정보보안 거버넌스의 구성요소가 종업원의 보안 인식과 행위에 미치는 영향에 관한 연구

A Study on the Influence of the Components Related to Information Security Governance on the Perception and Behavior of Employees

김영곤*

Young-Gon Kim*

요 약

본 연구는 정보보안 거버넌스(Information Security Governance)의 구성 요소인 리더십과 거버넌스, 보안 관리 조직, 보안 정책, 보안 프로그램 관리, 사용자 보안 관리, 기술적 보안과 조직 구성원의 보안 인식과 보안 행위 간의 관계를 가설 검증과 최적 모델 분석을 통해 요소간의 관계를 검증하였으며, ISG 확립을 위한 효과적인 방향을 제시하였다.

Abstract

The purpose of this study is to try to find out the relationship between the perception and behavior of employees and the Information Security Governance (ISG) which consists of leadership and governance, security management and organization, security policies, security program management, user security management, and technology protection and operations. Some effective suggestions from the verification of research hypotheses and the analysis of the most appropriate model were drawn out.

Key Words : IT Governance, Information Security Governance, Information Security Culture

I. 서 론

글로벌화와 지식 정보화를 지향하는 21세기에 사회 모든 분야에서 정보시스템과 인터넷의 활용과 비중이 증대됨에 따른 역기능으로 발생하는 정보 보안 사고는 심각한 사회적 문제로 대두되고 있다. 일반 문서와는 달리 전산 처리된 자료는 관리적인 통제나 물리적 통제만으로 보안 관리가 어렵다. 더구나 인터넷의 보편화로 네트워크를 통한 조직 내부 또는 외부로부터의 불법 침투가 보다 용이해져 정보보안(information security)의 중요성은 날로 부각되고 있는 실정이다.

정보보안은 조직의 IT 환경, 즉 정보시스템 및 통신망 등 기본 인프라에 대한 보안에 중점을 둔 기술적 측면의 조치로 시작한다. 조직은 이러한 기본 인프라에 대한 보안을 진행하면서 대부분 정보보안에

* 경남대학교 e-비즈니스학부(Department of E-Business, Kyungnam University)
· 제1저자 (First Author) : 김영곤
· 투고일자 : 2010년 11월 10일
· 심사(수정)일자 : 2010년 11월 10일 (수정일자 : 2010년 11월 26일)
· 게재일자 : 2010년 12월 30일

관리자의 역할 특히 최고경영자의 관여가 매우 중요하다는 것을 인식하게 되고, 이와 관련된 측면을 병행하여 추진하게 된다. 이것이 현재 대부분의 현실기업이 적용하고 있는 보안 수준이라 할 수 있다.

하지만 정보보안의 가장 큰 위협요소는 바로 인간적 요소이며, 이에 대한 관심을 증가시켜야 한다. 위협은 조직 외부와 내부 모두에서 발생할 수 있다. 일반적으로 외부보안의 문제가 어느 정도 해결되면, 내부보안의 문제를 중요하게 인식해야 한다. 즉 종업원이 일상 업무를 수행함에 있어 정보보안의 특징을 구체적으로 인식하고 수용하는 태도를 견지하는 정도를 말하는 정보보안 문화(IS culture)는 성숙된 정보보안 수준의 유지를 위해 특히 관심을 가져야 하는 것이다.

결국 정보보안을 충분하고도 안전하게 수행하기 위해서는 다양한 측면을 고려해야 하는 데, 여기에는 정보보안 관련 기술, 관련 업무 처리과정, 이해관계인에 대한 측면을 모두 고려한 정보보안 거버넌스(IS governance)의 모든 요소를 적용함으로써 가능하다고 본다. Cobit Security Baseline에 의하면, 경영진은 올바른 정보보안 문화와 통제 체제에 대한 책임이 있을 뿐 아니라, 정보보안에 대한 바람직한 태도를 가져야 한다고 언급하고 있다. 즉 정보보안 거버넌스의 개발과 역할에 대한 인식과 적용이 필요하다고 할 수 있을 것이다[5].

정보보안 거버넌스는 보안 위협을 완화시키기 위해 전개되는 정보보안과 관련된 제반 방법이 포함되는 다소 광범위한 개념이다. PriceWaterhouse Coopers의 보안침해 사례조사에 따르면, 정보 시스템 또는 데이터에 대한 기술관련 보안 침해 사고 건수도 높지만, 근본적인 원인을 찾아보면 기술 결함보다는 인간적 실수(error)로 인한 것이 더 많다고 한다[30]. 결국 훌륭한 정보보안 수준을 유지하기 위해서는 정보보안과 관련된 제반 위험을 감안한 정보보안 거버넌스가 중요하며, 기술적, 절차적, 인간행위적 요소의 3가지 측면을 모두 고려한 접근 방법을 견지할 필요가 있다고 할 수 있다.

지금까지 정보보안과 관련해 주로 연구 조사된 부문은 정보보안 지침과 절차에 대한 표준, 위험 관리, 정보보안 시스템(방화벽, 침입탐지, 침입방지, 서버 보안, 웹 보안, 데이터베이스 보안 등)과 관련한 기술적 문제에 중점적으로 이루어졌으며, 내부보안을 비롯한 조직 구성원의 정보보안 측면의 역할과 기능에 대한 중요성은 상대적으로 덜 강조된 것이 사실이다. 즉 정보보안 거버넌스 프레임워크에 관한 기본적인 연구는 다소 찾아 볼 수 있으나, 특히 정보보안 거버넌스의 수행을 위한 조직 구성원의 인간적 요인에 대한 구체적인 연구 사례는 찾아 볼 수가 없었다.

따라서 본 연구는 정보보안 거버넌스의 프레임워크를 구성하는 요소를 파악하고, 이러한 요소들이 조직 구성원들의 보안 인식과 보안 관련 행위에 어떠한 영향을 미치는 가를 연구함으로써 정보보안 거버넌스를 확립함에 있어 필요한 효과적인 접근 방법을 제시하고, 조직의 자원을 효율적으로 배분하기 위한 방안을 제시하며, 건전하고, 바람직하며 강한 정보보안 문화를 조성하기 위한 전략을 모색하는 데 도움을 줄 수 있는 방향을 제시하는 데 목적을 두고 수행하였다.

Ⅱ. 이론적 배경

2-1 기업 거버넌스와 IT 거버넌스

거버넌스(governance)의 사전적 의미는 '권력을 통한 통치 또는 지배, 대상 분야에 대한 영향력 행사, 가이드 또는 통제'이다. 그리고 기업 거버넌스는 흔히 기업의 통치, 기업의 운영, 기업의 지배구조로 해석되며, 이것은 보고 체계, 권한, 소유권(ownership), 관리 감독(oversight), 정책 시행(policy enforcement)과 같은 조직 통제를 말한다[11][20]. 이러한 기업 거버넌스는 조직이 기술자원을 어떻게 사용하고 통제하며, 어떻게 정보를 보호해야 하는 지를 정의하고 있는 정책이나 절차에 관한 IT 거버넌스와 관계가 있다[29].

IT 거버넌스에 대한 개념도 다양하다. IT 거버넌스는 핵심 IT업무와 관련한 의사결정 권한을 규정한다[22][35]. IT 거버넌스 협회는 IT 거버넌스가 이사회와 경영진의 책임이며, 기업 거버넌스의 통합적 부분으로, 조직의 전략과 목표 달성을 뒷받침하는 조직

구조와 프로세스, 그리고 리더십으로 구성된다고 하였다[17]. Van Grembergen는 IT 거버넌스는 IT 전략의 개발 및 추진을 관리하고 이를 통해 비즈니스와 IT를 융합시키기 위해 이사회, 경영진, IT 관리가가 추진하는 조직 기능이라고 하였다[39]. IT 거버넌스는 IT관리보다 넓은 의미로 사용되며 고객과 기업의 현재 및 미래 수요를 충족시키기 위해 IT를 운영하고 발전시키는 데 중점을 둔다[27]. 또한 IT 거버넌스는 전체 기업 거버넌스에 통합되어야 한다[12][14][27].

2-2 정보보안 거버넌스

정보보안 거버넌스는 정보보안의 패러다임의 변화와 관련이 있다. 2000년대 초반 이후부터 정보보안의 패러다임은 기술중심에서 조직과 거버넌스 중심으로 옮겨가고 있다. 사실 정보보안 패러다임은 1950년대 정보보안 기술 패러다임에서 1980년대 1990년대 중반까지는 정보보안 관리 패러다임으로, 1990년대 후반부터 2000년대 초반까지는 정보보안 조직화 패러다임으로, 2000년대 초반이후 현재까지는 정보보안 거버넌스 패러다임으로 바뀌고 있는 실정이다[1]. 이러한 패러다임의 변화는 정보보안이 경영에 의미있는 역할을 하고, 최고경영진이 여기에 동참함으로써 관리의 중요성이 높아진 것이다[43]. 특히 정보보안의 가장 큰 위협으로 인간적 요소가 언급되면서 조직내 정보보안 문화에 대한 관심도 증대되었다[7][[43]. 정보보안의 조직화란 구성원의 일상적인 업무의 하나로 정보보안이 차지하게 되는 단계를 말하며 이러한 과정을 통해 정보보안 문화가 조성되게 된다. 정보보안 문화란 구성원이 조직의 각종 업무를 수행할 때, 정보보안의 특징이 포함되도록 권장되고, 구성원이 이에 대한 인식과 수용하는 태도를 견지하는 것을 말한다[24].

