공공기관 정보보호 거버넌스 수준에 영향을 미치는 요인에 관한 연구

A Study on Factors Affecting the Level of Information Security Governance in Korea Government Institutions and Agencies

송정석(Jeongseok Song)*, 전민준(Minjun Jeon)** , 최명길(Myeonggil Choi)***

초 록

공공기관은 정보보호를 강화하기 위하여 정보보호 거버넌스 체제를 도입하고 있다. 공공기관은 정보보호 거버넌스 체계의 중요성을 인식하고, 정보보호 거버넌스의 확립을 위해서 정책 수립 및 제도 확립에 노력을 기울이고 있다. 본 연구는 공공기관의 정보보호 거버넌스 수준에 영향을 미치는 요인을 탐색하기 위하여 정보보호 거버넌스 수준 측정 모형과 요인 모형을 개발한다. 본 연구는 공공기관 정보보호 거버넌스 수준은 최고경영층의 지원에 의해서 결정되며, 공공기관 정보보호 거버넌스는 정보보호 예산 및 정보화 담당 부서의 규모와 밀접한 관련이 있음을 제시한다. 본 연구의 결과는 공공기관의 정보보호 거버넌스 확립을 위한 정책 방향을 제시한다.

ABSTRACT

To solidate information security, Korea government introduces information security governance. The public institutions and agencies in Korea have begun to recognize the importance of information security governance. For solidating information security governance, the government has tried to establish and solidate an information security policy and information security systems. This study suggests factors affecting the level of information security governance in the public agencies and institutions through the factor analysis and the linear regression analysis. The results of this study show that the CEO's support is able to elevate the level of information security governance. The level of information security governance has relation with the number of the staff in information departments, and the budget in the public agencies and the institutions. This study provides directions for the public agencies and the institution for elevating the levels of information security governance.

키워드 : 정보보호, 정보보호 거버넌스, 정보보호관리

Government, Security Governance, Information Security, Information Security Management Systems

이 논문은 2009년도 중앙대학교 연구장학기금 지원에 의한 것임.

* 제1저자, 중앙대학교 경영경제대학 교수

** 공동저자, 중앙대학교 경영학과 석사

*** 교신저자, 중앙대학교 경영경제대학 교수

2011년 01월 26일 접수, 2011년 02월 15일 심사완료 후 2011년 02월 18일 게재확정.

1. 서 론

지난 3~4년에 걸쳐 기업 거버넌스 분야의 발전은 정보보호의 중요성을 한층 더 발전시켰다. 정보보호 거버넌스 개념의 성숙과 발전이 이루어지고 있다. 정보보호 거버넌스체계에서 최고경영층이 조직의 정보보호 수행에 있어서 핵심적 역할을 한다. 조직 거버넌스의 핵심적인 부분인 정보보호 거버넌스는 정보보호에 대한 최고경영층의 헌신된 관리 및 지도력, 적절한 조직의 구조, 사용자 교육, 필요한 정책, 절차, 프로세스 기술 및 정보보호 집행 메커니즘 등을 포함한다[4].

정보보호 거버넌스의 핵심적 특징 중 하나는 순환 구조이다. 순환 구조는 최고경영층의 정보보호에 대한 지원에서부터 정보보호의 핵심 전략화, 정보보호정책 수립 및 정보보호에 적합한 조직 구조 확립, 정보보호를 위한 적합한 권한과 책임 부여 등의 프로세스 구성된다[23].

최근 많은 조직이 기술적인 보안 대책에 많은 자원투자가 이루어졌지만 정보보호는 기술적 대책에 의해서만 해결될 수 없다는 사실과 최고경영층 차원의 의사결정과 체계가 정보보호 문제를 해결할 수 있다는 인식이 자리 잡기 시작했다.

최근 공공기관은 정보보호 거버넌스 체계의 중요성을 인식하고, 정보보호 거버넌스의 확립을 위해서 정책 수립 및 제도 확립에 노력을 기울이고 있다. 우리나라는 정보보호수준 강화를 위해 공공기관에 정보보호전담관을 지정하는 등 다양한 정책적 지원을 강화하고 있는 실정이다. 본 연구는 공공기관의

정보보호 거버넌스 수준에 영향을 미치는 요인을 탐색하여, 향후 공공기관 정보보호 거버넌스 확립에 필요한 정책 및 제도 수립 방향을 탐색하고자 한다. 공공기관의 정보보호 강화는 정보보호 거버넌스 확립을 통해서 가능하다. 공공기관이 정보보호 거버넌스를 수준 향상을 위해서 투입하는 자원은 주로 정보보호시스템 도입 등을 강화하는 노력이다. 그러나 정보보호 거버넌스 확립은 정보보호시스템 도입 이외에도 많은 요인에 의해서 결정된다. 따라서 본 연구는 효과적인 공공기관의 정보보호 거버넌스 확립을 위해서 다양한 측면에서 정보보호 거버넌스 확립에 영향을 미치는 요인을 조사하고, 제시한다. 본 연구는 공공기관의 정보보호 거버넌스 수준을 측정하고, 공공기관의 정보보호 거버넌스 수준에 미치는 요인을 제시한다. 본 연구의 결과는 공공기관의 정보보호 거버넌스 수준 향상을 효과적으로 이행할 수 있는 정책적 시사점과 이론적 시사점을 제공한다.

2. 정보보호 거버넌스

2.1 정보보호 거버넌스 프레임워크

정보보호는 단순히 기술적인 이슈로만 인식되어 왔으며, 최고경영층의 주의를 끌지는 못했다. 정보보호는 기술적 이슈, 전략적 이슈 및 법적인 이슈를 포함한다[12]. Swindle and Conner는 정보보호는 최고경영진의 위험관리 노력, 보고체계, 책임을 강조하는 전사적 거버넌스로 다루어야 한다고 강조한다

[25]. 따라서 정보보호 거버넌스는 최고 경영층의 관점에서 정보보호를 총괄적으로 취급하는 프로세스라고 정의할 수 있다[1].

업무 정보의 기밀성, 무결성, 가용성을 위해서는 정보보호는 내, 외부의 정보보호 요구사항을 충족시켜야 한다. 외적 정보보호 요구사항은 1) 정보보호 관련 표준과 최상의 업무처리방식(best practices)의 채택과 2) 관련 법/규정 준수 의무로 구분된다. 정보보호표준은 ISO27000 시리즈(정보보호 관리체계 : ISMS) 등이 있고, 관련 법/규정은 미국의 Sarbanes-Oxley Act(2002)와 FISMA, 남아공의 Electronic Communications and Transactions Act(2002), 한국의 정보통신기반보호법(2001), 금융 산업의 International Basel II Accord 등이 있다.

내적 정보보호 요구사항은 1) 업무 관련 이슈, 2) IT 인프라 이슈로 구분할 수 있다. 정보보호 요구사항은 조직이 정상적으로 업무를 처리하기 위해서 정보처리 측면에서 전사적인 원칙, 목표 등을 요구한다[23].

IT 인프라 이슈는 ‘정보 백본’을 형성하는 핵심 인프라를 보호하기 위한 요구사항으로서 위험분석 및 관리 과정을 통해 처리된다.

조직은 정보보호를 거버넌스 관점으로 접근해야 한다. 궁극적으로는 현재의 정보보호 통제 구현 및 관리 등 기술적 측면에 치중한 접근방법으로는 한계가 있고, 보다 전략적 측면에서의 정보보호를 접근해야 한다[23].

