情報保護學會論文誌
第 22 卷 第 5 號, 2012. 10

정보보호 관리체계의 지속적인 정보보호 관리과정(PDCA)이 정보보호 성과에 미치는 영향에 관한 실증 연구

장 상 수,[1†] 이 상 준,[2‡] 노 봉 남[2]
[1]한국인터넷진흥원, [2]전남대학교

The effects of the operation of an information security management system on the performance of information security

Sang-soo Jang,[1†] Sang-joon Lee,[2‡] Bong-nam Noh[2]
[1]KISA, [2]Chonnam University

요 약

최근에는 정보보호 및 개인정보보호 관련 컴플라이언스 요구에 의한 정보보호 관리체계는 선택의 문제가 아니라 필수 문제로 부각되고 있다. 이러한 맥락에서 정보보호 관리체계 운용과 관리과정이 현실적 상황에서 얼마나 도움이 되고, 실효성 있는지를 실증적으로 검증하기 위해 측정 항목을 설정하고, 실제 보안전문가인 조직의 정보보호 관리체계 운영 담당자를 대상으로 설문조사를 실시하였고 이를 통해 신뢰성 및 타당성 분석을 실시하였다.

본 논문에서는 정보보호 관리과정이 정보보호 성과에 미치는 영향에 대해 알아보기 위해 확증적차원(confirmatory)에서 구조방정식에 사용되는 PLS(Partial Least Square, SmartPLS 2.0)를 이용한 1차 요인분석과 마지막으로 2차 요인분석을 하였다.

연구 결과 연구 모형에 대한 가설 검정 결과 총 16개중 채택 8개, 기각8개로 나타났으며, 정보보호 관리체계 관리과정이 대부분 정보보호 성과에 영향을 미치나 계획단계, 실행단계, 점검단계가 직접적인 영향을 미치는 것으로 나타났다.

ABSTRACT

Many domestic organizations are introducing and operating various information security management systems capable of coping with technical, administrative, and legal issues comprehensively and systematically, in order to prevent various infringement incidents such as personal information disclosure and hacking preemptively and actively. However, empirical analyses regarding the extent to which an information security management system contributes to information security performance have not been fully conducted, even though enterprises and organizations are actively introducing such systems in order to achieve their information security objectives as a part of their organizational management activities in line with their respective business, by investing considerable effort and resources in developing and operating these systems. This approach can be used to apply, develop, and operate the information management system actively within an organization. this study focused on analyzing how each specific phase of the information security management system affects information security performance, compared with previous studies, which generally focus on the information security control item in analyzing information security performance. The information security management system was analyzed empirically to determine how the Security PCDA cycling model affects information security performance.

Keywords: ISO27001, ISMS, PIMS, G-ISMS, RMF, Information Security Evaluation, Information SecurityPerformance, PLS

접수일(2012년 6월 11일), 수정일(2012년 9월 7일),
게재확정일(2012년 9월 27일)

† 주저자, ssjang0116@gmail.com
‡ 교신저자, s-lee@jnu.ac.kr

I. 서 론

1.1 연구 배경 및 목적

최근 IT 융·복합 환경의 급속한 변화로 인해 개인정보 및 기업정보 등 정보자산에 대한 위협 및 취약성을 어느 때보다 매우 심각하게 인식하게 되었으며, 이에 대한 적절한 위험관리 활동이 필요하게 되었다. 이를 위해 조직에서 정보자산을 보호하고 조직경쟁력을 강화하기 위한 수단으로 정보보호관리 프로세스 개선 활동의 하나로 정보보호 관리체계 구축 및 운용에 지속적인 노력을 기울이게 되었다. 사이버 공격에 능동적이고 선제적으로 대응하고 침해사고에 대해 사전적 예방을 위해서 국내·외적으로 정보보호 관리체계 도입을 제도화 하고 있다.

현재 국내·외에서 적용하고 있는 정보보호 관리체계로는 ISO27001(Information security management systems Requirements), NIST SP800-39(Managing Risk from Information Systems An Organizational Perspective), KISA ISMS(Korea Internet & Security Agency Information Security Management System, 정보보호 관리체계), PIMS(Personal Information Management System, 개인정보보호 관리체계), G-ISMS(Government-Information Security Management System, 전자정부 정보보호 관리체계), ISCS(Information Security Check Service, 정보보호 안전진단), CIIP(Critical Information Infrastructure Protection, 주요정보통신기반시설 취약점 분석·평가) 등에 대해 시행해 오고 있지만, 정보보호 특성상 성과나 효과로 나타내기에는 어려움이 있다.

따라서 본 연구의 목적은 국내 정보보호 관리체계를 구축·운용하는 조직을 대상으로 관리체계가 정보보호 성과에 영향을 미치는지 검증하기 위해 정보보호 관리과정인 PDCA(계획, 실행, 점검, 개선) 단계별 측정항목을 도출하고, 이를 토대로 정보보호 성과의 영향요인을 찾아내어 정보보호 관리체계 관리과정이 조직의 정보보호 성과에 미치는 영향을 실증적으로 분석하고자 하였다.

1.2 연구의 범위 및 방법

국내외적으로 수년전부터 적용 및 운용하고 있는 정보보호 관리체계인 ISO27001, NIST SP800-39, KISA ISMS, PIMS, G-ISMS, ISCS, CIIP 등에 대한 관리체계 프레임워크를 분석하여 정보보호 순환구조에 대한 모형과 선행 연구를 통해 정보보호 성과에 대한 측정 항목을 도출하였다.

본 논문에서는 가설 검정을 위해 각 독립변수가 정보보호 성과에 미치는 영향을 알아보기 위해 사회과학 분야에서 얻은 각종 자료를 컴퓨터를 이용해 쉽고 편리하게 분석하는 통계 전문 프로그램으로 전문 통계 패키지 중 가장 많이 쓰는 SPSS v17.0(Statistical Package for the Social Sciences)을 이용하여 통계분석을 실시하였다.

