2021.11.29

KiRi 리 포 트

포커스

주요국 정부의 사이버보험 공급 지원 동향 및 시사점

송윤아 연구위원, 홍보배 연구원

요 약

○ 사이버사고에 대한 우리나라의 정책적 대응은 주로 사전적 보안강화에 집중해 왔으나, 사이버사고의 경우 방어보다는 공격이 용이하다는 점에서, 사후적 피해회복에 대한 정책적 접근이 불가피함

- 그동안 사후적 피해회복에 대한 정책적 접근은 개인정보유출 및 제3자에 대한 배상책임으로 국한되고, 기업의 재물 및 영업중단손해 등에 대해서는 유의미한 논의가 전개되지 않음
- 테러조직 및 국가 배후 사이버공격이 증가하고 있는 가운데, 그 피해를 민간기업과 보험회사가 온전히 책임지는 것이 정당한지에 대한 문제 제기는 사후적 피해회복 수단으로서 보험 공급에 정부가 적극적으로 개입해야 할 당위성을 제공함

○ 주요국에서는 사후적 피해회복에 대한 정책적 접근이 보험을 통해 이루어지는데, 정부가 일부 사이버공격으로 인한 손해에 대해 재보험 및 유동성을 제공하고 그 범위를 확대하는 것을 검토 중임

- 주요국은 이미 자국에서 운영 중인 공사협력 테러보험 프로그램을 통해 '일부 사이버공격'으로 인한 기업의 재물·영업중단·배상책임손해에 대해 정부가 재보험 및 유동성을 제공하거나 제공여부를 논의 중임
- 다만, 기존의 테러보험 프로그램이 9·11 테러리즘 등 물리적 테러리즘을 계기로 도입되어 사이버공격으로 인한 보장공백을 해소하는 데에는 한계가 있는 바, 프로그램 범위 확대가 논의됨

○ 또한 지속가능한 사이버보험 공급을 위해 데이터 공유·리스크 모델링·전문인력 양성 등 보험공급 인프라 조성을 위한 지원이 논의됨

- 일찍이 OECD와 EIOPA는 사이버보험 시장의 지속가능성을 위해서는 경험데이터와 이에 기반한 리스크 측정이 급선무라 보고, 적극적인 데이터공유와 데이터베이스 구축을 권장함
- 미국의 사이버정책 개발 핵심기구인 CSC는 보안강화를 위한 사이버생태계 재구성 전략의 일환으로, 국토안보부 내 사이버통계국 설치와 사이버리스크 모델링을 위한 공사협력 작업반 구성, 연방정부의 사이버보험 전문인력 및 상품개발 지원 등을 제안함

○ 사이버리스크의 양적·질적 변화에 대응하여 정부는 사전적 보안강화 뿐만 아니라 사후적 피해회복을 위한 정책 방안을 선제적으로 수립해야 함

- 국가 배후 사이버공격, 사이버 대재해 등 보장공백이 예상되는 사이버사고에 대해 정부가 직접 보험을 제공하거나 재보험·지급보증·유동성 제공을 통해 보험회사의 자본력을 제고하는 방안을 고려할 수 있음
- 사이버리스크 모델링을 위해 정부·보안업계·보험업계 간 사이버사고 데이터 공유체계를 마련해야 함

1. 서론

○ 사이버사고의 진화와 함께 사이버리스크에 대한 기업의 보장 수요가 증가한 반면 보험업계의 사이버보험 공급은 신중한 기조를 보이며, 향후 사이버리스크에 대한 기업의 보장공백이 불가피할 것으로 보임[1)]

- 2010년대 들어 ① 사이버사고의 공격자는 개인 또는 범죄조직에서 국가, 준정부조직, 테러조직으로, ② 공격동기는 호기심, 금전, 과시욕에서 정치적, 군사적 동기로, ③ 공격표적은 개인 또는 보안이 취약한 중소기업에서 공급망 및 산업제어시스템 공격을 통한 대기업과 국가기반시설로, ④ 피해유형은 정보유출 및 개인정보침해에서 재물·신체·영업중단손해 등으로, ⑤ 피해심도는 파괴적인 수준으로 확대·진화함
- 사이버사고로 인한 재물·신체·영업중단손해, 물적 손실을 동반하지 않은 영업중단손해, 국가 배후 사이버공격, 사이버 대재해, 그리고 벌금 및 랜섬 담보에 대한 보장공백이 커질 것으로 보임

