情 報 保 護 學 會 誌
第23卷 第4號, 2013. 8

개인정보보호 관리체계 국제 표준화 필요성

염 흥 열*

요 약

개인정보보호 관리체계(PIMS: Personal Information/privacy Management System)는 개인정보에 특화해 기업이 고객들의 개인정보를 보호 활동을 지속적이고 체계적으로 수행하기 위한 체계를 지칭한다. 기업에 의해 다양한 개인정보가 수집되어 이용되고 있고 비즈니스 목적의 개인정보 국외 이전에 대한 요구가 증가하고 있는 점을 고려하면, 글로벌 차원에서 합의된 개인정보보호 관리체계의 국제 표준화된 지침 (관리 프로세스 요구사항과 리스크를 관리하기 위한 보호대책) 의 개발이 요구되고 있는 실정이다. 이러한 국제표준에 근거한 개인정보보호 관리체계를 위한 기준은 국경을 넘어선 개인정보의 이전을 가능케 하는 기반을 제공하며, 이 기준을 이용하면 국가별로 다르게 운영되고 있는 개인정보보호 관리체계에 대한 국가간 상호 인정도 가능케 할 것이다.

본 논문에서는 정보보호관리체계와 개인정보보호 관리체계의 주요 특성을 살펴보고, 두 체계 간의 유사점과 차이점을 식별하며, 개인정보관리체계의 운영을 위한 국제 표준 구성 요소를 제시한다. 또한, 한국 주도로 추진 중인 개인정보보호 관리체계 지침을 위해 2011년 8월 이후 ITU-T SG17과 ISO/IEC JTC 1/SC 27에 의해 추진되고 있는 지금까지 국제 표준화 추진 경과 사항을 살펴보고, 향후 표준화 전망을 제시한다.

Ⅰ. 서 론

최근 들어 국내에서 개인정보 유출 사고가 빈번히 발생하고 있어, 개인정보 보호를 위한 법제도적 정비에 더해 기술적 관리적 보호대책의 필요성이 요구되고 있다. 그러나 국가마다 지역마다 서로 다른 개인정보보호 법제도적 요구 수준의 차이로 인해 국가 또는 지역간 서로 다른 보호대책을 요구하게 되어, 국제표준에 근거한 지침의 부재는 국가 또는 지역간 개인정보의 이전을 저해하고 있는 요인이 되고 있다. 따라서 글로벌하게 합의된 프라이버시 원칙[31]에 기반을 둔 보안 및 프라이버시 측면의 보호대책(control)의 개발이 필요하게 되었다. 이렇게 글로벌하게 합의된 보호대책은 기업에 의한 개인정보보호관리체계 수립의 기준으로 활용될 수 있으며, 개인정보보호 관리체계의 국가간 상호 인정(mutual recognition)제공은 물론 국경을 넘는 개인정보의 원활한 이전을 가능케 할 것이다.

정보보호관리체계 (ISMS: Information Security Management System) 는 리스크 분석에 기반해 조직의 정보, 네트워크 장치 등의 정보자산에 대해 기밀성, 무결성, 가용성을 보존하기 위해 요구되는 체계를 수립, 구현, 운영, 모니터링, 유지, 그리고 개선하기 위한 조직의 관리 체계 이다. 또한, 개인정보보호 관리는 개인정보에 특화해 기업이 고객들의 개인정보를 보호하기 위한 것이고, 개인정보 관리체계(PIMS: Personal Information Management System)는 조직에 의한 이를 위한 지속적이고 체계적으로 수행하기 위한 체계이다.

현재 국가 차원에서 개인정보보호 관리체계를 운영하는 나라는 영국[1], 일본[2], 그리고 한국[3] 등이다. 한국은 국내에서 2011년부터 시행 중인 국내 개인정보 관리체계의 기준을 국제 표준으로 개발하기 위해 2011년 8월 ITU-T SG 17에 국제 표준을 개발할 것을 제안했고[4], 다시 2011년 10월 케냐 라이로비 ISO/IEC JTC 1/SC 27 회의에 국제 표준 개발 타당성 확인을 위한 연구준비기간(SP, study period)를 제안해[5] 두 제안 모두를 채택시킨 바 있다[6],[7]. 또한, 1년간의 SP

