Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.3, Jun. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.3.821

보안인증의 경제적 효과에 대한 연구동향 분석: ISMS(정보보호관리체계)를 중심으로*

공 희 경,† 전 효 정, 이 송 하, 강 민 성, 김 태 성‡
충북대학교

Research Trends in Economic Effects of Information Security Certification: Focused on the ISMS (Information Security Management System)*

Hee-Kyung Kong,† Hyo-Jung Jun, Song-Ha Lee, Min-Seong Kang, Tae-Sung Kim‡
Chungbuk National University

요 약

정보보호 공시제도 도입과 정보통신망법 개정에 따라 ISMS(정보보호관리체계) 인증대상이 확대되어 조직의 보안 컴플라이언스 환경이 변화하고 있다. 공시제도와 인증제도 도입을 위해 조직들은 적정수준의 투자를 고려하고 있으나 정보보호관리체계 도입에 대한 경제적 효과나 투자의 범위 및 대상에 대한 의사결정 기준이 명확하게 제시되지 않고 있다. 따라서 본 연구는 정보보호 분야의 각종 인증제도 효과를 분석하기 위한 국내외 연구동향에 대해 조사해보고, 연구된 논문들의 연구주제와 연구방법을 분석하였다. 이를 통해 관련분야 연구 활성화 및 정보보호관리체계 도입을 위한 기초자료 분석에 활용될 수 있을 것이다.

ABSTRACT

This study investigates the domestic and international research trends to analyze the economic effects of various information security certification systems. Results of the study can suggest future research topics for researchers, and help make rational decision-making on introducing information security management systems for practitioners.

Keywords: Research Trends, Information Security Certification, Economic Effects, ISMS

I. 서 론

미래창조과학부는 국가 사이버보안능력 제고와 국내 정보보호 산업의 진흥을 목적으로 정보보호최고책임자(Chief Information Security Officer, CISO) 신고 의무화(2014년 11월), ISMS 인증 의무대상 확대(2015년 11월; 정보통신망법 일부개정), 정보보호 준비도 평가 및 정보보호 공시제도 시행(2015년 12월; 정보보호산업진흥원 제정) 등을 추진하고 있다. 정부는 이러한 일련의 제도들을 통해 국내 기업 및 기관의 사이버보안 침해에 대한 대항력을 배양하고 나아가 정보보호 산업의 진흥을 도모할 수 있을 것으로 기대하고 있다. 특히, ISMS 인증 의무대상 기관이 침해사고 발생 시 사회·경제적 파급효과가 큰 대형 제조업체나 대국민 필수 서비스를 제공하는 전력·가스·에너지 관련 기관 등까지 포함하게 됨에 따라 단기적으로 의무 인증 대상 기업이 1,500~2,000개까지 늘어날 전망이다. 따라서, 인증에 도움을 주는 다양한 보안 장비나 솔루션, 컨설팅 수요도 함께 커지며 정보보호 시장이 성장할 것으

Received(03. 07. 2016), Modified(04. 07. 2016), Accepted(04. 07. 2016)
* 본 연구는 2011년도 정부(교육과학기술부 NRF-2011-0025512)의 재원으로 한국연구재단 기초연구사업의 지원을 받아 수행하였습니다.
† 주저자, konghk1@naver.com
‡ 교신저자, kimts@chungbuk.ac.kr(Corresponding author)

로 기대되고 있으며, 정보보호 전담 직원이나 조직이 없던 중소·중견 기업으로 범위가 확대되기 때문에 전반적으로 정보보호 전문인력에 대한 수요도 증가할 것으로 기대된다. 또한 정보통신망법의 개정에 따라 ISMS 인증 의무대상 기관이 확대되고 ISMS 인증을 받지 않는 기관에 대한 과태료도 상향조정될 예정이다. 더불어 정보보호산업진흥법에 의거하여 정보보호 준비도 평가 및 정보보호 공시제도가 시행(자율)될 예정이지만, 기업 및 기관의 정보보호에 대한 직접적인 투자가 확대되지 않는다면 일련의 이러한 조치들은 사회·경제적 효과를 보기도 전에 번거로운 행정절차로 전락할 가능성도 있다. 따라서, 제도의 시행과 함께 기업 및 기관들의 실질적인 정보보호 투자 확대를 이끌어낼 수 있는 강력한 유인책이 필요하다. 2015년 12월 23일 시행된 정보보호 공시제도의 공시항목에 정보보호 투자의 비중(IT투자 대비)과 정보보호 인력의 비중(정보화인력 대비) 등이 포함되어 있지만 의무적인 것은 아니며 반드시 맞춰야 할 하한선이 제시되어 있는 것도 아니다.

금융권에서는 2011년부터 이미 "5·5·7 규정"을 제정하여 시행하고 있다. 이는 전체 회사 인력 5%를 IT인력(내부+자회사+외주)으로, IT인력의 5%를 보안 인력으로, IT예산의 7%를 보안 예산으로 책정해야 한다고 명시하고 있는 것이다[1)][1]. 2013년에는 일련의 사이버보안 사고를 계기로 금융권 전산보안 전반에 대한 실태점검과 태스크포스 운영을 통해 종합적인 개선대책을 마련하여 발표하면서, 금융회사의 보안조직 및 인력 역량 강화를 의무화하였다[2]. 이와 관련하여, 한국은행(2015)의 조사에서는 2014년 현재 국내 금융기관 155개 중 81.9%(127개 기관)가 CISO를 지정하고 있으며 전임은 22.0%로 나타났다[3]. 정보보호 인력이 IT인력에서 차지하는 비중은 8.4%로 조사되었으며, 금융기관의 총 예산 66조 2,482억 원 중 IT예산은 5조 4,982억 원, 그 중 정보보호 예산은 5,666억 원(IT예산의 10.3%)으로 조사되었다. 이를 토대로 살펴보면, 금융기관들은 정보보안 강화를 위해 금융위원회가 제시하고 있는 5·5·7 규정을 대체적으로 준수하고 있는 것으로 볼 수 있으며, 정부가 제시한 최소한의 규정을 준수함으로써 정보보안 수준을 향상시킬 수 있을 것으로 여기고 있음을 알 수 있다.

향후, IT기업은 물론 비IT 분야에까지 ISMS 인증 의무대상이 확대되고 정보보호 공시제도(정보통신을 기반으로 사업을 영위하는 기업 대상)가 자율적으로 시행될 예정이지만, 이러한 제도들의 안정적인 운영과 효과성 확보를 위해서는 과연 어느 정도의 정보보호 예산이 투입되어야 하는가에 대한 가이드라인을 제시해 줄 필요가 있다. 미국을 중심으로 보안침해사고에 대한 공시가 의무화되는 추세에 있긴 하지만, 이의 주요 목적은 소비자들의 개인정보보호에 있음을 볼 때, 정보보호 공시제도가 잘 운영되기 위해서는 보다 강제적이고 구체적인 정보보호 투자에 대한 가이드라인이 필요하다. 또한, 정보보호관리체계 인증제도를 포함하여 정보보호 분야에 적용되고 있는 여러 제도들의 효과성에 대해서도 자료축적을 통한 지속적인 조사·분석이 필요하다.

