정 보 보 호 학 회 지
제34권 제4호, 2024. 8

국제 개인정보보호 표준화 동향 분석
(2024년 4월 SC27 WG5 회의 결과를 중심으로)

박 성 채*, 박 준 형**, 염 흥 열***

요 약

최근 생성형 인공지능, 메타버스 기반의 신규 ICT 서비스가 도입되면서 이러한 서비스에서 발생할 수 있는 프라이버시 위험의 적절한 관리는 매우 중요하게 부각되고 있다. 특히 챗GPT를 시작으로 한 생성형 인공지능의 급격한 발전과 활용은 데이터 수집, 처리, 분석 과정에서 개인정보보호에 대한 우려를 가중시킨다. 이와 관련하여 개인정보보호 국제표준은 국가나 조직의 관행과 기술을 글로벌 차원의 표준으로 개발하여 상호 연동이 가능한 서비스를 제공함으로써, 제품이나 서비스의 경쟁력을 강화 하는데 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 괴테대학의 카이 라넨버그(Kai Rannenberg) 교수가 이 그룹의 의장을 맡고 있다. 본 고에서는 2024년 4월 SC 27/WG 5 회의를 중심으로 개발 및 채택된 개인정보보호 국제표준과 동향을 살펴보고, 이와 관련된 주요 이슈와 표준화 대응 방안을 제시한다.

Ⅰ. 서 론

개인정보보호 관리체계(privacy information magngement system)란 개인 식별 정보(PII)를 처리하는 과정에서 잠재적으로 영향을 주는 개인정보 보호를 다루는 관리체계를 의미한다[1]. 뿐만아니라 모든 금융 서비스가 디지털화 되면서 정보기술과 금융 서비스의 결합인 핀테크 서비스에서의 정보주체의 개인정보 자기결정권과 관련 대책이 매우 중요하게 대두되고 있다. 또한 챗GPT 등 생성형 인공지능의 등장은 개인정보보호 분야에 새로운 과제를 제시하였다. 생성형 인공지능은 학습된 데이터를 기반으로 텍스트, 이미지, 비디오 등의 새로운 콘텐츠를 생성하는 인공지능의 한 유형으로 학습 데이터 내 개인정보 포함 문제, 생성 콘텐츠 내 개인정보 유·노출 문제 등의 프라이버시 이슈를 야기하고 있으며, 각국 정부와 국제 기구들은 이러한 문제를 해결하기 위해 관련 법령과 모범사례와 가이드라인 등을 제정하고 있다. 우리나라 개인정보보호위원회는 인공지능의 시대에 안전 장치를 마련하기 위해 개인정보보호법을 개정하였으며[2], 유럽연합(EU)의 개인정보보호 규정 (General Data Protection Regulation, GDPR) 역시 비슷한 양상을 보이고 있다[3].

ISO/IEC JTC 1/SC 27/WG 5 [4]는 개인정보보호와 관련된 국제표준을 개발하고 있는 표준화 그룹이다. 본 고는 [5], [6], [7], [8] 논문을 현행화한 논문이며, [8]은 2023년 하반기와 2024년 상반기 WG5에서 수행된 표준화 활동을 반영한 논문이다.

본 고의 내용은 [8]을 기반으로 업데이트했으므로, 독자의 편의와 본 논문의 완전성을 위해 많은 부분을 인용했음을 미리 알린다.

본 고의 2장에서는 ISO/IEC JTC 1/SC 27/WG 5에서 개발한 국제표준과 2023년 10월 회의 이후 2024년 4월 SC 27/WG 5 회의에서 채택한 신규 국제표준을 포함하여 현재 개발 중인 주요 개인정보보호 관련 국제표준의 현황과 내용을 살펴본다. 3장에서는 결론을 맺는다.

