디지털 경제 활성화를 위한 사이버보험 역할제고 방안

2018. 11

임준·이상우·이소양

KiRi 보험연구원
Korea Insurance Research Institute

머 리 말

4차 산업혁명에 의해 가상(Cyber)의 세계와 물리적인(Physical) 세계가 결합하고 있다. 사물인터넷(Internet of Things), 인공지능, 빅데이터 등의 기술발전과 함께 빠르게 디지털화되고 있으며, 스마트 카(Smart Car), 스마트 홈(Smart Home) 등 우리 주변의 모든 것이 인터넷에 연결되고 있다.

초연결사회(Hyper-connected Society)로 진화해감에 따라 주요 위협 요인의 하나로 사이버위험(Cyber Risk)이 부상하고 있으며, 사이버위험관리 수단 가운데 하나인 사이버보험(Cyber Insurance)의 중요성이 증대하고 있다.

그러나 국내에서는 아직 4차 산업혁명 시대 사이버보험의 역할과 관련하여 충분한 연구가 축적되어 있지 않은 상황이다.

이에 우리 원은 디지털 경제 활성화를 위한 사이버보험 역할제고 방안을 모색하고자 본 과제를 추진하였다. 이를 위해 주요국의 사이버보험 시장 및 발전 전략에 대해 살펴보고, 사이버위험 인식 및 사이버보험 상품의 수용도 관련 설문조사, 사례 분석 등을 통해 정책시사점을 도출하였다.

아무쪼록 본 보고서에서 제시된 방안들이 향후 사이버보험 관련 정책 수립에 활용됨으로써 디지털 경제 활성화에 기여할 수 있기를 기대한다. 마지막으로 본 보고서의 내용은 연구자 개인의 의견이며 우리 원의 공식적인 의견이 아님을 밝혀 둔다.

2018년 11월

보 험 연 구 원

원장 **한 기 정**

목차

표 차례

표 차례

그림 차례

Strategies to Enhance the Role of Cyber Insurance for the Promotion of the Digital Economy

This report examines the current status and policy issues of cyber insurance in Korea.

First, the introduction and expansion of mandates feature in the policies for cyber insurance. They mainly focus on the damage relief. Korea's cyber risk management system lacks the measures to reduce the cyber risk itself fundamentally. We need to introduce the incentive schemes for the encouragement of investment in the cyber security system. This will lower cyber risk and premiums, which raise the takeup rates of cyber insurance.

Second, according to our household survey, most respondents do not know about the sale of personal cyber insurance. Some of them have the willingness to purchase. Currently, insurance companies sell individual cyber insurance products only in the form of additional coverage. However, we find that there exist demands for the stand-alone type.

Third, the government has promoted "Open Government Data" movement since 2013. It implemented several policies. However, no risk financing strategy exists. In order to open public data more actively for data-driven innovation, we need the risk financing system. If the private insurance companies do not provide the coverage, the government should take the risk by itself. We suggest two alternatives: group captive insurance and government-backed reinsurance pool.

요 약

■ 본고의 목적은 국내 사이버보험 관련 현황에 대해 살펴보고 정책 시사점을 도출하는 데 있음

○ 기업시장, 가계시장, 공공부문으로 나누어 이슈를 제기하고 사례 분석 및 설문조사 등을 통해 시사점을 도출하였음

1. 기업시장

가. 이슈제기

■ 4차 산업혁명에 의해 사이버(Cyber) 세계와 물리적(Physical) 세계가 결합되는 초연결사회(Hyper-connected Society)로 진화해가고 있음

○ 기업의 경우 사물인터넷(Internet of Things)의 확산과 함께 정보기술(Information Technology)과 운영기술(Operational Technology)이 수렴하고 있음

■ 이처럼 초연결사회로 진화해감에 따라 사이버위험의 성격도 변화하고 있음

○ 과거에는 정보유출이 사이버 사고의 주를 이루었으며, 물리적 피해가 수반되지 않았음

○ 그러나 점차 사이버 사고의 피해가 단순히 프라이버시(Privacy)를 침해하는 것을 넘어 물리적 피해를 수반하게 되었음

- 예를 들어, 2014년 해커의 우크라이나 발전소 공격으로 인해 전력이 중단되는 사태가 발생하였음

■ 사이버 사고가 물리적 피해를 수반할 경우 정상적인 영업활동이 어려워지기 때문에 빠른 피해복구가 중요함

○ 이로 인해 피해복구 재원 조달을 위한 위험재무(Risk Financing) 전략의 중요성도 증대하였음

■ 사이버보험이 효과적인 위험재무 수단이기는 하나 수요 측면과 공급 측면의 여러 제약 요인에 의해 가입률이 저조한 상황임

○ 재앙적 수준의 손실 가능성에 대한 우려 때문에 보험회사는 적극적인 공급을 꺼리고 있으며, 공급하더라도 보험료를 높게 책정하고 있음

○ 보험 가입을 유도하기 위해 정책적으로 보험료를 낮추는 것도 보험제도의 건전성 측면에서 바람직하지 않음

■ 본고에서는 보험제도의 건전성도 유지하면서 보험 가입률을 제고할 수 있는 방안 모색을 위해 사례 분석을 시도하였음

나. 정책현황

■ 우리나라의 사이버보험 정책은 그동안 제3자(Third Party) 피해 보상 관련 의무화 도입을 중심으로 이루어져왔음

○ 2008년에는 전자금융거래법에, 그리고 2015년에는 신용정보법에 보험 등을 통한 손해배상 수단 마련의 의무화 조항이 도입되었음

○ 그리고 2018년에는 정보통신망법이 개정되어 일정 규모 이상의 정보통신서비스 제공자도 의무화 대상에 포함되었음

■ 이러한 의무화 중심의 사이버보험 정책이 가지는 한계와 보완 정책들에 대한 시사점을 얻기 위해 다음 두 가지 사례를 살펴보고자 함

○ 첫 번째는 동시대 주요국의 사이버보험 정책 사례이고, 두 번째는 사이버보험

보다 긴 역사를 가진 홍수보험 관련 정책 사례임

다. 해외사례

■ 사이버보험 시장 활성화를 위한 주요국의 전략을 살펴보면, 공급 측면은 사이버 사고 데이터 집적 및 표준화, 그리고 수요 측면은 사이버위험 인식 제고 등을 중심으로 추진되고 있음

○ 아직까지는 의무화나 보험 가입률 제고를 위한 인센티브 제도의 도입 등은 이루어지고 있지 않은 상황임

■ 미국의 경우 영리사업자인 NetDiligence, Advisen, Insurance Services Office 등에서 사이버 사고 관련 보험금 지급 데이터를 집적하였음

○ 한편, 2016년에는 Data Breach Insurance Act를 발의하였는데, 법안의 내용은 사이버보험에 가입하고 NIST의 보안 가이드라인을 준수할 경우 보험료의 15%를 세액공제 해주자는 것임

■ 유럽의 경우에는 GDPR의 시행과 함께 전 유럽 차원에서 통일된 형태의 사이버 사고 데이터를 집적하기 위해 유럽보험협회를 중심으로 사고 보고 양식인 Template for Data Breach Notifications을 마련하였음

○ 수요 측면의 경우에는 개별 국가의 보험협회를 중심으로 중소기업의 사이버위험 인식 제고를 위해 중소기업협회 등과 함께 홍보활동을 전개하였음

■ 일본의 경우에는 기업들이 상공회의소를 통해 손해보험회사에 맞춤형 사이버보험 상품개발을 의뢰하고 공동구매하는 방식을 채택하였음

○ 한편, 일본 경제산업성은 정부 및 공공사업의 발주 시 업체 선정에 있어서 사이버보험을 포함한 사이버 대책 수립 기업에 가점을 부여하는 방안을 검토하였음

■ 보험제도의 건전성 유지와 보험 가입률 제고 측면에서 국내 사이버보험 정책의 한계를 파악하기에는 주요국의 사이버보험 정책의 역사가 너무 짧음

○ 사이버보험과 유사한 특성을 가지면서 보다 긴 역사를 가진 홍수보험의 정책 사례를 살펴보고자 함

- 사이버위험과 자연재해 위험은 일어날 가능성은 낮으나, 일어나면 큰 피해를 주게 되는 LPHI(Low Probability and High Impact)의 성격을 가지고 있음

라. 홍수보험 사례 분석

■ 미국 홍수보험 관련 정책의 역사는 보험 가입률 제고와 보험제도의 건전성이라고 하는 두 개의 목표가 지속적으로 충돌하는 역사였음

○ 보험 가입률 제고를 위해서는 보험료를 인하해야 하고, 보험제도의 건전성을 위해서는 보험료를 인상해야 함

■ 미국에서 민영보험회사가 홍수보험을 팔기 시작한 것은 1895년이었음

○ 그러나 1927년 미시시피강 대홍수 이후 민영보험회사들은 홍수보험 판매를 중지하였음

■ 이후 여러 차례 민관협력 형태의 홍수보험 프로그램 도입이 시도되었으나, 모두 무산되었음

○ 그러다가 1968년 존슨 정부 당시 국가 홍수보험 프로그램인 National Flood Insurance Program(이하 'NFIP'이라 함)이 도입되었음

○ NFIP는 다음과 같은 특징을 가짐

- 민영보험회사와 정부가 함께 참여한 보험풀(Insurance Pool)임
- 보험풀의 재원이 부족할 경우, 정부는 대출기관 또는 재보험자로서의 기능을 수행하였음
- 보험 가입률 제고를 위해 고위험 지역의 경우에는 실제 위험에 상응하는 수준보

다 낮은 수준의 보험료를 부과하였음

■ 1969년 Camille와 1972년 Agnes의 두 차례의 태풍 피해를 겪으면서 NFIP의 문제점이 드러났음

○ 피해지역의 상당수 가구가 홍수보험에 가입되어 있지 않았음

■ 1973년 Flood Disaster Protection Act 제정을 통해 홍수위험지역의 경우 모기지 대출을 받기 위해서는 홍수보험에 가입해야 하는 조건부 의무화를 도입하였음

○ 그러나 1993년 미시시피강 대홍수 피해조사 과정에서 피해 가구의 상당수가 홍수보험에 가입되어 있지 않은 사실이 밝혀지자 조건부 의무화를 강화하는 조치를 도입하였음

- 모기지 대출자가 홍수보험에 가입하지 않을 경우 대출기관이 가입하도록 하였음

■ 2005년 Katrina, 2009년 Ike, 2011년 Sandy의 태풍 피해를 겪으면서 NFIP가 재정위기를 맞게 되자, 2012년 NFIP를 개혁하는 내용을 담은 Biggert-Waters Flood Insurance Reform Act(이하 'BW 2012'이라 함)가 제정되었음

○ BW 2012의 핵심 내용은 고위험 지역의 경우에도 위험 기반 보험료(Risk-Based Premium)를 부과하자는 것이었음

■ 그러나 기득권층의 극심한 저항에 부딪치자 점진적으로 보험료를 인상하는 방향으로 정책을 선회하였음

○ 한편, 의회는 보험제도의 건전성과 보험 가입률 제고의 정책 목표를 달성할 수 있는 정책 방안에 대한 연구를 National Research Council에 의뢰하였음

○ 연구 결과 다음과 같은 대안들이 제시되었는데, 이러한 대안들이 가지는 공통점은 직접적인 보험료 감면이 아니라 간접적인 보험료 감면임

- 홍수 대비 시설에 투자하는 경우 정책금융을 통해 장기 저리 대출
- 위험 기반 요율 적용 시 보험료가 급격히 상승하게 되는 가구를 대상으로 바우

처(Voucher) 발급

- 개인 또는 근로자 수가 50인 이하인 소기업이 일정 조건을 충족하는 경우 세액 공제 혜택 부여
- 소득공제 혜택을 받을 수 있는 재해저축계좌 도입: 재해저축계좌의 자금을 홍수 보험의 자기부담금 이하의 비용지출에 사용할 수 있다면 자기부담금 수준을 높임으로써 보험료를 낮출 수 있음

2. 가계시장

■ 기업성 사이버보험 시장뿐만 아니라 가계성 사이버보험 시장도 성장이 예상되고 있으나 아직 관련 국내연구가 활발하지 않은 상황임

○ 기초적인 연구도 부재한 상황인데, 본고에서는 개인의 사이버위험 인식 및 사이버보험 상품에 대한 수용도 관련 설문조사 결과를 소개하고자 함

- 사이버 금융범죄와 사이버 명예훼손을 중심으로 조사하였음

■ 사이버위험의 주관적 인식의 경우 사이버 사고를 당할 가능성이 낮다고 생각하는 응답자가 높다고 생각하는 응답자보다 상대적으로 많았음

○ 사이버 금융범죄의 경우 낮다고 생각하는 응답자의 비중은 약 42.1%, 높다고 생각하는 응답자의 비중은 약 19.1%였음

○ 사이버 명예훼손의 경우 낮다고 생각하는 응답자의 비중은 약 49.2%, 높다고 생각하는 응답자의 비중은 약 12.8%였음

■ 조사 대상자 중 현재 사이버보험에 가입해 있지 않은 사람들을 대상으로 관련 보험상품 판매 사실에 대해 물어본 결과 90% 이상이 모르고 있었음

○ 사이버 금융범죄 관련 보험상품의 경우 응답자의 약 8.4%만이 판매 사실에 대해 인지하고 있었음

○ 사이버 명예훼손 관련 보험상품의 경우 응답자의 약 5.3%만이 판매 사실에 대해 인지하고 있었음

■ 조사 대상자 중 사이버보험 가입 의향이 있는 사람들을 대상으로 구입 형태에 대해 조사한 결과, 단독형 상품에 대한 수요가 적지 않게 존재하였음

○ 사이버 금융범죄 관련 보험상품의 경우 응답자의 약 47.9%가 특약형 대신 단독형을 선호하였음

○ 사이버 명예훼손 관련 보험상품의 경우 응답자의 약 34.3%가 특약형 대신 단독형을 선호하였음

3. 공공부문

가. 이슈제기

■ 그동안 국내 사이버보험 정책은 의무화 대상을 확대하는 방향으로 추진되어 왔음

○ 2008년 전자금융업자와 집적정보통신시설사업자, 2015년 신용정보회사, 2018년 정보통신서비스제공자 등이 의무화 대상에 포함되었음

○ 기존 선행연구 등에서는 다음 의무화 대상으로 공공부문이 언급되고 있음

■ 공공부문의 사이버보험 정책으로 의무화 대안이 거론되는 것은 공공부문도 이전의 다른 경제주체들과 동일한 관점에서 접근하기 때문임

○ 본고에서는 기존 선행연구와는 다른 관점에서 접근함으로써 차별적인 시사점을 도출하고자 함

- 본고에서의 다른 관점이란 빅데이터 시대 공공부문의 역할과 관련이 되어 있음

나. 빅데이터 시대 정보보호

■ 현재의 정보보호 규제체계의 핵심원칙은 개인의 자기결정권에 있음

○ 즉, 자신의 개인정보를 제공할 것인지, 제공한다면 누구에 의해 어떻게 사용하도록 할 것인지에 대한 결정권을 개인에게 부여함

- 이러한 개인의 자기결정권 원칙이 실제적인 제도로 구현된 형태가 통지와 동의(Notice and Consent)임

○ 현행 정보보호 규제체계는 명시적으로는 아니나 암묵적으로 위험의 완전한 제거를 목표로 하고 있음

- 이로 인해 빅데이터의 혁신적인 활용을 통한 부가가치 창출이 어려움

■ 정보보호 관련 글로벌 싱크 탱크인 Center for Information Policy Leadership은 빅데이터 시대 정보보호 원칙으로 다음 세 가지를 제시하였음

○ 첫째, 정보사용자의 책임 강화

- 현행 정보보호 체계는 정부주체의 책임을 강조하고 있음

○ 둘째, 일정 수준의 위험은 수용하면서 위험관리 체계 도입

- 이 경우 사고 발생 시 피해복구를 위한 위험재무(보험 포함) 전략이 중요해짐

○ 셋째, 개인정보의 정의 등 기존 원칙의 재해석

다. 공공데이터 개방정책

■ 공공부문의 경우 대량의 데이터를 보유하고 있으나 혁신적인 활용에 있어서는 미흡했다는 비판이 제기되면서 민간에 개방하자는 Open Government Data 운동이 2009년 미국에서 시작되어 전 세계로 확대되었음

○ 국내에서도 2013년 '정부3.0'이라는 이름으로 공공데이터 개방 운동이 추진되었음

- 2013년 [정부3.0 비전]을 선포하였으며, 2014년 [정부3.0 추진위원회]가 출범되

었음

- 2015년 11개 분야의 공공데이터를 개방하였으며, 이후 점차 확대되어 2017년 현재 29개 분야 공공데이터를 개방하였음

■ 그동안 국내 공공데이터 개방정책을 평가해보면, 활용과 관련된 정책에 비해 위험재무 관련 전략이 부재함

○ 활용 과정에서 사고 발생 시 어떤 방식으로 피해구제 재원을 조달할 것인지에 대한 논의가 필요함

라. 위험재무 전략

■ 4차 산업혁명 시대 데이터 기반 혁신(Data-driven Innovation)을 촉진하기 위해서는 공공부문이 데이터 집적자로서의 소극적인 역할을 넘어 적극적인 데이터 공급자로서의 역할 수행이 필요함

○ 적극적인 역할을 수행하는 과정에서 발생하는 위험을 민영보험회사로 전가하기 어려운 경우, 공공부문이 위험의 일부 또는 전부를 보유하는 방안에 대해 검토할 필요가 있음

- 본고에서는 자가보험(Captive Insurance)과 정부지원 재보험풀(Government-backed Reinsurance Pool)의 두 가지 대안을 제시함

■ 먼저, 자가보험 모델의 경우에는 국가중점 데이터의 소관부처들이 그룹 자가보험(Group Captive Insurance)을 만들어 운영하는 것임

○ 1980년대 중반 미국에서 배상책임보험 위기가 발생하자 지자체, 항공, 의료 분야 등의 경우에는 시장을 통한 보험가입이 어려워졌음

- 이 분야들의 경우 산업별 그룹 자가보험을 만들어 대처하였음

■ 두 번째로 정부지원 재보험풀 모델의 경우에는 영국의 Pool Re가 하나의 사례가

될 수 있음

○ Pool Re는 1993년 영국의 손해보험회사와 로이즈가 공동 출자해서 만든 테러 위험 관련 상호회사 형태의 재보험회사(Mutual Reinsurer)임

○ 1990년대 초 원수보험회사와 재보험회사들은 엄청난 규모의 잠재적 피해 가능성과 미래 손실에 대한 신뢰할 만한 추정 방법의 부재로 인해 테러 위험 보장의 중단을 고려하였음

- 그러나 테러위험 보장의 중요성으로 인해 대안 모색 논의가 있었으며, 그 과정에서 Pool Re가 탄생하였음

○ 현재 Pool Re의 보상구조는 다음과 같음

- 피해규모가 1.5억 파운드까지는 Pool Re에 참여하고 있는 보험회사가 부담함
- 피해규모가 1.5억을 초과해서 80억 파운드까지는 Pool Re와 Pool Re로부터 재출재 받은 민간 재보험사가 부담함
- 그 이상의 피해에 대해서는 정부가 부담함

4. 정책과제

가. 기업시장

■ (현황문제) 위험통제와 위험재무가 포함된 종합적인 사이버위험관리 전략하에서 사이버보험 정책이 추진되지 않고 있음

○ 피해구제 중심의 의무화 정책이 주를 이루고 있음

■ (정책과제) 피해구제뿐만 아니라 사이버위험을 근원적으로 줄일 수 있는 대책 병행이 필요함

○ 예를 들어, 보안시설 투자 유도를 위한 정책금융 및 세제혜택 등의 인센티브 제도의 도입이 필요함

- 보안시설에 대한 투자를 증가하게 되면 위험이 감소하여 보험료 인하 효과가 발생함
- 인센티브 제도를 통해 간접적으로 보험료를 인하해줄 경우 보험 가입률도 제고하면서 보험제도의 건전성도 유지할 수 있음

나. 가계시장

■ (현황문제) 설문조사 결과에 의하면, 대부분의 응답자가 가계성 사이버보험의 판매 사실을 모르고 있었음

○ 한편, 판매 사실을 모르고 있던 응답자 가운데 일부는 보험 가입 의향을 밝혀, 잠재수요가 존재함을 확인할 수 있었음

○ 상품형태의 경우 현재는 주로 특약형으로 판매하고 있는데, 단독형에 대한 수요가 존재하였음

■ (정책과제) 단독형 상품의 경우 IoT업체 등과의 제휴에 의해 부가(Add On) 상품으로 판매하는 것이 하나의 대안이 될 수 있음

○ 단, 이 경우에 소비자가 인지하지 못한 상태에서 보험에 가입되는 사례 등이 발생할 우려가 있기 때문에 소비자보호 장치 마련이 필요함

다. 공공부문

■ (현황문제) 공공부문은 4차 산업혁명 시대 핵심자원의 하나로 부상하고 있는 데이터의 보고 가운데 하나임

○ 그동안 정부는 공공데이터 개방 확대 등 데이터 활용과 관련된 여러 정책들을 발표하였음

○ 그러나 피해 발생 시 보상과 관련된 위험재무 전략에 대한 논의는 미흡하였음

■ (정책과제) 민영보험회사에 위험을 전가하기 어려운 경우 데이터 기반 혁신을 촉진하기 위해 공공부문이 적극적으로 위험을 인수할 필요가 있음

○ 이 경우 그룹 자가보험과 정부지원 재보험풀 모델을 대안으로 검토해볼 수 있음

Ⅰ. 서론

1. 연구배경 및 목적

사물인터넷, 빅데이터, 인공지능 등 최근의 디지털 기술발전은 이전에 경험하지 못했던 새로운 혜택을 가져올 것으로 예측된다. 그러나 적절한 위험관리 및 피해구제체계를 구축하지 못할 경우 디지털 경제의 지속적인 발전은 어려울 것으로 예상된다.

사이버보험은 디지털 경제의 사이버 복원력(Cyber Resilience)을 제고하는 데 있어서 중요한 하나의 축으로 기능할 수 있는데, 현재는 여러 제약 요인에 의해 큰 역할을 하지 못하고 있다. 공급 측면에서 보면, 데이터의 부족 및 사이버위험의 진화로 인해 사이버보험 상품개발에 어려움을 겪고 있고, 인터넷 대란 등 거대 위험의 가능성 등으로 인해 보험회사가 사이버위험을 적극적으로 인수하지 않는 경향이 있다.

한편, 수요 측면에서는 사이버위험에 대한 이해부족, 사이버보험 상품 표준화 결여에 의한 약관 해석의 불확실성 등으로 인해 사이버보험 가입이 저조한 상황이다.

본고에서는 국내 사이버보험 관련 현황에 대해 살펴보고 사례 분석 등을 통해 정책 시사점을 제시하고자 한다.

2. 선행연구

국내 선행연구 가운데에는 이기형 외(2010)가 개인정보유출사고배상책임보험제도와 관련하여 다양한 이슈를 비교적 충실하게 다루었다. 보고서의 내용을 의무보험제도나 활성화 전략과 같은 실천과제 중심으로 소개하면, 우선 의무보험의 단계적 확대를

주장하였다. 그리고 보험제도가 보다 원활하게 운영되기 위해서는 정부와 민영보험회사의 적절한 역할 분담이 필요하다고 주장하였다. 정부의 역할로는 보험료 지원과 같은 직접 보조방식과 세제혜택과 같은 간접 보조방식 등을 제시하였다. 그리고 국가재보험에 대해서도 검토가 필요하다고 보았지만 연구 당시의 상황을 감안할 때 아직 국가재보험을 도입할 상황은 아니라고 판단하였다. 한편 민영보험회사의 역할로는 전문성을 발휘하여 적극적으로 참여할 것을 주장하였다.

이기형 외(2010) 이후의 연구들은 크게 두 개의 그룹으로 구분할 수 있는데, 첫 번째 그룹은 의무보험제도와 관련된 것이고, 두 번째 그룹은 사이버 보험시장 활성화에 관한 것이다.[1] 전자의 경우에는 주로 법학 분야의 전문가들이 다루었는데, 김은경(2014)과 박영준(2015)이 해당된다. 이들은 의무보험제도의 운용과 관련하여 가입기준, 보상범위, 보상한도 결정 시 고려해야 할 사항 등에 대해 다루었다.

사이버 보험시장 활성화를 다룬 연구에는 보험개발원(2012), 배경환·민경식(2013), 정철용 외(2013), 이승준(2017), 최우석(2017), 한국침해사고대응팀협의회(2017) 등이 있다. 대부분 국내현황, 해외사례, 수요 측면과 공급 측면의 활성화 제약요인, 활성화 방안으로 구성되어 있으며, 활성화 방안의 경우에는 구체화 정도나 논거에 있어서 이기형 외(2010)와 비교해서 크게 진전이 있었던 것처럼 보이지는 않는다.

이기형 외(2010)의 연구가 있은 지 상당한 시간이 흘렀음에도 불구하고 시장활성화 방안의 구체성이나 논거에서 왜 큰 진전이 없었을까 생각해보면, 한편으로 드는 생각은 그동안 사이버위험 이슈가 사회적으로 그리 시급한 이슈가 아니었던 데 있지 않을까 추측해본다. 정책당국이 행동에 들어가지 않으면 학술적인 영역에서의 노력만으로는 정책방안의 구체화가 쉽지 않다고 여겨진다. 그러나 최근 들어 해외뿐만 아니라 국내에서도 정책당국이 사이버위험에 관심을 가지고 있기 때문에 모멘텀이 형성되고 있는 시기라고 생각된다.

1) 그 외 기타로 해외사례를 다룬 연구에 송은지·오남호(2017)와 최창희·김혜란(2014)의 연구가 있음. 송은지·오남호(2017)는 사고 데이터 공유와 관련된 해외사례를, 그리고 최창희·김혜란(2014)은 해외 사이버 배상책임보험시장에 대해 조사하였음

3. 연구내용 및 방법

본 보고서는 크게 국내현황, 해외사례, 이슈 분석의 세 파트로 구성되어 있다. 제 Ⅱ 장 국내현황에서는 사이버 사고동향, 사이버보험 시장, 사이버 사고 관련 의무보험제도, 정보보호 관련 공법적 규제와 사법적 구제에 대해 살펴본다. 본 과제에서 다루는 사이버 사고의 범위 및 유형은 OECD(2017)을 따르고자 한다(〈표 Ⅰ-1〉 참조). 한편, 정보보호 관련 공법적 규제에서는 정보유출통지의무, 안전조치의무, 제재수단 등에 대해 살펴보고, 사법적 구제에서는 손해배상제도에 대해 소개하고자 한다.

제 Ⅲ 장 해외사례의 경우 미국, 유럽, 일본, 중국의 경우를 살펴볼 예정인데, 체계적 정리를 위해 국가별 세부목차를 다음과 같이 통일시켰다.

가. 사이버 사고동향
나. 사이버보험 시장동향
다. 사이버보험 시장활성화 전략

제 Ⅳ 장 이슈 분석에서는 기업시장, 가계시장, 공공부문별로 최근 제기되고 있는 이슈를 분석하고 시사점을 도출하고자 한다.

우선, 기업시장과 관련해서는 최근 정보통신망법이 개정되어 정보통신서비스 사업자의 경우 손해배상책임 이행을 위한 수단을 갖추도록 의무화되었다. 배상수단으로는 보험, 공제, 준비금 가운데 하나를 선택할 수 있게 하였다. 본고에서는 현재 의무화를 중심으로 진행되고 있는 국내 사이버보험 정책의 한계에 대해 살펴보고 정책 시사점을 제시하고자 한다.

둘째, 가계시장의 경우에는 국내 선행연구가 거의 없는 상황이다. 가계성 사이버보험과 관련된 기초적인 소비자 설문조사조차도 찾기 힘든 상황이다. 본고에서는 사이버 금융범죄, 사이버 폭력 등과 관련된 소비자의 위험 인식 및 사이버보험에 대한 수용도 설문조사 결과를 소개하고자 한다.

〈표 Ⅰ-1〉 사이버 사고 및 손실 유형

사고 유형			잠재적 손실
대분류	세분류	예시	
정보유출	제3자 정보유출	-	• 사고대응비용 • 프라이버시 피해배상 • 평판훼손 • 규제 및 법적 방어비용 • 금전적 제재 • 임원배상책임
	당사자 정보유출	영업기밀 유출	• 지재권 도난 • 임원배상책임
시스템 오작동	당사자 시스템 오작동	-	• 영업중단손실 • 금전적 제재 • 유형 자산 손실 • 신체상해 • 임원배상책임
	네트워크 통신 오작동	DDoS 공격	• 사고대응비용 • 영업중단손실 • 평판훼손 • 임원배상책임
	제3자 시스템 오류 야기	악성코드 전파	• 네트워크보안 소홀 책임 • 규제 및 법적 방어비용
	외부서비스 공급자 문제	클라우드 서비스 사업자 문제	• 영업중단손실
데이터 손상/ 이용제한	데이터 삭제	-	• 사고대응비용 • 데이터 및 소프트웨어 손실 • 규제 및 법적 방어비용 • 생산물배상책임 • 임원배상책임
	데이터 암호화	랜섬웨어	• 사고대응비용 • 사이버 랜섬 • 임원배상책임
기타	명예훼손/비방	-	-
	사이버사기/절도	소셜 엔지니어링을 통한 불법자금이체	• 금전적 손실 • 임원배상책임

자료: OECD(2017)

마지막으로, 공공부문과 관련해서는 위험재무(Risk Finance) 방식에 대해 다루고자 한다. 정보통신망법의 손해배상 의무화 조항 도입이 마무리되면서 세간의 관심이 자연스럽게 개인정보보호법으로 옮겨가고 있다. 그러나 개인정보보호법의 경우 대상 범위가 광범위하여 신용정보법이나 정보통신망법에 비해 의무화 도입이 쉽지 않은 상황이다. 이러한 이유에서 순차적 도입이 주장되고 있으며, 우선 도입 대상 후보로 공공기관이 거론되고 있다. 본고에서는 공공기관 사이버보험 도입방식과 관련하여 기존 선행연구와는 다른 관점에서 접근하여 시사점을 도출하고자 한다.

Ⅱ. 국내현황

1. 사고동향

사이버 사고동향의 경우에 아직 종합적이고 체계적인 통계체계가 구축되어 있지는 않다. 현재 여러 곳에서 개별적으로 통계가 집계되고 있는데, 주요 자료출처로 세 개 정도를 꼽을 수 있다. 첫 번째는 과학기술정보통신부와 한국인터넷진흥원의 "정보보호 실태조사"이다. 여기에는 기업의 사이버 사고와 관련된 설문조사 통계가 수록되어 있다. 최근 기업의 사이버 사고 경험 추이를 살펴보면, 악성코드에 의한 공격이나 스파이웨어 감염 피해는 감소하고 있는 반면, 랜섬웨어 사고는 증가하고 있다(〈표 Ⅱ-1〉 참조).

두 번째는 행정안전부와 개인정보보호위원회의 "개인정보보호 실태조사"이다. 여기에는 개인의 정보침해 경험에 관련된 설문조사 통계가 수록되어 있다. 조사대상자 가운데 개인정보 유출 경험이 있다고 응답한 비중은 40~50% 정도 되었다(〈표 Ⅱ-2〉 참조).

세 번째는 경찰청 사이버안전국의 사이버 범죄 통계이다. 크게 ① 정보통신망 침해범죄, ② 정보통신망 이용범죄, ③ 불법콘텐츠 범죄로 구분하고 있다(〈표 Ⅱ-3〉 참조). 발생 건수 측면에서 볼 때, 인터넷 사기, 사이버 금융범죄, 사이버 명예훼손이 많은 편에 속한다(〈표 Ⅱ-4〉 참조).

이러한 공식적인 통계 이외에도 주요 사이버 사고는 언론 기사 검색을 통해서도 수집이 가능한데, 〈표 Ⅱ-5〉에는 최근 주요 사이버 사고가 정리되어 있다.

〈표 Ⅱ-1〉 기업의 사이버 사고 경험 및 유형

(단위: %)

구분		2014년	2015년	2016년
사고경험		1.8	1.0	2.2
사고유형	악성코드에 의한 공격	93.5	91.0	75.5
	랜섬웨어	1.7	18.7	25.5
	애드웨어/스파이웨어 감염	33.2	19.7	13.0
	외부의 내부 데이터 비인가 접근	4.1	4.9	9.1
	DoS/DDoS 공격	8.7	2.9	8.5
	내부인력에 의한 정보유출	0.8	4.3	3.3
	APT 공격	0.8	2.6	0.2

주: 1) 2014년의 응답 기업 수는 8,121개, 2015년에는 9,586개, 2016년에는 9,130개임
2) 사고유형의 경우 사고 경험이 있는 기업을 대상으로 유형별로 사고 경험여부를 조사하였음(복수 응답)
3) APT는 Advanced Persistent Threat의 약자로, 정교한 수준의 전문 기술 또는 방대한 리소스를 가진 공격자가 특정 기업 또는 기관을 대상으로 여러 공격 경로를 사용하여 공격하는 것을 의미함

자료: 과학기술정보통신부·한국인터넷진흥원(2015, 2016, 2017)

〈표 Ⅱ-2〉 개인(정보주체)의 개인정보 침해 경험 및 유형

(단위: %)

구분	2012년	2013년	2014년	2015년
개인정보 무단수집·이용	59.7	44.4	43.4	50.1
과도한 개인정보 수집	44.6	31.3	28.3	40.7
주민등록번호 도용	28.8	17.1	17.5	19.9
개인정보 유출	49.9	46.7	39.5	49.9

주: 1) 2014년의 응답 기업 수는 8,121개, 2015년에는 9,586개, 2016년에는 9,130개임
2) 침해 유형별로 경험여부를 조사하였음(복수 응답)
3) 개인정보 무단수집·이용: 예를 들어, 동의를 받지 않고 고객의 개인정보를 수집하거나 동의 없이 활용하는 것이 해당됨(예: 홍보문자 전송 등)
4) 과도한 개인정보 수집: 예를 들어, 입사 지원서에 주민등록번호를 필수기재 사항으로 지정하는 것이 해당됨(주민등록번호는 입사지원서가 아니라 근로계약 체결 시 필요한 정보)
5) 주민등록번호 도용: 예를 들어, 타인의 주민등록번호를 이용하여 인터넷 홈페이지 등에 가입하는 것이 해당됨

자료: 행정안전부·개인정보보호위원회(2013, 2014, 2015, 2016)

〈표 Ⅱ-3〉 경찰청 사이버 범죄 통계자료의 사이버 범죄 유형 정의

유형		정의
정보통신망 침해범죄	해킹	정당한 접근 권한 없이 또는 허용된 접근 권한을 초과하여 정보통신망에 침입하는 행위(계정도용, 자료유출, 자료훼손 등이 해당됨)
	서비스거부 공격	정보통신망에 대량의 신호·데이터를 보내거나 부정한 명령을 처리하도록 하여 정보통신망에 장애를 야기한 경우
	악성 프로그램	정당한 사유 없이 정보통신 시스템, 데이터, 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프로그램을 전달 또는 유포하는 경우
정보통신망 이용범죄	인터넷 사기	직거래 사기(물품 거래 등에 관한 허위의 의사표시를 게시하여 발생한 대금 편취 사기), 쇼핑몰 사기(허위의 인터넷 쇼핑몰 등을 개설하여 발생한 대금 편취 사기) 등이 해당됨
	사이버 금융범죄	정보통신망을 이용하여 피해자의 계좌로부터 자금을 이체 받거나 소액 결제가 되게 하는 범죄로 피싱, 파밍, 스미싱 등이 해당됨
	개인위치 정보침해	이용자의 동의를 받지 않거나 속이는 행위 등으로 다른 사람의 개인위치정보를 불법적으로 수집·이용·제공한 경우
	사이버 저작권침해	정보통신망을 통하여 디지털 자료화된 저작물 또는 컴퓨터 프로그램 저작물에 대한 권리를 침해한 경우
불법콘텐츠 범죄	사이버 명예훼손	정보통신망을 통하여 다른 사람의 명예를 훼손하는 경우(정보통신망법 제44조의7 제1항 제2호)
	사이버 스토킹	정보통신망을 통하여 공포심이나 불안감을 유발하는 부호·문언·음향·화상 또는 영상을 반복적으로 상대방에게 도달하도록 하는 경우(정보통신망법 제44조의7 제1항 제3호)

자료: 경찰청 사이버안전국 홈페이지

〈표 Ⅱ-4〉 사이버 범죄 통계

(단위: 건)

구분		정보통신망 침해범죄			정보통신망 이용범죄				불법 콘텐츠 범죄	
		해킹	서비스거부 공격	악성 프로그램	인터넷 사기	사이버 금융범죄	개인위치 정보침해	사이버 저작권침해	사이버 명예훼손	사이버 스토킹
2014년	발생	1,648	26	130	56,667	15,596	939	14,168	8,880	363
	검거	540	16	69	40,657	6,567	635	7,198	6,241	300
2015년	발생	2,247	40	166	81,849	14,686	609	18,770	15,043	134
	검거	524	19	74	68,444	7,886	296	8,832	10,202	124
2016년	발생	1,847	192	137	100,369	6,721	2,410	9,796	14,908	56
	검거	537	164	98	89,364	4,034	2,125	5,616	10,539	53
2017년	발생	2,430	43	167	92,636	6,066	413	6,667	13,348	59
	검거	990	28	122	80,740	2,632	298	4,134	9,756	52

자료: 경찰청 사이버안전국 홈페이지

〈표 Ⅱ-5〉 최근 주요 사이버 사고 현황

사고명	사고일시	사고내용
3. 20 사이버 공격	2013년 3월	방송·금융기관 등 서버·PC 등 악성코드 감염
6. 25 사이버 공격	2013년 6월	총 69개 기관·업체 등에 대한 DDoS 공격 및 홈페이지 변조 사고 발생
KT 정보유출	2014년 3월	KT 홈페이지의 타인여부 인증절차 보안 취약점을 악용, KT 고객 개인정보 유출 사고
SKB DDoS 공격	2014년 11월	SKB DNS를 대상으로 DDoS 공격
한수원 해킹	2014년 12월 2015년 3,7,8월	해커그룹(Who am I)이 원전중단을 요구하며 원자력 관련 자료를 인터넷에 공개
뽐뿌 해킹	2015년 9월	보안 취약점을 이용하여 개인정보 유출
인터파크 개인정보유출	2016년 5월	내부직원의 PC가 악성코드에 감염된 후 사내 확산 및 DB파일 탈취
여기어때 개인정보유출	2017년 3월	개인정보 유출 후 금전 요구
워너크라이 랜섬웨어	2017년 5월	워너크라이 랜섬웨어에 감염되어 데이터 암호화 피해 발생
인터넷나야나 랜섬웨어감염	2017년 6월	인터넷나야나 호스팅 서버(153대)가 랜섬웨어에 감염되어 이용기관 홈페이지가 랜섬웨어 협박화면으로 변조
빗썸 사고	2017년 6월	빗썸 회원정보 유출

자료: 최우석(2017)

2. 보험시장

국내 사이버보험 시장규모 관련 공식적인 통계는 공개되고 있지 않으나 대략 300~400억 원 규모로 추정되고 있다.

가. 기업성 사이버보험

사이버보험상품을 크게 기업성과 가계성으로 구분할 때, 기업성 사이버보험의 경우 과거에는 담보의 범위가 주로 정보유출 배상책임에 국한되었으나, 최근 들어 담보 범

위가 확대되고 있다. 사이버 종합보험의 경우 사실상 거의 모든 담보를 포괄하고 있다. 고객의 요구에 따라 맞춤형으로 담보를 구성해 상품을 제공하고 있다.