본 연구는 미래창조과학부의 지원을 받는 방송통신표준기술력향상사업의 연구결과로 수행되었음(개인정보보호관리체계(PIMS) 국제 표준 개발, No. 2013-PK10-19).
* 정보보안산업표준포럼 의장 / 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr)

기간을 마치고, 2012년 10월 ISO/IEC JTC 1/SC 27 로마 회의는 세계 최초로 개인정보관리체계를 위한 국제 표준(ISO/IEC 27009, ISO/IEC 29151)에 대한 신규 표준화 아이템 (NWI, new work item) 추진을 채택했다[8],[9]. 이러한 활동을 통해 한국은 이 두 공적 표준화 기구에서 한국 주도로 개인정보보호 관리체계를 위한 인증 기준에 대한 국제 표준화를 추진하는 바탕을 마련하게 되었다.

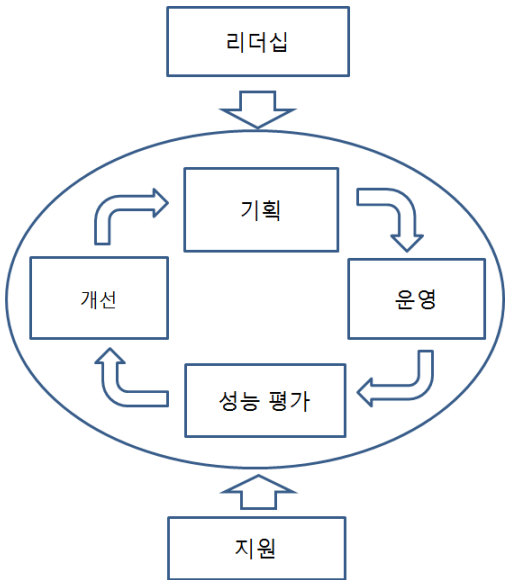
본 논문의 구성은 다음과 같다. 제2장에서는 정보보호 관리체계와 개인정보관리체계의 특징을 살펴보며, 각 관리체계의 차이점을 도출하며, 개인정보관리체계를 위해 요구되는 국제 표준 구성요소를 도출한다. 제3장에서는 2011년 8월 이래 양대 공적 표준화 기구인 ITU-T SG17과 ISO/IEC JTC 1/SC 27에서 추진되어온 한국 주도의 개인정보관리체계의 국제 표준화 추진동향을 제시한다. 제4장에서는 향후 추진 사항을 포함해 결론을 맺는다.

Ⅱ. 개인정보보호관리체계 표준화 개요

2.1 정보보호관리체계

정보보호관리체계는 기업의 비즈니스 목표를 달성하기 위한 기업내 조직, 정책, 활동, 책임 확인 및 할당, 가이드라인, 절차, 과정 (process) 등을 포함한다[13]. 정보자산은 기업에게 가치를 주는 아이템으로 정의되며, 정보, 소프트웨어, 하드웨어, 서비스, 조직원, 그리고 명성이나 이미지 등의 무형자산 등으로 구성된다[13].

정보보호(information security)는 기업이 관리하는 정보 자산(information asset)에 대한 무결성, 기밀성, 가용성을 보호하는 것이고, 정보보호관리체계는 기업의 경영 과정의 일부분으로서, 지속적이고 체계적으로 정보보호를 수립하고 운영하며, 검토하고 개선하는 체계를 지칭한다[12]. 정보보호관리체계의 목표는 기업이 관리하는 정보자산을 보호함으로써, 기업의 비즈니스 목표를 달성하는 것이다. 정보보호관리는 정보자산의 기밀성, 무결성, 그리고 가용성을 보존하는 것이다. 기업의 정보보호관리체계는 기업 스스로가 수립하고 운영하는 것이나, 제3의 신뢰기관 인 인증기관(예를 들어, 국내의 경우 한국인터넷진흥원)이 조직이 운영하고 있는 정보보호관리체계가 법에서 정해진 인증기준을 만족

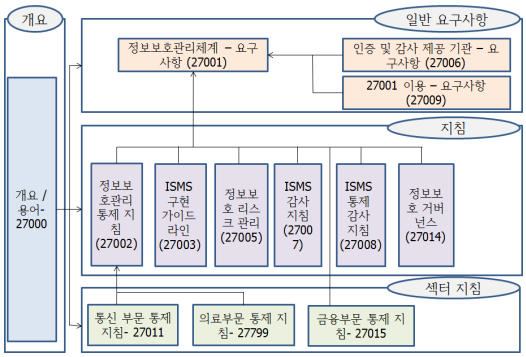


〔그림 1〕 ISMS 관리 프로세스

하는지를 점검하여 만족하면 해당 조직을 인증해 주는 제도를 운영한다. 따라서, 정보보호관리체계 인증을 수행하는 제3의 신뢰기관인 인증기관이 만족해야 할 요구사항을 제시한 국제 표준도 필요하다[17].