“이 논문은 2024년도 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 (대학원생, junhyung.park@sch.ac.kr)
*** 순천향대학교 정보보호학과 (교수, hyyoum@sch.ac.kr)

Ⅱ. SC 27/WG 5 개인정보보호 표준화 동향

2.1. 개인정보보호 관련 국제표준화 현황 개요

이 그룹에서는 [표 1]과 같이 프라이버시 프레임워크 (ISO/IEC 29100) [9], 프라이버시 영향평가 (ISO/IEC 29134) [10], 개인정보보호 준칙(ISO/IEC 29151) [11], 개인정보 수탁자로서 퍼블릭 클라우드에서 개인정보보호 준칙 (ISO/IEC 27018) [12], 개인정보관리체계 요구사항 및 지침 (ISO/IEC 27701) [13], 사용자 친화 온라인 고지 및 동의 (ISO/IEC 29184) [14], 개인정보 삭제 프레임워크 (ISO/IEC 27555) [15], 스마트시티 프라이버시 가이드라인 (ISO/IEC TS 27570) [16] 개발을 완료했고, 국내 마이데이터 서비스와 긴밀하게 연관된 사용자 중심 프라이버시 선호 관리 프레임워크 (ISO/IEC 27556) [17] 와 인공지능 이용 사례에서 보안과 프라이버시(ISO/IEC TR 27563) [18], 조직 프라이버시 리스크관리 (ISO/IEC

〔표 1〕 SC 27/WG 5에서 개발된 개인정보보호 분야 국제표준 (〔8〕 업데이트)

	표준 번호 및 제목	주요 내용	문서 상태	프로젝트 리더 (한국 볼드)
ISO/IEC JTC 1/ SC 27/ WG 5	▪ ISO/IEC 29100:2011, 프라이버시 프레임워크 [9]	▪ 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 (2014.8)	C. Mitchell(UK) / Chandramouli Ramaswamy(US), Hendrik Decroos(BE)
	▪ ISO/IEC 29134:2017, 개인정보 영향평가 가이드라인 [10]	▪ 개인정보영향평가(privacy impact assessment)를 위한 과정과 개인정보 영향평가 보고서의 구조와 내용에 대한 가이드라인을 제공한다.	IS (2017.06)	Mathias Reinis(GE), **Heung Youl Youm (KR)** / Okuma Mieko(JP)
	▪ ISO/IEC29151:2017, 개인정보보호 지침 [11]	▪ 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 (2017.04)	**Heung Youl Youm (KR),** Alan Shipman(UK) / **Heung Youl Youm (KR),** Alan Shipman(UK), Erik Boucher(FR), **Sungchae Park(KR)**
	▪ ISO/IEC 29190:2015, 개인정보보호 능력 평가 모델 [31]	▪ 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 [32]	▪ 다양한 데이터 비식별화 기술, 주요 용어 정의, 그리고 비식별화 기법의 유형을 제시한다.	IS (2017.11)	Mitchell Chris(UK), Lionel Vodzislawsky
	▪ ISO/IEC TS 29003:2018, 온라인 신원증명 (identity proofing) [33]	▪ 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 [13]	▪ 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), **Heung Youl Youm (KR)** etc
	▪ ISO/IEC 29184:2020, 사용자 친화 고지 및 통보 [14]	▪ 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 [15]	▪ 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)**

	표준 번호 및 제목	주요 내용	문서 상태	프로젝트 리더 (한국 볼드)
ISO/IEC JTC 1/ SC 27/ WG 5	▪ ISO/IEC 27556, 이용자 중심 프라이버시 선호 관리 프레임워크 [17]	▪ 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 [19]	▪ 조직의 개인정보 위험 관리 지침을 제공한다.	IS (2022.11)	Gierschmann Markus, HARPES Carlo, Lucy Kimberly(US), Magtalas Kelvin
	▪ ISO/IEC 27559, 프라이버시 강화 데이터 비식별화 프레임워크 [20]	▪ 비식별화된 데이터의 수명 주기와 관련된 위험과 재 식별 위험을 찾고 완화하기 위한 프레임워크를 제공한다.	IS (2022.11)	Townsend Malcolm(CA), Borel Santa
	▪ ISO/IEC TS 27560, 동의 레코드 정보 구조[22]	▪ 데이터 주체의 데이터 처리 동의를 기록하기 위해 상호 운용 가능하고 개방적이며 확장 가능한 정보 구조를 정의한다.	TS (2023.08)	Hughes Andrew, Lindquist Jan
	▪ ISO/IEC TR 27563, 인공지능 이용 사례에서 보안과 프라이버시 [18]	▪ 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 (2023.05)	Antonio Kung(FR), **Youm Heung Youl(KR)**, etc
	▪ ISO/IEC 27561, 프라이버시 운용 모델 및 엔지니어링 방법 [24]	▪ 개인정보 보호 원칙을 일련의 통제 및 기능적 기능으로 운용하는 모델과 방법을 설명한다.	IS (2024.03)	de Marco Dorotea Alessandra(IT), Kung Antonio(FR), Poosarla Srinivas(IN), etc.
	▪ ISO/IEC 29115:2013 , 객체 인증 보증을 관리하기 위한 프레임워크[34]	▪ 사용자나 시스템 등 개체의 인증 보증 수준을 관리하기 위한 프레임워크를 제공한다. 또한 네 가지 수준의 개체 인증 보증 레벨을 정의하고, 각 레벨을 달성하기 위한 기준과 가이드라인을 명시하며, 다른 인증 보증 체계를 이 네 가지 수준에 매핑하는 방법과 인증 결과를 교환하는 방법, 위협을 완화하기 위한 통제를 제시한다.	IS (2013.03)	**Heung Youl Youm(KR)**, Christophe Stenuit(BE), Eduard De Jong(FR), Janssen Esguerra(PH), etc.

