韓國IT서비스學會誌
第14卷 第4號
2015年 12月, pp.81-104

Journal of Information Technology Services
http://dx.doi.org/10.9716/KITS.2015.14.4.081

정보보안대책과 정보시스템 오남용과의 인과적 관계*

이준택** · 김상훈***

The Causal Relationship between Information Security Countermeasures and Information System Misuse*

Joontaik Lee** · Sanghoon Kim***

■ Abstract ■

Intentional information systems (IS) misuse is a serious problem in many organizations. This study aims at developing the theoretical framework of deterring IS misuse on the basis of Nagin's General Deterrence Theory (GDT) which is very famous in the area of socio-criminology. Applying GDT to the IS misuse situation could be reasoned that the perceived certainty and the perceived severity of sanctions associated with committing IS misuse have positive impact on deterring the deviant behaviors. Also, these two constructs (certainty of sanctions and severity of sanctions) could be inferred to be influenced by the four types of IS security countermeasures (security policies, security awareness program, monitoring practices and preventive security software) derived through critically reviewing IS security-relevant literature. The proposed research model and ten hypotheses were empirically analysed using structural equation modelling with the data collected by conducting a questionnaire survey of staff members in business organizations in Korea. As a result, it was found that five ones of ten hypotheses were supported. It is thought that this study makes theoretical contribution to expanding research area of IS security and also has strong implications for IS security management practices within organizations.

Keyword : General Deterrence Theory, IS Misuse, IS Security Countermeasures

Submitted : October 26, 2015 1st Revision : December 6, 2015 Accepted : December 11, 2015

* 이 논문은 2015년도 광운대학교 교내 학술연구비 지원에 의해 연구되었음.

** (주)토브스 대표이사

*** 광운대학교 경영학부 교수, 교신저자

1. 서 론

정보시스템 도입 및 활용은 조직 경영활동에 도움이 되는 순기능적 측면이 매우 크지만 정보시스템의 오남용(Misuse)으로 인해 조직 운영 및 발전에 역기능적인 심각한 문제를 야기하기도 한다. 특히 조직의 정보시스템에 대한 의존도가 증가할수록 정보시스템 오남용의 영향도 커지는 바(Kankanhalli et al., 2003; Chang and Jung, 2013), 정보기술 및 정보시스템의 의존도가 높은 조직일수록 정보의 기밀성, 무결성, 가용성의 유지가 중요하다. 더구나 정보시스템 오남용과 이로 인한 손실규모는 향후 조직구성원들의 컴퓨터 활용능력 향상과 인터넷 환경하에서의 가상작업(Virtual Work) 비중 증가와 함께 기능적으로 보다 고도화된 소프트웨어 도구의 가용성 증대 추세에 따라 지속적으로 커질 가능성이 높다. 이에 따라 대부분의 조직에 있어서 정보시스템 오남용에 대한 대책수립은 매우 중요한 경영관리 과제로 대두되고 있고, 이러한 현실적 과제해결에 도움을 줄 수 있는 이론적 측면에서의 연구가 절실히 요망되고 있다.

정보시스템 오남용(Misuse)을 최소화 하거나 방지하기 위한 정보시스템 보안에 대한 연구는 세가지 측면 즉, 기술적Technical)측면, 경제적/재정적(Economic/Financial)측면 및 행태적(Behavioral) 측면의 접근방법으로 진행되어 왔다. 우선 기술적 측면의 연구는 보안을 위한 적절한 하드웨어 및 소프트웨어 구성요소(Components)의 선정과 제반 정보자원 보호를 지향한 정보아키텍쳐 설계에 초점을 두고 있으며(Dutta and Roy, 2003), 경제적/재정적 측면에서의 연구는 조직의 정보보안기능 수행을 위한 비용/효과분석에 초점을 두고 보안위반 손실 추정, 위험관리 적정투자 규모 산정, 비용대비 효과적인 기술 구성, 다양한 기술들의 가치전개(Value Deployment) 접근방안 등의 주제를 다루고 있다(Cavusoglu and Raghunathan, 2004; Gordon et al., 2004). 그리고 행태적 측면에서의 연구는 정보시스템 보안행위를 정보시스템의 기밀성과 가용성, 무결성에 영향을 주는 복합적인 인간행위로 정의하고(Stanton et al., 2003), 이러한 행위에 긍정적인 영향을 주는 요인들을 밝히고자 했다. 즉, 행태론적인 정보시스템 보안 연구에서는 기술적인 보안조치들 만으로는 정보시스템 보안에 충분하지 않으며 정보시스템 보안에 대한 정보시스템 사용자들의 바람직한 심리적(psychological) 및 사회적(sociological) 행태를 유도하는 방안을 강구하여야 함을 강조하고 있다.

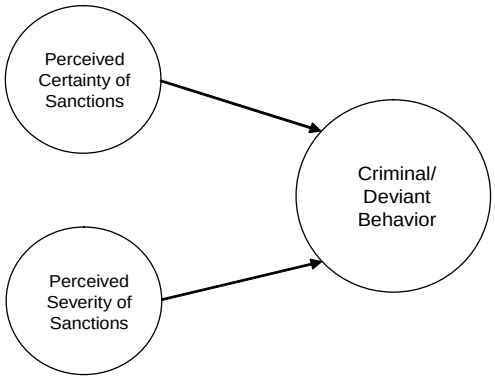
본 연구는 정보시스템 보안에 대한 이상의 세 가지 측면의 연구접근방법 유형들 중 행태적 측면의 접근방법에 의해 정보시스템 오남용(Misuse)에 대한 영향요인들을 이론적으로 도출하고, 실증적인 규명을 함으로써 향후 정보시스템 오남용 대책 수립을 위한 이론적 근거 및 실무적 지침을 제공하고자 한다.

2. 이론적 고찰

2.1 일반억제이론(GDT : General Deterrent Theory)

정보시스템 오남용(Misuse)은 일종의 범죄 또는 비정상적인 행위로서 이같은 행위 억제에 관한 연구는 사회범죄학에서부터 시작되었으며 사회범죄학 영역에서의 대표적인 이론은 Nagin의 일반억제이론(GDT : General Deterrent Theory)으로 알려져 있다. Nagin의 일반억제이론(GDT)은 불법적인 행동을 제재하거나 포기시키는 것 즉, 의욕을 꺾거나 불법행동을 제재하는 것과 이러한 제재의 효과성에 초점이 맞춰져 있다(Nagin, 1978; Tittle, 1980). Nagin의 일반억제이론(GDT)에 따르면 <Figure 1>에 도식화된 바와 같이 범죄 및 일탈행위는 이에 대한 '제재의 확실성 인지도(Perceived Certainty of Sanctions)' 및 '제재의 엄격성 인지도(Perceived Severity of Sanctions)'의 수준에 따라 영향을 받는 것으로 알려져 있다. 여기서 '제재의 확실

성'은 처벌 받을 가능성을 의미하며, '제재의 엄격성'은 처벌의 강도를 의미한다(Nagin, 1978). 즉, 일반억제이론은 불법적 행위에 대한 제재 또는 제재활동의 확실성과 엄격성이 강하다고 인지될수록 잠재적 범법자들의 불법적 행위 자행 가능성이 억제됨을 주장하고 있다. 일반억제이론(GDT)은 자신에 대한 보상을 최대화하고 비용부담을 최소화하고자하는 합리적 행위자들의 경제적 관점에도 부합하는 바, 자신이 도모한 활동으로 인한 보상보다 처벌의 가능성과 엄격성이 더 크게 느껴질 경우는 그러한 활동을 하지 않을 것임을 논리적으로 설명하고 있기 때문이다(Tittle, 1980; Weaver and Carroll, 1985).



〈Figure 1〉 General Deterrence Theory(Nagin, 1978)

일반억제이론(GDT)은 여러 다양한 인간유형, 업무환경이나 시대적 상황에 상관없이 실증적인 지지를 받는 연구 결과가 나타남으로써 사회범죄학에서는 높게 평가되고 있으며, 범죄와 비정상적 행위를 예측하는 능력에 있어서 '재재의 확실성 인지도(Perceived Certainty of Sanctions)'과 '제재의 엄격성 인지도(Perceived Severity of Sanctions)'의 두 개념(Constructs)은 불법적이거나 일탈적 행위를 예측함에 있어서의 설명력이 매우 높은 것으로 사회범죄학 전문가들 사이에 컨센서스가 형성되어 있다(Cook,1980; Nagin and Pogarsky, 2001; Tittle, 1980). 특히, 일반억제이론(GDT)은 규정과 규율이 비교적 잘 지켜지는 사무직 직원들의 정보시스템 오남용에도 적용될 수 있으며(Straub, 1990; Chang and Jung, 2013), Straub(1990)은 일반억제이론(GDT)을 정보시스템 사용환경에 성공적으로 적용함으로써 오남용 억제수단 및 정보보안 대책들이 정보시스템 오남용 수준을 낮추게 됨을 실증적으로 밝혔다.

이상과 같은 기존의 연구결과들에 근거할 때 일반억제이론(GDT)은 정보시스템 오남용 가능성을 점검하고 대처함에 있어서 적합한 이론적 기반을 제공할 수 있다고 추론되는 바, 본 연구에서도 정보보안대책의 정보시스템 오남용에 대한 영향을 규명함에 있어서 일반억제이론(GDT)을 근거 이론으로 채택하고자 한다.

2.2 정보시스템 오남용

2.2.1 정보시스템 오남용의 정의와 범위

정보시스템 오남용에 관하여는 기존의 연구들에서 다양한 용어들로 표현되어 왔다. Solarz(1987)는 컴퓨터 범죄를 '정보시스템과 연관되어 있으면서 형사법에 저촉되는 모든 범죄'로 정의하고 있으며, Saari(1987)는 '컴퓨터 기술 지식을 가지고 있어야 행할 수 있는 불법행위'를 컴퓨터 범죄로 정의하였다. 이러한 정의는 컴퓨터범죄를 컴퓨터 사용과 관련된 범죄행위로 국한하고 있는데 실제 현행법을 위반하지는 않지만 정보시스템 이용에 있어서 적절하지 못한 행위로 인해 조직이 피해를 보는 경우도 많기 때문에 정보시스템 오남용은 범법행위 뿐만 아니라 정보시스템 사용상의 고의적으로 자행되는 부적절한 행위까지를 모두 포함하는 개념으로 보는 것이 현실적 문제 해결에 보다 바람직할 것으로 본다.

이러한 맥락에서 Parker(1998)는 정보시스템 오남용을 '정보시스템 사용과 관련하여 범법하거나, 범법은 하지 않더라도 정보시스템을 자신의 편익추구를 위해 사용함으로써 다른 사람이 고통이나 손실을 초래하는 고의적 행위'로 정의하고 있으며, St-

raub(1990)은 정보시스템 오남용에 대한 보다 구체적이고 확장된 정의를 하였다. 즉, '조직 내 구성원 또는 합법적인 접속권한이 있는 외부인들에 의해 조직 내 정보시스템에 대해 자행되는 인가되지 않은 고의적 행위로서 다음 사항을 포함하는 일체의 행위'라고 정보시스템 오남용을 정의하였다.