정보보호관리체계는 조직이 보호해야 할 정보자산을 식별하고, 이 정보자산에 대한 리스크(risk)를 식별하고 분석하며 평가해, 조직이 수용할 수 없는 리스크 수위를 갖도록 다양한 리스크 관리 대책을 수립해야 한다. 따라서, 정보보호관리체계는 [그림 1]과 같이 조직의 최고책임자의 약속과 조직의 자원의 지원 하에 정보보호 관리체계를 구현하고, 상시적으로 모니터링하고 감사하며 성능을 평가하여, 지속적으로 개선하는 과정으로 구성된다. 정보보호관리체계를 위해 요구되는 국제 표준 구성 요소는 다음과 같다([그림 2] 참조).

- 개념 및 용어 정의 : 27000 [12]
- 관리 프로세스 요구사항[13]/인증기관 요구사항 [17]/부문별 관리체계 인증에 27001의 이용[20] : 27001/27006/27009
- 보안 통제(보호대책) 지침 : 27002 [14]
- 구현 지침 : 27003 [15]
- 리스크 평가 및 관리 지침 : 27005 [16]
- 감사 및 감사를 위한 통제 지침 : 27007 [18], 27008 [19]
- 정보보호 거버넌스 지침: 27014 [22]



〔그림 2〕 ISMS를 위한 국제표준 구성 요소

- 부문별 보안 통제 지침 (통신, 의료, 금융 부문 보안 통제 지침): 27011/27015/27799 [21], [23], [24]

2.2 개인정보보호 관리체계

개인정보보호 관리체계(PIMS: privacy/personal information management system)는 기업이 비즈니스 요구에 의해 수집해 이용하는 개인정보를 보호하기 위한 체계를 구축, 구현, 운영, 점검, 개선하기 위한 체계를 말한다[29]. 개인 정보 (PI: personal information)는 정보주체를 식별하거나 다른 정보와 결합해 쉽게 개인을 식별 할 수 있는 정보로 정의된다[10],[11]. 개인정보보호 관리체계는 조직이 보호해야 할 개인정보와 관련된 자산을 식별하고, 개인정보에 발생 가능한 리스크를 식별하고 분석하며 평가해, 이에 적절한 보호대책을 구현하고, 상시적으로 이 체계를 모니터링하여 개선하는 체계이다. 개인정보에 대한 리스크는 개인정보도 정보의 일부분이므로, 보안 리스크가 상속하게 된다. 그러나, PIMS에서는 개인정보보호 법/제도나 프라이버시 원칙을 위반하는 리스크를 고려해야 한다. 이러한 리스크를 프라이버시 리스크라 하며, 이러한 리스크를 감소 또는 없애기 위한 보호대책도 요구된다. 참고로, 개인정보보호 관리체계는 개인정보보호 법/제도 또는 프라이버시 원칙 (privacy principle) 의 준수를 유지하고 관리하기 위한 조직의 프레임워크이라고도 볼 수 있다. 참고로 [표 1]은 개인정보관리체계의 보호대책 지침 개발시 이용 가능한 세계경제협력기구(OECD) 프라이버서 원칙 [30] 과 국내 개인정보보호법 [10]에서 정의하고 있는 개인정보보호 원칙을 비교해 나타냈다.

〔표 1〕 개인정보보호 원칙

OECD	국내 개인정보보호법
목적 명확화	개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.
수집 제한	
이용 제한	개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.
정보의 질	개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.
안전성 확보	개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.
공개	개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.
정보주체의 참여	
책임	법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.
-	정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.
-	개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다.

2.3 PIMS/ISMS 비교

ISMS/PIMS의 특성을 파악하기 위해서는 다음과 같은 비교 항목의 도출이 필요하다.

