JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 21, No. 9, pp. 1653-1663, Sep. 2020

Check for updates

정보보안 정보 제공 활동과 피드백이 업무 장애 및 준수의도에 미치는 영향

황 인 호[1]
[1]국민대학교 교양대학 조교수

The Effect of Information Security Delivery Activities and Feedback on Work Impediment and Compliance Intention

Inho Hwang[1]
[1]Assistant Professor, Department of General Education, Kookmin University, Seoul 02707, Korea

[요 약]

최근 많은 조직들은 효과적인 정보보안 관리 필요성을 인식하고 있으며, 엄격한 보안 정책 도입 및 기술에 대한 투자를 높이고 있다. 하지만, 정보보안 정책 도입은 개인의 업무 장애를 높여 보안 준수에 부정적인 영향을 미칠 가능성이 있다. 본 연구의 목적은 부정적 행동의 원천인 정보보안 업무장애를 감소시키기 위한 방안을 제시하는 것이다. 설문은 금융업에 근무하는 조직원들을 대상으로 하고 284개의 유효 표본을 확보하였으며, 분석은 구조방정식 모델링을 실시하였다. 가설 검증 결과, 업무장애가 준수의도를 감소시키며, 정보보안 가시성이 업무 장애를 완화하는 것을 확인하였다. 또한, 정보보안 피드백이 업무장애와 준수의도간의 부정적 영향 관계를 완화하는 것을 확인하였다. 연구의 시사점은 엄격한 정보보안 수준의 부정적 영향과 완화 조건을 도출함으로써, 조직의 전략 수립 방향을 제시하였다.

[Abstract]

Recently, many organizations are recognizing the need for effective information security management and are increasing their investment in strict security policies and technologies. However, the adoption of the various information security systems may increase the work impediment of employee and may negatively affect the security compliance level of organization. The purpose of this study is to present the measures to reduce the information security work impediment which is the source of negative behavior. The survey was targeted at employees working in the financial industry and secured 284 valid samples. And the analysis performed structural equation modeling. As a result of hypothesis testing, it was confirmed that work impediment reduces compliance intention and security visibility mitigates work impediment. Additionally, it was confirmed that security feedback reduces the negative affect relationship between work impediment and compliance intention. The implication of this study is to suggest the organizational strategy direction by deriving the conditions to mitigate the negative effects of the strict level of information security.

색인어 : 커뮤니케이션, 가시성, 피드백, 업무 장애, 준수의도

Key word : Communication, Visibility, Feedback, Work impediment, Compliance intention

http://dx.doi.org/10.9728/dcs.2020.21.1.1653

Received 30 July 2020; **Revised** 18 August 2020
Accepted 18 August 2020

***Corresponding Author; Inho Hwang**

Tel: +82-02-910-6473
E-mail: hwanginho@kookmin.ac.kr

Ⅰ. 서 론

조직에서 정보 관리의 중요성이 지속적으로 증가함에 따라, 많은 기업들이 정보보안 시스템에 대한 투자를 높이고 있다. 실제로, 2019년의 전 세계 정보보안 시장의 규모는 1,565억달러에 달하며, 2027년까지 10.0% 수준의 연평균성장율로 가파르게 성장할 것으로 예측 되고 있다[1]. 보안 시스템에 대한 강력한 투자에도 불구하고, 정보보안 관련 사고는 감소하지 않고 있다. Verizon[2020]은 지난 10여년간 조직 내 정보보안 사고 유형을 분석하고 위협 요인에 대한 대처의 필요성을 제시하고 있는데, 보고서에 따르면 해킹, 멀웨어 등 시스템에 대한 침입을 통해서 발생한 보안 사고는 전체의 60~70% 수준이었으며, 정보보안 시스템에 접근이 가능한 내부 구성원들의 데이터 오남용 및 고의성 등으로 인하여 발생한 보안 사고는 20~30% 수준에 달하는 것으로 제시되고 있다. 특히, 조직의 정보보안 사고는 외부에 의해 드러나지 않는 한 개인 및 조직 차원에서 감추고자 하는 성향이 높은 것으로 나타나, 실제로는 보고된 사례보다 많은 사고가 발생하고 있는 것으로 파악되고 있다[2]. 즉, 오늘날 조직은 외부의 침입 등으로 인한 보안 사고 발생 가능성에 대한 높은 수준의 경각심을 요구받고 있다. 더욱이, 최근 전 세계적인 영향을 미친 코로나(COVID-19) 사태는 기업들의 업무 방식을 스마트 워크와 같이 비대면 방식의 업무 체계의 도입을 서두르게 하고 있어, 내부자들의 정보노출 가능성은 결코 낮아지지 않고 있다. 즉, 내부자들의 정보보호의 중요성 및 행동에 대한 의식 개선 지원 노력이 필요한 시점이다[3].

조직원에 의한 정보보안 사고 감소를 위한 선행 연구는 개인의 보안 준수 행동 및 의도 개선을 위한 동기적 관점에서 접근되어 왔으며, 사회학, 심리학 등의 이론을 활용하여 높은 시사점을 제시해왔다. 예를 들어, 조직 차원의 보안 준수에 대한 명확하고 강력한 제재가 개인의 보안 준수 행동을 높인다는 제재이론(deterrence theory)을 보안 분야에 적용한 연구[4,5], 보안 관련 행동은 동기 형성으로 인하여 결정된다고 보고, 내부적으로 형성된 동기와 외부적인 영향으로 인한 동기로 구분하여 동기 유형(motivation theory)을 상세하게 제시한 연구[6], 개인의 행동은 결국 합리적 의사결정에 의해 이루어지며, 보안 관련 행동의 혜택과 비용을 상세히 분석하여 보안 준수로 이어진다는 합리적선택이론(rational choice theory) 관련 연구[7], 그리고 개인의 행동이 태도의 형성, 외부의 영향, 자기 효능감 등으로 구성되어 있다는 계획된 행동이론(theory of planned behavior)과 보안 관련 타 이론과 연계한 연구[8] 등이 제시되고 있다. 이와 같은 선행 연구는 개인 관점에서 정보보안 준수 행동을 결정하는 동기적 매커니즘을 제시하였다는 측면에서 시사점을 가진다.

최근 몇몇 연구들은 기술 도입의 부정적인 측면인 기술스트레스(techno stress)의 문제점을 제시하고 있다[9,10]. 즉, 강력한 기술의 도입이 신 기술에 대한 부담감, 기존 업무 체계에 대한 변화를 발생시켜 조직원의 불만을 야기시키는 문제가 있음을 제시하고 있다. 정보보안 분야에서도 보안 기술에 의한 걱정, 업무 장애, 나아가 스트레스까지 발생시킨다는 연구[11,12]가 최근 제시되고 있다. 즉, 보안 기술의 지속적인 변화는 개인들의 업무 체계에 문제를 일으켜 준수행동에 부정적인 영향을 미치게 된다. 하지만, 보안 기술의 부정적인 영향에 대한 연구는 아직까지 탐색적 관점에서 대부분 접근되어, 보안 기술에 의한 부정적 영향을 최소화시키기 위한 조직 차원의 노력 방안을 제시한 연구들이 매우 부족한 실정이다.

