

# 조직의 정보보안 분위기가 조직 구성원의 정보보안 참여 행동에 미치는 영향\*

박재영\*\* · 김범수\*\*\*

〈 목 차 〉	
I. 서론	IV. 연구결과
II. 연구모형과 가설 설정	4.1 신뢰성 및 타당성 검증
2.1 조직의 정보보안 분위기	4.2 가설 검증
2.2 정보보안 분위기와 정보보안 참여 행동	V. 결론
2.3 정보보안 동기와 정보보안 지식	5.1 연구결과 요약 및 시사점
III. 연구방법	5.2 한계점 및 향후 연구방향
3.1 데이터 수집	참고문헌
3.2 변수의 조작적 정의	<Abstract>

## I. 서론

ICT 기술의 급속한 발전과 동시에 정보보호 위협 역시 증가하고 있다. 기업에서 침입탐지시스템(IDS, intrusion detection system), 침입방지시스템(IPS, intrusion prevention system), 방화벽 등과 같은 기술적 조치를 취함에도 불구하고, 개인정보유출사고가 지속적으로 발생하고 있다. 잼알토가 발표한 데이터 유출·침해 통계 보고서(breach level index)에 따르면, 2018년 상반기에만 945건의 데이터 유출 사고가 발생했으며, 약 45억 건의 데이터가 유출된 것

로 나타났다. 고객 정보를 유출 기업은 소송 비용, 매출 하락 등으로 상당한 손실을 경험하며, 시장으로부터 신뢰를 잃게 되어 기업가치가 하락한다(Campbell et al., 2003; Cavusoglu et al., 2004; 박상수, 이현철, 2018). 뿐만 아니라, 고객들에게도 외면을 받게 된다 (Lee and Lee, 2012). ‘개인정보 유출의 간접피해 비용 추정기법 연구’에 따르면, 2014년 카드 3사 개인정보 유출로 인한 직간접 피해 비용이 총 9조 2736억 원으로 추정되었다. 2013년 약 1억 1,000만 건의 고객 정보를 유출한 미국 대형 유통업체 target은 데이터 침해와 관련된 비용이 1억 6천

\* 이 저서(논문·예술연구)는 연세대학교 학술연구비의 지원으로 이루어진 것임.

\*\* 연세대학교 정보대학원, jaeyoungpark85@kakao.com(주저자)

\*\*\* 연세대학교 정보대학원, beomsookim@gmail.com(교신저자)

만 달러를 초과했다고 발표하였다. 이처럼 기업은 개인정보 유출로 인해 막대한 손실을 경험하기 때문에 조직의 정보보안 리스크를 줄이기 위한 방안을 연구하는 것이 중요하다.

최근 들어, 정보보안 관련 학계 및 산업계 전문가들은 정보보안 연구를 조직 행동 관점에서 바라볼 필요가 있다고 주장한다(Crossler et al., 2013; Guan and Hsu, 2020; Liu et al., 2020; 황인호, 허성호, 2020). 또 다른 연구에서도 정보보호정책 효과에 있어서 조직 구성원이 중요한 역할을 한다고 말한다(Knapp et al., 2007; Posey et al., 2014). 즉, 조직의 정보보안 수준을 향상시키기 위해서 기술적 조치 뿐 아니라 관리적 보안이 필요하다는 것이다. 예를 들어, 조직 구성원의 정보보안 정책 준수 행동을 높일 필요가 있다. 조직의 정보보안관리 측면에 있어서 직원은 가장 취약한 지점으로 간주되고 있기 때문이다(Padayachee, 2012).

정보보안 정책 준수 관련 연구를 살펴보면, 중화이론 (Siponen and Vance, 2010), 보호동기이론(Johnston and Warkentin, 2010), 억제이론(D'Arcy et al., 2009), 합리적 선택 이론(Bulgurcu et al., 2010), 사회적 교환 이론(황인호, 김상현, 2019)에 기반하여 정보보안 정책 준수의 선행요인을 밝혔다. 하지만, 기존 연구 대다수가 *역할 내 행동(in-role behaviors)*-조직 내에서 종업원이 담당하는 직무 또는 맡겨진 과업과 관련하여 공식적으로 요구되는 직무수행행동-에만 초점을 맞추었다. 즉, 조직 내 정보보안 정책에 명시되어 있는 사항을 준수하는 행위에만 집중하였다. 하지만, 이것만으로는 조직이 보유한 정보 자원의 적절한 보호를 보장할 수 없다. 정보보안 정책에 모든 사항을 명시

할 수 없기 때문이다(예를 들어, 신입/경력사원에게 정보보호 교육). 따라서, 조직의 정보 자원을 적절하게 보호하고 정보보호 리스크를 줄이기 위해서는 정보보안과 관련하여 공식적으로 요구되는 행동뿐 아니라 조직 구성원의 자발적 참여 행동이 필수적으로 요구된다.

조직 행동 연구를 살펴보면, 다수의 연구에서 *역할 외 행동(extra-role behaviors)* -직무상의 역할을 수행하는데 공식적으로 요구되지 않지만 조직의 성과에 도움을 줄 수 있는 행동으로 어떠한 강제에 의한 행동이 아니라 구성원 자신이 자발적으로 조직의 발전에 기여하는 행동-의 중요성을 강조하였다(Katz, 1964). 조직 구성원들의 역할 외 행동은 조직 성과에 긍정적인 영향을 준다(Podsakoff et al., 2000). 마찬가지로, 정보보안 정책 맥락에서도 공식적으로 요구되는 직무수행행동뿐 아니라 정보보안과 관련하여 직원들의 자발적 참여 행동(i.e. 역할 외 행동)이 중요하다(Chen and Li 2019; Guhr et al., 2019; Hsu et al., 2015). 정보보안 참여 행동은 조직의 정보보안 수준 향상을 위해 직원들이 자발적으로 정보보안 관련 행동을 하는 것을 말한다. 예를 들어, 동료가 정보보안 정책을 준수할 수 있도록 도움을 주는 행동이 있다. 즉, 정보보안 정책에 명시되어 있지 않지만 조직을 위해 조직의 정보보안 수준을 향상시킬 수 있는 행동을 하는 것을 말한다. 소수의 연구가 정보보안 정책 준수 분야에서 역할 외 행동을 살펴보았는데, 정보보안 정책 준수 관련 공식 통제(formal control)와 사회적 통제(social control)가 정보보안 정책 관련 역할 외 행동(e.g. helping, voicing)을 높였으며, 이에 따라 정보보안 정책 효과가 증가하는 것으로 나타났

다(Hsu et al., 2015). 즉, 기존 조직행동 연구와 마찬가지로 정보보안 맥락에서도 역할 외 행동(i.e. 정보보안 참여 행동)이 조직 성과(i.e. 정보보호 정책 효과)를 높여준다는 것을 확인한 것이다. 이는 직원들의 자발적인 정보보안 참여 행동이 중요하며, 직원들의 정보보안 참여 행동을 높일 수 있는 방안을 살펴볼 필요가 있음을 말해준다. 하지만, 소수의 연구를 제외하고 정보보안 참여 행동의 선행요인을 살펴본 연구가 거의 없는 실정이다(Chen and Li, 2019; Hsu et al., 2015; Guhret et al., 2019). 이에 본 연구에서는 조직 행동 문헌에서 조직 분위기(organizational climate) 개념을 가져와 조직의 정보보안 분위기가 직원들의 정보보안 참여 행동에 어떻게 영향을 주는지 살펴본다.

