



요약

사이버 리스크는 사회 전반에 걸쳐 급속히 확산하고 있는데, 리스크의 특성이 지속적으로 변화하고 있고 피해 규모가 대규모화되는 추세임. 사이버보험의 성장에도 불구하고 사이버 리스크 보장 격차는 큰 것으로 조사되고 있음. 국내에서는 보험의 보장범위, 면책사항 및 제공 서비스에서 보험회사별로 차이가 있으며, 사이버 리스크 및 피해에 대한 기준이 명확하지 않은 실정임. 보장 격차 해소를 위해서는 사이버 리스크 평가 모형 발전 및 사전적 손실통제 서비스 제공 확대와 함께 기업의 인식 제고가 필요함

○ 사이버 리스크는 사회 전반에 걸쳐 급속히 확산하고 있으며, 중요성과 관심도 증가하고 있음

- 세계경제포럼(WEF)은 사이버공간의 변화를 촉진하는 대표적인 변화로 유비쿼터스 연결성(Ubiquitous connectivity), 인공지능(AI), 양자 컴퓨팅(Quantum computing), 디지털 ID(Digital Identity)를 제시하고, 각각에 대해 주요 미래 사이버 위협을 전망한 바 있음¹⁾
- 세계경제포럼(WEF)은 사이버 범죄와 사이버 보안 취약 문제의 확산을 글로벌 10대 리스크 중 하나로 평가하고 있음²⁾
 - WEF는 Global Risks Perception Survey(GRPS)를 통해 주요 글로벌 리스크를 5개 분야(경제, 환경, 지정학, 사회, 기술)로 구분하여 발표하였는데, 사이버 리스크는 기술 분야에서 유일하게 언급된 10대 리스크 항목임

○ 사이버 리스크의 특성은 지속적으로 변화하고 있어 대응이 쉽지 않으며, 국가 간 갈등·분쟁을 배경으로 사이버 공격이 발생하기도 함

- 사이버 공격의 형태와 대상은 변화하고 있는데, 최근에는 랜섬웨어 공격과 그 피해 규모가 급격히 증가하고 있음³⁾
 - 사이버 범죄 대상은 보안이 비교적 취약한 중소기업을 대상으로 하는 경우가 많으며, 헬스케어, 금융서비스 등의 중요 산업에서는 디지털화로 인해 공급망 전체에서 사이버 취약성이 증가하였음
- 최근 사이버 범죄는 대규모화되고 있으며, 국가 간 갈등이나 분쟁을 배경으로 발생하는 사이버 공격도 있음
 - 반서방 국가들의 친서방 국가 및 기관을 상대로 한 사이버 공격, 또는 북한 해커집단의 타 국가 금융기관을 상대로 한 사이버 금융 탈취 사건들이 빈번히 발생하고 있음⁴⁾
 - 우크라이나 전력망 공격(2015년)과 NotPetya 공격(2017년)은 러시아가 우크라이나를 상대로 벌인 사이버 공격임

1) World Economic Forum(2020), "Future Series: Cybersecurity, emerging technology and systemic risk"

2) World Economic Forum(2023), "The Global Risks Report 2023", 18th edition

3) Swiss Re Institute(2022), "Cyber insurance: strengthening resilience for the digital transformation"

4) McAfee(2020), "The Hidden Costs of Cybercrime"

○ 사이버 리스크 증가와 함께 사이버보험시장도 성장하고 있지만, 사이버 리스크의 보장 격차(Protection gap)와 보험가입의 지역적 편차는 큰 것으로 나타남

