

요약

- 코로나19 이후 디지털 전환 가속과 LLM 기반 사이버 공격 확대로 산업 전반에서 사이버 리스크 노출도가 크게 증가함
- 최근 발생한 대규모 개인정보 유출 사고는 정보통신·디지털 플랫폼 등 사실상 '사회 인프라적 지위'를 가진 기업의 보안 실패가 전 산업·금융·사회로 확산되는 새로운 '시스템적 사이버 리스크'임을 보여줌
- 특히 빅테크·대형 디지털 플랫폼은 시스템적으로 중요한 기술의 성격을 가지므로, 이들의 정보보안 실패는 금융시스템의 시스템 리스크와 유사한 구조적 충격을 초래할 수 있음
- 사이버 리스크의 시스템적 특성은 전 세계적으로 사이버보험 수요를 확대시켰지만, 누적위험 증가·국가 지원 공격 등으로 인해 보험산업의 인수(Underwriting) 역량은 저해되고 있음
- 한국의 경우 개인정보 유출 과징금은 큰 반면 배상책임액이 매우 낮아 기업의 민사 리스크가 제한적이므로, 사이버보험 가입 유인이 충분히 형성되지 않는 구조적 문제가 존재함
- 시스템적 사이버 리스크에 대응하기 위해 기업은 전사적 리스크 관리체계 강화, 보험회사는 보안·언더라이팅 전문성 확보, 정부는 공시·징벌적 배상·공사협력 보험 프로그램 등 정책 기반 구축이 필수적임
- 금융당국은 극단적 사이버 사고 시나리오를 기반으로 '사이버 리스크 스트레스 테스트'를 도입하여, 금융기관의 시스템적 취약성을 평가할 뿐만 아니라 빅테크·플랫폼의 사이버 사고가 금융 안정성에 미치는 충격을 정량적으로 관리할 필요가 있음

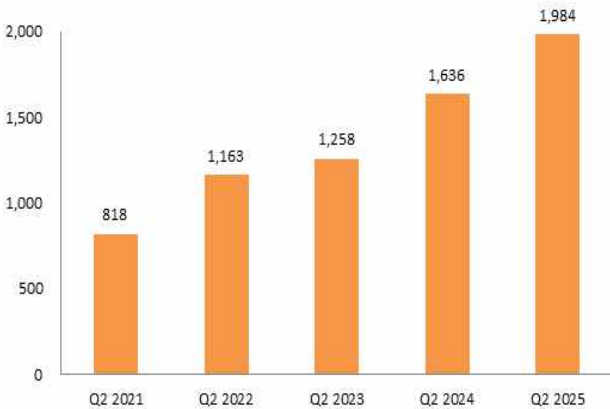
1. 서론

○ 코로나19 팬데믹(Pandemic)과 ChatGPT로 대표되는 거대언어모델(Large Language Model; LLM)의 등장은 글로벌 산업 전반에서 사이버 리스크 노출을 급격히 증가시키고 있음

- 팬데믹으로 인해 사회 전반에서의 비대면 활동 증가와 디지털 전환은 사이버 환경으로의 노출을 증가시키고, 사회 주요 인프라로의 공격을 확대함
- LLM을 통한 악성코드 생성 및 침해, 디지털 위·변조 확대 등 다양한 유형의 사이버 공격이 관찰되고 있음
- 실제로 주당 사이버 공격빈도는 코로나19 이후 꾸준히 증가하고 있으며(〈그림 1〉 참조), 대형 사이버 사고 보고 건수 또한 증가하고 있음(〈그림 2〉 참조)

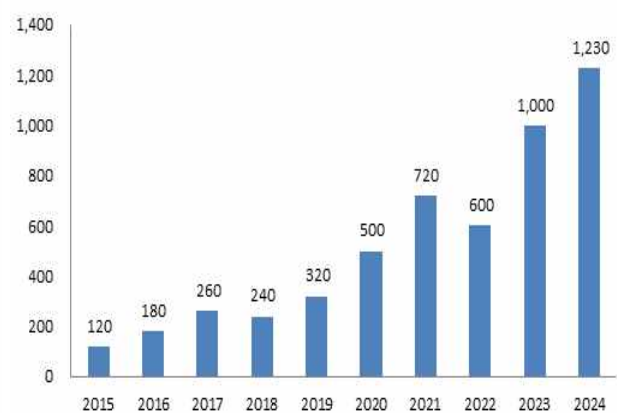
〈그림 1〉 주당 사이버 공격빈도

(단위: 건수)