Cobit 2004 보안 기준에 따르면 경영진은 올바른 정보보안 문화와 통제를 조성하고, 수용가능한 태도를 보여 주여야 하는 책임이 있다고 한다. 이 단계가 정보보안 거버넌스 패러다임의 개발과 역할이 중시되는 단계에 해당한다[44]..

정보보안 거버넌스는 IT 거버넌스 중 위기관리의 일부분이라 할 수 있고, 이것은 정보보안이 위험을 완화시키도록 전개되는 제반 방식을 말한다[6]. 또한 Weill & Vitale은 정보보안 거버넌스를 정보보안에 대한 의사결정 권한을 공유하고 정보보안에 대한 투자 성과를 모니터하기 위한 회사의 전반적인 프로세스를 의미한다고 한다[46]. Van Grembergen은 정보보안 전략의 개발 및 추진을 관리하고 이를 통해 비즈니스와 정보 보안을 융합시키기 위해 이사회, 경영진, IT 관리자, 정보보안 관리자가 추진하는 조직 기능으로 말하고 있다[39]. 현재까지의 다양한 정의를 정리해 보면 정보보안 거버넌스는 이사회와 경영진의 책임하에 수행되는 기업 거버넌스의 일부로서 정보보안에 대한 투자 성과를 기반으로 의사 결정에 대한 권한과 책임을 정의하고, 정보보안 활동이 조직의 전략과 목표를 유지하고 향상시킬 수 있게 하는 조직구조, 프로세스, 기술을 말한다고 할 수 있다.

2-3 정보보안 거버넌스 프레임워크

정보보안 거버넌스의 프레임워크 또는 구성요소에 대한 연구는 현재 진행 중이나, IT 거버넌스 협회에서는 IT 거버넌스의 구성 요소를 비즈니스 전략에 대한 정보보안의 전략적 연계(strategic alignment), 수용가능한 수준으로 정보자산의 잠재적 영향을 줄이고, 위험을 관리하기 위해 적절한 평가를 수행하는 위험관리(risk management), 정보보안 지식과 인프라를 효율적이고 효과적으로 운영하기 위한 자원 관리(resource management), 조직 목표 달성을 보증하기 위해 정보보안 거버넌스 척도를 기준으로 모니터링, 보고 및 평가를 수행하는 성과관리(performance manage- ment), 조직, 목표를 지원하는 정보보안 투자를 최적화하는 가치 전달(value delivery)의 다섯 가지로 들고 있다[18].

Posthumus & Solms는 정보보안 거버넌스 프레임워크를 조직의 비전, 전략, 임무에 도움을 줄 수 있고, 법적 규제를 반영한 정보보안 정책의 수립으로 구성원에게 명령과 지시를 하는 거버넌스 측면과 이러한 표준, 지침, 요구 절차가 IT 인프라를 통해 제대로 실행되는지를 통제하는 관리측면으로 나누었다. 정보보안 거버넌스에 대한 프레임워크에는 구성원의 행

위를 지시하기 위해 사용되는 구체적인 통제가 포함되며, 정보보안 문화를 조성하기 위한 구성원의 행위에 대한 조항이 포함된다. 정보보인 거버넌스 프레임워크에는 기술적, 절차적, 인간 행위적 요소를 모두 고려해야 함을 강조하고 있다[28].

Eloff는 정보보안 거버넌스의 주요 구성 요소로 리더쉽과 거버넌스, 보안 관리를 위한 조직, 보안 정책, 보안 프로그램 관리, 사용자 보안 관리, 기술적 보안 요소의 여섯 가지 요인으로 분류하였다[7].

리더십과 거버넌스는 정보자산을 보호하기 위해 이사회 또는 경영진 수준에서 정보보호에 대한 지원을 말하며, 이것은 IT 거버넌스와 기업 거버넌스(corporate governance)의 수준을 결정하는데 꼭 필요한 부분으로 받아들여지고 있다는 사실에 근거한다[44]. 리더십과 거버넌스는 위험 평가(risk assessment)와 정보보안 전략의 수립과 관련이 있으며, 이러한 정보보안 전략은 장단기에 걸쳐 조직의 목적이 달성되도록 조직 및 IT 전략과 연계되어야 한다. 그리고 정보보안의 위협을 방어하기에 얼마나 효과적인가를 측정할 수 있는 측정지표 또는 방법도 포함된다. 많은 조직들이 자신의 정보보안 프로그램에 대한 전반적인 효과성과 이 프로그램이 조직의 전략 달성에 기여하고 있는지를 평가하기 위해 보안사고의 수, 보안 인지 조사라는 측정지표를 사용하고 있다[47].

보안 관리 및 조직은 정보보안에 대한 조직 설계, 구성, 보고 체계를 포함한다. 정보보안 관리체계를 중앙집중형으로 할 것인지, 분산형으로 할 것인지 하는 조직 구성과 체계를 말한다. 여기에는 기업 수준의 정보보안을 위해 해당 조직이 수행해야 할 역할과 책임, 기술과 경험, 자원 수준에 대한 내용도 포함된다[26].

ISO/IEC 17799에는 보안 정책이란 경영자가 공식적으로 표현하는 정보보안에 대한 전반적인 의도(intention)와 지시사항(direction)을 말한다고 정의하고 있다[16]. 보안정책은 관련 법을 감안하여야 하며, 효과적인 방법으로 제대로 실행되어져야 하며, 이를 지속적으로 모니터링하여야 한다. 그리고 절차는 정책을 수행하기 위해 취해야 할 제반 단계를 말한다[45]. 이러한 절차는 암호 표준 또는 지침(guideline)과 같은 표준에 의해 뒷받침된다. 그리고 정보보안 지침에는 표준 업무 처리 절차(best practice)의 적용이 권장된다.

보안 프로그램 관리에는 보안 감사와 정보보안 프로그램의 적법한 운영과 모니터링을 말하며, 정보보안 프로그램의 적법한 운영과 측정은 필수적인 요소이며, 기술적 요소와 구성원의 행위는 보안 정책을 준수하는지, 보안 사고 발생 처리에 대한 효과적이고 적절한 대응하는지를 확인할 수 있어야 한다. 구성원의 행위에 대한 감시에는 불법 소프트웨어의 설치, 강한 패스워드의 사용, 방문하는 인터넷 사이트에 대한 것이 포함된다. 정보보안 감사는 보안 정책, 절차, 처리 방법들이 조직의 목적, 목표, 비전과 부합되는지 판단하기 위해 필요하다[45].

사용자 보안관리에는 사용자의 정보보호에 대한 인지(user awareness), 사용자 교육 훈련, 윤리 강령, 신뢰 확보, 개인정보보호가 포함된다. ISO/IEC 17799에서는 조직은 조직 구성원을 정보보안에 대해 인지시키고, 관련 교육을 효과적으로 시행하기 위한 계획과 프로그램을 가지고 있어야 한다고 하였다[16]. OECD의 정보시스템 및 네트워크 보안에 대한 가이드라인에 의하면 보안 문화를 조성하는 원칙중의 하나가 바라 윤리 강령이라고 하고 있다[3]. 윤리란 옳고 그름을 구분하는 가치 및 규칙이며, 이러한 윤리 행동 강령에 대한 마련은 경영자의 책임이다[15]. 정보보안 거버넌스에서 경영진은 구성원이 정보보안 정책을 준수할 것으로 믿을 수 있어야 한다. 한편 구성원은 경영진이 정보보안에 대한 실천 의지를 보여줄 것으로 믿는다[32]. 신뢰 관계는 외부 조직이나 고객과의 관계에서도 성립될 수 있다. 이러한 신뢰관계는 정보와 정보 자산이 안전하고, 구성원들이 정보보안 요구사항을 준수한다는 입증을 보여줌으로써 형성될 수 있다. 개인정보보호는 고객과의 관계에서 매우 중요한 요소이다[37]. 개인정보에 대한 보호를 하지 않는다면 신뢰를 형성될 수 없다[33]. 개인정보보호는 구성원과 고객 모두를 고려해야 하며 ID와 비밀번호에 대한 보호가 되어야 한다.

기술 보호와 운영은 정보보안 자산관리, 시스템 개발 요구사항, 사고 관리, 네트워크 보안과 같은 기술적 운영, 물리적 환경, 그리고 사업 연속성 통제를 포함한다. 자산관리는 자산의 재고관리, 정보 분류,

라벨 작업에 초점을 두며, 정보보안 시스템 개발과 도입은 정보시스템의 획득, 개발, 유지보수와 관련 것으로 사용자 개발 또는 정보보안 관련 패키지 프로그램의 안전성을 보장하는 것과 관련이 있다. 정보보안 사고 관리는 보안사고가 적시에 보고되고, 정확한 조치가 취해지는 것을 보장하는 것이며, 물리적 환경에 대한 접근통제는 인가받은 사람만이 정보보안 시설 및 장소에 접근하도록 허용하는 보안 통제를 말한다. 그리고 사업 연속성(business continuity)은 사업 연속성 계획 수립과 그것의 시험에 초점을 둔다.

