정보시스템 오남용 의도에 관한 실증적 연구 : 의료기관을 대상으로

김은지* · 이준택**

요 약

최근 정보보안 사건의 상당 부분을 의료 분야에서 차지함에도 불구하고 기존의 연구는 기업 중심으로 이루어졌다. 이에 따라 본 연구는 의료기관의 조직원을 대상으로 정보시스템을 사용한 오남용 의도에 관한 연구를 수행하였다. 분석 결과, 정보보안 관리 중 보안 소프트웨어가 인지된 제재 효과에 직접적인 영향을 미치는 것으로 나타났다. 반면 보안정책, 보안 인식 프로그램, 모니터링 실시는 본 설문의 변수의 경우의 수의 부족으로 신뢰성을 확보할 수 없었으나, 보안 소프트웨어와 동등한 제재효과가 있을 것으로 판단되어 추가 분석이 필요할 것으로 나타났다.

The Empirical Study on the Misuse Intention Using Information System : Focus on Healthcare Service Sector

Kim Eun Ji* · Lee Joon Taik**

ABSTRACT

Despite the number of security incidents in healthcare sector is considerable, earlier studies have been done in business sector. We have tried to empirically analyze the misuse intention using information system for healthcare sector. As a result, the preventative security software of the information security management have positive impact on the effectiveness of sanctions. Though further analysis is needed, the security policies, security awareness program and monitoring practices are determined to have a valid impact on the effectiveness of sanctions equivalent to the preventative security software.

Key words : Information System, Misuse Intention, Healthcare Sector

접수일(2016년 8월 22일), 게재확정일(2016년 9월 19일)

* 중앙대학교 산업융합보안학과
** 중앙대학교 산업보안학과 교수(교신저자)

1. 서 론

내부자로 인한 정보자원의 오남용은 조직의 운영에 있어 심각한 문제이다. ISACA에 의하면, 2014년 기업에 대한 정보보안 사건의 40.72%가 악의가 없는 내부자로 인해 발생했으며, 28.62%가 악의적인 내부자에 의하여 발생한 것으로 나타난다[1]. 정보보안 사건은 매년 증가하는 추세이며, 그 손실 또한 매년 증가하며 조직에 큰 위협이 되고 있다. 이와 같이 정보보안 사건이 증가함에 따라 내부자에 의한 정보시스템 오남용은 조직의 지속적인 위협 요소로 존재할 것으로 추측된다.

조직의 운영에 있어 정보시스템 오남용에 대한 정보보안 관리의 수립은 지속적인 과제이며, 이와 관련한 기존의 연구는 기업 부문을 중심으로 이루어져 왔다. 그러나 2016년 ITRC의 발표에 따르면, 2015년도 미국 개인정보 유출사고 전체 중 35.5%가 의료 분야에서 일어나며, 이는 기업 부문의 40%를 뒤따르는 수치이다[2]. 국내에서 또한 의료 분야에서의 개인정보 유출이 크게 우려되고 있다. 한국인터넷진흥원(2016)에 의하면, 개인정보 유출이 우려되는 분야로 의료 분야가 28.4%를 나타내며, 이는 금융 분야의 49.5%를 뒤따른다[3]. 즉, 의료 분야에 관한 정보보안의 필요성은 국내외를 불문하고 커지고 있으며, 그에 따라 기존의 연구를 확대하여 의료 분야에 적용하는 연구가 요망되고 있다.

본 연구는 정보시스템 오남용에 영향을 미치는 요인을 도출하고, 그 요인들이 의료 기관 종사자들에게 미치는 바를 실증적으로 규명함으로써 향후 의료 분야에서 사용할 수 있는 정보시스템 오남용 관리의 근거를 마련하고자 한다.

2. 이론적 배경

2.1 정보시스템 보안의 정의

정보시스템 보안이란 광의적으로는 정보보안의 필요한 부분 집합이며, 협의적으로는 조직의 컴퓨터 사용 시스템 안에서 존재하는 운영과 정보의 보호이다. 정보보안은 인가되지 않은 사람으로부터 조직의 정보자산이 노출되지 않도록 보호하는 시스템과 과정을 모두 포함하는 의미[4]이며, 가용성, 무결성, 진정성, 기밀성 네 가지 요소를 모두 충족시켜야 한다. 따라서 본 연구는 정보 시스템 보안을 가용성, 무결성, 진정성, 기밀성 측면에서 보호하고 보존하는 행위라고 정의한다.

