Journal of the Korea Academia-Industrial cooperation Society
Vol. 13, No. 9 pp. 4224-4233, 2012

http://dx.doi.org/10.5762/KAIS.2012.13.9.4224

정보보호관리체계[ISMS] 인증이 조직성과에 미치는 영향에 관한 연구

배영식[1*]
[1]동국대학교 법학과

A study of Effect of Information Security Management System [ISMS] Certification on Organization Performance

Young-Sik Bae[1*]
[1]**Department of law doctor course, Dongguk University**

요 약 본 논문은 최근 기업이나 조직에서는 산발적인 보안 관리에서 종합적이고 체계적인 정보보호관리체계가 요구되고 있으며 국내에서도 2001년 7월부터 정보보호관리체계(ISMS) 인증제도가 시행되어, 2012년 7월 현재 130개 업체가 인증을 받았으며. 이와 같이 ISMS 인증제도가 국내에 도입된 이래 인증수요는 꾸준히 증가하여 기업경쟁력의 중요한 수단으로 인식되어 가고 있는 추세인 반면 ISMS 인증의 실수요자가 인식하는 인증의 효과성 등의 질적인 측면이 미흡하다는 문제는 끊임없이 제기되어 오고 있다. 이에 따라 본 연구는 국내 ISMS 인증 취득기업 정보보호 담당자에 대한 설문조사를 통해 ISMS 인증이 기업의 경영성과에 얼마나 긍정적으로 영향을 미친다는 사실을 실증적으로 분석하여, 조직성과에 영향이 있다는 것을 입증하였으며 기업들로 하여금 ISMS 인증 취득의 효과를 인식하여 궁극적으로 ISMS 구축을 통해 보안 사고를 사전에 예방하고 기업성과를 향상시키는데 도움을 주고자 하였다.

Abstract As Internet usage is rapidly spreading, tasks that were only possible offline are now available in cyber space but at the same time, new security threats such as hacking and viruses have also increased. For that reason, Comprehensive and methodical information security systems are therefore required in enterprises and organizations.

Consequently, the Information Security Management System certification system has been in effect in Korea since July 2001. As of December 2012, 130 enterprises have been certified, and more than 120 ISO27001 certifications have been issued. As such, since the introduction of the ISMS certification system in Korea, the demand for the certification has been steadily increasing, and it is now recognized as an integral part of maintaining the competitiveness in an enterprise. However, the qualitative aspects of certification regarding the effectiveness of ISMS have been continuously questioned by actual customers. In order to clarify the situation and remove such doubts, this study will substantiate the fact that development and certification of ISMS positively affect the business performance of enterprises so that they will recognize the effect of obtaining ISMS certification and eventually prevent security accidents and improve their business performance by developing ISMS.

Key Words : Information Security Management System [ISMS], ISMS Certification, Benefits of Information Security, performance measurement, Measurement Method, Economic Effects on the Information Security Industry

*Corresponding Author : Young-Sik Bae
Tel: +82-2-750-2691 email : bae211@kcc.go.kr
접수일 12년 06월 18일 수정일 (1차 12년 07월 11일, 2차 12년 07월 24일, 3차 12년 08월 02일) 게재확정일 12년 09월 06일

1. 서론

정보통신기술의 발전 및 인터넷의 확산으로 개개인의 생활양식이 현격하게 바뀌고 있고 기업의 비즈니스 양태도 획기적으로 변화되고 있을 뿐만 아니라 새로운 비즈니스가 폭발적으로 창출되고 있다. 그러나 이러한 변화의 이면에는 해킹, 바이러스, 개인정보 유출 등의 역기능 또한 비약적으로 커지고 있다.

따라서 이러한 역기능에 효과적으로 대응하는 것이 정부, 기업, 개인 등의 각 행위주체들에게 핵심적인 과제로 대두되고 있다. 특히 현대사회의 중추라고 할 수 있는 기업들에게 경영에 있어서 보안관리(Information Security Management)는 하나의 경영관리요소로 인식되어 가고 있다. 이러한 보안 관리에 대한 외부의 독립적인 평가 또는 인증의 필요성도 점차 강조되고 있으며, 국내에서도 2001년 7월부터 정보보호관리체계(ISMS : Information Security Management System) 인증제도가 시행되어 오고 있으며 2012년 5월 현재 인증서 발급 누적 건수는 135건이며, ISO27001 인증건수도 110여건에 이르고 있다. 이와 같이 ISMS 인증제도가 국내에 도입된 이래 인증수요는 꾸준히 증가하여 기업경쟁력의 중요한 수단으로 인식되어 가고 있는 추세이다[20].

그러나 ISMS 인증제도는 기업의 정보자산을 보호하고 기업경쟁력을 강화하는 방안으로 활용되고 있으나 인증의 실수요자가 인식하는 인증의 효과성 등의 질적인 측면이 미흡하다는 문제가 제기되고 있다. 특히, 인증기업들이 인증을 통하여 기업 서비스의 질을 향상시켜 고객만족과 대외적인 신뢰 구축을 이루어 경영혁신의 기회로 삼아야 함에도 인증 획득 자체에만 몰두하여 인증의 본래 의미가 많이 상실되어 가는 실정이다[6].

이런 이유로 국내 ISMS 인증 기업수가 크게 증가하지 않는 것으로 보이며, 이는 인증을 통한 기업경쟁력 강화의 실효성을 느끼지 못하거나 인식하지 못하기 때문인 것으로 판단된다. 따라서 기업이 ISMS 인증획득만을 목적으로 삼기보다는 기업 생존여부의 수단으로 확실히 자리매김할 수 있도록 하는 유인책이 요구되는 시점이다. 즉, 기업은 정보보호 활동의 기반을 마련하고 조직의 지속성장이 가능하도록 비즈니스와 연계된 정보보호관리체계 구축이 필요한 것이다.

