KIPS Tr. Comp. and Comm. Sys.
Vol.3, No.9 pp.301~310 pISSN: 2287-5891

http://dx.doi.org/10.3745/KTCCS.2014.3.9.301

The Moderating Effects of Information Security Policy between Information Security Maturity and Organizational Performance

Park, Jeong Kuk† · Kim, Injai††

ABSTRACT

The absence of proactive information security management to ensure availability, accessibility and safety of information can bring serious risks to customers as well as to the organization's performance and competitiveness because improper security management undermines business continuity. This study analyzed the maturity of information security which affects the organizational performance. Through the literature reviews, a research model using the organizational performance as the dependent variable, the risk management process maturity and risk assessment process as independent variables and the information security policy indexes as moderate variables was proposed, and an empirical analysis was made on the basis of survey.

The results showed that there was a high causal relationship between information security maturity and organizational performance. However, even if the proportions of information security staff ratio and the information security budget ratio increased, information security maturity did not affect organizational performance. It suggests that information security maturity affects organizational performance, but information security regulations have their limitation as being a catalyst to improve organizational performance.

Keywords : Information Security, Risk Management, Risk Assessment, Information Security Maturity Level, Organizational Performance

정보보호 성숙도와 조직성과 간의 정보보호 정책의 효과분석

박 정 국† · 김 인 재††

요 약

정보의 가용성, 접근성, 안전성을 확보하기 위한 선제적인 정보보호 관리의 부재는 서비스 연속성을 훼손하여 고객에게 뿐만 아니라 조직의 성과와 경쟁력에 심각한 리스크를 가져다 줄 수 있다. 본 연구는 정보보호 성숙도가 조직성과에 미치는 영향을 분석하기 위하여 문헌 조사를 통해 조직성과, 위험 관리 프로세스 성숙도, 위험 평가 프로세스 성숙도, 정보보호 정책지표를 포함하는 연구모형을 만들고 설문을 통한 실증분석을 하였다.

연구결과 위험 관리 및 위험 평가의 프로세스 성숙도와 조직성과 간에는 높은 인과 관계가 있는 것으로 나타났다. 하지만 정보보호 인력비율, 정보보호 예산비율에 따라 정보보호 성숙도가 조직성과에 미치는 영향은 차이가 없는 것으로 나타났다. 이는 정보보호 성숙도 수준은 조직성과에 영향을 미치나, 실효성이 검증되지 않은 정보보호 정책 및 규제는 정보보호 성숙도가 조직의 성과 향상의 촉매제로 활용하는데 한계가 있음을 시사하고 있다.

키워드 : 정보보호, 위험관리, 위험평가, 정보보호 성숙도, 조직성과

1. 서 론

오늘날은 하나의 디바이스로 TV를 보고, 통화를 하며, 인터넷에 접속할 수 있는 시대를 넘어 자신이 지니거나 마주하는 모든 사물이 서로 연결되는 융합의 시대다. 가까운 미래에는 PC나 모바일뿐 아니라 자신이 원하는 모든 디바이스로 일상 활동을 할 수 있는 길이 열릴 것이다. 최근 소셜 미디어와 모바일 디바이스의 확산, 차세대 애플리케이션의 증가, 클라우드 컴퓨팅 등 IT 트렌드 변화는 새로운 보안 시스템에 대한 큰 도전이 될 것이다. 2013년에 과도한 정보의 수집과 내부 유출이 원인이 되었던 미국 국가정보국 감시 폭로 사건과 2014년 1월 국내 카드사의 1억 건 이상 개인정보 유출 사건, 이와 함께 특정 표적을 노리고 고급 정보를 빼내거

† 준 회 원 : 동국대학교 경영정보학과 박사과정
†† 정 회 원 : 동국대학교 경영학부 교수
Manuscript Received : July 21, 2014
First Revision : September 3, 2014
Accepted : September 3, 2014
* Corresponding Author : Kim, Injai(ijkim@dongguk.edu)

나 파괴하는 공격의 등장은 정보기술에 의존적인 현재 보안 체계를 뒤흔들었다. 보안사고로 인한 막대한 손해에서 보는 것처럼 이제 보안문제는 기술만이 아닌 기업의 사업과 경영 차원의 과제가 되었으며 효과적인 정보보호 전략 수립은 기업의 생존을 위한 필수불가결한 요소가 되었다[1].

조직이 보유한 정보 자산에 대하여 그 가치를 유지하고 보호하기 위한 정보보호는 기본 요소로서 정보에 대한 위험 관리체계 운영 등 정보보호 관리가 필수적이다[2]. 정보보호 관리의 성숙도와 성과 간에는 긍정적 상관관계가 있으며[3], 선제적인 정보보호 관리의 부재는 서비스 중단을 야기하여 고객뿐만 아니라 조직의 성과와 경쟁력에 심각한 리스크를 가져다 줄 수 있다[4].

앞으로 기업들은 비즈니스 연속성, 관련 법규 준수, 존중받는 조직 이미지와 정보의 기밀성, 자료의 무결성 및 가용성 확보를 위해 IT의 일부로 정보보호를 바라보는 시각에서 벗어나 조직성과에 영향을 미치는 비즈니스 이슈로 여기고 필요한 정보보호 관리 프로세스를 만들어 가야 한다.

본 연구는 문헌조사를 통해 정보보호 관리의 이론적 배경을 제시하고 정보보호 관리의 주요 구성요소인 위험 관리 프로세스 및 위험 평가 프로세스 성숙도가 조직성과에 어떤 영향을 미치는지를 검증하고, 정보보호 정책지표가 정보보호 관리 성숙도와 조직의 성과 간의 조절효과가 있는지를 실증적으로 분석하고자 한다.

2. 문헌 연구

2.1 정보보호 관리 성숙도에 관한 연구

ISO 27001에 따르면 정보보호는 정보에 대한 위험 관리이며 정보보호 관리의 주요 구성요소가 위험 관리와 위험 평가이다. 그들은 널리 알려져 있지만 위험 관리와 위험 평가에 대한 정의는 여러 관련 문헌에서 발견된다[5,6,7].

