처벌과 윤리교육이 정보보안준수에 미치는 영향: 조직유형의 조절효과를 중심으로

Impacts of Punishment and Ethics Training on Information Security Compliance: Focus on the Moderating Role of Organizational Type

안 중 호 (Joongho Ahn)	서울대학교 경영대학 교수, 제1저자
박 준 형 (Junhyung Park)	대한민국 육군 3사관학교 교수
성 기 문 (Kimoon Sung)	대한민국 공군본부, 교신저자
이 재 홍 (Jaehong Lee)	서울대학교 경영대학 박사과정

요 약

정보기술이 조직에게 다양한 혜택을 제공하고 있지만, 컴퓨터 바이러스, 해킹, 무단복제, 도용 등 정보보안 사고로 인해 조직에게 치명적인 피해를 주는 경우도 있다. 정보보안 사고의 원인은 정보보안 통제를 지키지 않고 이를 위반하는 개인의 행위와 밀접하게 관련되어 있다. 따라서 개인의 행위에 대한 자발적 통제를 이끌어내고 이를 감독하는 것이 정보보안을 유지하는데 있어서 근본적이고 핵심적인 해결책이 될 수 있다. 본 연구의 목적은 처벌과 윤리교육이 각 조직 구성원들이 정보보안정책을 준수하는데 있어서 어느 정도 효과가 있는지를 분석하고, 조직 구성원들이 조직유형에 따라 성향의 차이가 있는지를 파악하여, 조직 구성원의 행위 변화와 자기통제를 이끌어내는 방법을 찾고자 하는 것이다. 연구결과 조직유형에 관계없이 처벌과 윤리교육이 정보보안준수에 긍정적 영향을 주는 핵심 요인임을 확인하였다. 또 단일형태 조직 구성원에 비해 다분할 형태 조직 구성원이 처벌에 대한 인식이 높은 반면 윤리교육에 대한 인식은 상대적으로 낮고, 공공조직 구성원이 민간조직 구성원보다 처벌에 대한 인식이 높은 반면 윤리교육에 대한 인식은 낮은 것으로 파악되었다. 결론적으로, 처벌과 윤리교육이 조직의 정보보안준수에 영향을 주는 주요요인이며, 정보보안정책의 수립과 시행은 조직형태 및 특성을 이해하고 추진해야 함을 암시하고 있다. 따라서 조직은 정보보안정책의 수립 시 조직형태 및 특성에 따른 구성원의 성향을 먼저 인식하고, 구성원의 성향 차이를 정보보안정책에 반영한다면 정보보안정책을 수립하는데 있어서 더 큰 효과를 거둘 수 있을 것이다.

키워드 : 정보보안, 억제이론, 정보보안정책, 정보보안준수, 조직유형

† 본 연구는 논문은 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 육성·지원사업의 지원을 받아 연구되었음(NIPA-2010-C1090-1031-0002).

Ⅰ. 서 론

인간의 필요에 의해서 개발된 정보기술은 풍부한 확장성과 응용력으로 우리생활에 깊숙이 자리 잡았을 뿐 아니라, 사회전반에 폭넓게 응용되고 있다. 하지만 이러한 긍정적인 측면의 이면에는 컴퓨터 바이러스, 해킹, 무단복제 및 도용 등의 심각한 문제가 야기되고 있다. 따라서 정보보안에 대한 문제는 최근 정보기술 연구분야에서 중요한 연구주제 중 하나이다(Calluzzo and Cante, 2004).

정보보안 침해나 위반은 해킹, 정보도용, 소프트웨어 불법 복제행위와 같은 다양한 종류의 정보기술과 깊은 연관이 있다고 알려져 왔다(Harrington, 1997 Harrington, 1996). 그래서, 초기에는 보안사고를 예방하기 위하여 보안프로그램(Anti-Virus Software)과 같은 기술적 수단이나 출입통제, CCTV 등으로 사용자를 통제하는 물리적 수단으로 대응해 왔다. 이러한 이유 때문에 기존의 연구들은 보안 시스템을 위한 각종 기술의 제안이 주를 이루었다. 그러나 정보보안 문제의 또 다른 원인들은 정보보안의 통제를 지키지 않고 이를 위반하는 인간의 의지와 행위에 기초하고 있다(Sasse, 2004). 보안을 강화하면 사용상의 불편이 증가하게 되는 상충관계에 있으며, 기술적, 물리적 보안이 갖는 한계점을 인식하고 관리적 보안이 병행되어야만 한다. 정보보안정책의 수립을 위해서는 조직의 특성과 목적에 맞도록 조직 수준의 관점에서 고려해야 하며, 예외적인 상황에 대비하기 위한 사용자의 노력도 포함되어야 하는 것이다.

지금까지 정보기술분야에서 정보보안과 관련된 다양한 연구가 이루어져 왔지만, 보안규정의 수립이나 제재의 효과 등과 같은 정책에 대한 연구는 많지 않다. 기술적, 물리적 측면만을 고려하는 기존의 통제방법이나 단순한 개인적 성향에 중점을 둔 보안대책은 현대 조직사회의 보안정책을 구현하는 데 있어서 많은 어려움을 야기 시키고 있으며 이에 대한 효과적인 대책수립도 쉽지 않다. 특히, 개인의 차원이 아니라 조직차원에서 접근하여 조직의 특성을 고려한 정보보안정책에 대한 연구는 거의 이루어지지 않았다. 따라서 조직의 특성 및 구성원의 성향을 고려하여 가장 효과적이고 적절한 정보보안정책을 수립함으로써 근원적인 보안 문제를 예방하는 것이 중요하다.

억제이론(Deterrence Theory)에 따르면, 인간의 부적절한 행위를 예방하기 위해 인간의 행동에 영향을 주는 효과적인 요인으로는 인간의 두려움을 기초로 하는 제재적 억제방법인 '처벌(Punishment)'과 인간의 양심 및 자기통제 능력을 근간으로 하는 발전적 억제방법인 '윤리교육(Ethics Training)'이 있다(Workman and Gathegi, 2006). 이에 따라, 본 연구는 정보보안 예방방법으로서 조직유형에 따라 윤리교육과 처벌이 각 조직 구성원의 인식에 어떤 영향을 미치고 어떤 요소가 더 큰 영향력을 발휘할 것인가에 대해 알아봄으로써 정보보안 침해에 대한 문제를 분석해 보고자 한다.

본 연구의 목적은 기존의 기술적, 물리적 접근 방식에서 벗어나 정보보안준수를 향상시킬 수 있는 관리적 요인이 무엇인지 찾고, 조직형태와 특성을 기준으로 조직간의 차이에 따른 정보보안대책을 제안함으로써 보다 근본적으로 개인의 행위변화와 자기통제를 이끌어내는 방법을 제안하고자 하는 것이다.

연구목적 달성을 위해 본 연구는 첫째, '조직형태 및 조직특성의 차이에 따라 구성원들의 성향의 차이가 존재하는가?' 둘째, '다양한 특성과 목적을 가진 조직들이 정보보안정책을 수립하는데 있어서 동일한 방법으로 접근해야 할 것인가?' 셋째, '조직 유형에 따른 각 조직 구성원들이 정보보안정책을 준수하는데 있어서 처벌과 윤리교육을 통한 예방방법 중 어떤 요인이 더 효과적으로 사용될 수 있는가?'에 대한 답을 제안하고자 한다.

본 연구는 재 Ⅱ장에서 정보보안과 정보보안 정책의 필요성 및 인간의 행위를 통제하기 위한 방법으로 억제이론을 고찰하고, 조직형태 및 특성을 기준으로 조직을 분류한다. 제 Ⅲ장에서는 정보보안준수 분석을 위한 연구모형 및 가설을 제안하고, 제 Ⅳ장에서는 연구도구 개발, 자료수집, 설문대상집단 선정 등의 내용을 설명한다. 제 Ⅴ장은 연구도구에 대한 신뢰성과 타당성 검증 및 회귀분석과 변량분석을 통한 가설검증을 실시하고, 제 Ⅵ장에서는 본 연구성과를 설명하며, 끝으로 연구결론 및 향후 연구과제를 제안한다.

Ⅱ. 이론적 배경

2.1 정보보안

정보보안이란 비밀유지가 필요한 주요정보를 정보관련 제반사고로부터 보호하는 것을 말한다(하영길, 2004). 이에 대해, 정보보안정책은 조직의 관리자가 조직의 목적에 부합된 정보보안 프로그램을 생성하기 위해 규정과 지침을 만들고 이에 대한 책임을 할당하는 것을 말한다(NIST, 2007).

