Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.1, Feb. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.1.129

FAIR를 통한 개인정보 유출에 따른 기업의 손해금액 산출에 대한 연구

김 정 규,† 이 경 호‡
고려대학교

FAIR-Based Loss Measurement Caused by Personal Information Breach of a Company

Jeong-Gyu Kim,† Kyung-Ho Lee‡
Korea University

요 약

본 연구는 지속적으로 발생하고 있는 개인정보 유출사고에 대한 기업의 리스크와 손해금액 산출을 위해, 최신 리스크 분석방법론인 FAIR(Factor Analysis of Information Risk)를 사용하였다. FAIR를 통해서 실제 개인정보 유출 사고 기업을 예를들어, 손해금액을 분석하고 산출하는 방법론을 제시 하였다. 전문가 집단의 설문을 실시하고 AHP(Analytic Hierarchy Process) 방법론을 사용하여 손해금액 산정요소의 중요도와 적절성을 객관적으로 평가 하였다, 본 연구를 통해서 개인정보보호 실무 담당자는 스스로 손해금액을 최신 리스크 평가 방법론을 통해서 산정하고 입증할 수 있다. 또한 본 연구의 손해금액 산정요소를 해당기업에 맞게 선택하여 정확한 개인정보 유출에 따른 손해금액 등 경제적 손실을 추정할 수 있으며, 사고조치 및 예방대책의 수립과 경영진에게 보고할 수 있는 객관적인 근거를 확보 할 수 있다.

ABSTRACT

This study proposes a methodology to estimate the financial damages by personal information breach of a company and to analyse risk systematically through a case study of a company which experiences private information breach. Using FAIR(Factor Analysis of Information Risk) model, estimate the loss amount and to analyse risk objectively of a company by personal information breach. This study estimates adequacy and importance of corresponding factors applying AHP(Analytic Hierarchy Process) on each factors for assessing loss amount. By adopting proposed methodology in this study, the person in charge of actual work can assess and prove the loss amount though the latest risk estimation methodology. In addition, the person in charge can select the proper parameters for the corresponding company and can obtain the objective quantitative estimation. Hence it can be reported to the management by accurately assessing loss amount caused by personal information breach.

Keywords: FAIR, Personal Information, Personal Information Breach, AHP, Loss Measurement

I. 서 론

1.1 연구 목적

한국인터넷진흥원 개인정보침해센터 신고 접수자료에 의하면 2015년도 개인정보 침해건수는 총 152,151건이다. 정보통신망법 적용범위 내에서는 주민등록번호 등 타인 정보의 훼손·침해·도용에 관한 침해 신고가 77,598건으로 가장 많았으며(전체의 51.0% 차지), 그 다음으로 기술적·관리적 조

Received(11. 21. 2016), Modified(12. 19. 2016), Accepted(12. 27. 2016)

† 주저자, jeonggyu.kim@samsung.com
‡ 교신저자, kevinlee@korea.ac.kr(Corresponding author)

치 미비에 관한 침해신고가 4,006건 발생하였다. 최근 3년간 개인정보유출 피해규모를 보면, 2014년 73개업체 0.3억건, 2015년 13개업체 320만건, 2016년 19개업체 0.1억건의 개인정보 유출 사고가 발생하였다[1].

국내 개인정보 침해, 유출사고는 지속적으로 발생하고 있지만, 세부 발생내역과 규모를 정확히 파악하는 것은 어렵다. 일본의 경우 개인정보 유출사건이 발생하면 이를 공표하는 것이 법률로 정해져 있어, 발생한 사고의 내역을 확인 할 수 있다. 그러나 국내의 경우에는 이러한 법적제도가 마련되어 있지 않고, 관련기관에 신고만 하면 된다. 따라서 민간에서는 정확한 개인정보 유출사고의 규모 및 피해내용, 소요비용 등을 추정 할 수 없다.

지금까지의 개인정보 유출사고로 인한 소요비용 및 피해금액 산출을 위한 논문들은 개인정보 유출사고 기업의 사례를 인터뷰하여 일부 손해금액 요소에 대해 손해금액을 산정하거나, 설문을 통해서 통계 중심으로 분석하였다. 따라서 실제 기업 실무자들이 해당모델을 사용하여 자사의 개인정보 유출금액을 예상, 산정하기에는 무리가 있으며 객관적인 산출근거도 제시가 불가능 하였다.

개인정보 유출사고 발생에 따라 기업은 이미지 실추 및 실질적인 매출감소 등 생사를 좌우하게 된다. 하지만 해당업무 담당자는 객관적인 손해금액 산정방법이 없어 손해비용을 경영층에 효과적으로 설명하지 못한 채 피해복구에만 급급한 실태이다.

사고가 발생하지 않은 기업의 경우, 개인정보 유출에 대한 대책수립 및 투자방향을 결정함에 있어서, 사고발생시 대응을 위한 소요 비용과 유출방지를 위한 보안시설의 보완투자에 대해서 객관적으로 경영층을 설득할 투자 근거를 마련하기 힘든 상황이다.

본 연구에서는 리스크 분석 방법론인 FAIR (Factor Analysis of Information Risk)을 통해서 실제 개인정보 유출사고 기업을 사례로, 리스크를 실제 실무에서 활용할 수 있도록 순차적, 객관적으로 분석하고 손해금액을 산정하는 방법론을 제시한다. 또한 기업 보안책임자에게 설문을 실시한 후, AHP (Analytic Hierarchy Process)분석을 통해, 기업에서 실제 손해금액 산정시, 담당자들이 선택하는 손해금액 산정 요소의 중요도와 적절성에 대한 객관적인 평가를 실시한다.

본 연구를 바탕으로 실무 담당자는 스스로 해당 기업에 맞는 손해금액 산정요소를 중요도에 따라 선택하고 경제적 손해금액을 최신 방법론을 통해서 산정, 입증이 가능하며, 경영진의 의사결정에 도움이 되는 객관적인 사고조치 및 예방 대책을 수립할 수 있다.

1.2 연구 방법

1.2.1 연구 대상

본 연구의 대상은 개인정보 유출사고를 대상으로 한다. 개인정보 유출사고라 함은 “침해사고”와 “누출사고”가 해당된다. “침해사고”는 악성코드, 해킹, 도난 등에 의해 개인정보가 유출된 것을 침해사고 라고 본다. “누출사고”는 조직내부 혹은 협력업체 직원 등에 의해 개인정보가 실수 혹은 고의로 개인정보 처리 단계에서 잘못 처리되거나(시스템 오류 등) 개인정보 주체의 동의없이 제3자에게 제공, 판매되는 경우가 누출사고 이다. 이러한 ”침해사고“와 ”누출사고“의 결과인 ”개인정보 유출“을 연구대상으로 한정 하였다.

1.2.2 연구 단계 및 내용

본 연구는, 현업에서 개인정보보호 업무를 실제 수행한 경험과 사건·사고 대응절차를 가지고, 개인정보 유출로 인한 손해금액 산출을 위한 모델을 수립하고, 객관적인 입증을 위해 3단계로 연구를 수행하려 한다.

■ 1단계: 선행연구 분석
- 기존 연구를 분석, 문제점 및 개선방안 도출
  - 개인정보 유출에 따른 손해금액 산정요소 도출
  - FAIR를 통한 개인정보유출 RISK 분석 연구
  - AHP를 활용한 의사결정 평가방법 연구

■ 2단계: 실제 기업의 개인정보유출 사고 대응단계 리스크를 분석, 손해금액 산출 및 산출요소 개선
- 실제 개인정보유출 사고를 FAIR를 통해 분석
  - 단순 손해금액의 산술적인 합계에서 벗어나 개인정보 유출사고의 빈도, 규모의 가중치를 통한 손해 금액의 발생구간 등 객관적인 분석방법 제시
  - 분석된 리스크에 따른 손해금액 발생요소를 실제 기업에서 활용할 수 있는 객관적인 손해금액을 산출

■ 3단계: 기업 보안책임자의 설문 및 AHP 분석
- FAIR를 통해 분석한 손해금액 산정요소 선정의 중요도와 적절성을 전문가 집단의 설문 및 AHP 방법론을 통해 평가하고, 개인정보유출에 따른 대응 및 손해금액 산출시의 산정요소 선택의 의사결정 우선순위를 제시

II. 선행 연구

개인정보보호법 제2조에 의하면, "개인정보"란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다[2].

