Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.1, Feb. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.1.215

개인정보유출 피해 비용 산출 모델에 관한 연구*

임 규 건,† 류 미 나, 이 정 미‡
한양대학교 경영대학

A Study on the Damage Cost Estimation Model for Personal Information Leakage in Korea*

Gyoo Gun Lim,† Mei Na Liu, Jung Mi Lee‡
Business School, Hanyang University

요 약

한국은 단기간에 IT강국으로 급성장함에 따라 사이버 폭력, 개인정보 유출, 사이버 테러 등 사이버상의 각종 부작용이 새로운 사회적 문제로 대두되고 있다. 특히 안전한 사이버 생활의 기본이 되는 개인정보 유출에 대한 심각성은 전 세계적으로 심각한 문제로 부각되고 있다. 이와 관련하여 개인정보 유출에 따른 피해비용 규모의 추정이 필요한데 이와 관련한 연구는 국내에서는 아직 미흡한 상황이다. 이에 본 연구에서는 개인정보 유출에 따른 피해비용 산출 모델을 실거래 평균값 기반, 개인 인식 가치 기반, 보상금액 기반, 타 국가 기반의 네 가지 방식을 제시한다. 그리고, 2007년부터 2016년까지의 뉴스와 보고서 등의 자료를 분석하여 10년간의 개인정보 유출사건을 수집하여 피해비용을 추정하였다. 추정에 활용한 사건의 수는 65건이고 총 개인정보 유출 건수는 약 4억 3천만 건에 이른다. 추정결과 2016년의 개인정보 유출로 인한 피해비용은 최소 74억에서 최대 220조로 추산되었으며 10개년도 평균은 연간 약 107억에서 307조로 추산 되었다. 또한 개인정보 유출로 인한 추정 피해액이 3년 주기로 상승하는 특이점을 발견할 수 있었다. 앞으로 본 연구를 통해 개인정보 유출로 인한 피해비용을 조금 더 정확하게 측정할 수 있는 지표를 마련하고 그 피해비용을 줄일 수 있는 방안 마련의 지표로 사용되기를 기대한다.

ABSTRACT

As Korea is rapidly becoming an IT powerhouse in the short term, various side effects such as cyber violence, personal information leakage and cyber terrorism are emerging as new social problems. Especially, the seriousness of leakage of personal information, which is the basis of safe cyber life, has been highlighted all over the world. In this regard, it is necessary to estimate the amount of the damage cost due to the leakage of personal information. In this study, we propose four evaluation methods to calculate the cost of damages due to personal information leakage according to average real transactions value, personally recognized value, compensation amount basis, and comparison to similar countries. We analyzed data from 2007 to 2016 to collect personal information leakage cases for 10 years and estimated the cost of damages. The number of cases used in the estimation is 65, and the total number of personal information leakage is about 430 million. The estimated cost of personal information leakage in 2016 was estimated to be at least KRW 7.4 billion, up to KRW 220 billion, and the 10 year average was estimated at from KRW 10.7 billion to KRW 307 billion per year. Also, we could

Received(10. 16. 2017), Modified(12. 04. 2017), Accepted(12. 04. 2017)
* "본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 방송통신정책연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2016-0-003800021001)". 본 논문의 초기 버전은 2017년 한국IT서비스학회 춘계학술대회(pp. 182-184)에 발표되었음.
† 주저자, gglim@hanyang.ac.kr
‡ 교신저자, jungmi5800@gmail.com(Corresponding author)

find out the singularity that the estimated damage due to personal information leakage increases every three years. In the future, this study will be able to provide an index that can measure the damage cost caused by the leakage of personal information more accurately, and it can be used as an index of measures to reduce the damage cost due to personal information leakage.

Keywords: Cyber side-effect, personal information leakage, Infringement of rights, cost calculation model

I. 서 론

최근 세계적으로 스마트폰, 테블릿 PC, 넷북 등 다양한 IT 제품 및 서비스가 폭발적으로 증가함에 따라 사회전반에 걸쳐 정보의 검색과 공유가 그 어느 때 보다 자유로워졌다[1]. 정보의 검색과 공유가 자유로워진 만큼 일상에서 보안 사고를 경험하는 사건들도 늘어나고 있다. 정부의 웹사이트가 공격을 받아 개인정보가 유출되기도 하고, 자신의 컴퓨터가 좀비 PC가 되기도 한다. 이러한 보안사고는 정부 뿐 아니라 금융기관이나 온라인서비스 기업을 가리지 않고 빈번히 나타난다[2].

이와 같이 정보화 수준의 외형적 성장과는 달리 현재의 IT 환경은 결코 안전한 것이 아니다. 이에 대응해 민간분야는 물론 국가·공공분야에서도 정보통신망이나 정보화시스템에 대한 사이버공격을 실시간 탐지, 분석·대응하기 위하여 사이버 보안관제센터를 설립하여 운영하고 있다. 그러나, 보안관제에 관한 명확한 법 규정이나 관련 지침이 없고 보안관제 시스템 구축, 운영에 대한 표준화는 물론 각 보안관제 센터 간 사이버 위협정보나 관제기술 공유 등을 통한 사고 재발방지를 위한 공동 대응방안도 마련되어 있지 않아 효율적인 보안 관제업무가 어려운 실정이다[3].

이로 인해 발생하는 인터넷 상의 각종 부작용은 새로운 사회적 문제가 되고 있다. 인터넷 상의 부작용에 대한 문제제기와 해소방안에 대해서는 다양한 선행연구가 진행되어왔으나 이런 인터넷 상의 부작용으로 인한 개인과 기업, 국가 차원에서의 피해비용을 산출하고 그 피해 규모를 파악하는 연구는 미흡하였다. 특히 최근 사이버 공간의 접근과 이용제약 및 비대면성과 중독성에 따른 역기능 발생(사이버 폭력, 개인정보 유출, 사이버 따돌림, 사생활 침해, 명예훼손, 중독 등)으로 인한 사회적 문제가 점점 증가되고 있는 추세에 따라 이를 사회적 비용으로 추정하고 그 심각성을 파악하여 그에 대한 대응 정책과 제도 마련이 시급한 실정이다.

