조직구성원의 정보보안 의식과 조직의 정보보안 수준과의 관계 연구

정 해 철* · 김 현 수**

A study on the Relationship between Organizational Member's Information Security Mind and Organizational Information Security Level

Hae-Choul Jung* · Hyun-Su Kim**

Abstract

This study examines the relationship between the organizational member's information security mind and organizational information security level. The influential relationships among organizational members' information security mind are investigated, and the relationship between organization's information security level and information security mind has been analyzed.

As a result, top manager's information security mind is shown to give the biggest influence to other group in the organization. A strong positive correlation exists between organizational member's information security mind and the level of organization's physical, technical, managerial information security. However, there is no significant difference in information security level by types of business.

In the future, a more profound study on information security mind is necessary. And alternative methods of information security level estimation need to be studied.

* 국토연구원 GIS연구센터
** 국민대학교 정보관리학부

1. 서 론

최근 국내·외의 정보시스템 범죄나 정보 파괴·유출 같은 일련의 사건들은 정보화의 역기능으로서 기업은 물론 개인에게까지 많은 위협을 주고 있다. 특히 최근에 인터넷을 통한 정보시스템과 정보에 대한 위협이 증가하게 되었고, 결과적으로 조직의 정보시스템 및 정보에 대한 위험관리의 필요성이 대두되었다. 그러나 대부분의 기업들은 이에 대한 체계적인 대책보다는 부분적인 보안 시스템의 도입을 통해 해결하려는 경향을 보이고 있으며, 같은 업종의 경쟁기업이나 타 업종에서 성공한 보안 설비 및 대책을 여과없이 그대로 도입하는 경우가 많다. 이러한 현상은 기업의 문화, 환경 및 정보시스템 수준 등과 같은 상황적 요인을 고려하지 않았기 때문에 효율적인 정보보안을 기대하기 쉽지 않다.

국내 정보보안의 문제점으로 보안이 정보기술의 여타분야로 확장될 것이라는 기대심리는 높지만 아직은 그러한 기대심리에 인력이나 산업측면에서 모두 대응하기 어려운 상황이라고 보고 있다. 특히 정보보안 마인드가 부족하며, 해킹이나 바이러스 등 위협요소에 대한 인식이 약하고, 최고경영자의 마인드도 약한 것으로 평가되고 있다. 전자상거래가 부각되고 있지만 보안에 대한 관심도는 매우 낮으며, 또한 보안 관련 투자도 외국의 경우 정보기술 투자의 5%~7%를 정보보안에 투자하는데 반해 국내에서는 1~2% 미만에 머물고 있다[김홍선, 1999].

이와 같은 문제의식을 기초로 본 연구에서는 새로운 경영환경에 대처하기 위해서 국내 기업을 대상으로 보안수준과 조직 구성원들의 의식수준을 조사하여 이들간의 관계를 규명하고자 한다. 또한, 현재 국내 기업 및 조직의 보안수준과 조직구성원들의 의식수준을 분석·검토하고 문제점을 파악하여 개선방안을 도출하는데 본 연구의 목적이 있다.

이러한 연구 목적을 달성하기 위하여, 제 2장에서는 정보보안 개념과 정보보안 모델, 정보보안 지표 체계 등을 분석하고, 제 3장에서는 본 논문의 연구 모형과 연구가설의 도출 과정을 제시하고, 제 4장에서는 제시된 연구 모형을 토대로 연구가설에 대한 통계 분석 결과를 요약한다. 마지막으로 제 5장에서는 본 연구의 결론 및 향후 연구과제에 대하여 토의한다.

2. 정보보안의 개념과 지표

2.1 정보보안의 개념

2.1.1 정보보안의 정의

1960년대 초 시분할 시스템과 멀티 프로그래밍의 등장과 더불어 정보시스템의 보안에 대한 필요성이 인식되기 시작하였으며[Wilkes, 1991], 1967년에 미국에서 개최된 National Joint Computer Conference에서 컴퓨터 보안이 최초로 공개적으로 논의되기 시작하였다[Ware, 1988].

정보보안(Information Security)이란 '정보의 입력, 처리, 저장, 출력, 전송 등의 모든 단계에 걸쳐서 보호하는 것'을 말한다. 미국에서는 정보보안을 '시스템 및 정보를 고의 혹은 실수에 의한 공개, 변조, 파괴 및 지체로부터의 보호하는 활동'이라고 정의하고, 유럽에서는 '전자적인 형태의 정보를 처리, 통신, 저장의 모든 단계에 걸쳐서 보호하는 활동'으로 정의하고 있다[박태완, 1997]. 또한 '정보화촉진기본법'에서는 '정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 정보의 훼손, 변조, 유통 등을 방지하기 위한 관리적, 기술적 수단을 강구하는 것'이라고 정의하고 있다. 이러한 정의를 종합해 보면, 정보의 무결성, 비밀성, 가용성을 보장하고 정보의 정상적인 유지를 위하여 인위적, 물리적, 기술적, 자

연적인 장애요인을 사전에 예방 조치하고 사후 회복 조치하는 것이라고 볼 수 있다. 본 연구에서는 정보보안을 '시스템 및 정보를 고의 혹은 실수에 의한 공개, 변조, 파괴 및 지체로부터의 보호'라고 정의한다.

2.1.2 정보보안의 속성

정보보안의 정의인 '시스템 및 정보를 고의 혹은 실수에 의한 공개, 변조, 파괴 및 지체로부터의 보호'를 다른 말로 표현하면, 시스템 및 정보의 '기밀성(Confidentiality)', '무결성(Integrity)', '가용성(Availability)'을 확보하는 것이며 이들은 정보보안의 속성 혹은 목표가 될 수 있다[한국정보보호센터, 1996]. 기밀성(Confidentiality)은 정보는 소유자가 원하는 대로 비밀이 유지되어야 한다는 원칙이다. 정보는 소유자의 인가를 받은 사람만이 알아야 하며 인가되지 않은 정보의 공개는 절대로 금지되어야 함을 뜻한다. 무결성(Integrity)은 정해진 절차에 의해 그리고 주어진 권한에 의해서만 정보는 변경되어야 함을 의미한다. 정보는 항상 일정하게 유지되어야 하며, 오로지 인가 받은 방법에 의해서만 변경될 수 있다. 정보에 대한 정확도의 정도가 자세하게 명시되어 있어야만 하며 무결성에 대한 정책에는 정보 변경에 대한 통제뿐 아니라 오류나 태만으로부터의 예방도 포함해야 한다. 가용성(Availability)은 정보 시스템이 적절한 방법으로 작동되어야 하며 정당한 방법으로 권한이 주어진 사용자에게 정보 서비스가 거부되어서는 안된다는 것이다. 비행기 제어나 병원의 응급 시스템과 같이 생명이 관계된 상황에서는 적시에 주어지는 자원의 가용성은 무엇보다도 중요한 요소이다. 순서는 중요도(우선 순위)와도 상관관계가 있다. 원래 초기의 정보보안에 관한 연구는 대부분 미 국방성에 의해 주도되었으며 이로 인하여 기밀성이 가장 중요해졌고 무결성, 가용성 순으로 중요도가 결정되었다. 그러나 비밀을 취급하는 국가 기관을 제외한 일반적인 기업, 금융기관 등에서는 위의 우선 순위가 업종에 따라 달라질 수 있다.

2.1.3 정보보안 절차

정보보안은 프로세스적인 관점에서 보안계획, 위험분석, 보안설계, 정보시스템 보안구현, 사후관리 등으로 구분할 수 있다[김현수, 1999].

보안계획에서는 보안목표, 조직수준의 위협분석, 보안정책수립, 보안계획수립 등의 활동을 포함한다. 보안목표 설정 및 위협분석 활동은 보안의 본질 및 대상 정보시스템의 특징을 반영하여 수행되어야 한다.

위험분석 활동은 위협을 먼저 파악하고, 위험의 노출 정도를 분석하는 활동이라고 할 수 있다. 위험(Risk)은 '위협(Threat)이 현실적으로 발생하여 조직에 부정적인 영향을 미칠 수 있는 가능성'으로 정의된다. 위협(Threat)은 '주어진 상황에서 발생할 수 있는 그 어떤 사건'으로 정의되고 있다. 즉 위협은 위험을 발생시킬 수 있는 조건, 상황, 원인 제공자로서 정의된다. 위협을 식별할 때 일정한 분류법을 사용하면 식별이 용이하게 된다. 발생 가능한 위협의 유형에 대한 분류로 많이 사용되는 것은 다음과 같이 정보시스템 특성에 의한 분류, 위협의 원인에 따른 분류, 위협의 개념적 성격에 따른 분류 등이 있다[이형원, 1993].

