# 기업 정보보호 활동을 위한 조직 구성원들의 태도와 주요 영향 요인

박준경(제1저자)
LG CNS 구매부
(joonpark@lgcns.com)
김범수(제2저자)
연세대학교 정보대학원
(beonsookim@gmail.com)
조성우(제3저자, 교신저자)
Management School, The University of Liverpool
(csw0323@hotmail.com)

기업에서는 정보를 보호하기 위해 보안 시스템을 구축한 후 다양한 정책을 마련할 뿐만 아니라 조직 구성원의 보안 의식을 고취시키기 위한 활동도 더불어 실행하고 있다. 이러한 노력은 구성원에게 지속적으로 사내 홍보와 교육을 통하여 전달되고 있다. 현실은 아직도 개인의 보안 인식의 부족으로 인하여, 기업의 중요 정보의 유출이 빈번하게 일어나고 있다. 본 연구는 이런 현상을 설명하기 위하여 기업의 정보를 보호를 위한 다양한 활동에 영향을 주는 요인들을 조사하였으며, 기술수용모델(Technology Acceptance Model, TAM)을 바탕으로 억제이론(Deterrence theory)과 통제이론(Control theory)의 관점에서 접근해 보았다.

먼저 기술수용모델을 바탕으로 정보 보호에 대한 조직 구성원의 수용 태도에 영향을 주는 요인으로 지각된 유용성과 지각된 사용 편의성을 선정하였다. 이러한 요인은 억제이론의 보안 정책, 보안 시스템, 보안 교육 등의 변수를 유용성과 편의성 관점에서 추출하였으며, 통제이론에서는 처벌과 보상이라는 변수를 조직 구성원의 태도에 영향을 주는 요인으로 선택하였다. 정책, 시스템, 교육, 보상과 처벌이 정보 보호를 위한 기업자체의 노력에 대한 것이라면 개인적인 측면 역시 조직 구성원의 태도에 영향을 줄 수 있다. 그러므로 개인적인 경험, 실제 위험에 대한 인식, 보안과 업무 연관성 등을 추가적인 변수로 활용하였다.

실증분석을 위한 자료 수집은 설문조사를 통해 이루어졌으며 인터넷 설문을 통하여 수집된 총 242부의 자료가 분석에 사용되었다. 회귀 분석 결과 인지된 보안 교육과 보상의 유용성, 인지된 처벌의 유용성 그리고 보안에 관련된 위험 인식이 기업 조직 구성원의 태도에 직접적이고 긍정적인 영향을 미치는 것으로 나타났다. 본 연구 결과 기업에서는 보안 교육을 강화해야 할 필요가 있으며, 정보 보호에 대한 동기를 유발시키기 위한 적절한 보상이 필요함을 알 수 있었다. 또한 이러한 결과는 개인에 대한 처벌이 강화되고 보안에 관련된 위험 인식이 높아진다면 조직 구성원이 지속적인 정보 보호를 위해 노력하게 될 것임을 시사한다.

주제어: 기업 정보보호, 보안, 기술수용모델, 억제이론, 통제이론, 조직 구성원 태도

## Ⅰ. 서 론

1990년대 이후 발달한 정보통신 기술로 인하여 정보의 소유가 새로운 부가가치를 창출하게 되면서 기업 간의 정보 수집 경쟁 및 정보 보호를 위한 기술 개발이 치열해지게 되었다. 정보화 사회의 도래는 정보 전쟁 시대로의 돌입이라고 볼 수 있으며 (송주석, 1997), 네트워크의 발달로 유비쿼터스 시대를 맞는 지금 정보 보호는 매우 크고 중대한

논문접수일: 2011. 1 게재확정일: 2011. 6

문제로 인식되어 기업과 개개인에게도 심각한 영향을 주고 있다. 국내에서도 기업의 정보 보호에 관련해서는 수많은 유출 사건이 언론에 보도되어 경각심을 높이고 있는 실정이다. 2008년 한 해에 발생한 기업 정보 유출 사건으로 소송에 참가한 이들은 20만여 명에 이르며, 옥션, GS 칼텍스, 하나로텔레콤을 상대로 한 총 청구액이 2,100억 원대에 달한다고 한다. 이처럼 고객 정보 유출 등 기밀 자료 유출로 인한 기업들의 피해 사례에서 확인 할 수 있는 것처럼 정보 보호는 간과할 수 없는 기업의 운영에 중요한 활동으로 자리 잡았다(이상준, 2008).

특히 기업 정보의 유출에 대한 기업 자체의 방어 노력은 최근에 더욱 구체화 되고 있으며 학계에서도 많은 연구가 이루어지고 있는 실정이다. 지금까지 기업들은 기업 정보를 보호하기 위해 전형적으로 보안 시스템 구축, 백신, 방화벽 설치 등과 같은 기술적인 측면에 더 중점을 두었다. 그러나 기업에서 증가하는 보안 위협을 관리하고 통제하기 위해서 주로 사용하는 바이러스 예방 프로그램이나 침입통제 같은 기술적 측면에만 의존하는 것은 여전히 정보 유출의 가능성을 남겨두고 있다. 따라서 이를 보완하기 위해 보안 위협에 대한 개인 행동이나 보안 기술을 사용하는 조직 구성원을 대상으로 한 연구가 활발하게 이루어지고 있다(Goodhue, 1991; Straub and Welke, 1998). 또한 안전하게 기업의 정보와 시스템을 보호하기 위해서는 기술적인 측면보다 관리적 측면 즉, 효과적인 보안 정책을 세우고 이를 조직 구성원들이 실행할 수 있도록 동기 부여를 하는 것도 중요하다(Amitava and McCrohan, 2002). 2008년 8월 한국산업기술보호협회가 지식경제부와 공동으로 1176개 기업·기관을 상대로 조사에 따르면, 하드웨어 측면에 해당하는 물리적·기술적 보안은 상대적으로 만족도와 효과가 높은 반면 소프트웨어 측면에 해당하는 관리적·인적 보안은 상대적으로 낮은 수준으로 나타났다. 그 중에서도 특히 인적 보안은 만족도와 효과가 가장 낮은 것으로 조사되었다.

이러한 인적 보안에 대한 만족도와 효과 개선 및 조직 구성원들의 정보 보안에 대한 동기부여를 위하여 기업은 정보 보호에 관련된 교육에 힘을 쓰기 시작하였다. 이러한 교육의 목적은 기업의 정보 보안에 사람의 특성 및 태도에 대한 중요성이 대두되면서 회사에서 투자한 보안 시스템의 효과적인 활용뿐만 아니라 필요한 통제에 대한 보안 정책의 중요성도 널리 알리기 위함이다. 하지만 아직까지 기업의 보안 교육은 광범위하게 이루어지고 있지는 않은 실정이다. 최근 3년간 사내에서 산업기술보호교육을 실시한 경험이 있다고 응답한 기업은 34.1%에 불과했으며 기업 간 격차도 크게 나타났다. 종업원 1000명 이상 기업은 72.3%가 교육을 실시했다고 한 반면 300명 미만의 기업은 27.6%에 불과하였다(이경기, 2008).

국내외로 기업 정보 보호를 위하여 조직 구성원 차원에 대한 관심은 높아지고 있으나 문헌 연구 결과 대부분의 조사는 산업적 특성, 최고 경영층의 보안에 대한 관심 여부, 보안에 대한 경제성 등을 중심으로 이루어졌으며 이는 모두 기업을 대상으로 이루어지고 있다는 것을 알 수 있었다. 이러한 배경을 바탕으로 본 연구의 주제는 다음과 같이 정리될 수 있다.

- 기업에서는 조직 구성원의 정보 유출을 막기 위해 어떤 점에 중점을 두어야 하는 것일까?
- 기업에서는 추진하는 정보 보호 정책이나 시스템은 과연 개인의 행동이나 태도에 영향을

줄 수 있을까?

- 기업의 정보 보호 활동에 대한 교육만으로 조직 구성원의 태도에 변화를 주지 못한다면 구성원의 개인적인 어떤 특성이 보안에 관련된 태도에 영향을 주는 것일까?

본 연구의 목적은 상기의 연구주제에 초점을 맞추어 기업에서 실시하는 정보 보호를 위한 노력에 대해서 개인이 인지하고 있는 부분을 찾아내고, 그러한 변수들이 개인의 보안 태도에 어떠한 영향을 주는지 알아보는 것이다. 그러나 조직 구성원의 태도는 기업의 정보 보호 활동 노력에만 직접적으로 영향을 받거나 조직의 노력에만 따르는 것으로 결정되지는 않을 것이다. 따라서 본 연구에서는 기업의 보안 활동 외에 조직 구성원의 개인적 특성에 대한 부분도 함께 고려하여 어떠한 변수가 가장 개인의 보안 태도에 영향을 미치는지 여부도 함께 살펴보고자 한다.

## II. 이론적 배경

### 2.1 기업의 정보 보호

정보 보호(Information security)란 정보의 입력, 처리, 저장, 출력, 전송 등의 모든 단계에 걸쳐서 시스템을 보호하는 것을 말한다. 미국에서는 정보 보호를 "시스템 및 정보를 고의 혹은 실수에 의한 공개, 변조, 파괴 및 지체로부터의 보호하는 활동"이라고 정의하고, 유럽에서는 "전자적인 형태의 정보를 처리하거나 저장하는 모든 단계에 걸쳐서 정보를 보호하는 활동"으로 정의 하고 있다(박태완, 1997). 또한 정보 보호는 다양한 내·외적인 위협들로부터 조직의 손실을 최소화하고 이익을 극대화하는 것을 의미하기도 한다(Finne, 1998).

이러한 정보 보호를 위한 기업 자체의 방어 노력은 1960년대부터 출발하였다고 볼 수 있는데, 초기에는 주로 암호 관련 알고리즘이나 조직의 운영 시스템에 대한 보안에 집중되었다. 1980년대 중반 이후에는 컴퓨터 간의 통신 즉, 암호 프로토콜을 이용한 컴퓨터 침투와 관련된 보안에 연구가 많이 이루어졌으며, 1990년대에 들어서는 시스템 측면의 보안뿐만 아니라 보안 주체 즉 사람에 대한 요소도 고려되기 시작했다(Trcek *et al.*, 2007).

지금까지 기업에서 기술적인 측면 중심으로 보안에 대해 접근한 이유는 대부분 시스템을 통해 중앙집권적으로 조직을 통제하는 것이 가장 쉬운 방법이었기 때문이다. 하지만 이 방법이 가장 효과적이라고 말 할 수는 없다(Dhillon and Backhouse, 2000). 다양한 연구 결과와 기업의 정보 유출로 인한 빈번한 사고를 통해 알 수 있듯이 기업 보안의 가장 큰 문제점은 시스템으로 인한 사고보다는 내부 인원에 의한 사고가 많기 때문이다. 2006년 국가정보원이 실시한 산업스파이 적발사건 현황과 첨단 산업기술보호 동향이라는 주제의 보고서에 따르면 실제로 기업의 기술유출사고의 80% 이상은 전·현직 직원에 의해 발생하며, 협력업체 직원까지 포함했을 때 그 비율은 90% 이상이 되었다. 이에 Dhillon과 Backhouse(2000)는 시스템을 사용하는 주체가 인간이기 때문에 사회적, 조직적 이슈가 중요하다고 지적했다. 실제로 시스템과 상호작용하면서 시스템에 대해 책임지는 것은 인간이기 때문이다. 달리 생각해보면 기업이 조직 구성원의 행동을 보안에 대한 교육이나 보안 관련 보상이나 처벌을 통해 적절하게 통제하게 된다면 기술적

인 접근 보다 훨씬 효과적일 수도 있다는 것을 뜻하기도 한다(Straub, 1990).

정보 보호를 위한 전제, 즉 조직 구성원들이 항상 어떤 위험과 불확실성에 노출 되어 있다는 것은 사람들에게 이해시키기 어려운 개념이다. 그러나 기업의 측면에서는 정보 보호와 관련해 어떤 결정을 내릴 것인가, 직원들을 어떻게 인도할 것인가를 먼저 생각하는 것이 매우 중요하다. 예를 들어 단순하고 직관적인 인터페이스를 갖춘 보안 시스템을 구축하였다고 하더라도 직원들이 보안 경고를 무시해 버리는 경우나, 권고한 내용 대신 형편없는 시스템 설정을 선택해 버리는 경우, 의도적으로 회사 정책을 무시하는 경우에는 전혀 기업의 정보 보호에 도움을 주지 못한다. 시스템 보안에서 사용자 문제는 사용자 인터페이스나 시스템의 상호 작용과 전혀 무관하기 때문이다(West, 2008). 지금까지 대부분의 연구가 기업을 대상으로 이루어졌으며 만족도 혹은 경제성에 대한 효과 측정이었으므로 개인의 보안 활동에 대한 직접적인 효과 측정은 아니다(김종기 · 강다연, 2008). 실제로 개인의 보안 인식에 대한 효과를 객관적으로 측정하기는 어려운 부분이 있으므로 본 연구에서는 직원들이 정보 보호에 대한 태도를 중심으로 분석해보고자 한다.

