KiRi 리 포 트
글로벌 이슈

미국, 사이버보험 동향 및 과제

김성균 연구원

요 약

미국 내 데이터 침해 건수 및 데이터 침해 관련 평균 비용 모두 증가 추세에 있으며, 사이버 보안 리스크가 빠르게 확산되고 있음. 이에 대응하여 미국 내 사이버보험시장은 지난 7년간 괄목할 만한 성장세를 보이고 있으며, 최근에는 사이버보험시장 내 손해율 또한 개선되고 있음. 다만, 사이버보험시장의 추가적인 성장을 위해서는 보장내용, 재보험 측면에서 남아있는 과제를 해결해야 할 필요가 있음

○ 미국 내 데이터 침해 건수 및 데이터 침해 관련 평균 비용 모두 증가 추세에 있으며(〈그림 1〉, 〈그림 2〉 참조), 사이버 보안 리스크(Cybersecurity risk)가 빠르게 확산되고 있음[1)]

- 다만, 침해 영향 추정 피해자 수는 감소 추세에 있는데(〈그림 1〉 참조), Identity Theft Resource Center(이하 'ITRC')는 이를 특정 정보 및 신원 관련 사기에 초점을 맞춘 조직화된 범죄의 결과로 보고 있음
  - ITRC는 미국 내 유일하게 무료로 신원 범죄에 대한 조언과 피해자 지원을 실시간으로 제공하는 비영리기관임
- 데이터 침해는 주로 사이버 공격을 통해 발생하며, 사이버 공격의 주요 사례에는 ① 침입 시도(Intrusion attempts), ② 멀웨어(Malware), ③ 랜섬웨어(Ransomware), ④ 크립토재킹(Cryptojacking)이 있음[2)3)]

○ 이에 대응하여 미국 내 사이버보험시장은 지난 7년간 괄목할 만한 성장세를 보이고 있으며, 최근에는 사이버보험시장 내 손해율 또한 개선되고 있음[4)]

- 지난 7년간 미국 내 사이버보험시장은 원수보험료 기준으로 상품 형태별로 보나, 사업체 형태로 보나 두드러지게 성장하고 있음(〈그림 3〉, 〈그림 4〉 참조)
  - 전미보험감독자협의회(이하 'NAIC')는 사이버보험을 상품 형태 측면에서 독립형(Standalone) 상품과 패키지(Package) 상품으로, 판매하고 있는 사업체 형태 측면에서는 국내 보험자와 해외 보험자로 구분하고 있음[5)]
- NAIC의 보고서에 따르면 상위 20개 사의 평균 손해율은 2018년 35.3%에서 꾸준히 증가하여 2019년 44.6%, 2020년 66.9%를 기록하였으나, 2021년(66.4%)부터는 감소하기 시작하여 2022년에는 44.6%까지 개선됨

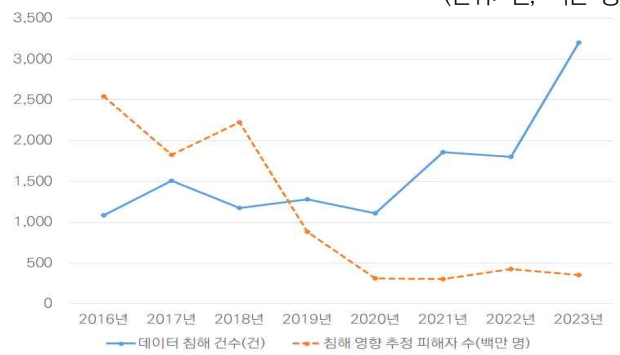
1) 사이버 보안 리스크는 대개 조직에 대한 사이버 공격 혹은 데이터 유출로 인한 노출 및 손실 가능성으로 정의됨
2) ITRC(2024), "2023 Data Breach Report"; SonicWall(2024), "2024 SonicWall Cyber Threat Report"를 참고함
3) 침입 시도는 컴퓨터 등에 무단으로 침입해 사용자의 정보에 접근하여 정보를 조작하거나 신뢰·이용할 수 없게 만드는 행위를, 멀웨어는 사용자의 동의 없이 컴퓨터 등에 설치되어 유해한 행동을 하는 악성 소프트웨어를, 랜섬웨어는 일정 금액을 지불할 때까지 컴퓨터 등에 대한 접근을 차단하도록 설계된 악성 소프트웨어를, 크립토재킹이란 사용자의 의지에 반하거나 동의 없이 암호화폐를 채굴하는 행위를 의미함
4) NAIC는 매년 해외 보험자를 제외한 상위 20개 사의 평균 손해율 통계를 제공하며, 손해율 계산 시 방어 및 비용절감 비용을 포함함
5) 사업체 형태 중 국내 보험자는 미국 내 승인된 보험회사와 국내 잉여 라인 보험자(Surplus line insurer)로 구성되며, 해외 보험자는 해외 잉여 라인 보험자를 의미함