보안 설계는 앞에서 도출된 보안 요구사항을 반영하여 보안 구조를 설계하는 활동이며, **보안 시스템 구현 활동**은 보안기능 구현 또는 제품 설치, 보안 교육, 보안성 평가, 승인 등의 세부 활동을 포함한다. 보안 구조는 물리적 보안, 기술적 보안, 관리적 보안 수단을 모두 고려하여 설계되어야 한다.

사후관리 활동은 첫째, 보안 유지보수와 관련하여 지속적으로 보안대책을 갱신 및 유지보수 하며, 위험을 유발할 수 있는 변경을 탐지하

기 위하여 변경사항에 대한 위협, 취약성, 자산 및 보안 대책을 감시하는 활동을 수행한다. 둘째, 보안 감시와 관련하여 정보를 보호하기 위한 보안기능들을 수행하고, 감사 추적과 보안관련 사항에 대한 조치와 보고 활동을 수행한다. 마지막으로 예상치 못한 사건에 대하여 적절한 조치를 취하기 위해서는 사건처리절차가 수립되어 있어야 한다.

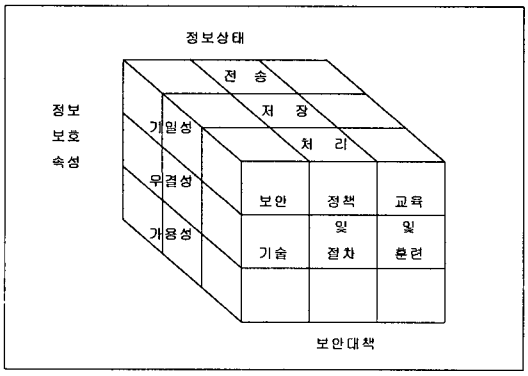
2.2 정보보안 모델체계

정보보안 모델의 구축을 위해서는 현재까지의 정보보안 기술 중심의 패러다임에서 정보 그 자체에 중점을 두는 패러다임으로의 변환이 필요하다[김정덕, 김기윤, 1998]. 정보는 어느 주어진 시점에서 전송, 저장, 처리라는 3가지 상태(state) 중의 어느 하나에 속해 있다. 이 3가지 상태는 정보 매개수단(media)에 관계없이 존재하므로 이 모델에서는 모든 정보 기술을 포함한다. 최종사용자는 정보의 특정 성격에 더 관심을 두고 있다. 정보의 특성은 내재적인 것으로서 정보보안 관련 특성은 기밀성, 무결성, 가용성으로 정의할 수 있으며, 이는 정보보안 모델의 구축에 중요한 구성요소이다.

보안 대책은 3개의 계층으로 분류할 수 있다. 첫 번째 계층은 보안 기술이다. 기술은 물리적 장치인 하드웨어, 펌웨어, 소프트웨어 형태로 구현된 것으로 정의할 수 있다. 두 번째 계층은 정책과 절차이다. 불법적인 소프트웨어 복제의 확산은 이러한 보안 정책의 부재에서 오는 대표적인 예이다. 마지막 계층은 정보보안에 관한 이해 수준을 표현한 것이라고 할 수 있는 교육, 훈련이라는 보안 대책이다.

기술과 정책은 여러 면에서 교육 및 훈련에 기초되어야 한다. 기술자와 과학자들은 정보보안의 원칙을 잘 이해하고 있어야 만이 시스템 설계 시 정보보안의 기능들을 포함시킬 수 있으며 효과적인 보안 정책의 구현을 위해서는 정보를 생성하고 사용하는 개인과 집단들이 교육 및 훈련을 통해 책임과 권한을 명확히 인지하고 있어야 한다. 따라서 교육 및 훈련은 효과적인 정보보안을 위한 기초적인 보안 대책이라고 할 수 있다.

(그림 1)은 3가지 정보 상태와 3가지 정보보안 속성의 조합인 9개의 독특한 상황이 있고 각 상황은 3개의 계층으로 구성된 모델을 보여준다.



(그림 1) 정보보안 모델체계

이 모델은 여러 면에서 적용 가능하다. 우선, 정보의 상태와 정보보안 속성으로 구성되는 2차원 메트릭스는 시스템 취약성을 파악하는데 사용되고 보안대책의 3계층은 이러한 취약성을 최소화시키기 위해 사용될 수 있다. 개발자는 이 모델을 이용하여 시스템 내의 다양한 정보상태를 파악할 수 있다. 일단 취약성이 파악되면, 보안대책의 3계층을 통해 정보보안 시스템 구축이 가능하다.

2.3 정보보안 지표 체계

2.3.1 정보보안 지표의 개념

정보보안 지표란 특정 조직의 정보보안 특성을 가장 간단하고 명확하게 나타내주는 통계수

치로서, 각종의 통계자료와 함께 정보보안 정책을 결정하는데 매우 유용하게 사용된다. 그러나 정보보안 지표는 산출방법이나 데이터 수집상의 문제로 인하여 현실적으로 많은 어려움을 수반하고 있다. 이상적인 정보보안 지표 개발을 위하여 요구되는 사항은 다음과 같다.

첫째, 정보보안의 범위와 목적을 분명하게 반영할 수 있어야 한다. 즉 정보보안과 관련된 여러 주체(사용자, 정보보안 산업, 일반 조직, 국가 등)의 관심과 현상을 표현할 수 있는 다양성을 포함하고 있어야 한다.

둘째, 정보보안 수준을 객관적이고 정확히 반영하고 측정할 수 있어야 한다.

셋째, 정보보안과 관련된 상황변화를 적절하게 반영할 수 있는 적시성을 구비하여야 한다.

넷째, 미래의 예측까지 가능하게 하는 체계적인 방법이어야 한다.

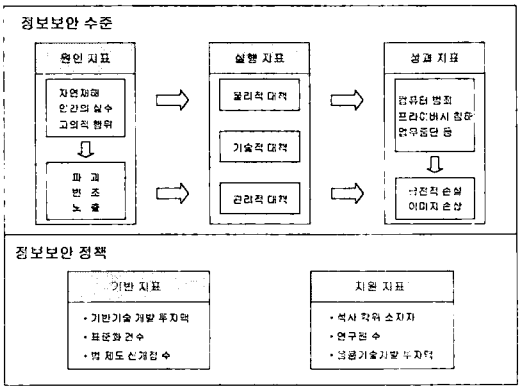
다섯째, 지표 측정이 현실적으로 가능하고 많은 비용을 초래하지 않아야 한다.

마지막으로 정보보안 지표 항목을 적절하게 통합할 수 있는 가중치 적용방법이 도출되어야 한다.

2.3.2 정보보안 지표 체계

(그림 2)는 정보보안 지표 체계를 이해하기 쉽게 잘 설명해 주고 있다. (그림 2)는 위협과 정보보안 대책간의 상관관계로 인하여 손실이 발생한다는 것에 기초하여 원인지표로서 위협요인을, 실행지표로서 정보보안 대책을, 성과지표로서 손실의 여러 형태를 포함하여 정보보안 수준을 측정하고 있다.

또한, 정부의 정보보안 정책이 정보화의 역기능을 감소시키고 정보보안 산업의 경쟁력 강화를 통해 안전하고 신뢰성 있는 정보서비스를 제공함으로서 건실한 정보화 사회로 이행하려는 목표를 달성하는데 기반이 된다고 보고, 정부가 해야할 역할을 정보보안 기반기술 개발의 촉진, 기술 표준화, 수요 창출을 위한 관련 법/제도 정비 등을 수행하는 기반(Infrastructure)구축 기능과 정보보안 전문인력 양성과 관련 산업체의 육성을 위한 투자를 담당하는 지원 기능으로 구분하고 있다.



(그림 2) 정보보안 지표 체계

2.3.3 국내외 정보보안 지표 체계 비교

정보보안 지표 연구는 직접적인 지표개발 목적으로 수행된 경우는 극소수이고, 정보시스템 감사 등의 목적으로 개발된 체크리스트 개발 연구가 대부분이다. 최근 국내의 관련 연구로는 김정덕과 김기윤(1998)의 '정보보호 지표 항목 개발 및 계량화 연구', 이형원(1993)의 '정보시스템 보안대책' 등이 있으며, 국외의 대표적인 지표로서 영국의 'BS7799'를 들 수 있다.

