# 정보자산보호 성과가 조직성과에 미치는 영향에 관한 연구: 관리활동과 통제활동을 중심으로

## A Study on the Effects of the Information Asset Protection Performance on the Organization Performance: Management Activity and Control Activity

김 경 규* · 신 호 경** · 박 성 식*** · 김 범 수****
Kyung-Kyu Kim · Ho-Kyoung Shin · Sung-Sik Park · Beom-Soo Kim

차 례



초 록

최근 기업에서는 정보자산을 여러 가지 통제 및 관리 수단을 통해 보호활동을 하고 있다. 그러나 보호수준을 높게 요구할수록 업무 수행의 불편함으로 단기적인 효율성 및 생산성이 감소하게 되었다. 이와 함께 조직의 정보보호를 위한 투자가 지속적으로 증가함에도 불구하고 정보보호 성과측정을 위한 체계적인 방법이 제시되지 않아 정보보호 투자 의사결정 및 정보보호 개선 방향 도출이 어려운 것이 현실이다. 본 연구에서는 기업의 정보자산의 보호에 대한 개념을 정립하고자 하였다. 이를 위해 문헌연구를 바탕으로 정보자산보호를 위한 활동의 유형을 관리활동과 통제활동으로 분류하여 이들이 정보자산보호 활동의 성과와 조직 성과에 미치는 영향을 연구하였다. 본 연구를 위해 이론연구와 더불어 실증적 연구분석을 위해 설문조사를 실시하였으며, 수집된 자료는 PLS(Partial Least Square)를 이용하여 측정모형 및 가설검증을 실시하였다. 통계분석 결과, 정보자산보호 관리활동은 정보자산보호 성과에 긍정적 영향을 미치며, 정보자산보호 통제활동은 정보자산보호 성과에 유의한 영향을 미치지 않는 것으로 나타났다. 또한 정보자산보호 성과는 조직 성과에 대해 긍정적인 영향을 미치는 것으로 나타났다. 이 외에 본 연구결과에 대한 의의 및 한계점을 논의하였으며, 향후 연구에 대한 시사점도 언급하였다.

* 연세대학교 정보대학원 교수
(Professor, Graduate School of Information, Yonsei University, kyu.kim@yonsei.ac.kr)
** 연세대학교 정보대학원 연구교수(교신저자)
(Research Professor, Graduate School of Information, Yonsei University, rosashin1@gmail.com)
*** KT SMB 고객부문 차장
(Manager, SMB Customer Center, KT, verve@KT.com)
**** 연세대학교 정보대학원 교수
(Professor, Graduate School of Information, Yonsei University, beomsookim@gmail.com)
• 논문접수일자: 2009년 8월 4일
• 최종심사일자: 2009년 9월 8일
• 게재확정일자: 2009년 9월 18일

**키 워 드**

정보자산보호, 정보자산보호 관리활동, 정보자산보호 통제활동, 정보자산보호 성과, 조직 성과

ABSTRACT

Recently, enterprises are protecting information assets with the various means of control and management. Nevertheless, they are confronted with the dilemma which the higher securitylevel they request, the lesser efficiency and productivity in short terms they acquire by the inconvenience of business process. In addition, in spite of the steady increase of organization's investment on information protection, the systematic way for the performance measurement of information protection has not been suggested, so that in reality, it is difficult to make the decision to invest on information-protection and elicit the direction to improve it. For this reason, this study intended to establish the concept of the protection and security of information assets of enterprises and to categorize the type of activities to protect information assets into management activity and control activity, and analyze the effects of management activity and control activity for information asset protection on the performance of information asset protection activity and organization. For this research, questionnaire survey was conducted with literature study and the PLS(Partial Least Square) was used to analyze the measurement model and hypotheses testing. The PLS analysis results indicate that management activity for information asset protection affects information asset protection performance. Further, organizational performance is influenced by information asset protection performance. Practical implications of these findings and future research implications are also discussed.

KEYWORDS

Information Asset Protection, Information Asset Protection Management Activity, Information Asset Protection Control Activity, Information Asset Protection Performance, Organizational Performance

## 1. 서 론

현대사회에서 기업환경은 정보화의 가속화, 인터넷의 보편적 보급, 유비쿼터스 환경실현 등 IT기술의 눈부신 발달로 환경이 급변되었고, 정보는 비즈니스 성공의 핵심으로써 중요성이 증대되고 있다. 또한 최근의 기업 경영의 패러다임이 되고 있는 지식경영의 중점사항은 기업이 보유한 모든 가용한 정보를 공유해 업무처리의 효율성을 높이고, 시장 대응력을 높여 기업경쟁력을 제고시키는 것이다. 하지만 날로 증가하는 수많은 정보를 제대로 보호하

고, 관리하기가 어려워지고 있으며, 인터넷이라는 공개된 범용의 거대 네트워크를 통한 상호접속이 보편화되고, 이를 통한 광범위한 정보자산의 공유로 말미암아 통제는 더욱 어려워지고 있다. 웜/바이러스의 창궐, 서비스거부 공격, 해킹 등의 외부에서의 침해공격이 일반화되며, 더욱 정교하고 집요해지고 있고, 이와 같은 고의적인 보안사고와 더불어 기업내부에서의 정보자원의 오용, 유출, 인적 실수와 같은 보안사고도 빈번하게 일어나고 있다(서승우 2008). 이에 대한 대응책으로 기업에서는 정보자산을 여러 가지 통제 및 관리 수단을 통해 보호활동을 하고 있으나, 보안수준을 높게 요구할수록 업무 수행의 불편함으로 단기적인 효율성 및 생산성이 감소하게 되는 어려움에 직면하고 있다. 그러므로 이러한 정보자산보호를 위해 기업에서는 우선적으로 보호해야 할 정보대상과 그 관리범위를 정의하고, 체계적이고 효율적인 정보보호관리 활동으로 적절한 균형을 맞춰야 할 필요가 있다.