결국 정보보안정책은 조직의 중요정보를 어떻게 관리하고, 보호하며, 배포하는가에 관한일련의 규칙과 실무지침을 규정해 놓은 것이다. 정보보안정책을 수립함으로써, 사용자 스스로 정보에 대한 부적절한 활용을 통제하여 보안을 강화하도록 하며, 정보침해의 차단 및 재발 가능성을 억제할 수 있도록 해준다.

정보보안의 중요성이 강조되면서 관련 연구가 많이 이루어지고 있지만 컴퓨터 바이러스나 정보침해에 대비하는 기술적 측면을 주로 연구해 왔다(김미희, 채기준, 2007). 기술이 정보보안 유지를 위한 중요한 대책 중 하나지만, 최근에는 보다 근본적인 대책의 필요성이 대두되면서 정보보안정책과 관련한 연구가 점차 늘고 있다.

정보보안정책에 대한 연구는 여러 방향에서 접근되어 왔는데 첫째는 보안정책 관리를 위한 보안 모델의 설계에 대한 연구이다(황윤철, 2001). 둘째는 보안통제와 정책이 보안효과 및 보안체계에 미치는 영향에 대한 연구이다(김종기 외, 2006; 백승훈 외, 2005). 이러한 연구들은 정보보안 체계가 물리적, 논리적, 환경적 측면에서 여러 가지 취약점이 있으며, 기업이나 공공기관과 같은 조직에서 보안을 설계하기 위해서는 기본적인 부분인 정보보안정책이 확고하게 다져져야 한다고 강조하였다. 마지막으로 보안정책의 설계에 있어서 개별적인 사용자 특성 분석에 대한 연구이다(Workman and Gathegi, 2006).

정보보안효과에 대한 연구는 다음과 같이 다양한 연구가 이루어져 왔다. 먼저, 조직에서 정보시스템의 기능을 통해 업무의 생산성과 효율성을 제공하고, 조직 내 핵심 보안자원에 대한 적극적인 투자는 보안효과의 극대화로 직결되며, 이는 결국 조직의 성과 향상으로 이어진다는 것을 주목해야 한다(Hoffer and Straub, 1989). Straub (1990)는 정보시스템 사용자의 관심을 정보보안준수에 있어서 중요한 요소로 보았으며, 보안대책의 만족도는 과업특성, 정보시스템 환경, 사용자의 개인적 특성에 영향을 받는 것으로 설명하였다. 특히, 정보시스템에 대한사용자의 보안인지와 지식이 조직의 적절한 보안대책을 선정하는데 중요한 영향을 미치는 것으로 평가하였다. Workman and Gathegi(2006)은 사용자의 관심과 자기 억제를 통한 정보보안 위반행위 방지를 정보보안준수의 중요한 요소로 보고 사용자의 개인특성에 따라 정보보안효과가 다르게 미치는 영향을 측정하였다.

2.2 억제이론

억제이론은 공격적 행위를 일으키는 동기를 유발시키면서 이를 통제해야 하는 군대 조직에서 파생되었다(Workman and Gathegi, 2006). 억제 이론에 따르면 사람들은 예상되는 개인적 이익에 대해 합리적 계산에 기초하여 범죄를 저지

르며, 법적 처벌의 두려움은 사람들의 범죄 동기를 자제시킨다(Scholtz, 1997). 억제이론을 바탕으로 다양한 조직에서 정보보안 위반자에 대해 벌금징수, 징계 등을 통해 처벌을 시행하였다(Theoharidou *et al.*, 2005; Scholtz, 1997; Straub, 1990; Hoffer and Straub, 1989). 처벌에 바탕을 둔 억제모델이 일부 성공적이었지만, 인간의 정보보안 위반 이유에 대한 잠재요인들이 잘 이해되지 않음으로써 그 성공은 다소 제한적이었다(Wenzel, 2004).

한편 도덕적인 토대를 근본으로 한 상황적 윤리교육이 인간의 잘못된 행동을 완화하는데 있어서 효과적인 모델로 제안되고 있다(Harrington, 1997; Harrington, 1996; Kurland, 1995). 윤리교육 억제모델은 보안정책 분야에서 폭넓게 적용되어 왔으며(SANS, 2005), 모델에 대한 다양한 사례연구를 통해 윤리교육이 특정 조건과 조직환경에서 효과가 있음을 확인하였다(Hsu and Kuo, 2003; Costa and Kallick, 1997; Kurland, 1995). 그러나 윤리교육 토대의 억제 모델은 직관적인 설득에 의존함으로써 실용적 측면에서 다소 비효율적이기 때문에 정보보안 위반 관련 문제해결에 한계가 있다(Calluzzo and Cante, 2004; Simpson *et al.*, 1994).

억제이론의 두 가지 모델은 상황과 특정조건에 따라 정보보안정책 분야에서 폭넓게 적용되어 왔다. Ajzen(1985)은 서로 연관이 없는 상이한 여러 일들을 설명할 수 있도록 개별인간의 태도를 설명해 주는 계획된 행위이론을 기초로 통합적 억제 모델을 제안하였다. Lee and Lee(2002)는 억제 이론을 통해 정보보안문제가 개인의 컴퓨터 남용에 있다고 보고 연구를 수행하였다. Straub (1990)는 관리자가 사용자에게 정보시스템의 사용에 있어서 허용되지 않는 행위에 대해 사용자들에게 공지하고, 부적절한 정보시스템 오남용에 대해서 벌칙을 부여할 경우 사고발생의 횟수, 기회비용 손실 등을 줄일 수 있음을 실증하였다.

이와 같이 억제에 대한 두 가지 태도를 처벌과 같은 제재적 태도와 윤리교육을 통한 발전적 태도로 설명할 수 있다. 두 가지 상이한 요인들이 조직 구성원들이 조직의 정보보안정책과 규정을 이해하고 행동으로 따르는 데 있어서 주요한 원인이 될 수 있다. 따라서 본 연구에서는 처벌을 통한 제재적 억제와 윤리교육에 따른 발전적 억제를 정보보안준수를 이끌어내는 중요한 차별적 요소로 보고 정보보안준수를 설명하기 위해 억제 이론을 중심이론으로 활용한다.

2.3 개인의 태도

정보보안에 대한 개인의 태도는 보안과 관련된 인간의 행위에 큰 영향을 끼칠 수 있다(Rahim *et al.*, 2001). 법의 기능 중 하나는 범죄를 억제하고 예방하는 것이다. 그래서 법은 컴퓨터 프로그래머의 부정행위를 막는 것과 같은 정보보안에 있어서 효과적인 수단이 될 수 있다(Straub and Welke, 1998; Straub, 1990; Straub and Nance, 1990). 법과 대중의 태도 및 행동과의 관계에서 2가지 견해가 있다(Aubert, 1969). 하나는 법이 정의와 도덕의 사회 정서를 투영해야 한다고 보는 것이고, 다른 하나는 법이 그러한 정서를 만들고 사회 변화를 야기한다고 보는 견해이다.

Tapp and Kohlberg(1977)는 사람들의 법에 대한 순응의 다양성을 도덕적 단계들의 구조적 분류로 나누어 설명하였다. 합리적이고 실용주의적인 특성의 사람들은 부정적인 결과나 처벌을 피하기 위해 규정을 따르려는 경향이 높고, 사회적인 지각을 중요하게 생각하는 사람들은 사회적 책임감으로서 규정을 따르려는 경향이 높다. 즉, 처벌이나 제재를 피하기 위해 법을 지키는 사람들은 제재에 의한 억제수단이 효과적인 반면, 사회적 지각과 타인에 대해 피해를 주지 않으려는 사람들은 윤리적인 교육이 더 효과적일 수 있다.

처벌에 대한 인간의 심리는 관찰과 판단에 의하여 인지된 보상과 위험에 의해 결정된다(Wenzel, 2004; Kankanhalli *et al.*, 2003; O'Donoghue and Rabin,

2000). 예를 들면, 동료들이 금지된 행동을 피하는 경우 그 행동의 결과에 대한 인식 대신 보상에 대한 기대가 커지고, 동료들이 처벌을 받을 경우 위험과 행동의 결과에 대한 인식이 커진다. 따라서 처벌은 사람들의 잘못된 행동을 제약하고 통제한다(Peace *et al.*, 2003; Straub, 1990). 그러나 동료들이 잘못된 행위를 저지를 때, 그 결과에 대한 위험성과 처벌이 가혹하다고 해도 거기에 참여하고 싶은 감정이 커지게 된다(Akers *et al.*, 1979). 또 잘못을 저지르는 사람이나 그에 대한 추종자를 잡거나 처벌하는 것이 어렵다면 이러한 경향은 더욱 커질 것이다. 따라서 여러 가지 영향 외에도 인간의 상호작용은 법에 대한 객관적인 사고 체계와 인간의 태도 사이에서 중요한 변수가 됨으로써 조직의 분위기와 의사소통이 개인의 행동에 영향을 미칠 수 있다.

