[정보보호] 개인정보보호관리 관련 국제표준화 진행 현황

개인정보보호에 대한 사회적 요구에 대응하여 정부에서는 관련 정책 및 제도를 수립하고 있다. 특히 개인정보영향평가제도를 시행하여 정보시스템 구축 설계 시, 사전적인 개인정보보호 조치를 취하도록 하고 있는 것이 대표적 사례이다. 그러나 개인정보를 보유하고 있는 기관/조직의 운영 측면에서 개인정보의 수명주기 전체(수집, 이용, 보유, 제공, 파기 등)에 걸친 체계적인 개인정보보호 관리활동은 적절하게 수행되고 있지 않다. 즉, 개인정보보호 조치로 단편적인 기술적 솔루션(PET)의 설치 및 운영이 대부분을 차지하고 있으며, 개인정보보호를 위한 제반 관리 활동이 체계적으로 수행되지 못하고 있으며, 주기적 점검을 통한 개인정보보호 수준의 지속적 개선 노력에도 한계를 보이고 있다. 따라서 일상적인 관리활동의 하나로써 개인정보의 생명주기 전체를 대상으로 개인정보보호를 위한 기획, 구현, 점검, 개선 등 일련의 활동으로 구성된 개인정보보호관리체계(Personal Information Management System: PIMS)를 구축할 필요가 있다.

PIMS의 요구사항을 살펴보면, 1) 기업 내부의 정보를 보호하려는 통상의 정보보호와는 달리 개인정보보호는 이용자권리 보호를 위한 자기정보 결정권의 특성을 반영한 보호조치를 취해야 하고, 2) 이용자의 개인정보는 동의획득을 통한 수집부터 이용 및 제공, 저장 및 관리, 파기단계에 이르는 생명주기에 따라 관리되어야 하며, 3) 일회성의 평가를 통하여 현황을 파악하는 것이 아니라 지속적인 개인정보취급 현황에 따른 위험을 판단하고, 4) 국내 관련법 및 OECD, APEC 등의 국제적 개인정보보호원칙 등 법적 요구사항 내에서 허용 가능한 위험수준으로 개인정보를 관리하여야 한다. 5) 마지막으로 개인정보보호의 요구사항이 IT 유관부서뿐만 아니라 전사적으로 개인정보취급자에게 광범위하게 보호조치들을 이행하여야 한다는 특성을 반영해야 한다.

따라서 PIMS의 설계사상은 PIMS 요구사항을 반영하여 개인정보측면에서는 개인정보의 특성 반영과 함께 생명주기(lifecycle) 관리를, 관리체계측면에서는 지속적인 관리와 전사적 보호조치를, 인증 측면에서는 실행 가능한 통제·문서화와 유관 법령 준수를 원칙으로 설정하고 있다.

관련 해외동향을 살펴보면 영국에서는 PIMS 표준을 제정하여 사용하고 있다. 2009년 5월 31일 영국표준협회(BSI)는 개인정보관리 표준(BS 10012: 2009 Data Protection - Specification for a personal information management system)」을 제정하였다. 표준의 주요 내용으로는 공공 및 민간 부분의 모든 기관들이 「개인정보법(Data Protection Act)」을 준수하기 위하여 갖추어야 하는 개인정보관리체계(PIMS)에 대한 요건을 규정하고 있다. 즉 개인정보를 담당하는 직원들에 대한 훈련과 인식 제고, 위험 평가, 개인정보 공유절차, 개인정보의 보유 및 처리, 개인정보를

제3자에게 공개하는 것 등에 관한 지침을 포함하고 있다. 영국표준에 의한 인증은 국내에서 2012년 3월 현재 10개 업체가 인증서를 교부 받았다. 반면 일본에서는 1998년부터 JISQ 15001(일본표준: 개인정보관리체계(Privacy Management System)을 제정하였고 이를 기반으로 Privacy Mark 제도를 수행하고 있으며, 2012년 3월 현재 20,666 업체가 인증서를 획득하였다.

이러한 PIMS 인증제도가 국내에서 성공하기 위한 요건은 아래와 같이 정리할 수 있다. 첫째, PIMS가 자발적 인증제도이지만 효과적 인센티브 제공이 필요하다. 예를 들면, 일본의 ISMS 인증사례를 보면 전세계 인증서 발행의 50%를 차지하는 이유는 정부조달에서 가산점을 부여하는 등 적극적인 인센티브를 제공하고 있기 때문이다. 인센티브에 대한 설문조사에 의하면 가장 효과가 높은 인센티브로써 조세혜택과 정부조달에서 가산점 제공이었다. 둘째, PIMS와 유사제도인 ISMS와의 상호 인정체계를 구축하는 것이다. 개인정보에 대한 기술적, 물리적 보호조치는 ISMS에서의 통제영역과 상당부분 중복되고 있다. 중복된 통제에 대해서는 동일한 기준을 적용해야 할 것이며 인증결과에 대한 상호인정을 통해 인증신청기관의 부담을 덜 필요가 있다. 셋째, 개인정보를 다수 보유하고 있는 중소규모의 업체에 대한 컨설팅 비용부담 또는 교육 제공 등 정책적 지원이 필요하다. 인적 자원이 희소하고 경영마인드가 부족한 중소규모의 업체로서는 개인정보보호관리체계 수립이 현실적으로 매우 어려운 상황에 있다고 볼 수 있다. 인증취득을 원하는 중소규모의 조직에 대해서는 경제적 지원을 통해 개인정보보호의 취약지대를 최소화 할 필요가 있다. 마지막으로 PIMS 제도에 대한 교육 및 홍보를 통해 PIMS에 대한 올바른 인식을 가지도록 할 필요가 있으며 조속한 제도 정착을 도모해야 할 것이다.

이러한 PIMS 국제표준화를 위한 노력의 일환으로 2011년 8월에 개최된 ITU-T SG17 회의에서 한국이 제안한 “정보통신기업의 개인정보관리를 위한 지침” 작업이 신 프로젝트로 결정되어 본격적인 논의가 시작되었고 2011년 10월에 개최된 ISO/IEC JTC1 SC27 나이로비 회의에서 신규 프로젝트 결정을 위한 6개월의 Study Period가 결정되었다. 2012년 2월에 개최된 ITU-T SG17 회의에서는 경영시스템(MS)에 대한 표준화는 ISO 표준기구의 주요 업무이므로 2012년 5월에 개최되는 ISO/IEC SC27 스톡홀름 회의 결과를 보고 상호협력방안 및 표준화 계획을 논의하기로 결정되었다. PIMS Study Period를 위한 기고문을 분석하면 대부분의 기고문에서는 PIMS/PMS(Privacy Management System) 국제표준화에 대해서는 대부분 동의하고 있으나, 표준 프로젝트 구성 및 방법에 대해서는 상이한 의견을 보이고 있다. 즉, PIMS 요구사항을 포함하는 일련의 표준(3개의 표준 프로젝트)을 별도로 제정할 것인가 아니면 ISO 27001을 PIMS 요구사항 표준으로 사용하고 프라이버시 보호통제를 위한 별도의 표준을 제정할 것인가에 대한 결정이 주요 쟁점으로 대두되고 있다. 어떠한 구조가 되었든, 본격적인 PIMS/PMS 국제표준화 작업은 2012년 5월 스톡홀름 회의에서부터 시작될 것으로 예상되며, 국내의 PIMS 기준 및 경험을 반영하고 주도적인 국제표준화 활동을 위해서는 에디터 지원 등 한국의 적극적 대응이 필요하다.

김정덕 (중앙대학교 정보시스템학과 교수, jdkimsac@cau.ac.kr)