따라서 국내 ISMS 인증 제도의 효과성 확보를 위한 연구와 정보보호에 대한 지속적인 개선 노력은 기업 경쟁력 강화에 있어서 중요한 문제라 할 수 있다. 이에 따라 본 연구는 ISMS 구축 및 인증이 기업의 경영성과에 긍정적인 영향을 미친다는 사실을 실증적으로 분석함으로써, 기업들로 하여금 ISMS 인증 취득의 효과를 인식하여 궁극적으로 ISMS 구축을 통해 보안 사고를 사전에 예방하고 기업성과를 향상시키는데 도움을 주고자 한다[14,15].

2. 이론적 배경

2.1 정보보호관리체계 인증제도

조직의 자산에 대한 안전성 및 신뢰성을 향상시키기 위한 절차와 과정을 체계적으로 수립하고 문서화하여 지속적으로 관리·운영하고 정보보호의 목표인 정보의 기밀성, 무결성, 가용성을 실현하기 위한 일련의 과정 및 정보보호에 대한 지속적인 개선활동을 정보보호관리체계(ISMS)라고 한다.

또한 기업(조직 또는 사업장의 일부 또는 전체)이 수립하여 운영하고 있는 이러한 정보보호관리체계가 일정한 인증심사기준에 적합한지 여부를 제3자인 인증기관이 객관적이고 독립적으로 평가하여 기준에 대한 적합 여부를 보증해주는 제도를 정보보호관리체계 인증제도하고 할 수 있다.

우리나라에서는 2002년도 「정보통신만이용촉진및정보보호등에관한법률」 제47조에 [정보보호관리체계의 인증] 이라는 법적 근거를 두고 기술적·물리적 보호조치를 포함한 종합적 관리체계가 인증심사기준에 적합한지 여부를 방송통신위원회 산하기관인 한국인터넷진흥원(KISA:Korea Internet & Security Agency)으로부터 인증받도록 하고 있다. 특히 2012년 3월에는 그동안 실효성 문제로 논란이 많았던 정보보호 안전진단 제도를 폐지하고 ISMS로 의무화하는 법안을 개정하였으며, 이와함께 개인정보보호관리체계(PIMS: Personal Information Management System) 인증 제도, 정보보호 사전점검, 정보보호관리 등급제 등을 도입하는 근거를 마련하였다[10,16].

2.2 국외 ISMS

국제 표준화 기구인ISO(International Organization for Standardization)와 IEC(International Electrotechnical Commission)는 연합위원회(Joint Technical Committee)를 구성하여 2005년에 보안관리 국제 표준화를 위해 ISMS(Information Security Manag ement System)에 대한 국제 표준인 ISO/IEC 27001(Information security management systems - Requirement)과 ISO/IEC 27002(Code of practice for information security management)를 발표하였다[21,22].

이 표준은 원래 BS(British Standard) 7799에서 발전한 것으로, 모범사례는 BS 7799 Part 1, 인증 기준은 BS7799 Part 2로 나뉘어져 BS 7799 Part 1이 ISO/IEC 17799로 먼저 국제 표준이 되었고, 인증심사기준인 BS 7799 Part 2가 뒤이어 국제 표준이 되었다. 개정 작업을 통하여 2005년에는 현재 인증기준을 위해 사용 중인 ISO/IEC 27001과 모범사례의 집합인 ISO/IEC 27002로 바뀌었다 [21,22].

정보보호관리체계에 대한 국제인증을 받기 위해서는 Part 1의 실행지침(ISO27002)에 따라 자체적인 체계를 수립하고, 일정 기간 이행한 기록을 토대로 Part 2 규격(ISO27001)에 따라 심사를 받아야 한다.

2.3 국내외 정보보호관리체계(ISMS) 비교 분석

2.3.1 정보보호관리체계(ISMS)인증 제도 비교 분석

국외 ISMS 인증제도로는 국제 표준에 따른 ISO27001 인증이 있으며, 전세계적으로 많은 나라에서 선택하여 공공 및 민간기업에서 도입 운영하고 있다. 국제 표준에 근거한 인증이라는 점에서 인지도는 높으나 아직 국가적으로 상호인정 등 미흡으로 국제적으로 통용되는 제도로는 인정을 받지 못하고 있다. 국내 ISMS 인증 제도 또한 2002년도부터 정보통신망법을 개정하여 법적 근거를 마련한바 있으나 국제 표준 출현과 도입에 따른 실질적인 혜택 부족과 기업들의 보안에 대한 투자 기피 등으로 활성화가 미흡하였다. 그러나 2012년 3월에 정보보호 안전진단 대상자에 대해 최소한의 보안수준을 요구하던 것을 수준이 높은 ISMS 인증을 취득하도록 의무화 법안을 제정함으로서 해당 기업들의 정보보호 수준이 크게 향상될 것으로 기대하고 있다. 그동안 지속적으로 제기되어왔던 인증 취득 후 취득기관의 자체 사후관리 미흡으로 보안사고 발생에 따른 제도의 실효성 부분이 의무화와 보다 현실적인 점검항목 개선을 통해 보안사고를 최소화하고 높은 정보보호수준을 유지하게 하여 10년간의 제도 운영을 보다 한 단계 고도화 되는 계기가 될 것이다. 국내 제도도 이제 국내 기업 환경에 적합하도록 정보자산의 가치에 따라 보호수준을 다르게 적용하게 하는 위험관리 방법을 개발하여 국제 표준이라는 인지도와 경쟁력을 뛰어넘어 우리나라의 정보보호 관리 모델과 방법론이 국제 표준으로 채택되어 많은 국가들이 도입하여 적용하게 될 날도 얼마 남지 않았다. 국내 적용 ISMS 인증 제도와 국제 ISO27001 인증제도에 대한 일반적인 비교 분석은 표 1과 같다[7,17].

