http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.20, No.2, May 2015, pp.93-106
http://dx.doi.org/10.7838/jsebs.2015.20.2.093

투자결정 모델을 활용한 개인정보유출의 기대손실 분석

Analysis of Loss Expectancy on Personal Information leakage using Quantitative Invest Decision Model

김정연(Jeong Yeon Kim)*

초 록

전자상거래의 성립을 위해 온라인 정보시스템 상에서 거래 당사자의 정보를 제공하는 것은 필수적이다. 거래의 간편성을 위해 서비스 제공 기업이 이를 보관하고 개인정보와 거래 정보를 가공하여 추가 서비스를 제공하는 것이 전자상거래 분야에서 일반화 되고 있다. 그러나 해당 정보의 임의적 보관은 거래의 간편화에 도움이 되는 반면 외부 유출로 인해 직접적 혹은 간접적 피해가 발생할 수 있는 가능성을 높인다.

본 연구는 시스템 운영 기업의 측면에서 정보유출 사고발생의 위험률과 이로 인해 발생할 수 있는 기대 손실을 분석하기 위해 정보보호 관리체계로 대표되는 정성적 정보보호 관리 방식과 더불어 대표적인 정량적 분석 방법인 개인정보에 대한 수요공급 곡선과 Gordon and Loeb 모델을 소개한다. 또한 한국인터넷진흥원에서 실시한 개인정보보호 수준 실태조사 결과 중 개인정보 누출사고가 있었던 조사 대상 사업자의 분포가 핵심사업분야나 기업규모에 따라 큰 편차를 나타내는 원인을 제시하였다. 이를 통해 징벌적 손해배상으로 유출사고로 인한 기업의 금전적 손실이 일정 수준을 유지하는 것과 법률로 요구하는 개인정보보호 기준을 최상위 등급으로 유지하는 것이 기업간 개인정보 취약점의 편차를 보완할 수 있는 방법으로 제시된다.

ABSTRACT

Providing trading partners with personal information to establish an e-commerce financial transaction is inevitable. Most e-commerce companies keep personal information and transaction data for user's convenience and develop additional services as their applications. However, keeping personal information increases the likelihood of identity theft causing direct or indirect damage while it may simplify repetitive financial transactions.

This study introduces risk management methods based on quantitative and qualitative analysis including demand-supply curve model and Gordon & Loeb model to analyze the risks for security management. The empirical analysis with survey results from KISA (Korea Information Security Agency) shows that the root cause of different statistics of personal information leakage incidents according to core business of internet companies is the difference in their Loss Expectancy caused by them. Also we suggest disciplinary compensation and higher standard for personal information protection as a solution to prevent the variation of investment on it between individual companies.

키워드 : 전자상거래, 정보유출, 개인정보보호, 정량적, 수요공급 곡선, 징벌적 손해배상
e-commerce, Identity Theft, Personal Information Protection, Quantitative, Demand-Supply Curve, Gordon & Loeb Model, Disciplinary Compensation

본 연구는 2014년도 상명대학교 교내연구비를 지원받아 수행하였음.

* Collage of Business Administration, Sangmyung University(jykim@smu.ac.kr)

Received: 2015-04-29, Review completed: 2015-05-18, Accepted: 2015-05-20

1. 서 론

최근 빠르게 전개되고 있는 정보사회로의 전환은 기존의 무형자산으로서의 정보 개념과 함께 개인정보와 같은 새로운 정보군의 보안 관리의 필요성을 부각시켰다. 정보 자체의 가치뿐만 아니라 정보유출 시 간접적인 피해나 기업에 미치는 부정적 효과가 새롭게 부각되었기 때문이다. 기업의 정보보호는 위험 관리 요소의 중요항목으로 관심수준이 높아졌으며, 정보보호를 위한 체계적인 투자의 필요성이 대두되고 있다[1].

기업의 관리자는 정보보호의 목적을 달성하고 효율적인 정보보호가 이루어 질 수 있도록 투자의 우선 순위를 결정하고 보안 투자의 결과와 그 성과를 측정하기 위한 기준을 필요로 한다. 이는 정보보호의 당위성과 더불어 비용 대비 효과라는 기업 경영의 관점에서 제기되는 문제이며 새로운 보안 기술의 개발, 보안 기술의 비교 및 선택, 사내 보안 정책의 적용 등 등 기업 정보보호 활동 전반의 분야에서 투자 결정의 합리적 판단 근거로서 활용 가치를 지닌다[7, 14].

그러나 정보보안 투자결정의 주체로서 관리자가 다양한 요구사항을 가진 반면 정보보호 투자 판단의 근거로 제시할 수 있는 객관적인 자료와 지표에 대해서는 여전히 논란 중에 있다. 근본적으로는 투자의 선행 요건 중 하나인 정보의 가치에 대한 합의가 이루어지지 않고 있기 때문이다. 무형자산의 하나로 인정되는 산업기술이나 디자인 등의 디지털 정보에 대해서도 해당 정보의 미래 가치를 어떻게 측정하는가의 문제는 논란 중에 있다. 더구나 전자상거래, 전자 금융 부분에서 빈번히 사용되는 개인정보 및 거래 정보 등과 같이 개별 정보의 활용 가치가 미미한 경우에는 해당 정보의 유출로 인한 간접적 손실 측면에서만 가치를 인정받고 있다. 그렇지만 실제 정보유출 발생 시에는 해당 가치의 정량적 분석 결과에 대해 당사자들간의 합의를 이끌어 내지 못하고 있는 상황이다.

