情 報 保 護 學 會 誌
第18卷 第4號, 2008. 8

ISO/IEC JTC1 SC27의 정보보호관리 국제표준화 동향

김 정 덕*, 이 경 석**

요 약

정보보호관리체계(Information Security Management System : ISMS)는 조직의 정보자산에 적합한 수준의 보호를 제공하고, 원하는 보호수준을 지속 가능하게 할 수 있을 뿐만 아니라, 인증을 통하여 정보보호에 대한 신뢰를 제공하는 등 다양한 이점을 제공한다. 현재 정보보호관리체계에 대한 국제표준은 어느 정도 안정화 단계에 접어든 상태이고, 향후에는 정보통신, 전자정부 등 기반시설을 포함하는 섹터별 정보보호관리체계 수립에 대한 표준화 작업이 본격적으로 수행될 것이다. 본 논문에서는 ISO/IEC SC27 WG1에서 수행하는 정보보호관리체계에 대한 국제표준화 동향을 살펴보고, 정보보호 거버넌스 등 새로운 국제표준화 항목에 대해서 소개한다.

정보보호는 기술적인 측면을 포함한 인적, 관리적, 경영적인 현안이며 조직의 경영이 그러하듯이 완벽한 정보보호는 기대하기 어렵다. 급변하는 경영 및 기술적 환경하에서 할 수 있는 최선의 방법은 해당 조직이 당면하고 있는 정보자산의 위험을 적절히 관리하기 위해 정보보호관리체계(Information Security Management System : ISMS)을 수립하고 이를 지속적으로 운영, 유지하는 것이다.

ISMS 수립을 통해 다음과 같은 이점을 기대할 수 있다. 첫째, 정보보호 대책을 관리체계 없이 구현하였을 경우, 그 대책의 보호 수준이 시간이 갈수록 저하하는 경향이 있다. 정보보호 제품은 일반적으로 도입 시 효과가 가장 높고 시간이 갈수록 그 효력이 떨어지게 된다. 예로서 항바이러스 제품의 경우 도입 후 업데이트를 수행하지 않으면 일주일도 안 되어 새로운 바이러스에 걸릴 수 있다. 그러나 정보보호관리체계를 수립한 경우 대책의 관리를 통하여 원하는 보호수준을 지속적으로 유지할 수 있다.

둘째, 조직의 정보자산에 적합한 수준의 보호를 제공할 수 있다. 정보보호관리체계는 초기에 분석과 계획을 실시함으로써 보호대책을 지나치게 구현하여 발생하는 비용을 감소시키는 한편 중요 자산을 적절히 보호하지 못하여 발생하는 위험을 막을 수 있다. 정보보호관리체계를 통해 조직은 자신의 정보자산을 조사하고 이 자산에 존재하는 위협과 취약성, 그리고 그로 인한 영향을 평가하여 적절한 보호를 수립하고 관리한다. 이러한 분석과 계획 없이는 무작정 새로운 보호대책을 도입하면서도 정작 중요한 자산에 대한 적절한 대책을 마련하지 못하여 피해가 발생할 수 있다. 즉, 정보보호관리체계의 수립과 운영을 통해 보안사고로 나타날 수 있는 자산의 피해와 이에 필요한 보호대책에 대한 투자비용 간의 균형을 맞출 수 있다.

셋째, 정보보호관리체계의 수립은 정보보호관리체계 인증의 토대가 될 수 있다. 정보보호관리체계를 수립하고 이에 대한 객관적인 제3자의 인증을 받아 홍보하게 되면 고객, 주주, 거래 파트너에게 정보보호에 대한 신뢰를 제공하고 우수고객을 유치하는 발판으로 삼을 수 있다.

넷째, 내부적으로 지속적인 정보보호관리체계를 갖춤으로써 정보보호 관련 기술 및 노하우를 조직 내부에 축적할 수 있다. 이러한 축적된 지식은 장기적으로 사고에 적시 대응할 수 있는 능력을 갖추게 되어 피해를 감소시킬 수 있다.

다섯째, 이렇게 체계화된 형태의 정보보호는 단순한 기존 정보자산의 보호뿐만 아니라 새로운 사업 자체를 가능하게 해주는 긍정적인 기반요소가 될 수 있다. 과거

* 중앙대학교 (jdkimsac@cau.ac.kr)
** 숭실대학교 (2008kslee@gmail.com)

