2021.11.15

KiRi 리 포 트

포커스

사이버사고의 진화와 사이버보험 시장 동향

송윤아 연구위원

요 약

○ 정보통신기술(ICT)의 발전으로 초연결사회 진입과 함께 사이버공격의 접점이 증가한 상황에서, 최근 사이버공격은 공격자, 표적, 피해양상 등에서 뚜렷한 변화를 보임

- 사이버공격은 비용 및 위험 대비 효과가 큰 대표적인 비대칭 전력으로, 사이버 공격자가 개인 또는 범죄조직에서 테러조직, 준정부조직, 국가로 확대됨
- 사이버공격의 표적도 보안이 취약한 개인 및 중소기업에서 공급망 및 산업제어시스템 공격을 통해 대기업 및 국가기반시설로 확대됨
- 사이버사고의 피해유형은 정보유출 및 개인정보 침해에서 재물·신체·영업중단손해 등으로 확대되고, 단 한 건의 성공한 사이버공격은 거대자연재해 또는 국지적 생화학공격에 준하는 경제적 피해를 초래함

○ 사이버공격의 빈도 및 심도 증가와 기업의 사이버 관련 규제리스크 증가에 따라, 사이버보험 수요가 증가하였으며, 이러한 추세는 사이버사고의 진화와 함께 지속될 것으로 예상됨

- 사이버보험의 청구실적을 보면 제3자에 대한 배상책임손해보다는 당사자손해가 약 80%를 차지하는데, 이로부터 재물·영업중단손해, 방어·복구비용, 랜섬, 벌금 등에 대한 높은 수요를 유추해 볼 수 있음

○ 반면, 사이버리스크의 양적·질적 변화로 인해 동 리스크에 대한 보험 공급은 위축될 것으로 예상됨

- 먼저, 전통적인 기업보험의 사이버면책 확대와 단독 사이버보험의 비포괄성으로 인해, 사이버사고로 인한 재물·신체·영업중단손해에 대한 보장이 감소할 것으로 보임
- 둘째, 2017년 낫페트야 공격으로 국가 배후 사이버공격에 대한 재래식 전쟁 면책 적용 논란이 발생하자, 보험업계는 사이버사고에 적합한 대재해 및 전쟁 면책을 검토 중임
- 셋째, 보험회사의 벌금 및 랜섬 담보 공급이 공공정책에 반한다는 주요국 정부의 입장 발표가 잦아짐에 따라 동 담보 제공에 대한 보험업계의 신중한 접근이 예상됨

○ 국내 기업의 사이버리스크를 면밀히 분석하고 이를 토대로 정책적 대응을 논의해야 할 시점임

- 자연재해나 물리적 테러리즘과 달리, 사이버사고로 인한 피해는 국경이 없고, 손해보험은 업의 속성상 활발한 국경 간 거래가 불가피한 산업이라는 점에서, 전술한 사이버사고와 사이버보험 시장 상황이 특정 국가에 국한된 것은 아님
- 특히, 국내 사이버보험 공급은 세계 보험시장을 선도하는 주요 국가의 보험정책, 손해율, 보험요율, 인수전략 등에 직접적인 영향을 받음

1. 서론

○ 정보통신기술(ICT)의 급속한 발전으로 사람과 사물이 물리·가상공간의 경계 없이 서로 유기적으로 연결되어 상호작용하는 초연결사회로 진입하였으나, 사이버사고의 접점도 그만큼 증가함

- 지난 10월 25일, 85분 가량의 KT 유무선 통신망 마비는 영업중단, 결제시스템 마비, 금융거래 차질, 원격 수업 및 회의 중단 등 큰 혼란과 경제적 피해를 초래하며 초연결사회에서 사이버사고의 위험을 여실히 드러냄

○ 최근에는 인간 및 시스템 오류에 의한 사이버사고보다는 사이버공격이 증가하고 있는데,[1] ICT 기술을 매개로 공격의 강도를 높이고 공격범위를 확장하여, 기업활동 중단은 물론 물리적 자산과 인명을 위협하는 수준에 이름