〈그림 2〉 대형 사이버 사고 보고건수

(단위: 건수)



자료: World Economic Forum(2025. 9. 30.), "Cybersecurity Awareness Month: 10 things to know in 2025"

자료: Aon(2025. 5. 14), "Cyber Risk Insurance Market Remains Buyer-Friendly"

○ 이러한 공격빈도, 피해규모 및 범위의 확대와 함께 최근의 사이버 리스크 발생 양상은 시스템적 특성(Systemic feature)을 나타내고 있음

- 시스템적 리스크(Systemic risk)는 하나의 사건으로 인해 시스템 내 다수의 경제 주체로의 광범위한 피해를 유발할 수 있는 리스크를 의미함
- 여기서 시스템은 산업시스템, 경제시스템, 금융시장 시스템 등 다수의 주체를 아우르는 개념이며¹⁾, 시스템적 리스크는 2008년 금융위기 이후 글로벌 금융시스템 붕괴 현상을 지칭하는 개념으로 활용됨
- 유럽연합의 시스템적 리스크 위원회(European Systemic Risk Board; ESRB)는 시스템적 사이버 리스크가 시스템적 리스크의 한 종류이며, 시장 및 실물 경제에 부정적인 결과를 초래할 수 있는 특정 산업에서의 사이버 사고를 시스템적 사이버 사고라고 정의함²⁾

1) Forscey, D., Bateman, J., Beecroft, N., and Woods, B.(2022), "Systemic cyber risk: A primer", Washington D.C: Carnegie Endowment for International Peace

2) European Systemic Risk Board(ESRB)(2020), "Systemic cyber risk. Frankfurt: European Commission"

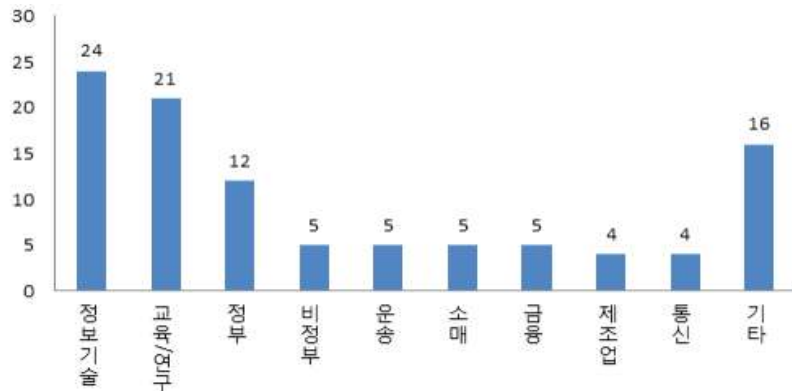
- 빈번한 사이버 공격과 시스템적 특성은 사이버 리스크에 대한 부보가능성(Insurability)을 저하시켜, 보험산업의 위험인수 역량을 약화시킬 우려가 있음
 - 코로나19 이후 산업 전반에서 사이버 리스크 노출이 커지면서 글로벌 사이버보험 시장 성장세가 두드러졌으나, 최근 대형 사이버 사고(예: CrowdStrike 윈도우 보안 프로그램 업데이트 오류로 인한 기업휴지, AT&T의 약 1억 명 개인정보 유출 등)의 빈번한 발생은 사이버 리스크 인수에 대한 회의적 시각을 확대함
 - 이를 극복하기 위해서는 공급 측면에서의 사이버 리스크 인수 역량 강화, 수요 측면에서의 사이버 리스크 관리에 관한 최적 의사결정 전략 수립, 공공부문에서의 시장 생태계 조성 등 사이버보험 시장의 수요과 공급이 균형을 이루기 위한 노력이 필요함
 - 특히, 사이버보험 시장 활성화를 위한 정책지원, 보안 규제 강화 등 공공부문에서의 노력이 병행되어야 사회 전반의 사이버 리스크 경감 효과를 가져올 수 있음
- 본고에서는 시스템적 사이버 리스크 발생 양상 및 증가하는 사이버 리스크에 대한 보험산업의 대응 전략을 살펴보고, 사이버 리스크 관리 역량 제고를 위한 정책적 제언을 하고자 함