2.4 조직의 유형

현대의 조직들은 그 이익과 목적에 따라 변화함으로써 다양한 형태(form)를 갖추어 왔다(Weir, 1995). Williamson(1975)은 조직의 형태를 단일형태(Unitary-form: U-form)와 다분할형태(Multi-form: M-form)를 기준으로 분류하였다.

단일형태 조직은 각 부서들이 기능적으로 구성되어 있으며, 조직대표가 조직의 모든 사업에 책임을 지고 각 부서들은 조직대표에게 수시로 보고하는 중간관리자들에 의해 운용되는 조직이다(Robbins, 1990). 단일형태 조직은 중소기업과 같이 비교적 규모가 작은 조직에 적합한 것으로 알려져 있다.

이에 비해 다분할형태 조직은 기능적 부서들이 준 자율적인 운영부서로 어느 정도 독립적인 업무를 수행한다. 다분할형태의 조직들은 대기업과 같이 조직의 규모가 큰 조직이 대부분이다. 규모가 큰 조직은 수익과 조직목표를 추구하는 단순한 조직에서 벗어나 사회와 문화에 대한 책임감을 갖게 되며, 이러한 현상은 조직구성원으로 하여금 보다 엄격한 도덕성과 윤리를 강조하게 한다(문태영, 1996; 홍재영, 1986).

한편 정부조직을 포함한 공공(Public) 조직과 민간(Private) 조직간 차이를 분별해 내는데 많은 연구가 이루어져 왔다. 목표가 다른 공공조직과 민간조직의 경우에 조직의 문화가 뚜렷이 구별되며 이는 조직구성원에게도 큰 영향을 미치게 된다(Schein, 1985). 공공조직과 민간조직간의 문화적 특성을 비교해보면 공공조직은 업무나 절차의 중요성을 중시하는 등 관료주의적 성향이 강하며, 비합리적인 지시에도 복종하는 경향이 있고, 보수적·수동적 관행이 보편화되어 있다. 또한 공공조직의 구성원들은 민간조직에 비해 조직 규범성이 크지 않다고 할 수 있다(김원형, 1996).

따라서 본 연구에서는 조직형태 및 조직규모를 기준으로 조직형태를 단일형태와 다분할형태로 분류하고(Williamson, 1975), 조직의 특성에 따라 공공조직과 민간조직으로 나누어 조직유형에 따른 정보보안준수를 분석하고자 한다 본 연구에서는 조직규모를 중소기업기본법 제2조 및 동법시행령 제3조에 따라 상시 근로자 300인을 기준으로 중소조직(단일형태)과 대조직(다분할형태)으로 구분한다[1](<그림 1> 참조).

따라서 조직은 M-Pr(다분할-민간조직)형, U-Pr(단일-민간조직)형, M-Pu(다분할-공공조직)형, U-Pu(단일-공공조직)형 등 4가지 유형으로 분류할 수 있으며, 유형별 특징은 <표 1>과 같다.

조직형태	민간조직(Private)	공공조직(Public)
다분형(Mul-)	M-Pr	M-Pu
단일형(Uni-)	U-Pr	U-Pu

〈그림 1〉 조직의 유형

1) 본 연구에서는 조직규모를 중소기업기본법 제2조 및 동법시행령 제3조에 따라 상시 근로자 300인을 기준으로 중소조직(단일형태)과 대조직(다분할형태)으로 구분한다.

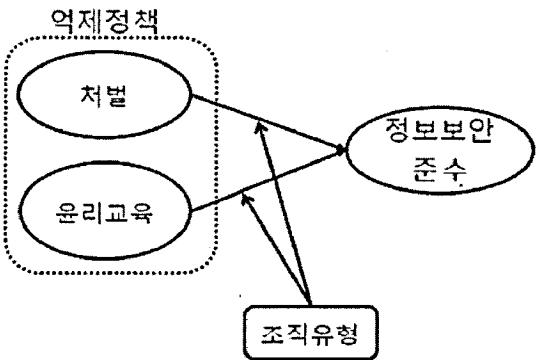
〈표 1〉 조직유형에 따른 특징

조직유형	특 징	근 거
U-Pr형	법적 절차와 규정에 대한 준수의식이 낮고 관료주의적인 성향도 가장 낮으며 개인의 노력과 성과를 중요시하여 구성원의 자기 통제력이 높음	Williamson *et al.*(1975)
M-Pr형	관료주의적이고 위계질서를 중요시하는 성향이 비교적 높은 반면 민간조직의 특성상 조직 관행 및 규정에 대한 순응도는 낮고 자기 통제력이 높음	Lynn(1981) Dahl, Lindblom(1953)
U-Pu형	법적인 절차와 규정에 대한 준수의식이 비교적 낮으나 공공 조직의 특성상 관료주의적인 성향이 나타나며 조직 관행에 대한 수동적인 모습이 강함	문태영(1996) 홍재영(1986)
M-Pu형	관료주의적이고 위계질서를 중요시하는 성향이 가장 높고 변화에 대한 저항이 크며 조직의 관행 및 규정에 대한 순응도가 높은 성향을 보임	김원형(1996)

Ⅲ. 연구모형 및 가설

3.1 연구모형 설계

본 연구에서는 문헌연구를 바탕으로 정보보안준수를 이끌어 내는 2가지 차별적 정책이 제재적 억제와 발전적 억제라는 것을 확인하였다. 이를 근거로 처벌과 윤리교육을 정보보안준수에 영향을 주는 주요요인으로 고려한다. 그리고 조직유형을 조직형태와 조직 특성을 기준으로 분류하고, 조직유형에 따라 구성원들간에 정보보안준수가 다르게 반영되는지를 확인하고자 한다. 따라서 정보보안준수에 영향을 주는 2가지 요인으로 제재적 억제와 발전적 억제를 독립변수로 하고, 조직유형을 조절변수로 하는 연구모형을 <그림 2>와 같이 제안한다.



〈그림 2〉 조직유형에 따른 정보보안준수모형

3.2 연구가설 설정

억제이론에 따르면 사람들은 예상되는 개인적 이익에 대한 기대와 법적 처벌의 두려움이 사람들의 억제동기를 만들어 낼 수 있다(Scholtz, 1997). 또한 도덕을 근본으로 한 윤리교육 시스템들 역시 규정위반에 대한 완화와 억제의 모델로서 제안되어 왔다(Harrington, 1997; Harrington, 1996; Kurland, 1995). 이러한 두 가지 요인은 정보보안 정책 분야에서 폭넓게 적용되어 왔으며 상황과 특정조건에 따라 두 가지 특성이 보완적으로 영향을 미치고 있다고 설명되어 왔다.

즉, 억제에 대한 2가지 태도로서 처벌과 같은 수단에 의한 제재적 태도와 윤리적 동기 유발이나 교육을 통한 발전적 태도로 정의할 수 있는데, 이렇게 상이한 근본적인 요소들이 조직 구성원들이 조직의 정보보안정책을 이해하고 행동으로 따르는 데 있어서 주요한 요인이 될 수 있을 것이다. 이러한 연구를 근거로 두 가지 억제요인인 처벌과 윤리교육이 정보보안준수에 미치는 영향을

다음과 같이 가설 1로 설정할 수 있다.

가설 1: 처벌과 윤리교육에 대한 인식이 높을 수록 정보보안준수가 높다.

기업은 규모가 크고 오래될수록 조직의 질서 유지를 위해 점차 많은 규정과 절차가 도입되며, 더 많은 계층과 부서가 생김에 따라 조직 상하 좌우간 의사소통의 장벽이 생기고 조직이 경직화되는 한편 유연성을 잃게 되는 등 관료주의 경향이 나타나게 된다(문태영, 1996). '관료적 형식주의, 거대조직, 공식화, 권한집중, 피라밋형 구조'는 대기업의 오래된 특징 중 하나가 되었다. 관료제하의 조직원들은 안정과 무사고를 지향하는 수동적 인간으로 변모될 가능성이 높다. 또한 개인의 창의력을 바탕으로 한 혁신적 아이디어의 도출과 이의 적응이 어려워져서 개인의 능력 발휘 가능성이 줄어든다. 이외에도 조직 구성원의 수가 많고 다양함에 따라 인사정책상 개별 구성원에 대한 성과측정이나 포상이 어려워지게 되어 조직의 처벌과 같은 강압적인 방법에 보다 순응하는 경향이 있다(윤순봉, 1994). 이러한 조직형태와 규모에 따라 다음과 같은 가설을 설정할 수 있다.