기업성 사이버보험의 요율은 크게 세 가지 형태로 구분할 수 있다. 첫째, 보험료가 보장한도의 일정 비율로 책정되는 경우, 둘째, 요율산정에 있어서 기업의 매출액이나 산업 유형 등을 고려하는 경우, 셋째, 보안 관리 상태를 반영하여 요율을 결정하는 형태인데, 가장 발전된 형태의 요율체계이다. 연구진이 인터뷰한 보험회사의 경우에는 첫 번째 유형의 요율체계를 사용하고 있었다. 그리고 보장한도의 경우에는 대기업, 중견기업, 중소기업별로 차별화된 보장한도를 제시하고 있다(〈표 Ⅱ-6〉 참조).

나. 가계성 사이버보험

가계성 사이버보험의 경우에는 기업성 사이버보험과 달리 단독형보다는 주로 다른 보험의 특약 형태로 판매되고 있다(〈표 Ⅱ-7〉 참조). 연구진이 인터뷰한 보험회사의 경우에 가계종합보험의 담보 가운데 하나로 개인정보 피해보상이 포함되어 있다.

가계성 사이버보험의 경우에는 보험료가 저렴해서 설계사 채널을 통해 단독형으로 판매하기에는 수수료 문제로 인해 한계가 있다. 따라서 설계사를 통해 판매하려면 종합보험의 형태로 판매해야 하는데, 그렇게 하면 상품이 복잡해지는 문제가 있다. 결국 단순한 형태의 단독형 사이버보험 상품을 팔기 위해서는 온라인 채널을 활용해야 하는데, 이럴 경우에는 적극적인 마케팅이 어려운 문제가 있다.[2)]

2) B사와의 인터뷰 내용임

〈표 Ⅱ-6〉 기업성 사이버보험 상품 예시(A사)

(단위: 억 원)

담보		담보별 보상한도액		
구분	설명	대기업	중견기업	중소기업
데이터 손해 또는 도난	데이터 복구비용, 악성 프로그램 제거 비용 등을 보장	100	30	10
정보유지위반 배상책임	고객과의 협의하에 보관하던 고객의 기밀정보 유출로 인한 법적 배상책임액을 보장	50	10	5
개인정보침해 피해담보	개인정보유출로 인해 피보험자가 부담하게 되는 비용 가운데 배상책임을 제외한 비용(예: 방어비용, 과징금 등)을 보장	100	30	10
개인정보침해 배상책임	개인정보유출로 인해 피보험자가 부담하게 되는 법적 배상책임액 보장	100	30	10
기업휴지손해	사업 활동의 중단에 의한 손실 담보	30	10	5
사이버협박	협상비용, 전문가 상담비용, 사이버범죄자에게 지불하는 비용 등을 보장	30	10	5
평판 리스크	사이버 사고 이후 평판위기를 관리하기 위해 홍보회사 등에 지불하는 비용을 보장	30	5	3
(특약)임원배상책임	법률상 손해배상금, 손해방지경감비용, 대위권 보전비용, 소송 관련 비용 등을 보장	20	5	3
(특약)사이버도난	피보험자 명의의 계좌 또는 전자적 지갑에서 불법적으로 전자적 자금이나 자산이 이체됨으로써 발생하는 금전적 손실 담보	5	2	1
공제금액	자기부담금을 의미하며, 보상한도액의 1% 수준	-	-	-
증권 보상한도액	-	100	30	10

주: 대기업은 매출액이 5,000억 원 초과, 중견기업은 매출액이 300~5,000억 원, 중소기업은 매출액이 300억 원 이하인 기업을 의미함
자료: A사 사이버보험상품 설명자료

〈표 Ⅱ-7〉 가계종합보험의 사이버보험 특약 예시(B사)

(단위: 원)

담보			가입금액	보험료
기본 담보	재산손해	화재(건물): 단독(1,2급)	80,000,000	5,250
		화재(가재도구): 단독(1,2급)	20,000,000	1,210
		화재(건물): 연립(1,2급)	80,000,000	3,360
		화재(가재도구): 연립(1,2급)	20,000,000	770
		화재(건물): 아파트(1,2급)	80,000,000	3,980
		화재(가재도구): 아파트(1,2급)	20,000,000	910
	급배수 설비	급배수설비 누출손해(건물)	5,000,000	2,600
		급배수설비 누출손해(동산)	5,000,000	750
	재산손해	임시거주비용확장	5,000,000	810
	전자제품	전자제품 파손	600,000	1,130
	재산손해	도난(가재도구)	1,000,000	400
		도난(귀중품)	1,000,000	560
	배상책임	가족일상 생활 중 배상책임	100,000,000	640
	배상책임	실화배상책임(단독)	100,000,000	40
		실화배상책임(연립)	100,000,000	10
		실화배상책임(아파트)	100,000,000	20
특약	개인정보 피해보상I	법률상담비용	1,000,000	1,580
		소송비용	15,000,000	860
		금전손실	3,000,000	1,250
		일실소득 및 기타 비용	1,000,000	120
	개인정보 피해보상II	법률상담비용	2,000,000	3,160
		소송비용	20,000,000	1,140
		금전손실	5,000,000	2,080
		일실소득 및 기타 비용	2,000,000	240

주: 보험료는 월보험료임
자료: B사 내부자료

3. 의무보험

신용정보법, 정보통신망법, 그리고 전자금융거래법 등에서는 정보유출 등의 사고에 대비하여 손해배상수단을 사전에 마련하도록 의무화하고 있다. 적용대상과 최저가입금액은 아래 〈표 Ⅱ-8〉~〈표 Ⅱ-10〉과 같다.

〈표 Ⅱ-8〉 신용정보법상 배상책임보험 최저가입금액

(단위: 원)

적용대상	최저가입금액
신용정보집중기관, 신용정보회사, 시중은행, 금융지주회사, 한국산업은행, 한국수출입은행, 농협은행, 중소기업은행, 한국주택공사	20억
지방은행, 외국은행의 국내지점, 금융투자업자, 증권금융회사, 종합금융회사, 자금중개회사, 명의개서대행회사, 보험회사, 여신전문금융회사, 기술보증기금, 신용보증기금, 한국무역보험공사, 예금보험공사	10억
기타	5억

〈표 Ⅱ-9〉 집적정보통신시설사업자의 배상책임보험 최저가입금액

(단위: 원)

적용대상	최저가입금액
매출액 100억 원 이상인 사업자	10억
매출액 10억 원 이상, 100억 원 미만인 사업자	1억
매출액 10억 원 미만인 사업자	5천만

주: 1) 집적정보통신시설사업자란 타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자를 의미함
2) 매출액은 배상책임보험에 가입하여야 할 연도의 직전 사업연도의 매출액을 의미함. 만약 직전 사업 연도의 매출액이 없거나 매출액 산정이 곤란한 경우에는 해당 사업자가 예측한 향후 1년간의 매출액을 사용함

〈표 Ⅱ-10〉 전자금융거래법상 배상책임보험 최저가입금액

(단위: 원)

적용대상	최저가입금액
시중은행, 농협은행, 중소기업은행	20억
지방은행, 외국은행의 국내지점, 산업은행, 수협은행, 체신 관서, 여신전문금융회사	10억
금융투자업자, 증권금융회사, 종합금융회사	5억
기타 금융회사	1억
전자자금이체 및 직불전자지급수단 발행·관리의 전자금융업자	2억
전자지급결제대행에 관한 업무의 전자금융업자 중 전자자금이체 및 직불전자지급수단 발행·관리에 속하는 금융회사가 발급한 신용카드, 직불카드 등 거래지시에 사용되는 접근매체의 정보를 저장하는 전자금융업자	10억
기타 전자금융업자	1억

2018년 5월 28일 정보통신망법이 개정되어 정보통신서비스 제공자도 의무적으로 손해배상 수단을 마련하여야 한다. 법 제32조의 3에 의하면, 일정규모 이상의 정보통신서비스 제공자 등은 손해배상책임의 이행을 위하여 보험 또는 공제에 가입하거나 준비금을 적립하는 등의 조치를 취하도록 되어 있다. 위반 시에는 2,000만 원 이하의 과태료가 부과된다. 적용대상 및 보험 최저가입금액은 향후 시행령 작업을 통해 구체화될 예정이다.

4. 공적규제

공적규제와 관련해서는 ① 정보유출통지의무, ② 안전조치의무, ③ 제재수단의 세 가지 내용을 소개하고자 한다.

우리나라 개인정보보호법에는 정보유출통지의무화 조항이 도입되어 있다. 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 ① 유출된 개인정보의 항목, ② 유출된 시점과 그 경위, ③ 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보, ④ 개인정보처리자의 대응조치 및 피해 구제절차, ⑤ 정보주체에게 피해가 발생한 경우 신고 등을 접할 수 있는 담당부서 및 연락처를 알려야 한다.[3] 1,000명 이상의 개인정보가 유출된 경우에는 정보주체뿐만 아니라 행정안전부장관 또는 한국인터넷진흥원에도 신고하여야 한다.[4]

개인정보보호법 제29조에는 안전조치의무 조항을 두어, 개인정보처리자가 안전성 확보에 필요한 기술적·관리적·물리적 조치를 취하도록 하였다. 세부기준은 행정안전부 고시인 「개인정보의 안전성 확보조치 기준」에 제시되어 있는데, 고시에 제시된 기준은 최소한의 기준이다.

개인정보보호법의 제재수단은 크게 과징금, 과태료, 벌칙(형사벌)의 세 가지가 존재

3) 개인정보보호법 제34조 제1항

4) 개인정보보호법 제34조 제3항, 개인정보보호법 시행령 제39조 제1항 및 제2항

한다. 먼저 과징금의 경우 개인정보처리자가 처리하는 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손된 경우에는 5억 원 이하의 과징금을 부과할 수 있다.[5] 유럽의 일반정보보호규칙(General Data Protection Regulation, 이하 'GDPR'이라 함)의 과징금과 비교하여 규모나 적용범위에 있어서 다소 제한적이다. 과태료의 경우에는 최대부과금액에 따라 5천만 원, 3천만 원, 1천만 원의 세 가지 유형이 존재한다.[6] 개인정보유출통지의무 위반은 세 가지 유형 가운데 두 번째인 3천만 원 이하의 과태료 적용 대상이다.[7] 벌칙은 최대 형량에 따라 네 가지가 존재한다. 10년 이하의 징역 또는 1억 원 이하의 벌금이 부과되는 경우,[8] 5년 이하의 징역 또는 5천만 원 이하의 벌금이 부과되는 경우,[9] 3년 이하의 징역 또는 3천만 원 이하의 벌금이 부과되는 경우,[10] 2년 이하의 징역 또는 2천만 원 이하의 벌금이 부과되는 경우이다.[11]

5. 손해배상

개인정보보호법에 의하면 정보주체는 개인정보처리자의 법 위반 행위로 인해 손해를 입을 경우 개인정보처리자에게 손해배상을 청구할 수 있다.[12] 현행 개인정보보호법의 손해배상제도의 특징은 크게 네 가지로 정리할 수 있다.

첫째, 과실책임주의에 입각해 있고, 입증 책임은 정보주체에서 개인정보처리자로 전환되어 있다. 법 제39조 제1항에 의하면, 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없도록 되어 있다.

둘째, 징벌적 손해배상제도가 도입되어 있다. 개인정보처리자의 고의 또는 중대한

5) 개인정보보호법 제34조의2 제1항
6) 개인정보보호법 제75조
7) 개인정보보호법 제75조 제2항 제8호 및 제9호
8) 개인정보보호법 제70조
9) 개인정보보호법 제71조
10) 개인정보보호법 제72조
11) 개인정보보호법 제73조
12) 개인정보보호법 제39조 제1항

과실로 인하여 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우로서 손해가 발생한 때에는 법원은 손해액의 3배를 넘지 아니하는 범위에서 손해배상액을 정할 수 있다.[13)]

셋째, 일반손해배상 이외에 법정손해배상제도[14)]도 추가로 도입하였다. 법 제39조의 2 제1항에 의하면, 정보주체는 개인정보처리자의 고의 또는 과실로 인하여 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우에는 300만 원 이하의 범위에서 배상을 청구할 수 있다.

넷째, 단체소송을 제기할 수 있다. 다만, 일정한 자격을 갖춘 단체에 한해서 가능한데, 법 제51조에서는 다음과 같이 규정하고 있다.

1. 「소비자기본법」 제29조에 따라 공정거래위원회에 등록한 소비자단체로서 다음 각 목의 요건을 모두 갖춘 단체
   가. 정관에 따라 상시적으로 정보주체의 권익을 주된 목적으로 하는 단체일 것
   나. 단체의 정회원수가 1천 명 이상일 것
   다. 「소비자기본법」 제29조에 따른 등록 후 3년이 경과하였을 것
2. 「비영리민간단체 지원법」 제2조에 따른 비영리민간단체로서 다음 각 목의 요건을 모두 갖춘 단체
   가. 법률상 또는 사실상 동일한 침해를 입은 100명 이상의 정보주체로부터 단체소송의 제기를 요청받을 것
   나. 정관에 개인정보 보호를 단체의 목적으로 명시한 후 최근 3년 이상 이를 위한 활동실적이 있을 것
   다. 단체의 상시 구성원수가 5천 명 이상일 것
   라. 중앙행정기관에 등록되어 있을 것

13) 개인정보보호법 제39조 제3항

14) 피해자의 실제 피해에 근거하여 배상액이 산정되는 것이 아니라 법률에 규정된 손해배상액의 규정에 근거하여 배상액이 결정되는 제도임. 법정손해배상제도에 의할 경우 사실상 아무런 손해가 발생하지 않더라도 강제규정에 근거하여 손해를 배상받을 수 있음

우리나라 개인정보보호법상 단체소송의 한계로는 다음 세 가지가 지적되고 있다.[15] 첫째, 일정한 법정요건을 갖춘 단체에게만 원고 적격이 인정된다. 둘째, 집단분쟁조정을 거친 경우에 한해서만 인정된다. 셋째, 권리침해 행위의 금지·중지만 인정할 뿐 권리침해 행위로 인한 결과를 제거하기 위한 조치(예: 손해배상)를 인정하지 않는다.

15) 함인선(2016)

Ⅲ. 해외사례

1. 미국

가. 사이버 사고동향

1) 개인정보 유출 사고

미국 신분도용자료센터(ITRC)[16]에 따르면 미국 기업의 고객정보 유출 사고[17]는 2013년 614건에서 2017년 1,579건으로 급증하였다. 2017년 기준 고객정보 유출 사고 건수를 기업 유형별로 볼 때, 비즈니스가 870건으로 1위를 차지하였으며, 다음으로 제약이 374건, 금융 134건, 교육 127건, 정부기관 74건의 순으로 나타났다.

사고유형별로 살펴보면, 2017년 기준 해킹이 940건으로 압도적 1위를 차지하였으며, 다음으로 무단접근이 170건, 직원의 실수가 163건, 인터넷상의 정보 노출이 101건, 직원의 절도가 83건 등의 순으로 나타났다.

미국 기업의 고객정보 유출은 사회보장번호 정보에 집중되어 있으며, 신용카드 정보 유출 비중도 그리 낮지 않다. 2017년 기준 사회보장번호 정보 유출은 52.7%, 신용카드 정보유출은 18.9%를 기록하였다.

16) Identity Theft Resource Center(2018)

17) 미국 신분도용자료센터가 미국 기업의 신고를 바탕으로 집계한 수치이기 때문에 실제 미국 기업의 고객정보 유출 사고 수치와 다를 수 있음

〈표 Ⅲ-1〉 미국 기업의 유형별 개인정보 유출 사고

(단위: 건, %)

구분	2013	2014	2015	2016	2017	증가율
비즈니스	195(32)	263(34)	312(40)	497(46)	870(55)	9.6
교육기관	54(9)	57(7)	58(7)	98(9)	127(8)	-0.9
정부기관	60(10)	92(12)	63(8)	72(7)	74(5)	-1.9
제약기업	271(44)	333(43)	275(35)	373(34)	374(24)	-10.6
금융기업	34(6)	38(5)	71(9)	51(5)	134(9)	3.8
전체	614	783	780	1,091	1,579	-

주: 1) 괄호 안은 전체에서 차지하는 비중을 의미함
2) 증가율은 2016년 대비 2017년 증가율을 의미함
자료: Identity Theft Resource Center(2018)

이러한 공식적인 통계 외에도 미국의 헤리티지재단(The Heritage Foundation)은 2014년부터 주요 개인정보 유출 사고를 집적하기 시작하였다. 〈표 Ⅲ-2〉에는 최근 주요 개인정보 유출 사고가 정리되어 있다.

〈표 Ⅲ-2〉 최근 미국의 주요 개인정보 유출 사고 현황

사고명	보도일시	사고내용
타깃(Target) 개인정보유출	2014년 10월	해킹으로 7,000만 명의 고객명, 주소, 전화번호 등의 같은 개인정보가 유출됨
JP 모건 체이스(J.P. Morgan Chase) 정보유출	2014년 10월	해킹으로 7,600만 건의 가계 정보 및 700만 건의 중소기업 정보가 유출됨
스테이플스(Staples) 카드정보유출	2014년 12월	해킹으로 120만 명의 카드정보가 유출됨
익스페리언(Experian) 개인정보유출	2015년 10월	해킹으로 1,500만 명의 고객정보 유출됨
링크드인(LinkedIn) 개인정보유출	2016년 5월	지난 2012년 해킹으로 유출된 가입 회원의 개인정보 유출 건수가 1억 6,700만 명인 것으로 확인됨
드롭박스(Dropbox) 개인정보유출	2016년 8월	해킹으로 6,800만 개의 계정정보가 유출됨
프렌드 파인더 네트웍스(FriendFinder Networks) 개인정보유출	2016년 11월	해킹으로 4억 1,200만 명의 가입 회원의 개인정보가 유출됨

〈표 Ⅲ-2〉 계속

사고명	보도일시	사고내용
리버 시티 미디어(River City Media) 개인정보유출	2017년 3월	데이터베이스 암호 미설정으로 13억 4,000만 개의 이메일 주소가 유출됨
버라이즌(Verizon) 개인정보유출	2017년 7월	버라이즌의 협력사인 나이스 시스템즈의 실수로 버라이즌의 600만 이상의 미국 고객의 개인정보가 유출됨
에퀴팩스(Equifax) 개인정보유출	2017년 9월	해킹으로 1억 4,300만 명의 미국인의 민감한 개인정보가 유출됨
야후(Yahoo) 개인정보유출	2017년 10월	지난 2013년 해킹으로 가입 회원의 개인정보 유출 건수가 10억 명이 아닌 30억 명인 것으로 드러남
우버(Uber) 개인정보유출	2017년 11월	해킹으로 5,700만 명의 고객과 운전기사의 개인정보가 유출됨

자료: Heritage Foundation(2014, 2015, 2016, 2018)

2) 사이버범죄 건수 및 피해규모

미국 연방수사국(FBI)[18]에 따르면, 사이버범죄 건수 및 피해규모[19]는 각각 2013년 26만 3천 건, 7억 8천 1백만 달러에서 2017년 30만 2천 건, 14억 1천 9백만 달러로 증가하였다.

〈표 Ⅲ-3〉 미국 사이버범죄 건수 및 피해규모

(단위: 천 건, 백만 달러)

구분	2013	2014	2015	2016	2017	합계
건수	263	269	288	299	302	1,421
피해규모	781	801	1,071	1,451	1,419	5,520

자료: Federal Bureau of Investigation(2018)

사이버범죄 건수 측면에서 유형별로 살펴보면, 2017년 기준 미지급 건수는 8만 4천 건으로 1위를 차지하였으며, 다음으로 개인정보 유출 건수가 3만 1천 건, 피싱이 2만 5천 건, 초과지급이 2만 3천 건, 위조 상품 관련 건수가 2만 건 등의 순으로 나타났다.

18) Federal Bureau of Investigation(2018)

19) 여기서 말하는 건수 및 피해규모는 미국 인터넷범죄신고센터가 소비자의 신고를 바탕으로 집계한 수치임

한편, 피해규모 측면에서 유형별로 살펴보면, 비즈니스 이메일 침해가 6억 7천 6백만 달러로 압도적 1위를 차지하였으며, 다음으로 신용 사기가 2억 1천 1백만 달러, 미지급이 1억 4천 1백만 달러, 투자사기가 9천 7백만 달러, 개인정보 유출이 7천 7백만 달러 등의 순으로 나타났다.

〈표 Ⅲ-4〉 2017년 미국 사이버범죄 유형별 건수 및 피해규모

(단위: 천 건, 백만 달러)

순위	유형	건수	순위	유형	피해규모
1	미지급	84	1	비즈니스 이메일 침해	676
2	개인정보 유출	31	2	신용 사기	211
3	피싱	25	3	미지급	141
4	초과지급	23	4	투자사기	97
5	위조 상품	20	5	개인정보 유출	77
전체		302	전체		1,419

자료: Federal Bureau of Investigation(2018)

나. 사이버보험 시장동향[20]

1) 개요

여기에서는 미국의 사이버보험 상품을 분석한 Romanosky et al.(2017)의 내용을 정리해서 소개하고자 한다.

Romanosky et al.(2017)의 추정에 의하면, 미국의 경우 전체적으로 약 2,000~3,000개의 사이버보험 상품이 존재할 것으로 추측된다. 따라서 모든 주를 대상으로 보험상품을 분석하기에는 대상 상품의 수가 너무 많아서, 인구 수 기준으로 인구 수가 많은 뉴욕, 펜실베니아, 캘리포니아 3개 주를 선택하여 분석하였다.

데이터의 출처는 NAIC의 SERFF Filing Access System[21]으로 2007년부터 2017년까

20) 전 세계 시장에서 미국시장이 대략 85~90%를 차지하고 있으며, 수입보험료 규모로는 25억~30억 달러 정도 됨(OECD 2017)

21) SERFF Filing Access System은 1990년대 NAIC가 보험상품 신고 절차를 보다 용이하게 하기 위해 만든 시스템임

지의 180개 신고서류를 대상으로 분석하였다.[22] Romanosky et al.(2017)의 분석 내용 가운데 본고에서는 담보와 요율체계를 중심으로 소개하고자 한다.

2) 담보

담보의 경우에는 2009년부터 2016년 사이의 69개 상품을 대상으로 분석하였는데, 아래 표에는 주요 보장(Coverage) 대상과 제외(Exclusion) 대상이 열거되어 있다. 관련 상품의 수에 따라 순위를 매겨 상위 10개 항목만 소개하였다. 예를 들어 보장 대상의 경우에는 배상책임 관련 비용이 가장 많은 수의 보험상품에 포함되어 있었고, 제외 대상의 경우에는 범죄 또는 사기행위가 1위를 차지하였다.

〈표 Ⅲ-5〉 미국 사이버보험 상품의 주요 보장대상과 제외대상

주요 보장(Coverage) 대상	주요 제외(Exclusion) 대상
1. 배상책임액(Cost of Claims Expenses)	1. 범죄 또는 사기행위(Criminal or Fraudulent Act)
2. 언론대응비용(Public Relations Services)	2. 부주의(Negligent Disregard for Computer Security)
3. 통지비용(Notifications to Affected Individuals)	3. 제3자 시스템 오작동으로 인한 손실(Loss to System Not Owned)
4. 사후서비스비용(Services to Affected Individuals)	4. 신체상해(Bodily Injury)
5. 데이터복구비용(Data Restoration)	5. 계약상 배상책임(Contractual Liability)
6. 영업손실(Business Income Loss)	6. 테러, 전쟁(Act of Terrorism, War, Military Action)
7. 과학수사비용(Forensics)	7. 천재지변(Act of God)
8. 협박으로 인한 지불액(Data Extortion Expense)	8. 지적재산권 도난(IP Theft)
9. 데이터손실(Data Loss)	9. 정부압류(Seizure or Destruction of Systems by Government)
10. 피해비용(Cost of Damages)	10. Fines, Penalties, Fees from affected institutions

자료: Romanosky et al.(2017)

22) 사이버보험 상품은 NAIC의 보험상품 분류에서 일반배상책임보험, 전문직배상책임보험 등의 항목에 해당됨

Romanosky et al.(2017)는 담보와 관련된 향후 이슈로 다음 두 가지를 언급하였다. 첫째, 현행 약관에는 '컴퓨터', '시스템', '네트워크' 등의 용어는 언급되어 있으나, '모바일 기기', '드론', 기타 'IoT 기기' 등에 대해서는 아무런 언급이 없다. 이러한 용어들이 '컴퓨터', '시스템', '네트워크' 등의 기존 개념에 포함되는지가 현재로서는 불분명하며, 따라서 향후 문제가 될 수 있다.

둘째, IT 인프라의 상호연관성이 증가하면서 2차 피해도 증가할 것으로 예상되는데, 이러한 2차 피해의 보장 여부가 주요 이슈가 될 것으로 예상하였다.

3) 요율체계

요율체계의 경우에는 96개의 상품을 대상으로 분석하였다. 요율체계의 경우에는 상품 관련 일반자료 이외에 주 보험감독국에 별도로 제출하는 설명 자료를 참조하였다. 신고 서류의 내용을 보면, 사이버보험은 새로운 분야여서 아직 손실 추정에 필요한 데이터가 충분히 집적되어 있지 않다고 답변하였다.

요율산출 방법의 경우 자체 요율을 사용하는 경우는 소수였으며, 대다수가 외부기관의 자료를 활용하였다. 빈도의 경우에는 Computer Security Institute Computer Crime and Security Survey나 Hartford Steam Boiler Inspection and Insurance Company(이하 'HSB'이라 함)/Ponemon Survey 등을 참고하였고, 심도의 경우에는 HSB/Ponemon Survey 또는 Graziado Business Review 등을 참고하였다. 일부는 추측에 의해 요율을 산정했다고 한 경우도 있고, 경쟁기업의 상품을 참고해서 개발한 경우도 있었다.

요율산출에 있어서 대다수가 청구 데이터(Claim Data)는 사용하지 않았는데, 그 이유는 최근 3년간 거의 지급사례가 없었기 때문이다. 대안으로 전문직 배상책임보험 등 유사 보험상품의 손실 데이터를 사용하기도 했다.

Romanosky et al.(2017)의 분석에 의하면, 미국 사이버보험 상품의 요율체계는 크게 세 가지로 구분할 수 있다. 첫째, 단일요율(Flat Rate Pricing), 둘째, 기본요율+보상한도액 인상계수(Base Rate with Modifications), 셋째, 정보보안 상태 추가반영 요율

(Information Security Pricing)로, 첫 번째가 가장 단순한 형태이고, 세 번째가 가장 발전된 형태의 요율체계이다.

96개의 상품 가운데 첫 번째 유형의 요율체계를 사용하는 상품은 모두 31개였고, 두 번째 유형도 31개, 세 번째 유형은 34개였다.

가) 단일요율

가장 대표적인 예는 Insurance Services Organization(ISO)에서 개발한 CyberOne 상품의 요율체계이다.

아래 표에는 보장한도가 10만 달러이고, 자기부담금은 1만 달러인 경우의 단일요율 사례가 제시되어 있다. 단일요율의 경우에는 빈도와 심도의 추정치만 있으면 보험료를 계산할 수 있다. 빈도와 심도의 추정은 대개 외부기관의 자료를 활용한다.

〈표 Ⅲ-6〉 미국 사이버보험 상품의 단일요율 사례

담보	빈도	심도	예상손실	사업비	보험료
컴퓨터 공격	0.20%	$49,800	$99.60	보험료의 35%	$153
네트워크 보안소홀 배상책임	0.17%	$86,100	$147.23	보험료의 35%	$227

주: 1) 예상손실=빈도×심도
2) 보험료=예상손실+사업비=예상손실+0.35×보험료 → 보험료=예상손실/0.65
3) 보장한도는 10만 달러, 자기부담금은 1만 달러
자료: Romanosky et al.(2017)

나) 기본요율+보상한도액 인상/할인계수

두 번째 요율체계의 경우에는 우선 기업의 매출액이나 자산규모에 따라 기본 보험료가 결정된다. 그 다음 보장한도, 자기부담금의 규모, 해당 기업이 속한 산업의 유형에 따라 보험료가 조정된다. 보장한도가 높을수록, 그리고 자기부담금은 낮을수록 보험료는 높아진다. 산업의 경우에는 상대적인 위험도에 따라 보험료의 가감이 있다. 이 경우 보험료는 기본 보험료에 보상한도액 인상계수 또는 할인계수를 곱해서 결정된다. 대다수 보험회사의 설명 자료에 인상계수 산출과정에 대한 명확한 설명이 없는 것으로 보아

아직까지는 객관적인 자료에 근거해 인상/할인계수가 산출되는 것 같지는 않다.

다음 표는 매출액과 자산규모에 따른 기본보험료 사례이다.

〈표 Ⅲ-7〉 미국 사이버보험 상품의 기본보험료 사례

[사례 ①]

(단위: 달러)

매출액	연간 기본보험료
1,000만 이하	1,913.91
1,000만~2,000만	2,602.92
2,000만~5,000만	3,502.46
5,000만~1억	5,224.98

[사례 ②]

(단위: 달러)

자산규모	기본요율	자기부담금
1억 이하	5,000	25,000
1억~2.5억	7,000	25,000
2.5억~5억	8,500	50,000
5억~10억	11,000	100,000
10억~25억	14,000	150,000
25억~50억	16,500	250,000
50억~100억	20,000	250,000
100억~250억	26,000	500,000
250억~500억	35,000	500,000
500억~750억	41, 000	1,000,000
750억~1,000억	45,000	1,000,000

자료: Romanosky et al.(2017)

다음 표는 보장한도 및 청구이력 관련 보상한도액 인상계수 사례이다. 기본보험료에 조정계수를 곱하게 되면 보험료가 가감된다.

〈표 Ⅲ-8〉 미국 사이버보험 상품의 보험요소 관련 인상/할인계수 사례

[보상한도 관련 인상/할인계수]

(단위: 달러)

보상한도	인상/할인계수
50만	0.809
100만	1.000
200만	1.132
300만	1.245
400만	1.371
500만	1.405

[청구이력 관련 인상/할인계수]

구분		최소값	최대값
양호	Very Favorable	0.75	0.85
↑	Favorable	0.90	0.99
	Average	1.00	1.00
	Slightly Unfavorable	1.01	1.15
	Materially Unfavorable	1.16	1.25
↓	Very Unfavorable	1.26	1.40
불량	Extremely Unfavorable	1.41	1.70

자료: Romanosky et al.(2017)

다음 표는 산업 관련 인상 및 할인계수 사례이다. 표에서 보듯이 회사별로 다양한 분류 방법이 사용되고 있다.

〈표 Ⅲ-9〉 미국 사이버보험 상품의 산업 관련 인상/할인계수 사례

[사례 ①]

구분	산업	인상/할인계수
저위험 그룹	회계, 광고, 건설, 제조업	0.85
중위험 그룹	에너지, 엔터테인먼트, 호텔	1.00
고위험 그룹	바이오, 정보집적, 게임, 공공분야	1.20

[사례 ②]

구분	개인정보 보유규모	산업
저위험 그룹	소규모의 개인정보 보유	농업
중위험 그룹	중규모의 개인정보 보유	도매
고위험 그룹	대규모의 개인정보 보유	소매

[사례 ③]

구분	내용	인상/할인계수
클래스 1	보유 정보는 단지 직원 관련 정보	0.804
클래스 2	고객의 금융계좌 정보 보유(사회보장번호는 미보유)	1.000
클래스 3	고객의 사회보장번호 보유	1.497
클래스 4	고객의 민감정보를 대량으로 보유	1.905

자료: Romanosky et al.(2017)

다) 정보보안 상태 추가반영 요율체계

보험요소 및 산업 관련 인상/할인계수 이외에 추가로 정보보안 상태를 반영한 요율체계로 현재로서는 가장 발전된 형태의 요율체계이다. 아래 표에 정보보안 상태 관련 인상/할인계수 사례가 있다.

〈표 Ⅲ-10〉 미국 사이버보험 상품의 정보보안상태 관련 인상/할인계수 사례

[사례 ①]

구분	인상/할인계수		
	평균 이하	보안상태 평균	평균 이상
Privacy Controls	1.20	1.00	0.80
Network Security Controls	1.20	1.00	0.80
Content Liability Controls	1.20	1.00	0.80
Laptop and Mobile Device Security Policy	1.10	1.00	0.90
Incident Response Plan	1.10	1.00	0.90

[사례 ②]

구분	인상/할인계수			
	Excellent	Good	Fair	Poor
Data Classification	0.75 ~ 0.85	0.85 ~ 1.00	1.00 ~ 1.25	1.25 ~ 1.50
Security Infrastructure				
Governance				
Risk and Compliance				
Payment Card Control				
Media Controls				
Computer System Interruption Loss				

자료: Romanosky et al.(2017)

다. 사이버보험 시장활성화 전략

사이버보험 시장활성화 전략은 크게 공급 측면과 수요 측면으로 구분할 수 있다. 공급 측면의 전략으로는 데이터 축적, 정부와 민간의 위험분담 등이 있고, 수요 측면의 전략으로는 사이버위험 인식제고, 상품 표준화, 조세지원 등이 있다.[23] 여기서는 조세지원 정책을 중심으로 살펴볼텐데, 그 이유는 주요국 가운데 미국이 유일하게 사이버보험 관련 조세유인 제도에 대해 논의가 진행되고 있기 때문이다.

2016년 펄머터(Perlmutter) 의원은 사이버보험에 가입한 기업에 세제혜택을 부여하는 법안인 Data Breach Insurance Act(이하 'DBIA'이라 함)를 발의하였다. 기업이 사이버 보안 가이드라인인 National Institute of Standards and Technology Cybersecurity Framework를 도입하고 사이버보험에 가입할 경우 보험료의 15%를 세액공제해주는 정책이다.

일반적으로 조세유인 정책이 정당화되는 경우는 경제학 용어로 '외부성(Externalities)'이 존재하는 경우이다. 외부성이 존재할 경우 정부의 적절한 개입이 없으면 개인이나 기업의 의사결정은 사적으로는 최적일 수 있지만 사회 전체적으로는 바람직하지 못한 결과를 가져오게 된다. DBIA의 발의도 바로 이러한 외부성 논리에 근거하고 있다. 적절한 조세유인 정책이 없을 경우 기업이 사회적으로 바람직한 수준의 위험관리 체계를 갖출 가능성은 낮다는 점이다.

DBIA와 연관성을 가지는 연구 가운데 Romanosky(2016)가 있다. 이 논문은 실증연구를 통해 기업이 자발적으로 보안투자를 늘릴 사적 유인(Private Incentive)이 없음을 보였다. 사적 유인 측면만 분석하고 사회 최적과 관련된 부분은 다루지 않았다는 점에서 DBIA의 정당성을 100% 뒷받침해주는 연구는 아니지만, 적어도 자발적으로 위험관리 수준을 제고할 유인은 없음을 보여준 점에서 DBIA와 관련성을 가지는 연구 가운데 하나로 거론되고 있다.

23) OECD(2017)

[참고] Romanosky(2016) 실증연구 소개

Romanosky(2016)는 기업들이 보안수준을 높이기 위해 자발적으로 투자할 유인이 존재하는지를 살펴보기 위해 사이버 사고의 피해비용을 분석하였다. 분석 대상은 2004년부터 2015년까지의 약 12,000건의 사이버 사고이고, 관련 데이터는 Advisen[24]으로부터 입수하였다.

Advisen이 집적하고 있는 사이버 사고는 크게 네 가지 유형으로 구분되는데 ① 정보유출, ② 보안사고(DoS 공격 등이 해당됨), ③ 프라이버시 침해(개인정보의 무단 수집이 해당됨), ④ 사이버 금융범죄(피싱 등이 해당됨)이다.

정보유출의 경우 사고비용은 크게 당사자(First-Party) 비용과 제3자 (Third-Party) 비용으로 구분된다. 당사자 비용에는 과학수사비용, 정보유출 대상 개인에게 통지하는 비용, 언론대응 비용, 정보유출 피해자의 신용 모니터링 또는 개인정보도용보험 가입 비용 등이 해당된다. 제3자 비용에는 배상손해액과 금전적 제재 지불액 등이 해당된다. 보안사고와 사이버 금융범죄의 경우에는 금전적 손해액으로 피해비용을 측정한다.

약 12,000건의 사고 데이터 가운데 피해비용 정보가 존재하는 데이터는 921건으로 전체 데이터의 약 7.3%에 해당된다. 또한, 피해비용의 내용과 관련하여 한 가지 주의할 점은 Advisen의 데이터에는 시장가치 변동, 평판손실, 외부효과 등은 포함되어 있지 않다. 사이버 사고 피해기업의 직접 비용만 포함되어 있고, 간접비용이나 사회적 비용 등은 제외되어 있다고 볼 수 있다.

비용분석 결과를 요약하면 다음과 같다. 첫째, 피해액의 평균값(Mean Value)은 약 600만 달러이고, 중간값(Median Value)은 약 17만 달러로 둘 사이에 큰 차이가 존재하였다. 이러한 결과가 나오는 것은 일부 피해액이 큰 사고가 평균값을 높이기 때문이다. 50% 이상의 사이버 사고는 피해액이 20만 달러 이하이다. 매출액 대비 비중으로는 0.4%에 해당한다. 이러한 결과는 보험금 지급 데이터를 분석한 NetDiligence(2014)의 결과와도 일치한다. 보험금 지급액의 중간값은 약 14.4만 달러였다. 반면, 대기업 관련 사고의 보험금 지급액 평균값은 약 300만 달러였다.

더구나 공개되지 않은 사이버 사고의 경우 피해액은 더 적을 가능성이 높기 때문에, 이러한 점을 고려한다면 Advisen DB에 포함되어 있지 않은 사고까지 포함한 전체 사고의 평균값과 중간값의 차이는 Romanosky(2016)의 경우보다 더욱 클 수 있다.

둘째, 2004년부터 2014까지의 사고유형별 피해액의 변화를 살펴보면, 금융범죄와 프라이버시 침해의 경우 사고 비용이 감소한 반면, 보안 사고의 경우는 완만한 증가 추세를, 그리고 정보유출의 경우는 2008년 이후 빠른 증가세를 보였다. 정보유출의 피해액이 가파르게 증가한 이유는 자산규모 상위 25%에 속하는 대기업 관련 사고의 피해액이 증가했기 때문이다. 오히려 중소기업의 경우에는 2005년 이후 피해액이 감소하였다.

셋째, 산업별로 피해액을 살펴보면 총 피해액과 사고 당 평균 피해액 규모면에서 상위 10개 분야는 각각 다음 표와 같다.

〈표 Ⅲ-11〉 총 피해액과 사고당 피해액 규모 기준 상위 10개 분야

총 피해액 규모 기준	사고당 평균 피해액 기준
1. 정보산업	1. Management
2. 제조업	2. 소매업
3. 소매업	3. 정보산업
4. 금융과 보험	4. 제조업
5. 의료	5. 도매업
6. 도매업	6. 숙박 및 음식
7. 과학·기술 서비스	7. 금융과 보험
8. 공공분야	8. 부동산, 임대, 리스
9. 숙박 및 음식	9. 과학·기술 서비스
10. 교통	10. 교통

넷째, 설문조사 자료에 의해 기업의 보안투자 지출규모를 추정해보면 대략 매출액의 0.025% 정도 된다. 이러한 수치를 이용해 추정한 기업의 보안투자 지출액과 사이버 사고 피해액을 비교해보면, 50% 이상의 기업의 사이버 사고 피해액과 보안투자 지출액이 거의 일치하였다.

이러한 결과로부터 Romanosky(2016)는 기업 입장에서 볼 때, 현재 수준보다 보안 투자를 더 늘릴 유인은 존재하지 않는다는 결론을 내렸다.