○ 사이버사고에 대한 정책적 대응은 사전적 보안강화와 사후적 피해회복으로 구분 가능한데, 사이버사고의 경우 방어보다는 공격이 용이하고 국가 배후 사이버공격의 책임에서 정부가 자유롭지 않다는 점에서, 사후적 피해회복 수단으로서 보험 공급에 정부가 적극적으로 개입해야 할 당위성을 가짐

- 사이버사고에 대한 우리나라의 정책적 대응은 주로 사전적 보안강화에 집중해 왔으나, 사이버사고의 경우 방어보다는 공격이 용이하다는 점에서, 보안강화 일변도의 정책 대응으로는 한계가 존재함
  - 피해회복에 대한 정책적 접근은 개인정보보호 관련법 위반에 따른 법률상 손해배상금의 보험가입 의무화 등 개인정보유출과 제3자 배상책임으로 국한되고, 기업의 재물 및 영업활동중단손해 등으로 전개되지 않음[2)]
- 더욱이 테러조직 및 국가 배후 사이버공격이 증가하고 있는 가운데, 그 피해를 민간기업과 보험회사가 온전히 책임지는 것이 정당한지, 국가 배후 사이버공격의 책임에서 정부가 자유로운지에 대한 문제 제기가 가능함

○ 본고에서는 세계 사이버보험 시장을 선도하는 주요국 정부의 사이버보험 공급 지원 동향을 자본 투입과 인프라 조성 측면에서 살펴보고, 우리나라에의 시사점을 도출함

- 정부 차원의 사이버보험 공급 지원은 ① 정부가 보험시장에 자본을 투입하는 방식과, ② 데이터 공유·리스크 모델링·전문인력 양성 등 보험공급 인프라 조성을 지원하는 방식으로 구분 가능함
  - 전자(①)는 정부가 보장공백이 발생한 사이버사고에 대해 직접 보험을 제공하거나 재보험담보·지급보증·유동성 제공을 통해 보험회사의 자본력을 제고하는 방식으로 구체화될 수 있음

1) 사이버보험 시장 변화에 대한 상세는 다음을 참고하기 바람; 송윤아(2021), 『사이버사고의 진화와 사이버보험 시장 동향』, 보험연구원
2) 신용정보의 이용 및 보호에 과한 법률 제43조의3, 전자금융거래법 제9조 제4호, 개인정보보호법 제39조의9 등은 관련 서비스 제공자가 손해배상책임의 이행을 위하여 금융위원회가 정하는 기준에 따라 보험 또는 공제에 가입하거나 준비금을 적립하도록 정함

2. 정부의 사이버보험 시장 내 자본 투입 동향

○ (접근방식) 주요국 정부는 이미 자국에서 운영 중인 공사협력 테러보험 프로그램을 통해 '일부 사이버공격'으로 인한 손해에 대해 재보험담보 및 유동성을 제공하거나 제공여부를 논의 중임