○ 다만, 사이버보험시장의 추가적인 성장을 위해서는 보장내용, 재보험 측면에서 남아있는 과제를 해결해야 할 필요가 있음

- NAIC는 최근 사이버보험시장 내 손해율 개선을 보다 엄격해진 보험계약(약관 강화 및 언더라이팅 정교화 등)에서 기인한 것으로 보고 있음
  - 일부 보험회사들은 시스템 리스크(Systemic risk)를 우려하여 대규모 공격 등으로 발생하는 청구에 대해 제외 사항을 도입하고 보장한도를 낮추는 등 약관을 강화하고 있음[6][7]
  - 또한, 보험회사들은 언더라이팅 시의 질문 사항 및 보험 보장을 위해 피보험자가 갖춰야 하는 보안 요구 사항을 늘리는 방식으로 언더라이팅을 정교화하고 있음
- S&P Global에 따르면 2022년 기준 사이버보험을 취급하는 원수보험회사들은 절반 이상의 리스크를 재보험회사에 양도하였으며, 원수보험회사와 달리 재보험회사의 손해율은 100%를 상회하며 낮은 수익성을 기록하였음

〈그림 1〉 데이터 침해 건수 및 침해 영향 추정 피해자 수 추이

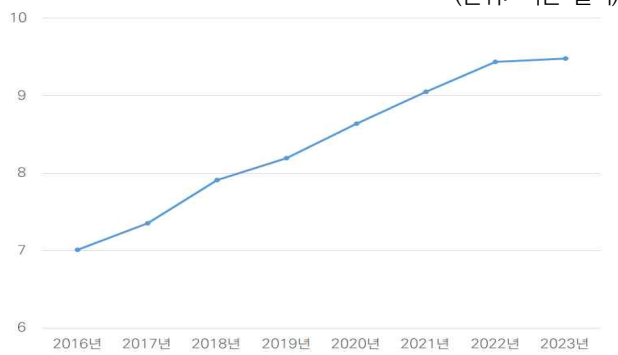
(단위: 건, 백만 명)



주: 두 그래프는 각 단위에 맞춰 세로축을 공유함
자료: ITRC(2024), "2023 Data Breach Report"

〈그림 2〉 데이터 침해 관련 평균 비용 추이

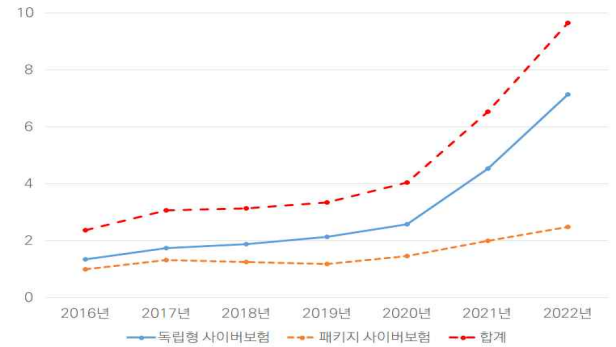
(단위: 백만 달러)



자료: Ponemon Institute and IBM Security(https://www.ibm.com/reports/data-breach); Statista(https://www.statista.com/statistics/273575/us-average-cost-incurred-by-a-data-breach/)

〈그림 3〉 독립형 및 패키지 사이버보험 원수보험료 추이

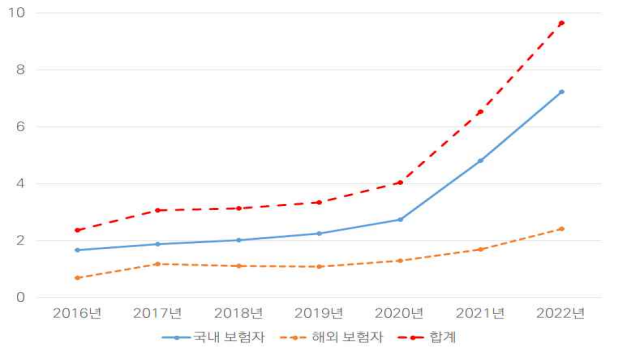
(단위: 십억 달러)



자료: NAIC(2022), "Report on the Cyber Insurance Market"; NAIC(2023), "Report on the Cybersecurity Insurance Market"

〈그림 4〉 국내 및 해외 보험자 사이버보험 원수보험료 추이

(단위: 십억 달러)



자료: NAIC(2022), "Report on the Cyber Insurance Market"; NAIC(2023), "Report on the Cybersecurity Insurance Market"

6) 한국ESG기준원(2019), 「시스템리스크의 기업집단에 적용」은 시스템 리스크를 개별기업의 리스크가 기업 간의 네트워크에 의해 혹은 개별 국가의 리스크가 상호 연결된 국가 간에 전이되고 확대되는 가능성으로 정의하고 있음

7) 예를 들어, 러시아·우크라이나 전쟁과 관련하여 발생하는 사이버 테러에 대해 보험 보장을 제외함