「정보시스템연구」 제25권 제2호
한국정보시스템학회
2016년 6월, pp. 51~77

http://dx.doi.org/10.5859/KAIS.2016.25.2.51

# 조직의 정보보안 환경이 조직구성원의 보안 준수의도에 미치는 영향

황 인 호* · 김 대 진**

〈목 차〉



## Ⅰ. 서 론

정보가 기업 가치의 핵심 요건이 되면서, 기업들은 정보보안 위협 예방을 위하여 많은 비용을 투자하고 있다(이장형·김종원, 2010). 전 세계적으로 보안 분야 정보시스템 구축 시장은 2014년 710억 달러에서 2018년 1,010억 달러로 급성장할 것으로 예상되고 있다(Gartner, 2014).

조직들이 정보보안을 위하여 많은 비용을 투자함에도 불구하고 보안 위협에 대한 불확실성은 지속적으로 발생하고 있으며(김종기, 1998), 정보 노출로 인한 피해가 관련 이해관계자에게 추가적인 이슈로 나타나고 있다. 일례로 2015년 8월 애슐리매디슨이 해킹되어 1차적으로 3천 200백 만 개의 고객의 이메일과 회원 정보가 유출되었으며(9.7기가바이트 규모), 2차적으로 소스코드 까지 포함되어 20기가바이트 규모의 정보가 유출되었다. 애슐리매디슨에 대한 해킹 사고는 정보 유출로 인하여 기업 경쟁력을 매우 약화시켰을 뿐만 아니라, 회원정보 유출로 인한 수많은 고객들의 가정 문제 및 사회적 문제로 그 이슈가 확대되었다. 국내의 경우, 국가

* (사)한국창업경영연구원, 정보전략 연구팀장, hwanginho@nate.com, 주저자
** 중앙대학교 경영학과 시간강사, yauchee@empas.com, 교신저자

정보원 산업기밀보호센터에 따르면 2005년~2014년 간 내부자에 의해 국내 첨단 기술을 해외로 불법으로 유출했거나 유출을 시도한 사건은 총 438건, 연평균 50조 원 피해로 나타났으며, 적발건수는 날로 급증하고 있는 것으로 나타났다(보안뉴스, 2015).

조직에서 발생 가능한 정보보안 사고 형태를 살펴보면, Loch et al.(1992)는 보안사고 원천을 행위 주체(Human, Non-human)와 침입 경로 관점(Internal, External)으로 분류하여 4가지 유형을 제시하였다. External / Non-Human 사례는 자연재해가 있으며, 이는 조직 차원의 보안 통제로 해결이 불가능한 경우이다. Internal / Non-human, External / Human 사례는 해킹에 의한 보안사고가 해당된다. 이는 조직의 정보보안 시스템에 대한 기술적 개선을 통하여 통제가 가능하다. 반면, Internal / Human의 경우 조직 정보 시스템에 대한 접근 권한이 부여된 내부 조직원에 의해 발생하는 문제이다. 그들은 내부자에 의한 정보보안 사건 발생가능성에 대한 통제와 예방이 가장 어려운 형태라고 하였다. 실제로 Verizon(2013) 정보보안 보고서에 따르면, 조직의 증명된 데이터 유출 사고 가운데 14%가 내부자에 의해 발생하였으며, 지속적으로 그 비율이 증가하고 있다고 하였다. 또한 데이터 유출자는 일반 사무직, 임원 등 IT 시스템 관리 업무 유형과 무관한 것으로 나타났다. 즉, 조직의 정보시스템에 접근 가능한 조직원은 모두가 정보 보안 관련 사고를 일으킬 수 있기 때문에, 정보보안 통제에 대한 불확실성은 높다고 할 수 있다(황인호 등, 2016; Whitman, 2004).

West(2008)는 내부자에 의한 정보보안 불확실성이 발생하는 원인을 조직원의 심리적인 관점에서 살펴보고 있다. 그는 일반적으로 조직에서 조직원의 개인적인 업무 목표는 조직의 정보보안 목표와 같지 아니하고, 조직원이 조직이 요구하는 수준의 정보보안을 지키는 것에 대한 정확한 비용과 혜택에 대한 측정을 할 수 없기 때문에, 정보보안에 대한 문제가 발생 시 회피하려는 행동을 한다고 보았다. 즉, 조직원의 정보보안 위반은 자신이 얼마나 심각하게 보안을 위반했는지를 명확하게 인식하지 못하기 때문에, 보안 미준수 행동이 일어난다(Stanton et al., 2005). 또한, 조직원은 자신의 보안 행동을 합리화하기 위하여 긍정 또는 부정적인 측면의 보안 환경 및 분위기 등에 편승하고자 한다(Siponen and Vance, 2010). 즉, 조직 내부의 정보보안 수준을 높이기 위해서는 조직원의 자발적인 보안 준수를 위한 접근이 필요하다.

조직원의 정보보안 준수 행동 수준을 높임으로써 보안 문제를 해결하기 위해 진행된 선행연구를 살펴보면, 대부분 조직원 차원의 보안 동기 개선 측면으로 접근하고 있다(D'Arcy et al., 2009; Guo et al., 2011; Herath and Rao, 2009; Ifinedo, 2011; Lee and Larsen, 2009). 선행 연구들의 공통점은 조직의 정책 및 규정 등에 대한 조직원의 심리적 태도에 초점을 맞추고 있다. 즉, 조직의 정보보안 사고 위협을 최소화하기 위하여 보안에 대한 조직원의 동기를 변화시키기 위한 조직의 노력을 강조한다.

하지만, 조직원은 조직의 보안 환경과 자신이 보유한 보안관련 제한된 정보를 결합하여 최선이 아닌 차선의 선택을 한다 (Hu et al., 2011). 즉, 조직원의 정보보안 준수 행동은 조직에 의해 구성된 보안 환경적 요인과 보안 준

수의 필요성과 불필요성을 가지게 하는 인지적 요인을 함께 고려함으로써 준수의도를 가지게 된다(West, 2008). 하지만, 복잡한 조직의 보안 환경에서 조직원의 보안 준수의도를 높이거나 감소시키는 동기적 요인을 찾는 연구는 아직 미진하다. 또한, 조직원의 보안 준수에 영향을 미치는 원인을 파악하기 위하여, 조직이 수행하고 있는 보안 행동과 동기적 요인간의 관계에 대한 연구가 아직 미진하다.

따라서 본 연구에서는 첫째, 선행 연구를 통해 정보보안 환경에 대한 조직원의 인식 요인(물리적 시스템 구축, 보안 커뮤니케이션), 조직원의 정보보안 준수의도 강화(조직 몰입, 동료 행동) 및 억제 요인(보안 시스템 걱정, 업무 장애)들을 제시하고 영향 관계를 찾고자 한다. 둘째, 조직에서 정보보안 준수의도를 강화 및 억제시키는 요인들과 준수의도와의 영향 관계를 찾고자 한다. 이를 통해 조직의 보안 관련 행동과 조직원간의 보안 준수의도간의 관계를 설명하고, 보다 체계적인 보안 구조화를 위한 시사점을 제시하고자 한다.

본 연구는 총 5개 단락으로 구성되어 있다. 첫째, 연구의 배경 및 목적을 설명한다. 둘째, 선행 연구를 기반으로 관련 이론 및 연구 가설을 제시한다. 셋째, 연구 방법을 설명한다. 넷째, 연구 모델의 타당성과 신뢰성을 파악하고, 연구가설을 검증한다. 마지막으로 본 연구의 시사점과 향후 연구 방향을 제시한다.

# Ⅱ. 이론적 배경

## 2.1 제한된 합리성 관점

합리적 선택(Rational Choice)은 경제적 편익의 극대화의 관점에서, 사람이 추구하는 선호에 따라 비용과 혜택의 관점으로 자신의 행동을 합리화하는 것을 지칭한다(Bulgurcu et al., 2010). 그러나 정말 사람들은 합리적인가? 에 대한 질문에 Simon(2000)은 사람의 합리성에 대하여 재해석을 하고 있다. 그는 사람들은 자신이 가지고 있는 문제 크기에 비해 보유하는 정보와 정보 처리 능력에 제약을 가지고 있으며, 완벽성과 정확성을 지킬 수 없다고 보았다. 또한 여러 제약 상황에서 개인은 최선의 선택이 아닌 차선의 판단과 결정을 하며, 정보처리자로서의 자신이 나름대로 구조화를 함으로써 의사결정의 방향성을 가진다고 보았다. 즉, 사람은 제한된 정보에 기반한 의사결정을 하게 되며, 이를 제한된 합리성(Bounded Rationality)이라 한다(Sims, 2003).

Todd and Gigerenzer(2003)는 조직과 개인의 관점에서 제한된 합리성을 접근하였으며, 제한된 합리성은 개인의 내적 인지 구조와 외적 환경 구조의 적합성(Fit) 관점에서 결정된다고 하였다. 그들은 이러한 합리성을 '생태학적 합리성(Ecological Rationality)개념으로 정의하였으며, 제한된 합리성을 확장하였다. 즉, 개인의 의사결정은 자신이 가진 정신적인 측면과 환경을 동시에 고려하기 때문에, 자신이 보유한 두 가지 측면의 정보를 기반으로 차선을 선택하는 또 다른 합리성이라고 하였다.

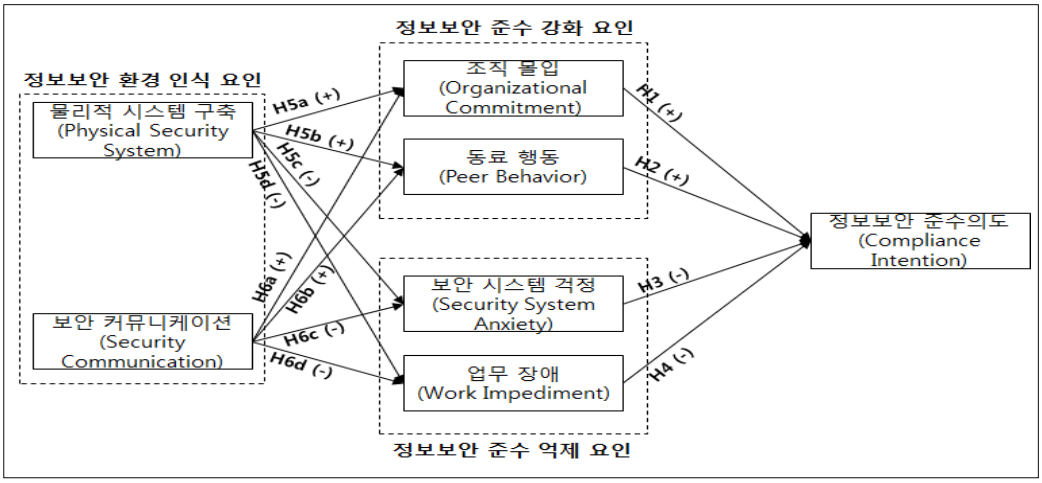
정보보안 영역에서 제한된 합리성은 조직원이 제한된 정보를 보유한 상태에서 정보보안 준수 여부를 결정할 때 고려하는 선행요인으로 활용되고 있다(Hu et al., 2011; West, 2008). 조직원은 조직의 정보보안 정책은 너무 복잡하고

이행하기 어려우며, 본연의 업무 목표를 달성하기 위해서는 보안을 지키는 것은 오히려 해가 될 수 있다고 생각한다(West, 2008). 반대로, 조직원이 조직에 대한 일체감이나 충성도를 가질 경우 조직의 보안 목표에 맞는 행동의 필요성을 인식한다(Santon et al., 2003). 즉, 조직원이 보유한 내적 감정은 긍정적인 부분과 부정적인 부분이 혼재해 있다. 더불어, 조직원은 그들이 속한 조직의 정보보안 행동 수준을 고려하여, 차선의 행동 의도를 가진다. Herath and Rao(2009b)는 조직원 주위의 동료행동에 의해 준수행동을 결정한다고 하였다. 즉, 조직원은 조직에서 자신을 둘러싼 주변사람들의 준수행동 수준과 자신의 내적 감정들을 고려하여 차선을 선택하며, 이러한 결과가 미준수 행동으로 나타날 수도 있다(West, 2008).

