개인정보보호투자의 성과측정방안에 관한 연구

김영일[*], 이재훈[**]

A Study on the Measurement Method of Personal Information Protection Investment Performance

Young-Il Kim[*], Jae-hoon Lee[**]

요 약 최근 기업의 개인정보 유출 사고와 관련한 금전적 손실이 점차 증가추세에 있으며 대외 이미지 손실 등의 간접적 피해도 무시 못 할 상황이 되었다. 이 같은 피해를 줄이기 위해서 개인정보보호투자에 대한 필요성이 증대되고 있다. 개인정보보호에 대한 투자가 활성화되기 위해서는 개인정보보호투자의 비용효과 분석 및 정성적 효과분석이 모두 반영된 성과측정 방법이 필요하다. 하지만 현재 국내외 개인정보보호 투자 성과측정에 관한 연구는 매우 미흡한 상황이다. 본 연구에서는 정량적 및 정성적 성과측정이 가능한 개인정보보호투자 모델을 제시하였다. 이를 위해 정보보호투자 및 IT 투자성과측정 관련 기존 연구의 비교분석을 수행하였고, 개인정보보호 특성과 현실적용 가능성 측면을 고려하여 정량적 및 정성적 측정이 모두 가능한 WiBe 접근 방법론을 선택하였다. WiBe 방법론을 기반으로 개인정보보호 투자에 적절한 성과측정 모델과 16개의 성과측정 지표를 제시하였다. 특히, 정량적 효과측정에서 사전위협평가방법을 기반으로 기업 및 조직의 성격에 따른 개인정보보호의 투자의사 결정이 가능한 방법을 제시하였다. 포커스 그룹 인터뷰를 통한 성과 측정 지표의 검토 결과, 성과측정 지표는 실현 가능성 및 중요성 측면에서 모두 의미 있는 것으로 판명되었다.

주제어 : 개인정보보호투자성과측정, 비용효과분석, 경제효율성평가, 정보보호투자성과측정, IT투자성과측정

Abstract Personal information protection has become one of the most impending business issues because leakage of personal information can cause tremendous financial losses and image degradation. Consequently, personal information protection initiatives have been recognized widely in business. To invigorate personal information protection investments, performance measurement method such as cost benefits analysis or qualitative analyses are needed, which have not been studied enough in the previous studies. This study proposes a performance measurement model which can include quantitative and qualitative analyses in the context of personal information protection investments. A comparative analysis has been performed on security investment and IT investment performance measurements, which leads to choose the WiBe method (developed by the German Interior Ministry), considering the privacy characteristics and the method's applicability. In particular, the quantitative effect measured how proactive threat assessment based on the way according to the nature of the businesses and organizations of privacy and possible investment decisions. This study proposes the 16 performance indicators, which turn out to be meaningful in terms of their materiality and feasibility by conducting focus group interviews of 25 experts on personal information protection.

Key Words : Personal information protection investments performance measurement, Cost benefit analysis, WiBe, Information security investments performance measurement, IT investments performance measurement

[*]이 논문은 2012년도 중앙대학교 연구장학기금 지원에 의한 것임
[*]중앙대학교 정보시스템학과 교수
[**]중앙대학교 일반대학원 경영학과 석사과정(교신저자)
논문접수: 2012년 11월 8일, 1차 수정을 거쳐, 심사완료: 2012년 12월 10일

1. 서 론

정보기술(IT) 인프라가 기업의 핵심 인프라로 자리 잡으면서, 기업은 고객에게 다양하고 유용한 서비스 및 재화를 제공하기 위하여 개인정보에 대한 의존도 및 활용도를 높이고 있다[11]. 이와 같은 현상의 역기능 측면에서 최근 기업의 개인정보 유출 사고는 기업에게 금전적 및 대외 이미지에 막대한 손실을 입히고 있다[11]. 이러한 손실로 인해 최고경영층은 개인정보보호투자에 관심을 보이고 있다. 그러나 현재 국내외에서 개인정보보호투자의 성과측정방법에 관한 연구는 매우 미흡한 실정이며[1], 개인정보보호투자 성과측정에 적합한 방법이 부재하여 최고경영층은 개인정보보호를 위해 어디에 얼마나 투자해야하는 지에 관하여 의구심을 가지고 있다. 또한 최근 국내 국가적인 차원에서 '개인정보보호법' 제정 및 한국인터넷진흥원의 '개인정보보호관리체계(PIMS)' 운영 등이 주요 이슈로 부각되고 있다.