- 미국, 호주를 포함하여 대부분의 유럽 국가에서는 2001년 9·11 테러리즘으로 인해 막대한 손실을 입은 (재)보험회사가 테러담보 제공을 중단하자 정부가 재보험담보 및 유동성을 제공하는 공사협력 테러보험 프로그램을 도입함[3)]
  - 9·11 테러리즘으로 인해 막대한 손실을 입은 (재)보험회사가 기업보험에 테러면책조항을 추가하거나 테러담보 제공을 중단하자, 진행 중이거나 계획되었던 건설 프로젝트, 부동산 거래들이 취소·지연됨
  - 현존 공사협력 테러보험은 물리적 테러리즘을 계기로 도입되어 프로그램 발동조건인 '테러리즘'이 물리적 테러리즘에 부합하게 정의됨(〈표 1〉 참고)
- 2010년대 들어 사이버공격의 빈도 및 심도가 증가하고 사이버공격이 테러조직의 공격수단으로 활용될 가능성이 커짐에 따라, 테러리스트의 사이버공격도 기존 공사협력 테러보험 프로그램의 보장 손인으로 포함시키는 경향을 보임
  - 기존 테러보험 프로그램이 존재하는 상황에서는 사이버사고를 동 프로그램의 손인으로 추가하는 것이 정책적으로 가장 용이한 접근이었을 뿐만 아니라, 사이버리스크에 대응한 공사협력 보험 프로그램을 새로이 구성하기에는 사이버리스크와 사이버보험 시장이 단기간에 급격하게 변함
  - 저자가 살펴본 바로는, 지금까지 사이버리스크에 대응한 별도의 공사협력 보험 프로그램이 존재하지는 않음

○ (미국) 재무부는 2017년부터 테러리스트의 사이버공격으로 인해 발생한 기업의 재물·영업중단·배상책임손해에 대해 보험회사에 비례방식의 재보험담보를 제공함

- 정부는 2002년 대부분의 기업보험에 테러리즘 담보 제공을 의무화하고 테러리즘으로 인한 보험금이 기준금액을 초과하면 보험산업 20%, 정부 80% 비율로 손실을 분담함
  - 전술한 테러위험 보험 프로그램인 TRIP(Terrorism Risk Insurance Program)은 전문가 배상책임보험, 의료과실보험, 보증보험 등에는 적용되지 않음
- 재무부는 2016년 12월, 사이버 배상책임을 보장하는 단독 사이버보험이 TRIP 적용 대상 보험에 포함된다는 지침을 발표함[4)]
  - 사이버배상책임 계통의 보험계약이 별도의 TRIP 적격 보험종목인지, 아니면 TRIP 비적격 보험종목인 전문가 배상책임보험(Professional liability)에 해당하는지를 두고 논쟁이 있었음

○ (영국) 재무부는 2018년 4월부터 테러리스트의 사이버공격으로 인한 재물 및 영업중단손해에 대해 보험회사 출자 상호 재보험사 Pool Re가 재보험담보를 제공하도록 하고 Pool Re에 상환조건부 지급보증을 제공하기로 함

3) 테러보험 공사협력 모형에 대한 상세는 다음을 참고하기 바람; 송윤아·홍보배(2021), 『공사협력 재난보험 프로그램 연구』, 보험연구원
4) U. S. Department of Treasury(2016), "Guidance Concerning Stand-Alone Cyber Liability Insurance Policies Under the Terrorism Risk Insurance Program", Federal Register, Vol. 81, No. 248

- 1990년대 초 12건의 테러리즘이 연속으로 발생, 테러위험에 대한 담보력 제공이 불가능해지자 Pool Re를 설립하여 테러리즘으로 인해 발생한 기업의 재물 및 영업중단손해를 보험회사로부터 수재하도록 하고 정부가 상환조건부로 무제한 지급보증을 제공함[5)]
- 1993년 설립 당시 Pool Re는 화재 및 폭발로 인한 재물 및 영업중단손해만 보장하였으나, 2000년 전쟁과 전자적 리스크를 제외한 모든 사고(Peril)로 인한 손해를 보장하기로 함
- 2018년에는 사이버 테러리즘이 사업장 내 전자기기를 파손하는 등 물적 손해를 동반한다는 점을 감안하여 사이버 트리거로 인한 직접적인 재물 및 영업중단 손해를 보장, 즉 RDI(Remote Digital Interference; 원격디지털장애) 담보를 제공하기로 함
  - 2017년 11월, Pool Re는 향후 3년 내 영국에서 가장 치명적인 피해를 줄 수 있는 공격은 항공기, 철도인프라, 화학반응기, 무기에 대한 사이버공격으로, 이는 모두 물적·인적 피해를 수반한다고 밝힘[6)]