- 보호 대상
- 보호 목표
- 관리 프로세스
- 리스크 유형
- 보호 요구사항 출처
- 리스크 평가 방법
- 보호대책의 유형

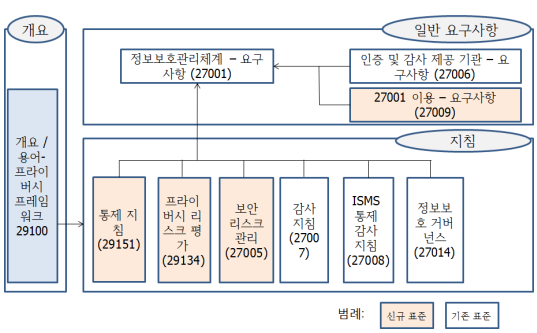
이들 비교 항목을 이용해 ISMS 와 PIMS를 비교하면 [표 2]와 같다.

〔표 2〕 PIMS와 ISMS 와의 비교분석

비교 항목	ISMS	PIMS
보호 대상	정보자산	개인정보
보호 목표	기밀성, 무결성, 가용성 보장	기밀성, 무결성, 가용성, 투명성, 개입가능성, 비연결성
관리 프로세스	PDCA(Plan-Do-Check-Act) 에 기반한 관리 프로세스 (27001)	PDCA(Plan-Do-Check-Act) 에 기반한 관리 프로세스 (27001) + 프라이버시 측면 관리 요구사항
리스크 유형	보안 측면의 리스크	보안 측면 리스크 + 프라이버시 측면 리스크
보호 요구사항 출처	조직 비즈니스 목표 고려 리스크 평가 + 법 제도적 요구사항	조직 비즈니스 목표 고려 리스크 평가 + 법제도적 요구사항 + 프라이버시 원칙
리스크 평가 방법	보안 리스크 관리 (ISO/IeC 27005)	보안 리스크 : 27005 프라이버시 리스크: 29134
보호 대책의 유형	보안 통제	보안 통제 + 프라이버시 통제

2.4 개인정보관리체계를 위한 국제 표준 구성요소

개인정보관리체계를 구현하기 위한 국제 표준 구성요소는 [그림 3] 과 같이 정리될 수 있다. PIMS에서 리스크는 보안 리스크와 프라이버시 리스크로 구분된다. 보안 리스크는 기존 27005 [16] 리스크 관리 프레임워크를 이용해 식별, 평가, 관리될 수 있으나, 프라이버시 리스크는 프라이버시 영향평가를 통해 프라이버시 리스크를 식별하고 평가해야 한다. 보안 리스크는 보안 통제로 리스크를 치료할 수 있으며, 프라이버시 리스크는 프라이버시 통제로 치료할 수 있다. 다라서, [그림 3]과 같



〔그림 3〕 PIMS를 위한 국제표준 구성요소

이 개인정보보호 관리체계를 위한 추가적 요구사항을 식별하기 위해 ISO/IEC 27009 [20] 를 이용해야 하며, 보안 통제와 프라이버시 통제를 위한 지침은 ISO/IEC 29151 [25] 을 이용해야 하며, 프라이버시 리스크를 식별하기 위해서는 ISO/IEC 29134 [32] 을 이용해야 한다. 나머지 관리 프로세스 요구사항 (27001), 인증 및 감사 제공기관 요구사항(27006), 통제 감사 요구사항 (27008), 감사 지침 (27007), 정보보호 거버넌스 (27014) 은 기존 국제 표준을 이용할 수 있다.

Ⅲ. 개인정보관리체계 국제 표준화 추진 동향

3.1 ITU-T SG 17 국제 표준화 추진 동향

ITU-T SG17 연구과제 3(Q.3, Question 3)은 한국(필자 등)의 제안 [4] 으로 2011년 8월 SG17 회의에서 통신조직을 위한 개인정보관리체계 가이드라인인 ITU-T X.gpim 권고를 개발키로 합의했고, 이 권고 개발을 책임질 에디터로 염흥열, 변순정 등(한국)을 결정한 바 있다[6]. 그 후 2012년 2월 SG 17 회의에서 한국