조직 분위기는 조직 내 공식적/비공식적 정책, 관행 및 절차에 대한 조직 구성원들의 공유된 인식을 의미한다(Reichers and Schneider, 1990). 조직 분위기는 직접적으로 조직 구성원들의 태도 및 행동에 영향을 주는 반면 조직 문화(organizational culture)는 조직 구성원들의 가치관에 영향을 준다는 점에서 이 두 개념은 서로 구분된다(Schneider et al., 2013). 조직 문화는 추상적인 상위 개념으로 실증 분석에 활용하기에 많은 어려움이 존재한다고 말하며(Kessler et al. 2020), 이에 따라 대다수 연구가 조직 문화보다는 조직 분위기를 맥락에 맞게 변형하여 사용한다. 조직 분위기는 윤리, 안전 등과 같이 다양한 맥락에서 사용되었으며, 조직 구성원의 행동에 영향을 주는 것으로 나타났다. 예를 들어, 안전 분위기가 안전 참여 행동을 높여주었다. 정보보안 맥락에 이를 적용하면, 마찬가지로 사회 정보 처리 이론에 따라서 정보

보안 분위기가 정보보안 참여 행동에 긍정적인 영향을 줄 것으로 예상할 수 있다. 여기에서 정보보안 분위기는 조직 내 정보보안과 관련된 정책, 관행 및 절차에 대한 직원들의 공유된 인식을 말한다(Kessler et al., 2020). 또한, Griffin and Neal(2000)이 제시한 프레임워크에 따르면, 정보보안 분위기가 정보보안 지식과 정보보안 동기에 긍정적인 영향을 주고 정보보안 지식과 정보보안 동기가 정보보안 참여 행동에 긍정적인 영향을 줄 것이다.

정리하면, 본 연구는 조직 행동 문헌과 Griffin and Neal(2000)의 프레임워크 그리고 사회 정보 처리 이론을 바탕으로 정보보안 분위기의 결정요인으로 정보보안 동기, 정보보안 지식, 성과요인으로 정보보안 참여 행동을 각각 제시하고 이를 실증적으로 분석한다.

## II. 연구모형과 가설 설정

### 2.1 조직의 정보보안 분위기

조직 분위기는 조직 내 공식적/비공식적 정책, 관행 및 절차에 대한 조직 구성원들의 공유된 인식을 말한다(Reichers and Schneider, 1990). 조직 분위기는 직원들의 특정 행동 변화(e.g. 안전 행동, 윤리적 행동)를 유도하기 위해서 해당 맥락에 맞게 변형되어 사용되고 있다. 대표적으로, 윤리 분위기(ethical climate), 안전 분위기(safety climate) 등을 들 수 있다. 최근 들어, 조직의 정보보안 수준 향상에 있어서 내부 구성원의 중요성이 강조되고 이에 따라 조직적 측면을 살펴볼 필요성이 증가하면서, 정보

보안 맥락에서도 정보보안 분위기라는 개념이 사용되기 시작하였다(Goo et al., 2014; Kessler et al., 2020; 임명성, 2012).

정보보안 분위기(information security climate)는 조직 내 정보보안과 관련된 정책, 관행 및 절차에 대한 직원들의 공유된 인식으로 정의된다(Kessler et al., 2020). 정보보안 분위기가 강한 조직은 정보보안을 중요한 것으로 인식한다. 기존 정보보안 분위기 관련 연구를 보면, 대다수가 정보보안 분위기를 1차 요인(first-order factors)들로 구성된 고차 요인(higher order factor)으로 개념화하였다. 조직 내에서 조직 구성원들이 정보보안을 가치가 있는 것으로 인식하게 만드는 다양한 조직 속성을 반영하는 것이다. 예를 들어, 임명성(2012)은 정보보안 분위기를 최고 경영진의 관심, 보안 강조, 보안 인식 교육, 보안 정책의 효과성으로 개념화 하였으며, Kessler et al.(2020)는 정보보안 실무관행(practices), 정보보안 중시(importance), 정보보안 우선순위(laxness)로 구성된 정보보안 분위기를 개발하였다. 기존 연구를 참고하여, 본 연구에서도 정보보안 분위기를 1차 요인인 정보보안 실무관행, 정보보안 중시, 보안 인식 교육으로 구성된 2차 요인(reflective-formative second-order)으로 개념화 하였다.

선행 연구에서 정보보안 분위기는 정보보안 정책 준수와 긍정적으로 관련이 있는 것으로 나타났다(Chan et al., 2005; Goo et al., 2014; 임명성, 2012). 하지만, 정보보안 분위기와 역할 외 행동(i.e. 정보보안 참여 행동) 간 관계를 살펴본 연구는 거의 없는 실정이다. 이에 본 연구에서는, 기존 연구의 한계점을 보완하고자, 정보보안 분위기가 정보보안 참여 행동에 어떻

게 영향을 주는지 살펴본다.

## 2.2 정보보안 분위기와 정보보안 참여 행동

사회 정보 처리 이론(social information processing theory)에 따르면, 조직 분위기는 조직 구성원의 행동에 영향을 준다. 구체적으로, 조직 구성원은 조직 내에서 무엇이 바람직한 행동인지 아닌지를 판단하기 위해 주변 환경의 중요한 단서와 정보(e.g., 상사나 동료의 행동)를 활용한다(Salancik and Pfeffer, 1978). 즉, 조직 구성원은 자신이 속한 조직이 우선시하는 것이 무엇인지를 파악하고 그것에 맞는 의사결정을 내리고 그에 맞는 행동을 한다는 것이다. 예를 들어, 정보보안을 강조하는 분위기가 형성되어 있는 조직에서는 직원들이 정보보안을 준수하는 또는/그리고 촉진하는 행동을 할 것이다. 정보보안 정책 준수 문헌을 살펴보면, 정보보안 분위기는 정보보안 정책을 준수하는 것에 긍정적인 태도를 가지게 만들었다(임명성, 2012). 또한, 정보보안 분위기는 조직에 대한 정서적 몰입(affective commitment)과 규범적 몰입(normative commitment)에 긍정적인 영향을 주었으며, 이것은 정보보안 정책 준수 의도가 증가하는 결과로 이어졌다(Goo et al., 2014). 또한, 정보보안 분위기와 정보보안 정책 준수 간 긍정적 상관관계가 있으며, 정보보안 분위기와 보안 위협을 증가시키는 행동 간 부정적 상관관계가 있다는 사실이 밝혀졌다(Kessler et al., 2020). 이처럼 정보보안을 강조하는 조직에서는 직원들이 정보보안 정책을 잘 준수하는 것으로 나타난다. 하지만, 정보보안 분위기의 영향이 직원의 역할 내 행동(i.e. 정보보안

정책 준수)에만 국한하지 않을 것으로 본다. 즉, 조직의 정보보안 분위기가 직원의 역할 외 행동(i.e. 정보보안 참여 행동)에도 영향을 줄 것이라고 예상된다.

