부합성 분석을 통한 정보보안 평가지표 도출

이영규*, 김상훈**

*중소기업기술정보진흥원, **광운대학교 경영정보학과

A Development of Evaluation Indicators for Information Security by means of the Coincidence Analysis

Lee, Yeongkyu, Kim, Sanghoon

TIPA, Kwangwoon University

E-mail : yklee@tipa.or.kr, shkim@kw.ac.kr

요 약

정보화의 진전과 더불어 삶의 편이성은 증대되고 있으나 개인과 조직은 물론이고 국가에 이르기까지 정보보안 사고로 피해와 고통 또한 증대되고 있는 실정이다. 이러한 사고로 인한 피해를 사전에 예방하거나 사후 손실을 최소화하기 위해서는 적절한 관리가 필요하며 이를 위해서는 무엇보다 실용적인 정보보안 평가지표의 개발이 필요하다. 본 연구에서는 정보보안을 대표하는 문헌을 참조하여 평가지표를 도출하고, 일련의 부합성 분석을 통해 보다 실용적인 정보보안 평가지표를 도출하여 제시하고자 한다.

1. 서론

정보화는 정보의 공유와 활용을 자유롭게 하여 이익을 극대화하고 편익을 증진시키는 등의 순기능적 역할을 하고 있는 반면, 중요 정보의 위·변조, 기술 유출, 사이버 테러 등을 불러일으켜 금전적 피해는 물론 명예 및 이미지 훼손 등으로 개인과 조직에 커다란 고통을 안겨주기도 한다. 이러한 역기능에 따른 피해와 손실을 최소화하기 위해 정보보안의 중요성이 나날이 커지고 있으며, 이를 극복하기 위해서는 무엇보다도 정보보안을 평가할 수 있는 체계를 마련하여 정보보안을 진단하고 발생가능한 문제나 발생된 문제를 해결할 수 있도록 해야 한다. 기존 연구의 경우 평가를 위한 지표의 구체성이 떨어지거나 일관성 확보가 어려워 현실적인 도움이 미흡한 실정으로 이는 적합한 평가지표를 도출하지 못했음을 의미한다고 볼 수 있다. 본 연구에서는 정보보안 평가에 대한 기존의 연구들 검토하여 평가영역과 평가지표를 도출하고, 도출된 평가지표가 실제 업무수행에 얼마나 적합한지 보안 전문가를 대상으로 일련의 부합성 분석을 실시하여 보다 실제적인 정보보안 평가지표를 제시하고자 한다.

2. 정보보안 평가영역 도출

정보보안의 제반적 측면을 체계적으로 평가하고 평가결과의 신뢰성과 유용성을 보장할 수 있는 평가영역을 개발하기 위한 노력이 지속되고 있지만 이론적 접근이 주류를 이루고 있어 현장의 실무적인 요구와 차이가 존재하여 평가활동이 활성화 되지 않고 있는 실정이다. 정보보안 평가영역은 연구별로 기준이나 명칭에서 다소 차이를 보이고 있지만 주요 문헌[ISO27001(2005), BS7799(2002), KISA-ISMS(2002), 김현수(1999), NIST SP800-53A(2006), 김정덕, 김기윤(1998)]을 토대로 보안정책, 보안조직, 자산관리, 인원보안, 물리적·환경적 보안, 통신 및

운영관리, 접근통제, 정보시스템 도입·개발·유지보수, 준거성으로 구성되어 있음을 알 수 있다.

3. 정보보안 평가영역별 평가지표 도출

3.1 보안정책

보안정책은 보안측면에서의 목표와 방향을 제시하고 있는 중요한 문서로, 최고경영자의 확고한 의지가 무엇보다도 중요하다. 이에 대한 선행연구[ISO27001(2005), BS7799(2002), KISA-ISMS(2002), 고일석, 김진영(2002), 김현수(1999), 김정덕, 김기윤(1998)]를 종합적으로 고찰한 결과 보안정책이 ① 경영목표, IT목표와 일관성을 유지되는지 ② 지침·표준·절차로 세분화하여 체계적으로 관리되는지 ③ 유효성을 유지하기 위해 정기적·비정기적으로 검토되는지를 주 내용으로 하는 5개의 평가지표를 도출하였다.