2.2 정보시스템 오남용

2.2.1 정보시스템 오남용의 정의

정보시스템의 오남용은 다양한 정의로 사용되고 있으며, 문헌에서는 이와 관련해 컴퓨터 오남용과 컴퓨터 범죄에 대한 정의를 주로 사용한다. Kesar & Rogerson(1998)에 따르면 컴퓨터 오남용이란 사기, 바이러스 감염, 불법 소프트웨어, 자료 도용, 프라이버시 침해와 같이 정보통신기술을 활용한 불법적인 행위들을 말한다[5]. Wasik(1991)에 의하면, 컴퓨터 오용은 컴퓨터, 프로그램, 자료에 관하여 비윤리적이거나 인가받지 않은 행위를 하는 것을 의미한다[6]. 반면 Fafinski(2013)은 컴퓨터 오용이 오로지 불법적인 행위만을 의미하지는 않는다고 강조한다[7].

이와 관련해 Straub(1986)의 컴퓨터 오용에 대한 정의는 불법적인 행위뿐만 아니라 부적절하거나 비윤리적인 행위까지 포함하고 있어 일반적으로 많이 사용되고 있다. Straub(1986)은 컴퓨터 오용이란 개인에 의해 자행되는 정보시스템 자산의 오용으로, 인가받지 않은 고의적이고 식별 가능한 것이라고 정의했다[8]. 이러한 오용은 하드웨어, 프로그램, 데이터, 컴퓨터 서비스에서의 위반 사항을 포함하며, 이에 대한 상세한 위반 사항으로는 터미널, CPU, 디스크 드라이브, 프린터와 같은 컴퓨터와 관련된 물리적 자산을 도난 혹은 훼손하는 것, 프로그램의 도난 혹은 수정, 데이터의 도용 혹은 수정, 인가되지 않은 서비스 사용 혹은 의도적인 서비스 중단 등이 있다[8].

본 연구는 조직의 정보시스템 활용 과정에 존재하는 모든 위협 요소에 대한 정보보안 관리의 근거를 마련하고자 하므로, Straub(1986)가 주장하는 정보시스템 오남용 정의를 따르고자 한다.

2.2.2 정보시스템 오남용 의도

정보시스템 오남용 의도란 오남용 행위를 실행할지

말지를 선택하는 개인의 의도이다. Ajzen(1991)에 의하면, 의도란 오남용에 대한 시도가 얼마나 어려운 지와 그 행위를 함에 있어 얼마만큼의 노력이 들어가는지에 따라 결정되는 지표이다[9]. 또한 의도란 개인이 앞으로 오남용 행위를 할 것인가에 대해 예측할 수 있게 해준다[9]. 이에 따라 본 논문에서는 제재가 이루어짐에 따라 오남용 의도가 어떻게 변화하는 지를 측정할 것이다.

2.3 제재의 확실성과 엄격성

범죄와 일탈적인 행동들을 예방하기 위한 제재의 효율성에 대한 연구는 범죄학으로부터 시작되었다. 범죄학 분야 내에서 일반억제이론(GDT, General Deterrence Theory)이라고 알려진 이 이론은 불법적인 행동을 저지르고자 하는 의욕을 꺾거나 제재를 가하는 것과 이러한 제재의 효과성에 초점이 맞춰져있다[10][11]. 일반억제이론에서 제재의 효과성은 인지된 제재의 확실성과 인지된 제재의 엄격성에 영향을 받는데, 제재의 확실성은 처벌 받을 가능성을 나타내며 제재의 엄격성은 처벌의 강도가 어떠한지를 나타낸다[10]. 제재 행위는 잠재적 범죄자들로부터 불법적 행동을 하지 못하도록 유도하며, 불법적 행위에 대한 제재가 보다 확실하고 엄격할수록 제재의 효과성이 커지게 된다. 이는 개인이 어떤 행동을 시도할 때에 그들의 보상은 극대화시키고, 비용은 최소화시키는 합리적인 방향을 선택하기 때문이다.