- 2010년 이란 원자력발전소 공격은 공격자가 국가이며 악성코드로 물리적 시설을 타격한다는 점에서 사이버보안 관점에서는 이정표가 되는 사건으로,[2] 이후 대규모 정전, 생산활동 중단, 시장교란을 야기하는 사이버공격이 빈번해짐
  - 2014년 독일 제철소 생산중단, 2015년 우크라이나 정전, 2017년 워너크라이(WannaCry)·낫페트야(NotPetya) 공격으로 세계적 기업활동 중단, 2019년 세계 최대 알루미늄 제조사 공격으로 알루미늄 가격 급등, 2021년 미국 콜로니얼 파이프라인 송유관 공격으로 일대 휘발유 가격 급등이 있음

○ 본고에서는 최근 사이버사고의 특성을 살펴봄으로써 사이버리스크의 양적·질적 변화를 구체화하고, 이에 대응한 사이버보험의 시장성과·수요·공급·감독기조를 살펴봄으로써 시사점을 도출함

2. 사이버사고의 진화

○ 2010년대 들어 사이버공격은 공격자 및 공격동기, 표적, 피해 유형 및 규모 등에서 뚜렷한 변화를 보임

○ (공격자) 구체적으로, 사이버공격은 비용 및 위험 대비 효과가 큰 대표적인 비대칭 전력으로, 사이버 공격자가 개인 또는 범죄조직에서 테러조직, 준정부조직, 국가로 확대됨

- 초기 정보사회에서는 해킹 능력의 과시욕 및 호기심이 사이버공격의 주된 동기였으나 2010년대 들어서는 경제적 이익, 그리고 정치적·이념적·군사적 동기의 사이버공격이 실행되고 있음

1) 사이버사고는 악의성 없는 사이버사고와 악의적인 사이버사고로 구분 가능하며, 이하에서는 후자만을 지칭 시 사이버공격으로 표현함
2) 미국·이스라엘은 스턱스넷(Stuxnet) 바이러스를 통해 이란 나탄즈 핵시설에 위치한 원심분리기의 잦은 속도변화 및 마모를 유도하여, 고농축 우라늄 원심분리기 교체를 초래함

• 사이버공간에서 국가가 공격자 또는 배후로 참여하여 타국의 안보에 실체적 위협으로 작용하기 시작한 것은 2010년대 들어서임

- 2010년 미국·이스라엘의 이란 핵시설 공격, 2015년 러시아의 우크라이나 배전소 공격, 2017년 북한의 워너크라이 공격, 2017년 러시아의 낫페트야 공격, 2020년 러시아의 솔라윈즈(SolarWinds) 공격[3] 등이 있음[4]
- 우리나라도 2011년 농협전산망 마비, 2013년 3.20 전산대란, 2013년 6.25 DDos 공격, 2014년 한국수력원자력 해킹 등 북한으로부터 지속적인 사이버공격을 받고 있음

○ **(표적) 사이버공격의 표적도 보안이 취약한 개인 및 중소기업에서 공급망 및 산업제어시스템 공격을 통해 대기업 및 국가기반시설로 확대됨**

• 산업제어시스템(Industry Control System; ICS)은 IoT 센서, 인공지능·빅데이터, 5G 등 다양한 정보통신기술(Information Communication Technology; ICT)과의 융합으로 외부 연결이 늘어남에 따라 공격의 표적이 됨[5]

• 특히, 국가기반기설이 전략적 공격 목표로 부상하여 이와 연결된 ICS에 대한 사이버공격이 더욱 증가함

- 금융, 통신, 의료, 교통, 정부시설, 에너지, 상수도, 제조 등 주요기반시설의 불능상태나 파괴는 안보 · 국가경제안보 · 국가보건 및 치안을 약화시킬 수 있음
- 국가기반시설에 대한 ICS 공격은 파괴적 피해를 초래한다는 점에서 금전목적의 범죄조직이나 정치적, 군사적 목적의 테러조직, 나아가 국가단위 공격자에게 가장 매력적인 표적이 됨

• 상대적으로 보안 체계가 강력한 대기업, 금융·안보기관 등을 우회 공격할 수단으로 공급망 공격이 이뤄지는데, 이는 피해사실 인지에 비교적 장시간이 소요됨에 따라 피해 범위 및 규모 확대가 불가피함[6]

- 공급망 공격(Supply chain attack)은 자사의 시스템 및 데이터에 접속할 수 있는 외부 협력업체나 공급업체를 통해 공격자가 시스템에 침투하여 피해를 야기하는 형태의 공격임