본 논문에서는 현재의 정보보호 관리체계인 ISO27001, NIST SP800-39, KISA ISMS, PIMS, G-ISMS, ISCS, CIIP등에 대해서 정보보호 관리과정을 비교 분석하여 공통 측정 항목을 도출하여 정보보호 관리과정과 정보보호 성과 측정 항목을 설정하여 실증분석을 통해 정보보호 관리 노력의 방향과 성과 향상 방법을 찾기 위한 기준을 제시하여, 경영성과 차원에서 효과적인 정보보호 투자와 의사결정을 하는데 도움을 주고자 하였다.

II. 관련 연구

2.1 정보보호 관리체계(S-PDCA) 비교 분석

PDCA 모형을 기반으로 정보보호 관리체계에서 공통적으로 적용하고 있는 관리과정의 구체적인 요구

〔표 1〕 S-PDCA 단계별 측정항목 비교

매개변수	관리과정	정보보호 관리체계 활동	연구문헌
정보보호 계획 단계 (Plan)	관리체계 범위설정	조직의 특성에 따라 조직의 핵심업무를 포함하는 관리체계의 적용 범위를 정의	ISO27001, G-ISMS, NIST, KISA-ISMS, PIMS, ICSC
	정보보호 정책수립	경영목표를 지원할 수 있도록 전략적이고 조직적인 위험관리를 총체적으로 기술한 정보보호 정책을 수립	ISO27001, G-ISMS, KISA-ISMS, PIMS, ICSC, CIIP
	위험관리 계획수립	조직의 목표 및 정책, 법적 요구사항 등을 고려하여 조직, 역할, 책임, 핵심업무 주요과정을 포함한 위험관리 전략 및 계획을 수립	ISO27001, G-ISMS, NIST, KISA-ISMS, PIMS, ICSC
	위험분석 및 평가	보유한 정보자산, 위협&취약성, 위험을 식별하고 분류하고, 정보자산의 가치와 위험을 고려하여 잠재적 손실에 대한 영향을 식별·분석	G-ISMS, KISA-ISMS, PIMS, 안전진단, CIIP

매개변수	관리과정	정보보호 관리체계 활동	연구문헌
	보호대책 선택	위험분석 및 평가에 의거하여, 위협처리 전략을 설정하고, 보호대책 및 통제사항 선택	ISO27001, G-ISMS, KISA-ISMS
정보보호 실행계획 (Do)	정보보호대책 계획수립	선택한 정보보호대책 및 통제사항을 구체적으로 구현하기 위한 계획을 상세하게 수립	ISO27001, G-ISMS, KISA-ISMS, PIMS, ICSC, CIIP
	정보보호 대책 구현	수립된 정보보호대책 계획을 근거로 정보보호 대책을 구현하도록 적절한 관리 조치와 통제항목 등에 맞게 적절하게 구현	ISO27001, G-ISMS, KISA-ISMS, PIMS, ICSC, CIIP
	정보보호 교육 및 훈련	정보보호 교육 및 훈련 프로그램을 수립 및 이행	G-ISMS, KISA-ISMS, CIIP, ISO27001,
	보호대책 유효성 설정	정보보호 계획 및 대책구현, 정보보호 교육과 훈련 등이 유효성을 측정을 위한 측정요소 정의	ISO27001, G-ISMS, KISA-ISMS, PIMS, ICSC, CIIP
정보보호 점검단계 (Check)	모니터링 검토	통제항목을 대상으로 상시 모니터링을 실시하고 기록 등을 유지	ISO27001, G-ISMS, KISA-ISMS,
	보안(내부) 감사	정기적으로 내부감사 수행하고 그 결과의 보고, 기록 유지	ISO27001, G-ISMS, NIST, KISA-ISMS, CIIP
	보안통제 유효성 평가	통제항목 등의 보안수준을 지속적으로 측정하고 평가	ISO27001, G-ISMS, NIST, KISA-ISMS, CIIP
	관리체계 재검토	관리체계의 효율성, 범위의 적절성, 위험수준, 보안절차 등의 관리체계를 적용성을 재검토	ISO27001, G-ISMS, NIST, KISA-ISMS,
정보보호 개선단계 (Act)	개선사항 조치	정보보호 정책, 정보보호 목적, 감사 결과, 사건 분석, 시정 및 예방조치, 검토 등 통해 ISMS를 지속적으로 개선	ISO27001, G-ISMS, NIST, KISA-ISMS, PIMS, ICSC
	개선조치 결과검토	개선요구 사항에 따른 조치결과를 공식적으로 조직 내 공지하여 목적달성 이행여부를 확인	ISO27001, G-ISMS, KISA-ISMS, PIMS, ICSC, CIIP

사항을 분석해서 정보보호 PDCA 모형으로 재분류하면 〔표 1〕과 같다.

2.2 국내·외 정보보호 성과 측정 체계 비교 분석

본 연구에서는 선행 연구 분석을 통해 〔표 2〕처럼 정보보호 성과를 정보보호 안전, 정보보호 기반, 정보보호 경영성과 등 3개영역으로 구분하였다. 이에 따른 안전성과, 기반성과, 경영성과 등 종속변수를 선정하였다.