또한, 한국인터넷진흥원 개인정보보호 포탈에서는 「정보통신망법」에서 정의하는 개인정보란, 생존하는 개인에 관한 정보로서 성명, 주민등록번호 등에 의하여 특정 개인을 알아볼 수 있는 부호, 문자, 음성 및 영상 등의 정보를 말한다. 개인정보의 주체는 자연인이어야 하며, 법인 또는 단체의 정보는 해당되지 않는다. 개인정보는 개인의 성명, 주민등록번호 등 인적사항에서 부터 사회·경제적 지위와 상태, 교육, 건강·의료, 재산, 문화 활동 및 정치적 성향과, 내면의 비밀에 이르기까지 그 종류가 매우 다양하고 폭 넓게 구분할 수 있다[3].

2.1 손해금액 산출에 대한 선행연구

본 연구에서 채택한 국내외의 개인정보 유출에 따른 손해금액 산정에 대한 연구를 통해서, 리스크 분석을 위해 사용한 최신 방법론인 FAIR에서 필요한 손해금액 산정요소를 실제 현장경험과 기존연구를 바탕으로 도출하였다.

또한, 손해금액 산정에 대한 객관적인 평가를 위한 FAIR 방법론과 손해금액 산정요소의 중요성 및 적절성 평가를 위한 AHP 의사결정론에 대해서, 기존연구를 참조하고, 분석에 활용하였으며, 기존 개인정보 유출에 따른 손해금액 산정방법의 문제점 및 개선방안을 도출 할 수 있었다.

2.1.1 전반적인 손해금액 산출에 대한 연구

Gordon & Loeb(2006)은 기업에서 발생할 수 있는 정보유출사고에 대해서 비용이 얼마나 발생하는지에 대해서 정량적 분석을 통한 표준모델을 제시하였다. 이 연구에서는 간접비용(Indirect Costs), 직접비용(Direct Costs) 및 명시적 비용(Explicit Costs)과 잠재적비용(Implicit Costs)으로 종합적인 분석을 통해서 유출된 개인정보의 가치를 분석하는 모델을 제시하였다[4].

유혜원외(2010)는 정보보호 침해사고로 인한 피해비용을 전자정부서비스 공공기관을 대상으로 Gordon & Loeb(2006)를 응용하여 직접비용, 간접비용, 파생비용으로 구분하였다. 침해사고 발생시점에 따라서 침해사고 기간내에 발생한 비용을 1차적 비용, 이후에 발생한 비용을 2차적 비용으로 구분하고, 계량화 하기 힘든 기업의 이미지 손상, 신뢰도, 주가하락은 논문에서 제외하였다.[5]

한창희외(2011)는 개인정보 유출사고 피해액을 산출하기 위해서 Gordon & Loeb(2006)의 모델 중에서 비용적인 부문만을 고려한 선행연구의 방법을 활용하였다. 가시적인 비용과 비가시적인 비용을 명시적, 잠재적, 간접, 직접기준에 따라 분류하였으며 보안전문연구소인 Information Shild Inc.에서 제시한 피해액 산출요소를 직접적으로 산출이 가능한 비용을 중심으로 대응인건비, IR대응, 고객감소로 인한 수익손실, 유출된 가치의 정보(보상금, 소용비용, 벌금 등)를 피해액으로 산출 하였다[6].

유진호외(2009)는 개인정보 침해사고의 손실비용을 산출하기 위해서 Gordon & Loeb(2006)이 제시한 모델을 바탕으로 직접비용과 간접비용, 명시적 비용과 잠재적 비용으로 구분하였다. 그리고 각각의 항목들을 침해사고 대응비용, 생산성 손실비용, 잠재적인 법적 책임비용을 상세하게 도출하고 2005년부터 2007년까지 발생한 개인정보 침해사고를 대상으로 내용을 분석하여 규모를 산출할 수 있는 방법을 제시하였다[7].

윤장호(2016)는 개인정보 유출사고 발생에 따른 손실측정을 FAIR 방법론을 통해서 분석하였다. 기존에 연구에서는 사고후 손실양의 측정에 대한 연구가 중점을 이루었으나 투자의 의사결정을 위한 손실측정을 사고전에 분석하는 방법으로 리스크를 분석하였다[8].

이희주(2015)는 한국형 원격의료체계의 기술적 안전성 평가를 위해서 개인정보 유출로 인한 피해 시나리오별로 FAIR를 통해서 영업손실, 사고대응 인건비, 소송금액에 대해서 피해규모를 예상, 측정하였

다[9].

김동욱외(2012)는 정보보호정책 및 전략에 대한 우선순위를 제안하기 위해 보안전문가들에게 AHP 계층모델을 통해 설문을 진행하고 이에 대한 가중치 분석을 통해서 정책중요도 측면 및 정책시급성 측면에서는 법제도 정비 및 인적기반 정비가 우선 되어야 한다는 결론을 도출 하였다[10].

김영희(2014)는 개인정보보호법에 따른 개인정보의 안전성확보조치 기준에서 기업에서 행해야 하는 주요 안전조치 항목을 선정하고 이 항목들에 대해서 AHP 기법을 활용하여 중요순위를 정해, 기업이 안전조치를 취할 때 어느 항목부터 우선적으로 시행해야 할지를 제안 하였다[11].

일본의 JNSA(Japan Network Security Association)에서는 기업의 개인정보 유출에 따른 피해액 산정을 위한 보고서를 지속적으로 발표하고 있으며, 정보의 기본가치 추정 모델을 'JO모델'(JNSA Damage Operation Model for Individual Information Leak)로 정하고 가치 추정에 적용 하였다[12].

JO모델에서의 손해배상액은()

= 유출 개인정보 가치 × 정보가 유출된 본래 조직의 사회적 책임도 × 사후 대응평가

JO모델 특징 중 하나는 EP(Economic Privacy) MAP을 활용했다는 것이다. EP MAP의 X축은 정신적 고통, Y축은 경제적 손실도를 나타내며 정보의 민감도를 3단계로 분류하여 유출된 개인정보를 X축의 최대치와 Y축의 최대치로 산정 하였다.

2.1.2 각각의 손해금액 산정요소에 대한 연구

차건상(2011)은 국내외 손해배상 실제 사례를 중심으로 개인정보 분쟁조정위원회의 분쟁 유형별 조정금액 및 판례를 분석 하였다. 국외의 경우에는 개인정보침해의 일종인 개인정보의 노출(Disclosure of Private Fact)에 대해서 실제 판례를 연구 하였다. 설문을 통해손해배상 금액의 수용여부를 개인정보 중요도, 피해규모, 과실 등이 손해배상에 미치는 영향에 따라 손해배상 금액 산정모델을 제시하였다. 연구결과에서는 피해규모는 실제 손해배상 금액의 정도를 결정하지는 않는 것으로 설명 하였다[13].

김정연(2013)은 개인정보 유출에 따른 주가변동이 발표 당일과 함께, 발표 다음날까지도 부정적 영향이 남아 있는 것을 볼 수 있다고 분석하였다. 오히려 변동 폭은 발표 다음날이 더 확실한 음의 영향을 보여준다고 하였다. 2010년 이후 발생한 개인정보유출의 경우, 개인정보보호법의 시행 및 정보통신망법상 개인정보 규제강화에 따라 영향을 받는 개인정보의 대상이 증가하고 소송으로까지 이어지는 등 사회적으로 큰 관심을 끄는 사고의 경우에는 주가에 장기적이고 크게 영향을 받는 사례가 더욱 많아졌다고 하였다[14].

홍일유외(2015)는 2008년부터 2013년까지의 대형 개인정보 유출사고 11건에 대해서 사고발표 시점에서 +5일에서 -5일간의 기간동안 기업의 주가패턴을 바탕으로 "비정상 수익율", "누적 비정상 수익률"을 분석결과, 사고기업의 비정상수익률은 코스피(닥)의 등락과 상관없이 독립적인 영향을 미치는 것을 확인 하였으며 특히, 사고발표 +1일에는 최대의 부정적인 영향을 미친다는 것을 도출 하였다[15].

2.1.3 미국 포네몬(Ponemon)연구소의 개인정보 유출시 피해금액 산정에 대한 연구

포네몬은 7년전 미국에서 최초로 사이버 범죄비용 연구를 시작으로 영국, 독일, 호주 및 일본에서 연구를 실시 하였다. 2015년에는 IBM과 포네몬 연구소가 11개국(미국, 영국, 독일, 호주, 프랑스, 브라질, 일본, 이탈리아, 인도, 아랍지역, 캐나다), 350개 기업 관계자와 진행한 인터뷰를 통해 데이터 유출(개인정보)에 대한 경제적 피해규모 비용을 연구하였다[16].

