韓國IT서비스學會誌
第7卷 第3號
2008年 9月

부합성 분석을 통한 정보보안 평가지표 개발*

이영규** · 김상훈***

A Development of Evaluation Indicators for Information Security by Means of the Coincidence Analyses*

Yeongkyu Lee** · Sanghoon Kim***

■ Abstract ■

The wide spread of the Internet has become a momentum to promote informatization, and thus individuals, organizations, and government bodies are competitively participating in this kind of new wave. Informatization enables us not only to circulate and utilize information without any limitation but also to maximize users' benefits and convenience. On the other hand, it brings about negative effects-security incidents such as cyber terror, Internet fraud and technology leakage, etc. Evaluation on security level should precede over all the others in order to minimize damage by security incidents since it diagnoses current status on security as it is and can be used as a guideline for appropriate security management. In this study, evaluation domains, items and indicators of information security to evaluate information security are theoretically developed on the basis of critically reviewing the major existing research. And then the coincidence level(content validity, ease and reliability of evaluation) of each evaluation indicators are empirically analyzed through performing the field study of 83 information security experts.

Keyword : Information Security, Information Security Evaluation, Coincidence Analyses

논문투고일 : 2008년 07월 18일 논문수정완료일 : 2008년 09월 08일 논문게재확정일 : 2008년 09월 18일
* 이 논문은 2008년도 광운대학교 교내학술연구비 지원에 의해 연구되었음.
** 중소기업기술정보진흥원 차장
*** 광운대학교 경영정보학과 교수

1. 서 론

정보화는 정보의 공유와 활용을 자유롭게 하여 이익을 극대화하고 편익을 증진시키는 등의 순기능적 역할을 하고 있는 반면, 중요 정보의 위·변조나 기술 유출, 사이버 테러 등을 불러일으켜 금전적 피해는 물론 명예 및 이미지 훼손 등으로 개인과 조직 그리고 국가에 커다란 고통을 안겨주기도 한다. 이러한 역기능에 따른 피해와 손실을 최소화하기 위해 보안의 중요성이 나날이 커지고 있으며, 이를 극복하기 위해서는 무엇보다도 정보보안을 평가할 수 있는 체계를 마련하여 체계적으로 추진할 수 있도록 방향을 제시하고 효율성을 제고해야 하는 필요성이 증대되고 있다. 이와 관련하여 정보보안 평가에 대한 기존 연구들의 경우 평가지표의 구체성이 떨어지고 일관성 확보가 어려워 정보보안을 실현함에 있어 직접적인 도움이 되지 못하고 있는 실정으로 이는 결국 정보보안 평가를 위한 타당하고 실용적인 지표를 개발하지 못했음을 의미한다고 볼 수 있다. 본 연구에서는 정보보안 평가와 관련이 있는 기존연구들을 검토하여 평가지표를 도출하고, 보안담당자와 보안컨설턴트 등 정보보안전문가들을 대상으로 평가관련 업무에 적용함에 있어 내용의 타당성과 평가의 용이성 그리고 평가의 신뢰성 측면에서 얼마나 적합한가에 대해 일련의 부합성 분석(coincidence analysis)을 실시하여 평가목적에 부합하는 정보보안 평가지표를 선정하여 제시하고자 한다.

2. 정보보안 평가영역, 평가항목 및 평가지표 도출

정보보안 평가지표를 묶는 평가영역의 구성은 연구별로 다소 차이가 있는 것이 현실이다. 이와 관련하여 본 연구에서는 ISO27001(2005), BS7799(2002), KISA(2002), 김현수(1999), NIST SP800-53A(2006), 김정덕, 김기윤(1998) 등 정보보안 분야의 대표적인 연구를 토대로 <표 1>과 같이 보안정책, 보안조직, 자산관리, 인원보안, 물리적·환경적 보안, 통신 및 운영관리, 접근통제, 정보시스템 도입·개발·유지보수, 준거성의 9개 평가영역으로 분류하였다[4, 6, 11-13, 15, 17].

정보보안 평가항목 및 평가지표 개발과정에서 고려해야 할 사항에 대해 임용현(2004), 김정덕(2003), 김정덕, 김기윤(1998) 등의 연구에서 공통으로 제시하고 있는 사항으로 ① 정보보안을 평가함에 있어 내용이 타당하고 평가의 용이성이 보장되어야 하고 ② 평가지표가 구체적이고 객관성이 보장되어야 하며 ③ 정보기술의 발전과 비즈니스 환경의 변화를 적절하게 반영해야 한다는 것이다[3, 4, 8].

이에 따라 본 연구에서는 정보보안 평가와 관련하여 학문적으로나 실무적으로 많이 활용되고 있는 ISO27001(2005), BS7799(2002), KISA(2002) 등을 참조하여 평가항목과 평가지표를 도출하였다[11-13, 15].

2.1 보안정책

보안정책은 조직의 목표와 방향에 맞추어 보안 측면에서의 목표와 방향을 제시하고 있는 중요한 문서로, 대부분의 조직에서 조직 구성원의 자발적인 참여보다는 하향적으로 통제적 측면에서 시행되는 특성이 있음으로, 최고경영자의 확고한 의지가 무엇보다도 중요하며 임직원과 관련 이해관계자 모두에게 공표되고 공감대가 형성되어 있어야 한다. 보안정책이 시스템적으로 실행되기 위해서는 무엇보다도 내용이 타당성하고 현실성을 확보하여야 한다. 이를 위해 상위의 경영목표나 IT 목표와 일관성이 있어야 하고, 지침·표준·절차로 구분하여 체계적으로 관리해야 한다. 또한 상시적으로 유효성을 보장하기 위해 정기적으로 검토하고 최신화해야 하는 바, 이를 반영한 5개의 지표로 구성되어 있음을 알 수 있다(<부록 1>의 “(1)항” 참조).

2.2 보안조직

보안조직에 관한 평가영역에서는 보안업무를 적

〈표 1〉 정보보안 평가영역 비교 및 분류

평가영역	김정덕, 김기윤(1998)	BS7799(2002)	KISA(2002)	ISO27001(2005)
보안정책		◦ 보안정책	◦ 정보보호정책	◦ 보안정책
보안조직	◦ 조직적보안	◦ 보안조직	◦ 정보보호조직 ◦ 외부자보안	◦ 보안조직
자산관리		◦ 자산관리	◦ 정보자산 분류	◦ 자산관리
인원보안	◦ 행정적보안 ◦ 인적보안	◦ 인원보안	◦ 인적보안 ◦ 보안사고관리 ◦ 교육 및 훈련	◦ 인적자원보안 ◦ 보안사고관리
물리적· 환경적 보안	◦ 환경보안 ◦ 물리적접근보안 ◦ 물적가용보안	◦ 물리적·환경적보안 ◦ 업무연속성관리	◦ 물리적보안 ◦ 업무연속성관리	◦ 물리적·환경적보안 ◦ 업무연속성관리
통신 및 운영관리	◦ 환경보안[1)] ◦ 물적가용보안[2)] ◦ 통신보안 ◦ 자료보안	◦ 통신 및 운영관리	◦ 암호통제 ◦ 운영관리 ◦ 전자거래보안	◦ 통신 및 운영관리
접근통제		◦ 접근통제	◦ 접근통제	◦ 접근통제
정보시스템 도입· 개발·유지보수	◦ 소프트웨어보안 ◦ 자료보안	◦ 정보시스템 도입· 개발·유지보수	◦ 시스템개발보안	◦ 정보시스템 도입· 개발·유지보수
준거성		◦ 준거성	◦ 검토, 모니터링 및 검사	◦ 준거성

절하게 수행·유지·관리하기 위해 보안담당자를 포함하여 관련 직원의 역할과 책임에 대해 정의하는지와 고객을 포함하여 외부기관과 접촉에 따른 위험에 대해 사전에 분석하고 이에 따른 보안대책을 수립하는지에 대해 평가함에 있다. 이와 관련 ISO27001(2005), BS7799(2002), KISA(2002), 고일석, 김진영(2002), 김현수(1999), NIST SP800-53A(2006) 등의 연구를 고찰한 결과 본 영역은 내부조직관리와 외부기관관리의 2개 평가항목으로 구성되어 있음을 알 수 있다(<부록 1>의 "(2)항" 참조)[1, 6, 11-13, 15, 17]. 내부 조직관리에서는 보안조직의 보안업무 수행과 관련하여 ① 보안업무를 적절하게 기획·조정·관리하는지 ② 보안조직이 독립적인 입장에서 보안업무를 수행하는지 ③ 각 부서의 보안업무가 원활하게 수행되도록 지원하고, 정기적으로 보안업무 수행실적을 검토하는지를 평가하는 지표들을 도출하였다. 외부기관관리에서는 고객이나 제 3자를 포함하는 외부기관과의 접촉에 따른 정보 및 정보처리설비의 안전을 목적으로 ① 고객이 정보자산에 접근하는 경우 보안대책을 수립하여 이행하고 있는지 ② 제 3자와의 계약 시 보안요구사항과 보안책임 등을 식별하고 관리하고 있는지를 평가하는 지표들이 있다.

