정보통신망법 정보보호 관리체계와 ISO/IEC 27001:2013 ISMS의 차이점 분석 (Gap Analysis) 연구

오익균*, 신승중**
*한세대학교 대학원 IT융합학과, 한국과학기술원 사이버보안연구센터
**한세대학교 대학원 IT융합학과 교수
e-mail: oik123@kaist.ac.kr, expersin@hansei.ac.kr

A Gap Analysis between ISO/IEC 27001:2013 ISMS and KISA ISMS

Ik-Kyoon Oh*, Seung-Jung Shin**
*Graduate School of IT Convergence, Hansei University, KAIST CSRC
**Graduate School of IT Convergence, Hansei University

요 약

개정된 정보통신망법 정보보호 관리체계에 대해 민간, 공공기관들의 관심과 인증을 준비하는 조직이 늘어나고 있다. 의무 인증대상자가 대. 중견기업, 비(非) 정보통신서비스 사업자로 확대되고 국제표준 요구사항의 일부 인정이 가능해지며 ISO/IEC 27001:2013과 정보보호 관리체계에 대한 동시 인증을 효과적으로 추진하기 위한 가이드라인이 필요하다. 본 연구에서는 '정보보호 관리체계'(ISMS)의 요구사항, 통제항목 및 심사 과정에서의 차이점 분석(gap analysis)을 통해, 국제표준과 국내 법령에 적합한 ISMS를 효과적으로 구현할 수 있도록 한다.

1. 서론

Information Security Management System(ISMS)는 조직의 정보자산을 보호하기 위한 정책, 절차, 지침을 수립하고 이와 관련된 자원 경영과 적절한 통제 활동을 관리하는 체계이다.[1] ISMS는 정보통신방법은 '정보보호 관리체계'[4], 한국산업표준으로 '정보보호 경영시스템'[8] 또는 '정보보안경영시스템'으로 표현하기도 한다.

ISMS는 조직에 내재된 정보보안 위험을 관리하기 위해 정보자산 식별과 위험평가를 거쳐 적정한 보안수준을 유지하도록 통제하며, 고객부터 직원에 이르는 이해관계자에 대한 보안 요구의 반영과 지속적 개선을 이루고, 관계된 법령과 규정, 기준, 계약 준거성을 확보할 수 있는 거버넌스, 위험, 컴플라이언스 플랫폼(GRC platform) 이다.

정부는 2013년 '정보통신망법'[4] 일부개정을 통하여 정보보호 관리체계 인증기준을 조정하고, '1. 정보통신망서비스 제공자, 2. 집적정보통신시설 사업자, 3. ① 정보통신서비스 부문 전년도 매출액이 100억원 이상인 자 ② 전년도 말 기준 직전 3개월간의 일일평균 이용자 수가 100만명 이상인 자'를 인증 의무대상자로 지정하였다.

또한, 2016년 동법 시행령 일부개정령안[5] 의결을 통하여 동년 6월 2일부터는 정보보호 관리체계 인증 대상자를 '매출액 또는 세입 등이 1,500억원 이상인 자로 가. 의료기관, 나. 금융회사, 다. 전년도 말 기준 직전 3개월간의 일일평균 이용자 수가 1만명 이상인 자'로 비(非) 정보통신서비스 사업자까지 확대하여 규제할 예정이다.

함께 의결된 동법 시행규칙 일부개정령안[6]에서는 '유효한 인증기관으로부터 동일한 범위의 국제표준 정보보호 인증, 즉 정보보호경영시스템(ISO/IEC 27001) 인증을 받은 경우 정보보호 관리체계 인증심사의 일부를 생략할 수 있게 되었다. 그러나 ISMS 국제표준과 국내 인증기준간의 명확한 차이점과 특성이 충분히 인지되고 있지 않다.

본 연구에서는 ISO/IEC 27001:2013 국제표준과 개정된 '정보통신망법' 및 동 법에 따른 '정보보호 관리체계 인증기준에 관한 고시'[8]의 요구사항, 통제항목 및 심사 과정에서의 차이점 분석(gap analysis)을 통해, 국제표준과 국내 법령에 적합한 ISMS를 효과적으로 구현할 수 있도록 한다.