포네몬의 조사에 따르면, 11개국 표본기업의 데이터 유출에 대한 주요 근본 원인은 아랍지역 기업의 경우 악의적인, 범죄목적의 공격이 56%로 가장 높으며 인도와 브라질 기업은 동일한 형태의 데이터 유출 가능성이 가장 낮다. 하지만 인도의 기업은 시스템 오작동이나 비즈니스 프로세스 실패로 데이터가 유출될 가능성이 가장 높다. 브라질과 호주의 기업에서는 인적오류로 인한 데이터 유출 가능성이 가장 높은 것으로 확인 됐다.

2015년 미국 포네몬 보고서에서는 연간 개인정보 유출 사건의 기록당 소요비용과 직접, 간접비용, 연간 총 피해비용, 기업별/조사대상 산업별 피해비용, 각각의 항목별 소요비용 등을 다루고 있다. 포네몬 보고서는 유출로 인한 손해금액 산출을 위해 사고의 단계를 탐지(Detection), 확대(Escalation), 통지

(Notification), 사후대응(Post data breach)의 단계로 나누어 손해금액을 산출하고 있으며 단계별 발생하는 비용에 대해서는 아래와 같이 설명하고 있다[17].

- 탐지/탐색: 기업에서 위험한 상태 또는 전송중인 개인데이터의 유출의 탐지활동
- 확대: 지정된 기한내에 해당책임자에게 보호대상 정보의 유출을 보고하는데 필요한 활동
- 통지: 기업에서 데이터 주체에게 우편, 전화, e-메일, 일반통지를 통해 정보의 분실 또는 도난사실을 알리기 위한 활동
- 사후대응: 유출 피해자가 잠재적 피해를 최소화하기위해 해당기업과 연락하여 추가질문을 하거나 조언을 받을 수 있게 하는 활동
  (신용 변동 모니터링, 신규계정(신용카드) 재발급 등)

위에서 열거한 단계별 피해금액을 산출하기 위해 포네몬에서는 아래와 같이 세부항목을 제안하였다[18].

Table 1.를 통해서 실제 기업에서 개인정보 유출 사고 발생으로 인한 어떤 비용이 소요 되었음을 추정할 수 있다. 잠재적으로 가장 큰 경제적인 영향을 미치는 비즈니스 상실요소는 꾸준히 증가해 왔으며 비정상적인 고객 이탈, 고객확보의 어려움 증가, 평판 하락, 영업권 감소 등이 포함된다. 사후대응 및 탐지 관련 비용도 3년간 계속 증가하고 있으며 사후비용에는 고객응대, 조사 활동, 법적비용, 제품할인, 신원보호 서비스, 감독기관의 개입 등이 포함된다.

Table 1. Actual damage amount ratio of each factors for estimating loss amount

(Unit : %)

Cost Item	'05	'06	'07	'08	'09
Investigation cost	8	8	8	9	8
Consulting/Audit cost	8	10	10	11	12
Customer contact cost	13	9	7	6	6
Cost to respond customer request	15	10	8	6	5
Advertisement cost	0	1	3	1	1
Legal cost-defense	5	6	8	9	14
Legal cost-cost for adjudication of implementation	3	3	3	1	2
Cost for free/discounted service	4	2	1	2	1
Cost for defending brand value	3	3	2	2	2
Loss from declining sales (Customer secession)	35	39	41	43	40
Cost for acquiring new customers	6	8	9	9	9

탐지 및 확대관련 데이터 유출비용에는 분석 및 조사활동, 평가 및 감사서비스, 재해관리, 경영진 및 이사회와의 커뮤니케이션 등이 포함된다.

통지관련 활동은 데이터 유출비용요소 중 비중이 가장 적으며 여기에는 주로 연락처 데이터베이스 구축을 위한 IT 활동, 모든 규정 요건 확인, 외부 전문가 채용, 우편비용, 우편/이메일수신 불가시 대체 연락처 등이 포함됩니다.

포네몬 보고서에는 데이터 유출 관련비용을 계산하기 위해 활동기 준비비용산정(activity-based costing)이라는 방법론을 적용하여 각종 활동을 파악하고 실제사용에 따른 비용을 부여한다.

2015년 벤치마크 조사에 포함된 기업들은 데이터 유출을 탐지하고 즉각적으로 대응하기 위해 일반적으로 다음과 같은 활동을 수행한다.

- 데이터 유출 근본원인 규명을 위한 조사 및 분석
- 데이터 유출의 잠재적 피해자 확인
- 사고대응팀 조직
- 커뮤니케이션 및 PR 활동수행
- 데이터유출 피해자 및 감독기관에 전달할 통지문서 및 기타 필수 공개자료 작성
- 콜센터 절차 및 전문교육 이행

데이터 유출을 발견한 후에는 일반적으로 다음과 같은 활동을 수행한다.

- 감사 및 컨설팅서비스
- 방어를 위한 법률서비스
- 컴플라이언스를 위한 법률서비스
- 유출 피해자에 대한 무료 또는 할인서비스
- 신원보호 서비스
- 고객이탈 추정치에 근거한 고객 비즈니스 상실
- 고객확보 및 우수 고객 프로그램 비용

포네몬 보고서에서는 기업에서 이런 활동에 대한 비용범위를 직접비용, 간접비용, 기회비용으로 분류하였다.

- 직접비용: 특정 활동 수행시 소요되는 비용
- 간접비용: 직접적인 자금지출은 아니지만 투입되는 시간, 노력, 등
- 기회비용: 데이터유출이 고객에게 통지, 공개된 후

인지도 저하로 인한 비즈니스 기회상실

포네몬 보고서는 개인정보 유출시 대응 단계별 소요비용을 실제 기업담당자간 인터뷰를 통해서 산출하였으며, 이에 대해 국가별, 기업군별 통계자료를 제공하고 있다.

III. FAIR를 통한 개인정보유출시 손해금액의 산정 및 RISK 분석

본 연구에서는 개인정보유출에 대한 손해금액에 대한 리스크를 FAIR 방법론을 통해서 단계적으로 새롭게 접근하려 한다. FAIR(Factor Analysis of Information Risk)는 2005년 Risk Management Insight LLC의 Jack Jones에 의해서 제안되었으며 FAIR의 기본은 "FAIR ISO/IEC 27005 cook book"에 방법론이 소개되고 있다[19]. FAIR의 특징은 리스크가 발생할 수 있는 가능성을 시나리오에 따라 분석하고 정량적으로 측정할 수 있으며 이를 바탕으로 기업에서 개인정보 유출을 방지하기 위한 대책 수립시 의사결정 수단으로 활용이 가능하다.

본 연구에서는 FAIR 단계별 RISK 분석방법론을 통해서 개인정보유출로 인한 손해금액의 산정모델을 제시한다. 기존 연구들은 손해금액 산정요소 중 일부 중요 요소의 합계 혹은 산정요소별 적절성 평가에 대한 연구이거나 개인정보 유출기업의 설문을 통해서 비용을 산정요소의 산출합계 방식으로 손해금액을 산정 하였다.

본 연구에서는 실제 개인정보가 유출된 기업을 사례를 들어서 FAIR를 활용하여 단계적으로 개인정보 유출에 따른 실제 기업의 리스크를 객관적으로 분석하고 손해금액을 산출하는 방법과 가이드를 제시하려고 한다.

따라서, 본연구를 통해서 기업의 실무자는 개인정보 유출에 대한 손해금액 산출을 FAIR를 통해 실질적으로 이해하고 타 사례에 충분히 적용 가능하게 된다. 또한 사고조치 계획 수립 및 예방을 위한 대책에 대한 논리적인 근거를 확보할 수 있다.

□ FAIR의 단계별 리스크 분석 및 손해금액 산정방법

- 1단계: 개인정보유출 사고 시나리오 구성, 자산식별
  - 해당 사고의 자산 및 사고 발생 위협을 식별
  - 기존 개인정보 유출사고를 통한 시나리오를 구성
- 2단계: 해당사고의 LEF를 산출
  - TEF, TCAP, RS를 산출
  - TCAP과 RS를 통해 Vulnerability를 산출
  - LEF, SLEF를 구함
- 3단계: 해당사고의 PLM과 SLM을 산출하여 PR, SR을 산출
- 4단계: Overall Risk 산출하여 개인정보유출 사고로 인한 손해금액 산정

FAIR의 기본개념 파악을 위해 FAIR에서 사용하는 기본 용어를 정의하면, 아래와 같다[20].

