레코드 정보 구조 (ISO/IEC TS 27560)[17]

이 국제표준은 2020년 4월 회의에서 신규 워크 아이템으로 채택되었고, 2023년 4월 TS로 채택되었다. 이 국제표준은 개인정보 처리에 대한 동의를 기록하기 위해 상호운용이 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

2.6. 프라이버시 운용 모델 및 엔지니어링 방법(ISO/IEC DIS 27561)[18]

이 국제표준은 2021년 1월 신규 워크 아이템으로 채택되어, 2023년 7월부터 DIS 상태에 있다. 이 국제표준은 개인정보보호 원칙을 일련의 통제 및 기능적 능력으로 운용하기 위한 모델과 방법을 제시한다. 운

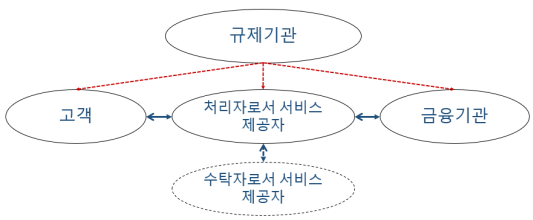
용 방법은 ISO/IEC/IEEE 24774 에 따른 프로세스와 ISO/IEC 29100에 나타난 보호 원칙을 기반으로 한다. 개인정보를 제어하거나 처리하는 시스템을 개발하는 엔지니어 및 기타 실무자를 위한 표준이다. 다른 표준 및 개인정보보호 지침과 함께 사용하도록 설계된다. 네트워크로 연결된 상호 의존적인 응용 프로그램 및 시스템을 지원한다.

2.7. 핀테크 서비스 프라이버시 가이드라인 (ISO/IEC CD2 27562)[19]

이 국제표준은 우리나라의 제안으로 2021년 1월 신규 워크 아이템으로 채택되어, 2023년 7월 28일 CD2 투표가 완료되었다.

이 국제표준은 핀테크 서비스에 대한 개인정보보호 지침을 제공하고 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 개인정보 통제를 제공한다. 또한 이 국제표준은 ISO/IEC 29100, ISO/IEC 27701 및 ISO/IEC 29184에 설명된 개인정보보호 원칙과 ISO/IEC 29134 및 ISO 31000 에 설명된 개인정보 영향평가 프레임워크를 기반으로 한다. 필자는 이 국제표준의 프로젝트 리더를 맡고 있다.

이 국제표준의 주요 이해당사자는 [그림 3]과 같다. 규제기관은 핀테크 서비스를 규제하는 기관이며, 고객은 정보주체로, 개인정보처리자로서의 핀테크 서비스 제공자, 수탁자로서의 서비스 제공자, 그리고 기존 금융 기관으로 구성된다. 이 국제표준은 각 이해당사자의 통제를 개발하는 것이다.



〔그림 3〕 핀테크 서비스를 위한 주요 이해당사자〔19〕

2.8. 인공지능의 보안과 프라이버시 모범 사례(ISO/IEC TR 27563)[13]

이 국제표준은 2021년 11월 CD 상태로 등록되었으며, 2023년 5월 TR로 최종 채택되었다. 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 제시한다. 특히 이 국제표준의 부록에는 120개의 이용 사례에 대한 보안 및 프라이버시 위험과 이 위험을 완화할 수 있는 통제를 제공하고 있다. 필자는 이 국제표준의 프로젝트 리더로 참여하였다.

2.9. 영지식 증명 이용 가이드라인 (ISO/IEC WD3 27565)[20]

영지식 증명 이용 가이드라인은 2021년 11월에 신규 워크 아이템으로 채택되었고, 현재 WD3 상태에 있다. 이 국제표준은 공유되는 정보를 최소화하여 조직과 이용자 간의 개인 데이터 공유 또는 전송과 관련된 위험을 줄임으로써 개인정보 보호를 개선하기 위해 영지식증명 (ZKP)을 사용하는 방법에 대한 지침을 제공한다. 또한 다양한 비즈니스 사용 사례와 관련된 몇 가지 영지식증명 기능 요구사항이 포함되어 있으며, 이러한 기능 요구사항을 안전하게 충족하기 위해 다양한 영지식증명 모델을 사용할 수 있는 방법을 설명한다.