〔표 3〕 통신조직을 위한 PIMS 지침 표준 개발 현황

일시 및 회의	주요 결정사항
2011년 8월 SG 17 회의	- 한국 (염흥열 외) 통신 조직을 위한 PIMS 지침 제안 - 토의후 신규 표준화 권고 (X.gpim)로 개발키로 합의 - 에디터로 염흥열, 변순정 (한국) 등을 임명 - 다만, 통신조직을 위한 지침 필요성 확인 요구
2012년 2월 SG 17 회의	- 한국은 통신조직을 위한 PIMS 지침 필요성에 대한 기고서 추가 제출 - SC27에서 PIMS 국제 표준 개발 타당성 조사를 위한 SP 논의 결과를 보고 나서 최종 결정키로 합의함
2012년 8월 SG 17회의	- 한국, X.gpim 기반 문서 제안 및 반영 - SC 27과의 협력 개발은 SC27 측의 SP 최종 논의 결과를 보고 결정키로 합의함 - X.gpim은 SC27 과 협력적으로 개발할 것을 합의함
2013년 4월 SG 17	- 한국은 ITU-T X.gpim 1차 수정 텍스트 제안 및 1차 수정 텍스트 합의 - SC 27이 일반 조직을 위한 PIMS 지침을 개발하기로 합의 결과 관찰 - X.gpim 공통 텍스트 추진을 위해 SG17 Q.3/SC 27 WG5 간의 조인트 회의를 통해 협력 개발 가능성 타진했으며, 조인트 회의 결과, 두 표준화 기구가 각자 독자적으로 개발하되, 표준 채택 과정에서 공통 텍스트 추진 여부 결정키로 합의함

은 통신 조직에 특화된 PIMS 가이드라인의 개발 필요성을 해명했고, 2012년 8월 SG 17 회의에서 제1차 드래프트 초안을 합의했다. 이때 이 권고를 ISO/IEC JTC 1/SC 27에게 협력 개발을 제안키로 했다. 2013년 4월 SG 17 회의에서 제2차 드래프트 권고가 합의되었다[29]. 또한, 이 권고를 ISO/IEC JTC 1/SC 27과 협력해 개발해야 한다고 다시 확인했다. 이를 시계열로 정리하면 [표 3]과 같다.

3.2 ISO/IEC JTC 1/SC 27 국제 표준화 추진 동향

한국(염흥열 등)은 2011년 10월 케냐 나이로비 SC27 회의에서 PIMS 관련 국제 표준을 개발 타당성 조사를 위한 준비기간인 SP(Study Period)를 제안했고[5], 한국의 제안이 채택되었다[7]. 6개월 동안의 준비활동을 주도할 SP 라포처로 염흥열(한국), 영국(J. Phillips), 프랑스(Mathiu Grall), 일본(Y. Satoh) 을 임명했다. 한국은 이 연구회기 동안 프로세스 요구사항, 보안 지침, 프라이버시 지침을 개발해야 한다는 국가 기고서를 제출했고, 프랑스도 한구과 입장이 같았으며, 영국은 지침 개발해야 한다는 국가 기고서를 제출했다. 라포처 그룹(염흥열 포함)은 이 결과를 2012년 스웨던 스톡홀름 SC 27 회의에 발표했다[26]. 2012년 5월 SC 27 회의에서는 관리 프로세스에 대한 표준을 별도로 개발하지 않고 기존의 ISO/IEC 27001을 이용하기로 합의했고, 한국의 제안대로 보안 통제 및 프라이버시 통제에 대한 국제 표준 개발의 필요성을 합의했으나, 추가 연구를 위한 SP 를 6개월 연장하기로 합의했다. 더불어, PIMS 인증을 위해 ISO/IEC 27001을 어떻게 이용할지에 대한 국제 표준 개발이 필요하다는 데에도 합의했다. 한국은 연장된 6개월의 SP 동안 “27001 을 PIMS 인증을 위해 이용”, “보안 통제”, “프라이버시 통제”에 대한 국제 표준 추진을 위한 신규표준화 아이템(NWIP: new work item proposal)을 제안했다. 영국도 “섹터 기반 인증을 위한 27001 이용” 과 “PIMS 통제”에 대한 NWIP를 제안했다. 라포처 그룹(염흥열 포함)은 한국과 영국 등의 기고서를 토대로 두 가지 형태의 NWIP (“27001 이용”, “통제 지침” 또는 “27001 이용”, “보안 통제 지침” “프라이버시 통제 지침”)를 2012년 10월 SC27 로마회의에 보고했다[27]. 2012년 SC 27 로마회의에서는 2가지 NWIP (“섹터 기반 인증을 위한 27001 이용”, “개인정보보호 지침”) 를 추진하기로 합의했다[28]. “개인정보보호 지침” NWIP의 경우 한국의 염흥열과 영국의 Bridget Kenyon을 액팅 에디터로 임명했다[8], [9]. 2013년 1월, 4월 2가지 NWIP 이 회원국의 투표에 의해 성공적으로 통과되었다. 2013년 4월 프랑스 SC 27 회의에서는 NWIP 동안 각 국가별 컴맨트가 검토하였고, “섹터 기반 제3자 인증을 위한 27001의 이용 및 적용” 국제 표준에 ISO/IEC 27009 표준 번호가 할당되었고, “개인정보보호 지침” 국제 표준에 ISO/IEC 29151 번호가 할당되었다. ISO/IEC 27009 표준 개발을 주도할 에디터로 영국의 알젤리카, 한국의 박태완, 일본 전문가가 임명되었고, ISO/IEC 29151 표준 개발을 주도할 에디터로 한국 염흥열과 영국 Bridget Kenyon을 임명했다. 또한, 1차 WD를 2013년 6월 15일까지 공개키로 했다.

