情報保護學會論文誌
第20卷 第6號, 2010. 12

정보보호 안전진단 성과관리 측정 모델 및 성과 분석 방안 연구

장 상 수[1†], 신 승 호[2‡] 노 봉 남[3]
[1]한국인터넷진흥원, [2]단국대학교, [3]전남대학교 시스템보안연구센터

A study of the ISCS(Information Security Check Service) on performance measurement model and analysis method.

Sang-Soo Jang,[1†], Seung-ho Shin[2‡] Bong-Nam Noh[3]
[1]Korea Internet&Security Agency, [2]Dankook University, [3]Chonnam University System Security Research Center

요 약

정보보호 안전진단 제도를 적용받는 정보통신서비스 기업의 지속적인 정보보호 수준을 제고하고, 정보보호 안전진단 성과측정 방법을 개발하여 안전진단대상 기관들이 스스로 수준측정을 하여 지속적인 정보보호 개선활동을 하도록 측정 지표 및 방법론을 제시하였다. 본 논문에서는 안전진단 수검 전후와 수검후의 지속적인 기업이 정보보호에 대한 투자와 노력에 대한 성과를 측정하여 기업 자체적으로 측정가능하게 하여 정보보호관리체계를 지속적이고 종합적으로 유지하고 관리하도록 하였다. 또한 정부에서도 제도 전반적인 이행의 근거와 타당성을 확보하여 안전진단 자체가 정보보호 수준을 한단계 높이는 실질적인 안전진단이 이루어 지도록하여 보안 사고를 사전에 예방하고 기업성과를 향상시키는데 도움을 주고자 한다.

ABSTRACT

This report has continuously improved in Information Security Level of Information Communication Service Companies which are applicable to Information Security Safety Inspection System. Also, it presents a decided methodology after verified propriety and considered the pre-research or expropriation by being developed the way of Information Security Safety Result Measurement. Management territory weighted value was established and it was given according to the point of view and the strategy target and the and outcome index to consider overall to a measurement item. Accordingly, an outome to the Information Security Check Service is analyzed by this paper and measurement model and oucome analysis methodology are shown with this, and gives help to analyze an outcome. Also it make sure the the substantial information security check service will be accomplished, prevent a maintenance accident beforehand and improve an enterprise outcome independently by institutional system performance securement and enterprise.g corporate performance.

Keywords: ISCS(Information Security Check Service), Measurement Model, Performance Analysis, Methodology.

I. 서 론

IT발전에 따라 유비쿼터스 사회 실현하려는데 대한 최대 장애인 정보화 역기능 사례의 증가에 따라 이를 예방과 구제하기 위한 대책과 대응 요구도 증가하고 있다. 정보화 역기능으로는 인터넷침해사고, 불법 스팸, 개인정보 침해 등이며, 이런 정보화 역기능으로 인해 인터넷 이용환경의 안전성이 침해되고 인터넷 경제

접수일(2010년 9월 24일), 게재확정일(2010년 11월 23일)
† 주저자, ssjang@kisa.or.kr
‡ 교신저자, kpdca@paran.com

의 신뢰성을 훼손하게 되며, 국가와 개인의 정보보호 수준이 하락하게 한다.

이러한 정보화 역기능 방지 활동들을 위해서는 선제적 예방 활동이 중요하며 이를 위해 정부는 2003.1.25 인터넷 침해사고 이후 기업들에게 최소한의 정보보호 조치를 할 수 있도록 매년 정보보호 안전진단을 받도록 하였다. 그러나 수년간 안전진단 제도 운영을 통해 제도운영 활동의 효율성과 정보보호에 미친 효과성에 대한 분석과 환류가 이루어지지 않았다. 그 결과 정보보호안전진단 대상기관들의 협력과 개선활동이 제대로 이루어지지 않고 대내외 적으로 제도 실효성에 대한 논란이 일고 있는 것이 사실이다.

이에 본 연구에서는 정보보호의 안전진단제도 운영 성과를 측정할 수 있는 측정지표를 개발하고, 개발된 측정지표를 이용하여 정보보호 안전진단 성과를 분석하고 개선방안을 제시하고자 한다.

II. 문헌연구

2.1 정보보호 안전진단 제도

정보보호 안전진단 제도는 '정보통신망이용촉진및정보보호등에관한법률(이하 "정보통신망법" 이라 한다)'에 인터넷을 기반으로 한 정보통신서비스의 정보보호 수준을 강화하여 안전한 이용 기반을 조성하고자 정보통신서비스제공자에 대한 주기적인 정보보호 현황 점검 및 자체적인 개선 노력을 통해 정보통신 서비스의 품질 향상을 도모하는 제도이다.

정보보호 안전진단 제도의 목적은 인터넷 이용자들에게 인터넷의 안전성·신뢰성을 유지하기 위한 최소한의 기본적인 안전조치 기준을 제시하고 이의 이행을 의무화하는 제도로서 인터넷망의 안전성을 확보하는데 있다.

정보보호 안전진단 대상자는 정보통신설비 및 시설을 활용하여 서비스를 제공하는 주체로서 주요정보통신서비스제공자(정보통신망법 제46조의3제1항제1호), 집적정보통신시설사업자(정보통신망법 제46조의3제1항제2호), 정보통신서비스제공자(정보통신망법시행규칙 제5조의4) 등이다. 정보보호 안전진단 대상자는 『정보보호 안전진단 대상 정보통신 설비 및 시설선정 지침』을 준수할 의무가 있다. 이 지침은 정보보호 안전진단 대상의 정보통신 설비 및 시설선정 지침은 크게 정보보호 안전진단 대상설비 및 시설개념과 선정방법 및 목록의 관리와 운영방법을 구체적으로 제시하고 있다.

정보보호 안전진단 수행체계는 안전진단을 위하여 준비단계=>안전진단 수행단계=>개선권고 조치단계=>개선명령 조치단계로 진행하여야 한다. 안전진단 대상자는 준비단계에서 진단계획을 수립과 정보보호 지침이행 계획을 수립을 해야 한다. 진단업무 전문업체는 안전진단 수행단계에서 방침, 실행, 실무지침 등에서 요구하는 증빙자료를 통한 서면검사와 현장검사를 한다. 안전진단대상자는 개선권 조치단계에서 안전진단결과를 접수하여 개선권고사항과 개선선고안을 이행해야 한다. 방송통신위원회는 개선명령 조치단계에서 개선명령 접수와 이행 및 결과통보, 이행결과 접수 등을 수행한다.

〔표 1〕 국가정보보호 평가항목

영역	관점	지표
정보보호 인프라	기술 인프라	신정보보호기술 보급속도, 정보보호기술 관련 R&D 수준, 정보보호기술 표준화 건수, 정보보안 웹서버 수, 침입차단시스템 보급, PKI(공개키기반구조)시스템, VPN(가상사설망) 시스템, 침입차단시스템 보급
	인력 인프라	IT관련 보안인력의 확보율, 정보보호 기술인력의 가용성
정보보호 활용	정보보호 제품	백신프로그램, 통합보안관리 솔루션, 취약점 점검도구, 보안사고 발생건수, 해킹건수
	정보보호 산업	정보보호산업체수, 정보보호산업체 인력현황, 정보보호 산업성장율, 정보보호 관련연구기관수, 정보보호 관련 학과수, 인터넷 접속방식, 정보보호소프트웨어 매출액, 보안서비스비율(서버/네트워크서비스), 정보보호 시장규모, 정보보호시스템 매출액
정보보호 투자	기업투자 규모	GDP대비 정보보호투자비율, 정보보호투자증가율, 정보보호시스템투자비율
	개인투자 규모	정보보호1인당투자비용(전체보안대비액)
정보보호 정책/ 마인드	정보보호 정책	정보보호마스터플랜 수립여부, 정보보호정책 수립현황, 정보보호정책 및 법제도, 정보보호 특허수, 정보보호 연구개발비 투자액
	정보보호 마인드	정보보호 마인드확산 활동, 정보보호 자격증 소지 현황, 정보보호 교육일수

〔표 2〕 중소기업의 정보화수준평가 항목 및 배점

평가영역	평가지표 및 항목
정보화 전략수립(15점)	최고경영자/임직원의 정보화 마인드(10점), 정보화 비전(3), 정보화 투자타당성 분석(2점)
정보화 추진환경(15점)	정보화 추진 · 인력 구성(3점), 정보화투자 수준(3점), 정보화 교육 수준(3점), 업무 관리체계 정비수준(3점)
정보화 구축현황(35점)	H/W 보급 및 유지(6점), 네트워크 구축 및 운영(6점), S/W 관리수준(4점), 정보시스템 구축 및 운영(14점), 정보보호(5)
정보화 활용수준(20점)	정보시스템의 업무활용수준(10점), IT기능의 활용수준(10점)
정보화 효과수준(15점)	개인/기업업무 효과(9점), IT도입 효과(6점)

2.2 정보보호 안전진단 성과분석의 선행연구

현재 정보보호 안전진단에 대한 성과 측정에 대한 연구는 정책적인 제도이다 보니 일반인이 접근하기가 쉽지 않고 관련 데이터 확보가 어려워 상당히 미흡한 실정이다. 그러나 정보보호 안전진단에 대한 성과 분석에 앞서 선행되어야할 정보보호 관련 성과측정의 연구는 다양하게 진행 되어왔다 할 수 있으며, 그 내용은 다음과 같다.

KISA(2002)에서는 국가 정보보호 평가항목에서는 일반적으로 정보보호 수준을 평가하기 위해서는 국가 전체적인 산업의 정보보호 수준을 반영할 수 있도록 정보보안과 관련된 산업 및 기업 그리고 최종적으로 국가의 상황을 반영할 수 있는 다양성을 포함하여야 한다고 하였으며, 또한 정보보호 수준을 객관적이고 정확히 반영하고 측정할 수 있어야 하고, 통계청 및 OECD등에서 실시하는 정확한 근거를 바탕으로 측정이 가능해야하며, 지표 측정이 현실적으로 가능하고 국가간의 비교가 가능한 항목들이 반영되야 한다고 하였다.