역할 외 행동은 직무상의 역할을 수행하는데 공식적으로 요구되지는 않지만, 조직의 성과에 도움을 줄 수 있는 행동으로 어떠한 강제에 의한 행동이 아니라 구성원 자신이 자발적으로 조직의 발전에 기여하는 행동이다(Van Dyne and Le Pine, 1998). 정보보안 정책 맥락에서 역할 외 행동은 조직의 정보보안 수준 향상을 위하여 자발적으로 타인을 돕는 행동(e.g. 동료 직원에게 정보보안 정책을 알려주는 행위)과 다양한 의견을 제시하는 행동(e.g. 정보보호 수준을 높일 수 있는 정보보안 정책 아이디어 제공)이며, 본 연구에서는 이와 같은 행동을 정보보안 참여 행동으로 정의한다. 즉, 정보보안 참여 행동은 조직의 정보보호 정책에 명시되어 있지 않지 않은 조직 구성원의 자발적인 정보보안 행동이다.

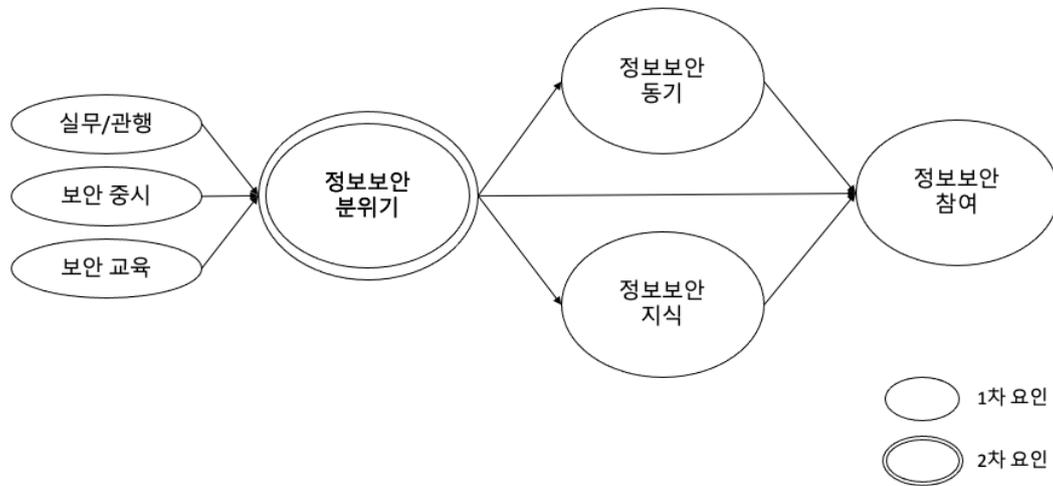
조직 분위기와 역할 외 행동 간 관계를 살펴본 연구를 보면, 안전 분위기가 안전 참여 행동에 긍정적인 영향을 주는 것으로 나타났으며(김영민, 2020), 윤리 분위기가 높아질수록 조직시민행동이 증가하는 것으로 나타났다(Teng et al., 2020). 또한, 정보보안 분위기와 정보보안 참여 행동이 긍정적 상관관계를 보였다(Kessler et al., 2020). 따라서, 조직 구성원이 우리 조직은 정보보안을 중요하게 생각한다고 인식할수록 그들의 정보보안 참여 행동이 증가할 것으로 예상할 수 있다. 이에 아래와 같이 가설 1을 설정한다.

*가설 1. 조직의 정보보안 분위기는 직원의 정보보안 참여 행동에 긍정적인 영향을 줄 것이다.*

## 2.3 정보보안 동기와 정보보안 지식

Griffin and Neal(2000)은 안전 분위기(safety climate)를 선행요인으로, 안전 지식(safety knowledge)과 안전 동기(safety motivation)를 결정 요인으로, 조직 구성원의 안전 참여 행동(safety participation behavior)을 성과로 하는 모델을 개발하고 이를 검증한 결과, 안전 분위기가 안전 지식과 안전 동기에 긍정적인 영향을 주었으며, 안전 지식과 안전 동기는 안전 참여 행동에 긍정적으로 영향을 미쳤다. 안전 지식은 안전 운영 절차와 적절한 안전 교육 및 지침에 대한 직원의 이해를 말한다(Hofmann et al., 1995). 안전 동기는 개인이 안전하게 행동하기 위해 노력을 기울이는 상태, 그리고 안전 행동에 중요성을 부여하는 상태를 말한다(Neal and Griffin, 2006). 기존 연구를 참고하여 본 연구에서 정보보안 지식을 조직의 정보보안 정책, 지침, 절차 등을 포함한 정보보안에 대한 직원의 전반적인 지식 및 이해로 정의하고, 정보보안 동기를 직원이 정보보안을 중요하게 생각하는 정도 및 정보보안 행동을 하기위해 노력을 기울이는 정도로 정의한다.

다수 연구에서 안전 분위기는 안전 동기의 중요한 선행요인으로 밝혀졌다(Payne et al., 2009; 김기식, 박영석, 2002; 정하진 등, 2015). 이것은 기대 이론(expectancy theory)으로 설명이 가능한데, 자신의 행동이 가치 있는 성과로 이어진다고 믿는다면, 그 행동에 대한 동기가 생겨난다는 것이다(Vroom, 1964). 이것을 정보



<그림 1> 연구모형

보안 맥락에 적용해보면, 자신의 조직이 정보보안을 중요하게 여긴다고 인식하는 조직 구성원은 정보보안을 중요하게 생각할 것이고, 결과적으로, 자신의 정보보안 행동이 가치 있는 중요한 행동이라고 믿게 되면서 정보보안 동기가 유발될 것이다.

조직 분위기는 조직 구성원의 동기 뿐 아니라 지식에도 긍정적인 영향을 줄 수 있다. 예를 들어, 조직 내에서 정보보안을 중요하게 여기는 분위기가 형성되면 조직 구성원들 간에 보안 지식을 공유하거나 조직 구성원 스스로 보안 지식을 습득한다(황인호 등, 2016). 따라서 정보보안 분위기가 보안 지식에 긍정적으로 영향을 줄 것이라고 예상된다.

안전 분야의 다수 연구(Griffin and Neal, 2000; Vinodkumar and Bhasi, 2010; 김영민, 2020; 정하진 등, 2015)에서 안전 동기가 안전 참여 행동에 긍정적으로 영향을 준다고 하였다. 마찬가지로, 정보보안 맥락에서 정보보안 동기가 정보보안 참여 행동을 높여줄 것으로 예상

할 수 있다. 또한, 안전 분야의 다수 연구에서 안전 지식이 안전 참여 행동에 긍정적으로 영향을 준다고 하였다(Griffin and Neal, 2000; Vinodkumar and Bhasi, 2010; 김영민, 2020). 이를 정보보안 맥락에 적용해보면, 조직 구성원의 정보보안 지식이 향상될수록 그들의 정보보안 참여 행동이 증가할 것으로 예상할 수 있다. 이상의 논의를 바탕으로 아래와 같이 가설을 설정한다.