이런 인터넷상의 각종 부작용 중 그 문제가 가장 심각한 것은 개인정보유출에 대한 부분이다. 최근 글로벌 온라인 포털업체인 YAHOO[4]에서 2014년 해킹으로 5억 명의 개인정보가 유출되었음을 2016년 9월에서야 공개한 사건이 있었으며, 앞서 2013년에도 해킹으로 10억 명의 개인정보가 유출된 적이 있었다. 한국에서도 2014년 1월 KB카드 약 5,300만 명, 롯데카드 2,600만 명, NH농협 2,500만 명의 개인정보가 유출된 사건은 금융시장을 패닉상태로 만들었으며, 이들 카드사가 부담해야 할 직접적 손실비용이 약 5,000억 원에 이를 것으로 예상되었다[5]. 일반적으로 유출사고 발생 시 기업은 유출정보에 대한 피해에 대한 정보를 대중에 선포하는 것을 꺼려한다. 따라서 많은 사건사고가 있었음에도 불구하고 실제 피해규모 손실을 정확하게 측정하는 것은 한계가 있다.

본 연구에서는 개인정보 유출로 인한 사회적 피해비용을 산출하는 방법을 선행연구를 바탕으로 개인, 기업, 국가 총 세 가지 기준에서 네 가지 산출 모델을 제시하고자 한다. 또한, 실제 개인정보 유출사고 데이터를 2007년부터 2016년까지의 뉴스와 보고서 등의 자료를 분석하여 10년간의 개인정보 유출사건을 수집하여 개인정보 유출로 인한 사회적 비용을 추정하고자 한다.

II. 선행연구

2.1 사이버 역기능

IT가 급속도로 발전하면서 인간 삶의 질이 향상되고 있으나 반면에 기술의 발달과 생활의 편리함의 이면에는 많은 사회적 문제점이 야기되고 있다. 사이버 역기능은 크게 범죄형 역기능과 비 범죄형 역기능으로 구분된다. 세부적으로 범죄형 역기능은 사이버 테러형 역기능과 일반 사이버 역기능으로 구분한다. 일반 사이버 역기능의 대표적인 유형에는 게임사기, 통신사기, 명예 훼손 및 성폭력, 개인 정보 침해, 저작권 침해, 인터넷 도박 등이 있다. 비 범죄형 사이버 역기능에 불건전한 유해 정보 유통과 인터넷 중독,

언어 파괴 등이 있다. 사이버의 역기능 중 가장 큰 문제점은 해킹이나 바이러스 같은 사이버 공격에 의해 사이버 공간이 파괴되는 것이다[6,7]. 또한 권정인 등[8]은 사회현상학 관점에서 인터넷 역기능 분류 표준을 미디어중독, 유해콘텐츠, 사이버폭력, 권리침해, 판단장애 등으로 분류하였다. 미디어중독에는 게임중독, 채팅중독, 음란물 등이 있고 유해콘텐츠 웹사이트와 매체가 있다. 사이버 폭력에는 명예회손, 언어폭력, 인간소외 등이 있고 권리침해에는 초상권, 저작권, 개인정보, 집단정보 등이 포함되어 있다. 마지막으로 판단장애에는 여론조작, 선동행위, 네카시즘 등이 있다.

서재철[9]의 인터넷 서비스의 역기능 분류에 관한 연구에서는 역기능을 사이버범죄와 사이버 일탈행위로 구분하여 분류하였다. 이는 인터넷 전반에 걸친 역기능이라기보다는 사이버 상에서 벌어지는 역기능에 초점을 맞춘 분류로 일반화하여 사회전체의 현상을 수용하기에는 부족하다. 권정인 등[8]은 인터넷 이용자 윤리 소양제고 기반 마련을 위한 연구에서 인터넷의 역기능을 인터넷 중독, 유해정보, 인격침해, 정보침해, 사이버테러, 일반범죄 등으로 구분하여 기존 연구의 특정부분에 대한 역기능 분류의 한계에서 벗어나 역기능의 분류를 일반화하고자 하는 시도를 했으나 분류의 구분이 명확하지 못하고 새로운 기술이나 기기에 대한 역기능의 문제점을 포괄하기에는 다소 미약하였다.

사이버역기능에 관련한 경제적 비용연구들로 강형등[10]은 사이버테러의 피해규모를 산정하기 위한 기존 접근방법을 분석하고 인수비용, 운영비용, 사업기회비용, 간접비용 등을 변수를 사용하여 구체적 피해규모 산정 모델을 제시하였다. 장종호 등[11]은 인터넷 공격으로 경제적 측면에 직접적 피해모델, 간접적 피해모델을 제시하고 가상적인 인터넷 공격의 경제적 피해를 산출하였다. Dubendorfer et al.[12]는 인터넷 공격으로 다운타임 손실, 재해복구, 회사부채, 소비자 손실 등의 경제적 피해모델을 제시하였다. Cashell et al.[13]은 사이버공격으로 인한 주식 시가 하락, 정보 유출 등 경제적 피해를 가상 시나리오를 모델에 적용해서 피해액을 산출하였다. 신진[14]은 정보보호 침해사고를 비용/편의분석(Cost Benefit Analysis) 방법을 통하여 연구하였고 직접비용, 간접비용, 명시적 비용과 잠재적 비용의 4 가지로 구분하였다.

최근 국내외 정부기관, 국제기구 및 민간 기업을 대상으로 DDoS 공격, 해킹, 개인정보 유출 등 사이버 침해사고가 잇따라 발생하고 있다. 2003년에는 1·25사태로 인해 전국 대부분의 네트워크가 마비되기도 했고, 해킹에 의한 금융 사고나 개인정보 유출과 관련된 사고도 빈번하게 일어나고 있다. 얼마 전에는 전자정부의 문서 위·변조 가능성이 국회에서 제기되기도 했으며, 정보유출의 주범인 스파이웨어들이 맹활약하고 있다는 보도가 줄을 있고 있다. 이에 따라서 우려되는 점은 사이버 공격이 직간접적인 경제 피해로 연결되는 경우가 많아지고 있다는 사실이다.

본 연구에서는 기존의 선행연구를 바탕으로 사이버 역기능을 크게 개인과 기업으로 대분류 하고 개인적 차원에서는 미디어중독, 유해콘텐츠, 사이버폭력, 권리침해, 판단장애, 인터넷사기, 사이버범죄/테러로 중분류 한다. 기업 차원에서는 사이버범죄/테러와 권리침해로 중분류 하였고 이에 따른 소분류로는 게임중독, 명예회손, 저작권 침해, 보이스피싱, 개인정보 유출 등으로 분류하였다. 본 연구에서 제시하는 사이버 역기능의 자세한 분류는 [표 1]과 같다.