〔표 3〕 정보보호 투자효과 측정 분류

유형	주요내용
정보보호 투자비용	가시적비용 + 비가시적 비용 H/W구입비 + 기술지원/유지지원비용 + 지원인력비용
정보보호 투자성과	정보보호사고 감소, 자산손실건수 감소, 비즈니스 기회 손실 감소, 타사 경쟁시 손해감소, 이미지 실추 건수감소, 사고발생시 처리시간 단축, 침해사고로 주식가치 감소
정보보호 연관효과	생산유발효과, 부가가치 유발효과, 수출유발효과, 고용창출 효과, 기업가치 시장 효과

국가정보보호수준을 평가하는 항목으로는 정보보호 인프라, 정보보호 활용, 정보보호 투자 및 정보보호정책/마인드 등을 영역으로 세부적으로 관점과 지표들이 적용되었다.

중소기업청(2008)은 중소기업을 대상으로 매년 실시되는 중소기업의 정보화수준평가 항목중에서 정보보안 영역에 대한 수준파악을 위한 지표는 정보화 전략수립, 추진환경, 구축현황, 활용수준 및 효과수준 등을 반영하여 각각 가중치를 부여 하였으며, 주요내용은 다음과 같다.

김정덕(2003), 선한길(2005)는 정보보호투자 성과를 정보보호관련 사고감소, 자산 손실건수 감소, 비즈니스 기회손실 감소, 타사 경쟁시 손해감소, 이미지 실추감소, 사고발생시 처리시간 등으로 나타난 비용을 TCO (Totol Cost Ownership)로 산정하는 효과분석의 방향성을 제시하였다. 특히, 정보보호에 대한 투자비용, 투자성과 및 연관효과를 고려한 분석항목을 상세하게 분류하였다.

KISA(2006)은 국가정보보호 수준평가 연구에서 지수산출을 위해 지표체계를 정보보호기반(T), 정보보호환경(E), 정보화역기능(N) 등 3개로 분류하여

〔표 4〕 국가정보보호 평가지수(2006년)

구분	분류	세부지표	지표산식
정보보호 수준	정보보호 기반	백신 보급율	(백신 S/W 이용자수/인터넷 이용자수)X100
		패치 보급율	(패치 설치수/인터넷 이용자수)X100
		PKI 보급율	(공인인증서 이용자수/인터넷 이용자수)X100
		방화벽 보급율	(Firewall 사용 기업체수/기업체수)X100
		IDS 보급율	(IDS를 사용하는 기업체수/기업체수)X100
		보안서버 보급율	(국내 보안서버 판매대수/인구수)X10만
	정보보호 환경	정보보호 예산	(정보보호 국가예산/정보화 국가예산)X100
		정보보호 인력비율	(정보보호 전문인력/정보화 전문인력)X100
		보안의식 수준비율	(필요/매우필요 응답자/전체 조사 대상자)X100
정보화 역기능 수준	정보화 역기능	해킹 바이러스 신고율	(해킹바이러스신고건수/전체 PC보급대수)X100
		개인 정보침해 신고율	(개인정보침해 신고건수/인터넷 사용자)X100
		스팸메일 수신비율	(수신스팸메일수/수신전체메일수) X100

〔표 5〕 정보보호 안전진단 관점별 전략목표

관점	전략목표	측정지표
성과관점	정보보호 매출증대	정보보호매출액(S/W, H/W),정보통신서비스 연간매출액
	정보보호 비용절감	시스템(S/W, H/W 복구비용, 기술지원/유지지원 비용, 책임보상금 또는 인원수, 데이터복구비용
	정보보호 안전진단 성과분석 강화	정보보호산업성장율, 고용창출효과, 부가가치유발효과, 수출유발 효과
	침해사고 처리시간 단축	서비스제공자 피해시간, 이용자 피해시간
프로세스관점	정보보호 전략계획 수립	당해년도 정보보호 실행계획 수립, 정보보호방침수립실적, 정보보호마스터플랜 수립실적, 침해사고대응계획의 수립
	정보보호 조직/정책 정립	정보보호조직(책임)구성율, 정보보호규정 준수율, 정보보호실무지침 보유실적
	정보보호 안전진단 확대	정보보호안전진단 대상실적, 정보보호안전진단 이행조치율, 안전진단설비/시설점검율, 안전진단대상자 침해사고율
정책관점	정보보호 솔루션 구축강화	정보보호시스템 보급률, 취약점 점검도구 보급실적, 통합보안관리 솔루션 보급실적, 인증시스템 이용율
	정보보호 관리체계활동 강화	설비와 시설목록 보유율, 백업시설과 설비구축, 보안관리서비스 비율(서버/네트워크), 유지보수 구성관리
	정보보호 기술체계활동 강화	안전진단 취약점 진단(장비)실적,보안설정(패치)적용율, 책임자 정기점검율
	침해사고 방지활동 강화	정보보호사고 발생실적, 개인정보 침해사고 신고 실적, 보안사고대응 조치실적, 해킹사고/바이러스 신고실적
학습성장관점	정보보호 역량강화	정보보호 전문기술인력수, IT관련 보안인력 확보율, 정보보호자격증 보유실적, 정보보호기술 표준화 건수
	정보보호 전문인재 강화	정보보호기본인식 교육, 정보보호전문교육시간
	정보보호 투자활동 증진	GDP대비 정보보호투자비율, 정보보호시스템 투자비율 정보보호 예산확보실적

정보보호기반지수는 시스템과 데이터보호를 측정하고, 정보보호 환경지수는 전문인력비율, 정보보호예산비율을 측정하고, 정보화 역기능 지수는 해킹, 바이러스, 개인정보침해비율 등을 측정하는 지표로 적용하였다.

또한, 정보보호안전진단기준 항목은(방통위 고시) 관리적·기술적·물리적 보호조치로 구성되어 있으며, 총 48개의 세부조치사항의 항목을 점검하도록 규정하였고 ISP, IDC, 쇼핑몰 등의 대상 업체별 서비스 환경을 고려하여 점검내용을 차별화하였다. 정보보호안전진단은 관리적 보호조치, 기술적 보호조치, 물리적 보호조치 영역별로 진단항목은 다음과 같다.

김태성(2006)은 기업의 정보보호 수준을 평가하기 위하여 BSC(Balanced Scorecard) 모형을 적용하여 기업의 정보보호 수준평가 모형을 개발하였다. 연구를 통해 정보보호 수준을 4가지 관점(성장학습, 내부프로세스, 사용자, 경영성과), 55개의 세부지표를 제시하였으며, 주요지표를 도출하기 위하여 ISO27001, 국정원 보안점검 항목 등을 반영하였다.

2.3 정보보호 안전진단 성과측정의 시사점

국내의 정보보호 수준평가 및 효과를 분석하는 연구사례는 정보기술 성과평가, 중소기업의 정보화수준평가 정보보호영역, 인터넷침해사고 피해액 산출 연구, 정보보호의 투자효과 측정, 국가정보보호수준 평가지수, 정보보호수준 평가지수, 정보보호 안전진단 등 관리하는 항목을 정리하였다. 하지만 실질적으로 연구의 방향에 대하여는 연구가 이루어졌지만 실질적인 효과를 분석하는 사례는 거의 없는 실정이다.

이에 정보보호안전진단의 정책적인 방향성을 제시하는 측면과 세부적인 실행과 이행조치 항목들까지 반영되어 있어 1차적으로 관리항목의 유사성을 고려하여 분류하였다. 그리고 분류되는 항목들을 정보보호 측면의 성과관리(BSC 모델)을 근거한 성과를 분석하는 절차에 의하여 정보보호안전진단의 주요항목을 고려하여 방향성을 설정하였다.

또한 다양한 연구사례를 통하여 정보보호 안전진단

〔표 6〕 정보보호 안전진단 성과측정 목표와 지표

전략목표	성과목표	성과지표	기존연구문헌
정보보호수준 제고	경제적 효과 달성	정보보호 매출액	안전진단, 정보보호수준평가, 중소기업정보화, 정보보호투자효과
		피해감소 실적	안전진단, 정보보호수준평가
	정보보호 능력 제고	침해사고 발생비율	안전진단, 중소기업정보화, 정보보호투자성과
		정보보호관리체계인증 실적	안전진단, 중소기업정보화
침해사고 방지 효과 제고	침해처리 시간단축	서비스업체(이용자) 피해시간	안전진단, 정보보호투자효과, 정보보호수준평가
		공급업체(제공자) 피해시간	안전진단, 정보보호수준평가
	침해사고방지활동 강화	해킹 사고/바이러스 신고실적	안전진단, 중소기업정보화, 정보보호투자성과
정보보호 관리 체계활동 강화	정보보호안전진단 확대	정보자산의 안정적 관리실적	안전진단, 정보보호투자효과
		안전진단 취약점 진단(장비)실적	안전진단, 정보보호수준평가
정보보호 기술 체계활동 강화	개인정보암호보안기술 역량 강화	암호화 통신율	정보보호수준평가, 국가정보보호지수
		암호화 저장율	정보보호수준평가, 국가정보보호지수
	침해사고조치 능력 제고	악성코드 일일점검 실적	안전진단, 정보보호수준평가
		보안설정(패치) 적용율	안전진단, 국가정보보호지수
이용자보호수준 제고	개인정보피해방지 체계 정비	주민등록번호 수집율	정보보호수준평가, 국가정보보호지수
		주민등록번호 대체수단 이용실적	정보보호수준평가, 국가정보보호지수
	개인정보인증체계 강화	공인인증서 사용율	정보보호수준평가, 국가정보보호지수
정보보호 정책 체계 강화	정보보호전략계획수립	정보보호방침 수립실적	안전진단, 정보보호수준평가
		정보보호마스터플랜 수립실적	안전진단, 정보보호수준평가
	정보보호 조직정책 정립	정보보호조직(책임)구성율	안전진단, 정보보호수준평가
정보보호시스템 구축 확대	정보보호 하드웨어구축 강화	보안서버 보급율	안전진단, 국가정보보호지수, 정보보호수준평가
	정보보호 소프트웨어 구축 강화	통합보안관리 솔루션 보급실적	안전진단, 국가정보보호지수, 정보보호수준평가
정보보안 역량 강화	정보보호 인적역량강화	정보보호전문교육시간	안전진단, 중소기업정보화, 정보보호수준평가
		IT관련 보안인력의 확보율	안전진단, 국가정보보호지수, 중소기업정보화, 정보보호수준평가
	정보보호 투자효과 증대	정부정보보호 예산집행액	안전진단, 국가정보보호지수, 중소기업정보화, 정보보호수준평가

을 위한 성과지표를 개발하기 위하여 적용할 관점과 전략목표를 설정하였다. 관점은 정보보호성과관점, 정보보호정책관점, 프로세스관점, 학습성장 관점 등이고 관점당 전략목표는 3-4개씩 구성하고, 전략목표당 성과지표도 2-3개 정도씩 반영하였다.