Fig. 1의 위험 관리 프로세스와 위험 평가에 관한 개념도에서 보는 바와 같이 위험 관리는 초기화 한 후 분석, 기획, 구현, 통제 및 측정값 모니터링, 시행된 보안 정책을 다루는 순환 활동이다. 반면, 위험 평가는 위험 관리 프로세스의 일부로서 정보보안 전문가들에게 일반적으로 인정된다. 위험 평가는 특정 시점(예를 들어 1년에 한 번, 필요 시)에 실행되며 - 다음 평가가 실행될 때까지 - 전체 위험 관리 프로세스에 대한 횡단적인 관점을 제공한다[8].

Hall[9]은 정보보호 관리 성숙도를 관련 법률, 계약, 그리고 내부의 요구사항을 준수하는 한편 기밀성, 무결성 그리고 가용성을 침해하는 보안위협으로부터 정보 및 정보시스템을 보호하고 정보자산에 대해 더 나은 통제를 제공하며,

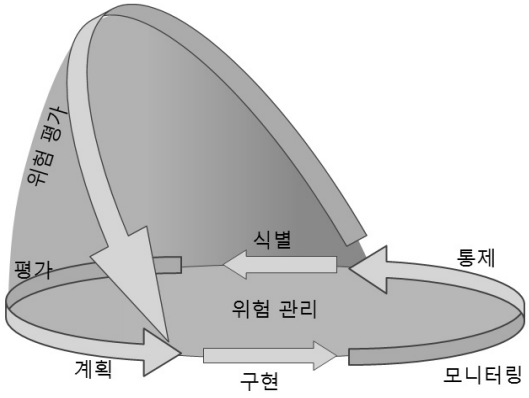


Fig. 1. Risk Management Process and Risk Assessment Process

공격에 대해 즉각적으로 대응하고 신속하게 복구하는 정도라고 정의하고 정보보호 관리 수준과 조직성과 간에는 긍정적 연관성이 있다고 했다.

조직이 성숙한 정보보호 수준을 달성하기 위해 다음과 같은 잘못된 인식을 극복해야 한다. 첫째, 조직들은 정보보호를 단순히 구입할 수 있는 생각을 가지고 정보보호 관련 문제를 해결하기 위해 비용을 지출하는 경향이 있다[10]. 그러나 Sommer[11]는 정보보호란 박스 안에 홀로 존재하는 것이 아니므로 조직은 하나의 제품이 아닌 프로세스로 보아야 한다고 했다. 둘째, 조직은 모든 정보보호 문제에 대한 기술적 해결책이 있다고 생각하고 싶어 한다. 따라서 조직은 기술에 과도하게 의존적인 단편적 접근 방식을 취하게 된다. 그러나 이는 정보보호를 주로 기술적 문제로 생각하는 경우, 다른 중요한 요소 즉, 물리적 보안 및 비 기술적, 절차적 정보보호가 무시되는 문제를 야기한다[12]. 셋째, 그들을 공격 목표로 만드는 행위를 하지 않기 때문에 자신들은 안전하고 믿는다. 그러나 사이버 세계에서의 많은 증거는 해커는 본질적으로 악의적이며 공격에 특별한 이유를 필요하지 않는다는 사실을 보여주고 있으므로 조직은 이를 깨달을 필요가 있다[13,14]. 마지막으로 그들은 아직 공격의 희생양이 되지 않았기 때문에, 자신의 정보 자산을 보호하기 위한 충분하고 효과적인 보안 조치를 가지고 있다고 조직은 믿는다. 그러나 조직의 정보시스템이 침해당하지 않았다는 단순한 사실은 조직이 좋은 보안대책을 운용하고 있다는 것을 의미하지는 않고 지금까지 단지 운이 좋았다는 것을 의미할 수도 있다고 했다[15].

정보보호 성숙도 평가 모델은 조직이 현재 수준을 알 수 있도록 가이드 역할을 하며 일반적으로 프로세스가 명시적으로 정의, 관리, 측정, 통제될 때 주어진 성숙도를 달성 한 것으로 간주된다. 여러 가지 성숙도 모델이 문헌조사에서 발견되었으며 주요 모델은 다음과 같다. 첫째, 통합된 능력

성숙모델(Capability Maturity Model Integration : CMMI)이다. 1987년 카네기 멜론 대학의 연구 센터인 SEI(Software Engineering Institute)가 개발하였으며, 모델의 목적이 조직의 프로세스 완성도를 평가하고 향상된 제품을 얻을 수 있도록 프로세스를 개선하는 것이다. CMMI는 단계적 표현(Staged Representation), 연속적 표현(Continuous Representation)이라는 2가지 표현을 가지고 있다. 단계적 표현이 5 단계 성숙도(Initial, Managed, Defined, Quantitatively Managed, and Optimizing)를 가지고 있는 한편, 연속적 표현은 0부터 5까지 6단계 역량 레벨을 가지고 있다[16]. 둘째, 정보와 관련 기술의 통제목적(Control Objectives for Information and related Technology : COBIT)이며, ITGI(IT Governance Institute)에서 관리한다[17]. IT프로세스, 관행, 통제에 대한 감사에 기초한 일련의 지침이며 위험 경감에 초점을 두고 있으며 무결성, 신뢰성 그리고 보안에 초점을 두며 IT 프로세스, IT 거버넌스, IT 성숙도의 3가지 모델로 구성되어 있다. 이 모델은 (0) Non-existent, (1) Initial/Ad Hoc, (2) Repeatable but Intuitive, (3) Defined Process, (4) Managed and Measurable, and (5) Optimized 의 6단계로 표현한다. 셋째, 조직의 프로젝트관리 성숙모델(Organizational Project Management Maturity Model : OPM3)이다. 이 모델은 PMI(Project Management Institute)에 의해 개발되었으며 PMBOK(Project Management Body of Knowledge)에 기반을 두고 있다. 이 모델은 전략이 성공적이고 일관성 있으며 예측 가능한 결과로 이어질 수 있도록 프로젝트, 프로그램, 포트폴리오의 3가지 도메인을 포함한다. Standardization, Measurement, Control and Continuous Improvement라는 4단계 성숙도와 관련되어 있다[18,19].