사이버보안 사고의 규모가 대형화되고 유형도 다양화되고 있어 더 이상 사전 예측 및 예방을 통한 보안이 불가능한 상황에서 정부는 규제가 아니라 자율적으로 기업 및 기관이 직접 정보보호 수준 향상을 위한 투자를 확대하기를 기대하지만, 정보보호에 대한 투자효과가 즉각적으로 나타나지 않는다는 점에서 이러한 자연적인 시장논리에 의한 투자확대가 실현되기까지는 상당한 시간이 필요하다. 더욱이, 정보보호를 위해 필요한 비용과 그러한 비용을 들임으로써 얻을 수 있는 편익에는 무형적 요소가 다수 존재하며, 정보보호의 성과가 광범위하여 범위설정이 어렵고 성과를 얻기까지 많은 시간이 소요되므로 직·간접적인 편익을 측정하는 데에도 많은 어려움이 존재한다. 따라서, 기업 및 조직의 자율적이면서도 보다 체계적인 정보보호 인프라 구축을 독려하기 위해서 투자의사결정을 지원할 수 있는 가이드라인이 필요하며, 이는 경영·사회적인 차원에서의 경제적 효과분석 연구로 진행되어야 한다. 본 논문에서는 국내·외에서 진행되고 있는 정보보호 분야 인증 및 제도에 대한 연구동향과 그 경제적 효과에 대한 연구동향을 조사해 봄으로써, 향후 보다 객관적인 정보보호 관리체계 인증의 효과분석을 위한 연구방향을 검토한다.

II. 이론적 배경

2.1 ISMS 인증의 개요 및 필요성

K-ISMS는 기업(조직)이 각종 위협으로부터 주

1) 전자금융감독규정 제8조(인력, 조직 및 예산) [시행 2015. 6.24.][금융위원회고시 제2015-18호, 20156.24., 일부개정]

요 정보자산을 보호하기 위해 수립·관리·운영하는 종합적인 체계(정보보호관리체계)의 적합성에 대해 인증을 부여하는 제도이다. 2001년부터 제도가 도입되어, 2002년부터 인증서 발급이 시작되었으며 현재까지 유지되고 있는 인증서는 총 396건이다[4]. 근거법령은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」제50조, 「정보보호관리체계 인증 등에 관한 고시 (미래창조과학부고시 제2013-36호)」 등이다. 의무대상자 외 기업이 인증 취득을 희망할 경우, 자율적인 신청을 통한 인증 심사가 가능하다.

K-ISMS 인증심사 기준은 정보보호 5단계 관리과정 요구사항 12개 통제사항, 정보보호대책 13개 분야 92개 통제사항 총 104개 통제사항으로 구성되어 있다. 2015년 12월 현재 ISMS 인증기관은 한국인터넷진흥원(KISA)이며, 인증심사기관은 한국정보통신진흥협회(KAIT)와 한국정보통신기술협회(TTA, 2015년 2월 지정) 등 2개 기관이다.

2016년부터는 K-ISMS, PIMS(Personal Information Management System, 개인정보보호관리체계), PIPL(Personal Information Protection Level, 개인정보보호 인증제도) 인증 통합이 본격화될 예정이며, K-ISMS 인증 대상이 비 ICT분야(의료·교육·에너지 등)로 확대되고 위반사업자에 대한 과태료도 대폭 상향될 예정이다. 또한, 인증기준의 최신성 확보를 위한 방안으로 인증기준 개정 수요 조사를 통해 인증기준을 정비할 방침이다. 이러한 상황에서, 향후 정보보호관리체계 인증을 비롯해 정보보호 분야에 적용되고 있는 각종 인증 및 제도들의 실효성과 효과성에 대한 객관적인 근거마련을 위한 연구가 촉발될 것으로 보인다. 정부는 인증 및 제도들을 통해 조직의 정보보호 성과를 높일 수 있기를 고대하지만, 실질적으로 기업 등은 인증 및 제도 도입을 비용(수수료)만 들 뿐 실질적으로 정보보호 성과 달성에 영향이 없거나 미미하다고 여겨 미온적 의무사항으로 여길 뿐 기업 내외부적으로 창출 가능한 인증 및 제도들의 성과를 측정하지 않고 있다. 따라서 인증 및 제도의 실효성 확보를 위해서는 인증 및 제도의 의무화(의무대상 확대)와 함께 도입 효과를 측정해 객관적인 판단근거를 마련해 주어야 한다. 정보보호관리체계 인증제도가 도입된 역사가 오래 되었기 때문에, 그 효과를 측정하기 위한 다방면에서의 노력이 있어 왔다. 그러나, 객관적인 측정에는 실제 인증 및 제도를 수행하는 기업의 적극적인 참여와 자료제공이 필요하지만, 이러한 데이터를 획득하는 것은 데이터의 보안성으로 인해 매우 제한되어 왔다.

2.2 국내·외 정보보호 인증 및 제도 현황

국내·외 정보보호 인증 및 제도 현황 등에 대한 연구는 구글 스칼라에서 (cyber)security certification, (cyber)security standard, 정보보호(보안) 인증, 정보보호(보안) 인증제도 등의 키워드 검색을 통해서 나오는 문헌들에서 주로 다루는 인증 및 제도를 대상으로 정리 하였다. 국내의 대표적인 정보보호 인증 및 제도로는 K-ISMS, PIMS, PIPL 등이 조사되었다. 국외 정보보호 인증 및 제도로는 ISO/IEC 27001, FISMA(Federal Information Security Management Act), JIPDEC ISMS(JISMS), CC(Common Criteria), TCSEC(Trust Computer System Evaluation Criteria), ITSEC(Information Technology Security Evaluation criteria), CMVP(Cryptographic Module Validation Program) 등이 조사되었다. ISO/IEC 27001은 국제 표준화 기구(ISO)에서 정보보호 관리를 위해 제정한 표준 실무규약으로 BS7799를 모태로 하고 있으며, 글로벌화 된 기업 및 정부의 정보보호에 대한 국제적인 인증의 필요성으로 인해 만들어졌다. 미국 FISMA는 2002년도 제정된 전자정부법(e-Government Act) 중 3편(Title III)의 SEC301(Information Security)에 포함된 법률로써 연방 정부의 정보와 운영 및 자산을 보호하기 위한 포괄적인 기본 프레임워크를 수립하고, 정부기관이 정보화 정보시스템 보호를 위해 전사적 정보보호 프로그램을 개발, 문서화, 구현을 요구하고, 연방정부 기관의 정보보안 강화를 위해 제정된 법으로 연방정보보안관리법이라고 할 수 있다. 일본의 JISMS(적합성 평가제도)는 JIPDEC(Japan Information Processing Development Corporation)이 운영하며, 국제 표준규격인 ISO/IEC 27001에 준거한 정보보안 매니지먼트 시스템에 대한 제3자 적합성 제도이다. 이는 일본의 정보보안 수준 전체의 향상에 공헌하며, 해외에서도 신뢰를 얻을 수 있는 정보보안 수준의 실현을 목적으로 하는 제도이다. TCSEC은 미국에서 오렌지북으

로 불리는 평가기준이며 1985년도에 제정되었다. 이후 영국의 그린북 시리즈, 독일의 블루&화이트북, 프랑스의 블루-화이트-레드북 등이 계속적으로 제정되면서 1990년에 영국, 독일, 프랑스, 네덜란드가 협력하여 유럽의 공통적인 평가기준서인 ITSEC이 출간되었다. 또한, 캐나다는 1991년 CTCPEC(Canadian Trusted Computer Product Evaluation Criteria)라는 평가기준을 제정하였다. CC(Common Criteria)는 각 나라별로 정보보호 평가기준이 상이하여 평가에 소요되는 비용과 시간이 많이 소요됨에 따라 평가기준 간 통합의 필요성에 의해 1996년 1월 CTCPEC, FC, TCSEC, ITSEC을 망라하여 단일의 국제 공통 평가 인증제도로 발표된 것이다. CC로 통합된 다양한 정보보호 인증 및 제도 중 자료를 구하기 힘든 것들은 제외하였으며, 가장 많이 언급된 키워드는 TCSEC, ITSEC, CC 등으로 분석된다.

