www.calsec.or.kr
http://dx.doi.org/10.7838/jsebs.2014.19.1.063

최고경영층의 정보보호 리더십에 따른 정보보호 통제활동의 차이 분석

Comparison of Information Security Controls by Leadership of Top Management

유진호(Jinho Yoo)

초 록

본 논문에서는 정보보호 거버넌스를 강조한 선행연구들을 바탕으로, 거버넌스 측면에서 가장 첫 번째에 해당하는 최고경영층의 정보보호에 대한 리더십이 정보보호 정책수립, 정보보호 조직과 인력 구성, 정보보호 교육 및 훈련, 기술적 대책 활동, 모니터링 및 감사활동 등과 같은 정보보호 통제활동에 어떤 영향을 주는 지에 대해 실증적으로 분석하고자 한다. 뿐만 아니라 최고경영층의 리더십과 비교되는 요인으로 조직 내에서 발생한 인터넷 침해사고 피해에 의해 정보보호 통제활동에 얼마나 차이가 있는지를 분석하여 시사점을 찾고자 한다.

ABSTRACT

This paper is to analyze how the information security leadership of top management affects controls of information security. Controls of information security include the activity related to making information security policy, the activity related to making up information security organizational structure and job responsibilities, the activity related to information security awareness and training, the activity related to technical measures installation and operation, and the activity related to emergency response, monitering and auditing. Additionally we will analyze how Internet incidents affect controls of information security and find implications.

키워드 : 정보보호 거버넌스, 최고경영층의 정보보호 리더십, 인터넷 침해사고, 정보보호 통제활동
Information Security Governance, Leadership of Top Management, Internet Incidents, Control Components of Information Security

---

본 연구는 2013학년도 상명대학교 교내연구비를 지원받아 수행하였음.
* Dept. of Business Administration, Sangmyung University(E-mail : jhyoo@smu.ac.kr)
2013년 10월 28일 접수, 2014년 01월 03일 심사완료 후 2014년 02월 04일 게재확정.

1. 서 론

인터넷상에서 침해사고 발생이 잦아지고 있다. 2009년 7월 7일에 발생한 DDoS 공격에 의해서는 인터넷을 이용한 매출이익이 발생하는 기업에 영향을 주었다. 인터넷을 통해 전자상거래를 하는 기업이나 금융기관의 사이트가 마비됨으로써 사이트가 마비된 시간 동안 인터넷 거래가 발생하지 못해 매출이익 손실이 발생하였다.

2011년 3월 4일에는 국내 40개 주요 웹사이트를 대상으로 DDoS 공격이 수차례 발생하였다. 공격은 주로 정부부처・공공기관 24개이었고, 금융기관도 9개, 포탈・쇼핑몰도 7개 사이트가 대상이 되었다. 2011년 3.4 DDoS 공격에 동원된 좀비PC의 규모는 '09년 7.7 DDoS와 비슷했으나, 공격방법은 지능적이고 파괴적으로 변모한 것으로 나타났다.

2011년 4월 농협전산장애로 인해서는 인터넷뱅킹과 현금자동입출금기(ATM), 창구 입출금 거래를 비롯한 창구거래 등 모든 은행업무가 마비된 바 있다.

최근 2013년 3월 20일에는 KBS, MBC, YTN, 농협, 신한은행, 제주은행의 전산망 마비사태 발생으로 방송사에서는 PC와 노트북이 먹통현상, 전산망 마미, 인터넷으로 운영되는 뉴스편성 시스템이 먹통이 되었고, 피해 은행에서는 본사와 영업점에 있는 PC 작동불가, 파일삭제 발생, 창구거래, 현금자동입출금기 사용 불가, 인터넷뱅킹이 중단되기도 하였다.

인터넷 침해사고에 대응하기 위해 그리고 새로운 침해위협에 대응하기 위해 기업이나 정부, 공공기관에서는 조직내 정보보호 수준을 제고하기 위해 다각적으로 노력하고 있다. 인터넷 침해사고를 예방하고 조직의 정보보호 수준을 높이기 위해서는 조직 내 다양한 정보보호 통제활동이 적절하게 이루어져야 한다. 이와 관련되어 최근에는 기업 거버넌스와 연관된 정보보호 거버넌스에 대한 관심도 높아지고 있다.

정보보호 거버넌스 관점에서 정보보호 통제활동은 최고경영자의 지침에 근거하여 정보보호 정책을 수립하고, 정보보호에 적합한 조직을 구성・운영하고, 직원의 수준별로 맞춤형 교육을 통해 이용자의 책무를 강화할 뿐만 아니라, 정보보호를 위해 필요한 기술적 대책활동을 수행하며, 수시로 위험관리 상태를 점검하여 최고경영자에게 알리는 순환구조이다.

본 논문에서는 정보보호 거버넌스를 강조한 선행연구들을 분석하고, 거버넌스 측면에서 중요한 최고경영층의 정보보호에 대한 리더십에 따라 정보보호 정책수립, 정보보호 조직과 인력 구성, 정보보호 교육 및 훈련, 기술적 대책 활동, 모니터링 및 감사활동 등이 어떻게 달라지는지에 대해 실증적으로 분석하고자 한다. 뿐만 아니라 기업 내에서 발생한 인터넷 침해사고 피해에 의해 정보보호 통제활동이 어떻게 달라지는지에 대해서도 분석하여 시사점을 찾고자 한다.