TEF는 자산에 대해서 위협을 가하는 시도의 수이다. TCAP는 자산에 대해서 위협을 가하는 능력의 가능성으로 TCAP가 높으면 위협을 가하는 개체의 능력이 높다고 판단할 수 있다.

RS는 위협에 대해 자산이 자산 스스로를 방어하고 지킬 수 있는 역량이다. Vulnerability는 자산이 취약한 정도로 TCAP와 RS로 산출한다. TCAP이 높으면 위협이 높아지므로 Vulnerability가 높아지고 RS가 높으면 자산의 자기방어력이 높으므로 Vulnerability가 낮아진다.

LEF는 주어진 기간동안 위협요소가 자산에 피해를 주는 발생 빈도를 말하며 TEF와 Vulnerability에 의해서 결정된다. SLEF는 자산의 간접손실이 발생하는 횟수이며 PLM은 자산의 피해에 직접적으로 받는 손해비용이다.

SLM은 자산의 손실에 따라 간접적으로 발생하는 손실이며 PR은 자산의 손실에 따라 직접적인 위험이고, SR은 간접적인 위험을 말한다. OR은 PR과 SR을 고려하여 산정된 총 위험을 말한다.

Table 2. Acronyms of FAIR

Name	Acronyms
Threat Event Frequency	TEF
Threat Capability	TCAP
Resistance Strength	RS
Vulnerability	-
Loss Event Frequency	LEF
Secondary Loss Event Frequency	SLEF
Primary Loss Magnitude	PLM
Secondary Loss Magnitude	SLM
Primary Risk	PR
Secondary Risk	SR
Overall Risk	OR

Table 3.은 FAIR에서 위험도를 도출하기 위해 사용하는 matrix 방법으로, Vulnerability는 TCAP과 RS, 두개의 변수에 의해 결정되며 TCAP가 H(high)이고 RS가 VH이면 Vulnerability는 L(Low)의 의미이다.

Fig. 1.는 FAIR의 분석 프로세스를 보여주는 그림으로 빈도 부분과 손실부분으로 나누어져 있고 모든 컴퍼넌트들은 5단계로 구분되어 있다[20].

Table 3. Matrix method of FAIR

TCAP						
	VH	VH	VH	VH	H	M
	H	VH	VH	H	M	**L**
	M	VH	H	M	L	VL
	L	H	M	L	VL	VL
	VL	M	L	VL	VL	VL
VUL		**VL**	**L**	**M**	**H**	**VH**
		RS				

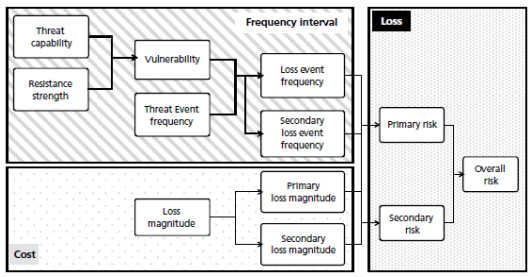

Fig. 1. FAIR risk analysis process

3.1 1단계 : 개인정보 유출사고 시나리오 구성 및 자산의 식별

본고에서는 2011년7월21일 중국 해커의 공격을 받아 개인정보가 유출된 SK커뮤니케이션즈(이하 'SK컴즈')가 운영하는 싸이월드와 네이트의 사례를 활용하려 한다.

해당사고는 약 3,500만명 회원의 개인정보가 유출된 사고로써, 본 사고에 대해 사고대응 단계별 손해비용 산정요소를 도출하고 사고발생에 따른 손해금액 리스크를 FAIR 방법론을 통해서 분석한다.

3.1.1 SK컴즈 사고관련 자산식별

SK컴즈 사고의 소송 판결문을 바탕으로 해당 판결문내에 해킹 경로, 방법 및 보안장비에 대해

Table 4. List of asset at the moment of accident

Division	Description
PC	DB technology team PC
Server	DB Members information DB
	Members information DB server
N/W equipment	Gateway
	Router
Security equipment	Firewall
	Intrusion blocking system
	DLP system
	Virus, Malicious code detection system
Software	Vaccine program
Private information	34,954,887 member information
Related Person	System administrator etc.

Table 4.과 같이 언급된 자산을 식별 하였다.

해당자산은 실제 운용자산과 상이할 수 있으나 보안사고와 직접적인 연관이 있는 자산을 식별하여야 실제 보안 리스크의 정도를 산정할 수 있다. 해당 자산을 식별은 위협의 대상을 파악하고 취약도를 산정하는 등 리스크 관리를 위한 핵심 요소이다.

3.1.2 위협자 프로파일링

자산에 대한 위협을 끼칠 수 있는 위협자를 프로파일링 한다. 본 사고는 신원미상의 중국 해커가 개인정보를 유출하여 금전적 이익도모를 목적으로 해킹

Table 5. Profiling for intimidator

Intimidator	Chinese hacker		
Reson for selection	Private information breach by malicious method to hack		
Motive	Intend to profit from private information breach		
Major intention	Intend to breach private information by connecting customer DB through installing malignant code in SK employee's PC by hacking		
Preferred target	Private information in DB server		
Ability	Skillful hacker who is able to make malignat code and to process DB		
Degree of Danger	Min.	Aver.	Max.
	80	90	95

을 하였다.

위험정도를 최대 100으로 보고 10단계로 분류하여 볼 때 해당 해커는 악성코드 제작이 가능하고 DB 명령어를 조작할 수 있는 것으로 판례에 명시되어 있다.

따라서, 위험도는 Table 5.와같이 80정도이며 최고 95정도의 위협을 끼칠 수 있을 것으로 추정 하였다.

3.1.3 SK컴즈 사건 시나리오 요약

① 중국 해커(신원미상)가 공개용 알집 업데이트 서버를 해킹하여 악성코드를 업로드
② 공개용 알집을 사용하던 SK컴즈의 직원이 해커가 업로드한 악성프로그램을 내려 받아 키로깅 프로그램에 감염 됨(DB기술팀 직원 PC)
③ 해커가 해당 PC에 원격 접속하여 키보드 로거를 사용, DB접속 아이디와 패스워드를 탈취
④ 해커가 탈취한 정보로 DB에 접속하여 고객 정보를 덤프 파일로 저장
(유출된 개인정보: ID, 비밀번호, 주민등록번호, 성명, 생년월일, 성별, 이메일주소, 전화번호, 주소, 닉네임)
⑤ 좀비 PC에서 FTP를 사용하여 34,954,887건의 개인정보 덤프파일을 해커 시스템으로 업로드

3.2 2단계 : 해당사고의 LEF를 산출

3.2.1 TEF, TCAP의 산출

- TEF(Threat Event Frequency)의 산출

TEP의 산출을 위해서 포네몬연구소의 2015년 사이버 범죄비용 연구보고서를 참조하였다[21]. 252개 업체에서 발생한 사이버 공격중 SK컴즈와 같은 악성코드 공격방식에 따라 사고가 발생한 확률을 59%로 보았다. 따라서 TEF 측정을 위해 등급기준표 Table 6.을 작성하여 참조하면 Moderate(M)이다.

- TCAP(Threat Capability)의 산출

3.1.2에서의 위협자 프로파일링에서 분석한 바와 같이 SK컴즈를 공격한 해커는 악성코드를 스스로 제작하여 백신 업데이트 서버를 해킹, 키로거 프로그램을 사용하여 DB까지 접근한 역량을 가지고 있으므로 위협자 역량에 따른 아래의 Table 7.의

Table 6. Table of criteria for TEF

Rating	Description
Very High(VH)	81~100%
High(H)	61~80%
Moderate(M)	41~60%
Low(L)	21~40%
Very Low(VL)	0~20%

TCAP 등급기준표에 따라 High(H) 이다. 해커의 레벨정의는 해커수준 분류관련 논문[22]을 참조 하여 TCAP 등급기준표를 작성 하였다.