가설 2-1: 대규모의 다분할형태 조직이 소규모의 단일형태 조직보다 처벌에 대한 인식이 높다.

가설 2-2: 소규모의 단일형태 조직이 대규모의 다분할형태 조직보다 윤리교육에 대한 인식이 높다.

앞에서 살펴본 바와 같이 최근의 다양한 조직유형의 발달과 더불어 조직유형 분류에는 많은 의견이 제시되고 있지만, 특히 공공조직과 민간조직으로 분류하고 그 차이를 분석하는데 많은 연구가 이루어져 왔다. 정의에 의하면 공과 사를 구별하는 기준으로 영향 받는 이익의 공공성, 시설재원 정보에 대한 접근성, 개인 혹은 지역에 대한 활동성의 3가지 요인들을 활용한다(Benn and Gaus, 1983). 공공조직과 민간조직을 상호 극단적으로 분류할 수는 없으며, 그 차이는 정도의 차이 또는 차원의 차이로 볼 수 밖에 없다. 예를 들어 국적 항공사가 공공조직이냐 민간조직이냐 하는 것은 공공성과 사익성의 연장선 상에서 정도의 차이를 가지고 식별할 수 밖에 없다(Bozeman, 1987). 이러한 조직의 특성에 따라 다음과 같은 가설을 설정할 수 있다.

가설 3-1: 공공조직의 구성원들이 민간조직의 구성원들보다 처벌에 대한 인식이 높다.

가설 3-2: 민간조직의 구성원들이 공공조직의 구성원들보다 윤리교육에 대한 인식이 높다.

앞에서 설명한 바와 같이 다분할형태를 갖춘 대규모 조직은 단일형태를 갖춘 소규모 조직과 비교하여 처벌과 윤리교육의 영향이 다르게 미칠 수 있음을 설명하였다. 이와 연관하여 이러한 영향의 차이가 정보보안준수에 있어서 어떤 차이를 보이는지를 살펴보고자 다음과 같이 가설을 설정한다.

가설 4-1: 대규모의 다분할형태 조직의 구성원들은 소규모의 단일형태 조직의 구성원들보다 정보보안에 대해서 처벌이 윤리교육보다 효과적이다.

가설 4-2: 소규모의 단일형태 조직의 구성원들은 대규모의 다분할형태 조직의 구성원들보다 정보보안에 대해서 윤리교육이 처벌보다 효과적이다.

같은 방법으로, 조직 특성에 따라 처벌과 윤리교육이 정보보안준수에 미치는 영향의 차이를 알아보기 위해 다음과 같은 가설을 설정할 수 있다.

가설 5-1: 공공조직의 구성원들이 민간조직의 구성원들보다 정보보안에 대해서 처벌이 윤리교육보다 효과적이다.

가설 5-2: 민간조직의 구성원들이 공공조직의 구성원들보다 정보보안에 대해서 윤리교육이 처벌보다 효과적이다.

마지막으로 조직형태 및 조직 특성을 기준으로 분류된 조직유형에 따라 상호 상반된 특징을 갖는 M-Pu유형과 U-Pr유형에 대해 처벌과 윤리교육이 정보보안준수에 미치는 영향의 차이를 확인하기 위해 다음과 같은 가설을 설정할 수 있다.

가설 6-1: M-Pu형 조직구성원들이 U-Pr형 조직구성원들보다 정보보안에 대해서 처벌이 윤리교육보다 효과적이다.

가설 6-2: U-Pr형 조직구성원들이 M-Pu형 조직구성원들보다 정보보안에 대해서 윤리교육이 처벌보다 효과적이다.

Ⅳ. 실증연구 절차

4.1 자료의 수집 및 표본 구성

자료수집을 위해 조직유형 기준에 따라 각 유형별 2개 조직씩 총 8개의 조직을 선정하여 정보시스템 사용자를 대상으로 설문조사를 실시하였다. 대기업 수준의 규모를 갖는 M-Pu형, M-Pr형 조직은 R, N, H, S1사를 선정하였고, 중소기업 수준의 규모를 갖는 U-Pu형과, U-Pr형 조직은 S2, M, G, A사를 대상으로 100부씩 총 800부의 설문지를 배포하였고, 그 중 492부가 회수되어 61.5%의 회수율을 보였다. 이 중 문항에 대해 응답하지 않았거나, 부적절하게 응답한 설문지를 제외하고 총 439부를 분석에 사용하였다.

빈도분석결과 300명 이상의 다분할형태 조직구성원들이 228명으로 52%를 차지하고 있으며,

〈표 2〉 인구통계자료

구 분	표본(명)	표본 수	백분율	계
조직 형태	U-형(300미만)	211	48%	439
	M-형(300이상)	228	52%	
조직 특성	공공조직	204	46%	439
	민간조직	235	54%	
연령	20대	168	38%	439
	30대	174	40%	
	40대	77	17%	
	50대	20	5%	
학력	고 졸	39	9%	439
	전문대졸	54	12%	
	대 졸	279	64%	
	대학원졸	67	15%	

300명 이하의 단일형태 조직의 구성원들이 211명으로 48%이었다. 또한 공공조직은 204명으로 46%, 민간조직은 235명으로 54%이었다. 응답자의 연령분포는 20대 및 30대가 전체의 78%이었으며, 대졸 이상 학력이 79%로 조사되었다.

4.2 측정도구 개발

본 연구에서 사용된 측정도구는 인구통계변수를 제외하고 총 29문항으로 구성되었으며, 모든 측정항목은 이미 기존연구를 통해 신뢰성과 타당성이 검증된 측정변수를 수정 및 보완하여 사용하였다. 보안업계 관계자와 연구자들이 문항을 검토하고, 약 30명을 대상으로 예비검사(Pilot Test)를 실시하여 부적합한 문항은 삭제하였다. 설문문항 구성은 <표 3>과 같으며 각 문항은 7점 척도로 측정하였다(<부록> 참조).

4.3 자료분석방법

본 연구에서는 먼저 표본 자료를 검토한 후 응답자에 대한 인구통계변수를 처리하고, 측정

〈표 3〉 측정 도구

구 분		문항 수	관련연구
규정 순응도		6	Peace *et al.*(2003), Straub(1990)
정보보안 통제능력		6	Workman and Gathgi(2006), Scholtz(1997)
정보보안 개인성향		6	Wenzel(2004), Kankanhalli *et al.*(2003), O'Donoghue and Rabin((2000)
조직유형		2	김원형(1996), Schein(1985), Williamson(1975)
억제 정책	처벌	5	Workman and Gathgi(2006), Theoharidou *et al.*(2005)
	윤리 교육	4	Workman and Gathegi(2006), Hsu and Kuo(2003), Harrington(1997)
계		29	

도구의 내적 일관성(Internal Consistency)를 검증하기 위해 Cronbach's α값을 사용하여 각 변수들의 신뢰성을 검증한다. 타당성(Validity) 검증은 탐색적 요인분석(Exploratory Factor Analysis)을 통해 검증한다.

가설검증은 먼저 집단 간의 차이를 파악하기 위해 다변량 분산분석(MANOVA)을 사용하고, 회귀분석을 통해 조직특성에 따른 독립변수의 영향도를 검증한다. 마지막으로 일반화 선형 모형(Generalized Linear Model)으로 회귀계수 및 신뢰구간을 파악하고, 집단 간의 영향도와 차이를 분석한다. 자료분석 방법을 요약하면 <표 4>와 같다. 본 연구는 실증분석을 위해 SPSS 15.0과 AMOS 7.0을 사용하였다.

〈표 4〉 자료분석방법

분석 방법	분석 내용
빈도 분석	샘플의 특성파악
신뢰도 분석	측정변수간 내적 일관성 파악
요인 분석	측정변수의 타당성 파악
다변량 분산분석	측정집단 간 차이 파악
회귀 분석	모형의 적합성 파악 및 가설검증
일반화 선형모형	

V. 자료분석 결과

5.1 측정도구의 신뢰성 및 타당성 분석

신뢰성은 측정의 안전성, 일관성, 예측 가능성, 정확성이 내포된 개념으로서 측정결과가 어느 정도 일관성 있는지 또는 측정 결과에 오차가 있는지 의미한다(채서일, 1996). 측정치의 신뢰성을 평가하기 위해 Cronbach's α 값을 사용하였다. Murphy와 David(1988)는 Cronbach's α 값이 0.6~0.7이면 신뢰도가 낮다고 보고, 0.7이상은 중간수준이며, 0.8이상이면 높은 수준이라고 주장하였다. <표 5>와 같이 구성개념에 대한 신뢰도 값이 0.8이상으로 신뢰성을 확보하고 있음을 확인할 수 있다.