따라서 본 연구의 목표는 개인정보보호투자에 적절한 성과측정 모델 제시 및 제시한 모델의 현실적용가능성 검토를 통하여 개인정보보호투자의 최고경영층 관심 유도이다.

2. 문헌연구

2.1 정보보호투자의 성과측정

<표 1>은 정보보호 투자의 비용 및 효과측정 관련 연구에 대한 기존 연구를 표로 재정리 한 것이다. 비용 및 효과 열은 각각을 측정하기 위한 척도라고 할 수 있다[19].

정보보호투자 성과측정에 관한 연구들을 종합해 보면 첫째, 정량적 및 정성적 기준이 혼재되어 있다. 둘째, 각각의 연구자마다 제시하고 있는 비용 및 효과 요소들이 다르다. 이는 투자 의사결정 및 정보보호 개선 방향 도출에 어려움이 있고 정확한 효과성 분석이 주요 이슈임을 시사한다[10]. 따라서 본 논문에서는 기존 정보보호투자 성과측정 연구를 분석하여 개인정보보호투자 성과측정에 적절한 비용 및 효과 지표를 도출하고 이를 정성적 및 정량적 효과분석 모델에 적용할 수 있도록 제안한다.

정보보호투자는 특정 서비스 및 사업단위로 그 범위를 한정하여 성과측정을 하는 것이 가능하다. 그러나 개인정보보호는 취급자와 시스템 등이 사업 부서를 횡단하는 구조로 되어 있어 전사적 관점에서 성과측정을 해야 한다[9]. 따라서 정보보호투자 효과에 관련된 연구만을 참고하여 개인정보보호투자의 성과측정모델을 제시하는 것은 한계가 있다. 개인정보보호투자의 성과측정 모델은 정보보호투자의 성과측정방법과는 달리 전체 사업부서 관점에서 효과를 측정하는 IT 성과측정 방법과 유사하다.

〈표 1〉 정보보호 투자의 비용 및 효과에 관한 연구

연구자	비용	효과
Davis(2005)	통제비용	운영비용 감소
	사고비용	순익 증대
Cavusoglu et al. (2004a, 2004b)	-	금전적 이익
		회사적 책임감소
		신뢰도 증가
Scott(1998, 2002)	-	생산성 증가
		이익 증가
		기업이미지 개선
		금전적 이익
Blakely(2001)	초기 도입 비용	새로운 업무수행 가능 및 손실 예방
	갱신비용	
	관리비용	
Witty(2001)	하드웨어	-
	소프트웨어	
	인적자원	
	외부서비스	
	물리적 보안	
Harris(2001)	제품 구매 비용	업무에 주는 영향
	설계 및 계획수립 비용	
	환경 구축 비용	
	연동 비용	
	유지보수 비용	
	테스트 비용	
	갱신비용	
	운영 및 관리 비용	
Roper(1999)	구매 비용	-
	유지보수 비용	
	관리비용 및 운영 인력비용	
김정덕, 박정은 (2003)	가시적 비용	-
	비가시적 비용	
이종선, 이희조 (2007)	지속적 관리활동	-
선한길(2005)	-	정보보호 사고의 감소
		자산의 손실건수 감소
		비즈니스 기회손실 감소
		타사 경쟁 시 손해 감소
		이미지 실추건수 감소
		사고발생시 신속한 처리

예를 들어, 정보보호관리체계(ISMS)의 인증심사는 특정 서비스 및 사업단위로 그 범위를 한정하는 것이 가능하지만 개인정보보호관리체계(PIMS)는 개인정보 취급자와 개인정보처리시스템 등 조직의 전체 사업 부서를 횡단하는 구조로 이루어진다[9].

다음 절에서는 개인정보보호투자에 대한 적절한 방법을 도출하기 위해 전체 사업부서 관점에서 효과를 측정하는 IT 성과측정 방법에 대하여 고찰한다.

2.2 IT 투자성과측정방법

<표 2>는 IT 성과측정의 5가지 관점이다[6].