○ **(호주) 재무부는 2018년부터 테러리스트의 사이버공격으로 인한 기업의 재물 및 영업중단손해에 대해 재보험담보 및 지급보증을 제공하는 방안을 심도 있게 검토 중임**

- 재무부는 2003년 산하에 테러리즘 전용 재보험기구, ARPC(Australian Reinsurance Pool Corporation; 호주 재보험풀)를 설립, 보험회사가 인수한 테러위험에 재보험을 제공하고, 100억 호주 달러 한도 내에서 지급을 보증함
  - Terrorism Insurance Act 2003(테러보험법)에 따르면, 총리가 테러리즘을 선언하면, 보험약관상 테러면책 여부에 상관없이, 보험회사는 테러리즘으로 인한 손해를 보장해야 함
- ARPC는 테러리즘으로 인한 기업의 재물·영업중단·배상책임손해를 보장하되, 전쟁, 핵폭발, 방사선 장해, 컴퓨터 범죄로 인해 발생한 손해는 보장하지 않음
- 재무부는 2018년 사이버 테러리즘으로 인한 재물손해에 대해 재보험담보 제공을 검토하였으나,[7)] 동 리스크에 대한 보장공백을 인정하면서도 정부가 개입해야할 만큼의 명확한 시장실패가 존재하지는 않는다고 결론지음[8)]
  - 구체적으로, ① 테러리스트 조직의 사이버공격 역량이 아직 우려할 정도로 파괴적이지 않다는 점, ② 민영 사이버보험 시장이 빠르게 성장하고 있다는 점, ③ 시장에 보장공백이 존재하기는 하지만, 보험회사가 공백을 메우기 위해 적극적으로 인수하고 있는 점에서 당시의 보장공백이 시장실패로 보기는 어렵다고 결론지음
- 2021년 7월 재무부는 ARPC 보장 대상에 물리적 재물 손실을 초래하는 사이버 테러리즘을 포함할 것인지 여부에 대한 자문보고서를 발표하고 이해관계자의 의견을 요청한 상태임[9)]
  - 2020년 12월, ARPC는 사이버공격으로 인한 재물손해는 예상가능한 모든 테러 수법 중 보장공백이 가장 심각한 항목으로 평가함[10)]

---

5) Reinsurance (Act of Terrorism) Act 1993
6) Pool Re & University of Cambridge(2017), "Cyber Terrorism: Assessment of the Threat to Insurance"
7) 호주 테러보험법과 ARPC를 통한 테러리즘 재보험제도는 임시적인 조치로, 3년 주기로 테러담보가 시장에서 자율적으로 공급되기 어려운 상황인지, 그리고 테러리즘 관련 추가적인 보장공백은 없는지를 검토함. 2006년 1차 검토(Triennial review)를 시작으로 2021년 6차 검토를 진행 중이며, 사이버 테러리즘으로 인한 재물손해의 테러보험 적용 여부가 5차, 6차에서 핵심의제로 검토됨
8) Australian Government: The Treasury(2018), "Terrorism Insurance Act Review"
9) Australian Government: The Treasury(2021), "2021 Triennial Review of the Terrorism Insurance Act 2003: Consultation Paper"
10) Australian Reinsurance Pool Corporation and The University of Queensland(2020), "Analysis of Identified Gaps in

○ (한계) 사이버공격은 물리적 테러리즘과 그 성격이 상이한데, 보장공백을 물리적 테러리즘에 초점을 맞춘 기존 테러보험 체계 내에서 해결하려다 보니, 여러 한계에 직면함