본 연구는 정보보안 정책 및 기술 도입에 의해 발생되는 조직원의 업무 장애를 완화시키기 위한 방안을 정보보안 정보 제공 활동 관점에서 살펴보고자 한다. 세부적으로, 정보보안 업무 장애가 보안 준수의도에 미치는 부정적인 영향을 제시하고, 업무 장애를 완화하기 위한 조직 차원의 보안 정보 제공 활동 요인(커뮤니케이션, 가시성)을 제시한다. 또한, 개인의 보안 관련 활동에 대한 조직 차원의 피드백 활동이 보안 정보 제공 활동 – 업무 장애 – 준수의도로 이어지는 부정적 관계를 완화하는 역할을 하는지 확인한다. 연구 모델 검증은 정보보안을 엄격하게 도입하고 있는 금융업에 재직 중인 근로자들을 대상으로 설문조사를 실시하고, 구조방정식모델링을 통해 결과를 확인한다. 연구의 결과는 개인에게 발생 가능한 보안에 의한 업무장애를 최소화하기 위한 조직 차원의 보안 관련 정보 제공 방식을 제시한다는 측면에서 이론적, 실무적 시사점을 가질 것으로 판단한다.

Ⅱ. 이론적 배경

2-1 정보보안 준수의도

정보보안 사고는 보안 정책 및 기술이 엄격하게 도입된 금융 산업에서도 지속적으로 발생하고 있다. 2019년 미국 주요 은행인 캐피털원의 해킹 사건은 1억명이 넘는 고객 정보를 외부로 노출시켰으며[13], 2013년 국내 A은행의 내부직원에 의한 고객 정보 복제 사건은 약 3만 4천여건의 신용정보를 외부로 노출시켰다[14]. 이와 같은 사건들은 높은 수준으로 개인 정보를 활용하고 있는 금융 산업에서 조차 보안 사고가 발생가능하다는 것으로, 조직 내외부의 정보 노출 위협을 최소화하기 위한 조직차원의 강력한 노력이 필요함을 제시한다. 세부적으로, 외부자의 보안 위협은 새로운 정보기술 및 정책의 도입으로 가능하지만, 내부자의 보안 위협은 개인들의 긍정적이고 자발적인 보안 준수 행동을 요구하도록 유도하는 것이 가장 중요한 조건이다[11].

West[2008]는 내부자의 정보보안 관련 행동 정보가 항상 조직보다 더 많기 때문에, 대리인 문제가 발생하며 개인은 언제든 도덕적 해이 관점에서 불성실한 행동 정보를 감출 수 있다고 보았다. 즉, 내부자의 정보보안 행동은 개인이 주어진 환경 내 심리적으로 행동 유무를 선택하는 조건이기 때문에, 조직은 개인의 보안 행동이 바람직하게 이어질 수 있도록 지원하는 것이 필

요하다고 보았다. 즉, 조직원의 정보보안 결과가 조직의 요구수준에 맞춰지기 위해서는 자발적인 준수의도 형성이 필요하다. 정보보안 준수의도는 조직의 주요 정보들을 내부, 외부의 위협으로부터 보호하고자 하는 개인들의 자발적 행동 의지로서[16], 보안 준수의도가 높은 개인들은 조직의 보안 관련 목표에 대한 긍정적이고 자발적인 행동을 함으로써, 공동체적 관점에서의 정보 관리를 할 가능성이 높다[17]. 반면, 정보보안을 위하여 정보기술의 도입은 개인의 업무 관련 문제를 발생시켜, 준수의도를 감소시킬 수 있어 [18], 개인의 보안 관련 문제를 감소시키기 위한 노력이 필요한 상황이다. 본 연구는 정보보안에 의해 발생되는 업무 장애와 이를 완화하기 위한 요인을 제시함으로써, 보안 준수 향상 방안을 제시하고자 한다.

2-2 정보보안 업무 장애

정보보안 정책과 기술의 도입은 조직의 정보보안 수준을 직접적으로 높이는 효과를 가진다[5]. 최근에는 웹 클라우드 시스템, 웹 정보 공유 시스템 등을 통해 개인이 직접 데이터를 가지지 않도록 하지만, 정보 공유가 가능하도록 하는 기업들이 증가하고 있다. 하지만, 정보보안에 대한 조직 차원의 엄격한 도입 및 지속적인 변화는 개인의 업무 절차 및 방식 등을 변화시키는 요인이기 때문에, 도입 초기에는 개인 업무 체계를 흔들어 스트레스를 일으키는 요인이 된다[11,12]. 또한, 조직에서 개인에게 주어진 1차적 목표는 정보보안이 아니라 성과 달성에 있기 때문에, 정보보안의 절차적 어려움 및 권한에 대한 문제 등은 개인의 정보보안 준수를 어렵게 만드는 요인이 된다[12].

업무 장애는 개인의 일상적인 업무 관련 활동에 있어 정보보안 정책의 요구사항을 준수함으로써 추가적으로 발생하는 업무에 부정적인 영향을 미치는 수준을 의미한다[7]. 예를 들어, 조직에서 요구하는 보안 관련 요구사항은 조직의 권한 승인 절차를 추가함으로써, 동료간의 정보 공유 활동을 어렵게 만들거나, 외부 파트너와의 협력 활동을 원천 차단하는 효과를 가질 수 있다. 또한, 엄격해진 보안 기술은 기존과는 다른 방식의 시스템을 이해하기 위한 노력을 개인에게 요구하여 업무 처리에 어려움을 줄 수도 있다. 즉, 정보보안 관련 활동은 개인이 업무 과정에서 지켜야할 추가적인 행동 체계이기 때문에 업무상 장애를 발생시킬 가능성이 존재한다.

업무장애는 보안 준수 행동에 부정적 영향을 미치는 요인이다. 합리적 선택이론을 정보보안 분야에 적용한 Bulgurcu et al.[2010]은 보안 정책 도입으로 인하여 추가적으로 발생한 업무 과정 및 행동 요구는 개인의 업무 장애를 일으켜 비용적 관점에서 보안을 판단하게 하는 요인이라고 하였으며, 나아가 준수의도에 부정적 영향을 준다고 보았다. Hwang et al.[2017]은 개인의 보안 미준수 원인을 제시하였으며, 보안 기술 도입으로 인한 업무 장애가 준수의도를 감소시키는 조건임을 증명하였다. 또한, Tarafdar et al.[2011]은 조직에 도입한 기술에 의해 스트레스가 발생되고 개인의 업무 관련 스트레스를 높여 생산성을 감소시킨다고 하였으며, Jena[2015]는 기술 관련 스트레스가 직업 만족도를 감소시켜 조직 몰입까지 부정적인 영향을 미치는 것을 확인하였다. 본 연구는 선행 연구를 기반으로 정보보안 업무 장애가 조직원의 보안 준수의도를 감소시킬 것으로 판단하고 연구가설을 제시한다.

H1 : 정보보안 업무장애는 정보보안 준수의도에 부정적인 영향을 미칠 것이다.

2-3 정보보안 커뮤니케이션

조직 내 커뮤니케이션의 목표는 조직원들에게 조직이 추구하는 비전, 목표, 가치 정립 등 방향성을 제시하고 행동하도록 이해시키는데 있다[20]. 조직 내 커뮤니케이션의 개념을 살펴보면, Frank and Brownell[1989]은 체계적이고 원활한 업무를 위하여 조직 내 이해관계자들을 대상으로 수행하는 정보 전달 활동으로 정의하였으며, Welch and Jackson[2007]은 조직 목적 달성을 위하여 다양한 구성원들의 상호 교환 활동을 통한 연계 활동 수준으로 정의하였다. 즉, 조직 내 커뮤니케이션은 조직의 목표 및 가치 달성에 기여할 수 있도록 구성원 상호 간의 정보 교류를 하는 수준으로 정의할 수 있다.

조직 내 커뮤니케이션이 활발할 경우 조직의 특정 목표달성에 도움을 준다. 조직원들의 원활한 상호 교류는 통해 조직의 목표 및 성과 체계를 이해하도록 도울 뿐 아니라, 업무의 효율적 수행 절차 및 행동 방향 등을 확립하도록 도움으로써, 업무 생산성에 긍정적인 영향을 주고 나아가 조직 성과 향상을 일으키는 선행 조건이다[23]. 반대로 커뮤니케이션이 부족한 조직들은 구성원 상호 간의 업무적 활동 및 산출물들을 이해하기 어렵기 때문에 업무 비효율성이 증가하게 되어 목표 달성이 어려워진다[24].