Table 1. Cyber side-effect classification

Cyber side-effect		
Main Category	Middle Category	Small Category
Individual	Media addiction	Game
		Chatting
		Shopping / Stock
		Pornography
		Information Search
		Sns
	Harmful content	Website
		Media
	Cyber violence	Insult
		Defamation
		Stalking
		Verbal Violence
		Abuse
		Human Alienation
		Malicious Comments
		Sexual Violence

Cyber side-effect		
Main Category	Middle Category	Small Category
Individual	Infringement of rights	Portrait
		Copyright
		Personal Information Extrusion
	Judgment disorder	Infodemix
		Manipulation Of Opinion
		Agitation
		Necassism
	Internet fraud	Electronic Commerce
		Game
		Voice Phishing
	Cybercrime / Terrorism	Hacking
		Virus
		Spyware
Enterprise	Cybercrime / Terrorism	Hacking
		Virus
		Spyware
		Material Leakage
		Bomb Spam
	Infringement of rights	Portrait
		Copyright
		Personal Information Extrusion

2.2 개인정보

인터넷을 이용할 때나 웹사이트에 회원가입 할 때 등 가상세계에서 서비스를 제공 받으려면 개인정보를 입력하는 것이 보편화 되어 있다. 정보보호법에서 정의하는 개인정보의 구성요소는 ①살아있는 개인(사망/실종, 법인 제외), ②특정 개인과의 관련성(개인 정체성과 관련: 설명, 주민번호, 생일, 주소 등이 해당되며 개인이 알아볼 수 없는 특정 대학의 해당연도 졸업생의 취업률 등을 제외), ③ 식별 가능성(다른 사람과 구분되고 다른 정보와 결합하여 구분되는 경우여야 하며 통계적으로 변환되어 개인을 식별할 수 없는 경우 제외) 등 3가지로 정의하고 있다[15]. 또한 개인정보보호위원회[16]에서는 개인정보를 다음 [표 2]와 같이 분류하고 있다.

Table 2. Personal Information Classification

Type	Category
General information	Name. resident registration number, driver's license number, address, phone number, date of birth, place of birth, home address, sex
Family Information	Family member name, place of birth, date of birth, resident registration number, occupation, telephone number
Education and Training Information	School attendance, final education, school records, technical qualifications and professional licenses, completed training programs, club activities
Military service information	Group number and rank, discharge type, peculiarity, working unit
Real estate information	Owned houses, land, cars, other possession vehicles, shops and buildings
Income information	Current salary, salary career, bonus and commission, other sources of income, interest income, business income, Other income insurance (health, life, etc.) subscription status, company expenses, investment program, retirement program, vacation, sick leave
Credit Information	Record of loan balance and payment status, mortgage, credit card, deferred payment and number of payments, notice of wage foreclosure notice
Employment Information	Current employer, company address, senior's name, job performance evaluation record, training record, attendance record, honor record, job attitude, personality test result
Legal Informat	Criminal record, vehicle traffic

Type	Category
ion	violation record, bankruptcy and collateral record, arrest record, divorce record, tax record
Medical Information	Family history, past medical records, mental illness record, physical disability, blood type, IQ, drug test, etc.
Organization information	Join unions, join religious groups, join political parties, club members
Communication information	E-mail, phone call contents, log file, cookies
Location information	Personal location information by GPS or mobile phone
Physical information	Fingerprints, iris, DNA, height, chest
Habits and hobby information	Smoking, drinking, preferred sports and entertainment, leisure activities, video rental records, gambling propensity

PIPC, "Personal Information Protection Annual Report." 2012

또한 개인정보협회[17]의 개인정보 가치와 개인정보 침해에 따른 사회적 비용 분석 관련 연구에서는 개인정보의 유형을 기본인적 정보(성명, 주소, 아이디 및 패스워드, 가족관계), 고유정보(주민등록번호, 여권번호, 운전면허 등록번호), 의료건강정보(병력, 병원 진료기록, 신체장애 정도, 건강상태), 경제정보(소득, 신용카드 및 통장계좌번호, 물품 구매내역, 대출 또는 담보설정). 사회관계정보(학력 및 학업성적, 친우관계, 동호회 활동 등 사회 활동 관련 정보), 통신위치정보(휴대폰번호, 이메일 주소 GPS위치정보), 법적 정보(전과 범죄기록, 납세기록, 과태료 부과 내역)로 정의하고 있다.

본 연구에서는 기존의 선행연구를 바탕으로 개인정보를 크게 인적사항, 신체정보, 의료정보, 금융정보, 사회정보, 통신정보 등 여섯 개의 유형으로 분류하였다. 세부내용으로는 기본 성명, 주민등록번호, 신용카드 및 통장계좌번호 뿐만 아니라 요즘 문제가 되는 지문, 홍채, 유전자 정보, GPS 등을 포함시켜 분류하였다. 본 연구에서 정의한 해당 분류의 세부내용은 다음 [표 3]과 같다.

Table 3. Personal Information Classification

type	category
Personal Information	Name, resident registration number, address, home address, phone number, contact information, date of birth, place of birth, Email address, family relationship, family member information, etc.
Physical information	Face, fingerprint, iris, voice, genetic information, height, weight, etc.
Medical Information	Health status, medical record, physical disability, disability grade, medical history, insurance and contract maintenance, gene analysis, etc.
Financial Information	Income, credit card and bankbook account number, purchase history of goods, loan or mortgage setting, Economic information includes commerce and financial transaction details, personal property / property holdings, credit rating information, etc.
Social information	Education, sexuality, criminal record, trial record, penalty payment history, workplace, high school, work place, work experience, military service, station number, working unit
Communication information	Phone call history, website access history, email, phone message, other GPS, etc.

2.3 개인정보 유출 피해비용 산출관련 선행연구

2000년을 전후로 개인정보유출 사건은 끊임없이 발생하고 있으며 그 규모와 범위는 더욱 커지고 다양화되고 있다. 2011년 이전엔 주로 해킹에 의한 정보유출이 발생하였다면, 2011년 이후에는 내부 직원이나 협력업체에 의한 정보유출 발생이 증가하고 있다.

또한, 최근의 카드 정보유출 사건은 협력 회사 직원이 고의로 정보를 유출하려고 했다는 특징을 가지고 있다[15].

Gordon and Loeb[18]은 정보보안의 3원칙을 기밀성 (confidentiality), 무결성(integrity), 가용성(availability)으로 제시하였다. 이러한 3원칙을 기본으로 하여 정보유출에 따른 피해발생비용을 직접비용(direct costs)과 간접비용(indirect costs) 으로 구분 하고 있다. 또한 피해발생비용을 명시적 비용(explicit costs)과 잠재적 비용(implicit costs)으로 구분하여 정의하였다.

개인정보유출과 조류독감의 간접피해비용 추정기법 연구에서는 침해사고의 피해비용을 간접비용, 직접비용, 명시적비용, 잠재적비용으로 구분하였다[15].