또한 정보의 가치에 대한 인식이 변화하고 있음에도 불구하고 기업들의 실제 정보보안 투자 현황은 크게 변화가 없다는 점에서도 그 차이를 확인한 수 있다. 정보 예산의 일부를 정보보호에 투자한 사업체는 점차 늘어나고 있지만 IT 예산 중 5% 이상을 정보보호 관련 분야에 지출한 사업체는 소수에 불과하다[13].

더구나 정보보호를 위한 투자의 범위가 넓고 투자 편익의 정량화가 어렵다는 점은 가치 판단의 어려움과 더불어 정보, 특히 개인정보 보호 투자에 대한 결정을 더욱 어렵게 한다. 이는 기업의 정보보호 취약성 관련 변수를 다양한 활동 분야에서 선정하고 정보보안 사고 처리 경과 비교를 통해 관련 변수들의 측정 과정을 표준화하는 것이 여전히 과제로 남아 있다는 사실에 기반한다.

이와 같은 어려움 때문에 정보보호에 대한 투자 연구는 정량적 측정보다는 정성적 측정 방법이 주로 제시된다. 성과측정 기록표(score card) 방식을 활용하면 정보보호에 필요한 표준 항목을 제시하고 관리자가 항목별 투자 우선 순위를 살필 수 있다. 이와 같은 방식은 계량화한 투자 효용 판단에 비하여 정보보호 목적에 보다 적합한 투자 우선 순위를 제시하는 장점이 있는 반면 투자 대비 효율 비교라는 측면에서는 제한된 정보만을 제공하는 단점을 가진다.

본 논문은 정보보안에 대한 투자와 편익의

상관관계를 정량적으로 분석하는 방법을 소개한다. 또한 한국인터넷진흥원의 개인정보보호 수준 실태조사 결과를 바탕으로 정보통신망법 적용 대상 사업자를 대상으로 개인정보유출 잠정 위험율을 유추하고 기업의 핵심사업 분야에 따라 개인정보유출 사고발생 빈도가 달라지는 원인을 정보보호 투자의 편익에 대한 인식 차이로 설명하고자 한다.

더불어 이와 같은 정량적 분석 사례를 통해 정보 산업군에 따라 나타날 수 있는 개인정보보호에 대한 인식의 차이를 비교하고 이를 바탕으로 효율적인 정보보호 투자를 위해 정성적 지표를 보완할 수 있는 추가 정보를 제공하고자 한다. 이는 개별 기업이 투자 우선 순위를 정하더라도 개별 투자의 효율성이 개인정보보호의 합목적성에 따라 올바른 방향으로 제고될 수 있도록 유도하기 위한 정책적 고려 사항으로 활용될 수 있을 것으로 기대한다.

2. 정보보호 투자의 이론적 배경

이론적으로 정보보호 활동은 정보의 비밀성(confidentiality), 가용성(availability), 무결성(integrity)을 유지하기 위한 노력을 의미한다. 외부와의 공유를 차단하고 정보의 기밀을 유지하는 것뿐 아니라 정보가 필요한 시점에 이를 사용자가 이용할 수 있도록 제공하고 내용 변조를 방지하여 기존 데이터와의 일관성을 유지하는 것을 목표로 한다. 이는 기업 정보시스템에서의 정보보호는 내부의 정보를 허가된 사람에게 허가된 작업만을 허용하는 것뿐 아니라 정보시스템의 가용성 및 정보의 일관성이 유지되기 위한 보다 포괄적인 관리를 의미한다. 정보보호를 통해 얻을 수 있는 편익 역시 보호하고 있는 정보의 가치와 더불어 정보시스템을 활용함으로써 얻게 되는 생산성 향상 등과 같은 간접적 가치, 정보유출로 인해 발생할 수 있는 법적 책임이나 기업 이미지 하락 등의 잠재적 비용 등을 모두 포함하는 개념으로 확장된다.

일반적으로 기업이 정보유출 혹은 정보시스템 침해로 인하여 발생하는 피해는 유출된 정보의 가치 손상을 포함한 직접적 손실 비용과 업무 정상화나 향후 예방조치를 취하기 위한 비용 등의 간접적 손실로 구분할 수 있다. 선행연구는 데이터 손실 시 복구에 필요한 인건비, 소모된 시간, 시스템 사용 불가로 인한 생산성 저하, 복구 불가능한 데이터의 가치 등을 간접적 비용으로 구분하였다[2]. 더불어 정보 손실 및 매출 변화, 시스템 복구에 필요한 추가 비용 등의 명시적 비용과 함께 법적 책임과 이미지 손상과 같은 잠재적 비용으로도 구분할 수 있다[9].

2.1 개인정보의 정의

정보시스템에 대한 보호 관리가 대부분 개별 기업의 무형자산 보호를 위한 자발적 투자에 의존하고 있는 반면 온라인 상에서 개별 사용자의 신분을 확인할 수 있는 개인정보의 경우는 국가적 차원에서 일정 수준의 정보보호 활동을 의무화하고 있다. 제 3자가 해당 정보를 이용하여 금융거래 등에 사용하는 간접적 피해 사례를 막기 위한 조치이다.

