균형성과표(BSC) 기반의 정보보호 성과 지표 개발 및 측정 방법에 관한 연구

장상수*

요 약

조직의 정보보호 목표를 효율적이고 효과적으로 달성하기 위해서는 정보보호 수준을 정확히 평가하고 개선 방향을 제시하는 정보보호 성과평가 지표와 측정방법이 필요하다. 그러나 이러한 요구사항에도 불구하고 국내 기업의 정보보호 활동에 대한 성과나 효과를 측정하기 위한 표준적인 지표나 활용 가능한 측정 방법이 미흡한 실정이다. 이로 인해 기업에서는 지속적인 보안투자 결정을 이끌어 내는데 큰 어려움을 겪고 있다. 본 연구의 목적은 이러한 각 기업 환경에 적합한 합리적인 성과평가를 위하여 성과평가에 영향을 주는 다양한 관점에서 성과평가지표를 도출하고, 평가지표간 중요도에 따른 가중치 부여를 통하여 평가 지표와 측정방법을 개발하는 것이다. 정보보호 활동의 다양한 성과 요인을 균형 있게 평가하기 위해 Norton과 Kaplan(1992)이 개발한 균형성과표 (BSC : Balanced Scorecard) 모형을 활용하였다. 본 연구 결과는 국내 기업들이 정보보호 수준을 파악하고 주기적인 성과측정을 통해 자사의 정보보호 현황 파악과 추이 분석이 가능하고 정보보호 투자 등 전략을 수립하는데 적용할 수 있다.

A Study on Developing of Performance Evaluation Index and Method of Measurement for Information Security Outcomes applying BSC

Jang Sang Soo*

ABSTRACT

In order to achieve efficient and effective organizational information security objectives, for the level of informatio n security to accurately evaluation and direction for improving that performance evaluation index and method of mea surement for information security outcomes are needed. For information security activities of domestic companies to measure the performance or effectiveness, that standard method of measuring and the available evaluation Index are insufficient. company is difficult to investment for information security budget. Therefore, the purpose of this study was developing of performance evaluation index and method of measurement for information security outcomes apply ing BSC available in the company. The results of this study that companies can determine the level of information s ecurity itself. Analysis of the information security status and the strategy establishment of the information sec urity investment can be applied.

Key words : BSC(Balanced Scorecard), Method of Measurement, Information Security Outcomes, Performance Evaluation Index

접수일(2014년 6월 10일), 수정일(1차: 2014년 6월 20일), 게재확정일(2014년 6월 24일)

* 아주대학교/지식정보보안학과

1. 서 론

최근 지속적으로 발생하고 있는 사이버 침해사고 , 강화되고 있는 정보보호 컴플라이언스, 기업의 사회적 책임 등에 대응하기 위해 기업에서는 다양한 위험관리 활동을 하고 있다. 이와 같은 정보보호 활동에 대한 성과에 대해 요구사항이 급증하고 있다. 그러나 이러한 정보보호 활동에 대한 성과나 효과를 측정하기 위한 국내의 표준적인 지표나 활용 가능한 측정 방법이 미흡한 실정이다. 또한 현재 국가적으로나 기업에서 정보보호 효과에 대하여 측정 가능한 지표가 부족하며 지속적인 보안투자 결정을 이끌어 내는데 큰 어려움으로 작용하고 있다. 정보보호 성과 지표 개발은 국가적 지표와 각 기업의 지표 등으로 구분할 수 있으며 각 기업의 성과 지표는 업종, 규모, 서비스 형태 등에 따라 적용 할 수 있는 항목이나 수준이 매우 달라서 지수화 및 측정 방법 자체가 어렵다. 더욱이 국가적 정보보호 수준 측정도 지표자체의 신뢰성 문제로 많은 어려움이 있는 것이 사실이다. 그동안 정보보호 성과 측정의 중요성을 인식하면서도 일반적으로 정보보호의 성과를 측정하는 것은 어렵다라는 것과 측정하지 못하는 것은 관리할 수 없다라는 의견이 팽팽하게 대립해 오고 있다. 과거에는 정보유출사고나 침해사고의 발생여부만으로 정보보호 성과를 인정받을 수 있었다. 그러나 최근에는 정보보호는 1회성이 아닌 지속적인 투자가 집행되어야 그 수준을 유지할 수 있고 고객정보/회사내부정보의 양과 질이 늘어남에 따라 보안에 투자되는 장비, 예산의 규모가 지속적으로 증가하고 있는 상태로 성과측정 및 관리가 매우 중요한 요소가 되고 있다. 일부 금융권 등 대기업의 경우에는 이미 내부인력 또는 외부 컨설팅을 통한 자체적인 정보보호 성과지표를 개발하여 측정하고 있으나 아직도 활용도가 매우 낮은 실정이다. 조직과 인력이 충분하지 않은 그 외 기업은 정보보호 성과지표를 만들고 싶어도 참고할 만한 가이드라인이 부족하고 자사의 환경에 직접 적용 가능한 정보보호 성과지표가 없는 상태이다[1,16].

본 연구에서는 각 기업 환경에 적합한 성과지표를 개발/선별할 수 있는 성과지표의 Pool을 제시하고 만들어진 성과지표의 객관성 확보와 실제 측정방법을 제시하여 국가적, 조직 내부적으로도 정보보호 성과 수준이 향상되는 것을 가시적으로 보일 수 있도록 하였다.

정보보호 성과지표의 의미는 정보보호 정책 수립 및 성과평가를 위한 합리적인 의사결정을 내릴 수 있도록 수치화를 시켜주는 도구로 기업의 정보보호 수준을 종합적으로 측정/평가할 수 있는 기준 및 계량화 지표로 조직별 정보보호 현황을 객관적 기준에 따라 평가할 수 있는 체계를 말한다. 정보보호 성과지표가 가져야 할 전제조건으로는 첫째 정보보호 범위와 목적을 분명하게 반영해야 하며, 정보보호와 관련된 여러 주제의 관심과 현상을 대표할 수 있어야 한다. 둘째 조직의 구성원들이 평가결과에 대해 공인된 지수로 받아들일 수 있는 신뢰성을 확보하여야 한다. 셋째 평가결과가 해당 조직의 정보보호 수준을 투명하고 객관적으로 반영해야 하며, 언제, 어디서, 누구에 의해서도 합리적이고 동일한 결과를 얻을 수 있어야 한다. 넷째 보안위협변화, 보안사고 유형 등의 정보보호 환경변화와 시대적 현상을 적시에 반영해야 한다. 다섯째 유사한 체크리스트, 점검항목, 시스템과 차별성을 갖추어야 한다[7,8,9].

