情報保護學會論文誌
第18卷 第3號, 2008. 6

정보보호정책의 성숙도에 영향을 미치는 요인에 관한 연구*

최 명 길†, 황 원 주, 김 명 수††
인제대학교, 강원대학교††

An Empirical Study on Factors Affecting the Maturity of Information Security Policy*

Myeonggil Choi†, Won-Joo Hwang, Myoung-Soo Kim††
Inje University, Kangwon University

요 약

조직은 정보의 획득과 관리를 통하여 조직의 전략을 관철한다. 특히 기술과 같은 기업의 사활을 결정짓는 중요한 정보의 유출은 조직의 생존에도 영향을 미친다. 따라서 조직의 효과적인 정보보호관리를 위해서 정보보호관리체계 및 정보보호정책의 수립이 필요하다. 본 연구는 조직의 정보보호에 근간이 되는 정보보호정책의 성숙도에 영향을 미치는 요인을 문헌 연구를 통해서 분석하고, 정보보호정책의 성숙도에 영향을 미치는 요인을 검증한다. 본 연구는 정보보호정책의 수립과 정보보호수준 제고를 위한 연구의 이론적 토대를 제공한다. 본 연구의 결과는 국가 및 민간기관이 효과적으로 정보보호정책의 수립을 위한 방향성을 제시하고 있다.

ABSTRACT

Enterprises accomplish their missions through obtaining and managing information. The unintended disclose of enterprises' sensitive information causes serious damage to enterprises, resulting in disruptive management. For effective security of enterprises, information security management systems and information security policy owing clear goals should be firmly established. This study analyzes factors influencing maturity of information security policy. and gives important hints to execute information security policy

Keywords : Information Security Policy, Maturity, Factor Analysis

Ⅰ. 서 론

조직의 정보시스템에 대한 의존도가 급속히 증가하고 있지만, 정보자산에 대한 위협 대처에 많은 자원을 투자하지 못하고 있는 실정이다. 제한된 여건에서 체계적인 정보보호를 위해서는 조직은 정보보호정책의 확립이 필요하다.[12,22,24]. 정보보호정책은 조직의 정보보호의 목적, 원칙, 가이드라인 등을 서술한 문서이다. 정보보호정책은 조직 구성원의 부적절한 행동을 방지하고, 정보자산에 대한 위협과 공격에 대한 조직 구성원의 인식 제고에 기반이 된다. 따라서 조직의 적절한 정보보호정책 수립 및 실행은 조직의 내재적인 가치 및 경쟁

접수일 : 2008년 2월 18일; 채택일 : 2008년 3월 25일
* 본 논문은 2005년도 인제대학교 학술연구비 조성에 의한 것임
† 주저자: 現 중앙대학교 근무, mgchoi@cau.ac.kr.

력을 증가시키는 역할을 한다[21].

정보보호정책은 프로그램 정보보호정책(program policy), 특정사안중심 정보보호정책(issue specific policy), 시스템 정보보호정책(system specific policy) 등으로 구분된다.[5,28]. 프로그램 정보보호정책은 정보보호와 관련된 조직의 기본적인 정책 및 구조를 정의하고 있다. 프로그램 정보보호정책은 정보보호정책의 목적, 범위, 책임소재, 관련된 부서의 책임 등을 서술하고 있다. 특정사안중심 정보보호정책은 정보시스템 개발, 최신기술개발 계획 등과 같은 사안을 다루기 위해 필요한 기본적인 정책 방향을 서술한다. 일반적으로 3계층의 정보보호정책은 구분되지 않고, 단일의 정보보안정책이 존재한다. 본 연구의 대상이 되는 정보보호정책은 3계층의 특성을 포함하고 있다고 가정한다. 실무차원에서 정보보호정책의 중요성에 대한 많은 논의에도 불구하고, 정보보호정책이 포함해야 할 항목, 정보보호정책을 형성을 촉진하는 원인, 정보보호정책이 정보보호수준 제고에 미치는 효과 등을 다루고 있는 연구가 부족하다. 저자는 부족한 원인을 산업적인 필요성, 연구자의 소극적인 태도, 정부의 정책 방향과 밀접한 관련이 있다고 판단한다.

효과적인 정보보호체계를 구축하기 위해서는 정보보호의 목적과 목표를 명확히 정의한 정보보호정책이 필수적이다[18]. Higgins는 "정보보호정책은 정보보호체계의 시작이다"라고 주장하고 있다[12].정보보호정책의 효과적인 수립은 효과적인 정보보호체계를 구축할 수 있게 한다. 조직의 목적에 맞지 않는 정보보호정책은 정보보호체계 확립시에 많은 비용을 수반하고, 효과적이지 못하다[19].

정보보호정책은 정보보호의 목적, 방향, 범위, 규칙 등을 정의하고, 조직의 정보보호에 대한 궁극적인 방향을 제시한다. 정보보호정책은 조직의 임무 수행에 있어서 경제성과 효율성을 향상시키며, 경영층의 지원 확인, 정책들 간의 마찰 최소화, 직원들의 책임 회피 방지, 감사의 참고 자료 활용된다[1,2,10,28]. 본 연구는 정보보호정책 프로세스, 정보보호정책의 대상이 되는 정보자산의 통제 범위, 정보보호정책에 대한 관리 등의 관점에서 정보보호정책의 성숙도를 정의하고자 한다.

정보보호정책은 정보보호대책 및 기술적 정보보호대책의 명세를 정의한 정보보호지침 및 규칙을 서술한 문서이다[16,17]. 정보보호정책은 보호대상이 되는 정보자산을 정의하고, 정의된 정보자산의 보호를 위한 보호대책을 명시한다[8,9]. 정보기술과 정보환경은 지속적으로 변화한다. 따라서 조직은 정보기술 및 정보환경의 변화에 대처할 수 있는 유연한 정보보호정책을 가지고 있어야 한다[3]. 정보보호정책은 정보기술의 변화를 즉각적으로 반영하는 절차 및 주체를 정의해야 한다. 즉 정보보호정책은 유연한 정보보호갱신 절차, 방법 및 주체를 명확하게 서술해야 한다. 본 연구는 위에서 언급한 관점을 기준으로 정보보호정책이 포함하고 있어야 할 항목을 식별하고, 식별된 항목의 구비 정도를 정보보호정책의 성숙도라고 정의한다. 본 연구는 정보보호정책의 성숙도를 측정하고, 성숙도에 미치는 요인을 제시한다. 본 연구는 정보보호정책의 성숙도에 미치는 요인을 식별하기 위해서 기존의 문헌으로부터 요인을 식별하고, 다양한 기관을 대상으로 설문을 실시하고, 획득된 데이터를 활용하여 요인을 분석한다. 본 연구는 정보보호정책의 성숙도에 최종적으로 영향을 미치는 요인을 탐색하고, 정보보호정책의 성숙도에 영향을 미치는 요인을 회귀 분석을 통해서 검증한다.