### 2.2 기술수용모델(TAM, Technology Acceptance Model)

정보기술이 도입되면서 학계에서는 사람들이 이를 어떻게 받아들이는지에 대한 연구가 지속적으로 이루어 졌는데, 현재 가장 널리 쓰이는 것은 기술수용모델(TAM, Technology Acceptance Model)이라고 할 수 있다. 기술수용모델은 정보기술에 관련하여 사람들이 이를 받아들이고 활용하는 행동을 설명하는 모형으로 널리 쓰이고 있으며 가장 설명력이 높은 모형으로도 인정받고 있다. 사람들의 태도에 영향을 주는 많은 변수들이 있지만 기술수용모형에서는 사용자의 수용태도가 인지된 유용성(Perceived usefulness)과 인지된 이용 용이성(Perceived ease of use)으로 구성 된다(Davis, 1989).

Davis(1989)는 인지된 유용성을 "정보기술이 자신들의 성과를 높이는데 도움을 줄 것으로 믿는 정도"로 정의하였으며 이는 기술을 수용하는 것이 수용하지 않고 살아가는 것보다 더 낫다고 지각되는 정도이다. 또한 인지된 이용 용의성은 "특정 시스템의 사용이 많은 노력을 필요하지 않을 것이라고 믿는 정도" 또는 "해당 기술을 사용하기 위한 수고에서 자유로운 정도"로 정의하였다. 즉, 정보 기술을 받아들이는 사람들이 그 정보 기술이 유용함은 알지만 사용하기 어렵고 그 기술을 사용함으로써 얻는 이익보다 기술을 사용하는데 드는 노력이 더 큰 경우 그 기술을 받아들이지 않는다는 것이다.

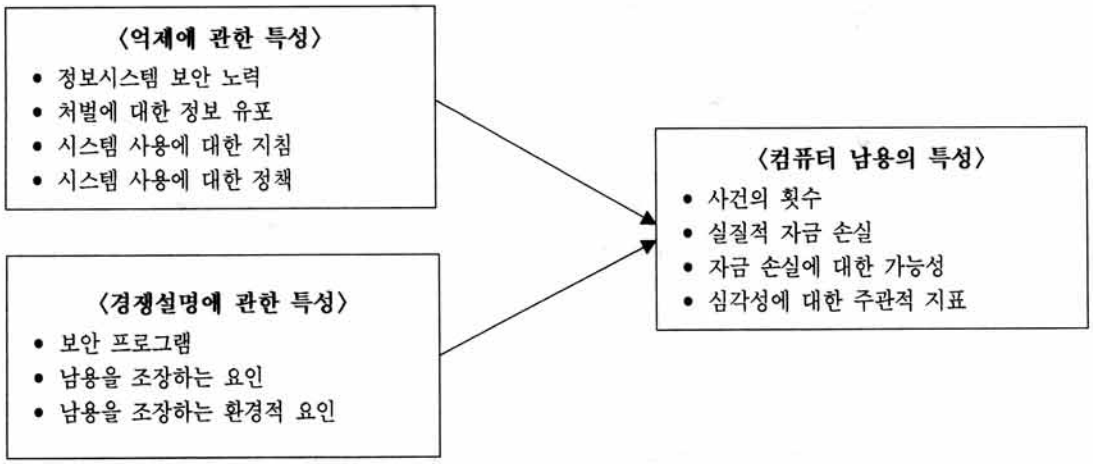
본 연구에서는 기술수용모델을 활용하여 정보 보호에 관련된 부분을 유용성과 용이성에 따라 구분하고, 개인의 보안태도는 조직 내에서 어떠한 요소에 의해 영향을 받는지 살펴보았다. 기업에서 실시하는 여러 가지 정보 보호에 대한 노력들을 인지된 유용성이 강조되는 부분과 인지된 사용 용이성이 강조되는 부분으로 나누어 조사하고, 개인의 수용태도에 어떠한 영향을 미칠 것인지 분석한다. 수용태도는 개인의 보안태도로 정의하고, 이에 영향을 미치는 요소를 기업의 자발적 노력에 의한 것과 개인의 특성에 의한 것으로 구분하였다. 먼저 기업이 정보의 오남용을 방지하기 위해 자발적으로 노력하는 부분에 대한 이론적인 바탕을 다음 장에서 살펴보고자 한다.

### 2.3 억제이론(Deterrence theory)

억제이론은 범죄학에서 출발한 이론으로 사람들에게 범죄로 얻는 이득보다는 범죄를 행한 후에 입는 피해가 더 크다는 것을 알려줌으로써 사람들이 범죄를 저지르지 않도록 하는 이론이다. Lebow와 Stein(1990)은 억제(Deterrence)를 바람직하지 못한 행위를 하려는 행위자로 하여금 행위의 비용이 이익보다 많다는 사실을 확인시킴으로써 그런 행위를 예방하고자 하는 것으로 정의했다. 이를 위하여 첫째, 방어자가 수용할 수 없는 행위를 정의하고, 둘째, 침략자를 응징하거나 단속하겠다는 약속을 표방하며, 셋째로는 그러한 의지를 과시하고, 마지막으로 이러한 위협을 실행할 능력을 갖추어야 한다고 설명하였다. 간단히 설명하면 억제란 상대방에게 그가 감당하기를 꺼려하는 위협을 노출시킴으로써 상대의 행위를 예방하거나 단념시키는 행위로 규정할 수 있다(전성훈, 2004). 이러한 억제는 상대방이 특정한 행위를 하지 못하도록 하는 소극적인 영향력을 행사하는 것으로 심리적인 부분이 크게 작용한다.

억제이론은 전쟁 같은 국가 간의 대립, 핵전략, 테러방지 등에도 다양하게 적용되어 왔으며, 정보보호연구로의 적용은 정보화가 시작되는 시기와 맞물리는데 국내에서 보다는 해외에서 이론적 연구가 활발했다. 특히, Straub(1990)는 여러 연구자들과 더불어 억제 이론을 정보 보호에 적용한 연구를 많이 진행하였는데 특히, "Effective IS Security: An Empirical Study" 연구에서 억제이론을 활용한 새로운 모델을 제시하였다(그림 1 참조). 이 연구에서는 정보 보호를 위한 노력과 처벌에 대한 부분, 시스템 사용에 대한 지침과 정책으로 대표되는 억제요소가 컴퓨터 남용에 영향을 준다는 결과를 발표하였다.

1998년에 발표된 Nance와 Straub의 연구에서는 "Security Action Cycle"을 통하여 과정을 억제(Deterrence), 예방(Prevention), 탐지(Detection), 치료(Remedy)의 4단계로 구분하고 각 단계마다




자료: Straub, D. W.(1990), "Effective IS Security: An Empirical Study", p. 26

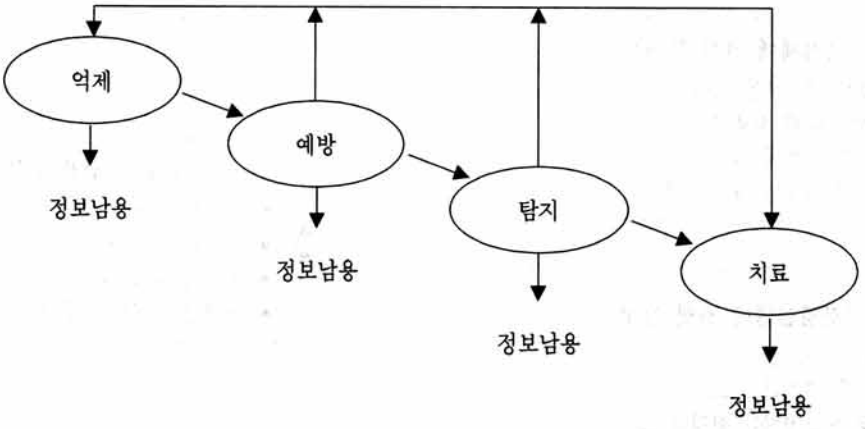
〈그림 1〉 보안 영향 모델( The security impact model)

정보의 남용이 이루어질 수 있다는 것을 증명하였으며 각 단계별 정보 보호 활동이 반복적으로 이루어진다는 것을 설명하였다. 즉, 처음에는 기업이 정보 보호를 위해 억제(Deterrence) 요소를 활용하지만 정보 남용이 발생하고 이를 방지하고자 예방(Prevention) 조치를 실시한다. 하지만 이 단계 역시 정보 남용이 발생하게 되고 탐지(Detection) 등의 노력을 하게 된다. 지속적인 모니터링 등을 통해 정보 남용을 방지하고자 하지만 정보 남용은 계속 발생하고 조직 구성원의 처벌과 보상 등을 실시하는 단계를 실시하게 되는 것이다. 이러한 단계적인 노력은 억제와 관련된 피드백을 통하여 보안 활동을 지속되게 한다(Theoharidou, 2005).

각 단계의 기업의 구체적인 노력에 대한 예시는 여러 문헌에서 다루고 있는데 첫째, 억제(Deterrence) 요소는 사람들로 하여금 제재에 대한 두려움을 통하여 범죄적 행동을 못하게 하는 시도를 뜻하며 보안 정책, 가이드라인 같은 수동적인 조치를 의미한다. 이에 반해서 예방(Preventive) 요소는 기업 내에서 시스템 보안, 특화된 보안 소프트웨어 설치, 비밀번호 관리 등의 통제(Control)를 통하여 범죄적 행동을 못하게 하려는 노력을 뜻한다. 이외에 탐지(Detection) 요소는 보안을 저해하려는 의심 행동을 스캐닝하거나 시스템 감시, 바이러스 조사 등의 모니터링 요소를 포함하고 있다. 마지막으로 회복(Recovery) 요소는 연구가 거듭되면서 치료(Remedy)의 요소로 전환되었으며 기업에서 실시하는 보상과 처벌을 의미한다.

### 2.4 통제이론(Control theory)

통제이론은 억제이론과 마찬가지로 개인의 잘못된 행위에 대한 원인을 탐색하는 연구 중의 하나이다. 억제이론과는 달리 통제이론에서는 잘못된 행동이 부정적 영향으로 인해 발생하기 보다는 긍정적 영향의 부재 속에서 발생하는 것으로 본다. 통제이론의 대표적인 논의는 허쉬(Hirschi)의 이론을 통해서 살펴 볼 수 있는데 먼저 그 기본적 가정




자료: Theoharidou *et al.*(2005), "The insider threat to information systems and the effectiveness of ISO17799", p. 475.

〈그림 2〉 보안활동주기 (Security action cycle)

은 모든 사람들이 일탈에 대한 동기를 어느 정도 가지고 있다는 것이다. 따라서 통제이론에서는 왜 사람들이 사회의 규칙에 복종하는가라는 질문에 관심을 가지게 된다. 일탈은 당연하다는 가정 하에 순응이 설명되어야 한다고 보는 것이다(Hirschi, 1969). 이에 대해 통제이론이 제시하는 답은 사회통제가 범죄를 저지르는 것을 막기 때문에 사람들이 순응한다는 것이다. 그리고 사회통제가 약하거나 깨질 때 일탈이 발생한다는 것이다. 이러한 사회통제이론은 이론적인 관점에서 볼 때 조직 내에서의 적절한 통제유형에 관한 논의는 주로 업무의 특성과 관련이 있었다. 즉, 특정한 업무가 가지고 있는 다양한 특성에 부합되는 통제방식을 사용하면 통제의 실현가능성이 높아지고 집행도 수월하다는 것이다(Govindarajan and Fisher, 1990).

사회통제이론 역시 정보 보호에 관련된 연구에서도 많이 활용되었는데, Kirsch와 Boss(2007)의 "Security behavior model"에서는 통제의 요소를 3개로 구분하여 개인의 보안 인식에 영향을 미친다고 하였으며, 이에 해당하는 요소는 다음과 같다. 첫 번째는 업무 상세(Specification)로 직무에 관련된 내용을 얼마나 상세하게 기술하였는지에 대한 내용이 포함되며 두 번째는 평가(Evaluation) 사항으로 개인의 행동이나 결과에 대한 정확한 평가에 관한 사항이며 마지막으로는 조직의 보상(Reward)과 처벌(Punishment)을 들고 있다.

본 연구에서는 통제이론과 억제이론에서의 공통적인 요소를 기업의 보안에 대한 노력으로 정하고, 정책 그리고 교육에 대한 유용성과 보안 시스템에 대한 용이성 인식이 개인의 태도에 어떤 영향을 살펴보는지 알아볼 것이다. 실제로 억제이론과 통제이론에서 제시하고 있는 요소들은 공통되는 부분이 발견된다. 특히 기업을 대상으로 하는 경우에 적용되었을 때 시스템적인 부분을 제외하고는 나머지 세 분야가 비슷한 분야를 핵심요소로 선택하고 있다〈표 1 참조〉.

억제이론과 통제이론 모두 기업의 정보 보호 활동을 설명하는 연구에 적용되었으므로 공통된 연구변수들을 살펴보면 기업에서 실시하는 정책적인 측면, 감시나 평가를 위한 시스템 부분, 처벌과 보상 부분 등을 선택 할 수 있으며, 변수에 대한 조작적 정의는 다음 장에서 살펴보도록 한다. 본 연구에서는 조직의 정보 보호 활동 중 구성원의 태도에 영향을 미치는 요소 중에서 억제이론 혹은 통제이론과 관련된 '정책', '시스템', '보상과 처벌' 요소를 앞서 기술한 인지된 유용성과 인지된 용이성에 관련하여 변수로 추출하고 관련 연구를 실시하였다. 추가적인 변수에 대해서도 모형과 가설을 통해 상세하게 정의하고 분석하였다.