〈표 2〉 IT 성과 측정 방법론 비교표

구분		방식	
		정량 분석	정성 분석
전통적	ROI	●	
	NPV	●	
	IRR	●	
	PBP	●	
경제적	TCO	●	
	TEI	●	
	EVS	●	
확률적	ROV	●	
정성적	IPM		●
	IE		●
다중적	BSC	●	●
	TVO	●	●
	VMM	●	●
	WiBe	●	●
	VOI	●	●

출처: [6]

전통적 방식, 경제적 방식, 확률적 접근방식은 주로 경제적인 측면에서의 비용과 편익을 고려하고 있으며, 정성적 가치의 중요성은 간과하고 있다. 이에 비해 다중적 접근방법들은 정량적 방법과 정성적 방법이 갖는 각각의 장점을 취하고 단점을 보완하기 위해 개발된 기법들로, 유형의 성과와 무형의 성과 간에 균형을 취하고 있으며 종합적인 관점의 평가를 가능하게 해주는 장점이 있다[6].

상기 문헌연구에 따른 개인정보보호투자의 성과측정은 전사적 관점에서 이루어져야 한다는 점, 정성적 및 정량적 성과를 종합적으로 측정해야 한다는 점에서 IT성과측정 방법 중 다중적 접근방법을 기반으로 도출하는 것이 적절하다고 판단된다[7][8][9].

IT 성과측정 방법에서 다중적 접근방법들의 시사점을 요약하면 <표 3>과 같다[6].

<표 3>의 시사점에 따라 정량적 분석과 정성적 분석이 모두 가능하다는 점, 성과측정 시 전사적으로 접근이 가능하다는 점, 기업의 투자 규모에 상관없이 성과측정이 가능하다는 점에서 WiBe 접근 방법론이 개인정보보호투자의 성과측정에 대한 적절한 방법이라 판단된다[7][8][9]. 또한, 개인정보보호는 최근 이슈화 되고 있어 투자에 대한 성과측정을 할 경우 데이터가 충분하지 않다는 측면에서 고려했을 때 WiBe 방법론이 개인정보보호투자의 성과측정 성격에 가장 적절하다고 판단된다.

〈표 3〉 다중적 IT 성과측정방법의 시사점

구분	방식	
균현 성과표 (BSC)	장점	· 널리 쓰이고 있는 방법 · 균형잡힌 관점에서 투자의 가치를 평가
	단점	· 하향식(top-down) 방식의 성과측정에 초점 · 단방향의 인과관계만을 표현 · 4 가지 관점이 IT에서도 그대로 적용될 수 있는지에 대해서는 논란이 많음
총기회 가치 (TVO)	장점	· 다각적인 분석과 조직 전체적인 의사소통의 기반을 제공
	단점	· 방법론을 적용하는 데에 많은 노력을 필요로 함
가치 측정 방법 (VMM)	장점	· 평가의 정교함을 제공
	단점	· 불확실성 분석이나 민감도 분석을 위한 노력이 소요 · 규모가 작은 정보화 사업의 평가를 위해서는 적합하지 않을 수 있음
투자 가치 (VOI)	장점	· 비재무적으로 나타나는 효과도 일정의 방법론을 통해 화폐화 가능
	단점	· 실제 화폐적 가치로 나타낸 것과 동일한 가치로 비교하는 것에 문제가 있을 수 있음
경제 효율성 평가 (WiBe)	장점	· 하향식 및 상향식 방식의 성과 측정 방법이 모두 가능하여 전사적으로 접근이 가능 · 기업의 투자의 규모에 상관없이 효과 분석이 가능 · 대규모 데이터 수집 작업이 요구되지 않는다는 조건에서 제시된 절차에 기초한 수행에 적용 방법이 쉽고 용이함

3. 개인정보보호투자의 성과측정 방법

WiBe 방법론은 경제적 효율성과 관련된 모든 변수(판단기준)를 정량적 및 정성적 성격에 따라 4가지 종류(module)로 나누어 측정한다[21]. WiBe 방법론의 주요내용은 아래와 같다.

1) 금전적 의미의 경제성(수익성)
- 정보시스템의 개발 및 운영과 관련하여 화폐단위로 계량화될 수 있는 모든 비용과 요소를 정의하고 그 값을 측정

2) 정보화사업의 긴급성
- 기존 시스템 교체의 긴급성 또는 규정 및 법률준수 효과를 측정

3) 정보화사업의 전략적 중요성
- 직무의 품질 향상 등 금전적으로 계량화하기는 어려우나 전략적으로 그 중요다가 높은 질적 효과를 측정

4) 정보화사업의 대/내외 이미지 개선효과
- 시민, 기업, 기타 행정기관 등 대/내외 고객에 미치는 효과를 측정

3.1 정량적 측정 방법

WiBe 방법론의 첫 번째 항목인 “금전적 의미의 경제성(수익성)”을 측정하기 위해서 Shawn A. Butler(2003)가 제시한 보안속성평가 방법(SAEM: Security Attribute Evaluation Method)을 활용하였다.