2.2 정보보호 성과에 관한 연구

정보보호 성과란 조직이 정보보호 관리 활동을 통해 얻을 수 있는 긍정적 결과이다. 다양한 이해당사자의 비즈니즈 목표와 가치를 생산하고 성취하는 정도를 조직성과로 정의한다. Hall[9]은 구체적 내용으로 고객으로부터 신뢰제고, 고객 등 이해당사자로부터 발생하는 고비용의 법적소송 방지, 브랜드 파워 또는 회사 평판에 대한 대중의 인지도 보호, 고객의 서비스 개선, 시장가치 유지, 지속적으로 변화하는 리스크 환경 속에서 비즈니스 복원력 확보라고 했다. 정보보호 효과를 리스크관리, 경제적, 법적, 문화적 관점으로 분류하고 원하지 않는 침해사고 감소, 투자로부터 기대 이익을 극대화, 법적 요구사항 위반에 대한 회피, 개인 및 조직의 인식과 행동 개선 효과가 있다[20]. 정보보호의 성과는 기회비용 성격이어서 정보자산보호가 잘 이루어지는 경우에는 손실이 발생하지 않고, 정보보호가 잘 이루어지지 않는 경우에만 손실이 발생하여 그 효과를 객관적으로 파악하는 데에는 한계가 있으므로 정보보호 성과를 금전적으로 측정하기에는 어려움이 있다[21].

조직구성원의 정보보호 행동과 조직의 정보보호 성과에 관한 연구에서 정보보호 사고 빈도 및 사고로 인한 손실 감소를 정보보호 성과로 측정하였다[22]. 다른 연구에서는 정보보호 성과를 정보자산보호 성과와 조직 성과로 구분하고 보안사고 감소 성과, 직원의 인식제고와 만족도 향상, 협력사간의 정보교류 신뢰도 향상, 개인 정보보호에 대한 고객 신뢰도 향상 등을 자산보호 성과에 포함하였고, 조직성과는 기술 및 서비스보호를 통한 자산손실 방지, 비즈니스 연속성 및 기회 성과, 이미지손실 방지에 따른 이미지 유지 성과, 고객유지 및 고객기반 확대 성과에 따른 매출증대 등을 포함하였다[23]. 정보자산 보호활동은 정보자산 보호성과에 긍정적인 영향을 미쳤으며, 정보자산 보호 성과 또한 조직의 본질적인 성과에 긍정적인 영향을 미치는 것으로 나타났다[23].

정보보호 성과를 보안사고 예방 및 손실방지와 같은 소극적인 것으로부터 경쟁우위, 공공이미지, 고객 만족과 같이 정보보호와 관련된 적극적인 것으로 구분할 수 있다. 다른 관점에서 보면 재무성과인 정보보호 사고에 의한 손실, 내부성과인 최고경영자의 인식제고와 보안조직의 직무만족, 조직 구성원의 정보보호 인식향상, 그리고 외부 성과인 협력사 및 공급사의 만족과 이미지 제고, 고객의 서비스 만족 등으로 정의할 수 있다[24].

2.3 정보보호 정책지표에 관한 연구

2014년 금융IT 정보보호동향 예측 분석에 따르면 전자금융의 보안 위협은 서비스와 직접적으로 관련이 없는 피싱, 파밍 공격 등을 통해 수집한 금융거래 정보로 부정거래를 유발하던 소극적인 방식에서 실제 전자금융거래 과정에 직접 개입하여 보다 정교한 방식으로 전자금융거래 정보를 실시간으로 수집·이용하는 적극적인 방식을 통해 금전적 이득을 취하려는 해킹 사고가 증가할 것으로 예측되어 앞으로 보안 투자와 대응 체계 방향은 알려지지 않은 공격과 기술뿐만 아니라 사람에 대한 투자에 중심을 두어야 한다고 했다[25].

Table 1. Delivery Channels for Banking Services

(단위 : %)

창구거래 (대면거래)	전자금융(비대면 거래)				합계
		CD/ATM	텔레뱅킹	인터넷뱅킹	
11.3	88.7	41.2	13.0	34.5	100.0

Source : Bank of Korea, 2014.5.

2014년 1분기 인터넷뱅킹 서비스 이용현황(한국은행, 2014.5)을 보면 스마트폰 기반 모바일 뱅킹 이용자가 4,034만 명을 기록하고 있으며, 하루 평균 이용건수와 거래금액은 2,737만 건, 1조 6,276억 원에 달하였다. 또한 인터넷뱅킹의 업무처리 비중이 꾸준히 상승하면서 Table 1과 같이 비대면 거래의 비중이 88.7%로 지속적으로 증가하고 있다. 이처럼 오늘날 금융환경은 은행이 태동하던 1950년대의 환경과는 비교 자체가 불가능할 정도로 다른 상황에 처해 있으며 금융거래에 있어 정보기술과 정보보호는 비즈니스를 지원하는 역할을 뛰어넘어 '비즈니스 그 자체'라고 할 수 있을 정도로 중요하다.

국내 금융회사의 정보보호 관련법의 핵심은 전자금융거래법과 전자금융감독규정, 금융회사 정보기술부문 보호업무 모범규준이다[26, 27, 28]. 금융당국은 경영진의 인식 전환과 정보기술 보안조직(인력・예산)의 실질적 역량 제고를 통한 금융보안 강화를 위해 지난 2011년 금융회사 정보기술부문 보호업무 모범규준 및 2013년 전자금융감독규정 제8조 제3항을 마련, 이른바 5・5・7 정책을 도입했다. 첫째, 총 임직원수의 100분의 5 이상을 정보기술부문 인력으로 확보하고, 둘째, 정보기술부문 인력의 100분의 5 이상을 정보보호 인력으로 확보하여야 한다. 셋째, 정보기술부문 예산의 100분의 7 이상을 정보보호 예산으로 확보하여야 한다.

'2013년 금융업권별 정보기술부문 보호업무 모범규준 이행실태 점검 결과 보고서'에 따르면 Table 2와 같이 4개 금융권역(권역별 평균 기준) 모두 3가지 정보보호 정책지표(정보기술부문 인력 비율, 정보보호 인력 비율, 정보보호 예산 비율)를 준수하고 있는 것으로 조사되었다.