〈표 1〉 억제이론과 통제이론 요소 비교

| 억제이론요소 | 항목 | 통제이론요소 |
|---|---|---|
| 억제 | 정책, 지침 관련 | 명세 |
| 예방 | 물리적, 시스템적 대책 | |
| 탐색 | 모니터링 및 평가 | 평가 |
| 치료 | 보상 및 처벌 | 보상 및 처벌 |

## III. 연구모형 및 연구가설

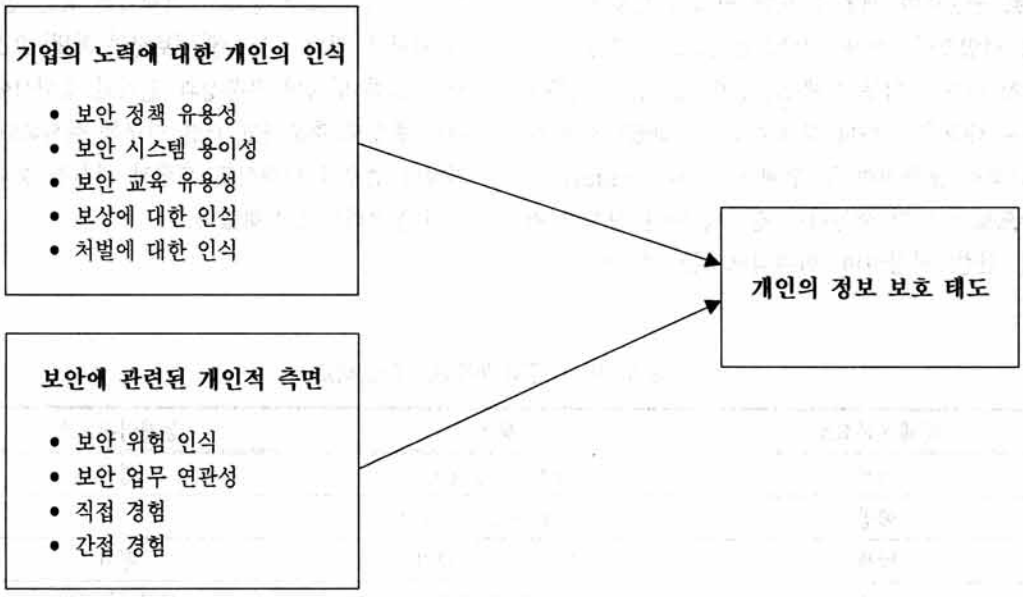
### 3.1 연구모형

앞서 기술수용모델(TAM)의 마지막 부분에서 살펴본 봐와 같이 본 연구에서는 수용 태도는 개인의 보안태도로 정의하고, 이에 영향을 미치는 요소를 기업의 노력에 대한 개인의 인식과 보안과 관련된 개인적 측면으로 구분하여 분석하고자 한다. 그리고 억제이론과 통제이론에서 발견되는 공통적인 요소(정책, 시스템, 보상 그리고 처벌)를 감안하여 아래와 같은 연구모형을 제시한다.

### 3.2 연구가설

개인들이 보안과 관련하여 반사회적인 행동을 하지 못하도록 하는데 가장 핵심적인 부분을 설명하기 위한 억제이론에서는 잠재적으로 정보 유출을 시도하고자 하는 사람들에 대한 통제가 필요하다고 가정하였으며, 이러한 가정은 정책으로 대변되는 활동과 위반 행위에 대한 처벌을 동반하는 것이라고 주장하였다(Straub and Nance, 1990).

여기에서 정책은 조직이 적절하고 안전한 시스템 사용을 위하여 제시하는 지침이라고 볼 수 있으며 조직의 정보 보호를 위한 보안 책임자들의 제시하는 가이드라인이다. 기업에서는 정보 보호를 위해서 다양한 정책이 제시되고 있으나 지속적인 정보 유출 사건이 발생되고 있다. 따라서 Wiant(2005)는 억제 이론을 활용하여 정보 보호에 관련된 요소 중에서 정책에 대한 부분에 초점을 맞추었으며 정책과 개인의 인식과의 관계를 살펴보았다. 특히, 자신의 연구에서 "The incident awareness model"을 제시하고 정책이 기업에서 발생하는 보안 사고




〈그림 3〉 연구모형

에 대한 인식에 영향을 준다고 하였다. 하지만 이 연구는 연구 대상이 병원에 종사하는 사람들에 대한 연구이므로 일반 기업에 확장할 필요가 있다.

Hayam과 Oz(1993)는 정보를 보호하기 위해서는 관리팀의 역할, 보안정책의 유무, 보안문제에 대한 홍보 그리고 이러한 활동에 필요한 예산의 할당과 자금지원이 중요하다고 강조하였으며, Poore (1980)는 정보를 보호하기 위한 보안정책과 예산 지원이 중요함을 실증분석을 통해 밝혔다. 조직내에서 효과적으로 정보를 보호하기 위한 첫 단계는 보안정책 수립하고 이를 조정하고 그리고 보완하는 것이다(von Solms and Meyer, 1995).

이러한 내용을 바탕으로 조직의 구성원들이 보안정책을 어떻게 받아들이고 있는지를 조사하기 위해 보안 정책의 유용성에 대한 가설1을 도출하였다.

H1: 인지된 보안정책의 유용성은 기업 정보 보호에 대한 조직 구성원의 태도에 직접적이고 긍정적인 영향을 미친다.

정보화의 확대로 인하여 국가 및 사회, 개인간의 정보 경쟁이 치열해짐에 따라 정보 보호의 중요성이 더욱 높아지고 있으며, 이에 정보 보호 시스템의 사용이 증가하고 있다. 기업의 정보 보호 시스템은 크게 프론트 앤드 시스템(Front end system)과 백 앤드 시스템(Back end system)으로 구성된 네트워크 기반 구조에서의 접근과 서버 자체환경으로의 접근으로 분류할 수 있다. 프론트 앤드 시스템은 클라이언트/서버(Client/Server) 환경에서 인터넷 환경에서처럼 신뢰할 수 없는 네트워크에 속한 외부 사용자, 내부 사용자들이 접근하여 자료를 얻거나 거래를 요청하는 시스템을 말한다. 백 앤드 시스템은 요청된 거래를 처리하고 데이터베이스의 갱신이 이루어지는 시스템을 의미하며 내부 사용자들이 필요한 자료를 요청하여 이를 이용하거나 신규로 생성된 데이터를 입력하는 일련의 과정을 뜻한다(Vassilacopoulos and Peppes, 1996).

Straub와 Welke(1998)는 기업의 정보 보호 활동은 시스템에 대한 위험을 관리하는 것만으로는 충분하지 않다는 연구배경을 바탕으로 기업에서 관리자의 역량이 중요할 것이라는 전제를 바탕으로 질적 연구를 수행하였다. 본 연구에서 '포춘(Fortune)지' 500대 기업을 대상으로 조사한 결과 보안에 대한 전문 지식의 결여, 적절한 조치 그리고 시스템 사용법에 대한 이해 부족으로 인해 위험에 노출되는 경우가 많다는 사실을 밝혔다.

Venkatesh(2000)에 따르면, 인지된 이용 유용성이 정보기술에 대한 사용자 수용과 이용행태에 영향을 미치는 중요한 요소임을 증명한 연구는 많이 수행되었지만 인지형태나 변화가 어떻게 이루어지는 지에 대한 연구는 부족한 점을 강조하였다. 그는 자신의 연구에서 시스템의 인지된 이용 용이성의 결정요인에 대한 부분을 사용자의 관점과 연계하여 분석하였다. 특히, 그는 사용자가 새로운 시스템의 이용 용이성에 초기에 결정함에 있어 판단기준으로 통제(Control), 본질적 동기(Intrinsic motivation) 그리고 감정(emotion)이 될 수 있다는 모델을 제안하고 이에 대해 분석했다.

보안을 위해 실제 정보 보호 시스템의 신뢰성 확보를 위한 제도적 장치로서 평가기준 및 평가, 인증 제도도 개발되어 국내외적으로 많이 시행되고 있으나, 실제 조직 구성원이 정보 보호 시스템을 다루는 부분에 있어서의 연구는 부족한 실정이다.

시스템적 측면은 대부분 기업 시스템의 구축 단계에서 설계되고 반영되는 것이 대부분이며 조직 구성원이 직접적으로 접근하는 분야는 주로 방화벽

설치, 바이러스 통제, 접근 통제 소프트웨어, 조직 구성원의 인증 등의 경우이다. 시스템에 대한 조직 구성원의 사용에 관련하여 본 연구는 이러한 개인이 직접적으로 다루는 시스템 분야를 중심으로 하였으며, 특히 사용시에 어느 정도 편리하게 이용할 수 있는지에 대해 초점을 맞추어 가설2를 도출하였다.

H2: 인지된 보안시스템의 사용 용이성은 기업 정보 보호에 대한 조직 구성원의 태도에 직접적이고 긍정적인 영향을 미친다.

최근 안중호 등(2010)은 윤리교육이 각 조직 구성원들이 정보보안정책을 준수하는데 있어서 어느 정도 효과가 있는지를 분석하고, 조직 구성원들이 조직유형에 따라 성향 차이가 있는지를 파악하여, 조직 구성원의 행위 변화가 자기통제를 이끌어내는 방법에 대하여 연구하였다. 이 연구에서는 조직유형에 관계없이 윤리교육이 정보보안준수에 긍정적인 영향을 주는 핵심요인임을 확인하였다. 이는 정보보안정책의 수립과 시행은 조직형태 및 특성을 이해하고 추진해야 함을 암시한다. 따라서 조직은 정보보안정책의 수립 시 조직형태 및 특성에 따른 구성원의 성향을 먼저 인식하고, 구성원의 성향 차이를 정보보안정책에 반영한다면 정보보안정책을 수립하는데 더 큰 효과를 거둘 수 있을 것이다.

오창규와 김종기(2003)는 정보보호 교육 및 훈련을 통해 정보보안인식을 제고함으로써 지속적인 정보보호 실제 행동을 촉진할 수 있다는 것을 밝혔다. 백민정(2010)은 정보보안행동 수준 향상을 위한 개선 방안으로 보안교육의 중요성을 언급하였으며, 보안 교육을 통해 정보보안행동이 습관화 되도록 반복적인 교육과 보안지식 또는 기술교육을 통해 개선해 나가야 함을 강조했다.

그리고 기업 교육 효과에 핵심적인 Piccoli 등(2001)연구에서는 교육 효과에 대한 변수를 업무 달성 정도나 업무에 관련된 시간 등 그 수행정도(Performance)와 교육 경험에 대한 만족도(Satisfaction)외에도 자존감(Self-efficacy)을 새로운 요소로 넣어 교육 효과에 대한 평가하였다. 그러나 이번 연구에서는 자존감에 대한 부분은 다루지 않기로 한다.

기업에서 실시하는 교육은 다양한 형태로 진행되고 있는데, 본 연구에서는 정보 보호와 관련해서 조직 구성원들에게 전달하는 모든 세미나, 교육 및 훈련 등 모든 분야를 교육으로 통칭한다. 또한 이러한 기업의 전달이 직원들에게 얼마나 정보 보호와 관련된 태도에 영향을 미치는 지를 알아보고자 다음의 가설을 도출하였다.

H3: 보안교육은 기업 정보 보호에 대한 조직 구성원의 태도에 직접적이고 긍정적인 영향을 미친다.

이선경(2010)은 "기업의 정보보호 정책과 구성원들의 정보보호 태도"라는 주제의 학위논문에서 보상, 처벌 그리고 정보보호교육이 기업의 정보보호 및 보안에 직접적이고 긍정적인 영향을 미친다는 것을 실증분석을 통해 증명하였다.

일반적으로 조직 구성원의 노동 동기를 자극하는 수단으로 보상을 생산성과 연계하기 위한 대표적인 노력은 성과주의 보상시스템의 도입 및 강화로 나타난다(Vroom, 1964). 이는 기업에서 실시하는 보상이 정보 보호를 위한 노력에 연계하여 직무수행의 수준이나 직무성과에 따른 보상은 구성원의 노동 동기를 자극할 수 있는 방법이 될 수 있을 것

이다. 조직 구성원이 보상에 대해서 불공정성이 지각되면 개인은 심리적으로 불편함을 느낄 것이며 자신의 공헌과 기여에 대한 불균형으로 조직에 참여하려는 의지가 약해질 것이다(한주희, 2006). 특히 기업의 정보 보호에 있어서 개인의 역할은 매우 큰 만큼 적절한 보상이 지원된다면 높은 수준의 보상을 받기 위해 동기가 유발 될 것이고 실제 업무에서도 보안에 민감하게 반응할 것이다. 따라서 조직의 보상에 관련된 여러 연구에서 네 번째 가설이 추출되었다.

H 4a: 인지된 보상의 유용성은 기업 정보 보호에 대한 조직 구성원의 태도에 직접적이고 긍정적인 영향을 미친다.

억제이론은 오랜 기간 연구되어왔다. Blumstein (1978)은 범죄에 대한 행위를 저해하는 부분에 초점을 맞춘 연구를 진행하였으며 처벌의 확실성과 처벌의 엄격성 2가지에 의해서 반사회적인 행동을 줄일 수 있다는 것을 이론적으로 설명하였다. 이 연구에서는 잠재적인 범죄자가 반사회적인 행동을 조절하려고 한다는 것을 가정하였다. 다시 말해서 사람들은 어떤 방침(Policing)에 반응한다는 것을 가정을 바탕으로 효과적인 방침과 처벌은 서로 관련이 있다는 것을 밝혔다.