관점내역으로는 정보보호 안전진단 성과측면에서는 매출증대, 비용절감, 성과분석 강화, 침해사고 처리시간 단축 등이고, 정보보호정책 측면에서는 솔루션 구축강

화, 관리체계와 기술체계활동 강화와 침해사고방지 활동 등이며, 프로세스 관점에서는 정보보호 전략계획수립과 조직과 정책의 정립, 안전진단 확대 등과 학습성장 관점에서는 안전진단의 역량강화, 전문인재 강화 및 투자활동의 증진사항이 전략목표의 안으로 설정하였다.

국내의 정보보호 관련하여 안전진단, 정보보호수준평가, 중소기업정보화, 정보보호투자효과 및 정보보호 성과분석 등 측정 및 평가 항목에 대한 성과지표의 공통적인 항목을 중심으로 분석하였다. 또한 정보보호 안전진단 성과측정의 항목을 도출하기 위하여 기존연구 문헌을 토대로 정보보호 안전진단 성과지표와 관련되는 사항으로 분석하였다.

III. 정보보호 안전진단 성과분석 모델

3.1 성과관리 방법론

〔그림 1〕에서 보는 바와 같이 성과관리는 투입->처리->산출->결과->효과의 과정에서 투입물과 처리활동 및 성과로서의 산출, 결과, 효과를 관리하는 것이다. 투입은 처리단계의 활동을 위해 인력, 재원 등의 생산요소를 공급하는 것을 의미하고, 처리는 업무처리나 집행활동이며, 산출은 단기성과로서 재화나 서비스 등을 의미하며, 결과는 산출이 사회와 고객에게 미치는 중기성과를 말하며, 효과는 결과들이 쌓여서 나타나는 장기성과를 말한다.

결과중심의 성과개념은 활동량이나 산출물에 기초하는 효율성 개념보다는 궁극적인 영향을 반영하는 효과성 개념을 강조하고 있다. 효율성은 능률성과 효과성을 말하며, 능률성은 투입 대비 산출간의 비율로서 활동성을 나타내며, 효과성은 단기성과로서 산출과 중기성과로서 결과 및 장기성과로서 효과가 실현되는 정도를 의미한다. 그러나 효율성은 회적인 문제를 얼마나 해소하였는가를 제시하는 데는 한계가 있다.

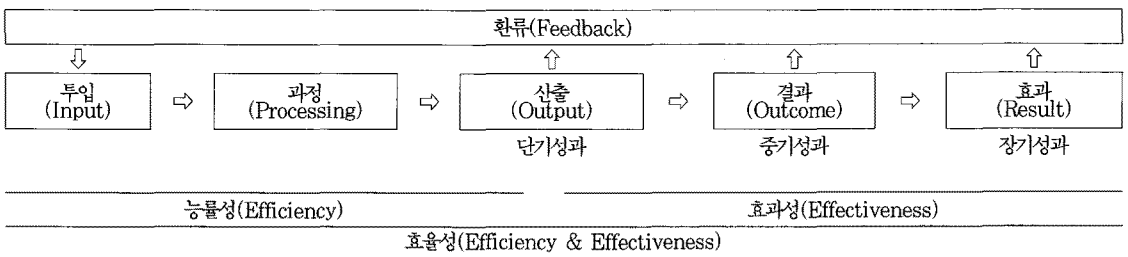
〔표 7〕 민간부문과 공공부문 BSC 관점과 측정지표 비교

구분	민간부문		공공부문			
	관심사	Kaplan와 Norton, 1992	관심사	Olve외, 1999	미국 OMB	김정덕, 1998
투입	산출 대비 투입 최소화	재무 (finance)	산출 대비 투입 최적화	성과 (performance)	투입지표 예산집행율	원인 지표
처리	재무적 성과 달성	절차 (process)	예산범위 최적집행	활동 (activity)	과정지표 활동공정율	실행 지표
산출	재무적 성과 창출	고객 (customer)	공공적 사명달성	관계 (relationship)	산출지표 생산제공량	성과 지표
환류	주주 가치 극대화	학습/성장 (learn/growth)	공익적 사명달성	학습/성장 (future)	결과지표 영향만족도	정책 지표

3.2 성과분석을 위한 균형성과표(BSC) 모델

경영활동의 성과분석을 위한 성과지표는 균형을 이루어야 한다. 균형잡힌 성과관리를 위해 Kaplan과 Norton(1992)가 개발한 성과평가모형로서의 균형성과표(BSC: Balanced ScoreCard)모델이 경영평가와 정부활동평가에 이용되고 있다. 균형성과표모델은 가치와 비전에 미션을 수행할 전략을 기반으로 재무(Finance)관점, 고객(Customer)관점, 절차(Process)관점, 학습(Learning)과 성장(Growth)관점으로 조직전체로부터 하위조직과 개인들까지 단계적으로 목표를 재분배(Cascading)하는 성과관리표(Scorecard)를 총체적으로 관리하는 가치중심의 성과분석기법이다(Niven, 2002).

정부업무의 성과관리는 "국정추진에 있어 기관의 임무, 중장기 목표, 연도별 목표 및 성과지표를 수립하



〔그림 1〕 성과의 개념

〔표 8〕 한국의 정보보호 안전진단 성과분석

구분	항목	단위	2007년	2008년	비 고
투입	국가정보보호 예산실적	%	4.7	5.5	0.17% 증가
처리	보안관제센터 설치실적	기관	10	10	-
	유통정보서버 암호실적	대수	20000	30000	0.50% 증대
	정보보호시스템 도입율	%	63.6	71.0	0.12% 증가
산출	정보보호제품 매출실적	억원	7,149	7,724	0.08% 증가
	정보보호제품 수출실적	억원	424	555	0.31% 증가
	주민번호의 수집감소율	%	65.6	46.1	0.30% 감소
결과	국가 정보보호지수	점수	63.4	68.4	5점 증가
영향	WEF 국제정보보호등수	순위	51	16	32개국 하락

고 그 집행과정 및 결과를 경제성, 능률성, 효과성 등의 관점에서 관리하는 일련의 활동으로서 조직의 목표설정, 지표개발, 성과측정(평가), 결과의 환류 등을 포함한다"(정부업무평가기본법, 2006).

〔표 7〕에서 보는 바와 같이 성과관리의 주요관심사가 민간부문과 공공부문에서 차이가 있다. 즉, 목표에서 민간부문은 주주 가치극대화에 중점을 두되 공공부문은 공익적 사명달성에 중점을 두며, 재무부문에서 민간부문은 재무적 성과달성에 초점을 두되 공공부문은 예산한도에서 최적집행에 초점을 두며, 고객측면에서 민간부문은 재무적 성과창출 대상으로 보되 공공부문은 공공사명 달성 대상으로 보고, 절차측면에서 민간부문은 수익성에 초점을 두되 공공부문은 공공가치의 균형달성에 초점을 둔다. 이에 Kaplan과 Norton의 민간형 균형성과표모델은 Olve 등(1999)에 의해 공공형의 수정모델이 제시되었다. 수정모델은 재무는 성과로, 고객은 관계로, 처리는 활동으로 수정하고, 학습과 성장은 그대로 수용하였다. 미국 OMB의 성과지표를 투입지표, 과정지표, 산출지표, 결과지표 등으로 분류한다.

한국정부는 정보보호의 성과관리 측정지표는 정보보호수준의 종합적이고 체계적으로 측정하기 위해 측정지표 체계를 개발하여 사용하고 있다. 정보보호 안전진단 성과지표는 국가간 정보보호 수준을 평가하기 위한 지표로 활용할 수 있도록 정책지표, 원인지표, 실행지표, 성과지표로 구분하여 세부적인 지표항목을 도출하였고, 성과지표는 투입단계에 정보보호 위협보호를 위한 자원투입, 처리단계에 위협에 대한 대응활동, 산출단계에 정보자산 보호의 단기효과로서 정보보호 산출의 중기효과로서 결과 및 결과의 장기효과로서 영

〔표 9〕 기존연구와 방송통신위의 전략목표를 정의

관점	정보보호 전략목표	
	기존 연구자료	방송통신위 전략목표
성과관점	정보보호 매출증대	경제적 효과달성
	정보보호 비용절감	
	정보보호 성과분석강화	국가정보보호수준제고 이용자보호수준제고
	침해사고 처리시간 단축	
처리관점	정보보호 전략계획 수립	개인정보피해 체계정비
	정보보호 조직/정책 정립	개인정보보호 정책수립
	정보보호 안전진단 확대	정보보호 안전진단 확대
정책관점	정보보호 솔루션 구축강화	보안프로그램 이용강화
	정보보호 관리체계활동 강화	물리적 보안통제 강화
	정보보호 기술체계활동강화	개인정보암호보안기술 ID/PW관리강화지수
	침해사고 방지활동 강화	침해사고조치 능력 제고
학습성장 관점	정보보호 역량강화	정보보호 역량강화
	정보보호 전문인재 강화	개인정보보호 조직/교육정착
	정보보호 투자활동 증진	정보보호 기반조성

