KiRi 리 포 트
글로벌 이슈

사이버 전쟁 면책 조항 도입

홍보배 연구원

요 약

국가 배후의 사이버 공격이 보험산업에 있어 중대한 시스템적 리스크로 부상하면서, 사이버 전쟁행위에 대한 보험 적용기준과 관련하여 업계의 시선이 집중됨. 최근, 국가 배후의 사이버 공격에 대해서는 보험의 전통적인 전쟁 면책이 적용되지 않는다는 판결이 선고됨. 이에 따라, 보험시장에서는 전쟁 면책 조항 수정을 통해 국가 배후의 사이버 공격 등에 대한 보장범위를 축소하여 시스템적 리스크를 관리하고자 함

○ 국가 배후의 사이버 공격이 보험산업의 중대한 시스템적 위험요인으로 부상하면서, 사이버 전쟁행위에 대한 보험 적용기준을 둘러싸고 업계의 시선이 집중됨

- 최근 지정학적 리스크가 고조되면서 국가 간 또는 국가 배후의 사이버 공격 및 이로 인한 손실이 증가하고 있음
  - 대표적으로, 2017년 발생한 낫페트야(NotPetya)[1] 공격과 워너크라이(WannaCry) 공격과 같은 국가 간 갈등을 배경으로 하는 대규모 사이버 공격으로 인해 전 세계적으로 다수의 기업이 약 33억 달러 이상의 손해를 경험함[2]
  - 독일 재보험회사인 Munich Re는 2023년에만 약 70여 개국에서 중요한 인프라, 지적 재산 등을 표적으로 삼는 사이버 전쟁이 발생할 수 있다고 예측하기도 함[3]
- 보험회사는 국가 배후의 사이버 공격은 전쟁 행위(Hostile or warlike action)에 해당하기 때문에 보험 약관상 전쟁 면책이 적용된다고 주장하며 보험금 지급을 거절하는 사례가 발생하였고, 이는 많은 분쟁 및 소송으로 이어짐
  - 낫페트야 공격으로 손해를 본 미국의 제과회사 몬델레즈(Mondelez)의 보험금 지급 요청을 전담 보험회사인 취리히 아메리칸 보험(Zurich American Insurance)이 전쟁 면책을 사유로 거절하면서 4년간 소송이 지속되었으나 2022년 비밀리에 합의로 종결된 것으로 알려짐[4]
  - 또한 미국 제약회사인 머크(Merck)는 낫페트야 공격으로 인해 약 14억 달러에 해당하는 손실을 입었으나, 전담 보험회사인 에이스 아메리칸 보험회사(Ace American Insurance)는 전쟁 면책을 이유로 보험금 지급을 거절함[5]

○ 국가 배후의 사이버 공격에 대한 보험의 전쟁 면책 적용과 관련하여, 최근 미국 법원은 국가 배후의 사이버 공격

1) 2017년 낫페트야 사건은 컴퓨터 시스템 파괴 공격의 일종으로, 64개국 이상에서 정부 기관을 비롯해 금융·전력·통신·교통 등 수많은 기반 시설이 운용에 차질을 빚거나 가동이 중단되었으며, 2018년 2월, 미국, 영국, 캐나다, 호주 등 다수의 국가 공동 성명서를 통해 낫페트야 사이버 공격을 러시아 정부 차원의 공격 행위로 발표함
2) Allianz(2019), “Making Noise About “Silent” Cyber”, Global Risk Dialogue Winter/Spring 2019 Edition
3) Munich Re(2023), “Cyber insurance: Risks and trends 2023”
4) Insurance Business(2022. 11. 8), “Zurich, Mondelez Settle Longstanding Lawsuit Over $100 Million Claim”
5) The Wall Street Journal(2023. 5. 2), “Merck’s Insurers On the Hook in $1.4 Billion NotPetya Attack, Court Says”

은 전통적인 재래식 전쟁 면책 조항이 적용될 수 없다고 판결함[6)]

- 지난 2022년 1월, 뉴저지 고등법원(Superior Court of New Jersey)은 머크사와 에이스 아메리칸 보험회사 간 소송에서 머크사의 손을 들어주며 에이스 아메리칸 보험회사에 14억 달러의 보험금을 지급해야 한다고 판결함
  - 판결의 배경으로는 ① 해당 보험은 포괄 위험(All-risk)보험으로, ② 전통적인 전쟁 면책 조항은 물리적인 재래식 군사적 행동(Military action)을 의미하며 사이버 전쟁행위를 포함한다는 명시적인 조항이 없고, ③ 약관(Policy)의 내용이 모호할 때는 작성자 불이익의 원칙에 따라 보험계약자에게 유리하게 판결한다는 원칙 등을 제시함
- 2023년 5월 열린 항소심(New Jersey Appeals Court)에서도 전통적인 전쟁 면책 조항은 사이버 공격에는 적용될 수 없다고 원심의 판결을 그대로 유지함

○ 이에 따라, 사이버 보험 시장에서는 전쟁 면책 조항을 수정함으로써 국가 지원의 대규모 사이버 공격 등에 대한 보장범위를 축소하는 모습임

- 2022년 8월, 세계 최대보험시장인 로이즈 보험 조합(Lloyd's of London)은 전쟁 면책 조항 수정본을 공식 발표하였으며, 이를 2023년 3월부터 신계약 또는 갱신계약 건부터 적용하기로 함[7)]
  - 수정된 전쟁 면책 조항의 주요 내용은 국가의 기능 또는 국가의 보안 능력을 크게 손상시키는 국가 지원의 사이버 공격으로 인해 발생하는 손실은 보험보장에서 제외하는 것임
  - 전쟁 및 국가 지원의 사이버 공격에 따른 직·간접적 손실(Loss, damage) 외에도 배상책임(Liability) 및 관련 비용(Cost, Expense) 등에 대해서도 면책하는 것으로 정함
  - 그리고 이러한 전쟁 면책 조항이 적용되는지에 대한 입증책임은 보험회사에 있음
- 보험회사들은 이러한 로이즈 보험 조합의 전쟁 면책 조항 예시를 참조하여 자사의 보험 약관에 보다 구체적인 사이버 전쟁 면책 조항을 포함할 수 있음

○ 그러나 이와 같은 사이버 전쟁 면책 조항 도입은 사이버 보험의 보장 의미를 다소 희석시킬 수 있다는 우려의 목소리도 있음[8)]

- 보험업계는 전쟁 면책 조항 수정을 통해 국가 지원의 사이버 공격 등에 대한 보장범위를 축소하여 시스템적 리스크를 미연에 방지할 수 있다고 평가함
  - 또한 약관을 통하여 법적 명확성을 제공함에 따라 향후 발생할 수 있는 분쟁을 사전에 방지하는 긍정적인 효과를 가져올 것으로 기대함
- 보장범위가 축소됨에 따라 가입자 측면에서는 사이버 보험 가입 효용 및 보장 의미가 감소할 수 있다는 의견이 있음
  - 전쟁 면책의 입증 책임을 지는 보험회사는 사이버 공격자가 국가임을 입증해야 하나, 사이버 전쟁행위의 정확한 배후를 규명하기 쉽지 않고, 장기간 소요되어 또 다른 비용을 야기할 수 있다는 우려도 큼

---

6) https://www.federalregister.gov/documents/2020/11/12/2020-24591/transparency-in-coverage
7) Lloyd's of London(2022. 8. 16), "State Backed Cyber-Attack Exclusions", Market Bulletin
8) Willis Towers Watson(2023. 6), "War Exclusions in Cyber Policies: the Important Details"