일본 네트워크 시큐리티협회[19]의 보고서에서는 개인정보유출 피해액 산출 요소를 기업 손실과 개인 손실로 보고 기업 손실에는 대응 인건비 제외, IR 대응 비용 제외, 수익 손실 제외, (실제 보상한) 법적 보상금으로 정의하였고 개인손실은 보상받지 못한 개인의 정보 가치로 정의하였다.

Ponemon[20]보고서에서는 개인정보의 피해액을 대응인건비, IR대응비용, 수익 손실, 실제 보상한 가치(기업손실)의 합으로 구성하였다.

기존의 개인정보 유출 사고로 인한 피해비용 산출 연구에서는 주로 가상가치접근법(CVM: Contingent Valuation Methods)방식을 사용하여 WTP(Willingness to Pay)와 WTA(Willingness to Accept)를 추정하여 그 피해비용을 산출하였다. 김여라 등[21], 유진호[22]는 CVM을 활용하여 이용자가 개인정보 유출방지를 위해 금전적으로 지불할 수 있는 금액 WTP를 추정하였으며 이해춘 등[23]은 CVM 방법론을 이용하여 개인정보 유출로 피해 가능성이 있는 응답자가, 기업이 제시하는 손해 배상을 수용하는 WTA를 화폐액으로 추정하여 개인정보 유출의 잠재적 손실액을 추정하였다.

그러나 이용자가 개인정보를 보호하기 위해 자신이 지불해야하는 WTP 추정금액은 상대적으로 낮게 추정되는 특징이 있고, 개인 정보가 침해당할 경우 기업이 제시하는 배상금액은 높게 하고 싶은 성향 때문에 WTA에 의한 추정 값은 상대적으로 과추정(over-estimate)되는 특징이 있다. 이 연구의 결과에서 이용자는 자신의 명의가 도용되어 특정 온라인 게임사이트에 가입된 사실을 알고 1인당 약 750만원의 배상금을 받기를 원하였다. 반면 김여라 등[21]의 연구 결과에서 이용자는 자신의 개인정보 보호를 위해 부가적인 통신서비스 요금을 낼 경우, 1개월에 약 3,900원을 지불할 의사가 있는 것으로 나타나 이용자의 양면적인 태도를 알 수 있다.

CVM 방법론은 이론적인 배경은 강점을 가지고 있으나, 실제 기업의 업무 환경을 직접적으로 반영하는 것 보다는 간접적인 측정방법으로서 한계점을 가진다. 특히 CVM 방법론은 이용자에게 제시하는 초기금액이나 가상시나리오에 의해 크게 영향을 받거나 조사자에 의한 편의(bias)가 발생할 수 있기 때문에 관련분야 전문가들의 면밀한 검토가 없으면 조사 시점마다 크게 달라질 수 있는 한계가 있다.

따라서 본 연구에서는 선행연구들의 한계를 보완한 방법으로 10년간 한국에서 발생한 실제피해유출 사고들의 데이터를 수집하여 분석하고자 하며 다양한 기준(개인기준, 기업기준, 국가기준)과 방법으로 개인정보 유출로 인한 피해비용을 추정함으로서 이러한 선행연구들의 한계점을 보완하고자 하였다.

개인기준으로는 실제 지하시장에서 거래되는 개인정보의 실거래가격과 개인입장에서의 보상받지 못한 개인정보 가치(개인 인식 가치)를 사용하여 개인정보 유출에 따른 피해비용을 산출하고자 한다. 또한 기업기준에서는 실제로 소송이 진행 되어 배상한 보상금액을 기준으로 하여 산출하고, 국가 기준으로는 타국가의 1인당GDP 대비, 인터넷 사용자 수 대비, 인구수 대비하여 한국의 개인정보 유출 피해비용을 추정한다.

III. 연구방법 및 프로세스

본 연구는 사이버 역기능과 개인정보, 개인정보 유출 피해비용 산출에 관한 선행연구를 분석하여 사이버 역기능과 개인정보를 정의하고 이에 따른 개인정보 피해비용 산출 모델을 수립하였다. 피해비용 산출 모델은 실거래 평균값 기반, 개인 인식가치 기반, 보상금액 기반, 타 국가 기반 추정 등 총 네 가지 방식으로 수립하였다. 데이터는 2007~2016년 까지 실제로 대한민국에서 발생한 개인정보 유출 사례와 Ponemon[20]보고서의 11개국 개인정보 유출 건당 평균 피해비용 데이터를 수집하여 활용하였다. 본 연구의 프로세스는 [그림 1]과 같다.

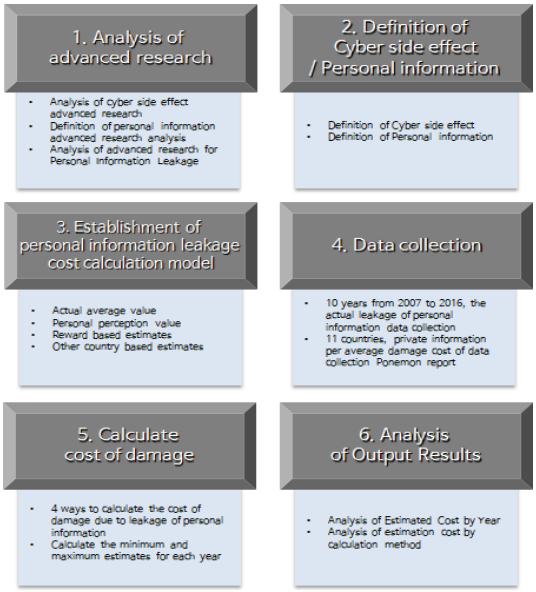

Fig. 1. Research Process

IV. 산출 모델

4.1 데이터 수집

개인정보 유출 데이터 수집은 직접수집방법을 이용하였다. 개인정보 유출이 기업과 개인의 입장에서 모두 민감한 부분으로 공공기관이나 논문 및 보고서에서 몇 년간의 데이터를 수집해 놓은 경우는 찾기 힘들다. 따라서 개인정보유출에 대한 데이터는 'DB 암호화 최신동향 및 보안기술 분석 보고서'와 한국방송통신위원회, 금융감독원 자료와 금융감독원 전자공시시스템, 뉴스를 바탕으로 직접 수집하였다. 수집기간은 2007년부터 2016년까지 총 10년으로 하였고 총 수집 사건 수는 65건이며 대표적인 사건으로는 2014년 카드 3사의 개인정보 유출을 들 수 있다.

수집된 데이터의 내용으로는 사건의 발생년도, 사건명, 기업명, 기업규모, 임직원 수, 총 유출건수, 그리고 개인을 상대로 보상이 진행 되었을 시 발생한 실제 보상액 등이다.