Table 7. Table of criteria for TCAP level

Rating	Description
Very High(VH)	Discover new weak spot, Implementation of hacking codes
High(H)	Able to apply announced hacking code to target system
Moderate(M)	Able to modify existing hacking code and understand hacking method
Low(L)	Able to attack by using existing hacking code verbatim
Very Low(VL)	Able to execute simple hacking command and hacking program

3.2.2 RS 및 Vulnerability를 산출

- RS(Resistance Strength)를 산출

RS는 자산이 스스로를 방어할 수 있는 역량으로 SK컴즈 사고의 경우, 해커의 의도대로 감염된 악성코드를 보안시스템에서 전혀 탐지를 못했다,

또한, 해커가 덤프한 DB에 대한 유출탐지 및 DB 접근통제 등도 미흡 하였으므로, Table 8.의 RS에 등급기준표에 따라 Very Low(VL)이다.

- Vulnerability(VUL)를 산출

VUL은 TCAP와 RS로 구한다. TCAP가 H이고 RS가 VL이므로 VUL은 Table 9.와 같이 VH이다

Table 8. Table of criteria for RS level

Rating	Description
Very High(VH)	Able to defend against upper 5% attack
High(H)	Able to defend against upper 15% attack
Moderate(M)	Able to defend against average threat
Low(L)	Able to defend against low 15% attack
Very Low(VL)	Able to defend against low 5% attack

Table 9. Table of VUL generation

T C A P	**VH**	VH	VH	VH	H	M
	H	**VH**	VH	H	M	L
	M	VH	H	M	L	VL
	L	H	M	L	VL	VL
	VL	M	L	VL	VL	VL
VUL		**VL**	**L**	**M**	**H**	**VH**
		RS				

3.2.3 LEF, SLEF의 산출

- LEF의 산출

LEF는 TEF와 VUL의 결과로 도출한다. TEF는 M이며 VUL은 VH이므로 Table 10. LEF 등급기준표를 참조 하여 LEF를 산출하면 M이다.

LEF는 주어진 기간동안 위협요소가 자산에 피해를 주는 발생 빈도이므로 확률구간으로 표시가 가능하다.

따라서 LEF는 Table 12.의 SLEF 와 같이 M이므로 30%~70% 확률로 발생한다

Table 10. Table of LEF generation

T E F	**VH**	M	H	VH	VH	VH
	H	L	M	H	H	H
	M	VL	L	M	M	**M**
	L	VL	VL	L	VL	VL
	VL	VL	VL	VL	VL	VL
LEF		**VL**	**L**	**M**	**H**	**VH**
		VUL				

- SLEF의 산출

SLEF는 TEF와 Secondary Loss Event(SLE)가 일어날 확률(SLE%)로 산출 한다. TEF는 M이며 SLE%는 개인정보 유출사고 발생시 직접비용과 함께 필수적으로 발생함으로 VH이다.

따라서 SLEF는 Table 11. SLEF 산출표에 따라서 M으로 산출할 수 있다. 따라서 SLEF는 Table 12.의 M의 구간인 30%~70% 확률로 발생한다.

Table 11. Table of SLEF generation

T E F	**VH**	M	H	VH	VH	VH
	H	L	M	H	H	H
	M	VL	L	M	M	**M**
	L	VL	VL	L	VL	VL
	VL	VL	VL	VL	VL	VL
SLEF		**VL**	**L**	**M**	**H**	**VH**
		SLE%				

Table 12. Table of SLEF range

Rating	Range Low End	Range High End
Very High(VH)	90%	100%
High(H)	70%	90%
Moderate(M)	30%	70%
Low(L)	10%	30%
Very Low(VL)	0%	10%

3.3 3단계 : 해당사고의 PLM과 SLM을 산출하여 PR, SR을 산출

3.3.1 PLM과 SLM의 산출

기업에서 사고 발생 대응단계별로 손해금액이 발생하며 비용구분을 직접손해금액, 간접손해금액의 구분은 선행연구의 포네몬 보고서[17]와 저자가 실제 현장에서 경험한 내용를 사용하였다.

- 직접 손해금액: 사고 조치, 대응을 위한 직접비용
- 간접 손해금액: 직접적인 자금지출은 아니지만 사고 발생으로 인한 손해금액

포네몬에서 조사한 세부 항목별 피해 비용 분석결과를 토대로 Table 15.의 2011년, 2012년 개인정

Table 13. Content of PLM and SLM for estimating loss amount

Level	Direct Loss Amount (PLM)	Indirect Loss Amount (SLM)
Cost for urgent response	· Cost for accident investigation and personnel expenses for corrective measure · Operation cost for call center · Expenses for notification to customers · Urgent investment for security	· Cost for advertisement (IR response)
Legal cost	· Various litigation expenses	· Fine payment/ penalty payment · Indemnification for damages
Cost for post-accident	· Cost for recurrence prevention (IT·Security Facilities investment/ consulting)	· Drop of sales · Decrease of stock value

보 유출사고 주요 손해금액을 분석 하였다.

전체 손해금액 중 평균적으로 사고조사 및 조치 인건비가 약 18%, 홍보비용이 15%, 법적 비용은 10%, 콜센터 운영 및 사고통지비용 17%, 고객 이탈로 인한 수익감소 등 매출손해금액이 40% 정도를 차지하는 것을 알 수 있다[23].

손해 배상비용, 과태료 및 벌금과 주식가치 하락에 따른 간접 손해금액은 포네몬 조사결과에서는 제외 되어 있지만, 최근의 개인정보 유출사례를 통해서 비용이 발생함을 확인 할 수 있다. 이중 개인정보위원회 보고를 위한 연구보고서(개인정보의 가치와 개인정보 침해에 따른 사회적 비용 분석)는 Table 15.와 같이 주요 손해금액을 산정 하였다[23].

손해금액 중 PLM과 SLM을 산정하기 위한 손해규모 등급표를 산정하는 방법은, 직접손해금액과 간접손해금액이 각각 차지하는 비율을 조사한 포네몬 조사결과인 Table 1.의 세부 항목별 피해비용 비율 2005년 ~ 2009년을 활용하여 직접손해금액과 간접손해금액의 비용을 추정할 수 있다. PLM 및 SLM 산정을 위한 각각의 손해규모 등급표는 아래와 같다.

- PLM의 손해규모 등급

Table 14. Level of PLM loss amount [unit: won]

Rating	Range Low End	Range High End
Very High(VH)	10 billion	More than 10 billion
High(H)	7 billion	9.9 billion
Moderate(M)	5 billion	6.9 billion
Low(L)	2.1 billion	4.9 billion
Very Low(VL)	0	2 billion

- PLM의 산출

SK컴즈에 대한 직접손해금액을 Table 15.를 기반으로 산정하면, 대응인건비가 43억원(18%)이므로 상대적으로 법적비용은 10%로 24억원, 콜센터 운영 및 사고통지비용은 17%로 40억원이 소요되었다고 추정할 수 있다. 재발방지를 위한 IT 및 시설보안투자 비용을 제외해도 107억으로 PLM의 손해규모 등급은 Table 14.와 같이 VH이다.

- SLM의 산출

SK컴즈에 대한 간접손해금액을 Table 15.를 바탕으로 산정하면, 홍보비는 36억원, 매출 등 기업손실은 61억원이며 과태료 및 벌금은 없다.

하지만, 법적 손해배상금액은 2013년 2월, 서울서부지방법원의 판결에 따라 인당 20만원을 2,882명에게 지급하여야 하므로 5.7억원 규모이나 실제 본소송을 근거로 개인정보가 유출된 3,500만명 중 5%만이 소송을 한다고 예상했을 때 3,500억원의 손해금액이 발생하며 1%가 소송에 참여할 경우에는 700억원 규모이다.

따라서 본고에서는 2%가 소송에 참여한다고 하였을 때 손해배상 비용은 1,400억원이며 간접손해금액의 총합은 1,497억원으로 추산할 수 있고, SLM의 손해규모 등급은 Talble 16.과 같이 VH이다.

