情 報 保 護 學 會 誌
第18卷 第6號, 2008. 12

국가기관의 정보보호수준 평가에 관한 연구

김 지 숙*, 최 명 길**

요 약

정보화 사회는 네트워크와 시스템에 대한 의존도가 큼에 따라 이에 대한 관리가 미흡할 경우 저장·유통되는 정보 및 자료의 위변조, 유출 등으로 인해 조직이 입는 피해는 금전적 손실뿐만 아니라 심할 경우 조직의 존립까지 위협할 수 있다. 이에 따라 정보보호의 중요성은 날로 증대하고 있으나 조직마다 다른 정보보호 접근 방법으로 인해 조직의 정보보호 수준은 차이가 심하다. 본 논문에서는 국제표준에 의한 정보보호 방법론적 요소들을 살펴보고 조직의 정보보호 수준에 영향을 미치는 요인이 무엇인지를 파악하여 조직의 정보보호 수준을 끌어올리기 위한 정책 방향 수립에 활용할 수 있도록 하고자 한다.

Ⅰ. 서 론

정보화 사회에서는 네트워크와 시스템에 의존하여 일상을 영위하고 사무를 처리하게 된다. 특히 사회의 각 조직들은 많은 개인정보들과 엄청난 양의 자료들을 서버와 PC에 저장하고 네트워크를 통해 유통하고 있다. 그런데 이에 대한 관리가 제대로 되지 않을 경우 비인가자에 의한 접근, 사용, 공개, 방해, 수정, 파괴 등이 발생할 수 있으며 정보시스템 자원(하드웨어, 소프트웨어, 펌웨어, 정보 및 데이터, 통신 포함)의 훼손, 변조, 유출 등으로 인해 조직의 피해는 금전적 손실뿐만 아니라 법적 소송에 휘말리거나 고객 신뢰의 상실 등 경영적 측면의 위험을 감수해야 하며 심할 경우 조직 존립의 위협에까지 이를 수 있다.

이에 각 조직들은 효율적인 정보보호를 위해 많은 노력을 기울이고 있다. 조직의 규모와 특성에 맞는 정보보호 시스템 도입과 인력 확충, 종사자에 대한 교육 등에 투자를 하고 있는 것이다. 그러나 기술의 발전 속도에 비하여 정보보호는 더디게 진행되고 있어 피해는 지속적으로 발생하고 있으며 피해규모는 더욱 더 증가하고 있는 추세다. 더욱이 조직마다 정보보호에 대한 접근 방법이 달라 조직의 정보보호 수준은 천차만별이다.

정보보호란 비인가자의 접근, 사용, 공개, 방해, 수정, 파괴로부터 정보와 정보시스템을 보호하여 궁극적으로 정보시스템 자원의 무결성, 가용성, 기밀성을 확보하는 것이다[1].

정보보호를 위한 일련의 활동을 정보보호 관리체계라고 할 때 여기에 적용되는 통제수단, 즉 정보보호 관리를 위한 방법론에 관한 많은 연구들이 수행되었는데 기술적 통제와 더불어 인적 통제, 운영 통제 및 교육 등 관리적 통제가 통합된 정보보호관리 방법론이 90년대 후반부터 등장하였다[2].

조직의 정보보호를 위해 인증된 방법론에 대한 필요는 영국에서 먼저 제기되어 BSI(British Standard Institute)에 의해 BS7799가 영국 표준으로 제정되었으며 이후 ISO17799로 채택되고 2005년 ISO/IEC 27000 시리즈로 국제표준으로 제정되었다[4].

ISO/IEC가 제정한 27000시리즈는 5가지로 분류되는데 ISO/IEC 27001은 PDCA (Plan-Do-Che-ck-Act) 프로세스에 의한 정보보호 요구서에 해당하며 27002는 정보보호 관리를 위한 실행지침서이다. 27003은 PDCA에 대한 실행지침서이며 27004는 정보보호 메트릭스와 측정에 관한 표준이다. 마지막으로 27005는 위험관리에 대한 표준이다.(이중 27004와 27005는 현재 draft 상태이다)[3,4]

본 논문에서는 ISO 27002에 규정한 정보보호 방법론적 요소들을 살펴보고 조직의 정보보호 수준에 영향을 미치는 요인이 무엇인지를 파악하여 조직의 정보보

* 고려대학교 박사과정 (주저자)
** 중앙대학교 조교수 (교신저자: mgchoi@cau.ac.kr)

호 수준을 끌어올리기 위한 정책방향을 수립하는데 활용할 수 있도록 하고자 한다.