2. 정보보호 성과측정 선행연구

2.1 정보보호 효과(투자효과)분석

2.1.1 정보보호 경제성 분석

정보보호 경제성 분석(신일순, 2005)에서는 <표 1>과 같이 정보화 사회가 진행될수록 정보보호의 중요성도 증가하고 있으며, 국내 정보보호의 경제성 분석 연구 현황을 개관하고, 국제적으로 진행되고 있는 연구들을 주제별로 사이버 공격에 의한 피해액 산출, 프라이버시 경제성연구, 정보보호 비용 및 투자가치에 대한 연구 등으로 나누어 분석하였다[5,6,11].

<표 1> 정보보호 경제성 분석 분류

분석	유형	주요내용
정보보호경제성분석	경제적 유인성	정보보호로 인한 위험을 관리하고 방지할 수 있는 경제주체에 책임성이 부과
	네트워크 외부성	하나의 네트워크에 속한 사람이 많아질 수록 그 네트워크의 가치가 증가하는 현상
	비대칭적 정보	비대칭적인 정보는 정보가 한쪽에만 존재하고 다른 쪽에는 존재하지 않은 현상
	가격차별과 개인정보	개인정보에 대한 보호와 침해가 동시에 가능해졌음에도 불구하고 현재까진 개인정보의 침해 강화보다는 훨씬 폭넓게 관철되어 사회적으로 문제되는 현상

2.1.2 인터넷침해사고 피해액 산출 연구

인터넷침해사고 피해액 산출 연구(KISA, 2006)에서는 인터넷 침해사고로 인한 사회경제적 손실액의 측정을 위해 국가전반의 실질적 손실비용과 이를 복구하기 위한 비용에 대한 실태조사를 수행하여 손실비용과 복구비용의 주요 요인들을 파악하고, 피해액을 산출할 수 있는 지표 개발을 연구하였다[13,14].

<표 2>와 같이 침해사고로 인하여 직접적인 손실요소인 손실이익과 복구비용이 발생되고, 간접손실로는 생산효율의 저하, 데이터손실/데이터재생비용, 책임보상액(추가제언) 등이 손실로 나타날 수 있다고 하였다[13,14].

<표 2> 인터넷 침해사고 피해액 산출

구분	직접손실	간접손실
기대손실	AA-손실이익	BB-생산효율저하
추가비용	CC-복구비용	DD-데이터손실/데이터재상비용 EE-책임보상액(추가)

인터넷 침해사고 피해액 산출 지표 적용되는 지표로는 <표 3>과 같이 다양한 항목을 산식으로 산정한 값이 반영될 수 있도록 하였다. 특히 최근에는 법적소송으로 인한 책임보상액 지급문제가 갈수록 증가되고 있어 이에 대한 지표의 추가적인 관리도 필요할 것이다[13,14].

<표 3> 인터넷 침해사고 피해액 산출 지표

기법	산식 1단계	산식 2단계	산식 3단계
침해사고총액산출기법	AA-매출이익 손실금액 (A1XA2XA3)	A1-인터넷 시간이익 (A11XA12X A13XA14)	A11-연간매출
			A12-매출영업이익율
			A13-인터넷의존도
			A14-연간인터넷영업 시간
		A2-피해시간	
		A3-침해사고영향도	
	BB-생산효율 손실액 (B1XB2XB3X B4)	B1-사고영향직원수	
		B2-시간당생산성	
		B3-피해시간	
		B4-생산효율저하비율	
	CC-복구비용 (C1+C2+C3+C 4)	C1-시스템복구비용	
		C2-S/W복구비용	
		C3-H/W복구비용	
		C4-데이터복구비용	
	DD-데이터손실가치 (D1XD2XD3)	D1-불릉 데이터량	
		D2-재생산소요시간	
		D3-재생산 시간당인건비	
	EE-책임보상액 (E1XE2)	E1-책임보상인원수	
		E2-보상금액	

2.1.3 정보보호의 투자효과 측정

김정덕/박정은(2003), 선한길(2005)은 정보보호의 투자효과 측정 연구에서 <표 4>와 같이 정보보호투자 성과 지표를 정보보호관련 사고감소, 자산 손실건수 감소, 비즈니스 기회손실 감소, 타사 경쟁시 손해감소, 이미지 실추감소, 사고발생시 처리시간 등으로 나타난 비용을 TCO(Totol Cost Ownership)로 산정하는 효과를 분석하였다[4,5,9].

<표 4> 정보보호 투자효과 측정 분류

분석	유형	주요내용
정보보호투자효과	정보보호 투자	TCO 측면의 투자 가시적비용 + 비가시적 비용 하드웨어가격 + 기술지원및유지지원 + 지원인력비용
	정보보호 투자성과	정보보호사고 감소 자산손실건수 감소 비즈니스 기회 손실 감소 타사 경쟁시 손해감소 이미지 실추 건수감소 사고발생시 처리시간 단축 침해사고로 주식가치 감소

	정보보호 산업 연관 분석효과	생산유발효과 부가가치 유발효과 수출유발 효과 고용창출 효과 기업가치 시장 효과

2.1.4 국가정보보호수준 평가지수

국가정보보호 수준평가지수 연구((KISA, 2006)에서는 <표 5>와 같이 지수산출을 위해 지표체계를 정보보호기반, 정보보호환경, 정보화역기능 등 3개로 분류하여 정보보호기반지수는 시스템과 데이터보호를 측정하고, 정보보호 환경지수는 전문인력비율, 정보보호예산비율을 측정하고, 정보화 역기능 지수는 해킹, 바이러스, 개인정보침해비율 등을 측정하는 지표로 적용하였다[13,14].