○ **(피해) 사이버사고의 피해유형은 정보유출 및 개인정보 침해에서 재물·신체·영업중단손해 등으로 확대되고, 단 한 건의 성공한 사이버공격은 거대자연재해 또는 국지적 생화학공격에 준하는 경제적 피해를 초래함**

• 초기 사이버공격은 정보의 유출, 훼손, 변조, 도용, 개인정보 및 저작권 침해 등이었으나, 최근에는 ICT 기술을 매개로 공격의 강도를 높이고 공격범위를 확장하여 물리적 자산과 인명을 위협하는 수준에 이름(〈그림 1〉 참고)

- ICS에 대한 표적 공격은 물리적인 피해와 직접적으로 연결되어 있어, 영업중단으로 인한 손실, 인명 피해 등을 초래하고, 국가기반시설과 연결된 ICS 공격은 대규모 정전 사태, 방사능 유출, 시장교란으로까지 이어짐[7]

• 2017년 낫페트야 공격은 64개국 이상의 다국적 기업에 100억 달러의 경제적 피해를 초래하였는데, 이는 거대자연

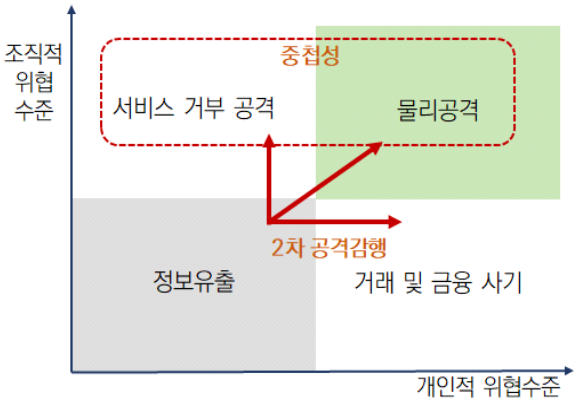
---

3) The White House(2021. 4. 15), "FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government"
4) 지금까지 사이버공격에서 배후로 지목된 국가가 공격을 인정한 사례는 없으며, 주로 피해국 국가기관에서 공격자를 공식 발표함. 국가 단위 주요 사이버공격은 다음을 참고하기 바람; USA Cyberspace Solarium Commission(2020), "A Warning from Tomorrow"; Center For Strategic and International Studies, "Significant Cyber Incidents Since 2006"
5) 최윤성(2021), 「스마트제조 및 산업제어시스템 융합보안 동향」, 『주간기술동향』, 1980호, 정보통신기획평가원
6) 2020년 2월 솔라윈즈 오리온 업데이트 버전에 악성코드가 포함된 이후, 이런 사실이 인지되기까지 약 10개월의 시간이 소요됨
7) 2021년 미국 플로리다에서는 팀뷰어(Teamviewer)를 통해 정수장 제어시설에 접근, 식수의 수산화나트륨 농도를 정량보다 100배 넘게 조작하여 인적 피해 가능성을 보여줌

재해의 경제적 손실액에 버금가는 수준임(〈그림 2〉 참고)

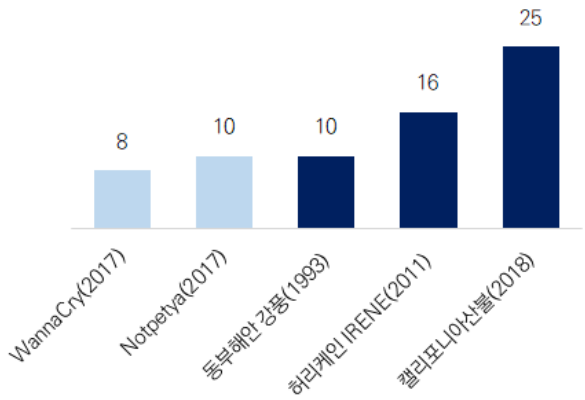
- 이후 연구에 따르면, 미국에서 사이버공격으로 클라우드 사용이 3일간 중단될 경우 미국 내 1,250만 개사에서 150억 달러의 손실이 예상되며,[8] 펌웨어 업데이트 등을 통해 정보통신 장비에 내장된 리튬이온 과열을 유도하여 호주 상업지구에서 대규모 폭발이 일어날 경우 손실액이 국지적 생화학공격에 근접할 것으로 추정됨[9]