Ⅱ. 이론적 배경

정보보호정책과 관련된 선행 연구를 살펴보자. 정보보호정책 연구는 세 가지로 나눌 수 있다. 첫째, 정보보호정책 정의 및 역할을 이론적으로 고찰하는 연구, 둘째, 정보보호정책의 내용을 실증적으로 조사한 연구, 셋째, 정보보호정책의 형성에 미치는 요인을 탐색한 연구 등이 있다.

2.1 정보보호정책의 정의 및 역할 연구

정보보호정책 정의 및 역할을 이론적으로 고찰한 연구로는 Hone and Eloff[13], Higgins[12], Baskerville et al.[3], T.L.Wiant[26] 등의 연구가 있다. Higgins는 "정보보호정책은 정보보호의 출발"이라고 정의하고 있으며, Hone and Eloff은 "정보보호정책은 정보보호에 있어서 가장 중요한 통제수단"이라고 언급하고 있다. Baskerville[3] and Siponenn[21]는 정보보호정책은 조직의 정보보호의 기초임을 강조하면서 효과적인 정보보호정책 개발을 위해 필요한 방법과 관련된 연구의 부재(不在)를 지적하면서, 정보보호정책 개발 방법론을 서술하고 있다. T.L.Wiant는 정보보호정책의 역할을 억제이론(deterrence theory)를 채용하여 설명하고 있다[26].

동 연구는 정보보호정책의 존재 효과를 컴퓨터에 침해하는 제3자에게 정보보호정책을 어기면 반드시 처벌받을 수 있다는 경각심을 심어준다는 것이다. 따라서 동 연구는 성문화된 정보보호정책이 컴퓨터 침해자에게 경각심을 준다는 점에서 비성문화된 정보보호정책보다 효과적이라고 주장한다.

2.2 정보보호정책의 내용 연구

정보보호정책의 내용을 실증적으로 조사한 연구로는 Fulford et al[9], BS7799[5], Whitman et al.[27] 등이 있다. 정보보호정책이 포함해야 할 항목에 대한 실증 연구는 많이 수행되지 않았고, 주로 정보보호지침 및 표준 등의 실무위주의 결과물을 고찰하고 있다. Fulford et al.는 정보보호정책이 포함해야 하는 항목을 실증적으로 조사하여 제시하고 있다. Fulford et al.연구는 정보보호정책이 포함해야 할 통제항목으로 시스템 통제, 인터넷 접근, 암호화, 비상계획, 물리적 보안 등 약 11개를 제시하고 있다. BS7799는 정보보호관리가 포함해야 하는 통제항목을 가장 폭넓게 정의하고 있고, 정보보호정책이 명시해야 할 항목의 대부분을 서술하고 있다. BS7799는 정책의 문서화, 인적 보안, 자산의 분류 및 통제, 접근통제 등 10개 분야의 통제 항목을 제시하고 있다. Whitman and Mattford은 정보보호정책은 조직의 임무(mission), 목적(goal)과 기업의 정보보호전략에 대한 경영층의 의지를 서술해야 한다고 주장한다.

2.3 정보보호정책 형성에 영향을 미치는 요인 연구

정보보호정책의 형성에 영향을 미치는 요인을 탐색하는 연구로는 Karydy et al[16,17], Heather Fulford et al[9] 등이 있다. Kardy et al의 연구는 정보보호정책의 형성(formulation), 이행(implementation), 및 수용(adoption)에 영향을 미치는 요인을 사례 연구를 통해서 분석하고 있다. Kardye et al.은 정보보호정책을 조직에 적용할 때, 영향을 미치는 요인으로 유연한 조직 구조(organizational structure), 모든 구성원이 공유하는 일관된 조직 문화(coherent organizational culture), 정보보호정책의 수용을 지원하는 적극적인 경영층의 지원(management support), 정보보호정책을 조직에 성공적으로 정착시킬 수 있는 자질을 갖춘 정보보호관리자의 역할(the role of the security office), 정보보호정책에 대한 지속적인 훈련 및 교육(training and edu- cation), 구성원의 업무에 대한 정보보호정책의 기여도 (contribution to user's goal) 및 사용자의 참여 (users' participation) 등을 제시하고 있다. Fulford는 정보보호정책의 형성에 있어서 미치는 요인으로 경영층의 명확한 지원, 정보위험에 대한 명확한 이해, 조직구성원에게 IT 정보보호정책의 배포, 정보보호요구사항에 대한 명확한 이해, 모든 구성원을 대상으로 정보보호 홍보, 적절한 구성원 훈련 및 교육, 업무 목표에 영향을 미치는 정보보호정책 담보, 조직의 문화와 일치하는 정보보호대책을 구현하는 접근법, 정보보호관리를 측정할 수 있는 시스템, 종업원의 정보보호정책의 개선에 대한 참여 등을 제시하고 있다.

Ⅲ. 정보보호정책의 성숙도 요인 모형

R.C.Beatty, et. al.[4]은 웹 수용에 미치는 요인을 기술적인 측면, 조직적인 측면, 경제적인 측면, 관리적인 측면으로 나누어 제시하고 있다. 동 연구는 정보기술에 수용에 있어서 영향을 미치는 유용한 분석 프레임웍을 제시하고 있다. 따라서 본 연구는 분석 프레임웍을 활용하여 정보보호정책의 성숙도에 영향을 미치는 요인을 조직적 관점, 관리적 관점, 경제적 관점에서 도출한다.