타당성(Validity)은 측정하고자 하는 개념이나 속성을 얼마나 정확히 측정하였는가를 말한다. 본 연구에서 사용된 측정 항목들은 기존 연구에서 타당성과 신뢰성이 검증된 측청치들을 사용하였으나, 과학적 연구의 관점에서 측정도구가 개념을 얼마나 적절하게 측정하고 있는가를 나타내는 개념 타당성이 특히 중요하므로 본 연구에서는 요인분석을 통한 변수들의 개념타당성을 검증하였다.

탐색적 요인분석은 어떤 변수들과 이들 변수들의 이면에 있는 공통요인들이 어떤 관련성을

〈표 5〉 신뢰도 측정결과

구성 개념	측정 항목	Cronbach α
처벌에 대한 태도	5	.832
윤리교육에 대한 태도	4	.843
규정 순응도	6	.822

가지는지 알아보기 위해 탐험적으로 요인분석을 실시하는 것이다. 본 연구에서는 요인 추출방법으로 주성분분석을 사용하였으며, 보다 정확한 값을 도출하기 위하여 요인 회전방법으로써 Varimax회전법을 사용하였다. <표 6>에서 보듯이 총 15개의 측정항목이 Eigenvalue 1.0이상을 기준으로 할 때 3개의 구성성분으로 각각 묶이고 있어 구성개념들이 집중타당성과 판별타당성을 확보하고 있음을 알 수 있다.

〈표 6〉 요인분석 결과

구 분	성 분		
	1	2	3
처벌에 대한 태도 2	**.891**	.140	-.107
처벌에 대한 태도 1	**.869**	.077	-.093
처벌에 대한 태도 5	**.843**	.093	-.106
처벌에 대한 태도 4	**.832**	.199	-.058
처벌에 대한 태도 3	**.790**	.201	-.069
정보보안준수 2	.174	**.805**	-.060
정보보안준수 1	.140	**.785**	-.146
정보보안준수 5	.123	**.777**	-.039
정보보안준수 6	.095	**.775**	-.074
정보보안준수 3	.073	**.711**	-.066
정보보안준수 4	.127	**.701**	-.108
윤리교육에 대한 태도 3	-.101	-.080	**.857**
윤리교육에 대한 태도 4	-.092	-.045	**.846**
윤리교육에 대한 태도 2	-.105	-.119	**.838**
윤리교육에 대한 태도 1	-.062	-.147	**.793**
Eigenvalue	**5.306**	**2.487**	**2.402**

5.2 가설 검증

처벌과 윤리교육이 정보보안준수에 영향을 미치는 가에 대한 가설 검증을 위해 처벌에 대한 인식과 윤리교육에 대한 인식을 각각 독립변수로 하고, 정보보안준수를 종속변수로 하여 회귀분석을 실시하였다.

앞의 <표 7>에서 보는 바와 같이 정보보안에 있어서 처벌에 대한 인식과 윤리교육에 대한 인식이 정보보안준수를 얼마만큼 설명하는가 하는 척도로서 설명력(R^2)은 18%로 나타나고 이때 유의수준 0.05에서 회귀식이 유의 하다는 것을 알 수 있다. 회귀계수는 처벌에 대한 인식이 0.361, 윤리교육에 대한 인식이 0.246으로 나타나고 있고 유의확률이 0.000으로 유의수준 0.05에서 유의하므로 결국 제재적 억제와 발전적 억제에 대한 인식이 정보보안준수에 긍정적 영향을 주는 요인임을 알 수 있다.

〈표 7〉 회귀분석 결과

◦모형 요약

모 형	R	R^2	수정된 R 제곱	추정 값의 표준오차	F	자유도	유의 확률
1	.431a	.186	.182	.94461	49.864	2	.000a

◦계수

모 형	비표준화 계수		표준화 계수	t	유의 확률
	B	표준오차	B		
1(상수)	1.935	.294	.384	6.591	.000
처 벌	.361	.041	.384	8.808	.000
윤리 교육	.246	.042	.258	5.911	.000

* 종속변수: 정보보안준수.

조직형태와 조직 특성 간 차이를 분석하기 위해 다변량 분산분석(MANOVA)을 실시하였다. 다변량 분산분석은 종속변수가 여러 개일 경우 특정 유의수준에서 집단 간의 차이를 검정하는 방법이다. 이번 검증에서는 조직형태에 의한 차이(M-형, U-형), 특성에 의한 차이(Public, Private)에 따라 처벌과 윤리교육에 대한 인식이 어떻게 다른지를 살펴보고자 하였다. 다변량 분산분석 결과는 <표 8>과 같다.

<표 8>는 Pillai's Trace, Wilks' Lambda, Hotelling's Trace, Roy's Largest Root에 의한 검정결과이다. Hotelling's Trace와 Roy's Largest Root는 큰 값을 가질수록, Pillai's Trace와 Wilks' Lambda 는 작은 값을 가질수록 집단 간의 평균의 차이를 나타내는 F-통계량의 값은 커진다(이순묵, 1990).

표의 2번째 열은 각각 계산한 검정통계량이며 3번째 열은 이들 값을 F-값으로 변환하였을 때의 F-통계량이다. 4번째 열과 5번째 열은 각각 집단간 분산 및 집단내 분산의 자유도이며 마지막 열의 유의확률은 귀무가설 하에서 F-검정 통계량보다 큰 F-값을 얻을 확률을 보여주고 있다. 분석결과 모두 0.000으로 유의수준 0.05에서 집단간 평균들이 차이가 있다고 볼 수 있다. 따라서 조직형태 및 특성의 차이에 따라 처벌과 윤리교육에 대한 구성원의 인식 차이가 있다고 할 수 있다.

<표 8>에서 보인 다변량 검정을 통해 집단간 차이가 존재함이 증명되었다. 따라서 가설 2-1, 가설 2-2, 가설 3-1, 가설 3-2은 모두 유의한 결과를 나타낸다. 분석결과는 조직형태 및 조직특성이 조직구성원들의 성향에 영향을 미친다고 할 수 있다. 조직구성원들은 개인적 성향이 분명히 존재하지만 조직의 형태와 특성에 따라 정보보안과 관련하여 처벌과 윤리교육에 대한 인식에 대해 차이가 있음을 의미한다. <표 9>는 다변량 분산분석의 기술 통계량이 나타나 있다.

처벌과 윤리교육 중 어떤 정보보안정책이 더 효과적인지를 구별하기 위해 조직의 형태와 특성에 따라 표본을 나눈 후 일반화 선형 모형분석을 실시하였다. 95% 신뢰 수준에서 각 집단 간에 두 독립 변수가 각각 얼마나 효과를 미치며 어떤 차이를 내는지를 살펴본 결과는 <표 10>과 같다.

조직형태에 따른 검정결과를 살펴보면 다분할형태 조직의 처벌에 대한 회귀계수가 0.481로서 단일형태 조직의 0.295보다 높으며 유의수준 0.05에서 유의하다. 또한 신뢰구간에서 회귀계수에 대해 두 집단의 차이가 있다고 설명하므로, 다분할형태의 조직 구성원은 단일형태 조직구성

〈표 8〉 다변량 검정결과

효 과	값	F	가설 자유도	오차 자유도	유의 확률
Intercept Pillai's Trace	.977	9051.940[b]	2.000	434.000	.000
Wilks' Lambda	.023	9051.940[b]	2.000	434.000	.000
Hotelling's Trace	41.714	9051.940[b]	2.000	434.000	.000
Roy's Largest Root	41.714	9051.940[b]	2.000	434.000	.000
Cons Pillai's Trace	.072	16.922[b]	2.000	434.000	.000
Wilks' Lambda	.928	16.922[b]	2.000	434.000	.000
Hotelling's Trace	.078	16.922[b]	2.000	434.000	.000
Roy's Largest Root	.078	16.922[b]	2.000	434.000	.000
Type Pillai's Trace	.135	33.946[b]	2.000	434.000	.000
Wilks' Lambda	.865	33.946[b]	2.000	434.000	.000
Hotelling's Trace	.156	33.946[b]	2.000	434.000	.000
Roy's Largest Root	.156	33.946[b]	2.000	434.000	.000

〈표 9〉 다변량 분산분석의 기술 통계량

조직 구분	정보보안 인식	평 균	표준 편차	N
다분할	처벌에 대한 인식	4.8518	1.03617	220
	윤리교육에 대한 인식	4.4330	1.14616	220
단일	처벌에 대한 인식	4.4466	1.14948	219
	윤리교육에 대한 인식	4.8630	1.00175	219
공공	처벌에 대한 인식	4.8833	1.03339	204
	윤리교육에 대한 인식	4.2721	1.18077	204
민간	처벌에 대한 인식	4.4468	1.13906	235
	윤리교육에 대한 인식	4.9734	.90114	235