따라서 본 연구는 제한된 합리성의 관점에서, 조직원의 정보보안 준수에 미치는 영향 요인을 도출하기 위하여 정보보안 준수 강화 관점과 정보보안 준수 억제 관점을 통합적으로 고려하여 제시한다. 또한, 조직에서 제공하는 정보보안 환경 인식 수준이 조직원의 정보보안 준수의도의 선행 요인에 미치는 영향 관계를 제시한다. 이를 통해 정보보안 환경, 조직원의 내적 감정, 그리고 자신을 둘러싼 보안 행동 수준을 고려했을 때 발생하는 조직원의 정보보안 준수의도 변화 요인을 제시한다.

## 2.2 조직원 정보보안 준수의도

조직의 정보보안 사고 유형 중 보안 통제의 불확실성이 높은 유형이 내부자에 의한 정보보안 미 준수 유형이다(Straub and Welke, 1998). 조직은 정보보안 정책을 반영한 시스템 도입을 통하여 보안측면에서 조직원을 통제하고자 하지만, 조직원은 자신을 둘러싼 보안 환경 및 내적 동기 등을 통하여 선택적 의사결정을 한다(Hu et al., 2011). 이러한 보안 환경에서 정보보안 수준을 높이기 위해서는 조직원의 자발적인 정보보안 준수 행동에 대한 의지가 필요하며,




<그림 1> 연구 모델

조직은 이러한 의지를 향상시키기 위한 노력이 필요하다(김종기 등, 2008; 김대진 등, 2016; D'Arcy et al., 2009; Guo et al., 2011; Ifinedo, 2011). 또한 정보보안 준수의도를 조직이 요구하는 방향으로 전환시킴으로써, 조직의 정보보안 활동 수준이 높아질 수 있다(Siponen et al., 2010).

정보보안 준수의도(Compliance Intention)의 개념적 정의를 살펴보면, Bulgurcu et al.(2010)은 조직의 정보와 기술 자원에 대한 잠재적 보안 위협을 보호하기 위한 조직원의 의도라고 정의하였으며, Vance et al.(2012)는 조직의 내부, 외부의 보안 위협으로부터 조직의 정보자원을 보호하려는 조직원의 의지로 정의하였다. 즉, 정보보안 준수의도는 조직원의 정보보안에 대한 자발적인 준수 의지를 의미한다. 그렇기 때문에, 조직은 조직원의 정보보안 준수의도를 높이기 위한 보안 준수 전략을 수립하고 조직원에게 제공하는 것이 필요하다(Bulgurcu et al., 2010).

조직에서 개인은 제한된 정보와 처리 능력으로 차선에 대한 대응을 가지기 때문에, 보안 준수의도를 결정하는 데 있어 자신을 둘러싼 환경 측면의 정보에 기반하여 형성된 보안에 대한 자신의 인지를 토대로 의사결정을 한다(Hu et al., 2011; West, 2008). 즉, 정보보안 준수는 조직 내 조직원의 업무와 조직 환경에 대한 자신의 인식, 그리고 개인의 내적 동기 등에서 준수에 대한 긍정적 측면과 부정적 측면을 복합적으로 고려함으로써 정보보안 준수의도를 가지게 될 것으로 판단할 수 있다.

따라서 본 연구는 정보보안 준수의도에 영향을 미치는 조직의 복합적인 보안 환경을 고려하였으며, 이를 통해 보안 준수 요인과 보안 미 준수 요인을 도출함으로써, 조직원의 정보보안 준수의도를 높이기 위한 방향을 제시하고자 한다.

## 2.3 정보보안 준수 선행 요인

### 2.3.1 정보보안 준수 강화 요인

(1) 조직몰입 (Organizational Commitment)

조직의 특성과 문화 등은 조직원 개개인들의 의도 및 행동들이 하나로 모여서 만들어 진다(Ernest Chang & Lin, 2007). 조직의 보안 정책에 대한 준수 또한 조직원들의 행동들이 모여 조직의 보안 수준이 결정 된다(Lee et al. 2004). 즉, 조직 목표 및 방향에 대하여 부합하고자하는 조직원들이 많을 경우, 조직은 목표 달성에 대한 합당한 행동을 할 수 있다. 조직원이 조직에 헌신하거나 일체화 하려는 성향의 정도가 몰입(Commitment)이다(Williams & Anderson, 1991). Steers(1977)는 몰입을 조직에서 개인들의 일체화 정도와 관여하고자 하는 정도로 정의하고 있으며, 조직의 목표와 가치의 수용에 대한 믿음(Belief), 조직에 노력을 하고자하는 의지(Willingness), 그리고 조직의 일원으로 남고자하는 강한 욕구(Desire)로 인하여 발생한다고 하였다.

조직에서 몰입은 조직원들 간에 차이가 있으나, 조직원들이 몰입을 하도록 조직 환경이 구축될 경우 조직원들은 더욱 헌신하는 경향이 있다(Brockner et al., 2004). 또한, 정서적인 몰입을 추구하는 조직원의 경우 그렇지 않은 조직원보다 업무 등 자신의 분야에 더 많은 노력을 기울이는 경향을 가지기 때문에(Murrell and Sprinkle, 1993), 보안 몰입을 위한 환경을 구축

하여 조직원의 몰입을 높일 수 있도록 하는 것이 중요하다(Lee et al., 2004).

이러한 조직에 대한 일체화, 관여를 포함하는 몰입은 조직원의 정보보안 준수의도에 영향을 미치는 요인이다. Li et al.(2010)는 조직원의 조직에 대한 일체화 정도가 보안 정책 준수의도를 강화시키는 선행 요인이라고 하였으며, Dugo(2007)는 조직 보안 몰입이 정보보안 준수의도를 억제하는 영향을 미친다고 하였다. 또한, Lee et al.(2004)는 조직 몰입이 개인의 준수 및 통제 의도에 영향을 미치는 변수라고 하였다. 따라서 조직 몰입은 정보보안 준수의도에 영향을 미칠 것으로 판단되며, 다음과 같은 연구 가설을 제시한다.

H1. 조직 몰입은 조직원의 정보보안 준수의도 형성에 정(+)의 영향을 미칠 것이다.

(2) 동료 행동 (Peer Behavior)

조직원들은 조직의 규범, 정책, 시스템 등의 구조적인 행동 요구사항에 대하여 자신을 둘러싼 사회적 압력에 의해서 은연중에 지시를 받는다(Johnston and Warkentin, 2010). Venkatesh et al.(2003)는 조직 내 정보시스템 수용 행동의도 결정 요인 중 사회적 영향(Social Influence)이 크게 작용하며, 성별, 나이, 경험 등에 의해 복합적으로 영향력이 나타난다고 하였다.

정보보안 관점에서, 조직원은 정보보안 행동에 대한 불확실성과 미 준수에 대한 두려움을 줄이기 위하여 동료들의 행동을 참고하여 일상적인 자신의 행동의 원천으로 가지기 때문에 (Hearth and Rao, 2009a), 조직원 정보보안 준수 기준은 동료들의 정보보안 행동 수준에 의해 결정 된다(Padayachee, 2012). 즉, 조직원의 정보보안 준수는 동료들의 준수 행동을 기반으로 의사결정이 이루어진다. 만일 자신의 정보보안 위반 행동이 조직에 발견될 경우에는, 주변 환경 및 동료들의 행동을 따라함으로써 책임에 대한 회피가 가능하다고 생각한다(Siponen and Vance, 2010).

이러한 동료들의 보안 행동은 조직원의 정보보안 준수의도에 영향을 미치는 요인이다. Chan et al.(2005)은 정보보안 준수 행동은 정보보안 분위기에 의해서 결정되고, 보안 분위기는 조직 구성원들의 실천 행동에 기반한다고 하였다. Herath and Rao(2009a)는 동료 행동이라는 외재적 동기가 보안 정책 준수의도를 강화하는 역할을 한다고 하였다. 즉, 동료의 정보보안 행동이 긍정적인 보안 준수로 이어질 경우, 조직원 자신 또한 비슷한 행동을 실행하기 위한 의도를 강화시킬 것으로 판단되며, 다음과 같은 연구 가설을 제시한다.

H2. 동료의 보안 행동은 조직원의 정보보안 준수의도 형성에 정(+)의 영향을 미칠 것이다.

### 2.3.2 정보보안 준수 억제 요인

(1) 보안 시스템 걱정 (Security System Anxiety)

걱정은 시스템 활용에 있어 개인의 내적 동기에 영향을 주는 요인이다. 정보시스템 분야에서 시스템에 대한 걱정에 대한 개념을 살펴보면, Simonson et al.(1987)은 정보시스템 사용 시 발생하는 개인의 우려 또는 두려움으로 정의하고 있다. 걱정은 개인의 시스템 활용 태도, 의도, 그리고 행동을 감소시키는 중요한 요인이며, 결과적으로 시스템 도입 목적인 업무 효율성을 감소시키는 직·간접적인 원인이 된다

(Compeau and Higgins, 1995; Venkatesh, 2000; Wilfong, 2006).

조직에서 개인의 보안 시스템 걱정은 조직 문화 및 분위기에 영향을 주기 때문에, 조직원의 정보보안 실행에 대한 걱정이 커질수록 조직의 정보보안 활동에 영향을 준다(Padayachee, 2012). 정보보안 시스템 걱정은 관련 시스템 활용의 어려움, 비 명확한 규정 및 규칙 등 개인에게 정보보안 위협 요인이 커질수록 높아진다(Brown, 2000). 정보보안 활동에서 발생하는 조직원의 보안 시스템 걱정은 추상적인 형태로 나타나며, 조직원이 보안 준수의 비용과 혜택을 평가 및 의사결정을 하는데 어려움을 제공하기 때문에 보안 준수 의지를 억제하는 역할을 한다(West, 2008). 즉, 정보보안 시스템에 대한 조직원의 걱정이 높아질수록 정보보안 준수의도는 억제될 것으로 판단되며, 다음과 같은 연구 가설을 제시한다.

