「정보시스템연구」 제23권 제3호
한국정보시스템학회
2014년 9월, pp. 99~125

http://dx.doi.org/10.5859/KAIS.2014.23.3.99

조직성과에 미치는 영향요인에 관한 연구:
정보보호 성숙도의 매개효과를 중심으로

박정국* · 김인재**

<목 차>

Ⅰ. 서 론

정보보호는 오늘날 조직의 정보자산을 안전하게 지키는 방법으로서 뿐만 아니라 글로벌 경제, 지속적으로 변화하는 기업의 위기관리, 비즈니스 환경에서 성공을 위한 IT의 경쟁력을 이루는 핵심적인 요소이며 조직 생존을 위한 필수 요소로 인식되고 있다.

따라서 최근 정보보호에 대한 투자와 비즈니스 성공을 위한 정보보호의 전략적 역할이 증대되고 있으나, 정보보호의 효과적 구현은 여전히 조직들이 직면하고 있는 큰 도전 요인이 되고 있다(Hall et al,2011). 이러한 도전은 정보보호 수준 향상을 통하여 보안사고 예방 등 조직의 정보보호 관련 위험을 경감시키고 나아가 조직의 미션, 비즈니스 목표를 달성할 수 있도록 하는 효과적인 정보보호 활동을 통해 극복될 수 있다(NIST SP 800-33,2001).

정보보호가 복합적이면서 동적이고 다면적인 특징을 가지고 있음에도 불구하고, 지금까지 조직관점에서 많은 연구들이 정보 및 정보시스템을 보호하는 방법으로 암호화, 접근 제어, 침입 탐지, 악성코드 보안 등 주로 기술적 관점에서 논의되어 왔다. 정보보호 이슈를 다룰 때에는 종합적이고 다학제적인 사고가 필요하므로

* 동국대학교-서울캠퍼스 대학원 경영정보학과, 주저자, arspark@kftc.or.kr
** 동국대학교-서울캠퍼스 경영대학 경영학부, 교신저자, ijkim@dongguk.edu

(Yngström,1996; Kowalski,1994), 정보보호의 효과적 구현 전략 제시를 위하여 조직의 정보보호 성숙도에 미치는 영향요인에 대한 포괄적인 탐색과 그 영향요인과 조직성과 간의 관계를 포함한 연구는 반드시 필요하다고 할 수 있다.

본 연구는 선행연구를 바탕으로 각 개인이 느끼는 정보보호 성숙도 수준의 매개적 역할을 실증하고자 하였다. 즉 개인적, 조직적, 기술적, 사회적 측면의 관련 요인들 중에서 어떤 요인이 각 개인이 느끼는 정보보호 성숙도 정도에 더 많은 영향을 주는지, 그리고 정보보호의 성숙도 수준과 조직성과 간에는 어떠한 인과관계가 있는지를 규명하고자 하였다. 본 연구의 결과는 실무현장에서 조직의 정보보호 수준 제고를 위한 정책방향을 제시하고, 정보보호 담당자의 관리역량을 높일 수 있으며, 마지막으로는 효과적인 정보보안 투자 및 의사결정에 기여할 수 있을 것으로 기대된다.

Ⅱ. 이론적 배경과 연구모형

2.1 정보보호 영향요인에 관한 연구

Solms(1997)는 정보통신망 환경을 보호하는데 있어서 항상 기술적 보호 메카니즘이 중요한 역할을 한다고 하였다. Schneier(2002)는 정보보호란 단순히 기술의 문제라기보다는 조직, 개인, 사회적 요소로 구성된 사회적 시스템이라고 하였다. “정보보호는 프로세스이지 결코 제품이 아니다”라고 말하면서 그간 정보보호 분야를 지배하고 있는 기술 중심적 인식을 지적하고, 그 프로세스는 실제 위협을 이해하고 처음부터 적절한 조치와 위협에 대응하는 보안정책을 만드는 것을 포함한다고 했다.

Solms and Solms(2004)는 정보보호는 조직의 미션, 목표를 포함하는 전략적 동인의 맥락 속에서 수립되고 해결되어야 하는 비즈니스 또는 조직적 차원의 문제라고 하였다. 어떤 정보에 대한 보호는 비즈니스 이슈이지 기술적인 이슈가 아니라는 사실을 조직은 깨달아야 한다. 정보보호 관리는 정보자산의 안전한 환경 확보를 위해 기업 거버넌스, 조직, 정책, 모범사례, 윤리적 컴플라이언스, 인식, 그리고 기술, 측정, 감사 등 다차원적이고 복합적인 요인을 고려하여야 한다.

Beznosov and Beznosova(2007)는 컴퓨터 보안 분야에서 공격자와 방어자 간의 관계를 하나의 게임으로 정의하고 기술적, 인적, 사회적 3가지 차원의 현상으로 설명했다. Werlinger et al(2009)는 조직 내 정보보호 관리상의 도전요인 18가지를 기술적, 인적, 조직적 관점에서 설명했다. 정보보호 전문가가 조직 내에서 직면해야 하는 사람, 조직, 기술적 측면의 요인을 제시함과 동시에 이들 요인 간의 상호 작용을 연구하였다. Dzazali(2012)는 조직의 정보보호 성숙도에 미치는 영향요인을 크게 기술적, 사회적으로 구분하고 그 요인간의 관계를 규명하기 위해 실증연구를 실시하였다. 이 연구는 실증적인 통찰을 제공하고 사회적 요인과 기술적 요인에 대한 여러 가지 중요한 차원을 보여준다. 연구결과 사회적 요인이 조직의 정보보호 성숙도에 많은 영향을 주는 것으로 연구되었으며, 또한 위험관리와 개인인식이라는 두 요인이 정보보호 성숙도가 낮은 조직과 높은 조직을 구

별하는 요인으로 나타났다.

Yngström(1996)의 시스템 총괄모형(Systemic-Holistic Model)과 Bostrom and Heinen(1977)와 Trist(1981)의 사회기술시스템 이론(Socio-Technical Systems Theory)은 정보보호 이슈를 다룰 때에는 종합적이고 다학제적 사고가 필요하다고 강조한다. 왜냐하면 완벽한 보안이 바람직하고 추구되어야 할 목표이지만 현실적으로 달성하기 어려운 목표이기 때문이다. Kowalski(1994)는 기술적 서브시스템과 사회적 서브시스템간의 상호작용을 제시하였는데 이는 정보보호 영향요인을 연구하는데 유용한 아이디어를 제공한다. 문헌연구를 통해서 정보보호의 영향요인과 관련한 주요 연구들은 기술적, 조직적, 개인적, 사회적 관점에서 요인들을 다루고 있는 것을 확인할 수 있다.

2.1.1 개인적 관점의 영향요인

개인관점의 영향요인은 기존의 문헌연구에 따르면 정보보호에 대한 인식 및 문화, 개인혁신성, 훈련 또는 교육, 정보보호 이슈에 대한 커뮤니케이션 역량 등이 있다. 사회과학, 심리학, 의학, 그리고 정보시스템 분야에서 널리 사용되고 있는 개념인 인식은 각 개인의 자각으로 정의될 수 있으며 정해진 이슈에 대한 관심이 증가하는 것으로 의식의 주요 구성요소 중 하나로 간주되는 개념이다. 정보보호 인식은 이슈에 대한 개인의 관심정도로 정보보호에 대한 자각 및 정보보호 활동에 대한 관심 정도라 할 수 있다(Choi et al.,2008). 또 다른 연구에서는 조직 구성원의 정보보호에 대한 일반적 지식과 조직의 정보보호 정책에 대한 인식 정도라고 정의하였다(Bulgurcu and Cavusoglu,2009). 임채호(2006)는 정보보호 인식을 사람들이 자신의 직무를 수행하는데 있어 정보보호의 함축된 상태를 잘 알 수 있도록 하는 프로세스로 여기에는 정보보호의 중요성, 보안사고가 발생할 때 이에 대한 대응방안과 보고체계 등이 포함된다고 하였다. 조직문화란 한 조직의 구성원이 어떤 일을 함에 있어서 구성원이 공유하고 있는 신념, 가치관 또는 체계라고 할 수 있을 것이다. 2013년 ISACA(Information Systems Audit and Control Association)는 “Creating a Culture of Security”에서 조직이나 기업 문화에 정보보안 개념의 내재화 필요성을 강조하면서 “보안문화는 보안지침 이상이다”라고 하였다. 전사적 차원에서 구성원의 보안 인식 증진과 기업 보안 활동에 대한 참여도 제고를 통하여 행동을 변화시키고 나아가 회사의 장기적인 보안 전략과 비전을 이해하도록 하는 정보보호 인식 및 문화 프로그램의 운영이 중요하다고 할 수 있다.

개인혁신성은 사회시스템 내에서 개인이 다른 구성원보다 혁신을 상대적으로 빨리 수용하는 정도를 의미하는 것으로 다른 사람의 조언이나 도움 없이 기꺼이 새로운 제품을 수용하려는 정도를 나타낸다(Rogers,2003; Midgley and Dowling,1978). Midgley and Dowling (1978)은 개인이 새로운 것을 얼마나 쉽고 빠르게 수용하는가를 의미한다고 개인혁신성을 정의하였고, Goldsmith and Hofacker(1991)는 새로운 것을 시도하고자 하는 의지의 정도로 정의하고 있다. 정보기술 분야에서 개인혁신성은 새로운 정보기술에 대한 개인의 인식 뿐만 아니라 사용의도에 까지 유의미한 영향을 미치는 것으로 연구 되었다(Agarwal and Prasad,1998). 김상현 외(2012) 연구는 개인혁신성이 프라이

버시 염려 감소와 위치기반서비스 사용의도 간의 관계를 더 강화시키는 경우를 보여주었다.

2.1.2 조직적 관점의 영향요인

조직적 관점의 영향요인은 기존의 문헌연구에 따르면 조직의 구조, 비즈니스 담당자의 IT 역량, 최고경영층의 지원, IT관리가 있다. 조직구조는 조직 내 도입된 정보보호관리 체계에서 책임과 의사소통 구조를 반영하는 지표들에 의해서 정의된다. 이상적으로, 정보보호 목표를 지원하는 조직구조는 유연해야 하고, 사용자 및 경영층의 자유로운 참여와 지원을 허용해야 한다. 가장 중요한 것은 정보보호를 조직에서 중요한 기능이라고 깨닫는 것이다(Dzazali and Zolait, 2012). Solms and Solms(2004)는 조직구조 속에 내재화된 책임성과 추적성은 정보보호 관리의 성공에 있어 결정적인 역할을 한다고 강조하였다.