2.3 자산관리

조직에서 자산은 조직의 비즈니스를 수행하거나 성공하기 위해 반드시 필요한 요소로 올바르게 관리하고 적절하게 보호되어야 한다. 이를 위해 자산현황을 파악하고, 관리책임에 대한 소재를 명확하게 하며, 중요도별로 적절하게 분류하여 관리하여야 하는 바, 본 평가영역은 5개의 평가지표로 구성된다(<부록 1>의 "(3)항" 참조).

2.4 인원보안

본 영역의 중점은 인원보안과 관련하여 임직원, 계약자, 제 3자 등 조직의 이해관계자를 대상으로 보안대책을 수립하는지와 보안사고 발생에 효과적

1) 환경보안 구성항목 중 백업과 복구에 관한 사항임.
2) 물적가용보안 구성항목 중 입력과 출력에 관한 사항임.

으로 대응하기 위해 보안대책을 마련하고 교육을 실시하는지에 대해 평가함에 있다. 이에 대한 선행연구를 고찰한 결과 인적자원관리와 보안사고관리의 2개 항목으로 구성되어 있음을 알 수 있다(<부록 1>의 “(4)항” 참조). 인적자원관리 항목에서는 조직과 관련이 있는 임직원이나 이해관계자에 의한 실수, 절도, 오용 등으로부터 위험을 감소시키기 위해 ① 채용 시 학력이나 경력 등 배경에 대해 검토하고 고용계약서에 보안책임을 명시하는지 ② 고용기간동안 보안정책의 이행과 보안교육을 실시하는지 ③ 퇴직 시 자산을 반납 받고 접근권한을 삭제하며 책임사항에 대해 전달하는지를 평가하는 지표들을 도출하였다. 보안사고관리 항목에서는 보안사고 발생 시 신속한 대응을 위해 ① 대응절차를 수립하고 정기적으로 훈련을 실시하는지 ② 예상되거나 관찰되는 보안취약점에 대해 적절한 채널을 통해 보고하는지 ③ 보안사고 발생 시 증거를 수집하고 분석하여 법적인 대응을 준비하는지 ④ 보안위반자에 대해 징계절차에 의거 조치하는지를 평가하는 지표들로 구성된다.

2.5 물리적 · 환경적 보안

본 영역은 정보처리설비를 갖춘 구역을 안전하게 보호하기 위해 보안구역을 설정하여 비인가인원에 대한 통제대책을 마련하고 있는지와 재난이나 재해가 발생하는 경우에도 조직의 중요 업무가 지속적으로 수행되도록 업무연속성관리를 적절하게 수행하고 있는지에 대해 평가함에 있다. 이에 대한 선행연구를 고찰한 결과 보안구역관리, 정보처리설비관리, 업무연속성관리의 3개 항목으로 구성되어 있음을 알 수 있다(<부록 1>의 “(5)항” 참조). 첫째, 보안구역관리 항목에서는 조직에서 중요도가 높은 민감한 정보처리설비구역은 비인가적 접근, 손괴, 방해 등으로부터 안전한 지역에 위치시켜야 한다. 이에 따라 ① 중요 정보처리설비 보호를 위한 별도의 보안구역을 설정하는지 ② 비인가인원의 보안구역 출입을 통제하는지 ③ 외부와의 접촉점에서의 비인가 인원의 활동을 제한하는지를 평가하는 지표들로 구성된다, 둘째, 정보처리설비관리 항목에서는 정보처리설비의 안정적 운영을 위해 ① 중요 정보처리설비를 보호하기 위해 적절한 온도와 습도를 유지하는지 ② 안정적인 전원공급 및 통신을 운영하는지 ③ 유지보수는 인가된 인원에 의해 수행되는지 ④ 정보처리 설비의 외부반출 시 안전하게 보호되는지에 대해 평가하는 지표들로 구성된다. 셋째, 업무연속성관리 항목에서는 각종 재해나 재난으로부터 중요 업무의 지속성 보장을 위해 대책을 마련하는 것으로 ① 업무연속성 보장을 위한 요구사항을 파악하는지 ② 재난이나 재해에 따른 대응방안을 마련하는지 ③ 효율성을 제고하기 위해 관련정책과 일치성을 유지하는지에 대해 평가하는 지표들로 구성된다.

2.6 통신 및 운영관리

본 영역에서는 정보처리설비를 올바르고 안전하게 보호하기 위해 ① 운영절차를 문서화하는지 ② 시스템과 네트워크의 운영에 대해 지속적으로 모니터링 하는지 ③ 매체를 적절하게 보호하는지 ④ 정보교환 시 안전성을 유지하는지에 대해 평가함에 있다. 이와 관련하여 선행연구를 고찰한 결과 운영절차 및 책임, 제 3자 서비스 인도관리, 시스템 운영관리, 네트워크 보안관리, 매체관리, 정보교환관리의 6개 항목으로 구성되어 있음을 알 수 있다(<부록 1>의 “(6)항” 참조). 첫째, 운영절차 및 책임 항목에서는 정보처리설비의 안전한 운영을 위해 ① 책임소재를 분명히 하고 있으며, 운영절차를 수립하고 있는지 ② 변경 시 사전승인이나 실패 시 복구대책 마련 등의 대책을 수립하고 있는지 ③ 비인가 수정이나 오용을 막기 위해 직무를 분리하고 있는지 ④ 비인가자의 접근을 통제하고 있는지를 평가하는 지표들로 구성된다. 둘째, 제 3자 서비스 인도관리 항목에서는 최근 경영효과 및 효율을 극대화하기 위한 방안으로 아웃소싱 기관과 같은 제 3자에게 정보처리설비를 위탁하는

것이 증가되고 있음에 따라 ① 제 3자 서비스 이용 시에는 서비스 제공수준에 대한 명확한 합의가 있는지 ② 계약서에 보안대책을 명시하고 있는지 ③ 정기적으로 서비스 이용에 대한 기록을 검토하는지를 평가하는 지표들을 도출하였다. 셋째, 시스템 운영관리 항목에서는 시스템 운영 시 가용성과 무결성을 확보하기 위해 ① 시스템 인수 시 관련 기준에 의거 테스트하는지 ② 시스템의 용량과 성능에 대해 정기적으로 모니터링 하는지 ③ 정보처리 이용에 대한 로그와 장애발생에 관한 사항을 분석하고 관리하는지 ④ 중요 정보처리 데이터는 악성코드나 바이러스로부터 보호하고 정기적으로 백업하고 있는지를 평가하는 지표들로 구성된다. 넷째, 네트워크 보안관리 항목에서는 네트워크 보안을 위해 ① 접속기록 검토, 시스템과의 운영분리 등 보안통제를 수행하는지 ② 제 3자 서비스 이용과 관련해서는 서비스 협정서에 서비스 수준, 보호대책 등을 포함하는지 ③ 인터넷 접속 시 방화벽을 통해 접속이 되도록 관리하는지를 평가하는 지표들을 도출하였다. 다섯째, 매체관리 항목에서는 정보의 저장・전달과 관련이 있는 매체로 문서, 테이프, 디스크, 입・출력데이터, 시스템문서 등이 있다. 이와 관련하여 비인가적 접근이나 오용 그리고 손괴 등으로부터 매체를 안전하게 보호하는지에 대해 평가하는 지표들을 도출하였고, 여섯째, 정보교환관리 항목에서는 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 있는지 ③ 홈페이지 등을 통해 공적으로 공개되는 정보가 정확성을 유지하고 있는지를 평가하는 지표들로 구성되어 있음을 알 수 있다.