2. 선행 연구

2.1 ISO/IEC 27001:2013 ISMS 특성

ISO/IEC 27001 ISMS(정보보안경영시스템)은 ISO 9001 QMS(품질경영시스템), ISO 14001 EMS(환경경영시스템), ISO/IEC 20000 ITSM(IT서비스경영시스템)와 같은 주제별 표준의 하나이다. 또한 ISMS를 통신, 금융[10], 의료, 교육 등 업종별 특성에 따라 현장 적용하기 위한 실행사례, 지침, 파생표준 등 27001 family들이 개발되고 있다.

2013년 대폭 개정된 ISMS 요구사항 구조인 HLS(High Level Structure)[9]는 향후 ISO에서 제정하는 모든 경영시스템이 동일한 구조를 갖으며, 위험관리(Risk Management) 원리는 ISO 31000[11]을 참조하도록 한다. 따라서 조직은 주제별 ISO 경영시스템의 요구에 대한 적합성(conformity) 유지와 효과적인 통합적인 경영이 가능

하게 되었다.

개정된 ISMS 부속서(Annex)의 정보보안 통제영역, 통제목적, 통제항목은 ISO/IEC 27002:2013 ISMS code of practice[3] 해설서와 각 쌍을 이루고 있어 ISMS 구현에 필요한 정보보안 위험처리를 위한 점검, 평가를 위한 템플릿으로 활용되고, 이를 정량화하여 정보보안 수준측정 및 효과성 평가, 인증심사 및 컨설팅에 응용되고 있다.

ISO/IEC 27001:2013 ISMS는 조직의 유형, 규모에 관계없이 일반 조직의 정보보안 경영을 위해 적용하며, 표-1과 같이 (1) 표준 개요 및 조직의 상황 (정보보안 요구/기대치 및 범위, 지속적 개선), (2) 정보보안 경영시스템의 6단계 프로세스 22개 요구사항, (3) 14개 정보보안 통제영역, 35개 통제목적, 114개 통제항목으로 구성된다.

<표 1 ISO/IEC 27001:2013 ISMS 요구사항>

ISO/IEC 27001:2013 ISMS 요구사항

1. 적용범위 Scope	
2. 인용표준 Normative reference	
3. 용어 및 정의 Terms and definitions	
4. 조직의 상황 Context of the organization	
경영시스템(관리체계) 프로세스	정보보안 위험처리 통제항목
5. 리더쉽 Leadership	A.5 정보보안 정책 Information Security Policies
6. 계획 Planning	A.6 정보보안 조직 Organization of Information Security
7. 지원 Support	A.7 인적자원 보안 Human resource security
8. 운영 Operation	A.8 자산 관리 Asset management
9. 성과 평가 Performance Evaluation	A.9 접근통제 Access control
10. 개선 Improvement	A.10 암호화 Cryptography
	A.11 물리적 환경적 보안 physical and environmental security
	A.12 운영 보안 Operations security
	A.13 통신 보안 Communications security
	A.14 시스템 도입, 개발 및 유지보수 System acquisition, development and maintenance
	A.15 공급자 관계 Supplier relationships
	A.16 정보보안 사고관리 Information security incident management
	A.17 업무연속성관리의 정보보안 Information security aspects of business continuity management
	A.18 준거성 Compliance

2.2 정보통신망법 정보보호 관리체계 특성

정보통신망법에 따른 '정보보호 관리체계' 인증기준은 최초 2001년 제정되어 2013년 개정안[7]을 고시하였다. 정보통신망법 목적에 명시된 '정보통신서비스를 이용하는 자'를 위한 '정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합 관리체계'이다.

2001년 민간 정보통신서비스 사업자를 대상으로 시작되었으나 2010년 전자정부 정보보호 관리체계(G-ISMS)가 통합되며 공공부문으로 확대되었고 2016년 대폭 개정되며 비(非) 정보통신서비스 제공자까지 포함되었다. 인증기준 프레임워크는 개인정보보호 관리체계(PIMS), 정보보호준비도 평가기준으로 파생되었다.