- 첫째, 보장공백이 가장 우려되는 국가 배후 사이버공격과 인간 및 시스템 오류에 의한 사이버 대재해는 테러보험 프로그램의 '테러리즘' 정의에 부합하지 않아 프로그램 적용에서 배제될 수 있음
  - 테러보험 프로그램의 발동요건인 '테러리즘'은 비국가행위자(Non-state actor)의 공격을 전제함(〈표 1〉 참고)
- 둘째, 물리적 테러리즘과 달리 사이버공격은 공격자를 특정하고 공격동기를 입증하기 어려워, 문제의 사이버공격이 공사협력 테러보험 프로그램 발동에 부합한 '테러리즘'임을 규정하기 어려움
  - 공격자가 특정되더라도 그러한 행위가 시민 및 정부의 협박으로 작용하는지 여부, 일반적인 사이버범죄인지 협박을 위한 테러리즘 행위인지 여부를 구분하기 쉽지 않음
- 셋째, 문제의 사이버공격이 테러리즘에 해당하는지에 대한 신속한 발표는 피해보상 및 복구에 있어 매우 중요한 사안이나, 사이버공격의 경우 공격자 및 공격동기를 밝히는데 많은 시간이 소요될 수 있음
  - 2017년 5월 12일 150개국 30만개 PC를 감염시킨 워너크라이(WannaCry) 랜섬웨어 공격의 경우 6개월이 지난 12월에 공격자가 공식적으로 확인됨
- 넷째, 미국, 영국, 호주 모두 테러보험 프로그램에서 보험회사의 전쟁면책이 유효하여, 사이버공격이 명백하게 테러리스트에 의한 것이 아니라면 보험회사가 전쟁면책을 들어 보험금 청구를 거절할 수도 있음

○ (추가논의) 사이버공격의 범위와 물리적 테러리즘과의 이질성을 고려하여, 기존 테러보험 체계에 매몰되지 않고 사이버리스크에 대한 보장공백 해소 방안이 검토되고 있음

- 미국 의회는 GAO(Government Accountability Office; 회계감사원)에 연말까지 다음을 검토하도록 함[11)]
  - ① 물리적 또는 디지털 손해를 초래할 수 있는 미국 공공 또는 민간 기반시설에 대한 사이버공격의 잠재적 비용과 취약성, ② 사이버배상책임이 사이버 테러리즘에 대한 적정한 담보인지 여부, ③ 보험산업이 사이버리스크에 대한 요율산출역량이 있는지 여부, ④ 현행 TRIA의 위험보유구조가 사이버 테러리즘에 적합한지 여부임
- 미국 법상 임시기구인 CSC(Cyberspace Solarium Commission; 사이버공간 솔라리움 위원회)는[12)] GAO에 사이버 대재해에 적합한 재보험 프로그램을 검토하도록 하면서,[13)] 사이버보장 확대를 위한 전면적인 변화를 예고함
  - 구체적으로 CSC는 GAO에 다음을 검토하도록 함: ① TRIP이 전쟁면책과 같은 현행 P&C 보험의 면책을 보장할 경우 어떠한 문제가 있는지, ② TRIP이 국가 배후 사이버사고를 보장하기에 충분한지, ③ 테러보험 프로그램 발

Australia's Terrorism Insurance Environment"; 테러리스트의 생화학공격이나 폭발로 인한 건물붕괴, 외로운 공격자(Lone actor) 등으로 인한 재물손해는 원 보험계약과 재보험계약에서 대부분 보장되며, 사이버공격의 재물손해로 인한 영업중단손해와 랜섬웨어로 인한 영업중단손해는, 비록 ARPC 재보험담보에는 포함되지 않지만, 제한적이나마 민영시장에서 거래되고 있기 때문에 사이버공격으로 인한 재물손해보다는 보장공백이 낮다고 봄

11) 2019년 테러보험 재승인법(Terrorism Risk Insurance Program Reauthorization Act of 2019, P.L. 116-94)에 따름

12) 미국은 사이버공격에 대한 방어 전략을 수립하고 공감대를 형성하기 위해, 2019년 국방수권법(National Defense Authorization Act)에 따라 CSC를 설립함. CSC는 국무부, 국방부, 법무부, FBI, 국토안보부, 상무부, 국가정보국 등 국가 핵심기관으로 구성된 임시기구로, 사이버공격에 대한 미국의 전략적 접근방안 개발 업무를 수행함. 2020년 3월 CSC의 80개의 권고사항이 발표된 후 2020년 12월 상원과 하원은 CSC의 권고사항 중 25개(31%)를 국가수권법에 반영하였으며, CSC의 권고안 중 4개는 사이버보험과 밀접한 관련이 있음