안중호 등(2010)은 정보보안 사고의 원인은 정보보안 통제를 지키지 않고 이를 위반하는 개인의 행위와 밀접하게 관련되어 있다고 밝히면서 개인의 행위에 대한 자발적 통제를 이끌어내고 이를 감독하는 것이 정보보안을 유지하는데 있어서 근본적이고 핵심적인 해결책이 될 수 있다고 주장했다. 그는 처벌이 정보보안준수에 긍정적인 영향을 주는 핵심요인임을 확인하였으며 더불어 단일형태 조직 구성원에 비해 다분할 형태 조직 구성원이 처벌에 대한 인식이 높고 공공조직 구성원이 민간조직 구성원보다 처벌에 대한 인식이 높다고 주장하였다.

최영찬(2008)은 억제이론을 활용하여 처벌의 확실성과 처벌의 엄격성이 증가하면 조직 구성원의 태도에 긍정적인 영향을 미친다는 결론을 도출하였다. 특히 개인의 태도에는 처벌의 확실성 보다 처벌의 엄격성이 더 큰 영향을 미친다는 결과가 나왔으며 이는 일반적으로 처벌의 확실성과 처벌의 엄격성은 모두 유의한 영향을 주는 것으로 나타난 선행 연구와는 차이가 있다. 상기의 연구는 베트남 사례를 통한 분석이 이루어졌다. 따라서 본 연구에서는 국내의 조직 구성원을 대상으로 조사를 실시하였다. 또한 처벌의 확실성과 엄격성을 구분하기 보다는 조직 구성원이 인식하고 있는 억제 노력을 처벌로 통일하여 본 연구에서는 처벌의 인지만을 다루기로 한다.

H 4b: 인지된 처벌의 유용성은 기업 정보 보호에 대한 조직 구성원의 태도에 직접적이고 긍정적인 영향을 미친다.

지금까지의 가설 도출은 기업에서 보안을 위해 노력하는 요소들에 대한 개인의 인식을 바탕으로 한 것이다. 그러나 개인의 직접적인 보안 활동은 오로지 기업의 노력을 따르는 것만으로 결정되지 않을 것이므로 개인적인 측면을 추가하였다.

위험은 손실 가능성 또는 어떤 의사 결정이 의도한 바와 같이 실현되거나 실현 될 수 있는 불확실성의 정도를 말한다. 위험에 대한 태도 즉, 위험한 상황에서 개인이 취한 의사 결정이 위험을 내포하고 있는 정도를 위협행위라고 하며 이에 대한 결정요인으로 위험 선호, 위험 지각, 위험 성향이 있

다. 여기에서 위험 지각은 어떠한 상황에 내재되어 있는 위험을 의사결정자가 지각할 확률을 말한다. 이러한 위험에 대한 지각은 위험한 상황에 주의를 기울이고 대응할 수 있는 개인의 능력, 위험한 상황을 평가하는 방법 등 다양한 요인에 의해서 영향을 받는다. 보안에 대한 개인의 위험인식은 여러 연구에서 다루고 있는데, 특히 인터넷 뱅킹이나(이웅규, 2005) 웹을 통한 전자 상거래(손달호, 2005) 등에 대한 보안 요인의 영향연구 등에서 살펴 볼 수 있다. 최근의 보안 통제에 대한 개인 인지도 영향에 대한 연구에 따르면 인터넷과 관련한 e-business 보안에 대한 기술적인 접근의 한계를 극복하고자 보안 통제에 대한 인지도에 초점을 맞추는 연구들이 늘고 있는 추세이다(서보일, 2006).

대부분의 연구 결과가 개인의 위험 인식은 직접적으로 개인의 태도에 영향을 준다는 결과가 나타났으며 기업의 정보 보호 활동에 대한 측면에서도 어떤 영향을 주는지 살펴 볼 필요가 있으므로 가설 5를 아래와 같이 도출하였다.

H5: 보안에 관련된 위험 인식은 기업 조직 구성원의 태도에 직접적이고 긍정적인 영향을 미친다.

개인의 정보기술 수용에 있어 지각된 용이성과 유용성이 개인의 태도에 영향을 미친다는 TAM 모형은 다양한 이론을 기반으로 지속적으로 연구가 이루어져 왔다. 특히 Festinger(1957) 인지부조화이론(Cognitive Dissonance Theory)에 따르면 신념, 태도 그리고 지식과 같은 인지적 요인과 행위가 일치하지 않을 때 부조화 관계(Dissonant relationship)가 발생하고 이것은 심리적 불편(Psychological uncomfortable)을 야기 시키며, 그 불편을 감소시키기 위해 인지적 요인인 태도를 변화시킨다는 이론이다. 즉, 과거의 경험(행위)이 현재의 태도에 영향을 미친다는 것으로 정보기술 수용의 경우 사용 경험을 통해 시스템에 대한 신념과 태도가 변화하는 것을 이론적으로 설명할 수 있다. 또한 이 부분은 이제는 정보 기술이 일상화 되어 정보 보호 기술에 대한 개인의 경험과 지식은 새로운 정보 기술 수용에 중요한 역할을 한다고 할 수 있다(Cohen 1990).

개인의 정보기술 수용에 있어서 경험의 영향력을 심도 있게 다룬 연구는 Goodhue와 Thompson (1995)이 대표적이다. 그들은 개인의 PC 사용에 영향을 미치는 경험을 독립변수, 매개 변수, 조절 변수로 나누어 분석하였는데 이 때 독립 변수 역할과 조절 변수 역할은 지지되었으나 매개 변수 역할은 상대적으로 실증적 뒷받침이 가장 약한 것으로 나타났다. 여기에서 개인의 정보 기술 수용에 영향

〈표 2〉 보안 통제에 대한 인지도의 영향에 관한 연구

| 기존 문헌 | 적용분야 | 보안 관련 변수 | 내생변수 |
|---|---|---|---|
| 이웅규 | 인터넷 뱅킹 | 보안 우려 | 인터넷 뱅킹 사용<br>용이성 및 유용성 |
| 김종석 등 | 인터넷 쇼핑몰 | 인지된 보안 | 인지된 사용 용이성,<br>유용성, 태도, 사용의도, 실제 사용 |
| 민천홍 등 | 모바일 결제시스템 | 인증, 접근제어, 커뮤니케이션에<br>대한 인식 정도 | 범용성 |

을 미치는 요인으로 경험을 본 연구의 독립 변수로 차용하며 특히 정보 보안 태도에 어떠한 영향을 미치는지 살펴보도록 한다. 정보 보안의 경우 직접적인 피해 경험이 없다고 하더라도 미디어나 주변의 간접적인 영향으로 보안에 대한 태도도 달라질 수 있으므로 경험을 직접적 경험과 간접적 경험으로 나누어 분석하고자 한다.

H6a: 보안에 관련된 직접적인 경험은 기업 조직 구성원의 태도에 직접적이고 긍정적인 영향을 미친다.

H6b: 보안에 관련된 간접적인 경험은 조직 구성원의 태도에 직접적이고 긍정적인 영향을 미친다.

이명희와 유재언(2007)은 유비쿼터스 환경에서 사용자(User)가 시스템의 정보에 접근하기 위해 필수적으로 알아야 할 사항과 그 정보를 갖고 지정된 업무(task)를 완료하기 위해 정보를 수정해야 하는 필수적인 사항을 제한하는 보안모델을 정의하면서 조직 구성원의 업무와 기업의 정보보호 활동의 연관성에 대해 언급하고 이의 중요성에 대해 선행연구를 통해 설명하였다.

개인의 업무가 기업의 보안과 관련이 있을 경우 기업의 정보보호 활동에 영향을 미칠 수 있음을 연구한 대표적인 연구자들(Ting, 1988; Mahling *et al.*, 1990)은 업무가 보안과 관련이 있을 경우 기업 보안 활동에 정(+)의 영향을 미칠 수 있음을 밝혔다.

이러한 배경으로 바탕으로 개인의 업무와 정보보호 활동과의 연관성을 추가적으로 조사하기 위해 아래 가설을 설정하였다. 설문 항목은 업무와 관련해서 직접적인 관련이 있는지 여부와 업무를 위해서 직원이나 고객의 민감한 정보를 다루는지, 영업기밀, 회사 비밀 등의 정보를 다루는지에 대한 항목 3가지로 구성되었다.

H7: 개인의 업무와 보안 연관성은 기업 조직 구성원의 태도에 직접적이고 긍정적인 영향을 미친다.

## Ⅳ. 연구방법

### 4.1 자료수집 및 연구방법

기존 연구에 사용되었던 측정문항을 기반으로 설문지를 구성하였으며 여러 분야의 인력을 대상으로 인터넷을 통한 설문조사를 수행하였다. 설문조사의 응답자의 대부분은 정보 보호에 관련된 구체적인 노력을 실시하고 있는 기업을 대상으로 하였으며, 최종적으로 통계적 실증 분석을 수행하였다. 본 연구에 대한 자료 수집은 2008년 11월부터 12월 10일까지 약 5주간 온라인 설문을 통하여 회사에 근무하는 직장인을 대상으로 실시하였다. 설문회수율은 온라인 설문방법 특성상(누락된 문항이 있으면 설문 제출이 불가능) 100%였으며 총 242부의 온라인 설문지가 회수되었다. 우선은 수집된 242개의 설문을 모두 분석에 이용하였다.

모든 구성개념은 다항목 측정으로 구성되었으며 가설검정 이전 정화절차를 거쳤다. 예비조사기간 동안 관련업계 관리자와 연구자들이 측정항목을 검토하였고 수정하였다. 그리고 예비조사 결과에 대한 측정도구의 타당성 확보과정에서 5개의 측정문항이 제거되어 최종적으로 설문항목은 정보 보호에

관련된 항목과 인구통계학적인 항목을 포함하여 53개 문항으로 구성되었다. 인구통계학적 특성에 대한 문항을 제외하고 모든 측정문항들은 리커트 7점 척도로 구성되었다.

본 연구에서는 먼저 수집된 설문들에 대해서 요인 분석을 통해 각 설문의 타당성을 검토한 후, Cronbach's Alpha Test를 이용하여 신뢰도를 검증하였다. 그리고 추출된 각 요인간의 가설 검증을 위해서 회귀분석을 실시하였으며 본 논문의 실증분석을 위하여 사회과학 통계패키지인 SPSS for windows 12.0을 활용하였다.

### 4.2 측정문항의 개발

본 논문에서는 제안된 연구모델을 평가하고 구성개념의 조작적 정의를 위하여 관련 선행연구를 심층적으로 분석하였고 이를 토대로 최초 설문문항을 개발하였다. 이러한 과정에서 높은 수준의 신뢰성과 타당성을 확보하고자 하였다. 가능한 한 선행연구논문들의 측정문항을 원용하고자 하였으나 연구목적의 달성을 위하여 필요한 경우, 측정문항을 수정하였으며 개별 구성개념에 대한 조작적 정의는 〈표 3〉과 같다.

언급한 바와 같이, 종속변수는 개인의 보안태도이었으며, 기존 선행연구인 Davis(1989), Boss (2007)의 연구에서 사용한 측정항목을 7점 척도를 사용하여 질의하였다. 아홉 개의 독립변수는 선행연구에서 사용한 측정항목을 바탕으로 7점 척도를 사용하여 문항을 구성했다. 각각의 측정항목은 다음의 연구를 바탕으로 구성되었다. 우선 보안정책의 유용성 항목은 Kankanhalli(2003), Wint (2005)가 개발한 측정항목들로 구성되었다. 다음으로 보안시스템의 용이성 요인은 Vassilacopoulos 등 (1996)이 주장한 개념을 바탕으로 보안교육의 유용성 항목은 Piccoli(2001)가 개발한 항목을 활용하였다. 보상과 처벌 항목은 Vroom(1964)와

〈표 3〉 구성개념의 조작적 정의

| 구성개념 | 조작적 정의 | 관련 선행연구 |
|---|---|---|
| 보안정책의 유용성 | 기업의 정보 보호 관련 정책이 조직 구성원의 업무에 미치는 유용성 정도 | Gordineer (2003)<br>Kankanhalli (2003) |
| 보안시스템의 용이성 | 입출력 용이성, 검색 및 분석과정의 용이성, 도움말 기능의 다양성과 편리성 | Vassilacopoulos & Peppes (1996) |
| 보안교육의 유용성 | 조직의 성과나 목표 달성을 위한 사용자의 지각된 효과 | Piccoli (2001) |
| 보상과 처벌 | 금전적 보상뿐만 아니라 동기 부여적 측면 및 직무 만족 그리고 개인에게 돌아오는 불이익 | Vroom (1964)<br>Blumstein (1978) |
| 위험인식 | 조직에 있어서 발생 가능한 손실가능성 | Porter & Perry (1984)<br>Boss (2007) |
| 경험 | 직접경험, 이전경험, 과거이용 혹은 습관 | Cohen (1990)<br>Goodhue & Thompson (1995) |
| 보안태도 | 기술을 사용하는데 있어 개인의 느낌이나 감정 | Davis (1989)<br>Boss (2007) |

Blumstein(1978)의 연구를 바탕으로 위험인식요인은 Boss(2007)의 측정항목을 수정 없이 사용하였다. 모든 설문지 문항은 〈별첨 1〉에 별도로 제시하였다.