〈표 10〉 일반화 선형 모형분석 결과

◦조직형태간 검정(가설 4-1, 가설 4-2)

Parameter	B	Std. Error	95% Wald Confidence Interval		Hypothesis Test		
			Lower	Upper	Wald χ2	df	Sig.
(Intercept)	1.769	.2896	1.201	2.336	37.292	1	.000
처벌(M-형)	.481	.0503	.382	.580	91.380	1	.000
처벌(U-형)	.295	.0480	.201	.389	37.717	1	.000
윤리(M-형)	.129	.0480	.035	.223	7.246	1	.007
윤리(U-형)	.362	.0514	.262	.463	49.715	1	.000

◦조직특성간 검정(가설 5-1, 가설 5-2)

Parameter	B	Std. Error	95% Wald Confidence Interval		Hypothesis Test		
			Lower	Upper	Wald χ2	df	Sig.
(Intercept)	1.790	.2795	1.243	2.338	41.041	1	.000
처벌(공공)	.515	.0477	.421	.608	116.168	1	.000
처벌(민간)	.296	.0463	.206	.387	41.011	1	.000
윤리(공공)	.036	.0453	-.053	.125	.632	1	.027
윤리(민간)	.384	.0530	.280	.488	52.579	1	.000

◦M-Pu, U-Pr간 검정(가설 6-1, 가설 6-2)

Parameter	B	Std. Error	95% Wald Confidence Interval		Hypothesis Test		
			Lower	Upper	Wald χ2	df	Sig.
(Intercept)	1.715	.2770	1.172	2.258	38.303	1	.000
처벌(M-Pu)	.610	.0557	.501	.719	119.848	1	.000
처벌(U-Pr)	.273	.0629	.150	.396	18.852	1	.000
윤리(M-Pu)	-.092	.0576	-.205	.020	2.577	1	.108
윤리(U-Pr)	.440	.0663	.310	.570	44.024	1	.000

원보다 정보보안에 있어 처벌과 같은 제재가 더 효과적인 것으로 판명되었다. 또한 다분할형태 조직은 유의수준 0.05에서 윤리교육에 대한 정보보안준수가 0.129로서 단일형태 조직의 0.362보다 낮다. 이를 통해 가설 4-1과 4-2가 각각 채택될 수 있으며, 이러한 방법으로 가설 5-1과 5-2 역시 가설검증결과가 유의함을 확인할 수 있다.

조직형태와 특성을 동시에 고려한 혼합된 조직유형 중 M-Pu형과 U-Pr형에 대한 검정결과를 분석해 보았다. 먼저 M-Pu형은 처벌에 대한 회귀계수가 0.610으로 U-Pr의 0.273보다 높으며, 이는 유의수준 0.05에서 유의하고, 95% 신뢰구간에서 두 집단의 차이가 존재한다. 또한 U-Pr형의 경우 윤리교육과 관련하여 회귀계수가 0.440이고, M-Pu형의 경우 유의수준 0.05에서 기각되어 영향이 없는 것으로 판명되었다. 하지만, M-Pu형은 각각의 특성인 M형과 공공조직이 반대되는 타 집단과 비교하여 윤리교육에 대한 효과가 비교적 적은 것으로 나타나, U-Pr형이 M-Pu형보다 발전적 억제에 대한 영향이 더 큰 것으로 볼 수 있다. 따라서 가설 6-1과 가설 6-2는 유의한 것으로 나타났다.

VI. 연구성과

본 연구의 성과를 요약하면 다음과 같다. 첫째, 인간통제의 요소로 선정한 처벌과 윤리교육이 정보보안준수에 영향을 미치는 주요 요인으로 확인되었다. 이러한 사실은 억제 이론과 최근의 관련 연구(Workman and Gathegi, 2006)의 결과와 동일한 결과를 나타내고 있다. 즉, 정보보안정책을 준수하는데 있어서 처벌과 윤리교육에 대한 인식이 정보보안준수에 영향을 미친다고 할 수 있다.

둘째, 조직의 형태를 대규모 조직에 적합한 다분할 형태와 소규모 조직에 적합한 단일형태로 구분하고, 조직의 문화적 특성에 따라 공공조직과 민간조직으로 분류한 후 조직 구성원들이 처벌과 윤리교육에 대한 인식의 차이가 있는지 검증하였다. 분석결과 다분할형태 조직이 단일형태 조직에 비해 처벌에 대한 인식이 높은 반면 윤리교육에 대한 인식은 상대적으로 낮은 것으로 나타났다. 또한 공공조직이 민간조직보다 처벌에 대한 인식이 높고 윤리교육에 대한 인식은 낮은 것으로 파악되었다. 이러한 결과는 보수적이고 관료주의적 위계질서가 강조되는 다분할형태 조직과 공공조직의 특징이 구성원의 성향에 반영되었다고 할 수 있다.

셋째, 조직 특성에 따라서 처벌과 윤리교육에 대한 인식이 정보보안준수에 미치는 영향을 검증한 결과, 다분할형태 조직이 단일형태 조직에 비해 처벌에 대한 인식이 높아질수록 정보보안준수에 더 큰 영향을 줄 수 있으며, 윤리교육에 대한 인식은 상대적으로 정보보안준수에 영향을 적게 주는 것으로 나타났다. 또한 공공조직이 민간조직보다 처벌에 대한 인식이 높아질수록 정보보안준수에 더 큰 영향을 줄 수 있으며, 윤리교육에 대한 인식은 상대적으로 영향을 적게 주는 것으로 나타났다. 이러한 사실은 조직의 정보보안효과를 증대시키는 데 있어서 처벌과 윤리교육을 조직의 특성에 맞게 비중을 둘 필요가 있음을 암시하는 것일 수 있다.

마지막으로, 다분할형태이면서 공공조직의 특성을 가진 조직과 단일형태이면서 민간조직의 특성을 가진 조직의 차이를 검증하였는데, 그 차이가 더욱 확연히 드러났다. 다분할형태이면서 공공조직의 특성을 가진 조직이 단일형태이면서 민간조직의 특성을 가진 조직에 비해 처벌에 대한 인식이 높을수록 정보보안준수가 상당히 높게 나타났다. 반면에 윤리교육에 대한 인식에 대해서는 다분할형태이면서 공공조직의 특성을 가진 조직은 효과가 거의 없는 반면, 단일형태이면서 민간조직의 특성을 가진 조직은 효과가 상당히 높게 나타났다. 이러한 결과를 토대로, 조직형태와 특성의 차이를 동시에 고려할 때 조직은 더욱 처벌과 윤리교육에 대한 현저한 인식의 차이가 나타나며 결국 정보보안준수에도 큰 차이

를 드러나게 했다고 할 수 있다.

Ⅶ. 결론 및 향후 연구과제

정보보안에 대한 문제들은 기술적 보안, 물리적 보안을 아무리 강화하더라도 인간의 행위와 정보보안통제를 지키지 않고 이를 위반하는 인간의 의지와 행위에 의해 발생할 수 있다(Sasse, 2004). 즉 인간행위에 대한 자발적 통제를 이끌어내고 이를 감독하는 것이 정보보안을 유지하는데 중요한 요소인 것이다. 이와 관련하여 최근 몇몇 연구에서는 사용자 특성에 따른 정보보안효과를 분석한 바 있다(Workman and Gathegi, 2006).

본 연구의 목적은 정보보안을 추구하는데 있어서 조직형태와 특성의 차이에 따른 정보보안정책에 초점을 맞춤으로써 보다 근본적인 조직구성원의 행위 변화와 자기통제를 이끌어내는 방법을 찾고자 하는 것이다. 정보보안 침해를 막는 데 있어서 기술적 보안 못지않게 중요한 것은 이를 직접 사용하는 인간이며 이러한 인간의 행위에 대한 변화와 통제가 없다면 우수한 보안기술도 무용지물과 다름없다. 본 연구에서는 인간의 행동에 제약을 주는 요소로 처벌에 따른 두려움과 인간의 양심에 호소하고 인간의 자기통제 능력을 믿음으로써 윤리에 따른 동기유발을 주요 요소로 선정하였다.

가설검증을 통해 조직이 다분할형태 조직이고, 공공조직의 성향이 강할수록 정보보안정책의 준수에 있어서 처벌과 같은 제재적 억제가 보다 효과적인 것을 알 수 있는데, 이는 조직의 관료주의적 성향과 형식적인 절차를 중시하는 풍조가 조직 구성원의 수동적인 성향을 강화시켜 준 것이라고 볼 수 있다. 또한 단일형태에 가깝고 민간조직의 성향이 강할수록 정보보안정책의 준수에 있어서 윤리교육과 같은 발전적 억제가 보다 효과적인 것으로 설명되었는데, 이는 조직의 높은 융통성과 성과 중심적인 성향이 조직구성원의 능동적인 성향을 강화시켰다고 볼 수 있다.