〈그림 1〉 사이버사고의 피해유형



자료: 유성민(2016), 「4차 산업혁명과 사이버 보안대책」, 『지능화 연구 시리즈 2016』, 한국정보화진흥원

〈그림 2〉 사이버사고와 자연재해의 피해규모 비교



주: 단위는 10억 달러임
자료: Bateman, J.(2020). "War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions", Carnegie Endowment for International Peace

3. 사이버보험 시장 동향

○ 사이버사고의 진화와 함께, 사이버보험의 시장성과, 수요, 그리고 공급에도 뚜렷한 변화가 관찰됨

○ (상품) 사이버사고는 약관에서 손인(Peril)로 명시적으로 열거하여 담보하거나 포괄위험(All-risk) 담보방식 재물 및 배상책임보험에서 암묵적으로 담보함

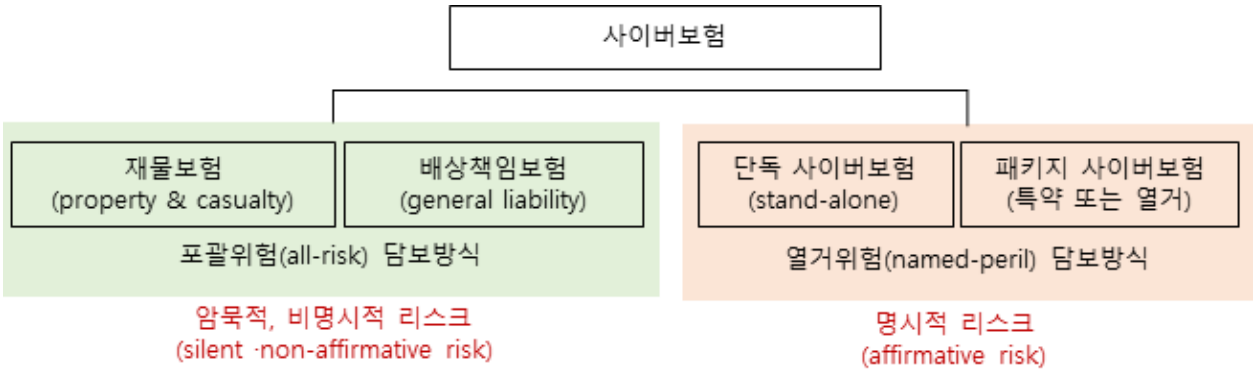
- 보험회사의 사이버담보 제공방식은 크게 다음 3가지로 구분 가능하며, ①과 ②를 명시적(Affirmative) 사이버보험, ③을 암묵적 또는 비명시적(Silent or non-affirmative) 사이버보험이라 함(〈그림 3〉 참고)
  - ① 사이버리스크 전용의 단독 사이버보험(Stand-alone), ② 기존 재물보험 또는 배상책임보험에 사이버리스크에

8) LLoyd's(2018), "Cloud Down: Impacts on the US Economy", Emerging Risk Report
9) ARPC, OECD, and University of Cambridge(2020), "Insurance Risk Assessment of Cyber Terrorism in Australia"

대한 보장을 특약으로 부대하거나 열거위험(Named-peril) 담보방식 기업보험에 사이버담보를 명시적으로 열거하여 보장하는 패키지보험, ③ 포괄위험 담보방식 재물보험과 배상책임보험처럼 사이버리스크에 대한 보상이 명시되어 있지는 않지만 약관상 포함된다고 해석되는 상품임

- 사이버보험은 기업의 직접 손실 및 비용, 그리고 제3자에 대한 배상책임손해를 보장함(〈표 1〉 참고)
  - 포괄위험 담보방식 재물보험과 배상책임보험은 각각 사이버사고로 인한 재물손해와 배상책임손해를 보장함
- 미국에서는 사이버사고 증가와 2002년 미국 캘리포니아를 시작으로 개인정보유출에 대한 통지의무와 처벌을 담은 법규 도입으로,[10] 명시적 사이버보험이 본격적으로 판매된 반면 나머지 지역에서는 암묵적 사이버담보에 의존함
  - 2019년 기준 미국이 명시적 사이버보험 원수보험료의 90% 이상을 차지함