2.7 접근통제

접근통제 영역의 중점은 중요 정보에 대한 비인가적 접근을 통제하기 위해 ① 사용자 책임을 명시하는지 ② 주기적으로 접근권한을 관리하는지 ③ 접근권한이 없는 비인가 인원의 시스템으로의 접근을 적절하게 통제하는지에 대해 평가함에 있다. 선행연구를 종합적으로 고찰한 결과 사용자 책임 및 접근관리, 네트워크 접근통제, 운영시스템 접근통제, 어플리케이션 및 정보 접근통제, 모바일 컴퓨팅 및 텔레워킹의 5개 항목으로 구성되어 있음을 알 수 있다(<부록 1>의 “(7)항” 참조). 첫째 사용자 책임 및 접근관리 항목에서는 정보시스템과 정보의 안정적 운영과 보호를 위해 ① 사용자 접근권한을 부여하는 공식적인 절차가 마련되어 있는지 ② 사용자 접근권한이 등록단계로부터 삭제 시까지 적절하게 관리되는지 ③ 사용자가 보안성이 높은 패스워드 사용하는지와 자리 이석 시 적절한 보호대책을 강구하는지를 평가하는 지표들을 도출하였다. 둘째, 네트워크 접근통제 항목에서는 네트워크 서비스를 보호하기 위해 내부 및 외부 네트워크 서비스에 대한 비인가 접근을 통제하기 위해 ① 원격사용자의 내부접근을 통제하는지 ② 서비스별, 사용자별 네트워크 서비스를 분리 운영하는지 ③ 원격접속 시 공인인증 등 적절한 인증 메커니즘을 적용하는지를 평가하는 지표들을 도출하였다. 셋째, 운영시스템 접근통제 항목에서는 운영시스템에 대한 비인가 접근을 통제하고 안정적으로 운영하기 위해 ① 사용자별・그룹별 별도의 계정을 부여하는지 ② 안전한 패스워드를 사용하는지 ③ 시스템 접속과 관련하여 연결시간을 제한하는지 ④ 시스템 유틸리티 프로그램의 사용을 제한하는지를 평가하는 지표들로 구성되며, 넷째, 어플리케이션 및 정보 접근통제 항목에서는 정보시스템 내부에 있는 정보에 대한 비인가적 접근을 통제하기 위해 ① 어플리케이션에 대한 접근을 제한하는지 ② 중요 정보시스템을 일반시스템과 별도로 분리하여 운영하는지를 평가하는 지표들로 구성된다. 다섯째, 모바일 컴퓨팅 및 텔레워킹 항목에서는 PDA, 노트북, 휴대폰 등 모바일 컴

퓨터 장비를 외부로 반출하여 사용하는 경우 적절한 보호대책이 필요하며, 재택근무와 같이 외부에서 작업 시 절도, 노출, 오용 등의 위험에 많이 노출이 됨으로 이에 대비하여 적절한 보호대책을 적용하는지를 평가하는 지표들이 있다.

2.8 정보시스템 도입 · 개발 · 유지보수

정보시스템의 도입 · 개발 · 유지보수과정에서 ① 안전성과 무결성 그리고 신뢰성을 유지하는지 ② 공식적인 변경절차를 수립하여 이행하는지 ③ 데이터의 정확성과 무결성 유지를 위해 적절하게 통제하는지 ④ 시스템파일을 안전하게 보호하는지를 점검하는 것은 정보보안을 유지하기 위한 중요한 요소라고 할 수 있다. 이와 관련하여 선행연구를 고찰한 결과 어플리케이션의 정확한 처리, 암호통제, 시스템파일 보안, 개발 및 지원프로세스 보안의 4개 항목으로 구성되어 있음을 알 수 있다(<부록 1>의 "(8)항" 참조). 어플리케이션의 정확한 처리 항목에서는 어플리케이션 프로그램이 실행되는 과정에서 입력데이터 · 처리데이터 · 출력데이터의 손실, 변조, 오용을 막기 위한 입력지침, 처리지침, 출력지침을 수립 · 이행하는지를 평가하는 지표들을 도출하였으며, 암호통제 항목에서는 정보의 기밀성 · 무결성 유지와 관련하여 암호솔루션 적용을 위한 정책의 수립 여부와 암호 키의 안전한 보호대책을 수립하고 있는지를 평가하는 지표들을 도출하였다. 시스템 파일보안 항목에서는 시스템 파일을 안전하게 보호하기 위해 S/W 설치 시 또는 시험데이터 선택 시 그리고 소스코드 접근 시 이에 대한 적절한 보안대책을 수립하여 이행하고 있는지를 평가하는 지표들로 구성된다. 마지막으로 개발 · 지원프로세스 보안 항목에서는 IT프로젝트 진행과정에서 ① 개발 초기단계부터 보안요구사항을 반영하는지 ② 변경 시 공식적인 절차를 수립하여 이행하는지 ③ 적절하게 개발하고 있는지에 대해 감독과 감시를 하는지 ④ 기술적 취약성에 대해 분석하는지를 평가하는 지표들이 있다.

2.9 준거성

정보보안을 올바르게 유지하고 관리하기 위해서는 준거성의 중요성은 간과할 수 없을 것이다. 본 영역에서의 중점은 법, 규정, 계약서 등을 검토하여 ① 조직과 관련이 있는 요구사항을 문서화하여 관리하는지 ② 이러한 요구사항들이 감사나 점검을 통해 이행되는지 ③ 감사도구를 안전하게 관리하는지에 대해 평가함에 있다. 이와 관련하여 선행연구를 종합적으로 고찰해보면 법적요구사항 준수와 보안감사의 2개 항목으로 구성되어 있음을 알 수 있다(<부록 1>의 "(9)항" 참조). 법적 요구사항 준수 항목에서는 법, 규정, 계약 등의 법적 요구사항에 대해 불이행이나 위반이 발생하지 않도록 ① 법적 요구사항에 대해 문서화 하는지 ② S/W 저작권 등 지적재산권에 대한 보호대책을 마련하는지 ③ 법이나 계약에 의거 중요한 데이터의 안전한 보호대책을 마련하는지를 평가하는 지표들로 구성되어 있다. 보안감사 항목에서는 조직의 보안정책을 제대로 이행하는지에 대해 감사 · 점검하는 활동으로 ① 신중하게 감사계획을 수립하여 이행하는지 ② 감사가 완료되더라도 지속적으로 사후관리 하는지 ③ 감사도구 사용 시 사후에 이를 안전하게 관리하는가에 대해 평가하는 지표들이 있다.

3. 부합성 분석을 위한 연구설계

3.1 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)이 주된 목적으로 일반적인 설문조사 작업 시 본 조사에 앞서서 실시하는 일종의 사전조사(pilot test, pretest)의 의미를 지닌다[10]. 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 개발하는데 의의가 있다고 할 수 있다[7].

3.2 부합성 분석을 위한 평가기준 설정 및 설문개발

평가지표의 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[5, 14, 16, 19]. 본 연구에서는 위 평가지표 선정을 위한 평가기준의 요구사항이 <표 2>에서 제시한 바와 같이 내용타당성, 평가용이성, 평가신뢰성으로 구분정리될 수 있다고 보며, 앞서 도출된 120개의 평가지표들을 대상으로 본 세 가지 평가기준에 의거한 부합성 분석을 실시하고자 한다. 부합성 분석을 위한 설문서는 각 평가지표가 정보보안 수준을 평가함에 있어 적합한 가를 검증하기 위해 각 평가지표별로 내용타당성, 평가용이성, 평가신뢰성 정도를 5점 척도로 측정할 수 있도록 구성하였다.

3.3 부합성 분석을 위한 자료수집

앞서 도출된 평가지표의 부합성에 대한 면밀한 검토를 위해 정보보안 평가와 관련하여 현장경험이 풍부한 250명을 대상으로 설문작성을 요청하였고, 이중 83명으로부터 유효한 응답을 받았다. 이들은 주로 보안컨설팅 기관에 종사하는 보안컨설턴트와 기업의 보안담당자, 보안관련 공공기관 연구원 등으로 구성되었다. 이들의 구성을 직위별로 살펴보면 과장급이 31명(37.3%)으로 가장 많고 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%)으로 가장 많고 1년~3년 미만 20명(24.1%), 3년~5년 미만 12명(14.5%), 10년 초과 10명(12%), 1년 미만 7명(8.4%) 순이다.

4. 부합성 분석

4.1 부합성 분석 절차

부합성 분석은 앞서 기존연구 및 국내외 표준을 통해 도출된 120개의 정보보안 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

〈표 2〉 부합성 분석을 위한 평가기준

평가기준	내 용
내 용 타당성	해당 평가지표를 통해 평가하는 경우 정보보안 수준을 평가하는데 얼마나 적합한가를 의미하는 것으로 정보보안 평가에 관련성이 높을수록 내용적인 타당성이 확보된 평가지표라고 볼 수 있음
평 가 용이성	해당 평가지표를 통해 평가하는 경우 평가가 얼마나 쉬운가를 의미하는 것으로 평가과정에서 많은 자료가 필요하다거나 수집된 자료에 대한 추가적인 계산과정에 많은 시간이 소요되는 경우 그 만큼 평가관련 업무량의 증대를 가져오게 됨
평 가 신뢰성	정보보안을 평가함에 있어, 해당 평가지표가 응답자의 특성이나 시·공간과 무관하게 얼마나 일관된 답을 얻을 수 있음으로써 신뢰성을 유지할 수 있는가를 의미

평가지표 확정 순으로 진행하였으며, 이때 도구로는 SPSS 12.0을 이용하였다[2].