Table 15. Major personal information breach accident presumed loss amount

Company	Breach amount (million)	Personnel expenses	IR response	Drop of sales	Total
Hyundai Capital	175	₩5,747,503,079	₩4,765,961,138	₩130,495,361,111	₩1,141,008,825,328
Hanhwa Insurances	16	₩5,446,916,861	₩4,516,708,165	₩15,500,000,000	₩25,463,625,027
Leading Investment Securities	26	₩1,196,812,823	₩992,294,176	₩4,030,000,000	₩6,219,106,999
SK comms.	3,500	₩4,329,062,539	₩3,588,968,981	₩6,113,200,000	₩14,031,231,520
EPSON	35	₩3,062,664,048	₩2,538,959,184	₩5,735,000,000	₩11,336,623,232
Nexon	1,320	₩4,086,082,961	₩3,387,529,024	₩34,317,000,000	₩41,790,611,985
2011 Total		₩23,869,042,312	₩19,790,420,669	₩196,190,561,111	₩239,850,024,091
KT	873	₩4,458,808,988	₩3,696,098,414	₩160,959,898,800	₩169,114,806,202
EBS	420	₩3,148,095,296	₩2,610,407,996	₩3,540,200,000	₩9,298,703,292
2012 Total		₩7,606,904,283	₩6,306,506,410	₩164,500,098,800	₩178,413,509,494

- SLM의 손해규모 등급

Table 16. Level of SLM loss amount (unit: won)

Rating	Low End	High End
Very High(VH)	1,00 billion	More than 100 billion
High(H)	70 billion	100 billion
Moderate(M)	50 billion	69.9 billion
Low(L)	30 billion	49.9 billion
Very Low(VL)	0	29.9 billion

3.4 4단계: Overall Risk 산출하여 개인정보유출 사고로 인한 피해금액 분석

Risk는 PR(Primary Risk), SR(Secondary Risk)과 PR과 SR을 통해 OR(Overall Risk)를 산출할 수 있다.

PR은 Table 17.과 같이 PLM이 VH이고 LEF가 M이므로 PR기준에 의해 VH이다. SR은 Table 18.과 같이 SLM이 VH이고 SLEF가 M이므로 SR 기준에 따라 VH이다.

OR은 PR이 VH이고 SR이 VH이므로 OR 기준에 의해 Table 19.와 같이 VH이다.

Table 17. Table of PR generation

P L M	**VH**	M	H	**VH**	VH	VH
	H	L	M	H	VH	VH
	M	VL	L	M	H	VH
	L	VL	VL	L	M	H
	VL	VL	VL	VL	L	M
PR		**VL**	**L**	**M**	**H**	**VH**
		LEF				

Table 18. Table of SR degree generation

S L M	**VH**	M	H	**VH**	VH	VH
	H	L	M	H	VH	VH
	M	VL	L	M	H	VH
	L	VL	VL	L	M	H
	VL	VL	VL	VL	L	M
SR		**VL**	**L**	**M**	**H**	**VH**
		SLEF				

Table 19. Table of OR generation

SR	**VH**	VH	VH	VH	VH	**VH**
	H	H	H	H	VH	VH
	M	M	M	H	H	VH
	L	L	L	M	H	VH
	VL	VL	L	M	H	VH
OR		**VL**	**L**	**M**	**H**	**VH**
		PR				

정량적인 Risk는 Loss에 확률구간을 곱하는 것으로 구한다. 확률구간은 앞서 LEF 산출시 확률구간을 구했으며 이를 활용하여 OR를 구하면 된다.

- 최대, 최소 손해금액 산정방법(Table 20.)

Table 20. Method for estimating loss amount (Maximum value, Minimum Maximum)

Item	Amount	probability range		Expected value of damage
PLM	A	MAX	α	A×α
		MIN	β	A×β
SLM	B	MAX	α″	B×α″
		MIN	β″	B×β″

- 최종 손해금액 규모 산정방법(Table 21.)

Table 21. Method for estimating final loss amount

Maximum value	Minimum value
(A×α) + (B×α″)	(A×β) + (B×β″)

따라서, FAIR를 통해 SK컴즈 개인정보 유출사고의 최대 손해금액과 최소 손해금액을 구하면 Table 22.와 Table 23.과 같다.

SK컴즈의 직접 손해금액(PLM)은 107억이며, 간접 손해금액(SLM)은 1,436억으로 총 손해금액은 1,543억으로 분석되었다.

또한 Risk 분석결과에 따라 PLM과 SLM이 VH로 나타났으므로 손해금액 발생구간을 0.9 ~ 1.0을 적용하면 최소 손해금액은 1,388억이며 최대 손해금액은 1,543억이 발생함을 할 수 있다.

따라서, 본 연구에 따른 방법론을 사용하면 SK컴즈의 사례를 통해서 분석된 결과와 같이 직접/간접 손해금액과 총 손해금액의 발생구간의 예측이 가능하다.

Table 22. Primary, Secondary loss amount
〔unit: 10 thousand won〕

Risk Type	Confi-dence	FRE.	LOSS
Primary	VH	0.9~1.0	1,070,000
Secondary	VH	0.9~1.0	14,360,000

Table 23. Maximum and minimum value of primary, and secondary final loss amount
〔unit: 10 thousand won〕

Risk Type	Min Loss	Max Loss
Primary	963,000	1,070,000
Secondary	12,924,000	14,360,000
Total	13,887,000	15,430,000

위와같이 FAIR를 통해서 기업의 개인정보 유출사고를 각각의 리스크 산출 항목들에 대해서 순차적으로 논리적으로 분석하고, 개인정보 유출사고 손해금액의 최소값, 최대값으로 도출하였다.

기업의 개인정보담당자는 본 연구결과를 통해서 손해금액에 대한 FAIR를 활용한 순차적 리스크 분석방법에 따라 리스크를 경영층에 객관적으로 설명할 수 있다. 또한 해당기업에서 취급하는 개인정보의 유출에 따른 손해금액 발생구간을 예측하여 개인정보 보호대책을 수립할 수 있다.

IV. AHP를 통한 손해금액 산출항목 선정에 대한 객관성 주요도 판단

4.1 AHP를 통한 분석단계

AHP(Analytic Hierarchy Process)는 다기준 의사결정 문제에서 평가기준과 대안을 계층적인 구조로 파악하여 최적 대안을 선택하는 의사결정 방법론으로 Thomas Saaty(1980)에 의해 개발되었다〔24〕.

본 연구에서는 보안책임자급 전문가들에게 설문을 실시하고, FAIR를 통해 산출한 개인정보 유출에 따른 손해금액 산정요소의 중요도와 적절성 판단을 위해서 AHP 분석을 실시하였다.

설문 및 분석 대상항목은 Table 13.에서 언급한 직접손해금액(PLM)과 간접손해금액(SLM)에 대한 긴급조치비용, 법적비용, 사후발생 손해금액 산정요소 13가지이다. AHP 분석은 아래와 같이 3단계로 방법으로 실시하였다.

- 1단계: 손해금액 분석시 산정요소에 대해 AHP 계층모델을 수립
- 2단계: 1단계의 계층모델을 바탕으로 회사 계열사별 보안책임자를 대상으로 설문조사를 실시

- 3단계: 설문결과에 따라 AHP 분석 툴로 가중치를 도출하고 손해금액 산정요소의 중요도 및 적절성을 평가

4.2 AHP 계층모델 수립(1단계) 및 설문 실시(2단계)

4.2.1 AHP 계층모델 수립

AHP 분석을 위해 손해금액 산정시 선정한 13개 요소를 Fig. 2.와 같이 1, 2 계층으로 구분하였다. 1계층은 긴급조치비용, 법적대응비용, 사후발생비용이다.

2계층은 긴급조치 비용관련 항목은 "사고조사·조치 인건비, 홍보(IR대응)비용, 고객통지비용, 콜센터 운영비, 긴급IT/시설투자 비용"이다.

법적대응 비용에는 "각종 소송비용, 고객손해배상비용, 과태료/벌금/과징금" 이다. 사후발생 비용은 "주식가치 하락손해, 매출감소, 컨설팅비, 재발방지 IT투자 및 재발방지 시설투자 비용으로 구분하였다. 이를 토대로 작성된 AHP 계층 모델은 아래의 Fig 2.과 같다.

4.2.2 AHP 분석을 위한 설문실시

Fig. 2.의 AHP 계층모델을 바탕으로 설문지를 작성하고 제조, 금융, 서비스, 유통 분야에서 근무하고 있는 보안책임자 23명에게 설문을 실시하였다.

설문을 통해서 손해금액 산정요소의 중요도 및 쌍대비교를 실시 하였으며, 각각의 1, 2계층의 쌍대비교 결과를 AHP 분석 전문 프로그램인 Export Choice 2000을 통해서 분석하였다.

쌍대비교 분석결과, CR(Consistency Ratio)값을 통해 일관성검사를 실시하였다. 검사결과 23개의 설문중 CR 값이 0.1 이상인 3건의 설문결과는 일관성이 떨어지는 것으로 판단되어 결과분석에서 제외하였다[24].