(1) 하드웨어 : 컴퓨터와 관련된 물리적인 자산들(예를 들어, 터미널, CPU, 디스크 드라이브, 프린터)을 훔치거나 손상을 입히는 것
(2) 프로그램 : 프로그램의 수정이나 절도
(3) 데이터 : 데이터의 수정이나 도용
(4) 서비스 : 인가되지 않은 서비스의 사용, 서비스의 중단

이러한 Straub(1990)의 정보시스템 오남용에 대한 정의는 정보기술(IT)의 전 분야에서 발생하는 불법적이거나 부적절하거나 비윤리적인 행위를 모두 포함하고 있고, 정보시스템 사용자의 범위도 전 일제 및 파트타임 근무자를 불문한 내부 임직원 모두를 포함하고 있을 뿐만 아니라 계약자들이나 사업 파트너와 같은 조직 내 정보시스템과 네트워크에 적법으로 접속할 수 있는 외부인까지를 포함하고 있기 때문에 정보시스템 오남용 현황을 보다 정확하게 포착하고 실효성 있는 대처방안을 마련하는 합리적 준거가 될 수 있다고 보며, 이에 본 연구에서는 정보시스템 오남용에 대한 정의로서 Straub (1990)의 정의를 따르기로 한다.

2.2.2 정보시스템 오남용 의도와 행위

정보시스템 오남용 의도(Intention)는 정보시스템 사용자가 정보시스템 오남용을 행하거나 행하지 않고자 하는 의도를 의미한다. 합리적 행동이론(TRA : Theory of Reasoned Action)에 의하면 의도는 행위에 영향을 주는 동기요인들(motivational factors)을 포함하며, 의도는 행위를 하고자 얼마나 열심히 시도하고자 하는가와 행위를 수행하는데 얼마나 많은 노력을 쏟을 계획을 하고 있는가를 나타내 주는 지표로서(Ajzen, 1988), 실제 미래 행위의 강력한 예측요인이 되는 것으로 여러 연구들에서 입증되어 왔다(Ajzen, 1991). 또한 정보시스템 오남용 억제에 관한 많은 연구들에서 종속변수로서 정보시스템 오남용 의도를 채택하고 있다(Lee et al., 2004; Peace et al., 2003; Bachman et al., 1992). 이는 정보시스템 오남용 행위에 대한 객관적이고 정확한 조사가 어렵기 때문으로 추론되는 바, 정보시스템 오남용에 관한 실증분석을 하고자 하는 본 연구에서도 의도가 행위의 강력한 선행지표임을 보여준 기존 연구결과에 의거하여 정보시스템 오남용의도를 종속변수로 포함하고자 한다.

2.3 정보보안 대책

정보보안 대책들은 정보시스템 오남용을 억제하기 위한 통제대책과 예방하기 위한 통제대책으로 구성된다(Straub, 1990). 정보시스템 오남용 억제대책(Deterrents)은 잠재적인 오남용 조직원들에게 오남용의 적발 가능성 및 이에 상응하는 처벌이란 위협을 통해 오남용을 억제하고자 하는 대책으로서 소극적 억제대책과 적극적 억제대책으로 구분될 수 있다. 전자는 정보시스템의 올바른 사용에 관한 정보와 올바르지 않은 사용시의 처벌 내용에 관한 정보를 제공함으로써 정보시스템의 오남용을 억제하고자 하는 대책으로서 보안정책 성명서(Security Policy Statement) 공지, 보안인식 프로그램(Security Awareness Program) 운영 등이 주된 대책이며, 후자의 대표적인 대책으로는 정보시스템 사용 증적 감사 등 사용현황 모니터링 실시(Monitering Practices)를 들 수 있다(Yu et al., 2008, Kankanhalli et at., 2003; Straub, 1990).

또한 정보시스템 오남용에 대한 예방대책(Preventives)은 비권한자에 대해 정보시스템 접속을 막는 것과 정보시스템의 특정기능을 제거함에 의해 정보시스템 오남용과 컴퓨터 범죄의 시도를 원천적으로 방지하는 것을 목표로 설계된 대책이며, 보안소프트웨어 설치가 대표적 대책으로서 비밀번호나 생체학적(지문, 홍채 등) 통제와 같은 접근통

제방법을 주로 사용한다(Ha and Kim, 2013; Ives et al., 2004; Straub, 1990).

이상과 기존의 연구들에서 제시된 정보시스템 오남용 억제대책(Deterrents)과 예방대책(Preventives)을 통합하여 본 연구에서는 보안정책 성명서 공지, 보안인식 프로그램 운영, 정보시스템 사용 현황 모니터링 실시, 보안 소프트웨어 설치 등 네 가지 대책을 정보시스템 오남용을 방지하거나 최소화하기 위한 대표적인 정보보안 대책들로 선정하였으며 각 보안대책별 구체적인 내용은 아래와 같다.

2.3.1 보안정책

보안정책은 통상적으로 정보보안에 대한 조직의 목표, 신념, 윤리, 통제방법 그리고 임직원들의 책임범위 등을 포함한다(Lee et al., 2004). 정보시스템 사용의 지침과 절차들은 보안정책으로부터 도출되며, 이들은 보안정책보다 구체적이고 명확한 보안행동 규정(Prescriptions)을 제공한다(Stanton et al., 2003). 중규모 이상의 대부분의 조직들은 정보시스템을 보호하기 위한 조직 나름의 보안정책을 가지고 있지만 모든 조직이 보안정책과 이에 기반한 보안절차 두 가지를 모두 가지고 있지는 않은 경우가 많으며(Lee and Lee, 2002), 조직의 규모가 작을수록 임직원들은 보안정책에 기반은 두되 조직구성원들 사이에 비공식적인 컨센서스를 통해 형성된 명문화되지 않은 보안절차를 따르는 경우가 많다(Stanton et al., 2003).

보안정책은 보호되어야 할 정보의 가치와 민감성과 정보의 손상, 수정 및 유출로 인해 조직에 미칠 수 있는 예상되는 영향정도에 따라 조직마다 크게 상이할 수 있다(Whitman et al., 2001). 그러나 일반적으로 보안정책은 정보시스템들의 안전하고 책임감이 있는 사용을 위해 사용자들과 관리자들에게 상세한 지침을 제공하여야 하며, 전형적인 보안정책은 (1) 정책의 범위 및 적용방향, 사용가능 보안기술, 정보시스템관리 및 운영 담당조직의 책임과 역할 등에 관한 개요 (2) 정보시스템에 대한 접근 및 사용에 대한 인가 및 통제 방법에 관한 개요 (3) 정보시스템 사용시 불법적이고 오남용 가능성이 있는 세부 사항 (4) 정보시스템 운영 및 관리시 보안정책 및 보안절차의 적용방안 (5) 보안정책 침해시 위반사항 및 처벌의 보고 절차 (6) 보안 정책의 정기적 검토 및 수정일정과 (7) 보안에 대한법적 책임 또는 면책사항 등 7가지 사항을 포함하여야 한다(Whitman et al., 2001).

2.3.2 보안인식 프로그램

조직의 정보시스템 보안에 관한 정책 및 절차는 조직원들이 그 내용을 이해하고 수용할 때 더욱 효과적일 수 있다. 그동안 여러 연구자들이 효과적인 정보시스템 오남용 통제를 위해 조직원들의 보안인식 강화를 위한 교육훈련 프로그램과 훈련의 필요성을 주장해 왔다(Furnell et al., 2002; Siponen, 2000). 보안인식 교육훈련 프로그램은 조직의 보안정책에 기반한 조직원들의 정보자원관리에 대한 책임과 의무 및 정보자원 오남용의 결과에 대한 인식수준을 제고하고 조직원들이 보안책임을 이행하는데 요구되는 기술을 알려주는데 초점을 둔다(Wybo and Straub, 1989).

보안인식 교육훈련 프로그램은 조직원들이 알아야 할 보안 정책, 시스템 인증, 정보시스템 사용허용 조건, 보안위반에 대한 처벌, 비밀번호 관리, 워크스테이션 보안, 랩탑 보안, 아이디 도용 및 바이러스 등 오남용으로부터 정보시스템 자산들을 보호하는 모든 주제를 포함하여야 하며(Schou and Trimmer, 2004; Jensen, 2003; Wybo and Straub, 1989), 효과적인 보안인식 프로그램이 되기 위하여는 임직원 오리엔테이션 프로그램 중에 실시되는 일회성의 교육훈련뿐만이 아니라 주기적인 비밀번호 변경 환기신호(reminder), 최신 바이러스 위협에 대한 이메일 및 뉴스레터 송부, 보안/감사 기준 준수 확인, 컴퓨터 화면 보호기(screen saver) 등과 같은 기법들을 동원한 지속적이고 일상적인 보안 업무프로세스가 병행되어야 한다(Hansche, 2001; Siponen, 2000).

2.3.3 보안 모니터링 실시

조직원들의 컴퓨터 이용과 관련된 활동들을 감시하고 추적하는 보안모니터링은 정보시스템 오남용 억제를 위한 적극적인 보안대책이다. 조직이 정한 보안규칙과 규정에 입각한 정보시스템의 활용이 이루어지도록 통제하기 위해 임직원들의 컴퓨터자원 사용행위의 감시(예를 들면, 비인가된 소프트웨어의 설치를 확인하기 위한 임직원 컴퓨터들에 대한 물리적인 증적 감사와 컴퓨터 사용 행위 기록 추적 등)와 임직원들의 이메일 사용이나 인터넷을 비롯한 통신망에 의한 컴퓨팅 작업 등의 감시를 포함하며 모니터링 수행을 위하여 주로 소프트웨어 도구를 사용하나 경우에 따라서는 비디오 카메라나 신분증 판독기(Badge Readers)와 같은 물리적 장치를 이용한다(Panko and Beh, 2002; Urbaczewski and Jessup, 2002).

2.3.4 보안 소프트웨어

정보시스템 오남용에 대처키 위하여는 보안정책, 보안인식 프로그램, 보안 모니터링과 같은 억제대책(Deterrents) 뿐만아니라 예방대책(Preventives)으로서의 보안기술도 실행되어야 함을 여러 연구자들이 주장하고 있다(Dhillon, 1999; Straub and Welke, 1998). 예방적 보안기술로는 부적절한 내용을 담은 이메일 메시지들을 차단하는 소프트웨어와 같은 특정용도의 소프트웨어를 비롯하여 정보시스템 사용권한 부여대상자를 인증함에 의해 적법한 사용자들의 접속은 허용하면서 침입자 및 신분위장자의 불법 접속은 통제함으로써 인가되지 않은 시스템 접속이나 파괴, 오남용 등으로부터 정보시스템들을 보호하는 소프트웨어를 포함한다. 이러한 보안 소프트웨어의 가장 일반적인 유형은 정보시스템 사용자를 인증하기 위해 사용자 아이디(ID) 또는 비밀번호(Password)를 이용하는 접속통제 소프트웨어이며, 보다 고도화된 인증방법으로는 토큰기반(token-based) 접근방법(예를 들어, 스마트카드와 같은)과 생체인식 솔루션(biometric solutiuons)을 들 수 있는데 생체인식 솔루션은 안면인식과 지문인식과 같이 자동적으로 인증대상자를 확인할 수 있는 물리적 측정이 가능한 특성에 의존한다(Ives et al., 2004; Irakleous et al., 2002).