3.2 보안조직

본 영역에서는 보안업무를 적절하게 수행·유지·관리하기 위해 내부조직과 외부기관을 통해 발생가능한 위험을 분석하고 이에 따른 보안대책을 수립하는지에 대해 평가함에 있다. 이에 대한 선행연구[ISO27001(2005), BS7799(2002), KISA-ISMS(2002), 고일석, 김진영(2002), 김현수(1999), 김정덕, 김기윤(1998)]를 종합적으로 고찰한 결과 내부조직관리와 외부기관관리 항목으로 구성됨을 알 수 있다. 내부조직관리에서는 보안 담당조직의 보안업무 추진과 관련하여 ① 보안업무를 적절하게 기획·조정·관리하는지 ② 각 부서의 보안업무가 원활하게 수행되도록 지원하는지를 포함하는 6개의 평가지표를 도출하였고, 외부기관관리에서는 외부기관과의 접촉에 따른 안전을 목적으로 ① 고객의 접근에 따른 보호대책을 수립하는지 ② 제 3자와의 계약 시 보안요구사항과 보안책임 등을 식별하고 관리하고 있는지를 포함하는 3개의 평가지표를 도출하였다.

3.3 자산관리

자산은 조직의 비즈니스를 수행하거나 성공하기 위해 반드시 필요한 요소로 올바르게 관리하고 적절하게 보호되어야 한다. 이에 대한 선행연구[ISO27001(2005), BS7799(2002), KISA-ISMS(2002), 고일석, 김진영(2002), 김현수(1999), 김정덕, 김기윤(1998)]를 종합적으로 고찰한 결과 자산현황을 파악하고, 관리책임을 명확하게 하며, 비용 대비 효과를 고려하여 중요도별로 적절하게 분류하여 관리하는지를 포함하는 5개의 평가지표를 도출하였다.

3.4 인원보안

본 영역에서는 이해관계자를 대상으로 보안대책을 수립하는지와 보안사고 발생에 효과적으로 대응하기 위해 사전 대책을 마련하고 교육훈련을 실시하는지를 평가함에 있다. 이에 대한 선행연구[NIST SP800-53A(2006), ISO27001(2005), BS7799(2002), KISA-ISMS(2002), 고일석, 김진영(2002), 김현수(1999), 김정덕, 김기윤(1998)]를 종합적으로 고찰한 결과 인적자원관리와 보안사고관리 항목으로 구성되어 있음을 알 수 있다. 인적자원관리에서는 조직과 관련이 있는 임직원이나 이해관계자에 의한 실수, 오용 등으로부터 위험을 감소시키기 위해 ① 채용 시 고용계약서에 보안책임을 명시하는지 ② 고용기간동안 보안정책의 이행과 보안교육을 실시하는지를 포함하는 8개의 평가지표를 도출하였고, 보안사고관리에서는 보안사고 발생 시 신속한 대응을 위해 ① 대응절차를 수립하고 정기적으로 훈련을 실시하는지 ② 예상되거나 관찰되는 보안취약점에 대해 적절한 채널을 통해 보고하는지를 포함하는 7개의 평가지표를 도출하였다.

3.5 물리적·환경적 보안

본 영역은 정보처리설비를 갖춘 구역을 안전하게 보호하기 위해 보안구역을 설정하고 통제대책을 마련하고 있는지와 재난이나 재해가 발생하는 경우에도 조직의 중요 업무가 지속적으로 수행되도록 업무연속성관리를 적절하게 수행하고 있는지를 평가함에 있다. 이와 관련 선행연구[NIST SP800-53A(2006), ISO27001(2005), BS7799 (2002), KISA-ISMS(2002), 고일석, 김진영(2002), 김현수(1999), 김정덕, 김기윤(1998)]를 종합적으로 고찰한 결과 보안구역관리, 정보처리설비관리, 업무연속성관리의 항목으로 구성되어 있음을 알 수 있다. 보안구역관리에서