Table 2. Current Fulfillment of Information Security in 2013

(단위 : %)

구분	정보기술부문 인력 비율	정보보호 인력 비율	정보보호 예산 비율
은행권역	5.6	6.1	9.3
증권권역	6.7	7.3	10.5
보험권역	6.3	6.7	10.2
카드권역	9.1	10.2	11.2

(Source : Financial Supervisory Service, 2014.2)

3. 연구모형 및 가설

3.1 연구모형의 설계

본 연구는 문헌연구를 통해 조사된 정보보호 활동의 조직성과를 종속변수로, 보안 위협으로부터 정보자산의 안전성을 확보할 수 있는 조직의 역량 수준 즉, 정보보호 관리 성숙도를 독립변수로, 정보보호 정책지표를 조절변수로 설정하여 이들 변수간의 인과관계를 분석하고자 Fig. 2의 연구모형을 설정하였다.

3.2 가설설정

본 연구에서는 연구모형에 포함된 독립변수(정보보호 관리 성숙도), 조절변수(정보보호 정책지표), 그리고 종속변수(조직성과) 간의 인과관계를 통계적으로 검증하기 위하여 선행연구를 바탕으로 다음과 같은 연구가설을 설정하였다.

H1 : 조직의 위험 관리 프로세스는 조직성과에 정(+)의 영향을 미칠 것이다.

H2 : 조직의 위험 평가 프로세스는 조직성과에 정(+)의 영향을 미칠 것이다.

H3 : 정보보호 인력 비율에 따라 위험 관리 프로세스가 조직성과에 미치는 영향은 달라질 것이다.

H4 : 정보보호 예산 비율에 따라 위험 관리 프로세스가 조직성과에 미치는 영향은 달라질 것이다.

H5 : 정보보호 인력 비율에 따라 위험 평가 프로세스가 조직성과에 미치는 영향은 달라질 것이다.

H6 : 정보보호 예산 비율에 따라 위험 평가 프로세스가 조직성과에 미치는 영향은 달라질 것이다.

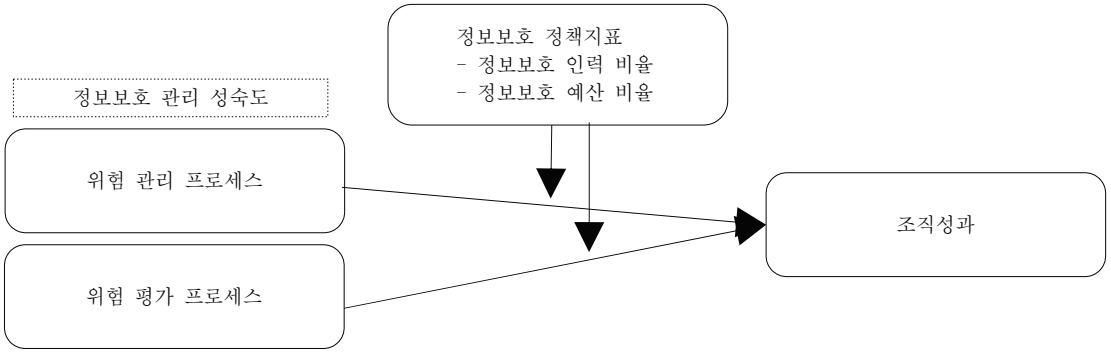


Fig. 2. Research Model

3.3 변수의 조작적 정의와 측정

본 연구에서는 독립변수로 위험 관리 프로세스 및 위험 평가 프로세스 기반의 정보보호 관리 성숙도, 종속변수로 조직성과를 그리고 조절변수로 정보보호 정책지표를 선정하였다. 사용된 설문항목은 리커트(Likert) 5점 척도를 사용하였다. 다음 Table 3은 사용된 연구변수에 대한 조작적 정의와 출처이다.

조작적 정의에 따른 연구변수의 측정을 위한 설문항목은 크게 3가지로 구성하였다. 첫째, 위험관리 프로세스 성숙도 수준 관련 설문이다. 위험관리 프로세스의 수준을 측정하기 위해 정보보호 의사소통, 정보보호 정책, 정보보호 추진계획, 정보보호 이행점검, 정보보호 교육, 정보보호 사고탐지 및 대응에 대해 설문을 하였다. 둘째, 위험평가 프로세스 성숙도 수준 관련 설문이다. 이를 측정하기 위해 위험평가 계획의 구체성, 위험평가의 내재화, 위험평가 절차의 문서화 등에 대해 설문을 실시하였다. 셋째, 정보보호 활동의 조직성과 관련 설문은 침해사고의 발생 감소, 조직 비즈니스의 복원력 확보, 신규 서비스 및 기술에 대한 투자효과 발생, 회사의 브랜드 파워 및 평판 유지, 모범사례 적용을 통한 서비스 품질 향상, 다양한 이해당사자로부터 제기되는 소송방지 등에 대해 설문을 실시하였다.

1) 정보보호 관리 성숙도

정보보호 관리 및 성숙도에 대한 선행 연구를 바탕으로 정보의 가용성, 접근성, 안전성을 확보하기 위한 선제적인 정보보호 관리가 필수적임을 알 수 있다. 이 정보보호 관리의 주요 구성 요소는 위험 관리와 위험 평가이다[5, 6].

본 연구에서 위험 관리 프로세스는 정보보호 정책 수립, 정보보호에 대한 구성원의 책임, 핵심시스템 관리, 공식화된 침해사고 대응절차 등을 측정한다. 위험 평가 프로세스는 위험 평가의 문서화, 평가 프로세스의 조직 내 내재화, 위험 평가 미 수행 시 발견 여부 등을 측정한다[5, 7].