분석에 사용한 CR값이 0.1 이하인 20건 설문의 각각의 쌍대비교에 대한 CR값의 평균은 0.03이다.

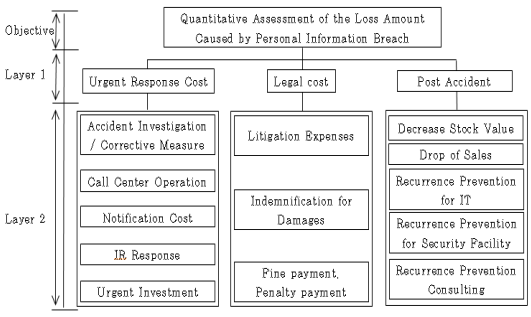

Fig. 2. AHP Layered Model for Personal information breach

4.3 3단계: 설문결과 손해금액 산정요소의 중요도 및 적절성 평가

4.3.1 손해금액 산정요소별 중요도 평가

개인정보 유출사고 발생시, 손해금액 산정을 위한 3개 구분, 13개 요소에 대해 보안책임자 23명에게 9점 만점 척도로 중요도 설문을 실시결과, Table 24.와 같이 중요도 측면에서는 법적대응 부분이 6.8점, 긴급조치 5.8점, 사후대응 5.0으로 나타났다.

기업의 보안관리자는 회사가 법적처벌이나 손해배상이 발생 될 경우 많은 리스크를 책임지게 되므로 긴급조치보다 법적대응을 중요하게 설문했다.

또한, 13개항목 중 매출감소 7.5, 과태료/벌금/과징금 7.0, 각종 소송비용/콜센터 운영비용 6.9의 순으로 중요도를 응답하였다.

사고 발생후 매출감소에 대한 부분을 기업으로서 가장 중요하게 판단 하였으며, 다음으로 과태료/벌금/과징금, 각종 소송비용/콜센터 운영비용 순으로 응답하였다.

긴급조치 항목 중에는 유출사고 발생시 대고객 대응을 위한 콜센터운영비용 6.9, 홍보/IR 비용 6.5로 설문했으며 고객통지비용의 중요도를 가장 낮게 평가하였다.

법적대응의 경우, 과태료/벌금/과징금 7.0, 각종 소송비용 6.9, 고객손해배상비용 6.5로 응답하여 과태료/벌금/과징금을 가장 중요하게 설문 하였다.

사후대응 측면에서는 매출감소 7.5, 주식가치 하락 5.8로 설문하고 재발방지를 위한 컨설팅비 4.0, IT/시설투자는 각각 4.9, 3.0으로 응답하였다.

Table 24. Survey result of degree of importance for each factors to estimate loss amount

Layer1	Layer 2	Average	Ranking
Urgency measure	Accident Investigation / Corrective Measure	5.7	9
	IR Response	6.4	6

	Notification Cost	3.9	12
	Call Center Operation	6.9	3
	Urgent Investment	6.1	7
	Average	**5.8**	
Legal cost	Litigation Expenses	6.8	4
	Indemnification for Damages	6.5	5
	Fine payment, Penalty payment	7.0	2
	Average	**6.8**	
Post Accident	Decrease Stock Value	5.8	8
	Drop of Sales	7.5	1
	Recurrence Prevention Consulting	4.0	11
	Recurrence Prevention for IT	4.9	10
	Recurrence Prevention for Security Facility	3.0	13
	Average	**5.0**	

4.3.2 AHP 분석결과

Expert choice 2000을 통해 AHP 분석결과, Table 25.와 같이 가중치가 도출 되었다. 1계층은 긴급조치(0.492), 법적대응(0.228), 사후대응(0.280)으로 가중치가 분석되어 보안책임자들은 개인정보 유출사고 발생시 긴급조치를 가장 먼저 대응해야 한다고 우선순위를 두었다.

개인정보 유출에 따른 손해금액 산출요소의 각각 최종 가중치는 1계층의 각각의 가중치와 2계층의 각 항목의 가중치의 곱으로 산정하였다. 최종 가중치를 바탕으로 개인정보 유출로 인한 손해금액 산정요소에 대한 기업 보안책임자들의 평가순위 및 가중치는 아래와 같다.

사고조사 및 조치 인건비(1순위, 0.200), 매출감소(2순위, 0.139), 손해배상 비용(3순위, 0.124), 주식가치하락(4순위, 0.090), 고객통지비용(5순위, 0.083), 과태료/벌금/과징금(6순위, 0.079), 콜센터운영비용(7순위, 0.078), 긴급 IT/시설보안투자(8순위, 0.066), 홍보/ IR비용(9순위, 0.064), 각종소송비용(10순위, 0.026), 재발방지 IT투자(11순위, 0.021), 재발방지 시설투자(12순위, 0.019), 재발방지 컨설팅(13순위, 0.011)으로 도출되었다.

1계층의 긴급조치의 가중치가 타 1계층 가중치의 2배 정도 임에도 불구하고 사고조사/조치 인건비를 제외하고 매출감소(2순위), 손해배상비용(3순위), 주식가치 하락(4순위)에 대한 가중치도 높게 도출되어 보안책임자들이 개인정보 유출사고 발생으로 인한 회사의 매출에 대해서 중요하게 판단하고 있다.

또한, 고객의 손해배상 청구로 인한 배상비용 및 주식가치 하락에 대해서 우선시 함을 알 수 있으며, 사고발생시 법에 따른 조치를 위한 고객통지비(5순위), 콜센터운영비(7순위)에 대해서도 가중치를 높게 판단하고 있음을 알 수 있다.

하지만 이와는 다르게 재발방지를 위한 IT투자(11순위), 시설투자(12순위), 컨설팅비(13순위)로 가중치가 낮게 도출되어 여전히 보안책임자 및 경영

Table 25. Weight Result of Estimated Loss Amount

Layer1	Weight	Layer2	Weight	Final Weight	Ranking
Urgency measure	0.492	Accident Investigation / Corrective Measure	0.408	0.200	1
		IR Response	0.130	0.064	9
		Notification Cost	0.169	0.083	5
		Call Center Operation	0.159	0.078	7
		Urgent Investment	0.134	0.066	8
Legal cost	0.228	Litigation Expenses	0.112	0.026	10
		Indemnification for Damages	0.544	0.124	3
		Fine payment, Penalty ayment	0.344	0.079	6
Post Accident	0.280	Decrease Stock Value	0.323	0.090	4
		Drop of Sales	0.495	0.139	2
		Recurrence Prevention Consulting	0.038	0.011	13
		Recurrence Prevention for IT	0.074	0.021	11
		Recurrence Prevention for Security Facility	0.070	0.019	12

층에서 재발방지에 대해서는 소극적인 면이 있음을 알 수 있다.

V. 결 론

본 연구를 통해서 기업의 개인정보 유출 리스크를 FAIR 방법론을 통해서 분석하고 손해금액을 산정하였다. 또한 손해금액 산정요소에 대해서 기업의 보안책임자급 전문가 집단을 통해서 중요도를 분석하고, 산정요소별 AHP를 통한 쌍대비교를 통해서 개인정보 유출에 따른 손해금액 산정요소 선택의 가중치와 적절성을 평가 하였다.

또한, 평가결과를 통해 손해금액 산정요소를 실제 업무에 적용하여 해당기업에 맞는 손해금액 산정요소를 선택함에 있어 적절한 항목을 선택할 수 있는 의사결정의 우선순위를 제시 하였다.

기업의 개인정보 유출관련 책임자가 개인정보 유출에 따른 손해금액을 효과적으로 산출하기 위해서는 본 연구의 3장, "FAIR의 단계별 RISK 분석 방법 요약"에서 와 같이 3단계의 분석단계를 거친다.

특히 1단계를 실행할 때 Table 24.와 Table 25를 고려하고 Table 13.을 참조하여 해당 회사에 맞는 손해금액 산정요소를 도출하고 Fig.2와 같이 개인정보 유출시 손해금액 산정을 위한 계층도를 완성한 후 수행하는 것이 바람직하다.

Fig 3.의 포메논 보고서에서도 본 연구와 같이 사고 긴급 조치, 법적대응 및 매출, 주식가치 하락 등 비즈니스 손실을 중요하게 판단 하였다[25]. 최종 의사결정시에는 반드시 Table 24.와 Table 25.