*가설 2. 조직의 정보보안 분위기는 직원의 정보보안 동기에 긍정적인 영향을 줄 것이다.*

*가설 3. 조직의 정보보안 분위기는 직원의 정보보안 지식에 긍정적인 영향을 줄 것이다.*

*가설 4. 정보보안 동기는 직원의 정보보안 참여 행동에 긍정적인 영향을 줄 것이다.*

*가설 5. 정보보안 지식은 직원의 정보보안 참여 행동에 긍정적인 영향을 줄 것이다.*

### Ⅲ. 연구방법

#### 3.1 데이터 수집

본 연구는 국내 리서치 전문 기업이 보유하고 있는 패널 대상으로 2020년 8월에 온라인

설문조사를 실시하였다. 연구목적에 맞게 정보보안 정책이 내부적으로 존재하지 않는 기업의 직원은 설문조사에서 제외하였다. 총 564명이 설문조사에 참여하였으며, 응답자의 인구통계학적 특성은 아래 <표 1>과 같다. 응답자 중 남성이 54.8%, 여성이 45.2%를 차지하였으며, 연

<표 1> 표본 특성 (n = 564)

		빈도	비중 (%)
성별	남성	309	54.8
	여성	255	45.2
연령	20-29	113	20.0
	30-39	117	20.7
	40-49	166	29.4
	50 이상	168	29.8
학력	고등학교 이하	57	10.1
	전문대학 (전문학사)	61	10.8
	대학교 (학사)	359	63.7
	대학원 (석사)	67	11.9
업종	대학교원 (박사)	20	3.5
	제조업	126	22.3
	건설업	40	7.1
	금융/보험업	25	4.4
	통신업	16	2.8
	유통업	40	7.1
	IT(정보기술)산업	61	10.8
기업규모	서비스업	163	28.9
	기타	93	16.5
	100명 미만	209	37.1
	100-499명	132	23.4
	500-999명	61	10.8
	1,000-2,499명	51	9.0
직급	2,500-9,999명	53	9.4
	10,000명 이상	58	10.3
	사원	184	32.6
	대리	129	22.9
	과장	107	19.0
직무	차장	65	11.5
	부장	79	14.0
	IT(전산)	53	9.4
	개인정보보호/정보보안	23	4.1
	영업/마케팅	83	14.7
	전략/기획	52	9.2
	재무/회계	50	8.9
	연구개발	63	11.2
	인사/총무/법무	101	17.9
IT 직무 경험	생산관리	68	12.1
	기타	71	12.6
	없음	344	61.0
	있음	220	39.0

령의 경우에는 20대가 20%, 30대가 20.7%, 40대가 29.4%, 50대가 29.8%를 각각 차지하여 특정 성별 혹은 연령에 편중되지 않고 비교적 고른 분포를 보이는 것으로 나타났다. 대학교 졸업자가 63.7%로 다수를 차지하였으며, 업종으로는 서비스업 (28.9%), 제조업 (22.3%), IT산업 (10.8%) 순으로 나타났다. 응답자 중 IT 직무 경험이 있는 사람은 220명으로 39%를 차지하였으며, 직급을 보면 사원 (32.6%), 대리 (22.9%), 과장 (19.0%) 순서대로 높은 비중을

보였다.

### 3.2 변수의 조작적 정의

본 연구에서 사용한 설문문항은 <표 2>와 같다. 각 문항은 기존 문헌을 토대로 개발하였으며, 국내 실정에 맞게 수정 보완하였다. 모든 문항은 Likert 7점 척도 (1점: 전혀 그렇지 않다 ~ 7점: 매우 그렇다)로 측정하였다.

<표 2> 설문문항

변수	설문문항	레퍼런스
정보보안 실무관행	1. 나의 상사는 부하 직원들이 정보보안 정책을 잘 준수하고 있는지 확인한다. 2. 나의 상사는 평소에 정보보안과 관련된 이슈에 대해 자주 이야기한다. 3. 나의 상사는 정보보안을 준수하는 행동에 대해서 칭찬을 해준다. 4. 나의 상사는 직원 성과 평가에 있어서 정보보안 정책 준수를 핵심 요소 중 하나로 생각한다.	Kessler et al. (2020)
정보보안 중시	1. 정보보안 정책을 준수하기 위해서 노력하는 것은 내가 속한 조직에서 가치 있는 일이다. 2. 내가 속한 조직은 정보보안 정책 준수를 항상 중요하게 여긴다. 3. 정보보안 위험을 줄이는 것은 내가 속한 조직에서 중요한 사항이다.	Kessler et al. (2020)
보안 인식 교육	1. 내가 속한 조직은 직원들의 정보보호 인식 향상을 위한 교육을 진행하고 있다. 2. 내가 속한 조직은 직원들의 정보보안 역량 강화를 위한 교육을 진행하고 있다. 3. 내가 속한 조직은 직원들 대상으로 사이버 침해 대응 모의 훈련 (예: 스팸 메일 대응 훈련 등)을 실시하고 있다. 4. 내가 속한 조직은 다양한 정보보호 활동 및 캠페인 (예: 보안 스티커 배포 등)을 실시하고 있다.	Goo et al. (2014); D'Arcy et al.(2009)
정보보안 동기	1. 나는 조직 내 개인정보를 보호하는 것은 가치가 있는 일이라고 생각한다. 2. 조직 내 개인정보를 보호하는 것은 중요하다. 3. 조직 내 정보보안 관련 위험 요소를 줄이는 것은 중요하다. 4. 조직의 정보보안 수준을 향상시키는 것은 중요하다.	Kessler et al. (2020); Neal et al. (2000)
정보보안 지식	1. 나는 정보보안 관련 지식이 풍부하다. 2. 나는 조직의 정보보안 수준을 높일 수 있는 방법을 알고 있다. 3. 나는 전반적으로 정보보안에 대해서 잘 알고 있다. 4. 나는 보안을 강화할 수 있는 방안을 알고 있다.	Neal et al. (2000)
정보보안 참여 행동	1. 나는 동료 직원들에게 정보보안 정책 준수를 권장하는 편이다. 2. 나는 조직의 정보보안 강화에 도움이 되는 업무나 활동을 자발적으로 수행한다. 3. 나는 동료 직원들이 정보보안 정책을 준수할 수 있도록 도움을 준다. 4. 나는 누가 시키지 않아도 우리 조직의 정보보안을 개선할 수 있는 방안을 제시한다. 5. 나는 조직의 정보보안 수준 유지 및 향상을 위해 노력한다.	Chen et al. (2019); Guhr et al. (2019); Neal et al.(2000)

## IV. 분석

### 4.1 신뢰성 및 타당성 분석

본 연구에서 제시한 가설을 검증하기에 앞서, 측정문항에 대한 신뢰성 및 타당성 검증을 실시하였다. <표 3>에서 보는 바와 같이, 측정문항의 cronbach's  $\alpha$  와 개념 신뢰도(composite reliability) 값이 모두 Gefen et al.(2000)이 제시한 기준치인 0.7 이상으로 나왔으므로 측정문항은 신뢰성이 있다고 할 수 있다. 또한, 요인 적재량(factor loading) 값이 0.7 이상이고 AVE 값이 0.5 이상으로 나왔다(표 3 참고). 따라서, 모든 측정문항에 대한 수렴타당성을 확보하였다. 다음으로 판별타당성을 검증하였는데, <표 4>와 같이, 각 변수의 AVE 값의 제곱근이 다른

변수들 간의 상관계수 값보다 크게 나타났으며, 각 측정항목에 대한 요인 적재량 값이 다른 변수들에 대한 교차 요인 적재량(cross-loadings) 보다 높은 값을 가졌으므로 측정문항은 판별타당성을 만족한다(Hair et al., 2011).