3. 연구모형 및 가설

3.1 연구모형 도출

본 연구는 사회범죄학 분야에서 범죄억제에 관한 대표적 이론인 Nagin의 일반억제이론(GDT : General Deterrence Theory)에 기반하여 정보시스템 오남용 억제를 위한 이론적 틀을 개발하는데 초점을 둔다. 즉, 불법적이거나 비정상적인 행위를 저지를 수 있는 잠재적 행위자들로 하여금 이러한 행위에 따른 제재(Sanctions)의 확실성과 엄격성을 인지하게 함으로써 행위를 시도할 가능성을 줄일 수 있다는 일반억제이론(GDT)에 근거할 때 정보시스템을 불법적이거나 비정상적으로 활용하는 정보시스템 오남용 행위에 대한 조직 내 제재가 확실하게 이루어지며 제재수준도 엄격하다고 조직구성원들이 느낄수록 이러한 오남용 행위가 줄어들 것으로 예상할 수 있다. 따라서 조직들은 이해관계자들의 정보시스템 오남용 행위에 효과적으로 대처하기 위해 오남용에 따른 제재의 확실성과 엄격성에 대한 이들의 인지수준을 높일 수 있는 대책으로서의 정보보안 대책을 강구하여야 하는 바, 기존 연구들에 대한 고찰결과에 의하면 조직들이 실시하고 있는 정보보안대책은 네 가지(보안정책, 보안인식 프로그램, 보안 모니터링 실시, 보안 소프트웨어)로 유형화됨을 알 수 있다. 즉, 조직들은 이러한 정보보안 대책을 수립 실시함으로써 정보시스템에 대한 잠재적 오남용 행위자들에게 정보시스템 오남용에 대한 제재의 확실성과 엄격성을 인지시킴으로써 오남용행위의 시도가 억제될 수 있다고 추론할 수 있다.

한편, Arjzen의 합리적 행동이론(TRA : Theory of Reasoned Action)에 의하면 행위(Behavior)에 앞서 의도(Intention)가 형성됨을 알 수 있는데 정

보시스템 오남용 행위에 있어서도 오남용 의도가 가장 영향력 있는 선행변수가 될 것이다. 본 연구에서는 정보보안 대책과 일반억제이론을 접목함에 의해 정보보안 대책의 정보시스템 오남용 억제 메커니즘을 실증적으로 규명하는데 주안점을 두고 있기 때문에 실증분석을 위한 오남용 행위 실태에 대한 솔직하고 객관적인 자료수집이 전제가 되어야 하나, 이러한 자료수집의 어려움과 한계가 매우 큰 것을 감안하여 오남용 행위의 강력한 선행변수인 오남용 의도를 종속변수로 설정하고자 한다.

이상과 같은 관련 이론들에 대한 논리적 추론(logical reasoning)에 근거하여 본연구의 연구모형은 아래의 <Figure 2>와 같이 제시될 수 있을 것이다.

3.2 가설 설정

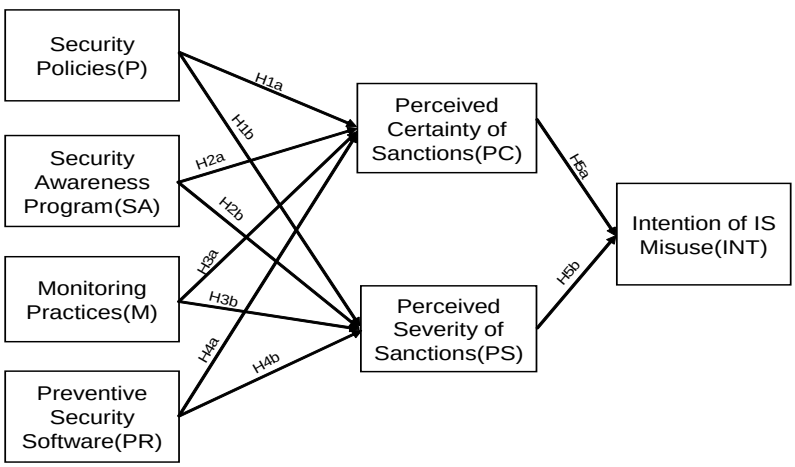
3.2.1 정보보안 대책과 제재의 확실성 및 엄격성 인지수준과의 관계(H1~H4)

보안정책들의 주된 목적은 정보시스템 사용 시의 불법적이거나 허용되지 않는 행동을 명확하게 정의하고 위반 시에는 처벌될 수 있다는 인식을 증가시킴으로 정보시스템 오남용을 억제하는데 있다(Lee and Lee, 2002). Straub(1990)는 보안정책의 명확함과 구체성은 정보시스템 오남용을 억제하는데 중요한 전제가 됨을 밝히면서 보다 자세하고 구체적인 보안정책이 공지될수록 허용되지 않는 시스템 사용에 대한 보다 강한 제재 효과가 있다고 주장하고 있다. 또한 Foltz(2000)는 조직의 정보시스템 사용에 관한 정책을 잘 알고 있는 조직 구성원들이 정보시스템 오남용의 부정적인 결과에 대한 인지수준이 보다 높음을 발견하고 보안정책과 처벌에 대한 인지수준간의 긍정적인 관계를 지지하는 실증적 연구결과를 제시하였다. 이러한 연구들에 의거할 때 보안정책의 수립 및 공지와 불법적이거나 허용되지 정보시스템 사용시 받을 수 있다고 인지되는 제재 수준간의 관계에 관하여 다음의 두 가지 가설이 설정될 수 있다.

(H1a) : 보안정책은 제재의 확실성 인지도에 정(正)의 영향을 미칠 것이다.

(H1b) : 보안정책은 제재의 엄격성 인지도에 정(正)의 영향을 미칠 것이다.

보안정책과 마찬가지로 보안인식 프로그램은 정보시스템의 정확하거나 정확하지 않은 사용방법과 잘못된 사용 시의 처벌에 대한 인식을 강화하기 위한 교육훈련 프로그램을 제공함으로써 정보시스템



〈Figure 2〉 Research Model

오남용 시도를 억제하기 위해 설계된 소극적인 보안 통제 방안이다(Straub, 1990). 즉, 보안인식 프로그램의 주된 목적은 잠재적인 정보시스템 오남용자들로 하여금 조직은 정보시스템을 보호하는데 엄격하며 의도적인 보안위반을 결코 가볍게 다루지 않는다는 것을 인식시키는데 주된 목적이 있다(Straub and Welke, 1998). 이와 같이 보안인식 프로그램은 정보시스템 오남용시의 제재의 확실성과 엄격함 모두를 모두 강조하고 있다고 보며, 이를 근거로 아래의 두 가지 가설이 설정될 수 있다.

(H2a) : 보안인식 프로그램은 제재의 확실성 인지도에 정(正)의 영향을 미칠 것이다.
(H2b) : 보안인식 프로그램은 제재의 엄격성 인지도에 정(正)의 영향을 미칠 것이다.

정보시스템 오남용 억제에 관한 연구들에 있어서 공통적인 주제는 적극적이고 가시적인 보안 노력은 오남용에 따른 결과에 대한 위협을 크게 증가시키는 경향이 있기 때문에 정보시스템 오남용을 억제할 수 있다는 것이다(Kankanhalli et al., 2003). Straub (1990)은 정보시스템 사용상의 허용범위에 관한 조직의 정책이 준수되는지 감시하고 이행되도록 강제화하는 정보보안 관리자의 노력과 같은 조직 내에서의 보안활동에 대해 조직 구성원들이 민감하게 반응함을 실증적으로 밝혔고, Straub and Nance(1990)는 정보시스템 오남용 억제는 위반행위의 탐지 및 적발을 통해 이루어짐을 강조하고 있다. 즉, 조직원들의 컴퓨팅 활동에 대한 모니터링은 여러 형태의 정보시스템 오남용의 탐지 및 적발가능성을 높이는 적극적인 오남용 억제 대책으로서 조직의 보안 모니터링 실시에 대해 조직원들이 인식하고 있다면 보안 모니터링으로 인해 적발될 가능성과 처벌될 가능성에 대한 잠재적 위반자들의 인지수준을 보다 제고할 것으로 기대되며, 이에 따라 아래의 두 가설을 설정될 수 있을 것이다.

(H3a) : 보안 모니터링 실시는 제재의 확실성 인지도에 정(正)의 영향을 미칠 것이다.
(H3b) : 보안 모니터링 실시는 제재의 엄격성 인지도에 정(正)의 영향을 미칠 것이다.

정보시스템 오남용을 예방하는 보안 소프트웨어는 인가되지 않은 컴퓨팅 활동과 정보자원에 대한 불법적 접근을 막음으로써 정보시스템 오남용에 직접적인 예방을 가능하게 할 수 있다. 그러나 Straub and Welke(1998)는 효과적인 보안 소프트웨어는 정보시스템 오남용에 대한 예방적 효과 뿐 만 아니라 잠재적 오남용자들로 하여금 처벌의 엄격함과 확실함을 확인시켜 줌으로써 향후 발생할 수도 있는 정보시스템 오남용 의도에 대한 억제 효과도 동시에 있음을 실증적인 연구결과로 제시하였으며, Lee and Lee(2002)의 연구에서도 보안 소프트웨어 사용 자체가 잠재적 오남용자들로 하여금 적발에 대한 공포를 증대시킬 수 있음을 주장하고 있다. 또한 Willson(2000)은 물리적이고 논리적인 예방대책들과 같은 범죄기회 감소체계가 오남용자들의 처벌 위험 인식수준을 증가시킴에 의해 정보시스템 오남용 사건의 발생이 감소될 수 있음을 예측함에 있어서 상황적 범죄예방 이론을 적용하였다. 이상과 같은 연구들로부터 잠재적인 오남용자들은 예방적인 보안통제 수단들을 자각하게 될수록 정보시스템 오남용에 따른 제재의 확실성과 엄격성을 더 크게 인식하게 됨을 추론할 수 있으며, 이로부터 아래의 두 가설이 설정될 수 있을 것이다.

(H4a) : 보안 소프트웨어 사용은 제재의 확실성 인지도에 정(正)의 영향을 미칠 것이다.
(H4b) : 보안 소프트웨어 사용은 제재의 엄격성 인지도에 정(正)의 영향을 미칠 것이다.

3.2.2 제재의 확실성 및 엄격성 인지도와 정보시스템 오남용 의도와의 관계(H5)

일반억제이론(GDT)은 공식적 및 비공식적 제재 실행에 따른 범죄 및 일탈행위에 대한 영향은 2가

지의 구성개념('제재의 확실성 인지도'와 '제재의 엄격성 인지도')을 통해 나타난다고 주장하였다(Nagin, 1978). 여기서 제재의 확실성은 처벌받을 가능성을 나타내며 제재의 엄격성은 처벌의 정도를 나타내는데 본 연구에서도 이 2가지 구성개념(Constructs)을 정보시스템 오남용 제재와 연관된 처벌의 가능성과 정도를 인식하는 정도로 보고자 한다.