국내의 경우에는 1995년 1월부터 개인정보보호법을 시행하고 있다. 보호 대상인 개인정보는 주민등록, 신원조회, 병역사항 및 각종 납

세자료 등 개인의 신상에 관한 모든 정보이다. 관련한 개인정보를 다루는 기업은 취득, 이용 목적을 명확히 공표 또는 통지할 의무를 가지며, 고객으로부터 정보 개시나 이용 정지 요구를 접수하는 창구를 설치하는 등 엄중한 안전관리를 규정하고 있다.

국내의 개인정보의 개념은 적용분야가 공공행정부문과 정보통신부문으로 한정되며 공공기관의 개인정보보호에 관한 법률 혹은 정보통신망 이용 촉진 및 보호 등에 관한 법률 등을 통해 구체적으로 규정되어 있다. 해당 규정에 따르면 개인정보란 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명, 주민등록번호 및 화상 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보 혹은 당해 개인을 알아볼 수 있는 부호, 문자, 음성, 음향 및 영상 등의 정보를 포함한다.

2.2 개인정보의 보호 규정

전자상거래 기업의 경우에도 온라인 상에서의 금융거래의 성립을 위해 거래 당사자의 정보를 취득하는 것은 필수적이다. 그러나 해당 정보의 임의적 보관은 거래의 간편화에 도움이 되는 반면 외부 유출로 인해 직접적 혹은 간접적 피해가 발생할 수 있는 가능성을 높인다.

이와 같은 피해를 줄이기 위해 개인정보 수탁자는 개인정보 처리자로부터 개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그밖에 이와 유사한 행위 등의 업무를 위탁 받아 처리할 때 개인정보보호법을 준용, 개인정보의 안전성 확보에 필요한 의무를 모두 시행해야 한다. 이의 구체적인 실천 의무 방안을 규정하기 위해 행정안전부가 제정, 고시한 '개인정보 안전성 확보조치 기준'은 크게 기술적 조치와 관리적 조치로 나뉜다. 관리적 조치사항은 내부관리계획 수립과 개인정보보호 책임자의 지정 등의 정책적 준수 사항이 포함되어 있으며 기술적인 조치 사항은 접근통제 시스템 운영, 개인정보 암호화, DB암호화, 악성프로그램 예방 프로그램 이용 등의 내용을 담고 있다.

2.3 정성적 투자결정 모델

국내의 가장 대표적인 정보보호 대책은 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조 '정보보호 관리체계 인증' 규정에 의한 정보보호 관리체계이다. 해당 규정은 연간 매출액 또는 이용자 수 등 법적 기준에 부합하는 정보통신서비스 제공자에 한하여 관련 정보보호 관리체계를 도입하고 이를 외부의 인증인증기관부터 검증을 받도록 의무화하였다.

정보보호 관리체계는 정보보호 절차와 과정을 체계적으로 수립하고 지속적으로 관리, 운영하는 과정을 5항목의 정보보호 관리과정 및 13항목의 정보보호 대책과 통제항목으로 구성한다[12]. 제시된 통제항목과 세부점검항목을 표준으로 각 조직에서는 정보보호관리에 필요한 통제항목을 선택하고 제시된 보안 요구사항에 맞게 관리체계를 구성할 수 있다.

<Table 1>은 개정된 정보통신망법에 따라 경영진의 책임 강화 등의 신규 항목과 기존 항목의 통합 혹은 삭제를 거쳐 104개 통제 항목 및 253개의 세부점검항목으로 구성된 내용을 보여주고 있다.

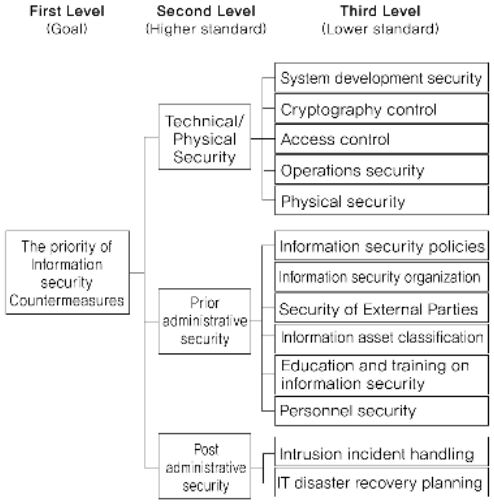
정보보호 관리체계에 대한 선행 연구[14]는 정보보호 투자 우선 순위를 평가하기 위해

〈Table 1〉 Checking List of ISMS (Information Security Management System) Certification

Type	Control Area	# of control Items	# of Checking point
Security Management	Set up security policy & scope	2	4
	responsibility of manager	2	4
	Risk management	3	11
	Implementation	2	3
	Post management	3	6
	Sub-Total	12	28
Security Measures	Security Policy	6	13
	Security Organization	4	7
	External Security	3	4
	Asset Categorization	3	7
	security training	4	10
	Individual Security	5	11
	Physical security	9	21
	System development security	10	22
	Password Control	2	8
	Access control	14	46
	Operational security	22	56
	incident management	7	14
	IT disaster recovery	3	6
	Sub-Total	92	225
Total		104	253

<Table 1>의 정보보호 대책 통제 항목 중 관리 항목을 사전 관리 작업, 사후 관리작업으로 구분하고 기술적/물리적 보안을 통합한 상위 기준(2^{nd} level)과 구체적인 하위 기준(3^{rd} level)으로 재구성하여 단계별 투자 중점 사항에 대해 논의하였다. <Figure 1>은 선행 연구에서 계층적으로 재구성한 정보보호 대책 항목들을 나타내고 있다[14].