H3. 정보보안 시스템 걱정은 조직원의 정보보안 준수의도 형성에 부(-)의 영향을 미칠 것이다.

(2) 업무 장애 (Work Impediment)

조직에서 조직원의 목표는 자신의 업무 목표에 대한 성과를 달성하는 것이며, 조직에서 제공하는 정보시스템의 자유로운 활용은 조직원의 목표 달성에 있어 도움을 주는 핵심 요인이다(Carr, 2003). 반면 조직은 정보보안을 위해 조직의 정보시스템 및 정보 활용 등을 통제하고, 정보 노출의 위협을 억제 및 예방하고자 한다(Loch et al., 1992). 즉, 조직의 정보보안 활동은 조직원에게 자유로운 비즈니스 활동을 제약을 하는 것이기 때문에, 조직의 정보보안 목표를 달성하는 것은 조직원의 비즈니스 기능을 저해할 수 있다(Pahnila et al. 2007).

업무 장애는 조직원들이 조직의 정보보안 요구사항 준수로 인하여 업무 절차, 행동 등의 제약이 발생되는 정도이다(Bulgurcu et al., 2011). 조직원들은 정보보안 활동이 자신들의 목표 업무 성과 달성에 방해가 된다고 판단할 경우, 정보보안 회피를 통해 업무 목표를 달성하고자 하는 경향이 있다(West, 2008). 예를 들어 조직 내·외 이해관계자들과의 정보교환, 외부 업무 활동 등을 사전에 보안팀의 승인을 받고 진행해야 한다면, 업무에 대한 불편함 또는 업무 효율성 감소를 느끼게 된다. 더불어 자신은 타인보다 위험에 덜 취약하다고 생각하는 경향이 있기 때문에 정보보안을 지키지 않더라도 자신의 행동이 외부에 알려지거나 조직에 피해를 주지 않을 것이라 판단한다(West, 2008).

Bulgrucu et al.(2010)은 업무 장애가 조직원의 정보보안 준수 태도 및 의도에 있어 비용측면의 요인이기 때문에, 조직원의 관점에서 정보보안 준수 행동을 억제 및 미 준수하게 하는 핵심 요인이라고 하였다. 즉, 정보보안으로 인한 업무 장애의 수준이 높아질수록 조직원의 정보보안 준수의도는 억제될 것으로 판단되며, 다음과 같은 연구 가설을 제시한다.

H4. 업무 장애는 조직원의 정보보안 준수의도 형성에 부(-)의 영향을 미칠 것이다.

### 2.4 조직 정보보안 환경 인식 요인

(1) 물리적 시스템 구축 (Physical Security System)

조직의 정보보안 활동은 조직의 핵심 정보, 자산 등을 외부의 위협으로부터 보호하고, 불법적인 정보기술 유출을 사전에 예방하여 조직의

가치 및 자산 손실에 대한 피해를 최소하기 위하여 운영 된다(Knapp et al., 2009). 조직차원에서 효과적인 정보보안은 조직원에 의한 정보유출을 사전에 방지하기 위하여 물리적 정보보호 시스템을 구축하는 것이다(Lee et al., 2004).

Kwok and Longley(1999)는 정보보안 시스템을 조직원의 정보자원 접근 통제 및 억제를 위한 물리적 시스템 구축 및 투자로 정의하였으며, 물리적 통제 관리, 데이터 센터에 대한 물리적 제어, 케이블 보안, 보안 설비 유지 보수 등 물리적 제어 시스템에 대한 효과적인 관리가 정보보안의 핵심 요건이라고 하였다. 또한, De Veiga and Eloff(2010)는 정보보안시스템 구축을 통해서 조직이 요구하는 수준의 조직원 정보보안 행동을 유도할 수 있는 보안 환경 및 분위기가 형성될 수 있다고 하였다. Lee and Lee(2002)는 조직에서 개인의 시스템 남용을 방지하기 위해서는 물리적 보안 시스템을 구축 및 제공하는 것이 우선적으로 고려되어야 한다고 하였다. 즉, 물리적 보안 시스템의 구축은 조직원을 직·간접적으로 통제할 수 있으며, 조직원의 보안 행동을 변화시킬 수 있는 중요 환경요인이다. 따라서 물리적 시스템 구축은 조직원의 조직 몰입 및 동료행동을 강화시키고 조직원의 보안 시스템 걱정 및 업무 장애 정도를 억제시킬 수 있는 선행 변수로 판단되며, 다음과 같은 연구 가설을 제시한다.

H5 a. 조직 차원의 물리적 보안 시스템 구축은 조직원의 조직 몰입에 정(+)의 영향을 미칠 것이다.

H5 b. 조직 차원의 물리적 보안 시스템 구축은 조직원의 동료 행동에 정(+)의 영향을 미칠 것이다.

H5 c. 조직 차원의 물리적 보안 시스템 구축은 조직원의 보안 시스템 걱정에 부(-)의 영향을 미칠 것이다.

H5 d. 조직 차원의 물리적 보안 시스템 구축은 조직원의 업무 장애에 부(-)의 영향을 미칠 것이다.

(2) 정보보안 커뮤니케이션 (Security Communication)

Moore and Benbasat(1991)는 조직 내 조직원들에게 정보기술의 수용 및 확산을 위해서는 시스템 적용에 의한 혁신의 불확실성을 감소시키는 것이 중요하며, 지속적인 정보 제공과 같은 가시적 활동이 불확실성 감소에 도움을 준다고 하였다. 커뮤니케이션은 특정 시스템 및 활동에 대하여 이해하고, 능동적 행동을 할 수 있도록 지원 및 공유함으로써 가시성을 확보하는 조직 및 개인 차원의 활동이다(Jimenez-Castilo and Sanchez-Perez, 2013).

많은 기업들은 미팅, 인트라넷, 이메일 등을 통해 관련 지식을 얻고 공유할 수 있도록 노력을 한다. 즉, 커뮤니케이션 활동을 통해 기업은 나타날 수 있는 부정적 영향을 회피하고, 인지된 정보 품질을 향상시키고, 조직원들과 관련 정보를 공유할 수 있다(Sinkula, 1994). Siponen et al.(2010)은 정보보안 정책을 조직원이 준수할 수 있도록 보안 캠페인, 동영상 제공, 이메일 활동 등 다양한 방법을 실시할 경우 조직구성원의 행동에 영향을 준다고 하였다. 또한 정보보안에 대한 필요 기술, 절차, 통제 방법 등의 정보를 지속적으로 제공할 경우, 조직원의 보안 지식수준과 보안 문화 수준이 높아진다(Faily and Flechais, 2010; Wang, 2010). 따라서 보안 커뮤니케이션은 조직원의 조직 몰입 및 동료행동을 강화시키고 조직원의 보안 시스템 걱정 및 업

무 장애 정도를 억제시킬 수 있는 선행변수로 판단되며, 다음과 같은 연구 가설을 제시한다.

H6 a. 조직 차원의 보안 커뮤니케이션 활동은 조직원의 조직 몰입에 정(+)의 영향을 미칠 것이다.

H6 b. 조직 차원의 보안 커뮤니케이션 활동은 조직원의 동료 행동에 정(+)의 영향을 미칠 것이다.

H6 c. 조직 차원의 보안 커뮤니케이션 활동은 조직원의 보안 시스템 걱정에 부(-)의 영향을 미칠 것이다.

H6 d. 조직 차원의 보안 커뮤니케이션 활동은 조직원의 업무 장애에 부(-)의 영향을 미칠 것이다.

## Ⅲ. 연구 방법

선행연구를 기반으로 본 연구는 조직원의 정보보안 준수의도에 영향을 미치는 요인들을 정보보안 환경 인식 (물리적 보안 시스템 구축, 보안 커뮤니케이션) 요인, 정보보안 준수 강화 (조직 몰입, 동료 행동) 및 억제 (보안 시스템 걱정, 업무 장애) 요인들을 제시하고 정보보안 준수의도 간의 영향관계를 분석하고자 한다. 이를 위하여 도출한 연구 모델은 <그림 1>과 같다. 본 연구 가설을 검증하기 위하여 구조방정식 모델을 사용하였다. 또한 선행 연구를 기반으로 연구 변수를 구성하였으며, 서베이 기법을 통하여 자료를 수집하였다.

### 3.1 연구변수 구성

연구 모형의 구성요소를 측정하기 위한 측정도구는 2단계로 진행하였다. 우선 선행 연구를 통해 관련 변수의 설문항목을 본 연구의 내용에 적합하게 수정 및 보완하였다.

우선 조직 보안 환경 요인(물리적 시스템 구축, 보안 커뮤니케이션)을 측정하기 위하여 각 설문항목의 선행연구에서 제시한 개인이 생각하는 조직 보안 환경 요인의 인식 수준의 측면으로 파악한다. 물리적 시스템 구축은 “조직원이 조직의 정보보안 시스템 도입을 위하여 투자하고 있다고 느끼는 정도”로 정의하며, Lee et al.(2004)의 연구를 기반으로 3개의 설문항목을 도출하였다. 보안 커뮤니케이션은 “정보보안 준수를 위해 조직에서 조직원들에게 정보보안 관련 정보를 제공해준다고 느끼는 정도”로 정의하며, Jimenez-Castilo and Sanchez-Perez (2013)의 연구를 기반으로 3개의 설문항목을 도출하였다.

그리고 조직원의 정보보안 준수 강화요인과 억제 요인, 그리고 준수의도는 조직원의 인지 수준의 측면으로 파악한다. 조직 몰입은 “조직원이 조직의 목표와 가치를 이해하고 일체화하려는 성향 정도”로 정의하며, Herath and Rao (2009b)의 연구를 기반으로 3개의 설문항목을 도출하였다. 동료행동은 “자신의 주변 동료들이 정보보안을 잘 준수하고 있다고 믿는 정도”로 정의하며, Herath and Rao(2009a)의 연구를 기반으로 3개의 설문항목을 도출하였다. 보안 시스템 걱정은 “조직의 보안 시스템에 대하여 자신이 느끼는 걱정 수준”으로 정의하며, Venkatesh et al.(2003)의 연구를 기반으로 4개의 항목을 도출하였다. 업무 장애는 “정보보안으로 인한 자신의 업무에 지장을 받는 정도”로 정의하며, Bulgrucu et al.(2010)의 연구를 기반으로 4개의 항목을 도출하였다. 그리고 정보보

안 준수의도는 “조직의 정보보안을 준수하려는 의지 수준”으로 정의하며, Herath and Rao (2009b)와 박철주와 임명성(2012) 연구를 기반으로 5개의 항목을 사용하였다. 즉, 연구 모형의 구성요소들은 조직원 관점에서 조직의 정보보안 환경 수준 인식 및 준수 의도와 관련된 여러 요인들을 측정한다. 각 측정 변수들은 7점 리커트 척도를 사용하였으며, “매우 그렇지 않다 (1점)”에서 “매우 그렇다 (7점)”로 설문 문항을 구성하였다.