종속변수 그리고 독립변수와 더불어 분석에 네 개의 통제변수가 포함되었다. 우선 성별변수는 남자의 경우 0, 여자는 1로 더미변수 처리하였다. 그리고 업종은 빈도분석을 실시하여 6개의 분류를 4개(제조, 유통/서비스, IT/통신, 공공기관/기타)로 변환하여 네 개의 범주를 세 개로 만들어 더미변수로 전환하였다. 그리고 회사규모, 교육정도, 나이는 5점 척도로 평가되었다.

## V. 실증분석

### 5.1 표본특성 및 기초통계분석

분석에 사용된 대상은 총 242명이며, 표본의 인구통계학적 사항은 〈표 4〉와 같다. 기업을 대상으로 한 조사이므로 직장인을 대상으로 하였으며, 성별과 나이, 교육 정도의 기본 조사 외에, 기업의 규모와 기업의 산업유형, 직위 등을 추가로 조사하였다. 특히 모든 변수에 대한 확실한 측정을 위하여 근무하는 기업에서 정보보호와 관련된 정책이나

〈표 4〉 표본의 인구통계학적 특성

| 구분 | 빈도 | 비율(%) | 구분 | 빈도 | 비율(%) |
|---|---|---|---|---|---|
| 성별 | 158 | 65.3 | 직위 | | |
| 남자 | 84 | 34.7 | 사원급 | 110 | 45.5 |
| 여자 | | | 대리급 | 64 | 26.4 |
| | | | 과장급 | 44 | 18.2 |
| 연령 | | | 차장급 | 10 | 4.1 |
| 25세 미만 | 16 | 6.6 | 부장급이상 | 14 | 5.8 |
| 26-30세 | 98 | 40.5 | 회상규모 | | |
| 31-35세 | 76 | 31.4 | 0-50명 | 22 | 9.1 |
| 36-40세 | 40 | 16.5 | 51-300명 | 60 | 24.8 |
| 41-45세 | 6 | 2.5 | 301-1000명 | 36 | 14.9 |
| 46세 이상 | 6 | 2.5 | 1000명 이상 | 124 | 51.2 |
| | | | 산업유형 | | |
| | | | 제조 | 46 | 19 |
| 학력 | | | 유통/서비스 | 64 | 26.4 |
| 고졸이하 | 2 | 0.8 | IT/통신 | 88 | 36.4 |
| 대학졸업 | 166 | 68.6 | 금융/보험 | 10 | 4.1 |
| 대학원재학&석사졸업 | 68 | 28.1 | 공공기관 | 10 | 4.1 |
| 박사이상 | 6 | 2.5 | 기타 | 24 | 9.9 |
| **합계** | **242** | **100.0** | **합계** | **242** | **100.0** |

시스템, 관련 교육, 처벌, 보상을 실시하고 있는 직장인만을 대상으로 실시하였다.

성별은 남자 65.3%, 여자 34.7% 로 기업에서 남자 직원이 차지하는 비율이 높은 만큼 본 연구에서도 남자의 응답 비율이 높았으며 학력 부분은 기업 실무진이 대부분이 대상인 만큼 대졸, 대학원 졸업 응답자가 96.7%를 차지하였다. 나이 역시 26세에서 40세까지가 88.4%를 차지하여 고른 분포를 보이지는 않았다. 그러나 기업에서 실무를 담당하고 있는 사람들을 대상으로 한 연구라고 본다면 표본은 비교적 대표성을 가지고 있다고 보여진다.

조사 대상이 기업이었다면 기업 하나씩을 대상으로 해야 하지만 본 설문조사는 각 기업에 종사하는 직원들을 대상으로 한 개인의 태도에 관한 연구이므로 산업 유형별 특성에 대한 분석은 본 연구에서 크게 의미가 없다고 하겠다. 그러나 직책에 대한 분류는 사원, 대리, 과장급의 실무진이 90.1%를 차지하고 있으며 차장급 이상은 9.9%에 불과하다. 따라서 실무를 담당하고 있는 직원들의 정보 보안 태도의 현실을 보여줄 수 있는 연구라고 할 수 있다.

설문 조사 결과 대부분이 규모가 큰 기업이 대부분이었다. 실제 조사 결과도 50명 이하의 중소기업은 9.1%에 불과하였으나 300명 이상의 큰 기업이 66%를 차지하였다. 이 중에서 1,000명 이상의 대기업은 51.2%를 차지하여 국내에서는 아직도 중소기업에서는 정보보호에 대한 관심도가 떨어진다고 볼 수 있다.

산업 유형에 관련된 특성을 살펴보면 IT/통신 분야가 36.4%를 차지하고 있으며 그 다음이 유통/서비스 분야로 26.4%를 차지하였다. 그 다음 제조분야, 기타, 금융/보험, 공공기관 순이었는데, 이는 기존 연구(Yeh and Chang, 2007)와 다른 결과를 나타내고 있다. 그러나 본 연구에서 금융/보험 분야의 응답 비율이 낮은 이유는 설문 조사를 위한 표본이 대부분 IT 관련 기업 종사자였기 때문으로 볼 수 있다. 기업 분류가 다른 이유도 있지만 설문 조사의 대상이 조직 구성원 중심으로 전 산업 분야를 고르게 대상으로 하지 않았기 때문이다.

### 5.2 문항분석

우선 각 항목별로 기술 분석을 실시하여 평균과 표준변차를 제시하였고 정규 분포 정도를 살펴보기 위하여 첨도(Skewness)와 왜도(Kurtosis) 및 이상치(Outlier)를 검토하였고 그 결과는 〈별첨 2〉에 제시되어 있다. 분석 결과에 따르면 각 문항의 첨도는 0.002~1.667, 왜도는 -0,022~3.008의 분포를 보였다. 이 수치들이 ±1 이상이면 그 자료가 정규 분포를 따른다고 가정하기 어렵다고 보는 의견들이 있기는 하지만, 실제로 편포도의 해석에 대해서는 크게 합의된 바가 없으며 궁극적으로 연구자에 따라 달라질 수 있다고 본다(홍두승, 2003). 뿐만 아니라 척도 타당화 분석에서 사용되는 구조방정식 모형에서 적용 가능한 정상 분포의 조건은 -2<왜도<2, -4<첨도<4로 보고 있으므로(김주환 · 김민규 · 홍세희, 2009), 편포도 이상치에 의해 제거 대상이 된 문항은 없었다. 또한 각 문항의 표준화 점수를 이용하여 이상치를 검토하는데, 표본수가 80 이상인 경우에 표준화 점수가 3이상인 경우 이상치로 판단하므로(김계수, 2007; Deveilleds, 1991) 본 연구에서는 해당되는 이상치가 없어 표본에서 제거된 문항은 없었다.

최종적으로 사용된 표본수는 요인분석을 실시하기 위하여 요구되는 최소표본수인 100을 충족시키므로(이학진 · 임지훈, 2005), 척도의 타당도 분석을 위한 최소한의 표본수가 확보된 것으로 볼 수

있다. 다음으로 전체와 개별 문항 간의 상관관계를 통하여 각 문항들의 동일 개념을 측정하고 있는지 살펴보았다. 일반적으로 전체와 개별 문항 간의 상관관계가 0.3 이하인 문항은 동일 개념을 측정하기 위한 다른 문항들과 내용적으로 다름을 의미하기 때문이다(Roobina, 1990). 그 결과는 〈별첨3〉에 제시되어 있으며, 전체와 0.3 이하의 낮은 상관관계를 보이는 문항(직접경험 2번과 6번 문항)은 분석에서 제외하였다. 또한 서로 중복되는 의미를 가지는 문항이 있는지 살펴보기 위하여 척도의 개별 문항 간의 상관관계 분석을 통해 다중공선성을 검토하였다. 그 결과, 문항 제거의 기준(Stevens, 1992)으로 제시되는 ±0.8이 넘는 높은 상관관계가 나타나지 않았다.

### 5.3 측정모형

신뢰도란 비교 가능한 독립된 측정 방법에 의해 대상을 측정하는 경우 결과가 비슷하게 되는 것을 의미하며, 일반적으로 동일한 개념에 대하여 비교 가능한 독립된 측정 도구를 사용하여 측정을 반복하였을 때 동일 또는 유사한 측정값을 얻을 가능성을 말한다. 이는 동일한 측정을 위한 항목간의 평균적인 관계에 근거하여 내적 일관성을 고려하는 것이라고 할 수 있다. 신뢰도는 Cronbach's α (alpha)라는 신뢰 계수(Reliability coefficient)를 이용하는 내적 일치법이 가장 일반적으로 사용된다.

Cronbach's α값은 표본으로부터 추출된 변수의 합이 모집단에서의 참값의 추정치를 어느 정도 신뢰할 수 있는 가를 알려주는 통계량으로 여러 변수들이 모두 같은 대상을 측정한 것인지에 대한 검정이다. 측정되는 변수의 성질과 상황에 따라 그 기준이 유동적이기는 하지만, 일반적으로 알파계수가 관대한 수준에서 0.6이상이면 신뢰도가 확보된 것으로 볼 수 있다(Nunnally, 1978). 사회과학 분야에서 0.8이상이면 상당히 신뢰도가 높다고 하고, 0.6이상이면 측정 도구의 신뢰도에 문제가 없는 것으로 보는데, 본 연구에서는 모두 0.8이상의 높은 값이 나와서 신뢰도가 매우 높은 것으로 나타났다.

내용타당성(Content validity)이란 측정하고자 하는 것을 올바르게 측정하였는가 하는 것이다(Churchill, 1979). 본 논문에서는 높은 수준의 내용타당성을 확보하기 위하여 기업 정보 보호 활동에 대한 개별 구성차원을 이해함에 있어 전문가 집단을 활용하였다. 전문가 집단은 연구와 관련된 주제를 전공하고 있는 박사과정 이상의 연구자와 정보통신 관련 연구소(한국인터넷진흥원, 통신정책연구원 등)의 연구원, 정보통신 관련기업의 최고경영자 그리고 해당분야의 전공교수로 구성되었으며 측정문항의 개발, 검토 그리고 예비조사과정 동안 측정도구의 수정 및 정화절차를 수행하여 높은 수준의 내용타당성이 확보되었다고 생각된다.

개념타당성(Construct validity)은 측정도구의 정확성으로 언급되며 측정문항의 통계적 유의성으로 개별 구성개념의 단일차원성을 평가하는 요인분석을 통하여 확보될 수 있다(Hair et al., 1998). 각 변수의 타당성의 정도를 측정하기 위해 주성분분석(Principal component analysis)으로 각 요인을 추출하였으며, Kaiser 정규화가 있는 varimax 회전 방법을 사용하였다. Kaiser(1974)는 단순상관계수와 부분상관계수의 크기를 비교하여 표본의 적절성을 측정하는 지수를 개발하였는데, 이를 Kaiser-Meyer-Olkin(KMO)의 표본 적절성 측정치라고 한다(양병화, 2006). KMO 값이 1에 가까울수록 표본의 상관은 요인분석하기에 적합하다.

본 연구에서는 KMO 값이 0.826로 요인분석하기에 양호한 것으로 보인다. 모든 변수들의 문항에 대한 회전된 성분행렬 결과 각 항목들이 모두 하나의 요인으로 묶였으며 선별된 문항과 변수들의 요인분석 결과는 〈표 5〉와 같다.

요인적재량(Factor loading)이 0.5 이하인 값의 몇 가지 문항은 주관적 판단 하에 설문 문항에서 제외 시켰다. 먼저 직접 경험의 경우 문항분석을 통해 전체와 개별상관에서 0.3이하의 낮은 상관을 보인 2번 문항과 6번 문항은 분석에서 제외시켰으며, 간접 경험의 경우에도 요인적재량이 0.5 이하인 2개의 문항(1번과 7번 문항), 보안 정책(4번 문항) 그리고 보안 태도(4번 문항) 각각 1문항이 제외되었다. 결론적으로 위험인식 6개 항목, 시스템 4개 항목, 간접 경험 5개 항목, 교육 4개 항목, 보상 4개 항목, 처벌 4개 항목, 보안 태도 4개 항목, 직접경험 4개 항목, 업무 연관성 3개 항목, 정책 3개 항목 등 총 41개 문항, 10개 요인을 변수로 사용하였다.

### 5.4 가설검증을 위한 회귀분석

〈별첨 3〉은 각 독립변수들의 Pearson 상관계수 값을 보여주고 있으며, Hair *et al.* (2003)은 상관계수값이 0.7을 상회하면 다중공선성을 의심해야 한다고 하였다. 따라서 본 연구의 독립변수들간에는 다중공선성을 염려할 만큼 심각한 상관관계가 없음을 확인할 수 있다.

상관계수를 확인해 본 결과 통제변수인 직책과 나이의 상관계수값이 0.759로 높아 직책을 제외하고 회귀분석을 실시하였다.

본 연구에서는 가설 검증을 위하여 회귀분석을 사용하였다. 회귀분석은 변수들 간의 함수적인 관련성을 규명하기 위하여 어떤 수학적 모형을 가정하고 측정된 자료를 이용하여 통계적 추정을 행하는 분석방법을 말하며, 자료로부터 얻어진 관계식을 이용하여 종속변수의 움직임을 예측하고 모형 전체와 독립변수들의 영향력에 관한 통계적 검정과 추정을 행하는데 사용된다.