[표 1] 정보보호관리체계(ISMS)인증 제도 비교 분석
[Table 1] Comparison of ISMS

구분	국내 ISMS	ISO 27001
인증기관	KISA 단일 인증기관 ※ 민간 인증기관 추가 지정 가능	BSI, DNV, DQS, TUV 등
인증기준	방통위 고시, TTA 표준	ISO 27001
구조	정보보호관리과정 5단계 14개 통제항목, 문서화 3개 통제항목, 정보보호대책 15개 분야 120개 통제항목(총 137개 통제항목에 446개 세부항목)	10개 관리통제영역, 36개 통제목적, 127개 통제사항
시행시기	2002년	1998년
심사방법	서면심사를 포함한 기술심사 위주 ※ 정책·규정·지침과 증적자료를 상호 비교하여, 실제 운영 여부 확인	서류 심사 위주 ※ ISO 9001, 14001과 동일한 심사 절차 사용
유효기간	3년	3년
사후관리	매년 1회	6개월 주기 1회
주요특징	법에 근거하여 공공기관이 인증 제도를 운영하고 있어, 신뢰성, 공정성 확보	ISO 국제 표준에 근거하고 있기 때문에, 대외적 신인도가 높으나, 상호 인정은 안됨
	취약점 점검 및 모의 해킹을 통하여 기업의 실제적인 정보보호 수준 측정	관리 프로세스와 계획의 수립 여부 점검을 중시
	정보보호 전문가로 구성한 인증 심사원을 활용하여 심사의 전문성 확보	민간 기업이 수익 사업 위주로 운영
	다양한 인증 취득 혜택 지원	사후 관리 심사 주기가 6개월로 짧음

2.3.2 정보보호관리체계(ISMS) 통제항목 비교 분석

국외 정보보호관리체계(ISMS) 인증심사기준으로 활용되는 국제 표준 규격인 ISO27001과 국내 ISMS 통제항목과는 큰 차이점을 보이지는 않는다. 왜냐하면 국내 ISMS 통제항목과 ISO27001 통제항목은 운영기간이 10년이상이 되었으며, 그동안 통제항목을 추가하거나 삭제하는 등 개정 기간을 걸치면서 두 기준간의 차이점은 많아 보이지 않는다. 다만, 국내 ISMS의 경우 국제표준(ISO27001)을 모두 포함하면서 국내 환경에 적합하도록 모형을 개발하여 5개 관리과정(14단계), 문서화, 15개 분야로 세분화함에 따라 ISO27001의 11개 항목에 추가된 4개 분야(3. 외부자 보안 5. 정보보호 교육 및 훈련 9. 암호

통제 12. 전자거래 보안)에 대해 보다 더 강조되어 설계되었다. [표 2] ISO27001과 국내 ISMS 통제항목 비교와 같이 ISO27001이 국내 ISMS 통제항목 120개 보다 많은 133개로 정보보호관리 과정과 문서화 부분을 제외하면 ISO27001이 통제항목 수에서는 많다. 그러나 통제항목의 많고 적음이 보안수준을 높이거나 낮추는 것은 아니지만 국내 ISMS의 경우 세부체크리스트가 442개로 ISO27001 보다 많은 통제항목으로 구성되었으며, 각 기업체의 정보보호관리체계에서 필요한 통제항목을 선택하고 각 보안요구사항에 대해 관리체계를 마련해 이행함으로써 보안수준을 체계적으로 향상시킬 수 있다[17].

[표 2] ISO27001과 국내 ISMS 통제항목 비교
[Table 2] Comparison of ISMS and ISO27001 Controls

ISO 27001		국내 ISMS	
분야	통제 항목	분야	통제 항목
1. 정보보호정책	2	1. 정보보호정책	5
2. 정보보호조직	11	2. 정보보호조직	4
3. 자산관리	5	3. 정보자산 분류	4
4. 인적 보안	9	4. 인적 보안	5
		5. 외부자 보안	4
		6. 정보보호 교육 및 훈련	4
5. 물리적 환경적 보안	13	7. 물리적 보안	12
6. 통신 및 운영관리	32	8. 운영관리	22
		9. 전자거래 보안	5
7. 접근통제	25	10. 접근통제	14
8. 스템개발보안	16	11. 시스템개발보안	13
		12. 암호통제	3
9. 보안사고관리	5	13. 보안사고관리	7
10. 업무연속성 관리	5	14. 업무연속성관리	7
11. 준거성	10	15. 검토, 모니터링, 감사	11
총계	133	총계	120

현재 국내에서는 ISMS 인증제도를 도입한 2002년 이후부터 국내 제도와 ISO27001 인증제도가 공존하고 있는 실정으로 ISO27001 인증의 경우 BSI, DNV와 같은 인증기관에서, 국내 ISMS의 경우 KISA(Korea Internet & Security Agency)에서 인증기관으로 인증업무와 심사업무를 수행하고 있다[18,21,22]].

2.5 정보보호 성과에 대한 선행 연구

현재 ISMS 인증의 기업성과에 미치는 영향에 대한 연구는 상당히 미흡한 실정이다. 그러나 ISMS 성과측정 연구에 앞서 선행되어야할 정보보호 관련 성과측정의 연구는 다양하게 진행 되어왔다 할 수 있으며, 그 내용은 다음과 같다.

