# [정보보호] ID 관리와 프라이버시 국제표준화 동향

ISO/IEC JTC1 SC27 WG5는 2006년 11월 남아공 Glenburn 회의에서 기존의 WG2에서 분리하여 새롭게 만들어진 Working Group으로 “Identity management(ID 관리)”와 “privacy technologies(프라이버시 기술)"를 주제로 프라이버시(privacy)에 관한 영역과 바이오인식(Biometrics)에 대한 내용을 다루고 있다. Published 된 표준은 일본에서 주도한 ACBio(Authentication Context for Biometrics) 하나뿐이다. 본 고에서는 이번 11월 미국 레드몬드에서 개최된 ISO/IEC JTC1 SC27 WG5 회의에서 논의된 주요 표준에 대해 살펴보기로 한다.

- ISO/IEC JTC 1/SC27 29100 : Privacy Framework

오늘날 모든 정보통신 시스템은 다양한 형태나 방식으로 개인 식별 정보(personally identifiable; PI)를 처리하고 있다. 그러나, 현존하는 정보보호 표준안 대부분이 개인이 자신의 정보를 통제할 수 있는 권리를 고려하지 않고 있으며, 개인정보의 프라이버시를 보호하기 위해 개인 확인 정보를 분류하고 시스템을 설치하는 일관적인 실행 방법을 포함하지 않는 경우가 많다.
개인 확인 정보의 상업적 이용의 증가와 법적 제도적 장치를 통한 개인정보의 공유, 정보통신 시스템의 복잡도 증가는 기업으로 하여금 고객의 프라이버시를 보호하고 다양한 프라이버시 규정을 준수하도록 요구하고 있다. 더욱이, 전자상거래가 활발해지면서 개인정보의 오용 증가에 따라 발생되는 특정 기업에 대한 고객의 불확실성이나 불신이 기업의 성공을 가로막는 중요한 장애 요소가 되고 있다.
이러한 사회, 경제적 현실에서 프라이버시의 표준화에 대한 요구는 계속하여 증대되고 있다. 전자상거래에 있어서 신뢰를 구축하는 것은 소비자의 개인정보가 프라이버시 관련 규정을 준수할 수 있게끔 처리하고 다루어질 수 있도록 보장하는 것뿐만 아니라 개인의 자기정보 통제권이 행사될 수 있도록 적절한 기술적 기능을 제공해 줄 수 있어야 한다. 본 프라이버시 표준안은 개인식별 정보를 처리하는데 있어 정보통신 기술 요구 사항에 대한 프라이버시 보호 가이드라인을 제시하는 것을 목표로 한다.

- ISO/IEC JTC 1/SC27 24760: A framework on identity management

신원관리(IdM)는 개체의 신분확인 관련 정보와 인증 과정에서의 신원정보의 안전한 관리라고 할 수 있다. 여기서, 개체(entity)는 유일하게 인식될 수 있는 사람, 동물, 디바이스, 물체, 그룹, 조직 등이다. 개체는 다수의 다른 상황에서 사용되는 다수의 신분(identities)을 가질 수 있다. 신분확인 과정은 어떤 조직 내에서나 또는 기관과의 연합체 내에서 사용될 수 있다. 본 표준안은 신원(identity)의 생명주기를 포함하고 신원정보가 만들어지고 수정되고, 종결되고, 저장되는 전

과정을 포함하고 있다. 신원관리 프레임워크는 신원 서비스를 포함하는 여러 IT 서비스와 연결될 수 있으며, 신원관리 시스템(IdM)은 신원정보를 만들어내거나 요구하는 다른 정보시스템과의 상호 연결이 필요하다.

신원관리는 신원의 절도나 신원 통제체계가 확립되지 않은 상황에서 그 중요성이 더해지며, 신원의 부인 방지나 불법유출 방지 보장하기 위해 다양한 상황에서 개인이나 기관에게 도움을 줄 수 있다. 사람들의 신원을 관리할 때, 신원관리의 구현은 프라이버시와 데이터보호 법률과 규정을 준수해야 하고, 프라이버시 정책과 신원관리 요구 조건이 상충할 때는 적절한 타협점을 가지고 적용 가능한 범위 내에서 이들 조건들을 체계화해야 한다. 또한, 신원관리 시스템의 디자인과 구조는 개인정보의 기밀성 보호를 위한 정보보안 통제를 갖추어야 한다.

- ISO/IEC JTC 1/SC27 24745 : Biometric Template Protection

바이오인식정보(biometric templates)의 생성과 이용에 관한 내용은 ISO/IEC JTC SC37의 19784 (BioAPI), 19785(CBEFF) 등의 문서에서 다루고 있다. 여기서, BioAPI는 바이오인식 시스템 구축을 위한 응용 프로그램 간의 인터페이스 표준에 초점을 두고 있으며, CBEFF는 BioAPI와 ISO 19092에서 기술된 공통의 자료구조를 기술하고 있다. 그러나 이러한 문서에서는 바이오인식정보에 대한 기밀성, 무결성, 프라이버시와 같은 요구 조건에 대해서는 기술하지 않고 있다.

표준에서 다루고자 하는 바이오인식정보는 개인을 식별할 수 있는 개인정보의 하나로 그 중에서도 가장 민감한 개인정보에 속한다고 할 수 있어서 그 보호 대책이 필요하다. 기밀성, 무결성, 가용성을 위한 다양한 요구조건 하에서의 바이오인식정보 보호 지침을 제공하는 것을 목표로 한다. 이를 위해 개인식별 정보와 바이오인식정보의 흐름을 정의하고 바이오인식 시스템의 보안 취약성과 그에 따른 대책을 기술하고자 하며, 특히 이들 개인정보의 기밀성과 무결성을 보장하기 위한 표준화된 암호화 기법 제시와 응용모델에 따른 프라이버시 및 보안 위협에 대해서도 기술한다.

**향후 추진 전망**

우리나라가 주도하고 있는 ISO/IEC 24745 - Biometric template protection(바이오 템플릿 보호) CD(Committee Draft) 문서에 대하여 2010년 4월 말레이시아 회의에 상정 후 표준안 제목을 Biometric template protection에서 본 표준에서 보호하려는 대상을 보다 포괄적으로 표현하기 위해 Biometric information protection으로 수정하기로 의결하였다. 또한, ITU-T SG17의 Q.10과 Liaison(협력문서)을 맺어 진행하고 있는 과제인 ISO/IEC Working Draft인 Entity authentication assurance에 대하여 효율적 표준화 추진을 위하여 ISO와 ITU-T 간의 공동 미팅이 제안되었다. WG5에서 한국은 범국가적인 개인정보 보호체계 고도화 사업을 지속적으로 모니터링하는 한편

Privacy-Enhancing Technologies(PETs) 등의 관련 기술에 대하여 프라이버시 아키텍처 등에 기고함으로써 지속적 활동이 기대된다.

신용녀 (한국은행 전자금융팀 과장, ynshin@bok.or.kr)