2) 조직성과

정보보호 성과란 조직이 정보보호 관리 활동을 통해 얻을 수 있는 긍정적 결과로서 조직에게 중요한 가치를 제공한다. 본 연구에서는 선행 연구 조사를 통해 정보보호의 조직성과 측정을 위한 재무지표의 사용 및 측정이 용이하지 않다는 결과를 얻었으므로 정보보호 성과에 대한 Hagen의 4가지 관점을 채택하였으며[20], 그 관점에 속하는 세부항목은 문헌연구를 통해 구성하였다. 법적 관점의 성과로 (1) 법적 소송방지, 경제적 관점의 성과로 (1) 브랜드 파워 및 평판보호, (2) 신규서비스 및 기술의 투자효과, (3) 서비스 품질향상비즈니스, 리스크관리 관점의 성과로 (1) 침해사고 발생 감소, (2) 비즈니스 복원력 확보, 문화적 관점의 성과로 (1) 구성원의 인식 및 행동 개선을 채택하였다.

3) 정보보호 정책지표

진화하는 보안 위협으로부터 전자금융거래의 안전성을 확보하기 위해 국내 금융정책 당국은 컨트롤타워 역할 강화, 금융권 보안 거버넌스 확립, 내부통제 강화, 보안 취약요소 개선 등을 위한 정책을 수립하였다. 특히 경영진의 인식 전환과 정보기술 보안조직(인력・예산)의 실질적 역량 강화를 위한 정책을 2011년 10월부터 시행하고 있다. 본 연구에서는 조직의 정보보호 역량을 중시하여 정보보호 인력 비율과 정보보호 예산 비율을 정책지표로 선정하였다.

3.4 자료수집

본 연구의 설문은 국내 금융회사의 직원을 대상으로 하였다. 금융회사 업무는 일반 국민의 생활과 관련성이 높을 뿐 아니라 취급하는 정보의 민감성으로 인해 정보보호가 상대적으로 중요시 되는 분야이다. 금융회사에서 정보기술과 정보보호는 비즈니스를 지원하는 역할을 뛰어 넘어 '비즈니스 인프라'로서 중요하다. 설문기간은 2013년 11월 13일부터 12월 31일까지 실시되었으며 온라인 설문(docs.google.com) 및 우

Table 3. Operational Definition Variables

구분	연구변수	조작적 정의	출 처
독립변수	위험 관리 프로세스	위험과 관련하여 분석, 기획, 구현, 통제, 측정 및 시행된 보안 정책의 모니터링을 다루는 순환 활동	[2], [6], [7], [8]
독립변수	위험 평가 프로세스	위험 관리 프로세스 전체를 종단적인 시점에서 체계적으로 평가하는 일련의 활동	[2], [6], [7], [8]
종속변수	조직성과	정보보호 활동을 통해 얻을 수 있는 리스크관리, 경제적, 법적, 문화적 측면의 효과	[9], [20], [23], [24]
조절변수	정보보호 정책지표	정보기술부문 인력 대비 정보보호인력 비율	[27], [28]
		정보기술부문 예산 대비 정보보호예산 비율	

편을 이용하였다. 설문대상자는 조직에 속해 있는 조직구성원들이다. 연구조사를 위해 총 700부의 설문을 배포하여 185부를 회수하였으며(회수율 : 26.4%), 이중 응답이 지나치게 불성실한 11부를 제외한 174부가 분석에 사용되었다. 응답자의 소속 금융회사 권역은 금융유관기관(43.7%), 은행(29.3%), 보험회사(15.5%)의 비율이 높았으며, 응답자의 직급은 실무자(58.0%), 중간 관리자(36.2%), 상급 관리자(3.5%) 순으로 나타났다. 표본에 대한 일반적 특성은 다음 Table 4와 같다.

Table 4. Demographic Data

(단위 : 명, %)

구 분	내 용		응답자 수	비율(%)
소속	금융회사	은행	51	29.3
		증권사	11	6.3
		보험사	27	15.5
		카드사	9	5.2
		금융유관기관	76	43.7
담당업무	정보보호		112	64.4
	프로그램개발		11	6.3
	시스템 운영관리		17	9.8
	e-비즈니스		20	11.5
	기타		14	8.0
담당업무의 정보보호 관련 정도	직접적으로 관련		128	73.5
	간접적으로 관련		41	23.6
	관련성이 적음		5	2.9
직급	상급 관리자		6	3.5
	중간 관리자		63	36.2
	실무자		101	58.0
	기타		4	2.3
업무 수행기간	10년 이상		35	20.1
	5년~9년		28	16.1
	3년~5년		31	17.8
	3년 이하		80	46.0
조직규모	15,000명 이상		10	5.7
	10,000~14,999명		7	4.0
	1,000~9,999명		37	21.3
	500~999명		97	55.8
	100~499명		20	11.5
	100명 이하		3	1.7

4. 연구결과 분석

4.1 측정모형 분석

본 연구모형에서 제시된 측정모형은 조절변수를 제외한 3개의 잠재변수를 나타내는 15개의 관측변수(Observatory Variable)로 174개의 데이터를 이용하여 분석하였다. Lisrel v.8.72의 Simplis(Simple Lisrel)를 이용하였는데 분석된 통계자료의 해석은 배병렬의 저서와 Koufteros and Marcoulides의 논문을 참고하였다[29, 30].

잠재변수가 관측변수에 의해 설명되는 정도를 알아보기 위해 집중타당성(Convergent Validity) 분석을 실시하여 요인적재 값이 0.7 이상(R^2은 0.5 이상)인 측정항목을 포함하였다. 그 과정에서 위험 관리 프로세스 8개, 위험 평가 프로세스 4개, 조직성과 2개의 측정항목이 탈락하여 Table 5와 같이 제시되었다.

내적일관성은 합성 신뢰도(Composite Reliability)와 평균분산 추출(Average Variance Extraction) 값을 통하여 검증하였다. 일반적으로 각 0.7과 0.5 이상이면 신뢰도가 있는 것으로 보기 때문에 잠재변수의 측정항목은 모두 기준치를 만족한다[29].

잠재변수에 대한 상관행렬을 이용하여 구성개념 간의 상관관계를 분석하였다. 일반적으로 상관계수가 0.8을 초과하면 잠재변수 간에 다중공선성이 발생한다고 본다. Table 6에서 보는 바와 같이 조직성과, 정보보호 관리 프로세스, 정보보호 위험평가 프로세스 간의 상관계수 값이 0.8보다 작은 것으로 나타났으므로 잠재변수 간의 다중공선성은 문제되지 않는다고 판단하였다. 평균분산추출의 제곱근은 값이 적어도 0.7 이상이고(즉 평균분산추출의 값이 0.5 이상), 각 대각선에 있는 이 제곱근의 값($\sqrt{AVE}$)이 잠재변수 간의 상관계수 값을 상회하므로 판별 타당성(Discriminant Validity)의 기준을 만족한다[31].

