2025.04.21.

KIRI 리포트

사이버 리스크 규제와 세계 보험산업 동향

| 글로벌 이슈 |

강윤지(姜允池) 연구원

요 약

다양한 유형의 사이버 공격이 증가함에 따라 사이버 리스크에 대한 인식도 함께 높아지고 있음. 유럽연합(EU), 미국 등은 사이버 리스크에 대응하기 위해 데이터 보호, AI 보안, 사고 대응 절차를 지속적으로 강화하고 있음. 보험업계도 사이버 보안이 상대적으로 취약한 중소기업을 대상으로 하는 보험상품을 제공하거나 사이버 전쟁 면책조항을 추가하는 등 다각도로 대응하고 있음

○ 랜섬웨어, 데이터 유출, 멀웨어 등 다양한 유형의 사이버 공격이 매년 증가함에 따라 사이버 리스크에 대한 사회, 기업, 개인의 인식도 함께 높아지고 있음

- IBM이 발표한 보고서에 따르면, 사이버 공격으로 인한 기업의 평균 피해액이 2023년 445만 달러에서 2024년 488만 달러로 9.6% 증가했으며, 랜섬웨어 공격 증가, 데이터 유출 사고 증가 등이 주요 원인으로 분석됨[1)]
  - 랜섬웨어 피해액은 2024년 상반기에만 4억 달러를 돌파하였고, 데이터 유출 사고는 2023년 한 해 동안 82억 건 이상 발생하는 등 주요 위협 요소로 지목된 유형의 사이버 공격이 크게 증가하고 있음[2)]
- 보험회사 트래블러스(Travelers)는 사이버 리스크를 미국 기업 경영진이 꼽은 가장 우려되는 요인이라고 발표하였고, 알리안츠(Allianz)는 사이버 리스크를 4년 연속 가장 중요한 비즈니스 리스크 1위로 선정함[3)]
- 개인을 대상으로 한 설문조사에 따르면, 사이버 보험 가입을 고려하고 있다는 응답 비율이 2021년 41%에서 2024년 51%로 증가하는 등 여러 관련 문항에서 사이버 보안에 대한 인식 수준이 높아진 것으로 나타남[4)]

○ 국제연합(UN), 유럽연합(EU), 미국 등은 사이버 리스크에 대응하기 위해 데이터 보호, AI 보안, 사고 대응 절차를 지속적으로 강화하고 있음

- UN은 2024년 12월 국제 사이버 범죄에 관한 협약을 채택하여 사이버 범죄 예방 및 대응을 위한 글로벌 차원의 법적·기술적 조치를 강화하고자 함[5)]
  - 동 협약은 사이버 범죄 대응을 위한 국제 협력을 촉진하고, 개발도상국을 대상으로 한 기술적 지원 및 역량 강화 프로그램 운영을 주요 내용으로 함
- EU는 2018년 일반 데이터 보호 규정을 도입하며 데이터 보호 규제를 강화했으며, AI 시스템의 데이터 요건을 동 규정과 연계하여 강화하는 것을 목표로 하는 AI 법을 2024년 5월에 제정함

1) IBM(2024. 10.), “データ侵害のコストに関する調査 2024”
2) Deloitte(2024. 10.), “Global Cyber Threat Intelligence (CTI): Semi-annual Cyberthreat Trends Report 2024”
3) Reinsurance News(2024. 9. 24.), “Cyber threats top the 2024 Travelers Risk Index, fourth time in six years”; Allianz(2024. 1.), “Allianz Risk Barometer”
4) Munich Re(2024. 9. 7.), “Global Cyber Risk and Insurance Survey 2024: Personal Lines”
5) United Nations(2024. 12. 24.), “UN General Assembly adopts landmark convention on cybercrime”