Romanosky(2016)가 논문에서 명시적으로 언급하지는 않았지만 그의 연구결과는 위험관리 수단의 선택과 관련하여 일부 함의를 제공한다. 사이버 사고의 위험관리 수단으로 보안투자와 사이버보험 두 가지를 생각해볼 수 있는데, Romanosky(2016)의 실증결과에 의하면 어떤 전략을 선택하는 것이 좋은가? 그의 연구에 의하면, 피해액의 평균값과 중간값이 상당한 차이를 보이고 중간값이 예상보다는 높지 않은 수준이었다. 이러한 점을 감안할 때 보안투자의 수준을 피해액 평균값에 맞추어서 강화하는 것은 기업 입장에서는 매우 큰 비용이 될 수 있다. 현실적인 접근법은 중간값 정도의 수준에서 보안 최소기준을 설정하고 그 이상의 위험은 보험을 통해 커버하는 전략이 더 바람직하지 않나 생각된다. 특히, 중소기업의 경우에는 피해액이 크지 않다는 점에서 더더욱 사이버보험이 유용한 위험관리 수단이 될 수 있지 않을까 생각해본다.

24) Advisen은 사이버 사고 관련 데이터를 집적하여 보험회사에 판매하는 미국계 영리기관임

2. 유럽

가. 사이버 사고동향

유럽 지역의 경우 사이버 사고동향에 관한 종합적이고 체계적인 통계체계가 아직 구축되어 있지 않다. 다만 2014년 중앙유럽대학교(CEU) 부속연구기관인 Center for Media, Data and Society(이하 'CMDS'이라 함)[25]는 유럽 30개국[26]을 대상으로 2005년부터 2014년 3/4분기까지의 개인정보 유출 사고를 조사하였다(〈표 Ⅲ-12〉 참조).[27] 국가별, 분야별 조사결과를 보면, 국가별로는 1인당 건수 측면에서 영국, 그리스, 노르웨이 순으로 나타났으며, 분야별로는 비즈니스의 개인정보 유출 건수가 가장 많은 비중을 차지하였다(〈표 Ⅲ-13〉와 〈표 Ⅲ-14〉 참조).

한편, 영국 국가통계청(ONS)[28]은 2016년 7월부터 설문조사를 통해 사이버 범죄 건수를 조사하기 시작하였다.[29] 영국 국가통계청(ONS)에 따르면 사이버 범죄 건수는 2016년 약 4만 5천 건에서 2017년 약 6만 9천 건으로 53.0% 증가하였다. 사이버 범죄 가운데는 괴롭힘(Harassment and Stalking)이 약 4만 2천 건으로 가장 많았으며, 다음으로 외설물(Obscene Publications)이 약 1만 건, 아동 성범죄(Child Sexual Offences)가 약 7천 건, 협박(Blackmail)이 약 2천 건 등의 순이었다(〈표 Ⅲ-15〉 참조).

25) Howard and Gulyas(2014)

26) 여기서 말하는 30개국은 EU회원국(28개)과 노르웨이, 스위스를 포함함

27) CMDS는 30개국의 개인정보 유출 사고에 관한 신문기사의 보도내용을 바탕으로 개인정보 유출 사고 건수 및 개인정보 유출 건수를 집계하였음

28) Office for National Statistics(2018)

29) 이는 영국 국가통계청이 실시한 설문조사 수치이며, 따라서 영국에서 발생한 실제 사이버 범죄 수치와 다를 수 있음

〈표 Ⅲ-12〉 유럽 지역 연도별 개인정보 유출 추이

(단위: 만 건)

구분	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014
건수	4,571	1,704	2,522	5,707	87	75	11,510	1,678	32,206	4,138

주: 2014년 개인정보 유출 건수는 2014년 3/4분기까지 집계된 수치임
자료: Howard and Gulyas(2014)

〈표 Ⅲ-13〉 유럽 지역 국가별 개인정보 유출 현황

(단위: 백만 명, 백만 건, %, 건)

국가	인구	건수	비중	1인당 건수
영국	63.5	139.7	63.7	200.0
독일	82.7	56.4	25.7	68.2
그리스	11.1	9.0	4.1	81.0
노르웨이	5.1	4.1	1.9	79.0
네덜란드	16.7	3.9	1.8	23.0
기타	344.5	2.8	2.8	-
전체	523.7	6.2	100.0	-

주: 개인정보 유출 건수는 2005년부터 2014년 3/4분까지 집계된 수치를 의미함
자료: Howard and Gulyas(2014)

〈표 Ⅲ-14〉 유럽 지역 분야별 개인정보 유출 현황

(단위: 백만 건, %)

구분	비즈니스	교육	정부	의료	군사	비영리	기타	전체
건수	538.3	0.0	59.2	9.3	0.9	1.8	32.3	606.9
비중	88.7	0.0	9.7	1.5	0.2	0.3	5.3	100.0

자료: Howard and Gulyas(2014)

〈표 Ⅲ-15〉 영국 사이버 범죄 현황

(단위: 천 건)

구분	괴롭힘	외설물	아동 성범죄	협박	기타	전체
2016	26.2	6.3	5.4	2.3	4.8	44.9
2017	41.8	10.0	7.3	2.2	7.4	68.6

자료: Office for National Statistics(2018)

한편, 어드바이젠(Advisen)에서 집계한 유럽의 대표적 사이버 사고는 다음과 같다(〈표 Ⅲ-16〉 참조).

〈표 Ⅲ-16〉 최근 유럽의 주요 사이버 사고 현황

사고명	보도일시	사고내용
뉴스 인터내셔널(News International)의 도청 행위	2011년 7월	전화 도청 행위로 영국의 뉴스 인터내셔널 발행이 중단되면서 총 4억 3천만 달러의 손실이 발생
스코틀랜드왕립은행(Royal Bank of Scotland) IT 시스템 사고	2013년 7월	소프트웨어 업데이트 오류로 인해 IT 시스템이 마비되면서 1억 2천 5백 만 유로의 손실이 발생
Crelan 은행 자금 도난	2016년 1월	피싱 공격으로 벨기에 은행인 Crelan에서 7천만 유로의 자금 도난이 발생
토크토크(Talk Talk) 개인정보유출	2016년 2월	해킹으로 영국 정보통신기업 토크토크 고객 10만 명의 정보가 유출되면서 약 6천만 유로의 손실이 발생
러시아 중앙은행(CBR) 자금 도난	2016년 12월	해킹으로 러시아 중앙은행에서 20억 루블의 자금 도난이 발생
생고빙(Saint Gobain) 랜섬웨어 감염	2017년 6월	랜섬웨어인 '페티아(Petya)' 공격으로 프랑스 생고빙의 IT 시스템이 마비되면서 약 2억 9천만 달러의 손실이 발생
A.P. 몰러머스크(A.P.Moller-Maersk) 랜섬웨어 감염	2017년 6월	랜섬웨어인 '페티아(Petya)' 공격으로 A.P.몰러머스크의 IT 시스템이 마비되면서 약 2억 5천만 달러의 손실이 발생
페이스북(Facebook) 고객정보 불법수집	2017년 9월	페이스북이 프랑스와 스페인에서 개인정보 무단 수집으로 각각 과징금 15만 유로, 120만 유로 처분을 받음

자료: Advisen(2017)

나. 사이버보험 시장동향[30]

1) 시장규모

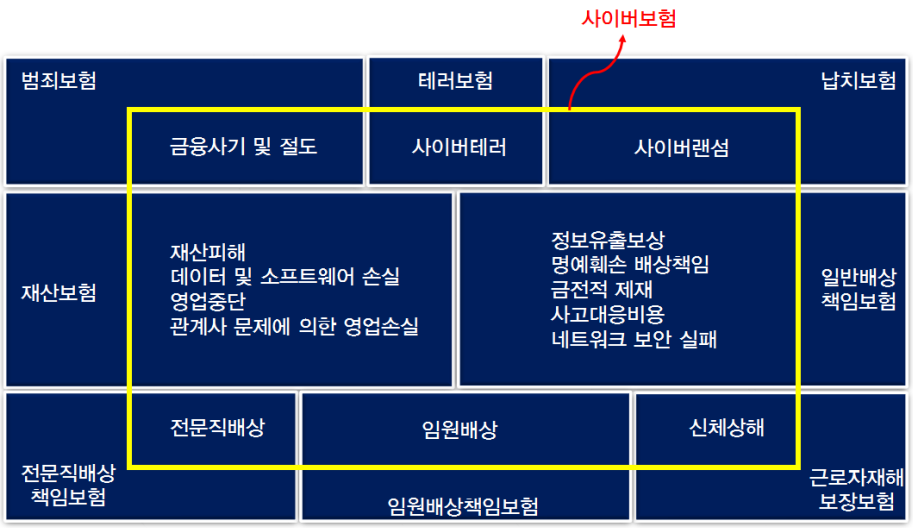
2016년 기준으로 단독형 사이버보험 상품의 전 세계 수입보험료 규모는 약 25억~35억 달러로 추정되고 있다. 전 세계 시장에서 유럽은 약 5~9% 비중을 차지하고

30) OECD(2017)에서 인용함

있으며, 수입보험료 규모는 1.5억~4억 달러 정도 된다.

한편, 기존 기업성 보험에 특약 형태로 포함되어 있는 사이버보험의 규모는 통계가 존재하지 않아 파악이 어렵다. 사이버보험과 기존 보험의 담보영역 중복은 다음 그림과 같다.

〈그림 Ⅲ-1〉 단독형 사이버보험과 기존보험의 담보영역 중복



자료: OECD(2017)

2) 담보[31]

OECD 국가의 보험회사들을 대상으로 설문조사한 결과에 의하면, 대부분의 보험상품에서 보장하는 손실과 거의 보장이 제공되지 않는 손실은 다음 표와 같다.

31) OECD(2017)의 설문조사에 의하면, 단독형 사이버보험 상품의 경우에 국가별로 차이를 보이지 않았는데, 그 이유는 대부분의 보험회사가 글로벌 시장을 대상으로 보험상품을 개발·공급하기 때문임

〈표 Ⅲ-17〉 OECD국가의 사이버보험 상품 담보

사고유형	대부분 보장이 제공되는 손실	거의 보장이 제공되지 않는 손실
정보유출	• 사고대응비용 • 규제 및 법적 방어비용 • 정보유출배상비용	• 지적재산권 도난 등 당사자 정보 유출 • 평판손실
시스템 오작동	• DoS 공격에 의한 영업중단 • 보안관리 소홀로 제3자 시스템에 준 피해 관련 배상책임	• 유형자산 피해 • 신체상해 • 제3자 서비스 사업자의 문제로 인한 영업 손실
데이터 손상	• 데이터 삭제나 훼손에 의한 손실 • 사이버 랜섬에 의한 손실	-
기타	-	• 금융 도난 및 사기 • 사이버 테러

자료: OECD(2017)

사이버 랜섬의 경우에 범죄자에게 지불하는 금액도 보상범위에 포함시켜야 하는지에 대해서는 논란의 여지가 있다.

지재권을 포함한 당사자 정보유출을 보장하는 상품은 거의 없었다. OECD(2017) 조사에 의하면, 조사 대상의 5% 이하였다. 지재권 도난이 일반적으로 보장범위에서 제외되는 이유는 가치평가의 어려움에 있다. 예를 들어, 아직 출시되지 않은 신제품의 디자인을 도난당한 경우 손실액 추정이 매우 어렵다.

유형자산 피해는 거의 보상하지 않았으나 최근 들어 일부 변화를 보이고 있다. 2013년에 로이즈가 SCADA 시스템에 대한 사이버 공격으로 인해 발생한 유형자산 피해에 대해 보상하였다.

금융 도난 및 사기의 경우에는 절반 이하의 상품에서 보상을 제공하였는데, 수치가 낮은 이유는 기존 범죄 보험에서 사이버 관련 범죄에 의한 손실도 보장하고 있기 때문이다. 사이버 테러는 대부분의 상품에서 제외 대상이었으나, 점차 테러 제외 조항을 삭제하는 방향으로 변화하고 있다.

개인을 대상으로 한 사이버보험 시장도 일부 새로운 움직임이 있는데, 현재는 주로 부유층을 대상으로 한 상품개발이 영국 등 일부 국가에서 이루어지고 있다.

3) 가입률

가입률은 설문조사에 따라 수치에 있어서 차이를 보여서 신뢰할만한 데이터라고 보기는 어렵다. 유럽 전체적으로는 가입률이 24~30% 정도 되었다. 영국의 경우에는 2~38%, 독일의 경우에는 30% 정도 되었다.

업종별로 보면, 대량의 제3자 개인정보를 수집하는 금융, 의료, 소매, 교육, 호텔, 게임 분야가 상대적으로 높은 가입률을 보였다.[32] 그러나 최근 들어 당사자 피해에 대한 관심이 높아지면서 제조업의 사이버보험 가입도 증가하고 있다.

기업규모별 가입률을 살펴보면, 중소기업의 가입률은 대부분의 국가에서 낮은 수치를 보였다. 예를 들어, 프랑스의 경우 한 설문조사에 의하면, 거대기업은 60~70%, 대·중기업은 40%, 중·소기업은 2~3%의 가입률을 기록했다. 그러나 최근 들어 중소기업의 가입률이 증가하고 있는데, 영국의 경우 2014년 2.1%에서 2016년 13.7%로 증가했다.

4) 보장한도

최대 보장한도는 대기업의 경우 약 5~7억 달러 정도 되며, 국가별로 큰 차이를 보이지는 않는다. 독일과 오스트리아의 경우 최대 5억 유로까지 보장한다.

평균 보장한도는 미국의 경우 2016년 기준으로 약 1,690만 달러 정도 되었으며, 영국의 경우에는 100만~500만 파운드, 그리고 프랑스의 중소기업은 15만~20만 유로 정도 되었다.

32) 영국의 경우에는 주로 소매, 의료, 금융 분야에 집중되었음

5) 요율

영국의 경우 보장한도가 100만 파운드인 한 사이버보험 상품의 보험료는 3만 파운드였다. 다른 일반 손해보험 상품의 경우 평균적으로 100만 파운드 보장 상품의 보험료는 약 1만 5천 파운드 정도이다.[33] 유럽의 경우에는 보장한도가 5,000만~9,000만 유로인 상품의 보험료는 100만 유로당 약 2,000~5,000유로 정도 되었다.

다. 사이버보험 시장활성화 전략

유럽의 경우 크게 공급 측면과 수요 측면 활성화 전략으로 구분할 때, 공급 측면의 경우에는 데이터 집적에, 그리고 수요 측면의 경우에는 위험인식 제고에 초점을 맞추고 있다.[34] 데이터 집적의 경우에는 전(全)유럽 차원에서, 그리고 인식 제고는 개별 국가별 보험협회 중심으로 추진되고 있다.

1) 전(全)유럽 차원

사이버보험 시장이 활성화되기 위해서는 공급 측면에서 상품개발 및 언더라이팅 능력 제고가 필요한데, 이러한 것들이 가능하기 위해서는 우선적으로 충분한 데이터의 집적이 필요하다. 유럽의 경우 2018년 5월부터 시행에 들어가는 일반정보보호규칙(General Data Protection Regulation, 이하 'GDPR'이라 함)의 주요 내용 가운데 하나가 정보유출 통지의무제도이다. 통지의무를 위반할 경우 강한 금전적 제재가 부과될 수 있다.

유럽 개별국가의 보험협회를 회원으로 하는 Insurance Europe은 GDPR의 시행을 통일된 형태의 사이버 사고 데이터 집적의 기회로 삼기 위해 노력하고 있으며, 그러한 노력의 일환으로 모든 나라에 공통으로 적용되는 사고 관련 보고 양식을 만들었다.

크게 3개 파트로 구성되어 있는데, 첫 번째 파트는 기업 관련 정보(Identification of

33) OECD(2017)의 설문조사에 의하면, 사이버보험 요율은 일반배상책임보험의 약 3배, 재물보험의 약 6배 정도 되었음

34) Insurance Europe 홈페이지 참조함

The Data Controller)이고, 두 번째 파트는 사고 관련 주요 정보(Principal Information on Data Breach)이고, 세 번째 파트는 보충 정보(Complementary Information)이다. 보고 양식의 세부 항목은 다음 [참고]와 같다.

[참고] Insurance Europe의 보고 양식[35)]

I. 회사 및 담당자 정보

1. 회사정보(Details of Company)
2. 담당자(Contact Person) 정보
3. 통지 유형
   1) 일괄통지(주요 정보와 보충 정보를 사고인지 후 72시간 이내에 일괄적으로 통지)
   2) 순차통지(주요 정보는 사고인지 후 72시간 이내에 통지하고, 보충 정보는 4주 이내에 통지)

II. 주요 정보

1. 해당 회사가 속한 산업(Sector of Affected Party)
2. 회사규모: 고용인수(Size: Number of Employees)
   1) 1~9
   2) 10~49
   3) 50~249
   4) 250~749
   5) 750~1,000
   6) 1,000~
3. 회사규모: 매출액(Size: Turnover)
   1) 200만 유로 이하
   2) 1,000만 유로 이하
   3) 5,000만 유로 이하
   4) 5,000만 유로 이상
4. 해당 회사의 본점 소재지(Member state where business has its main establishment)
5. 사고가 발생한 국가(Member state where the breach took place)
6. 사고발생 일시(Date/Time of the breach)
7. 사고인지 일시(Date/Time of detection)

35) Insurance Europe(2018)

8. 사고 원인을 알고 있는가?(모르는 경우에는 섹션 III의 8번에서 답변)
   1) 악의적 공격(Malicious Attack): 내부 또는 외부
   2) 사고(Accident): 시스템 오작동(System Failure)
   3) 부주의(Negligence): 인간의 실수(Human Error)
9. 악의적 공격의 결과라면, 다음 중 어디에 해당하는가?
   1) Trojans
   2) Encryption
   3) Cryptolockers
   4) DDoS(Distributed Denial of Service)
   5) Malware
   6) CEO-fraud
   7) Blackmailing
   8) Other(구체적으로 기술해주세요)
10. 사고에 의해 어떤 손실을 입었는가?
   1) Data Publication
   2) 데이터 도난(Data Theft)
   3) 신분도용 및 사기(Identity Theft or Fraud)
   4) 데이터 손실(Loss of Data)
   5) 데이터의 기밀성 훼손(Loss of Confidentiality of Personal Data)
   6) 재산피해(Property Damage)
   7) 직접적인 금전 손실(Direct Financial Loss)
   8) 영업 중단(Business Interruption)
   9) 배상책임 이슈(Liability Issues)
   10) 평판 훼손(Damage to the Reputation)
   11) 기타(구체적으로 기술해주세요)
11. 사고 데이터의 유형은?
   1) 개인(Personal) 정보
      (1) 민감(Sensitive) 정보: 의료 또는 유전자(Health or Genetic)
      (2) 非민감(Non-sensitive)
   2) 非개인(Non-personal) 정보
12. 사고 데이터의 유형이 개인정보인 경우 암호화(Encryption) 상태는?
   1) Full
   2) Partial
   3) None

13. 사고 데이터는 정보보호 영향평가의 대상이었는가?
 1) 예
 2) 아니오
14. IT 지원부서의 형태는?
 1) 내부
 2) 외부
15. 사고영향을 경감하기 위해 어떤 조치들을 취했는가?
 1) 데이터 복구
 2) 의심스러운 소프트웨어의 삭제
 3) 손상된 시스템의 교체
 4) 외부 전문가의 점검
 5) 보안조치의 강화
16. 해당 사고를 보장하는 보험에 가입했는가?
 1) 예
 2) 아니오

III. 보충 정보

1. 사고영향이 완료된 시점(Date/Time effects of attack ended)
2. Estimated Financial Damage
3. 피해대상 개인정보 범위(How many personal datasets were exploited/Affected/Stolen?)
4. 정보주체에게 유출 사실을 통지했나?
 1) 예
 2) 아니오
5. 몇 명의 정보주체에게 통지했나?
6. Estimated Financial Losses
 1) 통지비용(Cost of Notification)
 2) Financial Damage
7. 사이버 사고의 재발을 방지하기 위해 어떤 조치를 취했는가?
 1) 보안조치의 강화
  (1) 데이터 수집 절차의 감사 및 변경
  (2) 데이터 처리 절차의 감사 및 변경
  (3) 데이터 프로세서(Data Processor)의 감사 및 재평가
  (4) 데이터 암호화

2) 어떤 조치도 취하지 않았음
3) 기타 (구체적으로 기술해주세요)
8. 사고 원인은 무엇이었나?
1) 악의적인 공격
(1) 내부
(2) 외부
9. 원인이 밝혀졌다면, 악의적인 공격의 경우 그 배경은 무엇인가?
10. 원인이 밝혀졌다면, 악의적인 공격의 경우 어떤 소프트웨어가 공격의 수단으로 사용되었는가?
1) Malware
2) Ransomware
3) Phishing
4) SQL Injection Attack
5) Cross-Site Scripting(XSS)
6) Denial of Service(DoS)
7) Session Hijacking
8) Credential Reuse
9) Other(구체적으로 기술해주세요)

2) 개별 국가의 보험협회 차원

〈표 Ⅲ-18〉 EU 개별 국가별 보험협회 차원의 전략

국가	세부 전략
오스트리아	• (Development of Non-Binding Model Conditions for Cyber Insurance) 오스트리아 보험협회(VVO)는 권고 약관 개발을 추진
	• (Prevention and Awareness-Raising) 2017년 봄, 오스트리아 상공회의소(WKÖ)는 중소기업의 사이버위험 및 사이버보험 인식 제고를 위해 로드쇼 기획 • WKÖ의 온라인 플랫폼에서는 중소기업의 보안 상태를 자가 점검할 수 있는 온라인 테스트 제공
	• (Public-Private Partnership) 보험협회(VVO)는 도로안전위원회(KfV)와 함께 중소기업을 대상으로 사이버범죄 관련 설문조사를 실시하고 대비책 권고

〈표 Ⅲ-18〉 계속

국가	세부 전략
벨기에	• (Public-Private Partnership) 보험협회는 학계, 정부, 민간단체로 구성된 사이버 보안 협의체에 참여
덴마크	• (Public-Private Partnership) 보험협회는 덴마크 경찰과 국가 사이버 범죄 센터가 설립한 포럼의 회원으로 참여 • 포럼의 회원들은 사이버 공격 관련 정보 교환
프랑스	• (Public-Private Partnership) 보험협회는 정보 시스템 보안 관련 국가 기관인 ANSSI의 주도하에 설립된 GIP-ACYMA의 일원으로 참여 • ACYMA의 목적은 사이버 공격 피해자를 돕는 데 있음
	• (Prevention and Awareness-Raising) 2017년 5월, 보험협회는 중소기업에게 사이버위험에 대한 정보를 제공하기 위해 브로슈어 배포
	• ("Le Club des Juristes") 보험협회는 2016년 10월, 사이버위험 및 사이버보험 관련 싱크탱크인 "Le Club des Juristes"의 설립을 주도
	• (Standard-Setting and Certification) 보험협회 부속 표준화 기관인 CNPP에서는 2017년 6월에 보안표준인 APSAD D32 발표
	• (Digital Certificate for Insurers) 2020년까지 보험회사 직원들은 디지털 자격증을 획득해야 함
독일	• (Prevention and Awareness-Raising) 보험협회(GDV) 부속 표준화 기관은 중소기업을 위한 사이버 보안 가이드라인을 만들어 배포
	• (Non-Binding Wording for Cyber Insurance) 보험협회(GDV)는 2017년 3월 중소기업을 위한 권고 약관을 개발
네덜란드	• (Prevention and Awareness-Raising) 보험협회(VVN)는 2015년 정부, 중소기업협회와 함께 중소기업의 사이버위험 인식 제고를 위한 로드쇼 추진 • 또한, 소비자와 기업에 사이버위험 관련 정보를 제공하는 인터넷 포털을 구축
	• (Emergency Response Team for the Insurance Sector) 보험협회는 보험회사를 위한 사이버 사고 대응 팀을 조직
	• (Public-Private Partnership) 보험협회는 정부, 학계, 민간단체가 참여하는 사이버위험 인식 제고 캠페인인 Alert Online의 일원으로 참여
스페인	• (Prevention and Awareness-Raising) 보험협회 부석 표준화 기관인 Cepreven에서는 중소기업이 자신의 사이버위험을 점검할 수 있는 "자가진단 설문" 배포
스웨덴	• (Public-Private Partnership) 보험회사가 포함된 스웨덴 은행 주도 민관 협력체에서는 사이버 사고 시나리오 개발 중
스위스	• (Public-Private Partnership) 보험협회는 스위스 국가 사이버 전략 위원회의 일원으로 참여 • 보험협회의 사이버 워킹그룹은 시나리오 및 영향뿐만 아니라 데이터 교환 및 국가의 역할 등에 대해서도 연구

〈표 Ⅲ-18〉 계속

국가	세부 전략
영국	• (Prevention and Awareness-Raising) 보험협회는 2016년 5월, 중소기업을 위한 사이버보험 안내책자 발간
	• (Public-Private Partnership) 국가 사이버 보안 센터는 "사이버 보안 정보 공유 파트너십"을 통해 사이버 위협을 정부와 민간 사이에 실시간으로 공유 • 파트너십은 2013년에 시작되었고, 보험산업은 주요 회원 가운데 하나임
	• (Development of Cyber Scenarios) 로이즈를 중심으로 사이버 사고 시나리오 모델 개발

자료: Insurance Europe 홈페이지(2018년 5월 현재)

3. 일본

가. 사이버 사고동향

일본은 인터넷, IoT 등 사이버 공간을 활용하는 기기의 발전과 사이버 공격 빈도, 기술 진화, 추적기술 발전 등으로 2017년 사이버 공격 추적 건수가 사상 최대로 증가한 것으로 나타났다. 국립연구개발법인 정보통신연구기구(National Institute of Information and Communications Technology: 이하 'NICT'이라 함)에 의하면 〈표 Ⅲ-19〉와 같이 사이버 공격 건수가 2017년 1,504억 건으로 1 IP당 약 56만 건이 추적되어 2010년 대비 총 건수 약 2.5배, 1 IP당 건수 약 10배 이상 증가한 것으로 나타났다.[36]

〈표 Ⅲ-19〉 일본 사이버 공격 추적 건수 추이

(단위: 건)

구분	2005	2010	2015	2016	2017
연간 관측패킷 수	3.1억	56.5억	545.1억	1,281억	1504억
연간 관측IP 수	1.6만	12만	28만	30만	30만
IP당 연간 관측 수	19,066	50,128	115,323	469,104	559,125

자료: NICT(2018)

36) NICT(2018)

특히, IoT 보급에 따른 TV, 감시 카메라, 휴대형 라우터 등 IoT 기기 사용이 최근 크게 증가하고 있으나 IoT에 대한 낮은 보안의식과 보안대책 미흡으로 인하여 공격받은 기기 중에서 IoT 기기가 26% 비중을 차지하는 등 IoT 관련 사이버 공격이 크게 증가하고 있는 추세이다.

반면, 기업이 사이버 공격 사고가 발생하였다고 보고한 건수는 감소한 것으로 나타났다. 일본 JPCERT/CC(Japan Computer Emergency Response Team/Coordination Center)[37] 에 의하면 기업이 사이버 공격으로 사고가 발생했다고 보고한 건수가 〈표 Ⅲ-20〉과 같이 2017년 18,141건으로 2013년 29,191건보다 37.9% 감소한 것으로 보고하고 있다.

〈표 Ⅲ-20〉 일본 사이버 공격 사고 보고 건수 추이[1]

(단위: 건)

구분	2013	2014	2015	2016	2017
보고 건수	29,191	22,255	17,342	15,954	18,141

주: 1) JPCERT/CC에게 보고 접수한 Computer Security Incidents 보고 건수임
자료: JPCERT/CC(2018)

한편, 특정비영리활동법인 일본네트워크시큐리티협회(Japan Network Security Association: 이하 'JNSA'이라 함)[38] 개인정보 유출 사고[39]가 발생하였다고 공개적으로 기업 홈페이지 또는 신문기사 등에서 밝힌 건수가 감소하고 있지만 인터넷 등을 통한 대규모 유출에 따라 유출 피해자 수는 증가하고 있다고 조사하였다. JNSA 조사에 의하면 공개된 개인정보 유출 사고 건수는 〈표 Ⅲ-21〉과 같이 2016년 468건에 불과하나 유출된 인원 수는 1,396만 5,227명으로 2013년 대비 각각 66.3% 감소, 50.9% 증가한 것으로 추정하였다. 이에 따라 2016년 1건당 정보 유출 인원수는 3만 1,453명이며, 1건당 또는 1인당 평균 손해배상액은 각각 6억 2,811만 엔, 3만 1,646엔에 이를 것으로 판단하였다.

37) JPCERT/CC는 국내외 일본 기업 등에서 발생한 Computer Security Incidents 보고 접수 업무를 정부로부터 위탁받아 대행함

38) JNSA는 인터넷 또는 신문상에서 개인정보유출 건수를 수집하는 방식으로 집계함

39) PC, 휴대폰, 이메일, 인터넷, USB, FTP, 지면

〈표 Ⅲ-21〉 일본 개인정보 유출 관련 공개사고 건수 및 손해배상액

주요 내용	2013	2016
개인정보 유출 피해자 수	925만 2,305명	1,396만 5,227명
공개한 사고 건수	1,388건	468건
추정 손해 배상액	1,438억 7,184만 엔	2,788억 7,979만 엔
1건당 유출 인원 수[1)]	7,031명	3만 1,453명
1건당 추정 평균 손해배상액[1)]	1억 926만 엔	6억 2,811만 엔
1인당 추정 평균 손해배상액	2만 7,701엔	3만 1,646엔

주: 1) 피해자 불명인 사고 24건을 제외하여 산출함
자료: JNSA(2014); JNSA(2017a)

JNSA가 분석한 유출사고 원인은 〈표 Ⅲ-22〉와 같이 기업 및 수집자의 관리부실, 기기 및 통신 오작동, 부정 접촉, 분실, 부정한 정보 탈취, 도난, 설정오류, 시스템 취약, 바이러스 등의 순으로 비중이 높은 것으로 나타났다.

〈표 Ⅲ-22〉 일본 개인정보 유출 원인(유출 건수 기준)

(단위: %)

유출원인	비중	유출원인	비중
관리 부실	34.0	설정 오류	4.7
오동작	15.6	시스템 취약	1.7
부정 접촉	14.5	Worm 바이러스	1.1
분실	13.0	내부 부정행위	0.9
부정한 정보 탈취	6.8	목적 외 사용	0.4
도난	5.3	기타	1.9

자료: JNSA(2017b)

일본은 2015년 6월 일본연금기구[40)] 해킹으로 125만 명의 개인정보가 유출된 사건을 계기로 개인식별번호인 마이넘버의 도입이 이뤄지는 등, 일본 산업 전반에 걸쳐 정보보안 취약성에 대한 위기감과 주의 환기 의식이 점차 확산되고 있는 중이다.

40) 우리나라의 국민연금관리공단에 해당함

〈표 Ⅲ-23〉 일본 사이버 공격에 의한 주요 개인정보 유출 사례

연도	회사명	유출 건수	원인	주요내용
2013	Yahoo! JAPAN	최대 2,200만 건	해킹	해킹에 의해 ID가 유출되어 148만 건의 비밀번호 유출 추정
2014	Benesse Co.	760만 건	외부 반출	통신교육업체 개인정보 유출 가능성
2015	일본연금기구	125만 건	해킹	우리나라의 연금관리공단에 해당하는 연기금기구에서 가입자 개인정보가 유출
2016	IPSA	42만 건	해킹	화장품회사 서버에 보관된 가입자 개인정보 유출 가능성
2017	오사카대학	8.1만 건	해킹	재직 및 재학 중인 교수, 교직원, 학생 개인정보 유출
2017	Yamakei Co.	최대 22만 건	피싱	사이트 회원 이메일에 피싱 방법으로 개인정보 유출 가능성
2017	동경도청	67.6만 건	해킹	동경도청 세금납입 사이트에서 신용카드 정보 유출
2017	NHK	3,300건	직원 분실	외주업체 직원이 개인정보가 포함된 방송 수신료 결제정보 분실

자료: https://ja.wikipedia.org

나. 사이버보험 시장현황

1) 시장규모 및 가입률

일본은 2003년 개인정보보호 관련 법률이 제정된 후 개인정보 취급에 대한 사회 전반의 관심이 높아지고 있으나, 정보보호관련 보험시장 규모는 크게 성장하지 못하고 있다. 다만, 사이버 공격과 대규모 개인정보 유출 사고 발생 증가에 대비한 일본 정부의 사이버 사고 시 재산피해에 대한 리스크 관리 대책 마련 추진 등에 따라 향후 일본의 사이버 보험시장이 발전할 것으로 전망된다.

JNSA가 조사한 일본 사이버보험 시장규모는 2006년 70억 엔에 불과하였으나, 2015년 118억 엔으로 증가하였다. 최근에는 대기업의 정보 보안대책 강화와 기업의 정보유출 리스크 대비에 대응하는 차원에서 보험제도가 활용되고 다양한 부가서비스의 등장으로 2016년도 182억 엔, 2018년도 197억 엔으로 증가할 것으로 추정하였다.

〈표 Ⅲ-24〉 일본 보안 및 정보보호 보험시장 규모 추정

(단위: 억 엔, %)

구분	2014	2015	2016	2017	2018
정보보안 툴 시장	4,489	4,705	4,959	5,306	5,563
정보보안 서비스시장	3,939	4,260	4,523	4,659	4,892
정보보안 보험시장	105	118	182	188	197
보험시장 증가율	-	12.4	54.2	3.3	4.8
전체	8,533	9,083	9,664	10,153	10,652

자료: JNSA(2017a); JNSA(2018)

일본 독립행정법인 정보처리추진기구(Information-technology Promotion Agency: 이하 'IPA'이라 함)의 실태조사(복수응답)에 의한 사이버보험 가입률은 컴퓨터 수리보험, 정보유출 보험, 사이버보험 등 하나 이상의 보험에 가입한 기업의 비율이 14.6%로 주요 선진국보다 낮은 수준을 나타났다. 종목별 가입률은 정보유출보험 9.2%, 사이버보험 5.2%, 컴퓨터 복구비용 10.4%로 추정된다.

〈표 Ⅲ-25〉 일본 정보유출·사이버보험 가입률 실태

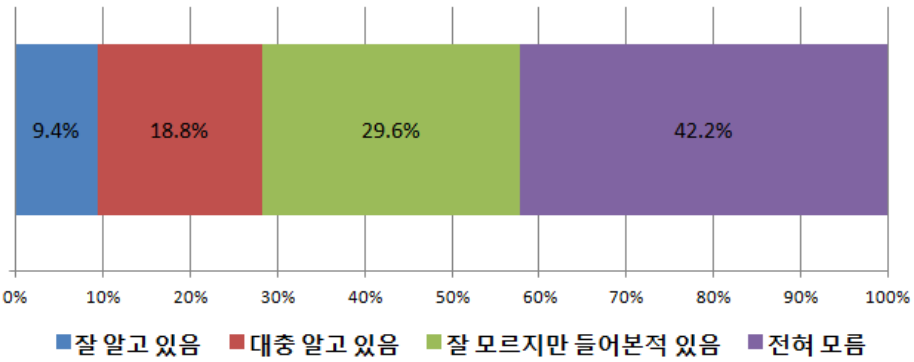
(단위: %)

구분	보험 인지 유무	컴퓨터 고장보험	정보유출 보험	사이버 보험
대기업(10억 엔 이상)	21.5	15.5	14.9	9.7
중견기업(10억 엔 미만 1억 엔 이상)	26.1	10.2	8.4	3.6
중소기업(1억 엔 미만)	17.4	4.9	3.9	1.7
전체	28.2	10.4	9.2	5.2

자료: IPA(2015)

일본의 낮은 보험 가입률은 최근 기업의 대규모 정보유출 사고 발생에도 불구하고 〈그림 Ⅲ-2〉에서 보는바와 같이 일본 기업의 사이버보험에 대한 낮은 인식에 기인한 것으로 판단된다.

〈그림 Ⅲ-2〉 일본 기업의 사이버보험 인식 실태



자료: IPA(2015)

2) 보험 유형

일본 정보보안 관련 보험은 IT시스템이나 IT시스템에서 취급되는 정보에 관련한 손해를 보장하는 보험이며, 주요 보장내용은 보험회사에 따라 차이가 있지만 3가지로 구분할 수 있다.

① 개인·회사 정보 유출 등에 따른 제3자 배상책임

② 이에 따른 기업 손해, 멸실 이익

③ 변호사비용·제3자 전문기관 조사비용 등

①의 보험상품은 1990년대 후반부터 제조업을 중심으로 가입이 활성화된 제조자책임(PL)보험 연장선에서 정보보안 피해보상특약을 부가적으로 기업이 가입하는 보험으로 보험시장의 대부분을 차지하고 있다. 반면, ②의 보험상품에는 아직까지 일본 기업들이 거의 가입하지 않은 실정이다.

일본의 보험상품 종류는 〈표 Ⅲ-26〉과 같이 크게 개인정보 취급사업자를 대상으로 한 개인정보유출 보험과 기업이 법인정보 및 IT시스템 운영 중에 업무상 고의 또는 실수 등으로 인하여 발생한 비용손해를 보장하는 IT정보보호 손해보험으로 구분할 수 있다.

〈표 Ⅲ-26〉 일본 정보보호 보험종류

보험종류	가입대상	보상내용
개인정보 취급사업자 보험	· 개인정보를 취급하는 모든 사업자 및 개인	· 개인정보DB 해킹 · 개인정보 기록물(서류, PC, CD 등) 도난, 분실 · 고객메일 송부 실수 등
IT 관련 정보보호 손해보험	· 정보 서비스 제공 · S/W 개발 · ISP · 콘텐츠 서비스 제공자 · 어플리케이션 서비스 제공자 등 · IT를 활용하는 제조업, 운송업, 학교 등	· 데이터 손실 파괴 · 시스템, 네트워크 중단·사용불능 · 정보유출 · 저작권 침해 · 프라이버시 침해 등

자료: 한국침해사고대응팀협의회(2017)

개인정보 취급사업자 대상 보험은 가입형태에 따라 대형IT업체를 대상으로 한 개별보험과 중소기업들이 보험상품을 공동 구매하는 형식을 띤 단체보험으로 구분할 수 있다.

단체보험은 일본 상공회의소 및 지방상공회의소 회원을 대상으로 개인정보유출보험이 판매되고 있다. 동 상품은 단체할인보험료를 적용하며, 개인정보보호법에 대응한 리스크 진단 서비스 등을 무료로 제공하여 중소기업의 개인정보 유출리스크를 경감하고 있다.

개별 기업성 상품의 주요 보장내용은 개인정보 유출 또는 그 유출 우려가 발생하여 피보험자가 법률상 손해배상책임을 부담함으로써 입는 손해와 사죄광고비용, 사죄글 작성비용 등의 사고 후 수습으로 지출한 비용 손해를 보상한다. 개인정보 유출보험은 〈표 Ⅲ-27〉과 같이 배상책임보장과 비용손해보장으로 구성되며 피보험자에게 보험기간중 일본 국내에서 손해배상청구가 이루어진 경우에 보상한다. 동 상품에서 신용카드 유출 위험담보 특약을 부대할 경우 신용카드번호, 계좌번호, 비밀번호 등의 유출로 인한 손해를 보상한다. 보험기간은 1년이다.