Ⅱ. ISO 27002의 정보보호실행 요소

정보보호 관리체계 국제표준인 ISO/IEC 27000시리즈 중 하나인 ISO27002는 2007.7월 마련한 "정보통신기술과 정보보호 방안에 대한 실행지침서"이다. ISO 27002는 정보보호 관리체계를 구축하고 실행하며 유지하는 조직에 정보보호 관리에 대한 실행방안을 제공하여 조직의 정보보호 목표인 무결성, 기밀성, 가용성을 충족하도록 하고 있다.

ISO 27002에 규정한 정보보호 요소는 12개 항목으로 나누어지는데 세부 내용은 다음과 같다[4].

〔표 1〕 ISO 27002에 규정된 정보보호 요소

법규 및 지침	조직 내·외부적으로 반드시 지켜야 하는 법적 규제사항이나 지침으로 전자문서를 통한 회계작성 준칙이나 원본문서 보관 등 IT 관련 법·제도
정보보호 정책	조직 전반에 걸쳐 정보보호 정책이 효과적으로 운영되도록 명확한 정책 방향 제시 및 가시적 지원
정보보호 조직	조직의 정보보호 하부구조로 외부 접근 보안 및 아웃소싱에 대한 요구사항
자산관리	정보자산의 분류, 자산에 대한 책임, 자산의 처리 절차
인적 보안	직무 정의, 종사자의 입사, 보직 변경 및 퇴사 등에 대한 관리, 사용자 훈련, 교육
물리적·환경적 보안	시스템 보호를 위한 보안구역, 장비 보안, 일반적인 물리적 통제
운영관리	시스템과 네트워크의 기술적 보안 통제에 대한 관리로 운영절차와 책임, 시스템 계획 및 승인, 관리 유지, 유해 소프트웨어에 대한 보안, 네트워크 관리, 미디어 취급 및 보안, 정보 및 소프트웨어의 교환
접근 통제	접근 통제에 대한 사업 요구사항, 사용자 접근관리, 사용자 책임, 네트워크 접근 통제, 운영시스템의 접근 통제, 어플리케이션 접근 제어, 접근 및 사용의 모니터링 시스템
시스템 개발과 관리	시스템 보안 요구사항, 어플리케이션 시스템 보안, 시스템 파일 보안, 개발 및 지원 프로세스에서의 보안
정보시스템 사고 관리	침해사고 긴급 대응, 사고처리, 사후 조치
위험 관리	정보보호 시스템 운영, 취약점 분석, 모의 해킹
사업 연속성 관리	재해 재난 발생시 업무의 연속성을 유지하기 위한 계획으로 데이터 백업 등 복구 및 시스템 이중화 등 고객 서비스의 지속성 보장, 핵심 업무 기능을 지속하는 환경 조성

Ⅲ. 조직 정보보호에 영향을 미치는 요인

본 장에서는 정보보호 실행요소에 영향을 미치는 요인을 분석한다. 정보보호 수준에 영향을 미치는 요인을 파악하기 위해서 99개 국가기관을 대상으로 설문조사 및 모 국가기관의 정보보호수준 측정결과를 활용하여 조직 요인과 정보보호 수준간의 관련성 을 탐색한다.

1. 정보보호 수준에 영향을 미치는 요인 탐색

설문조사를 통해 각 기관의 정보보호수준에 미치는 요인을 먼저 탐색하고, 둘째, 도출된 요인과 기관의 정보보호수준에 실제로 영향을 미치는 요인을 검증한다. 셋째, 개별 기관의 정보화 부서의 특성이 기관의 정보보호수준에 영향을 미치는 원인을 탐색하였다.