2013년 개정된 인증기준은 표-2과 같이 정보보호 관리과정, 정보보호대책(통제) 등 104개 인증기준을 갖는다.[7] 또한, 통제항목별 세부점검항목으로 446개 항을 부가 제시하고 있다. 이는 당시 진행 중이던 ISO/IEC 27001 개정 작업안의 검토를 통해 관리과정에 반영하고 DDoS, 무선 네트워크, 스마트워크 보안 등 새로운 ICT를 고려하였다.

<표 2 정보보호 관리체계 인증기준>

정보보호 관리체계 인증기준 (정보통신망법 제18조 관련)

정보보호관리과정 요구사항	정보보호대책 통제분야
1. 정보보호정책수립 및 범위설정	1. 정보보호 정책
2. 경영진 책임 및 조직구성	2. 정보보호 조직
3. 위험관리	3. 외부자 보안
4. 정보보호대책 구현	4. 정보자산 분류
5. 사후관리	5. 정보보호 교육
	6. 인적 보안
	7. 물리적 보안
	8. 시스템 개발 보안
	9. 암호 통제
	10. 접근 통제
	11. 운영 보안
	12. 침해사고 관리
	13. IT 재해복구

2.3 특성에 따른 시사점

ISO/IEC 27001:2013 ISMS는 정보보안 경영 국제표준으로 조직의 비즈니스에 필요한 품질경영(ISO 9001), IT서비스경영(ISO/IEC 20000), 사이버보안(ISO/IEC 27032), 사업연속성경영(ISO 22301), 위험관리(ISO 31000) 구현과 더불어 통합된 글로벌 스탠더드를 이루고자 한다.

정보보호 관리체계는 국내 정보통신망법에 근거한 인증의무대상자에 대해 인증심사하기 위한 기준으로, 개인정보보호법, 중소기업 기술보호법 준수를 위한 또 다른 관리체계와 연계하며 정보통신서비스 업종(사업자)의 제한을 넘어 금융, 의료, 교육 업종에 대한 정보보호관리 전문성 추구와 국가표준 프레임워크화를 추구하고 있다.

ISMS와 정보보호 관리체계의 요구사항과 인증심사 전개는 매우 유사하며 특히 통제항목은 관점과 기준치 차이는 있으나 통제 목적과 취지는 대동소이하다. 조직이 ICT와 밀접하거나 정보통신관련 업종이면 정보보호 관리체계 인증기준에 맞춰 지며 일반 업종의 조직일 경우 기존 경영 환경에 정보보안관리를 위한 ISMS를 채택하게 된다.

3. Gap 분석 결과

3.1 ISMS 요구사항과 정보보호 관리체계(가. 정보보호관리과정) 비교

ISMS는 미국 NIST SP 800-13[12] 표준과 같이 비즈니스 프로세스의 보안에 주안점을 두고, 조직 전반의 정보보안 위험과 유관된 영역 통제, 보안 활동을 위한 경영시스템이다. 정보보호 관리체계는 인증심사 범위내 정보통신망 환경의 정보자산 위험관리를 기반으로 정보보호 대책이 수립되고 지속적 통제가 이뤄지는 지 심사하는 기준이다.

ISMS는 조직 상황에 대한 이해를 요구하며 이를 기반으로 정보보안 프로세스를 경영(관리)하는 ISMS를 적용하도록 하며, 타 ISO 경영시스템과의 통합된 체계를 권고한다. 정보보호 관리체계에서는 조직 또는 인증심사 대상

영역에 대해 인증심사 신청시 사전 문서심사를 하며 정보보호 정책과 범위 설정에 적합하게 반영되도록 요구한다.

ISMS는 최고경영진에게 정보보안 리더쉽으로서의 기능과 역할, 의지를 구체적으로 요구하며, 정보보안 정책 수립과 정보보안 책임과 권한(R&R) 부여를 경영 행위로 본다. 정보보호 관리체계는 최고경영진이 국내 법령이 정한 '정보보호최고책임자' 지정 등 준거성과 정보보호 조직과 자원 확보를 통해 이러한 활동 지원을 보장하도록 한다.