다음으로 국내 정보보안 상황에 적합한 설문 보완을 위하여, 도출한 설문 문항을 실제 정보보안 정책을 적용하고 있는 기업에 다니는 10명과 정보보안 관련 20명의 대학원생들에게 측정항목에 대한 내용 타당성 (Content Validity) 검정을 실시하였다. Conbach’s Alpha 값이 0.6 이하로 나타난 변수가 없어 최종적으로 설문 항목을 확정하였다. 본 연구에서 사용한 변수 및 세부 항목은 다음 <표 1>과 같다.

<표 1> 연구 변수 구성

| 변수 | 세부 항목 | 관련문헌 |
|---|---|---|
| 물리적 시스템 구축 | 우리 조직의 정보보안 시스템은 효율적으로 사용하도록 구축되어 있다(Sys1).<br>우리 조직은 정보보안 시스템 구축을 위한 투자를 적절히 한다(Sys2).<br>우리 조직은 정보보안 시스템에 대한 예산을 충분히 배정한다(Sys3). | Lee et al.(2004) |
| 정보 보안 커뮤니케이션 | 우리 조직은 정보보안 정책 정보를 전달하는 사내 커뮤니케이션 채널 또는 도구(툴)를 제공한다 (SC1).<br>우리 조직은 정보보안의 목적과 가치를 직원들에게 제공한다(SC2).<br>우리 조직은 다양한 내부 매체(사내방송, 그룹웨어 등)를 통해 정확한 정보보안 행동지침을 제공한다(SC3). | Jimenez-Castilo and Sanchez-Perez (2013) |
| 조직 몰입 | 나는 우리 조직의 성공을 위해 기대 이상으로 기꺼이 노력할 것이다(OC1).<br>나는 정말로 우리 조직에 운명에 관심을 가지고 있다(OC2).<br>나에게 우리 조직은 업무 이행하는데 더할 나위 없이 좋다(CO3). | Herath and Rao (2009b) |
| 동료 행동 | 조직 내 다른 직원들이 보안 정책을 잘 준수하고 있다고 믿는다(PB1).<br>우리 직원들은 보안정책을 잘 지키고 있다고 말할 수 있다(PB2).<br>다른 직원들이 조직 보안 정책을 지키는 것은 조직의 정보보호에 도움을 주기 위한 것이다(PB3). | Herath and Rao (2009a) |
| 정보보안 시스템 걱정 | 나는 정보 보안 시스템을 사용하는 방법에 대한 우려를 느낀다 (SA1) (제외).<br>나는 정보 보안 시스템을 잘못 활용해서 정보를 잃을 수 있다고 생각한다(SA2) (제외).<br>나는 해결할 수 없는 실수가 있을 수 있어 보안 시스템 사용을 망설인다(SA3).<br>정보 보안 시스템은 나에게 다소 위협적이다(SA4). | Venkatesh et al. (2003) |
| 업무 장애 | 조직의 정보보안 요구사항을 준수하는 것은 실제 업무 수행을 지연시킨다(WI1) (제외).<br>조직의 정보보안 요구사항을 준수하는 것은 동료, 고객, 관리자 등에 대한 대응 시간을 느려지게 한다(WI2).<br>조직의 정보보안 요구사항을 준수하는 것은 업무 생산성을 저해한다(WI3).<br>조직의 정보보안 요구사항을 준수하는 것은 업무 효율성을 저해한다(WI4). | Bulgrucu et al. (2010) |
| 정보보안 준수의도 | 나는 우리 조직의 정보보안 정책을 지속적으로 따를 것이다(SCI1).<br>나는 우리 조직의 정보시스템을 보호하기 위해 조직의 정보시스템 보안 정책을 지속적으로 준수할 가능성이 높다(SCI2).<br>나는 우리 회사의 정보 시스템을 접속할 때마다 정보보안 정책을 준수할 것이다(SCI3).<br>나는 업무를 수행할 때마다 정보보안 절차를 준수할 것이다(SCI4).<br>나는 조직의 정보 보안 정책을 준수하겠다는 나의 태도에 대해 확신을 느낀다(SCI5). | 박철주・임명성 (2012)<br>Herath and Rao (2009a) |

### 3.2 자료 수집

본 연구는 조직의 정보보안 수준을 높이기 위하여 조직원 관점에서 정보보안 준수의 중요성을 인식하고, 정보보안 준수의도에 영향을 미치는 선행 요인과 조직 환경과의 관계를 도출하는 것을 목적으로 한다.

연구 목적에 맞는 실증분석을 위하여, 연구 설문 대상을 다음과 같이 설정하였다. 정보보안 정책 및 시스템을 도입 및 활용하고 있는 조직에서 근무하고 있으며, 개인의 업무에 정보보안 정책을 적용하고 있는 조직원들을 대상으로 한다. 정보보안 부서에서 근무하는 조직원들은 자신들의 업무 성과가 정보보안 예방 및 관리이기 때문에 본 연구의 목적에 맞지 않아 제외한다.

설문은 평생 교육원에서 수업을 듣는 직장인을 대상으로 하되, 연구진이 직접 수업 전에 방문하여 연구의 목적과 필요성을 명확하게 전달한 후 설문을 실시하였다. 정보보안 정책 및 시스템이 없는 조직에서 근무하는 직장인은 제외하였으며, 조직의 정보보안에 대하여 알고 있는 직장인들에게만 설문지를 제공하였다. 또한, 설문을 수행한 직장인들의 추천으로 각 지점을 방문하였으며, 같은 방식으로 설문을 진행하였다. 설문이 가능한 사람들은 설문지를 즉석에서 회수하였으며, 그렇지 못한 사람들은 이메일로 설문을 회수하였다.

설문기간은 2014년 5월 한달동안 진행되었다. 설문 결과 총 457개의 샘플이 수집되었으며, 이중 응답에 문제가 있는 42개의 샘플을 제외한 415개의 샘플을 본 분석에 적용하였다.

## Ⅳ. 가설 검증

### 4.1 설문응답자의 표본특성

설문 응답의 인구통계학적 특성은 다음 <표 2>와 같다. 총 415명의 응답 중 남성 208개 (50.1%), 여성 207개 (49.9%)가 수집되었으며, 업종는 제조업 117개 (28.2%), 서비스업 298개 (71.8%)가 수집되었다. 세부적으로 제조업 중 가 자동차 분야 (35개), 화학분야 (28개), 전기전자분야 (14개)가 가장 많았으며, 서비스업의 경우 금융 및 보험 분야 (213개), 방송통신 분야 (28개)가 가장 많은 것으로 나타났다. 연령, 업력, 그리고 직급은 각각 고르게 응답하여 대표성을 가지는 것을 확인하였다.

<표 2> 인구통계학적 특성

| 구분 | | 빈도 | 비율(%) |
|---|---|---|---|
| 합계 | | 415 | 100.0 |
| 성별 | 남성 | 208 | 50.1 |
| | 여성 | 207 | 49.9 |
| 연령 | < 30 | 114 | 27.5 |
| | 31~40 | 156 | 37.6 |
| | 41~50 | 115 | 27.7 |
| | > 50 | 30 | 7.2 |
| 업종 | 제조업 | 117 | 28.2 |
| | 서비스업 | 298 | 71.8 |
| 업력 | < 5년 | 136 | 32.8 |
| | 6~10년 | 83 | 20.0 |
| | 11~15년 | 71 | 17.1 |
| | 16~20년 | 41 | 9.9 |
| | > 21년 | 84 | 20.2 |
| 직급 | 사원 | 152 | 36.6 |
| | 대리 | 85 | 20.5 |
| | 과장 | 76 | 18.3 |
| | 차/부장 | 88 | 21.2 |
| | 임원 | 14 | 3.4 |

### 4.2 신뢰도 및 타당성 분석

연구의 구조모형 분석에 앞서 측정항목의 신뢰성과 타당성 검증을 실시하였다.

첫째, 신뢰도는 연구 대상에 대하여 반복 측정 하였을 때, 결과가 얼마나 일관성 있게 나타나는 가를 판단하는 개념으로, 내적 일관성(Internal Consistency)을 이용하여 신뢰도를 측정한다. 내적 일관성이란 동일한 개념을 측정하기 위해 여러 개의 항목을 이용할 경우 Cronbach's Alpha 계수를 이용하여 신뢰도를 저해하는 항목을 측정도구에서 제외시킴으로써 각 항목들의 내적 일관성을 높이는 방법이다. 신뢰성 검정 기준치는 0.7이상으로서 (Nunnally, 1978), 총 7개의 잠재변수를 측정하기 위해 25개의 항목을 분석하였다. 이중 정보보안 걱정 변수 2개, 업무 장애 변수 1개를 제외한 22개의 항목이 내적일관성을 보유하고 있는 것으로 나타났다. 즉, Cronbach's Alpha 계수가 0.843에서 0.968으로 나타나 권장치이상으로 신뢰성은 확보된 것으로 나타났다. 또한 변수의 구성항목들의 표준적재치 살펴보았다. 표준적재치는 엄격하게는 0.7이상을 요구하기도 하나, 구조방정식 모델링일 경우 일반적으로 0.5이상일 경우 문제는 발생하지 않는다(Tarafdar et al., 2007). 분석 결과 동료행동 항목이 0.619로 가장 낮게 나타났다.

둘째, 연구 변수들이 상이한 개념으로 되어 있는지를 점검하기 위하여 타당성 분석을 실시한다. 타당성 분석은 공분산 구조를 이용한 모수추정법을 기반으로 한 확인적 요인분석을 실시하여 적합도 검증을 하고, 적합도가 기준치 이상으로 도출될 때, 도출된 값을 이용하여 집중타당성 (Convergent Validity)과 판별 타당성 (Discriminant Validity)을 통해 검정한다.

분석 도구로는 AMOS 18.0을 사용하였으며, 전체 구성 개념에 대한 확인적 요인 분석의 적합도를 검정하였다. 적합도 검정의 판단 기준은 사회과학 연구에서 일반적으로 사용되는 상대적 카이스퀘어(X2/df), 적합지수(GFI), 수정된 기초부합지수(AGFI), 기대교차타당성지수 (CFI), 표준적합지수(NFI), 표준적합지수 (RMSEA)를 사용하였다. 적합도 검정 결과는 전체적으로 수용할 수 있는 수준으로 나타났다 <표 3>.