독립변수와 종속변수를 동일한 측정도구와 응답원에 의해 측정하였을 경우에 발생하는 오류(Common Method Bias)를 검증하기 위해 탐색적 요인분석을 실시한 결과 고유값(Eigen Value)이 1 이상인 요인이 1개 이상 도출되었으며, 한 요인의 분산 설명력이 절대적이지 않은 것(50% 이하)으로 나타나 연구모형 내 변수 간 관계의 정도를 증가시키거나 감소시켜 연구결과를 왜곡하는 현상은 없었다.

4.2 구조모형 분석

가설검증에 앞서 분석한 구조모형의 적합도를 평가하였다. 모형의 전반적인 적합도를 나타내는 지표인 잔차평균자승이중근(Root Mean Square Residual : RMSR)은 0.05 이하, 근사오차평균자승(Root Mean Square Error of Approximation : RMSEA)은 0.01~0.10 구간이면 양호한 것으로 평가하는데 본 모형의 각 0.025과 0.070이므로 양호한 것으로 판단하였다. 기초모형에 대한 제안모형의 적합정도를 나타내는 지수인 표준적합지수(Normed Fit Index : NFI), 비표준 적합지수(NNFI : Non Normed Fit Index : NNFI), 비교 적합지수(Comparative Fit Index : CFI)는 역시 0.9 이상이면 좋은

Table 5. Results of Measurement Model Analysis

잠재변수	관측변수			합성신뢰도 (CR)	평균분산추출 (AVE)
	측정항목(내용)	요인적재	t 값		
위험 관리 프로세스	isml-1-6(정보보호 의사소통)	0.81	1	0.9154	0.6436
	isml-1-7(정보보호 정책)	0.77	11.32		
	isml-1-8(정보보호 추진계획)	0.85	12.89		
	isml-1-11(정보보호 이행점검)	0.77	11.30		
	isml-1-13(정보보호 교육)	0.78	11.48		
	isml-1-14(정보보호 사고 탐지 및 대응)	0.83	12.52		
위험 평가 프로세스	isml-2-1(위험평가계획의 구체성)	0.85	1	0.8974	0.6868
	isml-2-2(위험평가의 내재화)	0.86	14.11		
	isml-2-3(위험평가 절차의 문서화)	0.85	13.71		
	isml-2-4(위험평가절차 미준수시 처리)	0.75	11.44		
조직성과	per3(신규서비스 및 기술에 대한 투자효과)	0.74	1	0.8627	0.5572
	per4(기업의 브랜드 파워 및 평판 유지)	0.73	9.13		
	per5(모범사례 적용을 통한 서비스 품질향상)	0.77	9.73		
	per6(법적 소송방지)	0.71	8.98		
	per7(구성원의 인식 및 행동 개선)	0.78	9.83		

Table 6. Correlation Matrix among Latent Variables

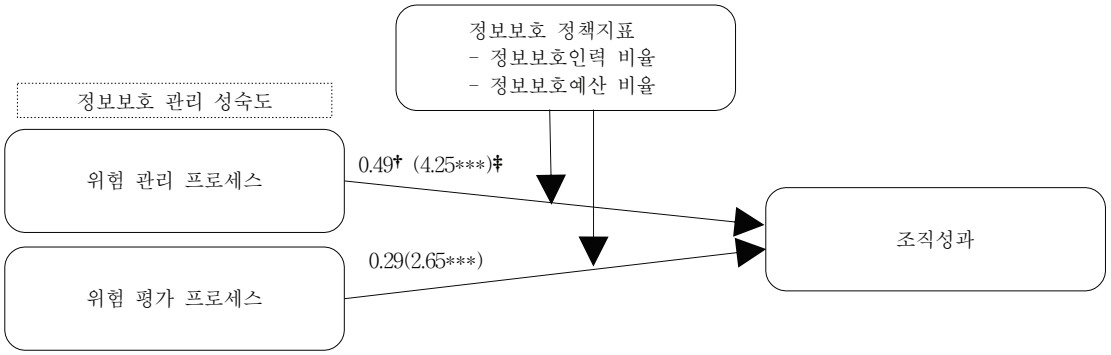
구분	조직성과	정보보호 관리 프로세스	정보보호 위험평가 프로세스
조직성과	0.74		
정보보호 관리 프로세스	0.71	0.80	
정보보호 위험평가 프로세스	0.66	0.75	0.82

* 대각선 음영친 부분은 평균분산추출(AVE)의 제곱근

적합도를 갖는 것으로 본다. 또한 표준 카이자승(Chi-Square)값은 카이자승(x^2)값을 자유도(df)로 나눈 값으로 일반적으로 x^2값이 자유도의 2배를 넘지 않으면 p값이 작아도 적합한 모형으로 평가한다. 분석결과 본 구조모형의 적합도(n=174, RMR=0.025, RMSEA=0.070, GFI=0.89, AGFI=0.85, NFI=0.97, NNFI=0.98, CFI=0.98, x^2/df=1.84(x^2=160.41, df=87))는 전반적으로 양호한 것으로 분석되었다.

본 연구의 가설검정은 잠재변수 간의 인과관계를 나타내는 각 경로로 Fig. 3과 같다. 인과관계를 분석할 때 가설의 방향성이 제시되었으므로 단측 검정을 사용하였으며 t값은 유의수준 α=0.05를 기준으로 |t|값이 1.645 이상인 값을 가설 채택의 기준으로 사용하였다. 아래 공변량 구조모형의 분석결과에서 보듯이 정보보호 관리 성숙도를 나타내는 위험 관리 프로세스, 위험 평가 프로세스는 조직성과에 유의한 영향을 미치는 것으로 나타났다.