ISMS는 계획단계에서 조직의 위험과 기회 파악, 정보보안 위험평가 및 처리, 정보보안 목표 수립과 달성 계획을 수립을 요구한다. 정보보호 관리체계는 관리적, 기술적, 물리적 법적 분야 등 조직 정보보호 전 영역에 대한 위험식별 및 평가, 위험관리 계획 수립, 정보보호 대책 선정 및 이행, 효과적 구현, 내부 공유 및 교육을 요구한다.

ISMS 개정판은 특히 위험과 기회에 관한 대응 조치를 반복적으로 강조하며, HLS에 따라 조직의 ISMS 지원, 문서화된 정보, 프로세스 운영 및 구현, 통제, 성과 평가와 내부감사, 경영진 검토를 통한 지속적 개선을 요구한다. 정보보호 관리체계는 법이 정한 의무사항 준수, 운영현황 관리 및 문서화, 정기적 내부감사, 사후관리를 요구한다.

3.2 ISMS 통제항목과 정보보호 관리체계(나. 정보보호대책) 비교

ISMS 부속서의 정보보안 통제항목은 필수 적용이 아닌 정보보안 위기관리를 위한 점검 또는 대책을 위한 '참조 템플릿'으로, 세분화된 통제영역과 통제항목 그룹들마다 통제의 목적을 두며 이를 달성하는 다양한 구현 인정과 함께 통제 적합성을 부여한다. 업종별 ISMS 실행사례, 가이드라인 등 ISMS family를 통해 적용성을 보완한다.

정보보호 관리체계의 '나. 정보보호대책 통제분야'는 '가. 정보보호관리과정 요구사항'과 동등한 필수 인증기준이다. 인증심사에서도 정보보호대책 통제사항과 내용을 통제항목으로 규정된 세부점검사항에 대한 결함(적합성) 여부를 심사한다. 개정판에서 법령에서 정한 조직의 경영진 책임을 강화하고 있으며 기술적 정보보안 통제가 강조된다.

3.3 ISMS 요구사항과 정보보호 관리체계 인증기준 비교

일반적으로 비교하는, ISO 경영프로세스의 요구사항을 제외한 ISMS 통제항목 114개와, 경영프로세스 요구사항에 준하는 가. 정보보호 관리과정이 포함된 정보보호 관리체계에서의 104개 인증기준으로 한 수량(數量)적 요구사항 비교는 의미가 없다. 또한, 정보보호 관리체계의 446개 세부점검항목 역시 인증심사 또는 컨설팅에서의 참고사항으로 상호 인정 여부를 검토할 때 제약 받을 필요가 없다.

정보보호 관리체계 가. 관리과정 인증기준에서 보면,

□ 1. 정보보호 정책 수립, 범위 설정에 관한 요구 내용은 유사하다. 다만, ISMS에서는 '5. 리더쉽'을 조직 보안 활동과 책임의 주체로 요구하고 있다.

□ 2. 경영진 참여와 정보보호 조직의 구성과 활동에 관한 요구 내용은 유사하다. 특히 '정보보호 최고책임자'라는 법적 용어를 사용하고 있다. ISMS '7. 지원'의 일부 요구사항을 포함하고 있다.

□ ISMS와 달리 3. 위험관리를 별도로 구성하여 위험관리 방법 및 계획, 식별 및 평가, 대책 선정 및 이행을 요구한다. ISMS에서는 '6. 계획'의 정보보안경영시스템 계획 및 수립단계에서 위험과 기회에 관한 평가, 처리, 정보보호 목표 및 달성계획을 수립하도록 요구한다.

□ 4. 정보보호대책의 효과적 구현과 내부 공유, 교육에 관한 인증기준은 ISMS '7. 지원' 요구사항과 유사하다.

□ 5. 사후관리에서 법적 요구사항 준수 검토, 문서를 통한 운영현황관리, 내부감사를 요구하고 있으며, ISMS에서는 '7. 지원'에서 문서화된 정보의 생성, 갱신, 통제, '8. 운영'에서 정보보안 프로세스 운영계획 및 통제, '9. 성과 평가'에서 모니터링, 측정, 분석, 평가 및 내부감사, 경영진 검토를 반영하고 있다.