Straub(1986)는 규정과 규칙이 존재하는 환경 하에서 컴퓨터 오남용이 발생하기 때문에 컴퓨터 오남용에 일반억제이론이 적용될 수 있다고 주장한다[8]. Hollinger & Clark(1983)는 조직의 이익에 반하는 개인의 이상행동 연구에 일반억제이론를 적용했으며, 제재의 범위가 범죄와 법에 관련한 통제뿐만 아니라 일반적인 조직의 제재에까지 미친다고 주장했다[12]. 따라서 본 연구는 일반억제이론을 적용하여 제재의 확실성과 엄격성이 정보시스템 오남용 행동에 어떠한 영향을 미치는 지 평가하고자 한다.

2.4 정보보안 관리

정보시스템 위협을 감소시키기 위한 조직의 전략은 제재, 예방, 탐지, 회복의 네 가지로 나뉘며, 정보시스템 오남용을 감소시키기 위한 전략으로는 제재와 예방에 초점이 맞춰져 있다.

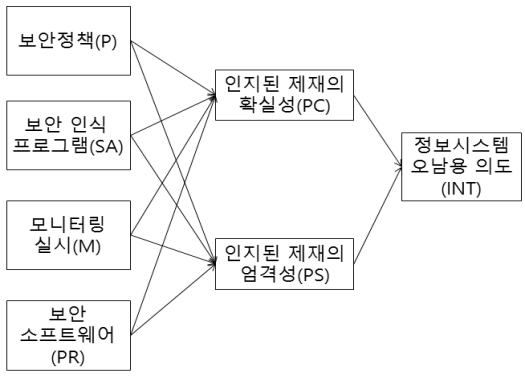
제재 대책은 소극적인 대책과 적극적인 대책으로 나눌 수 있는데, 두 대책의 주요한 목적은 정보시스템 오남용에 대한 처벌의 확실성과 엄격성을 통해 잠재적 오남용 사용자들을 막는 것이다. 소극적인 제재 대책이란 보안 정책, 보안 인식 프로그램과 같은 통제들을 통해 정보시스템의 올바른 사용과 관련된 정보와 오남용 시 처벌 내용을 제공하여 오남용 시도를 억제하는 것이다. 적극적 제재 대책이란 정보시스템 자산 사용에 대한 감사(audit)와 직원들의 컴퓨터 사용 활동 모니터링과 같은 적극적인 보안 활동을 의미한다.

예방 대책은 정보시스템 접속을 막거나 특정 정보시스템 기능의 사용 금지를 통해 정보시스템 오남용과 컴퓨터 범죄를 예방하는 정보보안 관리를 의미한다[8]. 예방 대책의 주된 목적은 불법적인 행동들을 막기 위한 정책과 가이드라인의 시행을 돕는 것이다.

정보시스템 오남용 제재 및 예방의 방법으로는 절차적이고 기술적인 통제들, 즉, 보안정책, 보안 인식 프로그램, 모니터링 실시, 보안 소프트웨어를 사용할 수 있다[13]. 따라서 본 논문에서는 정보보안 관리에 대한 변수로서 보안정책, 보안 인식 프로그램, 모니터링 실시, 보안 소프트웨어를 사용하고자 한다.

3. 연구 모형 및 가설

3.1 연구 모형



(그림 1) 연구 모형

본 연구는 앞서 살펴본 선행연구를 바탕으로 정보보안 관리들이 정보시스템 오남용과 연관된 처벌의 인지도를 증가시키고 그에 따라 정보시스템 오남용 의도에 어떤 영향을 미치는지 분석하기 위한 연구 모형을 (그림 1)과 같이 수립하였다.

3.2 연구가설

3.2.1 정보보안 관리와 인지된 제재의 확실성 및 엄격성과의 관계

보안정책이란 일반적으로 조직의 정보시스템 자원의 사용이 어떠한 경우 적절한지 혹은 적절하지 못한지를 상세히 설명한 가이드라인으로서, 사용자와 관리자가 정보시스템을 안전하고 책임감 있게 사용하도록 하는 자세한 내용을 제공해야 한다.