2. 시스템적 사이버 리스크 양상과 사이버보험 시장

- 시스템적 사이버 리스크를 촉발하는 주요 유형 중 하나는 단연 랜섬웨어(Ransomware) 공격임
 - 팔로알토 네트워크(Palo Alto Networks)라는 미국 보안회사의 2022년 통계에 따르면 보고된 사이버 손실사건의 가장 많은 유형이 랜섬웨어(전체의 36%) 공격에 의한 것으로 확인됨
 - 유럽 정보보호전문기관(ENISA)의 2022년 보고서에 따르면 주로 컴퓨터 시스템을 인질로 하여 비트코인이나 현금을 요구한 랜섬웨어 공격 중 60% 이상의 피해기업이 실제 대가를 지불하였음
 - Munich Re에 따르면 코로나19이후 2023년 1분기까지 서비스 산업, 제조업, 전자상거래, 헬스케어 및 의료 산업이 랜섬웨어 공격의 주요 타겟이며, 높은 가치를 내재하고 있는 기업 정보를 포함하여 광범위한 개인정보(금융, 소비행태, 생체정보 등) 노출이 상대적으로 높은 업종 중심으로 공격이 이루어졌다고 밝힘
- 지정학적 갈등과 충돌(Geopolitical conflict) 또한 시스템적 사이버 리스크를 촉발하는 요인으로 볼 수 있음
 - 최근 몇 년간 국제 정세는 러시아-우크라이나 전쟁, 이스라엘-팔레스타인 전쟁 등 국지적 갈등이 표면화되고, 보호무역주의의 확대로 인해 분절화(Fragmentation) 추세로 흘러가고 있음
 - 이로 인해 갈등의 골이 깊었던 지역에서의 물리적 충돌이 격화되고 국가지원 사이버 공격(State-backed cyberattacks)이 더욱 활발해지고 있는데, 이들의 주요 타겟 산업은 정보기술, 국가전략/싱크테크 기관, 교육기관 등에 집중됨(그림 3) 참조

〈그림 3〉 국가지원 사이버 공격자의 주요 공격대상 산업분포

(단위: %)



자료: Microsoft Nation State Notification Data(2024), "Microsoft Digital Defense Report 2024"

○ 국내에서 발생한 쿠팡 및 주요 통신사의 개인정보 유출 사고는 독점(또는 과점)적 지위에 있는 기업의 사이버 보안 실패가 2차·3차 피해를 유발할 수 있는 새로운 형태의 시스템적 사이버 리스크라고 볼 수 있음

- 소위 빅테크·플랫폼 집중 시장 구조에서 독점적 지위에 있는 기업이 사이버 보안에 실패하여 사실상 대다수 국민의 개인정보가 유출되는 사고는 특정 기업/산업을 넘어서 금융·실물·사회 시스템 전체에 광범위한 충격을 줄 수 있다는 점에서 시스템적 사이버 리스크의 특성을 가지고 있음
 - 실물 경제의 일시적 마비, 사회적 불안 정세 강화, 피해기업의 주주가치 훼손과 주식시장 교란 등 사회 전반으로의 부정적 결과를 초래할 수 있음
 - 특히, 유출된 개인정보를 활용하여 피싱(Phishing)·스미싱(SMiShing)³⁾ 등의 사이버 공격이 정밀화되고, 금융사기·명의도용·계정탈취 등 정보유출 피해 개인의 금융 자산으로까지 연쇄적 접근이 가능해져 2·3차 금융 피해를 유발할 가능성이 있음
 - Porcedda(2023)⁴⁾은 데이터 유출 범죄가 개인정보 거래, 거짓 신고(Swatting) 등 다양한 추가 범죄를 유발하는 연쇄적 효과(Cascading effect)를 내재하고 있음을 주장함