<표 3> 확인적 요인분석에 대한 적합도 결과

| 변수 | χ2/df | GFI | AGFI |
|---|---|---|---|
| 분석 결과 | 2.487 | 0.911 | 0.877 |
| 권고 사항 | < 3 | > 0.9 | > 0.8 |
| 변수 | CFI | NFI | RMSEA |
| 분석 결과 | 0.974 | 0.958 | 0.06 |
| 권고 사항 | > 0.9 | > 0.9 | < 0.1 |

타당성은 집중 타당성과 판별 타당성을 통해 검정하였다. 집중 타당성은 확인적 요인 분석 결과 중 개념 신뢰도(Construct Reliability)와 평균분산추출(Average Variance Extracted) 값을 사용하였다. 개념 신뢰도는 그 값이 0.7이상, 평균분산추출은 0.5 이상을 요구한다(Wixom and Watson, 2011). 개념 신뢰도를 계산한 결과 정보보안 걱정 (0.754)이 가장 낮은 값으로 나타났고, 평균분산추출지수는 업무장애가 가장 낮은 값으로 나타나 (0.604) 모두 권장치 이상으로 결과가 도출되어 개념 신뢰도를 확보하였다<표 4>.

<표 4> 측정 모형의 신뢰성 및 타당성 검증

| 변수 | 측정항목 명 | 표준적재치 | Cronbach's Alpha | Construct Reliability | Average Variance Extracted |
|---|---|---|---|---|---|
| 물리적 시스템 구축 | Sys1 | 0.786 | 0.947 | 0.894 | 0.739 |
| | Sys2 | 0.846 | | | |
| | Sys3 | 0.816 | | | |
| 정보보안 커뮤니케이션 | SC1 | 0.821 | 0.934 | 0.856 | 0.665 |
| | SC2 | 0.794 | | | |
| | SC3 | 0.793 | | | |
| 조직 몰입 | OC1 | 0.826 | 0.948 | 0.904 | 0.758 |
| | OC2 | 0.848 | | | |
| | OC3 | 0.802 | | | |
| 동료 행동 | PB1 | 0.715 | 0.937 | 0.897 | 0.744 |
| | PB2 | 0.747 | | | |
| | PB3 | 0.619 | | | |
| 보안시스템 걱정 | SA3 | 0.789 | 0.843 | 0.754 | 0.607 |
| | SA4 | 0.877 | | | |
| 업무 장애 | WI2 | 0.906 | 0.927 | 0.820 | 0.604 |
| | WI3 | 0.902 | | | |
| | WI4 | 0.902 | | | |
| 정보보안 준수의도 | SCI1 | 0.804 | 0.968 | 0.956 | 0.814 |
| | SCI2 | 0.829 | | | |
| | SCI3 | 0.821 | | | |
| | SCI4 | 0.812 | | | |
| | SCI5 | 0.789 | | | |

더불어, 판별 타당성 검증을 위하여 평균분산추출 값과 피어슨 상관관계 분석 비교 방법을 사용하였다(Fornell and Lacker, 1981). 판별 타당성은 구성개념의 상관관계가 평균분산추출의 제곱근 보다 낮아야 한다. 분석 결과, AVE 값의 제곱근이 종과 횡의 상관계수 값보다 높게 나타나 판별 타당성의 문제가 없는 것으로 나타났다 <표 5>. 측정 모형에 대한 신뢰성 및 타당성 검정 결과는 모든 설문문항의 내적 일관성과 타당성을 통계적으로 적합함을 증명하고 있다.

각 변수들의 상관관계 분석 결과, 상관관계가 다소 높은 것으로 나타나, 독립변수들에 대한 다중공선성의 가능성을 알아보았다. 독립변수의 다중공선성은 공차한계와 분산팽창요인(Variance Inflation Factor : VIF) 으로 분석하였다. 구조방정식 모델에서 VIF가 4이상, 공차한계가 0.1 이하 일 때 다중공선성이 존재한다고 판단한다(Walpole et al., 1993).

첫째, 물리적 시스템, 보안 커뮤니케이션 요인에 대한 다중공선성 분석결과, 물리적 시스템과 보안 커뮤니케이션의 공차는 0.558, VIF는 1.794로 나타났다. 둘째, 보안 몰입, 동료 행동, 보안 걱정, 업무 장애에 대한 다중공선성 분석결과, 조직일치 (공차=0.537, VIF=1.863), 동료 행동 (공차=0.486, VIF=2.058), 보안 걱정 (공차=0.707, VIF=1.414) 그리고 업무장애 (공차=0.833, VIF=1.200) 모두 공차와 VIF 기준에 적합한 것으로 나타났다. 즉, 모든 독립변수에 대한 다중공선성 문제는 없는 것으로 나타났다.

<표 5> 확인적 요인분석에서 구성 개념간 상관관계

| 변수 | 평균 | 표준편차 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|---|
| 물리적 시스템 구축 | 5.55 | 1.398 | **0.859** | | | | | | |
| 보안 커뮤니케이션 | 5.53 | 1.477 | .66*** | **0.815** | | | | | |
| 조직 몰입 | 5.60 | 1.346 | .47*** | .51*** | **0.871** | | | | |
| 동료 행동 | 5.71 | 1.291 | .65*** | .71*** | .66*** | **0.863** | | | |
| 정보보안 걱정 | 2.28 | 1.283 | -.51*** | -.50*** | -.43*** | -.51*** | **0.779** | | |
| 업무 장애 | 3.43 | 1.582 | -.37*** | -.29*** | -.35*** | -.36*** | .32*** | **0.777** | |
| 정보보안 준수의도 | 6.17 | 1.119 | .61*** | .61*** | .67*** | .70*** | -.53*** | -.32*** | **0.902** |

주) *** = p<0.01 / 대각선의 볼드체 값은 분산추출지수의 제곱근

## 4.3 구조 모형 분석

측정 모형에 대한 신뢰성 및 타당성 검정 후, 연구 모형에서 제시한 변수간의 인과관계를 분석하기 위하여 구조방정식(Structural Equation Modeling : SEM)을 활용하였다.

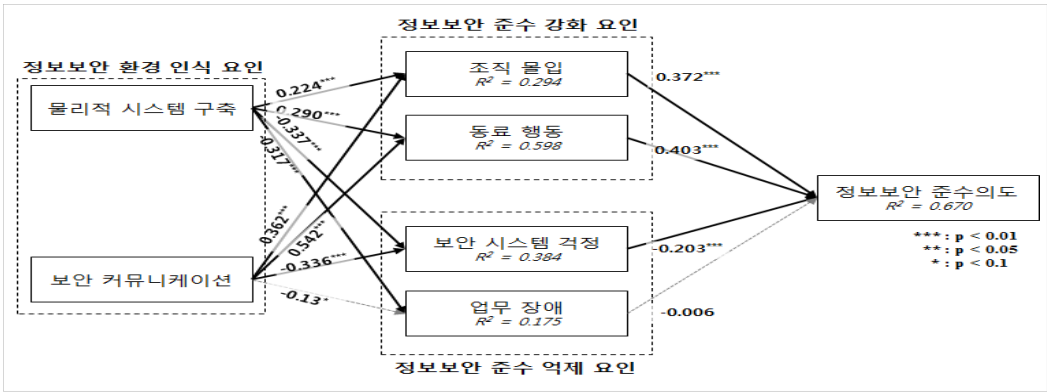
구조모형분석은 총 3가지(구조 모형에 대한 적합도 검정, 경로계수(β)를 기반한 변수들간의 영향관계 규명, 그리고 내생 변수에 대한 결정계수(R2))에 대해서 결과를 분석한다.

구조 모형에 대한 적합도 검증은 측정모형의 신뢰도 및 타당성 검증을 위하여 실시한 확인적 요인분석에서 사용한 지수를 활용하였다. 분석 결과 본 연구에 나타난 값들은 만족할 수준으로 구조방정식의 적합도를 측정하는데 무리가 없는 것으로 나타났다 <표 6>.

<표 6> 연구 모형에 대한 적합도 결과

| 변수 | χ2/df | GFI | AGFI |
|---|---|---|---|
| 분석 결과 | 2.422 | 0.910 | 0.879 |
| 권고 사항 | < 3 | > 0.9 | > 0.8 |
| 변수 | CFI | NFI | RMSEA |
| 분석 결과 | 0.975 | 0.958 | 0.059 |
| 권고 사항 | > 0.9 | > 0.9 | < 0.1 |

다음으로 경로계수(β) 를 통하여 연구 변수들간의 영향관계 및 연구가설을 검증하였다. <그림 2>, <표 7>.




<그림 2> 가설 검정 결과

<표 7> 가설검정 결과

| 가설 | | 경로 | 경로 계수 | 표준오차 | t-value | 결과 |
|---|---|---|---|---|---|---|
| H1 | | 조직 몰입→정보보안 준수의도 | 0.372 | 0.035 | 8.492*** | 채택 |
| H2 | | 동료 행동→정보보안 준수의도 | 0.403 | 0.049 | 8.253*** | 채택 |
| H3 | | 보안 시스템 걱정→정보보안 준수의도 | -0.203 | 0.032 | -5.173*** | 채택 |
| H4 | | 업무 장애→정보보안 준수의도 | -0.006 | 0.022 | -0.190 | 기각 |
| H5 | H5a | 물리적 시스템 구축→조직 몰입 | 0.224 | 0.060 | 3.603*** | 채택 |
| | H5b | 물리적 시스템 구축→동료 행동 | 0.290 | 0.039 | 5.782*** | 채택 |
| | H5c | 물리적 시스템 구축→보안 시스템 걱정 | -0.337 | 0.059 | -5.419*** | 채택 |
| | H5d | 물리적 시스템 구축→업무 장애 | -0.317 | 0.078 | -4.606*** | 채택 |
| H6 | H6a | 보안 커뮤니케이션→조직 몰입 | 0.362 | 0.056 | 5.745*** | 채택 |
| | H6b | 보안 커뮤니케이션→동료 행동 | 0.542 | 0.038 | 10.195*** | 채택 |
| | H6c | 보안 커뮤니케이션→보안 시스템 걱정 | -0.336 | 0.055 | -5.37*** | 채택 |
| | H6d | 보안 커뮤니케이션→업무 장애 | -0.13 | 0.073 | -1.886* | 기각 |

첫째, 조직 몰입이 조직원의 정보보안 준수의도에 긍정적 영향을 미칠 것이라는 가설 (H1)에 대한 검정 결과, 유의수준 5%에서 가설이 채택되었다 ($\beta$ = 0.372, P<0.01).

둘째, 동료 행동이 조직원의 정보보안 준수의도에 긍정적 영향을 미칠 것이라는 가설 (H2)에 대한 검정 결과, 유의수준 5%에서 가설이 채택되었다 ($\beta$ = 0.403, P<0.01).

셋째, 보안 시스템 걱정이 조직원의 정보보안 준수의도에 부정적 영향을 미칠 것이라는 가설 (H3)에 대한 검정 결과, 유의수준 5%에서 가설이 채택되었다 ($\beta$ = -0.384, P<0.01).