본 논문은 다음과 같이 크게 5장으로 구성되어 있다. 제 2장에서는 정보보호 거버넌스 관련 선행연구를 분석하고, 제 3장에서는 연구 모형을 설정하고 가설을 수립한다. 제 4장에서는 가설의 검증과정을 상세히 설명하고, 검증결과에 근거하여 시사점을 찾고자 한다. 마지막으로 제 5장에서는 본 연구 결과의 의미, 한계점 및 향후 연구방향을 밝히고자 한다.

2. 선행연구

정보보호 통제활동이란 기술적, 관리적, 물리적 정보보호 통제를 선택하고, 구현하며, 유지관리하기 위한 일련의 활동이다. ISO 27001에서는 <Table 1>과 같이 정보보호 통제활동을 11개 영역으로 나누어 관리하고 있다[1].

Solms[2]은 정보보호의 패러다임을 크게 4가지 흐름(Wave)으로 정의하였다. 1세대는 기술적인 이슈로 특징지어지는 세대를 말하고, 2세대는 관리적인 차원이 중요시 되어, 정책이나 관리대책이 중요시되는 세대이다. 제 3세대는 정보보호에 대한 표준화된 형태를 갖추고, 우수사례(Best Practice)나 인증(certification), 정보보호 문화, 정보보호에 대한 측정과 모니터링이 중요시되는 세대이며, 제4세대는 정보보호 거버넌스가 핵심 역할을 하는 세대라고 설명하였다. 특히 제 4세대 정보보호 거버넌스는 기업 거버넌스 발전뿐만 아니라 기업 기버넌스 관련 법령이나 규제 영역과도 아주 밀접하게 연관되어 있다고 하였다[2].

〈Table 1〉 Control Sections of ISO 27001

Sections	Descriptions
1. Security Policy	To aim to provide management direction and support for information security, including laws and regulations.
2. Organization of Information Security	To constitute the process implemented to manage information security within the organization.
3. Assets management	To focus on asset inventories, information classification, and labeling.
4. Human resources security	To consider permanent, contractor, and third-party user responsibilities to reduce the risk of theft, fraud, and misuse of facilities. This section also includes awareness, training, and education of employees.
5. Physical and environment security	To allow only authorized access to facilities and secure areas.
6. Communication and operations management	To focus on the correct and secure operation of information processing facilities, such as segregation of duties, change management, malicious code, and network security.
7. Access control	To manage user access to information and include clear desk principles, network access controls, operating system access controls, passwords, and teleworking.
8. Information system acquisition development and maintenance	To ensure the security of user-developed and off-the-shelf products.
9. Information security incident management	To ensure that incidents are communicated in a timely manner and that corrective action is taken.
10. Business continuity management	To focus on business continuity plans and the testing thereof.
11. Compliance	To focus statutory, regulatory or contractual, laws, audit and organizational policy requirements, or obligations.

Solms[2]은 정보보호 거버넌스의 기본적인 특징 중의 하나로 정보보호 거버넌스는 순환 반복(Closed Loop) 구조로 이루어져야 한다는 사실을 강조하였다. 첫 번째는, 정보보호에 대한 최고경영층(Top Management)의 약속과 책무로 시작한다. 경영층에서 기업의 IT 리스크를 관리하는 것에 대한 책임을 지고, 기업 존재가치의 전략적 중심축에 정보보호를 두겠다는 약속을 함으로써 시작한다는 것이다. 두 번째는, 이러한 약속과 책무는 기업에서 정보보호 정책수립과 이에 대한 이사회 승인으로 이어진다는 것이다. 세 번째는 이러한 정책은 지속적으로 정보보호 조직을 통해 지원을 받고 실행되어야 한다는 것이다. 네 번째는 기업의 정보보호에 대한 책임들은 반드시 IT 시스템의 모든 사용자(직원)들에 대한 인식제고 프로그램과 교육 및 훈련으로 강화되어야 한다는 것이다. 다섯 번째는 정보보호를 위해 필요한 기술들이 구축되고 관리되어야 한다는 것이고, 여섯 번째는 정보보호 정책이나 규정에 대한 준수(Compliance) 여부를 전사차원에서 모니터링하는 체계를 구축하고, 이를 조직차원에서 측정하고 관리해야 한다는 것이다. 마지막으로는 이러한 측정결과를 최고 경영층에게 보고해야 하고, 이러한 과정은 계속적으로 순환 반복(Closed Loop) 되어야 한다는 것이다[2].

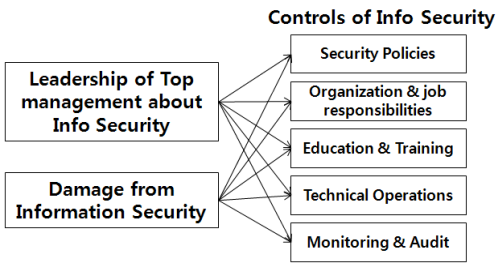
Veiga and Eloff[3]는 ISO 27001의 11개 정보보호 통제활동을 포함하는 통합적인 정보보호 거버넌스 체계를 제시하였다. 이 때 정보보호 거버넌스 체계를 1) 리더십과 거버넌스, 2) 정보보호관리 및 조직, 3) 정보보호 정책, 4) 정보보호 프로그램 관리, 5) 이용자 보안관리, 6) 기술적 대책 및 운영 등 6개의 주요 카테고리로 분류한 통합적인 프레임워크를 제시하였다[3]. 여기서 리더십과 거버넌스는 정보보호를 위한 경영층의 지원과 약속을 의미하고, 정보보호 관리 및 조직은 정보보호 조직을 설계하고 역할을 정의하는 것을 의미한다. 정보보호 정책은 직원들과 그들의 행위를 위한 가이드라인을 정하는 것을 의미하며, 정보보호 프로그램 관리는 정책에 대한 준수여부 확인 및 모니터링, 감사 등을 의미한다. 또한 이용자 보안관리는 이용자에 대한 인식제고 활동, 교육 및 훈련 등을 의미하고, 기술적 대책 및 운영은 전통적인 관점의 정보보호 수단으로서 기술적이고 물리적인 매커니즘을 구축하고 운영하는 것을 의미한다.