Corporate Governance Task Force[13]는 조직의 다양한 거버넌스 프로그램에 정보보호를 포함하기 위해서 정보보호는 내부통제에 일부로 포함되어야 하며, 전략적 측면으로 다루어져야 한다고 강조한다[13].

2.2 정보보호 거버넌스 수준 측정을 위한 정보보호관리체계

정보보호 거버넌스는 조직 거버넌스 차원에서 조직의 정보 위험에 대처할 수 있는 효과적인 전략 수립을 위해 두 가지 측면을 고려해야 한다. 첫째, 조직의 최고경영층이 정보보호 전략 및 방향을 설정하는 거버넌스 측면이 있고, 둘째, 조직의 정보보호 전략을 어떻게 구현하고 관리할 것인가에 관한 관리적 측면이 있다. 거버넌스 측면은 조직의 최고경영층이 정보보호에 대한 방향 제시와 통제 역할을 해야 한다는 의미이다. 조직의 최고경영층이 전사적 정보보호 정책 및 계획을 수립하여 정보보호에 대한 책임과 의지를 보여주고, 조직의 임무, 목표, 전사적 정보보호 전략 수행을 지원해야 한다[27]. 관리적 측면은 정보보호 정책을 조직내에서 구현하는 방안을 의미한다. 전사적 정보보호 정책에서 제시한 정보보호요구사항을 구현하기 위해서 조직의 부문 관리자가 책임지고 실행해야 한다. ISO27002는 조직의 일상적 활동 및 기능과 통합 정보보호대책을 제시하고 있다[17].

〈그림 1〉 정보보호 거버넌스 프레임워크

정보보호 거버넌스는 조직의 내적, 외적 정보보호 요구사항을 효과적으로 만족시켜 조직의 업무 정보를 위협으로부터 보호한다. 정보보호 거버넌스는 조직의 정보보호를 위해 효과적인 정보보호 전략 수립, 구현 및 모니터링 등의 방향을 제시한다. 정보보호 거버넌스는 기업 운영의 3가지 주요 요소(인적자원, 프로세스, 기술)에 대한 역할과 책임을 분명하게 해주는 효과가 있다[27]. <그림 1>은 효과적 정보보호 거버넌스 수립을 위한 프레임워크를 보여주고 있다.

정보보호 거버넌스는 조직의 정보보호의 방향 및 전략을 결정할 뿐만 아니라 구체적인 정보보호 정책, 정보보호 대책 구현, 정보보호통제 결과의 모니터링을 포함하고 있다. 정보보호 거버넌스는 ISO27000 시리즈, 정보보호관리체계(information security management systems) 형태 등으로 구체화될 수 있다. 정보보호 거버넌스가 정보보호 관리체계와 동일하지 않다. 그러나 현재 정보보호 거버넌스 프레임워크를 가장 구체적으로 표현한 대안으로 정보보호 관리체계를 들 수 있다. 따라서 정보보호 거버넌스를 구현한 정보보호 관리체계 등을 계량화시켜 평가함으로써 조직 전체의 정보보호 수준을 측정할 수 있다. 정보보호 거버넌스 프레임워크가 ISO27000, 정보보호 관리체계 등으로 구체화되고, 동 체계를 통한 조직의 정보보호를 점검하여 측정하면 조직전체의 정보보호수준을 측정할 수 있다. 정보보호 관리체계가 정보보호 거버넌스 수준을 측정하는 모형으로 활용할 수 있는 이유는 다음과 같다.

첫째, 정보보호 관리체계는 조직의 정보보호정책, 정보보호 정책을 구현을 위한 정보보

호대책 수립, 정보보호 대책에 대한 효과성 및 이행 여부에 대한 최고경영층에 대한 보고 등을 포함하고 있다. 따라서 정보보호 관리체계는 거버넌스의 전략적 측면과 관리적 측면을 모두 포함하고 있다. 정보보호 관리체계가 요구하는 정보보호정책은 거버넌스의 전략적 측면을 규정한다. 정보보호 관리체계가 규정하는 개별 정보보호대책, 감사 및 평가 프로세스는 정보보호 거버넌스의 관리적 측면을 포함하고 있다. 둘째, 정보보호 관리체계는 최고경영진의 위협관리 노력, 보고체계, 책임을 강조하는 전사적 거버넌스를 형태를 띠고 있다. 정보보호관리체계는 최고 경영층이 조직의 정보를 보호하기 위한 구체적인 정책, 프로세스 등을 정의하고 있으며, 최고경영층이 정보보호정책 수립에 참여를 규정하고 있다. 셋째, 정보보호 관리체계의 정보보호 거버넌스의 내적, 외적 정보보호 요구사항을 반영할 수 있는 형태로 개발된다. 정보보호 관리체계는 거버넌스의 내적 정보보호 요구사항인 업무 관련 이슈, IT 인프라 이슈 등을 정보보호정책을 근거하여 개별 정보보호대책으로 제시하고 있다. 정보보호 관리체계는 거버넌스의 외적 정보보호 요구사항인 법/규제, 선진 사례 및 표준화 등이 정보보호 정책에 반영될 수 있는 프로세스를 포함하고 있다.

2.3 정보보호 관리체계

현존하는 정보보호 관리체계는 정보보호 거버넌스 수준을 완전히 측정할 수 없다. 현존하는 정보보호 관리체계는 정보보호 거버넌스의 지향점, 체계 등을 완전히 포괄하지

못한다. 그러나 현존하는 정보보호 평가체계 중 정보보호 거버넌스 수준을 가장 근접하게 평가할 수 있는 도구가 정보보호 관리체계이다. 따라서 본 연구는 정보보호 거버넌스 수준을 측정할 수 있는 연구 모형 개발에 활용할 수 있는 정보보호 관리체계를 간략하게 살펴본다. 대표적인 정보보호 관리체계는 ISO 27000시리즈, 한국인터넷진흥원이 평가하는 정보보호 관리체계(ISMS), 행정안전부가 공공기관을 중심으로 정보보호 거버넌스를 평가하는 G-ISMS, 국가정보원의 정보보호 관리실태 평가 등이 있다.

2.3.1 ISO27000 시리즈

영국 BSI(British Standard Institute)는 조직 정보보호를 위한 인증 방법론인 BS7799를 영국 표준으로 제정하였다. ISO/IEC는 BS 7799를 모태로 정보보호 관리체계 국제표준인 ISO17799를 제정하였고, 2005년 수정 및 확장을 거쳐 ISO/IEC27000 시리즈로 제정한다[2]. ISO27000은 정보보호를 기술적 이슈로 간주하지 않고, 기술적, 물리적, 관리적 통제를 포함하는 전사적 차원의 정보보호를 구현하는 체계화된 경영시스템으로 자리매김하고 있다[2]. ISO27002에 규정한 정보보호 요소는 12개 항목으로 나누어진다.

2.3.2 한국인터넷진흥원의 ISMS

ISMS는 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조를 근거로 한국인터넷진흥원이 정보통신 서비스제공자, 정보통신 서비스를 위해 물리적 시설을 제공하는 자, 민간사업자 등 인증대상기관이 수립·운영하

고 있는 ISMS의 기술, 물리, 관리적 정보보호 대책이 인증심사기준에 적합한지를 평가하여 인증하는 제도이다[6].

2.3.3 행정기관 정보보호관리체계(G-ISMS)

정보보호관리체계 인증제도는 행정기관이 정보보호를 위해 필요한 관리적·기술적·물리적 기준에 적합한 정보보호관리체계를 갖추었는지 심사하여 인증기준에 따라 적절히 운영되고 있는 경우 인증서를 부여하고, 지속적으로 사후관리를 수행하는 체계이다[6].