〔표 2〕 국내 정보보호 성과 요인 선행연구 분석

연구문헌	정보보호성과 측정분류	비고
김경규〔01〕	고객정보안전도	안전성과
	정보보호 인식제고(인식제고)	안전성과
	정보자산통제도(자산손실방지)	안전성과
	악성코드 등 침해사고 조치율(보안사고)	기반성과
김태성〔02〕	위험관리대응도(위험관리)	안전성과
	정보보호 인식제고(교육/투자)	안전성과
	정보자산통제도(정보자산)	안전성과
	통합보안 적용성(운영관리, 정보보호 인프라)	기반성과
	업무만족도(내부이용 만족도)	경영성과
서한준〔03〕	악성코드 등 침해사고 조치율(분석능력증진)	기반성과
	업무만족도(생산성 증진)	경영성과
	매출증대(시장점유율증진(신규매출)	경영성과
	처리비용절감(비용절감(일반/원가/유통. 업무처리시간 단축)	경영성과
선한길〔04〕	정보자산통제도(자산의 손실건수 감소)	안전성과
	악성코드 등 침해사고 조치율(사고발생시 신속한 처리)	기반성과
	조직의 경쟁력증진(타사 경쟁 시 손해 감소, 이미지 실추건수 감소)	경영성과
	처리비용절감(비즈니스 기회손실 감소)	경영성과
이종선·이희조〔18〕	위험관리대응도(위험규모의 평가, 위험분석 선생)	안전성과
	유지보수 통제(정보보호활동 유지)	기반성과
홍기향〔08〕]	악성코드 등 침해사고 조치율(정보보호사고)	기반성과
BCMM	정보보호 인식제고(임직원 인식수준)	안전성과
	정보자산통제도(자원 지원)	안전성과
ISM3〔09〕	접근권한설정도(접근통제)	기반성과
	통합보안 적용성(개발보안)	기반성과
ISO27004〔10〕	법적요구준수도(법적준수,보안감사, 법적준수법과계약/요구준수,법적준수 보호규정, 관리체계효율(보안정책))	안전성과
	위험관리대응도(위험평가 및 처리, 입출력관리)	안전성과
	정보보호 인식제고(관리체계효율교육)	안전성과
	매출증대 (경제적성과 매출증대)	경영성과
	처리비용절감 (경제적성과 비용절감)	경영성과
	이미지 증대(조직의 가치증진)	경영성과
KISA〔06〕	통합보안 적용성(시스템과 데이터보호, 정보보호기반지수)	기반성과
	업무만족도(업무효율성)	경영성과
	악성코드 등 침해사고 조치율(해킹바이러스 침해, 개인정보 침해)	기반성과
	처리비용절감(피해절감)	경영성과
	매출증대	경영성과
	고객정보안전도(고객정보 안전관리)	안전성과
	조직의 경쟁력증진(경쟁력강화)	경영성과
	이미지 증대(조직의 가치증진)	경영성과
Marianthi〔13〕	법적요구준수도(감사 및 모니터링)	안전성과
	접근권한설정도(접근통제)	기반성과
	악성코드 등 침해사고 조치율(보안사고 대응, 대응 절차)	기반성과
Moulton〔14〕	위험관리대응도(위험관리 활동, 위험분석, 위험 식별)	안전성과
	정보보호 인식제고(교육 활동)	안전성과
	유지보수 통제(정보보호활동 유지)	기반성과
NIST SP800-55〔15〕	통합보안 적용성(정보보호프로그램 구현 수준 결정, 프로그램 구현)	기반성과
Shuchih Ernest Chang〔17〕	법적요구준수도(법규준수 , 보안정책)	안전성과
	정보자산통제도(자산 식별 및 통제)	안전성과
	유지보수 통제(시스템 개발 및 유지보수)	기반성과
	접근권한설정도(접근통제)	기반성과
	통합보안 적용성(물리적 보안, 시스템관리)	기반성과

III. 연구모형 및 가설설정

3.1 연구모형

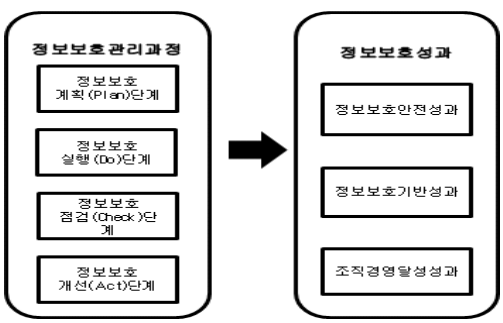
본 연구는 조직에서 도입 및 운용중인 정보보호 관리체계 관리과정과 정보보호 성과들을 변수로 설정한 후, 이들 간의 상관관계를 연구하고자 다음 〔그림 1〕에서 보는 바와 같은 연구모형을 설정하였다.

기본 연구 모형에서 정보보호 관리체계의 가장 중요한 부분인 관리과정을 PDCA 이론에 근거하여 재분류하면 계획단계, 실행단계, 점검단계, 개선단계로 분류하고 이 과정은 정보보호 목적을 달성하기 위하여 정보보호 관리체계를 위한 계획을 수립하고 실행하고 점검하고 개선하는 일련의 단계로써, 가장 중요한 위험분석과 이에 대한 대책을 선정하고 구현하는 활동을 의미한다. 그동안 정보보호 관리체계에 관한 선행 연구는 주로 통제항목을 중심으로 이루어졌다. 본 연구는 이러한 분석 이외에 정보보호 관리체계의 관리과정인 계획, 실행, 점검, 개선 단계들이 원활하게 진행되었을 때 정보보호를 통한 성과가 충분히 달성될 수 있는지를 실증적으로 분석한다.

본 연구에서 제시한 "정보보호 관리과정"은 정보보호 관리체계 프레임워크의 가장 중요한 부분으로 정보보호 관리체계의 기본 철학인 PDCA 순환주기를 반영한 Security PDCA의 순환주기로 정보보호 정책을 수립, 조직을 구성하고 책임을 설정하며, 범위와 자산을 식별하고 위험관리와 정보보호 대책을 구현하고 상시적인 모니터링, 재검토 등 일련의 과정으로 정보보호 관리체계의 순환주기로 정의하였다.

3.2 가설설정

정보보호 성과는 정보보호 관리체계 운용 전반에 대해서 뿐만 아니라 관리과정 각 단계의 다양한 요인에 의해 영향을 받는다. 따라서 정보보호 관리체계 구축 및 운용에 가장 중요한 요소로 정보보호 관리과정의 독립변수들은 종속변수인 정보보호 성과에 영향을 미치게 된다.



〔그림 1〕 연구모형

3.3 변수의 조작적 정의 및 설문구성

본 연구에서는 연구의 개념적 틀을 검정하기 위하여 16개의 가설로 연구문제를 설정하고, 관리과정 17개와 정보보호 성과에서 15개 총 32개의 측정항목을 통해 각 측정항목의 정도를 측정하기 위하여 리커트(Likert) 5점 척도로 측정하였다. 척도의 1은 `매우 아니다`로 그 변수가 미친 영향이 낮은 것을 의미하고, 척도의 5는 `매우 높다`로 그 변수의 영향이 아주 큰 것을 의미한다.