2.3 정보보호 인증 및 제도에 대한 연구

국내·외의 정보보호 인증 및 제도에 대한 연구는 주로 기존의 정보보호 인증 및 제도에 대한 분석, 정보보호 인증제도의 발전방향 및 개선방안 연구, 정보보호 인증 도입 시의 장애요인 분석, 평가지표개발 등으로 구분되었다. 국내 연구로는 김유진, 김정덕과 김도일은 조직의 정보보호 수준을 평가할 수 있도록 정보보호 프로세스 평가모델을 개발하여 제시하였으며[5], 홍영란과 김동수는 CC인증 기업을 대상으로 설문조사를 통해 CC 인증이 국내·외 보안 솔루션에 미친 긍정적 효과에 대해 실증분석을 하였다[6]. 박경태와 김세헌은 ISMS 인증 시 장애요인을 문헌연구를 통해 분석하고 이를 설문조사하여 검증하였다[7]. 강현선은 관리적, 기술적, 물리적 정보보안 대응방안의 통합적 모델인 정보보호 관리체계의 필요성과 국제적인 표준화 동향 및 국내·외 인증 제도(K-ISMS와 ISO 27001)를 분석하여 비교하였다[8]. 국외 연구로는 Eloff와 Von Solms가 조직의 보안수준강화를 위해 제품인증과 프로세스 인증을 동시에 고려하여 기업의 전반적인 보안수준이 향상되는 것을 정성적으로 분석하였다[9]. Huang 등[2006]은 대만의 제조업체를 대상으로 설문조사를 통해 BSC를 이용한 보안성과를 측정하였다[10].

2.4 정보보호 인증의 경제적 효과에 대한 연구

정보보호 관련 인증의 경제적 효과에 대한 연구로는 정보보호 인증 도입 요인에 대한 연구, 정보보호 인증 도입 효과 등의 연구가 대부분으로 분석되었다. 전반적으로 국내·외 인증의 경제적 효과에 관한 연구는 많지 않은 것으로 분석되었다. 정보보호 인증 도입의 효과분석에 대한 연구들도 관련 인증 도입으로 인해 기업에 긍정적인 영향을 미친다는 연구가 대다수였지만, 실제 경제적·재무적으로 정량적인 수치를 제시하는 연구보다는 조직의 성과향상과 같은 정성적인 연구가 주를 이루고 있으며, 세부적인 효과 측정을 위한 지표에 대한 연구는 부족하고, 측정방법론이 매우 간단하거나 정교하지 않다. 또한 특정 산업만의 인증에 대한 효과를 분석하는 등 많은 한계점을 보여주고 있다. 게다가 이 같은 인증 도입의 효과를 단순 설문조사와 문헌조사만을 통해 실효성이 없다고 주장하는 연구도 있다.

국내 연구로는 박성욱, 윤종민이 산업연관분석을 활용해 정보보호산업의 경제적 파급효과를 거시적 관점에서 분석하였다[11]. 김인관 등은 중소기업의 산업기술보호를 위해 국제표준(ISO 27001)의 영향요인을 분석하여 중소기업의 산업기술보호에 필요한 ISMS의 효과적 활용방안을 제시하였다[12][13]. 장상수는 ISMS 인증을 받은 조직을 대상으로 조건부가치측정법을 활용한 설문을 실시하여 경제적 가치를 측정하였다[14]. 박경태와 김세현은 ISMS 인증에 관심이 있는 기업을 대상으로 ISMS 인증 시 예상하는 효과요인이 인증의도에 어느 정도 영향을 미치는지를 설문조사를 통해 분석하였다[15]. 장상수와 김상춘은 ISMS 인증 취득 후 1년 이상 유지조직을 대상으로 설문조사를 실시하여 성과 측정 모형과 지표를 제시하였다[16]. 국외 연구로는 Humphreys이 ISMS의 통제항목 분석을 통해 내부자 위협을 감소시킬 수 있는 요인을 파악하였다[17]. Anderson과 Fuloria는 보험산업(도덕적 해이와 역선택)과 중고차 시장(정보의 비대칭성)을 예시로, 보안인증 및 평가의 실패이유를 제시하며, 새로운 보안위협에 대응 가능한 수요맞춤형 보안인증의 필요성을 제시하였다[18]. Boehmer는 ISMS의 핵심성과지표(KPI)를 효과성과 경제적 효율성으로 설정하여 수리적 모델을 이용해 두 지표 간 trade-off 관계를 분석하여 ISMS의 구현비용과 가치 사슬상의 투자효과에 대한 연구 필요성을 제기하였다[19].

Park 등은 ISMS 인증취득기업 CISO를 대상으로 설문조사를 실시하여 ISMS 인증이 조직성과에 긍정적인 영향이 있음을 회귀분석을 통해 증명하였다[20]. Chang은 중소기업을 선정하여 ISMS 인증 전후의 과거 3년간 재무정보를 유사기업과의 성과분석을 통해 비교, 인건비 부문에 효율성 개선이 있음을 제시하였다[21].

2.5 정보보호 제도의 경제적 효과에 대한 연구

정보보호 관련 제도는 다양한 제도가 존재하고 있지만, 경제적 효과와 관련된 연구는 사전진단제도, 정보보안 공시제도, 안전진단 등과 관련하여 경제적 효과를 분석한 연구들이 일부 있다. 많은 연구들이 정보보호 관련 제도의 경제적 효과에 대하여 산술식을 통해 정량적으로 경제적 효과를 표현하고 있지만, 양주 진품인증, 온라인게임 서비스 등 일부 사례에 적용하여 정량화하고 있어 일반적인 방법론으로 적용하는 데에는 한계점이 존재한다. 장상수 등은 성과관리방법론과 균형성과표(BSC) 모델을 이용하여 정보보호 안전진단 성과분석 모델을 제시하였으며[22], 정보보호 성과 지표 산식을 안전진단 성과분석 사례 적용을 통해 제시하였다. 공희경과 김태성은 정보보호 사전진단 투자효과를 BSC 관점의 정보보호 투자효과 분석 프레임워크에 적용하여 분석하고 사전진단 대상 서비스에 대한 보안사고 비용 산정 모형을 제시하고 정량적인 경제적 효과 수치를 분석하였다[23]. 유동영 등은 정보보호 사전진단 제도를 온라인게임에 적용하여 계량적인 성과를 측정할 수 있는 비용효과 산정결과를 분석하였다[24]. 전효정과 김태성은 정성적인 정보보안 공시제도 도입의 효과분석을 위해 시스템적 사고방식 기반의 시뮬레이션 모델링 기법인 인과지도(causal-loop)를 사용하여 정보보안 공시제도 도입의 타당성 및 필요성을 분석하였다[25].

III. 연구범위 및 연구방법

3.1 용어정의

ISMS(정보보호관리체계)를 중심으로 보안 인증 경제성 연구동향 분석을 하기 전에 먼저 'ISMS(정보보호관리체계)' 및 '보안 인증 경제성 연구'란 무엇인지 정의해 보고자 한다.

정보보호관리체계란 조직의 자산에 대한 안전성 및 신뢰성을 향상시키기 위한 절차와 과정을 체계적으로 수립, 문서화하고 지속적으로 관리·운영을 통하여 정보보호목표인 정보의 기밀성, 무결성, 가용성을 실현하기 위한 일련의 과정 및 활동을 말한다[2].

