KiRi 리포트 2017.5.2.
이슈 분석

사이버보험 시장의 활성화를 위한 정책적 과제

이승준 연구위원

정보통신의 활용도가 높아지면서 사이버리스크로 인한 재무적 손실위험을 전가하는 사이버보험에 대한 인식이 제고되고 있음. 사이버보험 시장 활성화를 가로막는 요인들로는 경험통계 부족, 비독립적리스크, 사이버 손실에 대한 인식 결여, 사이버보험의 복잡성 등이 있음. 따라서 사이버보험 시장 활성화를 위해서는 관련 통계의 표준화 등의 문제를 정부가 주도적으로 해결할 필요가 있음.

요약

■ 스마트폰 사용 등과 같은 정보통신의 활용도가 높아지면서 일상적 활동의 편의성 및 효율성의 증대라는 긍정적인 측면과 함께 이에 동반한 사이버리스크에 대한 우려도 높아지고 있음.

- 세계경제포럼 보고서에 따르면 이미 G7 국가 중 5개 나라에서 사이버리스크를 경제활동 관련 최고 또는 두 번째로 중요한 리스크로 인식하는 것으로 보고되고 있음.[1)]
- OECD 등 국제기구에서는 이미 사이버리스크와 관련된 프로젝트[2)]를 진행하고 있으며 이를 통해 회원국 차원의 리스크 경감 방안과 대책 등 정책적 대안을 논의 중에 있음.

■ 인터넷 등 정보통신기술을 활용하는 과정에서 발생할 수 있는 사이버리스크를 보험을 통해 해결하는 방안에 대한 인식도 높아지고 있어 향후 사이버보험 시장의 확대가 전망됨.

- 본고는 제4차 산업혁명 등 기술발전의 가속화와 함께 높아지는 사이버보험 시장의 중요성을 살펴보고 사이버보험 시장 활성화를 위한 과제와 정책적 시사점을 살펴봄.

■ 사이버리스크는 사이버 공격에 의한 또는 우발적인 정보통신체계의 기능장애로 인해 개인 및 기업의

1) World Economic Forum(2017), "Global Risks Report 2016", 12th Edition.
2) OECD는 디지털경제의 정보보안과 사생활(Security and Privacy in the Digital Economy) 작업반을 통해 사이버리스크와 이에 대한 대책을 담은 프로젝트를 진행 중임.

재무적 손실이나 평판의 저하를 가져오는 리스크로 정의될 수 있음.

- 사이버리스크는 사생활의 침해(privacy breach), 서비스장애(denial of service), 사이버 사기(cyber fraud), 사이버 협박(cyber extortion)과 사이버 공격(cyber attack) 등 다양한 형태로 나타남.

■ 사이버보험은 개인과 기업이 사이버리스크로 인한 재무적 위험 등을 보험시장을 통해 전가할 수 있도록 만들어 주며 이 과정에서 리스크에 대한 이해도가 높아지고 리스크 경감유인이 제공됨.

- 사이버보험을 찾는 과정에서 계약자는 보유한 리스크의 양과 성격을 충분히 인식하게 되고 이를 통해 얼마만큼의 보장이 필요한지 가늠할 수 있게 됨.
- 보험계약 인수과정에서 보험계약자와 보험회사가 계약자의 리스크 관리 정도와 실행 정도를 측정하고 이를 보험계약 내용에 반영하면서 계약자가 리스크를 경감시키는 유인을 제공함.
- 특히 기업이 리스크를 경감시키기 위한 투자와 노력을 하는 만큼 보험료의 감소로 이어지게 됨.

■ 사이버보험 시장은 아직 개발 초기단계로 여겨지고 있으며 단독보험의 형태와 함께 재물보험과 배상책임보험 등과 같은 보험의 특약 형태로도 공급되고 있음.

- 2016년 사이버보험 시장규모는 단독보험 원수보험료 기준으로 약 35억 달러로 추정되며 이 중 미국 보험회사가 30억 달러, 유럽 보험회사는 3억 달러를 각각 인수한 것으로 보고됨.
- 다른 배상책임의 기업 가입률이 100%에 달하는데 비해 사이버보험은 미국에서 모든 기업의 20~35%와 유럽 중대형회사의 20~25%만 가입한 정도에 불과함.