해당 전문가 설문조사의 결과는 정보보호 중요도 평가에서 상위기준 중 사전관리적 보안이, 하위기준에서는 침해사고 관리가 가장 중요한 것으로 인식되고 있음을 나타낸다. 이에 반하여 실제 정보보호 투자가 진행된 항목



〈Figure 1〉 ISMS Structure Hierarchy

으로는 상위기준 중 기술적/물리적 보안이, 하위 기준에서는 IT 재해복구 항목이 가장 많은 응답을 받은 것으로 조사되었다.

2.4 정량적 투자결정 모델

정성적 정보보호 관리의 장점은 기술적, 물리적 보안을 포함하여 개별 기업에서 필요한 전반적 관리 항목을 전체적으로 조망할 수 있다는 점과 항목별로 접근하기 때문에 타 기업과의 비교 등을 통해 상대적으로 평가 관리가 손쉬운 점을 꼽을 수 있다. 그러나 이와 같은 성과측정 기록표 방식에 의한 정보보호 관리 방안은 개별 기업에서 실제 최적 투자액의 결정이나 구현 방식 간의 상호 비교 등의 세부사항을 결정하기 위해서는 도움이 될 수 없다. 이를 위해서는 보다 세부적인 부가 정보, 즉 개인정보에 대한 보다 정량적인 분석이 필요하다[4, 5].

기업 성과 분석에서 투자효율성에 대한 가장 일반적인 접근은 기업의 경쟁력을 알아보는 지표 중의 하나인 투자 대비 이익률(ROI)을 활용하는 방법이다[15, 16]. 개인정보보호 투자 대비 편익에 대한 정량적 분석 중 하나는 전통적 수요공급 곡선을 활용한다. 이론적으로 자본시장에서의 개인정보의 수요와 공급은 개인정보의 사용으로 인한 편익이 그로 인한 손해보다 큰 경우 나타날 수 있다[6].

채승완[6]은 기존의 수요공급곡선에서 개인정보보호 수준을 함께 고려함으로써 발생할 수 있는 각각의 수요, 공급곡선과 균형가격의 변화를 제시하였다.

이에 따르면 개인정보보호 수준의 강화($R_1 < R_2$)는 개인정보 수요와 공급에 모두 영향을 미친다. 즉 개인정보 수요자들은 개인정보보호 수준의 강화에 따라 인프라를 추가로 구축해야 하는 등의 요인이 비용증가로 나타나게 되어[11] 개인정보 수요가 감소될 것으로 예상하였다. 이에 반하여 개인정보 공급자는 개인정보보호 수준이 강화되게 되면 개인정보 제공으로 인해 야기되는 손해의 가능성이 감소하게 되고 이는 결국 개인정보 공급을 증가시키게 될 것으로 예상하였다.

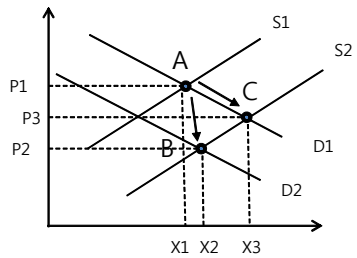
<Figure 2>에서 보는 바와 같이 개인정보보호 수준의 강화로 인해 발생되는 새로운 수요공급 곡선은 D2, S2로 나타나게 된다. 따라서 수요의 감소와 공급의 증가로 보다 엄격한 개인정보보호 수준을 준수하는 기업의 개인정보 수요공급 균형점은 점 A에서 점 B로 변경, 새로운 균형가격은 P2로 하락하게 된다.

〈Table 2〉 Benefits vs. Risk of Personal Information Online Usage

Subject		Benefit	Risk
Provider	Individual	Network service for digital content/government/finance	- identify theft, - spam
consumer	Private Corp.	- Profit Maximize - cost reduction	- security investment - identity verification
	Public org.	- efficient admin. - cost reduction	

Note: * modified from [6].

만일 새로운 개인정보보호 수준을 준수하는 기업과 대비하여 이를 준수하지 않는 기업이 존재한다면 이들은 추가적인 정보보호 투자를 거치지 않기 때문에 공급 곡선만이 S2로 변경할 것으로 예상, 점 A에서 점 C로 이동할 것으로 예측하였다.



〈Figure 2〉 Demand-Supply Curve for Personal Information

이러한 제반 상황에서 정보보호 투자에 따른 기대 편익은 추가 보안 투자로 인해 발생한 가격 변동과 실제 보관 중인 개인정보의 곱으로 나타날 수 있다. 또한 계산된 기대 편익과 실제 필요한 정보보호 투자액과 상호 비교함으로써 투자효율성을 검증할 수 있다.