행정기관 G-ISMS 인증기준은 기존 ISO27001과 같이 관리과정, 문서화, 통제항목(정보보호대책)의 3개 부분으로 구성된다. 관리과정은 ISO의 PDCA(Plan-Do-Check-Act)에 따라 4개 관리과정에 대하여 15개 요구사항으로 구성되며, 동 요구사항 달성 여부를 점검하기 위해 39개 점검 항목을 제시한다[7]. 행정기관용 정보보호 관리체계 인증제도는 전자정부서비스에 적용된 후, 중앙행정기관의 정보보호 관리체계를 수립하여 운영하는 경우를 고려하여 개발되었다[7].

2.3.4 공공기관 정보보안 관리실태 평가 제도

국가정보원은 전자정부법 제27조 제3항(정보통신망 등의 보안대책 수립·시행)[3] 동법 시행령 제35조(전자문서의 보관유통 관련 보안조치) 및 제36조(이행여부 확인), 공공기록물 관리법 시행령 제5조(전자기록물 보안관리)에 의거하여 공공기관을 대상으로 '정보보안 관리실태 평가'를 실시하고 있다[3]. 동 제도는 해당기관의 정보통신시스템에 대한 보안관리 체계가 제대로 구축, 운영되는지 실태

를 확인하고 미흡한 부분은 보완 및 보안대책을 지원하는 형식으로 운영되고 있다. 국정원은 2007년 99개 국가·공공기관 대상 최초 평가를 실시하였다.

정보보안 관리실태 평가는 기관 보안등급 분류 → 평가항목 자체평가 → 자체평가 내용 현장실사 → 평가결과 심의·통보의 4단계로 구분된다<그림 2>. 평가 결과를 토대로 미비점 개선 및 기관 실정에 맞는 보안 대책을 수립한다.

〈그림 2〉 정보보안 관리실태 평가 절차

정보보안 관리실태 평가의 1단계는 기관의 보안등급은 수행업무의 중요도, 정보시스템, 피해에 따른 영향력 등에 해당하는 14개 평가요소에 따라 가·나·다급으로 분류한다. 2단계는 국가정보원이 마련한 평가항목에 대해 각 기관이 자체평가를 실시한다. 국가정보원은 ISO/IEC 27002를 토대로 한 평가항목에 보안환경 변화를 고려하여 매년 새로운 평가항목을 제시한다[3]. 이 부분이 민간영역의 정보보호 관리체계 인증제도와 가장 큰 차이점이라 할 수 있다. 민간영역에서는 고정된 통제항목을 제시하고 있지만 공공영역은 정보통신 환경 및 국가 보안정책의 변화상을 적시 반영한다. 공공기관 평가를 처음 실시한 2007년도에는 분야별 보안정책과 관련규정 보유여부에 중점을 두어 9개 분야 246개 항목을 제시한다. 평가항목 8개 분야는 정책 및 업무수행, 정보자산 관리, 비밀관리, 인적보안, 침해사고 대응체계 구축, 접근보안, 운영관리, 물리적 보안으로 구성되어 있다<표 1>.

〈표 1〉 국가정보원의 2008 보안관리실태 평가 항목(135개)

대분류	중분류	지표수
1. 정책 및 업무수행	1.1 정보보안 정책, 1.2 정보보안 계획, 1.3 정보보안 업무수행	8
2. 정보자산 관리	2.1 정보자산 관리, 2.2 시스템 개발 및 운용	13
3. 비밀 관리	3.1 비밀 관리, 3.2 국가용 보안시스템	9
4. 인적 보안	4.1 정보보안 인력, 4.2 내부인원 관리, 4.3 정보보안 교육, 4.4 외부인력 관리	21
5. 침해사고 대응체계 구축	5.1 사전 대응, 5.2 사후 대응	10
6. 접근보안	6.1 정보통신망 보안, 6.2 정보시스템 보안, 6.3 정보보호시스템 보안, 6.4 사용자 계정 및 인증	27
7. 운영관리	7.1 서비스 관리, 7.2 정보통신기기 관리, 7.3 보조기억매체 관리, 7.4 로그 관리, 7.5 백업	40
8. 물리적 보안	8.1 출입 통제, 8.2 시설 보안, 8.3 기반시설 보호	7

3. 공공기관 정보보호 거버넌스 수준 분석을 위한 모형 개발

공공기관 정보보호 거버넌스 수준을 측정하기 위해서는 정보보호 관리체계를 활용한 정보보호 거버넌스 수준에 영향을 미치는 모형을 개발하기 위해서는 정보보호 거버넌스 수준 측정 모형 및 정보보호 거버넌스 수준에 영향을 미치는 요인 분석 모형 등 2가지 모형을 개발해야 한다. 따라서 본 연구는 정보보호 거버넌스 수준을 측정하기 위해서 ISO 27002를 활용하여 모형을 개발한다. 본 연구는 정보보호 거버넌스 수준에 영향을 미치는 요인 분석 모형은 선행 연구를 활용하여 개발한다.

3.1 정보보호 거버넌스 수준에 미치는 요인 선행 연구

본 연구는 정보보호 거버넌스 수준에 영향을 미치는 요인과 관련된 요인을 선행 연구를 통해서 탐색한다.

정보보호 거버넌스 수준에 미치는 요인을 탐색 연구와 관련성이 있는 연구는 정보보호 정책의 성숙도 수준과 관련된 요인을 탐색하는 연구, 조직의 정보보호 수준 향상에 영향을 미치는 요인을 탐색한 연구 등이 있다.

조직의 정보보호 수준 향상에 영향을 미치는 요인과 관련된 선행 연구는 첫째 경영층의 지원과 관련된 연구, 둘째, 정보보호와 기존 조직과의 조화는 정보보호 수준 향상과의 관련성 연구, 셋째, 정보보호와 조직성과 개선과의 관련된 연구, 넷째, 정보보호와 조직

문화와의 관련성 연구 등이 있다.

첫째, 정보보호 수준과 최고경영층의 지원과의 관련된 연구를 살펴보면 다음과 같다. 최고경영층의 지원은 조직의 정보기술수준 수용 촉진을 강화하는 중요한 요인으로 밝혀졌다[19, 20]. 많은 연구결과에서 최고 경영자의 적극적인 지원은 새로운 기술과 제도의 도입 또는 좋은 정책 개발의 성공 여부를 예측할 수 있는 척도라고 언급되고 있다[4]. 동요인을 토대로 최명길 외 연구는 최고경영층의 지원은 조직의 정보보호정책의 성숙도에 영향을 미치는 중요한 요인이라 실증하고 있다[5].

둘째, 정보보호와 기존 조직과의 조화는 정보보호의 향상과 관련된 연구를 살펴보면 다음과 같다.

Fulford 외 연구 및 Maria Karyda 연구는 정보보호 정책에 대한 구성원의 우호적인 태도 및 조직의 임무를 고려한 정보보호정책은 조직의 정보보호 정책 적용에 된다고 제시한다[15, 21]. 동요인은 조직이 높은 수준의 정보보호 정책을 수립하는 데 있어서 중요한 요인이라고 제시한다. 최명길 외 2인의 연구는 동요인이 정보보호 성숙도 수준에 영향을 미친다고 실증하고 있다[4].