SAEM의 단계를 요약하면 아래와 같다[24].

1) 기업의 보안담당자로부터 사전 인터뷰를 통한 위협의 빈도와 피해 측정하는 단계
2) 기업의 상황에 따른 각 위협의 가중치를 정하는 단계
3) 위협 인덱스(TI, Threat Index)를 측정하는 단계
4) 기업의 개인정보호호담당자 인터뷰를 통하여 각 위협에 대응하는 개인정보보호 기술의 효과성을 측정하는 단계

위 단계를 수행 후에 ROPI(Return on Personal information Investment)를 사용하여 개인정보보호 투자 시의 정량적 효과를 측정할 수 있다.

개인정보보호투자 성과측정 성격을 고려하여 SAEM 단계를 적용하면 다음과 같다.

<표 4>는 개인정보보호 투자 효과를 측정하기 위한 첫 번째 단계인 사전위협평가의 예시이다.

<표 4>는 유진호(2009)의 연구에서 제시한 개인정보 사고에 따른 위협 및 피해를 재구성하여 SAEM에 적용한 것이다. 사전위협평가는 개인정보보호 담당자의 사전 인터뷰에 따라 각 위협 속성의 최소, 중간, 최대값을 결정한다. 예를 들어, 주소정보침해 사고가 발생했을 경우 사고공지 비용의 최소(0원), 중간(0원), 최대값(50만원)을 도출할 수 있다.

〈표 4〉 위협 빈도와 위협에 따른 피해

위협 (년별 공격 빈도/년)		사고공지 비용 (만원)	자문 비용 (만원)	콜센터운용 비용 (만원)	보상서비스제공 비용 (만원)	생산성손실 (만원)
주소 정보 침해 (20/년)	최대	50	20	30	100	300
	중간	0	0	0	40	160
	최소	0	0	0	10	30
ID 정보 침해 (40/년)	최대	100	20	60	200	600
	중간	0	0	0	110	320
	최소	0	0	0	30	60
금융 정보 침해 (10/년)	최대	25	20	15	50	150
	중간	0	0	0	20	80
	최소	0	0	0	5	15
민감성 정보 침해 (5/년)	최대	12.5	20	7.5	25	75
	중간	0	0	0	10	40
	최소	0	0	0	2.5	7.5

출처: [24]

두 번째 단계는 기업의 상황에 따라 각 위협의 속성별 가중치를 정하는 것이다. 기업의 보안 담당자들은 속성별 중요도에 따라 1~100점을 줄 수 있고, 이를 표준화하여 가중치로 나타내면 <표 5>와 같이 나타낼 수 있다. 표준화한 가중치의 합은 1이 된다.

〈표 5〉 속성 별 중요도 및 가중치

속성	중요도	가중치(W)
사고공지 비용	100	.33
자문 비용	80	.27
콜센터운용 비용	60	.2
보상서비스제공 비용	40	.13
생산성손실 비용	20	.07

세 번째는 <표 4> 및 <표 5>의 각 값을 기반으로 위협인덱스(TI, Threat Index)를 산출하는 단계이다. 세 번째 단계의 수식은 식(1)와 같이 나타낼 수 있다.

$$TI_{속성} = Freq_{속성} \times [p_{최소} \times (\Sigma_{j=속성} W_j \times x_{j\,최소}) + p_{중간} \times (\Sigma_{j=속성} W_j \times x_{j\,중간}) + p_{최대} \times (\Sigma_{j=속성} W_j \times x_{j\,최대})] \quad (1)$$

위 식에서 $Freq_i$는 <표 4>에서 각 위협별 빈도수, p_i는 각 위협의 최소, 중간, 최대값이 발생할 확률이다. 다음으로 W_j는 각 위협속성비용의 가중치, x_{ji}는 위협의 최소, 중간, 최대값의 비용이다. 이에 따라 각 위협 속성을 기반으로 (Threat Index)를 산출할 수 있다. <표 6>은 사전위협평가의 최종 결과의 예시이다.