한편 정보자산보호의 성과는 기회 비용적 성격이어서 정보자산보호가 잘 이루어지는 경우에는 손실이 발생하지 않고, 정보자산보호가 잘 이루어지지 않는 경우에만 손실이 발생하여 그 효과를 객관적으로 파악하는 데에는 한계가 있으므로 정보자산보호 성과를 금전적으로 측정하기에는 어려움이 있다(Smith 1995). 정보자산 성과 측정을 위해서는 정보자산보호에 대한 개념의 재정립 필요성이 제기되며, 기업이 정보자산보호에 대한 투자를 할 때는 문제를 해결하고, 침해 사고의 발생 가능성을 줄이는 정도에 만족할 것이 아니라 적극적 투자를 통해 결과적으로 더 큰 잠재적 성과를 창출해 낼 필요가 있다. 또한 정보자산보호 수요가 지속적으로 증가함에도 불구하고 정보보호 성과에 대한 연구가 부족한 실정이며 이로 인해 정보자산보호에 관한 의사결정 및 정보보호 개선 방향 도출에 어려움이 있어 이에 대한 연구 필요성이 제기되고 있다(홍기향 2003).

이에 본 연구에서는 정보자산의 보호에 대한 개념을 알아보고 정보자산보호를 위한 활동의 유형을 관리적 활동과 기술기반의 통제적 활동으로 분류하여 분석하며, 효과적인 정보자산보호활동 방안 마련을 위해 정보자산보호 성과와 조직 성과에 미치는 정보자산보호를 위한 관리활동과 통제활동의 영향을 연구하고자 한다. 본 연구목적을 위해서 문헌연구를 통한 정보자산보호의 개념 및 관련 연구와 정보자산보호 활동 등에 대하여 알아보고, 국내 기업을 대상으로 한 설문 조사를 통하여, 각 기업조직의 정보자산보호 관련 관리 및 통제 활동과 성과에 대한 자료를 수집하여 이를 실증적으로 분석하였다.

## 2. 이론적 배경 및 연구 가설

### 2.1 정보자산보호 활동

정보자산(Information Asset)이란 기업이

비즈니스 목표를 달성하도록 지원하기 위해 사용하는 정보시스템 및 프로그램, 그리고 그 정보시스템이 만들거나 소유하고 있는 데이터를 포괄하는 개념이며, 기업의 서비스, 이미지, 브랜드 등 조직에 가치 있는 모든 정보를 포함한다(이준택 2007). 정보자산은 정보가 들어 있는 모든 매체인 정보매체를 통해 분류될 수 있다. 정보매체는 사람, 시스템 및 문서 등과 같이 정보를 저장하고 유통 시키는 모든 미디어를 의미하며, 정보자산은 이러한 정보매체를 기준으로 분류되는데, 정보자산의 분류를 통해 해당 정보자산과 관련된 위협과 취약성을 식별하여 정보자산을 보호할 수 있는 근거 자료가 된다. 즉, 정보자산의 보호를 위해서는 먼저 해당 정보자산이 어떤 정보매체에 존재하는지 그 소재를 파악하여 정보자산의 유형 및 특징, 그리고 취약성 등을 인식함으로써 적절한 정보자산보호를 위한 대책을 수립한다.

이 연구에서 정보란 개인 또는 법인이 특정 목적을 위하여 광 또는 전자적 방식으로 처리하여 부호, 문자, 음성, 음향 및 영상 등으로 표현한 모든 종류의 자료 또는 지식을 말한다. 또한 정보보호는 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적 · 기술적 수단을 강구하는 것을 말한다. 또한 정보자산보호란 발생 가능한 모든 정보자산의 유출 및 다양한 위협으로부터 기업의 가치 있는 정보자산을 보호하며, 기업비밀 및 정보자산이 관계자 외 또는 타 경쟁기업에 공개 혹은 유출되지 않도록 하는 유형 무형의 모든 예방 조치이며 위험상황 발생 시 사업에 피해를 최소화하여 사업의 연속성을 유지하기 위한 것을 말한다. 구체적으로, 정보자산의 주체가 의도하지 않은 정보의 누출, 변경, 파괴를 방지하는 것을 말하며, 정보자산의 생성, 처리, 저장, 전송, 출력 등 정보순환의 모든 과정에서 정보의 기밀성, 무결성, 가용성, 추적성, 인증성, 신뢰성을 확보하기 위한 제반 수단과 활동을 의미한다(Solms 등 1990).

정보자산보호의 목표는 보안사고를 사전에 방지하고, 발생 시에도 조직의 손실을 최소화하여 사업의 연속성을 보장하고 손실은 저감하고, 이익을 최대화하기 위하여 다양한 위협으로부터 정보자산을 보호하는 것으로 이런 목표는 세가지 목표로 귀결된다. 즉 기밀성, 무결성, 가용성을 유지하는 것이다. 기밀성(Confidentiality)은 비인가된 개인, 단체, 프로세스 등으로부터 중요한 정보를 보호하는 것이다. 접근통제의 모든 행위는 근본적으로 기밀성 보호를 위한 것으로 실패할 경우 조직의 이미지가 실추될 수 있으며, 개인의 안전이 위협받을 수 있다. 보통 정보의 기밀성은 성격에 따라 여러 단계 수준으로 분류하여 강력하면서도 효율적으로 정보자산보호를 제공한다. 이러한 등급별 관리는 각 정보자산의 보호수준에 따라 접근권한을 달리함으로써 적절한 보호수준을 유지할 수 있도록 하기 위함이다. 무결성(Integrity)은 정보의 저장과 전달 시

비인가된 방식으로 정보가 변경, 삭제, 파괴되지 않도록 정확성과 완전성을 보장하는 것이다. 일반적으로 무결성은 데이터의 변조를 확인하는 의미 외에 인증을 통한 신분의 확실성 여부에 대한 확인까지 포함하는 넓은 의미로 쓰이기도 한다. 그것은 인증이 데이터를 만든 주체나 사용자의 실체가 올바른지를 판단하는 것으로 신분에 대한 확실성 여부를 무결성 점검의 범주에 포함시키기 때문이다. 이러한 무결성의 결여는 부정확한 결정의 원인이 될 수 있다. 가용성(Availability)은 인가된 사용자가 정보나 서비스를 요구할 때 언제든지 즉시 사용 가능하도록 하는 것이다. 인가된 사용자에게는 정보자산에 대한 접근이 지연, 방해되어서는 안되며 즉시 또는 적시에 서비스이용이 가능하여야 한다. 그러기 위해서는 데이터에 대한 백업이 가장 중요하며 형상관리, 변경통제, 사업연속성 계획 및 재난복구계획을 수립하여야 한다. 가용성의 결여는 중요한 임무수행을 불가능하게 만들 수 있고, 복구비용 등 재정적 손실을 초래 할 수 있다.

