사이버위험과 금융안정성

황인창 연구위원

사이버위험(Cyber Risk)은 정보 및 정보 시스템의 기밀성, 가용성, 무결성에 훼손을 가져오는 운영위험을 의미함. 사이버위험과 시스템위험(Systemic Risk) 간 관계에 대한 연구는 초기 단계로 사이버위험이 시스템 위험으로 발전할 수 있는지에 대해 다양한 의견들이 제시되고 있음. 최근 금융기관과 자본시장 인프라에 대한 사이버공격이 잇달아 발생함에 따라 사이버위험은 금융안정성에 주요 위험요소로 인식되기 시작함. 금융산업이 사이버위험에 취약한 주된 이유는 금융기관들의 중요 시장 인프라와 고도로 상호 연결된 네트워크에 대한 의존도가 높기 때문임. 국내 금융산업의 경우, 중앙집권화된 시장 인프라에 대한 의존도가 높고, 기술 의존도도 갈수록 높이질 것으로 예상된다는 점에서 사이버위험의 시스템위험 발전 가능성에 대한 연구와 관련 정책 개발에 관심을 기울일 필요가 있음

요약

- 사이버위험(Cyber Risk)은 정보 및 정보 시스템의 기밀성(Confidentiality), 가용성(Availability), 무결성(Integrity)에 영향을 미치는 정보와 기술 자산에 대한 운영위험으로 정의할 수 있음(Cebula and Young 2010)
  - 기밀성이란 접근이 허가된 자만이 해당 정보에 접근할 수 있도록 보장하는 것으로 공개로부터의 보호를 의미함
  - 가용성이란 승인된 사용자가 필요 시 정보 및 관련 자산에 접근할 수 있도록 보장하는 것으로 파괴 및 지체로부터의 보호를 의미함
  - 무결성이란 정보 및 처리방법의 정확성과 완전성을 보장하는 것으로 변조로부터의 보호를 의미함
- 보험에서 보장하는 위험 유형과 비교해볼 때, 사이버위험은 일반손해보험위험뿐만 아니라 대재해위험, 운영위험의 특성을 모두 가지고 있음(Eling and Wirfs 2016)
  - 사이버위험은 사이버위험에 노출된 대상과 그 대상의 거래상대방인 제3자에게 영향을 미침
  - 사이버위험에 의한 손실은 빈도가 낮고 독립적이지만 심도가 클 수 있음
  - 사이버위험은 사이버공격(Cyber-Attack)과 관계가 없을 수 있는데, 예를 들어 소프트웨어 업그레이드 또는 자연재해는 범죄적 동기는 없지만 영업 중단을 일으켜 사이버위험을 현실화할 수 있음

■ 사이버위험과 시스템위험(Systemic Risk) 간 관계에 대한 연구는 초기 단계로 사이버위험이 시스템위험으로 발전할 수 있는지에 대해 다양한 의견들이 제시됨

- 사이버위험은 대개 개별 기업의 내부 IT 보안 문제로 경제주체들의 행동에 직접적인 영향을 미치지 못하고 시스템위험으로 발전하기 위해서는 너무 많은 조건들이 필요하기 때문에 거시건전성보다 미시건전성과 관련이 높음(Danielsson et al. 2016)
- 반면 사이버위험은 사이버공격과 같이 의도적이고 악의적인 동기에 의해 발생할 수 있기 때문에 경제 전체에 최대한 영향을 주도록 설계될 수 있음(Warren et al. 2018)
  - 예를 들어, 불확실성이 높은 시기에 맞춰 주요 금융기관에 대해 연쇄적으로 사이버공격을 가할 수 있음

■ 하지만 최근 금융기관과 자본시장 인프라에 대한 사이버공격이 잇달아 발생함에 따라 사이버위험은 금융안정성에 주요 위험요소로 인식되기 시작함(IIF 2017; OFR 2017; Bouveret 2018)

- 사이버공격은 정보 보안 측면에서 공격대상기관의 기밀성, 가용성, 무결성에 훼손을 가져오는데, 이에 따라 데이터 유출(Data Breaches), 영업 중단(Business Disruptions), 사기(Fraud)로 구분됨
  - 데이터 유출: 기업이 보유한 개인정보가 제3자에게 공개됨
  - 영업 중단: 시스템 작동이 중단되어 영업활동이 정지되거나 지체됨
  - 사기: 데이터 및 시스템이 승인 없이 변경되어 시스템이 오작동함
- 금융산업은 고객의 신용을 바탕으로 하기 때문에 사이버공격으로 인한 손실이 타 산업에 비해 큰 편이고, 특히 영업 중단의 경우, 단기적 전염효과(Contagion Effects)를 가질 수 있음
- 최근 신흥국뿐만 아니라 선진국 중앙은행에 대한 사이버공격이 발생하고 있으며, 피해액은 1억 1,700만 달러에 달함(〈표 1〉 참고)
  - 사이버공격의 유형별로 살펴보면, 선진국은 데이터 유출과 영업 중단이 대부분을 차지하고, 신흥국은 사기가 대부분을 차지함