제재에 관한 연구들은 제재의 두려움이 다양한 범죄와 일탈 행위들을 예방할 수 있음을 주장해 왔다(Nagin and Pogarsky, 2001). Silberman(1976)는 처벌에 대한 인지된 확실성과 엄격성은 폭력 및 기물파손, 음주 그리고 풍기문란과 같은 몇 가지 범죄적 행위와 부정적 상관관계가 있음을 발견했다. 그리고 Tittle(1980)은 제재의 두려움이 업무상의 일탈 행위뿐만 아니라 몇 가지 사회적 일탈 행위의 의도와 부정적인 연관성을 가지고 있음을 발견했다. 즉, 적발의 인지된 가능성과 처벌의 엄격성에 대한 인지정도가 소매상점에서 도둑질 하려는 개인의 의도에 대해 중요한 예측변수가 되는 연구결과를 제시하였다. 다른 실험에서는 조직 내의 절도범을 조사한 결과 조직의 제재의 확실성과 엄격성 정도를 낮게 인지한 종업원들이 고용주로부터 절도를 할 경향이 높았음을 발견함으로써 처벌에 대한 확실성과 엄격성 인지도가 높을수록 범죄와 일탈 행위가 감소함에 대한 강한 증거를 제공하고 있다. 이러한 연구들에 근거할 때 정보시스템 오남용과 같은 전형적으로 비전문가나 회사원의 부정행위도 조직의 법규와 규제를 위반하는 일탈 행위로서 이에 대한 제재의 확실성과 엄격성에 대한 인지수준이 높을수록 정보시스템 오남용 행위 의도는 약해질 것으로 추론된다.

(H5a) : 제재의 확실성 인지도는 정보시스템 오남용 의도에 부(負)의 영향을 미칠 것이다.

(H5b) : 제재의 엄격성 인지도는 정보시스템 오남용 의도에 부(負)의 영향을 미칠 것이다.

4. 연구방법론

4.1 자료수집방법 및 측정지표

4.1.1 시나리오 기반의 설문조사

본 연구는 실증분석을 위한 자료수집을 위해 설문에 의한 서베이(Survey) 조사 방법을 이용하였으며, 본 연구주제의 특성을 반영하여 제반 조직들에서 일반적으로 나타날 수 있는 정보시스템 오남용 발생상황을 묘사한 시나리오를 제시하고 응답자들이 시나리오을 읽고 해당 시나리오에 대한 자신의 의견에 따라 설문에 응답하도록 하였다.

시나리오[1]들은 응답자별 특수성에 영향을 받지 않은 표준화된 응답을 확보할 수 있을 뿐만아니라 보다 현실에 가까운 의사결정상황을 제공하는데 유용하며(Harrington, 1996), 시나리오가 응답자들이 접하는 현실적인 심리적 및 사회적 상황에 근사하게 작성될 경우 응답자들의 흥미를 유발하여 설문응답에 보다 적극적으로 참여하게 할 수 있다(Kerlinger, 1973). 또한 응답자들이 예민하게 반응할 수 있는 이슈에 대해 가정된 상황을 제공함으로써 응답자 자신이 아닌 해당 상황에 대한 응답을 하게 함으로써 응답에 따른 개인적인 불이익이나 위협을 느끼지 않게 할 수 있을 뿐만 아니라 응답 시에 사회적 바람직성(social desirability)에 의한 편향을 최소화할 수 있다는(Harrington, 1996) 장점이 있다. 이러한 시나리오 기반의 설문조사의 장점들을 감안할 때 본 연구의 주제인 정보시스템 오남용 행위와 같은 개인적으로 드러내고 싶지 않거나 스스로 경험하지 않은 상황에 대한 응답을 확보하는데 있어서 시나리오 기반의 설문조사가 매우 적합한 방안으로 판단되어 이를 채택하였다.

본 연구에서는 (1) 적절치 못한 이메일 메시지의 배포 (2) 비인가된 컴퓨터 소프트웨어의 사용 (3) 비밀번호 공유 (4) 인가받지 않은 정보시스템

1) 시나리오는 "응답자가 그들의 판단에 근거로 삼기 위해 필요로 하는 정보를 포함하는 가설적인 사람이나 상황들에 관한 간략한 기술"로 정의될 수 있다.

접속 (5) 정보시스템의 인가되지 않은 수정 등 5가지의 시나리오를 포함하였으며, 시나리오별 스토리는 응답자들이 시나리오 상황에 자신을 투사하게 할 수 있도록 가급적 그럴듯하고 현실적으로 여겨지도록 하기 위해 일상적으로 자주 발생하는 정보시스템 오남용 상황을 구체적으로 묘사하고자 했고, 시나리오상의 가상 인물들에 이름까지도 부여하고자 하였다(Finch, 1987).

시나리오는 응답의 편의(Bias)를 방지하기 위해 설문의 첫머리에 제시하였는데 시나리오를 읽기 전에 정보보안 대책에 관한 설문 문항을 보게 될 경우 시나리오에 대한 응답자의 반응과 시나리오와 관련되는 설문 응답에 영향을 미칠 수 있기 때문이다.

4.1.2 변수별 측정지표

본 연구의 연구모형에 포함된 7가지의 변수(보안정책, 보안인식 프로그램, 보안 모니터링 실시, 보안 소프트웨어, 제재의 확실성 인지도, 제재의 엄격성 인지도, 정보시스템 오남용 의도)를 측정하기 위한 측정지표를 기존의 관련 연구들(Lee et al., 2004; Stanton et al., 2003; Straub, 1990)을 참조하거나 정보시스템 보안전문가들로부터의 자문을 통해 개발하였으며 변수별 측정지표들은 아래와 같다.

1) 보안정책(P)

'보안정책(Security Policies; P)'의 수립 및 제공 수준은 '조직의 보안정책 및 컴퓨터 자원사용에 관한 지침의 수립 및 제공정도'로서 이를 평가하기 위하여 1) 이메일 사용에 대한 지침 및 가이드 제공 정도(P1), 2) 정보보안에 관한 정책 및 지침, 절차 제공 정도(P2), 3) 주요 시스템의 접근통제 정책 제공 정도(P3), 4) 공개형(무료)소프트웨어를 설치하는 것을 금지하는 정책제공 정도(P4), 5) 주요 시스템에 접속하기 위한 비밀번호의 사용에 대한 지침 제공정도(P5), 6) 민감 정보에 접속하는 것을 방지하기 위한 통제방법 제공정도(P6), 7) 개인컴퓨터용(PC) 사용지침 제공정도(P7), 8) 비인가자가 중요 데이터를 수정하는 것을 금지하기 위한 정책 제공 정도(P8) 등 8개 측정지표를 개발하였으며, 응답자들은 각 지표별로 1(매우 낮음)부터 7(매우 높음)까지의 리커트형(Likert-type) 7점 척도로 평가하였다.

2) 보안인식 프로그램(SA)

'보안인식 프로그램(Security Awareness Program : SA)' 수준은 '조직의 정보시스템 보안 교육과 훈련의 이행정도'로서 이를 평가하기 위해 1) 최신정보기술에 대한 교육 이행 정도(SA1), 2) 비밀번호의 관리와 책임에 대한 교육 이행 정도(SA2), 3) 임직원에 대한 정보보안교육 및 훈련 이행 정도(SA3), 4) 응용 소프트웨어 저작권에 대한 교육 이행 정도(SA4), 5) 주요 시스템 사용의 보안책임에 대한 교육 이행 정도(SA5), 6) 이메일 사용에 대한 교육 이행 정도(SA6) 등의 6개 측정지표를 개발하였으며, 응답자들은 각 지표별로 1(매우 낮음)부터 7(매우 높음)까지의 리커트형(Likert-type) 7점 척도로 평가하였다.

3) 보안 모니터링(M)

'보안 모니터링(Monitoring Practices : M)' 수준은 '조직원들의 컴퓨터 업무수행에 대한 모니터링 실시에 대한 인식정도'로서 이를 평가하기 위해 1) 전산화된 정보의 모든 변경에 대한 모니터링 정도(M1), 2) 주요 시스템에 대해 업무 이외의 내용의 사용이 있는지에 대한 모니터링 정도(M2), 3) 임직원들의 컴퓨터 사용 내용의 기록의 검토 수준(M3), 4) 인가되지 않은 소프트웨어의 사용에 대한 모니터링 수준(M4), 5) 민감한 정보에 접속하는 임직원들을 대상으로 한 모니터링 정도(M5), 6) 이메일 내용에 대한 모니터링 정도(M6), 7) 주요 시스템을 대상으로 권한이 없는 자의 접근에 대한 보고수준(M7) 등의 7개 측정지표들을 개발하였으며, 응답자들은 각 지표별로 1(매우 낮음)부터 7(매우 높음)까지의 리커트형(Likert-type) 7점 척도로 평가하였다.

4) 보안 소프트웨어(PR)

'보안 소프트웨어(Preventative Security Software : PR)' 수준은 '조직 내에서의 보안 소프트웨어 사용과 가용성 수준에 대한 인식정도'로서 이를 평가하기 위해 1) 비밀번호의 주기적 변경 수준(PR1), 2) 조직 내 제반 정보시스템의 접근통제 정도(PR2), 3) 접근권한 정책에 따라 인가된 권한으로 해당시스템에 접속하는 수준(PR3), 4) 모든 정보시스템에 대한 비밀번호 접속 정도(PR4), 5) 보안소프트웨어(백신 및 보안프로그램 등)를 일괄적으로 설치하도록 한 환경설정 정도(PR5) 등 5개의 측정지표들을 개발하였으며, 응답자들은 각 지표별로 1(매우 낮음)부터 7(매우 높음)까지의 리커트형(Likert-type) 7점 척도로 평가하였다.

5) 제재의 확실성 인지도(PC)

'제재의 확실성 인지도(Perceived Certainty of Sanctions : PC)'에 대한 측정지표는 Peace et al.(2003)의 연구에서 채택한 측정지표(조직의 정보시스템 오남용 행위자 적발가능성 정도(PC1))와 본 연구에서 개발된 측정지표(조직의 정보시스템 오남용 행위 발견가능성 정도(PC2)) 등 두 가지 지표에 의해 측정되었으며, 시나리오에서 묘사된 5가지 오남용행위 사례별로 측정지표에 대한 응답을 하도록 하였다. 즉, 응답자들은 자신의 업무환경에서 시나리오상의 인물들이 범한 정보시스템 오남용 행위가 발견되고 해당 오남용 행위자가 적발될 가능성에 대한 인지수준을 1(매우 낮음)부터 7(매우 높음)까지의 리커트형(Likert-type) 7점 척도로 평가하였는데 시나리오 인물들의 행위에 대한 응답자의 판단은 결국 그들 자신의 발각 가능성을 투사하는 것으로 여겨질 수 있다.

6) 제재의 엄격성 인지도(PS)

'제재의 엄격성 인지도(Perceived Severity of Sanctions : PS)' 수준에 대한 측정지표는 Peace et al.(2003)의 연구에서 채택한 측정지표(조직의 정보시스템 오남용 행위에 대한 처벌가능성 정도(PS1))와 본 연구에서 개발된 측정지표(조직의 정보시스템 오남용 행위에 대한 처벌 강도(PS2)) 등 두 가지 지표에 의해 측정되었으며, 시나리오에서 묘사된 5가지 오남용 행위 사례별로 측정지표에 대한 응답을 하도록 하였다. 즉, 응답자들은 자신이 속한 조직이 시나리오의 인물들이 범한 것과 같은 정보시스템 오남용 행위에 대하여 처벌할 가능성과 처벌강도에 대해 인지하고 있는 수준을 1(매우 낮음)부터 7(매우 높음)까지의 리커트형(Likert-type) 7점 척도로 평가하였는데 이 같은 응답자들의 판단은 결국 자신들이 그 같은 행위를 하였을 때 그들 자신의 처벌 가능성에 대한 인지수준을 투사하는 것으로 볼 수 있다.