셋째, 정보보호와 조직성과 개선과의 관련성 연구를 살펴보면 다음과 같다. 조직은 새로운 제도의 도입으로 조직의 성과가 개선될 수 있을 것이라는 인식이 있다면 기꺼이 새로운 제도를 선택한다[4]. 조직이 성숙한 정보보호정책의 수립과 이행을 통해 업무수행 비용 감소, 효율성 증가, 향상된 서비스 제공, 조직의 신뢰성 및 경쟁력 증가, 기존의 문제 해결, 새로운 사업 기회 획득 가능성 증가 등

의 가능성 증가를 인식하면 정보보호 정책 수행을 적극적으로 추진할 수 있다[25].

넷째, 조직문화와 정보보호문화와의 관련성이다. 조직의 정보보호 수준의 향상은 조직의 문화와 밀접한 관련이 있다[4]. 정보보호의 발전에 있어서 제3세대는 정보보호표준, 정보보호 국제인증, 정보보호문화, 조직의 정보보호측정 등의 4가지 요소로 이루어진다. 많은 조직은 자신의 구성원이 많은 경우에 있어서 IT 시스템을 위협하는 가장 큰 위협원이 될 수 있다는 사실을 인식하고, 많은 조직은 광범위한 정보보호 교육을 시작한다. 아무리 좋은 기술적인 대책과 절차적인 대책도 정보보호에 있어서 인적(人的) 측면을 완전히 해결할 수 없다. 정보보호 문화는 반드시 조직내에서 창조될 수밖에 없고, 모든 구성원이 정보보호를 자연스럽게 자신의 업무 수행의 일부분으로 여길 수 있도록 해야 한다. 정보보호 교육은 지속적으로 조직의 정보보호 계획에 내포되었고, 조직은 끈임 없이 정보보호를 일상의 한 부분으로 정착시켜야만 하는 압박에 시달린다. 적절한 정보보호 문화가 정착되지 않으면, 조직은 광대한 위험에 노출될 수밖에 없다는 사실을 인식한다.

본 연구는 기존 연구와 다음의 차이점이 있다. 첫째, 본 연구는 정보보호가 가장 발달한 공공기관을 대상으로 정보보호 거버넌스에 영향을 미치는 요인을 탐색하고 있다. 따라서 본 연구는 거버넌스에 영향을 미치는 요인을 가장 효과적으로 발견할 수 있다. 민간기관은 정보보호의 중요성은 인식하지만, 효과가 명확하지 않은 정보보호에 적절한 자원을 투자할 수 없다. 그러나 공공기관은 법적·제도적 뒷받침으로 비교적 정보보호에

많은 자원을 투자하고 있는 실정이다. 둘째, 본 연구는 정보보호 거버넌스에 영향을 미치는 다양한 요인을 모형에 포함하고 있어 정보보호 거버넌스 수준에 영향을 미치는 요인을 정확하게 식별할 수 있을 것이다. 기존 연구는 정보보호 거버넌스 수준에 영향을 미치는 요인을 1개 내지 2개를 대상으로 탐색적으로 제시하고 있다. 셋째, 본 연구는 정보보호 거버넌스 수준 향상에 필요한 실무적 시사점과 이론적 시사점을 동시에 제공하고 있어 공공기관 뿐만 아니라 민간기관 정보보호 수준 향상을 위한 효과적인 자원 및 노력 투입에 있어서 정당성을 제공하고 있다.

3.2 공공기관 정보보호 거버넌스 측정 선행 연구

정보보호 거버넌스 수준을 측정하는 모형은 제 2장에서 살펴본 바와 같이 다양한 모형이 존재한다. 본 연구는 제 2장에서 서술된 모형 중 국정원이 사용하는 정보보호 관리실태 평가 모형을 근거로 공공기관의 정보보호 거버넌스 수준을 측정한다. 정보보호 관리실태 평가 모형은 ISO27002와 유사하다. 본 연구가 사용한 공공기관의 조직의 정보보호 거버넌스 수준을 측정하는 모형은 ISO27002를 기반으로 <표 2>와 같이 도출할 수 있다.

본 연구는 총 9개 분야에 걸쳐서 135개 항목을 측정한다. 각 항목의 가중치는 정보보호 거버넌스 수준 평가에 참가한 전문가를 대상으로 한 포커스 그룹이 측정하였다. 공공기관의 정보보호 거버넌스 수준 측정은 135개 항목을 사용하여 5점 척도로 측정하였고, 총 측정수준 점수는 100점으로 환산하였다. 동 조

〈표 2〉 공공기관 정보보호 거버넌스 측정 항목

ISO27002	조직정보보호 거버넌스 측정 항목	항목수
1. 법규 또는 지침	1. 정책 및 업무수행 : 정보보안 정책, 정보보안 계획, 정보보안 업무수행	8
2. 정보보호정책 : 정보보호 정책의 효과적 운영·방향문서		
3. 정보보호조직 : 정보보호 하부구조 및 아웃소싱 요구사항	2. 인적 보안 : 정보보안 인력, 외부인력 관리	10
4. 자산관리 : 정보자산 분류, 책임, 처리 절차	3. 정보자산 관리	7
5. 인적보안 : 직무 정의, 종사자 입사, 보직변경시 보안	4. 인적 보안 : 내부인원 관리, 정보보안 교육	11
6. 물리적 환경적 보안 : 시스템 보호를 위한 보안 구역 및 일반적 물리적 통제	5. 물리적보안 : 출입통제, 시설보안, 기반 시설 보호	7
7. 운영관리 : 시스템에 대한 관리로 운영절차 및 책임	6. 운영관리 : 서비스 관리, 정보통신기기 관리, 보조기억매체관리, 로그관리, 백업	40
8. 접근 통제 : 접근통제에 대한 요구사항 사용자 책임	7. 접근보안 : 정보통신망·시스템 보안, 사용자 계정 및 인증	27
9. 시스템 개발 및 관리 : 시스템 개발 관련 보안 요구사항	8. 정보자산관리 : 시스템 개발 및 운용	6
10. 위험관리 : 정보시스템 운영 및 취약성 분석, 모의해킹	7. 접근보안 : 정보통신망 보안, 정보시스템 보안, 정보보호 시스템 보안, 사용자 계정 및 인증(7번항목 동일)	27
11. 사업연속성관리 : 재난발생시 업무연속성유지	8. 침해사고 대응체계구축 : 사전 대응, 사후 대응	10
	9. 비밀 관리 : 3.1 비밀관리, 3.2 국가용 보안시스템	9

사는 평가 전문가가 2008년 중앙행정기관 및 연구기관 등 99개 공공기관을 직접 방문하여 관련 항목을 측정하였다.

공공기관의 정보보호 거버넌스 수준 측정에 영향을 미치는 요인 모형을 개발하기 전에 공공기관의 정보보호 거버넌스 측정모형과 민간기관의 정보보호 거버넌스 측정모형을 비교를 통해 공공기관 특유의 정보보호 거버넌스를 식별하여, 정보보호 거버넌스 수

준에 영향을 미치는 요인 분석 모형에 활용한다.

3.3 정보보호 거버넌스 수준 영향을 미치는 요인

본 연구는 공공기관의 정보보호 거버넌스 수준에 영향을 미치는 요인 모형을 개발하기 위해서 선행연구 및 공공기관 및 민간기관의

정보보호 거버넌스 수준 모델과의 차이점 등을 고려하여 다음과 같은 요인을 추출한다.

첫째, 공공기관의 정보보호 거버넌스 수준에 영향을 미치는 중요한 요인으로 최고 경영층의 지원이다[5]. 최고 경영층의 지원은 정보기술수준 수용 촉진, 새로운 기술 및 제도의 도입, 정책 개발의 성공 여부이다. 본 연구는 ‘최고경영층의 지원’ 요인과 관련된 하부 요인을 5가지로 선정했다. 최고경영층의 정보보호에 대한 관심은 기관장의 정보보호에 대한 관심 및 정보화를 책임지는 기관의 정보화최고담당관의 정보보호에 대한 관심으로 나타날 것이다[5]. 공공기관의 경우 최고경영층의 지원뿐만 정보보호 거버넌스 향상을 위해서는 정보화최고담당관(CIO)의 정보보호에 대해서 관심이 높아야 한다.