2-4 구성원의 보안 인식과 행위

정보보안에 대한 구성원의 보안 인식과 행위의 수준은 정보보안 기술과 활용에 대한 인식과 행위로 판단할 수 있을 것이다. 전통적인 정보시스템 분야에서 매우 중요한 이론으로 간주되고 있는 Davis의 기술수용모형(technology acceptance model: TAM)에 의하면 개인이 자발적으로 새로운 정보기술을 수용함에 있어 개인의 태도 및 이용 의도에 가장 주요한 영향력을 미치는 요인으로 자신이 하고자 하는 일에 해당 정보기술이 얼마나 도움을 줄 것인가와 사용하기 쉬운 정도 즉, 지각된 유용성(perceived usefulness)과 지각된 사용 용이성(perceived ease of use)에 대한 판단에 의해 결정되는 것으로 알려져 있다[8]. 지각된 유용성은 사용자가 특정한 시스템을 사용함으로써 자신의 업무 성과를 향상시킬 것이라고 믿는 정도를 의미하며, 업무 성과의 개선, 업무의 질 향상, 업무 속도의 개선, 생산성 향상, 효과성 향상, 업무의 용이함 등으로 구체화 된다. 지각된 사용 용이성은 새로운 기술을 이용함에 있어 많은 노력과 시간을 할애하지 않아도 쉽게 이용할 수 있다는 개인의 기대 정도를 의미하며, 사용하기 쉬움, 배우기 쉬움, 이해하기 쉬움, 원하는 것을 얻기 쉬움, 숙달이 용이함 등으로 구체화된다.

이러한 기술모형은 다양한 방식으로 확장이 이루어졌고, 여러 유형의 정보기술 사용에서 타당성을 인정받고 있다[41]. 하지만 사용에 대한 태도나 의도의 예측에서는 매우 의미있는 설명을 보이고 있지만 실제 정보기술 사용까지 설명할 수 있는 것은 아니다. 즉 정보보안에 대한 필요성에 대해서 인식을 한다고 하여 그것이 실제 관련 행동으로 이어진다고 볼 수 없다는 것이며, 이러한 행동에 영향을 미치는 것으로는 제공하는 기능이나 자원을 충분히 통제할 수 있는 정도인 지각된 통제가능성(perceived controllability)에 따라 달라질 수 있다[4][25][36][42].

합리적 행동이론(theory of reasoned action: TRA)에 의하면 인간이 어떤 행동을 하기까지는 일련의 심리적 과정을 거치게 된다. 자신의 행동에 대한 여러 가지 행위적 믿음을 통해 행위에 대한 태도를 형성하고, 다른 사람들이 가지고 있으리라고 생각하는 규범적 믿음들에 의해 주관적 규범을 형성하나. 이와 같이 형성된 행위에 대한 태도와 주관적 규범은 그 행동을 하고 싶은 정도 즉, 행위에 대한 의도(intention)를 결정하고 의도는 직접적인 행동을 결정한다[13].

동기이론은 개인의 특정 행위를 설명하기 위한 조직이론으로, 개인의 정보기술 수용 행위를 설명하는데 이용되고 있다[10][21][34]. 이 이론에 의하면 개인의 행위는 일반적으로 즐거움, 재미, 만족감, 성취감 등과 같은 내재적 동기요인과 봉급의 인상, 승진 등과 같은 외재적 동기요인에 의해 유발된다[2][9][40].

본 연구에서는 구성원의 보안 인식을 정보보안이 얼마나 도움을 줄 것인가에 대한 지각된 유용성으로 판단하고, 구성원의 보안 행위는 정보보안과 관련된 실제 관련 행동에 영향을 미치는 지각된 통제가능성으로 그 정도를 판단하였다.

Ⅲ. 연구 모형

3-1 연구모형의 설계

본 연구에서는 정보보안 거버넌스에 영향을 미치는 주요 요인을 식별하기 위한 기본 틀로 Eloff(2007)의 연구를 참고하였으며, 정보보안에 대한 구성원의 보안 인식과 행위에 대한 요인은 정보시스템 분야에서 매우 중요한 이론으로 간주되고 있는 기술수용모형(TAM)을 참고하였다.

정보보안 거버넌스의 구성요소는 선행연구를 참고하여 리더쉽과 거버넌스, 보안 관리와 조직, 보안

정책, 보안 프로그램 관리, 사용자 보안 관리, 기술적 보안 요소의 6개의 독립변수요인으로 정하고, 이들 요인들이 구성원의 보안 인식과 구성원의 보안 행위에 어떠한 영향을 미치는지, 또한 구성원의 보안 인식이 구성원의 보안 행위에 어느 정도 영향을 미치는지를 연구하려 한다. 따라서 본 연구의 연구 모형은 아래 그림 1과 같이 제시하고자 한다.

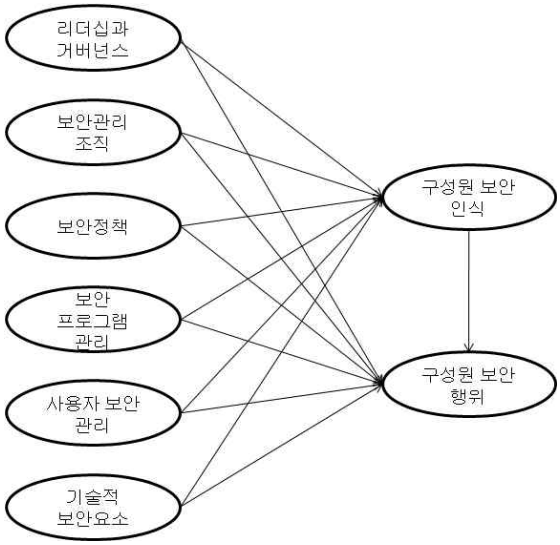

그림 1. 연구 모형
Fig. 1. Conceptual Framework

3-2 연구 가설의 설계

본 연구에서는 제2장에서 열거한 선행연구에 의거하여, 정보보안 거버넌스를 구성하는 요인을 독립변수로 정하고, 이러한 요인들이 구성원의 보안 인식과 구성원의 보안 행위에 영향으로 이어진다고 보아 다음과 같은 가설을 설정하였다.

첫째, 정보보안 거버넌스의 구성 요인인 리더쉽과 거버넌스, 보안 관리 조직, 보안 정책, 보안 프로그램 관리, 사용자 보안 관리, 기술적 보안 요소는 개별적인 수준이 양호하거나 관련 활동이 활발할수록 구성원의 보안 인식 수준에 정(+)의 영향을 미칠 것이라는 연구 가설을 설정하였다.

가설 Ⅰ. 정보보안 거버넌스 구성요인과 구성원의 보안 인식과의 관계

Ⅰ-1. 리더십과 거버넌스가 우수할수록 구성원의 보안 인식 수준이 높을 것이다.

Ⅰ-2. 보안관리조직의 수준이 높을수록 구성원의 보안 인식 수준이 높을 것이다.

Ⅰ-3. 보안정책이나 지침이 명확할수록 구성원의 보안 인식 수준이 높을 것이다.

Ⅰ-4. 보안프로그램의 관리 수준이 높을수록 구성원의 보안 인식 수준이 높을 것이다.

Ⅰ-5. 사용자보안관리 수준이 높을수록 구성원의 보안 인식 수준이 높을 것이다.

Ⅰ-6. 보안 관련 기술적 요소가 우수할수록 구성원의 보안 인식 수준이 높을 것이다.

둘째, 정보보안 거버넌스의 구성 요인인 리더쉽과 거버넌스, 보안 관리 조직, 보안 정책, 보안 프로그램 관리, 사용자 보안 관리, 기술적 보안 요소는 개별적인 수준이 양호하거나 관련 활동이 활발할수록 구성원의 보안 행위 수준에 정(+)의 영향을 미칠 것이라는 연구 가설을 설정하였다.

가설 Ⅱ. 정보보안 거버넌스 구성요인과 구성원의 보안 행위와의 관계

Ⅱ-1. 리더십과 거버넌스가 우수할수록 구성원의 보안 행위가 활발할 것이다.

Ⅱ-2. 보안 관리 조직의 수준이 높을수록 구성원의 보안 행위가 활발할 것이다.

Ⅱ-3. 보안 정책이나 지침이 명확할수록 구성원의 보안 행위가 활발할 것이다.

Ⅱ-4. 보안 프로그램의 관리 수준이 높을수록 구성원의 보안 행위가 활발할 것이다.

Ⅱ-5. 사용자 보안 관리 수준이 높을수록 구성원의 보안 행위가 활발할 것이다.

Ⅱ-6. 보안 관련 기술적 요소가 우수할수록 구성원의 보안 행위가 활발할 것이다.

셋째, 구성원의 보안 인식 수준이 높을수록 구성원의 보안 행위도 활동적으로(+) 나타날 것이라는 연구 가설도 설정하였다.

가설 Ⅲ. 구성원의 보안 인식과 구성원의 보안 행위와의 관계

Ⅲ-1. 구성원의 보안 인식 수준이 높을수록 구성원의 보안 행위가 활발할 것이다.