○ 특정 빅테크 플랫폼이 실질적인 사회 인프라가 된다면, 해당 플랫폼으로의 대형 사이버 사고는 전통적인 금융산업의 시스템적 리스크와 유사한 성격을 가질 수 있음

- 최근 다수의 학술문헌은 빅테크 또는 대형 디지털 플랫폼 기업이 가지는 시스템적 중요성을 강조하고 있음
 - Werbach and Zaring(2022)⁵⁾은 시스템적으로 중요한 기술(Systemically important technology) 개념을 제시하며, 빅테크 플랫폼의 데이터 유출이 금융규제에서 말하는 시스템적 리스크와 유사한 성격을 가질 수 있음을 논증함

3) 스미싱(SMiShing)은 SMS와 피싱의 합성어로서 휴대폰의 텍스트 메시지를 통해 악성 바이러스를 주입하여 개인정보를 탈취하거나 다른 휴대폰으로 확산시키는 새로운 해킹 기법임

4) Porcedda, M. G.(2023), "Sentencing data-driven cybercrime. How data crime with cascading effects is tackled by UK courts", *Computer Law & Security Review*, 48, 105793

5) Werbach, K., and Zaring, D.(2022), "Systemically Important Technology", *Texas. Law Review*, 101(4), pp. 811~875

- Jones and Samples(2023)⁶)은 디지털 플랫폼이 시스템적으로 중요한 인프라가 되는 매커니즘을 분석하면서 독점적 혹은 과점적 플랫폼의 실패가 구조적 리스크로 이어지는 경로를 논함
- Curran(2023)⁷)은 미국 신용평가사 Equifax의 대규모 개인정보 유출 사례를 통해 데이터 브로커(Data broker) 및 신용정보 회사의 사고가 어떻게 시스템적 디지털 리스크로 작동할 수 있는지를 설명함
- 결국 빅테크 및 대형 디지털 플랫폼 사업자가 보유한 디지털 기술을 시스템적으로 중요한 기술로 바라보면서, 이러한 기술과 그들이 가진 시장 지위를 사회적 인프라로 인식하는 것이 중요함

○ 이렇듯 증가하는 사이버 공격과 시스템적 피해에 대응하여 사이버보험 시장은 미국을 중심으로 빠르게 성장해 왔음

- 팬데믹 이전 사이버보험 시장은 가입자가 증가하고 있으나 보험청구가 많지 않아 수익성이 매우 높은 시장으로 알려졌으나, 최근 위험 노출이 급격히 증가하고, 가입자 수와 청구 건수가 모두 크게 증가하면서 수익성이 다소 악화되고 요율도 빠르게 증가하는 추세임
- 특히, 시스템적 사이버 리스크 노출 증가는 시장 내 위험인지(Risk awareness)를 제고하면서 공급과 수요를 증가시키는 효과를 가져왔지만 이로 인해 누적위험(Accumulation risk)과 국가지원 사이버 공격 대한 공급 측면에서의 우려 또한 크게 증가시킴
- 이를 극복하기 위한 방안으로 보험시장 확대 정책지원 및 민관협력 프로그램(Public-Private Partnership)의 필요성에 대한 목소리 또한 글로벌 시장 전반에서 커지고 있는 상황임
 - 즉, 정부차원에서의 사이버 보안정책(개인정보 유출신고 및 공시제도 강화, 징벌적 배상책임 제도 강화 등) 지원, 공격자의 기술을 제어할 수 있을 사이버 보안 기술의 발달과 이에 대한 사이버보험 회사의 적극적인 투자 (또는 사이버 보안 전문기업과의 적극적 파트너십)가 병행되어야 함

○ 국내 사이버보험 시장은 여전히 성장세가 더딘 상황이며, 특히 사이버보험 가입 대상인 기업의 정보보안 인식과 정책은 사이버보험 시장의 수요를 억제하는 요인으로 작동하고 있음