〔표 10〕 성과측정을 위한 성과지표 적정성 검토

순번	유형	전략목표	성과지표	측정요소(5/3/1)			총점	평균
				측정	구체	대표		
1	국가 정보보호수준제고	정보보호 안전진단 성과분석강화	고용창출 효과	3	5	5	13	4.3
2		정보보호 매출증대	정보보호 매출액 (S/W, H/W)	3	5	5	13	4.3
3		국가정보보호 수준제고	국가정보보호 지수	3	3	5	11	3.7
4		개인정보피해 체계정비	개인정보보호신뢰지수	3	3	5	11	3.7
5	이용자보호 수준 제고	ID/PW관리활동 강화	공인인증서 사용율	3	5	5	13	4.3
6		침해사고조치 능력 제고	악성코드 일일점검 실적	5	3	5	13	4.3
7		이용자보호 수준제고	휴대폰 스팸수신량 감소	3	3	5	11	3.7
8	정보보호 시스템 구축 확대	국가정보보호 수준제고	보안서버 보급율	3	5	5	13	4.3
9		정보보호솔루션 구축강화	통합보안관리 솔루션 보급실적	3	5	3	11	3.7
10	정보보호관리체계 활동 강화	정보보호 관리체계 활동강화	정보자산의 안정적관리실적 (설비와시설목록보유율)	5	3	5	13	4.3
11		물리적 보안통제 강화	물리적 접근통제율	5	5	3	13	4.3
12	정보보호기술체계 활동 강화	정보보호기술체계활동 강화	안전진단 취약점 진단(장비)실적	3	5	5	13	4.3
13		정보보호기술체계활동 강화	보안설정(패치) 적용율	3	5	3	11	3.7
14		개인정보암호보안기술	암호화 통신율	3	5	3	11	3.7
15		개인정보암호보안기술	암호화 저장율	3	5	3	11	3.7
16	개인정보 관리체계 강화	이용자보호 수준제고	주민등록번호 수집율	3	5	5	13	4.3
17		개인정보피해 체계정비	주민등록번호 대체수단 이용실적	3	5	5	13	4.3
18	침해사고 방지활동 증진	경제적 효과달성	피해감소 실적(국내피해/전세계)	3	5	5	13	4.3
19		침해처리 시간단축	서비스업체(이용자) 피해시간	3	3	5	11	3.7
20		침해처리 시간단축	공급업체(제공자) 피해시간	3	3	5	11	3.7
21		침해사고조치 능력제고	국가사이버공격 근원지 실적	3	3	5	11	3.7
22		침해사고방지활동 강화	해킹 사고/바이러스 신고실적	3	3	5	11	3.7
23		침해사고방지활동 강화	개인정보 침해사고 신고 실적	3	3	5	11	3.7
24		정보보호안전진단 확대	안전진단 대상자 침해사고 발생비율	3	3	5	11	3.7
25	정보보호 조직/지침 수립	정보보호전략계획수립	정보보호방침 수립실적	5	5	3	13	4.3
26		정보보호전략계획수립	정보보호마스터플랜 수립실적	5	5	3	13	4.3
27		정보보호 조직정책정립	정보보호실무지침 보유실적	3	5	5	13	4.3
28		정보보호 조직정책정립	정보보호조직(책임)구성율	3	5	5	13	4.3
29	정보보호 안전진단 확대	침해사고조치 능력제고	정보보호안전진단 수행실적	3	5	5	13	4.3
30		정보보호안전진단 확대	정보보호안전진단 대상실적	3	5	5	13	4.3
31		정보보호안전진단 확대	안전진단 설비/시설 점검율	3	5	3	11	3.7
32	보안전문 역량강화	정보보호 전문인재강화	정보보호전문교육시간	3	5	5	13	4.3
33		정보보호 역량강화	IT관련 보안인력의 확보율	3	5	5	13	4.3
34		정보보호 역량강화	정보보호전문자격증 보유실적	3	5	5	13	4.3
35	효율적인 정보보호투자	침해사고조치 능력제고	정부정보보호 예산집행액	3	3	5	11	3.7
36		정보보호투자활동 증진	GDP대비 정보보호투자비율	3	5	3	11	3.7
37		침해사고조치 능력제고	정보보호관리체계인증 실적	3	5	5	13	4.3

향이라는 측정지표를 사용하고 있다(김정덕, 1998).

정보보호에 대한 비용효익(ROSI : Return On Security Investment)을 분석하는 정보보호투자의 투입-처리-산출-결과-영향 분석을 통해 정보보호 투자의 정당화 수단으로 사용하고 있으며, 잠재적인 경제적 영향에 대한 분석 =〉 인터넷 비즈니스의 집약도 측정=〉 정보보호 비용조사 =〉 정보보호에 대한 ROI 산정 순으로 이루어진다(가트너, 1987).

3.3 정보보호 안전진단 성과측정 모델

정보보호에 있어서 전략은 고객 지향성과 경쟁 우위의 창출하는 핵심적인 요소라고 할 수 있다. 업무를 수행함에 한정된 자원을 통해 성과를 향상시키기 위해 끊

〔표 11〕 정보보호 안전진단 성과지표 통합지표 목록

관점	전략목표	성과목표	성과지표	지표 구분	연구	정책	개인	관리 영역
정보보호 성과	정보보호수준 제고	경제적 효과 달성	정보보호 매출액	결과	0	0		공통
			피해감소 실적	산출		0		공통
		정보보호 능력 제고	안전진단 대상자 침해사고 발생비율	산출		0		공통
			정보보호관리체계인증 실적	산출		0		민간
	침해사고 방지 효과 제고	침해처리 시간단축	서비스업체(이용자) 피해시간	산출	0	0		민간
			공급업체(제공자) 피해시간	산출	0	0		민간
		침해사고방지활동 강화	해킹 사고/바이러스 신고실적	산출	0	0		공통
			개인정보 침해사고 신고 실적	산출	0	0		정부
정보보호 활동	정보보호 관리 체계활동 강화	정보보호안전진단 확대	안전진단 설비 및 시설 점검율	과정	0	0		민간
			정보자산의 안정적 관리실적	과정	0			공통
			안전진단 취약점 진단(장비)실적	과정	0	0		민간
	정보보호 기술 체계활동 강화	개인정보암호보안기술역량 강화	암호화 통신율	과정		0		정부
			암호화 저장율	과정	0			정부
		침해사고조치 능력 제고	악성코드 일일점검 실적	과정			0	공통
			보안설정(패치) 적용율	과정	0		0	공통
	이용자보호수준 제고	개인정보피해방지 체계정비	주민등록번호 수집율	과정		0		정부
			주민등록번호 대체수단 이용실적	과정		0		정부
		개인정보인증체계 강화	공인인증서 사용율	과정	0	0	0	공통
정보보호 정책	정보보호 정책 체계 강화	정보보호전략계획수립	정보보호방침 수립실적	과정	0			공통
			정보보호마스터플랜 수립실적	과정	0			공통
		정보보호 조직정책 정립	정보보호조직(책임)구성율	과정	0	0	0	공통
정보보호 투자	정보보호시스템 구축 확대	정보보호 하드웨어구축 강화	보안서버 보급율	투입	0	0		공통
		정보보호 소프트웨어구축 강화	통합보안관리 솔루션 보급실적	투입	0			민간
	정보보안 역량 강화	정보보호 인적역량강화	정보보호전문교육시간	투입	0		0	공통
			IT관련 보안인력의 확보율	투입	0			공통
		정보보호 투자효과 증대	정부정보보호 예산집행액	투입	0	0		정부

임없이 노력하고 있고, 이러한 일련의 과정을 가능하게 하는 것은 핵심이 되는 가치를 향상시키고 지속적인 대응으로 고객만족을 유지해야 하기 때문이다.

본 연구에서는 관점은 정보보호 안전진단 성과의 중요성을 반영하여 정보보호성과관점, 정보보호정책관점, 프로세스관점, 학습성장 관점으로 정의를 하였다.

〔표 10〕에서 보는 바와 같이 기존 연구한 정보보호 안전진단 성과분석(효과, 투자 등) 연구 자료를 통하여 도출되는 전략목표와 방송통신위원회의 "인터넷정보보호 종합대책"의 중요한 요소를 분석하여 전략목표를 설정하였다.

〔표 10〕에서 보는 바와 같이 기존연구자료를 중심으로 성과측정을 위하여 POOL을 도출하고 도출된 지표 POOL에 대하여 41명의 정보보호 전문가들의 참여를 통하여 가중치를 부여한 결과이다. 3개의 항목인 측정가능성, 구체적 측정 및 측정의 대표성을 5점 척도로 부여하여 평균 3.7이상의 점수를 득한 지표를 중심으로 최종적으로 선정되었으며, 지표중에 중복성 등으로 고려하여 최종적으로 선정하였다.

〔표 11〕에서 보는 바와 같이 정보보호 안전진단 성과를 제도개선과 투입, 과정, 산출, 결과 지표로 구분하였으며, 연구참여자, 정책담당자, 개인적 요소 등으로 구분할 때 지표별로 차이가 있었다. 그리고 지표는 공통, 정부, 민간지표로 구분하였는데, 이는 지표성격별로 필요성에 따라 적용내용이 다르게 나타나고 있다.

IV. 정보보호 안전진단 성과측정 및 분석결과

4.1 정보보호성과 관점 측정 지표 및 분석 방법

성과분석을 위하여 자료확보는 안전진단 대상업체를 중심으로 개발된 지표를 상세하게 분석하는 것이 바람직하지만 정보보호 자료를 제공할 수 없는 구조적인 문제로 인하여 기존 연구자료나 정부 발표자료를 최대한 활용하여 성과분석을 수행하였다. 중장기적으로 정보보호 안전진단의 성과분석은 안전진단 대상업체를 중심으로 분석하는 것이 결과의 신뢰성이 높일 수 있을 것이다.

침해처리 시간단축 성과목표 달성을 위해서 측정하고자 했던, 서비스업체(이용자) 피해시간과 공급업체(제공자) 피해시간은 측정가능성 측면에서 어려움이 있기 때문에 성과지표 항목에서 제외하였다.

4.1.1 정보보호산업 성장률

지표는 정보보호산업 매출액을 조사하기 시작한 2005년을 기준으로 정보보호산업의 매출액 증가 대비 정보보호산업이 속해있는 정보통신사업의 매출액 증가를 비교해서 정보보호산업 성장률을 산출한다.

산식은 정보보호산업 성장률= 정보보호산업 매출액 CAGR/정보통신산업 매출액 CAGR[1]로 한다. 여기에서 정보보호산업 매출액 = 정보보호기업의 정보보호 제품(시스템, 네트워크) 매출액+ 정보보호서비스 매출액으로 한다(국내 정보보호산업 시장 및 동향조사, KISA, 한국정보보호산업협회). 정보통신산업 매출액 = 정보통신서비스 매출액 + 정보통신기기 매출액 + S/W 및 컴퓨터관련서비스 매출액로 한다(정보통신산업월보, IT산업통계포털(www.iti.or.kr)).

실적은 2008년도 정보보호산업 성장률이 4.3%이고, 정보통신산업 매출액은 6.6%이므로, 정보보호산업 성장률은 65.5%이다.

4.1.2 피해감소 실적

지표는 한국정보보호진흥원에서 발표한 년도별 정보보호실태조사 기업편의 침해사고로 인한 경제적 피해 경험비율로 정성적으로 피해감소 실적을 측정한다.