김정덕과 김기윤(1998)의 '정보보호 지표 항목개발 및 계량화 연구'에서는 관련 연구를 참조하여 기본통제에 관한 항목들을 도출하였다. 도출된 지표는 산출지표, 결과지표, 영향지표로 분류되었다. 산출지표는 보안장치의 생산성 및 효율성을 측정하고, 결과지표는 정보자산의 효과성을 측정하며, 1차적 영향지표는 내부업무의 효율성을, 2차적 영향지표는 정보통신인프라의 효과성을 측정한다.

이형원(1993)의 '정보시스템 보안대책'에서는 설비기준, 기술기준, 운용기준으로 구분하고, 그에 따른 세부 점검항목들로 구성되어 있다.

영국은 정보보안관리 지침인 'BS7799'를 토대로 정보보안 수준을 평가하고 있다. 'BS7799'에서 제시되는 주요 내용은 보안정책, 보안조직, 자산의 분류와 접근통제, 인사보안, 물리적·환경적 보안, 컴퓨터 및 네트워크 관리, 시스템 접근제어, 시스템 개발 및 유지보수, 업무지속성 계획, 준거성 등 10가지 항목으로 구분하여 평가하고 있다.

이러한 기존의 연구에서 도출된 정보보안 지표 항목과 계량화 방식은 대체로 물리적 보안, 논리적 보안, 관리적 보안 등 3가지 관점에서 지표 항목을 분류하고, 단순 가중치법을 사용하여 정보보안 수준을 지수화한다.

따라서, 기존의 연구는 크게 3가지 관점에서 문제점이 있다고 할 수 있다. 우선 보안시스템 자체의 완전성을 주목적으로 보안 지표 항목이 설계되어 있다. 이는 기업이나 국가의 관점에서 보안시스템을 조직의 목적에 맞게 활용하려 할 때, 정확한 정책방향을 제공하는데 문제가 있다.

또한 기존의 지표구성은 환경요소의 반영이 미흡하다. 구성원의 마인드(인식), 관련 규정/법/제도 등이 보안시스템의 평가에 중요한 변수가 될 수 있다.

마지막으로 보안은 정보시스템의 발전과 함께 지속적으로 발전되는 분야이다. 기존의 보안 지표 항목은 신기술의 반영이 미흡하다. 예를 들어 방화벽, 네트워크 보안, 바이러스 대책 등과 같은 신규 분야를 지표에 편입시키는 것이 필요하다.

이러한 요구사항을 충실히 반영된 지표항목으로 김현수 등(1999)의 '정보보안 지표 개발에 관한 탐색적 연구'에서의 지표항목을 들 수 있다. 이 연구에서는 정보보안의 분야와 정보보안의 목적 적합성 관점에서 지표 항목을 도출하였다. 위 연구에서는 정보보안을 크게 정보보안 기술, 정보보안 의식, 정보보안 제도 및 표준 등의 분야로 구분하여 하위 구성요소들로 세분하였다. 정보보안 기술은 정보보안 관리적 요소, 물리적 요소, 기술적 요소를 포함하며, 일반적인 사항으로서 정보보안 제도 및 표준 등의 분야를 포함하였다. 본 연구에서는 이 연구의 정보보안 지표 항목을 이용하여 정보보안 수준을 측정하였다.

3. 연구모형

3.1 개 요

일반적으로 정보보안을 위한 기본통제의 분류체계는 위협, 자산, 취약성에 대한 학자들의 관점에 따라 서로 다르다. 그 중에서도 현재 국·내외에서 가장 많이 쓰이고 있는 Solms 등[1990]의 분류체계를 살펴보면, 정보보안 통제에 대한 표준적인 분류체계를 물리적 보안, 논리적 보안, 관리적 보안으로 구분하고, 이에 대한 하위 구성요소들로 세분하여 분류하고 있다. 이러한 분류체계를 기초로 한 많은 연구들이 수행되었으며, 최근의 국내 연구로서 다음과 같은 연구들을 들 수 있다.

선행연구인 김정덕, 김기윤[1998]의 '정보보호 지표 항목개발 및 계량화 연구'에서는 (그림 2)의 정보보안 지표 체계에서 실행지표를 취약성 분류체계에 의하여 보안 지표를 개발하고자 하였다. 즉, 자산에 손실이 발생될 수 있는 약점을 식별하고 분류하여 위협을 감소시키는 취약성 평가에 중점을 두고 보안지표를 개발하였다. 이 연구에서도 정보보안 지표의 분류체계는 물리적, 기술적(논리적), 관리적 보안으로 구분하여 세부항목들을 도출하고 있다.

또한, 선행연구인 김현수 등[1999]의 '정보보안 지표 개발에 관한 탐색적 연구'에서는 정보보안의 분야와 정보보안의 목적 적합성 관점에서 지표 항목을 도출하였다. 이 연구에서는 정보보안을 크게 정보보안 기술, 정보보안 의식, 정보보안 제도 및 표준 등의 분야로 구분하여 하위 구성요소들로 세분하였다. 정보보안 기술은 정보보안 관리적 요소, 물리적 요소, 기술적 요소를 포함하며, 일반적인 사항으로서 정보보안 제도 및 표준 등의 분야를 포함하였다.

본 연구는 위 연구에서 개발한 정보보안 지표를 적용하여 조직구성원간의 정보보안 의식 관계, 조직구성원의 정보보안 의식과 조직의 정보보안 수준과의 관계를 연구하고, 추가적으로 업종에 따라 조직의 정보보안 수준에 차이를 보이는지에 대하여 연구하였다. 이를 위하여 다음과 같은 기본통제 요소들로 분류하고, 그에 따른 변수들을 설정하였다. 즉, 기본적인 분류는 선행연구들의 물리적 보안, 기술적 보안, 관리적 보안에 정보보안 의식 요소를 추가하여 대항목으로 설정하였다.

이들 중 물리적 보안, 기술적 보안, 관리적 보안을 정보보안 구성요소로 설정하고, CEO의 정보보안 의식, CIO의 정보보안 의식, 직원들의 정보보안 의식을 정보보안 의식에 대한 구성요소로 설정하였다. 또한 추가분석으로 업종을 추가하여 업종과 조직의 정보보안 수준, 업종과 조직구성원의 정보보안 의식과의 관계를 연구하였다.

3.2 가설의 설정

3.2.1 조직구성원간의 정보보안 의식 영향관계

정보보안과 관련된 조직구성을 보면, CEO, CIO 그리고 일반직원들로 구분할 수 있다. Straub와 Welke[1998]에 의하면 정보보안(Information Security)은 최고경영자, 중간관리자, 그리고 직원에 이르기까지 모든 조직구성원들에 의해 무시되어왔다고 한다. 그러한 무시의 결과로 조직 시스템이 안전과는 더욱 멀어지게 되었으며, 보안 침해의 사례가 더욱 늘고, 그 결과로 인한 손해는 더욱 증가되었다고 보고 있다. 주목할 만한 문제는 많은 경영자들이 시스템 위험(Risk)의 본질을 제대로 인식하지 못하고 있다는 것이다.

또한, 이러한 조직구성원들간의 영향관계를 보면 CEO의 의지는 CIO와 직원들 모두에게 여러 가지 경로를 통하여 영향을 미치게 된다. 또한 CIO의 의지는 직원들에게 직·간접적으로 영향을 준다고 볼 수 있다. 따라서, 다음과 같은 가설의 설정이 가능하다.

[가설 1] 상급자의 정보보안 의식 수준이 높으면 하급자의 정보보안 의식 수준도 높다.

[가설 1-1] CEO의 정보보안 의식 수준이 높으면 CIO의 정보보안 의식수준도 높다.

[가설 1-2] CEO의 정보보안 의식 수준이 높으면 직원들의 정보보안 의식 수준도 높다.

[가설 1-3] CIO의 정보보안 의식 수준이 높으면 직원들의 정보보안 의식 수준도 높다.

3.2.2 조직구성원의 정보보안 의식과 조직의 정보보안 수준과의 관계

조직구성원의 정보보안 의식은 조직의 정보보안 수준에 영향을 미칠 수 있는 요인이다. 이러한 요인은 다음과 같은 이유에서 정보보안 수준에 영향을 미친다고 볼 수 있다.

첫째, 최고경영자(CEO)는 정보기술의 실행에 수반되는 모든 인적, 물적 자원에 대한 결정 권

한을 가지는 사람이라고 할 수 있다[Zmud and Cox, 1979]. 또한 이들은 정보기술 실행의 활동에 대한 개괄적인 지침을 제시해야 하는 책임을 가진다[Doll, 1985].