IT역량은 비즈니스 관리자가 보유한 IT관련 지식 및 경험의 일체로 정의할 수 있으며(Bassellier et al.,2003), 이는 사람에게 내재된 지식, 스킬 및 기술시스템에 내장된 무형의 어떤 것으로 구성된다(Bassellier et al.,2001). IT 자원과 함께 관리자의 정보보호 지식은 정보보호 관리에 영향을 주는 핵심 요인임을 밝혀냈다. 만약 비즈니스 관리자들이 IT에 더 많은 지식을 가진다면 정보보호 활동에 자극을 주며 도움이 될 것이다. 비즈니스 관리자가 IT를 매우 깊게 이해할 필요는 없으나 IT가 어떻게 조직에게 가치를 제공하는지 그리고 IT 한계는 무엇인지를 알아야 한다(Alshawa et al., 2005) 고 하였다.

조직의 정보보호수준 향상에 필요한 많은 요인이 존재하지만 최고 경영자의 적극적인 지원은 새로운 기술과 제도의 도입 또는 좋은 정책 개발의 성공 여부를 예측할 수 있는 척도이다. 또한 최고경영층의 정보보호에 대한 관심은 조직 내에서 정보보호 부서와 타 부서간의 협조를 증진시켜 줄 것이다(NIST SP 800-100,2007; Kankanhalli et al,2003). 국내에서 발표된 연구에 따르면 최고경영층의 지원은 조직의 정보보호정책 성숙도에 영향을 미치는 가장 중요한 요인이라고 실증하였다(최명길 외 2인, 2009).

IT관리는 비즈니스와 IT의 전략적 통합이라는 전제 아래 기업의 운영 탁월성을 확보하는 것이라 정의할 수 있다. 정보보호 관점에서 IT 관리 책임의 분산은 보안 통제수단을 적용함에 있어 조직역량의 저하를 가져올 수 있으며 다른 외부 조직과의 상호작용 시에도 이에 따른 문제가 발생할 수 있다. 또한 조직 내 정보시스템의 복잡성, 보안 이슈의 소통 관점에서도 부정적 영향을 줄 수 있다(Werlinger et al.,2009).

2.1.3 기술적 관점의 영향요인

기술적 관점의 영향요인은 기존의 문헌연구에 따르면 취약점 분석·평가, 침해행위 대응 활동이 있다. 취약점 분석·평가란 악성코드 유포, 해킹 등 사이버 위협에 대한 정보 및 정보시스템의 취약점을 종합적으로 분석, 평가, 개선하는 일련의 과정이다(NIST SP 800-30,2012; 행정안전부,2012). 이 활동은 크게 평가 준비, 평가 수행, 평가 결과 공유, 평가 유지활동 단계로 구분된다. 특히 평가 수행단계는 세부적으로 보안위협이 되는 원천과 이벤트에 대한 식별, 취약점과 이를 유발하는 요인에 대한 식별, 사고발생의 가능성 평가, 사고 영향의 정도 평가,

마지막으로 위험에 대한 결정을 하는 단계로 수행된다(NIST SP 800-30,2012).

침해행위 대응이다. 컴퓨터 보안사고는 컴퓨터 보안정책, 허용되는 이용정책, 표준 보안관행에 대한 위반 또는 임박한 위협이다. 이러한 보안사고가 발생하였거나 발생할 징후가 인지되었을 때 신속하고 효율적으로 대응하는 활동이다(NIST SP 800-61 ,2007). 침해행위 대응 프로세스는 몇 개의 주요 단계(준비, 탐지 및 분석, 격리, 제거 및 복구, 사후 관리)를 가지고 있다. 침해행위 대응능력을 확보함으로서 얻는 이점은 사고처리 방법론 준수를 통하여 침해사고에 대한 조치가 일관성 있게 체계적으로 수행된다는 것이다. 그리고 담당자가 사건에 의해 야기된 정보의 손실 또는 절취, 서비스 중단을 최소화할 수 있도록 돕는다. 또 다른 혜택은 사고대응기간 획득한 정보의 처리 시 더 강한 보호를 제공하며 사고기간 동안 발생할 수 있는 법적 이슈를 적절하게 다룰 수 있도록 도와준다.

2.1.4 사회적 관점의 영향요인

사회적 관점의 영향요인은 기존의 문헌연구에 따르면 정보보호 컴플라이언스, 환경 불확실성이 있다. 컴플라이언스는 일반적으로 공식적인 의무사항에 대한 준수 그리고 합법성을 유지하기 위해 조직에게 요구되는 것으로 정의할 수 있다(Tashi,2009). 오늘날 기업이 정보보호 관련 법률, 규정 등을 위반하여 발생되는 컴플라이언스 위험에 적극적으로 대처하지 못할 경우 기업의 생존과 직결되는 중대한 결과를 초래할 수 있다. 기업의 비즈니스 연속성을 보장하는데 정보보호 컴플라이언스는 선택이 아닌 필수 사항으로 반드시 해결해야 하는 과제로 인식하게 되었다(금융 IT 보안컴플라이언스, 2011; Tashi, 2009; Alder, 2006; ISO / IEC27001, 2005).

환경 불확실성은 기술의 급격화 변화, 경쟁자의 행동, 고객의 보안 요구사항, 제도의 변경에 의해 야기되는 것으로 정의할 수 있다(Chang et al,2006). 급속히 확산되는 기술은 다양한 유형의 사용자를 발생시키고 종전에는 안전했던 정보에 취약점을 유입시킬 뿐 아니라, 위협에 대응할 수 있도록 보안시스템을 지속적으로 진화하게 한다. 그것은 보안시스템 자체를 새로운 환경에 끊임없이 변화하게 한다. 정교함과 여러 가지 동기를 가진 플레이어의 수가 증가하기 때문에 외부로부터의 불확실성은 정보보호 관리의 필요성에 영향을 미치는 중요한 요인 중의 하나이다(Doddrell,1996).

<표 1> 정보보호 영향요인 관련 문헌연구

관점	영향요인	연구결과	출처
개인적	개인혁신성	개인혁신성은 프라이버시 염려 감소와 위치기반 서비스 사용의도에 유의한 영향을 미침	김상현 외(2012)
개인적	정보보안 인식, 정보보안 행동	개인의 인식이 행동 그리고 정보보안 성과에 영향을 미침	백민정,손승희(2011)
개인적, 조직적	경영층의 지원,정보보호와 대국민 서비스 및 신뢰성, 구성원의 정보보호 인식 및 문화	최고경영층의 지원 요인이 공공기관의 정보보호 거버 넌스 수준에 영향을 미침	송정석 외(2011)

관점	영향요인	연구결과	출처
개인적, 조직적, 기술적	훈련 또는 경험, 조직문화, 보안이슈에 대한 소통, 조직규모, 최고경영층 지원, 위험산정, 시스템 복잡성	정보보호 관리상 필요한 18가지 요인 식별함	Werlinger et al(2009)
개인적, 조직적, 사회적	사람, 프로세스, 비즈니스 목표	암호학이 완벽한 보안을 보장하지는 않음. 보안은 컴퓨터가 아니라 사람이 하는 것이고, 예방 못지 않게 탐지와 대응이 중요하다고 강조	Schneier(2002)
개인적	개인혁신성	개인 혁신성은 기술수용모델을 넓게 확장하는데 이용가능	Agarwal and Prasad (1998)
조직적	정책과 조직 및 기술의 조화, 조직성과개선에 대한 인식, 최고경영층 지원, 정책수립 및 이행에 대한 인식	정보보호정책과 조직과의 조화, 정보보호정책이 가져올 이익에 대한 기대가 정보보호정책 성숙도에 영향을 미침	최명길 외(2008)
조직적	IT역량, 환경 불확실성, 조직규모, 업종	좌측의 4가지가 정보보호 관리의 영향요인임을 밝힘	Chang et al(2006)
조직적	최고경영층지원, 보안문화,정책시행	최고경영층의 지원이 조직문화 및 정책 집행 수준에 영향을 미침	Knapp et al(2006)
조직적, 사회적	조직 거버넌스, 복합적 속성, 위험 식별, 국제적 모범사례, 정보보호정책의 중요성, 규제준수 등	적절한 정보보호 프로그램 을 만드는 것은 기본적이며어려운 일이 아님	Solms and Solms(2004)
조직적	조직규모, 최고경영층지원, 업종	좌측의 3가지가 정보보안 효과의 영향요인임	Kankanhalli et al(2003)
사회적, 기술적	위험관리메카니즘, 조직구조, 개인인식, 인식 및 훈련문화, 사회적 또는 기술적 장애물	기술적요인(위험관리 메카니즘), 사회적 요인 순으로 정보보호 성숙도에 영향을 미침	Dzazali(2012)
사회적	규제준수, 정보보호 보증	규제준수는 규제위반 벌금 ,브랜드와 소비자의 신뢰 손상으로부터 조직보호	Tashi(2009)
사회적, 기술적, 인적	사람, 기술, 사회	공격자-방어자간의 경쟁을 기술적 뿐만 아니라 인적, 사회적 관점 고찰필요	Beznosov and Beznosova(2007)
사회적, 기술적	윤리적,정치적,법적,운영관리적,기술적IT보안요인	정보보호 이슈를 다룰때 통합적, 다학제적인 사고 필요	Kowalski(1994)
사회적, 기술적	사람, 기술, 보상	인간과 기술의 결합에 의한 최적화를 통하여 성과 극대화	Trist(1981)
사회적, 기술적	기술적체계-프로세스,업무,기술사회적체계-인간특성,인간간의 관계성,보상체계,권한구조	업무체계 설계시 기술중심적 관점 외에 사회적 관점의 고려 필요	Bostrom & Heinen(1977)
기술적, 비기술적	기술 및 비기술적 측면, 시스템이 작동되는 환경	설계, 구현 레벨에서 시스템 안전성을 세부적으로 고찰	Yngström(1996)

2.2 정보보호 성숙도에 관한 연구

정보보호 분야 연구에서 사용되고 있는 정보보호 성숙도는 보안 위협으로부터 안전성을 확보할 수 있는 조직의 역량 수준(Siponen,2002), 조직의 정보보호프로그램이 내·외부 보안위협으로부터 정보 및 정보시스템을 보호하고 지키는 정도(Hall et al., 2011), 조직 내에서 정보보호의 역할, 비즈니스 기획 시 정보보호의 통합 정도, 정보보호에 대한 종업원 및 경영층의 태도에 대한 현재 상태(Young,2008) 등으로 정의될 수 있다.