3-3 변수의 조작적 정의

본 연구의 정보보안 거버넌스와 구성원의 보안에 대한 인식과 행위에 대한 문항의 구성은 선행연구를 종합적으로 참조하여 결정하였으며, 정보보안 거버넌스의 구성 요소를 리더쉽과 거버넌스, 보안 관리와 조직, 보안 정책, 보안 프로그램 관리, 사용자 보안 관리, 기술적 보안 요소의 6개 요인으로 정하였다. 이러한 정보보안 거버넌스 구성 요인이 구성원에게 미치는 요인으로는 기술수용모형(TAM)을 활용하여 구성원의 보안 인식과 행위의 2가지 요인으로 하였다.

리더십과 거버넌스를 측정하기 위한 요소로는 선행연구를 종합하여 정보보안에 대한 경영진의 지원과 의지 정도, 정보보안 전략의 수립 여부, IT 거버넌스의 적용 여부, 위험 완화 전략과 통제 여부, 정보보안 프로그램의 효과 측정 정도 등 5가지 항목으로 측정하였다.

정보보안 프로그램 조직(program organization)은 정보보안에 대한 조직 설계, 구성, 보고 체계를 말한다. 보안 관리 및 보안 조직을 측정하기 위한 요소로는 정보보안 관리 조직의 구성 여부, 역할과 책임의 명기, 해당 조직의 기술과 경험의 수준, 보안 조직과 관련하여 관련 법에 명기된 사항의 준수 여부 등 4가지 항목으로 측정하였다.

정보보안에 대한 실천에 반드시 필요한 정보보안 정책, 절차, 표준, 가이드라인 등은 정보보안에 관해 구성원에게 요구되는 사항이 명시되어 있고, 구성원의 행위에 대한 가이드라인이 기술되어 있다[31]. 보안 정책 및 관련 사항을 측정하기 위한 요소로는 정보보안 정책 수립 정도, 정보보안 표준이나 절차의 존재, 정보보안 실무 지침의 작성과 활용의 3가지 항목으로 측정하였다.

보안 프로그램 관리에는 보안 감사 뿐만 아니라 정보보안 프로그램의 적법한 운영과 모니터링이 포함된다. 보안 프로그램 관리를 위한 측정 항목으로 위험관리를 고려하여 보안 프로그램을 작성 운영하고 있는지 여부, 보안 프로그램의 운영에 있어 관련 법을 적절하게 준수하는 지 여부, 구성원의 보안 행위를 보안 정책과 연계하여 기술하고 있으며, 이를 적절하게 감시하고 있는지 여부, 보안 사고 발생의 처리에 대한 효과적인 대응 정도의 4가지 항목으로 측정하였다.

사용자 보안 관리를 측정하기 위한 요소로는 사용자의 정보보호에 대한 의식(user awareness) 수준, 사용자 교육 훈련 프로그램의 존재 및 활용 정도, 윤리 강령 (ethical conduct), 신뢰 확보(trust), 개인정보보호(privacy) 등 5가지 항목으로 측정하였다. 정보보안 거버넌스에서 말하는 윤리 강령이란 개인정보 보호, 고객 정보의 불법 유출, 자료의 불법 변경 등과 같은 위험을 최소화하기 위한 것이다. 이러한 규칙은 구성원에게 보안 인지 프로그램의 일부분으로 교육되어야 한다. 신뢰 (trust)란 신뢰자가 신뢰를 받는 사람이 신뢰자의 취약점을 이용하지 않고 신뢰자에게 원하는 구체적인 기대치에 따라 행동할 것을 믿는 것을 말한다[23].

기술 보호와 운영은 정보보안의 전통적인 요소이다. 기술보호와 운영과 관련된 기술적 보안 요소를 측정하기 위해 정보보호 자산관리의 적절한 관리, 정보보안 시스템 개발과 도입 정도, 정보보안 사고의 관리 수준, 물리적 환경에 대한 접근 통제, 사업연속성 계획 수립 여부 등 5가지 항목으로 측정하였다.

구성원의 보안에 대한 인식 수준은 정보보안에 대해 구성원이 얼마나 필요한 일로 인지하고 있는지, 정보보안이 개인적 측면이나 조직적 측면에서 가치 있는 일로 다소 번거롭더라도 해야 하는 일이라고 인식하는 것으로 출발한다. 그리고 개인이 부담해야 하는 정보보안 관련 업무가 그렇게 어려운 일이 아니며, 쉽게 배울 수 있고 용이한 일로 인지하는 것으로 판단할 수 있다. 따라서 구성원의 보안 인식은 정보보안의 필요성 인지, 정보보안의 가치 인식, 정보보안 업무의 용이성 인지의 3가지 항목으로 측정하였다.

구성원의 보안 관련하여 구체적으로 나타낼 수 있는 행위는 자신의 PC에 정보보안 관련 프로그램을 설치하여 보안 침해에 대비하고, 일상적으로 실시하는 개인 PC에 대한 보안 점검 활동, 그리고 보안 정책이나 지침을 숙지하고 이를 준수하는 행위, 보안 교육 및 훈련에 능동적으로 참여하는 태도, 조직 내외의 타인에게 정보보안의 중요성을 홍보하는 행위 등으로 판단할 수 있다. 따라서 구성원의 보안 행위는 정보보안 프로그램의 설치 및 활용, 일상적인 개인 PC 점검, 보안 정책의 숙지 및 준수, 보안 교육 훈

련의 참여, 정보보안의 중요성 홍보의 5가지 항목으로 측정하였다.

본 연구에서는 정보보안 거버넌스 구성 요인과 정보기술에 대한 구성원의 인식과 태도에 대한 선행연구를 바탕으로 주요 변수의 측정항목을 다음 표 1과 같이 요약 정리하였다. 그리고 연구 변수의 측정은 인구통계적 특성을 제외한 각 측정 문항을 모두 Likert 5점 척도로 하고, 해당 질문에 대해 전혀 동의하지 않을 경우 1점, 보통 수준일 경우 3점, 전적으로 동의할 경우는 5점을 부여하도록 하였다.

표 1. 주요 변수의 측정 항목
Table 1. Operationalization of Variables

연구 변수	측정 항목	주요 관련 연구
리더십과 거버넌스	• 정보보안에 대한 경영진의 지원과 추진 의지 • 정보보안 전략의 수립 • IT 거버넌스의 적용 • 위험완화 전략과 통제 • 정보보안프로그램의 효과 측정	Tudor, 2000 McCathy et al, 2001 Eloff et al, 2005 Da Viega et al, 2007
보안 관리 조직	• 정보보안 관리 조직의 구성 • 정보보안 관리 조직의 역할과 책임 명시 • 정보보안 기술과 경험 요소 • 정보보안과 관련 법의 준수	Tudor, 2000 McCathy et al, 2001 ISO/IEC 17799, 2005 Eloff et al, 2005 Da Viega et al, 2007
보안 정책	• 정보보안 정책 수립 • 정보보안 표준과 절차 • 정보보안 실무 가이드라인	Tudor, 2000 McCathy et al, 2001 ISO/IEC 17799, 2005 Eloff et al, 2005 Da Viega et al, 2007
보안프로그램 관리	• 위험관리를 고려한 정보보안 프로그램의 운영 • 보안관련 법의 준수 여부 • 구성원의 행위 관리 • 보안사고 대처 정도	Tudor, 2000 McCathy et al, 2001 Da Viega et al, 2007 ISO/IEC 17799, 2005
사용자 보안 관리	• 사용자의 정보보호에 대한 인지 • 사용자 교육 훈련 • 윤리 강령 • 신뢰 확보 • 개인정보보호	Tudor, 2000 McCathy et al, 2001 Da Viega et al, 2007
기술적 보안 요소	• 자산관리 • 정보보안 시스템 개발과 도입 • 정보보안 사고 관리 • 물리적 환경 • 사업 연속성	McCathy et al, 2001 Eloff et al, 2005 Da Viega et al, 2007 ISO/IEC 17799, 2005
구성원의 보안 인식	• 정보보안의 필요성 인지 • 정보보안의 가치 인식 • 정보보안 업무의 용이성 인지	Davis, 1989 Davis et al, 1989
구성원의 보안 행위	• 정보보안 프로그램의 설치 및 활용 • 일상적인 개인 PC 점검 • 보안 정책의 숙지 및 준수 • 보안 교육 훈련의 참여 • 정보보안의 중요성 홍보	Mathieson, 1991 Taylor and Todd, 1995

Ⅳ. 실증분석 및 결과

4-1 표본의 선정과 분석 방법

정보보안은 조직의 성격이나 규모에 관계없이 중요한 일로 인식되고 있으며, 현실적으로는 기업의 규모나 조직의 성격에 따라 정보보안 거버넌스의 수준에 차이가 있을 것으로 추정된다. 하지만 본 연구는 특정 조직이나 규모에 제한하여 수행하는 것이 아니므로, 개인정보보호용 보안 프로그램을 포함하여 정보보안 관리를 어느 정도 하고 시행하고 있다고 판단되는 조직을 대상에 포함시켰다.