2.10. 개인정보 관리체계와 관련된 요구사항 및 지침 (ISO/IEC DIS 27701)[8]

이 국제표준은 조직이 개인정보 관리를 위해 ISO/IEC 27001 및 ISO/IEC 27002 를 확장한 형태로 개인정보 관리 시스템 (PIMS) 을 수립, 구현, 유지 관리 및 지속적으로 개선하기 위한 요구사항과 지침을 제공한다. 또한 PIMS 관련 요구사항과 PII 처리에 대한 책임과 의무를 지닌 PII 컨트롤러 및 PII 처리자를 위한 지침을 제시한다.

2016년 7월에 신규 워크 아이템으로 채택되었으며, 2019년 8월 국제표준으로 최종 채택되었다. 2023년 1월에는 DIS 상태로 등록되어 최소한의 개정을 시작하였다. FDIS 등록을 목표로 하였으나 이 국제표준의 내용과 범위 (Scope) 에 대한 추가적 보완이 요구되었기

때문에 DIS로 등록되었다. 2023년 10월 회의에서 이 국제표준에 대한 최종 수정 방향이 결정될 것으로 예상된다. 필자는 이 국제표준의 프로젝트 리더로 참여 중이다.

2.11. 연령 보증 (ISO/IEC WD 27566)[35]

연령 보증 국제표준 (ISO/IEC WD 27566) 은 2022년 10월 신규 워크 아이템으로 채택되어, 현재 WD2 상태에 있다. 이 국제표준은 연령 또는 자연인의 연령대에 대한 신뢰성 지표에 기반한 프레임워크를 설정한다. 연령에 따른 적격성 결정을 가능하게 하기 위한 목적으로 개인정보보호를 포함한 핵심 원칙을 수립한다.

Ⅲ. 결 론

본 고에서는 지난 2022년 10월 이후부터 2023년 4월 회의에서 수행된 개인정보보호 분야의 활동 결과를 중심으로 SC 27/WG 5에서 개발되었거나 개발 중인 주요 국제표준의 내용을 분석하고 제시하였다. 개인정보보호 제도나 관행은 국제표준에 근거해 시행되어야 글로벌 차원의 상호연동성을 보장받는다. 우리나라는 향후 개인정보보호 분야의 신흥 표준화 주제인 인공지능, 디지털 트윈, 핀테크 보안 등의 개인정보보호 분야에 집중하여 국제표준화 활동을 추진할 필요가 있다.

본 고는 우리나라가 개인정보보호 관련 국제표준화를 추진하고, 이와 관련된 국제 표준화 리더쉽을 확보하기 위한 참고 자료로 활용될 수 있다.

참 고 문 헌

[1] 법제처, 개인정보보호법

[2] EU, GDPR (general data protection regulation), 27 April 2016

[3] ISO/IEC JTC 1/SC 27, Information security, cybersecurity, privacy protection, http://www.iso.org/iso/iso_technical_committee?commid=45306

[4] ISO/IEC 29100:2011, Information technology – Security techniques – Privacy framework

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

[6] ISO/IEC 29151:2017, Code of practice for the protection of personally identifiable information, 2017.8

[7] ISO/IEC 27018:2014, Code of practice for protection of personally identifiable information (PII) in public clouds acting as PIII processors

[8] ISO/IEC DIS 27701, Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines

[9] ISO/IEC 29184, Guidelines for online privacy notices and consent, 2019.07

[10] ISO/IEC 27555, Guidelines on personally identifiable information deletion, 2021.10

[11] ISO/IEC TS 27570, Privacy guidelines for smart cities, January 2021

[12] ISO/IEC 27556, User-centric privacy preferences management framework

[13] ISO/IEC TR 27563, Security and privacy in artificial intelligence use cases – Best practices

[14] ISO/IEC 27557, Application of ISO 31000:2018 for organizational privacy risk management