Eloff(2002)는 정보보호 정책과 관련 절차를 평가하기 위해 모범규준을 사용해야 한다고 언급하였다. 그 모범규준은 다른 조직과 비교 할 수 있고, 보안 목적의 충족 여부를 판단할 수 있는 내용을 포함해야 한다고 하였다. 보안상태 평가에 대한 관심이 공학 지식 영역에서 메커니즘의 개발을 가져왔으며 그것이 바로 정보보호 프로세스 성숙도의 측정방법이다. 성숙도 평가 모델에는 COBIT(Control Objectives for Information and Related Technology V5.0,2012), ISM3(Information Security Management Maturity Model V1.0,2004), SSE-CMM(System Security Engineering-Capability Maturity Model V3.0,2003) 등이 있다.

SSE-CMM은 정보통신 기술과 공학 분야의 기술적 측면에 초점을 맞춘다. 이 방법은 생산된 산출물의 신뢰성 뿐 아니라 개념 정의, 보안 시스템 수명주기, 요구 사항 분석, 설계, 개발, 통합, 설치, 운영, 유지 보수 및 폐기를 포함하는 보안 엔지니어링 능력을 개선하고 평가하는 데 사용된다. 그러나 이는 사회적 관점을 고려하지 않는 기술적인 접근 방법이어서 순수 컴퓨터 시스템에게는 적합할 수 있으나, 사람 또는 사회적 구성요소가 존재하는 정보시스템 보안을 다루는데 있어서 충분하지 못하다(Dzazali,2012). COBIT과 ISM3는 조직의 환경 및 미션을 커버하기 때문에 두 모델은 정보통신 기술의 기술적 차원뿐만 아니라 사회적 차원을 포함하는 것으로 보인다. COBIT은 ISM3보다 간단하지만 의식, 훈련, 소통, 프로세스 및 관행, 기법 및 자동화, 컴플라이언스, 전문성 같은 기술적 뿐 아니라 사회적 차원을 정의함에 있어서 더욱 명시적이다. COBIT 프레임워크는 특정 상황에서 IT 관련 프로세스 성숙도를 더 정확하게 평가할 수 있도록 성숙도를 역량, 성능 및 통제 3가지 차원으로 구분한다.

정보보호 수준은 그 정보의 가치와 정보 자산의 부적절한 사용, 노출, 저하 또는 이용 방해로 인해 발생하는 손실과 관련되어야 한다(Schneier,2002; Peltier,2001). Hall et al(2011)은 정보보호 성숙도와 조직성과 관련 연구를 통해 내·외부 보안위협으로부터 정보 및 정보시스템을 보호하는 조직의 정보보호 프로그램 수준은 법적소송 방지, 시장가치 유지, 변화하는 리스크 환경 속에서 비즈니스 복원력 확보와 같은 조직성과에 긍정적 영향을 미친다고 했다. 정보보호 활동은 1차적으로 보안사고 감소, 직원의 인식제고와 만족도, 협력사 간의 정보교류 신뢰도 향상 같은 정보자산 보호 성과에 긍정적 영향을 미치며, 정보자산 보호 성과는 자산 손실 방지, 고객유지 및 확보 등 같은 조직의 본질적인 성과에 긍정적 영향을 미치는 것으로 밝혀졌다(김경규 외,2009). 현장에서 사용되는

<표 2> 정보보호 성숙도 관련 문헌연구

관점	연구목적	연구결과	출처
정보보호 성숙도의 영향요인	정보보호 성숙도의 영향요인, 성숙도와 식별된 요인 간의 관계 연구	정보보호 성숙도 높은 조직과 낮은 조직을 구별하는 요인은 위험관리와 개인 인식임	Dzazali (2012, 2006)
정보보호에서 조직역량의 영향	정보보호 프로그램과 조직성과 간의 관계 연구	조직역량이 정보보호 전략 구현 및 조직성과에 유의한 영향을 미침	Hall et al (2011)
정보보호 상태 개념 도입	정보보호 상태(수준)의 측정방법 및 정보보호 전략 활용 방법	정보보호 수준은 정보보호 활동, 통제수단의 효과적 이용에 관한 경영층 인식과 관계가 있음	Young(2008)
조직프로세스 성숙도와 조직성과	소프트웨어 프로세스 개선활동이 조직성과에 미치는 영향	높은 수준의 성숙도 달성 위해 관련 활동,목표에 대한 명확한 이해	윤재욱,김인재 (2006)
정보보호 정책 및 절차 개발	정보보호 정책 개발시 현장에서 직면하는 문제에 대한 해답 모색	정보보호 정책과 절차 평가시 정보보호 국제표준 활용이 바람직	Eloff(2002)
정보보호 성숙도의 대안 모델 요건	안전한 정보시스템과 소프트웨어 개발을 위한 대안 성숙도 모델분석	정보보호 관리 중심의 정보보호성숙도 모델이 필요	Siponen(2002)
프로세스 기반 정보보호 성숙도 평가모델	벤치마킹과 프로세스 성숙도 수준의 목표 차이를 분석 및 관리	조직의 비즈니스 요구사항과 연관된 IT거버넌스의 모든 측면	COBIT (ISACA,2012)
	정보보호 관리프로세스 관점에서 성숙도를 평가	4가지 영역의 조직의 환경 및 미션 : 정보보호관리시스템, 조직 시스템, 정보시스템, 정보보호 환경	ISM3 (Aceituno,2004)
	소프트웨어공학 조직의 개발보안프로세스 및 역량 평가	신뢰된 제품 또는 안전한 시스템 라이프싸이클 전체를 포함한 활동. 3가지 기본영역 : 리스크, 보증, 엔지니어링.	SSE-CMM (ISSEA,2003)

성숙도 평가방식이 목적과 대상범위가 조금 다르다하더라도 모두 조직 내 프로세스 지향의 표준이기 때문에 성숙도 수준은 고객만족도 제고, 제품의 품질 향상 같은 조직성과에 영향을 미친다(윤재욱, 김인재,2006).

2.3 정보보호 영향요인과 정보보호 성숙도

정보보호는 단지 기술뿐 아니라 조직, 개인, 사회적 요소로 구성된 사회적 시스템이다. 효과적인 정보보호 관리 시스템에 대한 연구는 기술적 요인 이외에 사회적 요인을 고려하지 않는다면 완성될 수 없다고 했다(Schneier, 2002; Dhillon and Backhouse, 2001). 사회기술시스템이론(Kowalski,1994;Trist,1981; Bostrom and Heinen,1977)과 시스템총괄모형(Yngström, 1996) 연구에 따르면 정보보호 이슈를 다룰 때에는 종합적이고 다학제적인 사고가 필요하다고 강조했다. 그 이유로 완벽한 보안은 바람직하며 추구해야 할 목표이지만 이는 현실적으로 달성이 어렵기 때문이라고 했다. Werlinger et al(2009)는 조직 내 정보보호 관리상의 도전요인 18가지를 기술적, 인적, 조직적 관점에서 설명하고 이들 요인 간의 상호작용을 연구하였다.

Dzazali(2012)는 조직의 정보보호 성숙도에 미치는 영향요인을 크게 기술적, 사회적으로 구분하고 그 요인간의 관계를 규명하기 위해 실증연구를 실시하였다. 이 연구는 사회적 요인이 조직의 정보보호 성숙도에 가장 많은 영향을 주는 것으로 보았다.

본 연구에서는 개인적 인지에 기반을 둔 정보보호 성숙도의 매개역할을 실증하기 위하여 조직의 정보보호 성숙도에 영향을 미치는 요인에 대한 선행연구의 결과(<표 1>, <표 2>)를 종합하고 본 연구의 목적성을 고려하여 4가지의 관점에서 영향요인을제시하였다. 즉 개인적 관점에서 1)인식 및 문화, 2)개인 혁신성; 조직적 관점에서 1)비즈니스 관리자의 IT역량, 2)최고경영층지원, 3)IT관리, 4)조직구조; 기술적 관점에서 1)취약점분석평가, 2)침해행위대응; 사회적 관점에서 1)정보보호 컴플라이언스 2)환경 불확실성을 영향변수로 채택하고 다음과 같은 연구가설을 도출하였다.

첫째, 개인적 관점의 영향변수와 정보보호 성숙도 간의 관계를 설명하였다.

H1 : 인식 및 문화는 조직의 정보보호 성숙도에 정(+)의 영향을 미칠 것이다.
H2 : 개인 혁신성은 조직의 정보보호 성숙도에 정(+)의 영향을 미칠 것이다.

둘째, 조직적 관점의 영향변수와 정보보호 성숙도 간의 관계를 설명하였다.

H3 : IT역량은 조직의 정보보호 성숙도에 정(+)의 영향을 미칠 것이다.
H4 : 최고경영층 지원은 조직의 정보보호 성숙도에 정(+)의 영향을 미칠 것이다.
H5 : IT관리는 조직의 정보보호 성숙도에 정(+)의 영향을 미칠 것이다.
H6 : 조직구조는 조직의 정보보호 성숙도에 정(+)의 영향을 미칠 것이다.

셋째, 기술적 관점의 영향변수와 정보보호 성숙도 간의 관계를 설명하였다.

H7 : 취약점 분석평가는 조직의 정보보호 성숙도에 정(+)의 영향을 미칠 것이다.
H8 : 침해행위 대응은 조직의 정보보호 성숙도에 정(+)의 영향을 미칠 것이다

넷째, 사회적 관점의 영향변수와 정보보호 성숙도 간의 관계를 설명하였다.

H9 : 정보보호 컴플라이언스는 조직의 정보보호 성숙도에 정(+)의 영향을 미칠 것이다.
H10: 환경 불확실성은 조직의 정보보호 성숙도에 정(+)의 영향을 미칠 것이다.

2.4 정보보호의 조직성과에 관한 연구

정보보호의 조직성과란 조직이 정보보안 관리 통제 또는 활동을 통해 얻을 수 있는 결과이다. 일반적으로 정보보호는 성과로써 해당 조직에게 중요한 가치를 제공한다. 보안사고 및 정보 누출로 인한 사고 방지를 보증하고, 보안사고 관련 손실을 최소화하며 정보의 부정확성으로 인해 조직과 고위경영진에게 부여되는 잠재적인 사회적, 법적 책임을 방지할 수 있다.

정보보호의 조직성과를 정보보안의 예방 및 손실방지와 같은 소극적인 것으로부터 경쟁우위, 공공이미지, 고객 만족과 같이 정보보안과 관련된 적극적인 것으로 구분할 수 있다. 다른

관점에서 보면 재무성과로써 정보보호 사고에 의한 손실, 내부성과로써 최고경영자의 인식제고와 보안조직의 직무만족과 지원, 조직 구성원의 정보보호 인식과 만족, 외부성과로써 협력사 및 공급사의 만족과 이미지, 고객의 이미지 및 서비스 만족, 공공 이미지 유지로 정의할 수 있다(홍기향,2003).

