[정보보호] X.1051 개정과 분야별 정보보안 경영체계 인증을 위한 국제 표준화 동향

2015년 국제 표준화된 'ISO/IEC 27002에 기초한 클라우드 서비스를 위한 정보보안통제 실무규약' ITU-T X.1631|ISO/IEC 27017에 이어 ITU-T와 ISO/IEC JTC 1이 공동으로 개발하고 있는 ITU-T X.1051|ISO/IEC 27011 'ISO/IEC 27002에 기초한 통신조직을 위한 정보보안통제 실무규약'이 AAP 승인을 통과하고 FDIS 투표 단계에 들어섰다. 한편 ISO/IEC JTC 1 SC 27에서는 이러한 분야별 통제 표준들을 이용하여 분야별 인증을 부여할 수 있도록 하는 방법에 관한 표준인 ISO/IEC 27009 'ISO 27001의 분야별 응용-요구사항'이 FDIS 투표를 통과하여 IS 발표를 앞두고 있다. 그러나 ISO 27009는 방법을 제시할 뿐이고 실제 분야별 인증을 위해서는 추가적인 작업이 필요하다. ISO/IEC에서는 실제 분야별 인증에 사용할 수 있는 인증기준을 위한 추가적인 노력을 진행하고 있다. 본 보고서에서는 X.1051의 개정현황과 ISO 27009의 내용, 그리고 앞으로 진행될 표준화 작업에 대해 소개한다.

1) ITU-T X.1051|ISO/IEC 27011 개정 현황

개정의 배경

ITU-T X.1051은 ITU-T 내 보안 연구 그룹인 SG17 의 정보보안관리를 담당하는 Question3 의 기본 문서로 활용되고 있는 문서이다. 또한 이 문서는 ISO에서 IT 보안 기법을 담당하는 ISO/IEC JTC 1/SC 27과 공동으로 개발하여 ISO에서는 ISO/IEC 27011로 발표되었다. 첫 버전은 2008년도에 발표되었으며 2013년 기초가 되는 ISO/IEC 27002의 대대적 개정이 이루어짐에 따라 2013년부터 ISO와 공동으로 개정 작업이 개시되었다.

2016년 3월 ITU-T 회의에서 한국은 지난 ISO/IEC의 DIS 투표결과 처리회의(BCM, Ballot Consultation Meeting)의 결과 및 이에 반영된 변경을 소개하고, 추가적인 editorial comment를 기고하여 반영하였다. 이 텍스트는 사전채택(consent)으로 승인되었으며 4주간의 AAP call을 거쳐 ISO/IEC로 보내어 FDIS 투표를 진행할 예정이다.

개정된 내용

2008년 버전과 비교할 때 우선 구조의 변경이 가장 먼저 다가온다. X.1051은 ISO/IEC 27002에 기초하고 있어 ISO.IEC 27002의 구조를 따르고 있으며, 27002의 기본구조가 변경되었기 때문에 X.1051도 그에 따라 변경되었다.

내용적인 측면에서는 ISO 27002에 새롭게 추가된 통제에 대하여 통신조직에서 추가적으로 유의해야 할 구현방법 등을 추가하였으며, 그간의 통신 기술 발달에 따른 변경이 반영되었다. 한편 기존 X.1051에 있던 구현 방법에 관한 설명이 ISO 27002에 새롭게 포함된 부분들이 상당부분 중복을 제거하기 위하여 삭제되었다. 예를 들어 사고대응 절차에 관해서는 기존의 X.1051이 더 상세한 설명을 제공하고 있었는데 이 중 통신조직 뿐만 아니라 일반적으로 적용 가능한 부분들이 ISO 27002로 흡수되었다.

향후 진행 프로세스

ITU-T와 ISO 양쪽의 표준화 기구에서 동일한 내용으로 각각의 승인 프로세스를 통과해야 하기 때문에 A.23 'ITU-T와 ISO/IEC JTC 1 공동작업을 위한 지침'에 따라 먼저 ITU-T에서 승인 절차를 밟고 승인을 통과한 동일한 텍스트로 ISO에서 FDIS 투표를 통과해야 한다. 한국은 ITU-T와 ISO/IEC 양 측의 에디터(TCA서비스 오경희 대표)를 겸임하고 있어 본 표준이 두 기관에서 원활하게 최종 승인되어 국제표준으로 발표될 수 있도록 지원하고 있다.