<표 5> 국가정보보호 평가지수

구분	분류	세부지표	지표산식
정보보호수준지수	정보보호기반	백신보급율	(백신 프로그램 이용자수/ 인터넷 이용자수)X100
		패치보급율	(패치 설치수/ 인터넷 이용자수)X100
		PKI 보급율	(공인인증서 이용자수/ 인터넷 이용자수)X100
		방화벽 보급율	(Firewall을 사용하는 기업체수/ 기업체수)X100
		IDS 보급율	(IDS를 사용하는 기업체수/ 기업체수)X100
		보안서버 보급율	(국내 보안서버 판매대수/ 인구수)X10만
	정보보호환경	정보보호관련 예산	(정보보호 관련 국가예산/정보화 관련 국가예산)X100
		정보보호전문인력	(정보보호 전문인력/정보화 전문인력)X100
		보안의식수준비율	(필요/매우필요 응답자-5점/ 전체조사 대상자)X100
정보화연기능수준	정보화역기능	해킹바이러스 신고비율	(해킹·바이러스 신고건수/ 전체 PC보급대수)X100
		개인정보침해신고비율	(개인정보침해 신고건수/ 인터넷 사용인구) X100
		스팸메일 수신비율	(1계정당수신되는 스팸메일수/1계정당 수신되는 전체 전자메일수) X 100

3. 정보보호 성과측정 모델

3.1 성과평가 지표 기준

성과평가 지표는 성과차원에서 단일화 해야 하며, 성과평가를 위해 본질적으로 요구되는 평가지표의 조건은 타당성, 신뢰성, 적시성, 비용성, 통제가능성 등이 적정해야 하지만 업무 특수성에 따라 일부항목이 추가 또는 감가하는 탄력성이 있을 수 있다. 타당성은 측정하려고 하는 것을 정확하게 측정할 수 있도록 지표를 개발해야 하며, 이 경우 사소한 내용의 경우 생략될 수 있지만 핵심적인 내용은 반드시 포함되어야 한다는 것을 의미이고, 신뢰성은 각각 다른 사람이 동일한 측정도구를 가지고 측정하였을 경우 동일한 결과가 도출될 수 있도록 측정지표가 분명한 의미를 가져야 하며, 적시성은 정책결정자와 관리자가 충분한 시간을 가지고 활용 할 수 있도록 신속하게 자료를 수집할 수 있어야 한다는 것이다. 또한 비용성은 측정결과를 활용함으로써 얻을 수 있는 이익이 측정비용을 상회하여야 한다는 것이며, 통제가능성은 성과측정결과가 잘못된 점을 통제할 수 있어야 한다는 것이다[7,8,9].

<표 6> 성과지표의 기준

타당성	실제로 측정하고자 하는 업무의 측면이나 질(Quality)을 나타낼 것
신뢰성	측정이 정확하고 평가자의 주관성이나 평가수단의 상이함으로 인한 평가치의 편차가 적을 것
이해가능성	오해의 소지가 없을 것
적시성	관리자나 정책결정자가 필요할 때 정보활용이 가능할 것
부작용 제어능력	업무의 다양한 측면을 지표에 반영하여 특정지표에만 노력하는 부작용을 방지할 것
종합성	중요한 요소는 모두 지표에 포함시킬 것
비중복성	개별 지표는 다른 지표와 중복되지 않을 것
측정비용 민감성	측정비용이 측정으로부터 얻을 수 있는 효과를 초과하지 말 것
제어 기능에 집중	업무성과를 향상시킬 수 있는 측면에 집중하여 측정할 것

본 연구에서는 국내의 정보보호 수준평가 및 효과를 분석하는 연구사례는 정보보호 경제성 분석, 인터넷침해사고 피해액 산출 연구, 정보보호의 투자효과 측정, 국가정보보호수준 평가지수, 정보보호수준 평가지수 등 관리하는 항목을 분석하였다.

특히, 정책적인 방향성을 제시하는 측면과 세부적인 실행과 이행조치 항목들까지 반영되어 있어 1차적으로 관리항목의 유사성을 고려하여 분류하였다. 그리고 분류되는 항목들을 정보보호 측면의 성과관리를 BSC(Balanced Scorecard 모델)를 근거한 성과를 분석하는 절차에 의하여 바람직한 정보보호 성과평가지표 및 측정방법을 개발하였다[1,2,7,8].

3.2 균형성과표(BSC)기반의 정보보호 성과

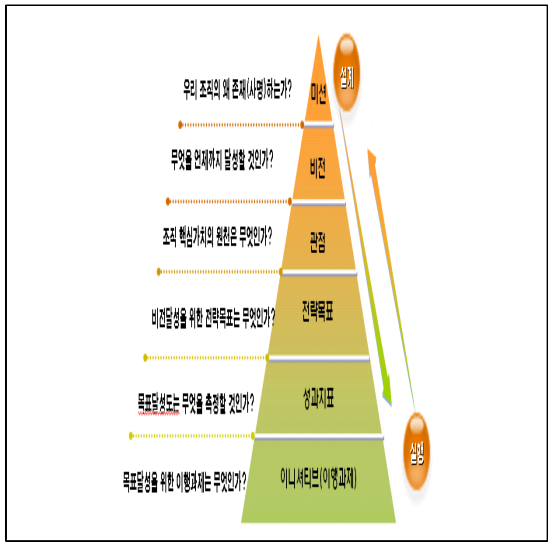
3.2.1 균형성과표(BSC)모델의 개념

BSC는 Kaplan 교수와 컨설턴트인 Norton에 의해 창안된 성과중심의 조직관리 툴(tool)로서 新경영성과 시스템으로 BSC의 핵심개념은 균형을 갖춘 지표체계, 전략에 초점을 둔 상호연계 그리고 조직 내 커뮤니케이션 수단으로 중요한 요소이며, 지표체계는 기존에 중요시해오던 재무적 관점 외에 고객·내부 프로세스·학습과 성장이라는 비재무적 관점도 같이 분석함으로써, 조직전략을 입체적으로 관리할 수 있도록 도와주는 효과적인 가치 중심의 성과측정 기법이다. Kaplan and Norton (1992)은 1990년초 다국적 기업총수들이 의뢰한 “미래조직의 성과측정”이라는 성과측정 모형 개발 프로젝트에서 성과측정의 개선방안으로 BSC의 모형을 제안하였다[7,8,9,10,11,12].