- 글로벌시장에서 사이버보험의 수입보험료는 매년 증가(2020년 70억 USD→2021년 100억 USD→2022년 130억 USD)하고 있으며, 2025년에는 230억 USD에 이를 것으로 예측됨⁵⁾
 - 미국시장에서 사이버보험 수입보험료는 2021년 65억 USD로, 2015년 이후 연평균 30% 성장하고 있음⁶⁾
- 사이버보험시장의 성장에도 불구하고, 사이버 리스크로 인한 손실에 비하면 보장 공백은 매우 큰 것으로 추정됨
 - McAfee에 의하면 2020년 사이버 범죄로 인한 금전적 손실은 약 9,450억 USD로 추정됨⁷⁾
 - McKinsey 런던 사무소의 파트너인 James Polyblank는 이를 근거로 2020년 기준 사이버 리스크의 보장 격차(Protection gap)는 99% 이상으로 추정된다고 언급한 바 있음⁸⁾
 - Cybersecurity Ventures는 2021년 사이버 범죄 피해가 6조 USD에 이른다고 추정하였으며,⁹⁾ 세계경제포럼은 이 추정치를 인용한 바 있는데,¹⁰⁾ 이를 반영할 경우 보장 격차는 훨씬 더 커지게 됨
- 사이버보험시장도 미주와 유럽에 편중되어 있어, 지역적 편차도 심한 것으로 조사됨¹¹⁾
 - 세계보험감독관협회(IAIS)가 발표한 2021년 글로벌 사이버보험 원수보험료 총액은 137억 USD인데, 미주 대륙이 전체 원수보험료의 71%(97억 USD), 유럽과 아프리카는 29%(39억 USD)를 차지하고 있음
 - 아시아·오세아니아 지역은 1% 미만(5,562만 USD)을 차지하고 있어, 경제 규모 등에 비해 보험 가입이 매우 저조한 것으로 나타남

○ 국내에서 기업의 사이버 위험을 보장하는 사이버보험의 보장내용은 표면적으로는 보험회사별로 큰 차이가 없어 보이지만, 세부적인 보장범위 및 면책사항, 사전적 리스크관리 서비스 제공 측면에서 차이가 있음

- 기업성 사이버보험은 의무보험과 임의보험으로 구분할 수 있음
 - 의무보험은 관련 법령에서 기업의 배상책임을 담보하기 위해 가입을 요구하는 보험으로 회사별 상품 차이가 없음¹²⁾
 - 임의보험은 기업의 재산손실, 영업손실 등을 추가로 보상하는 보험으로 회사별 차이가 있으며,¹³⁾ 제3자에 대한 배상책임뿐만 아니라 기업의 직접적인 재무적 손실을 보장하고 있음
- 임의보험(사이버 종합보험)의 보장 항목은 보험회사 간에 큰 차이는 없어 보이지만, 보장범위 및 면책사항 등에서 일부 차이가 있고, 위험관리 컨설팅과 같은 포괄적인 서비스 제공에 차이가 있음
 - 국내에서 판매되는 사이버 종합보험과 해외 재보험회사가 제공하는 사이버보험은 보장 항목에서는 큰 차이가 없음

5) Swiss Re Institute(2022), "Cyber insurance: strengthening resilience for the digital transformation"

6) NAIC(2022), "Report on the Cyber Insurance Market"

7) McAfee(2020), "The Hidden Costs of Cybercrime"

8) McKinsey(2023), "What's ahead for commercial property and casualty insurance", McKinsey Podcast

9) Steve Morgan(2020), "Cybercrime To Cost The World \$10.5 Trillion Annually By 2025", *Cybercrime Magazine*

10) World Economic Forum(2020), "The Global Risks Report 2020"

11) IAIS(2023), "Global Insurance Market Report: Special Topic Edition on Cyber"

12) 의무보험은 ① 개인정보보호 배상책임보험, ② e-Biz 배상책임보험, ③ 전자금융거래 배상책임보험이 있음

13) 개인의 사이버 피해에 대한 관심이 커지면서, 일부 보험회사들은 가계성 사이버보험을 판매하고 있는데, 피싱·해킹으로 인한 피해, 인터넷 직거래·쇼핑몰 사기 피해, 온라인 활동 중 배상책임 및 법률 비용이 주요 보장 대상임

- 그러나 일부 보험회사는 제3자 배상책임의 범위를 정보 유출 및 보안 실패로 인한 배상책임에 한정하거나, 프로그래밍 에러로 인한 손실을 면책사항으로 하는 등 세부 항목에서 차이가 있기도 함
- 또한 일부 보험회사는 사고 발생 후 보상에 중점을 두고 있어, 사이버 리스크 솔루션을 제공하는 등 사전적인 리스크관리를 병행하는 보험회사에 비해 사이버 리스크관리에 한계가 있을 것으로 보임