7) 정보시스템 오남용 의도(INT)

'정보시스템 오남용 의도(Intention of IS Misuse : INT)'에 대한 측정을 위하여 Leonard et al.(2004)의 연구에서 사용된 측정지표(자신의 정보시스템 오남용 가능성 정도(INT1))와 본 연구에서 개발한 측정지표(조직원들의 정보시스템 오남용 가능성 정도(INT2)), 두 가지 측정지표로 평가하였으며 1(매우 낮음)부터 7(매우 높음)까지의 리커트형(Likert-type) 7점 척도에 의하였다. 즉, 응답자 자신이 시나리오상의 인물들과 같은 상황에 처할 경우 비슷한 행위를 할 가능성과 응답자 자신에 대한 응답이 사회적 바람직성(social desirability)에 의한 편향으로 인해 미흡할 가능성이 있음을 고려하여 자신이 속한 조직 내의 평범한 구성원들이 시나리오상의 인물들이 처한 상황에서 유사한 오남용 행위를 할 가능성을 동시에 응답토록 함에 의해 자신의 정보시스템 오남용 행위 의도를 간접적으로 투사하도록 하였다.

4.2 표본추출과 응답자 특성

정보시스템 오남용 실태에 관한 기존의 연구들은 주로 정보시스템 업무 담당자들에게만 집중하고 있는 경향이 있었는데(Harrington, 1996), 이는

정보시스템 오남용의 가능성을 실제로 마주하고 있는 다수의 컴퓨터 사용자 집단의 상황을 반영하지 못할 가능성이 크다. 본 연구에서는 정보시스템업무 담당자 뿐만아니라 일상 업무환경에서 컴퓨터를 사용하는 모든 개인들을 조사대상으로 하고자 하였으며, 이를 위해 여러 업종에 속한 기업 조직들 내의 다양한 부서와 업무환경하의 컴퓨터 사용자들을 모집단으로 하여 표본 추출하였다.

표본추출 대상 회사 명단은 연구자의 개인적인 접촉과 일부 공공기관의 공개된 정보를 통해 입수하였고 해당 조사대상 기업의 임직원들 중에서 무작위로 설문응답자를 선정하여 협조 연락을 취하였다. 또한 오프라인상의 문서기반의 설문조사가 아닌 인터넷 기반의 설문조사를 실시함으로써 조사과정상의 지리적 및 시간적 제약을 최대한 극복하고자 하였다. 그리고 연구의 목적을 설명함과 동시에 협조요청을 구하기 위해 이메일을 송부하였으며 완성된 설문을 보내준 응답자들에게 감사의 이메일 및 문자메시지를 보냈다.

무작위로 추출된 450명의 조사 대상자에게 설문협조요청을 했으며 이들 중 158명이 설문에 응답해 줌으로써 응답률은 약 35.1%를 보였다. 또한 158명의 응답 설문들을 점검한 결과 미완성이거나 무성의하게 작성되어 사용할 수 없다고 판단되는 43개 설문(27.2%)을 제외한 후, 유효하다고 확인된 115명의 설문응답 결과를 사용하였으며 응답자의 인구통계학적 특성을 살펴보면 <Table 1>과 같다. 즉, 전체 응답자 중 남성은 87명(75.7%), 여성은

〈Table 1〉 Demographic Characteristics of Respondents

Classification		Frequency	Percent(%)
Gender	Male	87	75.7
	Female	28	24.3
	Total	115	100.0
Age	less than 24	10	8.7
	25~34	44	38.3
	35~44	33	28.7
	45~54	23	20
	over 55	5	4.3
	Total	115	100.0
Industry Field	Manufacturing	12	10.4
	Education Service	19	16.5
	Financial and Assurance	10	8.7
	Wholesale and Retail Trade	17	14.8
	Information and Communications	41	35.7
	Public Organization	6	5.2
	etc.	10	8.7
	Total	115	100.0
Job Type	Managerial	12	10.4
	Technical	18	15.7
	Professional	29	25.2
	Staff(Office Worker)	56	48.7
	Total	115	100.0

28명(24.3%) 이었으며, 응답자의 연령은 25~44세가 77명(67%)으로 가장 많았으며 45~55세 이상의 응답자도 28명(24.3%)로 전반적으로 대부분의 연령대를 포함한 응답 결과를 도출하였다. 또한 응답자가 속한 업종을 살펴보면, 정보기술업이 41명(35.7%)으로 가장 많았고 교육 서비스업 19명(23.5%), 도소매업 17명(14.8%) 그리고 금융 및 보험업이 10명(8.7%) 등 다양한 업종에 종사하는 것으로 나타났다. 아울러 응답자의 직책은 관리직/사무직이 56명(48.7%)로 제일 많았으며, 전문직 29명(25.2%), 기술직 18명(15.7%), 경영진 12명(10.4%)의 순으로 나타났다.

5. 실증분석 결과

5.1 변수의 신뢰성 및 타당성분석

연구모형에 포함된 변수들의 측정지표들 중에는 본 연구에서 처음 개발된 지표들과 기존 연구에서 사용되었지만 본 연구에서 수정된 지표들이 다수 포함되어 있어 변수의 신뢰성 및 타당성 분석을 위하여 탐색적 요인분석(EFA : Exploratory Factor Analysis)을 먼저 실시한 후 이어서 확인적 요인분석(CFA : Confirmatory Factor Analysis)을 실시하였다. 우선 베리맥스(Varimax) 회전방식에 의한

〈Table 2〉 The Result of Exploratory Factor Analysis

Variable	Intention of IS Misuse (INT)	Monitoring Practices (M)	Security Policies (P)	Perceived Certainty of Sanctions (PC)	Preventive Security Software (PR)	Perceived Severity of Sanctions (PS)	Security Awareness Program (SA)
INT1	**0.733**	-0.401	-0.361	-0.132	-0.269	-0.435	-0.436
INT2	**0.791**	-0.098	-0.097	-0.418	-0.167	-0.450	-0.085
M2	-0.277	**0.775**	0.653	0.174	0.482	0.324	0.626
M3	-0.340	**0.878**	0.634	0.344	0.503	0.426	0.661
M4	-0.360	**0.782**	0.697	0.142	0.520	0.365	0.690
M5	-0.300	**0.862**	0.749	0.292	0.620	0.376	0.771
M6	-0.136	**0.793**	0.591	0.179	0.408	0.352	0.571
M7	-0.203	**0.857**	0.643	0.240	0.541	0.412	0.666
P1	-0.312	0.680	**0.895**	0.210	0.699	0.282	0.751
P5	-0.137	0.716	**0.774**	0.059	0.592	0.227	0.640
P7	-0.255	0.682	**0.894**	0.157	0.616	0.324	0.704
PC1	-0.370	0.271	0.171	**0.928**	0.134	0.499	0.304
PC2	-0.238	0.291	0.201	**0.882**	0.159	0.445	0.291
PR1	-0.244	0.549	0.666	0.184	**0.871**	0.365	0.621
PR2	-0.296	0.528	0.663	0.128	**0.891**	0.356	0.595
PR3	-0.130	0.551	0.604	0.101	**0.854**	0.325	0.531
PS1	-0.416	0.475	0.457	0.330	0.435	**0.845**	0.499
PS2	-0.416	0.417	0.208	0.323	0.262	**0.855**	0.383
SA2	-0.321	0.715	0.772	0.275	0.671	0.413	**0.925**
SA4	-0.323	0.687	0.662	0.279	0.455	0.416	**0.837**
SA5	-0.221	0.738	0.739	0.277	0.661	0.412	**0.900**

탐색적 요인분석(EFA) 실시결과를 보면 <Table 2>와 같이 당초에 포함된 일부 측정지표들이 제외되기는 하였지만 모든 요인이 0.6 이상의 요인적재량 나타냄으로써 연구모형에 포함된 모든 변수들에 있어서 일차적인 수렴타당성(Convergent Validity) 및 판별타당성(Discriminant Validity)이 확보됨을 확인하였다.

이어서 탐색적 요인분석(EFA) 결과로 남게 된 각 변수별 측정지표들에 대한 신뢰성(Reliability)과 집중타당성(Convergent Validity) 및 판별타당성(Discriminant Validity) 등 측정모형(Measurement Model)의 검증과 변수들간의 관계의 통계적 유의성을 확인하기 위한 구조모형(Structural Model)의 검증을 위해서 PLS(Partial Least Square)통계분석기법을 바탕으로 확인적 요인분석(CFA)을 실시하였다. 본 연구에서 PLS 기법을 택한 것은 PLS의 경우 LISREL이나 AMOS 등 다른 구조방정식 모형(SEM : Structural Equation Modeling) 분석 기법과 달리 분석 데이터의 정규성(Normality)를 전제로 하지 않아 비교적 적은 샘플로도 분석이 가능하며(Chin, 1998), 측정모형과 구조모형을 동시에 검증할 수 있음으로써 전통적인 통계분석기법(예 : 요인분석 및 회귀분석 등)보다 다양한 분석을 효과적으로 행할 수 있을 뿐 아니라(Gefen et al., 2000), 이론적인 공분산 구조를 설명하는데 초점을 맞추고 있는 공분산 기반의 구조방정식 기법(LISREL 및 AMOS)과 비교해서 는 PLS가 보다 예측지향적이고 변수별로 설명된 분산을 최대화를 추구함으로써 데이터 중심의 분석의 비중이 큰 탐색적인 연구에 적합하기 때문이다(Barclay et al., 1995).

탐색적 요인분석(EFA)에 이어서 실시된 PLS분석에 의한 측정모형에 대한 검증결과로서 이상의 탐색적 요인분석(EFA)을 통해 밝혀진 변수별 측정지표들에 대한 신뢰성 검증 결과는 <Table 3>과 같다. PLS를 통한 신뢰성분석은 복합신뢰도(Composite Scale Reliability Index : CSRI)값이 기준치인 0.70을 상회하고 평균 분산추출값(Average Variance Extracted : AVE)이 0.50을 상회하는 경우 신뢰성이 있다고 판단하며(Fornell and Larker, 1981; Chin, 1998), 또한 크론바하 α(Cronbach's Alpha) 계수값이 0.60 이상이면 신뢰성이 있는 것으로 간주하는 바(Hair et al., 1998; Nunnally, 1978), <Table 3>에서 보는 바와 같이 탐색적 요인분석(EFA)후에 잔존한 측정지표들의 경우 제외되는 지표없이 모든 변수들에 있어서 신뢰성이 확보되는 것으로 나타났다.

PLS 분석시 구성변수들(Constructs)에 대한 타당성분석은 집중타당성(Convergent Validity)과 판별타당성(Discriminant Validity) 분석으로 구성되며 집중타당성은 탐색적 요인분석(EFA) 결과로 추출된 요인별로 묶인 측정지표들에 대한 확인적 요인분석(CFA)을 통해 검증이 이루어지며 이는 측정모형에 대한 검증결과로서 나타나게 된다. 확인적 요인분석에서는 변수 즉, 구성변수(Construct)에 대

〈Table 3〉 The Result of Reliability Testing

Variable	Number of Measurements	Composite Reliability	Average Variance Extracted	Cronbach's Alpha(α)
Monitoring Practices(M)	6	0.927	0.681	0.906
Preventive Security Software(PR)	3	0.905	0.760	0.843
Security Awareness Program(SA)	3	0.918	0.789	0.865
Security Policies(P)	3	0.891	0.733	0.820
Perceived Severity of Sanctions(PS)	2	0.854	0.662	0.742
Perceived Certainty of Sanctions(PC)	2	0.866	0.687	0.764
Intention of IS Misuse(INT)	2	0.780	0.543	0.601

한 요인적재량(Factor Loadings)이 0.70이어야 하며, 해당변수의 요인적재량은 그 외의 구성변수들과의 교차 요인적재량보다 커야 집중타당성이 확보되는 것으로 판단하는데 탐색적 요인분석 결과로 잔존한 측정지표들에 대한 PLS 분석결과 이 조건을 모두 만족함으로써 모든 변수들에 있어서 집중타당성이 확보된 것으로 확인되었다.