많은 연구에서 최고경영자의 지원이 성공적인 정보기술 구축의 결정요인이 될 수 있음을 제시하고 있다[Willoughby and Pye, 1977]. 이처럼 정보기술이 조직에서 성공적으로 실행되기 위해 최고경영자의 지원이 중요시되는 이유는 정보기술의 도입이 조직 사업중의 하나이기 때문이다[Cash et al., 1992].

정보보안과 관련된 각종 자원에의 투자결정 역시 CEO의 의지에 달려있으며, 이러한 투자결정을 위해서는 CEO가 정보보안의 필요성을 인식하고, 관련 지식을 갖고 있을 때 가능한 것이다.

둘째, 기업에서 정보시스템, 정보기술 및 정보자원을 관리하는 최고 책임자에 관한 논의는 연구자별로 다르게 제시되고 있다. 1970년대까지는 CIO라는 전문용어보다는 자료처리 관리자 또는 정보시스템 관리자라는 용어가 기업의 정보시스템을 담당하는 최고 직책을 의미하였으며, 1980년대부터 CIO라는 용어가 사용되었다[이재범, 안상협, 1997].

Ives와 Olson[1981]은 최고정보중역(CIO)은 기술자이기보다는 조직 전체에 실제적인 영향을 주는 일반적 관리자로서 대인관계 기술을 갖추고 있어야 하고, 부하 직원에 대한 동기부여와 지휘 능력 등을 갖출 것을 요구받는다고 하였다.

Grover 등[1993]은 CIO는 기업외부의 경쟁환경에 대응하기 위해서 최고 경영진과 효과적인 의사소통을 필요로 하고, 정보자원 관리에서 기업차원의 거시적 관점을 유지해야 하며, 조직전략에 대한 영향 및 정보기술 계획 수립에 대한 책임을 지는 등의 관리적 역할을 수행하는 상위수준의 정보시스템 담당 임원이라고 규정하였다.

이상과 같은 CIO의 역할은 조직의 전반적인 정보시스템에 큰 영향을 미치게 된다. 즉, 최고경영자와 일반 직원들 사이의 정보보안에 대한 의사소통 기능을 할 수 있는 위치에 있는 것이다.

셋째, 미국의 '98년 CSI/FBI 컴퓨터 범죄 및 보안 실태조사에 따르면, '97년 이후 내부자에 의한 정보 오남용사고가 전체 응답기관중 78%로 나타났다고 보고하고 있다. 영국의 비즈니스 인포메이션 시스템사에서 문서화한 컴퓨터 범죄자의 유형 중 내부자에 의한 범죄가 인가·비인가자를 합하여 75%를 보여주고 있다. 특히 인가된 내부자가 58%로 비인가된 내부자 17%에 비해 3배 이상 많은 것으로 조사되었다. 주요 침해범죄는 불만 직원과 임시직 직원에 의한 내부정보 및 정보자산의 유출 및 파괴, 스파이들에 의한 내부 정보의 유출 등으로 나타났다.

우리나라의 경우 '98년 1/4분기 동안 언론에 보도된 국내 정보보안 침해사례 중 내부자에 의한 정보오남용은 약 35%를 차지하고 있으며, 주요 유형은 금융기관에서의 컴퓨터 단말기 조작이나 텔레뱅킹을 통한 범죄가 대부분이며 내부직원에 의한 자료유출과 일반기업에서의 자료변조 등으로 나타났다[한국정보보호센터, 1999].

이와 같은 조직의 내부에서 나타나고 있는 내부자 정보오남용 현상은 주로 임직원, 퇴직자, 또는 협력관계의 직원에 의해 발생하며, 특히 실무를 담당하는 담당자에 의해 나타나고 있어 방지와 적발이 어렵다. 따라서, 효과적인 정보보안의 구현을 위해서는 정보를 생성하고 사용하는 내부 직원들에 대하여 교육 및 훈련을 통한 책임과 권한을 명확히 인지시키고, 철저한 정보보안 의식을 고취시키는 것이 가장 중요하다.

결국 조직 구성원인 직원들에 대한 합리적인 책임부여와 체계적인 교육을 통한 의식의 전환

을 통하여 조직의 정보보안의 효과를 높일 수 있다고 할 수 있다[김영결 등, 1998].

따라서 다음과 같은 가설들의 설정이 가능하다.

[가설 2] 조직구성원의 정보보안 의식 수준이 높으면 조직의 물리적 정보보안 수준도 높다.

[가설 2-1] CEO의 정보보안 의식 수준이 높으면 조직의 물리적 정보보안 수준도 높다.

[가설 2-2] CIO의 정보보안 의식 수준이 높으면 조직의 물리적 정보보안 수준도 높다.

[가설 2-3] 직원들의 정보보안 의식 수준이 높으면 조직의 물리적 정보보안 수준도 높다.

[가설 3] 조직구성원의 정보보안 의식 수준이 높으면 조직의 기술적 정보보안 수준도 높다.

[가설 3-1] CEO의 정보보안 의식 수준이 높으면 조직의 기술적 정보보안 수준도 높다.

[가설 3-2] CIO의 정보보안 의식 수준이 높으면 조직의 기술적 정보보안 수준도 높다.

[가설 3-3] 직원들의 정보보안 의식 수준이 높으면 조직의 기술적 정보보안 수준도 높다.

[가설 4] 조직구성원의 정보보안 의식 수준이 높으면 조직의 관리적 정보보안 수준도 높다.

[가설 4-1] CEO의 정보보안 의식 수준이 높으면 조직의 관리적 정보보안 수준도 높다.

[가설 4-2] CIO의 정보보안 의식 수준이 높으면 조직의 관리적 정보보안 수준도 높다.

[가설 4-3] 직원들의 정보보안 의식 수준이 높으면 조직의 관리적 정보보안 수준도 높다.

3.2.3 업종에 따른 조직구성원의 정보보안 의식 수준의 차이

조직구성원의 정보보안 의식에 영향을 미칠 수 있는 요인으로서 조직 문화특성을 들 수 있다. 모든 조직은 각자의 문화를 가지고 있다. 이러한 조직문화는 "조직변화 과정에서의 가치, 규범 등 문화적 요인으로 인해 생성되는 조직구성원의 행동과 조직체계를 형성하고 이들을 연결, 조정하는 종합요소"로 정의된다[김인수, 1996]. 특히 조직구성원들이 정보보안에 대해서 갖는 심리적 분위기는 조직에서의 정보보안에 대한 기대, 자세, 수용 태도와 선입견을 의미한다. 이러한 조직문화는 업무의 유형과 특성에 따라 공통점을 보이게 된다. 즉 업종에 따라 공통점을 갖는다는 것이다. 따라서 다음과 같은 가설의 설정이 가능하다.

[가설 5] 업종에 따라 조직구성원의 정보보안 의식 수준에 차이가 있을 것이다.

[가설 5-1] 업종에 따라 CEO의 정보보안 의식 수준에 차이가 있다.

[가설 5-2] 업종에 따라 CIO의 정보보안 의식 수준에 차이가 있다.

[가설 5-3] 업종에 따라 직원들의 정보보안 의식 수준에 차이가 있다.

3.2.4 업종에 따른 조직의 정보보안 수준의 차이

조직의 정보보안 수준에 큰 영향을 미치는 요인들로 조직의 규모와 위협에 대한 민감도를 들 수 있다. 규모가 큰 조직일수록 작은 조직에 비해 더욱 많은 자원을 확보하는 것이 용이하다[Karimi, 1988]. 일반적으로 규모가 큰 조직은

작은 조직에 비해 풍부한 인력이나 자금력을 가지고 조직구조나 기능면에서 훨씬 저렴하고 잘 개발된 정보시스템을 구축할 수 있다. 그러나 이러한 규모의 차이는 비용면에서의 부담의 차이가 있을 뿐 보안을 위한 대책이나 수준에는 큰 영향을 미치지 못한다. 예를 들어, 은행의 경우 규모의 차이는 있으나, 기본적인 보안대책은 거의 동일하다. 따라서, 업종의 유형에 따라서 보안수준의 차이가 있다고 볼 수 있다.

또한 위협에 대한 민감도는 위협 발생 시 조직에 미치는 영향으로 판단되며, 영향이 클수록 그에 따른 대책에 많은 인적·물적 자원을 투입하게 된다. 따라서 다음과 같은 가설의 설정이 가능하다.