넷째, 업무 장애가 조직원의 정보보안 준수의도에 부정적 영향을 미칠 것이라는 가설 (H4)에 대한 검정 결과, 유의수준 5%에서 가설이 기각되었다 ($\beta$ = -0.006, P>0.05).

다섯째, 조직의 물리적 시스템 구축이 정보보안 준수의도 강화 및 억제 요인에 영향을 미칠 것이라는 가설 검정 결과 (유의수준 5%), 부분 가설 모두 채택되었다 (H5a : $\beta$ = 0.224, P<0.01 / H5b : $\beta$ = 0.290, P<0.01 / H5c : $\beta$ = -0.337, P<0.01 / H5d : $\beta$ = -0.317, P<0.01).

마지막으로, 조직의 보안 커뮤니케이션 활동이 정보보안 준수의도 강화 및 억제 요인에 영향을 미칠 것이라는 가설 검정 결과 (유의수준 5%), 보안 커뮤니케이션과 업무장애간의 관계를 제외한 부분가설들이 채택되었다 (H6a : $\beta$ = 0.362, P<0.01 / H5b : $\beta$ = 0.542, P<0.01 / H5c : $\beta$ = -0.336, P<0.01 / H5d : $\beta$ = -0.130, P<0.1).

또한, 구조모형 분석 추가 결과인 내생변수 (Endogenous Variable)에 대한 결정계수 (R2)를 도출하였다. 결정계수는 연구모형의 총 변동 중 외생변수(설명변수, 독립변수)들에 의해 설명되는 비율을 의미한다.

연구모형에서 제안한 조직 몰입은 물리적 시스템과 보안 커뮤니케이션이 가지고 있는 분산의 29.4%의 설명력을 가지고 있는 것으로 나타났다. 동료 행동은 물리적 시스템과 보안 커뮤니케이션이 가지고 있는 분산의 59.8%의 설명력을 가지고 있는 것으로 나타났다. 보안 시스템 걱정은 물리적 시스템과 보안 커뮤니케이션

이 가지고 있는 분산의 38.4%의 설명력을 가지고 있는 것으로 나타났다. 업무 장애는 물리적 시스템과 보안 커뮤니케이션이 가지고 있는 분산의 17.5%의 설명력을 가지고 있는 것으로 나타났다. 마지막으로, 정보보안 준수의도는 조직 몰입, 동료 행동, 보안 시스템 걱정, 그리고 업무장애가 가지고 있는 분산의 67.0%의 설명력을 가지고 있는 것으로 나타났다.

### 4.4 결과 논의

정보보안은 조직의 중요 정보 및 자산을 보호하고 조직의 이해관계자들의 권리를 보호하기 위한 핵심 조건이다. 조직들은 정보보안을 위한 투자의 중요성을 느끼고 있으며, 실제 보안 시스템에 대한 많은 투자를 하고 있다. 그럼에도 불구하고 보안 시스템 및 보안 정책을 실행에 옮기는 조직원의 정보보안 사고 위협은 감소되지 않고 있으며, 오히려 정보보안은 조직원에게 합리적인 의사결정을 어렵게 하는 원인이 되고 있다.

조직원의 정보보안 준수의도를 높이기 위하여 조직 차원의 정보보안 환경 인식 요인, 조직원의 정보보안 준수의도 강화 및 억제 요인들을 제시하고 영향 관계를 분석한 결과, 업무 장애와 준수의도와의 영향 관계를 제외한 연구 가설들이 채택되었다.

첫째, 조직 몰입과 정보보안 준수의도와의 관계는 정(+)의 영향 관계임을 검증하였다 (H1). 조직 몰입은 조직원이 조직에 헌신 및 일체화하고자 하는 정도로서(Jex and Britt, 2008), 조직원의 조직에 대한 몰입 수준이 높을수록 조직의 목표와 함께 하려는 경향을 보인다. 더욱이 조직에서 조직원의 몰입을 위한 환경을 구축할 경우 더욱 높은 몰입을 보이기 때문에, 조직원에 대한 조직 몰입을 높이기 위한 노력이 필요하다. 조직 몰입을 높이기 위해서는 보안 관련 직무 및 역할을 명확하게 조직차원에서 제공하는 것이 필요하며, 보안 목표가 조직원들에게 합리적으로 이해될 수 있도록 제시 및 전달될 수 있도록 지원하는 것이 필요하다.

둘째, 동료 행동과 정보보안 준수의도와의 관계는 정(+)의 영향 관계임을 검증하였다 (H2). 동료 행동은 주변 동료들의 정보보안 준수 행동의 정도로서(Hearth and Rao, 2009a), 동료들의 능동적인 정보보안 행동은 조직원이 정보보안 준수의 필요성을 느끼게 함으로써, 준수 의도를 높이는 선행 요인이다. 특히, 동료행동은 정보보안 준수의도에 영향을 주는 요인 중 가장 높은 영향을 미치는 요인으로 나타났는데, 이러한 결과는  자신의 보안 행동의 합리화를 위하여 소속 집단의 행동이나 가치를 활용하려하는 사람들의 속성을 제시한 Siponen and Vance(2010)의 연구와 일맥상통한다. 즉, 자신을 둘러싼 동료들의 행동 유형에 의해 자신의 행동을 합리화한다. 따라서 조직은 조직원 개별에 대한 정보보안 준수를 위한 규정 또는 정책을 제시하는 것이 아닌, 팀 또는 부서 단위의 보안 목표를 제시하거나, 부서 내 직원들간 정보보안에 대한 필요성을 논의하기 위한 자리를 지속적으로 마련함으로써, 동료들 전체가 정보보안을 지키는 분위기를 형성하는 것이 필요하다.

셋째, 정보보안 시스템 걱정과 정보보안 준수의도와의 관계는 부(-)의 영향 관계임을 검증하였다 (H3). 걱정은 특정한 것 사용에 대한 개

인의 우려 또는 두려움 정도로서(Simonson et al., 1987), 정보보안 시스템 걱정수준이 높을수록 오히려 정보보안 준수에 대한 의도가 낮아지게 된다. 즉, 조직의 보안 정책 (규정, 시스템 등)이 너무 이해하기 어렵게 되어 있거나, 복잡한 구조로 되어 있어 정확한 정보보안의 이행에 어려움이 있다고 판단될 경우, 조직원은 정보보안을 지키지 않으려고 한다. 따라서 조직은 정보보안 목표 달성을 위한 명확하고 실행 가능한 보안 규정 및 시스템 구축을 통한 지원이 필요하며, 지속적인 보안 활동 정보와 절차 등의 정보를 제공하기 위한 노력이 필요하다.

반면, 업무 장애는 정보보안 준수의도에 부(-)의 영향을 미칠 것이라는 본 연구의 가설은 부정적 영향을 미치는 것이 아닌 것으로 나타나 기각되었다 (H4). 업무 장애는 보안 활동이 업무 절차 및 행동의 제약을 발생시키는 정도이다(Bulgurcu et al., 2010). 이러한 결과는 Bulgurcu et al.(2010)가 제시한 비용적 측면의 업무장애가 잠재적으로 준수의도를 감소시킨다는 결과와 상이하다. 이는 국내의 조직과 조직원의 관계 특성을 감안해야 할 것으로 판단된다. 조직 구성원들은 조직을 우리 조직으로 판단하는 경향이 있으며, 정보보안에 의하여 업무 과중이나 제약 등이 발생하더라고 조직을 위한 성향이 강하기 때문으로 판단된다.

또한 조직원의 정보보안 준수의도 강화 및 억제 요인과 조직 차원의 정보보안 환경 요인 간의 관계를 검증하였다.

첫째, 물리적 시스템 구축이 정보보안 준수의도 강화 및 억제 요인에 각각 정(+), 부(-)의 영향을 미치는 선행 요임임을 검증하였다. 물리적 시스템은 조직원의 정보자원 접근 통제를 위한 시스템 투자 정도로서(Kwok and Longley, 1999), 조직 내 정보시스템을 다루는 조직원에 대한 물리적 보안 시스템 구축을 통한 통제는 조직 몰입과 동료 행동에 정(+)의 영향을 미치며, 보안 시스템 걱정과 업무 장애에 부(-)의 영향을 미친다. 물리적 보안 시스템을 조직에 도입한다는 것은 기존 업무에 정보보안을 결합한 새로운 측면의 업무 표준화를 도입하는 개념이므로, 업무 매뉴얼 및 가이드라인 도출이 필수적이다. 또한 조직의 최고경영층 차원의 시스템 도입에 대한 투자가 이루어지는 것을 의미하기 때문에, 보안 목표가 보다 명확해짐을 의미한다. 이를 통해 조직원의 조직 몰입을 높일 수 있으며, 주변 동료들의 보안 행동이 외적으로 보안을 준수하는 형태로 나타나게 한다. 또한, 표준화된 업무 체계로 인하여 보안 활동 요구사항이 명확하지 않을 때 나타날 가능성이 높은 보안 시스템 걱정을 감소시키는 선행 요인이다. 또한 보안 활동과 개인의 업무가 연계되도록 시스템화 되어 있고, 반드시 조직 내 구성원이면 지켜야하는 활동으로 인식될 경우 보안 시스템이 업무 장애를 일으키는 요인이라는 것을 최소화 할 수 있을 것을 판단된다. 따라서 조직원의 보안 준수의도를 높이기 위해서는 조직에서 물리적 보안 시스템을 구축 시 단순히 새로운 보안 시스템을 도입하는 개념이 아닌, 보안 목표에서부터 실제 보안 시스템 활용 방법까지 명확하게 제시하는 것이 필요하다.

둘째, 정보보안 커뮤니케이션 활동이 정보보안 준수의도 강화 및 억제 요인에 각각 정(+), 부(-)의 영향을 미치는 선행 요임임을 검증하였다. 커뮤니케이션은 특정 활동에 대하여 지원

및 공유함으로써 가시성을 확보하는 활동의 정도로서(Jimenez-Castilo and Sanchez-Perez, 2013), 조직원이 보안 활동을 제대로 할 수 있도록 보안 정보 및 활동 방법 등을 얻고 공유할 수 있도록 지원하는 것을 의미한다. 조직 내 정보시스템을 다루는 조직원들에게 보안 정보 제공 및 공유하는 커뮤니케이션 활동은 조직 몰입과 동료 행동에 정(+)의 영향을 미치며, 보안 걱정과 부분적으로 업무 장애에 부(-)의 영향을 미친다. 조직원에게 보안 활동의 목표와 방법을 정확하게 전달 할 경우 조직 몰입 수준이 높아지고, 동료들의 자발적인 보안 행동의 수준이 높아지게 할 수 있음을 의미한다. 또한 명확한 보안 정보의 수준은 조직원의 보안 이행에 대한 걱정을 감소시킬 수 있다.