본 논문에서는 정보보호 거버넌스를 강조한 선행연구들을 바탕으로, 거버넌스 측면에서 가장 첫 번째에 해당하는 최고경영층의 정보보호에 대한 리더십이 나머지 5개 정보보호 통제활동에 어떤 영향을 주는 지에 대해 실증적으로 분석하고자 한다. 또한 기업내에서 발생한 인터넷 침해사고 피해에 의해 정보보호 통제활동이 차이가 있는지도 분석하고자 한다.

3. 연구모형 및 방법론

3.1 연구모형 및 가설설정

<Figure 1>은 본 논문에서 실증적으로 분석하고자 하는 연구모형이다. 연구모형에 따라 검증하기 위해 세운 가설은 다음과 같다.



〈Figure 1〉 Research Model

가설 1 : 정보보호에 대한 최고경영층의 리더십이 높은 조직은 그렇지 않은 조직에 비해, 정보보호 정책수립 활동, 정보보호 조직과 인력 구성 활동, 정보보호 교육 및 훈련 활동, 기술적 대책 활동, 모니터링 및 감사활동이 활발하다.

가설 2 : 인터넷 침해사고 피해가 없는 조직은 그렇지 않은 조직에 비해, 정보보호 정책수립 활동, 정보보호 조직과 인력구성 활동, 정보보호 교육 및 훈련활동, 기술적 대책 활동, 모니터링 및 감사활동이 활발하다.

3.2 변수의 조작적 정의 및 측정방법

가설 검증을 위해 사용된 변수들의 조작적인 정의(operational definition)와 이에 대한 측정방법은 다음과 같다.

3.2.1 정보보호 정책수립 활동

Wiant[4]는 정보보호 정책을 조직의 정보보호 관리의 방향을 명시하는 상위 수준의 문서로 정의하고, 조직 내에서 정보보호 임무를 수행하기 위해 필요한 요구사항이라고 하였다[4].

본 논문에서는 정보보호 정책수립 활동을 Wiant[4]와 ISO 27001의 정의를 기반으로 “조직의 정보보호 관리 방향을 명시하는 활동으로서, 조직 내에서 정보보호 임무를 수행하기 위한 문서화된 지침과 사용자 정보보호 지침 등을 제정하는 활동”이라고 정의하고자 한다.

정보보호 정책수립 활동은 공식적으로 정의되고 문서화된 정보보호 정책이 있는지, 사용자 보안을 위해 사용자 정보보호 지침을 제정하여 운영하는지, 사내 네트워크를 통한 SNS 이용에 대한 보안정책 및 가이드라인을 운영하는지, 무선랜 이용에 대한 보안정책을 수립하여 운영하는지 등을 측정하였다.

3.2.2 정보보호 조직과 인력 구성

Solms[5]은 성공적인 정보보호 구현을 위해서는 담당 조직을 구성하는 것이 반드시 필요하고, 조직을 구성하는 것뿐만 아니라 업무에 대한 책임과 역할을 부여하는 것도 필요하다고 하였다[5].

본 논문에서는 정보보호 조직과 인력 구성 활동을 ISO 27001의 정의를 기반으로 “정보보호 전담조직을 설치 운영하고, 정보보호 책임자를 임명하여 다각적인 역할을 수행하도록 하는 것”으로 정의를 하고자 한다.

정보보호 조직과 인력 구성은 IT 관련 업무의 총괄 책임자, 정보보호 책임자를 직제규정 등에 의거하여 명시적으로 임명하고 있는지와 정보보호 전담조직을 설치 운영하는 지의 여부를 바탕으로 측정하였다. 구체적인 항목으로는 정보관리 책임자(CIO : Chief Information Officer), 정보보호 책임자(CSO : Chief

Security Officer), 개인정보보호 책임자(CPO : Chief Privacy Officer)를 명시적으로 임명하고 있는 지, 정보보호 전담조직이나 개인정보보호 전담조직을 운영하고 있는 지에 대한 여부이다.

3.2.3 정보보호 교육 및 훈련

Solms[5]은 조직내 정보보호를 위해 조직원에 대한 교육활동이 필요할 뿐만 아니라, 침해사고 예방을 위해 인적 통제활동의 중요성을 강조하였다[5].

본 논문에서는 정보보호 교육활동을 “조직내 CEO 대상, 책임자급 대상, IT 실무자급 대상, 일반직원 대상으로 그 수준에 맞는 적절한 교육과 훈련을 통해 정보보호 인식을 제고하는 활동”으로 정의하고자 한다.

정보보호 교육 및 훈련은 CEO 등 최고경영층 대상, 정보보호 책임자 대상, 정보보호 실무자 대상, 일반 직원 대상, 개인정보보호 관리자 대상 등 다양한 계층별로 맞춤형 정보보호교육을 의무적으로 실시하거나 선택적으로 실시하는 지의 여부를 바탕으로 측정하였다.

3.2.4 기술적 대책 활동

Aron et al.[6]은 정보보호 S/W의 사용이 컴퓨터 바이러스의 감염을 감소시키는데 기여한다는 것을 제시하였고[6], Wei et al.[7]는 침입탐지시스템(IDS : Intrusion Detection System) 등과 같은 솔루션의 효과성을 검증하였다[7].