27557) [19], 프라이버시 개선 데이터 비식별화 프레임워크(ISO/IEC 27559) [20], 개인정보보호 관리체계의 인증 및 심사 기관 요구사항 (ISO/IEC 27006-2) [21], 동의 레코드 정보 구조 (ISO/IEC 27560) [22] 등도 국제표준으로 개발하였다. 특히 개인정보관리체계 요구사항 및 지침 (ISO/IEC 27701)의 내용이 개정되고 있음에 따라서 이와 관련된 개인정보보호 관리체계의 인증 및 심사 기관 요구사항(ISO/IEC 27006-2) 국제표준도 ISO/IEC 27706으로 새로운 번호가 부여됐으며, 2025년 1월 국제표준 최종 배포를 목표로 한다[23]. 2024년 3월에는 프라이버시 운용 모델 및 엔지니어링 방법 (ISO/IEC 27561)이 국제표준으로 최종 배포되었다[24]. 개인정보보호와 관련된 국제 표준과 관련해 신원 관리 및 프라이버시 작업반(WG5)이 2024년 4월까지 채택한 국제표준은 [표 1]과 같다.

또한 WG5에서는 핀테크 서비스 프라이버시 가이드라인 (ISO/IEC FDIS 27562)[25], 영지식 증명 기반 프라이버시 보존 가이드라인 (ISO/IEC CD 27565.2) [26] 등의 국제표준을 개발하고 있다.

특히 [표 2]와 같이 개인정보관리체계 요구사항 및 지침(ISO/IEC 27706.2) 뿐만아니라, 개인정보 수탁자로서 퍼블릭 클라우드에서 개인정보보호 준칙 (ISO/IEC DIS 27018)[27], 개인정보보호 지침 (ISO/IEC 2CD 29151)[28], 객체 인증 보증을 관리하기 위한 프레임워크 (ISO/IEC WD 29115)[29]도 개정 합의에 성공했다. 개인정보보호 지침(ISO/IEC 2CD 29151)는 ITU-T SG17과 공동으로 개발하는 국제표준이며, 객체 인증 보증 관리 프레임워크(ISO/IEC WD 29115)는 개정 합의에 따라 사전 표준화 활동 아이템(PWI)에서 WD로 진입하는데 성공했다. 이 두 표준 모두 한국이 주도로 개발 중인 국제표준이다. 2024년 4월 이후 현재까지 개발 중인 주요 국제 표준을 요약하면 [표 2]와 같다. 또한 현재 신규 워크 아이템 채택을 목표로 사전 준비 표준화 활동(PWI)이 진행 중인 아이템은 [표 3]과 같다.