BSC는 관점에 따라 기관의 전략과 비전을 가시화하고, 조직목표를 달성할 수 있게 하고, 구성원들로 하여금 그들의 사업 단위들이 현재와 미래 고객들을 위해 어떻게 가치를 창출할 것인지 그리고 미래 기관 성과를 향상시키는데 필요한 인력과 시스템, 절차에 대한 투자와 내부역량을 결합해야 하는지를 측정 가능케 할 수 있으며, 균형 있는 관점이 의미하는 바는 고객관계·구성원역량·연구개발·프로세스 효율성·품질 등의 무형자산이 장기적으로 조직성공의 핵심 동인(driver) 이라는 것에서 비롯된다[1,2,7,8,9,10,11,12].

전략은 고객 지향성과 경쟁 우위의 창출하는 핵심적인 요소라고 할 수 있다. 업무를 수행함에 한정된 자원을 통해 성과를 향상시키기 위해 끊임없이 노력하고 있고, 이러한 일련의 과정을 가능하게 하는 것은 핵심이 되는 가치를 향상시키고 지속적인 대응으로 고객만족을 유지해야 하기 때문이다. 성과관리(BSC)는 전략 수립의 과정이 구체화되어 있지 않으면, 업무를 수행하는 부서간의 단편적인 시각과 임의적인 방법으로 수립하여 보고하며, 이에 대한 피드백도 제대로 이루어지지 못하게 됨으로 BSC의 구축에 있어서 무엇보다 중요한 것은 전략목표를 명확히 하는 것이다[9,14].

본 연구에서는 (그림 1)과같이 BSC 관점에서 정보보호 성과측정 모델을 개발하기 위하여 균형을 갖춘 BSC 지표체계를 기본 프레임워크로 활용하였다.



(그림 1) BSC 성과평가 프레임워크

본 연구에서는 정보보호 성과나 효과를 측정하기 위하여 관점 체계, 전략목표, 성과지표를 개발하는 절차를 따르고 있으며, 이 절차에 의하여 정보보호 성과측정을 위한 모델을 구현하였다.

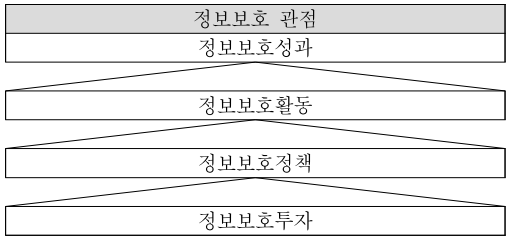
3.3 정보보호 성과평가 체계

3.3.3 정보보호 관점 체계 및 정의

BSC 기반에서의 미션은 조직이 존재하는 이유라

고 할 수 있다. 그 조직은 왜 존재하는가?, 그래서 얻고자 하는 것이 무엇인가를 설명할 수 있어야 한다. 따라서 미션은 그 조직이 존재이유가 되기 때문에 객관적이고 변하지 않은 것이며, 다른 어느 것보다 우선한다. 비전은 미션과 전략사이에서 미션을 달성하기 위한 다리 역할을 한다. 따라서 비전은 조직이 추구하는 장기적인 목표와 미래가치를 반영하고 있으며, 구체적이고 명확한 슬로건이 될 수 있어야 한다. 정보보호에서의 미션 및 비전은 큰 틀에서는 기업 경영의 연속성 확보라는 기본 개념은 동일한 것으로 간주하주 각 조직에 따라 미션 및 비전은 조금씩 상이할 것으로 보아 본 연구에서는 제외하였다.

비전달성을 위한 전략목표들은 “우리조직의 가치는 과연 어디에서 나오는 것인가?, 그리고 그 가치의 원천들은 어떻게 지속적으로 유지할 수 있을까?에 대한 답을 얻을 수 있다. 라는 가치창출의 원천을 관점이라고 하고 비전과 전략목표 사이의관점은 ”조직가치 창출의 원천 또는 전략적 성과지표들의 묶음“이라 할 수 있다. 본 연구에서는 BSC 기반의 관점에서 기업의 특성을 고려하여, 정보보호를 조직 핵심가치의 원천으로 관점을 정보보호성과관점, 정보보호정책관점, 정보보호활동관점, 정보보호투자관점 등으로 구성하였다. 이러한 구성내용은 기존의 연구자료를 중점으로 관련성이 높은 지표 풀을 도출하여 기업보안업무 담당자, 외부전문가 등의 검토회의를 통하여 최종적인 모델을 (그림 2)과 같이 개발하였다[15,16].



(그림 2) 정보보호 관점 체계

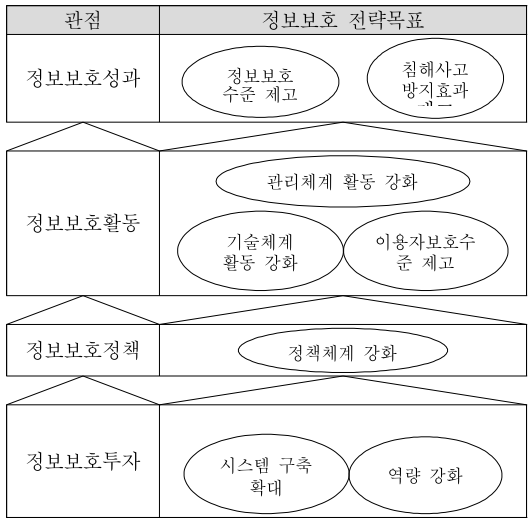
정보보호 성과관리체계 구축을 위하여 관점에 대한 정의는 다음과 (그림 3)와 같다.

관점	정의
정보보호 성과	정보보호 활동을 통한 정보보호 성과로 정보보호체계 강화와 침해사고 감소 등을 기대할 수 있다.
정보보호 활동	정보보호를 위한 기술적 보호조치로 정보보호활동을 수행한다.
정보보호 정책	정보보호를 위한 관리적 보호조치로 정보보호정책을 수립한다.
정보보호 투자	정보보호를 위한 인적투자, 물적투자, 재무적 투자를 수행한다.

(그림 3) 정보보호 관점 정의

3.3.4 정보보호 전략목표 및 정의

정보보호 성과관리체계 구축을 위한 전략목표는 4개 관점별로 전략목표를 설정하였으며, 전략목표간의 인과관계를 고려하여 8개의 전략목표를 (그림 4)과 같이 구성하였다.



