KiRi Weekly
2015.11.9 제358호

KiRi 보험연구원
Korea Insurance Research Institute

서울시 영등포구 국제금융로 6길 38 (여의도동 35-4) 8층 보험연구원 (문의 : 변철성 수석담당역 / 02-3775-9115)

KiRi Weekly 2015.11.9
포커스

사이버보험 동향 및 사이버리스크 관리 개선을 위한 고려사항

변혜원 연구위원

요약

정보통신기술의 발달로 사회가 직면한 사이버리스크는 확대되고 있는 추세임. 그러나 손실노출 예측의 어려움, 리스크 간의 높은 상관성, 손실의 관리가능성, 지불가능한 보험료 책정 측면에서 사이버리스크 보험 시장 발전의 장애가 존재함. 따라서 사이버보험 보장의 정의 및 계약 관련 용어 표준화, 통지 및 보안감사 등 사이버보안 관련 제도 개선, 사이버리스크 관련 데이터 공유 시스템의 구축 등이 필요할 것임.

■ 최근 들어 사이버공격으로 인해 기업들이 보유하고 있는 데이터베이스가 유출되는 사건들이 늘어나고 있으며, 피해는 해당 기업뿐만 아니라 데이터베이스에 담겨있는 정보와 관련된 개인들에게도 영향을 주고 있음.

- 사회의 정보통신기술(ICT: Information and Communication Technologies)에 대한 의존성이 심화되면서, 정보시스템에 대한 공격이나 고장으로 인한 피해의 범위도 확대, 심화됨.

■ 이에 본고는 지난 6월 OECD 보험 및 사적연금위원회(IPPC: Insurance and Private Pensions Committee)에서 논의되었던 내용을 중심으로 최근 사이버보험 동향과 사이버리스크 관리 개선을 위해 고려해야 할 사항들을 소개하고자 함.

- 사이버리스크에 대한 기업과 정부의 관심이 늘어나고 있으며, 영국, 미국 등에서는 사이버리스크와 관련된 국가적인 조치가 취해졌음.
  - 영국의 국가안보전략(National Security Strategy)은 사이버공격을 향후 5년 동안 우선순위를 갖고 대처해야 할 네 가지 리스크 중 하나로 지목함.
  - 미국은 2015년 2월에 있었던 사이버보안과 소비자보호 백악관 정상회담(the White House Summit on Cybersecurity and Consumer Protection)에서 사이버보안을 국가 우선순위로 정함.

■ 사이버리스크란 정보기술 체계의 고장으로 인해서 재무적 손실, 파괴, 또는 한 기관의 명성에 손해를 입을 수 있는 모든 리스크라고 정의할 수 있으며, 사이버 손실의 주요 원천은 다음과 같음.

- 재무적, 경제적, 정치적 목적에 의해 의도된 사이버 범죄와 사이버 테러리즘
- 시스템 오류나 고장 등에 의한 자신의 데이터나 다른 사람의 데이터의 돌발적 손실
- 화재, 도난, 자연재해, 전기사고, 산업사고 등으로 인한 시스템 기반구조(Infrastructure)의 물리적 손실
- 웹사이트 또는 이메일이 오해의 소지가 있는 내용이나 불법적인 내용을 포함하는 경우 등과 같이 손해배상 지급을 야기하는 온라인 활동의 배상책임

■ 사이버보험을 제공하는 보험회사의 대부분은 미국과 영국에 있으며, 미국시장이 가장 발전되어 있음.[1)]

- 2002년 1억 달러에 미치지 못했던 미국시장의 사이버보험 수입보험료는 2014년 약 20억 달러로 성장하였으며, 많은 보험회사들이 사이버보험시장에 진입하였음.
- 이에 비해 유럽시장은 수입보험료 수준이 약 1억 5천만 달러로 아직까지 규모는 작으나, 연평균 50~100% 성장률을 보이고 있음.

■ 일반적으로 전통적 보험계약은 사이버리스크 보장을 제외하므로, 사이버리스크에 특화된 사이버보험상품이 개발되어 유통되고 있는데, 일반적 보장내용은 〈표 1〉과 같음.