다음으로, 본 연구모형에서 설정한 2차 요인에 대한 타당성 검증을 실시하였다. 정보보안 분위기는 기존 문헌을 토대로 1차 요인인 정보보안 실무관행, 정보보안 중시, 보안 인식 교육으로 구성된 2차 형성 지표(formative indicator)로 설정되어 있다. 형성 지표로 구성된 변수는 다중공선성 분석을 통해 타당성이 평가되어진다. <표 5>에서 보는 바와 같이, 공차한계가 0.1보다 크고 분산팽창계수(VIF)가 10이하로 나타났다. 따라서, 정보보안 분위기의 구성개념에 대한 타당성이 확보되었다.

<표 3> 1차 요인 신뢰성 및 수렴타당성 검증 결과

변수	측정 항목	요인 적재량	T값	Cronbach's $\alpha$	CR	AVE
정보보안 참여 행동	parti1	0.904	103.678	0.941	0.955	0.809
	parti2	0.904	90.408			
	parti3	0.911	89.906			
	parti4	0.866	53.164			
	parti5	0.912	114.886			
보안 인식 교육	seta1	0.904	94.265	0.908	0.936	0.785
	seta2	0.921	125.473			
	seta3	0.854	54.172			
	seta4	0.863	58.235			
정보보안 실무관행	prac1	0.874	73.428	0.910	0.937	0.788
	prac2	0.898	81.018			
	prac3	0.885	77.32			
	prac4	0.893	87.58			
정보보안 중시	impor1	0.902	86.091	0.895	0.935	0.826
	impor2	0.925	120.105			
	impor3	0.899	71.574			

정보보안 지식	know1	0.910	95.938	0.946	0.961	0862
	know2	0.937	141.147			
	know3	0.928	121.005			
	know4	0.938	164.785			
정보보안 동기	mot1	0.911	114.319	0.939	0.956	0.845
	mot2	0.923	113.442			
	mot3	0.914	63.215			
	mot4	0.929	108.727			

<표 4> 1차 요인 판별타당성 검정 결과

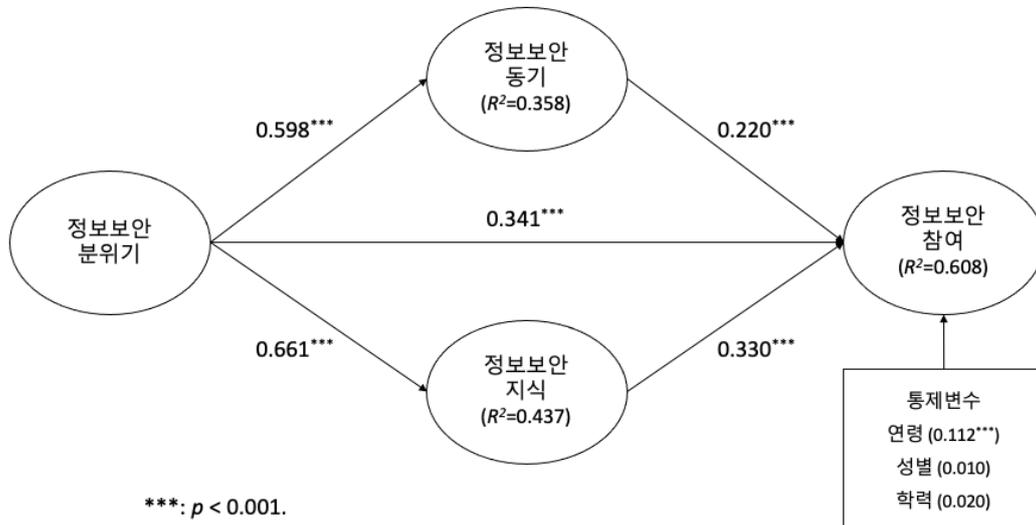
	Mean (S.D)	1	2	3	4	5	6
1	5.19 (1.13)	<b>0.909</b>					
2	4.62 (1.22)	0.548	<b>0.928</b>				
3	5.74 (.95)	0.620	0.463	<b>0.919</b>			
4	5.02 (1.10)	0.626	0.667	0.587	<b>0.899</b>		
5	4.53 (1.24)	0.665	0.626	0.414	0.616	<b>0.887</b>	
6	4.82 (1.32)	0.63	0.568	0.487	0.580	0.596	<b>0.886</b>

주 1) 1: 정보보안 중시, 2: 정보보안 지식, 3: 정보보안 동기, 4: 정보보안 참여, 5: 정보보안 실무관행, 6: 보안 인식 교육.

주 2) 대각선의 볼드체 값은 AVE의 제공근.

<표 5> 2차 요인 수렴타당성 및 다중공선성 검정 결과

	측정항목	가중치	T값	공차한계	분산팽창계수 (VIF)
정보보안 분위기	정보보안 실무관행	0.279	4.506	0.505	1.979
	정보보안 중시	0.519	7.281	0.473	2.113
	보안 인식 교육	0.346	6.169	0.547	1.827



<그림 2> 경로분석 결과

## 4.2 가설 검증

본 연구 가설 검증 결과는 <그림 2>와 같다. 첫째, 정보보안 분위기는 정보보안 참여 행동에 긍정적인 영향을 주었다( $\beta=0.341$ ,  $p<0.001$ ). 따라서, 가설 1은 채택되었다. 이것은 조직이 정보보안을 강조할수록 직원의 정보보안 참여 행동이 증가한다는 것을 말한다. 둘째, 정보보안 분위기는 정보보안 동기와 정보보안 지식에 모두 긍정적인 영향을 주었다( $\beta=0.598$ ,  $p<0.001$ ;  $\beta=0.661$ ,  $p<0.001$ ). 따라서, 가설 2와 3은 모두 채택되었다. 이러한 결과는 조직이 정보보안을 중요하게 생각할수록 직원의 정보보안 동기와 정보보안 지식이 향상된다는 것을 의미한다. 마지막으로 정보보안 동기와 정보보안 지식은 정보보안 참여 행동에 긍정적인 영향을 주었다( $\beta=0.220$ ,  $p<0.001$ ;  $\beta=0.330$ ,  $p<0.001$ ). 따라서, 가설 4와 5는 모두 채택되었다. 이와 같은 결과는 직원의 정보보안 동기와 정보보안 지식이

증가할수록 직원의 정보보안 참여 행동이 증가한다는 것을 뜻한다. 통제변수의 경우, 연령이 높을수록 정보보안 참여 행동이 증가하는 것으로 나타난 반면에 성별과 학력은 정보보안 참여 행동에 유의한 영향을 주지 않았다.