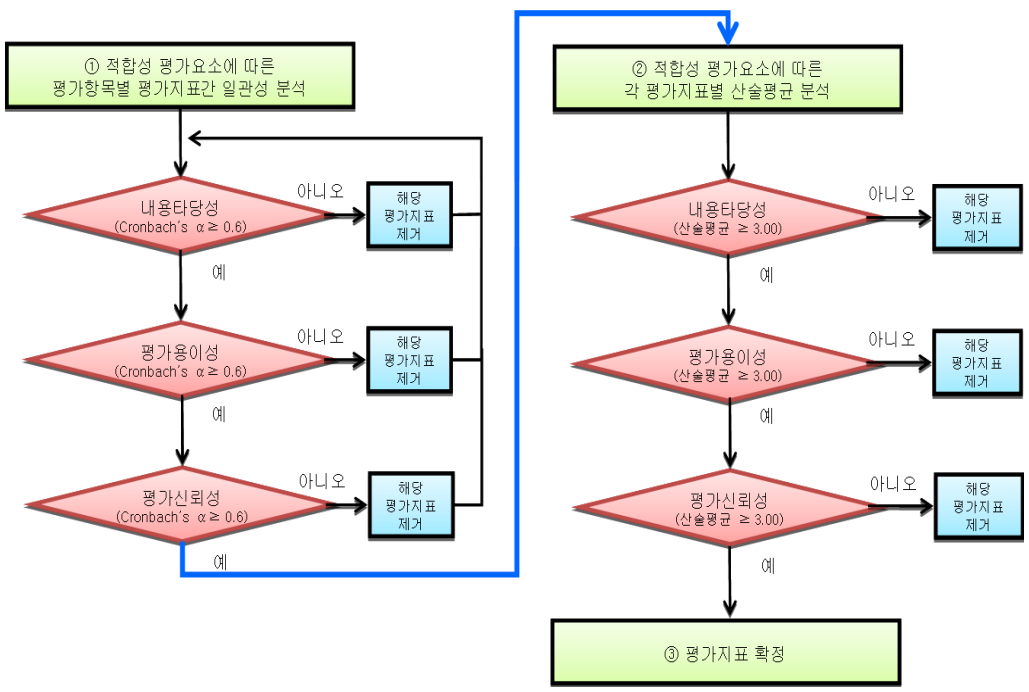
4.2 부합성 분석 결과

4.2.1 평가항목별 평가지표의 일관성 분석

일관성이란 동일한 개념에 대해 측정을 되풀이했을 때 동일한 측정값을 얻을 가능성을 의미하는 것(최점기, 2006)으로 대표적인 분석기법에는 내적 일관성, 반복측정 신뢰성, 대안항목 신뢰성이 널리 활용되고 있다[9]. 본 단계에서는 평가항목을 구성하고 있는 각 평가지표의 내용타당성, 평가용이성, 평가신뢰성에 대한 일관성이 어느 정도인지를 확인하는 것으로 Cronbach's α를 이용한 내적일관성에 대한 검증기법을 사용하였다([그림 1]의 ①참조). 내용타당성 측면에서 분석한 결과 Cronbach's α는 모두 0.6이상으로 나타나 Nunally(1978)가 주장하는 허용기준(0.6)을 상회하였고, 평가용이성 측면에서 분석한 결과도 모두 0.6이상으로 나타났으며, 평가신뢰성 측면에서의 분석결과 또한 모두 0.6이상으로 나타났다(<부록 2> 참조)[18]. 이를 통해 앞서 제 3장에서 도출된 26개의 평가항목과 120개의 평가지표들이 일관성이 확보되어 있다고 볼 수 있다.

4.2.2 평가지표별 산술평균 분석

본 연구에서는 보다 적합한 평가지표를 도출하고자 일관성에 대한 면밀한 분석을 실시함은 물론 추가로 평가지표별 산술평균을 통해 평가지표의 부합성을 판정하는 절차를 포함하였다([그림 1]의 ② 참조). 부합성에 대한 설문조사가 Likert 5점 척도를 기반으로 하였기 때문에 산술평균값인 3.00을 판정기준으로 설정하였으며 평가기준인 내용타당성, 평가용이성, 평가신뢰성 중에 어느 하나만이라도 위 판정기준에 미달하는 경우에는 평가가 용이하지 않거나, 평가한 내용을 신뢰할 수 없다거나, 정보보안 평가와 관련성이 없는 등 해당 평가지표의 현실성이 부족하다고 판단하여 평가항목의



[그림 1] 정보보안 평가지표의 부합성 분석절차

구성에서 제거하였다. 부합성 분석을 위한 평가지표별 산술평균값은 모두 판정의 기준이 되는 값 3.00이상으로 나타난 바, 평가지표별 산술평균 분석을 통해 제거된 평가지표가 발생하지 않았다(<부록 3> 참조). 따라서 앞서 제 3장에서 도출된 평가항목 및 평가지표들이 평가에 적합하다는 타당성을 충분히 확보하고 있다는 것을 알 수 있다.

5. 결 론

본 연구에서는 정보보안 평가를 대표하는 국내·외 문헌들에 대한 포괄적인 고찰을 통해 9개의 평가영역과 26개의 평가항목을 구성하였으며, 세부적으로 120개에 이르는 평가지표들을 개발하였다. 또한 도출된 평가항목 및 평가지표들이 현실적으로 평가 상황에 얼마나 부합되는지 그 적용가능성을 실증적으로 분석하기 위해 내용타당성, 평가용이성, 평가신뢰성의 3가지 평가기준을 설정하고 정보보안 평가와 관련이 있는 보안컨설턴트, 보안담당자, 연구원 등을 대상으로 설문조사를 실시하였고, 이를 통해 부합성 분석을 실시하였다. 부합성 분석은 도출된 정보보안 평가지표가 적합한가에 대해 정보보안 전문가를 대상으로 설문조사를 통해 실증적으로 분석하는 과정으로 ① 평가항목별 평가지표 간 일관성 분석 → ② 평가지표별 산술평균 분석 → ③ 평가지표 확정 순으로 진행하였다. 우선 평가항목별 평가지표 간 일관성 분석 결과 내용타당성, 평가용이성, 평가신뢰성 측면에서 앞서 제 3장에서 도출된 26개의 평가항목과 120개의 평가지표가 모두 일관성이 확보되어 있음을 알 수 있었다. 다음으로 내용타당성, 평가용이성, 평가신뢰성별 평가지표의 산술평균이 모두 판정의 기준이 되는 값 3.00이상으로 나타나 평가지표별 산술평균 분석을 통해 제거된 평가지표가 발생하지 않았다. 따라서 앞서 제 3장에서 도출된 120개의 평가지표가 정보보안 평가에 적합하다는 것을 알 수 있었다.

본 연구는 정보보안 평가지표들 자체에 대한 적정성 확보를 위해 각 지표들에 대한 부합성 분석을 실시하기 위한 기준 및 절차를 제시하였다는 이론적 의의를 가짐과 동시에 현실적인 정보보안 평가업무 수행 시 활용되어 질 수 있는 평가항목과 평가지표를 합리적으로 도출함으로써 향후 정보보안 업무 성과를 향상시키는데 기여할 수 있다고 본다. 본 연구의 제한사항으로는 정보보안 평가지표를 도출과정에서 방법론 제시가 미흡하였고, 부합성 분석을 위한 평가기준에 대한 조사가 심도 있게 이루어지지 못하였다. 또한 산술평균 분석을 통한 평가지표들의 부합성 여부 판단을 위한 기준치를 5점 척도 중 3.00점으로 설정한 것은 다소 임의적인 면을 가지고 있으므로 이에 대한 통계적·실증적 차원의 접근을 통한 객관적인 판단기준의 발굴도 중요하다고 볼 수 있다(산술평균 분석을 위한 기준치를 4.00으로 설정하는 경우 120개의 평가지표중 116개가 탈락함). 아울러 일련의 부합성 분석과정을 통해 도출된 평가지표들을 이용하여 정보보안 평가를 실제적으로 실시하고 이를 대상으로 이론적·실무적 차원의 타당도 및 신뢰도를 검증해보는 실증분석도 수반되어야 할 것이다.

