情 報 保 護 學 會 誌
第23卷 第4號, 2013. 8

정보보호 관리체계 도입의 필요성 고찰 (특허정보제공 기업을 중심으로)

강 윤 철*, 임 성 택**

요 약

영업비밀 관련 또는 특허문제로 소송이 빈번하게 발생하는 요즘 특허 전쟁에 있어서도 해당 정보를 적절하게 보호하고 유지하기 위한 특허정보 관리체계에 있어서의 정보보안은 매우 중요한 요인으로 인식되고 있다. 이러한 상황에서 보안사고가 발생했을 경우, 이에 효과적으로 대응하기 위한 방안들에 대해 기업 전반에 걸쳐 인지될 필요성 또한 부각되고 있으며 이를 가능하게 해주는 방안으로 국제인증 기준이 떠오르고 있다. 각종 정보보호의 중요성에 따른 기업 관리시스템들이 이러한 인증체계를 도입 및 운영하고 있는 추세이며 이를 뒷받침 해주기 위해 특허법을 비롯하여 관련 컴플라이언스를 준수하기 위한 개인정보보호법(안전성 확보조치), 정보통신망 이용촉진 및 정보보호 등에 관한 법률과 같은 정보보호 법률을 기준으로 제시할 수 있다. 사례 기업에서는 이 중 정보보호 국제인증의 대표격인 ISO27001을 바탕으로 현재 특허관련 기업에 필요한 정보보호관리체계를 정립 및 적용하였다. 해당 정보보호 관리체계는 특허관련 업무분장에서 주요하게 다루어지지 않았던 기술적, 관리적, 물리적 보안에 대한 부적합사항을 충족시키고 특허정보보호업무, 감사업무, 검사업무, 전산운영 등 분산된 업무를 일관된 업무로 통합하는 효과적인 관리체계가 될 수 있음을 제시하였다.

Ⅰ. 서 론

1.1 연구의 필요성 및 목적

2009년의 7.7 DDoS 대란, 2011년 3월 발생한 3.4 DDoS공격, 4월 농협전산망 장애, 7월 SK컴즈 개인정보유출, 2012년 6월 중앙일보 해킹, 10월 선관위 DDoS 공격, 2013년 3월 3.20 사이버테러, 6월 6.25 사이버 공격[1] 등 사이버 테러 국가 사이버 안보 위협이 고조됨에 따라 국내 주요 기업은 물론 방송사 및 금융권의 허술한 보안실태가 논란이 되고 있다. '방송, 금융권 전산마비는 막을 수 없었는가?'라는 질문을 던질 때 우리는 일부 언론에서의 발표처럼 "북한의 소행이다", "APT공격은 막을 수 없는 해킹이다"라는 식으로 방관하기 쉽다. 그러나 사실 각 단계에서 여러 취약점과 문제점이 있었던 것을 해킹의 원인으로 지목할 수 있다.[1] 이에 따라 민간기업과 공공기관 등의 외부/내부 위험요소를 고려한 전체적인 보안체계에 대한 점검이 논의되고 있으며 보안 위협을 체계적으로 분석하고 리스크를 관리하기 위한 필요성이 대두되고 있다. 일반적으로 금융기관뿐만 아니라 고객정보를 다루는 보험, 유통, 카드 및 기밀자료를 취급하는 제조업체에 이르기까지 보안사고가 발생했을 경우, 이에 효과적으로 대응하기 위한 방안들에 대해 기업 전반에 걸쳐 인지될 필요성 또한 부각되고 있으며 이를 가능하게 해주는 방안으로 국제인증 기준이 떠오르고 있다. 이러한 상황에서 각종 정보보호의 중요성에 따른 기업 관리시스템들이 관련 정보보안 인증체계를 도입 및 운영하고 있는 추세이며 이를 뒷받침 해주기 위해 특허법을 비롯하여 정보보호관련 법률, 규정들이 제정되고 개정되며 지식정보화 시대에 맞게 정

1) 최근 발생한 6·25 해킹 당일에는 청와대, 국무조정실, 새누리당 등 정부기관·정당 5곳과 언론사 11곳 등 16개기관의 홈페이지가 변조되거나 접속 장애를 겪는 해킹을 당한 것으로 파악됨

* 고려대학교 일반대학원 디지털경영학과 박사과정 (kcode000@korea.ac.kr)
** 고려대학교 일반대학원 디지털경영학과 교수 (misrim@korea.ac.kr)