홍기향(2003)은 정보보호 통제와 활동은 정보보호성과에 영향을 미치나, 활동이 통제보다는 직접적인 영향을 미치는 것으로 나타냈다. 또한 정보보호 통제는 활동이 성과에 미치는 영향을 조절하거나 활동을 통하여 성과에 간접적인 영향을 미치는 것으로 나타나 통제의 성과에 대한 영향도 검증하였다. 또한 정보보호 통제, 활동 및 성과 요인들은 일정한 유형을 형성하여 정보보호 통제, 활동, 성과 변수간의 내적 응집력이 확인되었으며, 조직의 정보보호 현황은 상위 및 하위 수준의 유형으로 분류될 수 있음이 확인 되었다[2,3].

신일순(2005)은 국내 정보보호의 경제성 분석 연구 현황을 개관하고, 국제적으로 진행되고 있는 연구들을 주제별로 사이버 공격에 의한 피해액 산출, 프라이버시 경제성연구, 정보보호 비용 및 투자가치에 대한 연구 등으로 나누어 분석하였다. 또한 정보보호의 경제적 분석 및 접근의 필요성을 명확히 하고, 국가 및 기업조직별 수준에 맞는 적절한 정보보호 정책의 입안 및 현실적인 정보보호를 달성할 수 있는 방안의 마련을 제시 하였다[4,5].

KISA(2008)는 인터넷 침해사고로 인한 사회경제적 손실액을 측정함에 있어 실질적 손실비용과 이를 복구하기 위한 비용에 대한 실태조사를 수행하여 손실비용과 복구비용의 주요 변인들을 파악하고, 동일한 상황이 발생할 시 적절한 대응방안을 제시한바 있다. 침해사고로 인하여 직접적인 손실요소인 손실이익과 복구비용이 발생되고, 간접손실로는 생산효율의 저하, 데이터손실/데이터재생비용, 책임보상액(추가제언) 등이 손실로 나타날 수 있다[9,11].

KISA(2006)는 국가정보보호 수준평가 연구에서 지수산출을 위해 지표체계를 정보보호기반(T), 정보보호환경(E), 정보화역기능(N) 등 3개로 분류하여 정보보호기반지수는 시스템과 데이터보호를 측정하고, 정보보호 환경지수는 전문인력비율, 정보보호예산비율을 측정하고, 정보화 역기능 지수는 해킹, 바이러스, 개인정보침해비율 등을 측정하는 지표로 제시하였다[19].

Ekenberg 등(1995)은 위험 분석 활동의 효과를 평가하기 위해 기업, 고객, 공급사 및 계약자, 기타 이해관계자에 대한 경제, 기술, 환경, 사회 및 심리적 측면의 성과를 확률 척도를 사용하여 측정하도록 함으로써 정보보호의 성과를 다양한 이해당사자의 측면에서 정의할 수 있음을

제시하였다[8].

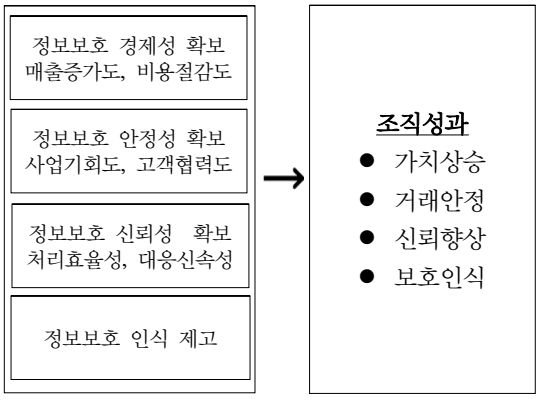
3. 연구모형, 가설설정 및 연구 방법

3.1 연구모형

최근 많은 기업들이 기업의 정보자산을 보호하고 기업 경쟁력을 강화하기 위한 수단으로 정보보호관리 프로세스 개선활동의 하나로 ISMS에 지속적인 노력을 기울이고 있다. 특히 7.7 DDoS 공격 등 지능화되고 있는 침해사고에 효율적으로 대응하기 위해서는 제품 중심의 기술적 대응에 한계가 있다는 것을 인식하고 정보보호관리체계 구축에 대한 관심이 고조되고 있다.

본 연구에서는 ISMS 인증 취득이 기업의 조직성과에 미치는 영향을 규명하기 위하여 정보보호에 대한 경제성 확보, 안정성 확보, 신뢰성 확보, 인식 제고에 대한 효과가 기업조직성과에 영향을 미치고 있는지 검증하고자 한다.

따라서 본 연구에서는 정보보호 성과측정 선행연구에서의 발견사항과 이론적 고찰을 통해 적절한 변수들을 선정하여 그림 1과 같이 ISMS 인증 취득기업이 인증 획득 후 기업 경영성과에 어떻게 영향을 미치는지를 규명하고자 한다. 조직성과에 영향을 미치는 요인으로 독립변수(측정지표) 8개와 종속변수(조직성과 지표) 4개를 유사한 성격의 지표 그룹으로 범주화하한 연구모형을 아래 그림 1과 같이 구성하였다[1,6,13].



[그림 1] 연구모형
[Fig. 1] Study Model

3.2 가설설정

연구모형에서 제시한 정보보호 경제성, 안정성, 신뢰성 확보 및 인식 제고 등 각 변수들 간 관계의 성립여부를 검증하기위해 다음과 같이 연구가설을 설정하였다[12].