## V. 결론

### 5.1 연구결과 요약 및 시사점

조직의 성과를 향상시키기 위해서는 조직 구성원의 역할 외 행동이 중요하다. 본 연구는 정보보안 정책 맥락에서 역할 외 행동, 즉, 정보보안 참여 행동을 다루었다. 정보보안 참여 행동은 조직 구성원이 조직의 정보보안 수준 향상을 위해 자발적으로 정보보안 행동을 하는 것이다. 대표적으로, 동료에게 정보보안 관련 도

움을 주는 행동, 정보보안 강화를 위한 아이디어를 제시하는 행동이 있다. 정보보안 참여 행동은 정보보안 정책에 명시된 행동을 말하는 정보보안 정책 준수와는 명확히 구분된다. 최근 연구에서 정보보안 참여 행동이 정보보호 성과를 향상시키는 것으로 나타났으며(Hsu et al., 2015), 일부 연구에서 정보보안 참여 행동의 중요성을 강조하고 있다(Chen and Li, 2019; Guhr et al., 2019). 하지만, 정보보안 참여 행동의 선행요인을 살펴보는 연구가 아직까지 거의 이루어지지 않아서 정보보안 참여를 어떻게 해야 증대시킬 수 있는지에 대한 논의가 필요한 실정이다.

이에 우리는 사회 정보 처리 이론을 바탕으로 정보보안 분위기가 정보보안 참여 행동에 미치는 영향을 규명함으로써, 정보보안 정책 준수 행위에만 초점을 맞춘 기존 연구의 한계점을 보완하였다. 구체적으로, 우리는 Griffin and Neal(2000)의 프레임워크를 정보보안 분야에 적용하여 정보보안 분위기의 결정요인으로 정보보안 동기와 정보보안 지식을, 성과요인으로 정보보안 참여를 각각 제시하는 연구모형을 개발하고 이것을 실증적으로 분석하였다. 이를 위해 선행연구를 참고하여 정보보안 분위기를 2차 요인으로 개념화하였으며, 조직 내 공식 문서로 작성된 (개인)정보보호 정책이 존재하는 다양한 산업 군에 속하는 기업의 임직원 564명을 대상으로 설문조사를 실시하였다.

구조방정식모형 분석 결과, 첫째, 조직의 정보보안 분위기는 조직 구성원의 정보보안 참여 행동에 긍정적으로 영향을 주었다. 이는 조직 구성원의 정보보안 관련 역할 외 행동(i.e. 정보보안 참여 행동)을 이끌어내는데 있어서 조직

의 정보보안 분위기가 중요한 역할을 한다는 것을 말한다. 기존 연구에 따르면, 정보보안 참여 행동은 조직의 정보보안 정책 효과에 긍정적인 영향을 준다(Hsu et al., 2015). 따라서, 조직은 조직의 정보보호 수준을 향상시키기 위해서 조직 구성원의 정보보안 참여 행동을 증진시킬 필요가 있다. 본 연구결과는 이에 대한 실무적 시사점을 제공한다. 기업 내 정보보안 실무 담당자 및 경영진은 본 연구에서 개념화한 정보보안 분위기를 구성하는 세 가지 요소, 정보보안 실무관행, 정보보안 중시와 보안 교육에 초점을 맞추어 조직 구성원에게 우리 조직은 정보보안을 중요하게 여긴다는 인식을 심어줄 필요가 있다. 이것은 조직 구성원의 정보보안 참여 행동으로 이어지고, 결과적으로, 조직 내 정보보안 리스크를 감소시킴으로써, 정보 유출과 같은 기업에게 막대한 손실을 끼칠 수 있는 사고를 미연에 방지할 수 있다.

둘째, 정보보안 동기와 정보보안 지식은 정보보안 참여 행동에 모두 긍정적인 영향을 주었다. 이러한 결과는 조직 구성원의 정보보안 행동에 대한 동기가 유발될수록 그리고 조직 구성원의 정보보안 지식이 향상될수록 직원의 정보보안 참여 행동이 증가한다는 것을 말해준다. 이는 기존 안전 연구(Griffin and Neal, 2000)와 일치하는 결과로 정보보안 맥락에서도 정보보안 관련 역할 외 행동을 이끌어내기 위해서는 정보보안 동기와 정보보안 지식이 선행되어야 함을 시사한다.

마지막으로, 정보보안 분위기는 정보보안 동기와 정보보안 지식에 모두 긍정적인 영향을 주었다. 이와 같은 결과는 조직 구성원이 우리 조직은 정보보안을 중요하게 생각한다고 인식

할수록 정보보안 행동을 하고자 하는 동기가 유발되고, 정보보안 지식이 향상된다는 것을 말한다. 위의 결과에서 정보보안 참여 행동을 촉진 시키는데 있어서 정보보안 동기와 정보보안 지식이 중요하다는 것을 확인하였다. 따라서, 조직은 직원들의 정보보안 동기와 정보보안 지식을 증가시킬 필요가 있는데, 본 연구결과는 이에 대한 실무적 시사점을 제공한다. 즉, 기업 실무 담당자와 경영진은 직원의 정보보안 동기와 정보보안 지식을 이끌어내기 위해서 우선적으로 조직 내에 정보보안을 강조하는 분위기를 형성해야 한다.

본 연구는 정보보안 정책 문헌에 두 가지 학술적 공헌을 가진다. 첫째, 안전 연구에서 주로 사용하던 Griffin and Neal(2000)의 프레임워크를 정보보안 정책에 적용함으로써 정보보안 정책 연구에 대한 이해의 폭을 넓혔다. 기존 정보보안 정책 연구는 범죄학 등과 같은 분야에서 억제 이론(D'Arcy et al., 2009), 합리적 선택 이론(Bulgurcu et al., 2010), 보호동기이론(Johnston and Warkentin, 2010) 등을 가져와 정보보안 정책 준수의 선행요인을 살펴본 반면에, 본 연구는 사회 정보 처리 이론과 안전 연구를 참고하여 조직 행동 관점에서 조직 구성원의 정보보안 참여 행동을 설명하였다. 본 연구는 Griffin and Neal(2000)의 프레임워크가 정보보안 참여 행동을 잘 설명할 수 있음을 보였다. 향후 정보보안 정책 연구자가 정보보안 맥락 특성을 보다 세밀하게 반영한 새로운 프레임워크를 제시하는데 있어서 본 연구가 도움이 될 수 있다.