그리하여 본 연구에 사용된 설문은 정보보안시스템을 판매, 설치, 지원하는 보안 전문업체에 문의하여 자신들이 보안시스템을 개발 또는 납품한 기업 또는 대학의 명단을 입수하여 해당 대학 또는 기업체의 정보보안 담당자에게 e-mail를 보냈다. 그리고 기념품 송부와 함께 수차에 걸친 부탁을 통해, 소속 구성원 중 10명 내외에 대해 설문을 작성하도록 하여 결과 자료를 e-mail로 회수하는 방식을 취하였다. 설문조사기간은 2009년 6월 초순부터 2009년 9월 중순까지 약 3개월에 걸쳐 실시되었으며, 이를 통해 회수된 383부의 설문지중 성의가 없거나 일관성이 없다고 판단되는 설문지 8부를 제외한 375부의 설문지를 본 연구의 분석대상으로 삼았다.

본 연구의 자료분석은 2단계에 걸쳐서 시행되었다. 1단계분석인 조사대상의 일반적인 특성과 측정변인의 기술통계분석은 Microsoft Excel을 이용하여 기본적인 분석을 실시하였다. 그리고 변수들 간 상호관계를 분석하기 위해서 SPSS/WIN 14.0을 이용하여 상관분석과 분산분석 등을 실시함으로써 가설 검증을 하였다. 본 연구에 사용된 유의성은 5% 수준에서 유의한 것으로 하였다.

그리고 2 단계분석인 연구모형의 적정성을 검증하기 위하여 LISREL8.30을 이용하여 공변량분석을 사용하였다. 설정된 분석문제를 실증적으로 검증하고 연구 모형의 탐색을 위해 수집된 자료는 SPSS/WIN과 LISREL8.30을 이용하여 처리하였다. 기초자료를 수집하기 위하여 측정도구로 이용된 설문지의 타당성과 신뢰성을 검증함에 있어 신뢰성 분석을 행하였고, 타당성 분석은 요인분석보다 연구모형에 관한 선행연구 및 요인별 성격, 이론적 상호연결성, 측정변수들 간의 상관관계 등 이론적 적합성에 의해 판단하였다.

4-2 일반적 특성 분석

본 조사에 참여한 대상자에 대한 인구통계적·사회경제적 특성을 파악해 본 결과, 전체 응답자 375명 중 남성이 282명으로 75%, 여성은 93명으로 25%를 차지하여 남성의 비중이 상대적으로 높았고, 연령별 분포를 파악해 본 결과 30~40대가 전체의 86% 를 차지하였다.

응답자의 학력 분포는 대졸이상이 58%를 차지하여 대부분 고학력이었고, 조직구분으로는 교육기관이 42%를 차지하여 비중이 다소 높았고, 소속 부서로는 IT 부서가 1/3을 차지하여 상대적으로 많았다. 또한 응답자의 조직 내부에서의 직위는 과장 이하가 70% 정도를 차지하여 실제 정보보안의 운영과 관리에 직간접으로 관련 있는 대상이 많았다. 응답자의 현 직장에서의 근속 년수는 5년 미만이 54%를 차지하고, 5년 이상 장기 근속자는 46%를 차지하였다. 본 연구의 설문 응답자에 대한 인구통계적·사회경제적 세부 특성은 표 2와 같이 요약된다.

그리고 구성원의 보안 인식과 행위에 영향을 주는 정보보안 거버넌스의 구성 요소별 각 하위요인별 측정 문항에 대한 기술통계량은 표 3과 같다.

표 2. 인구통계적·사회경제적 특성
Table 2. Demographic and Socioeconomic Characteristics

인구통계적 · 사회경제적 특성		인원수	유효비율 (%)
성별	남	282	75.2%
	여	93	24.8%
연령	20대	21	5.6%
	30대	152	40.5%
	40대	173	46.1%
	50대 이상	29	7.7%
학력	고졸 이하	27	7.2%
	전문대졸	59	15.7%
	대졸	219	58.4%
	대학원 이상	70	18.7%
조직구분	대기업	37	9.9%
	중견기업	117	31.2%
	중소기업	62	16.5%
	교육기관	159	42.4%
소속	IT부서	127	33.9%
	기획부서	72	19.2%
	관리부서	82	21.9%
	영업부서	45	12.0%
	기타	49	13.1%
직위	임원급	18	4.8%
	부장	67	17.9%
	차장	31	8.3%
	과장	81	21.6%
	대리 이하	178	47.5%
근무 연수	1년 미만	21	5.6%
	1~5년 미만	184	49.1%
	5~10년 미만	131	34.9%
	10년 이상	39	10.4%

표 3. 기술통계량
Table 3. Summary Statistics of Variables

구분	항목	평균	표준편차	평균 (표준편차)
구성원의 보안 인식	정보보안의 필요성 인지	3.61	0.96	3.49 (0.87)
	정보보안의 가치 인식	3.54	0.71	
	정보보안 업무의 용이성 인지	3.32	0.93	
구성원의 보안 행위	보안프로그램의 설치 및 활용	3.42	0.82	3.47 (0.86)
	일상적인 개인 PC 점검	3.75	0.72	
	보안 정책의 숙지 및 준수	3.32	0.94	
	보안 교육 훈련의 참여	3.62	0.93	
	정보보안의 중요성 홍보	3.25	0.89	
리더십과 거버넌스	정보보안에 대한 경영자 지원	3.89	0.72	3.58 (0.86)
	정보보안 전략의 수립	3.64	0.97	
	IT 거버넌스의 적용	3.72	0.77	
	위험완화 전략과 통제	3.45	0.92	
	보안프로그램의 효과 측정	3.21	0.93	
보안 관리 조직	보안 관리 조직의 구성	3.12	0.85	3.43 (0.82)
	관리 조직의 역할과 책임 명시	3.45	0.92	
	보안 기술과 경험 요소	3.53	0.72	
	정보보안 관련 법의 준수	3.61	0.79	
보안 정책	정보보안 정책 수립	3.62	0.88	3.59 (0.86)
	정보보안 표준과 절차	3.72	0.96	
	정보보안 실무 지침	3.45	0.74	
보안 프로그램 관리	위험관리 고려한 프로그램 운영	3.22	0.85	3.46 (0.86)
	보안 관련 법의 준수 여부	3.35	0.89	
	구성원의 불법 행위 관리	3.56	0.88	

	보안 사고 대처 정도	3.72	0.83	
사용자 보안 관리	정보보호에 대한 인지 정도	3.73	0.85	3.69 (0.91)
	사용자 교육 훈련 수준	3.83	0.97	
	윤리 강령	3.62	0.95	
	신뢰 확보 정도	3.45	0.92	
	개인정보보호 수준	3.82	0.86	
기술적 보안 요소	정보보안 자산 관리	3.17	0.94	3.54 (0.87)
	보안 시스템 개발과 도입	3.82	0.71	
	정보보안 사고 관리	3.52	0.97	
	물리적 환경(접근 통제)	3.72	0.82	
	사업 연속성 계획 수립	3.48	0.89	

4-3 측정 도구의 신뢰성 및 타당성 분석

본 연구에 이용된 설문항목들은 선행 연구를 통해 타당성과 신뢰성을 인정받고 있다. 그러나 정보보안 거버넌스의 구성요소와 구성원의 보안인식, 구성원의 보안행위에 대해 재정리하여 설계하였으므로, 각 문항이 대표하는 구성개념을 적절하게 측정하고 검증하기 위해 신뢰성 및 타당성을 검증하였다.

4-3-1 신뢰성 분석

본 연구의 구성 개념들은 조작적 정의를 기초로 하여 다항목척도에 대한 측정으로 이루어져 있으며, 동일한 구성 개념을 이루고 있는 항목들은 측정결과에 대해서 내적 일관성을 유지하여야 한다.

본 연구에 사용된 신뢰성측정 방법은 가장 일반적으로 사용되고 있는 방법으로 항목의 측정결과가 일관성을 유지하는가의 여부를 확인하기 위해 Cronbach's α 계수를 이용하여 신뢰성을 측정하였으며, 일반적으로 Cronbach's α 계수는 0.7을 넘으면 신뢰성이 상당히 양호하며, 0.6 이상이면 비교적 신뢰성이 높다고 본다. 본 연구의 신뢰성 검증을 위해 Cronbach's α 분석 결과는 표 4와 같으며, 각 변수의 신뢰성이 0.7이상으로 나타나 내적 일관성이 확보된 것으로 판단된다.

표 4에 명시된 분석의 결과를 보면 신뢰성 값은 모두 0.7이상으로 나타나 만족스러운 신뢰수준을 보여주고 있는 데, 이는 설문지의 구성항목들이 정보보안 거버넌스의 구성요소와 구성원의 보안인식 및 구성원의 보안행위를 평가함에 있어서 적절하게 선정된 것임을 나타낸다.

표 4. 측정변수들의 신뢰성 검증
Table 4. Reliability of Variables

연구 변수	항목수	α 계수
리더십과 거버넌스	5	0.787
보안 관리 조직	4	0.856
보안 정책	3	0.828
보안 프로그램 관리	4	0.815
사용자 보안 관리	5	0.875
기술적 보안 요소	5	0.819
구성원의 보안 인식	3	0.734
구성원의 보안 행위	5	0.791

4-3-2 요인 분석

신뢰성 분석 결과를 거친 측정항목들에 대하여 구성개념별로 확인요인분석(confirmatory factor analysis; CFA)을 실시하였다. 분석 결과는 표 5와 같이 나타났으며, 적합도를 나타내는 기초부합지수(GFI)는 0.93, 수정부합지수(AGFI)는 0.94, 표준부합지수(NFI)는 0.91, 비교부합지수(CFI)는 0.93, 표준카이자승치는 2.15, 표준화잔차는 2.61 등으로 나타나 현재의 수준에서 분석에 이용하였다.