더욱이, 커뮤니케이션 활성화는 조직의 정보시스템 활용 수준뿐만 아니라 정보보안 기술 및 정책 준수 행동을 증가시키는 요인이다. Jimenez- Castilo and Sanchez-Perez[2013]는 정보시스템 활용 관점에서 커뮤니케이션은 조직에 도입된 기술 및 새로운 표준 등 관련 정보에 대하여 노하우 등을 이전받음으로써, 보다 빠르게 개인들의 지식을 형성시키는 선행 조건이라고 하였으며, Hwang and Kim[2016]은 개인의 정보보안 준수는 조직의 환경적 조건에 영향을 받는다고 보고, 정보보안 환경 인식을 위한 커뮤니케이션 제공 활동이 개인의 정보보안 준수 강화 요인과 억제요인을 거쳐 준수의도를 높이는 선행 요인임을 증명하였다. 본 연구는 선행 연구를 기반으로 정보보안 관련 커뮤니케이션이 조직원의 보안 준수의도를 증가시킬 것으로 판단하고 연구가설을 제시한다.

H2 : 정보보안 커뮤니케이션은 정보보안 준수의도에 긍정적인 영향을 미칠 것이다.

최근 기업들은 IT기술을 활용하여 다양한 커뮤니케이션 채널(인트라넷, 이메일, SNS 등)을 제공함으로써 조직원들이 상호간에 업무관련 정보를 확보하고 성과로 이어지도록 지원하고 있다. 조직 내 다양한 커뮤니케이션 활동은 조직-개인의 관

계에서 상호 교환을 통해 개인에게 나타날 수 있는 부정적 문제를 최소화할 수 있는 기반이 된다[27]. 즉, 커뮤니케이션은 조직 구성원 상호간 관련 정보를 교환함으로써 조직에서 받을 수 있는 다양한 불확실성을 감소시킬 수 있는 선행 요인이다[28]. 이러한 커뮤니케이션의 특성은 정보보안 분야에서도 반영되고 있다. Hwang and Kim[2016]은 조직이 구축한 정보보안 커뮤니케이션 체계가 조직원의 보안 관련 업무 장애 및 보안 시스템 활용 걱정을 감소시키는 선행 조건임을 증명하였다. 본 연구는 선행연구를 기반으로 정보보안 관련 커뮤니케이션이 정보보안 업무 장애를 감소시킬 것으로 판단하고 연구가설을 제시한다.

H3 : 정보보안 커뮤니케이션은 정보보안 업무장애를 완화할 것이다

2-4 정보보안 가시성

조직 기술 관련 연구에서, 가시성에 대한 정의는 연구자별 조금씩 차이가 있다. Venkatesh et al.[2003]은 조직 내 다른 사람들이 사용하는 시스템 활용을 관찰하는 범위로 가시성을 정의하였으며, Hwang et al.[2019]은 단순한 시스템 활용에 대한 관찰을 넘어 타인의 시스템 활용에 대한 사용 수준의 이해까지 확대하여 가시성을 정의하였다. Hwang et al.[2017]은 조직과 개인의 관점에서 가시성을 제시하였는데, 조직의 바람직한 목표에 맞는 결정을 할 수 있도록 관련 정책, 활동, 사건 등을 눈에 띄도록 제공하는 수준으로 정의하였다. 즉, 개인 관점에서 가시성은 특정 활동에 대한 관찰을 통해 관련 특성을 이해하는 개념이며, 조직 관점에서 가시성은 특정 활동에 대한 명확한 정보를 제공함으로써 지식을 확보할 수 있도록 지원하는 개념이다. 대상의 차이가 있으나 공통적으로 특정 활동에 대하여 실제로 보고 이해하는 수준을 의미한다.

정보보안 관점에서 가시성은 정보보안 정책 준수에 영향을 주는 요인이다. 조직원은 정보보안 관련 활동에 대한 정보를 확보함으로써 자신의 행동을 합리화하고자 하는 경향이 있다[15]. 즉, 자신을 둘러싼 보안 환경 및 주변 사람들의 행동 정보가 본인의 정보보안 행동 합리화에 높은 영향을 준다[31]. 따라서, 정보보안 정책과 관련된 설득력 있는 메시지가 조직 전체에 영향을 줄 때, 개인은 보안 준수라는 합리적 의사결정을 내릴 수 있다. 예를 들어 휴게 공간의 영상 기반의 보안 캠페인, 포스터, 커피잔 광고 등은 개인에게 정보보안 가시성을 확보하도록 도움으로써 보안 지식을 형성하도록 돕는다[32]. 실제로, Hwang et al.[2019]는 정보보안 가시성이 개인의 보안 인지 수준을 높여 정보보안 준수의도에 긍정적인 영향을 주는 요인이라고 하였으며, Siponen et al.[2010]은 정보보안 정책에 대한 가시적 활동이 개인의 준수의도를 높이는 것을 증명하였다. 본 연구는 선행 연구를 기반으로 정보보안 가시성이 조직원의 보안 준수의도를 증가시킬 것으로 판단하고 연구가설을 제시한다.

H4 : 정보보안 가시성은 정보보안 준수의도에 긍정적인 영향을 미칠 것이다.

조직원이 조직 요구수준에 적합한 정보보안 행동을 하기 위해서는 보안 관련 행동 문화 형성이 무엇보다 중요하다[31]. 긍정적인 보안 문화 형성을 위해서는 조직원 관점에서 정보보안 기술, 절차, 행동, 통제 방법 등의 다양한 정보를 보다 쉽게 제공함으로써, 빨리 이해할 수 있도록 지원하는 것이 필요하다[32]. 즉, 개인에게 발생되는 추가적인 보안 활동에 대한 목적, 절차 등을 이해할 수 있도록 지원하는 것이 보안 행동에 도움을 준다.

뿐만 아니라, 정보보안 가시성은 개인의 불확실성을 감소시켜 준수의도에 긍정적인 영향을 준다. Hwang et al.[2017]은 개인의 정보보안 미준수 원인으로 업무장애, 정보보안 걱정, 동료들의 미준수를 제시하였으며, 정보보안 가시성 확보가 미준수 원인 완화의 방법이라고 하였다. 본 연구는 선행 연구를 기반으로 정보보안 가시성이 조직원의 정보보안 업무장애를 감소시킬 것으로 판단하고 연구가설을 제시한다.

H5 : 정보보안 가시성은 정보보안 업무장애를 완화할 것이다

2-5 정보보안 피드백

피드백은 조직 내 개인에게 부여된 역할에 대한 활동 과정, 결과 등에 대하여 정보를 제공하는 것을 의미한다[33]. 피드백은 상사, 동료 뿐만 아니라 고객, 파트너 등 조직에서 개인과 연계 되어 있는 이해관계자들로부터 다양한 형태와 방식으로 제공될뿐만 아니라, 단순 정보 제공으로서의 역할을 넘어 개인 행동에 대한 타인의 평가까지 포함되어 있기 때문에 개인의 역할 수립 및 성과 달성에 중요한 역할을 한다[34].

조직에서 피드백은 조직의 목표, 비전, 가치를 조직원에게 전달하고 행동하도록 돕는 요인이다. Campion and Lord[1992]는 조직의 피드백 시스템이 특정 목표 달성을 위한 가이드라인 역할을 하기 때문에, 개인이 관련 행동을 수행하는 과정에서 직, 간접적으로 도움을 주어 성과 달성에 도움을 준다고 하였다. 즉, 피드백은 개인의 행동 정보를 분석하고 개선하도록 도움으로써, 조직 목표 달성에 도움을 주는 요인이다[33].