보보안 패러다임의 변화가 일면서 관련 컴플라이언스를 준수하기 위한 개인정보보호법(안전성 확보조치), 정보통신망 이용촉진 및 정보보호 등에 관한 법률과 같은 다양한 법률들이 고시되었다. 국제적으로 인정받고 활용되고 있는 ISO27001 정보보호관리체계(ISMS), BS10012 개인정보보호관리체계(PIMS), ISO22301 비즈니스연속성관리체계(BCMS), ISO20000 IT서비스관리체계(ITSM) 등의 경영시스템을 통해 이러한 환경적인 이슈들을 반영하여 기업 전반에 관리적, 기술적, 물리적 통제를 효과적으로 적용 및 유지 할 수 있다. 위와 같은 통제를 달성하기 위한 방향 설정으로 거버넌스 차원의 내부통제를 말할 수 있으며 내부통제란 것은 기업의 정책, 절차, 지침, 규정 등을 수단으로 하여 기업의 목표, 즉 사업 목적을 달성시키는 일련의 것이다. 즉, 전략적인 달성과 업무의 효율성, 재무제표의 신뢰성 및 제반 관련 법규와 절차, 규정의 준수성의 목표를 달성할 수 있도록 이사회, 고위 경영진, 내부통제 관리자가 제정한 절차를 말한다. 또한 기업의 전체적인 시각에서 기업에 영향을 미칠 수 있는 잠재적인 위험이나 사건 등을 식별하여 일정한 수준의 위험관리를 하는 프로세스이기도 하다.[2] 지금까지 언급한 요소들을 고려하여 사례 기업에서는 다양한 분야에 적용할 수 있는 정보보호 국제인증의 대표격인 ISO27001을 바탕으로 현재 특허 관련 기업에 필요한 정보보호관리체계를 정립 및 적용하였으며 이를 통해 해당 정보보호관리체계의 도입 타당성 및 필요성을 검증하고자 한다.

1.2 정보보안 및 특허관련 주요 법률 및 법규

국내의 정보보호 법제도는 각각 제정 목적 및 기능별로 정립됐으며, 이는 국가기밀보호 관련 법령, 중요 정보의 국외유출 방지에 관한 법령, 전자서명 및 인증 관련 법령, 정보통신망과 정보시스템의 보호추진 관련 법령, 침해행위의 처벌에 관한 법령, 개인정보보호 관련 법령 등으로 분류할 수 있다. 이러한 분류에 따라 대표적인 주요 법령을 정리해보면 다음 [표 1]과 같다.

〔표 1〕 정보보호 관련 주요 법령 목록〔3〕

구분	법령명
국가기밀보호	군사기밀보호법, 보안업무규정, 군형법 등
중요 정보의 국외유출 방지	산업기술의 유출방지 및 보호에 관한 법률, 기술의 이전 및 사업화 촉진에 관한 법률, 민·군 겸용기술사업 촉진법, 부정경쟁방지 및 영업비밀보호에 관한 법률 등
전자서명 및 인증	전자서명법, 전자정부법 등
정보통신망과 정보시스템의 보호추진	국가정보화 기본법, 정보통신기반 보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 전자정부법, 전자거래기본법, 국가사이버안전관리규정 등
침해행위의 처벌	정보통신기반 보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 전자무역촉진에 관한 법률, 형법 등
개인정보보호	개인정보 보호법, 주민등록법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 신용정보의 이용 및 보호에 관한 법률 등

이 중 우리가 주의 깊게 살펴보아야 할 정보보안관련 주요 법률은 다음 [표 2]와 같다.