정보보호 정책지표의 조절효과를 분석한 결과 Table 7과 같이 자유 모형과 등가제약 모형의 x^2의 차이(정책지표가



n=174, RMR=0.025, RMSEA=0.070, GFI=0.89,AGFI=0.85, NFI=0.97, NNFI=0.98, CFI=0.98, x^2/df=1.84(x^2=160.41, df=87)
† : 표준경로계수, ‡ : t값(*: 0.05, **: 0.01, ***: 0.001)

Fig. 3. Path Analysis Results

Table 7. Result of Testing Interaction Effects

정책지표(중위값)	높은 그룹	낮은 그룹	조절효과 ($\Delta x^2 < 3.84$)
1. 정보보호 인력 비율(7.5%)	7.7% 이상 (N=33)	7.3% 이하 (N=86)	1) 위험 관리 프로세스: 없음(Δx^2= 342.46 - 340.22) 2) 위험 평가 프로세스: 없음(Δx^2= 340.28 - 340.22)
2. 정보보호 예산 비율(10.3%)	10.5% 이상 (N=37)	10.2% 이하 (N=82)	1) 위험 관리 프로세스: 없음(Δx^2= 406.73 - 405.30) 2) 위험 평가 프로세스: 없음(Δx^2= 406.11 - 405.30)

Table 8. Result of Hypotheses Tests

가 설		결 과	비 고
H1	위험 관리 프로세스는 조직성과에 정(+)의 영향을 미칠 것이다.	채택	독립변수와 종속변수 간의 관계
H2	위험 평가 프로세스는 조직성과에 정(+)의 영향을 미칠 것이다.	채택	
H3	정보보호인력 비율에 따라 위험 관리 프로세스가 조직성과에 미치는 영향은 달라질 것이다.	기각	독립변수와 종속변수 간 조절효과
H4	정보보호예산 비율에 따라 위험 관리 프로세스가 조직성과에 미치는 영향은 달라질 것이다.	기각	
H5	정보보호인력 비율에 따라 위험 평가 프로세스가 조직성과에 미치는 영향은 달라질 것이다.	기각	
H6	정보보호예산 비율에 따라 위험 평가 프로세스가 조직성과에 미치는 영향은 달라질 것이다.	기각	

큰 그룹의 x^2 값에서 정책지표가 작은 그룹의 x^2 값을 뺀 수치)가 3.84(자유도가 1일 경우에 임계값)보다 작아 조절효과가 없는 것으로 나타났다[30].

4.3 결과의 해석

구조모형 분석을 통해 확인된 가설의 채택여부는 위의 Table 8과 같다. 정보보호 관리의 성숙도가 조직성과에 미치는 영향은 선행연구와 동일하지만[4, 9] 정보보호 인력 및 예산의 조절효과가 나타나지 않는 것은 특이한 결과이고 이에 대한 조심스러운 해석이 요구된다.

1) 정보보호 관리 성숙도와 조직성과

정보보호 관리 성숙도와 조직성과 간의 관계를 분석한 결과 인과 관계가 있는 것으로 나타났다(위험 관리 프로세스: 0.49(|t|=4.25, p<0.001, 위험 평가 프로세스 : 0.29(|t|=2.65, p<0.001). 본 연구 결과는 위험에 대한 순환 활동인 위험 관리 프로세스의 수준과 특정 시점에서 실시하는 위험 평가 프로세스의 수준은 비즈니스 복원력 확보, 브랜드 파워 및 평판 보호, 법적 소송방지 등 조직성과에 영향을 미치며 장기적으로 조직 경쟁력에까지 영향을 미칠 수 있다는 것을 시사한다.

2) 정보보호 정책지표와 조직성과

정보보호 인력 및 정보보호 예산 비율은 정보보호 관리 성숙도와 조직성과 간의 조절효과가 없는 것으로 나타났다. 대부분의 금융회사가 이를 준수하고 있음에도 불구하고 끊임없이 대형 보안사고 발생하고 있는 현실에서 보듯이 제시된 정책지표가 금융회사의 보안사고 예방 등 보안 수준 향상을 견인하지 못하고 있다. 정보보호인력의 산정기준이 관대한 점, 정보보호예산의 확보비율과 집행비율의 현격한 차이 발생과 이행실태에 대한 느슨한 점검이 정책 운용상의 이유로 보이지만, 상기 정보보호 정책지표는 개별 금융회사의 특성이 반영되지 않은 일률적 타율규제로 인식하여 조직의 보안수준 향상의 계기로 활용하지 못하고 단순히 제재 또는 책임을 경감받기 위한 방편으로 이용하는 경향이 보다 근본적인 원인으로 생각된다. 앞으로 정보보호 정책은 금융회사가 스스로 능동적 보안강화 노력을 통하여 서비스의 경쟁력 확보와 보안성 강화를 함께 달성할 수 있도록 유도하는 자율규제로의 패러다임 전환이 필요한 것으로 보인다.

5. 결론 및 한계

본 연구는 정보보호 관리 성숙도가 조직성과에 미치는 영향을 분석하기 위하여 문헌 조사를 통해 조직성과, 위험관리 프로세스 성숙도, 위험평가 프로세스 성숙도, 그리고 정보보호 정책지표를 이용한 연구모형을 만들고 설문을 통한 실증 분석을 실시하였다. 본 연구의 결과를 요약하면 다음과 같다. 첫째, 정보보호 관리 성숙도와 조직성과 간에는 높은 인과 관계가 있다. 특히 정보보호 관리의 주요 구성요소인 위험 관리 프로세스 및 위험 평가 프로세스의 성숙도가 조직성과에 영향을 미친다는 연구결과를 얻었다. 정보보호 문제를 조직 경영 차원의 문제로 인식하고 정보보호 관리에 지속적인 관심과 의지를 가져야 함을 의미한다.

둘째, 정보보호 정책지표(정보보호 인력 비율, 정보보호 예산 비율)에 따라 정보보호 관리 성숙도가 조직성과에 미치는 영향은 차이가 없는 것으로 나타났다. 실효성이 검증되지 않은 정보보호 정책 및 규제는 조직성과에 영향을 미치는 정보보호 관리 성숙도 향상의 촉매제로 활용하는 데 한계가 있으니 앞으로 조직은 정보보호 수준 향상을 위해 최소한의 규제 준수 노력에서 벗어나 자율적 보안체계 수립에 노력을 경주해야 할 것으로 보인다.