표 5. 구성개념에 대한 확인요인분석 결과
Table 5. Confirmatory Factor Analysis of Variables

구분	항목	경로계수	표준오차	t값*
리더십과 거버넌스	정보보안에 대한 경영자 지원	0.91	0.06	14.93
	정보보안 전략의 수립	0.86	0.06	13.92
	IT 거버넌스의 적용	0.80	0.06	12.65
	위험완화 전략과 통제	0.73	0.06	11.38
	보안프로그램의 효과 측정	0.88	0.07	12.42
보안 관리 조직	보안 관리 조직의 구성	0.82	0.07	11.32
	관리 조직의 역할과 책임 명시	0.91	0.07	12.48
	보안 기술과 경험 요소	0.82	0.07	11.07
	정보보안 관련 법의 준수	0.84	0.06	13.17
보안 정책	정보보안 정책 수립	0.87	0.06	13.76
	정보보안 표준과 절차	0.80	0.06	12.97

	정보보안 실무 지침	0.84	0.06	13.61
보안 프로그램 관리	위험관리 고려한 프로그램 운영	0.87	0.07	12.21
	보안 관련 법의 준수 여부	0.86	0.07	11.97
	구성원의 불법 행위 관리	0.90	0.07	12.36
	보안 사고 대처 정도	0.93	0.06	15.16
사용자 보안 관리	정보보호에 대한 인지 정도	0.87	0.06	14.02
	사용자 교육 훈련 수준	0.87	0.06	13.84
	윤리 강령	0.94	0.06	14.61
	신뢰 확보 정도	0.84	0.06	13.25
	개인정보보호 수준	0.87	0.06	13.83
기술적 보안 요소	정보보안 자산 관리	0.81	0.07	11.11
	보안 시스템 개발과 도입	0.88	0.06	14.13
	정보보안 사고 관리	0.91	0.06	14.41
	물리적 환경(접근 통제)	0.87	0.06	14.31
	사업 연속성 계획 수립	0.81	0.07	11.44
구성원의 보안 인식	정보보안의 필요성 인지	0.85	0.07	11.86
	정보보안의 가치 인식	0.93	0.07	12.75
	정보보안 업무의 용이성 인지	0.83	0.07	11.26
구성원의 보안 행위	보안프로그램의 설치 및 활용	0.79	0.07	10.92
	일상적인 개인 PC 점검	0.84	0.06	13.58
	보안 정책의 숙지 및 준수	0.73	0.06	11.98
	보안 교육 훈련의 참여	0.84	0.06	13.27
	정보보안의 중요성 홍보	0.91	0.06	14.73

* 모든 t값은 $p<0.001$에서 유의하게 요인적재 되었음을 나타냄.

* 경로계수(factor loading)의 값은 표준화계수(standardized solution)임.

4-4 가설 검증

본 연구에서는 정보보안 거버넌스와 구성원의 보안 인식과 보안 행위 간의 관련성을 파악하기 위해 총 13가지의 연구가설을 정한 바 있다. 본 연구에서는 연구모형의 잠재변수들 간의 가설 검증을 위해 이론변수인 구성원의 보안 인식과 구성원의 보안 행위, 6가지 정보보안 거버넌스 구성 요소 간의 다중 회귀분석을 실시하였고, 그리고 구조 모델에 대한 분석도 병행하였다.

연구모형의 잠재변수들 간의 가설 검증을 위해 구조 모델을 표 6과 같이 분석하였으며, 측정 모델은 1 단계 분석을 통해 분석한 것이다. 이 결과를 볼 때 단측검증시 유의수준 0.01에서 H11, H14, H15, H21, H23, H24, H25, H31은 t값이 2.33을 초과하므로 가설은 채택되었으나, H12, H13, H16, H22, H26은 기각되었다.

표 6. 연구모형의 가설 검증 결과
Table 6. Results of Hypothesis Test

가설/방향	경로	경로계수	표준오차	t값	결과
$H_{11}(+)$	리더십과 거버넌스→구성원보안인식	0.40	0.07	4.35	채택
$H_{12}(+)$	보안관리조직→구성원보안인식	0.05	0.06	0.86	기각
$H_{13}(+)$	보안정책→구성원보안인식	0.05	0.06	0.92	기각
$H_{14}(+)$	보안프로그램관리→구성원보안인식	0.11	0.05	2.52	채택
$H_{15}(+)$	사용자 보안관리→구성원보안인식	0.29	0.06	4.91	채택
$H_{16}(+)$	기술적 보안요소→구성원보안인식	0.14	0.07	1.95	기각
$H_{21}(+)$	리더십과 거버넌스→구성원보안행위	0.25	0.05	5.47	채택
$H_{22}(+)$	보안관리조직→구성원보안행위	0.07	0.04	1.85	기각
$H_{23}(+)$	보안정책→구성원보안행위	0.22	0.04	6.08	채택
$H_{24}(+)$	보안프로그램관리→구성원보안행위	0.10	0.03	3.41	채택
$H_{25}(+)$	사용자 보안관리→구성원보안행위	0.24	0.04	5.95	채택
$H_{26}(+)$	기술적 보안요소→구성원보안행위	0.03	0.04	0.68	기각
$H_{31}(+)$	구성원보안인식→구성원보안행위	0.18	0.04	4.35	채택

* 구성원의 보안 인식의 R제곱 : 0.73 구성원의 보안 행위의 R제곱 : 0.88

4-5 연구 모형의 검토

본 연구에서는 연구모형을 기반으로 LISREL 기본 모형을 설계하고, 이를 기초로 하여 측정모형에 사용할 측정변수들을 가려낸 후 모형개선절차를 거쳐 최적 모형을 도출하려 하였으나, 기존의 측정변수를 모두 모형에 사용하기로 하였다. 물론 내생 및 외생 개념을 대표하기 위한 다른 많은 측정변수들이 사용될 수 있으나, 각 개념을 내용적으로 대표할 수 있는 주요 변수들만을 추출하여 사용하였으므로 별 무리는

없는 것으로 여겨진다. 본 연구의 측정모형에 대한 검증을 위해 사용된 LISREL 입력 매트릭스(matrix)는 표 7의 공분산 행렬을 사용하였다.

표 7. 연구모형분석에 이용된 공분산행렬
Table 7. Covariance matrix for Model testing

구분	구성원 보안 인식	구성원 보안 행위	리더십 거버넌스	보안 관리 조직	보안 정책	보안 프로그램 관리	사용자 보안 관리	기술적 보안 요소
구성원 보안 인식	0.832							
구성원 보안 행위	0.683	0.791						
리더십 거버넌스	0.605	0.632	0.697					
보안 관리 조직	0.508	0.531	0.438	0.808				
보안 정책	0.589	0.676	0.583	0.449	0.839			
보안 프로그램 관리	0.587	0.627	0.488	0.507	0.555	0.952		
사용자 보안 관리	0.603	0.648	0.532	0.447	0.587	0.552	0.751	
기술적 보안 요소	0.532	0.534	0.492	0.616	0.432	0.525	0.435	0.723

LISREL 실행 시 외생개념으로 구성원의 보안인식과 구성원의 보안행위를 잠재변수로 하였고, 정보보안 거버넌스의 구성 요소인 리더십과 거버넌스, 보안관리 조직, 보안정책, 보안프로그램관리, 사용자 보안관리, 기술적 보안 요소를 내생개념으로 정하여 그림 2와 같이 구조모델에 대한 추정 경로도를 구하였다.

구조 모델의 추정 경로도에서 정보보안 거버넌스의 구성요소 중에 리더십과 거버넌스, 사용자 보안관리, 보안정책 관련 요인들의 수준은 구성원의 보안 인식에 정(+)의 영향을 미친다고 볼 수 있다. 하지만 정보보안 거버넌스 구성 요소에서 보안 관리 조직과 기술적 구성 요소는 구성원의 보안 인식과 구성원의 보안 행위에 영향을 미친다고 할 수 없다. 또한 정보보안 거버넌스에 따른 구성원의 보안 행위를 활성화시키는 것은 정보보안 거버넌스 구성요소 중에 리더십과 거버넌스와 사용자 보안관리가 상대적으로 깊은 관련이 있으나, 보안 정책도 관련이 있는 것으로 나타났다.