〈표 6〉 사전 위협 평가 결과

$Freq_{측정} \times P_{최소/중간/최대} \times \sum(W_j \times x_{j최소/중간/최대})$				위협인덱스
위협	최소 $P_{최소}=.1$	중간 $P_{중간}=.89$	최대 $P_{최대}=.01$	(Threat Index)
주소정보침해	12.38	291.92	6.80	311.1
ID정보침해	47.36	1306.52	32.40	1,386.28
금융정보침해	3.37	72.98	1.70	78.05
민감성정보침해	0.98	18.25	0.43	19.66
총합	64.09	1,689.67	41.34	1,795.1

다음 네 번째는 기업의 개인정보호호담당자 인터뷰를 통하여 각 위협에 대응하는 개인정보보호 기술의 효과성을 측정하는 단계이다. 남기효(2008)가 제시한 개인정보보호기술을 적용하면, <표 7>과 같이 나타낼 수 있다. <표 7>은 기업의 개인정보보호담당자로부터 평가된 위험을 완화 시킬 수 있는 개인정보보호기술의 효과성의 예시이다. 두 개 이상의 보호기술을 조합할 경우의 효과성도 측정이 가능하다.

〈표 7〉 효과성 평가

위협 / 기술	사고공지 비용	법률/포렌식 자문비용	운영비용 콜센터	보상서비스 제공비용	손실비용 생산성
프라이버시보호 진단 기술	66%		40%	33%	40%
프라이버시노출 관리 기술	30%		40%	33%	30%
개인정보보호 통신 기술	45%		40%		32%
개인정보보호 저장 기술				10%	24%
개인정보보호 정책 기술	25%	30%			27%
개인정보보호정책 관리 기술	27%	30%			34%

마지막으로 ROPI는 다음 (2)식으로 나타낼 수 있다.

$$ROPI = \frac{Benefits - Cost\ of\ Investment}{Cost\ of\ Investment} \quad (2)$$

Shawn A. Butler(2003)가 제시한 연구에 따라 위의 식의 Benefits에 ALE(Annual Loss Expectancy)의 개념을 적용하면 Benefits은 다음 (3)의 식과 같이 나타낼 수 있다.

$$Benefits = ALE_{without\ investment} - ALE_{with\ investment} \quad (3)$$

SLE(Single Loss Exposure), AV(Asset Value), EF(Exposure Factor), ARO(Annual Rate of Occurrence)라 하면, 다음의 식 (4), (5)로부터 ALE를 도출 할 수 있다[24].

$$SLE = AV \times EF \quad (4)$$

$$ALE = SLE \times ARO \quad (5)$$

<표 8>은 기존 문헌연구의 중복성을 최소화하여 범주화한 개인정보보호투자의 상호배타적인 비용 항목이다. 아래의 측정항목을 위 식(2)에 대입하면 최종적으로 ROPI를 구할 수 있다.

〈표 8〉 개인정보보호 투자에 따른 비용

측정항목	비고
개인정보보호 서비스비용	개인정보자산 서비스 운영 비용 및 컨설팅을 통한 취약진단 자문비용 [12][18][25]
개인정보자산 보호 솔루션 비용	개인정보자산 보호 솔루션 도입 및 유지보수 비용 [12][18][22][25]
유지보수 비용	개인정보보호 투자의 향후 지속적 관리 비용 [5][12][19][22]

3.2 정성적 측정방법

다음으로 WiBe방법론의 정보화사업의 긴급성, 정보화사업의 전략적 중요성 및 대/내외 이미지 개선 효과를 개인정보보호 투자의 경우로 적용하면 1) 긴급성/준거성 2) 전략적 중요성 3) 대/내외 효과로 적용할 수 있다. WiBe를 적용한 세 가지 항목은 다음 <표 9>와 같다. 도출된 각 영역은 정보보호투자의 성과측정에 관한 연구를 기반으로 하였다[3][5][12][13][16][22][23][25].