Hagen(2008)은 정보보호의 조직성과를 리스크관리, 경제적, 법적, 문화적 관점으로 분류하고 침해사고 감소, 투자로부터 기대 이익을 극대화, 법적 요구사항 위반에 대한 회피, 개인 및 조직의 인식과 행동 개선 효과가 있다. Hall et al(2011)은 조직이 다양한 이해당사자의 비즈니즈 목표와 가치를 생산하고 성취하는 정도를 조직성과로 정의하였다. 여기서 조직성과란 고객의 신뢰 제고, 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 확보를 포함한다고 했다. 김경규 외(2009)는 정보보호의 조직성과를 정보자산보호 성과와 조직 성과로 구분하고 이들의 관계를 연구하였다. 정보자산보호 성과는 보안사고 감소 성과, 직원의 인식제고와 만족도 향상, 협력사 간의 정보교류 신뢰도 향상, 개인 정보보호에 대한 고객 신뢰도 향상 등으로 정의된다. 한편 조직성과는 기술 및 서비스보호를 통한 자산 손실 방지, 비즈니스 연속성 및 기회 성과, 이미지손실 방지에 따른 이미지 유지 성과, 고객유지 및 고객기반 확대 성과에 따른 매출증대 성과의 정도로 정의하였다. 연구결과 정보자산보호 관리활동은 정보자산보호 성과에 긍정적인 영향을 미치며 그리고 정보자산보호 성과 또한 조직의 본질적인 성과에 긍정적인 영향을 미치는 것으로 밝혀졌다. 백민정,손승희(2011)는 조직구성원의 정보보안행동과 조직의 정보보안 성과에 관한 연구에서 정보보안 사고 빈도 및 사고로 인한 손실 감소를 정보보안 성과로 측정하였다.

정보보호의 성과는 기회비용 성격이어서 정보자산 보호가 잘 이루어지는 경우에는 손실이 발생하지 않고, 정보보호가 잘 이루어지지 않는 경우에만 손실이 발생하여 그 효과를 객관적으로 파악하는 데에는 한계가 있으므로 정보보호의 조직성과를 금전적으로 측정하기에는 어려움이 있다(Smith 1995). 김인재 외(2010)는 조직의 성과 측정을 위해서는 ROI(Return On Investment) 등 다양한 재무적 지표 외에 수치화된 품질 및 생산성 지표 등의 객관적 지표를 사용하는 방법이 바람직하고 할 수 있다. 하지만 서로 다른 조직을 비교하는 실증적 연구에서는 지표 수집의 어려움, 조직 간에 서로 다른 지표의 사용, 다양한 요인이 ROI 등의 최종지표에 영향을 주는 교락효과(Confounding Effect)에 따른 잘못된 관계의 성립 등의 문제점이 발생될 수 있기 때문에 객관적 지표의 사용에 한계가 있다고 했다.

정보보호의 조직성과에 대한 기존 연구를 살펴본 결과, 객관성 있는 재무적 지표의 사용 및 측정이 용이하지 않으며 조직성과는 리스크관리, 경제적, 법적, 문화적 관점에서 정의할 수 있음을 알 수 있다.

<표 3> 정보보호의 조직성과 관련 문헌연구

관점	성과내용	연구결과	연구자
리스크 관리, 경제적, 법적,	비즈니스 복원력 확보, 고객의 신뢰 제고, 브랜드 파워 또는 회사 평판에 대한 대중의 인지도 보호, 고객의 서비스 개선, 시장가치 유지, 고비용의 법적소송 방지	조직 역량은 효과적인 정보보호 전략구현에 긍정적 영향을 미치고, 조직성과에 영향을 줌	Hall et al (2011)
리스크관리, 경제적	정보보안 사고빈도 감소,정보보안 사고손실 감소	조직구성원 개인차원의 정보보안 인식이 정보보안 행동에 영향을 미치고 결과적으로 조직 보안성과에 영향을 줌	백민정,손승희 (2011)
리스크관리, 경제적	기술 및 서비스보호를 통한 자산 손실 방지, 비즈니스 연속성 및 기회 성과, 이미지손실 방지, 고객유지 및 고객기반 확대 성과에 따른 매출 증대	정보자산보호 관리활동은 정보자산보호 성과에 긍정적 영향을 미치며, 정보자산보호 성과는 조직 성과에 대해 긍정적인 영향을 미침	김경규 외 (2009)
리스크관리, 경제적, 법적, 문화적	침해사고 발생 감소, 신규서비스 및 기술에 대한 투자효과, 법적 요구사항 위반에 대한 회피, 구성원의 인식 및 행동 개선	조직 정보보호 대책의 구현 정도와 대책의 효과는 역의 관계가 있음	Hagen(2008)
리스크관리 경제적, 법적, 문화적	정보보안 사고의 빈도와 영향, 공급자/협력자와 신뢰, 고객의 이미지와 서비스 만족, 공공이미지와 법 준수, 최고경영자의 인식제고와 지원, 보안조직의 직무만족과 역량강화, 직원의 인식제고	정보보호 통제와 활동은 정보보호 성과에 영향을 미치나 활동이 통제보다 직접적인 영향을 미침. 조직이 정보보호 성과를 향상시키기 위해서는 먼저 정보보호 활동을 강화할 필요가 있음	홍기향(2003)
리스크관리	컴퓨터바이러스에 의한 손실, 제3자에 의한 불법 접근 또는 침입, 내부정보유출에 의한 정보시스템 및 네트워크 위반	정보보안 사고 피해액을 표면적 피해와 잠재적 피해의 합으로 산출	IPA(Information Technology Promotion Agency (2001)
리스크관리, 법적	정보자산보호가 잘 이루어지지 않는 경우에만 손실이 발생하여 그 효과를 객관적으로 파악하는 데에는 한계가 있음	정보보호 성과는 기회 비용적 성격이 있으므로 금전적 측정이 어려움	Smith(1995)
경제적, 문화적	예산 준수, 일정 준수, 소프트웨어 품질, 개발자 생산성. 고객 만족도, 직원 만족도	동일한 성공요인이라 할지라도 그 조직이 갖고 있는 조직의 성숙도 즉, 소프트웨어 프로세스의 능력에 따라 그 성과가 다를 수 있음	김인재 외 (2010)
경제적	업무수행 비용감소, 효율성 증가, 향상된 서비스 제공, 조직의 신뢰성 및 경쟁력 증가, 기존의 문제 해결, 새로운 사업기회 획득가능성 증가	성숙도가 높은 정보보호 정책을 수립하기 위해서는 조직의 특성을 반영해야 함	최명길(2008)
경제적	직접 경제적 피해(복구비용), 간접 경제적 피해(생산효율 감소, 데이터손실), 파생 손실(조직이미지, 시장점유율 감소, 피해보상비용)	1차 피해(온라인 판매감소액의 기회비용,생산성 저하에 의한 생산감소액,복구비용), 2차 피해(손해배상,주가변동 등) 산정함	한국인터넷진흥원 (2006)

2.5 정보보호 성숙도와 조직성과

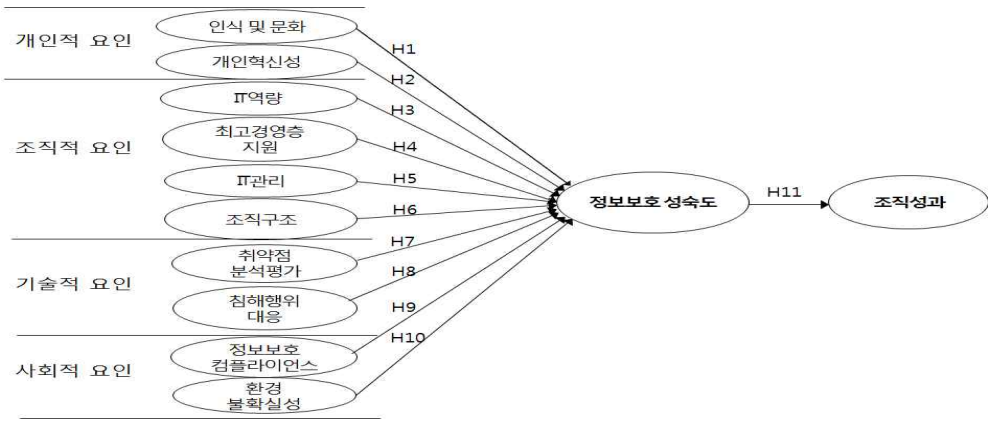
정보보호 전문가들은 어떤 특정한 상황에서 추구되는 정보보호 수준은 그 정보의 가치와 정보 자산의 부적절한 사용, 노출, 저하 또는 이용방해로 인해 발생하는 손실과 비례해야 한다(Schneier,2002; Peltier,2001). 내·외부 보안위협으로부터 정보 및 정보시스템을 보호하는 조직의 정보보호 프로그램 수준은 법적소송 방지, 시장가치 유지, 변화하는 리스크 환경 속에서 비즈니스 복원력 확보와 같은 조직성과에 긍정적 영향을 미친다(Hall et al,2011). 본 연구에서도 조직의 정보보호 수준 또는 역량이 조직성과에 영향을 미칠 것이라고 가정하였다.

본 연구에서는 정보보호의 조직성과에 대한 Hagen(2008)의 4가지 관점을 채택하였으며 그 관점에 속하는 세부항목은 문헌연구를 통해 구성하였다. 리스크관리 관점의 성과로 1)침해사고 발생 감소, 2)비즈니스 복원력 확보, 경제적 관점의 성과로 1)브랜드 파워 및 평판 보호, 2)신규서비스 및 기술의 투자효과, 3)서비스 품질 향상비즈니스, 법적 관점의 성과로 1) 법적 소송방지, 문화적 관점의 성과로 1)구성원의 인식 및 행동 개선을 채택하였다. 상기의 논의를 토대로 다음과 같은 연구가설을 도출하였으며, 이는 정보보호 성숙도와 조직성과 간의 관계를 설명한다.

H11 : 조직의 정보보호 성숙도는 조직성과에 정(+)의 영향을 미칠 것이다.