〔표 2〕 정보보안 관련 법제〔4〕

유형	세부 내용
정보통신망 이용촉진 및 정보보호 등에 관한 법률 (이하 정보통신망법)	· 사이버침해에 대한 예방 및 대응조치 전반을 규정함 ※ 정보통신망의 안정성 확보를 위해 정보보호 안전진단, 이용자의 정보보호, 정보통신망 침해행위 등의 금지, 침해사고의 대응 및 침해사고의 원인 분석 등 분산 서비스거부 공격(DDoS)의 대응에 관한 핵심적인 사항 명시
정보통신기반 보호법	· 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함 ※ 정보통신기반보호위원회의 창설, 보호지침의 수립·시행에 대한 사항 등 명시하고 있으며, 사이버위협에 대한 대응에 기본적인 근거 제공
국가정보화 기본법	· 정부기관들의 정보화 추진과정에서 정보보호를 보장하기 위한 기본적인 법적 근거 제공 ※ 정보화의 역기능 발생을 사전 방지하고 사회안전을 지키고자 하며, 사이버공격이 발생한 경우에도 효율적인 대응기반을 제공하는 사회적 환경을 구축하고자 함
전자거래기본법	· 전자거래의 안전성과 신뢰성을 확보하며 전자거래의 촉진을 위한 기반조성을 위해 정보통신시스템의 보호와 관련된 조항 명시(안전성 및 신뢰성 확보 시책, 암호제품의 사용, 촉진계획 등)
전자금융거래법	· 전자금융거래의 안전성과 신뢰성을 확보함과 아울러 전자금융업의 건전한 발전을 위한 기반조성을 함으로써 국민의

유형	세부 내용
	금융편의를 꾀하고 국민경제의 발전에 이바지 함 ※ 전자금융거래의 종류별 전자적 전송이나 처리를 위한 인력, 시설, 전자적 장치 등의 정보기술부문 및 전자금융 업무에 대한 방안과 관련된 조항 명시(사이버위협에 대한 충분한 주의의무 명시 및 공격발생 가능성 감소 역할 명시)
국방정보화 기반조성 및 국방정보자원관리에 관한 법률 (이하, 국방정보화법)	· 미래 정보사회에 걸맞은 선진정예강군 육성과 국방정보기술의 선진화에 이바지하고자 함 · 국방분야의 정보보호에 대한 전략적인 대응, 국방부장관 소속하에 국방사이버안전 전담기관 설치·지정, 사이버 침해·위협 정보기술의 동향조사, 침해된 정보의 유통 감시체계 구축, 침해 및 위협에 대한 역추적 등 대응기술 개발 명시

특허청 산하에 있는 특허관련기업들은 해당 법령 및 규칙들을 준수해야 하는데 이에 대한 산업재산권 법령 체계[5]는 아래 [표 3]과 같다.

〔표 3〕 산업재산권 법령 체계

법률	대통령령
특허법	- 특허법시행령 - 특허권 등의 등록령 - 특허권의수용·사용등에관한규정
실용신안법	- 실용신안법시행령 - 특허권 등의 등록령
디자인보호법	- 디자인보호법시행령 - 특허권 등의 등록령
상표법	- 상표법시행령 - 특허권 등의 등록령
발명진흥법	- 발명진흥법시행령 - 공무원직무 발명의 처분·관리및 보상등에 관한 규정
부정경쟁방지 및 영업 비밀보호에 관한 법률	- 부정경쟁방지 및 영업비밀보호에 관한 법률 시행령
반도체집적회로의 배치설계에 관한 법률	- 반도체집적회로의 배치설계에 관한 법률 시행령
변리사법	- 변리사법시행령
정부조직법	- 특허청과 그 소속기관직제

각각의 법률에서 공통적으로 언급하고 있는 관리적, 기술적, 물리적 보호에 관한 요구사항들을 준수하기 위해 다음의 정보보호인증체계를 활용할 수 있다.

1.3 연구참조 모델 - 국내/외 정보보호인증

기업의 전반적인 정보보안 체계를 다루는 KISA의 ISMS나 개인정보보호를 중점적으로 다루는 PIMS처럼 국내에서 법으로 강제하고 있는 인증체계들은 모두 국제인증 체계를 바탕으로 하고 있다. 본 연구에서 제시하고자 하는 특허기업의 정보보호관리체계 역시 해당 ISO국제규격을 기준으로 정보보호관리체계를 구축 하였으며 이에 대한 이해를 돕기 위해 주요 관련인증에 대해 먼저 살펴보기로 한다.