는 민감한 정보처리설비구역을 대상으로 비인가적 접근, 손괴, 방해 등으로부터 안전하게 보호해야 한다. 이에 따라 ① 중요 정보처리설비가 위치해 있는 장소에 대해 보안구역으로 설정하여 적절하게 관리하는지를 포함하는 5개의 평가지표를 도출하였고, 정보처리설비관리에서는 정보처리설비의 안정적 운영을 위해 ① 중요 정보처리설비를 보호하기 위해 적절한 온도와 습도를 유지하는지 ② 안정적인 전원공급 및 통신을 운영하는지를 포함하는 6개의 평가지표를 도출하였다. 업무연속성관리에서는 각종 재해나 재난으로부터 중요 업무의 지속을 위해 ① 업무연속성 보장을 위한 요구사항을 파악하고 있는지 ② 재난이나 재해에 따른 대응방안을 마련하고 있는지를 포함하는 4개의 평가지표를 도출하였다.

3.6 통신 및 운영관리

본 영역의 중점은 정보처리설비를 올바르고 안전하게 보호하고 있는지에 대해 평가함에 있다. 이에 대한 선행연구[NIST SP800-53A(2006), ISO27001(2005), BS7799(2002), KISA-ISMS(2002), 고일석, 김진영(2002)]를 종합적으로 고찰한 결과 운영절차 및 책임, 제 3자서비스 인도관리, 시스템 운영관리, 네트워크 보안관리, 매체관리, 정보교환관리 항목으로 구성되어 있음을 알 수 있다. 운영절차 및 책임에서는 정보처리설비의 안전한 운영을 위해 ① 책임소재를 분명히 하고 있으며, 운영절차를 수립하고 있는지 ② 변경 시 사전승인이나 실패 시 복구대책 마련 등의 대책을 수립하고 있는지를 주 내용으로 하는 4개의 평가지표를 도출하였고, 제3자서비스 인도관리에서는 최근 경영효과 및 효율을 극대화하기 위한 방안으로 아웃소싱이 증가되고 있음에 따라 ① 제3자 서비스 이용 시에는 서비스 제공수준에 대한 명확한 합의가 있는지 ② 정기적으로 서비스 이용에 대한 기록을 검토하는지를 평가하는 2개의 지표를 도출하였다. 시스템 운영관리에서는 시스템 운영 시 가용성과 무결성을 확보하기 위해 ① 시스템 인수 시 관련 기준에 의거 테스트하는지 ② 시스템의 용량과 성능에 대해 정기적으로 모니터링하는지를 포함하는 9개의 평가지표를 도출하였으며, 네트워크 보안관리에서는 네트워크 보안을 위해 ① 접속기록 검토, 시스템과의 운영분리 등 보안통제를 수행하는지 ② 제3자서비스 이용과 관련해서는 서비스협정서에 서비스 수준, 보호대책 등을 포함하는지를 포함하는 3개의 지표를 도출하였다. 매체관리에서는 비인가적 접근이나 오용 그리고 손괴 등으로부터 매체를 안전하게 보호하는지를 주 내용으로 하는 3개의 지표를 도출하였고, 정보교환관리에서는 조직내부 직원 간 또는 조직 간 정보교환 시 정보의 손실, 변조, 오용을 방지하기 위해 ① 사전에 위험을 분석하여 적절한 대책을 수립하고 있는지 ② 전자우편이나 전자상거래 정보의 전송 시 암호화 등의 보호대책을 수립하고 있는지를 포함하는 6개의 평가지표를 도출하였다.