기관장의 정보보호에 대한 관심은 기관의 정보보호를 위협하는 위협 요인을 파악할 수 있을 것이다[22].

최고경영자의 정보보호에 대한 관심 및 지원은 업무수행을 정보보호와 연관시키며, 궁극적으로 기관내 정보보호와 관련된 타부서와의 협조를 원활하게 한다. 기관장의 정보보호에 대한 관심은 정보보호와 관련된 정보보호부와 기타 부서와의 협조를 증진시켜 줄 수 있다[15, 21].

개별 기관의 특성을 고려한 정보보호 거버넌스 체계 구축을 위해서는 개별 기관의 정보보호 위협 요인에 대한 인식 및 기관장의 정보보호 위협 요인의 파악 등이 필수적이다. 기관장의 정보보호에 대한 관심은 기관의 정보보호 위협요인에 대한 인식을 제고해 줄 수 있다[14].

둘째, 공공기관의 정보보호 거버넌스 수준

을 향상을 위해서는 정보보호와 기관의 고유 업무와의 밀접한 정보보호와 대국민 서비스 및 신뢰성이 있어야 한다. 이 요인은 선행연구에서 제시된 정보보호와 조직성과와의 관련성을 기반으로 도출한 요인이다[5]. 동 요인과 관련된 하부요인은 다음과 같다.

‘정보보호와 대국민 서비스 및 신뢰성’ 요인을 구성하는 하부 요인은 정보보호 활동 강화와 기관의 업무 성과 개선과 관련성이 존재한다[9]. 정보보호는 기관의 업무 성과의 증진 뿐만 아니라 대국민 서비스를 품질 향상에 기여할 수 있다. 동 하부 요인은 정보보호가 더 나은 고객 서비스를 제공할 것이라는 요인에서 추출한다[9, 16].

정보보호는 업무 성과 개선과 관련이 있으므로 궁극적으로 기관의 경쟁력 향상[8], 기관의 신뢰성 향상[9]과 관련이 있다. 정보보호가 기관의 성과를 향상시킬 수 있다면 공공기관의 구성원은 정보보호 거버넌스 수준 향상을 위해서 자원을 투자하고, 동참할 것이다. 공공기관의 정보보호 거버넌스 측정 모형의 특징인 운영관리 요인 중 정보기기 관리에 대한 치중 등은 정보기기 관리는 정보보호정책 및 활동과 밀접한 관련이 있다.

셋째, 공공기관의 정보보호 거버넌스에 영향을 미치는 요인은 기관 구성원의 정보보호 업무에 대한 인식 및 정보보호 문화이다[4]. ‘기관 구성원의 정보보호 업무에 대한 인식 및 정보보호 문화’ 요인을 설명하는 하위 요인은 정보보호 예산의 적절성[18], 기관 구성원의 정보보호 활동에 대한 우호성[10], 기관장의 정보보안 담당부서에 필요한 권한 부여[10], 정보보호는 어렵다는 기관 구성원 인식[5] 등이다. 공공기관의 정보보호 거버넌스

〈표 3〉 공공기관 정보보호 거버넌스 수준에 영향을 미치는 요인

요인	하위 요인	설문 항목
경영층의 지원 (요인 1)	기관장의 정보보호에 대한 관심	5
	정보화 최고담당관의 정보보호에 대한 관심	6
	기관내 정보보호와 관련된 타부서 협조	9
	정보보호 위협 요인에 대한 인식	10
	기관장의 조직을 위협하고 있는 정보보호 위협 요인 파악	11
정보보호와 대국민 서비스 및 신뢰성 관련성 (요인 2)	정보보호 활동 강화와 기관의 업무 성과 관련성	12
	정보보호와 대국민 서비스 품질 관련성	14
	정보보호 및 활동과 기관 경쟁력 관련성	15
	정보보호 및 활동과 기관 신뢰성 관련성	16
구성원의 정보보호 업무에 대한 인식 및 문화 (요인 3)	정보보호예산의 적절성	4
	기관 구성원의 정보보호 활동에 대한 우호성	7
	기관장의 정보보안 담당부서에 필요한 권한 부여	8
	정보보호는 어렵다는 구성원의 인식	13

측정 모형의 특징인 프로세스 중심보다 업무 이행점검은 정보보호 활동에 대한 우호성 및 예산의 적절성, 정보보호에 대한 기관 구성원의 인식 등과 밀접한 관련이 있다. <표 3>은 공공기관의 정보보호 거버넌스의 수준에 영향을 미치는 요인 및 하위 요인, 요인을 측정하는 설문 항목을 나타낸다.

4. 공공기관 정보보호 거버넌스 수준 측정 및 영향 요인 분석

본 연구는 지난 2007년 11월 국가정보원이 99개 기관을 대상으로 실시한 정보보호 실태 평가 결과를 공공기관의 정보보호 거버넌스 수준 측정 결과로 활용한다. 국가정보원은 매년 공공기관을 대상으로 정보보호 수준을 측정한다. 국가정보원은 <표 3>의 항목을 전

공공기관의 정보보호 활동을 근거로 정보보호 수준을 측정한다.

각 항목의 가중치는 정보보호 거버넌스 수준 평가에 참가한 전문가를 대상으로 한 포커스 그룹이 측정하였다. 공공기관의 정보보호 거버넌스 수준 측정은 135개 항목을 사용하여 5점 척도로 측정하였고, 총 측정수준 점수는 100점으로 환산하였다.

본 연구는 정보보호 거버넌스 수준에 영향을 미치는 요인을 탐색하기 위해서 제 3장에서 개발한 정보보호 거버넌스 수준에 영향을 미치는 요인을 활용하여 설문지를 작성했다. 본 연구는 정보보호 거버넌스 수준에 영향을 미치는 요인을 탐색하기 위해서 동일한 99개 기관을 대상으로 설문 조사를 실시하였다.

동 연구는 공공기관의 정보보호 거버넌스 수준에 영향을 미치는 요인을 다음과 같은

단계로 도출한다.

첫째, 공공기관의 정보보호 거버넌스 수준에 영향을 미치는 요인을 도출하기 위해서 이론적으로 제시된 요인을 요인 분석을 통하여 통계적으로 검증한다. 둘째, 본 연구는 선형회귀분석 모형을 사용하여 요인분석에서 도출된 요인과 정보보호 거버넌스 측정 모형을 통해 획득한 개별 공공기관의 정보보호 거버넌스 수준을 나타내는 결과값간 관련성을 분석한다. 선형회귀분석은 결과값에 영향을 미치는 요인을 검증하여 공공기관의 정보보호 거버넌스 수준에 영향을 미치는 요인을 제시한다.

4.1 공공기관 정보보호 거버넌스에 영향을 미치는 요인 분석

본 절은 공공기관 정보보호 거버넌스 수준에 영향을 미칠 수 있는 요인을 검증하기 위

해서 설문 조사를 통해서 각 개별 요인을 대상으로 요인 분석을 실시한다. 요인분석은 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 항목의 그룹화 정도를 측정하기 위해서 요인부하(factor loading)를 관찰하였으며, factor loading > 0.6을 기준으로 관련된 항목을 그룹화 하였다. 하나의 항목이 그룹화 된 집단 이외의 요인에서 factor loading > 0.6일 경우 각 항목이 독립적으로 하나의 요인에만 포함되지 않다고 판단하여 모델에서 제거하였다.