〈표 Ⅲ-27〉 개별 기업형 개인정보유출보험 상품의 주요내용

구분	배상책임부분	비용 손해 부분
지급 사고	개인정보 유출 또는 유출 우려에 대해 피보험자에게 보험기간 중 손해배상을 청구할 경우	개인정보 유출 또는 유출 우려가 있고 그 사실이 공적기관에 보고되거나 TV, 신문 등에 발표된 경우
보장 내용	1. 법률상 손해배상금 2. 배상 책임에 관한 소송비용·변호사 비용 등의 소송비용 3. 구상권 보전 행사 등 손해방지 경감비용 4. 사고 발생 시의 긴급 조치비용 5. 보험사 요구에 따른 협력비용	1. 사과광고비용·회견비용 2. 사과문 작성 배송비용 3. 위로금·위문품 구입비용 4. 컨설팅 비용 5. 콜 센터 위탁비용 등
사전 동의 여부	· 1~4는 지출 전 보험사의 동의 · 2는 손해배상금 액수가 지불한도액을 초과할 경우 비율보상	· 4는 지출 전 보험사의 동의
한도액	1회 청구당 · 보험기간 중 500만 엔~10억 엔	사고당 · 보험기간 중 100만 엔~1억 엔
면책금액	1회 청구당 0엔 또는 1만 엔~1,000만 엔	사고당 0엔 또는 10만 엔 (단, 피해자 1명당 위로금 · 위문품 구입비용 500엔 한도, 컨설팅비용 사고당 500만 엔 한도)

자료: http://www.tokiomarine-nichido.co.jp/hojin/baiseki/roei/

개인정보 유출보험의 보험요율을 산출하기 위한 보험료 산출단위는 〈표 Ⅲ-28〉과 같이 해당 기업의 연간 매출액으로 하고 있으며, 기본요율과 리스크 관리 정도에 따른 할인할증이 적용된다.

〈표 Ⅲ-28〉 일본 개인정보유출보험 보험료 수준(연간 매출액 기준)

(단위: 엔)

구분	책임부분 보상한도액	비용부분 보상한도액	보험료
200억 엔 편의점	3억	3천만	약 47만
100억 엔 인터넷 소매, 통신판매업자	1억	3천만	약 39만
30억 엔 정보서비스 사업자	5천만	1천만	약 20만

자료: http://www.tokiomarine-nichido.co.jp/hojin/baiseki/roei/

기본요율은 업종과 보상한도액, 자기부담금의 조건에 따라 차이가 발생한다. 보험료에 대한 할인할증은 개인정보관리체계의 양호여부에 따라 최대 40%까지 할인이 가능하다. 프라이버시 마크나 ISO 등 국제기준의 인증을 취득한 경우에는 최대 30%까지 할인이 가능하며, 두 가지를 합산하여 최대 60%까지 할인이 가능하다.

〈표 Ⅲ-29〉와 같이 현재 대형 4개 손해보험회사의 개인정보 유출 관련 보험이 공통적으로 보장하는 담보는 멸실이익, 사업계속비용, 원인구명, 조사비용, 종업원 초과근무 각종 수당, 위로금 및 사죄 광고비용이다. 또한, 3개 손해보험회사가 공통적으로 보장하고 있는 담보는 소송비용, 컨설팅비용, 콜센터 운용비용, 해외소송대응비용, 리스크 평가 할인비용 등이다.

〈표 Ⅲ-29〉 손해보험회사의 사이버보험 담보현황

번호	담보내용	A사	B사	C사	D사
1	멸실이익	○	○	○	○
2	사업 계속비용	○	△	○	△
3	사업계속 불가능 시 손해배상, 소송비용	○	-	○	○
4	정보유출 손해배상, 소송비용	○	-	○	○
5	타인 매체의 정보유출에 의한 손해배상, 소송비용	-	-	○	○
6	신용카드 직접손해에 의한 손해배상, 소송비용	-	-	○	-
7	원인규명, 포렌식 조사의뢰비용	○	-	-	○
8	데이터 복구비용	○	○	○	○
9	2차 손해·피해확대 방지비용	○	-	○	-
10	종업원 초과근무·교통비·숙박비	-	○	-	○
11	기자회견·SNS·미디어 대응비용	○	○	○	○
12	종업원 초과근무·교통비·숙박비	○	-	-	○
13	컨설팅	-	○	○	○
14	콜센터 운영비용	○	○	○	-
15	위로금·사죄광고비용	○	○	○	○
16	재발방지책비용	-	○	-	-
17	공적기관으로부터 배상청구, 감사 대응비용	○	-	-	-
18	해외소송 대응	○	○	○	-
19	자사공개내용에 의한 타인 침해	-	-	○	○
20	교육프로그램 툴 제공	-	-	○	-
21	리스크 평가할인	-	○	○	○

자료: 歌原崇(2016)

보험회사의 사이버보험은 2012년 AIU사가 처음으로 종합 사이버 리스크에 대한 보험 상품을 판매하였으나 판매한 이후 2년 동안 판매실적이 부진하였다. 주요 이유는 일본 국내 총생산(GDP) 대비 사이버 범죄 손해액의 비율이 주요국[41]보다 현저히 낮고 일본 국내에서 사이버 범죄가 증가하고 있으나 사이버 리스크에 대한 기업들의 인식이 아직 부족한 상황이기 때문인 것으로 판단된다.

그러나 이러한 상황 속에서도 최근 세계적인 사이버 범죄의 증가 추세와 사이버 리스크 보험시장 확대 전망에 따라 일부 손해보험회사가 2015년부터 기업의 사이버 리스크에 대한 보험상품을 적극적으로 판매하기 시작했다.

〈표 Ⅲ-30〉 일본 손해보험회사에서 판매 중인 주요 사이버보험

구분	AIU	동경해상	미츠이스미토모	손보재팬
상품명	CyberEdge	사이버리스크 보험	사이버보안 종합보험	사이버보험
판매 시기	2012. 12	2015. 2	2015. 9	2015. 10
보상 내용	· 손해배상 책임 (손해배상, 소송비용 등) · 위기관리 대응 (사고원인 조사·피해확대 방지비용, 데이터 복구비용, 컨설팅비용 등) · 정보유출 대응 (위로금비용, 행정 지원비용 등) · 사업중단 대응 (사업 중단에 따른 손실이익 등)			
해외 소송	해외에서의 손해배상 청구 소송 배상금·소송비용도 담보			

자료: 篠原拓也(2016)

일본 사이보험의 특징은 첫째, 정보보안과 관련하여 보험가입 의무화를 명시한 조항은 없고 개인 또는 기업의 자율적 가입의사에 따른 임의보험 방식으로 운영되고 있다. 둘째, 기업을 상대로 개인정보 유출을 입증하는 데 곤란한 법률적 한계로 인하여 현재까지 일반 소비자의 개인정보 유출 리스크에 대비한 보험상품은 거의 없고 주로 개인사업자 또는 기업의 정보유출과 관련된 기업성 보험상품이 대부분이다.

41) 2014년 발표된 조사보고서에 의하면 국내총생산(GDP) 대비 사이버 범죄 손해액의 비율은 독일이 1.6%, 미국이 0.64%, 영국이 0.16%, 일본 0.02%임

다. 사이버보험 시장활성화 전략

1) 민간분야

가) 협회 등 공동가입 방식

일본상공회의소는 소속 회원사 제공을 목적으로 손해보험회사에 맞춤형으로 보험상품 개발을 의뢰하여, 현재 상공회의소 홈페이지에서 판매하고 있다. 일본 상공회의소가 보험상품을 직접 판매하고 있지는 않지만 상공회의소와 6개 손해보험회사(2018년 6월 말 기준)가 개발한 사이버보험 상품에 가입할 경우, 회원사에게 보험료 단체할인이 제공하므로 가입 유인이 상당히 큰 것으로 판단된다. 상공회의소가 판매 중인 개인정보유출 배상책임보험(사이버 리스크 보상형) 상품은 현재 동경해상을 포함하여 6개 손해보험회사가 인수하고 있으며, 상공회의소 회원기업은 6개 보험회사의 가격조건 등 제안내용을 평가하여 특정 보험회사를 선정할 경우 손해보험회사의 소속 보험대리점이 해당 보험회사의 가입 절차를 진행하게 된다.

일본상공회의소와 손해보험회사가 공동 개발한 정보유출배상책임보험은 〈표 Ⅲ-31〉과 같이 기본형 상품과 확장형 상품으로 구분된다. 기본형 상품은 일본 국내에서 발생하는 정보유출에 기인한 손해배상과 소송비용을 포함한 타인의 업무장해 등에 대한 손해배상을 보장한다.

확장형 상품은 일본 국내·외에서 발생하는 사고를 대상으로 한다. 보장내용은 기본형 상품의 보장에 추가적으로 사이버 공격에 기인한 타인의 신체장해·재물손괴에 관한 손해배상과 정보보안 관련 사고에 기인하여 발생할 우려가 있는 조사비용, 모니터링비용, 복구비용 피해예방비용, 재발방지비용 등의 비용보상 등을 보장한다.

〈표 Ⅲ-31〉 일본 상공회의소의 사이버보험 상품 개요

구분	구분	내용
기본형	보장내용	· 국내에서 발생하는 정보유출에 기인한 손해배상 · 소송비용 · 타인의 업무장해 등에 대한 손해배상
	보험료	· 기업의 업종, 매출액, 배상책임 한도에 따라 부과
	예시 보험료	· 연간 매출액 5,000만 엔 음식점업의 경우 1회 배상책임 한도를 1,000만 엔(비용보상 100만 엔)으로 설계할 경우 30,000엔 · 연간 매출액 3억 엔 인터넷서비스업의 경우 1회 배상책임 한도를 5,000만 엔(비용보상 500만 엔)으로 설계할 경우 81만 엔
확장형	보장내용	· 기본형 상품 보장 · 사이버 공격에 의한 타인의 신체장해·재물손괴에 관한 손해배상 · 정보보안 관련 사고에 기인하여 발생할 우려가 있는 조사비용, 모니터링비용, 복구비용 피해예방비용, 재발방지비용 등의 비용보상 등
	보험료	· 기업의 업종, 매출액, 배상책임 한도에 따라 부과
	예시 보험료	· 연간 매출액 5,000만 엔 음식점업의 경우 1회 배상책임 한도를 1,000만 엔(비용보상 100만 엔)으로 설계할 경우 30,000엔 · 연간 매출액 3억 엔 인터넷서비스업의 경우 1회 배상책임 한도를 5,000만 엔(비용보상 500만 엔)으로 설계할 경우 84만 엔

자료: https://hoken.jcci.or.jp/compromise

연간 보험료는 업종과 연간 매출액에 따라 차이가 있는데, 〈표 Ⅲ-32〉와 같이 연간 매출액 5,000만 엔 음식점업의 경우 1회 배상책임 한도를 1,000만 엔(비용보상 100만 엔)으로 설계할 경우 기본형과 확장형이 각각 3만 엔 수준이다.

또한, 연간 매출액 3억 엔 인터넷서비스업의 경우 1회 배상책임 한도를 5,000만 엔(비용보상 500만 엔)으로 설계할 경우 기본형과 확장형이 각각 81만 엔과 84만 엔 수준이다.

〈표 Ⅲ-32〉 상공회의소 단체보험(확장형) 보험료 수준(2018. 3기준)

(단위: 엔)

업종	연매출액	보상한도		면책	보험료
		배상책임	비용손해		
도매업	20억	3억	3천만	-	19만
제조업	10억	1억	1천만	-	9만
인터넷서비스업	3억	5천만	5백만	-	84만
음식점	5천만	1천만	100만	-	3만
건설업	10억	5천만	100만	10만	10만
인쇄업	2억	5천만	100만	10만	10만
일반소매업	2천만	1천만	100만	10만	3만

주: 1) 상기 보험료는 단체할인 20%가 반영되었으며, 면책금액 10만 엔 업종은 기본형 상품임
2) 인터넷서비스업 보험료는 IT업무특약이 포함된 가격임
자료: https://hoken.jcci.or.jp/compromise

나) 가전제품 등의 부가상품으로 개발

동경해상일동화재보험과 일본 마이크로소프트(MS)는 자택에서 원격 근무 시 정보 유출 손해를 보장하는 보험상품을 개발하여 2018년 2월부터 판매하고 있다. 최근 일본 기업의 35%가 재택근무제도를 도입하는 등 원격근무 수요가 확산됨에 따라 기업이 보급하는 PC를 통해 재택근무자가 본사에 보고하는 근로환경이 크게 변화하고 있다. 이러한 재택근무자 대부분은 현재 이미 Window 10(OS)이 탑재된 PC를 사용하거나 마이크로소프트(MS)의 Window 7 지원 종료 전략에 따라 2020년부터 Window 10이 탑재된 PC를 사용할 가능성이 높아졌다. 동경해상은 일본의 재택근무 활성화와 MS의 PC Window 환경변경 도래에 따라 재택근무자가 사용하는 PC에서의 사이버 리스크 발생 가능성을 예상하여 MS Japan과 판매제휴 전략을 체결하였다.

동경해상은 기업 또는 지자체 등을 대상으로 단독상품으로 판매하거나 MS 등 IT시스템회사와 공동으로 Window 10이 탑재되어 있는 PC를 판매할 경우 부대하는 보험상품으로 판매하고 있다. 보험금 지급사유는 컴퓨터를 인터넷에 접속했을 때 바이러스 감염으로 고객 정보가 유출 또는 단말기를 통해 공격하여 사내 시스템이 고장이 났을 경우의 손해 등과 단말기 분실도 보상한다. 보장한도는 1대 당 최대 300만~500만 엔의 보험금을 지급한다.[42]

42) 동경해상 보도자료(2018. 1. 21)

세계적인 전자제품 생산회사인 일본의 Canon은 중소기업용 보안기기와 손보재팬의 사이버보험을 세트하여 2017년 7월부터 판매하고 있다. 보안기기가 바이러스 피해를 입을 경우 보상한다.[43] 또한, Panasonic은 판매하는 IoT 기기를 구입하는 소비자의 사이버 피해를 보상하기 위하여 IoT 기기와 사이버보험(동경해상)을 결합하여 판매하고 있다.[44]

다) 중소기업 전용 공동상품 개발

미츠이스미토모해상과 아이오이닛세이동화손해보험은 중소기업의 사이버 사고 리스크에 대응하기 위하여 보험상품을 공동으로 개발하여, 2018년 1월부터 사이버 프로텍터, 사이버 보안보험의 명칭으로 각각 판매하고 있다. 동 보험상품은 보장범위에 따라 세 가지 플랜으로 구성되며, 보장특징은 해외에서 손해배상 청구 시 보험금 지급, 공적조사 대응비용, 피해확산 방지비용, 정보유출 및 바이러스 등 사고 피해 방지 예방비용, 복구비용, 재발방지비용을 보장한다.

라) 업무제휴와 부가서비스 제공[45]

최근 일본 손해보험사들은 사이버보험뿐만 아니라 전문회사와 업무 제휴를 통하여 사이버 사고 예방 부가서비스를 개발 및 제공하고 있는 사례가 증가하고 있다.

아이오이닛세이동화손해보험과 미츠이스미토모해상은 기업고객의 사이버 공격 예방 서비스를 제공하기 위하여 미국의 기업대상 사이버 보안 전문회사인 Stroz Friedberg[46]와 2018년 1월과 3월에 각각 업무제휴를 체결하였다. 사이버보험 계약 체결시 기업의 정보유출 손해배상을 보장함과 동시에 기업 IT시스템의 문제점을 파악하여 보안대책

43) Canon 보도자료(2017. 6. 13)

44) 동경해상 보도자료(2018. 1. 21)

45) NIKKEI NEWS(2018. 3. 8), あいおいニッセイ 米企業と提携、サイバー事業強化; _____(2018. 1. 25), 三井住友海上 サイバーリスク診断、米ベライゾンと提携

46) Stroz Friedberg는 미국 FBI 전 수사관들이 2000년에 설립한 사이버 보안회사로 사이버 범죄 조사가 주요업무이고, 구글과 아마존닷컴 등이 주요 고객임

을 제안하고 사고 발생 원인 조사 서비스를 부가적으로 제공하였다.

또한, 아이오이닛세이동화손해보험과 미츠이스미토모해상은 기업고객에게 사이버 리스크 진단서비스를 제공하기 위하여 사이버 공격 진단 서비스를 제공하는 미국의 Verizon Communications와 2018년 1월에 업무제휴를 체결하였다. Verizon은 시스템 위험도 점수화, 문제점 보완을 위한 예방대책 등을 제공하는데, 위험도 조사의 경우 사이버 사고 데이터를 기초로 기업의 고객정보 관리체계와 네트워크 감시체계를 점검한 후, Verizon이 보유한 정보유출 사고 등의 분석 결과를 활용하여 리스크를 수치로 나타낸다. 예방대책 수립의 경우에는 시스템 문제점이나 관리체계 미비 등을 검사하고, 제조 및 금융업 등 산업별 위험도를 평가한 후 바이러스 감염이나 스파이, 내부 비리 등 업종별로 유행하고 있는 최신 공격 방법에 대한 대책을 수립한다.

동경해상일동화재보험도 기업고객에게 사이버 리스크 진단 서비스를 제공하기 위해 미국의 Cyence(사이버 리스크 모델링 전문)사와 업무제휴를 체결하여 사이버 리스크 종합지원서비스인 Benchmark Reporting Service를 2017년 10월부터 시작하고 있다. 사이버보험에 가입한 기업을 대상으로 자사의 객관적인 정보에 근거한 분석 결과, 리스크 지표의 업계 보안수준을 파악할 수 있는 정보 등을 무료로 보고서 형태로 제공하고 있다.

마) 사이버 보안사업 진출

손해보험회사 그룹인 손보재팬은 고객에게 사이버 보안 관련 종합서비스를 제공하기 위하여 플랫폼을 구축하고, 2017년 1월부터 사이버 보안 사업에 진출하였다.[47] 고객의 사이버 리스크 실정에 맞는 해결방안을 리스크 진단에서 보험금 지급까지 원스톱으로 제공하는 플랫폼을 통해 사이버 보안대책 솔루션을 제공하고 있다. One-Stop플랫폼에는 간이보안진단, 고도진단, 내부기준 수립, 보안 강화 및 대책, 감시·감독, 사고대응, 보험금 지급의 각 서비스가 탑재 된다. 손보재팬은 진출 초기에 전문 회사와 업무제휴 형태로 서비스를 제공하지만 2019년부터 본사 내 SOMPO Digital Lab과 사이

47) 손보재팬 보도자료(2017. 12. 15)

버 보안사업 본부를 신설하여 서비스를 제공할 계획이다.

바) 보장확대 계획[48)]

일본은 2020년 동경올림픽 개최를 맞이하여 사이버 공격 및 테러 확대 전망으로, 사이버보험 시장규모가 2017년 대비 4배 성장하여 2020년에 약 600억 엔으로 확대될 전망이다. 이에 대비하여 일본 손보사들은 정보 유출 방지대책과 시스템 복구비, 사이버상 명예(이미지)훼손 피해보상, 보안진단 등의 상품과 부가 서비스 제공을 확대할 계획이다. 미츠이스미토모해상과 아이오이닛세이동화손해보험은 관련 공동상품을 개발하고 2018년 1월부터 판매한다. 손보재팬은 미국과 유럽의 보험자회사에서 판매하고 있는 사이버보험 상품개발 경험을 기초로 2020년 사이버보험 상품 판매 목표액 100억 엔에 대한 계획을 수립하였으며, 동경해상은 미국 IT가입과 연계하여 기업의 사이버 위험 진단 서비스를 개시하고 있다.

사) 가정용 IoT 보험상품 개발[49)]

손보재팬은 최근 일본 가정 내 사이버 침투사고가 크게 증가함에 따라 IoT 가전제품에 바이러스 침투 등 새로운 위험에 대비하기 위하여 IoT 기능의 TV, 카메라 등 가전제품이 사이버 공격을 받을 경우 피해를 보상하는 '스마트 하우스'용 화재보험을 2018년 8월부터 판매하고 있다. 동 상품은 화재보험에 가정용 IoT 보험을 부대하는 형식으로 종전의 화재보험뿐만 아니라 IoT 가전제품이 바이러스 감염될 경우 수리비 및 복구비를 보장한다. IoT 보험 보장내용은 사이버 공격에 의해서 인터넷에 연결되는 TV, 컴퓨터, 조명 기기 등이 고장 났을 때의 수리비, 데이터 복구비 등이다. 특약보험료는 표준적인 철근 주택에서 연간 약 2천 엔이며, 사이버 피해 보상액은 최대 50만 엔 수준이다.

48) NIKKEI NEWS(2017. 11. 8), サイバー保険 補償広く, 損保、風評対応やリスク診断

49) NIKKEI NEWS(2018. 4. 18), 省エネ住宅の火災保険、サイバー攻撃に対応、損保ジャパン

2) 민관협력

가) 공시 및 인증제도 도입 추진

일본 총무성은 기업의 보안체계에 대한 정보 공시(사이버 대책에 보험 등 리스크 이전 방식 명시)를 위해 상장기업을 대상으로 기업통합보고서 또는 유가증권 보고서에 별첨으로 정보보안 보고서를 공시하도록 관련규정 개정을 2018년에 권고하였다. 대표 사례인 히타치그룹의 경우 50페이지 가량의 정보보안 보고서를 공개하고 있다. 관련 작업반에 참여 중인 3개 손해보험회사들은 향후 정보보고서 도입이 기업의 사이버 리스크 평가 및 보험료 할인·할증 등에 활용될 것으로 기대하고 있다.[50]

IPA는 중소기업의 자율적인 사이버 보안대책 수립을 활성화하기 위해 중소기업 정보보안 대책 가이드라인을 제정하였다. 동 기준은 정보공개를 간이 정보공개(★)와 상세 정보공개(★★)로 구분하고 상세 정보공개(★★)로 인증 받은 기업에게 사이버보험 할인 혜택을 부여한다.

나) 보험가입 자율규제

개인정보유출보험은 개인정보보호법, 사이버보험은 Cyber Security 경영 가이드라인 Ver 1.0(2015. 12), Ver 2.0(2017. 11)에 근거하고 있다. Cyber Security 경영 가이드라인은 주무부처인 경제산업성이 Cyber Security 기본법에 근거하여 산업계에 제시하는 자율규제이며, 사이버보험 가입을 권고하고 있으나 강제하고 있지는 않다.

〈표 Ⅲ-33〉 Cyber Security 경영 가이드라인 Ver 1.0

Cyber Security 경영 권고사항 TOP 10 중에서
TOP 3: 사이버 보안 리스크 파악과 보안 수준을 감안한 목표와 계획 수립
사이버보험 활용 또는 보호할 자산에 대해 전문기업에 위탁을 포함한 리스크 이전(보험가입 포함) 방안을 검토한 다음, 기타 리스크를 파악한다.

자료: 経済産業省(2017)

50) NIKKEI NEWS(2017. 12. 22), サイバー対策、企業に開示指針 総務省、保険料優遇も検討

〈표 Ⅲ-34〉 Cyber Security 경영 가이드라인 Ver 2.0

Cyber Security 경영 권고사항 TOP 10 중에서
TOP 4: 사이버 보안 리스크 파악과 리스크 대책의 실현
기업의 경영전략 관점에서 보호할 정보를 특정하고 사이버 공격의 위협과 영향으로부터 사이버 보안 위험을 파악하고, 리스크에 대응하기 위한 계획을 수립한다. 이때 사이버보험의 활용이나 보호할 정보에 대해서 전문 벤더에 위탁을 포함한 리스크 이전(보험가입 등) 방안을 검토한 다음, 기타 리스크를 파악한다.
TOP 9: 공급사슬(Supply Chain) Security 대책 추진
계열기업, 공급사슬(Supply Chain) 비니지스 파트너·시스템 관리의 경우 위탁처에 기인한 손해에 대한 리스크관리 확보 수단으로서 위탁처가 사이버보험에 가입하는 것을 권장한다.

자료: 経済産業省(2017)

사이버보안 정책수립 정부기구인 내각관방정보보안센터(National center of Incident readiness and Strategy for Cyber Security: 이하 'NISC'이라 함)는 사이버공간 이용자 활성화를 위한 각 부처 추진상황을 2015년부터 매년 점검하고 연차보고서를 발표하고 있다. 또한, IPA는 기업 경영자 또는 리스크관리 책임자 등을 대상으로 사이버 리스크에 대한 체제정비 상황 및 리스크 이전 수단인 사이버보험의 활용실태를 파악 및 조사하여 보고하고 있다.

NISC 연차보고서[51]에 의하면, 정부의 보조사업(공공, 위탁 등)과 연구개발사업 등의 선정 시 평가항목에 사이버 보안 운영 가이드라인이나 제3자 인증 취득, 기업의 사이버 보안 대책 수립을 가점요소로 고려하는 등의 인센티브 방안을 2018년까지 검토할 것을 경제산업성이 제안하였다.

라. 요약 및 시사점

일본은 2005년 개인정보보호법 제정 이후 사이버 사고로 인한 피해가 지속적으로 증가하고 있지만 시장 규모와 가입률이 각각 197억 엔(2018년), 14.6%(2015년)에 불과하는 등 미국과 유럽에 비해 사이버보험 시장 발전이 더디게 진행되고 있다.

그러나 최근 2020년 동경올림픽 개최를 앞두고 사이버 사고에 대비하여 민·관이 위

51) NISC(2017)

기관리 시스템을 강화함에 따라 기업의 리스크 관리 수단으로서 사이버보험 가입 필요성이 확산되고 있다. 최근에는 인터넷과 IoT 기기 등의 기술 발전과 대규모 사이버 사고로 인하여 개인정보 유출에 대한 국민의 관심이 높아져 리스크 관리를 위해 기업과 개인의 보험 가입 니즈가 증가하고 있다.

일본 사이버보험은 그동안 개인상품보다 기업상품이 주를 이루었다. 개인정보보호법 시행 직후 손해배상책임과 간단한 비용을 보상하는 개인정보유출보험이 주로 판매되었으나 최근에는 제3자 손해배상책임과 비용보상보험과 함께 추가적으로 피해방지비, 데이터 및 시설복구비, 조사 및 컨설팅비, 개인 위로금, 기업 이미지 실추에 대비한 언론홍보비 등 다양한 비용보상을 보장하는 상품의 판매가 주를 이루고 있다. 매출액이 큰 대기업의 경우 그동안 보험회사와 거래 관계를 통해 사이버 리스크 진단을 받고 보험에 가입하게 되지만 매출액이 적은 상당수의 중소기업 및 자영업자 등은 중앙상공회의소, 지방상공회의소, 각 산업협회, 공제단체, 지역 공동체 등 자사가 소속된 단체를 통해 단체할인과 맞춤형 서비스를 통해 가입하고 있다. 이러한 경제단체들이 보험회사와 기업 사이에서 보험가입의 매개 역할을 수행하고 있는 것이다. 대표적인 사례로 일본 상공회의소는 현재 소속 회원사의 권익을 위하여 보험상품을 맞춤형으로 보험회사에 개발 의뢰하여 보험상품을 제공하고 있다.

최근에는 보험회사가 가전회사 등과 상품을 공동으로 개발하는 등 상품공급자의 다양한 시도가 확대하고 있어 시사하는 바가 크다. 동경해상은 MS사와 함께 MS사가 판매하고 있는 PC Window에 사이버보험을 부가하여 2018년 중에 판매할 예정이며, Canon사와 손보재팬은 2017년부터 Canon 디지털 카메라 등의 인터넷 기반의 제품 판매시 사이버보험을 결합하여 일본에서 판매하고 있다. 또한, 손보재팬은 홈 CCTV 등에 의한 정보유출 사고가 증가함에 따라 주택화재보험에 IoT 기기 사이버 사고 보상보험을 특약형태로 개발하여 2018년 중에 판매할 예정이다. 이외에도 손해보험사들이 공동으로 보험상품을 개발하거나 국내외 사이버 리스크 전문기업과 업무제휴하여 사이버 보험상품에 부대할 수 있는 사고 예방, 진단 컨설팅 등의 부가서비스 상품을 개발하여 결합상품으로 판매하는 사례가 증가하고 있다.

일본은 정부 차원에서도 사이버보험 보급 확대를 포함한 기업의 사이버 리스크 관

리 방안 등 다양한 정책들을 검토하고 있다. 특히, 일본 정부는 미국과 유사하게 상장기업이 유가증권 보고서 작성 시 보험상품을 포함한 사이버 리스크 이전 수단 등을 명시하도록 하는 공시제도 도입 계획을 2017년에 발표한 바 있고, 기업이 자율적으로 보험 가입 등 사이버 리스크 이전 수단을 마련할 것을 권고하는 기업 경영가이드라인이 제정되어 시행되고 있다. 또한, 경제산업성은 정부 및 공공사업을 민간업체에 발주할 경우 사이버보험 가입을 포함한 사이버 대책수립 여부 등을 업체 선정평가항목에 반영하는 방안을 검토하고 있다.

4. 중국

가. 사이버 사고동향

중국 국가사이버대응센터[52]가 사이버 공격 건수[53] 및 사이버 사고 민원 건수[54]를 집계하고 있다. 2013~2016년 중국 사이버 공격 건수는 지속적인 증가세를 보이고 있다. 중국 사이버 공격 건수를 유형별로 살펴보면, 모바일 악성 프로그램 건수가 증가하고 있는 반면 컴퓨터 가짜 홈페이지, 컴퓨터 목마 바이러스, 홈페이지 해킹, 홈페이지 변조, 보안 취약점 건수는 감소하고 있다(〈표 Ⅲ-35〉 참조).

사이버 사고 민원 건수는 2013년부터 2015년까지 지속적으로 증가하였으나 2016년에는 감소세로 전환하였다. 다만 2016년 사이버 사고 민원 건수의 감소는 2015년 사이버 사고 민원 건수의 급증에 따른 기저효과 때문인 것으로 분석된다. 2016년을 제외한 사이버 사고 민원 건수를 유형별 살펴보면, 가짜 홈페이지, 보안 취약점, 홈페이지 변조 및 홈페이지 변조 건수는 모두 증가하고 있다(〈표 Ⅲ-36〉 참조).

52) 国家互联网应急中心(2014, 2015, 2016, 2017)

53) 이는 중국 국가사이버대응센터가 주요 사이버 보안 서비스 기업이 제출한 사이버 공격 건수를 바탕으로 집계한 수치임

54) 이는 중국 국가 사이버대응센터가 각 산업별 기업에서 입수한 사이버 사고 민원 건수를 바탕으로 집계한 수치임

〈표 Ⅲ-35〉 중국 사이버 공격 건수 변화 추이[1)]

(단위: 건수, %)

구분		2013	2014	2015	2016
컴퓨터 목마 바이러스	건수	189,369	104,230	105,056	96,670
	비중	18.4	8.4	5.6	4.0
모바일 악성 프로그램	건수	702,861	951,059	1,477,450	2,053,501
	비중	68.2	76.6	78.8	84.2
보안 취약점	건수	7,854	9,163	8,080	10,822
	비중	0.8	0.7	0.4	0.4
가짜 홈페이지	건수	30,199	99,409	184,574	177,988
	비중	2.9	8.0	9.8	7.3
홈페이지 해킹	건수	76,160	40,186	75,028	82,072
	비중	7.4	3.2	4.0	3.4
홈페이지 변조	건수	24,034	36,969	24,550	16,758
	비중	2.3	3.0	1.3	0.7
합계	건수	1,030,477	1,241,016	1,874,738	2,437,811
	비중	100.0	100.0	100.0	100.0

주: 1) 중국 국가사이버대응센터가 전체 사이버 공격 건수를 발표하지 않고 있으며 주요 사이버 공격 건수를 통해 사이버 공격 상황을 보여주고 있음

자료: 国家互联网应急中心(2014, 2015, 2016, 2017)

〈표 Ⅲ-36〉 중국 사이버 사고 민원 건수 변화 추이

(단위: 건수, %)

구분		2013	2014	2015	2016
가짜 홈페이지	건수	10,573	18,034	75,896	53,531
	비중	33.4	32.1	59.8	42.6
보안 취약점	건수	10,921	20,450	25,637	31,164
	비중	34.5	36.4	20.2	24.8
악성 프로그램	건수	3,229	56	3,681	15,205
	비중	10.2	0.1	2.9	12.1
홈페이지 변조	건수	4,558	9,157	12,438	11,812
	비중	14.4	16.3	9.8	9.4
홈페이지 해킹	건수	1,804	3,146	4,188	9,173
	비중	5.7	5.6	3.3	7.3
악성코드	건수	190	4,775	3,300	3,142
	비중	0.6	8.5	2.6	2.5
기타[1)]	건수	380	674	1,777	1,634
	비중	1.2	1.2	1.4	1.3
합계	건수	31,655	56,180	126,916	125,660
	비중	100.0	100.0	100.0	100.0

주: 1) 기타는 홈페이지 악성코드 유포, 디도스 공격, 불법 접근 등이 있음
자료: 国家互联网应急中心(2014, 2015, 2016, 2017)

3) 개인 및 기업의 침해 사고

중국인터넷협회[55]는 설문조사를 통해 개인 침해 사고 현황을 집계하고 있다. 2016년 개인 침해 사고로 인한 중국인의 경제적 손해 금액은 915억 위안으로 추산되었는데, 이는 2015년 805억 위안보다 13.7% 상승한 수준이다. 불법 스팸, 사이버 금융사기 및 개인정보 유출은 중국인의 경제적 손해가 발생한 주요 원인인 것으로 나타났다. 특히 37%의 응답자는 사이버 금융사기 및 이에 따른 금전적 손해를 입은 경험이 있으며, 84%의 응답자는 개인정보 유출 및 이에 따른 피해를 입은 경험이 있다.

민간기관인 텐센트연합보안연구소[56]가 발표한 『2015년 기업 정보보안 조사보고서』에는 중국 기업의 인터넷 이용률 및 사이버 사고율에 관한 통계가 있다. 2015년 기준

55) 中国互联网协会(2016)
56) 腾讯安全联合实验室(2015)

90%의 중국 기업은 인터넷을 이용해 영업활동을 하고 있다. 또한 45%의 중국 기업은 과거 3년간 사이버 사고를 경험한 적이 있다. 특히 정보통신 기업은 사이버 사고율이 가장 높은 것으로 나타나고 있다.(〈표 Ⅲ-37〉 참조)

〈표 Ⅲ-37〉 중국 기업의 인터넷 의존도 및 사이버 사고율

(단위: %)

구분	금융	정보통신	IT	제조	교통운송	무역	전문서비스
인터넷 의존도	97.2	95.2	94.5	69.4	87.0	90.0	88.5
사이버 사고율[1)]	31.4	64.3	48.5	47.5	52.4	60.0	34.6

주: 1) 사이버 사고율은 산업별 중국 기업의 과거 3년 간 사이버 사고 경험을 바탕으로 집계된 수치임
자료: 腾讯安全联合实验室(2015)

이러한 공식적인 통계 이외에도 주요 사이버 사고는 언론 기사 검색을 통해서도 수집이 가능한데, 〈표 Ⅲ-38〉에는 최근 주요 사이버 사고가 정리되어 있다.

〈표 Ⅲ-38〉 최근 중국의 주요 사이버 사고 현황

사고명	보도일시	사고내용
GFan 회원정보유출	2015년 1월	웹의 취약점으로 2천 3백만 건의 가입 회원 정보가 유출
중국 사회보험관리기구 정보유출	2015년 4월	웹의 취약점으로 충칭, 상하이, 산시, 선양, 귀이양, 하난 등 지역에서 5천만 건 이상의 사회보험정보가 유출
중국인수생명보험회사 보험증권 정보유출	2015년 5월	웹의 취약점으로 80만 건의 보험증권 정보가 유출
Damai 회원정보유출	2015년 8월	해킹으로 600만 건의 가입 회원 정보가 유출
NetEase 이메일 이용자 정보 유출	2015년 12월	웹 취약점으로 1억 명 이상 이메일 이용자의 고객 정보가 유출
JD.COM 회원정보유출	2016년 12월	자사 직원의 불법 유출로 50억 건 이상의 개인정보가 유출
Youku 회원정보유출	2017년 4월	해킹으로 1억 건 이상의 회원정보가 유출
SF Express 정보유출	2017년 6월	자사 직원의 불법 유출로 200만 건 이상의 택배 배송자 개인정보가 유출
Huazhu Hotels 회원정보유출	2018년 8월	해킹으로 5억 건 이상의 회원 정보가 유출

자료: 공개 언론 기사를 바탕으로 정리됨

나. 사이버보험 시장동향

1) 시장규모

중국의 사이버보험은 미국을 비롯한 선진국은 물론 우리나라보다 늦게 출시되었다. 현재 11개 손해보험회사(외국계 4개, 중국계 7개)는 기업성 사이버보험을 판매하고 있다. 일부 외국계 손해보험회사는 미국, 유럽 등 선진국에서 축적된 사이버보험 관련 사이버 사고 데이터 및 경영 노하우에 힘입어 기업성 사이버보험을 출시하고 있다. 2013년 11월 취리히보험회사(Zurich Insurance)는 프라이버시권 침해 및 업무중단 손실 등을 보장하는 사이버종합보험을 중국 시장에서 처음으로 선보였다. 그 이후 알리안츠보험회사(Allianz Insurance), 에이아이지보험회사(AIG Insurance) 및 처브보험회사(Chubb Insurance)가 사이버보험을 출시하였다. 중국계 손해보험회사는 기업성 사이버보험 시장에서 외국계 손해보험회사에 뒤지지 않기 위해 기업성 사이버보험을 잇따라 출시하였거나 출시 준비를 하고 있다. 2015년 7월 중국평안손해보험회사, 중국인민손해보험회사 및 보해손해보험회사는 중국 정부부속 연구기관인 중국정보통신연구원과 함께 클라우드 서비스 기업을 대상으로 기업성 사이버보험(이하, '커싱윈 사이버보험'이라 함)을 출시하였다. 2016년 1월 중안보험회사는 클라우드 서비스 기업인 알리윈과 함께 '커싱윈 사이버보험'과 유사한 기업성 사이버보험을 출시하였다. 2017년 1월 중국평안손해보험회사, 안신농업보험회사는 사이버 보안 서비스 기업의 사이버 보안 제품을 판매하는 플랫폼인 '씽안재시엔'과 함께 사이버 보안 서비스 기업을 대상으로 기업성 사이버보험을 출시하였다. 이 외에도 중국양광손해보험회사, 중국태평양손해보험회사는 각각 기업성 사이버보험을 판매하고 있다. 다만 기업의 사이버 위험에 대한 인식 부족 때문에 중국 기업성 사이버보험 시장규모가 미미한 것으로 추정된다.[57]

가계성 사이버보험은 기업성 사이버보험과 달리 중국계 손해보험회사의 주도하에 출시되고 있다. 2017년 10월 기준 총 28개 중국계 손해보험회사가 53개의 금융계좌도

57) 赛迪网(2017)

용배상보험을 판매하고 있다. 2014년 9월 중안보험회사는 온라인 간편결제 서비스 기업인 알리페이(Alipay)와 함께 알리페이의 이용자를 대상으로 금융계좌도용배상보험을 출시하였다. 그 이후부터 많은 중국계 손해보험회사들이 금융계좌도용배상보험을 판매하기 시작하였다. 2016년 4월 기준 알리페이의 이용자를 대상으로 판매된 금융계좌도용배상보험 건수는 1.2억 건을 기록하였다.[58] 금융계좌도용배상보험의 활성화는 중국의 온라인 간편결제 서비스가 급성장하면서 타인의 도용, 보이스피싱으로 발생한 자금손실이 크게 증가하였기 때문이다.[59] 다만 현재 가계성 사이버보험은 금융계좌도용배상보험에 국한되고 있으며 사이버 폭력 등과 같은 사이버위험에 따른 피해를 보장하는 상품은 아직 판매되지 않고 있다.

2) 보험상품

현재 중국 시장에서 판매 중인 기업성 사이버보험은 가입자 유형에 따라 크게 일반 기업성 사이버보험 및 특화 기업성 사이버보험으로 분류할 수 있다. 가입자 제한이 없는 일반 기업성 사이버보험의 판매자는 외국계 손해보험회사 4개사(취리히손해보험회사, 알리안츠손해보험회사, 에이아이지보험회사 및 처브보험회사) 및 중국계 손해보험회사 3개사(양광손해보험회사, 중국태평양손해보험회사 및 중안보험회사)가 있다. 특정 산업에 속한 기업을 대상으로 판매되고 있는 특화 기업성 사이버보험은 클라우드 서비스 기업을 대상으로 출시된 '커싱윈 사이버보험' 및 사이버 보안 서비스 기업을 대상으로 출시된 '씽안재시엔 사이버보험' 등이 있다. '커싱윈 사이버보험'의 판매자는 중국계 손해보험회사인 중국평안손해보험회사, 중국인민손해보험회사, 보해손해보험회사가 있으며, '씽안재시엔 사이버보험'의 판매자는 안신농엽보험회사, 중국평안손해보험회사가 있다.