〈표 6〉과 〈표 7〉은 각 변수들이 종속변수인 조직 구성원의 보안태도에 미치는 영향을 알아보기 위한 다중회귀 분석결과이다. 독립변수인 간접경험, 업무연관성, 시스템, 보상, 처벌, 직접경험, 위험인식, 정책, 교육, 업종, 나이, 회사규모, 교육정도, 성별 등이 종속변수인 보안 태도에 대해 가지는 설명력(R square)은 33.5%이고, 회귀모형의 적합도를 평가하는 변량분석 결과, F값은 7.088, P=.000으로 유의수준 0.01수준에서 통계적으로 유의하여 $R^2$ 가 33.5%인 보안태도를 예측하는 회귀모형이 적합함을 나타내고 있다.

회귀분석 결과 각 독립 변수 별로 조직 구성원의 보안에 관련된 태도에 대한 영향을 살펴보면 다음과 같다. 우선 위험인식은 조직 구성원의 보안에 관련된 태도에 정적인 영향을 주는 유의한 변수로 나타났다(b=0.338, p<0.001). 또한 처벌에 대한 인식(b=0.170, p<0.05), 보안 교육의 유용성(b=0.223, p<0.05) 그리고 보상에 대한 인식(b=0.137, p<0.05)도 구성원의 보안에 관련된 태도에 정적인 영향을 주는 유의한 변수였으며, 직접 경험은 부적인 영향을 주는 변수로 타났다. 하지만 본 연구는 가설에 따라 우측단측검증을 실시해야 한다. 우선 검정통계량이 (-)이므로 공식(1-유의확률/2)에 따라 값을 구하면 0.92가 되어 가설은 기각된다(〈표 8〉 참조). 특히 위험에 대한 인식 변수는 통계적으로 유의한 변수들 가운데 상대적으로 가장 큰 영향력을 보이는 것으로 나타났다

〈표 5〉 탐색적 요인분석 결과

| 측정항목 | | α | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 위험인식 | Ri1 | .971 | .888 | | | | | | | | | |
| | Ri2 | | .862 | | | | | | | | | |
| | Ri3 | | .911 | | | | | | | | | |
| | Ri4 | | .917 | | | | | | | | | |
| | Ri5 | | .889 | | | | | | | | | |
| | Ri6 | | .896 | | | | | | | | | |
| 보안시스템의 용이성 | Sys1 | .940 | | .847 | | | | | | | | |
| | Sys2 | | | .882 | | | | | | | | |
| | Sys3 | | | .882 | | | | | | | | |
| | Sys4 | | | .771 | | | | | | | | |
| 간접경험 | Ie1 | .875 | | | .863 | | | | | | | |
| | Ie2 | | | | .836 | | | | | | | |
| | Ie3 | | | | .686 | | | | | | | |
| | Ie4 | | | | .772 | | | | | | | |
| | Ie5 | | | | .645 | | | | | | | |
| 보안교육의 유용성 | Ed1 | .938 | | | | .732 | | | | | | |
| | Ed2 | | | | | .786 | | | | | | |
| | Ed3 | | | | | .814 | | | | | | |
| | Ed4 | | | | | .811 | | | | | | |
| 보상 | Re1 | .929 | | | | | .859 | | | | | |
| | Re2 | | | | | | .866 | | | | | |
| | Re3 | | | | | | .859 | | | | | |
| | Re4 | | | | | | .751 | | | | | |
| 처벌 | Pu1 | .891 | | | | | | .800 | | | | |
| | Pu2 | | | | | | | .778 | | | | |
| | Pu3 | | | | | | | .744 | | | | |
| | Pu4 | | | | | | | .846 | | | | |
| 보안태도 | Att1 | .837 | | | | | | | .826 | | | |
| | Att2 | | | | | | | | .808 | | | |
| | Att3 | | | | | | | | .779 | | | |
| | Att4 | | | | | | | | .669 | | | |
| 직접경험 | De1 | .818 | | | | | | | | .773 | | |
| | De2 | | | | | | | | | .799 | | |
| | De3 | | | | | | | | | .673 | | |
| | De4 | | | | | | | | | .812 | | |
| 업무연관성 | Re1 | .871 | | | | | | | | | .881 | |
| | Re2 | | | | | | | | | | .883 | |
| | Re3 | | | | | | | | | | .869 | |
| 보안정책의 유용성 | Po1 | .971 | | | | | | | | | | .635 |
| | Po2 | | | | | | | | | | | .613 |
| | Po3 | | | | | | | | | | | .695 |
| 고유치 | | | 9.92 | 7.05 | 4.14 | 2.71 | 2.01 | 1.85 | 1.58 | 1.38 | 1.31 | .984 |
| 설명된 분산 (%) | | | 13.97 | 10.28 | 8.82 | 8.34 | 8.06 | 7.69 | 6.77 | 6.63 | 6.13 | 4.79 |
| 누적분산 (%) | | | 13.97 | 24.25 | 33.07 | 41.41 | 49.48 | 57.16 | 63.93 | 70.56 | 76.69 | 81.47 |

〈표 6〉 모형 요약

| 모형 | R | R제곱 | 수정된 R제곱 | 추정값의 표준오차 |
|---|---|---|---|---|
| | .579(a) | .335 | .288 | 1.07472 |

a 예측값 : (상수), 간접경험, 업무연관성, 시스템, 보상, 처벌, 직접경험, 간접경험, 정책, 교육, 업종, 나이, 회사규모, 교육정도, 성별

〈표 7〉 분산 분석

| 모형 | 제곱합 | 자유도 | 평균제곱 | F | 유의확률 |
|---|---|---|---|---|---|
| 회귀모형 | 130.980 | 16 | 8.186 | 7.088 | .000(a) |
| 잔차 | 259.879 | 225 | 1.155 | | |
| 합계 | 390.860 | 241 | | | |

a 예측값 : (상수), 간접경험, 업무연관성, 시스템, 보상, 처벌, 직접경험, 간접경험, 정책, 교육, 업종, 나이, 회사규모, 교육정도, 성별

b 종속변수 : 보안태도

(beta=0.338). 이와 같은 회귀분석 결과에 의한 가설의 검증은 〈표 9〉를 통하여 정리하였다.

예상했던 바와 같이, 본 연구는 일부 통제변수들의 경우 보안태도와 연관성이 있음을 알 수 있었다. 예를 들면, 나이의 경우 보안태도와 정(+)의 관계를 보임으로써 직급이 높아질수록(앞서 설명한 것과 같이 나이와 직급은 높은 상관관계 보였음) 보안에 대한 중요성을 더 많이 인지한다고 해석할 수 있다. 업종의 경우 유통/서비스가 IT/통신보다 보안태도가 높다는 결과를 보였는데 이러한 결과는 유통업의 경우 SCM(Supply Chian Management)의 중요성이 부각되면서 시스템 구축을 통한 효율적 경영에 대한 관심의 증가 그리고 이에 따른 사이버 위협에 대한 심각성을 인지, 서비스업의 경우 금융/보험이 포함된 것이 원인이라 할 수 있을 것이다. 회사규모의 경우 부(-)의 관계를 보였는데 이는 조직의 규모가 커질수록 전달체계의 한계로 인해 모든 구성원들에게 보안의 중요성을 각인시키는데 어려울 수도 있다는 내용을 뒷받침해준다.

본 연구에서는 Davis(1989)가 제안한 기술수용모델의 내용 즉, 지각된 유용성과 용이성이 개인의 태도에 영향을 준다는 내용을 바탕으로 조사되었으나 결과적으로 교육에 대한 유용성만이 채택되어 기술수용모델과 일치되지 않는 결과가 도출되었다. 이러한 결과에 대한 원인은 아래와 같이 분석할 수 있을 것이다.

첫째, 인지된 정책의 유용성은 조직 구성원의 태도에 유의하지 않은 것으로 나타나 가설이 기각되었다. 이에 대한 원인은 회사에서 실시하는 정책을 설문 조사에 응답하는 직원이 완전히 이해하고 있지 못하거나 관심도가 낮은데 원인이 있을 수 있다. 조사 대상의 대부분이 보안에 대한 정책을 실시하고 있는 대기업이 많았으나 실제 업무가 정보보호와 연관성이 없는 경우는 조직 구성원의 태도에 영향을 크게 미치지 못했을 것이라 생각된다.

둘째, 본 연구에서는 보안에 관련된 소프트웨어 설치, 바이러스 침투를 막기 위한 백신 설치, 외부접속을 위한 VPN 프로그램 설치 등 직접적인 시스템으로 대표되는 보안 기술에 대한 용이성을 조사하였다. 그러나 이에 대한 가설은 기각되었으며

〈표 8〉 회귀분석결과

| 모형 | 비표준화 계수 | | 표준화 계수 | t | 유의확률 |
|---|---|---|---|---|---|
| | B | 표준오차 | 베타 | | |
| (상수) | .591 | .724 | | .816 | .415 |
| 성별 | -.172 | .167 | -.065 | -1.034 | .302 |
| 제조 (업종 더미1) | -.014 | .216 | -.004 | -.066 | .948 |
| 유통/서비스 (업종 더미2) | .580 | .207 | .210 | 2.796 | .006 |
| 공공기관/기타 (업종 더미3) | .251 | .239 | .069 | 1.051 | .294 |
| 회사규모 | -.242 | .083 | -.201 | -2.926 | .004 |
| 나이 | .212 | .080 | .174 | 2.636 | .009 |
| 교육정도 | .015 | .159 | .006 | .096 | .923 |
| 정책 | -.046 | .082 | -.047 | -.561 | .575 |
| 시스템 | .071 | .078 | .071 | .909 | .364 |
| 교육 | .223 | .094 | .220 | 2.383 | .018 |
| 보상 | .137 | .066 | .153 | 2.067 | .040 |
| 처벌 | .170 | .065 | .187 | 2.596 | .010 |
| 위험인식 | .338 | .078 | .308 | 4.358 | .000 |
| 직접경험 | -.124 | .051 | -.159 | -2.417 | .016 |
| 간접경험 | .014 | .070 | .014 | .194 | .846 |
| 업무연관성 | .062 | .050 | .079 | 1.250 | .213 |

a. 종속변수: 보안태도

이는 실제로 보안에 관련해서 시스템적으로 소프트웨어 설치 등은 한 번 설치 후 자동 업데이트 등을 이용하는 경우가 많아서 용이성 판단을 하기는 힘들다는 직원들의 인식을 반영한 것이다. 회사에서 실시하는 보안 관련 특별 프로그램은 약간의 형식적인 것으로 생각하는 직원이 많다고도 볼 수 있고, 이미 시스템 구축 시 보안을 고려하여 설계된 경우가 많아 직원들이 실제 신경을 쓰지 않는 편이므로 용이성 여부에 대한 인식을 하고 있지 않은 것으로 생각된다.

반면에 회사에서 실시하는 정보 보호 교육은 유용하다는 가설이 채택되었는데 이는 회사에서 실시하는 정보 보호에 관련된 교육은 직원들의 인식에 직접적인 효과가 있다는 뜻이다. 정보 보호에 관련된 교육을 통하여 보안에 대한 인식이 바뀌고 실제 태도에 영향을 미치는 것이다. 조사대상이 대부분 정보 보호 교육을 실시하는 업체들이기 때문이기도 하겠지만 업무상 평소 보안에 대해 신경을 쓰고 있지 않았다가 교육의 기회를 통해서 보안에 관련된 인지도가 향상되고 중요성 또한 깨닫게 되는 것이

〈표 9〉 가설검증

| | 가설 | 검증 |
|---|---|---|
| H1 | 인지된 보안정책의 유용성은 기업 정보 보호에 대한 조직 구성원의 태도에 직접적이고 긍정적인 영향을 미친다. | 기각 |
| H2 | 인지된 보안시스템의 사용 용이성은 기업 정보 보호에 대한 조직 구성원의 태도에 직접적이고 긍정적인 영향을 미친다. | 기각 |
| H3 | 인지된 보안교육은 기업 정보 보호에 대한 조직 구성원의 태도에 직접적이고 긍정적인 영향을 미친다. | 채택 |
| H4a | 인지된 보상의 유용성은 기업 정보 보호에 대한 조직 구성원의 태도에 직접적이고 긍정적인 영향을 미친다. | 채택 |
| H4b | 인지된 처벌의 유용성은 기업 정보 보호에 대한 조직 구성원의 태도에 직접적이고 긍정적인 영향을 미친다. | 채택 |
| H5 | 보안에 관련된 위험 인식은 기업 조직 구성원의 태도에 직접적이고 긍정적인 영향을 미친다. | 채택 |
| H6a | 보안에 관련된 직접적인 경험은 기업 조직 구성원의 태도에 직접적이고 긍정적인 영향을 미친다. | 기각 |
| H6b | 보안에 관련된 간접적인 경험은 조직 구성원의 태도에 직접적이고 긍정적인 영향을 미친다. | 기각 |
| H7 | 개인의 업무와 보안 연관성은 기업 조직 구성원의 태도에 직접적이고 긍정적인 영향을 미친다. | 기각 |

라고 할 수 있다.

또한 인지된 보상의 유용성이 기업 정보 보호에 대한 조직 구성원의 태도에 직접적이고 긍정적인 영향을 미칠 것이라는 가설이 채택되었는데, 이는 직원들이 회사에서의 보상에 대해 가장 민감하게 반응하고 있다는 것을 보여준다. 대부분의 보상이 금전 혹은 승진과 연관되어 개인에게 직접적으로 작용하기 때문에 자신에게 유리하다면 당연히 따르고자 하는 직원들의 인식을 반영한 결과로 볼 수 있다. 대부분 보안에 관련된 연구는 직접적인 피해를 보기 전까지는 정보 보호에 신경 쓰지 않기 때문에 보안에 어려움이 있다고 이야기 하고 있으나 본 연구가 기업의 구성원들을 대상으로 했기 때문에 금전적인 측면에 민감한 직원의 특성으로 인하여 나타난 결과로도 볼 수 있다. 대부분의 연구에서 처벌과 보상은 반대로 움직이는 기재로 인식되고 있으나 본 연구에서는 인지된 처벌의 유용성은 기업 정보 보호에 대한 조직 구성원의 태도에 영향을 미치는 것으로 분석되었다.