1.3.1 국내정보보호관리체계 KISA-ISMS

정보보호 분야의 ISO국제인증 체계를 바탕으로 국내 실정에 좀 더 적합하게 제정 및 법제화한 국내인증체계인 정보보호 관리체계(ISMS) 인증제도는 '어떤 조직이 정보자산의 기밀성·무결성·가용성을 실현하기 위한 관리체계를 수립하여, 운영하고 있을 때, 그 관리체계가 방송통신위원회가 고시한 정보보호 관리체계 인증심사 기준에 적합한지를 방송통신위원회가 지정한 기관, 한국인터넷진흥원(KISA)에서 적합성 여부를 보증해 주는 것'이다.[6] 이는 정보보호에 대한 인식을 제고하여, 보호되어야 할 정보통신망 및 정보자산의 안전·신뢰성을 강화하고 국제적 신뢰도를 향상시키기 위한 것으로 정보통신망법 제47조에 법적근거를 두고 있다. 정보보호 관리체계(ISMS)인증심사 기준은 2002년 제도도입 이후 2013년 방송통신위원회고시(제2013-4호)로 개정기준을 공표하였으며 아래 [표 4]와 같이 정보보호 관리과정(5단계, 12개 통제항목)과 정보보호대책(13개 분야, 92개 통제항목)의 두 가지로 구성되어 있다.

〔표 4〕 정보보호 관리체계 인증 기준

통제 분야	통제내용	통제 항목 수	세부 점검 항목 수
관리 과정 (구축 단계)	1. 정보보호정책수립 및 범위설정	2	5
	2. 경영진 책임 및 조직구성	2	5
	3. 위험관리	3	11
	4. 정보보호대책 구현	2	3
	5. 사후관리	3	8
소 계		12	32

통제 분야	통제내용	통제 항목 수	세부 점검 항목 수
정보 보호 대책	1. 정보보호정책	6	12
	2. 정보보호조직	4	9
	3. 외부자 보안	3	6
	4. 정보자산분류	3	9
	5. 정보보호교육	4	10
	6. 인적보안	5	14
	7. 물리적 보안	9	20
	8. 시스템 개발보안	10	32
	9. 암호통제	2	5
	10. 접근통제	14	19
	11. 운영보안	22	67
	12. 침해사고 관리	7	19
	13. IT재해복구	3	7
소 계		92	229
총 계		104	261

이는 개정된 정보통신망법('11.12)에 따라, 기존의 실효성이 낮은 점검항목을 통합하고, 최신 보안관리 기준을 반영하는 등 인증 심사 기준의 통제항목을 137개에서 104개로 변경한 내용이다. 정보보호관리체계에 대한 ISMS는 민간기업(기관)을 대상으로 하며, 공공기관을 대상으로 하는 G-ISMS에 대해서는 생략하도록 한다.

1.3.2 국제정보보호관리체계 ISO27001

현재 ISO/IEC 27001:2005로 표기[2]되고 ISMS (Information Security Management Systems)라고도 불리는 정보보안경영시스템은 조직의 정보 자산이 적절히 보호되고 있는지를 인증하는 것으로, 조직이 위험평가를 실시하고 적절한 통제항목을 구현하여 국제적으로 인지되는 ISMS 규격에 적합한 정보보안경영시스템을 이행하여 왔음을 입증하는 것이다. 이는 PDCA Cycle에 따라 지속적인 개선을 추구하며, 조직의 규모에 상관없이 모든 산업분야에 적용 가능하다.[7] ISO/IEC 27001:2005 규격은 전체 11개 통제분야, 133개 통제항목을 인증심사기준으로 사용하고 있으며, 현재 최신의 보안 이슈가 반영되어 개정 중에 있다. 세부 통제 항목은 본문에서 다시 살펴보기로 한다.

2) 인증 규격은 관련 기관명, 해당 인증명, 발행년도 순으로 표기하며 여기서, ISO는 International Organization for Standardization(국제표준화기구)를 IEC는 International Electrotechnical Commission(국제전기표준회의)을 의미함