또한 변수별 판별타당성을 확인하는 방법은 해당변수와 다른 변수들과의 상관계수보다 해당변수의 평균 분산추출값(Average Variance Extracted : AVE)의 제곱근(Square Root)값이 크다면 판별타당성이 확보되었음을 판단할 수 있는데(Fornell and Larker, 1981), <Table 4>에서 보는 바와 같이 각 구성변수(Construct)별 평균 분산추출값(Average Variance Extracted : AVE)의 제곱근(Square Root)값인 대각선상의 수치가 해당 구성변수와 다른 구성변수와의 상관계수값보다 높게 나타났기 때문에 각 구성변수별 판별타당성이 확보되었음을 알 수 있다. 또한 판별타당성 확보여부의 추가적인 판단기준인 다중상관성(Multi-collinearity) 검증결과를 살펴보면 변수간 상관계수가 0.9보다 보다 크면 심각한 다중상관성이 있다고 보는 바(Bagozzi et al., 1991), <Table 4>에서 보면 변수들간 상관계수들 중 가장 높은 상관계수가 보안정책(P)과 보안인식 프로그램 실시(SA)간의 상관계수인 0.816으로 나타났는데 이는 다중상관성의 기준이 되는 0.9보다 낮아서 다중상관성 측면에서도 변수들간의 판별타당성은 확보되는 것으로 나타났다.

이상과 같은 PLS 분석을 통한 구성변수들의 측정모형에 대한 검증결과는 탐색적 요인분석을 통해 추출된 요인(구성변수)들 및 각 요인(구성변수)별 측정지표들의 신뢰성, 집중타당성과 판별타당성이 모두 확보되는 것으로 나타났다.

5.2 가설검증 결과

이상의 측정모형 검증을 통해 신뢰성과 타당성이 확인된 구성변수들간의 관계를 나타내는 구조모형을 검증함으로써 독립변수와 종속변수간 관계, 즉 본 연구의 가설들에 대한 검증을 실시하고자 하였다. PLS 분석에 있어서 구조모형의 검증은 독립변수와 종속변수간 관계의 강도를 나타내는 경로계수(Path Coefficients)와 독립변수들에 의해 설명되어지는 분산의 양을 의미하는 R^2 값을 추정함에 의해 이루어 진다(Chin 1998). 즉, R^2 값과 경로계수(적재량 및 통계적 유의성)는 구조모형이 얼마나 현실적으로 적합한지를 나타내는데 R^2 값은 구조모형의 예측 가능력을 의미하며 이는 회귀분석의 R^2 값와 같은 방식으로 설명될 수 있으며, 경로계수는 통계적으로 유의성이 있어야 하며 이론적 추론내용과 방향성이 동일하여야 한다. 또한 경로계수에 대한 유의성 검증결과는 당초 표본에

〈Table 4〉 The Result of Inter-Variable Correlations and Discriminant Validity Testing

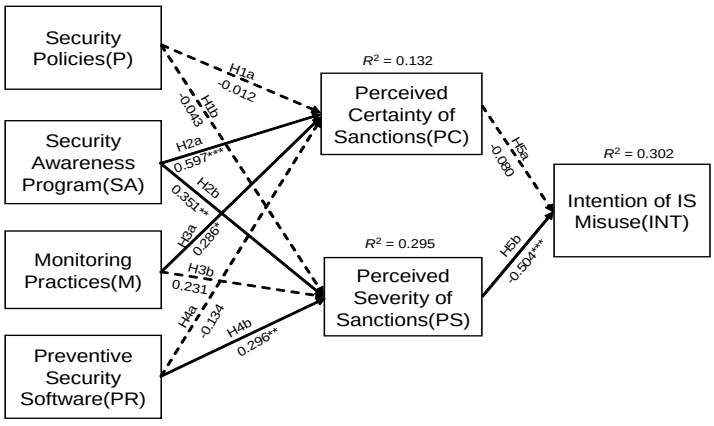
Variable(Construct)	M	PR	SA	P	PS	PC	INT
Monitoring Practices(M)	0.825						
Preventive Security Software(PR)	0.622	0.872					
Security Awareness Program(SA)	0.804	0.671	0.888				
Security Policies(P)	0.797	0.741	0.816	0.856			
Perceived Severity of Sanctions(PS)	0.458	0.401	0.466	0.329	0.814		
Perceived Certainty of Sanctions(PC)	0.287	0.161	0.312	0.177	0.504	0.829	
Intention of IS Misuse(INT)	-0.328	-0.260	-0.325	-0.286	-0.544	-0.343	0.737
AVE	0.681	0.760	0.789	0.733	0.662	0.687	0.543
SQRT of AVE	0.825	0.872	0.888	0.856	0.814	0.829	0.737

대한 PLS 분석에 의해 직접적으로 제공되지는 않으며 부트스트랩 기술을 이용한 표본 재추출을 통해 확보된 유사 데이터군에 PLS 분석을 실시한다. 일반적으로 PLS 분석기법을 적용한 기존의 정보시스템 에 관한 연구들에서는 500개의 서브샘플링을 많이 활용하고 있으며, 본 연구에서도 500개의 서브샘플링을 활용하여 경로계수에 대한 통계적 유의성을 검증하였다.

<Figure 3>은 PLS에 의한 구조모형 검증결과로서 R^2값을 살펴보면 정보보안 대책들인 독립변수들에 의해 '인지된 제재의 확실성(PC)'의 분산은 13.2%가 설명되며, '인지된 제재의 엄격성(PS)'의 분산은 29.5%가 설명되는 것으로 나타났다. 또한 최종 종속변수인 정보시스템 오남용 의도(INT)의 분산은 '인지된 제재의 확실성(PC)' 및 '인지된 제재의 엄격성(PS)'의 두 변수들에 의해 30.2%가 설명되는 것으로 나타나 경로계수의 해석을 의미있다고 판단하는 기준인 동시에 구조모형의 설명력의 실재(實在)함을 인정하는 기준으로서 Falk and Miller(1992)가 제시한 임계치인 10%를 상회하고 있는 것으로 나타났다. 아울러 <Figure 3>에서는 변수들간의 경로계수값(β)을 통계적 유의성과 함께 보여주고 있는데 이들 경로계수값(β)들을 기준으로 변수들간의 관계에 대한 이론적 추론 결과인 가설들에 대한 검증을 하였으며 각 가설별 검증결과는 아래와 같다.

5.2.1 정보보안 대책과 인지된 제재의 확실성 및 엄격성과의 관계(H1~H4)

<Figure 3>의 구조모형 검증결과상의 경로계수를 볼 때, 정보보안 대책들 중 '보안정책'의 수립은 '제재의 엄격성 인지도'와 '제재의 확실성 인지도'에 통계적으로 유의한 영향을 미치지 못하는 것으로 나타나 가설 H1a(보안정책은 제재의 확실성 인지도에 정(正)의 영향을 미칠 것이다) 및 가설 H1b(보안정책은 제재의 엄격성 인지도에 정(正)의 영향을 미칠 것이다)의 두 가설은 채택되지 못하였다. 즉, 이론적 추론과는 달리 현실에 있어서는 보안정책 수립 및 정비 그 자체만으로는 조직원들로 하여금 정보시스템 오남용에 따른 제재의 확실성과 엄격성의 인지수준이 높아지지는 않는다는 결과가 나타났다. 이는 우리나라 조직들에 있어서 많은 경우 정보시스템 오남용 억제를 위해 보안정책과 이에 의거한 보안지침이나 절차가 의례적으로 수립되고는 있으나 조직원들의 현업업무 수행과정에서 별 관심을 못 받을 뿐만 아니라 제대로 인지되지도



* p < 0.1, ** p < 0.05, *** p < 0.01.
Note) Paths in dash are not significant(p > 0.1).

〈Figure 3〉 The Result of Structural Model Testing by PLS Analysis

않기 때문인 것으로 추정된다.

그러나 '보안인식 프로그램'의 경우는 '제재의 확실성 인지도'(β = 0.597, $p < 0.01$)와 '제재의 엄격성 인지도'(β = 0.351, $p < 0.01$)에 큰 영향력을 유의하게 미치는 것으로 나타남으로써 가설 H2a(보안인식 프로그램은 제재의 확실성 인지도에 정(正)의 영향을 미칠 것이다) 및 가설 H2b(보안인식 프로그램 정책은 제재의 엄격성 인지도에 정(正)의 영향을 미칠 것이다)가 모두 채택되었다. 즉, 조직의 정보시스템 보안정책과 정보시스템의 바람직한 사용방법 및 오남용의 폐해, 오남용의 책임과 처벌 등을 인식시키기 위한 교육을 실시하는 것은 조직원들로 하여금 정보시스템을 오남용하게 되면 반드시 제재가 따르며 제재도 엄격히 이루어짐을 인지하게 하는데 매우 강력한 방안이 될 수 있음이 규명되었다.

조직원들의 정보시스템 이용에 관련된 활동을 감시하고 추적하는 '보안 모니터링 실시'는 '제재의 확실성 인지도'(β = 0.286, $p < 0.1$)에는 통계적으로 유의한 영향을 미치는 것으로 나타났으나, '제재의 엄격성 인지도'(β = 0.231, $p > 0.1$)에는 통계적으로 유의한 영향력이 없는 것으로 나타남으로써 가설 H3a(보안 모니터링 실시는 인식 프로그램은 제재의 확실성 인지도에 정(正)의 영향을 미칠 것이다)은 채택이 되었으나 가설 H3b(보안 모니터링 실시는 제재의 엄격성 인지도에 정(正)의 영향을 미칠 것이다)는 채택되지 못하였다. 이는 보안 모니터링을 실시하게 될 경우 조직원들은 정보시스템 오남용은 적발가능성이 높으며 오남용에 따른 제재가 반드시 있을 것이라고 인지하는 반면, 제재의 엄격성 수준이 높을 것이라고 인지하고 있지는 않음을 의미한다고 해석할 수 있다. 이와 같은 결과는 우리나라 조직들의 경우 보안모니터링이 비교적 상시로 이루어지고 있고 오남용 행위에 대한 제재도 확실하게 이루어지지만 조직에 초래하는 위해(危害) 정도가 큰 오남용 행위가 보안모니터링을 통해 적발되는 경우는 그다지 많지 않아 제재 수준 역시 높은 수준이 아니어서 보안 모니터링 실시가 조직원들이 인지하는 제재의 엄격성 수준에 유의한 영향을 못 미치는 것으로 판단된다.