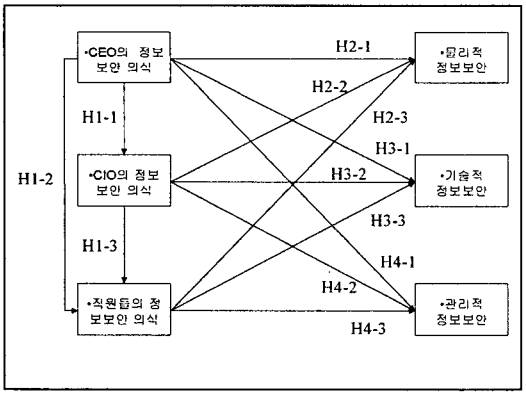
[가설 6] 업종에 따라 조직의 정보보안 수준에 차이가 있을 것이다.

[가설 6-1] 업종에 따라 조직의 물리적 정보보안 수준에 차이가 있다.

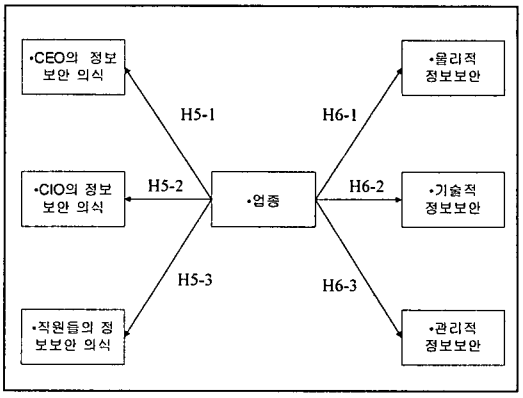
[가설 6-2] 업종에 따라 조직의 기술적 정보보안 수준에 차이가 있다.

[가설 6-3] 업종에 따라 조직의 관리적 정보보안 수준에 차이가 있다.

이러한 가설의 구조를 그림으로 도시하면 아래 (그림 3), (그림 4)와 같다.



(그림 3) 연구의 모형



(그림 4) 추가 분석 모형

3.3 자료수집 방법 및 표본 특성

본 연구에서는 제시된 가설을 검증하기 위하여 국내 중소·중견기업 및 대기업을 대상으로 조사서를 이용하여 자료를 수집하였다. 조사대상 기업의 선정은 정보보안 관련 공공기관에 등록된 기업을 대상으로 담당자와 전화 인터뷰 후 E-MAIL로 조사서를 전송하여 E-MAIL 또는 FAX로 회수하였다. 총 조사대상 기업 수는 120개 기업이었으며, 회수 기업 수는 52개 기업으로 회수율은 43.3%의 비교적 높은 회수율을 보였다.

조사서는 보안 관련 경력이 2년 이상 되는 대리급 이상의 사원들이 응답하였으며, 실제로 해당 기업의 보안을 담당하는 담당자들이었다. 대기업들은 그룹 및 각 계열사에 보안을 담당하는 팀을 보유하고 있었으며, 정보시스템 관련 중소·중견 기업들은 대체로 보안 관련 팀은 없으나 보안을 전담하는 담당자들을 두고 있었다.

응답 기업의 특성으로 업종만을 고려하였으며, 아래 <표 1>에 응답기업 분포를 제시하였다.

업종별 분포는 총 52개 응답기관중 정보통신이 14개(26.9%) 기관으로 가장 많이 응답했으며, 제조/일반산업 12(23.1%), 금융 9(17.3%), 정부/공공기관 8(15.4%), 유통/도소매업 5(9.6%),

건설업 4개 기관(7.7%)의 순으로 분포를 보이고 있다.

〈표 1〉 응답기업의 업종별 분포

업 종 구 분	빈도	퍼센트	유효퍼센트	누적퍼센트
금 융	9	17.3	17.3	17.3
제조/일반산업	12	23.1	23.1	40.4
정 보 통 신	14	26.9	26.9	67.3
정부/공공기관	8	15.4	15.4	82.7
유 통/도소매	5	9.6	9.6	92.3
건 설	4	7.7	7.7	100
합 계	52	100	100	

4. 결과분석 및 가설검증

본 연구에서는 앞 장에서 제시한 연구가설을 검증하기 위하여 SPSSWIN 7.5를 이용하였다.

4.1 신뢰성 및 타당성 분석

신뢰성(Reliability)은 동일한 개념에 대해 반복적으로 측정했을 때 나타나는 측정값들의 분산을 의미하는 것으로, 본 연구에서는 연구모형을 토대로 단일 차원으로 구성된 개념 내에서 실시하였다.

본 연구모형에서는 사용된 요인들을 동일한 개념으로 측정하기 위해 다항목이 이용되었으므로 동일한 측정을 위한 항목간의 평균적인 관계를 살펴보는 크론바하 알파(Cronbach's Alpha) 계수에 의한 내적 일관성 분석을 실시하였다. 이 방법을 사용하면 집단수준에서의 구성개념과 그리고 개인수준에서의 각 항목의 신뢰도를 각각 평가할 수 있다.

일반적으로 집단수준인 경우에는 크론바하 알파(Cronbach's α) 계수가 0.5 이상, 각 개별수준인 경우에는 0.9 이상이면 신뢰도가 높다고 할 수 있다[강병서, 1999].

본 연구에서는 <표 2>에서 보는 바와 같이 모든 측정변수의 알파 계수가 0.9023 이상으로 높게 나타났다. 따라서 분석단위가 집단(조직)인 연구에서 요구되는 신뢰성 수준을 충족시켜 주고 있다. 따라서 본 연구의 다항목 변수들은 구성항목 측정치의 산술평균치로서 유효하게 이용될 수 있으므로 이후 분석에서는 각 변수별 측정치를 이들 다항목 척도의 산술평균값으로 대체하여 사용하기로 한다.

〈표 2〉 연구변수 측정항목의 신뢰성 분석

측 정 변 수		항목수	Cronbach's α
조직구성원의 정보보안 의식	CEO의 정보보안의식	3	.9053
	CIO의 정보보안의식	3	.9500
	직원들의 정보보안의식	3	.9023
조직의 정보보안 수준	물리적 정보보안	18	.9571
	기술적 정보보안	27	.9734
	관리적 정보보안	20	.9702

타당성(Validity)은 측정하고자 하는 개념이나 속성을 어느 정도로 정확하게 측정하였는가를 나타낸다. 본 논문의 연구변수들을 구성하고 있는 항목들은 기존의 정보보안 측정 지표들을 바탕으로 하여 종합적으로 도출하여 보안관련 현업 전문가들로부터 내용타당성이 있는 것으로 인정받았다.

통계적인 구성타당성을 검증하는 방법으로는 흔히 요인분석기법이 사용된다. 본 연구에서 사용된 표본 수는 모두 52개로 요인분석을 할 수 있는 조건, 즉 요인분석 대상 항목 수(74개)에 비해 4~5배 이상의 표본 수 확보조건을 충족하지 못하고 있으므로 요인분석은 큰 의미가 없다고 판단된다.

4.2 연구변수의 기술통계량 및 상관관계 분석

4.2.1 기술통계량

본 연구에 포함된 조직구성원(CEO, CIO, 직

원들)의 정보보안 의식과 조직의 정보보안 수준(물리적, 기술적, 관리적 정보보안) 변수들에 대하여 5점 리커트 척도를 이용하여 측정하였다. <표 3>은 측정된 변수들의 기술 통계량을 보여주고 있다. 모든 변수의 평균값이 '보통'을 의미하는 3점 이상으로 비교적 높았으며, 상대적으로 물리적 정보보안과 관리적 정보보안에 대한 평가가 낮게 나타났다.

〈표 3〉 측정변수의 기술통계량

측 정 변 수		표본수	최소	최대	평균	표준편차	분산
조직구성원의 정보보안 의식	CEO의 정보보안 의식	52	1.67	5.00	3.47	.906	.821
	CIO의 정보보안 의식	52	2.00	5.00	3.71	.873	.763
	직원들의 정보보안 의식	52	1.00	5.00	3.34	.807	.651
조직의 정보보안 수준	물리적 정보보안	52	1.60	4.52	3.16	.810	.656
	기술적 정보보안	52	1.69	4.73	3.42	.746	.556
	관리적 정보보안	52	1.42	4.52	3.03	.782	.611

<표 3>의 기술통계량은 모든 변수들의 분포가 최대값 쪽으로 다소 치우쳐 있는 것을 보여주고 있다. 이것은 우리나라 기업들에 있어서 정보보안에 대한 인식이 확산되고 있음을 의미한다. 최근 국·내외의 잇따른 정보보안 사고로 인하여 정보보안에 대한 공감대가 형성되었기 때문이라고 판단된다.

4.2.2 상관관계 분석

본 연구에서는 모든 변수가 등간척도로 측정되었다. 따라서 모든 변수 상호간의 피어슨(Pearson) 상관분석을 실시하였다. <표 4>에서 보는 바와 같이 상관관계 분석 결과 모든 변수들간의 상관관계가 유의수준 0.01에서 유의한 것으로 나타났다.