본 연구는 관리적 관점, 조직적 관점에서 Karydy et al, Heather Fulford et al의 연구 결과를 바탕으로 정보보호정채의 성숙도에 영향을 미치는 요인을 도출한다. 본 연구는 Karydy et al, Heather Fulford et al의 연구 결과를 활용하여 최고 경영층의 지원[14,15,20],조직성과 개선[3], 정보보호정책과 조직 기술과의 조화[6], 정보보호정책과 조직특성과의 조화[16], 정보보호정책 수립 난이도에 대한 조직 구성원의 인식[7] 등의 요인을 도출한다. 본 연구는 R.C.Beatty, et. al.의 연구 결과를 바탕으로 경제적 관점과 관련된 요인인 '조직성과개선에 대한 인식'[7] 을 도출한다. [표 1]은 연구에 사용된 요인별 측정 항목과 방법을 서술하고 있으며, [그림 1]은 정보보호정책의 성숙도에 영향을 미치는 5가지 요인과의 관계를 표시한다.

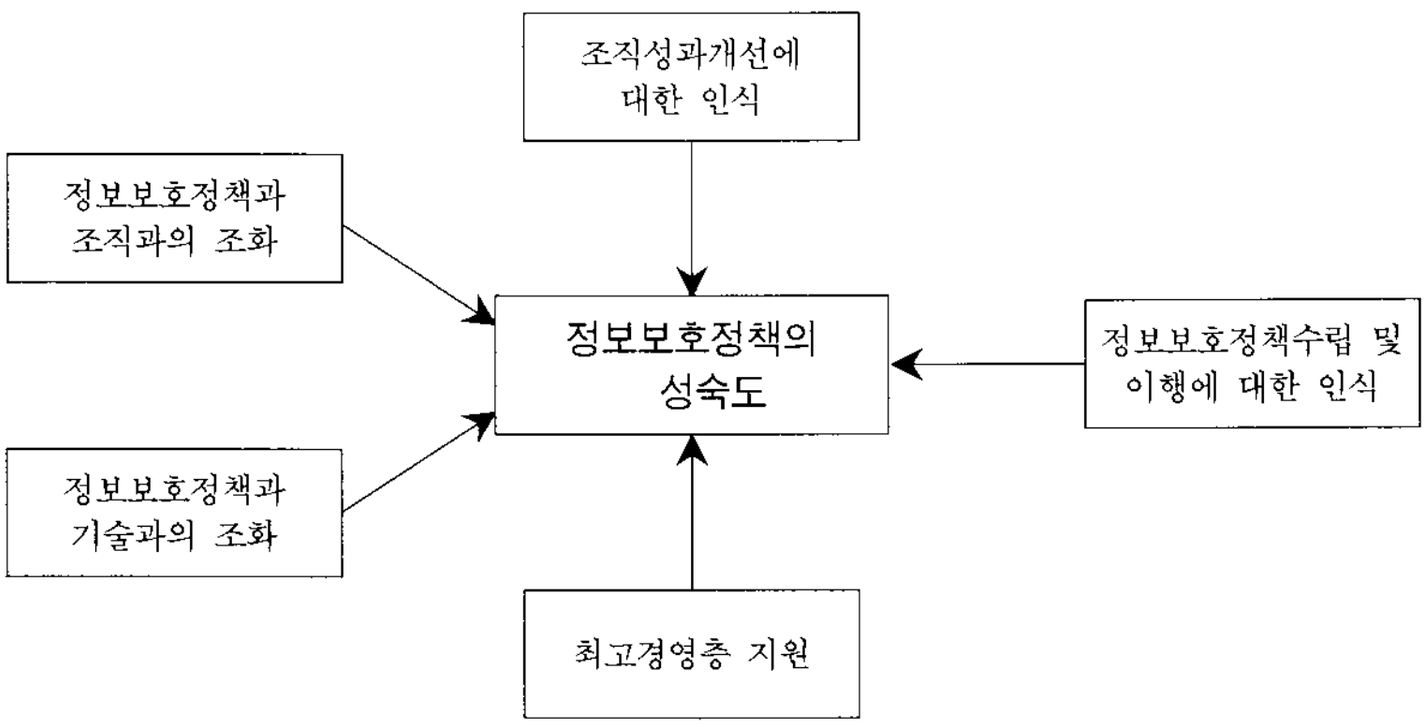
3.1 조직 성과 개선에 대한 인식

조직은 새로운 제도가 성과를 개선할 수 있다고 인식하면 새로운 제도를 도입하려고 한다. 조직이 정보보호

〔표 1〕 요인별 측정항목 및 평가방법

변 수	평가 방법	Cronbach 상관계수 α
최고 경영층의 지원	3개항목의 평균값	0.93
정보보호정책과 조직과의 조화	6개항목의 평균값	0.91
정보보호정책과 기술과의 조화	4개항목의 평균값	0.71
정보보호정책 수립 난이도에 대한 구성원의 인식	2개항목의 평균값	N/Aa
조직성과개선에 대한 인식	5개항목의 평균값	0.85

aN/A : 두개의 항목에 대한 Cronbach 상관계수는 의미가 없으므로 상관계수 α 값을 계산하지 않음.



〔그림 1〕 정보보호정책 요인 모델

정책의 수립을 통해 업무수행 비용 감소, 효율성 증가, 향상된 서비스 제공, 조직의 신뢰성 및 경쟁력 증가, 기존의 문제 해결, 새로운 사업 기회 획득 가능성 증가 등이 예상하면, 정보보호정책을 적극적으로 도입할 것이다[4,25]. 따라서 조직성과개선에 대한 인식이 높은 조직은 성숙도가 높은 정보보호정책을 수립할 것이라 예상할 수 있다.