정보보안 분야에서도 보안 행동에 대한 조직 차원의 모니터링 및 피드백 활동은 개인의 행동 준수에 긍정적인 영향을 주는 요인이다. D'Arcy et al.[2009]는 정보보안 미준수 행동 완화를 위한 조건을 제재와 보안 시스템 구축 및 지원 관점에서 제시하였다. 그들은 정보보안에 대한 모니터링 시스템 구축을 통한 보안 행동에 대한 피드백이 개인의 미준수 행동을 완화하는데 중요한 역할을 하는 것을 확인하였다. 또한, Knapp et al.[2009]은 정보보안 정책에 대한 행동에 모니터링 시스템 구축이 도움을 준다고 하였다.

더욱이, 조직 내 피드백 체계 구축은 구성원의 관련 스트레스를 감소시키거나 조절시키는 요인이다. Andrews and Kacmar[2001]은 조직에서 제공할 수 있는 피드백 유형을 조직 피드백, 업무 피드백 등 5가지로 구분하였으며, 스트레스와의 부정적 관계에 있음을 증명하였다. 특히 조직 피드백은 개인의

업무스트레스(업무 갈등, 업무 모호성)을 완화하는 것을 증명하였다. Hon et al.[2013]은 업무스트레스와 생산성의 부정적 관계가 있다고 보았으며, 긍정적인 업무 피드백 활동은 긍정적 조절효과를 가지지만, 부정적 피드백은 부정적 조절효과를 가지는 것을 확인하였다. 본 연구는 선행연구를 기반으로 정보보안 피드백 활동이 정보보안 정보 제공활동-업무장애-준수의도 간의 관계를 조절할 것으로 판단하고 다음의 연구가설을 제시한다.

H6 : 정보보안 피드백은 업무장애와 준수의도간의 관계에 조절효과를 가질 것이다.

H7 : 정보보안 피드백은 커뮤니케이션과 업무장애간의 관계에 조절효과를 가질 것이다.

H8 : 정보보안 피드백은 가시성과 업무장애간의 관계에 조절효과를 가질 것이다.

Ⅲ. 연구 모델 및 방법

3-1 연구모델

본 연구는 정보보안 정책 도입으로 인하여 발생하는 조직원의 업무장애 요인을 극복하기 위하여, 정보보안 관련 다양한 정보 제공 활동의 중요성과 개인에 대한 보안 활동 피드백의 중요성을 제시하는 것을 목적으로 한다. 즉, 업무 장애에 의해 감소된 개인의 정보보안 준수의도를 완화하기 위한 선행 조건을 제시하며, [그림 1]과 같다.

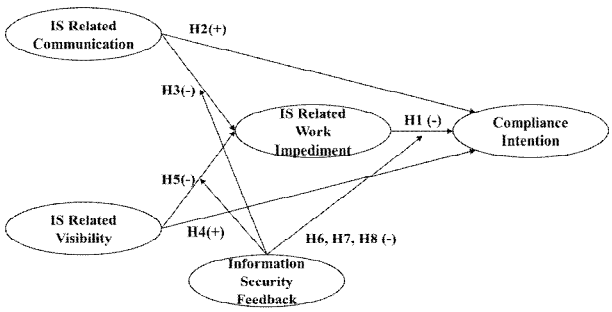

그림 1. 연구 모델
Fig. 1. Research Model

3-2 실증 분석 방법 및 표본 수집

연구 가설에 대한 실증 분석은 설문지 기법을 통해 데이터를 확보하고 구조방정식모델링을 적용하여 영향 관계를 증명하고자 한다. 우선, 정보보안 및 조직 내 개인의 특정 행동 관련 선행연구를 통해 연구 모델에 적용될 5개 요인과 요인별 다항목 기반의 설문 항목을 도출하였으며, 정보보안 분야에 맞도록 7점 리커트 척도로 재구성하였다.

종속변수인 준수의도는 "조직의 보안 목표 수준을 준수하고자하는 조직원의 의도 수준"으로 정의하였으며, Chen et al.[2012]의 연구를 통하여 3개의 설문 항목을 도출하였다. 정보보안 관련 업무 장애는 "정보보안 정책으로 인하여 추가되는 업무 절차 및 불편함 수준"으로 정의하였으며, Bulgurcu et al.[2010]의 연구를 통하여 4개의 설문 항목을 도출하였다. 정보보안 관련 정보 제공 활동요인은 커뮤니케이션과 가시성을 제시하였다. 정보보안 커뮤니케이션은 "조직 내 다양한 커뮤니케이션 채널로서 정보보안 관련 정보를 제공하는 수준"으로 정의하고 Jiménez-Castillo and Sánchez-Pérez[2013]의 연구를 통하여 3개의 설문 항목을 도출하였다. 정보보안 가시성은 "정보보안 관련 정보 및 행동 체계 등이 조직 내 노출되는 수준"으로 정의하였으며, Siponen et al.[2010]의 연구를 통하여 3개의 설문 항목을 도출하였다.

조절 변수인 정보보안 피드백은 "조직으로부터 정보보안 관련 행동의 정보 및 평가를 받는 수준"으로 정의하였으며, Wright[2004]의 연구를 통하여 4개의 설문 항목을 도출하였다. 설문 문항의 내적 타당도를 높이기 위하여, 설문을 구성한 후, 정보보안 정책을 도입한 조직에서 근무하는 대학원생 10명을 선정하여 문항의 적절성을 확인하였으며, 설문 항목을 완성하였다.

설문 대상은 금융업에서 근무하는 직장인이다. 직무적 특성으로는 정보보안을 일상 업무에 적용해야 하는 근로자를 대상으로 하였다. 즉, 전산팀, 보안 팀 등 IT 부서에서 근무하는 근로자는 제외하였다. 보안 부서를 제외한 이유는 업무의 목표가 보안 준수에 있으나, 그 외 부서의 경우 업무 상 우선적 목표가 보안 준수가 아닌 개인의 성과 달성에 있기 때문에 차이가 크다고 판단했기 때문이다. 설문은 특정 대학의 재직자 전형에 다니는 직장인 중 금융업에 근무하는 학생들만을 대상으로 하였으며, 설문지 배포 전 설문의 목표와 통계적 활용 방법 등에 대하여 명확하게 고지하고, 설문 응답을 거절한 학생들을 제외하고 설문을 수집하였다. 설문지는 총 300부를 배포하였으며, 불성실한 응답 등을 제외한 284부의 설문을 분석에 활용하였다. 284개 표본의 인구통계학 특성은 [표 1]과 같다.

표 1. 인구통계학적 특성
Table 1. Demographic Characteristics

Demographic Categories		Frequency	%
Gender	Male	103	36.3
	Female	181	63.7
Age	< 30	64	22.5
	31 ~ 40	116	40.8
	41 ~ 50	92	32.4
	> 50	12	4.2
Job Position	Staff	109	38.4
	Assistant Manager	54	19.0
	Manager	55	19.4
	General Manager	66	23.2
Total		284	100.0

Ⅳ. 가설 검증

4-1 신뢰성 및 타당성 분석

본 연구는 구조방정식모델링을 통하여 연구 가설을 검증하고자 한다. 분석에는 SPSS 21.0과 AMOS 22.0을 활용하였으며, 우선 구조모델 요인의 타당성과 신뢰성 분석을 실시한다.