58) 证券时报(2016)

59) 2017년 중국 전자상거래 시장규모는 24조 위안(약 3,984조 원)을 기록하였으나, 2016년 기준 한국 전자상거래 시장규모는 60조 원에 불과하였음. 2017년 7월 기준 중국 스마트폰 이용자 수는 6.55억 명으로 나타나고 있음. 2015년 기준 중국 보이스피싱 건수는 59.9만 건을 기록하였으며 이로 인한 경제적 손실은 200억 위안으로 나타났음

대표적인 일반 기업성 사이버보험 및 특화 기업성 사이버보험의 보장내용 및 부대서비스는 각각 다음과 같다. 에이아이지보험회사의 일반 기업성 사이버보험의 보장내용은 기본약관에는 영업중단 손실, 데이터 회복, 사이버 사고 조사, 언론 대응, 랜섬웨어 감염, 고객정보 유출 배상책임, 법적 대응, 특별약관에는 평판 회복, 고객정보 유출에 따른 통보, 법률 상담을 포함한다. 동 보험은 부대서비스를 제공하지 않는다. 중국양광손해보험회사의 일반 기업성 사이버보험은 사이버종합보험이다. 동 보험의 보장내용은 재산손실보험에는 데이터 회복, 사이버 사기 손실, 평판훼손, 영업중단 손실, 제3자 배상책임보험에는 고객 데이터 분실, 훼손, 유출 배상책임을 포함한다. 중국양광손해보험회사는 사이버 보안 서비스 기업과 제휴해 부대서비스로서 가입자에게 사이버위험 평가 서비스, 실시간 사이버위험 감시 및 보호 서비스, 사이버위험 긴급 처리 서비스를 제공하고 있다.

특화 기업성 사이버보험인 '커싱윈 사이버보험'의 보장내용은 기본약관에는 서비스 중단 손실, 고객정보 분실, 유출 배상책임, 특별약관에는 사이버 공격 손실을 포함한다. 또한 '커싱윈 사이버보험'은 가입자의 요구에 따라 상기 보장 내용에 국한하지 않고 맞춤형 보장내용을 제공할 수 있다. 특화 기업성 사이버보험인 '씽안재시엔 사이버보험'은 사이버 보안 서비스 기업의 사이버 보안 제품과 결합된 패키지 상품으로 판매되고 있다. 동 보험은 사이버 보안 서비스 기업의 사이버 사고 처리 비용을 보장하고 있다. 현재 중국의 기업성 사이버보험은 주로 오프라인 채널에서 판매되고 있다.

〈표 Ⅲ-39〉 중국의 기업성 사이버보험 비교

보험상품	일반 기업성 사이버보험	커싱윈 사이버보험	씽안재시엔 사이버보험
판매회사	에이아이지보험회사	중국평안손해보험회사, 중국인민손해보험회사, 보해손해보험회사	중국평안손해보험회사, 안신농업보험회사
판매채널	오프라인 채널	오프라인 채널	오프라인 채널
가입대상	가입대상 제한 없음	클라우드 서비스 기업	사이버 보안 서비스 기업
보장범위	·기본약관: 영업중단 손실, 데이터 회복, 사이버 사고 조사, 언론 대응, 랜섬웨어 감염, 고객정보 유출 배상책임, 법적 대응 ·특별약관: 평판 회복, 고객정보 유출에 따른 통보, 법률 상담	·기본약관: 서비스 중단 손실, 고객정보 분실, 유출 배상책임 ·특별약관: 사이버 공격 손실	고객의 사이버 사고 처리 비용
면책사항	인신 상해, 재산손실, 계약책임, 고용책임, 지재권, 인프라 시설 사고	보장 범위 외의 보험사고는 면책사항임	보장 범위 외의 보험사고는 면책사항임
비고	없음	가입자의 요구에 따라 맞춤형 보험상품 제공 가능	사이버 보안 서비스 기업의 사이버 보안 제품과 결합된 패키지 상품으로 판매

자료: 공개 자료를 바탕으로 정리됨

〈표 Ⅲ-40〉과 같이 현재 중국 시장에서 판매 중인 가계성 사이버보험은 금융계좌도용배상보험의 형태로 판매되고 있다. 금융계좌도용배상보험은 카드 분실, 타인의 도용, 개인의 계정과 비밀번호 유출, 보이스피싱 등의 원인으로 인한 금전적 손해를 보장하고 있다. 금융계좌도용배상보험은 3단계를 거쳐 발전해왔다. 1단계에서는 온라인 간편결제 서비스 계좌의 도용만을 보장했다. 2단계에서는 은행카드, 인터넷뱅킹 계좌의 도용까지 보장했다. 3단계의 금융계좌도용배상보험 보장대상은 보이스피싱으로 인한 금융계좌 도용까지 확대되었다.

〈표 Ⅲ-40〉 중국의 금융계좌도용배상보험 비교

보험상품	은행계좌도용배상보험	스마트폰뱅킹도용배상보험	보이스피싱배상보험
보험회사	중안보험회사	화태손해보험회사	태평손해보험회사
발전 단계	1단계	2단계	3단계
판매채널	회사 홈페이지 및 스마트폰 앱, 위챗[1]	알리페이[2]	알리페이
보장지역	중국 국내	중국 국내 및 해외	중국 국내 및 해외
은행카드	포함	포함	포함
온라인 간편결제 서비스 계좌	비포함	포함	포함
보장범위	카드 분실, 바이러스로 인한 계좌 도용, 강도의 협박에 따른 카드 도용으로 발생한 자금손실	스마트폰, 패블릿에 설치된 계인계좌에 타인의 도용이나 강도의 협박에 따른 계정과 비번 유출로 발생한 자금 손실	보이스피싱으로 발생한 자금손실
면책사항	중대한 과실, 동거인이나 가족의 도용, 보이스피싱으로 발생한 자금손실	중대한 과실, 타인에게 빌려준 동안 발생한 자금손실	중대한 과실, 백신 프로그램의 경고에도 불구하고 도용 위험이 높은 사이트에 등록한 경우
보험금액	플랜A: 1만 위안 플랜B: 5만 위안	플랜A: 2만 위안 플랜B: 5만 위안 플랜C: 10만 위안	1~5만 위안
보험료	플랜A: 5위안부터 플랜B: 20위안부터	플랜A: 6위안부터 플랜B: 15위안부터 플랜C: 30위안부터	9.9~69.6위안
보장기간	1년	1년	1년
비고	배상 횟수 제한이 없으나 최고 보험금액으로 제한됨	배상 횟수 제한이 없으나 최고 보험금액으로 제한됨	알리페이 신용등급이 양호한 고객만 가입 가능하고 신용점수에 따라 가입 가능한 보험금액이 다름

주: 1) 위챗은 스마트폰 메신저인 카카오와 달리 금융서비스 등 다양한 서비스를 제공하고 있음
2) 알리페이는 온라인 간편결제 서비스인 카카오페이와 달리 금융서비스 등 다양한 서비스를 제공하고 있음
자료: 공개 자료를 바탕으로 정리됨

중국 시장에서 판매 중인 금융계좌도용배상보험은 보험회사의 홈페이지, 보험회사의 스마트폰 앱, 스마트폰 메신저 앱인 위챗, 온라인 간편결제 서비스의 스마트폰 앱 등 온라인 채널에서 많이 판매되고 있다. 금융계좌도용배상보험은 보험금액이 상대적으로 높지만 보험료가 저렴한 편이다. 중국 보험회사들은 과도한 보험금 지출을 방지하기 위해 보험상품을 정액형 상품으로 설계하고 있으며 명확한 보장범위 및 면책사항을 공시하고 있다.

다. 사이버보험 시장활성화 전략

1) 정부차원

현재 사이버보험에 관한 법 및 규정은 없다. 법적 근거가 없기 때문에 사이버보험 개발에 있어서 중국 손해보험회사들은 어려움을 겪고 있으며, 사이버보험이 출시되었더라도 중국 기업 및 개인의 사이버보험 가입도 소극적인 것으로 나타났다. 최근 몇 년간 중국학자들은 기업성 사이버보험 활성화를 위해 선진국, 특히 미국 사례를 소개하면서 정부의 정책지원이 필요하다고 주장하고 있다.[60] 중국학자의 제안들은 사이버보험 개발 및 요율 산출의 법적 근거 마련을 위한 사이버보험에 관한 법 제정,[61] 사이버 사고 데이터 축적을 위한 사이버 사고 공개 및 사이버 보안 등급제도 도입,[62] 보험회사의 과도한 보험금 지출 완화를 위한 재보험제도 도입,[63] 도덕적 해이 및 역선택 문제 해소를 위한 보험회사와 사이버 보안 서비스 기업의 협력,[64] 사이버보험 관련 인재 육성[65] 등이 있다. 그러나 아직까지는 중국 정부나 부속기관의 사이버 침해 사고 대응 조치에 관한 논의가 사이버 보안 기술 혁신에 집중되어 있으며 사이버보험에 관한 논

60) 王新雷·王玥(2017)
61) 郭静·张昌福(2006)
62) 陈伟·吴刚·祁志敏(2016)
63) 汪丽(2016)
64) 王新雷(2011)
65) 高雷·吕文豪(2011)

의는 거의 없다. 다만 2016년 11월 중국 정부는 「사이버보안법」을 제정하였으며, 동 법은 개인정보 유출 기업이 주관기관 및 고객에게 고지하여야 한다고 규정하였다. 동 법의 제정으로 중국 기업의 사이버보험 수요가 증가할 것으로 예상한다.

2) 민간차원

일부 중국계 손해보험회사는 사이버보험 시장을 선점하기 위해 관련기업과 협력해 사이버보험을 적극적으로 출시하고 있다. 이는 보험회사의 협력 기업이 사이버보험 개발 및 요율 산출에 필요한 데이터를 제공할 수 있고 사이버보험 가입자에 필요한 사전 및 사후 부대서비스를 제공할 수 있기 때문이다. 또한 보험회사의 협력 기업들이 잠재적인 보험가입자를 많이 보유하고 있기 때문에 보험회사는 상대적으로 쉽게 사이버보험 가입자를 확보할 수 있다.

가) 기업성 사이버보험 시장

중안보험회사는 클라우드 서비스 기업인 알리윈과 함께 클라우드 사이버보험 및 데이터 사이버보험을 개발했다. 클라우드 사이버보험은 알리윈만을 위해 개발된 보험으로, 알리윈의 설비 장애로 인한 클라우드 서비스가 중단될 경우 알리윈의 클라우드 서비스를 이용하는 기업은 중안보험회사에서 보상을 받을 수 있다. 데이터 사이버보험은 알리윈뿐만 아니라 클라우드 서비스 기업인 덴센트윈 및 텐이윈의 클라우드 서비스를 이용하는 모든 기업이 가입할 수 있는 상품이다. 데이터 사이버보험은 기본약관에는 가입자의 데이터 복구 및 고객정보 유출에 따른 배상책임, 특별약관에는 보안 취약점에 따른 손실 및 디도스 공격에 따른 손실을 보장하고 있다. 또한 중안보험회사는 데이터 복구 서비스 기업인 궈신쟈닝(GXJN, Guo Xin Jia Ning)과 함께 가입자의 재산손실 및 제3자 배상책임을 보장하는 사이버종합보험을 판매하고 있다. 동 사이버종합보험은 데이터 사이버보험에는 데이터 복구 비용, 클라우드 사이버보험에는 데이터 북구 및 고객정보 유출에 따른 배상책임, 분쟁검정 사이버보험에는 인터넷 거래 분쟁에 대한 검정 비용을 보장하고 있다. 중안보험회사는 상기 사이버보험을 모두 온라인 채널

에서 판매하고 있으며, 가입자는 필요에 따라 전화로 상담을 받을 수 있다. 중안보험회사가 이용하는 온라인 채널은 자사 홈페이지 및 스마트폰 앱, 협력 기업인 알리윈 사이트 및 궈신쟈닝 사이트를 포함한다.

〈표 Ⅲ-41〉 중안보험회사의 기업성 사이버보험 비교

상품 명칭	협력 기업	보장내용	비고
클라우드 사이버보험	알리윈	알리윈의 설비 장애로 인한 클라우드 서비스 이용 기업의 영업중단 손실	알리윈이 보험료를 납입
데이터 사이버보험	알리윈	·기본약관: 클라우드 서비스 이용 기업의 데이터 복구 및 고객정보 유출에 따른 배상책임 ·특별약관: 보안 취약점에 따른 손실, 디도스 공격에 따른 손실	알리윈뿐만 아니라 덴센트윈, 덴이윈의 클라우드 서비스 이용자도 가입 가능
사이버종합보험	궈신쟈닝	데이터 사이버보험: 데이터 복구 비용 클라우드 사이버보험: 데이터 복구 및 고객정보 유출에 따른 배상책임 분쟁검정 사이버보험: 인터넷 거래 분쟁에 대한 검정 비용	맞춤형 데이터 북구 및 보험보장 패키지 제공 가능

자료: 중안보험회사, 알리윈 및 궈신쟈닝의 홈페이지

나) 가계성 사이버보험 시장

대다수 중국계 손해보험회사들은 온라인 간편결제 서비스 기업과 협력해 사업 위험이 상대적으로 낮은 금융계좌도용배상보험을 적극적으로 출시하고 있다. 중안보험회사는 온라인 간편결제 서비스 기업인 알리페이와 협력해 금융계좌도용배상보험을 판매하고 있다. 동 사이버보험은 알리페이의 스마트폰 앱에서 판매되고 있어서 잠재적인 보험 가입자의 접근 및 가입의 편의성이 높다. 가입자가 알리페이의 스마트폰 앱에서 보험안내 자료 열람 단계부터 보험료 납입 단계까지의 모든 보험 가입 절차를 처리할 수 있다. 보험 가입에 필요한 가입자의 개인정보는 알리페이에 등록되어 있는 개인 자료를 조회하고 자동으로 가져올 수 있다.

〈그림 Ⅲ-3〉 중안보험회사의 금융계좌도용배상보험 가입절차

주: 위 화면은 알리페이 스마트폰 앱에서 중안보험회사의 금융계좌도용배상보험을 가입할 때 나타나는 실제 화면으로 구성됨
자료: 알리페이 스마트폰 앱(2018. 8. 3 현재)

라. 요약 및 시사점

중국의 사이버보험은 미국을 비롯한 선진국은 물론 우리나라보다 늦게 출시되었다. 현재 11개 중국 손해보험회사(외국계 4개, 중국계 7계)가 기업성 사이버보험을 판매하고 있다. 다만 중국 기업의 사이버위험에 대한 인식 부족 때문에 중국의 기업성 사이버보험 시장규모가 미미한 것으로 추정된다. 가계성 사이버보험의 경우, 2017년 10월 기준 총 28개 중국 손해보험회사가 53개의 금융계좌도용배상보험을 판매하고 있다. 다만 현재 중국 시장에서 판매 중인 가계성 사이버보험은 금융계좌도용배상보험에 국한되어 있다.

중국의 기업성 사이버보험은 가입자 유형에 따라 크게 일반 기업성 사이버보험 및 특화 기업성 사이버보험으로 분류할 수 있다. 일반 기업성 사이버보험은 가입자 제한이 없으며 보장대상에는 영업중단 손실, 데이터 회복, 사이버 사고 조사, 언론 대응, 랜

섬웨어 감염, 고객정보 유출 배상책임, 법적 대응 등 다양한 내용을 포함하고 있다. 특화 기업성 사이버보험은 보험회사가 특정 산업에 속한 기업을 대상으로 출시된 사이버보험이다. 대표적인 특화 기업성 사이버보험은 클라우드 서비스 기업의 고객을 대상으로 출시된 '커싱윈 사이버보험' 및 사이버 보안 서비스 기업의 고객을 대상으로 판매된 '씽안재시엔 사이버보험' 등이 있다. 특화 기업성 사이버보험은 특정 보장대상에 국한 하지 않고 가입자 요구에 따라 맞춤형 보장내용을 제공할 수 있다.

한편, 가계성 사이버보험인 금융계좌도용배상보험은 온라인 간편결제 서비스의 계좌 도용부터 은행카드, 인터넷뱅킹 계좌의 도용, 보이스피싱으로 인한 금융계좌 도용까지 보장하고 있다.

중국의 경우 사이버보험에 관한 법 및 규정은 없다. 법적 근거가 없기 때문에 사이버보험 개발에 있어서 중국 손해보험회사들은 어려움을 겪고 있으며, 중국 기업 및 개인의 사이버보험 가입도 소극적인 것으로 나타났다. 다만 최근 몇 년간 중국학자들은 기업성 사이버보험 활성화를 위해 선진국 사례를 소개하면서 정부의 정책지원이 필요하다고 주장하고 있다. 한편, 2016년 11월 중국 정부는 「사이버보안법」을 제정하였으며, 동 법의 제정으로 중국 기업의 사이버보험 수요가 증가할 것으로 예상한다.

일부 중국계 손해보험회사는 사이버보험 시장을 선점하기 위해 관련기업과 협력해 사이버보험을 적극적으로 출시하고 있다. 이는 보험회사와 협력한 기업이 사이버보험 개발 및 요율 산출에 필요한 데이터를 제공할 수 있고 가입자에 필요한 사전 및 사후 부대서비스를 제공할 수 있기 때문이다. 또한 보험회사는 협력 기업들을 통해 사이버보험 가입자를 상대적으로 쉽게 확보할 수 있다. 중안보험회사는 클라우드 서비스 기업, 데이터 복구 서비스 기업과 협력해 기업 사이버보험을 개발하여 판매하고 있으며, 온라인 서비스 기업과 함께 금융계좌도용배상보험을 출시하고 있다.

5. 소결

본 장에서는 미국, 유럽, 일본, 중국 등 주요국의 사이버보험 현황 및 활성화 전략을 살펴보았다. 미국과 유럽의 경우 공급 측면과 관련해서는 주로 사이버 사고 데이터 집적 노력을, 그리고 수요 측면과 관련해서는 주로 사이버위험 관련 홍보 및 교육 등을 중심으로 정책이 추진되고 있었다. 아직 의무보험 도입이나 사이버보험 가입률 제고를 위한 적극적인 정부정책이 추진되고 있지는 않은 상황이다. 그러나 적극적인 정부개입과 관련한 논의가 일부 있었는데, 사이버보험에 가입하는 동시에 NIST의 보안 가이드라인을 준수하는 기업에 대해 법인세 세액공제 혜택을 부여하자는 미국의 Data Breach Insurance Act와 영국의 민관협력 Insurance Pool 논의가 그 예이다.

일본의 경우에도 사이버보험 가입을 유도하기 위한 인센티브 정책도입이 일부 검토되고 있으나, 보험 가입률 제고를 위한 의무보험이나 세제지원 등의 적극적인 정부개입은 아직 논의되고 있지 않다.

Ⅳ. 이슈 분석

1. 기업시장

가. 검토배경

제3장에서 주요국의 사이버보험 활성화 전략에 대해 살펴보았는데, 의무보험제도 도입 등 보험 가입률 제고를 위한 적극적인 정부정책을 시도하고 있는 사례는 아직 찾아보기 어려웠다. 미국의 경우 DBIA가 발의되고 영국의 경우 보험풀 논의가 있었던 정도이다.

따라서 국내에서 추진되고 있는 의무보험제도 도입 중심의 사이버보험 정책의 한계와 발전 방향에 대한 시사점을 사이버보험 관련 해외사례에서 찾기는 어려운 상황이다. 그래서 본고에서는 사이버위험과 유사한 특징을 보이는 자연재해위험(Natural Disaster Risk), 그 가운데에서도 특히, 홍수위험(Flood Risk) 사례를 참고하고자 한다. 홍수위험은 사이버위험과 마찬가지로 일어날 가능성은 낮으나 일어나면 큰 피해를 입게 되는 Low-Probability, High Impact (이하 'LPHI'이라 함)의 특성을 가지고 있다. 수요 측면의 경우 낮은 발생 가능성으로 인해 보험가입에 대한 유인이 적고, 공급 측면의 경우 재앙적 손실 가능성으로 인해 보험회사가 보험공급을 꺼리게 되는 경향이 있다.

주요국의 경우 홍수보험의 저조한 가입률을 제고하기 위해 여러 정책적 노력이 전개되었는데, 여기서는 미국과 영국사례를 소개하고자 한다. 미국의 경우에는 National Flood Insurance Program(이하 'NFIP'이라 함)을 중심으로, 그리고 영국의 경우에는 Flood Re가 도입되기까지의 과정을 역사적 접근법을 통해 고찰해봄으로써 시사점을 얻고자 한다.

나. 미국의 홍수보험 사례[66]

1) NFIP 도입 과정

1895년부터 1927년 사이에는 민영보험회사들이 홍수보험을 제공하였다. 그러나 1927년 미시시피강 지역의 홍수로 인해 큰 손실을 보게 되자 민영보험회사들은 홍수보험 판매를 중단하였다. 이후 홍수피해 복구비용은 정부의 자연재해기금을 통해 해결하게 되었다.

시간이 지나면서 정부의 부담이 증가하게 되자, 1952년 트루먼 대통령은 민관협력 형태의 홍수보험 프로그램을 제안하였다. 프로그램의 주요 내용은 1927년 이전처럼 민영보험회사가 홍수보험을 제공하되, 정부가 재보험을 통해 위험을 분담하는 것이었으나, 관련 법안이 의회를 통과하지 못했다.

1955년 아이젠하워 대통령은 개인, 주정부, 연방정부가 홍수위험을 분담하는 프로그램을 제안하였다. 관련 내용을 담은 법안[67]이 의회를 통과하였으나, 이후 의회에 제출한 실행방안의 현실성 부족으로 인해 중단되었다.

존슨 대통령은 보다 근본적인 개혁을 위해 홍수위험관리에 있어서 연방정부의 역할에 관한 광범위한 개혁안을 담은 보고서[68]를 1966년 의회에 제출하였다. 보고서에는 홍수위험에 대한 인식제고, 범람지역 개발 제한 등과 함께 민관협력 형태의 국가 홍수보험 프로그램에 대한 내용도 포함되어 있었다. 이 보고서의 내용을 토대로 1968년 National Flood Insurance Act(이하 'NFIA'이라 함)가 제정되었고, 국가 홍수보험 프로그램인 NFIP가 도입되었다.

2) NFIP 내용

NFIP는 다음과 같은 특징을 가지고 있었다. 첫째, 보험풀(Insurance Pool)을 형성하

66) National Research Council(2015)에서 인용함

67) Federal Flood Insurance Act of 1956

68) 보고서 제목은 "Unified National Program for Managing Flood Losses"

였다. 손해보험 허가를 받은 보험회사는 법안에서 규정한 일정조건만 충족하면 누구나 참여 가능하였다. 보험풀의 참여는 두 가지 형태로 가능하였다. 첫 번째는 자본참여(Capital Participation)이고, 두 번째는 판매대행만 하는 형태로 참여하는 것이다. 전자의 경우에는 보험풀의 운영 과정에서 발생한 이익이나 손실을 공유하게 되지만, 후자의 경우에는 판매 수수료만 받게 된다.

둘째, 정부가 대출기관 또는 재보험자로서의 기능을 수행했다. 홍수 피해 발생 시 보험금 지급을 위한 재원이 부족하게 되면 재무부(Treasury)가 보험풀에 대출을 해주었다. 대출금은 보험료수입이 지급보험금을 초과하는 해에 상환하도록 하였다.

셋째, 홍수보험 가입을 확대하기 위해 두 가지 요율체계를 사용하였다. 홍수보험 요율지도(Flood Insurance Rate Maps, 이하 'FIRMs'이라 함)가 만들어진 이후에 건립된 건축물 소유자의 경우에는 위험에 근거한 보험료(Risk-Based Premiums)가 부과된 반면, FIRMs 이전의 건축물의 경우에는 위험에 근거한 요율보다 낮은 수준의 보험료가 부과되었다. 위험에 근거한 요율을 적용할 경우의 보험료 수입과 실제 보험료 수입의 차는 매년 말 재무부의 보조금에 의해 보충되었다. 미국 정부가 보험풀에 재정적 지원을 하게 된 배경에는 시간이 지나면서 위험지역의 기존 건축물이 점차 감소함으로써 손실이 줄어들 것이라는 낙관적 기대가 있었기 때문이다.

그러나 2005년 허리케인 카트리나(Katrina), 2009년 허리케인 아이크(Ike), 2011년 허리케인 샌디(Sandy) 등 대규모 피해를 가져온 자연재해가 연속적으로 발생하게 되면서 NFIP의 부채는 빠르게 증가하였다. 2013년 부채액이 240억 달러로 증가하면서 NFIP의 개혁 필요성이 제기되었다.

3) NFIP 개혁

NFIP의 재정 건전성에 대한 우려로 인해 의회는 2012년 Biggert-Waters Flood Insurance Reform Act of 2012 (이하 'BW 2012'이라 함)를 통과시켰다. 법안의 목적은 요율체계를 단일화하여 모든 대상에 대해 위험 기반 보험료를 부과하는 것이었다. 기존 프로그램하에서는 홍수보험 요율지도가 만들어지기 이전의 건축물에 대해서는 위

험에 기반한 요율보다 낮은 수준의 보험료가 부과되는 기득권(Grandfathering) 조항이 있었는데, 이 조항을 5년에 걸쳐 폐지하도록 하였다.

BW 2012가 시행에 들어가면서, 여러 지역에서 불만이 제기되었다. 불만의 목소리는 대개 기득권 조항을 적용받는 가계들로부터 터져 나왔다. 기존 프로그램하에서는 일종의 보조금 지원을 통해 낮은 보험료를 납부하였으나, 새로운 프로그램하에서는 위험에 기반한 요율체계가 적용되면서 보험구입 자체가 가계의 재정적 부담이 될 정도로 보험료가 인상되었기 때문이다.

보험료 인상으로 인한 보험 가입률 저하의 우려가 제기되자, 의회는 2014년 Homeowner Flood Insurance Affordability Act of 2014(이하 'HFIAA 2014'이라 함)를 통과시켰다. 주요내용은 우선 BW 2012에서 폐지하기로 했던 기득권 조항을 부분적으로 부활시키는 것이었다. 소유주가 거주하고 있는 건축물의 경우에는 기득권 조항을 인정하였으나, 소유주가 거주하고 있지 않은 건축물이나 빈번하게 보험금이 지급된 경우에는 BW 2012의 개혁안대로 매년 25%씩 보험료를 인상하여 점차적으로 정부보조를 줄여나가도록 했다.

또한 NFIP의 재정 건전성 제고를 위해 모든 건축물 소유자에게 위험 기반 요율을 적용하기 이전까지 모든 홍수보험 가입자에게 추가적인 보험료(Premium Surcharges)를 부과할 수 있게 하였다. 이렇게 만들어진 재원은 기득권 조항을 적용받는 가구의 보험료 보조(Premium Subsidy)에 사용되었다.

4) 보험 가입률 제고 전략

NFIP는 재난기금을 보험으로 대체함으로써 자연재해로부터의 복구에 있어서 일반 국민의 세금 투입을 줄이려는 목적으로 만들어졌다. 보험을 통해 홍수위험을 관리할 경우 재난기금에 비해 상대적으로 보다 안정적인 홍수위험 관리가 가능하고, 위험 기반 보험료 부과를 통해 홍수 위험 지역 주민의 위험 인식을 제고할 수 있는 이점이 있다. 그러나 이러한 장점들이 실현되기 위해서는 보험가입의 확대가 필요하였고, 보험 가입률 제고를 위해 일부 건축물에 대해서는 보조금 지원을 통해 보험료를 인하시켜

주었다.

그럼에도 불구하고 홍수보험 가입률은 매우 저조하였다. 예를 들어, 1969년 허리케인 카밀(Camille)과 1972년 아그네스(Agnes)의 피해를 입은 지역 가운데 소수의 지자체만이 NFIP에 참여하고 있었다. 이를 계기로 의회는 1973년 Flood Disaster Protection Act를 통과시켰다. 법안의 주요 내용은 연방정부의 지원을 받거나 규제를 받는 대출기관으로부터 모기지(Mortgage)를 받거나 특별 홍수위험 지역(Special Flood Hazard Area)에 해당되는 경우에는 홍수보험 가입을 의무화하는 것이었다. 또한 지자체가 연방정부로부터 여러 지원을 받기 위해서는 NFIP에 반드시 참여해야 하였다. 그리고 보험 가입을 독려하기 위해 7년 동안 기존 건축물의 보험료를 인하시켜 주었다.

그러나 1993년 미주리와 미시시피 강의 대규모 홍수가 발생했을 때, 침수된 건물의 20% 이하만이 보험에 가입한 사실이 드러나자 1994년 보험가입 의무화를 보다 강화하는 National Flood Insurance Reform Act of 1994가 의회를 통과하였다. 대출기관은 에스크로(Escrow) 제도를 활용해서 모기지 대출 고객으로부터 보험료를 받아서 예탁할 수 있다. 만약 모기지 대출자가 홍수보험에 가입하지 않을 경우 대출기관이 대신 홍수보험에 가입해야 한다.

1994년 조건부 의무화 강화 이후에도 보험 가입률 제고 이슈는 지속적으로 제기되었다. 2012년과 2014년 NFIP 개혁 당시 위험 기반 요율의 도입과 함께 보험 가입률 제고 방안에 대한 연구도 병행하여 진행되었다. 당시 의회와 Federal Emergency Management Agency의 요구에 의해 National Research Council은 보고서를 발표하였는데, 보험 가입률 제고 방안으로 다음과 같은 것들이 포함되어 있다.

첫 번째 대안은 위험완화 수단에 투자할 경우 정책금융을 통해 장기 저리 대출을 해주는 것이다. 장기 저리 대출의 필요성을 간단한 사례를 통해 설명하면 다음과 같다. 가령 위험완화 수단에 투자하기 이전에 매년 400만 원의 보험료를 내는 가계가 있다고 하자. 그런데 2,500만 원을 들여 위험완화 수단을 구축하게 되면 보험료가 50만 원으로 감소한다고 하자. 이 경우 연이율 3%로 2,000만 원의 20년 장기대출을 받게 되면 매년 대출 상환금은 168만 원이 되고, 보험료 50만 원을 더하면 매년 지출되는 금액이 218만 원으로 투자 이전의 400만 원에 비해 182만 원의 이득을 보게 된다.

위험완화 수단에 투자할 경우 장기적으로는 이득을 보더라도 저소득층의 경우에는 초기 투자비용 조달이 어려울 수 있다. 이러한 경우 정책금융을 통해서 장기 저리의 대출을 해주게 되면 보험료 인하 효과를 통해 보험 가입률을 제고할 수 있다.

두 번째 대안은 위험 기반 요율 적용 시 보험료가 급격히 상승하게 되는 가구를 대상으로 바우처(Voucher)를[69] 발급해주는 것이다. 바우처는 보험료 납부나 위험완화 시설투자 대출금 상환에 사용할 수 있다.

세 번째 대안은 세제 지원이다. 2013년 Flood Mitigation Expense Relief Act가 도입되었는데, 법안의 내용은 다음과 같다. 개인 또는 근로자 수가 50인 이하의 소기업이 일정 조건을 충족할 경우 5,000 달러까지 세액공제(Tax Credit)를 받을 수 있도록 하였다. 일정 조건은 다음과 같다. 첫째, 홍수보험에 가입해있어야 한다. 둘째, 홍수 대비 시설 투자를 위한 지출이 있어야 한다. 셋째, 보험료가 인상된 경우로 제한한다. 2014년에는 수정법안이 제출되었는데, 세액공제 한도가 5,000달러에서 7,500달러로 상향 조정되었다. 세액공제 혜택은 2022년에 종료된다.[70]

마지막 네 번째 대안은 소득공제 혜택을 받을 수 있는 재해저축계좌(Disaster Savings Account)를 도입하는 것이다. 이 계좌에 넣어 둔 자금은 재해 피해 복구비용, 재해위험 완화시설 투자, 홍수보험 보험료 납부 등에 사용될 수 있다. 실제 2014년 Disaster Savings Account Act가 도입되었는데, 주택 소유자는 매년 5,000달러까지 납입할 수 있으며, 보험에 의해 보상받지 못하는 피해액이 3,000달러를 초과하는 경우 이 계좌의 자금을 피해 복구비용으로 사용할 수 있다. 이 대안이 보험 가입률 제고에 도움이 되는 것은 다음과 같은 이유 때문이다. 만약 재해저축계좌의 자금을 홍수보험의 자기부담금 이하의 비용 지출에 사용할 수 있게 되면, 자기부담금 수준을 높임으로써 보다 저렴한 가격에 보험을 구입할 수 있다.

위의 네 가지 방안의 특징은 직접적으로 보험료를 깎아 주는 것이 아니라 간접적으로 보험료를 낮추어주는 효과가 있다는 점이다.

---

69) 바우처란 특정 재화나 서비스의 획득에만 사용할 수 있도록 발급된 증서를 의미함. 예를 들어 푸드 스탬프(Food Stamp)는 식료품 구입에만 사용할 수 있음

70) 아직 법안이 의회를 통과하지는 못했음

다. 영국의 홍수보험 사례

1) Gentlemen's Agreement[71)]

영국에서는 1916년에 처음 홍수보험이 판매되기 시작해서 1922년 경에는 대부분의 회사가 판매하였다. 그러나 이 당시의 홍수보험은 가재(Contents)만 보장했으며 건물(Building)은 보장 대상에서 제외되었다. 한편, 보험회사들은 역선택(Adverse Selection)에 대한 우려로 인해 적극적으로 홍수보험을 판매하지 않았다.

1952년 8월 Lynmouth 홍수로 인해 큰 피해를 입었는데, 피해를 입은 가구 가운데 홍수위험을 보장하는 건물보험에 가입한 경우는 전무하였고, 가재보험도 일부만 가입하고 있었다. 당시 보험금 지급과 관련하여 보험회사와 보험계약자 간에 분쟁이 있었다. 원칙대로 하게 되면, 홍수는 보장 대상에서 제외되는 위험이기 때문에 보험금을 지급하지 않는 것이 맞으나, 여론에 밀려 보험금을 지급하였다.

1953년에는 East Coast 홍수가 발생하여 1952년 홍수보다 더 큰 피해를 입었다. 이번에는 피해규모가 너무 커서 보험회사들이 보험금 지급을 거절하였다. 상업적 생존가능성(Commercial Viability)을 고려하지 않은 채 계속해서 사회적 책임(Social Responsibility)만을 생각할 수는 없었기 때문이다.

보험회사가 보험금 지급을 거절하게 되면서, 처음으로 국가 홍수보험 프로그램의 필요성이 제기되었다. Woodburn의원은 제2차 세계대전 기간 동안 운영하였던 전쟁피해 보상제도(War Damage Arrangements)와 유사한 형태의 국가 홍수보험 프로그램을 만들 것을 정부에 요청하였다. 그러나 정부는 Woodburn의원의 제안에 반대의사를 표시했다. 국가 홍수보험 프로그램에 대한 영국 정부의 기본 입장은 다음 두 가지로 특징 지울 수 있다. 첫째, 홍수보험은 민영 보험시장이 담당할 영역이지 공적 영역은 아니라고 보았다. 그 이면에는 민영 보험시장의 축소를 두려워하여 국가 홍수보험 프로그램에 반대한 보험산업과의 충돌을 원하지 않았던 측면도 있었다. 둘째, 홍수방지 시설 등과 같은 인프라 구축은 공공 영역이 담당해야 할 사항이지만, 홍수보험은 개인이

71) 2000년 이전의 영국 홍수보험 역사는 Arnell et al.(1984)에서 인용함

책임져야하는 영역이라고 생각하였다. 이러한 영국 정부의 입장은 최근 민관 협력 홍수보험 프로그램인 Flood Re가 도입되기 이전까지 지속되었다.

1960년대 후반 잉글랜드 서남부와 웨일즈에서 홍수가 발생하여 큰 피해를 입게 되자 홍수보험제도 개선의 필요성이 다시 제기되었다. 하원의원인 Stewart의 주장에 의하면, 피해 가구의 90%, 상점의 50%가 홍수보험에 가입해있지 않았다. 홍수보험에 가입하지 않은 피해자들에 대한 비난도 있었지만 보험회사가 책임을 다하지 않았다는 비난도 있었다. 첫째, 홍수위험이 큰 지역의 경우에는 보험인수를 거절하였다. 둘째, 적극적으로 홍수보험을 판매하지 않아서 상당수 주택 소유자들이 홍수보험의 존재를 알지 못했다.

하원의 요구에 의해 정부는 국가재해기금(National Disaster Fund)을 만드는 것을 고려하였다. 기금의 실행 가능성 검토를 위해 보험협회와 접촉하는 과정에서 기금 도입 대신 보험산업이 보다 적극적으로 홍수보험을 판매하는 방향으로 정책이 선회하였다. 이때의 정부와 보험협회간 협정을 Gentlemen's Agreement라고 하는데, 2000년까지 지속되었다. 이번에도 장기적이고 구조적인 개혁보다는 단기적이고 이해집단 간 타협에 의한 임시방편적인 방안이 채택되었다. 협정의 주요내용을 보면, 우선 홍수위험을 보장하는 가재보험을 모든 영구 거주 건축물(Permanently Occupied Properties)을 대상으로 보장금액 100파운드 당 보험료 25펜스의 요율로 판매하기로 하였다. 단, 위험지역의 경우에는 100파운드 당 50펜스의 요율로 판매하였다. 또한 아주 위험한 지역이 아닌 경우에는 건물보험의 보장 대상에 홍수위험도 포함시키기로 했다. 그리고 상업이나 산업용 건축물을 대상으로 한 홍수보험도 판매하기로 하였다. 단, 위험지역은 제외할 수 있었다.

1961년의 Gentlemen's Agreement에 의해 홍수보험시장에 있어서 상당한 진전이 있었지만 이후 홍수 경험 과정에서 문제가 여전히 존재함이 드러났다. 1968년 홍수 피해 가구 가운데 상당수가 홍수보험에 가입해 있지 않았다. 예를 들어 Ashton Vale지역의 경우 단지 43%만이 홍수위험을 보장하는 가재 및 건물보험에 가입해 있었다. 낮은 위험인식, 높은 보험료 등이 저조한 가입의 원인으로 지적되었다. 홍수위험을 건물보험의 보장대상에 포함할 경우 보험료가 증가하였기 때문에, 보험가입이 의무가 아닌

선택 상황에서 상당수 가구가 보험료 절감을 위해 홍수위험을 보장 대상에서 제외하였다. 1968년의 홍수는 국가재해기금에 대한 논의를 다시 촉발시켰으나 이번에도 보험산업 차원에서 홍수보험에 대한 홍보를 강화하는 정도에서 마무리되었다.

2) Statement of Principles[72)]

1961년에 체결된 Gentlemen's Agreement 체제에 변화가 일어난 것은 2000년 들어와서이다. 변화의 동인은 2000년 홍수 피해였는데, 당시 보험산업에 대한 여론은 비교적 우호적이었던 반면, 정부에 대해서는 홍수위험 경고, 홍수방지시설 미비, 잘못된 국토계획 등을 이유로 비판이 쏟아졌다. 이로 인해 정부와 보험산업 간 협상력에 변화가 생겼다. 보험산업의 협상력이 증가하면서 홍수보험의 적극적 판매에 대한 대가로 홍수방지시설 투자확대 등 홍수위험을 감소시키기 위한 정부의 명시적인 노력을 요구하였다. 이러한 내용을 담은 협정이 2002년 체결되었는데, 이 협정의 명칭은 Statement of Principles on the Provision of Flood Insurance(이하 'SoP'이라 함)였다. SoP체제는 2016년 Flood Re가 도입되기 이전까지 지속되었다.