1.4 대상 기업과 적용 방법

국내 특허정보 서비스 기업 중 세계 주요국 특허정보 약 1억4천여 건의 정보를 제공하고 있으며 2012년 기준 매출액 200억 이상, 종업원 수 300명 이상인 W사에 본 연구모델을 적용하였다. 해당 기업은 특허/상표/디자인 조사, 상표분류, 디자인분류 등 광범위하게 개연되어 있는 특허정보 제공업무 특성과 관련하여 관련 법률 준수 및 적정 보안 수준을 유지하기 위해 체계적이고 효율적인 정보보안업무를 수행할 필요가 있었으며 이에 대한 방안으로 정보보호관리체계를 구축하였다. ISO27001인증 획득의 결정은 첫째, '정보보호 인증 획득의 필요성 대두'이다. 특허청에서 2009년 까지 ISO27001 인증업체에게만 선행기술조사 업무 수행할 수 있는 자격을 부여하였는데 즉, 특허청의 「선행기술조사 전문기관의 지정 및 운영에 관한 요령」[3] 제3조(전문기관의 지정요건) 및 제4조(전문기관의 지정계획 공고 및 지정신청)에 따라 선행기술조사 전문기관으로서 보안체계를 수립하여야 했다. 둘째, '미공개 출원 데이터 정보 보호 필요'이다. 즉, 미공개 출원 데이터 정보에 대한 국제적인 내/외부 위협이 존재하며 이러한 위협으로부터 관련 정보를 국제적 표준에 따라 보호할 필요가 있었다. 셋째, '위험평가 및 대응방안 수립'이다. 즉, 주요자산 식별 및 위협/취약점 분석 및 평가, 그리고 정보시스템에 대한 기술적 취약점 진단 및 평가를 통한 정보침해사고의 가능성을 진단할 필요가 있었으며, 이러한 요건들을 정보보호 관리체계의 수립 및 정책·지침·절차의 표준화를 통해 효과적인 사후 관리 및 교육 지원까지 가능할 수 있도록 하기 위함이었다. W사는 이러한 배경을 가지고 정보보호관리체계의 수립부터 ISO27001 정보보호인증을 획득하기까지 2010년 4월부터 약 두 달간 해당 정보보호관리체계의 적용을 진행하였다. 적용 과정은 아래 [표 5]와 같이 4단계로 진행되었다.

해당 정보보호관리체계의 도입 효과성 검증을 위해 2010년 8월에 ISO27001 국제인증에 대해 최초심사를 진행 후, 매년 사후심사를 통해 해당 정보보호관리체계의 효과성을 평가하였다. 본 연구는 사례기업에 대한 심층 조사연구의 특성을 가지고 있으며 인증 주기에 따라 3년간 수집된 데이터를 바탕으로 분석 되었다.

3) 개정 2013. 3. 28. 특허청고시 제2013-9호

〔표 5〕 정보보호관리체계 세부 적용 계획

적용 과정		
국제 보안 표준 인증 지원	1단계 (현황분석)	요구사항 분석 및 수행계획 수립
		ISO27001 인증범위 정의
		자산분류 및 중요도 평가
	2단계 (GAP분석)	관리/물리 취약점진단
		기술 취약점 진단
	3단계 (위험평가)	위험도 평가 및 위험분석
		정보보호 지표 도출
	4단계 (관리체계 수립)	정책/지침 개정(안) 수립
		마스터플랜 수행과제 도출
		마스터플랜 세부수행방안 작성
인증심사지원		내부감사
		증적자료 정리
		임직원 정보보호 교육
인증심사		문서 및 현장심사

Ⅱ. 본론

정보보호에 있어 외부 및 내부 위험요소라는 것은 내부의 취약점에 외부 또는 내부로부터 발생되는 위협이 가해졌을 때 조직에 부정적인 영향을 끼칠 수 있는 모든 것들이라고 볼 수 있다. 예를 들어, 침입탐지시스템(IDS)을 적용하여 컴퓨터 시스템의 비정상적인 사용, 오용, 남용 등을 실시간으로 탐지한다 하더라도 내부 직원에 대한 교육 부재나 관리자의 실수로 외부 바이러스나 해킹에 대한 대응을 신속하게 하지 못한다면 시스템의 다운과 같은 결과로 조직의 업무 연속성에 지장을 초래할 수 있다. 바이러스, DDos공격, 해킹 등 기술적인 부분의 관리가 필요하거나 지진대나 홍수 상습 피해지역을 피해서 서버룸을 구축하는 것과 같은 물리적인 부분 또한 고려해야 할 위험요소 중 하나이다. 업무 요구사항에 따른 효과적이고 효율적인 정보자산의 관리 및 지원에 있어 정보보호관리체계의 구축은 이러한 위험요소들을 통제하기 위한 적절한 기준을 제공할 수 있다. 이 장에서는 실제 ISO27001의 요구사항에 따라 정보보호관리체계를 구축한 기업의 정보보안 개선 효과를 이해하기 위해 ISO27001 인증의 주요사항을 살펴보고 해당 인증을 통한 효과성을 검증해 본다.

