개인정보관리체계 구축 국제표준 개발 현황

염흥열 순천향대 교수, ITU-T SG 17 국제 의장

1. 머리말

조직의 개인정보보호 능력을 인증하기 위한 개인정보보호관리체계 인증 제도를 시행하고 있는 국가는 영국(BSI 10012 근거), 일본(프라이버시 마크 인증), 한국(ISMS-P) 등이다. 개인정보의 침해사고가 빈번하게 발생하고 있어 침해 위험을 제거하는 기술적, 관리적, 조직적 보호대책을 제공하는 개인정보보호 체계 구축이 절실히 요구되어 왔다. 그러나 정보보호관리체계와는 달리 개인정보보호관리체계를 위해 요구되는 모든 국제표준은 지금까지 없었다. 이번 2019년 4월 ISO/IEC JTC 1/SC 27/WG 5 회의에서는 ISO/IEC 27552(개인정보보호관리체계 구축을 위한 프로세스 요구사항과 가이던스) 국제표준이 IS로 진행하기로 결정되었다. 본고에서는 이러한 표준화 활동을 중심으로 한국의 노력을 중심으로 서술한다.

2. 주요 이슈 및 논쟁사항

정보보호관리체계(ISMS)는 ISO/IEC 27001(정보보호관리체계 – 요구사항)에 근거해 구축되고 운영되고 있다. 정보보호관리체계에서 요구되는 표준은 프로세스에 대한 요구사항에 대한 국제표준인 ISO/IEC 27001과 보안 통제에 대한 국제표준인 ISO/IEC 27002에 근거하고 있다. 그럼 개인정보관리체계 구축을 위해 필요한 국제표준은 무엇인가? 비슷하게 개인정보보호관리체계에서 프로세스의 요구사항에 국제표준과 개인정보보호를 위한 프라이버시 측면의 통제에 대한 국제표준이 필요하다.

한국은 2011년 10월 케냐 나이로비 회의에 개인정보보호관리체계 구축을 위해 필요한 국제표준을 개발하기 위한 연구회기(Study Period)를 제안했다. 1년간의 노력으로 2012년 10월 로마 WG 5 회의에서 개인정보보호 통제에 대한 ISO/IEC 29151(개인정보보호준칙)이라는 국제표준의 신규워크아이템제안(NWIP)으로 진행하기로 했다. 2013년 4월 회의 이후 첫 번째 WD가 발표되었고, 4년간의 개발 기간을 거쳐 2017년 4월 회의에서 국제표준으로 채택한 바 있다. 필자는 이 국제표준의 에디터를 역임하면서 9번의 WG 5 회의에서 여러 번 에디팅 세션을 주재한 바 있다.

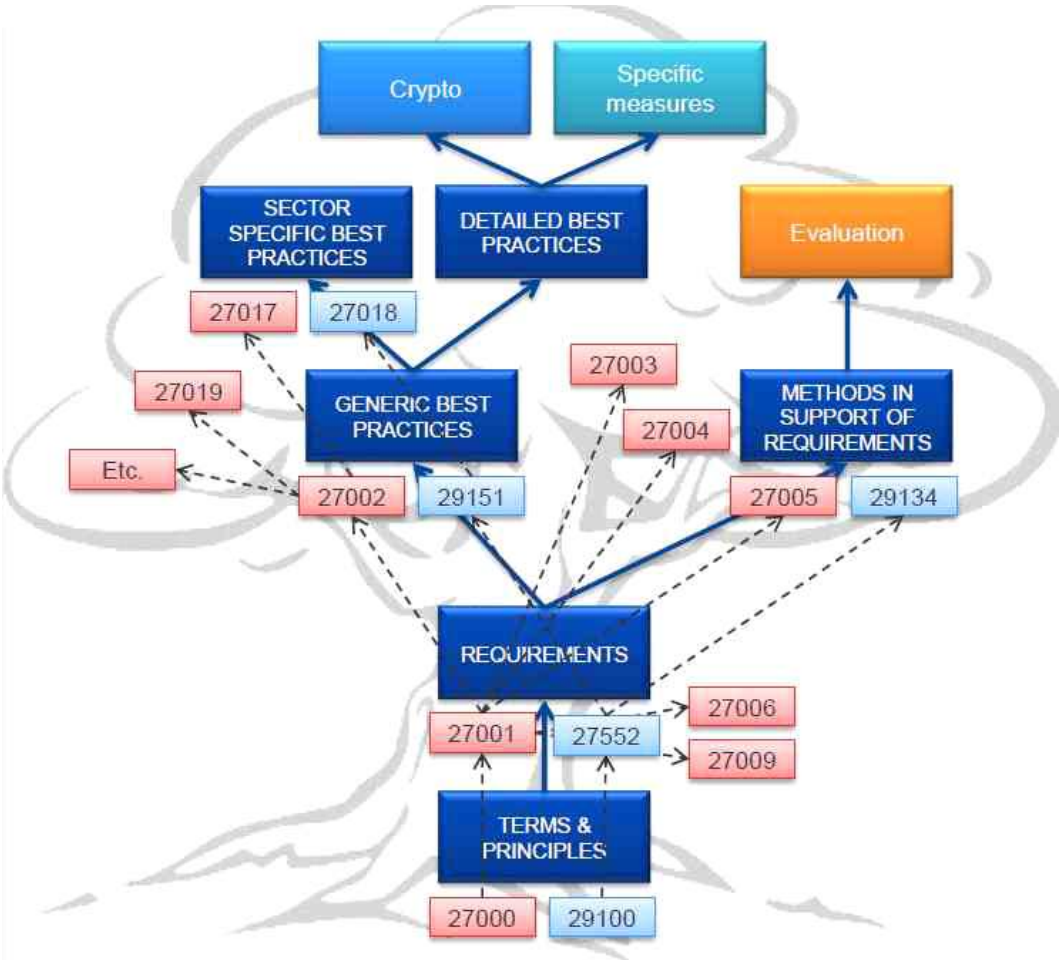
2016년 4월 WG 5 회의에서 개인정보관리체계 요구사항에 대한 국제표준인 ISO/IEC 27552에 대한 신규워크아이템 제안이 한국, 프랑스, 영국, 독일 등의 지지로 추진되었고 등록되었다. 2016년 10월 WG 5 회의에서 ISO/IEC 27552 신규워크아이템이 채택되었다. 필자는 영국 에디