4.2 산출 모델 수립

개인정보 유출로 인한 사회적 피해비용 산출 모델은 개인, 기업, 국가 기준으로 네 가지 모델을 통하여 각각의 방법으로 개인정보 유출로 인한 사회적 피해비용 추정액의 최소치와 최대치를 산출하고자 한다.

첫 번째로 A방식인 실거래 평균값 기반 방식은 개인정보가 지하시장에서 실제로 거래되는 거래액을 개인정보 유출로 인한 피해액으로 보고 그 값을 추정한다. 추정방식은 실제 개인정보 유출건수에 실거래 평균값을 곱하여 산출한다. 여기서 실거래 평균값이란 개인정보 데이터가 실제 지하시장에서 거래되는 금액의 평균값을 의미한다. 본 연구에서는 국립재난안전연구원[15]에서 연구한 "개인정보유출과 조류독감의 간접피해비용 추정기법 연구"에서 개인정보가 지하시장에서 거래되는 건당 거래액인 250원에 본 연구에서 조사한 실제 개인정보 유출건수를 곱하여 그 피해액을 추정한다.

두 번째로 B방식인 개인인식가치기반 방식은 지하시장에서 거래되는 개인정보의 거래액은 실제 개인정보가 지니는 가치에 비하여 과소평가될 가능성이 있는 A방식을 보완하는 방법이다. 개인이 인식하는 개인정보의 가치에 실제 유출건수를 곱한 피해액으로 개인정보 유출로 인한 피해비용을 추정한다. 위의 두 가지 방법은 개인 기준에 기반을 두어 산출하는 방식이다. 이해춘 등[23], 국립재난안전연구원[15] 등의 연구에서 사용한 방식이다.

세 번째로 C방식인 보상금액 기반 방식은 기업이 개인정보 유출로 인해 개인에게 실제로 보상해주는 금액이 개인정보의 가치를 대변할 수 있으므로 개인정보 유출로 인한 실제 보상금액을 개인정보의 가치로 보고 개인정보 유출로 인한 피해비용을 산출한다. 추정방식은 유출건수에 실제 보상액을 곱하여 산출한다. 개인정보 유출 사고로 인해 개인이 받은 실제 보상액을 조사하고 보상받지 못한 경우에는 해당 보상액을 추정하여 그 피해액을 추정한다. 국립재난안전연구원[15], JNSA[19], 개인정보협회[17]등의 연구에서 사용한 방식이다

마지막으로 D방식인 타 국가 기반 산출 방식은 IBM에서 진행한 'Ponemon 2016 Cost of Data Breach Study: Global Analysis' 보고서의 국가 별 개인정보 유출로 인한 피해액을 가지고 한국의 개인정보 유출로 인한 피해액을 추정한다. 해당보고서는 데이터 유출의 경제적 영향을 계량화하여 제시하였으며 직접비용과 간접비용을 모두 고려한 추정방식이다. 한국과 1인당GDP와 인구수, 인터넷 이용자 수가 가장 유사한 국가를 선정하여 추정함으로써 국가적 차원에서 추정이 가능하다. 자세한 방식은

Ponemon[20]보고서를 기반으로 타국가의 1인당 GDP 대비, 인터넷 사용자 수 대비, 인구수를 대비하여 한국의 개인정보 유출 피해비용을 추정한다. [표 4]는 위의 네 가지 산출 방식을 정리해 놓은 것이다.

Table 4. Damage Cost Estimation Model for Personal Information Leakage

Model	Basis	Equation	Perspective
A	Actual average value	Number of leakage* Actual average value	Individual
B	Personal perception value	Number of leakage* Personal perception value	
C	Reward based estimates	Number of leakage* Actual compensation amount	Enterprise
D	Other country-based estimates	Compared to GDP / Internet users Estimation of personal information leakage cost in Korea	Country

4.2.1 실거래 평균값 기반 방식

실거래 평균값 기반으로 계산한 A방법의 산출방식은 다음과 같다. 국립재난안전연구원[15]에서 조사한 "개인정보유출과 조류독감의 간접피해비용 추정기법 연구"에서 개인정보가 지하시장에서 거래되는 실제 금액은 50원에서 500원이라고 조사된 바가 있다. 본 연구에서는 개인정보의 건당 실제 거래액을 해당 연구의 평균값인 250원으로 적용하여 실제 유출건수(N)에 개인정보의 건당 실제 거래액(Vr)을 곱하여 개인정보의 유출 피해비용을 산출하였다.

A. Actual average base value = N * Vr
N = number of outflows
Vr = Actual transaction amount of personal information (thing)

Fig. 2. Actual average value-based calculation formula

4.2.2 개인 인식 가치 기반 방식

B방식인 개인 인식 가치 기반방식은 실제 유출건수(N)에 건당 개인이 인식하는 개인정보의 가치(Vp)를 곱하여 개인정보의 유출비용을 산출한다.

유진호 등[24]는 10~50대 이상 500명을 대상으로 개인정보 유형에 대한 보상수요금액(WTA)과 실제 통신사 및 카드사 정보유출 사고에 대한 보상수요금액(WTA)을 설문으로 진행한 바 있다. 또한 국립재난안전연구원[15]의 연구에서는 개인을 대상으로 "보상받지 못한 개인정보 가치비용"을 설문으로 피해비용을 도출하였다.

본 연구에서는 해당 선행연구들의 연구 결과를 바탕으로 개인이 인식하는 개인정보의 가치(WTA)의 평균값을 7,101,819원로 계산하고 해당 금액에 화폐가지를 적용하여 개인정보의 유출 피해비용을 산출하였다.

B. Personal perception value base = N * Vp
N = number of outflows
Vp = per-person perception value (case)

Fig. 3. Personal perception value-based calculation formula

4.2.3 보상금액 기반 방식

C방식인 보상금액 기반 방식은 실제 개인에게 보상한 금액을 기업기준의 피해비용으로 산출한다. 본 연구에서 산출한 보상금액 기반 피해비용은 총 보상금액을 의미하며 이 값은 실제 보상금액과 추정 보상금액의 합계로 산출하였다. 실제 보상액은 개인정보 유출로 인한 건당 보상액에 실제 보상받은 인원의 수를 곱하여 산출하였으며 추정 보상액은 개인정보 유출로 인한 건당 추정 보상액에 추정 보상인원을 곱하여 산출하였다. 추정 보상액은 실제 보상액들의 평균값으로 산출하였으며 추정 보상인원은 2014년 기준으로 서울 중앙지법에 접수된 카드사 정보유출에 따른 추정 소송비율인 0.78%(2014, 국민재난연구원)에 따라 산출하였다.