이미 언급한 개인정보의 수요공급 곡선을 이용한 정보보호 투자의 기대편익은 개인정보의 가격 변동이라는 가상의 개념을 기본으로 하여 실제적 측정과 평가가 어려운 단점을 지닌다. 실제로 정보보안 분야에서 정보보호 투자의 기대편익은 보통의 경우 보안사고발생 확률의 감소를 통해 측정된다[9]. 연간 보고되는 피해 사례 보고서 분석을 통해 각종 보안사고의 위험 요소들과 정보시스템이 이들 위험 요소에 노출될 수 있는 확률을 통계적 평균값으로 산출한다. 위험요소의 노출 위험도는 아래와 같은 단위 항목들이 사용된다[2].

- 단일기대손실(Single Loss Expectancy, SLE)
- 연간발생율(Annual rate of occurrence, ARO)
- 연간기대손실(Annual Loss Expectancy, ALE)

보안 측면에서 정보가 위험 요소에 노출될 확률은 대부분 과거 통계 데이터에 의존하고 있다. 따라서 기업의 정보시스템의 실제적 정보유출 위험도를 산출하기 위해서는 다양한 위험요소에 동시에 노출될 때 나타날 수 있는 확률적 상관관계의 분석을 시도되기도 한다[3].

이와는 별도로 기업의 보안 위험에 대한 시스템의 취약성을 정보보호 투자액과의 함수 관계로 모델링 하려는 다양한 시도가 있었다[17]. 가장 대표적인 보안 투자 모델링인 Gordon and Loeb 모델[2, 7, 8]은 주어진 정보에 대한 위험확률을 t, 주어진 정보에 대한 취약성 확률을 v, 주어진 정보의 보안을 위해 투자할 비용을 z로 가정할 때, 정보 투자 이후의 새로운 시스템 취약성 확률 v'(≤ v)을 제공하는 함수 S(z, v)를 제공한다.

보안침해 확률함수(Security Breach Probability Function)로 명명된 이 함수는 두 번의 미분이 가능한 연속함수라는 가정 이외에도 아래와 같은 추가적인 속성을 가진다.

- 임의의 z에 대해 S(z, 0) = 0
- 임의의 z에 대해 S(0, v) = v
- S(z, v) 함수를 z로 미분한 함수 dS(z, v)/dz는 음의 값을, 이를 다시 미분한 함수 d(dS(z, v)/dz)dz는 양의 값을 갖는다.

위의 속성은 기업의 보안 취약점은 보안 관

련 투자액을 늘려가면 반비례적으로 감소하며 해당 감소분은 점차 축소된다는 가정을 출발점으로 삼고 있다는 점을 잘 나타내고 있다.

추가적으로 Gordon and Loeb 모델에서 사용되는 변수의 내용은 아래와 같다.

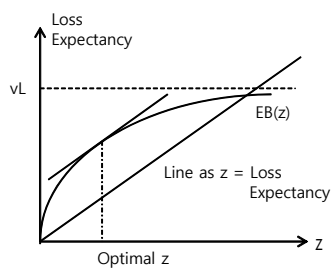
λ: 정보유출 사고가 발생한 경우 기업의 금전적 손실
t: 주어진 정보에 대한 위험 확률
v: 주어진 정보에 대한 취약성 확률
vtλ: 기업의 예상 손실
L(= tλ): 기업의 잠재적 손실
z: 주어진 정보의 보안을 위해 투자할 비용
S(z, v): 보안침해확률 함수

이 모델에 의하면 투자액 z에 의해 v의 값이 변화된 내용, v′ = v-S(z, v)에 따라 기업의 잠재적 손실 L은 v′L = (v- S(z, v))L 로 줄어들게 된다. 따라서 정보보호 투자에 따른 기대 편익 EB(z)는 아래와 같이 정의될 수 있다.

$$EB(z) = [v-S(z, v)]L$$

함수 S(z, v)에 대한 가정에 의해 EB(z)는 투자 대비 예상손실액 좌표에서 위로 볼록한 함수로 나타난다. 또한 투자액 대비 예상 손실액의 감소가 크게 나타날 때까지 지속적인 투자가 이루어지므로 기울기가 1인 접선을 가진 최적 투자액 z를 가진다.

<Figure 3>은 이와 같은 이론적 모델을 통한 최적 투자액 도출 과정을 잘 나타내 주고 있다.



〈Figure 3〉 Loss Expectancy vs. Security Investment

3. 정량적 투자결정 모델의 활용

본 연구는 정량적 투자결정 모델을 적용하기 위해 한국인터넷진흥원에서 2014년 11월 실시한 개인정보보호 수준 실태조사 결과를 활용한다. 해당 조사는 전국 17개 시도에서 총 유효표본 401개의 정보통신망법 적용 대상 사업자를 대상으로 개인정보보호 수준 측정을 목적으로 개인정보의 수집 및 이용, 개인정보의 기술적·관리적 조치 현황, 정보통신망법 제도의 이행 여부 및 적절성 평가, 정책성과 평가 및 홍보효과 측정 등을 조사하였다.