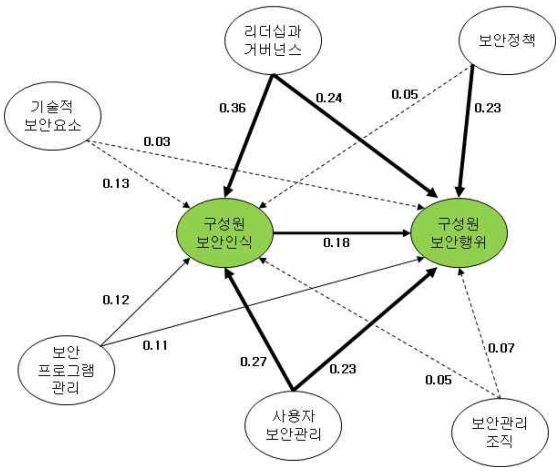

그림 2. 구조 모델
Fig. 2. Structural Model

구조 모델의 직접 및 간접 효과의 정도를 나타내는 표 8에서 보는 바와 같이 정보보안 거버넌스에 따른 구성원의 보안 인식에 직접적으로 영향을 미치는 것은 리더십과 거버넌스, 사용자 보안 관리, 보안 정책이며, 정보보안 거버넌스의 구성 요소 중 구성원의 보안 행위에 영향을 미치는 것은 리더십과 거버넌스, 보안 정책이 두드러진다고 할 수 있다. 그리고 정보보안 거버넌스에 따른 구성원의 보안 행위는 구성원의 보안 인식의 수준에 따라 가속될 수 있다고 판단된다.

이러한 LISREL 분석결과가 나타내는 구성 개념간의 관련성과 방향성의 정도를 기준으로 판단할 때 다음과 같은 몇 가지 특징을 지적할 수 있다.

첫째, 정보보안 거버넌스 구성요소 중 리더십과 거버넌스와 사용자 보안 관리는 정보보안 거버넌스 구성원의 보안 인식 및 구성원 보안 행위에 정(+)의 영향을 미친다고 할 수 있다.

둘째, 정보보안 거버넌스 구성요소 중 보안 정책은 다른 요인에 비해 정보보안 거버넌스 구성원의 보안 행위에 정(+)의 영향을 미친다고 볼 수 없다.

표 8. 구조 모델의 직접 및 간접 효과의 정도
Table 8. Direct and Indirect Effects of Structural Model

구조적 관계	총 효과	직접 효과	간접 효과
리더십과 거버넌스→구성원보안인식	0.36	0.36	-
보안관리조직→구성원보안인식	0.05	0.05	-
보안정책→구성원보안인식	0.05	0.05	-
보안프로그램관리→구성원보안인식	0.12	0.11	-
사용자보안관리→구성원보안인식	0.27	0.27	-
기술적 보안요소→구성원보안인식	0.13	0.13	-
리더십과 거버넌스→구성원보안행위	0.32	0.25	0.07
보안관리조직→구성원보안행위	0.08	0.07	0.01
보안정책→구성원보안행위	0.23	0.22	0.01
보안프로그램관리→구성원보안행위	0.12	0.10	0.02
사용자보안관리→구성원보안행위	0.29	0.24	0.05
기술적 보안요소→구성원보안행위	0.05	0.03	0.02
구성원 보안인식 → 구성원 보안행위	0.18	0.18	-

셋째, 정보보안 거버넌스 구성요소 중 보안 프로그램 관리도 구성원의 보안 인식 및 구성원 보안 행위에 어느 정도 정(+)의 영향을 미친다고 볼 수 없다.

넷째, 정보보안 거버넌스 구성원보안인식의 수준 향상이 구성원보안행위의 향상에 정(+)의 영향을 미친다고 볼 수 있다.

다섯째, 정보보안 거버넌스 구성요소 중 보안관리 조직과 기술적 구성요소는 구성원의 보안 인식 수준과 보안 행위를 결정하는 데 영향을 미친다고 할 수 없다.

Ⅴ. 결 론

정보보안 거버넌스를 계획하고 실행하며, 그 성과를 평가하고자 하는 조직의 입장에서 볼 때, 정보보안의 기술적, 관리적 측면보다 실패의 원인으로 지적되는 인적 자원이면서 정보보안을 일상적으로 실천해야 하는 구성원의 보안 인식과 행위는 매우 중요한 관심사이며 구체적인 대책을 강구해야 할 사안일 것이다. 하지만 기술적 문제, 처리 절차의 문제, 관련 이해관계인(사람) 문제 등을 종합적으로 고려해야 하는 정보보안의 문제는 결코 용이한 문제는 아니다. 하지만 본 연구의 결과는 정보보안 거버넌스를 확립하고자 하는 경영진 뿐만 아니라 보안 실무담당 책임자가 정보보안과 관련한 세부 실천 계획을 수립할 때 도움을 줄 수 있을 것으로 판단된다.

본 연구는 정보보안 거버넌스의 프레임워크를 구성하는 요소가 조직의 정보보안 거버넌스의 수준을 결정하는 데 영향을 줄 것으로 판단되며, 무엇보다 구성원의 정보보안에 대한 인식 제고 및 실천을 담보하기 위해 어떠한 구성 요소를 우선적으로 시행해야 하는 지에 대한 시사점을 준다. 또한 연구의 결과는 조직들이 현재 정보보안에 대해 어떤 측면에 더 투자를 하며, 신경을 쓰고 있는지도 간접적으로 파악할 수 있을 것이다.

정보보안 거버넌스의 구성요소와 구성원의 보안 인식과 행위와의 관계를 실증 분석한 결과 중에 주목할 몇 가지를 기술하면 다음과 같다.

첫째, 구성원의 정보보안에 대한 인식과 행위는 경영진의 리더십과 IT 거버넌스의 적용에 강한 영향을 받는 것으로 나타났다. 이것은 경영진의 정보보안에 대한 책임의식과 지원, 충분한 이해가 정보보안 거버넌스 향상에 필수적이라는 기존 연구에 부합된다[19].

둘째, 구성원의 보안 인식과 보안 행위를 활성화하기 위해서는 경영진의 리더십 뿐 만아니라 사용자에 대한 보안 관리가 중요하다. 이것은 사용자의 인식 변화에 직접적으로 영향을 미치는 행위이기 때문에 당연한 것으로 여겨지지만, 이에 대한 구체적인 실행 계획(교육, 훈련, 사내 홍보, 인지도 향상을 위한 프로그램 개발 등)을 강구하여 실천할 때 가능할 것이다.

셋째, 구성원의 보안 행위에 미치는 영향이 사용자에 대한 보안 관리보다는 보안 정책이 더 높다는 것이다. 이것은 보안의 필요성, 가치에 대한 인식을 구체적인 행동으로 나타나게 하는 것은 정보보안에 대한 정책, 표준, 지침 등이 더 구성원에게 강하게 느껴진다는 의미로 해석할 수 있을 것이다.

넷째, 보안 관리와 조직은 구성원의 보안 인식과 행위에 거의 영향을 미치지 못하고 있다. 이것은 정보보안 관련 조직의 구성, 책임과 역할, 기술 수준 등이 정보보안 거버넌스의 수준을 형성하는 주요한 요

소일 수는 있으나, 구성원에게는 직접적인 인식과 행동에는 영향을 미치지 못함을 의미한다.

다섯째, 정보보안의 기술적 구성 요소들은 구성원의 보안 인식과 행동에 거의 영향을 미치지 못하는 것으로 나타났다. 이 요소 또한 정보시스템의 사용자보다는 정보시스템 담당부서(보안담당자)에게 더 관계가 있는 요소이기 때문으로 해석할 수 있을 것이다.

그리고 정보보안 거버넌스에 영향을 주는 경영진과 이에 영향을 받는 구성원에 대한 연구가 부족한 현 시점에서 본 연구가 제시할 수 있는 몇 가지 시사점을 든다면, 첫째, 정보보안 거버넌스 프레임워크(구성요소)의 측정항목을 중심으로 자기 조직의 현재 정보보안 거버넌스 구성요소별 수준을 파악한 후에, 정보보안 시스템(인적, 물적, 제도적 체제)을 조직 상황에 맞도록 단계적으로 실천할 수 있는 투자 계획 수립에 활용한다면 전반적인 조직의 정보보안 수준을 향상시킬 수 있을 것이다. 둘째, 정보보안에 대한 조직 구성원의 보안 인식과 행동에 대한 수준을 측정할 수 있는 항목을 점검표(check list)로 하여 일반 기업이나 공공기관의 정보보안 수준을 자체적으로 점검(조사)해 본다면 정보보안 거버넌스의 실현 정도를 측정할 수 있을 것이며, 무계획적인 정보보안 시스템 도입으로 인한 비용손실을 예방하고, 정보보안 관련 비용 투입의 경중완급을 결정하는 데 참고가 될 수 있을 것으로 사료된다. 셋째, 개별 조직이 정보보안 거버넌스의 구성 요소별 문제점을 파악함으로써 정보보안의 성공적인 실행계획(action plan) 수립에 이를 반영하도록 하고, 조직구성원의 정보보안 인식과 태도, 행위 요소를 합목적적으로 변화시키기 위한 변화관리(change management) 전략의 수립에도 도움을 줄 수 있을 것이다. 넷째, 정보보안 거버넌스 도입에 따른 보안담당관의 전략적 접근 방법에 대한 고민을 해소할 수 있는 실용적인 방법론으로 활용될 수도 있다는 점을 들 수 있다. 특히, 조직이 현재 추구하고 있는 정보보안 거버넌스의 세부 항목에 조직 구성원의 정보보안 인식과 행위의 일상화를 위한 정보보안 문화적 요소를 세부적으로 보강하는 데 활용할 수도 있을 것이다. 특히 내부보안과 관련된 측면이 강화될 수도 있을 것이다.