특히 CEO의 정보보안 의식은 직원들보다 CIO의 정보보안 의식과 더 높은 상관관계를 보이고 있으며, 직원들의 정보보안 의식은 CEO의 정보보안 의식보다는 CIO의 정보보안 의식과 더 높은 상관관계를 보여주고 있다.

〈표 4〉 측정변수간 상관계수

Pearson 상관	CEO의 정보보안 의식	CIO의 정보보안 의식	직원들의 정보보안 의식	물리적 정보보안	기술적 정보보안	관리적 정보보안
CEO의 정보보안 의식	1.000					
CIO의 정보보안 의식	.887 (**)	1.000				
직원들의 정보보안 의식	.702 (**)	.726 (**)	1.000			
물리적 정보보안	.663 (**)	.615 (**)	.584 (**)	1.000		
기술적 정보보안	.727 (**)	.676 (**)	.652 (**)	.904 (**)	1.000	
관리적 정보보안	.742 (**)	.679 (**)	.628 (**)	.857 (**)	.891 (**)	1.000

** 상관계수는 0.01 수준(양쪽)에서 유의함.

4.3 가설의 검증

앞에서 설정한 가설을 검증하기 위하여 회귀분석과 분산분석을 이용하였다. 먼저 [가설 1]~[가설 4]는 회귀분석을 이용하여 검정하였으며, [가설 5]와 [가설 6]은 분산분석을 이용하여 검정하였다.

4.3.1 조직구성원간의 정보보안 의식 영향 관계 분석

[가설 1-1]을 검정하기 위하여 'CIO의 정보보안 의식'을 독립변수, 'CEO의 정보보안 의식'을 종속변수로 하여 회귀분석을 실시한 결과, 회귀식의 통계적 유의성을 검정하는 F통계량 값이 184.173이고 이에 대한 유의수준이 0.000으로 나타났다.(회귀식은 Y(CIO의 정보보안 의식) = 0.741 + 0.855 X1(CEO의 정보보안 의식)임). 따라서 [가설 1-1]의 'CEO의 정보보안 의식 수준이 높으면 CIO의 정보보안 의식 수준도 높다'는 가설을 채택한다.

[가설 1-2]와 [가설 1-3]을 검정하기 위하여 회귀분석을 실시한 결과 F통계량 값이 각각 48.573, 55.720으로 모두 유의수준 0.05에서 유의하게 나타났다. 따라서 [가설 1-2]의 'CEO의 정보보안 의식 수준이 높으면 직원들의 정보보안 의식 수준도 높다'는 가설과 [가설 1-3]의 'CIO의 정보보안 의식 수준이 높으면 직원들의 정보보안 의식 수준도 높다'는 가설을 모두 채택한다.

[가설 1]의 '상급자의 정보보안 의식 수준이 높으면 하급자의 정보보안 의식 수준도 높다'라는 기본가설에서 직원들의 상급자 계층은 CEO와 CIO 모두가 해당되므로 단계적으로 투입하는 stepwise 방식을 이용하여 회귀분석을 실시하였다. 그 결과 'CEO의 정보보안 의식' 변수가 제외되고 'CIO의 정보보안 의식' 변수만이 회귀식에 반영되었다. 이는 'CEO의 정보보안 의식'보다는 'CIO의 정보보안 의식'이 '직원들의 정보보안 의식'에 더 많은 영향을 미친다고 할 수 있다.

이상의 검정결과를 종합하면 다음의 <표 5>와 같다.

[가설 2]~[가설 4]의 검정에서는 각 변수간의 상관관계가 매우 높기 때문에 다중공선성 문제를 피하기 위해 stepwise 방식을 이용하였다.

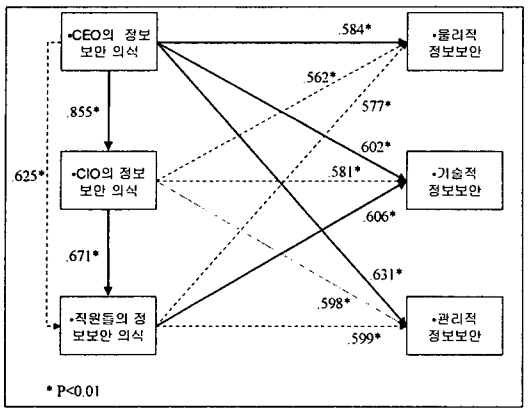
〈표 5〉 조직구성원간의 정보보안 의식 영향 관계에 대한 검정결과

가설 번호	가 설 내 용	검 정 결 과
가설 1	상급자의 정보보안 의식 수준이 높으면 하급자의 정보보안 의식 수준도 높다.	
가설 1-1	CEO의 정보보안 의식 수준이 높으면 CIO의 정보보안 의식 수준도 높다.	채택
가설 1-2	CEO의 정보보안 의식 수준이 높으면 직원들의 정보보안 의식 수준도 높다.	채택
가설 1-3	CIO의 정보보안 의식 수준이 높으면 직원들의 정보보안 의식 수준도 높다.	채택

[가설 2]를 검정하기 위하여 'CEO의 정보보안 의식', 'CIO의 정보보안 의식', 그리고 '직원들의 정보보안 의식' 등 3개의 변수를 독립변수로, '물리적 정보보안'을 종속변수로 하여 분석한 결과 'CIO의 정보보안 의식' 변수와 '직원들의 정보보안 의식' 변수 2개가 제거되고 'CEO의 정보보안 의식' 변수만이 투입되었다.(회귀식은 Y(물리적 정보보안) = 1.134 + 0.584 X1(CEO의 정보보안 의식) 임 : $p = 0.001 < 0.05$). 따라서 조직의 물리적 정보보안에 가장 많은 영향을 미치는 변수는 'CEO의 정보보안 의식' 변수인 것으로 분석되었다.

또한 [가설 3]의 검정에서도 위에서와 같이 'CEO의 정보보안 의식', 'CIO의 정보보안 의식', 그리고 '직원들의 정보보안 의식' 등 3개의 변수를 독립변수로, '기술적 정보보안'을 종속변수로 하여 분석한 결과 'CIO의 정보보안 의식' 변수만이 제거되고 'CEO의 정보보안 의식' 변수와 '직원들의 정보보안 의식' 변수 2개가 투입되었다.(회귀식은 Y(기술적 정보보안) = 0.986 + 0.439 X1(CEO의 정보보안 의식) + 0.260 X2(직원들의 정보보안 의식) 임). 결과적으로 조직의 기술적 정보보안에 영향을 미치는 변수로서 'CEO의 정보보안 의식'과 '직원들의 정보보안 의식' 변수가 유의하게 영향을 미치는 것으로 분석되었다.

마지막으로 [가설 4]의 검정은 위와 같은 독립변수와, '관리적 정보보안'을 종속변수로 하여 분석한 결과 [가설 2]의 검정에서와 같이 'CIO의 정보보안 의식' 변수와 '직원들의 정보보안 의식' 변수 2개가 제거되고 'CEO의 정보보안 의식' 변수만이 투입되었다. (회귀식은 Y(관리적 정보보안) = 0.845 + 0.631 X1(CEO의 정보보안 의식) 임 : $p = 0.05$). 따라서 조직의 관리적 정보보안에 'CEO의 정보보안 의식' 변수가 유의하게 영향을 미치는 것으로 분석되었다.



(그림 5) 연구모형의 회귀분석 결과(회귀계수)

〈표 6〉 조직구성원의 정보보안 의식과 조직의 정보보안 수준과의 관계에 대한 검정결과

가설 번호	가 설 내 용	검정 결과
가설 2	**조직구성원의 정보보안 의식 수준이 높으면 조직의 물리적 정보보안 수준도 높다.**	
가설 2-1	CEO의 정보보안 의식 수준이 높으면 조직의 물리적 정보보안 수준도 높다.	채택
가설 2-2	CIO의 정보보안 의식 수준이 높으면 조직의 물리적 정보보안 수준도 높다.	기각
가설 2-3	직원들의 정보보안 의식 수준이 높으면 조직의 물리적 정보보안 수준도 높다.	기각
가설 3	**조직구성원의 정보보안 의식 수준이 높으면 조직의 기술적 정보보안 수준도 높다.**	
가설 3-1	CEO의 정보보안 의식 수준이 높으면 조직의 기술적 정보보안 수준도 높다.	채택
가설 3-2	CIO의 정보보안 의식 수준이 높으면 조직의 기술적 정보보안 수준도 높다.	기각
가설 3-3	직원들의 정보보안 의식 수준이 높으면 조직의 기술적 정보보안 수준도 높다.	채택
가설 4	**조직구성원의 정보보안 의식 수준이 높으면 조직의 관리적 정보보안 수준도 높다.**	
가설 4-1	CEO의 정보보안 의식 수준이 높으면 조직의 관리적 정보보안 수준도 높다.	채택
가설 4-2	CIO의 정보보안 의식 수준이 높으면 조직의 관리적 정보보안 수준도 높다.	기각
가설 4-3	직원들의 정보보안 의식 수준이 높으면 조직의 관리적 정보보안 수준도 높다.	기각

(그림 5)는 [가설 1]~[가설 4]의 회귀분석결과를보여주고 있다. 점선으로 표시된 화살표는 단계적 투입방식(stepwise)으로 회귀분석을 수행하였을 때 제거된 변수간의 관계를 나타내고, 실선으로 표시된 화살표는 투입된 변수간의 관계를 보여주고 있다. 또한 위에서의 검정결과를 요약하면 <표 6>과 같다.