참 고 문 헌

[1] 고일석, 김진영 외, 「정보보호수준 평가 항목 및 방법론 개발」, 한국정보보호 진흥원, 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] 김정유, 이승아, “IT 투자평가 방법론과 활용 방안”, 「e-biz group working paper」, 제28호

(2001), pp.1-19.
[6] 김현수, "정보보안수준 계량화 연구", 「한국경영정보학회」, 제9권, 제4호(1999), pp.181-201.
[7] 안광호, 임병훈, 「SPSS를 활용한 사회 과학 조사방법론」, 학현사, 2004.
[8] 임용현, 「정보보호 수준의 자가 평가 모델」, 석사학위논문, 전남대학교, 2004.
[9] 최점기, 「정보화지원사업의 인과적 평가 모형 개발에 관한 실증적 연구」, 박사학위논문, 광운대학교, 2006.
[10] 중소기업청, 중소기업정보화경영원, 「중소기업 정보화지원정책 성과평가체계 연구」, 2005.
[11] KISA(한국정보보호진흥원), 「정보보호 관리체계 인증규격」, 2002.
[12] British Standards Institution, *BS7799-1 : Code of Practice for Information Security Management*, 2002.
[13] British Standards Institution, *BS7799-2 : Specification for information security management systems*, 2002.
[14] Hatry, Harry P., *Productivity and Motivation : A Review of State and Local Government Initiatives*, Urban Institute Press, 1980.
[15] ISO/IEC, *ISO27001 : Specification for information security management systems*, 2005.
[16] Lefrancois, R., "A Challenge for the 1980s : Productivity-Oriented University Management", *Cost and Management*, Vol.58, No.1(1984), pp.55-59.
[17] NIST, *Guide for Assessing the Security Controls in Federal Information Systems*, NIST Special Publication 800-53A, 2006.
[18] Nunally, J. C., *Psychometric Theory*, New York, McGraw Hill, 1978.
[19] Rosen, Ellen D., *Improving Public Sector Productivity*, London, Sage Publications, 1993.

〈부록 1〉 정보보안 평가지표 도출

(1) 보안정책

평가항목	평가지표	김현수 (1999)	고일석 (2002)	BS7799 (2002)	KISA (2002)	ISO27001 (2005)	NIST (2006)	CODE
보안정책 관 리	보안정책은 최고경영자의 승인을 받아야 한다.	○	○	○	○	○	-	SP-01
	보안정책은 모든 임직원 및 이해관계자에게 공표되어야 한다.	-	○	○	○	○	○	SP-02
	보안정책은 상위 경영목표, IT 목표와 일관성을 유지해야 한다.	-	-	-	○	-	-	SP-03
	보안정책 수행을 위해 필요한 지침, 표준, 절차 등을 구체적으로 개발해야 한다.	-	○	-	○	-	-	SP-04
	보안정책은 정기적 또는 변경사항이 있는 경우 검토되어 상시적으로 유효해야 한다.	○	○	○	○	○	-	SP-05

(2) 보안조직

평가항목	평가지표	김현수 (1999)	고일석 (2002)	BS7799 (2002)	KISA (2002)	ISO27001 (2005)	NIST (2006)	CODE
내부조직 관 리	보안조직을 구성하여 조직의 보안활동과 관련된 기획, 조정, 관리책임을 부여한다.	-	-	-	○	-	-	SO-01
	보안업무는 관련부서의 대표들과 공조하여 추진하여야 한다.	○	-	○	○	○	○	SO-02
	보안책임을 명확하게 정의하고 구체적으로 할당하여야 한다.	○	○	○	○	○	○	SO-03
	보안서약이 지속적으로 유효하도록 정기적으로 검토해야 한다.	-	○	○	○	○	○	SO-04
	최신 취약점에 대한 정보 공유 등 보안업무의 원활한 추진을 위해 보안 전문기관과의 적절한 접촉이 유지되어야 한다.	-	○	-	-	-	○	SO-05
	보안업무를 효과적으로 이행하기 위해 보안조직은 “독립적”인 위치에 있어야 한다.	○	○	○	-	○	-	SO-06
외부기관 관 리	외부기관과 관련된 정보나 정보처리설비에 대한 위험을 식별하고 적절한 통제를 수립하여야 한다.	-	-	○	-	○	○	SO-07
	고객이 조직의 정보자산에 접근하는 경우 보안 요구사항을 식별하고 관리해야 한다.	-	-	-	-	○	○	SO-08
	제 3자와 계약 시 보안요구사항, 서비스 수준, 보안책임 등을 식별하고 관리해야 한다.	-	-	○	○	○	○	SO-09

(3) 자산관리

평가항목	평가지표	김현수 (1999)	고일석 (2002)	BS7799 (2002)	KISA (2002)	ISO27001 (2005)	NIST (2006)	CODE
자산관리	모든 자산을 명확하게 정의하고, 중요한 자산에 대해서는 목록을 작성하여 관리하여야 한다.	○	-	○	○	○	○	AM-01
	조직의 모든 정보와 자산은 지정된 소유자에 의해 소유되어야 한다.	-	-	-	○	○	○	AM-02
	전자메일, USB 등의 정보자산에 대한 이용 지침을 수립하고, 이행하여야 한다.	-	-	-	-	○	○	AM-03
	정보는 법적요구사항, 가치, 위험도 등에 따라 분류되어야 한다.	○	○	○	○	○	-	AM-04
	중요정보는 분류지침에 의해 라벨(중요도, 취급절차, 파기 등)을 붙여 관리하여야 한다.	-	○	○	○	○	○	AM-05

(4) 인원보안

평가항목	평가지표	김현수 (1999)	고일석 (2002)	BS7799 (2002)	KISA (2002)	ISO27001 (2005)	NIST (2006)	CODE
인적자원 관 리	이해관계자(직원, 계약자, 제 3자 등)의 보안에 대한 역할과 책임을 정의하고, 이를 보안정책에 반영하여야 한다.	-	-	○	-	○	○	HR-01
	직원 채용 시 합법적 범위 안에서 채용인원에 대한 배경(학력, 경력 등)에 대해 검토하여야 한다.	-	-	○	○	○	○	HR-02
	고용계약서에 고용에 대한 조건과 약정 그리고 보안책임 등이 명시되어야 한다.	○	-	○	○	○	-	HR-03
	모든 직원은 보안 요구사항, 법적책임 등에 대해 적절한 교육을 받아야 한다.	○	○	○	○	○	○	HR-04
	보인교육 현황을 개인별로 문서화하여 관리해야 한다.	-	-	-	○	-	○	HR-05
	퇴직 시 고용 종료 후에도 지속되는 보안 요구사항과 법적책임 등에 대해 전달하여야 한다.	-	○	○	○	○	-	HR-06
	고용이 종료된 시점에서 퇴직자는 그동안 소유했던 조직의 모든 자산을 반환해야 한다.	-	○	○	○	○	○	HR-07
	퇴직자의 정보 접근권한은 고용이 종료되는 시점에서 제거하여야 한다.	-	-	○	○	○	○	HR-08

(4) 인원보안(계속)

평가항목	평가지표	김현수 (1999)	고일석 (2002)	BS7799 (2002)	KISA (2002)	ISO27001 (2005)	NIST (2006)	CODE
보안사고 관 리	보안사고 발생 시 신속하게 대응하기 위한 지침과 절차를 수립하여야 한다.	○	○	○	○	○	○	HR-09
	보안사고 발생에 대비하여 정기적으로 대응 절차에 대한 교육훈련을 실시하여야 한다.	-	-	-	○	-	○	HR-10
	모든 이해관계자(직원, 계약자, 제 3자)는 관찰되거나 예상되는 보안취약점에 대해 보고하여야 한다.	○	○	○	-	○	○	HR-11
	보안사고 진행과정을 추적하고 문서화해야 한다.	-	-	○	○	○	○	HR-12
	보안사고 발생 시 이를 분석하여 보안대책을 강구하는 메커니즘이 있어야 한다.	-	○	○	○	○	○	HR-13
	보안사고 발생 시 법적조치를 위해 각종 증거를 수집하고, 보유하여야 한다.	-	-	○	○	○	○	HR-14
	보안위반 시 조치를 위한 징계절차를 수립하여야 한다.	○	○	○	○	○	○	HR-15

(5) 물리적 · 환경적보안

평가항목	평가지표	김현수 (1999)	고일석 (2002)	BS7799 (2002)	KISA (2002)	ISO27001 (2005)	NIST (2006)	CODE
보안구역 관 리	조직의 중요 정보와 정보처리설비구역을 보호하기 위한 보안구역이 설정되어야 한다.	○	○	○	○	○	○	PE-01
	비인가 인원이 보안구역을 출입할 수 없도록 물리적으로 보호(출입일지, 출입증 등)되어야 한다.	○	○	○	○	○	○	PE-02
	중요 정보자산은 홍수, 지진, 침수 등 외부적 · 환경적 위협으로부터 보호되어야 한다.	-	-	-	○	○	○	PE-03
	보안구역에서의 작업을 통제하기 위한 보안지침(사진촬영 제한 등)이 수립되고 이행되어야 한다.	-	-	○	○	○	○	PE-04
	인도 및 선적구역과 같은 외부 접촉점에서 비인가 인원의 접근은 통제(선적구역과 인도구역의 분리 등)되어야 한다.	-	-	○	○	○	○	PE-05