보안정책들의 주된 목적은 불법적인 행동이나 받아들일 수 없는 행동을 명확하게 정의하고 처벌 위협의 인지를 증가시킴으로써 정보시스템 오남용을 억제하는 것이다[14]. 정책을 명확하게 정의하는 것은 효과적인 제재를 실행하기 위한 전제조건이며, 정책이 상세하게 기술될수록 부적절한 시스템 사용에 대한 제재 효과는 더 커진다. 또한 컴퓨터 이용 정책 인지가 높을수록 정보시스템 오남용에 부정적인 인식을 지니게 되므로 보안 정책과 처벌 인식 사이에는 긍정적인 영향관계가 존재한다. 따라서 보안 정책이 인지된 제재의 확실성과 엄격성에 영향을 미친다는 가설을 설정할 수 있다.

가설1-1: 보안 정책은 인지된 제재의 확실성에 긍정적으로 영향을 미친다.

가설1-2: 보안 정책은 인지된 제재의 엄격성에 긍정적으로 영향을 미친다.

보안 정책들과 절차들은 직원들이 그것들이 필요한 예방책임을 이해하고 받아들일 때에만 효과적이다. 그러므로 정보시스템 오남용을 효과적으로 통제하기 위해서는 보안 인식 프로그램이 필요하다[13]. 보안 인식 프로그램은 오남용의 결과와 자신의 책임을 이행하는데 필요한 능력들을 제공함으로써 직원들이 조직의 정보 자원에 대한 책임감을 인지하도록 독려하는 데 초점이 맞춰져있다[15].

보안 인식 프로그램의 주된 목표는 회사가 시스템을 보호하는 것을 중요시하고 의도적인 보안 위반들을 가볍게 다루지 않을 것이라는 인식을 잠재적인 오남용자들에게 심어주기 위한 것이다. 그러므로 보안 인식 프로그램이 인지된 제재의 확실성과 엄격성에 영향을 미친다는 가설을 도출할 수 있다.

가설2-1: 보안 인식 프로그램은 인지된 제재의 확실성에 긍정적으로 영향을 미친다.

가설2-2: 보안 인식 프로그램은 인지된 제재의 엄격성에 긍정적으로 영향을 미친다.

보안 제재 대책은 직원들의 컴퓨터 사용 활동을 감시 감독 하는 등 적극적인 보안 노력을 포함한다. 보안 모니터링은 직원들의 컴퓨터 사용 활동을 감시하고 기록하기 위해 전자적인 도구를 사용한다.

적극적인 보안 활동은 곧 오남용 행동에 대한 위협을 증가시키며, 결과적으로 정보시스템 오남용을 줄일 수 있다[16]. 직원들의 컴퓨터 사용 활동을 감시하는 것이 조직의 정보시스템 오남용 색출을 증가시키는 적극적인 정보보안 관리임을 고려하면, 잠재적 오남용자들이 그들의 컴퓨터 사용 활동이 감시되고 있다는 것을 안다고 가정했을 때 모니터링은 정보시스템 오남용에 대한 처벌과 위협의 인지를 상승시킬 것이라고 예상된다. 따라서 모니터링 실시가 인지된 제재의 확실성과 엄격성에 영향을 미친다는 가설을 수립할 수 있다.

가설3-1: 모니터링 실시는 인지된 제재의 확실성에 긍정적으로 영향을 미친다.

가설3-2: 모니터링 실시는 인지된 제재의 엄격성에 긍정적으로 영향을 미친다.

연구자들은 보안정책, 보안 인식 프로그램, 모니터링 실시와 같은 활동 외에도 보안 기술을 통해 정보시스템 오남용을 예방하기를 제안했다[13]. 보안 기술들은 부적절한 내용이 담긴 e-mail 메시지들을 차단하는 소프트웨어와 같이 정보시스템 오남용을 금지하는 소프트웨어를 포함하며, 이외에도 시스템 사용자의 신분을 인증하는 방법을 사용함으로써 부적절한 사용자로

부터 정보 시스템이 접근, 파괴, 오남용되는 것을 보호하는 소프트웨어 프로그램도 포함한다[17].

보안 기술의 사용은 오남용이 발견될 것이라는 공포를 증가시킨다[14]. 잠재적인 오남용자들이 보안 소프트웨어의 존재를 인식하면 처벌의 위협이 증가하여 컴퓨터 오남용 의도가 하락할 것으로 판단된다. 따라서 보안 소프트웨어는 인지된 제재의 확실성과 엄격성에 영향을 미친다는 가설을 설정할 수 있다.