본 연구의 실증분석에 사용되는 측정항목은 관련 연구와 전문가 검토를 통하여 그 타당성이 입증된 설문 측정항목을 수정하고 보완하여 설계하였다.

선행연구와 전문가 검토에서 개발된 측정도구는 정보보호 관리체계의 관리과정인 계획, 실행, 점검, 개선 등 분야에서 17개, 정보보호 성과 분야에서 15개 총 32개 측정항목을 리커트(Likert) 5점 척도로 측정하였다. 설문지는 크게 5부분으로 구성하였는데, 독립변수는 17개 측정항목으로 계획(Plan)에서는 4개 측정항목, 실행(Do)에서는 5개 측정항목, 점점(Check)에서는 4개 측정항목, 개선(Act)에서는 4개 측정항목을 리커트(Likert) 5점 척도로 측정하였다.

종속변수인 정보보호 성과를 측정하기 위한 정보보호 안전성과에서 5개, 정보보호 기반에서 5개, 정보보호 성과에서 5개 총 15개 측정항목을 리커트(Likert) 5점 척도로 측정하였다.

3.4 변수와 측정요소

정보보호 관리체계 단계별 관리과정이 정보보호 성과에 미치는 영향에 대해 분석하기 위하여 S-PDCA 모형을 기반으로 계획(Plan)단계, 실행(Do)단계, 점검(Check)단계, 개선(Act)단계의 독립변수와 정보보호 성과를 종속변수로 정의하였다.

IV. 통계분석

통계분석은 회수된 설문지를 분석하고 해석하는 장

으로, 표본 특성을 대상으로 인구 통계적 특성분석, 이 연구의 측정변수들에 대한 신뢰성, 타당성, 상관성 분석 및 기술적 통계를 분석하였다. 그리고 본 연구에서 정립한 연구가설을 검정하고 상세하게 해석하였다.

4.1 표본의 특성

조사 표본은 주요 정보제공자로서 정보보호 관리체계 구현 및 인증에 대하여 적극적으로 참여한 경험이 있는 조직의 정보보호 관리체계 담당자, 정보보호최고책임자 및 전문가를 중심으로 연구대상으로 수집하였다.

본 연구에서 이용될 자료의 신뢰성과 타당성을 높이기 위해 정보보호 관리체계 외부전문가들(예: 정보보호 컨설턴트, 학계, 인증심사원 등)의 면담을 통해 정보보호 관리체계 특성과 추진과정, 관리체계 이후의 방향성, 운용성과 및 오랜 실무경험 등을 토대로 연구과정에서 오차를 최소화하였다.

설문 설계를 통해 2011년 2월 예비조사(Pilot Test)를 실시하여 신뢰성을 저해 할 가능성이 있는 측정항목을 일부 수정하였으며, 본 조사는 2011년 2월 18일부터 03월 02일까지 정보보호 관리체계를 운용경험이 있는 전문기관(공공, 민간) 에 설문지를 배포하여 수집하였다.

설문 회수 현황은 다음 〔표 3〕과 같이 총 400부의 설문을 배포하여 117개의 설문지가 회수되었으며, 설문 중 결측치를 포함한 30개의 설문지를 제외한 87개의 설문지로 최종 분석하였다.

〔표 3〕 기업 및 기관에 대한 설문 회수 현황

구분	배포	회수	결측치	분석설문
배포 설문수	400	117	30	87
비율	100%	29%	7.5%	21.7%

4.1.1 신뢰성 분석

내적 일관성법은 동일개념의 측정을 위해 여러 개의 항목을 이용하는 경우 신뢰도를 저해하는 항목을 찾아내어 측정 도구에서 제외시켜 측정도구의 신뢰도를 높이는 방법으로 보통 Cronbach's alpha값을 이용한다. 연구변수의 신뢰성분석 결과는 〔표 4〕에서 보는 바와 같다.

일반적으로 개인수준은 Cronbach's Alpha값이 0.7이상, 집단수준은 Cronbach's Alpha값이 0.6 이상이면 비교적 신뢰성이 높다고 인정한다. 이러한

〔표 4〕 연구변수의 신뢰성 분석 결과

요인(변수)		항목수	Cronbach's Alpha
정보보호 계획단계		4	0.932
정보보호 실행단계		5	0.964
정보보호 점검단계		4	0.934
정보보호 개선단계		4	0.944
정보보호 성과 (Outcome)	안전성과	5	0.904
	기반성과	5	0.909
	경영성과	5	0.928
계		32	

내적 일관성법 이외에도 신뢰성은 측정된 변수들의 일관성, 정확성, 의존가능성, 안정성, 예측가능성과 관련된 개념을 의미하는 것으로, 동일한 개념에 대해 측정을 반복했을 때 동일한 측정값을 얻을 가능성을 말한다.

내적 일관성법은 동일개념의 측정을 위해 여러 개의 항목을 이용하는 경우 신뢰도를 저해하는 항목을 찾아내어 측정 도구에서 제외시켜 측정도구의 신뢰도를 높이는 방법으로 보통 Cronbach's alpha값을 이용한다.

일반적으로 신뢰성 계수는 0.7이상으로 무난한 것으로 판단되며, 측정요소의 신뢰성은 높다고 판단할 수 있다.

본 연구에서 측정했던 변수들은 신뢰성 계수가 대부분 0.9이상이고, 가장 낮은 값을 보인 "정보보호 안전성과"도 0.904로 권장치를 초과하는 수치를 보여주고 있어 설문조사의 측정결과에 대한 신뢰성은 매우 높다고 할 수 있다.

4.2 구조방정식을 통한 분석

본 연구에서는 정보보호 관리과정이 정보보호 성과에 미치는 영향을 평가하기 위해 우선적으로 제3절을 통해 회귀분석 방법으로 탐색적인 분석결과를 제시하고 있으며, 본 제4절에서는 확인적인 분석 방법으로 연구모형의 설명력을 높이기 위해 구조방정식모형을 통한 연구모형에 대한 실증분석을 수행하였다.