새로운 협정하에서 보험산업은 일정 기준의 위험수준을 정하고, 그 기준보다 위험수준이 낮은 지역에 한해 홍수보험 판매를 보장하였다. 이때의 기준위험은 75년에 한 번 꼴로 홍수가 발생하는 것이었다.

협정의 효력은 3년이었기 때문에 2005년 정부와 보험산업은 재협상에 들어갔으며 2006년 갱신되었다. 보험산업의 의무는 이전과 큰 변화가 없었으나 정부에 대한 요구사항은 보다 강화되었다. 홍수방지시설투자, 국토계획, 위험인식 제고를 위한 홍보 노력을 매년 점검토록 하였다.

2008년 정부와 보험산업은 협정의 재검토에 들어갔으며, 보험산업은 이전의 협정조건을 대부분 수용하였다. 그러나 2002년에 체결된 SoP의 큰 틀을 유지하면서 갱신하는 것은 이번이 마지막이라는 점을 분명히 했다.

72) 2000년 이후 영국 홍수보험 역사는 Penning-Rowsell et al.(2014)에서 인용함

3) Flood Re[73)]

정부와 보험산업은 SoP의 효력이 완전히 만료되는 2013년 이후의 홍수보험 시스템 마련을 위해 2010년 Flood Summit을 만들었다. 이 모임에서는 임시방편이 아닌 보다 근본적이고 영구적인 홍수보험 해결책에 대해 논의하였으며, 2013년 6월 마침내 합의에 이르렀다. 합의 내용은 일단 Memorandum of Understanding on Flood Re의 형태로 작성되었으며, 이후 2014 Water Act의 파트 4에 추가됨으로써 법제화되었다. 그리고 1년의 시험 운영 후에 2016년부터 본격적으로 시행에 들어갔다.

Flood Re는 일종의 재보험 기구(Reinsurance Vehicle)이고, 목적은 약 2%에 해당되는 고위험 건축물을 대상으로 홍수보험을 공급하는 데 있다. 운영은 다음과 같은 방식으로 이루어진다. 가계에 홍수보험을 판매하는 단계에서는 Flood Re가 개입하지는 않는다. 가계에 홍수보험을 판매하는 것은 민영보험회사가 담당한다.

민영보험회사는 가계로부터 홍수보험을 인수한 다음 해당 물건을 자신이 보유할지 아니면 Flood Re로 넘길지를 결정한다. Flood Re로 넘길 경우 재보험료는 위험을 완전히 반영한 요율이 적용되는 것이 아니라 그보다는 좀 낮은 수준의 고정 요율이 적용된다. 이렇게 하는 이유는 고위험 가구의 경우 위험을 완전히 반영한 요율을 적용하게 되면 보험료가 너무 비싸져서 사실상 홍수보험 가입이 어려워질 수 있기 때문이다.

고위험 가구를 대상으로 보험료를 보조하기 위해서는 추가적인 재원이 필요한데, 이 때 필요한 재원은 홍수보험을 판매하는 민영보험회사가 부담한다. 계약 건당 10.5 파운드의 부과금(Levy)을 Flood Re에 납부하도록 하였다. 그리고 만약 큰 홍수피해가 발생하여 재보험료와 부과금을 통해 마련된 재원이 소진되어 보험금 지급이 어려울 경우에는 사후적으로 보험회사들이 추가적인 재원을 Flood Re에 조달하도록 되어 있다.

Flood Re는 영구적인 조치는 아니고, 25년 동안 한시적으로 운영되는 임시 기구이다. 25년 내에 현재 상태에서 시장 메커니즘에 의해 보험료가 결정될 수 있는 상태로 이행하는 것을 목표로 하고 있다.

Flood Re가 고위험 가구의 홍수보험 구입가능성 제고 측면에서는 긍정적이나 다음

73) Flood Re 관련 내용은 Mantegazza(2017)에서 인용함

과 같은 점들은 문제점으로 지적되고 있다. 첫째, 보험료를 직접 깎아줌으로 인해 고위험 가구의 왜곡된 홍수위험 인식을 야기할 수 있다. 둘째, 홍수위험관리에 있어서 가장 중요한 것은 위험을 감소시킬 수 있는 조치인데 Flood Re의 경우에는 이와 관련된 인센티브 제도들이 결여되어 있다. 이러한 이유에서 25년 후 완전한 시장 메커니즘으로의 이행에 대해 의문을 제기하는 학자들이 있다.

라. 소결

미국과 영국의 홍수보험 사례로부터 다음과 같은 시사점을 얻을 수 있다. 첫째, 최근 정보통신망법의 개정 내용을 보면 손해배상 수단으로 보험, 공제, 준비금의 세 가지 가운데 선택할 수 있도록 하였다. 단기적으로는 세 가지 수단을 모두 허용하더라도 장기적으로는 보험을 선택하도록 유도하는 것이 적절하지 않나 여겨진다. 왜냐하면 피해구제 기능만 놓고 보면 준비금도 하나의 수단이 될 수 있으나, 위험 전달 기능까지 함께 고려할 경우에는 보험이 준비금에 비해 우월한 수단이 되기 때문이다.

둘째, 사이버위험관리의 근본적인 대책은 사이버위험 자체를 감소시키는 것이다. 사이버위험을 줄이지 않고서는 홍수보험 사례에서 보았듯이 보험제도의 존속이 어렵다. 따라서 의무보험 도입만으로는 사이버보험시장의 건전한 발전이 불가능하며, 보완정책의 도입이 필요하다. 미국의 경우 세제지원의 조건으로 사이버보험 가입과 함께 NIST의 사이버보안 가이드라인 준수도 요구하였는데, 그 이유는 정책의 목적이 단순히 피해구제에만 있었던 것이 아니라 사이버위험 완화에도 있었기 때문이다. 사이버보험은 피해구제와 위험전달 기능을 수행하고, NIST 사이버보안 가이드라인 준수는 위험 완화 기능을 수행한다. 우리나라의 경우에도 의무보험 도입과 함께 사이버위험을 완화할 수 있는 정책을 병행할 필요가 있다. 정책대안으로는 세제지원, 사이버 사고 방지 시설 투자 시 정책금융을 통한 장기 저리 대출, 바우처 제도 등을 생각해볼 수 있다.

2. 가계시장

가. 검토배경

개인의 사이버위험에 대한 주관적 인식과 사이버보험에 대한 수요는 낮을 것이라는 생각이 일반적인 통념이다. 그러나 아직 이를 실증적으로 보여준 국내 선행연구는 거의 없는 것 같다. 설문조사를 통한 아주 초보적인 형태의 조사조차도 없다.

본고에서는 2,440명을 대상으로 사이버위험 인식 및 사이버보험 수요를 조사한 연구결과를 소개하고자 한다.[74] 본 연구에서 소개하는 사이버 사고 유형은 세 가지다. 첫째는 사이버 금융범죄, 둘째는 사이버 폭력, 셋째는 웨어러블 디바이스 사용 시 정보유출이다.

나. 사이버위험 인식 및 사이버보험 수요

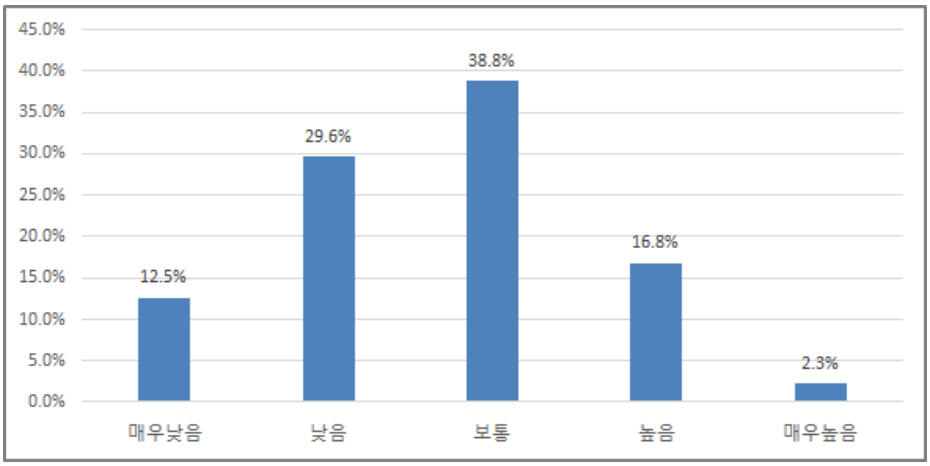
1) 사이버 금융범죄

사이버 금융범죄란 전화나 인터넷 등의 정보통신망을 이용하여 소비자에게 금전적 손해를 끼치는 범죄행위를 의미한다. 예를 들어, 대표적인 사이버 금융범죄 가운데 하나인 보이스피싱의 경우 범죄자가 소비자를 속여서 계좌번호, 비밀번호, 보안카드 등 개인의 금융정보를 알아낸 후, 소비자의 계좌에서 돈을 빼낸다. 만약 사이버 금융범죄 관련 보험상품에 가입한 경우 사고가 발생하면 보험금을 받게 된다.

조사대상 2440명 가운데 사이버 금융범죄에 의해 금전적 손실의 피해를 경험한 응답자는 총 25명이었다. 향후 피해자가 될 가능성과 관련해서는 그림에서 보듯이 가능성이 높다고 평가한 응답자보다는 낮다고 평가한 응답자의 비중이 상대적으로 컸다.

74) 동향분석실(2018)에서 인용함

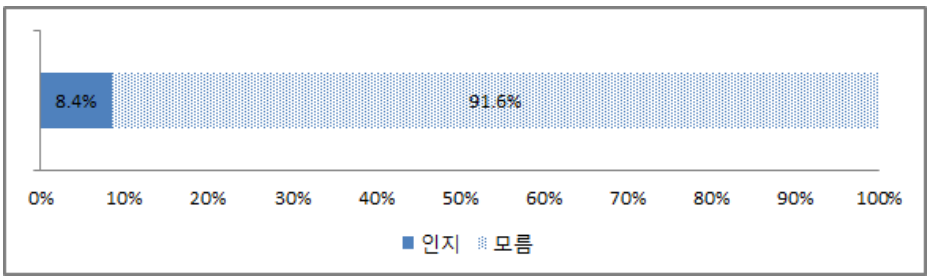
〈그림 Ⅳ-1〉 사이버 금융범죄 피해 가능성에 대한 주관적 인식



주: 전체 샘플 수는 2,440명임
자료: 동향분석실(2018)

조사 대상 가운데 11명만이 현재 사이버 금융범죄 관련 보험상품에 가입하고 있었다. 현재 가입하고 있지 않은 사람들을 대상으로 사이버 금융범죄 관련 보험상품 판매 사실의 인지 여부에 대해 조사하였는데, 단지 8.4%만이 인지하고 있었다.

〈그림 Ⅳ-2〉 사이버 금융범죄 관련 보험상품 판매 사실의 인지 여부



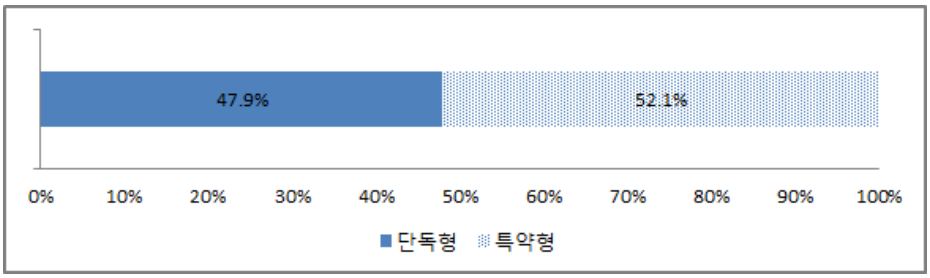
주: 현재 사이버 금융범죄 관련 보험상품에 가입하지 않은 2,429명을 대상으로 조사함
자료: 동향분석실(2018)

현재 사이버 금융범죄 관련 보험상품의 판매사실에 대해 모르고 있는 2,224명을 대상으로 보험가입 의향을 조사한 결과 211명이 가입 의향이 있다고 응답하였다.

가입 의향이 있는 211명을 대상으로 사이버 금융범죄에 따른 피해만을 보장하는 단

독형 보험상품과 화재 등 다양한 위험을 보장하는 종합형 보험에 사이버 금융범죄로 인한 금전적 손해 보장을 특약으로 추가하는 방식 가운데 어떤 형태로 구입하기 원하는지 조사하였는데, 거의 비슷한 비중을 차지하였다. 이러한 결과에 대해 두 가지 방식에 대한 선호도가 비슷하다고 해석하기보다는 단독형에 대한 수요가 약 50% 존재한다고 해석하는 것이 더 적절하지 않나 여겨진다.

〈그림 Ⅳ-3〉 사이버 금융범죄 관련 보험상품 희망 구입형태



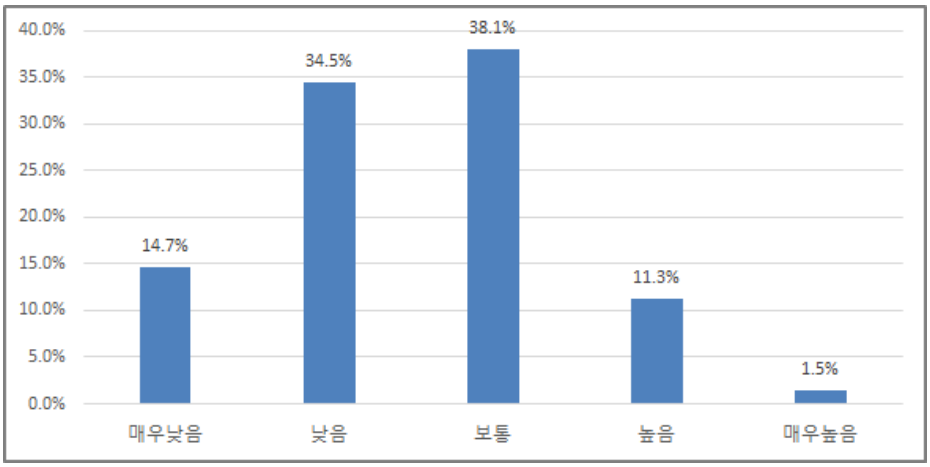
주: 사이버 금융범죄 관련 보험상품 구입 의향이 있는 211명을 대상으로 조사함
자료: 동향분석실(2018)

2) 사이버 폭력

사이버 폭력이란 인터넷 공간에서 특정인에게 글, 이미지, 음성 등으로 적대적인 표현 및 태도를 반복적으로 행하여 피해자에게 정신적 고통이나 재산적 손해를 끼치는 범죄행위를 의미한다. 예를 들어 대표적인 사이버 폭력인 사이버 명예훼손의 경우, 인터넷 공간에서 허위의 글이나 명예를 훼손하는 글을 유포하여 피해자로 하여금 정신적 고통을 입게 한다. 사이버 폭력 관련 보험상품에 가입하게 되면 경찰에 의해 범죄사실이 확인될 경우 보험회사로부터 보험금을 받을 수 있다.

조사대상 2,440명 가운데 사이버 폭력에 의해 피해를 경험한 응답자는 총 31명이었다. 향후 피해자가 될 가능성과 관련해서는 그림에서 보듯이 가능성이 높다고 평가한 응답자보다는 낮다고 평가한 응답자의 비중이 상대적으로 컸다.

〈그림 Ⅳ-4〉 사이버 폭력 피해 가능성에 대한 주관적 인식

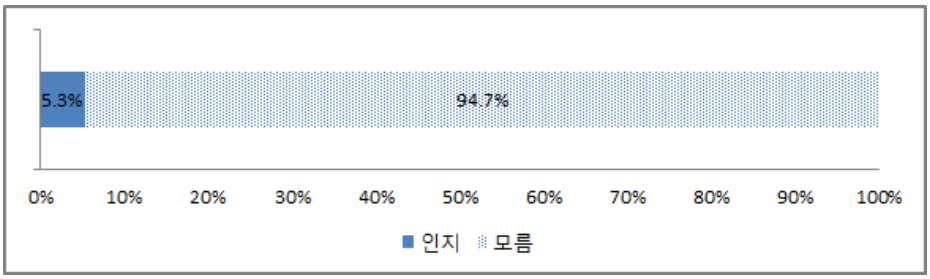


주: 전체 샘플 수는 2,440명임
자료: 동향분석실(2018)

조사 대상 가운데 5명만이 현재 사이버 폭력 관련 보험상품에 가입하고 있었다. 현재 가입하고 있지 않은 사람들을 대상으로 사이버 폭력 관련 보험상품 판매사실의 인지 여부에 대해 조사하였는데, 단지 5.3%만이 인지하고 있었다.

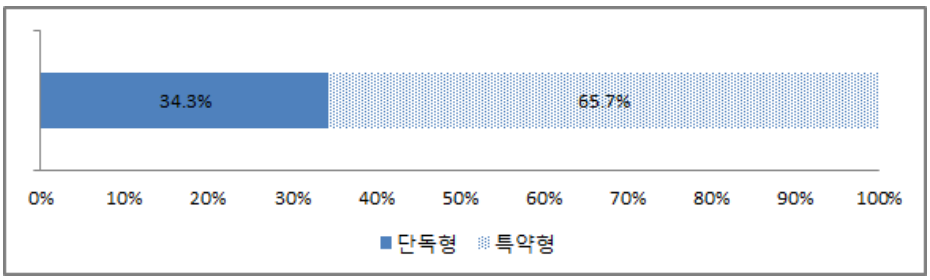
현재 사이버 폭력 관련 보험상품의 판매사실에 대해 모르고 있는 2,307명을 대상으로 보험가입 의향을 조사한 결과 99명이 가입 의향이 있다고 응답하였다. 가입 의향이 있는 99명을 대상으로 사이버 폭력에 따른 피해만을 보장하는 단독형 보험상품과 화재 등 다양한 위험을 보장하는 종합형 보험에 사이버 폭력으로 인한 피해 보장을 특약으로 추가하는 방식 가운데 어떤 형태로 구입하기를 원하는지 조사하였는데, 단독형에 대한 수요가 약 34.3% 존재하였다.

〈그림 Ⅳ-5〉 사이버 폭력 관련 보험상품 판매 사실의 인지 여부



주: 현재 사이버 폭력 관련 보험상품에 가입하지 않은 2,435명을 대상으로 조사함
자료: 동향분석실(2018)

〈그림 Ⅳ-6〉 사이버 폭력 관련 보험상품 희망 구입형태



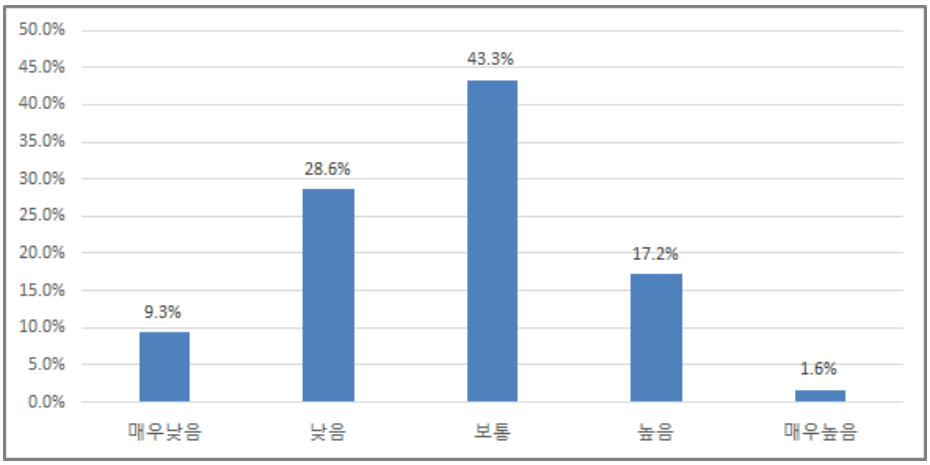
주: 사이버 폭력 관련 보험상품 구입 의향이 있는 99명을 대상으로 조사함
자료: 동향분석실(2018)

3) 웨어러블 디바이스

웨어러블 디바이스는 옷이나 신발, 액세서리의 형태로 몸에 부착하여 이용할 수 있는 전자기기를 의미하는데, 이 기기에 개인의 건강정보를 저장할 수 있다. 예를 들어, 손목시계 형태의 웨어러블 디바이스를 손목에 차고 있으면, 평상시 나의 혈압이나 기타 건강 관련 정보가 웨어러블 디바이스에 저장된다. 단, 이러한 웨어러블 디바이스 사용 시 우려 사항 가운데 하나는 개인의 건강정보 등이 해킹에 의해 유출될 수 있다는 점이다.

2,440명을 대상으로 조사한 결과, 향후 웨어러블 디바이스 사용 시 자신의 건강정보가 유출될 가능성이 높다고 평가한 응답자보다는 낮다고 평가한 응답자의 비중이 상대적으로 컸다.

〈그림 Ⅳ-7〉 웨어러블 디바이스 사용 중 건강정보 유출 가능성에 대한 주관적 인식



주: 전체 샘플 수는 2,440명임
자료: 동향분석실(2018)

다. 소결

사이버 금융범죄, 사이버 폭력, 웨어러블 디바이스의 세 가지 유형에 대해 위험인식 및 보험수요에 대해 조사했는데, 비슷한 패턴의 결과를 얻었다.

첫째, 피해 가능성에 대한 주관적 인식과 관련해서는 가능성이 높다고 응답한 경우보다 낮다고 응답한 비중이 상대적으로 컸다.

둘째, 조사대상자 가운데 보험상품 가입자 비중은 매우 낮았으며, 미가입자 가운데 관련 보험상품의 판매사실을 인지하고 있는 응답자의 비중도 낮았다.

셋째, 사이버위험 관련 보험상품의 판매사실을 모르고 있던 가입자에게 구입의향을 물어본 결과 일부 응답자의 경우 보험가입 의사를 밝혀 잠재적인 수요가 존재함을 확인할 수 있었다.

넷째, 보험상품 구입 형태의 경우 단독형과 특약형 가운데 선택하도록 하였는데, 단독형에 대한 수요가 적지 않게 존재하였다.

3. 공공부문

가. 검토배경

최근 정보통신망법이 개정되어 손해배상책임 관련 의무화 조항이 도입되었다. 일정 규모 이상의 정보통신서비스 제공자는 손해배상책임의 이행을 위하여 보험 또는 공제에 가입하거나 준비금을 적립하는 등의 조치를 취해야 한다.

정보통신망법 개정안이 국회를 통과하면서 의무화 조항 도입의 다음 대상인 개인정보보호법으로 자연스럽게 관심이 옮겨가고 있다. 그러나 개인정보보호법은 정보보호 분야의 일반법으로서 신용정보법이나 정보통신망법과 비교할 때, 적용대상의 범위가 훨씬 넓어 피해구제 수단의 의무화 조항 도입이 쉽지 않은 측면이 있다. 이러한 이유에서 선행연구 등에서는[75] 순차적인 도입을 제안하였으며, 우선적인 대상 가운데 하나가 공공기관이었다.[76]

이러한 배경하에 본고에서는 공공기관 관련 사이버보험을 별도의 이슈 가운데 하나로 다루고자 한다. 기존 선행연구 등에서는 공공기관도 다른 경제주체들과 유사한 관점에서 접근하여 대안을 제시하고 있는데, 본고에서는 조금 다른 시각에서 접근하여 시사점을 도출하고자 한다.

나. 공공데이터 개방과 정보보호 규제체계[77]

최근 들어 데이터의 중요성이 부각되면서, 새로이 관심을 가지게 된 분야가 공공데이터이다. 공공부문에 엄청난 규모의 데이터가 집적되어 있으나, 혁신적인 활용에 있어서는 한계가 있다는 지적과 함께 공공데이터를 민간에 개방하자는 공공데이터 개방

75) 이기형 외(2010)

76) 이기형 외(2010)는 공공기관의 의무화를 3단계로 나누어 1단계에서는 중앙행정기관, 2단계에서는 광역자치단체 및 기초자치단체, 3단계에서는 교육기관을 대상으로 의무화를 도입하는 방안을 제시하였음

77) 임준(2016, 2017)에서 인용함

(Open Government Data) 운동이 미국을 시작으로 전 세계적으로 전개되고 있다.[78]

미국의 경우 버락 오바마(Barak Obama) 대통령이 2009년 취임하면서 정부 데이터의 공개를 명령하였고, 그 결과 data.gov라고 하는 웹사이트가 만들어졌다. 시작 당시 약 47개였던 데이터 집합(Data Set)이 2012년에는 172개 기관의 약 45만 개로 증가하였다. 미국에 이어 영국, 유럽대륙, 호주, 브라질, 칠레, 케냐 등에서도 공공데이터 개방 운동이 전개되었다. 특히, 영국의 경우에는 월드와이드웹의 창시자인 팀 버너스리(Tim Berners-Lee)가 Open Data Institute를 설립하는 등 활발한 운동이 진행되고 있다.

우리나라의 경우에도 '정부3.0'이라는 타이틀 아래 공공기관이 보유하고 있는 데이터를 민간에 개방·공유하는 공공데이터 개방 운동이 펼쳐졌다. 2013년 6월 정부3.0 비전 선포와 정부3.0 기본계획 발표가 있었고, 2014년 7월 민·관 위원회인 정부3.0 추진위원회가 출범하였다. 이후 민·관 합동 테스크포스를 구성하여 개방이 시급한 국가 중점 데이터 36개 분야를[79] 선정하였는데, 여기에는 국토교통부의 건축정보, 국민건강보험공단의 국민건강정보, 건강보험심사평가원의 국민의료정보 등이 해당된다.[80]

국민건강보험공단의 국민건강정보 데이터를 예로 들어 세부 내용을 살펴보면, 전 국민의 약 2%에 해당되는 약 100만 명의 진료내역정보, 약품처방내역정보, 건강검진정보 등을 포함하고 있다. 진료내역정보에는 진료과목코드, 주상병코드, 요양일수 등이 포함되고, 약품처방내역정보에는 약품일반성분명코드, 1회 투약량 등이 포함되며, 건강검진정보에는 신장, 체중 등이 포함되는데 총 항목 수는 62개이다. 홈페이지의 홍

78) Mayer-Schönberger and Cukier(2013)

79) 36대 국가중점데이터에는 건축정보(국토교통부), 국민건강정보(국민건강보험공단), 상권정보(소상공인시장진흥공단), 수산정보(해양수산부), 실시간수도정보(한국수자원공사), 농수축산경락 및 조사가격정보(농림축산식품부), 등산로 및 국가생물종 정보(산림청), 부동산종합정보(국토교통부), 통합재정정보(기획재정부), 지방행정정보(행정안전부), 법령정보(법제처), 부동산거래관리정보(국토교통부), 지방재정정보(행정안전부), 식의약품종합정보(식품의약안전처), 도로명주소정보(행정안전부), 산업재산권정보(특허청), 노동보험정보(근로복지공단), 국가통계종합정보(통계청), 재난관리정보(국민안전처), 교육행정정보(교육부), 음식물쓰레기정보(한국환경공단), 국가공간정보(국토교통부), 해양공간정보(해양수산부), 기상정보(기상청), 국가종합전자조달정보(조달청), 수출입무역통계(관세청), 국민의료정보(건강보험심사평가원), 국민연금정보(국민연금공단), 고용보험정보(한국고용정보원), 도시계획정보(국토교통부), 사회보장정보(사회보장정보원), 산업기술정보(한국산업기술진흥원), 교통사고정보(사이버경찰청), 지진대피소정보(행정안전부), 생태자연도(환경부) 등이 해당됨

80) 현재 공공데이터 포털(www.data.go.kr)에 집적되어 있음

보 내용으로는 제약회사의 경우 국민건강정보를 활용하여 영업활동 전략을 수립할 수 있으며, 보험회사는 보험상품 개발을 위한 연구용 데이터로 활용할 수 있다고 되어 있다.

그러나 현재 공공데이터 개방 수준하에서는 큰 혁신 효과를 얻기에는 다소 한계가 존재한다. 좀 더 큰 혁신 효과를 얻기 위해서는 마이크로 데이터[81]의 적극적인 개방이 필요하다. 현재는 공공데이터 포털을 통해 주로 가공 데이터가 제공되고 있으며, 마이크로 데이터의 개방에 있어서는 소극적인 편이다. 특히, 건강 관련 정보 등 사람과 관계된 정보의 경우 개방에 있어서 더욱 소극적이다. 예를 들어, 보험회사의 경우 보험상품 개발을 위해서는 의료나 건강 관련 마이크로 데이터가 필요한데, 보험회사가 상업용 목적으로 활용하기 쉽지 않은 상황이다.

현재의 정보보호 규제체계하에서는 적극적인 데이터의 개방과 혁신적인 활용에 한계가 있다는 인식하에서 규제 패러다임의 전환이 필요하다는 주장이 제기되고 있다.[82] 그동안 대부분의 국가에 있어서 프라이버시 법(Privacy Laws)의 핵심적 원칙은 정보주체인 개인들에게 통제권을 주는 것이었다. 즉, 자신의 개인정보를 제공할 것인지, 제공한다면 누구에 의해 어떻게 사용되도록 할 것인지에 대한 결정권을 개인에게 주는 것인데, 이러한 원칙이 실제적인 제도로 구현된 형태는 '통지와 동의(Notice and Consent)' 방식이었다. 개인정보를 수집하는 주체는 정보주체인 개인에게 정보수집의 목적을 명확하게 알리고, 동의를 받아야 하며, 수집 목적 이외의 용도로 사용해서는 안 된다.

그러나 최근 들어 '빅데이터'로 대변되는 데이터 환경의 급격한 변화와 함께 전통적인 정보보호 접근법인 '통지와 동의' 방식의 적절성에 대한 이슈가 제기되고 있다.[83] 데이터라는 자원은 다른 자원과 달리 1차적 목적보다는 부차적 목적에서의 활용을 통해 더 많은 부가가치를 창출할 수 있으나, 기존 동의 방식하에서는 이러한 잠재적 가치를 충분히 실현하기 어렵다. 현행 개인정보보호 관련 법을 준수하기 위해서는 수입 이외의 목적으로 사용할 경우 일일이 개인의 동의를 받아야 하는데, 이는 현실적으로 용

81) 마이크로 데이터(Miro Data)란 통계조사 원자료(Raw Data)에서 입력오류, 조사오류, 논리오류 등을 제거하여 작성한 기초 데이터를 의미함

82) Center for Information Policy Leadership(2016)

83) Mayer-Schönberger and Cukier(2013)

이하지 않다. 부차적인 목적으로 데이터를 사용할 때, 개인의 동의를 일일이 받는 번거로움을 사전에 방지하기 위해 수집 당시 미래의 잠재적인 활용 목적에 대해 한꺼번에 동의를 받는 것도 현실적으로 불가능하다. 미래에 어떤 목적으로 활용될 지 수집 당시에 알 수 없기 때문이다.

이러한 배경하에 기존의 정보보호 접근 방식이 아닌 새로운 접근 방식에 대한 필요성이 제기되었고, 그러한 논의 가운데 하나가 사용자의 책임을 강화하고 정보보호에 위험관리(Risk Management) 기법을 도입하자는 것이다.[84] 위험관리 기법을 도입한다는 것의 의미는 데이터의 활용의 혜택(Benefits)과 피해(Harms)를 비교 분석하여 혜택이 피해보다 클 경우 데이터 활용을 허용한다는 것이다. 기존의 방식이 암묵적인 규제 목표를 위험 제로(Zero)에 두었다면, 위험관리 기법에 기반을 둔 규제의 경우에는 위험을 완전히 제거하는 것을 규제의 목적으로 하지 않고, 어느 정도의 위험은 수용하게 된다.

위험관리에 기반을 둔 규제체계의 경우 일정 수준의 위험은 수용하기 때문에 피해보상 체계의 확립과 이를 위한 리스크 재무(Risk Financing)가 매우 중요하게 된다.

다. 리스크 재무

리스크 재무란 발생한 손실의 재무적 결과를 최소화하고 손실을 복구하는 것을 의미한다.[85] 리스크 재무는 크게 리스크 보유(Risk Retention)와 리스크 전가(Risk Transfer)이며, 리스크 보유에는 기금적립, 자가보험(Captive Insurance), 공제 등이 해당되며, 리스크 전가의 경우에는 보험이 대표적인 예이다.

본고에서는 정부의 역할이 단순한 정보 집적자를 넘어 적극적인 정보 제공자로 전환할 경우 적절한 리스크 재무 방식에 대해 살펴보고자 한다. 적극적인 정보 제공자로서의 역할을 수행하게 되면 상대적으로 위험도 커지기 때문에 민간 보험회사에서 위험을 부담하기는 다소 버거울 수 있다. 따라서 공공부문에서 적극적으로 위험을 부담

84) Center for Information Policy Leadership(2016)
85) 이경룡(2008)

할 필요가 있다고 생각한다. 이하에서는 두 가지 대안에 대해 소개하고자 한다. 하나는 자가보험이고, 다른 하나는 정부지원 재보험풀(Government-Backed Reinsurance Pool)이다.

1) 자가보험

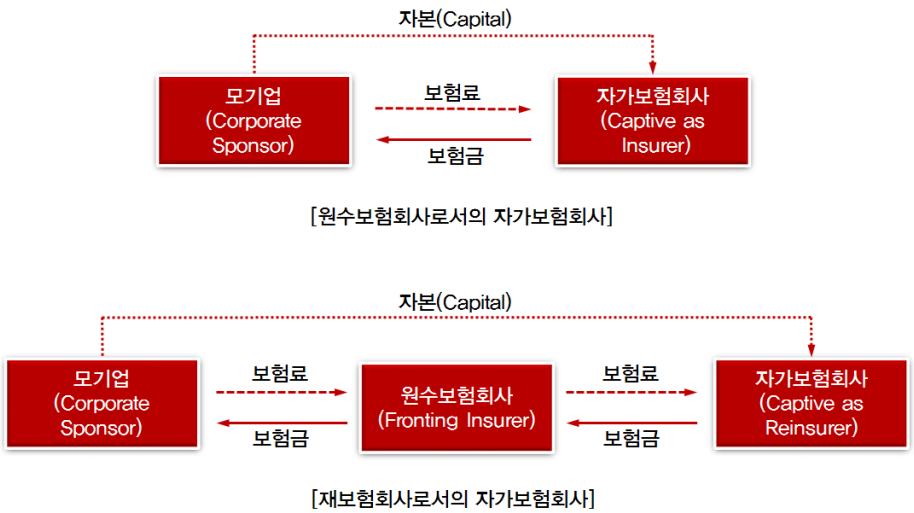
가) 자가보험의 유형[86]

자가보험회사의 형태가 계속적으로 발전하고 있어서 정의하기가 쉽지 않으나 일반적으로는 모회사의 위험을 인수하는 것이 주목적인 보험회사로 정의할 수 있다.[87] 자가보험회사의 증가와 감소는 일반 보험시장의 상황과 밀접한 관련을 가지고 있다. 미국의 경우 1970년대 보험회사들이 위험 인수에 소극적인 태도를 보이자 자가보험이 급속도로 확산되었다. 그러나 1980년대 들어 보험회사들이 위험인수에 있어서 적극성을 보이자 자가보험은 감소하였다. 그러다가 1990년 전사적 위험관리(Enterprise-Wide Risk Management)가 유행하면서 자가보험이 다시 인기를 얻게 되었다.

자가보험회사는 원수보험회사 형태로 설립할 수도 있고, 재보험회사 형태로 설립할 수도 있다. 재보험회사 형태로 설립할 경우에는 원수보험회사 형태로 설립할 경우에 비해 규제측면에서 덜 제약을 받을 수 있는 장점이 있다. 반면, 원수보험회사를 통해서 모기업의 위험을 인수하기 때문에 원수보험회사에 지급하는 수수료 비용이 발생하는 단점이 있다.

86) Banks(2004)에서 인용함
87) Ike(2016)

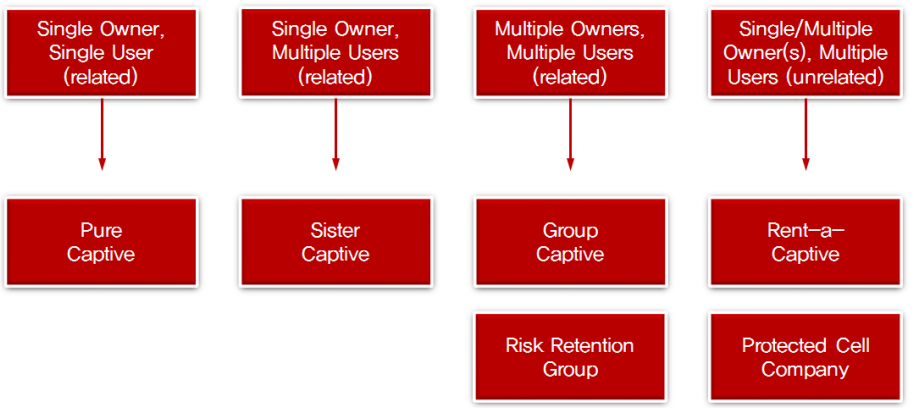
〈그림 Ⅳ-8〉 자가보험회사 형태: 원수보험회사 vs. 재보험회사



자료: Banks(2004)

자가보험은 소유기업 수와 이용기업 수에 따라 4가지 유형으로 구분된다. 첫 번째 유형은 소유기업도 하나이고 이용기업도 하나인 단순 자가보험(Pure Captive)이다.

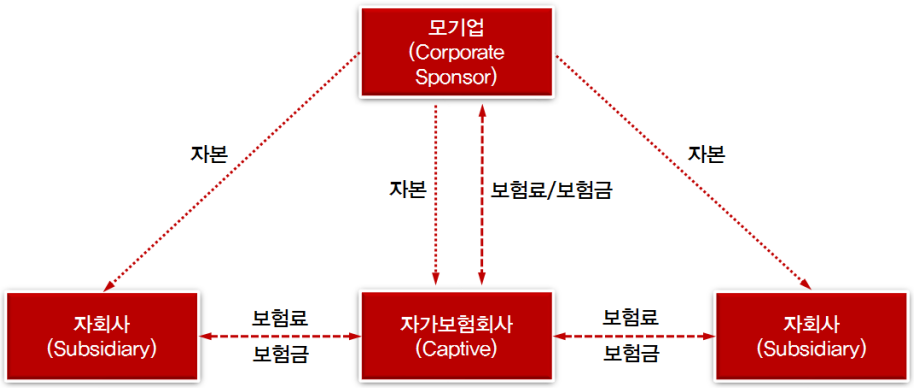
〈그림 Ⅳ-9〉 자가보험회사의 소유기업과 이용기업 수에 의한 자가보험의 유형 구분



자료: Banks(2004)

두 번째 유형은 자매 자가보험(Sister Captive)이다. 소유기업은 단순 자가보험과 마찬가지로 하나지만, 이용기업은 여러 개인 경우이다. 대규모 기업집단의 모기업이 자가보험회사를 설립하고, 자가보험회사가 모기업뿐만 아니라 모기업과 계열관계에 있는 자회사의 위험도 함께 인수하는 경우가 해당된다.