〈그림 3〉 사이버담보 제공방식



자료: 저자 작성

〈표 1〉 기업의 사이버리스크

당사자		제3자
직접손실	비용	
• 금융 도난 및 사기 • 지적재산 도난 • 영업중단손해 • 사이버협박 • 평판손실 • 물적 자산 손실	• 법률비용 • 계약상 벌과금 • IT 포렌식 • 통지 • 데이터 및 소프트웨어 손실 • 평판손실 관리 • 물적 자산 손실로 인한 비용	• 데이터침해 배상책임 • 금융 도난 및 사기 배상책임 • 네트워크 서비스 실패 배상책임 • 지적재산 도난 배상책임 • 인격권 침해 배상책임 • D&O 배상책임 • 일반자산손실 배상책임

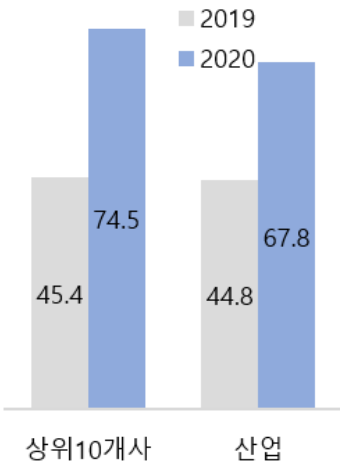
자료: Wrede, D., Stegen, T., and Johann-Matthias Graf von der Schulenburg(2020), "Affirmative and Silent Cyber Coverage in Traditional Insurance Policies: Qualitative Content Analysis of Selected Insurance Products from the German Insurance Market", *The Geneva Papers on Risk and Insurance-Issues and Practice*, 45, pp. 657~689

10) 2002년 미국 캘리포니아 주는 개인정보를 유출시킨 기업이 정보주체와 감독기관에 그 사실을 즉각 통보하도록 하고 불이행시 범칙금 부과, 사적소송 제기근거 입법화하였고(California Security Breach Notification Act 2002, California SB 1386), 이후 전 세계적으로 이러한 입법례가 증가함

○ (성과) 2010년대 중반 들어 명시적 사이버보험의 손해율과 요율이 급격히 증가함

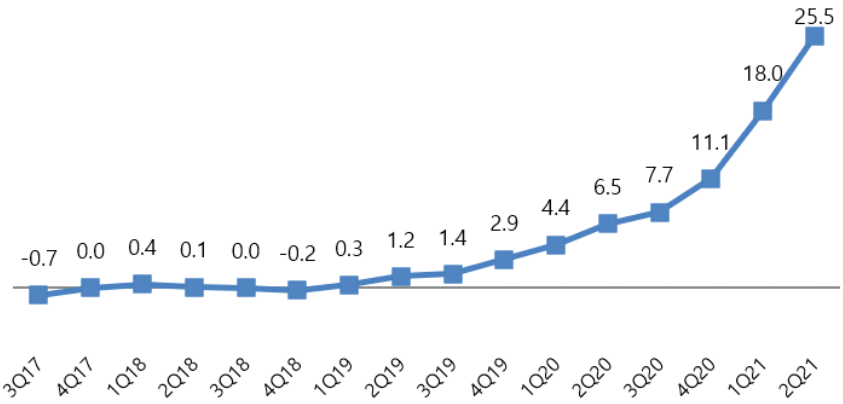
- 명시적 사이버보험 시장의 손해율은 2019년 44.8%에서 2020년 67.8%로, 23%p 증가함(〈그림 4〉 참고)
- 명시적 사이버보험 요율의 전분기 대비 증가율은 2019년 1.2%에서 불과 2년 만인 2021년 2분기에는 25.5%로, 보험요율이 빠른 속도로 증가함(〈그림 5〉 참고)

〈그림 4〉 명시적 사이버보험 손해율



주: 미국 시장 기준이며, 단위는 %임
자료: AM Best(2021), "Identified Challenges and Supervisory Considerations for Sustainable Market Development"