○ 국내 사이버 피해액과 보험가입 상황을 비교하면 글로벌시장처럼 사이버 리스크 보장 격차는 여전히 큰 상황인데, 사이버 리스크 및 피해에 대한 기준이 명확하지 않고 기업의 사이버 리스크에 대한 인식이 부족한 실정임

- 사이버 피해 규모 추정은 방법에 따라 큰 차이를 보이고 있어, 신뢰할만한 사이버 피해 측정 기준이 없다고 판단됨
 - 한국정보통신보안윤리학회는 2020년 국내 사이버 피해액을 1.7조 원(기업 6,956억 원, 개인 9,834억 원)으로 추정하였으나,¹⁴⁾ 미래창조과학부는 2015년 경제적 피해 규모를 연간 3.6조 원으로 추정한 바 있음¹⁵⁾
- 우리나라 사이버보험시장 규모는 공식적으로 집계되고 있지 않으나, 연간 수입보험료가 5백억 원 수준으로 추정됨
 - 과거 금융당국의 조사로 2016년 국내 보험회사의 사이버보험 수입보험료가 358억 원으로 집계된 적이 있으나, 이후에는 여러 실무보고서에서 연간 500억 원으로 추정되었을 뿐 정확한 규모는 확인되고 있지 않음
 - 보험회사마다 사이버보험 분류 기준도 상이한 것으로 확인되고 있음¹⁶⁾
- 기업들은 사이버 리스크에 대한 인식이 부족하고, 사이버 보안 수준을 과신하는 경향이 있음
 - 사이버종합보험은 일부 대기업 중심으로 가입되고 있어 중소기업의 보장 격차는 더 클 것으로 예상되며, 사이버 사고를 당했다는 사실이 알려지면 평판을 해칠 수 있다는 우려 때문에, 보험 가입을 꺼리는 기업도 있음
- 낮은 가입률과 역선택 증가로 인한 보험회사의 사이버 리스크 인수에 대한 부담 증가는 보험료 인상 요인이 되고, 보험가입이 줄어드는 악순환이 발생할 수 있음

○ 국내외를 망라하여 사이버 리스크 보장 격차를 해소하기 위해서는 보험회사의 사이버 리스크 평가 모형 발전 및 사전적 손실통제 서비스 제공 확대가 필요하며, 기업은 사이버 리스크에 대한 인식을 제고할 필요가 있음

- 사이버 사고는 빈도가 낮은 대신 심도가 커서 보험료 산출 시 리스크 마진을 높게 산정할 수밖에 없으며, 사이버 사고 데이터가 부족하고 사이버 리스크 평가 모델도 표준화되어 있지 않아, 보험료를 낮추는 것이 어려움
- 따라서 보험회사는 보장 격차 해소를 위해서, 리스크 평가 모형과 손실통제 서비스에 투자를 확대할 필요가 있음
 - 리스크 평가가 정교해지고 표준화되면 기업의 다양한 사이버 리스크를 더 정교하게 측정할 수 있어 보험료 인하는 가능하므로, 보험회사는 사이버 리스크 측정 모델에 투자를 늘리는 등 다양한 노력을 기울일 필요가 있음
 - 보안강화 서비스 및 사이버 리스크 대응 컨설팅 등 사전적인 손실통제 서비스 확대는 기업의 사이버 리스크에 대한 인식 제고와 함께 사이버보험시장 확대에 기여할 수 있는데, 특히 소기업에 대한 손실통제 서비스 확대는 체계적인 사이버 리스크 관리로 이어질 수 있을 것으로 기대됨

14) 한국정보통신보안윤리학회(2021), 「사이버 침해사고의 경제·사회적 비용 추정 연구」, 『한국 인터넷진흥원 연구용역 보고서』; 기업은 랜섬웨어 침해사고(74.3%), 개인은 악성코드(42.1%) 피해가 가장 큰 비중을 차지함

15) 미래창조과학부(2015), 「K-ICT 시큐리티 발전전략」

16) 예를 들어 개인정보보호 배상책임보험은 개인정보보호법에서 요구하는 의무보험으로 대부분 사이버보험으로 분류하지만, 보장범위가 사이버 리스크만 포함하고 있지 않으므로 일부 보험회사는 사이버보험으로 분류하지 않기도 함