4.3.2 업종에 따른 조직구성원의 정보보안 의식 수준의 차이분석

업종에 따라서 조직구성원 즉, CEO, CIO, 직원들의 정보보안 의식에 차이가 있는가를 분석하기 위하여 분산분석을 이용하였다.

〈표 7〉 업종에 따른 조직구성원의 정보보안 의식 차이에 대한 분산분석 결과

		유일접근법				
		제곱합	자유도	평균 제곱	F	유의 확률
CEO의 정보보안 의식	주효과 업종	2.179	5	.436	.505	.771
	모 형	2.179	5	.436	.505	.771
	잔 차	39.675	46	.863		
	전 체	41.855	51	.821		
CIO의 정보보안 의식	주효과 업종	1.651	5	.330	.408	.841
	모 형	1.651	5	.330	.408	.841
	잔 차	37.245	46	.810		
	전 체	38.895	51	.763		
직원들의 정보보안 의식	주효과 업종	3.073	5	.615	.938	.466
	모 형	3.073	5	.615	.938	.466
	잔 차	30.147	46	.655		
	전 체	33.220	51	.651		

<표 7>의 분산분석 결과를 보면 그룹간 자유도는 5, 그룹내 자유도는 46이다. 평균제곱은 각각 제곱합을 각 원천별 자유도로 나눈 값이 되며, F통계량은 그룹간 평균제곱을 그룹내 평균제곱으로 나눈 값이다.

F 분포에서 F(5, 46, 0.05)의 임계치는 약 2.40

인데 각각의 F 통계량이 0.505(CEO의 정보보안 의식), 0.408(CIO의 정보보안 의식), 0.938(직원들의 정보보안 의식)로 임계치 2.40보다 모두 작으므로 6개의 요인 수준의 평균이 동일하다는 귀무가설을 채택한다. 이것을 F 분포의 확률로 설명하면, 각각의 F 유의도 P=0.771(>0.05), P=0.841(>0.05), P=0.466(>0.05)이므로 귀무가설을 채택한다.

따라서 조직구성원의 정보보안 의식은 업종에 의해서는 유의한 차이를 보이지 않는다고 할 수 있다.

4.3.3 업종에 따른 조직의 정보보안 수준의 차이 분석

업종에 따라서 조직의 정보보안 수준에 차이가 있는가를 분석하기 위하여 앞에서와 마찬가지로 분산분석을 이용하였다.

〈표 8〉 업종에 따른 조직의 정보보안 수준 차이에 대한 분산분석 결과

		유일접근법				
		제곱합	자유도	평균제곱	F	유의확률
물리적 정보보안	주효과 | 업종	.706	5	.141	.204	.959
	모 형	.706	5	.141	.204	.959
	잔 차	31.771	46	.691		
	전 체	32.477	51	.637		
기술적 정보보안	주효과 | 업종	.960	5	.192	.318	.900
	모 형	.960	5	.192	.318	.900
	잔 차	27.765	46	.604		
	전 체	28.725	51	.563		
관리적 정보보안	주효과 | 업종	.916	5	.183	.288	.918
	모 형	.916	5	.183	.288	.918
	잔 차	29.295	46	.637		
	전 체	30.211	51	.592		

<표 8>의 분산분석 결과를 보면 그룹간 자유도는 5, 그룹내 자유도는 46이다. F 분포에서 F(5, 46, 0.05)의 임계치는 약 2.40인데 각각의 F 통계량이 0.204(물리적 정보보안), 0.318(기술적 정보보안), 0.288(관리적 정보보안)로 임계치 2.40보다 모두 작으므로 6개의 요인 수준의 평균이 동일하다는 귀무가설을 채택한다. 이것을 F 분포의 확률로 설명하면, 각각의 F 유의도 P = 0.959(> 0.05), P = 0.900(> 0.05), P=0.918(> 0.05)이므로 귀무가설을 채택한다. 위에서와 마찬가지로 조직의 보안수준은 업종에 의해서는 유의한 차이를 보이지 않는다고 할 수 있다.

[가설 5]와 [가설 6]의 검정결과를 종합하여 <표 9>와 같이 요약할 수 있다.

〈표 9〉 업종에 따른 조직구성원의 정보보안 의식차이 및 조직의 정보보안 수준차이 검정결과

가설번호	가 설 내 용	검정결과
가설 5	**업종에 따라 조직구성원의 정보보안 의식 수준에 차이가 있다.**	
가설 5-1	업종에 따라 CEO의 정보보안 의식 수준에 차이가 있다.	기각
가설 5-2	업종에 따라 CIO의 정보보안 의식 수준에 차이가 있다.	기각
가설 5-3	업종에 따라 직원들의 정보보안 의식 수준에 차이가 있다.	기각
가설 6	**업종에 따라 조직의 정보보안 수준에 차이가 있다.**	
가설 6-1	업종에 따라 조직의 물리적 정보보안 수준에 차이가 있다.	기각
가설 6-2	업종에 따라 조직의 기술적 정보보안 수준에 차이가 있다.	기각
가설 6-3	업종에 따라 조직의 관리적 정보보안 수준에 차이가 있다.	기각

5. 결 론

최근 전자메일을 통한 바이러스로 전 세계의 기업이나 단체 사용자가 심각한 피해를 입었다는 보도가 연일 끊이지 않고 있다. 그러나 피해를 본 후에 인식되는 보안 효과의 특성 때문에 현재의 보안 대책이 적정 수준으로 잘 되어 있는지 판단하기 어렵다. 일단 피해를 보게되면 더 큰 피해를 막기 위해 취해지는 후속 조치 활동이 보안 문제해결의 중심이 되며, 사전 예방을 위한 인식이 높지 못한 실정이다. 더구나 조

직 구성원들의 정보보안에 대한 마인드가 점차 확산되고는 있으나 전문인력의 부족으로 아직까지 뚜렷한 해결책이 마련되지 못한 상태이다.

따라서 정보보안을 위해서는 우선 조직구성원의 의식 측면에서의 변화와 이에 대한 연구 및 투자가 선행되어야 한다. 이러한 관점에서 수행된 조직구성원의 의식측면에 대한 연구 결과를 요약하면 다음과 같다.

첫째, 조직구성원의 정보보안 의식에 있어 직속상급자의 영향이 가장 큰 것으로 나타났다. 즉, CIO는 CEO에게서, 직원들은 CEO보다는 CIO에게서 더 많은 영향을 받는다는 것이다.

이러한 결과는 업무 또는 생활 속에서 직접적으로 대면하는 직속 상급자의 정보보안에 대한 강조, 교육, 행동 등이 하급자의 의식 변화에 영향을 미치기 때문이라고 할 수 있다.

둘째, CEO의 정보보안 의식이 높으면 조직의 물리적 · 기술적 · 관리적 정보보안 모두의 수준이 높은 것으로 나타났다.

이것은 정보보안의 구성요소(즉, 물리적 · 기술적 · 관리적 정보보안)와 관련된 정책결정권이 CEO에게 있기 때문이라고 판단된다. 즉, 보안 기술 및 장비, 인력 등과 관련된 정책 및 투자 결정권이 최고경영자에게 있기 때문이다.

셋째, 조직구성원의 정보보안 의식 수준에 있어서 업종에 의한 차이는 없는 것으로 나타났다.

이러한 결과는 모든 업종에서의 업무시스템이 전산화됨으로서 정보시스템에 대한 의존도가 높아지게 되고, 그에 따라 정보보안 의식도 평준화되고 있다고 볼 수 있다. 결국 정보보안 의식의 차이는 조직 구성원 개개인의 개인적인 경험, 교육, 업무 등에 따라 차이를 보일 뿐이며, 업종의 특성은 큰 영향을 미치지 않는다고 볼 수 있다.