〈그림 5〉 명시적 사이버보험의 분기별 요율 변화율



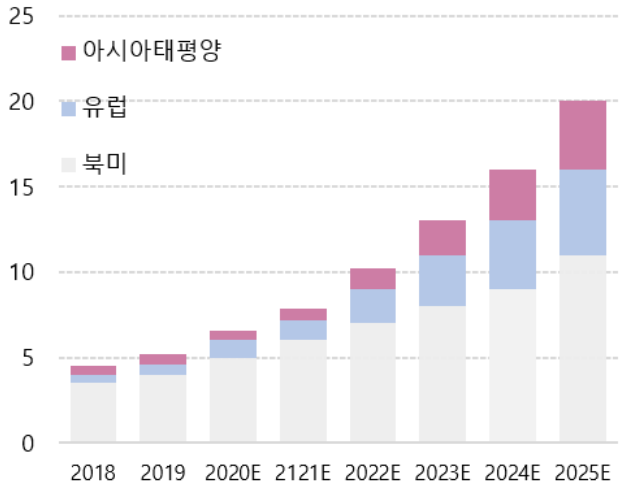
주: 미국 시장 기준이며, 단위는 %임
자료: Council of Insurance Agents&Brokers(2021), "Commercial Property·Casualty Market Index Q2/2021"

○ (수요) 2010년 중반 들어 랜섬웨어 공격의 빈도 및 심도 증가와 기업의 사이버관련 규제리스크 증가에 따라, 사이버보험 수요가 급증하였으며, 이러한 추세는 사이버사고의 진화와 함께 지속될 것으로 예상됨

- 개인정보보호 관련법 위반에 대한 벌금 대폭 상향, 대규모 피해의 랜섬웨어 공격, 사이버공격 빈도 및 심도 증가 등으로 보험가입 및 원수보험료가 증가함(〈그림 6〉 참고)
  - 명시적 사이버보험의 청구건수는 제3자에 대한 배상책임손해보다는 당사자손해가 약 80%를 차지하는데, 이로부터 재물·영업중단손해, 랜섬, 방어·복구비용, 벌금 등에 대한 높은 수요를 유추해 볼 수 있음(〈그림 7〉 참고)
- 2017년 이전까지는 사이버보험 지급보험금 중 랜섬과 사이버협박에 대한 보험금이 10~20% 수준이었으나, 2017년 워너크라이와 낫페트야 공격으로 21~31% 수준으로 증가함[11)]
- 개인정보보호법 중대위반에 대한 벌금의 상향조정은 국제적 흐름으로, 기업들의 벌금담보 수요가 높음
  - 유럽은 2018년 GDPR(General Data Protection Regulation; 일반개인정보보호법)을 시행, 중대위반에 대해서는 전 세계 매출액의 4% 또는 2천만 유로로 상향하였으며, 우리나라도 '관련' 매출액의 3%에서 '전체' 매출액의 3%로 상향하는 방안이 논의되고 있음[12)]

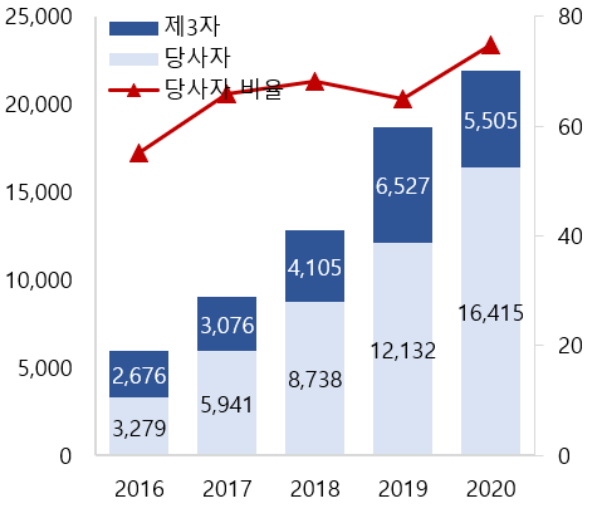
11) OECD(2020), "Insurance Coverage for Cyber Terrorism in Australia", OECD, Paris

〈그림 6〉 명시적 사이버보험 원수보험료



주: 단위는 10억 달러임
자료: IAIS(2020), "Cyber Risk Underwritin: Identified Challenges and Supervisory Considerations for Sustainable Market Development"

〈그림 7〉 명시적 사이버보험의 청구건수



주: 미국 시장 기준이며, 단위는 건, %임
자료: AM Best(2021), "Identified Challenges and Supervisory Considerations for Sustainable Market Development"