가설4-1: 보안 소프트웨어는 인지된 제재의 확실성에 긍정적으로 영향을 미친다.

가설4-2: 보안 소프트웨어는 인지된 제재의 엄격성에 긍정적으로 영향을 미친다.

3.2.2 인지된 제재의 확실성 및 엄격성과 정보시스템 오남용 의도와의 관계

일반억제이론을 통해 제재 활동은 제재의 확실성과 제재의 엄격성으로 구성되어 영향을 미친다는 것을 알 수 있다. Nagin(1978)에 의하면 제재의 확실성은 처벌받을 가능성을 나타내며 제재의 엄격성은 처벌의 정도를 나타낸다[10]. 최근의 연구에서 이 두 요소는 정보시스템 오남용에 관련된 처벌의 정도와 가능성에 대한 인식을 가늠하는 데 사용되므로, 본 논문에서도 이 두 가지 개념을 사용하고자 한다.

제재의 확실성과 엄격성은 증가할수록 범죄나 부적절한 행위에 부정적 영향을 미친다. Skinner & Fream(1997)은 불법 행위가 밝혀지는 것과, 그에 따른 처벌을 인지하는 것이 다른 학생들의 컴퓨터 계정에 불법적으로 접근하려는 의도를 가진 대학생들에게 부정적인 영향을 미친다는 것을 발견했다[18]. 그러므로 인지된 제재의 확실성과 엄격성이 정보시스템 오남용 의도에 영향을 미친다는 가설을 도출할 수 있다.

가설5: 인지된 제재의 확실성은 정보시스템 오남용 의도에 부정적인 영향을 미친다.

가설6: 인지된 제재의 엄격성은 정보시스템 오남용 의도에 부정적인 영향을 미친다.

4. 연구 분석 및 결과

4.1 설문의 구성 및 표본의 특성

4.1.1 설문지의 구성

본 연구는 실증분석을 위하여 설문조사 방식을 택하여 구성하였다. 설문은 민감한 사항에 대한 질문들이 응답자에게 위협이 되거나 강압적으로 받아들여지지 않도록 작성하였다. 분석 결과는 설문에 대한 내적 타당성을 증가하도록 하였다.

본 연구에 포함된 설문항목은 기존 연구들[8][19]의 이론을 바탕으로 설문지를 작성하였다. 인지된 제재의 확실성(PC), 인지된 제재의 엄격성(PS), 정보시스템 오남용 의도(INT)는 리커트 척도(7점)로 측정하고 측정항목 값의 합을 이용하였다.

정보보안 관리 존재 여부에 대한 문항은 보안정책(P) 문항, 보안 인식 프로그램(SA) 문항, 모니터링 실시(M) 문항, 보안 소프트웨어(PR)는 문항으로 총 26개 항목으로 구성하여 정보보안 관리의 각 변수를 측정하였다.

4.1.2 자료 수집 및 표본 특성

본 연구의 설문조사는 의료 기관 종사자들을 대상으로 인터넷 설문을 진행하였으며, 의료 기관 내 정보시스템 업무 담당자뿐만 아니라 업무환경에서 컴퓨터를 사용하는 모든 직원들을 조사 대상으로 하였다. 총 198명의 유효한 설문 응답 결과가 분석에 사용되었으며 표본의 인구통계학적 특성은 <표 1>과 같다.

<표 1> 응답자의 인구통계학적 특성

항목	내용	빈도	비율(%)
성별	남성	96	48.5
	여성	102	51.5
연령	24세 이하	6	3.0
	25세~34세	76	38.4
	35세~44세	69	34.8
	45세~54세	43	21.7
	55세 이상	4	2.0
세부기관	대학병원	58	29.3
	종합병원	60	30.3
	의원	29	14.6
	기타	51	25.8
전체		198	100

즉, 전체 응답자 중 남성은 96명(48.5%), 여성은 102명(51.5%)였으며, 응답자의 연령은 24~44세가 145명(73.2%)로 가장 많고 45세 이상의 응답자도 47명(23.7%)로 연령대가 고루 분포된 응답 결과가 도출되었다. 또한 응답자가 근무하는 세부 기관을 살펴보면, 종합병원이 60명(30.3%)로 가장 많았고 대학병원 58명(29.3%), 의원 29명(14.6%) 등 세부기관이 다양하게 분포되어 있는 것으로 나타났다.