따라서, 정보보호 관리체계 가. 관리과정 인증기준은 ISO 경영시스템을 따르는 조직에서의 ISMS 정보보안 활동 요구사항과 큰 차이가 없다. 다만, 정보보호 관리체계는 국내 법에 따른 준수사항과 세부적 기준(예를 들어 연1회 이상 내부감사 등)을 제시하며, ISMS는 정보보안 활동의 책임과 역할 및 기능의 주체를 명확히 하고자 했다.

정보보호 관리체계 나. 정보보호대책 통제분야 인증기준에서 보면,

□ 1. 정보보호 정책은 ISMS 통제항목 'A.5 정보보안 정책', 2. 정보보호 조직은 'A.6 정보보안 조직'과 유사한 내용을 갖는다. 정책의 승인자를 최고경영자로 하고있으며, ISMS에서는 경영진으로 요구하고 있다.

□ 별도 항목인 3. 외부자 보안은 외부 계약, 외부자 보안을 다루며, ISMS에서는 'A.15 공급자 관계'에서 공급자 계약과 제공 서비스, 관리를 통한 보안을 요구한다.

□ 4. 정보자산 분류는 'A.8 자산관리' 내용과 유사하다. 'A.8 자산관리'에 매체 취급이 추가되어 다뤄진다.

□ 5. 정보보호 교육, 6. 인적 보안은 'A.7 인적자원 보안'과 유사하다. 정보보호 관리체계에서는 교육을 강조하며 구체적 요구사항을 제시하고, ISMS에서는 고용인의 정보보안 활동에 대한 경영진 책임을 강조한다.

□ 7. 물리적 보안은 'A.11 물리적 환경적 보안'과 유사하며, 모바일기기를 포함하고 있다. ISMS에서는 'A.6.2 모바일 기기 및 원격 근무'에서 다루고 있다.

□ 8. 시스템 개발 보안은 'A.14 시스템 도입, 개발, 유지보수', 9. 암호 통제는 'A.10 암호화' 내용과 유사하다.

□ 10. 접근통제는 'A.9 접근통제'와 유사하며, 네트워크, 서버, 응용프로그램, 데이터베이스, 모바일기기, 인터넷 접속 등 영역별 접근통제 보안을 구체적으로 요구한다. ISMS에서는 사용자에 대한 접근관리, 책임을 강조한다.

□ 11. 운영보안은 'A. 12 운영 보안'과 유사하며, 시스템 및 서비스 운영 보안에서 원격운영, 스마트워크, 무선 네트워크, 전자거래 및 정보전송 보안을 구체적으로 요구한다. ISMS에서는 기술적 취약점 관리와 정보시스템 감사 내용을 반영하고 있다.

□ 12. 침해사고 관리는 'A.16 정보보안 사고관리'와 유사한 절차를 갖으나, 정보보호 관리체계에서는 정보통신망에 관한 침해사고로 보며 ISMS에서는 정보보안 이벤트 및 인시던트(incident)로 본다. 따라서 12.항은 사고후 대응과 조치를 강조하고 ISMS A.16항은 평시 정보보안 활동 과정에서 발생하는 이벤트, 인시던트의 관리, 보안 사고후 학습과 검토 여부에 주안점을 둔다.

□ 13. IT 재해복구는 자연재앙, 해킹, 통신장애, 전력중단 등 외부적 재해로부터 IT시스템 중단 또는 파손에 대비한 복구체계와 대책을 요구한다. ISMS에서는 조직의 사업 연속성을 보장하기 위한 관리(ISO/IEC 22301)를 요구한다.

□ 국내 법령에 따른 요구 준수는 정보보호 관리체계 전반에 걸쳐 반영되었으며, ISMS에서는 'A.18 준거성' 항에서 법령, 계약, 지적재산권의 보호, 프라이버시 및 개인정보, 기술기준 준수 등으로 함께 요구하고 있다.