3.2 정보보호정책과 조직과 조화

정보보호정책에 대한 구성원의 우호적인 태도, 조직의 특성을 반영한 정보보호정책은 정보보호정책의 수립에 도움이 될 수 있다[9,16]

정보보호정책과 조직과의 조화는 성공적인 정보보호정책 수립 및 이행을 위한 촉진제가 될 수 있다. 조직 구성원이 정보보호정책과 조직 문화, 가치, 기존의 업무 형태 및 정보시스템 기반구조와 일관성 있게 조화된다고 인식하면, 조직은 성숙도가 높은 정보보호정책을 수립할 가능성이 높을 것이다[11,23]. 조직이 정보보호정책을 수립하면 정보보호정책의 정착을 위해서 기존의 업무 방식을 개선하고, 정보보호정책과 조직과 조화를 위한 노력을 해야 한다. 이 요인은 조직이 성숙도가 높은 정보보호정책을 수립하는데 중요한 결정변수로 작용할 수 있다. 조직이 성숙도가 높은 정보보호정책을 수립할 경우, 조직 문화, 업무 관습 등에 긍정적인 영향을 미친다. 따라서 조직의 문화적 규범, 업무 및 사업 관행에 적합한 정보보호정책 수립하는 조직은 높은 성숙도를 가진 정보보호정책을 수립할 수 있다.

3.3 정보보호정책과 기술과의 조화

정보보호정책의 수립은 하드웨어, 소프트웨어, 네트워킹 또는 통신 아키텍쳐와 같은 기존 정보시스템의 기술적 환경과 관련성이 있다[6]. 만약 정보보호정책이 정보시스템의 기술적 환경과 조화가 될 수 없다면 정보보호정책의 도입은 현실적으로 어렵다. 성숙도가 높은 정보보호정책의 수립을 위해서는 조직은 기존의 정보시스템의 기술적 인프라, 구성 및 운영 방식을 변경해야 하며, 정보보호정책 도입으로 인해 현재 또는 미래에 예상되는 업무 방식의 변화를 평가해야 한다. 대부분의 최고경영자들은 새로운 정보보호정책을 수립하는 것은 기존의 IT 인프라의 많은 변경이 필요하고, 구성원들의 적

응을 위해서 많은 시간이 소요된다는 인식이 있어서 정보보호정책의 도입을 꺼리는 경향이 있다. 하지만 조직 인프라의 환경을 반영한 정보보호정책을 수립할 수 있는 조직은 성숙도가 높은 정보보호정책을 수립할 가능성이 높다.

3.4 정보보호정책 수립 및 이행에 대한 구성원 인식

조직의 구성원이 정보보호정책을 올바로 이해하고, 수립, 집행, 평가하는 것은 중요한 문제이다. 새로운 기술과 제도의 도입은 언제나 조직 구성원들에게는 부담이다. 특히 기술이 구성원으로 하여금 지금까지 수행했던 업무 및 사업 방식을 변화시키고, 현재까지 접해보지 못한 새로운 기술을 익힐 것을 요구하면 구성원의 부담은 가중될 수 있다[7,29]. 조직 구성원은 정보보호정책이 업무 및 근무 환경을 더 어렵게 할 수 있을 것이라 인식할 수 있다. 정보보호정책은 조직의 구성원에게 높은 수준의 신기술을 요구할 수 있음으로 조직 구성원은 정보보호정책에 대하여 부정적인 인식을 가질 수 있다.

3.5 최고 경영층 지원

조직의 정보보호수준 향상에 필요한 많은 요인이 존재하지만 가장 중요한 요인은 최고 경영자의 정보보호에 대한 지원이다[14,15,20]. 최고 경영자의 지원은 정신적, 경제적, 물리적인 모든 측면을 포함한다. 많은 연구결과에서 최고 경영자의 적극적인 지원은 새로운 기술과 제도의 도입 또는 좋은 정책 개발의 성공 여부를 예측할 수 있는 척도라고 언급되고 있다[4]. 정보보호도 최고경영자의 적극적이고 효과적인 지원 없이는 정보보호정책 수립이 불가능할 수 있다.

Ⅳ. 연구방법론

4.1 설문항목구성

본 연구는 사용한 설문은 조직의 정보보호정책 성숙도와 5가지 요인(factor)과의 상관관계 측정을 위해서 두개의 영역으로 구분된다. 설문의 타당성, 객관성 및 범용성을 유지하기 위해서 관련 연구, 자료, 실무에서 활용중인 정보보호지침서를 참조하였다.

첫째, 조직의 정보보호정책의 성숙도 측정을 위해서 총10개 항목을 사용하였다. 본 논문은 정보보호정책 수립에 영향을 미치는 요인을 분석할 목적으로 10개의 항목을 BS 7799의 10개의 정보보호 통제항목과 국방부가 사용하는"군사보안업무시행규칙"에서 추출하였다. BS7799가 제시하는 통제항목들은 조직의 정보보호를 위해 고려해야 하는 중요한 요소들을 포함하고 있다[5]. "군사보안업무시행규칙"은 현재 군의 전반적인 보안업무의 목적과 방향, 업무 처리절차, 준수사항 등을 정리한 보안정책서이다. 이 지침서는 보안정책을 9개의 분야로 나누어 제시하고 있다. 본 연구는 위의 문서에서 추출한 [표 2]와 같은 10개의 설문항목을 작성하여 정보보호정책의 성숙도를 측정한다. 측정을 위해서 설문지는 5점 척도를 사용하였다.

둘째는, 조직의 성숙한 정보보호정책 수립에 영향을 미치는 5가지 요인 분석을 위해 20개의 항목으로 구성된 설문을 조사했다. 일반적으로 정보보호정책의 성숙도가 높은 조직은 5개의 요인에서 높은 점수를 획득할 것이다. 본 연구의 설문은 IS(information systems) 조직의 정보보호관리자를 대상으로 수행하였다.

〔표 2〕 BS 7799와 군사보안업무시행규칙의 통제항목에서 추출한 설문 항목 분류

설문번호	BS 7799	군사 보안업무시행규칙
1	(1) 정책의 문서화	규칙의 문서화
2, 3	(2) 전담 인원 및 조직 존재	전담 책임관 및 부서 존재
4	(3) 자산의 분류 및 통제	문서 보안
5	(4) 인적 보안	인원 보안
6	(5) 물리적 환경적 정보보호	시설 보안
7	(6),(8) 시스템 운영관리 및 유지	컴퓨터시스템 보안대책
8	(7) 접근통제	인터넷 보안대책
9	(10) 준수 관리	보안업무 운영(교육)
10	(9) 업무 지속성 관리	보안업무 운영(긴급복구대책)

4.2. 설문 응답자 구성

본 연구는 다양한 산업 전반의 정보보호정책을 비교·분석을 위해 교육 기관, 연구 기관, IT 제조업, 통신 회사, 보안 회사, 공공 기관, 군 등을 대상으로 설문을 조사하였다. 전체 500부의 설문지를 이메일을 사용하여 발송하였고, 56개의 설문지를 회수하였다. 설문 응답율은 12%를 보였다. [표 3]은 설문 응답자의 구성이다.