산식은 침해사고로 인한 경제적 피해 경험비율 = (시스템 비정상 작동으로 인한 매출 손실 경험비율+시스템 비정상 작동으로 인한 업무효율 저하 경험비율+정보보안 침해사고로 인한 피해복구 경험비율+정보보안 침해사고로 인한 데이터의 영구 손실 피해 경험비율)/4로 한다.

실적은 2008년 시스템 비정상 작동으로 인한 매출 손실 경험비율은 7.3%이고, 시스템 비정상 작동으로 인한 업무효율 저하 경험비율은 23.6%이며, 정보보안 침해사고로 인한 피해복구 경험비율은 26.0%이며, 정보보안 침해사고로 인한 데이터의 영구 손실 피해 경험비율은 10.7%이므로 침해사고 경제적 피해 경험비율은 16.9%이다(정보보호실태조사 기업편(2006, 2007, 2008), KISA).

4.1.3 안전진단대상자 침해사고 발생비율

지표는 안전진단대상자가 안전진단 결과보고서 제출시 작성한 설문지에 응답한 업체 중에서 침해사고

1) CAGR : Compound Annual Growth Rate, 연평균복합성장률(시계열 공식에 의한 기하평균)

$$CAGR = \left\{ \left(\frac{\text{종료값}}{\text{시작값}} \right)^{\left(\frac{1}{\text{년수}} \right)} \right\} - 1$$

발생했다고 응답한 업체의 비율로 산출한다.

산식은 안전진단대상자 침해사고 발생비율 = 2회 이상 침해사고 경험비율+1회 침해사고 경험비율로 나타낸다.

실적은 2008년에 2회 이상 침해사고 경험비율이 13.44%이고, 1회 침해사고 경험비율은 6.99%이므로 안전진단대상자 침해사고 발생비율은 20.43%이다(안전진단 결과(2006, 2007, 2008), KISA)

4.1.4 정보보호관리체계인증 실적

지표는 KISA의 정보보호관리체계(ISMS) 인증 누적 업체수의 증가율로 정보보호관리체계인증 실적을 측정한다.

산식은

$$\left\{\frac{(\text{금년 누적업체수} - \text{전년누적업체수})}{\text{전년 누적업체수}}\right\} \times 100\%$$

이다.

실적은 2008년 누적 업체수가 58개이고 2007년 누계 업체수가 46개이므로 정보보호관리체계인증 실적은 26.09%이다(2008.12, 정보보호관리체계(ISMS) 모범사례집, KISA).

4.1.5 해킹 사고/바이러스 신고실적

지표는 전체 PC보급대수 대비 웜·바이러스와 해킹신고처리에 대해서 인터넷침해사고대응지원센터에 신고건수 비율로 해킹 사고 및 바이러스 신고실적을 산출한다.

산식은

$$\left\{\frac{(\text{웜·바이러스신고건수} + \text{해킹신고처리건수})}{\text{전체}PC\text{보급대수}} \times 100\%\right\}$$

이다.

실적은 KISA의 정보보호지수 측정항목 중 해킹바이러스신고비율 값을 적용할 수 있는데, 2008년도 실적이 2.2%이다(정보보호지수, KISA(2008).

4.1.6 개인정보 침해사고 신고 실적

지표는 KISA의 개인정보침해신고센터와 개인정보분쟁조정위원회에 개인정보침해 사유로 민원접수한 신고건수를 인터넷 이용자수로 나누어서 개인정보 침해사고 신고 실적을 산출한다.

산식은

$$\text{개인정보 침해사고신고실적} = \frac{\text{개인정보침해신고건수}}{\text{인터넷사용인구}} \times 100\%$$

이다.

실적은 2008년 한 해 동안 KISA의 개인정보침해신고센터와 개인정보분쟁조정위원회에 총 39,811건이고(국가정보원, 2009 국가정보보호백서), 인터넷 사용인구는 3,619만명이므로(2008년 인터넷이용실태조사, 방송통신위원회, KISA(2008.11)) 개인정보 침해사고 신고 실적은 11.0이다(정보보호지수, KISA(2008)).

4.2 정보보호활동 관점 성과분석

안전진단제도의 정보보호활동을 정보보호를 위한 정보보호관리체계활동과 기술적 보호조치 활동을 중심으로 목표로 설정하였다.

4.2.1 정보보호 안전진단 실적

지표는 정보보호 안전진단 실적은 안전진단을 처음 실시한 2005년을 기준년도로 해서 안전진단대상자의 연평균복합성장률(CAGR)을 산출한다.

산식은 정보보호 안전진단 실적 = 안전진단대상자 연평균복합성장률(CAGR)이다. 기실적은 2008년도 정보보호 안전진단 실적은 17.8이다(2009 국가정보보호백서, 국가정보원).

4.2.2 정보자산의 안정적 관리실적

지표는 안전진단대상자의 정보화 설비 중에서 안전진단 대상설비가 차지하는 비율과 대상 설비 중에서 현장검사 설비가 차지하는 비율의 평균값으로 정보자산의 안정적 관리실적을 산출한다.

산식은 정보자산의 안정적 관리실적 = (대상설비비율 + 현장검사비율)/2로 한다. 대상설비비율 = 대상설비수/총대수 × 100%이고, 현장검사비율 = 현장검사대수/대상설비수 × 100%이다.

실적은 2008년 전산설비의 총대수는 108,448대이고 안전진단 대상설비수는 72,736대이며, 현장검사대수는 5,694대이므로 대상설비비율은 67.1%이고 현장검사비율은 7.8%이므로 정보자산의 안정적 관리실적은 37.4%이다.(2008 안전진단 결과, KISA)

4.2.3 안전진단 취약점 진단 실적

지표는 안전진단대상자의 취약점 개수 설문에 응답한 기업을 기준으로 평균 취약점 개수를 계산한 후 전

년대비 증가율을 산출해서 안전진단 취약점 진단 실적을 산출한다.

산식은

$$\left(\frac{(\text{금년평균취약점개수}-\text{전년평균취약점개수})}{\text{전년평균취약점개수}}\times 100\%\right)$$

이다.

실적은 정보보호 안전진단대상자에 대한 설문조사 결과에서 2007년취약점수와 2008년취약점수를 분석한 결과 평균 취약점 개수가 82.1개에서 89개로 8.4%정도 증가하였다(2008 안전진단 결과, KISA).

4.2.4 암호화 통신율

지표는 방송통신위원회에서 매년 발표하는 개인정보보호지수 산출 및 수준 측정 결과의 기업영역 세부지표 중 암호화 통신율 값을 적용한다.

산식은

$$\text{암호화통신율}=\left(\frac{\text{모든 또는 일부 사이트에 보안서버를구축한 사업체}}{\text{개인정보수집 사업체중 "모르겠다"응답 사업체}}\right)\times 100\%$$

이다. 실적은 2008년도 암호화 통신율이 62.5%이다(방송통신위원회 보도자료(2009. 3. 6).

4.2.5 암호화 저장율

지표는 방송통신위원회에서 매년 발표하는 개인정보보호지수 산출 및 수준 측정 결과의 기업영역 세부지표 중 암호화 저장률 값을 적용한다.

산식은

$$\text{암호화저장율}=\left(\frac{DB\text{보안제품 사용사업체}}{DB\text{ 사용사업체}}\right)\times 100\%$$

이다.

실적은 2008년도 암호화 저장율이 59.9%이다(방송통신위원회 보도자료(2009. 3. 6).

4.2.6 악성코드 감염 실적

지표는 KISA 인터넷침해사고대응센터에서 발표하는 인터넷침해사고 월간통계의 전 세계 악성 Bot 감염 추정PC 대비 국내 감염률은 하향값이므로, 100%에서 악성코드 감염 비율을 빼서 악성코드 감염 실적 점수를 산출한다.

산식은

$$\text{악성코드감염실적}=\frac{\text{국내악성}\perp\text{감염추정}PC}{\text{전세계악성}\perp\text{감염추정}}\times 100\%$$

$$\text{점수(하향값)}=100\%-\text{악성코드감염실적}$$

로 한다.

실적은 점수(하향값) = 100%-악성코드 감염 실적 = 100%-8.10% = 91.9%이다(인터넷침해사고 월간통계, KISA, 인터넷침해사고대응센터).[2)]

4.2.7 보안설정(패치) 적용율

지표는 보안설정(패치) 적용율은 정성적 방법과 정량적 방법으로 측정할 수 있다. 정성적 방법은 KISA의 정보보호 실태조사 기업편 결과 중 보안관리(보안패치 적용) 현황 조사 결과 실시라고 응답한 업체의 비율을 계산하고, 정량적 방법은 정보보호지수 지표항목인 패치보급율 값을 인용할 수 있다. 본 연구에서는 정량적 방법인 패치보급율로 산출하였다.

산식은 $\text{패치보급율}=\left(\frac{\text{패치설치수}}{\text{인터넷이용자수}}\right)\times 100\%$로 한다.

실적은 2008년도 보안설정(패치) 적용율은 86.5%이다(정보보호지수 지표항목, KISA(2008)).

4.2.8 주민등록번호 수집율

지표는 정보보호 실태조사에 웹사이트를 통해 주민번호를 수집한다고 응답한 비율을 계산한 후에 하향값이기 때문에 100%에서 수집비율을 뺀값으로 주민등록번호 수집율을 산출한다.

산식은

$$\text{주민번호수집율}=\left(\frac{(\text{금년수집}-\text{전년수집})}{\text{전년수집}}\right)\times 100\%$$

로 하고, 점수(하향값)=100%-주민등록번호수집율로 한다.

실적은 2007년 수집비율이 62.2%이고 2008년 수집비율이 51.5%이므로 2008년도 점수(하향값) = 100% - 주민등록번호 수집율 = 100% - 10.7% = 89.3이다.

4.2.9 주민등록번호 대체수단 이용실적

지표는 주민등록번호 대체수단 이용실적은 KISA 정보보호 실태조사 기업편의 I-PIN 서비스 인지비율과 향후 I-PIN 서비스 이용의향 중 I-PIN서비스 이용비율을 평균해서 산출한다.

산식은

---

2) 전 세계 악성Bot감염 추정PC 대비 국내 감염률(%)로 산정하였다. 봇(Bot)이란, 운영체제 취약점, 비밀번호의 취약성, 웜·바이러스의 백도어 등을 이용하여 전파되며, 해킹명령 전달 사이트와의 백도어 연결 등을 통하여 스팸메일 전송이나 DDoS 공격에 악용이 가능한 프로그램 또는 실행 코드이다.