결론적으로 조직의 특징을 이해하지 않은 채, 조직 관리자들의 획일적인 정보보안정책의 수립과 시행은 그 효과가 상대적으로 낮을 수 밖에 없다. 따라서 조직관리자와 관련 부서들은 정보보안정책 수립 시 조직유형에 따른 구성원의 성향을 먼저 이해하고 이를 정책에 반영한다면 정보보안정책을 준수하는데 큰 효과를 거둘 수 있을 것이다.

본 연구는 중요한 연구적실무적 성과에도 불구하고 몇 가지 한계점을 갖고 있다. 첫째, 본 연구에서는 조직을 유형에 따라 분류하는 데 있어서 일상적으로 통용되는 조직의 형태 및 특성에 따라 분류하였다. 하지만, 최근의 조직은 급변하는 사회 현상과 맞물려 복잡하고 다양한 특징을 갖고 있으므로 이러한 경향에 맞추어 다양한 조직분류를 통해 분석한다면 조직의 정보보안정책 수립에 있어서 보다 큰 도움을 줄 수 있을 것이다.

둘째, 정보보안정책을 준수하게 하는 통제 수단으로써 처벌과 윤리교육을 선정하여 분석하였으나, 이 외에도 정보보안준수에 영향을 미칠 수 있는 여러 가지 다양한 통제수단이 있을 수 있으므로 이런 통제수단에 대한 연구와 추가적인 분석이 된다면 보다 발전된 연구결과를 얻을 수 있을 것이다.

셋째, 본 연구에서는 설문조사를 통해서 조직유형에 따른 처벌과 윤리교육이 정보보안준수에 미치는 영향을 분석하였다. 본 연구의 결과를 보다 실질적으로 검증하기 위해서 본 연구에서 사용된 설문조사 이외에 질적 연구방법(예: 정보보안정책담당자 인터뷰 등)이 추가적으로 수행된다면 보다 통합적이고 유용한 연구결과를 도출해 낼 수 있을 것이다.

마지막으로, 본 연구는 시간적, 예산적 제한 때문에 4개 조직 유형별로 각각 2개씩의 조직을 선정하였는데, 유형별로 2개씩 선정된 조직이 그 유형의 조직 특성을 충분히 반영한다거나 조직의 속성을 대표하는데 있어서 제한사항이 있

을 수 있다. 향후 더 많은 조직을 대상으로 추가적인 연구를 한다면 본 연구모형의 신뢰성이 제고될 것이라고 판단한다.

참 고 문 헌

김미희, 이명진, 채기준, 김호원, "센서 네트워크에서 AODV 라우팅 정보 변조공격에 대한 분석", 정보처리학회논문지, 제14-C권, 제3호, 통권 제113호, 2007, pp. 229-238.

김원형, 공기업과 민간기업간 조직풍토 비교분석, 대전대학교 사회과학연구소, 1996.

김종기, 전진환, 임호섭, "정보보안정책, 보안통제 및 사용자특성이 정보보안효과에 미치는 영향: 컴퓨터 바이러스를 중심으로", 정보시스템연구, 제15권, 제1호, 2006, pp. 145-168.

문태영, 대기업병과 치유방안에 관한 연구, 건국대학교, 1996.

백승훈, 민천홍, "보안통제와 정책이 기업의 보안체계에 미치는 영향에 대한 탐색적 연구", 한국경영정보학회 2004년 춘계학술대회, 2004, pp. 854-860.

윤순봉, 대기업병: 그 실체와 치유방안, 삼성경제연구소, 1994.

이순묵, 공변량 구조 분석, 성원사, 1990.

채서일, 사회과학조사방법론, 학현사, 1997.

하영길, "인터넷 정보보안 기술에 관한 연구", 상업기술연구, 제13호, 2004, pp. 176-187.

홍재영, 대기업병의 증세와 진단, 한국 경영자총협회, 1986.

황윤철, "체계적인 보안 정책 관리를 위한 계층적 보안 모델 설계", 컴퓨터 정보통신 연구, 제9권, 제1호, 2001, pp. 21-32.

Ajzen, I., From intentions to actions: A theory of planned behavior, In From cognition to behavior Action-control, J. Kuhl and J. Beckman (Eds.), *Heidelberg, Germany: Springer*, 1985.

Akers, R. L., M. D. Krohn, L. Lanza-Kaduce, and M. Rodosevich, "Social learning and deviant behavior: A specific test of a general theory", *American Sociological Review*, Vol.44, 1979, pp. 636-655.

Aubert, V., Sociology of law, Baltimore: Penguin Books, 1969.

Benn, S. I. and G. F. Gaus, Public and Private in Social life, New york: Palgrave Macmillan, 1983.

Bozeman, B., All Organizations are Public: Comparing Public and Private Organizations, *Beard Books*, 1987.

Calluzzo, V. J. and C. J. Cante, "Ethics in information technology and software use", *Journal of Business Ethics*, Vol.52, 2004, pp. 301-312.

Costa, A. L. and B. Kallick, Assessment in the learning organization: Shifting the paradigm, New York: ASCD Books, 1997.

Harrington, S. J., "The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions", *MIS Quarterly*, Vol.20, 1996, pp. 257-278.

Harrington, S. J., "A test of a person-Issue contingent model of ethical decision making in organizations", *Journal of Business Ethics*, Vol.16, 1997, pp. 363-375.

Hoffer, J. A. and D. W. Straub, "The 9 to 5 underground: Are you policing computer crimes?", *Sloan Management Review*, Vol.30, 1989, pp. 35-43.

Hsu, M. H. and F. Y. Kuo, "An investigation of volitional control in information ethics", *Behavior and Information Technology*, Vol.22, 2003, pp. 53-62.

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, 2003, pp. 139-154.

Kurland, N. B., "Ethical intentions and the theories

of reasoned action and planned behavior", *Journal of Applied Social Psychology*, Vol.25, 1995, pp. 297-313.

Lee, J. and Lee, Y., "A holistic model of computer abuse within organizations", *Information Management and Computer Security*, Vol.10, 2002, pp. 57-63.

NIST, An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12, National Institute of Standards and Technology, 1995.

O'Donoghue, T. and M. Rabin, "The economics of immediate gratification", *Journal of Behavioral Decision Making*, Vol.13, 2000, pp. 233-250.

Peace, A., G. Graham, F. Dennis, and J. Y. L. Thong, "Software piracy in the workplace: A model and empirical test", *Journal of Management Information Systems*, Vol.20, 2003, pp. 153-177.

Rahim, M. M. D., A. H. Seyal, and M. N. Rahman, "Factors affecting softlifing intention of computing students: An empirical study", *Journal of Educational Computing Research*, Vol.24, 2001, pp. 385-405.

Robbins, S. P., Organization Theory: Structure, Design and Applications, Third Edition, Prentice Hall, 1990.

SANS, "The SANS security policy project", Bethesda, MD: SANS Institute(URL: http://www.sans.org/resources/policies), 2005.

Sasse, M. A., "Usability and trust in information systems", *Cyber Trust and Crime Prevention Project*, University College London, 2004, pp. 1-18.

Schein, E. H., Organizational Culture and Leadership, San Francisco, CA: Jossey-Bass, 1985.

Scholtz, J. T., "Enforcement policy and corporate misconduct: The changing perspective of deterrence theory", *Law and Contemporary Problems*, Vol.60, 1997, pp. 253-268.

Simpson, P. M., D. Banerjee, and C. L. Simpson, "Softlifting: A model of motivating factors", *Journal of Business Ethics*, Vol.13, 1994, pp. 431-438.

Straub, D. W., "Effective IS security: An empirical study", *Information Systems Research*, Vol.1, 1990, pp. 255-276.

Straub, D. W. and W. D. Nance, "Discovering and disciplining computer abuse in organizations: A field study", *MIS Quarterly*, Vol.14, 1990, pp. 45-60.

Straub, D. W. and R. J. Welke, "Coping with systems risk: Security planning models for management decision-making", *MIS Quarterly*, Vol.22, 1998, pp. 441-469.

Tapp, J. L. and L. Kohlberg, Developing senses of law and legal justice, In Law, justice, and the individual in society: Psychological and legal issues, J. L. Tapp and F. J. Levine (eds.), New York: Holt, Rinehart and Winston, 1977.