(5) 물리적 · 환경적보안(계속)

평가항목	평가지표	김현수 (1999)	고일석 (2002)	BS7799 (2002)	KISA (2002)	ISO27001 (2005)	NIST (2006)	CODE
정보처리 설비관리	정보처리설비는 환경적인 위협(온도 및 습도, 낙뢰 등)이나 비인가적 접근으로 부터 보호되어야 한다.	○	○	○	○	○	○	PE-06
	UPS, 비상 전원차단장치 구비 등을 통해 정보처리설비를 보호하여야 한다.	-	○	○	○	○	○	PE-07
	정보서비스를 지원하는 전력이나 통신 케이블은 차단이나 피해로부터 보호(간섭방지, 문서화 등)되어야 한다.	○	-	○	○	○	○	PE-08
	정보처리설비는 가용성과 무결성 유지를 위해 정기적으로 인가인원에 의해 유지보수 되어야 한다.	-	○	○	○	○	○	PE-09
	전산장비 폐기 시 중요정보가 유출되지 않도록 저장장치를 겹쳐 쓰거나 물리적으로 파괴하여야 한다.	○	-	○	○	○	○	PE-10
	조직의 전산장비, S/W, 정보는 승인 없이 외부로 유출되지 않아야 한다.	○	○	○	-	○	○	PE-11
업무연속성 관리	재난발생시 중요 업무의 연속성을 유지하기 위해 자산식별, 보험가입 등 각종 보안 요구사항이 개발되어야 한다.	○	○	○	-	○	○	PE-12
	위험평가를 통해 예상되는 위험에 대한 대응방안을 마련해야 한다.	○	-	○	○	○	○	PE-13
	업무연속성계획에는 업무 중단 시 요구되는 정보의 가용성 수준, 복구시간 등이 포함되어야 한다.	-	○	○	○	○	○	PE-14
	업무연속성계획과 관련이 있는 각종 정책들은 서로 일치하여야 하며, 정기적인 테스트를 통해 유효성이 보장되어야 한다.	-	-	○	○	○	○	PE-15

(6) 통신 및 운영관리

평가항목	평가지표	김현수 (1999)	고일석 (2002)	BS7799 (2002)	KISA (2002)	ISO27001 (2005)	NIST (2006)	CODE
운영절차 및 책임	각종 정보처리설비 운영절차를 문서화하고 항상 운영될 수 있도록 최신화해야 한다.	○	○	○	○	○	○	CO-01
	정보처리설비 변경 시 보안통제(영향평가, 사전승인, 실패 시 복구방안 마련 등) 하여야 한다.	○	-	○	○	○	○	CO-02
	정보처리설비의 비인가 수정이나 오용을 최소화하기 위해 직무를 분리하여야 한다.	-	○	○	○	○	○	CO-03
	개발, 테스트, 운영 설비는 비인가 인원의 접근이나 변조의 위험을 줄이기 위하여 분리되어야 한다.	-	-	○	○	○	○	CO-04

(6) 통신 및 운영관리(계속)

평가항목	평가지표	김현수 (1999)	고일석 (2002)	BS7799 (2002)	KISA (2002)	ISO27001 (2005)	NIST (2006)	CODE
제 3자 서비스 인도관리	제 3자 서비스계약서에(아웃소싱 포함)서비스 제공수준, 보안통제사항 등이 명시되어야 한다.	-	○	-	○	○	○	CO-05
	아웃소싱 서비스에 대한 기록(사고기록, 오류 등)을 정기적으로 검토하여야 한다.	-	○	-	○	○	○	CO-06
시스템 운영관리	시스템의 가용성을 보장하기 위해 용량과 성능을 정기적으로 모니터링하고 관리하여야 한다.	-	○	○	○	○	○	CO-07
	시스템 인수 시 사전에 인수기준을 마련하고 적절한 테스트(에러복구대책, 비상계획)를 수행하여야 한다.	-	-	○	○	○	○	CO-08
	정보처리설비에 대한 모니터링 절차를 수립하고, 정기적으로 모니터링 하여야 한다.	○	○	○	○	○	○	CO-09
	정보처리 활용에 대한 로그 정보는 일정기간 보존되어야 하며 필요시 분석이 가능해야 한다.	○	○	○	○	○	○	CO-10
	정보처리활용 관련 로그정보는 비인가적 접근이나 간섭에 보호되어야 한다.	-	○	-	○	○	○	CO-11
	시스템 관리자나 운영자의 활동로그 (이벤트 발생시간, 이벤트 정보 등)를 기록 및 관리해야 한다.	-	○	-	○	○	○	CO-12
	정보처리설비의 장애발생에 관한 사항을 기록하고, 관리하고, 분석하여야 한다.	○	○	○	○	○	○	CO-13
	악성코드를 통제하기 위한 사용자 인식 교육과 사전 예방통제, 사고 후 복구통제가 이행되어야 한다.	○	○	○	○	○	○	CO-14
	백업정책에 의거 정보와 S/W에 대한 백업이 정기적으로 이루어져야 한다.	○	○	○	○	○	○	CO-15
네트워크 보안관리	네트워크 보안을 위해 시스템과의 운영분리, 접속기록 검토 등의 보안통제를 수행하여야 한다.	-	○	○	○	○	○	CO-16
	네트워크 보안통제를 위해 서비스 협정서에 서비스 수준, 보호대책 등을 포함하여야 한다.	-	-	○	-	○	-	CO-17
	인터넷 접속에 따른 보호대책이 수립되어야 하며, 방화벽을 통해 접속이 관리되어야 한다.	-	-	○	○	-	-	CO-18

(6) 통신 및 운영관리(계속)

평가항목	평가지표	김현수 (1999)	고일석 (2002)	BS7799 (2002)	KISA (2002)	ISO27001 (2005)	NIST (2006)	CODE
매체관리	테이프, 디스크, CD 등 컴퓨터 매체 관리를 위한 적절한 절차(사용승인, 기록유지 등)를 수립해야 한다.	○	-	○	○	○	○	CO-19
	민감한 정보를 담고 있는 컴퓨터 매체는 공식 절차를 통해 안전하게 처분해야 한다.	-	-	○	○	○	○	CO-20
	DB 설계서, 프로그램 소스 등이 있는 컴퓨터 매체는 비인가적 접근으로부터 안전하게 보호해야 한다.	-	○	○	○	○	○	CO-21
정보교환 관 리	내부 또는 외부 조직과 정보교환을 통제하기 위한 절차와 통제를 수립해야 한다.	-	-	○	-	○	○	CO-22
	전송중인 미디어를 보호하기 위해 신원이 증명된 배달부, 안전한 포장, 변조방지 등 보호대책을 강구해야 한다.	○	-	○	-	○	○	CO-23
	전자우편, MSN 등 전자 메세지 서비스 사용에 대한 적절한 보안대책을 강구해야 한다.	○	-	○	○	○	○	CO-24
	그룹웨어, ERP, 파일서버 등을 통해 정보공유시 적절한 보안대책을 마련해야 한다.	○	-	○	-	○	-	CO-25
	전자상거래 정보의 변조를 방지하기 위한 적절한 보안대책을 마련해야 한다.	-	-	○	○	○	○	CO-26
	공적으로 공개되는 정보는 정확성과 완전성을 유지하기 위해 보호해야 한다.	-	-	○	○	○	○	CO-27

(7) 접근통제

평가항목	평가지표	김현수 (1999)	고일석 (2002)	BS7799 (2002)	KISA (2002)	ISO27001 (2005)	NIST (2006)	CODE
사용자책임 및 접근관리	사용자는 패스워드의 사용에 있어 좋은 사례(영 · 숫자 혼합사용 등)를 따라야 한다.	○	○	○	-	○	○	AC-01
	사용자는 자리가 비어있는 장비를 적절하게 보호하여야 한다.	○	○	○	○	○	○	AC-02
	사용자는 책상정리와 화면보호정책을 이행하여야 한다.	○	○	○	○	○	○	AC-03
	정보에 대한 접근을 통제하기 위해 접근통제 정책이 문서화되어야 한다.	○	-	○	○	○	○	AC-04
	사용자의 정보시스템 접근권한을 등록하고 취소하는 절차가 마련되어야 한다.	○	○	○	○	○	○	AC-05
	특별권한의 정보시스템의 사용은 통제되어야 한다.	-	-	○	○	○	○	AC-06
	비인가 사용자의 접근을 통제하기 위해 사용자 패스워드는 공식적 관리절차에 의거 할당되어야 한다.	-	-	○	○	○	○	AC-07
	인사이동, 진급 등과 관련 사용자접근권한을 정기적으로 검토해야 한다.	○	○	○	○	○	○	AC-08