(그림 4) 정보보호 전략목표 체계

정보보호 성과관리체계 구축에 필요한 전략목표에 대한 정의는 <표 8>와 같이 설정하였다.

<표 8> 정보보호 전략목표 정의

관점	전략목표	정보보호 전략목표 정의
정보보호 성과	정보보호수준 제고	정보보호활동을 통한 경제적 효과를 달성하고 정보보호 능력을 제고한다.
	침해사고 방지효과 제고	침해사고방지활동을 강화하고 침해처리 시간을 단축한다.
정보보호 활동	관리체계 활동 강화	정보보호를 위해 관리체계 활동을 확대한다.
	기술체계 활동 강화	개인정보암호보안기술역량을 강화하고 침해사고조치 능력을 제고한다.
	이용자보호수준 제고	개인정보피해방지 체계를 정비하고 개인정보인증체계를 강화한다.
정보보호 정책	정책체계 강화	정보보호전략계획을 수립하고 정보보호 조직정책을 정립한다.
정보보호 투자	시스템 구축 확대	정보보호 하드웨어와 소프트웨어의 구축을 강화한다.
	역량 강화	정보보호 인적역량을 강화하고 정보보호 투자효과를 증대한다.

3.3.5 정보보호 성과측정 지표 개발

정보보호 성과측정용 지표를 도출하기 위하여 기존 연구 자료를 활용하여 81개의 지표 풀(Pool)을 <표 9>와 같이 도출하였다.

<표 9>정보보호 성과측정 지표 풀

구분	전략목표	성과지표 풀	
기존 연구 자료	침해처리 시간단축	공급업체(제공자) 피해시간	서비스업체(이용자) 피해시간
	침해사고 방지활동 강화	사고 발생실적, 개인정보 침해사고 신고실적	보안사고대응 조치실적, 해킹 사고/바이러스 신고실적
	투자활동 증진	GDP대비 정보보호투자비율, 정보보호시스템 투자비율	정보보호 예산확보실적
	전략계획 수립	정보보호 실행계획 수립, 정보보호방침 수립실적	정보보호마스터플랜 수립실적,침해사고대응계획의 수립
	솔루션 구축강화	정보보호시스템 보급률, 취약점 점검도구 보급실적	통합보안관리 솔루션 보급실적, 인증시스템 이용율
	기술체계 활동강화	취약점 진단실적,보안설정 적용율	책임자 정기점검율
	조직정책	보호조직구성율,	정보보호실무
	정립	보호규정 준수율	지침 보유실적
	전문인재 교육강화	인식 교육	전문교육시간
	역량강화	정보보호 인력의 수, IT관련 보안인력의 확보율	정보보호 자격증 보유실적, 정보보호기술 표준화 건수
	성과측정 강화	정보보호 산업성장율, 고용창출 효과	부가가치 유발효과, 수출유발 효과
	비용증대	시스템 복구비용,기술지원/유지지원 비용	책임보상금 또는 인원수, 데이터복구비용
	매출증대	정보보호 매출액	정보통신서비스 연간매출액
	관리체계 활동강화	설비와 시설목록 보유율, 보안관리서비스비율	백업시설과 설비구축,유지보수 구성관리
	침해사고 조치능력	국가사이버공격 근원지 파악실적, 악성코드 일일점검실적, 정보보호 소외계층 지원실적,관리체계인증 실적	관리체계 구축실적, 정부정보보호 예산집행액, 침해사고 모니터링 실적
	정보보호 기반조성	이용자 PC자동보안패치적용율,	정보보호전문자격취득실적
	이용자보호 수준제고	악성코드 재감염율, 주민등록번호 수집율	휴대폰 스팸수신량 감소
	국가정보보호 수준제고	국가사이버공격근원지 확인실적, 국가정보보호 지수	보안서버 보급율
	경제적 효과달성	피해감소 실적(국내피해/전세계)	
	개인정보 피해 체계정비	개인정보보호신뢰지수, 개인정보보호인증제 실적, 개인정보보호제도개선 실적	보안서버 보급실적, 주민등록번호 대체수단 이용실적, 침해사고민원처리기간 단축시간
	ID/PW관리활동 강화	PC/웹 비밀번호 관리율	공인인증서 사용율
	보안프로그램 이용강화	악성코드제거PG 사용율, 인터넷 보안설정율	OS업데이트율
	물리적 보안통제 강화	물리적 접근통제율	-
	개인정보 암호보안 기술	암호화 통신율	암호화 저장율
	개인정보보호 조직/교육 정착	정보보호조직구성율	정보보호교육 실시율
	개인정보보호 정책수립	정보보호 취급방침고지율	정보보호정책 확인율

3.4 정보보호 성과 지표 선정을 위한 검증

정보보호 성과분석을 위한 지표를 도출하는 것은 측정가능하고, 구체적이고, 전략적으로 중요성 등을 고려한 지표로 중장기적으로 의미가 있는 지표를 선정하여야 한다. 본 연구에서는 도출된 <표 9>정보보호 성과측정용 81개의 지표 풀에서 관점별 전략목표별 성과지표로 다시 분류하여 전문가의 의견(10명)을 통해 각 성과지표별 측정가능, 구체성, 대표성 3가지로 가중치를 평가하여(5/3/1) 도출하였다. 지표중에서 유사 중복 지표와, 평균 점수 3.7점 이상의 지표를 선정하여 <표 10>와 같이 BSC 기반 8개 전략목표별 15개 성과목표, 27개 세부 성과지표를 도출하였다.