① 가설1: 매출증가도는 가치상승도를 높이는데 영향을 줄 것이다.
② 가설2: 비용절감도는 가치상승도를 높이는데 영향을 줄 것이다.
③ 가설3: 사업기회도는 거래안정도를 높이는데 영향을 줄 것이다.
④ 가설4: 고객협력도는 거래안정도를 높이는데 영향을 줄 것이다.
⑤ 가설5: 처리효율성은 신뢰향상도를 높이는데 영향을 줄 것이다.
⑥ 가설6: 대응신속성은 신뢰향상도를 높이는데 영향을 줄 것이다.
⑦ 가설7: 보호역량도는 보호인식도를 높이는데 영향을 줄 것이다.
⑧ 가설8: 품질개선도는 보호인식도를 높이는데 영향을 줄 것이다.

3.3 측정방법

본 모형과 가설에 나타난 개념은 다양한 추상적 개념으로 구성되어 있어 실제로 이들의 개념을 측정하여 연구가설을 검정하기 위해서 아래 표 3과 같은 설문방법을 통해 측정하였다.

[표 3] ISMS 성과측정 방법
[Table 3] ISMS Benefit Measurement Method

개념	변수	측정 항목수	측정
정보보호 경제성 확보	매출증가도	2	리커드 7점 척도
	비용절감도		
정보보호 안정성 확보	사업기회도	2	
	고객협력도		
정보보호 신뢰성 확보	처리효율성	2	
	대응신속성		
정보보호 인식 제고	보호역량도	2	
	품질개선도		

ISMS 인증 도입 전후 개선 효과분석을 위해 2011년 11월 25일에서 12월 10일 까지 15일간 ISMS 인증 취득 76개 기업의 인증 담당자를 대상으로 설문 조사를 실시하였으며, 아래 표 4는 ISMS 인증 기업에 대한 업종현황을 나타낸 것이다.

[표 4] 정보보호관리체계 인증 현황
[Table 4] ISMS Certified Enterprises

업종	업종별 수	설문 응답	설문응답 비율(%)
정보보호업체	20	6	17
ISP/IDC	18	1	6
학교(원격대학)	17	16	94
금융/보험업	6	1	17
의료/항공운송	4	3	75
인터넷쇼핑몰/포털	3	3	100
기타	8	4	50
합계	76	34	

설문을 통해 ISMS 인증 취득 전후 효과를 정성적으로 평균을 측정한 항목별로 나타난 결과는 아래 표 5와 같이 분석되었으며, 특히, 정보보호 인식제고의 보호역량도는 약 68% 향상, 정보보호 신뢰성 확보의 처리효율성은 약 53% 향상, 정보보호 인식제고의 품질개선도 약 43% 향상 순으로 높게 나타내고 있다.

[표 5] ISMS 인증 취득 전후 효과
[Table 5] Benefits of ISMS Certification

변수	독립변수 (측정요소)	개선효과
정보보호 경제성 확보	매출증가도	14% 향상
	비용절감도	30% 감소
정보보호 안정성 확보	사업기회도	25% 향상
	고객협력도	39% 향상
정보보호 신뢰성 확보	처리효율성	53% 향상
	대응신속성	37% 향상
정보보호 인식 제고	보호역량도	68% 향상
	품질개선도	43% 향상

4. 검증 및 결과해석

4.1 분석 모형

표 5의 결과 값을 이용하여 조직성과에 미치는 정보보호 요인에 대해 ISMS인증제도 도입이전 대비 향상 정도가 얼마나 영향을 받았는지 알아보는 것으로 독립변수 8개와 종속변수 4개를 유사한 성격의 지표 그룹으로 범주화하여 경제적인 효과 정도를 알아보고자 회귀분석을 실시하였다. 또한 범주화한 방법과 회귀분석에 대한 가설설정은 아래 표 6과 같이 설계하여 분석을 실시하였다.

[표 6] 회귀분석에 대한 가설 설정
[Table 6] Assumptions for Regression Analysis

변수	독립변수 (측정요소)	종속 변수	가설설정
정보 보호 경제성 확보	매출증가도	가치 상승도	정보보호 경제성 확보(매출증가도, 비용절감도)는 가치상승도를 높이는데 영향을 줄 것이다.
	비용절감도		
정보 보호 안정성 확보	사업기회도	거래 안정도	정보보호 안정성 확보(사업기회도, 고객협력도)는 거래안정도를 높이는데 영향을 줄 것이다.
	고객협력도		
정보 보호 신뢰성 확보	처리효율성	신뢰 향상도	정보보호 신뢰성 확보(처리효율성, 대응신속성)는 신뢰향상도를 높이는데 영향을 줄 것이다.
	대응신속성		
정보 보호 인식 제고	보호역량도	보호 인식도	정보보호 인식 제고(보호역량도, 품질개선도)는 보호인식도를 높이는데 영향을 줄 것이다.
	품질개선도		

4.2 분석방법

조직성과에 미치는 정보보호 요인에 대해 ISMS인증제도 도입이전 대비 향상 정도가 얼마나 영향을 받았는지 검증하는 회귀분석의 가설검정을 위해 회귀방정식을 다음과 같이 설계하였다.