반면, 보안 커뮤니케이션과 업무 장애간의 영향관계는 유의수준 5%에서 기각되었는데, 유의수준 10%로 고려 시 부(-)의 영향을 미치는 요인인 것으로 나타났다. 따라서 조직원의 시스템 보안에 의한 업무장애는 커뮤니케이션 활동으로 미약하게나마 영향을 미칠 수 있는 요인이다. 이러한 정보보안 커뮤니케이션을 통한 보안 수준을 높이기 위해서는 조직 내 다양한 정보보안 캠페인 실행, 보안 활동 방법 및 피해 관련 시각적 차원의 영상 제공, 정보보안 이메일 활동, 그리고 조직의 정보보안에 대한 지식 관리 체계 등을 갖추는 것이 필요하다.

# Ⅴ. 결 론

본 연구는 조직 정보보안의 잠재적 위협 요인인 내부자의 정보보안 준수의도 개선 방안을 제시하고자 하였다. 이를 위해 조직원의 정보보안 준수의도에 영향을 미치는 요인들을 정보보안 환경 인식, 정보보안 준수 강화 및 억제 요인들을 제시하고 정보보안 준수의도 간의 영향관계를 분석하여, 조직원의 정보보안 준수의도를 높이고, 미 준수 요인을 감소시키는 방법을 제시하였다. 각 연구 가설에 대한 검증 결과, 업무 장애와 정보보안 준수의도간의 영향관계와 정보보안 커뮤니케이션과 업무 장애간의 영향 관계를 제외한 각 연구 가설이 채택되었다. 본 연구 결과의 시사점과 연구의 한계점은 다음과 같다.

## 5.1 연구의 시사점

본 연구는 조직과 조직원간의 관계에서 정보보안 준수의도에 영향을 미치는 요인들을 도출하고 영향 관계를 검정하였고, 각 영향 관계별 논의를 진행하였다. 이를 통하여 본 연구는 이론적 측면과 실무적 측면의 시사점을 제시한다.

첫째, 본 연구는 조직원의 정보보안 준수의도에 영향을 주는 요인을 제한된 합리성의 관점에서 정보보안 준수의도 강화 및 억제 요인을 제시하였으며, 관련 영향관계를 검증하였다. 기존 조직원의 보안 준수를 위한 선행연구는 대부분, 합리적 의사결정의 관점에서 준수 행동에 영향을 주는 동기를 설명하였다. 하지만, 조직원이 보유하는 정보보안의 수준이 적은 상황에서 최선이 아닌 차선의 선택을 한다는 제한된 합리성을 적용의 필요성을 견지하였으며, 연구가설을 제시 및 검증하였다. 즉, 이론적 측면에서 제한된 합리성의 관점을 정보보안 분야에 적용하여, 관련 선행 요인 두 가지 관점(준수의

도 강화 측면, 준수의도 억제 측면)으로 제시하였기 때문에, 조직원의 보안 준수의 동기적 차원을 보다 조직에서 발생할 수 있는 측면에서 다양하게 제시하였으며, 선행 연구로서의 시사점을 지닌다. 실무적인 측면에서 조직에서 고민하고 있는 조직원의 자발적인 정보보안 준수 행동을 유도하기 위한 방향을 제시하였다. 조직원들은 조직 몰입 수준이 높고, 주변 동료의 보안 행동이 강할수록 보안 준수의도를 높게 가지고 있는 것으로 나타났으며, 정보보안 시스템 걱정이 높을 경우 반대로 준수의도를 떨어뜨리는 것으로 나타났다. 따라서 조직 또는 정보보안 부서 차원에서 조직원의 정보보안 불확실성을 낮추고, 정보보안 성과를 높이기 위해서 접근해야할 방향성을 제시하였다.

둘째, 본 연구는 조직원의 정보보안 준수의도 강화 및 억제 요인을 변화시키기 위한 조직 차원의 정보보안 환경 요인 (물리적 시스템 구축, 정보보안 커뮤니케이션)을 제시하고 영향관계를 검증하였다. 이론적 측면에서, 조직원의 동기관련 선행 연구는 조직원 측면을 강조했다면, 본 연구는 조직원의 제한된 합리성에 영향을 주는 조직의 정보보안 환경이 있을 것으로 판단하였다. 실제 많은 조직은 물리적 정보보안 시스템을 구축하고 관련 정보를 제공함으로써, 조직원의 행동을 요구하고 통제하고 있다. 이러한 측면에서 본 연구는 물리적 시스템 구축과 커뮤니케이션의 수준이 조직원의 제한된 합리성 요인에 영향을 줄 것으로 판단하였으며, 관련 연관성을 검증하였다. 이러한 결과는 조직과 조직원간의 관계에서 정보보안에 대한 연구의 필요성을 제시하며, 향후 연구의 기반이 될 것으로 판단된다. 실무적인 측면에서 많은 조직들이 현재 보안 시스템을 구축하고 있으나, 실제 보안 시스템 구축이 조직원의 정보보안 준수의도에 영향을 미치는지 검증되지 않았다. 그러나 본 연구에서는 물리적 시스템 구축이 조직원의 몰입 수준과 동료 행동의 변화를 가져오고, 조직원의 보안 시스템 걱정 및 업무 장애에 대한 불만을 감소시킬 수 있음을 검증하였다. 또한 정보보안 커뮤니케이션 활동을 통해 정보 생성 및 공유가 활발하게 이루어질수록 조직 내 구성원들의 몰입,  동료 행동, 그리고 보안 시스템 걱정을 변화시킬 수 있는 선행 요인임을 검증하였다. 즉, 조직 또는 정보보안 부서에서 실제 조직원의 보안 준수 의도를 높이기 위해 고려해야하는 요인 및 분야를 제시하였다는 점에서 의미를 가진다.

## 5.2 연구의 한계점

본 연구는 몇 가지 측면에서 제약사항이 있으며, 향후 연구에서 보완될 필요성이 있다.

첫째, 본 연구는 제한된 합리성 관점에서 조직원의 정보보안 준수의도에 미치는 요인을 제시하였다. 비록 2가지 관점에서 요인의 다양성을 제시하고자 하였으나, 실제 제한된 합리성을 설명할 수 있는 요인이 더 있을 것으로 판단된다. 예를 들어, 정보보안 기술 스트레스와 같은 요인이 가능할 것으로 판단된다. 향후 연구에서는 조직원의 제한된 합리성의 구성 요인을 추가적으로 제시함으로써, 보다 효과적인 정보보안 수준을 유지하기 위한 방법을 제시하는 것이 필요하다.

둘째, 조직원이 인식하는 조직의 환경 요인으로서 물리적시스템 구축과 정보보안 커뮤니

케이션을 제시하였다. 조직 보안 환경에 대한 인식은 이외에 교육 및 훈련, 보안 가시성 등의 요인이 있을 것으로 판단된다. 향후 연구에서는 조직의 보안 환경을 구성하는 요인들을 다양하게 제시함으로써, 조직원에 의한 보안 위협 해결을 위한 접근 방법을 제시하는 것이 필요하다. 또한 조직의 보안 환경 인식 수준을 조직원에게 설문으로 파악하였기 때문에, 보다 정확하게 보안 환경을 파악하기 위하여 조직차원의 보안 환경을 측정하기 위한 도구를 활용함으로써 보다 정확한 보안 환경의 차이에 따른 조직원의 보안행동을 파악하는 것이 필요하다.

셋째, 본 연구는 조직원의 제한된 합리성에 기반하여 준수의도를 높이기 위한 방법을 찾고자 하였으나, 조직원이 보유하고 있는 원천적 특성에 기반한 차이를 비교하는 것이 필요하다. 예를 들어 조직의 정보보안 환경은 조직원의 대처(coping) 유형이나, 조직원이 보유한 조절초점(regulatory focus) 형태, 그리고 인구통계학적 특성 등에 의해서 달라질 것이다. 이러한 결과를 분석한다면, 상황별 정보보안 대응 방안을 마련할 수 있을 것으로 판단된다.

마지막으로, 본 연구는 설문 대상자를 정보보안 정책을 보유하고 있는 직장인을 대상으로 하였기 때문에, 편의상 대기업이나 금융권 위주로 설문을 실시하였다. 중소기업이나 외국계 기업, 그리고 국내뿐 아니라 타 국가와의 정보보안 특성 차이분석 등 샘플의 특성을 다양하게 분석하고, 설문 대상자가 속해 있는 조직의 보안 정책이나 보안 노력 등과 같은 현황을 추가적으로 제시한다면, 정보보안 준수에 대한 더욱 큰 시사점을 제시할 수 있을 것으로 판단된다.

## 참고문헌


김대진, 황인호, 김진수, “조직 구성원의 정보보안정책 준수행도에 대한 연구: 수정된 Triandis 모델의 적용,” 디지털정책연구, 제14권, 제4호, pp.209-220.

김종기, “정보시스템 보안의 효과성 모형에 관한 실증적 연구,” 정보시스템연구, 제7권 제2호, 1998, pp. 91-108.

김종기, 강다연, 전진환, “패스워드 선택을 위한 사용자의 보안행위의도에 영향을 미치는 요인,” 정보시스템연구, 제17권 제1호, 2008, pp. 23-43.

박철주, 임명성, “기술스트레스가 조직원의 보안 인식과 조직성과에 미치는 영향에 관한 연구,” 한국정보기술학회논문지, 제10권 제1호, 2012, pp.97-110.

이장형, 김종원, “보안 및 통제와 정보기술 사용자의 성격의 관계,” 정보시스템연구, 제19권 제3호, 2010, pp.1-12.

보안뉴스, 대담하고 지능적인 기술유출, 산업보안이 뒷받침돼야, 2015. 5. 14. http://www.boannews.com/media/view.asp?idx=46241

황인호, 김대진, 김태하, 김진수, “조직의 정보보안 문화형성이 조직구성원의 보안 지식 및 준수의도에 미치는 영향 연구,” *Information Systems Review,* 제18권, 제1호, 2016, pp.1-23.

Brockner, J., Spreitzer, G., Mishra, A., Hochwarter, W., Pepper, L., and Weinberg, J., “Perceived Control as an Antidote to the Negative Effects of Layoffs on Survivors' Organizational Commitment and Job Performance,”

*Administrative Science Quarterly,* Vol. 49, No. 1, 2004, pp.76-100.

Brown, W. S., "Ontological Security, Existential Anxiety and Workplace Privacy," *Journal of Business Ethics,* Vol. 23, No. 1, 2000, pp.61-65.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I., "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly,* Vol. 34, No. 3, 2010, pp.523-548.

Carr, N. G., "IT doesn't Matter," *Educause Review,* Vol. 38, 2003, pp.24-38.

Chan, M., Woon, I., and Kankanhalli, A. "Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior," *Journal of Information Privacy & Security,* Vol. 1, No. 3, 2005, pp.18-41.

Chen, Y., Ramamurthy, K., and Wen, K. W., "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?," *Journal of Management Information Systems,* Vol. 29, No. 3, 2012, pp.157-188.