2.6 연구모형

본 연구에서는 선행연구와 이상의 논의를 바탕으로 각 개인이 느끼는 정보보호 성숙도 수준이 매개적 역할을 하는지를 실증하고자 한다. 이를 위해 사회기술시스템이론(Socio-Technical Systems Theory)에 바탕을 두고 각 개인이 느끼는 정보보호 성숙도 에 4가지 관점(개인적, 조직적, 기술적, 사회적)의 영향요인이 포함되는지, 어떤 요인이 더 많은 영향을 주는지 그리고 정보보호의 성숙도 수준과 조직성과 간에는 어떠한 인과관계가 있는지를 검증하고자 <그림 1>의 본 연구의 모형을 설정하였다.



<그림 1> 연구 모형

Ⅲ. 조작적 정의와 설문구성

본 연구에서 설문항목은 기존연구의 요인들과 설문항목을 참고하되 연구목적에 맞게 일부 수정 및 보완하였으며 설문의 신뢰성을 높이기 위해 사전 설문 조사를 실시하였다. 연구의 진행은 설문조사를 통해 확보된 자료를 바탕으로 실증연구를 실시하였다. 본 연구에서는 독립변수로 인식 등 정보보호 영향요인, 매개변수로 정보보호 성숙도 그리고 종속변수로 조직성과를 선정하였다. 사용된 모든 설문항목은 리커드(Likert) 5점 척도를 사용하였다. 다음 <표 4>은 사용된 연구변수에 대한 조작적 정의와 출처이다.

조작적 정의에 따른 연구변수의 측정을 위한 설문항목은 크게 3가지로 구성하였다. 첫째, 조직성과에 영향을 미치는 정보보호 영향요인 관련 설문이다. 인식 및 문화는 정보보호가 구성원에게 공유된 규범으로 인식되고 있는지, 개인혁신성은 새로운 정보기술에 대한 수용성, IT역량은 IT에 관한 관리자의 지식·경험· 비전, 최고경영층지원은 정보보호에 대한 경영진의 실천

<표 4> 연구변수의 조작적 정의와 출처

구분	연구변수	조작적 정의	출 처
종속변수	조직성과	비즈니스 복원력, 브랜드 파워 및 평판, 서비스 품질, 법적소송 방지	Hall et al(2011), 김경규 외(2009), Hagen(2008), NIST(2007) 등
독립변수	인식 및 문화	정보보호에 대한 구성원의 인식 및 내재화 수준	Knapp et al(2006)
	개인 혁신성	사용자가 새로운 정보기술에 대해 타인과 비교하여 혁신적으로 먼저 수용하려는 정도	김상현외(2012) Agarwal and Prasad(1998)
	IT역량	비즈니스관리자가 보유한 IT관련 지식 및 경험의 총체	Chang and Ho(2006) Bassellier(2001)
	최고경영층 지원	조직 최고경영층의 지원정도	Dzazali et al(2012) Knapp et al(2006)
	IT관리	비지니스 목표 달성을 위한 IT기반 일련의 활동	Werlinger et al(2009)
	조직구조	정보보호에 관한 책임 및 의사소통구조	Dzazali et al(2012)
	취약점 분석·평가	정보자산 및 환경에 내재된 취약점을 분석·평가·개선하는 활동	ISO/IEC27001(2005)
	침해행위 대응	침해행위를 탐지·대응·복구하는 활동	NIST SP 800-61(2007) ISO/IEC27001(2005)
	정보보호 컴플라이언스	IT 정보보호 관련 법규 및 표준의 준수 활동	금융IT보안컴플라이언스(2011) Tashi(2009) ISO/IEC27001(2005)
	환경 불확실성	업무 관련한 환경의 불확실성의 정도	Chang and Ho(2006)
매개변수	정보보호 성숙도	보안 위협으로부터 안전성을 확보할 수 있는 조직의 역량 수준	Dzazali et al(2012) COBIT(2012) Dzazali et al(2006) Siponen(2002)

의지와 지원정도, IT관리는 비즈니스와 정보기술의 연계, 조직구조는 정보보호 담당조직의 역할 및 정보보호계획 운영, 취약점 분석·평가는 정보자산에 내재되어 있는 보안취약점에 대한 관리, 침해행위 대응은 침해 시도행위에 대한 탐지 및 대응활동, 정보보호 컴플라이언스는 관련 법규 및 표준의 준수 정도, 환경 불확성은 기술·제도의 가변성 및 고객의 보안요구사항 변경 등에 대해 설문을 하였다. 둘째, 정보보호 성숙도 수준 관련 설문이다. 위험관리 프로세스의 수준을 측정하기 위해 정보보호정책의 수립·시행, 핵심시스템 목록 관리, 사용하고 있는 운영절차의 정보보호정책 부합성, 정보보호 책임부여의 명확성 등 대해 설문을 하였으며, 위험평가 프로세스 수준을 측정하기 위해 위험평가 실시계획, 위험평가 절차의 문서화, 조직자산에 영향을 주는 변경 발생시 위험평가의 수행 여부 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 소송 방지 등에 대해 실시하였다.

Ⅳ. 실증분석

4.1 자료수집 및 표본 특성

본 연구의 설문은 국내 금융회사와 정보보호 기업의 종사자를 대상으로 하였다. 두 업종 종사자를 대상으로 한 이유는 금융회사의 경우 일반 국민의 생활과 관련성이 높을 뿐 아니라 취급하는 정보의 민감성으로 인해 정보보호가 상대적으로 중요시 되는 업종이 금융 분야이며 금융회사에서 IT와 정보보호는 비즈니스를 지원하는 역할을 뛰어 넘어 '비즈니스 그 자체'라고 할 수 있을 정도로 중요하다. 그리고 정보보안 기업 종사자는 정보보호의 특성을 가장 잘 이해할 수 있는 집단으로 판단되었기 때문이다. 설문기간은 2013년 9월 13일부터 10월 31일까지 실시되었으며 온라인 설문(docs.google.com) 및 우편을 이용하였다. 설문대상자는 조직에 속해 있는 조직구성원들이다. 연구 조사를 위해 총 1,000부의 설문을 배포하여 256부를 회수하였으며, 이중 응답이 비논리적이거나 지나치게 불성실한 11부를 제외한 245부가 분석에 사용되었다. 응답자의 소속 기업은 금융유관기관(29.4%)과 정보보안 기업(28.6%)의 비율이 높았으며, 응답자의 직급은 실무자(49,4%),중간 관리자(33.0),상급 관리자(14.3) 순으로 나타났다. 표본에 대한 일반적 특성은 다음<표 5>와 같다.

4.2 측정모형 분석

본 연구모형에서 제시된 측정모형은 조절변수를 제외한 12개의 잠재변수를 나타내는 52개의 관측변수(Observatory Variable)를 245개의 데이터를 이용하여 분석하였다. Lisrel 8.72의 Simplis(Simple Lisrel)를 이용하였고 분석된 통계자료의 해석은 배병렬(2006)의 저서와 Koufteros and Marcoulides(2006)의 논문을 참고하였다.

잠재변수가 관측변수에 의해 설명되는 정도

를 알아보기 위해 집중타당성(Convergent Validity) 분석을 실시하여 요인적재 값이 0.7이상(R2 은 0.5 이상)인 측정항목을 포함하였다. 그 과정에서 IT역량, 최고경영층지원, 침해행위 대응은 모든 측정항목이 포함되었으나, 인식 및 문화 3개, 개인 혁신성 1개, IT관리 1개, 조직구조 1개, 취약점 분석평가 1개, 정보보호 컴플라이언스 1개, 환경 불확실성 1개, 정보보호 성숙도 5개, 조직성과 1개의 측정항목이 탈락하여 <표 6>와 같이 제시되었다.

내적일관성은 합성신뢰도(Composite Reliability)와 평균분산추출(Average Variance Extraction) 값을 통하여 검증하였다. 일반적으로 각 0.7과 0.5 이상이면 신뢰도가 있는 것으로 보기 때문에(배병렬,2006,p161) 잠재변수의 측정항목은 모두 기준치를 만족한다.

<표 5> 인구통계학적 특성 (단위 : 명, %)

구 분	내 용		응답자 수	비율(%)	
소속	금융회사	은행	56	71.4	(22.9)
		증권사	11		(4.5)
		보험사	27		(11.0)
		카드사	9		(3.7)
		금융유관기관	72		(29.4)
	정보보안 기업		70	28.6	
담당업무	정보보호		149	60.8	
	프로그램개발		16	6.5	
	시스템 운영관리		19	7.8	
	e-비즈니스		33	13.5	
	기타		28	11.4	
담당업무의 정보보호 관련정도	직접적으로 관련		170	69.4	
	간접적으로 관련		70	28.6	
	관련성 없음		5	2.0	
직급	상급 관리자		35	14.3	
	중간 관리자		81	33.0	
	실무자		121	49.4	
	기타		8	3.3	
업무 수행기간	10년 이상		65	26.5	
	5년 ~ 9년		36	14.7	
	3년 ~ 5년		40	16.3	
	3년 이하		104	42.4	
조직규모	15,000명 이상		15	6.1	
	10,000 ~ 14,999명		7	2.9	
	1,000 ~ 9,999명		40	16.3	
	500 ~ 999명		116	47.3	
	100 ~ 499명		34	13.9	
	100명 이하		33	13.5	

<표 6> 측정모형 분석결과

잠재변수		관측변수			합성신뢰도 (CR)	평균분산추출 (AVE)
		측정항목	요인적재	t 값		
개인적 요인	인식 및 문화 (3)	aware1	0.76	1	0.8083	0.5855
		aware2	0.70	10.60		
		aware3	0.83	12.47		
	개인 혁신성 (3)	inno1	0.79	1	0.7944	0.5633
		inno2	0.73	9.80		
		inno4	0.73	9.83		
조직적 요인	IT역량 (3)	capa1	0.88	1	0.9063	0.7633
		capa2	0.90	18.48		
		capa3	0.84	16.77		
	최고경영층 지원 (5)	top1	0.86	1	0.9225	0.7050
		top2	0.83	16.54		
		top3	0.89	18.77		
		top4	0.87	18.05		
		top5	0.74	13.94		
	IT관리 (4)	ITmgt1	0.80	1	0.8846	0.6577
		ITmgt2	0.85	14.79		
		ITmgt3	0.84	14.56		
		ITmgt5	0.75	12.74		
	조직구조 (4)	org2	0.72	1	0.8500	0.5870
		org3	0.82	12.03		
		org4	0.79	11.66		
		org5	0.73	10.72		
기술적 요인	취약점 분석평가 (4)	vul2	0.72	1	0.8892	0.6691
		vul3	0.86	13.12		
		vul4	0.90	13.68		
		vul5	0.78	11.86		
	침해행위 대응 (5)	inci1	0.72	1	0.8994	0.6419
		inci2	0.81	12.18		
		inci3	0.80	12.06		
		inci4	0.85	12.77		
		inci5	0.82	12.40		
사회적 요인	정보보호 컴플라이언스 (4)	comp1	0.88	1	0.9126	0.7232
		comp2	0.81	16.62		
		comp3	0.86	18.41		
		comp4	0.85	17.99		
	환경 불확실성 (3)	env1	0.79	1	0.8208	0.6050
		env2	0.82	11.86		
		env3	0.72	10.73		