〈표 9〉 개인정보보호 투자에 따른 정성적 효과

정성적 효과	영역	측정항목
긴급성/준거성	고객정보에 대한 사회적 책임 강화	국내법률 준수
		국외개인정보지침 준수
대/내외 효과	고객만족도 제고효과	고객신뢰도 증진
		기업의 브랜드 이미지 제고
		고객 이탈 방지 효과
		고객 및 파트너사와의 협력관계 강화
		고객거래정보의 안전한 관리 및 활동 강화
전략적 중요성	업무효율성 증진효과	정형화된 업무처리를 통한 효율성 개선
		사고(업무) 대응처리 간소화
		개인정보자산 보호 인식 제고
		개인정보자산 보호 인식 제고
		개인정보자산 보호 인력 감소
		개인정보보호 대책의 유지 관리 증진
	기업경영 개선	신규 서비스 창출
		부가 서비스 창출

4. 연구방법검토

현재 국내외 조직에서 다중적 접근방법을 이용한 개인정보보호 투자의 성과에 관한 연구가 매우 미흡한 실정이므로 본 연구에서 제시한 효과 분석 모델의 타당성을 객관적으로 검증하는 것은 어려운 문제이다. 이에 따라 본 논문에서는 정보보호 분야의 전문가들로 구성된 포커스 그룹을 대상으로 설문과 심층 면접을 수행하였다.

4.1 검토방법

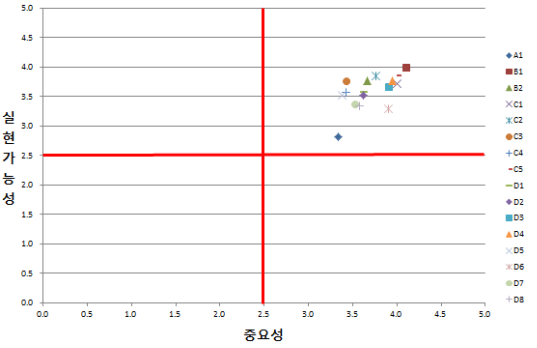
Sork(1982)은 우선순위 결정을 위해 5가지의 중요도 평가 기준과 3가지의 실행 가능성 평가기준에 따른 개별 선호도를 평가하고, 각각의 평가 점수들을 합산하여 선호도의 우선순위를 결정하는 집합적 의사결정(Aggregated Decision) 방법을 제시하였다[24].

Ozdemir, Miu(2009)는 기업 거버넌스 도입을 위해 제시된 바젤Ⅱ의 구현에 대해 연구하였는데, 바젤Ⅱ를 성공적으로 구현하기 위해 필요한 사항들을 중요성과 실행 가능성 기준으로 평가하여 우선순위를 결정하였다[14].

본 연구에서는 선행연구가 매우 미흡하고 객관성을 확보하기 위한 데이터가 매우 부족한 측면에서 Cabrera et. al.(2008)의 중요성과 실현 가능성을 검증 항목으로 사용하여 개인정보보호투자 성과측정 모델의 적정성을 판단하였다. 중요성 및 실현 가능성이 2.5 이하인 구성 요소는 성과측정 모델의 구성요소로서 부적합한 것으로 판단하였다.

4.2 검토결과

본 논문에서는 정성적 연구방법의 하나인 포커스 그룹 인터뷰를 사용하였다. 포커스 그룹 인터뷰를 수행하기 위해 연구소 및 개인정보보호 분야의 전문가 25명이 참여한 포커스 그룹을 구성하여 설문과 심층 면접을 수행하였다. 설문은 도출한 개인정보보호 성과측정 모델에서 정량적 및 정성적 성과측정 지표의 중요성과 실현 가능성을 측정하기 위해 리커드 5점 척도를 사용하였으며, 도출한 지표 이외에 추가적으로 필요한 요소나 개선사항에 대하여 작성하도록 하였다.포커스 그룹의 인터뷰 결과는 다음 [그림1] 및 <표 10>와 같다.



[그림 1] 포커스 그룹 인터뷰 결과

〈표 10〉 포커스 그룹 인터뷰 결과

개인정보보호 투자의 성과측정방법 구성요소	No	중요성	실현 가능성
ROPI	A1	3.3	2.8
국내법률 준수	B1	4.1	4.0
국외개인정보보호지침 준수	B2	3.7	3.8
고객신뢰도 증진	C1	4.0	3.7
기업 브랜드 이미지 제고	C2	3.8	3.9
고객 이탈 방지 효과	C3	3.4	3.8
고객 및 파트너사와의 협력 관계 강화	C4	3.4	3.6
고객거래정보의 안전한 관리	C5	4.0	3.9
정형화된 업무처리를 통한 효율성 개선	D1	3.6	3.6
사고(업무) 대응처리 간소화	D2	3.6	3.5
개인정보자산 보호 역량 강화	D3	3.9	3.7
개인정보자산 보호 인식 제고	D4	4.0	3.8
개인정보자산 보호 인력 감소	D5	3.4	3.5
개인정보보호 대책의 유지관리 증진	D6	3.9	3.3
신규서비스창출(기업측면)	D7	3.5	3.4
부가서비스창출(산업측면)	D8	3.6	3.3
평균		3.70	3.60