본 연구의 한계점은 첫째, 본 연구에서 선정한 표본이 제한된 산업분야에서 선정되었기 때문에 결과에 대한 일반화가 다소 제한적일 수 있다. 향후에는 다양한 산업군과 기업규모 등을 고려하여 표본을 폭 넓게 선정하면 의미 있는 연구가 될 수 있을 것이다. 둘째, 조직성과를 비재무적 요소들만을 측정요소 선택하였기 때문에 한계가 있을 수 있다. 향후에는 재무적 성과를 포함하여 정보보호의 조직성과를 객관적이며 종합적으로 평가할 수 있는 다양한 관점의 성과 측정방법에 대한 연구와 적용이 필요할 것이다.

References

[1] Suhazimah Dzazali and Ali Hussein Zolait, “Assessment of information security maturity: An exploration study of Malaysian public service organizations”, Journal of Systems and Information Technology, Vol.14, Issue.1, pp.23-57, 2013.

[2] ISO/IEC 27001-2005(E), “Information Technology-Security Techniques-Information Security Management Systems-Requirements”, 2005.

[3] M. Simonsson, P. Johnson, and M. Ekstedt, “The effect of IT governance maturity on IT governance performance”, Information Systems Management, Vol.27, pp.10-24, 2010.

[4] NIST SP 800-39, “Managing Information Security Risk: Organization, Mission and Information System View”, available at http://csrc.nist.gov/publications, 2011.

[5] ISO/IEC TR 13335-2, “Information technology -Guidelines for the management of IT Security- Part 2 : Managing and planning IT Security”, 1997.

[6] NIST SP 800-30, “Guide for Conducting Risk Assessment”, available at http://csrc.nist.gov/publications/, 2012.

[7] ENISA(European Network and Information Security Agency), “Regulation No 460/2004 of the european parliament and of the council”, 2004.

[8] OCTAVE, “Method Implementation Guide Version 2.0”, Carnegie Mellon University, 2001.

[9] J. H. Hall, S. Sarkani, and T. A. Mazzuchi, “Impacts of organizational capabilities in information security”, Information Management & Computer Security”, Vol.19, Issue.3, pp.155-176, 2011.

[10] J. Jenkins, “Organisational IT security theory and practices: and never the twain shall meet?”, available at www.sans.org/rr/securitybasics/ITsec2.php, 2003.

[11] R. Sommer, “How to buy information security”, available at www.virtualcity.co.uk.hottobuy.htm, 2003.

[12] R. Baskerville, “Designing Information System Security”, Wiley, Chichester, 1998.

[13] B. Schneier, “Secret and Lies-Digital Security in a Networked World”, Wiley Computer Publishing, New York, NY, 2002.

[14] S. Berinato, “After the storm, reform”, CIO Magazine, available at www.cio.com/archive/121503/securityfuture.html, 2003.

[15] K. N. Bhaskar, “Computer Security: Threat and Countermeasures”, NCC-Blackwell, Oxford, 1993.

[16] M. B. Chrissis, M. Konrad, and S. Shrum, “CMMI- Guidelines for Process Integration and Product Improvement”, United States : SEI, 2005.

[17] IT Governance Institute (ITGI), “Cobit 4.1”, Estados Unidos: ITGI, 2007.

[18] Project Management Institute (PMI), “PMI Fact Sheet”, USA: PMI, 2006.

[19] Project Management Institute (PMI), “A guide to the project management body of knowledge (PMBOK Guide)”, Upper Darby, PA, 2000.

[20] J. M. Hagen, E. Albrechtsen, and J. Hovden, “Implementation and effectiveness of organizational information security measures”, Information Management & Computer Security, Vol.16, Issue.4, pp.377-397, 2008.

[21] S. Smith, G. Stephen, and W. Malampy, “A financial Management Approach for Selecting Optimal, Cost-Effective Safeguards Upgrades for Computer and Information Security Risk Management.” Computer and Security, Vol.14, No.1, pp.28-29, 1995.

[22] M. J. Baek and S. H. Shon, “A Study on information security awareness and behavior affecting information security effectiveness in smaller member organization”, Small Business Research, Vol.33, No.2, pp.113-132, 2011.

[23] K. K. Kim, H. K. Shin, S. S. Park, and B.S. Kim, “A Study on impact information assets protection accomplish affecting organizational performance”, Information Management Research, Vol.40, No.3, pp.61-77, 2009.

[24] G. H. Hong, “A Study on Impact on Information Security control and activities affecting information security performance”, a doctoral thesis department of Kookmin University Graduate School, Information management department, 2003.

[25] Korea Financial Telecommunications & Clearings Institute, “The financial IT and information security trend prediction”, Payment and information technology, No.55 pp.90-126, 2014.
[27] Financial Supervisory Commission, “Electronic financial supervisory regulation”, 2014.
[28] Financial Supervisory Commission, “The financial institutions information technology security duties standard”, 2012.
[29] B. B. Yeol, “Structural equation model for understanding and use”, Publishing Daegyeong, 2006.
[30] X. Koufteros and G. Marcoulides, “Product development Practices and performance: A structural equation modeling-based multi-group analysis”, International Journal of Production Economics, pp.286-307, 2006.
[31] C. Fornell and D. Larcker, “Evaluating structural equation models with unobservable variables and measurement error”, Journal of Marketing Research, pp.39-50, 1981.

박 정 국
e-mail : arspark@kftc.or.kr
1991년 한양대학교 경제학(학사)
2003년 동국대학교 정보보호학(석사)
2011년~현 재 동국대학교 경영정보학과 박사과정
현 재 금융결제원 금융결제연구소 팀장
관심분야 : 전자금융보안, 정보보호 관리체계

김 인 재
e-mail : ijkim@dongguk.edu
1983년 서울대학교 산업공학(학사)
1985년 KAIST 경영과학(석사)
1996년 U. of Nebraska, Lincoln(박사)
1985~1991 LG전자 중앙연구소 연구원
현 재 동국대학교 경영학부 교수
관심분야 : 정보정책, 정보보안, SW품질