3.7 접근통제

본 영역의 중점은 중요 정보에 대한 비인가적 접근을 통제하는지에 대해 평가함에 있다. 이에 대한 선행연구[NIST SP800-53A(2006), ISO27001(2005), BS7799 (2002), KISA-ISMS(2002), 고일석, 김진영(2002)]를 종합적으로 고찰한 결과 사용자 책임 및 접근관리, 네트워크 접근통제, 운영시스템 접근통제, 어플리케이션 및 정보 접근통제, 모바일 컴퓨팅 및 텔레워킹 항목으로 구성되어 있음을 알 수 있다. 첫째 사용자 책임 및 접근관리에서는 정보시스템과 정보의 안정적 운영과 보호를 위해 ① 사용자 접근권한을 부여하는 공식적인 절차가 마련되어 있는지 ② 사용자 접근권한이 등록단계로부터 삭제 시까지 적절하게 관리되는지를 포함하는 8개의 지표를 도출하였고, 둘째, 네트워크 접근통제에서는 내부 및 외부 네트워크 서비스에 대한 비인가 접근을 통제하기 위해 ① 원격사용자의 내부접근을 통제하는지 ② 서비스별, 사용자별 네트워크 서비스를 분리 운영하는지를 포함하는 5개의 지표를 도출하였다. 셋째, 운영시스템 접근통제에서는 운영시스템에 대한 비인가 접근을 통제하기 위해 ① 사용자별·그룹별 별도의 계정을 부여하는지 ② 안전한 패스워드를 사용하는지를 주 내용으로 하는 5개의 지표를 도출하였고, 넷째, 어플리케이션 및 정보 접근통제에서는 정보시스템에 저장된 정보에 대한 비인가적 접근을 통제하기 위해 ① 어플리케이션에 대한 접근을 제한하는지 ② 중요 정보시스템을 일반

시스템과 별도로 분리하여 운영하는지를 평가하는 2개의 지표를 도출하였다. 다섯째, 모바일 컴퓨팅 및 텔레워킹에서는 PDA, 노트북, 휴대폰 등 모바일 컴퓨터 장비를 적절하게 보호하며, 외부에서 작업 시 절도나 노출 등에 대비하여 적절한 보안대책을 적용하는지를 평가하는 2개의 지표를 도출하였다.

3.8 정보시스템 도입·개발·유지보수

본 영역의 중점은 정보시스템의 도입·개발·유지보수과정에서 ① 안전성과 무결성, 그리고 신뢰성을 유지하는지 ② 데이터의 정확성과 무결성 유지를 위해 적절하게 통제하는지를 평가함에 있다. 이에 대한 선행연구[ISO27001(2005), BS7799(2002), KISA-ISMS(2002)]를 종합적으로 고찰한 결과 어플리케이션의 정확한 처리, 암호통제, 시스템파일보안, 개발 및 지원프로세스보안 항목으로 구성되어 있음을 알 수 있다. 첫째, 어플리케이션의 정확한 처리에서는 어플리케이션 프로그램이 실행되는 과정에서 입력·처리·출력 데이터의 손실, 변조, 오용을 막기 위한 지침을 수립·이행하는지를 포함하는 3개의 지표를 도출하였고, 둘째, 암호통제에서는 정보의 기밀성·무결성 유지와 관련하여 암호솔루션 적용을 위한 정책의 수립 여부와 암호 키의 안전한 보호대책을 수립하고 있는지를 평가하는 2개의 지표를 도출하였다. 셋째, 시스템 파일보안에서는 시스템 파일을 안전하게 보호하기 위해 S/W 설치 시, 시험데이터 선택 시, 소스코드 접근 시, 이에 대한 적절한 보안대책을 수립하여 이행하고 있는지를 평가하는 3개의 지표로 구성되며, 넷째, 개발·지원프로세스 보안에서는 IT프로젝트 진행과정에서 ① 개발 초기단계부터 보안요구사항을 반영하는지 ② 변경 시 공식적인 절차를 수립하여 이행하는지를 하는지를 포함하는 6개의 지표를 도출하였다.

3.9 준거성

본 영역의 중점은 조직과 관련이 있는 법, 규정, 계약서 등을 검토 이행하도록 함에 있다. 이에 대한 선행연구[ISO27001(2005), BS7799(2002), KISA-ISMS(2002)]를 종합적으로 고찰한 결과 법적요구사항 준수와 보안감사의 2개 항목으로 구성되어 있음을 알 수 있다. 법적 요구사항 준수에서는 법, 규정, 계약 등의 법적 요구사항에 대해 불이행이나 위반이 발생하지 않도록 ① 법적 요구사항에 대해 문서화하는지 ② S/W 저작권 등 지적재산권에 대한 보호대책을 마련하는지를 포함하는 4개의 지표를 도출하였고, 보안감사에서는 ① 신중하게 감사계획을 수립하여 이행하는지 ② 감사가 완료되더라도 지속적으로 사후관리 하는지를 포함하는 4개의 지표를 도출하였다.