■ 사이버보험 시장 활성화를 가로막는 요인들로는 불충분한 경험통계, 독립적이지 않은 리스크, 사이버 손실에 대한 인식 결여, 사이버보험의 보장위험 및 상품의 복잡성 등이 있음.

- 사이버리스크는 새로운 리스크로 아직 적정 요율 산출을 위한 경험통계가 충분히 집적되지 않았고, 특히 피해사실을 공유하지 않으려는 피해자 성향이 문제를 더욱 악화시킬 수 있음.
- 사이버리스크는 공통적인 소프트웨어 사용이나 네트워크로 연결되어 계약자들 사이의 리스크가 독립적이지 않고 상호 연결되어 있어 사이버보험 인수에서 오는 리스크를 증폭시킴.
- 사생활 침해, 서비스장애 등 사이버리스크에 대한 인식은 높아졌으나 많은 기업에서 사이버리스크로 인한 재무적 손실에 대한 인식은 결여되어 사이버보험 구매로 이어지지 않고 있음.

- 소비자는 단독형이나 특약형 등 사이버보험의 공급형태와 상품별 보장리스크의 차이 등 사이버보험 구매 단계에서의 복잡성과 보험금 청구 시 불확실성 때문에 구매를 망설임.

■ 사이버보험 시장을 통한 사이버리스크 경감과 손실관리가 이루어지기 위해서는 시장 활성화를 위한 정부차원의 정책적 고려도 필요함.

- 우선적으로 사이버보험 시장의 발달을 가로막는 장애물과 간극을 정부와 국제기구 차원에서 인식할 필요가 있는데, 향후 발표될 OECD 정책보고서[3] 등에 이러한 내용이 담길 예정임.

■ 사이버보험 상품개발에 필요한 데이터가 가용하도록 사이버사고로 인한 피해, 특히 개인정보와 같은 소비자 보호와 연관되는 내용에 대한 공시의무를 관련 규제에 반영할 필요가 있음.

- 사이버사고 및 손실의 유형을 표준화하여 관련 보험상품의 개발을 용이하게 만드는 효과
- 정부 등 신뢰할 수 있는 기관에서 관련 데이터를 수집, 관리하고 필요 시 제공
- 사고를 당한 기업과 보험금을 지급한 보험회사가 관련 정보를 공유하도록 하는 유인 또는 요건을 개발

■ 전반적인 사이버리스크 관리 수준을 높이기 위한 정부 차원의 사이버리스크 및 디지털보안 관련 정책은 기업 등 민간 부문의 전사적리스크관리(ERM)와 연계할 필요가 있음.

- 경제사회 번영을 위한 디지털보안리스크 관리에 관한 2015년 OECD 이사회 권고안[4]은 정책적으로 기업에 사이버리스크 노출에 대한 측정 및 관리를 위한 유인을 제공하도록 요구
- 기업지배구조 차원에서 사이버리스크를 넓은 개념의 전사적리스크관리에 통합하여 관리하도록 유도
- 보험감독자를 포함한 사이버보안(cyber security) 담당 정부기관 사이의 적극적인 협력과 정보공유도 사이버리스크의 정부차원 관리에 도움이 될 것으로 기대됨.

■ 정보통신강국인 우리나라도 사이버리스크에 대한 인식의 제고와 함께 사이버보험 시장의 활성화를 통한 사이버리스크 관리에 앞에서 제기된 정부 차원의 정책적 노력을 경주할 필요가 있음.

---

3) OECD 산하 보험 및 사적연금 위원회(IPPC)는 사이버리스크 보험에 관한 프로젝트를 진행 중이며 이에 대한 논의를 담아 보고서로 발간할 예정임.

4) OECD(2015), "2015 OECD Council Recommendation on Digital Security Risk Management for Economic and Social Prosperity".

- 우리나라는 인터넷 보급률 및 속도 등에서 자타가 공인하는 정보통신강국이므로 사이버리스크에 대한 노출도 광범위하고 사이버 공격[5]도 빈번하게 언론에 보도된 바 있음.
- 정부는 우선적으로 사이버보험 활성화의 주된 장애물인 사이버리스크 관련 경험통계의 부족과 표준화 문제 등의 해결을 위해 정책적 노력을 기울일 필요가 있음. KiRi

5) 예를 들어, 지난 3월 초 롯데면세점은 DDOS 공격으로 홈페이지가 마비됨.