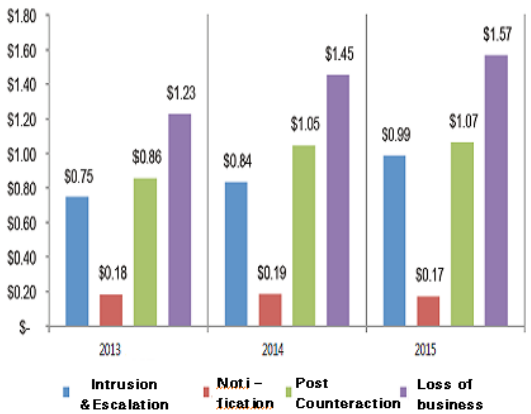

Fig. 3. The trend of major cost from data breach in last three years

의 중요도 및 가중치 순위를 고려한다.

순위가 낮은 항목은 산출이 난해하며, 영향도가 낮으므로 산정요소에서 담당자가 배제 하거나 참고사항으로 반영하여도 된다. 가중치가 높고 정책적으로 중요한 산정요소를 기업의 의사결정 포인트로 사용하여야 한다. 그런 다음, 아래의 순서에 따라 FAIR 방법론에 따른 손해금액을 산정한다.

① 1단계: 사고 시나리오 구성 및 자산식별
② 2단계: FAIR 방법론에 따라 각각의 항목을 산출 → 해당기업만의 손해금액 산정요소에 대한 소요비용을 사전에 관련부서를 통해 정확히 분석필요
③ 3단계: Overall Risk 산출하여 개인정보유출 사고로 인한 손해금액 분석 완료

위와 같이 FAIR 방법론을 통해서 손해금액을 산정하면 해당사고의 리스크 분석과 동시에 최종적으로 손해금액 구간을 정량적으로 도출할 수 있으며 손해금액 산정을 표준화된 논리적인 방법론에 따라 구할 수 있다.

향후, 분석된 내용을 통해서 손해금액 산정요소에 변화를 주면서 경영환경 변화를 반영하여 새로운 값을 산정할 수 있다. 또한 앞서 1단계에서 산정요소에 대한 계층도를 통해서 AHP 민감도를 계산하면 산정요소 변화에 따른 손해금액의 변화추이도 예상이 가능하여 유연하게 개인정보 유출사고에 대응하거나 사고를 예상하여 경영진을 설득하고 대응방안을 수립, 부족한 사고발생에 대한 대응요소를 효율적으로 보완 할 수 있을 것이다.

또한 본 연구의 방법론을 응용하여 보안관련 투자에 따른 비용발생에 대한 리스크를 사전에 예측하는 Security ROI(Return On Investment)분야에서도 충분히 응용이 가능하며, 사전에 분석한 시나리오와 계층도를 기반으로 AHP를 작성한후 각 투자항목에 대한 가중치 및 민감도를 분석하여 투자의 효율성에 따른 의사결정에 응용할 수 있다.

향후 국내에서도 개인정보사고발생시 조치금액 및 발생내역에 대해서 법적으로 공개하게 함으로써 개인정보 처리주체가 사고를 민감하게 받아들이고 조심하여, 개인정보 유출사고를 예방하고 정보를 공유할 수 있게 되어야 할 것이다.

References

[1] Copyright Statistics Korea, "Number of personal information infringements", "http://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx_cd=1366" 11. Aug. 2016

[2] Korea Ministry of Government Legislation, "Personal Information Protection Act", "http://www.law.go.kr/lsSc.do?menuId=0&p1=&subMenu=1&nwYn=1&section=&tabNo=&query=%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%20%EB%B3%B4%ED%98%B8%EB%B2%95#undefined"

[3] Korea Internet Security Agency, "Defintion of Personal Information", "https://www.i-privac y.kr/jsp/user4/intro/define1.jsp"

[4] Gordon, Lawrence A., and Martin P. Loeb., "Managing cybersecurity resources: a cost-benefit analysis," Vol. 1. New York: McGraw-Hill, 2006

[5] Hae Won, Yoo, "Damages amount model caused by Information protection infringement accident," Spring Conference of Korean Institute of Industrial Engineers, pp.671-677, Jun. 2010

[6] Chang Hee, Han, "A Quantitative Assessment Model of Private Information Breach," The Jounal of Society for e-Business Studies, v. 16, no. 4, pp.17-31, Nov. 2011

[7] Jin ho, Yoo, "Estimating Direct Costs of Enterprises by Personal Information Security Breaches," Journal of the Korea Institute of Information Security & Cryptology, v. 19, no. 4, pp. 63-75, Aug. 2009

[8] Jang Ho, Yun, "FAIR-Based Loss Measurement Model for Enterprise Personal Information Breach," Advances in Computer Science and Ubiquitous Computing, Springer Singapore, pp. 825-833, Feb. 2015

[9] Hee Joo, Lee, "A study on establishing a technical safety assessment system for the Korean telemedicine system," Journal of the Korean Medical Association, v. 58, no. 12, pp. 1159-1170, Dec. 2015

[10] Dong Wook, Kim, "A Study on Information Security Policy in the era of Smart Society," Journal of the Korea Institute of Information Security & Cryptology, v. 22, no. 4, pp. 883-899, Aug. 2012

[11] Young Hee, Kim, "A study of Priority Rankings of Actions Providing Personal Information Security," Jouranl of Information and Security, v. 14, no. 4, pp. 9-17, Jun. 2014

[12] Japan Network Security Association, "Survey Report on Information Security," 12. Aug. 2014

[13] Gun Sang, Cha, "A Study on the Criteria to Estimate the Compensation from the Infringement of Personal Information," Soong Sil University, v. 22, Nov. 2011

[14] Jeong Yeon, Kim, "Analyzing Effects on Firms' Market Value of Personal Information Security Breaches," The Jounal of Society for e-Business Studies, v. 18, no. 1, pp. 1-12, Feb. 2013

[15] Il Yoo, Hong, "The Effect of Official Announcement about Information Security Breach on Corporate Stock Value in the Market," Entrue Journal of Information Technology, v. 14, no. 2, pp. 33-56, Aug. 2015

[16] Ponemon Institute, "Ponemon Institute Cost of a Data Breach Study," "http://www-903.ibm.com/edm/B1508/0812_csj/2015%20Cost%20of%20Data%20Breach%20Study_Ponemon_Kor.pdf," May. 2015

[17] Ponemon Institute, "Ponemon Institute Cost of Data Breach Study: Global Analysis," pp. 26, May. 2015

[18] Ponemon Institute, "Fifth Annual US Cost of Data Breach," Jan. 2010

[19] http://www.businessofsecurity.com/do

cs/FAIR%20-%20ISO_IEC_27005%20Cookbook.pdf
〔20〕 J. Freund; J. Jones, " Measuring and Managing Information Risk: A FAIR Approach," book, pp. 17-201, 2015
〔21〕 Ponemon Institute, "Ponemon Institute Cost of Cyber Crime Study: Global ," pp. 12, Oct. 2015
〔22〕 Yang Seo, Choi, "Hacker and Hacking Method Level Classification for Security Assessment," Journal of the Korea Institute of Information Security & Cryptology, v. 11, no. 5, pp. 63-74, May. 2001
〔23〕 Korean Online Privacy Association, "According to Personal Information Value and Breach, Analysis of Social Amount," 28. NOV. 2013
〔24〕 Saaty T. L., "The Analytic Hierarchy ro-cess," McGraw-Hill, New York, 1980.
〔25〕 Ponemon Institute, "Ponemon Institute Cost of Data Breach Study: Global Analysis," pp. 18, May. 2015

〈저자소개〉

김 정 규 (Jeong-Gyu Kim) 정회원
1994년 3월: 동국대학교 전자계산학과 학사 졸업
2014년 9월~현재: 고려대학교 정보보호대학원 석사 과정
1994년 2월~현재: 삼성전자 정보보호부서 근무
〈관심분야〉 정보보호, 정책해킹취약점 분석, 위험관리, 정보보호 컨설팅, 개인정보보호

이 경 호 (Kyung-Ho Lee) 종신회원
1989년 8월: 서강대학교 수학과 학사
1997년 8월: 서강대학교 정보통신대학원 석사 졸업
2009년 8월: 고려대학교 정보경영대학원 박사 졸업
1994년 2월~2013년 12월 : 삼성그룹, 네이버(주), 시큐베이스 등 근무
2011년 9월~현재: 고려대학교 정보보호대학원 조교수, 부교수
〈관심분야〉 위험관리, 정보보호 컨설팅, 정보보호 및 개인정보보호정책