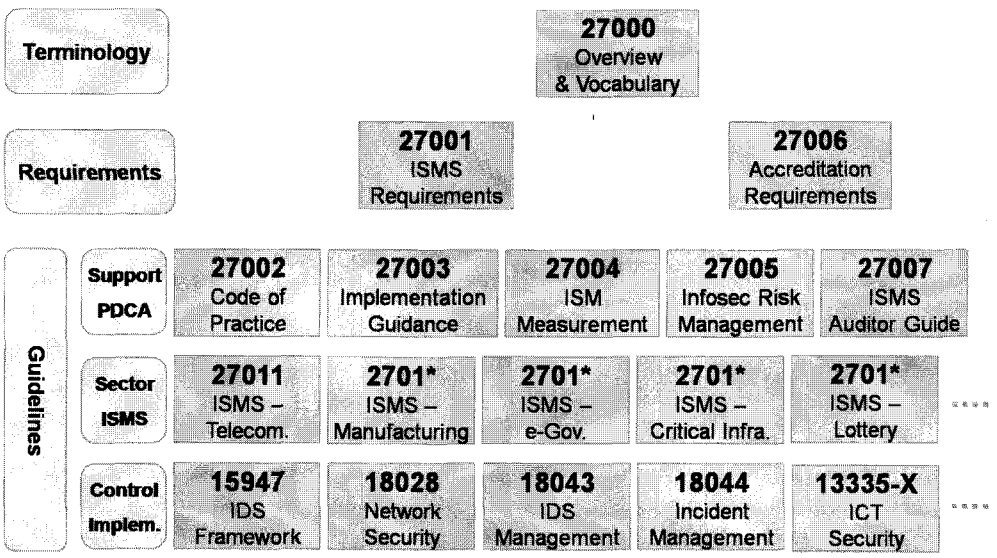
에는 정보보호가 단순히 최소화해야 하는 비용 요소로 간주되었다. 그러나 현재와 같이 인터넷을 통해 새로운 사업이 전개되고 관련 정보를 생성, 전송, 처리하는 상황에서는 정보보호가 고려되지 않고서는 인터넷 상의 각종 위협이 너무 크기 때문에 정보보호를 비용 요소로 간주하고 최소화시킨다면 차후에 발생하는 데이터 변조 및 삭제, 부정 거래 등의 위험을 감당할 수 없게 된다. 정보를 보호하기 위한 고려 없이 진행되는 인터넷 기반의 사업 프로세스는 그 사업이 성공적일 수록 더 많은 부정의 유혹을 불러 일으켜서 언젠가 보류해 두었던 비용을 치르게 될 수 있다.

이러한 정보보호관리체계에 대한 국제표준화는 [그림 1]과 같이 ISO/IEC SC27 WG1에서 수행하고 있으며 ISO 27000시리즈라는 일련의 표준이 바로 그것이다. 즉, ISO 27000시리즈는 정보보호를 단순히 기술적 이슈로 보는 것이 아니라 기술, 물리, 관리적 통제들을 포함하는 전사적 차원의 정보보호를 구현하기 위한 체계화된 일종의 경영시스템으로 보는 것이다. 즉 IS 9000 시리즈 (품질경영시스템)나 14000 시리즈 (환경경영시스템)와 같이 하나의 경영시스템으로서 정보보호를 계획, 구현, 유지보수 및 검토, 지속적 개선 등과 같은 일련의 프로세스로서의 활동을 중요시 하는 점이 기존의 정보보호 노력과 차이를 보이는 것이다.

최근 ISMS에 대한 국제표준화 작업이 안정화되면서 새로운 국면을 보이고 있다. 2005년에 ISMS 요구사항을 포함하는 문서인 ISO 27001과 ISMS 구현을 위한 정보보호 통제를 포함하는 ISO 17799 (2007년 이후 27002로 변경)이 국제표준으로 발표되었고 ISMS 인증기관을 인정하기 위한 요구사항을 포함한 문서인 ISO 27006이 2007년도에 국제표준이 되면서 주요 요구사항을 포함한 표준들이 국제표준화에 성공하였다. 이에 따라 현재는 1) 전체 시리즈의 개관을 보여주는 마케팅 문서인 27000과, 2) 27001에서 규정하고 있는 PDCA (Plan-Do-Check-Act) 사이클에 관한 지침 성격의 27003, 27004, 27005, 27007 등 4개 문서와 3) 섹터별 ISMS 최초의 문서인 ISO 27011"정보통신조직을 위한 정보보호관리"외 다수의 프로젝트가 진행 중이다.

지난 4월 중순 일본 쿄토에서 열린 SC27 WG1 36차 회의에서의 국제표준화 작업 동향을 요약하면 다음과 같다[표 1 참조]. ISO 27000(Overview & vocabulary)은 ISMS 관련 표준문서의 구조와 상관관계를 보여주며 공통적으로 사용하는 82개의 용어 정의를 포함한 문서로서 회의 당시 3rd CD상태였으며 차기 회의에서 FCD로서 결정되고, 2009년도에 국제표준으로 발표가 될 예정이다.

ISO 27003(Implementation guidance)은 ISMS 구현을 위한 프로젝트 수행 시 참고할 만한 구체적인 구현 권고사항을 규정한 규격으로, 문서구조를 프로젝트 관리 프로세스에 맞추어 작성하고 있다. 지난 회의에서는 WD(Working Draft) 상태이나 새로운 문서구조 하에



[그림 1] ISMS (ISO 27000 시리즈) 국제표준화 동향

어느 정도 안정화가 되었으므로 차기 회의에서는 CD(Committee Draft)로 될 예정이다.