신뢰성 분석은 요인의 구성요인이 다항목으로 구성될 때, 각 요인들이 일관성을 가지고 구성되어 있는지를 확인하는 분석으로, SPSS 21.0의 탐색적 요인분석을 통해 요인별 묶이는지 확인하고 cornbach's α를 활용하여 수준을 검증한다. Nunnally[1979]는 요인별 cornbach's α를 0.7이상이 필요하다고 보았으며, 분석결과 요인들의 17개 구성항목 중 4개 항목(가시성3, 업무장애 4, 피드백 1, 피드백4)을 제외하였으며, 신뢰성을 확보하였다[표 2].

타당성 분석은 연구 모델의 요인들의 구성이 요인 간 차별화가 되어 있고, 요인 내 연계된 특성을 가지고 있는지 확인하는 것으로서 집중타당성 분석과 판별타당성 분석을 실시한다. 집중타당성분석은 개념신뢰도(construct reliability) 분석과 평균분산추출(average variance extracted) 분석을 통해 확인한다[40].

집중타당성 분석을 위해서 AMOS 22.0을 이용하여 확인적 요인분석을 실시하였으며, 모델 적합도는 적합한 것으로 나타났다(χ2/df = 1.662, GFI = 0.952, AGFI = 0.921, CFI = 0.989, NFI = 0.973, RMSEA = 0.048). 개념신뢰도와 평균분산추출의 적합성은 각각 0.7이상, 0.5이상을 요구하며[41], 결과는 연구모델의 요인 전체가 합당한 것으로 나타났다[표 2].

표 2. 구성요인의 타당성 및 신뢰성 결과
Table 2. Result for Construct Validity and Reliability

Constructs		Factor Loading	Cronbach's Alpha	CR	AVE
SC	SC1	.870	0.921	0.868	0.688
	SC2	.852			
	SC3	.857			
SV	SV1	.863	0.865	0.763	0.618
	SV2	.905			
WI	WI1	.952	0.943	0.821	0.605
	WI2	.955			
	WI3	.898			
CI	CI1	.904	0.949	0.962	0.893
	CI2	.906			
	CI3	.896			
SF	SF2	.869	0.880	0.794	0.658
	SF3	.858			

※ SC(Security Communication), SV(Security Visibility), WI(Work Impediment), CI(Compliance Intention), SF(Security Feedback)

추가적으로, 모델 내 요인간의 차별성이 존재하는 것을 확인하기 위해 판별타당성 분석을 실시하였다. 판별타당성 분석은 요인의 상관관계 분석 값과 평균분산추출의 제곱근 값을 비교하는 것으로, 상관관계 값이 낮게 나타날 때 의미를 가진다[41]. 분석 결과 판별타당성이 존재하는 것으로 나타났다[표 3].

표 3. 판별타당성 결과
Table 3. Result for Discriminant Validity

Constructs	1	2	3	4	5
SC	***0.830***				
SV	.435**	***0.761***			
WI	.207**	.275**	***0.781***		
CI	.494**	.424**	.279**	***0.942***	
SF	.515**	.461**	.398**	.461**	***0.929***

※ SC(Security Communication), SV(Security Visibility), WI(Work Impediment), CI(Compliance Intention), SF(Security Feedback)
※ Values in bold type along the diagonal indicate the square root of the AVE , **: p < 0.01, *: p < 0.05

본 연구는 추가적으로 공통방법편의(common method bias) 분석을 실시한다. 연구는 다항목으로 구성된 요인에 대하여 개인의 설문 당시의 생각을 측정하는 것으로 데이터를 확보하였는데, 공통방법편의 문제가 있을 수 있다. 연구는 Podsakoff et al.[2003]이 제시한 단일 공통방법 기법(single common method factor)을 적용하여 분석하였다. 해당 기법은 공통 요인을 추가하지 않은 모형과 공통 요인을 추가한 모형을 비교하여, 항목간 차이가 적은지를 확인하는 기법으로, 공통 요인을 추가하지 않은 모델의 적합도(χ2/df = 1.662, GFI = 0.952, AGFI = 0.921, CFI = 0.989, NFI = 0.973, RMSEA = 0.048)와 추가한 모델의 적합도(χ2/df = 1.368, GFI = 0.969, AGFI = 0.934, CFI = 0.995, NFI = 0.983, RMSEA = 0.036)가 요구사항을 충족시켰으며, 항목간의 차이가 0.2 이하로 나타나, 공통방법편의 문제는 낮은 것으로 판단하여, 본 분석을 실시한다.

4-2 주효과 분석

연구 모델에 대한 검증은 조절효과를 제외한 주 모델에 대한 효과 분석을 우선적으로 실시한다. 구조모델을 통한 가설 검증은 모델의 적합도 분석, 연구 가설 경로 분석(β), 그리고 종속요인들의 결정계수 분석(R2)을 통해 증명한다.

우선, 연구 모델에서 제시한 구조모델의 적합도는 전체적으로 요구수준 보다 높은 것으로 나타났다(χ2/df = 1.706, GFI = 0.960, AGFI = 0.930, CFI = 0.991, NFI = 0.978, RMSEA = 0.05).

둘째, 연구 가설 분석을 위하여 가설 간 경로 분석(β)을 실시한다. 연구모델의 분석 결과는 다음 [그림 2], [표 4]와 같다.

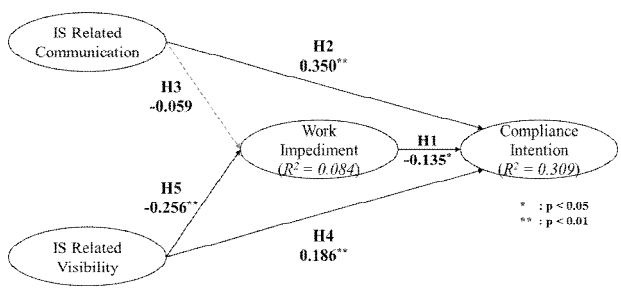

그림 2. 구조모델 결과 (주 효과)
Fig. 2. Results of the Structural Model (Main Effect)

표 4. 주효과 분석 요약
Table 4. Summary of Main Effect Tests

	Path	Coefficient	t-value	Result
H1	WI → CI	-0.135	-2.431*	Support
H2	SC → CI	0.390	6.188**	Support
H3	SC → WI	-0.059	-0.843	Reject
H4	SV → CI	0.186	2.883**	Support
H5	SV → WI	-0.256	-3.564**	Support

※ SC(Security Communication), SV(Security Visibility), WI(Work Impediment), CI(Compliance Intention), SF(Security Feedback)
**: $p < 0.01$, *: $p < 0.05$

연구가설 1은 정보보안 관련 업무 장애가 조직원의 정보보안 준수의도에 부정적 영향을 미친다는 것으로서, 분석 결과 두 요인은 부정적 영향 관계에 있는 것을 확인하였다(H1: β= -0.135, $p<0.05$). 이러한 결과는 정보보안으로 인하여 발생한 업무상 추가 절차 등 장애 요인이 개인의 준수 행동을 감소시킨다는 선행 연구[18]와 동일한 결과이다.

연구가설 2는 정보보안 관련 커뮤니케이션 활동이 정보보안 준수의도에 긍정적인 영향을 미친다는 것으로서, 분석 결과 두 요인은 긍정적 영향 관계에 있는 것을 확인하였다(H2: β= 0.390, $p<0.01$). 이러한 결과는 커뮤니케이션 활동이 조직 내 정보시스템 관련 지식을 형성함으로써 활동에 긍정적인 영향을 준다는 선행연구[25]와 유사한 결과이다.

연구가설 3은 정보보안 관련 커뮤니케이션 활동이 업무 장애를 완화시킨다는 것으로서, 분석 결과 영향을 미치지 않는 것으로 나타났다(H3: β= -0.059, $p>0.05$). 이러한 결과는 커뮤니케이션이 정보보안 부정적 행동 원인을 완화시킨다는 선행연구[26]와 다른 결과이다. 하지만, 요인간의 관계는 미비하지만 음의 영향 관계에 있는 것으로 나타나, 현재 국내 금융기업들의 보안 관련 커뮤니케이션 활동은 활발하지 않아 이러한 결과가 나타났다고 판단 된다.