13) 상세한 내용은 다음 보고서의 81~83쪽(권고안 4.4.2)을 참고 바람; CSC (2020), "A Warning from Tomorrow". 동 권고안은 National Defense Authorization Act for Fiscal Year 2021 Section 9005.(GAO Study of Cybersecurity Insurance)로 명문화됨

동 기준손해액(2020년 기준 2억 달러)이 재난적 사이버사고에 대해 적절한 규모인지, ④ 어떤 유형의 사이버사고가 TRIP 발동 요건인 '테러리즘 인정행위'에 해당하는지, ⑤ 대부분의 사이버 테러리즘이 TRIP 발동 요건인 '테러리즘 인정행위'에 포함되는지, '테러리즘 인정행위'에 부합하지 않아 TRIP이 적용되지 않는 사이버공격이 어느 정도인지, ⑥ 미국 기업에 대한 사이버공격이 타국 소재 자산에만 피해를 준 경우 TRIP 적용대상인지 여부임

- 호주 ARPC는 2020년 OECD, University of Cambridge와의 공동연구를 통해 재보험담보 제공 범위를 공격자에 상관없이 정치적·종교적·이념적 목적을 가진 악의적 사이버공격으로 확대할 것을 제안함[14)]
  - 동 연구에서는 국가 배후 사이버공격의 경우 원 보험계약의 전쟁면책 적용 가능성으로 인해 보장공백이 존재할 수 있다고 보고, 관련 법규를 개정하여 국가 배후 사이버공격으로 인한 재물 및 영업중단 손해를 테러보험 프로그램의 보장대상에 포함하는 방안을 제시함
- 영국의 경우 테러리즘 수법 및 피해양상 변화에 대한 재무부의 민첩한 대응에 비추어볼 때, 2018년 RDI담보에 이어 향후 추가적인 사이버담보가 공급될 것으로 예상됨
  - 2003년과 2018년에는 각각 핵·방사능·생화학 테러리즘, 사이버 테러리즘으로 인한 손해를 추가 보장하고, 2019년에는 테러리즘 발생 시 사업장 접근금지 등 행정명령으로 인해 영업을 중단해야 하는 경우가 발생함에 따라, 사업장 내 물적 손해를 동반하지 않는 영업중단손해를 보장함

〈표 1〉 공사협력 테러보험 프로그램의 테러리즘 정의

국가	테러리즘 정의	근거
미국	① 폭력적인 행위, 또는 생명, 재물, 주요기반시설에 위험한 행위이어야 하며, ② 미국 내, 항공, 미국 선박, 또는 미국 관할 내 손해를 초래해야 하며, ③ 미국 시민을 협박하거나 협박 또는 강요를 통해 미국정부의 행동 및 정책에 영향을 미치기 위한 노력의 일환으로서 개인 또는 개인들에 의해 행해지는 행위	법률 (Terrorism Risk Insurance Act of 2002)
영국	조직을 위하여 또는 조직과 관련된 개인들이 영국 정부를 전복시키거나 영향을 주기 위하여 사용하는 폭력적 또는 강압적 행위	법률 (Reinsurance (Acts of Terrorism) Act 1993)
호주	정치적, 종교적, 이념적 명분을 이루기 위해 정부 또는 대중을 협박하여 영향을 미치거나 강압하는 행위로서, 타인에 심각한 물리적 피해, 심각한 재물손해, 사망, 인명 위협, 공공의 안전 및 보건 위협, 전자시스템(예를 들어, 정보시스템, 정보통신시스템, 금융시스템, 주요 국가기반시설 시스템 등)의 심각한 방해 및 파괴를 초래하는 행위	법률 (Criminal Code Act 1995 Part 5.3 Section 101.1~101.2)

14) 상세한 내용은 다음을 참고하기 바람; ARPC, OECD and University of Cambridge(2020), "Insurance Risk Assessment of Cyber Terrorism in Australia"; OECD(2020), "Insurance Coverage for Cyber Terrorism in Australia"