〈Table 3〉 Category of Survey Participants

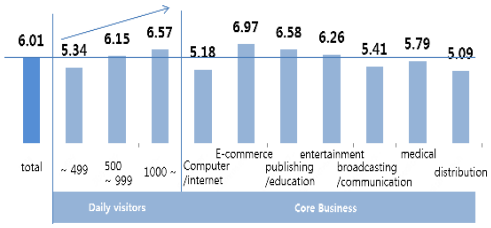
Category		%
Core Business	computer/internet	28.7%
	e-commerce	19.7%
	publishing/education	17.7%
	entertainment	15.5%
	broadcasting/ communication	8.5%
	medical	8.5%
	distribution	2.7%
Daily visitor	1000~	39.2%
	500~999	23.2%
	~499	37.7%
Company size	Small	40.6%
	Middle	33.9%
	Large	13.0%
	Listed	12.5%

본 조사에 참여한 401개 사업자의 월평균 홈페이지 방문자수, 기업 규모, 핵심사업 분야의 분포는 <Table 3>에서 살펴볼 수 있다.

기술된 표본기업에서 수집하는 개인정보항목은 모두 8개로 조사되었으며 각 항목은 아래와 같다.

- 이름
- 이메일주소
- 휴대폰전화
- ID
- 생년월일
- 집/회사 주소
- 비밀번호
- 집/회사 전화번호

개별 기업은 전체 항목의 일부를 개인정보로 수집, 저장하고 있으며 수집한 개인정보의 수의 분포는 <Figure 4>에서 확인할 수 있다.

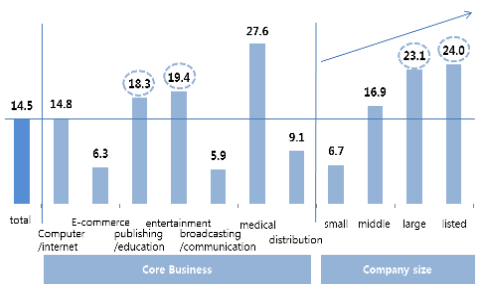


〈Figure 4〉 Number of Collected Personal Information Items

<Figure 4>에 나타난 조사 결과에 따르면 홈페이지 방문자수가 많은 기업일수록 보다 많은 개인정보를 수집하고 있으며 사업분야별로는 전자상거래 기업이 가장 많은 6.97개의 평균치를 나타내고 있다.

더불어 대부분의 기업에서 개인정보 저장을 위해 완전 암호화(28.4%) 혹은 부분 암호화(64.2%) 방식을 활용하여 개인정보를 암호화하고 있는 것으로 조사되었으며 전혀 암호화 방식을 사용하지 않는 기업도 전체의 7.4%로 조사되었다.

또한 조사 대상 사업자의 14.5%는 개인정보 누출사고가 있었던 것으로 조사되었으며 핵심사업분야나 기업규모에 따라 큰 편차를 나타낸다. 주로 기업 규모로는 주로 중견기업 이상의 기업이, 핵심사업분야로는 출판/교육, 엔터테인먼트, 건강/의료 분야의 기업이 평균치 이상의 개인정보 누출사고를 경험한 것으로 응답하였다. 또한 개인정보 누출사고 경험이 있는 사업자의 44.8%는 개인정보 누출사고를 신고하지 않은 것으로 조사되었다.



〈Figure 5〉 Frequency of Personal Information Leakage Incidents

4. 정량적 투자결정 모델의 활용

본 장에서는 앞서 요약된 개인정보보호 수준 실태조사 결과를 바탕으로 개인정보유출사고의 발생 빈도가 사업분야에 따라 달리 나타난 원인을 정량적 분석을 바탕으로 유추하고자 한다. 이를 위해 먼저 개별 기업의 관리자

가 모두 합리적인 개인정보보호 투자를 결정하였다고 가정한다.

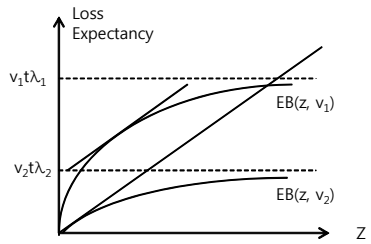
4.1 Gordon and Loeb 모델 활용

Gordon and Loeb 모델 방식의 분석을 시도하기 위해서 필요한 변수 중 위험확률 t는 한국인터넷진흥원의 2014년 개인정보보호 수준 실태조사에서 개인정보유출 사고가 발생한 14.5%로 설정한다. 또한 대부분의 응답 기업이 개인정보 저장을 위해 암호화 방식을 도입한 것으로 조사된 바 법적 요구 사항에 따른 일정 수준의 정보보호 투자는 모두 이루진 것으로 판단할 수 있다. 또한 보안침해확률함수 자체는 개별 기업에 따라 큰 차이를 나타내지 않을 것으로 예상된다.

그러나 이러한 가정하에서도 해당 기업들이 핵심사업분야에 따라 개인정보유출 사고의 빈도수가 차이를 나타내는 것은 주어진 정보에 대한 실제 취약성 확률이 다르게 나타나기 때문이다. 그러므로 경영자의 합리적 판단에 따른 투자결정은 대부분 정보유출 사고로 인한 기업의 금전적 손실에 대한 인식의 차이로 기인된다.