포커스 그룹 인터뷰 결과를 종합해보면, 개인정보보호 투자의 성과측정을 위한 지표들은 모두 채택 가능한 것으로 평가되었다. 그러나 중요성과 실현가능성의 평균은 각각 3.7점/5점, 3.6점/5점으로 높지 않은 결과를 나타내고 있다. 구체적으로 먼저, 정량적 부분의 금전적 의미의 경제성(수익성) 측면을 살펴보면, 중요성에 비해 실현가능성이 상대적으로 낮은 점수를 나타내고 있다. 이는 정량적 척도의 실현가능성 제고에 기여할 수 있는 추가적인 연구가 필요하다는 것을 시사한다.

다음으로 정성적 부분, 긴급성/준거성 영역의 고객정보에 대한 사회적 책임 강화 항목은 중요성 및 실현가능성이 공통적으로 높은 수준을 나타내고 있다. 이는 개인정보보호 투자의 성과측정을 할 때 국/내외 법률 준수가 핵심적인 항목임을 확인할 수 있는 결과이다.

그리고 대/내외 이미지효과 영역의 인터뷰 결과는 고

객만족도 제고 효과를 측정 할 경우 고객 신뢰도 증진 및 고객거래정보의 안전한 관리를 우선적으로 고려하여 측정해야 한다는 것을 보여준다.

마지막으로 전략적 중요성 영역의 업무 효율성 증진효과 항목을 측정할 경우 조직 내부 개인정보자산 보호 역량 강화 및 인식제고가 핵심사항임을 나타낸다. 또한, 기업경영개선 항목의 점수가 상대적으로 낮음을 확인할 수 있는데 이는 기업경영개선 항목에 중요성 및 실현가능성에 기여할 추가적인 연구가 필요하다는 것을 시사한다.

5. 결 론

본 연구에서는 단기적이고 유형적인 목표로 제시되는 비용 절감 관점 및 장기적, 무형적, 잠재적으로 나타날 수 있는 다양한 편익까지 포괄적으로 고려하는 관점을 정보보호투자의 효과측정 과 IT성과측정방법의 두 가지 측면에서 고찰하였다. 이를 기반으로 WiBe 방법론의 4가지 관점에서 개인정보보호투자 성과측정모델을 제시하였다.

또한, 기존 문헌연구의 혼재된 정량적과 정성적 효과 관점을 재분류 하여 효과측정방법을 둘러싼 오류와 혼란을 최소화 하였으며 특히, 정량적 효과측정에서 사전위협 평가방법을 기반으로 기업 및 조직의 성격에 따른 개인정보보호의 투자의사 결정이 가능한 방법을 제시하였다.

본 연구에서 제시한 개인정보보호투자 성과측정모델은 특정 투자 성과측정방법론이나 기법에 고착되지 않는 포괄적 방안으로서, 조직은 이러한 방법을 토대로 스스로 개인정보보호투자 성과측정을 점검, 조명, 설계, 추진할 수 있을 것으로 기대된다.

본 연구의 한계로는 개인정보보호 투자 성과측정 방법의 검증을 들 수 있다. 이러한 검증 결과는 객관성 확보 및 일반화가 어렵다는 한계점을 가지고 있다. 따라서 향후의 연구에서는 본 논문의 방법을 실제 기업에 적용한 사례 연구를 수행하여 본 방법을 진화시키는 연구가 필요할 것으로 판단된다.

참 고 문 헌

[1] 김정덕・박정은(2003), TCO 기반 정보보호 투자수익률 (ROSI)에 대한 연구, 한국디지털정책학회 창립학술대회, pp251-261.

[2] 남기효・박상중・강형석・남기환・김성인(2008), 개인정보보호기술의 최신 동향과 향후 전망, 한국정보보호학회 학회지, 제18권 제6호.

[3] 선한길(2005), 국내기업의 정보보호 정책 및 조직 요인이 정보보호성에 미치는 영향, 한국경영정보학회 춘계학술대회, pp.1087-1095.

[4] 유진호・지상호・임종인(2009), 개인정보 유・노출 사고로 인한 기업의 손실비용 추정, 한국정보보호학회 논문지, 제19권 제4호.