연구가설 4는 정보보안 가시성이 정보보안 준수의도에 긍정적인 영향을 미친다는 것으로서, 분석 결과 두 요인은 긍정적 영향 관계에 있는 것을 확인하였다(H4: β= 0.186, $p<0.01$). 이러한 결과는 보안 캠페인과 같은 가시성 확보 활동이 개인의 정보보안 정책 준수를 높이는 조건이라는 선행연구[32]와 같은 결과이다.

연구가설 5는 정보보안 가시성이 업무장애를 완화시킨다는 것으로서, 분석결과 요인간에는 부정적 관계가 있는 것으로 나타났다(H5: β= -0.256, $p<0.01$). 이러한 결과는 보안 캠페인과 같은 가시성 확보 활동이 부정적 행동 원인을 감소시킨다는 선행연구[26]와 같은 결과이다.

마지막으로, 독립변수들이 종속 요인에 미치는 영향력인 결정계수(R2)를 확인한다. 준수의도는 커뮤니케이션, 가시성, 그리고 업무 장애로부터 30.9%의 결정력을 가지는 것으로 나타났으며, 업무 장애는 커뮤니케이션과 가시성으로부터 8.4%의 결정력을 가지는 것으로 나타났다.

4-3 조절효과 분석

조절효과 분석은 정보보안 관련 피드백 활동이 정보보안 정책 정보 제공 활동(커뮤니케이션, 가시성), 보안 관련 업무 장애, 그리고 준수의도간의 상호 관계를 완화하거나 강화하는 등 조절효과를 가지는 것을 확인한다.

각 요인이 7점 리커트 척도로 구성되어 있기 때문에, 조절효과 분석은 AMOS 22.0을 활용하여 독립변수와 조절변수간의 상호작용(interaction effect) 분석을 통해 실시한다. 상호작용 분석은 분석 방법이 다양하나, 엄격한 분석 방식에 속하는 Lin et al.[2010]의 직교과접근법(orthogonalizing approach)을 적용하며, 분석결과는 다음 [표 5]와 같다.

표 5. 조절효과 분석 요약
Table 5. Summary of Moderating Effect Tests

	Path	Coefficient	t-value	Result
H6	WI → CI	-0.185	-3.388**	Support
	SF → CI	0.452	7.489**	
	WI x SF → CI	0.171	3.507**	
H7	SC → WI	-0.138	-1.598	Reject
	SF → WI	-0.07	-0.785	
	SC x SF → WI	0.02	0.321	
H8	SV → WI	-0.264	-3.942**	Reject
	SF → WI	-0.053	-0.752	
	SV x SF → WI	-0.048	-0.366	

※ SC(Security Communication), SV(Security Visibility), WI(Work Impediment), CI(Compliance Intention), SF(Security Feedback)
**: $p < 0.01$, *: $p < 0.05$

연구 가설 6은 피드백이 업무장애와 준수의도간의 부정적 영향관계를 조절할 것이라는 것으로서, 상호작용 분석 결과 조절효과가 있는 것으로 나타났다. 보다 상세하게 조절효과의 형태를 파악하기 위하여 Dowson[2014]의 2-way 상호작용 효과를 그래프로 표현하였다[그림 3]. 분석 결과, 업무 장애가 준수의도에 미치는 부정적 영향 관계는 존재하나, 피드백 수준이 높을 경우 높은 업무장애 시 준수의도 감소를 완화시키는 것으로 나타났다.

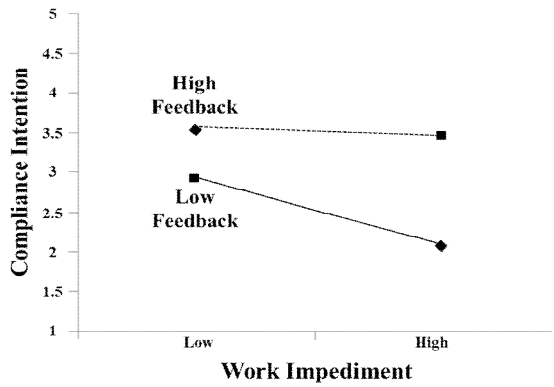

그림 3. 피드백의 조절효과 (H6)
Fig. 3. Moderation Effect of Feedback (H6)

연구 가설 7과 8은 피드백이 커뮤니케이션과 가시성이 업무 장애에 미치는 영향을 조절할 것이라는 것으로서, 상호작용 분석 결과 조절효과가 없는 것으로 나타났다.

Ⅴ. 결 론

5-1 연구의 요약

조직 내 정보 관리의 중요성이 지속적으로 부각되면서, 조직들은 정보보안 기술에 대한 투자를 통해 정보보안 수준을 높이고자 하고 있다. 그럼에도 불구하고, 정보 관리 체계가 엄격하게 도입되어 있는 금융권, 공공기관 등에서의 정보 노출 위협은 감소하지 않고 있다. 특히, 조직 구성원의 잠재적 보안 위협은 IT 시스템에 대한 접근이 다양한 채널을 통해 접근될 수 있게 됨에 따라 낮아지지 않고 있다. 하지만, 개인들의 정보보안 준수 수준 향상은 단순히 조직 차원의 시스템 도입과 같이 투자로서 결정되는 것이 아니라, 개인의 준수의지 향상을 통해 정보보안 준수행동을 자발적으로 실시하도록 지원하는 것이 필요하다.

본 연구는 정보보안 정책 도입으로 인하여 발생 되는 개인의 업무 장애가 준수의도에 부정적 영향을 주며, 업무 장애 수준을 완화하기 위해 조직 차원의 정보 제공 활동을 어떻게 해야하는지를 제시함으로써, 조직원의 보안 준수의도를 높이고자 하였다. 이에 정보보안을 엄격히 도입한 금융권에서 근무하는 조직원들을 대상으로 설문을 실시하였으며, 구조방정식 모델을 통해 연구 가설을 검증하였다. 결과는 업무장애가 준수의도를 떨어뜨리는 것을 확인하였으며, 가시성이 업무장애를 완화하는 것을 확인하였다. 또한, 정보보안 피드백이 업무장애와 준수의도간의 부정적 영향관계를 완화하는 조절효과를 가지는 것을 확인하였다.

5-2 연구의 시사점 및 향후 연구

본 연구는 조직-개인간의 관계에서 조직원의 정보보안 준수의도 향상을 위한 조건을 업무장애와 같은 부정적 측면과 조직 차원의 정보 제공 활동과 같은 긍정적 측면에서 살펴보았으며, 이론적, 실무적 시사점을 가진다.

첫째, 보다 엄격한 정보보안 정책 도입이 개인 본연의 업무상 불편함이 있을 수 있음을 제시하고 정보보안 준수의도간에 부정적 영향 관계가 있음을 확인하였다. 정보보안 정책 및 기술 도입은 개인의 업무의 절차, 방법 등을 변화시키는데, 보안이 엄격해질수록 업무 장애로 인식하게 된다. 보안 정책이 자신의 업무에 방해된다고 판단할 경우 보안 행동을 회피하려는 경향을 보이게 된다. 연구는 이론적 관점에서 보안 관련 스트레스 유형인 업무장애와 준수의도간의 부정적 관계에 있음을 증명함으로써, 정보보안의 부정적 영향에 대한 이론적 가치를 제시하였다. 또한, 실무적 관점에서 정보보안 정책의 엄격한 도입이 오히려 부정적 행동을 유발할 수 있기 때문에, 조직 구성원 관점에서 보안 정책 및 기술 도입이 고려되어야 하는 것을 제시하였다.