〈그림 Ⅳ-10〉 자매 자가보험(Sister Captive)



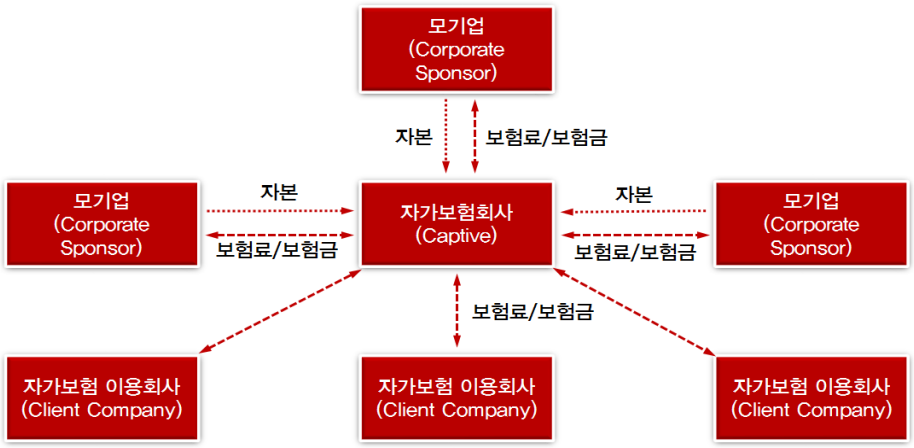
자료: Banks(2004)

세 번째 유형은 소유기업도 여러 개이고, 이용기업도 여러 개인 경우이다. 여기에 해당되는 사례는 그룹 자가보험(Group Captive)이다. 이 경우 소유 관계에 있는 기업뿐만 아니라 소유 관계에 있지 않는 기업들도 자가보험을 이용할 수 있다. 상호보험회사(Mutual Insurance Company)도 이 유형에 속하는 하나의 예로 볼 수 있다. 그룹 자가보험은 동질적인 위험을 가진 집단이 위험 풀(Insurance Pool)의 이점을 위해 형성하게 되는데, 에너지 자가보험, 항공 자가보험, 의료과실 자가보험 등이 산업별 그룹 자가보험의 예이다.

그룹 자가보험의 특수한 형태의 하나로 위험 보유 그룹(Risk Retention Groups)이 있다. 기본 구조는 그룹 자가보험과 동일하다. 그러나 담보가 배상책임으로 국한되어 있다. 1980년대 중반 미국에서 배상책임보험 위기(Liability Insurance Crisis)가 발생하자 보험회사들이 보험료를 인상하고 보상범위 등을 줄이거나 인수를 거절하게 되면서, 지자체, 항공, 의료 등의 분야에서는 보험 가입이 어려워지게 되었다. 이후 Risk

Retention Act of 1986의 제정을 통해 특별 배상책임 상호보험회사(Special Liability Mutual Insurance Company)의 설립을 허용하였다.

〈그림 Ⅳ-11〉 그룹 자가보험(Group Captive)



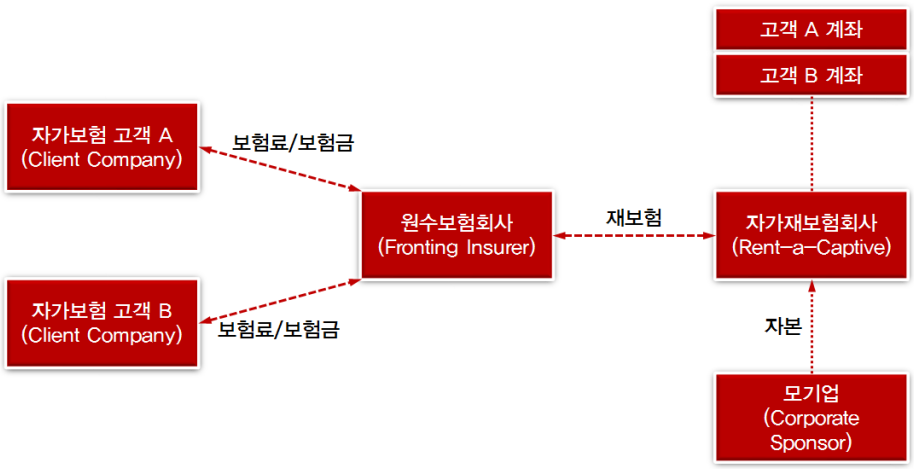
자료: Banks(2004)

네 번째 유형은 최근에 등장한 유형으로 '임대(For Hire)' 자가보험이다. 이 유형에는 Rent-a-Captive(이하 'RAC'이라 함)와 Protected Cell Company(이하 'PCC'이라 함)가 있다. 임대 자가보험은 위험을 보유하고 관리하는 프로그램을 자체적으로 이용하고 싶으나 새로운 기관을 설립하고 운영하는 번거로움을 원하지 않을 경우 유용한 방법이다.

RAC의 경우 세 번째 유형인 그룹 자가보험과 비슷한 구조를 가지고 있지만, 이용기업들과 자가재보험회사 간에 소유 관계가 존재하지는 않는다. 자가재보험회사는 이용기업과 관계가 없는 제3자가 소유하고 있다. 자가재보험회사는 대개 재보험회사나 브로커에 의해 관리되는 것이 일반적이다.

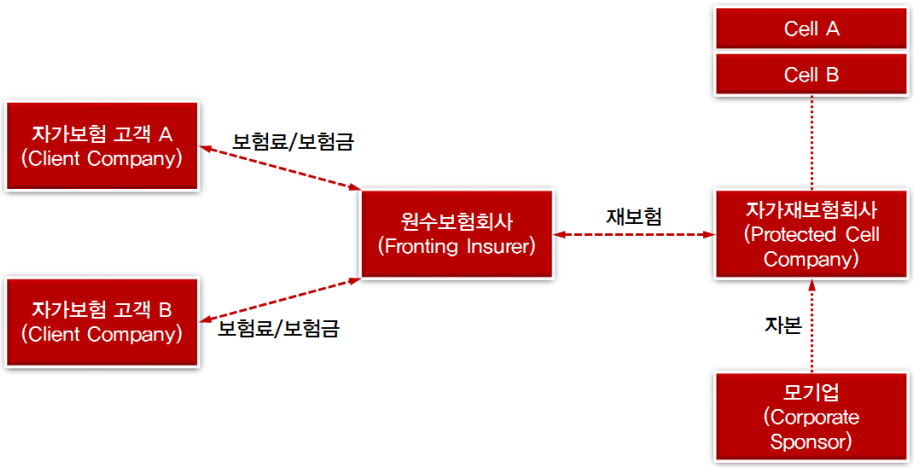
임대 자가보험의 두 번째 유형은 PCC인데, 한 가지를 제외하고는 RAC와 구조가 동일하다. RAC의 경우에는 이용기업들의 준비금 계좌가 분리되어 있지 않다. 그래서 한 이용기업이 큰 사고를 당했을 경우 보험금 지급을 위해 다른 이용기업의 계좌에 적립되어 있는 준비금을 사용할 수 있다. 반면, PCC의 경우에는 이용기업들의 준비금 계좌가 법에 의해 분리되어 있어서 교차해서 사용할 수 없다.

〈그림 Ⅳ-12〉 Rent-a-Captive



자료: Banks(2004)

〈그림 Ⅳ-13〉 Protected Cell Company



자료: Banks(2004)

위의 유형들 가운데 국내 공공기관의 사이버위험 보유를 위한 자가보험의 유형으로는 그룹 자가보험이 적절할 것으로 보인다. 공공기관들이 자가보험회사를 설립하고 보험풀을 만들어 위험관리를 하는 것이다. 예를 들어 36대 국가중점 데이터의 소관부처

들이 자가 보험회사를 만들어 운영하는 것이다. 공공기관의 자가보험 관리를 민간 재보험회사에 맡기는 방안도 생각해볼 수 있다.

나) 호주사례

호주 주정부들은 공공기관의 리스크 재무 방식으로 자가보험을 선택하였다. 여기서는 Queensland 주정부 사례를 소개하고자 한다.[88] Queensland 주정부는 2001년 자가보험 프로그램으로 Queensland Government Insurance Fund(이하 'QGIF'이라 함)를 설립하였다. 모든 주정부 부처(Departments)는 의무적으로 QGIF에 보험 가입을 해야 한다. 법정기구(Statutory Bodies)의 경우에는 QGIF에 참여할 수도 있고, 민간 보험시장에서 보험을 구입할 수도 있다. QGIF에서 담보하는 위험들에는 재물(Property), 일반 배상책임(General Liability), 전문직 배상책임(Professional Liability), 상해 및 질병(Accident and Illness), 항공(Aviation), 해상(Marine) 등이 있다.

2011년 일련의 자연재해를 겪게 되면서, 도로 등을 포함한 공공자산(Public Assets)의 리스크 재무와 관련하여 비용 측면에서 보다 효과적인 수단을 갖추도록 하는 Natural Disaster Relief and Recovery Arrangements(NDRRA) 가이드라인을 발표하였다.

한편, 최근 주요 위험 가운데 하나로 부상한 사이버위험의 경우에는 재물 및 일반배상책임 보험의 담보 가운데 하나로 포함시켜 보장하고 있다. 주요 보장내용에는 조사비용, 위기관리 및 언론 대응 비용, 자산복구, 업무중단, 소송비용, 제3자 손해배상 등이 포함된다.

호주사례의 경우 사이버위험만을 위해 자가보험회사를 설립한 것은 아니기 때문에 국내 공공기관의 사이버위험에 대한 리스크 재무 방식으로서 자가 보험회사의 도입 논거 사례로서는 적절하다고 볼 수 없다. 그 보다는 국내 도입이 결정되고 나서 조직이나 운영과 관련된 논의를 할 때 하나의 참고사례로 활용할 수 있다는 점에서 소개하였다.

88) https://www.qgif.qld.gov.au에서 인용함

2) 정부지원 재보험풀: 영국의 Pool Re 사례[89)]

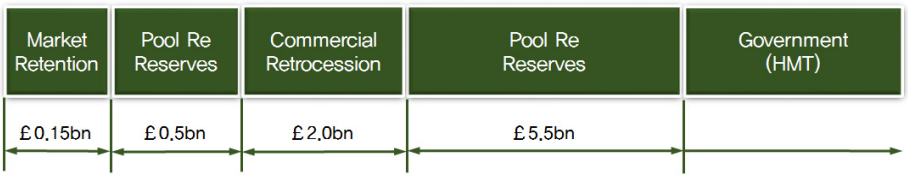
공공기관 사이버위험 관련 리스크 재무 방식의 대안 가운데 하나로 정부지원 재보험풀을 생각해볼 수 있는데, 여기서는 영국의 Pool Re 사례를 통해 그 구조에 대한 힌트를 얻고자 한다.

가) 개요

영국의 Pool Re는 1992년 IRA의 발트해운거래소(Baltic Exchange) 폭탄 테러 이후 보험산업과 정부가 협력하여 1993년 설립하였다. Pool Re는 영국의 손해보험회사와 로이즈가 출자해서 만든 상호회사 형태의 재보험회사(Mutual Reinsurer)이다.

2016년 6월 현재 Pool Re의 구조는 다음과 같다. 피해액의 규모가 1.5억 파운드까지는 Pool Re에 참여한 보험회사들이 부담한다. 1.5억 파운드에서부터 6.5억 파운드까지의 구간에 해당하는 5억 파운드에 대해서는 Pool Re에서 부담하고, 6.5억 파운드를 초과하는 피해액 가운데 추가적으로 20억 파운드까지는 스위스리 등과 같은 민간 재보험회사에 출재한 재재보험을 통해 해결한다. 그리고 민간 재보험회사가 담당하는 구간을 초과하여 피해가 발생한 경우 현재 Pool Re가 보유한 준비금으로는 추가적으로 55억 파운드까지 보상이 가능하다. 그 이상의 피해에 대해서는 정부가 지원하게 된다.

〈그림 Ⅳ-14〉 Pool Re 구조



주: 2016년 6월 현재
자료: Pool Re 홈페이지

89) 위키피디아와 Pool Re 홈페이지에서 인용함

나) 탄생배경

Pool Re는 1990년대 초 런던과 잉글랜드 여타 지역에서 발생한 일련의 테러 사건 이후 설립되었다. 당시 원수보험회사와 재보험회사들은 엄청난 규모의 잠재적 피해 가능성과 미래 손실에 대한 신뢰할만한 추정 방법의 부재로 인해 테러위험 보장의 중단을 고려하였다. 그러나 보험회사들이 테러위험 보험 판매를 중단할 경우 영국 경제에 미치는 영향이 매우 클 것으로 예상했기 때문에 새로운 테러위험 보험체계의 고안이 절실했다. 민간 보험회사들에게 전적으로 의존하는 전통적인 체계로는 한계가 있다고 보고 민관 협력모델인 Pool Re를 도입하게 되었다.

다) 변천과정

Pool Re는 2001년 9/11 사건 이후에 중요한 변화가 있었다. 그 이전까지는 화재나 폭발(Fire or Explosion)에 의한 피해만 Pool Re에서 보상하였고, 다른 유형의 테러에 대해서는 글로벌 재보험시장을 통해 해결하였다. 그러나 9/11 사건 이후 글로벌 재보험회사들이 테러위험에 대해 매우 보수적인 입장을 취하게 되면서, 기업들이 화재나 폭발 이외의 테러 유형에 대한 보장을 받기가 매우 어려워졌다.

이러한 상황을 타개하기 위해 보험산업, 보험수요자인 기업, 정부, Pool Re가 모여 논의를 시작하였고, 그 결과 2002년 7월 Pool Re의 담보 범위를 확대하기로 하였다. 이전에는 보장대상에서 제외되었던 화학(Chemical), 미생물(Biological), 방사능(Radiological), 핵(Nuclear) 관련 테러 공격도 보장대상으로 포함시켰다.

2017년 11월 15일에는 사이버 테러(Cyber Terrorism)도 Pool Re의 보장 대상에 포함되었다.

라. 소결

공공부문의 경우 사이버 사고가 발생할 경우 어떤 형태로든 결국 공적자금이 들어가게 되어 있다. 문제는 피해복구 및 손해배상을 위한 재원을 사전적으로 준비할 것인

지 아니면 사후적으로 조달할 지의 차이가 있을 뿐이다. 통상적으로 사후적인(Ex Post) 재원조달보다는 사전적인(Ex Ante) 리스크 재무 방식이 더 효율적이라고 알려져 있다.

공공부문의 사전 리스크 재무 방식(Ex Ante Risk Financing)은 공적 개입의 정도에 따라 크게 세 가지를 생각해볼 수 있다. 첫째, 공적 개입의 정도가 가장 약한 형태로 의무보험제도를 도입하고, 민간 보험회사들이 감당할 수 있는 정도의 최소한만 보험을 통해 보장하는 것이다. 그리고 그 이상은 사후적으로 공적자금을 투입해 해결하는 방식이다.

두 번째는 영국의 Pool Re 사례에서처럼 민관이 협력하는 방식이다. 민영보험회사들이 재보험풀(Reinsurance Pool)을 만들어, 1차적으로는 민영보험회사들이 부담하고, 그 다음은 재보험풀에서 담당하고, 그것도 초과하는 경우에는 정부에서 담당하는 형태이다.

세 번째는 공적개입의 정도가 가장 강한 형태로 공공부문의 사이버위험을 공공부문이 자가보험회사를 설립하여 전적으로 인수하는 방식이다. 그룹 자가보험회사가 하나의 형태가 될 수 있다.

위의 세 가지 방식 가운데 어떤 방식을 선택하느냐는 공공데이터와 관련된 정부의 역할에 따라 달라질 수 있다. 단순히 공공데이터의 집적자 역할만 한다면, 첫 번째 방식도 가능하리라 여겨진다. 그러나 공공데이터 집적자로서의 역할을 넘어 적극적인 공공데이터 제공자로서의 역할을 수행하기 위해서는 공공부문에서 좀 더 적극적으로 사이버위험을 인수할 필요가 있다고 여겨진다. 그럴 경우 두 번째나 세 번째 방식이 대안이 될 수 있지 않나 여겨진다.

현재 공공정보와 관련해서는 비식별 조치 등 활용과 관련된 정책이 주로 추진되고 있는데, 이러한 정책과 병행하여 위에서 언급한 리스크재무 전략도 함께 추진한다면 보다 효율적인 공공정보 활용이 가능하다고 생각한다.

V. 결론

본고에서는 국내 사이버보험 정책 수립과 관련하여 두 가지 측면에서 관점의 전환이 필요함을 주장하고자 한다. 첫째, 국내에서는 사이버보험 정책이 주로 피해구제의 관점에만 치중되어 있는 것 같다. 사이버보험만 분리해서 보면 그러한 관점이 타당할 수 있을지 모르나 사이버위험관리라고 하는 큰 틀 내에서 사이버보험을 접근하면 다른 시사점을 얻을 수 있다.

사이버위험관리의 궁극적 목적은 단순히 사후적인 피해구제에 있는 것이 아니라 사전적으로 사이버위험 자체를 감소시키는 데 있다. 사이버위험을 감소시키기 위해서는 기업이나 개인이 보안을 강화하도록 유도하는 것이 필요하다. 그와 관련하여 중요한 역할을 할 수 있는 것 가운데 하나가 바로 사이버보험이다. 보험의 경우 보험료 수준을 통해 경제주체에게 그들이 보유하고 있는 위험의 수준을 전달할 수 있다. 즉, 보험은 피해구제 기능뿐만 아니라 위험전달 기능도 가지고 있는 것이다. 이러한 측면에서 볼 때, 보험은 준비금에 비해 더 우월한 리스크 재무 수단이라고 볼 수 있다. 따라서 단기적으로는 손해배상 수단으로 보험, 공제, 준비금 가운데 선택할 수 있도록 하되, 장기적으로는 보험으로 단일화하는 것이 적절할 것으로 보인다.

사이버보험이 피해구제 기능과 위험완화 기능을 수행하는 데 있어서 매우 효율적인 도구이지만 사이버위험이 가진 LPHI(Low Probability and High Impact)의 특성 때문에 개인이나 기업의 위험인식은 낮고, 보험회사는 공급을 꺼리거나 공급하더라도 높은 보험료를 요구하고 있다. 따라서 사이버보험의 수요를 진작하기 위해서는 보험료 부담을 간접적으로 덜어줄 수 있는 세제지원, 정책금융, 바우처 제도 등이 병행하여 시행될 필요가 있다.

둘째, 현재 공공정보와 관련해서는 비식별 조치 등 활용과 관련된 정책이 주로 추진

되고 있는데, 이러한 정책과 병행하여 리스크 재무 전략도 함께 추진한다면 보다 효율적인 공공정보 활용이 가능하다고 생각된다. 리스크 재무 방식의 선택은 정부의 역할을 어떻게 자리매김하느냐에 따라 달라질 수 있다고 보는데, 단순히 공공데이터 집적자로서의 역할에 한정하게 되면 개인이나 기업 차원에 적용하던 논리를 연장하는 수준에 지나지 않겠지만, 만약 국내경제의 혁신 제고를 위해 정부가 적극적인 공공데이터 공급자로서 기능하게 될 경우에는 공공부문에서 좀 더 적극적으로 사이버위험을 인수하는 형태의 리스크 재무 방식의 도입이 필요하다고 여겨진다.

본고에서는 두 가지 대안을 생각해보았는데, 첫째는 공공부문에서 자가 보험회사를 설립하여 전적으로 공공부문의 사이버위험을 인수하는 것이다. 자가 보험회사 형태 가운데는 그룹 자가보험 형태가 우선적인 고려 대상이 될 수 있다. 둘째는 민관 협력모델로 일정부분은 민간이 담당하고, 초과하는 부분에 대해서는 정부가 담당하는 형태이다. 영국의 Pool Re가 하나의 벤치마킹 사례가 될 수 있다.

마지막으로 본 연구의 한계 및 향후 연구에 대해 언급하고 마무리하고자 한다. 첫째, 본고에서는 사이버보험 수요를 진작할 수 있는 인센티브 제도로 세제지원, 바우처, 대출 프로그램, 저축계정 등을 후보 대안으로 제시하였으나 국내 도입과 관련해서는 보다 심도있는 논의가 이루어질 필요가 있다.

둘째, 공공부문의 리스크 재무 수단의 하나로 자가 보험회사를 제안하였으나, 인터넷상으로는 공공부문의 자가 보험회사 관련 자료를 구하는 데 한계가 있어서 구체적인 형태에 대해서는 검토하지 못했다.

셋째, 본 연구에서는 정보보호 관련 공적규제 및 손해배상과 관련하여 국내 관련 내용만 소개하는 데 그쳤다. 왜냐하면 해외사례를 제대로 전달하기 위해서는 그 나라의 행정규제 체계와 사법체계에 대한 기본 지식이 선행되어야 하기 때문이다. 주요국의 정보보호 관련 공적규제와 손해배상에 대한 비교 분석연구도 의미 있는 향후 연구주제 가운데 하나라고 생각한다.

넷째, 중요한 이슈이지만 본고에서 심층적으로 다루지 않은 이슈 가운데 하나는 사고 데이터 집적 등 공급 측면의 역량 제고와 관련된 이슈이다. 데이터 집적과 관련해서는 주로 미국이나 유럽이 언급되고 있는데, 개인적인 생각으로는 벤치마킹 대상으로

미국이나 유럽이 적절한지 다소 의문이다. 규모가 큰 미국이나 유럽보다는 상대적으로 규모가 작은 호주나 싱가포르 사례를 검토하는 것이 더 바람직한 것 같다.

마지막으로 다섯째, 수요 측면의 시장활성화 장애요인 가운데 하나로 약관의 표준화 미흡이 지적되고 있는데, 이와 관련하여 독일 보험협회에서 만든 권고 약관(Non-Binding General Terms and Conditions for Cyber Risk Insurance)이 하나의 참고사례가 될 수 있다. 사이버보험 약관의 정비와 관련된 주요국 사례연구도 의미있는 연구주제 가운데 하나로 여겨진다.

참고문헌

과학기술정보통신부·한국인터넷진흥원(2017), 『2017년 정보보호 실태조사: 기업부문』

_____(2016), 『2016년 정보보호 실태조사: 기업부문』

_____(2015), 『2015년 정보보호 실태조사: 기업부문』

김규동(2017), 「보험을 이용한 개인의 사이버 리스크 대응 방안」, 『KIRI 리포트』, 보험연구원

김은경(2014), 「정보유출배상책임보험에 대한 소고」, 『금융법연구』, 11권 3호 pp. 149~175, 한국금융법학회

동향분석실(2018), 『2018년 보험소비자 설문조사』, 보험연구원

박영준(2015), 「정보유출배상책임보험의 가입 의무화에 관한 연구」, 『보험법연구』 제9권 제1호 pp. 63~91, 한국보험법학회

배경환·민경식(2013), 「국내 정보보호 보험시장 활성화 방안에 관한 정책제언」, 『KISA Report 2013-08』, 한국인터넷진흥원

보험개발원(2012), 「개인정보유출 배상책임보험의 활성화 방안」, 『CEO Report 2012-04』

송은지·오남호(2017), 「사이버보험을 위한 해외 주요국의 사고데이터 공유 현황」, 『주간기술동향』, 1811호, 정보통신산업진흥원

이경룡(2008), 『보험학원론』, 영지문화사

이기형·안철경·기승도·권오경(2010), 『개인정보 유출사고에 대한 위험관리 방안』, 용역보고서, 한국인터넷진흥원

이승준(2017), 「사이버보험 시장의 활성화를 위한 정책적 과제」, 『KIRI 리포트』, 보험연구원

임준(2017), 「공공데이터 개방과 인슈테크 스타트업」, 『KIRI 리포트』, 보험연구원

____(2016), 「정부3.0과 보험산업의 정보이용」, 『KIRI 리포트』, 보험연구원

정철용·유진호·장항배·김정연·유승동·김양훈·김민정·김태환·송신정·이해니(2013), 「인터넷침해사고 보험제도 도입을 위한 피해액 산정 연구」, 『방송통신정책연구 13-진흥-098』, 정보통신산업진흥원

최우석(2017), 「사이버위험관리 위한 보험의 역할 및 과제」, 『The Risk』 2017 No. 4 Vol. 4 pp. 3~11, 코리안리.

최창희·김혜란(2014), 「해외 사이버 배상책임보험시장 성장의 시사점」, 『KIRI Weekly』, 보험연구원

한국침해사고대응팀협의회(2017), 「지능정보사회 대비 사이버보험 활성화 방안 연구」, 『방송통신정책연구』, 17-방통-24, 과학기술정보통신부·정보통신기술진흥센터

함인선(2016), 『EU 개인정보보호법』, 마로니에

행정안전부·개인정보보호위원회(2017), 『2017년 개인정보보호 실태조사』

_____(2016), 『2016년 개인정보보호 실태조사』

_____(2015), 『2015년 개인정보보호 실태조사』

_____(2014), 『2014년 개인정보보호 실태조사』

_____(2013), 『2013년 개인정보보호 실태조사』

Advisen(2017), "Notable European Cyber Losses From 2011 – 2017"

Ambrosino, D., V. Fragnelli, and M.E. Marina(2006), "Resolving an Insurance Allocation Problem: A Procedural Approach", *Social Choice and Welfare*, 26(3), pp. 625~643

Anderson, R., C. Barton, R. Böhme, R. Clayton, M.J.G. van Eeten, M. Levi, T. Moore, and S. Savage(2013), "Measuring the Cost of Cybercrime" in R. Böhme(ed.) *The Economics of Information Security and Privacy*, Springer

Arnell, N.W., M.J. Clark, and A.M. Gurnell(1984), "Flood Insurance and Extreme Events: The Role of Crisis in Prompting Changes in British Institutional

Response to Flood Hazard", *Applied Geography*, 4, pp. 167~181

Banks, E.(2004), *Alternative Risk Transfer: Integrated Risk Management through Insurance, Reinsurance and the Capital Markets*, John Wiley & Sons, Ltd.

Biener, C., M. Eling, and J.H. Wirfs(2015), "Insurability of Cyber Risk: An Empirical Analysis", *The Geneva Papers on Risk and Insurance-Issues and Practice*, 40(1), pp. 131~158

Böhme, R. and G. Kataria (2006), "Models and Measures for Correlation in Cyber Insurance", Working Paper Presented at the Fifth Workshop on the Economics of Information Security(WEIS), University of Cambridge, pp. 26~28

Cavusoglu, H., B. Mishra, and S. Raghunathan(2004), "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers", *International Journal of Electronic Commerce* 9(1), pp. 70~104

Cebula, J.J. and L.R. Young(2010), "A Taxonomy of Operational Cyber Security Risks", Technical Note CMU/SEI-2010-TN-028, Carnegie Mellon University

Center for Information Policy Leadership(2016), "Protecting Privacy in a World of Big Data", Discussion Draft

Eling, Martin, Werner Schnell, and Fabian Sommerrock(2016), "Ten Key Questions on Cyber Risk and Cyber Risk Insurance", The Geneva Association

Federal Bureau of Investigation(2018), "2017 Internet Crime Report Released"

Fragnelli, V. and M.E. Marina(2003), "A Fair Procedure in Insurance", *Insurance: Mathematics and Economics*, 33(1), pp. 75~85

Heritage Foundation(2018), "Private Sector Cyber Incidents in 2017"

_____(2016), "Cyber Attacks on U.S. Companies in 2016"

_____(2015), "Cyber Attacks on U.S. Companies Since November 2014"

_____(2014), "Cyber Attacks on U.S. Companies in 2014"

Hochstätter, C.H. and M. Masiero(2009), "Angriffe auf das Internet: Wie Realistisch ist der Totalausfall?", *White Paper*

Howard, P.N. and O. Gulyas(2014), "Data Breaches in Europe: Reported Breaches of Compromised Personal Records in Europe, 2005~2014", Center for Media, Data and Society

Identity Theft Resource Center(2018), *2017 Annual Data Breach Year-End Review*

Ike, L.(2016), *Risk Management and Captive Insurance*, Xlibris

Insurance Europe(2018), "Template for Data Breach Notifications"

Kraut, G.(2014), "A Fair Pool Sharing Mechanism for Illiquid Catastrophe Risk Markets", Munich Risk and Insurance Center Working Paper No. 19

Lloyd's(2015), "Business Blackout-The Insurance Implications of a Cyber Attack on the US Power Grid"

Long Finance(2015), "Promoting UK Cyber Prosperity: Public-Private Cyber-Catastrophe Reinsurance"

Mayer-Schönberger, V. and K. Cukier(2013), *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, John Marray

McAfee (2014), "Net Losses: Estimating the Global Cost of Cybercrime"

Maillart, T. and D. Sornette(2010), "Heavy-Tailed Distribution of Cyber Risks", *The European Physical Journal B* 75(3), pp. 357~364

Mantegazza, I.(2017), *How Can the Introduction of Flood Re Mitigate Flood Hazard?: A Stakeholders' Perspective of the Role of the Reinsurance Vehicle in Flood Mitigation*, Amazon Digital Services LLC

National Association of Insurance Commission(2013), "Cybersecurity", http://www.naic.org/cipr_topics/topic_cyber_risk.htm

National Research Council(2015), *Affordability of National Flood Insurance Program Premiums: Report 1*, The National Academies Press

NetDiligence(2014), *Cyber Claims Study 2014*

OECD(2017), *Enhancing the Role of Insurance in Cyber Risk Management*

Office for National Statistics(2018), "Crime in England and Wales: Year Ending December 2017"

Penning-Rowsell, E., S. Priest, and C. Johson(2014), "The Evolution of UK Flood Insurance: Incremental Change over Six Decades", *International Journal of Water Resources Development*, 30(4), pp. 694~713

Romanosky, S.(2016), "Examining the Costs and Causes of Cyber Incidents", *Journal of Cybersecurity*, 2(2), pp. 121~135

Romanosky, S., L. Ablon, A. Kuehn, and T. Jones(2017), "Content Analysis of Cyber Insurance Policies: How Do Carriers Write Policies and Price Cyber Risk?", RAND Working Paper WR-1208

Shackelford, S.J.(2012), "Should Your Firms Invest in Cyber Risk Insurance", *Business Horizons* 55(4), pp. 349~356

Sinanaj, G. and J. Muntermann(2013), "Assessing Corporate Reputational Damage of Data Breaches: An Empirical Analysis", *Proceedings of the 26th International Bled eConference*, pp. 78~89

Smidt, G. and W.J. Wouter Botzen(2017), "Perceptions of Corporate Cyber Risks and Insurance Decision-Making", Working Paper#2017-18, Risk Management and Decision Processes Center, The Wharton School, University of Pennsylvania

Wang, S.(2017), "Put Insurance to Test", American Risk & Insurance Association Presentation Paper

World Economic Forum(2010), *Global Risk Report 2010—A Global Risk Network Report*

YouGov(2014), "Cyber Risiken im Privatberiech"

歌原 崇(2016), サイバーセキュリティと保険, CIPPS

篠原 拓也(2016),『サイバーリスク保険の普及』, 保険·年金フォーカス, ニッセイ基礎研究所

経済産業省(2017),「サイバーセキュリティ経営ガイドライン Ver 2.0」

Information-technology Promotion Agency(2017),『2016年度中小企業における情報セキュリティ対策の実態調査報告書』

_____(2016),『2016企業のCISO やCSIRT に関する実態調査報告書』

_____(2015),『2015企業におけるサイバーリスク管理の実態調査』

Japan Network Security Association(2018), 『2017年度情報セキュリティ市場調査報告書(速報値)』

_____(2017a), 『2016年度情報セキュリティ市場調査報告書』

_____(2017b), 『2017年情報セキュリティインシデントに関する調査報告書』

_____(2016),「サイバーリスク保険 商品 pamphlet」

_____(2014),『2013年情報セキュリティインシデントに関する調査報告書』

Japan Computer Emergency Response Team/Coordination Center(2018),『インシデント報告対応レポート』

National Institute of Information and Communications Technology(2018),『NICTER観測レポート2017の公開』

National center of Incident readiness and Strategy for Cyber Security(2017),『サイバーセキュリティ政策に係る年次報告』

王新雷·王玥(2017),「论网络安全保险发展初级阶段的问题与对策」,『情报杂志』, 第36卷 第12期

赛迪网(2017), "中国市场潜力巨大"

国家互联网应急中心(2017),『2017中国互联网网络安全报告』

_____(2016),『2016中国互联网网络安全报告』

_____(2015),『2015中国互联网网络安全报告』

_____(2014),『2014中国互联网网络安全报告』

陈伟·吴刚·祁志敏(2016.12),「浅析我国网络信息安全保险体系的建立与发展」, 信息安全等级保护技术大会入选论文, 2016年增刊

中国互联网协会(2016),『2016中国网民权益保护调查报告』

证券时报(2016), "支付宝推出银行卡安全险 , 拓展账户安全线"

汪丽(2016), "大力发展网络安全保险 , 助力网络强国建设"

滕讯安全联合实验室(2015),『CTO企业信息安全调查报告』

王新雷(2011),「网络安全保险法律政策的路线图」,『政法学刊』, 第28卷 第1期

高雷·吕文豪(2011),「论建立我国网络信息安全保险体系」,『保险研究』, 2011年第7期

郭静·张昌福(2006. 6),「推进我国网络安全保险的几点建议」,『商场现代化』, (下旬刊) 总第471期

부록. 선행연구 정리자료 소개

부록에서는 사이버위험 및 사이버보험에 대한 개괄적인 정보 제공을 위해 Eling et al.(2016)의 선행연구 정리자료의 내용을 요약·소개하고자 한다.

Eling et al.(2016)은 2000년 1월부터 2016년 5월 사이에 발간된 211개의 논문을 10개 주제로 구분하여 정리하였는데 10개 주제는 다음과 같다
① 사이버위험의 정의 및 특징
② 사이버위험의 피해규모 추정
③ 사이버위험 관련 데이터
④ 사이버위험 모델링
⑤ 미시적 관점: 사이버위험 관리
⑥ 거시적 관점: 사이버위험이 글로벌 경제에 미치는 영향
⑦ 사이버보험 시장현황 및 문제점
⑧ 향후 연구방향(실천적 관점): 보험산업의 역할
⑨ 향후 연구방향(실천적 관점): 정부의 역할
⑩ 향후 연구방향(학술적 관점)

①번에서부터 ⑦번까지는 기존 선행연구를 토대로 사이버위험 및 사이버보험에 대해 현재까지 알려진 사실을 정리한 것이고, ⑧번에서부터 ⑩번까지는 향후 연구방향에 관한 것이다. ⑧번과 ⑨번은 실천적(Practical) 관점의 연구방향이고, ⑩번은 학술적(Academic) 관점의 연구방향이다.

1. 사이버위험의 정의 및 특징

가. 사이버위험의 정의

아직 학문적으로 확립된 정의가 있는 것 같지는 않다. Eling et al.(2016)에서는 Cebula and Young(2010)의 정의를 채택하고 있는 것으로 보이는데 그들의 정의에 의하면, 사이버위험은 정보 및 정보 시스템의 보안성, 이용가능성, 완전성에 훼손을 가져오는 운영위험[90]을 의미한다.

개념적 정의의 경우에는 직관적으로 이해하기 쉽지 않은 측면이 있다. 이러한 점을 보완하기 위한 방법의 하나가 사례를 드는 것인데, National Association of Insurance Commission(2013)에서는 정보유출, 영업중단 등을 사이버위험의 사례로 들고 있다.

나. 사이버위험의 특징

사이버위험은 첫째, 위험 간 상호연관성이 매우 높고, 둘째, 막대한 피해를 가져오는 극단적인 사건의 발생확률이 상대적으로 높으며, 셋째, 기술의 발전과 함께 위험이 빠르게 진화하고 있다.

2. 사이버위험의 피해규모 추정

(개요) 사이버위험의 피해규모 추정치는 피해의 범위를 어디까지 포함시키느냐에 따라 상당히 달라질 수 있다. 사이버위험의 피해는 크게 직접 피해와 간접 피해로 구분할 수 있는데, 직접 피해에는 사이버 범죄자들에게 빼앗긴 금전의 규모 등이 해당되고, 간접 피해에는 신뢰 하락에 의한 손실 등이 포함된다. Anderson et al.(2013)에 의하

90) Operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems(Cebula and Young 2010)

면, 직접 피해보다는 간접 피해와 방어 비용(소프트웨어 구입 및 보험 가입 등)이 더 큰 비중을 차지하고 있다.

(전 세계) 여러 기관들이 사이버위험의 전 세계 연간 피해규모를 추정하였는데, 예를 들어, McAfee(2014)의 추정에 의하면 간접피해를 포함할 때 전 세계 연간 피해규모는 약 4,450억 달러 정도 되었다. 단, 사이버위험 피해규모 추정과 관련하여 주의할 점은 대부분의 추정치가 컨설팅 기관에 의한 것이어서 과대평가 가능성이 높다는 점이다.

(개별기업) 한편, 미시적 관점에서 개별 기업의 피해규모 추정은 주로 주가에 미친 영향 분석을 통해 이루어진다. 예를 들어, Cavusoglu et al.(2004)의 연구에 의하면 시가의 약 2.1%의 손실이 발생했다. 한편, Sinanaj and Muntermann (2013)의 연구에 의하면, 주가손실의 상당 부분이 평판이 나빠짐으로 인해 발생하였다.

3. 사이버위험 관련 데이터

(현황개요) 아직까지는 사이버위험 관련 데이터가 많이 집적되어 있지는 않다. 그 이유 가운데 하나는 사이버 공격의 피해를 받은 기업이 피해 사실을 공개하기 꺼리는 것에서 찾을 수 있다.

(사례소개) 이제까지 사이버위험 관련 실증연구는 대부분 정보유출 사건 정보에 의존하고 있는데, 손실과 관련된 정보는 결여되어 있었다. 최근 들어, 손실 관련 데이터베이스가 구축되었는데, 미국의 경우에는 NetDiligence(2014)가 있고, 전 세계를 대상으로 한 경우에는 Biener et al.(2015)가 있다.

4. 사이버위험 모델링

(현황개요) 데이터의 부족으로 인해 사이버위험의 모델링은 아직 초기 단계에 있다. 현업에서는 통계적 방법보다는 시나리오 분석(Scenario Analysis)에 의존하는 경우가

많다.

(실증연구) 일부 사이버위험 관련 실증연구가 있었는데, Maillart and Sornette (2010)은 신용카드, 은행계좌 관련 정보 유출 데이터를 가지고 사이버위험의 빈도와 심도에 대해 연구하였다. 빈도는 2001년부터 2006년까지 빠르게 증가하였으나, 2006년 이후는 정체 상태를 보였다. 심도[91]의 경우에는 꼬리가 두터운 분포 (Heavy-Tailed Distribution)[92] 형태를 보였다. 심도의 분포는 2006년 이전과 이후에 차이를 보이지 않았다.

(실증연구) 모델링과 관련된 또 다른 이슈는 개별위험의 상관성(Correlation)을 어떻게 모델링할 것이냐 인데, Böhme and Kataria(2006)는 t-copula로 모델링하였다. 그러나 그들은 단순히 시뮬레이션을 위해 t-copula를 사용하였을 뿐 모형의 추정 단계에까지는 이르지 못했다. 좀 더 적절한 모형을 찾기 위해서는 데이터의 집적이 필요하다고 보았다.

5. 미시적 관점: 기업의 사이버위험 관리

(현황개요) 전통적인 위험 관리 프로세스는 ① 목표 설정, ② 위험 식별, ③ 위험 평가 및 분석, ④ 실제 조치(위험회피, 위험완화, 위험전가, 위험보유), ⑤ 모니터링의 5단계로 구성된다. 현재는 위험관리가 주로 위험완화(보안투자)중심으로 이루어지고 있으며, 아직 위험전가(사이버보험)의 역할은 그리 크지 않다.

(실증연구) 미시적 관점의 또 다른 이슈 가운데 하나는 위험 관리 거버넌스와 관련된 것으로 기업의 사이버위험 관리를 위해 CIO(Chief Information Officer)를 두는 것이 효과적이겠는가 하는 것이다. Shackelford(2012)의 연구에 의하면, 정보유출 사고 발생 시 CIO가 있는 기업의 유출 정보 건당 피해액은 157달러였고, 반면 CIO가 없는

91) 심도는 사건 당 유출된 정보 건수로 측정하였음

92) 꼬리가 두터운 분포란, 정규분포(Normal Distribution)에 비해 양 끝 쪽에 있는 큰 값들의 밀도가 더 큰 분포를 의미하는데, 사이버위험과 관련하여 설명하면 매우 큰 피해가 일어날 가능성이 다른 위험들에 비해 높음을 의미함

경우에는 236달러였다.