2) ISO/IEC 27009 국제 표준화

배경

ISO/IEC 27001의 요구사항과 ISO/IEC 27002의 통제 및 구현 지침은 일반적이며 유형, 규모 또는 속성에 관계없이 모든 조직에 적용할 수 있도록 개발되었다. 비록 이 표준들이 영리 기업, 정부기관 및 비영리 기관을 포함하는 다양한 조직에서 광범위하게 받아들여지고 있긴 하지만, 분야별 표준에 대한 필요가 새롭게 부상하고 있다. ISO/IEC 27010, 27011, 27017, 27018 등 이미 ISO에서도 다양한 분야별 표준이 개발되었으며 다른 표준화 단체에서도 분야별 보안 표준을

개발하고 있다. 이에 따라 ISO에서는 기존 표준과 일관성을 유지하면서 분야별 요구사항을 반영할 수 있는 표준을 개발하기 위한 방법을 명시하기 위해 ISO/IEC 27009를 개발하게 되었다.

내용

ISO/IEC 27009는 어떤 특정 분야에서 ISO/IEC 27001를 적용하기 위한 요구사항을 정의한다. 즉 ISO/IEC 27001의 요구사항과 상충하지 않는 범위 내에서 분야별 적용을 위해 요구사항을 추가하거나, ISO/IEC 27001 요구사항을 상세화(또는 구체화, refined)하거나, 해석(interpreted)하는 방법을 설명한다. 또한 ISO/IEC 27001:2013의 부록 A에 대한 추가적인 통제 또는 통제 집합을 포함하는 방법을 설명한다. 즉 ISO/IEC 27002의 통제에 분야별 통제를 추가하거나 ISO/IEC 27002의 통제를 변경하는 방법을 제공한다. 변경되지 않은 ISO/IEC 27001 요구사항과 ISO/IEC 27002의 통제는 그대로 적용된다고 간주한다.

의의

ISO/IEC 27009의 표준화를 통해 ISO/IEC 27002 뿐만 아닌 다양한 분야별 표준에 기초하여 ISO/IEC 27001 인증을 받을 수 있게 된다. 기 개발된 표준들뿐만 아니라 개인정보보호, 에너지 등 다양한 분야의 정보보안경영 표준들이 개발되고 있으며 이는 분야별 인증 시장의 확대를 가져오게 될 것이다. 특히 MS 등 클라우드 서비스 업체들은 27009를 통해 ISO 27017에 따른 정보보안경영체계 인증을 받고자 이미 준비를 하고 있다.

3) 분야별 정보보안경영체계 인증

표준화 동향

그러나 앞서 설명한 바와 같이, ISO/IEC 27009는 ISO/IEC 27001의 분야별 적용을 위한 표준을 만드는 방법을 설명하는 표준으로서 이것만으로 바로 분야별 인증이 이루어질 수 있는 것은 아니다. 즉 기존의 분야별 표준들을 ISO/IEC 27009에 따라 변경하거나, 새로운 표준을 개발하여야 한다. SC 27에서는 2016년부터 이를 위한 기초연구(study period)로서 ISO/IEC

27009의 응용을 위한 유즈케이스 사례 개발을 개시하였다.

향후 전망

특히 ITU-T와 공동 개발한 X.1051|ISO/IEC 27011 및 X.1631|ISO/IEC 27017의 경우, 인증을 업무범위에서 제외하는 ITU-T 정책에 따라 해당 표준의 변경은 고려대상이 되지 않는다. 따라서 ISO/IEC 27009에 따른 통신 분야 또는 클라우드 분야의 인증을 위해서는 해당 표준에 기초한 새로운 표준 또는 문서를 ISO에서 단독으로 개발해야 한다.

한국은 ISO에서 이루어지는 통신 분야의 인증을 위한 문서 개발에 적극적으로 참여할 예정이다.

오경희(TCA서비스 대표, khoh@tcaservices.kr)