(7) 접근통제(계속)

평가항목	평가지표	김현수 (1999)	고일석 (2002)	BS7799 (2002)	KISA (2002)	ISO27001 (2005)	NIST (2006)	CODE
네트워크 접근통제	사용자의 네트워크 접근은 승인된 서비스에 대해서만 제공되어야 한다.	○	-	○	○	○	○	AC-09
	원격사용자의 내부접근을 통제하기 위한 적절한 인증 방법이 있어야 한다.	-	○	○	○	○	○	AC-10
	특정 장소나 장비로부터 접속인증을 위해 자동장비식별이 고려되어야 한다.	-	○	○	○	○	○	AC-11
	서비스별, 사용자별로 네트워크 사용자 그룹을 분리하여야 한다.	-	○	○	○	○	○	AC-12
	컴퓨터 접속경로와 정보의 흐름경로가 조직의 접근통제정책을 준수해야 한다.	-	○	○	○	○	○	AC-13
운영시스템 접근통제	운영시스템으로의 접근은 인증 등 안전한 보안 로그온 절차에 의해 통제되어야 한다.	-	○	○	○	○	○	AC-14
	모든 사용자는 ID와 인증(패스워드 등)를 사용하여야 한다.	-	○	○	○	○	○	AC-15
	패스워드 관리시스템은 대화식이어야 하며, 좋은 품질이 보장되어야 한다.	-	○	○	○	○	○	AC-16
	시스템 통제에 사용되는 막강한 각종 유틸리티 프로그램의 사용은 통제되어야 한다.	○	○	○	○	○	○	AC-17
	운영시스템의 접근통제를 위해 비활성 세션은 일정시간이 지나면 종료시켜야 한다.	-	○	○	-	○	○	AC-18
어플리케이션 및 정보접근 통제	접근통제 정책에 의거 정보와 응용시스템 접근에 대한 사용자의 권한을 제한하여야 한다.	-	○	○	○	○	○	AC-19
	중요한 정보시스템은 물리적, 기술적으로 별도 분리하여야 한다.	○	○	○	○	○	○	AC-20
모바일 컴퓨팅 및 텔레워킹	PDA, 노트북 등 모바일 컴퓨팅을 외부로 반출하여 사용하는 경우 적절한 보안대책을 수립하여 관리해야 한다.	-	○	○	○	○	○	AC-21
	재택근무를 통해 업무를 수행하는 경우 운영절차를 수립하고 이를 이행해야 한다.	-	○	○	○	○	○	AC-22

(8) 정보시스템 도입 · 개발 · 유지보수

평가항목	평가지표	김현수 (1999)	고일석 (2002)	BS7799 (2002)	KISA (2002)	ISO27001 (2005)	NIST (2006)	CODE
어플리케이션의 정확한 처리	어플리케이션에 대한 입력지침을 통해 입력데이터의 정확성을 보장해야 한다.	○	○	○	○	○	○	IS-01
	어플리케이션 처리지침을 통해 처리오류나 고의적 행동으로 인한 변조를 방지해야 한다.	-	○	○	○	○	○	IS-02
	어플리케이션 출력지침을 통해 출력 데이터의 정확성을 보장하여야 한다.	-	-	○	○	○	○	IS-03
암호통제	중요 정보보안을 위한 암호통제 정책을 수립하여 이행하여야 한다.	○	○	○	○	-	○	IS-04
	암호 키가 손실이나 변조되지 않도록 보호하여야 한다.	-	-	○	○	-	○	IS-05
시스템파일 보안	운영시스템에 S/W 설치를 통제하는 절차가 있어야 한다.	-	-	○	○	○	○	IS-06
	시험데이터는 신중히 선택되고, 안전하게 보호되어야 한다.	-	-	○	○	○	-	IS-07
	프로그램 소스코드에 접근은 제한되어야 한다.	○	-	○	-	○	○	IS-08
개발 및 지원 프로세스보안	어플리케이션 개발과정에 보안 요구사항을 별도로 식별하여 반영하여야 한다.	-	○	○	○	○	○	IS-09
	어플리케이션의 변경은 공식적인 변경절차에 의거 이행되어야 한다.	-	○	○	○	○	○	IS-10
	운영시스템 변경 후 어플리케이션의 안전성을 기술적으로 검토해야 한다.	-	-	○	○	○	○	IS-11
	패키지 변경은 최소화되어야 하며, 모든 변경은 통제되어야 한다.	-	○	○	○	○	○	IS-12
	S/W를 외주로 개발하는 경우 이를 감독하고 감시하여야 한다.	-	○	○	-	○	○	IS-13
	각종 기술적 취약성에 대한 정보를 획득하여 이에 대한 평가가 이뤄져야 한다.	○	-	-	-	○	○	IS-14

(9) 준거성

평가항목	평가지표	김현수 (1999)	고일석 (2002)	BS7799 (2002)	KISA (2002)	ISO27001 (2005)	NIST (2006)	CODE
법적요구사항 준 수	시스템에 관련이 있는 법적 요구사항을 문서화하고 관리해야 한다.	-	-	○	○	○	-	CO-01
	지적재산권과 S/W 저작권 보호를 위한 대책을 이행하여야 한다.	○	○	○	-	○	○	CO-02
	법, 규정, 계약에 의거 중요한 기록이 파괴나 변조되지 않도록 보호해야 한다.	-	-	○	-	○	○	CO-03
	개인정보 등의 중요 데이터는 법적 요구사항에 의거 보호되어야 한다.	-	-	○	-	○	○	CO-04
보안감사	관리자는 책임범위 내 모든 보안절차가 제대로 수행되는지 정기적으로 검토해야 한다.	○	○	○	○	○	○	CO-05
	감사는 신중하게 계획되고 실행되어야 하며, 업무수행에 대한 방해를 최소화하여야 한다.	○	-	○	○	○	-	CO-06
	감사완료시 감사보고서를 작성하여 보고하고, 지적사항이 이행되도록 지속적으로 사후관리 하여야 한다.	-	-	-	○	-	○	CO-07
	정보시스템 감사도구에 대한 접근은 오용이나 손실로부터 보호되어야 한다.	-	-	○	-	○	○	CO-08

〈부록 2〉 평가항목별 평가지표의 일관성 분석결과

평가영역	평가항목	분 석 지표수	내적일관성(Cronbach's α)			탈 락 지표수
			내용타당성	평가용이성	평가신뢰성	
보안정책	보안정책관리	5	0.695	0.660	0.827	0
보안조직	내부조직관리	6	0.712	0.691	0.780	0
	외부기관관리	3	0.724	0.661	0.734	0
자산관리	자산관리	5	0.717	0.696	0.739	0
인원보안	인적자원관리	8	0.788	0.780	0.831	0
	보안사고관리	7	0.849	0.853	0.891	0
물리적 · 환경적 보안	보안구역관리	5	0.809	0.823	0.829	0
	정보처리설비관리	6	0.886	0.795	0.857	0
	업무연속성관리	4	0.832	0.849	0.882	0
통신 및 운영관리	운영절차 및 책임	4	0.801	0.841	0.858	0
	제 3자 서비스 인도관리	2	0.806	0.685	0.703	0
	시스템운영관리	9	0.894	0.894	0.918	0
	네트워크 보안관리	3	0.705	0.697	0.785	0
	매체관리	3	0.710	0.738	0.800	0
	정보교환관리	6	0.864	0.828	0.871	0
접근통제	사용자 책임 및 접근관리	8	0.868	0.880	0.869	0
	네트워크 접근통제	5	0.858	0.814	0.844	0
	운영시스템 접근통제	5	0.737	0.819	0.780	0
	어플리케이션 및 정보 접근통제	2	0.662	0.688	0.649	0
	모바일컴퓨팅 및 텔레워킹	2	0.740	0.740	0.757	0
정보시스템 도입 · 개발 · 유지보수	어플리케이션의정확한처리	3	0.811	0.881	0.901	0
	암호통제	2	0.681	0.747	0.754	0
	시스템파일 보안	3	0.745	0.763	0.773	0
	개발 및 지원 프로세스 보안	6	0.882	0.883	0.903	0
준거성	법적 요구사항 준수	4	0.799	0.867	0.837	0
	보안감사	4	0.828	0.880	0.875	0
합 계		120	-	-	-	0