Theoharidou, M., S. Kokolakis, M. Karyda, and E. Kiountouzis, "The insider threat of information systems and the effectiveness of ISO17799", *Computers and Security*, Vol.24, 2005, pp. 472-484.

Weir, C., "Organizational structure and corporate performance", *Management Decision*, Vol.33, 1995, pp. 24-32.

Wenzel, M., "The social side of sanctions: Personal and social norms as moderators of deterrence", *Law and Human Behavior*, Vol.28, 2004, pp. 547-567.

Williamson, O. E., Markets and Hierarchies: Analysis and Antitrust Implications, New York: Macmillan Press, 1975.

Workman, M. and J. Gathegi, "Punishment and Ethics Deterrents: A Study of Insider Security Contravention", *Journal of the American Society for Information Science and Technology*, Vol.58, No.2, 2006, pp. 212-222.

〈부록〉 설문측정항목

Ⅰ. 조직의 규정(규칙) 준수 수준

1. 조직의 규정은 때로 불필요한 것이 많다고 느낄 때가 많다.
2. 나의 동료들은 상사로부터의 제재나 처벌이 걱정되어 규정을 따르는 경향이 있다.
3. 우리 조직의 규정은 많은 부분 수정되거나 없어져야 한다.
4. 조직의 규정은 결국 조직에 도움이 되는 것 이라고 믿고 있다.
5. 효율적인 업무수행을 위해 규정을 무시하는 경우가 가끔 있다.
6. 조직으로부터 제재나 처벌이 없다면 규정을 따르는 사람들이 많이 줄어들 것이다.

Ⅱ. 정보보안에 대한 자기통제 성향

1. 나는 사무실의 소프트웨어나 파일이 유용하다고 해도 개인적으로 사용할 수 없다.
2. 업무 효율을 위해 때로는 허가없이 업무자료를 공유 할 수 있다고 생각한다.
3. 나는 업무의 효율을 위해 업무와 관련된 자료를 집에 가져와서 해본 적이 있다.
4. 나는 사무실의 컴퓨터의 바이러스 감염여부에 대해 걱정해 본 적이 많다.
5. 조직의 정보보안과 관련된 규정이 번거롭기 때문에 지키기 어렵다고 생각한다.
6. 상사로부터의 제재나 통제가 없다면 정보보안 규정은 지켜지기 힘들 것이다.

Ⅲ. 정보보안에 대한 개인성향

1. 사무실 컴퓨터의 중요파일을 긴급한 업무처리를 위해 퇴근 후 집에서 사용해도 괜찮다.
2. 나는 사무실의 소프트웨어나 업무파일을 집에서 절대 사용하지 않을 것이다.
3. 내 동료들은 내가 내부자료를 허가 없이 외부에서 사용해서는 안 된다고 생각한다.
4. 내 동료들은 사무실 컴퓨터의 소프트웨어나 자료를 허가 없이 집에서 쓰는 경우가 있다.
5. 대부분의 사람들은 사무실 컴퓨터의 암호를 규정에 맞게 수시로 변경하고 있다.
6. 나는 귀찮더라도 규정에 맞게 컴퓨터 암호를 자주 교체하여 사용해야 한다고 생각한다.

Ⅳ. 정보보호를 위한 조직의 통제수단

1. 조직의 정보보안 관련 규정을 준수하기 위해서는 위반자의 제재와 처벌이 필요하다.
2. 조직의 정보보안 관련 규정에 대한 주기적인 교육이 중요하다.
3. 조직의 정보보안 관련 규정을 준수하기 위해서는 엄격한 상벌제도가 적용되어야 한다.
4. 조직의 정보보안 관련 규정에 대해 잘 이해하지 못하는 부분이 많다.
5. 조직의 정보보안 활동이 강화되어 위반자에 대한 감시와 감독이 이루어져야 한다.
6. 정보보안에 대한 중요성과 규정을 정확히 안다면 대부분 규정을 준수할 것이다.
7. 규정 위반자에 대한 통제와 처벌이 보안규정 교육과 같은 예방활동보다 효과적이다.
8. 정보침해 등 보안 위반 사례에 대한 교육이 조직원의 규정 준수의식을 높일 수 있다.
9. 제재와 처벌과 같은 통제로 인해 조직원들은 규정에 순응하게 될 것이다.

Ⅴ. 조직의 규모(구조) 및 유형

조직규모: 1) 100명 미만 2) 100~300명 3) 300~500명 4) 500명 이상
조직유형: 1) 공공조직(공기업) 2) 민간조직(일반기업) 3) 기타 _____

Information Systems Review
Volume 12 Number 1
April 2010

Impacts of Punishment and Ethics Training on Information Security Compliance: Focus on the Moderating Role of Organizational Type

Joongho Ahn* · Junhyung Park** · Kimoon Sung*** · Jaehong Lee****

Abstract

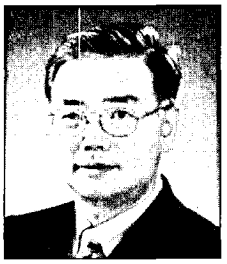
Although organizations are given various benefits with information technologies, they sometimes have suffered fatal damages due to information security incidents now such as computer virus, hacking, counterfeiting, plagiarizing, etc. The fundamentalcauses of information security incidents are closely related to individuals who do not comply with information security policy or rules. The spontaneous self-control of individuals and monitoring for individuals could be the most essential solution for the ongoing observance of information security policy. Thus, the purpose of this study is to analyze effects of punishment and ethics training on compliance of information security policy of individuals in organizations, to determine individual divide among security propensity depending on organization types, and to find the more fundamental solution which leads change of organizational members' behaviors and self-control. Regardless of the type of organizations, the results of the study suggest that there exist positive effects of punishment and ethics training in all types of organization on compliance of information security rules or regulations. A member of unitary form organization has higher cognition of punishment than a member's cognition of the multi-divisional form organization, while relatively lower awareness of ethics training. Also, a member of public organization has higher awareness of ethics training than a member's awareness of private organization, while lower cognition

* Professor, Graduate School of Business, Seoul National University
** Major, Republic of Korea Army, The 3rd Army Academy
*** Major, Republic of Korea Air Force, Korea Air Force Headquarters
**** Ph.D, candidate, College of Business Administration, Seoul National University

of punishment. Finally, the result shows that punishment and ethics training may be major factors which affect information security. It also suggests that organizational security managers have to understand and consider organization member's propensity relying on organization form and organization characteristics for establishment and enforcement of information security policy.

Keywords: ***Information Security, Deterrence Theory, Information Security Policy, Information Security Compliance, Organizational Type***

◐ 저 자 소 개 ◑



안 중 호 (jahn@snu.ac.kr)

현재 서울대학교 경영학과 교수로 재직하고 있으며, 한국 CEO학회장을 맡고 있다. 한국경영정보학회와 한국퍼실리티매지니먼트학회 회장 및 한국정보산업연합회 IT거버넌스 협회장을 역임하였다. 서울대학교 문리과대학 외교학과를 졸업하고, 서울대학교 행정대학원에서 행정학 석사를 취득한 후, 미국New York Universicy, Stern School of Business에서 Information System 석사 및 박사 학위를 취득하였다. Fordham Univ., Univ of Baltimore 조교수로 재직하였다. 주요 관심분야는 정보기술과 경영혁신 전략, m-business, e-business 등이다.

박 준 형 (zoons75@paran.com)

현재 육군 제 3사관학교 경영학과 교수로 재직하고 있다. 육군사관학교 관리학과를 졸업하고, 서울대학교 경영학과에서 석사학위를 취득하였다. 다수의 국방경영 관련 프로젝트를 수행하고 있으며, 주요 연구분야는 정보보안, 디지털 경영, IT 전략, 국방경영 혁신 등에 관심을 두고 있다.

성 기 문 (majsung@snu.ac.kr)

현재 대한민국 공군 소령으로, 공군본부 인사참모부에 재직하고 있다.
공군사관학교 전산통계학과를 졸업하고, 고려대학교에서 경영학 석사, 서울대학교 경영학과에서 박사 학위를 취득하였다. 주요 관심분야는 IT 상호작용성, IT와 조직, 모바일 비즈니스 전략 등이다.

이 재 홍 (jhonglee@snu.ac.kr)

현재 서울대학교 경영대학 경영학과(MIS전공) 박사과정을 수학중이다. 공군사관학교 경영학과를 졸업하고, 국방대학교에서 국방관리학 석사학위를 취득하였다. 주요 관심분야는 IT 경영전략, Knowledge Service, Network Dynamics 등이 있다.

논문접수일 : 2009년 12월 27일 **게재확정일 : 2010년 04월 08일**
1차 수정일 : 2010년 03월 30일