① 가치상승도 = 상수 + β_1매출증가도 + β_2비용절감도
② 거래안정도 = 상수 + β_1비용절감도 + β_2고객협력도
③ 신뢰향상도 = 상수 + β_1처리효율성 + β_2대응신속도
④ 보호인식도 = 상수 + β_1보호역량도 + β_2품질개선도

각 식에 대한 β_1과 β_2는 분석결과의 회귀분석 결과표에 자세히 나타내었다. 여기서 종속변수인 가치상승도, 거래안정도, 신뢰향상도, 보호인식도는 ISMS인증제도 도입이전 대비 향상 정도를 알아보기 위한 성과 지표로서 7점척도로 조사한 결과를 그대로 반영하였다. 또한 독립변수인 매출증가도, 비용절감도, 비용절감도, 고객협력도, 처리효율성, 대응신속도, 보호역량도, 품질개선도는 ISMS인증제도 도입이전 대비 향상 정도를 알아보기 위해 필요한 측정지표로서, 이것 역시 7점 척도로 조사한 결과를 그대로 반영하였다. 종속변수 및 독립변수 모두 동일한 척도로 사용하였기 때문에 100점 만점으로 조정

시키지 않고 그대로 반영하여 분석하였다.

4.3 분석결과

ISMS 인증업체에 설문을 통하여 34개 기업에 대하여 유효 표본을 이용하여 조직성과에 미치는 영향의 검증을 위한 회귀분석을 실시하였다.

첫 번째, 아래 표 7는 모형설계에 대한 회귀분석 결과 종속변수 가치상승도의 결과를 보면 매출증가도 각각 0.0005로 95% 신뢰구간에서 유의하고 비용절감도가 0.0565로 90%의 신뢰구간에서 유의한 것을 알 수 있다. 또한 베타 값을 통해 매출증가도와 비용절감도가 한 단위 변할 때 가치상승도는 각각 0.78183, 0.22258 만큼 증가하는 것을 알 수 있다. 회귀모형에 대한 P값 역시 0.0001로 매우 유의한 결과를 보여주며 R^2를 통해 52.68%의 설명력을 갖는다는 것을 알 수 있다. 다중공선성의 판단은 상관분석을 통해 알 수도 있지만 이처럼 VIF값을 이용해 판단할 수도 있듯이 VIF가 1.27965이므로 다중공선성이 발생하지 않았다.

[표 7] 가설1,2: 가치상승도 회귀분석 결과
[Table 7] Assumptions 1 and 2: Value Increase Regression Analysis Result

변수	상수	매출 증가도	비용 절감도	회귀 모형
자유도	1	1	1	2
베타	28.06739	078183	022258	
표준 오차	4.67939	0.20196	0.11219	
t값	6	3.87	1.98	
F값				16.7
R2				0.5268
P값	0.0001	0.0005	0.0565	0.0001
VIF	0	1.27965	1.27965	

두 번째, 거래안정도의 결과 표 8를 보면 사업기회도와 고객협력도의 P값이 각각 0.0521, 0.0346이므로 사업기회도와 고객협력도는 거래안정도에 영향을 준다. 구체적으로 사업기회도와 고객협력도가 한 단위 증가할 때 거래안정도는 각각 0.33361, 0.38153만큼 증가한다. 또한 회귀모형에 대해서도 매우 유의한 결과를 가져오며 39.18%의 설명력을 갖고 있으며, 다중공선성 역시 발생하지 않았다.

[표 8] 가설3,4: 거래안정도 회귀분석 결과
[Table 8] Assumptions 3 and 4: Result of Transaction Stability Regression Analysis

변수	상수	사업 기회도	고객 협력도	회귀 모형
자유도	1	1	1	2
베타	9.64706	0.33361	0.38153	
표준 오차	4.67939	0.20196	0.11219	
t값	1.1	2.02	2.21	
F값				9.66
R2				0.3918
P값	0.2801	0.0521	0.0346	0.0006
VIF	0	1.40241	1.40241	

세 번째, 신뢰향상도의 회귀분석 결과 [표 9], 처리효율성에 대해서는 유의한 결과를 가져오지만, 대응신속성에 대해서는 유의하지 않은 결과를 가져온다. 처리효율성이 한 단위 증가할 때 신뢰향상도는 0.36907만큼 증가한다. 회귀모형에 대해서는 P값이 0.0012이므로 유의하며, 36%의 설명력을 갖고 있으며, 다중공선성 역시 발생하지 않았다.

[표 9] 가설5,6: 신뢰향상도 회귀분석 결과
[Table 9] Assumptions 5 and 6: Result of Trust Increase Regression Analysis

변수	상수	처리 효율성	대응 신속성	회귀 모형
자유도	1	1	1	2
베타	31.7719	0.36907	0.20704	
표준 오차	7.96772	0.18093	0.15536	
t값	3.99	2.04	1.33	
F값				8.44
R2				0.36
P값	0.0004	0.0503	0.1927	0.0012
VIF	0	1.777171	1.777171	

마지막으로, 보호인식도의 회귀분석 결과 [표 10]는 보호역량도는 유의하지만 품질개선도는 유의하지 않은 결과가 나왔다. 하지만 회귀모형에 대해서는 유의한 결과가 나왔기 때문에 가설은 받아들여진다. 보호역량도가 한 단위 증가할 때 보호인식도는 0.89569만큼 증가하고, 회귀모형에 대한 설명력은 78.41%이고, 다중공선성은 발생하지 않았다.