정보보호정책의 성숙도를 측정하는 항목을 기준으로 정보보호정책의 성숙도의 점수를 측정하였다. 응답된 설문 결과 중 해당 항목이 전무한 조직은 분석 대상에서 제외하였다.

〔표 3〕 설문 응답자 구성

조직 유형	응답자	분포
학교/연구소	9	16
제조/통신회사	11	20
IT 제조업	18	32
공공기관/군	18	32
	56	100

V. 정보보호정책 성숙도 분석

5.1 요인분석

본 연구는 성숙도가 높은 정보보호정책 수립에 영향을 미치는 요인을 분석하기 위해 20가지의 항목을 채용하였다. 먼저 항목간의 적절성을 우선적으로 검증해야 한다[4]. 예를 들어, 1개의 항목이 한 요인에 영향을 받지 않고 여러 요인에 영향을 받을 수 있어 요인의 독립성에 대한 검증이 필요하다. 이 검증은 각 요인이 설문에 잘 반영되었는지에 대한 척도가 됨으로 요인의 타당성 검정을 위해 중요하다. [표 4]는 본 연구가 고려한 정보보호정책의 성숙도에 영향을 미치는 5가지 요인과 이를 반영하는 항목을 그룹화한 것이다. 항목간의 상관관계를 분석하면 각 항목이 요인에 의해서 적절히 그룹화 되었는지 확인할 수 있다. 예를 들면, 같은 요인을 반영하는 항목은 서로 강한 상관관계를 가지고 있으며 그 외의 요인을 반영하는 항목과는 상관관계가 약할 것으로 예상할 수 있다. [표 5]는 항목간의 상관관계행렬이다.

〔표 4〕 요인과 항목

요인	항목	LABEL
최고 경영층의 지원	정보보호에 대한 최고 경영층의 관심	TMS1
	정보보호정책의 중요성에 대한 최고 경영자의 인식	TMS2
	정보보호정책에 대한 경영층의 효과적인 지원	TMS3
정보보호정책과 조직과 조화	조직의 가치와 문화에 어울리는 정보보호정책 수립 방식	OC1
	정보보호정책에 대한 구성원들의 우호적인 태도	OC2
	정보보호정책에 따른 업무환경 악화	OC3
	정보보호정책수행에 따른 업무처리절차 변경	OC4
	정보보호정책에 따른 생산성 저하	OC5
	조직의 사업 목적을 반영하는 정보보호정책	OC6
정보보호정책과 기술적 조화	IT 인프라와 정보보호정책 간의 조화	TI1
	정보보호정책과 조직의 정보자원과의 조화	TI2
	조직의 정보보호 요구사항에 대한 정확한 인식	TI3
	정보보호정책에 따른 적응기간 소요	TI4
정보보호정책의 수립 및 이행에 대한 인식	정보보호정책은 절차의 복잡성이 증가할 것이라는 조직의 인식	COM1
	정보보호정책 개발의 어려움에 대한 조직의 인식	COM2
조직성과 개선에 대한 인식	정보보호정책수행에 따른 조직의 업무수행 비용 감소	PB1
	정보보호정책수행에 따른 조직의 향상된 서비스 제공	PB2
	정보보호정책수행에 따른 조직의 경쟁력 향상	PB3
	정보보호정책수행에 따른 조직의 신뢰성 증가	PB4
	정보보호정책수행에 따른 조직의 업무효율성 향상	PB5

〔표 5〕 항목간의 상관관계 행렬

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	1.00																			
2	0.90	1.00																		
3	0.73	0.77	1.00																	
4	0.54	0.59	0.68	1.00																
5	0.47	0.53	0.47	0.53	1.00															
6	0.62	0.63	0.67	0.72	0.36	1.00														
7	0.62	0.67	0.69	0.79	0.37	0.89	1.00													
8	0.49	0.61	0.63	0.71	0.43	0.76	0.74	1.00												
9	0.57	0.66	0.68	0.77	0.45	0.66	0.73	0.73	1.00											
10	-0.01	-0.07	-0.23	-0.31	-0.3	-0.01	-0.19	-0.12	-0.3	1.00										
11	0.44	0.33	0.23	0.09	0.12	0.11	0.17	0.08	0.19	0.05	1.00									
12	0.49	-0.09	-0.12	-0.27	-0.23	0.01	-0.12	-0.05	-0.1	0.55	0.22	1.00								
13	-0.2	-0.28	-0.22	-0.17	-0.01	-0.15	-0.16	-0.25	-0.22	0.2	0.1	0.35	1.00							
14	-0.51	-0.60	-0.57	-0.51	-0.53	-0.51	-0.54	-0.43	-0.47	0.42	-0.05	0.54	0.4	1.00						
15	-0.14	-0.17	0.03	-0.09	-0.07	-0.03	-0.13	0.05	-0.05	0.13	-0.23	0.22	0.05	0.23	1.00					
16	0.16	0.21	0.25	0.26	0.15	0.22	0.26	0.03	0.21	-0.38	-0.02	-0.39	-0.1	-0.27	-0.23	1.00				
17	0.04	0315	-0.05	0.2	0.17	0.12	0.17	0.23	0.24	-0.41	-0.05	-0.23	-0.18	-0.17	-0.43	0.36	1.00			
18	0.25	0.34	0.11	0.43	0.3	0.27	0..2	0.38	0.47	-0.38	-0.04	-0.22	-0.27	-0.27	-0.3	0.29	0.73	1.00		
19	0.23	0.29	0.23	0.45	0.19	0.36	0.41	0.39	0.5	-0.37	-0.13	-0.14	-0.14	-0.27	-0.12	0.17	0.51	0.68	1.00	
20	0.33	0.4	0.36	0.47	0.24	0.4	0.47	0.4	0.53	-0.47	0.06	-0.21	-0.24	-0.25	-0.31	0.47	0.64	0.71	0.48	1