Compeau, D. R., and Higgins, C. A., "Computer Self-Efficacy: Development of a Measure and Initial Test," *MIS Quarterly,* Vol. 19, No. 2, 1995, pp.189-211.

D'Arcy, J., Hovav, A., and Galletta, D., "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research,* Vol. 20, No. 1, 2009, pp.79-98.

Da Veiga, A., and Eloff, J. H., "A Framework and Assessment Instrument for Information Security Culture," *Computers & Security,* Vol. 29, No. 2, 2010, pp.196-207.

Dugo, T., *"The Insider Threat to Organizational Information,"* Auburn University, Auburn, AL., 2007.

Ernest Chang, S. and Lin, C. S., "Exploring Organizational Culture for Information Security Management," *Industrial Management & Data Systems,* Vol. 107, No. 3, 2007, pp.438-458.

Faily, S., and Fléchais, I., "Designing and Aligning e-Science Security Culture with Design," *Information Management & Computer Security,* Vol. 18, No. 5, 2000, pp.339-349.

Fornell, C., and Larcker, D. F., "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research,* Vol. 18, No. 1, 1981, pp.39-50.

Gartner, Gartner Says Worldwide Information Security Spending Will Grow Almost 8 Percent in 2014 as Organizations Become More Threat-Aware, 2014, http://www.gartner.com/newsroom/id/2828722

Guo, K. H., Yuan, Y., Archer, N. P. and Connelly, C. E., "Understanding Nonmalicious Security Violations in the

Workplace: A Composite Behavior Model," *Journal of Management Information Systems,* Vol. 28, No. 2, 2011, pp.203-236.

Herath, T., and Rao, H. R., "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems,* Vol. 47, No. 2, 2009a, pp.154-165.

Herath, T., and Rao, H. R., "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organizations," *European Journal of Information Systems,* Vol. 18, No. 2, 2009b, pp.106-125.

Hu, Q., Xu, Z., Dinev, T., and Ling, H., "Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?," *Communications of the ACM,* Vol. 54, No. 6, 2011, pp.54-60.

Ifinedo, P., "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory," *Computers & Security,* Vol. 31, No. 1, 2012, pp.83-95.

Jiménez-Castillo, D., and Sánchez-Pérez, M., "Nurturing Employee Market Knowledge Absorptive Capacity through Unified Internal Communication and Integrated Information Technology," *Information & Management,* Vol. 50, No. 2, 2013, pp.76-86.

Johnston, A. C., and Warkentin, M., "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly,* Vol. 34, No. 3, 2010, pp.549-566.

Knapp, K. J., Morris, R. F., Marshall, T. E., and Byrd, T. A., "Information Security Policy: An Organizational-Level Process Model," *Computers & Security,* Vol. 28, No. 7, 2009, pp.493-508.

Kwok, L. F., and Longley, D., "Information Security Management and Modelling," *Information Management & Computer Security,* Vol. 7, No. 1, 1999, pp.30-40.

Lee, J., and Lee, Y., "A Holistic Model of Computer Abuse within Organizations," *Information Management & Computer Security,* Vol. 10, No. 2, 2002, pp.57-63.

Lee, S. M., Lee, S. G., and Yoo, S., "An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories," *Information & Management,* Vol. 41, No. 6, 2004, pp.707-718.

Lee, Y., and Larsen, K. R., "Threat or Coping Appraisal: Determinants of SMB Executives' Decision to Adopt Anti-Malware Software," *European Journal of Information Systems,* Vol. 18, No. 2, 2009, pp.177-187.

Li, H., Zhang, J., and Sarathy, R., "Understanding Compliance with Internet Use Policy from the Perspective of Rational Choice

Theory," *Decision Support Systems,* Vol. 48, No. 4, 2010, pp.635–645.

Loch, K. D., Carr, H. H., and Warkentin, M. E., "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Quarterly,* Vol. 16, No. 2, 1992, pp.173-186.

Moore, G. C., and Benbasat, I., "Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation," *Information Systems Research,* Vol. 2, No. 3, 1991, pp.192-222.

Murrell, A. J., and Sprinkle, J., "The Impact of Negative Attitudes toward Computers on Employees' Satisfaction and Commitment within a Small Company," *Computers in Human Behavior,* Vol. 9, No. 1, 1993, pp.57-63.

Nunnally, J. C., "*Psychometric theory* (2nd ed.)," New York: McGraw-Hill, 1978.

Padayachee, K., "Taxonomy of Compliant Information Security Behavior," *Computers & Security,* Vol. 31, No. 5, 2012, pp.673-680.

Pahnila, S., Siponen, M., and Mahmood, A., *"Employees' Behavior towards IS Security Policy Compliance,"* In System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on (pp. 156b-156b). IEEE, 2007.

Rogers, R. W., "A Protection Motivation Theory of Fear Appeals and Attitude Change," *Journal of Psychology,* Vol. 91, No. 1, 1975, pp.93-114.

Simon, H. A., "Bounded Rationality in Social Science: Today and Tomorrow," *Mind & Society,* Vol. 1, No. 1, 2000, pp.25-39.

Simonson, M. R., Maurer, M., Montag-Torardi, M., and Whitaker, M., "Development of a Standardized Test of Computer Literacy and a Computer Anxiety Index," *Journal of Educational Computing Research,* Vol. 3, No. 2, 1987, pp.231-247.

Sims, C. A., "Implications of Rational Inattention," *Journal of Monetary Economics,* Vol. 50, No. 3, 2003, pp.665-690.

Sinkula, J. M., "Market Information Processing and Organizational Learning," *The Journal of Marketing,* Vol. 58, No. 1, 1994, pp.35-45.

Siponen, M., Pahnila, S., and Mahmood, M. A., "Compliance with Information Security Policies: An Empirical Investigation," *Computer,* Vol. 43, No. 2, 2010, pp.64-71.

Siponen, M., and Vance, A., "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly,* Vol. 34, No. 3, 2010, pp.487-502.

Son, J. Y., "Out of Fear or Desire? Toward a Better Understanding of Employees' Motivation to Follow IS Security Policies," *Information & Management,*

Vol. 48, No. 7, 2011, pp.296-302.

Stanton, J. M., Stam, K. R., Guzman, I., and Caldera, C., *"Examining the Linkage between Organizational Commitment and Information Security,"* In IEEE International Conference on Systems Man and Cybernetics, Vol. 3, 2003, October, pp. 2501-2506.

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.124-133.

Steers, R., "Antecedents and Outcomes of Organizational Commitment," *Administrative Science Quarterly,* Vol. 22, No.1, 1977, pp.46-56.

Straub, D. W., and Welke, R. J., "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly,* Vol. 22, No. 4, 1998, pp.441-464.

Tarafdar, M., Tu, Q., Ragu-Nathan, B. S., and Ragu-Nathan, T. S., "The Impact of Technostress on Role Stress and Productivity," *Journal of Management Information Systems,* Vol. 24, No.1, 2007, pp.301-328.

Todd, P. M., and Gigerenzer, G., "Bounding Rationality to the World," *Journal of Economic Psychology,* Vol. 24, No. 2, 2003, pp.143-165.

Vance, A., Siponen, M., and Pahnila, S., "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory," *Information & Management,* Vol. 49, No. 3, 2012, pp.190-198.

Venkatesh, V., "Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion into the Technology Acceptance Model," *Information Systems Research,* Vol. 11, No. 4, 2000, pp.342-365.

Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D., "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly,* Vol. 27, No. 3, 2003, pp.425-478.

Verizon., Verizon 2013 Data Breach Investigations Report, 2013.

Walpole, R. E., Myers, R. H., Myers, S. L., and Ye, K., *Probability and statistics for engineers and scientists* (Vol. 5). New York: Macmillan, 1993.

Wang, P. A., *"Information Security Knowledge and Behavior: An Adapted Model of Technology Acceptance,"* In Education Technology and Computer (ICETC), 2010 2nd International Conference on (Vol. 2, pp. V2-364). IEEE, 2010, June.

West, R., "The Psychology of Security," *Communications of the ACM,* Vol. 51, No. 4, 2008, pp.34-40.

Whitman, M. E., "In Defense of the Realm: Understanding the Threats to Information Security," *International Journal of Information Management,* Vol. 24, No. 1, 2004, pp.43-57.

Williams, L. J., and Anderson, S. E., "Job

Satisfaction and Organizational Commitment as Predictors of Organizational Citizenship and In-role Behaviors," *Journal of Management,* Vol. 17, No. 3, 1991, pp.601-617.

Wixom, B. H., and Watson, H. J., "An Empirical Investigation of the Factors Affecting Data Warehousing Success," *MIS Quarterly,* Vol. 25, No. 1, 2001, pp.17-41.

Zhang, J., Reithel, B. J., and Li, H,." Impact of Perceived Technical Protection on Security Behaviors," *Information Management & Computer Security,* Vol. 17, No. 4, 2009, pp.330-340.

**황인호(In-Ho Hwang)**

현재 (사)한국창업경영연구원 정보전략 연구팀장으로 재직하고 있다. 중앙대학교 경영학 박사학위를 수여하였다. 기술창업, IT 핵심성공요인, 디지털 콘텐츠, 정보보안 및 프라이버시 분야에 관심을 가지고 연구를 진행 중이다.

**김대진(Dae-Jin Kim)**

현재 중앙대학교 경영경제대학 시간강사로 활동하고 있다. 중앙대학교 경영학 박사학위를 수여하였다. IT수용, 비즈니스 모델, 정보보안 및 프라이버시 분야 등에 관심을 가지고 연구를 진행 중이다.

<Abstract>

# The Effect of Organizational Information Security Environment on the Compliance Intention of Employee

Inho Hwang · Daejin Kim

**Purpose**

Organizations invest significant portions of their budgets in fortifying information security. Nevertheless, the security threats by employees are still at large. We discuss methods to reduce security threats that are posed by employees in organization. This study finds antecedent factors that increases or decreases employee's compliance intention. Also, the study suggests organizations' security environmental factors which influences the antecedent factors of compliance intention.

**Design/methodology/approach**

The structural equation model is then applied in order to verify this research model and hypothesis. Data were collected on 415 employees working in organizations with an implemented information security policy in South Korea. We analyzed the fitness and validity of the research model via confirmatory factor analysis in order to verify the research hypothesis, then we analyzed structural model, and derived the result.

**Findings**

The result shows that organizational commitment and peer behavior increase security compliance intention of employees, while security system anxiety decreases compliance intention. And, organization's physical security system and security communication both have influence on antecedent factors for information security compliance of employees. Our findings help organizations to establish information security strategies that enhance employee security compliance intention.

***Keyword***: Compliance Intention, Organizational Commitment, Peer Behavior, Security System Anxiety,

Work Impediment, Physical Security System, Security Communication

* 이 논문은 2016년 1월 8일 접수, 2016년 2월 23일 1차 심사, 2016년 4월 20일 2차 심사, 2016년 5월 9일 게재 확정되었습니다.