정보보호대책 통제분야와 ISMS 통제항목의 세부내용은 통제 목적과 취지가 유사한 것처럼 비슷하다. 다만, 국내법에 따른 정보보호 관리체계는 법령 준수사항, ICT 기술적 보안을 구체화하였고, ISMS는 조직의 비즈니스 위기관리를 위한 정보보안 구현과 리더쉽 책임을 강조하였다.

4. 결언

정보보호 관리체계 '나. 정보보호대책 통제분야' 인증기준은 인증심사를 위한 필수적 지표이고 이를 기준으로 결함(부적합) 여부를 판단한다. ISO/IEC 27001:2013 ISMS 통제항목은 조직의 정보보안 활동사항을 점검하고 측정하는 지표로 참고하며 구현 방법과 내용의 다양성을 인정하고 있다. 따라서 ISO/IEC 27001 인증 취득기관이 정보보호 관리체계 인증심사를 받을 경우 경영체계 프로세스와 통제항목 구현에 대한 적절한 상호 보완을 통해 가능하다. 반대의 경우도 동일하다.

국제표준으로, 국내 법령에 의한 인증기준으로 자리잡은 정보보호 관리체계(ISMS)가 더욱 성숙되고 안정된 정보보안관리 모델로 발전하기 위해서, 정보보안 공학 측면의 ISMS 위험관리 참조모델, 정보보안 성숙도 측정(성과관리, 평가지표) 방법론 개발, 업종별 ISMS 모범사례의 발굴 등 더욱 심층적인 ISMS 주제에 대한 학술적 논의와 연구가 필요하다.

참고문헌

[1] ISO/IEC, International Standard ISO/IEC 27000:2016 'Information technology - Security techniques - Information security management systems - Overview and vocabulary', 2016.02.15

[2] ISO/IEC, International Standard ISO/IEC 27001:2013 'Information technology - Security techniques - Information security management systems - Requirements', 2013.10.01

[3] ISO/IEC, International Standard ISO/IEC 27002:2013 'Information technology - Security techniques - Code of practice for information security management', 2013.10.01

[4] 방송통신위원회, '정보통신망 이용촉진 및 정보보호 등에 관한 법률', 2016.06.02. 시행

[5] 미래창조과학부, '정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 일부개정령안', 2016.06.02. 시행

[6] 미래창조과학부, '정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행규칙 일부개정령안', 2016.06.02. 시행

[7] 미래창조과학부, '정보보호 관리체계 인증 등에 관한 고시', 2013.08.08

[8] 국가기술표준원, 한국산업표준 'KS X ISO/IEC 27001:2014 정보기술-보안기술-정보보호경영시스템-요구사항', 2014.12.12.

[9] ISO/IEC, ISO/IEC Directives - Part 1: Procedures for the technical work, Part 2: Rules for the structure and drafting of International Standards, 2014.05

[10] ISO/IEC, ISO/IEC Technical Report 27015;2012 Information technology - Security techniques - Information security management guidelines for financial services, 2012.12.01

[11] ISO, International Standard ISO 31000;2009 Risk management - Principles and guidelines, 2009.11.15

[12] NIST, NIST SP 800-13 Managing Information Security Risk - Organization, Mission, and Information System View, 2011.03

[13] Kristian Beckers, Stephan Fabender, Maritta Heisel, Holger Schmidt, Using Security Requirements Engineering Approaches to Support ISO 27001 information Security Management Systems Development and Documentation, 2012 Seventh International Conference on Availability, Reliability and Security IEEE, 2012

[14] Gaute Wangen, Einar Arthur Snekkenes, A Comparison between Business Process Management and Information security Management, Proceedings of the 2014 Federated Conference on Computer Science and Information systems pp. 901-910, 2014

[15] Olivier mangin, Beatrix Barafort, Patrick Heymans, Eric Dubois, Designing a Process Reference Model for Information Security Management Systems, SPICE 2012. CCIS, vol 290, pp. 129-140, Springer, Heidelberg, 2012

[16] Bahareh Shojaie, Hannes Federrath, Iman Saberi, Evaluating the effectiveness of ISO 27001:2013 based Annex A, 9th International Workshop on Frontiers in Availability, Reliability and Security (FARES 2014), 2014