마지막으로, 본 연구는 역할 내 행동인 정보보안 정책 준수 행위에서 벗어나 역할 외 행동

인 정보보안 참여 행동을 고려함으로써 기존 연구를 확장했다는 점에서 학술적 기여가 있다. 조직 행동 문헌을 살펴보면, 조직 구성원의 자발적 행위, 즉, 역할 외 행동이 조직의 성과에 핵심적인 역할을 하는 것으로 나타난다. 이에 조직 행동 분야의 다수 연구자들은 역할 외 행동, 즉, 조직시민행동의 선행요인을 밝히고자 노력했다. 하지만, 지금까지 정보보안 정책 맥락에서는 이러한 연구가 부족했다. 이에 본 연구는 역할 외 행동을 정보보안 참여 행동으로 정의하고, 정보보안 참여 행동의 선행요인을 찾고자 하였으며, 정보보안 분위기가 정보보안 참여 행동을 촉진시키는데 중요한 역할을 한다는 것을 밝혔다. 본 연구는 역할 내 행동인 정보보안 정책 준수의 선행요인을 살펴보는 것에서 벗어나 역할 외 행동인 정보보안 참여 행동의 선행요인을 새롭게 규명함으로써 향후 정보보안 참여 행동에 초점을 맞춘 연구가 진행될 수 있는 토대를 제공한다.

## 5.2 한계점 및 향후 연구방향

본 연구는 다음과 같은 한계점을 지니고 있다. 첫째, 본 연구는 정보보안 분위기와 정보보안 참여 행동 간 관계를 규명하였는데, 이 관계를 조절할 수 있는 요인에 대해서는 살펴보지 않았다. 예를 들어, 부하-상사 관계(LMX, leader-member exchange)의 질에 따라 정보보안 분위기가 정보보안 참여 행동에 미치는 영향이 달라질 수 있다. 즉, 상사와 관계의 질이 나쁜 직원은 조직의 분위기가 아무리 정보보안을 강조한다고 하더라도, 조직을 위해서 정보보안 참여 행동을 하지 않을 수 있다. 향후 연구에

서 이를 살펴본다면 의미 있는 시사점을 제공할 수 있을 것으로 본다. 둘째, 본 연구는 정보보안 분위기를 2차 요인으로 개념화 하였는데, 여기에서 다루지 않은 다른 요인이 존재할 수 있다. 예를 들어, 본 연구에서는 최고 경영진의 관심을 제외하였는데, 향후 연구에서 이를 포함하여 살펴보는 것이 의미가 있을 것이다. 마지막으로, 본 연구는 정보보안 분위기가 정보보안 참여 행동에 어떻게 영향을 주는지를 살펴보는 것에 그 목적이 있는 관계로 정보보안 분위기의 선행 요인까지 살펴보지 못하였다. 본 연구에서 정보보안 분위기가 중요하다라는 것이 밝혀진 만큼 향후 연구에서 정보보안 분위기를 강화시킬 수 있는 요인을 찾는다면 실무적으로 의미가 있을 것이다.

위와 같은 한계점에도 불구하고 본 연구는 기존 연구에서 거의 다루지 않았던 정보보안 참여 행동을 고려했다는 점에서 학술적으로 공헌하는 바가 크다고 할 수 있다. 전 세계적으로 개인정보가 끊임없이 유출되고 있으며, 이 중에서 내부자에 의한 유출이 상당수 존재한다. 실제로, 최근에 대한민국 국방과학연구소에서 내부 직원에 의해 약 68만 건의 연구 자료가 유출된 것으로 드러났다. 또한, 내부 직원의 업무 과실로 인한 고객 및 임직원 정보 유출 사고도 매년 지속적으로 발생하고 있다. 이것은 정보보안 정책 준수를 강조하는 것만으로는 정보 유출 방지에 한계가 있다는 것을 말해준다. 이에 본 연구는 정보보안 분위기, 정보보안 동기, 정보보안 지식, 정보보안 참여 행동으로 구성된 모델을 제시하고 이를 실증적으로 분석함으로써 조직의 정보보안 리스크를 줄이고 조직의 정보보안 성과를 높이고자 하는 정보보안 실무자에

게 유용한 시사점을 줄뿐 아니라 정보보안 정책 연구자에게 향후 연구의 새로운 방향을 제시한다.

## 참고문헌

- 김기식, 박영석, “안전 분위기가 안전 행동 및 사고에 미치는 효과,” 한국심리학회지: 산업 및 조직, 제15권, 제1호, 2020, pp. 19-39.
- 김영민, “물류 안전 분위기가 물류 안전행동 및 물류 안전성과에 미치는 영향: 물류 안전지식과 물류 안전동기의 매개효과,” 무역학회지, 제45권, 제1호, 2020, pp. 259-277.
- 박상수, 이현철, “개인정보 유출의 정보전이 효과,” 정보시스템연구, 제27권, 제1호, 2018, pp. 193-224.
- 임명성, “조직의 보안 분위기가 개인의 기회주의 행동에 미치는 영향에 관한 실증 연구,” 디지털융복합연구, 제10권, 제10호, 2012, pp. 31-46.
- 정하진, 이수란, 손영우, “변혁적 안전리더십이 안전행동에 미치는 영향,” 한국심리학회지: 산업 및 조직, 제28권, 제2호, 2015, pp. 249-274.
- 황인호, 김대진, 김태하, 김진수, “조직의 정보보안 문화 형성이 조직 구성원의 보안 지식 및 준수의도에 미치는 영향 연구,” Information Systems Review, 제18권, 제1호, 2016, pp. 1-23.
- 황인호, 김상현, “SCO Framework 을 적용한 조

- 직과 조직원의 정보보안 준수 관계 연구,” *정보시스템연구*, 제28권, 제4호, 2019, pp. 105-129.
- 황인호, 허성호, “조직 내 정보보안 기술스트레스 완화와 준수 의도,” *정보시스템연구*, 제29권, 제1호, 2020, pp. 23-50.
- 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.
- Campbell, K., Gordon, L.A., Loeb, M.P., and Zhou, L., “The Economic Cost of Publicly Announced Information Security Breaches : Empirical Evidence from the Stock Market,” *Journal of Computer Security*, Vol. 11, No. 3, 2003, pp. 431-448.
- Cavusoglu, H., Mishra, B., and Raghunathan, S., “The Effect of Internet Security Breach Announcements on Market Value : Capital Market Reactions for Breached Firms and Internet Security Developers,” *International Journal of Electronic Commerce*, Vol. 9, No. 1, 2004, pp. 70-104.
- 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 and security*, Vol. 1, No. 3, 2005, pp. 18-41.
- Chen, H., and Li, W., “Understanding commitment and apathy in is security extra-role behavior from a person-organization fit perspective,” *Behaviour & Information Technology*, Vol. 38, No. 5, 2019, pp. 454-468.
- Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R., “Future directions for behavioral information security research,” *Computers & Security*, Vol. 32, No. 1, 2013, pp. 90-101.
- 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.
- Gefen, D., Straub, D., and Boudreau, M. C., “Structural equation modeling and regression: Guidelines for research practice,” *Communications of the association for information systems*, Vol. 4, Article 7, 2000.
- Goo, J., Yim, M. S., and Kim, D. J., “A path to successful management of employee security compliance: An empirical study of information security climate,” *IEEE Transactions on Professional Communication*, Vol. 57, No. 4, 2014, pp. 286-308.
- Griffin, M. A., and Neal, A., “Perceptions of safety at work: a framework for linking