본 설문분석은 개별 기관의 정보보호수준에 영향을 미치는 요인을 다음과 같이 3개의 요인으로 선정한다. 첫째, 기관의 정보보호수준은 최고경영층의 지원[5,6], 둘째, 정보보호와 기관의 고유 업무와의 관련성[7], 셋째, 기관의 정보보호에 대한 인식 및 문화 등이다[8,9]. 본 연구는 3개의 요인이 정보보호수준에 미친다고 가정하고, 설문 분석을 통해서 영향을 미치는 요인을 검증한다. [표 2]은 기관의 정보보호수준에 영향을 미치는 요인을 파악하기 위해 작성된 설문 항목과 각 요인간의 관련성을 보여주고 있다.

첫째, 각 기관 경영층의 정보보호에 대한 지원을 파악하기 위해서 다음과 같은 항목을 설문으로 조사했다. ① 기관장과 정보화부문 최고담당관의 정보보호에 대한 관심, ② 정보보호와 관련된 부서간의 협조, ③ 정보화 환경에서 증가하는 정보보호 위협에 대한 인식 등이다.

둘째, 정보보호가 기관의 고유업무 수행에 도움을 줄 것인가 하는 것이다. 이를 위하여 설문 항목을 ① 정보보호가 각 기관의 업무성과 및 경쟁력 향상에 도움이 되는지를 인식하는 여부, ② 정보보호와 각 기관에 대한 국민의 신뢰성 사이에 관련이 있는지를 파악하였다.

셋째, 정보보호수준과 기관내의 정보보호에 대한 구성원의 인식과 문화가 밀접한 관련이 있을 것이라는 가정 아래 ① 정보보호예산의 적절성 및 담당자의 권한, ② 기관의 구성원이 정보보호에 대한 우호적인 태도 등을 설문 항목으로 구성하였다. 다만 예산 및 담당자의 권한은 본 요인 수립에서 이를 문화 및 인식으로 설정하여 분석하고자 한다.

〔표 2〕 정보보호수준에 미치는 요인

요인	세부 요인	요인
경영층의 지원 (요인 1)	기관장의 정보보안에 대해 관심	1
	정보화최고담당관의 정보보안에 대해 관심	2
	기관내 정보보안과 관련된 타부서와의 협조	3
	기관의 정보보안 위협요인에 대한 인식	4
	기관을 위협하고 있는 정보보안 위협 요인 파악	5
정보보호와 대국민 서비스 및 신뢰성 (요인 2)	정보보안 활동 강화는 기관의 업무 성과를 저하	6
	정보보호정책 및 활동은 대국민 서비스의 품질 향상	7
	정보보호정책 및 활동이 기관 경쟁력 향상에 관계	8
	정보보호정책 및 활동이 기관의 신뢰성 증가	9
기관의 정보보호 업무에 대한 인식 및 문화 (요인 3)	정보보호예산의 적절성	10
	기관 구성원의 정보보안활동에 대해서 우호적	11
	기관장은 정보보안 담당부서에 필요한 권한 부여	12
	기관은 정보보호를 어려운 것으로 인식	13

2. 정보보호수준에 영향을 미치는 요인 검정

국가기관의 정보보호수준에 영향을 미치는 요인을 검증하기 위해서 조사된 설문 항목에 대해서 요인분석을 실시하였다. 요인분석은 특정한 현상에 영향을 미치는 요인을 발견하기 위해서, 조사된 설문 항목간의 관련성을 파악하여 특정한 요인으로 그룹화하여 결과를 도출하는 통계학적 기법이다. 본 논문에서 요인분석은 사전에 가정한 요인이 적절한지를 알아보고 개별 요인에 해당하는 설문 항목이 특정 요인을 구성하고 있는지를 파악한다.

설문조사 결과를 요인분석 기법을 사용하여 파악된 요인은 [표 3]과 같다. 요인분석 결과 설문조사 전에 가정한 요인이 대부분 동일하게 나타났다. 다만 설문항목 중 8은 요인1과 요인3에 동시에 나타났다. 그러나 값이 요인3에 많이 나타나서 요인3으로 묶었다.