잠재변수	관측변수			합성신뢰도 (CR)	평균분산추출 (AVE)
	측정항목	요인적재	t 값		
정보보호 성숙도 (17)	isml1	0.73	1	0.9604	0.5884
	isml2	0.71	11.28		
	isml3	0.76	12.13		
	isml4	0.76	12.13		
	isml5	0.74	11.87		
	isml6	0.84	13.53		
	isml7	0.78	12.55		
	isml8	0.85	13.67		
	isml9	0.71	11.25		
	isml10	0.76	12.12		
	isml11	0.79	12.76		
	isml12	0.74	11.86		
	isml13	0.83	13.41		
	isml14	0.80	12.82		
	isml15	0.77	12.37		
	isml16	0.73	11.60		
	isml17	0.72	11.46		
조직성과 (6)	per2	0.73	1	0.8885	0.5707
	per3	0.72	10.92		
	per4	0.76	11.48		
	per5	0.79	11.99		
	per6	0.75	11.38		
	per7	0.78	11.71		

잠재변수에 대한 상관행렬을 이용하여 구성개념 간의 상관관계를 분석하였다. 일반적으로 상관계수가 0.8을 초과하면 잠재변수 간에 다중공선성이 발생한다고 본다. <표 7>에서 보는 바와 같이 정보보호 성숙도와 조직구조, 침해행위 대응, 정보보호 컴플라이언스 간의 상관계수 값이 0.80에 근접 또는 다소 초과하는 것으로 나타났다. SPSS를 이용하여 독립변수 간의 다중공선성을 진단한 결과[1]에서 보는 바와 같이 공차(Tolerance)한계는 최대가 .859, VIF(Variance Inflation Factor)는 2.766로서 독립변수 간의 상관이 문제가 될 정도로 높지 않음을 알 수 있다.

1) VIF를 이용한 독립변수의 다중공선성 진단 결과

모형		공선성 통계량	
		Tolerance	VIF
1	(상수)		
	인식및문화	.425	2.352
	개인혁신성	.859	1.164
	IT역량	.633	1.579
	최고경영층	.416	2.401

<표 7> 잠재변수 간의 상관행렬

구분	정보 보호 성숙도	조직 성과	인식 및 문화	개인 혁신성	IT 역량	최고 경영층 지원	IT 관리	조직 구조	취약점 분석 평가	침해 행위 대응	컴플 라이 언스	환경 불확 실성
정보보호성숙도	**0.77**											
조직성과	0.75	**0.76**										
인식및문화	0.64	0.47	**0.77**									
개인혁신성	0.17	0.13	0.25	**0.75**								
IT역량	0.40	0.30	0.45	0.36	**0.87**							
최고경영층지원	0.59	0.43	0.78	0.20	0.52	**0.84**						
IT관리	0.60	0.45	0.58	0.33	0.60	0.67	**0.81**					
조직구조	0.79	0.59	0.57	0.23	0.50	0.62	0.61	**0.77**				
취약점분석평가	0.73	0.54	0.51	0.20	0.37	0.52	0.55	0.65	**0.82**			
침해행위 대응	0.82	0.61	0.55	0.16	0.34	0.52	0.52	0.64	0.70	**0.80**		
IS컴플라이언스	0.85	0.63	0.55	0.06	0.34	0.53	0.52	0.69	0.70	0.76	**0.85**	
환경불확실성	0.53	0.40	0.36	0.23	0.24	0.37	0.44	0.34	0.57	0.47	0.49	**0.78**

* 대각선 음영친 부분은 평균분산추출(AVE)의 제곱근

독립평균분산추출의 제곱근은 값이 적어도 0.7 이상이고(즉 평균분산추출의 값이 0.5 이상), 각 대각선에 있는 이 제곱근의 값(√AVE)이 잠재변수 간의 상관계수 값을 상회하므로 판별 타당성(Discriminant Validity)의 기준을 만족한다(Fornell & Larcker,1981).

4.3 구조모형 분석

4.3.1 경로분석을 통한 가설검증

가설검증에 앞서 분석한 구조모형의 적합도를 평가하였다. 모형의 전반적인 적합도를 나타내는 지표인 잔차평균자승이중근(RMR,Root Mean Square Residual)과 근사오차평균자승(RMSEA,Root Mean Square Error of Approximation) 값은 0.05이하면 양호한 것으로 평가하는데(Tomarken and Waller, 2003; Steiger, 1990; Browne and Cudeck, 1993) 본 모형의 각 0.037과 0.059 이므로 양호한 것으로 판단하였다. 기초모형에 대한 제안모형의 적합정도를 나타내는 지수인 표준 적합지수(NFI: Normed Fit Index), 비표준 적합지수(NNFI: Non Normed Fit Index), 비교 적합지수(CFI: Comparative Fit Index)는 역시 0.9 이상이면 좋은 적합도를 갖는 것으로 본다. 또한 표준 카이자승(Chi-Square)값은 카이자승(X^2)값을 자유도(df)로 나눈 값으로 일반적으로 X^2값이 자

	IT관리	.434	2.303
	조직구조	.437	2.288
	취약점분석	.432	2.313
	침해행위	.434	2.303
	컴플라이언스	.362	2.766
	환경불확실성	.700	1.428

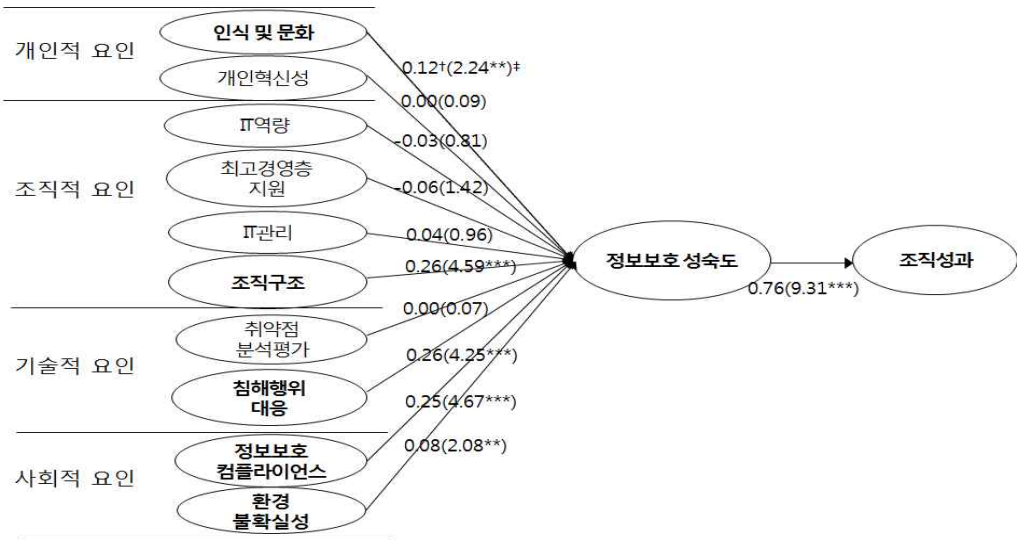
* 종속변수: 정보보호성숙도

<표 8> 잠재변수간의 총효과와 간접효과

구분		인식 및 문화	개인 혁신성	IT 역량	최고 경영층 지원	IT 관리	조직 구조	취약점 분석평가	침해 행위 대응	컴플라이언스	환경 불확실성	조직 성과
정보보호 성숙도	총효과	0.12 (2.24)	0.00 (0.09)	-0.03 (-0.81)	-0.06 (-1.42)	0.04 (0.96)	0.26 (4.59)	0.00 (0.07)	0.26 (4.25)	0.25 (4.67)	0.08 (2.08)	0.76 (9.31)
	간접 효과	—	—	—	—	—	—	—	—	—	—	—
조직 성과	총효과	0.09 (2.22)	0.00 (0.09)	-0.02 (-0.81)	-0.05 (-1.42)	0.03 (0.96)	0.20 (4.40)	0.00 (0.07)	0.20 (4.09)	0.19 (4.47)	0.06 (2.06)	—
	간접 효과	0.09 (2.22)	0.00 (0.09)	-0.02 (-0.81)	-0.05 (-1.42)	0.03 (0.96)	0.20 (4.40)	0.00 (0.07)	0.20 (4.09)	0.19 (4.47)	0.06 (2.06)	—

유도의 2배를 넘지 않으면 p값이 작아도 적합한 모형으로 평가한다. 분석결과 본 구조모형의 적합도(n=245, RMR=0.037, RMSEA=0.059, GFI=0.92, AGFI=0.91, NFI=0.96, NNFI=0.98, CFI=0.98, X^2/df=1.86(X^2=3186.96, df=1713))는 전반적으로 양호한 것으로 분석되었다. 잠재변수간의 총 효과와 간접효과는 <표 8>와 같다.

본 연구의 가설검증은 잠재변수 간의 인과관계를 나타내는 각 경로로써 <그림 2>와 같다. 인과관계를 분석할 때 가설의 방향성이 제시되었으므로 단측 검증을 사용하였으며 t값은 유의수준 α=0.05를 기준으로 |t|값이 1.645 이상인 값을 가설 채택의 기준으로 사용하였다. 아래 공변량 구조모형의 분석결과에서 보듯이 정보보호 영향요인은 정보보호 성숙도에 유의한 영향을 미치는 것으로 나탔다. 또한 매개변수와 종속변수 관계에서는 정보보호 성숙도는 조직성과에 유의한 영향을 미치는 것으로 나타났다.



n=245, RMR=0.037, RMSEA=0.059, GFI=0.92, AGFI=0.91, NFI=0.96, NNFI=0.98, CFI=0.98, X^2/df=1.86(X^2=3186.96, df=1713), †: 표준경로계수, ‡: t값(*: 0.05, **: 0.01, ***: 0.001)

<그림 2> 경로 분석결과

4.4 검증결과의 해석

앞서 분석을 통해 확인된 가설의 채택여부는 아래 <표 9>와 같다. 가설의 채택여부에 대한 해석은 연구의 목적과 특성에 맞게 구성하였다.