본 연구에서 구조방정식모형을 이용한 분석에 사용되는 도구(tool) 중에서 대표적으로 사용되는 최소부분자승법(PLS: Partial Least Square)를 이용하여 수집된 데이터를 분석하였으며, 연구모형의 분석을 위한 통계 패키지로 SmartPLS 2.0을 활용하였다.

본 절에서 다루어질 구조방정식모형(SEM : St-

ructural Equation Model)은 측정모형(Measurement Model)과 이론모형(Structural Model)을 통해서 모형간의 인과관계를 파악하는 방정식을 의미하며, 흔히 구조방정식모형은 구성개념(construct)[1] 간의 이론적인 인과관계와 상관성의 측정지표를 통한 경험적 인과관계를 분석할 수 있도록 개발된 공분산 구조방정식(Covariance Structural Modeling)의 통계기법이다. 구조방정식모형은 확인요인분석(confirmatory factor analysis)을 통하여 측정오차가 없는 잠재요인을 발견하고 회귀분석으로 잠재요인들을 연결하는 방법이다. 구조방정식 모형을 통해서 다중변수관계를 포괄적으로 측정하고 탐색적인 분석에서 확인적인 분석까지 실시할 수 있는 전체적이고 체계적인 분석 방법이다. 한마디로 구조방정식 모형은 인과관계를 위하여 요인분석과 회귀분석을 발전적으로 결합한 형태라고 할 수 있다.

4.2.1 1차 요인의 측정모형 분석

본 연구에서 구조모형에 대한 실증분석을 위해 전체 87개의 표본을 사용하였다. 또한 실증분석은 가설검정 이전에 변수의 신뢰성, 수렴타당성과 판별타당성 분석을 통해 측정모형을 평가한 뒤 이의 분석결과를 바탕으로 구조모형을 평가함으로써 구성개념 간 경로의 유의성을 검증하였다. 이때 실증분석에서는 32개의 연구변수를 활용하였다. 이들 연구변수는 5점 척도로 조사에 사용되었으며, 지표의 방향성은 관측변수가 개념의 실제 값을 반영하고 있음을 의미하는 반영지표(reflective indicator)로 측정되었다.

먼저, 정보보호 관리과정과 정보보호 성과의 1차 요인에 대한 측정모형의 수렴타당성을 평가하기 위해 모든 측정항목의 요인적재량(item to construct loadings)을 구하였다. 개별 측정항목과 관련된 변수가 서로 공유한 분산(shared variance)이 오차분산(error variance)보다 크기 위해서는 요인적재량(standardized loadings)이 0.7 이상의 수용기준이 요구된다. 이에 따라 측정항목에 대한 1차 요인적재량과 교차적재량을 분석한 결과 대부분의 요인적재량의 t-값(t-value)이 모두 2.576을 초과하여 1% 유의수준에서 유의한 것으로 나타났다.

다음으로 구성개념에 대한 신뢰성 평가는 Cronbach-α와 유사한 종합요인 신뢰성 지수인 CSRI (composite scale reliability index)와 분산추출지수인 AVE(average variance extracted)값을 이용하였다. 일반적으로 CSRI가 0.7 이상이면 각 변수가 내적일관성이 있다고 판단하며 개념 신뢰성을 만족시키기 위해 AVE 값이 0.5이상 되어야 한다. 아래의 〔표 4〕에서 알 수 있듯이 정보보호 관리활동과 정보보호 성과와 관련된 1차 요인(first order factor)의 AVE 값이 수용기준을 상회하는 것으로 나타나 수렴타당성을 확보한 것으로 평가하였다.

그리고 정보보호 관리과정 및 정보보호 성과를 구성하는 1차 구성개념에 대한 판별타당성을 평가하기 위해 AVE의 제곱근을 산출하였다. AVE 제곱근은 0.7이상이며, AVE 제곱근이 다른 구성개념의 상관계수 값보다 커야 판별타당성이 있는 것으로 판단 한다

따라서 본 연구에서 사용된 구성개념들은 모두 판별타당성을 확보한 것으로 나타났다.

4.2.2 1차 요인의 구조모형 분석

다음으로 가설로 설정된 1차 요인에 대한 구조모형을 평가하기 위해 개별경로 간 유의성을 검정하였다. 구조모형의 분석결과에 따른 측정된 경로계수는 화살표 위에 표기하였으며, 괄호 안에 t-값을 표기하였다. 또한, 공분산 경로는 내생변수들 간에만 연결이 가능하며 연구개념 안에 경로분석 결과에 의한 내생변수(endogenous)들의 설명된 분산(variance explained (R^2))을 표기함으로써 연구 개념의 설명력을 나타내었다. 경로계수 아래 표시된 t-값은 부트스트랩(bootstrapping)을 통한 반복추출 서브샘플링 생성을 통해 계산된 값으로 서브샘플링의 수는 500회로 분석하였다

본 연구모형의 개별 경로를 살펴보면 정보보호 관리체계 관리과정에서 계획단계는 기반성과에 긍정적 영향($t = 3.258$, $p < 0.01$)을 미치는 것으로 나타났으며, 점검단계는 안전성과에 긍정적 영향($t = 2.144$, $p < 0.05$)을 미치는 것으로 나타났다. 또한, 점검단계는 달성성과에 $t=2.073$($p < 0.05$)으로 통계적으로 유의하게 나타나 긍정적 영향을 미치는 것으로 분석되었다.

요약하면 연구가설에 대한 검정결과 계획단계에서는 기반성과, 점검단계에서는 안전성과와 경영성과의

1) 구성개념(construct) : 잠재변수(latent variables)이라 부르며 직접적인 관찰이 불가능한 변수를 의미한다. 내용이 유사한 변수들이 서로 높은 상관관계를 나타낼 때 이러한 변수들의 영향을 주는 공통원인으로 구성개념이라 할 수 있다.