한편, 정보자산보호 활동은 조직이 보유한 정보 자산에 대하여 그 가치를 유지하고 보호하기 위한 활동으로 정의되며, 정보에 대한 위험관리 체계를 운영함을 의미한다(이경호 2006). 이 때의 위험이란 조직을 운영함에 있어 외부의 위협이 내부의 취약성을 이용하여 보유한 각종 자산에 피해를 입힐 수 있는 잠재적인 가능성을 말한다. 따라서 정보자산보호는 정보에 대한 위험관리이며 모든 정보보호 활동, 즉 정보보호정책을 수립하고 이를 수행하기 위한 조직을 구성하며 다양한 정보자산에 대하여 그 위협과 취약성을 판별하여 위험을 산출하고 대응책을 마련하는 일련의 활동이 정보자산보호 활동이라고 정의된다. 정보자산 위험에 대응하기 위한 정보자산보호 활동은 자산의 식별, 위험분석, 정책수립, 조직의 구성, 구성원의 인식수준 및 교육, 사후처리 등의 관리활동 관점과 물리적, 운영적, 기술적으로 주요 정보자산에 대한 접근 제한을 통한 통제활동 관점으로 구분 할 수 있다(이경호 2006).

### 2.2 정보자산보호 통제활동

과거에 문서로 정보를 관리하던 시대와 전산시설이 독립적으로 사용 되던 컴퓨터 초창기에는 문서나 컴퓨터가 있는 건물이나 사무실에 대하여 사람이 신체적으로 접근하는 것을 통제하는 물리적 보안통제를 통해 정보자산보호가 이루어 졌다. 그러나 현재와 같은 정보화 시대에서는 전체적인 정보보호의 일부분이 되었으나, 여전히 정보자산시설 보호에 중요한 부분을 차지하고 있으며, 정보자산보호의 기초적인 요소라고 할 수 있다. 정보자산보호 활동 중 기술적 통제활동은 광범위 하지만 시스템 보안과 네트워크 보안 분야로 크게 두 부분으로 나뉜다(서승우 2008). 시스템 보안은 암호화를 통한 파일이나 데이터의 안전한 저장 외에 시스템 접근권한 제어, 계정관리, 사용자 권한관리, 저작권보호, 바이러스 보안,

소프트웨어 검사, 데이터베이스 보안 등이 포함된다. 현재 모든 기업과 기관 등이 주요 보안 솔루션으로써 방화벽, VPN, IPS, Anti-Virus, Anti-Spam, 네트워크 접속 관리(NAC), 기타 Contents 보안 제품 등이 구축되어 각종 정보자산을 보호하고 있다.

정보자산보호 활동 중 운영적 통제활동은 급변하는 조직환경에서 운영의 필요사항과 변화하는 우선순위 및 과거에는 예상치 못한 새로운 위협과 취약점을 고려하고 도입된 통제방식이 수립된 정보보호정책에 의거하여 적절하게 운영되고 있는지를 확인하는 통제활동으로 Ariss(2001), Smith(1995) 등에 의해 제시되었다. 구체적인 활동으로는 정보자산보호 대상범위, 통제활동 등 정보보호정책 및 표준의 문서화, 조직내부 모든 구성원 및 조직과 업무계약을 맺은 외부사업자들에 대한 정보보호정책과 표준에 대한 지침 배부, 정보자산보호정책에 의거한물리적, 기술적 통제활동 운영의 적절성 확인, 시스템 개발 및 운영, 유지보수 수행 시 정보자산보호 통제활동 반영, 정보자산보호 정책 위반 시 적절한 징계절차 수행, 정보자산보호 통제활동을 관련 이슈사항 조정위원회 등 통제조직 운영 등이다.

### 2.3 정보자산보호 관리활동

물리적, 기술적, 운영적 통제활동만으로 성취할 수 있는 정보자산보호는 제한적이며 기술적인 방법은 적절한 정책 및 관리와 지침으로 지원될 필요가 있다. 이러한 정보자산보호 관리체계를 구축하기 위해서는 여러 가지 다양한 관점에서 정책/관리적 방안이 반영되어 통제 방안들과 상호 보완적으로 관리 운영체계가 구축되어야 한다. 정보자산보호 관리활동에 대한 기존 연구들은 정보자산보호 관리활동과 관련하여 조직차원에서의 관리활동이 중요함을 제시하고 있다(홍기향 2003). Caminada 등(1998)은 방화벽과 같은 정보보호 대책 및 유지 보수 활동을 강조했으며, Badenhorst 등(1994)은 위험분석, 위험 해결과 함께 지속적인 위험 관리를 통해 조직내 정보자산보호에 대한 일정한 수준에 대한 관리의 필요성을 주장하였다. Post 등(2000)은 실증연구를 통해 적절한 정보자산보호의 분류 및 구성원 교육 필요성을 경영층 및 조직원들에게 인식하게 하고, 정보자산보호 관리 등에 필요한 투자의 증가를 통해 능동적인 정보자산보호 아키텍처의 수립 및 활동 등을 수행할 수 있다고 하였다. 또한 Aron 등(2002)은 정보자산보호 중 사고에 대한 처리 및 관리와 정보자산보호 체계의 변경에 대한 관리 필요성을 제시하였다.

이상의 정보자산보호 관리활동에 대한 기존 연구를 살펴본 결과, 정보자산보호 관리활동에 대해서는 지속적인 위험관리 활동, 정보자산보호에 대한 분류 및 아키텍처, 조직에서의 참여 및 교육에 대한 필요성이 있음을 알 수 있다.