이는 전자상거래나 유통/물류 분야나 방송/통신의 컨텐트 제공과 같이 금융거래를 수반할 가능성이 높은 사업 부문에서 개인정보유출 빈도가 낮게 나타났다는 점에서도 동일한 추론을 가능하게 한다.

<Figure 6>은 동일한 t 위험확률에 대하여 기업이 예상되는 손실 λ_1와 $\lambda_2(\lambda_1>\lambda_2)$, 체감 취약성 확률 v_1와 $v_2(v_1>v_2)$를 가진 두 기업에 대한 최적 보안 투자 분석을 진행한 결과를 나타낸다. 낮은 기대손실과 체감 취약성 확률을 가진 기업일수록 보안 투자를 하지 않는 것이 오히려 합리적인 결정임을 보인다.



〈Figure 6〉 Loss Expectancy vs. Security Investment for v_1 and v_2 ($v_1 > v_2$)

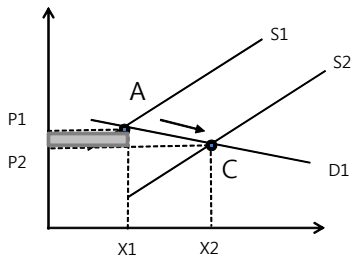
4.2 개인정보의 수요공급 법칙 활용

한국인터넷진흥원의 2014년 개인정보보호 수준 실태조사에서 기업들이 핵심사업 분야에 따라 개인정보유출 사고의 빈도수가 차이를 나타내는 것을 개인정보의 수요공급 곡선으로 이해하기 위해서는 개별 사업분야에 따라 개인정보보호 기준이 달리 적용되고 있다고 분석할 수 있다. 즉, 전자상거래, 유통/물류, 방송/통신 등의 핵심사업분야에는 보다 높은 수준의 개인정보보호 기준이 설정되어 있는 반면 출판/의료, 엔터테인먼트, 건강/의료 분야의 기업은 해당 기준에는 미치지 못하는 개인정보보호 수준을 적용 받고 있음을 나타낸다.

<Figure 2>에서 언급된 사례에서 높은 개인정보보호 수준을 적용 받음으로써 점 A에서 점 B로 이동하는 시나리오와 개별 기업이 개인정보보호 수준을 준수하지 않음으로써 점 A에서 점 C로 이동하는 시나리오가 각각의 기업군에 적용되고 있다.

또한 가격 변화에 따른 수요의 탄력성이 개별 기업군에 따라 다르게 나타나게 된다는 점

도 함께 고려하면 개인정보보호 투자로 인해 나타나는 편익 역시 기업군마다 달라진다는 점이 추가되어야 할 것이다.



〈Figure 7〉 Demand-Supply Curve for Personal Information

<Figure 7>은 수요의 탄력성이 낮은 기업군에서 개인정보보호 기준의 강화로 인해 얻을 수 있는 기대 수익의 크기가 상대적으로 작게 나타날 수 있음을 보인다.

5. 결 론

전자상거래의 금융거래의 성립을 위해 온라인 정보시스템 상에서 거래 당사자의 정보를 제공하는 것은 필수적이다. 개인정보의 임의적 보관은 거래의 간편화에 도움이 되는 반면 외부 유출로 인해 직접적 혹은 간접적 피해가 발생할 가능성을 높인다. 본 연구는 시스템 운영 기업의 측면에서 정보 침해 사고발생의 위험률과 이로 인해 발생할 수 있는 손실을 감안한 최적 투자 산출을 위해 필요한 정성적 분석 방법과 정량적 분석 방법을 비교하였다.

정보보호 관리체계로 대표되는 정성적 정보보호 관리의 장점은 기술적, 물리적 보안을 포함하여 개별 기업에서 필요한 전반적 관리 항목을 전체적으로 조망할 수 있다는 점과 항목별로 타 기업과의 비교 등을 통해 평가 관리가 손쉬운 점을 꼽을 수 있다. 그러나 개별 기업에서 실제 최적 투자액의 결정이나 구현 방식의 상호 비교 등의 세부 사항을 결정하기 위해서는 보다 세부적인 정량적 분석이 필요하다.

본 연구는 대표적인 정량적 분석 방법으로 개인정보에 대한 수요공급 곡선 방식과 Gordon and Loeb 모델 방식의 분석을 제시하였다. 또한 한국인터넷진흥원에서 실시한 개인정보보호 수준 실태조사 결과 중 개인정보 누출사고가 있었던 조사 대상 사업자의 분포가 핵심사업분야나 기업규모에 따라 큰 편차를 나타내는 원인을 제시하였다.

분석 결과를 바탕으로 도출된 본 연구의 주요 시사점은 다음과 같다.

첫째, 핵심사업 분야에 따라 개인정보유출 사고의 빈도수가 차이를 나타내는 것은 오히려 경영자의 합리적 판단에 따른 투자결정에 기인한 바가 크며 이는 대부분 정보유출 사고로 인한 기업의 금전적 손실에 대한 과소 평가가 주요 원인으로 지목된다. 따라서 개인정보유출 사고로 인한 기업의 금전적 손실에 대한 인식을 크게 높일 수 있도록 징벌적 손해배상이 이루어져야 한다. 개별 기업이 속한 사업 영역에 따라 개인정보의 직간접적 가치에 대해 상이한 인식을 가지는 것은 오히려 당연한 결과로 판단된다.