둘째, 정보보안 업무 장애를 완화하기 위한 조건으로 조직 차원의 보안 관련 정보 제공 활동의 중요성을 제시하였다. 즉, 본 연구는 정보보안 커뮤니케이션 활동과 가시성 활동이 업무 장애를 감소시킨다고 보고, 영향 관계를 증명하고자 하였다. 이론적 관점에서, 결과는 가시적 활동의 업무장애에 대한 완화 효과를 증명하였다. 즉, 엄격한 보안 정책 및 기술에 의해서 개인에게 발생한 업무상 불편함인 장애 요인에 대한 인식은 관련 보안 활동에 필요성, 조직의 보안 목표, 보안 행동 관련 지식정보를 명확하게 제시할 때 개선될 수 있음을 의미한다. 이러한 결과는 정보보안 관련 기술스트레스를 완화하는 선행 요인으로서 가치를 가진다. 더불어 실무적 관점에서 결과는 조직 차원의 보안 관련 정보 제공활동이 준수의도 향상 및 개인의 업무 장애 감소를 위한 선행 조건임을 제시하였다. 즉, 이메일, SNS 등 정보보안 정보 제공을 위한 조직 차원의 커뮤니케이션 활동은 보안 준수 행동에 긍정적 영향을 주며, 정보보안 관련 다양한 캠페인 활동은 개인의 실질적 보안 지식을 형성시킴으로써 업무에 자연스럽게 적용할 수 있도록 돕는다. 따라서, 개인의 보안 준수 수준 향상을 위한 조직차원의 접근 전략을 제시하였다는 측면에서 시사점을 가진다.

셋째, 정보보안 피드백 활동이 업무 장애와 준수의도 간의 부정적 영향 관계를 완화하는 것을 확인하였다. 이론적 관점에서, 결과는 개인에게 형성된 보안 관련 장애 인식은 준수의도를 감소시키지만, 개인 행동에 대한 피드백 활동이 제공될 경우, 업무장애가 준수의도에 미치는 부정적 영향을 감소시키는 것을 확인하였다. 즉, 보안 관련 스트레스와 준수 행동간의 관계를 개선하는 요인을 제시한 선행연구로서의 시사점을 가진다. 더불어, 실무적 관점에서 결과는 조직차원의 보안관련 피드백 활동이 업무장애의 부정적 영향을 직접적으로 조절하는 것을 확인하였기 때문에, 인지된 업무 장애 수준 감소를 위한 조직 차원의 접근 활동 방안을 제시하였다는 측면에서 시사점을 가진다.

본 연구는 정보보안으로 인해 발생하는 업무장애와 완화요인을 제시하였다는 측면에서 시사점을 가지지만, 부분적으로 한계를 가지며 향후 연구에서 보완될 필요성이 있다. 첫째, 본 연구는 금융업 근로자들을 대상으로 조직의 보안 활동 및 개인의 보안 준수 수준을 당시의 인식 수준으로 측정하였다. 개인 관점에서 판단하는 조직 차원의 보안 정보 제공 활동과 개인의 보안 수준에 대한 인지 측면을 확인하였다는 측면에서 시사점을 가진다. 향후, 조직의 정보보안 정보 제공 활동(커뮤니케이션, 가시성, 피드백)이 보다 명확한 수준에서 이루어지고 있음을 제시하기 위한 실험적 연구가 제시된다면, 실무적 시사점을 보다 높일 수 있을 것으로 판단된다. 둘째, 설문 대상은 금융업 일반 직무를 가진 조직원들을 대상으로 하였다. 하지만, 직무별

보안에 대한 의식 수준은 차이가 발생할 것으로 판단하는데, 특히 스마트 워크 시스템 도입은 보안 정책 준수 행동을 보다 어렵게 만드는 요건이 될 수 있다. 따라서, 직무별 조직 특성별 조사를 실시한다면 보다 면밀한 시사점을 가질 것으로 판단된다. 마지막으로, 개인의 업무 장애에 대한 인식은 개인, 조직, 국가 등 성향에 따라 차이가 발생할 가능성이 높다. 예를 들어, 정보보안 정책의 부정적인 인식과 개선에 대한 논의는 집단주의, 개인주의 등에 따라 차별화되어야 할 것으로 판단되며, 향후 연구에서 결과가 반영된다면 보다 높은 실무적 시사점을 가질 것으로 판단한다.

참고문헌

[1] Grandviewresearch. Cyber Security Market Size, Share & Trends Analysis Report by Component, by Security Type, by Solution, by Service, by Deployment, by Organization, by Application, and Segment Forecasts, 2019 – 2025, 2019. Available: https://www.globenewswire.com.

[2] Verizon. 2020 Data Breach Investigations Report, 2020.

[3] S. Ha and H. Kim, “The Effects of User’s Security Awareness on Password Security Behavior,” Journal of Digital Contents Society, Vol. 14, No. 2, pp. 179-189, 2013. DOI : 10.9728/dcs.2013.14.2.179.

[4] J. D'Arcy, A. Hovav, and D. Galletta, “User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach,” Information Systems Research, Vol. 20, No. 1, pp. 79-98, 2009. DOI : 10.1287/isre.1070.0160.

[5] M. I. Merhi and P. Ahluwalia, “Examining the Impact of Deterrence Factors and Norms on Resistance to Information Systems Security,” Computers in Human Behavior, Vol. 92, pp. 37-46, 2019. DOI : 10.1016/j.chb.2018.10.031

[6] C. Posey, T. L. Roberts, and P. B. Lowry, “The Impact of Organizational Commitment on Insiders’ Motivation to Protect Organizational Information Assets,” Journal of Management Information Systems, Vol. 32, No. 4, pp. 179-214, 2015. DOI : 10.1080/07421222.2015.1138374.

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

[8] S. Aurigemma and T. Mattson, “Deterrence and Punishment Experience Impacts on ISP Compliance Attitudes,” Information and Computer Security, Vol. 25, No. 4, pp. 421-436, 2017. DOI : 10.1108/ICS-11-2016-0089.

[9] T. S. Ragu-Nathan, M. Tarafdar, B. S. Ragu-Nathan, and Q. Tu, “The Consequences of Technostress for End Users in Organizations: Conceptual Development and Empirical Validation,” Information Systems Research, Vol. 19, No. 4, pp. 417-433, 2008. DOI : 10.1287/isre.1070.0165.

[10] M. Tarafdar, Q. Tu, T. S. Ragu-Nathan, and B. S. Ragu-Nathan, “Crossing to the Dark Side: Examining Creators, Outcomes, and Inhibitors of Technostress,” Communications of the ACM, Vol. 54, No. 9, pp. 113-120, 2011. DOI : 10.1145/1995376.1995403.

[11] J. D'Arcy, T. Herath, and M. K. Shoss, “Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective,” Journal of Management Information Systems, Vol. 31, NO. 2, pp. 285-318, 2014. DOI : 10.2753/MIS0742-1222310210.

[12] I. Hwang and O. Cha, “Examining Technostress Creators and Role Stress as Potential Threats to Employees' Information Security Compliance,” Computers in Human Behavior, Vol. 81, pp. 282-293, 2018. DOI : 10.1016/j.chb.2017.12.022.

[13] BBC. Capital One Data Breach: Arrest after Details of 106m People Stolen, 2019. Available: https://www.bbc.com

[14] KBresearch. KB Knowledge Vitamin: Recent Information Security Trend of Financial Institution and Outlook, 2015.

[15] R. West, “The Psychology of Security,” Communications of the ACM, Vol. 51, No. 4, pp. 34-40, 2008. DOI : 10.1145/1330311.1330320.