C. Total amount of cost(TAOC) = AOC + AOC ′
a. Actual amount of cost(AOC) = Vc x Nr x 0.0078
b. Estimated amount of cost(AOC′) = Vc′ x Ne x 0.0078

TAOC = Total Rewards
AOC = Actual Rewards Calculated
AOC ′= Estimated Rewards Calculated
Vc = Rewards due to personal information leakage
Vc ′= Estimated Rewards due to personal information leakage
Nr = Actual Rewards
Ne = Estimated Rewards

Fig. 4. Reward based calculation formula

4.2.4 타 국가 기반 산출 방식

D방식인 타 국가 기반 산출 방식은 2016년에 IBM에서 진행한 'Ponemon 2016 Cost of Data Breach Study: Global Analysis' 보고서의 자료를 활용하였다. 해당 보고서에서는 총 11개국(United States, United Kingdom, India, Brazil, Germany, France, Japan, Australia, Canada, Italy, South Africa)의 383개 회사를 인터뷰를 통해 10개월 간 조사를 진행하여 데이터 유출의 경제적 영향을 계량화하여 제시하였다. 해당 연구에서는 직접비용으로 법의학 전문가 참여비용 + 법률 회사의 고용 비용 + 피해자의 신원 보호서비스 제공 비용 + 그 외 경비 지출 비용으로 분류하였으며 간접비용으로는 데이터 유출 해결 중에 소비 시간 + 노력 + 조직 리스크 + 영업권 손실 + 고객이탈 가능성으로 분류하였다. 보고서의 결과로는 기업의 평균 데이터 유출 비용은 약 4백만 달러였으며 분실 또는 도난으로 인한 지불비용은 평균 158달러로 밝혀졌다.

D.Other country-based estimates
a. Per capita GDP = PPP / PPP ′* avgCost * N
b. Population ratio = P / P ′* avgCost * N
c. Internet users = IP / IP ′* avgCost * N

N = number of leakage
PPP = GDP per capita in Korea
PPP ′= CDP per capita in other countries
avgCost = Damage cost per individual leakage of personal information by country
P = Korea population
P ′= Number of people in other countries
IP = number of Korean Internet users
IP ′= Number of Internet users in other countries

Fig. 5. Other country-based calculation formula

신진[14]의 연구에 따르면 사이버범죄로 인한 국가적 피해비용을 Ponnemon 보고서로 조사된 국가들의 GDP대비, 인터넷 이용자 수를 대비하여 한국의 사이버범죄로 인한 국가적 피해비용을 추정한 바 있다. 하지만 본 연구에서는 단순히 국가의 GDP 규모나 인터넷 규모를 다른 국가와 비교하지 않고 1인당 GDP와 인구 수, 인터넷 이용자 수가 가장 유사한 국가를 선정하여 해당 국가 대비 한국의 개인정보 유출로 인한 피해비용을 추정 하였다.

우선 해당 보고서를 바탕으로 국가 별로 개인정보 유출로 인한 1건당 피해비용을 정리하였고 해당 국가들의 1인당 GDP와 인구 수, 인터넷 이용자 수를 한국과 비교하여 각각 순위를 매긴 후 순위의 합산이 가장 적은 국가인 이탈리아를 한국과 경제적 환경과 인터넷 환경이 가장 유사한 국가로 선정하였다. 한국의 1인당 GDP와 인구 수, 인터넷 이용자 수를 각각 이탈리아의 값으로 나눈 후 데이터 유출로 인한 건당 피해비용을 곱하여 각각의 단위비용을 산출하여 진행하였다. 마지막으로 조정된 단위 비용을 한국의 2016년 개인정보 유출건수에 곱하여 한국의 개인정보 유출로 인한 총 피해비용을 산출하였다.

V. 산출 결과

본 연구의 산출결과 2007-2016년까지의 개인정보 유출건수는 총 약 4억3천만 건이었으며 개인정보 유출의 최다 발생 시기는 2014년으로 약 2억 건의 유출 사고가 발생하였다.

피해비용 추정결과 A방식인 실거래 평균값 기반은 2009년 최소 약 375만원에서 2014년 최대 약 5,234만원으로 추정되었다. 실거래 평균값 기반의 10개년도 총 추정 액은 약 1,073억으로 나타났으며 과소 추정될 것이라는 예상과 맞게 전체 방법의 추정 방식 중 가장 낮은 추정금액을 보였다.

B방식인 개인 인식 가치 기반 추정결과 2009년

최소 약 9,733억에서 2014년 최대 약 1,524조로 추정되었다. 개인 인식 가치 기반의 10개년도 총 추정 액은 약 3,073조로 나타났으며 전체 방법의 추정 방식 중 가장 높은 추정금액을 보였다.

C방식인 보상금액 기반 추정결과 2009년 최소 약 1억 5,600만원에서 2014년 최대 약 1,100억으로 추정되었다. 보상금액 기반의 10개년도 총 추정 액은 약 3,548억으로 나타났으며 A방식과 B방식의 사이 값으로 A방식에 조금 더 가까운 추정 값을 나타냈다. 현재까지 추정한 A,B,C방식의 자세한 내용은 〔표 5〕과 같다.

마지막으로 D방식인 타 국가 기반 방식은 2016년에 보고된 Ponemon〔20〕보고서를 사용하였기 때문에 2016년의 피해비용만 추정하였다. 타 국가 기반 방식은 우리나라와 1인당 GDP, 인구수, 인터넷 이용자 수가 가장 비슷한 나라인 이탈리아를 선정하여 이탈리아의 개인정보 유출로 인한 피해비용 대비 우리나라의 피해비용을 추정하였다. 타 국가 기반 방식의 추정 결과 우리나라의 개인정보 유출로 인한 피해비용은 1인당 GDP대비 약 4조 7330억으로 추정되었으며 인구수 대비 약 4조 2610억으로 나타났다. 또한 인터넷 이용자수 대비 약 4조 5360억으로 추정되었다. 자세한 내용은 〔표 6〕과 같다.

10개년도 개인정보 유출로 인한 피해비용의 평균액은 연간 107억에서 307조로 추산되었으며 개인정보 유출로 인한 최대 추정 액은 2014년 523억~1524조로 추산되었다. 2016년에는 약 74억~220조의 피해금액이 추산 되었으며 자세한 추정 피해비용 산출결과는 〔표 7〕과 같다.