〔표 5〕 구조방정식 연구가설 검정결과

가설경로(인과관계)			가설	경로	t-값	R^2	p값	검정
가설	From	To	방향	계수				결과
H1-1	계획	안전	+	0.060	0.428	0.455	-	기각
H1-2	실행	안전	+	0.253	1.914	0.455	-	기각
H1-3	점검	안전	+	0.316**	2.114	0.455	p 〈0.05	채택
H1-4	개선	안전	+	0.124	0.867	0.455	-	기각
H2-1	계획	기반	+	0.352**	3.404	0.643	p 〈0.01	채택
H2-2	실행	기반	+	0.153	1.223	0.643	-	기각
H2-3	점검	기반	+	0.294	1.775	0.643	-	기각
H2-4	개선	기반	+	0.110	0.829	0.643	-	기각
H3-1	계획	경영	+	-0.042	0.311	0.328	-	기각
H3-2	실행	경영	+	0.128	0.934	0.328	-	기각
H3-3	점검	경영	+	0.329**	2.155	0.328	p 〈0.05	채택
H3-4	개선	경영	+	0.205	1.214	0.328	-	기각

※ 주) **: 유의수준 p〈0.01 *: 유의수준 p〈0.05
※ 유의확률 검정값(t-값) : t 〈1.96 일 경우 p 〈0.05, t 〈2.54 일 경우 p 〈0.01에서 유의

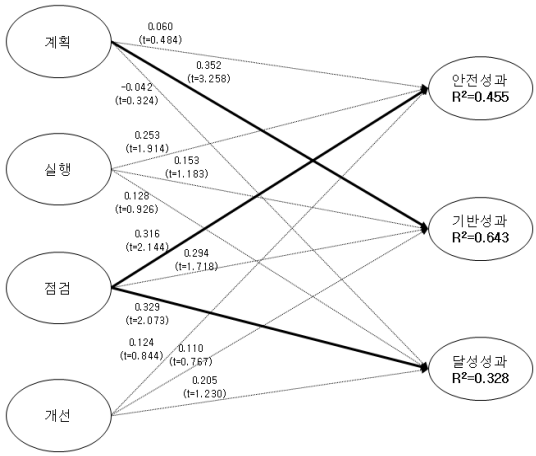
인과관계가 통계적으로 유의하여 채택되었다. 하지만 요약하면 다음의 〔표 5〕와 같이 연구가설에 대한 검정결과 계획단계에서는 기반성과, 점검단계에서는 안전성과와 경영성과의 인과관계가 통계적으로 유의하여 채택되었다. 하지만 실행 및 개선단계는 경로계수의 t-값이 통계적으로 유의하지 않아 모두 기각되었다.

실행 및 개선단계는 경로계수의 t-값이 통계적으로 유의하지 않아 모두 기각되었다.

이처럼 실행 및 개선단계가 모두 기각된 이유는 본 연구를 위해 참조한 선행연구들에서 발생하는 인지적 차이에서 발생한다고 볼 수 있다. 기존 연구들이 경영학 또는 관리적 차원에서 접근한 유사 정보보호 선행연구들이기 때문에 실질적인 정보보호 분야와 관련된 연구를 본 연구에 반영하는 정도가 미흡했거나 또는 부족했기 때문이다. 이에 따라 이들 선행연구를 토대로 수립된 본 연구의 연구모형과 설문내용이 정보보호의 실무적 차원에서 대입하기에 약간의 괴리를 발생시킨 것으로 판단할 수 있다.

두 번째로, 기존 연구에서 연구결과는 조직 내 정보보호를 담당하는 실질 응답자를 대상으로 하지 않았기 때문이라 할 수 있다. 즉, 기존 연구에서는 일반 정보시스템 관리자를 대상으로 평가한 내용을 근간으로 정보보안의 효과를 유추하기 때문에 동일한 질문에 정보보호를 담당하는 응답자에게서는 다른 연구결과가 도출되었다고 볼 수 있다.

세 번째로, 본 연구에서 적용한 설문대상자에도 문제가 있을 수 있다. 본 연구를 위해 정보보호 관리체계 운용에 대한 정보보호 성과를 민간 인증취득 기업뿐만 아니라 공공기관의 정보보호담당자 및 최고책임자에게 질문하였기 때문에 나타나는 문제라 판단할 수도 있다. 즉, 민간기업 에서는 정보보호 성과를 특정 경제적 편익의 차원에서 평가하지만, 공공기관에서는 경제적 측면보다는 보안사고 없이 업무지속성(business continuity)이 유지되는 상황을 정보보호 성과라 평가할 수 있기 때문에 나타나는 정보보호성과를 판단하는 괴리에서 발생한 결과로도 볼 수 있다.



〔그림 2〕 1차 요인의 구조모형 분석 결과

※ 주) 괄호 위 경로계수, 괄호 안 t-값
**: 유의수준 p〈0.01, *: 유의수준 p〈0.05

4.2.3 2차 요인의 측정모형 분석

다음으로 연구모형에서 2차 요인(second order factor)으로 개념화한 정보보호 관리과정과 정보보호 성과의 1차 요인을 통해 측정되는지를 살펴보았다. 통상 PLS가 2차 요인에 대한 분석을 지원하기 않기 때문에 복수의 측정항목으로 구성된 1차 요인을 PLS 분석에 적합하도록 단일 측정치로 변환하여 2차 구성개념의 측정지표로 사용한다. 이때 복수의 측정치를 단일 측정치로 변환하는데 요인점수(factor score), 다변량[2] 평균(multi-variate mean), 요인가중치를 이용한 가중평균값 등을 사용한다

본 연구에서는 잠재변수 요인점수를 사용하여 정보

2) 다변량 분석 : 변수들 간의 인과관계를 규명·분석하거나 변수들 간의 상관 관계를 이용하여 변수를 축약하거나 개체들을 분류하는데 관련된 분석방법.

보호 관리과정과 정보보호 성과에 대한 2차 요인의 측정모형을 평가하였다.

