[정보보호] 개인정보보호관리체계 국제표준화 추진현황

국제표준화기구/국제전기위원회 합동기술위원회/부위원회 27/작업반 5(ISO/IEC JTC 1/SC 27/WG 5) 회의가 2015년 10월 26일부터 30일까지 5일간 인도 자이푸르에서 열린 바 있다. 이 회의에서는 한국이 주도적으로 개발하고 있는 개인정보보호 관리체계 관련 두 가지 국제표준(ISO/IEC 29151, ISO/IEC 27009)이 심도 깊게 논의되었다. 본고에서는 이와 관련된 주요 논쟁 및 합의사항을 중심으로 기술한다.

주요 이슈 및 논쟁사항

개인정보보호관리체계를 구축하기 위해서는 개인정보를 안전하게 보호하기 위한 요구사항/프로세스와 정보보안 측면의 보호대책에 더해 개인정보보호 측면의 기술적·관리적·물리적 보호대책을 추가로 요구한다. 개인정보보호 관리체계 국제 표준화는 2011년 10월 케냐 나이로비 SC27 회의에서 한국의 제안으로 시작되었으며, 한국은 개인정보보호 관리체계를 위한 요구사항/프로세스와 지침에 대한 국제 표준을 개발할 것을 제안해 1년 동안의 연구회기(Study Period on PIMS, personal information/privacy management)가 시작되었다. 이 연구회기를 마치고, 2012년 10월 로마 SC27 회의에서는 다음 사항을 합의했다.

- 개인정보보호 관리체계를 위한 기본 요구사항을 별도로 개발하지 않고 기존의 ISO/IEC 27001 표준을 이용함
- 섹터에 특화된 추가 요구사항이나 추가 보호대책에 대한 국제표준을 만들기 위한 템플릿을 개발하기 위한 국제표준 개발(ISO/IEC 27009, 한국에디터: 박태완)
- “개인정보 보호 지침”에 대한 국제 표준 개발(ISO/IEC 29151, 한국 에디터: 염흥열)

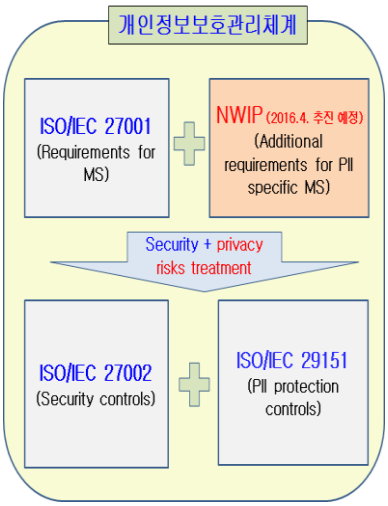
이 합의로 2012년 10월 로마 SC27 회의에서는 두 가지 신규워크아이템 제안(ISO/IEC NP 27009, ISO/IEC NP 29151)이 추진되었다. 2013년 4월 프랑스 SC27 회의에서 위의 두 가지 신규워크아이템이 채택되었다. 이와는 별도로 SC 27/WG 5에서는 ISO/IEC 27009 표준과 호환을 갖는 “개인정보보호 관리를 위한 ISO/IEC 27001 표준의 이용”이라는 문서를 SD5로 개발해

왔다. 2014년 4월 홍콩 SC27 회의에서는 두 공적 표준화 기구(ITU-T SG17, ISO/IEC SC27)가 각각 따로 개발되어 오던 “통신조직을 위한 개인정보보호 지침”인 ITU-T X.gpim과 “개인정보보호 지침”인 ISO/IEC 29151를 통합한 공통 표준(ITU-T X.gpim | ISO/IEC 29151)을 합의했다.

2015년 10월 SC 27/WG 5 회의에서는 ITU-T X.gpim | ISO/IEC 29151 표준을 2번째 위원회문서(CD)로 진행키로 합의했고, ISO/IEC 27009 표준을 최종드래프트국제표준(FDIS)으로 진행하기로 합의했다. 개인정보 보호 지침(ITU-T X.gpim | ISO/IEC 29151) 관련해 이번 회의에서 가장 중요 결정사항은 독일에 의해 제안된 “개인정보보호 정책의 이용”과 관련된 통제를 기존의 “정보보호 정책” 통제 이외에 별도로 두기로 합의한 점이다. 이외에도 한 NB가 개인정보 위험 평가를 수행하기 위해 먼저 필요성을 검토하고 그 이후 필요에 의해 개인정보 위험 평가를 수행하자는 제안을 했고, 이에 반해 다른 NB는 개인정보위험평가를 조건 없이 수행해야 한다고 주장했다. 토론 후 개인정보 위험 평가 필요성을 검토하고 필요 시 위험 평가를 수행하는 것으로 합의되었다.

이와는 별도로, 2015년 10월 SC27 회의에서는 ISO/IEC 27009에 근거해 “개인정보보호 관리체계를 위한 추가적인 요구사항”에 대한 신규워크아이템 제안을 프랑스, 한국, 독일, 인도 등이 추진했다. 그러나, 검토 시간이 필요하다는 의견을 반영해 다음 2016년 4월 미국 탬파 SC27 회의에서 신규워크아이템으로 추진하는 것으로 했다. 이 신규워크아이템 제안은 WG5에서 개발중인 SD5 문서에 근거하고 있다. 따라서 SD5 문서의 성숙도를 고려해 이 신규워크아이템은 3년의 표준 개발 기간이 아니라 1년의 표준 개발 기간을 갖는 신속 개발 과정으로 제안될 예정이다. 이 제안이 채택되면 이 신규워크아이템은 첫 번째 CD에서 시작됨을 의미한다.

개인정보보호 관리체계 구축을 위한 추가적인 개인정보보호 요구사항에 대한 신규워크아이템이 채택되면, 개인정보보호 관리체계 국제표준을 위한 전체 국제표준 집합은 <그림 1>과 같이 구성될 수 있다. 이 개인정보관리체계 국제표준화가 국내 개인정보보호 관리체계와 호환성을 가지며 한국 주도로 추진되었다는 점에서 매우 의미가 있다.



<그림 1> 개인정보관리체계를 위해 요구되는 국제표준 집합

향후 추진 전망

<그림 1>과 같은 모든 국제표준의 개발이 완료되면, 국내에서 2011년부터 운영되고 있는 개인정보보호 관리체계와 호환성을 갖는 모든 국제 표준 집합을 2018년까지 갖게 됨을 의미한다. 따라서 2018년이후에는 이 국제표준을 이용해 글로벌 차원의 개인정보보호 관리체계 인증도 시작될 수 있을 것으로 예상된다. 국내 개인정보보호 관리체계 인증 관련 전문가의 관심이 필요한 시점이다.

염흥열 (순천향대 교수, ITU-T SG 17 부의장, ITU-T SG 17 WP 3 의장, hyyoum@sch.ac.kr)