### 2.4 정보자산보호 성과 및 조직 성과

기업의 조직정보 유출 및 고객 정보 유출 사건 사례들은 기업의 이미지 영향을 미치는 것은 물론 기업의 생존여부를 좌우하기도 한다. 이러한 환경에서 정보자산보호 활동의 성과는 정보자산 유출 방지와 예방, 파트너 기업 간과 고객 간의 신뢰도 정보보호 효율성과 같은 1차적인 보호 성과와 경쟁우위 확보, 기업 및 조직의 이미지 개선 그리고, 이를 통한 고객기반 확보 및 매출증대 등 기업 및 조직의 궁극적인 목표 달성의 성과가 있다(홍기향 2003). 정보자산보호 활동 및 조직 성과에 대한 선행연구에 따르면, Kabay(1993)는 정보자산보호를 사회적 측면에서 고찰하여 정보자산보호 정책수립 및 문화, 인식제고 등의 활동이 조직 구성원의 정보보호 인식과 태도를 향상시켜 정보보호 사고를 방지할 수 있다고 하였다. Osborne(1996)은 증가하는 정보보호 부서의 비용 효과성을 향상시키기 위해 정책 수립, 위험분석, 인식제고, 교육 활동이 필요하다고 하였고, 정보보호 활동에 대해 정보보호 부서의비용대비 효과를 강조하였다. Moulton 등(1996)은 위험관리 활동에 대해 위험의 식별, 통제의 평가와 선택 등을 강조하였다. 또한 위험관리 활동이 정보보호 사고에 대한 예방 효과가 있다고 설명함으로써 정보보호 프로세스 개선을 강조하였다. Giidhue 등(1991)은 시스템 오용에 대한 사용자의 의심과 인식제고가 사용자의 정보보호 서비스 만족에 긍정적 영향을 준다는 실증연구를 통하여 정보자산보호 활동의 목적을 사용자의 정보보호 서비스 만족이라고 하였다. Blight(1997)는 금융업종의 개인 정보보호 서비스에 대한 고객만족을 조사한 결과, 고객의 정보보호 요구를 명시하고, 고객의 정보보호에 대한 책임과 권리를 명시하는 것이 서비스 만족도를 향상시킨다고 하였다. Parker(1997)는 제조업 분야의 정보가치에 대한 사례연구를 통해 정보자산보호의 목적은 정보기술 촉진, 자산보호와 같은 정보보호 성과뿐만 아니라 경쟁우위 확보, 이미지 개선 등의 기업의 본질적인 성과까지 포함되어 있다고 하였다. 또한 Ariss(2001)는 정보자산보호 활동에 대해 정보시스템 및 네트워크와 같은 정보자산에 대한 통제를 통해 정보 자산의 남용 방지뿐만 아니라 법 준수와 같은 공공만족의 성과를 가진다고 하였다. 이상의 선행연구를 살펴본 결과, 정보자산보호 기술들과 정책들은 정보자산보호 활동의 현실과 기술적 불완전함을 얼마나 또는 어떻게 잘 극복해 나갈 것인가라는 문제와 직결된다고 할 수 있다. 따라서 조직에서 정보자산보호 활동의 성과를 위해서는 정보자산보호 활동에 대한 투자 성과를 기반으로 의사결정에 대한 권한과 책임이 필요하며 통제적, 정책적 모든 활동이 함께 반영되고 정보자산보호 활동과 조직의 목표 사이의 균형을 맞출 필요가 있음을 알 수 있다(Smith 2001).

### 2.5 연구 가설의 설정

정보자산보호 활동에 대한 본 연구에서는

정보자산보호 활동이 정보자산보호 성과에 영향을 미치며, 정보자산보호 성과가 조직의 본질적인 성과에 기여한다는 것이 관련 연구들을 통하여 제시되어 이를 검증하고자 하며, 다음과 같은 가설을 설정하였다. 이에 대한 연구모형이 〈그림 1〉에 제시되어 있다.

가설1. 정보자산보호 관리활동은 정보자산보호 성과에 영향을 미친다

가설2. 정보자산보호 통제활동은 정보자산보호 성과에 영향을 미친다

가설3. 정보자산보호 성과는 조직의 성과에 영향을 미친다.

### 2.6 연구 모형

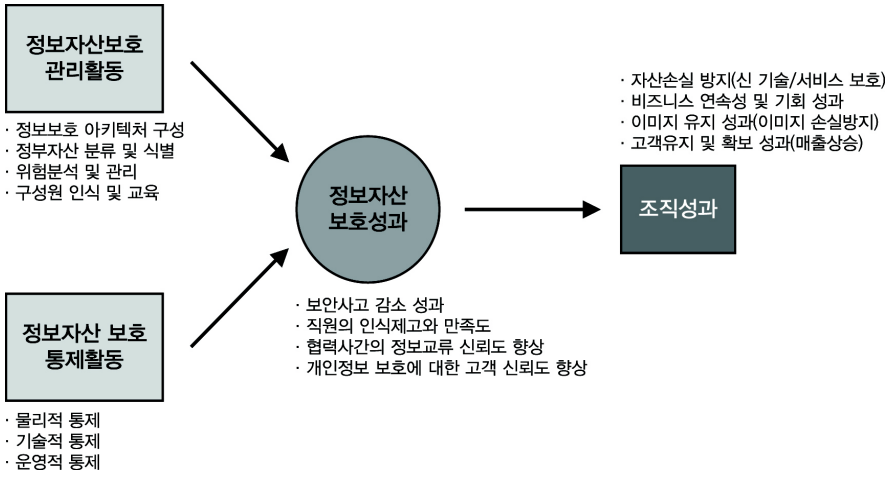
정보자산보호 활동과 정보자산보호 성과 및 조직 성과에 대한 본 연구의 개념적 모형은 〈그림 1〉에 나타나 있다. 위 연구에서 설명한 바와 같이 본 연구에서는 문헌 연구를 통해 정보자산보호 성과에 미치는 요인으로 정보자산보호 관리 및 통제활동을 설정하였다. 또한 조직 성과에 영향을 미치는 요인으로 정보자산보호 성과를 설정하였다.

따라서 정보자산보호를 위한 관리활동과 통제활동에 관한 연구모형은 다음의 〈그림 1〉과 같이 제시될 수 있다.

## 3. 연구 방법

### 3.1 표본 및 자료수집

본 연구의 자료수집은 대한상공회의소 선정 100대 기업 및 기관(2007년 매출액 기준) 중 50여 개 기업 및 기관을 대상으로 2008년 11월 10일부터 11월 30일까지 약 3주간 설문




〈그림 1〉 연구 모형

조사 방법으로 실시하였다. 본 연구의 분석 단위는 조직이며, 설문대상자는 각 기업 및 기관의 정보보호 관련 업무 종사자와 또는 유관업무 종사자를 대상으로 기업 및 기관당 1명씩 설문지를 배포, 수집하였다. 설문 회수 현황은 다음 〈표 1〉과 같이 총 52부의 설문이 배포되어 39부의 설문지가 회수되었으며, 설문 중 결측치를 포함하는 8개의 설문지를 제외한 31개의 설문지로 최종 분석하였다.