〔표 2〕 SC 27/WG 5에서 개발 또는 개정 중인 주요 국제 표준 요약 (2024년 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 DIS 27018, 개인정보 수탁자로서 퍼블릭 클라우드에서 개인정보보호 준칙 [27]	▪ 공공 클라우드 환경에서 개인정보를 보호하기 위한 통제, 통제 목표, 통제 구현 가이드라인을 제시한다. 이 문서는 ISO/IEC 27002에 근거한다.	DIS (개정중)	2024.12	Chandramouli Ramaswamy(US), Hendrik Decroos(BE)
	▪ ISO/IEC 2CD 29151, 개인정보보호 지침 (개정) [28]	▪ 개인정보보호와 관련된 위험 평가 결과에 의해 식별된 요구사항을 만족하기 위한 통제와 구현 가이드라인 등을 제시한다. 이 국제표준은 2023년 10월 회의에서 CD 상태로 개정하기로 합의했으며, 2024년 4월 회의에서 2CD 진입에 성공했다.	2CD (개정중)	**2024.10**	**Heung Youl Youm (KR),** Alan Shipman(UK), Erik Boucher(FR), **Sungchae Park(KR)**
	▪ ISO/IEC 2DIS 27701, 개인정보보호 관리체계 – 요구사항 및 지침 [1]	▪ 개인정보보호 관리체계 – 요구사항 및 가이던스를 제공한다. 이 국제표준은 2022년 10월 회의에서 DIS 상태에서 개정하기로 합의했으며, 개인정보보호 관리체계 – 요구사항 및 가이던스로 타이틀을 변경하였다.	2DIS (개정중)	2025.10	Shipman Alan(UK), **Heung Youl Youm (KR),** etc
	▪ ISO/IEC WD 29115, 객체 인증 보증 프레임워크 [29]	▪ 사용자나 시스템 등 개체의 인증 보증 수준을 관리하기 위한 프레임워크를 제공한다. 또한 네 가지 수준의 개체 인증 보증 레벨을 정의하고, 각 레벨을 달성하기 위한 기준과 가이드라인을 명시하며, 다른 인증 보증 체계를 이 네 가지 수준에 매핑하는 방법과 인증 결과를 교환하는 방법, 위협을 완화하기 위한 통제를 제시한다. 2024년 4월 회의에서, 인증 위협과 이에 대한 통제사항, 보증레벨 기준, 관련 용어에 대한 명확한 기준을 제시함으로써 개정 합의되었다.	WD (개정중)	2027.06	**Heung Youl Youm(KR)**, Christophe Stenuit(BE), Eduard De Jong(FR), Janssen Esguerra(PH), etc.
	▪ ISO/IEC DIS 27706-2, 개인정보보호 파리시스템의 감사 및 인증을 제공하는 기관에 대한 요구사항[23]	▪ 조직의 개인정보 관리체계 (PIMS)를 심사 및 인증을 제공하는 기관에 대한 요구사항을 지정하고 지침을 제공한다. 주로 PIMS 인증을 제공하는 인증 기관의 구현 및 운영을 지원하기 위한 것이다.	DIS	2024.12	Azetsu Fuki, Lucy Kimberly, Robinson Gigi
	▪ ISO/IEC FDIS 27562, 핀테크 서비스 프라이버시 가이드라인 [25]	▪ 핀테크에서 프라이버시 가이드라인을 제공한다.	FDIS	2024.7	**Youm Heung Youl (KR)**, Janssen Esguerra(PH)
	▪ ISO/IEC 2CD 27565, 영지식 증명 기반 프라이버시 보존 가이드라인 [26]	▪ 영지식 증명 기술 이용을 위한 가이드라인을 제공한다.	2CD	2025.10	Curry Patrick(UK), Poosarla Srinivas(IN), zhang bingsheng(CH)
	▪ ISO/IEC CD 27566-1, 연령 보증 시스템-프레임워크 [35]	▪ 연령 보증 시스템의 프레임워크, 보증 수준 및 개인정보보에 대한 정보를 제공한다. 연령 관련 자격 결정을 가능하게 하기 위한 목적으로 개인 정보 보호 및 보안을 포함한 핵심 원칙을 제공한다.	CD	2025.11	Tony Allen (GB), Denis PINKAS(FR), Mark SBANCAREK (US)
	▪ ISO/IEC NP 27566-2. 연령 보증 시스템 – 구현을 위한 기술적 접근 및 가이드라인 [36]	▪ 연령 보증 시스템을 위한 다양한 생태계에 적합한 다양한 기술적 접근 방식과 구현 지침을 제공한다.	NP	2027.7	Tony Allen (GB), Denis PINKAS(FR), Mark SBANCAREK (US)
	▪ ISO/IEC WD 27566-3.2, 연령 보증 시스템 – 벤치마킹 분석을 위한 벤치마크 [37]	▪ 연령 보증 방법 및 구성 요소의 특성을 지정, 차별화 및 비교하기 위한 벤치마크를 제공한다.	WD	2026.10	Tony Allen (GB), Denis PINKAS(FR), Mark SBANCAREK (US)