2.1 ISO27001 적용 주요사항

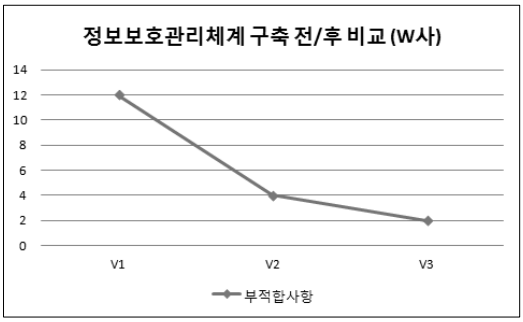
ISO인증은 기본적으로 최초심사와 사후심사로 구분할 수 있다. 최초심사에서는 문서심사와 현장심사로 다시 나눌 수 있으며, 사후심사에서는 현장심사만 진행한다. 최초심사 후 매년 1회 이상의 사후심사를 수행해야 하며 인증 유효기간인 3년이 경과하면 갱신심사를 통해 최초심사와 마찬가지로 새롭게 인증심사를 진행한다. 이는 주위 환경이 급격히 변함에 따라 관련 이슈에 대한 사항이 많이 달라졌음을 인정하는 것이며 달라진 규격 요건이나 법적 요소들을 반영하여 정보보안 수준을 지속적으로 개선시켜 나갈 수 있다. 인증 심사에서 발생한 부적합(Nonconformity)은 중부적합과 경부적합으로 나뉘며, 중부적합(Major Nonconformity)은 정보보안경영시스템에 중대한 영향을 미치는 발견사항을 의미하고. 경부적합(Minor Nonconformity)의 경우, 정보보안경영시스템에 중대한 영향을 미치지 않는 발견사항을 의미한다. 부적합사항 외 객관적인 증거부족으로 부적합 판정이 어려운 경우 또는 관리부재로 인해 부적합/손실로 악화될 수 있는 경우에는 관찰사항으로 분류하는데 심사원의 판단 및 경험으로 개선이 권고되는 경우 개선권고사항으로 분류될 수 있다. 최종 결과에서 중부적합이 없는 경우 인증 추천이 이루어지며, 경부적합만 발견되는 경우, 인증 유지/추천이 가능하나 시정조치계획의 제출 및 차기 심사에서 시정조치의 유효성을 검증해야 한다.

2.2 정보보호관리체계 구축 전/후 비교

정보보안은 더 이상 국한된 범위의 업무사항이 아니라 기업 거버넌스 차원에서 다루어져야 하는 주요 이슈임이 명확해짐에 따라 국내에서도 정보보호관리체계를 구축하고 해당 국제인증인 ISO27001인증을 받은 기업들이 증가하고 있으며, IT업종뿐만 아니라 금융권을 비롯하여 인쇄업, 제조업 등 분야에 상관없이 다양하다. 그 중 특허 분야와 관련된 기업의 정보보호관리체계 구축 전과 후를 비교해 보고자 한다. 비교 방식은 정보보호관리체계 구축 후 최초심사에서 발견된 부적합건수 및 개선권고사항이 매년 사후심사가 진행됨에 따라 얼마나 감소하는지에 대한 통계치를 활용해 검증해 보고자 한다. 비교 대상으로는 앞서 설명한 2012년 기준 매

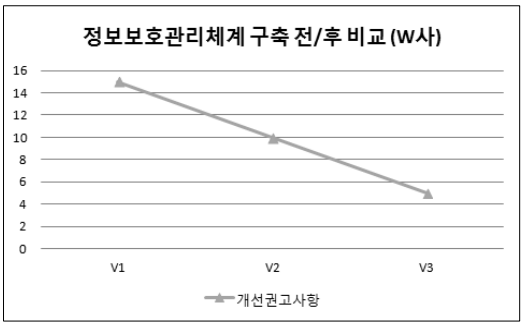
출액 200억 이상, 종업원 수 300명 이상인 특허정보제공서비스기업 W사 한 곳을 선정하였다. 대상 업체는 2010년 8월에 최초심사가 진행되어 2013년 현재 3년 주기의 인증 사이클에 따라 심사가 완료되어 갱신심사를 앞두고 있다.

정보보호관리체계 수립 후 ISO27001 국제인증의 최초심사에서 3년 주기가 지나는 동안 아래의 <그림 1>과 같이 부적합 건수가 매년 감소하고 있음을 확인할 수 있었다.