〈표 1〉 조직 대상 설문회수 현황

| 구분 | 배포 | 회수 | 결측설문 | 분석설문 |
|---|---|---|---|---|
| 배포 설문 수 | 52 | 39 | 8 | 31 |
| 비율 | 100% | 75% | 15% | 60% |

〈표 2〉 설문응답조직의 업종분석

| 업종 | 샘플 수 | 비율 |
|---|---|---|
| 공공기관/정부투자기관 | 3 | 10% |
| 건설/제조업 | 6 | 19% |
| 금융업 | 5 | 16% |
| 정보통신업 | 11 | 35% |
| 교육/문화업 | 4 | 13% |
| 기타 | 2 | 6% |
| 계 | 31 | 100% |

〈표 3〉 설문응답조직 규모분석

| 종업원수 | 샘플수 | 비율 |
|---|---|---|
| 10,000명 이상 | 1 | 3% |
| 10,000명 미만 | 1 | 3% |
| 5,000명 미만 | 9 | 29% |
| 1,000명 미만 | 12 | 39% |
| 100명 미만 | 8 | 26% |
| 계 | 31 | 100% |

〈표 4〉 설문응답조직 정보보호 인력규모(전체 IT인력 대비)

| 정보보호 인력규모 | 샘플수 | 비율 |
|---|---|---|
| 30%이상 | 0 | 0% |
| 20%미만 | 1 | 3% |
| 10%미만 | 4 | 13% |
| 5%미만 | 8 | 26% |
| 3%미만 | 11 | 35% |
| 별도 없음 | 7 | 23% |
| 계 | 31 | 100% |

### 3.2 연구변수의 측정

본 연구에서 논의된 연구변수들의 조작적 정의와 측정도구는 아래와 같다.

#### 3.2.1 정보자산보호 통제활동

정보자산보호 통제활동은 정보보호 성과를 위한 직접적인 활동으로서 운영적, 기술적, 물리적 통제활동의 정도로 정의된다. 정보에 대한 인가된 사람에게 접근을 허용하고 인가되지 않은 사람에게는 접근을 통제하는 물리적 보안활동, 네트워크, 응용시스템에 대한 기술적 접근통제활동과 외부인의 불법적인 접근시도와 내부 관련자들의 부주의나 고의적인 행동에 의해 불법 접근이 이루어질 가능성은 항상 존재한다. 이러한 불법적 접근에 의한 마지막 보호수단인 암호화와 정보보호정책에 의거하여 적절하게 운영되고 있는 지를 확인하는 통제활동인 운영적 통제를 변수로 구성하였다. 본 연구에서는 위 조작적 정의를 바탕으로 해당 8개 측정항목을 리커트 5점 척도로 측정하였다.

#### 3.2.2 정보자산보호 관리활동

정보자산보호 관리활동은 정보자산보호 성과라는 목표를 달성하기 위하여 조직이 수행하는 행위로써 직접적인 기능보다는 효과적이며 효율적인 정보보호 성과를 위한 관리활동의 정도로 정의된다. 보호대상 정보자산 식별 및 평가 리스크 분석 및 평가, 조직체계 수립 및 교육, 정보자산보호 정책수립, 사고대응 및 사후관리로 이어지는 정보자산보호 아키텍처 수립활동 내용을 이론적 고찰을 통하여 변수로 구성하였다. 본 연구에서는 위 조작적 정의를 바탕으로 해당 9개 측정항목을 리커트 5점 척도로 측정하였다.

#### 3.2.3 정보자산보호 성과

정보자산보호 성과는 조직이 목표로 보안사고 감소 성과, 직원의 인식제고와 만족도 향상, 협력사 간의 정보교류 신뢰도 향상, 개인정보보호에 대한 고객 신뢰도 향상과 같은 정보자산보호 활동 성과의 정도로 정의된다. 본 연구에서는 위 조작적 정의를 바탕으로 해당 5개 측정항목을 리커트 5점 척도로 측정하였다.

#### 3.2.4 조직 성과

조직 성과는 기술/서비스보호를 통한 자산손실 방지, 비즈니스 연속성 및 기회 성과, 이미지손실 방지에 따른 이미지 유지 성과, 고객유지 및 고객기반 확대 성과에 따른 매출 증대 성과의 정도로 정의된다. 본 연구에서는 위 조작적 정의를 바탕으로 해당 3개 측정항목을 리커트 5점 척도로 측정하였다.

## 4. 연구의 분석 및 결과

### 4.1 측정 모형의 검증

본 연구에서는 자료 분석을 위하여 PLS

(Partial Least Squares)를 사용하였다. PLS는 AMOS 등의 구조 방정식 분석기법에 비해 상대적으로 적은 수의 표본을 대상으로도 사용 가능하며, 변수의 타당성을 측정하는 측정모델(measurement model)과 변수의 경로와 설명력을 나타내는 구조 모형(structural model)을 동시에 측정할 수 있다(Yoo and Alavi 2001). Barclay 등(1995)은 PLS가 정보시스템과 관련된 조직 및 사회 현상을 연구하는 데 적합한 도구라고 설명하였으며, 이 연구에서와 같이 측정 도구가 개발되지 않았거나 측정모형이 탐험적인 연구에 PLS 연구가많이 사용되고 있다. 이 연구의 목적도 인과관계 증명에 있으며, 설문대상이 조직이므로 표본 수 확보에 대한 제한성으로 PLS가 본 연구에 적합하다고 판단된다. 가설 검증을 위한 구조 모형(structural model) 검증에 앞서 측정치의 신뢰성과 타당성 분석을 위한 측정 모형(measurement model)의 검증을 수행하였다.