6. 거시적 관점: 글로벌 경제에 미치는 영향

(주요이슈) 거시적 관점의 주요 이슈는 전 세계 인터넷 대란이 일어날 가능성이 있는가이다. 대부분 전문가의 대답은 '아니다'이다. 그러한 답변의 논거로는 인터넷의 분산적인 구조를 제시하고 있다. 비록 전 세계 차원의 인터넷 대란 가능성은 낮지만, 국지적인 마비는 이미 수차례 발생하였다.[93]

(피해규모) World Economic Forum(2010)의 추정에 의하면, 인터넷 대란이 발생할 경우 발생 초기 2~3일 동안의 피해액만 해도 약 2,500억 달러에 이르렀다. Lloyd's(2015)는 미국 15개 주의 파워 그리드에 대한 사이버 공격이 발생할 경우 피해규모가 약 2,430억 달러에서 1조 달러에 이를 것으로 추정하였다.

7. 사이버보험 시장 현황 및 문제점

(현황전망) 사이버보험 시장은 아직 초기 단계로 규모가 크지 않으나[94] 성장 가능성이 큰 시장으로 여겨지고 있다. 2015년 기준으로 전 세계 사이버보험 시장에서 미국이 차지하는 비중은 약 85% 정도 되었는데,[95] 이처럼 미국이 세계시장을 주도한 이유 가운데 하나는 2002년에 도입한 정보유출 보고 의무화에서 찾을 수 있다. 상품별로 시장 비중을 살펴보면, 미국의 경우에는 제3자(Third Party) 배상과 관련된 사이버보험 상품이 주를 이루고 있다. 반면 유럽의 경우에는 기존 상품들이 계약자 자신의(First Party) 피해를 보상하는 데 초점이 맞추어져 있었다. 그러나 2018년 5월부터 일반정보보호규

93) Hochstätter and Masiero(2009)

94) 2015년 기준 전 세계 사이버보험의 수입보험료는 약 25억 달러 정도 되었다. 같은 해 전 세계 손해보험의 수입보험료는 약 2조 달러였다(Wang 2017).

95) Wang(2017)

칙(General Data Protection Regulation)이 시행될 예정이어서 제3자 배상 관련 상품이 증가할 것으로 예상된다.

(제약요인) 현재 사이버보험 시장 규모가 미미한 것은 여러 제약 요인들 때문인데, Biener et al.(2015)은 다음 3가지를 지적하였다. 첫째, 사이버위험은 위험들이 독립적이지 않고 상호연관성이 높아서 위험 풀링(Pooling)이 제대로 기능하지 않을 수 있다. 또한 데이터가 부족하고, 현재 집적되어 있는 데이터의 경우에도 위험의 진화로 인해 유용성이 떨어져 위험의 모델링이 어렵다.

둘째, 다른 보험의 경우와 마찬가지로 정보의 비대칭성으로 인해 역선택과 도덕적 해이의 문제가 존재한다. 보안이 취약한 기업일수록 사이버보험에 가입할 가능성이 높고, 사이버보험에 가입하게 되면 보안투자에 소홀할 유인이 존재한다.

셋째, 상품의 표준화 미비로 인해 보장여부가 불명확하다. 약관의 용어들이 표준화되어 있지 않아서 사고 발생 시 보험금 수령 여부가 명확하지 않아 가입을 꺼리는 요인으로 작용하고 있다.

(가계시장) 가계시장은 기업시장에 비해 상대적으로 덜 발달되어 있지만 잠재성은 매우 클 것으로 예상하고 있다.[96]

8. 향후 연구방향(실천적 관점): 보험산업의 역할

(개요) 사이버보험 시장의 활성화를 위해 보험산업이 해야 할 과제에는 ① 상품의 표준화, ② 비식별 데이터 풀(Anonymised Data Pools) 구축, ③ 보험풀(Insurance Pools) 구축 등이 포함된다.

(선행연구) 이들 과제 가운데 선행연구는 주로 보험풀에 관한 것이 주를 이루었다.[97] 현재 사이버보험의 경우 가입 건수가 적어서 개별 보험회사별로는 충분한 규모

96) 개인시장에 대한 연구로 Eling et al.(2016)에서 언급한 문헌으로는 YouGov(2014)가 있음. 국내 문헌으로는 김규동(2017)이 있음

97) 영국의 경우에는 이미 사이버위험 관련 보험풀에 대한 논의가 재보험의 관점에서 있었음 (Long Finance 2015)

와 범위의 경제를 달성하기 어려우며, 이러한 문제를 해결하기 위한 방안의 하나로 보험풀이 논의되고 있다. Fragnelli and Marina(2003), Ambrosino et al.(2006), Kraut(2014) 등은 보험풀의 형성을 위해서는 공정한 배분 절차(Fair Sharing Mechanism)가 중요함을 지적하였다.

9. 향후 연구방향(실천적 관점): 정부의 역할

정부의 역할을 ① 사이버위험 방지와 ② 사이버보험 활성화로 크게 구분할 때, 전자에 해당하는 것들에는 정보유출 보고 의무화(Reporting Obligations) 도입 및 위반 시 제재(Penalties) 강화, 정보보안 관련 최소 기준(Minimum Standards for Risk Mitigation) 도입 등이 해당된다.

사이버보험 활성화를 위한 정부 정책들로는 정부와 민간 보험회사간 파트너십을 통한 위험 분담,[98] 비식별 데이터풀(Anonymised Data Pool) 구축 지원,[99] 보험풀(Insurance Pool) 형성 지원, 대체 위험 전가 수단(Alternative Risk Transfer Mechanism)[100] 개발 지원 등이 해당된다.

사이버위험 방지 정책들도 간접적으로 사이버보험 활성화와 관련을 가진다. 미국의 사이버보험 시장이 유럽에 비해 활성화된 요인의 하나로 정보유출 보고 의무화를 꼽고 있다. 유럽의 경우 2018년부터 정보유출 보고 의무화가 도입되는데, 제도의 도입이 미국의 경우처럼 사이버보험 활성화의 촉매로 작용할 것인지가 향후 하나의 재미있는 실증연구 이슈가 될 것으로 예상된다. 한편, 정보보안 관련 최소 기준 도입도 사이버보험의 도덕적 해이 문제를 완화할 수 있다는 측면에서 사이버보험 활성화와 간접적으로 관련성을 가진다.

98) 미국의 경우 2016년에 사이버위험도 테러위험보험법(Terrorism Risk Insurance Act)의 적용을 받게 되었음

99) 예는 미국의 National Vulnerability Database(NIST)임

100) 대체위험전가 수단의 한 예는 Cyber Cat Bonds임

10. 향후 연구방향(학술적 관점)

첫째, 사이버보험의 수요측과 관련된 연구가 부족한 상황이다. 예를 들면, 사이버위험에 대한 인식,[101] 보안투자와 사이버보험 간 최적 선택 등에 대한 연구가 필요하다.

둘째, 데이터의 축적과 함께 사이버위험의 특징 및 모델링에 대한 연구가 지속적으로 필요하다.

101) 사이버위험에 대한 주관적 인식과 객관적 위험을 비교한 최근 연구로는 Smidt and Botzen(2017)이 있음

보험연구원(KIRI) 발간물 안내

※ 2017년부터 기존의 연구보고서, 정책보고서, 경영보고서, 조사보고서가 연구보고서로 통합되었습니다.

■ 연구보고서

2017-1 보험산업 미래 / 김석영·윤성훈·이선주 2017.2
2017-2 자동차보험 과실상계제도 개선방안 / 전용식·채원영 2017.2
2017-3 상호협정 관련 입법정책 연구 / 정호열 2017.2
2017-4 저소득층 노후소득 보장을 위한 공사연계연금 연구 / 정원석·강성호·마지혜 2017.3
2017-5 자영업자를 위한 사적소득보상체계 개선방안 / 류건식·강성호·김동겸 2017.3
2017-6 우리나라 사회안전망 개선을 위한 현안 과제 / 이태열·최장훈·김유미 2017.4
2017-7 일본의 보험회사 도산처리제도 및 사례 / 정봉은 2017.5
2017-8 보험회사 업무위탁 관련 제도 개선방안 / 이승준·정인영 2017.5
2017-9 부채시가평가제도와 생명보험회사의 자본관리 / 조영현·이혜은 2017.8
2017-10 효율적 의료비 지출을 통한 국민건강보험의 보장성 강화 방안 / 김대환 2017.8
2017-11 인슈어테크 혁명: 현황 점검 및 과제 고찰 / 박소정·박지윤 2017.8
2017-12 생산물 배상책임보험 역할 제고 방안 / 이기형·이규성 2017.9
2017-13 보험금청구권과 소멸시효 / 권영준 2017.9
2017-14 2017년 보험소비자 설문조사 / 동향분석실 2017.10
2017-15 2018년도 보험산업 전망과 과제 / 동향분석실 2017.11
2017-16 퇴직연금 환경변화와 연금세제 개편 방향 / 강성호·류건식·김동겸 2017.12
2017-17 자동차보험 한방진료 현황과 개선방안 / 송윤아·이소양 2017.12
2017-18 베이비부머 세대의 노후소득 / 최장훈·이태열·김미화 2017.12
2017-19 연금세제 효과연구 / 정원석·이선주 2017.12
2017-20 주요국의 지진보험 운영 현황 및 시사점 / 최창희·한성원 2017.12
2017-21 사적연금의 장기연금수령 유도방안 / 김세중·김유미 2017.12
2017-22 누적전망이론을 이용한 생명보험과 연금의 유보가격 측정 연구 / 지홍민 2017.12
2018-1 보증연장 서비스 규제 방안 / 백영화·박정희 2018.1
2018-2 건강생활서비스 공·사 협력 방안 / 조용운·오승연·김동겸 2018.2

2018-3 퇴직연금 가입자교육 개선 방안 / 류건식·강성호·이상우 2018.2
2018-4 IFRS 9과 보험회사의 ALM 및 자산배분 / 조영현·이혜은 2018.2
2018-5 보험상품 변천과 개발 방향 / 김석영·김세영·이선주 2018.2
2018-6 계리적 관점에서 본 실손의료보험 개선 방안 / 조재린·정성희 2018.3
2018-7 국내 보험회사의 금융겸업 현황과 시사점 / 전용식·이혜은 2018.3
2018-8 장애인의 위험보장 강화 방안 / 오승연·김석영·이선주 2018.4
2018-9 주요국 공·사 건강보험 연계 체계 분석 / 정성희·이태열·김유미 2018.4
2018-10 정신질환 위험보장 강화 방안 / 이정택·임태준·김동겸 2018.4
2018-11 기초서류 준수의무 위반시 과징금 부과기준 개선방안 / 황현아·백영화·권오경 2018.8
2018-12 2018년 보험소비자 설문조사 / 동향분석실 2018.9
2018-13 상속법의 관점에서 본 생명보험 / 최준규 2018.9
2018-14 호주 퇴직연금제도 현황과 시사점 / 이경희 2018.9
2018-15 빅데이터 기반의 사이버위험 측정 방법 및 사이버사고 예측모형 연구 / 이진무 2018.9
2018-16 빅데이터 분석에 의한 요율산정 방법 비교: 실손의료보험 적용 사례 / 이항석 2018.9
2018-17 보험 모집 행위의 의미 및 범위에 대한 검토 / 백영화·손민숙 2018.10
2018-18 보험회사 해외채권투자와 환헤지 / 황인창·임준환·채원영 2018.10
2018-19 베트남 생명보험산업의 현황 및 시사점 / 조용운·김동겸 2018.10
2018-20 여성 관련 연금정책 평가와 개선 방향 / 강성호·류건식·김동겸 2018.10

■ 연구보고서(구)

2008-1 보험회사의 리스크 중심 경영전략에 관한 연구 / 최영목·장동식·김동겸 2008.1
2008-2 한국 보험시장과 공정거래법 / 정호열 2008.6
2008-3 확정급여형 퇴직연금의 자산운용 / 류건식·이경희·김동겸 2008.3
2009-1 보험설계사의 특성분석과 고능률화 방안 / 안철경·권오경 2009.1
2009-2 자동차사고의 사회적 비용 최소화 방안 / 기승도 2009.2
2009-3 우리나라 가계부채 문제의 진단과 평가 / 유경원·이혜은 2009.3
2009-4 사적연금의 노후소득보장 기능제고 방안 / 류건식·이창우·김동겸 2009.3
2009-5 일반화선형모형(GLM)을 이용한 자동차보험 요율상대도 산출 방법 연구 / 기승도·김대환 2009.8

2009-6 주행거리에 연동한 자동차보험제도 연구 / 기승도·김대환·김혜란 2010.1
2010-1 우리나라 가계 금융자산 축적 부진의 원인과 시사점 / 유경원·이혜은 2010.4
2010-2 생명보험 상품별 해지율 추정 및 예측 모형 / 황진태·이경희 2010.5
2010-3 보험회사 자산관리서비스 사업모형 검토 / 진 익·김동겸 2010.7

■ 정책보고서(구)

2008-2 환경오염리스크관리를 위한 보험제도 활용방안 / 이기형 2008.3
2008-3 금융상품의 정의 및 분류에 관한 연구 / 유지호·최 원 2008.3
2008-4 2009년도 보험산업 전망과 과제 / 이진면·이태열·신종협·황진태·유진아·김세환·이정환·박정희·김세중·최이섭 2008.11
2009-1 현 금융위기 진단과 위기극복을 위한 정책제언 / 진 익·이민환·유경원·최영목·최형선·최 원·이경아·이혜은 2009.2
2009-2 퇴직연금의 급여 지급 방식 다양화 방안 / 이경희 2009.3
2009-3 보험분쟁의 재판외적 해결 활성화 방안 / 오영수·김경환·이종욱 2009.3
2009-4 2010년도 보험산업 전망과 과제 / 이진면·황진태·변혜원·이경희·이정환·박정희·김세중·최이섭 2009.12
2009-5 금융상품판매전문회사의 도입이 보험회사에 미치는 영향 / 안철경·변혜원·권오경 2010.1
2010-1 보험사기 영향요인과 방지방안 / 송윤아 2010.3
2010-2 2011년도 보험산업 전망과 과제 / 이진면·김대환·이경희·이정환·최 원·김세중·최이섭 2010.12
2011-1 금융소비자 보호 체계 개선방안 / 오영수·안철경·변혜원·최영목·최형선·김경환·이상우·박정희·김미화 2010.4
2011-2 일반공제사업 규제의 합리화 방안 / 오영수·김경환·박정희 2011.7
2011-3 퇴직연금 적립금의 연금전환 유도방안 / 이경희 2011.5
2011-4 저출산·고령화와 금융의 역할 / 윤성훈·류건식·오영수·조용운·진 익·유진아·변혜원 2011.7
2011-5 소비자 보호를 위한 보험유통채널 개선방안 / 안철경·이경희 2011.11
2011-6 2012년도 보험산업 전망과 과제 / 윤성훈·황진태·이정환·최 원·김세중·오병국 2011.12
2012-1 인적사고 보험금의 지급방식 다양화 방안 / 조재린·이기형·정인영 2012.8
2012-2 보험산업 진입 및 퇴출에 관한 연구 / 이기형·변혜원·정인영 2012.10
2012-3 금융위기 이후 보험규제 변화 및 시사점 / 임준환·유진아·이경아 2012.11

2012-4 소비자중심의 변액연금보험 개선방안 연구: 공시 및 상품설계 개선을 중심으로 / 이기형·임준환·김해식·이경희·조영현·정인영 2012.12
2013-1 생명보험의 자살면책기간이 자살에 미치는 영향 / 이창우·윤상호 2013.1
2013-2 퇴직연금 지배구조체계 개선방안 / 류건식·김대환·이상우 2013.1
2013-3 2013년도 보험산업 전망과 과제 / 윤성훈·전용식·이정환·최 원·김세중·채원영 2013.2
2013-4 사회안전망 체제 개편과 보험산업 역할 / 진 익·오병국·이성은 2013.3
2013-5 보험지주회사 감독체계 개선방안 연구 / 이승준·김해식·조재린 2013.5
2013-6 2014년도 보험산업 전망과 과제 / 윤성훈·전용식·최 원·김세중·채원영 2013.12
2014-1 보험시장 경쟁정책 투명성 제고방안 / 이승준·강민규·이해랑 2014.3
2014-2 국내 보험회사 지급여력규제 평가 및 개선방안 / 조재린·김해식·김석영 2014.3
2014-3 공·사 사회안전망의 효율적인 역할 제고 방안 / 이태열·강성호·김유미 2014.4
2014-4 2015년도 보험산업 전망과 과제 / 윤성훈·김석영·김진억·최 원·채원영·이아름·이해랑 2014.11
2014-5 의료보장체계 합리화를 위한 공·사건강보험 협력방안 / 조용운·김경환·김미화 2014.12
2015-1 보험회사 재무건전성 규제 - IFRS와 RBC 연계방안 / 김해식·조재린·이경아 2015.2
2015-2 2016년도 보험산업 전망과 과제 / 윤성훈·김석영·김진억·최 원·채원영·이아름·이해랑 2015.11
2016-1 정년연장의 노후소득 개선 효과와 개인연금의 정책방향 / 강성호·정봉은·김유미 2016.2
2016-2 국민건강보험 보장률 인상 정책 평가: DSGE 접근법 / 임태준·이정택·김혜란 2016.11
2016-3 2017년도 보험산업 전망과 과제 / 동향분석실 2016.12

■ 경영보고서(구)

2009-1 기업휴지보험 활성화 방안 연구 / 이기형·한상용 2009.3
2009-2 자산관리서비스 활성화 방안 / 진 익 2009.3
2009-3 탄소시장 및 녹색보험 활성화 방안 / 진 익·유시용·이경아 2009.3

2009-4 생명보험회사의 지속가능성장에 관한 연구 / 최영목·최 원 2009.6
2010-1 독립판매채널의 성장과 생명보험회사의 대응 / 안철경·권오경 2010.2
2010-2 보험회사의 윤리경영 운영실태 및 개선방안 / 오영수·김경환 2010.2
2010-3 보험회사의 퇴직연금사업 운영전략 / 류건식·이창우·이상우 2010.3
2010-4(1) 보험환경변화에 따른 보험산업 성장방안 / 산업연구실·정책연구실·동향분석실 2010.6
2010-4(2) 종합금융서비스를 활용한 보험산업 성장방안 / 금융제도실·재무연구실 2010.6
2010-5 변액보험 보증리스크관리연구 / 권용재·장동식·서성민 2010.4
2010-6 RBC 내부모형 도입 방안 / 김해식·최영목·김소연·장동식·서성민 2010.10
2010-7 금융보증보험 가격결정모형 / 최영수 2010.7
2011-1 보험회사의 비대면채널 활용방안 / 안철경·변혜원·서성민 2011.1
2011-2 보증보험의 특성과 리스크 평가 / 최영목·김소연·김동겸 2011.2
2011-3 충성도를 고려한 자동차보험 마케팅전략 연구 / 기승도·황진태 2011.3
2011-4 보험회사의 상조서비스 기여방안 / 황진태·기승도·권오경 2011.5
2011-5 사기성클레임에 대한 최적조사방안 / 송윤아·정인영 2011.6
2011-6 민영의료보험의 보험리스크관리방안 / 조용운·황진태·김미화 2011.8
2011-7 보험회사의 개인형 퇴직연금 운영방안 / 류건식·김대환·이상우 2011.9
2011-8 퇴직연금시장의 환경변화에 따른 확정기여형 퇴직연금 운영방안 / 김대환·류건식·이상우 2011.10
2012-1 국내 생명보험회사의 기업공개 평가와 시사점 / 조영현·전용식·이혜은 2012.7
2012-2 보험산업 비전 2020 : ⓝ sure 4.0 / 진 익·김동겸·김혜란 2012.7
2012-3 현금흐름방식 보험료 산출의 시행과 과제 / 김해식·김석영·김세영·이혜은 2012.9
2012-4 보험회사의 장수리스크 발생원인과 관리방안 / 김대환·류건식·김동겸 2012.9
2012-5 은퇴가구의 경제형태 분석 / 유경원 2012.9
2012-6 보험회사의 날씨리스크 인수 활성화 방안: 지수형 날씨보험을 중심으로 / 조재린·황진태·권용재·채원영 2012.10
2013-1 자동차보험시장의 가격경쟁이 손해율에 미치는 영향과 시사점 / 전용식·채원영 2013.3
2013-2 중국 자동차보험 시장점유율 확대방안 연구 / 기승도·조용운·이소양 2013.5
2016-1 뉴 노멀 시대의 보험회사 경영전략 / 임준환·정봉은·황인창·이혜은·김혜란·

정승연 2016.4
2016-2 금융보증보험 잠재 시장 연구: 지방자치단체 자금조달 시장을 중심으로 / 최창희·황인창·이경아 2016.5
2016-3 퇴직연금시장 환경변화와 보험회사 대응방안 / 류건식·강성호·김동겸 2016.5

■ 조사보고서(구)

2008-1 보험회사 글로벌화를 위한 해외보험시장 조사 / 양성문·김진억·지재원·박정희·김세중 2008.2
2008-2 노인장기요양보험 제도 도입에 대응한 장기간병보험 운영 방안 / 오영수 2008.3
2008-3 2008년 보험소비자 설문조사 / 안철경·기승도·이상우 2008.4
2008-4 주요국의 보험상품 판매권유 규제 / 이상우 2008.3
2009-1 2009년 보험소비자 설문조사 / 안철경·이상우·권오경 2009.3
2009-2 Solvency II의 리스크 평가모형 및 측정 방법 연구 / 장동식 2009.3
2009-3 이슬람 보험시장 진출방안 / 이진면·이정환·최이섭·정중영·최태영 2009.3
2009-4 미국 생명보험 정산거래의 현황과 시사점 / 김해식 2009.3
2009-5 헤지펀드 운용전략 활용방안 / 진 익·김상수·김종훈·변귀영·유시용 2009.3
2009-6 복합금융 그룹의 리스크와 감독 / 이민환·전선애·최 원 2009.4
2009-7 보험산업 글로벌화를 위한 정책적 지원방안 / 서대교·오영수·김영진 2009.4
2009-8 구조화금융 관점에서 본 금융위기 분석 및 시사점 / 임준환·이민환·윤건용·최 원 2009.7
2009-9 보험리스크 측정 및 평가 방법에 관한 연구 / 조용운·김세환·김세중 2009.7
2009-10 생명보험계약의 효력상실·해약분석 / 류건식·장동식 2009.8
2010-1 과거 금융위기 사례분석을 통한 최근 글로벌 금융위기 전망 / 신종협·최형선·최 원 2010.3
2010-2 금융산업의 영업행위 규제 개선방안 / 서대교·김미화 2010.3
2010-3 주요국의 민영건강보험의 운영체계와 시사점 / 이창우·이상우 2010.4
2010-4 2010년 보험소비자 설문조사 / 변혜원·박정희 2010.4
2010-5 산재보험의 운영체계에 대한 연구 / 송윤아 2010.5
2010-6 보험산업 내 공정거래규제 조화방안 / 이승준·이종욱 2010.5
2010-7 보험종류별 진료수가 차등적용 개선방안 / 조용운·서대교·김미화 2010.4
2010-8 보험회사의 금리위험 대응전략 / 진 익·김해식·유진아·김동겸 2011.1
2010-9 퇴직연금 규제체계 및 정책방향 / 류건식·이창우·이상우 2010.7

2011-1 생명보험설계사 활동실태 및 만족도 분석 / 안철경·황진태·서성민 2011.6
2011-2 2011년 보험소비자 설문조사 / 김대환·최 원 2011.5
2011-3 보험회사 녹색금융 참여방안 / 진 익·김해식·김혜란 2011.7
2011-4 의료시장 변화에 따른 민영실손의료보험의 대응 / 이창우·이기형 2011.8
2011-5 아세안 주요국의 보험시장 규제제도 연구 / 조용운·변혜원·이승준·김경환·오병국 2011.11
2012-1 2012년 보험소비자 설문조사 / 황진태·전용식·윤상호·기승도·이상우·최 원 2012.6
2012-2 일본의 퇴직연금제도 운영체계 특징과 시사점 / 이상우·오병국 2012.12
2012-3 솔벤시 Ⅱ의 보고 및 공시 체계와 시사점 / 장동식·김경환 2012.12
2013-1 2013년 보험소비자 설문조사 / 전용식·황진태·변혜원·정원석·박선영·이상우·최 원 2013.8
2013-2 건강보험 진료비 전망 및 활용방안 / 조용운·황진태·조재린 2013.9
2013-3 소비자 신뢰 제고와 보험상품 정보공시 개선방안 / 김해식·변혜원·황진태 2013.12
2013-4 보험회사의 사회적 책임 이행에 관한 연구 / 변혜원·조영현 2013.12
2014-1 주택연금 연계 간병보험제도 도입 방안 / 박선영·권오경 2014.3
2014-2 소득수준을 고려한 개인연금 세제 효율화방안: 보험료 납입단계의 세제방식 중심으로 / 정원석·강성호·이상우 2014.4
2014-3 보험규제에 관한 주요국의 법제연구: 모집채널, 행위 규제 등을 중심으로 / 한기정·최준규 2014.4
2014-4 보험산업 환경변화와 판매채널 전략 연구 / 황진태·박선영·권오경 2014.4
2014-5 거시경제 환경변화의 보험산업 파급효과 분석 / 전성주·전용식 2014.5
2014-6 국내경제의 일본식 장기부진 가능성 검토 / 전용식·윤성훈·채원영 2014.5
2014-7 건강생활관리서비스 사업모형 연구 / 조용운·오승연·김미화 2014.7
2014-8 보험개인정보 보호법제 개선방안 / 김경환·강민규·이해랑 2014.8
2014-9 2014년 보험소비자 설문조사 / 전용식·변혜원·정원석·박선영·오승연·이상우·최 원 2014.8
2014-10 보험회사 수익구조 진단 및 개선방안 / 김석영·김세중·김혜란 2014.11
2014-11 국내 보험회사의 해외사업 평가와 제언 / 전용식·조영현·채원영 2014.12
2015-1 보험민원 해결 프로세스 선진화 방안 / 박선영·권오경 2015.1
2015-2 재무건전성 규제 강화와 생명보험회사의 자본관리 / 조영현·조재린·김혜란 2015.2
2015-3 국내 배상책임보험 시장 성장 저해 요인 분석 - 대인사고 손해배상액 산정

기준을 중심으로 - / 최창희·정인영 2015.3
2015-4 보험산업 신뢰도 제고 방안 / 이태열·황진태·이선주 2015.3
2015-5 2015년 보험소비자 설문조사 / 동향분석실 2015.8
2015-6 인구 및 가구구조 변화가 보험 수요에 미치는 영향 / 오승연·김유미 2015.8
2016-1 경영환경 변화와 주요 해외 보험회사의 대응 전략 / 전용식·조영현 2016.2
2016-2 시스템리스크를 고려한 복합금융그룹 감독방안 / 이승준·민세진 2016.3
2016-3 저성장 시대 보험회사의 비용관리 / 김해식·김세중·김현경 2016.4
2016-4 자동차보험 해외사업 경영성과 분석과 시사점 / 전용식·송윤아·채원영 2016.4
2016-5 금융·보험세제연구: 집합투자기구, 보험 그리고 연금세제를 중심으로 / 정원석·임 준·김유미 2016.5
2016-6 가용자본 산출 방식에 따른국내 보험회사 지급여력 비교 / 조재린·황인창·이경아 2016.5
2016-7 해외 사례를 통해 본 중·소형 보험회사의 생존전략 / 이태열·김해식·김현경 2016.5
2016-8 생명보험회사의 연금상품 다양화 방안: 종신소득 보장기능을 중심으로 / 김세중·김혜란 2016.6
2016-9 2016년 보험소비자 설문조사 / 동향분석실 2016.8
2016-10 자율주행자동차 보험제도 연구 / 이기형·김혜란 2016.9

■ 조사자료집

2014-1 보험시장 자유화에 따른 보험산업 환경변화 / 최 원·김세중 2014.6
2014-2 주요국 내부자본적정성 평가 및 관리 제도 연구 - Own Risk and Solvency Assessment - / 장동식·이정환 2014.8
2015-1 고령층 대상 보험시장 현황과 해외사례 / 강성호·정원석·김동겸 2015.1
2015-2 경증치매자 보호를 위한 보험사의 치매신탁 도입방안 / 정봉은·이선주 2015.2
2015-3 소비자 금융이해력 강화 방안: 보험 및 연금 / 변혜원·이해랑 2015.4
2015-4 글로벌 금융위기 이후 세계경제의 구조적 변화 / 박대근·박춘원·이항용 2015.5
2015-5 노후소득보장을 위한 주택연금 활성화 방안 / 전성주·박선영·김유미 2015.5
2015-6 고령화에 대응한 생애자산관리 서비스 활성화 방안 / 정원석·김미화 2015.5
2015-7 일반 손해보험 요율제도 개선방안 연구 / 김석영·김혜란 2015.12

2018-1 변액연금 최저보증 및 사업비 부과 현황 조사 / 김세환 2018.2

■ 연차보고서

제 1 호 2008년 연차보고서 / 보험연구원 2009.4
제 2 호 2009년 연차보고서 / 보험연구원 2010.3
제 3 호 2010년 연차보고서 / 보험연구원 2011.3
제 4 호 2011년 연차보고서 / 보험연구원 2012.3
제 5 호 2012년 연차보고서 / 보험연구원 2013.3
제 6 호 2013년 연차보고서 / 보험연구원 2013.12
제 7 호 2014년 연차보고서 / 보험연구원 2014.12
제 8 호 2015년 연차보고서 / 보험연구원 2015.12
제 9 호 2016년 연차보고서 / 보험연구원 2017.1
제 10 호 2017년 연차보고서 / 보험연구원 2018.1

■ 영문발간물

제 7 호 Korean Insurance Industry 2008 / KIRI, 2008.9
제 8 호 Korean Insurance Industry 2009 / KIRI, 2009.9
제 9 호 Korean Insurance Industry 2010 / KIRI, 2010.8
제10호 Korean Insurance Industry 2011 / KIRI, 2011.10
제11호 Korean Insurance Industry 2012 / KIRI, 2012.11
제12호 Korean Insurance Industry 2013 / KIRI, 2013.12
제13호 Korean Insurance Industry 2014 / KIRI, 2014.8
제14호 Korean Insurance Industry 2015 / KIRI, 2015.8
제15호 Korean Insurance Industry 2016 / KIRI, 2016.8
제16호 Korean Insurance Industry 2017 / KIRI, 2017.8
제 7 호 Korean Insurance Industry Trend 2Q FY2013 / KIRI, 2014.2
제 8 호 Korean Insurance Industry Trend 3Q FY2013 / KIRI, 2014.5
제 9 호 Korean Insurance Industry Trend 1Q FY2014 / KIRI, 2014.8
제10호 Korean Insurance Industry Trend 2Q FY2014 / KIRI, 2014.10
제11호 Korean Insurance Industry Trend 3Q FY2014 / KIRI, 2015.2
제12호 Korean Insurance Industry Trend 4Q FY2014 / KIRI, 2015.4
제13호 Korean Insurance Industry Trend 1Q FY2015 / KIRI, 2015.8
제14호 Korean Insurance Industry Trend 2Q FY2015 / KIRI, 2015.11

제15호 Korean Insurance Industry Trend 3Q FY2015 / KIRI, 2016.2
제16호 Korean Insurance Industry Trend 4Q FY2015/ KIRI, 2016.6
제17호 Korean Insurance Industry Trend 1Q FY2016/ KIRI, 2016.9
제18호 Korean Insurance Industry Trend 2Q FY2016/ KIRI, 2016.12
제19호 Korean Insurance Industry Trend 3Q FY2016/ KIRI, 2017.2
제20호 Korean Insurance Industry Trend 4Q FY2016/ KIRI, 2017.5
제21호 Korean Insurance Industry Trend 1Q FY2017/ KIRI, 2017.9
제22호 Korean Insurance Industry Trend 2Q FY2017/ KIRI, 2017.11

■ CEO Report

2008-1 자동차보험 물적담보 손해율 관리 방안 / 기승도 2008.6
2008-2 보험산업 소액지급결제시스템 참여 관련 주요 이슈 / 이태열 2008.6
2008-3 FY2008 수입보험료 전망 / 동향분석실 2008.8
2008-4 퇴직급여보장법 개정안의 영향과 보험회사 대응과제 / 류건식·서성민 2008.12
2009-1 FY2009 보험산업 수정전망과 대응과제 / 동향분석실 2009.2
2009-2 퇴직연금 예금보험요율 적용의 타당성 검토 / 류건식·김동겸 2009.3
2009-3 퇴직연금 사업자 관련규제의 적정성 검토 / 류건식·이상우 2009.6
2009-4 퇴직연금 가입 및 인식실태 조사 / 류건식·이상우 2009.10
2010-1 복수사용자 퇴직연금제도의 도입 및 보험회사의 대응과제 / 김대환·이상우·김혜란 2010.4
2010-2 FY2010 수입보험료 전망 / 동향분석실 2010.6
2010-3 보험소비자 보호의 경영전략적 접근 / 오영수 2010.7
2010-4 장기손해보험 보험사기 방지를 위한 보험금 지급심사제도 개선 / 김대환·이기형 2010.9
2010-5 퇴직금 중간정산의 문제점과 개선과제 / 류건식·이상우 2010.9
2010-6 우리나라 신용카드시장의 특징 및 개선논의 / 최형선 2010.11
2011-1 G20 정상회의의 금융규제 논의 내용 및 보험산업에 대한 시사점 / 김동겸 2011.2
2011-2 영국의 공동계정 운영체계 / 최형선·김동겸 2011.3
2011-3 FY2011 수입보험료 전망 / 동향분석실 2011.7
2011-4 근퇴법 개정에 따른 퇴직연금 운영방안과 과제 / 김대환·류건식 2011.8
2012-1 FY2012 수입보험료 전망 / 동향분석실 2012.8

2012-2 건강생활서비스법 제정(안)에 대한 검토 / 조용운·이상우 2012.11
2012-3 보험연구원 명사초청 보험발전 간담회 토론 내용 / 윤성훈·전용식·전성주·채원영 2012.12
2012-4 새정부의 보험산업 정책(Ⅰ): 정책공약집을 중심으로 / 이기형·정인영 2012.12
2013-1 새정부의 보험산업 정책(Ⅱ): 국민건강보험 본인부담경감제 정책에 대한 평가 / 김대환·이상우 2013.1
2013-2 새정부의 보험산업 정책(Ⅲ): 제18대 대통령직인수위원회 제안 국정과제를 중심으로 / 이승준 2013.3
2013-3 FY2013 수입보험료 수정 전망 / 동향분석실 2013.7
2013-4 유럽 복합금융그룹의 보험사업 매각 원인과 시사점 / 전용식·윤성훈 2013.7
2014-1 2014년 수입보험료 수정 전망 / 동향분석실 2014.6
2014-2 인구구조 변화가 보험계약규모에 미치는 영향 분석 / 김석영·김세중 2014.6
2014-3 『보험 혁신 및 건전화 방안』의 주요 내용과 시사점 / 이태열·조재린·황진태·송윤아 2014.7
2014-4 아베노믹스 평가와 시사점 / 임준환·황인창·이혜은 2014.10
2015-1 연말정산 논란을 통해 본 소득세제 개선 방향 / 강성호·류건식·정원석 2015.2
2015-2 2015년 수입보험료 수정 전망 / 동향분석실 2015.6
2015-3 보험산업 경쟁력 제고 방안 및 이의 영향 / 김석영 2015.10
2016-1 금융규제 운영규정 제정 의미와 시사점 / 김석영 2016.1
2016-3 2016년 수입보험료 수정 전망 / 동향분석실 2016.7
2016-4 EU Solvency Ⅱ 경과조치의 의미와 시사점 / 황인창·조재린 2016.7
2016-5 비급여 진료비 관련 최근 논의 동향과 시사점 / 정성희·이태열 2016.9
2017-1 보험부채 시가평가와 보험산업의 과제 / 김해식 2017.2
2017-2 2017년 수입보험료 수정 전망 / 동향분석실 2017.7
2017-3 1인 1 퇴직연금시대의 보험회사 IRP 전략 / 류건식·이태열 2017.7
2018-1 2018년 수입보험료 수정 전망 / 동향분석실 2018.7
2018-2 북한 보험산업의 이해와 대응 / 안철경·정인영 2018.7

■ Insurance Business Report

26호 퇴직연금 중심의 근로자 노후소득보장 과제 / 류건식·김동겸 2008.2
27호 보험부채의 리스크마진 측정 및 적용 사례 / 이경희 2008.6

28호 일본 금융상품판매법의 주요내용과 보험산업에 대한 영향 / 이기형 2008.6
29호 보험회사의 노인장기요양 사업 진출 방안 / 오영수 2008.6
30호 교차모집제도의 활용의향 분석 / 안철경·권오경 2008.7
31호 퇴직연금 국제회계기준의 도입영향과 대응과제 / 류건식·김동겸 2008.7
32호 보험회사의 헤지펀드 활용방안 / 진 익 2008.7
33호 연금보험의 확대와 보험회사의 대응과제 / 이경희·서성민 2008.9

■ 간행물

○ 보험동향 / 연 4회
○ 보험금융연구 / 연 4회

※ 2008년 이전 발간물은 보험연구원 홈페이지(http://www.kiri.or.kr)에서 확인하시기 바랍니다.

『도서회원 가입안내』

회원 및 제공자료

	법인회원	특별회원	개인회원
연회비	₩300,000원	₩150,000원	₩150,000원
제공자료	- 연구보고서 - 기타보고서 - 연속간행물 · 보험금융연구 · 보험동향 · KIRI 포커스 모음집 · KIRI 이슈 모음집 · KOREA INSURANCE INDUSTRY	- 연구보고서 - 기타보고서 - 연속간행물 · 보험금융연구 · 보험동향 · KIRI 포커스 모음집 · KIRI 이슈 모음집 · KOREA INSURANCE INDUSTRY	- 연구보고서 - 기타보고서 - 연속간행물 · 보험금융연구 · 보험동향 · KIRI 포커스 모음집 · KIRI 이슈 모음집 · KOREA INSURANCE INDUSTRY
	- 영문연차보고서	-	-

※ 특별회원 가입대상 : 도서관 및 독서진흥법에 의하여 설립된 공공도서관 및 대학도서관

가입문의

보험연구원 도서회원 담당
전화 : (02) 3775 - 9080　팩스 : (02) 3775 - 9102

회비납입방법

- 무통장입금 : 국민은행 (400401 - 01 - 125198)
  예금주 : 보험연구원

가입절차

보험연구원 홈페이지(www.kiri.or.kr)에 접속 후 도서회원가입신청서를 작성·등록 후
회비입금을 하시면 확인 후 1년간 회원자격이 주어집니다.

자료구입처

서울 : 보험연구원 자료실 (02-3775-9115 / cbyun@kiri.or.kr)

저 자 약 력

임 준
Michigan 주립대 경제학 박사
보험연구원 연구위원
(E-mail : limjoon@kiri.or.kr)

이 상 우
홍익대학교, 박사과정 수료
일본 중앙대 상학 석사
보험연구원 수석연구원
(E-mail : swlee@kiri.or.kr)

이 소 양
중앙대 경영학 석사
보험연구원 연구원
(E-mail : lishaoyang@kiri.or.kr)

연구보고서 2018-21

디지털 경제 활성화를 위한 사이버보험 역할제고 방안

발행일	2018년 11월
발행인	한 기 정
발행처	**보 험 연 구 원** 서울특별시 영등포구 국제금융로 6길 38 화재보험협회빌딩 대표전화 : (02) 3775-9000
조판및 인 쇄	고려씨엔피

ISBN 979-11-85691-78-7 94320
979-11-85691-50-3 (세트) 정가 10,000원