KiRi 리포트 2017.4.17.
글로벌 이슈

사이버리스크에 대한 각국 보험감독규제 현황[1)]

채원영 연구원

요약

사이버리스크는 보험회사에 운영리스크로 작용함. 국제보험감독자협의회(IAIS)는 보험회사의 사이버리스크 대응능력 감독과 관련된 보험핵심원칙(ICP)을 제시하였음. IAIS의 조사 결과, 미국, EU, 영국 등의 감독당국은 보험회사의 사이버 복원력 향상을 위한 조치를 취하고 있으며, 각 감독당국이 사이버리스크의 중요성에 대해 인식하는 정도와 대응 수단이 국가마다 다양한 것으로 나타남. 이에 IAIS는 각국 감독당국에 사이버리스크에 대한 이해도를 제고하고 보험산업의 사이버 복원력에 대한 감독 능력을 향상시켜야 한다고 권고함.

■ 보험회사에게 사이버리스크는 사이버 공격 등에 따른 계약자(기업, 개인) 정보 유출, 운영 방해(disruption of operations), 기업 평판 하락 등 운영리스크로 작용함.

- 사이버리스크 관련 운영리스크는 보험회사가 다른 회사의 사이버리스크를 담보함으로써 발생하는 보험리스크(underwriting risk)와 구분됨.

■ 이에 국제보험감독자협의회(IAIS: International Association of Insurance Supervisors)는 보험회사의 사이버 복원력(cyber resilience)[2)]과 관련된 보험핵심원칙(ICP: Insurance Core Principle)[3)]을 제시함.

- 보험회사들은 지배구조(governance) 개선을 통해 사이버 보안 사고를 이해, 예방, 탐지, 대응 및 처리할 수 있는 리스크관리 체계를 갖추어야 함.
  - 또한 사이버 보안 취약성 평가, 시나리오 기반 테스트 등을 실시해야 함.
- ICP 7 기업지배구조(Corporate Governance), ICP 8 리스크관리 및 내부통제(Risk Management and Internal Controls), ICP 9 감독 검사 및 보고(Supervisory Review and Reporting), ICP 19

1) IAIS(2016. 8), "Issues Paper on Cyber Risk to the Insurance Sector", https://www.iaisweb.org/.
2) 사이버 복원력이란 사이버 공격을 예측하고 이를 견딜 수 있으며 피해를 신속하게 복구할 수 있는 능력을 말함; BIS(2015. 11), "Guidance on Cyber Resilience for Financial Market Infrastructures", http://www.bis.org/press/p151124.htm.
3) 보험핵심원칙은 사이버리스크 및 사이버 복원력을 구체적으로 다루지는 않지만, 중요한 리스크 및 관련 내부 통제를 경영진에게 요구함으로써 사이버리스크 및 사이버 복원력과 관련한 일반 원칙을 제공함.

영업행위(Conduct of Business), ICP 21 보험사기 예방 및 근절(Countering Fraud in Insurance) 등이 사이버리스크 감독과 관련 있는 항목임.

- 추가적으로 ICP 16 재무건전성 목적의 전사적 리스크 관리(Enterprise Risk Management for Solvency Purposes), ICP 18 모집종사자(Intermediaries) 등이 관련 있을 수 있음.

■ **IAIS 조사[4] 결과, 미국, EU, 영국 등 주요국은 보험회사의 사이버 복원력 향상을 위한 조치를 취하고 있으나 감독 당국이 사이버리스크의 중요성에 대해 인식하는 정도와 대응 수단이 국가마다 상이한 것으로 나타남.**

- EU-U.S. Insurance Project[5] 운영위원회는 2017년에 사이버리스크 등이 보험회사의 사업 모델에 미치는 영향을 중점적으로 조사하기로 함.[6]
- 미국 보험감독자협의회(NAIC: National Association of Insurance Commissioners)는 2017년 8월까지 「Data security model law」를 완성할 예정임.
  - 동 법안은 2016년 3월 초안이 발표되었으며, 보험회사뿐만 아니라 대리인, 중개인, 기타 이해관계자 등을 대상으로 데이터 보안 및 조사 등에 대한 표준을 제시함.
  - 법안에 따르면 보험회사 등은 개인 정보를 보호하기 위한 관리, 기술 및 물리적 안전장치를 포함한 정보 보안 프로그램을 사용해야 함.
- 유럽보험연금감독청(EIOPA: European Insurance and Occupational Pensions Authority)은 Solvency II에서 사이버리스크와 관련된 운영리스크 식별 프로세스를 문서화하여 감독자에게 제공하도록 하고 있음.
- 영국의 경우 2015년 7월, 건전성감독청(PRA: Prudential Regulation Authority)과 금융감독청(FCA: Financial Conduct Authority)이 금융산업 전반의 사이버리스크 취약성 평가 프레임을 완성하였음.
  - 특히 2015년 8월, PRA는 보험산업에 대해 사이버 복원력을 평가하기 위한 조사를 실시하였으나 명확한 조사결과를 발표하지는 않고 있음.

■ **IAIS는 향후 사이버리스크가 지속적으로 확대될 것으로 전망하며 각국 감독자는 사이버리스크에 대한 이해도를 제고하고 보험산업의 사이버 복원력에 대한 감독 능력을 향상시켜야 한다고 권고함.** KiRi

4) 2015년 1~2월, IAIS의 금융범죄대책반(FCTF: Financial Crime Task Force)이 IAIS 회원국을 대상으로 사이버 범죄와 관련된 조사를 실시하였음; IAIS(2016. 8) 참조.
5) EU-U.S. Insurance Project는 2012년 초 E.C. EIOPA, NAIC와 FIO(Federal Insurance Office, 미연방보험청)가 미국과 EU 간의 사업 기회, 소비자 보호 및 효과적인 감독을 촉진하기 위해 설립한 협의체임.
6) EIOPA(2017. 1. 17), "THE EU - U.S. INSURANCE PROJECT ADDRESSES CYBER RISK", https://eiopa.europa.eu.