마지막으로 조직원들의 부적절한 정보시스템 사용을 차단하거나 적법한 권한을 가진 조직원들만 해당 시스템을 접속 이용하게 할 수 있도록 함으로써 정보시스템 오남용의 가능성을 원천적으로 봉쇄하거나 예방하기 위한 소프트웨어를 설치 및 운영하는 것은 앞서의 보안 모니터링 실시와는 상반되는 가설검증 결과가 나타났다. 즉, 보안소프트웨어의 설치·운영은 '제재의 확실성 인지도'(β = −0.134, $p > 0.1$)에는 통계적으로 유의한 영향을 미치지 못하는 것으로 나타나 가설 H4a(보안 소프트웨어는 제재의 확실성 인지도에 정(正)의 영향을 미칠 것이다)는 채택되지 못하였으나, '제재의 엄격성 인지도'(β = 0.296, $p < 0.05$)에는 통계적으로 유의한 영향력이 있는 것으로 나타남으로써 가설 H4b(보안 소프트웨어는 제재의 엄격성 인지도에 정(正)의 영향을 미칠 것이다)는 채택되었다. 이는 조직원들이 보안 소프트웨어의 기능 및 성능을 충분히 신뢰하지 아니하여 보안 소프트웨어를 설치·운영한다고 해도 오남용 행위의 적발 및 이에 대한 제재가 반드시 이루어지지는 못할 것으로 보는 경향이 강하기 때문으로 추정된다. 그러나 보안 소프트웨어에 의해 적발이 되는 경우는 오남용 행위에 대한 부인이 불가능하여 이로 인한 자신이 조직 내에서 부담해야 할 불이익이 명확하기 때문에 오남용 행위에 따른 제재의 엄격성은 크게 인지하는 것으로 유추된다.

5.2.2 제재의 확실성 및 엄격성 인지도와 정보시스템 오남용 의도와의 관계(H5)

정보시스템 오남용 행위가 적발될 가능성에 대한 인지수준은 오남용 의도에 유의한 영향을 미치지 못하는 것으로 나타난 반면(β = −0.080, $p > 0.1$), 오남용 행위가 적발될 시 오남용 행위에 대한 처벌 가능성 및 처벌강도에 대한 수준이 높게 인지될수록 정보시스템 오남용 의도는 낮아짐이 통계적으로 유의성있게 나타남으로써(β = −0.504, $p < 0.01$),

가설 H5a(제재의 확실성 인지수준은 정보시스템 오남용 의도에 부(負)의 영향을 비칠 것이다)는 채택되지 못하였으나, 가설 H5b(제재의 엄격성 인지수준은 정보시스템 오남용 의도에 부(負)의 영향을 비칠 것이다)는 채택되었다. 이는 제재의 확실성과 엄격성이 공히 범죄행위 시도를 억제한다는 Nagin의 일반억제이론(GDT)이 사회범죄학 분야 연구에서는 대부분 실증적으로 지지되는 것으로 나타났으나, 정보시스템 오남용 분야에서는 제재의 확실성을 인지하는 것만으로는 오남용 억제에 도움이 되지 않으며 그 제재가 엄격함을 인지하여야 오남용 억제가 됨을 의미한다고 볼 수 있다. 이러한 결과가 나타난 것은 우리나라의 많은 조직들의 경우 조직원들이 자신의 정보시스템 오남용 행위의 적발 및 이에 대한 제재는 확실히 이루어진다고 생각하지만 그 제재수준이 높지 않아 제재로 인한 불이익을 크게 받았다는 느낌을 받지는 않고 있어 제재의 확실성만으로는 오남용 의도를 억제하지는 못하기 때문인 것으로 해석된다.

이상과 같이 기술된 바와 같은 PLS 분석에 의한 구조모형 검증결과에 기반한 가설검증 결과를 요약·제시하면 <Table 5>와 같다.

6. 결 론

본 연구는 제반 조직들의 정보기술 활용 및 정보시스템 의존도가 증가함에 따라 날로 심각성이 커지고 있는 정보시스템 오남용에 대처하기 위한 방안 수립에 근거가 될 수 있는 이론적 틀(Framework)을 제시하는데 초점을 두고 행태적인 측면에서의 오남용 억제요인 및 억제과정을 실증적으로 규명하고자 하였다. 이를 위해 사회범죄학 분야의 Nagin의 일반억제이론(GDT : General Deterrent Theory)을 기반으로 하여 정보시스템 오남용 억제를 위한 인과적 연구모형을 구축하고 이에 따른 연구가설을 도출하였다. 독립변수는 행태적 연구

〈Table 5〉 The Result of Hypothesis Testing

Hypothesis	Path Coefficient	T-value	Sig. Level(p)	Adoption/Rejection
Security Policies -> Perceived Certainty of Sanctions**(H1a)**	-0.012	0.092	0.339	Rejected
Security Policies -> Perceived Severity of Sanctions**(H1b)**	-0.043	0.583	0.198	Rejected
Security Awareness Program -> Perceived Certainty of Sanctions**(H2a)**	0.597	2.885	0.009	Adopted
Security Awareness Program -> Perceived Severity of Sanctions**(H2b)**	0.351	1.777	0.035	Adopted
Monitoring Practices -> Perceived Certainty of Sanctions**(H3a)**	0.286	1.347	0.093	Adopted
Monitoring Practices -> Perceived Severity of Sanctions**(H3b)**	0.231	1.112	0.127	Rejected
Preventive Security Software -> Perceived Certainty of Sanctions**(H4a)**	-0.134	0.776	0.223	Rejected
Preventive Security Software -> Perceived Severity of Sanctions**(H4b)**	0.296	1.670	0.042	Adopted
Perceived Certainty of Sanctions -> Intention of IS Misuse**(H5a)**	-0.080	0.739	0.202	Rejected
Perceived Severity of Sanctions -> Intention of IS Misuse**(H5b)**	-0.504	5.487	0.001	Adopted

접근방법에 의한 기존의 정보보안에 관한 연구들을 고찰함에 의해 보안정책 수립, 보안 인식프로그램 추진, 보안 모니터링 실시, 보안 소프트웨어 설치·운영 등 4가지 정보보안 대책을 개념적인 중복 없이 도출하였으며, 매개변수로는 Nagin의 일반억제이론(GDT)에 입각하여 정보시스템 오남용 행위에 대한 제재의 확실성과 제재의 엄격성을 설정하였다. 또한 종속변수로는 정보시스템 오남용 행위에 대한 정확한 데이터 수집의 어려움을 감안하여 오남용 의도로 정하였는데 이는 의도가 행위의 강력한 예측요인으로 밝혀진 기존 연구들(Ajzen, 1991; Ajzen, 1988)에 근거한 것이다.

연구모형 및 가설검증을 위하여 여러 업종에 속한 국내 기업들에서 450명의 임직원을 임의표본추출하여 시나리오 기반의 설문조사를 실시하였으며 이중 유효한 158명의 응답설문을 대상으로 PLS 분석기법에 의한 구조방정식 모형 검증을 하였다. 분석결과는 보안정책의 경우는 제재의 확실성과 엄격성 모두에 유의한 영향을 미치지 못하는 것으로 나타났으나, 보안인식 프로그램의 경우는 확실성과 엄격성 모두에 유의한 영향을 미치는 것으로 나타났는데 이는 보안정책의 수립 자체만으로는 정보시스템 사용자들이 자신의 오남용 행위에 대한 조직의 제재 가능성 및 제재의 엄격성을 체감하지 못하며, 교육 및 훈련을 통해 조직원들로 하여금 조직의 보안정책이나 적용 가능한 보안기술 및 방법론 전반을 폭넓게 인식시키는 것을 통해 정보보안 시스템 오남용에 대한 제재의 확실성과 엄격성에 대한 조직원들의 인지수준을 높일 수 있음을 시사하고 있다. 또한 보안 모니터링실시는 제재의 가능성 내지 확실성에 대한 조직원들의 인지수준에는 유의한 영향을 미치는 것으로 나타났으나 제재의 엄격성에는 유의한 영향을 미치지 못하는 것으로 나타난 반면, 적절한 보안 소프트웨어의 설치·운영은 제재의 확실성의 인지수준에는 유의한 영향을 미치지 못하는 것으로 나타났으나 재재의 엄격성에는 유의한 영향을 미치는 것으로 나타났는데 이는 이 두 가지 보안 대책이 반드시 상호보완적이고 병행적으로 추진되어야 할 필요성이 있음을 의미한다고 볼 수 있다. 한편 제재의 확실성과 엄격성 인지수준이 종속변수인 정보시스템 오남용 의도에 미치는 영향은 제재의 엄격성을 높게 인지할수록 오남용의도가 낮아지는 결과가 유의하게 나타났으나 제재의 확실성에 대한 인지수준은 오남용의도에 유의한 영향을 미치지 못하는 것으로 나타나 정보시스템 오남용을 억제하기 위해서는 적발 및 제재의 확실성을 높이는 것보다는 적발시에 엄격히 게재됨을 인지하게 하는 것이 오남용 방지에 더욱 효과가 있음이 밝혀졌다.

본 연구의 이론적 측면에서의 기여도는 기존의 정보시스템 보안연구들에 대한 체계적인 고찰을 통해 행태적 연구 접근방법에 의한 정보시스템 보안 연구 수행 시에 포함하여야 할 전형적인 정보보안대책들을 도출하였고 사회범죄학분야의 일반억제이론(GDT)을 정보시스템 보안 분야에도 적용함으로써 향후 정보시스템 보안연구의 위한 이론적 외연을 확대하였으며, 실증분석을 위해 연구모형 내 포함된 제 구성변수들에 대한 신뢰성 및 타당성 있는 측정지표들을 개발함으로써 향후 정보시스템 오남용 분야의 실증연구 수행을 보다 용이하게 하였다는 것이다. 특히, 본 연구에서는 기존의 정보보안 연구와 달리 정보시스템업무 담당자의 관점이 아닌 정보시스템 사용자의 관점에서 측정지표를 개발하였다는 점에서 향후 증가할 것으로 예상되는 정보시스템 사용자를 대상으로 한 정보보안 연구에 많은 도움이 될 것으로 판단된다. 아울러 본 연구결과로부터 도출될 수 있는 현실적인 측면에서의 시사점은 우선 정보보안 정책의 수립 및 정비만으로는 정보시스템 오남용의도를 억제하기 어려우며 조직원들을 대상으로 한 보안정책의 적극적인 홍보 및 교육이 수반되어야 하고, 특히 경영층의 보안정책의 추진 및 실행의지가 확고하여야 함을 알 수 있다. 또한 보안 소프트웨어를 이용한 정보시스템 오남용 행위의 적발 및 이에 따른 제재의 확실성을 높이기 위해 기능 및 성능 면에서 충분히 검증된 보안 소프트웨어의 개발 및 설치·

운영으로 조직원들의 보안 소프트웨어에 대한 신뢰감을 제고하여야 할 것이다. 보안모니터링 실시에 있어서도 오남용 행위별로 조직에 초래하는 위해(危害)의 정도를 평가하여 보안 모니터링을 보다 집중해야 할 오남용 행위의 우선순위 관리를 행하고 제재의 엄격성 수준도 차별화할 필요가 있다. 아울러 정보시스템 오남용 억제를 위해서는 조직원들로 하여금 제재의 확실성을 인지시키는 것만으로는 의미가 없으며, 반드시 제재의 엄격성이 높다는 인식을 조직원들이 인지하도록 해야 할 것이다.