〔표 3〕 SC 27/WG 5에서 사전 표준화 활동 아이템(PWI) (2024년 7월 현재)

	표준 번호 및 제목	주요 내용	문서 상태	프로젝트 리더(한국 볼드)
ISO/IEC JTC 1/SC 27/WG 5	▪ PWI 27569 개인정보 처리 기록 정보 구조 [38]	▪ 개인 식별 정보(PII) 처리 기록 정보 구조를 제공한다.	PWI	Jan LINDQUIST(SE)
	▪ PWI 27573 메타버스에서 사용자 아바타와 시스템 아바타 상호작용의 개인정보보호 [39]	▪ 메타버스에서 사용자 아바타와 시스템 아바타 간의 상호 작용 중에 개인정보를 보호하기 위한 프레임워크를 제공한다.	PWI	**Hoon Jae LEE(KR), Hee Bong CHOI(KR)**, Rusne JUOZAPAITIENE(LT), Dae-KI KANG(KR), Vishnu KANHERE(IN), Antonio KUNG(FR)

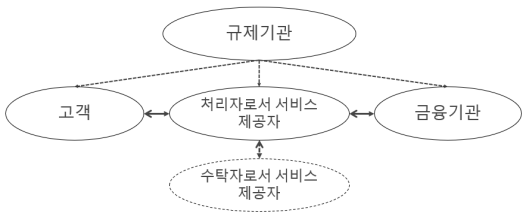
다음 절부터는 2024년 4월 이후에 채택되었거나 개발 또는 개정 중인 개인정보보호 관련 주요 국제표준 중에서 대표적인 국제표준의 세부 내용을 제공한다.

2.2. 핀테크 서비스 프라이버시 가이드라인 (ISO/IEC FDIS 27562) [25]

이 국제표준은 우리나라의 제안으로 2021년 1월 신규 워크 아이템으로 채택되어, 2024년 4월 11일 DIS 투표가 완료되었다.

이 국제표준은 핀테크 서비스에 대한 개인정보보호 지침을 제공한다. 특히 핀터크 서비스를 위한 주요 주체를 식별하고, 각각의 역할을 정의하며, 각 주체에 대한 위험을 제시한다. 이 위험을 경감하기 위한 프라이버시 보호 대책을 제공한다. 이 국제표준은 ISO/IEC 29100, ISO/IEC 27701 및 ISO/IEC 29184에 설명된 개인정보보호 원칙과 ISO/IEC 29134 및 ISO 31000에 설명된 개인정보 영향평가 프레임워크를 기반으로 한다. 필자(염흥열 교수)는 이 국제표준의 프로젝트 리더를 맡고 있다.

이 국제표준의 주요 이해당사자는 [그림 1]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 1〕 핀테크 서비스를 위한 주요 이해당사자〔25〕

2.3. 개인정보 관리체계 - 요구사항 및 지침 (개정안) (ISO/IEC DIS 27701) [1]

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 이 표준의 기반 표준인 ISO/IEC 27002가 2022년에 개정됨에 따라서 DIS 상태로 시작해서 개정 작업을 시작하였다. FDIS 등록을 목표로 하였으나 이 국제표준의 내용과 범위 (Scope) 에 대한 추가적 보완이 요구되었기 때문에 DIS로 등록되었다. 2024년 4월 회의에서는 “ISO/IEC 27001 및 ISO/IEC 27002의 확장”을 제목과 범위에서 삭제하였다. 또한, IS 목표 시기를 2024년 11월로 연장하였다. 2024년 10월 회의에서 이 국제표준에 대한 최종 수정 방향이 결정될 것으로 예상된다. 필자(염흥열 교수)는 이 국제표준의 프로젝트 리더로 참여 중이다.

2.4. 개인정보 수탁자로서 퍼블릭 클라우드에서 개인정보보호 준칙 (개정안) (ISO/IEC DIS 27018) [27]

이 국제표준은 퍼블릭 클라우드 컴퓨팅 환경에서 개인 식별 정보(PII)를 보호하기 위한 일반적인 통제, 통제 방법 및 지침을 제시한다. 또한 ISO/IEC 29100에서 제시하는 개인정보 보호 원칙을 준수하며, ISO/IEC 27002를 기반으로 PII 보호와 관련된 규제 요구 사항을 고려하여 개발되었다.