2013년 SC 27 회의동안 ITU-T X.gpim 과 ISO/IEC 29151이 내용과 목적이 유사하므로, 구 그룹간의 공통 표준으로 개발할 것에 대해 논의했고, 회의 결과, 일단 두 그룹이 독자적으로 개발하되, 연락문서 교환을 통해 혀벽 개발하고, 최종 채택 순간에 공통 표준 개발에 대해 다시 검토하기로 합의했다.

이렇게 함으로써, 1년 6개월간의 PIMS 관련 국제표준 타당성 과정을 거쳐 한국이 제안대로 “섹터기반 제3자 인증을 위한 27001의 이용 및 적용“ 국제 표준(ISO/IEC 27009)와 ”개인정보보호 지침“(ISO/IEC 29151)에 대한 국제 표준을 개발키로 합의했고, 두 국제 표준의 개발 책임자인 에디터로 한국 보안 전문가가 참여하게 되어서, 한국 주도의 PIMS 국제 표준 추진을 위한 기반을 마련했다. 현재 두 표준은 2016년도에 표준 개발을 완료한다는 목표로 향후 개발될 예정이다. 이 과정을 시계열로 요약하면 [표 4] 와 같다.

〔표 4〕 PIMS 국제표준 추진 현황

일시 및 회의	주요 결정사항
2011년 10월 케냐 나이로비 SC 27회의	- 한국 (염흥열 외) PIMS 국제 표준 개발 타당성 확인을 위한 연구회기(SP) 제안 및 채택 - SP를 이끌 라포처로 염흥열(한국), 프랑스, 영국, 일본 전문가 임명
2011년 10월 - 2012년 5월 1차 SP	- 한국과 프랑스는 관리 프로세스, 보안 통제, 프라이버시 통제에 대한 국제 표준이 필요하다는 기고서 제출