[표 10] 가설7,8: 보호인식도 회귀분석 결과
[Table 10] Assumptions 7 and 8: Result of Security Awareness Regression Analysis

변수	상수	보호 역량도	품질 개선도	회귀 모형
자유도	1	1	1	2
베타	4.1402	0.89569	0.1256	
표준 오차	6.72883	0.11288	0.11183	
t값	0.62	7.93	1.12	
F값				54.47
R2				0.7841
P값	0.543	0.0001	0.2703	0.0001
VIF	0	1.40241	1.40241	

ISMS인증제도가 조직성과에 미치는 영향요인들에 회귀분석을 통해 각각의 요인이 조직업무의 개선효과 및 도입이전 대비 향상 정도가 얼마나 영향을 받았는지를 실증적으로 검증하였다. 또한 전체 업무의 개선효과 및 도입이전 대비 향상 정도를 8개의 효과 군으로 분류하여 분석한 결과, 가치상승도, 정보보호 경제성 확보, 신뢰향상도, 정보보호 안정성 확보, 정보보호 신뢰성 확보, 정보보호 인식 제고 등 총 6개의 효과 군에서 보다 높은 효과가 있다는 결과가 아래 [표 11]과 같이 도출되었다. 즉, 연구모형의 가설들을 받아들일 수 있다는 결과로 검증되었다. 따라서 정보보호 경제성 확보, 정보보호 안정성 확보, 정보보호 신뢰성 확보, 정보보호 인식 제고 모두 경제적인 효과를 높이는데 기여하였다는 결론을 내릴 수 있다.

[표 11] 연구 모형 검증 결과 요약
[Table 11] Summary of Study Model Verification Result

가설	내용	검증 결과
1	ISMS인증기업의 매출증가도는 가치상승도를 높이는데 영향을 줄 것이다.	채택
2	ISMS인증기업의 비용절감도는 가치상승도를 높이는데 영향을 줄 것이다.	채택
3	ISMS인증기업의 사업기회도는 거래안정도를 높이는데 영향을 줄 것이다.	채택
4	ISMS인증기업의 고객협력도는 거래안정도를 높이는데 영향을 줄 것이다.	채택
5	ISMS인증기업의 처리효율성은 신뢰향상도를 높이는데 영향을 줄 것이다.	채택
6	ISMS인증기업의 대응신속성은 신뢰향상도를 높이는데 영향을 줄 것이다	기각
7	ISMS인증기업의 보호역량도는 보호인식도를 높이는데 영향을 줄 것이다.	채택
8	ISMS인증기업의 품질개선도는 보호인식도를 높이는데 영향을 줄 것이다.	기각

가설들을 통해 알아본 위의 검증 결과로 ISMS 인증이 가치상승도, 거래안정도, 신뢰향상도, 보호인식도를 향상시키며 경제적인 효과를 높이는데 기여하였다는 결론을 내릴 수 있었다. 이러한 ISMS 인증의 효과에는 정부의 정책적, 법률적, 제도적인 지원과 관심이 큰 영향을 끼쳤다고 판단이 되는데 그 근거는 다음과 같다.

국내에서는 ISMS 인증기업에 정책적으로 국가공공기관, 신용평가기관, 기술보증기금, 민간 기관들의 조달·입찰, 기업신용평가 등에 가산점을 부여하고 있으며, ISMS 인증을 받은 경우 의무적으로 받아야하는 정보보호안전진단을 면제하는 한편 보험사의 정보보호관련 보험 가입 시 할인율을 적용하는 등 다양한 혜택을 부여하고 있다. 이러한 정책적 지원과 혜택은 특히, 조직의 가치상승 및 신뢰향상에 긍정적 영향을 끼치고 있는 것으로 판단된다.

특히 ISP, IDC, 쇼핑몰 등 기업에 대한 정보보호수준 제고를 위해 2003년 1.25 인터넷 침해사고이후 기업들이 최소한의 정보보호 조치를 취하도록 의무화하여 일반 국민들이 안전하게 인터넷 이용을 할 수 있도록 한 정보보호안전진단제도와 본 연구에서 다루는 ISMS 인증 제도를 추진해 오고 있는데, 이러한 제도들은 가치상승, 거래안정, 신뢰향상, 보호인식 모두에 긍정적 영향을 끼치고 있는 것으로 판단된다.

따라서 회귀분석을 통하여 각각의 가설들이 ISMS인증기업의 조직성과에 긍정적으로 미치는 영향을 검증한 결과를 유추해볼 때, 매출증가도와 비용절감도, 사업기회도, 고객협력도, 처리효율성, 보호역량도 등이 조직성과의 중요한 항목인 정보보호의 경제성 확보에 직접적으로 기인한다는 것이 확인되었으니 이를 경영진과 담당자들에게 지속적인 인식제고가 필요하며, 조직의 경영전략, 정보화전략 및 정보보호전략 등이 일관성 있도록 추진하고, 이에 걸맞는 정보보호관리체계 인증이 조직 내에 활성화되도록 하는 등 이에 따른 타당성과 중요성을 항상 강조할 필요가 있다.

본 연구는 정보보호관리체계 인증이 기업경영성과에 어떻게 영향을 미치는지 살펴보고자 하는 것이다. 이를 위해 정보보호 경제성 확보, 안정성 확보, 신뢰성 확보, 인식 제고 변수를 포함한 연구모형과 가설을 설정하고, 검증한 결과는 다음과 같이 요약 할 수 있다.

첫째, 정보보호 경제성 확보는 기업의 가치상승도를 높이는데 긍정적 영향을 미치고 있다. 기업이 정보보호관리체계 인증을 취득함으로써 기업 이미지 제고 등 홍보효과로 인해 고객 확보로 연계되어 궁극적으로 기업의 매출액이 증가하게 되고 침해사고에 대한 사전 예방을 통해 발생 가능한 잠재적 사고에 대한 피해 예방으로 비

용절감 효과가 있음을 확인하였다.

둘째, 정보보호 안정성 확보는 거래안정도를 높이는데 영향이 있는 것으로 검증되었다. ISMS 인증이 기업 가치 상승에 직접적으로 성과에 영향을 미치지만 안정성 확보를 통해 거래 안정도에 영향을 주고 있으므로 기업 정보자산의 안정성 확보에 노력해야 한다.