4.2 측정항목의 분석

연구 모형에 대한 통계적 분석은 SPSS 18.0과 smartPLS 2.0을 사용하여 분석 절차를 거쳤다. 본 연구는 가설 검증에 앞서 연구모형 변수의 신뢰성 및 타당성 분석을 위해 탐색적 요인분석(exploratory factor analysis)을 시행하였다. 이후 smartPLS 2.0을 사용해 측정모형을 분석하여 수렴타당도와 판별타당도를 검증하고, 가설검증을 위해 PLS로 구조모형을 분석하였다. 본 연구에서 PLS 기법을 선택한 이유는 Chin(1998)에 따르면 PLS는 표본 크기와 잔차 분포에 대한 요구사항이 적으며, 분석 데이터의 정규성을 전제로 하지 않거나 비교적 표본의 수가 적을 때에도 유용하기 때문이다[20].

<표 2> 측정항목의 타당성과 신뢰성

변수	측정항목	요인적재량	AVE	CR	Cronbach's α
INT	INT1	0.888	0.758	0.861	0.724
	INT2	0.874			
PC	PC1	0.891	0.800	0.889	0.762
	PC2	0.778			
PS	PS1	0.896	0.877	0.934	0.861
	PS2	0.882			
PR	PR2	0.584	0.698	0.873	0.785
	PR3	0.798			
	PR4	0.756			
M	M3	0.641	0.395	0.064	0.368
	M6	0.558			
P	P3	0.700	0.248	0.266	0.738
	P5	0.681			
	P6	0.529			
SA	SA4	0.709	0.532	0.644	0.664
	SA6	0.741			

탐색적 요인분석 실시결과와 PLS 분석에 의한 검증결과로서 나타난 변수별 측정지표에 대한 신뢰성 검증 결과는 <표 2>와 같다. 일반적으로 요인 적재량은 0.5 이상이면 집중타당성이 있다고 평가되기 때문에, 당초에 포함된 일부 측정지표 중 0.5를 넘지 못하거나 두 가지 요인을 반영하는 것은 제외되었다. Chin(1998)에 따르면 측정항목의 타당성과 신뢰도는 요인 적재량, 평균분산추출(AVE)과 합성신뢰도(Composite Reliability)로 평가된다[20]. 평균분산추출은 0.5가 기준으로 그 이상이면 집중타당성이 있으며, 합성신뢰도는 0.7을 기준으로 하여 내적일관성과 집중타당성이 확보된다[21]. 본 논문은 <표 2>에 의해 크론바하 α(cronbach's α) 계수값이 0.6 미만이며, 평균분산추출, 합성신뢰도 또한 기준 미만인 모니터링 실시 변수와 크론바하 α 값은 기준 이상이지만 평균분산추출이나 합성신뢰도 기준 미달인 보안 정책, 보안 인식 프로그램 변수를 제외하고 구조모형을 분석하였다.

변수별 판별타당성을 확인하기 위해서는 각 연구변수와 다른 변수들과의 상관계수가 해당 변수의 평균분산추출의 제곱근 값보다 작아야 한다[21]. 또한에 의하면 판별타당성을 확인하기 위한 추가적인 판단기준으로 다중상관성(multi-collinearity) 검증이 있으며, 검증결과 변수 간 상관계수가 0.9보다 크면 다중상관성이 심각하다고 판단할 수 있다. <표 3>에서 보면 변수 간 상관계수들 중 인지된 제재의 확실성(PC)과 인지된 제재의 엄격성(PS) 간의 상관계수가 0.789로 나타났으나 다중상관성의 기준이 되는 0.9보다 낮기 때문에 다중상관성 측면에서 변수들 간의 판별타당성이 확보된다고 볼 수 있다.