4.4.1 정보보호 영향변수와 정보보호 성숙도

정보보호 영향요인과 정보보호 성숙도 간의 인과관계를 분석한 결과 개인적, 조직적, 기술적, 사회적 관점의 모든 요인이 정보보호 성숙도에 영향을 미치는 것으로 나타났다. 이는 정보보호가 복합적인 속성을 가지고 있으므로 조직의 정보보호 수준 향상을 위한 방안 수립시 종합적인 사고와 포괄적인 접근이 필요하다는 것을 의미한다.

4가지 관점 중 사회적 요인(정보보호 컴플라이언스, 환경 불확실성)과 조직적 요인(조직구조)이 다른 요인보다 정보보호 성숙도에 미치는 영향이 큰 것으로 나타났는데 이는 지금까지 정보보호가 구성원의 정보보호 인식 제고 노력, 조직의 목표 달성을 전략적으로 지원하기보다는 외부 규제 준수 같은 통제 위주의 보안 정책을 수동적으로 추진되어 왔음을 암시할 뿐 아니라 정보보호 수준 제고를 방안 수립 시 조직 특성이 반드시 반영되어야 함을 시사한다. 앞으로는 날로 지능화하는 공격, 복잡해지는 시스템 및 업무환경으로 인한 각종 보안사고에 대비하기 위해서는 외부의 가이드라인이나 규제를 준수하는 것도 중요하지만 전사적 차원에서 자발적이고 적극적인 보안 강화 노력이 필

<표 9> 가설검증 결과

가설		결과	비고
H1	인식 및 문화는 조직의 정보보호 성숙도에 정(+)의 영향을 미칠 것이다.	채택	개인적 요인
H2	개인혁신성은 조직의 정보보호 성숙도에 정(+)의 영향을 미칠 것이다.	기각	
H3	IT역량은 조직의 정보보호 성숙도에 정(+)의 영향을 미칠 것이다.	기각	조직적 요인
H4	최고경영층 지원은 조직의 정보보호 성숙도에 정(+)의 영향을 미칠 것이다.	기각	
H5	IT관리는 조직의 정보보호 성숙도에 정(+)의 영향을 미칠 것이다.	기각	
H6	조직구조는 조직의 정보보호 성숙도에 정(+)의 영향을 미칠 것이다.	채택	
H7	취약점 분석평가는 조직의 정보보호 성숙도에 정(+)의 영향을 미칠 것이다.	기각	기술적 요인
H8	침해행위 대응은 조직의 정보보호 성숙도에 정(+)의 영향을 미칠 것이다.	채택	
H9	정보보호 컴플라이언스는 조직의 정보보호 성숙도에 정(+)의 영향을 미칠 것이다.	채택	사회적 요인
H10	환경 불확실성은 조직의 정보보호 성숙도에 정(+)의 영향을 미칠 것이다.	채택	
H11	조직의 정보보호 성숙도는 조직의 성과에 정(+)의 영향을 미칠 것이다.	채택	매개변수와 종속변수 관계

요할 것이다.

또한 정보보호 성숙도 향상을 위해 정보보호에 대한 인식 제고와 정보보호 활동을 조직문화로써 내재화시키는 것이 중요한 것으로 나타났기 때문에 우선적으로 구성원의 흥미, 관심을 유발할 수 있는 보안정책의 수립과 시행이 필요하다는 것을 알 수 있다.

한편, 선행연구에서 대부분 채택되었던 조직적 요인인 최고경영층 지원이 정보보호 성숙도에 영향을 미치지 않는 것인데 이는 설문응답자 중 기술 중심의 업무를 수행하는 실무자의 높은 비중(49.4%)과 최고경영층과 현장 실무자 간의 정보보호에 대한 인식의 차이와 관련 있는 것으로 보인다. 또한 보안사고 예방을 위한 대표적 활동인 취약점 분석평가가 정보보호 성숙도에 유의한 영향을 주지 못하는 반면에 공격 시도 행위 감시, 사고발생 시 대응 및 복구 활동인 침해행위 대응만 채택된 결과이다. 이는 최근의 보안사고가 지능적이며 광범위한 영역에서 발생하기 때문에 사고를 미연에 방지하는 것은 쉽지 않다는 인식과 관련이 있는 것으로 보인다. 새로운 정보기술과 서비스에 대한 수용의 정도를 의미하는 개인혁신성은 일반적으로 성숙도에 영향을 주는 요인이지만 본 연구에서 채택되지 않은 것은 보안(保安), 유지(維持)라는 정보보호 업무의 특수성과 관련 있는 것으로 보인다. IT역량은 조직의 정보보호 역량에 영향을 미치는 요인이지만 본 설문응답자 중 정보보호 담당자 비중(60.8%)과 IT업무 종사자로 볼 수 있는 프로그램 개발 및 시스템 운영자 비중(14.3%) 간의 현격한 차이와 관련 있는 것으로 판단된다. 비즈니스 목표 달성을 위한 IT기반 활동인 IT관리와 조직의 정보보호 성숙도 수준 간의 연관성에 대해 정보보호 업무 담당자 대부분은 충분히 인식하고 있지 않는 것으로 보인다.

본 연구는 사회기술시스템이론(Socio-Technical Systems Theory) 및 시스템 총괄모형(Systemic-Holistic Model)에 이론적 근거를 두었다. 개인적, 조직적, 기술적, 사회적 4가지 관점의 요인이 정보보호 성숙도 수준에 영향을 미친다는 연구 가설을 검증하고자 하였다. 기각된 가설이 다소 있더라도 연구모형의 적합도와 연구목적을 충실하게 따랐기 때문에 도출된 연구결과를 조심스럽게 해석한다면 큰 무리가 없다고 생각된다.

4.4.2 정보보호 성숙도와 조직성과

정보보호 성숙도와 조직성과 간의 관계를 분석한 결과가 0.75(|t|=9.31, p<0.001)로 높은 인과 관계가 있는 것으로 나타났다. 본 연구는 다양한 정보보호 활동은 소송방지, 비즈니스 연속성 확보, 이미지 유지 및 개선 등 조직이 궁극적으로 달성하고자 하는 성과를 가져온다(Hall et al, 2011; 김경규,2009; 홍기향,2003)는 선행연구와 같은 결과를 보여주고 있다. 본 연구 결과는 정보보호 수준 또는 역량이 조직성과에 영향을 미치며 장기적으로 기업 경쟁력에도 영향을 미치게 된다는 것을 시사한다. 또한 정보보호의 조직성과를 보안위협으로부터 중요 자산 보호 라는 전통적 관점에서 벗어나 경제적 관점의 신규 서비스 및 기술에 대한 투자효과, 표준 준수를 통한 서비스 품질 향상으로 까지 확장할 수 있음을 보여주고 있다.

Ⅴ. 결론 및 한계

본 연구는 정보보호 관점에서 1) 정보보호 성숙도 영향요인을 개인, 조직, 기술, 사회적 관점에서 각각 도출하였으며, 2) 이들 영향요인이 어떻게 정보보호 성숙도를 매개하여 조직성과에 영향을 미치는지를 살펴보았다.

본 연구의 결과를 요약하면 다음과 같다. 첫째, 정보보호에 대한 인식, 조직구조, 침해행위 대응, 정보보호 컴플라이언스, 환경 불확실성이 정보보호 성숙도에 유의한 영향을 미치는 것으로 나타났다. 이는 조직의 정보보호 수준 향상을 위한 방안 수립시 종합적인 사고와 포괄적인 접근이 필요하다(Yngström,1996; Kowalski, 1994; Trist,1981; Bostrom and Heinen,1977)는 선행 연구 결과를 증명해 주고 있다. 정보보호 성숙도를 효율적으로 향상시키기 위해서는 기술적 관점의 침해행위 대응능력을 제고시킬 뿐 아니라 보안조직 외에 모든 구성원의 보안의식 및 행동이 일상화 될 수 있도록 내재화하는 작업, 그리고 고객에 대한 지속적인 홍보와 함께 조직경영의 관점에서 종합적인 접근이 필요하다 것을 시사하고 있다.

둘째, 정보보호 성숙도와 조직성과 간의 관계를 분석한 결과 인과 관계가 있는 것으로 나타났다. 이는 정보보호 수준 또는 역량이 조직성과에 큰 영향을 미치며 나아가 기업 경쟁력에도 영향을 미치게 된다는 점을 시사하고 있다. 그러므로 기업들은 지속가능한 성장을 위해 정보보호 수준 향상과 관련된 투자를 매몰비용이 아닌 생산비용으로 인식할 필요가 있다고 판단된다. 나아가 조직성과에 기여하는 정보보호의 구현은 정보보호 성숙도의 매개적 역할을 이용하는 것이 효과적임을 시사해 주고 있다.

본 연구의 의의는 정보보호의 조직성과를 침해사고 예방이라는 소극적 관점에서 벗어나 경제적 관점의 신규 서비스 및 기술에 대한 투자 효과, 표준 준수를 통한 서비스 품질 향상까지 확장하였다는 데서 찾을 수 있다. 실무적으로 정보보호의 효과적 구현을 위해 정보보호 성숙도를 활용하는 정책을 수립할 수 있고, 담당자의 관리역량을 높이는데 활용할 수 있으며, 마지막으로는 효과적인 정보보안 투자 및 의사결정에 기여할 수 있을 것으로 보인다.

본 연구의 한계점은 첫째, 본 연구의 분석단위가 조직과 개인으로 혼돈되는 부분은 향후 연구에서 정교한 연구모형으로 보완할 필요성이 있다. 둘째, 본 연구에서 선정한 표본이 제한된 산업분야에서 선정되었기 때문에 다른 산업분야의 결과와는 다를 수 있을 것이나, 향후에는 다양한 산업 군과 기업규모 등을 고려하여 폭 넓게 표본을 선정하면 의미 있는 연구가 될 수 있을 것이다. 셋째는 본 연구가 횡단적 연구이기 때문에 향후에는 종단적 연구를 수행하면 더 많은 시사점을 얻을 수 있을 것이다. 넷째, 조직성과에 대해 비 재무적 요소들만을 측정요소 선택하였기 때문에 한계가 있을 수 있다. 향후에는 재무적 성과를 포함하여 정보보호의 조직성과를 객관적이며 종합적으로 평가할 수 있는 측정방법의 연구와 적용이 필요할 것이다.

참고문헌

금융보안연구원, “금융IT 보안컴플라이언스,” 2011.

금융위원회, “금융회사 정보기술 보호업무 모범규준,” 2012.

김경규, 신호경, 박성식, 김범수, “정보자산보호 성과가 조직성과에 미치는 영향에 관한 연구 : 관리활동과 통제활동을 중심으로,” 정보관리연구, 제40권, 제3호, 2009, pp.61-77.