다만 개인정보보호 투자결정에 보다 긍정적인 영향을 미치기 위해서는 유출사고로 인한 금전적 손실이 징벌적 손해배상을 통해 일정 수준을 유지하는 것이 기업간 편차를 보완할 수 있는 대책이 될 수 있다.

둘째, 정보보호 관리체계 인증 등과 같이 개

인정보 관련 법률로 요구하는 개인정보보호 기준이 최상위 등급을 유지하도록 지속적으로 보완해야 할 필요가 있다. 개인정보 수요공급 곡선의 논의에서 살펴 본 바와 같이 일부 기업은 개인정보보호 수준을 준수하지 않음으로써 필요한 투자를 기피하는 것이 보다 합리적인 결정이 될 수 있기 때문이다. 일정 수준의 개인정보보호 장치가 모든 기업에 적용되기 위해서는 되도록 최상위 등급의 기준을 제시하고 이를 지속적으로 점검하는 것이 바람직하다.

이를 통해 개별 기업이 투자 우선 순위를 정하더라도 개별 투자의 효율성과 함께 개인정보보호의 합목적성을 함께 고려할 수 있도록 개인정보보호 정책의 방향이 설정되어야 할 것이다. 본 연구의 결과와 시사점이 실제 사례에 충분히 반영되고 전체적인 정보보호 수준이 유지될 수 있도록 개별 기업의 투자결정을 유도하기 위한 고려 사항으로 활용되기를 기대한다.

References

[1] Ahn, J. H., Choi, K. C., Sung, K. M., and Lee, J. H., "A Study on the Impact of Security Risk on the Usage of Knowledge Management System: Focus on Parameter of Trust," The Journal of Society for e-Business Studies, Vol. 15, No. 4, pp. 143-163, 2011.

[2] Anderson, R. and Moore, T., "The economics of information security," Science, Vol. 314, No. 5799, pp. 610-613, 2006.

[3] Andre, A., Fredrik, V., Giovanni, V., and Richard, A. K., Using hidden markov models to evaluate the risks of intrusions. In: Recent Advances in Intrusion Detection. Springer Berlin Heidelberg, pp. 145-164, 2006.

[4] Bojanc, R. and Jerman-Blažič, B., "Quantitative Model for Economic Analyses of information Security investment in an Enterprise information System," Organizacija, Vol. 45, No. 6, pp. 276-288, 2012.

[5] Bojanc, R., Jerman-Blažič, B., and Tekavčič, M., "Managing the Investment in Information Security Technology by use of Quantitative Modeling Approach," Information Processing & Management, Vol. 48, No. 6, pp. 1031-1052, 2012.

[6] Chai, S. W., "Economic Effects of Personal Information Protection," Journal of consumer policy studies, pp. 43-64, 2008.

[7] Chae, J. W. and Jeong, J. H., "Study on decision making for the industrial security management factor's priority," Journal of Security Engineering, Vol. 10, No. 2, pp. 123-140, 2013.

[8] Gordon, L. A. and Loeb, M. P., "The economics of information security investment," ACM Transactions on Information and System Security (TISSEC), Vol. 5, No. 4, pp. 438-457, 2002.

[9] Gordon, A. L. and Richardson, R.(April 13, 2004), "The New Economics of Information Security," Information Week, 53-56. Retrieved February 11th, 2007.

[10] Han, C. H., Chai, S. W., Yoo, B. J., Ahn, D. H., and Park, C. H., "A Quantitative Assessment Model of Private Information Breach," The Journal of Society for e-Business Studies, Vol. 16, No. 4, pp. 17-31, 2011.

[11] Kim, S. H. and Park, S. Y., "Influencing Factors for Compliance Intention of Information Security Policy," The Journal of Society for e-Business Studies, Vol. 16, No. 4, pp. 33-51, 2011.

[12] Korea Internet & Security Agency, A handbook on ISMS certification system, Jun 2013.

[13] Korea Internet & Security Agency, 2013 Research on the actual condition of the information security, Dec. 2013.

[14] Lee, C. C., KIM, J., and Lee, C. H., "A comparative study on the priorities between perceived importance and investment of the areas for Information Security Management System," Journal of The Korea Institute of Information Security and Cryptology, Vol. 24, No. 5, pp. 919-929, 2014.

[15] Mclean, G. and Brown, J., Determining the ROI in IT Security, CA Magazine, 2003.

[16] Purser, S. A., "Improving the ROI of the security management process," Computers and Security, Vol. 23, No. 7, pp. 542-546, 2004.

[17] Sklavos, N., Souras, P., "Economic Models & Approaches in Information Security for Computer Networks," IJ Network Security, Vol. 2, No. 1, pp. 14-20, 2006.

저 자 소 개

김정연	(E-mail: jykim@smu.ac.kr)
2002년	University of Michigan (석사)
2003년	University of Minnesota (박사과정)
2008~2011년	㈜세린 경영자문이사
2010년	상명대학교 경영학 (박사)
2011년~현재	상명대학교 경영대학 경영학과 조교수
관심분야	이익예측, 전자거래, 정보보안