보안[3] 인증의 경우에는 보안 인증을 경제적 관점으로 접근한 연구들을 포괄적으로 정의하는 용어가 명확하지 않아, 본 연구에는 '보안 인증 경제성' 이라는 용어를 사용하였다. 보안 인증 경제성은 보안 인증 효과(분석), 보안 인증 성과 측정 등의 용어와 맥락을 같이한다고 볼 수 있으며 사전적 의미 등을 참고하여 다음과 같이 정의하였다. 먼저 '(정보)보안'이란 정보시스템 및 정보통신망을 통해 수집·가공·저장·검색·송수신 되는 정보의 유출·위변조·훼손 등을 방지하기 위하여 관리적·물리적·기술적 수단을 강구하는 일체의 행위로서 사이버안전을 포함하는 것[4]이며, '인증(Certification)'이란 제품 등 평가대상을 일정한 표준기준 또는 기술규정 등에 적합한지 여부를 평가하여 안전성 및 신뢰성 등을 인증하는 절차 및 제도이다. '경제성'은 재물, 자원, 노력, 시간 따위가 적게 들면서도 이득이 되는 성질[5]을 뜻하기 때문에, 따라서 보안 인증 경제성이란 '(정보시스템 및 정보통신망을 통해 수집·가공·저장·검색·송수신 되는) 정보의 유출·위변조·훼손 등을 방지하기 위한 관리적·물리적·기술적 수단이 일정한 표준기준 또는 기술 규정 등에 적합한지 여부를 평가하고, 이에 대한 평가를 통해 재물, 자원, 노력, 시간 따위가 적게 들면서도 이득이 되게 하는 성질' 을 의미한다. 즉, 보안 인증 경제성 연구란 ' 보안 인증 도입으로 인한 비용효과를 경제적 관점으로 분석한 연구 또는 연구결과가 개인 및 조직의 보안 인증 도입 관련 의사결정에 도움이 되는 연구'를 의미하며, 이 같은 정의를 기반으로 연구를 진행하였다.

3.2 연구범위

본 연구는 구글스칼라, RISS, NDSL 등의 논문검색 데이터베이스에서 사전에 조사한 국내외 정보보

2) 한경 경제용어사전(2015.06.27.)
3) 본 연구에서는 '(정보)보안'과 '(정보)보호'를 동일한 의미로 사용함
4) 산업통상자원부 훈령 제3호, 산업통상자원부 정보보안 세부지침 전부개정령안(2013.4.22.)
5) 국립국어원, http://stdweb2.korean.go.kr/search/List_dic.jsp

호 인증 및 제도의 명칭(ISO/IEC 27001, ISMS, PIMS, TCSEC, Information security certification 등)과 경제성분석 관련 키워드(Economic Effect, Effectiveness, cost benefit)들을 조합하여 전수조사 하였다. 추가로 보고서의 경우에는 구글을 이용하여 검색하였다.

본 연구는 정보보호 인증 및 제도에 대한 경제성 관련 연구를 개괄적으로 파악하는데 중점을 두어, 개별 논문을 분석단위로 사용하였다. 또한 세부적으로는 주제 및 방법론으로 분류하여 연구 현황과 한계점 및 향후 연구방향을 제시하고자 한다.

키워드를 통해 총 30개의 논문 및 보고서가 검색되었으며 이 중 논문은 총 25개로 국내 18개 및 국외 7개이며 보고서는 총 5개로 국내 3개, 국외 2개를 찾을 수 있었다. 그러나 국외 보고서중 1개는 내용면에서 본 연구와 관련이 없다고 판단되어 제외시키고 29개의 연구를 분석하였다.

3.3 연구방법

본 연구는 총 29개의 연구를 주제 중심으로 분류해 보고자 하였으며, 이를 위해 개별 연구들의 키워드를 사용하였다. 1차적으로는 키워드 분류를 위해 논문에서 사용된 전체 키워드(중복 허용, 110개; 중복/유사 단어 통합 및 주제와 무관한 키워드 제외, 45개)를 나열하여 비슷한 항목으로 그룹화하여 총 4개의 대분류(인증 및 제도, 경제성, 표준(화), 기타)로 나눌 수 있었으며, 3명의 연구자가 개별적으로 각 논문의 키워드를 바탕으로 대분류에 따라 연구를 정리하였다. 키워드가 제시되지 않은 논문이나 보고서의 경우에는 제목 및 요약을 활용해 키워드를 도출하여 이용하였다. 모든 연구의 분류 결과에 대해 3명의 연구자의 의견이 일치 할 때 까지 반복적으로 검토하여 분류를 명확히 하였다.

Table 1.의 키워드 분류표에 따라, 각 논문의 키워드에 보안 관련 인증 및 제도와 기타 키워드만 있는 경우에는 정보보호 인증 및 제도에 대한 연구, 보안 관련 인증과 경제성 키워드 및 기타 키워드가 있는 경우에는 정보보호 인증의 경제적 효과에 관한 연구, 보안 관련 제도와 경제성 키워드 및 기타 키워드가 있는 경우에는 정보보호 제도의 경제적 효과에 대한 연구, 표준화 및 경제성 키워드를 가진 논문은 표준화의 경제성에 관한 논문으로 분류를 하였고, 기타 키워드만 제시된 논문 및 보고서 7개는 연구자들이 제목, 본론, 결론, 서론, 내용 순으로 검토를 한 후 분류를 실시하였다.

Table 2.는 키워드분석을 통한 주제별 분류 결과로서 정보보호 인증 및 제도에 대한 논문 및 보고서

Table 1. Classification of Keywords

Classification(n)	Keyword
Security Certification (5)	Common criteria, ISMS, Certification standards, Accreditation, ISO/IEC 27001
Security Systems (3)	Personal Information Protection system, ISCS(Information Security Check Service), Advanced Diagnosis for Information Security
Economics (15)	Performance measures, Economic (analysis), Ripple Effect, Information Security investment, Effect Analysis, Certification Effectiveness, Performance Analysis, Security Economics, Efficiency, Economic Effects, Effectiveness, Business Performance, ISMS Certification Economic effect, Standards Economic Effect
Standard(1)	Standardization
Etc. (21)	Information Security, Assessment, TOE, Outcomes, Improvement of Certification Program, Obstacle Factors, Protection Profile, Guideline, Information Security Industry, Industrial Technology, Technique Security, Security Consciousness, Security Incidents, Certification Scheme, Certification System, Analysis of Industry, Insider Threats, Knapsack Problem, Financial Organization, Systems Evaluation and Process Certification, Methodology

* 상기 표에 제시된 키워드들의 경우 전체 100개의 키워드 중 ISMS 및 ISMS Standard등은 ISMS로 통합하는 등의 중복/유사단어 통합과정을 가졌으며, 키워드로 제시된 분석방법은 Methodology로 통합하였음

Table 2. Classification Standard of Research Theme

Theme	Domestic		Foreign	
	Paper	White paper	Study	White paper
Study on Security Certification & Systems	6	1	2	-
	[5],[6] [7],[8] [15],[7]	[26],	[9],[10]	-
Study on Economic Effect of Security Certification & Systems	8	2	5	1
	[12],[13] [14],[16] [22],[23] [24],[25]	[28],[29]	[17],[18] [19],[20] [21]	[27]
Study on Economic Effect of IT Stand-ardization	4	-	-	-
	[30],[31] [32],[33]	-	-	-
Total	18	3	7	1

는 국내 7개, 국외 2개가 있었으며, 정보보호 인증 및 제도의 경제적 효과에 관한 연구로는 국내 10개, 국외 6개로 분류 되었다. IT관련 표준(화)의 경제적 효과에 대한 연구로는 국내 4개가 있는 것으로 파악되었다. 이 중 본 연구의 중심이 되는 보안인증 경제성에 대한 연구의 개수는 4개이지만, 주된 연구자는 김인관, 장상수 등 2명으로 축약 될 수 있다. 또한 4편의 연구 중 1건은 학술지이기 때문에 국내에서 보안인증 경제성에 대한 연구는 매우 희박하다는 것을 알 수 있다.

방법론의 분류기준으로는 기존 연구에서는 보안관련 인증 제도의 경제적 분석 연구동향을 방법론으로 분류한 사례가 없기 때문에, 일반적인 사회과학 연구방법인 정량적 연구와 정성적 연구로 나누었으며[34], 더불어 사회과학 분야에서 우수한 저작 활동의 대다수가 심층적인 사례분석을 바탕으로 하고 있다는 점[35]을 바탕으로 연구방법론을 정성적 연구, 정량적 연구, 사례연구 등 총 3가지로 Table 3.에서 분류하였다.