연구 모형에 포함되어 있는 변수의 측정을 위한 설문 항목들의 신뢰성(reliability)과 개념타당성(construct validity)을 확인적 요인분석(confirmatory factory analysis)으로 평가하였다. 이를 위해 기본적으로 각 변수별 개별항목 신뢰성(individual item reliability), 내적 일관성(internal consistency), 그리고 판별타당성(discriminant validity)을 분석하였다. 개별항목 신뢰성은 측정하고자 하는 개념(construct)과 관련된 설문 항목들의 요인적재값(factor loading)으로 평가된다. 개별 항목 신뢰성은 수렴타당성 (convergent validity)으로도 간주된다. Yoo and Alavi(2001)는 개별 항목 신뢰성, 내적 일관성, 판별타당성으로 측정모형을 검증, 즉 설문 항목의 신뢰성과 타당성을 검증한 바 있는데 요인 적재값이 0.6 이상의 경우 개별항목 신뢰성이 있는 것으로 간주하였다. 내적 일관성은 종합요인 신뢰성 지수(composite scale reliability index)를 사용하여 분석하였다. 종합요인 신뢰성 지수가 0.7 이상이면 각 변수의 측정이 내적 일관성이 있다고 판단된다. 판별타당성의 평가는 추출된 평균분산(AVE: average variance extracted)의 제곱근 값을 사용한다(Barclay et al. 1995). 각 측정 항목은 모형 내의 다른 개념보다 자신이 나타내고자 하는 개념과 더 큰 분산을 공유하여야 하는데, 추출된 평균분산의 제곱근 값이 다른 측정 변수와의 분산 공유 정도보다 높고 0.7 이상이면 판별타당성이 있다고 볼 수 있다. 판별타당성의 또 다른 평가는 교차요인 적재값(cross-factor loading)과 요인 적재값의 비교를 통해서 이루어질 수 있다. 각 측정항목의 요인 적재값은 교차요인 적재값보다 높아야 판별타당성이 존재하는 것으로 평가된다.

〈표 5〉에는 연구 모형에 있는 변수인 정보보호 통제활동과 정보보호 관리활동, 그리고 종속 변수인 정보보호 성과와 조직성과에 대한 측정항목들의 요인 적재값과 교차요인 적재값을 보여준다. 모든 항목의 요인 적재값은 동일 항목의 교차요인 적재값 보다 크고, 그 크기도

〈표 5〉 연구변수의 요인 적재값과 교차요인 적재값

| 변수 | 측정항목 | 정보보호 통제활동 | 정보보호 관리활동 | 정보보호 성과 | 조직성과 |
|---|---|---|---|---|---|
| 정보자산보호 통제활동 | 시스템 라이프 사이클 통제 | 0.876 | 0.514 | 0.447 | 0.536 |
| | 악성소프트웨어 방지시스템 활용 | 0.728 | 0.548 | 0.354 | 0.473 |
| | 시스템 도입 및 개선 시 인수 절차 | 0.780 | 0.530 | 0.327 | 0.437 |
| | 핵심 DB와 S/W의 백업 및 테스트 | 0.720 | 0.437 | 0.257 | 0.394 |
| | 안전한 외부 설비 운용(DR센터) | 0.765 | 0.454 | 0.335 | 0.400 |
| | 정보자산 포함 매체의 제거 및 폐기 통제 | 0.691 | 0.485 | 0.272 | 0.395 |
| | ID및 패스워드 구성표준 | 0.661 | 0.466 | 0.465 | 0.411 |
| | 사내 네트워크 접속 인식 및 통제 | 0.810 | 0.595 | 0.470 | 0.505 |
| | 시스템의 통제가 부적절시 통제권한 부여 | 0.680 | 0.529 | 0.402 | 0.559 |
| 정보자산보호 관리활동 | 중요 정보보호 이슈 CIO 직보 체계 | 0.406 | 0.777 | 0.398 | 0.485 |
| | 정보보호 의식교육 | 0.507 | 0.828 | 0.545 | 0.424 |
| | 임직원의 의지 및 인식 | 0.455 | 0.657 | 0.394 | 0.532 |
| | 외부전문가 집단, 기관, 업체 긴밀도 | 0.628 | 0.675 | 0.472 | 0.404 |
| | 정보자산 식별, 목록화 및 관리 | 0.561 | 0.784 | 0.638 | 0.635 |
| | 정보자산 분류의 업무목적 연관성 검토 | 0.522 | 0.732 | 0.442 | 0.345 |
| | 정보자산의 소유/사용부서 명시 및 자산 가치 명시 | 0.504 | 0.760 | 0.561 | 0.506 |
| | 리스크 분석시 자연적 및 인적 위협 고려 | 0.454 | 0.715 | 0.520 | 0.457 |
| 정보자산보호 성과 | 정보보호 사고 감소 | 0.441 | 0.540 | 0.783 | 0.570 |
| | 정보보호 효율성 증대 | 0.499 | 0.572 | 0.815 | 0.597 |
| | 임직원의 정보보호 교육 참여도 상승 | 0.480 | 0.633 | 0.906 | 0.627 |
| | 임직원의 정보보호 업무 만족도 상승 | 0.347 | 0.501 | 0.804 | 0.557 |
| | 임직원이 정보보호 책임의식 상승 | 0.344 | 0.557 | 0.808 | 0.633 |
| 조직성과 | 비즈니스 연속성 확보 | 0.636 | 0.543 | 0.608 | 0.854 |
| | 기업 신뢰도와 이미지 상승 | 0.508 | 0.643 | 0.747 | 0.949 |
| | 고객유지 및 확보 영향도 | 0.513 | 0.504 | 0.542 | 0.842 |

모두 0.6 이상이며, 측정항목의 개별항목 신뢰성과 판별타당성을 보여주는 것이다. 〈표 6〉은 내적 일관성 및 판별타당성의 분석 결과를 보여준다. 모든 종합요인 신뢰성 지수가 0.8 이상으로 각 측정 항목은 신뢰성이 있다고 볼 수 있다. 추출된 평균분산의 제곱근 값이 모두