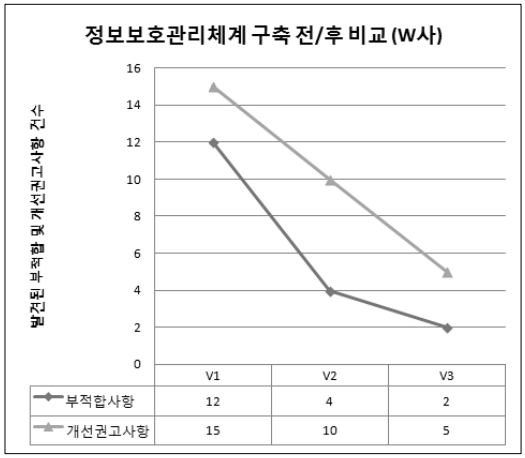
〈그림 1〉 정보보호관리체계 구축 후 부적합 추이

위의 <그림 1>에서 x축은 최초심사(V1), 사후심사(V2, V3)를 나타내며, y축은 발견된 경부적합(Minor Nonconformity)건수를 의미한다. 마찬가지로 아래의 <그림 2>와 같이 개선권고사항 역시 매년 감소하고 있음을 확인할 수 있었다.



〈그림 2〉 정보보호관리체계 구축 후 개선권고 추이

물론 개선권고사항은 주위 환경이 변화함에 따라 새로운 이슈대응을 위해 증가할 수도 있으므로 본 연구에서는 해당 기업이 다양한 정보보안 활동을 통해 지속적인 개선을 수행하고 있어 추가적인 개선 사항이 적다는 의미로만 참고하였다. 이처럼 해당기업에 3년 동안 11개 도매인 133개 통제항목에 비추어 정보보호관리체계에 대한 인증심사를 수행하였고 이에 대한 결과로 경부적합사항 및 개선권고사항은 아래 <그림 3>처럼 꾸준히 감소하였음을 다시 한 번 확인 할 수 있다.



〈그림 3〉 부적합사항 및 개선권고사항 감소 추이

이처럼 최초심사 기준으로 매년 67%, 50%의 부적합사항의 감소가 이루어졌으며, 정보보호관리체계가 부재했던 상황과 비교하여 해당 인증체계 도입 후 3년 동안 최초 대비 약 83%의 부적합사항이 감소했음을 확인할 수 있었다. 위의 통계 자료는 특허관련 기업에서 정보보호관리체계가 보안의 완전성을 보장하지는 못해도 상대적으로 통제에 필요한 기준을 제시하고 이에 따라 기업이 가진 리스크를 감소 시켰다는 것을 의미한다.

본 연구에서 제시하고자 하는 특허관련 기업의 정보보호관리체계는 국제 인증에 따른 물리적, 기술적, 관리적 보안통제는 물론 법규 및 컴플라이언스에 따른 리스크 통제가 가능하든 것을 보여주는 사례라고 할 수 있다.

Ⅲ. 결론 및 향후 연구과제

정보보호관리체계는 해당 시스템이 '법적, 제도적 정보보호 요구사항에 맞춰 기업 업무 프로세스 전반에 대한 보안 조건을 충족하고 지속적으로 유지하는 있음을 보증하는 것'이다. 물론 정보보호관리체계를 갖춘다고 하여 정보보호에 대해 완전하다고 말할 수는 없다. 이는

기업이 정보보호관리체계를 갖추고 해당 인증을 획득한다고 하더라도 해킹, 정보유출 등의 보안 사고를 모두 막을 수 있는 것도 아닐뿐더러, 각 기업들의 '정보보호관리체계'를 합격, 불합격으로 재단하기에는 무리가 따르기 때문이다. 즉, 정보보호관리체계를 갖춤으로써 조직의 정보보호 수준이 해당 기준에 부합함(conformity)을 합리적인 수준으로 보증(assurance)할 수 있다는 의미이지 절대적으로 보장(guarantee)한다는 의미가 아니다.[8] 하지만 정보보안을 위한 최소한의 기준이나 가이드가 없다면 수많은 리스크로부터 조직의 어느 부분을 어떻게 보호해야 할지에 대한 방향조차 잡을 수가 없을 것이다. 정보보호는 더 이상 일부의 업무 분야가 아니라 조직 전반의 모든 구성원들이 훈련 및 인식교육을 통해 내재화되어야 하는 필수 사항이다.