$\frac{(i-IIN서비스\ 인지비율 + i-IIN서비스이용비율)}{2}$로 한다.

실적은 2008년 i-PIN 서비스 인지율은 38.4%이고, i-PIN 서비스 이용율은 3.0%이므로 주민등록번호 대체수단 이용실적은 20.7%이다.[3)]

4.2.10 공인인증서 사용율

지표는 공인인증서 사용율은 KISA 인터넷이용실태조사의 인터넷 이용자수 대비 국가방보원 국가정보보호백서의 연도별 공인인증서 이용자수의 비율로 산출한다.

산식은

$$공인인증서보급률 = \left(\frac{공인인증서이용자수}{인터넷이용자수}\right) \times 100\%$$

실적은 2008년 인터넷 이용자수가 3,619만명, 공인인증서 이용자수는 1,856만명이므로 공인인증서 사용율은 51.3%이다.[4)]

4.3 정보보호정책 관점 성과지표

정보보호정책 관점의 성과지표로는 정보보호방침 수립실적, 정보보호마스터플랜 수립실적, 정보보호조직 구성율 등 3개로 구성되어 있다. 정보보호마스터플랜 수립실적은 정보보호방침 수립실적에 포함시켜서 "정보보호방침 수립실적"만 측정한다.

4.3.1 공인인증서 사용율

지표는 안전진단대상자의 설문결과를 분석해서 정보보호방침 및 지침을 수립했다고 응답한 설문대상업체의 비율로 정보보호방침 수립실적을 산출한다.

산식은

$$정보보호방침\ 수립 = \left\{\frac{(진단이전부터\ 수립 + 진단을위해\ 수립)}{설문대상업체수}\right\} \times 100\%$$

이다.

실적은 2008년도 정보보호방침이 진단이전부터 수립한 곳은 83.33%이고, 진단을 위해 수립한 곳은 13.99%이고 설문대상자는 186개이므로 정보보호전략계획 수립 점수는 97.3%이다(2008 안전진단 결과, KISA).

4.3.2 정보보호조직 구성율

지표는 안전진단대상자의 설문결과를 분석해서 정보보호조직을 구성했다고 응답한 설문대상업체의 비율로 정보보호조직 구성율을 산출한다.

산식은

$$정보보호조직구성율 = \left\{\frac{(진단이전부터\ 구성 + 진단을위해\ 구성)}{설문대상업체수}\right\} \times 100\%$$

이다.

실적은 2008년도 정보보호조직이 진단이전부터 구성한 곳은 69.35%이고, 진단을 위해 구성한 곳은 20.97%이고 설문대상자는 186개이므로 정보보호조직 구성율 점수는 90.3%이다(2008 안전진단 결과, KISA).

4.4 정보보호투자 관점 성과지표

정보보호투자 관점의 성과지표로는 보안서버 보급률, 통합보안관리 솔루션 보급실적, 정보보호전문 교육실적, IT관련 보안인력의 확보율, 정부정보보호 예산 집행액 등 5개로 구성되어 있다.

4.4.1 보안서버 보급률

지표는 보안서버 보급률을 측정하는 방법은 정성적인 방법과 정량적인 방법이 있다. 정성적인 방법은 정보보호 실태조사의 보안서버 구축 형식에 도입이라고 응답한 비율을 산출해서 산출하는 것이고, 정량적인 방법은 KISA의 정보보호지수 지표항목인 인구 10만명당 보안서버 보급률을 적용하는 것이다. 본 연구에서는 정량적인 방법으로 보안서버 보급률을 산출하였다.

산식은

$$보안서버\ 보급률 = \left(\frac{국내\ 보안서버\ 판매대수}{인구수}\right) \times 10만$$

이다.

실적은 2008년도 정보보호지수 지표항목을 인용하면 62.5이다(보보호지수, KISA(2008)).

4.4.2 통합보안관리 솔루션 보급실적

지표는 안전진단대상자의 설문 항목에 ESM(Enter-

3) 개인정보를 수집하는 사업체(종사자수 5명 이상, 네트워크로 연결된 컴퓨터 1대 이상 보유, 2007년 12월 현재) 중 웹사이트를 통해 주민번호를 수집하는 경우로 한다. 자료출처는 2008 정보보호 실태조사 기업편, 방송통신위원회, KISA

4) 연도별 공인인증서 이용자 수 : 2009년 국가정보보호백서, 행정안전부(2008년 12월), 인터넷 이용자수 : 2008년 인터넷이용실태조사, 방송통신위원회, KISA(2008.11).

〔표 12〕 정보보호 안전진단 성과분석 결과와 가중치 설정

관점	W1	전략목표	W2	성과목표	W3	성과지표	W4	가중치	2007년 측정값	가중치 반영값	지표구분	관리영역
정보보호 성과	0.30	정보보호 수준 제고	0.50	경제적 효과 달성	0.50	정보보호산업 성장률	0.60	0.045	65.5	2.95	결과	공통
						피해감소 실적	0.40	0.030	16.9	0.51	산출	공통
				정보보호 능력 제고	0.50	안전진단 대상자 침해사고 발생비율	0.60	0.045	20.43	0.92	산출	공통
						정보보호관리체계인증 실적	0.40	0.030	26.09	0.78	산출	민간
		침해사고 방지 효과 제고	0.50	침해사고방지활동 강화	1.00	해킹 사고/바이러스 신고실적	0.50	0.075	2.2	0.17	산출	공통
						개인정보 침해사고 신고 실적	0.50	0.075	11	0.83	산출	정부
정보보호 활동	0.40	정보보호 관리체계활동 강화	0.40	정보보호안전진단 확대	1.00	정보보호 안전진단 실적	0.40	0.064	17.8	1.14	과정	민간
						정보자산의 안정적 관리실적	0.30	0.048	37.4	1.80	과정	공통
						안전진단 취약점 진단 실적	0.30	0.048	8.4	0.40	과정	민간
		정보보호 기술 체계활동 강화	0.30	개인정보암호보안 기술역량 강화	0.50	암호화 통신율	0.50	0.030	62.5	1.88	과정	정부
						암호화 저장율	0.50	0.030	59.9	1.80	과정	정부
				침해사고조치 능력 제고	0.50	악성코드 일일점검 실적	0.40	0.024	91.9	2.21	과정	공통
						보안설정(패치) 적용율	0.60	0.036	86.5	3.11	과정	공통
		이용자보호 수준 제고	0.30	개인정보피해방지 체계정비	0.50	주민등록번호 수집율	0.50	0.030	89.3	2.68	과정	정부
						주민등록번호 대체수단 이용실적	0.50	0.030	20.7	0.62	과정	정부
				개인정보인증체계 강화	0.50	공인인증서 사용율	1.00	0.060	51.3	3.08	과정	공통
정보보호 정책	0.15	정보보호 정책 체계 강화	1.00	정보보호전략계획 수립	0.50	정보보호방침 수립실적	1.00	0.075	97.3	7.30	과정	공통
				정보보호 조직정책 정립	0.50	정보보호조직(책임)구성율	1.00	0.075	90.3	6.77	과정	공통
정보보호 투자	0.15	정보보호시스템 구축 확대	0.50	정보보호 하드웨어구축 강화	0.50	보안서버 보급율	1.00	0.038	62.5	2.34	투입	공통
				정보보호 소프트웨어구축 강화	0.50	통합보안관리 솔루션 보급실적	1.00	0.038	1.0	0.04	투입	민간
		정보보안 역량 강화	0.50	정보보호 인적역량강화	0.50	정보보호전문교육실적	0.50	0.019	16.71	0.31	투입	공통
						IT관련 보안인력의 확보율	0.50	0.019	10.4	0.20	투입	공통
				정보보호 투자효과 증대	0.50	정부정보보호 예산집행액	0.60	0.023	43	0.97	투입	정부
						민간 정보보호 투자 실적	0.40	0.015	55.4	0.83	투입	민간
합계	1.0		-		-		-	1.0		43.61		

주 : 가중치 = W1*W2*W3*W4

W1 : 관점별 가중치로 관점별 가중치의 합이 1이 되게 정보보호 측정 전문가그룹의 브래인스토밍을 통해 가중치를 배분하였다.

W2 : 전략목표별 가중치로서 관점별로 가중치의 합이 1이 되게 배분하였다.

W3 : 성과목표별 가중치로서 전략목표별로 가중치의 합이 1이 되게 배분하였다.

W4 : 성과지표별 가중치로서 성과목표별로 가중치의 합이 1이 되게 배분하였다.

prise Security Management, 통합보안관제시스템)과 UTM(Unified Threat Management, 통합위협관리시스템), 통합보안관제서비스 등의 항목을 추가해서 설문응답업체 대상으로 평균 통합보안관리 솔루션 보급 실적의 CAGR을 계산해서 통합보안관리 솔루션 보급실적을 산출한다.

산식은 $\left\{\left(\frac{\text{현재값}}{\text{기준값}}\right)^{(1/\text{년수})} - 1\right\} \times 100\%$ 이다.

실적은 2005년부터 2007년까지의 보안관제 안전진단대상설비수를 확인할 수 없으므로, 통합보안관리 솔루션 보급실적은 산출하지 않았다. 2008년에는 설문응답업체가 25곳, 보안관제 안전진단대상설비수 162대이

고 평균 보안관제안전진단 대상설비수는 6.5대이다.

4.4.3 정보보호전문교육 실적

지표는 정보보호 전문교육실적은 KISA에서 실시하는 정보보호 일반교육과 전문교육 인원수의 증가율로 산출한다.

산식은

$$\text{정보보호 전문교육실적} = \frac{(\text{금년 인원수} - \text{전년인원수})}{\text{전년 인원수}} \times 100\%$$ 이다.

실적은 2008년 보안교육인원수가 6, 210명이고 2007년에는 5,415명, 2005년에는 3,906명이므로 CAGR은 16.71%이다(국가정보보호백서(2005, 2006, 2007, 2008), 국가정보원).

4.4.4 IT관련 보안인력 확보율

지표는 안전진단대상자가 응답한 설문결과를 분석해서 정보보호 전담조직 인원의 합계를 계산한 후 설문에 응답한 업체수로 나누어서 평균 정보보호 전담조직 인원수를 계산한 후에 2006년 이후의 CAGR로 IT관련 보안인력 확보율을 산출한다.