셋째, 정보보호 신뢰성 확보는 신뢰향상도를 높이는데 긍정적 영향을 주는 것으로 나타났다. 하위변수인 ISMS 인증에 따른 업무 처리 효율성은 신뢰향상도에 영향을 미치는 것으로 나타났으나, 대응신속성 면에서는 영향이 없는 것으로 나타났다.

넷째, 정보보호 인식 제고는 보호인식도를 높이는데 영향을 미치는 것으로 나타났다. ISMS 인증을 취득함으로써 전 직원에 대한 동기부여와 함께 정보보호 활동을 통해서 직원의 역량강화와 정보보호 인식도에 영향을 미치는 것으로 나타났다. 다만, 품질개선 면에서는 영향이 없음이 검증되었다.

5. 결론

결론적으로 본 연구에서는 ISMS인증제도가 조직성과에 미치는 영향요인들에 대한 회귀분석을 통해 각각의 요인이 조직업무의 개선효과 및 도입이전 대비 향상 정도에 얼마나 영향을 주었는지 알아보았다. 또한 전체 업무의 개선효과 및 도입이전 대비 향상 정도를 8개의 효과군으로 분류하여 분석한 결과, 가치상승도, 정보보호 경제성 확보, 신뢰향상도, 정보보호 안정성 확보, 정보보호 신뢰성 확보, 정보보호 인식 제고 등 총 6개의 효과 군에서 보다 높은 효과를 보인다는 결과가 도출되었다. 즉, 연구모형의 가설들을 받아들일 수 있다는 결과로 검증되었다. 따라서 정보보호 경제성 확보, 정보보호 안정성 확보, 정보보호 신뢰성 확보, 정보보호 인식 제고 모두 경제적인 효과를 높이는데 기여하였다.

따라서 향후 정보보호관리체계 인증의 성과측정에 관한 연구가 활발하게 진행되고, 정보보호 지원 분야별 특성에 맞는 다양한 측정모형을 개발하고 기업의 성과뿐만 아니라 국가차원의 정보보호 성과를 측정 하는데 활용될 수 있도록 발전 되어야 할 것이며, 정보보호관리체계 성과측정을 위한 국제기준이 마련되어 국제표준으로 활용할 수 있는 모형이 개발되고 발전되어야 할 것이다.

References

[1] Shin Seung ho, “Study of Effect of BSC Operation to Public Agency Performance”, PhD Dissertation, Dankuk University, pp.65 89, 2007.

[2] Hong Gi hyang, “Study of Effect of Information Security Control and Activities to Information Security Performance”, PhD Dissertation, Kukmin University, pp.68 138 2003

[3] Kim Jeong deok and Park Jeong eun, “Study of Return on Investment of TCO Based Information Security (ROSI)”, Korea Society of Digital Policy Foundation Conference Proceeding, pp.251 261, 2003.

[4] Seon Han gil, "Effect of Koran Enterprises’ Information Security Policy and Organization Factors on Information Security", Korea Society of Management Information Systems, Spring Conference Proceeding, pp.1087 1095, 2005.

[5] Shin Il sun, “Exploratory Study of Economic Significance of Information Security”, Information Security Review, Vo. 1, No. 1, pp.27 40, 2005.

[6] Goh Hyeon u and Jeong Young bae, "The Effect of ISO 9001:2000 Quality Management System's Requirement on Business Performance" Journal of Society of Korea and Systems Engineering Vol, 30, No. 3, pp.135 149, September 2007.

[7] Nah Jung su and Jeon Seong hyeon, “Study of Effect of Information System Auditor’s Competency on Auditing Performance”, Informatization Policy, Vol. 14, No. 2, Summer 2007, pp.3~18.

[8] Ekenberg, L., Subhash Oberol, & Istvan Orci, " A cost model for managing information security hazards", Computer Security, Vol. 14, pp.707-717, 1995.

[9] Frank, J., Boas Shamir, & Warren Briggs, "Security-related behavior of PC users in organizations", Information & Management Vol. 21, pp.127-135, 1991.

[10] Legal Knowledge Information System, Act for Information and Communication Network Usage Promotion, Information Security, etc., 2011.

[11] KISA, “2008 Information Security Status Survey - Enterprises”, 2008.

[12] Kim In ho, Gu Tae yong and Choe Geol seong, “An Empirical Suudy on the Firm Performance of Quality”, Management System (ISO9001/00)

[13] Kim Yu jin, “Study of Information Security Process Model Development”, Joongang University, 2000.

[14] KISA, “Study of Information Security Governance Standardization for Information and Communication

Enterprises", 2008.
[15] KISA, "Development of Enterprise Information Security Level Evaluation Methodology", 2008.
[16] KISA, "Study of Enhancement of Information Security Safety Diagnosis System Operation", 2009.
[17] KISA, "Study of Information Security Management System Development to Introduce Information Security Governance Concept", 2009.
[18] KISA, "Development of Information Security Level Evaluation Items and Methodology", 2002.
[19] KISA, "Calculation of National Information Security Level Evaluation Index and Study of Drive for Globalization", 2006.
[20] KISA, "2011 Information Security Status Survey - Enterprises", 2011.
[21] ISO/IEC27001: Information technology – Security techniques – Information security management systems – Requirements, 2005.
[22] ISO/IEC27002: Information technology – Security techniques – Code of practice for information security management, 2005.

배 영 식(Young-Sik Bae) **[정회원]**

- 2011년 2월 : 연세대행정대학원 행정학과(행정학 석사)
- 2011년 2월 ~ 현재 : 동국대학교 법학과 박사과정

<관심분야>
정보통신