정량적 연구는 통계적으로 분석 가능한 수치자료를 산출하므로, 측정기술이나 표집방법, 통계조사 등을 사용하며, 정성적 연구는 수치로 된 자료 대신 말

Table 3. Classification Standard of Methodology

Methodology	Qualitative Analysis
	Quantitative Analysis
	Case Study

(words)의 형태로 된 자료를 사용하는 연구로 비통계적 기법으로 연구결과를 도출하고 해석하는 것이다. 사례연구는 선행 연구결과나 기초이론의 영향을 받지 않고 새로운 통찰을 얻기 위해 서론이나 연구문제 설정에서 선행연구 결과나 기초이론을 취급하지 않는 것을 말한다.

IV. 연구동향 분석결과

4.1 주제

Fig. 1은 4개의 기준으로 분류하여 빈도 분석한 결과, 정보보호 인증의 경제적 효과에 대한 연구(34%)가 가장 많았으며, 정보보호 인증 및 제도에 대한 연구(31%), 정보보호 관련 제도의 경제적 효과에 대한 연구(21%), 표준의 경제적 효과에 대한 연구(14%) 순으로 결과가 나타났다. 이는 정보보호 인증 및 제도에 대한 관심이 점차적으로 증가하고 있음을 보여준다. 최근 들어 정보보호 관련 침해사고 피해로 인해 정보보호 인증 및 제도의 도입이 활성화되고 더 나아가 의무화 되면서 이에 대한 투자효과에도 관심이 증가한 것으로 보인다. 이에 따라 경쟁우위의 핵심요소로 등장한 정보보호 인증 및 제도에 대한 연구도 활발해지고 있음을 알 수 있다. 그러나 국내·외 모두 발표된 연구결과의 전체 수가 그리 많지 않은 실정이다. 특히, 정보보호 분야의 연구가 주로

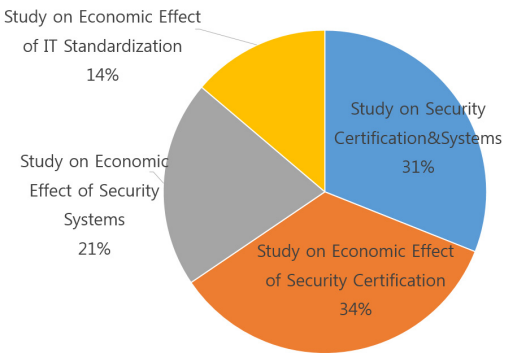

Fig. 1. Frequency of Research Theme

기술적인 대안의 발굴 또는 개선에 집중되고, 정보보호 인증 및 제도 효과분석에 대한 연구에 중요성을 높게 인식하고 있지 못하기 때문인 것으로 파악된다. 따라서 국내 학계 및 산업계를 중심으로 정보보호 인증 및 제도의 효과분석과 그에 대한 연구에 관심을 갖고 관련 연구 및 활동들이 활성화되도록 하는 노력이 요구된다.

Fig. 2는 국내 문헌만 대상으로 빈도 분석을 실시한 결과로써 정보보호 인증 및 제도에 대한 연구(33%)가 정보보호 관련 제도의 경제적 효과에 대한 연구(29%)보다 많이 빈도분석 되었으며 정보보호 인증의 경제적 효과에 대한 연구(19%)와 표준의 경제적 효과에 대한 연구(19%)는 동일한 빈도분석이 되었다. 국외 문헌만 대상으로 빈도 분석을 실시한 결과 정보보호 인증의 경제적 효과에 대한 연구(75%)와 정보보호 인증 및 제도에 대한 연구(25%)가 주류를 이루고 있었다.

국내문헌 빈도수와 국외문헌 빈도수 분석결과 국내의 경우 정보보호 인증 및 제도에 대한 연구가 활발히 진행되고 있으나, 국외 문헌의 경우 정보보호 인증의 경제적 효과에 대한 연구가 주된 연구라 할 수 있으며, 국내의 경우 정보보호 관련 제도의 경제적 효과에 대한 연구도 정보보호 인증 및 제도에 대한 연구만큼 이루어지고 있다. 국내에서는 상대적으로 정보보호 인증의 경제적 효과에 대한 연구에 대한 빈도수 분석이 적게 나타났다.

Fig. 3의 연도에 따른 주제별 변화를 살펴보면 정보보호 인증 및 제도에 대한 연구의 경우 2000~2003년 이후로 하락하는 경향을 보였으며,

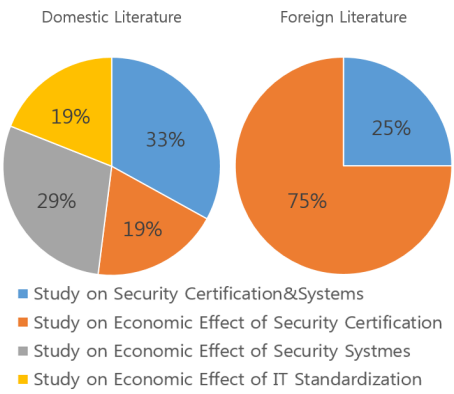

Fig. 2. Frequency of Research Theme Domestic and Foreign

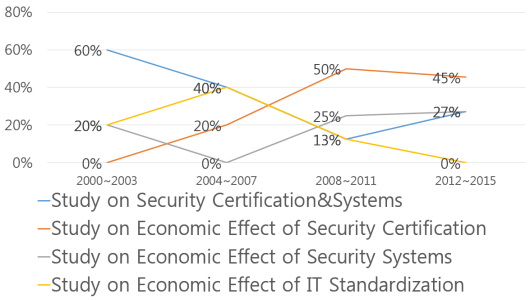

Fig. 3. Research Theme Trend

그와 반대로 정보보호 인증의 경제적 효과에 대한 연구의 경우 2000~2003년 이후로 점차 증가하는 추세를 보여주고 있었다. 2008~2011년 가장 많은 연구가 진행되었는데, 이는 ISMS 인증 도입이 2002년부터 시행 및 점차 확산 되었으며, 2008년 이후 기업의 개인정보유출에 관한 사고가 증가함에 따라 정보보호 인증의 경제적 효과에 대한 연구가 증가한 것으로 파악된다.

Table 4.에서는 연도별 논문 빈도분석도 실시하였는데, 분석대상 논문 수(29개) 대비 검색연도가(15개)가 많아 전반적인 연구동향 파악을 수월히 하고자 2000년부터 2015년까지 4년 단위로 그룹지어

Tabel 4. Frequency Table of Research Theme

	2000~2003	2004~2007	2008~2011	2012~2015	Total
Study on Security Certification &Systems	3 60%	2 40%	1 13%	3 27%	9 32%
Study on Economic Effect of Security Certification	0 0%	1 20%	4 50%	5 45%	10 34%
Study on Economic Effect of Security Systems	1 20%	0 0%	2 25%	3 27%	6 20%
Study on Economic Effect of IT Stand-ardization	1 27%	2 45%	1 27%	0 0%	4 14%
Total	5 100%	5 100%	8 100%	11 100%	29 100%

연구동향을 파악하였다.

각 세부 주제별 연구에 대한 전반적인 동향은 다음과 같다.

4.1.1 정보보호 인증 및 제도에 대한 연구

본 주제를 통해서는 정보보호 인증 및 제도에 대한 연구들의 전반적인 동향을 살펴 볼 수 있었다. 국내·외의 정보보호 인증 및 제도에 관한 연구는 주로 정보보호 인증 도입 시의 장애요인 분석, 기존의 정보보호 인증 및 제도에 대한 분석, 정보보호 인증제도의 발전방향 및 개선방안 연구, 평가지표 개발 등으로 나눌 수 있었다. 정보보호 인증 및 제도에 대한 연구를 분석한 결과 정보보호 인증 및 제도 등 의 연구는 주로 최근 연구들로 구성되어 있으며, 정보보호 관리체계 인증 및 제도의 향후 발전방향에 대한 연구가 주를 이루었다.