<표 10> BSC 기반의 정보보호 성과지표

순번	관점	전략목표	성과목표	성과지표
1	정보보호성과	정보보호수준 제고	경제적 효과 달성	정보보호 매출액
2				피해감소 실적
3			정보보호 능력 제고	침해사고 발생비율
4				관리체계 수립 실적
5		침해사고 방지 효과 제고	침해처리 시간단축	서비스업체(이용자) 피해시간
6				공급업체(제공자) 피해시간
7			침해사고방지 활동 강화	해킹 사고/바이러스 신고실적
8				개인정보 침해사고 신고 실적
9	정보보호활동	관리 체계 강화	관리 체계 확대	설비 및 시설 점검율
10				정보자산의 안정적 관리실적
11				취약점 진단(장비)실적
12		기술 체계 강화	개인정보암호 보안기술역량 강화	암호화 통신율
13				암호화 저장율
14			침해사고조치 능력 제고	악성코드 일일점검 실적
15				보안설정(패치) 적용율
16		이용자 보호 수준 제고	개인정보피해 방지 체계정비	주민등록번호 수집율
17				주민등록번호 대체수단 이용실적
18			개인정보인증 체계 강화	공인인증서 사용율
19	정보보호정책	정책 체계 강화	전략계획 수립	정보보호방침 수립실적
20				정보보호마스터플랜 수립실적
21			조직정책 정립	정보보호조직 구성율
22	정보보	보안	하드웨어	보안서버 보급율
	호투자	시스템 구축 확대	구축 강화	
23			소프트웨어구축 강화	통합보안관리 솔루션 보급실적
24		역량 강화	인적역량강화	정보보호전문교육시간
25				IT관련 보안인력의 확보율
26			투자효과 증대	정부정보보호 예산집행액
27				정보보호 투자실적

4. 정보보호 성과측정 방법

4.1 정보보호 설과 측정 결과

본 연구는 도출된 BSC 기반의 정보보호 성과지표에 대한 평가를 수행하기 위해 <표 11>과 같이 2013년 12월 1일부터 12월 29일 동안 무작위 추출보다는 실제 정보보호와 연관관계가 가장 높은 정보보호 관리체계(ISMS) 인증을 받은 조직을 대상으로 설문을 시행하였다. 연구대상에 포함되는 2013년도 인증 취득 예정기업 257개 업체(의무대상자 129개, 권고취득업체 128) 중 설문조사 기간안에 인증 미 취득 또는 인증 취득 6개월 미만 기업 98개 업체를 제외한 159개 업체 중 설문지를 불충분하게 작성하거나 혹은 설문 문항에 대한 이해부족으로 인한 작성 오류로 인해 제외된 25개, 미 응답 업체 18개 업체를 제외한 116개 업체를 최종 대상으로 하였다. 본 연구에서 제시하고자 하는 목적에 부합하는 적정 표본수를 가지고 있다고 해석할 수 있다. 설문은 기본정보, 정보보호 성과 관점, 저보보호 활동 관점, 정보보호 정책 관점 등으로 설문조사를 실시하였다[15,16].

<표 11> 설문분석 조사 개요

구 분	내 용
조 사 기 간	2013년 12월 1일 ~ 12월 29일
조 사 대 상	정보보호 관리체계(ISMS) 인증 취득 예상 업체(257개)
표 본 크 기	설문조사 대상기관 유효표본 (116업체)
조 사 방 법	현장방문 조사, 이메일 개별조사, 세미나 개최시 설문
주요설문항목	설문기업의 기본정보, 정보보호 성과 관점, 저보보호 활동 관점, 정보보호 정책 관점 등

4.1.1 정보보호성과 관점 성과측정 지표

정보보호성과 관점의 성과지표로는 <표 12>과 같이 정보보호산업 성장률, 해킹 사고/바이러스 신고실적 등 6개로 구성되어 있다. 정보보호 매출액은 정보보호산업 성장률로 변경하였다. 침해처리 시간단축 성과목표 달성을 위해서 측정하고자 했던 서비스업체(이용자) 피해시간과 공급업체(제공자) 피해시간은 측정가능성 측면에서 어려움이 있기 때문에 성과지표 항목에서 제외하였다.

<표 12> 정보보호성과 관점 성과지표 측정값

관점	전략목표	성과목표	성과지표	측정점수('13년)	방향성
정보보호성과	정보보호수준 제고	경제적 효과 달성	정보보호산업 성장률(매출액)	65.5	상향
			피해감소 실적	16.9	하향
		보호능력 제고	침해사고 발생비율	20.43	하향
			관리체계 수립 실적	26.09	상향
	침해사고 방지효과 제고	침해사고 방지활동 강화	해킹 사고/바이러스 신고실적	2.2	하향
			개인정보 침해사고 신고 실적	11	하향

4.1.2 정보보호활동 관점 성과측정 지표

정보보호활동 관점에서는 정보보호를 위한 정보보호 관리체계 활동과 기술적 보호조치 활동을 중심으로 목표를 설정하고 성과지표별 설문조사 결과 내용을 바탕으로 분석한 결과 성과 측정 점수는 <표 13>와 같다.

<표 13> 정보보호활동 관점 성과지표 측정값

관점	전략목표	성과목표	성과지표	측정점수('13년)	방향성
정보보호활동	관리체계 활동 강화	관리체계 확대	정보보호 실적	17.8	상향
			정보자산 안정적 관리실적	37.4	상향
			취약점 진단(장비)실적	8.4	하향
	기술체계 활동 강화	암호보안기술 역량 강화	암호화 통신율	62.5	상향
			암호화 저장율	59.9	상향
		침해사고조치 능력 제고	악성코드 일일점검 실적	91.9	하향
			보안설정적용율	86.5	상향
	이용자 보호수준 제고	피해방지 체계 정비	주민등록번호 수집율	89.3	하향
			주민등록번호 대체수단 이용실적	20.7	상향
		개인정보 체계 강화	공인인증서 사용율	51.3	상향

4.1.3 정보보호정책 관점 성과측정 지표

정보보호정책 관점의 성과지표로는 <표 14>와 같이 정보보호방침 수립실적, 정보보호조직 구성율 등 2개로 구성되어 있다. 정보보호마스터플랜 수립실적은 정보보호방침 수립실적에 포함시켜서 “정보보호방침 수립실적”만 측정하였다.

<표 14> 정보보호정책 관점 성과지표 측정값

관점	전략목표	성과목표	성과지표	측정점수('13년)	방향성
보호정책	정보보호 정책체계 강화	전략계획 수립	정보보호 방침 수립실적	97.3	상향
		조직정책 정립	정보보호 조직구성율	90.3	상향

4.1.3 정보보호투자 관점 성과지표

정보보호투자 관점의 성과지표로는 보안서버 보급률, 보안인력의 확보율, 정보보호 예산투자실적 등 6개로 구성하고 성과 지표에 따는 측정결과는 <표 15>와 같다. 통합보안관리 솔루션 보급실적은 응답자가 없어 제외하였다.