이상과 같은 본 연구를 통해 예상되는 이론적 기여나 현실적 시사점에도 불구하고, 본 연구는 몇 가지 측면의 한계가 있다. 우선 연구방법론적인 측면에서 정보시스템 오남용의 실제 행위를 측정하지 못하고 오남용 의도를 대리지표로 이용한 점인데, 물론 의도가 행위의 강력한 예측지표이긴 하지만 향후 연구에서는 정보시스템 오남용 행위 자체를 종속변수로 하여 본 연구 결과와 비교할 필요성이 있다고 본다. 또한 일부 변수의 경우 이를 측정키 위한 지표수가 적어서 내용타당도가 우려되기도 하는 바, 향후 보다 많은 정보보안 전문가들로부터의 의견수렴과 관련 연구들에 대한 광범위한 고찰을 통해 측정지표들을 늘려갈 필요가 있다.

References

Ajzen, I., *Attitude, Personality, and Behavior*, Chicago : Dorsey Press, 1988.

Ajzen, I., "The Theory of Planned Behavior", *Organizational Behavior and Human Decision Processes*, Vol.50, No.2, 1991, 179-211.

Bachman, R., R. Paternoster, and S. Ward, "The Rationality of Sexual Offending : Testing a Deterrence/Rational Choice Conception of Sexual Assault", *Law and Society Review*, Vol.26, No.2, 1992, 343-372.

Bagozzi, R.P., Y. Yi, and L.W. Phillips, "Assessing Construct Validity in Organizational Research", *Administrative Science Quarterly*, Vol.36, No.3, 1991, 421-458.

Barclay, D.C., C. Higgins, and R. Thompson, "The Partial Least Squares Approach to Causal Modeling : Personal Computer Adoption and Use as an Illustration", *Technology Studies*, Vol.2, No.2, 1995, 285-308.

Cavusoglu, H. and S. Raghunathan, "Economics of IT Security Management : Four Improvements to Current Security Practices", *Communications of the AIS*, Vol.14, No.3, 2004, 65-75.

Chang, H.S. and D.H. Jung, "Organizational and Personal Characteristics to Determine the Intentions and Actions of the Computer Abuse", *Informatization Policy*, Vol.20, No.1, 2013, 42-60.

(장활식, 정대현, "컴퓨터 오남용의 의도와 행동을 결정하는 조직 및 개인적 특성", *정보화정책*, 제20권, 제1호, 2013, 42-60.)

Chin, W.W., "The Partial Least Squares Approach to Structural Equation Modeling", *In Modern methods for business research*, Vol.295, No.2, 1998, 295-336.

Cook, P.J., "Research In Criminal Deterrence : Laying the Groundwork for the Second Decade", *In Crime and Justice*, Vol.2, 1880, 211-268.

Dhillon, G., "Managing and Controlling Computer Misuse", *Information Management and Computer Security*, Vol.7, No.4, 1999, 171-175.

Dutta, A. and R. Roy, "The Dynamics of Organizational Information Security", *In Proceedings of the Twenty-Fourth International Conference on Information Systems*, December 14-17, Seattle, WA, 2003.

Falk, R.F. and N.B. Miller, *A Primer for Soft Modelling*, Akron, OH : Univ. of Akron Press, 1992.

Finch, J., "The Vignette Technique in Survey Research", *Sociology,* Vol.21, No.1, 1987, 105-114.

Foltz, C.B., "The Impact of Deterrent Countermeasures upon Individual Intent to Commit Misuse : A Behavioral Approach", Ph.D. diss, University of Arkansas, 2000.

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

Furnell, S.M., M. Gennatou, and P.S. Dowland, "A Prototype Tool for Information Security Awareness and Training", *Logistics Information Management*, Vol.15, No.5, 2002, 352-357.

Gefen, D., D.W. Straub, and M.C. Boudreau, "Structural Equation Modeling Techniques and Regression : Guidelines for Research Practice", *Communications of the AIS*, Vol.7, No.7, 2000, 1-78.

Gordon, L.A., M.P. Loeb, W. Lucyshyn, and R. Richardson, *2004 CSI/FBI Computer Crime and Security Survey*, *Computer Security Journal*, Vol.20, No.3, 2004, 33-51.

Ha, S.W. and H.J. Kim, "The Effects of User's Security Awareness on Password Security Behavior", *Journal of Digital Contents Society,* Vol.14, No.2, 2013, 179-189.

(하상원, 김형중, "정보보안의식이 패스워드 보안 행동에 미치는 영향에 관한 연구", *한국디지털콘텐츠학회논문지*, 제14권, 제2호, 2013, 179-189.)

Hair, J.F., R.E. Anderson, R.L. Tatham, and W.C. Black, *Multivariate Data Analysis,* Englewood Ciffs, NJ : Prentice Hall, 1998.

Hansche, S., "Designing a Security Awareness Program : Part 1", *Information Systems Security,* Vol.9, No.6, 2001, 14-22.

Harrington, S.J., "The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions", *MIS Quarterly*, Vol.20, No.3, 1996, 257-278.

Irakleous, I., S.M. Furnell, P.S. Dowland, and M. Papadaki, "An Experimental Comparison of Secret-Based User Authentication Technologies", *Information Management and Computer Security,* Vol.10, No.3, 2002, 100-108.

Ives, B., K.R. Walsh, and H. Schneider, "The Domino Effect of Password Reuse", *Communications of the ACM,* Vol.47, No.4, 2004, 75-78.

Jensen, B., "The Importance of Security Awareness Traing", Available at http://www.giac.org/practical/GSEC/Beth_Jensen_GSEC.pdf (Accessed May 13, 2003).

Kankanhalli, A., H.H. Teo, B.C.Y. Tan, and K.K. Wei, "An Integrative Study of Information Systems Security Effectiveness", *International Journal of Information Management*, Vol.23, No.2, 2003, 139-154.

Kerlinger, F.N., *Foundations of Behavioral Research, Second Edition*, New York : Holt, Rinehart and Winston, 1973.

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

Lee, S.M., S.G. Lee, and S. Yoo, "An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theorices", *Information and Management*, Vol.41, No.6,

2004, 707-718.

Leonard, L.N.K., T.P. Cronan, and J. Kreie., "What Influences IT Ethical Behavior Intentions -Planned Behavior, Reasoned Action, Perceived Importance, Individual Characteristics?", *Information and Management*, Vol.42, No.1, 2004. 143-158.

Nagin, D.S., "General Deterrence : A Review of the Empirical Evidence", In *Deterrence and incapacitation : Estimating the effexts of criminal sanctions on crime rates*, edited by A. Blumstein, J. Cohen and D.S. Nagin, Washington, D.C. : National Academy of Sciences, 1978.

Nagin, D.S. and G. Pogarsky, "Integrating Celerity, Impulsivity, and Extralegal Sanction Threats into a Model of General Deterrence and Evidence", *Criminology*, Vol.39, No.4, 2001, 865-891.

Nunnally, J.C., *Psychometric Theory*, *Second Edition,* New York : McGraw-Hill, 1978.

Panko, R.R. and H.G. Beh, "Monitoring for Pornography and Sexual Harrassment", *Communications of the ACM*, Vol.45, No.1, 2002, 84-87.

Parker, D.B., *Fighting Computer Crime*, New York : John Wiley and Sons, 1998.

Peace, A.G., D.F. Galletta, and J.Y.L. Thong, "Software Piracy in the Workplace : A Model and Empirical Test", *Journal of Management Information System,* Vol.20, No.1, 2003, 153-177.

Saari, J., "Computer Crime-Numbers Lie", *Computers and Security,* Vol.6 No.2, 1987, 111-117.

Schou, C.D. and K. Trimmer, J., "Information Assurance and Security", *Journal of Organizational and End User Computing*, Vol.16, No.3, 2004, 1-7.

Silberman, M., "Toward a Theory of Criminal Deterrence", *American Sociological Review,* Vol.41, No.3, 1976, 442-461.

Siponen, M.T., "A Conceptual Foundation for Organizational Information Security Awareness", *Information Management and Computer Security*, Vol.8, No.1, 2000, 31-41.

Solarz, A., "Computer-Related Embezzlement", *Computers and Security*, Vol.6 No.1, 1987, 49-53.

Stanton, J.M., C. Caldera, A. Issac, K.R. Stam, and S.J. Marchinlowski, "Behavioral Information Security : Defining the Criterion Space", *The Systems Assurance Institute*, Syracuse University, Syracuse, New York, 2003.

Straub, D.W., "Effective IS Security : An Empirical Study", *Information Systems Research*, Vol.1, No.3, 1990, 255-276.

Straub, D.W. and W.D. Nance, "Discovering and Disciplining Computer Abuse in Organizations : A Field Study", *MIS Quarterly*, Vol. 14, No.1, 1990, 45-60.

Straub, D.W. and R.J. Welke, "Coping with Systems Risk : Security Planning Models for Management Decision Making", *MIS Quarterly*, Vol.22, No.4, 1998, 441-469.

Tittle, C.R., *Sanctions and Social Deviance : The Question of Deterrence*, New York : Praeger, 1980.

Urbaczewski, A. and L.M. Jessup, "Does Electronic Monitoring of Employee Internet Usage Work?", *Communications of the ACM,* Vol. 45, No.1, 2002, 80-83.

Weaver, F.M. and J.S. Carroll, "Crime Perceptions in a Natural Setting by Expert and Novice Shoplifters", *Social Psychology Quar-*

terly, Vol.48, No.4, 1985, 349-359.

Whitman, M.E., A.M. Townsen, and R.J. Alberts, "Information Systems Security and the Need for Policy", In *Information security management : Global challenges in the new millenium*, edited by M. Khosrowpou, Hershey, PA : Idea Group Publishing, 2001.

Willson, R., "Understanding and Addressing Criminal Opportunity : The Application of Situational Crime Prevention to IS Security", *Journal of Financial Crime*, Vol.7, No.3, 2000, 201-210.

Wybo, M.D. and D.W. Straub, "Protecting Organizational Information Resources", *Information Resources Management Journal*, Vol.2, No.4, 1989, 1-15.

Yu, K.H., W.C. Choi, S.K. Kim, and C.Y. Goo, "A Study on Establishing Guidelines for Information Protection and Security for Educational Institutes", *Journal of the Korea Society of IT Services*, Vol.7, No.3, 23-43.

(유기훈, 최웅철, 김신곤, 구천열, "학내 정보보호 수립에 관한 연구", *한국IT서비스학회지*, 제7권, 제3호, 2008, 23-43.)

About the Authors

Joontaik Lee (securityzen@tovss.com)

Joontaik Lee is a CEO of the ToVSS Co., LTD. and a professor of the College of Industry Security Administration at ChungAng University, Seoul, Korea. He graduated from Kwangwoon University Department of Management Information Systems (MIS), where he earned his master and doctorate degree. His major research interests have been in the area of Information Security Strategy. Also, he has international standard auditor (Leader Auditor, Assessment Examination, Skill Examination of ISMS and ScyMS in Exemplar Global) qualification.

Sanghoon Kim (shk5432@gmail.com)

Sanghoon Kim is a professor of the College of Business Administration at Kwangwoon University, Seoul, Korea. He graduated from Seoul National University where he earned his BS in economics. And he received the MS and Ph.D in IS from the Korea Advanced Institute of Science and Technology (KAIST). He has published his research papers in several international journals including Information and Management, Information Processing and Management, Computer Personnel (ACM SIGCPR), Information Resources Management Journal, Journal of Organizational Computing and Electronic Commerce, Service Business, The Scientific World Journal and ect. His major research interests have been in the areas of IT strategy, change management for IT implementation, Management Innovation thru IT, IS evaluation, ERP systems implementation and S/W development project management.