마지막으로 조직의 정보보안 수준도 업종에 의한 차이를 보이지 않는 것으로 나타났다.

이것은 대부분의 조직에서 정보보안과 관련된 장비, 기술, 관리기법 등에 있어 자체개발보다는 외부 전문업체로부터 도입하거나 아웃소싱하기 때문에 업종 특성은 많은 영향을 미치지 못한다고 판단할 수 있다. 결국 조직의 정보보안 수준은 조직구성원의 정보보안 의식 수준과 투자 정도에 따라 차이가 발생한다고 볼 수 있다.

본 연구의 가장 큰 의의는, 첫째 기존 연구들의 대부분은 물리적, 기술적, 관리적 정보보안 측면에서 접근하여 실질적으로 정보보안을 계획하고 실행하는 인적 측면을 배제하였으나, 본 연구에서는 조직의 정보보안 구성요소를 조직구성원의 의식 요소를 추가하여 연구함으로서 향후 정보보안 연구의 또 다른 방향의 토대를 마련하였다는데 의의를 둘 수 있다.

둘째, 본 연구에서의 조사서는 기존 연구들의 설문서 조사 대상이 단일 또는 다수 조직내의 개인들에 국한된 반면 기업(조직)단위로 확대하여 단일조직에 1부씩으로 제한하여 조사하였다는 것이다. 특히 정보보안에 대한 데이터는 보안이라는 이유로 외부로의 유출을 꺼려하는 실정에서 많은 조직의 데이터를 수집했다는데 의의가 있다고 하겠다.

반면, 본 연구는 조직의 정보보안 수준을 측정하기 위한 평가항목을 만드는 과정에서 현업에 종사하는 전문가들과 인터뷰를 하는 과정에서 의식측면이 중요하다는 아이디어를 얻어 시작되었다. 그러나 앞에서도 말하였듯이 자료의 수집이 어려워 통계분석에 충분한 데이터를 수집하지 못하였다. 그러므로 해서 본 연구결과의 해석에 있어 신중하여야 하겠다.

이러한 맥락에서 본 연구의 한계 및 문제점을 요약하면 다음과 같다.

첫째, 통계분석에 필요한 충분한 자료 확보가 되지 않아 결과분석에 있어 신중한 해석이 요구된다.

둘째, 조사된 기업들이 중견기업 이상의 큰 조직을 대상으로 조사되었으므로 국내 전체 조직을 대표하지 못한다.

마지막으로, 정보보안 의식 및 정보보안 수준 측정을 위한 선행연구의 부족으로 연구 내용의 한계가 있다.

향후 연구방향으로는 이러한 연구의 한계를 극복하는 것은 물론 다음과 같은 내용이 보완되어 연구되어야 할 것이다.

첫째, 정보보안 의식 측면에 관한 보다 깊은 연구가 필요하다. 기존의 연구에는 기술적인 측면이나 부분적인 측면의 연구가 주류를 이루고 있는 실정으로 가장 중요한 조직 구성원들의 의식을 배제하는 결과를 초래하였다.

둘째, 정보보안 수준 평가에 있어 가중치를 적용하는 방안이 심도 있게 연구되어야 할 것이다. 이것은 정보보안 수준 측정을 위한 요소들에 따라 중요도가 다르다. 따라서 중요도에 따른 가중치 개발을 위한 연구가 필요하다.

마지막으로, 정보보안 성과에 대한 지속적인 연구가 필요하다. 정보보안 정책의 판정은 사고가 발생한 후에 평가된다. 따라서 대부분 적정 수준을 유지하는 수준에서 투자를 하고 사고가 발생하지 않기를 기대하는 것이 대부분이다. 그러나 한 번의 보안 사고는 조직의 치명적인 영향을 미칠 수 있다. 따라서 사전에 정보보안의 성과를 측정할 수 있는 방법에 관한 연구가 필요하다.

참 고 문 헌

[1] 강병서, 김계수, *통계분석을 위한 SPSSWIN Easy*, 법문사, 1998.

[2] 강병서, *인과분석을 위한 연구방법론*, 무역경영사, 1999.

[3] 김영걸, 이종만, 이재남, "정보시스템의 위험도 분석에 관한 연구 : 통합적인 분석 틀을 중심으로", *경영정보학연구*, 제8권 제2호, 1998. pp.105-118.

[4] 김인수, 거시조직이론 : 조직설계의 이론과 실제, 무역경영사, 1996.

[5] 김정덕, 김기윤, 정보보호지표 항목개발 및 계량화 연구, 정보보호센터, 1998. 12.

[6] 김현수, 정보시스템 진단과 감리, 법영사, 1999.

[7] 김현수, 정해철, "정보보안 지표 개발에 관한 탐색적 연구", *한국데이터베이스 학회 국제컨퍼런스*, 1999. 10., pp.119-127.

[8] 박태완, 정보시스템 보안감리, *정보시스템 감리*, 한국전산원 교육교재, 1997. 10, pp. 815-837.

[9] 이재범, 안상협, "정보담당 최고임원(CIO)의 경영자 역할이 사용자에 미치는 직접적 영향에 관한 연구", 경영정보학 연구, 제7권 제3호, 1997, p.127.

[10] 이형원, 정보시스템 안전대책, 영진출판사, 1993.

[11] 한국정보보호센터, 전자상거래 피해사례 분석, 1999. 2.

[12] 한국정보보호센터, 정보보호 총서, 1996, p.5.

[13] Cash, J.I., F.W. McFarlan, and J.L. McKenney, Corporate Information Systems Management-The Issues Facing Senior Executive, 3rd ed., Business One Irwin, Homewood, Illinois, 1992.

[14] Doll, W.J., "Avenues for Top Management Involvement in Successful MIS Development," *MIS Quqrterly*, Vol.9, No1, 1985, pp.16-35.

[15] Grover, V., S.R. Jeong, W.J. Kettinger and C.C. Lee, "The Chief Information Officer : A Study of Managerial Roles," *Journal of Management Information Systems*, Vol.10, No.2, 1993, pp.107-130.

[16] Ives, B. and M.H. Olson, "Manager or Technician? The Nature of the Information Systems Manager's Job," *MIS Quarterly*, Vol.5, No.4, 1981, pp49-62.

[17] Karimi, J., "Strategic Planning for IS : Requirements & Information Engineering Method," *Journal of MIS*, Vol.4, No.4, 1988, pp.5-24.

[18] Straub, D.W., and R.J. Welke, "Coping With Systems Risk : Security Planning Models for Management Decision Making," *MIS Quarterly*, December 1998, pp. 441-468.

[19] Von Solms, R., J.H.P. Eloff, and S.H. Von Solms, "Computer security management : a framework for effective management involvement," *Information Age*, Vol.12, No. 4, Oct. 1990, pp217-222.

[20] Ware, W.H., *Perspectives on Trusted Computer Systems*, RAND Corporation, September, 1988.

[21] Wilkes, M.V., "Revisiting Computer Security in the Business World," *Communications of the ACM*, Vol.34, No.8, August 1991.

[22] Willoughby, T.C., and A. Pye, "Top Management's Computer Role," *Journal of Systems Management*, Sep. 1977, pp.10-13.

[23] Zmud, R.W., and J.F. Cox, "The Implementation Process : A Change Approach," *MIS Quqrterly*, Vol.3, No.2, 1979, pp.35-43.

[24] 한국전산원(http://www.nca.or.kr)

[25] 한국정보보호센터(http://www.kisa.or.kr)

[26] Computer Professionals for Social Responsibility(http://www.cpsr.org)

[27] Firewalls.R.Us(http://www.frus.com)

[28] RSA Data Security(http://www.rsa.com)

[29] SAIC Security Web Site(http://mis.saic.com)

저자소개

정 해 철

국민대학교 정보관리학과를 졸업하고, 동 대학원에서 정보시스템 전공으로 경영학석사를 취득하였다. 현재 국토연구원 GIS 연구센터에서 연구원으로 재직하고 있으며, 주요관심분야는 정보시스템 감리 및 GIS 분야이다.

김 현 수

서울대학교 원자핵공학과를 졸업하고, 한국과학기술원에서 경영과학으로 석사, 그리고 University of Florida에서 경영정보학으로 박사학위를 취득하였으며 (주) 데이콤 등에서 정보시스템 관련 업무를 담당하였다. 현재 국민대학교 경상대학 정보관리학부 부교수로 재직하고 있으며 관심분야는 경영정보학 분야이다.