정 보 보 호 학 회 지
제25권 제4호, 2015. 8

개인정보보호 국제표준화 분석

염 흥 열*

요 약

기업에 의해 수집되어 관리되고 있는 개인정보가 유출되는 사고가 빈번하게 발생하고 있어서 기업의 개인정보보호 대응능력을 강화하기 위한 관리체계의 도입이 요구되고 있다[1,2]. 국제표준화위원회/전기위원회 합동위원회 1의 정보보호 기술연구반 아이덴터티 관리 및 프라이버시 작업반 (ISO/IEC JTC 1/SC 27/WG 5)에서는 기업을 위한 개인정보보호 원칙을 제시하고, 개인정보보호 위험 평가 지침을 제시하며 개인정보보호를 위한 각종 통제를 제시하기 위한 국제 표준화 작업을 수행하고 있다[18]. 정보보호관리체계 작업반(WG 1)에서는 2013년부터 정보보호관리 요구사항을 다룬 ISO/IEC 27001[6]을 이용해 여러 섹터에 적용되는 정보보호관리체계 구축을 위한 요구사항에 대한 국제표준화를 추진하고 있다.

본 논문에서는 작업반 1과 작업반 5에서 수행되고 있는 개인정보보호 관련 국제 표준화 활동의 동향을 살펴보고, 개인정보보호 관리체계 구축을 위한 국제 표준의 배열을 제시한다.

Ⅰ. 서 론

정보보호관리체계의 목표는 기업의 정보자산에 대한 기밀성, 무결성, 가용성을 보장하는데 있다[6]. 정보보호관리체계는 정보자산에 대한 위험을 식별하고 평가해 위험 수준을 결정한다. 이 위험 수준을 기업이 원하는 수준으로 낮추어야 한다고 결정하면 보호조치인 정보보안 통제를 적용해야 한다.

정보보호관리체계는 정보보호관리체계 운영을 위한 정보보호 조직을 구성하고, 조직이 지켜야할 정보자산을 식별해 정보자산에 대한 위험을 평가해 보호조치를 취하는 위험 평가 프로세스를 수행하고, 독립성이 보장된 감사팀에 의해 관리체계 운영의 타당성과 효과성을 감사받으며, 보호조치를 취하기 위한 정보보호 통제를 요구한다.

이와 마찬가지로 개인정보보호 관리체계를 구축하기 위해서는 개인정보도 정보이므로 기밀성, 무결성, 가용성을 위한 요구사항을 만족해야 할 뿐 아니라, 이에 더해 개인정보의 오용과 남용을 막기 위한 추가적인 개인정보 특화 통제가 필요하다. 따라서 정보보호 위험 평가와 다른 개인정보보호 위험 평가 가이드라인이 요구되며, 이 위험 평가 결과 위험의 수준을 낮추는 추가적인 개인정보보호 특화 통제의 개발이 요구된다. 개인정보보호 요구사항은 국내 개인정보보호법과 정보통신망 이용촉진 및 정보보호 등에 관한 법에 있다.[3,4]

본 논문에서는 SC 27/WG 1에서 수행하고 있는 ISO/IEC 27001을 이용한 섹터 특정 정보보호관리체계 구축을 위한 요구사항 문서의 개념과 내용을 분석하고, 개인정보보호관리체계를 구축하기 위해 요구되는 개인정보보호 특화 위험 평가 가이드라인과 개인정보보호 특화 통제에 관한 표준화 동향을 살펴본다[5,6].