3. 정보보호수준에 영향을 미치는 요인 검정을 위한 회귀분석

요인분석에서 도출된 요인은 기관의 정보보호수준에

〔표 3〕 가정요인과 설문항목간 요인분석 결과

세부요인 \ 요인	요인1 정보보호에 대한 경영층지원	요인 2 정보보호와 대국민 서비스 및 신뢰성	요인 3 정보보호에 대한 인식 및 문화
세부요인 5	0.7793	0.1038	0.2020
세부요인 6	0.7816	0.1129	0.2097
세부요인 9	0.6137	0.0842	0.5679
세부요인 10	0.6463	0.0920	0.4248
세부요인 11	0.8361	0.1081	0.0581
세부요인 12	-0.0054	0.7178	0.3181
세부요인 14	0.0173	0.7847	0.1537
세부요인 15	0.1653	0.8604	0.0609
세부요인 16	0.2390	0.7488	-0.0879
세부요인 4	0.1092	0.0214	0.6548
세부요인 7	0.4930	0.2479	0.6292
세부요인 8	0.5219	0.0946	0.6032
세부요인 13	0.1666	0.1660	0.7072

실제로 영향을 주고 있는지를 분석하기 위한 중간 과정이다. 따라서 개별 기관의 정보보호수준에 어느 요인이 영향을 주고 있는지를 알기 위해서는 도출된 요인과 실제 정보보호 수준측정 결과와의 관련성을 분석해야 한다. 관련성 분석을 위해서 개별 요인과 각 기관의 정보화수준 측정값간의 선형회귀분석을 실시하였다. 선형회귀분석 결과는 [표 4]와 같다.

〔표 4〕 요인과 정보보호 수준 측정치의 선형회귀분석

모형	요인	비표준화계수 (B)	표준오차	유의확률
1	상 수	58.02	4.79	0.00
	요 인 1	4.78	1.89	0.01
	요 인 2	2.16	1.56	0.17
	요 인 3	1.57	1.78	0.38
2	종속변수	개별기관의 정보보호수준 측정 점수		

선형회귀분석은 개별 요인과 개별 기관의 정보보호수준 측정값간의 관련성을 분석하는 기법이다. 개별 요인이 선형회귀분석에서 의미를 가지기 위해서는 유의도가 0.05이하가 되어야 한다.

본 선형회귀분석에서 개별 기관의 정보보호수준에 영향을 미치는 요인으로는 '경영층의 지원'으로 나타났다. 다른 요인은 개별 기관의 정보보호수준에 영향을 미

치지 않는 것으로 나타났다. 분석 결과는 해석하면 다음과 같다. 첫째, 정보보호에 대한 개별 기관의 경영층의 의지와 지원에 따라 정보보호를 위한 부서간의 협조가 이루어지고, 정보보호의 중요성이 강조됨에 따라 기관을 둘러싸고 있는 위협이 강조되고 있기 때문이다. 둘째, 정보보호와 대국민 서비스 및 신뢰성은 개별 기관의 정보보호 수준에 영향을 미치지 않는 것으로 나타났다. 두 번째 요인이 개별 기관의 정보보호 수준에 영향을 미치지 않는 이유는 공공기관은 특성상 국민의 신뢰를 받고 있으므로 개별 기관의 정보보호 수준에 영향을 미치지 않는다고 판단된다. 그리고 정보보호수준과 개별 기관의 업무 성과는 별개로 나타나고 있다. 셋째, 구성원의 정보보호인식과 문화는 개별 기관의 정보보호 수준에 영향을 미치지 않는 것으로 나타났다. 이는 각 기관 구성원이 정보보호 중요성에 대한 인식보다는 경영층의 지원과 관리가 더 중요하다고 인식하기 때문인 것이다.

4. 기관의 특성과 정보보호수준과의 관계 검증

기관의 정보부서의 특성과 정보보호수준과의 관계를 분석하였다[10]. 이를 위하여 설문 항목 1번에서 4번을 대상으로 분석하였으며, 분석결과 정보보호담당자와 개별 기관의 정보보호수준과는 관련성이 없다고 나타났다. 그러나 [표 5]에서와 같이 정보화관련부서의 인원, 정보보호예산과 개별 기관의 정보보호수준은 관련성이 있는 것으로 나타났다.