산식은

$$\text{평균정보보호전담조직인원수} = \left(\frac{\text{전담조직인원합계}}{\text{설문응답업체수}}\right)$$ 이며,

$$\text{전기대비증가율} = \left(\frac{\text{금년평균인원수} - \text{전년평균인원수}}{\text{전년평균인원수}}\right) \times 100\%$$

이다.

실적은 정보보호 전담조직 인원은 2006년 485명, 2007년 590명, 2008년 786명이고, 설문에 응답한 업체수는 2006년 101곳, 2007년 123곳, 2008년 147곳이다. 그러므로 2008년 IT관련 보안인력 확보율은 10.4%이다(정보보호 안전진단 결과검토 보고서(2006,2007,2008)).

4.4.5 정부 정보보호 예산비율

지표는 정부 정보보호 예산비율은 정보화관련 국가예산 중에서 정보보호 관련 국가예산이 차지하는 비율을 측정해서 산출한다.

산식은

$$\text{정부정보보호예산비율} = \left(\frac{\text{정보보호관련국가예산}}{\text{보화관련국가예산}}\right) \times 100\%$$

이다.

실적은 정보보호 예산비율은 KISA에서 조사하는 정보보호지수 지표항목 중의 하나로 이 결과를 인용하면 2008년도는 43%이다(정보보호지수 지표항목, KISA(2008)).

4.4.6 민간 정보보호 투자 실적

지표는 민간 기업에서 정보보호 장비를 도입하거나 서비스를 이용하기 위해서 지출한 정보보호 투자 실적을 측정하기 위해서 KISA에서 매년 실시하는 정보보호 실태조사 기업편의 정보화 투자 대비 정보보호 투자 비율 중 정보보호지출이 있다고 응답한 설문자의 비율로 산출한다.

산식은 정보보호 투자 실적 = 정보보호지출이 있다고 응답한 설문자의 비율(%)이다.

실적은 2008년 정보화 투자 대비 정보보호 투자 비율은 55.4%이다(정보보호 실태조사 기업편, 방송통신위원회, KISA(2009)).

4.5 정보보호 안전진단 성과측정 실증 분석 결과

4.5.1 성과분석과 가중치 설정

정보보호 안전진단 성과분석에 대한 결과를 정리하면 〔표 11〕에서 보는 바와 같다. 각 측정항목에 대해 종합적으로 검토하기 위해 관리영역 가중치를 설정하였다. 가중치는 전체를 합을 1.0으로 정보보호 안전진단 성과분석의 참여자 41명이 부여한 값을 기준으로 전체 가중평균값을 산정하였으며, 그 결과를 최종가중치를 정의하였다. 그리고 가중치는 관점, 전략목표별, 성과지표별로 부여 하였다.

〔표 12〕에서 보는 바와 같이 2008년도 정보보호 안전진단 성과지표를 가중치를 반영하여 계산한 전체 수준은 43.61이다. 각각의 가중치의 산정은 전략적인 측면에서 AHP기업을 응용하여 관점, 전략목표, 성과지표별로 가중치를 부여하였다. 참여 인력으로는 중소기업의 정보보호담당자의 교육과정에 참여한 41명의 설문값을 단순평균으로 가중치를 부여하였다. 그리고 연구과정에서 전문가 참여를 통하여 최종적으로 지표를 설정하고 가중치를 부여하였다.

실질적으로 성과측정을 위한 데이터는 정부정책 발표자료, 통계분석보고서, 안전진단 대상기관의 실적 등을 고려하여 결과를 도출하였다.

4.5.2 국가·사회적 측면 성과측정 분석

관리영역 안전진단 성과지수 48.21점으로 국가정보보호지수 중 정보보호수준지수에 비하여 상대적으로 낮은 점수로 분석되었다. 민간(기업) 관리영역 안전진

〔표 13〕 년도별 정보보호 안전진단 성과측정 결과

관점	전략목표	성과목표	성과지표	측정값			
				2005년	2006년	2007년	2008년
정보보호 성과	정보보호수준 제고	경제적 효과 달성	정보보호산업 성장률	-	85.9	41.3	65.5
			피해감소 실적	-	8.8	6.8	16.9
		정보보호 능력 제고	안전진단 대상자 침해사고 발생비율	17.9	10	10	20.43
			정보보호관리체계인증 실적	36	11.76	21.05	26.09
	침해사고 방지 효과 제고	침해사고방지활동 강화	해킹 사고/바이러스 신고실적	1.9	1.9	1.03	2.2
			개인정보 침해사고 신고 실적	5.6	5.6	7.6	11
정보보호 활동	정보보호 관리체계활동 강화	정보보호안전진단 확대	정보보호 안전진단 실적	-	12.7	20.7	17.8
			정보자산의 안정적 관리실적	-	-	-	37.4
			안전진단 취약점 진단 실적	-	-	-	8.4
	정보보호 기술 체계활동 강화	개인정보암호보안기술 역량 강화	암호화 통신율	-	-	53.9	62.5
			암호화 저장율	-	-	59.9	59.9
		침해사고조치 능력 제고	악성코드 일일점검 실적	81.2	87.5	88.7	91.9
			보안설정(패치) 적용율	82	82	84.4	86.5
	이용자보호수준 제고	개인정보피해방지 체계정비	주민등록번호 수집율	-	-	96.6	89.3
			주민등록번호 대체수단 이용실적	-	20	16.7	20.7
		개인정보인증체계 강화	공인인증서 사용율	32.5	41.2	48.2	51.3
정보보호 정책	정보보호 정책체계 강화	정보보호전략계획수립	정보보호방침 수립실적	73.6	93	94	97.3
		정보보호 조직정책 정립	정보보호조직(책임)구성율	86.3	88.6	92	90.3
정보보호 투자	정보보호시스템 구축 확대	정보보호 하드웨어구축 강화	보안서버 보급율	43	43	54	62.5
		정보보호 소프트웨어 구축 강화	통합보안관리 솔루션 보급실적	-	-	-	-
	정보보안 역량 강화	정보보호 인적역량강화	정보보호전문교육시간	-	17.38	17.74	16.71
			IT관련 보안인력의 확보율	-	-	-	10.4
		정보보호 투자효과 증대	정부정보보호 예산집행액	35	35	50	43
			민간 정보보호 투자 실적	59.9	55.3	48.9	55.4

단 성과지수 44.66점으로 기업영역 정보보호 지수에 비하여 상대적으로 낮은 점수로 분석되었다. 그리고 공공관리영역의 안전진단 성과지수는 48.21점으로 분석되었다.

위에서 설정된 정보보호 안전진단 성과측정 지표를 이용하여 공공기관의 분석자료와 안전진단수행기관의 통계를 분석하여 실적값을 반영하였으며, 이 과정을 통하여 도출된 정보보호 안전진단 성과측정결과는 아래와 같다.

비록 일부지표는 국가측면에서 관리하지 못한 부분도 있으나 중장기적으로 측정항목의 체계적인 관리가 필요하며, 정부의 정보보호 안전진단 성과지수의 증감율과 국가정보보호 지수의 증감율을 비교해서 정보보호 안전진단 효과성을 체계적으로 분석할 필요가 있을 것이다.

V. 결론

안전진단 제도의 제도적 현황, 추진실적 및 수행절차 등을 분석하고, 국가적 측면 및 기업측면에서 주요 보안요소를 분석하며, 지속적인 정보보호 수준을 제고하기 위하여 정부/민간의 정보보호 안전진단 성과분석 방법을 개발함에 있어 정보보호의 성과관리지표/지수를 검토하여 정성적, 정량적인 지표를 발굴하여 정보보호 효과분석에 활용하기 위하여 자료수집 및 수용성 등을 고려하여 이해관계기관과 협의를 통한 타당성을 검증한 후 확정된 방법론을 제시하였다.

성과측정 분석 방법론에 대한 설문항목은 이해관계기관의 업무이해 및 인터뷰를 통하여 자료를 수집하거나 내부, 외부전문가의 검토를 통하여 안전진단 대상업체의 효과분석을 위하여 대상업체별로 분석한 결과를 이용하여 성과분석을 추진하였다.

정보보호 사업지원은 계획, 실행, 점검, 지속개선 과정을 통하여 이루어지고 있어 실질적인 정보보호의 효과를 창출하기 위해서는 조직의 목표와 현실적으로 적합한지, 목표와 방법적으로 지속적으로 측정이 가능한지, 체계적으로 접근하여 문제해결을 통하여 정보보호의 중요성을 고려한 성과분석이 진행되었다.

이러한 성과분석을 위한 기연구자료, 방통위 정보보호정책 및 내부 및 외부전문가의 자문을 통하여 정보보호 안전진단을 정부(공공) 및 기업(민간)으로 구분하여 정리하였으며, 이러한 지표를 발굴하고 정의서를 개발하였으며, 이러한 절차를 통하여 성과분석을 실시하였다. 성과분석은 크게 공공기관의 분석자료와 안전진단 수행기관의 통계를 분석하여 실적값을 반영하였다. 보다 발전하는 정보보호성과분석을 위하여 추가적으로 노력이 필요한 사항으로는 다음과 같다.

첫째로 성과/효과분석을 위한 적정성과 수용성 검토가 필요하다. IT기술투자에 대하여는 효과성을 도출할 수 없다고 일부 연구자들은 논하기도 한다. 하지만 정보보호가 기업은 물론 국가정책적으로 추진하는 중요사업인 만큼 자발적인 안정화를 기반을 확보하기 전까지는 정부에서 많은 역할을 해야한다. 특히 정책목적성을 고려한다면 정보보호성과를 분석하는 것이 다양한 위험을 줄이는 방법보다는 정책방향을 설정하는 역할에 영향을 미칠 있다. 본 연구가 안전진단 성과분석하는 것이 초기단계로 지속적인 방법과 목적성을 명확하게 정의하여 지속적으로 분석한다면 의미가 있는 일이다. 무엇보다도 무결성 있는 데이터를 확보하는 것이 가장 관건이고, 설정된 지표에 대한 수용성을 검증하는 방법이 추가적으로 필요하다.

둘째는 단기간내에 현재 신뢰할 수 있는 데이터 중심으로 결과를 도출하는 것이 필요하다. 정보보호안전진단과 국가정책적으로 다양하게 분석관리하는 지표에 대하여 중요성과 목적성을 고려하여 안전진단 대상업체에게 의무적으로 데이터를 수령할 수 있는 방법을 강구할 필요가 있다. 그리고 안전진단의 설문지를 보완하여 성과분석을 하기 위한 지표중심으로 변경하여 활용하는 방법이 필요하다.