본 논문의 2장에서는 ISO/IEC JTC 1/SC 27에서 추진되고 있는 3개의 국제 표준의 개발 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 주요 표준화 이슈

2.1. 개인정보보호관리체계 관련 국제표준

정보보호관리체계 작업반(WG1)과 아이덴터티 관리 및 프라이버시 작업반(WG5)에서 수행하고 있는 주요

이 논문은 2015년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (R-20150224-000293, IoT 환경에서 프라이버시 보호 국제 표준화)

* 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr),

〔표 1〕 개인정보관리체계 관련 국제 표준(2015.8)

작업반	표준 제목 및 번호	주요 내용	문서 상태
작업반 1	■ ISO/IEC 27009, 섹터 기반 관리체계 구축을 위하여 ISO/IEC 27001 국제 표준을 이용하기 위한 요구사항[9]	■ 섹터 기반 관리체계에 ISO/IEC 27001 국제 표준을 생성하기 위한 요구사항을 정의한다. 여기서는 ISO/IEC 27001 국제표준에 존재하는 요구사항에 더해 추가적으로 필요한 요구사항을 정의하고 기존의 요구사항을 개선하기 위한 방법을 제시한다.	DIS (draft international standard)
작업반 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 개인정보 영향평가 보고서의 구조와 내용에 대한 가이드라인을 제공한다.	1st CD (committee draft)
	■ ISO/IEC 29151, 개인정보보호 지침	■ 개인정보보호와 관련된 위험 평가 결과에 의해 식별된 요구사항을 만족하기 위한 통제와 구현 가이드라인 등을 제시한다.	1st CD (committee draft)
	■ 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.	-

국제 표준을 요약하면 [표 1]과 같다.

2.2. ISO/IEC 29100[13]

프라이버시 프레임워크에 관한 표준은 ISO/IEC 29100 [10]이며, 이 표준은 2011년 국제 표준으로 채택되었다. 이 표준에서는 프라이버시 관련 용어 정의, 주요 구성요소와 역할, 프라이버시 보호 요구사항, 그리고 11개의 프라이버시 보호 원칙을 제시하고 있다.

프라이버시 프레임워크에서 주요 주체는 개인정보주체(PII principal), 개인정보제어자(PII controller), 개인정보처리자(PII processor) 그리고 제3의 당사자(Third party) 로 구성된다. 여기서 개인정보제어자는 국내에서는 개인정보처리자로 지칭하고 있다. 개인정보주체는 자유 의지로 개인정보를 개인정보제어자에게 제공하는 자연인이다. 개인정보제어자는 개인정보의 처리 목적과 처리 방법을 처리지침으로 결정하며, 11개 개인정보보호 원칙을 준수한다. 개인정보처리자는 개인정보제어자 대신 개인정보를 처리한다. 제3의 당사자는 개인정보제어자나 개인정보처리자로부터 개인정보를 제공받아 자신의 권한을 갖는 개인정보제어자의 역할을 수행한다.

프라이버시 보호 요구사항은 크게 법준수 요구사항, 계약 행위 등의 요구사항, 비즈니스 요구사항, 비즈니스 모델에 종속되는 비즈니스 요구사항, 조직 자체에 의해 설정된 요구사항 등으로 구분된다.

이 표준에서 제시한 11 가지 프라이버시 보호 원칙은 [표 2]와 같다.

2.3. ISO/IEC 27009[09]

ISO/IEC 27001 국제표준은 정보보호관리체계를 구축하고 운영하기 위한 요구사항을 정의하고 있다. 이 표준의 상태는 현재 DIS 이다.

ISO/IEC 27002 국제표준은 조직의 정보보호 통제에 대한 지침을 제공한다. 이 표준은 통제 목표, 통제, 통제 구현 가이던스, 기타 정보 등의 계층적 구조를 갖는다. 이 지침은 조직의 유형이나 크기에 무관하게 적용될 수 있다. ISO/IEC 27002[7]에 제시된 통제 목표와 통제는 ISO/IEC 27001 부록 A[6]에 포함된다. ISO/IEC 27001에서는 위험 평가 결과로 선택된 통제를 결정하고, 그 결과를 ISO/IEC 27001 의 부록 A에 나와 있는 통제와 비교해 필요한 통제가 빠지지 않도록 확인한다.