〈표 1〉 최근 중앙은행에 대한 사이버공격

기관	연도	공격 유형	세부내용
클리브랜드 연방준비은행	2010	데이터 유출	12.2만 개 신용카드 정보 유출
뉴욕 연방준비은행	2012	데이터 유출	9,500만 달러 상당의 고유 소프트웨어 코드 유출
스웨덴 중앙은행	2012	영업 중단	DDoS 공격으로 인해 5시간 동안 웹사이트 접속 중단
에콰도르 중앙은행	2013	사기	중앙은행에 있는 Riobamba 도시의 계정에서 1,330만 달러 도난
세인트루이스 연방준비은행	2013	데이터 유출	4천 개 미국 은행 임원진들의 개인정보 공개
스위스 중앙은행	2014	사기	68.8만 달러 도난

〈표 1〉 계속

ECB	2014	데이터 유출	2만 개 이메일 주소 및 연락처 유출
노르웨이 중앙은행	2014	영업 중단	7개 대형 금융기관에 대한 DDoS 공격으로 영업 지연
아제르바이잔 중앙은행	2015	데이터 유출	수천 개의 고객 정보 유출
방글라데시 중앙은행	2016	사기	8,100만 달러 불법 송금
러시아 중앙은행	2016	사기	2,200만 달러 손실
이탈리아 중앙은행	2017	데이터 유출	전직 임원들의 이메일 해킹

자료: Bouveret(2018)

■ 금융산업이 사이버위험에 취약한 주된 이유는 금융기관들의 중요 시장 인프라와 고도로 상호 연결된 네트워크에 대한 의존도가 높기 때문임

- 중요 시장 인프라로 지급결제시스템, 증권거래소, 증권예탁원 등이 있으며, 일반적으로 중앙집권화된 시스템을 가짐
- 자본시장 인프라와 대형 금융기관의 영업 중단은 위험 집중과 이러한 인프라에 대한 대체재 부족으로 인해 경제 전체에 심각한 영향을 끼칠 수 있음(Kopp et al. 2017)
  - 예를 들어, 지급결제시스템이 작동하지 않는다면 시장참여자들은 거래에 참여할 수 없게 되어 유동성위험과 파산위험에 노출됨
  - 또한 대형 금융기관의 영업 중단 및 거래 정지는 이러한 기관들의 거래상대방의 유동성위험과 파산위험을 높이게 됨

■ 현재 WEF, OECD 등 국제기구를 중심으로 사이버위험 관리를 위한 정책 수단들에 대한 논의가 시작되고 있음

- WEF(2016)은 사이버위험이 시스템위험으로 발전하지 않도록 관리 수단이 필요하고, 이를 위해 사이버위험에 대한 이해가 선행되어야 한다고 강조함
- OECD(2017)은 사이버위험 관리를 위해 보험의 역할이 강화될 필요가 있다고 주장함

■ 국내 금융산업의 경우, 중앙집권화된 시장 인프라에 대한 의존도가 높고, 기술 의존도도 갈수록 높이질 것으로 예상된다는 점에서 사이버위험의 시스템위험 발전 가능성에 대한 연구와 관련 정책 개발에 관심을 기울일 필요가 있음 KiRi

참고문헌

Bouveret, A.(2018), “Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment”, IMF Working Paper, No. 18/143

Cebula, J. J. and L. R. Young(2010), “A taxonomy of Operational Cyber Security Risks”, Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University

Danielsson, J., M. Fouché and R. Macrae(2016), “Cyber risk as systemic risk”, CEPR Policy Portal

Eling, M. and J. H. Wirfs(2016), “Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class”, Institute of Insurance Economics, University of St. Gallen

Institute of International Finance(2017. 9), “Cyber Security and Financial Stability: How cyber-attacks could materially impact the global financial system”

Kopp, E., L. Kaffenberger and C. Wilson(2017), “Cyber Risk, Market Failures, and Financial Stability”, IMF Working Paper, No. 17/185

Office of Financial Research(2017. 2), “Cybersecurity and Financial Stability: Risks and Resilience”, *OFR Viewpoint*

Organization for Economic Cooperation and Development(2017), “Supporting an Effective Cyber Insurance Market”, OECD Report for the G7 Presidency

Warren, P., K. Kaivanto and D. Prince(2018), “Could a Cyber Attack Cause a Systemic Impact in the Financial Sector?”, Quarterly Bulletin, Bank of England

World Economic Forum(2016), “Understanding Systemic Cyber Risk”, White Paper