[16] A. Vance, M. Siponen, and S. Pahnila, “Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory,” Information & Management, Vol. 49, No. 3-4, pp. 190-198, 2012. DOI : 10.1016/j.im.2012.04.002.

[17] H. J. Lee, H. S. Kho, E. H. Roh, and K. S. Han, “A Study on the Factors of Experience and Habit on Information Security Behavior of New Services-based on PMT and UTAUT2,” Journal of Digital Contents Society, Vol. 19, No. 1, pp. 93-102, 2018. DOI : 10.9728/dcs.2018.19.1.93.

[18] I. Hwang, D. Kim, T. Kim, and S. Kim, “Why not Comply with Information Security? An Empirical Approach for the Causes of Non-compliance,” Online Information Review, Vol. 41, No. 1, pp. 1-17, 2017. DOI : 10.1108/OIR-11-2015-0358.

[19] R. K. Jena, “Technostress in ICT Enabled Collaborative Learning Environment: An Empirical Study among Indian Academician,” Computers in Human Behavior, Vol. 51, pp. 1116-1123, 2015. DOI : 10.1016/j.chb.2015.03.020.

[20] H. Shin and S. Shin, “Comparison of Internal Communications for Korean Company and Multinational Company Based on the Diagnosis Model of Internal Communication,” Journal of Public Relations, Vol. 7, No. 1, pp. 196-230, 2003.

[21] A. Frank and J. Brownell, Organizational Communication and Behavior: Communication to Improve Performance,

Orlando, FL: Holt, Rinehart, & Winston, 1989.

[22] M. Welch and P. R. Jackson, "Rethinking Internal Communication: A Stakeholder Approach," Corporate Communications: An International Journal, Vol. 12, No. 2, pp. 177-198, 2007.

[23] J. E. Grunig and D. M. Dozier, Excellent Public Relations and Effective Organizations: A Study of Communication Management in Three Countries, Routledge, 2003.

[24] J. E. Grunig and T. T. Hunt, Managing Public Relations, Holt, Rinehart and Winston, 1984.

[25] D. Jiménez-Castillo and M. Sánchez-Pérez, "Nurturing Employee Market Knowledge Absorptive Capacity through Unified Internal Communication and Integrated Information Technology," Information & Management, Vol. 50, No. 2-3, pp. 76-86, 2013. DOI : 10.1016/j.im.2013.01.001.

[26] H. Hwang and D. Kim, "The Effect of Organizational Information Security Environment on the Compliance Intention of Employee," The Journal of Information Systems, Vol. 25, No. 2, pp. 51-77, 2016. DOI : 10.5859/KAIS.2016.25.2.51.

[27] T. Vander Elst, E. Baillien, N. De Cuyper, and H. De Witte, "The Role of Organizational Communication and Participation in Reducing Job Insecurity and its Negative Association with Work-related Well-being," Economic and Industrial Democracy, Vol. 31, No. 2, pp. 249-264, 2010. DOI : 10.1177/0143831X09358372.

[28] P. Bordia, E. Hobman, E. Jones, C. Gallois, and V. J. Callan, "Uncertainty during Organizational Change: Types, Consequences, and Management Strategies," Journal of Business and Psychology, Vol. 18, No. 4, pp. 507-532, 2004. DOI : 10.1023/B:JOBU.0000028449.99127.f7.

[29] V. Venkatesh, M. Morris, G. Davis, and F. Davis, "User Acceptance of Information Technology: Toward a Unified View," MIS Quarterly. Vol. 27, No. 3. pp. 425–478, 2003. DOI : 10.2307/30036540.

[30] I. Hwang, R. Wakefield, S. Kim, and T. Kim, "Security Awareness: The First Step in Information Security Compliance Behavior," Journal of Computer Information Systems, pp. 1-12, 2019. DOI: 10.1080/08874417.2019.1650676.

[31] A. AlHogail, "Design and Validation of Information Security Culture Framework," Computers in Human Behavior, Vol. 49, pp. 567-575, 2015. DOI : 10.1016/j.chb.2015.03.054.

[32] M. Siponen, S. Pahnila, and M. A. Mahmood, "Compliance with Information Security Policies: An Empirical Investigation," Computer, Vol. 43, No. 2, pp. 64-71, 2010. DOI: 10.1109/MC.2010.35.

[33] B. E. Wright. (2004). The role of work context in work motivation: A public sector application of goal and social cognitive theories. Journal of Public Administration Research and Theory, 14(1), 59-78. DOI : 10.1093/jopart/muh004.

[34] M. C. Andrews and K. M. Kacmar, "Confirmation and Extension of the Sources of Feedback Scale in Service-based Organizations," The Journal of Business Communication, Vol. 38, No. 2, pp. 206-226, 2001. DOI : 10.1177/002194360103800204.

[35] M. A. Campion and R. G. Lord, "A Control Systems Conceptualization of the Goal-Setting and Changing Process," Organizational Behavior and Human Performance, Vol. 30, No. 2, pp. 265-287, 1982. DOI : 0.1016/0030-5073(82)90221-5.

[36] K. J. Knapp, R. F. Morris Jr, T. E. Marshall, and T. A. Byrd, "Information Security Policy: An Organizational-Level Process Model," Computers & Security, Vol. 28, No. 7, pp. 493-508, 2009. DOI : 10.1016/j.cose.2009.07.001.

[37] A. H. Hon, W. W. Chan, and L. Lu, "Overcoming Work-Related Stress and Promoting Employee Creativity in Hotel Industry: The Role of Task Feedback from Supervisor," International Journal of Hospitality Management, Vol. 33, pp. 416-424 2013. DOI : 10.1016/j.ijhm.2012.11.001.

[38] Y. Chen, K. Ramamurthy, and K. W. Wen, "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?," Journal of Management Information Systems, Vol. 29, No. 3, pp. 157-188, 2012. DOI : 10.2753/MIS0742-1222290305.

[39] J. C. Nunnally, Psychometric Theory (2nd ed.). New York: McGraw-Hill, 1978.

[40] B. H. Wixom and H. J. Watson, "An Empirical Investigation of the Factors Affecting Data Warehousing Success," MIS Quarterly, Vol. 25, No.1, pp. 17-41, 2001. DOI : 10.2307/3250957.

[41] C. Fornell and D. F. Larcker, "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," Journal of Marketing Research, Vol. 18, No.1, pp. 39-50, 1981. DOI: 10.2307/3151312.

[42] P. M. Podsakoff, S. B. MacKenzie, J. Y. Lee, and N. P. Podsakoff, "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," Journal of Applied Psychology, Vol. 88, No.5, pp. 879-903, 2003. DOI : 10.1037/0021-9010.88.5.879.

[43] G. C. Lin, Z. Wen, H. W. Marsh, and H. S. Lin, "Structural Equation Models of Latent Interactions: Clarification of Orthogonalizing and Double-mean-centering Strategies," Structural Equation Modeling, Vol. 17, No. 3, pp. 374-391, 2010. DOI : 10.1080/10705511.2010.488999.

[44] J. F. Dawson, "Moderation in Management Research: What, Why, When and Howm," Journal of Business and Psychology, Vol. 29, pp. 1-19, 2014. DOI : 10.1007/s10869-013-9308-7.

황인호(Inho Hwang)

2007년 : 중앙대학교 대학원 (경영학석사)
2014년 : 중앙대학교 대학원 (경영학박사)

2014년～2018년 : (사)한국창업경영연구원
2018년～2020년 : 한국산업기술대학교
2020년～현　재 : 국민대학교 교양대학 조교수
※관심분야 : IT 핵심성공요인(IT CSF), 디지털 콘텐츠(Digital Content), 정보보안(Information Security), 프라이버시(Privacy) 등