일시 및 회의	주요 결정사항
	- 영국은 관리 프로세스는 개발하지 말고, 보안 통제와 프라이버시 통제에 대한 국제 표준이 필요하다는 기고서 제출 - 라포처 그룹은 2012년 5월 SC17 회의에 SP 보고서 제출
2012년 5월 스톡홀름 SC27 회의	- SP 보고서에 대한 토론이 진행됨 - 관리 프로세스는 별도로 개발하지 않고 ISO/IEC 27001을 이용하기로 했고, 보안 통제와 프라이버시 통제에 대한 국제 표준 개발이 필요함을 합의함 - 또한, 특화된 요구사항을 개발하기 위한 27001을 섹터 기반 인증에 이용하는 표준을 개발키로 합의함 - 추가적인 연구를 위해 6개월 간 더 SP를 연장키로 합의함
2012년 5월 - 10월	- 한국은 “27001 이용”, “보안 통제”, “프라이버시 통제”에 대한 NWIP 제안 - 영국도 2가지 NWIP 제안 - 프랑스는 한국 입장을 지지했고 일본 등도 지지 - 라포처그룹(염흥열 등)제2차 SP 보고서 작성 및 2012년 10월 로마 SC 27 회의에 보고됨
2012년 10월 로마 SC 27회의	- SP 보고서 검토 - 2가지 NWIP 로 진행키로 합의함 . 섹터 기반 인증에 27001 이용 . 개인정보보호를 위한 지침 - 27001을 섹터 기반 인증에 이용을 위한 NWIP의 액팅 에디터로 영국의 알젤리카로 임명함 - 개인정보보호를 위한 지침 NWIP의 액팅 에디터로 염흥열(한국)과 영국 보안 전문가를 임명함
2012년 10월 - 2013년 4월	- 2013년 1월 27001을 섹터 인증을 위한 NWIP 투표 통과 - 2013년 4월 개인정보보호를 위한 NWIP 통과
2013년 4월 프랑스 SC 27 회의	- 두 국제 표준 번호로 ISO/IEC 27009(섹터 기반 제3자의 인증에 27001의 이용 및 적용), ISO/IEC 29151(개인정보보호 지침) 부여함 - ISO/IEC 27009 에디터로 박태완(한국), Angelika Plate(영국), 일본 전문가 임명 - ISO/IEC 29151 에디터로 염흥열(한국)과 영국 보안 전문가 임명 - ITU-T X.gpim 공통 택스트 추진을 위해 SG17 Q.3/SC 27 WG5 간의 조인트 회의를 통해 협력 개발 가능성 타진했으며, 조인트 회의결과, 각자 독자적으로 개발하되, 표준 채택 과정에서 공통 택스트 추진 여부 결정키로 합의함

Ⅵ. 결 론

양대 공적 표준화 기구는 개인정보보호 관리체계에 대한 국제 표준 필요성을 인정하고 표준을 개발키로 합의하고 이를 진행하고 있다. 이러한 활동은 한국의 개인정보보호 관리체계 지침의 국제표준화로 추진하기 위한 활동으로 볼 수 있다. 현재 개인정보보호 관리 체계를 위해서는 ITU-T 의 경우, 1가지 국제표준(ITU-T X.gpim)이 개발되고 있고, ISO/IEC JTC 1/SC 27의 경우, 3가지 국제 표준(ISO/IEC 27009, ISO/IEC 29151, ISO/IEC 29134)이 개발되고 있다. 이러한 표준은 2016년도 개발 완료를 목표로 표준화가 진행 중에 있다.

본 논문에서는 정보보호관리체계와 개인정보보호 관리체계의 특성을 살펴보았고, 두 체계 간의 유사점과 차이점을 비교 분석했으며, 개인정보관리체계 운영을 위해 요구되는 국제 표준 요소를 제시했다. 또한, 한국 주도로 현재 개발이 진행되고 있는 개인정보보호 관리체계에 대한 국제 표준 개발을 위해 2011년 8월 이후 ITU-T SG17과 ISO/IEC JTC 1/SC 27에 의해 추진된 지금까지 경과 사항을 살펴보았고, 향후 추진 전망을 제시했다. 본 논문의 결과는 개인정보관리체계를 위한 국제표준 추진을 위해 활용 될 것으로 기대된다.

참고문헌

[1] BS 10012:2009, Data protection – Specification for a personal information management system, BSI, 2009

[2] JIS Q 15001:2006, Personal information protection management systems – Requirements, Japanese Standards Association Japan Institute for Promotion of Digital Economy and Community, 2006

[3] KCS.KO-12.0001, 개인정보보호 관리 체계(PIMS), 미래창조과학부, 2011

[4] ITU-T SG17 C467, New work item proposal for personally identifiable information management system for telecommunication sector, 염흥열 외, 2011.8

[5] N10319, Korean National Body proposal for a new WG 1 Study Period on ”Personal information management based on ISO/IEC 27001

and 29100", JTC 1/SC 27, 염흥열 외, 2011.10

[6] ITU-T SG 17, The structure of new work item on Recommendation ITU-T X.gpim, Guideline for management of personally identifiable information for telecommunication organizations, 염흥열 외, TD 2275 Rev.4, 2011.8