본 논문에서는 기술적 대책 활동을 “조직내에서 사용하고 있는 네트워크, 서버, PC, S/W, 컨텐츠, 데이터베이스 등을 보다 더 안전하게 운영하기 위해서 취하는 다양한 기술적인 보호조치 활동”으로 정의를 하고자 한다.

기술적 대책 활동은 조직 내 정보보호를 위한 기술적인 대책으로서, 네트워크 보안을 위한 기술적 대책, S/W 보안, 컨텐츠 보안, PC 보안을 위한 기술적 대책, 접근관리 및 인증을 위한 기술적 대책 등을 바탕으로 측정하였다.

3.2.5 모니터링 및 감사활동

Solms[8]은 정책이나 규정에 대한 준수여부(Compliance)를 측정하고 강화하는 것은 조직에서 기본적으로 중요하다고 하였다[8]. Vroom and Solms[9]는 기술과 조직원들의 행위는 정보보호 정책에 대한 준수여부 확인을 위해 관리되어야 한다고 하였고, 정보보호 감사는 정보보호 정책, 프로세스, 통제요소들이 조직의 목표나 비전 등과 연계되어 있다는 것을 보장하기 위해 필요하다고 하였다[9].

Caminada et al.[10]은 보안 감사활동이 침해사고를 감소시키는데 긍정적인 효과가 있고, 적절한 탐지 및 대응활동이 없는 조직은 침해사고 발생빈도가 높아진다고 하였다[10].

본 논문에서는 모니터링 및 감사활동을 “조직 내 정보보호에 대한 평가 수단으로 보안감사나 다각적인 모니터링을 하는 활동뿐만 아니라 침해사고에 대해 적시에 대응하기 위한 계획을 수립하고 운영하는 활동”으로 정의를 하고자 한다.

모니터링 및 감사활동은 침해사고 예방을 위해 다양한 위협과 취약성을 분석하고, 트래픽을 모니터링 하는 등 신속하게 체계적으로 응대하거나, 사고 후 긴급연락체계 구축, 사고 복구조직 운영 등 실시간 대응여부를 합산하여 측정하였다.

3.2.6 최고경영층의 정보보호 리더십

Joshi[11]는 조직의 정보보호 수준 향상에 가장 중요한 요인은 최고경영자의 정보보호에 대한 지원이라고 하였고[11], 최명길[12]는 최고경영자에 의한 조직적 차원의 지원은 정보보호 성숙도 수준에 긍정적인 영향을 준다고 하였다[12].

본 논문에서는 최고경영층의 정보보호 리더십을 “CEO 등 최고경영층이 경영계획을 수립할 때, 정보보호를 중요하게 생각하는 정도”라고 정의를 내리고자 한다.

〈Table 2〉 Operational Definition and Measurement of Variables

Sections	Operational Definition	Measurement	Previous Research
Security Policies	Activity related to making information security policies, procedures, guidelines	• Documented Security Policies • Information Security guidelines for User • Information Security guidelines for using SNS service • Security Policies for using wireless LAN • Security Policies for commercial wireless internet service • Security Policies for mobile office	Wiant(2005)
Organization and Job Responsibilities	Activity related to making up information security organizational structure and job responsibilities	• Appointing CIO • Appointing CSO • Appointing CPO • Operating organizational structure for information security • Operating organizational structure for personal information protection	Solms(2001)
Education and Training	Activity related to information security awareness and training for employees and executives	• Education program for CEO • Education program for CSO/CISO • Education program for staffs of Information Security • Education program for general employee • Education program for managers of personal information protection	Solms(2001)
Technical Operations	Activity related to technical measures installation and operation	• Technical measures for network security • Technical measures for S/W, contents, PC security • Technical measures for access control and authentication	Aron et al.(2001)
Monitoring and Audit	Activity related to incidents emergency response and information security audit	• Operating CERT • Planning for emergency response • Operating emergency response channel or hotline • Operating incidents recovery team • Security Auditing by internal staffs • Security Auditing by external experts • Penetration Test by internal staffs • Penetration Test by external experts • Monitoring using auto-tools • e-Mail monitoring • Web monitoring	Solms(2005) Vroom and Solms(2004) Caminada et al.(1998)
Leadership of Top Management	Degree of importance that top management thinks about information security	• Degree of importance that top management thinks about information security when they make strategic management plans.	Joshi(1989) Choi, M.(2009)
Damage of Internet Incidents	Frequency of Internet incidents	• Frequency of damage caused via worm/virus • Frequency of damage caused via unauthorized access • Frequency of damage caused via DoS/DDoS • Frequency of damage caused via adware/spyware	Caminada et al.(1998)

최고경영층의 정보보호 리더십은 조직 내에서 CEO 등 최고경영층이 경영계획을 수립할 때, 정보보호를 중요하게 생각하는 정도를 측정하여 사용하였다.

3.2.7 인터넷 침해사고

Caminada et al.[10]는 사이버 공격은 취약점을 이용하여 정보보호의 안전성을 무너뜨리기 위한 시도이고, 인터넷 침해사고는 그 공격이 성공적으로 이루어져 발생하는 것으로, 비인가 접속, 서비스거부 공격, 악성코드 유포 등에 의해 발생한다고 하였다[10].

본 논문에서는 인터넷 침해사고를 “웜・바이러스, 비인가 접속, DoS・DDoS 공격, 애드웨어・스파이웨어 유포 등에 의해 가용성, 비밀성, 무결성이 상실되어 실질적인 손실비용이 발생한 침해사고”라고 정의를 내리고자 한다.