<표 15> 정보보호투자 관점 성과지표 측정값

관점	전략목표	성과목표	성과지표	측정값('13년)	방향성
정보보호투자	정보보호 시스템 구축 확대	정보보호 하드웨어 구축 강화	보안서버 보급율	62.5	상향
		정보보호 소프트웨어 구축 강화	통합보안관리 솔루션 보급실적	-	상향
	정보보안 역량 강화	정보보호 인적역량 강화	정보보호전문 교육실적	16.71	상향
			IT관련 보안인력의 확보율	10.4	상향
		정보보호 투자효과 증대	정부정보보호 예산집행액	43	상향
			정보보호 투자실적	55.4	상향

4.2 성과지표별 측정 산식 및 측정 결과

4.2.1 성과지표별 측정 산식

기존 선행연구의 지표에 따른 측정 방식과 기업정보보호실태조사(KISA, 2013), 국가정보보호백서(KISA, 2014) 등을 기반으로 정보보호 성과측정 지표 정의서에 따라 측정 산식을 다음 <표 16>와 같이 정했다[15,16].

<표 16> 성과지표 측정 산식

관점	성과지표	측정 산식
정보보호성과	정보보호산업 성장률	정보보호산업 성장률 = 정보보호산업 매출액 CAGR/정보통신산업 매출액 CAGR
	피해감소 실적	침해사고로 인한 경제적 피해 경험비율 = (시스템 비정상 작동으로 인한 매출 손실 경험비율+시스템 비정상 작동으로 인한 업무효율 저하 경험비율+침해사고로 인한 피해복구 경험비율+침해사고로 인한 데이터의 영구 손실 피해 경험비율)/4
	침해사고 발생비율	침해사고 발생비율 = 2회 이상 침해사고 경험비율+1회 침해사고 경험비율
	관리체계 구축 실적	정보보호관리체계구축실적 = {(금년 누적 업체수 − 전년 누적 업체수) / 전년 누적 업체수} × 100%
	해킹 바이러스 신고실적	해킹사고/바이러스신고실적 = {(웹·바이러스신고건수 + 해킹신고처리건수) / 전체PC보급대수} × 100%
	개인정보 신고 실적	개인정보 침해사고 신고 실적 = 개인정보침해신고건수 / 인터넷사용인구 × 100%
정보보호활동	관리체계 확대 실적	관리체계 확대 실적 = 대상자 연평균복합성장률(CAGR)
	정보자산의 안정적 관리실적	정보자산의 안정적 관리실적 = (대상설비비율 + 현장검사비율)/2
	취약점 진단 실적	평균취약점 개수의 증가율 = {(금년평균취약점개수 − 전년평균취약점개수) / 전년평균취약점개수} × 100%
	암호화 통신율	암호화통신율 = {모든 또는 일부 사이트에 보안서버를구축한 사업체 / 개인정보수집 사업체중 모르겠다응답 사업체} ×100%
	암호화 저장율	암호화저장율 = {DB보안제품 사용사업체 / DB 사용사업체} × 100%
	악성코드 일일점검 실적	악성코드감염실적 = 국내악성 ⊥ 감염추정PC / 전세계악성 ⊥ 감염추정 × 100% 점수(하향값) = 100% − 악성코드감염실적
	보안설정 (패치) 적용율	보안패치 적용 실시율 = {실시항목응답자수 / 전체설문대상자수} × 100%
	주민등록번호 수집율	주민번호수집율 = {(금년수집 − 전년수집) / 전년수집} ×100% 점수(하향값) = 100% − 주민등록번호수집율
	주민등록번호 대체수단 이용실적	주민등록번호대체수단 이용실적 = (i-PIN서비스 인지비율 + i-PIN서비스이용비율) / 2
	공인인증서 사용율	공인인증서보급률 = {공인인증서이용자수 / 인터넷이용자수} × 100%
보호정책	정보보호방침 수립실적	보호방침 수립 = {(조사이전부터 수립+조사를위해 수립) / 설문대상업체수} ×
	정보보호조직 구성율	보호조직구성율 = {(조사이전부터 구성+조사를위해 구성) / 설문대상업체수} ×
정보보호투자	보안서버 보급율	보안서버 보급률 = {국내 보안서버 판매대수 / 인구수} × 10만
	통합보안관리 솔루션 보급실적	평균 보안관제 설비수 $CAGR = \left\{\left(\frac{\text{현재값}}{\text{기준값}}\right)^{(1/\text{년수})} - 1\right\} \times 100\%$
	정보보호전문 교육시간	정보보호 전문교육 실적 = (금년 인원수 − 전년 인원수) / 전년 인원수 × 100%
	IT관련 보안인력의 확보율	평균정보보호전담조직인원수 = {전담조직인원합계 / 설문응답업체수} 전기대비증가율 = {금년평균인원수 − 전년평균인원수 / 전년평균인원수} ×
	정부 정보보호 예산 집행액	정부정보보호예산비율 = {정보보호관련국가예산 / 보화관련국가예산} × 100%
	민간 정보보호 투자 실적	투자 실적 = 정보보호투자가 있다고 응답한 설문자의 비율(%)

4.2.2 성과지표별 측정 결과

BSC 기반의 정보보호 성과 측정 지표별 측정 방법인 <표 16>과 같은 산식에 따라 측정한 결과 국내 기업의 정보보호 성과는 <표 17>와 같이 나타났다. 이는 방향성에 따라 기업별 측정을 통해 매년 수준에 따라 투자 우선순위 등 의사결정이 가능하다 하겠다.