4.1.2 정보보호 관련 인증의 경제적 효과에 대한 연구

정보보호 관련 인증의 경제적 효과에 대한 연구는 전반적으로 국내·외 인증의 경제적 효과에 관한 연구 현황이 많지 않은 것으로 파악되며, 인증 도입 요인, 도입 후 영향을 주는 요인에 대한 연구가 많고, 도입효과에 대한 연구는 많지 않은 것으로 파악된다. 정보보호 인증 도입의 효과분석에 대한 연구들은 관련 인증 도입으로 인해 기업에 긍정적인 영향을 미친다는 연구가 대다수였지만, 실제 경제적·재무적으로 정량적인 수치를 제시하는 연구보다는 조직의 성과향상과 같은 정성적인 연구가 주를 이르고 있으며, 세부적인 효과 측정을 위한 지표에 대한 연구는 부족하다. 또한 측정방법론이 매우 간단하거나 제한적이고 정교하지 않다. 또한 특정 산업만의 인증에 대한 효과를 분석하는 등 많은 한계점을 보여주고 있다. 게다가 이 같은 인증도입의 효과를 단순 설문조사와 문헌조사만을 통해 분석하는 것은 실효성이 없다고 주장하는 연구도 있다. 이 같은 이유는 여러 문헌에서 언급하듯이 정보보호 투자의 특성과 마찬가지로 정보보호 관련 인증 도입은 기업의 전 영역에 걸쳐 영향을 미치기 때문에 인증 도입으로 인한 정확한 효과를 측정하기는 어려우며, 기업이 정보보호 사고를 숨기는 경향이 있기 때문에 개인 연구자가 인증 및 제도의 실제적인 성과 측정을 위한 자료를 직접 확보하는 데에는 한계가 있는 것으로 파악된다. 그러나, 기업의 ISMS 도입 활성화를 위해서는 기업이나 조직차원에서 정보보호 관련 인증 도입에 대한 투자 의사결정을 위해 인증 도입의 경제적 효과를 수치화한 분석이 필요하다. 이를 위해 ISMS 등 정보보호 관련 인증 도입에 대한 경제적 효과 분석에 대한 연구의 필요성이 중요하게 요구된다.

4.1.3 정보보호 관련 제도의 경제적 효과에 대한 연구

정보보호와 관련된 다양한 제도들이 있으나, 사전진단제도, 정보보안 공시제도, 안전진단 등과 같은 일부 제도들에 대한 경제적 효과에 관한 연구가 진행되고 있었다. 대부분의 연구들이 정보보호 관련 제도의 경제적 효과에 대하여 산술식을 통해 정량적으로 경제적 효과를 표현하고자 하였으나, 직접적인 수치를 도출한 연구는 부족하였다. 따라서 정보보호 인증을 포함한 관련 제도의 활성화를 위해서는 정보보호 기술측면 뿐만 아니라 정보보호 제도 측면의 여러 가지 다양한 연구가 필요하다. 정보보호 제도의 도입효과 분석과 함께 제도 도입을 위한 주요 요인 및 지표 등에 대한 연구가 활성화 되어야 할 것이다.

4.1.4 표준(화)의 경제적 효과에 대한 연구

다양한 표준이 존재하고 있으나, 표준에 대한 경제적 효과 연구 자체가 거의 존재하지 않았다. 표준의 경제적 효과에 대한 연구들은 경제적 효과에 대하여 산술식을 통해 정량적으로 표현하고자 하였으나, 직접적인 수치를 도출한 연구는 부족하였다. 따라서 보안인증 표준화 연구 이전에 보안인증의 도입효과 및 경제적 효과 등에 대한 연구가 선행되어 관련 분야의 표준화로 연계가 수행되는 것이 필요하다. 보안인증의 경제적 효과가 분석되어 연구 결과가 확산되고 보안인증이 활성화되면 보안인증의 표준화에 대한 선도적인 기반이 확보될 것이다.

4.2 방법론

과학적 연구조사는 목적에 따라 크게 문제의 규명을 위한 탐색조사(exploratory research), 현상의 기술과 설명을 위한 기술조사(descriptive research), 인과관계의 규명을 위한 인과조사(causal research)의 세 가지 범주로 나누어 볼 수 있다. 본 연구에서는 이 세 가지 범주의 관점에서

기존에 발표된 논문들을 정리하였다.

보안인증의 경제적 효과 연구의 다양성을 확인하기 위해 조사 대상 논문들을 주제별로 분류한 결과, 많은 연구에서 인증 및 제도의 경제적 효과를 정성적 방법론이나 단순 설문방법을 통해 도출하고 있는 것으로 나타났으며, 정량적·재무적 지표로 분석한 연구는 내·외부 공격과 관련된 위험의 정도나 기대손실, 또는 이를 방어하기 위한 정보보호 분야의 지출이나 관련 투자규모 및 수준을 측정할 수 있는 가치평가 분석방법을 개발한 정도이다. 또한 효과성에 대한 모델링을 통해 정성적 효과를 규명하고 있는 것으로 나타났다. 더욱이, 경제적 효과를 분석한 일부 연구에서는 특정분야인 제조 기업을 중심으로 케이스 스터디로 분석하였기 때문에 아직까지 서비스업이나 모든 기업에 적용 가능하도록 일반화하기는 한계가 있으며, 일반화된 방법론이 정립되기까지는 더 많은 연구가 필요할 것으로 보인다. 또한 BSC 등 다양한 방법론을 통해 정량적· 정성적 지표들을 활용한 투자효과 분석에 대한 연구들도 존재하지만 가시적이고 수치적인 경제적 효과를 분석하기 위한 모델링에 대한 연구는 미흡하다. 정보보호 관련 인증 및 제도의 경제적 효과분석에 대한 연구결과들은 제도도입 전·후 기업 및 조직의 재무상태 변화를 비교하거나, 제도도입으로 인한 침해사고 발생 등 사례분석을 통해 사고피해액의 크기를 비교하고 해당 제도도입을 통한 성과제표를 개발하여 성과분석 모델 제시를 통해 피해액을 산정하고 있다. Fig. 4의 3개의 기준으로 분류하여 빈도 분석한 결과, 정성적 연구(52%)가 가장 많으며, 케이스 스터디(28%), 정량적 연구(17%) 순으로 결과가 나타났으며, 정량적 분석방법과 정성적 분석방법을 둘 다 이용한 연구도 존재하였다.

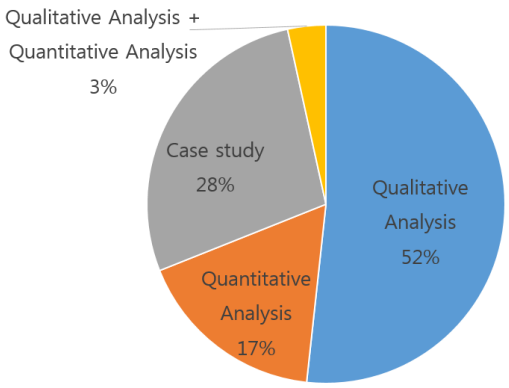

Fig. 4. Frequency of Research Methodology

Fig. 5와 Table. 5에서는 방법론별로 연도에 따른 변화를 살펴보았다. 정성적 연구가 전체적으로 많은 비중을 차지하고 있다. 케이스 스터디는 2011년 이후 하락하였지만 정량적 연구는 증가하는 추세를 보여주고 있다.

Fig. 6에서는 2011년 이전의 경우 케이스 스터디 방법론을 이용한 논문이 40%정도 나타났는데, 케이스 스터디를 정량적 방법과 정성적 방법으로 나눈 결과는 정성적 방법(13%)이 정량적 방법(87%)에 비해 많은 부분을 차지하고 있었다. 이러한 결과로 볼 때 연구에서 케이스 스터디 방법론을 이용함으로 정량적인 수치를 제시하고자 한 것을 유추해 볼 수 있다. 하지만 이러한 케이스 스터디는 특정 분야에 한정하여 정량적 수치를 제시하기 때문에 보편적으로 적용하는데 어려움이 존재한다.