네 가지 방식의 개인정보 유출 피해비용 산출 모델을 적용해 본 결과 실거래 평균값 기반 방식이 최

Table 5. Output result 1(method A/B/C)

(Unit: thousand won)

Standard year	Total number of personal information leakage by year (Run out)	Personal basis		
		Based on average value A method	Personal perception value base B Method	Based on compensation amount C method
2007	6,000,000	1,500,000	35,959,248,000	6,239,984
2008	23,466,205	5,866,551	148,177,633,067	24,404,792
2009	150,000	37,500	973,396,200	156,000
2010	3,300,000	825,000	22,039,614,300	3,431,991
2011	59,780,828	14,945,207	415,366,040,507	80,371,997
2012	47,212,672	11,803,168	335,261,669,076	46,820,879
2013	397,000	99,250	2,853,831,721	308,879
2014	209,364,707	52,341,177	1,524,839,799,905	110,079,021
2015	50,098,211	12,524,553	367,428,144,893	52,102,009
2016	29,751,923	7,437,981	220,372,136,638	30,941,923
Annual average	42,952,155	10,738,039	307,327,151,431	35,485,748
Total	429,521,546	107,380,387	3,073,271,514,306	354,857,476

Table 6. Output result 2(method D)

(Unit: thousand won)

year	Based on other countries D method		
	Per capita GDP	Population	Internet users
2016	4,733,178,239	4,261,484,543	4,536,052,302

Table 7. Output result 3(Min/ Max estimated amount by year)

(Unit: thousand won)

Standard year	Min / Max estimated amount	
	Min estimate	Max estimate
2007	1,500,000	35,959,248,000
2008	5,866,551	148,177,633,067
2009	37,500	973,396,200
2010	825,000	22,039,614,300
2011	14,945,207	415,366,040,507
2012	11,803,168	335,261,669,076
2013	99,250	2,853,831,721
2014	52,341,176	1,524,839,799,905
2015	12,524,552	367,428,144,893
2016	7,437,980	220,372,136,638
Annual average	10,738,039	307,327,151,431
Total	107,380,386	3,073,271,514,306

소 추정 액으로 나타났고 그 다음 보상금액 기반 방식, 타 국가 기반방식, 마지막으로 개인인식 가치 기반 방식이 최대 추정액으로 나타났다.

VI. 결론 및 시사점

최근 국내에서는 개인정보 유출로 인한 피해가 점점 증가하고 있는 추세이며 개인정보에 대한 중요도와 관심이 점점 커져가고 있다. 특히 개인정보에 대한 범위가 단순 이름, 주민등록, 주소지 등에서 지문, 홍채, GPS 기록 등 그 범위가 점점 넓어짐에 따라 그 중요도는 더욱 증가하고 있는 추세이다. 따라서 본 연구의 목적은 개인정보 유출로 인한 피해비용을 추정할 수 있는 모델을 수립하고 수립한 모델을 통해 개인정보 유출로 인한 개인, 기업, 국가 기준에서의 피해비용을 추정하고 더 나아가 추정 피해비용을 통해 우리나라의 개인정보 유출로 인한 사고의 심각성을 파악하는 것에 그 초점을 맞추었다.

본 연구에서는 개인정보 유출로 인한 피해비용을 개인 기준에서는 실거래 평균값 기반과 개인인식 가치 기반 두 가지 방식으로 산출 진행하였다. 실거래 평균값 기반은 개인정보의 건당 실제 거래액을 해당 연구의 평균값인 250원으로 적용하여 실제 유출건수(N)에 개인정보의 건당 실제 거래액(Vr)을 곱하여 개인정보의 유출 피해비용을 산출하였다. 또한 개인인식 가치 기반방식은 실제 유출건수(N)에 건당 개인이 인식하는 개인정보의 가치(Vp)를 곱하여 개인정보의 유출비용을 산출하였다.

기업 기준의 피해비용 산출방식인 보상금액 기반 방식은 기업의 실제 보상금액과 추정 보상금액의 합계로 산출하였다. 실제 보상액은 개인정보 유출로 인한 건당 보상액에 실제 보상받은 인원의 수를 곱하여 산출하였으며 추정 보상액은 개인정보 유출로 인한 건당 추정 보상액에 추정 보상인원을 곱하여 산출하였다.

국가 기준 피해비용 산출 방식은 타 국가를 기반으로 산출하였으며 IBM에서 진행한 Ponemon보고서를 활용하였다. 국가 별로 개인정보 유출로 인한 1건당 피해비용을 정리하였고 해당 국가들의 1인당 GDP와 인구 수, 인터넷 이용자 수를 한국과 비교하여 각각 순위를 매긴 후 순위의 합산이 가장 적은 국가인 이탈리아를 한국과 가장 유사한 국가로 선정하여 1인당 GDP와 인구 수, 인터넷 이용자 수에 비례하여 한국의 개인정보 유출로 인한 피해비용을 산출 진행하였다.

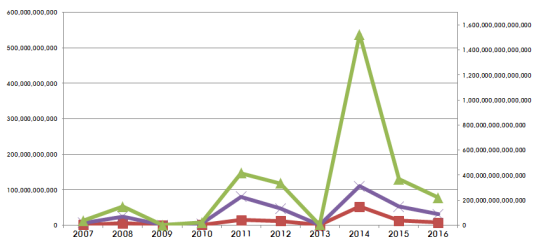

Fig. 6. 10year damage cost calculation graph

개인정보 유출로 인한 피해비용은 2009년이 최소 추정 액이었으며 우리나라 최대 금융회사 개인정보 유출 사고가 있었던 2014년이 최대 추정 피해액으로 나타났다. 2016년의 개인정보 유출로 인한 피해비용은 최소 74억에서 최대 220조로 추산되었으며 10개년도 평균은 연간 약 107억에서 307조로 추산 되었다. 전체 그래프 모습은 〔그림 6〕과 같은 양상을 나타냈는데 개인정보 유출로 인한 추정 피해액이 3년 주기로 상승하는 특이점을 발견할 수 있었다.

본 연구의 한계점은 10년간 이슈가 된 개인정보 유출 사건을 수집하였으나 실제 유출이 되어도 기사화 되지 않은 사건이나 소규모의 사건은 모두 다루어지지 못했다는 한계점이 존재한다. 또한 산출 모델 수립 과정에서 보상금액 기반 산출 방식은 실제로 보상이 이루어진 사례가 극히 드문 관계로 대부분 추정으로 산출할 수밖에 없었다는 한계점이 존재한다.