Ⅳ. 결 론

정보보호에 영향을 미치는 요인에 대한 분석은 해당 요인의 강화를 통해 조직의 정보보호 수준을 향상시키는 데 목적이 있다.

〔표 5〕 정보화 부서의 특성과 정보보호 수준간 선형회귀분석

모형	요인	비표준화계수 (B)	표준오차	유의확률
1	정보화부서 인원	2.24	0.74	0.00
2	종속변수	개별기관 정보보호 수준		
1	정보보호예산	2.63	1.03	0.01
2	종속변수	개별기관 점수		

이상에서 분석한 결과 정보보호에 영향을 미치는 요인으로는 경영층의 지원, 정보화부서의 인원, 정보보호 예산 등으로 나타났다. 검증 결과를 토대로 다음의 결론을 얻을 수 있다.

첫째, 주어진 여건 속에서 조직의 정보보호 수준 향상을 위해서는 개별기관 경영층의 지원이 필수적인 것으로 확인되었다. 따라서 향후 각 조직은 정보보호 수준의 향상을 위해서 경영층의 인식 개선 및 지원 확대를 위해서 경영층을 대상으로 지속적인 교육 및 홍보가 필요할 것으로 기대된다. 둘째, 정보보호 수준은 정보보호 담당자의 노력만으로 이루어질 수 없고, 정보화 부서의 인원에 의해서 영향을 받는다. 즉, 정보보호 수준의 향상은 정보보호담당자 뿐만 아니라 관련 부서의 협조 및 인원의 지원을 통해서 이루어진다는 것을 알 수 있다. 셋째, 기관의 특성을 고려한 장기적인 정보보호예산 확충이 필요하다. 정보보호예산은 여러 가지를 고려해야 하므로 적절한 정보보호예산 확보를 위한 경영층의 이해와 지원이 필요할 것으로 보인다.

본 연구 결과 국제표준에 규정한 정보보호 요소가 효과적으로 실행되기 위해서는 경영층의 지원과 정보화 부서의 인원, 정보보호 예산이 조직의 정보보호 목표에 합당하게 설정되어야 하며 이들 요인에 대한 적정 투자를 통해 조직의 정보보호 목표를 달성할 수 있을 것이다.

참고문헌

[1] 최 명길 외 2인, "정보보호정책의 성숙도에 미치는 요인에 관한 연구", 정보보호학회논문지, 제18권, 제3호, 2008년 3월.

[2] NIST, An Introduction to Computer Security; The NIST handbook ,NIST, 1999

[3] Don Holden, "ISO 17799 Security Standa -rd; How will It fit with other standards", CISSP-ISSMP, pp. 10~15 2006

[4] BS7799 정보보안 경영시스템,http://www. dnv.co.kr/binaries/BS7799 description, tcm34-89786.pdf. pp. 1~4

[5] S. Banerjee and D.Y. Golhar, "Electronic Data Interchange : Characteristics of Users and Nonusers", Information and Management 26(2),

pp.65-74, 1994.

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

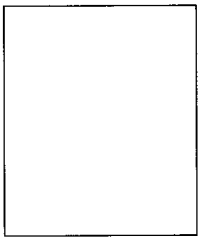
[7] R. C. Beatty, J. P. Shim and M. C. Jones, "Factors Influencing Corporate Web Site Adoption : a Time-Based Assessment", Information & Management 38, pp.337-354, 2001.

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

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

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

〈著者紹介〉



김 지 숙 (Kim Ji Sook)
2007년 3월~현재 : 고려대학교 정보경영공학전문대학원 박사과정 재학
관심분야:정보보호정책,정보보호수준평가, 정보보호관리

최 명 길 (Myeonggil Choi)
종신회원
2004년 : 한국과학기술원 박사
2005년~2007년:인제대학교 조교수
2008년~현재:중앙대학교 조교수
관심분야: 보안성평가, 홈네트워크 보안, 정보보호정책 및 관리