Fig. 7에서는 정보보호 인증의 경제적 효과의 연구 방법론을 분류한 결과 정성적 연구(50%), 정량적 연구(30%), 케이스 스터디(20%) 순으로 나타났

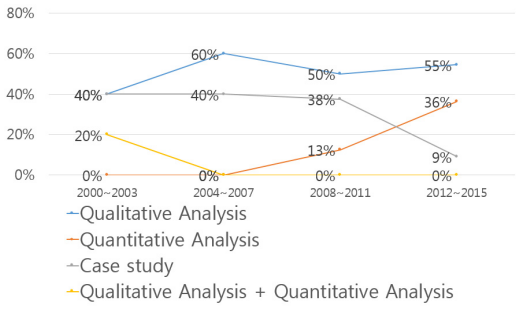

Fig. 5. Research Methodology Trends

Table 6. Frequency Table of Research methodology

	2000~2003	2004~2007	2008~2011	2012~2015	Total
Qualitative Analysis	2 40%	3 60%	4 50%	6 55%	15 52%
Quantitative Analysis	0 0%	0 0%	1 13%	4 36%	5 17%
Case Study	2 40%	2 40%	3 38%	1 9%	8 28%
Qualitative Analysis + Quantitative Analysis	1 20%	0 20%	0 20%	0 20%	1 3%
Total	5 100%	4 100%	9 100%	12 100%	30 100%

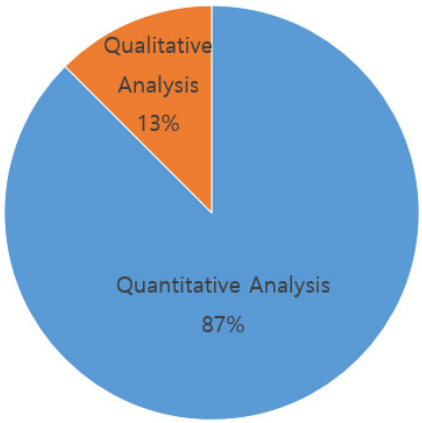

Fig. 6. Frequency of Research Case study Methodology

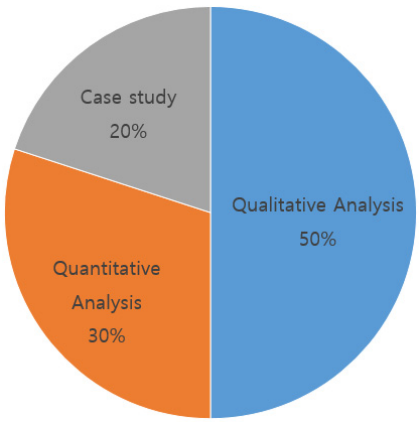

Fig. 7. Frequency of Research Study on Economic Effect of Security certification

다. 정보보호 인증의 경제적 효과에 대한 연구는 경제적 효과를 분석하는 연구임에도 불구하고 정성적 연구가 절반을 차지하고 있었으며, 케이스 스터디의 경우 보편적으로 적용하기에는 어려움이 있으며, 정량적인 연구의 경우도 특정 분야만 적용이 가능한 한계점이 있었다.

V. 결 론

최근 많은 보안관련 사고가 발생하였고, 앞으로는 모든 사물들이 인터넷으로 연결 되는 초 연결시대가 도래하면서 보안사고의 파급효과는 더욱 커질 전망이다. 이에 정부 주도로 다양한 보안관련 인증 및 공시제도가 시행되고 있다. 그러나, 공시제도와 인증제도 도입을 위해 조직들은 적정수준의 투자를 고려하고 있지만 정보보호관리체계 도입에 대한 경제적 효과나 투자의 범위 및 대상에 대한 의사결정 기준이 명확하게 제시되지 않고 있어 조직의 보안 관련 인증 획득의 속도가 더딘 편이다. 따라서 본 연구는 정보보호 분야의 각종 인증제도 효과를 분석하기 위한 국내외 연구동향에 대해 조사해보고, 연구된 논문들의 연구주제와 연구방법을 분석하고자 하였다.

연구방법으로는 구글스칼라, RISS, NDSL 등의 문헌검색 DB에서 보안관련 인증 및 제도와 경제성 키워드를 조합하여 문헌검색을 하였으며, 총 국내 21개, 국외 8개의 관련 문헌을 도출하였다. 본 논문들의 분류는 보안 인증 및 제도에 대한 연구, 보안 인증 및 제도의 경제적 효과에 대한 연구, 표준의 경제적 효과에 대한 연구 등 3가지로 분류 할 수 있었으며, 연구 방법론으로는 정확한 수치를 제시하는 정량적인 연구보다는 사례조사 등의 경험적 연구와, 기존 제도의 문제점 및 개선사항을 도출하는 연구 및 정책의제에 관련된 연구가 대부분을 차지하였다. 따라서 앞으로는 보안관련 인증 및 제도 도입 의사결정에 도움을 주기 위해 경제적 측면에서의 정량적인 효과의 연구가 이루어져야 할 것이다. 이를 통해서 기업들이 ISMS와 같은 보안 인증 제도를 획득하는 가이드라인을 제시 해 줄 수 있을 것이며, 이는 곧 국가보안성을 향상 시킬 수 있는 계기가 될 것이다.

본 연구는 보안 관련분야 연구 활성화 및 정보보호관리체계 도입을 위한 기초자료 분석에 활용될 수 있다는 의의를 지니고 있으며, 보안인증과 관련된 경제적 효과에 대한 정량적 연구의 필요성을 제시하고 있다. 그러나, 한계점으로는 기존 문헌의 수가 워낙 적기 때문에 정확한 연구 추세 및 방법론을 파악하지 못했다는 점이 있다.

References

[1] http://www.law.go.kr/admRulInfoP.do?admRulSeq=2100000021445&chrClsCd=010201(Korea Ministry of Government Legislation, 2015.06.24)
[2] Financial Services Commission, "The Comprehensive Financial Computerized Security Measures for Improving the Safety of Electronic Banking," 2013
[3] The bank of Korea, "Implementation