〈부록 3〉 평가지표별 산술평균 분석결과

평가영역	평가항목	CODE	평균 값			채택여부
			내용타당성	평가용이성	평가신뢰성	
보안정책	보안정책관리	SP-01	4.42	3.93	3.92	채택
		SP-02	4.47	3.71	3.75	채택
		SP-03	4.20	3.25	3.36	채택
		SP-04	4.41	3.67	3.67	채택
		SP-05	4.35	3.75	3.73	채택
보안조직	내부 조직관리	SO-01	4.18	3.76	3.73	채택
		SO-02	4.06	3.47	3.30	채택
		SO-03	4.33	3.61	3.63	채택
		SO-04	4.00	3.92	3.83	채택
		SO-05	4.07	3.46	3.53	채택
		SO-06	4.07	3.54	3.51	채택
	외부 기관관리	SO-07	4.17	3.35	3.45	채택
		SO-08	4.19	3.47	3.45	채택
		SO-09	4.33	3.70	3.63	채택
자산관리	자산관리	AM-01	4.30	3.76	3.73	채택
		AM-02	3.96	3.63	3.55	채택
		AM-03	4.20	3.67	3.55	채택
		AM-04	4.11	3.29	3.33	채택
		AM-05	4.12	3.80	3.71	채택
인원보안	인적자원관리	HR-01	4.27	3.75	3.60	채택
		HR-02	3.71	3.24	3.19	채택
		HR-03	4.30	4.08	3.99	채택
		HR-04	4.47	3.90	3.80	채택
		HR-05	3.48	3.49	3.41	채택
		HR-06	4.04	3.36	3.31	채택
		HR-07	4.48	3.80	3.61	채택
		HR-08	4.64	4.02	3.96	채택
	보안사고관리	HR-09	4.53	3.99	3.92	채택
		HR-10	4.34	3.75	3.61	채택
		HR-11	4.06	3.18	3.12	채택
		HR-12	4.05	3.48	3.49	채택
		HR-13	4.08	3.49	3.48	채택
		HR-14	4.30	3.56	3.51	채택
		HR-15	4.14	3.78	3.71	채택
물리적·환경적 보안	보안구역관리	PE-01	4.37	4.11	4.04	채택
		PE-02	4.49	4.22	4.12	채택
		PE-03	4.25	3.70	3.58	채택
		PE-04	4.25	3.69	3.75	채택
		PE-05	3.98	3.46	3.41	채택

평가영역	평가항목	CODE	평균 값			채택여부
			내용타당성	평가용이성	평가신뢰성	
물리적 · 환경적 보안	정보처리설비 관리	PE-06	4.36	3.80	3.75	채택
		PE-07	4.41	4.02	4.01	채택
		PE-08	4.02	3.58	3.57	채택
		PE-09	4.19	3.75	3.65	채택
		PE-10	4.42	3.58	3.61	채택
		PE-11	4.43	3.46	3.40	채택
	업무연속성관리	PE-12	4.12	3.54	3.47	채택
		PE-13	4.07	3.30	3.29	채택
		PE-14	4.17	3.49	3.39	채택
		PE-15	3.96	3.18	3.19	채택
통신 및 운영관리	운영절차 및 책임	CO-01	4.16	3.55	3.57	채택
		CO-02	4.23	3.51	3.58	채택
		CO-03	3.90	3.37	3.31	채택
		CO-04	4.17	3.55	3.49	채택
	제 3자 서비스 인도관리	CO-05	4.16	3.77	3.70	채택
		CO-06	4.00	3.63	3.46	채택
	시스템운영관리	CO-07	4.16	3.73	3.72	채택
		CO-08	4.13	3.59	3.52	채택
		CO-09	4.07	3.69	3.55	채택
		CO-10	4.30	3.87	3.87	채택
		CO-11	4.25	3.67	3.64	채택
		CO-12	4.17	3.72	3.65	채택
		CO-13	4.20	3.83	3.75	채택
		CO-14	4.12	3.51	3.42	채택
		CO-15	4.35	3.95	3.86	채택
	네트워크보안관리	CO-16	4.14	3.51	3.49	채택
		CO-17	4.01	3.65	3.59	채택
		CO-18	4.34	4.06	3.94	채택
	매체관리	CO-19	4.13	3.79	3.76	채택
		CO-20	4.24	3.64	3.58	채택
		CO-21	4.24	3.59	3.59	채택
	정보교환관리	CO-22	4.00	3.42	3.42	채택
		CO-23	3.77	3.18	3.27	채택
		CO-24	4.10	3.61	3.63	채택
		CO-25	4.17	3.70	3.69	채택
		CO-26	4.20	3.58	3.63	채택
		CO-27	3.92	3.34	3.37	채택
접근통제	사용자 책임 및 접근관리	AC-01	4.33	3.93	3.94	채택
		AC-02	3.98	3.51	3.51	채택
		AC-03	4.02	3.63	3.64	채택
		AC-04	4.13	3.72	3.69	채택
		AC-05	4.12	3.87	3.80	채택
		AC-06	4.22	3.65	3.67	채택
		AC-07	4.08	3.81	3.71	채택
		AC-08	4.10	3.46	3.57	채택

평가영역	평가항목	CODE	평균 값			채택여부
			내용타당성	평가용이성	평가신뢰성	
접근통제	네트워크 접근통제	AC-09	4.27	3.73	3.67	채택
		AC-10	4.37	3.93	3.90	채택
		AC-11	3.78	3.42	3.37	채택
		AC-12	4.05	3.60	3.61	채택
		AC-13	4.04	3.30	3.34	채택
	운영시스템 접근통제	AC-14	4.24	3.89	3.90	채택
		AC-15	4.41	4.08	4.00	채택
		AC-16	3.67	3.43	3.41	채택
		AC-17	3.86	3.24	3.29	채택
		AC-18	4.19	3.82	3.78	채택
	어플리케이션 및 정보접근통제	AC-19	4.20	3.71	3.76	채택
		AC-20	4.20	3.70	3.67	채택
	모바일컴퓨팅 및 텔레워킹	AC-21	4.28	3.58	3.42	채택
		AC-22	3.95	3.29	3.29	채택
정보시스템 도입·개발·유지 보수	어플리케이션의 정확한처리	IS-01	3.95	3.40	3.41	채택
		IS-02	4.07	3.28	3.29	채택
		IS-03	3.84	3.27	3.40	채택
	암호통제	IS-04	4.18	3.58	3.60	채택
		IS-05	4.28	3.59	3.60	채택
	시스템파일 보안	IS-06	4.05	3.58	3.47	채택
		IS-07	3.92	3.35	3.45	채택
		IS-08	4.31	3.67	3.65	채택
	개발 및 지원 프로세스 보안	IS-09	4.12	3.53	3.42	채택
		IS-10	4.16	3.58	3.55	채택
		IS-11	4.02	3.24	3.34	채택
		IS-12	3.99	3.30	3.29	채택
		IS-13	4.19	3.24	3.33	채택
		IS-14	4.00	3.24	3.24	채택
준거성	법적 요구사항 준수	CO-01	4.08	3.67	3.69	채택
		CO-02	4.12	3.60	3.58	채택
		CO-03	4.33	3.59	3.66	채택
		CO-04	4.41	3.64	3.67	채택
	보안감사	CO-05	4.14	3.59	3.60	채택
		CO-06	4.05	3.40	3.31	채택
		CO-07	4.17	3.65	3.55	채택
		CO-08	4.06	3.53	3.49	채택

◈ 저 자 소 개 ◈

이 영 규 (L7307@dreamwiz.com)

현재 중소기업기술정보진흥원 정보화사업부에 차장으로 재직 중이며, 연세대학교에서 경영학 석사, 광운대학교 경영정보학과에서 박사를 취득하였다. 정보화추진과 관련하여 전략지휘소자동화체계사업(전략C4I)과 과학화전투훈련장구축사업(KCTC)에 참여한 적이 있다. 또한 정보보안과 관련하여 BC카드, 수협중앙회, 전라북도 보안컨설팅 프로젝트 등에 참여하였으며, 중소기업 역기능방지사업과 중소기업 기술유출방지사업을 담당하여 추진한 적이 있다. 주요 관심분야는 정보화경영체제, 정보보안, 프로젝트관리기법 등이다.

김 상 훈 (shkim@kw.ac.kr)

현재 광운대학교 경영정보학과 교수로 재직 중이며, 서울대학교 경제학과를 졸업하고 한국과학기술원(KAIST) 경영과학과에서 석사 및 박사를 취득하였다. Information and Management, Information Processing and Management, Computer (ACM SIGCPR), Information Resources Management Journal 등의 국제학술지 및 경영학연구, 한국경영과학회지, 경영정보학 연구 등의 국내학술지에 논문을 게재한 바 있다. 주요 관심분야는 정보화 전략 수립 및 추진, 정보시스템실행을 위한 변화관리, 경영혁신과 정보기술활용, 정보시스템평가, ERP(Enterprise Resource Planning) 시스템 구현, S/W 개발 프로젝트관리 등이다.