<표 17> 성과지표별 측정값

관점	전략목표	성과목표	성과지표	측정점수('13년)
정보보호성과	정보보호 수준 제고	경제적 효과 달성	정보보호산업 성장률(매출액)	65.5
			피해감소 실적	16.9
		정보보호 능력 제고	침해사고 발생비율	20.43
			관리체계 구축 실적	26.09
	침해사고 방지 효과 제고	침해사고 방지활동 강화	해킹 사고/바이러스 신고실적	2.2
			개인정보 침해사고 신고 실적	11
정보보호활동	정보보호 관리체계 활동 강화	관리체계 확대	관리체계 확대 실적	17.8
			정보자산의 안정적 관리실적	37.4
			취약점 진단 실적	8.4
	정보보호 기술체계 활동 강화	개인정보 암호보안 기술역량 강화	암호화 통신율	62.5
			암호화 저장율	59.9
		침해사고 조치 능력 제고	악성코드 일일점검 실적	91.9
			보안설정(패치) 적용율	86.5
	이용자 보호수준 제고	개인정보 피해방지 체계정비	주민등록번호 수집율	89.3
			주민등록번호 대체수단 이용실적	20.7
		개인정보 체계강화	공인인증서 사용율	51.3
보호정책	정책체계 강화	전략계획 수립	정보보호방침 수립실적	97.3
		조직정책 정립	정보보호조직 구성율	90.3
정보보호투자	시스템 구축 확대	H/W	보안서버 보급율	62.5
		S/W	통합보안관리 솔루션 보급실적	-
	정보보호 역량 강화	인적역량 강화	전문교육시간	16.71
			IT관련 보안인력의 확보율	10.4
		정보보호 투자효과 증대	정부 정보보호 예산집행액	43
			민간 정보보호 투자 실적	55.4

5. 결 론

본 연구에서는 국가적 측면 보다는 기업측면에서 정보보호 성과측정에 필요한 주요 보안요소를 분석하여, 지속적인 정보보호 수준을 제고하기 위하여 기업의 정보보호 효과분석 지표 및 방법을 개발하였다. 기존 선행연구에서 정보보호의 성과관리지표/지수를 검토하여 정성적, 정량적인 지표를 발굴하고 정보보호 효과분석에 활용하기 위하여 자료수집 및 수용성 등을 고려하여 이해관계조직과 협의를 통한 타당성을 검증한 후 확정된 지표와 방법론을 제시하였다. 또한 개발된 지표 및 효과분석 방법론에 대한 검증을 위해 일반 기업을 대상으로 설문조사를 실시하였다. 설문항목은 이해관계조직의 업무이해 및 인터뷰를 통하여 자료를 수집하거나 내부, 외부전문가의 검토를 통해 대상업체별로 분석한 결과를 이용하여 성과측정을 실시하였다.

정보보호 성과측정을 위한 기존연구자료 및 외부전문가의 자문을 통하여 지표를 발굴하고 정의서를 개발하였으며, 이러한 절차를 통하여 성과측정을 실시하였다. 본 연구를 통해 국내 기업의 정보보호 수준을 파악할 수 있었으며, 정부는 국가의 정보보호 수준을 측정하기 위한 기본 자료로 활용가능하며 정책적 대

책을 개발하는데 활용이 가능하며 기업에서는 자체적으로 측정이 가능하여 기업별 정보보호 수준을 측정하여 매년 정보보호 투자 등 의사결정에 도움이 될 것으로 보인다. 향후 발전 방안은 본 연구가 실제 기업을 상대로 정보보호의 성과를 측정하는 것이 처음이라 지속적인 방법과 목적성을 명확하게 정의하여 지속적으로 분석한다면 의미가 있는 일이다. 조직에서는 이러한 지표와 측정방법을 가지고 정보보호 성과를 분석하여 조직성과와 연계하여 활용해야 한다. 정보보호 활동의 수행성과를 조직내의 부서 또는 개인의 성과와 연계시켜 활용할 수 있도록 제도적인 적용이 필요하다.

본 연구 결과는 국내 기업들의 정보보호 수준을 파악하고 주기적인 성과지표 측정을 통해 자사의 전사적인 정보보호 현황분석/추이분석이 가능하고 추후 정보보호 전략을 수립하는데 적용할 수 있다. 또한 정보보호 추진방향 제시를 통한 전사적 정보보호 수준 제고 및 활성화하고 자사에 적절한 정보보호 척도 수립을 통해 보다 효율적이고 효과적인 정보보호 투자 방안을 제시할 수 있다. 마지막으로 정보보호 중요성 인식 제고 및 기업의 정보보호 촉진과 정보보호 전략 수행을 통하여 기업의 경쟁력 강화를 촉진할 수 있다.

참고문헌

[1] 공희경, “BSC관점에 의한 정보보호 투자효과 분석”, 충북대학교 박사학위논문, 2008.

[2] 공희경, 김태성, “정보보호 투자효과에 대한 연구동향”, 정보보호학회지, 제17권-제4호, pp.12-19, 2007.

[3] 권영옥, 김병도, “정보보호사고와 사고방지 관련 투자가 기업가치에 미치는 영향”, Information System Review, 제9권-제1호, pp.105-120, 2007.

[4] 김정덕, 박정은, “TCO 기반 정보보호 투자수익률(ROSI)에 대한 연구”, 디지털정책학회 창립학술대회, pp.251-261, 2003.

[5] 선한길, “국내기업의 정보보호 정책 및 조직 요인이 정보보호성과에 미치는 영향”, 한국경영정보학회, pp.1087-1095, 2005.

[6] 신일순, “정보보호의 경제학적 의미에 대한 소고”, Information Security Review, 제1권-제1권, pp.27-40, 2005.

[7] 이정훈, 신택수, 임종호, “PLS경로모형을 이용한 IT조직의 BSC성공요인간의 인과관계분석”, 경영정보학회, 제17권-제4호, pp.207-228, 2007.

[8] 정선호, 이영찬, “BSC를 이용한 IT조직의 성과관리체계에 관한 연구”, 한국산업경영시스템학회, pp.49-52, 2005.

[9] 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.

[10] 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.

[11] 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.

[12] NIA, ‘공공부문 정보화 사업평가를 위한 BSC 모형’, 2001.

[13] KISA, ‘국가 정보보호수준 평가지수 산출과 국제화 추진에 관한 연구;, 2006.

[14] KISA, ‘인터넷침해사고 피해액 산출 연구’, 2006.

[15] KISA, ‘기업정보보호실태조사’ 2013.

[16] KISA, ‘2014년 국가정보보호백서’ 2014.

[저 자 소 개]

장 상 수 (Sang-soo Jang)

1989년 2월 한국항공대학교 학사
2003년 2월 동국대학교 석사
2011년 8월 전남대학교 박사
현재 아주대학교 지식정보보안학과
특임교수

email : ssjang0116@gmail.com