질문1-3 : TMS1-TMS3, 질문4-9 : OC1-OC6, 질문10-13 : TI1-TI4, 질문14-15 : COM1-COM2,질문16-20 : PB1-PB5,
질문은 5점 척도로 계산되었다. (1 : 매우 그렇지 않다 2 : 그렇지 않다 3 : 보통이다 4 : 그렇다 5 : 매우 그렇다)

[표 5]가 나타내듯이 '최고 경영층의 지원'과 관련된 항목 1-3 간은 상관관계가 매우 강하다. 이 항목은 '정보보호정책과 조직과 조화'에 관한 항목 4-9와도 강한 상관관계를 가진다. 따라서 처음에 예상한 바와 달리 이 두 요인은 독립적이지 않고 강한 상관관계를 가진다. 이 항목은 그 외의 요인과는 강한 상관관계를 가지지 않는다. 상관관계행렬을 보면 '조직성과개선에 대한 인식'에 관한 항목 16-20사이에도 강한 상관관계가 존재한다. 항목 16과 다른 항목과는 상관관계가 다소 약하지만 전체적으로 볼 때 요인에 따른 그룹화가 어느 정도 되어있다.

'정보보호정책과 기술적 조화'에 관한 항목인 10-13을 보면 항목들 사이에는 강한 상관관계를 가지고 있다고 보기는 어려우며, 항목10과 12만이 강한 상관관계를 가지고 있다. 특히 항목 11은 다른 모든 항목과 강한 상관관계를 가지고 있지 않다. 이들의 상관관계가 약한 것은 이 요인을 나타내는 항목들의 그룹화가 잘 되어 있지 않을 가능성이 있기 때문이다. 더불어, '정보보호정책의 수립 및 이행에 대한 구성원의 인식'에 관한 항목들은 서로 상관관계가 약하다. 항목 14의 경우 '정보보호정책과 기술적 조화'에 관한 항목인 항목10과 12와 강한 상관관계를 가진다. 따라서 몇 가지 항목들에서 그룹화가 잘 되어 있지 않을 가능성이 있어, 효과적인 항목의 그룹화를 위해서는 좀 더 효과적인 방법을 이용해야 할 필요가 있다. 인간의 인식과 기호는 매우 복잡함으로 이를 측정하는 것은 어려움으로 상관관계 행렬이 나타낼 수 없는 관계가 존재할 가능성이 있다[4].

요인분석방법은 요인의 타당성을 측정하기 위한 좋은 방법이다. 요인분석은 변수간의 상관관계를 이용하여 여러 변수들을 측정한 자료를 소수의 차원으로 묶어서 새로운 변수로 묶는 방법으로 변수간의 구조를 파악할 수 있는 방법이다. 이 방법은 항목간의 구조를 파악하고, 그룹화 된 항목이 어떠한 요인을 반영하고 있는지를 확인하는데 유용한 방법이다.

본 연구는 항목간의 구조를 파악하기 위해 VARIMAX 변환을 이용한 주성분분석을 적용한다. 각 항목

의 그룹화 정도를 측정하기 위해서 요인부하(factor loading)을 관찰하였으며, factor loading > 0.5를 기준으로 관련된 항목을 그룹화 하였다. 하나의 항목이 그룹화된 집단 이외의 요인에서 factor loading > 0.4일 경우 각 항목이 독립적으로 하나의 요인에만 포함되지 않다고 판단하여 모델에서 제거하였다.

첫 번째 요인분석 결과, 전체 항목은 4개의 요인으로 그룹화 되었다. TMS1-TMS3가 하나의 그룹으로 그룹화 되었고, OC1-OC6도 동일한 그룹으로 분류되었다. 이 결과는 [표 6]의 상관관계 행렬에서 예상된 결과로 최고 경영층의 마인드가 조직 문화와 조직에 크게 영향을 미친다는 사실을 고려할 때 타당하다. 결과적으로 본 연구는 '정보보호정책과 조직과의 조화'와 '최고 경영층의 지원'이라는 2개의 요인을 1개의 요인으로 간주하여 '정보보호정책에 대한 조직의 지원'으로 명명하였다. '정보보호정책의 수립 및 이행에 대한 조직의 지원'은 최고 경영층의 지원뿐만 아니라 조직 전 구성원의 관심과 지원이 정보보호정책의 성숙도에 큰 영향을 미친다는 의미이다.

PB1-PB5은 PB1을 제외하고 하나의 요인에 의해서 그룹화 되었다. 즉 '조직성과개선에 대한 인식'요인과 이 요인을 반영하는 항목이 적절히 그룹화 되었고, 하나의 독립적인 요인으로 존재한다고 의미한다. 이 결과는 상관관계행렬에서도 확인되었다.

'IT인프라와 정보보호정책간의 조화(TI1)', '조직의 정보보호요구사항에 대한 정확한 인식(TI3)' 및 '정보보호정책에 따른 적응기간 소요(TI4)' 및 '정보보호정책에 따른 조직의 업무수행 비용 감소(PB1)'은 세번째 요인으로 구성되었다.

'정보보호정책과 조직의 정보자원과의 조화(TI2)' 및 '정보보호정책 개발의 어려움에 대한 조직의 인식(COM2)' 등은 세 번째 요인이 되었다. 다만 '정보보호정책에 따른 조직의 업무수행 비용 감소(PB1)'라는 항목이 포함된 것은 업무수행을 정보보호와 관련된 업무수행으로 해석되어, 설문 응답자는 기술과 조화된 정보보호정책의 수립은 정보보호와 관련된 업무수행 비용의

〔표 6〕 요인 분석 결과[a]