본 연구에서 요인분석은 이론적으로 개발된 요인이 적절한지를 알아본다. 요인분석을 활용하여 통계적으로 검증된 요인은 <표 4>와 같다. 요인분석 결과 연구모형으로 설계된 요인과 유사하게 도출되었다. 다만 설문항목

〈표 4〉 요인분석 결과

항목 \ 요인	요인 1	요인 2	요인 3
	경영층의 정보보호지원	대국민 서비스 및 신뢰성	정보보호인식 및 문화
기관장의 정보보호에 대한 관심(5)	0.7921	0.0958	0.2190
정보화최고담당관의 정보보호에 대한 관심(6)	0.7860	0.1062	0.2266
정보보호 위협 요인에 대한 인식(10)	0.6491	0.0875	0.3412
기관장의 조직 위협하는 정보보호 위협요인 파악(11)	0.8335	0.1155	0.0349
정보보호 활동강화와 기관의 업무 성과 관련성(12)	-0.000	0.7171	0.3146
정보보호와 대국민 서비스 품질 관련성(14)	0.0179	0.7850	0.1524
정보보호 및 활동과 기관 경쟁력 관련성(15)	0.1672	0.8597	0.0615
정보보호 및 활동과 기관 신뢰성 관련성(16)	0.2299	0.7487	-0.083
정보보호예산의 적절성(4)	0.1044	0.0126	0.6904
정보보호는 어렵다는 구성원의 인식(13)	0.1810	0.1681	0.6938

중 설문항목 7번, 설문항목 8, 설문항목 9번은 요인 1과 요인 3에 동시에 적재되었다. 따라서 연구자는 항목 7번, 항목 8번, 항목 9번을 제거하고 요인분석을 실시하였다. 요인분석 결과 설문조사 전에 제시된 이론적 요인과 통계적으로 검증된 요인간의 관계가 의미가 있다. 대부분의 설문 항목은 이론적으로 제시된 요인과 동일한 결과를 나타낸다. 요인 적재량 요인적재치가 어느 정도 커야 하는가에 대한 일반적인 기준은 보통 0.3이상이면 유의하다.

설문항목의 신뢰도를 위해서 신뢰성 분석 결과 전체 항목의 신뢰성을 나타내는 크론바알파는 0.833268이며, 요인 1을 구성하는 항목의 신뢰도는 0.82757, 요인 2를 구성하는 항목의 신뢰도는 0.795650, 요인 3을 구성하는 항목의 신뢰도는 0.634111 등으로 나타났다. 연구 항목의 신뢰도를 나타내는 크론바알파 계수는 일반적으로 0.6이상이면 항목의 타당성이 있다고 판단한다. 따라서 본 연구 항목의 타당성은 존재한다.

4.2 공공기관 정보보호 거버넌스에 영향을 미치는 요인 도출을 위한 선행회귀분석

개별 공공기관의 정보보호 거버넌스 수준에 어느 요인이 영향을 미치는지 파악하기 위해서 도출된 요인과 개별 공공기관의 정보보호 거버넌스 수준 측정 결과값간 관련성을 선행회귀분석을 실시한다. 선행회귀분석 결과는 <표 5>와 같다.

3개의 요인이 정보보호 거버넌스 수준에 영향을 미치는 것을 검증하는 도구인 선행회귀

분석 모형을 분석하면 다음과 같다. 독립변수와 종속변수와 상관관계를 나타내는 R값은 0.48122, 및 선형 회귀모형의 설명력, 종속변수가 독립변수를 설명력을 나타내는 R제곱합은 0.2315로 각각 나타났다. 동 값은 조직을 대상으로 조사한 결과로 비교적 양호하다. 공공기관의 정보보호 거버넌스 수준을 설명하기 위해서 도입한 ‘정보보호에 대한 경영층의 지원’, ‘정보보호와 대국민 서비스 및 신뢰성’, ‘정보보호인식 및 문화’ 등을 독립변수로 도입한 동 회귀모형은 유의하다.

<표 5> 선형회귀분석 결과값

모형	R	R제곱합	조정된 R값	추정값의 표준오차	
	0.4812	0.2315	0.2071	8.7601	
	요인		비표준화 계수(B)	표준 오차	유의 확률
1	상 수		57.28	4.94	0.00
독립 변수	정보보호에 대한 경영층 지원		5.157	1.65	0.002
	정보보호와 대국민 서비스 및 신뢰성		2.279	1.574	0.150
	정보보호인식 및 문화		1.167	1.527	0.446
종속 변수	정보보호 거버넌스 측정 결과값		개별기관의 거버넌스 측정값		

선행회귀분석에서 개별 독립변수와 종속변수간 유의도가 0.05이하가 되면 독립 변수인 검증된 요인과 종속변수인 정보보호 거버넌스 측정 결과값간 관련성이 있다. 본 선행회귀분석 결과 개별 공공기관의 정보보호 거버넌스 수준에 영향을 미치는 요인은 ‘정보보호에 대한 경영층의 지원’이다. 정보보호와 대

국민 서비스 및 신뢰성 및 정보보호 인식 및 문화 등은 공공 기관의 정보보호 거버넌스 수준에 영향을 미치지 않는다.

설문 항목 1번에서 4번을 사용하여 기관의 정보부서의 특성과 정보보호 수준과의 관계를 분석하였다. 분석 결과 정보보호 담당자와 개별 기관의 정보보호 수준과는 관련성이 없다고 나타났다.

그러나 <표 6>과 같이 정보화관련부서의 인원, 정보보호 예산과 개별 기관의 정보보호 수준은 관련성이 있는 것으로 나타났다.

<표 6> 정보화 부서의 특성과 정보보호 거버넌스 수준간의 연관성 분석(선형회귀분석)

모형	요인	비표준화 계수(B)	표준 오차	유의 확률
1	정보화부서 인원	2.24	0.74	0.00
2	종속변수	개별기관 점수		
1	정보보호예산	2.63	1.03	0.01
2	종속변수	개별기관 점수		

5. 시사점

정보보호에 대한 최고경영층의 지원은 최고정보화담당관의 정보보호에 대한 관심과 정책 우선순위에 영향을 줄 수 있다. 본 연구는 최고경영층의 기관 운영 권한은 인력 자원, 재정적 자원, 시설 자원 등의 배분에 영향을 미칠 수 있고, 특히 부서간의 업무 조정 및 권한 부여에 상당한 영향을 미칠 수 있다고만 추정한다. 현재 공공기관의 정보보호관리실태 평가결과는 제도적으로 공공기관 최

고경영자의 업적 평가에 반영된다. 업적 평가 반영은 공공기관의 정보보호 거버넌스 수준을 향상시킬 수 있는 적절한 정책으로 판단된다. 공공기관 최고경영층의 지원이 공공기관 정보보호 거버넌스 수준에 영향을 미치는 유일한 요소로 나타났다면, 최고경영층의 정보보호에 대한 지원 형태, 강도, 횟수 등을 다양하게 측정할 필요가 있다. 그러나 본 연구는 설문조사를 통하여 최고 경영층의 지원을 측정하였으므로 한계가 있다. 추후 연구는 사례연구를 통하여 공공기관 최고 경영층의 정보보호 거버넌스 수준에 미치는 영향을 정교하게 수행할 필요가 있다.