특히, 이 지침은 퍼블릭 클라우드 서비스 제공자의 정보 보안 위험 환경에서 적용될 수 있는 요구사항을 반영하며, 공공 및 민간 기업, 정부 기관, 비영리 단체 등 다양한 조직에 적용될 수 있다. 이러한 조직들은 클라우드 컴퓨팅을 통해 다른 조직을 대신하여 PII를 처리하는 역할을 수행하는 경우 이 문서의 지침을 따를 수 있다. 또한, 이 표준은 PII 처리자뿐만 아니라 PII 통제자 역할을 하는 조직에도 유의미한 지침을 제공할 수 있으며, 퍼블릭 클라우드 환경에서 PII 보호를 위한 체계적이고 포괄적인 지침을 제공한다.

기존의 문서에서 몇 가지 통제 항목을 추가하는 것을 제안함으로써 2023년 10월 회의에서 ISO/IEC 27002가 2002년에 개정됨에 따라 DIS 상태로 개정을 합의하고 2024년 4월 IS를 목표로 했으나, DIS에 대한 투표가 지연됨에 따라 IS 배포가 2024년 12월로

미뤄졌다.

2.5. 개인정보보호 준칙 (개정안) (ISO/IEC CD 29151|ITU-T X.1058) [28]

개인정보보호 준칙은 2017년에 국제표준은 양대 공적 표준화 기구인 ISO/IEC JTC 1과 ITU-T(SG17)이 협력하여 제정된 공동 국제표준으로, 개인정보 보호와 관련된 위험 평가 결과에서 도출된 요구사항을 충족하기 위한 가이드라인을 제공한다. 이 국제표준은 개인정보(PII) 보호와 관련된 위험 및 영향 평가를 통해 도출된 요구 사항을 충족하기 위한 통제 목표와 방법, 및 지침을 제시하며, 특히, 조직의 정보 보안 위험 환경에서 PII 처리 요구 사항을 고려하여 정보보호 통제(ISO/IEC 27002)를 기반으로 한 구체적인 지침을 제공하는 것을 목표로 한다.

이 국제표준의 기반표준인 ISO/IEC 27002가 2022년 개정됨에 따라 2023년 10월 회의에서 CD 상태로 이 표준을 개정하기로 합의했다. 2024년 4월 맨체스터 WG 5 회의에서는 CD2 진입에 성공했으며, 이 회의에는 양 표준화 기구의 전문가들이 참여해 향후 개정 일정과 방향 등을 논의하였다. 이 국제표준의 프로젝트 리더로 필자 (염흥열 교수, 박성채 팀장) 등이 참여하고 있다.

2.6. 객체 인증 보증프레임워크 (개정안) (ISO/IEC WD 29115) [29]

객체 인증 보증을 위한 프레임워크는 2013년 최초 제정된 국제표준으로, 객체 인증 보증을 통해 신원 인증에 대한 신뢰성을 제공하기 위한 프레임워크를 제시한다. 이 프레임워크는 네 가지 인증 보증 수준(Levels of Assurance, LoA)으로 이루어져 있으며, 각 수준을 달성하기 위한 기준과 지침을 설명한다. 또한, 다른 인증 보증 스키마를 이 네 가지 수준에 매핑하는 방법, 해당 수준을 기반으로 한 인증 결과를 교환하는 방법, 그리고 인증 과정에서 발생할 수 있는 위협을 완화하기 위한 통제 방안을 제시하는 것을 목표로 한다. [표 4]는 인증 보증을 위한 네 가지 보증레벨을 설명하고 있다. 2024년 4월 회의에서 이 표준에 대한 개정을 합의했으며 WD 상태에서 개발을 시작하기로 했다. 필자 (순천향대 염흥열 교수)는 이 국제표준 개정의 프로젝트 리더로 참여하고 있다.