○ (공급) 사이버리스크의 양적·질적 변화로 인해 사이버리스크에 대한 보험담보 공급이 위축될 것으로 예상됨

- 구체적으로 먼저, 보험업계는 그 동안 사이버사고의 집합리스크와 꼬리리스크 과소평가, 암묵적 사이버보험의 언더라이팅 리스크 과소평가 등을 인지하고[13] 최근 자발적으로 인수심사를 강화하고 보험가입 금액을 축소함[14]
- 둘째, 포괄위험 담보방식 재물·배상책임보험 내 사이버면책 확대 움직임이 있으며, 이는 사이버사고로 인한 보험회사의 재물·영업중단·배상책임손해를 면책함
  - 영국 건전성감독청은 2021년까지 기존 포괄위험 담보방식 재물·배상책임보험과 특약재보험 약관에 사이버사고 면책여부를 명시적으로 표기하도록 함
  - 미국 대부분의 주는 2014년 영업배상책임보험에 사이버사고 면책을 반영, 2021년 2월부터 재물보험에 사이버사고 면책 조항을 의무적으로 추가하도록 함
- 셋째, 실제 시장에서 거래되는 단독 사이버보험은 정보유출 관련 배상책임과 랜섬 및 비용 담보에 집중하는 반면,

12) GDPR 시행 이전, 영국의 경우 벌금이 50만 파운드에 불과함. 최근 호주도 개인정보보호 관련법 위반에 대한 벌금을 210만 호주 달러에서 Max(1천만 호주 달러, 부당이득의 3배, 매출액의 10%)로 상향하는 방안을 논의 중으로, 자국 기업의 역차별 방지를 위해 개인정보보호 관련법 위반에 대한 벌금의 국제적 수렴이 불가피함

13) EIOPA: European Insurance and Occupational Pensions Authority(2018), "Understanding Cyber Insurance – A Structured Dialogue with Insurance Companies"; U.K. Prudential Regulation Authority(2017), "Cyber Insurance Underwriting Risk", Policy Statement PS15/17(July), Bank of England

14) Government Accountability Office(2021), "Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market", Report to Congressional Committee, GAO-21-477

재물손해, 신체상해, 금융도난, 정신적 손해 등에 대한 보장이 현저히 낮음[15]

- 넷째, 2017년 낫페트야 공격으로 국가 배후 사이버공격에 대한 재래식 전쟁 면책 적용 논란이 발생하자, 보험업계는 사이버사고에 적합한 대재해 및 전쟁 면책을 검토 중임[16]
  - 보험회사가 낫페트야 공격을 국가차원의 적대적 전쟁행위로 보아 보험약관에 규정된 전쟁면책 적용을 주장하며 보험금 지급을 거절하자, 세계적 제약회사 머크(Merck&Co)와 미국 식품 대기업 멘델레즈(Mondelez)는 2018년 10월 보험회사를 상대로 계약불이행 확인 소송을 제기하였으며, 법원에 계류 중임[17]
  - 키네틱전(Kinetic war)과 달리, 사이버전은 공격자를 특정하기 어려운 데다, 공격자를 특정하더라도 공격자와 특정 국가와의 관계를 규명하기 어렵고 사이버공간에서의 행위를 적대행위 또는 전쟁행위로 규정하기 어렵다는 점에서, 재래식 전쟁면책 적용에 한계가 있음[18]
- 다섯째, 개인정보보호법 위반에 따른 벌금이 사후적 처벌보다는 사전적 억제의 성격이 강하다는 점에서, 보험회사의 벌금담보 제공이 법적 조치를 무력화하는 등 공공정책에 반할 수 있다고 보아 이를 대체로 금지함
  - 노르웨이, 슬로바키아, 스웨덴을 제외한 모든 유럽 국가는 보험회사의 벌금담보 제공을 암묵적·명시적으로 금지하며, 미국은 주마다 상이함[19]
  - 사이버사고는 방어보다는 공격이 용이하다는 점, 기업의 벌금부담이 가볍지 않다는 점, 그리고 국제적 정합성이 필요하다는 점에서 OECD를 중심으로 추가 논의가 전개될 것으로 예상됨[20]
- 마지막으로, 보험회사의 랜섬담보가 공공정책에 반할 뿐만 아니라 랜섬웨어 공격을 자극할 수 있다는 경고가 빈번해짐에 따라, 동 담보에 대한 보험업계의 신중한 접근이 예상됨
  - 미국 재무부 내 해외자산통제국(Office of Foreign Assets Control; OFAC)은 2020년 10월, OFAC 제재 대상과 연관 단체에 랜섬을 지급하는 것을 '국가 안보 이익을 위협 하는 행위'로 규정하고, 해당자에 랜섬 지급전 OFAC 승인을 받도록 함[21]
  - 프랑스 국가안보보안국(ANSSI)은 랜섬웨어 공격자들이 사이버보험을 구입한 기업을 표적으로 삼는다는 점에서, 보험회사의 랜섬웨어 담보 제공이 그로 인한 피해를 확대시킨다고 경고하였으며,[22] 프랑스 손해보험회사 AXA는 2021년 5월 프랑스 내 랜섬웨어 담보 제공 중단을 발표함[23]