본 연구의 한계점을 지적한다면 조사 대상자가 속한 산업군, 조직의 규모, 현재 담당하고 있는 직무에 따른 차이 등을 충분히 고려하지 못한 점은 있으나, 정보보안 거버넌스의 실천 대상으로서 구성원은 그 차이를 구분하지 않아도 동일한 결과를 가져올 것으로 판단하였다. 하지만 향후 정보보안 거버넌스와 구성원과의 관계와 관련한 연구를 할 경우에 조직의 규모와 산업군에 따른 차이, 조직 구성원의 직무에 따른 차이 등 추가적인 연구가 필요할 것으로 여겨진다.

감사의 글

이 연구결과물은 2008학년도 경남대학교 학술진흥연구비 지원에 의하여 이루어졌음.

참 고 문 헌

[1] 김정덕, 홍기향, “정보보호 거버넌스 이슈 및 연구 과제,” *정보보호학회지, 제17권 제4호*, pp. 18-25, 2007.

[2] 최훈, 김진우, “불확실성 회피성향이 수용 후 행동에 미치는 영향: 모바일 인터넷 서비스를 중심으로,” *경영정보학연구, 제16권 제3호*, pp. 95-116, 2006.

[3] Baggett, W. O., “Creating a culture of security”. *The Internal Auditor, Vol. 60, No. 3*, pp. 37-41, 2003.

[4] Chau, P.Y.K. and Hu, P.J.H,; “Information Technology Acceptance by Individual Professionals: A Model Comparison Approach,” *Decision Sciences, Vol. 32. No. 4*, pp. 699-719, 2001.

[5] COBIT security baseline— An information security survival kit. (2004). Rolling Meadows, USA: *IT Governance Institute*.

[6] Da Veiga, A. and Eloff J. H. P., “An Information Security Governance Framework,” *Information Systems Management, Vol. 24,* pp. 361-372, 2007.

[7] Da Veiga, A., Martins, N., and Eloff J. H. P., “Information security culture—validation of an assessment instrument,” *Southern African Business Review, Vol. 11, No. 1,* pp. 147-66, 2007.

[8] Davis, F.D., "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly, Vol. 13, No. 3*, pp. 319-340, 1989.

[9] Davis, F.D., Bagozzi, R.P., and Warshaw, P.R., "Extrinsic and Intrinsic Motivation to Use Computers in the Workplace," *Journal of Applied Social Psychology, Vol. 22, No. 14,* pp. 1111-1132, 1992.

[10] Deci, E.L., Intrinsic Motivation, Plenum Press, New York. 1975.

[11] Donaldson, W. H., U.S. capital markets in the post-Sarbanes-Oxley world: Why our markets should matter to foreign issuers. U.S. Securities and Exchange Commission. *London School of Economics and Political Science*, 2005.

[12] Duffy, J., IT Governance and business value part 1: IT Governance - An issue of critical importance. IDC document #27291, 2002.

[13] Fishbein M. and Ajzen, I., Belief, Attitude, Intentions and Behavior: *An Introduction to Theory and Research, Addison-Wesley.* 1975.

[14] Guldentops, E., IT Governance: Part and parcel of corporate governance, CIO Summit, European Financial Management & Marketing(EFMA) Conference, Brussels, 2003.

[15] Hellriegel, D., Slocum, J. W. (Jr), & Woodman, R. W., Organizational Behavior, (8th ed.). Cincinnati, OH: *South-Western College,* 1998.

[16] ISO/IEC 17799 (BS 7799-1), Information technology. Security techniques. *Code of practice for information security management, Britain,* 2005.

[17] IT Governance Institute, Board briefing on IT Governance (www.itgi.org), 2001.

[18] IT Governance Institute, CobiT Mapping: *Overview of International IT Guidance*, 2004.

[19] Johnston, Allen C. and Hale, Ron, "Improved Security through Information Security Governance," *Communications of the ACM, Vol. 52 Issue 1,* pp. 126-129, Jan. 2009.

[20] King Report. (2001). The King Report of corporate governance for South Africa, 2001 (Retrieved 12 January 2006 from http://www.iod sa co.za /down loads/ King_Report_CDRom_Bro chure.pdf)

[21] Lee, I., Kim, J.S., and Kim, J.W., "Use Contexts for the Mobile Data: A Longitudinal Study Monitoring Actual Use of Mobile Data Services," *International Journal of Human Computer Interaction, Vol. 18, No. 3,* pp. 269-292, 2005.

[22] Luftman, J. and T. Brier, "Achieving and Sustaining Busiess - IT Alignment," *California Management Review. Vol. 42, No. 1*, pp. 109-122, 1999.

[23] Martins, N., "A model for managing trust," *International Journal of Manpower, Vol. 23, No. 8,* pp. 754–69, 2002.

[24] Martins, A. & Eloff, J. H. P., Information Security Culture. In Security in the information society, IFIP/SEC2002. Boston: *Kluwer Academic Publishers*, 2002.

[25] Mathieson, K., "Predicting User Intention: Comparing the Technology Acceptance Model with Theory of Planned Behavior," *Information Systems Research, Vol. 2. No. 3,* pp. 173-191, 1991.

[26] McCarthy, M. P. & Campbell, S., Security Transformation, McGraw-Hill: *New York.,* 2001.

[27] Peterson, R. R., Information stratgeies and tactics for Information Technology governance, Hershey. PA: *Idea Group Publishing*, 2003.

[28] Posthumus, S. & von Solms. R., "A framework for the governance of information security," *Computers and Security, Vol. 23,* pp. 638-646, 2004.

[29] Posthumus, S. & Von Solms, R., "IT Governance," *Computer Fraud and Security, Vol.* 6, pp. 11–17, 2005.

[30] PriceWaterhouseCoopers. Information Security Breaches Survey, 2004. (Retrieved 12 March 2005 from http://www.dti.gov.uk/industry_files/pdf /isbs_2004 v3.pdf)

[31] Richards, N., "The critical importance of information security to financial institutions," *Business Credit, Vol. 104, NO. 9,* pp. 35-36, 2002.

[32] Robbins, S., Organizational Behaviour, (9th ed.), *New Jersey: Prentice Hall*, 2001.

[33] Ross, B., "New directives beef up trust in e-commerce," *Computer Weekly News, Vol. 172*, 2000.

[34] Ryan R.M. and Deci, E.L., "Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions," *Contemporary Educational Psychology, Vol. 25,* pp. 54-67, 2000.

[35] Sambamurthy, V. and R.W. Zmud, "Arrangements for Inforamtion Technology Governance: A Theory of Multiple Contingencies," *MIS Quarterly, Vol. 23, No. 2,* pp. 261-290, 1999.

[36] Taylor, S. and Todd, P., "Understanding Information Technology Use: A Test of Competing Models," *Information System Research, Vol. 6, NO. 2,* pp. 144-176, 1995.

[37] Tretic, B., "Can you keep a secret?" *Intelligent Enterprise, Vol. 4, No. 1,* Jan. 2001.

[38] Tudor, J. K., Information Security Architecture—An integrated approach to security in an organization, Boca Raton, FL: Auerbach, 2000.

[39] Van Grembergen, W., "Introduction to the Minitrack: IT governance and the mechanisms," *Proceedings of the 35th Hawaii International Conference on System Sciences (HICSS), IEEE.*, 2002.

[40] Venkatesh, V. and Brown, S.A., "A Longitudinal Investigation of Personal Computers in Homes: Adoption Determinants and Emerging Challenges," *MIS Quarterly, Vol. 25, No. 1*, pp. 71-102, 2001.

[41] Venkatesh, V. and Davis, F.D., "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies," *Management Science, Vol. 46, No. 2.* pp. 186-204, 2000.

[42] Venkatesh, V. Morris, M.G, Davis. G.B, and Davis, F.D., "User Acceptance of Information Technology toward a Unified View," *MIS Quarterly, Vol. 27, No. 3,* pp. 425-478, 2003.

[43] Von Solms, B., "Information security—the third wave?" *Computers and Security, Vol. 19, No. 7,* pp. 615-620, Nov. 2000.

[44] Von Solms, S. H., "Information Security Governance—compliance management vs. operational Management," *Computers and Security, Vol. 24, No. 6,* pp. 443–447, 2005.

[45] Vroom, C., & Von Solms, R., "Towards information security behavioural compliance," *Computers and Security, Vol. 23, No. 33,* pp. 191–198, 2004.

[46] Weill, P. and M. Vitale, "What IT infrastructure capabilities are needed to implement e-business models," *MIS Quarterly Executive, Vol. 1, No. 1,* pp. 17-34, 2002.

[47] Witty, R.J. & Hallawell, A., Client issues for security policies and architecture. Gartner. ID number: K-20-7780, 2003.

김 영 곤 (金英坤)

1980년 2월 : 한국외국어대학교 무역학과(상학사)
1986년 2월 : 한국외국어대학교 경영정보학과(경영학석사)
2000년 8월 : 창원대학교 경영학과 (경영학박사)
1994년 6월~현재 : 경남대학교 e-비즈니스학부 부교수
관심분야 : 정보보안, 웹 시스템 개발, 데이터베이스