최고 경영층의 지원이 정보보호 거버넌스에 영향을 미친다는 동 연구의 결과는 기존 연구 결과와 일치한다. 기존 연구는 최고경영층의 지원이 정보보호정책 성숙도나 신기술 도입에 영향을 미친다고 적시하고 있다[4, 19, 20]. 따라서 동 연구는 정보보호에 있어서 최고경영층의 지원이 가장 중요한 요인임을 확인하고 있다.

동 연구는 공공기관과 민간기관에 있어서 동일하게 최고경영층의 지원이 정보보호에 중요한 영향을 미친다는 이론적 시사점을 제공하고 있다. 따라서 민간기관이나 공공기관의 정보보호를 위해서는 최고경영층의 지원이 반드시 필요하다는 이론에 도달할 수 있다.

공공 기관 최고 경영층의 관심이 정보보호 거버넌스 수준에 어떤 경로로 영향을 미치는가에 대해서 추가 연구가 필요하다. 다만 정보보호를 위협하는 인식 및 기관장의 정보보호를 위협하는 인식은 통계적으로 검증되었으나 추가적인 연구를 통해서 검증이 필요하다. 동 연구와 기존 연구는 최고경영층의 정

보호에 대한 지원에 대한 의사결정과정이나 동기형성과정을 제시하지 않고 있다. 따라서 향후 연구는 최고경영층의 정보보호 지원 의사결정과정이나 동기형성과정 대한 연구가 필요하다.

둘째, ‘정보보호와 대국민 서비스 및 신뢰성’ 요인은 공공기관의 정보보호 거버넌스 수준에 영향을 미치지 않는다. 공공기관의 구성원은 정보보호가 기관 특유의 업무에 영향을 주지 않는 것으로 인식하고 있다. 정보보호의 중요성을 인식하지만, 정보보호가 개별 기관의 업무 성과 및 대국민 신뢰성과 직접적으로 연결이 되지 않는다고 인식하고 있다. 공공기관은 국민의 신뢰를 바탕으로 정책 결정 및 대국민 서비스를 제공한다. 공공기관은 기관이 제공하는 서비스의 품질 향상에 따라 국민으로부터 신뢰가 결정된다고 인식할 수 있다. 따라서 공공기관은 정보보호가 공공기관 고유 업무 향상이나 신뢰성 향상에 영향을 받지 않는다고 인식할 수 있다.

그러나 동 조사 실시 시점이 어느 정도 경과하였으므로 공공기관 구성원의 인식이 변할 수 있다. 따라서 동일한 모델을 사용하여 조사를 향후에 실시하면 다른 결과가 도출될 수 있다.

동 연구 결과는 기존 연구 결과와의 차이점을 나타내고 있다. 기존 연구는 정보보호 정책의 적극적인 수행은 조직성과 개선에 영향을 미친다고 밝히고 있다[25]. 그러나 동 연구 결과는 조직성과개선은 정보보호 거버넌스 수준에 전혀 영향을 미치지 못하고 있음을 밝히고 있다. 정보보호정책은 실행 가능성이 고려되지 않은 선언적 형태로 존재할 가능성이 높은 반면, 정보보호 거버넌스는 실

행 가능성이 전제 조건이다. 따라서 조직성과는 실행 가능성이 전제 조건인 정보보호 거버넌스 수준에 영향을 미치지 않을 수 있다. 따라서 본 연구는 성과개선과 정보보호 거버넌스에 영향을 미치지 않을 수 있음을 시사한다. 추후 본 요인은 민간기관을 대상으로 검증할 필요가 있다.

셋째, 공공기관 구성원의 정보보호인식과 문화는 공공기관의 정보보호 거버넌스 수준에 영향을 미치지 않는 것으로 나타났다. 공공기관 구성원의 정보보호인식과 문화가 정보보호 거버넌스 수준을 영향을 미치지 않는 이유는 조사 대상 공공기관 구성원의 낮은 정보보호 인식과 정보보호 문화의 부재 등이다.

공공기관의 자원배분, 특정 활동에 대한 중요성 인식, 권한 부여 등은 최고경영층의 지원만으로 해결될 수 없다. 최고경영층의 지원은 자원 배분과 업무 조정에 우선순위를 부여할 있지만, 공공기관 구성원 및 공공기관을 지배하는 암묵지를 변경할 수 없다. 암묵지는 형식화되지 않은 지식이지만 조직과 인간 행동을 결정하는 지식이다. 암묵지는 문화와 밀접한 관련이 있다. 따라서 공공기관 구성원의 정보보호 인식과 정보보호 문화 창출을 위해서는 정보보호의 중요성에 대한 교육과 절차 및 제도의 창출이 필요하다.

기존 연구는 정보보호문화는 정보보호와 밀접한 관련성을 제시하고 있어 동 연구의 결과와 배치된다. 본 연구 결과와 기존의 연구 결과가 배치되는 이유는 우리나라 공공기관의 정보보호문화가 아직 형성되지 않음을 반영할 수 있다. 따라서 향후 우리나라의 정보보호문화의 수준에 대해서 측정 연구를 수행할 필요가 있다.

6. 결 론

정보보호 거버넌스는 정보보호를 조직의 업무와 연계하고, 조직의 목적 달성을 위한 법, 제도, 최고경영층의 의사결정, 정보보호정책, 기술적 대책 등을 유기적으로 결합한 프로세스이다. 정보보호 거버넌스는 조직의 현재 정보보호 수준과 미래의 정보보호 수준을 결정하는 전략적 체계이며, 구체적 행위를 명시하는 체계이다. 본 연구는 거버넌스의 중요성을 인식하고, 공공기관의 정보보호 거버넌스 수준을 향상에 필요한 요인을 탐색하였다.

본 연구는 공공기관 정보보호 거버넌스 수준을 측정할 수 있는 모형을 탐색하고, 적합한 모형을 활용하여 공공기관 정보보호 거버넌스 수준을 측정하였다. 본 연구는 공공기관의 정보보호 거버넌스 수준에 영향을 미치는 요인을 통계적 방법을 통하여 도출하였다. 본 연구는 공공기관 정보보호 거버넌스 수준에 영향을 미치는 3가지 요인을 문헌연구를 통해서 추출 및 검증하였고, 최종적으로 ‘최고경영층의 지원’ 요인이 공공기관의 정보보호 거버넌스 수준에 영향을 미친다는 사실을 확인하였다.

본 연구의 결과를 정리하면 다음과 같다.

첫째, 주어진 여건 속에서 공공기관의 정보보호 거버넌스 수준을 향상시키기 위해서는 공공기관 최고경영층의 지원이 필수적이다. 따라서 향후 정부는 최고경영층의 정보보호에 대한 지원을 강화하기 위해서 최고경영층의 인식 개선 및 지원을 확대하고, 최고경영층을 대상으로 지속적인 교육 및 홍보가 필요하다.

둘째, 공공기관의 정보보호 거버넌스 수준

은 정보화 부서의 인원 규모에 의해서 영향을 받는다. 정보화 부서의 인원 규모가 크다는 의미는 정보보호를 전담하는 담당자가 확보가 가능하다는 의미를 내포하고 있다. 따라서 공공기관의 정보보호 거버넌스 향상을 위해서는 반드시 정보보호 담당자의 확보가 필요하다.

셋째, 정보보호 거버넌스 수준이 높은 공공기관은 정보보호 예산이 적절하다. 따라서 정보보호 예산의 확충을 위해서는 경영층의 지원 및 정보보호 문화의 정착이 필요하다.