---

15) OECD(2020), "Insurance Coverage for Cyber Terrorism in Australia", OECD, Paris France
16) 제네바협회(Geneva Association; GA)와 국제 테러리즘 리스크 보험풀 포럼(International Forum of Terrorism Risk (Re)Insurance Pools; IFTRIP)이 2020년부터 작업 중이며, 검토 내용을 지금까지 세 차례에 걸쳐 공개함
17) 2017년 낫페트야 공격은 러시아가 회계프로그램 미독의 업데이트 서버에 침투, 악성코드를 전파하고 시스템을 파괴하여, 64개국 이상의 다국적 기업에 피해를 입힌 사건으로, 보험산업 관점에서는 ① 사이버리스크의 지리적 위험분산 불가 확인, ② 사이버 대재해 현실화, ③ 사이버전쟁 면책 촉발 등의 의미를 가짐
18) 일반적인 전쟁면책 문구는 다음과 같음. "동 보험증권은 그 원인이 무엇이든 다음의 사고로 인해 직간접적으로 발생한 손실을 면책한다: 전시 또는 평화 시 적대적 또는 전쟁 행위(Hostile or warlike action)로서, ① 정부 또는 (법상 또는 사실상) 주권을 가진 조직, ② 육군, 해군, 공군, ③ ① 또는 ②의 대리인 등에 의해 실제 발생한, 임박한, 또는 향후 예상되는 공격을 저지·전투·방어하는 것을 포함한다."
19) 영국에서는 불법원인급여 법리(Ex turpi causa)에 따라 벌금담보 제공을 금지하며, FCA Handbook에서 이를 명문화함; FCA Handbook GEN 6.1.5(Insurance against financial penalties)
20) 2020년 OECD에서 한 차례 논의가 있었음; OECD (2020), "Encouraging Clarity in Cyber Insurance Coverage: The Role of Public Policy and Regulation", OECD, Paris France
21) 국제긴급경제권한법(International Emergency Economic Powers Act; IEEPA)과 적성국교역법(Trading With the Enemy Act; TWEA)에 의거, 미국인과 단체들은 제재 대상자와 포괄적 제재를 받고 있는 북한 등과의 직·간접적인 거래가 금지됨
22) ANSSI: Agence Nationale De La Sécurité Des Systèmes D'Information(2021), "Etat De La Menace Rançongiciel"
23) 프랑스 사법부와 ANSSI는 보험회사의 랜섬담보가 자금세탁금지와 테러리즘 자금지원 관련 법 위반 소지가 있다고 경고함

4. 결론

○ 사이버공격의 진화와 함께 사이버보험에 대한 기업의 수요는 증가한 반면 보험업계의 공급은 위축됨에 따라, 향후 주요 손해유형에 대한 보장공백이 불가피할 것으로 보임

- 특히, 사이버사고로 인한 재물·신체·영업중단손해, 무형자산 손해, 물리적 손실이 동반되지 않은 영업중단손해 등에 대한 보장공백이 두드러짐

○ 국내 기업의 사이버리스크를 면밀히 분석하고, 이를 토대로 정책적 대응을 논의해야 할 시점임

- 자연재해나 물리적 테러리즘과 달리, 사이버사고로 인한 피해는 국경이 없고, 손해보험은 업의 속성상 활발한 국경 간 거래가 불가피한 산업이라는 점에서, 전술한 사이버리스크 및 사이버보험 시장 상황이 특정 국가에 국한된 것은 아님
- 특히, 국내 사이버보험 공급은 세계 보험시장을 선도하는 주요 국가의 보험정책, 손해율, 보험요율, 인수전략 등에 직접적인 영향을 받음