[5] 이종선・이희조(2007), TCO기반 Security ROI를 활용한 정보보호 투자성과 평가방법, 한국정보처리학회 춘계학술대회, pp.1125-1128.

[6] 정보화진흥원(2008), IT성과측정방법론..

[7] 채승완(2008), 개인정보보호의 경제적 효과, 소비자문제연구, 제33호.

[8] 한국인터넷진흥원(2007), 가상가치접근법(CVM)을 활용한 개인정보보호의 가치 산출 방법론 고찰.

[9] 한국인터넷진흥원(2007), 개인정보보호와 i-PIN.

[10] 한국인터넷진흥원(2010), 정보보호 사전점검 제고 활성화에 관한 연구.

[11] 황수하・김정덕(2011), 개인정보보호 거버넌스의 효과적인 구현을 위한 핵심성공요인에 관한 연구, 한국정보보호학회 논문지, 제21권 제5호.

[12] Blakley, B.(2001), Returns on Security Investment: an Imprecise but Necessary Calculation, Secure Business Quarterly, Vol.1, No.2.

[13] Blatchford, C.(1995), Information Security Controls -Are They Cost-effective, Computer Audit Journal, Vol.3, pp.11-19.

[14] Bogie Ozdemir & Peter Miu(2009). Basel II Implementation: A Guide to Developing and Validating a Compliant, Internal Risk Rating System. McGRAW-HILL.

[15] Cavusoglu, H.(Hasan), Cavusoglu, H.(Huseyin) and Raghunathan S.(2004), Economics of IT Security Management: Four Improvements to Current Security Practices, Communications of the Association for Information System, Vol.14, pp.65-75.

[16] Cavusoglu, H., Mishra, B. and Raghunathan, S.(2004), A Model for Evaluating IT Security Investments, Communications of the ACM, Vol.47, No.7, pp.87-92.

[17] Davis, A.(2005), Return on Security Investment

-Proving It's Worth It, Network Security, Vol.2, pp.8 - 10.

[18] Harris, S.(2001), CISSP All-in-One Exam Guide, McGraw-Hill.

[19] Hee-kyung Kong, Tae-Sung Kim and Jungduk Kim(2012), An analysis on effects of information security investments: a BSC perspective, Journal of Intelligent Manufacturing, Vol.23, pp.941-953.

[20] Lee, Vincent C.S(2003)., A Fuzzy Multi-criteria Decision Model for Information System Security Investment, Lecture Notes in Computer Science, Vol.2690, pp.436 - 441.

[21] Peter Röthig(2004), WiBe 4.0 Recommendations on Economic Efficiency Assessments in the German Federal Administration, in Particular with Regard to the Use of Information Technology Version 4.0, KBSt.

[22] Roper, C.A.(2004), Risk Management for Security Professionals, Butterworth-Heinemann, Boston, MA, 1999.ns of the ACM, Vol.47, No.7, pp.87-92.

[23] Scott, D.(2002), Best Practices and Trends in Business Continuity Planning, U.S. Symposium/ ITxpo, Orlando, FL.

[24] Shawn A. Butler(2003), Security Attribute Evaluation Method, School of Computer Science Carnegie Mellon University, Pittsburgh, PA 15213, PhD.

[24] Sork, T. J(1982). Determining Priorities, Vancouver, Canada, University of British Columbia.

[25] Witty, R.J, Girard, J., Graff, J.W., Hallawell, A., Hildreth, B., MacDonald, N., Malik, W.J., Pescatore, J., Reynolds, M., Russell, K., Wheatman, V., Dubiel, J.P., and Weintraub, A.(2001), The Price of Information Security, Gartner Inc., Stamford, CT.

김 영 일

- 1975년 2월: 서울대학교 고고인류학과(문학사)
- 1981년 6월: 미국 인디아나대학교 경영학과(경영학석사)
- 1987년 10월: 미국 미네소타대학교 경영학과(경영학박사)
- 1989년 3월~현재: 중앙대학교 경영학부 교수
- 관심분야: 정보화 정책, IS 및 e-Biz, 계량 및 응용통계
- E-Mail: yik01@cau.ac.kr

이 재 훈

- 2011년 2월: 중앙대학교 정보시스템학과(정보학사)
- 2011년 3월~현재 : 중앙대학교 일반대학원 경영학과 재학중
- 관심분야: 개인정보보호, 개인정보보호 거버넌스, 정보화 정책
- E-Mail: secejhlee@gmail.com