Status of Financial Information in 2014", 2015
〔4〕 http://isms.kisa.or.kr/kor/issue/issue01.jsp?certType=ISMS (Korea Internet & Security Agency, 2015.12.21.)
〔5〕 Yujin Kim, JungDuk Kim, DoIl Kim, "A Study on the Development of an Evaluation Model for Information Security Processes," Journal of Industry and Management, 10(1), pp. 187-207, Dec. 2001.
〔6〕 YoungRan Hong, DongSoo Kim, "Analysis of the Effects of Common Criteria Certification on the Information Security Solutions, " Society for e-Business Studies, 17(4), pp. 57-68, Nov. 2012
〔7〕 KyeongTae Park, SeHun Kim, "An Empirical Study on the Obstacle Factors of ISMS Certification Using Exploratory Factor Analysis," Journal of The Korea Institute of Information Security and Cryptology, 24(5), pp. 951-959, Oct. 2014
〔8〕 HyunSun Kang, "An Analysis of Information Security Management System and Certification Standard for Information Security," Journal of Security Engineering, 11(6), pp. 455-468, Dec. 2014
〔9〕 Eloff, M. M. & Von Solms, S. H., "Information security management: an approach to combine process certification and product evaluation." Computers & Security, 19(8), pp. 698-709, Dec. 2000
〔10〕 Huang, S. M., Lee, C. L., & Kao, A. C, "Balancing performance measures for information security management: A balanced scorecard framework," Industrial Management & Data Systems, 106(2), pp. 242-255, Jun. 2006
〔11〕 SungWook Park, JongMin Yoon, "A Study on Economic Contribution of Development of Information Security Industry Investment by the Industry Association Analysis" Korea Technology Innovation Society conference, 2006(5), pp. 19-29, May, 2006
〔12〕 InKwan Kim, Seunghyun Lee, Jaemin Park. "An Study on the Effect of Security awareness about Industrial Technology and Information security Investment to get ISMS Certification," Korea Technology Innovation Society conference, pp. 101-115, Jun. 2011
〔13〕 InKwan Kim, JaeMin Park, JoogYang Jeon, "An Study on the Effects of ISMS Certification and the Performance of Small and Medium Enterprises," Journal of Digital Convergence, 11(1), pp. 47-60, Jan. 2013
〔14〕 SangSoo Jang, "Estimating The Economic Value of Information Security Management System(ISMS) Certification by CVM," Journal of the Korea Academia-Industrial cooperation Society, 15(9), pp. 5783-5789, Sep. 2014
〔15〕 KyeongTae Park, SeHun Kim, "An Empirical Study on Expectation Factors and Certification Intention of ISMS," Journal of The Korea Institute of Information Security and Cryptology, 25(2), pp. 375-381, Apr. 2015
〔16〕 SangSoo Jang, SangChoon Kim, "An Empirical Study on the Effects of Business Performance by Information Security Management System(ISMS)," Convergence Security Journal, 15(3), pp. 107-114, Sep. 2015
〔17〕 Humphreys, E. "Information security management standards: Compliance, governance and risk management," Information Security Technical Report 13(4), pp. 247-255, Nov. 2008
〔18〕 Anderson, R., & Fuloria, S. "Certification and evaluation: A security economics perspective," IEEE Emerging Technologies & Factory Automation, pp. 1-7, Sep. 2009

[19] Boehmer, W, "Cost-benefit trade-off analysis of an ISMS based on ISO 27001." Availability, Reliability and Security, pp. 392-399, Mar. 2009
[20] CheolSoon Park, SangSoo Jang, and YongTae Park, "A study of effect of Information Security Management System [ISMS] certification on organization performance." International Journal of Computer Science and Network Security, 10(3), pp. 10-21, Dec. 2010
[21] Chang, H. "Is ISMS for financial organizations effective on their business?." Mathematical and Computer Modelling, 58(1), pp. 79-84, Jul. 2013
[22] SnagSoo Jang, SeungHo Shin, BongHam Noh, "A study of th ISCS(Information Security Chech Service) on performance measurement model and analysis method," Journal of The Korea Institute of Information Security and Cryptology, 20(6), pp. 127-146, Dec. 2010
[23] HeeKyung Kong, TaeSung Kim, "Economic Effects of Advance Diagnosis for Information Security: A Case Study," Journal of The Korea Institute of Information Security and Cryptology, 20(6), pp. 157-169, Dec. 2010
[24] DongYoung Yoo, DongNam Seo, Huy Kang Kim, "A Study for Effectiveness of Preliminary Security Assessment on Online Game Service Domain," Journal of the Korea Society of IT services, 10(2), pp. 293-308, Jun. 2011
[25] HyoJung Jun, TaeSung Kim, "A Feasibility Study on Introduction of Information Security Disclosure," Journal of The Korea Institute of Information Security and Cryptology, 22(6), pp. 1393-1405, Dec. 2012
[26] Korea Internet & security Agency "A Study on the Improvement of Certification Program for Information Security Management System," , 2003
[27] Wright, S, "Measuring the Effectiveness of Security using ISO 27001," White paper, 2006
[28] Korea Information Society Development Institute, "Analysis of the Economic and Social Impact about implementing Personal Information Protection Accreditation", 2001
[29] Korea Internet & Security Agency, "A Study on the Analysis of the Economic Effects of the Pre-Check Institution for Information Security and Its Activation Plans", 2012
[30] ShinWon Kang, "An Analysis of IT Standardization Effects", The Journal of Korean Institute of Communications and Information Sciences, 2006(7), pp. 1818-1821, Jul. 2006.
[31] YoungTae Im, KangDae Lee, "A Basic study on searching methods to analyze the economic effect of logistics standardization," Korean Society of Transportation Conference, 2006(3), pp. 95-104, 2006
[32] SukBong Choi, TaeSoo Chung, SeokHong Jo, "An analysis of the Economic Effects of Standardization in BcN Industries," The Journal of Internet Electronic Commerce Research, 10(2), pp. 153-170, Jun. 2010.
[33] BumFwan Kim, YeonSang Cho, JongBong Park. "Analysis of Economic Effect of Standardization - Theoretical Approaches and Case Study about ICT Sector," The korea Society for Innovation Management&Economics conference, pp. 91-116, Feb. 2002
[34] Ragin, Charles C. "The comparative method: Moving beyond qualitative and quantitative strategies," Univ of California Press, Oakland, California, 2014.
[35] YoungCheol Lee, "Is A Case Study Method

A Second Citizen in the Social Sciences Research?" Korean Public Administration Review, 40(1), pp. 71-90, Mar. 2006

〔36〕 HanKyung economic dictionary of The Korea Economic Daily, http://dic.hankyung.com/, 2015.06.27.

〔37〕 http://www.motie.go.kr/motie/in/ay/instruct/directive/bbs/bbsView.do?bbs_seq_n=61718&bbs_cd_n=28(final check, 2016.02.27)

〔38〕 Standard Korean Dictionary of The National Institute of The Korean Language, http://stdweb2.korean.go.kr/search/List_dic.jsp

〈저자소개〉

공 희 경 (Hee-Kyung Kong) 정회원
2001년 8월: 충북대학교 정보산업과 석사 졸업
2008년 8월: 충북대학교 경영학 박사
2009년 3월~2012년 4월: 한국전자통신연구원 기술전략연구본부 선임연구원
2012년 9월~현재: 충북대학교 전자정보대학 정보통신공학과 초빙부교수
〈관심분야〉 정보보호 정책, 보안경제성, 정보통신경영

전 효 정 (Hyo-Jung Jun) 정회원
2003년 8월: 충북대학교 경영정보학과 석사 졸업
2003년 9월~2007년 5월: 한국전자통신연구원 기획본부 기술원
2014년 2월: 충북대학교 경영정보학과 박사 졸업
2014년 3월~현재: 충북대학교 정보보호경영학과 박사후연구원
〈관심분야〉 정보보호 인력정책, 보안경제성

이 송 하 (Song-ha Lee) 학생회원
2015년 2월: 충북대학교 경영정보학과 졸업
2016년 3월~현재: 충북대학교 경영정보학과 석사과정
〈관심분야〉 정보보호 교육 및 인력, 정보보호 정책, 정보보호 경제성

강 민 성 (Min-Seong Kang) 학생회원
2015년 2월: 충북대학교 경영정보학과 졸업
2016년 3월~현재: 충북대학교 경영정보학과 석사과정
〈관심분야〉 정보보호, 정보보호 경제성, 정보보호 정책, 기술경영

김 태 성 (Tae-Sung Kim) 종신회원
1997년 2월: KAIST 산업경영학과 박사
1997년 2월~2000년 8월: 한국전자통신연구원 정보통신기술경영연구소 선임연구원
2005년 1월~2006년 2월: Univ. of North Carolina at Charlotte 방문교수
2010년 7월~2012년 7월: Arizona State University 방문연구원
2000년 9월~현재: 충북대학교 경영정보학과 교수 및 학과장, 보안컨설팅연계전공 주임교수, 일반대학원 정보보호경영전공 주임교수, 국가정보원 보안관리실태평가 자문 및 평가위원, 금융보안원 금융보안컴플라이언스 자문위원, 전자정부 민관협력포럼 자문위원
〈관심분야〉 정보통신과 정보보호 분야의 경영 및 정책 의사결정