〈표 6〉 연구 변수의 내적 일관성 및 판별타당성

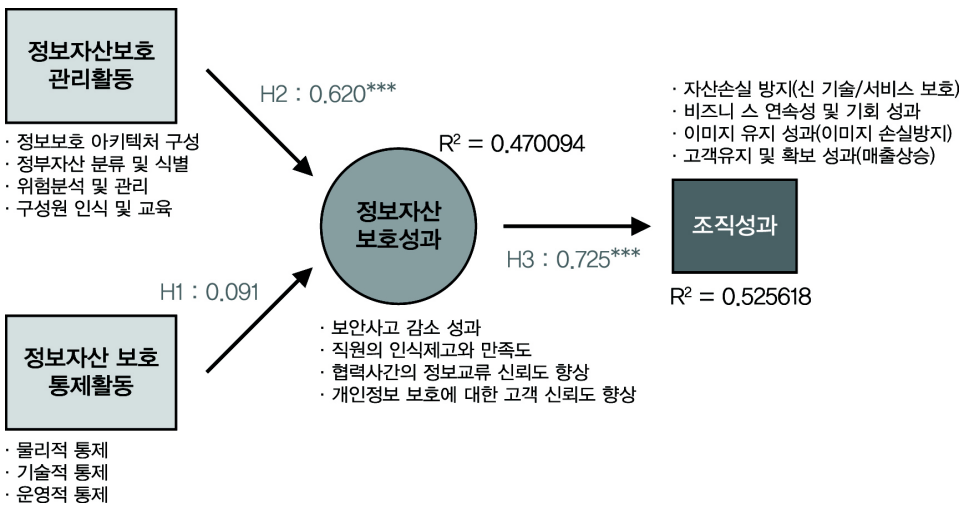
| 변수 | 측정 항목수 | 종합 신뢰성 지수 | 추출된 평균분산의 제곱근 값 | | | |
|---|---|---|---|---|---|---|
| | | | 정보자산보호 통제활동 | 정보자산보호 관리활동 | 정보자산 보호성과 | 조직성과 |
| 정보자산보호 통제활동 | 9 | 0.92 | 0.75 | | | |
| 정보자산보호 관리활동 | 8 | 0.91 | 0.63 | 0.74 | | |
| 정보자산보호 성과 | 5 | 0.91 | 0.60 | 0.72 | 0.82 | |
| 조직성과 | 3 | 0.91 | 0.31 | 0.41 | 0.38 | 0.88 |

0.7 이상이며, 다른 상관 계수값보다 높은 것을 보여준다. 이는 이 연구의 측정 항목들이 판별타당성 조건을 만족한다고 볼 수 있다.

### 4.2 구조 모형의 검증

PLS를 통한 구조 모형의 경로 분석 결과가 〈그림 2〉와 〈표 7〉에 요약되어 있다.

구조 모형의 분석 결과, 정보자산보호 관리활동은 정보자산보호 성과에 긍정적인 영향을 미치는 것으로 나타났다(가설 2의 채택, t=7.851, p=0.001). 그리고 정보자산보호 성과 또한 조직의 본질적인 성과에 긍정적인 영향을 미치는 것으로 밝혀졌다(가설 3의 채택, t=18.855, p=0.001). 그러나, 정보자산보호 통제활동은 정보자산보호 성과에 미치는 영향은 기각 되었다(가설 1의 기각, t=1.101, p=0.28). 즉, 정보자산보호 성과를 위해서는 강제적이고 단편적인 통제 중심의 활동보다는 체계적인 관리적, 정책적 활동과 이에 따른 위한 조직구성, 구성원의 정보보호에 대한 인식변화가 긍정적인 영향을 미치며, 이와 같은 정보자산보호 활




〈그림 2〉 가설검증 결과

〈표 7〉 경로 분석 결과

| 구분 | 경로 | 경로계수값 | T-값 | P값 | 가설검증결과 |
|---|---|---|---|---|---|
| 가설 1 | 정보자산보호통제활동 → 정보자산보호 성과 | 0.091 | 1.101 | 0.28 | 기각 |
| 가설 2 | 정보자산보호관리활동 → 정보자산보호 성과 | 0.620 | 7.851 | 0.00 | 채택 |
| 가설 3 | 정보자산보호 성과 → 조직성과 | 0.725 | 18.855 | 0.00 | 채택 |

동을 통한 보안사고 감소, 임직원의 정보보호 인식제고와 같은 정보자산보호 성과 또한 고객 기반 확대, 매출 증대 등 조직의 본질적인 성과에 긍정적인 영향을 미치는 것으로 분석되었다.

## 5. 결 론

### 5.1 연구의 의의와 시사점

본 연구는 기존 연구 문헌들과 실제 사례 및 현황 조사를 토대로 정보자산보호 활동이 정보자산보호 성과에 영향을 미친다는 전제하에 정보보호 성과에 영향을 미치는 정보자산보호 활동을 직접적인 통제활동과 정보자산보호 성과를 효율화, 효과 극대화를 위한 정책, 관리활동으로 측정 항목을 도출하여 유의성을 살펴 보았고, 이어서 이러한 정보자산보호 성과가 조직의 본질적인 성과에 미치는 영향을 살펴보았다.

연구분석 결과, 정보자산보호 관리활동은 정보자산보호 성과에 영향을 미치지만 정보자산 통제활동은 정보자산보호 성과에 미치는 영향은 미약한 것으로 검증되었으며, 이어서 정보자산보호 성과는 조직의 본질적인 성과에 대한 영향에 대한 검증도 채택되었다. 정보자산보호 통제활동이 정보자산보호 성과에 유의한 영향을 미치지 못하는 것으로 나타난 결과는 국내기업들이 정보자산보호를 위한 통제활동에 대한 투자 등 리소스 투입의 노력에 비하여 성과에 대한 결과가 미흡하거나 불확실한 것으로 인식되고 있는 것으로 사려된다. 즉, 정보자산보호 성과를 위해서는 강제적이고 단편적인 통제중심의 활동보다는 체계적인 관리적, 정책적 활동과 이에 따른 조직구성, 구성원의 정보보호에 대한 인식변화가 긍정적인 영향을 미치며, 이와 같은 정보자산보호 활동을 통한 보안사고 감소, 임직원의 정보보호 인식제고와 같은 정보자산보호 성과 또한 고객 기반 확대, 매출 증대 등 조직의 본질적인 성과에 긍정적인 영향을 미치는 것으로 분석되었다.