본 연구에서는 정보보호관리체계를 구축하는데 있어 고려해야하는 요소들을 살펴보고 실제 정보보호관리체계를 구축함으로써 조직전반에 정보보호 수준이 개선된 사례를 살펴보았다. 기업의 보안업무를 수행하는데 있어 얼마나 효율적이었는지에 대한 부분은 관련 담당자마다 다를 수 있으나 준수사항이 많아지고 이에 대한 체계적인 관리가 이루어지면 기업의 보안수준은 올라간다는 것을 해당 사례 분석을 통해 확인할 수 있었다. 본 연구에 국한해서는 정보보안에 관련된 개인정보보호관리체계 즉, BS10012인증과의 연계성을 분석하여 관련 조직의 정보보호 관리체계의 효과에 영향을 끼치는지에 대한 상관 분석을 수행하고 이에 따른 비용 및 인력 절감 등의 부가적인 제반사항들이 깊이 있게 다루어진다면 정보보호관리체계의 구축을 통한 보안업무의 효율성 또한 심도 있게 측정해 볼 수 있으리라 본다. 다만, 해당 기업이 특허관련 기업 전체를 대표할 수 없으므로 특허정보 제공서비스 기업 한 곳에만 적용되어 특허관련기업 전체에 끼치는 효과성에 대한 비교 할 수 없는 상태이다. 향후 연구과제에서는 또 다른 특허관련 기업들에 적용된 사례를 분석하여 정보보호관리체계 정책적 용방안을 제시하고, 특허관련 업무 전반의 성과측정이 되는 연구를 포함할 필요가 있다. 아울러, 해당 관리체계의 적용에 있어 업종별로 주요하게 다루는 통제항목의 차이가 있을 수 있다. 하지만 ISO국제인증 체계 특성상 금융, 제조, 인쇄, 특허 등 관련 산업 특성에 상관없이 모든 산업 분야에 적용할 수 있어 동종 업계는 물론 타업종과의 효과성 정도 차이에 대해서도 지속적인 검증이 가능하리라 본다. 따라서 해당 연구모형이 얼마나 적절했는지에 대한 추가적인 검토를 위해 1차적으로는 유사 업종 내에서의 비교를 수행하고 2차적으로 다른 산업분야 간의 비교를 통해 정보보호관리체계의 영향을 분석함으로써 해당 인증체계의 타당성을 보다 폭넓게 검증할 수 있을 것이라 기대한다.

참고문헌

[1]1 35p, 금융시스템에 대한 인증제도의 필요성, 마이크로소프트웨어 2013년 4월호, 박성갑

[2] 15p, "IT 거버넌스 프레임워크 코빗 - COBIT 4.1을 중심으로, 2010. 04. 17, 조희준

[3] 43p, 정보보호 관련 주요 법령 목록, 2013 국가정보보호백서

[4] 국가법령센터 http://www.law.go.kr

[5] 특허청 http://www.kipo.go.kr

[6] 정보보호 관리체계(ISMS)인증제도 해설서 (KISA)

[7] ISO/IEC27001:2005 Requirement

[8] 120p, 법 제도에 따른 정보보안 인증제도 현황, 마이크로소프트웨어 2013년 4월호, 강윤철

〈著者紹介〉

강 윤 철 (Kang, Youn-Chul)
2009년 2월: 고려대학교 경영정보학과 졸업
2011년 2월: 한양대학교 정보시스템학과 석사
2012년 3월~현재: 고려대학교 디지털경영학과 경영학 박사과정
<관심분야> IT거버넌스 및 정보보호 거버넌스, IT감사, 내부감사, 내부통제, ISMS(정보보호관리체계), PIMS(개인정보관리체계), IT-SM(IT서비스관리체계), BCMS(비지니스연속성관리체계) 등

임 성 택 (Rim, Seongtaek)
1982년 2월 : 서울대학교 불어교육과 졸업
1986년 8월 : 조지아주립대학교 경영정보학 석사
1992년 3월 : 조지아주립대학교 경영정보학 박사
1992년 3월 - 1994년 2월 : 대전대학교 경영학과 조교수
1994년 3월~현재 : 고려대학교 경영정보학과 교수
<관심분야> 정보시스템전략, 통신 비즈니스 모델, IT 생태계 및 플랫폼 비즈니스 전략