2차 요인 역시 1차 요인에서 활용한 분석절차와 기준에 따라 수렴타당성, 내적일관성, 판별타당성이 평가되었으며, 2차 요인으로 구성한 요인 적재량의 t-값은 모두 2.576을 초과하여 1% 유의수준에서 유의한 것으로 나타났다. 또한, 2차 요인들이 수렴타당성과 판별타당성의 기준을 상회하는 것으로 나타났다. 이때 2차 요인인 정보보호 관리과정은 계획단계, 실행단계, 점검단계, 개선단계에 관한 4개의 1차 요인을 측정한 총 17개의 항목으로 측정되었으며, 2차 요인인 정보보호 성과는 안전성과, 기반성과, 경영성과의 3개 1차 요인을 측정한 15개의 측정항목으로 평가되었다.

4.2.4 2차 요인의 구조모형 분석

다음으로 가설로 설정된 구조모형을 평가하기 위해 개별 경로 간 유의성을 검정하였다. 〔그림 2〕에서 구조모형의 분석결과에 따른 측정된 경로계수는 화살표 위에 표기하였으며, 괄호 안에 t-값을 표기하였다. 또한, 연구개념 안에 경로분석 결과에 의한 내생변수(endogenous)들의 설명된 분산(variance explained (R^2))을 표기함으로써 연구 개념의 설명력을 나타내었다. 경로계수 아래 표시된 t-값은 부트스트랩[3](bootstrapping)을 통한 반복추출 서브샘플링 생성을 통해 계산된 값으로 서브샘플링의 수는 500회로 분석하였다.

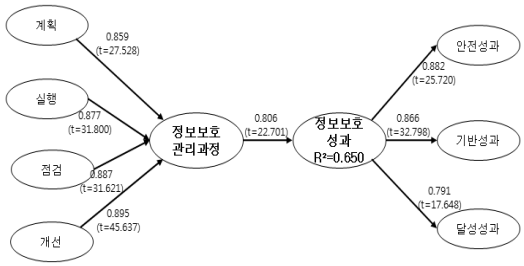
또한, 연구모형의 개별 경로를 살펴보면 조직 내 정보보호 관리과정은 정보보호 성과에 긍정적인 영향(t=22.701, p〈0.01)을 미치는 것으로 나타나 ISMS 관리과정과 정보보호 성과 사이의 인과관계는 성립하는 것으로 나타났다. 이로써 본 연구를 위해 설정한 연구가설은 유의수준(p) 〈0.01에서 채택되는 것으로 나타났다.

〔표 6〕 연구가설 검정결과

가설경로(인과관계)			경로계수	가설 방향	t-값	R^2	검정 결과
From	→	To					
정보보호 관리과정	→	정보보호 성과	0.806**	+	22.701	0.650	채택

※ 주) **: 유의수준 p〈0.01 *: 유의수준 p〈0.05

3) 부트스트랩(bootstrapping) : 데이터에서 얻어진 통계량의 표본오차를 확률 분포의 가정을 두지 않고 논 파라메트릭(non-para-metric)하게 평가하기 위한 하나의 방법



〔그림 3〕 2차 요인의 구조모형 분석결과

※ 주) 괄호 위 경로계수, 괄호 안 t-값
**: 유의수준 p〈0.01, *: 유의수준 p〈0.05

이로써 본 연구를 위해 설정한 연구가설은 유의수준(p〈0.01)에서 채택되는 것으로 나타났으며, 다음의 〔표 6〕과 같이 연구가설의 검정결과를 요약할 수 있다.

V. 결론

5.1 연구결과의 요약

본 연구에서는 설정된 변수들이 정보보호 관리과정을 기반으로 하여 정보보호 성과에 미치는 영향정도를 상관분석을 실시하였다. 독립변수로는 계획단계, 실행단계, 점검단계, 개선단계 등이고, 종속변수로는 안전성과, 기반성과, 경영성과로 설정한 결과 모든 변수쌍에서 모두 통계적으로 유의한 상관관계를 확보하고 있는 것으로 판명되었다.

이러한, 검증결과를 유추해 볼 때 Security PDCA 모형을 이용한 정보보호 성과의 영향요인을 통하여 도출된 4개 요인과 정보보호 성과와의 선형회귀분석(Linear Regression) 기법을 이용하여 분석한 결과 유의수준 5%를 기준으로 할 때 계획단계, 실행단계, 점검단계 등이 상관관계를 가지고 있으며, 정보보호 성과에 유의한 영향을 미치는 요소인 것으로 판별되었다.

연구 결과 1차 요인의 구조모형 분석결과 총 12개 중 채택 3개, 기각 9개로 나타났으며, 2차 요인의 구조모형 분석결과 정보보호 관리과정이 정보보호 성과에 영향을 미치고 있음을 확인하였다. 정보보호 관리체계 관리과정이 대부분 정보보호 성과에 영향을 미치나 계획단계, 실행단계, 점검단계가 직접적인 영향을 미치는 것으로 나타났다.

5.2 연구의 의의 및 시사점

이러한 정보보호 관리체계의 관리과정이 정보보호 성과에 미치는 영향에 관한 실증연구의 의의 및 시사점은 다음과 같다.

첫째, 기존에는 정부나 조직에서 일방적으로 정보보호 관리체계를 도입·운영해 왔으나 정보보호 성과에 미치는 영향에 관한 연구 자료가 여전히 부재하였다. 본 연구에서는 조직에서 운영하는 S-PDCA 모형이 정보보호 성과를 향상시키기 위한 방향을 제시하였고, 단순한 통제항목 중심의 정보보호 활동보다는 관리과정을 통해 조직 환경에 적합한 관리체계를 수립 운용함으로써 정보보호 활동을 통해 정보보호 성과를 향상시킬 수 있는 모형을 정립하였다.

둘째, 조직 내의 막연한 정보보호관리 활동에 대한 방향과 현재의 정보보호 위치, 수준을 측정하기 위한 기준을 제시하였고 효과적인 정보보호 투자와 비즈니스와 연계한 조직의 경영활동의 일환으로 정보보호활동이 존재한 다는 것을 입증하였다.