[7] ISO/IEC JTC 1/SC 27/N10546, Terms of reference for a joint ISO/IEC JTC 1/SC 27/WG 1 and ISO/IEC JTC 1/SC 27/WG 5 Study Period on Privacy/Personal Information Management Systems (PIMS) starting in October 2011, JTC 1/SC 27/WG 1 - WG 5, 2011.10

[8] ISO/IEC JTC 1/SC 27/N11724, Proposal for a new work item on Code of practice for the protection of personally identifiable information, JTC 1/SC 27/WG 5, 2013.1(제안자: 염흥열)

[9] ISO/IEC JTC 1/SC 27/N11881, Proposal for a new work item on The Use and Application of ISO/IEC 27001 for Sector/Service-Specific Third-Party Accredited Certifications, JTC 1/SC 27/WG 1, 2012.11

[10] 법제처, 개인정보보호법, 2011

[11] 법제처, 정보통신망이용촉진 및 정보보호 등에 관한 법

[12] ISO/IEC 27000:2009, Information security management systems – Overview and vocabulary

[13] ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements

[14] ISO/IEC 27002:2005, Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management system

[15] ISO/IEC 27003:2010, Information technology – Security techniques – Information security management system implementation guidance

[16] ISO/IEC 27005:2011, Information security risk management

[17] ISO/IEC 27006:2011, Information technology – Security techniques –Requirements for bodies providing audit and certification of information security management systems

[18] ISO/IEC 27007:2011, Information technology – Security techniques – Guidelines for information security management systems auditing

[19] ISO/IEC TR 27008:2011, Information technology – Security techniques –Guidelines for auditors on information security controls

[20] ISO/IEC NP 27009, The Use and Application of ISO/IEC 27001 for Sector/Service-Specific Third-Party Accredited Certifications

[21] ISO/IEC 27011:2008, Information technology – Security techniques – Information security management guidelines for telecommunications organisations based on ISO/IEC 27002

[22] ISO/IEC FDIS 27014, Information technology - Security techniques - Governance of information security

[23] ISO/IEC DTR 27015, Information technology - Security techniques - Information security management guidelines for financial services

[24] ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002

[25] ISO/IEC NWI 29151, Code of practice for the protection of personally identifiable information, 2013.4

[26] N10946, Study period report on Privacy / Personal information management system (PIMS), 염흥열외, 2012-04-02

[27] N11590, Output of the Study Period Rapporteurs assessment in response to SC 27 N11143 Call for Contributions on WG 1 Study Period on Alignment for Privacy / Personal Information Management Systems (PIMS), 염흥열외, 2012-10-02

[28] N11918, Meeting report - Study Period on privacy/personal information management system, 염흥열외, 2012-11-05

[29] ITU-T X.gpim, Guideline for management of personally identifiable information for telecommunication organizations, The 2nd revised text for Recommendation ITU-T X.gpim, 염흥열외, TD 227 Rev.1, 2013.4

[30] OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD, 1980
[31] ISO/IEC 29100(2011), Information technology - Security techniques - Privacy framework
[32] ISO/IEC 29134, Privacy Impact Assessment - Methodology, 2013.4

〈著者紹介〉

염흥열 (Heung-Youl 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
1997년 3월~2000년 3월 : 순천향대학교 산업기술연구소 소장
2000년 4월~2006년 2월 : 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재 : 한국정보보호학회 총무이사, 학술이사, 교육이사, 총무이사, 논문지편집위원 위원장, 수석부회장(역), 명예회장(현)
2005년~2008년 : ITU-T SG17 Q.9 Rapporteur(역)
2006년 11월~2009년 2월 (구) 정통부 정보보호 PM/, 정보통신연구진흥원 정보보호전문위원
2011년 1월 ~ 12월 : 한국정보보호학회 회장(역)
2008년 7월 ~현재 : 방송통신위원회 자체평가위원회
2008년 7월 ~2013년 2월 : 행정안전부 정책자문위원회
2013년 5월 ~현재 : 미래창조과학부 자체평가위원회
2009년 5월~현재 : 국정원 암호검증위원회 위원
2009년~현재 : ITU-T SG17 부의장/SG17 WP3 의장
2012년 6월 ~현재 : 정보보안산업 표준 포럼 의장
<관심분야> 인터넷 보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