본 연구에서 제시한 4가지 방식은 그 관점에 따라 비용 산출이 다르게 나올 수 있고 그 범위를 보여주는데 의의가 있다고 볼 수 있다. 어느 방식이 더 정확도가 높고 타당한 가에 대한 것을 전문가나 일반인을 대상으로 인식 조사 등의 향후 연구가 필요하다. 또한, 추후 개인정보 유출로 인한 피해비용은 사회적 비용으로 그 범위를 넓혀 예방 비용, 기회비용 등을 나누어 산출할 수 있을 것으로 기대되며 개인정보의 중요도를 나누어 조금 더 정확하고 구체적인 피해비용 산출이 가능할 것으로 기대한다.

References

〔1〕 Gyoo-Gun Lim, Soon-han Bae, Dae-Chul Lee, Sang-Ho Jie and Seung Ik Baek, "A Development of a Framework for the Measuring National Information Security Level"

Journal of Korea IT Services Society, 12(4), pp. 1-17, Jun. 2014.
〔2〕 Hun-Yeong Kwon, "Information and Communication Security legal system's problems and improvement plan," Journal of the Korea Institute of Information Security & Cryptology, 25(5), pp. 1269-1279, Oct. 2015.
〔3〕 Young-Jin Kim, Su-yeon Lee, Hun-Yeong Kwon and Jong-in Lim, "A Study on the Improvement of Effectiveness in National Cyber Security Monitoring and Control Services," Journal of the Korea Institute of Information Security & Cryptology, 19(1), pp. 103-111, Feb. 2009.
[4] JNSA, "Survey Report on Information Security Incidents", 2014.
〔5〕 Sang-bong Kim, Sie-on Kim and Hyeon-yong Hae, "The situation of personal information leakage and system improvement direction of domestic financial institution, credit card review", 2014
〔6〕 Yun-bae Lee, "The Improvement Method of Internet Ethics Education for the Prevention of Internet Aftereffect," The Journal of the Korea Information and Communications Society, 17(6), pp. 1432-1440, Jun. 2013
〔7〕 Mae-ri Woo, "Internet Dysfunction and Internet Ethics Activation Plan," Theology and ministry, 43, pp. 297-318, May. 2015.
〔8〕 Jeong-in Gwon, Seong-cheol Lee and Seong-jin An, "A Standardizing research of Internet adverse effects catalog from Societal phenomenological pointview," Journal of Computer Education, 14(6), pp. 1-10, Nov. 2011.
〔9〕 Jae-cheol Seo, "A Study on Classification of Dysfunctions of Internet Services," Korean Internet Information Society Conference, pp. 183-184, Oct. 2010.
〔10〕 Hyeong Gang, Gwang-cheol Park, Won-hyeong Park and Gwang-ho Guk, "A Study on Model for Assessment of Economic Damages Due to Cyber Terror," Jouranl of Information and Security, 9(3), pp. 25-33, Sep. 2009.
〔11〕 Jong-ho Jang, Gi-hyeon Jeong, Gyeong-hui Choi and Sang-jung Kim, "A Study on Economic Damage due to Internet Attack," Korean Internet Information Society Conference, 7(2), pp. 573-578, Nov. 2006.
〔12〕 Dubendorfer, T., Wagner, A., and Plattner, B., "An economic damage model for large-scale internet attacks," In Enabling Technologies: Infrastructure for Collaborative Enterprises, WET ICE 2004. 13th IEEE International Workshops on (pp. 223-228). IEEE, Jun. 2004.
〔13〕 Cashell, B., Jackson, W. D., Jickling, M., and Webel, B. "The economic impact of cyber-attacks. Congressional Research Service Documents," CRS RL32331 (Washington DC), Apr. 2004.
〔14〕 Jin Sin, "Economic Analysis on Effects of Cyber Information Security in Korea: Focused on Estimation of National Loss," Journal of The Korea Institute of Information Security and Cryptology, 23(1), pp. 89-96, Feb. 2013.
〔15〕 "Studies on Estimating Methods of Indirect Damage Costs for Personal Information Leak and Avian Influenza," 11-1750140-000001-01, National Disaster Management Research Institute, 2014.
〔16〕 PIPC, "Personal Information Prote-

ction Annual Report", 2012.
〔17〕 Korea Online Privacy Association "Analysis of the value of personal information and social cost due to infringement of personal information", 2013.
〔18〕 Gordon, L. A and M. P, Loeb, Managing Cybersecurity Resources:A Cost-Benefit Analysis, 2005.
〔19〕 JNSA, "Survey Report on Information Security Incidents", 2010.
〔20〕 Ponemon Institute 2016 Cost of Cyber Crime Study: Global
〔21〕 Yeo-ra Gim, Hae-chun Lee and Jin-Hoo Yoo, "A methodology for calculating the value of personal information protection using CVM." Information security issue report, Korea Information Security Agency, pp.1-22, 2007.
〔22〕 Jin-Ho Yoo, Sang-Ho Jie, and Jong-In Lim. "Estimating Direct Costs of Enterprises by Personal Information Security Breaches." Journal of The Korea Institute of Information Security and Cryptology 19(4). pp. 63-75. Aug. 2009.
〔23〕 Hae-chun Lee and Gyeon-gae An. " The evaluation of Personal Information Leakage Loss using the Contingent Valuation Methods. "Productivity Review, 22(2), pp. 1-24, Jun. 2008.
〔24〕 Jin-Hoo Yoo, Sang-Ho Jie, Hye-In Song, Gyeong-ho Jeong and Jong-In Lim. "Estimating Economic Damages from Internet Incidents." Journal of The Korea Institute of Information Security and Cryptology, 19(4), pp. 63-75, Aug. 2009.

〈저자소개〉

임 규 건 (Gyoo-gun Lim) 정회원
1991년 2월: KAIST 전산학과 졸업
1993년 2월: POSTECH 전자계산학과 석사
2001년 6월: KAIST 경영공학(MIS) 박사
2002년 2월: 세종대학교 경영대학 교수
2006년~현재: 한양대학교 경영대학 교수
〈관심분야〉 혁신 비즈니스모델, IT서비스, 정보보호, 지능정보와 지식경영, 디지털콘텐츠 식별체계(UCI), IT 지수 및 성과분석

류 미 나 (Mei-na Liu) 학생회원
2012년 2월: 한양대학교 경영학과 졸업
2016년 3월~현재: 한양대학교 경영정보시스템 석사과정
〈관심분야〉 빅데이터, 데이터마이닝, 정보보호, 지능정보, 혁신 비즈니스모델

이 정 미 (Jung-mi Lee) 학생회원
2014년 8월: 국민대학교 경제학과 졸업
2016년 3월~현재: 한양대학교 비즈니스 인포매틱스 석사과정
〈관심분야〉 빅데이터, 데이터마이닝, 정보보호 지능정보, 혁신 비즈니스모델