앞부분의 연구 결과가 기업의 정보 보호 노력에 대한 부분이었다면 개인적인 경험이나 평소 보안 위험에 대한 인식, 업무 연관성 등은 개인적인 측면에서의 조사이다. 이 부분에서는 보안에 관련된 위험 인식을 제외한 모든 변수가 기각되었는데, 예상했던 바와 같이, 보안에 관련된 위험 인식이 기업 조직 구성원의 태도에 가장 직접적이고 긍정적인 영향을 미친다는 결과가 나왔다. 평소 위험에 대해 민감하게 반응하는 사람은 대개 스스로 위험

에 대한 대비를 하는 경향이 있으므로 개인의 보안 태도에도 긍정적이 되는 것이다. 하지만 개인의 직·간접적인 경험과 업무가 보안과 연관성이 있다고 해서 보안태도에 직접적인 영향을 미치지는 않는 것으로 나타났다.

## Ⅵ. 결론

지금까지의 연구가 기업을 대상으로 실시되었다면 본 연구는 기업 조직 구성원을 중심으로 다루었다는 부분이 특징적이라고 할 수 있다. 특히 기업의 정보 보호 노력 중에서 직원의 보안 태도에 미치는 요인들을 다양한 변수를 활용해서 살펴보았다는 점이 다른 부분이다. 하지만 표본 수가 242명에 불과하며 다양한 기업을 조사하기 보다는 한 직장 내의 여러 명을 대상으로 조사하였기 때문에 연구 결과가 전체 기업 구성원을 대표하는 것이라고 할 수는 없다는 데 한계가 있다. 차후 연구에서는 기업 구성원에 대한 대표성을 가질 수 있는 표본으로 확대하여 연구 모형을 검증할 필요성이 제기되며, 상호작용효과(Interaction effect)를 고려하여 분석하는 것도 의미가 있을 것이다.

그러나 본 연구의 교육과 보상이 조직원들에게 큰 영향을 준다는 점은 향후 연구 방향에 다양한 점을 시사하고 있다. 먼저 기업의 정보 보호 교육에 있어 효과적인 방법에 있어서 구체적인 연구가 필요하다는 점이다. 개인적인 측면에서의 연구 결과에서 알 수 있듯이 간접적인 경험은 조직 구성원들의 태도에 큰 영향을 주지 않는 다는 결과에서처럼 정보 보호 교육 시에 타 기업 사례의 나열 등은 오히려 남의 일처럼 느껴질 수 도 있기 때문이다. 따라서 보안 가이드라인이나 지침의 전달이 얼마나 개인에게 효과적으로 연결될 수 있는가에 대한 연구가 필요할 것이다.

대부분의 보안 시스템은 소프트웨어 구축이나 기존 시스템에 내재되어 있는 것이 일반적이며 업무에 영향을 미치지 않도록 설계되어 있는 것이 일반적이다. 하지만 시스템의 용이성과 조직 구성원의 정보 보호 태도는 크게 상관이 없다는 것이 밝혀졌다. 이에 따라서 기업은 단순하게 보안 소프트웨어를 설치하도록 하고 업데이트를 하도록 권고하는 것 뿐 만이 아니라 왜 그러한 시스템을 설치하게 되었는지 어떤 효과가 있는 것인지에 대한 인식을 하게 할 수 있는 노력도 필요하다.

정보 보호 관련 위험에 대한 인식은 각종 매스컴과 기업 자체 교육 등의 노력으로 대부분의 사람들이 인지하게 되었다. 본 연구 결과에서도 위험에 대한 인식은 조직 구성원의 보안 태도에 가장 직접적인 영향을 끼치는 것으로 나타났다. 하지만 기존 연구에서는 직, 간접적인 경험이 위험 인식에 영향을 준다는 연구 결과도 있다. 그러므로 가장 유의한 결과를 나타내었던 위험의 인식 부분에 대한 추가적인 연구의 필요성이 있다. 일반적인 업무를 하는 조직 구성원들에게 보안 담당자 수준의 역할을 기대할 수는 없는 것이 현실이다. 그러므로 기업의 보안은 누구나 가장 쉽게 인식할 수 있고 관련 시스템이나 마인드에 접근할 수 있도록 하는 노력이 필요하다고 볼 수 있다. 기업에서 실시하는 정보 보호를 위한 노력에서 가장 중요한 것은 무엇보다 사후 조치가 아닌 사전 예방적인 활동이 필요하다는 점이다. 이는 비용적인 측면뿐만 아니라 다양한 측면에서 정보 보호를 위한 활동을 미리 준비할 수 있다는 점에서 효율적이기 때문이다. 특히 기업에서는 조직 구성원에 초점을 맞춘 정보 보호 노력을

지속적으로 실시해야 할 것이다.

## 참고문헌


김계수(2007), **Amos 7.0 구조방정식 모형 분석**, 서울, 도서출판 한나래.

김종기, 강다연(2008), "보안정책, 보안의식, 개인적 특성이 패스워드 보안효과에 미치는 영향," **정보보호학회논문지**, 18, 123-133.

김종석, 김기윤, 나관식(2004), **인지된 보안이 인터넷 쇼핑몰 사용의도에 미치는 영향**, 경영정보학회, 학술대회발표논문, 380-391.

김주환, 김민규, 홍세희(2009), **구조방정식으로 논문쓰기**, 서울, 커뮤니케이션북스.

민천홍, 고완석(2005), "모바일 보안 서비스에 대한 인식 정도가 모바일 결제 시스템 범용성에 미치는 영향에 관한 연구," **인터넷비즈니스연구**, 6, 43-53.

박태완(1997), **정보시스템 보안 감리**, 서울, 한국전산원.

백민정(2010), **정보윤리활동이 정보보안성과에 미치는 영향에 관한 연구**, 단국대학교 박사학위 논문.

서보밀(2006), "인지된 보안통제가 고객의 인터넷 뱅킹 수용에 미치는 영향," **한국전자거래학회지**, 11, 25-52.

손달호(2005), "웹거래의 신뢰성에 대한 보안요인의 영향에 관한 연구," **경영연구**, 20, 1-27.

송주석(1997), **전파통신 정보보호 정책방향에 관한 연구**, 서울, 정보통신산업진흥원.

안중호, 박준형, 성기문, 이재홍(2010), "처벌과 윤리교육이 정보보안준수에 미치는 영향: 조직유형의 조절효과를 중심으로," **경영정보학연구**, 12, 23-42.

양병화(2006), **다변량 데이터 분석법의 이해**, 서울, 커뮤니케이션북스.

오창규, 김종기(2003), "효과적인 정보보호 교육 및 훈련을 위한 프레임워크 개발," **정보보호학회논문지**, 13, 59-69.

이경기(2008), **[기술보국이 미래사회 희망]<3부>우리 사회 보안전략이 필요하다**, 내일 신문, http://www.naeil.com/News/politics/ViewNews.asp?nnum=431765&sid=E&tid=0(검색일: 2009년 11월 17일).

이상준(2008), **정보보호는 기업을 살리는 전략적 투자**, 보안뉴스, http://www.boannews.com/media/view.asp?idx=12803&kind=1(검색일: 2009년 11월 15일).

이선경(2010), **기업의 정보보호 정책과 구성원들의 정보보호 태도**, 연세대학교 석사학위 논문.

이웅규(2005), "보안위험, 편리성, 사회적 영향이 인터넷 뱅킹 사용에 미치는 효과 - 계좌이체와 잔액조회 서비스의 비교," **정보시스템연구**, 14, 1-23.

이학진, 임지훈(2005), **SPSS 12.0 메뉴얼**, 서울, 법문사.

전성훈(2004), "억지이론과 억지전략에 대한 소고," **전략연구**, 11, 123-148.

최영찬, 김미숙, 유철우(2008), "베트남 사례를 통한 불법 소프트웨어 사용요인 연구," **e-비즈니스연구**, 9, 237-258.

홍두승(2003), **사회조사분석 제3판**, 서울, 다산출판사.

Amitava, D. and K. McCrohan(2002), "Management's Role in Information Security in a Cyber Economy," *California Management Review*, 45, 67-87.

Blumstein, A., J. Cohen and D. Nagin(1978), *Deterrence and Incapacitation - Estimating the Effect of Criminal Sanctions on Crime Rates*, Washington, National Academy of Sciences.

Churchill, G. A.(1979), "A Paradigm for Developing Better Measures of Marketing Constructs," *Journal of Marketing Research*, 16, 64-73.

Cohen, W. M. and D. A. Levinthal(1990), "Absorptive Capacity: A New Perspective on

Learning and Innovation," *Administrative Science Quarterly*, 35, 128-152.

Davis, F. D.(1989), "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly*, 13, 319-340.

Detmar, W., D. W. Straub and W. D. Nance (1990), "Discovering and Disciplining Computer Abuse in Organizations: A Field Study," *MIS Quarterly*, 14, 45-60.

Devillis, R. F.(2003), *Scale development: Theory and applications*, 2nd Edition, California, Sage publications.

Dhillon, G. and J. Backhouse(2000), "Information System Security Management in the New Millennium," *Communications of the ACM*, 43, 125-128.

Festinger, L.(1957), *A theory of cognitive dissonance*, California, Row, Peterson and Company.

Finne, T.(1998), "A conceptual framework for information security management" *Computers & Security*, 17, 303-307.

Goodhue, D. L. and D. W. Straub(1991), "Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security Measures," *Information & Management*, 20, 13-27.

Goodhue D. L. and R. L. Thompson(1995), "Task-Technology Fir and Individual Performance," *MIS Quarterly*, 19, 213-236.

Gordineer, J.(2003), "Blended Threats: A New Era in Anti-Virus Protection," *Information Systems Security*, 12, 45-47.

Govindarajan, V. and J. Fisher(1990), "Strategy, Control Systems, and Resource Sharing: Effects on Business-Unit Performance," *Academy of Management Journal*, 33, 259-285.

Hair, J. F., R. E. Anderson and R. L. Tatham (1998), *Multivariate Data Analysis*, Third edition, New York, Macmillan.

Hayam, A. and E. Oz(1993), "Integrating data security into the systems development life cycle," *Journal of Systems Management*, 44 (8), 16-20.

Hirschi, T.(1969), *CAUSES OF DELINQUENCY*, Berkeley and Los Angeles, California, University of California Press.

Kaiser, H. F.(1974), "An index of factorial simplicity," *Psychometrika*, 39, 31-36.

Kankanhalli, A., H. H. Teo, B. C. Y. Tan and K. K.(2003), "An integrative study of information systems security effectiveness," *International Journal of Information Management*, 23, 139-154.

Kirsch, L. J. and S. R. Boss(2007), *The Last Line of Defense: Motivating Employees to Follow Corporate Security Guidelines*, 28th International Conference on Information System, Montreal, Information Systems Privacy and Security.

Lebow, R. N. and J. G. Stein(1990), "Deterrence: The Elusive Dependent Variable," *World Politics*, 42, 336-369.

Nunnally, J. C.(1978), *Psychometric Theory*, Second edition, New York, McGraw-Hill.

Piccoli, G., R. Ahmad and B. Ives(2001), "Web-Based Virtual Learning Environments: A Research Framework and a Preliminary Assessment of Effectiveness in Basic IT Skills Training," *MIS Quarterly*, 25, 401-426.

Poore, R. S.(1980), "Holistic approach needed for

healthy security program," *Computing Canada*, 6(25), 7.

Roobina, O.(1990), "Constuction and validation of a scale to measure celebrity," *Journal of Advertising*, 31, 39-52.

Straub, D. W.(1990), "Effective IS Security: An Empirical Study," *Information Systems Research*, 1, 255-276.

Straub, D. W. and R. J. Welke(1998), "Coping With Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly*, 22, 441-469.

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

Trcek, D., R. Trobec, N. Pavesic and J. F. Tasic (2007), "Information systems security and human behaviour," *Behaviour & Information Technology*, 26, 113-118.

Vassilacopoulos, G. and D. Peppes(1996), "A front end authorization mechanism for hospital information systems," *Med. Inf.* 21, 93-103.

von Solms, R. and L. R. Meyer(1995), Information security accreditation - the ISO 9000 route. *Information security the next decade*. In: Eloff, J. and S. von Solms editors. Proceedings of the IFIP TC11 eleventh international conference on information security, South Africa: May 9-12, 40-49.

Vroom, V. H.(1964), *Work and Motivation*, New York, Wiley.

West, R.(2008), "The psychology of security," *Communications of the ACM*, 51, 34-40.

Wiant, T. L.(2005), "Information security policy's impact on reporting security incidents," *Computers & Security*, 24, 448-459.

Yeh, Q. J. and J. T. Chang(2007), "Threats and countermeasures for information system security: A cross-industry study," *Information & Management* 44, 480-491.