〔표 4〕 개체 보증 레벨 〔30〕

LoA	설명	목표	검증방법	처리 방법
낮음	주장 혹은 증언된 신원에 대한 낮은 수준의 신뢰도	컨택스트 내에서의 유일성	자가 주장 또는 자가 증언	Local/ remote
중간	주장 혹은 증언된 신원에 대한 중간 수준의 신뢰도	컨택스트 내에서의 유일성 + 존재성	협력기관의 신원정보를 활용한 신원 확인	Loal/ remote
높음	주장 혹은 증언된 신원에 대한 높은 수준의 신뢰도	컨택스트 내에서의 유일성 + 존재성 + 약한 수준의 연계성	협력기관의 신원정보를 활용한 신원 확인 + 신원 정보 검증	Local/ remote
매우 높음	주장 혹은 증언된 신원에 대한 매우 높은 수준의 신뢰도	컨택스트 내에서의 유일성 + 존재성 + 강한 수준의 연계성	협력기관의 신원정보를 활용한 신원 확인 + 신원 정보 검증 + 실체에 대한 대면 목격	Local

2.7. 영지식 증명 기 반 프라이버시 보존 가이드라인 (ISO/IEC CD 27565) [26]

영지식 증명 이용 가이드라인은 2021년 11월에 신규 워크 아이템으로 채택되었고, 현재 CD 상태에 있으며 2025년 12월 IS 배포를 목표로 한다. 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.

2.8. 연령 보증 시스템 (ISO/IEC 27566)[35][36][37]

연령 보증 국제표준 (ISO/IEC 27566) 은 2022년 10월 신규 워크 아이템으로 채택되어, 현재 파트 1 [35], 파트 2 [36], 파트 3 [37]이 개발중이다.

파트 1은 연령 관련 자격 결정을 가능하게 하기 위한 목적으로 개인정보 보호 및 보안을 포함한 핵심 원칙을 수립하는 것을 목적으로 하며, 현재 CD 상태에 있다. 파트 2는 신규 프로젝트(NP) 투표가 진행중이

며, 연령 보장 시스템을 위한 다양한 에코시스템에 적합한 다양한 기술적 접근 방식과 이를 구현하기 위한 지침을 제공한다. 파트 3은 현재 2WD 상태에 진입했으며, 특정 연령 확인 방법과 구성 요소의 특성을 정의하고, 구분하며, 비교하기 위한 기준을 제시함으로써 령 확인 방법이 어떤 기준에 따라 설정되고, 서로 어떻게 다른지 구별할 수 있으며, 그 특성을 비교할 수 있는 지침을 제공하고자 한다.

Ⅲ. 결 론

본 고에서는 지난 2023년 10월 이후부터 2024년 4월 회의에서 수행된 개인정보보호 분야의 활동 결과를 중심으로 SC 27/WG 5에서 개발되었거나 개발 중인 주요 국제표준의 내용을 분석하고 살펴보았다.

개인정보보호 국제표준은 서비스나 제품의 경쟁력 강화를 위해 매우 중요하다. 향후에도 우리나라가 이러한 국제표준 개발에 적극적으로 참여하고 이를 주도할 필요가 있다.

참 고 문 헌

[1] ISO/IEC DIS 27701.2, Information security, cybersecurity and privacy protection − Privacy information management systems − Requirements and guidance

[2] 개인정보보호위원회, 인공지능(AI) 시대, 개인정보 안전장치 시행된다, 2024.03.06., https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=9969

[3] James Clark, Muhammed Demircan, Kalyna Kettas, Europe: The EU AI Act’s relationship with data protection law: key takeaways, Privacy Matters DLA Piper's Global Privacy and Data Protection Resource, 2024.04.25. https://privacymatters.dlapiper.com/2024/04/europe-the-eu-ai-acts-relationship-with-data-protection-law-key-takeaways/

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

[5] 염흥열, 국제 개인정보보호 표준화 동향 분석 (2019년 4월 이스라엘 텔아비브 SC27 회의 결과를 중심으로), 한국정보보호학회 학회지, 제29권 제4호, 2019.08

[6] 염흥열, 국제 개인정보보호 표준화 동향 분석 (2020년 4월 전자 회의 결과를 중심으로), 한국정보보호학회 학회지, 제30권 제4호, 2020.08

[7] 염흥열, 국제 개인정보보호 표준화 동향 분석 (2022년 4월 전자 회의 결과를 중심으로), 한국정보보호학회 학회지, 제32권 제4호, 2022.08