- 기업의 경영진이 사이버 보안의 중요성을 정확히 인식하고, 이와 관련한 거버넌스를 보다 체계화할 필요가 있음
- 당국에서도 기업의 내부통제 시스템에 사이버 리스크 관리체계 수립 및 시행 여부를 감독하고 보안 투자에 관한 공시기준을 마련하여 산업 전반의 사이버 보안수준을 상향시키는 제도가 필요함

○ 또한, 개인정보 유출로 인해 발생하는 배상책임액이 크지 않아 기업 입장에서 사이버보험을 가입할 유인이 높지 않음

- 예를 들어, 2014년 발생한 카드사 고객 개인정보 유출 사고와 2016년 발생한 인터파크 고객 개인정보 유출 사고의 최종 배상책임 판결액은 소송에 참가한 고객 대상으로 1인당 10만 원 수준에 그쳤음

6) Jones, L. S., and Samples, T. R.(2023), "On the systemic importance of digital platforms", *University of Pennsylvania Journal of Business Law*, 25(1), pp. 141~207

7) Curran, D.(2023), "Surveillance capitalism and systemic digital risk: The imperative to collect and connect and the risks of interconnectedness", *Big Data & Society*, 10(1), 20539517231177621

- 올해부터 적용된 개인정보 보호법의 과징금 기준이 매출액 3%로 상향되었으나, 피해 고객에의 실질적 보상으로서 배상책임액은 여전히 매우 제한적이라는 점에서 민사배상 리스크가 매우 낮고 이는 보험 가입 유인을 저해할 수 있음

3. 시사점

- 대규모 개인정보 유출 사고, 국가 기반시설로의 사이버 공격, 랜섬웨어에 의한 전산망 마비 등 시스템적 사이버 리스크 사건에 효과적으로 대응하기 위해서는 기업, 보험산업, 정부의 공동 노력이 요구됨
 - 전사적 리스크 관리체계의 고도화를 통해 전사적 사이버 리스크 관리체계의 구축과 발전이 필요함
 - 위험평가 및 언더라이팅 역량 제고를 위한 사이버 보안 전문성 확보, 배상책임 및 Public Relations(대민 관계) 관리, 사이버 손해사정 기능 강화 등 보험회사의 사이버 리스크 관리 모델 고도화가 필요함
 - 징벌적 개인정보 유출 배상책임 제도 구축, 공사협력 (재)보험 제도 구축, 사이버 리스크 스트레스 테스트 도입 검토 등 공공부문에서의 사이버 리스크 대응 정책을 신속히 수립할 필요가 있음
- 전사적 사이버 리스크 관리체계 확립의 핵심은 리스크 관리 의사결정 체계화 및 효율화, 지배구조에서의 전문성 강화임
 - 기업은 사이버 보안을 더 이상 기업의 매몰비용으로 인식하는 것이 아니라 기업가치를 높이는 전략적 도구로 활용할 수 있음을 인지할 필요가 있음
 - 기업의 내부통제 체계하에서 사이버 리스크를 유발하는 경제적 시나리오를 구축하고 예상 손실을 추정하는 정량적 리스크 관리 전략이 필요함
 - 또한, 기업의 디지털 전환, AI 성장 전략과 잠재적인 사이버 리스크 간 관계를 경영진이 이해하고, 디지털 전략과 사이버 리스크 관리체계 발전 전략을 연계할 필요가 있음
 - CRO(최고리스크책임자) 및 CISO(최고정보보안책임자)의 권한을 강화하고, 기업 내 다양한 기능과 부서 간 상호 연계된 사이버 리스크 관리를 체계화하며, 보안관련 부서와 기능이 충분한 예산 지원과 관심을 받도록 이사회 주요 안건으로 논의해야 함
- 사이버 리스크는 네트워크 특성상 시간이 지날수록 피해가 확산되고 2·3차 피해로 직·간접적 피해자가 증가할 수 있어, 이를 최소화하기 위한 사전적 리스크 관리와 대응 역량 강화가 필요함
 - 이러한 특성은 기존 보험시장에서 담보하는 위험의 특성과 차이가 있으며, 리스크 사건 발생에 따른 결과의 불확실성 크다고 할 수 있음
 - 따라서, 보험회사가 사이버 리스크를 인수하기 위해서는 정보보안 및 언더라이팅 역량 제고를 위한 전문가를 적극 채용하거나 사이버 보안 업체와의 협력을 통한 리스크 관리 컨소시엄 구축하여 사고 발생 가능성 및 발생 시 피해