# 〈별첨 1〉 설문문항

**I. 보안 정책**
1. 우리 조직의 보안 정책은 나의 업무 보안에 실제 적용 가능한 내용을 포함하고 있다.
2. 우리 조직의 보안 정책은 내가 더 나은 보안 활동을 하는데 유용하다.
3. 우리 조직의 보안 정책은 내가 원하는 보안 활동을 찾는데 유용하다.
4. 우리 조직의 보안 정책은 내가 혼자 보안 활동을 하는 것보다 효과적이다.

**II. 보안 시스템**
1. 우리 조직의 보안 시스템은 쉽게 배울 수 있었다.
2. 우리 조직의 보안 시스템은 사용법이 쉽다고 생각한다.
3. 우리 조직의 보안 시스템에 능숙해지기 쉽다고 생각한다.
4. 우리 조직의 보안 시스템은 타 시스템과 유연하게 상호작용한다고 생각한다.

**III. 보안 교육**
1. 우리 조직의 보안 교육은 나에게 유익한 내용을 포함하고 있다고 생각한다.
2. 우리 조직의 보안 교육은 내게 적합한 방식이었다고 생각한다.
3. 우리 조직의 보안 교육은 나의 정보나 회사의 정보를 보호하기 위한 활동에 적합하다고 생각한다.
4. 우리 조직의 보안 교육은 조직 생활에 적응하기 쉬웠다고 생각한다.

**IV. 보상**
1. 나의 급여는 조직의 보안 정책을 따르고 있는지 아닌지 여부에 따라 올라갈 수 있다.
2. 조직의 보안 정책을 잘 따르는 경우 나는 칭찬이나 상을 받게 된다.
3. 나는 조직의 보안 정책을 잘 따른다면 급여 이외의 금전적 보상을 받을 수도 있다.
4. 조직의 보안 정책을 잘 따르는 경우 향후 나의 커리어에 긍정적 영향을 준다.

**V. 처벌**
1. 내가 보안 정책을 따르지 않는 경우 관리자 및 상위 관리자에게도 통보가 된다.
2. 나는 조직의 보안 정책에 따르지 않는 경우 시스템 사용에 제한을 받는다.
3. 나는 조직의 보안 정책에 따르지 않는 경우의 불이익을 잘 알고 있다.
4. 나는 조직의 보안 정책에 따르지 않는 경우 업무 활동에 제한을 받는다.

**VI. 위협 인식**
1. 내 컴퓨터가 바이러스나 웜에 의하여 위험해 질 수도 있다는 것을 알고 있다.
2. 내 컴퓨터에 해커가 침투할 수도 있다는 것을 알고 있다.
3. 바이러스나 사이버 공격으로 인하여 내 컴퓨터의 데이터가 위험해질 수도 있다는 것을 알고 있다.
4. 나의 개인 정보(신용카드 번호, 주민등록 번호, 은행 계좌 정보 등)가 도용당할 수도 있다는 것을 알고 있다.
5. 인터넷이나 이메일을 통하여 파일을 다운 받을 때 바이러스에 감염될 수도 있다는 것을 알고 있다.
6. 타인의 개인 정보를 유출하면 어려움에 처한다는 것을 알고 있다.

**VII. 직접적인 경험**
1. 내 컴퓨터가 바이러스나 웜에 의하여 위험해 진 적이 있다.
2. 내 컴퓨터에 해커가 침투할 수도 있다는 것을 알고 있다.
3. 바이러스나 사이버 공격으로 인하여 내 컴퓨터의 데이터가 위험해 진 적이 있다.
4. 나의 개인 정보(신용카드 번호, 주민등록 번호, 은행 계좌 정보 등)가 도용당한 적이 있다.
5. 인터넷이나 이메일을 통하여 파일을 다운 받을 때 바이러스에 감염된 적이 있다.
6. 나는 직원이나 고개의 개인 정보를 유출하면 어려움에 처한 적이 있다.

**VIII. 간접적인 경험**
1. 타인의 컴퓨터가 바이러스나 웜에 의하여 위험해 졌다는 것을 듣거나 본 적이 있다.
2. 누군가의 컴퓨터에 해커가 침투한 적이 있었다는 것을 듣거나 본 적이 있다.
3. 바이러스나 사이버 공격으로 인하여 누군가의 컴퓨터의 데이터가 위험해 진 적이 있었다는 것을 듣거나 본 적이 있다.
4. 타인의 개인 정보(신용카드 번호, 주민등록 번호, 은행 계좌 정보 등)가 도용된 적이 있었다는 것을 듣거나 본 적이 있다.
5. 타인이 인터넷이나 이메일을 통하여 파일을 다운 받을 때 바이러스에 감염된 적이 있었다는 것을 듣거나 본 적이 있다.
6. 직원이나 고개의 개인 정보를 유출로 문제가 생겼다는 것을 들어본 적이 있다.
7. TV나 신문, 잡지 등에서 정보보안에 관한 프로그램을 보거나 읽은 적이 있다.

**IX. 보안에 관련된 태도**
1. 나는 어디서든지 내가 사용하는 컴퓨터가 안전한 지 항상 신경을 쓰고 있다.
2. 나는 보안 관련된 최신 정보를 습득하거나 보안 프로그램 업데이트 등에 항상 신경을 쓰고 있다.
3. 나는 스팸 메일 방지를 위한 필터링 등의 노력을 규칙적으로 한다.
4. 나는 다른 사람에게 나의 비밀번호를 알려 주지 않는다.
5. 나는 바이러스 감염이나 의심스러운 메일을 받는 경우 시스템이나 보안 담당자에게 바로 알린다.

**X. 업무와 보안과의 관련성**
1. 나는 업무를 위하여 직원이나 고객의 민감한 정보를 다룬다.
2. 나는 업무를 위하여 회사 비밀이나 영업 기밀 등의 정보를 다룬다.
3. 나의 업무는 보안과 직접적인 관련이 있다.

## 〈별첨 2〉 기술통계량

| | 평균 | 표준편차 | 왜도 | 첨도 |
|---|---|---|---|---|
| 정책1 | 4.7686 | 1.42159 | -.231 | -.659 |
| 정책2 | 4.5785 | 1.37405 | -.407 | -.446 |
| 정책3 | 4.4298 | 1.41026 | -.419 | -.237 |
| 정책4 | 4.8678 | 1.59325 | -.638 | -.179 |
| 시스템1 | 4.5455 | 1.36342 | -.086 | -.520 |
| 시스템2 | 4.5868 | 1.40933 | -.080 | -.806 |
| 시스템3 | 4.5289 | 1.28234 | -.184 | -.093 |
| 시스템4 | 4.1322 | 1.47422 | .146 | -.676 |
| 교육1 | 4.2975 | 1.34284 | .044 | .072 |
| 교육2 | 4.1901 | 1.34080 | .002 | -.022 |
| 교육3 | 4.3554 | 1.42217 | -.193 | -.146 |
| 교육4 | 4.3223 | 1.35864 | -.281 | .167 |
| 보상1 | 2.5620 | 1.50734 | .892 | .194 |
| 보상2 | 2.8182 | 1.54598 | .634 | -.312 |
| 보상3 | 2.4050 | 1.60175 | 1.127 | .485 |
| 보상4 | 3.0496 | 1.60317 | .418 | -.487 |
| 처벌1 | 4.7273 | 1.67975 | -.506 | -.712 |
| 처벌2 | 4.6033 | 1.76400 | -.488 | -.805 |
| 처벌3 | 4.6694 | 1.50456 | -.396 | -.347 |
| 처벌4 | 4.6446 | 1.51265 | -.425 | -.349 |
| 위험인식1 | 5.9669 | 1.22853 | -1.534 | 2.983 |
| 위험인식2 | 5.8595 | 1.18291 | -1.060 | 1.278 |
| 위험인식3 | 5.8512 | 1.29897 | -1.278 | 1.779 |
| 위험인식4 | 5.9835 | 1.24229 | -1.487 | 2.689 |
| 위험인식5 | 6.0331 | 1.28143 | -1.565 | 2.707 |
| 위험인식6 | 6.0165 | 1.22886 | -1.547 | 3.008 |
| 직접경험1 | 4.5537 | 1.99564 | -.494 | -.977 |
| 직접경험2 | 2.6198 | 1.69086 | .924 | -.057 |
| 직접경험3 | 3.8595 | 2.05043 | .016 | -1.327 |
| 직접경험4 | 3.4215 | 2.05627 | .362 | -1.194 |
| 직접경험5 | 4.4711 | 2.06562 | -.420 | -1.193 |
| 직접경험6 | 2.0331 | 1.47417 | 1.667 | 2.251 |
| 간접경험1 | 5.4876 | 1.44697 | -.796 | -.156 |
| 간접경험2 | 4.7851 | 1.79537 | -4.98 | -.638 |
| 간접경험3 | 5.1736 | 1.67816 | -.765 | -.200 |
| 간접경험4 | 5.3306 | 1.62137 | -1.042 | .516 |
| 간접경험5 | 5.5041 | 1.43532 | -.951 | .631 |
| 간접경험6 | 5.4793 | 1.45812 | -.987 | .557 |
| 간접경험7 | 5.8512 | 1.26662 | -1.027 | .565 |
| 보안태도1 | 4.9917 | 1.42005 | -.459 | -.356 |
| 보안태도2 | 4.7851 | 1.50356 | -.323 | -.551 |
| 보안태도3 | 4.7769 | 1.59088 | -.377 | -.730 |
| 보안태도4 | 5.5124 | 1.37624 | -.575 | -.402 |
| 보안태도5 | 4.1570 | 1.68965 | -.010 | -.783 |
| 업무연관성1 | 4.2397 | 1.78525 | -.181 | -.964 |
| 업무연관성2 | 4.2810 | 1.78152 | -.129 | -.994 |
| 업무연관성3 | 4.0826 | 1.88282 | -.030 | -1.032 |

## 〈별첨 3〉 상관계수

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 정책 | 1 | | | | | | | | | | | | | |
| 시스템 | .629** | 1 | | | | | | | | | | | | |
| 간접경험 | .662** | .613** | 1 | | | | | | | | | | | |
| 보상 | .070 | .027 | .048 | 1 | | | | | | | | | | |
| 처벌 | .307** | .308** | .394** | -.045 | 1 | | | | | | | | | |
| 보안태도 | .460** | .377** | .533** | .228** | .293** | 1 | | | | | | | | |
| 직접경험 | -.043 | -.084 | .136* | .424** | .220** | .168 | 1 | | | | | | | |
| 업무연관성 | .157* | .050 | .158* | .024 | .184** | .098 | .023 | 1 | | | | | | |
| 위험인식 | .106 | .038 | .067 | .424** | -.377** | .236** | .076 | -.001 | 1 | | | | | |
| 성별 | -.052 | -.049 | -.003 | .071 | .058 | .049 | .080 | -.248 | .040 | 1 | | | | |
| 업종 | -.087 | -.010 | .089 | .078 | .141* | -.035 | .110 | -.161* | -.122 | .125 | 1 | | | |
| 회사규모 | .179** | .194** | .200** | -.180** | .170** | .190** | -.091 | .124 | -.118 | -.205** | -.140* | 1 | | |
| 나이 | .129* | .028 | .096 | .036 | -.152* | -.004 | -.046 | .265** | .183** | -.325** | .035 | -.116 | 1 | |
| 교육 정도 | -.021 | .009 | .082 | .217** | -.064 | -.097 | .081 | -.200** | .103 | -.017 | .276** | -.370** | .247** | 1 |

N=242, ** p<0.01, *<0.05

# Primary Factors Affecting Corporate Employees' Attitudes Toward Information Security

Joonkyong Park* · Beomsoo Kim** · Sungwoo Cho***

Abstract

Businesses have been adopting security systems and making a variety of practical policies promoting and implementing information security awareness among employees in order to safeguard valuable corporate information and resources. To achieve this goal, firms implement public relations activities and offer security and privacy education for their staffs continuously; in reality, however, corporate confidential information can be frequently stolen due to lack of employees' security awareness. The main purpose of this study is to investigate employees' attitudes toward enterprise information security based on the technology acceptance model (TAM) from both deterrence and control theory perspectives.

Technology acceptance models present perceived usefulness and the perceived ease of use as primary factors that affect employees' attitudes toward security. In relation to perceived usefulness and convenience, security policy, security systems, and education are chosen from deterrence theory. From control theory, punishment and rewards are identified as variables influencing employees' attitudes toward security. In addition to these variables, personal level characteristics can also play a role in shaping individuals' security attitude. Thus, personal experience, perceived risk, and the level of security involvement in their jobs are selected as additional variables.

Empirical analysis was conducted based on data collected from a total of 242 questionnaires. Regression analysis shows that security education, usefulness of reward, perceived security risk, and personal experience all directly and positively affect employees' security attitude.

* The purchasing division, LG CNS
** Graduate School of Information, Yonsei University
*** Management School, The University of Liverpool

Hypotheses on security policy and security systems from deterrence theory failed to be adopted. This result is strikingly different from the technology acceptance model. These results imply that enterprises should enhance security education and appropriate rewards which are essential for motivating employees on information security in an organization. This can help employees to recognize the risk of compromised information and provide personal experience so that they may continually strive to protect enterprise information and resources.

Up until now, little research has been conducted on employees security attitudes within an organization. Especially, this study focuses on significant factors which can affect employees' security awareness. However, we must discuss the limitations of this study. The study has been conducted via a questionnaire survey; the collected data is somewhat small in scale; and the extension of implications should be done with caution.

Key words: Enterprise-wide Security, Information Protection, Technology Acceptance Model, Deterrence Theory, Control Theory, Employee Security Attitude