- 또한 EU는 2024년 10월 "사이버 복원력 법(Cyber Resilience Act)"을 채택하였는데, 동 법안은 디지털 요소가 포함된 제품의 보안 요구사항을 규정하며 IoT 기기, 소프트웨어, 원격 데이터 처리 장비 등을 주요 대상에 포함함[6)]
  - 동 법안은 디지털 제품 공급망의 보안 요건을 강화하고, 공급업체 및 제조업체의 책임을 명확히 하며, 정부와 기업 간 사이버 보안 협력의 확대를 요구함
- 미국은 2023년 12월 기업의 사이버 보안 관련 정보 공개를 의무화하는 새로운 규정을 발표했으며, 2024년 9월에는 AI 개발 및 클라우드 사업자에 대한 보안 규정 강화를 발표하는 등 사이버 리스크에 적극 대응하고 있음
  - 상장 기업은 사이버 공격이 중대하다고 판단할 경우 영업일 기준 4일 이내 공시해야 하며 연차 보고서에 사이버 보안 전략 등 관련 정보를 공개해야 함

○ **보험업계는 사이버 보안이 상대적으로 취약한 중소기업을 대상으로 저렴한 보험상품을 제공하거나 사이버 리스크 관리 교육을 실시하고, 사이버 전쟁 면책조항을 추가하는 등 다각도로 대응하고 있음**

- 영국 보험회사 아비바(Aviva)는 2023년에 사이버 보험 'Aviva Cyber Respond'를 출시했으며, 중소기업을 대상으로 사이버 리스크 관리 교육 프로그램을 운영하여 보안 대응 및 위험 평가 방법 등을 안내하고 있음[7)]
  - 동 보험은 연간 50파운드의 저렴한 보험료로 제공되며, 데이터 보호 및 신용 모니터링 서비스, 24시간 대응팀과 IT 전문가 지원 서비스도 포함됨
- 악사(AXA) XL은 사이버 보험 'Cyber Risk connect Policy'에 AI 트레이닝 데이터 유출, 지식재산권 침해 보상 등을 포함하는 AI 관련 사고 보상을 추가함[8)]
- 사이버 공격에 전통적인 전쟁 면책조항을 적용하는 것에 대한 법적 논란이 일어나자, 주요 재보험사들은 사이버 전쟁 면책조항을 추가해 국가 연계 사이버 공격에 대한 보험 적용 여부를 엄격히 관리하고 있음
  - 미국에서 보험회사가 전쟁 면책조항을 이유로 사이버 공격 피해에 대한 보험금 지급을 거부해 소송이 제기되었는데, 대법원은 면책조항이 사이버 공격에 적용되지 않는다는 등의 이유로 보험회사에 패소 판결을 내림[9)]
  - 로이드(Lloyd's)는 전쟁 면책조항을 사이버 전쟁 유형별로 구분하여 국가 연계 사이버 공격도 면책조항에 포함함

○ **사이버 보험시장은 빠르게 성장하고 있으며, 특히 IT가 발달한 아시아 지역은 미래 성장 가능성이 높은 시장으로 평가받고 있어 국내 보험산업도 사이버 리스크 평가 및 대응 방안을 지속적으로 개선할 필요가 있음**

- 전 세계 사이버 보험시장은 2017년부터 2022년까지 연평균 32%의 성장률을 기록했으며, 향후 몇 년간도 계속해서 연평균 두 자릿수의 성장률이 전망됨[10)]
- 아시아 지역은 전 세계 사이버 공격의 23%를 차지하는 반면 사이버 보험시장은 전 세계 시장의 약 7%를 차지해 낮은 보험침투율을 보이며, 상대적으로 향후 성장잠재력이 큰 것으로 평가됨

---

6) EU(2024. 10. 10.), "Cyber resilience act: Council adopts new law on security requirements for digital products"
7) Insurance Business(2023. 10. 25.), "Aviva to roll out cyber product for UK micro-SMEs"
8) Insurance Business(2024. 10. 22.), "AXA XL launches insurance coverage for Gen AI risks"
9) 2017년 낫페트야(NotPetya) 공격으로 제약회사 머크(Merck)가 대규모 피해를 입고 보험회사 Ace American에 14억 달러의 보상을 요청했으며, 보험회사가 보험금 지급을 거부하자 2019년에 소송을 제기, 2022년 뉴저지 대법원이 보험금 지급 판결을 내린 사건임
10) Swiss Re(2024. 11.), "Reality check on the future of the cyber insurance market"