터와 함께 코에디터로 선임되었다. 이 2016년 10월 WG 5 회의 이후 1차 WD가 발표되었으며, 2018년 10월 회의에서 DIS 상태로 진행하기로 했다. 2018년 10월 이후 4개월 동안 DIS 투표 반대의견이 제출되지 않아서 이번 텔아비브 SG 27/WG 5 회의에서 FDIS 상태 없이 바로 IS로 진행하기로 했다. 이번 텔아비브 회의에서 한국은 이 ISO/IEC 27552 국제표준과 기존 프라이버시 통제에 대한 ISO/IEC 29151과의 관계를 국가 코멘트로 제출해 수정반영한 바 있다.

정보보호관리체계의 보안 측면의 위험을 식별하기 위한 국제표준으로 ISO/IEC 27005를 이용할 수 있듯이, 프라이버시 측면의 위험 평가와 프라이버시 영향평가를 위한 국제표준으로 ISO/IEC 29134를 이용할 수 있게 되었다. 한국은 2013년 4월 ISO/IEC 29134 신규워크아이템이 채택되어 2017년 4월 국제표준으로 채택되었다. 필자는 독일 에디터와 함께 ISO/IEC 29134 국제표준의 코에디터로 선임되어, 9번의 에디팅 세션을 독일 에디터와 함께 주재한 바 있다.

따라서 한국은 개인정보관리체계 구축을 위한 3가지 국제표준(ISO/IEC 27552, ISO/IEC 29151, ISO/IEC 29134) 개발을 주도했다고 볼 수 있으며, 매 회의마다 한국의 개인정보보호 요구사항을 반영한 국가 코멘트를 제출해 반영한 바 있다.

참고로 정보보호관리체계 구축과 개인정보관리체계 구축을 위해 필요한 국제표준과 이들 표준과의 관계는 [그림 1]로 나타낼 수 있다.



※ 출처: CNIL, 데이터 규제기관의 국제표준화 활동, 2017.09.

[그림 1] 정보보호관리체계와 개인정보관리체계를 위한 국제표준 간 관계

3. 향후 추진 전망

이번 국제표준 채택으로 인해 글로벌 차원에서 개인정보보호관리체계 구축과 운영을 위한 국제표준의 개발이 완료되었다. 유럽 지역을 중심으로 유럽개인정보보호규정(GDPR)에서 요구되는 개인정보 요구사항을 보증하기 위한 인증 메커니즘에 필요한 국제표준으로 활용 가능하다. 먼저, 프랑스가 이 국제표준에 근거해 개인정보보호관리체계 인증 메커니즘을 운영할 가능성이 크며, 장차로 유럽 차원으로 확대될 가능성이 크므로, 국내에서도 이에 대한 대비가 필요하다.