범위를 억제할 수 있는 리스크 사전 관리 서비스 능력 확보가 필요함

- 또한, 개인정보 유출 신고 의무제도 대응 및 대민 관계 관리를 위하여 공격 발생 여부 탐지, 피해 범위의 신속한 파악 등 사이버 손해사정 역량이 필수적임
- 결론적으로 종합적 사이버 리스크 관리 서비스 공급자로서의 보험회사 정체성을 확고히 하여 사이버보험 시장에서의 공급 역량을 제고할 필요가 있음

○ 사이버보험 시장에서 수요(기업)와 공급(보험회사)의 균형을 확보하고 안정적 성장 기반을 마련해 사회 전반의 사이버 리스크 관리 수준을 높이기 위해서는 공공부문의 적극적인 정책 수립과 지원이 필요함

- 기업의 개인정보 보호에 대한 안일한 인식을 개선하려면 과징금 강화뿐 아니라 배상책임을 확대해, 사이버 리스크 관리 실패가 기업의 재정건전성과 가치에 심각한 손실을 초래할 수 있는 환경을 조성할 필요가 있음
 - 미국의 징벌적 배상책임제도는 사이버 사고로 인한 배상책임을 재무적 충격을 유발할 수 있기 때문에 기업의 사이버보험 수요 확대에 이르고 있으며, 실제 배상책임 판결액이 수천억원 수준에 이르고 있음(예, 2017년 Equifax 개인정보 유출 사고)
 - 거대 과징금과 배상책임액은 기업의 유동성 압박 요인으로 작용할 수 있으며, 현금 조달의 어려움 등으로 보험 가입 유인이 커질 수 있음
 - 또한, 공시제도 강화를 통해 “개인정보 보호 및 사이버 보안 역량 확대 = 주주 가치 제고” 인식을 확대할 필요가 있음
- 또한, 국가지원 사이버 공격(혹은 사이버 테러리즘)이 보험의 면책 사항임을 감안했을 때 국가 재보험 제도 또는 공사협력 보험 프로그램 구축이 필요할 수 있음⁸⁾
 - 미국 재무부는 기존 테러위험 보험 프로그램(Terrorism Risk Insurance Program; TRIP)에 사이버 배상책임을 보장하는 사이버보험을 포함한다는 지침을 발표함
 - 영국 정부 또한 보험회사로부터 테러위험을 수재하는 기존 재보험 프로그램(Pool Re)에 사이버 테러로 인한 기업의 재물 손해 및 영업중단 피해로 보장을 확대함
- 금융당국은 사이버 리스크를 시스템적 리스크로 규정하고 스트레스 테스트 모델을 구축해, 금융·보험회사뿐 아니라 빅테크와 대형 디지털 플랫폼에서 발생할 시스템적 사이버 사고의 금융 영향을 추정할 필요가 있음
 - 앞서 언급한 대규모 개인정보 유출 사고, 국가 기반시설로의 사이버 공격, 랜섬웨어에 의한 전산망 마비 등 극단적 사이버 사고 시나리오를 설정하고, 시나리오별 개인정보 유출 범위, 재무적 손실, 기업휴지 비용, 산업 및 사회경제적 영향 등을 정량적으로 평가해야 함
 - 또한, 시스템적 사이버 사고로 인해 발생할 수 있는 금융·결제 시스템 충격을 평가하고, 금융회사 간 상호연결성 환경 및 사이버 보안 수준에 따라 피해 민감성 평가가 필요함
 - 보험산업의 경우 보험회사의 고객 개인정보 유출 피해 시나리오 평가를 포함하여 언더라이팅 측면에서 사이버 리스크의 영향 범위를 평가함으로써 보험회사 지급여력비율로의 영향을 평가할 필요가 있음

8) 송윤아·홍보배(2021), 『주요국 정부의 사이버보험 시장 참여 배경 및 동향』, 이슈보고서, 보험연구원