인터넷 침해사고 피해는 연간 가용성, 기밀성, 무결성을 상실시키고 실질적인 손실 또는 비용을 동반한 인터넷 침해사고의 발생빈도로 측정하였다. 구체적으로는 웜・바이러스, 트로이전 등에 의한 공격, 내부시스템에 대한 외부로 부터의 비인가 접속, DDoS 공격, 애드웨어・스파이웨어에 의한 감염 등으로 실질적 피해가 발생한 횟수를 측정하였다.

3.4 자료수집

설문조사 자료로는 한국인터넷진흥원에서 2011년도에 실시한 정보보호 실태조사(기업부문) 중에서 종업원 수가 50명 이상이고 250명 미만인 중소기업에 해당하는 내용을 활용하였다. 이들의 산업유형은 농림수산업, 제조업, 건설업, 도매 및 소매업, 운수업, 숙박 및 음식업, 출판, 영상, 방송통신 및 정보서비스업, 금융 및 보험업, 부동산 및 임대업, 전문, 과학 및 기술서비스업, 사업시설관리 및 사업지원 서비스업 등으로 분류된다. <Table 3>

〈Table 3〉 Distribution of Survey Response Companies

Industry Category	Frequency	Percentage(%)
Agriculture, forestry and fishery	30	2.90
Manufacturing	128	12.37
Construction	62	5.99
Wholesale and retail	81	7.83
Transport	108	10.43
Accommodation and catering	60	5.80
Publishing, video, broadcast communications, and information services	89	8.60
Finance and insurance	58	5.60
Real Estate and Leasing	54	5.22
Professional, Scientific and Technical Services	76	7.34
Business facilities management and business support services	99	9.57
Association, organization, repair and other personal services	67	6.47
etc	123	11.88
Total	1,035	100

은 설문에 응답한 표본의 업종별 구성 비율이다.

설문지에는 정보보호 정책 수립, 정보보호 조직과 인력 구성, 정보보호 교육 및 훈련, 기술적 대책 활동, 모니터링 및 감사활동, 최고경영층의 정보보호 리더십, 인터넷 침해사고 피해빈도 등을 포함하고 있다.

4. 연구결과 분석

본 논문에서는 가설을 검증하기 위해 Cronbach's alpha 계수분석, 상관분석, 요인분석(Factor Analysis), 다변량분산분석(MANOVA), 판별분석(Discriminant Analysis) 등의 통계적 기법을 사용하였다.

4.1 신뢰성 검증

추상적 개념을 경험적 지표로 구현시키는 과정에서 문제가 되는 측정(Measurement)의 신뢰성(reliability) 검증을 위해 Cronbach's alpha 계수를 사용하였다. <Table 4>는 변수에 대한 신뢰성 검증을 한 결과이다. 초기 변수 중에서 신뢰도가 낮은 변수를 제외하고, Cronbach's alpha 계수를 측정한 값이 0.7 이상이므로 신뢰도에는 크게 이상이 없는 것으로 판단된다.

4.2 측정도구의 타당성 검증

측정변수간의 타당성(validity) 분석을 위해서는 요인분석(Factor Analysis)을 수행하였다. <Table 5>는 변수간의 그룹이 타당한지를 보여주는 요인분석 결과이다. 요인분석의 Varimax법에 의한 직각회전 결과로서 회전후의 요인패턴과 각 요인의 고유값, 설명분산 비율 등을 제시하였다. Factor 1과 Factor 2 요인은 24개 변수들에 대해서 전체 분산의 약 81.3%를 설명하는 것으로 나타났다. 전체적으로 볼 때 변수들의 그룹핑도 사전에 분류된 것처럼 유사한 패턴을 보이고 있으므로 타당성 검증에도 크게 이상이 없는 것으로 판단된다.

정보보호정책 변수들은 사후적으로 기술적 대책과 함께 그룹화되는 것으로 나왔지만 설계자가 사전적으로 문항 그룹화하여 신뢰도를 검증한 Cronbach's alpha 계수에서는 높은 내적 합치도(internal consistency)를 보이고 있으므로, 서로 다른 요인(Factor)으로 묶어서 활용해도 될 것으로 판단되어 기술적 대책과 나누어 그룹화하였다.

〈Table 4〉 Result of Reliability Test

Sections	Initial Variables	Final Variables	Cronbach's alpha
Security Policies	6	4	0.72
Organization and Job Responsibilities	5	5	0.80
Education and Training	5	5	0.88
Technical Operations	3	3	0.84
Monitoring and Audit	11	7	0.82
Total	30	24	-

또한 정보보호 조직 및 인력 구성 변수들은 2개 그룹으로 나뉘어 그룹화되는 것으로 나왔지만, 이 역시 신뢰도를 검증한 Cronbach's alpha 계수에서는 높은 내적 합치도를 보이고 있으므로, 동일 요인으로 묶어서 활용하였다.

요인분석의 결과만을 활용할 경우 설문지 설계자의 사전 문항 그룹화를 전적으로 무시하게 되고, Cronbach's alpha 계수에 의한 신뢰성 분석결과에만 의존할 경우에는 사전적 문항 그룹화에 전적으로 의존하기 때문에 이를 적절히 중화시키는 것이 필요하다. 즉, 설문 설계자의 의도를 존중하되 그것이 자료분석결과에 의하여 어느 정도 지지되는 지를 검토하는 과정을 갖는 것이 바람직하다[13].