셋째로 안전진단업체를 중심으로 성과분석을 실시하는 것이다. 현재 선정된 안전진단대상업체들이 정보통신기반과 서비스분야에서 대부분 우수한업체들로 선정되어 있어, 체계적인 성과분석을 실시할 필요가 있다. 실제적인 데이터를 수집하여 분석하여 실질적인 효과를 분석하는 방법이 필요하다. 본 연구에서는 지표도출과 개발을 주로하였으며, 일부 도출가능한 부분은 분석하였으나 안전진단의 영역을 중심으로 진행되지 않아 관련부서에서 활용하는 것은 한계가 있다.

넷째로 안전진단 성과를 분석하여 조직성과와 연계하여 활용해야 한다. 정보보호안전진단의 수행성과를 조직내의 부서 또는 개인의 성과와 연계시켜 활용할 수 있도록 제도적인 적용이 필요하다.

본 연구는 정보보호 안전진단 제도에 대한 성과측정 지표 개발을 시도 했다는 점에서는 대단한 의미가 있으나 정책적 제도에 기반한 연구로 한계가 있다 하겠다. 향후 정책적 과제에 대한 분석을 연구한 것으로 지표의 안전성, 객관성, 효율성을 측정하기 위하여 보다 많은 연구가 필요하다. 이는 정보보호분야에 대한 성과나 효과를 측정한다는 것은 조금 이르다는 느낌도 있지만 중장기적으로 AHP, 상관관계, 회기분석 등을 통하여 실질적 성과를 단계적으로 검증하는 방법도 적극적으로 검토할 필요가 있다.

참고문헌

[1] 공희경, "BCS 관점에 의한 정보보호 투자효과 분석," 경영대학 박사학위논문, 충북대학교, 2008년 8월.

[2] 공희경, 김태성, "정보보호 투자효과에 대한 연구동향," 정보보호학회지, 17(4), pp. 12-19, 2007년 8월.

[3] 김태성, "정보보호 안전진단 성과측정의 연구," KISA, 2009년.

[4] 국가정보원, 2007 정보보안 관리실태평가 해설, 2007년.

[5] 권영옥, 김병도, "정보보안사고와 사고방지 관련 투자가 기업가치에 미치는 영향," Information System Review, 제9호, 제1호, pp. 105-120, 2007년 4월.

[6] 진경수, "기업업무관점의 업종별 특성을 고려한 기업정보화수준평가에 관한 연구," 석사학위논문, 연세대학교, 2002년 2월.

[7] 김인주, "정보화수준 성숙모델 기반의 통합평가시스템 개발," 박사학위논문, 연세대학교, 2000년 2월.

[8] 김정덕,박Z정은, "TCO 기반 정보보호 투자수익률(ROSI)에 대한 연구," 디지털정책학회 창립학술대회 논문집, pp. 251-261, 2003년 12월.

[9] 김찬식, "개인정보화 수준 평가시스템 개발 및 적용에 대한 연구," 석사학위논문, 연세대학교, 2003

년, 2월.
[10] 남상훈, "기업 정보보호 투자효과 분석방법에서 보안 Event가 주식가격에 미치는 영향 실증연구," 박사학위논문, 고려대학교, 2006년 2월.
[11] 박성욱,윤종민, "산업연관분석을 이용한 정보보호 산업의 연구개발투자에 대한 경제기여도," 한국기술혁신학회 춘계학술대회 논문집, pp. 19-29, 2006년 1월.
[12] 백승민, "기업 정보보호 수준평가 방법론에 대한 비교 연구," 석사학위논문, 한양대학교공과대학원 pp. 82-86, 2007년 2월.
[13] 선한길, "국내기업의 정보보호 정책 및 조직 요인이 정보보호성에 미치는 영향," 한국경영정보학회 춘계학술대회 논문집, pp. 1087-1095, 2005년.
[14] 시스코 시스템즈, 네트워크 정보보호에 대한 투자 수익, 백서, 2003년
[15] 신승호, "공공부분 BSC운용이 조직성과에 미치는 영향에 관한 실증연구:PDCA 중심으로," 박사학위논문, 단국대학교, 2007년 2월.
[16] 신일순, "정보보호의 경제학적 의미에 대한 소고," Information Security Review, 1(1), pp. 27-40, 2004년 5월.
[17] 유석천,이재우,염정호, "정보보호 부문에 대한 투자모형에 관한 연구," 정보통신정책연구, 8(2), pp. 17-48, 2001년 1월.
[18] 이정훈,신택수,임종호, "PLS경로모형을 이용한 IT조직의 BSC성공요인간의 인과관계분석," 경영정보학연구, 17(4), pp. 207-228, 2007년 12월.
[19] 이종선,이희조, "TCO기반 Security ROI를 활용훈 정보보호 투자 성과 평가방법," 한국정보처리학회 춘계학술대회 논문집, 14(1), pp. 1125-1128, 2007년 5월.
[20] 임영희, 손명호, 이희석, "IT균형성과표를 활용한 IT성과지표의 비교분석," 한국경영정보학회 춘계학술대회, 2004년.
[21] 정선호,이영찬, "BSC를 이용한 IT조직의 성과관리체계에 관한 연구," 한국산업경영시스템학회 추계학술대회, pp. 49-52. 2005년 10월.
[22] 한국전산원, 공공부문 정보화 사업평가를 위한 BCS 모형, 2001년 1월.
[23] 한국전산원, 제10회 기업정보화평가사업-2006 기업정보화수준평가 설문서(은행, 증권업종), 정보통신부, 2006년.
[24] KISA, 2007 정보보호 실태조사-기업편, 2007년.
[25] KISA, 국가 정보보호수준 평가지수 산출과 국제화 추진에 관한 연구, 2006년.
[26] KISA, 이메일 및 휴대전화 스팸지수에 대한 스팸스코어링 개발, 2007년.
[27] KISA, 중소기업 정보보호수준 자가측정서비스, 2007년.
[28] KISA, 기업 정보보호 진단 체크리스트, 2008년.
[29] 한국정보사회진흥원, 2007 기업정보화수준평가 결과보고서, 2007년.
[30] 홍기향, "정보보호 통제와 활동이 정보보호 안전진단 성과에 미치는 영향에 관한 연구", 박사학위논문 국민대학교, 2004년 2월.
[31] Al-Humaigani, M. and Dunn, D.B., "A model of return on investment for information systems security," Circuits and Systems, Vol.1, pp. 483-485 2003.
[32] Bodin, L.D., L.A and Loed, M.P, "Evaluating infortmaion security investment using the analytic hierarchy process," Communication of the ACM, Vol.11, No3, pp. 431-448, 2005.
[33] Campbell, K., Gordon, L.A., Loeb, M.P. and Zhou, L., "The economic cost of publicly announced information security breaches: Empirical evidence from the stock market," Journal of Comtuter Security, Vol.11, No.3, pp. 431-448, 2003.
[34] Cavusoglu, H, Cavusoglu, H.(Huseyin) and Raghunathan S., "Economics of IT security management: Four improvements to current security practices," Communications of the Association for Information System, Vol.14, pp .65-75 2004.
[35] Cavusoglu, H., Mishra, B. and Raghunathan, S., "A model for evaluating IT security investments," Communications of the ACM, Vol.47, No.7, pp. 87-92, Jul 2004.
[36] CSI/FBI, Computer Crime and Security Survey, 2007.
[37] Davis, A., "Return on security investment- proving it's worth it," Network Security, Vol.2, pp .8-10, 2005.

[38] Grembergen, W.V., Saull,R. and Haesm S.D., "Linking IT balaced scorecard to the business objectives at a major canadian financial group," Journal of Information Technology Cases and Applications, pp. 23-50, 2003.

[39] Hair, J. F. Jr., Black, W. C., Babin, B. J., Anderson, R. E. and Tatham, R. L., "Multivariate data analysis," Prentice-Hall International, 2006.

[40] Kim, S. and Leem, C.S., "implementation of the sicurity system for instant messengers," Lecture Notes in Computer Science, Vol.3314, pp. 739-744, 2004.

[41] Kumar, R.L., "A framework for assessiing the business value of information technology infrastructures," Journal of Management Information Systems, Vol.21, No.2, pp. 11-32, 2004.

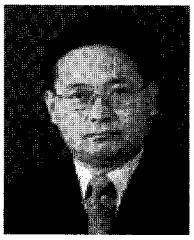
[42] NIST, Security Considerations in the Information System Development Life Cycle, SP 800-64 Revision 2, 2008.

[43] Odlyzko, Economics, Psychology, and Sociology of Security, Springer Berlin, pp. 182-189, 2003.

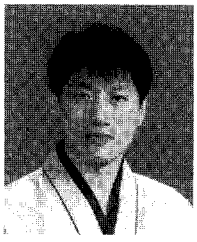
[44] Tsiakis, T. and S., George, "The ecomomic approach of information security," Computers & Security, Vol. 24, No.2, pp 105-108, 2005.

〈著者紹介〉

장 상 수 (Sang-Soo Jang) 정회원
1989년 2월: 한국항공대학교 항공정보통신공학과 졸업(학사)
2000년 2월: 동국대 대학원 정보보호학과 졸업(석사)
2000년~현재: KISA, KISA 팀장
2004년~현재: 전남대학교 대학원 정보보호학과 박사과정
〈관심분야〉 ISMS, IT위험관리, 정보보호 거버넌스, 시스템 및 네트워크 보안



신 승 호 (Seung-ho Shin) 정회원
1992년: 방송대대학교 전자계산학과(이 학사)
1995년: 성균관대학교 대학원 감사행정학과(컴퓨터감사 석사)
2007년: 단국대학교 대학원 경영정보학과(경영학 박사)
2003~현재: 단국대 경영정보학과/건국대 정보통신대학원의 겸임교수역임
대한경영평가원 이사 재직중
<관심분야> PDCA Cycle, 경영성과(조직, 정보화, 사업 등), 정보보호성과정보관리기술사, ISO27001, K-ISMS, G-ISMS 심사원



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 ~ 현재: 시스템보안 연구센터 소장
〈관심분야〉 컴퓨터와 네트워크 보안, 정보보호시스템, 전자상거래 보안, 사이버사회와 윤리