셋째, 기존 연구를 통해 도출된 정보보호 관리체계 관리과정과 정보보호 성과 측정 항목의 타당성, 신뢰성, 유효성 측면에서 실제 조직에서 정보보호 관리체계를 구축 운용하는 정보보호 전문가를 대상으로 설문을 수집하였으며, 통계분석을 실시하여 보다 현실적이고 실증적인 결과를 도출하였다.

넷째, 본 연구의 모형 및 측정 항목 내용은 전사적인 측면에서 정보보호관련 선행연구 및 문헌에서 제시하는 주요 항목을 대부분 반영하였기에 정보화 발전과 비즈니스 환경변화에 능동적으로 대응할 수 있으며, 어떠한 조직에서나 적용이 가능하고, 또한 정보보호 업무를 수행하는데 한층 더 실효성이 증진될 수 있게 하였다.

다섯째, 본 연구 결과를 적용하면, 정부는 정보보호 관리체계 도입에 대한 타당성을 검증할 수 있으며, 적극적인 제도 활성화 기반을 마련할 수 있다. 또한, 민간조직에서는 본 연구의 결과를 활용해 적극적인 정보보호 관리체계 도입의 계기를 마련할 수 있으며, 이를 통해 기 운영 중인 정보보호 관리체계의 개선방향을 제시함으로써 정부뿐만 아니라 민간조직의 정보보호 수준제고에 크게 기여 할 것으로 사료된다.

여섯째, 최근 정부는 정보보호 관리체계에 대한 검증되지 않은 다양한 프레임워크를 개발하여 제도화 추진을 검토하고 있는데 본 연구를 통해 이러한 과정에서 발생할 수 있는 시행착오를 최소화하고 무분별한 모델 개발보다는 기존모델 검토를 통해 논리성, 타당성, 적합성 등의 심도 있게 검토하여 정보보호 관리체계를 선도할 수 있도록 조직에 적합한 모형을 개발하여 활용될 수 있게 하였다.

VI. 참고문헌

〔1〕 김경규, "정보자산보호 성과가 정보보호 성과에 미치는 영향에 관한 연구," 정보관리연구, 제40권, 3호, pp. 61-77, 2009.

〔2〕 김태성, "기업의 정보보호 수준평가 방법론 개발," 2009.

〔3〕 서한준, "비즈니스-IT의 전략적 연계에 따른 IT투자와 IT 거버넌스 성숙도가 IT성과에 미치는 영향." 서울과학종합대학원 박사학위논문, 2009.

〔4〕 선한길, "국내 기업의 정보보호 정책 및 조직 요인이 정보보호 성과에 미치는 영향," 한국경영학정보학회 춘계학술대회, pp. 1087-1095, 2005.

〔5〕 이학식, 임지훈, 『SPSS 12.0 통계분석방법 및 해설』, 법문사, 2010.

〔6〕 한국인터넷진흥원(KISA), "07년 국가정보보호 수준 평가지수 산출과 시사점," 정보보호 이슈리포트, 2008.

〔7〕 한국인터넷진흥원(KISA), "정보보호 관리체계 수준평가 방법론 및 등급기준 연구," 2010.

〔8〕 홍기향, "정보보호 통제와 활동이 정보보호 성과에 미치는 영향에 관한 연구," 국민대학교대학원 박사학위논문, 2003.

〔9〕 ISM3 v2.3, Information Security Management Maturity Model, 2009.

〔10〕 ISO27004,Information technology-Security techniques-Informationsecurity management-Measurement, 2010.

〔11〕 Janne Merete Hagen, Eirik Albrechtsen, Jan Hovden, Implementation and effectiveness of organizational information security measures, Inf. Manag. Comput. Security 16(4), pp. 377-397, 2008.

〔12〕 JIPDEC, ISMS 적합성 제도 도입에 관한 실태조사, 2002, 2009.

〔13〕 Marianthi Theoharidou and Spyros Kokolakis, The insider threat to information systems and the effectiveness of ISO-

17799, Information Security governance, 2005.
〔14〕 Moulton, R.T. and Moulton, M.E, Electronic Communications Risk Management : A Checklist for Business Managers, Computers & Security, Vol. 15, 1996.
〔15〕 NIST Special Publication 800-39, Managing Risk from Information Systems An Organizational Perspective, 2007.
〔16〕 NIST Special Publication 800-55 Revision 1, Performance Measurement Guide for Information Security(DRAFT), 2007.
〔17〕 Shuchih Ernest Chang, Chienta Bruce Ho, Organizational factors to the effectiveness of implementing information security management, Information Security Governance, 2006.
〔18〕 The Complete Public Domain BCMM, Virtual Corporation, 20052010.

〈著者紹介〉

장 상 수 (Sang-Soo Jang) 정회원
1989년 2월: 한국항공대학교 항공정보통신공학과 졸업(학사)
2000년 2월: 동국대 대학원 정보보호학과 졸업(석사)
2011년 8월: 전남대학교 대학원 정보보호학과 졸업(박사)
2001년~현재: KISA 보안관리 팀장
〈관심분야〉 ISMS, IT위험관리, 정보보호 거버넌스, 시스템 및 네트워크 보안

이 상 준 (Sang-Joon Lee) 정회원
1991년: 전남대학교 전산통계학과(이학사)
1993년: 전남대학교 전산통계학과(이학석사)
1999년: 전남대학교 전산통계학과(이학박사)
1995~2005년: 서남대학교 경영전산정보학과 조교수
2005~2007년: 신경대학교 인터넷정보통신학과 조교수
2007~현재: 전남대학교 경영학과 부교수
〈관심분야〉 경영정보시스템, 스마트컴퓨팅, 소프트웨어공학

노 봉 남 (Bong-Nam Noh) 정회원
1978년 2월: 전남대학교 수학교육과 졸업(학사)
1982년 2월: KAIST 대학원 전산학과 졸업(석사)
1994년 2월: 전북대학교 대학원 전산과 졸업(박사)
1983년~현재 : 전남대학교 전자컴퓨터정보통신공학부 교수
2000년~시스템 보안 연구센터 소장
〈관심분야〉 컴퓨터와 네트워크 보안, 정보보호시스템, 전자상거래 보안, 사이버사회와 윤리