3. 정부의 사이버보험 공급 인프라 지원 동향

○ 일찍이 OECD와 EIOPA는 사이버보험 시장의 지속가능성을 위해서는 경험데이터와 이에 기반한 리스크 측정이 급선무라 보고, 적극적인 데이터공유와 데이터베이스 구축을 권장함

- OECD(2017)는 경험데이터 부족, 보험업계의 담보력 부족, 사이버보험 약관의 불명확성을 사이버보험 공급의 도전과제로 꼽았는데, 이중에서도 사이버리스크 측정에 필요한 경험데이터 부족이 가장 심각한 문제로 거론됨[15)]
  - 리스크의 가변성에도 불구하고 자연재해, 감염병, 재래식 전쟁, 물리적 테러리즘 등은 인류가 오랜 기간 경험해왔던 리스크인데 반해, 사이버사고에 대한 경험은 수십 년에 불과하고 기술발전과 함께 리스크 속성도 빠르게 변함
- OECD(2020)는 사이버보험 언더라이팅을 위한 데이터 가용성 제고를 위해 각국 정부에 다음을 제안함[16)]
  - 보험감독당국은 보험회사 간 사이버보험 사고 및 지급에 대한 데이터 공유에 장애가 되는 법규를 제거해야 함[17)]
  - 일부 (재)보험회사가 자발적인 데이터 공유를 꺼릴 경우, 정부는 사고 및 지급 관련 데이터 공유 메커니즘을 도입하고 데이터 개선이 리스크관리, 언더라이팅, 그리고 시장경쟁에 중요하다는 점을 설득해야 함
- EIOPA(European Insurance and Occupational Pensions Authority; 유럽 보험연금청)는 유럽 내 사이버사고 및 사이버보험 지급에 대한 데이터베이스 구축을 제안함[18)]

○ 미국 CSC는 보안강화를 위한 사이버생태계 재구성 전략의 일환으로, 국토안보부 내 사이버통계국 설치와 사이버리스크 모델링을 위한 공사협력 작업반 구성, 사이버보험 전문인력 및 상품개발 지원 등을 제안함[19)]

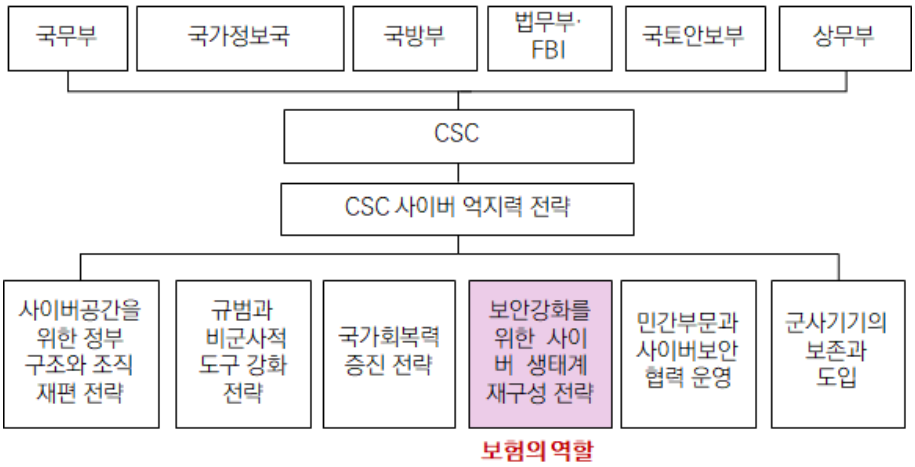
- CSC는 보험산업이 사실상 기업행태의 감독자로 역할하기 위해서는 실제 리스크를 반영한 요율 산출이 전제되어야 하고 정확한 요율 산출을 위해서는 양질의 경험데이터가 있어야 한다고 봄
  - 보험시장이 충분히 효율적이라면 보험료 및 보상한도는 피보험기업의 리스크 수준을 나타내는 지표로서 피보험기업으로 하여금 자발적으로 사이버리스크를 줄이도록, 즉 사이버보안을 강화토록 하는 기제로 작용할 수 있음
- CSC는 정부가 효과적인 사이버보안 정책을 구상하고 보험산업이 보다 정확하게 사이버리스크를 평가할 수 있도록 국토안보부(Department of Homeland Security) 내 사이버 통계국 설치를 제안함(권고안 4.3)
  - 사이버통계국(Bureau of Cyber Statistics)은 사이버보안 사고 대응 조직 또는 사이버보험을 제공하는 조직으로부터 수집된 사이버보험 위협 데이터를 수집, 분석, 공개하는 업무를 수행하며, 보안회사와 보험회사는 사이버통계국에 6개월 주기로 관련 정보를 보고함