공공기관의 정보보호 거버넌스를 강화하기 위해서 정부는 다양한 제도 및 활동을 추진하고 있다. 따라서 정보보호전담기관 및 정책입안자는 본 연구의 결과는 공공기관의 정보보호 거버넌스 수준 개선 활동 및 이론적 기초로 활용할 수 있다.

본 논문의 한계는 다음과 같다. 첫째, 본 연구가 사용한 설문조사는 최고경영층의 지원이 공공기관 정보보호 거버넌스에 영향을 미치는 원인, 최고 경영층의 지원의 종류, 최고경영층의 지원이 공공기관 정보보호 거버넌스 수준에 영향을 미치는 경로 등을 심층적으로 분석하지 못한다. 그러나 본 연구가 제시하는 ‘최고경영층의 지원’ 요인을 질적인 연구를 통하여 심층적으로 분석할 수 있는 토대를 마련하였다.

둘째, 본 연구가 사용한 조사 데이터가 시간이 경과하여 최신 상황을 반영하지 못하고 있다. 그러나 사회 현상이 1년~2년 내 쉽게 변하지 않는다. 따라서 2년 전 수행되었음을 감안하면 정보보호 거버넌스 수준과 관련된 현상의 변화는 크지 않을 수 있다. 다만 급격하게 변화하는 한국 사회의 특성을 감안하여

2년 주기의 종단 연구는 공공기관의 정보보호 거버넌스 변화를 관찰할 수 있다.

본 연구의 한계를 보완하기 위해서 향후 정보보호 거버넌스 수준이 향상 방법 등을 연구하는 질적 연구가 절실히 필요하다.

참 고 문 헌

- [1] 김정덕 외 1인, “정보보호 거버넌스 이슈 및 연구과제”, 정보보호학회지, 제17권, 제4호, 2007, pp. 2-8.
- [2] 김정덕, 이경석, “ISO/IEC JTC1 SC27의 정보보호관리 국제표준화 동향”, 정보보호학회지, 제18권, 제4호, 2008, pp. 1-4.
- [3] 김지숙 외 2인, “민간기업과 공공기관의 정보보호 관리체계 차이 비교”, 한국정보보호학회논문지, 제20권, 제2호, 2010, pp. 117-129.
- [4] 최명길 외 1인, “정보보호 패러다임 변화 및 정보보호동향에 대한 고찰”, 한국정보보호학회논문지, 제17권, 제4호, 2007, pp. 12-17.
- [5] 최명길 외 2인, “정보보호정책 성숙도 수준에 영향을 미치는 요인에 관한 연구”, 한국정보보호학회논문지, 제18권, 제3호, 2008, pp. 131-142.
- [6] 한국정보보호진흥원, “ISMS 인증제도 소개”, 2007, pp. 6-19.
- [7] 한근희, “전자정부 정보보호관리체계(G-ISMS) 적용 정책”, 한국정보보호학회논문지, 제19권, 제5호, 2009, pp. 119-131.
- [8] Ahmad Abu-Musa, “Exploring Information Technology Governance in Developing Countries : An Empirical Study”, The International Journal of Digital Accounting Research, Vol. 7, No. 13, 2007, pp. 71-117.
- [9] Ahmad Abu-Musa, “Information Security Governance in Saudi Organizations : An Empirical Study,” Information Management and Computer Security, Vol. 18, No. 4, 2010, pp. 226-276.
- [10] Allen J. H. and Westby, J. R., “Governing for Enterprise Security (GES) : Implementation Guide, Article 1 : Characteristics of Effective Security Governance,” White Paper, Carnegie Mellon University, Pittsburgh, P.A.
- [11] Beatty, R. C., Shim, J. P., and Jones, M. C., “Factors Influencing Corporate Web Site Adoption : a Time-Based Assessment,” Information and Management Vol. 38, 2001, pp. 337-354.
- [12] Birman, “KP, The Next-Generation Internet : Unsafe at Any Speed,” IEEE Computer, Vol. 30, No. 8, 2000, pp. 54-60.
- [13] Corporate Governance Task Force, “Information Security Governance : a Call to Action,” April 2004.
- [14] Faily S. and Fléchaïs, I., “Designing and Aligning e-Science Security Culture with Design,” Information Management and Computer Security, Vol. 18, No. 5, 2010.
- [15] Fulford, H. and Doherty, N. F., “The

- Application of Information Security Policies in Large UK-based Organizations : an Exploratory Investigation,” Information Management and Computer Security, Vol. 11, No. 3, 2003, pp. 106-114.
- [16] Huang, S.-M., Lee, C. L., and Kao, A. C., “Balancing Performance Measures for Information Security Management: a Balanced Scorecard Framework,” Industrial Management and Data Systems, Vol. 106, No. 2, 2006, pp. 242-255.
- [17] ISO17799, “A Code of Practice for Information Security,” 2005.
- [18] ITGI, “Information Security Governance, Guidance for Boards of Directors and Executive Management, 2nd Ed., IT Governance Institute, Rolling Meadows, IL, 2006.
- [19] B. Ives and Learmouth, G. P., “The Information Systems as a Competitive Weapon,” Communications of the ACM, Vol. 27, No. 12, 1984, pp. 586-603.
- [20] Joshi, K., “The Measurement of Fairness or Equity Perceptions of Management Information Systems Users,” MIS Quarterly, Vol. 13, No. 3, 1989, pp. 343-358.
- [21] Maria Karyda, Evangelos Kiountouzis, and Spyros Kokolakis, “Information Systems Security Policies : a Contextual Perspectives,” Computers and Security, Vol. 24, No. 3, 2004, pp. 246-260.
- [22] National Cyber Security Summit Task Force, Information Security Governance : a Call to Action, Corporate Governance Task Force Report, April, CS1/05-0047, available at www.technet.org/resources/IfoSecGov4_04.pdf.
- [23] Solm, B., “Information Security_The Forth Wave,” Computers and Security, Vol. 25, 2006, pp. 165-168.
- [24] Jeff Smith, H. S., Milberg, J. S., Burke, J., “Information Privacy : Measuring Individuals’ Concerns about Organizational Practices,” MIS Quarterly, Vol. 20, No. 2, 1996, pp. 167-196.
- [25] Swindle O. and Coner B., “The Link Between Information Security and Corporate governance,” May 2004.
- [26] Symon, V., “A Review of Information Systems Evaluation : Content, Context and Process,” Journal of Information Systems, Vol. 1, No. 3, 1991, pp. 205-212.
- [27] Whitman M. E. and Mattford H. J., “Principles of Information Security,” Course Technology, 2003, pp. 153-90.
- [28] William, “Information Governance,” Information Security Technical Report, Vol. 6, No. 3, 2001, pp. 60-70.

저 자 소 개

송정석 (E-mail : jssong@cau.ac.kr)
2004년 Michigan State (박사)
2004년~2006년 한국경제연구원 연구위원
2006년~현재 중앙대학교 부교수
관심분야 산업정책, 창업, 정보보호정책

최명길 (E-mail : mgchoi@cau.ac.kr)
2004년 한국과학기술원 (박사)
1995년~2000년 국방 과학연구소 연구원
2000년~2005년 한국 전자통신연구원 선임연구원
2005년~2008년 인제 대학교 조교수
2008년~현재 중앙대학교 조교수
관심분야 창업정책, 기술창업, 보안성평가, 정보보호정책 및 관리

전민준 (E-mail : daniel8151@wm.cau.ac.kr)
2000년~2008년 인제대학교 시스템경영공학과 학사 졸업
2009년~현재 중앙대학교 일반대학원 경영학과 (석사)
관심분야 온톨로지, 비즈니스 모델, 기술창업, 정보보호정책 및 관리