김상현, 박현선, “위치기반서비스 사용에 영향을 미치는 프라이버시 염려감소 선행요인, 신뢰 그리고 개인혁신성의 조절효과,” 한국정보시스템학회지, 제21권 제2호, 2012, pp.73-96.

김인재, 설경환, “조직성과에 미치는 SPI 영향요인에 관한 연구,” 정보시스템연구, 제19권, 제2호, 2010, pp.97-118.

백민정, 손승희, “중소규모 조직구성원의 정보보안인식과 행동이 정보보안성과에 미치는 영향에 관한 연구,” 중소기업연구, 제33권, 제2호, 2011, pp. 113-132.

배병렬, “구조방정식모델 이해와 활용,” 도서출판 대경, 2011.

송정석, 전민준, 최명길, “공공기관 정보보호 거버넌스 수준에 영향을 미치는 요인에 관한 연구,” 한국전자거래학회지, 제16권 제1호, 2011, pp.133-151.

윤재욱, 김인재(2006), “소프트웨어 프로세스 개선활동이 조직성과에 미치는 영향,” 한국경영과학회지, 제31권, 제1호, 2006, pp.37-53.

임채호, “효과적인 정보보호인식제고 방안,” 정보보호학회지, 제16권, 제2호, 2006, pp.30-36.

전자금융거래법 시행령 제 11조의2, 2012.

최명길, 황원주, 김명수, “정보보호정책의 성숙도에 영향을 미치는 요인에 관한 연구,” 한국정보보호학회지, 제18권, 제3호, 2008, pp.132-142.

한국정보보호진흥원, “인터넷 침해사고 피해액 산출모형 개발에 관한 연구,” 2006.

Agarwal, R. and Prasad, J., “A Conceptual and Operational Definition of Personal Innovativeness in the Domain of Information Technology,” Information Systems Research, vol.9 No.2, 1998, pp.204-215.

Alder, M. P., “A unified approach to information security compliance,” EDUCASE Review, Vol.41, No.5, 2006, pp.46-48.

Alshawaf, A.H., Ali, J.M.H. and Hasan, M.H., “A benchmarking framework for information systems management issues in Kuwait,” Benchmarking: An International Journal, Vol.12 No.1, 2005, pp.30-44.

Bassellier, G., Reich, B.H. and Benbasat, I., “Information Technology Competence of Business Managers: A Definition and Research Model,” Journal of Management Information Systems, Vol.17, No.4, 2001, pp.159-182.

Beznosov, K. and Beznosova, O., “On the imbalance of the security problem space and its expected consequences,” Information Management & Computer Security, Vol.15, No.5, 2007, pp. 420-431.

Bostrom, R.P., & Heinen,J.S.. "A socio-technical perspective. Part Ⅰ:The causes," MIS Quarterly, Vol.1, No.3, 1977, pp.17-32.

Bulgurcu,B.H. and Cavusoglu,H., "Roles of Information Security Awareness and Perceived Fairness in Information Security Policy Compliance," AMCIS 2009, pp.419.

Chang, S.E. and Ho, C. B., "Organizational factors to the effectiveness of implementing information security management," Industrial Management & Data Systems, Vol.106, No.3, 2006, pp.345 - 361.

Choi, N. and D. Kim, "Knowing is doing," Information Management and Computer Security, Vol.16, No.5, 2008, pp.484-501.

COBIT(Control Objectives for Information and Related Technology) 5, ISACA, 2012.

Dzazali, S. and Zolait, A. H., "Assessment of information security maturity: An exploration study of Malaysian public service organizations," Journal of Systems and Information Technology, Vol.14 No.1, 2012, pp.23 - 57.

Dzazali, S., "Social Factors Influencing the Information Security Maturity of Malaysian Public Service Organisation: An Empirical Analysis," ACIS 2006 Proceedings, 2006, pp.103.

Dhillon, G. and Backhouse, J., "Current direction in IS security research: toward socio-technical perspectives," Information System, Vol.11, No.2, 2001, pp. 127-53.

Doddrell, G.R., "Information security and the internet," Internet Research, Vol.6, No.1, 1996, pp.5-9.

Eloff, J.H.P., "Information security policy－what do international information security standards say?," Computers & Security, Vol.21, No.5, 2002, pp.402-409.

Fornell, C. and D. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," Journal of Marketing Research, Vol.18, 1981, pp.39-50.

Goldsmith, R. E., and Hofacker, C. F., "Measuring Consumer Innovativeness," Journal of the Academy of Marketing Science, Vol.19, No.3, 1991, pp.209-221.

Hagen, J.M., Albrechtsen, E. and Hovden, J., "Implementation and effectiveness of organizational information security measures," Information Management & Computer Security, Vol.16, No.4, 2008, pp.377 - 397.

Hall, J. H., Sarkani, S. and Mazzuchi, T.A., "Impacts of organizational capabilities in information security," Information Management & Computer Security, Vol.19, No.3, 2011, pp.155 - 176.

ISO27001, "ISO/IEC 27001-2005(E): Information Technology-Security Techniques-Information Security Management

Systems-Requirements," International Organisation for Standardization, Geneva, 2005.

Kankanhalli, A., Teo, H., Bernard, C.Y. and Tan, K. W., "An integrative study of information systems security effectiveness", International Journal of Information Management Vol.23, 2003, pp.139 – 154.

Knapp, K.J., Marshall, T.E., Rainer, R.K. and Ford, F.N., "Information security: management's effect on culture and policy," Information Management & Computer Security, Vol.14, No.1, 2006, pp.24-36.

Koufteros, X., and G. Marcoulides., "Product development Practices and performan ce: A structural equation modeling-based multi-group analysis," International Journal of Production Economics, Vol.103, No.1, 2006, pp.286-307.

Kowalski, S., "IT Insecurity: A Multi-disciplinary Inquiry. Diss. The Royal Institute of Technology," Department of Computer and Systems Science Stockholm Univ. Report series No 94-040, 1994.

Midgley, D. and Dowling, G. R., "Innovativeness: The Concept and Its Measurement," Journal of Consumer Research, Vol.4, No.4, 1978, pp.229-242.

NIST SP 800-30, "Guide for Conducting Risk Assessment," 2012.

NIST SP 800-33, "Underlying Technical Models for Information Technology Security," 2001.

NIST SP 800-61, "Computer Security Incident Handling Guide," 2007.

NIST SP 800-100, "Information Security Handbook: A Guide for Managers," 2007.

Peltier, T.R., "Information Security Risk Analysis," Auerbach Publications, New York, 2001.

Rogers, E. M., "Diffusion of Innovation," The Free Press, New York, 2003.

Schneier, B., "Secret and Lies – Digital Security in a Networked World," Wiley Computer Publishing, New York, 2002.

Smith, S., Stephen, G., and Malampy, W., "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, 1995, pp.28-29.

Solms, R., "Driving safely on the information superhighway," Information Management & Computer Security, Vol.5, No.1, 1997, pp.20-22.

Stanton, J.M., Stam, K.R., Mastrangelo, P. and Jolton, J., "Analysis of end user security behaviors," Computers & Security, Vol.24, No.2, 2005, pp.124-33.

Steven J. Ross, Risk Masters and ISACA, "Creating a culture of Security," 2011.

Tashi, I., “Regulatory Compliance and Information Security Assurance,” 2009 International Conference on Availability, Reliability and Security, 2009, pp.670-674.

Thomson, K. and Solms, R., “Information security obedience: a definition,” Computers & Security, Vol.24, 2005, pp.69-75.

Trist, E., “The evolution of socio-technical systems,” Vol.2, Wiley, 1981.

Werlinger, R., Hawkey, K. and Beznosov, K., “An integrated view of human, organizational and technological challenges of IT security management,” Information Management & Computer Security, Vol.17 No.1, 2009, pp.4 – 19.

Yngström, L., “A Systemic- Holistic Approach to Academic Programmes in IT Security,” Ph.D Thesis, Department of Computer and Systems Science, University of Stockholm and the Royal Institute of Technology, 1996, Stockholm.

Young, R.F, “Defining the Information Security Posture : An Empirical Examination of Structure and Managerial Effectiveness,” University of North Texas, 2008.

박정국(Jeong Kuk Park)

금융결제원 금융결제연구소 팀장으로 재직 중이다. 한양대학교에서 경제학으로 학사 학위를 받았으며(1991), 동국대학교 국제정보대학원에서 정보보호학 석사 학위(2003)를 받았다. 현재는 동국대학교 대학원 박사과정에 재학 중이다. 주요 관심 분야는 전자금융보안, 정보보호 관리체계, 전략적 IT 응용 등이다.

김인재(Injai Kim)

동국대학교 경영대학 경영정보학과 교수로 재직 중이다. 서울대학교 산업공학과 학사(1983), 한국과학기술원 경영과학 석사(1985), University of Nebraska-Lincoln 경영정보학 박사학위(1996)를 받았다. LG 전자 중앙연구소 전산실 개발팀장으로 재직하였다. 국내외 주요 저널에 다수의 논문을 발표하였다. 주요 관심 분야는 정보기술의 수용과 혁신, 소프트웨어 품질, 빅 데이터와 소셜 네트워크 분석, 정보기술을 매체로 한 커뮤니케이션, 정보보안, 감성경영, 바이오텍 클러스터, 유웰니스 등이다.

<Abstract>

A Study for Influencing Factors of Organizational Performance:

The Perspective of the Mediating Effect of Information Security Maturity Level

Jeong Kuk Park, Injai Kim

Internet environment and innovative ICT(information and communication technology) have brought about big changes to our lifestyle and industrial structure. In spite of the convenience of Internet, various cyber incidents such as malicious code infection, personal information leakage, smishing(sms + phishing), and pharming have frequently occurred. Information security must be recognized as a key and compulsory element for surviving in a global economy. Strategic roles of information security have recently been increasing, but effective implementation of information security is still a major challenge to organizations.

Our study examines the influencing factors of information security and investigates the causal relationship between information security maturity level and organizational performance through an empirical survey. According to the results of our study, personal, organizational, technical, and social factors affect organizations's information security maturity level altogether. This result suggests that when dealing with security issues, the holistic and multi-disciplinary approaches should be required. In addition, there is a causal relationship between information security maturity level and organizational performance, and organizations aim to establish the efficient and effective ways to enhance information security maturity level on the basis of the results of this study.

Key words : Information Security, Security Policy, Information Security Maturity Level, Organizational Performance, Mediating Effect

* 이 논문은 2014년 8월 4일 접수하여 1차 수정을 거쳐 2014년 9월 17일 게재 확정되었습니다.