〈Table 5〉 Result of Factor Analysis

Category	Variables	Factor1	Factor2	Factor3	Factor4	Factor5
Education and Training	• Education program for CEO	0.77014				
	• Education program for CSO/CISO	0.73106				
	• Education for staffs of Information Security	0.70036				
	• Education program for general employee	0.68004				
	• Education for managers of personal information protection	0.56398				
Monitoring and Audit	• Planning for emergency response		0.66434			
	• Operating emergency response channel		0.64741			
	• Security Auditing by internal staffs		0.63102			
	• Operating CERT		0.62079			
	• Operating incidents recovery team		0.54356			
	• Web monitoring		0.48233			
	• Penetration Test by internal staffs		0.47262			
Technical Operations	• Technical measures for S/W, contents, PC security			0.73282		
	• Technical measures for network security			0.70892		
	• Technical measures for access control and authentication			0.70372		
Security Policies	• Information Security guidelines for User			0.45904	0.33470	
	• Documented Security Policies			0.41474	0.33732	
	• Security Policies for using wireless LAN			0.37951	0.09357	
	• Information Security guidelines for using SNS service			0.25392	0.11912	
Organization and Job Responsibilities	• Appointing CSO				0.76455	0.20482
	• Appointing CIO				0.75905	0.16648
	• Appointing CPO				0.28723	0.66784
	• Operating organizational structure for personal information protection				0.12512	0.66055
	• Operating organizational structure for information security				0.28096	0.32889

Category	Factor1	Factor2	Factor3	Factor4	Factor5
Eigenvalue	7.72	1.64	1.17	0.92	0.61
% of Variance(%)	67.05	14.24	10.16	8.01	5.33

4.3 최고경영층의 정보보호 거버넌스 리더쉽에 따른 정보보호 통제활동간 차이 분석

<가설 1>은 정보보호에 대한 최고경영층의 리더십이 높은 조직은 그렇지 않은 조직에 비해, 5가지 정보보호 통제활동이 활발하다는 것이다. 이 가설을 검증하기 위해 다변량분산분석(MANOVA)을 사용하였다.

정보보호에 대한 최고경영층의 리더십이 높은 기업, 보통인 기업, 낮은 기업으로 나누고, 그룹별 정보보호 정책수립 활동, 정보보호 조직과 인력 구성, 정보보호 교육활동, 기술적 대책 활동, 모니터링 및 감사활동의 차이를 분석하였다. 정보보호에 대한 최고경영층의 리더십이 높은 기업(High), 보통인 기업(Medium), 낮은 기업(Low)의 분포는 각각 전체의 68.0%, 25.9%, 6.1%를 차지하고 있다.

<Table 6>은 가설 검증결과이다. MANOVA 분석을 통해 최고경영층의 정보보호 리더십 그룹별로, 정책수립 활동, 조직과 인력 구성, 정보보호 교육 및 훈련, 기술적 대책 활동, 모니터링 및 감사활동 등 5개 정보보호 통제활동에 차이가 있는 것으로 나타났다. 특히, 정보보호 교육 및 훈련, 정보보호 정책수립활동이 가장 큰 차이가 있는 것으로 나타났다(F-value 각각 35.75, 32.06). 실제로 평균값을 비교한 <Table 7>을 통해서도, 최고경영층의 정보보호 리더십이 강한 기업은 그렇지 않은 기업에 비해 모든 정보보호 통제활동이 활발하게 이루어지고 있고, 특히 정보보호 교육 및 훈련, 정책수립활동이 월등히 높음을 알 수 있다.

〈Table 6〉 Results of MANOVA(by Leadership of Top Management)

Category	F-value	p-value
(Total) Comparison of Groups	9.19	< .0001***
1. Security Policies	32.06	< .0001***
2. Organization and Job Responsibilities	20.12	< .0001***
3. Education and Training	35.75	< .0001***
4. Technical Operations	19.00	< .0001***
5. Monitoring and Audit	8.38	0.0002***

Significant Level : ***p-value < 0.01, **p-value < 0.05, *p-value < 0.1.

〈Table 7〉 Means of Information Security Controls(by Leadership of Top Management)

Category	Security Policies	Organization and Job Responsibilities	Education and Training	Technical Operations	Monitoring and Audit
High (704 companies, 68.0%)	38.56	31.50	23.43	21.92	14.02
Medium (268 companies, 25.9%)	22.29	18.73	8.24	15.29	8.36
Low (63 companies, 6.1%)	18.25	15.23	3.96	13.47	6.57
Means	33.11	27.20	18.31	19.69	12.10

〈Table 8〉 Results of MANOVA(by Damage of Internet Incidents)

Category	F-value	p-value
(Total) Comparison of Groups	2.43	0.0070
1. Security Policies	0.06	0.9385
2. Organization and Job Responsibilities	2.68	0.0692*
3. Education and Training	1.40	0.2477
4. Technical Operations	0.19	0.8269
5. Monitoring and Audit	2.70	0.0680*

Significant Level : ***p-value < 0.01, **p-value < 0.05, *p-value < 0.1.

〈Table 9〉 Means of Information Security Controls(by Damage of Internet Incidents)

Category	Security Policies	Organization and Job Responsibilities	Education and Training	Technical Operations	Monitoring and Audit
No Frequency of damage (866 companies, 83.7%)	32.99	26.53	18.93	19.75	11.48
Medium Frequency of damage (89 companies, 8.6%)	33.14	34.83	16.62	18.67	13.48
High Frequency of damage (80 companies, 7.7%)	34.37	26.00	13.50	20.20	17.32
Means	33.11	27.20	18.31	19.69	12.10

반면에 피해빈도 그룹간에 정책수립 활동, 조직과 인력 구성, 정보보호 교육 및 훈련, 기술적 대책 활동, 모니터링 및 감사활동 등 5개 정보보호 통제활동은 유의수준 5%하에서 차이가 없는 것으로 나타났다. 다만, 유의수준 10%하에서 정보보호 조직과 인력 구성, 모니터링 및 감사활동만이 차이가 있는 것으로 나타났다(F-value 각각 2.68, 2.70). 이러한 차이는 최고경영층의 리더십 그룹에 비하면 아주 작음을 알 수 있다. 이는 <Table 9>의 실제 평균값을 통해서도 확인할 수 있다.