<표 3> 연구 변수의 판별타당성

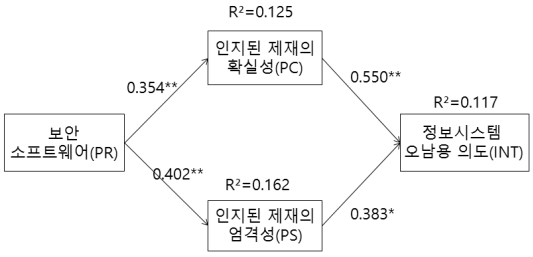
	INT	PC	PR	PS
INT	**0.871**			
PC	-0.248	**0.894**		
PR	0.069	0.354	**0.835**	
PS	-0.054	0.789	0.403	**0.936**

Note: 대각선에 존재하는 값(굵은 표시)은 각 개념에 대한 평균분산추출(AVE) 값의 제곱근 값임

4.3 가설검증 및 결과

PLS는 경로계수의 유의성을 확인하기 위해 부트스트래핑 방법을 이용하여 표본을 재추출하며 이를 통해 확보된 유사 데이터 군을 통계 분석에 사용한다. 기존의 정보시스템에 관한 연구들에서는 일반적으로 500개의 리샘플을 사용하므로, 본 연구에서는 500개의 리샘플을 생성하여 경로계수에 대한 통계적 유의성을 검증하였다. 그 결과는 (그림 2)와 같이 요약된다. PLS에서 가설은 구조모형을 통해 실험되는데, 이를 위해 경로계수와 R^2값이 지표로 사용된다[20]. 경로계수는 독립변수와 종속변수 간 관계의 강도를 나타내며, R^2는 독립변수에 의해 설명되는 분산의 양을 의미한다.

(그림 2)를 살펴보면, 구조모형에서 인지된 제재의 확실성에 대한 분산은 12.5%가 설명되며, 인지된 제재의 엄격성에 대한 분산은 16.2%, 그리고 정보시스템 오남용 의도에 대한 분산은 11.7%가 설명된다. R^2 값의 일반적인 기준치는 0.1로, 모든 종속변수의 R^2 값이 기준치보다 높기 때문에 본 측정모형은 적합하다고 할 수 있다.



(그림 2) 가설 검증 결과

Note: * p<0.005, ** p<0.001

본 연구의 가설을 검증한 결과, <표 4>와 같이 보안 소프트웨어가 인지된 제재의 확실성과 인지된 제재의 엄격성에 유의한 영향을 미치는 것으로 나타났으며, 인지된 제재의 확실성과 인지된 제재의 엄격성이 정보시스템 오남용 의도에 유의한 영향을 미치는 것으로 확인되었다.

<표 4> 가설 검증 결과 요약

가설	경로계수	유의수준	결과
PR→PC	0.354	5.055**	채택
PR→PS	0.402	6.281**	채택
PC→INT	0.550	5.663**	채택
PS→INT	0.383	3.050*	채택

Note: * p<0.005, ** p<0.001 (양측검정 기준)

5. 결 론

기존의 연구들은 정보보안 사건으로 가장 큰 위협을 받고 있는 기업을 중심으로 하여 연구를 진행해왔다. 그러나 최근 연구에 의하면, 증가하는 정보보안 사건의 상당 부분을 의료 보안이 차지하며 이를 관리하기 위한 연구의 필요성이 높아지고 있다.

이에 따라 본 연구에서는 의료 기관에 종사하는 조직원들을 대상으로 하여 정보시스템을 사용한 오남용 의도에 관해 연구를 수행하였다.

정보시스템의 변수로 보안정책, 보안 인식 프로그램, 모니터링 실시, 보안 소프트웨어가 인지된 제재 효과에 미치는 영향을 살펴본 결과, 보안 소프트웨어가 인지된 제재 효과에 직접적인 영향을 미치고 있는 것으로 나타났다. 즉, 정보보안 사건을 예방하기 위하여 보안 소프트웨어를 사용하는 것은 의료 기관 종사자가 지닌 정보관리시스템을 사용한 오남용 의도를 명확히 줄일 수 있는 방책임을 시사하는 것이라 할 수 있다. 반면, 보안정책, 보안 인식 프로그램, 모니터링 실시 또한 보안 소프트웨어와 동등한 제재효과가 있을 것으로 판단되나 본 설문의 변수의 경우의 수의 부족으로 신뢰성을 확보할 수 없었다. 향후 연구에서는 이를 보완하여 추가 연구가 필요할 것으로 판단된다.

의료기관 종사자가 제재를 인식한 효과에 대해 분석한 결과, 제재를 확실히 인식할수록 정보시스템 오남용 의도에 유의한 영향을 미치는 것으로 나타났다. 즉, 정보보안 관리의 효과성을 높인다면 정보시스템 오남용 의도를 확연히 줄일 수 있음을 의미한다.