[8] 박성채, 염흥열, 국제 개인정보보호 표준화 동향 분석 (2023년 4월 ISO/IEC JTC 1/SC 27/WG 5 회의 결과를 중심으로), 한국정보보호학회 학회지, 제33권 제4호, 2023.08

[9] ISO/IEC 29100:2011, Information technology - Security techniques - Privacy framework

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

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

[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 27701:2019, Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines

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

[15] ISO/IEC 27555, Guidelines on personally identifiable information deletion, October 2021

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

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

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

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

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

[21] ISO/IEC 27006-2, Requirements for bodies pro-

viding audit and certification of information security management systems - Part 2: Privacy Information Management Systems
[22] ISO/IEC TS 27560, Consent record information structure
[23] ISO/IEC DIS 27706.2, Requirements for bodies providing audit and certification of privacy information management systems
[24] ISO/IEC 27561, Privacy operationalisation model and method for engineering (POMME)
[25] ISO/IEC FDIS 27562, Privacy guidelines for fintech services
[26] ISO/IEC CD 27565.2, Guidelines on privacy preservation based on zero knowledge proofs
[27] ISO/IEC DIS 27018, Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
[28] ISO/IEC CD 29151.2, Information technology - Security techniques - Code of practice for personally identifiable information protection
[29] ISO/IEC WD 29115, Information technology - Security techniques - Entity authentication assurance framework
[30] 김경한, 유동현, 김수형, 윤봉중, 염흥열, 국내 전자금융 서비스 환경을 위한 ISO/IEC 29115와 ISO/IEC 29003의 갭분석, 한국 인터넷 정보학회, 제16권 제2호, 2015.12
[31] ISO/IEC 29190:2015, Information technology - Security techniques - Privacy capability assessment model
[32] ISO/IEC 20889:2018, Privacy enhancing data de-identification terminology and classification of techniques
[33] ISO/IEC TS 29003:2018, Information technology - Security techniques - Identity proofing
[34] ISO/IEC 29115:2013, Information technology - Security techniques - Entity authentication assurance framework
[35] ISO/IEC CD 27566-1, Information security, cybersecurity and privacy protection - Age assurance systems - Framework - Part 1: Framework
[36] ISO/IEC NP 27566-2, Age assurance systems - Part 2: Technical approaches and guidance for implementation
[37] ISO/IEC WD 27566-3.2, Age assurance systems - Part 3: Benchmarks for benchmarking analysis
[38] ISO/IEC PWI TS 27569, Personal identifiable information (PII) processing record information structure
[39] ISO/IEC PWI 27573, Privacy protection of user avatar and system avatar interactions in the metaverse

〈저 자 소 개〉

박 성 채 (Sungchae Park)
종신회원
순천향대학교 정보보호학과 학사 졸업
순천향대학교 대학원 정보보호학과 석·박사 통합 과정
2007년 10월~2009년 5월 : 어울림정보기술(주) 연구원
2010년 1월~2011년 5월 : 이글루시큐리티 주임연구원
2017년 8월~2020년 1월 : KB손해보험 법인영업부, 팀장
개인정보보호배상책임보험(II) 담당
2020년 2월~2022년 4월 : ㈜보다비 AI연구소 리더
2022년 5월~현재 : 순천향대학교 차세대보안 표준전문 연구실 선임연구원
<관심분야> 암호, AI 보안, 양자암호통신, 블록체인 보안, 5G/6G 보안, 개인정보보호 기술

박 준 형 (Junhyung Park)
순천향대학교 정보보호학과 학사 졸업
순천향대학교 대학원 정보보호학과 학·석사과정
<관심분야> 정보보호관리체계, 개인정보보호, 네트워크 보안, 인공지능 보안, 제로트러스트, 악성코드 분석

염 흥 열 (Heung Youl Youm)
종신회원
한양대학교 전자공학과 학사 졸업
한양대학교 대학원 전자공학과 석사 졸업
한양대학교 대학원 전자공학과 박사 졸업
2024년 3월~현재 : 순천향대학교 정보보호학과 명예교수
1990년 9월~2024년 2월 : 순천향대학교 정보보호학과 정교수, 명예교수
1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
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 국제의장
2019년8월~현재 : 분산신원증명 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