4. 부합성 분석을 위한 연구설계

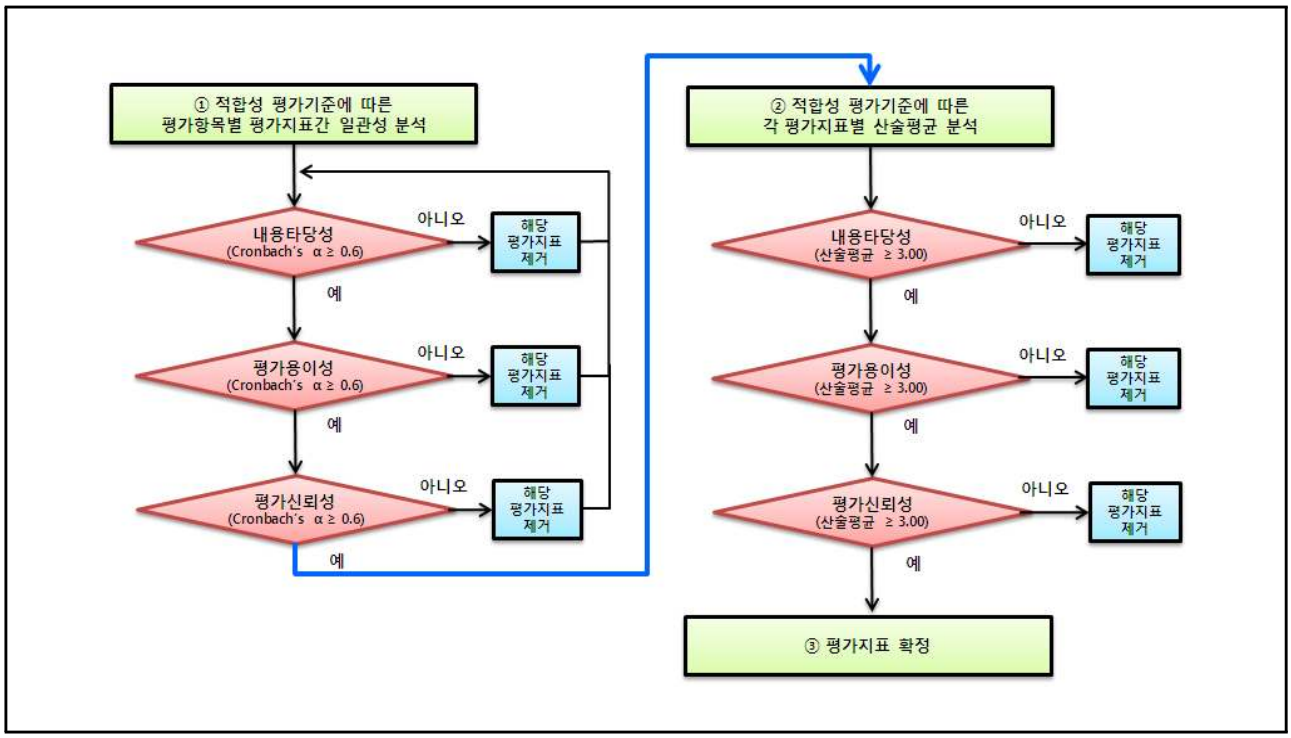
4.1 부합성 분석의 의의

부합성 분석이란 정보보안 평가를 위해 도출된 각 평가항목의 평가지표를 실제로 평가업무에 적용함에 있어서 평가의 용이성과 평가의 신뢰성, 그리고 내용적인 적합성이 어느 정도 확보되어 있는지를 검증하는 것(중소기업청, 중소기업정보화경영원, 2005)으로 일반적인 설문조사 작업 시 본 조사에 앞서서 실시하는 일종의 사전조사(pilot test)와 그 맥락을 같이한다. 즉, 평가지표의 내용이나 사용된 용어가 너무 어렵다거나, 너무 많은 시간이 소요되거나, 질문의 순서가 자연스럽지 않는 등의 예상치 못한 문제점들에 대해 점검하는 것(안광호, 임병훈, 2004)을 비롯하여, 실질적 결과를 제시할 수 있는 평가지표를 선정하여 적용가능성이 높은 평가지표를 도출하는데 의의가 있다고 할 수 있다.