본 연구에서는 기존의 연구를 통해 기업의 측정변수를 고려하여 측정 및 반영함으로 인해 의료기관에

적합한 측정 변수들을 모두 포함하지 못했다는 점에서 연구의 한계점이 있으며, 변수들을 재검토할 필요가 있다. 또한 향후 연구에서는 이러한 한계를 보완하여 기업 부문과 의료 부문의 비교연구를 고려해볼 수 있을 것이다.

참고문헌

[1] ISACA, 'State of Cybersecurity:Implications for 2015', 보도자료, 2015.

[2] ITRC, 'Data Breaches Reports 2015', 2015.

[3] 한국인터넷진흥원, '2016 인터넷 및 정보보호 10대 이슈 전망', 2015.

[4] Hill, L. B. and Pemberton, J. M, "Information security: An overview and resource guide for inf.", Information Management, Vol.29, No.1, pp.14-24, 1995.

[5] Kesar, S. and S. Rogerson. "Developing ethical practices to minimize computer misuse", Social science computer review, Vol.16, No.3, pp.240-251, 1998.

[6] Wasik, M. 'Crime and the Computer', Oxford: Clarendon Press, 1991.

[7] Fafinski, S. 'Computer Misuse: Response, regulation and the law', Routledge, 2013.

[8] Straub, D. W. 'Deterring computer abuse: The effectiveness of deterrent countermeasures in the computer security environment', Diss, 1989.

[9] Ajzen, I. "The theory of planned behavior", Organizational behavior and human decision processes, Vol.50, No.2 pp.179-211, 1991.

[10] Nagin, D. "Crime rates, sanction levels, and constraints on prison population", Law and Society Review, pp.341-366, 1978.

[11] Tittle, C. R. 'Sanctions and social deviance: The question of deterrence', Praeger, 1980.

[12] Hollinger, R. C., and John P. C. "Deterrence in the workplace: Perceived certainty, perceived severity, and employee theft", Social forces, Vol.62 No.2 pp.398-418, 1983.

[13] Dhillon, G. "Managing and controlling computer misuse", Information Management & Computer Security, Vol.7 No.4 pp.171-175, 1999.

[14] Lee, J. and Y. Lee. "A holistic model of computer abuse within organizations", Information management&computer security, Vol.10 No.2 pp.57-63, 2002.

[15] Wybo, M. D. and D. W. Straub Jr. "Protecting organizational information resources", Information Resources Management Journal, Vol.2 No.4 pp.1-16, 1989.

[16] Kankanhalli, A. et al. "An integrative study of information systems security effectiveness", International journal of information management, Vol.23 No.2 pp.139-154, 2003.

[17] Irakleous, I. et al. "An experimental comparison of secret-based user authentication technologies", Information Management&Computer Security, Vol.10 No.3 pp.100-108, 2002.

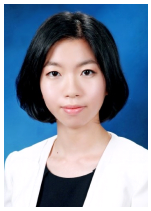
[18] Skinner, W. F. and A. M. Fream, "A social learning theory analysis of computer crime among college students". Journal of research in crime and delinquency, Vol.34 No.4 pp.495-518, 1997.

[19] Stanton, J. et al. "Behavioral information security: two end user survey studies of motivation and security practices", AMCIS 2004 Proceedings, 2004.

[20] Chin, W. W. "The partial least squares approach to structural equation modeling", Modern methods for business research, Vol.295 No.2 pp.295-336, 1998.

[21] Gefen, D, D. Straub, and Marie-Claude B. "Structural equation modeling and regression: Guidelines for research practice", Communications of the association for information systems, Vol.4 No.1, 2000.

[저 자 소 개]



김 은 지 (Eun-Ji Kim)

2015년 2월 숙명여자대학교 수학과 졸업
2015년 3월~ 중앙대학교 일반대학원 산업융합보안학과 석사과정

email : eunjik43@gmail.com

이 준 택 (Joon-taik Lee)

2008년 2월 용인대학교 전산통계학 학사
2010년 2월 성균관대학교 일반대학원 이동통신공학 전공 석사
2013년 2월 광운대학교 일반대학원 경영정보시스템 전공 박사
현 재 중앙대학교 산업보안학과 교수

email : securityzen@cau.ac.kr