---

15) OECD(2017), "Enhancing the Role of Insurance in Cyber Risk Management"
16) OECD(2020), "Enhancing the Availability of Data for Cyber Insurance Underwriting, The Role of Public Policy and Regulation"
17) 최근 미국 손해보험 7개사는 사이버사고에 대한 데이터는 물론 기술 및 노하우 공유를 위해, 공동출자로 CyberAcuView를 설립함. 여기에는 미국 손해보험 상위 6개사가 포함됨
18) EIOPA: European Insurance and Occupational Pensions Austhority(2019), "Cyber Risk For Insurers-Challenges and Opportunities"
19) CSC(2020), "A Warning from Tomorrow"

- 국가안보부 내에 공사협력 작업반을 만들어 보험회사와 리스크 모델링 업체가 사이버 리스크 모델링을 개선할 데이터와 이용 가능한 통계를 공동으로 작업하도록 제안함(권고안 4.4.1)
  - 국토안보부 내에 사이버 통계국을 설치하여 사이버사고에 대한 통계를 구축하고, 국토안보부 내에 보험회사와 리스크모델링 업체로 구성된 작업반을 설치하여 양질의 데이터로 리스크 모델링을 개선할 필요가 있다고 봄
- 사이버보험 전문 언더라이터와 손해사정사 교육 및 인증 프로그램을 개설하고 주정부와 협의하여 사이버보험상품을 개발할 수 있도록 연방정부의 자금 지원을 제안함(권고안 4.4)

〈그림 1〉 미국 CSC의 구성과 사이버 억지력 전략



자료: CSC(2020), "A Warning from Tomorrow"를 참고하여 작성함

4. 시사점

○ 사이버리스크의 양적·질적 변화에 대응하여 정부는 사전적 보안강화뿐만 아니라 사후적 피해회복을 위한 정책방안을 선제적으로 수립해야 함(〈그림 2〉 참고)

- 그동안 우리나라의 사후적 피해회복에 대한 정책적 접근은 개인정보유출 및 제3자에 대한 배상책임으로 국한되고, 기업의 재물 및 영업중단손해 등에 대해서는 어떠한 논의도 이뤄지지 못하였음

○ 구체적으로, 국가 배후 사이버공격, 사이버 대재해 등 보장공백이 예상되는 사이버사고에 대해 정부가 직접 보험을 제공하거나 재보험·지급보증·유동성 제공을 통해 보험회사의 자본력을 제고하는 방안을 고려할 수 있음

- 다만, 보험이 정책수단으로 활용되기 위해서는 효과성뿐만 아니라, 타 정책수단 대비 비용효율성 우위 입증이 선제되어야 함
- 정부가 공급자로서 보험시장에 참여하는 구체적인 방법은 우리나라 보험산업의 인수역량에 따라 달라질 수 있음

- 미국, 영국, 호주 등은 정부가 재보험자 또는 유동성제공자로 시장에 참여하고 보험회사가 정부와 위험을 공동으로 인수하는 파트너로서 기능함

○ 다음으로, 사이버리스크 모델링을 위해 정부·보안업계·보험업계간 사이버사고 데이터 공유 체계를 마련해야 함

• 사이버공격을 받은 피해 기업은 평판손실 또는 행정제재 등을 우려하여 피해 사실의 노출을 꺼려함

〈그림 2〉 사이버리스크에 대한 정책적 대응