그러나 최근에는 통신 조직[10], 클라우드 서비스 제공자[11,12] 등과 같은 섹터별 정보보호관리체계의 필요성이 대두되고 있고, 이를 위한 국제표준의 개발이 요

〔표 2〕 프라이버시 보호 원칙〔13,21〕

프라이버시 원칙	세부 설명
동의와 선택	정보 주체에게 개인 정보의 처리 허용 여부에 대한 동의 선택 권한이 주어지며, 정보주체의 자유의지로 동의가 이뤄져야 한다.
목적 합법성과 명세	처리 목적은 관련 법에 근거해야 하며, 분명하게 잘 설명되어야 한다.
수집 제한	개인정보는 법에서 규정한 목적에 맞게 필요한 항목으로 제한해 수집되어야 한다.
데이터 최소화	개인정보는 관련 이해 당사자와 개인정보취급자에게만 최소로 제공되어야 한다.
이용, 보유, 공개 제공	개인정보의 이용, 보유, 제공 목적을 명확히 하고, 이는 합법적 목적으로 꼭 필요한 개인정보로 제한되어야 한다.
정확성 및 품질	개인정보는 정확하고, 완전하며, 이용 목적에 적합하고 최신으로 유지되어야 한다.
공개, 투명, 그리고 고지	개인정보 처리를 위한 정책, 처리과정과 지침은 쉽고 접근하기 쉬운 형태로 개인정보 주체에게 제공되어야 한다.
개별 참여와 접근	개인정보 주체의 신원이 인증된 후 개인정보 제어자에 의해 처리되고 있는 자신의 개인정보를 검토할 권한이 부여되어야 한다.
책임성	특정 개인이 개인정보관련 정책, 절차, 관행을 이행하기 위한 업무에 할당되어야 한다.
정보 보안	개인정보는 무결성, 기밀성 그리고 가용성을 만족하기 위한 기술적 관리적 보호조치로 보호되어야 한다.
프라이버시 법 준수	내부 및 외부 감사자는 주기적인 감사를 실시하여 개인정보 처리가 보호 요구 사항을 준수하는지를 검사해야 한다.

구되고 있다. 예를 들어 ISO/IEC 27001 요구사항과 ISO/IEC 27002 통제, 그리고 특정 섹터에 적용되는 추가 통제를 이용해 해당 섹터에 적용 가능한 정보보호관리체계를 구축할 수 있다. 예를 들어, 개인정보보호를 위한 지침과 결합되면 개인정보보호 특화 정보보호관리체계 (즉, 개인정보보호관리체계) 를 구축할 수 있고, 통신 조직에 특화된 통제와 결합되면 통신조직을 위한 정보보호관리체계를 구축할 수 있다.

이 국제표준은 해당 섹터에 추가되어야 할 요구사항을 추가할 수 있다. 또한 추가적인 통제가 요구되는 경우, 위험 처리 통제 관련 요구사항이 개선되어야 할 것이다. 섹터에 특화된 통제 목표, 통제, 그리고 가이던스 등의 추가도 가능하고, 기존 통제의 변경도 가능하다.

부록에는 섹터 특화 표준을 개발하기 위한 다음과 같은 템플릿을 제공하고 있다.

서론
1. 범위
2. 참조문헌
3. 용어정의
4. 섹터 특화 ISMS (information security management system) 요구사항
5. 섹터 특화 통제

개인정보보호관리체계는 ISO/IEC 27001 요구사항에 추가 요구사항을 더하고, ISO/IEC 27002 통제와 ISO/IEC 29151 [16] 통제를 더하면 구축이 가능함을 의미한다.

2.4. ISO/IEC 29134[15]

이 국제 표준은 이 논문 작성 시점에 1차 CD 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]. 이 표준에서는 프라이버시 영향 평가를 위한 가이드라인을 제공하고 있다. 이 표준은 영향평가를 위한 여러 프로세스들을 식별하고 개인정보영향평가 보고서의 내용과 구조를 제시하고 있다. 개인정보영향평가의 보고서의 내용은 다음의 사항을 포함해야 한다.