특히, 정보보호 조직과 인력 구성, 모니터링 및 감사활동 조차도 오히려 피해가 없는 기업이 정보보호활동이 낮은 것으로 나타나, 인터넷 침해사고 피해가 없는 조직이 그렇지 않은 조직에 비해 정보보호 통제활동이 활발하다는 가설은 입증되지 못함을 확인하였다. 오히려 피해빈도가 높은 기업이 정보보호 통제활동이 높은 것은 나타나 사고 이후에 정보보호 통제활동을 강화했을 가능성을 보인다. 즉, 정보보호 통제활동이 사고 후 대처방안으로 이루어졌을 가능성이 존재한다는 것이다. 이것에 대한 연구는 향후 과제로 남기고자 한다.

위와 같은 결과를 통해, 인터넷 침해사고 피해보다는 정보보호에 대한 최고경영층의 리더십이 조직내 정보보호 통제활동에 미치는 영향이 크다는 것을 알 수 있다. 따라서 조직내 정보보호 수준을 높이기 위해서는 정보보호에 대한 최고경영층의 리더십이 아주 중요하다고 할 수 있다.

〈Table 10〉 Result of Discriminant Analysis

Category	Standardized Canonical Coefficients of Canonical Function 1	Standardized Canonical Coefficients of Canonical Function 2
Security Policies	0.480	-1.002
Organization and Job Responsibilities	0.100	-0.029
Education and Training	0.574	0.557
Technical Operations	0.181	0.045
Monitoring and Audit	-0.112	0.773
% of Variance	99.97	0.03
Canonical Corelation Coefficient	0.289	0.004

이와 같은 결과에 대해 다른 관점에서 재확인하고, 정보보호에 대한 최고경영층의 리더십이 높은 그룹과 그렇지 않은 그룹간에 가장 공헌도가 높은 변수 찾고자 판별분석(Discriminant Analysis)을 실시하였다. 판별분석은 두 개 이상의 그룹을 구분하는데 가장 큰 공헌을 하는 요인을 찾고자 할 때 사용하는 통계적인 분석방법이고, 표준화에 의해 판별변수들의 상대적 공헌도를 분석하고자 할 때 표준정준계수(standardized canonical coefficient)를 활용한다[14].

<Table 10>에서 보는 바와 같이, 판별함수 1이 전체 분산에서 차지하는 비중은 99.97%로서 판별함수 2에 비해 월등히 높기 때문에 판별함수 1을 중심으로 분석을 해도 충분함을 알 수 있다.

최고경영층 리더십 그룹이 높은 그룹과 그렇지 않은 그룹을 분류하는 데에는 정보보호 교육 및 훈련(0.574), 정책수립활동(0.480)이 가장 큰 공헌을 하는 것으로 나타나, 앞선 MANOVA 분석과 동일한 결과를 확인할 수 있었다. 즉, 최고경영층의 리더십이 강하면 조직내 정보보호 통제활동 중에서 조직원에 대한 정보보호 교육 및 훈련, 정보보호 정책수립 활동이 상대적으로 크게 활발해 진다는 것을 의미한다.

5. 결 론

본 논문에서는 정보보호 거버넌스를 강조한 선행연구들을 바탕으로, 거버넌스 측면에서 가장 중요하게 판단하고 있는 최고경영층의 정보보호에 대한 리더십이 정보보호 정책수립, 정보보호 조직과 인력 구성, 정보보호 교육 및 훈련, 기술적 대책 활동, 모니터링 및 감사활동 등과 같은 정보보호 통제활동에 크게 영향을 준다는 것을 실증적으로 분석하였다. 반면에 본 논문의 분석결과, 조직 내 인터넷 침해사고 피해는 정보보호 통제활동에 직접적으로 유의한 영향을 주지 않는 것으로 나타났다.

본 연구가 가지는 의미는 다음과 같다. 첫째, Solms[2]이 제시한 정보보호 거버넌스의 순환 반복구조에서 정보보호에 대한 최고경영층의 약속과 리더십이 조직 내 실질적인

정보보호 통제활동으로 이어진다는 것을 실증적으로 보여주었다는 것이다. 따라서 조직 차원에서 정보보호 수준을 향상시키기 위해서는 최고경영층의 정보보호에 대한 리더십이 매우 중요하다는 것을 확인할 수 있었다. 이는 공공기관에서 최고경영층의 지원이 정보보호 거버넌스에 크게 영향을 미치고, 정보보호에 있어서 가장 중요한 요인임을 확인한 기존의 연구와도 일치하고[15], 기업의 경영진 사이에 정보보호를 중요시하는 문화가 강할수록 정보보호 규정에 대한 중요성 인식 결핍 등이 줄어든다는 기존 연구결과와도 일치한다[16].