기업 및 조직에서는 정보자산을 여러 가지 통제 및 관리 수단을 통해 보호활동을 하고 있으나, 보안수준을 높게 요구할수록 업무 수행의 불편함으로 단기적인 효율성 및 생산성이 감소하게 되는 딜레마에 빠지게 된다. 이러한 상황으로 인해 정보자산보호 활동이 조직적이고 체계적으로 수행할 수 있는 정보자산보호 아키텍처와 같은 관리적/정책적 프로세스 정립이 요원하며 단편적인 통제활동 중심으로 이루어지고 있으나, 본 연구 결과에서 나타났듯이 조직이 정보자산보호 성과를 극대화시키기 위해서는 단편적인 통제활동보다는 체계적인 관리활동이 유의함이 증명 되었으며, 이와 같은 정보자산보호 활동에 대한 투자에 따른 성과가 조직의 본질적인 성과에 긍정적인 영향을 미치는 것으로 나타났다. 본 연구의 결과는 기업 등 조직에서 통제 중심의 정보보호 활동을 장단기에 걸친 관리 및 투자 중심으로 확

대하고 정보자산보호 활동방향 수립 시 관리적, 정책적 요소의 중요성이 반영되고, 조직의 성과와 정보자산보호에 대한 리소스 투입 간의 관계된 의사결정 시 긍정적인 방향으로 기여 할 것으로 기대된다.

### 5.2 연구의 한계 및 향후 발전방향

본 연구는 다음과 같은 한계점을 가지고 있다. 이와 같은 한계점은 향후 연구에서 보완되어 더욱 발전적인 방향으로 나아가도록 해야 할 것이다.

첫째, 정보자산보호 활동과 관련하여 횡단적(cross-sectional) 연구를 수행하여 보호활동 이전과 이후에 대한 성과 관련성에 관한 연구를 수행하지 못했다는 점이다. 정보자산보호 활동 이전과 이후에 대한 차이 분석이 수행될 필요가 있으므로, 차후의 연구에서는 종단적(longitudinal) 차원의 연구가 수행된다면 현재의 연구보다 진보된 연구로 평가될 것이다.

둘째, 조직 특성별 영향 요인이나 차이에 대한 설명이 부족하다. 본 연구에서는 조사 대상인 조직별 특성들을 고려하지 않고 정보자산보호 활동에 관한 자료 수집과 조사가 이루어졌기 때문에 이러한 세부적 차이에 대한 설명이 부족하다. 이들 특성들이 분석대상으로 포함되었다면 연구결과에 대해 좀 더 일반론적인 대표성을 가질 수 있었을 것이다. 또한 기업 및 조직내 정보보호 담당자라는 조직 단위의 설문대상의 제한성으로 절대적인 샘플 확보가 부족하여 분석결과에 한계가 있다.

연구의 한계에서도 지적했듯이 향후 연구방향은 정보자산보호 활동에 대한 더욱 많은 영향 요소들을 고려한 포괄적인 연구모델의 개발의 필요성이 제기된다. 또한 정보자산의 종류와 기업 업종에 따른 연구가 이루어진다면 더욱 구체적이고 실제적인 연구결과로서 활용할 수 있을 것으로 생각된다. 정보자산보호 활동의 핵심요인 도출 및 성과에 대한 실증적 연구가 부족한 상황이다. 향후 연구에서는 기업 및 조직의 정보자산보호 활동의 효과를 극대화하고 보편화한 연구가 진행될 필요가 있으며, 이는 정보자산보호 활동 연구에 있어서 큰 의의가 있을 것으로 판단된다.

## 참 고 문 헌

서승우. 2008.『보안경제학』. 서울: 서울대학교 출판부.

이경호. 2006.『위험관리와 정보보호 사례 분석』. [서울]: 한국교육학술정보원. RM2006-75.

이준택. 2007.『정보보호학개론』. 서울: 생능출판사.

홍기향. 2003.『정보보호 통제와 활동이 정보보호 성과에 미치는 영향에 대한 연구』. 박사학위논문, 국민대학교 대학원, 정보관리학과.

Ariss, S. S. 2002. "Computer Monitoring: Benefits and Pitfalls Facing Mana-

gement." *Information & Management*, 39(7): 553-558.

Aron, J. L., O'Leary, M. Gove, R. A. Azadegan, S. ,and Schneider, M. C. 2002. "The Benefits of a Notification Process in Addressing the Worsening Computer Virus Problem: Results of a Survey and a Simulation Model." *Computer & Society*, 21(2): 142-163.

Badenhorst, K. P. and Eloff, J. H. P. 1994. "TOPM: a Formal Approach to the Optimization of Information Technology Risk Management." *Computers and Security*, 13(5): 411-435.

Barclay, D., Higgins, C., and Thompson, R. 1995. "The Partial Least Squares [PLS] Approach to Causal Modeling, Personal Computer Adoption and Use as an Illustration." *Technology Studies*, 2(2): 285-309.

Blight. J. 1997. "Customer Privacy versus Customer Service." *Information Security Technical Report*, 21(1): 43-46.

Caminada, M., Reind van de Riet, Arjen van Zanten, and Leendert van Doorn. 1998. "Internet Security Incidents, a Survey within Dutch Organizations." *Computer and Security*, 17(5): 417-433.

Giidhue, D. I. and Straub, D. W. 1991. "A Study of Perceptions of the Adequacy of Security." *Information & Management*, 20: 13-27.

Kabay, M. F. 1993. "Social Psychology and Information Security." Datapro: 101-105.

Moulton, R. T. and Moulton. M. E. 1996. "Electronic Communications Risk Management: A Checklist for Business Managers." *Computers and Security*, 15(5): 377-386.

Osborne, K. 1996. "Cost-Effective IT Security." Datapro: 1-8.

Parker, D. B. 1997. "The Strategic Values of Information Security in Business." *Computer and Security*, 16(7): 572-582.

Post, G. and Karan, A. 2000. "Management Tradeoffs in Anti-virus Strategies." *Information & Management*, 37(1): 13-24.

Solms, R., Eloff, J. J. P., and Solms, S. H. 1990. "Computer Security Management: A Framework for Effective Management Involvement." *Security*, 12(4): 217-222.

Smith, S., Stephen, G., and Malampy, W. 1995. "A financial Management Approach for Selecting Optimal, Cost-Effective Safeguards Upgrades

for Computer and Information Security Risk Management." *Computer and Security*, 14(1): 28-29.

Yoo, Y. J. and Alavi, M. 2001. "Media and Group Cohesion: Relative Influences on Social Presence, Task Participation, and Group Consensus." *MIS Quarterly*, 25(3): 371-390.