〈표 1〉 사이버보험계약의 일반적 보장내용

보장	사이버손실의 종류	보장되는 손실
제3자		
사생활 배상책임	● 컴퓨터 네트워크나 오프라인 접속을 통해 부주의, 의도된 행위, 손실, 도난으로 인해서, 해당회사가 집적하거나 관리하고 있던 비밀정보가 공개된 경우	● 법적 배상책임(변호비용, 소송비용 등) ● 대리 배상책임 ● 위기 통제 ● 신용 감시(신용감시, 사기감시 등과 관련된 비용)
네트워크 보안 배상책임	● 의도하지 않은 컴퓨터 바이러스의 삽입이 제 3자의 피해를 가져온 경우 ● 피보험(회사)의 승인되지 않은 접근이 제	● 데이터 회복비용(데이터 및 소프트웨어 복구 또는 구축) ● 법적 소송절차비용

1) Kostadinov(2014), "Cyber Insurance", InfoSec Institute.

	3자의 시스템에 피해를 발생시킨 경우 ● 고객의 승인된 접근에 대한 방해(Disturbance) ● 지적재산의 남용	
지적재산권 및 미디어 유출	● 소프트웨어, 트레이드마크 유출, 미디어 노출	● 법적 배상책임
당사자		
위기관리	● 정보 및 기술자산에 대한 적대적 공격	● 명성을 회복하기위한 전문서비스 비용 ● 이해관계자들에 대한 고지비용 및 감시 비용
조업중단	● 해킹 ● 서비스거부 공격	● 시스템 복귀비용 ● 이윤손실 ● 데이터 복구비용을 위한 보장
데이터자산 보호	● 컴퓨터 공격에 의한 정보 및 데이터 자산의 변경, 오류, 또는 파괴 ● 기타 무형자산의 훼손이나 파괴	● 데이터 복구 또는 교체비용 ● 지적재산 복구 또는 교체비용
사이버강탈	● 정보나 기술자산을 방출하거나 이전하기 위한 강탈 ● 정보나 기술자산을 변경하거나 훼손하거나 파괴하기 위한 강탈 ● 서비스를 방해	● 강탈지불(Extortion Payment)비용 ● 강탈을 회피하기 위한 비용 ● 랜섬(Ransom)비용

자료: Biener et al.(2015), "Insurability of Cyber Risk: an Empirical Anlaysis", Working Papers on Risk management and Insurance No. 151. University of St. Gallen.

■ **사이버보험 보험료 수준은 피보험기관의 규모, 리스크 요인, 선택된 보장범위나 종류, 자기부담금의 규모에 따라 다양한데, 미국시장에서는 100만 달러 보장 당 대기업의 경우 2만 5천 달러에서 5만 달러, 중소형 기업의 경우 만 5천 달러에서 2만 달러의 보험료가 책정된 것으로 조사됨.[2)]**

- 보험회사는 사이버리스크로 인한 잠재적 손실의 불확실성을 관리하기 위해 보장한도를 정하거나 높은 자기부담금을 설정하기도 하는데, 2013년 기준으로 개별 보험회사가 설정한 보장 최대제한은 천만 달러에서 2천만 달러 사이였음.
- 계약에 따라 보험금 지급의 기준이 되는 시점(Trigger Date)을 손실이 발생한 시점으로 정하는 경우와 피보험자로부터 보험지급신청이 이루어진 시점으로 정하는 경우가 있음.

2) Kostadinov(2014).

– 사이버공격은 몇 달 동안 또는 몇 년 동안 발견되지 않는 경우도 있으므로, 보험금 지급의 기준이 되는 시점이 계약의 중요한 요소가 됨.

■ 그러나 손실노출의 예측가능성, 리스크 간의 상관성, 관리가능한 수준의 손실규모, 지불 가능한 보험료 책정 측면 등 보험가능성의 기준으로 판단할 때, 사이버보험 시장이 발전하는 데에 몇 가지 장애요인들이 존재함.[3)]

- 사이버리스크는 새로운 리스크이므로 손실에 대한 충분한 데이터가 축적되어 있지 않으며, 기술발달에 따라 계속 진화하므로 지속적인 연구와 감시가 필요하고, 손실 또한 무형인 경우가 많다는 어려움을 가지고 있음.
- 보험이 가능하기 위해서는 해당 리스크가 무작위로 발생해야 하며 다른 위험과도 독립적이어야 하지만, 사이버리스크는 네트워크와 연결되어 있으므로, 개별 기업 또는 개인과 함께 연결되어 있는 다른 기업, 개인들과 상호 연결되어 있다는 특성을 가짐.
- 사이버리스크 관련 손실의 최대치, 사건 당 평균손실, 손실빈도 등 사이버보안 관련 사건에 대한 과거 데이터가 부족하며, 향후 전망에 대해서도 연구에 따라 매우 다른 예측을 제시하고 있음.
- 잠재적 손실과 확산효과로 인해 사이버리스크를 계량화는 것이 어려우므로, 보험회사들은 안전할증(Safety/Uncertainty Margins)을 확보함으로써 높은 보험료를 부과하는 경향을 보이는데, 높은 보험료는 사이버보험시장의 활성화에 장애가 될 수 있음.