둘째, 인터넷 침해사고 피해가 없는 조직이 정보보호 통제활동이 활발하다는 것을 의미하지는 않고, 오히려 침해사고가 발생한 조직들이 정보보호 통제활동이 더 활발한 모습도 보이고 있음을 알 수 있었다. 즉, 사고의 유무가 조직의 정보보호 수준을 말해주는 것은 아니고, 사고가 발생하지 않았기 때문에 현재의 정보보호 수준이 높고, 정보보호 통제활동도 충분하다고 생각하면 안된다는 것이다. 따라서 기업에서는 정보보호 거버넌스 차원에서 조직의 정보보호 수준을 높이는 꾸준한 활동을 통해 발생할 수 있는 피해를 최소화하는 것에 집중할 필요가 있다.

본 논문에서는 최고경영층의 정보보호에 대한 리더십에 따라 정보보호 통제활동에 차이가 있다는 것을 분석하였으나, 최고경영층의 정보보호에 대한 리더십과 침해사고 피해빈도, 정보보호 통제활동 간의 인과관계에 대해서는 제시하지 못하고 있다. 따라서 향후 연구는 조직 내 인터넷 침해사고 감소에 영향을 주는 요인을 탐색할 필요가 있고, 요인들간의 인과관계에 대해 살펴볼 필요가 있을 것으로 보인다. 또한 중소기업을 대상으로 조사하였기 때문에 대기업의 경우에는 어떻게 다른지에 대해서도 분석할 필요가 있을 것으로 보인다.

아울러 정보보호 거버넌스 측면에서 정보보호 성과에 대한 변수를 추가적으로 도출하여 성과에 영향을 미치는 요인들간의 연관성을 분석하는 것도 필요하다고 판단된다. 이를 위해 단편적인 cross-sectional 데이터 확보에서 벗어나 longitudinal 분석을 위한 데이터도 확보할 필요가 있다고 판단된다. 따라서 향후에는 관련 영역들의 범위를 확장하면서 추가적인 연구를 진행할 계획이다.

References

[1] ISO/IEC 27001, Information technology-Security techniques-Information security management systems-Requirements, 2005.

[2] Solms, Basie von, “Information Security-The Fourth Wave,” Computers and Security, Vol. 25, pp. 165-168, 2006.

[3] Veiga, A. D. and Eloff, J. H. P., “An Information Security Governance Framework,” Information System Management, Vol. 24, pp. 361-372, 2007.

[4] Wiant, T. L., “Information security policy’s impact on reporting security incidents,” Computers and Security, Vol. 24, No. 6, pp. 448-459, September 2005.

[5] Solms, Basie von, “Information Security-A Multidimensional Discipline,” Computers and Security, Vol. 20, pp. 504-508, 2001.

[6] Aron, J. L., Gove, R. A., Azadegan, S., and Schneider, M. C., “The Benefits of a Notification Process in Addressing the Worsening Computer Virus Problem : Results of a Survey and a Simulation Model,” Computers and Security, Vol. 20, No. 8, pp. 693-714, 2001.

[7] Wei, H., Frincke, D., Carter, O., and Ritter, C., “Cost-benefit analysis for network intrusion detection systems,” CSI 28th Annual Computer Security Conference, pp. 29-31 October, Washington DC, USA, 2001.

[8] Solms, Basie von, “Information Security Governance-Compliance management vs. operational Management,” Computers and Security, Vol. 24, No. 6, pp. 443-447, 2005.

[9] Vroom, C. and Von Solms, R., “Towards information security behavioural compliance,” Computers and Security, Vol. 23, No. 33, pp. 191-198, 2004.

[10] Caminada, M., Riet, R. V. D., Zanten, A. V., and Doorn, L. V., “Internet Security Incidents, a Survey Within Dutch Organizations,” Computers and Security, Vol. 17, No. 5, pp. 417-433, 1998.

[11] Joshi, K., “The measurement of fairness or equity perceptions of management information systems users,” MIS Quarterly, Vol. 13, No. 3, pp. 343-358, 1989.

[12] Choi, M. G., “An Exploring Study on Relation Between Maturity Levels of Organizations and Factors Affecting Information Security Policy,” Journal of Korean Academic Association of Business Administration, Vol. 22, No. 3, pp. 1729-1748, 2009.

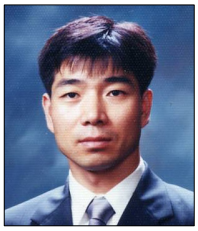
[13] Huh, M., Understanding of Statistical Consulting, Jayu Academy, 1993.

[14] Kim, K. and Chun, M., SAS Discriminant and Classification Analysis, Jayu Academy, 1990. 1.

[15] Song, J. S., Jeon, M. J., and Choi, M. G., “A Study on Factors Affecting the Level of Information Security Governance in Korea Government Institutions and Agencies,” The Journal of Society for e-Business Studies, Vol. 16, No. 1, pp. 133-151, 2011.

[16] Kim, H. J. and Ahn, J. H., “An Empirical Study of Employee’s Deviant Behavior for Improving Efficiency of Information Security Governance,” The Journal of Society for e-Business Studies, Vol. 18, No. 1, pp. 147-164, 2013.

저 자 소 개



유진호	(E-mail : jhyoo@smu.ac.kr)
1988년~1992년	고려대 이과대학 수학과 (이학사)
1992년~1994년	고려대 일반대학원 통계학과 (이학석사)
2006년~2010년	고려대 정보경영공학전문대학원 정보경영공학과 (공학박사) (세부전공 : 정보보호전공)
1993년~1999년	한국전자통신연구원(ETRI) 연구원
2000년~2004년	IBM Korea 차장 (CRM/데이터마이닝 컨설턴트)
2004년~2013년	한국인터넷진흥원(KISA) 인터넷문화진흥단장
2013년~현재	상명대학교 경영학과 조교수
관심분야	정보보호, 개인정보보호, MIS