Label	질문	조직차원의 지원 7.41(42%)	성과개선에 대한 인식 2.93(16%)	기술적 조화 2.5(14%)	복잡성 1.4(7%)
TMS1	정보보호에 대한 최고 경영자의 관심	0.77			
TMS2	정보보호정책수행의 중요성에 대한 최고 경영자의 인식	0.80			
TMS3	정보보호정책수행에 대한 경영층의 효과적인 지원	0.87			
OC1	조직의 가치와 문화에 어울리는 정보보호정책 수립 방식	0.82			
OC2	정보보호정책에 대한 구성원들의 우호적인 태도	0.56			
OC3	정보보호정책에 따른 업무환경 악화	0.86			
OC4	정보보호정책에 따른 업무처리절차 변경	0.85			
OC5	정보보호정책에 따른 생산성 저하	0.82			
OC6	조직의 사업 목적을 반영하는 정보보호정책	0.81			
PB2	정보보호정책수행에 따른 조직의 향상된 서비스 제공		0.86		
PB3	정보보호정책수행에 따른 조직의 경쟁력 향상		0.86		
PB4	정보보호정책수행에 따른 조직의 신뢰성 증가		0.72		
PB5	정보보호정책수행에 따른 조직의 업무효율성 향상		0.70		
TI1	IT 인프라와 정보보호정책간의 조화			0.76	
TI3	조직의 정보보호 요구사항에 대한 정확한 인식			0.83	
TI4	정보보호정책수행에 따른 적응기간 소요			0.92	
PB1	정보보호정책수행에 따른 조직의 업무수행 비용 감소			0.63	
TI2	정보보호정책과 정보자원과의 조화				0.75
COM2	정보보호정책 개발의 어려움에 대한 조직의 인식				0.7

a 각 요인들의 아래에 적혀있는 값들은 eigenvalue와 요인에 의해 발생한 분산을 의미

감소로 인식한 것 같다.

이 중에서 정보보호정책은 절차의 복잡성이 증가할 것이라는 조직의 인식(COM1)은 첫 번째 요인과 세 번째 요인에 중복되어 적재되어 두 번째 요인분석에서는 제외되었다. COM1을 제거한 후, 다시 요인 분석을 수행하였다. 수행 결과 여전히 4개의 요인으로 각 질문들이 그룹화 되었고, 각 그룹에 속한 요인들에는 변화가 발생하지 않았다. 또한 중복 적재된 질문이 존재하지 않아 요인 분석을 종료하였다. 최종적으로 19개의 질문이 4개의 독립적인 요인으로 그룹화 되었다.([표 6] 참조)

요인분석 과정에서 제거된 질문을 살펴보면 설문자의 인식에 대한 새로운 의미를 발견할 수 있다. '정보보호정책에 따른 절차의 복잡성이 증가(COM1)'의 경우 '조직성과개선에 대한 인식'과 '기술적 조화'에 중복 적재되었는데, 이는 업무환경의 악화는 직접적으로 조직성과와 기술과 조직의 조화에 영향을 미친다는 것을 고려할 때 타당한 결과로 해석된다.

5.2 회귀분석

요인분석 결과에 따라 앞에서 선정한 5개의 요인을 4개의 요인으로 재구성하였다. 그 과정에서'최고 경영층의 지원'과 '조직성과의 조화'를 묶여서 '조직차원의 지원'으로 조정하였고, '기술적 조화'와 '복잡성'이 재그룹화 되었다. 이렇게 결정된 요인과 조직의 정보보호정책의 성숙도에 미치는 영향을 검정하기 위해서 중회귀분석(multiple regression analysis)를 사용한다. 중회귀분석에서 독립변수는 위에서 도출된 네 개의 요인을 사용하였고, 종속변수는 조직의 정보보보정책의 성숙도 측정값을 적용하였다.

네 개의 요인이 정보보호정책의 성숙도에 영향을 미치는 것을 검증하는 도구인 중회귀분석 모형의 타당성을 먼저 검증하는 분산분석(ANOVA)을 유의확률 0.05 수준에서 검증하면 F값은 5.49, 유의확률은 0.000이다. 따라서 정보보호정책의 성숙도를 설명하기 위해서 도입한 '정보보호정책에 대한 조직의 지원', '성과개선에 대한 인식', '정보보호정책과 기술과의 조화', '정보보호정책의 수립 및 이행에 대한 구성원의 인식' 등이 독립변수로 도입한 이 회귀모형은 유의하다.

각 요인들이 정보보호정책의 성숙도에 영향을 미치는지의 여부를 중회귀모형에서 검증해야 한다. 개별 요인이 정보보호정책의 성숙도에 영향을 미치는지의 여부

〔표 7〕 중회귀분석

검정 대상	t	유의확률
조직차원의 지원	4.043	0.000
성과개선에 대한 인식	1.380	0.174
기술적 조화	1.386	0.172
복잡성	0.665	0.509

는 유의확률 0.05 수준에서 검정할 때, 유의확률이 0.05 이하이면 유의하다. 따라서 [표 7]에 의하면 '정보보호정책의 수립 및 이행에 대한 조직의 지원'만 중회귀분석모형에서 유의하다. 따라서 '정보보호정책에 대한 조직의 지원' 요인만 정보보호정책의 성숙도에 영향을 미친다고 할 수 있다. 이 점이 시사하는 바는 정보보호정책의 성숙도는 정보보호정책과 조직의 조화, 경영자의 지원에 의해서만 영향을 받을 뿐 다른 요인에 의해서 영향을 받지 않는다. 따라서 성숙도가 높은 정보보호정책을 수립하기 위해서는 조직의 특성을 반드시 고려해야 한다.

Ⅵ. 결 론

본 연구는 조직의 정보보호정책 성숙도에 영향을 미치는 요인을 도출하고, 분석하였다. 정보보호정책 성숙도의 측정을 위해 본 연구는 설문조사를 통해서 대상 조직의 정보보호정책의 성숙도를 측정하였다. 본 연구는 정보보호정책의 성숙도에 영향을 미치는 4가지 요인을 문헌연구를 통해서 추출 및 검증하였고, '정보보호정책에 대한 조직의 지원'이 정보보호정책의 성숙도에 미치는 영향을 확인하였다. 본 논문이 가지는 한계는 설문조사의 어려움으로 인해서 설문분석 대상이 부족하여 광범위한 데이터를 분석하지 못하였지만, 데이터 분석 결과는 의미 있는 결과를 도출하고 있다.