ISO27004(Measurement)은 ISMS와 구현된 정보보호 통제의 유효성(Effectiveness)을 측정하기 위한 프로그램과 프로세스를 규정한 규격으로 무엇을, 어떻게, 언제 측정할 것인지를 제시하여 정보보안의 수준을 파악하고 지속적으로 개선시키기 위한 문서이다. 지난 회의에서는 3rd WD이었으며 차기 회의에서 FCD로서 결정되고, 2009년도에 국제표준으로 발표가 될 예정이다.

ISO 27005(Risk management)는 위험관리 과정을 환경설정, 위험평가, 위험처리, 위험수용, 위험소통, 위험모니터링 및 검토 등 6개의 프로세스로 구분하고, 각 프로세스별 활동을 input, action, implementation guidance, output으로 구분하여 기술한 문서로 지난 회의 당시 FDIS 상태이며 차기 회의 시에는 국제표준으로 발표될 예정이다.

이렇게 주요 요구사항을 포함하는 문서가 2005년도에 국제표준으로 발표되었고 주요 지침을 포함하는 문서가 2009년도에 국제표준으로 발표되게 됨에 따라, 이를 바탕으로 섹터별 정보보호관리 관련 표준작업이 새롭게 진행되고 있다.

지난 회의에서 표준화 연구검토 단계였던 "주요기반시설(CI : Critical Infrastructure) 보안관리"가 대부분 참여국의 찬성을 통해 새로운 표준화 프로젝트(Information security management: sector to sector interworking and communications for industry and government)로 결정되었고, 에너지 등 주요 섹터별 보안관리 지침 작업도 시작되었다.

"전자정부서비스 보안관리" 프로젝트도 새로운 표준화 항목으로 결정되었고, 이에 대해서도 한국의 전자정부 보안 경험 및 활동을 토대로 적극적 역할 수행을 약속하였다.

"정보보호 거버넌스" 국제표준화 프로젝트 제의(캐나다)에 대해 연구검토 기간을 가지기로 하였으며 중앙대 김정덕 교수가 의장으로서 역할을 수행하게 되었고 차기 회의에서 새로운 표준화 항목으로 결정될 경우, 선임 에디터가 될 예정이다.

이상과 같이, ISO SC27에서 ISMS 국제표준화 활동이 본격화되고 있음을 확인할 수 있었다. 주목할 만한 동향은 전반적인 ISMS 표준이 안정화 단계에 접어들면서 국가기반시설 및 전자정부 등을 포함하는 섹터별 정보보호관리체계 수립에 관한 표준화 작업이 활발하게 진행될 것이며, 정보보호를 위한 거버넌스 표준화 작업이 시작된 점을 지적할 수 있다.

〔표 1〕 ISO/IEC JTC1 SC27 WG1 정보보호관리시스템 국제표준화 동향

ISO 과제 번호	제목	표준화 진행상태	
		제35차('07.4)	제36차('08.04)
ISO/IEC 27000	Overview & vocabulary	3rd CD	FCD
ISO/IEC 27001	Information security management systems requirements	IS (2005년 10월)	IS (2005년 10월)
ISO/IEC 27002	Code of practice for information security management (ISO/IEC 17799)	IS (2007년 4월)	IS (2007년 4월)
ISO/IEC 27003	ISMS Implementation guidelines	FWD	1st CD
ISO/IEC 27004	ISMS measurement	3rd CD	FCD
ISO/IEC 27005	Information security risk management	FDIS	IS (2008년 6월 예정)
ISO/IEC 27006	Requirement for the accreditation of bodies providing certification of ISMS	IS (2007년 2월)	IS (2007년 2월)
ISO/IEC 27007	ISMS auditor guidelines	1st WD	2nd WD
ISO/IEC 27011	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002(x.1051/27011)	FDIS	IS (2008년 6월 예정)
ISO/IEC 2700?	Information security governance		Study Periods
ISO/IEC 2700?	Information security mgmt for Sector to Sector Interworking and communications for industry and government	Study Periods	NP
ISO/IEC 2700?	Information security for e-government services	Study Periods	NP

참고문헌

[1] ISO 27001, "Information Security Management Systems Requirement", ISO/IEC, 2005

[2] ISO 27002, "Code of Practice for Information Security Management", ISO/IEC, 2007.

[3] Solm B, "Information Security_The Fourth Wave", Computers and Security, Vol. 25, pp. 165-168, 2006.

〈著者紹介〉

김 정 덕 (Kim Jungduk)
정회원

1991년 2월 : Texas A&M Univ 박사
1986년 5월 : Univ. Carolina 석사
1979년 2월 : 연세대 학사
<관심분야> 정보보호 거버넌스, 정보보호 관리, IT 감사, 정보시스템의 전략적 응용

이 경 석 (Kyung-Seok LEE)
종신회원

1986년 12월 : Univ. Paris 7 박사
1981년 8월 : 성균관대 석사
1978년 2월 : 숭실대 학사
<관심분야> 암호이론, 보안정책, 보안표준, 보안관리