- 서론: 개인정보영향평가의 제목, 수행 이유, 수행 시기, 수행 주체, 수행 프로젝트 내용, 방법론 등을 설명.
- 개인정보영향평가 범위: 기본적으로 범위를 설명

하며, 개인정보 처리 과정, 처리 목적, 개인정보 처리자, 프라이버시 프로세스 구현 방법, 처리되는 개인정보 유형, 지원 자산 등을 포함.

- 프라이버시 요구사항: 준수 요구사항과 준수 점검 사항을 포함.
- 위험 평가: 위험 소유자, 프라이버시 위험의 결과 및 등급 결정, 위험의 발생 확률 등을 포함한다.
- 위험 치료 대책
- 결론

2.5. ISO/IEC 29151[16]

이 국제표준은 개인정보관리체계를 위한 추가 통제를 제공하고 있다. 이 국제표준은 이 논문 작성 시점에 1차 CD 상태에 있다.

ISO/IEC 29151은 개인정보제어자(PII controller)에 적용 가능한 보호조치를 위한 통제 목표, 통제, 구현 가이던스, 그리고 기타 정보를 제공한다[13]. 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.

2.6. 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].

- ISO/IEC 27001 요구사항 이외에 ISO/IEC 29100 개인정보보호 원칙을 고려해야 한다.
- 리스크 관리를 위해서는 ISO/IEC 27001 의 6.1 절을 적용하되 정보보호 리스크에 더해 프라이버시 리스크에 대한 위험평가 프로세스를 정의해야 한다. 또한 정보보호 치료 대책에 더해 프라이버시 치료 대책도 고려해야 한다.
- ISO/IEC 27002 정보보호 통제에 더해서 ISO/IEC 29151에서 제시된 통제와 ISO/IEC 27108 통제를 적용해야 한다.[20]

Ⅲ. 결 론

개인정보보호에 대한 국제 표준 개발은 ISO/IEC JTC 1/SC 27/WG 5에서 추진되고 있다. 개인정보는 식별이 가능한 살아있는 개인에 관한 정보이다. 기업이 개인정보관리체계를 구축하기 위한 위험 평가 가이드라인으로 ISO/IEC 29134, 추가적인 통제로 ISO/IEC 29151, 그리고 섹터 특화 정보보호관리체계 구축을 위해 요구되는 표준을 개발하는데 필요한 지침을 제공하는 ISO/IEC 27009, 그리고 개인정보관리체계 구축과 관련해 추가 요구사항과 추가 통제 등을 규정하는 SD 5/WG 5의 문서 등이 존재한다.

본 논문에서 분석된 개인정보보호 관련 국제표준은 방통위가 2011년부터 시행하고 있는 개인정보보호관리체계의 글로벌 상호 인증시에 활용 가능하며, 2018년초에 현재 개발되고 있는 개인정보보호 지침과 위험평가 가이드라인에 대한 국제표준이 채택되고 나면, 그 결과는 국내 개인정보보호관리체계 인증을 위한 기준을 고도화하는데 이용가능하다.

본 논문에서 제시된 개인정보보호 프레임워크, 프라이버시 보호 원칙, 개인정보보호 지침, 그리고 개인정보 영향평가 가이드라인은 개인정보제어자가 개인정보관리체계를 구축하기 위해 유용하게 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 27000:2009, 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 DIS 27009, TInformation 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 FDIS 27017, Code of practice for information security controls based on ISO/IEC 27002 for cloud services
[12] ISO/IEC 27018, 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 FDIS 29190, Information technology - Security techniques - Information technology -- Security techniques -- Privacy capability assessment model
[15] ISO/IEC 1st CD 29134, Privacy Impact Assessment - Methodology, 2014.5
[16] ISO/IEC 1st CD 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, 2014.4
[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

〈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
관심분야 : 네트워크 보안, 개인정보보호관리체계, IoT 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