본 연구가 제시하는 정보보호정책의 성숙도에 영향을 미치는 요인은 향후 정보보호정책 수립에 있어서 중요한 시사점을 제공한다. 정보보호는 기술적, 물리적, 관리적 측면을 내포하고 있는 통합적인 성격을 가지고 있다. 따라서 성숙도가 높은 정보보호정책을 수립하기 위해서는 조직의 특성을 반드시 고려해야 한다. 특히 정보보호안전성진단, 정부기관의 정보보호수준평가 등의 제도가 시행되고 있는 시점에서 조직의 특성을 반영하지 않은 명목상의 정보보호정책은 특정 조직의 정보보호수준제고에 도움이 되지 않는다. 따라서 본 연구 결과

가 제시하듯이 조직의 정보보호정책은 반드시 조직의 특성을 반영해야 한다. 특히 정보보호정책의 수립 및 이행은 강력한 경영자의 지원이 필요하다. 따라서 국가기관 및 민간기관이 경영자를 대상으로 정보보호정책의 중요성을 일깨울 수 있는 교육 프로그램의 개설이 시급하다 할 수 있다. 본 연구는 정보보호정책의 성숙도에 영향과의 관계만을 한정하여 연구를 수행하였다. 본 연구 결과를 바탕으로 조직의 정보보호수준에 미치는 요인을 탐색하는 연구, 조직의 정보보호정책이 정보보호수준 제고에 미치는 경로 분석 등의 연구가 수행된다면, 정보보호수준을 제고를 위한 정책 수립 및 집행에 기초가 될 것이다.

참고문헌

[1] 김세헌, *정보보호 관리 및 정책*, 생능출판사, 2002.

[2] S. Banerjee and D.Y. Golhar, "Electronic Data Interchange : Characteristics of Users and Nonusers", *Information and Management* 26(2), pp.65-74, 1994.

[3] R. Baskerville and M. Siponen,"An Information Security Meta-Policy for Emergent Organizations", *Logistics Information Management,* 15, pp.337-346, 2002.

[4] R. C. Beatty, J. P. Shim and M. C. Jones, "Factors Influencing Corporate Web Site Adoption : a Time-Based Assessment", *Information & Management* 38, pp.337-354, 2001.

[5] British Standards Institute(BSI), *Information Security Management BS7791-I*, BSI, London, 1999.

[6] R. O'Callaghan, P. J. Kaufman and B. Kronsynski, "Adoption Correlates and Share Effects of Electronic Data Interchange in Marketing Channels", *Journal of Marketing* 5(1), pp.9-19, 1992.

[7] R. Cooper and R. Zmud, "Information Technology Implementation : a Technological Diffusion Approach", *Management Science* 36(2), pp.156-172, 1996.

[8] Ernst & Young, *Information Security Survey*, Ernst & Young, 2004, London.

[9] H. Fulford and N. F. Doherty, "The Appli- cation of Information Security Policies in Large UK-based Organizations : an Explora- tory Investigation", *Information Management & Computer Security*, 11(3), pp.106-114, 2003.

[10] D. Gritzalis, "A Baseline Security Policy for Distributed Healthcare Information Systems", *Computers and Security,* 16(8), pp.709-719, 1997.

[11] V. Grover and J. T. C. Teng, "An Examination of DBMS Adoption and Success in American Organizations", *Information and Management,* 23(5), pp.239-248, 1992.

[12] H. N. Higgins, "Corporate System Security : Towards an Integrated Management Approach", *Information Management & Computer Security*, 7(5), pp.217-222, 1999.

[13] K. Hone and J. H. P. Eloff,"Information Security Policy-What Do International Security Standards Say?", *Computers & Security*, 21(5), pp.402-409, 2002.

[14] K. Joshi, "The Measurement of Fairness or Equity Perceptions of Management Information Systems Users", *MIS Quarterly* 13(3), pp.343-358, 1989.

[15] B. Ives and G. P. Learmouth, "The Information Systems as a Competitive Weapon", *Communications of the ACM,* 27(12), pp.586-603, 1984.

[16] Maria Karyda, Evangelos Kiountouzis, and Spyros Kokolakis, "Information Systems Security Polices : a Contextual Perspectives", *Computers & Security,* 24(3), pp.246-260, 2004.

[17] Karyda M.,Kokolakis S, Kiountouzis E., Content, Context, Process Analysis of IS Security Policy Formation, *Proceedings of 18th IFIP International Conference on Information Security*, Kluwer Academic Publishers, 2003.

[18] T. H. Kwon and R. Zmud, *Unifying the*

Fragmented Models of Information Systems Implementation, in : R. J. Boland, R. A. Herschhein(Eds), Critical Issues in Informaton Systems Research, Wiley, New York, pp.227-252, 1987.

[19] T. Peltier, *Information Security Policies and Procedures : a Practitioner's Reference,* CRC Press, 1999.

[20] L. E. Raho, K. A. Belohlav and K. D. Fiedler, "Assimilating New Technologies into the Organization : an Assessment of McFarlan and McKinney's model", *MIS Quarterly*. 11(1), pp.47-57, 1987.

[21] M. Siponen, "A Conceptual Foundation for Organizational Information Security Awarness", *Information Management & Computer Security,* 8(2), pp.31-41, 2000.

[22] M. Siponen, "Towards Maturity of Information Security Maturity Criteria : Six Lessons Learned from Softwware Maturity Criteria", *Information Management & Computer Security, 10*(5), pp.210-224, 2002.

[23] H. Jeff Smith, S. J. Milberg, S. J. Burke, "Information Privacy : Measuring Individuals' concerns about Organizational Practices", *MIS Quarterly,* 20(2), pp.167-196, 1996.

[24] R. V. Solms, "Information Security Management : Why Information Security is so Important", *Information Management & Computer Security*, 6(5), pp.224-225, 1998.

[25] V. Symon, "A Review of Information Systems Evaluation : Content, Context and Process", Journal of Information Systems, 1(3), pp.205-212, 1991.

[26] T. L. Wiant, "Information Security Policy's Impact on Reporting Security Incidents", *Information Management and Computer Security,* 13(24), pp.448-459, 2005.

[27] Whitman ME, Mattford HJ, *Principles of Information Security Course Technnology*, pp.153-190, 2003.

[28] C. Wood, *Security Policies Made Easy* Baseline Software, 1999.

[29] R. Zmud, "Diffusion of Modern Softwware Practices : Influence of Centralization and Formalization", *Management Science,* 28(12), pp.1421-1431, 1982.