4.2 부합성 분석을 위한 평가기준 설정 및 설문개발

평가지표 선정과 관련하여 Hatry(1980)와 Rosen(1993)은 시의적절성, 신뢰성, 이해가능성, 타당성, 독창성, 정확성, 통제성, 역행태의 유발가능성, 자료수집비, 종합성, 명확성, 통제성, 민감성, 현실성, 종합성을 고려해야 한다고 제시하였고, Lefrancois(1984)는 이해가 쉽고, 사용이 간편하며, 관리가 용이하고, 비용대비 효과적이어야 한다고 하였으며, 김정유, 이승아(2001)는 획득가능성, 측정가능성, 일관성이 충족되어야 함을 강조하였다. 본 연구에서는 위 평가지표 선정을 위한 평가기준의 요구사항을 고려하여 앞서 3장에서 도출된 120개의 평가지표들을 대상으로 내용타당성, 평가용이성, 평가신뢰성

[그림 1] 정보보안 평가지표의 부합성 분석절차



측면에서 부합성 분석을 실시하고자 한다.

4.3 부합성 분석을 위한 자료수집

앞서 도출된 평가지표의 부합성에 대한 분석을 위해 정보보안과 관련이 있는 83명으로부터 유효한 응답을 받았다. 이들은 주로 보안컨설턴트, 보안담당자, 연구원으로 구성되었다. 이들을 직위별로 살펴보면 과장급이 31명(37.3%), 대리급 14명(16.9%), 임원급 14명(16.9%), 부장급 11명(13.3%), 사원급 8명(9.6%), 기타 5명(6%)이고, 경력별로 살펴보면 5년 ~ 10년 미만이 34명(41%), 1년 ~ 3년 미만 20명(24.1%), 3년 ~ 5년 미만 12명(14.5%), 10년 초과 10명(12%), 1년 미만 7명(8.4%) 순이다.

5. 부합성 분석

5.1 부합성 분석절차

부합성 분석은 앞서 도출된 120개의 평가지표가 적합한가에 대해 설문조사를 통해 실증적으로 분석하는 과정으로 김상훈, 최점기(2006)의 연구를 응용하여 [그림 1]과 같이 ① 평가항목별 평가지표 간 일관성 분석 → ② 평가지표별 산술평균 분석 → ③ 평가지표 확정 순으로 진행하였다.

5.2 부합성 분석의 실행

5.2.1 평가항목별 평가지표의 일관성 분석

일관성이란 동일한 개념에 대해 측정을 되풀이했을 때 동일한 측정값을 얻을 가능성을 의미하는 것(최점기, 2006)으로 본 연구에서는 평가항목을 구성하고 있는 각 평가지표의 내용타당성, 평가용이성, 평가신뢰성에 대한 일관성이 어느 정도인지를 확인하기 위해 Cronbach's α를 이용하였다([그림 1]의 ①참조). 설문조사 결과를 분석한 결과 Cronbach's α는 모두 0.6이상으로 나타나 Nunally(1978)가 주장하는 허용기준(0.6)을 상회하였다. 평가용이성 측면과 평가신뢰성 측면에서도 Cronbach's α가 모두 0.6이상으로 나타났다. 이를 통해 앞서 3장에서 도출된 26개의 평가항목과 120개의 평가지표들이 일관성이 있음을 알 수 있다.

5.2.2 평가지표별 산술평균 분석

본 연구에서는 보다 적합한 평가지표를 도출하고자 일관성분석 외에 평가지표별 산술평균을 통해 부합성을 판정하는 절차를 포함하였다([그림 1]의 ②참조). 부합성 분석을 위한 설문조사가 Likert 5점 척도를 기반으로 하였기 때문에 산술평균값인 3.0을 판정기준으로 설정하였으며 내용타당성, 평가용이성, 평가신뢰성 중에 어느 하나만이라도 위 판정기준에 미달하는 경우에는 평가가 용이하지 않거나, 평가내용을 신뢰할 수 없다거나, 평가와 관련성이 없다고 판단하여 평가지표에서 제거하고자 하였다. 평가지표별 산술평균 분석결과 내용타당성, 평가용이성, 평가신뢰성별 모두 판정기준이 되는 3.0이상으로 나타났다. 따라서 앞서 도출한 평가항목 및 평가지표들이 평가에 적합하다는 타당성을 충분히 확보하고 있다는 것을 알 수 있다.