[15] ISO/IEC 27559, Privacy enhancing data de-identification framework

[16] ISO/IEC 27006-2, Requirements for bodies providing audit and certification of information security management systems -- Part 2: Privacy Information Management Systems

[17] ISO/IEC TS 27560, Consent record information structure

[18] ISO/IEC DIS 27561, Privacy operationalisation model and method for engineering (POMME)

[19] ISO/IEC CD2 27562, Privacy guidelines for fintech services

[20] ISO/IEC WD3 27565, Guidelines on privacy preservation based on zero knowledge proofs

[21] 염흥열, 국제 개인정보보호 표준화 동향 분석 (2017년 4월 해밀턴 SC27 회의 결과를 중심으로)), 한국정보보호학회 학회지, 제27권 제5호, pp.6-11, 2017.10

[22] 염흥열, 국제 개인정보보호 표준화 동향 분석 (2019년 4월 이스라엘 텔아비브 SC27 회의 결과를 중심으로)), 한국정보보호학회 학회지, 제29권 제4

호, 2019.08
[23] 염흥열, 국제 개인정보보호 표준화 동향 분석 (2020년 4월 전자 회의 결과를 중심으로), 한국정보보호학회 학회지, 제30권 제4호, 2020.08
[24] 염흥열, 국제 개인정보보호 표준화 동향 분석 (2022년 4월 전자 회의 결과를 중심으로), 한국정보보호학회 학회지, 제32권 제4호, 2022.08
[25] ISO/IEC JTC 1/SC 27, Information security, cybersecurity, privacy protection, http://www.iso.org/iso/iso_technical_committee?commid=45306
[26] ISO 31000:2018, Risk management
[27] ISO-IEC JTC 1-SC 27-WG 5_N3701_WG 5 SD1 Roadmap, 2023.6.14.
[28] ISO/IEC JTC 1/SC 27/WG 5 N 3693 Call for comments on SC 27/WG 5 Standing Document 2 (WG 5 SD2) - Privacy references list, 2023.8.31.
[29] ISO/IEC 29190:2015, Privacy capability assessment model
[30] ISO/IEC 20889:2018, Privacy enhancing data de-identification terminology and classification of techniques
[31] ISO/IEC TS 29003:2018, Identity proofing
[32] ISO/IEC PWI 8887, Authority on identity information quality and related architecture description
[33] ISO/IEC PWI 6087, Digital authentication: Risks and mitigations
[34] ISO/IEC PWI 27568, Security and privacy of digital twins
[35] ISO/IEC WD 27566, Age verification

〈저 자 소 개〉

박 성 채 (Sungchae PARK)
증신회원
순천향대학교 정보보호학과 학사 졸업
순천향대학교 대학원 정보보호학과 석·박사 과정
2007년 10월~2009년 5월 : 어울림정보기술(주) 연구원
2010년 1월~2011년 5월 : 이글루시큐리티 주임연구원
2020년 2월~2022년 4월 : ㈜보다비 AI연구소 리더
2022년 5월~현재 : 순천향대학교 차세대보안 표준전문 연구실 선임연구원
<관심분야> AI 보안, 암호, 양자암호통신, 블록체인 보안, 5G/6G 보안, 개인정보보호 기술

염 흥 열 (Heung Youl YOUM)
증신회원
한양대학교 전자공학과 학사 졸업
한양대학교 대학원 전자공학과 석사 졸업
한양대학교 대학원 전자공학과 박사 졸업

1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 정보보호학과 정교수
2011년 1월~12월 : 한국정보보호학회 회장(역), 명예회장(현)
2009년~2016년 : ITU-T SG17 부의장
2009년~2016년 : ITU-T SG17 WP3 의장
2017년~현재 : ITU-T SG17 의장
2019년 8월~현재 : 분산신원관리 기술 및 표준화 포럼 의장
2020년 8월 5일~2023년 8월 4일 : 개인정보보호위원회 위원 (역)
<관심분야> 정보보호관리체계, 개인정보보호, IoT 보안, 네트워크 보안, 암호 프로토콜, 인공지능 보안과 프라이버시. 블록체인 보안, 5G/6G 보안