- safety climate to safety performance, knowledge, and motivation,” *Journal of occupational health psychology*, Vol. 5, No. 3, 2000, 347-358.
- Guan, B., and Hsu, C., “The role of abusive supervision and organizational commitment on employees' information security policy noncompliance intention,” *Internet Research*, 2020.
- Hair, J. F., Ringle, C. M., and Sarstedt, M., “PLS-SEM: Indeed a silver bullet,” *Journal of Marketing theory and Practice*, Vol. 19, No. 2, 2011, pp. 139-152.
- Hofmann, D. A., Jacobs, R., and Landy, F., “High reliability process industries: Individual, micro, and macro organizational influences on safety performance,” *Journal of safety research*, Vol. 26, No. 3, 1995, pp. 131-149.
- Hsu, J. S. C., Shih, S. P., Hung, Y. W., and Lowry, P. B., “The role of extra-role behaviors and social controls in information security policy effectiveness,” *Information Systems Research*, Vol. 26, No. 2, 2015, pp. 282-300.
- Johnston, A. C., and Warkentin, M., “Fear Appeals and Information Security Behaviors: An Empirical Study,” *Management Information Systems Quarterly*, Vol. 34, No. 3, 2010, pp. 549-566.
- Katz, D., “The motivational basis of organizational behavior,” *Behavioral science*, Vol. 9, No. 2, 1964, pp. 131-146.
- Knapp, K. J., Marshall, T. E., Rainer Jr, R. K., and Ford, F. N., “Information security effectiveness: Conceptualization and validation of a theory,” *International Journal of Information Security and Privacy*, Vol. 1, No.2, 2007, pp. 37-60.
- Lee, M., and Lee, J., “The impact of information security failure on customer behaviors: A study on a large-scale hacking incident on the internet,” *Information Systems Frontiers*, Vol. 14, No. 2, 2012, pp. 375-393.
- Liu, C., Wang, N., and Liang, H., “Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment,” *International Journal of Information Management*, 54, 2020.
- Neal, A., and Griffin, M. A., “A study of the lagged relationships among safety climate, safety motivation, safety behavior, and accidents at the individual and group levels,” *Journal of applied psychology*, Vol. 91, No. 4, 2006, pp. 946-953.
- Padayachee, K., “Taxonomy of compliant information security behavior,” *Computers & Security*, Vol. 31, No. 5, 2012, pp. 673-680.

- Payne, S. C., Bergman, M. E., Beus, J. M., Rodríguez, J. M., and Henning, J. B., "Safety climate: Leading or lagging indicator of safety outcomes?," *Journal of Loss Prevention in the Process Industries*, Vol. 22, No. 6, 2009, pp. 735-739.
- Podsakoff, P. M., MacKenzie, S. B., Paine, J. B., and Bachrach, D. G., "Organizational citizenship behaviors: A critical review of the theoretical and empirical literature and suggestions for future research," *Journal of management*, Vol. 26, No. 3, 2000, pp. 513-563.
- Posey, C., Roberts, T. L., Lowry, P. B., and Hightower, R. T., "Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders," *Information & management*, Vol. 51, No. 5, 2014, pp. 551-567.
- Reichers, A. E., and Schneider, B., "Climate and Culture: An Evolution of Constructs," *Organizational climate and culture*, 1, 1990, pp. 5-39.
- Salancik, G. R., and Pfeffer, J., "A social information processing approach to job attitudes and task design," *Administrative science quarterly*, Vol. 23, No. 2, 1978, pp. 224-253.
- Schneider, B., Ehrhart, M. G., and Macey, W. H., "Organizational climate and culture," *Annual review of psychology*, Vol. 64, 2013, pp. 361-388.
- Siponen, M., and Vance, A. O., "Neutralization: New Insights into the Problem of Employee Systems Security Policy Violations," *Management Information Systems Quarterly*, Vol. 34, No. 3, 2010, pp. 487-502.
- Teng, C. C., Lu, A. C. C., Huang, Z. Y., and Fang, C. H., "Ethical work climate, organizational identification, leader-member-exchange (LMX) and organizational citizenship behavior (OCB)," *International Journal of Contemporary Hospitality Management*, Vol. 32, No.1, 2020, pp. 212-229.
- Van Dyne, L., and LePine, J. A., "Helping and voice extra-role behaviors: Evidence of construct and predictive validity," *Academy of Management Journal*, Vol. 41, No. 1, 1998, pp. 108-119.
- Vinodkumar, M. N., and Bhasi, M., "Safety management practices and safety behaviour: Assessing the mediating role of safety knowledge and motivation," *Accident Analysis & Prevention*, Vol. 42, No. 6, 2010, pp. 2082-2093.
- Vroom, V. H., *Work and motivation*, NY: John Wiley and Sons, 1964.

**박 재 영 (Park, Jaeyoung)**



연세대학교 정보대학원에서 박사과정을 수료하였다. 숭실대학교에서 학사, 연세대학교 정보대학원에서 정보시스템 석사학위를 취득하였다. 주요 관심분야는 개인정보보호, 정보보안, 프라이버시이다.

**김 범 수 (Kim, Beomsoo)**



현재 연세대학교 정보대학원 교수로 재직 중이다. 서울대학교에서 학사와 석사를 취득하였으며, 미국 University of Texas at Austin에서 경영학 박사학위를 취득하였다. 주요 관심분야는 Privacy laws and policies, Information security and Privacy practices, IT values and ethics, Knowledge management, Economic issues in IT industry이다.

<Abstract>

## **The Impact of Organizational Information Security Climate on Employees' Information Security Participation Behavior**

Park, Jaeyoung · Kim, Beomsoo

### **Purpose**

Although examining the antecedents of employees' extra-role behavior (i.e. information security participation behavior) in the information security context is significant for researchers and practitioners, most behavioral security studies have focused on employees' in-role behavior (i.e. information security policy compliance). Thus, this research addresses this gap by investigating how organizational information security climate influences information security participation behavior based on social information processing theory and Griffin and Neal's safety model.

### **Design/methodology/approach**

We developed a research model by applying Griffin and Neal's safety model to the information security context and then tested our research model by conducting an online survey for employees of organizations with information security policies. Structural equation modeling (SEM) with SmartPLS 3.3.2 is used to test the corresponding hypothesis.

### **Findings**

Our results show that organizational information security climate, information security knowledge, information security motivation are effective in motivating information security participation behavior. Also, we find that organizational information security climate positively influences both information security knowledge and information security motivation. Our findings emphasize the importance of organizational information security climate because it is capable of affecting employees on information security participation behavior. Our study contributes to the literature on information security by exploring the role of organizational information security climate in enhancing employees' information security participation behavior.

**Keyword:** Social Information Processing Theory, Information Security Climate, Information Security Participation, Information Security Policy, Security Motivation, Security Knowledge

\* 이 논문은 2020년 10월 29일 접수, 2020년 12월 4일 게재 확정되었습니다.