6. 결 론

본 연구에서는 정보보안을 대표하는 연구 및 문헌들에 대한 포괄적인 고찰을 통해 26개의 평가항목 그리고 120개의 평가지표들을 도출하였다. 이후 앞서 도출된 평가지표들이 얼마나 실무에 적합한지를 분석하기 위해 내용타당성, 평가용이성, 평가신뢰성의 3가지 평가기준을 설정하였고, 보안전문가를 대상으로 설문조사를 통해 부합성 분석을 실시하였다. 부합성 분석은 ① 평가항목별 평가지표간 일관성 분석 → ② 평가지표별 산술평균 분석 → ③ 평가지표 확정 순으로 진행하였다. 우선 평가항목별 평가지표 간 일관성 분석결과 모두 일관성이 확보되어 있음을 알 수 있었으며, 다음 산술평균 분석에서도 도출된 평가지표별 판정기준이 되는 값인 3.0이상으로 나타나 120개의 평가지표가 정보보안 평가에 모두 적합하다는 것을 알 수 있다.

본 연구의 의의로는 정보보안 평가 시 간과되었던 부합성 분석을 위한 기준과 분석절차를 체계적으로 확립했다는 것과 이를 통해 120개의 정보보안 평가지표를 합리적으로 도출했다는 것에 큰 의의가 있다고 볼 수 있다. 본 연구의 제한사항으로는 평가지표를 도출과정에서 방법론에 대한 제시가 미흡하였고, 산술평균 분석을 통한 평가지표들의 부합성 여부 판단을 위한 기준치를 3.0으로 설정한 것은 다소 임의적이라고 할 수 있음으로 향후 이에 대한 실증적 차원의 연구가 필요하다고 볼 수 있다. 아울러 일련의 부합성 분석을 통해 도출된 평가지표를 이용하여 실제적으로 평가를 실시하여 검증해보는 실증분석도 수반되어야 할 것이다.

[참고문헌]

[1] 고일석, 김진영 외, 「정보보호수준 평가항목 및 방법론 개발」, 한국정보보호진흥원, 2002.

[2] 김상훈, 최점기 외, "부합성 분석을 이용한 정보화지원사업 성과평가지표의 합리적 도출 방안", 「한국데이타베이스학회」, 제13권, 제3호, 2006, pp.145-179.

[3] 김정덕, "정보보호 분야의 평가방법론 및 지표 개발", 「산업경영연구」, 제12권, 제2호, 2003, pp.21-39.

[4] 김정덕, 김기윤, 「정보보호지표 항목개발 및 계량화 연구」, 한국정보보호센터, 1998.

[5] 김현수, "정보보안수준 계량화 연구", 「한국경영정보학회」, 제9권, 제4호, 1999, pp.181-201.

[6] 임용현, 「정보보호 수준의 자가 평가 모델」, 석사학위논문, 전남대학교, 2004.

[7] 중소기업청, 중소기업정보화경영원, 「중소기업 정보화 지원정책 성과평가체계 연구」, 2005.

[8] 한국정보보호진흥원(KISA), 「정보보호 관리체계 인증 규격」, 2002.

[9] Hatry, Harry P., *Productivity and Motivation : A Review of State and Local Government Initiatives*, Urban Institute Press, 1980.

[10] ISO/IEC, ISO17799 *: Code of Practice for Information Security Management*, 2005.

[11] ISO/IEC, *ISO27001 : Specification for information security management systems*, 2005.

[12] Lefrancois, R., "A Challenge for the 1980s : Productivity", *Cost & Management*, Vol.58, No.1, 1984, pp.55-59.

[13] NIST, *Guide for Assessing the Security Controls in Federal Information Systems*, NIST Special Publication 800-53A, 2006.

[14] Nunally, J. C., *Psychometric Theory*, New York, McGraw Hill, 1978.