■ 사이버보안을 개선하고 보험을 통해 사이버리스크를 관리하기 위해서는 사이버보험 보장의 정의 및 계약 관련 용어 표준화, 통지 및 보안감사 등 사이버리스크 관련 감독요건 검토, 사이버보안 사고 관련 데이터의 공유 등이 필요할 것임.

■ 먼저 사이버보험의 수요자가 보험계약을 이해하고 보험을 통해 적절한 리스크관리를 할 수 있도록 현존하는 사이버보험계약 보장의 정의와 보험계약에 사용되는 용어를 표준화할 필요가 있음.

- 현재 시장에서 유통되고 있는 사이버보험계약들은 제공하는 보험회사에 따라 보장내용, 보장제외사항, 계약에 사용되는 용어 등이 매우 다름.
- 아울러 사이버보험이 보장하는 사건의 정확한 범위를 이해하기 위해서는 보장하는 리스크와 보험

3) 일반적으로 보험가능성, 즉 어떠한 리스크를 보장하는 보험이 가능하기 위해서는 손실노출(Loss Exposure)이 예측 가능해야 하며, 리스크들이 비교적 상관성이 낮아야 하며, 사건 당 평균 손실과 최고가능 손실이 감당가능하고, 지불 가능한 보험료를 책정할 수 있으며, 이를 뒷받침할 만한 법적 체계가 있어야 함.

금지급을 결정하는 조건(Trigger)에 대한 명확하고 투명한 정의가 필요함.

■ 다음으로 법적으로 정보유출에 대해 알릴 의무를 강제하는 경우, 정보유출사건은 높은 고지비용을 발생시킬 것이므로 기업의 보험가입과 손실 관련 데이터 집적 유인을 높일 것임.

- 미국의 47개 주에서는 개인정보손실을 야기하는 유출을 당국에 알려야 하는 의무와 개인정보와 관련된 보안유출에 대해 잠재적으로 피해가 있을 모든 당사자들에게 이를 알려야 하는 의무가 있음.
- EU는 데이터보호규제(EU Data Protection Regulation) 초안에서 데이터유출로 인해 잠재적으로 위협을 받을 수 있는 모든 당사자들에게 고지할 의무를 담음.
  - 독일의 경우 지역 데이터보호당국에 고지할 의무를 규정하고 있으며, 이를 위반할 경우 최고 300만 유로의 벌금을 부과할 수 있음.

■ 또한 보험회사가 사이버보험 계약자(기업)의 보안도구 및 활동을 평가하는 심화사이버보안검사(In-depth Cyber Security Audits)를 하도록 의무화하는 방안도 고려할 수 있음.

- 보험회사의 언더라이팅, 위험노출 모니터링의 일부로서 보험회사가 의무적으로 계약자의 사이버보안 검사를 실시하도록 할 경우, 계약자의 보험을 통한 위험감소 효과를 더욱 강화시킬 수 있을 것임.
- 이와 함께 보험회사는 보험료 인하와 보장확대 등을 통해 계약자의 사이버리스크 경감 및 회피를 유도할 수 있음.

■ 마지막으로 사이버리스크의 보험가능성에 가장 큰 장애가 되는 데이터 부족 현상을 개선하기 위해, 사이버리스크 관련 데이터 집적과 공유를 위한 데이터 풀(Data Pool)이 구축되어야 할 것임.

- 사이버리스크의 보험가능성에 가장 큰 어려움을 주는 부분이 손실 데이터의 과거시계열 부재, 사이버보안 사고의 빈도 및 심도와 관련된 계리정보의 부족, 사이버위협의 변동성 등이라고 할 수 있음.
- 따라서 사이버위협에 대한 데이터와 지식의 공유는 보험회사가 사이버리스크를 계량화할 수 있는 능력을 개선시킬 것임.
- 올해 2월 미국은 사이버위협정보통합센터(CTIIC: Cyber Threat Intelligence Integration Center)를 설립할 계획임을 밝힌 바 있음. KiRi